Cisco Identity Services Engine リリース 3.4 管理者ガイド

初版：2024 年 8 月 5 日

最終更新：2024 年 8 月 12 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章 新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章 Cisco ISE の概要 7

Cisco ISE の概要 7

Cisco ISE の機能 8

Cisco ISE 管理者 9

CLI 管理者への外部 ID ストアの使用の強制 10

新しい管理者の作成 11

Cisco ISE 管理者グループ 12

管理者グループの作成 21

Cisco ISE への管理アクセス 22

Cisco ISE でのロールベースの管理者アクセス コントロール 23

ロールベースの権限 24

RBAC ポリシー 24

デフォルトのメニュー アクセス権限 24

メニュー アクセス権限の設定 365

データ アクセス権限を付与するための前提条件 365

デフォルトのデータ アクセス権限 366

データ アクセス権限の設定 389

読み取り専用管理ポリシー 390

読み取り専用管理者のメニュー アクセスのカスタマイズ 390

第 3 章 ライセンス 393

Cisco ISE ライセンス 393
階層ライセンス 395
デバイス管理ライセンス 397
評価ライセンス 397
Cisco ISE スマート ライセンス 398
スマートライセンスの登録とアクティブ化 399
Cisco ISE でのスマートライセンスの管理 400
トラブルシューティング：未登録ライセンスの使用 401
エアギャップネットワークのスマートライセンス 402
スマートライセンス用の Smart Software Manager オンプレミスの設定 403
特定ライセンス予約 404
特定ライセンス予約の有効化 407
特定ライセンス予約の更新 409
特定ライセンス予約の返却 410

第 4 章

Cisco ISE の展開 413
Cisco ISE デプロイメントの用語 414
分散 Cisco ISE 展開のペルソナ 414
Cisco ISE ノードの設定 414
プライマリポリシー管理ノード（PAN）の設定 415
セカンダリ Cisco ISE ノードの登録 416
複数の展開シナリオのサポート 417
Cisco ISE 分散展開 418
Cisco ISE 展開の設定 418
プライマリ Cisco ISE ノードからセカンダリ Cisco ISE ノードへのデータ レプリケーション 418
Cisco ISE ノードの登録解除 419
Cisco ISE 展開でのノードのステータス 420
分散展開を設定する場合のガイドライン 422
プライマリ ノードおよびセカンダリ ノードで使用可能なメニュー オプション 423
展開とノードの設定 424

展開ノードリストウィンドウ 424
ノードの一般設定 425
プロファイリング ノードの設定 431
ロギングの設定 434
リモート ロギング ターゲットの設定 434
セキュア Syslog ターゲット接続のためのクライアント認証の設定 436
ロギングカテゴリの設定 437
管理者アクセスの設定 438
管理者パスワード ポリシーの設定 438
セッション タイムアウトおよびセッション情報の設定 440
管理ノード 441
管理ノードの高可用性 441
ハイアベイラビリティのヘルスチェックノード 443
ヘルスチェックノード 444
セカンダリ PAN への自動フェールオーバー 445
自動フェールオーバーが回避された場合のシナリオ例 446
PAN 自動フェールオーバー機能の影響を受ける機能 447
自動フェールオーバー用のプライマリ PAN の設定 448
セカンダリ PAN のプライマリへの手動昇格 449
新しい Cisco ISE 展開での既存の Cisco ISE 展開のノードのプライマリ PAN としての再利用 450
プライマリ PAN にサービスを復元 450
管理ノードの自動フェールオーバーのサポート 450
ポリシー サービス ノード 451
ポリシー サービス ノードのハイ アベイラビリティ 451
PSN 間で均等に要求を分散するためのロードバランサ 452
ポリシー サービス ノードでのセッション フェールオーバー 452
ポリシー サービス ノード グループ内のノード数 452
ライト データ ディストリビューション 453
RADIUS セッションディレクトリ 454
エンドポイント オーナー ディレクトリ 454

モニタリング ノード 455
MnT ロールの手動変更 456
Cisco ISE メッセージングサービスを介した syslog 456
MnT ノードでの自動フェールオーバー 458
モニタリング データベース 460
モニタリングデータベースのバックアップと復元 460
モニタリングデータベースの消去 460
モニタリングデータベースの消去に関するガイドライン 461
運用データの消去 461
古い運用データの消去 462
自動フェールオーバー用の MnT ノードの設定 463
Cisco pxGridノード 464
Cisco pxGrid ノードの展開 466
Cisco pxGrid の設定 466
Cisco pxGrid 証明書の生成 467
Cisco pxGrid クライアントの権限の制御 469
pxGrid の操作とサービスのユースケース 471
展開内のノードの表示 472
MnT ノードからのエンドポイント統計データのダウンロード 472
データベースのクラッシュまたはファイルの破損の問題 473
モニタリングのためのデバイス設定 473
プライマリおよびセカンダリの Cisco ISE ノードの同期 473
ノード ペルソナとサービスの変更 474
Cisco ISE でのノードの変更による影響 474
ポリシー サービス ノード グループの作成 475
展開からのノードの削除 476
Cisco ISE ノードのシャットダウン 477
ノードを再登録する必要があるシナリオ 478
スタンドアロン Cisco ISE ノードのホスト名または IP アドレスの変更 479

第 5 章 基本的なセットアップ 481

管理ポータル 482
インタラクティブヘルプ 490
カスタマー エクスペリエンス アンケート 491
デフォルトモードまたはダークモードの適用 491
Cisco ISE ホームのダッシュボード 492
ホーム ダッシュボードの設定 493
[コンテキストの可視性（Context Visibility）] のビュー 494
コンテキストの可視性の属性 496
アプリケーション ダッシュボード 497
ハードウェア ダッシュボード 499
ダッシュレット 502
ビューに表示するデータのフィルタリング 503
カスタムフィルタの作成 504
拡張フィルタを使用した条件によるデータのフィルタリング 504
クイックフィルタを使用したフィールド属性によるデータのフィルタリング 505
ダッシュレットビューでのエンドポイントアクション 505
Cisco ISE ダッシュボード 506
Cisco ISE 国際化およびローカリゼーション 510
サポートされている言語 510
エンドユーザー Web ポータルのローカリゼーション 511
UTF-8 文字データ エントリのサポート 511
UTF-8 クレデンシャル認証 511
UTF-8 ポリシーおよびポスチャ評価 512
サプリカントに送信されるメッセージの UTF-8 サポート 512
レポートおよびアラートの UTF-8 サポート 512
ポータルでの UTF-8 文字のサポート 513
Cisco ISE ユーザーインターフェイス以外での UTF-8 サポート 516
UTF-8 の値のインポートおよびエクスポートのサポート 517
REST での UTF-8 サポート 517
ID ストアの許可データの UTF-8 サポート 517
MAC アドレスの正規化 517

Cisco ISE 展開のアップグレード 518
管理者アクセス コンソール 519
管理者ログインブラウザのサポート 519
ログインの試行による管理者のロックアウト 519
Cisco ISE でのプロキシの設定 520
管理ポータルで使用されるポート 521
Cisco ISE アプリケーション プログラミング インターフェイス ゲートウェイの設定 521
API サービスの有効化 523
API サービスの外部 Active Directory アクセスの有効化 529
外部 RESTful サービスソフトウェア開発キット 530
Data Connect 530
Data Connect ライセンスの要件 531
Data Connect に対する展開変更の影響 531
Data Connect の有効化 532
Data Connect での管理者証明書の使用 533
Data Connect のモニタリング 534
システム時刻とネットワーク タイム プロトコル サーバー設定の指定 535
システムのタイムゾーンの変更 536
通知をサポートするための SMTP サーバーの設定 537
セキュアなロック解除クライアントメカニズムの有効化 538
連邦情報処理標準モードのサポート 540
Cisco ISE での連邦情報処理標準モードの有効化 541
管理者共通アクセスカード認証用の Cisco ISE の設定 542
Diffie-Hellman アルゴリズムを使用したセキュアな SSH キー交換 545
セキュア syslog 送信のための Cisco ISE の設定 545
セキュア syslog リモート ロギング ターゲットの設定 546
リモート ロギング ターゲットの設定 547
セキュア syslog ターゲットに監査可能なイベントを送信するためのロギング カテゴリの有効化 549
ロギングカテゴリの設定 549
TCP syslog コレクタと UDP syslog コレクタの無効化 550

デフォルトのセキュア syslog コレクタ 551
オフライン メンテナンス 552
エンドポイント ログイン クレデンシャルの設定 553
Cisco ISE でのホスト名の変更 553
Cisco ISE での証明書の管理 554
セキュアなアクセスを可能にするための Cisco ISE での証明書の設定 554
証明書の使用 555
Cisco ISE の証明書の一致 558
X.509 証明書の有効性 558
Cisco ISE での公開キーインフラストラクチャの有効化 559
ワイルドカード証明書 560
Cisco ISE のワイルドカード証明書のサポート 561
HTTPS と拡張認証プロトコル通信用のワイルドカード証明書 561
URL リダイレクションの完全修飾ドメイン名 562
ワイルドカード証明書を使用する利点 563
ワイルドカード証明書を使用することの欠点 564
ワイルドカード証明書の互換性 564
証明書階層 565
システム証明書 565
システム証明書の表示 567
管理証明書更新後のアプリケーション再起動のスケジュール設定 568
システム証明書のインポート 569
システム証明書のインポート設定 570
自己署名証明書の生成 572
自己署名証明書の設定 572
システム証明書の編集 574
システム証明書の削除 576
システム証明書のエクスポート 577
信頼できる証明書ストア 577
信頼できる証明書ストアの証明書 579
信頼できる証明書のリスト 579

信頼できる証明書の命名の制約 580
信頼できる証明書の表示 582
信頼できる証明書ストアの証明書のステータス変更 582
信頼できる証明書ストアへの証明書の追加 582
信頼できる証明書の編集 583
信頼できる証明書の設定 583
信頼できる証明書の削除 586
信頼できる証明書ストアからの証明書のエクスポート 587
信頼できる証明書ストアへのルート証明書のインポート 587
信頼できる証明書のインポート設定 588
証明書チェーンのインポート 589
Cisco ISE ノード間通信の信頼できる証明書のインストール 590
Cisco ISE でのデフォルトの信頼できる証明書 591
古いシステムと信頼できる証明書 595
証明書署名要求 595
証明書署名要求の作成と認証局への送信 596
証明書署名要求への CA 署名付き証明書のバインド 596
証明書署名要求のエクスポート 598
証明書署名要求の設定 598
ポータルで使用する証明書のセットアップ 604
CA 署名付き証明書へのデフォルトのポータル証明書グループ タグの再割り当て 604
ノードの登録前のポータル証明書タグの関連付け 605
ユーザーおよびエンドポイントの証明書の更新 606
ポリシー条件で証明書更新に使用されるディクショナリ属性 607
証明書を更新するための CWA リダイレクト 607
ユーザーによる証明書の更新を許可する Cisco ISE の設定 607
許可されるプロトコルの設定の更新 608
CWA リダイレクションの許可ポリシー プロファイルの作成 608
ゲストポータルでの BYOD 設定の有効化 609
Apple iOS デバイスの証明書更新の失敗 609
証明書定期チェックの設定 609

.pfx ファイルからの証明書と秘密キーの抽出 611
Cisco ISE CA サービス 611
Cisco ISE 証明書フィンガープリント 612
SHA-256 フィンガープリントを使用したポリシーの作成 613
SHA-256 フィンガープリントを使用した認証ポリシーの作成とマッピング 613
認証ポリシーの作成 614
PRRT ログの確認 615
管理ノードとポリシーサービスノードでプロビジョニングされる Cisco ISE CA 証明書 615
Cisco ISE と相互運用するための CA の要件 616
Cisco ISE CA チェーンの再生成 618
外部 CA による Cisco ISE メッセージング証明書のサポート 618
楕円曲線暗号化証明書のサポート 619
Cisco ISE 認証局証明書 621
Cisco ISE CA 証明書の編集 621
Cisco ISE CA 証明書のエクスポート 622
Cisco ISE CA 証明書のインポート 622
証明書テンプレート 623
証明書テンプレート名の拡張子 623
許可ポリシー条件での証明書テンプレート名の使用 623
pxGrid コントローラ用の Cisco ISE CA 証明書の展開 624
BYOD の MAC ランダム化 625
Simple Certificate Enrollment Protocol プロファイル 626
発行された証明書 626
発行および失効した証明書 627
Cisco ISE CA 証明書およびキーのバックアップと復元 628
Cisco ISE CA 証明書およびキーのエクスポート 628
Cisco ISE CA 証明書およびキーのインポート 629
プライマリ PAN および PSN でのルート CA および下位 CA の生成 630
外部 PKI の下位 CA としての Cisco ISE ルート CA の設定 631
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 631
Employee ユーザーグループへのユーザーの追加 632

TLS ベース認証の証明書認証プロファイルの作成 633
TLS ベース認証の ID ソース順序の作成 633
認証局の設定 634
CA テンプレートの作成 635
内部 CA の設定 637
クライアント プロビジョニング ポリシーで使用されるネイティブ サプリカント プロファイルの作成 638
Cisco からの Windows および Mac OS X オペレーティングシステムのエージェントリソースのダウンロード 639
Apple iOS、Android および MAC OS X デバイスのクライアント プロビジョニング ポリシー ルールの作成 639
TLS ベース認証の Dot1X 認証ポリシー ルールの設定 640
中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成 641
許可ポリシー ルールの作成 642
CA サービス ポリシーのリファレンス 642
証明書サービスのクライアント プロビジョニング ポリシー ルール 642
証明書サービスの許可プロファイル 644
証明書サービスの許可ポリシー ルール 645
Cisco ISE CA による ASA VPN ユーザーへの証明書の発行 646
VPN 接続の証明書プロビジョニングフロー 647
ASA VPN ユーザーに証明書を発行する Cisco ISE CA の設定 647
エンドポイント証明書の失効 651
OCSP サービス 652
Cisco ISE CA サービスの Online Certificate Status Protocol 応答側 652
OCSP 証明書のステータスの値 653
OCSP レスポンダ証明書の更新 653
OCSP ハイ アベイラビリティ 654
OCSP の障害 654
OCSP クライアント プロファイルの追加 655
OCSP クライアント プロファイル設定 655
OCSP 統計情報カウンタ 659
管理者のアクセス ポリシーの設定 660

管理者アクセスの設定 661
同時管理セッションとログインバナーの最大数の設定 662
IP アドレスの選択からの Cisco ISE への管理アクセスの許可 662
Cisco ISE の MnT ノードへのアクセスの許可 663
管理者アカウントのパスワード ポリシーの設定 664
管理者アカウントのアカウント無効化ポリシーの設定 665
管理者アカウントのロック設定または一時停止設定 666
管理者のセッション タイムアウトの設定 667
アクティブな管理セッションの終了 667
管理者の名前の変更 667
管理者アクセスの設定 668
管理者パスワード ポリシーの設定 668
セッション タイムアウトおよびセッション情報の設定 670

第 6 章 メンテナンスとモニター 673
適応型ネットワーク制御 674
Cisco ISE での適応型ネットワーク制御の有効化 675
ネットワーク アクセスの設定 675
ANC によるネットワーク アクセスの許可プロファイルの作成 676
ANC NAS ポートのシャットダウン フロー 677
エンドポイントの消去の設定 677
隔離済みエンドポイントがポリシー変更の後に認証を更新しない 679
ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する 679
外部認証された管理者が ANC 操作を実行できない 680
バックアップ データのタイプ 680
バックアップ/復元リポジトリ 681
リポジトリの作成 683
リポジトリの設定 685
SFTP リポジトリでの RSA 公開キー認証の有効化 686
ローカルディスクからのファイルのダウンロード 687
ローカルディスクへのファイルのアップロード 687

オンデマンドおよびスケジュール バックアップ 687
オンデマンド バックアップの実行 688
オンデマンド バックアップの設定 690
バックアップのスケジュール 691
スケジュール バックアップの設定 692
CLI を使用したバックアップ 693
バックアップ履歴 693
バックアップの失敗 694
Cisco ISE 復元操作 694
データの復元に関するガイドライン 695
CLI からの設定またはモニタリング（操作）バックアップの復元 696
GUI からの設定バックアップの復元 698
モニタリング データベースの復元 699
スタンドアロン環境でのモニタリング（運用）バックアップの復元 700
管理およびモニタリングペルソナによるモニタリング バックアップの復元 700
モニタリング ペルソナによるモニタリング バックアップの復元 701
復元履歴 701
認証および許可ポリシー設定のエクスポート 702
ポリシーのエクスポート設定のスケジュール 702
分散環境でのプライマリ ノードとセカンダリ ノードの同期 703
スタンドアロンおよび分散展開での失われたノードの復元 704
分散展開での既存 IP アドレスとホスト名を使用しての失われたノードの復元 704
分散展開の新 IP アドレスとホスト名を使用しての失われたノードの復元 705
スタンドアロン展開の既存 IP アドレスとホスト名によるノードの復元 705
スタンドアロン展開の新 IP アドレスとホスト名によるノードの復元 706
設定のロール バック 706
分散展開での障害発生時のプライマリ ノードの復元 707
分散展開での障害発生時のセカンダリ ノードの復元 707
Cisco ISE ロギング メカニズム 708
syslog の消去の設定 709
Cisco ISE システム ログ 709

リモート syslog 収集場所の設定 710
Cisco ISE メッセージ コード 712
メッセージ コードのシビラティ（重大度）レベルの設定 712
Cisco ISE メッセージ カタログ 713
エンドポイントのデバッグ ログ コレクタ 713
特定のエンドポイントのデバッグ ログのダウンロード 713
収集フィルタ 714
収集フィルタの設定 715
イベント抑制バイパス フィルタ 715
システム 360 716
モニタリング 716
Grafana でのクエリの実行 718
Grafana ダッシュボードの自動更新を構成 718
Log Analytics 719
Kibana ダッシュボードの作成 721
モニタリングおよび Log Analytics 設定 723
Cisco ISE レポート 724
レポート フィルタ 724
クイック フィルタ条件の作成 725
拡張フィルタ条件の作成 726
レポートの実行および表示 726
レポートのナビゲーション 727
レポートのエクスポート 727
マイレポート 728
Cisco ISE レポートのスケジュール 729
ユースケース：スケジュール済みレポート 730
Cisco ISE のアクティブな RADIUS セッション 731
RADIUS セッションの許可の変更 732
使用可能なレポート 734
RADIUS ライブ ログ 774
認証遅延 778

RADIUS ライブ セッション 778
TACACS ライブ ログ 783
エクスポート サマリ 786

第 7 章 デバイス管理 789
TACACS+ デバイス管理 789
デバイス管理ワーク センター 791
デバイス管理の展開設定 791
デバイス管理ポリシー セット 792
デバイス管理ポリシー セットの作成 793
TACACS+ 認証設定と共有秘密 795
デバイス管理：許可ポリシーの結果 797
TACACS+ デバイス管理を許可された FIPS および非 FIPS モードのプロトコル 797
TACACS+ コマンド セット 797
コマンド セットのワイルドカードと正規表現 797
コマンド ラインおよびコマンド セットのリストの一致 798
複数のコマンド セットを持つルールの処理 799
TACACS+ コマンド セットの作成 799
TACACS+ プロファイル 800
TACACS+ プロファイルの作成 801
共通タスク設定 802
CLI によるイネーブルパスワードの変更 804
TACACS+ のグローバル設定 805
Cisco Secure ACS から Cisco ISE へのデータ移行 806
デバイス管理アクティビティのモニター 806
TACACS ライブ ログ 807

第 8 章 ゲストおよびセキュア Wi-Fi 811
Cisco ISE ゲスト サービス 811
分散環境のエンドユーザーのゲスト ポータルとスポンサー ポータル 812
ゲスト アカウントとスポンサー アカウント 812

ゲスト タイプおよびユーザー ID グループ 813
ゲスト タイプの作成または編集 814
ゲスト タイプの無効化 821
エンドポイント ユーザーの最大同時ログイン数の設定 822
期限切れのゲスト アカウントを消去するスケジューリング設定 823
ゲスト アカウント作成用のカスタム フィールドの追加 824
電子メールでの通知用の電子メール アドレスおよび SMTP サーバーの指定 825
ゲストのロケーションおよび SSID の割り当て 826
ゲスト パスワード ポリシーのルール 827
ゲスト パスワード ポリシーと有効期限の設定 828
ゲスト ユーザー名ポリシーのルール 829
ゲスト ユーザー名ポリシーの設定 829
SMS プロバイダーおよびサービス 830
ゲストに SMS 通知を送信するための SMS ゲートウェイの設定 831
アカウント登録ゲストのソーシャル ログイン 834
ソーシャル ログインの設定 838
ゲスト ポータル 840
ゲスト ポータルのクレデンシャル 840
ホットスポット ゲスト ポータルを使用したゲスト アクセス 842
クレデンシャルを持つゲスト ポータルを使用したゲスト アクセス 842
クレデンシャルを持つゲスト ポータルを使用した従業員アクセス 843
ゲスト デバイスのコンプライアンス 843
ゲスト ポータルの設定タスク 843
ポリシー サービスの有効化 845
ゲスト ポータルの証明書の追加 845
外部 ID ソースの作成 845
ID ソース順序の作成 847
エンドポイント ID グループの作成 848
ホットスポット ゲスト ポータルの作成 848
Sponsored-Guest ポータルの作成 849
アカウント登録ゲスト ポータルの作成 851

ポータルの許可 856
ゲスト ポータルのカスタマイズ 857
定期的な AUP 受け入れの設定 858
定期的な AUP の強制 858
ゲスト ユーザー情報を保存 859
スポンサー ポータル 859
スポンサー ポータルでのゲスト アカウントの管理 859
スポンサー アカウントの管理 861
スポンサー アカウント作成のためのアカウント コンテンツの設定 867
スポンサー ポータル フローの設定 868
ポリシー サービスの有効化 869
ゲスト サービスの証明書の追加 869
外部 ID ソースの作成 870
ID ソース順序の作成 870
スポンサー ポータルの作成 871
スポンサー ポータルのカスタマイズ 872
スポンサー アカウント作成のためのアカウント コンテンツの設定 872
スポンサーに対して使用可能な時間設定項目の設定 873
スポンサー ポータルの Kerberos 認証 874
スポンサーがスポンサー ポータルにログインできない 876
ゲストとスポンサーのアクティビティのモニター 876
メトリック ダッシュボード 877
AUP 受け入れステータス レポート 877
ゲスト アカウンティング レポート 877
プライマリゲストレポート 877
スポンサーのログインおよび監査レポート 878
ゲストおよびスポンサー ポータルの監査ロギング 878
ゲスト アクセス Web 認証オプション 879
中央 WebAuth プロセス対応の NAD 879
ローカル WebAuth プロセス対応のワイヤレス LAN コントローラ 881
ローカル WebAuth プロセス対応の有線 NAD 882

Login.html ページに必要な IP アドレスおよびポートの値 883
NAD での HTTPS サーバーの有効化 884
NAD 上でのカスタマイズされた認証プロキシ Web ページのサポート 884
NAD の Web 認証の設定 884
デバイス登録 WebAuth プロセス 885
ゲストポータルの設定 886
ポータル ID 設定 886
ホットスポット ゲスト ポータルのポータル設定 888
ホットスポット ゲスト ポータルの利用規定（AUP）ページ設定 890
ホットスポット ポータルのポストアクセス バナー ページ設定 891
クレデンシャルを持つゲスト ポータルのポータル設定 892
クレデンシャルを持つゲスト ポータルのログイン ページ設定 894
アカウント登録ページの設定 896
アカウント登録成功ページの設定 900
クレデンシャルを持つゲスト ポータルの利用規定（AUP）ページ設定 902
クレデンシャルを持つゲスト ポータルのゲストによるパスワード変更の設定 903
クレデンシャルを持つゲスト ポータルのゲスト デバイス登録の設定 903
クレデンシャルを持つゲスト ポータルの BYOD 設定 904
クレデンシャルを持つゲスト ポータルのポストログイン バナー ページ設定 905
クレデンシャルを持つゲスト ポータルのゲスト デバイスのコンプライアンス設定 906
ゲスト ポータルの VLAN DHCP リリース ページ設定 907
ゲスト ポータルの認証成功の設定 907
ゲスト ポータルのサポート情報ページの設定 908
スポンサー ポータル アプリケーションの設定 910
ポータル ID 設定 910
スポンサー ポータルのポータル設定 911
スポンサー ポータルのログイン設定 914
スポンサー ポータルの利用規定（AUP）設定 915
スポンサー ポータルのスポンサーのパスワード変更設定 916
スポンサー ポータルのポストログイン バナー設定 916
スポンサー ポータルのサポート情報ページの設定 916

スポンサー ポータルのゲストへの通知のカスタマイズ 918
スポンサー ポータルのカスタマイズの管理と承認 918
ゲストおよびスポンサー ポータルのグローバル設定 919
ゲスト タイプの設定 920
スポンサー グループ設定 923
エンドユーザー ポータル 928
エンドユーザー Web ポータルのカスタマイズ 928
ポータル コンテンツのタイプ 929
ポータルの基本的なカスタマイズ 930
ポータルのテーマ カラーの変更 931
ポータルの表示言語の変更 932
ポータルのアイコン、イメージ、およびロゴの変更 932
ポータルのバナーおよびフッター要素の更新 933
タイトル、手順、ボタン、およびラベル テキストの変更 934
テキスト ボックスの内容のフォーマットおよびスタイル 934
ポータル ページのカスタマイズ用の変数 935
カスタマイズの参照 940
カスタム ポータル ファイル 940
ポータルの高度なカスタマイズ 941
ポータル テーマと構造 CSS ファイル 942
jQuery Mobile によるテーマカラーの変更 943
jQuery Mobile によるテーマ カラーの変更 944
ロケーションに基づくカスタマイズ 945
ユーザー デバイス タイプに基づくカスタマイズ 946
ポータルのデフォルト テーマ CSS ファイルのエクスポート 946
カスタム ポータル テーマ CSS ファイルの作成 947
ポータル コンテンツに組み込まれたリンク 948
動的なテキスト更新の変数の挿入 949
テキストをフォーマットし、リンクを含めるソース コードの使用 950
アドバタイズメントとしてのイメージの追加 951
カルーセル アドバタイジングの設定 952

ゲスト ロケーションに基づいたグリーティングのカスタマイズ 954
ユーザー デバイス タイプに基づいたグリーティングのカスタマイズ 955
ポータル ページのレイアウトの変更 956
カスタム ポータル テーマ CSS ファイルのインポート 958
カスタム ポータル テーマの削除 958
カスタマイズの参照 959
ポータル言語のカスタマイズ 960
言語ファイルのエクスポート 961
言語ファイルでの言語の追加または削除 962
更新された言語ファイルのインポート 963
ゲスト通知、承認、およびエラー メッセージのカスタマイズ 964
電子メールでの通知のカスタマイズ 964
SMS テキスト メッセージ通知のカスタマイズ 965
印刷通知のカスタマイズ 966
承認要求の電子メールでの通知のカスタマイズ 967
エラー メッセージの編集 968
ポータル ページのタイトル、コンテンツおよびラベルの文字数制限 969
ポータル ページのタイトル、コンテンツおよびラベルの文字数制限 969
ポータルのカスタマイズ 972
エンドユーザー ポータルのページ レイアウトの CSS クラスと説明 972
ポータル言語ファイルの HTML サポート 973
ブロック済みリストポータル言語ファイルの HTML サポート 973
個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート 974
証明書プロビジョニング ポータルの言語ファイルの HTML サポート 975
クライアント プロビジョニング ポータルの言語ファイルの HTML サポート 976
クレデンシャル ゲスト ポータルの言語ファイルの HTML サポート 977
ホットスポット ゲスト ポータルの言語ファイルの HTML サポート 980
モバイル デバイス管理ポータルの言語ファイルの HTML サポート 981
デバイス ポータルの言語ファイルの HTML サポート 981
スポンサー ポータルの言語ファイルの HTML サポート 983

第 9 章 アセットの可視性 985

外部 ID ストアを使用した Cisco ISE への管理アクセス 987

外部認証および許可 987

外部 ID ストアを使用したパスワード ベースの認証の設定 988

外部管理者グループの作成 988

内部読み取り専用管理者の作成 989

外部グループを読み取り専用管理者グループにマッピング 989

外部管理者グループのメニューアクセス権限とデータアクセス権限の設定 989

外部管理者認証の RBAC ポリシーの作成 990

内部許可を伴う認証に対する外部 ID ストアを使用した管理アクセスの設定 991

外部認証のプロセス フロー 991

外部 ID ソース 992

LDAP ID ソースの設定 992

RADIUS トークン ID ソースの設定 1000

RSA SecurID ID ソースの設定 1002

Cisco ISE ユーザー 1004

ユーザー ID 1005

ユーザー グループ 1005

ユーザー ID グループ 1005

ユーザー ロール 1006

ユーザー アカウントのカスタム属性 1006

ユーザー認証の設定 1007

ユーザーおよび管理者用の自動パスワードの生成 1009

内部ユーザー操作 1010

ユーザーの追加方法 1010

Cisco ISE ユーザー データのエクスポート 1011

Cisco ISE 内部ユーザーのインポート 1012

エンドポイント設定 1013

エンドポイントの LDAP からのインポートの設定 1015

ID グループ操作 1017

ユーザー ID グループの作成 1017
ユーザー ID グループのエクスポート 1017
ユーザー ID グループのインポート 1018
エンドポイント ID グループの設定 1018
最大同時セッション数の設定 1019
グループの最大同時セッション数 1019
カウンタの時間制限の設定 1020
アカウントの無効化ポリシー 1021
個別のユーザー アカウントの無効化 1022
グローバルにユーザー アカウントを無効化 1022
内部 ID ソースと外部 ID ソース 1023
外部 ID ソースの作成 1025
外部 ID ストアパスワードに対する内部ユーザーの認証 1026
証明書認証プロファイル 1027
証明書認証プロファイルの追加 1027
外部 ID ソースとしての Active Directory 1028
Active Directory でサポートされる認証プロトコルおよび機能 1028
許可ポリシーで使用する Active Directory 属性およびグループの取得 1030
ブール属性のサポート 1032
証明書ベース認証の Active Directory 証明書の取得 1032
Active Directory ユーザー認証プロセス フロー 1033
Microsoft Entra ID の Cisco ISE への接続 1033
Entra ID でユーザーを認証するためのリソース オーナー パスワード クレデンシャル フローの設定 1033
Microsoft Entra ID でのリソース オーナー パスワード クレデンシャル フロー用アプリケーションの設定 1033
Cisco ISE でのリソースオーナーパスワードクレデンシャルフローの設定 1035
Microsoft Entra ID を使用した EAP-TLS および TEAP 認証 1036
Active Directory マルチドメイン フォレストのサポート 1037
Active Directory と Cisco ISE の統合の前提条件 1037
さまざまな操作の実行に必要な Active Directory アカウント権限 1038

通信用に開放するネットワークポート 1039
DNS サーバー 1040
外部 ID ソースとしての Active Directory の設定 1040
Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 1041
ドメイン コントローラの追加 1043
パッシブ ID の MSRPC プロトコル 1044
Active Directory ドメインの脱退 1047
認証ドメインの設定 1048
Active Directory ユーザー グループの設定 1049
Active Directory ユーザーとマシンの属性の設定 1050
パスワード変更、マシン認証、およびマシン アクセス制限の設定の変更 1050
Active Directory アカウントに対するパスワードの最大試行回数の設定 1051
マシンアクセス制限キャッシュ 1053
カスタム スキーマの設定 1054
Active Directory の複数参加設定のサポート 1055
Active Directory 参加ポイントを追加する新しいスコープの作成 1056
ID 書き換え 1056
ID 書き換えの有効化 1057
ID 解決の設定 1058
ID 解決問題の回避 1058
ID 解決の設定 1059
Active Directory 認証のためのユーザーのテスト 1060
Active Directory の設定の削除 1060
ノードの Active Directory の参加の表示 1061
Active Directory の問題の診断 1061
Active Directory デバッグ ログの有効化 1062
トラブルシューティング用の Active Directory ログ ファイルの入手 1063
Active Directory のアラームおよびレポート 1063
Active Directory の高度な調整 1064
優先ドメインコントローラの設定 1064
優先順位によるドメインコントローラの選択の強制 1065

Active Directory アイデンティティ検索属性 1065
Active Directory が構成された Cisco ISE をセットアップするための補足情報 1066
Active Directory のグループ ポリシーの設定 1067
Active Directory に対する EAP-TLS マシン認証のための Odyssey 5.X サプリカントの設定 1067
マシン認証のためのエージェントの設定 1068
Active Directory でEasy Connect およびパッシブ ID サービスをサポートするための要件 1068
パッシブ ID サービス の Active Directory の設定 1069
Windows 監査ポリシーの設定 1072
Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定 1073
ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限 1073
ドメイン コントローラで DCOM を使用するための権限 1075
Easy Connect 1077
Easy Connect 適用モードの設定 1081
Easy Connect 可視性モードの設定 1082
PassiveID ワーク センター 1083
初期セットアップと設定 1084
PassiveID ワーク センター ダッシュボード 1085
プローブおよびプロバイダーとしての Active Directory 1085
PassiveID セットアップの使用を開始 1086
Active Directory プロバイダーの管理 1088
Active Directory の設定 1088
その他の パッシブ ID サービス プロバイダー 1094
Active Directory エージェント 1098
Active Directory エージェントの自動インストールおよび展開 1099
Active Directory エージェントの手動インストールおよび展開 1100
エージェントのアンインストール 1102
Active Directory エージェントの設定 1102
API プロバイダー 1103
パッシブ ID サービス の ISE REST サービスへのブリッジの設定 1105
パッシブ ID REST サービスへの API コールの送信 1105

API プロバイダーの設定 1106
API コール 1107
SPAN 1108
SPAN の使用 1109
SPAN 設定 1110
syslog プロバイダー 1110
syslog クライアントの設定 1111
syslog メッセージ構造のカスタマイズ（テンプレート） 1115
Syslog 事前定義メッセージテンプレートの使用 1122
パッシブ ID サービスのフィルタリング 1134
エンドポイント プローブ 1134
エンドポイント プローブの使用 1136
エンドポイント プローブ設定 1136
サブスクライバ 1137
サブスクライバの pxGrid 証明書の生成 1138
サブスクライバの有効化 1140
ライブ ログからのサブスクライバ イベントの表示 1141
サブスクライバの設定 1141
PassiveID ワーク センター でのサービスのモニタリングとトラブルシューティング 1141
LDAP 1142
LDAP ディレクトリ サービス 1142
複数の LDAP インスタンス 1142
LDAP フェールオーバー 1143
LDAP 接続管理 1143
LDAP ユーザー認証 1143
許可ポリシーで使用する LDAP グループおよび属性の取得 1144
LDAP サーバーによって返されるエラー 1146
LDAP ユーザー ルックアップ 1147
LDAP MAC アドレス ルックアップ 1147
LDAP ID ソースの追加 1148
LDAP ID ソースの設定 1148

LDAP スキーマの設定 1157
プライマリおよびセカンダリ LDAP サーバーの設定 1157
LDAP サーバーからの属性を取得するための Cisco ISE の有効化 1157
LDAP サーバーからのグループ メンバーシップ詳細の取得 1158
LDAP サーバーからのユーザー属性の取得 1159
LDAP ID ソースによるセキュア認証の有効化 1159
ODBC ID ソース 1160
ODBC データベースのクレデンシャルチェック 1161
ODBC ID ソースの追加 1165
RADIUS トークン ID ソース 1169
RADIUS トークンサーバーでサポートされる認証プロトコル 1169
RADIUS トークンサーバーで通信に使用されるポート 1170
RADIUS 共有秘密 1170
RADIUS トークン サーバーでのフェールオーバー 1170
RADIUS トークン サーバーの設定可能なパスワード プロンプト 1170
RADIUS トークン サーバーのユーザー認証 1170
RADIUS トークン サーバーのユーザー属性キャッシュ 1170
ID 順序での RADIUS ID ソース 1171
RADIUS サーバーがすべてのエラーに対して同じメッセージを返す 1171
Safeword サーバーでサポートされる特別なユーザー名の形式 1172
RADIUS トークン サーバーでの認証要求と応答 1172
RADIUS トークン ID ソースの設定 1173
RADIUS トークン サーバーの追加 1174
RADIUS トークン サーバーの削除 1176
RSA ID ソース 1176
Cisco ISE と RSA SecurID サーバーの統合 1177
Cisco ISE の RSA 設定 1177
RSA SecurID サーバーに対する RSA エージェント認証 1177
分散 Cisco ISE 環境の RSA ID ソース 1178
Cisco ISE 展開の RSA サーバーの更新 1178
自動 RSA ルーティングの上書き 1178

RSA ノード秘密リセット 1178
RSA の自動可用性のリセット 1179
RSA SecurID ID ソースの設定 1179
RSA ID ソースの追加 1181
RSA コンフィギュレーション ファイルのインポート 1181
Cisco ISE サーバーのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット 1182
RSA ID ソースの認証制御オプションの設定 1183
RSA プロンプトの設定 1184
RSA メッセージの設定 1184
外部 ID ソースとしての SAMLv2 ID プロバイダー 1185
セッションサービスの有効化 1186
Cisco ISE での SAML ID プロバイダーの設定 1187
Cisco ISE への SAML ID プロバイダーの追加 1187
ポータルの認証方式としての SAML ID プロバイダの追加 1188
SAML ID プロバイダーの設定 1188
ID プロバイダーの削除 1192
SAML ベースの管理者ログイン 1192
認証失敗ログ 1194
Cisco pxGrid Direct 1195
データ同期の間隔 1197
「今すぐ同期」を使用したオンデマンドの pxGrid 直接データ同期 1198
オープン API を使用したコネクタの作成 1200
GUI を使用したコネクタの作成 1201
URL プッシャコネクタタイプの作成 1202
URL フェッチャコネクタタイプの作成 1203
コネクタ属性を使用した認証プロファイルの設定 1206
ID ソース順序 1206
ID ソース順序の作成 1207
ID ソース順序の削除 1207
レポートでの ID ソースの詳細 1208

[認証（Authentications）] ダッシュレット 1208
ID ソース レポート 1208
ネットワークのプロファイリングされたエンドポイント 1208
プロファイラ条件の設定 1209
Cisco ISE プロファイリング サービス 1210
プロファイラ ワーク センター 1210
[プロファイラ（Profiler）] ダッシュボード 1210
プロファイリング サービスを使用したエンドポイント インベントリ 1211
Cisco ISE プロファイラ キュー制限の設定 1211
Martian IP アドレス 1212
プロファイラフォワーダ永続キュー 1212
Cisco ISE ノードでのプロファイリング サービスの設定 1213
プロファイリング サービスによって使用されるネットワーク プローブ 1213
IP アドレスと MAC アドレスのバインディング 1214
NetFlow プローブ 1214
DHCP プローブ 1215
DHCP ブリッジ モードのワイヤレス LAN コントローラ設定 1216
DHCP SPAN プローブ 1216
HTTP プローブ 1216
HTTP SPAN プローブ 1217
VMware で実行中の Cisco ISE の HTTP 属性の収集の無効化 1217
pxGrid プローブ 1217
RADIUS プローブ 1218
ネットワーク スキャン（NMAP）プローブ 1219
NMAP の手動サブネット スキャンの SNMP 読み取り専用コミュニティ ストリング 1220
手動 NMAP スキャンの結果 1221
DNS プローブ 1222
DNS FQDN ルックアップ 1222
WLC Web インターフェイスでの呼出端末 ID タイプの設定 1222
SNMP クエリ プローブ 1223
SNMP クエリに関する Cisco Discovery Protocol のサポート 1223

SNMP クエリに関する Link Layer Discovery Protocol のサポート 1224
SNMP トラップ プローブ 1225
Active Directory プローブ 1226
Cisco ISE ノードごとのプローブの設定 1226
CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定 1227
認証されたエンドポイントに対する許可変更のグローバル設定 1229
許可変更の発行の使用例 1229
許可変更の発行の免除 1230
CoA 設定の各タイプに発行される許可変更 1231
ISE データベースの持続性とパフォーマンスの属性フィルタ 1232
エンドポイント属性をフィルタリングするグローバル設定 1232
Cisco IOS センサー組み込みスイッチからの属性の収集 1235
Cisco IOS センサー組み込みネットワーク アクセス デバイス 1235
Cisco IOS センサー組み込みネットワーク アクセス デバイスの設定チェックリスト 1235
ISE プロファイラによる Cisco IND コントローラのサポート 1237
MUD の Cisco ISE サポート 1239
多要素分類による拡張エンドポイントの可視化 1242
AI 分析によって実現されるサービス 1245
Cisco AI Analytics の有効化 1245
エンドポイント プロファイリングに対する Cisco AI-ML ルール提案 1247
プロファイラ条件 1250
プロファイリング ネットワーク スキャン アクション 1250
新しいネットワーク スキャン アクションの作成 1251
NMAP オペレーティング システム スキャン 1252
オペレーティング システム ポート 1253
NMAP SNMP ポート スキャン 1256
NMAP 一般ポート スキャン 1257
一般ポート 1257
NMAP カスタム ポート スキャン 1258
サービス バージョン情報を含む NMAP スキャン 1258
NMAP SMB 検出スキャン 1259

NMAP ホスト検出のスキップ 1259
NMAP スキャン ワークフロー 1260
NMAP スキャンからのサブネットの除外 1262
手動 NMAP スキャンの設定 1262
McAfee ePolicy Orchestrator を使用したプロファイリング ポリシーの設定 1264
プロファイラ エンドポイント カスタム属性 1266
プロファイラ条件の作成 1267
エンドポイント プロファイリング ポリシー ルール 1267
エンドポイント プロファイリング ポリシーの設定 1269
エンドポイント プロファイリング ポリシーの作成 1274
エンドポイント プロファイリング ポリシーごとの認可変更の設定 1275
エンドポイント プロファイリング ポリシーのインポート 1276
エンドポイント プロファイリング ポリシーのエクスポート 1277
事前定義されたエンドポイント プロファイリング ポリシー 1278
アップグレード中に上書きされる事前定義されたエンドポイント プロファイリング ポリシー 1279
エンドポイント プロファイリング ポリシーを削除できない 1279
Draeger 医療機器用の事前定義済みプロファイリング ポリシー 1279
不明なエンドポイントのエンドポイント プロファイリング ポリシー 1280
静的に追加されたエンドポイントのエンドポイント プロファイリング ポリシー 1281
スタティック IP デバイスのエンドポイント プロファイリング ポリシー 1281
エンドポイント プロファイリング ポリシーの一致 1281
許可に使用するエンドポイント プロファイリング ポリシー 1282
Cisco Catalyst 9800 ワイヤレス LAN コントローラからの Wi-Fi デバイス分析データ 1282
エンドポイント プロファイリング ポリシーの論理プロファイルによるグループ化 1284
論理プロファイルの作成 1284
プロファイリング例外アクション 1285
例外アクションの作成 1285
ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 1286
CSV ファイルを使用したエンドポイントのインポート 1287
エンドポイントで使用可能なデフォルトのインポート テンプレート 1288

インポート中の不明なエンドポイントの再プロファイリング 1289
インポートされない無効な属性を持つエンドポイント 1290
LDAP サーバーからのエンドポイントのインポート 1290
CSV ファイルを使用したエンドポイントのエクスポート 1291
識別されたエンドポイント 1292
識別されたエンドポイントの、ポリシー サービス ノード データベースへのローカル保存 1293
クラスタのポリシー サービス ノード 1294
エンドポイント ID グループの作成 1294
識別されたエンドポイントの、エンドポイント ID グループでのグループ化 1295
エンドポイントに対して作成されるデフォルトのエンドポイント ID グループ 1295
一致するエンドポイント プロファイリング ポリシーに対して作成されるエンドポイント ID グループ 1296
エンドポイント ID グループでの静的なエンドポイントの追加 1296
ダイナミック エンドポイントの、ID グループへの追加または削除後の再プロファイリング 1297
許可ルールで使用されるエンドポイント ID グループ 1297
エニーキャストおよびプロファイラサービス 1298
プロファイラ フィード サービス 1298
プロファイラ フィード サービスの設定 1299
オフラインでのプロファイラ フィード サービスの設定 1301
オフライン更新プログラム パッケージのダウンロード 1301
オフライン フィード更新の適用 1302
プロファイルと OUI の更新に関する電子メール通知の設定 1303
フィード更新の取り消し 1303
プロファイラ レポート 1303
エンドポイントの異常な動作の検出 1304
異常な動作が発生しているエンドポイントに関する許可ポリシー ルールの設定 1305
異常な動作が発生しているエンドポイントの表示 1305
クライアント マシン上のエージェントのダウンロードの問題 1306
エンドポイント 1307
エンドポイント設定 1307

エンドポイントの LDAP からのインポートの設定 1310
エンドポイント プロファイリング ポリシーの設定 1311
UDID 属性を使用するエンドポイント コンテキストの可視性 1317
エンドポイントコンテキストの可視性ウィンドウのGUIDを持つエンドポイントの単一エントリ 1317
Windows および MacOS エンドポイント用のエンドポイント スクリプト ウィザード 1318
エンドポイントスクリプトのプロビジョニングのサマリーレポート 1320
IF-MIB 1321
SNMPv2-MIB 1321
IP-MIB 1322
CISCO-CDP-MIB 1322
CISCO-VTP-MIB 1323
CISCO-STACK-MIB 1323
BRIDGE-MIB 1323
OLD-CISCO-INTERFACE-MIB 1324
CISCO-LWAPP-AP-MIB 1324
CISCO-LWAPP-DOT11-CLIENT-MIB 1325
CISCO-AUTH-FRAMEWORK-MIB 1326
EEE8021-PAE-MIB: RFC IEEE 802.1X 1326
HOST-RESOURCES-MIB 1327
LLDP-MIB 1327
エンドポイントのセッションのトレース 1327
ディレクトリからのセッションの削除 1329
エンドポイントのグローバル検索 1329

第 10 章 **個人所有デバイスの持ち込み（BYOD） 1331**
企業ネットワークのパーソナル デバイス（BYOD） 1331
分散環境のエンドユーザーのデバイス ポータル 1332
デバイス ポータルのグローバル設定 1332
パーソナル デバイス ポータル 1332
デバイス ポータルへのアクセス 1333
ブロックリスト ポータル 1333

証明書プロビジョニング ポータル 1334
個人所有デバイスの持ち込みポータル 1334
クライアント プロビジョニング ポータル 1335
モバイル デバイス管理ポータル 1335
デバイス ポータル 1336
BYOD の展開オプションとステータス ワークフロー 1337
従業員が登録するパーソナル デバイス数の制限 1340
ネイティブ サプリカントを使用したデバイス登録のサポート 1341
ネイティブ サプリカントがサポートするオペレーティング システム 1341
クレデンシャルを持つゲスト ポータルを使用したパーソナル デバイスの登録を従業員に許可 1341
BYOD 登録に再接続する URL の提供 1342
デバイス ポータルの設定タスク 1342
ポリシー サービスの有効化 1344
デバイス ポータルへの証明書の追加 1344
外部 ID ソースの作成 1345
ID ソース順序の作成 1346
エンドポイント ID グループの作成 1346
ブロックリスト ポータルの編集 1347
BYOD ポータルの作成 1350
クライアント プロビジョニング ポータルの作成 1352
クライアント プロビジョニング ポータルの作成 1353
MDM ポータルの作成 1355
デバイス ポータルの作成 1357
許可プロファイルの作成 1358
許可プロファイルの作成 1358
許可ポリシー ルールの作成 1359
デバイス ポータルのカスタマイズ 1360
従業員が追加するパーソナル デバイスの管理 1360
従業員が追加したデバイスの表示 1360
デバイスをデバイス ポータルに追加するときのエラー 1360

デバイス ポータルから削除されたデバイスはエンドポイント データベースに残っている 1361
従業員が登録するパーソナル デバイス数の制限 1361
デバイス ポータルおよびエンドポイント アクティビティのモニター 1362
デバイス ログインおよび監査レポート 1362
登録済みエンドポイント レポート 1362

第 11 章 セキュアなアクセス 1365
Cisco ISE でのネットワークデバイスの定義 1365
Cisco ISE でのデフォルト ネットワーク デバイスの定義 1366
ネットワーク デバイス 1367
ネットワーク デバイス定義の設定 1367
デフォルトのネットワーク デバイス定義の設定 1381
ネットワーク デバイスのインポート設定 1384
Cisco ISE でのネットワークデバイスの追加 1385
Cisco ISE へのネットワーク デバイスのインポート 1386
Cisco ISE からのネットワーク デバイスのエクスポート 1387
ネットワーク デバイス設定の問題のトラブルシューティング 1388
Execute Network Device Command 診断ツール 1388
Cisco ISE でのサードパーティ ネットワーク デバイスのサポート 1389
ネットワーク デバイス プロファイル 1392
Cisco ISE でのサードパーティ製ネットワークデバイスの設定 1394
ネットワーク デバイス プロファイルの作成 1395
Cisco ISE からのネットワーク デバイス プロファイルのエクスポート 1397
Cisco ISE へのネットワーク デバイス プロファイルのインポート 1397
ネットワーク デバイス グループの管理 1398
ネットワーク デバイス グループの設定 1398
ネットワーク デバイス グループのインポート設定 1399
ネットワーク デバイス グループ 1400
ポリシー評価で Cisco ISE が使用するネットワークデバイスの属性 1401
Cisco ISE へのネットワーク デバイス グループのインポート 1402

Cisco ISE からのネットワーク デバイス グループのエクスポート 1402
ネットワーク デバイス グループの管理 1403
ネットワーク デバイス グループの設定 1403
ネットワーク デバイス グループのインポート設定 1404
Cisco ISE でのテンプレートのインポート 1404
ネットワーク デバイスのインポート テンプレート形式 1405
ネットワーク デバイス グループのインポート テンプレート形式 1408
Cisco ISE と NAD 間の通信を保護する IPSec セキュリティ 1409
Cisco ISE でのネイティブ IPSec の設定 1410
Cisco ISE で [ネイティブIPSec設定（Native IPsec Configuration）] を表示して修正 1413
Cisco ISE でのレガシー IPSec からネイティブ IPSec への移行 1413
Mobile Device Manager と Cisco ISE との相互運用性 1416
サポートされているモバイルデバイス管理の使用例 1417
サポートされている統合エンドポイント管理およびモバイルデバイス管理サーバー 1421
モバイルデバイス管理サーバーで使用されるポート 1422
モバイルデバイス管理の統合プロセスフロー 1423
モバイルデバイス管理サーバーを使用した、ランダムで変化する MAC アドレスの処理 1424
Cisco ISE を使用したモバイルデバイス管理サーバーのセットアップ 1426
Cisco ISE へのモバイルデバイス管理サーバー証明書のインポート 1426
Cisco ISE でのデバイス管理サーバーの定義 1427
Cisco ISE でのモバイルデバイス管理サーバーの設定 1427
全般的な MDM 設定または UEM 設定の構成 1432
MDM または UEM サーバーのタイムアウトの設定 1433
Microsoft Intune と Microsoft SCCM 用の Cisco ISE MDM サポート 1433
Microsoft System Center Configuration Manager のポリシー設定例 1435
Cisco ISE 用の Microsoft System Center Configuration Manager サーバーの設定 1436
Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定 1437
ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限 1437
ドメイン コントローラで DCOM を使用するための権限 1439
WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 1441

WMI アクセス用にファイアウォール ポートを開く 1442
デスクトップ デバイス マネージャ サーバーでのエンドポイント コンプライアンスの設定基準ポリシーの選択 1443
未登録のデバイスのリダイレクトのための許可プロファイルの設定 1445
MDM 使用例の許可ポリシー ルールの設定 1446
MDM 相互運用性のためのワイヤレス LAN コントローラでの ACL の設定 1447
デバイスのワイプまたはロック 1448
モバイルデバイス管理レポートの表示 1449
モバイルデバイス管理ログの表示 1449
サービスとしての Cisco Private 5G の設定 1449
サービスとしての Cisco Private 5G の設定 1453

第 12 章 セグメンテーション 1459
ポリシー セット 1460
ポリシー セットの構成時の設定 1461
認証ポリシー 1463
認証失敗：ポリシー結果オプション 1465
認証失敗時の一連のアクションとして [続行（Continue）] を使用するユースケース 1466
認証ポリシーの設定 1467
認証ポリシーの構成設定 1468
パスワード ベースの認証 1471
暗号化されたパスワードと暗号化技術を使用したセキュアな認証 1471
認証方式と許可特権 1472
認証ダッシュレット 1472
認証結果の表示 1472
認証レポートおよびトラブルシューティング ツール 1473
許可ポリシー 1474
Cisco ISE の許可プロファイル 1474
許可プロファイルの権限 1475
ダウンロード可能 ACL 1475
Active Directory ユーザー許可のためのマシン アクセス制限 1477

許可ポリシーおよびプロファイルの設定のガイドライン 1478
許可ポリシーの設定 1479
許可ポリシーの設定 1482
許可プロファイルの設定 1485
許可ポリシーの例外 1489
ローカル例外およびグローバル例外の構成時の設定 1490
ポリシー条件 1490
ディクショナリおよびディクショナリ属性 1492
システム定義のディクショナリとディクショナリ属性 1497
システム ディクショナリおよびディクショナリ属性の表示 1497
ユーザー定義のディクショナリとディクショナリ属性 1497
ユーザー定義のディクショナリの作成 1498
ユーザー定義のディクショナリ属性の作成 1498
RADIUS ベンダー ディクショナリ 1499
RADIUS ベンダー ディクショナリの作成 1499
RADIUS ベンダー ディクショナリ属性の作成 1499
HP RADIUS IETF サービス タイプ属性 1500
RADIUS ベンダー ディクショナリ属性の設定 1500
[条件スタジオ（Conditions Studio）] の操作 1502
ポリシー条件の設定、編集および管理 1507
特別なネットワーク アクセス条件 1513
デバイス ネットワーク条件の設定 1514
デバイス ポート ネットワーク条件の設定 1514
エンドステーション ネットワーク条件の設定 1515
時刻と日付の条件の作成 1515
許可ポリシーで IPv6 条件属性を使用 1516
ポリシー セット プロトコルの設定 1518
サポートされているネットワーク アクセス ポリシー セット プロトコル 1518
プロトコルとして EAP-FAST を使用するためのガイドライン 1518
EAP-FAST の設定 1519
EAP-FAST の PAC の生成 1520

EAP-FAST 設定 1520
PAC の設定 1521
認証プロトコルとしての EAP-TTLS の使用 1523
EAP-TLS の設定 1523
EAP-TTLS 設定 1523
EAP-TLS の設定 1524
EAP-TLS 設定 1525
PEAP の設定 1526
PEAP 設定 1526
RADIUS の設定 1527
RADIUS 設定 1527
セキュリティ設定の構成 1534
サポートされる暗号スイート 1541
Cisco ISE の RADIUS プロトコルのサポート 1545
許可されるプロトコル 1546
PAC オプション 1563
RADIUS プロキシ サーバーとして機能する CIsco ISE 1567
外部 RADIUS サーバーの設定 1567
RADIUS サーバー順序の定義 1568
TACACS+ プロキシ クライアントとして機能する CIsco ISE 1568
外部 TACACS+ サーバーの設定 1569
TACACS+ 外部サーバーの設定 1569
TACACS+ サーバー順序の定義 1570
TACACS+ サーバー順序の設定 1571
多要素認証のための Cisco Duo と Cisco ISE の統合 1572
Duo 接続へのアイデンティティ同期の追加 1575
ネットワーク アクセス サービス 1577
ネットワーク アクセスの許可されるプロトコルの定義 1577
ユーザーのネットワーク アクセス 1578
シスコ以外のデバイスからの MAB の有効化 1585
シスコ デバイスからの MAB の有効化 1586

TrustSec アーキテクチャ 1588
TrustSec のコンポーネント 1589
TrustSec の用語 1590
TrustSec のサポートされるスイッチと必要なコンポーネント 1592
Cisco Catalyst Center との統合 1592
TrustSec ダッシュボード 1594
メトリック 1594
現在のネットワーク ステータス 1595
アクティブな SGT セッション 1595
アラーム 1595
クイック ビュー 1596
ライブログ 1598
TrustSec のグローバル設定 1598
一般 TrustSec の設定 1599
TrustSec マトリックスの設定 1602
TrustSec マトリックスの設定 1603
TrustSec デバイスの設定 1605
OOB TrustSec PAC 1606
[設定（Settings）] 画面からの TrustSec PAC の生成 1606
[ネットワーク デバイス（Network Devices）] 画面からの TrustSec PAC の生成 1606
[ネットワーク デバイス リスト（Network Devices List）] 画面からの TrustSec PAC の生成 1607
[プッシュ（Push）] ボタン 1608
Cisco TrustSec AAA サーバーの設定 1608
TrustSec HTTPS サーバー 1609
Cisco ISE TrustSec HTTPS サーバーへの外部サーバーの追加 1610
セキュリティ グループの設定 1612
Cisco ISE でのセキュリティグループの管理 1612
Cisco ISE へのセキュリティ グループのインポート 1613
Cisco ISE からのセキュリティ グループのエクスポート 1614
IP SGT スタティック マッピングの追加 1614

IP SGT スタティック マッピングの展開 1615
Cisco ISE への IP SGT スタティック マッピングのインポート 1616
Cisco ISE からの IP SGT スタティック マッピングのエクスポート 1617
SGT マッピング グループの追加 1617
セキュリティ グループ アクセス コントロール リストの追加 1618
出力ポリシー 1620
送信元ツリー ビュー 1620
宛先ツリー ビュー 1621
マトリクス ビュー 1621
マトリクスの次元 1622
カスタム ビューの作成 1622
マトリクス操作 1623
ワーク プロセスの設定 1624
[マトリックス登録（Matrices Listing）] ページ 1625
TrustSec マトリックス ワークフロー プロセス 1626
出力ポリシー テーブル セルの設定 1639
出力ポリシー セルのマッピングの追加 1639
出力ポリシーのエクスポート 1640
出力ポリシーのインポート 1641
出力ポリシーの SGT の設定 1642
モニター モード 1642
モニター モードの機能 1642
不明セキュリティ グループ 1643
デフォルト ポリシー 1643
SGT の割り当て 1643
NDAC 許可 1644
NDAC 許可の設定 1644
エンドユーザーの許可の設定 1645
TrustSec の設定およびポリシー プッシュ 1646
CoA でサポートされるネットワーク デバイス 1646
非 CoA サポート デバイスへの設定変更のプッシュ 1647

SSH キーの検証 1647
環境 CoA 通知のフロー 1648
環境 CoA トリガー 1649
SGACL コンテンツ更新のフロー 1651
SGACL 名前付きリストの更新 CoA の開始 1652
ポリシーの更新 CoA 通知のフロー 1653
SGT マトリクスの更新 CoA のフロー 1653
出力ポリシーからの、SGT マトリクスの更新 CoA の開始 1654
TrustSec CoA の概要 1655
セキュリティ グループ タグの交換プロトコル 1656
SXP デバイスの追加 1658
SGT ドメインフィルタの追加 1659
SXP の設定 1660
Cisco ISE でのシスコ アプリケーション セントリック インフラストラクチャ接続 1661
Cisco ACI 接続の追加 1663
インバウンドおよびアウトバウンド SGT ドメインルールの追加 1666
SGTドメインの作成 1667
SGTバインディング 1668
Cisco ACI 統合の互換性マトリックス 1668
ACI コネクタのデバッグログ 1669
Cisco ACI 統合で発生するアラーム 1669
レガシー ACI 統合から新しい ACI 接続ワークフローへの移行 1670
仮想ネットワーク認識による Cisco ACI と Cisco SD-Access の統合 1670
Cisco ACI と Cisco SD-Access の統合のための Cisco ISE の設定 1677
Cisco ACI と Cisco SD-Access の統合の確認 1678
ユーザー レポート別上位 N 個の RBACL ドロップの実行 1681
Cisco Meraki ダッシュボードと Cisco ISE の接続 1682
Cisco ISE での Cisco Meraki 接続の表示と変更 1685

第 13 章 コンプライアンス 1687
ポスチャ タイプ 1688

エージェントレス ポスチャ 1690
エージェントレスポスチャのトラブルシューティング 1695
ポスチャ管理の設定 1696
ポスチャワークフローでの未検証のオペレーティング システム リリースのサポートの強化 1696
クライアントのポスチャ要件 1697
クライアントのタイマー設定 1699
指定した時間内で修復するためのクライアントの修復タイマーの設定 1699
クライアントの遷移のためのネットワーク遷移遅延タイマーの設定 1699
ログイン成功ウィンドウを自動的に閉じる設定 1700
非エージェント デバイスへのポスチャ ステータスの設定 1700
ポスチャのリース 1701
定期的再評価 1702
定期的再評価の設定 1702
ポスチャのトラブルシューティングの設定 1703
ポスチャの全般設定 1705
Cisco ISE へのポスチャ更新のダウンロード 1706
Cisco ISE オフライン更新 1707
1708
ポスチャ更新の自動ダウンロード 1709
ポスチャの利用規定の構成設定 1709
ポスチャ評価の利用規定の設定 1711
ポスチャ条件 1711
単純ポスチャ条件 1712
単純ポスチャ条件の作成 1712
複合ポスチャ条件 1713
複合ポスチャ条件の作成 1713
ディクショナリ複合条件の設定 1714
Windows クライアントでの自動アップデートを有効にするための事前定義の条件 1715
事前設定済みアンチウイルスおよびアンチスパイウェア条件 1715
アンチウイルスとアンチスパイウェア サポート表 1716

コンプライアンス モジュール 1717
ポスチャ コンプライアンスのチェック 1718
パッチ管理条件の作成 1718
ディスク暗号化条件の作成 1719
ポスチャ条件の設定 1720
ファイル条件の設定 1720
ファイアウォール条件の設定 1729
レジストリ条件の設定 1730
継続的なエンドポイント属性モニタリング 1732
アプリケーション条件の設定 1732
サービス条件の設定 1734
ポスチャ複合条件の設定 1735
ウイルス対策条件の設定 1737
アンチスパイウェア複合条件の設定 1740
マルウェア対策条件の設定 1741
ディクショナリ単純条件の設定 1744
ディクショナリ複合条件の設定 1744
パッチ管理条件の設定 1746
ディスク暗号化条件の設定 1748
USB 条件の設定 1750
ハードウェア属性条件の設定 1750
ポスチャ外部データソース条件 1751
スクリプト条件の追加 1751
スクリプト条件を実行するために信頼を確立 1753
スクリプト終了コード 1754
スクリプトのダウンロード 1755
ポスチャ ポリシーの設定 1755
エージェントのワークフローの設定 1758
証明書ベースの条件のための前提条件 1759
デフォルトのポスチャ ポリシー 1760
クライアント ポスチャ評価 1762

ポスチャ評価オプション 1762
ポスチャ修復オプション 1763
ポスチャのカスタム条件 1764
ポスチャ エンドポイント カスタム属性 1765
エンドポイント カスタム属性を使用したポスチャ ポリシーの作成 1765
カスタム ポスチャ修復アクション 1766
アンチスパイウェア修復の追加 1766
アンチウイルス修復の追加 1767
ファイル修復の追加 1767
スクリプト修復の追加 1768
スクリプト条件を実行するために信頼を確立 1769
スクリプトのダウンロード 1770
プログラム修復起動の追加 1771
プログラム修復起動のトラブルシューティング 1771
リンク修復の追加 1771
パッチ管理修復の追加 1772
Windows Server Update Services 修復の追加 1772
Windows Update 修復の追加 1773
ポスチャ評価要件 1773
非準拠ステートでスタックしたクライアント システム 1775
クライアントのポスチャ要件の作成 1775
ポスチャ再評価の構成設定 1777
ポスチャのカスタム権限 1779
標準許可ポリシーの設定 1780
ポスチャとネットワーク ドライブ マッピングのベスト プラクティス 1781
エージェントステルスモードのワークフローの設定 1781
エージェントプロファイルの作成 1782
エージェントパッケージのエージェント 設定の作成 1783
Cisco ISE へのオープン DNS プロファイルのアップロード 1783
クライアント プロビジョニング ポリシーの作成 1784
ポスチャ条件の作成 1784

ポスチャ修復の作成 1785
ステルス モードでのポスチャ要件の作成 1785
ポスチャ ポリシーの作成 1785
エージェントステルスモード通知の有効化 1786
Cisco Temporal Agent のワークフローの設定 1787
ポスチャ条件の作成 1787
ポスチャ要件の作成 1788
ポスチャ ポリシーの作成 1788
クライアント プロビジョニング ポリシーの設定 1789
Cisco Temporal Agent のダウンロードと起動 1789
ポスチャのトラブルシューティング ツール 1789
エンドポイント ログイン クレデンシャルの設定 1790
エンドポイントスクリプト設定 1790
Cisco ISE でのクライアント プロビジョニングの設定 1791
クライアント プロビジョニン リソース 1792
シスコからのクライアント プロビジョニング リソースの追加 1793
ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加 1795
ローカルマシンからのエージェント用の顧客作成リソースの追加 1796
ARM64 バージョンのエージェントに対するクライアントプロビジョニング ポリシーの設定 1797
ネイティブ サプリカント プロファイルの作成 1799
ネイティブ サプリカント プロファイルの設定 1800
各種ネットワークでの URL リダイレクトなしでのクライアント プロビジョニング 1802
AMP イネーブラ プロファイルの設定 1804
組み込みプロファイル エディタを使用した AMP イネーブラ プロファイルの作成 1805
スタンドアロン エディタを使用した AMP イネーブラ プロファイルの作成 1806
一般的な AMP イネーブラ インストール エラーのトラブルシューティング 1808
Cisco ISE の Chromebook デバイスのオンボーディングのサポート 1808
共有環境での Chromebook デバイスの使用のベスト プラクティス 1810
Chromebook オンボーディング プロセス 1811
Google 管理コンソールでのネットワークの設定と拡張機能の強制 1811

Chromebook オンボーディング用の Cisco ISE の設定 1813
Chromebook デバイスのワイプ 1814
Google 管理コンソールへの Chromebook の登録 1815
BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続 1815
Google 管理コンソール：Wi-Fi ネットワーク設定 1816
Cisco ISE での Chromebook デバイス アクティビティのモニター 1821
オンボーディング中の Chromebook デバイスのトラブルシューティング 1821
Cisco Secure クライアント 1822
エージェント設定の作成 1823
ポスチャ エージェント プロファイルの作成 1825
クライアント IP アドレスのリフレッシュ設定 1825
ポスチャ プロトコル設定 1827
継続的なエンドポイント属性モニタリング 1828
ポスチャステータスの同期 1829
ポスチャ状態の同期の設定 1830
Cisco Web Agent 1832
クライアント プロビジョニング リソース ポリシーの設定 1832
クライアント プロビジョニング ポリシーの Cisco ISE ポスチャ エージェントの設定 1834
パーソナル デバイスのネイティブ サプリカントの設定 1834
クライアント プロビジョニング レポート 1835
クライアント プロビジョニング イベント ログ 1836
クライアント プロビジョニング ポータルのポータル設定 1836
クライアント プロビジョニング ポータルの言語ファイルの HTML サポート 1840

第 14 章 脅威の封じ込め 1843
脅威中心型 NAC サービス 1843
脅威中心型 NAC サービスの有効化 1847
SourceFire FireAMP アダプタの追加 1848
Cognitive Threat Analytics アダプタの追加 1849
CTA アダプタの許可プロファイルの設定 1851
Course of Action 属性を使用した許可ポリシーの設定 1851

Cisco ISE での脆弱性アセスメントのサポート 1852
脆弱性アセスメント サービスの有効化と設定 1853
脅威中心型 NAC サービスの有効化 1854
Qualys アダプタの設定 1854
Nexpose アダプタの設定 1858
Tenable アダプタの設定 1860
認可プロファイルの設定 1863
脆弱なエンドポイントを隔離する例外ルールの設定 1864
脆弱性アセスメント ログ 1865
信頼できる証明書の設定 1865
メンテナンスの設定 1868
リポジトリの設定 1868
オンデマンド バックアップの設定 1869
スケジュール バックアップの設定 1870
ポリシーのエクスポート設定のスケジュール 1872
一般 TrustSec の設定 1873
ネットワーク リソース 1876
セッション認識型ネットワーク（SAnet）のサポート 1876
ネットワーク デバイス 1877
ネットワーク デバイス定義の設定 1877
デフォルトのネットワーク デバイス定義の設定 1890
デバイス セキュリティ設定 1893
ネットワーク デバイスのインポート設定 1893
ネットワーク デバイス グループの管理 1894
ネットワーク デバイス グループの設定 1895
ネットワーク デバイス グループのインポート設定 1895
ネットワーク デバイス プロファイル設定 1896
外部 RADIUS サーバーの設定 1903
RADIUS サーバー順序 1904
デバイス ポータルの管理 1907
デバイス ポータルの設定 1907

デバイス ポータルのポータル ID 設定 1907
BYOD と MDM ポータルのポータル設定 1908
BYOD ポータルの BYOD 設定 1911
証明書プロビジョニング ポータルのポータル設定 1912
クライアント プロビジョニング ポータルのポータル設定 1916
MDM ポータルの従業員のモバイル デバイス管理設定 1919
デバイス ポータルのポータル設定 1920
デバイス ポータルのログイン ページ設定 1923
デバイス ポータルの利用規定ページ設定 1924
デバイス ポータルのポストログイン バナー ページ設定 1925
デバイス ポータルの従業員によるパスワード変更の設定 1925
デバイス ポータルのデバイス管理設定 1926
デバイス ポータルのデバイス カスタマイズの追加、編集、および検索 1927
デバイス ポータルのサポート情報ページの設定 1927

第 15 章 Cisco pxGrid 1931
Cisco pxGrid と ISE 1931
pxGrid のフィルタリング 1935
pxGrid の概要ページ 1935
pxGrid クライアント管理 1936
pxGrid ポリシーの制御 1936
pxGridサービスの有効化 1938
pxGrid 診断 1938
pxGrid 設定 1939
Cisco pxGrid 証明書の生成 1939
pxGrid証明書の生成における既知の制限 1941
pxGrid 証明書テンプレートのキーサイズの変更 1941

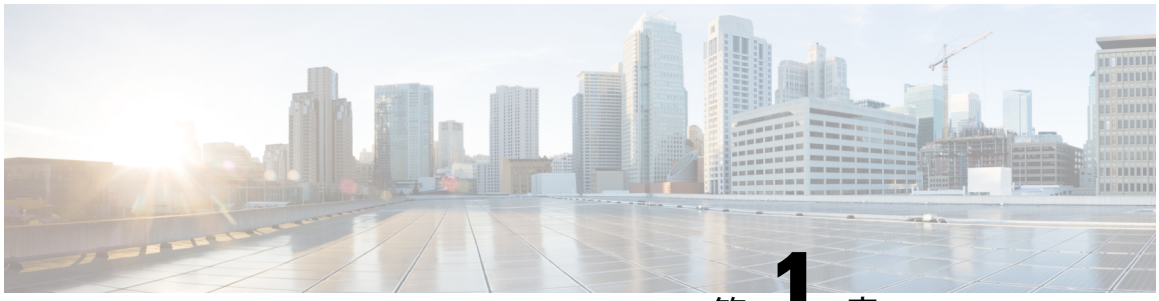
第 16 章 統合 1943
スイッチでの標準 Web 認証のサポートの有効化 1944
代理 RADIUS トランザクション用のローカルユーザー名とパスワードの定義 1944

ログとアカウンティングのタイムスタンプの正確性を保証するための NTP サーバー設定 1944
AAA 機能を有効にするコマンド 1944
スイッチ上の RADIUS サーバーの設定 1945
RADIUS 認可変更（CoA）を処理するスイッチの有効化 1946
スイッチポートでのデバイストラッキングと DHCP スヌーピングの有効化 1946
スイッチポート用 802.1X ポートベースの認証の有効化 1947
クリティカルな認証に対する EAP の有効化 1947
リカバリの遅延を使用した AAA 要求のスロットリング 1947
適用状態に基づく VLAN の定義 1947
スイッチでのローカル（デフォルト）アクセスリスト（ACL）の定義 1948
802.1X および MAB のスイッチ ポートの有効化 1949
Identity-Based Network Services に基づいて 802.1X を有効にするコマンド 1951
EPM ロギングの有効化 1952
SNMP トラップを受信するためのスイッチの有効化 1953
プロファイリング用の SNMP v3 クエリーの有効化 1953
プロファイラによる収集を可能にするための MAC 通知トラップの有効化 1953
スイッチ上での RADIUS アイドルタイムアウトの設定 1954
iOS サプリカントのプロビジョニング用のワイヤレスコントローラの構成 1954
MDM 相互運用性のためのワイヤレス LAN コントローラでの ACL の設定 1955

第 17 章 トラブルシューティング 1957
Cisco ISE のモニタリングとトラブルシューティング サービス 1957
TAC サポートケースのオープン 1958
ヘルス チェック 1959
ヘルスチェックの実行 1960
Network Privilege Framework のイベントフロープロセス 1962
モニタリングおよびトラブルシューティング機能のユーザー ロールと権限 1962
モニタリングデータベースに格納されているデータ 1962
Cisco ISE テレメトリ 1963
テレメトリが収集する情報 1963
Cisco ISE をモニターする SNMP トラップ 1966

Cisco ISE アラーム 1970
アラーム設定 1990
認証結果アラームの設定 1991
カスタム アラームの追加 1993
Cisco ISE アラーム通知およびしきい値 1994
アラームの有効化および設定 1994
モニタリング用の Cisco ISE アラーム 1994
モニタリング アラームの表示 1995
ログ収集 1995
アラーム syslog 収集場所 1996
RADIUS ライブ ログ 1996
TACACS ライブ ログ 2000
ライブ認証 2002
ライブ認証のモニター 2002
[ライブ認証（Live Authentications）] ページでのデータのフィルタ処理 2003
RADIUS ライブ セッション 2004
エクスポート サマリ 2009
認証概要レポート 2011
ネットワーク アクセスの問題のトラブルシューティング 2012
展開およびサポート情報のための Cisco Support Diagnostics 2012
Cisco Support Diagnostics Connector を使用した構成バックアップの取得 2014
診断トラブルシューティング ツール 2014
RADIUS 認証のトラブルシューティング ツール 2015
予期せぬ RADIUS 認証結果のトラブルシューティング 2015
Execute Network Device Command 診断ツール 2016
設定を確認する Cisco IOS show コマンドの実行 2016
設定バリデータの評価ツール 2017
エージェントレスポスチャのトラブルシューティング 2017
ネットワーク デバイス設定の問題のトラブルシューティング 2018
エンドポイント ポスチャの障害のトラブルシューティング 2018
セッション トレース テスト ケース 2019

セッション トレース テスト ケースの設定 2019
着信トラフィックを検証する TCP ダンプユーティリティ 2020
ネットワーク トラフィックのモニタリングでの TCP ダンプの使用 2021
TCP ダンプ ファイルの保存 2022
エンドポイントまたはユーザーの予期しない SGACL の比較 2022
出力ポリシー診断フロー 2023
SXP-IP マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング 2023
IP-SGT マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング 2024
デバイス SGT ツール 2024
デバイス SGT マッピングの比較による TrustSec 対応ネットワークの接続問題のトラブルシューティング 2024
その他のトラブルシューティング情報の入手 2025
Cisco ISE のサポート バンドル 2025
サポート バンドル 2026
Cisco ISE ログ ファイルのダウンロード 2026
Cisco ISE デバッグ ログ 2027
デバッグ ログの入手 2028
デバッグログの設定 2028
Cisco ISE コンポーネントおよび対応するデバッグ ログ 2029
機能別のデバッグウィザードの設定 2031
デバッグ ログのダウンロード 2032



第 1 章

新機能および変更された機能に関する情報

• 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

（注） Cisco ISE リリース 3.4 および対応するガイドは、段階的なロールアウトで入手できます。ソフトウェアの一般提供が開始されるまでは、シスコのアカウントマネージャに連絡して、このリリースをリクエストしてください。段階的なロールアウトが完了すると、Cisco ISE リリース 3.4 および対応するガイドがすべてのお客様に一般提供されます。

次の表に、新機能および変更された機能の要約と参照先を示します。

表 *1 : Cisco ISE* リリース *3.4* の新機能および変更された機能

特長	説明
Cisco ISE のレジリエンシ	Cisco ISE リリース 3.4 以降、Cisco ISE のレジリエンシを維持するために、**過剰な RADIUS ネットワークデバイス通信**アラームと**過剰なエンドポイント通信**アラームが追加されています。 「Cisco ISE アラーム」を参照してください。
デバッグログの設定	各デバッグログコンポーネントに許可される最大ファイルサイズと最大ファイル数を設定できます。これらの値をデフォルトにリセットする必要がある日時を指定することもできます。 デバッグログの設定 （2028 ページ）を参照してください。

新機能および変更された機能に関する情報

特長	説明
URL プッシャ pxGrid Direct コネクタタイプの作成	Cisco ISE GUI を使用して、pxGrid Direct コネクタを作成できます。pxGrid Direct コネクタタイプには、[URLフェッチャ（URL Fetcher）] と [URLプッシャ（URL Pusher）] の 2 種類があります。Cisco ISE リリース 3.4 以降では、[URL フェッチャ（URL Fetcher）] の pxGrid Direct コネクタタイプまたは [URLプッシャ（URL Pusher）] の pxGrid Direct コネクタタイプのいずれかを選択できます。pxGrid Direct プッシュ API を使用して、エンドポイントデータを Cisco ISE にプッシュすることができます。 Cisco ISE リリース 3.4 以降では、配列を含むコネクタ属性を使用して認証プロファイルを設定することもできます。 URL プッシャコネクタタイプの作成（1202 ページ）を参照してください。
レガシー IPSec（ESR）のサポート終了	Cisco ISE リリース 3.4 以降、レガシー IPSec（ESR）は Cisco ISE でサポートされません。Cisco ISE のすべての IPSec 設定が、ネイティブ IPSec 設定になります。トンネルとトンネルの設定が失われないように、Cisco ISE リリース にアップグレードする前に、レガシー IPSec（ESR）からネイティブ IPSec に移行することをお勧めします。 Cisco ISE でのレガシー IPSec からネイティブ IPSec への移行（1413 ページ）を参照してください。
優先順位によるドメインコントローラの選択の強制	優先ドメインコントローラのフェールオーバーが発生した場合に、Cisco ISE のドメインコントローラ選択をオーバーライドすることを選択できるようになりました。このオプションを有効にすると、Cisco ISE は既存の優先順位値をオーバーライドし、左から右への入力順序で優先リスト内の次のドメインコントローラを選択します。 優先ドメインコントローラの設定（1064 ページ）を参照してください。

新機能および変更された機能に関する情報

特長	説明
拡張パスワードセキュリティ	Cisco ISE では、次の機能拡張によりパスワードのセキュリティが向上しています。 • 次のフィールド値の [表示（Show）] ボタンを非表示にして、編集中にプレーンテキストで表示されないようにすることができます。 [ネットワークデバイス（Network Devices）] で、 • RADIUS共有秘密（RADIUS Shared Secret） • Radiusの2番目の共有秘密（Radius Second Shared Secret） [ネイティブIPSec（Native IPSec）] で、 • 事前共有キー（Pre-shared Key） セキュリティ設定の構成（1534ページ）を参照してください。 • ネットワークデバイスのインポートおよびエクスポート中に RADIUS の共有秘密と 2 番目の共有秘密がプレーンテキストで表示されないようにするために、[PasswordEncrypted:Boolean(true|false)] というヘッダーを持つ新しい列が [ネットワークデバイスのインポートテンプレート形式（Network Devices Import Template Format）] に追加されました。この列に必要なフィールド値はありません。 ネットワーク デバイスのインポート テンプレート形式（1405 ページ）を参照してください。
「今すぐ同期」を使用したオンデマンドのpxGrid直接データ同期	Cisco ISE リリース 3.4 以降では、[Sync Now（今すぐ同期）] 機能を使用して、pxGrid Direct コネクタのデータのオンデマンド同期を実行できます。完全同期と増分同期の両方をオンデマンドで実行できます。オンデマンドのデータ同期は、Cisco ISE GUI または OpenAPI を使用して実行できます。 「今すぐ同期」を使用したオンデマンドのpxGrid直接データ同期（1198 ページ）を参照してください。

新機能および変更された機能に関する情報

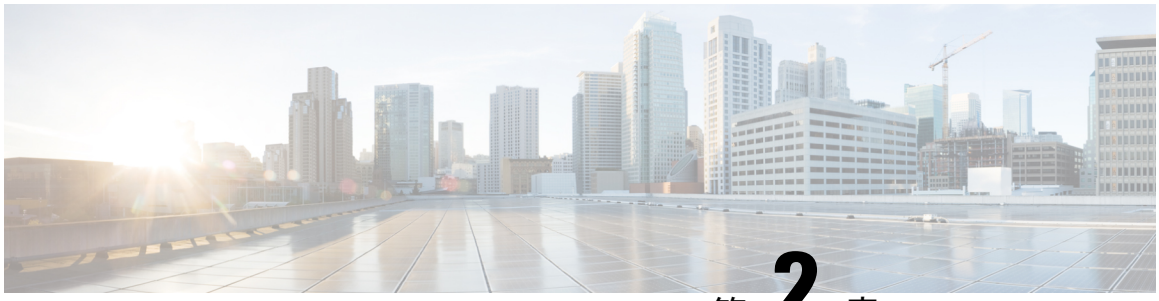
特長	説明
Duo 接続の作成後にアイデンティティ同期を追加するオプション	Duo 接続の作成中に Active Directory と Duo 間のユーザーデータ同期を設定しない場合は、[アイデンティティ同期（Identity Sync）] ページで [スキップ（Skip）] をクリックします。[サマリー（Summary）] ページに直接移動します。 Duo 接続を作成した後は、いつでもアイデンティティ同期設定を追加できます。 多要素認証のための Cisco Duo と Cisco ISE の統合 （1572 ページ）を参照してください。
ユーザーごとの動的アクセス制御リストの動作変更	ユーザーごとの動的アクセス制御リスト（DACL）を使用して認証プロファイルを評価するときに、DACL が Cisco ISE 設定に存在しない場合、認証は失敗し、Cisco ISE はそのユーザーに Access-Reject 応答を送信します。この情報は、[ライブログの詳細（Live Log Details）] ページと [AAA 診断（AAA Diagnostics）] レポートで確認できます。Cisco ISE リリース 3.4 以降では、Cisco ISE ダッシュボードの [アラーム（Alarms）] ダッシュレットにも認証失敗アラームが表示されます。 ダウンロード可能 ACL （1475 ページ）を参照してください。
複数の Cisco Application Centric Infrastructure コネクタのサポート	Cisco ISE を使用すると、複数のドメイン間で一貫したアクセスポリシーを作成して適用できます。Cisco ISE では、Cisco Application Centric Infrastructure（Cisco ACI）を使用して SGT および SGT バインディングを共有できます。また、Cisco ACI からエンドポイントグループ（EPG）、エンドポイント セキュリティ グループ（ESG）、およびエンドポイント情報を学習することもできます。Cisco ISE に複数の Cisco ACI 接続を追加できます。 Cisco ISE で学習したコンテキストを管理し、Cisco ISE コネクタと Cisco ACI コネクタ間のコンテキストフローを最適化するルールを設定できます。 Cisco ISE は、Cisco ACI マルチテナントおよび Multi-Virtual Routing and Forwarding の展開をサポートしています。複数の接続を介してマルチファブリックを定義できます。この統合では、マルチポッドおよび個々の Cisco ACI ファブリックがサポートされます。 Cisco ISE でのシスコ アプリケーション セントリック インフラストラクチャ接続 （1661 ページ）を参照してください。

新機能および変更された機能に関する情報

特長	説明
認証ポリシーのディクショナリグループ内の配列に対する pxGrid Direct のサポート	Cisco ISE リリース 3.4 以降では、ディクショナリ属性として配列とともに pxGrid Direct コネクタのデータを使用して、認証ポリシーを設定することもできます。ポリシーの設定時には、“Contains” または “Matches” の演算子（正規表現の場合）を使用する必要があります。配列がある場合、”Equals” と “In” の演算子は機能しません。"AND" または "OR" 条件を使用して、複数の属性をネストできます。 許可ポリシーの設定（1479ページ）を参照してください。
RADIUS 抑制およびレポートの機能拡張	Cisco ISE リリース 3.4 以降、RADIUS の抑制とレポートに関する機能が拡張され、RADIUS（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS] > [RADIUS設定（RADIUS Settings）]**）設定の運用が容易になっています。 「RADIUS 設定」を参照してください。
トランスポートゲートウェイのサポートの削除	Cisco ISEではトランスポートゲートウェイがサポートされなくなりました。次の Cisco ISE 機能では、接続方法としてトランスポートゲートウェイが使用されていました。 • Cisco ISE スマート ライセンス スマートライセンス設定の接続方法としてトランスポートゲートウェイを使用している場合は、Cisco ISE リリース 3.4 にアップグレードする前に設定を編集する必要があります。Cisco ISE リリース 3.4 ではトランスポートゲートウェイがサポートされていないため、別の接続方法を選択する必要があります。接続方法を更新せずに Cisco ISE リリース 3.4 に更新すると、アップグレードプロセス中に HTTPS 直接接続方法を使用するようにスマートライセンス設定が自動的に更新されます。接続方法は、アップグレード後にいつでも変更できます。 • Cisco ISE テレメトリ Cisco ISE テレメトリを使用する場合、トランスポートゲートウェイは接続方法として使用できなくなりました。テレメトリワークフローは、この変更の影響を受けません。

新機能および変更された機能に関する情報

特長	説明
Cisco ISE ワークフローの TLS 1.3 サポート	Cisco ISE リリース 3.4 では、TLS 1.3 が次のワークフローでピアと通信できます。 • Cisco ISE は、EAP-TLS サーバーとして設定されます • Cisco ISE は、TEAP サーバーとして設定されます **注目** Cisco ISE リリース 3.4 の時点では、TEAP TLS 1.3 が使用可能なクライアント OS でサポートされていないため、TEAP サーバーとして設定された Cisco ISE の TLS 1.3 サポートは、内部テスト条件下でテストされています。 • Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます 「セキュリティ設定の構成（1534 ページ）」を参照してください。

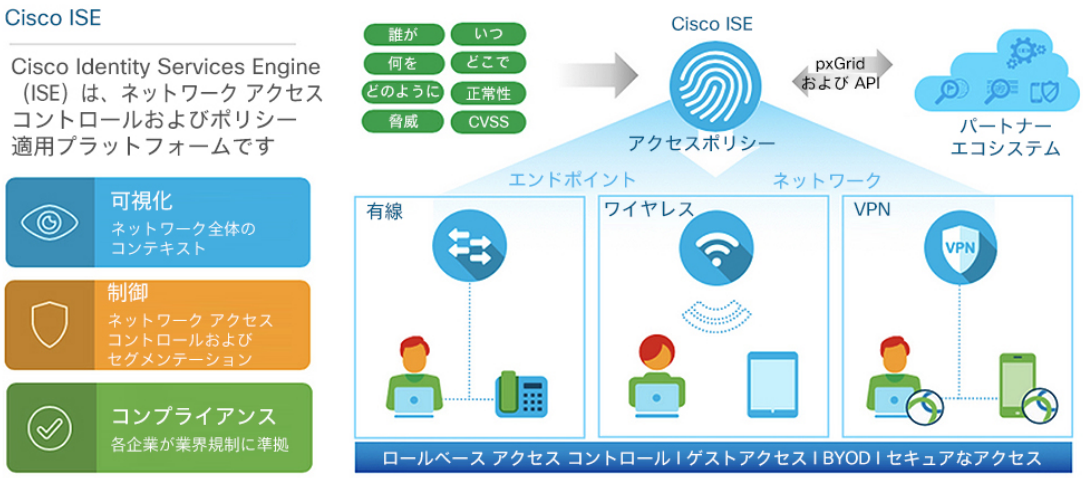


第 2 章

Cisco ISE の概要

- Cisco ISE の概要 （7 ページ）
- Cisco ISE の機能 （8 ページ）
- Cisco ISE 管理者 （9 ページ）
- Cisco ISE 管理者グループ （12 ページ）
- Cisco ISE への管理アクセス （22 ページ）

Cisco ISE の概要



Cisco Identity Services Engine（ISE）は、アイデンティティベースのネットワーク アクセス コントロールおよびポリシー適用システムです。企業におけるエンドポイントのアクセスコントロールとネットワークデバイスの管理を可能にする共通のポリシーエンジンとして機能します。

Cisco ISE を活用すると、コンプライアンスを確保し、インフラストラクチャのセキュリティを強化し、サービス運用を合理化することができます。

Cisco ISE 管理者は、ユーザー/ユーザーグループ（誰が）、デバイスタイプ（何を）、アクセス時間（いつ）、アクセスロケーション（どこで）、アクセスタイプ（有線、ワイヤレス、ま

たはVPN）（どのように）、ネットワークの脅威と脆弱性といった、ネットワークのリアルタイムのコンテキストデータを収集できます。

その後、Cisco ISE 管理者は、この情報を使用してネットワークガバナンス上の決定を下すことができます。また、アイデンティティデータをさまざまなネットワーク要素に結び付けて、ネットワークのアクセスと使用率を管理するポリシーを作成することもできます。

Cisco ISE の機能

Cisco ISE ソフトウェアはそのままインストールする必要があります。基盤となるオペレーティング システム レベルで他のサードパーティ製アプリケーションをインストールすることはできません。

Cisco ISE は、次の機能を備えています。

- **デバイス管理**：Cisco ISE は、TACACS+ セキュリティプロトコルを使用して、ネットワークデバイスの設定を制御および監査します。これによって、どのネットワークデバイスに誰がアクセスできて関連するネットワーク設定を変更できるかについて、きめ細かい制御が容易になります。ネットワークデバイスは、デバイス管理者の操作の認証と許可のために Cisco ISE にクエリを行うように設定できます。また、これらのデバイスは、アカウンティングメッセージを Cisco ISE に送信して、そのような操作を記録します。
- **ゲストおよびセキュアワイヤレス**：Cisco ISE を使用すると、ビジター、請負業者、コンサルタント、および顧客にセキュアなネットワークアクセスを提供できます。Web ベースポータルとモバイルポータルを使用して、企業のネットワークと内部リソースに対するゲストのオンボーディングを行うことができます。さまざまなタイプのゲストのアクセス権限を定義し、スポンサーを割り当てて、ゲストアカウントを作成および管理することができます。
- **個人所有デバイスの持ち込み（BYOD）**：Cisco ISE を使用すると、従業員とゲストが、企業ネットワークで個人のデバイスを安全に使用できるようになります。BYOD機能のエンドユーザーは、設定された手順でデバイスを追加し、事前に定義された認証とネットワークアクセスのレベルをプロビジョニングできます。
- **アセットの可視性**：Cisco ISE を使用すると、ワイヤレス、有線、および VPN 接続の全体にわたって、一貫性のある方法で、ネットワーク上のユーザーとデバイスを可視化し、制御することができます。Cisco ISE は、プローブとデバイスセンサーを使用して、デバイスがネットワークに接続する方法をリッスンします。その後、広範囲にわたる Cisco ISE プロファイルデータベースによって、デバイスが分類されます。これにより、適切なレベルのネットワークアクセスを許可するために必要な可視性とコンテキストが提供されます。
- **セキュアアクセス**：Cisco ISE は、さまざまな認証プロトコルを使用して、ネットワークデバイスとエンドポイントにセキュアなネットワークアクセスを提供します。これには、802.1X、RADIUS、MAB、Web ベース、EasyConnect、および外部エージェント対応の認証方式が含まれます（これらに限定されない）。
- **セグメンテーション**：Cisco ISE は、ネットワークデバイスとエンドポイントに関するコンテキストデータを使用して、ネットワーク セグメンテーションを容易にします。Cisco ISE

がセキュアなネットワークセグメンテーションを実現する方法には、セキュリティグループタグ、アクセス制御リスト、ネットワーク アクセス プロトコル、ポリシーセット（認可、アクセス、認証を定義）などがあります。

- **ポスチャまたはコンプライアンス**：Cisco ISE を使用すると、エンドポイントにネットワークへの接続を許可する前に、そのエンドポイントのコンプライアンス（ポスチャとも呼ばれる）を確認できます。エンドポイントがポスチャサービスに適したポスチャエージェントを確実に受け取るようにすることができます。
- **脅威の封じ込め**：Cisco ISE がエンドポイントから脅威または脆弱性の属性を検出すると、適応型ネットワーク制御ポリシーが送信され、エンドポイントのアクセスレベルが動的に変更されます。脅威または脆弱性が評価され、対処されると、エンドポイントは元のアクセスポリシーに戻されます。
- **セキュリティエコシステム統合**：pxGrid 機能により、Cisco ISE は、接続されたネットワークデバイス、サードパーティベンダー、またはシスコパートナーシステムと、コンテキスト依存情報、ポリシー、設定データなどを安全に共有できます。

Cisco ISE 管理者

管理者は、次の目的で管理者ポータルを使用できます。

- 展開、ヘルプデスク操作、ネットワークデバイス、およびノードのモニタリングとトラブルシューティングの管理。
- Cisco ISE のサービス、ポリシー、管理者アカウント、およびシステム設定と操作の管理。
- 管理者パスワードおよびユーザーパスワードの変更。

CLI 管理者は Cisco ISE アプリケーションの開始と停止、ソフトウェアパッチとアップグレードの適用、Cisco ISE アプライアンスのリロードとシャットダウン、およびすべてのシステムログとアプリケーションログの表示を行うことができます。CLI 管理者には特別な権限が付与されているため、CLI 管理者クレデンシャルを保護し、Cisco ISE 展開を設定および管理する Web ベースの管理者を作成することが推奨されます。

セットアップ時に設定したユーザー名とパスワードは、CLI への管理アクセスにのみ使用されます。このロールは、CLI 管理ユーザー（CLI 管理者）と見なされます。デフォルトでは、CLI 管理ユーザーのユーザー名は admin、パスワードはセットアップで定義したパスワードです。デフォルトのパスワードはありません。この CLI 管理ユーザーはデフォルトの admin ユーザーであり、このユーザーアカウントは削除できません。ただし、他の管理者は編集することが可能で、これには対応するアカウントのパスワードを有効化、無効化、または変更するオプションが含まれています。

管理者を作成するか、または既存のユーザーを管理者ロールに昇格できます。管理者は、対応する管理者権限を無効にすることで、単純なネットワーク ユーザー ステータスに降格することもできます。

管理者は、Cisco ISE システムを設定および操作するローカル権限を持つユーザーです。

管理者は、1 つ以上の管理者グループに割り当てられます。

（注） Cisco ISE リリース 2.7 以降から、Cisco ISE でユーザーアカウントを作成するときには英数字の値を使用します。

関連トピック

Cisco ISE 管理者グループ （12 ページ）

CLI 管理者への外部 ID ストアの使用の強制

外部 ID ソースによる認証は、内部データベースを使用するよりも安全性が高くなります。

Active Directory ユーザーディレクトリでのユーザーの属性の定義

Active Directory を実行している Windows サーバーを使用して、CLI 管理者として設定する予定の各ユーザーの属性を変更します。

1. [サーバーマネージャ（Server Manager）] ウィンドウで、**[サーバーマネージャ（Server Manager）] > [ロール（Roles）] > [Active Directoryドメインサービス（Active Directory Domain Services）] > [Active Directoryのユーザーとコンピュータ（Active Directory Users And Computers）] > [ad.adserver] <*ad_server*>.local>** を選択します。
2. [表示（View）] メニューで [高度な機能（Advanced Features）] を有効にし、ユーザーの属性を編集できるようにします。
3. すべての管理者ユーザーのリストが含まれている Active Directory グループに移動し、ユーザーを選択します。
4. 対応するユーザー ID をダブルクリックします。

   [プロパティ（Properties）] ウィンドウが表示されます。
5. [属性エディタ（Attribute Editor）] をクリックします。
6. 属性をクリックして「**gid**」と入力し、*gidNumber* を見つけます。gidNumber 属性が見つからない場合は、[フィルタ（Filter）] ボタンをクリックし、[値が設定されている属性のみを表示（Show only attributes that have values）] チェックボックスをオフにします。
7. 属性名をダブルクリックして各属性を編集します。各ユーザーの設定を無効にする場合：
   - *uidNumber* に 60000 よりも大きな値を割り当て、この値が一意であることを確認します。割り当ての後に uidNumber を変更しないでください。
   - *gidNumber* に 110 または 111 を割り当てます。110 は管理者ユーザーを表し、111 は読み取り専用ユーザーを示します。gidNumber を変更した場合は、SSH 接続を行う前に 5 分以上待機してください。

Active Directory ドメインへの管理者 CLI ユーザーの参加

Cisco ISE CLI に接続し、**identity-store** コマンドを実行して管理者ユーザーを ID ストアに割り当てます。たとえば、CLI 管理者ユーザーを adpool1 として ISE に定義されている Active Directory にマッピングするには、**identity-store active-directory domain-name adpool1 user admincliuser** コマンドを実行します。

参加が完了したら、Cisco ISE CLI に接続し、管理者 CLI ユーザーとしてログインして設定を確認します。

このコマンドで使用するドメインが以前に ISE ノードに参加していた場合は、管理者コンソールでドメインに再参加する必要があります。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）]。
2. 左側のペインで、[Active Directory] をクリックし、Active Directory の名前を選択します。

（注） MS-RPC または Kerberos のいずれかを使用してテストユーザーとの接続をテストする場合は、Active Directory 接続のステータスに [使用可能（Operational）] と表示されても、エラーメッセージが表示される場合があります。

3. 管理者 CLI ユーザーとして Cisco ISE CLI にこの時点でもログインできることを確認します。

新しい管理者の作成

Cisco ISE 管理者は、特定の管理タスクを実行するために、特定のロールが割り当てられたアカウントが必要です。複数の管理者アカウントを作成して、管理者が実行する必要がある管理タスクに基づいて 1 つ以上のロールを割り当てることができます。

[管理者ユーザー（Admin Users）] ウィンドウを使用して、Cisco ISE 管理者の属性の表示、作成、変更、削除、ステータスの変更、複製、または検索を実行します。

（注） 管理者ユーザーのドメインが CLI と GUI の両方で同じである場合は、CLI で Active Directory アクセスを設定してから GUI に参加することをお勧めします。それ以外の場合は、そのドメインへの認証の失敗を回避するために、GUI からドメインに再参加する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）] > [追加（Add）]**。

ステップ 2 [追加（Add）] ドロップダウンリストから、次のオプションのいずれかを選択します。

- 管理者ユーザーの作成（Create an Admin User）

  [管理者ユーザーの作成（Create an Admin User）] を選択した場合は、[新しい管理者（New Administrator）] ウィンドウが表示されます。このウィンドウから新しい管理者ユーザーのアカウント情報を設定できます。

- ネットワーク アクセス ユーザーからの選択（Select from Network Access Users）

  [ネットワークアクセスユーザーからの選択（Select from Network Access Users）] を選択した場合は、現在のユーザーのリストが表示され、そこからユーザーを選択できます。次に、このユーザーに対応する [管理者ユーザー（Admin User）] ウィンドウが表示されます。

ステップ 3 フィールドに値を入力します。[名前（Name）] フィールドでサポートされる文字は # $ ’ ( ) * + - . / @ _ です。

管理者ユーザー名は一意にする必要があります。既存のユーザー名を入力した場合は、次のメッセージがエラー ポップアップ ウィンドウに表示されます。

```
User can't be created. A User with that name already exists.
```

ステップ 4 [送信（Submit）] をクリックして、新しい管理者を Cisco ISE 内部データベースに作成します。

関連トピック

読み取り専用管理ポリシー （390 ページ）
読み取り専用管理者のメニュー アクセスのカスタマイズ （390 ページ）

Cisco ISE 管理者グループ

管理者グループは、Cisco ISE のロールベース アクセス コントロール（RBAC）グループです。同じグループに属するすべての管理者は、共通の ID を共有し、同じ権限を持ちます。特定の管理者グループのメンバーとしての管理者の ID は、許可ポリシーの条件として使用できます。管理者は、複数の管理者グループに属することができます。

Cisco ISE では、管理者によるユーザーアクセス管理を強化するために、複数の外部 ID ストアがサポートされています。

どのアクセスレベルの管理者アカウントでも、管理者がアクセスできるすべてのウィンドウの、権限を持つオブジェクトを変更または削除できます。

Cisco ISE セキュリティモデルでは、管理者が、その管理者が持っている同じ権限セットが含まれる管理者グループを作成することが制限されます。付与される権限は、Cisco ISE データベースで定義されているユーザーの管理ロールに基づいています。このようにして、管理者グループは、Cisco ISE システムにアクセスするための権限を定義する基礎を形成します。

次の表に、Cisco ISE で事前定義された管理者グループ、およびこれらのグループのメンバーが実行できるタスクを示します。

表 *2 : Cisco ISE* 管理者グループ、アクセス レベル、権限、および制約事項

管理者グループロール	アクセス レベル	権限	制約事項
カスタマイズ管理者	スポンサー、ゲスト、およびパーソナルデバイスポータルの管理。	• ゲストおよびスポンサー アクセスの設定。 • ゲスト アクセス設定の管理。 • エンドユーザー Web ポータルの管理。	• Cisco ISE のすべてのポリシー管理、ID 管理、またはシステムレベルの設定タスクを実行できません。 • レポートを表示できません。
ヘルプデスク管理者	クエリのモニタリングおよびトラブルシューティング操作	• すべてのレポートの実行。 • すべてのトラブルシューティング フローの実行。 • Cisco ISE ダッシュボードとライブログの表示。 • アラームの表示。	レポート、トラブルシューティング フロー、ライブ認証、またはアラームの作成、更新、または削除を実行できません。
ID 管理者	• ユーザーアカウントおよびエンドポイントの管理。 • ID ソースの管理。	• ユーザーアカウントおよびエンドポイントの追加、編集、および削除。 • ID ソースの追加、編集、および削除。 • ID ソース順序の追加、編集、および削除。 • ユーザーアカウントの一般的な設定（属性およびパスワードポリシー）。 • Cisco ISE ダッシュボード、ライブログ、アラーム、およびレポートの表示。 • すべてのトラブルシューティング フローの実行。	Cisco ISE のすべてのポリシー管理またはシステムレベルの設定タスクを実行できません。

管理者グループロール	アクセス レベル	権限	制約事項
MnT 管理者	すべてのモニタリングおよびトラブルシューティング操作の実行。	• すべてのレポートの管理（実行、作成、および削除）。 • すべてのトラブルシューティングフローの実行。 • Cisco ISE ダッシュボードとライブログの表示。 • アラームの管理（作成、更新、表示、および削除）。	Cisco ISE のすべてのポリシー管理、ID 管理、またはシステムレベルの設定タスクを実行できません。
ネットワーク デバイス管理者	Cisco ISE ネットワークデバイスおよびネットワーク デバイス リポジトリの管理。	• ネットワーク デバイスに対する読み取りおよび書き込み権限 • ネットワーク デバイス グループおよびすべてのネットワーク リソース オブジェクト タイプに対する読み取りおよび書き込み権限。 • Cisco ISE ダッシュボード、ライブログ、アラーム、およびレポートの表示。 • すべてのトラブルシューティングフローの実行。	Cisco ISE のすべてのポリシー管理、ID 管理、またはシステムレベルの設定タスクを実行できません。

管理者グループロール	アクセス レベル	権限	制約事項
ポリシー管理者	認証、許可、ポスチャ、プロファイラ、クライアント プロビジョニング、およびワークセンターに関連する、ネットワーク上のすべての Cisco ISE サービスのポリシーの作成および管理。	• ポリシーで使用されるすべての要素（認証プロファイル、ネットワーク デバイス グループ（NDG）、条件など）に対する読み取りおよび書き込み権限。 • ID、エンドポイント、および ID グループ（ユーザー ID グループおよびエンドポイント ID グループ）に対する読み取りおよび書き込み権限。 • サービスポリシーおよび設定に対する読み取りおよび書き込み権限。 • Cisco ISE ダッシュボード、ライブログ、アラーム、およびレポートの表示。 • すべてのトラブルシューティング フローの実行。 • デバイス管理：デバイス管理ワークセンターにアクセス。TACACS ポリシーの条件および結果に関する権限。TACACS プロキシおよびプロキシシーケンスのネットワークデバイス権限。	Cisco ISE のすべての ID 管理またはシステムレベルの設定タスクを実行できません。 デバイス管理：ワークセンターへのアクセスは下位リンクへのアクセスを保証していません。

管理者グループロール	アクセス レベル	権限	制約事項
RBAC 管理者	適応型ネットワーク制御を除く、[操作（Operations）] メニューの下のすべてのタスク、および [管理（Administration）] の下のいくつかのメニュー項目への部分的なアクセス。	• 認証の詳細の表示。 • 適応型ネットワーク制御の有効化/無効化 • アラームの作成、編集、および削除、レポートの生成と表示、Cisco ISE を使用したネットワーク内の問題のトラブルシューティング。 • 管理者アカウント設定および管理者グループ設定に対する読み取り権限 • [RBAC ポリシー（RBAC Policy）] ウィンドウでの管理者アクセス権限とデータアクセス権限に対する表示権限。 • Cisco ISE ダッシュボード、ライブログ、アラーム、およびレポートの表示。 • すべてのトラブルシューティングフローの実行。	Cisco ISE のすべての ID 管理またはシステムレベルの設定タスクを実行できません。

管理者グループロール	アクセス レベル	権限	制約事項
読み取り専用管理者	ISE GUI への読み取り専用アクセス。	• データのフィルタリング、クエリーの実行、オプションの保存、印刷、データのエクスポートなど、ダッシュボード、レポート、およびライブログまたはセッションの機能の表示および使用。 • 自分のアカウントのパスワードの変更。 • グローバル検索、レポート、およびライブログまたはセッションを使用した ISE への照会。 • 属性に基づいたデータのフィルタリングおよび保存。 • 認証ポリシー、プロファイル ポリシー、ユーザー、エンドポイント、ネットワークデバイス、ネットワーク デバイス グループ、ID（グループを含む）、およびその他の構成に関するデータのエクスポート。 • レポート クエリのカスタマイズ、保存、印刷、およびエクスポート。 • カスタム レポート クエリの生成、結果の保存、印刷、またはエクスポート。 • 今後の参照用にGUI設定を保存。 • **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）]** ウィンドウからの ise-psc-log などのログのダウンロード。	

管理者グループロール	アクセス レベル	権限	制約事項
			• 許可ポリシー、認証ポリシー、ポスチャポリシー、プロファイラポリシー、エンドポイント、ユーザーなど、オブジェクトの作成、更新、削除、インポート、検疫、およびモバイルデバイス管理（MDM）アクションなどの構成変更の実行。 • バックアップおよび復元、ノードの登録または登録解除、ノードの同期化、ノードグループの作成、編集、削除、またはパッチのアップグレードおよびインストールなどのシステム操作の実行。 • ポリシー、ネットワークデバイス、ネットワークデバイス グループ、ID（グループを含む）、およびその他の設定に関するデータのインポート。 • CoA、エンドポイントのデバッグ、収集フィルタの変更、ライブセッションデータの抑止のバイパス、PAN-HA フェールオーバー設定の変更、Cisco ISE ノードのペルソナまたはサービスの編集などの操作の実行。 • パフォーマンスに重大な影響を与える可能性のあるコマンドの実行。たとえば、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般的なツール（General Tools）]**

管理者グループロール	アクセス レベル	権限	制約事項
			ウィンドウの [TCP ダンプ（TCP Dump）] へのアクセスは制限されています。 • サポート バンドルの生成。
スーパー管理者	すべての Cisco ISE 管理機能。デフォルトの管理者アカウントは、このグループに属します。	すべての Cisco ISE リソースに対する作成、読み取り、更新、削除、および実行（CRUDX）権限。 スーパー管理者は、Cisco ISE ローカルユーザーのログイン情報をいつでも変更できます。 （注） スーパー管理者ユーザーは、デフォルトのシステム生成 RBAC ポリシーおよび権限は変更できません。これを行うには、ニーズに基づいた必要な権限が含まれた新しい RBACポリシーを作成し、これらのポリシーを管理者グループにマッピングする必要があります。 デバイス管理：デバイス管理ワークセンターにアクセス。TACACSポリシーの条件および結果に関する権限。TACACSプロキシおよびプロキシシーケンスのネットワークデバイス権限。さらに、TACACS グローバル プロトコル設定をイネーブルにする権限。	• デバイス管理：ワークセンターへのアクセスは下位リンクへのアクセスを保証していません。 • 他の管理者ユーザーを変更または削除できるのは、デフォルトの上級管理者グループの管理者ユーザーのみです。上級管理者グループのメニューとデータのアクセス権限で複製された管理者グループに含まれる外部からマッピングされたユーザーであっても、管理者ユーザーを変更または削除することはできません。

管理者グループロール	アクセス レベル	権限	制約事項
システム管理者	すべての Cisco ISE 設定およびメンテナンスのタスク。	[操作（Operations）] タブの下のすべてのアクティビティを実行するためのフルアクセス（読み取りおよび書き込み権限）、および [管理（Administration）] タブの下のいくつかのメニュー項目への部分的なアクセス。 • 管理者アカウント設定および管理者グループ設定に対する読み取り権限。 • RBAC ポリシーウィンドウに加えて、管理者アクセスおよびデータアクセス権限に対する読み取り権限。 • **[管理（Administration）] > [システム（System）]** のすべてのオプションに対する読み取りおよび書き込み権限。 • 認証の詳細の表示。 • 適応型ネットワーク制御の有効化/無効化 • アラームの作成、編集、および削除、レポートの生成と表示、Cisco ISE を使用したネットワーク内の問題のトラブルシューティング。 • デバイス管理：TACACS グローバルプロトコル設定を有効にする権限。	Cisco ISE のすべてのポリシー管理またはシステムレベルの設定タスクを実行できません。
昇格されたシステム管理者（Cisco ISE リリース 2.6、パッチ 2 以降で使用可能）	すべての Cisco ISE 設定およびメンテナンスのタスク。	昇格されたシステム管理者は、システム管理者のすべての権限があるほか、管理者ユーザーを作成できます。	• ネットワーク管理者ユーザーを作成または削除することはできません。 • ネットワーク管理者グループを管理することはできません。

管理者グループロール	アクセス レベル	権限	制約事項
外部 RESTful サービス（ERS）管理者	GET、POST、DELETE、PUT など、すべての ERS API 要求へのフル アクセス	• ERS API 要求の作成、読み取り、更新、および削除。	ロールは、内部ユーザー、アイデンティティグループ、エンドポイント、エンドポイントグループ、および SGT をサポートする ERS 許可のみを対象としています。
外部 RESTful サービス（ERS）オペレータ	ERS API への読み取り専用アクセス、GET のみ	• ERS API 要求の読み取りのみ可能	ロールは、内部ユーザー、ID グループ、エンドポイント、エンドポイントグループ、および SGT をサポートする ERS 許可のみを対象としています。
TACACS+ 管理者	フル アクセス	アクセス先： • デバイス管理ワーク センター。 • 展開（Deployment）：TACACS+ サービスを有効にします。 • 外部 ID ストア。 • **[操作（Operations）] > [TACACS ライブログ（TACACS Live Logs）]** ウィンドウ。	—

関連トピック

Cisco ISE 管理者 （9 ページ）

管理者グループの作成

[管理者グループ（Admin Groups）] ウィンドウでは、Cisco ISE ネットワーク管理者グループを表示、作成、変更、削除、複製、またはフィルタリングできます。

始める前に

外部管理者グループ タイプを設定するには、1 つ以上の外部 ID ストアが指定されている必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]**。

ステップ 2 [追加（Add）] をクリックして名前と説明を入力します。

[名前（Name）] フィールドでサポートされる特殊文字は、スペース、# $ & ‘ ( ) * + -. / @ _ です。

ステップ 3 対応するチェックボックスをオンにして、設定する管理者グループの [タイプ（Type）] を指定します。

- [内部（Internal）]：このグループタイプに割り当てられた管理者は、Cisco ISE 内部データベースに保存されたクレデンシャルに対して認証を行います。
- [外部（External）]：このグループに割り当てられた管理者は、[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [認証方式（Authentication Method）] ウィンドウで選択した外部アイデンティティストアに保存されているクレデンシャルに対して認証を行います。必要に応じて、外部グループを指定できます。

（注） 内部ユーザーに認証用の外部 ID ストアが設定されている場合、内部ユーザーは ISE 管理者用ポータルにログインするときに、その外部 ID ストアを [IDソース（Identity Source）] として選択する必要があります。[内部IDソース（Internal Identity Source）] を選択すると認証が失敗します。

ステップ 4 [メンバーユーザー（Member Users）] 領域の [追加（Add）] をクリックして、ユーザーをこの管理者グループに追加します。ユーザーを管理者グループから削除するには、削除するユーザーに対応するチェックボックスをオンにして、[削除（Remove）] をクリックします。

ステップ 5 [送信（Submit）] をクリックします。

Cisco ISE への管理アクセス

Cisco ISE 管理者は、自分が属する管理者グループに基づいてさまざまな管理タスクを実行できます。これらの管理タスクは重要です。ネットワーク内の Cisco ISE の管理が許可されているユーザーにのみ、管理アクセス権を付与します。

（注） Cisco ISE サーバーがネットワークに追加されると、その Web インターフェイスが起動した後に実行状態になるとマークされます。ただし、ポスチャサービスなどの一部のアドバンスドサービスが使用可能になるまでに時間がかかる場合があるため、すべてのサービスが完全に動作するまでに時間がかかることがあります。

管理アクセスの方法

Cisco ISE サーバーには、いくつかの方法で接続することができます。ポリシー管理ノード（PAN）は、管理者ポータルを実行します。ログインするには管理者パスワードが必要です。CLI を実行できる SSH またはコンソールを使用すると、他の ISE ペルソナサーバーにアクセスできます。このセクションでは、各接続タイプで利用可能なプロセスとパスワードのオプションについて説明します。

- [管理者パスワード（Admin password）]：インストール時に作成した Cisco ISE 管理者ユーザーのタイムアウトは、デフォルトで 45 日間です。**[管理（Administration）] > [システム（System）] > [管理者設定（Admin Settings）]** から [パスワードの有効期間（Password

Lifetime）]をオフにすると、これを回避できます。[パスワードポリシー（Password Policy）]タブをクリックし、[パスワードライフタイム（Password Lifetime）]で[管理パスワードの有効期限（Administrative passwords expire）]チェックボックスをオフにします。

この操作を行わないと、パスワードの有効期限が切れます。管理者パスワードは CLI で **application reset-passwd** コマンドを実行してリセットできます。CLI にアクセスするコンソールに接続するか、またはブートオプションメニューにアクセスする ISE イメージファイルを再起動することにより、管理者パスワードをリセットできます。

- [CLI パスワード（CLI password）]：CLI パスワードはインストール時に指定する必要があります。無効なパスワードが原因で CLI へのログインに問題がある場合は、CLI パスワードをリセットできます。コンソールに接続し、**password** CLI コマンドを実行して、パスワードをリセットします。詳細については、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。
- [CLIへのSSHアクセス（SSH access to the CLI）]：インストール中またはインストール後に **service sshd** コマンドを使用して、SSH アクセスを有効にすることができます。また、SSH 接続でキーを使用するように強制することもできます。この場合、ネットワークデバイスすべてへの SSH 接続にもそのキーを使用します。詳細については、SSH キーの検証（1647 ページ）を参照してください。SSH キーで Diffie-Hellman アルゴリズムの使用を強制できます。ECDSA キーは、SSH キーではサポートされないことに注意してください。

Cisco ISE でのロールベースの管理者アクセス コントロール

Cisco ISE では、管理権限を制限することでセキュリティを確保するロールベース アクセス コントロール（RBAC）ポリシーが提供されます。RBAC ポリシーは、ロールおよび権限を定義するためにデフォルトの管理者グループに関連付けられています。標準的な権限セット（メニューおよびデータ アクセス）が、事前定義された管理者グループそれぞれとペアになっており、それによって、関連付けられたロールおよび職務機能と整合性がとられています。

ユーザーインターフェイスにある一部の機能には、使用するために特定の権限が必要です。ある機能が使用できない場合、または特定のタスクの実行が許可されない場合、その機能を利用するタスクを実行するのに必要な権限が自分の管理者グループにない場合があります。

アクセスレベルに関係なく、すべての管理者アカウントは、管理者がアクセスできるすべてのウィンドウで、権限を持つオブジェクトを変更または削除できます。

（注） ネットワーク管理者または読み取り専用管理者の権限を持つシステム定義の管理者ユーザーのみが、ユーザーグループに含まれていないアイデンティティベースのユーザーを表示できます。これらの権限なしで作成した管理者は、それぞれのユーザーを表示することはできません。

ロールベースの権限

Cisco ISE ではメニューおよびデータレベルの権限を設定することができます。これらは、メニューアクセス権限とデータアクセス権限と呼ばれます。

メニューアクセス権限により、Cisco ISE 管理インターフェイスのメニューおよびサブメニュー項目を表示または非表示にすることができます。この機能によって、メニュー レベルのアクセスを制限または有効にすることができるように権限を作成することができます。

データアクセス権限により、Cisco ISE インターフェイスの管理者グループ、ユーザー ID グループ、エンドポイント ID グループ、ロケーション、およびデバイスタイプのデータへ、読み取り/書き込みアクセス権、読み取り専用アクセス権、またはアクセス権なしを付与できます。

RBAC ポリシー

RBAC ポリシーにより、管理者にメニュー項目やその他の ID グループ データ要素への特定のタイプのアクセスを付与できるかどうかが決定されます。RBAC ポリシーを使用して、管理者グループに基づく管理者に、メニュー項目または ID グループデータ要素へのアクセスを許可または拒否できます。管理者は、管理者ポータルにログインすると、関連付けられている管理者グループに定義されているポリシーおよび権限に基づいて、メニューおよびデータにアクセスできます。

RBAC ポリシーは、管理者グループをメニュー アクセス権限とデータ アクセス権限にマッピングします。たとえば、ネットワーク管理者に[管理者アクセス（Admin Access）]操作メニューおよびポリシーデータ要素を表示しないようにすることができます。これは、ネットワーク管理者が関連付けられるカスタム RBAC ポリシーを管理者グループに作成することで実現できます。

（注） 管理者アクセス用にカスタマイズされた RBAC ポリシーを使用している場合は、特定のデータ アクセスに関連するすべてのメニューアクセスが提供されていることを確認します。たとえば、ID またはポリシー管理者のデータ アクセス権を持つエンドポイントを追加または削除するには、[ワークセンター（Work Center）] > [ネットワークアクセス（Network Access）] と [管理（Administration）] > [IDの管理（Identity Management）] のメニュー アクセスを指定する必要があります。

デフォルトのメニュー アクセス権限

Cisco ISE では、事前定義された一連の管理者グループに関連付けられた、すぐに使用できる権限セットが用意されています。事前定義済みの管理者グループ権限により、任意の管理者グループのメンバーが、管理インターフェイス内のメニュー項目へのフルアクセス権または制限されたアクセス権（メニューアクセスと呼ばれます）を持つように権限を設定したり、その他の管理者グループのデータ アクセス要素の使用（データ アクセスと呼ばれます）を管理者グループに委任するように権限を設定したりできます。これらの権限は、さまざまな管理者グループ用の RBAC ポリシーの策定にさらに使用できる再利用可能なエンティティです。Cisco ISE では、デフォルトの RBAC ポリシーですでに使用されている一連のシステム定義メニュー

アクセス権限が用意されています。定義済みのメニュー アクセス権限とは別に、Cisco ISE では RBAC ポリシーで使用できるカスタム メニュー アクセス権限を作成することができます。キーアイコンはメニューとサブメニューのメニューアクセス権限を表し、クロス付きのキーアイコンは異なる RBAC グループのアクセス権限がないことを表します。

（注） 上級管理者ユーザーの場合、すべてのメニュー項目が使用可能です。その他の管理者ユーザーの場合、[メニューアクセス権限（Menu Access Privileges）] カラムのすべてのメニュー項目はスタンドアロン展開、および分散展開におけるプライマリノードで使用可能です。分散展開のセカンダリノードの場合、[管理（Administration）] タブの下のメニュー項目は使用不可です。

表 *3:* さまざまな管理者グループのデフォルトメニューアクセス許可

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
ホーム（Home）	√	√	√	√	√	√	√	√	x	x
[ホーム（Home）] > [概要（Inclution）]	√	√	√	√	√	√	√	√	x	x
[ホーム（Home）] > [ダッシュボード（Dshbord）]	√	√	√	√	√	√	√	√	x	x
コンテキストの可視性（Context Visibility）	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]	√	√	√	√	√	√	√	√	x	x
[コンテキストの可視性（Context Visibility）] > [ユーザー（Users）]	√	√	√	√	√	√	√	√	x	x
[コンテキストの可視性（Context Visibility）] > [ネットワークデバイス（Network Devices）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[コンテキストの可視性（Context Visibility）] > [アプリケーション（Application）]	√	√	√	√	√	√	√	√	x	x
操作（Operations）	√	√	√	√	√	√	√	√	x	√
[操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）]	√	√	x	x	x	x	x	x	x	x
[操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）] > [ポリシーリスト（Policy List）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）] > [エンドポイント割り当て（Endpoint Assignment）]	√	√	x	x	x	x	x	x	x	x
[操作（Operations）] > [レポート（Reports）]	√	√	√	√	√	√	√	√	x	x
[操作（Operations）] > [RADIUS]	√	√	√	√	√	√	√	√	x	x
[操作（Operations）] > [RADIUS] > [ライブログ（Live logs）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [RADIUS] > [ライブセッション（Live Sessions）]	√	√	√	√	√	√	√	√	x	x
[操作（Operations）] > [脅威中心型 NAC のライブログ（Threat Centric NAC Live Log）]	√	√	√	√	√	√	√	√	x	x
[操作（Operations）] > [TACACS]	√	√	√	√	√	√	√	√	x	√
[操作（Operations）] > [TACACS] > [ライブログ（Live Logs）]	√	√	√	√	√	√	√	√	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshoot）]	√	√	√	√	√	√	√	√	x	x
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）]	√	x	x	x	x	x	x	x	x	x
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ネットワークデバイスコマンドの実行（Execute Network Device Command）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [設定バリデータの評価（Evaluate Configuration Validator）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ポスチャのトラブルシューティング（Posture Troubleshooting）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断（Diagnostics）] > [一般ツール（General Tools）] > [エージェントレスポスチャのトラブルシューティング（Agentless Posture Troubleshooting）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [エンドポイントデバッグ（Endpoint Debug）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [TCP ダンプ（TCP Dump）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [セッショントレーステスト（Session Trace Test）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [セキュリティグループアクセスツール（Security Group Access Tools）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [セキュリティグループアクセスツール（Security Group Access Tools）] > [SXP-IP マッピング（SXP-IP Mappings）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [セキュリティグループアクセスツール（Security Group Access Tools）] > [IP ユーザー SGT（IP User SGT）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [セキュリティグループアクセスツール（Security Group Access Tools）] > [出力（SGACL）ポリシー（Egress (SGACL) Policy）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [セキュリティグループアクセスツール（Security Group Access Tools）] > [デバイス SGT（Device SGT）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [デバッグウィザード（Debug Wizard）]	√	√	√	√	√	√	√	√	x	x
[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグログの設定（Debug Log Configuration）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [デバッグウィザード（Debug Wizard）] > [デバッグプロファイルの設定（Debug Profile Configuration）]	√	√	√	√	√	√	√	√	x	x
ポリシー（Policy）	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ライブラリ条件（Library Conditions）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ライブラリ条件（Library Conditions）] > [単純条件（Simple Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [スマート条件（Smart Conditions）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [単純条件（Simple Conditions）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [複合条件（Compound Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [時刻と日付（Time and Date）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [スパイウェア対策条件（Anti-Spyware Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [アプリケーション条件（Application Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディクショナリ複合条件（Dictionary Compound Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディクショナリ単純条件（Dictionary Simple Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [外部データソース条件（External DataSource Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ファイル条件（File Conditions）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ファイアウォール条件（Firewall Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ハードウェア属性条件（Hardware Attributes Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [パッチ管理条件（Patch Management Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [レジストリ条件（Registry Conditions）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [サービス条件（Service Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [USB 条件（USB Conditions）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [マルウェア対策条件（AntiMalware Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ウイルス対策条件（AntiSpyware Conditions）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [複合条件（Compund Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [エンドステーションネットワーク条件（Endstation Network Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [デバイスポートネットワーク条件（Device Port Network Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [デバイスポートネットワーク条件（Device Port Network Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [プロファイリング（Profiling）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されたプロトコル（Allowed Protocols）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [例外アクション（Exception Actions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Actions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [マルウェア対策修復（AntiMalware Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [ウィルス対策修復（Anti-Virus Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [ファイアウォール修復（Firewall Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [リンク修復（Link Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [スクリプト修復（Script Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [USB 修復（USB Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [Windows 更新修復（Windows Update Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [アプリケーション修復（Application Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [スパイウェア対策修復（Anti-Spyware Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [ファイル修復（File Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [起動プログラム修復（Launch Program Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [パッチ管理修復（Patch Management Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [修復アクション（Remediation Actions）] > [Windows サーバー更新サービス修復（Windows Server Update Service Remediation）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [認証（Authentication）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ポリシー（Policy）] > [許可（Authorization）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [プロファイリング（Profiling）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [ポスチャ（Posture）]	√	√	x	x	x	x	x	x	x	x
[ポリシー（Policy）] > [クライアントプロビジョニング（Client Provisioning）]	√	√	x	x	x	x	x	x	x	x
管理（Administration）	√	√	x	√	√	√	√	x	√	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ID管理（Identity Management）]	√	√	x	√	x	x	x	x	x	√
[管理（Administration）] > [ID管理（Identity Management）] > [ID（Identities）]	√	√	x	√	x	x	x	x	x	x
[管理（Administration）] > [ID管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ID管理（Identity Management）] > [ID（Identities）] > [最新の手動ネットワークスキャン結果（Latest Manual Network Scan Results）]	√	√	x	√	x	x	x	x	x	x
[管理（Administration）] > [ID管理（Identity Management）] > [グループ（Groups）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）]	√	√	x	√	x	x	x	x	x	√
[管理（Administration）] > [ID管理（Identity Management）] > [IDソース順序（Identity Source Sequences）]	√	√	x	√	x	x	x	x	x	x
[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [ユーザーカスタム属性（User Custom Attributes）]	√	√	x	√	x	x	x	x	x	x
[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [エンドポイントの消去（Endpoint Purge）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [ユーザー認証設定（User Authentication Settings）]	√	√	x	√	x	x	x	x	x	x
[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [エンドポイントカスタム属性（Endpoint Custom Attributes）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [REST IDストア設定（REST ID Store Settings）]	√	√	x	√	x	x	x	x	x	x
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）]	√	√	x	x	x	x	x	x	√	x
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [BYOD]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [クライアントプロビジョニング（Client Provisioning）]	√	√	x	x	x	x	x	x	√	x
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイス（My Devices）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [ブロックリスト（Blocked List）]	√	√	x	x	x	x	x	x	√	x
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [モバイルデバイス管理（Mobile Device Management）]	√	√	x	x	x	x	x	x	√	x
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [カスタムポータルファイル（Custom Portal Files）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）]	√	√	x	x	x	x	x	x	√	x
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [再試行URL（Retry URL）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）]	√	√	x	x	x	x	x	x	√	x
[管理（Administration）] > [ネットワークリソース（Network Resources）]	√	x	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]	√	x	x	x	√	x	x	x	x	x
[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デフォルトのデバイス（Default Devices）]	√	x	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [ネットワークデバイス（Network Devices）]	√	x	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デバイスセキュリティ設定（Device Security Settings）]	√	x	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）]	√	x	x	x	√	x	x	x	x	x
[管理（Administration）] > [ネットワークリソース（Network Resources）] > [外部 RADIUS サーバー（External RADIUS Servers）]	√	x	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）]	√	x	x	x	√	x	x	x	x	x
[管理（Administration）] > [ネットワークリソース（Network Resources）] > [RADIUS サーバー順序（RADIUS Server Sequences）]	√	x	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [ネットワークリソース（Network Resources）] > [外部 MDM（External MDM）]	√	x	x	x	x	x	x	x	x	x
[管理（Administration）] > [pxGrid サービス（pxGrid Services）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [概要（Summary）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント管理（Client Management）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント管理（Client Management）] > [クライアント（Clients）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント管理（Client Management）] > [ポリシー（Policy）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント管理（Client Management）] > [グループ（Groups）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント管理（Client Management）] > [証明書（Certificates）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント管理（Client Management）] > [pxGrid 接続（pxGrid Connection）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント管理（Client Management）] > [pxCloud ポリシー（pxCloud Policy）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [診断（Diagnostics）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [診断（Diagnostics）] > [WebSocket]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [診断（Diagnostics）] > [ログ（Log）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [診断（Diagnostics）] > [テスト（Tests）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）]	√	√	x	x	x	√	√	x	x	√
[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup & Restore）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup & Restore）] > [ポリシーのエクスポート（Policy Export）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup & Restore）] > [バックアップと復元（Backup & Restore）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）]	√	x	x	x	x	√	√	x	x	x
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）]	√	x	x	x	x	√	√	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）]	√	x	x	x	x	√	√	x	x	x
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]	√	x	x	x	x	√	√	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]	√	x	x	x	x	√	√	x	x	x
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）]	√	x	x	x	x	√	√	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [権限（Permissions）]	√	x	x	x	x	√	√	x	x	x
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [権限（Permissions）] > [メニューアクセス（Menu Access）]	√	x	x	x	x	√	√	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [権限（Permissions）] > [データアクセス（Data Access）]	√	x	x	x	x	√	√	x	x	x
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [ポリシー（Policy）]	√	x	x	x	x	√	√	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [アクセス（Access）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [セッション（Session）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [管理アクセス（Admin Access）] > [設定（Settings）] > [ポータルのカスタマイズ（Portal Customization）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [最大セッション数（Max Sessions）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [インタラクティブユーザーガイド（Interactive User Guide）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [DHCP および DNS サービス（DHCP & DNS Services）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ライトセッションディレクトリ（Light Session Directory）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [EAP-FAST の設定（EAP-FAST Settings）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [PAC の生成（Generate PAC）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-TLS]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-TLS]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [PEAP]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [IPSec]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [Network Success Diagnostics]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [Network Success Diagnostics] > [テレメトリ（Telemetry）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [Network Success Diagnostics] > [Cisco Support Diagnostics]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアントプロビジョニング（Client Provisioning）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [FIPS モード（FIPS Mode）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMTP サーバ（SMTP Server）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMS ゲートウェイ（SMS Gateway）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [システム時刻（プライマリノード）（System Time (Primary Node)）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarm Settings）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [アクセプタブル ユース ポリシー（Acceptable Use Policy）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）] > [ログイン設定（Login Configuration）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）] > [設定（Settings）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [設定（Settings）] > [API ゲートウェイ設定（API Gateway Settings）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [展開（Deployment）]	√	x	x	x	x	√	x	x	x	√
[管理（Administration）] > [システム（System）] > [ライセンシング（Licensing）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [アップグレード（Upgrade）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [ヘルスチェック（Health Checks）]	√	x	x	x	x	x	x	x	x	x
[管理（Administration）] > [システム（System）] > [証明書（Certificates）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書署名要求（Certificate Signing Requests）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [システム証明書（System Certificates）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [OCSP クライアント プロファイル（OCSP Client Profile）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書定期チェックの設定（Certificate Periodic Check Settings）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [概要（Overview）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [発行された証明書（Issued Certificates）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [内部 CA 設定（Internal CA Settings）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [証明書テンプレート（Certificate Templates）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [外部 CA 設定（External CA Settings）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [ロギング（Logging）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [収集フィルタ（Collection Filters）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ログ設定（Log Settings）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモートロギング ターゲット（Remote Logging Targets）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージカタログ（Message Catalog）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [ローカルディスク管理（Local Disk Management）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [運用データの消去（Operational Data Purging）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [セッション情報（Session Info）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [システム（System）] > [システム時刻（セカンダリノード）（System Time (Secondary Node)）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [サーバー証明書（Server Certificate）]	√	x	x	x	x	√	x	x	x	x
[管理（Administration）] > [システム（System）] > [証明書署名要求（Certificate Signing Requests）]	√	x	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [フィードサービス（Feed Service）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [フィードサービス（Feed Service）] > [プロファイラ（Profiler）]	√	√	x	x	x	√	x	x	x	x
[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）]	√	x	x	x	x	x	x	x	x	x
ワークセンター（Work Centers）	√	√	√	√	√	√	√	√	√	√
[ワークセンター（Work Centers）] > [TrustSec]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGT スタティックマッピング（IP SGT Static Mapping）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティ グループ（Security Groups）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ ACL（Security Group ACLs）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [TrustSec サーバー（TrustSec Servers）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [TrustSec サーバー（TrustSec Servers）] > [AAA サーバー（AAA Servers）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [TrustSec サーバー（TrustSec Servers）] > [HTTPS サーバー（HTTPS Servers）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [宛先ツリー（Destination Tree）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [送信元ツリー（Source Tree）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [ネットワークデバイス認証（Network Device Authorization）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [ポリシーセット（Policy Set）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [許可ポリシー（Authorization Policy）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [SXP]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXP デバイス（SXP Devices）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [すべての SXP マッピング（All SXP Mappings）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [ACI]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [レポート（Reports）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [概要（Overview）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [概要（Overview）] > [はじめに（Introduction）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [概要（Overview）] > [ダッシュボード（Dashboard）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [ポリシーセット（Policy Set）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [ポリシーセット（Policy Set）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [認証ポリシー（Authorization Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [トラブルシューティング（Troubleshoot）]	√	√	√	√	√	√	√	√	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [トラブルシューティング（Troubleshoot）] > [出力（SGACL）ポリシー（Egress (SGACL) Policy）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [トラブルシューティング（Troubleshoot）] > [IP ユーザー SGT（IP User SGT）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [トラブルシューティング（Troubleshoot）] > [SXP-IP マッピング（SXP-IP Mapping）]	√	√	√	√	√	√	√	√	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [トラブルシューティング（Troubleshoot）] > [デバイス SGT（Device SGT）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSecの全般設定（General TrustSec Settings）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ワークプロセスの設定（Work Process Settings）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ACI 設定（ACI Settings）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSec マトリックスの設定（TrustSec Matrix Settings）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [SXP 設定（SXP Settings）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）]	√	√	√	√	√	√	√	√	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [外部 ID ソース（Ext Id Sources）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [エンドポイントの分類（Endpoint Classification）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ノード設定（Node Config）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャンの結果（Manual NMAP Scan Results）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャン（Manual NMAP Scan）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシーセット（Policy Set）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [許可ポリシー（Authorization Policy）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [レポート（Reports）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [フィード（Feeds）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシー要素（Policy Elements）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシー要素（Policy Elements）] > [プロファイラ条件（Profiler Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシー要素（Policy Elements）] > [NMAP スキャンアクション（NMAP Scan Actions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシー要素（Policy Elements）] > [例外アクション（Exception Actions）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [プロファイリングポリシー（Profiling Policies）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシーセット（Policy Set）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [トラブルシューティング（Troubleshoot）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [トラブルシューティング（Troubleshoot）] > [ネットワークデバイスコマンドの実行（Execute Network Device Command）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [トラブルシューティング（Troubleshoot）] > [エンドポイントのデバッグ（EndPoint Debug）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [トラブルシューティング（Troubleshoot）] > [設定バリデータの評価（Evaluate Configuration Validator）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [トラブルシューティング（Troubleshoot）] > [TCP ダンプ（TCP Dump）]	√	x	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）] > [プロファイラの設定（Profiler Settings）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）] > [NMAP スキャンサブネット除外（NMAP Scan Subnet Exclusions）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ディクショナリ（Dictionaries）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [概要（Overview）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ネットワークデバイス（Network Devices）]	√	√	x	x	√	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）]	√	√	√	√	√	√	√	√	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ネットワークデバイス（Network Devices）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャポリシー（Posture Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [許可ポリシー（Authorization Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [レポート（Reports）]	√	√	√	√	√	√	√	√	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ポスチャの全般設定（Posture General Settings）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [アクセプタブル ユース ポリシー（Acceptable Use Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアの更新（Software Updates）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアの更新（Software Updates）] > [クライアントプロビジョニング（Client Provisioning）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアの更新（Software Updates）] > [ポスチャの更新（Posture Updates）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアの更新（Software Updates）] > [プロキシの設定（Proxy Settings）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [再評価設定（Reassessment configurations）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [概要（Overview）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [クライアントプロビジョニング（Client Provisioning）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [クライアントプロビジョニング（Client Provisioning）] > [クライアントプロビジョニングポリシー（Client Provisioning Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [クライアントプロビジョニング（Client Provisioning）] > [クライアントプロビジョニングポータル（Client Provisioning Portal）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [スパイウェア対策（Anti-Spyware）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [アプリケーション（Application）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [複合（Compound）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ディクショナリ複合（Dictionary Compound）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ファイル（File）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [レジストリ（Registry）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [マルウェア対策（AntiMalware）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ウイルス対策（Anti-Virus）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ディクショナリ単純（Dictionary Simple）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ディスク暗号化（Disk Encryption）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [外部データソース（External DataSource）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ファイアウォール条件（Firewall Condition）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ハードウェア属性条件（Hardware Attributes Condition）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [パッチ管理（Patch Management）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Condtions）] > [サービス（Service）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Condtions）] > [USB]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [要件（Requirements）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [修復（Remediations）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediations）] > [ウィルス対策（AntiVirus）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediation）] > [ファイアウォール（Firewall）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediation）] > [リンク（Link）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediation）] > [スクリプト（Script）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediation）] > [Windows Server Update Services]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediations）] > [マルウェア対策（AM Rule）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediations）] > [スパイウェア対策（Antispyware）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediation）] > [ファイル（File）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediation）] > [プログラムの起動（Launch Program）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediation）] > [パッチ管理（Patch Management）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediation）] > [USB]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [修復（Remediation）] > [Windows Update]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [許可プロファイル（Administration Profiles）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [認証ポリシー（Authentication Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [トラブルシューティング（Troubleshoot）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [トラブルシューティング（Troubleshooting）] > [エージェントレスポスチャのトラブルシューティング（Agentless Posture Troubleshooting）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）]	√	√	√	√	√	√	√	√	x	√
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）] > [はじめに（Introduction）]	√	√	x	x	x	x	x	x	x	√
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）] > [TACACS ライブログ（TACACS Livelog）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）] > [展開（Deployment）]	√	√	x	x	x	x	x	x	x	√
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ID（Identities）]	√	√	x	√	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ID（Identities）] > [ユーザー（Users）]	√	√	x	√	x	x	x	x	x	√
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ユーザーID グループ（User Identity Groups）]	√	√	x	√	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [外部 ID ソース（Ext Id Sources）]	√	√	x	√	x	x	x	x	x	√
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）]	√	√	x	x	√	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスグループ（Network Device Groups）]	√	√	x	x	√	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク リソース（Network Resources）] > [デフォルトのデバイス（Default Devices）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [TACACS 外部サーバー（TACACS External Servers）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [TACACS サーバー順序（TACACS Server Sequence）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）]	√	√	x	x	x	x	x	x	x	√
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [認証の単純条件（Authentication Simple Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ライブラリ条件（Library Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [スマート条件（Smart Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可の単純条件（Administration Simple Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可の複合条件（Authorization Compound Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [ネットワーク条件（Network Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [ネットワーク条件（Network Conditions）] > [エンドステーションネットワーク条件（Endstation Network Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [ネットワーク条件（Network Conditions）] > [デバイスネットワーク条件（Device Network Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [ネットワーク条件（Network Conditions）] > [デバイスポートネットワーク条件（Device Port Network Conditions）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可されるプロトコル（Allowed Protocols）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS コマンドセット（TACACS Command Sets）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）]	√	√	x	x	x	x	x	x	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]	√	√	x	x	x	x	x	x	x	√
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [レポート（Reports）]	√	√	√	√	√	√	√	√	x	√

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）]	√	√	x	x	x	x	x	x	x	√
[ワークセンター（Work Centers）] > [PassiveID]	√	√	√	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [概要（Overview）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [概要（Overview）] > [はじめに（Introduction）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [概要（Overview）] > [ダッシュボード（Dashboard）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [概要（Overview）] > [ライブセッション（Live Sessions）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [トラブルシューティング（Troubleshoot）]	√	√	√	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [システム証明書（System Certificates）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [OCSP クライアントプロファイル（OCSP Client Profile）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [証明書の定期的なチェックの設定（Certificate Periodic Check Settings）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [発行した証明書（Issued Certificates）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [内部CAの設定（Internal CA Settings）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [証明書テンプレート（Certificate Templates）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [概要（Overview）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [証明書（Certificates）] > [認証局証明書（Certificate Authority Certificates）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [レポート（Reports）]	√	√	√	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [エージェント（Agents）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [SPAN]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [マッピングフィルタ（Mapping Filters）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [Active Directory]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [API プロバイダー（API Providers）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [Syslog プロバイダー（Syslog Providers）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [エンドポイントプローブ（Endpoint Probes）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [PassiveID] > [サブスクライバ（Subscribers）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD]	√	√	√	√	√	√	√	√	√	x
[ワークセンター（Work Centers）] > [BYOD] > [概要（Overview）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ネットワークデバイス（Network Devices）]	√	√	x	x	√	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [クライアントプロビジョニング（Client Provisioning）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [クライアントプロビジョニング（Client Provisioning）] > [クライアントプロビジョニングポリシー（Client Provisioning Policy）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [結果（Results）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Admission Profiles）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可されるプロトコル（Allowed Protocols）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ダウンロード可能 ACL（Downloadable ACLs）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [条件（Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [認証の単純条件（Authentication Simple Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可の単純条件（Authorization Simple Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ライブラリ条件（Library Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [スマート条件（Smart Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可の複合条件（Authorization Compound Conditions）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [認証ポリシー（Authentication Policy）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [レポート（Reports）]	√	√	√	√	√	√	√	√	x	x
[ワークセンター（Work Centers）] > [BYOD] > [設定（Settings）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [設定（Settings）] > [従業員が登録済みのデバイス（Employee Registered Devices）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [設定（Settings）] > [クライアントプロビジョニング（Client Provisioning）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [設定（Settings）] > [再試行URL（Retry URL）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [ID（Identities）]	√	√	x	√	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [ID（Identities）] > [エンドポイント（Endpoints）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ID（Identities）] > [ID ソース順序（Identity Source Sequences）]	√	√	x	√	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [ID（Identities）] > [ネットワークアクセス ユーザー（Network Access Users）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [IDグループ（Identity Groups）]	√	√	x	√	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [外部IDソース（Ext Id Sources）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）]	√	√	x	x	x	x	x	x	√	x
[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [BYOD ポータル（BYOD Portals）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [ブロックリストのポータル（Blocked List Portal）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [デバイスポータル（My Devices Portals）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [証明書（Certificates）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [証明書テンプレート（Certificate Template）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [証明書（Certificates）] > [内部CAの設定（Internal CA Settings）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [証明書（Certificates）] > [外部CAテンプレート（External CA Templates）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [BYOD] > [許可ポリシー（Admission Policy）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [BYOD] > [カスタムポータルファイル（Custom Portal Files）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）]	√	√	√	√	√	√	√	√	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [認証ポリシー（Authentication Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [レポート（Reports）]	√	√	√	√	√	√	√	√	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [クライアントプロビジョニング（Client Provisioning）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [コレクションフィルタ（Collection Filters）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [プロトコル（Protocols）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP TLS]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [EAP FAST]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [PACの生成（Generate PAC）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [プロトコル（Protocols）] > [PEAP]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [設定（Settings）] > [プロキシ設定（Proxy Settings）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ディクショナリ（Dictionaries）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [概要（Overview）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [概要（Overview）] > [はじめに（Introduction）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [概要（Overview）] > [RADIUS ライブログ（RADIUS Livelog）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [ネットワークアクセスユーザー（Network Access Users）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [ID ソース順序（Identity Source Sequences）]	√	√	x	√	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [IDグループ（Id Groups）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [外部 ID ソース（Ext Id Sources）]	√	√	x	√	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ネットワークリソース（Network Resources）]	√	√	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]	√	√	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ネットワークリソース（Network Resources）] > [デバイスグループ（Device Groups）]	√	√	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ネットワークリソース（Network Resources）] > [デフォルトデバイス（Default Device）]	√	√	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ネットワークリソース（Network Resources）] > [外部 RADIUS サーバー（External RADIUS Servers）]	√	√	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ネットワークリソース（Network Resources）] > [RADIUS サーバーの順序（RADIUS Server Sequences）]	√	√	x	x	√	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ネットワークリソース（Network Resources）] > [外部 MDM サーバー（External MDM Servers）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [認証の単純条件（Authentication Simple Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ライブラリ条件（Library Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [スマート条件（Smart Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可の単純条件（Authorization Simple Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可の複合条件（Authorization Compound Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [時刻と日付の条件（Time and Date Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可されるプロトコル（Allowed Protocols）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Admission Profiles）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ダウンロード可能 ACL（Downloadable ACLs）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [許可ポリシー（Authorization Policy）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [トラブルシューティング（Troubleshoot）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [トラブルシューティング（Troubleshoot）] > [エンドポイントのデバッグ（EndPoint Debug）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [トラブルシューティング（Troubleshoot）] > [TCP ダンプ（TCP Dump）]	√	x	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [トラブルシューティング（Troubleshoot）] > [コレクションフィルタ（Collection Filters）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [トラブルシューティング（Troubleshoot）] > [RADIUS 認証のトラブルシューティング（RADIUS Authentication Troubleshooting）]	√	√	√	√	√	√	√	√	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）]	√	√	√	√	√	√	√	√	√	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [概要（Overview）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [管理（Administration）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [管理（Administration）] > [SMS ゲートウェイプロバイダー（SMS Gateway Providers）]	√	√	x	x	x	√	x	x	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [管理（Administration）] > [証明書（Certificates）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [管理（Administration）] > [証明書（Certificates）] > [システム証明書（System Certificates）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [管理（Administration）] > [証明書（Certificates）] > [証明書の定期的なチェックの設定（Certificate Periodic Check Settings）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [管理（Administration）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]	√	√	x	x	x	√	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [管理（Administration）] > [SMTP サーバー（SMTP Server）]	√	√	x	x	x	√	x	x	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストタイプ（Guest Types）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Center）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーグループ（Sponsor Groups）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [許可ポリシー（Authorization Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [カスタムポータルファイル（Custom Portal Files）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ID（Identities）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ID（Identities）] > [ネットワークアクセスユーザー（Network Access Users）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ID（Identities）] > [ID ソース順序（Identity Source Sequences）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [IDグループ（Identity Groups）]	√	√	x	√	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [外部 ID ソース（Ext Id Sources）]	√	√	x	√	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ネットワークデバイス（Network Devices）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [アカウントの管理（Manage Accounts）]	√	√	x	x	x	x	x	x	√	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可の単純条件（Authorization Simple Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [時刻と日付の一般条件（Common Time and Date Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可の複合条件（Authorization Compound Conditions）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可されるプロトコル（Allowed Protocols）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ダウンロード可能 ACL（Downloadable ACLs）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシーセット（Policy Sets）]	√	√	x	x	x	x	x	x	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [認証ポリシー（Authentication Policy）]	√	√	x	x	x	x	x	x	x	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [レポート（Reports）]	√	√	√	√	√	√	√	√	x	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲストパスワードポリシー（Guest Password Policy）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲストアカウント消去ポリシー（Guest Account Purge Policy）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲスト電子メールの設定（Guest Email Settings）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] < [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲストユーザー名ポリシー（Guest Username Policy）]	√	√	x	x	x	x	x	x	√	x
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ロギング（Logging）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [カスタムフィールド（Custom Fields）]	√	√	x	x	x	x	x	x	√	x

メニューおよびサブメニュー	スーパー管理者のメニューアクセス	ポリシー管理者のメニューアクセス	ヘルプデスク管理者のメニューアクセス	ID 管理者のメニューアクセス	ネットワーク管理者のメニューアクセス	システム管理者のメニューアクセス	RBAC 管理者のメニューアクセス	MnT 管理者のメニューアクセス	カスタマイズ管理者のメニューアクセス	TACACS+ 管理者のメニューアクセス
[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲストロケーションおよび SSID（Guest Locations and SSIDs）]	√	√	x	x	x	x	x	x	√	x
[ワークセンター（Work Centers）] > [GPC]	√	√	√	x	x	x	x	x	x	x
ウィザード（Wizard）	√	x	x	x	x	x	x	x	x	x
設定（Settings）	√	x	x	x	x	x	x	x	x	x

メニュー アクセス権限の設定

Cisco ISE では、RBAC ポリシーにマッピングできるカスタム メニュー アクセス権限を作成することができます。管理者のロールに応じて、管理者の特定のメニュー オプションのみへのアクセスを許可できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[許可（Authorization）]** > **[権限（Permissions）]** > **[メニューアクセス（Menu Access）]**。

ステップ 2 [追加（Add）] をクリックし、[名前（Name）] フィールドおよび [説明（Description）] フィールドに値を入力します。

a) [ISEナビゲーション構造（ISE Navigation Structure）] メニューを必要なレベルまで展開し、権限を作成するオプションをクリックします。

b) [メニューアクセスの権限（Permissions for Menu Access）] ペインで [表示（Show）] をクリックします。

ステップ 3 [送信（Submit）] をクリックします。

データ アクセス権限を付与するための前提条件

RBAC 管理者がオブジェクト（たとえば**「ユーザー アイデンティティ グループ」**データ型の**「従業員」**）へのフルアクセス権限を持っている場合、管理者はそのグループに属するユーザーの表示、追加、更新、削除を行うことができます。管理者に [ユーザー（Users）] ウィンドウのメニューのアクセス権限が付与されていることを確認します（[管理（Administration）] > [IDの管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]）。これは、ネットワークデバイスとエンドポイントオブジェクトに当てはまります（**ネットワーク デバイス グループ**および**エンドポイント アイデンティティ グループ**のデータ型に付与されたアクセス権限に基づく）。

デフォルトのネットワーク デバイス グループ オブジェクト（すべてのデバイス タイプおよびすべてのロケーション）に属するネットワーク デバイスのデータ アクセスを有効にしたり、制限したりすることはできません。これらのデフォルト ネットワーク デバイス グループ オブジェクトの下に作成されたオブジェクトに対するフルアクセスデータ権限が付与される場合、すべてのネットワークデバイスが表示されます。このため、デフォルト ネットワーク デバイス グループ オブジェクトに依存しない、**ネットワーク デバイス グループ**のデータ型の階層を別個に作成することをお勧めします。制限付きアクセスを作成するには、新たに作成されたネットワーク デバイス グループに、ネットワーク デバイス オブジェクトを割り当てる必要があります。

（注） 管理者グループに対してではなく、ユーザー アイデンティティ グループ、ネットワーク デバイス グループ、およびエンドポイント アイデンティティ グループに関してのみ、データアクセス権限を有効にしたり制限したりできます。

デフォルトのデータ アクセス権限

Cisco ISE では、事前定義されたデータ アクセス権限のセットが付属しています。これらの権限により、複数の管理者が、同じユーザー母集団内でデータアクセス権限を持つことができます。データアクセス権限の使用を1つ以上の管理者グループに対して有効化または制限することができます。このプロセスにより、1 つの管理者グループの管理者に対する自律委任制御が可能となり、選択的関連付けを介して選択済みの管理者グループのデータアクセス権限を再利用できます。データアクセス権限の範囲は、フルアクセス権から、選択された管理者グループまたはネットワーク デバイス グループを表示するためのアクセス権なしまでとなります。RBACポリシーは、管理者（RBAC）グループ、メニューアクセス、データアクセス権限に基づいて定義されます。最初に、メニューアクセス権限とデータアクセス権限を作成し、次に、対応するメニューアクセス権限とデータアクセス権限に管理者グループを関連付けるRBACポリシーを作成する必要があります。RBAC ポリシーには、次の形式を使用します。admin_group=Super Admin の場合、スーパー管理者メニューアクセス権限とスーパー管理者データアクセス権限を割り当てます。定義済みのデータ アクセス権限とは別に、Cisco ISE では RBAC ポリシーと関連付けることができるカスタム データ アクセス権限を作成することができます。

管理者グループに付与することができる、フルアクセス、アクセスなし、読み取り専用という名前の 3 つのデータアクセス権限があります。

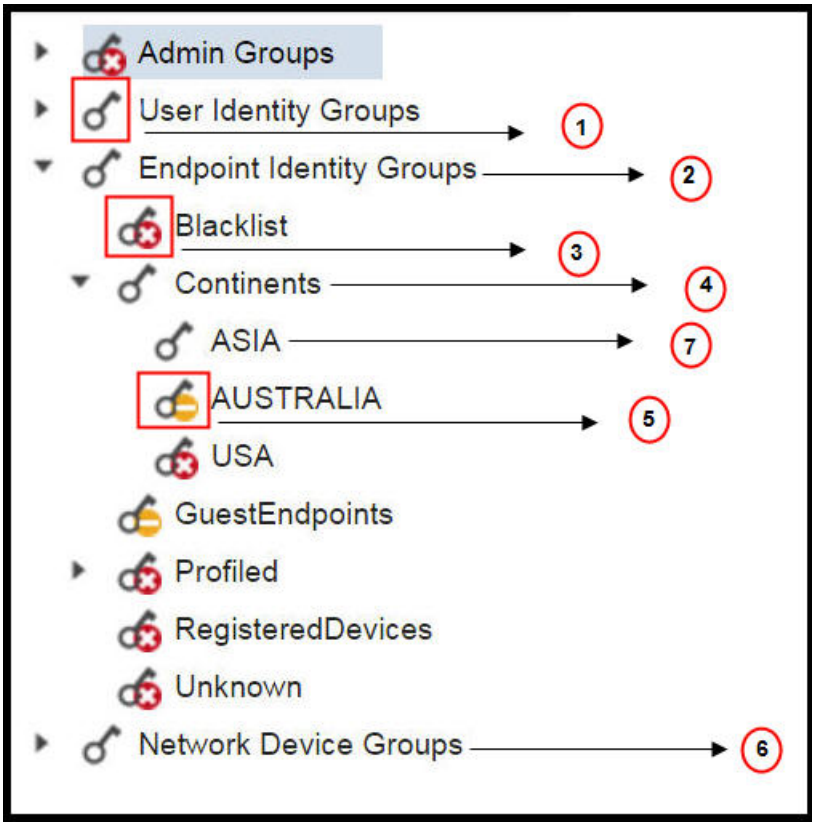
読み取り専用権限は次の管理者グループに付与できます。

- **[管理（Administration）] > [管理アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]**
- **[管理（Administration）] > [グループ（Groups）] > [ユーザーIDグループ（User Identity Group）]**
- **[管理（Administration）] > [グループ（Groups）] > [エンドポイントIDグループ（Endpoint Identity Groups）]**
- **[ネットワーク可視性（Network Visibility）] > [エンドポイント（Endpoints）]**
- **[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスグループ（Network Device Groups）]**
- **[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]**
- **[管理（Administration）] > [ID管理（Identity Management）] > [ID（Identities）]**
- **[管理（Administration）] > [ID管理（Identity Management）] > [グループ（Groups）] > [ユーザーIDグループ（User Identity Groups）]**
- **[管理（Administration）] > [ID管理（Identity Management）] > [グループ（Groups）] > [エンドポイントIDグループ（Endpoint Identity Groups）]**

データタイプ（エンドポイントIDグループなど）に対して読み取り専用の権限を持つ場合は、そのデータタイプに CRUD 操作を実行することはできません。オブジェクト（GuestEndpoints など）に対して読み取り専用権限を持つ場合には、そのオブジェクトに編集または削除操作を実行することはできません。

以下の図に、さまざまなRBACグループのための追加のサブメニューまたはオプションを含む2番目または3番目のレベルのメニューで、データアクセス権限がどのように適用されるかを示します。

図 *1* : データ アクセス権限（*Data Access Privileges*）



ラベル	説明
1	[ユーザーIDグループ（User Identity Groups）] データタイプのフルアクセス権を示しています。
2	[エンドポイントIDグループ（Endpoint Identity Groups）] が、その子（この図で示されている例では [アジア（Asia）]）に付与されている最大の権限（フルアクセス権）を得ていることを示しています。
3	オブジェクト（[ブロックリスト（Blocked List）]）にはアクセス権限がないことを示しています。
4	親（[大陸（Continents）]）が、その子（[アジア（Asia）]）に付与されている最大のアクセス権限を得ていることを示しています。
5	オブジェクト（[オーストラリア（Australia）]）には読み取り専用のアクセス権があることを示しています。

ラベル	説明
6	親（[ネットワークデバイスグループ（Network Device Groups）]）にフルアクセスが付与されている場合は、子が自動的に権限を継承します。
7	親（[アジア（Asia）]）にフルアクセスが付与されている場合は、オブジェクトに権限が明示的に付与されていない限り、オブジェクトがフルアクセス権限を継承することを示しています。

次の表に、さまざまな管理者グループのデフォルトのデータアクセス権限を示します。

√：ユーザーがフルアクセス権を持っていることを示します

x：ユーザーがアクセス権を持っていないことを示します

!：ユーザーが読み取り専用のアクセス権を持っていることを示します

表 *4*: データアクセス権限

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
管理者グループ（Admin Groups）	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [ネットワーク管理者（Super Admin）]	√	x	x	x	√	√	x	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[管理者グループ（Admin Groups）] > [ポリシー管理者（Policy Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [ヘルプデスク管理者（Helpdesk Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [ID管理者（Identity Admin）]	√	x	x	x	√	√	x	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[管理者グループ（Admin Groups）] > [ネットワークデバイス管理者（Network Device Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [システム管理者（System Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [RBAC 管理者（RBAC Admin）]	√	x	x	x	√	√	x	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[管理者グループ（Admin Groups）] > [MnT 管理者（MnT Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [ERS 管理者（ERS Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [ERS オペレータ（ERS Operator）]	√	x	x	x	√	√	x	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[管理者グループ（Admin Groups）] > [カスタマイズ管理者（Customization Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [TACACS+ 管理者（TACACS+ Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [読み取り専用管理者（Read Only Admin）]	√	x	x	x	√	√	x	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[管理者グループ（Admin Groups）] > [昇格されたシステム管理者（Elevated System Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [SPOG 管理者（SPOG Admin）]	√	x	x	x	√	√	x	x	!
[管理者グループ（Admin Groups）] > [ERS Trustsec]	√	x	x	x	√	√	x	x	!
ユーザーIDグループ（User Identity Groups）	√	√	√	x	x	x	√	√	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[ユーザーID グループ（User Identity Groups）] > [GuestType_Weekly]（デフォルト）	√	√	√	x	x	x	√	√	!
[ユーザーID グループ（User Identity Groups）] > [OWN_ACCOUNTS]（デフォルト）	√	√	√	x	x	x	√	√	!
[ユーザーID グループ（User Identity Groups）] > [RBAC_ACCOUNTS]（デフォルト）	√	√	√	x	x	x	√	√	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[ユーザーID グループ（User Identity Groups）] > [redacted]（デフォルト）	√	√	√	x	x	x	√	√	!
[ユーザーID グループ（User Identity Groups）] > [従業員（Employee）]	√	√	√	x	x	x	√	√	!
[ユーザーID グループ（User Identity Groups）] > [redacted]（デフォルト）	√	√	√	x	x	x	√	√	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[ユーザーIDグループ（User Identity Groups）] > [GuestType_Contractor]（デフォルト）	√	√	√	x	x	x	√	√	!
[ユーザーIDグループ（User Identity Groups）] > [ALL_ACCOUNTS]（デフォルト）	√	√	√	x	x	x	√	√	!
エンドポイントIDグループ（Endpoint Identity Groups）	√	√	√	x	x	x	√	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[エンドポイントIDグループ（Endpoint Identity Groups）] > [ブロックリスト（Blocked List）]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [GuestEndpoints]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [RegisteredDevices]	√	√	√	x	x	x	√	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[エンドポイントIDグループ（Endpoint Identity Groups）] > [不明（Unknown）]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [Sony-Device]	√	√	√	x	x	x	√	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [Cisco-Meraki-Device]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [Windows7-Workstation]	√	√	√	x	x	x	√	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [AppleiDevice]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [BlackBerry]	√	√	√	x	x	x	√	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [Android]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [Axis-Device]	√	√	√	x	x	x	√	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [JuniperDevice]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [EpsonDevice]	√	√	√	x	x	x	√	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [Synology-Device]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [Vizio-Device]	√	√	√	x	x	x	√	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [IntelDevice]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [CiscoIPPhone]	√	√	√	x	x	x	√	x	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [Cisco IP-Phone]	√	√	√	x	x	x	√	x	!
[エンドポイントIDグループ（Endpoint Identity Groups）] > [プロファイル済み（Profiled）] > [ワークステーション（Workstation）]	√	√	√	x	x	x	√	x	!
ネットワークデバイス グループ（Network Device Groups）	√	x	x	√	x	x	x	√	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[ネットワークデバイスグループ（Network Device Groups）] > [すべての場所（All Location）]	√	x	x	√	x	x	x	√	!
[ネットワークデバイスグループ（Network Device Groups）] > [すべての場所（All Location）] > [アジア（Asia）]	√	x	x	√	x	x	x	√	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[ネットワークデバイスグループ（Network Device Groups）] > [すべての場所（All Location）] > [アジア（Asia）] > [インド（India）]	√	x	x	√	x	x	x	√	!
[ネットワークデバイスグループ（Network Device Groups）] > [IPSec デバイスである（Is IPsec Device）]	√	x	x	√	x	x	x	√	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[ネットワークデバイスグループ（Network Device Groups）] > [IPSec デバイスである（Is IPsec Device）] > [はい（Yes）]	√	x	x	√	x	x	x	√	!
[ネットワークデバイスグループ（Network Device Groups）] > [IPSEC デバイスである（Is IPsec Device）] > [いいえ（No）]	√	x	x	√	x	x	x	√	!

メニューおよびサブメニュー	スーパー管理者のデータアクセス	ポリシー管理のデータアクセス	ID 管理者のデータアクセス	ネットワーク管理者のデータ アクセス	システム管理者のデータアクセス	RBAC 管理者のデータ アクセス	カスタマイズ管理者のデータアクセス	TACACS+ 管理者のデータアクセス	読み取り専用管理者のデータアクセス
[ネットワークデバイスグループ（Network Device Groups）] > [IPSEC デバイスである（Is IPSEC Device）] > [すべてのデバイスタイプ（All Device Types）]	√	x	x	√	x	x	x	√	!
カスタマイゼーション（Customization）	N/A	N/A	N/A	N/A	N/A	N/A	√	N/A	N/A

データ アクセス権限の設定

Cisco ISE では、RBAC ポリシーにマッピングできるカスタム データ アクセス権限を作成することができます。管理者のロールに基づいて、データを選択するのみのアクセス権の提供を選択できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[許可（Authorization）]** > **[権限（Permissions）]** を選択します。

ステップ 2 **[権限（Permissions）]** > **[データ アクセス（Data Access）]** を選択します。

ステップ 3 [追加（Add）] をクリックし、[名前（Name）] フィールドおよび [説明（Description）] フィールドに値を入力します。

a) 管理者グループをクリックして展開し、対応する管理者グループを選択します。

b) [フル アクセス（Full Access）]、[読み取り専用アクセス（Read Only Access）]、または [アクセスなし（No Access）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

読み取り専用管理ポリシー

デフォルトの読み取り専用管理者ポリシーは、[管理（Administration）]>[システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [**RBAC** ポリシー（RBAC Policy）] ウィンドウで利用できます。このポリシーは、新規インストールとアップグレードされた展開の両方で使用できます。読み取り専用管理ポリシーは、読み取り専用管理者グループに適用されます。デフォルトでは、ネットワーク管理者メニュー アクセス権と読み取り専用データ アクセス権は、読み取り専用管理者に付与されます。このポリシーは複製できず、関連するデータアクセス権限は編集できません。

（注）
- デフォルトの読み取り専用ポリシーは、読み取り専用管理者グループに割り当てられます。読み取り専用管理者グループを使用してカスタムRBACポリシーを作成することはできません。
- Cisco ISEは、読み取り専用管理者グループの静的チェックのみに基づく読み取り専用機能をサポートします。

読み取り専用管理者のメニュー アクセスのカスタマイズ

デフォルトでは、読み取り専用管理者にはネットワーク管理者メニューアクセス権と読み取り専用管理者データ アクセス権が与えられます。ただし、ネットワーク管理者が読み取り専用管理者に [ホーム（Home）] タブと [管理（Administration）] タブのみを表示する必要がある場合、ネットワーク管理者はカスタムメニューアクセス権を作成したり、デフォルトのアクセス許可を MnT 管理者メニュー アクセス権またはポリシー管理者メニューアクセス権にカスタマイズすることができます。ネットワーク管理者は、読み取り専用管理ポリシーにマップされた読み取り専用データ アクセスを変更することはできません。

ステップ 1 管理者用ポータルにネットワーク管理者としてログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[許可（Authorization）]** > **[権限（Permissions）]** > **[メニューアクセス（Menu Access）]**。

ステップ 3 [追加（Add）] をクリックして、[名前（Name）]（MyMenu など）と [説明（Description）] を入力します。

ステップ 4 [メニューアクセス権限（Menu Access Privileges）] セクションでは、[表示（Show）] または [非表示（Hide）] オプションを有効にして、読み取り専用管理者に表示する必要があるオプション（[ホーム（Home）] タブや [管理（Administration）] タブなど）を選択できます。

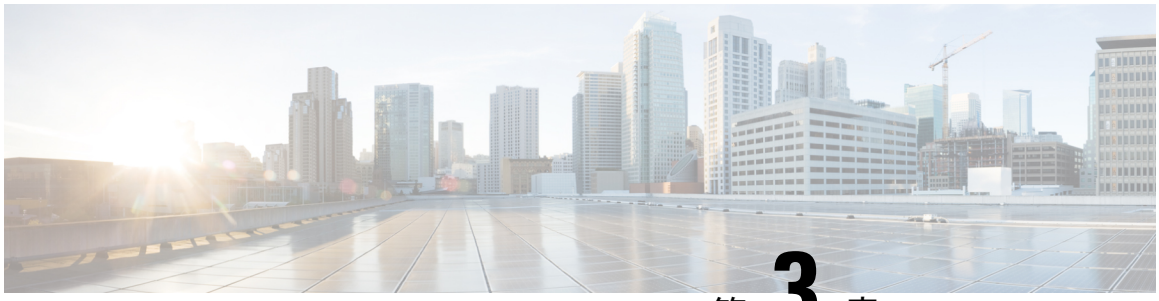
ステップ 5 [送信 (Submit)] をクリックします。
カスタムメニューアクセス権限は、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [ポリシー（Policy）]** ウィンドウに表示される、読み取り専用管理ポリシーに対応する **[権限（Permissions）]** ドロップダウンリストに表示されます。

ステップ 6 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authorization）] > [RBACポリシー（RBAC Policy）] > [ポリシー（Policy）] を選択します。

ステップ 7 [読み取り専用管理者ポリシー（Read-Only Admin Policy）] に対応する [権限（Permissions）] ドロップダウンリストをクリックし、デフォルト（[MnT管理者メニューアクセス（MnT Admin Menu Access）]）か、または**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [権限（Permissions）] > [メニューアクセス（Menu Access）]**ウィンドウで作成したカスタムメニューアクセス権限（MyMenu）を選択します。

ステップ 8 [保存（Save）] をクリックします。

（注）
- 読み取り専用管理者ポリシーに**データアクセス**権限を選択すると、エラーが発生します。
- 読み取り専用管理者用ポータルにログインすると、ウィンドウ上部に読み取り専用のアイコンが表示され、指定したメニューオプションのみを表示できます（データアクセスなし）。



第 3 章

ライセンス

- Cisco ISE ライセンス （393 ページ）
- Cisco ISE スマート ライセンス （398 ページ）
- エアギャップネットワークのスマートライセンス （402 ページ）

Cisco ISE ライセンス

Cisco ISE サービスは、ネットワーク内の増加するエンドポイントに対する可視性と制御を提供します。Cisco ISE 機能は特定のライセンスにマッピングされ、組織のニーズを満たすために必要な Cisco ISE 機能を提供するライセンスを有効にできます。

Cisco ISE は、次の主要な機能を持つライセンスメカニズムにバンドルされています。

- 組み込みライセンス：Cisco ISE には、90 日間有効な組み込みの評価ライセンスが付属しています。Cisco ISE のインストール直後に Cisco ISE ライセンスをインストールする必要はありません。Cisco ISE のすべての機能が提供される評価ライセンスを使用できます。

（注） Cisco AI Analytics は、組み込みの評価ライセンスではサポートされていません。詳細については、「Cisco AI Analytics」セクションを確認してください。

- ライセンスの集中管理：Cisco ISE プライマリ管理ノード（PAN）は、Cisco ISE ライセンスを集中管理します。プライマリ PAN とセカンダリ PAN がある分散展開では、プライマリ PAN は自動的にセカンダリ PAN とライセンス情報を共有します。
- 同時アクティブエンドポイント数：Cisco ISE ライセンスには、各階層ライセンスのカウント値が含まれます。各階層ライセンスでは、いつでも特定の数のアクティブエンドポイントがサポートされます。カウント値は、いつでも特定の Cisco ISE サービスを使用している展開全体のアクティブエンドポイントの数を指します。Cisco ISE ライセンスは RADIUS アカウンティングに依存しているため、ネットワークデバイスで RADIUS サービスを有効にする必要があります。

同時アクティブエンドポイント数は、サポートされるユーザーとデバイスの総数を指します。ここで、エンドポイントとは、ユーザー、PC、ラップトップ、IP電話、スマートフォン、ゲームコンソール、プリンタ、ファクス機、またはその他のネットワークデバイスを意味します。

Cisco ISE リリース 3.0 以降のリリースでは、Cisco ISE リリース 2.x で使用されていたレガシーライセンス（Base、Plus、Apex ライセンスなど）はサポートされていません。Cisco ISE リリース 3.x ライセンスは、Cisco Smart Software Manager（CSSM）と呼ばれる集中型データベースを介して完全に管理されます。単一のトークン登録で、すべてのライセンスを簡単かつ効率的に登録、アクティブ化、および管理できます。

お客様の経済性を最大化するために、Cisco ISE のライセンスは次のパッケージで提供されます。

- **階層ライセンス**

  Cisco ISE リリース 3.0 以降、階層ライセンスと呼ばれる新しいライセンスのセットが、リリース 3.0 以前のリリースで使用されていた Base、Apex、および Plus ライセンスに置き換わります。階層ライセンスには、Essentials、Advantage、Premier の 3 つのライセンスが用意されています。

  現在、Base、Apex、または Plus ライセンスがある場合は、CSSM を使用して新しいライセンスタイプに変換します。

- **デバイス管理ライセンス**

  TACACS+ ペルソナが有効になっているポリシーサービスノード（PSN）では、デバイス管理ライセンスが使用されます。

- **仮想アプライアンスのライセンス**

  Cisco ISE リリース 3.1 およびそれ以降のリリースでは、ISE VM ライセンスがされています。このライセンスは、3.1 より前のリリースでサポートされていた小規模 VM、中規模 VM、および大規模 VM ライセンスに代わるものです。ISE VM ライセンスは、オンプレミス展開とクラウド展開の両方の Cisco ISE VM ノードを対象としています。

  仮想アプライアンスが使用されているものの、Cisco ISE にアクティブな VM ライセンスがない場合、VM ライセンスを入手してインストールするまで、非準拠ライセンスの使用に関する警告と通知が表示されます。ただし、Cisco ISE サービスは中断されません。

- **評価ライセンス**

  評価ライセンスは、Cisco ISE リリース 3.0 以降を初めてインストールしたときにデフォルトで有効になり、100 エンドポイントまでサポートします。評価ライセンスは、すべての Cisco ISE 機能にアクセスできる 90 日間ライセンスです。評価期間中、CSSM にライセンスの使用は報告されません。

Base、Apex および Plus ライセンスのスマートライセンスを使用して Cisco ISE リリース 3.0 以降にアップグレードする場合、スマートライセンスは Cisco ISE の新しいライセンスタイプにアップグレードされます。ただし、アップグレード先の Cisco ISE リリースでライセンスをアクティブ化するには、CSSM で新しいライセンスタイプを登録する必要があります。

従来のCisco ISEライセンスを所有している場合は、それらをスマートライセンスに変換して、Cisco ISE リリース 3.0 以降でのライセンスの使用を有効にする必要があります。Cisco ISE 2.x ライセンスを新しいライセンスタイプに変換するには、http://cs.co/scmswl で Support Case Manager を通じてオンラインでケースを開くか、http://cs.co/TAC-worldwide に記載されている連絡先情報を使用します。

非準拠ライセンスの消費に関する通知も Cisco ISE に表示されます。ライセンスの使用が 60 日の期間のうち 30 日間にわたってコンプライアンスに違反している場合は、必要なライセンスを購入してアクティブ化するまで、Cisco ISE のすべての管理制御が失われます。

あるライセンスパッケージから別のライセンスパッケージにアップグレードする場合、Cisco ISEはアップグレード以前のパッケージで使用できたすべての機能を提供し続けます。ただし、設定済みの設定は再設定する必要があります。たとえば、現在、Essentials ライセンスを使用していて、その後に Advantage ライセンスを追加した場合、Essentials ライセンスを使用してすでに設定されている機能は変更されません。

次の場合は、ライセンス契約を更新する必要があります。

- 評価期間が終了し、まだライセンスを登録していない。
- ライセンスの有効期限が切れている。
- エンドポイントの使用がライセンス契約を超える。

Cisco ISE コミュニティリソース

Cisco Identity Services Engine Ordering Guide

評価版ライセンスを入手する方法については、How to Get ISE Evaluation Licenses を参照してください。

階層ライセンス

次の表に、新しい階層ライセンスで有効になるものを示します。

表 *5 : Cisco ISE* 階層ライセンス

ライセンス名	このライセンスで有効になるもの
Essentials	• RADIUS 認証、許可、およびアカウンティング（802.1X、MAC 認証バイパスと Easy Connect、Web 認証を含む）。 • MACsec。 • シングルサインオン（SSO）、セキュリティアサーションマークアップ言語（SAML）、およびオープン データベース コネクティビティ（ODBC）標準に基づく認証。 • ゲストアクセスとスポンサーサービス。 • モニタリング目的の Representational State Transfer（REST）API、および CRUD 操作用の外部 RESTful サービス API。 • パッシブ ID サービス。 • セキュアな有線およびワイヤレスアクセス。
Advantage	• Cisco ISE Essentials ライセンスで有効になっているすべての機能。 • 組み込みの認証局を使用した Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）デバイス登録とプロビジョニング。デバイスの登録は、設定済みのデバイスポータルを介して行われます。 • セキュリティグループタギング、TrustSec、および Cisco Application Centric Infrastructure（ACI）の統合。 • 基本的なアセットの可視性および適用機能を含むプロファイリングサービス。 • フィードサービス。 • コンテキスト共有（pxGrid など）、およびセキュリティエコシステムの統合。 • Rapid Threat Containment（適応型ネットワーク制御とコンテキスト共有サービスを使用）。 • Cisco AI エンドポイント分析の可視性と適用。

ライセンス名	このライセンスで有効になるもの
Premier	• Cisco ISE Essentials および Advantage ライセンスで有効になっているすべての機能。 • ポスチャの可視性とエンフォースメント。 • 企業モビリティ管理とモバイルデバイス管理によるコンプライアンスの可視性とエンフォースメント。 • 脅威中心型ネットワークアクセスコントロールの可視性とエンフォースメント。

（注） エンドポイントのプライバシー設定で MAC のランダム化または MAC のローテーションと変更が許可されている場合は、Cisco ISE ライセンスの消費数が増加する可能性があります。エンドポイントが新しいランダム MAC アドレスで認証されると、新しい Cisco ISE セッションが作成されます。

デバイス管理ライセンス

デバイス管理ライセンスでは、ポリシーサービスノードでTACACSサービスを使用できます。高可用性スタンドアロン展開では、デバイス管理ライセンスによって、高可用性ペアの1つのポリシーサービスノードで TACACS サービスを使用することが許可されます。

評価ライセンス

評価ライセンスは、Cisco ISE リリース 3.0 以降をインストールまたはアップグレードするとデフォルトでアクティブ化され、100エンドポイントまでサポートします。評価ライセンスは90日間有効で、この期間中は Cisco ISE のすべての機能にアクセスできます。評価ライセンスが使用されている場合、Cisco ISE は評価モードであると見なされます。

Cisco ISE GUI に、評価モードの残り日数を示すメッセージが表示されます。メッセージには次のタイプがあります。

情報：評価モードが終了する 90 ～ 60 日前

警告：評価モードが終了する 60 ～ 30 日前

重要：評価モードの終了まで 30 日

（注） Cisco ISE の必要な機能を引き続き使用するには、評価モードの終了までに Cisco ISE ライセンスを購入し、登録する必要があります。

Cisco ISE スマート ライセンス

Cisco ISE の管理ポータルでスマートライセンストークンがアクティブになっており、登録されている場合は、CSSMが各エンドポイントセッションによってライセンスの消費を製品ライセンスごとにモニターします。スマートライセンスでは、Cisco ISE のシンプルな表レイアウトでエンドポイントセッションによるライセンスの消費が管理者に通知されます。スマートライセンスは、有効な各ライセンスのピーク使用量を集中型データベースに毎日レポートします。ライセンスが使用できる状態で消費されていない場合、使用可能なライセンスについて管理者に通知され、使用量のモニターを継続できます。消費量が使用可能なライセンスの数を超えると、アラームが起動し、アラームと通知によって管理者に通知されます。

スマートライセンスでは、Essentials、Advantage、Premier、または Device Admin などの、シスコのスマートアカウントを介して含まれているさまざまなライセンス権限を管理することもできます。Cisco ISE から、ライセンス権限ごとの基本的な消費統計情報をモニターできます。CSSMアカウントから、追加情報、統計情報、通知を表示したり、アカウントや権限に変更を加えたりできます。

Cisco ISE はライセンス消費の内部サンプルを 30 分ごとに取得します。ライセンスのコンプライアンスと消費がそれに応じて更新されます。Cisco ISE の [ライセンス（Licenses）] テーブルにこの情報を表示するには、メインメニューから **[管理（Administration）] > [システム（System）] > [ライセンス（Licensing）]** を選択し、[更新（Refresh）] をクリックします。

Cisco ISE プライマリ管理ノード（PAN）を CSSM に登録した時点から、Cisco ISE は 6 時間ごとにライセンス消費のピークカウントをCSSMサーバーに報告します。ピークカウントレポートは、Cisco ISE でのライセンス消費が購入および登録されたライセンスに準拠していることを確認するのに役立ちます。Cisco ISE は、CSSM 証明書のローカルコピーを保存することで、CSSM サーバーと通信します。CSSM 証明書は、日常の同期中と [ライセンス（Licenses）] テーブルの更新時に自動的に再認証されます。通常、CSSM 証明書の有効期間は 6 ヵ月です。

Cisco ISE が CSSM サーバーと同期したときにコンプライアンスステータスに変更があった場合、[ライセンス（Licenses）] テーブルの [最後の認証（Last Authorization）] 列がそれに応じて更新されます。また、権限がコンプライアンスを満たさなくなった場合には、コンプライアンス外となっている日数が [コンプライアンス外の日数（Days Out of Compliancy）] 列に表示されます。コンプライアンス違反は、[ライセンス（Licensing）] 領域の上部にある [通知（Notifications）] と、[ライセンス警告（License Warning）] リンクの横にある Cisco ISE ツールバーにも表示されます。通知に加えて、アラームも確認できます。

（注） Device Admin ライセンスは Cisco ISE が CSSM サーバーと通信したときに承認されますが、セッションベースではないため、[ライセンス（Licenses）] テーブルにはライセンスの消費数は関連付けられません。

[ライセンス（Licenses）] テーブルのコンプライアンスの列には、次のいずれかの値が表示されます。

- [コンプライアンス（In Compliance）]：このライセンスの使用はコンプライアンスに準拠しています。
- [リリースされた権限（Release Entitlement）]：ライセンスは、購入され、使用するためにリリースされましたが、この Cisco ISE 展開ではまだ使用されていません。このようなシナリオでは、ライセンスの [消費数（Consumption Count）] は 0 です。
- [評価（Evaluation）]：評価ライセンスを使用できます。

スマートライセンスの登録とアクティブ化

始める前に

- 従来の Cisco ISE ライセンスがある場合は、スマートライセンスに変換する必要があります。
- 既存のスマートライセンスを使用して Cisco ISE リリース 3.0 以降にアップグレードする場合は、CSSM でライセンスを新しいスマートライセンスタイプに変換します。
- 登録トークンを受信するには、新しいスマートライセンスタイプを CSSM に登録します。

既存のスマートライセンスを使用して Cisco ISE リリース 3.4 にアップグレードし、ライセンス接続方法としてトランスポートゲートウェイを使用する場合は、そのリリースにアップグレードする前に設定を編集する必要があります。Cisco ISE リリース 3.4 ではトランスポートゲートウェイがサポートされていないため、別の接続方法を選択する必要があります。接続方法を更新せずに Cisco ISE リリース 3.4 にアップグレードすると、アップグレードプロセス中に HTTPS 直接接続方法を使用するようにスマートライセンス設定が自動的に更新されます。接続方法は、アップグレード後にいつでも変更できます。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [ライセンス（Licensing）]** を選択します。

ステップ 2 表示される [ライセンス（Licensing）] ウィンドウで、[登録の詳細（Registration Details）] をクリックします。

ステップ 3 表示される [登録の詳細（Registration Details）] 領域に、CSSM から [登録トークン（Registration Token）] フィールドで受信した登録トークンを入力します。

ステップ 4 [接続方式（Connection Method）] ドロップダウンリストから接続方式を選択します。

- インターネットへの直接接続を設定している場合には、[直接HTTPS（Direct HTTPS）] を選択します。
- インターネットへの直接接続がなく、プロキシサーバーを使用する必要がある場合には、[HTTPSプロキシ（HTTPS Proxy）] を選択します（Cisco ISE スマートライセンスの登録後にプロキシサーバーの設定を変更した場合は、[ライセンス（Licensing）] ウィンドウでスマートライセンスの設定を更新する必要があります。Cisco ISE は、更新されたプロキシサーバーを使用して CSSM との接続を確立し、Cisco ISE サービスの中断を回避します）。

- 設定済みの SSM オンプレミスサーバーに接続する **SSM オンプレミスサーバー**を選択します。このオプションは、Cisco ISE リリース 3.0 パッチ 2 以降で使用できます。エアギャップネットワークのスマートライセンス （402 ページ）を参照してください。

ステップ 5 [階層（Tier）] 領域と [仮想アプライアンス（Virtual Appliance）] 領域で、有効にする必要があるすべてのライセンスのチェックボックスをオンにします。選択したライセンスがアクティブ化され、その使用量が CSSM によって追跡されます。

ステップ 6 [登録（Register）] をクリックします。

Cisco ISE でのスマートライセンスの管理

スマートライセンストークンをアクティブ化して登録すると、Cisco ISE のライセンス権限を次の方法で管理することができます。

- ライセンス権限資格証明書の有効化、無効化、および更新。
- スマート ライセンスの登録の更新。
- 準拠および非準拠ライセンスの問題の特定。

レガシーの、または新しい Cisco ISE の分割アップグレードプロセスを実行した場合、プロセス中にセカンダリ PAN がプライマリ PAN に昇格されます。Cisco ISE の管理ポータルで、**[管理（Administration）] > [ライセンス（Licensing）]** を選択します。[シスコスマートライセンス（Cisco Smart Licensing）] 領域で、[更新（Update）] をクリックします。

ライセンスを更新するまで、ライセンスアラームが Cisco ISE に表示されます。

始める前に

スマートライセンストークンをアクティブ化して登録していることを確認します。

ステップ 1 （任意）初めて Cisco ISE リリース 3.0 以降をインストールした場合は、すべてのソフトウェア利用資格が評価モードの一部として自動的に有効になります。ライセンストークンを登録すると、CSSM アカウントに特定の権限が含まれず、登録時にそれらを無効にしていなかった場合は、非準拠通知が Cisco ISE に表示されます。それらの権限を CSSM アカウントに追加し（サポートが必要な場合は、CSSM アカウント担当者にお問い合わせください）、[ライセンス（Licenses）] テーブルの [更新（Refresh）] をクリックし、非準拠通知を削除して、関連機能を使い続けます。承認を更新したらログアウトして、関連する非準拠メッセージを削除するために Cisco ISE に再度ログインします。

ステップ 2 （任意）日次の自動承認が何らかの理由で成功しない場合、非準拠メッセージが表示されることがあります。[更新（Refresh）] をクリックして権限を再承認します。承認を更新したら、ログアウトして、関連する削除する非準拠メッセージのために Cisco ISE に再度ログインします。

ステップ 3 （任意）初めて Cisco ISE リリース 3.0 以降をインストールした場合は、すべてのソフトウェア利用資格が評価期間の一部として自動的に有効になります。トークンを登録すると、CSSM アカウントに特定の権限が含まれず、登録時にそれらを無効にしていなかった場合は、不必要な非準拠通知を回避するために、ISE のスマートライセンスからそれらの権限を無効のままにすることができます。[ライセンス（Licenses）]

テーブルから、トークンに含まれていないライセンス権限のチェックボックスをオンにし、ツールバーから [無効化（Disable）] をクリックします。ライセンス権限を無効にした後、ログアウトしてから Cisco ISE にもう一度ログインし、メニューから関連機能を削除したり、非準拠メッセージを削除します。

ステップ 4 （任意）アカウントに権限を追加したら、追加した権限を有効にします。[ライセンス（Licenses）] テーブルから、無効化された必要なライセンスのチェックボックスをオンにし、ツールバーから [有効化（Enable）] をクリックします。

ステップ 5 （任意）登録証明書は 6 ヵ月ごとに自動的に更新されます。手動でスマートライセンス証明書の登録を更新するには、[ライセンス（Licensing）] ウィンドウの上部にある [登録の更新（Renew Registration）] をクリックします。

ステップ 6 （任意）Cisco ISE 登録（UDI により示されます）をスマートアカウントから削除する一方で、評価期間の終了までスマートライセンスを引き続き使用するには、[シスコスマートライセンス（Cisco Smart Licensing）] 領域の上部にある [登録解除（Deregister）] をクリックします。たとえば、登録プロセスの一環として示した UDI を変更する必要がある場合に、これを行うことができます。まだ評価期間に残りがあれば、Cisco ISE はスマートライセンスのままです。評価期間の終了時点である場合は、ブラウザを更新したときに通知が表示されます。スマートライセンスの登録を解除したら、同一または別の UDI で登録するために登録プロセスを再度実行できます。

ステップ 7 （任意）Cisco ISE 登録（UDI により示されます）をスマートアカウントから完全に削除し、従来のライセンスに戻すには、[シスコスマートライセンス（Cisco Smart Licensing）] 領域の上部にある [無効化（Disable）] をクリックします。たとえば、登録プロセスの一環として示した UDI を変更する必要がある場合に、これを行うことができます。スマートライセンスを無効にしたら、同一または別の UDI でアクティブ化および登録するために登録プロセスを再度実行できます。

トラブルシューティング：未登録ライセンスの使用

問題

エンドポイントライセンスの使用は、エンドポイントが一致する認証ポリシー内に使用される属性に依存します。

90 日間の評価ライセンスを削除したため、システムに Cisco ISE の Essentials ライセンスのみが登録されているというシナリオを検討します。対応する Cisco ISE の Essentials メニュー項目と機能を表示および設定できます。

Premier ライセンスを必要とする機能（Session:PostureStatus 属性を使用している場合など）を使用するための認証ポリシーを設定し、エンドポイントがこの認証ポリシーに一致した場合は、次のようになります。

- エンドポイントでは、Cisco Premier ライセンスがシステムに登録されていないにもかかわらず、Cisco ISE Premier ライセンスが使用されます。
- ログインするたびに、非準拠ライセンスの使用の通知が表示されます。
- Cisco ISEに `Exceeded license usage than allowed` という通知とアラームが表示されます。これは、Cisco ISE の CSSM に Cisco ISE Premier ライセンスがないにもかかわらず、エンドポイントがそのライセンスを使用しているためです。

（注） ライセンスアラームは、必要なライセンスを登録してライセンスの問題を修正した場合でも、非準拠ライセンスが最初に使用されてから約 60 日間表示されます。

3 階層のすべてのライセンスが使用され、60 日の期間のうち 30 日間にわたってコンプライアンスに違反する場合は、正しいライセンスを登録するまで、Cisco ISE の管理制御が失われます。正しいライセンスが登録されるまでは、Cisco ISE の管理ポータルの [ライセンス（Licensing）] ウィンドウにのみアクセスできます。ただし、Cisco ISE では引き続き認証が処理されます。

考えられる原因

認証ポリシーの設定が原因で、[ライセンス（Licensing）]テーブルに、購入していないのに登録したライセンスを Cisco ISE が使用したことが報告されます。、Advantage ライセンスまたは Premier ライセンスを購入するまでは Cisco ISE 管理ポータルにはそのライセンスが適用される機能は表示されません。ただし、これらのライセンスを購入すると、ライセンスが期限切れになったり、ライセンスのエンドポイントの消費が設定された制限を超えたりしても、ライセンスによって有効になっている機能が引き続き表示されます。そのため、有効なライセンスがない場合でも、機能を設定できます。

ソリューション

Cisco ISE の管理ポータルで、[メニュー（Menu）] アイコン（☰）をクリックし、**[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** を選択し、登録済みライセンスがない機能を使用している認証ルールを特定してそのルールを再設定します。

エアギャップネットワークのスマートライセンス

エアギャップネットワークでは、セキュリティで保護されたネットワークと外部ネットワーク間の通信は許可されません。Cisco ISE スマートライセンスでは、Cisco ISE を CSSM と通信させる必要があります。ネットワークがエアギャップである場合、Cisco ISE はライセンスの使用状況を CSSM に報告できず、この報告がないと、Cisco ISE への管理アクセスが失われ、Cisco ISE 機能が制限されます。

このライセンス方式は、Cisco ISE リリース 3.0 パッチ 2 以降のリリースで使用できます。

エアギャップネットワークでのライセンスの問題を回避し、Cisco ISE の全機能を有効にするには、次のことを行います。

- Smart Software Manager（SSM）オンプレミスサーバーを設定します。このライセンス方式は、Cisco ISE リリース 3.0 パッチ 2 以降のリリースで使用できます。

  SSM オンプレミスサーバーを設定し、Cisco ISE がこのサーバーに到達できるようにします。このサーバーは、エアギャップされたネットワーク内での CSSM の役割を引き継ぎ、必要に応じてライセンス権限を解放して、使用状況メトリックを追跡します。SSM オンプ

レミスサーバーは、ライセンスの消費と有効性に関連する通知、アラーム、および警告メッセージも送信します。

SSMオンプレミスサーバー接続を設定する方法の詳細については、スマートライセンス用の Smart Software Manager オンプレミスの設定 （403 ページ）を参照してください。

- 特定のライセンス予約を有効にします。これは、組織のセキュリティ要件で Cisco ISE と SSM 間の永続的な接続が許可されていない場合にスマートライセンスを管理するためのスマートライセンス方式です。特定のライセンス予約では、Cisco ISE PAN で特定のソフトウェア利用資格を予約できます。

  詳細については、特定ライセンス予約 （404 ページ） を参照してください。

スマートライセンス用の Smart Software Manager オンプレミスの設定

始める前に

SSM オンプレミスサーバーを設定し、Cisco ISE がこのサーバーに到達できることを確認します。詳細については、「Smart Software Manager On-Prem Resources」を参照してください。

Cisco ISE 3.0 以降でライセンスを正常に登録するには、SSM オンプレミスリリース 8-202108 以降に更新する必要があります。

ライセンスを追加購入するか、購入したライセンスを変更する場合は、SSMオンプレミスサーバーを CSSM に接続し、ローカルサーバーで変更内容を使用できるようにする必要があります。

（注） ISE-PIC 2.7 以前ではスマートライセンスはサポートされていません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [ライセンシング（Licensing）]**

ステップ 2 [登録の詳細（Registration Details）] をクリックします。

ステップ 3 表示される [登録の詳細（Registration Details）] 領域の [登録トークン（Registration Token）] フィールドに、CSSM から受信した登録トークンを入力します。

ステップ 4 [接続方式（Connection Method）] ドロップダウンリストから [SSMオンプレミスサーバー（SSM On-Prem server）] を選択します。

SSM オンプレミスポータルの [証明書（Certificates）] に、接続されている SSM オンプレミスサーバーの IP アドレスまたはホスト名（あるいは FQDN）のいずれかが表示されます。

ステップ 5 [SSMオンプレミスサーバーホスト（SSM On-Prem server Host）] フィールドに、設定した IP アドレスまたはホスト名（あるいは FQDN）を入力します。

ステップ 6 [階層（Tier）] 領域と [仮想アプライアンス（Virtual Appliance）] 領域で、有効にするすべてのライセンスのチェックボックスをオンにします。選択したライセンスがアクティブ化され、その使用量が CSSM によって追跡されます。

ステップ 7 [登録（Register）] をクリックします。

（注） Cisco ISE を SSM オンプレミスサーバーに登録するときに、ポート 443 と ICMP 通信に使用されるポートが開いていることを確認します。Cisco ISE は、MITM（Man In The Middle）デバイスによってインターセプトされずに、ポート 443 を介して SSM オンプレミスサーバーと直接通信できる必要があります。アップグレードとパッチのインストールプロセスを除き、スマートライセンスの信頼ストアへの変更はサポートされていません。

特定ライセンス予約

特定ライセンス予約は、組織のセキュリティ要件で Cisco ISE と Cisco Smart Software Manager（CSSM）間の永続的な接続が許可されていない場合にスマートライセンスを管理するためのスマートライセンス方式です。特定ライセンス予約では、Cisco ISE PAN で特定のソフトウェア利用資格を予約できます。

Cisco ISE スマートライセンスは、上位階層のライセンスに下位階層のすべての機能が含まれるネストモデルとして機能しますが、特定ライセンス予約はそのようなモデルをサポートしていません。特定ライセンス予約では、Cisco ISE ライセンスタイプごとに必要なライセンス数を予約してアクティブ化する必要があります。たとえば、Advantage ライセンスと Premier ライセンスで有効になっている Cisco ISE 機能を使用したい場合は、Advantage ライセンスと Premier ライセンスの両方を予約する必要があります。Cisco ISE に Premier ライセンスしか含まれていない場合は、エラーまたは不正な動作が通知されます。

予約する必要があるライセンスのタイプと数を定義して特定ライセンス予約を作成し、Cisco ISE ノードで予約をアクティブ化できます。登録して予約を有効にした Cisco ISE ノードは、ライセンスの使用を追跡し、ライセンス消費のコンプライアンスを適用します。

特定のライセンス予約は、それが生成された Cisco ISE ノードでのみ有効にできます。分散展開では、プライマリおよびセカンダリ PAN で特定ライセンス予約を有効にすることをお勧めします。

セカンダリ PAN に Cisco ISE ライセンスが登録されていない場合、プライマリ PAN に障害が発生すると、Cisco ISE のアクセスとサービスが影響を受けます。Cisco ISE のポリシーまたは要素を表示または変更することができなくなります。Cisco ISE に中断なくアクセスするため、プライマリ PAN とセカンダリ PAN の両方で Cisco ISE ライセンスを登録することを強く推奨します。

Cisco ISE ライセンスがセカンダリ PAN にも登録されている場合、プライマリ PAN のフェールオーバーが発生しても、Cisco ISE には新しく昇格したセカンダリ PAN を介して引き続きアクセスできます。その後、プライマリ PAN を元の状態に戻す作業を行うことができます。

階層ライセンス（Essentials、Advantage、Premier）の場合は、必要なライセンスの 100% をプライマリ PAN に登録し、追加のライセンス数をセカンダリ PAN に登録することをお勧めします。次の表では、100 階層ライセンスが必要な場合に、Cisco ISE へのアクセスが中断されないようにするための 2 つのアプローチについて説明します。

表 *6*：階層ライセンスの推奨ライセンス配布

Cisco ISE を中断なく実行するために必要な最小ライセンス配布。		プライマリ PAN のフェールオーバーが発生した場合の想定事項	Cisco ISE を非準拠アラームなしで中断なく実行するための最大ライセンス配布。		プライマリ PAN のフェールオーバーが発生した場合の想定事項
プライマリ PAN	セカンダリ PAN		プライマリ PAN	セカンダリ PAN	
100	1	新しく昇格したプライマリ PAN に十分なライセンスがないため、Cisco ISE は非準拠になります。Cisco ISE は 30 日間の猶予期間に入ります。 猶予期間が終了する前に、ライセンス数の多い元のプライマリ PAN に再参加します。 または、新しく昇格したプライマリ PAN で作業を続行するために、元の PAN で予約されているライセンスを解放し、新しく昇格した PAN で必要なライセンスを予約します。	100	100	Cisco ISE のサービスや操作には影響しません。 修復アクションは必要ありません。元の PAN を Cisco ISE に再参加させるだけです。

デバイス管理ライセンスと仮想アプライアンスライセンスの場合、Cisco ISE でいずれかのタイプのライセンスが 10 個必要な場合は、プライマリ PAN に 10 個、セカンダリ PAN に少なく

とも 1 個を登録します。次の表では、10 個の仮想ライセンスまたは 10 個のデバイス管理ライセンスが必要な場合に、Cisco ISE への中断のないアクセスを確保するための 2 つのアプローチについて説明します。

表 7: 仮想ライセンスとデバイス管理ライセンスの推奨ライセンス配布

Cisco ISE を中断なく実行するために必要な最小ライセンス配布。		プライマリ PAN のフェールオーバーが発生した場合の想定事項	Cisco ISE を非準拠アラームなしで中断なく実行するための最大ライセンス配布。		プライマリ PAN のフェールオーバーが発生した場合の想定事項
プライマリ PAN	セカンダリ PAN		プライマリ PAN	セカンダリ PAN	

10	1	新しく昇格したプライマリ PAN に十分なライセンスがないため、Cisco ISE は非準拠になります。Cisco ISE は 30 日間の猶予期間に入ります。 猶予期間が終了する前に、ライセンス数の多い元のプライマリ PAN に再参加します。 または、新しく昇格したプライマリ PAN で作業を続行するために、元の PAN で予約されているライセンスを解放し、新しく昇格した PAN で必要なライセンスを予約します。	10	10	Cisco ISE のサービスや操作には影響しません。 修復アクションは必要ありません。元の PAN を Cisco ISE に再参加させるだけです。

特定のライセンス予約に含まれていないライセンス権限を使用することはできません。ライセンス使用状況がライセンス予約に準拠していない場合、Cisco ISE 管理ポータルにコンプライアンス違反アラートが表示されます。

特定ライセンス予約の有効化

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [ライセンシング（Licensing）]** を選択します。

ステップ 2 [ライセンスタイプ（License Type）] 領域で、[特定のライセンス予約（Specific License Reservation）] オプションボタンをクリックします。

ステップ 3 [SLR構成（SLR Configuration）] 領域で、[スタンドアロン/プライマリPAN（Standalone/Primary PAN）] の [コードの生成（Generate Code）] をクリックします。

コードが横にある [予約コード（Reservation Code）] フィールドに表示されます。

（注） 予約コードを生成した後で、[リクエストのキャンセル（Cancel Request）] をクリックして予約コードを CSSM サーバーに返却します。その後、このコードは無効になります。次回、プライマリ PAN で特定のライセンス予約をインストールして有効にする場合は、新しい予約コードを生成する必要があります。

ステップ 4 CSSM ポータルで送信するために、予約コードをコピーします（ステップ 8）。

ステップ 5 software.cisco.com ポータルにログインし、メインメニューから**[ライセンス（License）]** > **[スマートソフトウェアライセンシング（Smart Software Licensing）]**を選択します。

ステップ 6 購入したスマートライセンス、使用中のライセンス権限、および使用可能な権限を表示するには、**[インベントリ（Inventory）]** > **[ライセンス（Licenses）]**を選択します。

ステップ 7 [ライセンスの予約（License Reservation）] をクリックします。

[スマートライセンス予約ワークフロー（Smart License Reservation workflow）] ダイアログボックスが表示されます。

ステップ 8 [ステップ1：要求コードの入力（Step 1: Enter Request Code）] タブで、表示されるフィールドに、Cisco ISE から受信した予約コードを入力します（ステップ 3）。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [ステップ2：ライセンスを選択する（Step 2: Select Licenses）] タブで、[特定のライセンスを予約する（Reserve a specific license）] ラジオボックスをクリックします。次に、表示されるテーブルの [予約（Reserve）] 列に、各ライセンスタイプについて、プライマリ PAN で予約するライセンス権限の数を入力します。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [ステップ3：レビューと確認（Step 3: Review and Confirm）] タブで、特定ライセンス予約の詳細を確認し、[承認コードの生成（Generate Authorization Code）] をクリックします。

ステップ 13 [ステップ 4：承認コード（Step 4: Authorization Code）] タブには、承認コードを XML 形式で表示するフィールドがあります。この XML コンテンツには、SLR が生成されるライセンス予約と Cisco ISE ノードに関する情報が含まれます。改ざんされたコードは Cisco ISE によって拒否されるため、このコンテンツは変更しないでください。[ファイルとしてダウンロード（Download As File）] をクリックし、XML コンテンツを含む .txt ファイルをローカルシステムにダウンロードします。

ステップ 14 Cisco ISE 管理ポータルの [ライセンシング（Licensing）] ウィンドウの [プライマリPAN（Primary PAN）] 領域で、[SLRライセンスキーのアップロード（Upload SLR License Key）] をクリックし、CSSM ポータルからダウンロードした XML ファイルを選択します。

キーがノードにアップロードされ、特定のライセンス予約がアクティブ化されるまでに数分かかります。

ステップ 15 セカンダリ PAN で特定のライセンス予約を設定するには、[セカンダリPAN（オプション）（Secondary PAN (optional)）] 領域で次の手順を実行します。

1. [コードの生成（Generate Code）] をクリックします。

   コードが横にある [予約コード（Reservation Code）] フィールドに表示されます。

（注） 予約コードを生成した後で、[リクエストのキャンセル（Cancel Request）] をクリックして予約コードを CSSM サーバーに返却します。その後、このコードは無効になります。次回、セカンダリ PAN で特定のライセンス予約をインストールして有効にする場合は、新しい予約コードを生成する必要があります。

2. ステップ 5 ー 13 を繰り返して、セカンダリ PAN の特定ライセンス予約を設定します。
3. [セカンダリPAN（Secondary PAN）] 領域で、[SLRライセンスキーのアップロード（Upload SLR License Key）] をクリックし、CSSM ポータルからダウンロードした XML ファイルを選択します。

   キーがノードにアップロードされ、特定ライセンス予約がアクティブ化されるまでに数分かかります。

特定ライセンス予約の更新

必要に応じて、ノードの特定ライセンス予約を変更できます。次のシナリオでは、特定ライセンス予約を更新する必要がある場合があります。

- ライセンスの予約を変更する必要がある進化するビジネスニーズ。
- プライマリ PAN を回復できないプライマリ PAN フェールオーバー。プライマリ PAN で障害が発生すると、その PAN で予約されているライセンス権限は Cisco ISE で使用できなくなります。非準拠ライセンスの使用による Cisco ISE への管理アクセス権の喪失を回避するには、ノードで有効にした特定ライセンス予約を返却し、新しいプライマリ PAN（昇格したセカンダリ PAN）の特定ライセンス予約を適切に更新する必要があります。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [ライセンシング（Licensing）]** を選択します。

ステップ 2 [UDIの詳細（UDI Details）] 領域から、特定のライセンス予約を更新するノードのシリアル番号をコピーします。

ステップ 3 software.cisco.com ポータルにログインし、メインメニューから**[ライセンス（License）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]**を選択します。

ステップ 4 [製品インベントリ（Product Inventory）] を選択します。

ステップ 5 インベントリリストの上に表示される検索バーに Cisco ISE からコピーしたシリアル番号を入力して、対応するエントリを表示します。

ステップ 6 [アクション（Actions）] ドロップダウンリストから、[予約済みライセンスの更新（Update Reserved Licenses）] を選択します。

ステップ 7 [特定ライセンスの予約（Reserve a Specific License）] オプションボタンをクリックして、ライセンスのリストを表示します。[予約（Reserve）] 列の対応するフィールドで、ライセンスの予約数を編集します。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [ステップ3：レビューと確認（Step 3: Review and Confirm）] タブで、特定ライセンス予約の詳細を確認し、[承認コードの生成（Generate Authorization Code）] をクリックします。

ステップ 10 [ステップ 4：承認コード（Step 4: Authorization Code）] タブには、承認コードを XML 形式で表示するフィールドがあります。Cisco ISE は改ざんされたコードを拒否するため、この内容を変更しないでください。

ステップ 11 [ファイルとしてダウンロード（Download As File）] をクリックします。XML コンテンツを含む .txt ファイルをローカルシステムにダウンロードします。

ステップ 12 Cisco ISE 管理ポータルの [ライセンシング（Licensing）] ウィンドウの必要な [PAN] 領域で、[SLRコードの更新（Update SLR Code）] をクリックし、CSSM ポータルからダウンロードした XML ファイルを選択します。

キーがノードにアップロードされ、特定ライセンス予約がアクティブ化されるまでに数分かかります。

ステップ 13 更新された特定のライセンス予約コードを送信すると、[予約の更新（Update Reservation）] ダイアログボックスに確認コードが表示されます。CSSM ポータルで送信するには、この確認コードをコピーします。

ステップ 14 ステップ 3 と 4 を繰り返し、表示されるダイアログボックスで [確認コードの入力（Enter Confirmation Code）] をクリックし、Cisco ISE によって生成された確認コードを入力します。

特定ライセンス予約の返却

特定のライセンス予約が複数のノードで有効になっている場合は、ノードごとに返却予約プロセスを実行して、特定のライセンスの予約を完全に削除する必要があります。

セカンダリ PAN で特定のライセンス予約がアクティブで、プライマリ PAN でアクティブな特定のライセンス予約を返却すると、セカンダリ PAN の予約も自動的に返却されます。

高可用性 PAN 構成では、プライマリ PAN で特定ライセンス予約を返却すると、セカンダリ PAN の特定ライセンス予約も返却されます。

各ノードには固有のリターンコードが生成されます。ノードから特定ライセンス予約を削除するには、CSSM で各リターンコードを送信する必要があります。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[ライセンス（Licensing）]** を選択します。

ステップ 2 特定のライセンス予約を返却するノードの [予約の返却（Return Reservation）] をクリックします。

[予約の返却（Return Reservation）] ダイアログボックスにリターンコードが表示されます。

ステップ 3 予約返却プロセスを完了するには、このコードをコピーして CSSM で送信します。

ステップ 4 software.cisco.com ポータルにログインし、メインメニューから **[ライセンス（License）]** > **[スマートソフトウェアライセンス（Smart Software Licensing）]** を選択します。

ステップ 5 [スマートソフトウェアライセンス（Smart Software Licensing）] ウィンドウで、[製品インベントリ（Product Inventory）] をクリックします。

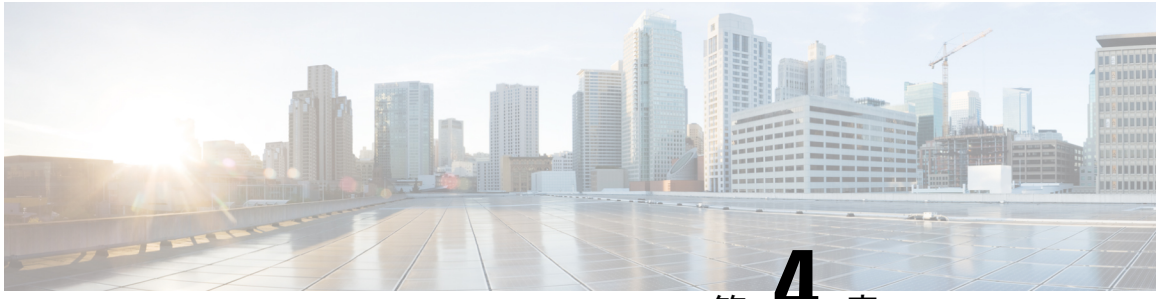
ステップ 6 インベントリリストの上に表示される検索バーに Cisco ISE からコピーしたシリアル番号を入力して、対応するエントリを表示します。

ステップ 7 [アクション（Actions）] ドロップダウンリストから、[削除（Remove）] を選択します。

ステップ 8 表示される [製品インスタンスの削除（Remove Product Instance）] ダイアログボックスで、Cisco ISE から受信した予約返却コードを入力します。

ステップ 9 [製品インスタンスの削除（Remove Product Instance）] をクリックします。

ライセンス予約のライセンス権限がリリースされ、CSSM で使用できるようになりました。



第 4 章

Cisco ISE の展開

- Cisco ISE デプロイメントの用語 （414 ページ）
- 分散 Cisco ISE 展開のペルソナ （414 ページ）
- Cisco ISE ノードの設定 （414 ページ）
- 複数の展開シナリオのサポート （417 ページ）
- Cisco ISE 分散展開 （418 ページ）
- 展開とノードの設定 （424 ページ）
- ロギングの設定 （434 ページ）
- 管理者アクセスの設定 （438 ページ）
- 管理ノード （441 ページ）
- 管理ノードの自動フェールオーバーのサポート （450 ページ）
- ポリシー サービス ノード （451 ページ）
- モニタリング ノード （455 ページ）
- モニタリング データベース （460 ページ）
- 自動フェールオーバー用の MnT ノードの設定 （463 ページ）
- Cisco pxGridノード （464 ページ）
- 展開内のノードの表示 （472 ページ）
- MnT ノードからのエンドポイント統計データのダウンロード （472 ページ）
- データベースのクラッシュまたはファイルの破損の問題 （473 ページ）
- モニタリングのためのデバイス設定 （473 ページ）
- プライマリおよびセカンダリの Cisco ISE ノードの同期 （473 ページ）
- ノード ペルソナとサービスの変更 （474 ページ）
- Cisco ISE でのノードの変更による影響 （474 ページ）
- ポリシー サービス ノード グループの作成 （475 ページ）
- 展開からのノードの削除 （476 ページ）
- Cisco ISE ノードのシャットダウン （477 ページ）
- ノードを再登録する必要があるシナリオ （478 ページ）
- スタンドアロン Cisco ISE ノードのホスト名または IP アドレスの変更 （479 ページ）

Cisco ISE デプロイメントの用語

次の用語は Cisco ISE 展開シナリオの説明に一般に使用されるものです。

- サービス：サービスは、ネットワークアクセス、プロファイラ、ポスチャ、セキュリティグループアクセス、モニタリング、トラブルシューティングなど、ペルソナが提供する固有の機能です。
- ノード：Cisco ISE ソフトウェアを実行する個別インスタンスです。Cisco ISE はアプライアンスとして使用でき、VMware で実行できるソフトウェアとしても使用できます。Cisco ISE ソフトウェアを実行する各インスタンス、アプライアンス、または VMware はノードと呼ばれます。
- ペルソナ：ノードのペルソナによって、そのノードが提供するサービスが決まります。Cisco ISE ノードは、管理、ポリシー サービス、モニタリング、および pxGrid のペルソナのいずれかを担うことができます。管理者ポータルで使用できるメニューオプションは、Cisco ISE ノードが担当するロールおよびペルソナによって異なります。
- 展開モデル：展開が分散か、スタンドアロンか、スタンドアロンのハイアベイラビリティ（基本的な 2 ノード構成）かを決定します。

分散 Cisco ISE 展開のペルソナ

Cisco ISE ノードは、管理、ポリシー サービス、またはモニタリングのペルソナを担当できます。

Cisco ISE ノードは担当するペルソナに基づき、各種のサービスを提供できます。展開の各ノードは、管理、ポリシーサービス、およびモニタリングのペルソナのいずれかを担当することができます。分散展開では、ネットワークで次の組み合わせのノードを使用できます。

- 高可用性を実現するプライマリポリシー管理ノード（プライマリ PAN）およびセカンダリポリシー管理ノード（セカンダリ PAN）
- 高可用性を実現するプライマリモニタリングノード（プライマリ MnT ノード）およびセカンダリモニタリングノード（セカンダリ MnT ノード）
- プライマリ PAN 自動フェールオーバー用のヘルス チェックノードのペアまたは単一のヘルス チェックノード
- セッションフェールオーバー用の 1 つ以上のポリシーサービスノード（PSN）

Cisco ISE ノードの設定

Cisco ISE ノードをインストールすると、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナによって提供されるすべてのデフォルト サービスがそのノードで実行

されます。このノードはスタンドアロン状態となります。Cisco ISE ノードの管理者ポータルにログインして設定する必要があります。スタンドアロン Cisco ISE ノードのペルソナまたはサービスは編集できません。ただし、プライマリおよびセカンダリ Cisco ISE ノードのペルソナおよびサービスは編集できます。最初にプライマリ ISE ノードを設定し、その後、セカンダリ ISE ノードをプライマリ ISE ノードに登録する必要があります。

ノードに初めてログインする場合は、デフォルトの管理パスワードを変更し、有効なライセンスをインストールする必要があります。

実稼働環境の Cisco ISE で設定済みのホスト名とドメイン名は、変更しないことを推奨します。変更が必要な場合は、初期展開時にアプライアンスのイメージを再作成し、変更を加え、詳細を設定します。

始める前に

Cisco ISE での分散展開の設定方法に関する基礎を理解しておく必要があります。「分散展開を設定する場合のガイドライン」を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。

ステップ 2 設定する Cisco ISE ノードの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 必要に応じて値を入力し、[保存（Save）] をクリックします。

プライマリポリシー管理ノード（PAN）の設定

分散展開を設定するには、最初に Cisco ISE ノードをプライマリ PAN として設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。

最初は [登録（Register）] ボタンが無効になっています。このボタンを有効にするには、プライマリ PAN を設定します。

ステップ 2 現在のノードの隣にあるチェックボックスをオンにして [編集（Edit）] をクリックします。

ステップ 3 [プライマリにする（Make Primary）] をクリックして、プライマリ PAN を設定します。

ステップ 4 [保存（Save）] をクリックしてノード設定を保存します。

次のタスク

1. 展開にセカンダリ ノードを追加します。
2. 必要に応じて、プロファイラ サービスを有効にし、プローブを設定します。

セカンダリ Cisco ISE ノードの登録

Cisco ISE ノードを複数ノード展開形式でプライマリ PANに登録できます。展開内のプライマリ PAN 以外のノードはセカンダリノードと呼ばれます。ノードを登録する際に、ノード上で有効にする必要があるペルソナとサービスを選択できます。登録されたノードは、プライマリ PANから管理することができます（たとえば、ノードのペルソナ、サービス、証明書、ライセンス、パッチの適用などの管理）。

ノードが登録されると、プライマリ PAN は設定データをセカンダリノードにプッシュし、セカンダリノード上のアプリケーションサーバーが再起動します。データの複製の完了後、プライマリ PAN で行われた追加の設定変更がセカンダリノードに複製されます。セカンダリノードで変更が複製されるのにかかる時間は、ネットワーク遅延、システムへの負荷などのさまざまな要因によって決まります。

始める前に

プライマリ PAN と登録されているノードが相互に DNS 解決可能であることを確認します。登録されているノードが信頼できない自己署名証明書を使用している場合は、証明書の詳細が記載された証明書の警告がプロンプト表示されます。証明書を受け入れると、プライマリ PAN の信頼できる証明書ストアに追加され、ノードとの TLS 通信が可能になります。

ノードが自己署名されていない証明書（たとえば外部 CA によって署名された証明書）を使用している場合、そのノードの関連する証明書チェーンをプライマリ PAN の信頼できる証明書ストアに手動でインポートする必要があります。信頼できる証明書ストアにセカンダリノードの証明書をインポートする場合は、セカンダリノードの証明書を検証するように、[信頼できる証明書（Trusted Certificates）] ウィンドウで PAN の [ISE 内の認証用に信頼する（Trust for Authentication within ISE）] チェックボックスをオンにします。

セッション サービスが有効になっているノード（ネットワーク アクセス、ゲスト、ポスチャなど）を登録する場合は、それをノードグループに追加できます。詳細については、ポリシー サービス ノード グループの作成 （475 ページ）を参照してください。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。

ステップ 3 [登録（Register）] をクリックして、セカンダリ ノードの登録を開始します。

ステップ 4 登録するスタンドアロン ノードの DNS 解決可能な完全修飾ドメイン名（FQDN）を入力します（hostname.domain-name の形式（たとえば、abc.xyz.com））。プライマリ PAN の FQDN と登録されているノードは、互いに解決可能でなければなりません。

ステップ 5 [ユーザー名（Username）] フィールドと [パスワード（Password）] フィールドに、セカンダリノードの GUI ベースの管理者ログイン情報を入力します。

ステップ 6 [次へ（Next）] をクリックします。

プライマリ PAN はノードの登録後、（最初の）TLS 通信の確立を試みます。

- ノードが信頼できる証明書を使用している場合は、手順 7 に進むことができます。

- ノードが信頼されていない自己署名証明書を使用している場合は、証明書の警告メッセージには、ノード上の実際の証明書と照合できる証明書に関する詳細（発行先、発行元、シリアル番号など）が表示されます。[証明書のインポートと続行（Import Certificate and Proceed）] オプションをクリックして、この証明書を信頼し、登録を続行します。Cisco ISE は、そのノードのデフォルトの自己署名証明書をプライマリ PAN の信頼できる証明書ストアにインポートします。デフォルトの自己署名証明書を使用しない場合は、[登録のキャンセル（Cancel Registration）] をクリックし、そのノードの関連する証明書チェーンをプライマリ PAN の信頼できる証明書ストアに手動でインポートします。信頼できる証明書ストアにセカンダリノードの証明書をインポートする場合は、セカンダリノードの証明書を検証するように、対応するPAN の横にある [ISE 内の認証用に信頼する（Trust for Authentication within ISE）] チェックボックスをオンにします。
- ノードが CA 署名付き証明書を使用する場合は、証明書の信頼が設定されるまで登録を続行できないというエラーメッセージが表示されます。

ステップ 7 チェックボックスをオンにして、ノード上で有効にするペルソナとサービスを選択し、[保存（Save）] をクリックします。

ノードが登録されると、プライマリ PAN でアラーム（ノードが展開に追加されたことを確認するアラーム）が生成されます。このアラームは、Cisco ISE の GUI ダッシュボードの [アラーム（Alarms）] ダッシュレットで確認できます。登録済みノードを同期して再起動したら、プライマリ PAN で使用されているのと同じクレデンシャルを使用してセカンダリノードの GUI にログインできます。

次のタスク

- ゲストユーザーのアクセスと許可、ロギングなどの時間依存タスクの場合は、ノード間のシステム時刻が同期されていることを確認します。
- セカンダリ PAN を登録し、内部 Cisco ISE CA サービスを使用している場合は、プライマリ PAN から Cisco ISE CA 証明書とキーをバックアップし、セカンダリ PAN に復元する必要があります。

複数の展開シナリオのサポート

Cisco ISE は企業インフラストラクチャ全体に展開することが可能で、802.1X 有線、無線、およびバーチャル プライベート ネットワーク（VPN）がサポートされます。

Cisco ISE アーキテクチャでは、1 台のマシンがプライマリロール、もう 1 台のバックアップマシンがセカンダリロールとなる環境において、スタンドアロン展開と分散（別名高可用性または冗長）展開の両方がサポートされます。Cisco ISE は、個別の設定可能なペルソナ、サービス、およびロールを特徴としており、これらを使用して、Cisco ISE サービスを作成し、ネットワーク内の必要な箇所に適用できます。これにより、フル機能を備え統合されたシステムとして動作する包括的な Cisco ISE 展開が実現します。

Cisco ISE ノードは、1 つ以上の管理、モニタリング、ポリシーサービスペルソナで展開できます。各ペルソナは、ネットワークポリシー管理トポロジ全体で異なる、しかし重要な部分を実

行します。Cisco ISE を管理ペルソナとしてインストールすると、集中型ポータルからネットワークを設定および管理することによって、効率と使いやすさを向上させることができます。

Cisco ISE 分散展開

複数の Cisco ISE ノードがある展開は、分散展開と呼ばれます。フェールオーバーをサポートし、パフォーマンスを改善するために、展開に複数の Cisco ISE ノードを分散方式でセットアップできます。Cisco ISE の分散型展開では、管理とモニタリングのアクティビティは一元化されており、処理は PSN 間で分配されます。パフォーマンスのニーズに応じて、導入環境の規模を変更できます。展開の各 Cisco ISE ノードは、管理、ポリシー サービス、およびモニタリングのペルソナのいずれかを担当することができます。

Cisco ISE 展開の設定

『Cisco Identity Services Engine Hardware Installation Guide』で説明されているように Cisco ISE をすべてのノードにインストールした後、ノードはスタンドアロン状態で稼働します。次に、1 つのノードをプライマリ PAN として定義する必要があります。プライマリ PAN の定義時に、そのノードで管理ペルソナおよびモニタリング ペルソナを有効にする必要があります。必要に応じて、プライマリ PAN でポリシーサービスペルソナを有効にできます。プライマリ PAN のペルソナ定義のタスクの完了後に、他のセカンダリ ノードをプライマリ PAN に登録し、セカンダリ ノードのペルソナを定義できます。

すべての Cisco ISE システムと機能に関連する設定は、プライマリ PAN でのみ実行する必要があります。プライマリ PAN で行った設定の変更は、展開内のすべてのセカンダリ ノードに複製されます。

分散展開には 1 つ以上の MnT が必要です。プライマリ PAN の設定時に、モニタリングペルソナを有効にする必要があります。展開内の MnT ノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリングペルソナを無効にしたりできます。

プライマリ Cisco ISE ノードからセカンダリ Cisco ISE ノードへのデータ レプリケーション

1 つの Cisco ISE ノードをセカンダリ ノードとして登録すると、Cisco ISE はプライマリ ノードからセカンダリ ノードへのデータ レプリケーション チャネルをすぐに作成し、複製のプロセスを開始します。複製は、プライマリ ノードからセカンダリ ノードに Cisco ISE 設定データを共有するプロセスです。複製によって、展開を構成するすべての Cisco ISE ノードで使用可能な設定データの整合性を確保できます。Cisco ISE リリース 3.3 から、動的に検出されたエンドポイントは、Cisco ISE 展開内のすべてのノードに自動的に複製されません。[エンドポイント複製（Endpoint Replication）] ウィンドウ（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[エンドポイント複製（Endpoint Replication）]**）で、対応するオプションボタンをクリックして、Cisco ISE 展開内のすべてのノードで動的に検出されたエンドポイントの複製を有効または無効にします。

- Cisco ISE 展開内のすべてのノードへのエンドポイント情報の複製を有効にするには、[エンドポイントをすべてのノードに複製（Replicate endpoints to all nodes）] をクリックします。
- Cisco ISE 展開内のすべてのノードへのエンドポイント情報の複製を無効にするには、[すべてのノードへのエンドポイント複製を無効にする（Disable endpoint replication to all nodes）] をクリックします。この設定は、デフォルトでオンになっています。

静的に設定されたエンドポイント、CSV ファイルからインポートされたエンドポイント、OpenAPI を使用して作成されたエンドポイント、およびゲストおよびポスチャ対応エンドポイントは、すべての Cisco ISE ノード間で自動的に複製されます。

OpenAPI を使用してエンドポイント複製を有効または無効にするには、『Cisco ISE API Reference Guide』を参照してください。

通常、最初に Cisco ISE ノードをセカンダリノードとして登録したときに、完全な複製が実行されます。完全な複製の実行後は差分複製が実行され、PAN での設定データに対する新しい変更（追加、変更、削除など）がセカンダリノードに反映されます。複製のプロセスでは、展開内のすべての Cisco ISE ノードが同期されます。Cisco ISE 管理者ポータルの [展開（Deployment）] ウィンドウの [ノード ステータス（Node Status）] 列で複製のステータスを表示できます。セカンダリノードとして Cisco ISE ノードを登録するか、または PAN との手動同期を実行すると、要求されたアクションが進行中であることを示すオレンジのアイコンがノードステータスに表示されます。同期が完了すると、ノードステータスは、セカンダリノードが PAN と同期されたことを示す緑に変わります。

（注）

- [すべてのノードへのエンドポイント複製を無効にする（Disable endpoint replication to all nodes）] では動的エンドポイントの複製のみを停止するため、データ損失にはつながりません。
- Cisco ISE の複製では、プライマリノードが複製イベントをセカンダリノードに公開できず、公開されていないイベントの数が 150 万を超えると、システムですべてのセカンダリノードが [同期していない（OUT OF SYNC）] とマークされます。

  一方、公開されたシーケンスと複製イベントを消費するセカンダリノードの差分が 200 万を超えると、システムでそれらの特定の PSN が [同期していない（OUT OF SYNC）] とマークされます。

Cisco ISE ノードの登録解除

展開からノードを削除するには、ノードの登録を解除する必要があります。プライマリ PAN からセカンダリノードの登録を解除すると、登録解除されたノードのステータスがスタンドアロンに変わり、プライマリノードとセカンダリノード間の接続が失われます。複製の更新は、登録解除されたスタンドアロン ノードに送信されなくなります。

PSN の登録が取り消されると、エンドポイント データは失われます。スタンドアロン ノードになった後も PSN にエンドポイント データを残すには、以下のいずれかを実行します。

- プライマリ PAN からバックアップを取得し、PSN がスタンドアロンノードになったときに、このデータバックアップを復元します。
- PSN のペルソナを管理者（セカンダリ PAN）に変更し、管理者ポータルの [展開（Deployment）] ウィンドウからデータを同期してから、ノードを登録解除します。この時点で、このノードに、すべてのデータがあります。この後、既存の展開にセカンダリ PAN を追加できます。

（注） プライマリ PAN は登録解除できません。

Cisco ISE 展開でのノードのステータス

表 *8 : Cisco ISE* ノードのステータス

ノードステータス	説明	ガイドライン
接続済み（Connected）	ノードが接続され、複製が正常に動作します。	-
複製が停止（Replication Stopped）	ノードは接続されていますが、複製が停止しています。ノードはポート 443 および 12001 で到達可能です。 これは、根本的な複製の問題が解決されると変更される、一時的なステータスです。	根本的な問題は、それ自体で解決する場合があります。解決しない場合は、Cisco ISE GUI にログインし、[展開（Deployment）] ウィンドウから手動同期を実行します。
ノードに到達不能（Node Not Reachable）	ノードはポート 443 に到達できませんが、複製は正常に機能します。	根本的な問題が解決すると、ノードが自動的に復旧することがあります。解決しない場合は、Cisco ISE GUI にログインし、[展開（Deployment）] ウィンドウから手動同期を実行します。

ノードステータス	説明	ガイドライン
切断（Disconnected）	ノードに到達できず、複製が停止しました。	このステータスは、ノードが5分以上ダウンしている場合に設定されます。 根本的な問題が解決すると、ノードが自動的に復旧することがあります。解決しない場合は、Cisco ISE GUI にログインし、[展開（Deployment）] ウィンドウから手動同期を実行します。
登録失敗（Registration Failed）	ノードの登録に失敗しました。	手動同期を実行します。影響を受ける Cisco ISE ノードを登録解除してから登録し直します。
進行中（In Progress）	ノードの登録または手動同期が進行中です。 現在、[進行中（In Progress）] ステータスのタイムアウト値は 300 分です。その後、ステータスは次のように変わります。 • 登録または手動同期が正常に完了した場合は接続されます。 • ノードの登録に失敗した場合は、[登録失敗（Registration Failed）] と表示されます。 • 手動同期が失敗した場合は、[未同期（Not in Sync）] と表示されます。	ステータスが [接続済み（Connected）] に変更された場合、アクションは必要ありません。ステータスが [登録失敗（Registration Failed）] または [未同期（Not in Sync）] に変更された場合は、それぞれの行を確認し、必要なアクションを実行します。
未同期（Not in Sync）	ノードが同期されていません。	手動同期を実行します。影響を受ける Cisco ISE ノードを登録解除してから登録し直します。
アップグレード（Upgrading）	ノードのアップグレードが進行中です。	-

分散展開を設定する場合のガイドライン

分散環境で Cisco ISE を設定する前に、次の内容をよく読んでください。

- Cisco ISE サーバーのノードタイプを選択します。管理、ポリシー、サービス、およびモニタリング機能には Cisco ISE ノードを選択する必要があります。
- すべてのノードで、同じ Network Time Protocol（NTP）サーバーを選択します。ノード間のタイムゾーンの問題を回避するには、各ノードのセットアップ時に同じ NTP サーバー名を指定する必要があります。この設定で、展開内にあるさまざまなノードからのレポートとログが常にタイムスタンプで同期されるようになります。
- Cisco ISE のインストール時に Cisco ISE 管理者パスワードを設定します。以前の Cisco ISE 管理者のデフォルトのログインクレデンシャル（admin/cisco）は無効になっています。初期セットアップ中に作成したユーザー名とパスワードを使用するか、後でパスワードを変更した場合はそのパスワードを使用します。
- DNS サーバーを設定します。DNS サーバーに、分散展開に含まれるすべての Cisco ISE ノードの IP アドレスと完全修飾ドメイン名（FQDN）を入力します。解決できない場合は、ノード登録が失敗します。
- DNS サーバーの分散展開のすべての Cisco ISE ノードの正引きおよび逆引き DNS ルックアップを設定します。設定しなかった場合、Cisco ISE ノードの登録時および再起動時に、展開に関する問題が発生することがあります。すべてのノードで逆引き DNS ルックアップが設定されていない場合、パフォーマンスが低下する可能性があります。
- （オプション）プライマリ PAN からセカンダリ Cisco ISE ノードを登録解除して、Cisco ISE をアンインストールします。
- プライマリ MnT をバックアップし、新しいセカンダリ MnT にデータを復元します。これにより、新しい変更が複製されるときに、プライマリ MnT の履歴が新しい MnT と同期されます。
- プライマリ PAN と、セカンダリノードとして登録しようとしているスタンドアロンノードで、同じバージョンの Cisco ISE が実行されていることを確認します。
- 展開に別のノードを追加する前に、Cisco ISE プライマリ PAN で**内部 CA 設定**を有効にして、Cisco ISE 証明書サービスが期待どおりに機能することを確認します。内部 CA 設定を有効にするには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [内部CA設定（Internal CA Settings）]**の順に選択します。
- 新しいノードを展開に追加する際に、ワイルドカード証明書の発行元証明書チェーンが新しいノードの信頼できる証明書に含まれていることを確認します。新しいノードが展開に追加されると、ワイルドカード証明書が新しいノードに複製されます。
- Cisco TrustSec をサポートするように Cisco ISE 展開を設定する場合、または Cisco ISE が Cisco Catalyst Center と統合されている場合は、PSN を SXP 専用として設定しないでください。SXP は、Cisco TrustSec デバイスと Cisco TrustSec 以外のデバイス間のインターフェイスです。SXP は、Cisco TrustSec 対応ネットワークデバイスと通信しません。

プライマリ ノードおよびセカンダリ ノードで使用可能なメニュー オプション

分散展開を構成する Cisco ISE ノードで使用可能なメニューオプションは、ノードで有効なペルソナによって異なります。すべての管理およびモニタリングアクティビティは、プライマリ PAN を介して実行する必要があります。その他のタスクについては、セカンダリ ノードを使用する必要があります。このため、セカンダリノードのユーザーインターフェイスでは、ノードで有効なペルソナに基づく限定されたメニューオプションが提供されます。

1 つのノードが、ポリシーサービスペルソナとプライマリロールのモニタリングペルソナを担当するなど、複数のペルソナを担当する場合、PSN およびプライマリ MnT にリストされているメニューオプションがそのノードで使用可能となります。

次の表に、それぞれのペルソナを担当する Cisco ISE ノードで使用可能なメニューオプションを示します。

表 *9 : Cisco ISE* ノードおよび使用可能なメニュー オプション

Cisco ISE ノード	使用可能なメニュー オプション
すべてのノード	• システム時刻と NTP サーバー設定の表示および設定。 • サーバー証明書のインストールと証明書署名要求の管理。すべてのサーバー証明書を一元的に管理するプライマリ PAN 経由で、展開内のすべてのノードに対し、サーバー証明書の操作を実行できます。 （注） 秘密キーは、ローカルデータベースに格納されず、関連ノードからコピーされません。秘密キーは、ローカルファイルシステムに格納されます。
プライマリポリシー管理ノード（プライマリ PAN）	すべてのメニューおよびサブメニュー。
プライマリ モニタリング ノード（プライマリ MnT ノード）	• モニタリングデータへのアクセスを提供。 （注） [操作（Operations）] メニューはプライマリ PAN からのみ表示できます。[操作（Operations）] メニューはモニタリングノードには表示されません。
PSN（ポリシーサービスノード）	Active Directory 接続への参加、脱退、およびテストを行うオプションを使用できます。各 PSN が別個に Active Directory ドメインに参加している必要があります。最初にドメイン情報を定義し、PAN を Active Directory ドメインに参加させる必要があります。次に、他の PSN を Active Directory ドメインに個別に参加させます。

Cisco ISE ノード	使用可能なメニュー オプション
セカンダリポリシー管理ノード（セカンダリ PAN）	セカンダリ PAN をプライマリ PAN に昇格させるオプション。 （注） プライマリ PAN にセカンダリ ノードを登録した後は、いずれのセカンダリ ノードの管理者ポータルにログインする場合にも、プライマリ PAN のログイン情報を使用する必要があります。

展開とノードの設定

[展開ノード（Deployment Nodes）] ウィンドウを使用すると、Cisco ISE（PAN、PSN、および MnT）ノードを設定して、展開を設定することができます。

展開ノードリストウィンドウ

次の表に、展開内の Cisco ISE ノードを設定するために使用できる [展開のノードリスト（Deployment Nodes List）] ウィンドウのフィールドを示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。

表 *10* : 展開ノードリスト

フィールド名	使用上のガイドライン
ホスト名（Hostname）	ノードのホスト名を表示します。
ペルソナ（Personas）	（ノードタイプが Cisco ISE の場合のみ表示されます）Cisco ISE ノードが想定しているペルソナ（管理、ポリシーサービス、モニタリング、pxGrid など）が表示されます。 例えば、[管理（Administration）]、[ポリシーサービス（Policy Service）]、[モニタリング（Monitoring）]、または [pxGrid] などです。
ロール（Role）	このノードで管理ペルソナまたはモニタリングペルソナが有効になっている場合、これらのペルソナが担当しているロール（プライマリ、セカンダリ、またはスタンドアロン）が示されます。ロールは、次のうちの 1 つまたは複数にできます。 • **[PRI(A)]**：プライマリ PAN を意味します。 • **[SEC(A)]**：セカンダリ PAN を意味します。 • **[PRI(M)]**：プライマリ MnT を意味します。 • **[SEC(M)]**：セカンダリ MnT を意味します。

フィールド名	使用上のガイドライン
サービス（Services）	（ポリシー サービス ペルソナが有効な場合のみ表示されます）この Cisco ISE ノードで実行されているサービスが表示されます。サービスは、次のいずれか 1 つとなります。 • **ID マッピング** • **セッション** • **プロファイリング** • **すべて**
ノードステータス（Node Status）	データレプリケーション用の展開内の各 Cisco ISE ノードのステータスを示します。 • [緑（接続済み）（Green（Connected））]：すでに展開に登録されている Cisco ISE ノードがプライマリ PAN と同期していることを示します。 • [赤（切断）（Red（Disconnected））]：Cisco ISE ノードに到達できないか、またはダウンしているか、あるいはデータレプリケーションが行われていないことを示します。 • [オレンジ（進行中）（Orange（In Progress））]：Cisco ISE ノードがプライマリ PAN に新規に登録されているか、または 手動同期操作を実行したか、あるいは Cisco ISE ノードがプライマリ PAN と同期していないことを示します。 詳細については、[ノードステータス（Node Status）]列で各 Cisco ISE ノードのクイックビューアイコンをクリックします。

関連トピック

Cisco ISE 分散展開 （418 ページ）
Cisco ISE デプロイメントの用語 （414 ページ）
Cisco ISE ノードの設定 （414 ページ）
セカンダリ Cisco ISE ノードの登録 （416 ページ）

ノードの一般設定

次の表で、Cisco ISE ノードの [全般設定 (General Settings)] ウィンドウのフィールドについて説明します。このウィンドウでは、ペルソナをノードに割り当て、そのサービスを実行するように設定できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [展開ノード（Deployment Node）] > [編集（Edit）] > [全般設定（General Settings）]** です。

表 *11 :* ノードの一般設定

フィールド名	使用上のガイドライン
ホスト名（Hostname）	Cisco ISE ノードのホスト名を表示します。
FQDN	Cisco ISE ノードの完全修飾ドメイン名を表示します（例：ise1.cisco.com）。
IP ドレス（IP Address）	Cisco ISE ノードの IP アドレスを表示します。
ノードタイプ（Node Type）	ノードタイプを表示します。
ペルソナ（Personas）	
管理（Administration）	Cisco ISE ノードに管理ペルソナを担当させる場合は、このトグルボタンを有効にします。管理ペルソナは、管理サービスを提供するようライセンスされているノードでのみ有効にできます。 [ロール（Role）]：管理ペルソナが展開で担当しているロールを表示します。ペルソナは[スタンドアロン（Standalone）]、[プライマリ（Primary）]、[セカンダリ（Secondary）] のいずれかの値を受け持てます。 [プライマリにする（Make Primary）]：ノードをプライマリ Cisco ISE ノードにする場合にこれをクリックします。展開では 1 つのプライマリ Cisco ISE ノードのみを使用できます。このウィンドウのその他のオプションは、ノードをプライマリにした後にのみアクティブになります。展開では 2 つの管理ノードのみを使用できます。ノードに[スタンドアロン（Standalone）] ロールがある場合は、横に [プライマリにする（Make Primary）] ボタンが表示されます。ノードに [セカンダリ（Secondary）] ロールがある場合は、横に [プライマリに昇格（Promote to Primary）] ボタンが表示されます。ノードに [プライマリ（Primary）] ロールがあり、他のノードが登録されていない場合は、横に [スタンドアロンにする（Make Standalone）] ボタンが表示されます。[スタンドアロンにする（Make Standalone）] ボタンをクリックして、プライマリノードをスタンドアロンノードにします。

フィールド名	使用上のガイドライン
モニタリング（Monitoring）	Cisco ISE ノードにモニタリングペルソナを担当させ、ログコレクタとして機能させる場合は、このトグルボタンをクリックします。分散展開内にモニタリング ノードが少なくとも 1 つ存在する必要があります。プライマリ PAN の設定時に、モニタリングペルソナを有効にする必要があります。展開内のセカンダリ モニタリング ノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリングペルソナを無効にしたりできます。 VMware プラットフォームで Cisco ISE ノードをログコレクタとして設定するには、次のガイドラインに従って最低限必要なディスク領域を決定します。1 日あたりネットワーク内のエンドポイント 1 つにつき 180 KB、1 日あたりネットワーク内の Cisco ISE ノード 1 つにつき 2.5 MB となります。 モニタリング ノードに何ヵ月分のデータを格納するかに応じて、必要な最大ディスク領域を計算します。展開にモニタリング ノードが 1 つしかない場合は、スタンドアロン ロールを担当します。展開に 2 つのモニタリング ノードがある場合は、Cisco ISE にプライマリ/セカンダリ ロールを設定する他のモニタリングノードの名前も表示されます。これらのロールを設定するには、次のいずれかを選択します。 • [プライマリ（Primary）]：現在のノードをプライマリ モニタリング ノードにする場合。 • [セカンダリ（Secondary）]：現在のノードをセカンダリ モニタリング ノードにする場合。 • [なし（None）]：モニタリングノードにプライマリ/セカンダリ ロールを担当させない場合。 モニタリング ノードの 1 つをプライマリまたはセカンダリとして設定すると、もう一方のモニタリング ノードが自動的にそれぞれセカンダリ ノードまたはプライマリ ノードになります。プライマリ モニタリング ノードおよびセカンダリ モニタリング ノードは、管理ログおよびポリシー サービス ログを受信します。1 つのモニタリングノードのロールを [なし（None）] に変更すると、もう 1 つのモニタリングノードのロールも [なし（None）] になるため、ノードをモニタリングノードに指定した後はハイアベイラビリティペアが取り消されます。このノードは、[リモートロギングターゲット（Remote Logging Targets）] ウィンドウに syslog ターゲットとしてリストされます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[リモートロギングターゲット（Remote Logging Targets）]**。

フィールド名	使用上のガイドライン
ポリシーサービス（Policy Service）	

フィールド名	使用上のガイドライン
	次のサービスのいずれか1つまたはすべてを有効にするには、このトグルボタンをクリックします。 • [セッションサービスの有効化（Enable Session Services）]：ネットワーク アクセス サービス、ポスチャサービス、ゲストサービス、およびクライアント プロビジョニング サービスを有効にするには、このチェックボックスをオンにします。[ノードをノードグループに含める（Include Node in Node Group）] ドロップダウンリストから、このポリシーサービスノードが所属するグループを選択します。認証局（CA）サービスと Enrollment over Secure Transport （EST）サービスは、セッションサービスが有効になっているポリシーサービスノードでのみ実行できることに注意してください。 [ノードをノードグループに含める（Include Node in Node Group）] については、このポリシーサービスモードをグループに含めない場合は [なし（None）] を選択します。 同じノード グループ内のすべてのノードが、ネットワーク アクセス デバイス（NAD）で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノードグループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロード バランサを使用していない場合、ノードグループ内のノードは、NAD で設定されている RADIUS サーバーおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバーとしても設定できます。 多数の ISE ノード（RADIUS サーバーや動的許可クライアントとして）を持つ単一の NAD は設定できますが、すべてのノードが同じノードグループに所属している必要はありません。 ノード グループのメンバーは、ギガビット イーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノード グループのメンバーは L2 隣接関係である必要はありませんが、十分な帯域幅と到達可能性を確保するには L2 隣接関係が強く推奨されます。詳細については、ポリシー サービス ノード グループの作成 （475 ページ） を参照してください。 • [プロファイリングサービスの有効化（Enable Profiling Service）]：プロファイラサービスを有効にするには、このチェックボックスをオンにします。プロファイリングサービスを有効にする場合は、[プロファイリング設定（Profiling Configuration）] タブをクリックし、必要に応じて詳細を入力する必要があります。ポリシー サービス ノードで実行されるサービスを有効または無効にしたり、このノードを変更したりする場合は、そのサービスが実行されるアプリケーション サーバー プロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。ノードでアプリケーションサーバーがいつ再起動した

フィールド名	使用上のガイドライン
	かを確認するには、CLI で **show application status ise** コマンドを使用します。 • [脅威中心型 NAC サービスの有効化（Enable Threat Centric NAC Service）]：脅威中心型ネットワーク アクセス コントロール（TC-NAC）機能を有効にするには、このチェックボックスをオンにします。この機能では、脅威と脆弱性のアダプタから受信した脅威と脆弱性の属性に基づいて認証ポリシーを作成することができます。脅威のシビラティ（重大度）レベルと脆弱性評価の結果は、エンドポイントまたはユーザーのアクセス レベルを動的に制御するために使用できます。 • [SXPサービスの有効化（Enable SXP Service）]：ノードで SXP サービスを有効にするには、このチェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。 NIC ボンディングまたはチーミングを設定している場合は、ボンディングされたインターフェイスも物理インターフェイスとともに [使用インターフェイス（Use Interface）] ドロップダウン リストに表示されます。 • [デバイス管理サービスの有効化（Enable Device Admin Service）]：TACACS ポリシーセット、ポリシー結果などを作成し、ネットワークデバイスの設定を制御および監査するには、このチェックボックスをオンにします。 • [パッシブ ID サービスの有効化（Enable Passive Identity Service）]：ID マッピング機能を有効にするには、このチェックボックスをオンにします。この機能を使用すると、Cisco ISE ではなくドメインコントローラで認証されるユーザーをモニターすることができます。Cisco ISE がユーザーのネットワークアクセスをアクティブには認証しないネットワークでは、ID マッピング機能を使用して、Active Directory ドメインコントローラからユーザー認証情報を収集することができます。
pxGrid	pxGrid ペルソナを有効にするには、このチェックボックスをオンにします。Cisco pxGrid は、Cisco ISE セッションディレクトリから Cisco 適応型セキュリティアプライアンス（ASA）などの他のポリシー ネットワーク システムへコンテキスト依存情報を共有するために使用されます。pxGrid フレームワークは、ポリシーデータや設定データをノード間で交換するためにも使用できます（たとえば、ISE とサードパーティベンダー間でのタグやポリシーオブジェクトの共有）。また、脅威情報など、ISE 関連以外の情報の交換用にも使用できます。

関連トピック

分散 Cisco ISE 展開のペルソナ （414 ページ）

管理ノード （441 ページ）
ポリシー サービス ノード （451 ページ）
モニタリング ノード （455 ページ）
Cisco pxGridノード （464 ページ）
プライマリおよびセカンダリの Cisco ISE ノードの同期 （473 ページ）
ポリシー サービス ノード グループの作成 （475 ページ）
Cisco pxGrid ノードの展開 （466 ページ）
ノード ペルソナとサービスの変更 （474 ページ）
自動フェールオーバー用の MnT ノードの設定 （463 ページ）

プロファイリング ノードの設定

次の表では、プロファイラサービスのプローブの設定に使用できる [プロファイリング設定（Profiling Configuration）] ウィンドウのフィールドについて説明します。このウィンドウにアクセスするには、**[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [ISE ノード（ISE Node）] > [編集（Edit）] > [プロファイルング設定（Profiling Configuration）]** の順に選択します。

表 *12* : プロファイリング ノードの設定

フィールド名	使用上のガイドライン
NetFlow	ルータから送信された NetFlow パケットを受信するためにポリシーサービス ペルソナを担当していた Cisco ISE ノードごとに NetFlow を有効にするには、このトグルボタンをクリックします。次のオプションに必要な値を入力します。 • [インターフェイス（Interface）]：Cisco ISE ノード上のインターフェイスを選択します。 • [ポート（Port）]：NetFlow エクスポートがルータから受信した NetFlow リスナーポート番号を入力します。デフォルト ポートは 9996 です。
DHCP	IP ヘルパーからの DHCP パケットをリッスンするためにポリシーサービス ペルソナを担当していた Cisco ISE ノードごとに DHCP を有効にするには、このトグルボタンをクリックします。次のオプションの値を指定します。 • [インターフェイス（Interface）]：Cisco ISE ノード上のインターフェイスを選択します。 • [ポート（Port）]：DHCP サーバーの UDP ポート番号を入力します。デフォルト ポートは 67 です。

フィールド名	使用上のガイドライン
DHCP SPAN	DHCP パケットをリッスンするためにポリシーサービスペルソナを担当していた Cisco ISE ノードごとに DHCP SPAN を有効にするには、このトグルボタンをクリックします。 • [インターフェイス（Interface）]：Cisco ISE ノード上のインターフェイスを選択します。
HTTP	HTTP パケットを受信し、解析するためにポリシーサービスペルソナを担当していた Cisco ISE ノードごとに HTTP を有効にする場合は、コンコトグルボタンをクリックします。 • [インターフェイス（Interface）]：Cisco ISE ノード上のインターフェイスを選択します。
RADIUS	Cisco IOS センサー対応デバイスからの RADIUS セッション属性およびシスコサービスペルソナ（CDP）属性と Link Layer Discovery Protocol（LLDP）属性を収集するためにポリシーサービスペルソナを担当していた ISE ノードごとに RADIUS サーバーを有効にするには、このトグルボタンをクリックします。
ネットワークスキャン（NMAP）（Network Scan (NMAP)）	NMAP ノードを有効にするには、このトグルボタンをクリックします。
DNS	FQDN の DNS ルックアップを実行するためにポリシーサービスペルソナを担当していた Cisco ISE ノードごとに DNS を有効にするには、このトグルボタンをクリックします。[タイムアウト（Timeout）]の時間を秒単位で入力します。 （注） DNS プローブを分散展開内の特定の Cisco ISE ノードで動作させるには、DHCP、DHCP SPAN、HTTP、RADIUS、SNMP のいずれかのプローブを有効にする必要があります。DNS ルックアップの場合、これらのいずれかのプローブを DNS プローブとともに起動する必要があります。

フィールド名	使用上のガイドライン
SNMPクエリ（SNMP Query）	指定した間隔でネットワークデバイスをポーリングするためにポリシーサービスペルソナを担当していた Cisco ISE ノードごとに SNMP クエリを有効にするには、このトグルボタンをクリックします。[再試行回数（Retries）]、[タイムアウト（Timeout）]、[イベントタイムアウト（Event Timeout）]（必須）、および[説明（Description）]（任意）フィールドに値を入力します。 （注） SNMP クエリプローブの設定に加えて、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]**にある他の SNMP 設定も行う必要があります。ネットワークデバイスで SNMP 設定を行う場合は、ネットワークデバイス上で CDP と LLDP がグローバルに有効になっていることを確認します。
SNMP トラップ（SNMP Trap）	ネットワークデバイスから linkUp、linkDown、および MAC の通知トラップを受信するためにポリシーサービスペルソナを担当していた Cisco ISE ノードごとに SNMP トラッププローブを有効にするには、このトグルボタンをクリックします。次の情報を入力または有効にします。 • [リンクトラップクエリ（Link Trap Query）]：SNMP トラップを介して受信する通知を受信して解釈するには、このトグルボタンを有効にします。 • [MAC トラップクエリ（MAC Trap Query）]：SNMP トラップを介して受信する MAC 通知を受信して解釈するには、このトグルボタンを有効にします。 • [インターフェイス（Interface）]：Cisco ISE ノードのインターフェイスを選択します。 • [ポート（Port）]：使用するホストの UDP ポートを入力します。デフォルト ポートは 162 です。
Active Directory	定義された Active Directory サーバーをスキャンして Windows ユーザーに関する情報を探すには、このトグルボタンをクリックします。 • [再スキャン前の日数（Days before rescan）]：スキャンを再度実行するまでの日数を選択します。
pxGrid	Cisco ISE が pxGrid を介してエンドポイント属性を収集（プロファイル）できるようにするには、このトグルボタンをクリックします。

関連トピック

Cisco ISE プロファイリング サービス （1210 ページ）
プロファイリング サービスによって使用されるネットワーク プローブ （1213 ページ）

Cisco ISE ノードでのプロファイリング サービスの設定 （1213 ページ）

ロギングの設定

以降の項では、デバッグログのシビラティ（重大度）の設定、外部ログターゲットの作成、およびこれらの外部ログターゲットにログメッセージを送信するための Cisco ISE の有効化の方法について説明します。

リモート ロギング ターゲットの設定

次の表では、外部の場所（syslog サーバー）を作成してロギングメッセージを保存するために使用する [リモートロギングターゲット（Remote Logging Targets）] ウィンドウのフィールドについて説明します。このウィンドウにアクセスするには、**[管理（Administration）] > [システム（System）] > [ロギング （Logging）] > [リモートロギングターゲット（Remote Logging Targets）]** を選択し、[追加（Add）] をクリックします。

表 *13 :* リモート ロギング ターゲットの設定

フィールド名	使用上のガイドライン
名前（Name）	新しい syslog ターゲットの名前を入力します。
ターゲットタイプ（Target Type）	ドロップダウンリストから、該当するターゲットタイプを選択します。デフォルト値は [UDP Syslog] です。
説明（Description）	新しいターゲットの簡単な説明を入力します。
IPアドレス（IP Address）	ログを格納する宛先マシンの IP アドレスまたはホスト名を入力します。Cisco ISE は、ロギング用に IPv4 形式と IPv6 形式をサポートします。
ポート（Port）	宛先マシンのポート番号を入力します。
ファシリティコード（Facility Code）	ロギングに使用する必要がある syslog ファシリティコードをドロップダウンリストから選択します。有効なオプションは、Local0 ～ Local7 です。
最大長（Maximum Length）	リモート ログ ターゲット メッセージの最大長を入力します。有効な値は 200 ～ 1024 バイトです。
このターゲットのアラームを含める（Include Alarms for this Target）	このチェックボックスをオンにすると、アラームメッセージもリモートサーバーに送信されます。

フィールド名	使用上のガイドライン
RFC 3164に準拠する（Comply to RFC 3164）	このチェックボックスをオンにすると、バックスラッシュ（\）が使用されている場合でも、リモートサーバーに送信されるsyslogメッセージのデリミタ（(, ; { } \ \）はエスケープされません。
サーバーダウン時のバッファメッセージ（Buffer Message When Server Down）	このチェックボックスは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [TCP Syslog] または [セキュアな syslog（Secure Syslog）] を選択すると表示されます。TCP syslog ターゲットまたはセキュアな syslog ターゲットが使用できないときに syslog メッセージを Cisco ISE がバッファできるようにするには、このチェックボックスをオンにします。Cisco ISE は、ターゲットへの接続が再開されるとターゲットへのメッセージの送信を再試行します。接続が再開されると、メッセージは最も古いものから順に送信されます。バッファされたメッセージは、常に新しいメッセージの前に送信されます。バッファがいっぱいになると、古いメッセージが廃棄されます。
バッファサイズ（MB）（Buffer Size (MB)）	各ターゲットのバッファサイズを設定します。デフォルトでは、100 MB に設定されます。バッファサイズを変更するとバッファがクリアされ、特定のターゲットのバッファリングされた既存のすべてのメッセージが失われます。
再接続タイムアウト（秒）（Reconnect Timeout (Sec)）	サーバーがダウンした場合に TCP とセキュアな syslog を破棄するまで保存する期間を設定する期間を秒単位で入力します。
CA証明書の選択（Select CA Certificate）	このドロップダウンリストは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [セキュアな syslog（Secure Syslog）] を選択すると表示されます。ドロップダウンリストからクライアント証明書を選択します。
サーバー証明書有効性を無視（Ignore Server Certificate validation）	このチェックボックスは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [セキュアな syslog（Secure Syslog）] を選択すると表示されます。サーバー証明書の認証を無視し、syslog サーバーを許可するには、Cisco ISE のこのチェックボックスをオンにします。デフォルトでは、このオプションが無効になっているときにシステムが FIPS モードでない限り、このオプションはオフに設定されます。

関連トピック

Cisco ISE ロギング メカニズム （708 ページ）
Cisco ISE システム ログ （709 ページ）
Cisco ISE メッセージ カタログ （713 ページ）
収集フィルタ （714 ページ）
イベント抑制バイパス フィルタ （715 ページ）
リモート syslog 収集場所の設定 （710 ページ）

収集フィルタの設定 （715 ページ）

セキュア Syslog ターゲット接続のためのクライアント認証の設定

Cisco ISE リリース 3.3 以降、クライアントがセキュアな syslog ターゲットに接続しようとする場合、クライアント認証は必須です。クライアント認証では、Cisco ISE サーバーと共有する証明書を Cisco ISE の信頼できる証明書ストアにインポートする必要があります。この信頼できる証明書は、共通名（CN）またはサブジェクト代替名（SAN）フィールドにクライアントのホスト名が含まれている必要があります。

2 つのスタンドアロン Cisco ISE ノードがあり、一方がクライアントでもう一方がリモート syslog ターゲットである場合は、次の手順を実行します。この例では、10.0.0.1 がクライアントで、10.0.0.2 がリモート syslog ターゲットです。

1. 10.0.0.1 では、[リモートロギングターゲット（Remote Logging Targets）] ウィンドウで、[ホスト/IPアドレス（Host/IP Address）] フィールドに **10.0.0.2** を入力して新しいリモート syslog ターゲットを設定します。
2. 10.0.0.2 では、[リモートロギングターゲット（Remote Logging Targets）] ウィンドウで、デフォルトの **SecureSyslogCollector** を有効にします。
3. 10.0.0.1 の信頼できる証明書を 10.0.0.2 の信頼できる証明書ストアにアップロードします。
   - 10.0.0.1 のリモート syslog ターゲット設定で、[CA証明書の選択（Select CA Certificate）] フィールドで自己署名証明書を選択した場合は、その自己署名証明書を 10.0.0.2 で信頼できる証明書としてアップロードします。
   - 10.0.0.1 のリモート syslog ターゲット設定で、[CA証明書の選択（Select CA Certificate）] フィールドでサードパーティの CA 証明書を選択した場合は、ルート CA 証明書と CA 署名付き証明書のチェーンを 10.0.0.2 で信頼できる証明書としてアップロードします。
4. 10.0.0.2 の信頼できる証明書を 10.0.0.1 の信頼できる証明書ストアにアップロードします。
   - 10.0.0.2 のリモート syslog ターゲット設定で、[CA証明書の選択（Select CA Certificate）] フィールドで自己署名証明書を選択した場合は、その自己署名証明書を 10.0.0.1 で信頼できる証明書としてアップロードします。
   - 10.0.0.2 のリモート syslog ターゲット設定で、[CA証明書の選択（Select CA Certificate）] フィールドでサードパーティの CA 証明書を選択した場合は、ルート CA 証明書と CA 署名付き証明書のチェーンを 10.0.0.1 で信頼できる証明書としてアップロードします。
5. 10.0.0.2 は、設定した証明書（自己署名または CA 署名付きのいずれか）を認証のために 10.0.0.1 に送信します。
6. 10.0.0.1 は 10.0.0.2 から証明書を受信し、設定した信頼できる証明書で応答して認証ワークフローを完了します。

ロギングカテゴリの設定

次の表では、ロギングカテゴリを設定するために使用可能なフィールドについて説明します。ログのシビラティ（重大度）レベルを設定し、ロギングカテゴリのログにロギングターゲットを選択します。このウィンドウにアクセスするには、**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** の順に選択します。

表示するロギングカテゴリの横のオプションボタンをクリックし、[編集（Edit）] をクリックします。次の表では、ロギングカテゴリの編集ウィンドウに表示されるフィールドについて説明します。

表 *14*：ロギング カテゴリの設定

フィールド名	使用上のガイドライン
名前（Name）	ロギング カテゴリの名前を表示します。
ログのシビラティ（重大度）レベル（Log Severity Level）	一部のロギングカテゴリでは、この値はデフォルトで設定されており、編集できません。一部のロギングカテゴリでは、次のシビラティ（重大度）レベルのいずれかをドロップダウンリストから選択できます。 • [重大（FATAL）]：緊急事態レベル。このレベルは、Cisco ISE を使用できず、必要なアクションをただちに実行する必要があることを意味します。 • [エラー（ERROR）]：このオプションは、深刻な状態またはエラー状態を示します。 • [警告（WARN）]：このオプションは、通常の状態ではあるが重大な状態を示します。これは、多くのロギングカテゴリに設定されるデフォルトのレベルです。 • [情報（INFO）]：このレベルは、情報メッセージを示します。 • [デバッグ（DEBUG）]：このレベルは、診断バグメッセージを示します。
ローカルロギング（Local Logging）	ローカルノードでこのカテゴリのロギングイベントを有効にするには、このチェックボックスをオンにします。
ターゲット（Targets）	この領域では、左右の矢印アイコンを使用し、[使用可能（Available）] 領域と [選択済み（Selected）] 領域間でターゲットを移動して、ロギングカテゴリのターゲットを選択できます。 [使用可能（Available）] 領域には、ローカル（事前定義済み）と外部（ユーザー定義）の両方の既存のロギングターゲットが含まれています。 [選択済み（Selected）] 領域（最初は空）には、カテゴリに選択されたターゲットが表示されます。

関連トピック

Cisco ISE メッセージ コード （712 ページ）
リモート syslog 収集場所の設定 （710 ページ）
メッセージ コードのシビラティ（重大度）レベルの設定 （712 ページ）

管理者アクセスの設定

これらのセクションで、管理者のアクセス設定を行うことができます。

管理者パスワード ポリシーの設定

次の表では、管理者パスワードが満たす必要のある基準を定義するために使用できる[パスワードポリシー（Password Policy）]ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理アクセス（Admin Access）] > [認証（Authentication）] > [パスワードポリシー（Password Policy）]**。

表 *15 :* 管理者パスワード ポリシーの設定

フィールド名	使用上のガイドライン
最小長（Minimum Length）	パスワードの最小長（文字数）を指定します。デフォルトは6文字です。

フィールド名	使用上のガイドライン
パスワードに使用できない文字（Password may not contain）	[管理者名またはその文字の逆順（Admin name or its characters in reverse order）]：このチェックボックスをオンにして、管理者ユーザー名またはその文字の逆順でのパスワードとしての使用を制限します。
	[Ciscoまたはその文字の逆順（Cisco or its characters in reverse order）]：このチェックボックスをオンにして、単語「Cisco」またはその文字の逆順でのパスワードとしての使用を制限します。
	[この単語またはその文字の逆順（This word or its characters in reverse order）]：このチェックボックスをオンにして、定義したすべての単語またはその文字の逆順でのパスワードとしての使用を制限します。
	[4回以上連続する繰り返し文字の使用（Repeated characters four or more times consecutively）]：このチェックボックスをオンにして、4 回以上連続する繰り返し文字のパスワードとしての使用を制限します。
	[辞書の単語、その文字の逆順、または文字の置き換え（Dictionary words, their characters in reverse order or their letters replaced with other characters）]：辞書の単語、単語の文字の逆順での使用、または単語の文字の置き換えでのパスワードとしての使用を制限します。 「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」などに置き換えることはできません。たとえば、「Pa $$ w0rd」は許可されません。 • [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。 このオプションは、デフォルトで選択されます。 • [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。**[ファイルの選択（Choose File）]** をクリックし、カスタム辞書ファイルを選択します。このテキストファイルは、改行文字で区切られた（JSON 形式の）単語、.dic 拡張子、20 MB 以下のサイズで成り立っている必要があります。
パスワードには選択したタイプの文字がそれぞれ1文字以上含まれている必要があります（Password must contain at least one character of each of the selected types）	管理者のパスワードに含める必要がある文字のタイプのチェックボックスをオンにします。次の 1 つまたは複数のオプションを選択します。 • **小文字の英文字** • **大文字の英文字** • **数字** • **英数字以外の文字**

フィールド名	使用上のガイドライン
パスワード履歴（Password History）	同じパスワードが繰り返し使用されるのを防ぐために、新しいパスワードと異なっている必要がある以前のパスワードの数を指定します。[パスワードは以前のnバージョンとは異なる必要があります（Password must be different from the previous n versions）] チェックボックスをオンにし、対応するフィールドに数字を入力します。 ユーザーがパスワードを再使用できない日数を入力します。[パスワードをn日以内に再利用することはできません（Cannot reuse password within n days）] をオンにし、対応するフィールドに数字を入力します。
パスワードライフタイム（Password Lifetime）	次のオプションのチェックボックスをオンにして、指定した期間後にパスワードを変更するようユーザーに強制します。 • [管理者パスワードは作成後または最終変更後n日で有効期限が切れます（Administrator passwords expire n days after creation or last change）]：パスワードを変更しない場合に管理者アカウントが無効になるまでの時間（日数）。有効な範囲は 1 ～ 3,650 日です。 • [パスワードの有効期限のn日前に管理者に電子メールリマインダを送信します（Send an email reminder to administrators n days prior to password expiration）]：パスワードが期限切れになることを管理者に通知するまでの時間（日数）。有効な範囲は 1 ～ 3,650 日です。
ネットワークデバイスの機密データの表示	
管理者パスワードが必要（Require Admin Password）	共有秘密やパスワードなどのネットワークデバイスの機密データを表示するために管理者ユーザーがログインパスワードを入力するようにする場合には、このチェックボックスをオンにします。
パスワードをn分間キャッシュします（Password cached for n Minutes）	管理者ユーザーによって入力されたパスワードは、この期間キャッシュされます。管理ユーザーはこの間、ネットワークデバイスの機密データを表示するのにパスワードの再入力を求められることはありません。有効な範囲は 1 ～ 60 分です。

関連トピック

Cisco ISE 管理者 （9 ページ）
新しい管理者の作成 （11 ページ）

セッション タイムアウトおよびセッション情報の設定

次の表では、セッションタイムアウトを定義し、アクティブな管理セッションを終了するために使用できる[セッション（Session）]ウィンドウのフィールドについて説明します。ウィンドウにアクセスするには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理**

（Administration ）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [セッション（Session）] の順に選択します。

表 *16*：セッション タイムアウトおよびセッション情報の設定

フィールド名	使用上のガイドライン
セッションタイムアウト（Session Timeout）	
セッション アイドル タイムアウト（Session Idle Timeout）	アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。
セッション情報（Session Info）	
無効化（Invalidate）	終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。

関連トピック

管理者アクセスの設定 （661 ページ）
管理者のセッション タイムアウトの設定 （667 ページ）
アクティブな管理セッションの終了 （667 ページ）

管理ノード

管理ペルソナの Cisco ISE ノードは、Cisco ISE のすべての管理操作を実行することができます。認証、許可、監査などの機能に関連したすべてのシステム関連設定を処理します。分散環境では、最大2つの管理ペルソナを実行するノードを実行できます。管理ペルソナは、スタンドアロン、プライマリ、またはセカンダリのロールのいずれかを担当できます。

管理ノードの高可用性

ハイアベイラビリティ構成では、プライマリポリシー管理ノード（PAN）がアクティブな状態です。セカンダリ PAN はスタンバイ状態です。これは、セカンダリ PAN がプライマリ PAN からすべての設定更新を受信するものの、Cisco ISE ネットワークではアクティブではないことを意味します。

Cisco ISE は、手動および自動フェールオーバーをサポートします。自動フェールオーバーでは、プライマリ PAN がダウンした場合にセカンダリ PAN の自動昇格が開始されます。自動フェールオーバーでは、ヘルスチェックノードと呼ばれる非管理セカンダリノードが必要です。ヘルスチェックノードは、プライマリ PAN の正常性を確認します。プライマリ PAN がダウンするか、または到達不能であることが検出された場合、ヘルスチェックノードがセカンダリ PAN の昇格を開始して、プライマリロールが引き継がれます。

自動フェールオーバー機能を展開するには、3 つ以上のノードが必要です。このうちの 2 つが管理ペルソナとなり、1 つはヘルスチェックノードとして機能します。ヘルスチェックノードは非管理ノードで、PSN、MnT、または pxGrid ノード、あるいはそれらの組み合わせにできます。プライマリ PAN とセカンダリ PAN が異なるデータセンターにある場合、それぞれの PAN に正常性チェックノードが必要です。

次の表に、プライマリ PAN がダウンし、セカンダリ PAN がまだ引き継がれていない場合に影響を受ける機能を示します。

表 *17:* アベイラビリティという機能

機能名	プライマリ **PAN** がダウンしている場合に使用できますか。（はい/いいえ）
既存の内部ユーザーの RADIUS 認証	はい
既存または新しい AD ユーザーの RADIUS 認証	はい
プロファイル変更がない既存のエンドポイント	はい
プロファイル変更がある既存のエンドポイント	いいえ
プロファイリングで学習した新しいエンドポイント	いいえ
既存のゲスト：ローカル Web 認証（LWA）	はい
既存のゲスト：中央 Web 認証（CWA）	はい（自動デバイス登録機能を持つ ホットスポット、BYOD、CWA などのデバイス登録に有効なフローを除く）
ゲストのパスワード変更	いいえ
ゲスト：AUP	いいえ
ゲスト：ログイン失敗の最大回数の適用	いいえ

機能名	プライマリ PAN がダウンしている場合に使用できますか。（はい/いいえ）
新しいゲスト（Sponsored-Guest またはアカウント登録）	いいえ
ポスチャ	はい
内部 CA による BYOD	いいえ
登録済みの既存のデバイス	はい
MDM オンボーディング	いいえ
pxGrid サービス	いいえ
セカンダリノードの GUI へのログイン	はい（ログインプロセスは、PAN へのコールのブロックが最後のログイン詳細を更新しようとしたときに遅延します。ログインは、このコールタイムアウト後に続行されます。）

（注） 内部 CA による証明書のプロビジョニングをサポートするには、昇格後に、元のプライマリ PAN のルート証明書とそのキーを新しいプライマリノードにインポートする必要があります。セカンダリノードからプライマリ PAN への昇格後に追加された PSN ノードでは、自動フェールオーバー後に証明書のプロビジョニングが機能しません。

ハイアベイラビリティのヘルスチェックノード

プライマリ PAN のヘルスチェックノードをアクティブ ヘルス チェック ノードと呼びます。セカンダリ PAN のヘルスチェックノードをパッシブ ヘルス チェック ノードと呼びます。アクティブ ヘルス チェック ノードは、プライマリ PAN のステータスを検査し、管理ノードの自動フェールオーバーを管理します。ヘルスチェックノードとして 2 つの非管理 ISE ノードを使用することをお勧めします。1 つはプライマリ PAN、もう 1 つはセカンダリ PAN です。1 つだけヘルスチェックノードを使用する場合、そのノードがダウンすると、自動フェールオーバーは発生しません。

両方の PAN が同じデータセンターにある場合、1 つの非管理 ISE ノードをプライマリ PAN とセカンダリ PAN の両方のヘルスチェックノードとして使用できます。単一のヘルスチェックノードがプライマリ PAN とセカンダリ PAN の両方の状態を検査する場合、そのノードはアクティブ/パッシブ両方の役割を担います。

ヘルスチェックノードは非管理ノードです。つまり、ポリシーサービスノード、モニタリングノード、または pxGrid ノード、あるいはこれらの組み合わせにできます。管理ノードと同じデータセンター内の PSN ノードをヘルスチェックノードとして指定することをお勧めします。ただし、2 つの管理ノードが同じ場所（LAN またはデータセンター）にない小規模または一元化された展開では、管理ペルソナを持っていないノード（PSN/pxGrid/MnT）をヘルスチェックノードとして使用できます。

（注） 自動フェールオーバーを無効にし、プライマリ PAN の障害発生時に手動でセカンダリノードを昇格させることを選択した場合には、チェックノードは不要です。

セカンダリ PAN のヘルスチェックノード

セカンダリ PAN のヘルスチェックノードはパッシブモニターです。セカンダリ PAN がプライマリ PAN として昇格するまで、このノードはアクションを実行しません。セカンダリ PAN がプライマリロールを引き継ぐと、関連するヘルスチェックノードは管理ノードの自動フェールオーバーを管理するアクティブロールを担います。以前のプライマリ PAN のヘルスチェックノードはセカンダリ PAN のヘルスチェックノードになり、受動的にモニタリングを行います。

ヘルスチェックの無効化と再起動

ノードがヘルスチェックロールから削除された場合、または自動フェールオーバー設定が無効な場合、ヘルスチェックサービスはそのノードで停止します。自動フェールオーバー設定が指定されたハイアベイラビリティ ヘルス チェック ノードで有効になると、ノードは管理ノードの正常性のチェックを再度開始します。ノードのハイアベイラビリティ ヘルス チェック ロールを指定または削除しても、そのノードのいずれのアプリケーションが再起動されることはありません。ヘルス チェック アクティビティのみが開始または停止します。

ハイアベイラビリティのヘルスチェックノードを再起動すると、プライマリ PAN の以前のダウンタイムが無視され、再びヘルスステータスのチェックが開始されます。

ヘルスチェックノード

アクティブなヘルスチェックノードは、設定したポーリング間隔でプライマリ PAN のヘルスステータスをチェックします。ヘルスチェックノードはプライマリ PAN に要求を送信し、それに対する応答が構成内容に一致する場合は、プライマリ PAN が良好な状態であると見なします。プライマリ PAN の状態が設定済みフェールオーバー期間を超えて継続的に不良である場合、ヘルスチェックノードはセカンダリ PAN へのフェールオーバーを開始します。

ヘルスチェックの任意の時点で、フェールオーバー期間中に不良と報告されたヘルスステータスがその後で良好になったことが検出されると、ヘルスチェックノードはプライマリ PAN のステータスを良好としてマークし、ヘルスチェックサイクルをリセットします。

プライマリ PAN ヘルスチェックからの応答は、そのヘルスチェックノードで使用可能な設定値に照らして検証されます。応答が一致しない場合、アラームが発生します。ただし、プロモーション要求はセカンダリ PAN に対して行われます。

ヘルスノードの変更

ヘルスチェックに使用している Cisco ISE ノードを変更できますが、考慮すべき点がいくつかあります。

たとえば、ヘルスチェックノード（H1）が非同期になり、別のノード（H2）がプライマリ PAN のヘルスチェックノードになったとします。この場合、プライマリ PAN がダウンした時点で、同じプライマリ PAN を検査している別のノード（H2）があることを H1 が認識する方法はありません。その後、H2 がダウンしたりネットワークから切断されたりした場合に、実際のフェールオーバーが必要になります。しかし、セカンダリ PAN はプロモーション要求を拒否する権限を保持します。したがって、セカンダリ PAN がプライマリロールに昇格すると、H2 からのプロモーション要求が拒否されてエラーが発生します。プライマリ PAN のヘルスチェックノードは、非同期になった場合でもプライマリ PAN の状態を引き続き検査します。

セカンダリ PAN への自動フェールオーバー

プライマリ PAN が使用できなくなったときにセカンダリ PAN を自動的に昇格させるように Cisco ISE を設定できます。この設定は、[展開（Deployment）] ウィンドウのプライマリ PAN で実行できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。フェールオーバー時間は、[フェールオーバーの前に障害が発生したポール数（Number of Failure Polls before Failover）] で設定された回数と [ポーリング間隔（Polling Interval）] で設定された秒数をかけて得られる値として定義されます。デフォルト設定では、この時間は 10 分です。セカンダリ PAN からプライマリ PAN への昇格には、さらに 10 分かかります。つまりデフォルトでは、プライマリ PAN の障害発生からセカンダリ PAN の動作開始までの時間は 20 分です。

セカンダリ PAN がフェールオーバーコールを受信すると、実際のフェールオーバーに進む前に、次の検証が行われます。

- ネットワークでプライマリ PAN が使用不能になっている。
- 有効なヘルスチェックノードからフェールオーバー要求が受信された。
- セカンダリ PAN に関するフェールオーバー要求である。

すべての検証に合格すると、セカンダリ PAN はプライマリロールに自身を昇格させます。

次に、セカンダリ PAN の自動フェールオーバーが試行されるシナリオの例を示します（ただしこれに限定されません）。

- ポーリング期間中に、プライマリ PAN のヘルスが [フェールオーバーの前に障害が発生したポール数（Number of failure polls before failover）] の値に対して一貫して良好でない。
- プライマリ PAN 上の Cisco ISE サービスが手動で停止され、フェールオーバー時間にわたって停止状態のままである。
- ソフト停止またはリブートオプションを使ってプライマリ PAN がシャットダウンされ、設定済みのフェールオーバー時間にわたってシャットダウン状態のままである。

- プライマリ PAN が突然ダウン（電源オフ）し、フェールオーバー時間にわたってダウン状態のままである。
- プライマリ PAN のネットワーク インターフェイスがダウンした（ネットワークポートが閉じた、またはネットワークサービスがダウンした）、あるいは他の理由でヘルスチェックノードから到達不能になり、設定済みのフェールオーバー時間にわたってダウン状態のままである。

ヘルスチェックノードの再起動

再起動すると、ハイアベイラビリティのヘルスチェックノードでは、プライマリ PAN の以前のダウンタイムが無視され、再びヘルスステータスが確認されます。

セカンダリ PAN への自動フェールオーバーの場合の個人所有デバイスの持ち込み

プライマリ PAN がダウンしている場合、プライマリ PAN ルート CA チェーンによってすでに発行された証明書が存在するエンドポイントに対して認証が中断されることはありません。これは、展開内のすべてのノードに、信頼と検証のための証明書チェーン全体が含まれているためです。

ただし、セカンダリ PAN がプライマリに昇格されるまで、新しい BYOD デバイスはオンボードされません。BYOD のオンボードには、アクティブなプライマリ PAN が必要です。

元のプライマリ PAN が復帰するか、セカンダリ PAN が昇格すると、新しい BYOD エンドポイントは問題なくオンボードされます。

障害が発生したプライマリ PAN をプライマリ PAN として再結合できない場合は、新たに昇格したプライマリ PAN（元のセカンダリ PAN）でルート CA 証明書を再生成します。

既存の証明書チェーンの場合、新しいルート CA 証明書をトリガーすると、下位 CA 証明書が自動的に生成されます。新しい下位証明書が生成された場合でも、以前のチェーンによって生成されたエンドポイント証明書は引き続き有効です。

自動フェールオーバーが回避された場合のシナリオ例

次に、ヘルスチェックノードによる自動フェールオーバーが回避された場合、またはセカンダリノードへのプロモーション要求が拒否された場合を表すシナリオの例を示します。

- 昇格要求を受信するノードがセカンダリノードではない。
- セカンダリ PAN が受信した昇格要求にプライマリ PAN の正しい情報がない。
- 不正なヘルスチェックノードから昇格要求を受信した。
- 昇格要求は受信したが、プライマリ PAN は起動していて良好な状態である。
- 昇格要求を受信するノードが同期していない。

PAN 自動フェールオーバー機能の影響を受ける機能

次の表に、PANの自動フェールオーバーの設定が展開で有効になっている場合にブロックされる機能、または追加の設定変更を必要とする機能を示します。

機能	影響の詳細
ブロックされる操作	
アップグレード	CLI によるアップグレードがブロックされます。 デフォルトでは、この機能は無効になっています。 自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルスチェックノードとして機能します。（ヘルスチェックノードは非管理ノードで、PSN、MnT、または pxGrid ノード、あるいはそれらの組み合わせにできます）。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルスチェックノードが必要です。
バックアップの復元	CLI による復元アクションおよびユーザーインターフェイスがブロックされます。 PANの自動フェールオーバーの設定が復元前に有効だった場合は、正常に復元した後に再設定する必要があります。
ノード ペルソナの変更	GUI による以下のノードペルソナの変更はブロックされます。 • プライマリ PAN とセカンダリ PAN の両方の管理ペルソナ • PAN のペルソナ • PAN の自動フェールオーバー機能を有効にした後のヘルスチェックノードの登録解除
その他の CLI 操作	CLI による次の管理操作がブロックされます。 • パッチのインストールとロールバック • DNS サーバーの変更 • eth1、eth2、および eth3 インターフェイスの IP アドレスの変更 • eth1、eth2、および eth3 インターフェイスのホスト エイリアスの変更 • タイムゾーンの変更

機能	影響の詳細
他の管理ポータル操作	GUI による次の管理操作がブロックされます。 • パッチのインストールとロールバック • HTTPS 証明書の変更 • 管理者認証タイプの変更（パスワードベースの認証から証明書ベースの認証へとその逆）。
すでに最大数のデバイスに接続しているユーザーは接続できません。	障害の発生した PAN に一部のセッションデータが格納されていたため、PSN によってこれを更新できません。
PAN の自動フェールオーバーを無効にする必要がある操作	
CLI の操作	PAN の自動フェールオーバー設定が有効になっている場合は、CLI を介した次の管理操作で警告メッセージが表示されます。サービスまたはシステムがフェールオーバーのウィンドウ内に再起動されない場合は、これらの操作によって自動フェールオーバーが起動する場合があります。そのため、以下の操作の実行時には、PAN の自動フェールオーバーの設定を無効にすることを推奨します。 • Cisco ISE サービスの手動停止 • 管理 CLI を使用した Cisco ISE のソフトリロード（リブート）

自動フェールオーバー用のプライマリ PAN の設定

始める前に

自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルスチェックノードとして機能します。ヘルスチェックノードは非管理ノードで、PSN、MnT、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルスチェックノードが必要です。

ステップ 1 プライマリ PAN GUI にログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [PANのフェールオーバー（PAN Failover）]**。

ステップ 3 プライマリ PAN の自動フェールオーバーを有効にするには、[PANの自動フェールオーバーを有効にする（Enable PAN Auto Failover）] チェックボックスをオンにします。

（注） セカンダリ PAN をプライマリ PAN に昇格させることしかできません。PSN、MnT、または pxGrid ノード、あるいはそれらの組み合わせのみを担当する Cisco ISE ノードはプライマリ PAN に昇格できません。

ステップ 4 使用可能なすべてのセカンダリノードを含む [プライマリヘルスチェックノード（Primary Health Check Node）] ドロップダウンリストから、プライマリ PAN のヘルスチェックノードを選択します。

このノードは、プライマリ PAN と同じロケーションまたはデータセンターに置くことを推奨します。

ステップ 5 使用可能なすべてのセカンダリノードを含む [セカンダリヘルスチェックノード（Secondary Health Check Node）] ドロップダウンリストから、セカンダリ PAN のヘルスチェックノードを選択します。

このノードは、セカンダリ PAN と同じロケーションまたはデータセンターに置くことを推奨します。

ステップ 6 PAN のステータスがチェックされるまでの [ポーリング間隔（Polling Interval）] 時間を指定します。有効な値の範囲は 30 ～ 300 秒です。

ステップ 7 [フェールオーバーの前に障害が発生したポール数（Number of Failure Polls before Failover）] の数を指定します。

フェールオーバーは、PAN のステータスに障害が発生したポール数として指定された数に対して良好でない場合に発生します。有効な範囲は 2 ～ 60 です。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

セカンダリ PAN のプライマリ PAN へのプロモーション後に、次の操作を実行します。

- 手動で古いプライマリ PAN を同期して、展開内に戻します。
- 手動で同期されていない他のセカンダリノードを同期して、展開内に戻します。

セカンダリ PAN のプライマリへの手動昇格

プライマリ PAN が失敗し、PAN の自動フェールオーバーを設定していない場合は、セカンダリ PAN を新しいプライマリ PAN に手動で昇格させる必要があります。

始める前に

プライマリ PAN に昇格するように管理ペルソナで設定された 2 番目の Cisco ISE ノードがあることを確認します。

ステップ 1 セカンダリ PAN GUI にログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 3 [ノードの編集（Edit Node）] ウィンドウで、[プライマリに昇格（Promote to Primary）] をクリックします。

（注） セカンダリ PAN をプライマリ PAN に昇格させることしかできません。ポリシーサービスペルソナまたはモニタリングペルソナ、あるいはその両方のみを担当する Cisco ISE ノードはプライマリ PAN に昇格できません。

元はプライマリ PAN であったノードが復帰した場合は、自動的にレベル下げされ、セカンダリ PAN になります。このノード（元のプライマリ PAN）で手動で同期を実行し、ノードを展開に戻す必要があります。

セカンダリノードの [ノードの編集（Edit Node）] ウィンドウでは、オプションが無効なためペルソナまたはサービスを変更できません。変更を加えるには、管理者ポータルにログインする必要があります。

ステップ 4 [保存（Save）] をクリックします。

新しい Cisco ISE 展開での既存の Cisco ISE 展開のノードのプライマリ PAN としての再利用

既存の Cisco ISE 展開のノードを新しい Cisco ISE 展開のプライマリ PAN で再利用する場合は、次の手順を実行する必要があります。

ステップ 1 お使いの Cisco ISE バージョンに応じた『Cisco ISE インストールガイド』の説明のとおりに、Cisco ISE ユーティリティ「システムの消去の実行」を実行します。このドキュメントはhttps://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.htmlで入手できます。

ステップ 2 Cisco ISE インストールガイドの説明のとおりに、Cisco ISE の新規インストールを実行します。

ステップ 3 プライマリポリシー管理ノード（PAN）の設定 （415 ページ）を参照して、スタンドアロンノードをプライマリポリシー管理ノードとして設定します。

プライマリ PAN にサービスを復元

Cisco ISE は、元のプライマリ PAN への自動フォールバックをサポートしていません。セカンダリ PAN への自動フェールオーバーが開始された後、元のプライマリ PAN をネットワークに戻す場合は、それをセカンダリ PAN として設定する必要があります。

管理ノードの自動フェールオーバーのサポート

Cisco ISE は、管理ペルソナの自動フェールオーバーをサポートしています。自動フェールオーバー機能を有効にするには、分散セットアップで少なくとも 2 つのノードが管理ペルソナを引き継ぎ、1 つのノードが非管理ペルソナを引き継ぐ必要があります。プライマリ PAN がダウンした場合は、セカンダリ PAN の自動昇格が開始されます。この場合、非管理セカンダリノードが各管理ノードのヘルスチェックノードとして指定されます。ヘルスチェックノードは、設定された間隔で PAN の正常性を確認します。プライマリ PAN について受信したヘルスチェッ

ク応答がデバイスのダウンや到達不能などで良好でない場合、ヘルスチェックノードは設定したしきい値まで待機した後にプライマリロールを引き継ぐようにセカンダリ PAN の昇格を開始します。セカンダリ PAN の自動フェールオーバー後、いくつかの機能は使用できなくなります。Cisco ISE は元のプライマリ PAN へのフォールバックはサポートしていません。「管理ノードの高可用性」を参照してください。

ポリシー サービス ノード

ポリシーサービスモード（PSN）は Cisco ISE ノードであり、ポリシーサービスペルソナを使用して、ネットワークアクセス、ポスチャ、ゲストアクセス、クライアント プロビジョニング、およびプロファイリングの各サービスを提供します。

分散セットアップでは、少なくとも 1 つのノードがポリシーサービスペルソナを担当する必要があります。このペルソナはポリシーを評価し、すべての決定を行います。通常、1 つの分散型の展開に複数の PSN が存在します。

同じ高速ローカルエリアネットワーク（LAN）か、またはロードバランサの背後に存在するすべての PSN をまとめてグループ化し、ノードグループを形成することができます。ノードグループのいずれかのノードで障害が発生した場合、その他のノードは障害を検出し、URL にリダイレクトされたセッションをリセットします。

ポリシー サービス ノードのハイ アベイラビリティ

ノード障害を検出し、障害が発生したノードで URL がリダイレクトされたすべてのセッションをリセットするために、2 つ以上の PSN を同じノードグループに配置できます。ノードグループに属しているノードがダウンすると、同じノードグループの別のノードが、障害が発生したノードで URL がリダイレクトされたすべてのセッションに関する許可変更（CoA）を発行します。

同じノードグループ内のすべてのノードが、ネットワーク アクセス デバイス（NAD）で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノードグループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロードバランサを使用していない場合、ノードグループ内のノードは、NAD で設定されている RADIUS サーバーおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバーとしても設定できます。

（注） RADIUS サーバーやダイナミック認証クライアントとして多数の Cisco ISE ノードを持つ単一の NAD は設定できますが、すべてのノードが同じノードグループに所属している必要はありません。

ノードグループのメンバーは、ギガビットイーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノードグループのメンバーは L2 隣接関係である必要はありませ

んが、十分な帯域幅と到達可能性を確保するには L2 隣接関係が強く推奨されます。詳細については、ポリシー サービス ノード グループの作成 （475 ページ）を参照してください。

PSN 間で均等に要求を分散するためのロードバランサ

展開内に複数の PSN がある場合は、ロードバランサを使用して要求を均等に分散できます。ロードバランサは、その背後にある機能ノードに要求を分散します。PSN をロードバランサの背後に展開する詳細とベストプラクティスについては、『Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP』を参照してください。

ポリシー サービス ノードでのセッション フェールオーバー

ノードグループ内の PSN はセッション情報を共有します。ノードはハートビートメッセージを交換して、ノードの障害を検出します。ノードに障害が発生した場合、障害が発生した PSN のセッションをノードグループのピアの 1 つが認識し、それらのセッションの接続を解除するための CoA を発行します。ほとんどのクライアントが自動的に再接続し、新しいセッションを確立します。

一部のクライアントは自動的に再接続しません。たとえば、クライアントが VPN 経由で接続する場合、そのクライアントは CoA を認識しない可能性があります。IP Phone、マルチホスト 802.1X ポート、または仮想マシンであるクライアントも、CoA を認識しないか、または CoA に応答できない場合があります。URL リダイレクトクライアント（Web 認証）も自動的に接続できません。これらのクライアントは手動で再接続する必要があります。

タイミングの問題も再接続を妨げる可能性があります。たとえば、PSN フェールオーバー時にポスチャ状態が保留中の場合です。

PSN セッション共有の詳細については、ライトデータディストリビューション （453 ページ）を参照してください。

ポリシー サービス ノード グループ内のノード数

ノードグループに含めることができるノードの数は、展開要件によって異なります。ノードグループを使用すると、確実に、ノードの障害が検出され、許可されたがポスチャされていないセッションに関する CoA がピアによって発行されます。ノードグループのサイズはあまり大きくする必要はありません。

ノードグループのサイズが大きくなると、ノード間で交換されるメッセージおよびハートビートの数が大幅に増加します。その結果、トラフィックも増加します。ノードグループ内のノードの数を少なくすることで、トラフィックを削減でき、同時に PSN の障害を検出するのに十分な冗長性が提供されます。

ノードグループクラスタに含めることができる PSN の数にはハード制限はありません。

ライト データ ディストリビューション

ライト データ ディストリビューションを使用すると、ユーザーセッション情報を保存し、展開の PSN 全体で複製できるため、ユーザーセッションの詳細に関して PAN または MnT ノードに依存する必要がなくなります。

ライト データ ディストリビューションは、次のディレクトリから構成されています。

- RADIUS セッションディレクトリ
- エンドポイント オーナー ディレクトリ

さらに、[詳細設定（Advanced Settings）] から次のオプションを設定できます。

- [バッチ サイズ（Batch Size）]：セッション更新をバッチで送信できます。この値は、ライト データ ディストリビューション インスタンスから展開内の他の PSN に各バッチで送信するレコードの数を指定します。このフィールドを 1 に設定すると、セッション更新はバッチで送信されません。デフォルト値は 10 レコードです。
- [TTL]：この値は、Light Data Distributionの更新が完了するまでバッチのセッションが待機する最大時間を指定します。デフォルト値は、1000 ミリ秒です。

PSN 間の接続不良の場合（PSN がダウンした場合など）は、セッションの詳細を MnT セッションディレクトリから取得して今後使用するために保存されます。

大規模展開では、最大 2,000,000 セッション レコードを保持できます。小規模展開では、1,000,000 セッション レコードを保存できます。セッションのアカウンティングの停止要求を受信すると、対応するセッション データがすべてのライト データ ディストリビューション インスタンスから削除されます。保存されているレコードの数が上限を超えると、タイムスタンプに基づいて最も古いセッションが削除されます。

（注）

- セッションの IPv6 プレフィックス長が 128 ビット未満で、インターフェイス ID が指定されていない場合、IPv6プレフィックスは拒否されるため、複数のセッションで同じキーが使用されることはありません。
- ライト データ ディストリビューションは、ノード間通信に Cisco ISE メッセージングサービスを使用します。Cisco ISE リリース 3.0 以降では、Cisco ISE メッセージングサービスの証明書署名要求の生成がサポートされています。したがって、Cisco ISE リリース 3.0 以降では、ISE メッセージングサービスの内部と外部の両方の CA がサポートされています。Cisco ISE メッセージングサービスで問題が発生している場合は、Cisco ISE メッセージングサービス証明書を再生成する必要があります。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書署名要求（Certificate Signing Requests）]** の順に選択します。
2. [証明書の使用先（Certificate(s) will be used for）] セクションで、[ISEメッセージングサービス（ISE Messaging service）] を選択します。
3. [ISEメッセージングサービス証明書の生成（generate ISE messaging service certificate）] をクリックします。

RADIUS セッションディレクトリ

[RADIUS セッションディレクトリ（RADIUS Session Directory）] は、ユーザーセッション情報を保存し、展開の PSN 全体に複製するために使用されます。このディレクトリには、CoA に必要なセッション属性のみが保存されます。

この機能は、Cisco ISE リリース 2.7 以降ではデフォルトで有効になっています。この機能は、[ライトデータディストリビューション（Light Data Distribution）] の [RADIUSセッションディレクトリ（RADIUS Session Directory）] チェックボックスをオンまたはオフにして有効または無効にすることができます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ライト データ ディストリビューション（Light Data Distribution）]** です。

エンドポイント オーナー ディレクトリ

Cisco ISE リリース 2.6 までは、エンドポイントのプローブがその特定のエンドポイントの要求を最初に処理したものとは異なるポリシーサービスノード（PSN）で受信されると、エンドポイントのオーナーが新しい PSN に変更されます。これにより、エンドポイントの所有権のフラッピングが発生します。

Cisco ISE リリース2.7 では、[エンドポイント オーナーディレクトリ（Endpoint Owner Directory）] を使用して、Cisco ISE に接続している各 MAC アドレスの PSN FQDN を保存し、このデータ

を展開内の PSN 全体に複製します。これにより、すべての PSN がすべてのエンドポイントのオーナーを認識するため、エンドポイントの所有権のフラッピングが回避されます。エンドポイントの所有権は、そのエンドポイントの RADIUS 認証が別の PSN で成功した場合にのみ変更されるようになりました。

さらに、静的なエンドポイントの割り当てが着信プローブで受信された同じエンドポイントの属性よりも優先されるため、属性のオーバーライドの問題が回避されます。

この機能は、Cisco ISE リリース 2.7 以降ではデフォルトで有効になっています。必要な場合、これを無効にして、エンドポイント オーナー ディレクトリを使用していない古いメカニズムにフォールバックできます。[エンドポイント オーナー ディレクトリ（Endpoint Owner Directory）] は、プロファイリングでも使用されます。このオプションを無効にすると、レガシープロファイラのオーナーディレクトリが使用されます。この機能を有効または無効にするには、[ライト データ ディストリビューション（Light Data Distribution）] ウィンドウで [エンドポイント オーナー ディレクトリの有効化（Enable Endpoint Owner Directory）] チェックボックスをオンまたはオフにします。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]**>**[システム（System）]**>**[設定（Settings）]**>**[ライト データ ディストリビューション（Light Data Distribution）]**の順に選択します。

モニタリング ノード

モニタリングペルソナの機能を持つCisco ISEノードがログコレクタとして動作し、ネットワーク内の PAN と PSN からのログメッセージを保存します。このペルソナは、ネットワークとリソースを効果的に管理するために使用できる高度な監視およびトラブルシューティング ツールを提供します。このペルソナのノードは、収集するデータを集約して関連付けて、意味のある情報をレポートの形で提供します。

Cisco ISE では、プライマリ ロールまたはセカンダリ ロールを担うことができるこのペルソナを持つノードを最大2つ使用してハイ アベイラビリティを実現できます。プライマリ MnT ノードとセカンダリ MnT ノードの両方がログメッセージを収集します。プライマリ MnT がダウンした場合、プライマリ PANがモニタリングデータを収集するセカンダリノードを指定します。ただし、セカンダリノードがプライマリに自動的に昇格されることはありません。その場合は、「MnT ロールの手動変更」で説明されている手順に従って行う必要があります。

分散セットアップでは、少なくとも1つのノードが監視ペルソナを担当する必要があります。同じ Cisco ISE ノードで、モニタリングペルソナとポリシーサービスペルソナを有効にしないこと、および最適なパフォーマンスが得られるように、ノードは監視専用にすることをお勧めします。

展開内の PANから [モニタリング（Monitoring）] メニューにアクセスできます。

（注） pxGrid を有効にした場合は、pxGrid ノードの新しい証明書を作成する必要があります。デジタル署名を使用して証明書テンプレートを作成し、新しい PxGrid 証明書を生成します。

MnT ロールの手動変更

プライマリ PAN から MnT ロールを手動で変更できます（プライマリからセカンダリとセカンダリからプライマリの両方）。

ステップ 1 プライマリ PAN GUI にログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。

ステップ 3 ノードのリストで、ロールを変更するMnTノードの横にあるチェックボックスをオンにします。

ステップ 4 [編集（Edit）] をクリックします。

ステップ 5 [モニタリング（Monitoring）] セクションで、[プライマリ（Primary）] または[セカンダリ（Secondary）] にロールを変更します。

そのノードで有効になっている他のすべてのペルソナおよびサービスを無効にする場合は、[専用MnT（Dedicated MnT）] オプションを有効にします。このオプションを有効にすると、設定データ レプリケーションプロセスがそのノードで停止します。これにより、MnT ノードのパフォーマンスが向上します。このオプションを無効にすると、手動同期がトリガーされます。

ステップ 6 [保存（Save）] をクリックします。

Cisco ISE メッセージングサービスを介した syslog

Cisco ISE リリース 2.6 は、デフォルトで組み込みの UDP syslog 収集ターゲット（LogCollector および LogCollector2）用の MnT WAN 存続可能性を提供します。この存続可能性は、[MnTにUDP Syslogを伝送するために「ISEメッセージングサービス」を使用（Use "ISE Messaging Service" for UDP Syslogs delivery to MnT）] オプション（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[システム（System）] > [ロギング（Logging）] > [ログ設定（Log Settings）]**）によって有効になります。このオプションを有効にすると、UDP syslog が Transport Layer Security（TLS）によって保護されます。

[MnTにUDP Syslogを伝送するために「ISEメッセージングサービス」を使用（Use "ISE Messaging Service" for UDP Syslogs delivery to MnT）] オプションは、Cisco ISE リリース 2.6、First Customer Ship（FCS）ではデフォルトで無効になっています。このオプションは、Cisco ISE リリース 2.6 累積パッチ 2 以降のリリースではデフォルトで有効になっています。

UDP syslog に Cisco ISE メッセージングサービスを使用すると、MnT ノードにアクセスできなくても、運用データは一定期間保持されます。MnT WAN 存続可能性の期間は約 2 時間 30 分です。

このサービスは、TCP ポート 8671 を使用します。それに応じてネットワークを設定し、展開内の他のすべての Cisco ISE ノードから各 Cisco ISE ノードの TCP ポート 8671 への接続を許可してください。

（注） 展開環境で Cisco ISE 展開に TCP または Secure syslog を使用する場合、機能は以前のリリースと同じままになります。

IP アドレスを使用して UDP syslog ターゲットを定義することをお勧めします。これにより、DNS 名または DNS サーバーを使用して UDP syslog ターゲットを定義するときに発生する遅延が回避されます。

キューリンクアラーム

Cisco ISE メッセージングサービスは、さまざまな証明書（内部 CA のチェーンで署名された証明書）を使用します。Cisco ISE の GUI ダッシュボードの [アラーム（Alarms）] ダッシュレットに `queue-link alarm` メッセージが表示されます。アラームを解決するには、次のことができているか確認します。

- すべてのノードが接続され、同期されている。
- すべてのノードと Cisco ISE メッセージングサービスが機能している。
- Cisco ISE メッセージング サービス ポートは、ファイアウォールなどの外部エンティティによってブロックされていない。
- 各ノードの Cisco ISE メッセージング証明書チェーンが破損しておらず、証明書の状態が良好である。

キューリンクアラームを解決するには、Cisco ISE ルート CA チェーンを再生成します。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書署名要求（Certificate Signing Requests）]** の順に選択します。
2. [証明書署名要求の作成（Generate Certificate Signing Request）] をクリックし、[証明書の使用先（Certificate(s) will be used for）] ドロップダウンリストから [ISEルートCA（ISE Root CA）] を選択します。
3. [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA Certificate Chain）] をクリックします。

[キューリンクエラー（Queue Link Error）] アラームは、次のシナリオで生成されます。

- タイムアウト：Cisco ISE 展開内の 2 つノード間でネットワークの問題がある場合は、[タイムアウト（Timeout）] が原因で [キューリンクエラー（Queue Link Error）] アラームが発生します。このエラーをトラブルシューティングするには、ポート 8671 の接続を確認します。
- 不明な CA：[システム証明書（System Certificates）] ウィンドウ内（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]**）に破損した Cisco ISE メッセージング証明書が存在する場合、[不

明なCA（Unknown CA）] が原因で [キューリンクエラー（Queue Link Error）] アラームが発生します。この問題は、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書署名要求（Certificate Signing Requests）]** を選択し、Cisco ISE GUI で [証明書署名要求（CSR）の生成（Generate Certificate Signing Request (CSR)）] をクリックして、Cisco ISE メッセージング証明書を再生成することで解決できます。

（注） Cisco ISE ルート CA 証明書チェーンをすでに置き換えている場合は、再生成は必要ありません。

Cisco ISE ルート CA チェーンを置き換えると、Cisco ISE メッセージングサービス証明書も置き換えられます。その後、Cisco ISE メッセージングサービスが約 2 分のダウンタイムで再起動されます。このダウンタイム中に syslog が失われます。ダウンタイム中に syslog が失われるのを防ぐために、Cisco ISE メッセージングサービスを短期間無効化できます。

MnT に UDP Syslog を伝送するために Cisco ISE メッセージングサービスを有効または無効にするには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[システム（System）] > [ロギング（Logging）] > [ログ設定（Log Settings）]**。

ステップ 2 [MnTにUDP Syslogを伝送するために「ISEメッセージングサービス」を使用（Use “ISE Messaging Service” for UDP Syslogs delivery to MnT）] チェックボックスをオンまたはオフにして、Cisco ISE メッセージングサービスの使用を有効または無効にします。

ステップ 3 [保存（Save）] をクリックします。

Cisco ISE コミュニティリソース

キューリンクアラームの詳細については、「キューリンクエラー」を参照してください。

MnT ノードでの自動フェールオーバー

MnT ノードはハイアベイラビリティを実装しませんが、アクティブスタンバイを提供します。PSN は、プライマリとセカンダリの両方の MnT ノードに操作監査データをコピーします。

自動フェールオーバー プロセス

プライマリ MnT ノードがダウンした場合は、セカンダリ MnT ノードがすべてのモニタリング情報とトラブルシューティング情報を引き継ぎます。

セカンダリノードをプライマリノードに手動で変換するには、「MnT ロールの手動変更」を参照してください。セカンダリノードが昇格された後にプライマリノードが復旧した場合、プラ

イマリノードはセカンダリロールを担当します。セカンダリノードが昇格されなかった場合、プライマリ MnT ノードは復旧後にプライマリロールを再開します。

⚠

注意 プライマリノードがフェールオーバー後に復旧すると、セカンダリのバックアップを得てデータを復元し、プライマリノードを最新の状態にします。

MnT ノードのアクティブ/スタンバイペアを設定するためのガイドライン

Cisco ISE ネットワークでは 2 つの MnT ノードを指定して、アクティブ/スタンバイペアを設定できます。プライマリ MnT ノードをバックアップし、新しいセカンダリ MnT ノードにデータを復元することを推奨します。これにより、プライマリが新しいデータを複製するため、プライマリ MnR ノードの履歴が新しいセカンダリノードと同期されます。アクティブ/スタンバイペアには、次のルールが適用されます。

- すべての変更はプライマリ MnT ノードに記録されます。セカンダリ ノードは読み取り専用です。
- プライマリノードで行った変更は、セカンダリノードに自動的に複製されます。
- プライマリ ノードとセカンダリ ノードは両方とも、他のノードがログを送信するログ コレクタとしてリストされます。
- Cisco ISE ダッシュボードは、モニタリングおよびトラブルシューティングの主要なエントリ ポイントとなります。PAN からのモニタリング情報は、ダッシュボードに表示されます。プライマリ ノードがダウンした場合、セカンダリ ノードでモニタリング情報が利用できます。
- MnT データのバックアップおよび消去は、標準 Cisco ISE ノードのバックアッププロセスでは行われません。プライマリとセカンダリの両方の MnT ノードでバックアップとデータ消去用のリポジトリを設定し、それぞれに同じリポジトリを使用する必要があります。

MnT ノードのフェールオーバーシナリオ

次のシナリオは、MnT ノード数に応じてアクティブ/スタンバイまたは単一ノード構成に適用されます。

- MnT ノードのアクティブ/スタンバイ構成では、プライマリ PAN は、常にプライマリ MnT ノードに接続してモニタリングデータを収集します。プライマリ MnT ノードに障害が発生した後に、PAN はスタンバイ MnT ノードに接続します。プライマリノードからスタンバイノードへのフェールオーバーは、プライマリノードのダウンから 5 分以上経過した後に行われます。

  ただし、プライマリノードに障害が発生した後、セカンダリノードはプライマリノードになりません。プライマリノードが復旧した場合、PAN ノードは再開されたプライマリノードからのモニタリングデータの収集を再び開始します。
- プライマリ MnT ノードがダウンしたときにスタンバイ MnT ノードをアクティブステータスに昇格する場合は、MnT ロールの手動変更時の手順に従うか、既存のプライマリ MnT

ノードの登録を解除することで、スタンバイ MnT ノードをプライマリに昇格することができます。既存のプライマリ MnT ノードの登録を解除すると、スタンバイノードがプライマリ MnT ノードになり、PAN は新しく昇格されたプライマリノードに自動的に接続します。

- アクティブ/スタンバイペアで、セカンダリ MnT ノードの登録を解除するか、またはセカンダリ MnT ノードがダウンした場合は、既存のプライマリ MnT ノードが現在のプライマリノードのままになります。
- ISE 展開内にMnT ノードが 1 つだけ存在する場合、そのノードはプライマリ MnT ノードとして機能し、PAN にモニタリングデータを提供します。ただし、新しい MnT ノードを登録して展開内でプライマリノードにすると、既存のプライマリ MnT ノードが自動的にスタンバイノードになります。PAN は、新しく登録されたプライマリ MnT ノードに接続し、モニタリングデータを収集します。

モニタリング データベース

モニタリング機能によって利用されるデータレートとデータ量には、これらを目的とした専用のノード上に別のデータベースが必要です。

PSN のように、MnT ノードにはこの項で説明するトピックなどのメンテナンスタスクの実行に必要な専用のデータベースが備わっています。

モニタリングデータベースのバックアップと復元

モニタリングデータベースは、大量のデータを処理します。時間が経つにつれ、MnT ノードのパフォーマンスと効率は、そのデータをどう管理するかによって変わってきます。効率を高めるために、データを定期的にバックアップして、それをリモートのリポジトリに転送することを推奨します。このタスクは、自動バックアップをスケジュールすることによって自動化できます。

（注） 消去操作の実行中には、バックアップを実行しないでください。消去操作の実行中にバックアップが開始されると、消去操作が停止または失敗します。

セカンダリ MnT ノードを登録する場合は、最初にプライマリ MnT ノードをバックアップしてから、新しいセカンダリ MnT ノードにデータを復元することを推奨します。これにより、新しい変更内容が複製されるため、プライマリ MnT ノードの履歴が新しいセカンダリノードと同期状態となります。

モニタリングデータベースの消去

消去プロセスでは、消去時にデータを保持する月数を指定することで、モニタリングデータベースのサイズを管理できます。デフォルトは3ヵ月間です。この値は、消去用のディスク容

量使用率しきい値（合計ディスク容量の80%）に達したときに使用されます。このオプションでは、各月は 30 日で構成されます。デフォルトの 3 ヵ月は 90 日間です。

モニタリングデータベースの消去に関するガイドライン

次に示すような、最適なモニタリングデータベースのディスク使用に関するこれらのガイドラインに従います。

- モニタリングデータベースのディスク使用量がしきい値設定の80%（すなわち合計ディスク容量の60%）を超えた場合、データベースサイズが割り当てられたディスクサイズの最大値を超過しそうであることを示すクリティカルアラームが生成されます。ディスク使用量がしきい値設定の90%（すなわち合計ディスク容量の70%）を超えた場合、データベースサイズが割り当てられたディスクサイズの最大値を超過したことを示す、別のクリティカルアラームが生成されます。

  消去プロセスが実行され、ステータス履歴レポートが作成されます。このレポートは、[データ消去の監査（Data Purging Audit）] ウィンドウで確認できます。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [レポート（Reports）] > [レポート（Reports）] > [監査（Audit）] > [データ消去の監査（Data Purging Audit）]**。消去の完了後に情報（INFO）アラームが生成されます。

- 消去は、データベースの使用済みディスク領域のパーセンテージにも基づきます。モニタリングデータベースの使用済みディスク容量がしきい値（デフォルトは合計ディスク容量の80%）以上になると、消去プロセスが開始されます。このプロセスは、管理者ポータルの設定に関係なく、最も古い7日間のモニターリングデータのみを削除します。ディスク領域が 80% 未満になるまで繰り返しこのプロセスを続行します。消去では、処理の前にモニタリングデータベースのディスク容量制限が常にチェックされます。

運用データの消去

Cisco ISE モニタリング運用データベースには、Cisco ISE レポートとして生成された情報が含まれています。最近の Cisco ISE のリリース（Cisco ISE リリース 2.4 以降）には、モニタリング運用データを消去するオプションと、**application configure ise** コマンドを実行する際にモニタリングデータベースをリセットするオプションが備わっています。

パージオプションは、データのクリーンアップに使用します。また、保持する日数を尋ねるプロンプトを表示します。リセットオプションを使用すると、データベースが工場出荷時の初期状態にリセットされるため、バックアップされているすべてのデータが完全に削除されます。ファイルがファイルシステム領域を過度に消費している場合、データベースを指定することができます。

（注） リセットオプションを使用すると、Cisco ISE サービスが一時的に利用できなくなります。

[運用データの消去（Operational Data Purging）] ウィンドウには、[データベース使用率（Database Utilization）] および [データを今すぐ消去（Purge Data Now）] 領域があります。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [運用データの消去（Operational Data Purging）]** です。[データベースの使用状況（Database Utilization）] 領域には、使用可能なデータベース容量の合計と、保存されている RADIUS および TACACS データが表示されます。ステータスバーをマウスオーバーすると、利用可能なディスク容量と、データベースに既存データが保存されている日数が表示されます。RADIUS データと TACACS データを保持できる期間を [データ保存期間（Data Retention Period）] 領域に指定します。データは毎朝午前 4 時に消去されます。また、保存日数を指定して、消去前にデータをリポジトリにエクスポートするように設定できます。[リポジトリのエクスポートを有効にする（Enable Export Repository）] チェックボックスをオンにし、リポジトリを選択して作成し、[暗号キー（Encryption Key）] を指定します。

[データを今すぐ消去（Purge Data Now）] 領域では、すべての RADIUS および TACACS データを消去するか、またはデータ消去までに保存できる日数を指定できます。

（注） 消去前にリポジトリにエクスポートできるテーブルは、RADIUS 認証およびアカウンティング、TACACS 認証およびアカウンティング、RADIUS エラー、および設定が誤っているサプリカントの各テーブルです。

関連トピック

古い運用データの消去 （462 ページ）

古い運用データの消去

運用データはサーバーに一定期間集められています。すぐに削除することも、定期的に削除することもできます。[データ消去の監査（Data Purging Audit）] レポートを表示して、データ消去が成功したかどうかを確認できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [運用データの消去（Operational Data Purging）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [データ保持期間（Data Retention Period ）] 領域で次の操作を行います。

1. RADIUS または TACACS データを保持する期間を日単位で指定します。指定した期間より前のデータはすべてリポジトリにエクスポートされます。

2. [リポジトリ（Repository）] 領域で、[リポジトリのエクスポートを有効にする（Enable Export Repository）] チェックボックスをオンにし、データを保存するリポジトリを選択します。
3. [暗号キー（Encryption Key）] フィールドに必要なパスワードを入力します。
4. [保存（Save）] をクリックします。

（注） 設定した保持期間が診断データに対応する既存の保持しきい値未満の場合、設定値は既存のしきい値を上書きします。たとえば、保持期間を 3 日に設定し、この値が診断テーブルの既存のしきい値（たとえば、デフォルトの 5 日）未満の場合、データはこのウィンドウで設定した値（3 日）に従って消去されます。

- [データを今すぐ消去（Purge Data Now）] 領域で、次の操作を行います。

1. すべてのデータを消去するか、または指定された日数よりも古いデータを消去します。データはリポジトリに保存されません。
2. [除去（Purge）] をクリックします。

自動フェールオーバー用の MnT ノードの設定

展開に 2 つの MnT ノードがある場合は、自動フェールオーバーのプライマリ-セカンダリペアを設定して、Cisco ISE モニタリングサービスのダウンタイムを回避します。プライマリ-セカンダリペアによって、プライマリノードに障害が発生した場合に、セカンダリ MnT ノードが確実に自動的にモニタリングを始めるようにします。

始める前に

- 自動フェールオーバー用の MnT ノードを設定するには、MnT ノードが Cisco ISE ノードとして登録されている必要があります。
- 両方のノードでモニタリングロールおよびサービスを設定し、必要に応じてこれらのノードにプライマリロールおよびセカンダリロールの名前を付けます。
- プライマリ MnT ノードとセカンダリ MnT ノードの両方でバックアップとデータ消去用のリポジトリを設定します。バックアップおよび消去を正しく動作させるには、両方のノードに同じリポジトリを使用します。消去は、冗長ペアのプライマリ ノードおよびセカンダリ ノードの両方で行われます。たとえば、プライマリ MnT ノードでバックアップおよび消去に 2 つのリポジトリが使用されている場合、セカンダリノードに同じリポジトリを指定する必要があります。

  システム CLI の **repository** コマンドを使用して MnT ノードのデータリポジトリを設定します。

（注） スケジュールバックアップと消去をモニタリング冗長ペアのノードで正しく動作させるには、CLI を使用して、プライマリノードとセカンダリノードの両方で同じリポジトリを設定します。リポジトリは、2 つのノードの間で自動的に同期されません。

Cisco ISE ダッシュボードで、MnT ノードの準備ができていることを確認します。[システム概要（System Summary）] ダッシュレットに、サービスが準備完了の場合は左側に緑色のチェックマークが付いた MnT ノードが表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。

ステップ 2 [展開ノード（Deployment Nodes）] ウィンドウで、プライマリとして指定する MnT ノードの横にあるチェックボックスをオンにし、**Edit** をクリックします。

ステップ 3 [全般設定（General Settings）] タブをクリックし、[ロール（Role）] ドロップダウン リストから [プライマリ（Primary）] を選択します。

MnT ノードをプライマリとして選択すると、他の MnT ノードが自動的にセカンダリになります。スタンドアロン展開の場合、プライマリおよびセカンダリのロール設定は無効になります。

ステップ 4 **Save** をクリックします。プライマリノードとセカンダリノードの両方が再起動します。

Cisco pxGridノード

Cisco pxGrid を使用すると、Cisco ISE セッションディレクトリからの状況依存情報を、Cisco ISE エコシステムのパートナーシステムなどの余暇のネットワークシステムやシスコの他のプラットフォームと共有できます。pxGrid フレームワークは、Cisco ISE とサードパーティのベンダー間でのタグやポリシーオブジェクトの共有のように、ノード間でのポリシーおよび設定データの交換に使用できます。また、その他の情報交換にも使用できます。また、Cisco pxGrid では、サードパーティ製のシステムが適応型のネットワーク制御アクション（ANC）を呼び出すことができるため、ネットワークまたはセキュリティイベントに応じてユーザーまたはデバイス（またはその両方）を隔離できます。タグ定義、値、および説明などの Cisco TrustSec 情報は、Cisco TrustSec のトピックを通して Cisco ISE から他のネットワークに渡すことができます。完全修飾名（FQN）を持つエンドポイントプロファイルは、エンドポイントプロファイルメタ トピックを通じて Cisco ISE から他のネットワークに渡すことができます。Cisco pxGrid は、タグおよびエンドポイント プロファイルの一括ダウンロードもサポートしています。

Cisco pxGrid 経由で SXP バインディング（IP-SGT マッピング）を公開および登録できます。SXP バインディングの詳細については、セキュリティ グループ タグの交換プロトコル （1656 ページ）を参照してください。

Cisco pxGrid ノードでは、次のログを使用できます。

- pxgrid.log：状態変更を通知します。

- pxgrid-cm.log：パブリッシャまたはサブスクライバ、あるいはその両方、およびクライアントとサーバー間でのデータ交換アクティビティの更新について表示します。
- pxgrid-controller.log：クライアント機能、グループ、およびクライアント許可の詳細を表示します。
- pxgrid-jabberd.log：システムの状態と認証に関連するすべてのログを表示します。
- pxgrid-pubsub.log：パブリッシャとサブスクライバのイベントに関するすべての情報を表示します。

（注）
- Cisco pxGrid と Cisco pxGrid ペルソナは、Cisco ISE Advantage ライセンスで有効にできます。
- パッシブ ID ワークセンターで使用するには Cisco pxGrid を定義する必要があります。詳細については、PassiveID ワーク センター （1083 ページ）を参照してください。

pxGrid 2.0 のハイアベイラビリティ

pxGrid 2.0 ノードはアクティブ/アクティブ構成で動作します。ハイアベイラビリティを実現するには、導入環境に少なくとも 2 つの pxGrid ノードが必要です。大規模な導入では、拡張性と冗長性を高めるために最大4つのノードを使用できます。あるノードがダウンした場合に、そのノードのクライアントが動作中のノードに接続できるように、すべてのノードの IP アドレスを設定することを推奨します。PAN がダウンすると、pxGrid サーバーは、アクティブ化処理を停止します。pxGrid サーバーをアクティブにするには、PAN を手動で昇格させます。pxgrid-cm.log 展開に関する詳細については、『**Performance and Scalability Guide for Cisco Identity Services Engine**』を参照してください。

すべての pxGrid サービスプロバイダーのクライアントは、7.5 分以内に pxGrid コントローラに定期的に再登録します。クライアントが再登録しない場合、PAN ノードはそのクライアントが非アクティブであると見なし、削除します。PAN ノードが 7.5 分を超えてダウンした場合、再度起動すると、タイムスタンプ値が 7.5 分よりも古いすべてのクライアントが削除されます。これらのクライアントはすべて、pxGrid コントローラに再度登録する必要があります。

pxGrid 2.0 クライアントでは、PubSub やクエリに WebSocket および REST ベースの API を使用しています。これらの API は、ポート 8910 で ISE アプリケーションサーバーによって提供されます。`show logging application pxgrid` を実行して表示される pxGrid プロセスは、pxGrid 2.0 には適用されません。

（注）GUI および CLI で pxGrid 1.0 プロセスへのすべての参照が削除されました。

Cisco pxGrid ノードの展開

スタンドアロン ノードと分散展開ノードの両方で、Cisco pxGrid ペルソナを有効にできます。

始める前に

- Cisco pxGrid ペルソナを有効にするには、Cisco ISE Advantage ライセンスが必要です。ライセンス要件については、『ISE Licensing / Ordering』を参照してください。
- すべてのノードは、Cisco pxGrid サービス用に CA 証明書を使用します。アップグレード前に Cisco pxGrid サービスにデフォルトの証明書を使用した場合、アップグレードによってその証明書が内部 CA 証明書に置き換えられます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。

ステップ 2 [展開ノード（Deployment Nodes）] ウィンドウで、Cisco pxGrid サービスを有効にするノードの横にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 [全般設定（General Settings）] タブをクリックし、[pxGrid] トグルボタンを有効にします。[pxGrid] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

（注） 以前のバージョンからアップグレードすると、[保存（Save）] オプションが無効になることがあります。このことは、ブラウザのキャッシュが旧バージョンの Cisco ISE の古いファイルを参照する場合に発生します。[保存（Save）] オプションを有効にするには、ブラウザのキャッシュを消去します。

Cisco pxGrid の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）]**。

ステップ 2 要件に基づき、次のいずれかのチェックボックスをオンにします。

- [新しいアカウントの自動承認（Automatically Approve New Accounts）]：このチェックボックスをオンにすると、新しい Cisco pxGrid クライアントからの接続要求が自動的に承認されます。
- [パスワードベースのアカウント作成の許可（Allow password--based account creation）]：このチェックボックスをオンにすると、Cisco pxGrid クライアントのユーザー名またはパスワードベースの認証が有

効になります。このオプションを有効にした場合、Cisco pxGrid クライアントを自動的に承認することはできません。

ステップ 3 [保存（Save）] をクリックします。

Cisco pxGrid の [設定（Settings）] ウィンドウで [テスト（Test）] オプションを使用して、Cisco pxGrid ノードでヘルスチェックを実行します。pxgrid ファイルまたは pxgrid-test.log ファイルの詳細を表示します。

pxGrid クライアント自動承認 API を使用して、次のことができます。

- 新しい pxGrid クライアントからの証明書ベースの接続要求の自動承認を有効にします。環境内のすべてのクライアントを信頼している場合にのみ、このオプションを有効にします。
- pxGrid クライアントのユーザー名またはパスワードベースの認証を有効にします。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。pxGrid クライアントは、REST API を介してユーザー名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

pxGrid クライアント自動承認 API の詳細については、ERS SDK の「pxGrid Settings」のセクションを参照してください。次の URL で ERS SDK にアクセスできます。

https://<ISE-Admin-Node>:9060/ers/sdk

[ERS管理者（ERS Admin）] のロールを持つユーザーのみが、ERS SDK にアクセスできます。

Cisco pxGrid 証明書の生成

始める前に

- Cisco ISE pxGrid サーバーと pxGrid クライアントに同じ証明書を使用しないでください。pxGrid クライアントにはクライアント証明書を使用する必要があります。クライアント証明書を生成するには、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）]** を選択します。
- Cisco ISE の一部のバージョンには NetscapeCertType を使用する Cisco pxGrid の証明書があります。新しい証明書を生成することを推奨します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- pxGrid 証明書はプライマリ PAN から生成する必要があります。
- Cisco pxGrid 証明書がサブジェクト代替名（SAN）の拡張を使用する場合、DNS 名のエントリとしてサブジェクト ID の FQDN が含まれるようにします。
- デジタル署名を使用して証明書テンプレートを作成し、新しい Cisco pxGrid 証明書を生成します。

（注） FIPS モードが有効になっている場合、pxGrid 証明書テンプレートの RSA 秘密キーのサイズは 2048 ビット以上である必要があります。それ以外の場合、pxGrid 証明書を生成しようとするとエラーが表示されます。証明書テンプレートの秘密キーサイズを変更するには、pxGrid証明書テンプレートのキーサイズの変更（1941 ページ） を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [クライアント管理（Client Management）] > [証明書（Certificates）]**。

ステップ 2 [処理の選択（I want to）] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）]：このオプションを選択した場合は、共通名（CN）を入力する必要があります。
- [単一の証明書の生成（証明書署名要求あり）（Generate a single certificate (with a certificate signing request)）]：このオプションを選択した場合は、証明書署名要求の詳細を入力する必要があります。

ステップ 3 （オプション）この証明書の説明を入力します。

ステップ 4 [pxGrig_Certificate_Template] のリンクをクリックして証明書テンプレートをダウンロードし、必要に応じて編集します。

ステップ 5 [サブジェクト代替名（SAN）（Subject Alternative Name (SAN)）] を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- [IPアドレス（IP address）]：この証明書に関連付ける Cisco pxGrid クライアントの IP アドレスを入力します。
- [FQDN]：pxGrid クライアントの FQDN を入力します。

ステップ 6 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウンリストから、以下のいずれかのオプションを選択します。

- [Private Enhanced Electronic Mail（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）（Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)）]：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY----」タグで終わります。
- [PKCS12形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で1ファイル）（PKCS12 format (including certificate chain; one file for both the certificate chain and key)）]：1 つの暗号化ファイルに

ルート CA 証明書、中間 CA 証明書、およびエンドエンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成（Create）] をクリックします。

作成した証明書は、[発行された証明書（Issued Certificates）] ウィンドウに表示されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[発行された証明書（Issued Certificates）]**。

（注） Cisco ISE 2.4 パッチ 13 以降、pxGrid サービスの証明書要件がより厳格になりました。pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、Cisco ISE 2.4 パッチ 13 以降の適用後に証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の以前のバージョンに、**SSL サーバー**として指定された **Netscape Cert Type** 拡張があるためです。これは現在は失敗するようになっています（現在はクライアント証明書も必要）。

非準拠の証明書を持つクライアントは、Cisco ISE と統合できません。内部 CA によって発行された証明書を使用するか、適切な使用拡張で新しい証明書を生成します。

- 証明書の [キーの使用方法（Key Usage）] の拡張には、[デジタル署名（Digital Signature）] フィールドと [キー暗号化（Key Encipherment）] フィールドが含まれている必要があります。
- 証明書の [拡張キーの使用方法（Extended Key Usage）] の拡張には、[クライアント承認（Client Authentication）] フィールドと [サーバー承認（Server Authentication）] フィールドが含まれている必要があります。
- 証明書に [Netscape証明書タイプ（Nestscape Certificate Type）] の拡張は必要ありません。その拡張を含める場合は、[SSLクライアント（SSL Client）] と [SSLサーバー（SSL Server）] の両方を拡張に追加します。
- 自己署名証明書を使用している場合は、[基本制約CA（Basic Constraints CA）] フィールドを **TRUE** にし、[キーの使用方法（Key Usage）] の拡張に [キー証明書署名（Key Cert Sign）] フィールドを含める必要があります。

Cisco pxGrid クライアントの権限の制御

Cisco pxGrid クライアントの権限を制御するために、pxGrid 許可ルールを作成できます。これらのルールを使用して、Cisco pxGrid クライアントに提供されるサービスを制御します。

さまざまな種類のグループを作成し、Cisco pxGrid クライアントに提供されるサービスをこれらのグループにマッピングできます。[クライアント管理（Client Management）] ウィンドウの [グループ（Groups）] オプションを使用して、新しいグループを追加します。[クライアント管理（Client Management）] > [ポリシー（Policies）] ウィンドウで、許可ルールの例を表示できます。事前に定義されたルールで更新できるのは [カスタム操作（Custom Operations）] フィールドのみであることに注意してください。

pxGrid クライアントの許可ルールを作成するには、以下の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント管理（Client Management）] > [ポリシー（Policy）]**。

ステップ 2 [サービス（Service）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

ステップ 3 [操作（Operations）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **<ANY>**
- **publish**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**：このオプションを選択すると、カスタム操作を指定できます。

詳細については、「pxGrid の操作とサービスのユースケース」を参照してください。

（注） 次の追加属性は、Cisco ISE 3.0 パッチ 5 以降のリリースの REST ID ストアの /topic/com.cisco.ise.session に公開されます。

- identityProvider:Azure
- oid
- tenantID
- preferredUsername

ステップ 4 [グループ（Groups）] ドロップダウン リストから、このサービスにマッピングするグループを選択します。

ANC、および手動で追加したグループがこのドロップダウンリストに表示されます。

（注） ポリシーに含まれるグループに属するクライアントのみが、そのポリシーで指定されたサービスに登録できます。たとえば、com.cisco.ise.pubsub サービスの pxGrid ポリシーを定義し、このポリシーに ANC グループを割り当てた場合、ANC グループに属するクライアントのみが com.cisco.ise.pubsub サービスに登録できます。

pxGrid の操作とサービスのユースケース

新しい pxGrid ポリシーを作成する場合、一部の pxGrid 操作は特定のサービスにのみ適用されることに注意してください。

Cisco ISE GUI には、次の pxGrid 操作があります。

<すべて>の操作（Operation <ANY>）

サービスおよび特定のユーザーグループで <すべて> の操作を使用する場合、そのサービスに関連する操作には、選択したユーザーグループのユーザーのみがアクセスできます。

次の例について考えます。

サービス：com.cisco.ise.session、操作：<すべて>、グループ：SessionUsers。

この例では、‘SessionUsers’ グループの一部である pxGrid クライアントのみが、セッショントピックに関連する操作（登録/取得操作など）を実行できます。

パブリッシュ操作（Operation publish）

すべてのパブリッシュ関連の操作は、com.cisco.ise.pubsub がサービスとして選択されている場合にのみ適用されます。パブリッシュ操作を使用して、特定のユーザーグループの pxGrid クライアントのみが、選択したトピックまたはすべてのトピックをパブリッシュできることを指定する pxGrid ポリシーを作成できます。

<カスタム>操作（Operation <Custom>）

<カスタム> 操作を使用して、[操作（Operation）] ドロップダウンリストに提供されていない操作を指定できます。現在、pxGrid では次の操作がサポートされていますが、すべての操作が [操作（Operation）] ドロップダウンリストに表示されているわけではありません。

1. 'sets'（pubsub を除くすべてのサービスとトピックに適用可能）：これを使用して、設定操作を実行する REST API コールへのアクセスを制限できます。
2. 'gets'（pubsub を除くすべてのサービスとトピックに適用可能）：これを使用して、取得操作を実行する REST API コールへのアクセスを制限できます。
3. 特定のトピック名が後ろに続く 'publish'（pubsub サービスにのみ適用可能）：これを使用して、特定のトピックをパブリッシュできるユーザーにアクセスを制限できます。

たとえば、サービス：com.cisco.ise.pubsub、操作：publish/topic/com.cisco.ise.session などです。

ただし、同じ操作、サービス、およびトピックを持つ一部のルールは理解されないため、使用しないようにする必要があります。たとえば、サービス：com.cisco.ise.session、操作：publish /topic/com.cisco.ise.session などです。

4. トピック名が後ろに続く 'subscribe'（pubsub サービスにのみ適用可能）：これを使用して、特定のトピックに登録できるユーザーにアクセスを制限できます。

   たとえば、サービス：com.cisco.ise.pubsub、操作：publish /topic/com.cisco.ise.session などです。

展開内のノードの表示

[展開ノード（Deployment Nodes）] ウィンドウで、展開を構成するプライマリとセカンダリのすべての Cisco ISE ノードを表示できます。

ステップ 1 プライマリ Cisco ISE 管理者ポータルにログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** の順に選択します。

ステップ 3 左側のナビゲーションウィンドウで、[展開（Deployment）] をクリックします。

展開を構成するすべての Cisco ISE ノードが表示されます。

MnT ノードからのエンドポイント統計データのダウンロード

MnT ノードからネットワークに接続するエンドポイントの統計データをダウンロードできます。ロード、CPU 使用率、認証トラフィックデータを含む主要評価指標（KPM）が使用可能です。このデータをネットワークの問題のモニターおよびトラブルシュートに使用できます。日次 KPM 統計または過去 8 週間の KPM 統計をダウンロードするには、Cisco ISE（CLI）から、**application configure ise** コマンドを実行し、オプション 12 またはオプション 13 を選択します。

このコマンドの出力では、エンドポイントに関する次のデータが提供されます。

- ネットワーク上のエンドポイントの総数
- 正常な接続を確立したエンドポイントの数
- 認証に失敗したエンドポイントの数

- 毎日の接続済みの新しいエンドポイントの総数
- 毎日のオンボーディングしたエンドポイントの総数

出力には、タイムスタンプの詳細、展開内の各ポリシーサービスノード（PSN）を介して接続したエンドポイントの総数、エンドポイントの総数、アクティブエンドポイント、負荷、および認証トラフィックの詳細も含まれています。

このコマンドの詳細については、『Cisco Identity Services Engine CLI リファレンスガイド』を参照してください。

データベースのクラッシュまたはファイルの破損の問題

Cisco ISE は、データ損失を引き起こす停電またはその他の理由により Oracle データベースファイルが破損している場合、クラッシュすることがあります。インシデントに応じて、データ損失から回復するには、次の手順を実行します。

- 展開で PAN が破損した場合は、セカンダリ PAN をプライマリ PAN に昇格する必要があります。展開が小規模である、またはその他の理由により、セカンダリ PAN を昇格できない場合は、『Cisco Identity Services Engine CLI Reference Guide』の説明に従って、利用可能な最新のバックアップを復元します。
- PSN が破損している場合は、『Cisco Identity Services Engine CLI Reference Guide』の説明に従って、登録解除、設定のリセット、および登録を行います。
- スタンドアロンデバイスの場合は、『Cisco Identity Services Engine CLI Reference Guide』の説明に従って、利用可能な最新のバックアップを復元します。

（注） 最新の構成変更が失われないようにするために、スタンドアロンデバイスからバックアップを定期的に取得します。

モニタリングのためのデバイス設定

MnT ノードは、ネットワーク上のデバイスからのデータを受信し、使用して、ダッシュボードに表示されます。MnT ノードとネットワークデバイス間の通信を有効にするには、スイッチと NAD を正しく設定する必要があります。

プライマリおよびセカンダリの Cisco ISE ノードの同期

Cisco ISE の構成に変更を加えることができるのは、プライマリ PAN からのみです。設定変更はすべてのセカンダリ ノードに複製されます。何らかの理由でこの複製が正しく実行されない場合は、プライマリ PAN に手動でセカンダリ PAN を同期できます。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 3 プライマリ PAN と同期させるノードの横にあるチェックボックスをオンにし、[同期を更新（Syncup）] をクリックして完全データベース複製を強制的に実行します。

ノード ペルソナとサービスの変更

（注） PSN で実行されるサービスを有効または無効にしたり、PSN を変更したりする場合は、そのサービスが実行されるアプリケーション サーバー プロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。このサービスの再起動の遅延により、展開内で有効になっている場合、自動フェールオーバーが開始される場合があります。これを回避するには、自動フェールオーバー構成がオフになっていることを確認します。

Cisco ISE ノードの設定を編集して、そのノードで実行されているペルソナおよびサービスを変更できます。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。

ステップ 3 ペルソナまたはサービスを変更するノードの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 4 変更したいペルソナおよびサービスを選択します。

ステップ 5 [Save（保存）] をクリックします。

ステップ 6 プライマリ PAN でアラームの受信を確認して、ペルソナまたはサービスの変更を確認します。ペルソナまたはサービスの変更が正常に保存されなかった場合、アラームは生成されません。

Cisco ISE でのノードの変更による影響

Cisco ISE で次のいずれかの変更を行うと、そのノードが再起動するため、遅延が発生します。

- ノードの登録（スタンドアロンからセカンダリへ）
- ノードの登録解除（セカンダリからスタンドアロンへ）

- プライマリ ノードからスタンドアロンへの変更（他のノードが登録されていない場合は、プライマリからスタンドアロンに変更されます）
- 管理ノードの昇格（セカンダリからプライマリへ）
- ペルソナの変更（ノードからポリシーサービスまたは監視ペルソナを割り当てたり、削除したりする場合）
- ポリシー サービス ノードでのサービスの変更（セッションとプロファイラ サービスを有効または無効にします）
- プライマリでのバックアップの復元（同期操作がトリガーされ、プライマリ ノードからセカンダリ ノードにデータが複製されます）

（注） セカンダリ管理ノードをプライマリ PAN の位置に昇格させると、プライマリノードがセカンダリロールになります。これにより、プライマリノードとセカンダリノードの両方が再起動し、遅延が発生します。

ポリシー サービス ノード グループの作成

2つ以上のポリシーサービス ノード（PSN）が同じ高速ローカルエリア ネットワーク（LAN）に接続されている場合は、同じノードグループに配置することを推奨します。この設計は、グループにローカルの重要度が低い属性を保持し、ネットワークのリモートノードに複製される情報を減らすことによって、エンドポイント プロファイリング データのレプリケーションを最適化します。ノード グループ メンバーは、ピア グループ メンバーの可用性もチェックします。グループがメンバーに障害が発生したことを検出すると、障害が発生したノードの URL にリダイレクトされたすべてのセッションをリセットし、回復することを試行します。

ノードグループは、URL リダイレクト（ポスチャサービス、ゲストサービス、およびMDM）が適用されるセッションの PSN フェールオーバーに使用されます。

（注） すべての PSN を同じノードグループの一部として同じローカルネットワークに置くことを推奨します。PSNは、負荷分散クラスタの一部でなければ同じノードグループに参加できないわけではありません。ただし、負荷分散クラスタの各ローカル PSN は通常同じノードグループに属している必要があります。

ノード グループ メンバーは TCP/7800 を使用して通信できます。

ノードグループにメンバーとして PSN を追加する前に、ノードグループを作成する必要があります。管理者ポータルの [展開（Deployment）] ウィンドウで、PSN グループを作成、編集、および削除できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 2 左側のナビゲーションウィンドウの上部にある [設定（Settings）] アイコンをクリックします。

ステップ 3 [ノードグループの作成（Create Node Group）] をクリックします。

ステップ 4 ノードグループに付ける一意の名前を入力します。

（注） ノード登録中に問題が発生する可能性があるため、**None** という名前でノードグループを設定しないことをお勧めします。

ステップ 5 （任意）ノードグループの説明を入力します。

ステップ 6 （任意）[MAR キャッシュ分散の有効化（Enable MAR Cache Distribution）] チェックボックスをオンにし、その他のオプションを入力します。このチェックボックスをオンにする前に、[Active Directory] ウィンドウで MAR が有効になっていることを確認します。

ステップ 7 [送信（Submit）] をクリックして、ノードグループを保存します。

ノードグループを保存すると、左側のナビゲーションウィンドウにそのグループが表示されます。左側のペインにノードグループが表示されていない場合、そのグループは非表示になっている可能性があります。非表示オブジェクトを表示するには、ナビゲーションペインで [展開（Expand）] ボタンをクリックします。

ノードグループにノードを追加するか、またはノードを編集するには、[ポリシーサービス（Policy Service）] 領域の [ノードをノードグループに含める（Include node in node group）] ドロップダウンリストからノードグループを選択します。

展開からのノードの削除

展開からノードを削除するには、ノードの登録を解除する必要があります。登録解除されたノードは、スタンドアロン Cisco ISE ノードになります。

これはプライマリ PAN から受信した最後の設定を保持し、管理、ポリシーサービス、またはモニタリングであるスタンドアロンノードのデフォルトのペルソナを担当します。MnT ノードを登録解除した場合、このノードは syslog ターゲットではなくなります。

プライマリ PSN の登録が取り消されると、エンドポイント データは失われます。スタンドアロンノードになった後も PSN にエンドポイント データを残すには、以下のいずれかを実行します。

- プライマリ PAN からバックアップを取得し、PSN がスタンドアロンノードになったときに、このデータバックアップを復元します。
- PSN のペルソナを管理者（セカンダリ PAN）に変更し、管理者ポートルの [展開（Deployment）] ウィンドウからデータを同期してから、ノードを登録解除します。この

時点で、このノードに、すべてのデータがあります。この後、既存の展開にセカンダリ PAN を追加できます。

プライマリ PAN の [展開（Deployment）] ウィンドウからこれらの変更を表示できます。ただし、変更が反映され、[展開（Deployment）] ウィンドウに表示されるには 5 分間の遅延が生じます。

始める前に

展開からセカンダリノードを削除する前に、必要に応じて後で復元できるように Cisco ISE 設定のバックアップを実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 2 削除するセカンダリノードの隣のチェックボックスをオンにして、[登録解除（Deregister）] をクリックします。

ステップ 3 [OK] をクリックします。

ステップ 4 プライマリ PAN のアラームの受信を確認し、セカンダリノードの登録が正常に解除されたことを確認します。セカンダリノードのプライマリ PAN からの登録解除が失敗した場合は、このアラームは生成されないことになります。

Cisco ISE ノードのシャットダウン

Cisco ISE CLI から **halt** コマンドを実行する前に、Cisco ISE アプリケーションサービスを停止し、バックアップ、復元、インストール、アップグレード、または削除操作を実行中でないことを確認します。Cisco ISE がこれらのいずれかの操作を行っている間に **halt** コマンドを発行すると、次のいずれかの警告メッセージが表示されます。

```
WARNING: A backup or restore is currently in progress! Continue with halt?

WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

halt コマンドの使用時に他のプロセスが実行されていない場合、または表示される警告メッセージに応じて `Yes` と入力した場合は、次の質問に応答する必要があります。

```
Do you want to save the current configuration?
```

既存の Cisco ISE 構成を保存するために `Yes` と入力すると、次のメッセージが表示されます。

```
Saved the running configuration to startup successfully.
```

（注） アプライアンスを再起動する前に、アプリケーションプロセスを停止することをお勧めします。

また、Cisco ISE を再起動する前にも、アプリケーションプロセスを停止することをお勧めします。詳細については、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

ノードを再登録する必要があるシナリオ

次の表は、ノードが破損した場合にノードを再登録する必要があるシナリオの一部をまとめたものです。

シナリオ	必要な作業
プライマリ PAN 以外のノードのいずれかが破損している場合	1. 障害が発生したノードを展開から登録解除します。 2. 障害が発生したノードに Cisco ISE を再インストールします。 3. 既存の展開にノードを再登録します。 （注） 登録の前または後に、古い証明書をノードにインポートする必要があります。
プライマリ PAN が破損している場合	たとえば、N1（プライマリ PAN）と N2（セカンダリ PAN）の 2 つのノードがある場合は、次の操作を行います。 1. セカンダリ PAN（N2）をプライマリ PAN に昇格させます。 2. 障害が発生したノード（N1）を展開から削除します。 3. 障害が発生したノード（N1）に Cisco ISE を再インストールします。 4. 展開するセカンダリ PAN としてノード（N1）を登録します。 5. 登録が完了したら、古い証明書をノード（N1）にインポートします。 6. ノード（N1）をプライマリ PAN に再昇格させ、以前と同様の展開にします。

シナリオ	必要な作業
プライマリ PAN とセカンダリ PAN の両方が破損している場合	たとえば、N1（プライマリ PAN）と N2（セカンダリ PAN）の 2 つのノードがある場合は、次の操作を行います。 **1.** プライマリ PAN ノード（N1）とセカンダリ PAN ノード（N2）に Cisco ISE を再インストールします。 **2.** プライマリ PAN ノード（N1）で設定のバックアップを復元します。 **3.** プライマリ PAN ノード（N1）で古い証明書をインポートします。 **4.** 展開するセカンダリ PAN として他のノード（N2）を登録します。 **5.** 他のノードで reset-config を実行し、展開にノードを登録します。 **6.** すべてのノードに証明書をインポートします。 （注） プライマリ PAN とセカンダリ PAN が VM の場合、Cisco ISE を再インストールすると UDI が変更される可能性があるため、新しい UDI でライセンスを再インストールする必要があります。

スタンドアロン Cisco ISE ノードのホスト名または IP アドレスの変更

スタンドアロン Cisco ISE ノードのホスト名、IP アドレス、またはドメイン名を変更できます。ただし、ノードのホスト名として **localhost** を使用することはできません。

始める前に

Cisco ISE ノードが分散展開の一部である場合、展開から削除し、スタンドアロンノードであることを確認する必要があります。

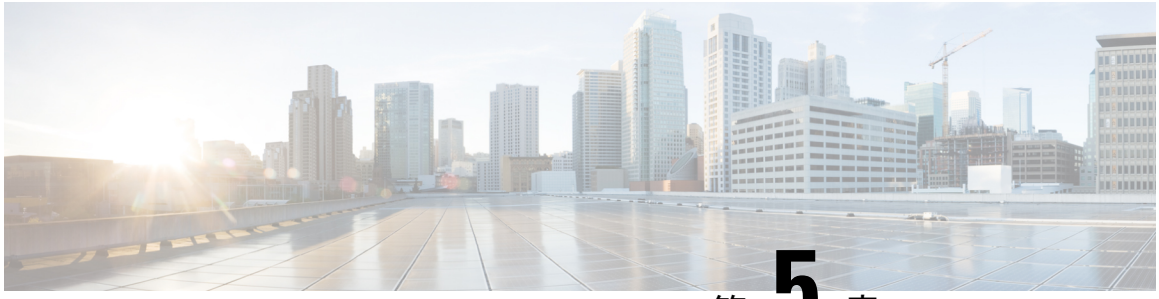
ステップ 1 Cisco ISE CLI から **hostname**、**ip address**、または **ip domain-name** の各コマンドを使用して Cisco ISE ノードのホスト名または IP アドレスを変更します。

ステップ 2 すべてのサービスを再起動するために、Cisco ISE CLI から **application stop ise** コマンドを使用して Cisco ISE アプリケーション設定をリセットします。

ステップ 3 Cisco ISE ノードは、分散 展開の一部である場合はプライマリ PAN に登録します。

（注） Cisco ISE ノードの登録時にホスト名を使用する場合、登録するスタンドアロンノードの完全修飾ドメイン名（FQDN）（たとえば、*abc.xyz.com*）は、プライマリ PAN から DNS を使用して解決できる必要があります。解決できない場合は、ノード登録が失敗します。DNS サーバーに、分散展開の一部である Cisco ISE ノードの IP アドレスと FQDN を入力する必要があります。

セカンダリノードとして Cisco ISE ノードを登録した後、プライマリ PAN は IP アドレス、ホスト名、またはドメイン名への変更を展開内の他の Cisco ISE ノードに複製します。



第 5 章

基本的なセットアップ

- 管理ポータル （482 ページ）
- Cisco ISE 国際化およびローカリゼーション （510 ページ）
- MAC アドレスの正規化 （517 ページ）
- Cisco ISE 展開のアップグレード （518 ページ）
- 管理者アクセス コンソール （519 ページ）
- Cisco ISE でのプロキシの設定 （520 ページ）
- 管理ポータルで使用されるポート （521 ページ）
- Cisco ISE アプリケーション プログラミング インターフェイス ゲートウェイの設定 （521 ページ）
- API サービスの有効化 （523 ページ）
- 外部 RESTful サービスソフトウェア開発キット （530 ページ）
- Data Connect （530 ページ）
- システム時刻とネットワーク タイム プロトコル サーバー設定の指定 （535 ページ）
- システムのタイムゾーンの変更 （536 ページ）
- 通知をサポートするための SMTP サーバーの設定 （537 ページ）
- セキュアなロック解除クライアントメカニズムの有効化 （538 ページ）
- 連邦情報処理標準モードのサポート （540 ページ）
- Diffie-Hellman アルゴリズムを使用したセキュアな SSH キー交換 （545 ページ）
- セキュア syslog 送信のための Cisco ISE の設定 （545 ページ）
- デフォルトのセキュア syslog コレクタ （551 ページ）
- オフライン メンテナンス （552 ページ）
- エンドポイント ログイン クレデンシャルの設定 （553 ページ）
- Cisco ISE でのホスト名の変更 （553 ページ）
- Cisco ISE での証明書の管理 （554 ページ）
- Cisco ISE CA サービス （611 ページ）
- OCSP サービス （652 ページ）
- 管理者のアクセス ポリシーの設定 （660 ページ）
- 管理者アクセスの設定 （661 ページ）

管理ポータル

図 *2 : Cisco ISE* 管理ポータル

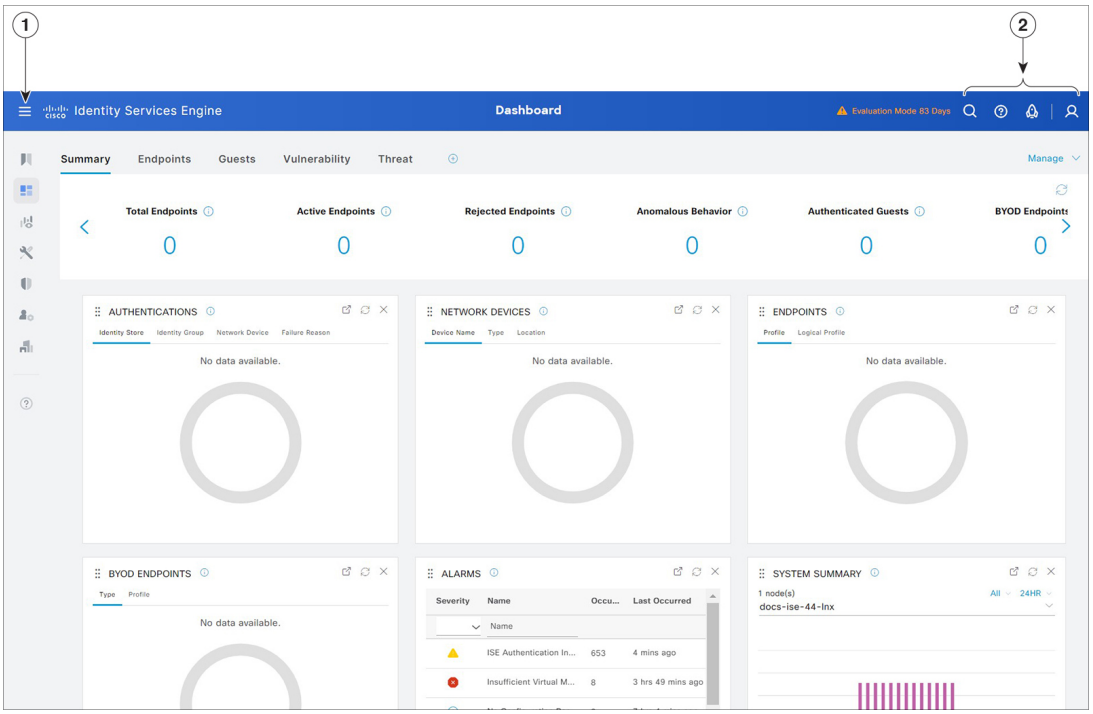
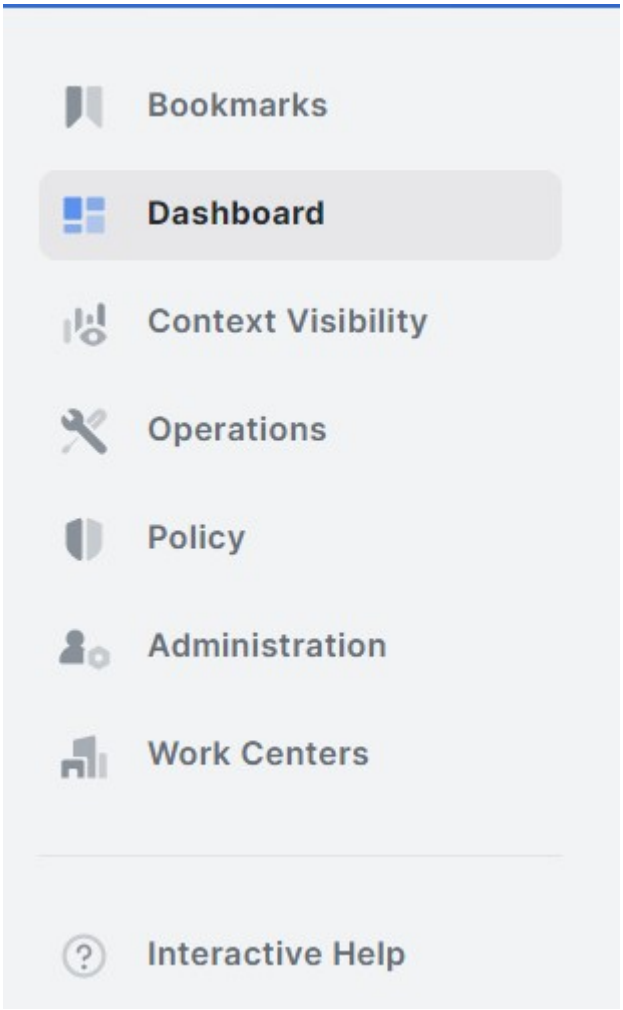


表 *18 : Cisco ISE* 管理ポータルのコンポーネント

1	メニューアイコン	

デフォルトでは、次のメニューオプションを含むペインがホームページの left サイドに表示されます。**メニュー**アイコン（☰）をクリックして left ペインを非表示にします。メニューオプションにカーソルを合わせると、サブメニューが表示されます。ホームページで [ダッシュボード（Dashboard）] をクリックします。

図 *3 : Cisco ISE* メインメニュー

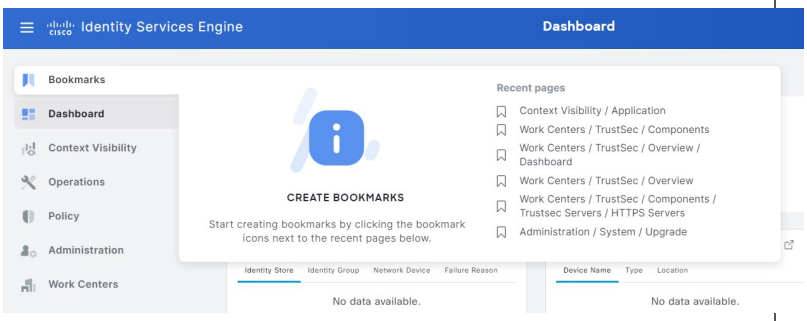


left ペインには、[ブックマーク（Bookmarks）] オプションもあります。それらのページをブックマークするには、最近表示した対応するページの横にある（🔖）アイコンをクリックします。最大 15 個のブックマークを保存できます。ブックマークの保存は、ブックマークされたのと同じ順序になります。

left ペインが表示されているときにログアウトし、再度ログインすると、ペインは引き続き表示されます。ただし、ペインが非表示になった後にログアウトし、再度ログインした場合、ペインを再度表示するには、メニューアイコンをクリックする必要があり

ます。

図 *4 : Cisco ISE* の *[*ブックマーク（*Bookmarks***）*]* タブ**



left ペインのメニューオプションは次のとおりです。

		• **[コンテキストの可視性（Context Visibility）]**：コンテキスト可視性ウィンドウには、エンドポイント、ユーザー、およびネットワーク アクセス デバイス（NAD）に関する情報が表示されます。コンテキスト可視性情報は、登録したライセンスに応じて、機能、アプリケーション、Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）、およびその他のカテゴリでグループ化されます。コンテキスト可視性ウィンドウは、中央データベースを使用し、データベース テーブル、キャッシュ、バッファから情報を収集します。その結果、コンテキスト可視性ダッシュレットとリストのコンテンツがすぐに更新されます。コンテキスト可視性ウィンドウは上部のダッシュレットおよび下部の情報のリストから構成されます。リストのカラム属性を変更することによってデータをフィルタすると、変更したコンテンツを表示するためにダッシュレットが更新されます。
		• **[操作（Operations）]**：[操作（Operations）] ウィンドウには、RADIUS、TACACS+、および TC-NAC ライブログ、適応型ネットワーク制御（ANC）ポリシー、および Cisco ISE 展開に関連する問題を診断およびデバッグするためのトラブルシューティング オプションを表示するためのツールが含まれています。
		• **[ポリシー（Policy）]**：ポリシーウィンドウには、認証、許可、プロファイリング、ポスチャ、クライアントプロビジョニングの領域でネットワークセキュリティを管理するためのツールが含まれています。
		• **[管理（Administration）]**：管理ウィンドウには、Cisco ISE ノード、ライセンス、証明書、ネットワークデバイス、ユーザー、エンドポイント、およびゲストサービスを管理するためのツールが含まれています。
		• **[ワークセンター（Work Centers）]**：[ワークセンター（Work Centers）] には、次の展開可能なサブメニューが表示されます。これらのサブメニューは、Cisco ISE 管理者が Cisco ISE 展開内の関連機能を設定するための単一の出発点として機能します。
		  • **ネットワークアクセス**
		  • **ゲストアクセス**
		  • **TrustSec**
		  • **BYOD**
		  • **プロファイラ**
		  • **ポスチャ**

		• デバイス管理 • **PassiveID**

2	右上のメニューアイコン	

- 

  このアイコンを使用してエンドポイントを検索し、プロファイル、障害、ID ストア、ロケーション、デバイスタイプ別にそれらの分布を表示します。このオプションを使用して、新しいページを検索したり、最近検索したページにアクセスしたりすることもできます。

- 

  アイコンをクリックすると、複数のリソースへのアクセスを提供する [対話型ヘルプ（Interactive Help）] メニューが表示されます。

- 

  このアイコンをクリックすると、次のオプションにアクセスできます。

  - [PassiveIDセットアップ（PassiveID Setup）]：[PassiveIDセットアップ（PassiveID Setup）] オプションでは、Active Directory を使用してパッシブ ID をセットアップする [PassiveIDセットアップ（PassiveID Setup）] ウィザードが起動されます。外部認証サーバーからユーザー ID と IP アドレスを収集し、認証済み IP アドレスを対応するサブスクライバに配信するように、サーバーを設定します。

  - [可視性セットアップ（Visibility Setup）]：[可視性セットアップ（Visibility Setup）] は、アプリケーション、ハードウェアインベントリ、USB ステータス、ファイアウォールステータス、Windows エンドポイントの全般的なコンプライアンスステータスなどのエンドポイントデータを収集する、価値の実証（PoV）サービスです。収集されたデータは、Cisco ISE に送信されます。[ISE 可視性セットアップ（ISE Visibility Setup）] ウィザードを起動すると、IP アドレスの範囲を指定して、ネットワークの特定セグメントまたはエンドポイントグループに対してエンドポイント検出を実行できます。

    PoV サービスは Cisco Stealth Temporal エージェントを使用して、エンドポイントポスチャデータを収集します。Cisco ISE は、管理者アカウントタイプで Windows を実行しているコンピュータに Cisco Stealth Temporal エージェントをプッシュし、一時的な実行ファイルを自動実行してコンテキストを収集します。その後、エージェントが自動的に削除します。Cisco Stealth Temporal エージェントのオプションデバッグ機能を使用するには、

		[エンドポイントロギング（Endpoint Logging）] チェックボックス（[メニュー（Menu）] アイコン（☰）をクリックして、**[可視性セットアップ（Visibility Setup）]** > **[ポスチャ（Posture）]** を選択）をチェックして、1つまたは複数のエンドポイントにデバッグログを保存します。ログは、次のいずれかの場所で参照できます。 • C:\WINDOWS\syswow64\config\systemprofile\（64ビット オペレーティング システム） • C:\WINDOWS\system32\config\systemprofile\（32ビット オペレーティング システム） • [エンドポイントスクリプトの実行（Run Endpoint Scripts）]：接続されたエンドポイントでスクリプトを実行して、組織の要件に準拠する管理タスクを実行するには、このオプションを選択します。これには、使用されていないソフトウェアのアンインストール、プロセスやアプリケーションの開始または終了、特定のサービスの有効化または無効化などのタスクが含まれます。 •  このアイコンをクリックすると、オンラインヘルプの起動やアカウント設定の構成など、システムアクティビティのメニューが表示されます。

インタラクティブヘルプ

インタラクティブヘルプを使用すると、簡単にタスクを完了するためのヒントとステップバイステップのガイダンスが提供され、ユーザーはCisco ISEで効果的に作業することができます。

この機能はデフォルトで無効になっています。この機能を無効にするには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[インタラクティブ機能（Interactive Features）]** を選択します。次に、[インタラクティブヘルプの有効化（Enable Interactive Help）] チェックボックスをオフにします。

[表示（Show）] ボタンをクリックして、[インタラクティブヘルプ（Interactive Help）] メニューを表示します。

Google Chrome シークレットウィンドウからCisco ISE管理者ポータルにアクセスする場合、インタラクティブヘルプを表示してアクセスするには、サードパーティの Cookie を有効にする必要があります。「Third-party cookie controls in Incognito mode」を参照してください。

カスタマー エクスペリエンス アンケート

Cisco ISE では管理ポータル内でユーザーに顧客満足度アンケートが提示されます。顧客満足度を定期的に評価することで、シスコではお客様の Cisco ISE のエクスペリエンスをより深く理解し、何が良好に機能しているかを追跡し、改善すべき領域を特定することができます。Cisco ISE 管理ポータルにログインすると、ダイアログボックスにアンケートが表示されます。アンケートを送信すると、その後 90 日間は別のアンケートは表示されません。

Cisco ISE アンケート機能は、すべての Cisco ISE 展開およびすべてのユーザーに対してデフォルトで有効になっています。この機能の設定は、管理ポータルの **[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[インタラクティブ機能（Interactive Features）]** ページの [ISEアンケート（ISE Surveys）] 領域にあります。この機能を使用するには、*.qualtrics.com の URL にアクセスする必要があります。

Cisco ISE ユーザーは、次の手順を実行してアンケート機能を無効にすることができます。

1. Cisco ISE 管理ポータルの右上隅にあるプロファイルアイコンをクリックします。
2. [アカウント設定（Account Settings）] をクリックします。
3. [Cisco ISEの改善に役立つ顧客体験調査にご参加ください（Take customer experience surveys to help improve Cisco ISE）] チェックボックスをオフにします。

ユーザーまたは Cisco ISE 展開に対して Cisco ISE アンケート機能を無効にすると、この機能は再度有効にするまで無効のままになります。

デフォルトモードまたはダークモードの適用

Cisco ISE をデフォルト（ライト）モードまたはダークモードで表示できるようになりました。Cisco ISE の管理者ポータルにログインした後、次の手順を実行します。

ステップ 1 右上隅にあるアイコンをクリックします。

ステップ 2 [アカウント設定（Account Settings）] をクリックします。

ステップ 3 [テーマ（Theme）] 領域で、[デフォルトモード（Default Mode）] または [ダークモード（Dark Mode）] のオプションボタンをクリックします。

ステップ 4 [保存（Save）] をクリックします。

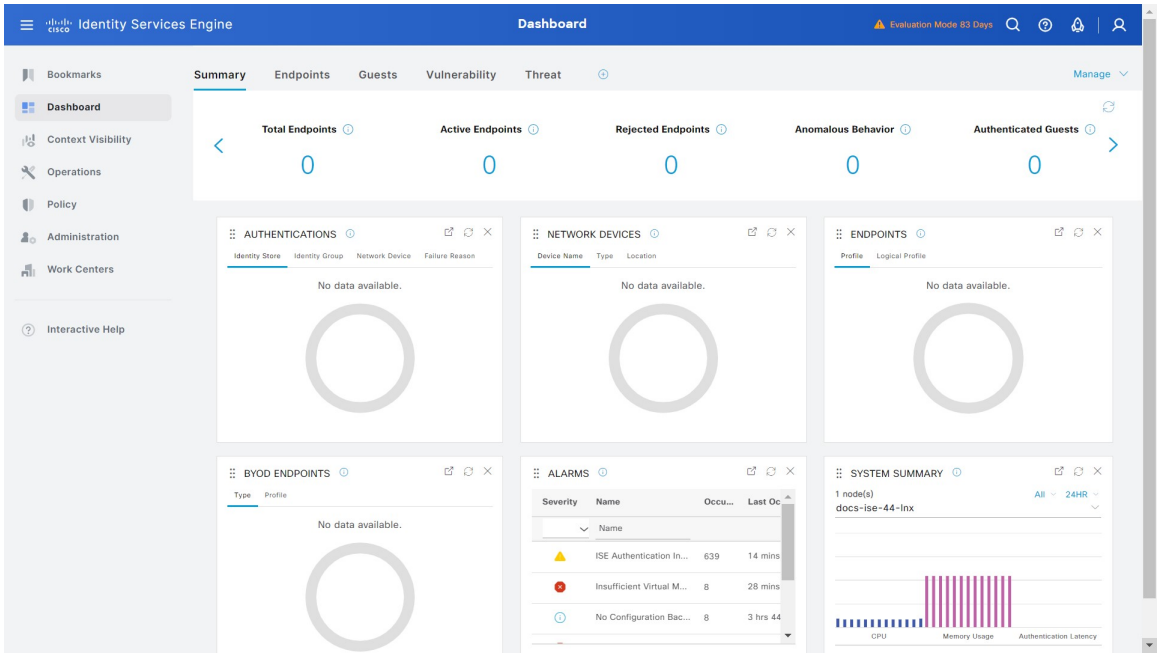
Cisco ISE は、選択した表示モードをブラウザストレージにキャッシュします。したがって、表示モードを保存するブラウザキャッシュが使用できない次のシナリオでは、Cisco ISE GUI が数秒間ライトモードで表示されます。

1. 別のブラウザから Cisco ISE ノードにログインします。
2. プライマリノードでダークモードが適用された後、初めてセカンダリ Cisco ISE ノードにログインします。

Cisco ISE ホームのダッシュボード

Cisco ISE ホームダッシュボードには、効果的なモニタリングおよびトラブルシューティングに必要不可欠な、統合された相関性のあるライブ統計データが表示されます。ダッシュボード要素には通常、24 時間のアクティビティが表示されます。次の図に、Cisco ISE ダッシュボードで使用できる情報を例示します。Cisco ISE ダッシュボードデータはプライマリポリシー管理ノード（PAN）のポータルでのみ表示されます。

図 *5 : Cisco ISE* ホームダッシュボード



[ホーム（Home）] ページには、Cisco ISE データを表示する 5 つのデフォルトのダッシュボードがあります。これらの各ダッシュボードには、複数の事前定義ダッシュレットがあります。

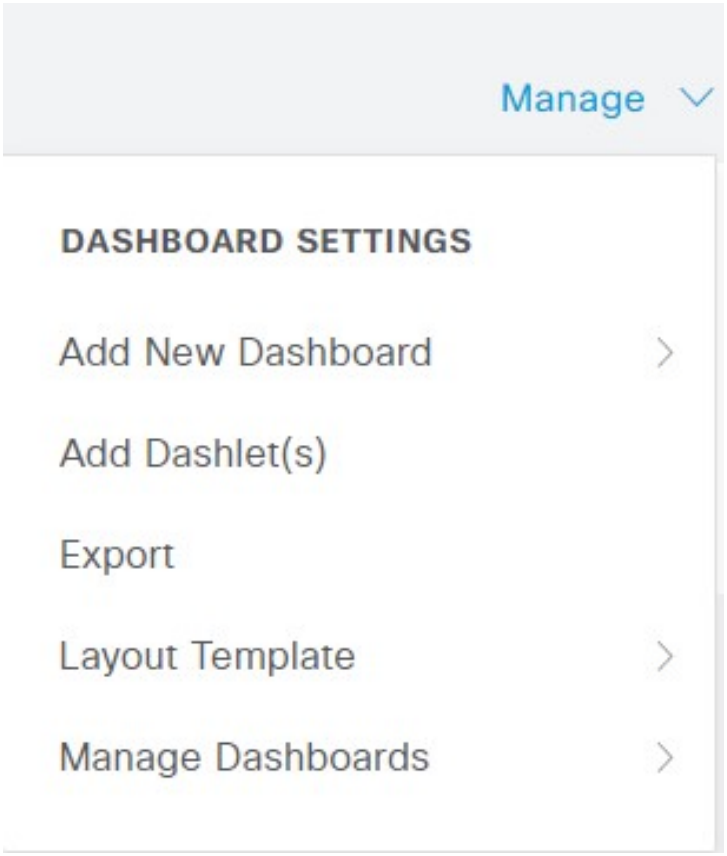
- [概要（Summary）]：このダッシュボードには、線形の [メトリック（Metrics）] ダッシュレット、円グラフダッシュレット、およびリストダッシュレットがあります。[メトリック（Metrics）] ダッシュレットは設定できません。このダッシュボードにはデフォルトでは、[ステータス（Status）]、[エンドポイント（Endpoints）]、[エンドポイントカテゴリ（Endpoint Categories）]、[ネットワークデバイス（Network Devices）] があります。
- [エンドポイント（Endpoints）]：このダッシュボードにはデフォルトでは、[ステータス（Status）]、[エンドポイント（Endpoints）]、[（エンドポイントカテゴリ（Endpoint Categories）]、[ネットワークデバイス（Network Devices）] があります。
- [ゲスト（Guests）]：このダッシュボードには、ゲストユーザータイプ、ログイン失敗、およびアクティビティのロケーションに関する情報を提供するダッシュレットがあります。
- [脆弱性（Vulnerability）]：このダッシュボードには、脆弱性サーバーが Cisco ISE にレポートする情報が表示されます。

- [脅威（Threat）]：このダッシュボードには、Cisco ISE に送信された脅威サーバーのレポートの情報が表示されます。

ホーム ダッシュボードの設定

ホームページダッシュボードをカスタマイズするには、ページの右上隅にある [管理（Manage）] アイコンをクリックします。

図 *6*：ダッシュボードのカスタマイズ



ドロップダウンリストには、次のオプションが表示されます。

- [新しいダッシュボードの追加（Add New Dashboard）] では、新しいダッシュボードを追加できます。表示されたフィールドに値を入力し、[適用（Apply）] をクリックします。
- [ダッシュレットの追加（Add Dashlet(s)）] は、使用可能なダッシュレットのリストを含むダイアログボックスを表示します。ダッシュレットをダッシュボードに追加または削除するには、ダッシュレット名の横にある [追加（Add）] または [削除（Remove）] をクリックします。
- [エクスポート（Export）] を選択すると、選択されているホームビューを PDF に保存します。

- [レイアウトテンプレート（Layout Template）] を選択すると、このビューに表示されるカラムの数を設定します。
- [ダッシュボード管理（Manage Dashboards）] には、次の 2 つのオプションがあります。
  - [デフォルトダッシュボードとしてマーク（Mark As Default Dashboard）]：このオプションを選択すると、[ホーム（Home）] を選択したときに現在のダッシュボードがデフォルトビューになります。
  - [すべてのダッシュボードをリセット（Reset All Dashboards）]：このオプションを使用すると、すべてのダッシュボードもリセットし、すべてのホームダッシュボードの設定を削除します。

[コンテキストの可視性（Context Visibility）] のビュー

[コンテキストの可視性（Context Visibility）] ウィンドウの構造はホームページに似ていますが、[コンテキストの可視性（Context Visibility）] ウィンドウでは次の点が異なります。

- 表示データをフィルタリングするときに、現在のコンテキストを維持する（ブラウザ ウィンドウ）
- より細かなカスタマイズが可能である
- エンドポイント データを中心としている

プライマリ PAN からのコンテキストの可視性データのみを表示できます。

[コンテキストの可視性（Context Visibility）] ウィンドウのダッシュレットには、エンドポイントと、エンドポイントから NAD への接続に関する情報が表示されます。現在表示されている情報は、各ウィンドウのダッシュレットの下にあるデータのリストの内容に基づいています。各ウィンドウには、タブの名前に基づいてエンドポイントデータが表示されます。データをフィルタリングすると、リストとダッシュレットの両方が更新されます。データをフィルタリングするには、1 つ以上の円グラフの特定部分をクリックするか、表で行をフィルタリングするか、またはこれらの操作を組み合わせて実行します。複数のフィルタを選択した場合、フィルタ結果は加算的になります。これはカスケードフィルタと呼ばれます。これにより、ドリルダウンして特定のデータを見つけることができます。また、リストでエンドポイントをクリックして、そのエンドポイントの詳細ビューを表示することもできます。

アカウンティングの開始と更新の情報が Cisco ISE に確実に送信されるように、ネットワーク アクセス デバイス（NAD）でアカウンティングの設定を有効にすることを推奨します。

Cisco ISE では、アカウンティングが有効になっている場合にのみ、最新の IP アドレス、セッションのステータス（ [接続（Connected）]、[切断（Disconnected）]、または [拒否（Rejected）]）、エンドポイントの非アクティブな日数などのアカウンティング情報を収集できます。この情報は、Cisco ISE 管理ポータルの [ライブログ（Live Logs）]、[ライブセッション（Live Sessions）]、および [コンテキストの可視性（Context Visibility）] の各ウィンドウに表示されます。NAD でアカウンティングが無効になっている場合、[ライブセッション（Live Sessions）]、[ライブログ（Live Logs）]、および [コンテキストの可視性（Context Visibility）]

の各ウィンドウ間でアカウンティング情報が欠落しているか、間違っているか、または一致していない可能性があります。

[コンテキストの可視性（Context Visibility）] の下には、4 つのメインメニューオプションがあります。

- [エンドポイント（Endpoints）]：デバイスのタイプ、コンプライアンス ステータス、認証タイプ、ハードウェアインベントリなどに基づいて表示するエンドポイントをフィルタ処理できます。詳細については、ハードウェア ダッシュボード（499 ページ）を参照してください。

（注） Cisco ISE 管理ポータルのホームページで使用可能な [可視性の設定（Visibility Setup）] ワークフローでは、エンドポイント検出用の IP アドレス範囲のリストを追加できます。このワークフローの設定後に Cisco ISE はエンドポイントを認証しますが、設定した IP アドレス範囲内に含まれていないエンドポイントは、**[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]** ウィンドウと [エンドポイント（Endpoints）] のリストページ（**[ワークセンター（Work Centers）] > [ネットワークアクセス（Endpoints）] > [ID（Identities）] > [エンドポイント（Endpoints）]**）に表示されません。

- [ユーザー（Users）]：ユーザー ID ソースからのユーザーベースの情報を表示します。

  ユーザー名またはパスワード属性が変更されると、認証ステータスが変更された時点で [ユーザー（Users）] ウィンドウに反映されます。

  Microsoft Active Directory でユーザー名が変更されると、再認証後すぐに [ユーザー（Users）] ウィンドウに更新された変更が表示されます。

  Microsoft Active Directory で電子メール、電話番号、部門など、その他の属性が変更されると、再認証から 24 時間後に [ユーザー（Users）] ウィンドウに更新された属性が表示されます。

（注） AD からのユーザー属性の更新は、Active Directory プローブで設定されている間隔によって異なります。詳細については、「Active Directory プローブ」を参照してください。

- [ネットワークデバイス（Network Devices）]：このウィンドウには、接続しているエンドポイントがある NAD のリストが表示されます。任意の NAD について、対応する [エンドポイント数（Number of endpoints）] 列に表示されるエンドポイントの数をクリックします。その NAD によってフィルタ処理されたすべてのデバイスをリストしたウィンドウが表示されます。

（注） ネットワークデバイスに SNMPv3 パラメータを設定した場合、Cisco ISE モニタリングサービス（**[操作（Operations）]** > **[レポート（Reports）]** > **[カタログ（Catalog）]** > **[ネットワークデバイス（Network Device）]** > **[セッションステータス概要（Session Status Summary）]**）によって提供される [ネットワークデバイスセッションステータス概要（Network Device Session Status Summary）] レポートを生成できません。ネットワークデバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。

- [アプリケーション（Application）]：このウィンドウを使用して、インストールされている特定のアプリケーションがあるエンドポイントの数を識別します。結果は、グラフ形式と表形式で表示されます。グラフ表示は、比較分析に役立ちます。たとえば、Google Chrome ソフトウェアを使用してエンドポイントの数をバージョン、ベンダー、カテゴリ（フィッシング詐欺対策、ブラウザなど）と共に、表や棒グラフで確認することができます。詳細については、「アプリケーション ダッシュボード」を参照してください。

[コンテキストの可視性（Context Visibility）] ウィンドウの新しいタブを作成し、カスタムリストを作成して、さらにフィルタリングを行います。カスタムビューではダッシュレットはサポートされていません。

ダッシュレット内の円形グラフのセクションをクリックすると、そのダッシュレットからフィルタ処理されたデータを含む新しいウィンドウが表示されます。この新しいウィンドウから、ビューに表示するデータのフィルタリング（503 ページ）の説明に従って、表示されたデータを引き続きフィルタ処理できます。

エンドポイントデータを特定するための [コンテキストの可視性（Context Visibility）] ウィンドウの使用に関する詳細については、Cisco YouTube ビデオ（https://www.youtube.com/watch?v=HvonGhrydfg）を参照してください。

関連トピック

ハードウェア ダッシュボード （499 ページ）

コンテキストの可視性の属性

コンテキストの可視性の属性を提供するシステムとサービスでは、同じ属性名に異なる値を使用していることがよくあります。次に、いくつかの例を示します。

オペレーティング システム

- *OperatingSystem*：ポスチャ オペレーティング システム。
- *operating-system*：NMAP オペレーティングシステム。
- *operating-system-result*：プロファイラ統合オペレーティングシステム。

（注） CiscoISEでエンドポイントに複数のプローブを有効にした場合、[コンテキストの可視性（Context Visibility）] ページに表示されるエンドポイントのオペレーティングシステムのデータにいくつかの不一致が生じることがあります。

ポータル名

- *Portal.Name*：デバイス登録が有効な場合のゲストポータル名。
- *PortalName*：デバイス登録が無効な場合のゲスト ポータル名。

ポータルユーザー

- *User-Name*：RADIUS 認証のユーザー名。
- *GuestUserName*：ゲストユーザー名。
- *PortalUser*：ポータルユーザー名。

アプリケーション ダッシュボード

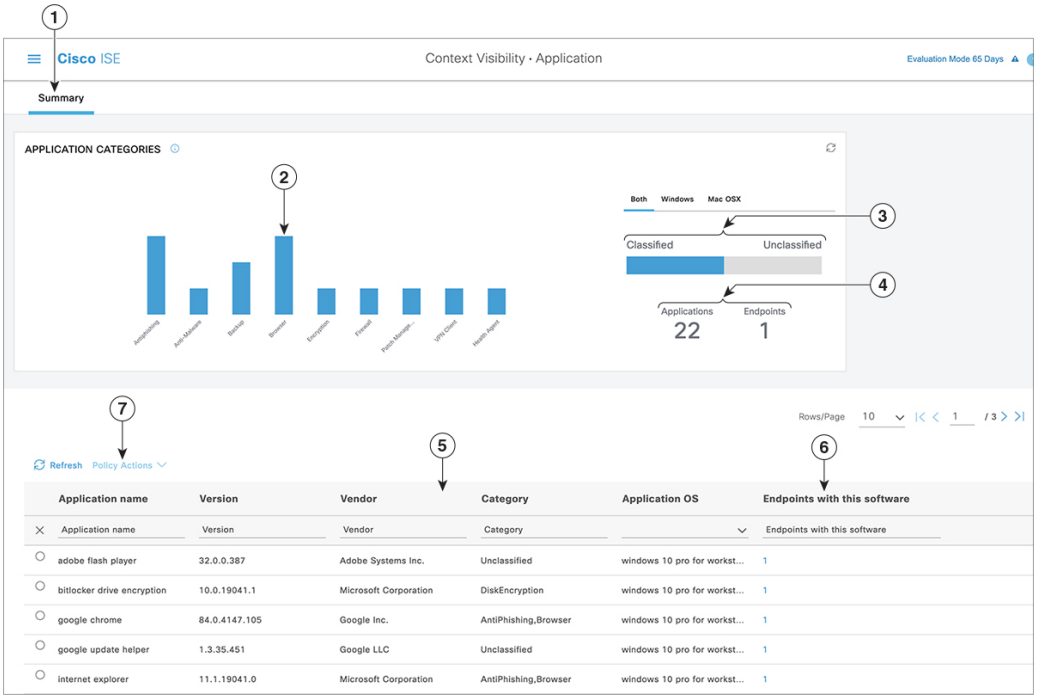


表 *19 :* アプリケーション ダッシュボードの説明

ラベル	説明
1	[要約（Summary）] タブは、デフォルトでホームページに表示されます。棒グラフを含む[アプリケーション カテゴリ（Application Categories）] ダッシュレットが表示されます。アプリケーションは13のカテゴリに分類されます。これらのカテゴリに属さないアプリケーションは、[未分類（Unclassified）] としてグループ化されます。 利用可能なカテゴリは、[マルウェア対策（Anti-Malware）]、[フィッシング対策（Antiphishing）]、[バックアップ（Backup）]、[ブラウザ（Browser）]、[データ漏洩防止（Data Loss Prevention）]、[データ ストレージ（Data Storage）]、[暗号化（Encryption）]、[ファイアウォール（Firewall）]、[メッセンジャ（Messenger）]、[パッチ管理（Patch Management）]、[パブリック ファイル共有（Public File Sharing）]、[仮想マシン（Virtual Machine）]、[VPN クライアント（VPN Client）] です。
2	各バーは、分類されたカテゴリに対応します。各バーの上にマウスを置くと、選択したアプリケーションカテゴリに対応するアプリケーションとエンドポイントの合計数が表示されます。
3	分類されたカテゴリに該当するアプリケーションとエンドポイントは青色で表示されます。未分類のアプリケーションとエンドポイントはグレーで表示されます。分類されたカテゴリバーまたは分類されていないカテゴリバーの上にマウスを置くと、そのカテゴリに属するアプリケーションとエンドポイントの合計数が表示されます。[分類済み（Classified）] をクリックして、ウィンドウ内の棒グラフと表で結果を表示できます。[未分類（Unclassified）] をクリックすると、ウィンドウ内の棒グラフが無効になり（グレー表示）、表に結果が表示されます。
4	アプリケーションとエンドポイントは、選択されたフィルタに基づいて表示されます。異なるフィルタをクリックすると、パンくずリストを表示できます。**[すべてのフィルタをクリア（Clear All Filters）]** の順にクリックして、すべてのフィルタを削除できます。

<table>
<tr><th>ラベル</th><th>説明</th></tr>
<tr><td>5</td><td>複数のバーをクリックすると、対応する分類されたアプリケーションとエンドポイントが表に表示されます。たとえば、[マルウェア対策（Antimalware）]および[パッチ管理（Patch Management）] カテゴリを選択すると、次の結果が表示されます。
<table>
<tr><th>アプリケーション</th><th>バージョン</th><th>ベンダー</th><th>カテゴリ</th><th>アプリケーション OS</th><th>このソフトウェアで使用するエンドポイント</th></tr>
<tr><td>Gatekeeper</td><td>9.9.5</td><td>Apple Inc.</td><td>マルウェア対策</td><td>windows 7 64 ビット、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
<tr><td>Gatekeeper</td><td>10.9.5</td><td>Apple Inc.</td><td>マルウェア対策</td><td>windows 8 64 ビット、mac osx 10.10</td><td>3</td></tr>
<tr><td>ソフトウェア更新</td><td>2.3</td><td>Apple Inc.</td><td>パッチ管理</td><td>windows 7 64 ビット、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
</table></td></tr>
<tr><td>6</td><td>表の [このソフトウェアで使用するエンドポイント（Endpoints With This Software）] 列のエンドポイントをクリックして、Mac アドレス、NAD IP アドレス、NAD ポート ID/SSID、IPv4 アドレスなどのエンドポイントの詳細を表示します。</td></tr>
<tr><td>7</td><td>アプリケーションのコンプライアンス条件と修復を作成するには、アプリケーション名を選択し、[ポリシー アクション（Policy Actions）] ドロップダウンリストから [アプリケーション コンプライアンスの作成（Create App Compliance）] オプションを選択します。</td></tr>
</table>

ハードウェア ダッシュボード

[コンテキストの可視性（context visibility）] の下の [エンドポイント ハードウェア（endpoint hardware）] タブは、短期間にエンドポイント ハードウェア インベントリ情報を収集、分析、およびレポートするのに役立ちます。メモリ容量が小さいエンドポイントの検出や、エンドポイントのBIOSモデル/バージョンの検出など、情報を収集することができます。これらの結果に基づいて、メモリ容量を増やしたり、BIOS バージョンをアップグレードすることができます。アセットの購入を計画する前に、要件を評価することができます。リソースを適時に交換することができます。モジュールをインストールしたりエンドポイントとやりとりすることなく、この情報を収集できます。要約すると、アセットのライフサイクルを効果的に管理できます。

（注） ハードウェア インベントリ データは、ISE GUI に表示されるまでに 120 秒かかります。ハードウェア インベントリ データは、ポスチャ準拠および非準拠の状態について収集されます。

[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [ハードウェア（Hardware）] ページには、[製造者（Manufacturers）] および [エンドポイント使用率（Endpoint Utilizations）] ダッシュレットが表示されます。これらのダッシュレットは、選択されたフィルタに基づく変更を反映します。[製造者（Manufacturers）] ダッシュレットには、Windows および Mac OS が搭載されたエンドポイントのハードウェア インベントリの詳細が表示されます。[エンドポイント使用率（Endpoint Utilizations）] ダッシュレットには、エンドポイントの CPU、メモリ、およびディスク使用率が表示されます。3 つのオプションのいずれかを選択すると、利用率をパーセンテージで表示できます。

- [CPU 使用率が n% を超えるデバイス（Devices With Over n% CPU Usage）]
- [メモリ使用率が n% を超えるデバイス（Devices With Over n% Memory Usage）]
- [ディスク使用率が n% を超えるデバイス（Devices With Over n% Disk Usage）]

（注）
- [ハードウェアの可視性（Hardware Visibility）] ページのクイック フィルタには、3 文字以上入力する必要があります。クイック フィルタを効率的に機能させるには、文字の入力後に他のカラム属性のフィルタをクリックする方法もあります。
- 次の表はハードウェアに関連した属性に基づいたフィルタリングにのみ使用されるため、一部のカラム属性はグレー表示されています。
- オペレーティング システムのフィルタは、[製造元（Manufacturers）] チャートにのみ適用されます。これは、次の表には関連しません。

エンドポイントとその接続された外部デバイスのハードウェア属性は表形式で表示されます。次のハードウェア属性が表示されます。

- MAC アドレス
- BIOS 製造元
- BIOS シリアル番号
- BIOS モデル
- 接続デバイス
- CPU 名
- CPU 速度（GHz）
- CPU 使用率（%）

- コア数
- プロセッサ数
- メモリサイズ（GB）
- メモリ使用率（%）
- 内部ディスクの合計サイズ（GB）
- 内部ディスクの合計フリーサイズ（GB）
- 内部ディスクの合計使用率（%）
- 内部ディスク数
- NAD ポート ID
- ステータス
- ネットワークデバイス名
- Location
- UDID
- IPv4 アドレス
- ユーザー名
- ホスト名
- OS タイプ
- 異常な動作
- エンドポイントプロファイル
- 説明
- エンドポイントタイプ
- ID グループ
- 登録日
- ID ストア
- 許可プロファイル

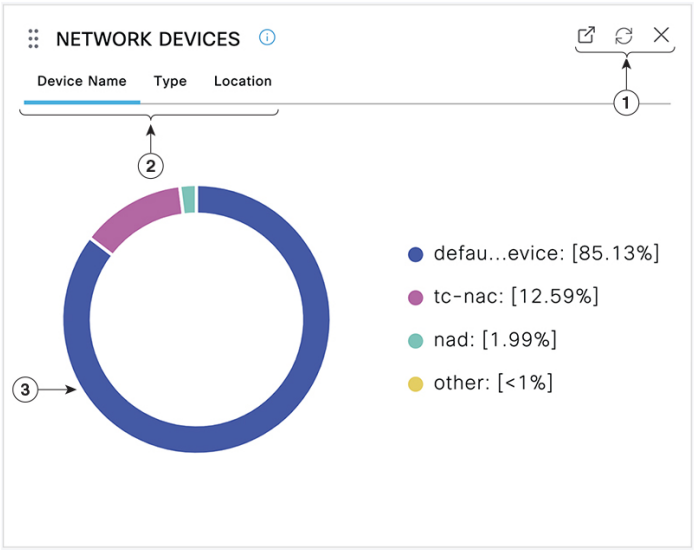
エンドポイントに対応する [接続デバイス（Attached Devices）] 列の番号をクリックすると、現在エンドポイントに接続されている USB デバイスの名前、カテゴリ、製造元、タイプ、製品 ID、およびベンダー ID を表示できます。

（注） Cisco ISE はクライアントのシステムのハードウェア属性をプロファイリングしますが、Cisco ISE がプロファイリングしないハードウェア属性がいくつか存在することがあります。これらのハードウェア属性は、[ハードウェア コンテキストの可視性（Hardware Context Visibility）] ページに表示されないことがあります。

ハードウェア インベントリ データの収集間隔は、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]** ページで制御できます。デフォルトの間隔は 5 分です。

ダッシュレット

次のイメージは、ダッシュレットの例です。



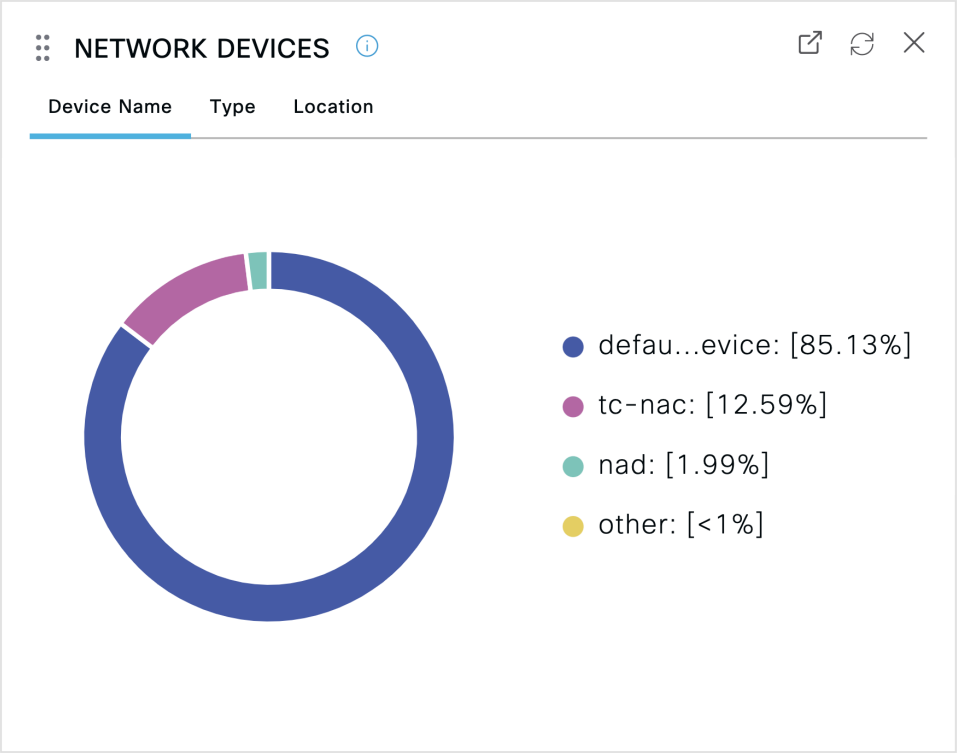
1. [新しいウィンドウを開く（Open New Window）] アイコンにより、新しいブラウザウィンドウでこのダッシュレットを開きます。円グラフが更新されます。このダッシュレットを削除するには、**[X]** をクリックします。このオプションは、ホームページでのみ使用できます。[コンテキストの可視性（Context Visibility）] ウィンドウでダッシュレットを削除するには、画面右上隅にある歯車のシンボルを使用します。
2. 一部のダッシュレットには異なるカテゴリのデータが表示されます。カテゴリをクリックすると、そのデータセットの円グラフが表示されます。
3. 円グラフには、選択したデータが表示されます。円グラフの 1 つのセグメントをクリックすると、新しいタブが開き、その円グラフセグメントに基づいてフィルタリングされたデータが表示されます。

ホームページダッシュボードの円グラフのセクションをクリックすると、新しいブラウザウィンドウでグラフを開きます。新しいウィンドウには、クリックした円グラフのセクションでフィルタリングされたデータが表示されます。

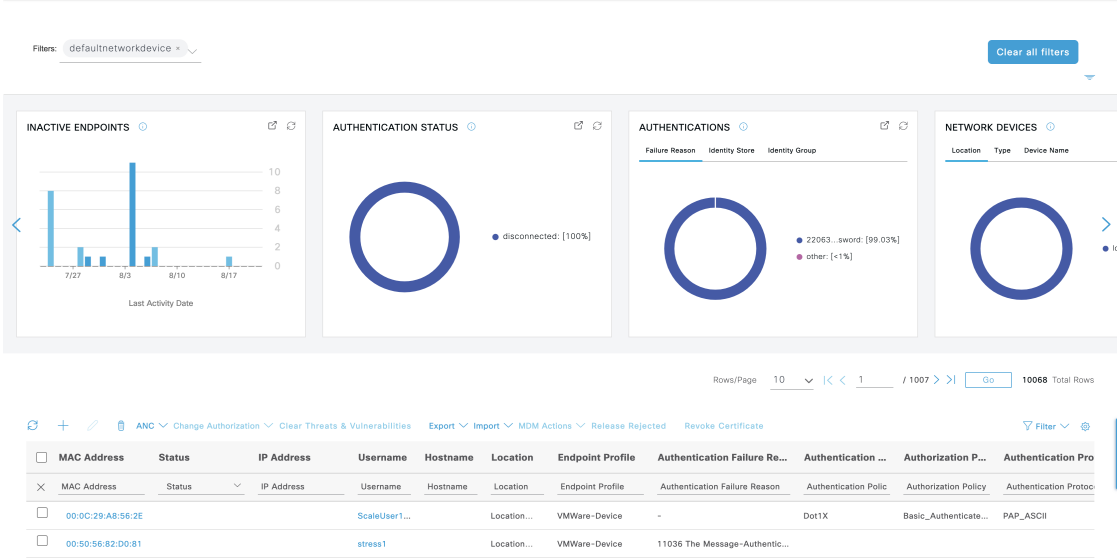
[コンテキストの可視性（Context Visibility）] ウィンドウで円グラフのセクションをクリックすると、表示されるデータはフィルタリングされますが、コンテキストは変更されません。フィルタリングされたデータは、同じブラウザウィンドウで表示されます。

ビューに表示するデータのフィルタリング

[コンテキストの可視性（Context Visibility）] ウィンドウでダッシュレットをクリックすると、対応するデータがクリックした項目でフィルタ処理されて表示されます。たとえば、円グラフのセクションをクリックすると、選択したセクションのデータがフィルタ処理されて表示されます。



[ネットワークデバイス（Network Devices）] ダッシュレットで **defau...evice** をクリックすると、次のイメージに示すように、新しいウィンドウにデータが表示されます。



円グラフのその他のセクションをクリックして、データをさらにフィルタ処理します。[フィルタ（Filter）] ドロップダウンリストまたはデータのリストの右上隅にある歯車アイコンを使用して、表示されるデータを管理することもできます。

カスタムフィルタを保存します。

カスタムフィルタの作成

自分だけがアクセスできるユーザー固有のカスタムフィルタを作成して保存します。Cisco ISE にログインしている他のユーザーは、作成したカスタムフィルタを表示できません。これらのカスタムフィルタは Cisco ISE データベースに保存されます。Cisco ISE にログインしているコンピュータやブラウザからアクセスできます。

ステップ 1 **[フィルタ（Filter）]**をクリックし、ドロップダウンリストから [高度なフィルタ（Advanced Filter）] を選択します。

ステップ 2 [フィルタ（Filter）] メニューからフィールド、演算子、値などの検索属性を指定します。

ステップ 3 [+] をクリックして、その他の条件を追加します。

ステップ 4 [実行（Go）] をクリックして、指定された属性に一致するエントリを表示します。

ステップ 5 [保存 (Save)] をクリックして、フィルタを保存します。

ステップ 6 名前を入力し、[Save（保存）] をクリックします。[フィルタ（Filter）] ドロップダウンリストにフィルタが表示されるようになりました。

拡張フィルタを使用した条件によるデータのフィルタリング

拡張フィルタを使用して、指定した条件（名 = Mike、ユーザー グループ = 従業員など）に基づいて情報をフィルタリングできます。複数の条件を指定できます。

ステップ 1 **[フィルタ（Filter）]**をクリックし、[高度なフィルタ（Advanced Filter）] を選択します。
ステップ 2 [フィルタ（Filter）] メニューから検索属性（フィールド、演算子、値など）を指定します。
ステップ 3 [+] をクリックして、その他の条件を追加します。
ステップ 4 [実行（Go）] をクリックして、指定した属性に一致するエントリを表示します。

クイックフィルタを使用したフィールド属性によるデータのフィルタリング

クイックフィルタを使用して、リストページに表示されるフィールド属性の値を入力し、ページをリフレッシュすることで、フィルタ基準に一致するレコードのみを一覧表示できます。

ステップ 1 **[フィルタ（Filter）]** をクリックし、ドロップダウンリストから [クィックフィルタ（Quick Filter）] を選択します。
ステップ 2 属性フィールドの 1 つ以上に検索条件を入力すると、指定した属性に一致するエントリが自動的に表示されます。

ダッシュレットビューでのエンドポイントアクション

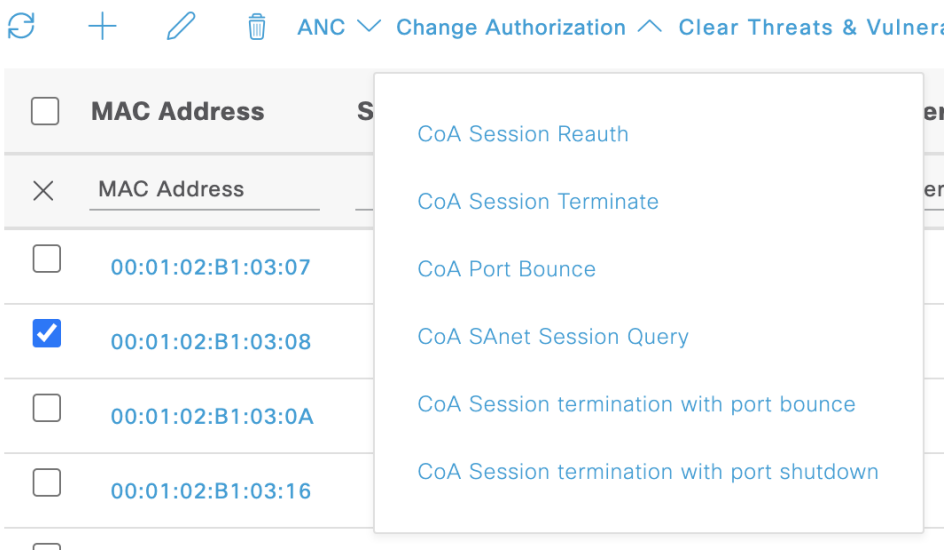
リストの上部にあるツールバーでは、選択したリスト内のエンドポイント上でアクションを実行できます。すべてのリストですべてのアクションが有効になっているわけではありません。使用可能になっている機能によってアクションは異なります。使用する前に Cisco ISE で有効にする必要がある 2 つのエンドポイントアクションを次のリストに示します。

- **適応型ネットワーク制御アクション**

  適応型ネットワーク制御を有効にした場合、リストでエンドポイントを選択して、ネットワークアクセスを割り当てたり、取り消したりできます。また、認可変更も発行できます。

  ホームページダッシュレットで円グラフをクリックすると、表示される新しいウィンドウに [ANC] オプション と[認可変更（Change Authorization）] オプションが表示されます。アクションを実行するエンドポイントのチェックボックスをオンにし、[ANC] ドロップダウンリストと [認可変更（Change Authorization）] ドロップダウンリストから必要なアクションを選択します。

図 7: ダッシュレットビューでのエンドポイントアクション



- **MDM アクション**

  MDM サーバーを Cisco ISE に接続すると、選択したエンドポイントで MDM アクションを実行できます。[MDM アクション（MDM Actions）] ドロップダウンリストから必要なアクションを選択します。

Cisco ISE ダッシュボード

Cisco ISE のダッシュボードまたはホームページ（[メニュー（Menu）] アイコン（☰）をクリックし [ダッシュボード（Dashboard）] を選択）は、Cisco ISE 管理ポータルへのログイン後に表示されるランディングページです。ダッシュボードは、ウィンドウの上部に沿って表示されるメトリック メーターと下にあるダッシュレットで構成された、集中化された管理コンソールです。デフォルトのダッシュボードは、[概要（Summary）]、[エンドポイント（Endpoints）]、[ゲスト（Guests）]、[脆弱性（Vulnerability）]、[脅威（Threat）] です。Cisco ISE ホームのダッシュボード （492 ページ）を参照してください。

（注） Cisco ISE プライマリ PAN ポータルでのみ、このダッシュボードを表示できます。

ダッシュボードのリアルタイムデータによって、ネットワークにアクセスしているデバイスとユーザーを一目で確認できるステータスと、システムの正常性の概要が表示されます。

2 番目のレベルのメニューバーにある歯車アイコンをクリックして、ダッシュボード設定のドロップダウンリストを表示します。次の表では、ドロップダウンリストで使用可能なダッシュボード設定オプションについて説明します。

ドロップダウンリスト オプション	説明
新しいダッシュボードの追加（Add New Dashboard）	5つのデフォルトのダッシュボードを含めて、最大で 20 個のダッシュボードを設定できます。
ダッシュボードの名前の変更（Rename Dashboard）	（このオプションはカスタムダッシュボードでのみ使用可能）ダッシュボードの名前を変更するには、次の手順を実行します。 **1.** [ダッシュボードの名前の変更（Rename Dashboard）] をクリックします。 **2.** 新しい名前を指定します。 **3.** [適用（Apply）] をクリックします。
ダッシュレットの追加（Add Dashlet）	ホームページダッシュボードにダッシュレットを追加するには、次の手順を実行します。 **1.** [ダッシュレットの追加（Add Dashlets）] をクリックします。 **2.** [ダッシュレットの追加（Add Dashlets）] ウィンドウで、追加するダッシュレットの横にある [追加（Add）] をクリックします。 **3.** [保存（Save）] をクリックします。 （注） ダッシュボードごとに最大で 9 個のダッシュレットを追加できます。

ドロップダウンリスト オプション	説明
エクスポート（Export）	ダッシュボードのデータは PDF または CSV ファイルとしてエクスポートできます。 **1.** [エクスポート（Export）] をクリックします。 **2.** [エクスポート（Export）] ダイアログボックスで、次のいずれかのファイル形式の横にあるオプションボタンをクリックします。 • [PDF]：選択したダッシュレットのスナップショットビューを表示するには、 PDF 形式を選択します。 • [CSV]：選択したダッシュボードのデータを zip ファイルとしてダウンロードするには、CSV 形式を選択します。 **3.** [エクスポート（Export）] ダイアログボックスで、エクスポートするダッシュレットの横にあるチェックボックスをオンにします。 **4.** [エクスポート（Export）] をクリックします。 zip ファイルには、選択したダッシュボードの個々のダッシュレット CSV ファイルが含まれています。ダッシュレットの各タブに関連するデータは、対応するダッシュレット CSV ファイルで個別のセクションとして示されます。 カスタムダッシュボードをエクスポートする場合、zip ファイルは同じ名前でエクスポートされます。たとえば、MyDashboard という名前のカスタムダッシュボードをエクスポートすると、エクスポートされたファイルの名前は MyDashboard.zip となります。

ドロップダウンリスト オプション	説明
レイアウトテンプレート（Layout Template）	ダッシュレットが表示されるテンプレートのレイアウトを変更できます。 レイアウトを変更するには、次の手順を実行します。 **1.** [レイアウトテンプレート（Layout Template）] をクリックします。 **2.** 使用可能なオプションから必要なレイアウトを選択します。
ダッシュボードの管理（Manage Dashboards）	[ダッシュボードの管理（Manage Dashboards）] をクリックし、次のいずれかのオプションを選択します。 • [デフォルトのダッシュボードにする（Mark as Default Dashboard）]：ダッシュボードをデフォルトのダッシュボード（ホームページ）として設定するには、このオプションを使用します。 • [すべてのダッシュボードのリセット（Reset all Dashboards）]：すべてのダッシュボードを元の設定にリセットするには、このオプションを使用します。

対応するカスタムダッシュボードの横にある閉じる（**x**）アイコンをクリックすることで、作成したダッシュボードを削除できます。

（注） デフォルト ダッシュボードの名前を変更したり、削除することはできません。

各ダッシュレットの右上隅には、次の操作を実行できるツールバーがあります。

- [分離（Detach）]：別のウィンドウにダッシュレットを表示します。
- [更新（Refresh）]：ダッシュレットを更新します。
- [削除（Remove）]：ダッシュボードからダッシュレットを削除します。

ダッシュレットの左上隅にあるグリッパ アイコンを使用して、ダッシュレットをドラッグ アンド ドロップできます。

[アラーム（Alarms）] ダッシュレットには、[シビラティ（重大度）（Severity）] 列のクイックフィルタが含まれています。[シビラティ（重大度）（Severity）] ドロップダウンリストから

[クリティカル（Critical）]、[警告（Warning）]、または [情報（Info）] を選択して、アラームをシビラティ（重大度）でフィルタ処理できます。

Cisco ISE 国際化およびローカリゼーション

Cisco ISE 国際化では、サポートされている言語にユーザーインターフェイスを合わせます。ユーザーインターフェイスのローカリゼーションでは、ロケール固有のコンポーネントと翻訳されたテキストが組み込まれます。Windows、MAC OSX、およびAndroidデバイスの場合、ネイティブ サプリカント プロビジョニング ウィザードは、次のサポートされている言語のいずれかで使用できます。

Cisco ISE の国際化およびローカリゼーションのサポートでは、ポータルに接するエンドユーザーに対してUTF-8符号化で英語以外のテキストをサポートすることと管理者ポータルの選択的フィールドに重点を置いています。

サポートされている言語

Cisco ISE では、次の言語とブラウザ ロケールのローカリゼーションおよび国際化がサポートされています。

表 *20* : サポートされる言語とロケール

言語	ブラウザ ロケール
中国語（繁体字）	zh-tw
中国語（簡体字）	zh-cn
チェコ語	cs-cz
オランダ語	nl-nl
英語	en
フランス語	fr-fr
ドイツ語	de-de
ハンガリー語	hu-hu
イタリア語	it-it
日本語	ja-jp
韓国語	ko-kr
ポーランド語	pl-pl
ポルトガル語（ブラジル）	pt-br

言語	ブラウザ ロケール
ロシア語	ru-ru
スペイン語	es-es

エンドユーザー Web ポータルのローカリゼーション

ゲスト、スポンサー、デバイスおよびクライアントプロビジョニングの各ポータルは、サポートされているすべての言語およびロケールにローカライズされています。ローカライズには、テキスト ラベル、メッセージ、フィールド名およびボタン ラベルが含まれます。クライアントブラウザがCisco ISEテンプレートにマッピングされていないロケールを要求した場合、ポータルは英語のテンプレートを使用して内容を表示します。

管理ポータルを使用して、各言語のゲスト、スポンサー、デバイスの各ポータルで使用されるフィールドを変更できます。また、言語を追加することも可能です。現在、クライアントプロビジョニング ポータルについては、これらのフィールドはカスタマイズできません。

HTML ページを Cisco ISE にアップロードすることによって、ゲスト ポータルを詳細にカスタマイズできます。カスタマイズしたページをアップロードする場合は、展開に対する適切なローカリゼーション サポートに責任を負います。Cisco ISE では、サンプル HTML ページを含むローカリゼーション サポート例が提供されており、これをガイドとして使用できます。Cisco ISE では、国際化されたカスタム HTML ページをアップロード、格納、および表示することができます。

（注） NAC および MAC エージェントのインストーラおよび WebAgent ページはローカライズされていません。

UTF-8 文字データ エントリのサポート

エンドユーザーに（Cisco クライアントエージェントまたはサプリカント、あるいはスポンサー、ゲスト、デバイス、クライアントプロビジョニングの各ポータルを介して）公開される Cisco ISE フィールドは、すべての言語の UTF-8 文字セットをサポートします。UTF-8 は、Unicode 文字セット用のマルチバイト文字エンコーディングであり、ヘブライ語、サンスクリット語、アラビア語を含む、多数の異なる言語文字セットがあります。

文字の値は、管理設定データベースに UTF-8 で格納され、UTF-8 文字はレポートおよびユーザー インターフェイス コンポーネントで正しく表示されます。

UTF-8 クレデンシャル認証

ネットワーク アクセス認証では、UTF-8 ユーザー名およびパスワードのクレデンシャルがサポートされます。これには、RADIUS、Extensible Authentication Protocol（EAP）、RADIUS プロキシ、RADIUS トークン、ゲストおよび管理ポータルのログイン認証からの Web 認証が含

まれます。ユーザー名とパスワードの UTF-8 サポートは、ローカル ID ストアと外部 ID ストアを照合する認証に適用されます。

UTF-8認証は、ネットワーク ログインに使用されるクライアント サプリカントに依存します。一部の Windows ネイティブ サプリカントでは、UTF-8 クレデンシャルはサポートされません。

（注） RSA は UTF-8 ユーザーをサポートしていないため、RSA での UTF-8 認証はサポートされていません。Cisco ISE と互換性がある RSA サーバーも UTF-8 をサポートしていません。

UTF-8 ポリシーおよびポスチャ評価

属性値に基づいて決定される Cisco ISE のポリシー ルールに、UTF-8 テキストが含まれている場合があります。UTF-8 属性値はルール評価でサポートされます。また、管理ポータルで UTF-8 の値を使用して条件を設定できます。

ポスチャ要件を、UTF-8 文字セットに基づくファイル、アプリケーション、およびサービス条件として変更します。

サプリカントに送信されるメッセージの UTF-8 サポート

RSA プロンプトおよびメッセージは、RADIUS 属性 REPLY-MESSAGE を使用して、または EAP データ内で、サプリカントに転送されます。テキストに UTF-8 データが含まれている場合は、サプリカントによって、クライアントのローカル オペレーティング システムの言語サポートに基づいて表示されます。一部の Windows ネイティブ サプリカントでは、UTF-8 クレデンシャルはサポートされません。

Cisco ISE プロンプトとメッセージは、サプリカントが実行されているクライアントのオペレーティングシステムのロケールと同期していない場合があります。エンドユーザーのサプリカントのロケールを Cisco ISE によってサポートされている言語に合わせる必要があります。

レポートおよびアラートの UTF-8 サポート

モニタリングとトラブルシューティングのレポートおよびアラートでは、Cisco ISE でサポートされている言語について、次のように関連属性の UTF-8 の値がサポートされています。次のアクティビティがサポートされています。

- ライブ認証の表示。
- レポート レコードの詳細ページの表示。
- レポートのエクスポートと保存。
- Cisco ISE ダッシュボードの表示。
- アラート情報の表示。
- tcpdump データの表示。

ポータルでの UTF-8 文字のサポート

Cisco ISE フィールド（UTF-8）では、ポータルとエンドユーザーメッセージでローカリゼーション用に現在サポートされているよりも多くの文字セットがサポートされています。たとえば、Cisco ISE では、ヘブライ語やアラビア語などの右から左へ記述する言語はサポートされていません（文字セット自体はサポートされています）。

次の表に、データの入力および表示にUTF-8 文字をサポートする管理者ポータルおよびエンドユーザー ポータルのフィールドを示します。次の制限があります。

- Cisco ISE では、UTF-8 文字を使用したゲストのユーザー名とパスワードはサポートされません。
- Cisco ISE では、証明書で UTF-8 文字を使用することはできません。

表 *21 : [*管理（*Administration***）*]* ポータルの *UTF-8* 文字フィールド**

[管理（Administration）] ポータルの要素	**UTF-8 フィールド**
ネットワーク アクセスのユーザー設定	• **ユーザー名** ユーザー名には、大文字と小文字、数字、スペース、特殊文字（`、%、^、;、:、[、{、|、}、]、\、‘、“、=、<、>、?、!、制御文字を除く）を組み合わせて使用できます。スペースのみのユーザー名は送信できません。 • **名** • **姓** • **電子メール**
ユーザー リスト	• すべてのフィルタフィールド。 • [ユーザーリスト（User List）] ウィンドウに表示される値。 • 左側のナビゲーション クイック ビューに表示される値。

[管理（Administration）] ポータルの要素	UTF-8 フィールド
ユーザー パスワード ポリシー	パスワードには、大文字と小文字、数字、特殊文字（「!」、@、#、$、^、&、*、（、および）の組み合わせを使用できます。[パスワード（Password）] フィールドでは、UTF-8 文字を含むあらゆる文字を使用できますが、制御文字は使用できません。 言語の中には大文字または小文字のアルファベットがないものがあります。ユーザーパスワードポリシーでユーザーに大文字または小文字でパスワードを入力することを求め、ユーザーの言語がこれらの文字をサポートしていない場合、ユーザーはパスワードを設定できません。ユーザーパスワードフィールドで UTF-8 文字に対応するには、[ユーザーパスワードポリシー（User Password Policy）] ページ（[メニュー（Menu）] アイコンをクリックし、**[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [ユーザー管理設定（User Authentication Settings）] > [パスワードポリシー（Password Policy）]** を選択します）で次のチェックボックスをオフにします。 • **小文字の英文字** • **大文字の英文字** 辞書に載っている単語とその順序を逆にした文字列、またはその文字を他の文字に置き換えた文字列は使用できません。
管理者リスト	• すべてのフィルタフィールド。 • 管理者リストウィンドウに表示される値。 • 左側のナビゲーションクイックビューに表示される値。
管理者ログイン ページ	• **ユーザー名**
RSA	• メッセージ • プロンプト
RADIUS トークン	• [認証（Authentication）] タブ > [プロンプト（Prompt）]
ポスチャ要件	• 名前 • [修復アクション（Remediation action）] > エージェント ユーザーに表示されるメッセージ • 要件リスト表示

[管理（Administration）] ポータルの要素	UTF-8 フィールド
ポスチャ条件	**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** ウィンドウの次のフィールドは次のとおりです。 • **[ファイル条件（File condition）]** > **[追加（Add）]** > **[ファイルパス（File path）]**。 • **[アプリケーション条件（Application Condition）]** > **[追加（Add）]** > **[プロセス名（Process Name）]**。 • **[サービス条件（Service condition）]** > **[追加（Add）]** > **[サービス名（Service name）]**。 • 条件リストが表示されます。
ゲストおよびデバイスの設定	• [スポンサー（Sponsor）] > [言語テンプレート（Language Template）]：サポートされているすべての言語、すべてのフィールド • [ゲスト（Guest）] > [言語テンプレート（Language Template）]：サポートされているすべての言語、すべてのフィールド • [デバイス（My Devices）] > [言語テンプレート（Language Template）]：サポートされているすべての言語、すべてのフィールド
システム設定	• [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲスト電子メールの設定（Guest Email Settings）]
[操作（Operations）] > [アラーム（Alarms）] > [ルール（Rule）]	• [基準（Criteria）] > [ユーザー（User）] • [通知（Notification）] > [電子メール通知ユーザー リスト（e-mail Notification user list）]
[操作（Operations）] > [レポート（Reports）]	• [操作（Operations）] > [ライブ認証（Live Authentications）] > [フィルタ（Filter）] フィールド • [操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] > [レポートフィルタ（Report filter）] フィールド
[操作（Operations）] > [トラブルシューティング（Troubleshoot）]	• [一般ツール（General Tools）] > [RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）] > [ユーザー名（Username）]

[管理（Administration）] ポータルの要素	UTF-8 フィールド
ポリシー	• [認証（Authentication）] > ポリシー条件内でのウィルス対策式の値 • [許可（Authorization）] または [ポスチャ（Posture）]、あるいは [クライアント プロビジョニング（Client Provisioning）] > [その他の条件（Other Conditions）] > ポリシー条件内でのウィルス対策式の値
ポリシー ライブラリ条件の属性値	• [認証（Authentication）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > ウィルス対策式の値 • [認証（Authentication）] > 単純条件リスト表示 • [認証（Authentication）] > 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [許可（Authorization）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > ウィルス対策式の値 • [許可（Authorization）] > 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [ポスチャ（Posture）] > [ディクショナリ単純条件/ディクショナリ複合条件（Dictionary Simple Condition/Dictionary Compound Condition）] > ウィルス対策式の値 • [ゲスト（Guest）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > ウィルス対策式の値

Cisco ISE ユーザーインターフェイス以外での UTF-8 サポート

この項では、Cisco ISE ユーザー インターフェイス外で UTF-8 がサポートされる領域について説明します。

デバッグ ログおよび CLI 関連の UTF-8 サポート

一部のデバッグ ログには、属性値とポスチャ条件の詳細が表示されます。すべてのデバッグログが UTF-8 値を受け入れます。raw UTF-8 データを含むデバッグログをダウンロードして、UTF-8 対応ビューアで表示できます。

Cisco Secure ACS 移行での UTF-8 サポート

Cisco ISE では、Cisco Secure Access Control Server（ACS）の UTF-8 設定のオブジェクトと値を移行できます。一部の UTF-8 オブジェクトの移行は、Cisco ISE UTF-8 言語でサポートされない場合があります。そのため、移行中に提供される UTF-8 データの一部は、管理ポータルまたはレポート方式を使用して読み取れない表示になる場合があります。（Cisco Secure ACS から移行された）読み取り不能な UTF-8 値を ASCII テキストに変換します。Cisco Secure ACS から

Cisco ISE への移行の詳細については、お使いの ISE バージョンの『Cisco Secure ACS to Cisco ISE Migration Tool』を参照してください。

UTF-8 の値のインポートおよびエクスポートのサポート

管理ポータルとスポンサー ポータルは、ユーザー アカウントの詳細をインポートするときに使用される UTF-8 値のプレーンテキストファイルと CSV ファイルをサポートしています。エクスポートされたファイルは CSV ファイルとして提供されます。

REST での UTF-8 サポート

External Representational State Transfer（REST）通信は、UTF-8 値をサポートします。これは、管理者認証を除き、Cisco ISE ユーザーインターフェイスの UTF-8 がサポートされる設定可能項目に適用されます。REST での管理者認証には、ログインのために ASCII テキストクレデンシャルが必要です。

ID ストアの許可データの UTF-8 サポート

Cisco ISE では、Microsoft Active Directory および Lightweight Directory Access Protocol（LDAP）がポリシー処理のために許可ポリシーで UTF- 8 データを使用できます。

MAC アドレスの正規化

Cisco ISE は次のいずれかの形式で入力した MAC アドレスの正規化をサポートしています。

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

Cisco ISE の次のウィンドウには、MAC アドレスが完全な状態で、または部分的に表示されます。

- **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]**
- **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）]** > [許可（Authorization）]
- [認証（Authentications）] > [フィルタ（Filters）]（エンドポイント カラムおよび ID カラム）
- グローバル検索（Global search）
- **[操作（Operations）] > [レポート（Reports）]** > [レポートフィルタ（Reports Filters）]

- **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [エンドポイントデバッグ（Endpoint Debug）]**

次の Cisco ISE API ウィンドウには、完全な MAC アドレス（「:」または「-」、あるいは「.」で区切られた 6 オクテット）が表示されます。

- [操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）]
- **[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）]**
- **[操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ポスチャのトラブルシューティング（Posture Troubleshooting）]**
- [管理（Administration）] > [ID（Identities）] > [エンドポイント（Endpoints）]
- **[管理（Administration）] > [システム（System）] > [展開（Deployment）]**
- **[管理（Administration）] > [ロギング（Logging）] > [収集フィルタ（Collection Filter）]**

REST API でも、完全な MAC アドレスの正規化がサポートされます。

オクテットの有効な範囲は、0 ー 9、a ー f、または A ー Fです。

Cisco ISE 展開のアップグレード

Cisco ISE では、管理ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードの進行状況とノードのステータスが Cisco ISE の GUI に表示されます。実行する必要があるアップグレード前およびアップグレード後のタスクについては、アップグレード先の Cisco ISE リリースの『Cisco Identity Services Engine Upgrade Guide』を参照してください。

アップグレードの [概要（Overview）] ウィンドウ（**[管理（Administration）] > [システム（System）] > [アップグレード（Upgrade）] > [概要（Overview）]**）には展開内のすべてのノード、それらのノードで有効になっているペルソナ、現在使用されている Cisco ISE のバージョン、および各ノードのステータス（そのノードがアクティブか非アクティブか）がリストされます。ノードが [アクティブ（Active）] な状態である場合にのみアップグレードを開始できます。

（注） Cisco ISE リリース 3.2 以降にアップグレードすると、ルート CA の再生成がアップグレードフローで自動的に行われます。したがって、アップグレード後のルート CA の再生成は必要ありません。

管理者アクセス コンソール

次の手順では、管理ポータルにログインする方法について説明します。

ステップ 1 Cisco ISE URL をブラウザのアドレス バーに入力します（たとえば https://<ise hostname or ip address>/admin/）。

ステップ 2 ユーザー名と、Cisco ISE の初期セットアップで指定して設定した大文字と小文字が区別されるパスワードを入力します。

ステップ 3 [ログイン（Login）] をクリックするか、Enter を押します。

ログインに失敗した場合は、[ログイン（Login）] ウィンドウの [ログインで問題が発生する場合（Problem logging in?）] リンクをクリックして、表示される手順に従ってください。

管理者ログインブラウザのサポート

Cisco ISE 管理ポータルは次の HTTPS 対応ブラウザをサポートしています。

- Mozilla Firefox 107 以前のバージョン（バージョン 82 以降）
- Mozilla Firefox ESR 102.4 以前のバージョン
- Google Chrome 107 以前のバージョン（バージョン 86 以降）
- Microsoft Edge の最新バージョンと最新バージョンより 1 つ前のバージョン

ISE コミュニティ リソース

ISE Pages Fail to Fully Load When Adblock Plus is Used

ログインの試行による管理者のロックアウト

管理者ユーザー ID に対して誤ったパスワードを何度も入力すると、アカウントは指定された時間一時停止されるか、またはロックアウトされます（設定による）。ユーザーをロックアウトするように Cisco ISE が設定されている場合、管理ポータルによってシステムからロックアウトされます。Cisco ISE は、サーバー管理者ログインレポートにログエントリを追加し、その管理者 ID のログイン情報を一時停止します。その管理者 ID のパスワードをリセットするには、『Cisco Identity Services Engine Installation Guide』の「Reset a Disabled Password Due to Administrator Lockout」のセクションでの説明に従います。管理者アカウントが無効になるまでに失敗できるログイン試行の回数は、『Cisco Identity Services Engine Administrator Guide』のセクションに記載されているとおりに設定されます。管理者ユーザーアカウントがロックアウトされると、関連付けられたユーザーに Cisco ISE から電子メールが送信されます（この情報が設定されている場合）。

ネットワーク管理者の役割を持つ管理者（Microsoft Active Directory ユーザーを含む）のみが、管理者アクセスを無効にするオプションを設定できます。

Cisco ISE でのプロキシの設定

既存のネットワークトポロジで、Cisco ISE が外部リソース（クライアント プロビジョニングやポスチャ関連のリソースがあるリモートのダウンロードサイトなど）にアクセスできるようにするためにプロキシサーバーを使用する必要がある場合は、管理ポータルを使用してプロキシ設定を行います。

プロキシ設定は次の Cisco ISE 機能に影響します。

- パートナー モバイル管理
- エンドポイント プロファイラ フィード サービスの更新
- エンドポイント ポスチャの更新
- エンドポイント ポスチャ エージェント リソースのダウンロード
- 証明書失効リスト（CRL）のダウンロード
- ゲスト通知
- SMS メッセージの送信
- ソーシャル ログイン
- Microsoft Entra ID
- pxGrid クラウド
- pxGrid Direct

Cisco ISE プロキシ設定はプロキシ サーバーの基本認証をサポートします。NT LAN Manager（NTLM）認証はサポートされていません。

（注） MDM の設定と統合の [OAuth Authentication Type] を選択すると、Cisco ISE はプロキシサーバーに NTLM 認証を使用します。

ステップ 1 Cisco ISE の GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロキシ（Proxy）]** を選択します。

ステップ 2 プロキシの IP アドレスまたは DNS 解決可能ホスト名を入力し、Cisco ISE との間のプロキシトラフィックを通過させるポートを [プロキシホストサーバー：ポート（Proxy host server : port）] フィールドに指定します。

ステップ 3 必要に応じて、[パスワード必須（Password required）] チェックボックスをオンにします。

ステップ 4 [ユーザー名（User Name）] フィールドと [パスワード（Password）] フィールドにプロキシサーバーへの認証に使用するユーザー名とパスワードを入力します。[パスワードの確認（Confirm Password）] フィールドにパスワードを再入力します。

ステップ 5 [次のホストとドメインに対するプロキシをバイパス（Bypass proxy for these hosts and domain）] テキストボックスに、バイパスする必要があるホストまたはドメインの IP アドレスまたはアドレス範囲を入力します。

ステップ 6 [保存（Save）] をクリックします。

管理ポータルで使用されるポート

管理ポータルは、HTTP ポート 80 と HTTPS ポート 443 を使用します。ユーザーはこれらの設定を変更できません。管理ポータルのリスクを軽減するために、これらのポートを使用するようにエンドユーザーポータルを設定することはできません。

Cisco ISE アプリケーション プログラミング インターフェイス ゲートウェイの設定

Cisco ISE の API ゲートウェイは、複数の Cisco ISE サービス API への単一のエントリポイントとして機能する API 管理ソリューションであり、セキュリティとトラフィック管理を向上させます。外部クライアントからの API 要求は、Cisco ISE の API ゲートウェイにルーティングされます。内部アルゴリズムに基づいて、サービス API が実行されている Cisco ISE ノードに要求が転送されます。

Cisco ISE リリース 3.1 以降、MnT（モニタリング）API、ERS API、およびオープン API はすべて API ゲートウェイを介してルーティングされます。API ゲートウェイノードと、それぞれの API の展開内の他のすべてのノード間で、次のポートを開く必要があります。

- MnT API：9443
- オープン API：9070
- ERS API：9060

API ゲートウェイを有効にする Cisco ISE ノードを選択できます。Cisco ISE 展開では、2 つ以上のノードで API ゲートウェイを実行することを推奨します。

ERS および Open API サービスがそのノードで無効になっている場合でも、API ゲートウェイは常にスタンドアロンノードで有効になります。分散展開の場合、API ゲートウェイが展開内の他のノードで有効になっていない場合に API ゲートウェイはデフォルトでプライマリ PAN で有効になります。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [API 設定（API Settings）] > [AIP ゲートウェイ設定（API Gateway Settings）]**。

ステップ 3 [ISE API ゲートウェイノードリスト（ISE API Gateway Nodes List）] 領域で、API ゲートウェイを有効にするノードの横にあるチェックボックスをオンにします。

ステップ 4 [有効化（Enable）] をクリックします。

トラブルシューティング

API ゲートウェイ関連の問題をトラブルシューティングするには、[デバッグログの設定（Debug Log Configuration）] ウィンドウで、次のコンポーネントの [ログレベル（Log Level）] を [デバッグ（DEBUG）] に設定します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグログの設定（Debug Log Configuration）]**

- **ise-kong**
- **kong**

ログは、[ログのダウンロード（Download Logs）] ウィンドウからダウンロードできます（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）]**）。[サポートバンドル（Support Bundle）] タブからサポートバンドルをダウンロード（タブの [ダウンロード（Download）] ボタンをクリック）するか、または [デバッグログ（Debug Logs）] タブから kong デバッグログをダウンロードします（**kong** デバッグログの [ログファイル（Log File）] の値をクリック）。

確認

Cisco ISE プライマリ PAN に毎回正常にログインできる場合は、API ゲートウェイの設定は想定どおりに機能しています。

（注） GUI にログインしている同じ Web ブラウザの別のタブにある API ゲートウェイを介して REST API にアクセスすると、GUI からログアウトします。

これは、API が API ゲートウェイノード以外のリモートノードによって提供されている場合にのみ発生します。

Cisco ISE 3.0 以降、ポート 443 の UI サービスは Docker サービスを介して提供されるため、複数のネットワークインターフェイスコントローラ（NIC）シナリオを含む場合に動作が変更される可能性があります。管理シェルから **ip route** コマンドを使用して、特定のニーズに基づいて目的のインターフェイスまたはゲートウェイを介してパケットがルーティングされるように、ルートを調整する必要がある場合があります。**ip route** コマンドの詳細については、『Cisco ISE CLI Reference Guide』の「Cisco ISE CLI Commands in Configuration Mode」の章を参照してください。

API サービスの有効化

Cisco ISE API サービスは、Cisco ISE 環境で Web アプリケーションを開発および展開するためのフレームワークを提供します。この機能は REST API をドキュメント化します。REST API を使用すると、さまざまな言語でコードを生成したり、API を理解するためにユーザー間でコードを共有したりできます。Cisco ISE API サービスは、REST API を記述するために業界で広く受け入れられている OpenAPI 仕様に基づいています。

API サービスにアクセスするには、API ゲートウェイを有効にする必要があります。すべての API サービス要求は、Cisco ISE のスタンドアロンと分散型の両方の展開で API ゲートウェイを介して Cisco ISE に入ります。API ゲートウェイは、ポート 443 を介して API サービス要求を受信します。

スタンドアロンの Cisco ISE ノードでは、API 要求を受信した後、API ゲートウェイは API サービスに要求を転送します。

分散環境では、読み取り要求は PSN またはプライマリ PAN のいずれかに転送されますが、書き込み要求はプライマリ PAN にのみ転送されます。プライマリ PAN は、展開環境で書き込み権限を持つ唯一のノードです。

Cisco ISE では、次の 2 種類の API 形式を使用して Cisco ISE ノードを管理するための API アクセスが可能です。

- **外部 RESTful サービス API**

  外部 RESTful サービス（ERS）API は、標準 HTTPS ポート 443（ポート 9060 も使用できます）で動作する HTTPS プロトコルに基づく REST API です。ERS API は基本認証をサポートしています。認証クレデンシャルは、暗号化され、要求ヘッダーの一部となっています。JAVA、cURL Linux コマンド、Python などの REST クライアントやその他のクライアントを使用して、外部 RESTful サービス API コールを呼び出すことができます。

（注）

- ERS API は TLS 1.1 および TLS 1.2 をサポートしていますが、[セキュリティ設定（Security Settings）] ウィンドウ（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]**）で TLS 1.0 を有効にした場合でも、TLS 1.0 をサポートしません。[セキュリティ設定（Security Settings）] ウィンドウで TLS 1.0 を有効にしても、EAP プロトコルのみに関係し、ERS API には影響しません。
- ERS セッションのアイドルタイムアウトは 60 秒です。この期間中に複数の要求が送信された場合、同じクロスサイトリクエスト フォージェリ（CSRF）トークンで同じセッションが使用されます。セッションがアイドル状態になっている時間が 60 秒を超えると、そのセッションはリセットされ、新しい CSRF トークンが使用されます。
- Cisco ISE 管理パスワードは、REST API を使用して変更することはできません。

ERS API の SDK 定義については、https://<*ise-ip*>:9060/ers/sdk または https://<ise-ip>/ers/sdk にアクセスしてください。この情報は、**[API設定（API Settings）]** ウィンドウ（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [API設定（API Settings）] > [概要（Overview）]**）の **[概要（Overview）]** セクションにもあります。

Cisco ISE の Amazon マシンイメージ（AMI）バージョンが VMware クラウド環境に展開されている場合、ERS サービスはデフォルトで有効になっています。これにより、Cisco ISE GUI から ERS サービスを有効にすることなく、Cisco ISE と他のシスコ製品およびサードパーティ製アプリケーションを簡単に統合できます。

（注） ユーザーデータの取得は、メタデータバージョン V1（IMDSv1）でのみ機能し、V2 では機能しません。

ERS の Open API 仕様

ERS API の Open API 仕様（JSON ファイル）は、Cisco ISE の [API設定（API Settings）] ウィンドウの [概要（Overview）] セクションでダウンロードできます（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [API設定（API Settings）] > [概要（Overview）]**）。この Open API JSON ファイルは、Python、JAVA などのプログラミング言語を使用した API クライアントコードの自動生成に使用できます。Open API の仕様とツールの詳細については、https://openapi.tools/ を参照してください。

- **オープン API**

オープン API は、ポート 443 で動作する HTTPS に基づく REST API です。Cisco ISE リリース 3.1 では、新しい API をオープン API 形式で使用できます。Cisco ISE オープン API の詳細については、https://<*ise-ip*>/api/swagger-ui/index.html または Cisco ISE Open API にアクセスしてください。

（注） Cisco ISE クラウドの設定で、AWS クラウド内の API ドキュメントページにアクセスするには、iptables を使用してファイアウォールルールを開く必要があります。

Cisco ISE リリース 3.1 では、次の Open API が導入されています。

- **リポジトリ**：これらの API は、リポジトリを管理する機能を提供します。リポジトリ設定を作成、取得、更新、および削除し、設定されたリポジトリからファイルを一覧表示できます。
- **バックアップと復元**：これらの API は、バックアップと復元の操作を管理する機能を提供します。設定のバックアップを作成、キャンセル、更新、および復元できます。また最後のバックアップのステータスを一覧表示できます。ユーザーはバックアップスケジュールを作成および編集することもできます。
- **証明書**：これらの API は、証明書を管理する機能を提供します。システム証明書と信頼できる証明書の作成、取得、更新、削除、証明書署名要求（CSR）の作成、および証明書のエクスポートとインポートが可能です。自己署名証明書 API の生成は、Cisco ISE リリース 3.1 パッチ 1 以降で使用できます。
- **ポリシー**：これらの API は、ポリシーを管理する機能を提供します。次の 2 つのタイプがあります。
  - **RADIUS ポリシー**：これらの API は、RADIUS ポリシーを管理する機能を提供します。必要なすべての境界（認証プロファイル、SecurityGroup、IdentityStore、プロファイル）とディスカバリ ディクショナリ フィルタ ヘルパーのリストを取得できます。これらの API により、ディクショナリと属性の管理、条件管理（ライブラリ、ネットワーク、時刻と日付の条件）、および AuthN ルール、Authz ルール、例外ルール、グローバル例外ルールを含むポリシーセットの管理が可能です。
  - **TACACS+ ポリシー**：これらの API は、TACACS+ ポリシーを管理する機能を提供します。必要なすべての境界（コマンドセット、TACACS プロファイル、IdentityStore、ServiceName）のリストと、TACACS ヘルパーに関連するディクショナリのディスカバリを取得できます。これらの API により、条件管理（ライブラリ、ネットワーク、時刻と日付の条件）、および AuthN ルール、Authz ルール、例外ルール、グローバル例外ルールを含むポリシーセットの管理が可能です。
- **TrustSec**：これらの API は、仮想ネットワーク（VN）、セキュリティグループ - 仮想ネットワークマッピング（SG-VN マッピング）、VN-VLAN マッピングなどの TrustSec 関連の操作を管理します。

- **タスクサービス**：これらのAPIは、CiscoISEで実行されるさまざまなタスクのステータスをモニターする機能を提供します。
- **展開**：これらの API は、Cisco ISEノードを設定し、展開を設定する機能を提供します。
- **パッチおよびホットパッチ**：これらの API は、パッチのインストール、パッチの削除、インストールされているすべてのパッチの一覧表示など、パッチ関連の操作を実行する機能を提供します。

（注） この API は、プライマリ PAN サービスが稼働している場合にのみ機能します。プライマリ PANサービスがダウンしている場合、セカンダリ PAN の API コールは失敗します。

- **ライセンス**：これらのAPIは、スマートライセンスを登録、有効化、および管理する機能を提供します。
- **システム設定**：これらの API は、Cisco ISE でプロキシ設定を構成および更新する機能を提供します。

Cisco ISE リリース 3.2 では、次の Open API が導入されています。

- **pxGrid Direct**：これらの API は、pxGrid Direct コネクタを作成する機能を提供します。

（注） サブネットからの OpenAPI 要求に存在する IP アドレスは、そのネットワークからのリモート IP アドレスとして表示されることが予想されます。

APIサービスで操作するユーザーに特別な権限を割り当てる必要があります。APIサービスユーザーは、内部ユーザーか、または外部の Microsoft Active Directory グループに所属することができます。内部ユーザーまたは外部ユーザーが所属する Active Directory グループは [ERS 管理者（ERS Admin）] または [ERS オペレータ（ERS Operator）] のグループのいずれかにマッピングする必要があります。

- [ERS管理者（ERS Admin）]：これらのユーザーは外部RESTfulサービスAPI要求を作成、読み取り、および削除できます。すべての外部 RESTful サービス API（GET、POST、DELETE、および PUT）へのフルアクセスを備えています。
- [ERSオペレータ（ERS Operator）]：これらのユーザーには読み取り専用アクセス（GET 要求のみ）があります。
- [MnT管理者（MnT Admin）]：これらのユーザーはモニタリング REST API の作成、読み取り、更新、および削除ができます。

（注） スーパー管理者ロールを持つユーザーは、すべての API サービスにアクセスできます。

[管理（Admin）] > **[システム（System）]** > **[管理アクセス（Admin Access）]** > **[認証（Authentication）]** > **[認証方式（Authentication Method）]** ウィンドウで、API 管理や OpenAPI 管理などの API 管理ユーザーの認証設定をします。[API認証タイプ（API Authentication Type）] セクションでは、パスワードベースまたは証明書ベースの認証、あるいはその両方を許可できます。これらの認証設定は、pxGrid REST、MnT REST、およびその他の REST の管理ユーザーなどの REST 管理ユーザーには適用されません。

[認証方式（Authentication Method）] ウィンドウで、[アイデンティティソース（Identity Source）] ドロップダウンリストから、選択した API 認証設定に適用するオプションを選択します。ただし、証明書ベースの API 認証では、**内部** ID ソースのみがサポートされます。

証明書ベースの認証のために信頼できる証明書ストアにインポートする証明書は、次の点で信頼されている必要があります。

1. ISE 内の認証への信頼
2. クライアント認証およびsyslogへの信頼
3. 管理者認証に基づく証明書への信頼

Cisco ISE リリース 3.4 以降、OpenAPI はデフォルトで有効になっています。ERS API サービスはデフォルトで無効になっています。Cisco ISE で API サービスを有効にする前に API コールを呼び出すと、エラーメッセージが表示されます。Cisco ISE REST API 用に開発されたアプリケーションを Cisco ISE にアクセスできるようにするには、Cisco ISE REST API 機能を有効にします。ERS API は標準 HTTPS ポート 443（ポート 9060 も使用できます）を使用し、Open API は HTTPS ポート 9070 を使用します。これらのポートはどちらも、デフォルトで無効になっています。Cisco ISE 管理サーバーで API サービスが有効になっていない場合、クライアントアプリケーションはゲスト REST API 要求に対してサーバーからタイムアウトエラーを受信します。

ステップ 1 Cisco ISE の GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[API設定（API Settings）]** > **[APIサービス設定（API Service Settings）]** を選択します。

ステップ 2 [プライマリ管理ノードのAPIサービス設定（API Service Settings for Primary Administration Node）] 領域で、[ERS（読み取り/書き込み）（ERS (Read/Write)）] トグルボタンをクリックしてプライマリ管理ノード（PAN）の外部 RESTful サービスを有効にします。Cisco ISE リリース 3.4 以降、OpenAPI はデフォルトで有効になっています。

ステップ 3 [他のすべてのノードのAPIサービス設定（API Service Settings for All Other Nodes）] 領域で、[ERS（読み取り/書き込み）（ERS (Read/Write)）] トグルボタンをクリックして他のすべてのノードで外部 RESTful サービスを有効にします。Cisco ISE リリース 3.4 以降、OpenAPI はデフォルトで有効になっています。

ステップ 4 [CSRFチェック（CSRF Check）] 領域で、次のオプションのいずれかのオプションボタンをクリックします。

- [セキュリティの強化に CSRF チェックを使用する（Use CSRF Check for Enhanced Security）]：このオプションを有効にした場合、外部 RESTful サービスクライアントは GET 要求を送信して Cisco ISE から CSRF トークンを取得し、Cisco ISE に送信する要求内にその CSRF トークンを含める必要があります。その後、Cisco ISE は、外部 RESTful サービスクライアントから要求を受信したときに CSRF トークンを検証します。Cisco ISE は、トークンが有効な場合にのみ要求を処理します。このオプションは、Cisco ISE リリース 2.3 より前のリリースの外部 RESTful サービスクライアントには適用されません。
- [ERS 要求に対して CSRF を無効にする（Disable CSRF for ERS Request）]：このオプションを有効にすると、CSRF 検証は実行されません。このオプションは、Cisco ISE リリース 2.3 より前のリリースの外部 RESTful サービスクライアントに使用できます。

ステップ 5 [保存（Save）] をクリックします。

（注） Cisco ISE ノードが PAN に登録されると、OpenAPI はデフォルトで以前の有効な状態から無効になります。上記の手順に従って、Cisco ISE GUI で OpenAPI を再度有効にして、ゼロタッチ OpenAPI 展開を維持します。

Cisco ISE は、GET 操作と UPDATE 操作に異なる API を提供します。

GET：

- URL：https://<ise-node>/admin/API/apiService/get
- **応答**：{"id": "1234","papIsEnabled":false,"psnsIsEnabled":true}

UPDATE：

- URL：https://<ise-node>/admin/API/apiService/update
- **要求の本文**：{"papIsEnabled":false,"psnsIsEnabled":false}
- **応答**：{"id": "1234","papIsEnabled":false,"psnsIsEnabled":false}

トラブルシューティング

すべての REST 操作が監査され、ログがシステム ログに記録されます。オープン API に関連する問題をトラブルシューティングするには、[デバッグログの設定（Debug Log Configuration）] ウィンドウで **apiservice** コンポーネントの [ログレベル（Log Level）] を [デバッグ（DEBUG ）] に設定します。ERS API 関連の問題をトラブルシューティングするには、[デバッグログの設定（Debug Log Configuration）] ウィンドウ（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグログの設定（Debug Log Configuration）]**）で ers コンポーネントの [ログレベル（Log Level）] を [デバッグ（DEBUG ）] に設定します。

[ログのダウンロード（Download Logs）] ウィンドウ（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）]**）からログをダウンロードできます。[サポートバンドル（Support Bundle）] タブからサポートバンドルをダウンロード（タブの [ダウンロード（Download）] ボタンをクリック）するか、または [デバッグログ（Debug Logs）] タブから **API サービス**のデバッグログをダウンロード（api-service デバッグログの [ログファイル（Log File）] の値をクリック）します。

確認

API サービス GUI ページ（https://<*iseip*>:<*port*>/api/swagger-ui/index.html または https://<*iseip*>/ers/sdk など）にアクセスできる場合、API サービスは期待どおりに動作しています。

関連トピック

外部 RESTful サービスソフトウェア開発キット （530 ページ）

API サービスの外部 Active Directory アクセスの有効化

ステップ 1 Cisco ISE の GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）] > [ID 管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 外部ユーザーが所属する Active Directory グループを外部 ID ソースとして追加します。

ステップ 3 Active Directory からユーザーグループを追加します。

ステップ 4 Cisco ISE の GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）] > [管理アクセス（Admin Access）] > [認証（Authentication）] > [認証方式（Authentication Method）]** を選択します。

ステップ 5 [ID ソース（Identity Source）] ドロップダウンリストから [AD：<参加ポイント名>（AD:<Join Point Name>）] を選択します。

ステップ 6 [パスワードベース（Password Based）] または [クライアント証明書ベース（Client Certificate Based）] のいずれかの認証を対応するオプションボタンをクリックして選択します。

ステップ 7 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]** を選択します。

ステップ 8 管理グループのリストから [ERS管理者（ERS Admin）] グループまたは [ERSオペレータ（ERS Operator）] をクリックします。

ステップ 9 [追加（Add）] をクリックして外部グループをメンバーユーザーとして管理者グループに追加します。

ステップ 10 [保存（Save）] をクリックします。

（注） Cisco ISE リリース 3.1 では、Cisco ISE GUI（[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]）で管理者アクセス用に外部 ID ストアが設定されている場合、内部管理者ユーザーに ERS 管理者ロールを割り当てることはできません。外部管理者ユーザーのみに ERS 管理者ロールを割り当てることができます。

外部 RESTful サービスソフトウェア開発キット

独自のツールを作成するには、外部 RESTful サービス（ERS）のソフトウェア開発キット（SDK）ページを使用できます。URL https://<ISE-ADMIN-NODE>:9060/ers/sdk で、外部 RESTful サービス SDK にアクセスできます。[ERS管理者（ERS Admin）] のロールを持つユーザーのみが、外部 RESTful サービス SDK にアクセスできます。

SDK は、次のコンポーネントで構成されています。

- クイックリファレンス API マニュアル
- すべての利用可能な API 操作の完全なリスト
- ダウンロード可能なスキーマファイル
- ダウンロード可能な Java のサンプルアプリケーション
- cURL スクリプト形式の使用例
- Python スクリプト形式の使用例
- Chrome POSTMAN の使用方法

Data Connect

Data Connect 機能は Cisco ISE へのデータベースアクセスを提供するため、データベースサーバーを直接照会して、選択したレポートを生成できます。データへの読み取りアクセスのみが提供されます。

ビジネス要件に応じて、ネットワークに関する構成または運用データを抽出し、それを使用して洞察に富んだレポートとダッシュボードを生成できます。

次のセクションでは、Cisco ISE で Data Connect 機能を有効にし、クライアントから Cisco ISE へのデータベース接続を正常に確立する方法と、この機能を展開する際に留意すべきさまざまな考慮事項について説明します。

Data Connect を正常に設定し、Cisco ISE へのデータベース接続を確立したら、「Data Connect on DevNet」を参照して、使用可能なビューと使用例の詳細を確認してください。

Data Connect ライセンスの要件

Data Connect 機能には、Essentials Cisco ISE ライセンスが必要です。

アクセスライセンスが期限切れになるか、非準拠になった場合、この機能は無効になり、現在のデータベースセッションは終了し、ライセンスが更新されるまで新しいセッションは許可されません。有効な Essentials Cisco ISE ライセンスなしにこの機能の API 要求を実行しようとすると、その API 要求は失敗します。

Data Connect に対する展開変更の影響

プライマリ モニタリング ペルソナとセカンダリ モニタリング ペルソナの両方で構成される分散型の展開の場合、Data Connect 機能が有効になっていると、デフォルトではセカンダリモニタリング（MnT）ノードで Data Connect 機能がアクティブになります。これは、プライマリ MnT ノードが展開全体のログの収集、有用なレポートへの変換、および他の機能に使用される一方、セカンダリ MnT ノードの負担は比較的少ないためです。

（注） セカンダリ MnT ノードのアイドル状態のリソースを利用して負荷を分散するため、セカンダリ MnT ノードでこの機能を有効にすることを推奨します。

次のシナリオでは、環境での展開またはペルソナの変更によって Data Connect 機能がどのように影響を受けるかについて説明します。

- セカンダリ MnT ノードを展開に追加すると、Data Connect がプライマリ MnT ノードですでに有効になっている場合、変更は生じず、この機能はプライマリ MnT ノードで有効のままになります。セカンダリ MnT ノードを追加した後に、この機能を無効にしてから有効にすると、Data Connect 機能はセカンダリ MnT ノードで有効になります。
- プライマリ MnT ペルソナを無効にすると、Data Connect が有効になっているセカンダリ MnT ノードがプライマリ MnT ノードに昇格され、Data Connect は同じノードで有効のままになります。
- セカンダリ MnT ノードが展開から手動で削除された場合、Data Connect 機能は自動的にプライマリ MnT ノードで有効になります。[Data Connect] ウィンドウの [ホスト名（Hostname）] フィールドは、プライマリ MnT ノードを指すようになりました。Data Connect 機能が有効になっているホスト名に注意してください。

専用 MnT

Data Connect が有効になっている専用 MnT ノードを使用した展開の場合、エンドポイントデータベースのクエリと構成データは、プライマリポリシー管理ノード（PAN）に内部的にルーティングされます。

PAN フェールオーバー

PAN フェールオーバーは、専用 MnT ノードがない場合、または Data Connect が無効になっている専用の MnT ノードがある場合、Data Connect 機能に影響しません。Data Connect が有効に

なっている専用 MnT ノードがある場合、古いプライマリ PAN のデータベースビューが削除され、新しいデータベースビューが新しいプライマリ PAN に作成されます。

（注） Data Connect 機能がノードで無効になり、別のノードで有効になるたびに、そのノードの管理証明書がインポートされます。新しい証明書を再度ダウンロードし、エンドクライアントにアップロードして、セッションを再確立する必要があります。ノードの変更が発生するたびに、アラームと監査ログが生成されて通知します。

Data Connect の有効化

始める前に

リソースを最適に使用するためのレポートを生成する場合にのみ、Data Connect 機能を有効にすることをお勧めします。

ステップ 1 Cisco ISE の GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[Data Connect]** を選択します。

ステップ 2 [Data Connect] トグルボタンをクリックして、Data Connect 機能を有効にします。

ステップ 3 パスワードを入力します。

パスワード長は 12 ～ 30 文字で、1 つ以上の大文字（A ～ Z）、1 つ以上の小文字（a ～ z）、1 つ以上の数字（0 ～ 9）、および 1 つ以上の特殊文字（#$%&*+,-.:;=?^_~）を含める必要があります。

（注） このパスワードはいつでもリセットできます。パスワードをリセットする場合は、それまでの 5 つのパスワードと同じものにならないようにします。パスワードは頻繁に変更することをお勧めします。

ステップ 4 パスワードを確認します。

ステップ 5 [パスワードの有効期限（Password Expiry）] フィールドに、パスワードをリセットするまでの日数を入力します。

有効な範囲は、1 ～ 3650 日です。デフォルト値は 90 日です。

ステップ 6 [保存（Save）] をクリックします。

パスワードを設定すると、[Data Connect] ウィンドウに以下の詳細情報が表示されます。これらの詳細情報は、スクリプトや SQL クライアントツールを使用して Cisco ISE モニタリングデータベースに接続しようとするときに必要です。

- [ユーザー名（Username）] : ユーザー名は **dataconnect** に設定されます。これはデフォルトで設定されており、変更できません。
- [ホスト名/IP（Hostname / IP）] : Data Connect 機能が有効になっているモニタリングノードのホスト名を表示します。

- [ポート（Port）]：TCP ポート 2484 は、Oracle TCPS（SSL を使用した TCP）プロトコルを介した Cisco ISE へのデータベース接続の確立に使用されます。
- [サービス名（Service Name）]：サービス名は **cpm10** に設定されます。これはデフォルトで設定されており、変更できません。
- [パスワードの有効期限 （Password Expires on）]：パスワードの有効期限が切れる日付と時刻を表示します。

次のタスク

1. Data Connect での管理者証明書の使用。
2. JAVA や Python などのプログラミング言語、または Oracle SQL Developer、JDBC クライアントなどの SQL クライアントツールを使用して、Cisco ISE へのデータベース接続を確立します。詳細については、クライアントから Cisco ISE データベースへの接続を参照してください。

（注） 間違ったパスワードを使用して Cisco ISE データベースに 6 回以上接続しようとすると、アカウントが 24 時間ロックされ、ODBC SQL クライアントツールに次のエラーメッセージが表示されます。

ORA-28000：アカウントはロックされています。（ORA-28000: The account is locked.）

回避するには、Cisco ISE GUI から（上記の手順のステップ 1 の後、3 ～ 6 を実行する）、または OpenAPI を使用して、Data Connect パスワードをリセットします。その後、新しいパスワードを使用してデータベースに接続できるようになります。あるいは、ロックが解除されるまで 24 時間待つことも可能です。その後は再び古いパスワードを使用してログインできます。

Data Connect での管理者証明書の使用

Data Connect 機能は、既存の管理者証明書を使用し、TCPS（SSL を使用した TCP）プロトコルを使用してセキュアな通信チャネルを作成します。この接続を確立するには、該当の信頼できる証明書がクライアントの信頼ストアに存在する必要があります。管理者証明書が CA により発行されたものか、自己署名証明書であるかによって、Data Connect に接続するためにインポートする必要がある証明書は異なります。

- **管理者証明書が CA により発行されたものである場合**：管理者証明書が CA によって発行された場合、クライアントは、管理者証明書の署名に使用された証明書チェーンの一部であるすべての証明書を取得する必要があります。この証明書チェーンは、クライアントの信頼できるウォレットにインポートする必要があります。ただし、管理者証明書をインポートする必要はありません。

- **管理者証明書が自己署名証明書である場合**：管理者証明書が自己署名証明書の場合は、管理者証明書をクライアントの信頼ストアにインポートする必要があります。次の手順を使用して、管理者証明書をインポートします。

1. Cisco ISE の管理者ポータルで、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書管理（Certificate Management）]** > **[システム証明書（System Certificates）]**を選択します。
2. **管理者証明書**という名前の証明書の横にあるチェックボックスをオンにします。
3. [エクスポート（Export）] をクリックします。

   管理者証明書がローカルマシンにダウンロードされます。これをクライアントの信頼ストアに追加して、TCPS 接続を確立します。

次のタスク

JAVA や Python などのプログラミング言語、または Oracle SQL Developer、JDBC クライアントなどの SQL クライアントツールを使用して、Cisco ISE へのデータベース接続を確立します。詳細については、クライアントから Cisco ISE データベースへの接続を参照してください。

使用可能なデータベースビューとその用途については、データベースビューを参照してください。

Data Connect のモニタリング

Data Connect のアラートとアラームは、次のシナリオで生成されます。

- **ライセンスの有効期限**：Essentials ライセンスの有効期限が切れると、Cisco ISE GUI と Data Connect 機能が無効になります。
- **パスワードの有効期限**：Data Connect パスワードの有効期限が切れた場合、Cisco ISE へのデータベース接続を正常に確立するためにパスワードをリセットする必要があります。
- **証明書の有効期限**：Data Connect 証明書の有効期限が切れた場合は、証明書を再生成し、クライアントで更新して、Cisco ISE へのデータベース接続を正常に確立する必要があります。

[構成変更の監査（Change Configuration Audit）] ログ（**[運用（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[監査（Audits）]** > **[構成変更の監査（Change Configuration Audit）]**）は、Data Connect 機能が管理者によって有効または無効にされたときに、またはペルソナの変更が行われた場合に生成されます。このログには、機能がいつ有効または無効にされたか、どのノードで変更が行われたか、および変更が Cisco ISE GUI から行われたか、OpenAPI を使用して行われたかに関する情報が提供されます。このレポートには、サードパーティ製ツールを使用して作成されたログインに関する情報は含まれません。

Data Connect のロギング

Data Connect に関連する GUI および Open API の変更に関する追加のログは、**ise-psc.log** で入手できます。

データベース接続と実行されたクエリは、Cisco ISE ログから追跡またはデバッグできません。管理者が Cisco ISE からの上位クエリを追跡する場合、管理者は AWR レポートを含むサービスバンドルを生成できます。AWR レポートには、最大の時間とリソースを消費した上位 5 つのクエリが含まれます。

システム時刻とネットワークタイムプロトコルサーバー設定の指定

Cisco ISE では、NTP サーバーを 3 台まで設定することができます。正確な時刻を維持し、異なるタイムゾーンの間で時刻を同期するために NTP サーバーを使用します。また、Cisco ISE が認証済みの NTP サーバーのみを使用する必要があるかどうかを指定したり、そのために 1 つまたは複数の認証キーを入力することもできます。

すべての Cisco ISE ノードを協定世界時（UTC）のタイムゾーンに設定することを推奨します（特に Cisco ISE ノードが分散展開されてインストールされている場合）。この手順では、展開内のさまざまなノードからのレポートとログのタイムスタンプが常に同期されるようにします。

Cisco ISE は、NTP サーバーの公開キー認証をサポートしています。NTP バージョン 4 は対称キー暗号化を使用します。また、公開キー暗号化に基づく新しい Autokey セキュリティモデルも提供します。公開キー暗号化は、対称キー暗号化よりも安全であると見なされています。これは、セキュリティが各サーバーによって生成され、公開されないプライベート値に基づいているためです。Autokey セキュリティモデルでは、すべてのキー配布および管理機能には公開値のみが含まれているため、キーの配布と保管が大幅に簡素化されます。

コンフィギュレーション モードで Cisco ISE の CLI から NTP サーバーに Autokey セキュリティモデルを設定できます。敵味方識別（IFF）システムは最も広く採用されているシステムであるため、このシステムを使用することを推奨します。

始める前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

展開内にプライマリとセカンダリの両方の Cisco ISE ノードがある場合は、各ノードのユーザーインターフェイスにログインし、システム時刻と Network Time Protocol（NTP）サーバーの設定を行います。

ステップ 1 Cisco ISE の GUI で [メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [システム時刻（System Time）]** を選択します。

ステップ 2 [NTPサーバーの設定（NTP Server Configuration）] 領域で、NTP サーバーの一意の IP アドレス（IPv4 または IPv6 または完全修飾ドメイン名（FQDN））を入力します。

ステップ 3 （オプション）秘密キーを使用してNTPサーバーを認証する場合に、指定したサーバーのいずれかが認証キーによる認証を必要としている場合は、[NTP認証キー（NTP Authentication Keys）] タブをクリックし、1 つ以上の認証キーを指定します。次の手順を実行します。

a) [追加（Add）] をクリックします。

b) [キーID（Key ID）] フィールドと [キー値（Key Value）] フィールドに必要な値を入力します。[HMAC] ドロップダウンリストから、必要なハッシュメッセージ認証コード（HMAC）値を選択します。[キーID（Key ID）] フィールドは 1 ～ 65535 の数値をサポートし、[キー値（Key Value）] フィールドは最大 15 文字の英数字をサポートします。

c) [OK] をクリックします。

d) [NTPサーバーの設定（NTP Server Configuration）] タブに戻ります。

ステップ 4 （オプション）公開キー認証を使用して NTP サーバーを認証するには、CLI から Cisco ISE に Autokey セキュリティモデルを設定します。Cisco ISE のリリースについては、『Cisco Identity Services Engine CLI Reference Guide』の **ntp server** コマンドと **crypto** コマンドを参照してください。

ステップ 5 [保存（Save）] をクリックします。

（注） 3 つ以上の NTP サーバーを使用すると、サーバーの 1 つに障害が発生した、または 2 つのサーバーが同期しない場合でも、ネットワーク全体での正確な時刻の同期を保証します。https://insights.sei.cmu.edu/blog/best-practices-for-ntp-services を参照してください。

システムのタイムゾーンの変更

一度設定すると、管理ポータルからのタイムゾーンの編集はできません。タイムゾーン設定を変更するには、Cisco ISE CLI で次のコマンドを入力します。

clock timezone タイムゾーン

clock timezone コマンドの詳細については、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

（注） Cisco ISE は、タイムゾーン名と出力の省略形に Portable Operating System Interface（POSIX）スタイルの記号を使用します。そのため、グリニッジの西にあるゾーンはプラス記号を持ち、グリニッジの東にあるゾーンはマイナス記号を持ちます。たとえば、TZ='Etc/GMT+4' はグリニッジ標準時（UT）の 4 時間遅れに対応します。

⚠

注意 インストール後に Cisco ISE アプライアンスでタイムゾーンを変更すると、その特定のノードで Cisco ISE サービスが再起動します。メンテナンスウィンドウ内でこのような変更を行うことを推奨します。また、単一 CIsco ISE 展開内のすべてのノードが同じタイムゾーンに設定されていることが重要です。複数の Cisco ISE ノードが異なる地理的な場所やタイムゾーンにある場合は、すべての Cisco ISE ノードで UTC などのグローバルなタイムゾーンを使用する必要があります。

通知をサポートするための SMTP サーバーの設定

次の目的で電子メール通知を送信できるように、Cisco ISE の SMTP サーバーを設定します。

- アラーム。
- スポンサーがログインクレデンシャルとパスワードのリセット手順に関する電子メール通知をゲストに送信する場合。
- ゲストが自身を正常に登録した後でログインクレデンシャルを自動的に受け取る場合と、ゲストアカウントが期限切れになる前にゲストに求められるアクション。

アラーム通知の受信者は、[電子メールにシステムアラームを含む（Include system alarms in emails）] オプションが有効になっている内部管理者ユーザーです。アラーム通知を送信する送信者の電子メールアドレスは、デフォルトで ise@<hostname> として設定されていますが、必要に応じて設定することもできます。送信者の電子メールアドレスを設定するには、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarm Settings）] > [アラーム通知（Alarm Notification）]** の順にクリックし、**[送信者の電子メールを入力：（Enter sender e-mail:）]** フィールドに入力します。

次の表に、電子メールを送信する分散 Cisco ISE 環境内のノードを示します。

表 *22 :* 電子メールを送信する *Cisco ISE* ノード

電子メールの目的	電子メールを送信するノード
ゲストアクセスの有効期限	プライマリポリシー管理ノード（PAN）
アラーム	MnT モニタリングおよびトラブルシューティング ノード（MnT）
ゲストポータルとスポンサーポータルからのスポンサー通知とゲスト通知	ポリシーサービスモード（PSN）
パスワードの有効期限	プライマリ PAN

Simple Mail Transfer Protocol（SMTP）サーバーを設定するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMTPサーバー（SMTP Server）]** を選択します。次のフィールドを設定します。

- [SMTPサーバーの設定（SMTP Server Settings）] 領域で、次の手順を実行します。
  - [SMTPサーバー（SMTP Server）]：アウトバウンド SMTP サーバーのホスト名を入力します。
  - [SMTPポート（SMTP Port）]：SMTP ポート番号を入力します。SMTP サーバーに接続するには、このポートが開かれている必要があります。
  - [接続タイムアウト（Connection Timeout）]：Cisco ISE が新しい接続を開始する前に SMTP サーバーへの接続を待機する最大時間を入力します。タイムアウト値は秒単位で設定します。
- セキュアな SMTP サーバーと通信するには、[暗号化設定（Encryption Settings）] で [TLS/SSL 暗号化を使用（Use TLS/SSL Encryption）] をオンにします。セキュアソケットレイヤ（SSL）を使用する場合は、SMTP サーバーのルート証明書を Cisco ISE の信頼できる証明書に追加します。
- [認証設定（Authentication Settings）] 領域で、[パスワード認証を使用する（Use Password Authentication）] チェックボックスをオンにして、SSL の代わりに認証にユーザー名とパスワードを使用します。

セキュアなロック解除クライアントメカニズムの有効化

セキュアなロック解除クライアントメカニズムは、Cisco ISE の CLI でルートシェルへのアクセスを一定期間にわたって提供します。セッションを終了するか、または閉じた場合、ルートアクセスも無効になります。

セキュアなロック解除機能は、同意トークンツールを使用して実装されます。同意トークンは、お客様とシスコの両方からの相互の同意が得られた後でのみ、信頼できる方法でシスコ製品の特権アクセスを安全に付与するための統一された多要素認証方式です。

Cisco ISE CLI でルートシェルを有効にするには、次の手順を実行します。

ステップ 1 Cisco ISE CLI で、**permit rootaccess** と入力します。

```
ise/admin# permit rootaccess
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
```

ステップ 2 オプション **1** を選択して、同意トークンチャレンジを生成します。

```
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
```

```
3. Show History
4. Exit
Enter CLI Option:
1
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
**********************************************************************************
GLOXgAAQEBAQAAABAgAEAAAAAMACmJxgibOhitBAQiUw+XeD3pnJ4HnJy3OXQABAAADhAGAANUOUHAZJUOVCQlQIAANUOUACcJIDUNQCNjgwIIFmzEtOWIOZS0wZjYIIRdlZDlMGQlM2UxNQ=
**********************************************************************************
Starting background timer of 15mins
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
```

ステップ 3 同意トークンチャレンジを Cisco テクニカル アシスタンス センター（TAC）に送信します。

Cisco TAC は、送信される同意トークンチャレンジを使用して同意トークン応答を生成します。

ステップ 4 オプション **2** を選択してから、Cisco TAC により提供された同意トークン応答を入力します。

```
Enter CLI Option:
2
Please input the response when you are ready .........................
[redacted]
Response Signature Verified successfully !
Granting shell access
sh-4.2# ls
```

（注） 応答の署名の検証が成功すると、特権アクセスが有効になります。

次のタスク

シェルモードを終了するには、**exit** コマンドを実行します。

```
sh-4.2# exit
exit
Root shell exited
```

オプション **3** を選択して、ルートアクセスセッションの履歴を表示します。

```
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
3
**********************************
        SN No : 1
**********************************
Challenge
3WcyAAAQEBAQAAABAgAEAAAAAMAM89hCTWBAQc9yianfOC5il+8AQABAADhAGAANUOUHAZJUOVCQlQIAANUOUACcJIDUNQCNjgwIIFmzEtOWIOZS0wZjYIIRdlZDlMGQlM2UxNQ=
 generated at 2019-06-12 15:40:01.000
**********************************
        SN No : 2
**********************************
```

連邦情報処理標準モードのサポート

Cisco ISE は、組み込みの連邦情報処理標準（FIPS）140-2 検証済み暗号化モジュール、Cisco Common Cryptographic Module（証明書 #1643 および証明書 #2100）を使用します。FIPS 準拠要求の詳細については、『FIPS Compliance Letter』を参照してください。

FIPS モードを有効にすると、Cisco ISE 管理者インターフェイスのウィンドウの右上隅のノード名の左側に FIPS モード アイコンが表示されます。

Cisco ISE は、FIPS 140-2 標準でサポートされないプロトコルまたは証明書の使用を検出すると、準拠していないプロトコルまたは証明書の名前とともに警告を表示し、FIPS モードは有効になりません。必ず FIPS に準拠したプロトコルのみを選択し、FIPS モードを有効にする前に FIPS に非準拠の証明書を交換してください。

Cisco ISE にインストールされている証明書で使用されている暗号アルゴリズムまたはそのパラメータが FIPS でサポートされていない場合には、証明書を再発行する必要があります。

FIPS モードを有効にすると、次の機能が影響を受けます。

- SSL を介した Lightweight Directory Access Protocol（LDAP）

Cisco ISE による FIPS 140-2 準拠の有効化の手段として、RADIUS の共有秘密とキー管理が使用されます。FIPS モードが有効になると、FIPS 非準拠アルゴリズムを使用するすべての機能は失敗します。

FIPS モードを有効にする場合：

- EAP-TLS、PEAP、TEAP、EAP-TTLS および EAP-FAST ですべての FIPS 非準拠暗号スイートは無効になります。
- 証明書と秘密キーには、FIPS 準拠ハッシュと暗号化アルゴリズムのみを使用する必要があります。
- RSA 秘密キーには、2048 ビット以上を指定する必要があります。
- ECDSA 秘密キーには、224 ビット以上を指定する必要があります。
- DHE 暗号は、すべての Cisco ISE TLS クライアントの DH パラメータが 2048 ビット以上の場合に機能します。
- SHA-1 は、Cisco ISE ローカルサーバー証明書の生成に使用できません。
- pxGrid 証明書テンプレートの RSA キー サイズは、2048 ビット以上である必要があります。

（注） FIPS モードを有効にするには、pxGrid 証明書テンプレートの RSA 秘密キーのサイズが 2048 ビット以上である必要があります。キーサイズが不十分な場合、FIPS モードを有効にしようとするとエラーメッセージが表示されます。

- EAP-FAST の匿名 PAC プロビジョニングオプションは無効です。
- ローカル SSH サーバーは FIPS モードで動作します。
- RADIUS は次のプロトコルをサポートしていません。
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

FIPS モードを有効にすると、展開内のすべてのノードが自動的に再起動されます。Cisco ISE はローリング再起動を実行します。具体的には、最初にプライマリ PAN を再起動し、その後でセカンダリノードを 1 つずつ再起動します。そのため、設定を変更する前にダウンタイムを計画することをお勧めします。

ヒント データベース移行プロセスを行う場合は、移行が完了してから FIPS モードを有効にすることを推奨します。

Cisco ISE での連邦情報処理標準モードの有効化

Cisco ISE で FIPS モードを有効化するには、次の手順に従います。

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[FIPSモード（FIPS Mode]** を選択します。

ステップ 2 [FIPSモード（FIPS Mode）] ドロップダウンリストから [有効（Enabled）] を選択します。

ステップ 3 [保存（Save）] をクリックして、マシンを再起動します。

次のタスク

FIPS モードを有効にしたら、次の FIPS 140 準拠機能を有効にして設定します。

- 自己署名証明書の生成 （572 ページ）。
- 証明書署名要求の作成と認証局への送信 （596 ページ）。
- ネットワーク デバイス定義の設定 （1367ページ）に記載されているとおり、RADIUS 認証を設定します。

共通アクセスカード機能を使用して管理者アカウントの許可を有効にすることができます。許可のために共通アクセスカード機能を使用することは、厳密にはFIPS 140の要件ではありませんが、セキュアアクセスの手法としてよく知られており、複数の環境でFIPS 140準拠を強化するために使用されています。

管理者共通アクセスカード認証用の Cisco ISE の設定

始める前に

- （オプション）Cisco ISE で FIPS モードを有効にします。FIPS モードは証明書ベースの認証には必要ありませんが、この2つのセキュリティ手段は多くの場合、組み合わせて使用されます。Cisco ISE を FIPS 140 準拠の環境に展開し、共通アクセスカード証明書ベースの認証を使用する予定の場合は、FIPS モードを有効にし、適切な秘密キーと暗号化/復号化設定を最初に指定します。
- Cisco ISE のドメイン ネーム サーバー（DNS）が Active Directory に設定されていることを確認します。
- Active Directory のユーザーとユーザー グループ メンバーシップが、管理者証明書ごとに定義されていることを確認します。

Cisco ISE による管理者の認証と許可を、ブラウザから送信された共通アクセスカードベースのクライアント証明書に基づいてできるようにします。これには、次を設定します。

- 外部 ID ソース（次の例では Active Directory）
- 管理者が所属する Active Directory のユーザーグループ
- ユーザーの ID を証明書の中で見つける方法
- Active Directory ユーザーグループから Cisco ISE RBAC 権限へのマッピング
- クライアント証明書に署名する認証局（信頼）証明書
- クライアント証明書が CA によって失効させられたかどうかを判断する方法

Cisco ISE にログインする場合、クレデンシャルを認証するために 共通アクセスカードを使用できます。

ステップ 1 FIPS モードを有効にすると、システムの再起動が求められます。認証局証明書もインポートする場合は、再起動を遅らせることができます。

ステップ 2 Cisco ISE の Active Directory ID ソースを設定し、Active Directory にすべての Cisco ISE ノードを追加します。

ステップ 3 ガイドラインに従って証明書認証プロファイルを設定します。

[プリンシパル名 X.509 属性（Principal Name X.509 Attribute）] フィールドでは、証明書内で管理者ユーザー名が格納されている属性を選択します。共通アクセスカードの場合は、カード上の署名証明書が通常は Active Directory でのユーザーの検索に使用されます。プリンシパル名は、この証明書の [サブジェクトの代替名（Subject Alternative Name）] 拡張情報（具体的には、この拡張情報の [別の名前（Other Name）] フィー

ルド）にあります。したがって、ここでは、属性として[サブジェクト代替名：別の名前（Subject Alternative Name - Other Name）] を選択します。

ユーザーの Active Directory レコードにユーザーの証明書が格納されている場合に、ブラウザから受信した証明書を Active Directory の証明書と比較するには、[証明書のバイナリ比較（Binary Certificate Comparison）] チェックボックスをオンにして、以前に指定した Active Directory インスタンス名を選択します。

ステップ 4 パスワードベースの管理者認証に Active Directory を有効にします。Cisco ISE に接続し結合された Active Directory インスタンス名を選択します。

（注） その他の設定が完了するまでは、パスワードベースの認証を使用します。この手順の最後に、認証タイプをクライアント証明書ベースに変更できます。

ステップ 5 外部管理者グループを作成して、Active Directory グループにマッピングします。Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次のように選択します。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]**。外部システム管理者グループを作成します。

ステップ 6 外部管理者グループに RBAC 権限を割り当てる管理者認証ポリシーを設定します。

注意 外部ネットワーク管理者グループを作成して Active Directory グループにマッピングし、ネットワーク管理者権限を持つ管理者認証ポリシー（メニューアクセスおよびデータアクセス）を設定して、Active Directory グループに少なくとも 1 人のユーザーを作成することを強く推奨します。このマッピングにより、[クライアント証明書ベースの認証（Client Certificate-Based Authentication）] が有効になると、少なくとも 1 人の外部管理者がスーパー管理者権限を持つことが保証されます。これができないと、Cisco ISE 管理者が管理ポータルの重要な機能から締め出される状況になる可能性があります。

ステップ 7 認証局証明書を Cisco ISE の信頼できる証明書ストアにインポートするには、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書ストア（Certificate Store）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

Cisco ISE がクライアント証明書を受け入れるには、そのクライアント証明書の信頼チェーン内の認証局証明書が Cisco ISE 証明書ストアの中にあることが条件となります。Cisco ISE 証明書ストアには適切な認証局証明書をインポートする必要があります。

a) [インポート（Import）] をクリックし、[証明書ファイル（Certificate File）] 領域で [ファイルの選択（Choose File）] をクリックします。
b) [クライアント認証を信頼（Trust for client authentication）] と **[Syslog]** チェックボックスをオンにします。
c) [送信（Submit）] をクリックします。

Cisco ISE は、証明書をインポートしたら展開内のすべてのノードを再起動することを促します。すべての証明書をインポートするまで、再起動を遅らせることができます。ただし、すべての証明書をインポートしたら、次に進む前に Cisco ISE を再起動する必要があります。

ステップ 8 失効ステータス確認のための認証局証明書を設定します。

a) **[管理（Administration）] > [システム（System ）] > [証明書（Certificates）] > [OSCP クライアントプロファイル（OSCP Client Profile）]**。

b) [追加（Add）] をクリックします。
c) 対応するフィールドに OSCP サーバーの名前、説明（任意）、サーバーの URL を入力します。
d) **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書ストア（Certificate Store）]**。
e) クライアント証明書に署名できる認証局証明書のそれぞれについて、その認証局の失効ステータスチェックを行う方法を指定します。リストから認証局証明書を選択して [編集（Edit）] をクリックします。[編集（Edit）] ページで、OCSP または証明書失効リスト（CRL）検証、あるいはその両方を選択します。OCSP を選択した場合は、認証局に使用する OCSP サービスを選択します。CRL を選択した場合は、CRL Distribution URL などの設定パラメータを指定します。

ステップ 9 クライアント証明書ベースの認証を有効にします。**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[認証（Authentication）]** を選択します。

a) [認証方式（Authentication Method）] タブで、[クライアント証明書ベース（Client Certificate Based）] オプションボタンを選択します。
b) [証明書認証プロファイル（Certificate Authentication Profile）] ドロップダウンリストから、以前に設定した証明書認証プロファイルを選択します。
c) [ID ソース（Identity Source）] から Active Directory インスタンス名を選択します。
d) [保存（Save）] をクリックします。

ここで、パスワード ベースの認証からクライアント証明書ベースの認証に切り替えます。設定済みの証明書認証プロファイルにより、管理者による証明書の認証方法を指定します。管理者は外部 ID ソースを使用して許可されます。この例では、Active Directory です。

Active Directory での管理者の検索には、証明書認証プロファイルからのプリンシパル名属性が使用されます。

サポートされる Common Access Card 標準

Cisco ISE は、共通アクセスカード認証デバイスを使用して自身を認証する米国政府ユーザーをサポートします。共通アクセスカードは特定の従業員を識別する一連の X.509 クライアント証明書を含む電子チップの認識票です。共通アクセスカードによるアクセスには、カードを挿入し PIN を入力するカードリーダーが必要です。カードからの証明書が Windows の証明書ストアに転送されます。Windows の証明書ストアは、Cisco ISE などのローカル ブラウザで実行されているアプリケーションで使用可能です。

Cisco ISE での共通アクセス カードの動作

Cisco ISE 認証がクライアント証明書を介してのみ行われるように、管理ポータルを設定できます。ユーザー ID またはパスワードを必要とするクレデンシャルベースの認証は許可されません。クライアント証明書ベースの認証では、共通アクセスカードを挿入して PIN を入力してから、ブラウザのアドレスフィールドに Cisco ISE 管理ポータルの URL を入力します。ブラウザによって証明書が Cisco ISE に転送され、Cisco ISE はログイン セッションを証明書の内容に基づいて認証および許可します。このプロセスが完了すると、[Cisco ISEモニタリングおよびトラブルシューティング（Cisco ISE Monitoring and Troubleshooting）] ホームページに表示され、ユーザーには適切な RBAC 権限が与えられます。

Diffie-Hellman アルゴリズムを使用したセキュアな SSH キー交換

Diffie-Hellman-Group14-SHA1 Secure Shell（SSH） キー交換のみを許可するように Cisco ISE を設定します。Cisco ISE の CLI コンフィギュレーション モード から次のコマンドを入力します。

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

次に例を示します。

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

セキュア syslog 送信のための Cisco ISE の設定

始める前に

Cisco ISE ノード間で、およびモニタリングノードに対して、TLS 保護されたセキュア syslog のみを送信するように Cisco ISE を設定するには、次の手順を実行します。

- 展開内のすべての Cisco ISE ノードに適切なサーバー証明書が設定されていることを確認します。FIPS 140 に準拠するように設定するには、証明書キーのキーサイズは 2048 ビット以上にする必要があります。
- 管理ポータルの FIPS モードを有効にします。
- デフォルト ネットワーク アクセス認証ポリシーが、あらゆるバージョンの SSL プロトコルを許可しないことを確認します。FIPS 認定アルゴリズムとともに、FIPS モードで TLS プロトコルを使用します。
- 展開内のすべてのノードがプライマリ PAN に登録されていることを確認します。また、展開の少なくとも 1 つのノードに、セキュア syslog レシーバ（TLS サーバー）としての動作が有効になっているモニタリングペルソナが含まれることも確認します。
- syslog でサポートされている RFC 標準規格を確認します。お使いのバージョンの Cisco ISE リリースの『Cisco Identity Services Engine Network Component Compatibility』ガイドを参照してください。

ステップ 1 セキュア syslog リモートロギングターゲットを設定します。

ステップ 2 セキュア syslog リモートロギングターゲットに監査可能なイベントを送信するロギングカテゴリを有効にします。

ステップ 3 TCP syslog および UDP syslog コレクタを無効にします。TLS 保護された syslog コレクタのみを有効にします。

（注） UDP syslog を MnT ノードに配信するために Cisco ISE メッセージングサービスの使用を有効にした場合、Cisco ISE リリース 2.6 以降のリリースには、TLS 保護された UDP syslog が含まれます。

セキュア syslog リモート ロギング ターゲットの設定

Cisco ISE システム ログは、さまざまな目的のために、ログ コレクタによって収集され保存されます。セキュアなsyslogターゲットを設定するには、モニタリングペルソナが有効になっている Cisco ISE ノードをログコレクタとして選択します。

ステップ 1 Cisco ISE 管理ポータルにログインします。

ステップ 2 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[リモート ロギング ターゲット（Remote Logging Targets）]** を選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 セキュア syslog サーバーの名前を入力します。

ステップ 5 [ターゲットタイプ（Target Type）] ドロップダウンリストから [セキュアな syslog（Secure Syslog）] を選択します。

ステップ 6 [ステータス（Status）] ドロップダウンリストで [有効化（Enabled）] を選択します。

ステップ 7 展開内の Cisco ISE モニタリングノードのホスト名と IP アドレスを [ホスト/IP アドレス（Host/IP Address）] フィールドに入力します。

ステップ 8 [ポート（Port）] フィールドに、ポート番号として *6514* を入力します。セキュア syslog レシーバは TCP ポート 6514 をリッスンします。

ステップ 9 [ファシリティコード（Facility Code）] ドロップダウンリストから syslog ファシリティコードを選択します。デフォルト値は [LOCAL6] です。

ステップ 10 対応する設定を有効にするには、次のチェックボックスをオンにします。

a) **[このターゲットのアラームを含める（Include Alarms For This Target）]**

b) **[RFC 3164 に準拠する（Comply to RFC 3164）]**

c) **[サーバー ID チェックを有効にする（Enable Server Identity Check）]**

ステップ 11 [サーバーダウンの場合はメッセージをバッファする（Buffer Messages When Server is Down）] チェックボックスをオンにします。このオプションがオンの場合、Cisco ISE は、セキュアな syslog レシーバが到達不能な場合にはログを格納し、セキュアな syslog レシーバを定期的に検査し、セキュア syslog レシーバが起動するとログを転送します。

a) [バッファサイズ（MB）（Buffer Size (MB)）] フィールドにバッファサイズを入力します。

b) Cisco ISE がセキュアな syslog レシーバを定期的に確認するように、[再接続時間（秒）（Reconnect Time (Sec)）] フィールドに再接続タイムアウト値を入力します。タイムアウト値は秒単位で設定します。

ステップ 12 [CA 証明書の選択（Select CA Certificate）] ドロップダウンリストから、Cisco ISE がセキュアな syslog サーバーに提示する必要がある CA 証明書を選択します。

ステップ 13 セキュアな syslog を設定するときに、[サーバー証明書の検証を無視（Ignore Server Certificate validation）] チェックボックスがオフになっていることを確認します。

ステップ 14 [送信（Submit）] をクリックします。

リモート ロギング ターゲットの設定

次の表では、外部の場所（syslog サーバー）を作成してロギングメッセージを保存するために使用する [リモートロギングターゲット（Remote Logging Targets）] ウィンドウのフィールドについて説明します。このウィンドウにアクセスするには、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモートロギングターゲット（Remote Logging Targets）]** を選択し、[追加（Add）] をクリックします。

表 *23 :* リモート ロギング ターゲットの設定

フィールド名	使用上のガイドライン
名前（Name）	新しい syslog ターゲットの名前を入力します。
ターゲットタイプ（Target Type）	ドロップダウンリストから、該当するターゲットタイプを選択します。デフォルト値は [UDP Syslog] です。
説明（Description）	新しいターゲットの簡単な説明を入力します。
IPアドレス（IP Address）	ログを格納する宛先マシンの IP アドレスまたはホスト名を入力します。Cisco ISE は、ロギング用に IPv4 形式と IPv6 形式をサポートします。
ポート（Port）	宛先マシンのポート番号を入力します。
ファシリティコード（Facility Code）	ロギングに使用する必要がある syslog ファシリティコードをドロップダウンリストから選択します。有効なオプションは、Local0 ～ Local7 です。
最大長（Maximum Length）	リモート ログ ターゲット メッセージの最大長を入力します。有効な値は 200 ～ 1024 バイトです。
このターゲットのアラームを含める（Include Alarms for this Target）	このチェックボックスをオンにすると、アラームメッセージもリモートサーバーに送信されます。
RFC 3164に準拠する（Comply to RFC 3164）	このチェックボックスをオンにすると、バックスラッシュ（\）が使用されている場合でも、リモートサーバーに送信される syslog メッセージのデリミタ（(, ; { } \ \）はエスケープされません。

フィールド名	使用上のガイドライン
サーバーダウン時のバッファメッセージ（Buffer Message When Server Down）	このチェックボックスは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [TCP Syslog] または [セキュアな syslog（Secure Syslog）] を選択すると表示されます。TCP syslog ターゲットまたはセキュアな syslog ターゲットが使用できないときに syslog メッセージを Cisco ISE がバッファできるようにするには、このチェックボックスをオンにします。Cisco ISE は、ターゲットへの接続が再開されるとターゲットへのメッセージの送信を再試行します。接続が再開されると、メッセージは最も古いものから順に送信されます。バッファされたメッセージは、常に新しいメッセージの前に送信されます。バッファがいっぱいになると、古いメッセージが廃棄されます。
バッファサイズ（MB）（Buffer Size (MB)）	各ターゲットのバッファサイズを設定します。デフォルトでは、100 MB に設定されます。バッファサイズを変更するとバッファがクリアされ、特定のターゲットのバッファリングされた既存のすべてのメッセージが失われます。
再接続タイムアウト（秒）（Reconnect Timeout (Sec)）	サーバーがダウンした場合に TCP とセキュアな syslog を破棄するまで保存する期間を設定する期間を秒単位で入力します。
CA証明書の選択（Select CA Certificate）	このドロップダウンリストは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [セキュアな syslog（Secure Syslog）] を選択すると表示されます。ドロップダウンリストからクライアント証明書を選択します。
サーバー証明書有効性を無視（Ignore Server Certificate validation）	このチェックボックスは、[ターゲットタイプ（Target Type）] ドロップダウンリストから [セキュアな syslog（Secure Syslog）] を選択すると表示されます。サーバー証明書の認証を無視し、syslog サーバーを許可するには、Cisco ISE のこのチェックボックスをオンにします。デフォルトでは、このオプションが無効になっているときにシステムが FIPS モードでない限り、このオプションはオフに設定されます。

関連トピック

Cisco ISE ロギング メカニズム （708 ページ）
Cisco ISE システム ログ （709 ページ）
Cisco ISE メッセージ カタログ （713 ページ）
収集フィルタ （714 ページ）
イベント抑制バイパス フィルタ （715 ページ）
リモート syslog 収集場所の設定 （710 ページ）
収集フィルタの設定 （715 ページ）

セキュア syslog ターゲットに監査可能なイベントを送信するためのロギング カテゴリの有効化

Cisco ISE によってセキュア syslog ターゲットに監査可能なイベントが送信されるようにするには、ロギングカテゴリを有効にします。

ステップ 1 Cisco ISE 管理ポータルで、**[メニュー（Menu）]**アイコン（☰）をクリックし、**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）**>**[ロギングカテゴリ（Logging Categories）]**を選択します。

ステップ 2 [管理および運用の監査（Administrative and Operational Audit）] ロギングカテゴリの横にあるオプション ボタンをクリックし、次に [編集（Edit）] をクリックします。

ステップ 3 [ログシビラティ（重大度）レベル（Log Severity Level）] ドロップダウンリストから [警告（WARN）] を選択します。

ステップ 4 [ターゲット（Targets）] 領域で、以前に作成したセキュアな syslog リモートロギングターゲットを、[選択済み（Selected）] 領域に移動します。

ステップ 5 [保存（Save）]をクリックします。

ステップ 6 次のロギングカテゴリを有効にする場合は、このタスクを繰り返し行います。これらのロギングカテゴリは両方とも、デフォルトログのシビラティ（重大度）レベルとして[情報（INFO）]を持ち、編集できません。

- [AAA 監査（AAA Audit）]
- [ポスチャおよびクライアントプロビジョニングの監査（Posture and Client Provisioning Audit）]

ロギングカテゴリの設定

次の表では、ロギングカテゴリを設定するために使用可能なフィールドについて説明します。ログのシビラティ（重大度）レベルを設定し、ロギングカテゴリのログにロギングターゲットを選択します。このウィンドウにアクセスするには、**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギングカテゴリ（Logging Categories）]**の順に選択します。

表示するロギングカテゴリの横のオプションボタンをクリックし、[編集（Edit）] をクリックします。次の表では、ロギングカテゴリの編集ウィンドウに表示されるフィールドについて説明します。

表 *24 :* ロギング カテゴリの設定

フィールド名	使用上のガイドライン
名前（Name）	ロギング カテゴリの名前を表示します。

フィールド名	使用上のガイドライン
ログのシビラティ（重大度）レベル（Log Severity Level）	一部のロギングカテゴリでは、この値はデフォルトで設定されており、編集できません。一部のロギングカテゴリでは、次のシビラティ（重大度）レベルのいずれかをドロップダウンリストから選択できます。 • [重大（FATAL）]：緊急事態レベル。このレベルは、Cisco ISE を使用できず、必要なアクションをただちに実行する必要があることを意味します。 • [エラー（ERROR）]：このオプションは、深刻な状態またはエラー状態を示します。 • [警告（WARN）]：このオプションは、通常の状態ではあるが重大な状態を示します。これは、多くのロギングカテゴリに設定されるデフォルトのレベルです。 • [情報（INFO）]：このレベルは、情報メッセージを示します。 • [デバッグ（DEBUG）]：このレベルは、診断バグメッセージを示します。
ローカルロギング（Local Logging）	ローカルノードでこのカテゴリのロギングイベントを有効にするには、このチェックボックスをオンにします。
ターゲット（Targets）	この領域では、左右の矢印アイコンを使用し、[使用可能（Available）]領域と [選択済み（Selected）] 領域間でターゲットを移動して、ロギングカテゴリのターゲットを選択できます。 [使用可能（Available）]領域には、ローカル（事前定義済み）と外部（ユーザー定義）の両方の既存のロギングターゲットが含まれています。 [選択済み（Selected）]領域（最初は空）には、カテゴリに選択されたターゲットが表示されます。

関連トピック

Cisco ISE メッセージ コード （712 ページ）
リモート syslog 収集場所の設定 （710 ページ）
メッセージ コードのシビラティ（重大度）レベルの設定 （712 ページ）

TCP syslog コレクタと UDP syslog コレクタの無効化

Cisco ISE が ISE ノード間でセキュアな syslog のみを送信するには、TCP と UDP syslog コレクタを無効にして、セキュアな syslog コレクタのみを有効にする必要があります。

（注） UDP syslog を MnT ノードに配信するために Cisco ISE メッセージングサービスの使用を有効にした場合、Cisco ISE リリース 2.6 以降のリリースには、TLS 保護された UDP syslog が含まれます。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** を選択します。

ステップ 2 TCP または UDP syslog コレクタの横にあるオプションボタンをクリックします。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 [ステータス（Status）] ドロップダウン リストから [無効化（Disabled）] を選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 すべての TCP または UDP syslog コレクタが無効になるまで、このプロセスを繰り返します。

デフォルトのセキュア syslog コレクタ

Cisco ISE には、MnT ノード用のデフォルトのセキュア syslog コレクタがあります。デフォルトでは、これらのデフォルト セキュア syslog コレクタにはロギング カテゴリはマッピングされません。デフォルト セキュア syslog コレクタの名前は次のとおりです。

- プライマリ MnT ノード：SecureSyslogCollector
- セカンダリ MnT ノード：SecureSyslogCollector2

[リモートロギングターゲット（Remote Logging Targets）]（**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモートロギングターゲット（Remote Logging Targets）]**）ウィンドウにこの情報を表示できます。デフォルトの syslog コレクタは削除できません。また、デフォルトの syslog コレクタの次のフィールドは更新できません。

- 名前（Name）
- ターゲットタイプ（Target Type）
- IP/ホストアドレス（IP/Host address）
- ポート（Port）

Cisco ISE の新規インストール時に、**Default Self-signed Server Certificate** という名前の証明書が信頼できる証明書ストアに追加されます。この証明書は、[クライアント認証と syslog 用に信頼する（Trust for Client authentication and Syslog）] の使用方法の場合にマークされ、セキュアな syslog の使用方法で利用できるようになります。展開を設定する場合または証明書を更新する場合には、関連する証明書をセキュア syslog ターゲットに割り当てる必要があります。

Cisco ISE のアップグレード時に、ポート 6514で MnT ノードを指す既存のセキュアな syslog ターゲットがある場合、ターゲットの名前と設定は保持されます。アップグレード後は、これらのsyslogターゲットを削除することはできません。また、次のフィールドを編集することもできません。

- 名前（Name）
- ターゲットタイプ（Target Type）
- IP/ホストアドレス（IP/Host address）
- ポート（Port）

アップグレードの時点でこのようなターゲットが存在しない場合、新規インストールの場合と同様にデフォルトのセキュアなsyslogターゲットが作成されますが、証明書のマッピングは行われません。これらのsyslogターゲットに関連証明書を割り当てることができます。どの証明書にもマッピングされていないセキュアなsyslogターゲットをロギングカテゴリにマッピングしようとすると、Cisco ISE は次のメッセージを表示します。

```
log_target_name の証明書を設定してください（Please configure the certificate for
log_target_name）
```

（注） 既存のターゲットのホスト名またはIPアドレスとポートを使用して、新しいロギングターゲットを作成することはできません。各ロギングターゲットには、一意のホスト名または IP アドレスとポートが必要です。

オフライン メンテナンス

メンテナンス時間が 1 時間未満の場合、Cisco ISE ノードをオフラインにしてメンテナンス作業を行います。ノードをオンラインに戻すと、メンテナンス時間中に行われたすべての変更が PAN ノードにより自動的に同期されます。変更が自動的に同期されない場合は、PAN を使用して手動で同期できます。

メンテナンス時間が1時間を超える場合は、メンテナンスの時点でノードを登録解除し、ノードを展開に再び追加するときにノードを再登録します。

処理があまり行われていない時間帯にメンテナンスをスケジュールすることが推奨されます。

（注）
1. キューに格納されているメッセージの数が 1,000,000 を超えるか、または Cisco ISE ノードが 6 時間を超えてオフラインになっている場合には、データの複製の問題が発生している可能性があります。
2. プライマリ MnT ノードでメンテナンスを行う場合は、メンテナンスアクティビティを実行する前に、MnT ノードの操作バックアップを作成しておくことを推奨します。

エンドポイント ログイン クレデンシャルの設定

[エンドポイントログイン設定（Endpoint Login Configuration）] ウィンドウでは、Cisco ISE がクライアントにログインできるようにログインクレデンシャルを設定します。このウィンドウで設定されたログインクレデンシャルは、次の Cisco ISE 機能で使用されます。

Cisco ISE の GUIで、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）] > [設定（Settings）]** を選択します。

次のタブが表示されます。

- [Windowsドメインユーザー（Windows Domain User）]：Cisco ISE が SSH 経由でクライアントにログインするために使用する必要があるドメインクレデンシャルを設定します。[+（Plus）] アイコンをクリックして、必要な数の Windows ログインを入力します。ドメインごとに、[ドメイン（Domain）]、[ユーザー名（Username）]、および [パスワード（Password）] の各フィールドに必要な値を入力します。ドメインクレデンシャルを設定すると、[Windowsローカルユーザー（Windows Local User）] タブで設定されたローカルユーザー クレデンシャルは無視されます。
- [Windowsローカルユーザー（Windows Local User）]：Cisco ISE が SSH 経由でクライアントにアクセスするために使用するローカルアカウントを設定します。このローカルアカウントで、PowerShell および PowerShell リモートを実行できる必要があります。
- [MACローカルユーザー（MAC Local User）]：Cisco ISE が SSH 経由でクライアントにアクセスするために使用するローカルアカウントを設定します。このローカルアカウントで、PowerShell および PowerShell リモートを実行できる必要があります。[ユーザー名（Username）] フィールドに、ローカルアカウントのアカウント名を入力します。Mac OS アカウント名を表示するには、ターミナルで次のコマンドを実行します。

```
whoami
```

Cisco ISE でのホスト名の変更

Cisco ISE では、CLI を介してのみホスト名を変更できます。詳細については、お使いのバージョンの『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

ホスト名を変更する前の考慮事項：

- ホスト名が変更されると、すべての Cisco ISE サービスがスタンドアロンノードレベルで自動的に再起動されます。
- このノードで CA 署名付き証明書が使用されていた場合は、正しいホスト名を使用してこの証明書を再度インポートする必要があります。
- このノードが新しい Active Directory ドメインに参加する場合は、ホスト名を変更する前に現在の Active Directory ドメインから脱退する必要があります。このノードが既存の Active

Directory ドメインにすでに参加している場合は、現在参加しているすべての参加ポイントに再参加して、現在と以前のホスト名と参加マシンアカウント名の不一致を避けることを強く推奨します。

- 内部 CA 署名付き証明書が使用されている場合は、ISE ルート CA 証明書を再生成する必要があります。
- ホスト名を変更すると、古いホスト名を使用している証明書が無効になります。そのため、新しいホスト名を使用する新しい自己署名証明書が、HTTPS または EAP で使用するために生成されます。

（注） 上記のすべての考慮事項は、ドメイン名の変更にも適用されます。

Cisco ISE での証明書の管理

証明書は、個人、サーバー、会社、または別のエンティティを識別し、そのエンティティを公開キーに関連付ける電子文書です。自己署名証明書は、作成者によって署名されます。証明書は、自己署名したり、外部の CA がデジタルで署名したりできます。CA 署名付きデジタル証明書は、業界標準であり、自己署名証明書よりセキュアです。

証明書は、ネットワークに対するセキュアなアクセスを提供するために使用されます。証明書は、エンドポイントに対して Cisco ISE ノードを識別し、そのエンドポイントと Cisco ISE ノード間の通信を保護します。

Cisco ISE は、次の目的で証明書を使用します。

- Cisco ISE ノード間の通信。
- Cisco ISE と syslog やフィードサーバーなどの外部サーバー間の通信。
- Cisco ISE と、ゲスト、スポンサー、BYOD ポータルなどのエンドユーザーポータル間の通信。

Cisco ISE 管理ポータルを通じて、展開内のすべてのノードの証明書を管理します。

セキュアなアクセスを可能にするための Cisco ISE での証明書の設定

Cisco ISE は、公開キーインフラストラクチャ（PKI）に依存し、エンドポイントおよび管理者の両方とのセキュアな通信とマルチノード展開内の複数の Cisco ISE ノード間のセキュアな通信を実現しています。PKI は X.509 デジタル証明書に依存して、メッセージの暗号化と復号化のための公開キーの転送、およびユーザーとデバイスを表す他の証明書の信頼性の検証を行います。Cisco ISE の管理ポータルでは、次の 2 つのカテゴリの X.509 証明書を管理できます。

- システム証明書：これらはクライアント アプリケーションに対して Cisco ISE ノードを識別するサーバー証明書です。各 Cisco ISE ノードには独自のシステム証明書があり、対応する秘密キーとともにノードに格納されています。

（注） Cisco ISE は、同じ秘密キーを持つ複数の証明書をインポートできません。証明書が更新され、秘密鍵を変更せずにインポートされた場合、既存の証明書はインポートされた証明書に置き換えられます。

- 信頼できる証明書：これらの証明書は、ユーザーやデバイスから受信した公開キーの信頼を確立するために使用される CA 証明書です。信頼できる証明書ストアには、Simple Certificate Enrollment Protocol（SCEP）から配信された証明書も含まれます。これにより、モバイルデバイスを企業ネットワークに登録できるようになります。信頼できる証明書はプライマリ PAN で管理され、Cisco ISE 展開内の他のすべてのノードに自動的に複製されます。

分散展開では、証明書を PAN の証明書信頼リスト（CTL）のみにインポートする必要があります。この証明書はセカンダリ ノードに複製されます。

Cisco ISE で証明書認証が証明書による確認機能のわずかな違いの影響を受けないようにするために、ネットワークに展開されているすべての Cisco ISE ノードには小文字のホスト名を使用してください。

証明書の使用

Cisco ISE に証明書をインポートする場合は、証明書の使用目的を指定します。Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates]** を選択し、[インポート（Import）] をクリックします。

次の使用方法の 1 つ以上を選択します。

- [管理者（Admin）]：ノード間通信と管理者ポータルの認証。
- [EAP 認証（EAP Authentication）]：TLS ベースの EAP 認証。
- [RADIUS DTLS]： RADIUS DTLS サーバー認証。
- [ポータル（Portal）]：すべての Cisco ISE エンドユーザーポータルとの通信。
- [SAML]：SAML 応答が正しい ID プロバイダーから受信されていることを確認。
- [pxGrid]：pxGrid コントローラとの通信。

管理ポータル（使用方法は管理）、pxGrid コントローラ（使用方法は pxGrid）との通信、および TLS ベースの EPA 認証（使用方法は EAP 認証）のための各ノードからさまざまな証明書を

関連付けます。ただし、これらの各目的に各ノードから関連付けることができる証明書は1つのみです。

Cisco ISE に証明書をインポートするごとに、その証明書に対して常に新しい秘密キーを使用する必要があります。複数の証明書にわたって秘密キーを再利用すると、Red Hat NSS データベースの制限により、アプリケーションの初期化エラーが発生する可能性があります。

新しい証明書が Red Hat NSS データベースにインポートされると、同じ秘密キーを持つ既存の証明書は上書きされます。管理者証明書の秘密キーが上書きされると、Cisco ISE アプリケーションの初期化が影響を受けます。

Web ポータル要求を処理できる展開に複数の PSN がある場合、Cisco ISE には一意の ID が必要です。この ID で、ポータルの通信に使用する必要がある証明書を識別します。ポータルでの使用に指定された証明書を追加またはインポートする場合、証明書グループタグを定義して、それを展開内の各ノードの対応する証明書に関連付けます。この証明書グループタグを対応するエンドユーザーポータル（ゲスト、スポンサー、およびパーソナルデバイスポータル）に関連付けます。この証明書グループタグは一意の ID で、Cisco ISE が各ポータルと通信する際に使用する必要がある証明書を識別する場合に役立ちます。ポータルごとに各ノードから指定できる証明書は 1 つのみです。

（注） EAP-TLS クライアント証明書では、以下の暗号に KeyUsage=Key Agreement と ExtendedKeyUsage=Client Authentication が必要です。

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS クライアント証明書では、以下の暗号に KeyUsage=Key Encipherment と ExtendedKeyUsage=Client Authentication が必要です。

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

この要件をバイパスするには、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）] の順に選択し、[目的の検証なしで証明書を受け入れる（Accept Certificates without Validating Purpose）] チェックボックスをオンにします。

Cisco ISE の証明書の一致

展開内で Cisco ISE ノードをセットアップすると、ノードが相互に通信します。システムは各 ISE ノードの FQDN を調べ、FQDN が一致することを確認します（たとえば ise1.cisco.com と ise2.cisco.com、またはワイルドカード証明書を使用している場合は *.cisco.com）。また、外部マシンから Cisco ISE サーバーに証明書が提示される場合、認証のために提示される外部証明書が、Cisco ISE サーバーの証明書と照合されます。2 つの証明書が一致すると、認証は成功します。

Cisco では、Cisco ノード間（2 ノードの場合）、または Cisco と pxGrid の間で照合が実行されます。

Cisco ISE は、サブジェクト名の一致を次のようにして確認します。

1. Cisco ISE により証明書のサブジェクト代替名の拡張が確認されます。サブジェクト代替名に 1 つ以上の DNS 名が含まれている場合は、それらの DNS 名の 1 つが Cisco ISE ノードの FQDN に一致している必要があります。ワイルドカード証明書が使用されている場合、ワイルドカード ドメイン名は Cisco ISE ノードの FQDN ドメインに一致している必要があります。
2. サブジェクト代替名に DNS 名が存在しない場合、またはサブジェクト代替名全体が欠落している場合は、証明書の [サブジェクト（Subject）] フィールドの一般名または証明書の [サブジェクト（Subject）] フィールドのワイルドカードドメインが、ノードの FQDN に一致している必要があります。
3. 一致しない場合、証明書は拒否されます。

（注） Cisco ISE にインポートされる X.509 証明書は、プライバシー強化メール（PEM）または識別符号化規則（DER）形式である必要があります。証明書チェーン（システム証明書、およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。

X.509 証明書の有効性

X.509 証明書が有効なのは、指定された特定の日付までです。システム証明書が期限切れになった場合、その証明書に依存する Cisco ISE 機能が影響を受けます。Cisco ISE は、有効期限が 90 日以内になると、システム証明書の有効期間の残りについて通知します。この通知は、いくつかの方法で表示されます。

- 配色された有効期限の状態アイコンが、[システム証明書（System Certificates）] ウィンドウに表示されます。このウィンドウを表示するには、[Menu（メニュー）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書の管理（Certificate Management）] > [システム証明書（System Certificates）]** を選択します。
- 期限切れメッセージが Cisco ISE システム診断レポートに表示されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）]>**

[レポート（Reports）] > **[レポート（Reports）]** > **[診断（Diagnostics）]** > **[システム診断（System Diagnostic）]** を選択します。

- 有効期限のアラームは、有効期限の 90 日前、60 日前、30 日間に生成されます。有効期限のアラームは、有効期限前の最後の 30 日間には毎日生成されます。

失効した証明書が自己署名証明書の場合は、この証明書を編集して有効期限を延長できます。認証局署名付き証明書の場合は、認証局から新しい証明書を取得するのに十分な期間を確保する必要があります。

Cisco ISE での公開キーインフラストラクチャの有効化

PKI は、セキュアな通信を可能にし、デジタル署名を使用してユーザーの ID を確認する暗号化技術です。

ステップ 1 展開内の各ノードで次のシステム証明書を設定します。

- EAP-TLS などの TLS 対応認証プロトコル。
- 管理ポータルの認証。
- ブラウザと REST クライアントを使用した Cisco ISE Web ポータルへのアクセスの許可。
- pxGrid コントローラへのアクセスの許可。

デフォルトで、Cisco ISE ノードには EAP 認証と、管理ポータル、エンドユーザーポータル、および pxGrid コントローラへのアクセスに使用される自己署名証明書があらかじめインストールされています。一般的な企業環境では、この自己署名証明書は、信頼できる CA によって署名されたサーバー証明書に置き換えられます。

ステップ 2 信頼できる証明書ストアに、ユーザーとの信頼を確立するために使用される CA 署名証明書と、Cisco ISE に提示されるデバイス証明書を配置します。

ルート CA 証明書と 1 つ以上の中間 CA 証明書で構成されている証明書チェーンでユーザーまたはデバイス証明書の信頼性を確認するには、次の手順を実行します。

- ルート CA に関連する信頼オプションを有効にします。

  Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] を選択します。このウィンドウで、ルート CA 証明書のチェックボックスをオンにし、[編集（Edit）] をクリックします。[使用状況（Usage）] 領域で、[信頼先（Trusted For）] 領域内の必要なチェックボックスをオンにします。

ノード間の通信では、Cisco ISE 展開内の各ノードに所属する管理者システム証明書を検証する信頼証明書を、信頼できる証明書ストアに配置する必要があります。デフォルトの自己署名証明書をノード間通信に使用するには、この証明書を Cisco ISE の各ノードの [システム証明書（System Certificates）] ウィンドウからエクスポートし、信頼できる証明書ストアにインポートします。自己署名証明書を CA 署名証明書で置

き換える場合に必要なのは、適切なルート CA 証明書と中間 CA 証明書を信頼できる証明書ストアに配置することだけです。この手順を完了するまでは、ノードを Cisco ISE 展開に登録できません。

展開内でクライアントと PSN の間のセキュアな通信に自己署名証明書を使用する場合、BYOD ユーザーがある場所から別の場所に移動すると、EAP-TLS ユーザー認証は失敗します。一部の PSN 間で提供される必要があるこのような認証要求の場合、外部で署名された CA 証明書を使用してクライアントと PSN の間の通信を保護するか、または外部の CA によって署名されたワイルドカード証明書を使用する必要があります。

公開署名証明書を取得する場合、または Cisco ISE 展開が FIPS モードで動作する場合は、すべてのシステム証明書および信頼できる証明書が FIPS 準拠であることを確認する必要があります。つまり、各証明書のキー サイズが 2048 バイト以上であり、SHA-1 または SHA-256 暗号化を使用する必要があります。

（注） スタンドアロンの Cisco ISE または PAN からバックアップを取得した後に、展開内の 1 つ以上のノードの証明書設定を変更する場合は、データを復元するために別のバックアップを取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。

ワイルドカード証明書

ワイルドカード証明書はワイルドカード表記（ドメイン名の前にアスタリスクとピリオドの形式）を使用しており、組織内の複数のホスト間で証明書を共有できます。たとえば、証明書サブジェクトの **CN** 値は aaa.ise.local などの汎用ホスト名であり、SAN フィールドには、同じ汎用ホスト名と DNS.1=aaa.ise.local や DNS.2=*.ise.local などのワイルドカード表記が含まれます。

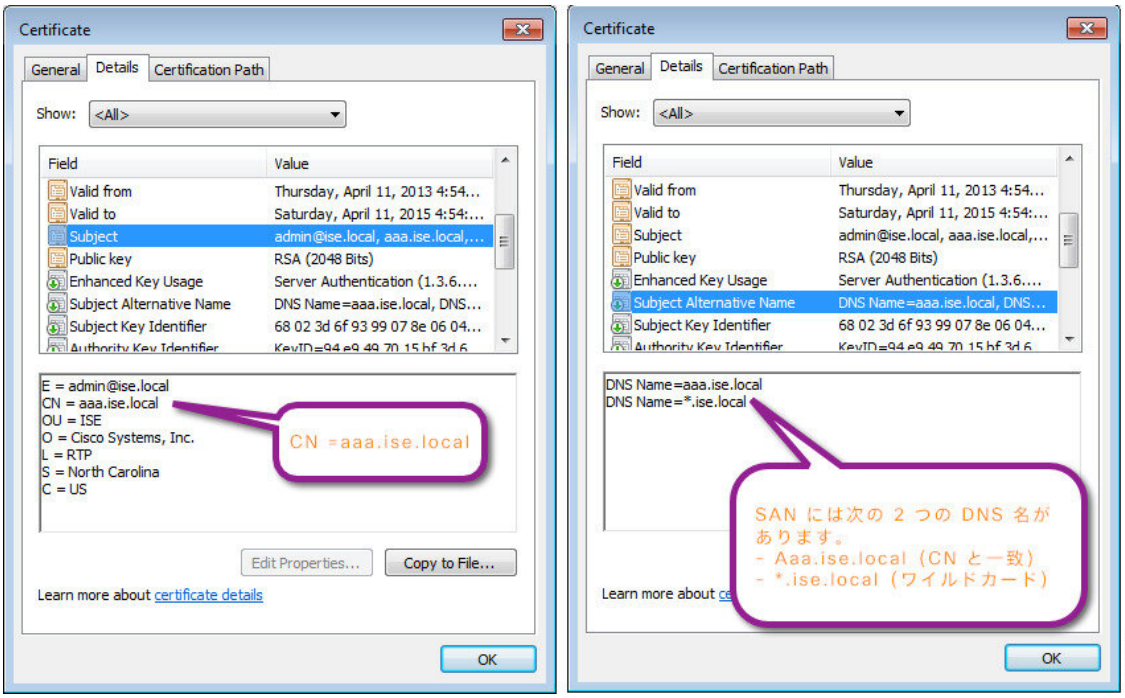
psn.ise.local. のように *.ise.local を使用してワイルドカード証明書を設定すると、その同じ証明書を使用して、次のような DNS 名が「.ise.local」で終了する他のすべてのホストを保護することができます。

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

ワイルドカード証明書は通常の証明書と同じ方法で通信を保護し、要求は同じ検証方式を使用して処理されます。

次の図に、Web サイトの保護に使用されるワイルドカード証明書の例を示します。

図 *8 :* ワイルドカード証明書の例



Cisco ISE のワイルドカード証明書のサポート

Cisco ISE はワイルドカード証明書をサポートしています。以前のリリースの Cisco ISE では、HTTPS に対して有効になったすべての証明書を検証し、[共通名（Common Name）] フィールドがホストの FQDN と正確に一致することを確認していました。フィールドが一致しない場合、その証明書は HTTPS 通信に使用できませんでした。

以前のリリースの Cisco ISE では、[共通名（Common Name）] 値を使用して、url-redirect A-V ペア文字列の変数を置き換えていました。この共通名の値は、すべての Centralized Web Authentication（CWA）、オンボーディング、ポスチャ リダイレクションなどに使用されました。

Cisco ISE は共通名として ISE ノードのホスト名を使用します。

HTTPS と拡張認証プロトコル通信用のワイルドカード証明書

SSL/TLS トンネリングを使用する 管理（Web ベースのサービス）と EAP プロトコルに対して、Cisco ISE でワイルドカードサーバー証明書を使用できます。ワイルドカード証明書を使用する場合は、Cisco ISE の各ノードに固有の証明書を生成する必要はありません。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用して展開内の複数のノードで単一の証明書を共有することができ、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書の使用は、各 Cisco ISE ノードに固有のサーバー証明書を割り当てる場合よりも安全性が低いと見なされます。

ゲストポータルに公開ワイルドカード証明書を割り当て、ルート CA 証明書を使用してサブ CA をインポートする場合、Cisco ISE サービスが再起動されるまで証明書チェーンは送信されません。

（注） ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、重大なセキュリティ問題が発生する可能性があります。

ワイルドカード証明書では、ドメイン名の前にアスタリスク（*）とピリオドが使用されます。たとえば、証明書のサブジェクト名の共通名の値は aaa.ise.local などの汎用ホスト名になり、SAN フィールドには *.ise.local のようなワイルドカード文字が入力されます。Cisco ISE は、ワイルドカード証明書（提示される識別子の一番左の文字がワイルドカード文字（*））をサポートします。たとえば、*.example.com または *.ind.example.com です。提示される識別子に他の文字とワイルドカード文字が含まれた証明書はサポートされません。たとえば、abc*.example.com、a*b.example.com、または *abc.example.com です。

（注） CN または SAN でワイルドカード文字（*）を使用してノードに CSR を生成する場合、証明書はワイルドカードと見なされます。Cisco ISE はそれを PAN に追加し、他のすべてのノードに複製します。

URL リダイレクションの完全修飾ドメイン名

認証プロファイルのリダイレクトは、中央 Web 認証、デバイス登録 Web 認証、ネイティブサプリカントのプロビジョニング、モバイルデバイスの管理、クライアントのプロビジョニング、およびポスチャサービスのために実行されます。Cisco ISE が認証プロファイルのリダイレクトを作成すると、結果の cisco-av-pair には次のような文字列が含まれます。

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

この要求を処理するときに、Cisco ISE は文字列の一部のキーワードを実際の値で置き換えます。たとえば、SessionIdValue は、要求の実際のセッション ID に置き換えられます。eth0 インターフェイスの場合、Cisco ISE は URL 内の IP を Cisco ISE ノードの FQDN で置き換えます。eth0 以外のインターフェイスの場合、Cisco ISE は URL 内の IP アドレスを使用します。インターフェイス eth1 から eth3 にはホストのエイリアス（名前）を割り当てることができます。このエイリアスは Cisco ISE が URL リダイレクション中に IP アドレスの代わりに置き換えることができます。

これを行うために、次のように、Cisco ISE CLI の ISE /admin(config)# プロンプトからコンフィギュレーション モードで **ip host** コマンドを使用します。

ip host *IP_address host-alias FQDN-string*

ここで、*IP_address* はネットワーク インターフェイス（eth1 または eth2 または eth3）の IP アドレスで、*host-alias* はネットワーク インターフェイスに割り当てる名前です。*FQDN-string*

は、ネットワーク インターフェイスの完全修飾ドメイン名です。このコマンドを使用して、ネットワーク インターフェイスに *host-alias* または *FQDN-string* あるいはその両方を割り当てることができます。

ip host コマンドの使用例：ip host a.b.c.d sales sales.amerxyz.com

eth0 以外のインターフェイスにホストエイリアスを割り当てたら、**application start ise** コマンドを使用して Cisco ISE でアプリケーション サービスを再起動します。

このホストエイリアスのネットワーク インターフェイスとの関連付けを削除するには、次のようにこのコマンドの **no** 形式を使用します。

no ip host *IP_address host-alias FQDN-string*

ホストのエイリアスの定義を表示するには、**show running-config** コマンドを使用します。

FQDN-string を指定している場合は、その FQDN で URL 内の IP アドレスが置き換えられます。ホストエイリアスのみを指定した場合は、Cisco ISE はそのホストエイリアスと設定された IP ドメイン名を結合して完全な FQDN を形成し、URL 内の IP アドレスをその FQDN で置き換えます。ネットワーク インターフェイスをホストのエイリアスにマッピングしない場合は、URL 内のネットワーク インターフェイスの IP アドレスが使用されます。

クライアントのプロビジョニング、ネイティブサプリカント、またはゲストフローに対して eth0 以外のインターフェイスを使用する場合は、eth0 以外のインターフェイスの IP アドレスまたはホストエイリアスが PSN 証明書の SAN フィールドに適切に設定されていることを確認します。

ワイルドカード証明書を使用する利点

- コスト削減：サードパーティ CA によって署名された証明書は、特にサーバーの数が増えると高額になります。ワイルドカード証明書は、Cisco ISE 展開内の複数ノードで使用できます。
- 運用効率：ワイルドカード証明書により、すべての PSN が EAP と Web サービス用に同じ証明書を共有できます。証明書を 1 回作成して、すべての PSN に適用することにより、コストを大幅に削減できるだけでなく、証明書の管理も簡素化されます。
- 認証エラーの削減：ワイルドカード証明書は、クライアントがプロファイル内に信頼できる証明書を保存しており、そのクライアントが iOS のキーチェーン（署名ルートが信頼されている）に従っていない Apple iOS デバイスで発生する問題に対処します。iOS クライアントが最初に PSN と通信する際、このクライアントはその PSN の証明書を（信頼できる CA が署名している場合でも）明示的に信頼しません。ワイルドカード証明書を使用すると、この証明書がすべての PSN で同一になるため、ユーザーは証明書の受け入れを 1 回行えばよく、その後の異なる PSN に対する認証はエラーやプロンプトが表示されることなく進行します。
- 簡略化されたサプリカントの設定：たとえば、PEAP-MSCHAPv2 と信頼できるサーバー証明書がある Microsoft Windows サプリカントでは、各サーバー証明書を信頼するように指定することが必要とされており、そのように指定さしない場合は、そのクライアントが別の PSN を使用して接続を行うと、各 PSN 証明書を信用するように、ユーザーにプロンプ

トが出される可能性があります。ワイルドカード証明書を使用すると、各 PSN の個別の証明書ではなく、単一のサーバー証明書を信頼するだけで済みます。

- ワイルドカード証明書を使用すると、プロンプトの提示が減り、よりシームレスな接続が実現されることにより、ユーザー エクスペリエンスが改善されます。

ワイルドカード証明書を使用することの欠点

次に、ワイルドカード証明書の使用に関連するセキュリティ上の考慮事項の一部を説明します。

- 監査性と否認防止性の低下
- 秘密キーの露出の増加
- 一般的ではなく、管理者により理解されていない

ワイルドカード証明書は各 Cisco ISE ノードで固有のサーバー証明書を使用するよりも安全性が低いと見なされています。ただし、コスト、およびその他の運用関連の要因がセキュリティリスクに勝っています。

Cisco 適応型セキュリティアプライアンスなどのセキュリティデバイスも、ワイルドカード証明書をサポートしています。

ワイルドカード証明書を展開する場合には注意が必要です。たとえば、*.company.local を使用して証明書を作成したとします。該当の秘密キーを攻撃者が回復できた場合、攻撃者は company.local ドメイン内のすべてのサーバーをスプーフィングすることができます。したがって、このタイプの危険を回避するために、ドメイン領域を分割することがベストプラクティスと見なされています。

この想定される問題に対処し、利用範囲を制限するために、ワイルドカード証明書を使用して組織の特定のサブドメインを保護することもできます。ワイルドカードを指定する一般名のサブドメイン領域に、アスタリスク（*）を追加します。

たとえば、*.ise.company.local に対してワイルドカード証明書を設定すると、その証明書は次のような、DNS 名が「.ise.company.local」で終わるすべてのホストを保護するために使用できます。

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

ワイルドカード証明書の互換性

ワイルドカード証明書は通常、証明書サブジェクトの共通名としてリストされているワイルドカードを使用して作成されます。Cisco ISE は、このタイプの作成をサポートします。ただし、すべてのエンドポイントサプリカントが証明書サブジェクトのワイルドカード文字をサポートしているわけではありません。

テスト済みのすべてのMicrosoftネイティブサプリカント（販売が終了しているWindows Mobileを含む）の一部は、証明書サブジェクトのワイルドカード文字をサポートしていません。

Network Access Managerなど、[サブジェクト（Subject）]フィールドでのワイルドカード文字の使用をサポートできる他のサプリカントを使用できます。

また、DigiCertのWildcard Plusなど、証明書のサブジェクト代替名に特定のサブドメインを含めることで、互換性のないデバイスを使用するように設計された、特別なワイルドカード証明書を使用することもできます。

Microsoftサプリカントの制限はワイルドカード証明書の使用にとって妨げになるように見えますが、Microsoftのネイティブサプリカントを含む、セキュアなアクセスについてテスト済みのすべてのデバイスを使用できるようにする代替の方法があります。

これを行うには、サブジェクトにワイルドカード文字を使用する代わりに、[サブジェクト代替名（Subject Alterative Name）]フィールドでワイルドカード文字を使用する必要があります。[サブジェクト代替名（Subject Alternative Name）]フィールドには、ドメイン名（DNS名）を確認するように指定された拡張子が保持されます。詳細については、RFC 6125とRFC 2128を参照してください。

証明書階層

[管理（Administration）]ポータルには、すべてのエンドポイント、システム、および信頼できる証明書の証明書階層または信頼書信頼チェーンが表示されます。証明書階層には、証明書、すべての中間CA証明書、およびルート証明書が含まれています。たとえば、[管理（Administration）]ポータルからシステム証明書を表示すると、デフォルトの対応するシステム証明書の詳細が表示されます。証明書階層は、証明書の上部に表示されます。詳細を表示するには、その階層で証明書をクリックします。自己署名証明書には階層または信頼チェーンがありません。

証明書のリストウィンドウで、[ステータス（Status）]列に次のアイコンのいずれかが表示されます。

- 緑色のアイコン：有効な証明書（有効な信頼チェーン）を示します。
- 赤色のアイコン：エラーを示します（たとえば、信頼証明書の欠落または期限切れ）。
- 黄色のアイコン：証明書が期限切れ間近であることを警告し、更新処理を求めます。

システム証明書

Cisco ISEシステム証明書は、展開内のその他のノードおよびクライアントアプリケーションに対してCisco ISEノードを識別するサーバー証明書です。システム証明書の用途は次のとおりです。

- Cisco ISE展開でノード間通信に使用されます。これらの証明書の[使用方法（Usage）]領域で[管理（Admin）]チェックボックスをオンにします。

- Cisco ISE Web ポータルに接続するブラウザおよび REST クライアントで使用されます。これらの証明書の [使用方法（Usage）] 領域の [ポータル（Portal）] チェックボックスをオンにします。
- PEAP および EAP-FAST を使用する外部 TLS トンネルを形成するために使用されます。EAP-TLS、PEAP、および EAP-FAST による相互認証の場合、[使用方法（Usage）] 領域の [EAP 認証（EAP Authentication）] チェックボックスをオンにします。
- RADIUS DTLS サーバー認証に使用されます。
- SAML ID プロバイダーとの通信に使用されます。この証明書の [使用方法（Usage）] 領域の [SAML] チェックボックスをオンにします。[SAML] オプションを選択すると、その他のサービスにこの証明書を使用することはできません。

  SAML 証明書は、ポスチャサービスや Cisco ISE と Cisco Smart Software Manager 間のライセンス通信など、複数の Cisco ISE サービスで使用されます。Cisco ISE から SAML 証明書を削除すると、関連するサービスが中断されます。
- pxGrid コントローラとの通信に使用されます。これらの証明書の [使用方法（Usage）] 領域の [pxGrid] チェックボックスをオンにします。

Cisco ISE 展開の各ノードに有効なシステム証明書をインストールします。デフォルトでは、インストール時に Cisco ISE ノードに 2 つの自己署名証明書と、内部 Cisco ISE CA により署名された 1 つの証明書が作成されます。

- [EAP]、[管理（Admin）]、[ポータル（Portal）]、および [RADIUS DTLS] のための自己署名サーバー証明書（キー サイズは 2048 で 1 年間有効です）。
- SAML ID プロバイダーとの安全な通信に使用できる自己署名 SAML サーバー証明書（キー サイズは 2048 で 1 年間有効です）。
- pxGrid クライアントとの安全な通信に使用できる内部 Cisco ISE CA 署名付きサーバー証明書（キー サイズは 4096 で 1 年間有効です）。

展開をセットアップし、セカンダリノードを登録すると、pxGrid コントローラ用の証明書が自動的にプライマリノードの CA 署名付き証明書に置き換わります。したがってすべての pxGrid 証明書が同一 PKI トラスト階層の一部となります。

（注）

- ワイルドカードシステム証明書をエクスポートして、（ノード間通信用に）他のノードにインポートする場合は、必ず証明書と秘密キーをエクスポートして、暗号化パスワードを指定してください。インポート時は、証明書、秘密キー、および暗号化パスワードが必要です。
- Cisco ISE では、EAP-TLS 認証の信頼できる証明書およびエンドポイント証明書に対してのみ、RSASSA-PSS アルゴリズムの使用がサポートされています。証明書を表示すると、署名アルゴリズムは、アルゴリズム名ではなく、1.2.840.113549.1.1.10 としてリストされます。

  Cisco ISE では、署名アルゴリズムとして RSASSA-PSS を使用するシステム証明書はサポートされていません。これは、サーバー証明書、ルート証明書、および中間 CA 証明書に適用されます。
- クラウド形成テンプレート（CFT）を使用して Cisco ISE を AWS に展開すると、[システム証明書（System Certificates）] ウィンドウに DefaultISE.ise.com ベースの証明書が表示される場合があります。これは、Cisco ISE の機能には影響しません。CA 証明書が再生成されると、それらの追加の証明書はアクティブにならず、無視できます。

お使いのリリースでサポートされているキーと暗号については、該当バージョンの『 Cisco Identity Services Engine Network Component Compatibility 』ガイドを参照してください。

セキュリティを強化するために、自己署名証明書を CA 署名付き証明書で置き換えることを推奨します。CA 署名付き証明書を取得するには、以下を行う必要があります。

1. 証明書署名要求の作成と認証局への送信 （596 ページ）
2. 信頼できる証明書ストアへのルート証明書のインポート （587 ページ）
3. 証明書署名要求への CA 署名付き証明書のバインド （596 ページ）

ISE コミュニティ リソース

How To: Implement ISE Server-Side Certificates

Certificate Renewal on Cisco Identity Services Engine Configuration Guide

システム証明書の表示

[システム証明書（System Certificate）] ウィンドウに、Cisco ISE に追加されたすべてのシステム証明書のリストが表示されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 [システム証明書（System Certificates）] ウィンドウには、次の列が表示されます。

- [フレンドリ名（Friendly Name）]：証明書の名前。
- [使用方法（Usage）]：この証明書が使用されるサービス。
- [ポータルグループタグ（Portal group tag）]：ポータルを使用するように指定された証明書に対してのみ適用できます。このフィールドはポータルに使用する必要がある証明書を指定します。
- [発行先（Issued To）]：証明書のサブジェクトの共通名。
- [発行元（Issued By）]：証明書発行者の共通名
- [有効期限の開始（Valid From）]：証明書の作成日付（「Not Before」証明書属性）。
- [期限日（Expiration Date）]：証明書の有効期限（「Not After」証明書属性）。有効期限の横に次のアイコンが表示されます。
  - 緑色のアイコン：期限切れまで 91 日以上。
  - 青色のアイコン：期限切れまで 90 日以内。
  - 黄色のアイコン：期限切れまで 60 日以内。
  - オレンジ色のアイコン：期限切れまで 30 日以内。
  - 赤色のアイコン： 期限切れ。

管理証明書更新後のアプリケーション再起動のスケジュール設定

プライマリ PAN で管理証明書（管理用に設定された証明書）を更新した後は、展開内のすべてのノードを再起動する必要があります。各ノードをすぐに再起動することも、後での再起動をスケジュールすることもできます。この機能を使用すると、実行中のプロセスが自動再起動によって中断されないようにすることができ、プロセスをより詳細に制御できます。

再起動は、証明書の更新から 15 日以内、または証明書の有効期限が切れる前のいずれか早い方でスケジュールする必要があります。Cisco ISE 管理ポータルのアプリケーション再起動機能のスケジュールピッカーには、それに応じて日付と時刻のオプションが表示されます。

証明書の更新を続行するには、展開内のすべてのノードの再起動時間を選択する必要があります。

次のウィンドウで、管理証明書をインポート、編集、バインド、または生成した後のアプリケーションの再起動を設定できます。

- **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] > [サーバー証明書のインポート（Import Server Certificate）]**

- **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** > **[自己署名証明書の生成（Generate Self Signed Certificate）]**
- **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]**

スケジュールした再起動は、Cisco ISE リリース 3.3 から利用できる **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[管理証明書ノードの再起動（Admin Certificate Node Restart）]** ウィンドウで表示および編集できます。

管理証明書の制御された再起動 という名前の 3 つのアラームは、Cisco ISE ノード全体でスケジュールされているアプリケーションの再起動と、もしあれば再起動失敗のイベントを通知します。**変更された設定** アラームは、この機能に関連する設定変更も通知します。アラームの詳細については、アラーム設定 （1990 ページ） を参照してください。

スケジュールされたノードアプリケーションの再起動に関連するイベントログは、**[操作（Operations）]** > **[レポート（Reports）]** ウィンドウの次のセクションで確認できます。

- 操作監査
- 変更設定監査

システム証明書のインポート

管理者ポータルから、任意の Cisco ISE ノードのシステム証明書をインポートできます。

（注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。プライマリ PAN の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

始める前に

- クライアントブラウザで実行しているシステムに、システム証明書と秘密キーファイルがあることを確認します。
- インポートするシステム証明書が外部 CA によって署名されている場合は、関連するルート CA および中間 CA の証明書を信頼できる証明書ストアにインポートします（**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]**）。
- インポートするシステム証明書に、CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。
[証明書インポートウィザード（Certificate Import Wizard）] ウィンドウが表示されます。

ステップ 3 インポートする証明書の値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

システム証明書のインポート設定

次の表では、サーバー証明書をインポートするために使用できる [システム証明書のインポート（Import System Certificate）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** です。[インポート（Import）] をクリックします。

表 *25 :* システム証明書のインポート設定

フィールド名	説明
ノードの選択（Select Node）	（必須）システム証明書をインポートする Cisco ISE ノードをドロップダウンリストから選択します。
証明書ファイル（Certificate file）	（必須）**[ファイルの選択（Choose File）]** の順にクリックして、ローカルシステムから証明書ファイルを選択します。
秘密キーファイル（Private key file）	（必須）**[ファイルの選択（Choose File）]** の順にクリックして、ローカルシステムから秘密キーファイルを選択します。
パスワード（Password）	（必須）秘密キーファイルを復号化するためのパスワードを入力します。
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE により <common name> **#** <issuer> **#** <nnnnn> の形式で自動的に名前が作成されます。ここで、 <nnnnn> は固有の 5 桁の数字です。
ワイルドカード証明書の許可（Allow Wildcard Certificates）	ワイルドカード証明書をインポートする場合は、このチェックボックスをオンにします。ワイルドカード証明書では、ワイルドカード表記（ドメイン名の前にアスタリスク（*）およびピリオド）が使用されます。ワイルドカード証明書は、組織内の複数のホスト間で共有されます。 このチェックボックスをオンにすると、Cisco ISE は展開内の他のすべてのノードにこの証明書をインポートします。

フィールド名	説明
証明書の拡張の検証（Validate Certificate Extensions）	Cisco ISE に証明書の拡張の検証を許可する場合は、このチェックボックスをオンにします。このチェックボックスをオンにし、かつインポートする証明書に CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在することを確認します。keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方を設定する必要があります。
使用方法（Usage）	このシステム証明書を使用する必要があるサービスを選択します。 • [管理者（Admin）]：管理ポータルとの通信および展開内の Cisco ISE ノード間の通信の保護に使用されるサーバー証明書。 （注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべての Cisco ISE ノード上のサービスが再起動されます。 • [EAP認証（EAP Authentication）]：SSL トンネリングまたは TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバー証明書。 • [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバー証明書。 • [pxGrid]：pxGrid クライアントとサーバーの間の通信を保護するクライアントおよびサーバー証明書。 • [ISEメッセージングサービス（ISE Messaging Service）]：**Cisco ISE メッセージングを介した Syslog** 機能に使用されます。組み込みの UDP syslog 収集ターゲット（LogCollector および LogCollector2）用の MnT WAN 存続を有効にします。 • [SAML]：SAML ID プロバイダーとのセキュアな通信に使用するサーバー証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバー証明書

（注） 証明書が Cisco ISE ではなく他のサードパーティ製ツールによって生成された場合、証明書またはその秘密キーを Cisco ISE にインポートすることはできません。

関連トピック

システム証明書 （565 ページ）
システム証明書の表示 （567 ページ）
システム証明書のインポート （569 ページ）

自己署名証明書の生成

自己署名証明書を生成することで、新しいローカル証明書を追加します。自己署名証明書は、内部テストと評価のニーズに対してのみ使用することを推奨します。実稼働環境に Cisco ISE を展開することを計画している場合は、可能な限り CA 署名付き証明書を使用して、実稼働ネットワーク全体でより均一な受け入れが行われるようにします。

（注） 自己署名証明書を使用しており、Cisco ISE ノードのホスト名を変更する場合は、 Cisco ISE ノードの管理ポータルにログインし、古いホスト名が使用されている自己署名証明書を削除してから、新しい自己署名証明書を生成します。そうしないと、Cisco ISE は古いホスト名が使用された自己署名証明書を引き続き使用します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

自己署名証明書の設定

次の表では、[自己署名証明書の生成（Generate Self Signed Certificate）] ウィンドウのフィールドについて説明します。このウィンドウでは、ノード間通信、EAP-TLS 認証、Cisco ISE Web ポータル、および pxGrid コントローラとの通信用のシステム証明書を作成できます。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]**。[自己署名証明書の生成（Generate Self Signed Certificate）] をクリックします。

表 *26 :* 自己署名証明書の設定

フィールド名	使用上のガイドライン
ノードの選択（Select Node）	（必須）システム証明書を生成するノードをドロップダウンリストから選択します。
共通名（Common Name）（CN）	（SAN を指定しない場合に必須）デフォルトでは、共通名は自己署名証明書を生成する Cisco ISE ノードの FQDN です。
組織ユニット（Organizational Unit）（OU）	組織ユニット名。Engineering など。
組織（Organization）（O）	組織名。Cisco など。
都市（City）（L）	（省略不可）都市名。San Jose など。

フィールド名	使用上のガイドライン
州（State）（ST）	（省略不可）州名。California など。
国（Country）（C）	国名。2 文字の ISO 国番号を入力します。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	証明書に関連付けられた IP アドレス、DNS 名、または Uniform Resource Identifier（URI）。
キータイプ（Key Typ）	RSA または ECDSA のいずれかの公開キーの作成に使用するアルゴリズム。
キーの長さ（Key Length）	公開キーのビットサイズ。ドロップダウンリストから、RSA に次のいずれかのオプションを選択します。 • 512 • 1024 • 2048 • 4096 ドロップダウンリストから、ECDSA に次のいずれかのオプションを選択します。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティレベルで異なるキー長を持つことがあります。 パブリック CA 署名付き証明書を取得する場合、または FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は、2048 を選択します。
署名するダイジェスト（Digest to Sign With）	ドロップダウンリストから、次のハッシュアルゴリズムのいずれかを選択します。 • SHA-1 • SHA-256
証明書ポリシー（Certificate Policies）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。

フィールド名	使用上のガイドライン
TTL有効期限（Expiration TTL）	証明書が失効するまでの日数を指定します。ドロップダウンリストから値を選択します。
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ワイルドカード証明書の許可（Allow Wildcard Certificates）	自己署名ワイルドカード証明書を生成する場合は、このチェックボックスをオンにします。ワイルドカード証明書はワイルドカード表記（ドメイン名の前にアスタリスクとピリオドの形式）を使用し、組織の複数のホスト間で証明書を共有できるようにします。
使用方法（Usage）	このシステム証明書を使用する必要があるサービスを選択します。 • [管理者（Admin）]：管理ポータルとの通信および展開内の Cisco ISE ノード間の通信の保護に使用されるサーバー証明書。 • [EAP認証（EAP Authentication）]：SSL トンネリングまたは TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバー証明書。 • [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバー証明書。 • [pxGrid]：pxGrid クライアントとサーバーの間の通信を保護するクライアントおよびサーバー証明書。 • [SAML]：SAML ID プロバイダーとのセキュアな通信に使用するサーバー証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバー証明書。

関連トピック

システム証明書 （565 ページ）
システム証明書の表示 （567 ページ）
自己署名証明書の生成 （572 ページ）

システム証明書の編集

このウィンドウを使用して、システム証明書を編集し、自己署名証明書を更新します。ワイルドカード証明書を編集すると、変更が展開内のすべてのノードに複製されます。ワイルドカード証明書を削除した場合、そのワイルドカード証明書は展開内のすべてのノードから削除されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]**を選択します。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 自己署名証明書を更新するには、**[更新期間（Renewal Period）]** チェックボックスをオンにして、有効期限 TTL（存続可能時間）を日、週、月、または年単位で入力します。ドロップダウンリストから必要な値を選択します。

ステップ 4 [保存（Save）]をクリックします。

[管理者（Admin）] チェックボックスがオンになっている場合、Cisco ISE ノードのアプリケーションサーバーが再起動します。また、その Cisco ISE ノードが展開の PAN である場合は、展開内のその他すべてのノードでもアプリケーションサーバーが再起動します。プライマリ PAN の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

トラブルシューティングの詳細については、Google Chrome 65 を使用した BYOD ポータルの起動 （575 ページ）Mozilla Firefox 64 を使用したワイヤレス BYOD セットアップの設定 （576 ページ）を参照してください。

Google Chrome 65 を使用した BYOD ポータルの起動

Chrome 65 以上を使用して Cisco ISE を起動すると、URL が正しくリダイレクトされたにもかかわらず、BYOD ポータルまたはゲストポータルがブラウザで起動に失敗することがあります。これは、すべての証明書に **Subject Alternative Name** フィールドを必要とする、Google で導入された新しいセキュリティ機能が原因です。Cisco ISE リリース 2.4 以降の場合、**Subject Alternative Name** フィールドに値が必要となります。

Chrome 65 以上で BYOD ポータルを起動するには、次の手順に従います。

ステップ 1 [サブジェクトの別名（Subject Alternative Name）] フィールドに入力することで、Cisco ISE GUI から新しい自己署名証明書を生成します。DNS と IP アドレスの両方を入力する必要があります。

ステップ 2 Cisco ISE サービスが再起動します。

ステップ 3 Chrome ブラウザでポータルにリダイレクトされます。

ステップ 4 ブラウザで次のように操作します。 **[証明書の表示（View Certificates）] > [詳細（Details）] > base-64 エンコードを選択して証明書をコピー**

ステップ 5 高信頼パスで証明書をインストールします。

ステップ 6 Chrome ブラウザを終了し、ポータルのリダイレクトを試みます。

Mozilla Firefox 64 を使用したワイヤレス BYOD セットアップの設定

Win RS4 または RS5 のオペレーティングシステムでブラウザ Firefox 64 以降のリリースのワイヤレス BYOD セットアップを設定する場合は、証明書の例外を追加することができない場合があります。この現象は Firefox 64 以降のリリースの新規インストール時に発生することがあります。以前のバージョンから Firefox 64 以降にアップグレードした場合は発生しません。次の手順では、このような場合でも証明書の例外を追加することができます。

ステップ 1 BYOD フローのシングル PEAP またはデュアル PEAP または TLS を設定します。

ステップ 2 Windows のすべてのオプションで CP ポリシーを設定します。

ステップ 3 エンドクライアント Windows RS4 または Windows RS5 で、Dot1.x または MAB SSID に接続します。

ステップ 4 ゲストポータルまたは BYOD ポータルにリダイレクトするには、FF64 ブラウザに 何らか URL を入力します。

ステップ 5 **[例外を追加（Add Exception）]** > **[証明書を追加できない（Unable to add certificate）]** をクリックし、フローを続行します。

回避策として、Firefox 64 の証明書を手動で追加します。Firefox 64 のブラウザで、**[オプション（Options）]** > **[プライバシー&設定（Privacy & Settings）]** > **[証明書の表示（View Certificates）]** > **[サーバー（Servers）]** > **[例外の追加（Add Exception）]** を選択します。

システム証明書の削除

[管理（Administration）] > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** で [未使用（Not in use）] とタグ付けされたシステム証明書を削除しても安全です。

システム証明書ストアから複数の証明書を一度に削除できますが、管理および EAP 認証に使用する証明書を少なくとも 1 つ所有する必要があります。また、管理、EAP 認証、ポータル、または pxGrid コントローラに使用される証明書は削除できません。ただし、サービスがディセーブルの場合は、pxGrid 証明書を削除できます。

ワイルドカード証明書を削除することを選択した場合、証明書は展開内のすべての Cisco ISE ノードから削除されます。

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]**を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。

ステップ 3 [はい（Yes）] をクリックして、証明書を削除します。

システム証明書のエクスポート

システム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]**。

ステップ 2 エクスポートする証明書の横にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント 値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカードシステム証明書をエクスポートしてノード間通信用に他の Cisco ISE ノードにインポートする場合）は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE ノードにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート（Export）] をクリックして、クライアント ブラウザを実行しているファイル システムに証明書を保存します。

証明書のみをエクスポートする場合、証明書はPEM形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書はPEM形式の証明書と暗号化された秘密キーファイルを含む .zip ファイルとしてエクスポートされます。

信頼できる証明書ストア

信頼できる証明書ストアには、信頼に使用される、Simple Certificate Enrollment Protocol（SCEP）用の X.509 証明書が含まれています。

Cisco ISE にインポートされる X.509 証明書は、PEM 形式か、または識別符号化規則形式である必要があります。証明書チェーン（システム証明書およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。

ゲストポータルに公開ワイルドカード証明書を割り当て、ルート CA 証明書を使用してサブ CA をインポートする場合、Cisco ISE サービスが再起動されるまで証明書チェーンは送信されません。

信頼できる証明書ストア内の証明書はプライマリ PAN で管理され、Cisco ISE 展開内の他のすべてのノードに複製されます。Cisco ISE はワイルドカード証明書をサポートしています。

Cisco ISE は、次の目的で信頼できる証明書を使用します。

- エンドポイントによる認証と、証明書ベースの管理者認証を使用してISE-PIC管理ポータルにアクセスする Cisco ISE 管理者による認証に使用するクライアント証明書を確認するため。
- 展開内の Cisco ISE ノード間のセキュアな通信を可能にするため。信頼できる証明書ストアには、展開内の各ノードのシステム証明書との信頼を確立するために必要な CA 証明書のチェーンが含まれている必要があります。
  - 自己署名証明書をシステム証明書に使用する場合は、各ノードの自己署名証明書を PAN の信頼できる証明書ストアに配置する必要があります。
  - CA署名付き証明書をシステム証明書に使用する場合は、CAルート証明書と信頼チェーン内のすべての中間証明書も PAN の信頼できる証明書ストアに配置する必要があります。
- セキュアな LDAP 認証を有効にするには、SSL を経由してアクセスされる LDAP ID ソースを定義するときに、証明書ストアから証明書を選択する必要があります。
- パーソナル デバイス ポータルを使用してネットワークへの登録を準備しているパーソナル デバイスに配信するため。Cisco ISE は、パーソナルデバイスの登録をサポートするために、PSN に SCEP を実装しています。登録するデバイスは、SCEP プロトコルを使用して PSN からクライアント証明書を要求します。PSN には、仲介として機能する登録局（RA）が含まれています。RA は、登録するデバイスからの要求を受信して検証した後、クライアント証明書を発行する外部 CA または内部 Cisco ISE CA にその要求を転送します。CA は RA に証明書を返し、RA が証明書をデバイスに返します。

  Cisco ISE によって使用される各 SCEP CA は、SCEP RA プロファイルによって定義されます。SCEP RA のプロファイルが作成されると、次の 2 つの証明書が信頼できる証明書ストアに自動的に追加されます。
  - CA 証明書（自己署名証明書）
  - CA によって署名された RA 証明書（証明書要求のエージェントの証明書）

  SCEP プロトコルでは、これらの 2 つの証明書が RA によって登録デバイスに提供されている必要があります。信頼できる証明書ストアにこの 2 つの証明書を配置すると、これらのノードの RA が使用するために、証明書がすべての PSN ノードに複製されます。

（注） SCEP RA プロファイルが削除されると、関連付けられている CA チェーンが信頼できる証明書ストアからも削除されます。ただし、セキュアな syslog、LDAP、システム、または信頼証明書によって同じ証明書が参照されている場合は、SCEP プロファイルだけが削除されます。

ISE コミュニティ リソース

ISE へのサードパーティ CA 証明書のインストール

信頼できる証明書ストアの証明書

信頼できる証明書ストアは、次の信頼できる証明書で事前設定されています。製造業者証明書、ルート証明書、その他の信頼できる証明書。ルート証明書（Cisco Root CA）は、製造業者（Cisco CA Manufacturing）証明書に署名します。これらの証明書は、デフォルトでは無効になっています。展開でエンドポイントとして Cisco IP Phone を使用している場合は、ルート証明書と製造業者証明書を有効にすると電話機用にシスコが署名したクライアント証明が認証されます。

信頼できる証明書のリスト

次の表に、管理ノードに追加された信頼できる証明書のリストが表示される [信頼できる証明書（Trusted Certificates）] ウィンドウの列を示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** です。

表 *27 : [[*信頼できる証明書（***Trusted Certificates***）*]* ウィンドウの列

フィールド名	使用上のガイドライン
フレンドリ名（**Friendly Name**）	証明書の名前を表示します。
ステータス（**Status**）	この列には [有効（Enabled）] または [無効（Disabled）] が表示されます。証明書が無効の場合、Cisco ISE は信頼を確立するために証明書を使用しません。
信頼対象（**Trusted for**）	証明書を使用する次のサービスのうち、1 つ以上を表示します。 • インフラストラクチャ • シスコ サービス • エンドポイント

フィールド名	使用上のガイドライン
発行先（Issued To）	証明書件名の共通名を表示します。
発行元（Issued By）	証明書発行者の共通名を表示します。
有効期限の開始（Valid From）	証明書が発行された日付と時刻を表示します。この値は、「Not Before」証明書属性とも呼ばれます。
有効期限日（Expiration Date）	証明書の有効期限が切れる日付と時刻を表示します。この値は、「Not Afte」証明書属性とも呼ばれます。
有効期限ステータス（Expiration Status）	証明書の有効期限のステータスに関する情報です。このコラムに表示される Informational（情報提供）メッセージには 5 つのアイコンとカテゴリがあります。 • **緑色**：期限切れまで 91 日以上 • **青色**：期限切れまで 90 日以内 • **黄色**：期限切れまで 60 日以内 • **オレンジ色**：期限切れまで 30 日以内 • **赤色**: 期限切れ

関連トピック

信頼できる証明書ストア （577 ページ）
信頼できる証明書の表示 （582 ページ）
信頼できる証明書ストアの証明書のステータス変更 （582 ページ）
信頼できる証明書ストアへの証明書の追加 （582 ページ）

信頼できる証明書の命名の制約

CTL の信頼できる証明書には名前の制約の拡張が含まれている場合があります。この拡張は、証明書チェーンの後続のすべての証明書のサブジェクト名とサブジェクト代替名フィールドの値の名前空間を定義します。Cisco ISE は、ルート証明書で指定された制約を検査しません。

Cisco ISE は、次の名前の制約をサポートしています。

- ディレクトリ名

  ディレクトリ名の制約は、サブジェクトのディレクトリ名またはサブジェクトの別名フィールドのプレフィクスです。例：

  - 正しいサブジェクト プレフィクス：

    CA 証明書の名前の制約：Permitted: O=Cisco

クライアント証明書のサブジェクト：O=Cisco,CN=Salomon

- 不正なサブジェクト プレフィクス：

  CA 証明書の名前の制約：Permitted: O=Cisco

  クライアント証明書のサブジェクト：CN=Salomon,O=Cisco

- DNS
- E メール
- URI（URI の制約は、http://、https://、ftp://、または ldap:// のような URI プレフィクスで始まる必要があります）。

Cisco ISE は、次の名前の制約をサポートしていません。

- IP アドレス
- OtherName

信頼できる証明書にサポートされていない制約が含まれており、検証中の証明書に該当のフィールドが含まれていない場合は、Cisco ISE がサポートされない制約を検証できないため、その証明書は拒否されます。

信頼できる証明書内の名前の制約の定義例を次に示します。

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
                  email:.abcde.be
                  email:.abcde.bg
                  email:.abcde.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
                 DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100

                  URI:.dir
                  IP:172.23.0.171/255.255.255.255
                Excluded:
                  DNS:.dir
                  URI:.dir
```

受け入れ可能なクライアント証明書のサブジェクトは、次のように上記の定義に一致します。

```
           Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

信頼できる証明書の表示

[信頼できる証明書（Trusted Certificates）] ウィンドウに、Cisco ISE で使用可能なすべての信頼できる証明書が一覧表示されます。信頼できる証明書を表示するには、スーパー管理者またはシステム管理者である必要があります。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 すべての証明書を表示するには、[メニュー（Menu）]アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**を選択します。表示される [信頼できる証明書（Trusted Certificates）] ウィンドウにはすべての信頼できる証明書のリストが表示されます。

ステップ 2 [信頼できる証明書（Trusted Certificate）] のチェックボックスをオンにし、[編集（Edit）]、[表示（View）]、[エクスポート（Export）]、または [削除（Delete）] をクリックして必要なタスクを実行します。

信頼できる証明書ストアの証明書のステータス変更

証明書のステータスが有効になっている必要があります。これにより、Cisco ISE が信頼の確立にこの証明書を使用できるようになります。証明書が信頼できる証明書ストアにインポートされると、この証明書は自動的に有効になります。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**。

ステップ 3 有効または無効にする証明書の隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 4 [ステータス（Status）] ドロップダウン リストからステータス条件を選択します。

ステップ 5 [保存（Save）] をクリックします。

信頼できる証明書ストアへの証明書の追加

[信頼できる証明書ストア（Trusted Certificate Store）] ウィンドウでは、Cisco ISE に CA 証明書を追加できます。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

- 追加する証明書は、ブラウザを実行しているコンピュータのファイルシステムにある必要があります。証明書は PEM または DER 形式である必要があります。
- 管理者認証またはEAP認証に証明書を使用するには、基本的な制約を証明書内に定義し、CA フラグを true に設定します。

信頼できる証明書の編集

証明書を信頼できる証明書ストアに追加したら、[編集（Edit）] のオプションを使用して、その証明書をさらに編集できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、 次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 （オプション）[フレンドリ名（Friendly Name）] フィールドに証明書の名前を入力します。フレンドリ名を指定しない場合、デフォルト名は次の形式で生成されます。

common-name#issuer#nnnnn

ステップ 4 [信頼先（Trusted For）] 領域で必要なチェックボックスをオンにして、証明書の用途を定義します。

ステップ 5 （オプション）[説明（Description）] フィールドに、証明書の説明を入力します。

ステップ 6 [保存（Save）] をクリックします。

信頼できる証明書の設定

次の表では、信頼できる証明書の [編集（Edit）] ウィンドウのフィールドについて説明します。このウィンドウで CA 証明書の属性を編集します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** です。編集する信頼できる証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

表 *28* : 信頼できる証明書の編集設定

フィールド名	使用上のガイドライン
証明書発行元（Certificate Issuer）	

フィールド名	使用上のガイドライン
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。これはオプションのフィールドです。フレンドリ名を入力しない場合は、次の形式でデフォルト名が生成されます。 *common-name#issuer#nnnnn*
ステータス（Status）	ドロップダウンリストから [有効（Enabled）] または [無効（Disabled）] を選択します。証明書が無効の場合、Cisco ISE は信頼を確立するために証明書を使用しません。
説明（Description）	（任意）説明を入力します。
使用方法（Usage）	
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書で（他の Cisco ISE ノードまたは LDAP サーバーからの）サーバー証明書を確認する場合は、このチェックボックスをオンにします。
クライアント認証および syslog 用に信頼する（Trust for client authentication and Syslog）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した Cisco ISE に接続するエンドポイントを認証します。 • syslog サーバーを信頼します。
証明書ベースの管理者認証用に信頼する（Trust for certificate based admin authentication）	このチェックボックスをオンにできるのは、[クライアント認証および Syslog 用に信頼する（Trust for client authentication and Syslog）] が選択されている場合のみです。 管理者アクセスの証明書ベースの認証の使用を有効にするには、このチェックボックスをオンにします。信頼できる証明書ストアに必要な証明書チェーンをインポートします。
シスコ サービスの認証用に信頼する（Trust for authentication of Cisco Services）	フィードサービスなどの外部シスコサービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
証明書ステータスの検証（Certificate Status Validation）	Cisco ISE は、特定の CA が発行するクライアントまたはサーバー証明書の失効ステータスをチェックする 2 とおりの方法をサポートしています。1 つめの方法は、Online Certificate Status Protocol（OCSP）を使用して証明書を検証することです（OCSP は、CA によって保持される OCSP サービスに要求を行います）。2 つめの方法は、Cisco ISE に CA からダウンロードした証明書失効リスト（CRL）と照合して証明書を検証することです。どちらの方法も、OCSP を最初に使用してステータスを判断できないときに限り CRL を使用する場合に使用できます。
OCSP サービスに対して検証する（Validate Against OCSP Service）	OCSP サービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まず OCSP サービスを作成する必要があります。
OCSP が不明なステータスを返した場合は要求を拒否する（Reject the request if OCSP returns UNKNOWN status）	証明書ステータスが OCSP サービスによって判断されなかった場合に要求を拒否するには、このチェックボックスをオンにします。このチェックボックスをオンにした場合、OCSP サービスによって不明なステータス値が返されると、Cisco ISE は現在評価しているクライアントまたはサーバー証明書を拒否します。
OCSP応答側が到達不能な場合は要求を拒否する（Reject the request if OCSP Responder is unreachable）	OCSP 応答側が到達不能な場合に Cisco ISE が要求を拒否するには、このチェックボックスをオンにします。
CRL のダウンロード（Download CRL）	Cisco ISE で CRL をダウンロードするには、このチェックボックスをオンにします。
CRL 配信 URL（CRL Distribution URL）	CA から CRL をダウンロードするための URL を入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URL は「http」、「https」、または「ldap」で始まる必要があります。
CRL の取得（Retrieve CRL）	CRL は、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。

フィールド名	使用上のガイドライン
ダウンロードが失敗した場合は待機する（If download failed, wait）	Cisco ISE が CRL を再度ダウンロードするまでに Cisco ISE に必要な試行を待機する必要がある時間間隔を設定します。
CRL を受信しない場合 CRL 検証をバイパスする（Bypass CRL Verification if CRL is not Received）	このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。
CRL がまだ有効でないか、または期限切れの場合は無視する（Ignore that CRL is not yet valid or expired）	Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。 Cisco ISE で [有効日（Effective Date）] フィールドの開始日と [次の更新（Next Update）] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRL がまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。

関連トピック

信頼できる証明書ストア （577 ページ）
信頼できる証明書の編集 （583 ページ）

信頼できる証明書の削除

今後使用しない信頼できる証明書を削除できます。ただし、Cisco ISE 内部 CA 証明書は削除しないでください。Cisco ISE 内部 CA 証明書を削除できるのは、展開全体の Cisco ISE ルート証明書チェーンを置き換える場合のみです。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。Cisco ISE 内部 CA 証明書を削除するには、次のいずれかのオプションをクリックします。

- **[削除（Delete）]**：Cisco ISE 内部 CA 証明書を削除する場合。Cisco ISE 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークに参加できません。エンドポイントをネットワークで再度有効にするには、信頼できる証明書ストアに同じ Cisco ISE 内部 CA 証明書をインポートします。
- **[削除および取消（Delete & Revoke）]**：Cisco ISE 内部 CA 証明書を削除して取り消します。Cisco ISE 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネット

ワークにアクセスできません。この操作は取り消すことができません。展開全体のCisco ISEルート証明書チェーンを置き換える必要があります。

ステップ3 [はい（Yes）] をクリックして、証明書を削除します。

信頼できる証明書ストアからの証明書のエクスポート

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

（注） 内部CAから証明書をエクスポートし、そのエクスポートされた証明書を使用してバックアップから復元する場合は、CLIコマンド **application configure ise** を使用する必要があります。Cisco ISE CA 証明書およびキーのエクスポート （628 ページ）を参照してください。

ステップ1 Cisco ISEのGUIで、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。一度に1つの証明書のみをエクスポートできます。

ステップ3 選択した証明書は、クライアントブラウザを実行しているファイルシステムにPEM形式でダウンロードされます。

信頼できる証明書ストアへのルート証明書のインポート

ルートCA証明書および中間CA証明書をインポートするとき、信頼できるCA証明書を使用する対象のサービスを指定できます。

外部ルートCA証明書をインポートするときに、次のタスクのステップ5で、[管理者認証に基づく証明書への信頼（Trust for certificate based admin authentication）] オプションを有効にします。

始める前に

証明書署名要求に署名し、デジタルで署名されたCA証明書を返したCAのルート証明書と他の中間証明書が必要です。

ステップ1 Cisco ISEのGUIで、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ2 [インポート（Import）] をクリックします。

ステップ 3 [証明書ストアへの新しい証明書のインポート（Import a new Certificate into the Certificate Store）] ウィンドウで、[ファイルの選択（Choose File）] をクリックし、CA によって署名され、返されたルート CA 証明書を選択します。

ステップ 4 [フレンドリ名（Friendly Name）] を入力します。

[フレンドリ名（Friendly Name）] を入力しないと、Cisco ISE により、このフィールドには、*common-name#issuer#nnnnn* 形式（*nnnnn* は一意の番号）で名前が自動的に入力されます。後で証明書を編集して、[フレンドリ名（Friendly Name）] を変更できます。

ステップ 5 この信頼できる証明書を使用するサービスの横にあるチェックボックスをオンにします。

ステップ 6 （任意）[説明（Description）] フィールドに証明書の説明を入力します。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

信頼できる証明書ストアに中間 CA 証明書をインポートします（該当する場合）。

信頼できる証明書のインポート設定

次の表では、CA 証明書を Cisco ISE に追加するために使用できる [信頼できる証明書のインポート（Trusted Certificate Import）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]**。

表 *29* : 信頼できる証明書のインポート設定

フィールド名	説明
証明書ファイル（Certificate file）	[参照（Browse）] をクリックして、ブラウザを実行しているコンピュータから証明書ファイルを選択します。
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE により <common name>#<issuer>#<nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書を（他の ISE ノードまたは LDAP サーバーから）サーバー証明書の検証に使用する場合は、このチェックボックスをオンにします。

フィールド名	説明
クライアント認証および syslog 用に信頼する（Trust for client authentication and Syslog）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した ISE に接続するエンドポイントの認証 • syslog サーバーの信頼
シスコ サービスの認証用に信頼する（Trust for authentication of Cisco Services）	フィード サービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書の拡張の検証（Validate Certificate Extensions）	（[クライアント認証用に信頼する（Trust for client authentication）] オプションと [証明書拡張の検証を有効にする（Enable Validation of Certificate Extensions）] オプションの両方をオンにした場合のみ）「keyUsage」拡張が存在し、「keyCertSign」ビットが設定されていることと、CA フラグが true に設定された基本制約拡張が存在することを確認します。
説明（Description）	任意で説明を入力します。

関連トピック

信頼できる証明書ストア （577 ページ）
証明書チェーンのインポート （589 ページ）
信頼できる証明書ストアへのルート証明書のインポート （587 ページ）

証明書チェーンのインポート

証明書ストアから受信した証明書チェーンを含む単一のファイルから、複数の証明書をインポートすることができます。ファイル内のすべての証明書は PEM の形式であり、証明書は次の順序に並べられている必要があります。

- ファイル内の最後の証明書は、CA によって発行されたクライアント証明書またはサーバー証明書である必要があります。
- 前にあるすべての証明書は、ルート CA 証明書と、発行された証明書の署名のチェーンにあるすべて中間 CA 証明書である必要があります。

証明書チェーンのインポートは、次の 2 ステップのプロセスです。

1. Cisco ISE 管理ポータルで信頼できる証明書ストアに証明書チェーンファイルをインポートします。この操作により、最後の 1 つを除き、すべての証明書がファイルから信頼できる証明書ストアにインポートされます。

2. CA 署名付き証明書のバインド操作を使用して証明書チェーン ファイルをインポートします。この操作により、最後の証明書がローカル証明書としてファイルからインポートされます。

Cisco ISE ノード間通信の信頼できる証明書のインストール

展開をセットアップする場合、セカンダリノードを登録する前に、セカンダリノードの管理者証明書の検証に使用される適切な CA 証明書を PAN の CTL に配置する必要があります。PAN の CTL に入力する手順は、シナリオに応じて異なります。

- セカンダリノードが Cisco ISE 管理ポータルとの通信に CA 署名付き証明書を使用する場合は、セカンダリノードの CA 署名付き証明書、関連する中間証明書（ある場合）、および（セカンダリノードの証明書に署名した CA の）ルート CA 証明書を PAN の CTL にインポートする必要があります。
- セカンダリノードが Cisco ISE 管理ポータルとの通信に自己署名証明書を使用する場合は、PAN の CTL にセカンダリノードの自己署名証明書をインポートできます。

（注）
- 登録されたセカンダリノードの管理者証明書を変更する場合は、セカンダリノードの管理者証明書の検証に使用できる適切な CA 証明書を取得し、PAN の CTL にインポートする必要があります。
- 展開内でクライアントと PSN の間のセキュアな通信に自己署名証明書を使用する場合、BYOD ユーザーがある場所から別の場所に移動すると、EAP-TLS ユーザー認証は失敗します。一部の PSN 間で提供される必要があるこのような認証要求の場合、外部で署名された CA 証明書を使用してクライアントと PSN の間の通信を保護するか、または外部の CA によって署名されたワイルドカード証明書を使用する必要があります。

外部 CA から発行された証明書に基本制約が定義されており、CA フラグが true に設定されていることを確認します。ノード間通信用の CA 署名付き証明書のインストール：

ステップ 1 証明書署名要求の作成と認証局への送信 （596 ページ）
ステップ 2 信頼できる証明書ストアへのルート証明書のインポート （587 ページ）
ステップ 3 証明書署名要求への CA 署名付き証明書のバインド （596 ページ）

Cisco ISE でのデフォルトの信頼できる証明書

Cisco ISE の信頼できる証明書ストア（[メニュー（Menu）]（☰）アイコンをクリックし、次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**）には、デフォルトで使用可能な証明書がいくつか含まれています。これらの証明書は、セキュリティ要件を満たすためにストアに自動的にインポートされます。ただし、これらすべてを使用する必要はありません。次の表に記載されている場合を除き、すでに使用可能になっている証明書ではなく、自分で選択した証明書を使用できます。

表 *30* : デフォルトの信頼できる証明書

信頼できる証明書の名前	シリアル番号	証明書の目的	証明書を含む Cisco ISE リリース
Baltimore CyberTrust Root CA	02 00 00 B9	この証明書は、一部の地域で cisco.com が使用する CA チェーン内のルート CA 証明書として機能することができます。また、この証明書は、https://s3.amazonaws.com でホストされている ISE 2.4 のポスチャ/CP 更新 XML ファイルでも使用されていました。	リリース 2.4 以降。
DST Root CA X3 Certificate Authority	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	この証明書は、cisco.com が使用する CA チェーンのルート CA 証明書として機能することができます。	リリース 2.4 以降。
Thawte Primary Root CA	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	この証明書は、cisco.com と perfigo.com が使用する CA チェーンのルート CA 証明書として機能することができます。	リリース 2.4 以降。

信頼できる証明書の名前	シリアル番号	証明書の目的	証明書を含む Cisco ISE リリース
VeriSign Class 3 Public Primary Certification Authority	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	この証明書は、VeriSign Class 3 Secure Server CA-G3 のルート CA 証明書として機能します。 Cisco ISE でプロファイラ フィード サービスを設定する場合は、この証明書を使用する必要があります。	リリース 2.4 以降。
VeriSign Class 3 Secure Server CA - G3	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	これは、2020 年 2 月 7 日に期限切れになる中間 CA 証明書です。この証明書を更新する必要はありません。 証明書を削除するには、下記のタスクを実行します。	リリース 2.4 以降。
Cisco CA Manufacturing	6A 69 67 B3 00 00 00 00 00 03	この証明書は、Cisco ISE に接続している特定のシスコデバイスが使用する場合があります。この証明書はデフォルトでは無効になっています。	リリース 2.4 および 2.6。
Cisco Manufacturing CA SHA2	02	この証明書は、管理者認証、エンドポイント認証、および展開インフラストラクチャフローの CA チェーン内で使用できます。	リリース 2.4 以降。
Cisco Root CA 2048	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	この証明書は、Cisco ISE に接続している特定のシスコデバイスが使用することができます。この証明書はデフォルトでは無効になっています。	リリース 2.4 以降。

信頼できる証明書の名前	シリアル番号	証明書の目的	証明書を含む Cisco ISE リリース
Cisco Root CA M2	01	この証明書は、管理者認証、エンドポイント認証、および展開インフラストラクチャフローの CA チェーン内で使用できます。	リリース 2.4 以降。
DigiCert Root CA	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	Facebook を使用したゲストログインを使用しているフローには、この証明書を使用する必要があります。	リリース 2.4 以降。
DigiCert SHA2 High Assurance Server CA	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	Facebook を使用したゲストログインを使用しているフローには、この証明書を使用する必要があります。	リリース 2.4 以降。
HydrantID SSL ICA G2	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	シスコサービスで信頼されています。	リリース 2.4 および 2.6。
QuoVadis Root CA 2	05 09	この証明書は、プロファイラ、ポスチャ、およびクライアントプロビジョニングフロー内で使用する必要があります。	リリース 2.4 以降。
Cisco ECC Root CA	01	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6。
Cisco Licensing Root CA	01	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。

信頼できる証明書の名前	シリアル番号	証明書の目的	証明書を含む Cisco ISE リリース
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
Cisco RXC-R2	01	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
Cisco ECC Root CA 2099	03	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。

Cisco ISE からのデフォルトの信頼できる証明書の削除

- 信頼できるすべての証明書を表示するには、Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します。**[管理（Administration）] > [システム（System）** > **][証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**
- 削除する証明書をエクスポートして保存します。これにより、必要に応じて再度インポートできるようになります。

  エクスポートする証明書のチェックボックスをクリックし、上にあるメニューバーの [エクスポート（Export）] をオンにします。キーチェーンがシステムにダウンロードされます。
- 証明書を削除します。削除する証明書のチェックボックスをオンにし、上部のメニューバーの [削除（Delete）] をクリックします。CA チェーン、セキュアな syslog、またはセキュアな LDAP によって使用されている場合は、その証明書を削除することはできません。
- CA チェーン、セキュアな syslog、および それが含まれている syslog から証明書を削除するために必要な設定変更を行います。その後で、証明書を削除します。
- 証明書を削除したら、関連するサービス（証明書の目的を参照）が想定どおりに動作していることを確認します。

古いシステムと信頼できる証明書

古い証明書は、展開内のどのノードにも属していない証明書です。これらの冗長な証明書は、システムおよび信頼できる証明書ストアに大量に蓄積される可能性があり、メモリ不足と遅延の問題につながります。Cisco ISE リリース 3.1 以降、そのような冗長な証明書は [古い証明書（Stale Certificate）] ステータスを持ち、それらを確認して削除できるようになりました。

古いシステム証明書と信頼できる証明書の確認

古いシステム証明書と信頼できる証明書を識別するために、次のチェックが実行されます。

古いシステム証明書	古い信頼できる証明書
• [発行先（Issued To）] フィールドをチェックして、展開内のいずれかのノードのホスト名が発行されたシステム証明書の一部であるかどうかを確認します。一致するものがない場合、システム証明書は古いと見なされます。 • 発行されたシステム証明書の [SAN拡張（SAN Extension）] フィールドは、展開内のノードの FQDN と一致する必要があります。一致するものがない場合、システム証明書は古いと見なされます。 • [Subject Name Alternative (SAN)] フィールドでワイルドカードエントリの有無がチェックされます。ワイルドカード文字がない場合、システム証明書は古いと見なされます。 （注） 古い証明書のチェックは、サードパーティ CA または Cisco ISE CA によって署名された証明書に対して実行されます。自己署名証明書は、これらのチェックから除外されます。	• 内部 CA 証明書のステータスを確認するときに、ステータスが [非アクティブ（Inactive）] と表示され、[StatusChangeReason] が [CertSuperseded] の場合、信頼できる証明書は古いと見なされます。 • [発行先（Issued To）] フィールドをチェックして、展開内のいずれかのノードのホスト名が発行された信頼できる証明書の一部であるかどうかを確認します。一致するものがない場合、信頼できる証明書は古いと見なされます。

証明書署名要求

CA が署名付き証明書を発行するには、証明書署名要求を作成して CA に送信する必要があります。

作成した証明書署名要求のリストは、[証明書署名要求（Certificate-Signing Requests）] ウィンドウに表示されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証**

明書署名要求（Certificate-Signing Requests）] を選択します。CA から署名を取得するには、証明書署名要求をエクスポートし、その証明書を CA に送信する必要があります。証明書は CA によって署名され、返されます。

Cisco ISE の管理ポータルから証明書を一元的に管理できます。展開内のすべてのノードの証明書署名要求を作成し、それらをエクスポートできます。その後、証明書署名要求を CA に送信し、CA から署名付き証明書を取得し、CA によって返されたルートおよび中間 CA 証明書を信頼できる証明書ストアにインポートし、証明書署名要求に CA 署名付き証明書をバインドする必要があります。

証明書署名要求の作成と認証局への送信

証明書署名要求（CSR）を生成して、展開内のノードの CA 署名付き証明書を取得できます。展開内の特定のノードまたは展開内のすべてのノード用の証明書署名要求（CSR）を生成できます。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate-Signing Requests (CSR)）] をクリックして、証明書署名要求を生成します。

ステップ 3 証明書署名要求を生成するための値を入力します。表示されるウィンドウの各フィールドについては、信頼できる証明書の設定 （583 ページ）を参照してください。

ステップ 4 （オプション）ダウンロードする署名要求のチェックボックスをオンにし、[エクスポート（Export）] をクリックして要求をダウンロードします。

ステップ 5 「 **-----BEGIN CERTIFICATE REQUEST-----** 」から「 **-----END CERTIFICATE REQUEST-----** 」までのすべてのテキストをコピーし、選択した CA の証明書要求に要求の内容を貼り付けます。

ステップ 6 署名済みの証明書をダウンロードする。

CA によっては、署名付き証明書が電子メールで送信される場合があります。署名付き証明書は、zip ファイルの形式で、Cisco ISE の信頼できる証明書ストアに追加する必要がある、新規発行の証明書と CA のパブリック署名証明書が含まれています。デジタル署名された CA 証明書、ルート CA 証明書、および他の中間 CA 証明書（該当する場合）をクライアントブラウザを実行するローカルシステムにダウンロードできます。

証明書署名要求への CA 署名付き証明書のバインド

CA がデジタル署名付き証明書を返してから、その証明書を証明書署名要求にバインドする必要があります。Cisco ISE 管理者ポータルから展開内のすべてのノードに対してバインド操作を実行できます。

始める前に

- デジタル署名付き証明書、および関連するルート中間 CA 証明書を CA から受け取る必要があります。

- 信頼できる証明書ストアに関連するルート CA 証明書と中間 CA 証明書をインポートします（**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します）。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 CA 署名付き証明書とバインドする必要がある証明書署名要求の横にあるチェックボックスをオンにします。

ステップ 3 **[証明書のバインド（Bind Certificate）]** をクリックします。

ステップ 4 表示される [CA 署名付き証明書（Bind CA Signed Certificate）] ウィンドウで、**[ファイルの選択（Choose File）]** をクリックし、CA 署名付き証明書を選択します。

ステップ 5 [フレンドリ名（Friendly Name）] フィールドに値を入力します。

ステップ 6 Cisco ISE に証明書の拡張の検証を許可する場合は、[証明書の拡張の検証（Validate Certificate Extensions）] チェックボックスをオンにします。

[証明書の拡張の検証（Validate Certificate Extensions）] オプションが有効になっており、インポートする証明書に CA フラグが True に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。

（注） Cisco ISE では、EAP-TLS クライアント証明書にデジタル署名のキー使用拡張を使用する必要があります。

ステップ 7 （オプション）[使用方法（Usage）] 領域で、この証明書が使用されるサービスをオンにします。

この情報は、証明書署名要求の生成時に [使用方法（Usage）] オプションを有効にした場合は自動入力されます。また、後で証明書を編集して使用方法を指定することもできます。

プライマリ PAN で使用方法が [管理者（Admin）] の証明書を変更すると、他のすべてのノードでサービスが再起動します。プライマリ PAN 再起動後にシステムは一度に 1 つのノードを再起動します。

ステップ 8 **[送信（Submit）]** をクリックして証明書署名要求を CA 署名付き証明書とバインドします。

この証明書の使用方法が Cisco ISE ノード間通信用としてマークされている場合は、Cisco ISE ノードのアプリケーションサーバーが再起動します。

このプロセスを繰り返して、証明書署名要求と展開内の他のノード上の CA 署名付き証明書をバインドします。

次のタスク

信頼できる証明書ストアへのルート証明書のインポート （587 ページ）

証明書署名要求のエクスポート

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 証明書署名要求がローカルファイルシステムにダウンロードされます。

証明書署名要求の設定

Cisco ISE では、1 つの要求で、管理者ポータルから展開内のすべてのノードの証明書署名要求を生成することができます。また、展開内の単一ノードか、または複数両方のノードのどちらの証明書署名要求を生成するのかを選択することもできます。単一ノードの証明書署名要求を生成する場合、ISE は証明書サブジェクトの [CN] フィールドを、その特定ノードの完全修飾ドメイン名（FQDN）に自動的に置き換えます。[CN] フィールドにそのノードの FQDN 以外のドメイン名を入力すると、Cisco ISE はその証明書による認証を拒否します。証明書の [サブジェクト代替名（Subject Alternative Name (SAN)）] フィールドにエントリを含めることを選択した場合、他の SAN 属性に加えて ISE ノードの FQDN を入力する必要があります。必要に応じて、[SAN] フィールドに FQDN を追加することもできます。展開内のすべてのノードの証明書署名要求を生成することを選択した場合は、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] チェックボックスをオンにして、[SAN] フィールド（DNS 名）にワイルドカード表記で FQDN を入力します（*.amer.example.com など）。EAP 認証に証明書を使用する場合は、[CN=] フィールドにワイルドカード値を入力しないでください。

ワイルドカード証明書を使用することにより、各 Cisco ISE ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用すると、展開内の複数の両方のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバー証明書を割り当てる場合よりも安全性が低いと見なされます。

次の表では、認証局（CA）が署名可能な証明書署名要求の生成に使用できる [証明書署名要求（Certificate Signing Request）] ページのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書管理（Certificate Management）]** > **[証明書署名要求（Certificate Signing Request）]** の順に選択します。

表 *31 :* 証明書署名要求の設定

フィールド	使用上のガイドライン
証明書の用途（Certificate(s) will be used for）	

フィールド	使用上のガイドライン
	証明書を使用するサービスを選択します。 **Cisco ISE ID 証明書** • [複数使用（Multi-Use）]：複数のサービス（管理者、EAP-TLS 認証、pxGrid、およびポータル）に使用されます。複数使用の証明書は、クライアントとサーバー両方のキーの用途を使用します。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [管理者（Admin）]：サーバー認証に使用されます（管理者ポータルとの通信および展開内の ISE ノード間の通信を保護するため）。署名 CA の証明書テンプレートは、Web サーバー証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） • [EAP 認証（EAP Authentication）]：サーバー認証に使用されます。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） （注） EAP-TLS クライアント証明書にデジタル署名キー使用法を使用する必要があります。 • [RADIUS DTLS]：RADIUS DTLS サーバーの認証に使用されます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） • [ISEメッセージングサービス（ISE Messaging Service）]：Cisco ISE メッセージングを介した Syslog 機能に使用されます。組み込みの UDP syslog 収集ターゲット（LogCollector および LogCollector2）用の MnT WAN 存続を有効にします。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） • [ポータル（Portal）]：サーバー認証に使用されます（すべての ISE Web ポータルとの通

フィールド	使用上のガイドライン
	信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） • [pxGrid]：クライアント認証とサーバー認証の両方に使用されます（pxGrid クライアントとサーバー間の通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバー証明書。SAML での使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） （注） 拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用しないことをお勧めします。拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用する場合、証明書は無効と見なされ、次のエラー メッセージが表示されます。 `source=local ; type=fatal ; message="unsupported certificate"` **Cisco ISE 認証局証明書**

フィールド	使用上のガイドライン
	• [ISE ルート CA（ISE Root CA）]：（内部 CA サービスにのみ適用可能）プライマリ PAN のルート CA および PSN の下位 CA を含む内部 CA 証明書チェーン全体を再生成するために使用されます。 • [ISE 中間 CA（ISE Intermediate）]：（ISE が外部 PKI の中間 CA として機能する場合に内部 CA サービスにのみ適用可能）プライマリ PAN の中間 CA 証明書および PSN の下位 CA 証明書の生成に使用されます。署名 CA の証明書テンプレートは、下位認証局と呼ばれます。このテンプレートには、次のプロパティがあります。 • [基本制約（Basic Constraints）]：重要、認証局 • [キーの用途（Key Usage）]：証明書の署名、デジタル署名 • [キーの拡張用途（Extended Key Usage）]：OCSP 署名（1.3.6.1.5.5.7.3.9） • [ISE OCSP 応答側証明書の更新（Renew ISE OCSP Responder Certificates）]：（内部 CA サービスにのみ適用可能）展開全体の ISE OCSP 応答側証明書の更新に使用されます（証明書署名要求ではありません）。セキュリティ上の理由から、ISE OCSP 応答側証明書を 6 ヵ月ごとに更新することを推奨します。
ワイルドカード証明書の許可（Allow Wildcard Certificates）	証明書の [SAN] フィールドの CN/DNS 名にワイルドカード文字（*）を使用するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、展開内のすべてのノードが自動的に選択されます。左端のラベルの位置にアスタリスク（*）ワイルドカード文字を使用する必要があります。ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、セキュリティ上の問題が発生する可能性があります。
これらのノードの CSR の生成（Generate CSRs for these Nodes）	証明書を生成するノードの隣のチェックボックスをオンにします。展開内の選択されたノードの CSR を生成するには、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオフにします。
共通名（Common Name）（CN）	デフォルトでは、共通名は証明書署名要求を生成する ISE ノードの FQDN です。$FQDN$ は ISE ノードの FQDN を意味します。展開内の複数ノードの証明書署名要求を生成すると、証明書署名要求の [共通名（Common Name）] フィールドは各 ISE ノードの FQDN に置き換えられます。
組織ユニット（Organizational Unit）（OU）	組織ユニット名。Engineering など。
組織（Organization）（O）	組織名。Cisco など。
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。

フィールド	使用上のガイドライン
国（Country）（C）	国名。2 文字の ISO 国番号を入力する必要があります。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	証明書に関連付けられている IP アドレス、DNS 名、Uniform Resource Identifier（URI）、またはディレクトリ名。 • [DNS 名（DNS Name）]：DNS 名を選択した場合は、ISE ノードの完全修飾ドメイン名を入力します。[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオンにした場合は、ワイルドカード表記（ドメイン名の前にアスタリスクとピリオドを入力）を指定します。*.amer.example.com など。 • [IP アドレス（IP Address）]：証明書に関連付けられる ISE ノードの IP アドレス。 • [ユニフォームリソース識別子（Uniform Resource Identifier）]：証明書に関連付ける URI。 • [ディレクトリ名（Directory Name）]：RFC 2253 に従って定義される識別名（DN）の文字列表現。DN 間はカンマ（,）で区切ります。「dnQualifier」RDN の場合は、カンマをエスケープし、区切り文字としてバックスラッシュ カンマ「\,」を使用します。たとえば、CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL などです。
キータイプ（Key Type）	RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。
キーの長さ（Key Length）	公開キーのビット サイズを指定します。 RSA には、次のオプションを使用できます。 • 512 • 1024 • 2048 • 4096 ECDSA には、次のオプションを使用できます。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。 パブリック CA の署名付き証明書を取得するか、FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は 2048 以上を選択します。
署名するダイジェスト（Digest to Sign With）	ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。
証明書ポリシー（Certificate Policies）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。

関連トピック

証明書署名要求 （595 ページ）
証明書署名要求の作成と認証局への送信 （596 ページ）
証明書署名要求への CA 署名付き証明書のバインド （596 ページ）

ポータルで使用する証明書のセットアップ

Web ポータル要求を処理できる展開に複数の PSN がある場合、Cisco ISE には一意の ID が必要です。この ID で、ポータルの通信に使用する必要がある証明書を識別します。ポータルでの使用に指定された証明書を追加またはインポートする場合、証明書グループタグを定義して、それを展開内の各ノードの対応する証明書に関連付けます。この証明書グループタグを対応するエンドユーザーポータル（ゲスト、スポンサー、およびパーソナルデバイスポータル）に関連付けます。この証明書グループタグは一意の ID で、Cisco ISE が各ポータルと通信する際に使用する必要がある証明書を識別する場合に役立ちます。ポータルごとに各ノードから指定できる証明書は 1 つのみです。

（注） Cisco ISE は TCP ポート 8443（またはポータルが使用するように設定したポート）でポータル証明書を提示します。

ステップ 1 証明書署名要求の作成と認証局への送信 （596 ページ）。

すでに定義済みの証明書グループ タグを選択するか、ポータル用に新しく作成する必要があります。たとえば、mydevicesportal などです。

ステップ 2 信頼できる証明書ストアへのルート証明書のインポート （587 ページ）。

ステップ 3 証明書署名要求への CA 署名付き証明書のバインド （596 ページ）。

CA 署名付き証明書へのデフォルトのポータル証明書グループ タグの再割り当て

デフォルトでは、すべての Cisco ISE ポータルは自己署名証明書を使用します。ポータルに CA 署名付き証明書を使用する場合は、デフォルトのポータル証明書グループ タグを CA 署名付き証明書に割り当てることができます。既存の CA 署名付き証明書を使用するか、または CSR を生成して、ポータルに使用する新しい CA 署名付き証明書を取得できます。1 つの証明書から別の証明書にポータル グループ タグを再割り当てすることができます。

（注） 新しい証明書を追加するときに、ポータルグループタグをデフォルトのポータル証明書グループタグから別のポータルグループタグに再割り当てできます。これにより、デフォルトで証明書に関連付けられているすべてのポータルが、そのポータルグループタグのみにマッピングされているポータルに変更されます。これらのポータルのリストが表示されます。既存の証明書を編集する場合、証明書に関連付けられているポータルタグがいずれかのポータルですでに使用されている場合は、デフォルトのポータル証明書グループタグまたは他のポータルグループタグをこの証明書に再割り当てすることはできません。

次に、CA 署名付き証明書にデフォルトのポータル証明書グループ タグを再割り当てする手順について説明します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

このタグを使用するポータルのリストを表示するには、デフォルトのポータル証明書グループ タグの横にある i アイコンにマウス ポインタを合わせます。このタグが割り当てられているポータル証明書がある展開内の ISE ノードを表示することもできます。

ステップ 2 ポータルに使用する CA 署名付き証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

いずれのポータルでも使用されていない CA 署名付き証明書を選択してください。

ステップ 3 [使用方法（Usage）] 領域で、[ポータル（Portal）] チェックボックスをオンにして、デフォルトのポータル証明書グループ タグを選択します。

ステップ 4 [保存（Save）] をクリックします。

警告メッセージが表示されます。

ステップ 5 [はい（Yes）] をクリックして、CA 署名付き証明書にデフォルトのポータル証明書グループ タグを再割り当てします。

ノードの登録前のポータル証明書タグの関連付け

展開内のすべてのポータルに「デフォルト ポータル証明書グループ」タグを使用する場合は、新しい ISE ノードを登録する前に、関連する CA 署名付き証明書をインポートし、サービスとして「ポータル」を選択し、この証明書に「デフォルト ポータル証明書グループ」タグを関連付けます。

展開に新しいノードを追加すると、デフォルトの自己署名証明書が「デフォルト ポータル証明書グループ」タグに関連付けられ、このタグを使用するようにポータルが設定されます。

新しいノードの登録後、証明書グループ タグの関連付けは変更できません。したがって、展開にノードを登録する前に、次を実行してください。

ステップ 1 自己署名証明書を作成し、サービスとして「ポータル」を選択し、別の証明書グループ タグ（たとえば、tempportaltag）を割り当てます。

ステップ 2 新しく作成した証明書グループ タグ（tempportaltag）を使用するようにポータル設定を変更します。

ステップ 3 デフォルト自己署名証明書を編集し、ポータル ロールを削除します。

このオプションは、デフォルト ポータル証明書グループ タグとデフォルト自己署名証明書との関連付けを削除します。

ステップ 4 次のいずれかを実行します。

オプション	説明
CSR の生成	CSR を生成するときは、次を実行します。 **1.** この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。 **2.** CSR を CA に送信し、署名付きの証明書を取得します。 **3.** 信頼できる証明書ストアに証明書に署名した CA のルートおよび他の中間証明書をインポートします。 **4.** CSR に CA 署名付き証明書をバインドします。
秘密キーと CA 署名付き証明書のインポート	CA 署名付き証明書をインポートするときは、次を実行します。 **1.** この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。 **2.** 信頼できる証明書ストアに証明書に署名した CA のルートおよび他の中間証明書をインポートします。
既存の CA 署名付き証明書の編集	既存の CA 署名付き証明書を編集するときは、次を実行します。 この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。

ステップ 5 展開に ISE ノードを登録します。
展開内のポータル構成は「デフォルト ポータル証明書グループ」タグに設定され、ポータルは新しいノードの「デフォルト ポータル証明書グループ」タグに関連付けられた CA 署名付き証明書を使用するように設定されます。

ユーザーおよびエンドポイントの証明書の更新

デフォルトでは、Cisco ISE は証明書が期限切れになったデバイスからの要求を拒否します。ただし、このデフォルト動作を変更し、このような要求を処理し、ユーザーに証明書の更新を求めるように ISE を設定できます。

ユーザーが証明書を更新することを許可する場合は、要求をさらに処理する前に証明書が更新されたかどうかを判断する許可ポリシールールを設定することを推奨します。証明書が期限切れになったデバイスからの要求を処理することで、潜在的なセキュリティ脅威が発生する可能性があります。組織のセキュリティが侵害されていないことを保証するには、適切な許可プロファイルおよびルールを設定する必要があります。

あるデバイスは有効期限の前後に証明書を更新できます。ただし、Windows デバイスでは、期限切れになる前にだけ証明書を更新できます。Apple iOS、Mac OSX、および Android デバイスでは、有効期限の前または後に証明書を更新できます。

ポリシー条件で証明書更新に使用されるディクショナリ属性

Cisco ISE 証明書ディクショナリには、ユーザーに証明書更新を許可するポリシー条件で使用される次の属性が含まれます。

- [有効期限までの日数（Days to Expiry）]：この属性は、証明書が有効な日数を指定します。この属性を使用して、許可ポリシーで使用できる条件を作成できます。この属性には、0 ～ 15 の値を指定できます。0 の値は、証明書の有効期限がすでに切れていることを示します。1 の値は、証明書の有効期限が切れるまで 1 日未満であることを示します。
- [有効期限切れ（Is Expired）]：このブール属性は、証明書が有効期限切れかどうかを示します。証明書の有効期限が近く、有効期限切れではない場合にのみ証明書更新を許可する場合は、許可ポリシー条件でこの属性を使用します。

証明書を更新するための CWA リダイレクト

ユーザー証明書が期限切れになる前に失効している場合、Cisco ISE は、CA がパブリッシュした CRL をチェックして認証要求を拒否します。失効した証明書の期限が切れている場合は、CA が CRL でこの証明書をパブリッシュしない可能性があります。このシナリオでは、失効した証明書が Cisco ISE によって更新される可能性があります。このことを避けるために、証明書を更新する前に、要求が中央 Web 認証（CWA）にリダイレクトされ、完全認証が実行されるようにします。CWA のユーザーをリダイレクトするには、許可プロファイルを作成する必要があります。

ユーザーによる証明書の更新を許可する Cisco ISE の設定

ユーザーが証明書を更新できるように Cisco ISE を設定するには、この手順で示すタスクを実行する必要があります。

始める前に

WLC で制限されたアクセス ACL を設定して、CWA 要求をリダイレクトします。

ステップ 1 許可されるプロトコルの設定の更新 （608 ページ）

ステップ 2 CWA リダイレクションの許可ポリシー プロファイルの作成 （608 ページ）

ステップ 3 証明書を更新する認証ポリシールールを作成します。

ステップ 4 ゲストポータルでの BYOD 設定の有効化 （609 ページ）

許可されるプロトコルの設定の更新

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）] > [デフォルト ネットワーク アクセス（Default Network Access）]** を選択します。

ステップ 2 PEAP および EAP-FAST プロトコルの EAP-TLS プロトコルおよび EAP-TLS 内部方式の下の [許可ポリシーの証明書更新を可能にするために失効した証明書の認証を許可（Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy）] チェックボックスをオンにします。

EAP-TLS プロトコルを使用する要求が NSP フローを通過します。

PEAP および EAP-FAST プロトコルの場合、Cisco ISE が要求を処理するには Cisco Secure Client（AnyConnect を含む）のネットワーク アクセス マネージャ コンポーネントを手動でインストールして設定する必要があります。

ステップ 3 [送信（Submit）] をクリックします。

次のタスク

CWA リダイレクションの許可ポリシー プロファイルの作成 （608 ページ）

CWA リダイレクションの許可ポリシー プロファイルの作成

始める前に

WLC で制限されたアクセス ACL が設定されていることを確認します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 許可プロファイルの名前を入力します。たとえば、CertRenewal_CWA です。

ステップ 4 [共通タスク（Common Tasks）] 領域の [Web リダイレクション（CWA、DRW、MDM、NSP、CPP）（Web Redirection (CWA, DRW, MDM, NSP, CPP)）] チェックボックスをオンにします。

ステップ 5 ドロップダウン リストの [中央集中 Web 認証（Centralized Web Auth）] および制限されたアクセス ACL を選択します。

ステップ 6 [証明書更新メッセージの表示（Display Certificates Renewal Message）] チェックボックスをオンにします。

url-redirect 属性値が変更され、この値に証明書が有効である日数が含まれます。

ステップ 7 [送信（Submit）] をクリックします。

ゲストポータルでの BYOD 設定の有効化

ユーザーがパーソナル デバイス証明書を更新できるようにするには、選択したゲスト ポータルで BYOD 設定を有効にする必要があります。

ステップ 1 **[ワークセンター（Work Center）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）]** を選択します。

a) 目的の CWA ポータルを選択して、[編集（Edit）] をクリックします。

ステップ 2 [BYOD 設定（BYOD Settings）] から [従業員にネットワークでのパーソナルデバイスの使用を許可する（Allow employees to use personal devices on the network）] チェックボックスをオンにします。

ステップ 3 [保存（Save）] をクリックします。

Apple iOS デバイスの証明書更新の失敗

ISE を使用して Apple iOS デバイスのエンドポイント証明書を更新する場合、「プロファイル済みでインストールできませんでした（Profiled Failed to Install）」エラー メッセージが表示される場合があります。このエラー メッセージは、同じポリシー サービス ノード（PSN）または別の PSN で、期限切れ間近または期限切れのネットワーク プロファイルが更新のプロセス時に使用されるものとは異なる管理者 HTTPS 証明書によって署名されている場合に表示されます。

回避策としては、展開内のすべての PSN で管理者 HTTPS 用にマルチドメイン SSL 証明書（通称 Unified Communications Certificates（UCC））またはワイルドカード証明書を使用します。

証明書定期チェックの設定

Cisco ISE は、証明書失効リスト（CRL）を定期的にチェックします。このウィンドウを使用して、自動的にダウンロードされた CRL に対して進行中のセッションを確認するように Cisco ISE を設定できます。OCSP または CRL のチェックを毎日開始する時刻と、OCSP サーバーまたは CRL を再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定できます。

次の表では、[証明書定期チェックの設定（Certificate Periodic Check Settings）] ウィンドウのフィールドについて説明します。このページを使用して、証明書（OCSP または CRL）のステータスを確認する時間間隔を指定できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [証明書定期チェックの設定（Certificate Periodic Check Settings）]**。

表 *32*：証明書定期チェックの設定

フィールド名	使用上のガイドライン
証明書チェックの設定	
自動的に取得されたCRLに対する進行中のセッションのチェック（Check ongoing sessions against automatically retrieved CRL）	Cisco ISE が自動的にダウンロードされた CRL に対する進行中のセッションをチェックするようにするには、このチェックボックスをオンにします。
CRL/OCSP の定期的な証明書チェック	
最初のチェック時刻（First check at）	CRL または OCSP のチェックを毎日開始する時刻を指定します。00:00 ～ 23:59 の時間範囲の値を入力します。
チェック間隔（Check every）	CRL または OCSP サーバーを再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定します。

Cisco ISE は、CRL 取得設定で LDAP バインディングタイプの指定を許可せず、証明書配布ポイントで匿名バインドを使用して LDAP URL に接続します。Cisco ISE では、LDAP サーバーへの認証用に LDAP バインディングのみがサポートされます。

Cisco ISE は、デフォルトで HTTP（ポート 80）、HTTPS（ポート 443）、および LDAP（ポート 389）プロトコルを CRL プロセスに使用します。Windows Vista SP1 および Windows Server 2008 エンドポイントの場合、Microsoft は CRL に対して次のプロトコルのみをサポートします。

- HTTP：PKI クライアントは、ローカルで設定されたプロキシに対してのみ認証を実行します。デフォルトでは、プロキシサーバーがプロキシ認証が必要であるというエラーメッセージを返した場合にのみ、認証が実行されます。
- LDAP：PKI クライアントは、PKI オブジェクトのすべての LDAP トラフィックに署名して暗号化し、ネットワークの取得に認証が必要な場合にのみ Kerberos 認証を使用します。

詳細については、「What's New in Certificate Revocation in Windows Vista and Windows Server 2008」[英語] を参照してください。

関連トピック

OCSP サービス （652 ページ）
OCSP クライアント プロファイルの追加 （655 ページ）

.pfx ファイルからの証明書と秘密キーの抽出

Cisco ISE では、.pfx 形式の証明書のインポートは許可されません。したがって、インポートする証明書が .pfx 形式の場合は、インポートする前に .pem または .key ファイル形式に変換する必要があります。

始める前に

SSL 証明書を含むサーバーに OpenSSL がインストールされていることを確認します。

ステップ 1 OpenSSL\bin フォルダから OpenSSL を起動します。

ステップ 2 コマンドプロンプトを開き、.pfx ファイルを含むフォルダに移動します。

ステップ 3 次のコマンドを実行して、秘密キーを .pem 形式で抽出します。**openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes**

インポートパスワードを入力するように求められます。.pfx ファイルを作成したときにキーペアを保護するために使用したパスワードを入力します。作成する .pem ファイルを保護するために、新しいパスワードを入力するように再度求められます。誤用を防ぐために、パスワードを安全な場所のキーファイルに保存します。

ステップ 4 次のコマンドを実行して、証明書を .pem 形式で抽出します。**openssl pkcs12 -in certname.pfx -nokeys -out cert.pem**

ステップ 5 次のコマンドを実行して、秘密キーを復号します。**openssl rsa -in key.pem -out server.key**

前の手順で秘密キーファイルを保護するために作成したパスワードを入力します。

.pem ファイルと復号化および暗号化された .key ファイルは、OpenSSL を起動したパスで使用できます。

Cisco ISE CA サービス

証明書は、自己署名したり、外部認証局（CA）がデジタルで署名したりできます。Cisco ISE 内部認証局（ISE CA）は、従業員が企業ネットワークでパーソナル デバイスを使用できるように、一元的なコンソールからエンドポイントのデジタル証明書を発行し、管理します。CA 署名付きデジタル証明書は、業界標準であり、よりセキュアです。プライマリ PAN は、ルート CA です。ポリシー サービス ノード（PSN）は、プライマリ PAN の下位 CA です（SCEP RA）。ISE CA には次の機能があります。

- 証明書の発行：ネットワークに接続するエンドポイントの証明書署名要求（CSR）を検証し、署名します。
- キー管理：PAN ノードと PSN ノードの両方でキーと証明書を生成し、セキュアに保存します。
- 証明書ストレージ：ユーザーやデバイスに発行された証明書を保存します。

- Online Certificate Status Protocol（OCSP）サポート：OCSP 応答側に証明書の有効性を確認する手段を提供します。

CA サービスがプライマリ管理ノードで無効になっている場合でも、CA サービスはセカンダリ管理ノードの CLI で実行中として表示されます。理想的には、CA サービスは無効として表示される必要があります。これは、Cisco ISE の既知の問題です。

Cisco ISE 証明書フィンガープリント

証明書フィンガープリントプロセスは、証明書の即時発行者のフィンガープリント SHA256 を評価し、信頼できる証明書と照合するために使用されます。これにより、複数の CA が異なるドメインをサポートするためのセキュアなメカニズムが適用され、802.1x プロトコルに対して信頼できる CA をロックすることもできます。

ポリシー条件で証明書を更新する前に、発行者：フィンガープリント SHA-256 証明書が Cisco ISE 展開に追加されていることを確認します。

（注） 信頼できる証明書をポリシーで設定した後は、その証明書を削除できません。[信頼できる証明書（Trusted Certificates）] ウィンドウの、[この信頼できる証明書はポリシーセットで参照される（This Trusted Certificate Refered by Policy Sets）] セクションに、次のメッセージが表示されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]>[システム（System）]>[証明書（Certificates）]>[信頼できる証明書（Trusted Certificates）]** を選択します。

```
Certificate cannot be deleted because it is used in a policy. To delete
the certificate, please modify policy condition first.
```

Cisco ISE の証明書フィンガープリントを設定するには、次の順序に従って手順を実行します。

1. 内部ユーザーを作成します。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.0』の「Asset Visibility」の章にある「Add Users」のセクションを参照してください。
2. ネットワークデバイスを追加します。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.0』の「Basic Setup」の章にある「Add a Network Device in Cisco ISE」のセクションを参照してください。
3. 外部証明書に外部 CA をインポートします。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.0』の「Basic Setup」の章にある「Import a System Certificate」のセクションを参照してください。

   SCEP プロトコルを使用して Issuer-Fingerprint SHA-256 証明書をインポートすることもできます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]>[システム（System）]>[証明書（Certificates）]>[認証局（Certificate Authority）]>[外部 CA 設定（External CA Settings）]** を選択します。表示される [SCEP RA プロファイルの追加（Add SCEP RA Profile）] ウィンドウで、[追加（Add）] をクリックします。[名前（Name）] フィールドに、証明書名を入力します。[URL] フィー

ルドに、CA サーバーの URL を入力します。[テスト接続（Test Connection）] をクリックします。

4. SHA-256 フィンガープリントを使用したポリシーの作成。
5. SHA-256 フィンガープリントを使用した認証ポリシーの作成とマッピング。
6. 認証ポリシーの作成。
7. PRRT ログの確認。

SHA-256 フィンガープリントを使用したポリシーの作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシーセット（Policy Set）]**。

ステップ 2 表示される [ポリシーセット（Policy Set）] ウィンドウで [設定（Settings）] をクリックし、ドロップダウンリストから [新しい行の挿入（insert a new row）] を選択します。

ステップ 3 [新しいポリシー名（New Policy Name）] フィールドに名前を入力します。

ステップ 4 ポリシーの [説明（Description）] を入力します。

ステップ 5 [条件（Conditions）] 列の下にある新しい [ポリシーセット名（Policy Set Name）] の横にある [追加（Add）]（+）アイコンをクリックします。

ステップ 6 表示される [条件スタジオ（Condition Studio）] ウィンドウで、[クリックして属性を追加（Click to Add Attribute）] フィールドをクリックします。

ステップ 7 [すべてのディクショナリ（All Dictionary）] ドロップダウンリストから、[ネットワークアクセスとプロトコル（Network Access-Protocol）]（[ディクショナリと属性（Dictionary-Attribute）]）の組み合わせを選択します。

ステップ 8 論理条件を作成するには、[等号（Equals）] 演算子を選択します。

ステップ 9 [リストから選択するか入力する（Choose from List or Type）] ドロップダウンリストから [RADIUS] を選択します。

ステップ 10 [使用（Use）] をクリックします。

ステップ 11 表示される [ポリシーセット（Policy Set）] ウィンドウの [許可されるプロトコル/サーバーの順序（Allowed Protocols/ Server Sequence）] ドロップダウンリストから、[デフォルトのネットワークアクセス（Default Network Access）] を選択します。

ステップ 12 [保存（Save）] をクリックします。

SHA-256 フィンガープリントを使用した認証ポリシーの作成とマッピング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] > [デフォルト（Default）]**。

ステップ 2 [認証ポリシー（Authentication Policy）] をクリックします。

ステップ 3 設定アイコンをクリックし、[新しい行の挿入（insert a new row）] を選択します。

ステップ 4 [認証ルール名（Authentication Rule Name）] ウィンドウに名前を入力します。

ステップ 5 ルール名の横にある [追加（Add）] アイコン（[+]）をクリックします。

ステップ 6 表示される [条件スタジオ（Condition Studio）] ウィンドウで、[クリックして属性を追加（Click to add Attributes）] フィールドをクリックします。

ステップ 7 [すべてのディクショナリ（All Dictionary）] ドロップダウンリストから、**CERTIFICATE-Issuer- Fingerprint SHA-256**（[ディクショナリと属性（Dictionary-Attribute）]）の組み合わせを選択します。

ステップ 8 論理条件を作成するには、[等号（Equals）] 演算子を選択します。

ステップ 9 [リストまたはタイプから選択（Choose from List or Type）] ドロップダウンリストから [Cisco Manufacturing CA SHA2 fingerprint sha256] を選択します。

ステップ 10 [使用（Use）] をクリックします。

ステップ 11 表示される [ポリシーセット（Policy Set）] ウィンドウの [許可されるプロトコル/サーバーの順序（Allowed Protocols/ Server Sequence）] ドロップダウンリストから、[Preloaded_Certificate_Profile] を選択します。

ステップ 12 [保存（Save）] をクリックします。

認証ポリシーの作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] > [デフォルト（Default）]** を選択します。

ステップ 2 [認証ポリシー（Authorization Policy）] をクリックします。

ステップ 3 設定アイコンをクリックし、ドロップダウンリストから [新しい行の挿入（insert a new row）] を選択します。

ステップ 4 [認証ルール名（Authentication Rule Name）] ウィンドウで、名前を入力します。

ステップ 5 ルール名の横にある [追加（Add）] アイコン（[+]）をクリックします。

ステップ 6 表示される [条件スタジオ（Condition Studio）] ウィンドウで、[クリックして属性を追加（Click to add Attributes）] フィールドをクリックします。

ステップ 7 [すべてのディクショナリ（All Dictionary）] ドロップダウンリストから、**CERTIFICATE-Issuer- Fingerprint SHA-256**（[ディクショナリと属性（Dictionary-Attribute）]）の組み合わせを選択します。

ステップ 8 論理条件を作成するには、[等号（Equals）] 演算子を選択します。

ステップ 9 [リストまたはタイプから選択（Choose from List or Type）] ドロップダウンリストから、[Cisco Root CA 2099 フィンガープリント SHA（Cisco Root CA 2099 fingerprint sha）] を選択します。

ステップ 10 [使用（Use）] をクリックします。

ステップ 11 表示された [ポリシーセット（Policy Set）] ウィンドウの [許可されるプロトコル/サーバーの順序（Allowed Protocols/ Server Sequence）] ドロップダウンリストから、[PermitAccess] を選択します。

ステップ 12 [保存（Save）] をクリックします。

PRRT ログの確認

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[RADIUS]** > **[ライブログ（Live Logs）]**。

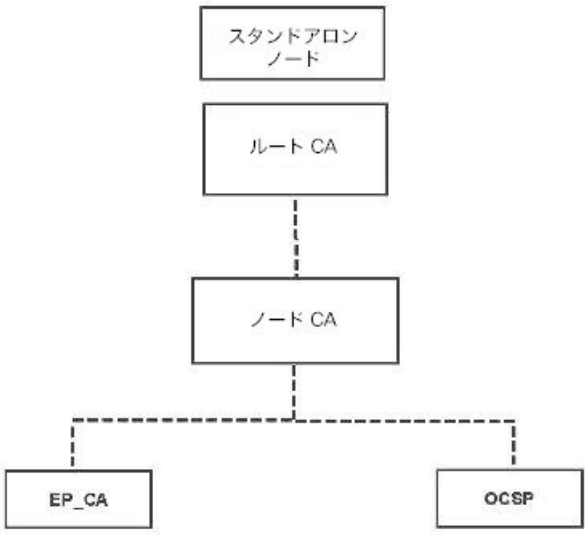
ステップ 2 表示される [ライブログ（Live Logs）] ウィンドウで、最新のログの詳細をクリックします。

ステップ 3 表示される [認証の詳細（Authentication Details）] ウィンドウで、[発行者：フィンガープリント SHA-256（Issuer-Fingerprint SHA-256）] 列の SHA-256 値を確認し、[発行者：フィンガープリント SHA-256（Issuer-Fingerprint SHA-256）] 証明書が正常に追加され、検証されていることを確認します。

管理ノードとポリシーサービスノードでプロビジョニングされるCisco ISE CA 証明書

インストール後に、Cisco ISE ノードはルート CA 証明書およびノード CA 証明書でプロビジョニングされ、エンドポイントの証明書が管理されます。

図 *9:* スタンドアロンノードでプロビジョニングされる *Cisco ISE CA* 証明書

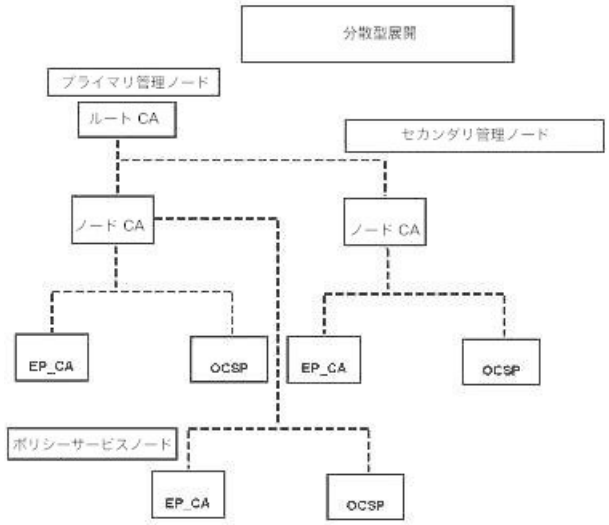


展開をセットアップすると、プライマリ管理ノード（PAN）として指定したノードがルート CA になります。PAN には、ルート CA 証明書と、ルート CA によって署名されたノード CA 証明書があります。

PAN にセカンダリ管理ノードを登録すると、ノード CA 証明書が生成され、プライマリ管理ノードでルート CA によって署名されます。

PAN に登録したポリシー サービス ノード（PSN）には、エンドポイント CA と、PAN のノード CA によって署名された OCSP 証明書がプロビジョニングされます。ポリシー サービス ノード（PSN）は、PAN の下位 CA です。ISE CA を使用すると、PSN のエンドポイント CA によってネットワークにアクセスするエンドポイントに証明書が発行されます。

図 *10 :* 展開内の管理ノードおよびポリシーサービスノードでプロビジョニングされる *Cisco ISE CA* 証明書



Cisco ISE と相互運用するための CA の要件

Cisco ISE で CA サーバーを使用しているときは、次の要件を満たしている必要があります。

- キー サイズは 1024、2048、またはそれ以上にする必要があります。CA サーバーでは、キー サイズは証明書テンプレートを使用して定義されます。サプリカント プロファイルを使用して Cisco ISE でキー サイズを定義できます。
- キーの使用法では、拡張された署名と暗号化を許可する必要があります。
- SCEP プロトコルを介して GetCACapabilities を使用する場合は、暗号化アルゴリズムと要求ハッシュがサポートされている必要があります。RSA と SHA1 を使用することをお勧めします。
- Online Certificate Status Protocol（OCSP）がサポートされます。これは BYOD では直接使用されませんが、OCSP サーバーとして機能できる CA は証明書失効に使用できます。

（注） Cisco ISE は、PEAP、EAP-TLS などの標準 EAP 認証用の Enterprise Java Beans 認証局（EJBCA）をサポートします。プロキシ SCEP の EJBCA サポートを有効にするには、EJBCA で [エンドエンティティ プロファイル制限の有効化（Enable End Entity Profile Limitations）] オプション（[システム（System）]>[基本設定（Basic Configurations）] の下）を無効にする必要があります。

- エンタープライズ PKI を使用して Apple iOS デバイスの証明書を発行する場合は、SCEP テンプレートでキーの使用法を設定し、[キーの暗号化（Key Encipherment）] オプションを有効にする必要があります。

Microsoft CA を使用する場合は、証明書テンプレートのキー使用法拡張機能を編集します。[暗号化（Encryption）] 領域で、[キーの暗号化でのみキーの交換を許可する（Allow key exchange only with key encryption (key encipherment)）] オプションボタンをクリックし、[ユーザーデータの暗号化を許可する（Allow encryption of user data）] チェックボックスもオンにします。

- Cisco ISE は、EAP-TLS 認証の信頼できる証明書およびエンドポイント証明書に対して、RSASSA-PSS アルゴリズムの使用をサポートしています。証明書を表示すると、署名アルゴリズムは、アルゴリズム名ではなく、1.2.840.113549.1.1.10 としてリストされます。

（注） BYOD フローに Cisco ISE 内部の CA を使用する場合、管理証明書は（外部 CA で）RSASSA-PSS アルゴリズムを使用して署名できません。Cisco ISE 内部の CA は、このアルゴリズムを使用して署名された管理証明書を検証できず、要求が失敗します。

証明書ベースの認証のためのクライアント証明書の要件

Cisco ISE による証明書ベースの認証では、クライアント証明書が次の要件を満たしている必要があります。

表 *33* : クライアント *RSA* および *ECC* の証明書要件

RSA		
サポートされているキーサイズ	1024、2048、および 4096 ビット	
サポートされているセキュアハッシュ アルゴリズム（SHA）	SHA-1 および SHA-2（SHA-256 を含む）	
ECC [12]		
サポートされる曲線タイプ	P-192、P-256、P-384、および P-521	
サポートされているセキュアハッシュ アルゴリズム（SHA）	SHA-256	
クライアントマシンのオペレーティングシステムとサポートされている曲線タイプ		
Windows	8 以降	P-256、P-384、P-521

Android	4.4 以降 （注） Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ（P-192 曲線タイプをサポートしていない Androidv6.0 を除く）。

[1] Windows 7 と Apple iOS は、EAP-TLS 認証用の ECC をネイティブでサポートしていません。

[2] Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

Cisco ISE CA チェーンの再生成

Cisco ISE CA チェーンを再生成すると、ルート CA、ノード CA、およびエンドポイント CA 証明書を含むすべての証明書が再生成されます。PAN または PSN のドメイン名またはホスト名を変更すると、ISE CA チェーンを再生する必要があります。

システム証明書を再生成すると、ルート CA または中間 CA 証明書のいずれでも、ISE メッセージングサービスが再起動して新しい証明書チェーンがロードされます。監査ログは、ISE メッセージングサービスが再び利用可能になるまで失われます。

（注） 展開で Cisco ISE の内部 CA を置き換えるたびに、完全な証明書チェーンを取得するように ISE メッセージングサービスも更新する必要があります。

Cisco ISE 内部 CA チェーンを再生成すると、チェーン内のすべての証明書の [有効期限の開始（Valid From）] フィールドに、再生成の 1 日前の日付が表示されます。

ドメインまたはホスト名に変更があり、ルート CA チェーンが再生成されると、システム証明書を含むすべての証明書が、SAML 証明書を除く新しいドメインまたはホスト名で更新されます。SAML 証明書は個別に再生成する必要があります。

外部 CA による Cisco ISE メッセージング証明書のサポート

外部 CA によって署名された Cisco ISE メッセージング証明書は、EKU クライアントおよびサーバー認証（pxGrid など）で設定する必要があります。pxgrid テンプレートを設定するには、https://community.cisco.com/t5/security-documents/deploying-certificates-with-cisco-pxgrid-using-an-external/ta-p/3639677 を参照してください。Cisco ISE メッセージング証明書は、すべてのノードで Cisco ISE によって内部的に署名されるか、外部（サードパーティ）CA によって署名される必要があります。両方の署名を組み合わせることはできません。

ワイルドカード証明書はサポートされていません。

楕円曲線暗号化証明書のサポート

Cisco ISE CA サービスが、楕円曲線暗号化（ECC）アルゴリズムに基づく証明書をサポートするようになりました。ECC は、より小さいキー サイズを使用している場合でも、他の暗号化アルゴリズムよりも高いセキュリティとパフォーマンスを提供します。

次の表では、ECC および RSA のキー サイズとセキュリティ強度を比較しています。

ECC のキー サイズ（ビット単位）	**RSA のキー サイズ（ビット単位）**
160	1024
224	2048
256	3072
384	7680
521	15360

キー サイズが小さいため、暗号化が迅速になります。

Cisco ISE では、次の ECC 曲線タイプがサポートされています。曲線タイプまたはキー サイズが大きくなると、セキュリティが強化されます。

- P-192
- P-256
- P-384
- P-521

ISE は、証明書の EC 部分の明示的なパラメータをサポートしていません。明示的なパラメータで証明書をインポートしようとすると、「証明書の検証に失敗しました」というエラーが表示されます。名前付き ECParameters のみがサポートされています。

Cisco ISE CA サービスは、BYOD フローを介して接続するデバイスの ECC 証明書をサポートします。また、証明書プロビジョニング ポータルから ECC 証明書を生成することもできます。

（注） 次の表に、ECC をサポートしているオペレーティング システムおよびバージョンと、サポートされている曲線タイプを示します。デバイスがサポートされているオペレーティング システムを実行していない場合、またはサポートされているバージョンでない場合には、代わりに RSA ベースの証明書を使用することもできます。

オペレーティングシステム	サポートされるバージョン	サポートされる曲線タイプ
Windows	8 以降	P-256、P-384、P-521
Android	4.4 以降 （注） Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ（P-192 曲線タイプをサポートしていない Android 6.0 を除く）。

Windows 7 と Apple iOS は、EAP-TLS を介した認証用の ECC をネイティブでサポートしていません。Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

Enrollment over Secure Transport（EST）プロトコルを備えた BYOD フローが適切に機能しない場合は、次のことを確認します。

- 証明書サービス エンドポイント サブ CA 証明書チェーンが完全であることを確認します。証明書チェーンが完全かどうかを確認するには：
  1. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）] の順に選択します。
  2. 確認する証明書の横にあるチェック ボックスをオンにして、[表示（View）]をクリックします。
- CA および EST サービスが起動し、実行されていることを確認します。サービスが実行されていない場合は、[管理（Administration）]>[システム（System）]>[証明書（Certificates）] > [認証局（Certificate Authority）] > [内部CAの設定（Internal CA Settings）] に移動して CA サービスを有効にします。

（注）

- Cisco ISE のこのリリースでは、EST クライアントが Cisco ISE に存在する EST サーバーに対して直接認証を行うことはサポートされていません。Android または Windows エンドポイントでのオンボーディング時に、要求が ECC ベースの証明書用である場合には、ISE が EST フローをトリガーします。
- 認証プロファイルで静的 IP アドレス、FQDN、またはホスト名とともに EST プロトコルを使用すると、Android クライアントでの BYOD フローが失敗することがあります。回避策は、EST の代わりに SCEP を使用することです。ネイティブ サプリカント プロファイルで SCEP を設定できます。詳細については、「ネイティブ サプリカント プロファイルの作成」を参照してください。

Cisco ISE 認証局証明書

[認証局（CA）証明書（Certificate Authority (CA) Certificates）] ページには、内部 Cisco ISE CA に関連するすべての証明書が表示されます。以前のリリースでは、これらの CA 証明書は信頼できる証明書ストアにありましたが、現在は [CA 証明書（CA Certificates）] ページに移動しています。これらの証明書は、このページにノード方式で表示されます。ノードを展開して、その特定のノードの ISE CA 証明書をすべて表示することができます。プライマリおよびセカンダリ管理ノードには、ルート CA、ノード CA、下位 CA、OCSP レスポンダ証明書があります。展開内の他のノードには、エンドポイント下位 CA および OCSP 証明書があります。

Cisco ISE CA サービスを有効にすると、すべてのノードでこれらの証明書が自動的に生成され、インストールされます。また、ISE ルート CA チェーン全体を置き換えると、すべてのノードでこれらの証明書が自動的に再生成され、インストールされます。手動による介入は必要ありません。

Cisco ISE CA 証明書は **Certificate Services <エンドポイント サブ *CA*/ノード *CA*/ルート *CA*/*OCSP* レスポンダ>-**<ノードのホスト名>**#**証明書番号という命名規則に従います。

[CA 証明書（CA Certificates）] ページで Cisco ISE CA 証明書を編集、インポート、エクスポート、削除、表示できます。

Cisco ISE CA 証明書の編集

証明書を Cisco ISE CA 証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。。

ステップ 2 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 。

ステップ 3 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 4 必要に応じて編集可能なフィールドを変更します。フィールドの説明については、信頼できる証明書の設定 （583 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックして、証明書ストアに対して行った変更を保存します。

Cisco ISE CA 証明書のエクスポート

Cisco ISE ルート CA およびノード CA 証明書をエクスポートするには、次の手順を実行します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。

ステップ 2 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 。

ステップ 3 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 4 クライアント ブラウザを実行しているファイル システムに Privacy Enhanced Mail ファイルを保存します。

Cisco ISE CA 証明書のインポート

エンドポイントが別の展開の Cisco ISE CA によって発行された証明書を使用してネットワークへの認証を試みる場合、Cisco ISE ルート CA、ノード CA、エンドポイント サブ CA 証明書をその展開から Cisco ISE の信頼できる証明書ストアにインポートする必要があります。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ISE ルート CA、ノード CA、エンドポイント サブ CA 証明書を、エンドポイント証明書が署名されている展開からエクスポートし、ブラウザが実行されているコンピュータのファイル システムに保存します。

ステップ 1 エンドポイントが認証されている展開の管理者用ポータルにログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 3 [インポート（Import）] をクリックします。

ステップ 4 必要に応じてフィールドの値を設定します。詳細については、信頼できる証明書のインポート設定 （588 ページ）を参照してください。

クライアント証明書ベースの認証が有効である場合は、Cisco ISE により展開内の各ノードのアプリケーション サーバーが再起動されます（最初に PAN のアプリケーション サーバーが再起動され、続いて追加のノードのアプリケーション サーバーが 1 つずつ再起動されます）。

証明書テンプレート

証明書テンプレートには、そのテンプレートに基づいて認証局（CA）によって発行されたすべての証明書に共通のプロパティが含まれています。証明書テンプレートは、件名、サブジェクト代替名（SAN）、キー タイプ、キー サイズ、使用する必要がある SCEP RA プロファイル、証明書の有効期間、証明書がクライアントまたはサーバーの認証またはその両方に使用される必要があるかどうかを指定した拡張キーの使用状況（EKU）を定義します。内部 Cisco ISE CA（ISE CA）は、証明書テンプレートを使用し、そのテンプレートに基づいて証明書を発行します。

Cisco ISE には、次の ISE CA のデフォルトの証明書テンプレートが付属しています。必要に応じて、追加の証明書テンプレートを作成できます。デフォルトの証明書テンプレートは次のとおりです。

- CA_SERVICE_Certificate_Template：Cisco ISE を認証局として使用するその他のネットワーク サービス用。たとえば、ASA VPN ユーザーに対し証明書を発行するには、ISE の設定時にこの証明書テンプレートを使用します。この証明書テンプレートでは、有効期間のみを変更できます。
- EAP_Authentication_Certificate_Template：EAP 認証用。
- pxGrid_Certificate_Template：証明書プロビジョニング ポータルから証明書を生成するときの pxGrid コントローラ用。

証明書テンプレート名の拡張子

Cisco ISE の内部 CA には、エンドポイント証明書を作成するために使用された証明書テンプレートを表す拡張子が含まれています。内部 CA によって発行されたすべてのエンドポイント証明書には、証明書テンプレート名の拡張子が含まれています。この拡張子は、そのエンドポイント証明書を作成するために使用された証明書テンプレートを表します。拡張子の ID は 1.3.6.1.4.1.9.21.2.5 です。CERTIFICATE: テンプレート名属性を許可ポリシーの条件に使用して、評価の結果に基づいて適切なアクセス権限を割り当てることができます。

許可ポリシー条件での証明書テンプレート名の使用

許可ポリシー ルールで証明書テンプレート名の拡張子を使用できます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー セット（Policy Sets）]** を選択し、許可ポリシー ルールを表示するデフォルトのポリシー セットを展開します。

ステップ 2 新しいルールを追加するか、既存のルールを編集します。次に、Compliant_Device_Access ルールを編集する例を示します。

a) Compliant_Device_Access ルールを編集します。
b) [属性/値の追加（Add Attribute/Value）] を選択します。
c) ディクショナリから、**CERTIFICATE: Template Name** 属性と **Equals** 演算子を選択します。
d) 証明書テンプレート名の値を入力します。たとえば、EAP_Authentication_Certificate_Template などです。

ステップ 3 [保存（Save）] をクリックします。

pxGrid コントローラ用の Cisco ISE CA 証明書の展開

Cisco ISE CA は、証明書プロビジョニング ポータルから証明書を生成するための pxGrid コントローラの証明書テンプレートを提供します。

始める前に

pxGrid クライアントの証明書署名要求（CSR）を生成し、CSR の内容をクリップボードにコピーします。

ステップ 1 ネットワーク アクセス ユーザー アカウントを作成します（[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [追加（Add）]）。

ユーザーが割り当てられているユーザー グループをメモします。

ステップ 2 証明書プロビジョニング ポータルの設定を編集します（[管理（Administration）]>[デバイス ポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）]）。

a) 証明書プロビジョニング ポータルを選択して、[編集（Edit）] をクリックします。
b) [ポータル設定（Portal Settings）] ドロップダウン リストをクリックします。[承認済みグループの設定（Configure authorized groups）] の選択可能なリストから、ネットワーク アクセス ユーザーが属すユーザー グループを選択して、選択済みリストに移動します。
c) [証明書プロビジョニング ポータル設定（Certificate Provisioning Portal Settings）] ドロップダウン リストをクリックします。[pxGrid_Certificate_Template] を選択します。詳しくは証明書プロビジョニング ポータルのポータル設定 （1912 ページ）を参照してください。
d) ポータル設定を保存します。

ステップ 3 証明書プロビジョニング ポータルを起動します。[ポータル テスト URL（Portal test URL）] リンクをクリックします。

a) 手順 1 で作成したユーザー アカウントを使用して証明書プロビジョニング ポータルにログインします。
b) AUP を受け入れ、[続行（Continue）] をクリックします。

c) [処理の選択（I want to）] ドロップダウン リストから、[単一の証明書の生成（証明書署名要求あり）（Generate a single certificate (with certificate signing request)）] を選択します。

d) [証明書署名要求の詳細（Certificate Signing Request Details）] フィールドに、クリップボードから CSR の内容を貼り付けます。

e) [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、[PKCS8 形式（PKCS8 format）] を選択します。

（注） [PKCS12 形式（PKCS12 format）] を選択する場合は、1 つの証明書ファイルを証明書ファイルとキー ファイルに分けて変換する必要があります。Cisco ISE にインポートする前に、証明書とキー ファイルはバイナリ DER エンコードまたは PEM 形式にする必要があります。

f) [証明書テンプレートの選択（Choose Certificate Template）] ドロップダウン リストから、[pxGrid_Certificate_Template] を選択します。

g) 証明書のパスワードを入力します。

h) [生成（Generate）] をクリックします。

証明書が生成されます。

i) 証明書をエクスポートします。

証明書チェーンとともに証明書がエクスポートされます。

ステップ 4 pxGrid クライアントの信頼できる証明書ストアに Cisco ISE CA チェーンをインポートします。

BYOD の MAC ランダム化

Android および iOS デバイスは、デフォルトでランダム MAC アドレスプロパティを使用するようになっています。ランダム MAC アドレス機能が有効になっているデバイスは、接続するすべての SSID にランダム MAC アドレスを使用します。Cisco ISE およびモバイルデバイス管理（MDM）システムは、サービスのために接続している SSID に応じて、同じデバイスの異なる MAC アドレスを受信します。したがって、GUID と呼ばれる一意の識別子が Cisco ISE プロビジョニングサービスによって生成され、両方のシステムで同じ値を使用してエンドポイントが識別されます。

EAP-TLS プロトコルを介した MAC アドレスと GUID によるエンドポイントの再認証の場合、コンテキスト可視性サービスを更新するための 1 秒あたりのトランザクション（TPS）は、1 秒あたり 12 ～ 15 エンドポイントです。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[証明書テンプレート（Certificate Templates）]**を選択します。

ステップ 2 [EAP証明書テンプレート（EAP Certificate Template）] の横にあるチェックボックスをオンにします。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 [サブジェクト代替名（SAN）（Subject Alternative Name (SAN)）] ドロップダウンリストで、[MAC アドレスと GUID（MAC Address and GUID）] を選択します。

BYOD フローでランダムおよび変更 MAC アドレスを処理するために、Cisco ISE プロビジョニングサービスは Windows、iOS、および Android エンドポイントの GUID 値を生成します。BYOD フローでランダム MAC アドレスを処理するために、GUID 値を証明書のサブジェクト代替名（SAN）に含めるように設定している場合は、AD ユーザーを認証する [TLS ベース認証の証明書認証プロファイルの作成] を設定するときに、ID 検証の証明書属性として [サブジェクト - 一般名（Subject - Common Name）] を選択します。

ステップ 5 [保存（Save）] をクリックします。

Simple Certificate Enrollment Protocol プロファイル

ユーザーがネットワークで登録できるさまざまなモバイルデバイスの証明書のプロビジョニング機能を有効にするために、1 つ以上の Simple Certificate Enrollment Protocol（SCEP）認証局（CA）プロファイル（Cisco ISE 外部 CA 設定と呼ばれます）を設定して、Cisco ISE に複数の CA の場所を指定できます。複数のプロファイルを使用できる利点は、ハイ アベイラビリティを実現し、指定した CA の場所の間でロードバランシングを実行できることです。特定の SCEP CA への要求に 3 回連続して応答がなかった場合、Cisco ISE は特定のサーバーが使用不能であると宣言し、次に負荷が小さく応答時間が短い既知の CA に自動的に移動し、サーバーがオンラインに復帰するまで、定期的なポーリングを開始します。

Microsoft SCEP サーバーを Cisco ISE と相互運用するように設定する方法については、次を参照してください。

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf

発行された証明書

管理者ポータルには、内部 ISE CA によってエンドポイントに対して発行されたすべての証明書のリストが示されます（[管理（Administration）] > [システム（System）] > [証明書（Certificates）]> [エンドポイント証明書（Endpoint Certificates）]）。[発行された証明書（Issued Certificates）] ページでは、証明書ステータスを一目で確認できます。証明書が失効している場合は、[ステータス（Status）] 列の上にマウス カーソルを移動すると、失効の理由を確認できます。[証明書テンプレート（Certificate Template）] 列の上にマウス カーソルを移動すると、キー タイプ、キー サイズ、曲線タイプ、サブジェクト、サブジェクト代替名（SAN）、証明書の有効性などの詳細情報を表示できます。エンドポイント証明書クリックして、証明書を表示できます。

ISE CA によって発行されたすべての証明書（BYOD フローを介して自動的にプロビジョニングされた証明書と証明書プロビジョニング ポータルから取得された証明書）は、[エンドポイント証明書（Endpoint Certificates）] ページにリストされます。このページからこれらの証明書を管理できます。

たとえば user7 に発行された証明書を確認する場合は、[フレンドリ名（Friendly Name）] フィールドの下に表示されるテキスト ボックスに「user7」と入力します。このユーザーに Cisco ISE によって発行されたすべての証明書が表示されます。フィルタをキャンセルするには、テキスト ボックスから検索語を削除します。また、[拡張フィルタ（Advanced Filter）] オプションを使用して、さまざまな検索基準に基づいてレコードを表示することもできます。

この [エンドポイント証明書（Endpoint Certificates）] ページには、必要に応じてエンドポイント証明書を取り消すためのオプションもあります。

[証明書管理概要（Certificate Management Overview）] ページには、展開内の各 PSN ノードによって発行されたエンドポイント証明書の合計数が表示されます。また、失効した証明書の合計数と失敗した証明書の合計数をノードごとに確認することもできます。このページのデータは任意の属性に基づいてフィルタリングできます。

発行および失効した証明書

次の表で、[発行および失効した証明書の概要（Overview of Issued and Revoked Certificates）] ウィンドウのフィールドについて説明します。展開内の PSN ノードがエンドポイントに証明書を発行します。このウィンドウでは、展開内の各 PSN ノードが発行するエンドポイント証明書に関する情報を示します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[概要（Overview）]** です。

（注） 期限切れまたは失効した発行済み証明書は、30 日後に自動的に削除されます。

表 *34* : 発行された証明書と失効した証明書

フィールド	使用上のガイドライン
[ノード名（Node Name）]	証明書を発行したポリシー サービス ノード（PSN）の名前。
[発行された証明書（Certificates Issued）]	PSN ノードが発行したエンドポイント証明書の数。
[取り消された証明書（Certificates Revoked）]	失効したエンドポイント証明書（PSN ノードが発行した証明書）の数。
[証明書要求（Certificates Requests）]	PSN ノードが処理した証明書ベースの認証要求の数。
[失敗した証明書（Certificates Failed）]	PSN ノードが処理する失敗した認証要求の数。

関連トピック

発行された証明書 （626 ページ）
ユーザーおよびエンドポイントの証明書の更新 （606 ページ）

証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 （631 ページ）
ユーザーによる証明書の更新を許可する Cisco ISE の設定 （607 ページ）
エンドポイント証明書の失効 （651 ページ）

Cisco ISE CA 証明書およびキーのバックアップと復元

PPAN に障害が発生し、セカンダリ管理ノードを外部 PKI のルート CA または中間 CA として機能させるために昇格する場合に備え、Cisco ISE CA 証明書およびキーをセキュアにバックアップして、セカンダリ管理ノードにこれらを復元できるようにする必要があります。Cisco ISE 設定のバックアップには、CA 証明書とキーは含まれていません。CA 証明書およびキーをリポジトリにエクスポートおよびインポートするには、代わりにコマンドライン インターフェイス（CLI）を使用する必要があります。**application configure ise** コマンドには、CA 証明書およびキーのバックアップと復元のためのエクスポートおよびインポートのオプションが含まれています。

信頼できる証明書ストアからの次の証明書が、セカンダリ管理ノードで復元されます。

- Cisco ISE ルート CA 証明書
- Cisco ISE サブ CA 証明書
- Cisco ISE エンドポイント RA 証明書
- Cisco ISE OCSP 応答側証明書

次の場合、Cisco ISE CA 証明書およびキーのバックアップおよび復元が必要となります。

- 展開内にセカンダリ管理ノードが存在する
- Cisco ISE CA ルート チェーン全体を置き換える
- 外部 PKI の下位 CA として機能するように Cisco ISE ルート CA を設定する
- 設定のバックアップからデータを復元する。この場合、最初に Cisco ISE CA ルート チェーンを再生成し、次に ISE CA 証明書およびキーのバックアップと復元を行う必要があります。

（注） 展開で Cisco ISE の内部 CA を置き換えるたびに、完全な証明書チェーンを取得するように ISE メッセージング サービスも更新する必要があります。

Cisco ISE CA 証明書およびキーのエクスポート

CA 証明書およびキーを PAN からエクスポートし、セカンダリ管理ノードでインポートする必要があります。このオプションでは、PAN がダウンした場合にセカンダリ管理ノードでエンドポイントの証明書を発行および管理し、セカンダリ管理ノードを PAN に昇格させることができます。

始める前に

CA 証明書およびキーを格納するためのリポジトリを作成したことを確認します。

ステップ 1 Cisco ISE CLI から、**application configure ise** コマンドを入力します。

ステップ 2 7 を入力して、証明書およびキーをエクスポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 暗号キーを入力します。

エクスポートされた証明書のリスト、件名、発行者、およびシリアル番号とともに成功メッセージが表示されます。

例：

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Cisco ISE CA 証明書およびキーのインポート

セカンダリ管理ノードを登録したら、PAN から CA 証明書およびキーをエクスポートし、セカンダリ管理ノードにインポートします。

ステップ 1 Cisco ISE CLI から、**application configure ise** コマンドを入力します。

ステップ 2 8 を入力して、CA 証明書およびキーをインポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 インポートするファイルの名前を入力します。ファイル名は **ise_ca_key_pairs_of_<vm hostname>** 形式である必要があります。

ステップ 5 ファイルを復号化するための暗号キーを入力します。

処理が正常に完了したことを知らせるメッセージが表示されます。

例：

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
```

```
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

（注） エクスポートされたキーファイルの暗号化は、Cisco ISE リリース 2.6 で導入されました。Cisco ISE リリース 2.4 以前のバージョンからのキーのエクスポート、および Cisco ISE リリース 2.6 以降のバージョンでのキーのインポートは成功しません。

プライマリ PAN および PSN でのルート CA および下位 CA の生成

展開をセットアップする場合、Cisco ISE は、Cisco ISE CA サービスの PSN のプライマリ PAN と下位の CA 証明書でルート CA を生成します。ただし、プライマリ PAN または PSN のドメイン名またはホスト名を変更する場合は、プライマリ PAN でルート CA、PSN で下位 CA をそれぞれ再生成する必要があります。

PSN のホスト名を変更する場合は、プライマリ PAN および PSN でそれぞれルート CA と下位 CA を再生成する代わりに、ホスト名を変更する前に PSN を登録解除し、再登録できます。新しい下位証明書は PSN 上で自動的にプロビジョニングされます。

（注） PXgrid および IMS 証明書は、それぞれの証明書が外部で署名されている場合、ルート CA の再生成中に内部 CA によって置き換えられません。

PXgrid 証明書の内部 CA による署名を変更する場合は、自己署名 Pxgrid 証明書を生成し、ルート CA を再生成します。

Cisco ISE メッセージングサービス証明書の内部 CA による署名を変更する場合は、CSR ページから Cisco ISE メッセージングサービス証明書を再生成します。

ステップ 1 次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]**

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用先（Certificate(s) will be used for）] ドロップダウン リストから ISE ルート CA を選択します。

ステップ 4 [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA Certificate chain）] をクリックします。

ルート CA と下位 CA 証明書が、展開内のすべてのノードに対して生成されます。

外部 PKI の下位 CA としての Cisco ISE ルート CA の設定

外部 PKI の下位 CA として機能する PAN のルート CA が必要な場合は、ISE 中間 CA 証明書署名要求を生成して、外部 CA に送信し、ルートおよび CA 署名付き証明書を入手して、ルート CA 証明書を信頼できる証明書ストアにインポートし、CA 署名付き証明書を CSR にバインドします。この場合、外部 CA はルート CA、プライマリ PAN は外部 CA の下位 CA、PSN はプライマリ PAN の下位 CA です。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用目的（Certificate(s) will be used for）] ドロップダウン リストから [ISE 中間 CA（ISE Intermediate CA）] を選択します。

ステップ 4 [生成（Generate）] をクリックします。

ステップ 5 CSR をエクスポートし、外部 CA に送信して、CA 署名付き証明書を取得します。

ステップ 6 信頼できる証明書ストアに外部 CA のルート CA 証明書をインポートします。

ステップ 7 CSR に CA 署名付き証明書をバインドします。

次のタスク

展開にセカンダリ PAN がある場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ PAN で復元します。サーバー証明書とルート証明書は、セカンダリ PAN に自動的に複製されます。この複製によって、管理ノードに障害が発生した場合に、セカンダリ PAN が外部 PKI の下位 CA として機能するようになります。

証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定

ネットワークに接続するエンドポイント（パーソナルデバイス）の証明書を発行し、管理するように Cisco ISE を設定できます。内部 Cisco ISE CA サービスを使用して、エンドポイントから証明書署名要求に署名したり、外部 CA に CSR を転送したりすることができます。

始める前に

- プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、ディザスタリカバリのため、安全な場所に保管してください。

ステップ 1 Employee ユーザーグループへのユーザーの追加 （632 ページ）。

内部 ID ストアまたは Microsoft Active Directory などの外部 ID ストアにユーザーを追加できます。

ステップ 2 TLS ベース認証の証明書認証プロファイルの作成 （633 ページ）。

ステップ 3 TLS ベース認証の ID ソース順序の作成 （633 ページ）。

ステップ 4 クライアント プロビジョニング ポリシーの作成：

a) 認証局の設定 （634 ページ）

b) CA テンプレートの作成 （635 ページ）

c) クライアント プロビジョニング ポリシーで使用されるネイティブ サプリカント プロファイルの作成 （638 ページ）

d) Cisco からの Windows および Mac OS X オペレーティングシステムのエージェントリソースのダウンロード （639 ページ）

e) Apple iOS、Android および MAC OS X デバイスのクライアント プロビジョニング ポリシー ルールの作成 （639 ページ）

ステップ 5 TLS ベース認証の Dot1X 認証ポリシー ルールの設定 （640 ページ）

ステップ 6 TLS ベース認証用の許可ポリシー ルールを設定します。

a) 中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成 （641 ページ）

b) 許可ポリシー ルールの作成 （642 ページ）

パーソナル デバイスからワイヤレス SSID に接続するときに ECC RSA ベースの証明書を使用すると、2 回目のパスワード入力を行うよう求められます。

Employee ユーザーグループへのユーザーの追加

次の手順では、Cisco ISE ID ストアの Employee ユーザー グループにユーザーを追加する方法について説明します。外部 ID ストアを使用した場合でも、ユーザーを追加できる Employee ユーザー グループがあることを確認します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ユーザーの詳細情報を入力します。

ステップ 4 [パスワード（Passwords）] セクションで、[ログインパスワード（Login Password）] と [TACACS+イネーブルパスワード（TACACS+ Enable Password）] を選択し、ネットワーク デバイスにアクセス レベルを設定します。

ステップ 5 [ユーザー グループ（User Group）] ドロップダウン リストから [従業員（Employee）] を選択します。

Employee ユーザー グループに属するすべてのユーザーが同じ権限セットを共有します。

ステップ 6 [送信（Submit）] をクリックします。

次のタスク

TLS ベース認証の証明書認証プロファイルの作成 （633 ページ）

TLS ベース認証の証明書認証プロファイルの作成

ネットワークに接続するエンドポイントの認証に証明書を使用するには、Cisco ISE で証明書認証プロファイルを定義するか、またはデフォルトの Preloaded_Certificate_Profile を編集する必要があります。証明書認証プロファイルには、プリンシパルユーザー名として使用する必要がある証明書フィールドが含まれています。たとえば、ユーザー名が [一般名（Common Name）] フィールドにある場合は、証明書認証プロファイルを [プリンシパル ユーザー名（Principal Username）] が [サブジェクト - 一般名（Subject - Common Name）] であるとして定義できます。これは ID ストアに照らして確認できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [証明書認証プロファイル（Certificate Authentication Profile）]** を選択します。

ステップ 2 証明書認証プロファイルの名前を入力します。たとえば、CAP となります。

ステップ 3 [サブジェクト - 一般名（Subject - Common Name）] に [プリンシパル ユーザー名 X509 属性（Principal Username X509 Attribute）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

TLS ベース認証の ID ソース順序の作成 （633 ページ）

TLS ベース認証の ID ソース順序の作成

証明書認証プロファイルを作成したら、Cisco ISE が証明書の属性を取得し、定義した ID ソースを ID ソース順序で照合できるように、証明書認証プロファイルを ID ソース順序に追加します。

始める前に

次のタスクが完了していることを確認します。

- Employee ユーザー グループへのユーザーの追加。
- 証明書ベースの認証の証明書認証プロファイルの作成。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ID ソース順序の名前を入力します。たとえば、Dot1X となります。

ステップ 4 [証明書認証プロファイルの選択（Select Certificate Authentication Profile）] チェックボックスをオンにし、作成した証明書認証プロファイル、つまり CAP を選択します。

ステップ 5 ユーザー情報を含む ID ソースを [認証検索リスト（Authentication Search List）] 領域の [選択済み（Selected）] リスト ボックスに移動します。

追加の ID ソースを追加すると、一致が見つかるまで Cisco ISE は、これらのデータ ストアを順に検索します。

ステップ 6 [ユーザーが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）] オプション ボタンをクリックします。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

認証局の設定 （634 ページ）

認証局の設定

CSR への署名に外部 CA を使用する場合、外部 CA を設定する必要があります。外部 CA 設定は Cisco ISE の以前のリリースでは、SCEP RA プロファイルと呼ばれていました。Cisco ISE CA を使用する場合、CA 設定を明示的に設定する必要はありません。[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [内部 CA 設定（Internal CA Settings）] で、内部 CA 設定を確認できます。

ユーザーのデバイスが検証済みの証明書を受信すると、証明書はデバイス上の次の表の場所に置かれます。

表 *35 :* デバイス証明書の場所

デバイス	証明書ストレージの場所	アクセス方式
iPhone/iPad	標準の証明書ストア	[設定（Settings）] > [一般（General）] > [プロファイル（Profile）]
Android	暗号化された証明書ストア	エンド ユーザーに不可視です。 （注） 証明書は、[設定（Settings）] > [ロケーションおよびセキュリティ（Location & Security）] > [ストレージのクリア（Clear Storage）] を使用して削除できます。
Windows	標準の証明書ストア	**/cmd** プロンプトから mmc.exe を起動するか、または証明書スナップインで表示します。

デバイス	証明書ストレージの場所	アクセス方式
Mac	標準の証明書ストア	[アプリケーション（Application）] > [ユーティリティ（Utilities）] > [キーチェーン アクセス（Keychain Access）]

始める前に

証明書署名要求（CSR）への署名に外部認証局（CA）を使用する場合は、外部 CA の URL が必要となります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [外部 CA 設定（External CA Settings）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 外部 CA 設定の名前を入力します。たとえば、EXTERNAL_SCEP などです。

ステップ 4 [URL] テキスト ボックスに、外部 CA サーバーの URL を入力します。

外部 CA が到達可能かどうかを確認するには、[テスト接続（Test Connection）] をクリックします。追加 CA サーバーの URL を入力するには、[+] ボタンをクリックします。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

CA テンプレートの作成 （635 ページ）

CA テンプレートの作成

証明書テンプレートは、（内部または外部 CA のために）使用する必要がある SCEP RA プロファイル、キー タイプ、キー サイズ、曲線タイプ、サブジェクト、サブジェクト代替名（SAN）、証明書の有効期間、拡張キーの使用状況を定義します。この例では、内部 Cisco ISE CA を使用すると想定します。外部 CA テンプレートの場合、有効期間は外部 CA によって決定され、指定することはできません。

新しい CA テンプレートを作成するか、デフォルトの証明書テンプレート EAP_Authentication_Certificate_Template を編集できます。

デフォルトでは、次の CA テンプレートが Cisco ISE で使用できます。

- CA_SERVICE_Certificate_Template：ISE CA を使用する他のネットワーク サービス用。たとえば、ASA VPN ユーザーに対し証明書を発行するには、ISE の設定時にこの証明書テンプレートを使用します。
- EAP_Authentication_Certificate_Template：EAP 認証用。
- pxGrid_Certificate_Template：証明書プロビジョニング ポータルから証明書を生成する際の pxGrid コントローラ用。

（注） ECC キー タイプを使用する証明書テンプレートは、内部 Cisco ISE CA とのみ使用することができます。

始める前に

CA が設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [CA サービス（CA Service）] > [内部 CA 証明書テンプレート（Internal CA Certificate Template）]** を選択します。

ステップ 2 内部 CA テンプレートの名前を入力します。たとえば、Internal_CA_Template とします。

ステップ 3 （オプション）[組織単位（Organizational Unit）]、[組織（Organization）]、[市（City）]、[州/都道府県（State）]、[国（Country）] フィールドに値を入力します。

証明書テンプレート フィールド（[組織単位（Organizational Unit）]、[組織（Organization）]、[市（City）]、[州/都道府県（State）]、および [国（Country）]）の UTF-8 文字はサポートしていません。UTF-8 文字を証明書テンプレートで使用すると、証明書プロビジョニングが失敗します。

証明書を生成する内部ユーザーのユーザー名が、証明書の共通名として使用されます。Cisco ISE 内部 CA は、「+」または「*」の文字を [共通名（Common Name）] フィールドでサポートしていません。ユーザー名に「+」または「*」の特殊文字が含まれていないことを確認してください。

ステップ 4 サブジェクト代替名（SAN）および証明書の有効期間を指定します。

ステップ 5 キー タイプを指定します。RSA または ECC を選択します。

次の表に、ECC をサポートしているオペレーティング システムおよびバージョンと、サポートされている曲線タイプを示します。デバイスがサポートされているオペレーティング システムを実行していない場合、またはサポートされているバージョンでない場合には、代わりに RSA ベースの証明書を使用することもできます。

オペレーティングシステム	サポートされるバージョン	サポートされる曲線タイプ
Windows	8 以降	P-256、P-384、P-521
Android	4.4 以降 （注） Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ（P-192 曲線タイプをサポートしていない Android 6.0 を除く）。

Windows 7 と Apple iOS は、EAP-TLS 認証用の ECC をネイティブでサポートしていません。Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

ネットワークのデバイスがサポートされていないオペレーティング システム（Windows 7、MAC OS X、Apple iOS）を実行する場合は、キー タイプとして RSA を選択することを推奨します。

ステップ 6 （RSA キー タイプを選択する場合に適用）キー サイズを指定します。1024 以上のキー サイズを選択する必要があります。

ステップ 7 （ECC キー タイプを選択する場合にのみ適用）曲線タイプを指定します。デフォルトは P-384 です。

ステップ 8 ISE 内部 CA を SCEP RA プロファイルとして選択します。

ステップ 9 有効期間を日数単位で入力します。デフォルトは 730 日です。有効な範囲は 1 ～ 730 です。

ステップ 10 拡張キーの使用状況を指定します。証明書をクライアント認証に使用する場合は、[クライアント認証（Client Authentication）] チェック ボックスにマークを付けます。証明書をサーバー認証に使用する場合は、[サーバー認証（Server Authentication）] チェック ボックスにマークを付けます。

ステップ 11 [送信（Submit）] をクリックします。

内部 CA 証明書テンプレートが作成され、クライアント プロビジョニング ポリシーによって使用されます。

次のタスク

クライアント プロビジョニング ポリシーで使用されるネイティブ サプリカント プロファイルの作成 （638 ページ）

内部 CA の設定

次の表では、[内部 CA の設定（Internal CA Settings）] ウィンドウのフィールドについて説明します。内部 CA の設定を表示し、このウィンドウから内部 CA サービスを無効にできます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [内部 CA 設定（Internal CA Settings）]**。

表 *36* : 内部 *CA* の設定

フィールド名	使用上のガイドライン
認証局の無効化（Disable Certificate Authority）	内部 CA サービスを無効にするには、このボタンをクリックします。
ホスト名（Host Name）	CA サービスを実行している Cisco ISE ノードのホスト名。
ペルソナ（Personas）	CA サービスを実行しているノードで有効な Cisco ISE ノードのペルソナ。たとえば、管理、ポリシー サービスなどです。
ロール（Role(s)）	CA サービスを実行する Cisco ISE ノードが担当するロール。たとえば、スタンドアロンまたはプライマリまたはセカンダリです。

フィールド名	使用上のガイドライン
CA、EST、およびOCSP応答側のステータス（CA, EST & OCSP Responder Status）	有効または無効
OCSP 応答側 URL（OCSP Responder URL）	OCSP サーバーにアクセスするための Cisco ISE ノードの URL。
SCEP URL	SCEP サーバーにアクセスするための Cisco ISE ノードの URL。

関連トピック

Cisco ISE CA サービス （611 ページ）
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 （631 ページ）

クライアントプロビジョニングポリシーで使用されるネイティブサプリカントプロファイルの作成

ネイティブサプリカントプロファイルを作成して、ユーザーがパーソナルデバイスを企業ネットワークに含めることができます。Cisco ISE では、異なるオペレーティング システムごとに異なるポリシー ルールを使用します。各クライアント プロビジョニング ポリシー ルールには、どのオペレーティング システムにどのプロビジョニング ウィザードを使用するかを指定するネイティブ サプリカント プロファイルが含まれています。

始める前に

- Cisco ISE で CA 証明書テンプレートを設定します。
- TCP ポート 8905 および UDP ポート 8905 を開き、クライアントエージェントとサプリカントのプロビジョニングウィザードのインストールを有効にします。ポートの使用法の詳細については、『Cisco Identity Services Engine Hardware Installation Guide』の付録「Cisco ISE Appliance Ports Reference」を参照してください。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [ネイティブ サプリカント プロファイル（Native Supplicant Profile）]** を選択します。

ステップ 3 ネイティブ サプリカント プロファイルの名前を入力します。たとえば、EAP_TLS_INTERNAL となります。

ステップ 4 [オペレーティング システム（Operating System）] ドロップダウン リストから [すべて（ALL）] を選択します。

（注） MAC OS バージョン 10.10 のユーザーは、デュアル SSID PEAP フローに対してプロビジョニングされた SSID に手動で接続する必要があります。

ステップ 5 [有線（Wired）] または [無線（Wireless）] チェックボックスをオンにします。

ステップ 6 [許可されるプロトコル（Allowed Protocol）] ドロップダウン リストから [TLS] を選択します。

ステップ 7 以前に作成した CA 証明書テンプレートを選択します。

ステップ 8 [送信（Submit）] をクリックします。

次のタスク

Cisco からの Windows および Mac OS X オペレーティングシステムのエージェントリソースのダウンロード （639 ページ）

Cisco からの Windows および Mac OS X オペレーティングシステムのエージェントリソースのダウンロード

Windows および Mac OS X オペレーティング システムでは、Cisco サイトからリモート リソースをダウンロードする必要があります。

始める前に

ネットワークのプロキシ設定が正しく設定されていることを確認し、適切なリモート ロケーションにアクセスして、クライアント プロビジョニング リソースを Cisco ISE にダウンロードできることを確認します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [リソース（Resources）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [Cisco サイトのエージェント リソース（Agent resources from Cisco site）]** を選択します。

ステップ 3 [Windows] および [MAC OS X] パッケージの隣にあるチェックボックスをオンにします。必ず最新バージョンを含めます。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

Apple iOS、Android および MAC OS X デバイスのクライアント プロビジョニング ポリシー ルールの作成 （639 ページ）

Apple iOS、Android および MAC OS X デバイスのクライアント プロビジョニング ポリシー ルールの作成

クライアント プロビジョニング リソース ポリシーは、どのユーザーがリソース（エージェント、エージェント コンプライアンス モジュール、エージェント カスタマイズ パッケージ/プロファイル）のどのバージョン（または複数のバージョン）をログイン時およびユーザー セッション開始時に Cisco ISE から受信するかを決定します。

エージェント コンプライアンス モジュールをダウンロードすると、システムで使用している既存のモジュールがあれば常にそれが上書きされます。

従業員がiOS、Android、およびMAC OS Xデバイスを持ち込むことができるようにするには、[クライアントプロビジョニングポリシー（Client Provisioning Policy）] ページでこれらの各デバイスのポリシールールを作成する必要があります。

始める前に

必要なネイティブ サプリカント プロファイルを設定し、[クライアント プロビジョニング ポリシー（Client Provisioning Policy）] ページから必要なエージェントをダウンロードしておく必要があります。

ステップ 1 **[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 Apple iOS、Android および MAC OS X デバイスのクライアント プロビジョニング ポリシー ルールを作成します。

ステップ 3 [保存（Save）] をクリックします。

次のタスク

TLS ベース認証の Dot1X 認証ポリシー ルールの設定 （640 ページ）

TLS ベース認証の Dot1X 認証ポリシー ルールの設定

このタスクは、TLS ベース認証の Dot1X 認証ポリシー ルールを更新する方法を示します。

始める前に

TLS ベース認証用に作成された証明書認証プロファイルが存在することを確認します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー セット（Policy Sets）]** を選択します。

ステップ 2 [表示（View）] 列から矢印アイコン › をクリックすると、[設定（Set）] ビュー画面が開き、認証ポリシーを表示、管理、および更新できます。

デフォルトのルールベースの認証ポリシーには、Dot1X 認証用のルールが含まれます。

ステップ 3 Dot1X 認証ポリシー ルールの条件を編集するには、[条件（Conditions）] 列のセルにカーソルを合わせ、  をクリックします。[条件スタジオ（Conditions Studio）] が開きます。

ステップ 4 Dot1X ポリシー ルールの [アクション（Actions）] 列で、歯車アイコンをクリックし、必要に応じてドロップダウンメニューから、挿入または複製オプションのいずれかを選択して新しいポリシー セットを挿入します。
[ポリシー セット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 5 ルールの名前を入力します。たとえば、eap-tls と入力します。

ステップ 6 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 7 [条件スタジオ（Conditions Studio）]ページで必要な条件を作成します。[エディタ（Editor）]セクションで、[クリックして属性を追加する（Click To Add an Attribute）]テキスト ボックスをクリックし、必要なディクショナリと属性（たとえば、Network Access:UserName Equals User1）を選択します。

ライブラリ条件を[クリックして属性を追加する（Click To Add An Attribute）]テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 8 [使用（Use）] をクリックします。

ステップ 9 デフォルト ルールは、そのままにします。

ステップ 10 [保存（Save）] をクリックします。

次のタスク

中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成 （641 ページ）

中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成

許可プロファイルを定義して、証明書ベースの認証の成功後にユーザーに付与するアクセスを決定します。

始める前に

ワイヤレス LAN コントローラ（WLC）に必要なアクセス コントロール リスト（ACL）が設定されていることを確認します。WLC での ACL の作成方法については、『TrustSec How-To Guide: Using Certificates for Differentiated Access』を参照してください。

この例では、WLC で次の ACL が作成されていると仮定します。

- NSP-ACL：ネイティブ サプリカント プロビジョニング用
- BLACKHOLE：ブロックリストに登録されているデバイスへのアクセスの制限
- NSP-ACL-Google：Android デバイスのプロビジョニング

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 新しい許可プロファイルを作成するには、[追加（Add）] をクリックします。

ステップ 3 許可プロファイルの名前を入力します。

ステップ 4 [アクセス タイプ（Access Type）] ドロップダウン リストから、[ACCESS_ACCEPT] を選択します。

ステップ 5 中央 Web 認証、Google Play の中央 Web 認証、ネイティブ サプリカント プロビジョニング、および Google のネイティブ サプリカント プロビジョニングの許可プロファイルを追加するには、[追加（Add）]をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

許可ポリシー ルールの作成 （642 ページ）

許可ポリシー ルールの作成

Cisco ISE は、許可ポリシー ルールを評価し、ポリシー ルールで指定された許可プロファイルに基づいてネットワーク リソースへのアクセス権をユーザーに付与します。

始める前に

必要な許可プロファイルを作成済みであることを確認します。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択し、許可ポリシー ルールを表示するポリシー セットを展開します。

ステップ 2 デフォルトのルールの上に追加のポリシー ルールを挿入します。

ステップ 3 [保存（Save）] をクリックします。

CA サービス ポリシーのリファレンス

ここでは、Cisco ISE CA サービスを有効にする前に作成する必要がある許可ポリシー ルールおよびクライアント プロビジョニング ポリシー ルールの詳細情報について説明します。

証明書サービスのクライアント プロビジョニング ポリシー ルール

ここでは、Cisco ISE 証明書サービスを使用している場合に作成する必要があるクライアント プロビジョニング ポリシー ルールについて説明します。次の表に詳細を示します。

ルール名	ID グループ	オペレーティング システム	その他の条件	結果
iOS	任意（Any）	Apple iOS すべて	条件	EAP_TLS_INTERNAL（以前に作成したネイティブ サプリカント プロファイル）。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカント プロファイルを選択します。

ルール名	ID グループ	オペレーティング システム	その他の条件	結果
Android	任意（Any）	Android	条件	EAP_TLS_INTERNAL（以前に作成したネイティブ サプリカント プロファイル）。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカント プロファイルを選択します。

ルール名	ID グループ	オペレーティングシステム	その他の条件	結果
MAC OS X	任意（Any）	MACOSX	条件	ネイティブ サプリカントの設定で、次を指定してください。 **1.** [設定ウィザード（Config Wizard）]：シスコのサイトからダウンロードした MAC OS X サプリカントのウィザードを選択します。 **2.** [ウィザードプロファイル（Wizard Profile）]：以前作成した EAP_TLS_INTERNAL ネイティブ サプリカントのプロファイルを選択します。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカント プロファイルを選択します。

証明書サービスの許可プロファイル

ここでは、Cisco ISE で証明書ベースの認証を有効にするために作成する必要がある許可プロファイルについて説明します。ワイヤレス LAN コントローラ（WLC）の ACL（NSP-ACL および NSP-ACL-Google）がすでに作成されている必要があります。

- CWA：このプロファイルは、中央 Web 認証フローを使用するデバイス用です。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [中央集中（Centralized）] を選択し、ACL テキスト ボックスに NSP-ACL を入力します。
- CWA_GooglePlay：このプロファイルは、中央 Web 認証フローを使用する Android デバイス用です。このプロファイルによって、Android デバイスは Google Play ストアにアクセスし、Cisco Network Setup Assistant をダウンロードできます。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [中央集中（Centralized）] を選択し、ACL テキスト ボックスに NSP-ACL-Google を入力します。
- NSP：このプロファイルは、サプリカント プロビジョニング フローを使用する非 Android デバイス用です。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [サプリカント プロビジョニング（Supplicant Provisioning）] を選択し、ACL テキスト ボックスに NSP-ACL を入力します。
- NSP-Google：このプロファイルは、サプリカント プロビジョニング フローを使用する Android デバイス用です。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [サプリカント プロビジョニング（Supplicant Provisioning）] を選択し、ACL テキスト ボックスに NSP-ACL-Google を入力します。

デフォルトの Block_Wireless_Access 認証プロファイル（ワイヤレスブロックリストのデフォルト認証ポリシーで使用）を確認します。高度な属性設定を次のように設定する必要があります。

- Cisco:cisco-av-pair = url-redirect=https://*ip:port*/blockedportal/gateway?portal=*PortalID*
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

証明書サービスの許可ポリシー ルール

ここでは、Cisco ISE CA サービスを有効にするときに作成する必要がある許可ポリシー ルールについて説明します。

- 企業資産：このルールは、802.1X および MSCHAPV2 プロトコルを使用して企業のワイヤレス SSID に接続する企業のデバイス用です。
- Android_SingleSSID：このルールは、Google Play ストアにアクセスして、プロビジョニングのために Cisco Network Setup Assistant をダウンロードする Android デバイス用です。このルールは、シングル SSID 設定に固有です。
- Android_DualSSID：このルールは、Google Play ストアにアクセスして、プロビジョニングのために Cisco Network Setup Assistant をダウンロードする Android デバイス用です。このルールは、デュアル SSID 設定に固有です。
- CWA：このルールは、中央 Web 認証フローを使用するデバイス用です。
- NSP：このルールは、EAP-TLS 認証の証明書を使用するネイティブ サプリカント プロビジョニング フローを使用するデバイス用です。
- EAP-TLS：このルールは、サプリカント プロビジョニング フローを完了したデバイスおよび証明書でプロビジョニングされるデバイス用です。デバイスには、ネットワークへのアクセス権限が付与されます。

次の表に、Cisco ISE CA サービスの許可ポリシー ルールを設定するときに選択する必要がある属性および値を示します。この例では、Cisco ISE で対応する許可プロファイルも設定しているものと想定します。

ルール名	条件	権限（適用される許可プロファイル）
Corporate Assets	Corp_Assets AND（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2）	PermitAccess
Android_SingleSSID	（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android）	NSP_Google
Android_DualSSID	（Wireless_MAB AND Session:Device-OS EQUALS Android）	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2）	NSP
EAP-TLS	（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI	PermitAccess

Cisco ISE CA による ASA VPN ユーザーへの証明書の発行

ISE CA は、ASA VPN 経由で接続しているクライアント マシンに証明書を発行します。この機能を使用して、ASA VPN 経由で接続しているエンド デバイスに証明書を自動的にプロビジョニングできます。

Cisco ISE は、Simple Certificate Enrollment Protocol（SCEP）を使用して登録を行い、証明書をクライアント マシンにプロビジョニングします。エージェントは、HTTPS 接続で ASA に SCEP 要求を送信します。ASA は、Cisco ISE と ASA の間に確立された HTTP 接続を介して Cisco ISE に要求を中継する前に、要求を評価し、ポリシーを適用します。Cisco ISE CA からの応答はクライアントに中継されます。ASA は、SCEP メッセージの内容を読み取ることはできず、Cisco ISE CA のプロキシとして機能します。Cisco ISE CA は、クライアントからの SCEP メッセージを復号化し、暗号化された形式で応答を送信します。

ISE CA SCEP URL は http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe です。ISE ノードの FQDN を使用する場合は、ASA に接続されている DNS サーバーが FQDN を解決できる必要があります。

エージェントのプロファイルの期限が切れる前に、証明書の更新を設定できます。証明書がすでに期限切れの場合、更新フローは新規登録と同様です。

サポートされているバージョンは次のとおりです。

- ソフトウェア バージョン 8.x を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco AnyConnect VPN バージョン 2.4 以降

VPN 接続の証明書プロビジョニングフロー

1. ユーザーが VPN 接続を開始します。
2. エージェントは、クライアントマシンをスキャンし、固有デバイス識別子（たとえば IMEI）などの属性を ASA に送信します。
3. ASA はクライアントからの証明書ベースの認証を要求します。証明書がないため、認証は失敗します。
4. ASA は、ユーザー名/パスワードを使用してプライマリ ユーザー認証（AAA）に進み、情報を認証サーバー（ISE）に渡します。
    1. 認証が失敗すると、接続はただちに終了します。
    2. 認証が成功すると、制限付きアクセスが許可されます。aaa.cisco.sceprequired 属性を使用して証明書を要求するクライアント マシンでダイナミック アクセス ポリシー（DAP）を設定できます。この属性の値を「true」に設定し、ACL および Web ACL を適用できます。
5. VPN 接続は、関連するポリシーと ACL が適用された後に確立されます。クライアントは、AAA 認証が成功し、VPN 接続が確立された後にのみ、SCEP のキー生成を開始します。
6. クライアントは、SCEP 登録を開始し、HTTP を介して ASA に SCEP 要求を送信します。
7. ASA は、要求のセッション情報を検索し、セッションが登録を許可されている場合は、ISE CA に要求をリレーします。
8. ASA は ISE CA からの応答をクライアントにリレー バックします。
9. 登録が成功すると、クライアントにユーザーに対する設定可能メッセージが表示され、VPN セッションが接続解除されます。
10. ユーザーは証明書を使用して再度認証を行うことができ、正常な VPN 接続が確立されます。

ASA VPN ユーザーに証明書を発行する Cisco ISE CA の設定

ASA VPN ユーザーに証明書をプロビジョニングするには、Cisco ISE および ASA で次の設定を行う必要があります。

始める前に

- VPN ユーザー アカウントが Cisco ISE の内部または外部の ID ソースに存在することを確認します。
- ASA および Cisco ISE のポリシー サービス ノードが同じ NTP サーバーを使用して同期されていることを確認します。

ステップ 1 Cisco ISE で ASA をネットワーク アクセス デバイスとして定義します。ネットワーク デバイスとして ASA を追加する方法については、Cisco ISE でのネットワークデバイスの追加 （648 ページ） を参照してください。

ステップ 2 ASA でのグループ ポリシーの設定 （649 ページ）。

ステップ 3 SCEP 登録用の エージェント接続プロファイルの設定 （649 ページ）。

ステップ 4 ASDM での VPN クライアント プロファイルの設定 （650 ページ）。

ステップ 5 ASA への Cisco ISE CA 証明書のインポート。

Cisco ISE でのネットワークデバイスの追加

Cisco ISE でネットワークデバイスを追加したり、デフォルトのネットワークデバイスを使用したりできます。

[ネットワークデバイス（Network Devices）]（**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]**）ウィンドウでもネットワークデバイスを追加できます。

始める前に

追加するネットワークデバイスで AAA 機能を有効にする必要があります。AAA 機能を有効にするコマンド （1944 ページ）を参照してください。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Device）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）]、[説明（Description）]、および [IP アドレス（IP Address）] の各フィールドに対応する値を入力します。

ステップ 4 [デバイスプロファイル（Device Profile）]、[モデル名（Model Name）]、[ソフトウェアバージョン（Software Version）]、および [ネットワーク デバイス グループ（Network Device Group）] ドロップダウンリストから必要な値を選択します。

ステップ 5 （任意）[RADIUS 認証設定（RADIUS Authentication Settings）] チェックボックスをオンにして、RADIUS プロトコル認証を設定します。

ステップ 6 （任意）[TACACS 認証設定（TACACS Authentication Settings）] チェックボックスをオンにして、TACACS プロトコル認証を設定します。

ステップ 7 （オプション）[SNMP の設定（SNMP Settings）] チェックボックスをオンにして、ネットワークデバイスから情報を収集するように Cisco ISE プロファイリングサービスに SNMP を設定します。

ステップ 8 （オプション）TrustSec 対応デバイスを設定するには [高度なTrustSec 設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 9 [送信（Submit）] をクリックします。

ASA でのグループ ポリシーの設定

ASA でグループポリシーを設定し、SCEP 登録要求を転送するための エージェント用の ISE CA URL を定義します。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN（Remote Access VPN）] ナビゲーション ペインから、[グループポリシー（Group Policies）] をクリックします。

ステップ 3 [追加（Add）] をクリックして、グループ ポリシーを作成します。

ステップ 4 グループ ポリシーの名前を入力します。たとえば、ISE_CA_SCEP のようになります。

ステップ 5 [SCEP転送URL（SCEP forwarding URL）] フィールドで、[継承（Inherit）] チェックボックスをオフにして、ポート番号を含む ISE SCEP URL を入力します。

ISE ノードの FQDN を使用する場合は、ASA に接続されている DNS サーバーが ISE ノードの FQDN を解決できる必要があります。

例：

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.

ステップ 6 [OK] をクリックして、グループ ポリシーを保存します。

SCEP 登録用の エージェント接続プロファイルの設定

ISE CA サーバー、認証方式、および ISE CA SCEP URL を指定するには、ASA で エージェント接続プロファイルを設定します。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN（Remote Access VPN）] ナビゲーションウィンドウで、**[エージェント接続プロファイル（Agent Connection Profiles）]** をクリックします。

ステップ 3 [追加（Add）] をクリックして、接続プロファイルを作成します。

ステップ 4 接続プロファイルの名前を入力します。たとえば、Cert-Group と入力します。

ステップ 5 （オプション）[エイリアス（Aliases）]フィールドに接続プロファイルの説明を入力します。たとえば、SCEP-Call-ASA とします。

ステップ 6 [認証（Authentication）] 領域で、次の情報を指定します。

- [方式（Method）] : [両方（Both）] オプション ボタンをクリックします

- [AAAサーバーグループ（AAA Server Group）] : [管理（Manage）] をクリックして ISE サーバーを選択します

ステップ 7 [クライアントアドレスの割り当て（Client Address Assignment）] 領域で、使用する DHCP サーバーおよびクライアント アドレス プールを選択します。

ステップ 8 [デフォルトグループポリシー（Default Group Policy）] 領域で、[管理（Manage）] をクリックし、ISE SCEP URL とポート番号で作成したグループ ポリシーを選択します。

例：

たとえば、ISE_CA_SCEP のようになります。

ステップ 9 **[詳細設定（Advanced）]**>**[一般（General）]** を選択し、この接続プロファイルに対して [Simple Certificate Enrollment Protocolを有効にする（Enable Simple Certificate Enrollment Protocol）] チェックボックスをオンにします。

ステップ 10 [OK] をクリックします。
エージェント接続プロファイルが作成されます。

ASDM での VPN クライアント プロファイルの設定

SCEP 登録用のエージェントでの VPN クライアント プロファイルの設定

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN（Remote Access VPN）] ナビゲーション ペインから、[AnyConnectクライアントプロファイル（AnyConnect Client Profile）] をクリックします。

ステップ 3 使用するクライアント プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 4 左側の [プロファイル（Profile）] ナビゲーション ペインで、[証明書の登録（Certificate Enrollment）] をクリックします。

ステップ 5 [証明書の登録（Certificate Enrollment）] チェックボックスをオンにします。

ステップ 6 次のフィールドに値を入力します。

- [証明書失効しきい値（Certificate Expiration Threshold）] : エージェントがユーザーに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するか（SCEPが有効な場合はサポートされません）。デフォルトは 0（警告は表示しない）です。値の範囲は 0 ～ 180 日です。
- [自動SCEPホスト（Automatic SCEP Host）] : SCEP 証明書取得が設定されている ASA のホスト名および接続プロファイル（トンネル グループ）を入力します。ASA の完全修飾ドメイン名（FQDN）または接続プロファイル名を入力してください。たとえば、ホスト名 asa.cisco.com、接続プロファイル名 Cert_Group などです。
- [CA URL] : SCEP CA サーバーを識別します。ISE サーバーの FQDN または IP アドレスを入力します。たとえば、http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe などです。

ステップ 7 証明書の内容をクライアントが要求する方法を定義する値を [証明書の内容（Certificate Contents）] に入力します。

ステップ 8 [OK] をクリックします。

エージェントクライアントプロファイルが作成されました。詳細については、お使いのエージェントバージョンの『Cisco AnyConnect Secure Mobility Client』を参照してください。

ASA への Cisco ISE CA 証明書のインポート

Cisco ISE 内部 CA 証明書を ASA にインポートします。

始める前に

Cisco ISE 内部 CA 証明書をエクスポートします。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[認証局証明書（Certificate Authority Certificates）]** に移動します。[証明書サービスノードCA（Certificate Services Node CA）] および [証明書サービスルートCA（Certificate Services Root CA）] 証明書の横にあるチェックボックスをオンにして、これらの証明書を一度に 1 つずつエクスポートします。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセス VPN（Remote Access VPN）] ナビゲーションペインから、**[証明書管理（Certificate Management）]** > **[CA 証明書（CA Certificates）]** を選択します。

ステップ 3 [追加（Add）] をクリックして Cisco ISE 内部 CA 証明書を選択し、ASA にインポートします。

エンドポイント証明書の失効

従業員のパーソナル デバイスに対して発行された証明書を取り消す必要がある場合は、[エンドポイント証明書（Endpoint Certificates）] ページから取り消すことができます。たとえば、従業員のデバイスが盗難されたり、紛失したりした場合には、Cisco ISE 管理者ポータルにログインし、そのデバイスに発行された証明書を [エンドポイント証明書（Endpoint Certificates）] ページから取り消すことができます。フレンドリ名、デバイスの一意の ID、シリアル番号に基づいて、このページのデータをフィルタリングできます。

PSN（サブ CA）が侵害された場合は、[エンドポイント証明書（Endpoint Certificates）] ページの [発行元（Issued By）] フィールドでフィルタリングすることによって、その PSN によって発行されたすべての証明書を取り消すことができます。

従業員に対して発行された証明書を取り消すときに、アクティブなセッション（その証明書を使用して認証された）がある場合、セッションは即座に終了します。証明書を取り消すと、その直後に、許可されていないユーザーはリソースにアクセスできなくなります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[発行された証明書（Issued Certificates）]** を選択します。

ステップ 2 取り消すエンドポイント証明書の隣にあるチェックボックスをオンにし、[失効（Revoke）] をクリックします。

フレンドリ名とデバイス タイプに基づいて証明書を検索できます。

ステップ 3 証明書を取り消す理由を入力します。

ステップ 4 [はい（Yes）] をクリックします。

OCSP サービス

Online Certificate Status Protocol（OCSP）は、x.509 デジタル証明書のステータスのチェックに使用されるプロトコルです。このプロトコルは証明書失効リスト（CRL）に代わるものであり、CRL の処理が必要となる問題に対処します。

Cisco ISE には HTTP を介して OCSP サーバーと通信し、認証で証明書のステータスを検証する機能があります。OCSP のコンフィギュレーションは、Cisco ISE で設定されるいずれかの認証局（CA）証明書から参照できる再利用可能な設定オブジェクトで設定されます。

CRL 検証と OCSP 検証の両方または一方を CA ごとに設定できます。両方を選択すると、Cisco ISE では最初に OCSP を介した検証が実行されます。プライマリ OCSP サーバーとセカンダリ OCSP サーバーの両方で通信の問題が検出された場合、または特定の証明書に対して不明のステータスが返された場合、Cisco ISE は CRL チェックの実行に切り替えます。

Cisco ISE CA サービスの Online Certificate Status Protocol 応答側

Cisco ISE CA OCSP 応答側は、OCSP クライアントと通信するサーバーです。Cisco ISE CA の OCSP クライアントには、Cisco ISE の内部 OCSP クライアントと適応型セキュリティ アプライアンス（ASA）の OCSP クライアントがあります。OCSP クライアントは、RFC 2560、5019 で定義されている OCSP 要求/応答構造を使用して、OCSP 応答側と通信する必要があります。

Cisco ISE CA は、OCSP 応答側に証明書を発行します。OCSP 応答側は、着信要求をポート 2560 でリッスンします。このポートは、OCSP トラフィックのみを許可するように設定されています。

OCSP 応答側は RFC 2560、5019 で規定された構造に従って要求を受け入れます。OCSP 要求ではナンス拡張がサポートされます。OCSP 応答側は証明書のステータスを取得し、OCSP 応答を作成して署名します。OCSP 応答は、OCSP 応答側ではキャッシュされませんが、クライアントでは最大 24 時間 OCSP 応答をキャッシュすることができます。OCSP クライアントでは、OCSP 応答の署名を検証する必要があります。

PAN 上の自己署名 CA 証明書（ISE が外部 CA の中間 CA として機能する場合は、中間 CA 証明書）によって、OCSP 応答側証明書が発行されます。PAN 上のこの CA 証明書によって、PAN および PSN の OCSP 証明書が発行されます。この自己署名 CA 証明書は、展開全体に対するルート証明書でもあります。展開全体のすべての OCSP 証明書が、これらの証明書を使用して署名された応答を ISE で検証するために、信頼できる証明書ストアに格納されます。

（注） Cisco ISE は OCSP 応答側サーバーから thisUpdate 値を受信します。この値は、最後の証明書失効からの時間を示します。thisUpdate 値が 7 日より大きい場合、Cisco ISE で OCSP 証明書の検証が失敗します。

OCSP 証明書のステータスの値

OCSP サービスでは、所定の証明書要求に対して次の値が返されます。

- [良好（Good）]：ステータスの問い合わせへの肯定的な応答を示します。証明書が失効していないこと、および状態が次の時間間隔（存続可能時間）値までは良好であることを示します。
- [失効（Revoked）]：証明書は失効しています。
- [不明（Unknown）]：証明書のステータスは不明です。この OCSP 応答側の CA で証明書が発行されなかった場合、OCSP サービスはこの値を返します。
- [エラー（ERROR）]：OCSP 要求に対する応答を受信しませんでした。

OCSPレスポンダ証明書の更新

Cisco ISE リリース 3.1 累積パッチ 3 以降では、Cisco ISE の内部 CA の階層が変更されています。これには、Cisco ISE の OCSP レスポンダ証明書の 1 回限りの更新が必要です。

Cisco ISE リリース 3.1 累積パッチ 3 以降では、OCSP レスポンダ証明書の更新に次のルールが適用されます。

- Cisco ISE リリース 3.1 累積パッチ 2 以前のパッチから Cisco ISE リリース 3.1 累積パッチ 3 以降のパッチに更新する場合
  - マルチノード Cisco ISE 展開の場合、Cisco ISE GUI を介してパッチをインストールすると、OCSP 証明書が自動的に更新されます。Cisco ISE CLI を介してパッチをインストールする場合は、OCSP 証明書を手動で更新することをお勧めします。
  - スタンドアロン Cisco ISE 展開の場合、Cisco ISE GUI、または Cisco ISE CLI のどちらを介してパッチをインストールしたかに関わらず、OCSP 証明書が自動的に更新されます。
  - パッチ 3 以降のパッチをアンインストールする場合は、OCSP 証明書を手動で更新する必要があります。
- 以前の Cisco ISE リリースから Cisco ISE 3.2 以降のリリースにフルアップグレードすると、OCSP レスポンダ証明書が更新されます。
- 分割アップグレード（レガシーアップグレードと新しいアップグレードの両方）では、Cisco ISE の内部ルート CA が再生成されます。

- バックアップを復元すると、Cisco ISE の内部ルート CA が再生成されます。

（注） Cisco ISE リリース 3.1 累積パッチ 3 以降のパッチで Cisco ISE の内部ルート CA を再生成すると、新しい内部 CA 階層を使用して OCSP レスポンダ証明書が作成されます。

OCSP ハイ アベイラビリティ

Cisco ISE では CA ごとに最大 2 つの OCSP サーバーを設定でき、それらのサーバーはプライマリおよびセカンダリ OCSP サーバーと呼ばれます。各 OCSP サーバー設定には、次のパラメータが含まれます。

- [URL]：OCSP サーバーの URL。
- [ナンス（Nonce）]：要求で送信される乱数。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。
- [応答の検証（Validate Response）]：Cisco ISE は OCSP サーバーから受信した応答の署名を検証します。

Cisco ISE がプライマリ OCSP サーバーと通信しているときに、タイムアウト（5 秒）が発生した場合、Cisco ISE はセカンダリ OCSP サーバーに切り替えます。

Cisco ISE はプライマリ サーバーの再使用を試行する前に、設定可能な期間セカンダリ OCSP サーバーを使用します。

OCSP の障害

3 つの一般的な OCSP 障害のシナリオは次のとおりです。

- OCSP キャッシュまたは OCSP クライアント側（Cisco ISE）の失敗による障害。
- 失敗した OCSP 応答側のシナリオ。例：

  最初のプライマリ OCSP 応答側が応答せず、セカンダリ OCSP 応答側が Cisco ISE OCSP 要求に応答します。

  Cisco ISE OCSP 要求からエラーまたは応答が受信されません。

  OCSP 応答側が、Cisco ISE OCSP 要求への応答を提供しないか、失敗の OCSP 応答のステータスを返している可能性があります。OCSP 応答のステータス値は次のようになります。

  - tryLater
  - signRequired
  - unauthorized
  - internalError
  - malformedRequest

OCSP 要求には、多数の日時チェック、署名の有効性チェックなどがあります。詳細については、エラー状態を含むすべての可能性のある状態について説明している『RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP』を参照してください。

- 失敗した OCSP レポート

OCSP クライアント プロファイルの追加

[OCSP クライアント プロファイル（OCSP Client Profile）] ページを使用して、Cisco ISE に新しい OCSP クライアント プロファイルを追加できます。

始める前に

認証局（CA）が非標準ポート（80 または 443 以外）で OCSP サービスを実行している場合は、そのポートで Cisco ISE と CA 間の通信を可能にするためにスイッチで ACL を設定する必要があります。次に例を示します。

permit tcp <*source ip*> <接続先 *ip*> **eq** <*OCSP* ポート番号>

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [OCSP クライアントプロファイル（OCSP Client Profile）]** を選択します 。

ステップ 2 OCSP クライアント プロファイルを追加するための値を入力します。

ステップ 3 [送信（Submit）] をクリックします。

OCSP クライアント プロファイル設定

次の表では、OCSP クライアントプロファイル設定を行うために使用できる [OCSP クライアント プロファイル（OCSP Client Profile）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [OCSP クライアント プロファイル（OCSP Client Profile）]** です。

表 *37 : OCSP* クライアント プロファイル設定

フィールド名	使用上のガイドライン
名前（**Name**）	OCSP クライアント プロファイル名。
説明（**Description**）	任意で説明を入力します。
OCSP応答側の設定（Configure OCSP Responder）	

フィールド名	使用上のガイドライン
セカンダリ サーバーの有効化（**Enable Secondary Server**）	ハイアベイラビリティのセカンダリOCSPサーバーを有効にするには、このチェックボックスをオンにします。
常にプライマリ サーバーに最初にアクセスする（**Always Access Primary Server First**）	このオプションは、セカンダリ サーバーへの移動を試行する前にプライマリ サーバーをチェックする場合に使用します。プライマリが以前にチェックされ、応答しないことがわかっている場合にも、Cisco ISE はセカンダリ サーバーに移動する前にプライマリ サーバーへの要求の送信を試行します。
n 分経過後にプライマリ サーバーにフォールバック（**Fallback to Primary Server After Interval *n* Minutes**）	このオプションは、Cisco ISE がセカンダリ サーバーに移動してから、再度プライマリ サーバーにフォールバックする場合に使用します。この場合、その他の要求はすべてスキップされ、テキスト ボックスで設定した時間セカンダリ サーバーが使用されます。許可される時間の範囲は 1 ～ 999 分です。
プライマリ サーバーとセカンダリ サーバー（**Primary and Secondary Servers**）	
URL	プライマリおよびセカンダリ OCSP サーバーの URL を入力します。
ナンス拡張サポートの有効化（**Enable Nonce Extension Support**）	ナンスが OCSP 要求の一部として送信されるように設定できます。ナンスには、OCSP要求の疑似乱数が含まれます。応答で受信される数値は要求に含まれる数値と同じであることが検証されています。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。

フィールド名	使用上のガイドライン
応答の署名の検証（**Validate Response Signature**）	OCSP応答側は、次のいずれかの証明書を使用して応答に署名します。 • CA 証明書 • CA 証明書とは別の証明書 Cisco ISE が応答の署名を検証するためには、OCSP応答側が応答を証明書とともに送信する必要があります。そうでない場合、応答の検証は失敗し、証明書のステータスは利用できません。RFC に従い、OCSPは異なる証明書を使用して応答に署名できます。このことは、OCSP が Cisco ISEによる検証用に応答に署名した証明書を送信する限り当てはまります。OCSPがCisco ISE で設定されているものとは異なる証明書を使用して応答に署名した場合、応答の検証は失敗します。
Authority Information Access（AIA）に指定されたOCSP URLを使用する（Use OCSP URLs specified in Authority Information Access (AIA)）	Authority Information Access の拡張で指定されている OCSP URL を使用するには、オプション ボタンをクリックします。
応答キャッシュ（**Response Cache**）	

フィールド名	使用上のガイドライン
キャッシュ エントリの存続可能時間 n 分（**Cache Entry Time To Live *n* Minutes**）	キャッシュ エントリが期限切れになる時間を分単位で入力します。OCSP サーバーからの各応答には nextUpdate 値が含まれています。この値は、証明書のステータスがサーバーで次にいつ更新されるかを示します。OCSP 応答がキャッシュされるとき、2 つの値（1 つは設定から、もう 1 つは応答から）が比較され、この 2 つの最小値の時間だけ応答がキャッシュされます。nextUpdate 値が 0 の場合、応答はまったくキャッシュされません。Cisco ISE は設定された時間 OCSP 応答をキャッシュします。キャッシュは複製されず、永続的でもないため、Cisco ISE が再起動するとキャッシュはクリアされます。次の理由により、OCSP キャッシュは OCSP 応答を保持するために使用されます。 • 既知の証明書に関する OCSP サーバーからのネットワーク トラフィックと負荷を低減するため • 既知の証明書のステータスをキャッシュすることによって Cisco ISE のパフォーマンスを向上させるため デフォルトでは、キャッシュは内部 CA OCSP クライアント プロファイルに対し 2 分に設定されています。エンドポイントが最初の認証から 2 分以内にもう一度認証すると、OCSP のキャッシュが使用され、OCSP 応答側には問い合わせされません。エンドポイントの証明書がキャッシュ期間内に失効した場合、以前の OCSP のステータス [良好（Good）] が使用され、認証は成功します。キャッシュを 0 分に設定すると、応答はキャッシュされません。このオプションでは、セキュリティは向上しますが、認証のパフォーマンスは低下します。

フィールド名	使用上のガイドライン
キャッシュのクリア（**Clear Cache**）	OCSP サービスに接続されているすべての認証局のエントリをクリアするには、[キャッシュのクリア（Clear Cache）] をクリックします。 展開内で、[キャッシュのクリア（Clear Cache）] はすべてのノードと相互作用して、処理を実行します。このメカニズムでは、展開内のすべてのノードが更新されます。

関連トピック

OCSP サービス （652 ページ）
Cisco ISE CA サービスの Online Certificate Status Protocol 応答側 （652 ページ）
OCSP 証明書のステータスの値 （653 ページ）
OCSP ハイ アベイラビリティ （654 ページ）
OCSP の障害 （654 ページ）
OCSP 統計情報カウンタ （659 ページ）
OCSP クライアント プロファイルの追加 （655 ページ）

OCSP 統計情報カウンタ

Cisco ISE では、OCSP カウンタを使用して、OCSP サーバーのデータと健全性をロギングおよびモニタリングします。ロギングは 5 分ごとに実行されます。Cisco ISE はモニタリング ノードに syslog メッセージを送信し、それはローカル ストアに保持されます。ローカル ストアには過去 5 分のデータが含まれています。Cisco ISE が syslog メッセージを送信した後、カウンタは次の間隔について再計算されます。つまり、5 分後に、新しい 5 分間の間隔が再度開始されます。

次の表に、OCSP syslog メッセージとその説明を示します。

表 38 : OCSP Syslog メッセージ

メッセージ	説明
OCSPPrimaryNotResponsiveCount	応答のないプライマリ要求の数
OCSPSecondaryNotResponsiveCount	応答のないセカンダリ要求の数
OCSPPrimaryCertsGoodCount	プライマリ OCSP サーバーを使用して返された所定の CA の「良好な」証明書の数
OCSPSecondaryCertsGoodCount	プライマリ OCSP サーバーを使用して返された所定の CA の「良好な」ステータスの数
OCSPPrimaryCertsRevokedCount	プライマリ OCSP サーバーを使用して返された所定の CA の「失効した」ステータスの数

メッセージ	説明
OCSPSecondaryCertsRevokedCount	セカンダリ OCSP サーバーを使用して返された所定の CA の「失効した」ステータスの数
OCSPPrimaryCertsUnknownCount	プライマリ OCSP サーバーを使用して返された所定の CA の「不明の」ステータスの数
OCSPSecondaryCertsUnknownCount	セカンダリ OCSP サーバーを使用して返された所定の CA の「不明の」ステータスの数
OCSPPrimaryCertsFoundCount	プライマリの送信元からのキャッシュ内に見つかった証明書の数
OCSPSecondaryCertsFoundCount	セカンダリの送信元からのキャッシュ内に見つかった証明書の数
ClearCacheInvokedCount	一定間隔の後にキャッシュのクリアがトリガーされた回数
OCSPCertsCleanedUpCount	t 間隔の後にクリーンアップされたキャッシュ エントリの数
NumOfCertsFoundInCache	キャッシュから実行された要求の数
OCSPCacheCertsCount	OCSP キャッシュ内に見つかった証明書の数

管理者のアクセス ポリシーの設定

RBAC ポリシーは if-then 形式で表され、ここで if は RBAC 管理者グループの値、および「then」は RBAC 権限の値になります。

[RBACポリシー（RBAC policies）] ウィンドウ（**[メニュー（Menu）** アイコン（☰）をクリックして、**[管理（Administration）]**>**[システム（System）]**>**[管理者アクセス（Admin Access）]**>**[許可（Authorization）]** > **[RBACポリシー（RBAC Policy）]** を選択）には、デフォルトポリシーのリストが含まれています。これらのデフォルトポリシーは編集または削除できません。ただし、読み取り専用管理ポリシーのデータ アクセス許可は編集できます。[RBAC ポリシー（RBAC policies）] ページでは、特に職場の管理者グループ用にカスタム RBAC ポリシーを作成し、パーソナライズされた管理者グループに適用できます。

制限付きメニュー アクセスを割り当てるときには、データ アクセス権限により、指定されているメニューを使用するために必要なデータに管理者がアクセスできることを確認してください。たとえばデバイス ポータルへのメニュー アクセスを付与するが、エンドポイント ID グループへのデータ アクセスを許可しないと、管理者はポータルを変更できません。

（注） 管理者ユーザーは、エンドポイントの MAC アドレスを、読み取り専用アクセス権を持つエンドポイント ID グループから、フルアクセス権を持つエンドポイント ID グループに移動できます。その逆はできません。

始める前に

- ロールベースアクセス コントロール（RBAC）ポリシーを定義するすべての管理者グループを作成します。
- これらの管理者グループが、個々の管理者ユーザーにマッピングされていることを確認します。
- メニューアクセス権限やデータアクセス権限など、RBAC 権限を設定していることを確認します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [RBACポリシー（RBAC Policy）]** を選択します。

[RBAC ポリシー（RBAC Policies）] ページには、デフォルトの管理者グループ用にすぐに使用できる定義済みの一連のポリシーが含まれています。これらのデフォルト ポリシーは編集または削除できません。ただし、デフォルトの読み取り専用管理ポリシーのデータ アクセス許可は編集できます。

ステップ 2 デフォルト RBAC ポリシー ルールのいずれかの隣にある [操作（Action）] をクリックします。

ここでは、新しい RBAC ポリシーを挿入し、既存の RBAC ポリシーを複製し、既存の RBAC ポリシーを削除できます。

ステップ 3 [新しいポリシーの挿入（Insert New Policy）] をクリックします。

ステップ 4 [ルール名（Rule Name）]、[RBAC グループ（RBAC Group(s)）]、および [権限（Permissions）] フィールドに値を入力します。

RBAC ポリシーの作成時に、複数のメニューアクセス権限とデータ アクセス権限を選択することはできません。

ステップ 5 [保存（Save）] をクリックします。

管理者アクセスの設定

Cisco ISE では、セキュリティ強化のために管理者アカウントにルールを定義できます。管理インターフェイスへのアクセスを制限したり、強力なパスワードの使用やパスワードの定期的な変更を管理者に強制することができます。Cisco ISE の [管理者アカウントの設定（Administrator Account Settings）] で定義するパスワードポリシーは、すべての管理者アカウントに適用されます。

Cisco ISE では、管理者パスワードでの UTF-8 文字の使用はサポートされていません。

同時管理セッションとログインバナーの最大数の設定

同時管理 GUI または CLI（SSH）セッションの最大数、および管理 Web または CLI インターフェイスにアクセスする管理者を手助け、ガイドするログインバナーを設定できます。管理者のログイン前後に表示されるログインバナーを設定できます。デフォルトでは、これらのログインバナーは無効になっています。ただし、個々の管理者アカウントの同時セッションの最大数を設定することはできません。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]>[システム（System）]>[管理者アクセス（Admin Access）]>[設定（Settings）]>[アクセス（Access）]>[セッション（Session）]** を選択します。

ステップ 2 GUI および CLI インターフェイスを介した同時管理セッションの、許可する最大数を入力します。同時管理 GUI セッションの有効範囲は 1 ～ 20 です。同時管理 CLI セッションの有効範囲は 1 ～ 10 です。

ステップ 3 Cisco ISE で管理者がログインする前にメッセージを表示する場合は、[プリログイン バナー（Pre-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

ステップ 4 Cisco ISE で管理者がログインした後にメッセージを表示する場合は、[ポストログイン バナー（Post-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

ステップ 5 [保存（Save）] をクリックします。

（注） 文字制限は、ログイン前バナーでは 1500 字、ログイン後バナーでは 3000 字に設定されています。**%** と **<** を除くすべての文字がサポートされています。CLI を通じたログインバナーのインストールでは、使用するファイル名の長さは最大で 256 文字です。

関連トピック

IP アドレスの選択からの Cisco ISE への管理アクセスの許可 （662 ページ）

IP アドレスの選択からの Cisco ISE への管理アクセスの許可

Cisco ISE では、管理者が Cisco ISE 管理インターフェイスにアクセスできる IP アドレスのリストを設定することができます。

管理者アクセスコントロール設定は、管理ペルソナ、ポリシーサービスペルソナ、またはモニタリングペルソナを担う Cisco ISE ノードに対してのみ適用できます。これらの制限は、プライマリ ノードからセカンダリ ノードに複製されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[アクセス（Access）]** を選択します。

ステップ 2 対応するサービスタブをクリックして、アクセス制限を設定するサービスを選択します。次のサービスのアクセス制限を設定できます。

- **管理 GUI および CLI**
- **管理サービス**（ERS API、OpenAPI、pxGrid、および Data Connect）
- **ユーザーサービス**（ゲスト、BYOD、およびポスチャ）

ステップ 3 [リストにあるIPアドレスだけに接続を許可（Allow only listed IP addresses to connect）] オプションボタンをクリックします。

（注） 管理アクセスにはポート 161（SNMP）の接続を使用します。ただし、IP アクセス制限が設定されている場合は、実行元のノードで管理アクセスが設定されていないと **snmpwalk** が失敗します。

ステップ 4 **[アクセス許可のIPリストの設定（Configure IP List for Access Permission）]** 領域で、[追加（Add）] をクリックします。

ステップ 5 [IP CIDR の追加（Add IP CIDR）] ダイアログボックスで、[IP アドレス（IP Address）] フィールドに IP アドレスをクラスレスドメイン間ルーティング（CIDR）形式で入力します。

（注） この IP アドレスは、IPv4 または IPv6 アドレスにすることができます。Cisco ISE ノードに複数の IPv6 アドレスを設定できます。

ステップ 6 [CIDR 形式のネットマスク（Netmask in CIDR format）] フィールドにサブネットマスクを入力します。

ステップ 7 [OK] をクリックします。

ステップ 4 ～ 7 を繰り返して、他の IP アドレス範囲をこのリストに追加します。

ステップ 8 [保存（Save）] をクリックして、変更内容を保存します。

ステップ 9 [IP アクセス（IP Access）] ウィンドウを更新するには、[リセット（Reset）] をクリックします。

Cisco ISE の MnT ノードへのアクセスの許可

Cisco ISE では、展開内のノードのみが MnT ノードにログとアラームを送信できるようにするか、制限を設定しないかを選択できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE ホームページから、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [アクセス（Access）]** を選択します。

ステップ 2 [MnTアクセス（MnT Access）] タブをクリックします。

ステップ 3 展開内または展開外のいずれかのノードまたはエンティティが MnT に syslog を送信できるようにするには、[MnTへの接続を任意のIPアドレスに許可します（Allow any IP address to connect to MnT）] ラジオボタンをクリックします。展開内のノードまたはエンティティのみが syslog を MnT に送信できるようにするには、[MnTへの接続を展開内のノードのみに許可します（Allow only the nodes in the deployment to connect to MnT）] ラジオボタンをクリックします。

（注） ISE 2.6 P2 以降では、Cisco ISE メッセージングサービスを介した syslog がデフォルトでオンになっています。これにより、アラーム、設定変更、セッション情報などの syslog イベントを、展開外の他のエンティティから受信できます。

管理者アカウントのパスワード ポリシーの設定

Cisco ISE では、セキュリティ向上のために管理者アカウントにパスワード ポリシーを作成することもできます。パスワードベースまたはクライアント証明書ベースの管理者認証のいずれが必要かを定義できます。ここで定義したパスワードポリシーは、Cisco ISE 内のすべての管理者アカウントに適用されます。

（注）

- 内部管理者ユーザーの電子メール通知は root@host に送信されます。電子メール アドレスは設定できません。多くの SMTP サーバーがこの電子メールを拒否します。

  未解決の不具合 CSCui5583 を確認できます。これは、電子メールアドレスの変更を許可する拡張機能です。

- Cisco ISE では、管理者パスワードでの UTF-8 文字の使用はサポートされていません。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- 展開内で自動フェールオーバー設定が有効になっている場合は、オフにします。「管理ノードの自動フェールオーバーのサポート （450 ページ）」を参照してください。

  認証方式を変更すると、アプリケーション サーバー プロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ管理ノードの自動フェールオーバーが開始される場合があります。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]**選択します。

ステップ 2 次のいずれかの認証方式のオプションボタンをクリックします。

- [パスワードベース（Password Based）]：管理者ログインに標準ユーザー ID とパスワードクレデンシャルを使用します。[ID ソース（Identity Source）] ドロップダウンリストから [内部（Internal）] または [外部（External）] を選択します。

  （注） LDAP などの外部 ID ストアを設定しており、それを認証ソースとして使用して管理者ユーザーにアクセス権を付与する場合は、その ID ソースを [ID ソース（Identity Source）] リスト ボックスから選択する必要があります。

- [クライアント証明書ベース（Client Certificate Based）]：証明書ベースのポリシーを指定するには、このオプションを選択します。[証明書認証プロファイル（Certificate Authentication Profile）] ドロップダウンリストから、既存の認証プロファイルを選択します。[ID ソース（Identity Source）] ドロップダウンリストから必要な値を選択します。

ステップ 3 [パスワードポリシー（Password Policy）] タブをクリックし、Cisco ISE の GUI と CLI のパスワード要件を設定するために必要な値を入力します。

ステップ 4 [保存（Save）] をクリックして、管理者パスワード ポリシーを保存します。

（注） 外部 ID ストアを使用してログイン時に管理者を認証する場合は、管理者プロファイルに適用されるパスワードポリシーにこの設定値が設定されている場合でも、外部 ID ストアが依然として管理者のユーザー名とパスワードを認証することに注意してください。

関連トピック

管理者パスワード ポリシーの設定 （438 ページ）
管理者アカウントのアカウント無効化ポリシーの設定 （665 ページ）
管理者アカウントのロック設定または一時停止設定 （666 ページ）

管理者アカウントのアカウント無効化ポリシーの設定

Cisco ISE では、設定した連続日数の間に管理者アカウントが認証されなかった場合は、管理者アカウントを無効にすることができます。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [アカウント無効化ポリシー（Account Disable Policy）]）** を選択します。

ステップ 2 [非アクティブになってからn日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオンにして、対応するフィールドに日数を入力します。

このオプションでは、管理者アカウントが指定した日数の間非アクティブだった場合に管理者アカウントを無効にすることができます。ただし、**[管理（Administration）] > [システム（System）] > [管理者アクセ**

ス（**Admin Access**）] > **[管理者（Administrators）]** > **[管理ユーザー（Admin Users）]** ウィンドウの [非アクティブアカウントを無効化しない（Inactive Account Never Disabled）] オプションを使用して、このアカウント無効化ポリシーから個々の管理者アカウントを除外することができます。

管理者アカウントを無効にして後で有効にすると、24 時間以上アクティブのままになりません。管理者アカウントを無効にしてもアクティブなままにしたい場合は、[*n*日間の非アクティブ後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオフのままにします。

注目　[収集フィルタ（Collection Filters）]（**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[設定（Settings）]** > **[収集フィルタ（Collection Filters）]** > **[すべてをフィルタリング（Filter All）]**）が設定されている管理者アカウントの場合、Cisco ISE は [非アクティブになってからn日後にアカウントを無効にする（Disable account after n days of inactivity）] オプションをサポートしません（このオプションが有効になっている場合でも）。

ステップ 3　[保存（Save）] をクリックして、管理者のグローバル アカウント無効化ポリシーを設定します。

管理者アカウントのロック設定または一時停止設定

Cisco ISE では、指定されたログイン試行失敗回数を超えた管理者アカウント（パスワードベースの内部管理者アカウントと証明書ベースの管理者アカウントを含む）をロックまたは一時停止できます。

ステップ 1　Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[認証（Authentication）]** > **[設定のロック/一時停止（Lock/Suspend Settings）]** を選択します。

ステップ 2　[ログイン試行が間違っているアカウントを一時停止またはロックする（Suspend or Lock Account With Incorrect Login Attempts）] チェックボックスをオンにして、アクションを実行するまでの試行失敗の回数を入力します。有効な範囲は、3 ～ 20 です。次のオプションのいずれかのオプションボタンをクリックします。

- [*n* 分間アカウントを一時停止（Suspend Account For n Minutes）]：指定した間違ったログイン試行回数を超えるアカウントを一時停止するには、このオプションを選択します。有効な範囲は、15 ～ 1440 です。
- [アカウントのロック（Lock Account）]：指定した間違ったログイン試行回数を超えるアカウントをロックするには、このオプションを選択します。

エンドユーザーにヘルプデスクに連絡してアカウントのロックを解除するよう要求するなどの、修復を依頼するカスタムの電子メールメッセージを入力することができます。[ログイン試行が間違っているアカウントを一時停止またはロックする（Suspend Or Lock Account With Incorrect Login Attempts）] オプションを無効にしてから有効にすることで、ロックされたすべてのアカウントのロックを解除することもできます。

管理者のセッション タイムアウトの設定

Cisco ISE を使用すると、管理 GUI セッションが非アクティブであっても依然として接続状態である時間を決定できます。分単位の時間を指定することができ、その時間が経過するとCisco ISEは管理者をログアウトします。セッションのタイムアウト後、管理者は、Cisco ISE 管理者ポータルにアクセスするには再びログインする必要があります。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** > **[セッションのタイムアウト（Session Timeout）]** を選択します。

ステップ 2 アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。

ステップ 3 [保存（Save）] をクリックします。

アクティブな管理セッションの終了

Cisco ISE では、すべてのアクティブな管理セッションが表示され、そこからセッションを選択し、必要が生じた場合はいつでも終了できます。同時管理 GUI セッションの最大数は 20 です。GUIセッションの最大数に達した場合、スーパー管理者グループに属する管理者がログインして一部のセッションを終了できます。

始める前に

次のタスクを実行するには、スーパー管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** > **[セッション情報（Session Info）]** を選択します。

ステップ 2 終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。

管理者の名前の変更

Cisco ISE では、Cisco ISE GUI からユーザー名を変更できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE 管理ポータルにログインします。

ステップ 2 Cisco ISE GUI の右上隅にある [歯車（gear）] アイコン（⚙）をクリックし、ドロップダウンリストから [アカウント設定（Account Settings）] を選択します。

ステップ 3 表示される [管理者ユーザー（Admin User）] ダイアログボックスに新しいユーザー名を入力します。

ステップ 4 変更するアカウントに関するその他の詳細を編集します。

ステップ 5 [保存（Save）] をクリックします。

管理者アクセスの設定

これらのセクションで、管理者のアクセス設定を行うことができます。

管理者パスワード ポリシーの設定

次の表では、管理者パスワードが満たす必要のある基準を定義するために使用できる [パスワードポリシー（Password Policy）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理アクセス（Admin Access）] > [認証（Authentication）] > [パスワードポリシー（Password Policy）]**。

表 *39 :* 管理者パスワード ポリシーの設定

フィールド名	使用上のガイドライン
最小長（Minimum Length）	パスワードの最小長（文字数）を指定します。デフォルトは 6 文字です。

フィールド名	使用上のガイドライン
パスワードに使用できない文字（Password may not contain）	[管理者名またはその文字の逆順（Admin name or its characters in reverse order）]：このチェックボックスをオンにして、管理者ユーザー名またはその文字の逆順でのパスワードとしての使用を制限します。
	[Ciscoまたはその文字の逆順（Cisco or its characters in reverse order）]：このチェックボックスをオンにして、単語「Cisco」またはその文字の逆順でのパスワードとしての使用を制限します。
	[この単語またはその文字の逆順（This word or its characters in reverse order）]：このチェックボックスをオンにして、定義したすべての単語またはその文字の逆順でのパスワードとしての使用を制限します。
	[4回以上連続する繰り返し文字の使用（Repeated characters four or more times consecutively）]：このチェックボックスをオンにして、4 回以上連続する繰り返し文字のパスワードとしての使用を制限します。
	[辞書の単語、その文字の逆順、または文字の置き換え（Dictionary words, their characters in reverse order or their letters replaced with other characters）]：辞書の単語、単語の文字の逆順での使用、または単語の文字の置き換えでのパスワードとしての使用を制限します。 「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」などに置き換えることはできません。たとえば、「Pa $$ w0rd」は許可されません。 • [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。 このオプションは、デフォルトで選択されます。 • [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。**[ファイルの選択（Choose File）]** をクリックし、カスタム辞書ファイルを選択します。このテキストファイルは、改行文字で区切られた（JSON 形式の）単語、.dic 拡張子、20 MB 以下のサイズで成り立っている必要があります。
パスワードには選択したタイプの文字がそれぞれ1文字以上含まれている必要があります（Password must contain at least one character of each of the selected types）	管理者のパスワードに含める必要がある文字のタイプのチェックボックスをオンにします。次の 1 つまたは複数のオプションを選択します。 • **小文字の英文字** • **大文字の英文字** • **数字** • **英数字以外の文字**

フィールド名	使用上のガイドライン
パスワード履歴（Password History）	同じパスワードが繰り返し使用されるのを防ぐために、新しいパスワードと異なっている必要がある以前のパスワードの数を指定します。[パスワードは以前のnバージョンとは異なる必要があります（Password must be different from the previous n versions）] チェックボックスをオンにし、対応するフィールドに数字を入力します。 ユーザーがパスワードを再使用できない日数を入力します。[パスワードをn日以内に再利用することはできません（Cannot reuse password within n days）] をオンにし、対応するフィールドに数字を入力します。
パスワードライフタイム（Password Lifetime）	次のオプションのチェックボックスをオンにして、指定した期間後にパスワードを変更するようユーザーに強制します。 • [管理者パスワードは作成後または最終変更後n日で有効期限が切れます（Administrator passwords expire n days after creation or last change）]：パスワードを変更しない場合に管理者アカウントが無効になるまでの時間（日数）。有効な範囲は 1 ～ 3,650 日です。 • [パスワードの有効期限のn日前に管理者に電子メールリマインダを送信します（Send an email reminder to administrators n days prior to password expiration）]：パスワードが期限切れになることを管理者に通知するまでの時間（日数）。有効な範囲は 1 ～ 3,650 日です。
ネットワークデバイスの機密データの表示	
管理者パスワードが必要（Require Admin Password）	共有秘密やパスワードなどのネットワークデバイスの機密データを表示するために管理者ユーザーがログインパスワードを入力するようにする場合には、このチェックボックスをオンにします。
パスワードをn分間キャッシュします（Password cached for n Minutes）	管理者ユーザーによって入力されたパスワードは、この期間キャッシュされます。管理ユーザーはこの間、ネットワークデバイスの機密データを表示するのにパスワードの再入力を求められることはありません。有効な範囲は 1 ～ 60 分です。

関連トピック

Cisco ISE 管理者 （9 ページ）
新しい管理者の作成 （11 ページ）

セッション タイムアウトおよびセッション情報の設定

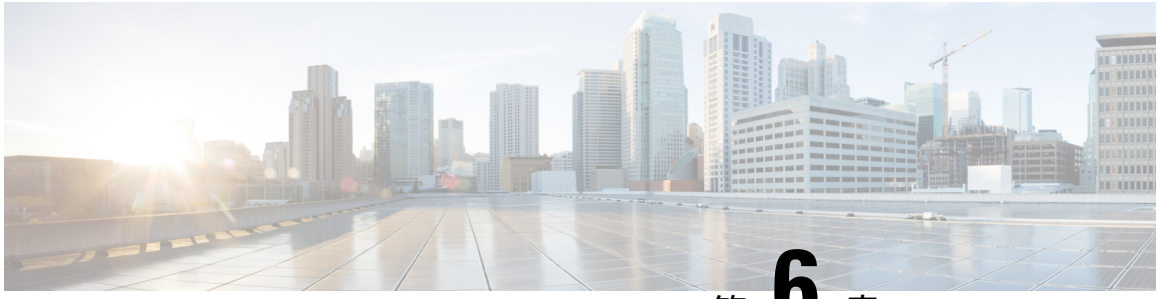
次の表では、セッションタイムアウトを定義し、アクティブな管理セッションを終了するために使用できる [セッション（Session）] ウィンドウのフィールドについて説明します。ウィンドウにアクセスするには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [セッション（Session）]** の順に選択します。

表 *40* : セッション タイムアウトおよびセッション情報の設定

フィールド名	使用上のガイドライン
セッションタイムアウト（Session Timeout）	
セッション アイドル タイムアウト（Session Idle Timeout）	アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。
セッション情報（Session Info）	
無効化（Invalidate）	終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。

関連トピック

管理者アクセスの設定 （661 ページ）
管理者のセッション タイムアウトの設定 （667 ページ）
アクティブな管理セッションの終了 （667 ページ）



第 6 章

メンテナンスとモニター

- 適応型ネットワーク制御 （674 ページ）
- Cisco ISE での適応型ネットワーク制御の有効化 （675 ページ）
- ネットワーク アクセスの設定 （675 ページ）
- ANC NAS ポートのシャットダウン フロー （677 ページ）
- エンドポイントの消去の設定 （677 ページ）
- 隔離済みエンドポイントがポリシー変更の後に認証を更新しない （679 ページ）
- ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する （679 ページ）
- 外部認証された管理者が ANC 操作を実行できない （680 ページ）
- バックアップ データのタイプ （680 ページ）
- バックアップ/復元リポジトリ （681 ページ）
- オンデマンドおよびスケジュール バックアップ （687 ページ）
- Cisco ISE 復元操作 （694 ページ）
- 認証および許可ポリシー設定のエクスポート （702 ページ）
- ポリシーのエクスポート設定のスケジュール （702 ページ）
- 分散環境でのプライマリ ノードとセカンダリ ノードの同期 （703 ページ）
- スタンドアロンおよび分散展開での失われたノードの復元 （704 ページ）
- Cisco ISE ロギング メカニズム （708 ページ）
- Cisco ISE システム ログ （709 ページ）
- リモート syslog 収集場所の設定 （710 ページ）
- Cisco ISE メッセージ コード （712 ページ）
- Cisco ISE メッセージ カタログ （713 ページ）
- エンドポイントのデバッグ ログ コレクタ （713 ページ）
- 収集フィルタ （714 ページ）
- システム 360 （716 ページ）
- Cisco ISE レポート （724 ページ）
- レポート フィルタ （724 ページ）
- クイック フィルタ条件の作成 （725 ページ）
- 拡張フィルタ条件の作成 （726 ページ）

- レポートの実行および表示 （726 ページ）
- レポートのナビゲーション （727 ページ）
- レポートのエクスポート （727 ページ）
- マイ レポート （728 ページ）
- Cisco ISE レポートのスケジュール （729 ページ）
- Cisco ISE のアクティブな RADIUS セッション （731 ページ）
- 使用可能なレポート （734 ページ）
- RADIUS ライブ ログ （774 ページ）
- RADIUS ライブ セッション （778 ページ）
- TACACS ライブ ログ （783 ページ）
- エクスポート サマリ （786 ページ）

適応型ネットワーク制御

適応型ネットワーク制御（ANC）は、管理ノードで実行されるサービスです。このサービスは、エンドポイントのネットワークアクセスをモニターおよび制御します。ANCは、ISE管理者が管理 GUI で呼び出すことも、サードパーティ製システムから pxGrid を介して呼び出すこともできます。 ANCは有線展開とワイヤレス展開をサポートしており、ライセンスとAdvantageライセンスが必要です。

ANC を使用すると、システムの許可ポリシー全体を変更することなく許可状態を変更できます。ANC を使用すると、エンドポイントを隔離するときに認証状態を設定できます。その結果、ANCPolicyを確認してネットワークアクセスを制限または拒否するように認証ポリシーが定義されている認証ポリシーが確立されます。エンドポイントを隔離解除して、フル ネットワーク アクセスを可能にできます。ネットワークからエンドポイントを接続解除するNetwork Attached System（NAS）上のポートをシャットダウンすることもできます。

一度に隔離できるユーザーの数に制限はありません。また、隔離期間の長さに時間的な制約はありません。

ANC によってネットワーク アクセスをモニターおよび制御するには、次の操作を実行できます。

- [隔離（Quarantine）]：例外ポリシー（認証ポリシー）を使用して、ネットワークへのエンドポイントアクセスを制限または拒否することができます。 ANCPolicyに応じて異なる許可プロファイル（権限）を割り当てるために、例外ポリシーを作成する必要があります。隔離状態に設定すると、基本的に、デフォルトの VLAN から指定した隔離 VLAN にエンドポイントが移動します。エンドポイントと同じ NAS でサポートされる隔離 VLAN を事前に定義する必要があります。

- [隔離解除（Unquarantine）]：隔離ステータスを元に戻し、エンドポイントのネットワークへのフルアクセスを許可します。これは、エンドポイントを元の VLAN に戻すことで発生します。

- [シャットダウン（Shutdown）]：NAS 上のポートを非アクティブ化して、ネットワークからエンドポイントの接続を解除できます。エンドポイントが接続されている NAS でポー

トがシャットダウンされたら、NASのポートを再度手動でリセットします。これにより、エンドポイントがネットワークに接続できるようになります。これはワイヤレス展開には使用できません。

アクティブ エンドポイントに対する隔離および隔離解除操作は、セッション ディレクトリ レポートからトリガーできます。

（注） 隔離されていたセッションが隔離解除された場合、新たに隔離解除されたセッションの開始方法は、スイッチ設定で指定されている認証方法によって決まります。

Cisco ISE での適応型ネットワーク制御の有効化

ANC は、デフォルトで無効になっています。ANC は pxGrid が有効にされた場合にのみ有効になり、管理者ポータルでサービスを手動で無効にするまで有効のままになります。

ネットワーク アクセスの設定

ANC によってエンドポイントのネットワークアクセスのステータスをポートの隔離、隔離解除、またはシャットダウンにリセットできます。これらは、ネットワーク内のエンドポイントの許可の程度を定義します。

エンドポイントの隔離や隔離解除、またはエンドポイントが接続されているネットワーク アクセス サーバー（NAS）ポートのシャットダウンを行うには、エンドポイントの IP アドレスまたは MAC アドレスを使用します。同時に実行しない限り、同じエンドポイントに複数回、隔離操作および隔離解除操作を実行できます。ネットワーク上に悪意のあるエンドポイントを見つけた場合は、 ANC を使用してそのエンドポイントのアクセスをシャットダウンし、NAS ポートを閉じることができます。

ANC ポリシーをエンドポイントに割り当てるには、次の手順を実行します。

始める前に

- ANC を有効にします。
- ANC の認証プロファイルと例外タイプの認証ポリシーを作成します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[適応型ネットワーク制御（Adaptive Network Control）]** > **[ポリシーリスト（Policy List）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ANC ポリシーの名前を入力し、ANC アクションを指定します。次のオプションを使用できます。

- Quarantine

- Shut_Down
- Port_Bounce
- Re_Authenticate

[Quarantine] と [Re_Authenticate] は、組み合わせることができる唯一の 2 つのアクションです。

[Quarantine]、[Port_Bounce]、または [Re_Authenticate] を含む ANC ポリシーがアクティブなエンドポイントに割り当てられるか、割り当て解除されると、そのエンドポイントに対して CoA がトリガーされます。

[Shut_Down] アクションを含む ANC ポリシーがアクティブなエンドポイントに割り当てられると、CoA がトリガーされてスイッチインターフェイスがシャットダウンされます。ただし、[Shut_Down] アクションを含む ANC ポリシーが割り当て解除されるときは、CoA はトリガーされません。

ステップ 4 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択して、ポリシー セットを展開します。

ステップ 5 ANCPolicy 属性を使用して ANC ポリシーを対応する許可ポリシーに関連付けます。

ステップ 6 [操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）] > [エンドポイント割り当て（Endpoint Assignment）] の順に選択します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 エンドポイントの IP アドレスまたは MAC アドレスを入力し、[ポリシー割り当て（Policy Assignment）] ドロップダウン リストからポリシーを選択します。

ステップ 9 [送信（Submit）] をクリックします。

ANC によるネットワーク アクセスの許可プロファイルの作成

ANC と使用する認証プロファイルを作成する必要があります。認証プロファイルは、標準認証プロファイルのリストに表示できます。エンドポイントはネットワークで認証および許可されますが、ネットワークへのアクセスが制限されています。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[許可（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 認証プロファイルの一意の名前と説明を入力し、[アクセス タイプ（Access Type）] は [ACCESS_ACCEPT] に更新します。

ステップ 4 [DACL 名（DACL Name）] チェックボックスをオンにし、ドロップダウン リストから [DENY_ALL_TRAFFIC] を選択します。

ステップ 5 [送信（Submit）] をクリックします。

例外許可ポリシーは、特別な条件や権限、または緊急の要件を満たすために制限付きアクセスを許可することを目的としています。ANC 許可用に、すべての標準認証ポリシーの前に処理

される隔離例外ポリシーを作成する必要があります。次の条件で例外ルールを作成する必要があります。

セッション：ANCPolicy EQUALS Quarantine。

ANC NAS ポートのシャットダウン フロー

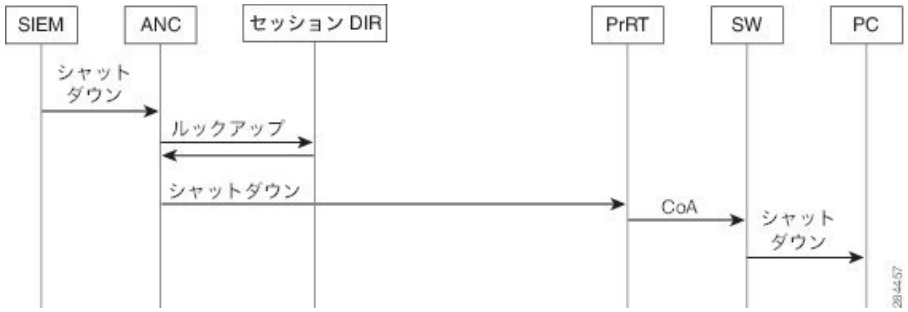
エンドポイントのIPアドレスまたはMACアドレスを使用して、エンドポイントの接続先NASポートをシャット ダウンできます。

シャットダウンを使用すると、MAC アドレスに指定された IP アドレスに基づいて NAS ポートを閉じることができます。手動でポートを復元して、エンドポイントをネットワークに戻す必要があります。これは、有線メディアで接続されたエンドポイントのみに有効です。

シャットダウンはすべてのデバイスでサポートされているわけではありません。ただし、大部分のスイッチでシャットダウン コマンドがサポートされています。getResult() コマンドを使用すると、シャットダウンが正常に実行されたかどうかを確認できます。

この図は、 ANC のシャットダウンのフローを示しています。クライアントデバイスでは、このクライアントデバイスがネットワークにアクセスするために使用する NAS でシャットダウン操作が実行されます。

図 *11 : ANC* のシャットダウン フロー



エンドポイントの消去の設定

ID グループとその他の条件に基づいた設定ルールで、エンドポイントの消去ポリシーを定義できます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイントの消去（Endpoint Purge）]** の順に選択します。指定したエンドポイントを消去しないことや、選択したプロファイリング条件に基づいてエンドポイントを消去することを選択できます。

エンドポイント消去ジョブをスケジュールできます。このエンドポイント消去スケジュールはデフォルトで有効です。Cisco ISE はデフォルトで、30 日よりも古い登録デバイスとエンドポイントを削除します。消去ジョブは、プライマリ管理ノード（PAN）で設定されたタイムゾーンに基づいて毎日午前 1 時（深夜）に実行されます。

エンドポイントの消去では、3 分ごとに 5000 以上のエンドポイントが削除されます。

次に、エンドポイントの消去に使用できる条件と例の一部を示します。

- InactivityDays：エンドポイントでの最後のプロファイリング アクティビティまたは更新からの日数。
  - この条件によって、時間の経過に伴って蓄積した古いデバイス（一般的には一時的なゲストやパーソナルデバイス）、または廃止されたデバイスが消去されます。これらのエンドポイントは、ネットワーク上でアクティブでないか、近い将来に使用される可能性が低いため、展開でノイズとなる傾向があります。それらが再度接続した場合は、必要に応じて再検出、プロファイリング、登録などが行われます。
  - エンドポイントから更新が発生すると、InactivityDays はプロファイリングが有効である場合にのみ 0 にリセットされます。
- ElapsedDays：オブジェクトが作成されてからの日数。
  - この条件は、ゲストまたは請負業者のエンドポイント、ネットワーク アクセスに WebAuth を利用する従業員などの、未認証アクセスまたは条件付きアクセスが一定期間認められたエンドポイントに使用できます。許可された接続猶予期間が経過した後、それらは完全に再認証および登録される必要があります。
- PurgeDate：エンドポイントを消去する日付。
  - このオプションは、作成または開始時間に関係なく一定期間のアクセスを許可する、特別なイベントやグループに使用できます。このオプションでは、すべてのエンドポイントを同時に消去できます。たとえば、展示会、会議、または毎週メンバーが入れ替わる週ごとのトレーニングクラスでは、絶対的な日や週や月ではなく、特定の週や月にアクセスを許可する場合に使用します。

エンドポイント消去ポリシーの条件としてカスタム属性を使用することはできません。

（注） 消去するエンドポイント数が 10,000 を超える場合、初回の消去時に最初の 10,000 エンドポイントのみが消去されます。1 時間後に、次の 10000 エンドポイントのセットを削除するために別のパージが開始されます。この消去サイクルは、一致する消去条件に基づいてすべてのエンドポイントが消去されるまで続きます。この動作により、システムパフォーマンスが最適化されます。

隔離済みエンドポイントがポリシー変更の後に認証を更新しない

問題

ポリシー変更またはIDの追加後に認証が失敗し、再認証が行われません。認証が失敗するか、問題のエンドポイントがネットワークに接続できなくなります。この問題は、ユーザーロールに割り当てられるポスチャポリシーごとのポスチャ評価に失敗するクライアントマシンで頻繁に発生します。

考えられる原因

クライアントマシンで認証タイマーが正しく設定されていないか、またはスイッチ上で認証間隔が正しく設定されていません。

ソリューション

この問題には、解決策がいくつか考えられます。

1. Cisco ISE で、指定された NAD またはスイッチの [セッションステータス概要（Session Status Summary）] レポートを検査し、インターフェイスに適切な認証間隔が設定されていることを確認します。
2. NAD/スイッチ上で "show running configuration" と入力し、適切な "authentication timer restart" 設定でインターフェイスが設定されていることを確認します（たとえば、"authentication timer restart 15" および "authentication timer reauthenticate 15"）。
3. NAD/スイッチ上で “interface shutdown” および "no shutdown" と入力してポートをバウンスし、Cisco ISE で構成変更があったと考えられる場合には再認証を適用します。

（注） CoA は MAC アドレスまたはセッション ID を必要とするので、Network Device SNMP レポートに表示されるポートをバウンスしないように推奨しています。

ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する

エンドポイントで実行する ANC 操作は、そのエンドポイントのアクティブなセッションに IP アドレスに関する情報が含まれていない場合に失敗します。このことは、そのエンドポイントの MAC アドレスおよびセッション ID にも適用されます。

（注） ANC を介してエンドポイントの許可状態を変更する場合は、エンドポイントの IP アドレスまたは MAC アドレスを指定する必要があります。エンドポイントのアクティブなセッションで IP アドレスまたは MAC アドレスが見つからない場合は、次のエラーメッセージが表示されます。

```
この MAC アドレス、IP アドレス、またはセッション ID のアクティブなセッションが見つかりません（No active session found for this MAC address, IP Address or Session ID）
```

。

外部認証された管理者が ANC 操作を実行できない

外部認証された管理者がライブ セッションから CoA 隔離を発行しようとすると、Cisco ISE は次のエラー メッセージを返します。

```
xx: xx: xx: xx: xx: xx に対する隔離の CoA アクションを開始できません。（原因：内部でユーザーが見つかりません。サポートされていない外部認証されたユーザーを使用している可能性があります（CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User not found internally. Possible use of unsupported externally authenticated user）
```

外部認証された管理者が、エンドポイントの IP アドレスまたは MAC アドレスを使用して、Cisco ISE の **[操作（Operations）]** から ANC 操作を実行すると、Cisco ISE は次のエラーメッセージを返します。

```
サーバー障害：内部でユーザーが見つかりません。サポートされていない外部認証されたユーザーを使用している可能性があります（Server failure: User not found internally. Possible use of unsupported externally authenticated user）
```

バックアップ データのタイプ

Cisco ISE では、プライマリ PAN とモニタリングノードからデータをバックアップできます。バックアップは CLI またはユーザー インターフェイスから実行できます。

Cisco ISE では次のタイプのデータのバックアップが可能です。

- 設定データ：アプリケーション固有および Cisco ADE オペレーティング システム両方の設定データが含まれます。バックアップは、GUI または CLI を使用してプライマリ PAN を介して実行できます。

- 運用データ：モニタリングおよびトラブルシューティング データが含まれます。バックアップは、プライマリ PAN GUI を介して、またはモニタリングノードの場合は CLI を使用して実行できます。

Cisco ISE が VMware で実行されている場合、ISE データをバックアップするのに、VMware スナップショットはサポートされていません。

（注） Cisco ISE は、ISE データのバックアップ用の VMware スナップショットをサポートしていません。これは、VMware スナップショットが特定の時点で VM のステータスを保存するためです。マルチノード Cisco ISE 環境では、すべてのノードのデータが現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。データのバックアップおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。

VMware スナップショットまたはサードパーティのバックアップサービスを使用して Cisco ISE データをバックアップすると、Cisco ISE サービスが割り込まれることがあります。バックアップが VMware または CommVault SAN レベルのバックアップのようなサードパーティのバックアップサービスによって開始された場合、ファイルシステムを休止してクラッシュ整合を維持するために、Cisco ISE 機能がフリーズする可能性があります。Cisco ISE 展開でサービスを再開するには再起動が必要です。

復元操作は、以前のバージョンの Cisco ISE のバックアップファイルを使用して実行でき、以前のバージョンが以降のバージョンでサポートされている直接アップグレードパスにある場合、以降のバージョンで復元できます。

Cisco ISE リリース 3.4 は、リリース 3.1 以降から取得したバックアップからの復元をサポートしています。

（注） データをバックアップおよび復元した後に展開を再作成するときに、両方のノードのデータが同期されるようにするには、プライマリ PAN とセカンダリ PAN の両方の [コンテキストの可視性リセット（Context Visibility Reset）] が必要です。

バックアップ/復元リポジトリ

Cisco ISE では管理者ポータルを使用してリポジトリを作成および削除できます。次のタイプのリポジトリを作成できます。

- DISK
- FTP
- SFTP
- NFS

- CD-ROM
- HTTP
- HTTPS

（注） リポジトリは、各デバイスに対してローカルです。

どのタイプの展開（小規模、中規模、大規模）であっても、最低でも 100 GB のリポジトリ サイズを用意することを推奨します。

次の表に、Cisco ISE の操作と外部リポジトリのタイプ間でのサポート情報を示します。

表 *41* : 外部リポジトリのサポート マトリックス

リポジトリ タイプ	バックアップの設定	復元の設定	アップグレード	操作バックアップ	復元操作	サポートバンドル	ユーザー インターフェイスからの検証	ユーザー インターフェイスからのレポートのエクスポート	ユーザーインターフェイスからのポリシーのエクスポート
FTP	√	√	√	√	√	√	√	√	√
SFTP	√	√	√	√	√	√	√	√	√
TFTP	X	X	X	X	X	X	X	X	X
HTTP	X	X	√	X	X	X	X	X	X
HTTPS	X	*X*	√	X	X	X	X	X	X
NFS	√	√	√	√	√	√	√	√	√

リポジトリの作成

リポジトリを作成するには、CLI と GUI を使用できます。次の理由により、GUI を使用することを推奨します。

- CLI で作成されたリポジトリはローカルに保存され、他の展開ノードに複製されません。これらのリポジトリは、GUI のリポジトリ ページに表示されません。
- プライマリ PAN で作成されたリポジトリが他の展開ノードに複製されます。

キーはプライマリ PAN でのみ GUI で生成されます。このため、アップグレード時に新しいプライマリ管理ノードの GUI でキーを再生成して、SFTP サーバーにエクスポートする必要があります。展開からノードを除去する場合、管理対象以外のノードの GUI でキーを生成し、SFTP サーバーにエクスポートする必要があります。

RSA 公開キー認証を使用する Cisco ISE の SFTP リポジトリを設定できます。データベースとログを暗号化するために管理者が作成したパスワードを使用する代わりに、セキュア キーを使用する RSA 公開キー認証を選択できます。RSA 公開キーを使用して作成された SFTP リポジトリの場合、GUI から作成されたリポジトリは CLI では複製されず、CLI から作成されたリポジトリは GUI では複製されません。CLI と GUI で同じリポジトリを設定するには、CLI と GUI の両方で RSA 公開キーを生成し、この両方のキーを SFTP サーバーにエクスポートします。

（注） Cisco ISE は、FIPS モードが ISE で有効になっていない場合でも、FIPS モードで発信 SSH または SFTP 接続を開始します。ISE と通信するリモート SSH または SFTP サーバーが FIPS 140 承認暗号化アルゴリズムを許可していることを確認します。

Cisco ISE では、組み込みの FIPS 140 の検証済み暗号化モジュールが使用されています。FIPS コンプライアンスの要求の詳細については、『FIPS Compliance Letter』を参照してください。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者の権限が必要です。
- RSA 公開キー認証を使用して SFTP リポジトリを作成する場合は、次の手順を実行します。
  - SFTP リポジトリの RSA 公開キー認証を有効にします。
  - 管理 CLI ユーザーとしてログインする必要があります。**crypto host_key add** コマンドを使用して Cisco ISE CLI から SFTP サーバーのホスト キーを入力します。ホストキー文字列は、リポジトリの設定ページで、[パス（Path）] フィールドに入力したホスト名と一致する必要があります。
  - GUI でキーペアを生成し、ローカル システムに公開キーをエクスポートします。Cisco ISE CLI から **crypto key generate rsa passphrase** *test123* コマンドを使用してキーペアを生成し（この場合パスフレーズは 14 文字以上でなければなりません）、キーを任意のリポジトリ（ローカルディスクまたは設定されているその他のリポジトリ）にエクスポートします。

- エクスポートした RSA 公開キーを PKI 対応の SFTP サーバーにコピーし、「authorized_keys」ファイルに追加します。

（注） プライマリ PAN とプライマリ MnT が別々のノードである場合、[リポジトリリスト（Repository List）] ウィンドウの [キーペアの生成（Generate Key Pairs）] オプションを使用して、プライマリ PAN とプライマリ MnT ノードの両方の RSA キーを生成できます。[リポジトリリスト（Repository List）] ウィンドウの [公開キーのエクスポート（Export Public Key）] オプションを使用して、プライマリ PAN ノードとプライマリ MnT ノードの両方から生成された RSA キーをエクスポートできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）]

ステップ 2 [追加（Add）] をクリックして、新しいリポジトリを追加します。

ステップ 3 新しいリポジトリのセットアップの必要に応じて値を入力します。フィールドの説明については、リポジトリの設定 （685 ページ）を参照してください。

ステップ 4 [送信（Submit）] をクリックしてリポジトリを作成します。

ステップ 5 左側の [操作（Operations）] ナビゲーションペインで [リポジトリ（Repository）] をクリックするか、または [リポジトリ（Repository）] ウィンドウ上部の [リポジトリリスト（Repository List）] リンクをクリックして、リポジトリのリスト ページに移動して、リポジトリが正常に作成されていることを確認します。

次のタスク

- 作成したリポジトリが有効であることを確認します。これは、[リポジトリのリスト（Repository Listing）] ウィンドウから行います。対応するリポジトリを選択し、[検証（Validate）] をクリックします。また、Cisco ISE コマンドライン インターフェイスから次のコマンドを実行することもできます。

  show repository *repository_name*

  ここで、*repository_name* は作成したリポジトリの名前です。

（注） リポジトリの作成時に指定したパスが存在しない場合、次のエラーが表示されます。

```
%Invalid Directory
```

- オンデマンド バックアップを実行するかバックアップのスケジュールを設定します。

リポジトリの設定

次の表では、リポジトリを作成してバックアップ ファイルを保存するために使用できる [リポジトリリスト（Repository List）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）]**。

表 *42 :* リポジトリの設定

フィールド	使用上のガイドライン
リポジトリ（**Repository**）	リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。
プロトコル（**Protocol**）	使用する使用可能なプロトコルの 1 つを選択します。
サーバー名（**Server Name**）	（TFTP、HTTP、HTTPS、FTP、SFTP、および NFS で必須）リポジトリの作成先サーバーのホスト名または IP アドレス（IPv4 または IPv6）を入力します。 （注） IPv6 アドレスを使用してリポジトリを追加する場合は、IPv6 アドレスを使用して ISE eth0 インターフェイスが設定されていることを確認します。
パス（**Path**）	リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。 この値は、サーバーのルート ディレクトリを示す 2 つのスラッシュ（//）または単一のスラッシュ（/）で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ（/）はルートディレクトリではなく、ローカル デバイス ホーム ディレクトリの FTP を示します。
PKI認証の有効化（**Enable PKI authentication**）	（オプション：SFTP リポジトリにのみ適用）SFTP リポジトリで RSA 公開キー認証を有効にするには、このチェック ボックスをオンにします。
ユーザー名（**User Name**）	（FTP、SFTP で必須）指定されたサーバーに対する書き込み権限を持つユーザー名を入力します。ユーザー名には、英数字と _-. /@\$ 文字を含めることができます。

フィールド	使用上のガイドライン
パスワード（**Password**）	（FTP、SFTP で必須）指定されたサーバーへのアクセスに使用するパスワードを入力します。パスワードに使用できる文字は、0 ～ 9、a ～ z、A ～ Z、-、.、|、@、#、$、^、&、*、,、+、および = です。 !、?、~ のような一部の特殊文字（上記のリストには含まれていません）は、GUI を介した FTP および SFTP パスワード設定で許可されていることに注意してください。ただし、これらの特殊文字は、CLI または Open API による設定には使用できません。

関連トピック

バックアップ/復元リポジトリ （681 ページ）
リポジトリの作成 （683 ページ）

SFTP リポジトリでの RSA 公開キー認証の有効化

SFTP サーバーでは、各ノードに 2 つの RSA 公開キー（CLI 用と GUI 用にそれぞれ 1 つずつ）が必要です。SFTP リポジトリで RSA 公開キー認証を有効にするには、次の手順を実行します。

（注） SFTP リポジトリで RSA 公開キー認証を有効にすると、SFTP ログイン情報を使用してログインできなくなります。PKI ベースの認証またはログイン情報ベースの認証を使用できます。ログイン情報ベースの認証を再度使用する場合は、SFTP サーバーから公開キーペアを削除する必要があります。

ステップ 1 */Etc/ssh/sshd_config.file* を編集する権限を持つアカウントで SFTP サーバーにログインします。

（注） *sshd_config* ファイルのロケーションは、インストールされているオペレーティング システムによって異なる可能性があります。

ステップ 2 **vi etc/ssh/sshd_config** コマンドを入力します。

Sshd_config ファイルの内容がリストされます。

ステップ 3 RSA 公開キー認証を有効にするには、以下の行の「#」記号を削除します。

- RSAAuthentication yes
- PubkeyAuthentication yes

（注） Public Auth Key が no の場合は yes に変更してください。

- AuthorizedKeysFile ~/.ssh/authorized_keys

ローカルディスクからのファイルのダウンロード

ローカルディスク管理に使用されるファイルは、簡単に追加、ダウンロード、または削除できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[システム（System）] > [メンテナンス（Maintenance）] > [ローカルディスク管理（Localdisk Management）]** を選択します。

ステップ 2 ダウンロードするファイルの横にあるチェックボックスをオンにします。

ステップ 3 [ダウンロード（Download）] をクリックします。

ステップ 4 （任意）Cisco ISE CLI から次のコマンドを実行して、ローカルディスクからファイルをダウンロードします。#copy disk:/ filename repository repository_name

ローカルディスクへのファイルのアップロード

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[システム（System）] > [メンテナンス（Maintenance）] > [ローカルディスク管理（Localdisk Management）]** を選択します。

ステップ 2 ファイルをアップロードするには、[アップロード（Upload ）] をクリックします。

ステップ 3 [ファイルの選択（Select File）] をクリックして、アップロードするファイルを参照して選択します。ファイルをドラッグアンドドロップすることもできます。

ステップ 4 [アップロードの開始（Start Upload）] をクリックします。

オンデマンドおよびスケジュール バックアップ

プライマリ PAN とプライマリ モニタリング ノードのオンデマンドバックアップを設定できます。バックアップデータがすぐに必要な場合にオンデマンドバックアップを実行します。

システムレベルのバックアップは、1 回のみ、毎日、毎週、または毎月実行するようにスケジュールできます。バックアップ操作は長時間かかる場合がありますが、スケジュールできるため中断が発生することはありません。管理者ポータルからバックアップをスケジュールできます。

（注） 内部 CA を使用している場合は、CLI を使用して証明書とキーをエクスポートする必要があります。管理ポータルでのバックアップでは、CA チェーンはバックアップされません。

詳細については、『Cisco Identity Services Engine Administrator Guide』の「Basic Setup」の章にある「Export Cisco ISE CA Certificates and Keys」の項を参照してください。

Cisco ISE の設定バックアップおよび運用バックアップは、短時間でシステムがオーバーロードになる可能性があります。この一時的なシステムオーバーロードで予想される動作は、システムの設定とモニタリングデータベースのサイズによって異なります。

関連トピック

メンテナンスの設定 （1868 ページ）

オンデマンド バックアップの実行

オンデマンドバックアップを実行して、設定データまたはモニタリング（運用）データを即座にバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。

重要 バックアップと復元を行う場合、復元によってターゲットシステム上の信頼できる証明書のリストがソースシステムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  長所：ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲットシステムによって発行された新しい証明書は、同じキーによって署名されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  長所：このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソースシステムによって発行された証明書は引き続き信頼されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

始める前に

- オンデマンドバックアップを実行する前に、Cisco ISE 内のバックアップデータタイプの基本を理解しておく必要があります。

- バックアップファイルを保存するためのリポジトリが作成されていることを確認します。
- ローカルリポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- バックアップを取得する前に、すべての証明書関連の変更を実行します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

（注） バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。バックアップを復元するには、リポジトリを選択し、[復元（Restore）] をクリックします。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup and Restore）]** を選択します。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup and Restore）]**。

ステップ 3 バックアップのタイプ [設定（Configuration）] または [動作中（Operational）] を選択します。

ステップ 4 [すぐにバックアップ（Backup Now）] をクリックします。

ステップ 5 バックアップを実行するために必要な値を入力します。

ステップ 6 **[バックアップ（Backup）]** をクリックします。

ステップ 7 バックアップが正常に完了したことを確認します。

Cisco ISE はタイムスタンプを持つバックアップ ファイル名を付け、指定されたリポジトリにファイルを保存します。タイムスタンプに加えて、Cisco ISE は設定バックアップには CFG タグ、操作バックアップには OPS タグを追加します。バックアップファイルが指定リポジトリにあることを確認します。

分散展開では、バックアップの実行中にノードのロールを変更したり、ノードの設定を行ったりすることはできません。バックアップの実行中にノードのロールを変更すると、すべてのプロセスがシャットダウンし、データに不一致が生じる場合があります。ノードのロールを変更する際は、バックアップが完了するまで待機してください。

バックアップの実行中はノードを昇格しないでください。これによりすべてのプロセスがシャットダウンし、バックアップを同時に実行中の場合はデータに不一致が生じる場合があります。ノードを変更する際は、バックアップが完了するまで待ってください。

（注） バックアップが実行されているときに、高い CPU 使用率が観察されたり、[負荷平均が高い（High Load Average）] アラームが表示されたりする可能性があります。バックアップが完了すると、CPU 使用率は通常に戻ります。

関連トピック

Cisco ISE 復元操作 （694 ページ）
認証および許可ポリシー設定のエクスポート （702 ページ）

オンデマンド バックアップの設定

次の表では、バックアップを任意の時点で取得するために使用できる [オンデマンドバックアップ（On-Demand Backup）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup & Restore）]** です。

表 *43* : オンデマンド バックアップの設定

フィールド名	使用上のガイドライン
タイプ（**Type**）	次のいずれかを実行します。 • **[設定データのバックアップ（Configuration Data Backup）]**：アプリケーション固有および Cisco ADE オペレーティングシステム両方の構成データが含まれます。 • **[運用データのバックアップ（Operational Data Backup）]**：モニタリングおよびトラブルシューティング データが含まれます。
バックアップ名（**Backup Name**）	バックアップ ファイルの名前を入力します。
リポジトリ名（**Repository Name**）	バックアップ ファイルを保存するリポジトリ。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（**Encryption Key**）	このキーは、バックアップ ファイルの暗号化および解読に使用されます。

関連トピック

バックアップ データのタイプ （680 ページ）
オンデマンドおよびスケジュール バックアップ （687 ページ）
バックアップ履歴 （693 ページ）
バックアップの失敗 （694 ページ）

Cisco ISE 復元操作 （694 ページ）
認証および許可ポリシー設定のエクスポート （702 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （703 ページ）
オンデマンド バックアップの実行 （688 ページ）

バックアップのスケジュール

オンデマンドバックアップを実行して、設定データまたはモニタリング（運用）データを即座にバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。

重要 バックアップと復元を行う場合、復元によってターゲットシステム上の信頼できる証明書のリストがソースシステムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  長所：ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲット システムによって発行された新しい証明書は、同じキーによって署名されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  長所：このオプションは推奨される適切な方法です。元のソースの証明書または元のターゲットの証明書が使用されます。元のソース システムによって発行された証明書は引き続き信頼されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

始める前に

- バックアップをスケジュールする前に、Cisco ISE 内のバックアップデータタイプの基本を理解しておく必要があります。
- リポジトリを設定していることを確認します。

- ローカルリポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

（注） バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

スケジュール バックアップの設定

次の表では、フルバックアップまたは増分バックアップの復元に使用できる[スケジュールバックアップ（Scheduled Backup）]ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup and Restore）]** です。

表 *44* : スケジュール バックアップの設定

フィールド名	使用上のガイドライン
タイプ（**Type**）	次のいずれかを実行します。 • **[設定データのバックアップ（Configuration Data Backup）]**：アプリケーション固有およびCisco ADE オペレーティングシステム両方の構成データが含まれます。 • **[運用データのバックアップ（Operational Data Backup）]**：モニタリングおよびトラブルシューティング データが含まれます。
名前（**Name**）	バックアップ ファイルの名前を入力します。任意のわかりやすい名前を入力できます。Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加して、ファイルをリポジトリに格納します。複数のバックアップを作成するように設定しても、一意なバックアップ ファイル名を得ることができます。[スケジュールバックアップ（Scheduled Backup）]リストウィンドウで、ファイル名の先頭に「backup_occur」が追加され、このファイルが **kron** ジョブであることを示します。
説明（**Description**）	バックアップの説明を入力します。

フィールド名	使用上のガイドライン
リポジトリ名（**Repository Name**）	バックアップ ファイルを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（**Encryption Key**）	バックアップ ファイルを暗号化および復号化するためのキーを入力します。
スケジューリング オプション（**Schedule Options**）	スケジュール バックアップの頻度を選択し、適宜他のオプションに入力します。

関連トピック

バックアップ データのタイプ （680 ページ）
オンデマンドおよびスケジュール バックアップ （687 ページ）
バックアップ履歴 （693 ページ）
バックアップの失敗 （694 ページ）
Cisco ISE 復元操作 （694 ページ）
認証および許可ポリシー設定のエクスポート （702 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （703 ページ）
CLI を使用したバックアップ （693 ページ）
バックアップのスケジュール （691 ページ）

CLI を使用したバックアップ

CLI と GUI の両方からバックアップのスケジュールを設定できますが、GUI の使用を推奨します。ただし、セカンダリ モニタリング ノードの操作バックアップは、CLI からのみ実行できます。

バックアップ履歴

バックアップ履歴は、スケジュールまたはオンデマンドバックアップに関する基本情報です。バックアップ履歴には、バックアップ名、バックアップ ファイルのサイズ、バックアップが保存されているリポジトリ、バックアップが取られたタイム スタンプを表示します。この情報は、操作監査レポートまたは、履歴テーブルの [バックアップ/復元（Backup and Restore）] ページから入手できます。

バックアップが失敗すると、Cisco ISE がアラームをトリガーします。バックアップ履歴ページに失敗の原因が表示されます。障害の原因は操作監査レポートにも記載されます。障害の原因が欠落しているか明確でない場合は、Cisco ISE CLI から **backup-logs** コマンドを実行し、ADE.log でより詳細な情報を確認できます。

バックアップ操作の実行中は、**show backup status** CLI コマンドを使用して、バックアップ操作の進行状況を確認することができます。

バックアップ履歴は、Cisco ADE オペレーティング システムの設定データとともに保存されています。つまり、アプリケーションのアップグレード後もそこに残っており、PAN のイメージを再作成した場合にのみ削除されます。

バックアップの失敗

バックアップが失敗した場合は、次を確認してください。

- NTP 同期またはサービス障害の問題があるかどうかを確認します。Cisco ISE の NTP サービスが動作していない場合、Cisco ISE では、[NTPサービスの障害（NTP Service Failure）] のアラームが発生します。Cisco ISE が、設定されているすべての NTP サーバーと同期できない場合、Cisco ISE では、[NTP同期に失敗（NTP Sync Failure）] のアラームが発生します。NTP サービスがダウンしている場合、または同期の問題がある場合は、Cisco ISE のバックアップが失敗する可能性があります。バックアップ操作を再試行する前に、[アラーム（Alarm）] ダッシュレットを確認し、NTP 同期またはサービスの問題を修正してください。
- 他のバックアップが同時に実行されていないことを確認します。
- 設定したリポジトリの使用可能なディスク領域を確認します。
  - （操作）バックアップのモニタリングは、モニタリング データがモニタリング データベースに割り当てられたサイズの 75% を超えると失敗します。たとえばモニタリング ノードに 600 GB 割り当てられており、モニタリング データがストレージの 450 GB を超える領域を消費すると、モニタリングのバックアップは失敗します。
  - データベースのディスク使用量が 90% を超える場合、消去が発生してデータベースを割り当てられたサイズの 75% 以下のサイズにします。
- 消去が進行中かどうかを確認します。消去の進行中はバックアップ/復元操作は動作しません。
- リポジトリが正しく設定されていることを確認します。

Cisco ISE 復元操作

プライマリまたはスタンドアロン 管理ノードで設定データを復元できます。プライマリ PAN にデータを復元したら、手動でセカンダリ ノードをプライマリ PAN と同期する必要があります。

運用データを復元するプロセスは、展開のタイプによって異なります。

（注） Cisco ISE の新しいバックアップ/復元ユーザー インターフェイスでは、バックアップ ファイル名にメタデータが使用されます。したがって、バックアップが完了後に、バックアップ ファイル名を手動で変更しないでください。バックアップ ファイルの名前を手動で変更すると、Cisco ISE バックアップ/復元ユーザー インターフェイスがそのバックアップ ファイルを認識できなくなります。バックアップ ファイル名を変更しなければならない場合は、バックアップの復元に Cisco ISE CLI を使用する必要があります。

データの復元に関するガイドライン

（注）
- Cisco ISE リリース 3.2 以降では、ルート CA の再生成は復元フローで自動的に行われます。したがって、構成バックアップ後のルート CA の再生成は必要ありません。

次は、Cisco ISE バックアップ データを復元する場合に従うべきガイドラインです。

- Cisco ISE では、ある ISE ノード（A）からバックアップを取得して、別の ISE ノード（B）に復元することができます。両方のノードは同じホスト名（IP アドレスは異なる）です。ただし、ノード B 上のバックアップを復元した後は、証明書とポータル グループ タグの問題が生じる可能性があるため、ノード B のホスト名を変更することはできません。
- あるタイムゾーン内のプライマリ PAN からバックアップを取得して、別のタイムゾーン内の別の Cisco ISE ノードに復元する場合、復元プロセスが失敗することがあります。この問題は、バックアップ ファイルのタイムスタンプが、バックアップが復元される Cisco ISE ノードのシステム時刻より新しい場合に発生します。同じバックアップを、取得後 1 日経過してから復元すると、バックアップ ファイルのタイムスタンプが過去のものになり、復元プロセスは成功します。
- バックアップを取得したホスト名と別のホスト名を持つプライマリ PAN にバックアップを復元すると、プライマリ PAN はスタンドアロン ノードになります。展開が切断し、セカンダリ ノードは機能しなくなります。スタンドアロン ノードをプライマリ ノードにし、セカンダリ ノードの設定をリセットしてプライマリ ノードに再登録する必要があります。Cisco ISE ノードの設定をリセットするには、Cisco ISE CLI から次のコマンドを入力してください。
  - **application reset-config ise**
- システムのタイムゾーンは、最初の Cisco ISE インストールおよびセットアップ後に変更しないことを推奨します。
- 展開の 1 つ以上のノードの証明書設定を変更した場合は、データを復元するための別のバックアップをスタンドアロン Cisco ISE ノードまたはプライマリ PAN から取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。

- プライマリ PAN 上で設定バックアップを復元した後に、以前にエクスポートした Cisco ISE CA 証明書およびキーをインポートできます。

（注） Cisco ISE CA 証明書およびキーをエクスポートしなかった場合は、プライマリ PAN 上で設定バックアップを復元した後に、プライマリ PAN およびポリシー サービス ノード（PSN）でルート CA および下位 CA を生成します。

- 適切な FQDN（プラチナ データベースの FQDN）を使用せずにプラチナ データベースを復元する場合は、CA 証明書を再生成する必要があります。（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）] > [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA certificate chain）]**）。ただし、適切な FQDN でプラチナ データベースを復元する場合は、CA 証明書が自動的に再生成されます。
- Cisco ISE がバックアップ ファイルを格納するデータ リポジトリが必要です。オンデマンドまたはスケジュール設定されたバックアップを実行する前に、リポジトリを作成する必要があります。
- スタンドアロン管理ノードに障害が発生した場合、設定バックアップを実行して復元する必要があります。プライマリ PAN で障害が発生した場合、分散セットアップを使用してセカンダリ管理ノードをプライマリに昇格できます。その後、新しいプライマリ PAN にデータを復元できます。

（注） Cisco ISE では、**backup-logs** CLI コマンドも使用できます。このコマンドを使用して、ログやコンフィギュレーションファイルの収集を行い、これらをトラブルシューティングに利用できます。

CLI からの設定またはモニタリング（操作）バックアップの復元

Cisco ISE CLI から設定データを復元するには、EXEC モードで **restore** コマンドを使用します。設定または操作バックアップからデータを復元するには、次のコマンドを使用します。

restore *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

構文の説明

restore	設定または操作バックアップからデータを復元するには、このコマンドを入力します。

filename	リポジトリに存在するバックアップファイルのファイル名。最大120文字の英数字をサポートします。 （注） ファイル名の後に、tar.gpg という拡張子を付ける必要があります（myfile.tar.gpg など）。
repository	バックアップを含むリポジトリを指定します。
repository-name	バックアップを復元するリポジトリの名前。
encryption-key	（オプション）バックアップを復元するユーザー定義の暗号キーを指定します。
hash	バックアップを復元するためのハッシュされた暗号キー。使用する暗号化された（ハッシュ化された）暗号化キーを指定します。40文字までで指定します。
plain	バックアップを復元するためのプレーンテキストの暗号キー。使用する暗号化されたプレーンテキストの暗号化キーを指定します。15文字までで指定します。
encryption-key name	暗号キーを入力します。
include-adeos	（オプション、設定バックアップのみに該当）設定バックアップから ADE-OS 設定を復元する場合に、このコマンド オペレータ パラメータを入力します。設定バックアップを復元する場合にこのパラメータを含めないと、Cisco ISE は Cisco ISE アプリケーション設定データのみを復元します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

使用上のガイドライン

Cisco ISE で restore コマンドを使用すると、Cisco ISE サーバーが自動的に再起動します。

データの復元処理で、暗号キーはオプションです。暗号キーを指定しなかった以前のバックアップの復元をサポートするために、暗号キーなしで **restore** コマンドを使用できます。

例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
```

```
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

関連コマンド

	説明
backup	バックアップ（Cisco ISE と Cisco ADE OS）を実行して、そのバックアップをリポジトリに保存します。
backup-logs	システム ログをバックアップします。
repository	バックアップ設定のリポジトリ サブモードを入力します。
show repository	特定のリポジトリにある使用可能なバックアップ ファイルを表示します。
show backup history	システムのバックアップ履歴を表示します。
show backup status	バックアップ操作のステータスを表示します。
show restore status	復元操作のステータスを表示します。

いずれかのセカンダリ ノードでアプリケーション復元後の同期ステータスおよび複製ステータスが [非同期（Out of Sync）] になっている場合、該当セカンダリ ノードの証明書をプライマリ PAN に再インポートして、手動同期を実行する必要があります。

GUI からの設定バックアップの復元

管理者ポータルで設定バックアップを復元できます。

始める前に

プライマリ PAN の自動フェールオーバー構成が展開で有効になっている場合はオフにします。設定バックアップを復元すると、アプリケーション サーバー プロセスが再起動されます。こ

れらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ PAN の自動フェールオーバーが開始される場合があります。

構成のバックアップ時に展開がデュアルノード展開の場合は、次のことを確認します。

- 復元のソースノードとターゲットノードは、構成のバックアップに使用されたものと同じで、ターゲットノードはスタンドアロンまたはプライマリのいずれかです。
- 復元のソースノードとターゲットノードは、構成のバックアップで使用されたものとは異なり、ターゲットノードはスタンドアロンである必要があります。

（注） 構成データベースのバックアップを復元し、プライマリ PAN でのみルート CA を再生成することができます。ただし、登録済みの PAN でコンフィギュレーション データベースのバックアップは復元できません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup and Restore）]**。

ステップ 2 バックアップの名前を設定バックアップのリストから選択し、[復元（Restore）] をクリックします。

ステップ 3 バックアップ時に使用した暗号キーを入力します。

ステップ 4 [復元（Restore）] をクリックします。

次のタスク

Cisco ISE CA サービスを使用する場合は、次のことを実行する必要があります。

1. Cisco ISE CA ルート チェーン全体を再生成します。
2. Cisco ISE CA 証明書およびキーのバックアップをプライマリ PAN から取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN が外部 PKI のルート CA または下位 CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

モニタリング データベースの復元

モニタリングデータベースを復元するプロセスは、展開のタイプによって異なります。次の項では、スタンドアロンおよび分散展開でモニタリングデータベースを復元する方法について説明します。

Cisco ISE の以前のリリースからのオンデマンド モニタリング データベースのバックアップを復元するには、CLI を使用する必要があります。Cisco ISE リリース間でのスケジュール バックアップの復元はサポートされていません。

（注） データが取得されたノードとは別のノードにデータを復元しようとする場合、新しいノードを指すロギング ターゲット設定を設定する必要があります。これにより、モニタリング syslog が正しいノードに送信されるようになります。

スタンドアロン環境でのモニタリング（運用）バックアップの復元

GUIには現在のリリースから取得されたバックアップのみが表示されます。前のリリースから取得されたバックアップを復元するには、CLI から restore コマンドを使用します。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup and Restore）]** を選択します。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup and Restore）]**。

ステップ 3 バックアップの名前を操作バックアップのリストから選択し、[復元（Restore）] をクリックします。

ステップ 4 バックアップ時に使用した暗号キーを入力します。

ステップ 5 [復元（Restore）] をクリックします。

管理およびモニタリングペルソナによるモニタリング バックアップの復元

管理およびモニタリングペルソナを使用して、分散環境でのモニタリングバックアップを復元することができます。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 プライマリとセカンダリ PAN を使用している場合は、PAN と同期します。

PAN と同期する場合、PAN を選択し、それをアクティブなプライマリに昇格させる必要があります。

ステップ 2 モニタリング ノードを登録解除する前に、モニタリング ペルソナを展開内の別のノードに割り当てます。

展開ごとに、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 3 バックアップするモニタリングノードを登録解除します。
ステップ 4 新しく登録解除されたノードにモニタリング バックアップを復元します。
ステップ 5 現在の管理ノードにより新たに復元されたノードを登録します。
ステップ 6 新たに復元されて登録されたノードをアクティブなモニタリング ノードに昇格します。

モニタリング ペルソナによるモニタリング バックアップの復元

分散環境のモニタリングバックアップは、モニタリングペルソナによってのみ復元できます。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 復元されるノードの登録を解除する準備をします。これを行うには、モニタリングペルソナを展開内の別のノードに割り当てます。

展開内に、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 2 復元されるノードを登録解除します。

（注） 登録解除が完了するのを待機してから、復元に進みます。復元を続行する前に、ノードがスタンドアロン状態になっている必要があります。

ステップ 3 新しく登録解除されたノードにモニタリング バックアップを復元します。
ステップ 4 現在の管理ノードにより新たに復元されたノードを登録します。
ステップ 5 新たに復元されて登録されたノードをアクティブなモニタリング ノードに昇格します。

復元履歴

[操作監査レポート（Operations Audit Report）] ウィンドウから、すべての復元操作、ログイベント、ステータスに関する情報を取得できます。

（注） ただし [操作監査レポート（Operations Audit Report）] には、前回の復元操作に対応する開始時間に関する情報はありません。

トラブルシューティング情報を入手するには、Cisco ISE CLI から **backup-logs** コマンドを実行して、ADE.log ファイルを調べる必要があります。

復元操作の進行中は、すべての Cisco ISE サービスは停止します。**show restore status** CLI コマンドを使用して、復元操作の進行状況を確認できます。

認証および許可ポリシー設定のエクスポート

認証および許可ポリシー設定を XML ファイルの形式でエクスポートし、これをオフラインで読み取って設定エラーを特定し、トラブルシューティングのために使用できます。この XML ファイルには認証および許可ポリシールール、単純および複合ポリシー条件、任意アクセス制御リスト（DACL）、および認証プロファイルが含まれます。XML ファイルを電子メールで送信するか、ローカル システムに保存することを選択できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup & Restore）]**。

ステップ 2 [ポリシーのエクスポート（Policy Export）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [エクスポート（Export）] をクリックします。

XML ファイルの内容を表示するには、ワードパッドなどのテキスト エディタを使用します。

ポリシーのエクスポート設定のスケジュール

次の表では、[ポリシーのエクスポートのスケジュール（Schedule Policy Export）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]>[システム（System）]> [バックアップ/復元（Backup and Restore）] > [ポリシーのエクスポート（Policy Export）]** です。

表 *45 :* ポリシーのエクスポート設定のスケジュール

フィールド名	使用上のガイドライン
暗号化（Encryption）	
暗号キー（Encryption Key）	エクスポートデータを暗号化および復号化するためのキーを入力します。このフィールドは、[暗号キーを使用したエクスポート（Export with Encryption Key）] オプションを選択した場合にのみ有効になります。
宛先（Destination）	
ローカル コンピュータにファイルをダウンロード（Download file to local computer）	ポリシー エクスポート ファイルをローカル システムにダウンロードできます。

フィールド名	使用上のガイドライン
ファイルをメールで送信（**Email file to**）	複数の電子メールアドレスは、カンマで区切ることで入力できます。
リポジトリ（**Repository**）	ポリシーデータをエクスポートするリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウンリストから利用可能なリポジトリのみを選択できます。ポリシーのエクスポートのスケジュールを設定する前に、リポジトリを作成してください。
今すぐエクスポート（**Export Now**）	データをローカルコンピュータにエクスポートするか、電子メールの添付ファイルとして送信するには、このオプションをクリックします。リポジトリにエクスポートすることはできません。リポジトリのエクスポートのみをスケジュールできます。
スケジュール（**Schedule**）	
スケジューリングオプション（**Schedule Options**）	エクスポートのスケジュールの頻度を選択し、それに応じてその他の詳細を入力します。

分散環境でのプライマリノードとセカンダリノードの同期

分散環境では、PANのバックアップファイルの復元後に、プライマリおよびセカンダリノードの Cisco ISE データベースが自動的に同期されないことがあります。この場合には、PAN からセカンダリ ISE ノードへの完全複製を手動で強制実行できます。強制同期は、PANからセカンダリ ノードにのみ可能です。同期操作中は、設定を変更することはできません。Cisco ISE では、同期が完全に完了した後にのみ、他の Cisco ISE 管理者ポータル ページに移動して設定変更を行うことができます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。

ステップ 2 非同期レプリケーション ステータスのセカンダリ ISE ノードの横にあるチェックボックスをオンにします。

ステップ 3 [同期を更新（Syncup）] をクリックし、ノードが PAN と同期されるまで待ちます。Cisco ISE 管理者ポータルへのアクセスは、このプロセスが完了するのを待たなければなりません。

スタンドアロンおよび分散展開での失われたノードの復元

この項では、スタンドアロンおよび分散展開での失われたノードの復元に使用できるトラブルシューティング情報を提供します。次の使用例の一部では、失われたデータの復旧にバックアップと復元機能を使用し、その他の使用例では、複製機能を使用しています。

分散展開での既存IPアドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。復元後に、既存 IP アドレスとホストネームを使用します。

たとえば、2 つのノード、N1（プライマリ ポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリ ポリシー管理ノードすなわちセカンダリ PAN）があります。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。

前提

展開内のすべての Cisco ISE ノードが破壊されました。同じホスト名と IP アドレスを使用して、新しいハードウェアのイメージが作成されました。

解決手順

1. N1 および N2 ノードの両方を置き換える必要があります。N1 および N2 ノードはスタンドアロン構成になりました。
2. N1 と N2 のノードの UDI を使用してライセンスを取得し、N1 ノードにインストールします。
3. 置き換えた N1 ノードでバックアップを復元する必要があります。復元スクリプトは N2 にデータを同期しようとしますが、N2 はスタンドアロン ノードであるため同期は失敗します。N1 のデータは時刻 T1 にリセットされます。
4. N1 の管理者ポータルにログインして、N2 ノードを削除して再登録する必要があります。これで、N1 および N2 ノードのデータが時刻 T1 にリセットされます。

分散展開の新IPアドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。新しいハードウェアのイメージが新しい場所で再作成され、新しい IP アドレスとホスト名が必要です。

たとえば、2 つの ISE、ノード N1（プライマリポリシー管理ノード（プライマリ PAN））と N2（セカンダリ ポリシー サービス ノード）があるとします。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。Cisco ISE ノードが新しいロケーションで置き換えられ、新しいホスト名は N1A（プライマリ PAN）および N2A（セカンダリ ポリシー サービス ノード）です。N1A および N2A はこの時点ではスタンドアロン ノードです。

前提条件

展開内のすべての Cisco ISE ノードが破壊されました。新しいハードウェアのイメージが、異なるホスト名と IP アドレスを使用して異なる場所で作成されました。

解決手順

1. N1 のバックアップを入手し、これを N1A 上で復元します。復元スクリプトは、ホスト名とドメイン名の変更を認識し、現在のホスト名に基づいて展開設定内のホスト名とドメイン名を更新します。
2. 新しい自己署名証明書を生成する必要があります。
3. N1A の Cisco ISE 管理者ポータルにログインする必要があります。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択して、次の操作を行う必要があります。

   古い N2 ノードを削除します。

   新しい N2A ノードをセカンダリ ノードとして登録します。N1A ノードのデータが N2A ノードに複製されます。

スタンドアロン展開の既存IPアドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノードN1があったとします。N1データベースのバックアップは、時刻 T1 に取得されました。物理的な障害により N1 ノードがダウンし、イメージの再作

成または新しいハードウェアが必要です。N1 ノードを、同じ IP アドレスとホスト名を使用して回復させる必要があります。

前提条件

この展開はスタンドアロン展開であり、新規またはイメージを再作成したハードウェアは、同じ IP アドレスとホスト名を持ちます。

解決手順

イメージの再作成後、または同一 IP アドレスとホスト名で新しい Cisco ISE ノードを導入した後に N1 ノードが起動したら、古い N1 ノードから取得したバックアップを復元する必要があります。ロールを変更する必要はありません。

スタンドアロン展開の新 IP アドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノード N1 があったとします。時刻 T1 に取得された N1 データベースのバックアップが利用可能です。物理的な障害により N1 ノードがダウンし、異なる IP アドレスとホスト名を使用した新しいハードウェアに別のロケーションで置き換えられます。

前提条件

これはスタンドアロン展開であり、置き換えられたハードウェアは、異なる IP アドレスとホスト名を持ちます。

解決手順

1. 新しいハードウェアで N1 ノードを置き換えます。このノードはスタンドアロン状態となり、ホスト名は N1B です。
2. バックアップを N1B ノード上で復元できます。ロールを変更する必要はありません。

設定のロール バック

問題

意図せずに設定を変更してしまい、後でそれが正しくないことがわかる場合があります。たとえば、いくつかの NAD を削除したり、一部の RADIUS 属性を誤って修正したりして、数時間後にこの問題に気付く場合があります。この場合、変更を行う前に取得したバックアップを復元することにより、元の構成に戻すことができます。

考えられる原因

N1（プライマリポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリポリシー管理ノードすなわちセカンダリ PAN）の 2 つのノードがあり、N1 ノードのバックアップを使用できます。N1 上で誤った変更をいくつか行い、変更を元に戻す必要があります。

ソリューション

誤った設定変更を行う前に取得したN1ノードのバックアップを入手します。N1ノード上でこのバックアップを復元します。復元スクリプトにより、N1 のデータで N2 が同期されます。

分散展開での障害発生時のプライマリ ノードの復元

シナリオ

マルチノード展開内で、PAN に障害が発生しました。

たとえば、2 つの Cisco ISE ノード、N1（PAN）と N2（セカンダリ管理ノード）があります。ハードウェアの問題で N1 に障害が発生します。

前提条件

分散展開内のプライマリ ノードのみに障害が発生します。

解決手順

1. N2 管理者ポータルにログインします。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]**。N2 をプライマリノードとして設定します。

   N1 ノードが新しいハードウェアで置き換えられ、イメージが再作成され、スタンドアロン状態となります。

2. N2 管理者ポータルで、セカンダリノードとして新しい N1 ノードを登録します。

   これで、N2 ノードがプライマリ ノードになり、N1 ノードがセカンダリ ノードになります。

N1 ノードを再びプライマリノードにするには、N1 の管理者ポータルにログインして、このノードをプライマリノードに設定します。N2 は、自動的にセカンダリ サーバーとなります。データが失われることはありません。

分散展開での障害発生時のセカンダリ ノードの復元

シナリオ

マルチノード展開で、1 台のセカンダリ ノードに障害が発生しました。復元の必要はありません。

たとえば、N1（プライマリ PAN）、N2（セカンダリ PAN）、N3（セカンダリ ポリシー サービス ノード）、N4（セカンダリ ポリシー サービス ノード）の複数のノードが存在します。セカンダリ ノードの 1 つである N3 に障害が発生しました。

解決手順

1. 新しいN3A ノードのイメージを再作成して、デフォルトのスタンドアロン状態にします。
2. N1 の管理者ポータルにログインし、N3 ノードを削除します。
3. N3A ノードを登録します。

   N1 から N3A へ、データが複製されます。復元の必要はありません。

Cisco ISE ロギング メカニズム

Cisco ISE には、監査、障害管理、およびトラブルシューティングに使用されるロギング メカニズムが備わっています。このロギング メカニズムは、展開されたサービスの障害状態を識別したり、問題のトラブルシューティングを効率的に行う場合に役立ちます。また、プライマリ ノードのモニタリングおよびトラブルシューティングのロギング出力が一貫した形式で生成されます。

仮想ループバック アドレスを使用してローカル システムにログを収集するように Cisco ISE ノードを設定できます。ログを外部に収集するには、ターゲットと呼ばれる外部 syslog サーバーを設定します。ログは事前定義された各種のカテゴリに分類されます。ターゲット、シビラティ（重大度）レベルなどに応じてカテゴリを編集することにより、ロギング出力をカスタマイズできます。

ベストプラクティスとして、Cisco ISE のモニタリングおよびトラブルシューティング（MnT）ノードに syslog を送信するようにネットワーク デバイスを設定しないでください。これは、一部のネットワーク アクセス デバイス（NAD）の syslog が失われる可能性があるほか、MnT サーバーが過負荷になりロードの問題が発生するためです。NAD syslog が MnT に直接送信されるように設定されている場合、セッション管理機能が停止します。NAD syslog は、トラブルシューティングのために外部 syslog サーバーに送信できますが、MnT には送信できません。

ノードで ISE メッセージング サービスに障害が発生した場合、プロセス ダウン アラームがトリガーされなくなりました。ノードで ISE メッセージング サービスに障害が発生すると、そのノードでメッセージング サービスが再開されるまで、すべての syslog およびプロセス ダウン アラームが失われます。

この場合、管理者は、Cisco ISE のホーム ウィンドウの [アラーム（Alarm）] ダッシュレットにリストされるキュー リンク エラー アラームを検索する必要があります。アラームをクリックすると、[推奨されるアクション（Suggested Actions）] セクションが含まれた新しいウィンドウが開きます。問題を解決するには、次の手順に従ってください。

（注） モニタリング ノードがネットワーク デバイスの syslog サーバーとして設定されている場合、ロギング ソースが次の形式で正しいネットワーク アクセス サーバー（NAS）の IP アドレスを送信することを確認してください。

<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

そうしないと、これは NAS の IP アドレスに依存する機能に影響を及ぼすことがあります。

syslog の消去の設定

このプロセスを使用して、ローカル ログ格納期間を設定し、特定の期間後にローカル ログを削除します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ローカルログ設定（Local Log Settings）]**。

ステップ 2 [ローカル ログ格納期間（Local Log Storage Period）] フィールドに、設定ソースでログ エントリを保持する最大日数を入力します。

localStore フォルダのサイズによっては、設定された [ローカルログの保存期間（Local Log Storage Period）] よりも前にログが削除されることがあります。

ディスクサイズ	ローカルの保存サイズ上限
100 GB 未満	10 GB
250 GB 未満	30 GB
400 GB 未満	50 GB
400 GB 超	95 GB

ステップ 3 格納期間が経過する前に既存のログ ファイルを削除するには、[今すぐログを削除（Delete Logs Now）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

Cisco ISE システム ログ

Cisco ISE では、システム ログはロギング ターゲットと呼ばれる場所で収集されます。ターゲットは、ログを収集して格納するサーバーの IP アドレスを参照します。ログをローカルで生成して格納することも、FTP ファシリティを使用して外部サーバーに転送することもできま

す。Cisco ISE には、次のデフォルト ターゲットがあり、これらはローカル システムのループバック アドレスに動的に設定されます。

- LogCollector：ログ コレクタのデフォルトの syslog ターゲット。
- ProfilerRadiusProbe：プロファイラ Radius プローブのデフォルトの syslog ターゲット。

デフォルトでは、AAA 診断サブカテゴリとシステム診断サブカテゴリのロギング ターゲットは、ディスク領域を減らすために、新規 Cisco ISE インストールまたはアップグレード時に無効になります。これらのサブカテゴリのロギング ターゲットを手動で設定できますが、これらのサブカテゴリのローカル ロギングは常に有効です。

Cisco ISE インストールの最後にローカルに設定されるデフォルトのロギング ターゲットを使用するか、またはログを保存する外部ターゲットを作成することができます。

（注） syslog サーバーが分散展開で設定されている場合、syslog メッセージは MnT ノードではなく認証 PSN から syslog サーバーへ直接送信されます。

関連トピック

Cisco ISE メッセージ コード （712 ページ）

リモート syslog 収集場所の設定

Web インターフェイスを使用して、システム ログ メッセージの送信先になるリモート syslog サーバー ターゲットを作成できます。ログ メッセージは、syslog プロトコル標準（RFC-3164 を参照）に従ってリモート syslog サーバー ターゲットに送信されます。syslog プロトコルはセキュアでない UDP です。

メッセージは、イベントが発生したときに生成されます。イベントは、プログラムの終了時に表示されるメッセージやアラームなどのステータスを表示するものである場合があります。カーネル、メール、ユーザーレベルなど、異なるファシリティから生成されたさまざまなタイプのイベントメッセージがあります。イベントメッセージはシビラティ（重大度）レベルに関連付けられており、管理者はメッセージをフィルタリングし、優先度付けできます。数値コードはファシリティおよびシビラティ（重大度）レベルに割り当てられます。syslog サーバーはイベント メッセージ コレクタで、これらのファシリティからイベント メッセージを収集します。管理者は、シビラティ（重大度）レベルに基づいて、メッセージを転送するイベントメッセージコレクタを選択できます。

UDP syslog（ログ コレクタ）はデフォルトのリモート ロギング ターゲットです。このロギングターゲットを無効にした場合、ログコレクタとして動作しなくなり、[ロギングカテゴリ（Logging Categories）] ウィンドウから削除されます。このロギングターゲットを有効にした場合は、[ロギングカテゴリ（Logging Categories）] ウィンドウのログコレクタになります。

（注） デフォルトのリモートロギングターゲット SecureSyslogCollector を変更すると、Cisco ISE Monitoring & Troubleshooting Log Processor サービスが再起動されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 次の必須詳細情報を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リモート ロギング ターゲット（Remote Logging Targets）] ページに移動し、新しいターゲットが作成されたことを確認します。

その後、ロギングターゲットを、以下のそれぞれのロギングカテゴリにマッピングできます。PSN ノードは、それらのノードで有効になっているサービスに応じて、該当するログをリモートロギングターゲットに送信します。

- AAA 監査
- AAA の診断
- アカウンティング
- 外部 MDM
- パッシブ ID
- ポスチャおよびクライアント プロビジョニングの監査
- ポスチャおよびクライアント プロビジョニングの診断
- プロファイラ

展開内のすべてのノードによって、次のカテゴリのログがロギング ターゲットに送信されます。

- 管理および操作の監査
- システム診断
- システム統計

Cisco ISE メッセージ コード

ロギング カテゴリは、ACS の機能、フロー、または使用例を説明するメッセージ コードのバンドルです。Cisco ISE では、各ログにはログ メッセージの内容に従ってロギング カテゴリにバンドルされているメッセージ コードが関連付けられています。ロギング カテゴリは、含まれているメッセージの内容を説明する場合に役立ちます。

ロギング カテゴリはロギング設定で役立ちます。各カテゴリには、アプリケーションの要件に応じて設定可能な名前、ターゲット、およびシビラティ（重大度）レベルがあります。

Cisco ISE では、サービスに対して事前定義されたロギング カテゴリ（[ポスチャ（Posture）]、[プロファイラ（Profiler）]、[ゲスト（Guest）]、[AAA（認証、許可、アカウンティング）（AAA (authentication, authorization, and accounting)）] など）が提供されており、これらにログ ターゲットを割り当てることができます。

ロギングカテゴリが [成功した認証（Passed Authentications）] の場合、ローカルロギングを許可するオプションは、デフォルトでは無効になっています。このカテゴリのローカルロギングを有効にすると、運用スペースの使用率が高くなり、iseLocalStore.log とともに prrt-server.log がいっぱいになります。

[成功した認証（Passed Authentications）] のローカルロギングを有効にする場合は、**[管理（Administration）] > [システム（System）] > [ロギング（logging）] > [ロギングカテゴリ（logging Categories）]** に移動し、[カテゴリ（category）] セクションから [成功した認証（Passed Authentications）] をクリックして、[ローカルロギング（Local Logging）] のチェックボックスをオンにします。

関連トピック

メッセージ コードのシビラティ（重大度）レベルの設定 （712 ページ）

メッセージ コードのシビラティ（重大度）レベルの設定

ログのシビラティ（重大度）レベルを設定し、選択したカテゴリのログが格納されるロギング ターゲットを選択できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]**。

ステップ 2 編集するカテゴリの隣のオプション ボタンをクリックにして、[編集（Edit）] をクリックします。

ステップ 3 必須フィールドの値を変更します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [ロギング カテゴリ（Logging Categories）] ページに移動し、特定のカテゴリに対して行われた設定の変更内容を確認します。

Cisco ISE メッセージ カタログ

可能性があるすべてのログメッセージと説明を表示するために、[メッセージカタログ（Message Catalog）] ページを使用できます。**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[メッセージカタログ（Message Catalog）]** を選択します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[メッセージカタログ（Message Catalog）]** を選択します。

[ログ メッセージ カタログ（Log Message Catalog）] ページが表示されます。このページでは、ログ ファイルに記録される可能性があるすべてのログ メッセージを表示できます。すべての Syslog メッセージを CSV ファイル形式でエクスポートするには、[エクスポート（Export）] を選択します。

Cisco ISE から送信される syslog メッセージの包括的なリスト、syslog メッセージの意味、ローカルおよびリモートターゲットでの syslog メッセージの記録方法については、『Cisco ISE Syslogs』ドキュメントを参照してください。

エンドポイントのデバッグ ログ コレクタ

特定のエンドポイントの問題をトラブルシューティングするために、IP アドレスまたは MAC アドレスに基づいて、特定のエンドポイントのデバッグ ログをダウンロードできます。その特定のエンドポイント固有のログが、展開内のさまざまなノードから 1 つのファイルに収集されるため、迅速かつ効率的に問題をトラブルシューティングできます。このトラブルシューティング ツールは、一度に 1 つのエンドポイントに対してのみ実行できます。ログ ファイルが GUI に表示されます。1 つのノードまたは展開内のすべてのノードからエンドポイントのログをダウンロードできます。

特定のエンドポイントのデバッグ ログのダウンロード

ネットワーク内の特定のエンドポイントの問題をトラブルシューティングするには、管理者ポータルからデバッグ エンドポイント ツールを使用できます。または、このツールを [認証（Authentications）] ページから実行できます。[認証（Authentications）] ページの [エンドポイント ID（Endpoint ID）] を右クリックして、[エンドポイント デバッグ（Endpoint Debug）] をクリックします。このツールでは、単一ファイルの特定のエンドポイントに関連するすべてのサービスに関するすべてのデバッグ情報が提供されます。

始める前に

デバッグ ログを収集するエンドポイントの IP アドレスまたは MAC アドレスが必要です。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般ツール（General Tools）]** > **[エンドポイントデバッグ（Endpoint Debug）]**。

ステップ 2 [MAC アドレス（MAC Address）] または [IP] オプション ボタンをクリックし、エンドポイントの MAC または IP アドレスを入力します。

ステップ 3 一定の時間が経過した後にログ収集を停止する場合は、[*n* 分後に自動的に無効化（Automatic disable after n Minutes）] チェックボックスをオンにします。このチェックボックスをオンにする場合は、1 ～ 60 分の時間を入力する必要があります。

次のメッセージが表示されます。「エンドポイントデバッグによって、展開のパフォーマンスが低下します。続行しますか?（Endpoint Debug degrades the deployment performance. Would you like to continue?）」

ステップ 4 ログを収集するには、[続行（Continue）] をクリックします。

ステップ 5 手動でログの収集を中止する場合は、[停止（Stop）] をクリックします。

関連トピック

エンドポイントのデバッグ ログ コレクタ （713 ページ）

収集フィルタ

収集フィルタを設定して、モニタリング サーバーおよび外部サーバーに送信される syslog メッセージを抑制できます。抑制は、異なる属性タイプに基づいてポリシー サービス ノード レベルで実行できます。特定の属性タイプおよび対応する値を使用して複数のフィルタを定義できます。

モニタリング ノードまたは外部サーバーに syslog メッセージを送信する前に、Cisco ISE は送信する syslog メッセージのフィールドとそれらの値を比較します。一致が見つかった場合、対応するメッセージは送信されません。

（注） 任意の [属性（Attribute）] および [ファイルタイプ（Filter Type）] に対して収集フィルタ（**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[収集フィルタ（Collection Filter）]**）を設定していて、[非アクティブになってからn日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックス（**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[ユーザー認証の設定（User Authentication Settings）]** > **[アカウントの無効化ポリシー（Disable Account Policy）]**）をオンにしている場合、認証成功の syslog メッセージがモニタリングノードにリレーされない結果、アカウントが無効になる可能性があります。

収集フィルタの設定

さまざまな属性のタイプに基づいて複数の収集フィルタを設定できます。フィルタ数を 20 に制限することを推奨します。収集フィルタを追加、編集、または削除できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[収集フィルタ（Collection Filters）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 次のリストから**フィルタ タイプ**を選択します。

- ユーザー名（User Name）
- MACアドレス（MAC Address）
- ポリシーセット名（Policy Set Name）
- NAS IPアドレス（NAS IP Address）
- デバイスIPアドレス（Device IP Address）

ステップ 4 選択したフィルタ タイプの対応する**値**を入力します。

ステップ 5 ドロップダウン リストから**結果**を選択します。結果は、[すべて（All）]、[成功（Passed）]、または [失敗（Failed）] になります。

ステップ 6 [送信（Submit）] をクリックします。

関連トピック

収集フィルタ （714 ページ）
イベント抑制バイパス フィルタ （715 ページ）

イベント抑制バイパス フィルタ

Cisco ISE では、フィルタを設定し、収集フィルタを使用して、一部の syslog メッセージがモニタリング ノードおよび他の外部サーバーに送信されることを抑制できます。場合によっては、これらの抑制されたログ メッセージにアクセスすることが必要になります。Cisco ISE は、設定可能な時間について、ユーザー名などの属性に基づいてイベント抑制をバイパスするオプションを提供します。デフォルトは 50 分ですが、5 分から 480 分（8 時間）の期間を設定できます。イベント抑制バイパスは、設定した後すぐに有効になります。設定した期間が経過すると、バイパス抑制フィルタは失効します。

抑制バイパス フィルタは、Cisco ISE ユーザー インターフェイスの [収集フィルタ（Collection Filters）] ページから設定できます。この機能を使用して、特定の ID（ユーザー）のすべてのログを表示し、その ID の問題をリアルタイムでトラブルシューティングできます。

フィルタは有効または無効にできます。バイパス イベント フィルタで設定した期間が経過すると、フィルタは再度有効にするまで自動的に無効になります。Cisco ISE は設定変更監査レ

ポートでこれらの設定変更を取得します。このレポートは、イベント抑制またはバイパス抑制を設定したユーザー、およびイベントが抑制された期間または抑制がバイパスされた期間に関する情報を提供します。

システム 360

システム 360 には、[モニタリング（Monitoring）] と [Log Analytics] が含まれています。

[モニタリング（Monitoring）] 機能を使用すると、一元化されたコンソールから、展開内のすべてのノードの幅広いアプリケーションとシステム統計、および主要業績評価指標（KPI）を監視できます。KPI は、ノード環境の全体的な状態を把握するのに役立ちます。統計は、システム構成と使用率固有のデータを簡略化して表示します。詳細については、モニタリング（716 ページ）を参照してください。

ログ分析は、エンドポイントの認証、許可、およびアカウンティング（AAA）とプロファイリング syslog データを詳細に分析するための柔軟な分析システムを提供します。Cisco ISE の正常性サマリーとプロセスステータスを分析することもできます。Cisco ISE カウンタおよび正常性サマリーレポートと同様のレポートを生成できます。詳細については、Log Analytics（719 ページ）を参照してください。

モニタリング

Cisco ISE 3.2 以降のリリースは、Grafana および Prometheus と統合されています。Grafana は、サードパーティのメトリクスダッシュボードおよびグラフエディタです。これは、Prometheus データベースで収集された統計とカウンタをグラフィックまたはテキストベースで表示します。Prometheus は、KPI を時系列形式で格納するためのデータストアとして使用されます。Grafana の詳細については、Grafana のドキュメントを参照してください。

Grafana ダッシュボードは、システムメトリックを分析し、情報に基づいた意思決定を行うのに役立つ、量的および質的データの包括的なセットを表示します。カスタマイズされた Grafana ダッシュボードを作成して、必要なシステムメトリックを分析および監視できます。Cisco ISE でカスタマイズされた Grafana ダッシュボードを作成するには、**[操作（Operations）] > [システム360（System 360）] > [モニタリング（Monitoring）]** を選択します。

Prometheus データソースから必要なデータを取得するため、組み込みクエリまたはカスタムクエリを使用できます。Grafana ダッシュボードを作成しながら、新しいダッシュボードパネルを追加し、Prometheus データの取得に使用するクエリを [クエリ（Queries）] タブで指定できます。Prometheus クエリ形式については、Prometheus のドキュメントを参照してください。

Grafana と Prometheus は、PAN ノードにのみインストールされます。ただし、ノードエクスポータはすべてのノード（PAN、PSN、および MnT）で実行され、システムメトリックを収集します。Prometheus は、このデータを定期的に取得して、必要な KPI を取得します。KPI は 5 秒ごとに収集され、Prometheus データベースに保存されます。このデータは、ダッシュボードに入力するために Grafana によってアクセスされます。

ノードエクスポータは、次の KPI を収集します。

- CPU：全体の CPU 使用率
- Diskstats：HDD および SSD ディスクの統計
- Loadavg：定義された期間のノードのシステム負荷
- Filefd：使用中のファイル記述子の数（ファイル記述子の統計は /proc/sys/fs/file-nr から取得されます）
- Filesystem：ノードストレージに保存されているファイルのコレクション
- Meminfo：RAM 使用状況の統計
- Netclass：インターフェイスクラス
- Netstat：ネットワークレベルのノード統計
- Netdev：ネットワークデバイス数
- Uname：システム名、リリース、バージョン、マシン、ノード、およびドメイン名の組み合わせ
- Stat：システムカーネル統計
- Time：システム時刻

KPI の詳細については、Prometheus のドキュメントを参照してください。

このデータは、Prometheus データベースに 7 日間保持されます。

モニタリングサービスはデフォルトで有効になっています。このサービスは、**[操作（Operations）] > [システム360（System 360）] > [設定（Settings）]** ウィンドウから無効にできます。

サポートバンドルのモニタリング関連のログを表示するには、サポートバンドルの生成中に [デバッグログを含める（Include Debug Logs）] チェックボックスをオンにします。Grafana、Prometheus、およびノードエクスポータのログを表示するには、[操作（Operations）]>[トラブルシューティング（Troubleshoot）]>[ログのダウンロード（Download Logs）] を選択します。[アプライアンスノードリスト（Appliance Node List）] からノードを選択し、[デバッグログ（Debug Logs）] をクリックします。

（注）
- Grafana ダッシュボードにはロールベースのアクセス制御がないことに注意してください。Grafana ダッシュボードにアクセスするすべてのユーザーには、管理者権限が付与されます。
- Grafana ダッシュボードに表示される **[サインイン（Sign in）]** オプションを使用して Grafana にサインインすることはできません。**[サインイン（Sign in）]** オプションをクリックしてから **[モニタリング（Monitoring）]** ウィンドウに戻るには、**[操作（Operations）] > [システム360（System 360）] > [モニタリング（Monitoring）]** を選択します。

Grafana でのクエリの実行

Grafana は、1 つ以上のクエリで取得されたデータを視覚化するパネルを表示します。ダッシュボードから定型クエリとカスタムクエリを実行できます。定型クエリは、構文が定義された状態でダッシュボードに事前に存在します。カスタムクエリを使用すると、特定の情報を返すクエリを作成できます。

ステップ 1 [操作（Operations）] > [システム360（System 360）] > [モニタリング（Monitoring）] を選択します。

ステップ 2 左側のペインで、[エクスプローラ（Explore）] アイコンをクリックします。

ステップ 3 [エクスプローラ（Explore）] ペインで、データソースとして [Prometheus] を選択します。

ステップ 4 次のいずれかを実行します。

- 組み込みのクエリを実行するには、[メトリックブラウザ（Metrics Browser）] ドロップダウンリストで、実行するクエリを選択します。
- カスタムクエリを実行するには、[メトリックブラウザ（Metrics Browser）] の隣のフィールドにクエリを入力します。

  ノードエクスポータによって収集されたデータを取得するには、文字列「node_」で始まる定義済みクエリを使用できます。たとえば、ネットワークの詳細を表示する場合は、[メトリックブラウザ（Metrics Browser）] ドロップダウンリストから node_network_info を選択できます。

ステップ 5 [クエリの実行（Run Query）] をクリックします。

このクエリは、Prometheus データベースから情報を取得し、それをグラフィック表現で表示します。

ダッシュボードを表示しているときに、[ホスト（Host）] ドロップダウンリストからメトリックを表示するノードを選択できます。日付と時刻のセレクタから必要な時間範囲を選択することもできます。

Grafana ダッシュボードの設定の詳細については、Grafana のドキュメントを参照してください。

Grafana ダッシュボードの自動更新を構成

自動更新を構成して、Grafana ダッシュボードに最新の情報が表示できるようにすることができます。

ステップ 1 [操作（Operations）] > [システム360（System 360）] > [モニタリング（Monitoring）] を選択します。

ステップ 2 右上隅にある [ダッシュボード設定（Dashboard Settings）] アイコンをクリックして、[設定（Settings）] ウィンドウを開きます。

ステップ 3 [全般（General）] ペインで、[時間オプション（Time Options）] セクションに移動し、[自動更新（Auto Refresh）] フィールドに時間範囲を入力します。範囲は、秒、分、時、日の形式で指定できます。

範囲を指定しない場合、ダッシュボードはデフォルトの間隔（30 秒）で更新されます。

（注） ダッシュボードに表示されるディスク領域の使用率は、Cisco ISE CLI コマンド `showdisks` で表示される出力とは異なる場合があります。

これは、Linux OS がルートユーザー用に 5% のディスク領域を予約しているためです。Grafana はルートユーザーとして実行されませんが、管理 CLI ユーザーはルートユーザーとして動作します。したがって、モニタリングダッシュボードに表示されるディスク領域の使用率は、CLI 出力に表示される使用率よりも 4 ～ 5% 高くなります。

Log Analytics

オープンソースのデータ可視化プラットフォームである Kibana を使用して、syslog データを分析および可視化し、Elasticsearch を使用して、syslog データを保存およびインデックス化します。

Log Analytics を有効にするには、Cisco ISE GUI で、[操作（Operations）]>[システム360（System 360）] > [設定（Settings）] の順に選択し、[Log Analytics] サービスを有効にします。

Log Analytics サービスを有効にする際には、次の点に注意してください。

- このサービスは、MnT ノードでのみ実行されます。
- このサービスは、少なくとも 8 つの CPU コアと 32 GB の RAM を備えた MnT ノードでのみ有効にできます。したがって、Cisco ISE 評価インスタンスで Log Analytics を有効にすることはできません。
- プライマリおよびセカンダリ MnT ノードを構成している場合は、これらのハードウェア要件を満たす MnT ノードで Log Analytics を有効にすることができます。プライマリノードとセカンダリノードの両方がこれらの要件を満たしている場合、両方のノードで Log Analytics サービスを有効にすることができますが、Kibana ダッシュボードはセカンダリ MnT ノードからのみ起動されます。要件を満たすノードがない場合、Log Analytics サービスを有効にすることはできません。

[Elasticsearch] パネルで、[メニュー（Menu）] アイコンをクリックし、[分析（Analytics）]> [ダッシュボード（Dashboard）] を選択して、事前設定された Kibana ダッシュボードを表示します。

- [ISE可観測性ダッシュボード（ISE Observability Dashboard）]：認証および承認トラフィックを表示します。
- [ISE概要ダッシュボード（ISE Overview Dashboard）]：ISE システム全体の概要を提供します。
- [ISEトラブルシューティングダッシュボード（ISE Troubleshooting Dashboard）]：RADIUS 認証を監視し、問題があればトラブルシューティングするのに役立ちます。

- [ISEプロセスサマリー（ISE Process Summary）]：さまざまなプロセスステータスのサマリーを提供します。
- [プロファイラパフォーマンス（Profiler Performance）]：選択した期間のプロファイラパフォーマンス関連情報（プロファイラの平均TPS、プロファイリングされたイベントの合計、プロファイラの最大イベント、一意のプロファイリングされたエンドポイント、一意のネットワークデバイスからのプロファイライベントなど）を表示します。
- [プロファイラサマリー（Profiler Summary）]：エンドポイントソース（プローブ）、アイデンティティグループなどでグループ化された、さまざまなタイプのプロファイリングされたエンドポイントのサマリーを提供します。
- [RADIUSアカウンティングサマリー（RADIUS Accounting Summary）]：受信したすべてのRADIUS アカウンティングイベントのサマリーを提供します。
- [RADIUS認証サマリー（RADIUS Authentication Summary）]：さまざまなエンドポイントからのすべての RADIUS 認証のサマリーを提供します。
- [TACACSアカウンティングサマリー（TACACS Accounting Summary）]：受信したすべての TACACS アカウンティングイベントのサマリーを提供します。
- [TACACS認証サマリー（TACACS Authentication Summary）]：さまざまなエンドポイントからのすべての TACACS 認証のサマリーを提供します。
- [RADIUSステップ遅延（RADIUS Step Latency）]：指定された期間の RADIUS 認証フローステップの最大遅延と平均遅延を表示します。また、Active Directory 認証フローステップ（Active Directory がそのノードで設定されている場合）の最大遅延および平均遅延、および最大遅延または平均遅延のうち上位 N 個の RADIUS 認証手順を表示することもできます。

  手順を追加または削除するには、次の手順を実行します。

  1. [RADIUSステップ遅延（RADIUS Step Latency）]ダッシュボードの右上隅にある[編集（Edit）]をクリックします。
  2. 編集するダッシュレットの右上隅にある歯車アイコンをクリックします。
  3. [レンズの編集（Edit Lens）]をクリックします。
  4. 必要に応じて、手順を追加または削除します。

（注） Cisco ISE リリース 3.3 から、**RADIUS 認証の詳細**レポート（**[操作（Operations）]、[RADIUS]、[ライブログ（Live Logs）]**）ですべての手順の遅延（ミリ秒単位）を表示できます。

これらのダッシュボードを複製するか、要件に基づいて新しいダッシュボードを最初から作成することができます。

[検索（Search）] フィールドに Lucene 構文形式でクエリを入力して、特定のフィールドでログをフィルタリングできます。

Kibana の使用に関する詳細については、Kibana のドキュメントを参照してください。

特定の間隔で自動更新するように Kibana ダッシュボードを設定できます。自動更新を有効にするには、ダッシュボードの右上隅にある日付をクリックし、[自動更新（Auto-Refresh）] をクリックして、値を設定します。

（注）

- ログ分析では、5 分ごとにシステムの正常性に関連する情報を収集します。5 秒ごとにデータを追跡したり、CPU、メモリなど、システムの正常性に関連するさまざまな KPI を監視したりするには、モニタリング機能を使用します。
- Elasticsearch データベースには、過去 7 日間の syslog データが保存されます。
- 使用可能な空きストレージ領域の 5% は、ElasticSearch ストレージ用に予約されています。たとえば、600 GB の空き容量がある場合、ElasticSearch ストレージ用に 30 GB が予約されています。
- [Elasticsearch] パネルの **[メニュー（Menu）]** > **[Overview]** ウィンドウで、[データの追加（Add Data）] オプションをクリックすると、次のエラーメッセージが表示されます。

  アプリケーションが見つかりません。このURLでアプリケーションが見つかりませんでした。戻るか、メニューからアプリケーションを選択してみてください。

  これは、Cisco ISE のデータ取り込み機能が無効になっているためです。

（注） Cisco ISE リリース 3.3 では、ログ分析機能がデフォルトで有効になっています。トラフィックが中程度や高いときには、MnT ペルソナを持つノード、または PAN ペルソナと MnT ペルソナを併せ持つノードに対するログ分析の機能を、SNS-3615 や SNS-3715 デバイスの下位モデルでは無効にすることを推奨します。

詳しくは、（『Release Notes for Cisco Identity Services Engine, Release 3.3』の「Open Caveats in Cisco ISE Release 3.3」を参照してください。

Kibana ダッシュボードの作成

ステップ 1 [操作（Operatons）] > [システム360（System 360）] > [Log Analytics] を選択します。

ステップ 2 インデックスパターンを作成します。

a) [管理（Management）] > [スタック管理（Stack Management）] > [Kibana] > [インデックスパターン（Index Patterns）] を選択します。

b) [インデックスパターンの作成（Create Index Pattern）] をクリックします。

インデックスのリストを表示するには、[管理（Management）] > [スタック管理（Stack Management）] > [データ（Data）] > [インデックス管理（Index Management）] を選択します。展開時に次のインデックスが作成されます。

- [mnt_analytics_radius_authentication]：RADIUS 認証の失敗および成功の履歴を確認するために使用します。
- [mnt_analytics_radius_accounting]：ユーザーがネットワーク上にいる時間を確認するために使用します。
- [mnt_analytics_radius]：RADIUS 認証とアカウンティングデータの両方を取得するために使用します。
- [mnt_analytics_aggregate_steplatency]：すべての RADIUS 認証フローステップの最大および平均遅延を表示するために使用します。
- [mnt_analytics_steplatency_detail]：最大および平均遅延ダッシュレットによる上位 N のステップに含まれるすべてのステップの最大および平均遅延の詳細を表示するために使用します。
- [mnt_analytics_tacacs_authentication]：最も一般的な認証の詳細および認証失敗の理由（ある場合）を表示するために使用します。
- [mnt_analytics_tacacs_accounting]：デバイスセッションの TACACS アカウンティングの詳細を表示するために使用します。
- [mnt_analytics_tacacs]：TACACS 認証とアカウンティングデータの両方を取得するために使用します。
- [mnt_analytics_process_status]：ISE プロセスのステータスを表示するために使用します。
- [mnt_analytics_system_status]：CPU 使用率、ディスク容量、負荷平均、メモリ使用率、ネットワーク使用率、RADIUS 要求遅延、TACACS 要求遅延などのシステム統計を表示するために使用します。このデータを使用して、システム正常性サマリーレポートを作成できます。
- [mnt_analytics_ise_counters]：さまざまな属性のしきい値をリスト表示します。このデータを評価してトレンドを確認し、しきい値よりも高い値を検出した場合には、展開内で発生している問題にこの情報を関連付け、考えられる原因を特定できます。

c) インデックスパターンの名前とタイムスタンプを入力します。複数の文字と一致するアスタリスク（*）を使用します。

ステップ 3 インデックスパターンの可視化の作成

a) [分析（Analytics）] > [ライブラリの可視化（Visualize Library）] を選択します。
b) [可視化の作成（Create Visualization）] をクリックし、可視化タイプを選択します。
c) 複数の行を追加するには、[バケット（Buckets）] > [追加（Add）] > [行を分割（Split Rows）] を選択し、必要な詳細を入力します。
d) [更新（Update）] をクリックします。
e) [保存（Save）] をクリックします。

[可視化の保存（Save Visualization）] ウィンドウが表示されます。

ステップ 4 可視化をダッシュボードに追加します。

a) [可視化の保存（Save Visualization）] ウィンドウで、可視化の名前を入力します。
b) [ダッシュボードに追加（Add to Dashboard）] セクションで、[新規（New）] をクリックし、[ライブラリに追加（Add to Library）] チェックボックスをオンにします。
c) [保存してダッシュボードに移動（Save and go to Dashboard）] をクリックします。
d) [保存（Save）] をクリックします。
e) ダッシュボードの名前と説明を入力します。

同様に、要件に基づいて、作成したダッシュボードに複数の可視化を追加できます。

ダッシュボードの複製、ダッシュボードのエクスポート、フィルタの追加、視覚化のエクスポートなど、Kibana 固有のタスクについては、Kibana のドキュメントを参照してください。

モニタリングおよび Log Analytics 設定

[モニタリング（Monitoring）] 機能を使用すると、一元化されたコンソールから、展開内のすべてのノードの幅広いアプリケーションとシステム統計、および主要業績評価指標（KPI）を監視できます。モニタリングサービスはデフォルトで有効になっています。このサービスは、[操作（Operations）] > [システム360（System 360）] > [設定（Settings）] から無効または再度有効にすることができます。

Log Analytics は、さまざまなエンドポイントから生成された syslog データを詳細に分析するための柔軟な分析システムを提供します。デフォルトでは、Log Analytics サービスは MnT ノードで無効になっています。Log Analytics を有効にするには、[操作（Operations）] > [システム360（System 360）] > [設定（Settings）] の順に選択し、[Log Analytics] トグルボタンをクリックします。

⚠

注意 MnT システムのパフォーマンスへの影響を避けるため、必要な場合にのみ Log Analytics サービスを有効にすることをお勧めします。

モニタリングと Log Analytics サービスの状態を表示するには、**show application status ise** コマンドを使用します。

モニタリングが有効になっている場合、次のサービスがコマンド出力に一覧表示されます。

- `30774 を実行している ISE ノードエクスポータ`
- `32862 を実行している ISE Prometheus サービス`
- `36380 を実行している ISE Grafana サービス`

Log Analytics が有効になっている場合、次のサービスがコマンド出力に一覧表示されます。

- `63388 を実行している ISE MNT LogAnalytics Elasticsearch`
- `68472 を実行している ISE Logstash サービス`

- 71007 を実行している ISE Kibana サービス

（注） モニタリングおよびLog Analyticsのデータは、それぞれのサービスが有効になっている場合にのみ収集されます。サービスが無効になっている期間はデータが収集されません。

Cisco ISE レポート

モニターリング機能およびトラブルシューティング機能とともに Cisco Identity Services Engine（ISE）レポートを使用して、集中管理する場所からのトレンドの分析、システム パフォーマンスおよびネットワーク アクティビティのモニターリングを行います。

Cisco ISE はネットワークからログおよび設定データを収集します。その後、表示と分析のために、データがレポートに集約されます。Cisco ISE には、使用可能な事前定義されたレポートが用意されており、必要に応じてカスタマイズできます。

Cisco ISE レポートは事前設定されており、認証、セッショントラフィック、デバイス管理、設定、管理、およびトラブルシューティングに関する情報のカテゴリにグループ化されます。

関連トピック

レポートの実行および表示 （726 ページ）
レポートのエクスポート （727 ページ）
使用可能なレポート （734 ページ）

レポート フィルタ

レポートには、シングルセクション レポートとマルチセクション レポートの 2 種類があります。シングルセクション レポートには 1 つのグリッドが含まれており（RADIUS 認証レポート）、マルチセクション レポートには複数のグリッドが含まれており（認証概要レポート）、データがグラフと表の形式で示されます。シングルセクション レポートの [フィルタ（Filter）] ドロップダウン メニューには、[クイック フィルタ（Quick Filter）] と [拡張フィルタ（Advanced Filter）] があります。マルチセクション レポートでは、拡張フィルタだけを指定できます。

マルチセクション レポートには、入力が必要な必須拡張フィルタが 1 つ以上含まれていることがあります。たとえば、健全性の概要レポート（[操作（Operations）] > [レポート（Reports）] > [診断（Diagnostics）] ページ）をクリックすると、2 つの必須拡張フィルタ（[サーバー（Server）] と [時間範囲（Time Range）]）が表示されます。レポートを生成するには、この両方のフィルタで演算子コマンド、サーバー名、必要な値を指定し、[実行（Go）] をクリックする必要があります。プラス記号（+）をクリックして新しい拡張フィルタを追加できます。マルチセクション レポートは PDF 形式でのみエクスポートできます。特定の時刻または時間間隔で Cisco ISE マルチセクション レポートを実行または再実行するようにスケジュールすることはできません。

（注） レポートをクリックすると、デフォルトでは最新のデータが生成されます。ただし一部のマルチセクション レポートでは、時間範囲以外にもユーザーが入力する必要のある項目があります。

シングルセクション レポートでは、デフォルトでクイック フィルタが 1 番目の行として表示されます。フィールドには、検索基準を選択できるドロップダウン リストまたはテキスト ボックスが含まれています。

拡張フィルタには、1 つ以上の内部条件を含む外部条件が含まれています。外部条件では、検索で指定された内部条件すべてに一致する必要があるか、またはいずれかに一致する必要があるかを指定します。内部条件には、カテゴリ（[エンドポイント ID（Endpoint ID）]、[ID グループ（Identity Group）]）、メソッド（Contains、Does Not Contain などの演算子コマンド）、および時間範囲を条件として指定するために使用される 1 つ以上の条件が含まれています。

[クイックフィルタ（Quick Filter）] を使用すると、[記録日時（Logged At）] ドロップダウン リストから日付または時刻を選択し、過去 30 日以内にログインしたデータ セットのレポートを生成できます。30 日より前の日付または時刻のレポートを生成する場合は、[高度なフィルタ（Advanced Filters）] を使用して、ドロップダウン リストの [カスタム（Custom）] オプションの [開始日（From）] と [終了日（To）] のフィールドに必要な時間枠を設定します。

クイック フィルタ条件の作成

ここでは、クイック フィルタ条件の作成方法を説明します。クイック フィルタ条件はシングルセクション レポートでのみ作成できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[レポート（Reports）]** で、必要なレポートをクリックします。

ステップ 2 [設定（Settings）] ドロップダウン リストから必須フィールドを選択します。

ステップ 3 データをフィルタリングするため、必須フィールドでドロップダウン リストから選択するか、または特定の文字を入力できます。検索では Contains 演算子コマンドが使用されます。たとえば、「K」で始まるテキストをフィルタリングするには K と入力し、テキスト内の任意の位置に「geo」が含まれているテキストをフィルタリングするには geo と入力します。また、アスタリスク（*）を使用することもできます。たとえば、*abc で始まり *def で終わる正規表現などです。

クイック フィルタで使用される条件には、contains、starts with、ends with、starts with or ends with、および OR 演算子で結合する複数の値があります。

ステップ 4 **Enter** を押します。

拡張フィルタ条件の作成

ここでは、拡張フィルタ条件の作成方法を説明します。拡張フィルタは、シングルセクション レポートとマルチセクション レポートで作成できます。シングルセクション レポートの [フィルタ（Filter）] ドロップダウン メニューには、[クイック フィルタ（Quick Filter）] と [拡張フィルタ（Advanced Filter）] があります。マルチセクション レポートでは、拡張フィルタだけを指定できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[レポート（Reports）]** で、必要なレポートをクリックします。

ステップ 2 [フィルタ（Filters）] セクションで [一致（Match）] ドロップダウン リストから次のいずれかのオプションを選択します。

a) 指定したすべての条件に一致する必要がある場合は、[すべて（All）] を選択します。

b) 指定したいずれか 1 つの条件に一致すればよい場合は、[いずれか（Any）] を選択します。

ステップ 3 [時間範囲（Time Range）] ドロップダウンリストから必要なカテゴリを選択します。

ステップ 4 [演算子コマンド（Operator Commands）] ドロップダウンリストから、必要なコマンドを選択します。たとえば、特定の文字で始まるテキストや（[次の文字で始まる（Begin With）] を使用）、テキスト内の任意の位置に特定の文字が含まれているテキスト（[次の文字を含む（Contains）] を使用）をフィルタリングできます。あるいは、[ログに記録された時刻（Logged Time）] と対応する [カスタム（Custom）] オプションを選択し、カレンダーからデータをフィルタリングする期間の開始日時と終了日時を指定します。

ステップ 5 [時間範囲（Time Range）] ドロップダウンリストから必要なオプションを選択します。

ステップ 6 [移動（Go）] をクリックします。

今後の参照のために、フィルタリングされたレポートを保存し、[フィルタ（Filter）] ドロップダウンリストから取得することができます。

レポートの実行および表示

ここでは、Reports View を使用してレポートを実行、表示、およびナビゲートする方法について説明します。デフォルトでは、レポートをクリックすると過去 7 日間のデータが生成されます。各レポートでは、ページごとに 500 行のデータが表示されます。レポートにデータを表示する時間の増分を指定できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[レポート（Reports）]** > **[ISE レポート（ISE Reports）]** を選択します。

また、各ワーク センターの [レポート（Reports）] リンクに移動して、ワーク センター固有の一連のレポートを確認することもできます。

ステップ 2 使用可能な**レポート** カテゴリからレポートをクリックします。

ステップ 3 レポートを実行する 1 つ以上のフィルタを選択します。各レポートに、異なるフィルタを使用できます。フィルタの一部は必須で一部は任意選択です。

ステップ 4 フィルタに適切な値を入力します。

ステップ 5 [移動（Go）] をクリックします。

関連トピック

レポートのエクスポート （727 ページ）
使用可能なレポート （734 ページ）

レポートのナビゲーション

レポート出力から詳細情報を取得できます。たとえば、5 ヵ月の期間に 1 つのレポートを生成した場合、グラフと表には月単位の目盛りでレポートの集約データが表示されます。

表内の特定の値をクリックすると、この特定のフィールドに関連する別のレポートを表示できます。たとえば、認証概要レポートには、ユーザーまたはユーザー グループの失敗したカウントが表示されます。失敗したカウントをクリックすると、その特定の失敗したカウントについての認証概要レポートが開きます。

レポートのエクスポート

次のレポートは PDF ファイル形式でののみエクスポートできます。

- 認証概要
- 健全性の概要
- RBACL ドロップ概要

（注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。

- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス

ステップ 1 「レポートの実行と表示」の項の説明に従ってレポートを実行します。

ステップ 2 レポートの要約ページの右上隅にある **[エクスポート先（Export To）]** をクリックします。

ステップ 3 次のいずれかのオプションを選択します。

- [リポジトリ（CSV）（Repository (CSV)）]：レポートを CSV ファイル形式でリポジトリにエクスポートします。
- [ローカル（CSV）（Local (CSV)）]：レポートを CSV ファイル形式でローカルディスクにエクスポートします。
- [ローカル（PDF）（Local (PDF)）]：レポートを PDF ファイル形式でローカルディスクにエクスポートします。

（注）
- ローカル CSV または PDF オプションを選択すると、最初の 500 個のレコードのみがエクスポートされます。[リポジトリ（CSV）（Repository CSV）] オプションを使用すると、すべてのレコードをエクスポートできます。
- ローカル PDF オプションを使用してマルチセクションレポートをエクスポートすると、各セクションの最初の 100 行のみがエクスポートされます。

マイレポート

事前設定されたシステムレポートと個人的にフィルタリングされたレポートを [マイレポート（My Reports）] セクションに追加できます。[マイレポート（My Reports）] セクションに保存されたレポートには、適用されたフィルタが保持されます。

ステップ 1 [レポート（Reports）] ウィンドウ（**[操作（Operations）]**>**[レポート（Reports）]**）で、左側に表示される [レポート（Reports）] ドロップダウンメニューから必要なレポートをクリックします。

ステップ 2 （オプション）選択したレポートが開いたら、必要なフィルタを追加してレポートをカスタマイズします。

ステップ 3 ウィンドウの右上隅にある [マイレポートに追加（Add to My Reports）] ボタンをクリックします。

ステップ 4 [マイレポートに保存（Save to My Reports）] ダイアログボックスが開きます。レポートの名前と説明は自動的に入力されます。必要に応じて、これらのフィールドを編集できます。

ステップ 5 （オプション）選択したレポートは、適用可能なフィルタとともに保存されるため、カスタマイズが保持されます。

ステップ 6 [保存（Save）] をクリックして、レポートを保存します。レポートが正常に保存されたことを示すダイアログボックスが表示されます。

ステップ 7 選択したレポートは、簡単にアクセスできるように [マイレポート（My Reports）] ドロップダウンリストに表示されます。

[マイレポート（My Reports）] セクションに追加されたレポートを削除するには、ウィンドウの右上隅にある [マイレポートから削除（Remove From My Reports）] ボタンをクリックしま

す。表示される [アラート（Alert）] ダイアログボックスで [OK] をクリックすると、レポートが [マイレポート（My Reports）] セクションから削除されます。

Cisco ISE レポートのスケジュール

Cisco ISE レポートをスケジュールして、特定の時間または時間間隔で実行および再実行することができます。選択したレポートに適切なフィルタを適用することもできます。毎時、日次、週次、月次、年次の頻度でCisco ISEで実行するようにレポートをスケジュールできます。1回限りのレポートスケジューリングジョブにすることもできます。レポートの開始日と終了日を選択し、レポートをスケジュールする曜日を選択できます。スケジュールされたレポートを実行する時間を決定できます。

生成されたレポートに関する電子メール通知を送受信することもできます。これらの電子メール通知により、スケジュールされたレポートが正常に実行されたかどうかが通知され、リポジトリの詳細、スケジュールされたレポートの時刻なども含まれます。

時間単位の頻度でレポートをスケジュールする場合は、レポートを複数の日にわたって実行することはできますが、日をまたぐ時間枠を設定することはできません。

たとえば、時間単位のレポートを 2019 年 5 月 4 日から 5 月 8 日までスケジューリングする場合は、時間間隔を各日の午前 6 時から午後 11 時までに設定することはできますが、ある日の午後 6 時から翌日の午前 11 時までに設定することはできません。後者の場合、Cisco ISE は、時間範囲が無効であることを示すエラー メッセージを表示します。

次のレポートはスケジュールできません。

- 認証概要
- 健全性の概要
- RBACL ドロップ概要

（注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。

- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス

ステップ 1 [レポート（Reports）] ウィンドウ（**[操作（Operations）]**>**[レポート（Reports）]**）で、左側に表示される [レポート（Reports）] ドロップダウンメニューから、スケジュールするレポートを選択します。

ステップ 2 （オプション）選択したレポートが開いたら、レポートに適用するフィルタを適用します。

ステップ 3 ウィンドウの右上隅にある [スケジュール（Schedule）] ボタンをクリックします。

ステップ 4 [スケジュールとして保存（Save as Schedule）] ダイアログボックスが開きます。

ステップ 5 スケジュールジョブの名前、説明、電子メール、日付、時刻などの詳細を入力します。

ステップ 6 [リポジトリ（Repository）] ドロップダウンリストから、スケジュールされたレポートを保存する外部リポジトリを選択します。詳細については、『Cisco ISE Administrator Guide』の「Backup and Restore Repositories」セクションにある「Table 1. Supportability Matrix for External Repositories」を参照してください。

ステップ 7 [頻度（Frequency）] ドロップダウンリストから、必要に応じてスケジュールの頻度を選択します。たとえば、過去 12 時間のデータのみが必要な場合は、レポートのスケジュール時に [過去12時間（Last 12 hours）] データフィールドを選択します。

ステップ 8 必要に応じて [開始日（Start Date）] と [終了日（End Date）] を選択し、[保存（Save）] をクリックします。

ステップ 9 選択したすべてのフィルタは、スケジュール時にレポートに自動的に適用されます。

ステップ 10 ウィンドウの下部にある [スケジュールされたレポート（Scheduled Reports）] セクションで、作成されたスケジュールと適用されたフィルタを確認できます。

必要に応じて、スケジュールされたレポートを編集および削除することもできます。[スケジュールされたレポート（Scheduled Reports）] ドロップダウンリスト（**[操作（Operations）]** > **[レポート（Reports）]** > **[スケジュールされたレポート（Scheduled Reports）]**）から、スケジュールされたレポートを選択します。[スケジュールの編集（Edit Schedule）] をクリックして、スケジュールされたレポートを変更し、[保存（Save）] をクリックします。スケジュール設定されたレポートを削除するには、[スケジュールの削除（Delete Schedule）] をクリックします。

ユースケース：スケジュール済みレポート

当日の午前 12 時に前日のデータを取得するには、次の手順に従ってレポートをスケジュールします。

ステップ 1 [レポート（Reports）] ウィンドウ（**[操作（Operations）]** > **[レポート（Reports）]**）で、左側に表示される [レポート（Reports）] ドロップダウンメニューから、スケジュールするレポートを選択します。

ステップ 2 （オプション）選択したレポートが開いたら、レポートに適用するフィルタを適用します。

ステップ 3 このシナリオで、前日のデータを取得するには、[ログ取得時（Logged at）] フィールドを選択し、[昨日（Yesterday）] フィルタを適用します。これにより、スケジュールされたレポートが実行されるたびに前日のデータが返されます。過去 12 時間のデータのみが必要な場合は、レポートのスケジュール時に [スケジュールとして保存（Save as Schedule）] ダイアログボックスの [過去12時間のデータ（Last 12 hours data）] フィールドを選択します。

ステップ 4 ウィンドウの右上隅にある [スケジュール（Schedule）] ボタンをクリックします。

ステップ 5 [スケジュールとして保存（Save as Schedule）] ダイアログボックスが開きます。

ステップ 6 スケジュールジョブの名前、説明、電子メール、日付、時刻などの詳細を入力します。

ステップ 7 [リポジトリ（Repository）] ドロップダウンリストから、スケジュールされたレポートを保存する外部リポジトリを選択します。詳細については、『Cisco ISE Administrator Guide』の「Backup and Restore

Repositories」セクションにある「Table 1. Supportability Matrix for External Repositories」を参照してください。

ステップ 8 [頻度（Frequency）] ドロップダウンリストから、必要に応じてスケジュールの頻度を選択します。たとえば、過去 12 時間のデータのみが必要な場合は、レポートのスケジュール時に [過去12時間（Last 12 hours）] データフィールドを選択します。

ステップ 9 必要に応じて [開始日（Start Date）] と [終了日（End Date）] を選択し、[保存（Save）] をクリックします。

ステップ 10 選択したすべてのフィルタは、スケジュール時にレポートに自動的に適用されます。

ステップ 11 ウィンドウの下部にある [スケジュールされたレポート（Scheduled Reports）] セクションで、作成されたスケジュールと適用されたフィルタを確認できます。

（注）

- スケジュールされたレポートのほとんどは、.csv 形式でエクスポートされます。ただし、Radius 認証、Radius アカウンティング、TACACS 認証、TACACS アカウンティング、および操作監査のスケジュールされたレポートは、.csv ファイルを含む .zip フォルダにエクスポートされます。
- 外部の管理者（Active Directory の管理者など）が電子メール ID フィールドを指定せずにスケジュール設定されたレポートを作成すると、電子メール通知は送信されません。
- 内部または外部の Cisco ISE ユーザーの削除は、その特定のユーザーによって作成されたスケジュールされたレポートを削除した後にのみ行い、ユーザーの削除後にアクティブなスケジュールが実行されないようにする必要があります。
- Cisco ISE レポートの保存またはスケジューリング（フィルタの適用）は、PAN からのみ実行できます。
- スケジュールされたレポートジョブは、プライマリ MnT とセカンダリ MnT ノードの両方で実行されます。プライマリ MnT がダウンしている場合、セカンダリ MnT がスケジュールを実行します。このようなシナリオでは、セカンダリ MnT が最初にプライマリ MnT に ping を送信します。ping が失敗した場合にのみ、セカンダリ MnT はスケジュールされたエクスポートジョブを実行します。
- Cisco ISE 3.1 パッチ 1 以降、エクスポートされたレポートの日付のフォーマットが YYYY-MM-DD から DD-MM-YY に変更されました。時間のフォーマットが hh:mm:ss.sss から hh:mm:ss.sss AM/PM（24 時間形式から 12 時間形式）に変更されました。

Cisco ISE のアクティブな RADIUS セッション

Cisco ISE では、ライブ セッション用の動的な許可変更（CoA）機能が提供されます。この機能を使用すると、アクティブなRADIUSセッションを動的に制御できます。次のタスクを実行するために再認証または接続解除要求をネットワーク アクセス デバイス（NAD）に送信できます。

- 認証に関連する問題のトラブルシューティング：[セッション再認証（Session reauthentication）] オプションを使用して、再認証を試みることができます。ただし、アクセスを制限するためにこのオプションを使用しないでください。アクセスを制限するには、シャットダウン オプションを使用します。
- 問題のあるホストのブロック：[ポート シャットダウンによるセッション終了（Session termination with port shutdown）] オプションを使用して、ネットワークに大量のトラフィックを送信する、ウイルスなどに感染したホストをブロックできます。ただし、RADIUS プロトコルでは、シャットダウンされたポートを再度有効にするための方法は現在サポートされていません。
- エンドポイントでの IP アドレス再取得の強制：サプリカントまたはクライアントを持たないエンドポイントに対して [ポート バウンスでのセッション終了（Session termination with port bounce）] オプションを使用し、VLAN 変更後に DHCP 要求を生成できます。
- エンドポイントへの更新された許可ポリシーのプッシュ：[セッション再認証（Session reauthentication）] オプションを使用して、管理者の裁量に基づいた既存のセッションの許可ポリシーの変更などの、更新されたポリシー設定を適用できます。たとえば、ポスチャ確認が有効である場合にエンドポイントが最初にアクセスを許可されると、通常、エンドポイントは隔離されます。エンドポイントのアイデンティティおよびポスチャが確認された後、Session reauthentication コマンドをエンドポイントに送信して、エンドポイントがそのポスチャに基づいて実際の許可ポリシーを取得できるようにすることが可能です。

デバイスによって CoA コマンドが認識されるためには、適切にオプションを設定することが重要です。

CoA が適切に動作するには、動的な許可変更を必要とする各デバイスの共有秘密情報を設定する必要があります。Cisco ISE では、デバイスからのアクセス要求、およびデバイスへの CoA コマンドの発行において、共有秘密情報設定が使用されます。

（注） このリリースの Cisco ISE では、表示可能な認証されたエンドポイント セッションの最大数が 100,000 に制限されています。

関連トピック

RADIUS セッションの許可の変更 （732 ページ）

RADIUS セッションの許可の変更

ネットワークの一部のネットワーク アクセス デバイスでは、リロード後にアカウンティング停止パケットまたはアカウンティング オフ パケットが送信されないことがあります。このため、[セッション ディレクトリ（Session Directory）] の下のレポートでは、有効なセッションと期限切れのセッションの 2 つのセッションが表示される場合があります。

アクティブな RADIUS セッションの許可を動的に変更する場合や、アクティブな RADIUS セッションの接続を解除する場合には、最新のセッションを選択する必要があります。

ステップ 1 Cisco ISE GUI で[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[操作（Operations）]**> **[RADIUSライブログ（RADIUS Livelog）]**。

ステップ 2 [ライブ セッションの表示（Show Live Session）] にビューを切り替えてください。

ステップ 3 CoA を発行する RADIUS セッションの CoA リンクをクリックし、次のいずれかのオプションを選択します。

- [SAnet セッション クエリー（SAnet Session Query）]：SAnet でサポートされるデバイスからのセッションに関する情報をクエリーするために使用します。
- [セッション再認証（Session reauthentication）]：セッションを再認証します。CoA をサポートする ASA デバイスに確立されるセッションにこのオプションを選択すると、セッションポリシープッシュ CoA が呼び出されます。
- [最後の方式でのセッション再認証（Session reauthentication with last）]：そのセッションに対して、最後に成功した認証方式を使用します。
- [再実行によるセッション再認証（Session reauthentication with rerun）]：設定されている認証方式を最初から実行します。

  （注） [最後の方式でのセッション再認証（Session reauthentication with last）] オプションおよび [再実行によるセッション再認証（Session reauthentication with rerun）] オプションは、Cisco IOS ソフトウェアで現在サポートされていません。

- [セッション終了（Session termination）]：単にセッションを終了します。スイッチは、異なるセッションでクライアントを再認証します。
- [ポート バウンスでのセッション終了（Session termination with port bounce）]：セッションを終了し、ポートを再起動します。
- [ポート シャットダウンによるセッション終了（Session termination with port shut down）]：セッションを終了し、ポートをシャットダウンします。

ステップ 4 [実行（Run）] をクリックして、選択した再認証または終了オプションとともに CoA を発行します。

CoA に失敗した場合は、次の理由が考えられます。

- デバイスで CoA がサポートされていない。
- アイデンティティまたは許可ポリシーに変更があった。
- 共有秘密が一致しない。

使用可能なレポート

次の表に、事前設定済みレポートをカテゴリ別に分類して示します。また、レポートの機能およびロギング カテゴリについても説明します。

ロギングカテゴリの syslog を生成するには、[ログのシビラティ（重大度）レベル（Log Severity Level）] を [情報（Info）] に設定します。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]。
- syslog を生成する必要があるロギングカテゴリをクリックします。
- [ログ重大度レベル（Log Severity Level）] ドロップダウンリストから、[情報（Info）] を選択します。
- [保存（Save）] をクリックします。

（注） Cisco ISE リリース 2.6 以降では、IPv6 アドレスを使用するユーザーには次のイベントが監査レポートに記録されます。ログイン/ログアウト、パスワードの変更、および運用変更など。管理者ログイン、ユーザーの変更パスワードの監査、および運用監査レポートでは、IPv4 と IPv6 のレコード別にログをフィルタリングできます。

レポート名	説明	ロギング カテゴリ
監査		
適応型ネットワーク制御の監査	適応型ネットワーク制御の監査レポートは、RADIUS アカウンティングに基づきます。つまり、エンドポイントごとにすべてのネットワークセッションの履歴レポートを表示します。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[成功した認証（Passed Authentications）] および [RADIUSアカウンティング（RADIUS Accounting）] をクリックします。
管理者ログイン	管理者ログインレポートには、GUI ベースの管理者ログインイベントと成功した CLI ログインイベントに関する情報が提供されます。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational Audit）] をクリックします。

レポート名	説明	ロギング カテゴリ
変更設定監査	変更設定監査レポートは、指定した期間内の設定変更の詳細を提供します。機能をトラブルシューティングする必要がある場合、このレポートは、最新の設定変更が問題の原因となったかどうかを決定するのに役立ちます。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational Audit）] をクリックします。

レポート名	説明	ロギング カテゴリ
データ消去の監査		—

レポート名	説明	ロギング カテゴリ
	データ消去の監査レポートは、ロギングデータが消去されている時間を記録します。 このレポートは、データ消去の 2 つのソースを反映します。 毎日午前 4 時に、Cisco ISE は、[管理（Administration）] > [メンテナンス（Maintenance）] > [データ消去（Data Purging）] ウィンドウで設定した基準に一致するロギングファイルがあるかどうかを確認します。あった場合は、ファイルが削除され、このレポートに記録されます。さらに、Cisco ISE は、ログファイルに使用される記憶容量（しきい値）を常に 80% 以下に保ちます。1 時間ごとに、Cisco ISE はこの割合を確認し、しきい値に再び到達するまで、最も古いデータが削除されます。この情報もこのレポートに記録されます。 ディスク容量使用率が高い場合、しきい値の 80%（すなわち合計ディスク容量の 60%）で、「ISE モニターノードはもうすぐ割り当てられている最大量を超えます（ISE Monitor node(s) is about to exceed the maximum amount allocated）」というアラートメッセージが表示されます。その後、しきい値の 90%（すなわち合計ディスク容量の 70%）	

レポート名	説明	ロギング カテゴリ
	で、「ISE モニターノードは割り当てられている最大量を超えました（ISE Monitor node(s) has exceeded the maximum amount allocated）」というアラートメッセージが表示されます。	
エンドポイントのアクティビティ消去	エンドポイントのアクティビティ消去レポートを使用すると、エンドポイントのアクティビティ消去の履歴を確認できます。このレポートは、プロファイラロギングカテゴリが有効である必要があります。（このカテゴリはデフォルトで有効になっている点に注意してください。）	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[プロファイラ（Profiler）] をクリックします。
内部管理者の概要	内部管理者の概要レポートを使用すると、管理者ユーザーのエンタイトルメントを確認できます。このレポートから、管理者ログイン レポートおよび変更設定監査レポートにもアクセスでき、それにより、管理者ごとにこれらの詳細を表示できます。	—
操作監査	操作監査レポートは、次のような操作の変更に関する詳細を提供します。バックアップの実行、Cisco ISE ノードの登録、またはアプリケーションの再起動。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational Audit）] をクリックします。

レポート名	説明	ロギング カテゴリ
pxGrid管理者の監査	pxGrid管理者の監査レポートは、プライマリ PAN でのクライアントの登録、クライアントの登録解除、クライアントの承認、トピックの作成、トピックの削除、パブリッシャとサブスクライバの追加、およびパブリッシャとサブスクライバの削除など、pxGridの管理処理の詳細を提供します。 すべてのレコードに、ノードで処理を実行した管理者の名前が示されます。 管理者およびメッセージの基準に基づいて、pxGrid管理者の監査レポートをフィルタできます。	—
セキュアな通信の監査	セキュアな通信の監査レポートには、認証の失敗、ブレークインの可能性がある試み、SSHログイン、失敗したパスワード、SSHログアウト、無効なユーザーアカウントなどが含まれる、Cisco ISE管理CLIのセキュリティ関連イベントに関する監査の詳細が提供されます。	—
ユーザー変更パスワードの監査	ユーザー変更パスワードの監査レポートは、従業員のパスワード変更に関する検証を表示します。	Cisco ISE GUIで[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational Audit）]をクリックします。

レポート名	説明	ロギング カテゴリ
TrustSec 監査	TrustSec 監査ログには次の内容が含まれます。 • TrustSec コンポーネントの管理（作成、名前変更、更新、削除）。 • TrustSec 対応 NAD への SGACL および SGT の導入 • TrustSec セッション。 Cisco ISE が Catalyst Center と統合され、SD Access が Catalyst Center によって管理されている場合、このログは空です。	—
デバイス管理		
TACACS 認証の概要	TACACS 認証概要レポートには、最も一般的な認証および認証失敗の理由の詳細が示されています。	—
TACACS アカウンティング	TACACS アカウンティングレポートは、デバイスセッションのアカウンティングの詳細を提供します。ユーザーおよびデバイスの生成された時刻およびログに記録された時刻に関する情報が表示されます。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[TACACSアカウンティング（TACACS Accounting）] を選択します。
失敗の理由別上位 N の認証	失敗の理由別上位 N の認証レポートには、選択したパラメータに基づいて、特定の期間における失敗の理由別の認証の合計数が表示されます。	—

レポート名	説明	ロギング カテゴリ
ネットワーク デバイス別上位 N の認証	ネットワークデバイス別上位Nの認証レポートには、選択されたパラメータに基づいて、特定の期間におけるネットワークデバイス名ごとの合格および不合格の認証数が表示されます。	—
ユーザー別上位Nの認証	ユーザー別上位Nの認証レポートには、選択したパラメータに基づいて、特定の期間におけるユーザー名ごとの合格および不合格の認証数が表示されます。	—
診断		

レポート名	説明	ロギング カテゴリ
AAA の診断	AAA の診断レポートは、Cisco ISE とユーザー間のすべてのネットワークセッションの詳細を提供します。ユーザーがネットワークにアクセスできない場合、トレンドを識別し、問題が特定のユーザーに隔離されているか、またはより広範囲の問題を示しているかを識別するために、このレポートを確認できます。 （注） ISE は、ユーザー認証が進行中のときにエンドポイントのアカウンティング停止要求をサイレントにドロップする場合があります。ただし、ISE はユーザー認証が完了した後、すべてのアカウンティング要求の認識を開始します。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、次のロギングカテゴリを選択します。[ポリシー診断（Policy Diagnostics）]、[IDストア診断（Identity Stores Diagnostics）]、[認証フロー診断（Authentication Flow Diagnostics）]、および [RADIUS診断（RADIUS Diagnostics）]。

レポート名	説明	ロギング カテゴリ
AD コネクタ操作	AD コネクタ操作レポートは、Cisco ISE サーバーのパスワードのリフレッシュ、Kerberos チケットの管理、DNS クエリ、DC 検出、LDAP、および RPC 接続管理など、AD コネクタが実行する操作のログを提供します。 AD の障害がいくつか発生している場合、このレポートで詳細を確認して考えられる原因を特定できます。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[ADコネクタ（AD Connector）] を選択します。
エンドポイントプロファイルの変更	エンドポイント（MAC アドレス）別上位認証レポートは、ネットワークにアクセスするために各エンドポイントの MAC アドレスが Cisco ISE によって許可された回数を表示します。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[成功した認証（Passed Authentications）] および [失敗した試行（Failed Attempts）] を選択します。

レポート名	説明	ロギング カテゴリ
健全性の概要	健全性の概要レポートは、ダッシュボードのような詳細を提供します。ただし、ダッシュボードには過去24時間のデータのみが表示されます。また、このレポートを使用して、より多くの履歴データを確認できます。 データの一貫したパターンを調べるためにこのデータを評価できます。たとえば、大多数の従業員が就業時間を開始するときに、非常に高い CPU 使用率が予想されます。これらのトレンドの不整合がわかれば、潜在的な問題を識別できます。 [CPU 使用率（CPU Usage）]テーブルには、各種 Cisco ISE 機能の CPU 使用率（%）が表示されます。**show cpu usage** CLI コマンドの出力がこのテーブルに表示されるため、これらの値を、展開内で発生している問題と関連付け、原因を特定することができます。	—

レポート名	説明	ロギング カテゴリ
ISE カウンタ	ISE カウンタ レポートには、さまざまな属性のしきい値が示されます。各種属性の値の収集間隔は異なり、またデータは表形式で表示されます。5 分間隔で収集される属性と 5 分よりも長い間隔で収集される属性があります。 このデータを評価してトレンドを確認し、しきい値よりも高い値を検出した場合には、展開内で発生している問題にこの情報を関連付け、考えられる原因を特定できます。 Cisco ISE はデフォルトでこれらの属性の値を収集します。**application configure ise** コマンドを使用して、Cisco ISE CLI からこのデータ収集を無効にすることができます。カウンタ属性の収集を有効または無効にするには、**オプション 14** を選択します。	—
主要パフォーマンス測定指標	主要パフォーマンス測定指標レポートには、展開に接続しているエンドポイントの数と、1 時間あたりに各 PAN が処理する RADIUS 要求の数に関する統計情報が表示されます。このレポートには、サーバーの平均負荷、要求あたりの平均遅延、および平均トランザクション数/秒が示されます。	—

レポート名	説明	ロギング カテゴリ
設定が誤っている NAS	設定が誤っている NAS レポートは、通常、アカウンティング情報を頻繁に送信するときに、アカウンティング頻度が不正確な NAD に関する一般情報を提供します。修正処置を行い、設定が誤っている NAD を修正すると、レポートはレポートに修正済み確認を表示します。 （注） このレポートを実行するには、**RADIUS 抑制**を有効にする必要があります。	—
設定が誤っているサプリカント	設定が誤っているサプリカントのレポートは、特定のサプリカントが実行した失敗試行のため、設定が誤っているサプリカントの一覧および統計情報を提供します。修正処置を行い、設定が誤っているサプリカントを修正すると、レポートはレポートに修正済み確認を表示します。 （注） このレポートを実行するには、**RADIUS 抑制**を有効にする必要があります。	—

レポート名	説明	ロギング カテゴリ
ネットワーク デバイスのセッション ステータス	ネットワークデバイスのセッションステータス概要レポートを使用すると、直接スイッチにログインせずにスイッチ設定を表示することができます。 Cisco ISE は SNMP クエリを使用してこれらの詳細にアクセスするので、ネットワークデバイスは SNMP v1 または v2c を使用して設定されている必要があります。 ユーザーにネットワークの問題が発生している場合に、このレポートは、問題がスイッチの設定に関連しているかまたは Cisco ISE に関連しているかを識別するのに役立ちます。	—

レポート名	説明	ロギング カテゴリ
OCSP モニタリング	OCSP モニタリング レポートは、Online Certificate Status Protocol（OCSP）サービスのステータスを指定します。Cisco ISE が正常に証明書サーバーに連絡し、証明書ステータス監査を提供できるかどうかを識別します。また、Cisco ISE によって実行されたすべての OCSP 証明書検証操作の概要も提供されます。適切な/失効したプライマリ/セカンダリ証明書に関連する情報を OCSP サーバーから取得します。Cisco ISE は、応答をキャッシュし、後続の OCSP モニタリング レポートの生成に使用します。キャッシュがクリアされる場合は、OCSP サーバーから情報を取得します。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[システム診断（System Diagnostics）] を選択します。
RADIUS エラー	RADIUS エラーレポートを使用すると、ドロップされた RADIUS 要求（未知のネットワーク アクセス デバイスからの廃棄された認証またはアカウンティング要求）、EAP接続タイムアウトおよび未知の NAD をチェックできます。 （注） 過去 5 日間のレポートのみを表示できます。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[失敗した試行（Failed Attempts）] を選択します。

レポート名	説明	ロギング カテゴリ
システム診断	システム診断レポートは Cisco ISE ノードのステータスの詳細を提供します。Cisco ISE ノードが登録できない場合、このレポートを確認して問題をトラブルシューティングすることができます。 このレポートでは、最初に複数の診断ロギングカテゴリを有効にする必要があります。これらのログを収集すると、Cisco ISE パフォーマンスに悪影響を及ぼすことがあります。したがって、これらのカテゴリはデフォルトで有効ではなく、データを収集するのに十分な時間だけ有効にする必要があります。そうでない場合は、30 分後に自動的に無効になります。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、次のロギングカテゴリを選択します。[内部操作診断（Internal Operations Diagnostics）]、[分散管理（Distributed Management）]、および [管理者の認証と許可（Administrator Authentication and Authorization）]。
エンドポイントとユーザー		
エージェントレスポスチャ	エージェントレスポスチャを実行したすべてのエンドポイントが一覧表示されます。	—

レポート名	説明	ロギング カテゴリ
認証概要	認証概要レポートは、RADIUS 認証に基づいています。それにより、最も一般的な認証および認証失敗の原因（ある場合）を特定することができます。たとえば、ある Cisco ISE サーバーが他のサーバーよりもはるかに多くの認証を処理している場合、負荷を適切に分散するためにユーザーを別の Cisco ISE サーバーに再割り当てする場合があります。 （注） 認証概要レポートまたはダッシュボードが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。	—

レポート名	説明	ロギング カテゴリ
クライアント プロビジョニング	クライアントプロビジョニング レポートは、特定のエンドポイントに適用されるクライアントプロビジョニングエージェントについて示します。このレポートを使用すると、各エンドポイントに適用されるポリシーを確認し、次にこれを使用して、エンドポイントが正しくプロビジョニングされたことを確認することができます。 （注） エンドポイントが ISE に接続されない（セッションが確立されない）場合、またはネットワークアドレス変換（NAT）アドレスがセッションで使用される場合、エンドポイントの MAC アドレスは [エンドポイントID（Endpoint ID）] 列に表示されません。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[ポスチャおよびクライアントプロビジョニングの監査（Posture and Client Provisioning Audit）] および [ポスチャおよびクライアントプロビジョニングの診断（Posture and Client Provisioning Diagnostics）] を選択します。

レポート名	説明	ロギング カテゴリ
現在のアクティブなセッション	現在アクティブなセッションレポートを使用すると、指定の期間内にネットワーク上に存在する者に関する詳細を含むレポートをエクスポートできます。 ユーザーがネットワークにアクセスできない場合、セッションが認証または終了されているかどうか、またはセッションに別の問題があるかどうかを確認できます。	—

レポート名	説明	ロギング カテゴリ
エンドポイントプロファイルと論理プロファイルの概要		—

レポート名	説明	ロギング カテゴリ
	このレポートには、論理プロファイルとエンドポイントプロファイル、およびそれらのプロファイルに一致するエンドポイントの数が表示されます。 論理プロファイルおよびエンドポイントプロファイルについては、「アセットの可視性」の章を参照してください。 このレポートをスケジュールするときは、次の点に注意してください。 • エクスポートしたCSVファイルの [説明（Description）] フィールドに入力した説明テキストをエクスポートするには、[説明（Description）] フィールドの最初の行にキーワード「Export Description=」を入力し、次の行にエクスポートする必要がある説明テキストを続けます。 「Deployment ID」キーワードが説明テキストに含まれている場合、Cisco ISEはスケジュール設定されたレポートにデプロイメントIDを追加します。 • 論理プロファイルテーブルのカスタムヘッダーをエクスポートするには、キーワード「LogicalProfile=」を使用し、その後にエクス	

レポート名	説明	ロギング カテゴリ
	ポートするカスタムヘッダーを続けます。このキーワードが見つからない場合、エクスポートされた CSV レポートのこのセクションには、デフォルトのヘッダー（論理プロファイル）が使用されます。 • エンドポイント プロファイルテーブルのカスタムヘッダーをエクスポートするには、キーワード「EndPointPolicy=」を使用し、その後にエクスポートするカスタムヘッダーを続けます。このキーワードが見つからない場合、エクスポートされた CSV レポートのこのセクションには、デフォルトのヘッダー（エンドポイントプロファイル）が使用されます。 • 論理プロファイルサマリー レポートとエンドポイントプロファイルサマリー レポートを個別にエクスポートすることはできません。	

レポート名	説明	ロギング カテゴリ
エンドポイントスクリプトのプロビジョニングの概要	[エンドポイントスクリプトのプロビジョニングの概要（Endpoint Scripts Provisioning Summary）] ウィンドウには、過去 30 日間に [エンドポイントスクリプト（Endpoint Scripts）] ウィンドウを介して実行されたジョブの詳細が表示されます。	—
外部モバイル デバイス管理	外部モバイルデバイス管理レポートは、Cisco ISE と外部モバイル デバイス管理（MDM）サーバー間の統合に関する詳細を提供します。 このレポートを使用すると、MDM サーバーに直接ログインせずに、MDM サーバーによってプロビジョニングされたエンドポイントを確認することができます。また、登録および MDM コンプライアンス ステータスなどの情報が表示されます。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[MDM] を選択します。
パッシブ ID	パッシブ ID レポートでは、ドメインコントローラへの WMI 接続の状態をモニターし、関連する統計情報（受信した通知の数、1 秒あたりのユーザーログイン/ログアウト回数など）を収集することができます。 （注） この方法で認証されたセッションには、レポートの認証の詳細がありません。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[ID マッピング（Identity Mapping）] を選択します。

レポート名	説明	ロギング カテゴリ
手動証明書プロビジョニング	手動証明書プロビジョニング レポートには、証明書プロビジョニング ポータル経由で手動でプロビジョニングされたすべての証明書がリストされます。	—
条件によるポスチャ アセスメント	条件によるポスチャ アセスメント レポートでは、ISE に設定されたポスチャ ポリシー条件に基づいてレコードを表示し、最新のセキュリティ設定またはアプリケーションがクライアント マシンで利用可能かどうかを確認できます。	—

レポート名	説明	ロギング カテゴリ
エンドポイントによるポスチャ アセスメント	エンドポイントによるポスチャ アセスメント レポートには、エンドポイントの時間、ステータス、PRA アクションなどの詳細な情報が提供されます。[詳細（Details）] をクリックして、エンドポイントの詳細情報を表示することができます。 （注） エンドポイントによるポスチャ アセスメント レポートでは、エンドポイントのアプリケーションおよびハードウェア属性のポスチャ ポリシーの詳細は提供されません。[コンテキストの可視性（Context Visibility）] ページでのみこの情報を確認できます。	—

レポート名	説明	ロギング カテゴリ
ポスチャスクリプト修復		—

レポート名	説明	ロギング カテゴリ
	ポスチャスクリプト修復は、修復スクリプトの実行ステータスを確認するために使用されます。 ステータスは次のいずれかになります。 • 修復スクリプトの実行に成功しました。 • 修復が試行され、スクリプトは失敗して終了しました。 • 修復は試行されませんでした（デフォルト）。 • 修復の試行に失敗しました。含まれているポリシーが改ざんされている可能性があるため、スクリプトは整合性チェックに失敗しました。 • 修復の試行に失敗しました。クライアントがスクリプトのダウンロードに失敗しました。 • 修復の試行に失敗しました。スクリプトが破損しているか、改ざんされている可能性があるため、スクリプトは整合性テストに失敗しました。 • 修復の試行に失敗しました。スクリプトは実行されましたが、時間内に終了しませんでした（タイムアウト）。 • 修復の試行に失敗しま	

レポート名	説明	ロギング カテゴリ
	した。一般的な内部システム障害が発生しました。 • 修復の試行に失敗しました。スクリプトタイプはサポートされていません。 • 修復の試行に失敗しました。スクリプトの起動に失敗しました。 • 証明書の確認に失敗しました。クライアントは、Cisco ISE によって提示されたサーバー証明書を確認できませんでした。	
プロファイリングされたエンドポイントの概要	プロファイリングされたエンドポイントの概要レポートは、ネットワークにアクセスしているエンドポイントに関するプロファイリングの詳細を提供します。 （注） Cisco IP Phone など、セッション時間を登録しないエンドポイントの場合、[エンドポイント（Endpoint）] セッション時間フィールドに、[該当なし（Not Applicable）] と表示されます。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[プロファイラ（Profiler）] を選択します。

レポート名	説明	ロギング カテゴリ
RADIUS アカウンティング	RADIUS アカウンティングレポートは、ユーザーがネットワーク上に存在した時間を識別します。ユーザーがネットワークにアクセスできない場合、Cisco ISE がネットワーク接続問題の原因であるかどうか、このレポートを使用して識別できます。 （注） 暫定アップデートに、指定されたセッションの IPv4 または IPv6 アドレスの変更に関する情報が含まれている場合、Radius アカウンティング暫定アップデートは RADIUS アカウンティングレポートに含まれています。	
RADIUS 認証	RADIUS 認証レポートを使用すると、認証失敗および成功の履歴を確認できます。ユーザーがネットワークにアクセスできない場合、このレポートの詳細を確認して考えられる原因を識別できます。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、次のロギングカテゴリを選択します。[成功した認証（Passed Authentications）] および [失敗した試行（Failed Attempts）]。
登録済みエンドポイント	登録済みエンドポイントレポートは、従業員によって登録されているすべてのパーソナルデバイスを表示します。	—

レポート名	説明	ロギング カテゴリ
拒否エンドポイント	拒否エンドポイント レポートには、従業員が登録したパーソナル デバイスのうち、拒否されたデバイスまたはリリースされたデバイスがすべて表示されます。	—
サプリカント プロビジョニング	サプリカントプロビジョニング レポートは、従業員のパーソナルデバイスにプロビジョニングされたサプリカントに関する詳細を提供します。	ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）
エンドポイントによる上位承認	エンドポイント（MAC アドレス）別上位認証レポートは、ネットワークにアクセスするために各エンドポイントの MAC アドレスが Cisco ISE によって許可された回数を表示します。	成功した認証、失敗した試行（Passed Authentications, Failed Attempts）
ユーザー別上位認証	ユーザー別上位認証レポートは、ネットワークにアクセスするために各ユーザーが Cisco ISE によって許可された回数を表示します。	成功した認証、失敗した試行（Passed Authentications, Failed Attempts）
アクセス サービス別上位 N の認証	アクセス サービス別上位 N の認証レポートには、選択されたパラメータに基づいて、特定の期間におけるアクセス サービス タイプごとの合格および不合格の認証数が表示されます。	—
失敗の理由別上位 N の認証	失敗の理由別上位 N の認証レポートには、選択したパラメータに基づいて、特定の期間における失敗の理由別の認証の合計数が表示されます。	—

レポート名	説明	ロギング カテゴリ
ネットワーク デバイス別上位 N の認証	ネットワーク デバイス別上位 N の認証レポートには、選択されたパラメータに基づいて、特定の期間におけるネットワーク デバイス名ごとの合格および不合格の認証数が表示されます。	—
ユーザー別上位 N の認証	ユーザー別上位 N の認証レポートには、選択したパラメータに基づいて、特定の期間におけるユーザー名ごとの合格および不合格の認証数が表示されます。	—
ゲスト		
AUP 受け入れステータス	AUP 受け入れステータス レポートには、すべてのゲスト ポータルからの AUP 承認の詳細が示されます。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[ゲスト（Guest）] を選択します。
ゲスト アカウンティング	ゲスト アカウンティング レポートは、RADIUS アカウンティング レポートのサブセットです。アクティブなゲストまたはゲスト ID グループに割り当てられたすべてのユーザーがこのレポートに表示されます。	—

レポート名	説明	ロギング カテゴリ
プライマリゲストレポート		Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[成功した認証（Passed Authentications）] を選択します。

レポート名	説明	ロギング カテゴリ
	プライマリゲストレポートは、さまざまなゲストアクセスレポートからデータを結合し、異なるレポートソースからデータをエクスポートできるようにします。プライマリゲストレポートは、ゲストユーザーがアクセスしているWebサイトに関する詳細も提供します。このレポートは、セキュリティ監査の目的で使用し、ゲスト ユーザーがネットワークにアクセスした時間、およびそこで行った操作を示すことができます。 また、ゲストトラフィックに使用するネットワーク アクセス デバイス（NAD）のHTTPインスペクションを有効にする必要もあります。この情報は、NADによってCisco ISEに返送されます。 クライアントが最大同時セッションの制限数に到達した時期を確認するには、管理者ポータルから、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）] の順に選択し、次を実行します。 **1.** 「認証フロー診断」のロギングカテゴリのログ レベルを [警告（WARN）] から [情報（INFO）] に上げます。 **2.** AAA	

レポート名	説明	ロギング カテゴリ
	診断の[ロギングカテゴリ（Logging Category）] の下で [LogCollectorターゲット（LogCollector Target）] を [使用可能（Available）] から [選択済み（Selected）] に変更します。	
デバイスのログインおよび監査	デバイスのログインおよび監査レポートは、デバイスポータルのデバイスでユーザーが実行するログインアクティビティと操作についての詳細を提供します。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[デバイス（My Devices）] を選択します。
スポンサーのログインおよび監査	スポンサーのログインおよび監査レポートは、スポンサー ポータルでのゲストユーザーのログイン、追加、削除、有効化、一時停止、および更新操作の詳細、ならびにスポンサーのログインアクティビティの詳細を提供します。 ゲストユーザーを一括で追加すると、[ゲスト ユーザー（Guest Users）] カラムの下に表示されます。このカラムは、デフォルトでは非表示です。エクスポート時に、これらの一括処理されたユーザーもエクスポートファイルに存在します。	Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[ゲスト（Guest）] を選択します。
SXP		
SXPバインディング	SXPバインディング レポートは、SXP接続を介して交換される IP-SGT バインディングに関する情報を提供します。	—

レポート名	説明	ロギング カテゴリ
SXP 接続	このレポートを使用して、SXP接続のステータスをモニターしたり、ピア IP、SXP ノード IP、VPN 名、SXP モードなど、その接続に関連する情報を収集できます。	—
TrustSec		
RBACL ドロップ概要	RBACL ドロップ概要レポートは、拡張 Cisco ISE ライセンスのみで使用できる TrustSec 機能に固有です。 また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。 ユーザーが特定のポリシーまたはアクセスに違反した場合、パケットがドロップされ、このレポートに示されます。 （注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。	—

レポート名	説明	ロギング カテゴリ
ユーザー別上位N個の RBACL ドロップ	ユーザー別上位 N 個の RBACL ドロップ レポートは、拡張 Cisco ISE ライセンスのみで使用できる TrustSec 機能に固有です。 また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。 このレポートは、特定のユーザー別にポリシー違反（パケット ドロップに基づく）を表示します。 （注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。	—
TrustSec ACI	このレポートには、IEPG、EEPG、エンドポイント、APIC のサブネット設定と同期された SGT および SXP のマッピングが一覧表示されます。これらの詳細は、TrustSec APIC 統合機能が有効になっている場合にのみ表示されます。	—

レポート名	説明	ロギング カテゴリ
TrustSec 展開の検証		—

レポート名	説明	ロギング カテゴリ
	このレポートを使用すると、最新の TrustSec ポリシーがすべてのネットワークデバイスで展開されているかどうか、Cisco ISE とネットワークデバイスで設定されたポリシーに不一致があるかどうかを確認できます。 検証プロセスの結果を表示するには、[詳細（Details）] アイコンをクリックします。次の詳細情報を表示できます。 • 検証プロセスの開始時期と終了時期 • 最新の TrustSec ポリシーがネットワークデバイスで正常に展開されているかどうか。また、最新の TrustSec ポリシーを展開するネットワークデバイスの名前およびIPアドレスを表示することもできます。 • Cisco ISE とネットワークデバイスで設定されたポリシーに不一致があるかどうか。デバイス名、IP アドレス、および各ポリシーの違いの対応するエラーメッセージが表示されます。 [アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] と [ホー	

レポート名	説明	ロギング カテゴリ
	ム（Home）] > [サマリー（Summary）]）で、TrustSec 展開の検証アラームを表示できます。 （注） • レポート作成にかかる時間は、展開内のネットワークデバイスと TrustSec グループの数に応じて異なります。 • TrustSec 展開の検証レポートのエラーメッセージの長さは、現在 480 文字に制限されています。480 文字を超えるエラーメッセージは切り捨てられます。最初から 480 文字のみがレポートに表示されます。	

レポート名	説明	ロギング カテゴリ
TrustSec ポリシーのダウンロード	このレポートには、ポリシー（SGT/SGACL）のダウンロードのためにネットワークデバイスによって送信された要求と、ISE によって送信された詳細が一覧表示されます。ワークフローモードを有効にしている場合、要求を実稼働マトリックスまたはステージング マトリックスに対してフィルタ処理することができます。	このレポートを表示するには、次の手順を実行する必要があります。 **1.** Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択します。 **2.** **[AAA診断（AAA Diagnostics）]** > **[RADIUS診断（RADIUS Diagnostics）]** を選択します。 **3.** RADIUS 診断の [ログシビラティ（重大度）レベル（Log Severity Level）] を DEBUG に設定します。
脅威中心型 NAC サービス		
アダプタのステータス	アダプタのステータス レポートには、脅威および脆弱性のアダプタのステータスが表示されます。	—
COA イベント	脆弱性イベントがエンドポイントに受信されると、Cisco ISE はそのエンドポイントの CoA をトリガーします。CoA イベント レポートには、これらの CoA イベントのステータスが表示されます。また、これらのエンドポイントの新旧の認証ルールとプロファイルの詳細が表示されます。	—
脅威イベント	脅威イベント レポートには、設定したさまざまなアダプタから Cisco ISE が受信した脅威イベントがすべて表示されます。	—

レポート名	説明	ロギング カテゴリ
脆弱性アセスメント	脆弱性アセスメント レポートには、エンドポイントで行われているアセスメントに関する情報が提供されます。このレポートを表示して、設定されたポリシーに基づいてアセスメントが行われているかどうかを確認することができます。	—
ワークロード		
ACI	ACI レポートは、接続済みの Cisco ACI コントローラで学習されたワークロードに関する情報を提供します。このレポートでは、送信元、テナント、VRF、アプリケーションプロファイル、ESG、EPG、および SGT 関連の詳細を確認できます。	—

RADIUS ライブ ログ

次の表では、最近の RADIUS 認証を表示する [ライブログ（Live Logs）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[RADIUS]** > **[ライブログ（Live Logs）]**を選択します。RADIUS ライブログはプライマリ PAN でのみ確認できます。

表 *46 : RADIUS* ライブ ログ

フィールド名	説明
時刻（Time）	モニタリングおよびトラブルシューティング収集エージェントがログを受信した時刻を表示します。このカラムは必須です。選択解除することはできません。
ステータス（Status）	認証の成功/失敗を表示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。

フィールド名	説明
詳細（**Details**）	そのセッションのアカウンティングイベントが処理された場合、[詳細（Details）] 列の下にあるアイコンをクリックすると、[アカウンティングの詳細（Accounting Detail）] レポートが開きます。セッションが認証済みの状態である場合、[詳細（Details）] 列の下にあるアイコンをクリックすると、[認証の詳細（Authentication Detail）] レポートが表示されます。 [認証の詳細（Authentication Detail）] レポートの [応答時間（Response Time）] は、Cisco ISE で認証フローを処理するのにかかった合計時間です。たとえば、認証が 3 つのラウンドトリップメッセージで構成されている場合（最初のメッセージは 300 ミリ秒、次のメッセージは 150 ミリ秒、最後のメッセージは 100 ミリ秒）、[応答時間（Response Time）] は、300 + 150 + 100 = 550 ミリ秒になります。 （注） 7 日を超えてアクティブになっているエンドポイントの詳細を表示することはできません。7 日を超えてアクティブになっているエンドポイントの [詳細（Details）] アイコンをクリックすると、次のメッセージがウィンドウに表示されます。`No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.`
繰り返し回数（**Repeat Count**）	ID、ネットワークデバイス、および許可のコンテキストで変更がなく、直近の 24 時間で認証要求が繰り返された回数を表示します。
ID（**Identity**）	ログイン済みの認証に関連付けられているユーザー名を示します。 ユーザー名が ID ストアに存在しない場合は、`INVALID` と表示されます。その他の原因で認証に失敗した場合は、`USERNAME` と表示されます。 （注） これはユーザーにのみ適用されます。これは MAC アドレスには適用されません。 デバッグをサポートするために、無効なユーザー名の開示を ISE に強制できます。これを行うには、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]** で [無効なユーザー名を開示する（Disclose invalid usernames）] チェックボックスをオンにします。また、[無効なユーザー名を開示する（Disclose Invalid Usernames）] オプションを設定して、タイムアウトを設定し、手動でオフにする必要をなくすこともできます。
エンドポイント ID（**Endpoint ID**）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。

フィールド名	説明
エンドポイントプロファイル（Endpoint Profile）	プロファイリングされるエンドポイントのタイプを示します（たとえば、iPhone、Android、MacBook、Xbox になるようにプロファイリングされます）。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（Authorization Policy）	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル（Authorization Profiles）	認証に使用された認証プロファイルを表示します。
IP アドレス（IP Address）	エンドポイントデバイスの IP アドレスを表示します。
ネットワークデバイス（Network Device）	ネットワーク アクセス デバイスの IP アドレスを表示します。
デバイスポート（Device Port）	エンドポイントが接続されているポート番号を表示します。
ID グループ（Identity Group）	ログの生成対象となるユーザーまたはエンドポイントに割り当てられる ID グループを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
サーバー（Server）	ログの生成元になったポリシーサービスが示されます。
MDMサーバー名（MDM Server Name）	MDM サーバーの名前を表示します。
イベント（Event）	イベントステータスを表示します。

フィールド名	説明
失敗の理由（**Failure Reason**）	認証が失敗した場合、失敗の詳細な理由を表示します。
認証方式（**Auth Method**）	Microsoft チャレンジハンドシェイク認証プロトコルバージョン 2（MS-CHAPv2）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（**Authentication Protocol**）	Protected Extensible Authentication Protocol（PEAP）や Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）など、使用される認証プロトコルを表示します。
セキュリティグループ（**Security Group**）	認証ログによって識別されるグループを表示します。
セッション ID（**Session ID**）	セッション ID を表示します。

（注） [RADIUS ライブログ（RADIUS Live Logs）] と [TACACS+ ライブログ（TACACS+ Live Logs）] ウィンドウでは、各ポリシーの認証ルールに対する最初の属性として [クエリ済み PIP（Queried PIP）] エントリが表示されます。認証ルール内のすべての属性が、以前のルールについてすでにクエリされているディクショナリに関連している場合、追加の [クエリ済み PIP（Queried PIP）] エントリは表示されません。

[RADIUS ライブログ（RADIUS Live Logs）] ウィンドウでは、次の操作を実行できます。

- データを CSV または PDF 形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタ処理します。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） ユーザーのカスタマイズはすべて、ユーザー設定として保存されます。

認証遅延

認証遅延は、認証プロセスが開始された時点からの RADIUS 認証プロセスの平均応答時間です。**[ダッシュボード（Dashboard）]** > **[システム概要（System Summary）]** ダッシュレットを選択します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。Cisco ISE 認証遅延は、**[ダッシュボード（Dashboard）]** > **[システム概要（System Summary）]** ダッシュレットから確認できます。

ドロップダウンリストから次の認証遅延タイムフレームを選択できます。

- [60 分（60 mins）]：このオプションでは、過去 60 分間に開始された認証の認証遅延が指定されます。
- [12 時間（12 hrs）]：このオプションでは、過去 24 時間に開始された認証プロセスの認証遅延が指定されます。

表示される応答時間はミリ秒（ms）単位です。認証遅延の詳細レポートを表示するには、[ライブログ（Live Logs）] ウィンドウで最新のログをクリックします。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）]** > **[RADIUS]** を選択します。

RADIUS ライブ セッション

次の表では、ライブ認証が表示される [RADIUSライブセッション（RADIUS Live Sessions）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。RADIUS ライブ セッションはプライマリ PAN だけで表示されます。

表 *47 : RADIUS* ライブ セッション

フィールド名	説明
開始（Initiated）	セッション開始時のタイムスタンプを表示します。
更新済み（Updated）	変更のためにセッションが最後に更新された時点のタイムスタンプを表示します。
アカウント セッション時間（Account Session Time）	ユーザー セッションの期間（秒単位）を表示します。
セッション ステータス（Session Status）	エンドポイントデバイスの現在のステータスを表示します。

フィールド名	説明
アクション（**Action**）	アクティブなRADIUSセッションを再認証または切断するには、[アクション（Actions）] アイコンをクリックします。
繰り返し回数（**Repeat Count**）	ユーザーまたはエンドポイントの再認証回数を表示します。
エンドポイント ID（**Endpoint ID**）	エンドポイントの一意の識別子を表示します。通常はMACまたはIPアドレスです。
ID（**Identity**）	エンドポイントデバイスのユーザー名を表示します。
IP アドレス（**IP Address**）	エンドポイントデバイスの IP アドレスを表示します。
監査セッション ID（**Audit Session ID**）	固有のセッション ID を表示します。
アカウント セッション ID（**Account Session ID**）	ネットワークデバイスから提供される一意の ID を表示します。
エンドポイント プロファイル（**Endpoint Profile**）	デバイスのエンドポイントプロファイルを表示します。
ポスチャ ステータス（**Posture Status**）	ポスチャ検証のステータスと認証の詳細を表示します。
セキュリティ グループ（**Security Group**）	認証ログによって識別されるグループを表示します。
サーバー（**Server**）	ログを生成したポリシー サービス ノードを示します。
認証方式（**Auth Method**）	パスワード認証プロトコル（PAP）、チャレンジハンドシェイク認証プロトコル（CHAP）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。

フィールド名	説明
認証プロトコル（**Authentication Protocol**）	Protected Extensible Authentication Protocol（PEAP）や Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）など、使用される認証プロトコルを表示します。
認証ポリシー（**Authentication policy**）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（**Authorization Policy**）	特定の許可に選択されているポリシーの名前を表示します。
許可プロファイル（**Authorization Profiles**）	認証に使用された許可プロファイルを表示します。
NAS IP アドレス（**NAS IP Address**）	ネットワークデバイスの IP アドレスを表示します。
デバイス ポート（**Device Port**）	ネットワークデバイスに接続されたポートを表示します。
PRA アクション（**PRA Action**）	ネットワークでのコンプライアンスのためにクライアントが正常にポスチャされた後、そのクライアントで実行される定期的な再評価アクションを表示します。
ANCステータス（**ANC Status**）	デバイスの適応型ネットワーク制御のステータス（[隔離（Quarantine）]、[隔離解除（Unquarantine）]、または[シャットダウン（Shutdown）]）を表示します。
WLC ローミング（**WLC Roam**）	ローミング中にエンドポイントがワイヤレス LAN コントローラ（WLC）間でハンドオフされたことを追跡するために使用されるブール値（Y/N）を表示します。cisco-av-pair=nas-update の値は Y または N です。 （注） Cisco ISE では、セッションの状態がローミングであるかの判定を WLC の nas-update=true 属性に依存して行っています。元の WLC が nas-update=true のアカウンティング停止属性を送信する場合、再認証を回避するために ISE のセッションは削除されません。ローミングが失敗する場合、ISE は 5 日間非アクティブだった場合にセッションを消去します。
パケット入力（**Packets In**）	受信したパケットの数を表示します。

フィールド名	説明
パケット出力（**Packets Out**）	送信したパケットの数を表示します。
受信バイト数（**Bytes In**）	受信したバイト数を表示します。
送信バイト数（**Bytes Out**）	送信したバイト数を表示します。
セッション送信元（**Session Source**）	RADIUS セッションであるか、パッシブ ID セッションであるかを示します。
ユーザードメイン名（**User Domain Name**）	ユーザーの登録済み DNS 名を示します。
ホストドメイン名（**Host Domain Name**）	ホストの登録済み DNS 名を示します。
ユーザーNetBIOS名（**User NetBIOS Name**）	ユーザーの NetBIOS 名を示します。
ホストNetBIOS名（**Host NetBIOS Name**）	ホストの NetBIOS 名を示します。
ライセンスのタイプ（**License Type**）	使用されているライセンスのタイプ（Base、Plus、Apex、または Plus と Apex）を表示します。
ライセンスの詳細（**License Details**）	ライセンスの詳細を表示します。

フィールド名	説明
プロバイダー（Provider）	エンドポイントイベントはさまざまなsyslogソースから学習されます。これらのsyslogソースはプロバイダーと呼ばれます。 • Windows Management Instrumentation（WMI）：WMIは、オペレーティングシステム、デバイス、アプリケーション、およびサービスに関する管理情報にアクセスするための共通インターフェイスとオブジェクトモデルを提供するWindowsサービスです。 • エージェント：クライアントまたは別のプログラムの代わりにクライアントで実行されるプログラム。 • syslog：クライアントがイベントメッセージを送信するロギングサーバー。 • REST：クライアントはターミナルサーバーで認証されます。このsyslogソースの場合、[TSエージェントID（TS Agent ID）]、[開始送信元ポート（Source Port Start）]、[終了送信元ポート（Source Port End）]、[最初の送信元ポート（Source First Port）]の値が表示されます。 • SPAN：ネットワーク情報はSPANプローブを使用して検出されます。 • DHCP：DHCPイベント。 • エンドポイント （注） 異なるプロバイダの2つのイベントがエンドポイントセッションから学習または取得されると、それらのプロバイダは[ライブセッション（Live Sessions）]ウィンドウにカンマ区切り値として表示されます。
MACアドレス（MAC Address）	クライアントのMACアドレスを表示します。
エンドポイントチェック時刻（Endpoint Check Time）	エンドポイントプローブによってエンドポイントが最後にチェックされた時刻を表示します。
エンドポイントチェック結果（Endpoint Check Result）	エンドポイントプローブの結果が表示されます。設定可能な値は次のとおりです。 • [到達不要（Unreachable）] • [ユーザー ログアウト（User Logout）] • [アクティブ ユーザー（Active User）]

フィールド名	説明
送信元ポートの開始（Source Port Start）	（REST プロバイダーの場合にのみ値が表示されます。）ポート範囲の最初のポートの番号を示します。
送信元ポートの終了（Source Port End）	（REST プロバイダーの場合にのみ値が表示されます。）ポート範囲の最後のポート番号を示します。
最初の送信元ポート（Source First Port）	（REST プロバイダーの場合にのみ値が表示されます）ターミナル サーバー エージェントによって割り当てられた最初のポートを示します。 ターミナルサーバーとは、複数のエンドポイントがモデムまたはネットワーク インターフェイスなしで接続でき、複数のエンドポイントが LAN ネットワークに接続できるようにするサーバーまたはネットワークデバイスを指します。複数のエンドポイントに同一 IP アドレスが割り当てられている場合、特定ユーザーの IP アドレスの識別が困難になります。このため、特定ユーザーを識別する目的でターミナル サーバー エージェントがサーバーにインストールされ、各ユーザーにポート範囲が割り当てられます。これにより、IP アドレス - ポート - ユーザーのマッピングが作成されます。
TS エージェント ID（TS Agent ID）	（REST プロバイダーの場合にのみ値が表示されます）エンドポイントにインストールされているターミナル サーバー エージェントの一意の ID を表示します。
AD ユーザー解決 ID（AD User Resolved Identities）	（AD ユーザーの場合にのみ値が表示されます。）一致したアカウントの候補が表示されます。
AD ユーザー解決 DN（AD User Resolved DNs）	（AD ユーザーの場合にのみ値が表示されます。）AD ユーザーの識別名（例：CN=chris,CN=Users,DC=R1,DC=com）を表示します。

TACACS ライブ ログ

次の表では、TACACS+ AAA の詳細を表示する [TACACS ライブログ（TACACS Live Logs）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]**>**[TACACS]**>**[ライブログ（Live Logs）]**。TACACS ライブ ログはプライマリ PAN だけで表示されます。

表 *48 : TACACS* ライブ ログ

フィールド名	使用上のガイドライン
生成日時（**Generated Time**）	特定のイベントがトリガーされた時点に基づいて、syslog の生成日時を示します。
ログに記録された時刻（**Logged Time**）	syslogがモニタリング ノードによって処理され、保存された時刻を示します。このカラムは必須です。選択解除することはできません。
ステータス（**Status**）	認証の成功/失敗を表示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細（**Details**）	虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。
セッションキー（**Session Key**）	ISEによってネットワーク デバイスに返される（EAPの成功メッセージまたはEAP の失敗メッセージにある）セッション キーを示します。
ユーザー名（**Username**）	デバイス管理者のユーザー名を示します。このカラムは必須です。選択解除することはできません。
タイプ（**Type**）	[認証（Authentication）] および [承認（Authorization）] の 2 つのタイプで構成されます。認証、承認、または両方を通過または失敗したユーザー名を表示します。このカラムは必須です。選択解除することはできません。
認証ポリシー（**Authentication policy**）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（**Authorization Policy**）	特定の許可に選択されているポリシーの名前を表示します。
ISEノード（**ISE Node**）	アクセス要求が処理される ISE ノードの名前を表示します。
ネットワークデバイス名（**Network Device Name**）	ネットワーク デバイスの名前を示します。
ネットワークデバイスIP（**Network Device IP**）	アクセス要求を処理するネットワーク デバイスのIPアドレスを示します。

フィールド名	使用上のガイドライン
ネットワークデバイスグループ（**Network Device Groups**）	ネットワークデバイスが属する対応するネットワーク デバイス グループの名前を表示します。
デバイスタイプ（**Device Type**）	異なるネットワークデバイスからのアクセス要求の処理に使用されるデバイスタイプポリシーを示します。
ロケーション（**Location**）	ネットワークデバイスからのアクセス要求の処理に使用されるロケーションベースのポリシーを示します。
デバイスポート（**Device Port**）	アクセス要求が行われるデバイスのポート番号を示します。
失敗の理由（**Failure Reason**）	ネットワークデバイスによって行われたアクセス要求を拒否した理由を示します。
リモートアドレス（**Remote Address**）	エンドステーションを一意に識別するIPアドレス、MACアドレス、またはその他の任意の文字列を示します。
一致したコマンドセット（**Matched Command Set**）	MatchedCommandSet 属性値が存在する場合はその値を表示し、MatchedCommandSet属性値が空の場合、または属性自体がsyslogに存在しない場合は空の値を表示します。
シェルプロファイル（**Shell Profile**）	ネットワークデバイスでコマンドを実行するためのデバイス管理者に付与された権限を示します。

[TACACSライブログ（TACACS Live Logs）] ウィンドウで、次の手順を実行できます。

- データを CSV または PDF 形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタ処理します。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） ユーザーのカスタマイズはすべて、ユーザー設定として保存されます。

エクスポート サマリ

過去7日間にすべてのユーザーによってエクスポートされたレポートの詳細をステータスとともに表示できます。エクスポート サマリには、手動レポートとスケジュールされたレポートの両方が含まれます。[エクスポートの概要（Export Summary）] ウィンドウは、2 分ごとに自動的に更新されます。[更新（Refresh）]アイコンをクリックすると、[エクスポートの概要（Export Summary）] ウィンドウが手動で更新されます。

ネットワーク管理者は、[進行中（In-Progess）] または [キュー登録済み（Queued）] 状態のエクスポートを取り消すことができます。他のユーザーは、自分が開始したエクスポートプロセスをキャンセルすることのみが許可されています。

デフォルトでは、任意の時点で3つのレポートの手動エクスポートのみを実行でき、残りのトリガーされたレポートの手動エクスポートはキューに入れられます。スケジュールされたレポートのエクスポートには、このような制限はありません。

（注） キューに入れられた状態のすべてのレポートが再度スケジューリングされ、Cisco ISE サーバーの再起動時に [進行中（In-progress）] または [キャンセル処理中（Cancellation-in-progress）] 状態のレポートには [失敗しました（failed）] とマークがつきます。プライマリ MnT ノードがダウンしている場合、スケジュールされたレポートエクスポートジョブはセカンダリ MnT ノードで実行されます。

次の表では、[エクスポートの概要（Export Summary）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）] > [レポート（Reports）] > [エクスポートの概要（Export Summary）]**。

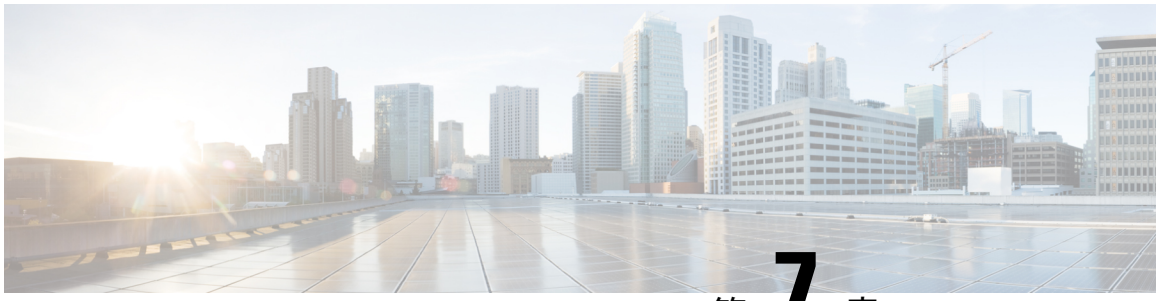
表 *49 :* エクスポート サマリ

フィールド名	説明
エクスポートされたレポート（Report Exported）	レポートの名前を表示します。
エクスポート実行ユーザー（Exported By）	エクスポート プロセスを開始したユーザーのロールを示します。
スケジュール済み（Scheduled）	レポートのエクスポートが予定されているものであるかどうかを示します。
トリガー時刻（Triggered On）	システムでエクスポートプロセスがトリガーされた時刻を示します。

フィールド名	説明
リポジトリ（**Repository**）	エクスポートされたデータを格納するリポジトリの名前を表示します。
フィルタ パラメータ（**Filter Parameters**）	レポートのエクスポート中に選択されたフィルタ パラメータを示します。
ステータス（**Status**）	エクスポートされたレポートのステータスを示します。次のいずれかを設定できます。 • キュー（Queued） • 進行中（In-progress） • 完了（Completed） • キャンセル処理中（Cancellation-in-progress） • キャンセル済み（Cancelled） • 失敗しました（Failed） • 省略（Skipped） （注） [失敗しました（Failed）] ステータスは、失敗の理由を示します。[省略（Skipped）] ステータスは、プライマリ MnT ノードがダウンしているため、スケジュールされたレポートのエクスポートが省略されることを示します。

[エクスポートの概要（Export Summary）] ウィンドウで次の操作を実行できます。

- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタム フィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。



第 7 章

デバイス管理

- TACACS+ デバイス管理 （789 ページ）
- デバイス管理ワーク センター （791 ページ）
- デバイス管理の展開設定 （791 ページ）
- デバイス管理ポリシー セット （792 ページ）
- デバイス管理ポリシー セットの作成 （793 ページ）
- TACACS+ 認証設定と共有秘密 （795 ページ）
- デバイス管理：許可ポリシーの結果 （797 ページ）
- CLI によるイネーブルパスワードの変更 （804 ページ）
- TACACS+ のグローバル設定 （805 ページ）
- Cisco Secure ACS から Cisco ISE へのデータ移行 （806 ページ）
- デバイス管理アクティビティのモニター （806 ページ）

TACACS+ デバイス管理

Cisco ISE は、ネットワークデバイスの設定の制御と監査を行うため、TACACS+ セキュリティ プロトコルを使用したデバイス管理をサポートしています。ネットワークデバイスは、デバイス管理者の操作の認証および許可のために Cisco ISE にクエリを行うために設定され、Cisco ISE のアカウンティングメッセージを送信して操作をログに記録します。これによって、どのネットワーク デバイスに誰がアクセスできて関連するネットワーク設定を変更できるかについて、きめ細かい制御が容易になります。Cisco ISE 管理者は、コマンドセットやシェルプロファイルなどの TACACS 結果をデバイス管理アクセスサービスの認証ポリシールールで選択できるようにするポリシーセットを作成できます。Cisco ISE モニタリングノードでは、デバイス管理に関する高度なレポートが提供されます。[ワークセンター（Work Center）] メニューには、すべてのデバイス管理ページが含まれており、ISE 管理者の単一の始点として機能します。

Cisco ISE には、TACACS+ を使用するためのデバイス管理ライセンスが必要です。

デバイス管理については 2 つのタイプの管理者がいます。

- デバイス管理者
- Cisco ISE 管理者

デバイス管理者は、管理対象デバイスの設定と保守を実行するために、（通常は SSH を介して）スイッチ、ワイヤレスアクセスポイント、ルータ、ゲートウェイなどのネットワークデバイスにログインするユーザーです。Cisco ISE 管理者は、デバイス管理者がログインするデバイスの設定と調整のために Cisco ISE にログインします。

Cisco ISE にログインしてデバイス管理者の操作を制御する設定を行う Cisco ISE 管理者がこのドキュメントの対象読者です。Cisco ISE 管理者は、デバイス管理機能（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work centers）] > [デバイス管理（Device Administration）]**）を使用して、ネットワークデバイスの構成を制御および監査します。デバイスは、TACACS のセキュリティプロトコルを使用して Cisco ISE サーバーにクエリを行うように設定できます。Cisco ISE モニタリングノードでは、デバイス管理に関する高度なレポートが提供されます。Cisco ISE 管理者は、次のタスクを実行できます。

- TACACS+ の詳細（共有秘密）によるネットワーク デバイスの設定。
- 内部ユーザーとしてのデバイス管理者の追加、および必要に応じてイネーブルパスワードの設定。
- コマンドセットやシェル プロファイルなどの TACACS 結果をデバイス管理アクセス サービスの許可ポリシー ルールで選択できるようにするポリシー セットの作成。
- デバイス管理者がポリシーセットに基づいてデバイスにアクセスできるようにするための Cisco ISE での TACACS サーバーの設定。

デバイス管理者は、Cisco ISE サーバーと通信するためのデバイスの設定タスクを実行します。デバイス管理者がデバイスにログインすると、デバイスは Cisco ISE サーバーにクエリを行い、次に内部または外部の ID ストアにクエリを行い、デバイス管理者の詳細を検証します。検証が Cisco ISE サーバーによって行われると、デバイスは、アカウンティングと監査の目的で、各セッションまたはコマンド許可操作の最終結果を Cisco ISE サーバーに通知します。

ISE 管理者は、TACACS および TACACS+ を使用してデバイスを管理できます。

（注） TACACS+ の操作を有効にするには、[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [全般設定（General Settings）] ページの [デバイス管理サービスの有効化（Enable Device Admin Service）] チェックボックスをオンにする必要があります。このオプションは展開内の各 PSN で必ず有効にしてください。

TACACS+ プロトコルの既知の制限により、スイッチまたはルータと Cisco ISE 間のセキュアな接続を確立するため、IP セキュリティプロトコルが二者間に展開されていることを確認してください。

ISE コミュニティ リソース

デバイス管理属性については、「ISE Device Administration Attributes」を参照してください。

ワイヤレス LAN コントローラ、Cisco IOS ネットワークデバイス、Cisco NX-OS ネットワークデバイス、およびネットワークデバイスの TACACS+ 設定については、「ISE Device Administration (TACACS+)」を参照してください。

デバイス管理ワーク センター

[ワークセンター（Work Center）] メニューには、すべてのデバイス管理ページが含まれており、Cisco ISE 管理者の単一の始点として機能します。ただし、ユーザー、ユーザー ID グループ、ネットワーク デバイス、デフォルト ネットワーク デバイス、ネットワーク デバイス グループ、認証および許可条件などのデバイス管理に固有ではないページは、[管理（Administration）] などの元のメニュー オプションから、アクセスすることができます。[ワークセンター（Work Centers）] オプションは、正しい TACACS+ ライセンスが取得され、インストールされている場合にのみ使用できます。

[デバイス管理（Device Administration）] メニューには、次のメニュー オプションが含まれています。[概要（Overview）]、[ID（Identities）]、[ユーザー ID グループ（User Identity Groups）]、[外部 ID ストア（Ext ID Stores）]、[ネットワーク リソース（Network Resources）]、[ネットワーク デバイス グループ（Network Device Groups）]、[ポリシー要素（Policy Elements）]、[デバイス管理ポリシーセット（Device Admin Policy Sets）]、[レポート（Reports）] および [設定（Settings）]。

デバイス管理の展開設定

[デバイス管理の展開（Device Administration Deployment）] ページ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）] > [展開（Deployment）]**）では、Cisco ISE 管理者は [展開（deployment）] セクションで各ノードを確認することなく、デバイス管理システムを一元的に表示できます。

[デバイス管理の展開（Device Administration Deployment）] ページには、展開内の PSN が一覧表示されます。これにより、展開内の各 PSN でデバイス管理サービスを個別に有効にする作業が簡単になります。次のオプションを選択することで、多くの PSN に対するデバイス管理サービスを集合的に有効にできます。

表 *50 : [デバイス管理の展開（Device Administration Deployment）] ウィンドウのオプションリスト*

オプション	説明
なし（None）	デフォルトでは、デバイス管理サービスはすべてのノードで無効になっています。

オプション	説明
すべてのポリシーサービスノード（All Policy Service Nodes）	すべての PSN でデバイス管理サービスを有効にします。このオプションを使用すると、新しい PSN はデバイス管理のために追加されるときに自動的に有効になります。
特定のノード（Specific Nodes）	展開内のすべての PSN をリストしている [ISE ノード（ISE Nodes）] セクションが表示されます。デバイス管理サービスを有効にする必要があるノードを選択できます。

（注） 展開に TACACS+ のライセンスがない場合、上記のオプションは無効になります。

[TACACSポート（TACACS Ports）] フィールドでは、最大 4 つの TCP ポートをカンマ区切りで入力できます。ポート値の範囲は 1 ～ 65535 です。Cisco ISE ノードおよびそのインターフェイスは指定されたポートで TACACS+ 要求をリッスンします。指定されたポートが他のサービスで使用されないようにする必要があります。デフォルトの TACACS+ ポート値は 49 です。

[保存（Save）] をクリックすると、**[管理（Administration）] > [システム（System）] > [展開のリスト（Deployment Listing）]** ウィンドウで指定されたノードと変更が同期されます。

デバイス管理ポリシー セット

[デバイス管理ポリシーセット（Device Admin Policy Sets）] ウィンドウ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]**）には、Cisco ISE 管理者が TACACS+ デバイス管理者の認証と許可を制御するために管理するポリシーセットのリストが含まれています。各ポリシーでは、[通常（Regular）] および [プロキシシーケンス（Proxy Sequence）] の 2 つのモードのいずれかを使用できます。

通常のポリシー セットは認証ルール テーブルおよび許可ルール テーブルから成ります。認証ルールテーブルには、ネットワーク デバイスの認証に必要なアクションを選択する一連のルールが含まれています。

許可ルール テーブルは、承認ビジネス モデルを実装するために必要な特定の承認結果を選択するための一連のルールが含まれています。各許可ルールは、連動するようにルールに一致する必要がある 1 つ以上の条件と、許可プロセスを制御するために選択される一連のコマンド セット、および/またはシェル プロファイルで構成されます。各ルール テーブルには、特定の状況のルールを上書きするために使用できる例外ポリシーがあり、多くの場合、例外テーブルは一時的な状況に使用されます。

（注） TACACS + CHAP アウトバウンド認証はサポートされていません。

プロキシ シーケンス ポリシー セットには、単一の選択されたプロキシ シーケンスが含まれています。ポリシーセットがこのモードである場合、1 台以上のリモートプロキシサーバーが要求の処理に使用されます（ただし、ローカルアカウンティングがプロキシシーケンスで設定されている場合があります）。

デバイス管理ポリシー セットの作成

デバイス管理ポリシー セットを作成するには、次の手順を実行します。

始める前に

- [ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）] > [展開（Deployment）] ウィンドウで、デバイス管理が TACACS+ 操作に対して有効になっていることを確認します。
- ポリシーに必要なユーザー ID グループ（たとえば、System_Admin、Helpdesk）が作成されていることを確認します。（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ユーザー ID グループ（User Identity Groups）]** ページ）。メンバーユーザー（たとえば、ABC、XYZ）が対応するグループに割り当てられていることを確認します。（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ID（Identities）] > [ユーザー（Users）] ウィンドウ）
- 管理しなければならないデバイスで TACACS 設定を行います。（デバイスが Cisco ISE にクエリを行いやすいようにするために、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [TACACS 認証設定（TACACS Authentication Settings）] チェックボックスがイネーブルで、TACACS およびデバイスの共有秘密が同一になっています）
- デバイス タイプとロケーションに基づいたネットワーク デバイス グループが作成されていることを確認します。（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスグループ（Network Device Groups）]** ウィンドウ）

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]**。

ステップ 2 いずれかの行の [アクション（Actions）] 列から、歯車アイコンをクリックし、ドロップダウンリストから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して新しいポリシー セットを挿入します。
[ポリシー セット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 3 ポリシー セットの名前と説明を入力します。

ステップ 4 必要であれば、[許可されているプロトコル/サーバー順序（Allowed Protocols/Server Sequence）] 列から、（+）記号をクリックし、次のいずれかを選択します。

a) 新しい許可されているプロトコルを作成（Create a New Allowed Protocol）
b) TACACS サーバー順序を作成（Create a TACACS Server Sequence）

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性（たとえば、Device-Location Equals Europe）を選択します。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 7 [使用（Use）] をクリックします。

ステップ 8 [表示（View）] 列から、 をクリックしてすべてのポリシーセットの詳細にアクセスし、認証および許可ポリシーとポリシー例外を作成します。

ステップ 9 必要な認証ポリシーを作成します（たとえば、Rule Name: ATN_Internal_Users、Conditions: DEVICE:Location EQUALS Location #All Locations#Europe：このポリシーは、ヨーロッパ内にあるデバイスにのみ一致します）。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 必要な許可ポリシーを作成します。

例 1：ルール名：Sys_Admin_rule、条件：if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8。この例で、ポリシーはユーザー名 ABC のシステム管理者を照合し、指定されたコマンドの実行を許可し、特権レベル 8 を割り当てます。

例 2：ルール名：HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1。この例で、ポリシーはユーザー名 XYZ のシステム管理者を照合し、指定されたコマンドの実行を許可し、特権レベル 1 を割り当てます。

上記の例で、

- コマンドセット cmd_Sys_Admin と cmd_HDesk は、[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS コマンドセット（TACACS Command Sets）] > [追加（Add）] ウィンドウで作成されます。
- TACACS プロファイル Profile_Priv_1 と Profile_priv_8 は、[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）] > [追加（Add）] ウィンドウで作成されます。

（注） 認証および許可ポリシーで使用される条件で、デバイス IP アドレス属性に IPv4 または IPv6 の単一アドレスを追加できます。

ステップ 12　[保存（Save）] をクリックします。

TACACS+ 認証設定と共有秘密

次の表では、ネットワークデバイスのTACACS+認証を設定するために使用できる[ネットワークデバイス（Network Devices）] ウィンドウのフィールドについて説明します。ナビゲーション パスは次のとおりです。

- （ネットワーク デバイスの場合）Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]>[デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [TACACS認証設定（TACACS Authentication Settings）]**。
- （デフォルトのデバイスの場合）Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]>[デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [デフォルトのデバイス（Default Devices）] > [TACACS認証設定（TACACS Authentication Settings）]**。詳細については、「Cisco ISE でのデフォルト ネットワーク デバイスの定義」を参照してください。

フィールド名	使用上のガイドライン
共有秘密鍵（Shared Secret）	TACACS+ プロトコルが有効のときにネットワークデバイスに割り当てられたテキストの文字列。ユーザーは、ネットワーク デバイスによってユーザー名およびパスワードが認証される前にテキストを入力する必要があります。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。これは必須フィールドではありません。
廃止された共有秘密がアクティブです（Retired Shared Secret is Active）	リタイアメント期間がアクティブな場合に表示されます。
廃止（Retire）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、メッセージボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。

フィールド名	使用上のガイドライン
残りの廃止期間（Remaining Retired Period）	（上のメッセージボックスで [はい（Yes）] を選択した場合にのみ利用可能）次のナビゲーションパスで指定されたデフォルト値が表示されます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[設定（Settings）]** > **[接続設定（Connection Settings）]** > **[デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]**。デフォルト値は変更することができます。 これにより、新しい共有秘密を入力でき、古い共有秘密は指定された日数にわたってアクティブなままになります。
終了（End）	（上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。
シングル接続モードを有効にする（Enable Single Connect Mode）	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを実行します。 • [レガシーシスコデバイス（Legacy Cisco Devices）] • または、[TACACS+ドラフトコンプライアンスシングル接続のサポート（TACACS+ Draft Compliance Single Connect Support）]。シングル接続モードを無効にすると、ISE はすべての TACACS+ 要求に対して新しい TCP 接続を使用します。

要約すると、次のことができます。

- 廃止期間を日数として指定することで（範囲は 1 ～ 99 です）、古い共有秘密を廃止し、同時に新しい共有秘密を設定することができます。
- 廃止期間中は新旧の共有秘密を使用できます。
- 期限切れになる前に廃止期間を延長できます。
- 廃止期間の終了までは、古い共有秘密のみを使用できます。
- 期限切れになる前に廃止期間を終了できます（[終了（End）] をクリックしてから [送信（Submit）] をクリックします）。

（注） Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[TACACS+ 認証設定（TACACS+ Authentication Settings）] オプションにアクセスするには、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** > **[追加（Add）]** ウィンドウ。

デバイス管理：許可ポリシーの結果

Cisco ISE 管理者は、TACACS+ コマンドセットおよび TACACS+ プロファイル（ポリシー結果）を使用して、デバイス管理者に付与される権限およびコマンドを制御することができます。ポリシーはネットワークデバイスとともに動作するので、行われる可能性がある偶発的または悪意のある設定変更が回避されます。そのような変更が発生した場合は、デバイス管理の監査レポートを使用して、特定のコマンドを実行したデバイス管理者を追跡することができます。

TACACS+ デバイス管理を許可された FIPS および非 FIPS モードのプロトコル

ポリシーの結果を作成するための Cisco ISE が提供する多数の許可された認証プロトコル サービスがあります。ただし、TACACS+ プロトコルに適用される PAP/ASCII、CHAP および MS-CHAPv1 などの認証プロトコルサービスは、RADIUS の FIPS 対応 Cisco ISE アプライアンスで無効になります。その結果、FIPS 対応（**[管理（Administration）]** > **[システム設定（System Settings）]** > **[FIPSモード（FIPS Mode）]**）Cisco ISEアプライアンスを使用している場合は、デバイスの管理のために **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可されているプロトコル（Allowed Protocols）]** ウィンドウでこれらのプロトコルを有効にすることはできません。

デバイス管理ポリシーの結果で PAP/ASCII、CHAP および MS-CHAPv1 プロトコルを設定するには、FIPS モードと非 FIPS モードのどちらの場合も、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可されているプロトコル（Allowed Protocols）]** ウィンドウに移動する必要があります。FIPS モードを有効にすると、デフォルト デバイス管理で許可されたプロトコル設定のみが使用できます。このオプションは、RADIUS では使用できません。

TACACS+ コマンド セット

コマンドセットは、デバイス管理者が実行できるコマンドの指定されたリストを適用します。デバイス管理者がネットワークデバイスに対して操作コマンドを発行すると、その管理者がこれらのコマンドの発行を認可されているかどうかを判定する問い合わせが Cisco ISE に行われます。これは、コマンド認可とも呼ばれます。

コマンド セットのワイルドカードと正規表現

コマンド ラインは、コマンドと 0 個以上の引数から成ります。Cisco ISE は、コマンド ライン（要求）を受信すると、次のさまざまな方法でコマンドおよび引数を処理します。

- ワイルドカード照合パラダイムを使用して、要求内のコマンドをコマンドセットのリストに指定されたコマンドと照合します。

  例：Sh?? または S*

- 正規表現（regex）照合パラダイムを使用して、要求内の引数をコマンドセットのリストに指定された引数と照合します。

  例：Show interface[1-4] port[1-9]:tty*

コマンド ラインおよびコマンド セットのリストの一致

要求されたコマンドラインをワイルドカードおよび正規表現を含むコマンドセットリストと照合するには、次の手順を実行します。

1. コマンド セットのリストを反復し、一致するコマンドを検出します。

   ワイルドカード照合では以下が許可されています。

   - 大文字小文字の区別なし。
   - コマンドセット内のコマンドの任意の文字を「?」にし、要求されたコマンドに存在する必要がある個別の文字に一致させることができます。
   - コマンドセット内のコマンドの任意の文字を「*」にし、要求されたコマンド内の 0 個以上の文字に一致させることができます。

     次に、例を示します。

要求	コマンド セット	一致	説明
show	show	Y	—
show	SHOW	Y	大文字小文字の区別なし
show	Sh??	Y	任意の文字と一致します
show	Sho??	N	2つ目の「?」は存在しない文字と交差します
show	S*	Y	「*」は任意の文字と一致します
show	S*w	Y	「*」は文字「ho」と一致します
show	S*p	N	文字「p」は対応しません

2. 一致する各コマンドに対し、Cisco ISE は引数を検証します。

   コマンドセットリストには、各コマンドのスペースで区切られた一連の引数が含まれています。

例：Show interface[1-4] port[1-9]:tty.*

このコマンドには、2 つの引数があります。

1. 引数 1：interface[1-4]

2. 引数 2：port[1-9]:tty.*

要求内のコマンド引数は、パケットに表示される位置が重要な順序で実行されます。コマンド定義内のすべての引数が要求内の引数に一致すると、このコマンドまたは引数は一致していると見なされます。要求内の無関係な引数はすべて無視されます。

（注） 引数には標準の Unix 正規表現を使用します。

複数のコマンド セットを持つルールの処理

1. コマンドセットにコマンドとその引数との一致が含まれる場合、その一致が Deny Always であると、Cisco ISE によってそのコマンドセットは Commandset-DenyAlways として指定されます。
2. コマンドセット内のコマンド一致に Deny Always が含まれていない場合は、Cisco ISE によって最初の一致が見つかるまで、コマンドセット内のすべてのコマンドが順番にチェックされます。
    1. 最初の一致が Permit である場合、Cisco ISE はそのコマンドセットを Commandset-Permit として指定します。
    2. 最初の一致が Deny である場合、Cisco ISE はそのコマンド セットを Commandset-Deny として指定します。
3. Cisco ISE は、すべてのコマンドセットを分析したあと、コマンドを次のように認可します。
    1. Cisco ISE がコマンドセットを Commandset-DenyAlways として指定した場合は、Cisco ISE はそのコマンドを拒否します。
    2. Commandset-DenyAlways がない場合、Cisco ISE はコマンドセットが Commandset-Permit であれば、そのコマンドを許可します。そうでない場合、そのコマンドを拒否します。唯一の例外は、[不一致（Unmatched）] チェックボックスがオンになっている場合です。

TACACS+ コマンド セットの作成

TACACS+ コマンドセットのポリシー結果を使用してポリシーセットを作成するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS コマンドセット（TACACS Command Sets）]**。

[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）] ページで TACACS コマンドセットを設定することもできます。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 名前と説明を入力します。

ステップ 4 [追加（Add）] をクリックして、権限の付与、コマンドおよび引数を指定します。

ステップ 5 [付与（Grant）] ドロップダウンで、以下のいずれかを選択できます。

- [許可（Permit）]：指定したコマンドを許可する場合（たとえば、permit show、permit con* Argument terminal など）。
- [拒否（Deny）]：指定したコマンドを拒否する場合（たとえば、deny mtrace）。
- [常に拒否（Deny Always）]：他のコマンドセットで許可されているコマンドをオーバーライドする場合（たとえば、clear auditlogs）。

（注） [付与（Grant）]、[コマンド（Command）] および [引数（Argument）] フィールドの列幅を増やしたり減らしたりするには、アクション アイコンをクリックします。

ステップ 6 [下にリストされていないコマンドを許可（Permit any command that is not listed below）] チェックボックスをオンにして、[付与（Grant）] 列で [許可（Permit）]、[拒否（Deny）] または [常に拒否（Deny Always）] として指定されていないコマンドおよび引数を許可します。

TACACS+ プロファイル

TACACS+ プロファイルは、デバイス管理者の最初のログイン セッションを制御します。セッションは、個々の認証、許可、またはアカウンティングの要求を参照します。ネットワーク デバイスへのセッション認可要求により、Cisco ISE 応答が発生します。この応答には、ネットワークデバイスにより解釈されるトークンが含まれており、これはセッション期間中に実行できるコマンドを制限します。デバイス管理アクセス サービス用の許可ポリシーでは、単一のシェル プロファイルおよび複数のコマンド セットを含めることができます。TACACS+ プロファイル定義は、次の 2 つのコンポーネントに分けられています。

- 共通タスク
- カスタム属性

[TACACS+ プロファイル（TACACS+ Profiles）] ウィンドウ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）]**）には、**[タスク属性（Task**

Attribute）] ビューと **[未処理（Raw）]** ビューの 2 つのビューがあります。共通タスクは [タスク属性（Task Attribute）] ビューを使用して入力でき、カスタム属性は [タスク属性（Task Attribute）] ビューおよび [未処理（Raw）] ビューで作成できます。

[共通タスク（Common Tasks）] セクションを使用すると、頻繁に使用されるプロファイルの属性を選択および設定できます。ここに含まれる属性は、TACACS+ プロトコル ドラフト仕様で定義された属性です。ただし、これらの値は、他のサービスからの要求の許可に使用される場合があります。[タスク属性（Task Attribute）] ビューでは、Cisco ISE 管理者はデバイス管理者に割り当てられる権限を設定できます。一般的なタスクのタイプは次のとおりです。

- Shell
- Cisco WLC
- Cisco Nexus
- 汎用

[カスタム属性（Custom Attributes）] セクションでは、追加の属性を設定できます。[共通タスク（Common Tasks）] セクションで認識されていない属性のリストも提供されます。各定義は、属性名、属性が必須であるか任意であるかの指定、および属性の値で構成されています。

（注） TACACS 対応ネットワークデバイスには、合計 24 個のタスク属性を定義できます。24 を超えるタスク属性を定義した場合、いずれの属性も TACACS 対応ネットワークデバイスに送信されません。

[未処理（Raw）] ビューでは、属性名とその値の間に等号（=）を使用して必須属性を入力でき、属性名とその値の間にアスタリスク（*）を使用して任意の属性を入力できます。[未処理（Raw）] ビューセクションで入力した属性は、[タスク属性（Task Attribute）] ビューの [カスタム属性（Custom Attributes）] セクションに反映され、その逆も同様です。[未処理（Raw）] ビューセクションは、クリップボードから属性リスト（たとえば、別の製品の属性リスト）を Cisco ISE にコピーアンドペーストするためにも使用されます。カスタム属性は、非シェル サービスに対して定義できます。

TACACS+ プロファイルの作成

TACACS+ プロファイルを作成するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[TACACSプロファイル（TACACS Profiles）]**。

[ワークセンター（Work Centers）] > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** ページで TACACS コマンドセットを設定することもできます。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [TACACSプロファイル（TACACS Profile）] セクションで、名前と説明を入力します。

ステップ 4 [タスク属性ビュー（Task Attribute View）] タブで、必要な**共通タスク**を確認します。共通タスク設定 （802 ページ）ページを参照してください。

ステップ 5 [タスク属性ビュー（Task Attribute View）] タブの [カスタム属性（Custom Attributes）] セクションで、[追加（Add）] をクリックして必須属性を入力します。

共通タスク設定

共通タスクの設定ウィンドウを表示するには、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）] > [追加（Add）]**。一般的なタスクタイプは、Shell、Cisco WLC、Cisco Nexus および Generic です。

Shell

次のオプションは、Cisco ISE の管理者がデバイスの管理者権限を設定するために使用できます。

オプション	説明
デフォルトの権限（Default Privilege）	シェル認可のデバイス管理者のデフォルトの（最初の）権限レベルを有効にします。次のオプションのいずれかを選択します。 • 0 ～ 15 の範囲の値を選択します。 • 必要な ID ストア属性を選択します。
最大権限（Maximum Privilege）	イネーブル認証の最大権限レベルを有効にします。0 ～ 15 の範囲の値を選択できます。
アクセス コントロール リスト（Access Control List）	ASCII 文字列（1-251*）または必要な ID ストア属性を選択します。
自動コマンド（Auto Command）	ASCII 文字列（1-248*）または必要な ID ストア属性を選択します。
エスケープなし（No Escape）	エスケープ文字に、次のいずれかのオプションを選択します。 • [はい（True）]：エスケープ防止を有効にすることを指定します。 • [いいえ（False）]：エスケープ防止を有効にしないことを指定します。 • 必要な ID ストア属性を選択します。

オプション	説明
タイムアウト（Timeout）	0 ～ 9999 の範囲の値または必要な ID ストア属性を選択します。
アイドル時間（Idle Time）	0 ～ 9999 の範囲の値または必要な ID ストア属性を選択します。

Cisco WLC

次のオプションは、Cisco ISE の管理者がデバイス管理者による Cisco WLC アプリケーションのタブへのアクセスを制御するために使用できます。Cisco WLC アプリケーションには次のタブが含まれます。[WLAN]、[コントローラ（Controller）]、[ワイヤレス（Wireless）]、[セキュリティ（Security）]、[管理（Management）] および [コマンド（Commands）]。

オプション	説明
すべて（All）	デバイスの管理者はすべての Cisco WLC アプリケーションのタブにアクセスできます。
モニタ（Monitor）	デバイス管理者は Cisco WLC アプリケーションのタブへの読み取り専用アクセス権を持ちます。
ロビー（Lobby）	デバイス管理者は限定された設定の権限のみを持ちます。
選択（Selected）	デバイス管理者は次のチェックボックスから Cisco ISE 管理者がチェックしたタブにアクセスできます。[WLAN]、[コントローラ（Controller）]、[ワイヤレス（Wireless）]、[セキュリティ（Security）]、[管理（Management）] および [コマンド（Commands）]。

Nexus

次のオプションは、Cisco ISE の管理者がデバイス管理者による Cisco Nexus スイッチへのアクセスを制御するために使用できます。

オプション	説明
属性の設定（Set Attribute As）	Cisco ISE の管理者は、任意または必須として一般的なタスクによって生成された Nexus 属性を指定できます。

オプション	説明
ネットワークロール（Network Role）	Nexus が Cisco ISE を使用して認証するように設定されると、デバイス管理者は、デフォルトでは、読み取り専用アクセス権を持ちます。デバイス管理者は、これらのロールのいずれかに割り当てることができます。各ロールは許可された操作を定義します。 • [なし（None）]：権限はありません。 • [オペレータ（Operator）]（読み取り専用）：全NX-OSデバイスへの完全な読み取りアクセス権を持ちます。 • [管理者（Administrator）]（読み取り/書き込み）：全NX-OSデバイスへの完全な読み取り/書き込みアクセス権を持ちます。
仮想デバイスコンテキスト（VDC）（Virtual Device Context (VDC)）	[なし（None）]：権限はありません。 [オペレータ（Operator）]（読み取り専用）：VDC への限定された読み取りアクセス [管理者（Administrator）]（読み取り/書き込み）：VDCへの限定された読み取り/書き込みアクセス

汎用

Cisco ISE 管理者は、一般的なタスクでは使用できないカスタム属性を指定するオプションを使用します。

CLI によるイネーブルパスワードの変更

イネーブル パスワードを変更するには、次の手順を実行します。

始める前に

一部のコマンドは特権モードに割り当てられます。したがって、デバイスの管理者がこのモードに認証されているときしか実行できません。

そのデバイスの管理者が特権モードに入ろうとする際に、デバイスは特別なイネーブル認証タイプを送信します。Cisco ISE は、この特別なイネーブル認証タイプを検証するために別のイネーブル パスワードをサポートします。別のイネーブル パスワードはデバイスの管理者が内部 ID ストアに認証されているときに使用されます。外部 ID ストアとの認証では、同じパスワードが通常のログインに対して使用されます。

ステップ 1 スイッチにログインします。

ステップ 2 Enter を押して次のプロンプトを表示します。

```
Switch>
```

ステップ 3 次のコマンドを実行して、イネーブル パスワードを設定します。

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

（注） パスワードの有効期間がログイン パスワードおよびイネーブル パスワードに設定されている場合、パスワードが指定された時間期間内に変更されないと、ユーザー アカウントは無効になります。Cisco ISE が TACACS+ サーバーとして構成され、ネットワーク デバイスで [バイパスを有効にする（Enable Bypass）] オプションが設定されている場合、CLI から（telnet 経由で）イネーブル パスワードを変更できません。内部ユーザーの enable パスワードを変更するには、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** 。

TACACS+ のグローバル設定

TACACS+ のグローバル設定を行うには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）]**。

[接続設定（Connection Settings）] タブで、必須フィールドのデフォルト値を変更できます。

- [認証キャッシュタイムアウト（Authorization cache timeout）] フィールドで、内部ユーザーの特定の属性を最初の認証要求時にキャッシュ化するために存続可能時間（TTL）の値を設定できます。キャッシュ化された属性には、ユーザー名と、UserGroup などのユーザー固有の属性が含まれます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[システム管理（System Administration）] > [設定（Configuration）] > [ディクショナリ（Dictionaries）] > [ID（Identity）] > [内部ユーザー（Internal Users）]** で属性を作成します。デフォルト値は 0 です。つまり、認証キャッシュが無効になっています。
- 単一接続のサポート（Single Connect Support）：シングル接続モードを無効にすると、ISE はすべての TACACS+ 要求に対して新しい TCP 接続を使用します。

ステップ 2 [パスワード変更制御（Password Change Control）] タブで、パスワードの更新を TACACS+ を介して許可するかどうかを制御するのに必要なフィールドを定義します。

[Telnetパスワード変更を有効にする（Enable Telnet Change Password）] セクションのプロンプトは、このオプションが選択されている場合にのみ有効です。選択されていない場合は、[Telnetパスワード変更を無効にする（Disable Telnet Change Password）] のプロンプトが有効になります。パスワード プロンプトはすべてカスタマイズ可能で、必要に応じて変更できます。

[パスワード ポリシー違反メッセージ（Password Policy Violation Message）] フィールドに、新しいパスワードが指定された条件と一致しない場合に、内部ユーザーが設定したパスワードに適したエラー メッセージを表示できます。

ステップ 3 [セッションキーの割り当て（Session Key Assignment）] タブで、セッションに TACACS+ 要求をリンクするために必要なフィールドを選択します。

セッション キーは、クライアントからの AAA 要求をリンクするためにモニタリング ノードによって使用されます。デフォルト設定では、[NASアドレス（NAS-Address）]、[ポート（Port）]、[リモートアドレス（Remote-Address）]、および [ユーザー（User）] フィールドが有効になっています。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

TACACS+ 認証設定と共有秘密 （795 ページ）

Cisco Secure ACS から Cisco ISE へのデータ移行

移行ツールを使用して、Cisco Secure ACS 5.5 以降からデータをインポートし、すべてのネットワークデバイスにデフォルトの TACACS+ 秘密を設定できます。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[概要（Overview）]**Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[準備（Prepare）] セクションで、[ソフトウェアのダウンロード Web ページ（Download Software Webpage）] をクリックして移行ツールをダウンロードします。ツールを PC に保存し、[migTool] フォルダから migration.bat ファイルを実行し、移行プロセスを開始します。移行に関する詳細については、お使いのバージョンの Cisco ISE の『Migration Guide』を参照してください。

デバイス管理アクティビティのモニター

Cisco ISE では、TACACS+ で設定されたデバイスのアカウンティング、認証、承認、およびコマンドアカウンティングに関する情報を参照できる、さまざまなレポートおよびログが提供されます。オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[レポート（Reports）]** > **[レポート（Reports）]**。.

別の場所でレポートを表示することもできます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** ページを選択します。

ステップ 2 [レポート セレクタ（Report Selector）] で、[デバイス管理（Device Administration）] を展開し、[認証概要（Authentication Summary）]、[TACACS アカウンティング（TACACS Accounting）]、[TACACS 認証（TACACS Authentication）]、[TACACS 許可（TACACS Authorization）]、[TACACS コマンド アカウンティング（TACACS Command Accounting）]、[失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）]、[ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）]、[ユーザー別上位 N の認証（Top N Authentication by User）] レポートを表示します。

ステップ 3 レポートを選択し、[フィルタ（Filters）] ドロップダウン リストを使用して、検索するデータを選択します。

ステップ 4 データを表示する [時間範囲（Time Range）] を選択します。

ステップ 5 [実行（Run）] をクリックします。

TACACS ライブ ログ

次の表では、TACACS+ AAA の詳細を表示する [TACACS ライブログ（TACACS Live Logs）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[TACACS]** > **[ライブログ（Live Logs）]**。TACACS ライブ ログはプライマリ PAN だけで表示されます。

表 *51 : TACACS* ライブ ログ

フィールド名	使用上のガイドライン
生成日時（Generated Time）	特定のイベントがトリガーされた時点に基づいて、syslog の生成日時を示します。
ログに記録された時刻（Logged Time）	syslog がモニタリング ノードによって処理され、保存された時刻を示します。このカラムは必須です。選択解除することはできません。
ステータス（Status）	認証の成功/失敗を表示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細（Details）	虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。
セッションキー（Session Key）	ISE によってネットワーク デバイスに返される（EAP の成功メッセージまたはEAP の失敗メッセージにある）セッション キーを示します。

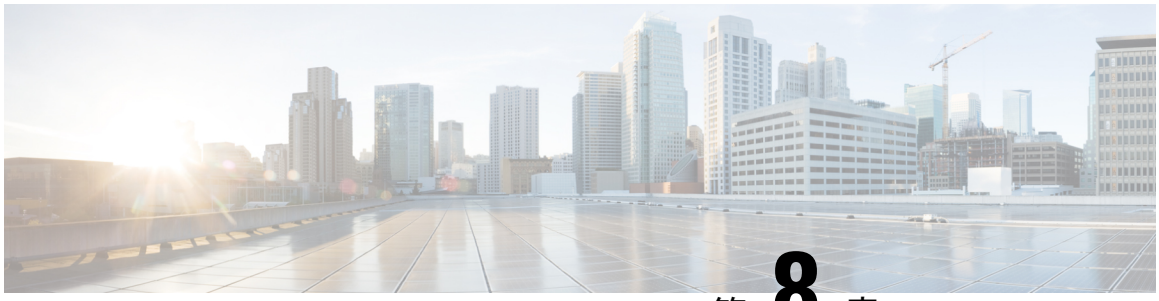
フィールド名	使用上のガイドライン
ユーザー名（**Username**）	デバイス管理者のユーザー名を示します。このカラムは必須です。選択解除することはできません。
タイプ（**Type**）	[認証（Authentication）] および [承認（Authorization）] の 2 つのタイプで構成されます。認証、承認、または両方を通過または失敗したユーザー名を表示します。このカラムは必須です。選択解除することはできません。
認証ポリシー（**Authentication policy**）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（**Authorization Policy**）	特定の許可に選択されているポリシーの名前を表示します。
ISEノード（**ISE Node**）	アクセス要求が処理される ISE ノードの名前を表示します。
ネットワークデバイス名（**Network Device Name**）	ネットワーク デバイスの名前を示します。
ネットワークデバイスIP（**Network Device IP**）	アクセス要求を処理するネットワークデバイスのIPアドレスを示します。
ネットワークデバイスグループ（**Network Device Groups**）	ネットワークデバイスが属する対応するネットワーク デバイス グループの名前を表示します。
デバイスタイプ（**Device Type**）	異なるネットワークデバイスからのアクセス要求の処理に使用されるデバイスタイプポリシーを示します。
ロケーション（**Location**）	ネットワークデバイスからのアクセス要求の処理に使用されるロケーションベースのポリシーを示します。
デバイスポート（**Device Port**）	アクセス要求が行われるデバイスのポート番号を示します。
失敗の理由（**Failure Reason**）	ネットワークデバイスによって行われたアクセス要求を拒否した理由を示します。
リモートアドレス（**Remote Address**）	エンドステーションを一意に識別するIPアドレス、MACアドレス、またはその他の任意の文字列を示します。

フィールド名	使用上のガイドライン
一致したコマンドセット（**Matched Command Set**）	MatchedCommandSet 属性値が存在する場合はその値を表示し、MatchedCommandSet 属性値が空の場合、または属性自体が syslog に存在しない場合は空の値を表示します。
シェルプロファイル（**Shell Profile**）	ネットワーク デバイスでコマンドを実行するためのデバイス管理者に付与された権限を示します。

[TACACSライブログ（TACACS Live Logs）] ウィンドウで、次の手順を実行できます。

- データを CSV または PDF 形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタ処理します。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） ユーザーのカスタマイズはすべて、ユーザー設定として保存されます。



第 8 章

ゲストおよびセキュア Wi-Fi

- Cisco ISE ゲスト サービス （811 ページ）
- ゲスト アカウントとスポンサー アカウント （812 ページ）
- ゲスト ポータル （840 ページ）
- スポンサー ポータル （859 ページ）
- ゲストとスポンサーのアクティビティのモニター （876 ページ）
- ゲスト アクセス Web 認証オプション （879 ページ）
- ゲストポータルの設定 （886 ページ）
- スポンサー ポータル アプリケーションの設定 （910 ページ）
- ゲストおよびスポンサー ポータルのグローバル設定 （919 ページ）
- ゲスト タイプの設定 （920 ページ）
- スポンサー グループ設定 （923 ページ）
- エンドユーザー ポータル （928 ページ）
- エンドユーザー Web ポータルのカスタマイズ （928 ページ）
- ポータル コンテンツのタイプ （929 ページ）
- ポータルの基本的なカスタマイズ （930 ページ）
- ポータルの高度なカスタマイズ （941 ページ）
- ポータル言語のカスタマイズ （960 ページ）
- ゲスト通知、承認、およびエラー メッセージのカスタマイズ （964 ページ）
- ポータル ページのタイトル、コンテンツおよびラベルの文字数制限 （969 ページ）
- ポータルのカスタマイズ （972 ページ）
- ポータル言語ファイルの HTML サポート （973 ページ）

Cisco ISE ゲスト サービス

Cisco Identity Services Engine（Cisco ISE）のゲストサービスを使用すると、ビジター、請負業者、コンサルタント、顧客などのゲストにセキュアなネットワークアクセスを提供することができます。Cisco ISE の基本ライセンスを持つゲストをサポートでき、会社のインフラストラクチャと機能の要件に応じて複数の展開オプションから選択できます。

Cisco ISE は、企業のネットワークおよび内部リソースとサービスへのゲストおよび従業員のオンボーディングを行う Web ベースのモバイル ポータルを提供します。

管理者ポータルで、ゲスト ポータルおよびスポンサー ポータルの作成と編集、ゲスト タイプの定義によるゲストアクセス権限の設定、ゲストアカウントの作成と管理のためのスポンサー権限の割り当てを行うことができます。

- ゲスト ポータル （840 ページ）
- ゲスト タイプおよびユーザー ID グループ （813 ページ）
- スポンサー ポータル （859 ページ）
- スポンサー グループ （861 ページ）

ISE コミュニティ リソース

ISE ゲストと Web 認証に関する ISE コミュニティリソースのリストについては、「ISE Guest Access - ISE Guest and Web Authentication」を参照してください。

分散環境のエンドユーザーのゲスト ポータルとスポンサー ポータル

Cisco ISE のエンドユーザー Web ポータルは、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナに基づき、設定、セッション サポート、およびレポート作成を提供します。

- [ポリシー管理ノード（PAN）（Policy Administration node (PAN)）]：ユーザー、デバイス、およびエンドユーザーポータルが PAN に書き込まれる構成の変更。
- [ポリシーサービスノード（PSN）（Policy Service node (PSN)）]：エンドユーザーポータルは PSN で実行する必要があります。ここでは、ネットワークアクセス、クライアントプロビジョニング、ゲストサービス、ポスチャ、およびプロファイリングを含むすべてのセッショントラフィックが処理されます。PSN がノードグループに含まれる場合、1 つのノードで障害が発生すると、他のノードが障害を検出し、保留中のセッションをリセットします。
- [モニタリングノード（MnT ノード）（Monitoring node (MnT node)）]：MnT ノードは、デバイスポータル、スポンサーポータル、およびゲストポータルでのエンドユーザーおよびデバイスのアクティビティについて、データを収集、集約、およびレポートします。プライマリ MnT ノードに障害が発生すると、セカンダリ MnT ノードが自動的にプライマリ MonT ノードになります。

ゲスト アカウントとスポンサー アカウント

- **ゲストアカウント**：ゲストとは、通常、ネットワークへの一時アクセスを必要とする承認ユーザー、担当者、顧客、その他のユーザーを表します。いずれかのゲスト展開シナリオを使用して、従業員のネットワーク アクセスを許可する場合は、従業員用のゲスト アカ

ウントを使用することもできます。スポンサーポータルにアクセスして、スポンサーおよびアカウント登録ゲストによって作成されたゲスト アカウントを表示できます。

- **スポンサーアカウント**：[スポンサー（Sponsor）]ポータルを使用して、承認ユーザー用の一時アカウントを作成し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲストアカウントを作成した後、スポンサーポータルを使用してそれらのアカウントを管理し、ゲストにアカウントの詳細を提供できます。

次のユーザーがゲストアカウントを作成できます。

- **スポンサー**：管理者ポータルで、ゲストアカウントを作成し管理する[スポンサー（Sponsor）]ポータルにアクセスできる、スポンサーのアクセス権限と機能のサポートを定義できます。
- **ゲスト**：ゲストは、アカウント登録ゲストポータルに自分自身を登録することによって、独自のアカウントを作成することもできます。これらのアカウント登録ゲストは、ポータル設定に基づいて、ログイン クレデンシャルを受け取る前にスポンサーの承認が必要になる場合があります。

  ゲストは、ホットスポット ゲスト ポータルを使用してネットワークにアクセスすることもできます。このポータルでは、ゲストアカウントやユーザー名およびパスワードなどのログイン クレデンシャルを作成する必要はありません。
- **従業員**：ID ストア（Active Directory、LDAP、内部ユーザーなど）に含まれている従業員は、クレデンシャルを持つゲストポータル（Sponsored-Guest ポータルおよびアカウント登録ゲスト ポータル）が設定されている場合には、これを使用してアクセスすることもできます。

Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）ワークフローを通じてオンボーディングされたデバイスは、ゲストデバイスとして扱われず、設定されているエンドポイント ID グループは変更されません。Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）の詳細については、「Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）」を参照してください。

ゲスト アカウントが作成されると、ゲストは Sponsored-Guest ポータルを使用してネットワークにログインおよびアクセスできます。

（注） 正常なゲストフロー時、*Access-Accept* 内で、Cisco ISE はゲストアカウント有効期間の残り時間（秒単位）に設定された値を含む RADIUS Session-Timeout 属性を送信します。ただし、適切な許可プロファイルのカスタム Session-Timeout 属性は、RADIUS Session-Timeout 属性の動作よりも優先されます。

ゲスト タイプおよびユーザー ID グループ

各ゲストアカウントをゲストタイプに関連付ける必要があります。ゲストタイプを使用して、スポンサーは、ゲスト アカウントに対して、さまざまなレベルのアクセス権や、さまざまな

ネットワーク接続時間を割り当てることができます。これらのゲストタイプは、特定のネットワーク アクセス ポリシーに関連付けられます。Cisco ISE には、次のデフォルト ゲスト タイプが含まれます。

- [担当者（Contractor）]：長期間（最大1年）にわたってネットワークへのアクセスを必要とするユーザー。
- [毎日（Daily）]：1 ～ 5 日間の短期間に、ネットワーク上のリソースへのアクセスを必要とするゲスト。
- [毎週（Weekly）]：2 ～ 3 週間の間、ネットワークへのアクセスを必要とするユーザー。

ゲスト アカウントを作成する場合、特定のスポンサー グループを特定のゲスト タイプを使用するように制限することができます。このようなグループのメンバーは、そのゲストタイプに指定された機能のみを持つゲストを作成できます。たとえば、スポンサー グループ ALL_ACCOUNTS は担当者ゲスト タイプのみを使用するように設定でき、スポンサー グループ OWN_ACCOUNTS および GROUP_ACCOUNTS は日次または週次ゲスト タイプを使用するに設定できます。通常、アカウント登録ゲストポータルを使用するアカウント登録ゲストは、1日のみのアクセスを必要とするため、これらのゲストには[毎日（Daily）]のゲストタイプを割り当てることができます。

ゲスト タイプは、ゲストのユーザー ID グループを定義します。

詳細については、以下を参照してください。

- ユーザー ID グループ （1005 ページ）
- ユーザー ID グループの作成 （1017 ページ）

ゲスト タイプの作成または編集

デフォルトのゲストタイプとデフォルトのアクセス権限や設定を編集できます。または、新しいゲストタイプを作成できます。ユーザーが行う変更は、特にこのゲストタイプを使用して作成された既存のゲストアカウントに適用されます。ログインしているゲストユーザーには、ログアウトして再度ログインするまで、これらの変更はわかりません。また、ゲストタイプを複製して、同じアクセス権限を持つゲストタイプを追加で作成することもできます。

各ゲストタイプに名前、説明、およびこのゲストタイプでゲストアカウントを作成できるスポンサーグループのリストがあります。ゲストタイプに対して、アカウント登録ゲストにのみ使用すること、（任意のスポンサーグループによる）ゲストアカウントの作成には使用しないこと、などを指定できます。

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ゲストアクセス（Guest Access）]** > **[設定（Configure）]** > **[ゲストタイプ（Guest Types）]**の順に選択し、必要な詳細を入力します。

これらの設定を使用して、ネットワークにアクセスできるゲストのタイプおよびそのアクセス権限を作成します。また、ゲストタイプを作成できるスポンサーグループを指定できます。

フィールド名	使用上のガイドライン
ゲストタイプ名（**Guest type name**）	デフォルトのゲストタイプおよび作成した別のタイプと区別できるこのゲストタイプの名前を入力します（1 ～ 256 文字）。
説明（**Description**）	このゲストタイプの推奨される使用方法に関する追加情報（最大 2000 文字）を入力します（「アカウント登録ゲストに使用」、「ゲストアカウントの作成に使用禁止」など）。
言語ファイル（**Language File**）	このゲストタイプを使用してポータルに使用する言語ファイルをエクスポートまたはインポートします。
追加データの収集（**Collect Additional Data**）	ゲストの追加情報を収集するにはカスタムフィールドを選択します。 このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ゲストアクセス（Guest Access）] > [設定（Settings）] > [カスタムフィールド（Custom Fields）]**。

フィールド名	使用上のガイドライン
最大アクセス時間—アカウント有効期間の開始（**Maximum Access Time—Account Duration Starts**）	**[最初のログインから（From first login）]**：アカウントの開始時刻は、ゲストユーザーがゲストポータルに最初にログインしたときに開始され、終了時刻は指定された期間に相当します。ゲストユーザーがログインしなければ、そのアカウントはゲストアカウントの消去ポリシーによって削除されるまで、初回ログイン待ち状態のままになります。アカウント登録されたり、スポンサーが作成したりしたユーザーアカウントは、ゲストユーザーがアカウントを作成してそのアカウントにログインしたときから開始となります。 （注） **[これらの曜日および時間のみアクセスを許可（Allow access only on these days and times）]** を選択すると、ロケーションを使用して、これらの時間のコンテキスト確立します。**[最初のログインから（From First Login）]** アクセスがロケーションに基づかないようにするには、アクセス用の日付と時刻を設定しないでください。 **[スポンサーが指定した日付から（From sponsor-specified date）]**：このゲストタイプのゲストがアクセスでき、ネットワークに接続し続けることができる、最大の日数、時間または分を 1 ～ 999 で指定します。 この設定を変更した場合、変更内容はこのゲストタイプを使用して作成された既存のゲストアカウントには適用されません。
これらの曜日および時間のみアクセスを許可（**Allow access only on these days and times**）	時間範囲を入力し、曜日を選択して、このゲストタイプがいつネットワークにアクセスできるかを指定します。このゲストタイプがこれらの時間パラメータを超えて接続を維持している場合、ログアウトされます。時間範囲は、このゲストタイプを使用してゲストに割り当てられた場所で定義されたタイムゾーンに基づきます。 **+** または **-** をクリックして、アクセス時間制限を増減します。

フィールド名	使用上のガイドライン
ゲストアカウントの消去ポリシーの設定（**Configure guest account Purge Policy**）	エンドポイント消去ジョブをスケジュールできます。エンドポイントの消去スケジュールはデフォルトで有効になっており、Cisco ISE は 30 日以上経過したエンドポイントを削除します。詳細については、エンドポイントの消去の設定 （677 ページ）を参照してください。
ログイン オプション—最大同時ログイン数（**Login Options—Maximum simultaneous logins**）	このゲスト タイプが同時に実行できる最大ユーザー セッション数を入力します。
ゲストが制限を超えた場合（**When guest exceeds limit**）	**[最大同時ログイン数（Maximum simultaneous logins）]** を選択した場合は、その制限に到達した後にユーザーが接続したときに実行するアクションも選択する必要があります。 ゲストが制限を超えた場合： • 最も古い接続を切断（**Disconnect the oldest connection**） • 最も新しい接続を切断（**Disconnect the newest connection**） • **[エラーメッセージが表示されたポータル ページにユーザーをリダイレクトする（Redirect user to a portal page showing an error message）]**：設定可能な期間、エラーメッセージが表示されます。その後、セッションが切断され、ユーザーはゲストポータルにリダイレクトされます。エラーページの内容は、**[メッセージ（Messages）] > [エラーメッセージ（Error Messages）]** タブの **[ポータルページのカスタマイズ（Portal Page Customization）]** ダイアログボックスで設定します。

フィールド名	使用上のガイドライン
ゲストが登録可能な最大デバイス数（Maximum devices guests can register）	各ゲストに登録できるデバイスの最大数を入力します。そのゲストタイプのゲストに登録済みの値より小さい値を最大数として設定できます。この値は、新しく作成されたゲストアカウントにのみ適用されます。 ゲストユーザーが登録できるデバイスの最大数に達すると、次のいずれかの方法で続行できることを通知する通知が表示されます。 • デバイスリストから削除する登録済みデバイスを選択し、新しいデバイスを追加します。 • 新しいデバイスの登録に進みます。このシナリオでは、リストにある最も古い登録済みデバイスが自動的に登録解除されます。

フィールド名	使用上のガイドライン
ゲストデバイスにエンドポイントアイデンティティグループを割り当てる（**Assign Endpoint Identity Groups for Guest Devices**）	ゲストデバイス登録ワークフローにエンドポイントアイデンティティ グループを割り当てる必要があります。 対応するオプションボタンをクリックして、 **標準**エンドポイント アイデンティティ グループまたは**ダイナミック**エンドポイントアイデンティティグループというそれぞれ次のようなグループを割り当てます。 • **[標準（Standard）]**：**[アイデンティティグループ（identitygroup）]** ドロップダウンリストから、必要なエンドポイント アイデンティティグループを選択します。 • **[ダイナミック（Dynamic）]**：ダイナミックオプションを介してのみ、LDAP ユーザーグループを割り当てることができます。 ユーザーが複数のユーザーグループに属している場合、Cisco ISEは次のリストを順番にチェックし、ユーザーが一致する最初のユーザーグループ(設定されたアイデンティティグループ)に進みます。 • **[ユーザーグループ（User Group）]** ドロップダウンリストから、必要な LDAP ユーザーグループを選択します。 • **[アイデンティティグループ（identitygroup）]** ドロップダウンリストから、必要なエンドポイント アイデンティティ グループを選択します。

フィールド名	使用上のガイドライン
ゲストにゲストポータルのバイパスを許可する（**Allow guest to bypass the Guest portal**）	クレデンシャルを持つゲストのキャプティブ ポータル（Web 認証ページ）をバイパスし、有線およびワイヤレス（dot1x）サプリカントまたは VPN クライアントに認証情報を提供することでネットワークにアクセスすることをユーザーに許可します。ゲストアカウントは、[初期ログインを待機（Awaiting Initial Login）] 状態と AUP ページをバイパスして [アクティブ（Active）] 状態になります。 この設定を有効にしない場合、ユーザーは初めにクレデンシャルを持つゲストのキャプティブ ポータルを使用してログインしないと、ネットワークの他の部分にアクセスできません。
アカウント期限切れ通知—アカウント期限切れの__日前にアカウント期限切れ通知を送信する（**Account Expiration Notification—Send account expiration notification __ days before account expires**）	ゲストのアカウントが期限切れになる前にゲストに通知を送信します。期限切れの何日前、何時間前、または何分前に通知するかを指定します。
メッセージの表示言語（**View messages in**）	電子メールまたは SMS 通知の表示言語を指定します。
Eメール（**Email**）	アカウントの失効通知に使用する手段としてメールを選択します。
次のカスタマイズを使用（**Use customization from**）	別のポータルから電子メールのカスタマイズを選択します。
メッセージ（**Messages**）	アカウントの有効期限通知に使用するテキストを入力します。
テキストのコピー元（**Copy text from**）	アカウントの期限切れ通知のために別のゲスト タイプ用に作成した電子メール テキストを再利用します。
テスト電子メールの送信先（**Send test email to me at**）	自分の電子メール アドレスに送信することによって、電子メール通知が意図したとおりに表示されることを確認します。
SMS	アカウントの失効通知に使用する手段としてテキスト（SMS）を選択します。
メッセージ（**Messages**）	アカウントの有効期限通知に使用するテキストを入力します。
テキストのコピー元（**Copy text from**）	別のゲスト タイプ用に作成したテキスト メッセージを再使用します。

フィールド名	使用上のガイドライン
テスト SMS の送信先（**Send test SMS to me at**）	自分の携帯電話に送信することによって、テキスト通知が意図したとおりに表示されることを確認します。
これらのスポンサー グループはこのゲスト タイプを作成できる（**These sponsor groups can create this guest type**）	このゲスト タイプでゲスト アカウントを作成できるスポンサー グループを選択します。 このゲスト タイプの使用を無効にする場合は、いずれのスポンサー グループにも割り当てないでください。このゲスト タイプの使用を中止するには、リストされたスポンサー グループを削除します。

次のタスク

- このゲスト タイプを使用するスポンサー グループを作成または変更します。
- 該当する場合は、アカウント登録ゲスト ポータルで、このゲスト タイプをアカウント登録ゲストに割り当てます。

ゲスト タイプの無効化

ゲスト アカウントで使用されているゲスト タイプのうち、最後に残ったゲスト タイプは削除できません。使用されているゲスト タイプを削除するには、最初にそのゲスト タイプが使用できなくなることを確認します。ゲスト タイプをディセーブルにしても、そのゲスト タイプで作成したゲスト アカウントには影響しません。

次の手順で、ターゲット ゲスト タイプを準備および無効にする方法を説明します。

ステップ 1 ターゲット ゲスト タイプを使用して、スポンサーがゲストを作成するのを許可しているスポンサー グループを識別します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Configure）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー グループ（Sponsor Groups）]**。各スポンサー グループを開いて、[このスポンサー グループはこれらのゲスト タイプを使用してアカウントを作成できます（This sponsor group can create accounts using these guest types）] リストを調べます。

ステップ 2 ターゲット ゲスト タイプを割り当てるアカウント登録ポータルを識別します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Center）] > [ゲスト アクセス（Guest Access）] > [設定（Configure）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）]**。各アカウント登録ゲスト ポータルを開きます。ポータルが特定のゲスト タイプを使用している場合、[ポータル設定（Portal Settings）] を展開し、**[ゲストとしてこのポータルを使用する従業員のログイン オプションと動的エンドポイント グループ割り当ての継承元（Employees using this portal as guests inherit login options and dynamic endpoint group assignment from）]** フィールドに割り当てられたゲスト タイプを変更します。

ステップ 3 削除するゲストタイプを開き、前の手順で識別したすべてのスポンサー グループを削除します。この操作により、効果的に、すべてのスポンサーがこのゲストタイプの新しいゲストアカウントの作成を使用できなくします。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Center）]** > **[ゲストアクセス（Guest Access）]** > **[設定（Configure）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストタイプ（Guest Type）]**。

エンドポイント ユーザーの最大同時ログイン数の設定

ゲストに許可される同時ログインの最大数を設定できます。

ユーザーがゲストポータルにログインし、正常に認証されると、ユーザーがすでにログインの最大数に達しているかどうかを確認するために、ユーザーの既存のログイン数がチェックされます。その場合、ゲストユーザーはエラーページにリダイレクトされます。エラーページが表示され、セッションが停止します。そのユーザーがインターネットに再度アクセスしようとすると、ユーザーの接続はゲスト ポータルのログイン ページにリダイレクトされます。

始める前に

このポータルの許可ポリシーで使用している許可プロファイルで [アクセス タイプ（Access Type）] が *Access_Accept* に設定されていることを確認します。[アクセスタイプ（Access Type）] が *Access_Reject* に設定されている場合は、最大同時ログイン数は機能しません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストタイプ（Guest Type）]**。[ログインオプション（Login Options）] の下で、次の手順を実行します。

a) [最大同時ログイン数（Maximum simultaneous logins）] チェックボックスをオンにして、許可される同時ログインの最大数を入力します。

b) [ゲストが制限を超えた場合（When guest exceeds limit）] の下で、[最も新しい接続を切断（Disconnect the newest connection）] オプションをクリックします。

c) [エラーメッセージを表示するポータルページにユーザーをリダイレクトする（Redirect user to a portal page showing an error message）] チェックボックスをオンにします

ステップ 2 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** を選択して認証プロファイルを作成します。

a) [共通タスク（Common Tasks）] で、[Web リダイレクション（Web Redirection）] をオンにし、次の手順を実行します。

- 最初のドロップダウンで、[中央集中Web認証（Centralized Web Auth）] を選択します。
- 前提条件の一部として作成した **ACL** を入力します。
- [値（Value）] の場合、リダイレクト先のゲスト ポータルを選択します。

b) [共通タスク（Common Tasks）] で下にスクロールし、[再認証（Reauthentication）] チェックボックスをオンにして、次の手順を実行します。

- [タイマー（Timer）] に、ユーザーがゲスト ポータルにリダイレクトされる前にエラー ページが表示される時間を入力します。
- [再認証中に接続を維持（Maintain Connectivity During Reauthentication）] で、[デフォルト（Default）] を選択します。

ステップ 3 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]**。属性 NetworkAccess.SessionLimitExceeded が true の場合にユーザーがポータルにリダイレクトされるように、認証ポリシーを作成します。

次のタスク

[ポータルページのカスタマイズ（Portal Page Customization）] タブでエラーページのテキストをカスタマイズできます。[メッセージ（Messages）] > [エラーメッセージ（Error Messages）] を選択し、エラーメッセージキー *ui_max_login_sessions_exceeded_error* のテキストを変更します。

期限切れのゲスト アカウントを消去するスケジューリング設定

アクティブなまたは一時停止されたゲストアカウントがアカウント有効期間（スポンサーがアカウントを作成するときに定義）の終了に達すると、そのアカウントは失効します。ゲストアカウントが期限切れになった場合、影響を受けるゲストはネットワークにアクセスできません。スポンサーは、期限切れになったアカウントを、消去される前に延長することができます。ただし、アカウントが消去された場合、スポンサーは、新しいアカウントを作成する必要があります。

期限切れになったゲストアカウントが消去された場合、関連するエンドポイントおよびレポート情報とロギング情報は保持されます。

Cisco ISE は、デフォルトで 15 日ごとに期限切れになったゲスト アカウントを自動的に消去します。[次回消去日（Date of next purge）] は、次の消去の発生時期を示します。次のことも実行できます。

- X 日ごとに消去が行われるようにスケジュール設定します。最初の消去は X 日後の**消去の時刻**に行われ、その後消去は X 日ごとに行われます。
- X 週間ごとに特定の曜日に消去が行われるようにスケジュール設定します。最初の消去は次のその**曜日**の**消去の時刻**に行われ、その後消去は設定された週数おきにその曜日と時刻に行われます。たとえば、月曜日に、5 週間おきに木曜日に消去が行われるように設定したとします。次の消去は、今から 5 週間後の木曜日ではなく、その週の木曜日に行われます。
- [今すぐ消去（Purge Now）] をクリックして、ただちに消去を行います。

消去が実行されるようにスケジュールされているときに Cisco ISE サーバーがダウンした場合は、消去は行われません。消去プロセスは、サーバーがその時点で動作していれば、次にスケジュールされている消去時刻に再度実行されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲストアカウント消去ポリシー（Guest Account Purge Policy）]**。

ステップ 2 次のオプションのいずれかを選択します。

- 期限切れのゲスト アカウント レコードを即時に消去するには、[今すぐ消去（Purge Now）] をクリックします。
- 消去をスケジュールするには、[期限切れのゲスト アカウントの消去のスケジュール（Schedule purge of expired guest accounts）] をオンにします。

（注） 各消去の完了後に、[次回消去日（Date of next purge）] が次にスケジュールされている消去に合わせてリセットされます。

ステップ 3 [経過後にポータル ユーザー情報を期限切れにする（Expire portal-user information after）] で、ユーザーを期限切れにするための非アクティブ日数を指定します。この設定により、使用されていない LDAP および Active Directory アカウントが ISE データベースに無期限に残ることを防ぎます。

最初のログインが行われない場合、指定された期間の終了時にゲスト アカウントが期限切れ状態になり、設定された消去ポリシーに基づいて消去されます。

また、期限切れになったゲストアカウントを消去する必要がある頻度（日数または週数）を指定することもできます。[_ 週ごとに消去（Purge occurs every _ weeks）] オプションを選択した場合は、期限切れのアカウントを消去する日時も指定できます。

ステップ 4 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

ゲスト アカウント作成用のカスタム フィールドの追加

ゲスト アクセスを提供する場合、名前、電子メール アドレス、電話番号以外の情報をゲストから収集する必要がある場合があります。Cisco ISE には、会社のニーズに固有の、ゲストに関する追加情報の収集に使用できるカスタム フィールドが用意されています。ゲスト タイプおよびアカウント登録ゲスト ポータルとスポンサー ポータルにカスタム フィールドを関連付けることができます。Cisco ISE はデフォルトのカスタム フィールドを提供しません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ゲストアクセス（Guest Access）] > [設定（Settings）] > [カスタムフィールド（Custom Fields）]**。

ステップ 2 [カスタム フィールド名（Custom Field Name）] に入力し、ドロップダウン リストから**データ タイプ**を選択し、カスタム フィールドに関する追加情報を提供するのに役立つ**ヒント テキスト**を入力します。たとえ

ば、Date of Birth と入力し、[Date-MDY] を選択して、日付形式に関するヒントとして MM/DD/YYYY を入力します。

ステップ 3 [追加（Add）] をクリックします。

カスタム フィールドがリストにアルファベット順またはソート順序のコンテキストで表示されます。

ステップ 4 [保存（Save）]をクリックします。設定の更新を保存しない場合は、[リセット（Reset）]をクリックして、最後に保存した値に戻します。

（注） カスタム フィールドを削除すると、ゲスト タイプの [カスタム フィールド（Custom Fields）] リスト、およびアカウント登録ゲスト ポータルとスポンサー ポータルの設定で選択できなくなります。フィールドが使用されている場合、[削除（Delete）] は無効になります。

次のタスク

目的のカスタム フィールドを含めることが可能です。

- そのゲスト タイプで作成されたアカウントにこの情報が含まれるようにゲスト タイプを定義する場合。「ゲスト タイプの作成または編集」を参照してください。
- ゲストアカウントの作成時にスポンサーが使用するスポンサー ポータルを設定する場合。スポンサー ポータルのカスタマイズ （872 ページ）を参照してください。
- アカウント登録ゲスト ポータルを使用してアカウント登録ゲストからの情報を要求する場合。「アカウント登録ゲスト ポータルの作成 （851 ページ）」を参照してください。

電子メールでの通知用の電子メール アドレスおよび SMTP サーバーの指定

Cisco ISE では、スポンサーおよびゲストに、情報と手順を通知する電子メールを送信できます。これらの電子メールでの通知を配信するように SMTP サーバーを設定できます。また、ゲストに通知を送信する電子メール アドレスを指定できます。

（注） ゲスト通知には、UTF-8 に互換性がある電子メール クライアントが必要です。

シングル クリック スポンサーの承認機能を使用するには、HTML 対応の電子メール クライアント（機能を有効にする）が必要です。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲスト電子メールの設定（Guest Email Settings）]**。

ステップ 2 [ゲストへの電子メール通知を有効にする（Enable email notifications to guests）] はデフォルトでオンになっています。この設定を無効にした場合、ゲストは、ゲスト ポータルとスポンサー ポータルの設定中に有効にした他の設定に関係なく、電子メールでの通知を受信しません。

ステップ 3 ゲストに電子メールでの通知を送信するために指定されている [デフォルトの送信元メールアドレス（Default “From” email address）] を入力します。たとえば、donotreply@*yourcompany*.com と入力します。

ステップ 4 次のいずれかを実行します。

- ゲストのアカウントを作成したスポンサーからの通知をゲストが受信するようにする場合は、[スポンサーの電子メールアドレスから通知を送信する（スポンサードの場合）（Send notifications from sponsor's email address (if sponsored)）] をオンにします。アカウント登録ゲストは、デフォルトの電子メール アドレスから通知を受信します。
- ゲストがスポンサードかアカウント登録かに関係なく通知を受信するようにする場合は、[常にデフォルトの電子メール アドレスから通知を送信する（Always send notifications from the default email address）] をオンにします。

ステップ 5 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

ゲストのロケーションおよび SSID の割り当て

ゲスト ロケーションはタイム ゾーンの名前を定義し、ゲストにログインした時間関連設定を適用するために ISE によって使用されます。ゲスト ロケーションは、ゲスト アカウントを作成するスポンサー、およびアカウント登録ゲストによってゲストアカウントに割り当てられます。デフォルトのゲスト ロケーションは San Jose です。他のゲスト ロケーションが追加されていない場合、すべてのアカウントにこのゲスト ロケーションが割り当てられます。1 つ以上の新しいロケーションを作成しないと、San Jose のゲスト ロケーションは削除できません。すべてのゲストが San Jose と同じタイムゾーンにいる場合を除き、必要なタイムゾーンで少なくとも 1 つのゲスト ロケーションを作成します。

（注） ゲスト アクセスの時間は、ゲスト ロケーションのタイム ゾーンに基づきます。ゲスト ロケーションのタイム ゾーンがシステムのタイム ゾーンと一致しないと、ゲスト ユーザーはログインできなくなることがあります。この場合、ゲスト ユーザーには「認証に失敗しました（Authentication Failed）」エラーが表示されることがあります。デバッグ レポートに「ゲストのアクティブ時間はまだ開始していません（Guest active time period not yet started）」というエラー メッセージが表示されることがあります。回避策として、[アカウントの管理（Manage Accounts）] オプションを使用して、ゲスト ユーザーのローカル タイム ゾーンに一致するようにゲストのアクセス開始時刻を調整できます。

ここで追加する SSID はスポンサー ポータルで使用できるため、スポンサーは接続する SSID をゲストに伝えることができます。

ゲスト ロケーションまたは SSID がスポンサー ポータルで設定されている場合、またはゲスト アカウントに割り当てられている場合は、削除できません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ポータルとコンポーネント（Portals & Components）] > [設定（Settings）] > [ゲスト ロケーションおよび SSID（Guest Locations and SSIDs）]**。

ステップ 2 [ゲスト ロケーション（Guest Locations）] :

a) サポートが必要な各タイムゾーンに対し、[ロケーション名（Location name）] に入力し、ドロップダウン リストから [タイムゾーン（Time zone）] を選択します。

b) [追加（Add）] をクリックします。

（注） ゲスト ロケーションでは、場所の名前、タイム ゾーンの名前、および GMT オフセットはスタティックであり、これらを変更できません。GMT オフセットは夏時間の変更によって変更されません。GMT オフセットは、リストに表示されているオフセットとは逆です。たとえば、*Etc/GMT+3* は実際には GMT-3 です。

（注） 初回ログインのゲスト タイプの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト タイプ（Guest Types）]** ページでアクセス時間制限を設定する場合にのみ、ゲスト ロケーション（タイム ゾーン）を設定することを確認してください。

ステップ 3 [ゲスト SSID（Guest SSIDs）] :

a) ゲスト ロケーションでゲストが使用できるネットワークの **SSID** 名を入力します。

b) [追加（Add）] をクリックします。

ステップ 4 [保存（Save）]をクリックします。最後に保存した値に戻すには、[リセット（Reset）]をクリックします。

次のタスク

新しいゲスト ロケーションまたは SSID を追加すると、次のことが可能になります。

- スポンサーがゲスト アカウントを作成するときに使用できる SSID を提供します。スポンサー ポータルのポータル設定 （911 ページ）を参照してください。
- スポンサーグループにゲストロケーションを追加して、ゲストアカウントの作成時にそのグループに割り当てられたスポンサーが使用できるようにします。スポンサー グループの設定 （862 ページ）を参照してください。
- アカウント登録ゲスト ポータルを使用してアカウント登録ゲストに使用可能なゲスト ロケーションを割り当てます。アカウント登録ゲスト ポータルの作成 （851 ページ）を参照してください。
- 既存のゲスト アカウントの場合は、アカウントを手動で編集して SSID またはロケーションを追加します。

ゲスト パスワード ポリシーのルール

Cisco ISE には、ゲスト ユーザー パスワードについて次の組み込みルールがあります。

- ゲスト パスワード ポリシーは、スポンサー ポータル、アカウント登録ポータル、CSV ファイルでアップロードされたアカウント、ERS API を使用して作成されたパスワード、およびユーザーが作成したパスワードに適用されます。
- ゲスト パスワード ポリシーに対する変更は、ゲスト パスワードの期限が切れて変更が必要になるまで、既存のアカウントに影響しません。
- パスワードは大文字・小文字の区別をします。
- 特殊文字（<、>、/、スペース、カンマ、%）を使用することはできません。
- 最小長および最小必須文字数は、すべてのパスワードに適用されます。
- パスワードとユーザー名を同じにすることはできません。
- 新規パスワードと既存パスワードを同じにすることはできません。
- ゲストアカウントの期限切れとは異なり、ゲストはパスワードが期限切れになる前に通知を受信しません。ゲスト パスワードが期限切れになった場合は、スポンサーがパスワードをランダム パスワードにリセットするか、ゲストが現在のログイン クレデンシャルを使用してログインしてからパスワードを変更することができます。

（注） ゲストのデフォルト ユーザー名は 4 文字の英字からなり、パスワードは 4 文字の数字からなります。短期間のゲストには、短く覚えやすいユーザー名とパスワードが適切です。必要に応じて ISE でユーザー名とパスワードの長さを変更できます。

ゲスト パスワード ポリシーと有効期限の設定

すべてのゲスト ポータルのパスワード ポリシーを定義できます。ゲスト パスワード ポリシーは、すべてのゲストアカウントのパスワードの生成方法を決定します。パスワードはアルファベット、数字、特殊文字を組み合わせて作成することができます。また、ゲスト パスワードが期限切れになるまでの日数を設定し、ゲストにパスワードのリセットを要求することができます。

ゲスト パスワード ポリシーは、スポンサー ポータル、アカウント登録ポータル、CSV ファイルでアップロードされたアカウント、ERS API を使用して作成されたパスワード、およびユーザーが作成したパスワードに適用されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲストパスワードポリシー（Guest Password Policy）]**。

ステップ 2 ゲスト パスワードの [最小パスワード長（Minimum password length）]（文字数）を入力します。

ステップ 3 パスワードの作成にゲストが使用できる各文字セットの文字を指定します。

[許可される文字数と最小値（Allowed Characters and Minimums）] で次のいずれか 1 つのオプションを選択して、ゲスト用のパスワード ポリシーを指定します。

- 各文字セットのすべての文字を使用します。
- 特定の文字の使用を防止するには、ドロップダウン メニューから [カスタム（Custom）] を選択し、その文字を事前定義済みの完全なセットから削除します。

ステップ 4 各セットから、使用する最小文字数を入力します。

4つの文字セットの必須文字数の合計が、全体の**最小パスワード長**を超えないようにする必要があります。

ステップ 5 [パスワードの有効期限（Password Expiration）] で、次のオプションのいずれかを選択します。

- 最初にログインしてからゲストがパスワードを変更する必要がある頻度（日数）を指定します。期限切れになる前にゲストがパスワードをリセットしないと、次回に元のログイン クレデンシャルを使用してネットワークにログインするときに、パスワードを変更するように促されます。
- パスワードを無期限に設定します。

ステップ 6 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

次のタスク

パスワード要件を提示するためのパスワード ポリシーに関連したエラー メッセージをカスタマイズする必要があります。

1. **[ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [Sponsored-Guest ポータル（Sponsored-Guest Portals）] または [アカウント登録ゲスト ポータル（Self-Registered Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [エラー メッセージ（Error Messages）]** を選択します。
2. キーワード policy を検索します。

ゲスト ユーザー名ポリシーのルール

Cisco ISE には、ゲスト ユーザー名ポリシーについて次の組み込みルールがあります。

- ゲスト ユーザー名ポリシーに対する変更は、ゲスト アカウントの期限が切れて変更が必要になるまで、既存のアカウントに影響しません。
- 特殊文字（<、>、/、スペース、カンマ、%）を使用することはできません。
- 最小長および最小必須文字数は、電子メール アドレスに基づいたユーザー名を含め、すべてのシステム生成ユーザー名に適用されます。
- パスワードとユーザー名を同じにすることはできません。

ゲスト ユーザー名ポリシーの設定

ゲストユーザー名の作成方法に関するルールを設定できます。生成されるユーザー名は、電子メール アドレスに基づいて、またはゲストの姓と名に基づいて作成できます。またスポンサー

は、ランダムな数のゲストアカウントを作成し、複数のゲストを作成する場合、またはゲストの名前と電子メールアドレスが利用できない場合に時間を短縮することもできます。ランダムに生成されたゲストユーザー名は、アルファベット、数字、および特殊文字の組み合わせから成ります。これらの設定は、すべてのゲストに影響します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲストユーザー名ポリシー（Guest Username Policy）]**。

ステップ 2 ゲスト ユーザー名の [ユーザー名の最小長（Minimum username length）]（文字数）を入力します。

ステップ 3 [既知のゲストのユーザー名基準（Username Criteria for Known Guests）] で次のいずれか 1 つのオプションを選択して、既知のゲストのユーザー名を作成するためのポリシーを指定します。

ステップ 4 [ランダムに生成されるユーザー名で使用できる文字（Characters Allowed in Randomly-Generated Usernames）] で次のいずれか 1 つのオプションを選択して、ゲストのランダム ユーザー名を作成するためのポリシーを指定します。

- 各文字セットのすべての文字を使用します。
- 特定の文字の使用を防止するには、ドロップダウン メニューから [カスタム（Custom）] を選択し、その文字を事前定義済みの完全なセットから削除します。

ステップ 5 各セットから、使用する最小文字数を入力します。

3 つの文字セットからの合計文字数は、[ユーザー名の最小長（Minimum username length）] に指定されている数を超えないようにする必要があります。

ステップ 6 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

次のタスク

ユーザー名要件を提示するためのユーザー名ポリシーに関連したエラー メッセージをカスタマイズする必要があります。

1. **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [Sponsored-Guest ポータル（Sponsored-Guest Portal）]、[アカウント登録ゲスト ポータル（Self-Registered Guest Portals）]、[スポンサー ポータル（Sponsor Portals）]、または [デバイス ポータル（My Devices Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [エラー メッセージ（Error Messages）]** の順に選択します。
2. キーワード `policy` を検索します。

SMS プロバイダーおよびサービス

SMS サービスは、クレデンシャルを持つゲスト ポータルを使用しているゲストに SMS 通知を送信します。SMS メッセージを送信する予定がある場合は、このサービスを有効にします。可

能な限り、会社の経費を削減するために、無料の SMS サービス プロバイダーを設定および提供します。

Cisco ISE は、加入者に無料の SMS サービスを提供するさまざまなセルラー サービス プロバイダーをサポートします。Cisco ISE でサービス契約とアカウント クレデンシャルを設定せずに、これらのプロバイダーを使用できます。セルラー サービス プロバイダーには、ATT、Orange、Sprint、T-Mobile、Verizon などがあります。

また、無料の SMS サービスを提供するその他のセルラー サービス プロバイダー、または Click-A-Tell などのグローバル SMS サービス プロバイダーも追加できます。デフォルトのグローバル SMS サービス プロバイダーには、サービス契約が必要です。また、Cisco ISE のアカウント クレデンシャルを設定する必要があります。

- アカウント登録ゲストがアカウント登録フォームで無料 SMS サービス プロバイダーを選択すると、SMS 通知がログイン クレデンシャルとともに無料で送信されます。SMS サービス プロバイダーを選択しない場合は、会社が契約したデフォルトのグローバル SMS サービス プロバイダーが SMS 通知を送信します。
- 自分が作成したゲスト アカウントに対してスポンサーが SMS 通知を送信できるようにする場合は、スポンサー ポータルをカスタマイズして、使用できる適切な SMS サービス プロバイダーをすべて選択します。スポンサー ポータル用の SMS サービス プロバイダーを選択しない場合は、会社が契約したデフォルトのグローバル SMS サービス プロバイダーが SMS サービスを提供します。

SMS プロバイダーは、Cisco ISE の SMS ゲートウェイとして設定されます。Cisco ISE からの電子メールは SMS ゲートウェイにより SMS に変換されます。SMS ゲートウェイはプロキシ サーバーの背後に配置できます。

（注） Cisco ISE SMS ゲートウェイは、JSON フォーマットの承認コードをサポートしていません。

ゲストに SMS 通知を送信するための SMS ゲートウェイの設定

次のことができるようにするには、Cisco ISE で SMS ゲートウェイを設定する必要があります。

- ログイン クレデンシャルおよびパスワード リセット手順に関する SMS 通知をスポンサーがゲストに手動で送信します。
- ゲストが、自分自身の登録に成功した後、自分のログイン資格情報が含まれた SMS 通知を自動的に受信します。
- ゲスト アカウントの期限が切れる前に実行するアクションに関する SMS 通知をゲストが自動的に受信します。

情報をフィールドに入力するときは、[USERNAME]、[PASSWORD]、[PROVIDER_ID] など、[ ] 内のすべてのテキストを、SMS プロバイダーのアカウントに固有の情報で更新する必要があります。

始める前に

[SMS 電子メール ゲートウェイ（SMS Email Gateway）] オプションに使用するデフォルト SMTP サーバーを設定します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMS ゲートウェイ（SMS Gateway）] > [SMS ゲートウェイ プロバイダー（SMS Gateway Providers）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 次の詳細情報を入力して SMS ゲートウェイを設定します。

フィールド名	使用上のガイドライン
SMS ゲートウェイ プロバイダー ドメイン（SMS Gateway Provider Domain）	プロバイダー ドメインと、ゲスト アカウントの携帯電話の番号を入力します。プロバイダーの SMS/MMS ゲートウェイにメッセージを送信するとき、前者が電子メール アドレスのホスト部として使用され、後者はユーザー部分として使用されます。
プロバイダー アカウント アドレス（Provider account address）	（オプション） アカウントアドレスを入力します。これは、電子メールの送信元アドレス（通常、アカウントアドレス）として使用され、**[ゲストアクセス（Guest Access）] > [設定（Settings）]** の [デフォルトの電子（Default Email Address）] グローバル設定を上書きします。
SMTP API 宛先アドレス（SMTP API destination address）	（オプション） Clickatell SMTP API などの、特定のアカウント受信者アドレスを必要とする SMTP SMS API を使用する場合は、SMTP API 宛先アドレスを入力します。 これは、電子メールの送信先アドレスとして使用され、メッセージ本文のテンプレートはゲストアカウントの携帯電話の番号に置き換えられます。

フィールド名	使用上のガイドライン
SMTP API 本文テンプレート（SMTP API body template）	（オプション） Clicketell SMTP API など、SMS の送信に特定の電子メール本文テンプレートを必要とする SMTP SMS API を使用する場合は、SMTP API 本文テンプレートを入力します。 サポートされる動的置換は $mobilenumber$、（形式 $YYYYMMDDHHHMISSmimi$ の）$timestamp$、および $message$ です。 URL に固有識別子が必要な SMS ゲートウェイには $timestamp$$mobilenumber$ を使用できます。

HTTP API（GET 方式または POST 方式）でゲストとスポンサーに SMS メッセージを送信するように設定するには、次の設定を使用します。

フィールド	使用上のガイドライン
URL	API の URL を入力します。 このフィールドは、符号化された URL ではありません。ゲストアカウントの携帯電話の番号は、URL に置き換えられます。サポートされる動的置換は $mobilenumber$ および $message$ です。 HTTP API で HTTPS を使用した場合、HTTPS を URL 文字列に含め、Cisco ISE にプロバイダーの信頼できる証明書をアップロードします。Cisco ISE GUI で [メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**。
データ（URL エンコード部分）（Data (Url encoded portion)）	GET 要求または POST 要求のデータ（URL エンコード部分）を入力します。 このフィールドは、符号化された URL です。デフォルトの GET 方式を使用している場合、データが上で指定した URL に付加されます。
データ部分に HTTP POST 方式を使用（Use HTTP POST method for data portion）	POST 方式を使用する場合は、このオプションをオンにします。 上で指定したデータは、POST 要求の内容として使用されます。
HTTP POST データ コンテンツ タイプ（HTTP POST data content type）	POST 方式を使用する場合は、「plain/text」や「application/xml」などのコンテンツタイプを指定します。

フィールド	使用上のガイドライン
HTTPS ユーザー名（HTTPS Username） HTTPS パスワード（HTTPS Password） HTTPS ホスト名（HTTPS Host name） HTTPS ポート番号（HTTPS Port number）	この情報を入力します。

ステップ 4 （オプション）SMSプロバイダーに送信される前にモバイル番号をフォーマットするjavascriptを追加する場合は、[モバイル番号フォーマットを有効にする（Enable Mobile Number Format）] チェックボックスをオンにします。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

新しい SMS ゲートウェイを追加すると、次のことが可能になります。

- 期限切れのアカウントに関する SMS 通知をゲストに送信するときに、SMS サービス プロバイダーを選択します。「ゲスト タイプの作成または編集」を参照してください。
- [アカウント登録（Self-Registration）] フォームでアカウント登録ゲストに示される選択肢として、SMSプロバイダーのうちのどれを表示するかを指定します。「アカウント登録ゲスト ポータルの作成 （851 ページ）」を参照してください。

アカウント登録ゲストのソーシャル ログイン

ゲストは、ゲスト ポータルにユーザー名とパスワードを入力する代わりに、アカウント登録ゲストでクレデンシャルを提供する方法としてソーシャル メディア プロバイダーを選択できます。これを有効にするには、ソーシャル メディア サイトを外部 ID ソースとして設定し、ユーザーがその外部 ID（ソーシャル メディア プロバイダー）を使用できるようにするポータルを設定します。Cisco ISE のソーシャル メディア ログインに関する追加情報は、次を参照してください。 https://community.cisco.com/t5/security-documents/how-to-configure-amp-use-a-facebook-social-media-login-on-ise/ta-p/3609532

ソーシャル メディアで認証した後、ゲストはソーシャル メディア サイトから取得した情報を編集できます。ソーシャルメディアのクレデンシャルが使用されているにもかかわらず、ソーシャルメディアサイトは、ユーザーがそのサイトの情報を使用してログインしたことを認識していません。ISE は引き続き、ソーシャルメディアサイトから取得された情報を今後の追跡のために内部的に使用します。

ユーザーがソーシャル メディア サイトから取得した情報を変更しないようにゲスト ポータルを設定したり、登録フォームの表示を抑制することもできます。

ソーシャル ログイン ゲスト フロー

ログインフローは、ポータル設定を行う方法によって異なります。ソーシャル メディアのログインは、ユーザー登録なし、ユーザー登録あり、またはユーザー登録とスポンサー承認ありで設定できます。

1. ユーザーはアカウント登録ポータルに接続し、ソーシャル メディアを使用してログインすることを選択します。アクセス コードを設定した場合、ユーザーはログイン ページにアクセス コードも入力する必要があります。
2. ユーザーは認証のためにソーシャル メディア サイトにリダイレクトされます。ユーザーは、ソーシャル メディア サイトの基本的なプロファイル情報の使用を承認する必要があります。
3. ソーシャルメディアサイトへのログインが成功すると、ISE はユーザーに関する追加情報をソーシャルメディアサイトから取得します。Cisco ISE はソーシャルメディア情報を使用してユーザーをログオンします。
4. ログイン後、設定に応じて、ユーザーは AUP を受け入れなくてはならない場合があります。
5. ログイン フローの次のアクションは設定によって異なります。
   - 登録なし：登録はバックグラウンドで行われます。Facebook はログイン用にユーザーのデバイスのトークンを Cisco ISE に提供します。
   - 登録あり：ユーザーには、ソーシャル メディア プロバイダーからの情報が事前に入力された登録フォームを完了するよう指示されます。これにより、ユーザーは不足している情報を修正および追加し、ログインのために更新された情報を提出することができます。登録フォームの設定で登録コードを設定した場合、ユーザーは登録コードも入力する必要があります。
   - 登録およびスポンサー承認あり：ユーザーにソーシャルメディア提供の情報を更新させることに加えて、ユーザーはスポンサーの承認を待たなければならないという通知を受けます。スポンサーは、アカウントの承認または拒否を要求する電子メールを受け取ります。スポンサーがアカウントを承認すると、Cisco ISE はユーザーにアクセス権を電子メール送信します。ユーザーはゲスト ポータルに接続し、ソーシャル メディア トークンで自動的にログインします。
6. 登録が成功します。ユーザーは [登録フォーム設定（Registration Form Settings）] の [アカウント登録のためゲストフォームを送信後にゲストを次の場所に誘導する（After submitting the guest form for self-registration, direct guest to）] に設定されているオプションに誘導されます。ユーザーのアカウントは、ポータルのゲスト タイプ用に設定されたエンドポイント ID グループに追加されます。
7. ゲスト アカウントが期限切れになるか、またはユーザーがネットワークから切断するまで、ユーザーはアクセス権を持ちます。

アカウントの有効期限が切れた場合、ユーザーのログインを許可する唯一の方法は、アカウントを再アクティブ化することです（そうでない場合は、アカウントを削除します）。ユーザーはログイン フローを再度実行する必要があります。

ユーザーがネットワークから切断して再接続した場合、Cisco ISE の処理は認証ルールによって異なります。ユーザーが次のような認証を取得した場合：

```
rule if guestendpoint then permit access
```

ユーザーがエンドポイント グループにまだ存在する場合、ユーザーはログオン ページにリダイレクトされます。ユーザーがまだ有効なトークンを持っている場合は、自動的にログインします。持っていない場合は、登録をやり直す必要があります。

ユーザーが現在はエンドポイントグループに所属していない場合、ユーザーはゲストページにリダイレクトされ、登録をやり直します。

ソーシャル ログイン アカウントの期間

アカウント再認証は接続方法によって異なります。

- 802.1x の場合、デフォルトの許可ルールでは、

  ```
  if guestendpoint then permit access
  ```

  ユーザーデバイスがスリープ状態になった場合、または別の建物にローミングした場合に、ゲストが再接続できるようにします。ユーザーが再接続すると、そのユーザーはゲストページにリダイレクトされ、トークンを使用して自動ログインするか、または再度登録を開始します。

- MAB では、再接続するたびにユーザーはゲストポータルにリダイレクトされ、ソーシャルメディアを再度クリックする必要があります。Cisco ISE にそのユーザーのアカウントのトークン（ゲストアカウントの有効期限が切れていない）がまだある場合は、ソーシャル メディア プロバイダーに接続する必要はなく、ログインが即座に成功します。

  すべての再接続が別のソーシャル ログインにリダイレクトされないようにするには、デバイスを記憶し、アカウントが期限切れになるまでアクセスを許可する許可ルールを設定できます。アカウントが期限切れになると、そのアカウントはエンドポイント グループから削除され、フローはゲスト リダイレクトのルールにリダイレクトされます。次に例を示します。

  ```
  if wireless_mab and guest endpoint then permit access
  if wireless_mab then redirect to self-registration social media portal
  ```

レポートとユーザー トラッキング

Cisco ISE ライブログと Facebook

- **Authentication Identity Store**：Cisco ISE のソーシャル メディア アプリケーションで作成したアプリケーションの名前です。

- **Facebook username**：Facebook によって報告されたユーザー名です。ユーザーが登録時にユーザー名を変更できるようにする場合、Cisco ISE によって報告される名前はソーシャルメディアのユーザー名です。
- **SocialMediaIdentifier**：ここでは、

  ```
  https://facebook.com/<number>
  ```

  number はソーシャルメディアユーザーを識別します。

[ISE レポート（ISE Reports）]：ゲストユーザー名は、ソーシャルメディアサイトのユーザー名です。

[Facebook 分析（Facebook Analytics）]：Facebook の分析を使用して、Facebook のソーシャルログオンを通じてゲストネットワークを使用しているユーザーを確認することができます。

[ワイヤレスと Facebook（Wireless and Facebook）]：ワイヤレスコントローラの [ユーザー名（User Name）] は、ライブログの **SocialMediaIdentifier** と同じ一意の Facebook ID です。ワイヤレス UI の設定を表示するには、**[モニター（Monitor）]** > **[クライアント（Clients）]** > **[詳細（Detail）]** を選択し、[ユーザー名（User Name）] フィールドを確認します。

ソーシャル メディアで認証されたゲストのブロック

個々のソーシャル メディア ユーザーをブロックする許可ルールを作成することができます。これは、トークンが期限切れになっていない場合に Facebook を認証に使用する際に便利です。次の例は、Facebook ユーザー名を使用してブロックされた Wi-Fi 接続のゲスト ユーザーを示します。

図 *12 : Facebook* ユーザー名を使用してブロックされた *Wi-Fi* 接続のゲストユーザー

Cisco ISE のソーシャルログインの設定については、ソーシャル ログインの設定 （838 ページ）を参照してください。

ソーシャル ログインの設定

始める前に

Cisco ISE が接続できるようにソーシャルメディアサイトを設定します。現在は Facebook のみがサポートされています。

Cisco ISE が Facebook にアクセスできるように、次の HTTPS 443 URL が NAD を介して開かれていることを確認します。

```
facebook.co
akamaihd.net
akamai.co
fbcdn.net
```

（注） Facebook のソーシャル ログイン URL は HTTPS です。すべての NAD が HTTPS URL へのリダイレクションをサポートしているわけではありません。https://communities.cisco.com/thread/79494?start=0&tstart=0&mobileredirect=trueを参照してください。

ステップ 1 Facebook で、Facebook アプリケーションを作成します。

a) https://developers.facebook.com にログオンし、開発者としてサインアップします。

b) ヘッダーで [アプリ（Apps）] を選択し、[新しいアプリの追加（Add a New App）] をクリックします。

ステップ 2 タイプが [Web] の新しい [製品（Product）]、[Facebook ログイン（Facebook Login）] を追加します。[設定（Settings）] をクリックして次の値を設定します。

- [クライアント OAuth ログイン（Client OAuth Login）] : [いいえ（NO）]
- [Web OAuth ログイン（Web OAuth Login）] : [はい（YES）]
- [Web OAuth の再認証を強制（Force Web OAuth Reauthentication）] : [いいえ（NO）]
- [組み込みブラウザ OAuth ログイン（Embedded Browser OAuth Login）] : [いいえ（NO）]
- [有効な OAuth リダイレクト URI（Valid OAuth redirect URIs）] : ISE から自動リダイレクト URL を追加します
- [デバイスからログイン（Login from Devices）] : [いいえ（NO）]

ステップ 3 [アプリレビュー（App Review）] をクリックして、[アプリは現在実行中でパブリックで利用可能です（Your app is currently live and available to the public）] に [はい（Yes）] を選択します。

ステップ 4 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [ソーシャルログイン（Social Login）]**。[追加（Add）] をクリックして、新しいソーシャルログイン外部 ID ソースを作成します。

- [タイプ（Type）] : ソーシャル ログイン プロバイダーのタイプを選択します。Facebook が現在のところ唯一の選択肢です。
- [アプリケーション ID（App ID）] : Facebook アプリケーションからアプリケーション ID を入力します。
- [アプリケーション シークレット（App Secret）] : Facebook アプリケーションからアプリケーション シークレットを入力します。

ステップ 5 Cisco ISE で、アカウント登録ポータルでの [ソーシャルメディアのログイン（Social Media Login）] を有効にします。ポータルページで、**[ポータルとページの設定（Portal & Page Settings）] > [ログインページの設定（Login Page Settings）]** を選択し、[ソーシャルログインの許可（Allow Social Login）] チェックボックスをオンにし、次の詳細を入力します。

- [ソーシャルログイン後に登録フォームを表示（Show registration form after social login）] : これにより、ユーザーは Facebook によって提供される情報を変更できます。
- [ゲストの承認が必要（Require guests to be approved）] : スポンサーがアカウントを承認する必要があることをユーザーに通知し、ログイン用のクレデンシャルを送信します。

ステップ 6 **[管理（Administration）] > [外部 ID ソース（External Identity Sources）]** を選択し、[Facebook ログイン（Facebook Login）] ウィンドウを選択して Facebook の外部 ID ソースを編集します。

これによりリダイレクト URI が作成され、これを Facebook アプリケーションに追加します。

ステップ 7 Facebook で、前のステップの URI を Facebook アプリケーションに追加します。

次のタスク

Facebook では、アプリに関するデータを表示できます。このデータには、Facebook ソーシャル ログインでのゲスト アクティビティが表示されます。

ゲスト ポータル

企業の訪問者が企業のネットワークを使用してインターネットまたはネットワーク上のリソースおよびサービスにアクセスしようとしている場合、ゲスト ポータルを使用してネットワーク アクセスを提供することができます。設定すると、従業員はゲスト ポータルを使用して会社のネットワークにアクセスできます。

3 つのデフォルトのゲスト ポータルがあります。

- [ホットスポットゲストポータル（Hotspot Guest portal）]：ネットワークアクセスはログイン情報を必要とせずに許可されます。通常、ネットワーク アクセスを許可する前にユーザー ポリシーの認可（AUP）が承認される必要があります。
- [Sponsored-Guest ポータル（Sponsored-Guest portal）]：ゲストのアカウントを作成したスポンサーによりネットワークアクセスが許可され、ゲストにログイン情報が提供されます。
- [アカウント登録ゲストポータル（Self-Registered Guest portal）]：ゲストは各自のアカウントのログイン情報を作成できます。ネットワークアクセスが付与される前に、スポンサー承認が必要となることがあります。

Cisco ISE は、事前に定義されたデフォルト ポータルなど、複数のゲスト ポータルをホストすることができます。

デフォルトのポータル テーマには、管理者ポータルからカスタマイズできる標準のシスコ ブランドが適用されています。

Wireless Setup には独自のデフォルトテーマ（CSS）があります。ロゴ、バナー、背景画像、色、フォントなどの基本的な設定の一部を変更できます。ISE では、他の設定を変更することでポータルをさらにカスタマイズでき、高度なカスタマイズを行うこともできます。

ゲスト ポータルのクレデンシャル

Cisco ISE では、ゲストにさまざまなタイプのクレデンシャルを使用したログインを要求することによって、保護されたネットワーク アクセスを提供します。ゲストがこれらのクレデンシャルの 1 つまたは組み合わせを使用してログインすることを要求できます。

- [ユーザー名（MAC Local User）]：必須。エンドユーザー ポータル（ホットスポット ゲスト ポータルを除く）を使用するすべてのゲストに適用され、ユーザー名ポリシーから取得

されます。ユーザー名ポリシーはシステムによって生成されたユーザー名のみに適用され、ゲスト API プログラミング インターフェイスまたはアカウント登録プロセスを使用して指定されたユーザー名には適用されません。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[設定（Settings）]** > **[ゲストユーザー名ポリシー（Guest Username Policy）]** で、ユーザー名に適用するポリシーを設定できます。ゲストは、電子メール、SMS、または印刷形式で、ユーザー名の通知を受け取ることができます。

- [パスワード（Password）]：必須エンドユーザー ポータル（ホットスポット ゲスト ポータルを除く）を使用するすべてのゲストに適用され、パスワード ポリシーから取得されます。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[設定（Settings）]** > **[ゲストパスワードポリシー（Guest Password Policy）]** で、パスワードに適用するポリシーを設定できます。ゲストは、電子メール、SMS、または印刷形式で、パスワードの通知を受け取ることができます。

- [アクセスコード（Access code）]：オプション。ホットスポット ゲスト ポータルおよびクレデンシャルを持つゲスト ポータルを使用するゲストに適用されます。アクセス コードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです（ホワイトボードによって視覚的に、またはロビー アンバサダーにより口頭で）。ネットワークにアクセスするために、屋外にいる誰かに知られたり使用されたりすることはありません。アクセス コードの設定を有効にした場合、次のようになります。

  - スポンサー付きゲストは、[ログイン（Login）]ページで（ユーザー名およびパスワードとともに）これを入力するよう求められます。

  - ホットスポット ゲスト ポータルを使用するゲストは、[利用規定（Acceptable Use Policy (AUP)）] ページでこれを入力するよう求められます。

- [登録コード（Registration code）]：オプション。アカウント登録ゲストに適用され、アカウント登録ゲストに提供される方法においてアクセス コードと似ています。登録コード設定が有効な場合、アカウント登録ゲストはアカウント登録フォームでこれを入力するよう求められます。

ユーザー名とパスワードは、社内のスポンサーが（スポンサー付きゲストに対して）提供できます。または、ゲストが自分自身を登録してこれらのクレデンシャルを取得できるように、クレデンシャルを持つゲスト ポータルを設定できます。

（注） ゲストポータルでユーザーエントリの一括インポートを実行する場合は、電話番号が E.164 形式で指定されていることを確認します。さらに、Excel ファイルで電話番号列の形式が [テキスト（Text）] に設定されていることを確認します。

関連トピック

ゲスト タイプおよびユーザー ID グループ （813 ページ）

ホットスポット ゲスト ポータルを使用したゲスト アクセス

Cisco ISE にはネットワーク アクセス機能があり、その機能には「ホットスポット」が含まれています。これは、アクセスポイントで、ゲストはこれを使用してログインにクレデンシャルを必要とすることなくインターネットにアクセスできます。ゲストがコンピュータまたはWebブラウザを搭載した任意のデバイスでホットスポット ネットワークに接続して、Web サイトに接続しようとすると、自動的にホットスポット ゲスト ポータルにリダイレクトされます。この機能では、有線接続と無線接続（Wi-Fi）の両方がサポートされます。

ホットスポット ゲスト ポータルは代替となるゲスト ポータルで、これを使用すると、ゲストにユーザー名とパスワードを要求することなく、ネットワーク アクセスを提供することができ、ゲスト アカウントを管理する必要性が軽減されます。代わりに、ゲスト デバイスにネットワーク アクセスを直接提供するために、Cisco ISE はネットワーク アクセス デバイス（NAD）およびデバイス登録 Web 認証（デバイス登録 WebAuth）とともに動作します。場合によって、ゲストは、アクセス コードを使用してログインするよう要求されることがあります。通常、これは社内に物理的に存在しているゲストにローカルに提供されるコードです。

ホットスポット ゲスト ポータルをサポートしている場合：

- ホットスポット ゲスト ポータルの設定に基づいて、ゲスト アクセスの条件を満たしている場合、ゲストにネットワーク アクセスが付与されます。
- Cisco ISE によってデフォルトのゲスト ID グループ GuestEndpoints が提供され、これを使用して、ゲスト デバイスを一元的に追跡できます。

クレデンシャルを持つゲスト ポータルを使用したゲスト アクセス

クレデンシャルを持つゲスト ポータルを使用して、外部ユーザーの内部ネットワークおよびサービスと、インターネットへの一時アクセスを識別し許可することができます。スポンサーは、ポータルの [ログイン（Login）] ページでこれらのクレデンシャルを入力することによって、ネットワークにアクセスできる承認ユーザーの一時的なユーザー名およびパスワードを作成できます。

次のように取得したユーザー名とパスワードを使用してゲストがログインできるように、クレデンシャルを持つゲスト ポータルを設定できます。

- スポンサーから付与されます。このゲスト フローでは、ゲストは、社内に入って個人のゲスト アカウントで設定されたとき、ロビー アンバサダーなどのスポンサーによるグリーティングを受け取ります。
- オプションの登録コードまたはアクセス コードを使用して自分自身を登録した後に付与されます。このゲスト フローでは、ゲストは人間の介入なしでインターネットにアクセスでき、これらのゲストにコンプライアンスに使用可能な一意の識別子があることが Cisco ISE によって保証されます。
- オプションの登録コードまたはアクセス コードを使用して自分自身を登録した後に付与されます。ただし、ゲスト アカウントの要求がスポンサーによって承認された後のみです。

このゲストフローでは、ゲストにネットワークへのアクセスが提供されますが、追加のスクリーニング レベルが実行された後でのみ提供されます。

また、ログイン時にユーザーに新しいパスワードを入力するよう強制できます。

Cisco ISE では、複数のクレデンシャルを持つゲスト ポータルを作成し、これを使用してさまざまな基準に基づいてゲストアクセスを許可することができます。たとえば、日次訪問者に使用されるポータルとは別の、月次担当者向けのポータルを設定できます。

クレデンシャルを持つゲスト ポータルを使用した従業員アクセス

従業員は、そのポータルに設定された ID ソース順序でクレデンシャルにアクセスできれば、従業員クレデンシャルを使用してサインインすることによって、クレデンシャルを持つゲストポータルを使用してネットワークにアクセスすることもできます。

ゲスト デバイスのコンプライアンス

ゲストおよび非ゲストがクレデンシャルを持つゲストポータルを介してネットワークにアクセスした場合、アクセスを許可する前に、そのデバイスのコンプライアンスをチェックすることができます。ゲストおよびゲスト以外を[クライアントプロビジョニング（Client Provisioning）]ウィンドウにルーティングして、最初にポスチャエージェントをダウンロードするよう要求することができます。このエージェントは、ポスチャプロファイルを確認し、デバイスが準拠しているかどうかを検証します。これは、クレデンシャルを持つゲストポータルで、[ゲストデバイスのコンプライアンス設定（Guest Device Compliance Settings）] のオプションを有効にすることで実行できます。これによって、[クライアントプロビジョニング（Client Provisioning）]ウィンドウがゲストフローの一部として表示されます。

（注） ゲストフローのクライアントポスチャ アセスメントは、テンポラルエージェントのみをサポートしています。

クライアント プロビジョニング サービスでは、ゲストのポスチャ評価および修復が提供されます。クライアントプロビジョニング ポータルは、中央 Web 認証（CWA）のゲスト展開でのみ使用できます。ゲスト ログイン フローによって CWA が実行され、クレデンシャルを持つゲスト ポータルは、利用規定やパスワード変更のチェックを実行した後、クライアント プロビジョニング ポータルにリダイレクトされます。いったんポスチャが評価されると、ポスチャ サブシステムはネットワーク アクセス デバイスに対して許可変更（CoA）を実行し、クライアント再接続を再認証します。

ゲスト ポータルの設定タスク

デフォルトポータルと、証明書、エンドポイントID グループ、ID ソース順序、ポータルテーマ、イメージ、および Cisco ISE によって提供されるその他の詳細などのデフォルト設定を使用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合

うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

新しいポータルを作成したり、デフォルトポータルを編集した後は、ポータルの使用を承認する必要があります。いったんポータルの使用を承認すると、後続の設定変更はただちに有効になります。

ポータルを削除する場合は、関連付けられている許可ポリシールールおよび許可プロファイルを先に削除するか、別のポータルを使用するように変更する必要があります。

さまざまなゲストポータルの設定に関連するタスクについては、この表を参照してください。

タスク	ホットスポットゲストポータル	Sponsored-Guest ポータル	アカウント登録ゲストポータル
ポリシーサービスの有効化 （845 ページ）	必須	必須	必須
ゲストポータルの証明書の追加 （845 ページ）	必須	必須	必須
外部 ID ソースの作成（845 ページ）	N/A	必須	必須
ID ソース順序の作成（847 ページ）	N/A	必須	必須
エンドポイント ID グループの作成 （1294 ページ）	必須	不要（ゲストタイプによって定義される）	不要（ゲストタイプによって定義される）
ホットスポットゲストポータルの作成 （848 ページ）	必須	N/A	N/A
Sponsored-Guest ポータルの作成 （849 ページ）	N/A	必須	N/A
アカウント登録ゲストポータルの作成 （851 ページ）	N/A	N/A	必須
ポータルの許可 （856 ページ）	必須	必須	必須
ゲストポータルのカスタマイズ （857 ページ）	オプション	オプション	オプション

ポリシー サービスの有効化

Cisco ISE エンドユーザー Web ポータルをサポートするには、ホストするノードでポータルポリシーサービスを有効にする必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 2 ノードをクリックして、[編集（Edit）] をクリックします。

ステップ 3 [全般設定（General Settings）] タブで [ポリシーサービス（Policy Service）] トグルボタンを有効にします。

ステップ 4 [セッションサービスの有効化（Enable Session Services）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

ゲスト ポータルの証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループ タグに割り当てることができます。すべてのエンドユーザー Web ポータルに使用されるデフォルトの証明書グループ タグは [デフォルト ポータル証明書グループ（Default Portal Certificate Group）] です。

ステップ 1

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]**。

ステップ 3 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。

この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。

ステップ 4 **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成または編集（Create or Edit）] > [ポータル設定（Portal Settings）]** の順に選択します。

ステップ 5 新しく追加された証明書に関連付けられた [証明書グループ タグ（Certificate group tag）] ドロップダウン リストから特定の証明書グループ タグを選択します。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバーなどの外部 ID ソースに接続して、認証/許可のユーザー情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザー ID を受信して共有できるようにするパッシブ ID サービスを使用するには、その他の パッシブ ID サービス プロバイダー （1094 ページ）を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。
- Active Directory：外部 ID ソースとして Active Directory に接続する場合。詳細については、外部 ID ソースとしての Active Directory （1028 ページ）を参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、LDAP （1142 ページ）を参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバーを追加する場合。詳細については、RADIUS トークン ID ソース （1169 ページ）を参照してください。
- RSA SecurID：RSA SecurID サーバーを追加する場合。詳細については、RSA ID ソース （1176 ページ）を参照してください。
- SAML IDプロバイダー（SAML Id Providers）：Oracle Access Manager などの ID プロバイダー（IdP）を追加する場合。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダー （1185 ページ）を参照してください。
- ソーシャルログイン（Social Login）：Facebook などのソーシャルログインを外部 ID ソースとして追加する場合。詳細については、アカウント登録ゲストのソーシャル ログイン （834 ページ）を参照してください。

認証用の SAML IDP ポータルにリダイレクトするためのゲスト ポータルの設定

ゲスト ポータルを設定して、ユーザーが認証のために SAML IDP ポータルにリダイレクトされるようにすることができます。

ゲストポータルで [ログインに次の ID プロバイダーゲストポータルの使用を許可（Allow the following identity-provider guest portal to be used for login）] オプションを設定することで、そのポータルで新しいログイン領域が有効になります。ユーザーがそのログイン オプションを選択した場合、代替 ID ポータルにリダイレクトされてから（表示されません）、認証のために SAML IDP ログオン ポータルにリダイレクトされます。

たとえば、ゲスト ポータルには従業員ログインのためのリンクがある場合があります。既存のポータルにログインする代わりに、ユーザーは従業員ログオン リンクをクリックし、SAML IDP シングル サインオン ポータルにリダイレクトされます。従業員はこの SAML IDP による最後のログオンからのトークンを使用して再接続されるか、その SAML サイトでログインします。これにより、同じポータルでシングル SSID からゲストと従業員の両方を扱うことができます。

次の手順は、SAML IDP を認証用に使用するように設定されている別のポータルを呼び出すゲスト ポータルを設定する方法を示しています。

ステップ 1 外部 ID ソースを設定します。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダー （1185 ページ）を参照してください。

ステップ 2 SAML プロバイダーのゲスト ポータルを作成します。ポータル設定で [認証方式（Authentication method）] を SAML プロバイダーに設定します。ユーザーにはこのポータルは表示されず、これは単にユーザーを SAML IDP ログオン ページにつなぐためのプレースホルダです。次に説明するように、他のポータルをこのサブポータルにリダイレクトするように設定できます。

ステップ 3 作成したばかりの SAML プロバイダー ポータルのゲスト ポータルにリダイレクトするためのオプションを備えたゲスト ポータルを作成します。これはメイン ポータルで、サブポータルにリダイレクトします。

SAML プロバイダーに見えるように、このポータルの外観をカスタマイズする場合もあります。

a) メイン ポータルの [ログイン ページの設定（Login Page Settings）] で、[ログインに次の ID プロバイダー ゲスト ポータルの使用を許可（Allow the following identity-provider guest portal to be used for login）] にマークを付けます。

b) SAML プロバイダーと使用するために設定したゲスト ポータルを選択します。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲストユーザーがローカル WebAuth を使用して認証できるようにするには、ゲストポータル認証ソースと ID ソース順序の両方に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）]** を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リストフィールドの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストフィールドのデータベースを並べ替えます。

ステップ 6 選択したアイデンティティストアに認証のためにアクセスできない場合は、[高度な検索リスト（Advanced Search List）] 領域で次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus属性をProcessErrorに設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]
- [ユーザーが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]

  Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストフィールドに Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイントIDグループ（Endpoint Identity Groups）] ウィンドウでは、追加のエンドポイント ID グループも作成できます。作成したエンドポイント ID グループを編集または削除できます。システムで定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集または削除することはできません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するエンドポイント ID グループの [名前（Name）] に入力します（エンドポイント ID グループの名前にはスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの [説明（Description）] に入力します。

ステップ 5 [親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

ホットスポット ゲスト ポータルの作成

ホットスポット ゲスト ポータルを提供して、ゲストが、ログインにユーザー名とパスワードを要求されずにネットワークに接続できるようにすることができます。ログイン時にアクセスコードが必要な場合があります。

新しいホットスポット ゲスト ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのホットスポット ゲスト ポータルを削除できます。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、ゲストフロー図のグラフィカルフローに反映されます。AUP ページなどのページを有効にすると、そのページがフローに表示され、ゲストはポータルで使用できるようになります。無効にすると、フローから削除され、次に有効なページがゲストに表示されます。

[認証成功の設定（Authentication Success Settings）] を除くすべてのページ設定は、任意です。

始める前に

- このポータルで使用するために、必要な証明書とエンドポイント ID グループが設定されていることを確認します。
- ゲストがホットスポットポータルのために接続する WLC が Cisco ISE でサポートされていることを確認します。お使いのバージョンの Cisco ISE の『Identity Services Engine Network Component Compatibility』ガイドを参照してください。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

Sponsored-Guest ポータルの作成

Sponsored-Guest ポータルを提供して、指定されたスポンサーがゲストにアクセスを許可できるようにすることができます。

新しい Sponsored-Guest ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含む、任意の Sponsored-Guest ポータルを削除できます。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、ゲストフロー図のグラフィカルフローに反映されます。AUP ページなどのページを有効にすると、そのページがフローに表示され、ゲストはポータルで使用できるようになります。無効にすると、フローから削除され、次に有効なページがゲストに表示されます。

次のすべてのページ設定によって、ゲスト用の利用規定（AUP）を表示し、その同意を要求することができます。

- ログイン ページの設定（Login Page Settings）
- 利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）
- BYOD 設定（BYOD Settings）

始める前に

このポータルで使用するために、必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）]**。

ステップ 2 新しいポータルを作成する場合は、[ゲスト ポータルの作成（Create Guest Portal）] ダイアログ ボックスで、ポータル タイプとして [Sponsored-Guest ポータル（Sponsored-Guest Portal）] を選択し、[続行（Continue）] をクリックします。

ステップ 3 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザー ポータルに使用されていないことを確認します。

ステップ 4 [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 5 [ポータル設定（Portal Settings）] でポート、イーサネット インターフェイス、証明書グループ タグ、ID ソース順序、認証方式などのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 特定のページのそれぞれに適用される次の設定を更新してください。

- [ログインページの設定（Login Page Settings）]：ゲストクレデンシャルおよびログインガイドラインを指定します。[ゲストが自分のアカウントを作成することを許可する（Allow guests to create their accounts）] オプションを選択した場合、ユーザーは独自のゲスト アカウントを作成できます。このオプションが選択されていない場合は、スポンサーがゲスト アカウントを作成する必要があります。

  （注） [認証方式（Authentication Method）] フィールドで ID プロバイダー IdP）を選択している場合は、[ログインページ設定（Login Page Settings）] オプションは無効です。

- [アクセプタブル ユース ポリシー（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]：別の AUP ページを追加し、クレデンシャルを持つゲストポータルを使用する従業員を含むゲスト用のアクセプタブル ユース ポリシーの動作を定義します。
- [従業員のパスワード変更の設定（Employee Change Password Settings）]：初めてログインした後にパスワードを変更するようにゲストに要求します。
- [ゲストデバイス登録の設定（Guest Device Registration Settings）]：Cisco ISE に自動的にゲストデバイスが登録されるようにするか、またはゲストが手動でこれらのデバイスを登録できるページを表示するかどうかを選択します。
- [BYOD 設定（BYOD Settings）]：従業員が自分のパーソナルデバイスを使用してネットワークにアクセスすることを許可します。
- [ポストログインバナーページの設定（Post-Login Banner Page Settings）]：ネットワーク アクセスを許可する前にゲストに追加情報を通知します。
- [ゲストデバイスのコンプライアンス設定（Guest Device Compliance Settings）]：ゲストを [クライアント プロビジョニング（Client Provisioning）] ページにルーティングし、最初にポスチャエージェントをダウンロードするようにゲストに要求します。
- [VLAN DHCP リリースページの設定（VLAN DHCP Release Page Settings）]：ゲストデバイスの IP アドレスをゲスト VLAN から解放し、ネットワークの他の VLAN にアクセスするように更新します。
- [認証成功の設定（Authentication Success Settings）]：認証されたゲストに対する表示内容を指定します。

- [サポート情報ページの設定（Support Information Page Settings）]：ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクによって使用される情報をゲストが提供するのを支援します。

ステップ 7 [保存（Save）] をクリックします。システム生成の URL がポータル テスト URL として表示されます。この URL を使用して、ポータルにアクセスし、テストすることができます。

次のタスク

（注） テストポータルはRADIUSセッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

アカウント登録ゲスト ポータルの作成

アカウント登録ゲストポータルを提供して、ゲストが自分自身を登録し、自分のアカウントを作成して、ネットワークにアクセスできるようにすることができます。これらのアカウントに対しては、その後も、アクセスを許可する前に、スポンサーによる承認を要求できます。

新しいアカウント登録ゲストポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのアカウント登録ゲスト ポータルを削除できます。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、ゲストフロー図のグラフィカルフローに反映されます。AUPページなどのページを有効にすると、そのページがフローに表示され、ゲストはポータルで使用できるようになります。無効にすると、フローから削除され、次に有効なページがゲストに表示されます。

次のすべてのページ設定によって、ゲスト用の利用規定（AUP）を表示し、その同意を要求することができます。

- ログイン ページの設定（Login Page Settings）
- アカウント登録ページの設定（Self-Registration Page Settings）
- アカウント登録成功ページの設定（Self-Registration Success Page Settings）
- 利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）
- BYOD 設定（BYOD Settings）

始める前に

このポータルに必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）]**。.

ステップ 2 新しいポータルを作成する場合は、[ゲスト ポータルの作成（Create Guest Portal）] ダイアログ ボックスで、ポータル タイプとして [アカウント登録ゲスト ポータル（Self-Registered Guest Portal）] を選択し、[続行（Continue）] をクリックします。

ステップ 3 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザー ポータルに使用されていないことを確認します。

ステップ 4 [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 5 [ポータル設定（Portal Settings）] で、ポート、イーサネット インターフェイス、証明書グループ タグ、ID ソース シーケンス、認証方式、およびこのポータルの動作を定義するその他の設定のデフォルト値を更新します。

ポータル設定フィールドの詳細については、クレデンシャルを持つゲスト ポータルのポータル設定 （892 ページ）を参照してください。

ステップ 6 特定のページのそれぞれに適用される次の設定を更新してください。

- [ログインページの設定（Login Page Settings）]：ゲストクレデンシャルおよびログインガイドラインを指定します。詳細については、クレデンシャルを持つゲスト ポータルのログイン ページ設定 （894 ページ）を参照してください。
- [アカウント登録ページの設定（Self-Registration Page Settings）]：ゲストが [アカウント登録（Self-Registration）] フォームを送信した後のゲストエクスペリエンス以外に、アカウント登録ゲストが読み取る情報、および [アカウント登録（Self-Registration）] フォームに入力する必要がある情報を指定します。
- [アクセプタブル ユース ポリシー（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]：別の AUP ページを追加し、クレデンシャルを持つゲストポータルを使用する従業員を含むゲスト用のアクセプタブル ユース ポリシーの動作を定義します。詳細については、クレデンシャルを持つゲスト ポータルの利用規定（AUP）ページ設定 （902 ページ）を参照してください。
- [従業員のパスワード変更の設定（Employee Change Password Settings）]：初めてログインした後にパスワードを変更するようにゲストに要求します。
- [ゲストデバイス登録の設定（Guest Device Registration Settings）]：Cisco ISE に自動的にゲストデバイスが登録されるようにするか、またはゲストが手動でこれらのデバイスを登録できるページを表示するかどうかを選択します。
- [BYOD 設定（BYOD Settings）]：従業員が自分のパーソナルデバイスを使用してネットワークにアクセスすることを許可します。詳細については、クレデンシャルを持つゲスト ポータルの BYOD 設定 （904 ページ）を参照してください。
- [ポストログイン バナー ページ設定（Post-Login Banner Page Settings）]：ユーザーが正常にログインした後、ネットワークアクセスを付与される前に追加情報を表示します。

- [ゲストデバイスのコンプライアンス設定（Guest Device Compliance Settings）]：ポスチャアセスメントのためにゲストを [クライアント プロビジョニング（Client Provisioning）] ページにリダイレクトします。詳細については、クレデンシャルを持つゲスト ポータルのゲスト デバイスのコンプライアンス設定 （906 ページ）を参照してください。
- [VLAN DHCP リリースページの設定（VLAN DHCP Release Page Settings）]：ゲストデバイスの IP アドレスをゲスト VLAN から解放し、ネットワークの他の VLAN にアクセスするように更新します。詳細については、クレデンシャルを持つゲスト ポータルの BYOD 設定 （904 ページ）を参照してください。
- [認証成功の設定（Authentication Success Settings）]：認証後のゲストの宛先を指定します。認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。詳細については、ゲスト ポータルの認証成功の設定 （907 ページ）を参照してください。
- [サポート情報ページの設定（Support Information Page Settings）]：ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクによって使用される情報をゲストが提供するのを支援します。

ステップ 7 [保存（Save）] をクリックします。システム生成の URL がポータル テスト URL として表示されます。この URL を使用して、ポータルにアクセスし、テストすることができます。

次のタスク

（注） テストポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

スポンサーによるアカウント登録のアカウントの承認

登録済みゲストがアカウントの承認を要求するように設定すると、Cisco ISE は、アカウントの承認のために電子メールを承認者に送信します。承認者は、訪問先担当者またはスポンサー ユーザーのいずれかです。

承認者がスポンサーの場合、アカウントを拒否または承認するリンクを含めるように電子メールを設定できます。承認リンクには、承認をスポンサーの電子メール アドレスに関連付けるトークンが含まれています。スポンサーに認証を要求できます。これにより、トークンは無視されます。トークンはタイムアウトすることもあります。タイムアウトすると、スポンサーは、アカウントを承認する前に認証を受ける必要があります。

アカウント承認オプションは、自己登録ポータルの [登録フォームの設定（Registration Form Settings）] で設定します。この機能は、シングルクリック スポンサー承認とも呼ばれます。

スポンサーが電子メールを開いて承認リンクをクリックすると実行されるアクションは、承認者の設定に応じて異なります。

[承認要求電子メール送信先（Email approval request to）]が次のいずれかに設定されている場合について説明します。

- **[訪問先担当者（person being visited）]**
  - また、ゲストアカウントに認証が**不要**な場合は、1 回のクリックでアカウントが承認されます。
  - ゲストアカウントに承認が**必要**な場合は、スポンサーにスポンサーポータルが表示されます。このポータルでは、アカウントの承認前にスポンサーがクレデンシャルを入力する必要があります。

- [下に示すスポンサーの電子メールアドレス（Sponsor email addresses listed below）]：Cisco ISE は、指定されるすべての電子メールアドレスに電子メールを送信します。これらのスポンサーのいずれかが承認リンクまたは拒否リンクをクリックすると、スポンサーポータルが表示されます。そのスポンサーがクレデンシャルを入力し、確認されます。スポンサーが所属するスポンサー グループで、スポンサーによるゲスト アカウントの承認が許可されている場合、スポンサーはアカウントを承認できます。クレデンシャルが失敗すると、Cisco ISE は、スポンサーポータルにログインしてアカウントを手動で承認するようスポンサーに通知します。

説明

- 前のバージョンの Cisco ISE からデータベースをアップグレードまたは復元する場合は、承認または拒否のリンクを手動で挿入する必要があります。アカウント登録ゲストポータルを開き、[ポータルページのカスタマイズ（Portal Page Customizations）] タブを選択します。下方向にスクロールし、[承認要求の電子メール（Approval Request Email）] ウィンドウを選択します。そのウィンドウの**電子メール本文**セクションで [承認/拒否のリンクを挿入する（Insert Approve/Deny Links）] をクリックします。
- Active Directory および LDAP で認証するスポンサー ポータルのみがサポートされています。スポンサーがマッピングするスポンサー グループには、スポンサーが属する Active Directory グループが含まれている必要があります。
- スポンサーのリストがある場合、最初のポータルが、スポンサーがログインするポータルではない場合でも、最初のポータルのカスタマイズ内容が使用されます。
- スポンサーは、承認リンクと拒否リンクを使用するために、HTM 対応の電子メール クライアントを使用する必要があります。
- スポンサーの電子メールアドレスが有効なスポンサー用ではない場合、承認電子メールは送信されません。

シングルクリックスポンサーの承認の詳細については、Cisco ISE コミュニティリソースの『**ISE Single Click Sponsor Approval FAQ**』を参照してください。このドキュメントには、プロセス全体を説明するビデオへのリンクも含まれています。

アカウント承認メール リンクの設定

ネットワークにアクセスする前に、アカウント登録ゲストの承認を要求できます。Cisco ISE は、訪問先担当者の電子メールアドレスを使用して、承認者に通知します。承認者は、訪問先担当者またはスポンサーのいずれかです。承認の詳細については、スポンサーによるアカウント登録のアカウントの承認 （853 ページ）を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [ゲスト（Guest）] > [設定（Configure）] > [ゲストポータル（Guest Portals）]**。電子メールアカウント承認リンクを設定するアカウント登録ポータルを選択します。

ステップ 2 [アカウント登録ページの設定（Self Registration Page Settings）] タブを展開します。

ステップ 3 [アカウント登録ゲストの承認が必要である（Require self-registered guests to be approved）] をオンにします。

[承認/拒否リンクの設定（Approve/Deny Link Settings）] セクションが表示されます。また、[承認要求メール（Approval Request Email）] の電子メール設定に、承認リンクと拒否リンクが取り込まれます。

次の詳細を入力します。

- [アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）]：このポータルを使用するアカウント登録ゲストは、ゲストのクレデンシャルを受信する前にスポンサーによる承認が必要であることを指定します。このオプションをクリックすると、スポンサーがアカウント登録ゲストを承認する方法に関する追加のオプションが表示されます。
  - [アカウント登録したゲストにスポンサーの承認後に自動ログインを許可（Allow guests to login automatically from self-registration after sponsor's approval）]：アカウント登録ゲストは、スポンサーの承認後に自動的にログインします。
  - [承認要求電子メール送信先（Email approval request to）]：
    - [下に示すスポンサーの電子メールアドレス（Sponsor email addresses listed below）]：承認者として指名されたスポンサーの 1 つ以上の電子、またはすべてのゲストの承認要求の送信先となるメール ソフトウェアを入力します。電子メールアドレスが無効な場合、承認は失敗します。
    - [訪問先担当者（Person being visited）]：[スポンサーに承認用クレデンシャルの入力を求める（Require sponsor to provide credentials for authentication）] フィールドが表示され、[含めるフィールド（Fields to include）] の [必須（Required）] オプションが有効になります（以前は無効だった場合）。これらのフィールドはアカウント登録フォームに表示され、アカウント登録ゲストからこの情報を要求します。電子メール アドレスが無効な場合、承認は失敗します。
  - [承認/拒否リンクの設定（Approve/Deny Link Settings）]：
    - [リンクの有効期間（Links are valid for）]：アカウント承認リンクの有効期間を設定できます。
    - [スポンサーに承認用クレデンシャルの入力を求める（Require sponsor to provide credentials for authentication ）]：このセクションの設定でスポンサーによるアカウント承認用のクレデンシャルの入力が必須ではない場合にも、スポンサーにこの情報を入力させるには、このフィールドをオンにします。このフィールドは、[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] が [訪問先担当者（person being visited）] に設定されている場合にだけ表示されます。

- [承認権限を検証するためスポンサーがスポンサー ポータルと照合される（Sponsor is matched to a Sponsor Portal to verify approval privileges）] : [詳細（Details）] をクリックして、スポンサーが有効なシステムユーザーであり、スポンサーグループのメンバーであり、そのスポンサー グループのメンバーにアカウント承認権限があることを確認するために検索されるポータルを選択します。各スポンサーポータルには、スポンサーを識別するために使用される ID ソース シーケンスがあります。ポータルはリストされている順序で使用されます。リストの 1 番目のポータルは、スポンサー ポータルで使用されているスタイルとカスタマイズ内容を決定します。

ポータルの許可

ポータルを許可するときは、ネットワーク アクセス用のネットワーク許可プロファイルおよびルールを設定します。

始める前に

ポータルを許可する前にポータルを作成する必要があります。

ステップ 1 ポータルの特別な許可プロファイルを設定します。

ステップ 2 プロファイルの許可ポリシー ルールを作成します。

許可プロファイルの作成

各ポータルには、特別な許可プロファイルを設定する必要があります。

始める前に

デフォルトのポータルを使用しない場合は、許可プロファイルとポータル名を関連付けることができるように、最初にポータルを作成する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 使用を許可するポータル名を使用して許可プロファイルを作成します。

次のタスク

新しく作成される許可プロファイルを使用するポータル許可ポリシールールを作成する必要があります。

ホットスポット ポータルおよび MDM ポータル用の許可ポリシー ルールの作成

ユーザー（ゲスト、スポンサー、従業員）のアクセス要求への応答に使用するポータルのリダイレクション URL を設定するには、そのポータル用の許可ポリシー ルールを定義します。

url-redirect は、ポータル タイプに基づいて次の形式になります。

ip:port ：IP アドレスとポート番号

PortalID：一意のポータル名

ホットスポット ゲスト ポータル：
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

モバイル デバイス管理（MDM）ポータル：
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]**> **[ポリシーセット（Policy Sets）]** を選択して、[標準（Standard）] ポリシーで新しい認証ポリシールールを作成します。

ステップ 2 [条件（Conditions）] には、ポータルの検証に使用するエンドポイント ID グループを選択します。たとえば、ホットスポット ゲスト ポータルの場合は、デフォルトの [GuestEndpoints] エンドポイント ID グループを選択し、MDM、ポータルの場合は、デフォルトの [RegisteredDevices] エンドポイント ID グループを選択します。

（注） Reauthenticate および Terminate CoA タイプは、ホットスポット ゲスト ポータルでサポートされています。ホットスポット ゲスト ポータルで Reauthentication CoA タイプが選択されている場合のみ、ホットスポットゲスト認証ポリシーの検証条件の 1 つとして [ネットワークアクセス：ユースケースEQUALSゲストフロー（Network Access:UseCase EQUALS Guest Flow）] を使用できます。

ステップ 3 [権限（Permissions）] には、作成したポータル許可プロファイルを選択します。

（注） RADIUS.Calling-Station-ID など、MAC オプションが有効になっているディクショナリ属性を使用して許可条件を作成する場合は、さまざまな MAC 形式をサポートするために Mac 演算子（Mac_equals など）を使用する必要があります。

ゲスト ポータルのカスタマイズ

ポータルの外観およびユーザー（必要に応じてゲスト、スポンサー、または従業員）エクスペリエンスをカスタマイズするには、ポータルテーマをカスタマイズし、ポータルページの UI 要素を変更して、ユーザーに表示されるエラーメッセージと通知を編集します。ポータルのカスタマイズの詳細については、エンドユーザー Web ポータルのカスタマイズ （928 ページ）を参照してください。

定期的な AUP 受け入れの設定

[ポリシー（Policy）] > **[ポリシーセット（Policy Sets）]** を選択し、AUP の期限が切れた場合にゲストユーザーをログイン情報を持つポータルにリダイレクトする新しい認証ルールをリストの上部に作成します。LastAUPAcceptanceHours を目的の最大時間と比較するために条件（LastAUPAcceptanceHours > 8 など）を使用します。時間の範囲 1 ～ 999 をチェックできます。

次のタスク

エンドポイントが AUP 設定を受信したことを確認するには、次の手順を実行します。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]**。
2. AUP が最後に受け入れられた時刻を確認するエンドポイントをクリックします（*AUPAcceptedTime*）。

定期的な AUP の強制

ポリシーで LastAUPAcceptance を使用して、AUP を承認することをユーザーに強制できます。

```
If LastAUPAcceptance >= 24: Hotspot Redirect
If LastAUPacceptance < 24: PermitAccess
If Wireless_MAB: Hotspot Redirect
```

この例では、24 時間ごとにホットスポット ポータルに AUP を強制する方法を示します。

1. ユーザーが 24 時間以上前に AUP を承認済みの場合、AUP を受け入れる（初めからやり直す）必要があります。
2. ユーザーが 24 時間前以内に AUP を承認済みの場合、セッションを続行します。
3. ネットワーク（MAB）への最初のアクセス時は AUP を承認する必要があります。

クレデンシャルを持つポータルでは、そのポータルの AUP が有効であれば同じ規則を使用できます。

（注）

- エンドポイントへのゲスト AUP ページの通信を確立するには、次に示すとおり、ゲストポータルのリダイレクト認証ルールに LastAUPAcceptanceHours 条件を追加します。

  ```
  If AUP <= "X hours": Add in the Permit Access Rule
  If AUP > "X hours": Add in the Redirection Rule
  ```

- 新規ユーザーは、LastAUPAcceptanceHours 条件なしでリダイレクト認証ルールを設定できます。

ゲスト ユーザー情報を保存

この機能により、Cisco ISE はレポートとログに MAC アドレスではなくゲストのユーザー名を表示できます。

ゲストが初回認証されると、ユーザーのデバイスの MAC アドレスがエンドポイントグループに保存され、レポートでユーザー名が使用されます。ユーザーが切断され、ネットワークに再接続された場合、MAC アドレスはすでにエンドポイント グループに存在するため、ユーザーは再びログイン（認証）する必要はありません。この場合、ユーザー名は利用できないため、レポートとログには MAC アドレスが使用されます。

Cisco ISE はポータルユーザー ID を保持し、一部のレポートで使用します。この機能を無効にするには、**[ゲスト（Guest）]** > **[設定（Settings）]** > **[ロギング（Logging）]** に移動します。この機能は新規インストール時にデフォルトで有効になっています。

[アカウントを記憶する（Remember Me）] のロギングの問題に関する詳細については、Cisco ISE コミュニティのリソースの『ISE 2.3+ Remember Me guest using guest endpoint group logging display』を参照してください。

[アカウントを記憶する（Remember Me）] の設定に関する詳細については、『Cisco ISE Guest Access Deployment』のガイドを参照してください。 https://communities.cisco.com/docs/DOC-77590

各リリースでサポートされるレポート方法に関する詳細については、該当するリリースのリリース ノートを参照してください。

スポンサー ポータル

スポンサー ポータルは、Cisco ISE ゲスト サービスの主要コンポーネントの 1 つです。スポンサー ポータルを使用して、スポンサーは承認ユーザー用の一時アカウントを作成および管理し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲストアカウントを作成した後、スポンサーは、スポンサー ポータルを使用して、印刷、電子メール送信、または携帯電話による送信を行ってゲストにアカウントの詳細を提供することもできます。アカウント登録ゲストに企業ネットワークへのアクセス権を提供する前に、スポンサーはゲスト アカウントを承認するように電子メールで要求されることがあります。

スポンサー ポータルでのゲスト アカウントの管理

スポンサー ポータルのログオンのフロー

スポンサー グループにより、スポンサー ユーザーに割り当てられる権限のセットが指定されます。スポンサーがスポンサー ポータルにログインすると、次の処理が行われます。

1. ISE がスポンサーのクレデンシャルを検証します。
2. スポンサーの認証が成功すると、Cisco ISE は使用可能なすべてのスポンサーグループを検索して、スポンサーが属するスポンサーグループを見つけます。次の両方の条件を満たしている場合は、スポンサーがスポンサー グループに一致しているか、属しています。

- スポンサーは、設定されているいずれかのメンバー グループのメンバーである。
- [その他の条件（Other Conditions）] を使用している場合は、そのスポンサーについてすべての条件が true である。

3. スポンサーがスポンサー グループに属している場合、スポンサーはそのグループの権限を取得します。スポンサーは複数のスポンサー グループに属することができます。この場合、属しているすべてのグループの権限が組み合わせられます。スポンサーがどのスポンサー グループにも属していない場合、スポンサー ポータルへのログインは失敗します。

スポンサー グループとその権限は、スポンサー ポータルから独立しています。スポンサーがログインするスポンサー ポータルに関係なく、スポンサー グループの照合には同一アルゴリズムが使用されます。

スポンサー ポータルの使用

スポンサーポータルを使用して、承認された訪問者が企業ネットワークまたはインターネットにセキュアにアクセスできるようにする一時ゲスト アカウントを作成します。ゲスト アカウントを作成したら、スポンサーポータルを使用してこれらのアカウントを管理し、アカウントの詳細情報をゲストに提供することができます。

スポンサー ポータルでは、スポンサーが新しいゲスト アカウントを個別に作成するか、またはファイルからユーザー グループをインポートすることができます。

（注） Active Directory などの外部 ID ストアから承認された ISE 管理者は、スポンサー グループに所属できます。ただし、内部管理者アカウント（デフォルトの「admin」アカウントなど）はスポンサー グループに含めることができません。

スポンサー ポータルを開く方法はいくつかあります。

- [管理者（Administrators）] コンソールで、[アカウントの管理（Manage Accounts）] リンクを使用します。[管理者（Administrators）] コンソールで、[ゲストアクセス（Guest Access）] をクリックしてから、[アカウントの管理（Manage Accounts）] をクリックします。[アカウントの管理（Manage Accounts）] をクリックすると、ALL_ACCOUNTS にアクセスできるデフォルトのスポンサーグループに割り当てられます。新しいゲストアカウントを作成できますが、ゲストに対して通知することはできません。これは、ゲストからのアカウントアクティブ化要求を受信するための電子メールアドレスがないためです。同じ権限を持ち、スポンサーポータルにログインしてこれらのアカウントを検索するスポンサーは、通知を送信できます。

  このステップでは、[スポンサー（Sponsor）] ポータルの [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] ウィンドウで設定した FQDN が DNS サーバーに存在している必要があります。

  NAT ファイアウォールを介してスポンサーポータルにアクセスしている場合、接続はポート 9002 を使用します。

- [管理者（Administrators）] コンソールの [スポンサーポータル（Sponsor Portal）] 設定ウィンドウから、次の操作を実行します。**[ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）]** をクリックしてスポンサーポータルを開き、 [説明（Description）] フィールドの右側にある [ポータルテスト URL（Portal Test URL）] リンクをクリックします。
- ブラウザで、スポンサーポータルの [ポータル設定（Portal Settings）] ウィンドウで設定した URL（FQDN）を開きます。この URL（FQDN）は DNS サーバーで定義されている必要があります。

次の作業

スポンサー ポータルの使用法については、お使いのバージョンの ISE の『Sponsor Portal User Guide』（https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html）を参照してください。

スポンサー アカウントの管理

スポンサーは、スポンサー ポータルからゲスト ユーザー アカウントを作成および管理する組織の従業員または請負業者となります。Cisco ISE は、ローカル データベースあるいは外部の Lightweight Directory Access Protocol（LDAP）、Microsoft Active Directory、または SAML ID ストア経由でスポンサーを認証します。外部ソースを使用しない場合、スポンサー用の内部ユーザー アカウントを作成する必要があります。

スポンサー グループ

スポンサー グループは、スポンサー ポータルの使用時にスポンサーに付与される権限を制御します。スポンサーがスポンサー グループのメンバーである場合、スポンサーにはグループに定義されている権限が付与されます。

スポンサーは、次の両方が当てはまる場合にスポンサー グループのメンバーであると見なされます。

1. スポンサーが、スポンサー グループで定義されているメンバー グループの少なくとも 1 つに属している。メンバー グループは、ユーザー ID グループか、Active Directory などの外部 ID ソースから選択されたグループです。
2. スポンサーが、スポンサー グループで指定されているすべてのその他の条件を満たしている。オプションのその他の条件は、ディクショナリ属性で定義される条件です。これらの条件は、許可ポリシーで使用されるものと動作が似ています。

スポンサーは、複数のスポンサー グループのメンバーにすることができます。その場合、スポンサーにはそれらすべてのグループから次のように組み合わされた権限が付与されます。

- いずれかのグループで有効になっている場合、「ゲストのアカウントの削除」などの個々の権限が付与されます。
- スポンサーは、任意のグループでゲスト タイプを使用してゲストを作成できます。
- スポンサーは、任意のグループの場所にゲストを作成できます。

- バッチ サイズ制限などの数値は、グループの最大値が使用されます。

スポンサーがいずれかのスポンサー グループのメンバーでない場合、そのスポンサーはスポンサー ポータルにログインできません。

- ALL_ACCOUNTS：スポンサーは、すべてのゲストアカウントを管理できます。
- GROUP_ACCOUNTS：スポンサーは、同じスポンサーグループのスポンサーが作成したゲストアカウントを管理できます。
- OWN_ACCOUNTS：スポンサーは、作成したゲストアカウントのみを管理できます。

特定のスポンサー グループで使用可能な機能をカスタマイズでき、それによりスポンサー ポータルの機能を制限または拡張できます。

スポンサー アカウントの作成およびスポンサー グループへの割り当て

内部スポンサー ユーザー アカウントを作成し、スポンサー ポータルを使用できるスポンサーを指定するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** を選択します。適切なユーザー ID グループに内部スポンサー ユーザー アカウントを割り当てます。

（注） デフォルトのスポンサー グループには、デフォルトの ID グループ Guest_Portal_Sequence が割り当てられています。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーグループ（Sponsor Groups）] > [作成、編集または複製（Create, Edit or Duplicate）]** の順に選択し、[メンバー（Members）] をクリックします。スポンサー ユーザー ID グループをスポンサー グループにマッピングします。

次のタスク

スポンサーで使用するために、追加で組織に固有のユーザー ID グループを作成することもできます。**[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ユーザー ID グループ（User Identity Groups）]** を選択します。

スポンサー グループの設定

シスコはデフォルトのスポンサー グループを提供します。デフォルト オプションを使用しない場合、新しいスポンサー グループを作成するか、またはデフォルトのスポンサー グループを編集して設定を変更できます。スポンサー グループを複製して、同じ設定と権限を持つスポンサー グループをさらに作成することもできます。

スポンサー グループを無効にすることができます。無効になったグループのメンバーはスポンサー ポータルにログインできなくなります。Cisco ISE によって提供されているデフォルトのスポンサー グループ以外のスポンサー グループを削除できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals and Components）] > [スポンサーグループ（Sponsor Groups）] > [作成、編集または複製（Create, Edit or Duplicate）]** の順に選択します。

ステップ 2 [スポンサーグループ名（Sponsor group name）] と [説明（Description）] に入力します。

ステップ 3 [一致基準（Match Criteria）] セクションに次の詳細を入力します。

- [メンバーグループ（Member Groups）]：[メンバー（Members）] をクリックして 1 つ以上のユーザー（ID）グループと外部 ID ソースグループを選択し、それらのグループを追加します。ユーザーがこのスポンサー グループのメンバーになるためには、少なくとも 1 つの設定済みグループに属している必要があります。
- [その他の条件（Other conditions）]：[新しい条件の作成（Create New Condition）] をクリックして、このスポンサーグループに含めるためにスポンサーが満たす必要がある条件を 1 つ以上構築します。Active Directory、LDAP、SAML、ODBC の ID ストアからの認証属性を使用できますが、RADIUS トークンまたは RSA SecurID ストアは使用できません。内部ユーザー属性も使用できます。条件には、属性、演算子、値があります。
  - ディクショナリ属性 *Name* を使用して条件を作成するには、ID グループ名の前にユーザー ID グループを付けます。次に例を示します。

    InternalUser:Name EQUALS bsmith

    この場合、「bsmith」という名前の内部ユーザーだけがこのスポンサー グループに所属できます。
  - Active Directory インスタンスの ExternalGroups 属性を使用して条件を作成するには、一致させるスポンサー ユーザーの AD「プライマリ グループ」を選択します。たとえば、ユーザーの名前が Smith の場合は *AD1:LastName EQUALS Smith* になります。

1 つ以上の設定されたメンバー グループとの一致に加えて、スポンサーはここで作成する**すべての**条件に一致する必要があります。認証しているスポンサー ユーザーが複数のスポンサー グループの一致基準を満たす場合には、そのユーザーには次のようにアクセス許可が付与されます。

- ゲストのアカウントの削除などの個々の権限は、一致するグループのいずれかで有効になっている場合に付与されます。
- スポンサーは、一致するグループのいずれかのゲスト タイプを使用してゲストを作成することができます。
- スポンサーは、一致するグループのいずれかのゲスト タイプを使用してゲストを作成することができます。
- スポンサーは、一致するグループのいずれかの場所でゲストを作成することができます。

- バッチ サイズ制限などの数値については、一致するグループの最も大きな値が使用されます。

[メンバー グループ（Member Groups）] のみが指定されている一致基準、または [その他の条件（Other Conditions）] のみが指定されている一致基準を作成できます。[その他の条件（Other Conditions）] のみを指定する場合、スポンサー グループのスポンサーのメンバーシップは、一致するディクショナリ属性のみに基づいて決定されます。

ステップ 4 このスポンサーグループに基づいてスポンサーが作成できるゲストタイプを指定するには、[このスポンサーグループはこれらのゲストタイプを使用してアカウントを作成可能（This sponsor group can create accounts using these guest types）] をクリックして、1 つ以上のゲストタイプを選択します。

[次の場所にゲストタイプを作成（Create Guest Types at）] の下のリンクをクリックして、このスポンサーグループに割り当てるゲストタイプをさらに作成できます。新しいゲストタイプを作成した後、その新しいゲスト タイプを選択するには、スポンサー グループを保存して閉じ、再度開いてください。

ステップ 5 [ゲストが訪問するロケーションを選択（Select the locations that guests will be visiting）] を使用して、ゲストアカウントの作成時にスポンサー グループのスポンサーが選択できるロケーション（ゲストの時間帯の設定に使用）を指定します。

[次の場所にゲストロケーションを設定（Configure guest locations at）] の下のリンクをクリックして、ゲストロケーションを追加することで、選択できるロケーションをさらに追加できます。新しいゲストロケーションを作成した後、その新しいゲストロケーションを選択するには、スポンサー グループを保存して閉じ、再度開いてください。

これによって、ゲストが他のロケーションからログインできなくなることはありません。

ステップ 6 スポンサーがユーザーの作成後に [通知（Notify）] をクリックする操作を行わずにすむようにするには、[自動ゲスト通知（Automatic guest notification）] の下の [電子メール アドレスが使用可能な場合はアカウント作成時にゲストに電子メールを自動的に送信する（Automatically email guests upon account creation if email address is available）] をオンにします。これにより、電子メールが送信されたことを示すウィンドウが表示されます。また、このオプションをオンにすると、[ゲスト通知は自動送信されました（Guest notifications are sent automatically] というヘッダーがスポンサー ポータルに追加されます。

ステップ 7 [スポンサー作成可能（Sponsor Can Create）] で、このグループ内のスポンサーがゲスト アカウントを作成するために使用できるオプションを設定します。

- [特定のゲストに割り当てられた複数のゲストアカウント（インポート）（Multiple guest accounts assigned to specific guests (Import)）]：スポンサーがファイルから姓名などのゲストの詳細をインポートすることによって、複数のゲストアカウントを作成できるようにします。

  このオプションが有効になっている場合、[インポート（Import）] オプションが [スポンサー（Sponsor）] ポータルの [アカウントの作成（Create Accounts）] ウィンドウに表示されます。[インポート（Import）] オプションは、Internet Explorer、Firefox、Safari などのデスクトップ ブラウザだけで使用可能です（モバイルは不可）

- [バッチ処理の制限（Limit to batch of）]：このスポンサーグループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲストアカウントの数を指定します。

  スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- [ゲストへの複数のゲストアカウントの割り当て（ランダム）（Multiple guest accounts to be assigned to any guests (Random)）]：スポンサーが、未知のゲストのプレースホルダとして複数のランダムゲストアカウントを作成するか、または、または複数のアカウントをすばやく作成することができるようにします。

  このオプションが有効になっている場合、[ランダム（Random）] オプションが [スポンサー（Sponsor）] ポータルの [アカウントの作成（Create Accounts）] ページに表示されます。

- [デフォルトユーザー名プレフィックス（Default username prefix）]：スポンサーが複数のランダムなゲストアカウントを作成する場合に使用できるユーザー名プレフィックスを指定します。指定した場合、このプレフィックスはランダムなゲストアカウントを作成するときにスポンサー ポータルに表示されます。また、[スポンサーにユーザー名プレフィックスの指定を許可（Allow sponsor to specify a username prefix）] の設定により、次のようになります。

  - [有効（Enabled）]：スポンサーは、[スポンサー（Sponsor）]ポータルでデフォルトのプレフィックスを編集できます。
  - [無効（Not enabled）]：スポンサーは [スポンサー（Sponsor）] ポータルでデフォルトのプレフィックスを編集できません。

  ユーザー名プレフィックスを指定しないか、またはスポンサーにユーザー名プレフィックスの指定を許可しない場合、スポンサーはスポンサー ポータルでユーザー名プレフィックスを割り当てることができません。

- [スポンサーにユーザー名プレフィックスの指定を許可（Allow sponsor to specify a username prefix）]：このスポンサーグループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲストアカウントの数を指定します。

  スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

ステップ 8 [スポンサーが管理可能（Sponsor Can Manage）] で、このスポンサー グループのメンバーが表示および管理できるゲスト アカウントを制限できます。

- [スポンサーが作成したアカウントのみ（Only accounts sponsor has created）]：このグループのスポンサーは、スポンサーの電子メール アカウントに基づいて、スポンサーが作成したゲストアカウントのみを表示および管理できます。
- [このスポンサーグループのメンバーによって作成されたアカウント（Accounts created by members of this sponsor group）]：このグループのスポンサーは、このスポンサーグループ内のスポンサーが作成したゲストアカウントを表示および管理できます。
- [すべてのゲストアカウント（All guest accounts）]：スポンサーはすべての保留中のゲストアカウントを表示および管理できます。

ステップ 9 [スポンサーの権限（Sponsor Can）] で、このスポンサー グループのメンバーに、ゲストのパスワードおよびアカウントに関連する追加の権限を提供できます。

- [ゲストの連絡先情報（電子メール、電話番号）の更新（Update guests' contact information (email, Phone Number)）]：スポンサーは、自分が管理できるゲストアカウントについて、ゲストの連絡先情報を変更できます
- [ゲストのパスワードの表示/印刷（View/print guests' passwords）]：このオプションをオンにすると、スポンサーはゲストのパスワードを印刷することができます。スポンサーは [アカウントの管理（Manage Accounts）] ウィンドウとゲストの詳細にゲストのパスワードを表示できます。これがオフの場合、スポンサーはパスワードを印刷できませんが、ユーザーは電子メールまたは SMS（設定済みの場合）を介してパスワードを取得できます。
- [ゲストのクレデンシャルを含む SMS 通知の送信（Send SMS notifications with guests' credentials）]：スポンサーは、自分が管理できるゲストアカウントについて、アカウントの詳細とログインクレデンシャルとともにゲストに SMS（テキスト）通知を送信できます。
- [ゲストアカウントのパスワードのリセット（Reset guest account passwords）]：スポンサーは、自分が管理できるゲストアカウントについて、そのパスワードを Cisco ISE によって生成されたランダムなパスワードにリセットできます。
- [ゲストのアカウントの延長（Extend guests' accounts）]：スポンサーは、自分が管理できるゲストアカウントについて、その有効期限を延長できます。スポンサーは、アカウントの有効期限に関してゲストに送信される電子メール通知に自動的にコピーされます。
- [ゲストのアカウントの削除（Delete guests' accounts）]：スポンサーは、自分が管理できるゲストアカウントについて、アカウントを削除し、ゲストが企業のネットワークにアクセスすることを防ぐことができます。
- [ゲストのアカウントの一時停止（Suspend guests' accounts）]：スポンサーは、自分が管理できるゲストアカウントについて、アカウントを一時停止してゲストが一時的にログインすることを防ぐことができます。

  また、このアクションは、許可変更（CoA）終了を発行して、一時停止されていたゲストをネットワークから排除できます。

  - [スポンサーに理由の入力を求める（Require sponsor to provide a reason）]：ゲストアカウントの一時停止に対する説明の入力をスポンサーに求めます。

- [アカウント登録ゲストからの要求の承認および表示（Approve and view requests from self-registering guests）]：このスポンサーグループに含まれているスポンサーは、（承認が必要な）アカウント登録ゲストからのすべての保留中のアカウント要求を表示するか、アクセス先の担当者としてユーザーがスポンサーの電子メールアドレスを入力した要求のみを表示できます。この機能では、アカウント登録ゲストによって使用されるポータルで[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] にマークが付けられていて、スポンサーの電子メールが連絡先の担当者としてリストされている必要があります。この機能では、スポンサーのアイデンティティ送信元で**電子メール**属性が適切に設定されている必要もあります。

  - [保留中のすべてのアカウント（Any pending accounts）]：このグループに所属するスポンサーは、他のスポンサーによって作成されたアカウントを承認およびレビューします。

- [このスポンサーに割り当てられている保留中のアカウントのみ（Only pending accounts assigned to this sponsor）]：このグループに所属するスポンサーは、スポンサー自身が作成したアカウントだけを表示および承認できます。

（注） **電子メール**属性は、**ユーザー情報属性**の一部です。**電子メール**属性の詳細については、次を参照してください。

- カスタム スキーマの設定 （1054 ページ）
- LDAP ID ソースの設定 （992 ページ） の [LDAP一般設定（LDAP General Settings）] テーブルの [スキーマ（Schema）] と [ユーザー情報（User Info）] 属性。
- SAML ID プロバイダーの設定 （1188 ページ） の手順 8。

- [プログラムによるインターフェイス（Guest REST API）を使用した Cisco ISE ゲストアカウントへのアクセス（Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)）]：スポンサーは、自分が管理できるゲストアカウントについて、Guest REST API プログラミング インターフェイスを使用してゲストアカウントにアクセスできます。

ステップ 10 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

スポンサー アカウント作成のためのアカウント コンテンツの設定

ゲストとスポンサーが新しいゲスト アカウントの作成時に指定する必要があるユーザー データのタイプを設定できます。ISEアカウントを識別するために必要なフィールドがありますが、その他のフィールドを削除し、独自のカスタム フィールドを追加することができます。

スポンサーによるアカウント作成用のフィールドを設定するには、次の手順に従います。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Sponsor Portals）]** を選択し、スポンサーポータルを編集します。
2. [ポータル ページのカスタマイズ（Portal Page Customization）] タブを選択します。
3. 下にスクロールして [既知のゲストのアカウント作成（Create Account for Known Guests)] を選択します。
4. 右側の [プレビュー（Preview）] 表示で [設定（Settings）] を選択します。

これらの設定により、スポンサー ポータルでのゲスト アカウントの作成時に表示される、ゲスト アカウントに必要なフィールドが決定します。この設定は、ゲスト タイプ [既知（Known）]、[ランダム（Random）]、および[インポート（Imported）] に適用されます。新しいユーザーをインポートするためにスポンサーがダウンロードするテンプレートは動的に作成されるので、[既知のゲスト（Known Guests）] で設定したフィールドだけが含まれます。

アカウントのユーザー名とパスワードのインポート

スポンサーはユーザー名とパスワードをインポートできますが、スポンサーがCSVテンプレートをダウンロードするときにはこれらの行がテンプレートに追加されません。スポンサーはこれらのヘッダーを追加できます。ISE が列を認識できるように、ヘッダーの名前が正しく設定されている必要があります。

- [ユーザー名（Username）]：*User Name* または *UserName* です。
- [パスワード（Password）]：**password** である必要があります。

スポンサー ポータルの特別な設定

次の設定は、[インポートされたゲストにアカウントを作成（Create Account for Imported Guests）]ページ、[ポータルページのカスタマイズ（Portal Page Customizations）]タブ、スポンサー ポータルで一意です。

- [スポンサーによるゲストクレデンシャルの電子メールのコピーを許可（Allow sponsor to be copied in Guest Credentials email）]：このオプションを有効にすると、インポートされたゲストに正常に送信されるゲストレデンシャルの各電子メールがスポンサーにも送信されます。デフォルトでは、電子メールはスポンサーに送信されません。
- [スポンサーによるサマリーの電子メールの受信を許可（Allow sponsor to receive summary email）]：スポンサーがユーザーリストをインポートすると、ISE はインポートされたすべてのユーザーを含むサマリーの電子メールを 1 つ送信します。このオプションをオフにすると、スポンサーはインポートされたユーザーごとにそれぞれ電子メールを受信します。

スポンサー ポータル フローの設定

デフォルト ポータルと、証明書、エンドポイント ID グループ、ID ソース順序、ポータル テーマ、イメージ、および Cisco ISE によって提供されるその他の詳細などのデフォルト設定を使用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

会社の営業所やその小売の場所にさまざまなブランディングがある場合、会社にさまざまな製品ブランドがある場合、または市役所が火災、警察、およびその他の部門で異なるテーマのポータルを必要とする場合は、複数のスポンサー ポータルを作成することもできます。

これらは、スポンサー ポータルの設定に関連するタスクです。

始める前に

スポンサー グループの設定 （862 ページ）の説明に従い、サイトの既存のスポンサー グループを設定または編集します。

ステップ 1 ポリシー サービスの有効化 （869 ページ）。

ステップ 2 ゲスト サービスの証明書の追加 （869 ページ）。
ステップ 3 外部 ID ソースの作成 （870 ページ）。
ステップ 4 ID ソース順序の作成 （870 ページ）。
ステップ 5 スポンサー ポータルの作成 （871 ページ）。
ステップ 6 （任意） スポンサー ポータルのカスタマイズ （872 ページ）。

ポリシー サービスの有効化

Cisco ISE エンドユーザー Web ポータルをサポートするには、ホストするノードでポータルポリシーサービスを有効にする必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。
ステップ 2 ノードをクリックして、[編集（Edit）] をクリックします。
ステップ 3 [全般設定（General Settings）] タブで [ポリシーサービス（Policy Service）] トグルボタンを有効にします。
ステップ 4 [セッションサービスの有効化（Enable Session Services）] チェックボックスをオンにします。
ステップ 5 [保存（Save）] をクリックします。

ゲスト サービスの証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループ タグに割り当てることができます。すべてのエンドユーザー Web ポータルに使用されるデフォルトの証明書グループ タグは [デフォルト ポータル証明書グループ（Default Portal Certificate Group）] です。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]**。
ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。
この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。
ステップ 3 **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > [作成または編集（Create or Edit）] > [ポータル設定（Portal Settings）]** を選択します。
ステップ 4 新しく追加された証明書に関連付けられた [証明書グループ タグ（Certificate Group Tag）] ドロップダウン リストから特定の証明書グループ タグを選択します。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバーなどの外部 ID ソースに接続して、認証/許可のユーザー情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザー ID を受信して共有できるようにするパッシブ ID サービスを使用するには、その他の パッシブ ID サービス プロバイダー （1094 ページ）を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。
- Active Directory：外部 ID ソースとして Active Directory に接続する場合。詳細については、外部 ID ソースとしての Active Directory （1028 ページ）を参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、LDAP （1142 ページ）を参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバーを追加する場合。詳細については、RADIUS トークン ID ソース （1169 ページ）を参照してください。
- RSA SecurID：RSA SecurID サーバーを追加する場合。詳細については、RSA ID ソース （1176 ページ）を参照してください。
- SAML IDプロバイダー（SAML Id Providers）：Oracle Access Manager などの ID プロバイダー（IdP）を追加する場合。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダー （1185 ページ）を参照してください。
- ソーシャルログイン（Social Login）：Facebook などのソーシャルログインを外部 ID ソースとして追加する場合。詳細については、アカウント登録ゲストのソーシャル ログイン （834 ページ）を参照してください。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲストユーザーがローカル WebAuth を使用して認証できるようにするには、ゲストポータル認証ソースと ID ソース順序の両方に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）]** を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リストフィールドの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストフィールドのデータベースを並べ替えます。

ステップ 6 選択したアイデンティティストアに認証のためにアクセスできない場合は、[高度な検索リスト（Advanced Search List）] 領域で次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus属性をProcessErrorに設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]
- [ユーザーが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]

  Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストフィールドに Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

スポンサー ポータルの作成

スポンサーポータルを提供して、ネットワークに接続してインターネットと内部リソースおよびサービスにアクセスするゲストのアカウントをスポンサーが作成、管理、および承認できるようにすることができます。

Cisco ISE では、別のポータルを作成する必要なく使用できるデフォルトのスポンサー ポータルが用意されています。ただし、新しいスポンサーポータルを作成するか、既存のものを編集または複製できます。デフォルトのスポンサーポータル以外のすべてのポータルを削除できます。IPv6 は、スポンサーポータルのログインではサポートされていません。Cisco ISE リリース 3.3 以降では、スポンサーポータルは内部ユーザー向けに IPv6 をサポートしています。SAML を使用したスポンサーポータルのログインは IPv6 をサポートしていません。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブの [ページ設定（Page Settings）] で行った変更は、スポンサー フロー図のグラフィカル フローに反映されます。[AUP] ページなどのページを有効にすると、そのページがフローに表示され、スポンサーはポータルでそれを確認します。無効にした場合は、そのページがフローから削除され、次に有効にされたページがスポンサーに表示されます。

始める前に

このポータルで使用するために、必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

ステップ 1 スポンサー ポータルのポータル設定（911 ページ） の説明に従って、[ポータル設定（Portal Settings）] ページを設定します。

ここで使用するポータル名が他のエンドユーザー ポータルに使用されていないことを確認します。

ステップ 2 スポンサー ポータルのログイン設定（914 ページ） の説明に従って、[ログイン設定（Login Settings）] ページを設定します。

ステップ 3 スポンサー ポータルの利用規定（AUP）設定（915 ページ） の説明に従って、[利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）] ページを設定します。

ステップ 4 スポンサー ポータルのスポンサーのパスワード変更設定（916 ページ） の説明に従って、[スポンサー変更パスワード設定（Sponsor Change Password Settings）] オプションを設定します。

ステップ 5 スポンサー ポータルのポストログイン バナー設定（916 ページ） の説明に従って、[ポストログインバナーページ設定（Post-Login Banner Page Settings）] ページを設定します。

ステップ 6 ポータルをカスタマイズする場合は、[スポンサー ポータル アプリケーション設定（Sponsor Portal Application Settings）] をクリックします。

ステップ 7 [保存（Save）]をクリックします。

スポンサー ポータルのカスタマイズ

ポータルの外観およびユーザー エクスペリエンスをカスタマイズするには、ポータル テーマをカスタマイズし、ポータル ページの UI 要素を変更して、ユーザーに表示されるエラー メッセージと通知を編集します。ポータルのカスタマイズの詳細については、エンドユーザー Web ポータルのカスタマイズ （928 ページ） を参照してください。

スポンサー アカウント作成のためのアカウント コンテンツの設定

ゲストとスポンサーが新しいゲスト アカウントの作成時に指定する必要があるユーザー データのタイプを設定できます。ISE アカウントを識別するために必要なフィールドがありますが、その他のフィールドを削除し、独自のカスタム フィールドを追加することができます。

スポンサーによるアカウント作成用のフィールドを設定するには、次の手順に従います。

1. **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）]** を選択し、スポンサーポータルを編集します。
2. [ポータル ページのカスタマイズ（Portal Page Customization）] タブを選択します。
3. 下にスクロールして [既知のゲストのアカウント作成（Create Account for Known Guests)] を選択します。

右側の [プレビュー（Preview）] 表示で [設定（Settings）] を選択します。これらの設定により、スポンサーポータルでのゲストアカウントの作成時に表示される、ゲストアカウントに必要なフィールドが決定します。

この設定は、ゲスト タイプ [既知（Known）]、[ランダム（Random）]、および [インポート（Imported）] に適用されます。新しいユーザーをインポートするためにスポンサーがダウンロードするテンプレートは動的に作成されるので、[既知のゲスト（Known Guests）] で設定したフィールドだけが含まれます。

スポンサーによるアカウントのユーザー名とパスワードのインポート

スポンサーはユーザー名とパスワードをインポートできますが、スポンサーがテンプレートをダウンロードするときにはこれらの行はテンプレートに追加されません。スポンサーはこれらのヘッダーを追加できます。Cisco ISE が列を認識できるように、ヘッダーの名前が正しく設定されている必要があります。

- [ユーザー名（Username）]：**`User Name`** または **`UserName`** です。
- [パスワード（Password）]：password です。

スポンサーに対して使用可能な時間設定項目の設定

スポンサーは新しいゲストアカウントを作成するときに、アカウントがアクティブである期間を設定します。スポンサーが使用できるオプションを設定して、スポンサーがアカウントの期間と、開始時刻および終了時刻を設定できるようにすることができます。これらのオプションはゲスト タイプ別に設定されます。スポンサーに対し、[アクセス情報（Access Information）] というヘッダーの下に結果が表示されます。

スポンサーポータル アカウント期間オプションを制御する [ゲストタイプ（Guest Type）] 設定は、[最大アクセス時間（Maximum Access Time）] ヘッダーの下にあります。この設定について次に説明します。

- [最初のログインから（From first login）]：スポンサーポータルには、最初のログイン後にアカウントがアクティブ化されている期間が表示されます。

  ゲストタイプ設定の [最大アカウント期間（Maximum Account Duration）] により、スポンサーがその期間に対して入力できる値が決定されます。

- [スポンサーが指定した日付から（From sponsor-specified date）（該当する場合はアカウント登録の日付）]：スポンサーは、期間を [営業日の終わり（End of business day）] として設定するか、または [営業日の終わり（End of business day）] フィールドをオフにして、期間、開始時刻、および終了時刻を設定するかを選択できます。

  期間と有効な日付を制御するゲストタイプ設定は、[アクセスを許可する日付と時刻（Allow access only on these days and times）] ヘッダーの下にあります。

  - 選択した曜日により、スポンサーのカレンダーで選択できる日付が制限されます。
  - 期間と日付を選択すると、スポンサー ポータルで最大アカウント期間が適用されます。

スポンサー ポータルの Kerberos 認証

Cisco ISE を設定して、Windows にログオンしているスポンサーユーザーの [スポンサー（Sponsor）] ポータルへのアクセスの認証に Kerberos を使用できます。このプロセスは、Kerberos チケットでログインしているスポンサー ユーザーの Active Directory クレデンシャルを使用します。ブラウザが Cisco ISE との SSL 接続を確立した後、セキュアなトンネル内で Kerberos SSO が実行されます。

次の項目は同じ Active Directory ドメインに存在する必要があります。

- スポンサーの PC
- ISE PSN
- このスポンサー ポータルに設定された FQDN

この要件は、Microsoft では Active Directory フォレスト間の双方向の信頼での Kerberos SSO がサポートされていないため必要です。

スポンサー ユーザーは、Windows にログオンする必要があります。

ゲスト ポータルの Kerberos 認証はサポートされていません。

Kerberos の設定

[スポンサー（Sponsor）] ポータルで Kerberos を有効にするには、[スポンサー設定とカスタマイズ（Sponsor Settings and Customization）] ウィンドウで [Kerberos SSO を許可する（Allow Kerberos SSO）] チェックボックスをオンにします。

スポンサーのブラウザも正しく設定されていなければなりません。次のセクションでは、各ブラウザを手動で設定する方法を説明します。

（注） Active Directory のユーザー名とユーザープリンシパル名が一致している必要があります。SSO は、ユーザーのセッションを識別するユーザープリンシパル名によって決まります。

ブラウザからスポンサーポータル FQDN を使用してスポンサーポータルにアクセスしている間、Cisco ISE は設定されたスポンサーポータル FQDN ではなく PSN FQDN に要求をリダイレクトします。

たとえば、スポンサーポータルの FQDN が `sponsor.example.com` で PSN の FQDN が `psn.example.com` の場合、ブラウザから `https://sponsor.example.com` にアクセスしようとすると、`https://ise.example.com:8445/sponsorportal/PortalSetup.action?portal=b7e7d773-7bb3-442b-a50b-42837c12248a` にリダイレクトされます。

この動作は、[Kerberos SSO を許可（Allow Kerberos SSO）] オプションを有効にしているときにのみ発生します。

Firefox を手動で設定するには

1. アドレス バーに `about:config` と入力します。

2. 表示される警告は無視し、クリックして続行します。
3. 検索バーで `negotiate` を検索します。
4. `network.negotiate-auth.delegation-uris` と `network.negotiate-auth.trusted-uris` に FQDN を追加します。各属性の URL の一覧はコンマで区切られます。
5. タブを閉じます。ブラウザが使用可能になり、再起動は必要ありません。

Internet Explorer を手動で設定するには

1. 右上の歯車をクリックし、[インターネットオプション（Internet Options）] を選択します。
2. [セキュリティ（Security）] タブをクリックします。
3. [ローカルイントラネット（Local Intranet）] をクリックします。
4. [サイト（Sites）] をクリックし、[詳細設定（Advanced）] をクリックします。
5. 文字列に `<mydomain>.com` を追加します（`<mydomain>` はスポンサー ポータル FQDN のワイルド カード）、または FQDN を入力します。
6. [閉じる（Close）] をクリックし、[OK] をクリックします。
7. [詳細（Advanced）] タブをクリックします。
8. [セキュリティ（Security）] セクションまで下方向にスクロールし、[統合 Windows 認証を有効にする（Enable Integrated Windows Authentication）] チェックボックスをオンにします。
9. コンピュータを再起動します。

Chrome は Internet Explorer から設定を取得します

トラブルシューティング

- コマンド プロンプトで `set user` を実行し、マシンが適切な AD ドメインに連結されていることを確認します。
- コマンド プロンプトで `klist` を実行し、キャッシュされた Kerberos チケットとホスト名の一覧を表示します。
- SPNEGO トークンデータを見ます。NTLM パスワードベースのトークン文字列は、Kerberos トークン文字列よりもはるかに短く、正しいトークン文字列は 1 行に収まりません。
- `kerberos` フィルタを使用して Wireshark を使用し、存在する場合は Kerberos 要求をキャプチャします。

（注） Kerberos SSO オプションを有効にすると、ユーザーは、Kerberos SSO が正しく機能するノード FQDN でスポンサー ポータルにアクセスする必要があります。スポンサー ポータルでポータル FQDN が設定されている場合、ユーザーがポータル FQDN に接続すると、そのノード FQDN によってこのポータルにリダイレクトされます。

スポンサーがスポンサー ポータルにログインできない

問題

次のエラー メッセージは、スポンサーがスポンサー ポータルにログインしようとしたときに表示されます。

```
“Invalid username or password. Please try again.”
```

原因

- スポンサーが無効なクレデンシャルを入力しました。
- スポンサーは、ユーザー レコードがデータベース（内部ユーザーまたはActive Directory）にないため無効です。
- スポンサーが属するスポンサー グループは無効です。
- スポンサーのユーザー アカウントがアクティブな/有効なスポンサー グループのメンバーではありません。これは、スポンサー ユーザーの ID グループがいずれのスポンサー グループのメンバーでもないことを意味します。
- スポンサーの内部ユーザー アカウントは無効（一時停止中）です。

ソリューション

- ユーザーのクレデンシャルを確認します。
- スポンサー グループを有効にします。
- ユーザー アカウントが無効になっている場合は復元します。
- スポンサー ユーザーの ID グループをスポンサー グループのメンバーとして追加します。

ゲストとスポンサーのアクティビティのモニター

Cisco ISEは、エンドポイントおよびユーザー管理情報、およびゲストとスポンサーのアクティビティを参照できるさまざまなレポートとログを提供します。

オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 Cisco ISE GUIで[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[操作（Operations）]**>**[レポート（Reports）]**>**[レポート（Reports）]**。

ステップ 2 [ゲスト（Guest）] または [エンドポイントとユーザー（Endpoints and Users）] を選択して、さまざまなゲスト、スポンサー、およびエンドポイント関連のレポートを表示します。

ステップ 3 [フィルタ（Filters）] ドロップダウンリストを使用して検索するデータを選択します。

ステップ 4 データを表示する [時間範囲（Time Range）] を選択します。

ステップ 5 [実行（Run）] をクリックします。

メトリック ダッシュボード

Cisco ISE では、Cisco ISE ホーム ページに表示されるメトリック ダッシュボードで、ネットワークの [認証されたゲスト（Authenticated Guests）] と [アクティブ エンドポイント（Active Endpoints）] を一目で確認できます。

[アクティブエンドポイント（Active Endpoints）] に表示されている番号をクリックすると、[ライブセッション（Live Sessions）] ウィンドウが開き、アクティブなセッションがあるエンドポイントの詳細が表示されます。

（注） ホットスポットフローの場合は、[認証されたゲスト（Authenticated Guests）] ダッシュレットにエンドポイントが表示されません。

AUP 受け入れステータス レポート

AUP 受け入れステータス レポートには、すべてのゲスト ポータルからの、ゲストによる利用規定（AUP）の受け入れのステータスが示されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [レポート（Reports）] > [ゲスト（Guest）] > [AUP 受け入れステータス（AUP Acceptance Status）]**

レポートを使用して、特定の期間のすべての許可および拒否された AUP 接続を追跡できます。

ゲスト アカウンティング レポート

ゲスト アカウンティング レポートは、指定された期間のゲスト ログイン履歴を表示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [レポート（Reports）] > [ゲスト（Guest）] > [ゲストアカウンティング（Guest Accounting）]**

プライマリゲストレポート

プライマリゲストレポートは、さまざまなレポートからのデータを単一のビューへ結合して、複数の異なるレポートソースからデータをエクスポートできるようにします。データ カラムをさらに追加したり、表示またはエクスポートしないデータ カラムを削除したりできます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [レポート（Reports）] > [レポート（Reports）] > [ゲスト（Guest）] > [プライマリゲストレポート（Primary Guest Report）]**。

このレポートはすべてのゲスト アクティビティを収集し、ゲスト ユーザーがアクセスした Web サイトに関する詳細を提供します。このレポートをセキュリティ監査の目的で使用して、ゲス

トユーザーがいつネットワークにアクセスして、何を行ったかを確認できます。アクセスした Web サイトの URL などのゲストのインターネット アクティビティを表示するには、初めに次の操作を行う必要があります。

- 成功した認証のロギング カテゴリを有効にします。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[成功した認証（Passed Authentications）] を選択します。
- ゲスト トラフィックで使用するファイアウォールで次のオプションを有効にします。
  - HTTP トラフィックを検査し、Cisco ISE モニタリング ノードにデータを送信します。Cisco ISE はゲスト アクティビティ レポートに対して IP アドレスおよびアクセスした URL だけを必要とするため、可能な場合は、この情報だけが含まれるようにデータを制限します。
  - Cisco ISE モニタリング ノードに syslog を送信します。

スポンサーのログインおよび監査レポート

スポンサー ログインおよび監査レポートは、次を追跡する統合レポートです。

- スポンサー ポータルでのスポンサーによるログイン アクティビティ。
- スポンサー ポータルでスポンサーが実行したゲスト関連の操作。

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [レポート（Reports）] > [ゲストアクセスレポート（Guest Access Reports）] > [スポンサーログインおよび監査（Sponsor Login and Audit）]** で使用できます。

ゲストおよびスポンサー ポータルの監査ロギング

ゲスト ポータルおよびスポンサー ポータルで特定のアクションが実行されると、基礎となる監査システムに監査ログ メッセージが送信されます。これらのメッセージを表示するには、**show logging application localStore/iseLocalStore.log** コマンドを使用します。

これらのメッセージを syslog によってモニタリング/トラブルシューティング システムおよびログ コレクタに送信するように設定することができます。モニタリング サブシステムによって、適切なスポンサー、デバイス監査ログ、およびゲストのアクティビティ ログにこの情報が示されます。

ゲスト ログイン フローは、ゲスト ログインが成功したか失敗したかにかかわらず、監査ログに記録されます。

ゲスト アクセス Web 認証オプション

Cisco ISE ゲスト サービスと Web 認証サービスでは、セキュアなゲスト アクセスを有効にするための複数の展開オプションがサポートされています。ローカルまたは中央 Web 認証とデバイス登録 Web 認証を使用した有線または無線のゲスト接続を提供することができます。

- [中央 Web 認証（Central WebAuth）]：すべてのゲスト ポータルに適用されます。有線および無線の両方の接続要求に対して、中央 Cisco ISE RADIUS サーバーを介した Web 認証を使用します。ゲストは、ホットスポット ゲスト ポータルでオプションのアクセス コードを入力するか、クレデンシャルを持つゲスト ポータルでユーザー名とパスワードを入力することにより、後で認証されます。

（注） リダイレクト時に、ブラウザが複数のタブを開いていると、Cisco ISE はすべてのタブにリダイレクトします。ユーザーはポータルにログインできますが、Cisco ISE はセッションを承認できず、ユーザーはアクセスに失敗します。この問題を回避するには、ユーザーがブラウザ上で 1 つを除くすべてのタブを閉じる必要があります。

- [ローカル Web 認証（ローカル WebAuth）]：クレデンシャルを持つ [ゲスト（Guest）] ポータルに適用されます。ゲストは、有線接続の場合はスイッチに接続し、ワイヤレス接続の場合はワイヤレス LAN コントローラ（WLC）に接続します。ネットワーク アクセス デバイス（NAD）は、認証用の Web ページにゲストを転送します。ゲストは、認証のために、クレデンシャルを持つゲスト ポータルでユーザー名とパスワードを入力します。

- [デバイス登録 Web 認証（デバイス登録 WebAuth）]：ホットスポット ゲスト ポータルにのみ適用されます。Cisco ISE は、Web 認証の前にゲスト デバイスを登録して承認します。ゲストが有線またはワイヤレス NAD に接続すると、ゲストはホットスポット ゲスト ポータルに転送されます。ゲストは、クレデンシャル（ユーザー名とパスワード）を入力せずにネットワークにアクセスします。

ISE Community Resource

ゲスト アクセスを提供するように Cisco ISE と Cisco ワイヤレス コントローラを設定する方法については、『ISE Guest AccessPrescriptive Deployment Guide』を参照してください。

ISE のテクニカルノート『ISE Wireless Guest Setup Guide & Wizard』も参照してください。

中央 WebAuth プロセス対応の NAD

このシナリオでは、ネットワーク アクセス デバイス（NAD）で、不明なエンドポイント接続から Cisco ISE RADIUS サーバーへの新しい認証要求を作成します。これで、エンドポイントは Cisco ISE への URL-redirect を受け取ります。

（注） webauth-vrf-aware コマンドは、IOS XE 3.7E、IOS 15.2(4)E 以降のバージョンでのみサポートされています。その他のスイッチでは、Virtual Route Forwarding（VRF）環境での WebAuth URL リダイレクトはサポートされていません。このような場合、回避策として、トラフィックを VRF に戻すためのルートをグローバル ルーティング テーブルに追加できます。

ゲストデバイスが NAD に接続されている場合、ゲスト サービスのインタラクションは、ゲスト ポータルの中央 WebAuth のログインにつながる MAC 認証バイパス（MAB）要求の形式を取ります。無線と有線の両方のネットワーク アクセス デバイスに適用される後続の中央 Web 認証（中央 WebAuth）プロセスの概要は、次のとおりです。

1. ゲスト デバイスは、有線接続によって NAD に接続します。ゲスト デバイス上に 802.1X サプリカントはありません。
2. MAB のサービス タイプを扱う認証ポリシーにより、MAB が引き続き失敗し、中央 WebAuth ユーザー インターフェイスの URL-redirect を含む制限付きネットワーク プロファイルが返されます。
3. NAD は、Cisco ISE RADIUS サーバーに対して MAB 要求を認証するように設定されています。
4. Cisco ISE RADIUS サーバーで MAB 要求が処理されますが、ゲスト デバイスのエンドポイントが見つかりません。

   この MAB の失敗により、制限付きネットワーク プロファイルが適用され、プロファイル内の URL-redirect 値が access-accept で NAD に返されます。この機能をサポートするには、許可ポリシーが存在し、適切な有線または無線 MAB（複合条件下で）と、任意で「Session:Posture Status=Unknown」条件が備わっていることを確認します。NAD では、この値に基づいて、デフォルト ポート 8443 のすべてのゲスト HTTPS トラフィックが URL-redirect 値にリダイレクトされます。

   この場合の標準の URL 値は次のとおりです。

   ```
   https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&portal=<PortalID>&action=cwa
   ```

5. ゲスト デバイスが、Web ブラウザから URL をリダイレクトするための HTTP 要求を開始します。
6. NAD により、最初の access-accept から返された URL-redirect 値に要求がリダイレクトされます。
7. CWA をアクションとしたゲートウェイ URL 値は、ゲスト ポータル ログイン ページにリダイレクトされます。
8. ゲストはログイン クレデンシャルを入力してログイン フォームを送信します。
9. ゲスト サーバーはログイン クレデンシャルを認証します。
10. フローのタイプに応じて、次の処理が実行されます。

- クライアントプロビジョニングを実行するようにゲストポータルが設定されていない非ポスチャフロー（これ以上の検証がない認証）の場合、ゲストサーバーはCoAを NAD に送信します。この CoA により、NAD は Cisco ISE RADIUS サーバーを使用してゲストデバイスを再認証します。設定されたネットワーク アクセスとともに新しい access-accept が NAD に返されます。クライアント プロビジョニングが未設定で、VLAN を変更する必要がある場合、ゲスト ポータルで VLAN IP の更新が行われます。ゲストはログイン クレデンシャルを再入力する必要はありません。初回ログイン時に入力したユーザー名とパスワードが自動的に使用されます。
- クライアントプロビジョニングを実行するようにゲストポータルが設定されているポスチャ フローの場合、ゲスト デバイスの Web ブラウザに、ポスチャ エージェントのインストールおよびコンプライアンスのための [クライアント プロビジョニング（Client Provisioning）] ページが表示されます。（必要に応じて、クライアント プロビジョニング リソース ポリシーに「NetworkAccess:UseCase=GuestFlow」条件を含めることもできます）。

Linux 向けのクライアント プロビジョニングやポスチャエージェントは存在しないため、ゲストポータルはクライアント プロビジョニング ポータルにリダイレクトされ、クライアント プロビジョニング ポータルは元のゲスト認証サーブレットにリダイレクトされます。この認証サーブレットで、必要に応じて IP リリース/更新が行われてから、CoA が実行されます。

クライアント プロビジョニング ポータルへのリダイレクションを使用して、クライアント プロビジョニング サービスはゲスト デバイスに非永続的 Web エージェントをダウンロードし、デバイスのポスチャ チェックを実行します必要に応じて、ポスチャポリシーに「NetworkAccess:UseCase=GuestFlow」条件を含めることもできます。

ゲスト デバイスが非準拠の場合、「NetworkAccess:UseCase=GuestFlow」条件および「Session:Posture Status=NonCompliant」条件を備えた許可ポリシーが設定済みであることを確認してください。

ゲスト デバイスが準拠している場合は、設定した許可ポリシーに「NetworkAccess:UseCase=GuestFlow」条件および「Session:Posture Status=Compliant」条件が含まれていることを確認してください。ここから、クライアント プロビジョニング サービスによって NAD に対して CoA が発行されます。この CoA により、NAD は Cisco ISE RADIUS サーバーを使用してゲストを再認証します。設定されたネットワーク アクセスとともに新しい access-accept が NAD に返されます。

（注） 「NetworkAccess: UseCase=GuestFlow」は、ゲストとしてログインする Active Directory および LDAP ユーザーにも適用できます。

ローカル WebAuth プロセス対応のワイヤレス LAN コントローラ

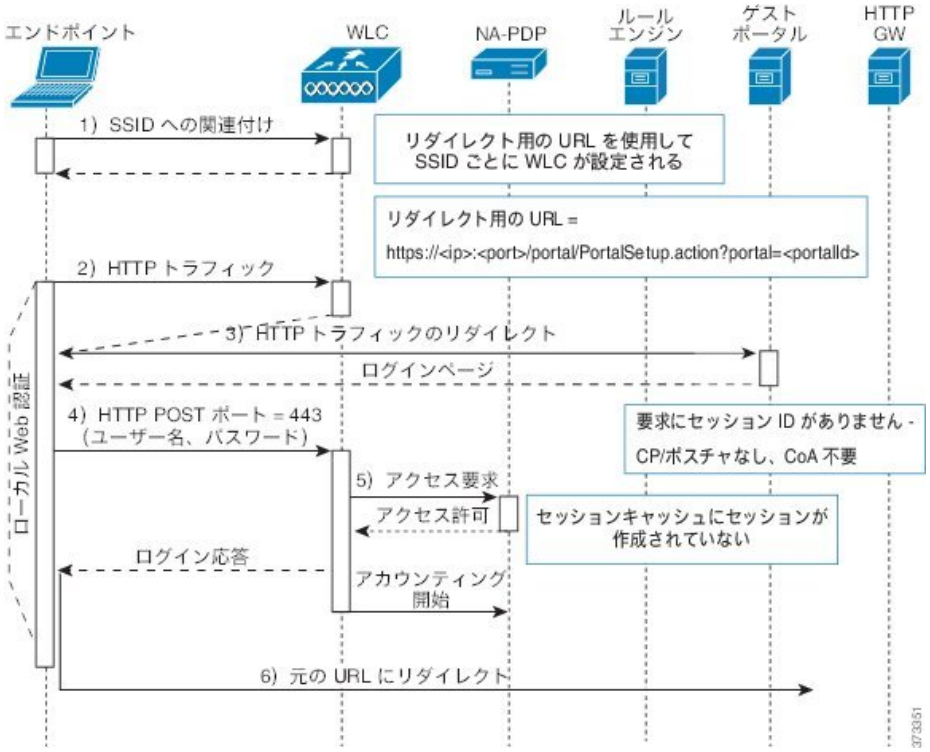
このシナリオでは、ゲストがログインすると、ワイヤレス LAN コントローラ（WLC）に転送されます。その後、WLC はゲストをゲスト ポータルにリダイレクトします。ゲスト ポータル

では、ログイン クレデンシャルの入力を求められ、必要に応じて利用規定（AUP）の受け入れやパスワードの変更を実行することもできます。

完了したら、ゲスト デバイスのブラウザは WLC にリダイレクトされ、POST 経由でログイン クレデンシャルが提供されます。

WLC は、Cisco ISE RADIUS サーバー経由でゲストのログイン処理を行うことができます。その処理が完了したら、WLC はゲスト デバイスのブラウザを元の URL の宛先にリダイレクトします。ゲスト ポータルの元の URL リダイレクトをサポートするためのワイヤレス LAN コントローラ（WLC）とネットワーク アクセス デバイス（NAD）の要件は、リリース IOS-XE 3.6.0.E および 15.2(2)E が動作する WLC 5760 および Cisco Catalyst 3850、3650、2000、3000、および 4000 シリーズ アクセス スイッチです。

図 *13 :* ローカル *WebAuth* 対応 *WLC* の *Non-Posture* フロー



ローカル WebAuth プロセス対応の有線 NAD

このシナリオでは、ゲスト ポータルにより、ゲストのログイン要求がスイッチ（有線 NAD）にリダイレクトされます。ログイン要求は、スイッチにポストされる HTTPS URL の形式になり、ログイン クレデンシャルが含まれます。スイッチにゲスト ログイン要求が届くと、設定済みの Cisco ISE RADIUS サーバーを使用してゲストの認証が行われます。

1. Cisco ISE により、HTML リダイレクトを含む login.html ファイルを NAD にアップロードするよう要求されます。HTTPS 要求が発生すると、この login.html ファイルがゲスト デバイスのブラウザに返されます。

2. ゲスト デバイスのブラウザがゲスト ポータルにリダイレクトされます。ここで、ゲストのログイン クレデンシャルが入力されます。
3. 利用規定（AUP）とパスワード変更が処理された後（両方ともオプションです）、ゲスト ポータルにより、ログイン クレデンシャルをポストするゲスト デバイスのブラウザが NAD にリダイレクトされます。
4. NAD により、Cisco ISE RADIUS サーバーに対して RADIUS 要求が発行され、ゲストの認証と許可が行われます。

Login.html ページに必要な IP アドレスおよびポートの値

login.html ページの次の HTML コードで、IP アドレスとポートの値を Cisco ISE ポリシー サービス ノードと同じ値に変更する必要があります。デフォルト ポートは 8443 ですが、この値を変更できます。そのため、スイッチに割り当てた値が Cisco ISE の設定と一致していることを確認してください。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/portal/PortalSetup.action?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/portal/PortalSetup.action?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</HTML>
```

カスタム ログイン ページはパブリック Web フォームであるため、次のガイドラインに従ってください。

- ログイン フォームは、ユーザーによるユーザー名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページ タイムアウト、パスワード非表示、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

NAD での HTTPS サーバーの有効化

Web ベース認証を使用するには、**ip http secure-server** コマンドを使用してスイッチ内で HTTPS サーバーを有効にする必要があります。

NAD 上でのカスタマイズされた認証プロキシ Web ページのサポート

成功、失効、失敗に関するカスタム ページを NAD にアップロードできます。Cisco ISE では特定のカスタマイズは必要ないため、NAD に付属する標準の設定手順を使用して、これらのページを作成できます。

NAD の Web 認証の設定

デフォルトの HTML ページをカスタム ファイルで置き換えて、NAD における Web 認証を完了する必要があります。

始める前に

Web ベースの認証中、スイッチのデフォルト HTML ページの代わりに使用する 4 つの代替 HTML ページを作成します。

ステップ 1 カスタム認証プロキシ Web ページを使用するように指定するには、最初にカスタム HTML ファイルをスイッチのフラッシュ メモリに格納します。スイッチのフラッシュ メモリに HTML ファイルをコピーするには、スイッチで次のコマンドを実行します。

copy tftp/ftp flash

ステップ 2 スイッチに HTML ファイルをコピーした後、グローバル コンフィギュレーション モードで次のコマンドを実行します。

ip admission proxy http login page file device:*login-filename*	スイッチのメモリ ファイル システム内で、デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの場所を指定します。device: はフラッシュ メモリです。
ip admission proxy http success page file device:*success-filename*	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ip admission proxy http failure page file device:*fail-filename*	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ip admission proxy http login expired page file device:*expired-filename*	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。

ステップ 3 スイッチによって提供されるガイドラインに従って、カスタマイズされた認証プロキシ Web ページを設定します。

ステップ 4 次の例に示すように、カスタム認証プロキシ Web ページの設定を確認します。

```
Switch# show ip admission configuration
Authentication proxy webpage
 Login page           : flash:login.htm
 Success page         : flash:success.htm
 Fail Page            : flash:fail.htm
 Login expired Page   : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

デバイス登録 WebAuth プロセス

デバイス登録 Web 認証（デバイス登録 WebAuth）およびホットスポット ゲスト ポータルを使用すると、ユーザー名とパスワードを要求しないで、プライベート ネットワークへの接続をゲスト デバイスに許可できます。

このシナリオでは、ゲストは無線接続でネットワークに接続します。デバイス登録 WebAuth プロセス フローの例については、図 14 : ワイヤレス デバイス登録 Web 認証フロー を参照してください。

後続のデバイス登録 WebAuth プロセスの概要を次に説明します。無線接続と有線接続の両方で同様のプロセスとなります。

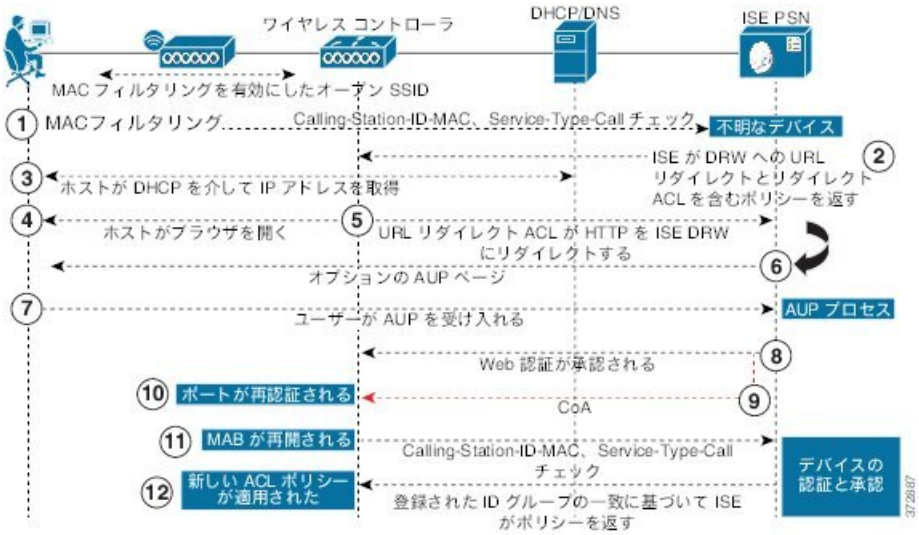
1. ネットワーク アクセス デバイス（NAD）がホットスポット ゲスト ポータルにリダイレクトを送信します。
2. ゲスト デバイスの MAC アドレスがいずれのエンドポイント ID グループにも含まれていないか、利用規定（AUP）accepted 属性が true に設定されていない場合、Cisco ISE は許可プロファイルに指定された URL リダイレクションを使用して応答します。
3. ゲストが何らかの URL にアクセスしようとすると、URL リダイレクションによって AUP ページ（有効な場合）が示されます。
   - ゲストが AUP を受け入れると、デバイスの MAC アドレスに関連付けられたエンドポイントが、設定されたエンドポイント ID グループに割り当てられます。ゲストによる AUP の受け入れを追跡できるよう、この時点で、このエンドポイントの AUP accepted 属性は true に設定されます。
   - ゲストが AUP を受け入れない場合、または、エンドポイントの作成中や更新中などにエラーが発生した場合、エラー メッセージが表示されます。
4. ホットスポット ゲスト ポータルの設定に基づいて、追加情報を含むポスト アクセス バナー ページが表示される場合があります（有効な場合）。

5. エンドポイントが作成または更新された後、許可変更（CoA）終了が NAD に送信されます。
6. CoA の後、NAD は MAC 認証バイパス（MAB）の新しい要求でゲスト接続を再認証します。新規認証では、エンドポイントとそれに関連付けられているエンドポイント ID グループが検索され、設定されているアクセスが NAD に返されます。
7. ホットスポット ゲスト ポータルの設定に基づいて、ゲストは、アクセスを要求した URL、管理者が指定したカスタム URL、または認証の成功ページに誘導されます。

有線とワイヤレスのどちらの場合も、CoA タイプは Termination CoA です。VLAN DHCP リリース（および更新）を実行するようにホットスポット ゲスト ポータルを設定し、それによって、有線と無線の両方の CoA タイプを許可変更に再許可できます。

VLAN DHCP リリースのサポートは、Windows デバイスのみで使用可能です。モバイル デバイスでは利用できません。登録するデバイスがモバイルで、[VLAN DHCP リリース（VLAN DHCP Release）] オプションが有効の場合、ゲストは手動で IP アドレスを更新することを要求されます。モバイル デバイスのユーザーの場合は、VLAN を使用するよりも、WLC でアクセス コントロール リスト（ACL）を使用することを推奨します。

図 *14 :* ワイヤレス デバイス登録 *Web* 認証フロー



ゲストポータルの設定

ポータル ID 設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータルまたはスポンサーポータル（Guest Portals or Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] >**

[ゲストポータルおよびスポンサーポータルの設定とカスタマイズ（Guest Portals or Sponsor Portals Settings and Customization）] です。

- [ポータル名（Portal Name）]：このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル（[ブロック済みリスト（Blocked List）]、[個人所有デバイス持ち込み（BYOD）（Bring Your Own Device (BYOD)）]、[クライアント プロビジョニング（Client Provisioning）]、[モバイルデバイス管理（MDM）（Mobile Device Management (MDM)）]、または [デバイス（My Devices）] の各ポータル）に使用しないでください。

  この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- [説明（Description）]：オプションです。

- [ポータルテスト URL（Portal test URL）]：[保存（Save）] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

  リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

（注） テストポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアントプロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

- [言語ファイル（Language File）]：各ポータルタイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

  言語ファイルには、特定のブラウザロケール設定へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。1つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

  1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザー Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイスポータルにも適用されます。

[ポータルページのカスタマイズ（Portal Page Customizations）] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に 1 つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

ホットスポット ゲスト ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで 8443 です。ただし、ブロックリストポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**

- スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディング インターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - NIC チーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイ

スへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループタグ（Certificate Group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループタグを選択します。
- [エンドポイント ID グループ（Endpoint Identity Group）]：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。
- [__日に達した場合にこの ID グループ内のエンドポイントを消去する（Purge Endpoints in this Identity Group when they Reach __ Days）]：Cisco ISE データベースからデバイスが消去されるまでの日数を指定します。消去は毎日実行され、消去アクティビティは全体的な消去タイミングと同期されます。変更は、このエンドポイント ID グループ全体に適用されます。

  その他のポリシー条件に基づいてエンドポイント消去ポリシーに変更が加えられた場合、この設定は使用できなくなります。
- **表示言語**
  - [ブラウザのロケールを使用する（Use Browser Locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語（Fallback Language）] が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback Language）]：ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always Use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する（User Browser Locale）] オプションを上書きします。

ホットスポット ゲスト ポータルの利用規定（AUP）ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal**

Behavior and Flow Settings）]>[アクセプタブル ユース ポリシー（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）] です。

- [AUP ページを含める（Include an AUP Page）]：会社のネットワーク使用諸条件を、別のページでユーザーに表示します。
- [アクセスコードが必要（Require an Access Code）]：複数のゲストがネットワークへのアクセスを獲得するために使用する必要があるログイン クレデンシャルとして、アクセス コードを割り当てます。アクセス コードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです（ホワイトボードによって視覚的に、またはロビーアンバサダーにより口頭で）。これは、ネットワークにアクセスするために部外者に認知されることも使用されることもありません。

  個別のゲストにログインクレデンシャルとして提供されるユーザー名とパスワードに加えて、このオプションを使用できます。
- [AUPの最後までのスクロールが必要（Require scrolling to end of AUP）]：ユーザーが AUP を完全に読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。AUP がユーザーに表示された場合に設定します。

ホットスポット ゲスト ポータルのフローを設定する場合、AUP アクセス コードはエンドポイント ID グループのデバイス登録によって異なります。

AUP アクセス コード ページは、MAC アドレスがホットスポット ポータルの設定に関連付けられたエンドポイントID グループから削除された後にのみ表示されます。エンドポイントは、Cisco ISE の [コンテキストの可視性（Context Visibility）] ページを介してデータベースから手動で削除するか、エンドポイント消去機能を使用し、エンドポイント消去ポリシーを設定して消去します。

ホットスポット ポータルのポストアクセス バナー ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）]>[ゲスト アクセス（Guest Access）]>[ポータルとコンポーネント（Portal s& Components）]>[ゲスト ポータル（Guest Portals）]>[作成、編集または複製（Create, Edit or Duplicate）]>[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]>[アクセス後のバナー ページ設定（Post-Access Banner Page Settings）]** です。

この設定を使用して、ゲストにアクセス ステータスおよび必要に応じてその他の追加アクションを通知します。

フィールド	使用上のガイドライン
アクセス後バナー ページを含める（Include a Post-Access Banner page）	ゲストが正常に認証された後、ネットワーク アクセスを付与される前に追加情報を表示します。

クレデンシャルを持つゲスト ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで8443です。ただし、ブロックリストポータルは8444です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニング ポータルはポート8905および8909も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

  同じHTTPSポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサーポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサーポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサーポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリストポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサーポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサーポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリストポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディング インターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - NIC チーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- **[認証方式（AuthenticationMethod）]**：ユーザー認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ID ソース順序は、ユーザークレデンシャルを確認するために順番に検索される ID ストアのリストです。

  Cisco ISE には、スポンサーポータル Sponsor_Portal_Sequence 用のデフォルトの ID ソース順序が含まれています。

  IdP を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

  ID ソース順序を設定するには、[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] を選択します。
- [ゲストとしてこのポータルを使用する従業員のログインオプションとダイナミック エンドポイント グループの割り当ての継承元（Employees Using this Portal as Guests Inherit Login Options and Dynamic Endpoint Group Assignment from）]：従業員がこのポータルにログインしたときに割り当てられるゲストタイプを選択します。従業員のエンドポイントデータは、そのゲストタイプで [エンドポイント アイデンティティ グループにデバイス情報を保存する（Store device information in endpoint identity group）] 属性に設定されたエンドポイント アイデンティティ グループに保存されます。関連付けられたゲスト タイプの他の属性は継承されません。
- **表示言語**
  - [ブラウザのロケールを使用する（Use Browser Locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語（Fallback Language）] が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback Language）]：ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always Use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する（User Browser Locale）] オプションを上書きします。

クレデンシャルを持つゲスト ポータルのログイン ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[作成、**

編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ログインページの設定（Login Page Settings）] です。

- [アクセスコードが必要（Require an Access Code）]：複数のゲストがネットワークへのアクセスを獲得するために使用する必要があるログイン クレデンシャルとして、アクセス コードを割り当てます。アクセス コードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです（ホワイトボードによって視覚的に、またはロビーアンバサダーにより口頭で）。これは、ネットワークにアクセスするために部外者に認知されることも使用されることもありません。

  個別のゲストにログイン クレデンシャルとして提供されるユーザー名とパスワードに加えて、このオプションを使用できます。

- [レート制限までの最大ログイン試行失敗数（Maximum Failed Login Attempts Before Rate Limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。

- [レート制限時のログイン試行間隔（Time Between Login Attempts when Rate Limiting）]：[レート制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザーが再度ログインを試行するまでに待機する必要がある時間（スロットル率）を分単位で設定します。

- [AUP を含める（Include an AUP）]：フローにアクセプタブル ユース ポリシー ウィンドウを追加します。AUP をウィンドウに追加したり、別のウィンドウへのリンクを設定することができます。

- [ゲストに自分自身のアカウントの作成を許可（Allow Guests to Create their Own Accounts）]：このポータルの [ログイン（Login）] ページで、ゲストが自身を登録するためのオプションが提供されます。このオプションが選択されていない場合は、スポンサーがゲストアカウントを作成します。これを有効にすることで、このページのタブが有効になり、[アカウント登録ページの設定（Self-Registration Page Settings）] および [アカウント登録成功ページの設定（Self-Registration Success Page Settings）] を設定できます。

  ゲストがこのオプションを選択した場合、自身のゲストアカウントを作成するために必要な情報を入力できるアカウント登録フォームが示されます。

- [ゲストにパスワードのリセットを許可（Allow Guests to Recover the Password）]：このオプションは、アカウント登録ゲストに対し、ゲストポータルの [パスワードのリセット（Reset Password）] ボタンを有効にします。有効なアカウントを持つアカウント登録ゲストがログイン ポータルに接続し、パスワードを忘れた場合は、[パスワードのリセット（Reset Password）] をクリックできます。これにより、ゲストは自分の電話番号または電子メール（いずれかを登録に使用）を入力できるアカウント登録ウィンドウに戻ります。

- [ソーシャルログインを許可（Allow Social Login）]：このポータルのユーザーのログイン クレデンシャルを取得するためにソーシャル メディア サイトを使用します。このオプションをチェックすると、次の設定が表示されます。

- [ソーシャルログイン後に登録フォームを表示（Show registration form after social login）]：これにより、ユーザーはFacebookによって提供される情報を変更できます。
- [ゲストの承認が必要（Require guests to be approved）]：スポンサーがアカウントを承認する必要があることをユーザーに通知し、ログイン用のクレデンシャルを送信します。

- [ゲストにログイン後のパスワード変更を許可（Allow guests to change password after login）]：ゲストが正常に認証され、AUPに同意した後に、ゲストに必要に応じてパスワードを変更することを許可します。ゲストが自分のパスワードを変更した場合、スポンサーはゲストにログインクレデンシャル情報を提供できません。スポンサーは、ゲストのパスワードをランダム パスワードにリセットすることだけが可能です。

（注） ゲストポータルからログインした内部ユーザーは、パスワードをリセットできません。

- [ログインに次の ID プロバイダーゲストポータルの使用を許可（Allow the following identity-provider guest portal to be used for login）]：このオプションをオンにし、SAML Id ID プロバイダーを選択すると、その SAML ID のリンクがこのポータルに追加されます。このサブ ポータルは、ユーザーが証明書を提供している SAML IDP のように見えるように設定できます。
- [ソーシャルログインを許可（Allow social login）]：このポータルはすべて、ユーザーログインにソーシャルメディアタイプを使用します。ソーシャルログインの設定の詳細については、アカウント登録ゲストのソーシャルログイン（834ページ）を参照してください。

アカウント登録ページの設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portal & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [アカウント登録ページの設定（Self-Registration Page Settings）]** です。これらの設定を使用して、ゲストが自身を登録し、提供する必要がある情報をアカウント登録フォームで指定できるようにします。

- [ゲストタイプへのアカウント登録ゲストの割り当て（Assign self-registered guests to guest type）]：このポータルを使用するすべてのアカウント登録ゲストに割り当てるゲストタイプを選択します。
- [アカウントの有効期間（Account valid for）]：アカウントの有効期間を、日、時間、または分で指定します。この期間を超過した場合、管理者またはスポンサーがスポンサーポータルでアカウントの有効期間を延長した場合を除き、アカウントは失効します。

- [アカウント登録に登録コードを必要とする（Require a registration code for self registration）]：アカウント登録ゲストがアカウント登録フォームを正常に送信するために入力する必要があるコードを割り当てます。部外者がシステムにアクセスすることを防ぐために、アクセス コードと同様に、登録コードはオフラインで提供されます。

- [含めるフィールド（Fields to include）]：アカウント登録フォームに表示するフィールドのチェックボックスをオンにします。その後、ゲストがこのフォームを送信してゲストアカウントを受信するために入力が必須であるフィールドのチェックボックスをオンにします。アカウント登録ゲストから重要な情報を収集するために、[SMS サービス プロバイダー（SMS Service Provider）] および [訪問先担当者（Person being Visited）] フィールドを必須にすることができます。

  - [場所（Location）]：アカウント登録ゲストが定義済みリストを使用して登録時に選択できる場所を入力します。これにより、これらのゲストの有効なアクセス時間として自動的に関連するタイム ゾーンが割り当てられます。場所の名前は、選択時に混乱を回避するために具体的なものを使用します（たとえば、ボストン オフィス、500 Park Ave New York、シンガポールなど）。

    ゲスト アクセスを時間で制限する予定の場合は、その時間を設定するときにタイム ゾーンを使用します。アクセス時間が制御されたゲスト全員がサンノゼのタイム ゾーンにいる場合を除き、各自のロケールのタイム ゾーンを作成します。場所が 1 つだけである場合は、その場所がデフォルトの場所として自動的に割り当てられ、ポータルではこのフィールドがゲストに対して表示されません。また、[場所（Location）] は、[含めるフィールド（Fields to include）] のリスト内で無効になります。

  - [SMS サービスプロバイダー（SMS Service Provider）]：アカウント登録フォームに SMS プロバイダーを表示して、アカウント登録ゲストが自分の SMS プロバイダーを選択できるようにします。これで、会社の経費を最小化するために、ゲストの SMS サービスを使用して SMS 通知を送信できるようになります。ゲストが使用できる SMS プロバイダーを 1 つだけ選択した場合は、このフィールドはアカウント登録フォームに表示されません。

  - [訪問先担当者（Person being Visited）]：これはテキストフィールドです。そのため、このフィールドを使用する場合には、このフィールドに入力する情報についてゲストに説明してください。

  - [カスタムフィールド（Custom Fields）]：アカウント登録ゲストから追加のデータを収集するために作成したカスタムフィールドを選択します。その後、ゲストがアカウント登録フォームを送信してゲスト アカウントを受信するために入力が必須であるフィールドのチェックボックスをオンにします。これらのフィールドは名前のアルファベット順に表示されます。追加のカスタムフィールドを追加するには、**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[設定（Settings）]** > **[カスタムフィールド（Custom Fields）]** でこれらのフィールドを作成します。

  - [AUP を含める（Include an AUP）]：会社のネットワークの使用についての諸条件を、現在ユーザーに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。

- [同意が必要（Require acceptance）]：ユーザーが AUP を最後まで読んだことを確認します。これにより、アカウント登録ページの [同意する（Accept）] ボタンが設定されます。AUP を [ページ（as on page）] として設定する場合は、ユーザーが AUP の終わりまでスクロールするまで [同意する（Accept）] ボタンを無効にすることもできます。

- [次の電子メールアドレスを持つゲストのみを許可（Only allow guests with an email address from）]：アカウント登録ゲストが電子メールアドレスを作成するときに [電子メールアドレス（Email Address）] で使用できるドメイン（例：cisco.com）の許可されたリストを指定します。

  このフィールドを空白のままにすると、[次の電子メール アドレスを持つゲストを許可しない（Do not allow guests with email address from）] にリストされているドメイン以外のすべての電子メール アドレスが有効になります。

- [次の電子メールアドレスを持つゲストを許可しない（Do not allow guests with email address from）]：アカウント登録ゲストが電子メールアドレスを作成するときに [電子メールアドレス（Email Address）] に使用できないドメイン（例：czgtgj.com）のブロック済みリストを指定します。

- [アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）]：このポータルを使用するアカウント登録ゲストは、ゲストのクレデンシャルを受信する前にスポンサーによる承認が必要であることを指定します。このオプションをクリックすると、スポンサーがアカウント登録ゲストを承認する方法に関する追加のオプションが表示されます。

  - [アカウント登録したゲストにスポンサーの承認後に自動ログインを許可（Allow guests to login automatically from self-registration after sponsor's approval）]：アカウント登録ゲストは、スポンサーの承認後に自動的にログインします。

  - [承認要求電子メール送信先（Email approval request to）]：

    - [下に示すスポンサーの電子メールアドレス（Sponsor email addresses listed below）]：承認者として指名されたスポンサーの 1 つ以上の電子、またはすべてのゲストの承認要求の送信先となるメール ソフトウェアを入力します。電子メール アドレスが無効な場合、承認は失敗します。

    - [訪問先担当者（Person being visited）]：[スポンサーに承認用クレデンシャルの入力を求める（Require sponsor to provide credentials for authentication）] フィールドが表示され、[含めるフィールド（Fields to include）] の [必須（Required）] オプションが有効になります（以前は無効だった場合）。これらのフィールドはアカウント登録フォームに表示され、アカウント登録ゲストからこの情報を要求します。電子メール アドレスが無効な場合、承認は失敗します。

  - [承認/拒否リンクの設定（Approve/Deny Link Settings）]：

    - [リンクの有効期間（Links are valid for）]：アカウント承認リンクの有効期間を設定できます。

- [スポンサーに承認用クレデンシャルの入力を求める（Require sponsor to provide credentials for authentication）]：このセクションの設定でスポンサーによるアカウント承認用のクレデンシャルの入力が必須ではない場合にも、スポンサーにこの情報を入力させるには、このフィールドをオンにします。このフィールドは、[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] が [訪問先担当者（person being visited）] に設定されている場合にだけ表示されます。
- [承認権限を検証するためスポンサーがスポンサーポータルと照合される（Sponsor is matched to a Sponsor Portal to verify approval privileges）]：[詳細（Details）] をクリックして、スポンサーが有効なシステム ユーザーであり、スポンサー グループのメンバーであり、そのスポンサー グループのメンバーにアカウント承認権限があることを確認するために検索されるポータルを選択します。各スポンサーポータルには、スポンサーを識別するために使用される ID ソース シーケンスがあります。ポータルはリストされている順序で使用されます。リストの 1 番目のポータルは、スポンサーポータルで使用されているスタイルとカスタマイズ内容を決定します。

- [登録の送信後のゲストの誘導先（After registration submission, direct guest to）]：登録の正常完了後にアカウント登録ゲストを誘導する場所を選択します。
  - [アカウント登録成功（Self-Registration Success）] ページ：アカウント登録に成功したゲストを [アカウント登録成功（Self-Registration Success）] ウィンドウに誘導します。このウィンドウには、[アカウント登録成功ページ設定（Self Registration Success Page Settings）] で指定したフィールドとメッセージが表示されます。

    すべての情報を表示することが望ましくない場合があります。システムはアカウントの承認待ち（このウィンドウで有効になっている場合）であるか、またはこのウィンドウで指定された許可されたリストのドメインおよびブロックされているリストのドメインに基づいて電子メールアドレスまたは電話番号にログインクレデンシャルを提供する可能性があるためです。

    [アカウント登録成功ページの設定（Self Registration Success Page Settings）] で [ゲストのアカウント登録成功ページからの直接ログインを許可する（Allow guests to log in directly from the Self-Registration Success page）] を有効にした場合、アカウント登録に成功したゲストはこのウィンドウから直接ログインすることができます。これが有効になっていない場合、ゲストは [アカウント登録成功（Self-Registration Success）] ウィンドウが表示された後にポータルのログイン ウィンドウに誘導されます。
  - [ログインクレデンシャルを取得する方法の手順を含むログインページ（Login page with instructions about how to obtain login credentials）]：アカウント登録に成功したゲストをポータルのログインウィンドウに再び誘導し、「ゲスト クレデンシャルが電子メール、SMS、または印刷物で提供されるのを待ってからログインに進んでください。（Please wait for your guest credentials to be delivered either via email, SMS, or print format and proceed with logging in）」などのメッセージを表示します。

デフォルト メッセージをカスタマイズするには、[ポータル ページのカスタマイズ（Portal Page Customization）] タブをクリックして、[アカウント登録ページ設定（Self Registration Page Settings）] を選択します。

システムはアカウントの承認待ち（このウィンドウで有効になっている場合）であるか、またはこのウィンドウで指定された許可されたリスト、ブロックされているリストのドメインに基づいて電子メールアドレスまたは電話番号にログインクレデンシャルを提供する可能性があります。

- [URL]：アカウント登録に成功したゲストを、アカウントクレデンシャルの提供を待機している間に、指定された URL に誘導します。

  システムはアカウントの承認待ち（このウィンドウで有効になっている場合）であるか、またはこのウィンドウで指定された許可されたリスト、ブロックされているリストのドメインに基づいて電子メールアドレスまたは電話番号にログインクレデンシャルを提供する可能性があります。

- [クレデンシャル通知自動送信手段（Send credential notification automatically using）]：
  - [電子メール（Email）]：アカウント登録に成功したゲストがログインクレデンシャルを受信する手段のオプションとして電子メールを選択します。このオプションを選択した場合、[電子メール アドレス（Email address）] が [含めるフィールド（Fields to include）] のリストで必須フィールドになり、このオプションを無効にできなくなります。
  - [SMS]：アカウント登録に成功したゲストがログインクレデンシャルを受信する手段のオプションとして SMS を選択します。このオプションを選択した場合、[SMS サービス プロバイダー（SMS Service Provider）] が [含めるフィールド（Fields to include）] のリストで必須フィールドになり、このオプションを無効にできなくなります。

アカウント登録成功ページの設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portal s& Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [アカウント登録成功ページ設定（Self Registration Success Page**

Settings）] です。これらの設定を使用して、正常にアカウント登録したゲストに、ネットワークへのアクセスを獲得するために必要なクレデンシャルを通知します。

フィールド	使用上のガイドライン
アカウント登録の成功ページにこの情報を含める（Include this information on the Self-Registration Success page）	[アカウント登録成功（Self-Registration Success）] ページで正常に登録されたゲストに表示されるフィールドのチェックボックスをオンにします。 スポンサーによるゲストの承認が必要ない場合は、[ユーザー名（Username）] と [パスワード（Password）] のチェックボックスをオンにして、ゲストにこれらのクレデンシャルを表示します。スポンサーの承認が必要な場合、クレデンシャルはゲストが承認された後にのみ提供されるため、これらのフィールドを無効にします。
ゲストは次の手段で情報を自分に送信できる（Allow guest to send information to self using）	正常にアカウント登録したゲストが自分自身にクレデンシャル情報を送信するためのオプションのチェックボックスをオンにします。[印刷（Print）]、[電子メール（Email）]、または [SMS]。
AUPをページに含める/AUPをリンクとして含める（Include an AUP (on page/as link)）	会社のネットワーク使用の諸条件を、現在ユーザーに表示されているウィンドウ上のテキストとして、またはAUPテキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
同意が必要（Require Acceptance）	ユーザーのアカウントが完全に有効になる前に、ユーザーはAUPに同意する必要があります。[ログイン（Login）] ボタンは、ユーザーがAUPを受け入れない場合は有効になりません。ユーザーがAUPに同意しない場合、ネットワークにアクセスできません。
AUPの最後までのスクロールが必要（Require scrolling to end of AUP）	このフィールドは、[ページ上の AUP（AUP on page）] オプションを選択した場合のみ表示されます。 ユーザーがAUPを最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーがAUPの最後までスクロールすると有効になります。

フィールド	使用上のガイドライン
ゲストをアカウント登録の成功ページから直接ログインできるようにする（Allow guests to log in directly from the Self-Registration Success page）	[アカウント登録の成功（Self-Registration Success）] ページ下部に [ログイン（Login）] ボタンを表示します。これにより、ゲストはログイン ページをバイパスし、自動的にログイン クレデンシャルをポータルに提供して、ポータル フローの次のページ（たとえばAUP ページ）を表示できるようになります。

クレデンシャルを持つゲスト ポータルの利用規定（AUP）ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [アクセプタブル ユース ポリシー（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]** です。

- [AUP ページを含める（Include an AUP Page）]：会社のネットワーク使用諸条件を、別のページでユーザーに表示します。
- [従業員に別の AUP を使用する（Use Different AUP for Employees）]：従業員専用に別の AUP およびネットワーク使用諸条件を表示します。このオプションを選択すると、[従業員用の AUP をスキップ（Skip AUP for employees）] は選択できません。
- [従業員用の AUP をスキップ（Skip AUP for Employees）]：従業員は、ネットワークにアクセスする前に AUP に同意する必要はありません。このオプションを選択すると、[従業員に別の AUP を使用する（Use different AUP for employees）] は選択できません。
- [AUP の最後までのスクロールが必要（Require Scrolling to End of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。

  ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。AUP がユーザーに表示された場合に設定します。

  - [初回のログインのみ（On First Login only）]：ユーザーが初めてネットワークまたはポータルにログインしたときに AUP を表示します。
  - [ログインごと（On Every Login）]：ユーザーがネットワークまたはポータルにログインするごとに、AUP を表示します。
  - [__ 日ごと（初回のログインから）（Every __ Days (starting at first login)）]：ネットワークやポータルにユーザーが初めてログインした後は、AUP を定期的に表示します。

クレデンシャルを持つゲストポータルのゲストによるパスワード変更の設定

ゲストのパスワード変更設定（Guest Change Password Settings）

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ゲストによるパスワード変更設定（Guest Change Password Settings）]** です。

- [ゲストにログイン後のパスワード変更を許可（Allow guests to change password after login）]：ゲストが正常に認証され、AUPに同意した後に、ゲストに必要に応じてパスワードを変更することを許可します。ゲストが自分のパスワードを変更した場合、スポンサーはゲストにログインクレデンシャル情報を提供できません。スポンサーは、ゲストのパスワードをランダム パスワードにリセットすることだけが可能です。

（注） ゲストポータルからログインした内部ユーザーは、パスワードをリセットできません。

クレデンシャルを持つゲスト ポータルのゲスト デバイス登録の設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ゲストデバイス登録設定（Guest Device Registration Settings）]** です。

これらの設定を使用して、ゲストがログインしたら Cisco ISE がゲストのデバイスを自動的に登録するようにするか、ゲストがログイン後に手動で自身のデバイスを登録することを許可できます。

各ゲスト タイプの最大デバイス数は、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト タイプ（Guest Types）]** で指定されます。

- [ゲストのデバイスを自動登録（Automatically Register Guest Devices）]：ゲストがこのポータルにアクセスするデバイスのエンドポイントを自動的に作成します。エンドポイントは、このポータルに指定されたエンドポイント ID グループに追加されます。

  許可ルールの作成が可能になり、該当 ID グループ内のエンドポイントへのアクセスが許可されます。そのため、Web 認証は不要になります。

登録済みデバイスの最大数に到達すると、システムは自動的に最初の登録デバイスを削除し、ゲストがログインしようとしているデバイスを登録し、このことをゲストに通知します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストタイプ（Guest Types）]** を選択し、ゲストが登録できるデバイスの最大数を変更します。

- [ゲストにデバイスの登録を許可（Allow Guests to Register Devices）]：ゲストは、名前、説明、および MAC アドレスを入力して、自分のデバイスを手動で登録できます。MAC アドレスはエンドポイント ID グループに関連付けられます。

  登録済みデバイスの最大数に到達した場合に別のデバイスを登録できるようにするには、ゲストは少なくとも 1 個のデバイスを削除する必要があります。

クレデンシャルを持つゲスト ポータルの BYOD 設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[BYOD 設定（BYOD Settings）]** です。

この設定を使用して、従業員などゲスト以外の個人所有デバイスの持ち込み（BYOD）機能を有効にし、クレデンシャルを持つゲスト ポータルを使用して企業ネットワークにアクセスできるようにします。

フィールド	使用上のガイドライン
従業員がネットワークでパーソナルデバイスを使用することを許可する（Allow Employees to use Personal Devices on the Network）	このポータルに [BYOD の登録（BYOD Registration）] ウィンドウを追加して、従業員がデバイス登録プロセスを実行できるようにして、場合によってはネイティブサプリカントおよび証明書のプロビジョニングを実行できるようにします。これは、従業員のパーソナルデバイスタイプ（iOS、Android、OSX など）のクライアント プロビジョニングの設定に応じて異なります。
エンドポイント ID グループ（Endpoint Identity Group）	ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

フィールド	使用上のガイドライン
従業員にゲスト アクセスの選択のみを許可する（**Allow employees to choose to get guest access only**）	従業員をゲスト ネットワークにアクセスさせて、企業ネットワークへのアクセスに必要になることがある追加のプロビジョニングおよび登録を避けます。
登録時にデバイス ID フィールドを表示する（**Display Device ID Field During Registration**）	登録プロセス中に、デバイス ID をユーザーに表示します。これは、デバイス ID が事前設定されており、BYOD ポータルを使用しているときに変更できない場合も含みます。
元の URL（**Originating URL**）	ネットワークへの認証に成功すると、可能な場合はユーザーのブラウザを、ユーザーがアクセスしようとしていた元の Web サイトにリダイレクトします。使用できない場合は、[認証成功（Authentication Success）] ウィンドウが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の Cisco ISE で設定された認証プロファイルにより、PSN のポート 8443 で動作することを確認します。 Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザード アプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS（dot1X）およびサポート対象外のデバイス（ネットワーク アクセスが許可されている）では、この URL にリダイレクトされます。
成功ページ（**Success page**）	デバイスの登録が成功したことを示すページを表示します。
URL	ネットワークへの認証に成功すると、ユーザーのブラウザを指定された URL（会社の Web サイトなど）にリダイレクトします。

クレデンシャルを持つゲスト ポータルのポストログイン バナー ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータルまたはスポンサーポータル**

（Guest Portals or Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポストログインバナーページ設定（Post-Login Banner Page Settings））] です。

これらの設定を使用して、正常なログイン後にユーザー（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

フィールド	使用上のガイドライン
ポストログインバナーページを含める（Include a Post-Login Banner page）	ユーザーが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

クレデンシャルを持つゲスト ポータルのゲスト デバイスのコンプライアンス設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ゲストデバイスのコンプライアンス設定（Guest Device Compliance Settings）]** です。これらの設定を使用して、ネットワークにアクセスするためにデバイスのクライアント プロビジョニングを実行するようゲストおよびゲスト ポータルを使用する従業員に要求します。

- [ゲスト デバイス コンプライアンスが必要（Require guest device compliance）]：ゲストをポスチャ エージェントのダウンロードを要求する [クライアントプロビジョニング（Client Provisioning）] ページにリダイレクトします。これにより、ウイルス対策ソフトウェアのチェックなど、ゲストのポスチャ ポリシーを設定するゲスト フローにクライアント プロビジョニングが追加されます。

  ゲストが、ネットワークへのアクセスにクレデンシャルを持つゲスト ポータルを使用している従業員の場合：

  - [BYOD 設定（BYOD Settings）] で [従業員にネットワークでのパーソナル デバイスの使用を許可する（Allow employees to use personal devices on the network）] が有効になっている場合、従業員はBYODフローにリダイレクトされ、クライアントのプロビジョニングは実行されません。

  - [BYOD 設定（BYOD Settings）] で [従業員にネットワークでのパーソナル デバイスの使用を許可する（Allow employees to use personal devices on the network）] および [従業員にゲスト アクセスの選択のみを許可する（Allow employees to choose to get guest access only）] が有効になっていて、従業員がゲスト アクセスを選択する場合、[クライアント プロビジョニング（Client Provisioning）] ページにルーティングされます。

ゲスト ポータルの VLAN DHCP リリース ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portal s& Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [VLAN DHCP リリースページの設定（VLAN DHCP Release Page Settings）]** です。

- [VLAN DHCPリリースを有効にする（Enable VLAN DHCP release）]：有線環境と無線環境の両方でVLANが変更された後、WindowsデバイスのゲストのIPアドレスを更新します。

  これは、ネットワーク アクセスでゲスト VLAN が新しい VLAN に変更されたときに、最終的な許可処理時の中央 WebAuth（CWA）フローに影響します。ゲストの古い IP アドレスは VLAN の変更の前にリリースされる必要があり、ゲストが新しい VLAN に接続するときに新しいゲスト IP アドレスが DHCP を介して要求される必要があります。IP アドレスのリリースと更新操作は、DirectX コントロールを使用する Internet Explorer ブラウザのみでサポートされています。

  VLAN DHCP リリース オプションは、モバイル デバイスでは動作しません。代わりに、ゲストが IP アドレスを手動でリセットする必要があります。この方法はデバイスによって異なります。たとえば、Apple iOS デバイスでは、ゲストは Wi-Fi ネットワークを選択して、[リースを更新（Renew Lease）] ボタンをクリックできます。

- [リリースを__秒遅延（Delay to Release __ Seconds）]：リリース遅延時間を入力します。リリースは、アプレットをダウンロードした直後から、Cisco ISE サーバーが CoA 要求を再認証するよう NAD に指示するまでの間に行う必要があるため、この時間は短くすることを推奨します。

- [CoA を__秒遅延（Delay to CoA __ Seconds）]：Cisco ISE が CoA の実行を遅延する時間を入力します。十分な時間を指定して（ガイドラインとしてデフォルト値を使用）、アプレットによるクライアント上での IP リリースのダウンロードと実行を可能にします。

- [更新を__秒遅延（Delay to Renew __ Seconds）]：更新を遅延する値を入力します。この時間は IP リリース値に追加され、コントロールがダウンロードされるまで計時が開始されません。十分な時間を指定して（ガイドラインとしてデフォルト値を使用）、CoAの処理を可能にし、新しい VLAN アクセスが付与されるようにします。

ゲスト ポータルの認証成功の設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [認証成功の設定（Authentication Success Settings）]** です。

これらの設定では、ユーザー（状況に応じてゲスト、スポンサーまたは従業員）に認証の成功が通知されるか、または URL が表示されます。[認証されたらゲストに次を表示：（Once authenticated, take guest to:）] で、次のフィールドを設定します。

- [元の URL（Originating URL）]：ネットワークへの認証に成功すると、可能な場合はユーザーのブラウザを、ユーザーがアクセスしようとしていた元の Web サイトにリダイレクトします。使用できない場合は、[認証成功（Authentication Success）] ウィンドウが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。

  Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザード アプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS（dot1X）およびサポート対象外のデバイス（ネットワーク アクセスが許可されている）では、この URL にリダイレクトされます。

- [認証の成功（Authentication Success）] ページ：ユーザー認証成功の通知。
- [URL]：ネットワークへの認証に成功すると、ユーザーのブラウザを指定された URL（会社の Web サイトなど）にリダイレクトします。

（注） 認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。

ゲスト ポータルのサポート情報ページの設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [サポート情報ページの設定（Support Information Page Settings）]** です。

これらの設定を使用して、ヘルプデスクがユーザー（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

フィールド	使用上のガイドライン
サポート情報ページを含める（Include a Support Information Page）	該当ポータルのすべての有効なページ上で、[問い合わせ先（Contact Us）] などの情報へのリンクを表示します。

フィールド	使用上のガイドライン
MAC アドレス（MAC Address）	[サポート情報（Support Information）] ウィンドウにデバイスの MAC アドレスを含めます。
IP アドレス（IP Address）	[サポート情報（Support Information）] ウィンドウにデバイスの IP アドレスを含めます。
ブラウザのユーザーエージェント（Browser User Agent）	[サポート情報（Support Information）] ページに、要求の発信元の製品名とバージョン、レイアウトエンジン、ユーザーエージェントのバージョンなど、ブラウザの詳細を含めます。
ポリシーサーバー（Policy Server）	[サポート情報（Support Information）] ウィンドウに、このポータルを提供している ISE ポリシーサービスノード（PSN）の IP アドレスを含めます。
障害コード（Failure code）	可能な場合は、ログメッセージカタログ内の対応する番号を含めます。メッセージカタログを表示するには、**[管理（Administration）]**> **[システム（System）]** > **[ロギング（Logging）]**>**[メッセージカタログ（Message Catalog）]** を選択します。
フィールドを非表示にする（Hide Field）	含める情報が存在しない場合、[サポート情報（Support Information）] ウィンドウ上の該当するフィールドのラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード（Failure Code）] は、選択されている場合でも表示されません。
値のないラベルを表示（Display label with no value）	含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを [サポート情報（Support Information）] ウィンドウに表示します。たとえば、障害コードが不明な場合、[障害コード（Failure Code）] は空白であっても表示されます。
デフォルト値でラベルを表示（Display Label with Default Value）	含める情報が存在しない場合、[サポート情報（Support Information）] ウィンドウ上の選択されているすべてのフィールドにこのテキストが表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード（Failure code）] に [使用できません（Not Available）] と表示されます。

スポンサー ポータル アプリケーションの設定

ポータル ID 設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータルまたはスポンサーポータル（Guest Portals or Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ゲストポータルおよびスポンサーポータルの設定とカスタマイズ（Guest Portals or Sponsor Portals Settings and Customization）]** です。

- [ポータル名（Portal Name）]：このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル（[ブロック済みリスト（Blocked List）]、[個人所有デバイス持ち込み（BYOD）（Bring Your Own Device (BYOD)）]、[クライアント プロビジョニング（Client Provisioning）]、[モバイルデバイス管理（MDM）（Mobile Device Management (MDM)）]、または [デバイス（My Devices）] の各ポータル）に使用しないでください。

  この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- [説明（Description）]：オプションです。

- [ポータルテスト URL（Portal test URL）]：[保存（Save）] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

  リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

（注） テストポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアントプロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

- [言語ファイル（Language File）]：各ポータルタイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファ

イルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

言語ファイルには、特定のブラウザロケール設定へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。1つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザー Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイスポータルにも適用されます。

[ポータルページのカスタマイズ（Portal Page Customizations）] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に 1 つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

スポンサー ポータルのポータル設定

これらの設定を設定して、ポータルを特定し、すべてのポータルページで使用する言語ファイルを選択します。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで 8443 です。ただし、ブロックリストポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**

- スポンサーポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリストポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**

- 無効な組み合わせには次が含まれます。
  - スポンサーポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサーポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリストポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシーサービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディング インターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記

録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。

- NIC チーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループタグ（Certificate Group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループタグを選択します。

- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：[スポンサー（Sponsor）] ポータルまたは [デバイス（MyDevices）] ポータルの固有の FQDN またはホスト名を 1 つの以上入力します。たとえば、**sponsorportal.yourcompany.com,sponsor** と入力することで、ユーザーはブラウザにこれらのいずれかを入力すると、が表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

  デフォルトの FQDN を変更する場合は、次を実行します。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。

  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカルサーバー証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。[Kerberos SSO を許可（Allow Kerberos SSO）] オプションがスポンサーポータルで有効になっている場合は、ポータルで使用されるローカルサーバー証明書の SAN 属性に Cisco ISE PSN の FQDN またはワイルドカードを含める必要があります。

- **[認証方式（AuthenticationMethod）]**：ユーザー認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ID ソース順序は、ユーザークレデンシャルを確認するために順番に検索される ID ストアのリストです。

  Cisco ISE には、スポンサーポータル Sponsor_Portal_Sequence 用のデフォルトの ID ソース順序が含まれています。

  IdP を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

  ID ソース順序を設定するには、[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] を選択します。

- [アイドルタイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザーをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。
- [Kerberos を許可する（Allow Kerberos）]：スポンサーポータルへアクセスするためのスポンサーの認証に Kerberos を使用します。ブラウザが ISE との SSL 接続を確立した後、セキュア トンネル内で Kerberos SSO が実行されます。

  Kerberos 認証には、同じドメイン内に存在する次の項目が必要です。

  - スポンサーの PC
  - ISE PSN
  - このスポンサー ポータルに設定された FQDN

（注） ゲスト ポータルの Kerberos 認証はサポートされていません。

- **表示言語**
  - [ブラウザのロケールを使用する（Use Browser Locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語（Fallback Language）] が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback Language）]：ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always Use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する（User Browser Locale）] オプションを上書きします。
- [スポンサーに使用可能な SSID（SSIDs Available to Sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッションサービス識別子）を入力します。

スポンサー ポータルのログイン設定

スポンサー ポータルのログイン ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Sponsor Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ログインページの設定（Login Page Settings）]** です。

- [レート制限までの最大ログイン試行失敗数（Maximum Failed Login Attempts Before Rate Limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [レート制限時のログイン試行間隔（Time Between Login Attempts when Rate Limiting）]：[レート制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザーが再度ログインを試行するまでに待機する必要がある時間（スロットル率）を分単位で設定します。
- [AUP を含める（Include an AUP）]：フローにアクセプタブル ユース ポリシー ウィンドウを追加します。AUP をウィンドウに追加したり、別のウィンドウへのリンクを設定することができます。

スポンサー ポータルの利用規定（AUP）設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [アクセプタブル ユース ポリシー（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]** です。

これらの設定を使用して、ユーザー（状況に応じてゲスト、スポンサーまたは従業員）に対して AUP エクスペリエンスを定義します。

フィールド	使用上のガイドライン
AUP ページを含める（Include AUP Page）	会社のネットワーク使用諸条件を、別のページでユーザーに表示します。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールすると有効になります。
初回ログイン時のみ（On First Login only）	ユーザーがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
ログインごと（On Every Login）	ユーザーがネットワークまたはポータルにログインするごとに、AUP を表示します。
__日ごと（初回のログインから）（Every __ Days (starting at first login)）	ユーザーがネットワークまたはポータルに初めてログインした後に、定期的に AUP を表示します。

スポンサー ポータルのスポンサーのパスワード変更設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] > [スポンサーによるパスワード変更設定（Sponsor Change Password Settings）]**。これらの設定により、スポンサー ポータルを使用するスポンサーのパスワード要件が定義されます。

フィールド	使用上のガイドライン
スポンサーは自身のパスワードを変更可能（Allow sponsors to change their own passwords）	スポンサーは、スポンサー ポータルにログインした後、自身のパスワードを変更できます。このオプションは、スポンサーが内部ユーザー データベースの一部である場合にだけ、[パスワードの変更（Change Password）] ページを表示します。

スポンサー ポータルのポストログイン バナー設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータルまたはスポンサーポータル（Guest Portals or Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポストログインバナーページ設定（Post-Login Banner Page Settings）] です。**

これらの設定を使用して、正常なログイン後にユーザー（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

フィールド	使用上のガイドライン
ポストログインバナーページを含める（Include a Post-Login Banner page）	ユーザーが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

スポンサー ポータルのサポート情報ページの設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [サポート情報ページの設定（Support Information Page Settings）] です。**

これらの設定を使用して、ヘルプデスクがユーザー（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

フィールド	使用上のガイドライン
サポート情報ページを含める（**Include a Support Information Page**）	該当ポータルのすべての有効なページ上で、[問い合わせ先（Contact Us）] などの情報へのリンクを表示します。
MAC アドレス（MAC Address）	[サポート情報（Support Information）] ウィンドウにデバイスの MAC アドレスを含めます。
IP アドレス（IP Address）	[サポート情報（Support Information）] ウィンドウにデバイスの IP アドレスを含めます。
ブラウザのユーザーエージェント（**Browser User Agent**）	[サポート情報（Support Information）] ページに、要求の発信元の製品名とバージョン、レイアウトエンジン、ユーザーエージェントのバージョンなど、ブラウザの詳細を含めます。
ポリシーサーバー（**Policy Server**）	[サポート情報（Support Information）] ウィンドウに、このポータルを提供している ISE ポリシーサービスノード（PSN）の IP アドレスを含めます。
障害コード（**Failure code**）	可能な場合は、ログメッセージカタログ内の対応する番号を含めます。メッセージカタログを表示するには、**[管理（Administration）]**> **[システム（System）]** > **[ロギング（Logging）]**> **[メッセージカタログ（Message Catalog）]** を選択します。
フィールドを非表示にする（**Hide Field**）	含める情報が存在しない場合、[サポート情報（Support Information）] ウィンドウ上の該当するフィールドのラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード（Failure Code）] は、選択されている場合でも表示されません。
値のないラベルを表示（**Display label with no value**）	含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを [サポート情報（Support Information）] ウィンドウに表示します。たとえば、障害コードが不明な場合、[障害コード（Failure Code）] は空白であっても表示されます。

フィールド	使用上のガイドライン
デフォルト値でラベルを表示（Display Label with Default Value）	含める情報が存在しない場合、[サポート情報（Support Information）] ウィンドウ上の選択されているすべてのフィールドにこのテキストが表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード（Failure code）] に [使用できません（Not Available）] と表示されます。

スポンサー ポータルのゲストへの通知のカスタマイズ

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > 作成、編集または複製（Create, Edit or Duplicate）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [ゲストへの通知（Notify Guests）]** です。

[ページのカスタマイズ（Page Customizations）] で、スポンサーがスポンサー ポータルからゲストに送信する通知に表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

[設定（Settings）] では、スポンサーが電子メールまたは SMS を使用してゲストにユーザー名とパスワードを個別に送信できるかどうかを指定できます。また、ヘルプデスクがアクセスの問題をトラブルシューティングするために使用できる情報を提供するために、スポンサーがゲストに [サポート情報（Support Information）] ページを表示できるかどうかを指定できます。

スポンサー ポータルのカスタマイズの管理と承認

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [管理と承認（Manage and Approve）]** です。

[ページのカスタマイズ（Page Customizations）] で、スポンサー ポータルの [管理と承認（Manage and Approve）] タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

これらには、アカウント（登録済みおよび保留）の概要および詳細ビュー、スポンサーがゲストアカウントに対して実行する編集、拡張、一時停止などの操作に基づいて表示されるポップアップ ダイアログ、さらに汎用ポータルやアカウント アクション メッセージが含まれています。

ゲストおよびスポンサー ポータルのグローバル設定

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ゲストアクセス（Guest Access）] > [設定（Settings）]** を選択します。Cisco ISE 内のゲスト ポータル、スポンサー ポータル、ゲスト タイプ、およびスポンサー グループに適用される、次の一般設定を設定できます。

- ゲスト アカウントの消去、およびユーザー名とパスワードの生成のポリシー。
- 電子メールおよび SMS 通知をゲスト アカウントとスポンサーに送信するときに使用する SMTP サーバーおよび SMS ゲートウェイ。
- アカウント登録ゲスト ポータルを使用したゲスト アカウントの作成およびゲストの登録時に選択する場所、タイム ゾーン、SSID およびカスタム フィールド。

これらのグローバル設定を指定したら、特定の [ゲスト（Guest）] ポータルと [スポンサー（Sponsor）] ポータル、ゲストタイプおよびスポンサーグループの設定時にそれらを必要に応じて使用できます。

[ポータル設定（Portal settings）] ページには、次のタブがあります。

- [ゲストアカウントの消去ポリシー（Guest Account Purge Policy）]：期限が切れたゲストアカウントを消去する時期をスケジューリングします。詳細については、期限切れのゲストアカウントを消去するスケジューリング設定 （823 ページ）を参照してください。
- [カスタムフィールド（Custom Fields）]：ユーザーから追加情報を取得するためにゲストポータルで使用するカスタムフィールドを追加します。詳細については、ゲストアカウント作成用のカスタム フィールドの追加 （824 ページ）を参照してください。
- [ゲスト電子メールの設定（Guest Email Settings）]：アカウントの変更をゲストに電子メール通知するかどうかを決定します。詳細については、電子メールでの通知用の電子メールアドレスおよび SMTP サーバーの指定 （825 ページ）を参照してください。
- [ゲストのロケーションと SSID（Guest Locations and SSIDs）]：ロケーションと、ゲストがそのロケーションで使用できるネットワークのサービス セット識別子（SSID）を設定します。詳細については、ゲストのロケーションおよび SSID の割り当て （826 ページ）を参照してください。
- [ゲストユーザー名ポリシー（Guest Username Policy）]：ゲストユーザー名の作成方法を設定します。詳細については、ゲストユーザー名ポリシーの設定 （829 ページ）およびゲスト パスワード ポリシーのルール （827 ページ）を参照してください。
- [ゲストパスワードポリシー（Guest Password Policy）]：すべての [ゲスト（Guest）] ポータルと [スポンサー（Sponsor）] ポータルのゲストパスワードポリシーを定義します。詳細については、ゲスト パスワード ポリシーと有効期限の設定 （828 ページ）を参照してください。
- [ロギング（Logging）]：ゲストユーザーは、デバイスの MAC アドレスで追跡されます。ゲスト ユーザーがレポートに表示される場合、ユーザー名は MAC アドレスです。このオ

プションを選択すると、ユーザー名として MAC アドレスではなく、ポータル ユーザー ID がレポートに表示されます。このオプションの詳細については、ゲスト ユーザー情報を保存 （859 ページ）を参照してください。

ゲスト タイプの設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストタイプ（Guest Types）]** です。これらの設定を使用して、ネットワークにアクセスできるゲストのタイプおよびそのアクセス権限を作成します。また、このタイプのゲストを作成できるスポンサー グループを指定できます。

- **[ゲストタイプ名（Guest type name）]**：このゲストタイプを他のゲストタイプと区別する名前（1 ～ 256 文字）を指定します。
- **[説明（Description）]**：このゲストタイプの推奨される使用方法に関する追加情報（最大 2000 文字）を指定します。たとえば、アカウント登録ゲスト用です。
- **[言語ファイル（Language File）]**：このフィールドでは、サポート対象のすべての言語で、電子メールの件名、電子メールメッセージ、およびSMS メッセージの内容を含む言語ファイルをエクスポートおよびインポートできます。これらの言語とコンテンツは、アカウントが期限切れになった旨の通知に使用され、このゲストタイプに割り当てられているゲストに送信されます。新しいゲスト タイプを作成すると、ゲスト タイプを保存するまではこの機能は無効です。言語ファイルの編集の詳細については、ポータル言語のカスタマイズ （960 ページ） を参照してください。
- **[追加データを収集（Collect Additional Data）]**：[カスタムフィールド（Custom Fields）] オプションをクリックして、このゲストタイプを使用しているゲストから追加データを収集するために使用するカスタムフィールドを選択します。

  カスタム フィールドを管理するには、**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[設定（Settings）]** > **[カスタムフィールド（Custom Fields）]** を選択します。
- **最大アクセス時間**
  - **[アカウント有効期間の開始（Account duration starts）]**：[最初のログインから（From first login）] を選択した場合、アカウントの開始時間は、ゲストユーザーがゲストポータルに最初にログインしたときに開始され、終了時間は指定された期間に相当します。ゲスト ユーザーがログインしなければ、アカウントがゲスト アカウント消去ポリシーによって削除されるまで、アカウントは `Awaiting first login` 状態のままになります。

    値は、1 から 999 日、時間、または分です。

    アカウント登録ユーザーのアカウントは、ユーザーがアカウントを作成し、自分のアカウントにログオンしたときに開始されます。

[スポンサーが指定した日付から（From sponsor-specified date）] を選択した場合は、このゲスト タイプのゲストがネットワークにアクセスして接続を保持できる最大日数、時間数、または分数を入力します。

この設定を変更した場合、変更内容はこのゲストタイプを使用して作成された既存のゲスト アカウントには適用されません。

- **[最大アカウント有効期間（Maximum account duration）]**：このゲストタイプが割り当てられているゲストがログインできる期間（日数、時間数、または分数）を入力します。

（注） アカウント消去ポリシーにより期限切れのゲストアカウントが確認され、期限切れ通知が送信されます。このポリシーは 20 分ごとに実行されるため、アカウント期間を 20 分未満に設定すると、アカウントの消去前に期限切れ通知が送信されることがあります。

[アクセスを許可する日付と時刻（Allow access only on these days and times）] オプションを使用して、このゲストタイプのゲストにアクセスを提供する期間や曜日を指定できます。

- 選択した曜日によって、スポンサーのカレンダーで選択できる日付へのアクセスが制限されます。
- スポンサーが期間と日付を選択すると、スポンサー ポータルで最大アカウント期間が適用されます。

ここで設定するアクセス時刻の設定は、ゲスト アカウントの作成時にスポンサー ポータルで使用できる時刻設定に影響します。詳細については、スポンサーに対して使用可能な時間設定項目の設定 （873 ページ）を参照してください。

- **ログイン オプション**
  - **[最大同時ログイン数（Maximum simultaneous logins）]**：このゲストタイプに割り当てられたユーザーが同時に実行できる最大ユーザーセッション数を入力します。
  - **[ゲストが制限を超えた場合（When guest exceeds limit）]**：[最大同時ログイン数（Maximum simultaneous logins）] を選択した場合は、その最大ログイン数に到達した後でユーザーが接続したときに実行するアクションも選択する必要があります。
    - **最も古い接続を切断（Disconnect the oldest connection）**
    - **[最も新しい接続を切断（Disconnect the newest connection）]**：[エラーメッセージを示すポータルページにユーザーをリダイレクトする（Redirect user to a portal page showing an error message）] を選択する場合、特定の時間にわたってエラーメッセージが表示され、その後セッションが切断されてユーザーがゲストポータルにリダイレクトされます。エラーメッセージが表示される時間は設定可能です。エラーページの内容は、**[メッセージ（Messages）]** > **[エラーメッセージ（Error**

Messages）] ウィンドウの [ポータルページのカスタマイズ（Portal Page Customization）] ダイアログで設定します。

- **[ゲストが登録できるデバイスの最大数（Maximum devices guests can register）]**：各ゲストに登録できるデバイスの最大数を入力します。そのゲストタイプのゲストに登録済みの値より小さい値を最大数として設定できます。この値は、新しく作成されたゲスト アカウントにのみ適用されます。新しいデバイスを追加し、最大数に達すると、最も古いデバイスが切断されます。
- **[ゲストデバイス登録のためのエンドポイントIDグループ（Endpoint identity group for guest device registration）]**：ゲストのデバイスに割り当てるエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。
- **[ゲストに対しゲストポータルのバイパスを許可する（Allow guest to bypass the Guest portal）]**：ログイン情報を持つゲストタイプのキャプティブポータル（Web 認証ページ）をバイパスし、有線およびワイヤレス（dot1x）サプリカントまたは VPN クライアントに認証情報を提供することでネットワークにアクセスすることをユーザーに許可します。ゲスト アカウントは、AUP が必要な場合でも、[初期ログインを待機（Awaiting Initial Login）] 状態と AUP ページをバイパスして [アクティブ（Active）] 状態になります。

  この設定を有効にしない場合、ユーザーは初めにクレデンシャルを持つゲストのキャプティブ ポータルを使用してログインしないと、ネットワークの他の部分にアクセスできません。

- アカウント有効期限通知
  - **[アカウント有効期限の __ 日前にアカウント有効期限通知を送信する（Send account expiration notification __ days before account expires）]**：アカウントが期限切れになる前にゲストに通知を送信します。有効期限前の日数、時間数、または分数を指定します。
  - **[メッセージ表示原語（View messages in）]**：電子メールまたは SMS 通知の表示言語を指定します。
  - **[電子メール（Email）]**：アカウント有効期限通知を電子メールで送信します。
  - **[次のポータルのカスタマイズを使用する（Use customization from）]**：選択したポータルに対して設定した同一のカスタマイズ内容をこのゲストタイプのアカウント有効期限メールに適用します。
  - **[テキストのコピー元（Copy text from）]**：別のゲストタイプのアカウント有効期限メールに、作成した電子メールテキストを再利用します。
  - **[SMS]**：アカウント有効期限通知を SMS で送信します。

    SMS の設定は、電子メール通知の設定と同一ですが、[テスト SMS の送信（Send test SMS to me）] の SMS ゲートウェイを選択する点が異なります。

- **[スポンサーグループ（Sponsor Groups）]**：このゲストタイプを使用してメンバーがゲストアカウントを作成できるスポンサーグループを指定します。このゲストタイプにアクセスできないようにするスポンサー グループは削除します。

スポンサー グループ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーグループ（Sponsor Groups）]** です。スポンサー グループにメンバーを追加したり、ゲスト タイプおよびロケーション特権を定義したり、ゲストアカウントの作成と管理に関連する権限を設定したりする場合に、これらの設定を使用します。

- [スポンサーグループの無効化（Disable Sponsor Group）]：このスポンサーグループのメンバーが [スポンサー（Sponsor）] ポータルにアクセスできないようにします。

  たとえば、管理者ポータルで設定を変更している間、スポンサーが一時的にスポンサーポータルにログインできないようにします。あるいは、再びアクティブ化する必要があるまで、年次会議のスポンサーシップ ゲストなど、頻繁には発生しないアクティビティに関するスポンサー グループを無効にします。

- [スポンサーグループ名（Sponsor group name）]：一意の名前を入力します（1 ～ 256 文字）。

- [説明（Description）]：このスポンサーグループで使用されるゲストタイプなどの有益な情報を入力します（最大 2000 文字）。

- [ゲストタイプの設定（Configure Guest Types）]：必要とするゲストタイプが使用可能でない場合は、**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストタイプ（Guest Types）]** をクリックし、新しいゲストタイプを作成するか、または既存のゲストタイプを編集します。

- **一致基準**

  - [メンバー（Members）]：[スポンサーグループメンバーの選択（Select Sponsor Group Members）] ボックスを表示する場合にクリックします。ここでは、使用可能なユーザー ID グループを（内部および外部の ID ストアから）選択し、このスポンサーグループのメンバーとして追加できます。

    - [スポンサーグループメンバー（Sponsor Group Members）]：選択したスポンサーグループのリストを検索およびフィルタリングし、含めないグループを削除します

  - [その他の条件（Other conditions）]：[新しい条件の作成（Create New Condition）] をクリックして、このスポンサーグループに含めるためにスポンサーが満たす必要がある条件を 1 つ以上構築します。Active Directory、LDAP、SAML、ODBC の ID ストアからの認証属性を使用できますが、RADIUS トークンまたは RSA SecurID ストアは使用

できません。内部ユーザー属性も使用できます。条件には、属性、演算子、値があります。

- ディクショナリ属性 *Name* を使用して条件を作成するには、ID グループ名の前にユーザー ID グループを付けます。次に例を示します。

  InternalUser:Name EQUALS bsmith

  この場合、「bsmith」という名前の内部ユーザーだけがこのスポンサー グループに所属できます。

- [このスポンサーグループはこれらのゲストタイプを使用してアカウントを作成可能（This sponsor group can create accounts using these guest types）]：このスポンサーグループのメンバーがゲストアカウントの作成時に使用できるゲストタイプを指定します。有効にするスポンサー グループには、使用できる少なくとも 1 つのゲスト タイプが設定されている必要があります。

  このスポンサーグループに1つのゲストタイプのみを割り当てる場合、それが使用可能な唯一の有効なゲストであるため、[スポンサー（Sponsor）]ポータルに表示しないことを選択できます。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Sponsor Portal）]** > **[ページのカスタマイズ（Page Customization）]** > **[アカウントの作成（Create Accounts）]** > **[ゲストタイプ（Guest Types）]** > **[設定（Settings）]** を選択します。このオプションを有効にするには、[スポンサーで 1 つのみ使用できる場合はゲスト タイプを非表示（Hide guest type if only one is available to sponsor）] をオンにします。

- [ゲストがアクセスするロケーションを選択（Select the locations that guests will be visiting）]：アカウントを作成中にゲストに割り当てることができるロケーションを選択します。これは、これらのゲストアカウントの有効なタイムゾーンを定義し、有効なアクセス時間などゲストに適用するすべての時間パラメータを指定する場合に役立ちます。これにより、ゲストが他のロケーションからネットワークに接続できなくなることはありません。

  有効にするスポンサー グループには、使用できる少なくとも1つのロケーションが設定されている必要があります。

  このスポンサー グループに1つのロケーションのみを割り当てると、それが、メンバーが作成するゲスト アカウントの唯一の有効な時間帯になります。デフォルトでは、スポンサー ポータルに表示されません。

スポンサーが作成可能（Sponsor Can Create）

- [特定のゲストに割り当てられた複数のゲストアカウント（インポート）（Multiple guest accounts assigned to specific guests (Import)）]：スポンサーがファイルから姓名などのゲストの詳細をインポートすることによって、複数のゲストアカウントを作成できるようにします。

  このオプションが有効になっている場合、[インポート（Import）] オプションが [スポンサー（Sponsor）] ポータルの [アカウントの作成（Create Accounts）] ページに表示されま

す。[インポート（Import）] オプションは、Internet Explorer、Firefox、Safari などのデスクトップブラウザのみで使用可能です（モバイルは不可）。

- [バッチ処理の制限（Limit to batch of）]：このスポンサーグループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲストアカウントの数を指定します。

  スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- [ゲストへの複数のゲストアカウントの割り当て（ランダム）（Multiple guest accounts to be assigned to any guests (Random)）]：スポンサーが、未知のゲストのプレースホルダとして、または複数のアカウントをすばやく作成する必要がある場合に複数のランダムゲストアカウントを作成できるようにします。

  このオプションが有効になっている場合、[ランダム（Random）] オプションが [スポンサー（Sponsor）] ポータルの [アカウントの作成（Create Accounts）] ページに表示されます。

- [デフォルトユーザー名プレフィックス（Default username prefix）]：スポンサーが複数のランダムなゲストアカウントを作成する場合に使用できるユーザー名プレフィックスを指定します。指定した場合、このプレフィックスはランダムなゲストアカウントを作成するときにスポンサー ポータルに表示されます。また、[スポンサーにユーザー名プレフィックスの指定を許可（Allow sponsor to specify a username prefix）] の設定により、次のようになります。

  - [有効（Enabled）]：スポンサーは、[スポンサー（Sponsor）] ポータルでデフォルトのプレフィックスを編集できます。
  - [無効（Not enabled）]：スポンサーは [スポンサー（Sponsor）] ポータルでデフォルトのプレフィックスを編集できません。

  ユーザー名プレフィックスを指定しないか、またはスポンサーにユーザー名プレフィックスの指定を許可しない場合、スポンサーはスポンサー ポータルでユーザー名プレフィックスを割り当てることができません。

- [スポンサーにユーザー名プレフィックスの指定を許可（Allow sponsor to specify a username prefix）]：このスポンサーグループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲストアカウントの数を指定します。

  スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- [開始日を__日後より遅くすることはできない（Start date can be no more than __ days into the future）]：スポンサーが作成されている複数のゲストアカウントの開始日をこの日数以内に設定する必要がある日数を指定します。

スポンサーが管理可能（Sponsor Can Manage）

- [スポンサーが作成したアカウントのみ（Only accounts sponsor has created）]：このグループのスポンサーは、スポンサーの電子メールアカウントに基づいて、スポンサーが作成したゲストアカウントのみを表示および管理できます。
- [このスポンサーグループのメンバーによって作成されたアカウント（Accounts created by members of this sponsor group）]：このグループのスポンサーは、このスポンサーグループ内のスポンサーが作成したゲストアカウントを表示および管理できます。
- [すべてのゲストアカウント（All guest accounts）]：スポンサーはすべての保留中のゲストアカウントを表示および管理できます。

（注） [アカウント登録ゲストからの要求の承認および表示（Approve and view requests from self-registering guests）] にマークを付けて、[スポンサーが可能（Sponsor Can）] の下で [このスポンサーに割り当てられた保留中のアカウントのみ（Only pending accounts assigned to this sponsor）] オプションを使用していない限り、グループ メンバーシップにかかわらず、すべてのスポンサーがすべての保留中のアカウントを表示できます。

スポンサーが可能（Sponsor Can）

- [ゲストの連絡先情報（電子メール、電話番号）の更新（Update guests' contact information (email, Phone Number)）]：スポンサーは、自分が管理できるゲストアカウントについて、ゲストの連絡先情報を変更できます
- [ゲストのパスワードの表示/印刷（View/print guests' passwords）]：このオプションをオンにすると、スポンサーはゲストのパスワードを印刷することができます。スポンサーは [アカウントの管理（Manage Accounts）] ウィンドウとゲストの詳細にゲストのパスワードを表示できます。これがオフの場合、スポンサーはパスワードを印刷できませんが、ユーザーは電子メールまたは SMS（設定済みの場合）を介してパスワードを取得できます。
- [ゲストのクレデンシャルを含む SMS 通知の送信（Send SMS notifications with guests' credentials）]：スポンサーは、自分が管理できるゲストアカウントについて、アカウントの詳細とログインクレデンシャルとともにゲストに SMS（テキスト）通知を送信できます。
- [ゲストアカウントのパスワードのリセット（Reset guest account passwords）]：スポンサーは、自分が管理できるゲストアカウントについて、そのパスワードを Cisco ISE によって生成されたランダムなパスワードにリセットできます。
- [ゲストのアカウントの延長（Extend guests' accounts）]：スポンサーは、自分が管理できるゲストアカウントについて、その有効期限を延長できます。スポンサーは、アカウントの有効期限に関してゲストに送信される電子メール通知に自動的にコピーされます。
- [ゲストのアカウントの削除（Delete guests' accounts）]：スポンサーは、自分が管理できるゲストアカウントについて、アカウントを削除し、ゲストが企業のネットワークにアクセスすることを防ぐことができます。

- [ゲストのアカウントの一時停止（Suspend guests' accounts）]：スポンサーは、自分が管理できるゲストアカウントについて、アカウントを一時停止してゲストが一時的にログインすることを防ぐことができます。

  また、このアクションは、許可変更（CoA）終了を発行して、一時停止されていたゲストをネットワークから排除できます。

  - [スポンサーに理由の入力を求める（Require sponsor to provide a reason）]：ゲストアカウントの一時停止に対する説明の入力をスポンサーに求めます。

- [アカウント登録ゲストからの要求の承認および表示（Approve and view requests from self-registering guests）]：このスポンサーグループに含まれているスポンサーは、（承認が必要な）アカウント登録ゲストからのすべての保留中のアカウント要求を表示するか、アクセス先の担当者としてユーザーがスポンサーの電子メールアドレスを入力した要求のみを表示できます。この機能では、アカウント登録ゲストによって使用されるポータルで[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）]にマークが付けられていて、スポンサーの電子メールが連絡先の担当者としてリストされている必要があります。この機能では、スポンサーのアイデンティティ送信元で**電子メール**属性が適切に設定されている必要もあります。

  - [保留中のすべてのアカウント（Any pending accounts）]：このグループに所属するスポンサーは、他のスポンサーによって作成されたアカウントを承認およびレビューします。

  - [このスポンサーに割り当てられている保留中のアカウントのみ（Only pending accounts assigned to this sponsor）]：このグループに所属するスポンサーは、スポンサー自身が作成したアカウントだけを表示および承認できます。

（注） **電子メール**属性は、**ユーザー情報属性**の一部です。**電子メール**属性の詳細については、次を参照してください。

- カスタム スキーマの設定 （1054 ページ）
- LDAP ID ソースの設定 （992 ページ） の [LDAP一般設定（LDAP General Settings）] テーブルの [スキーマ（Schema）] と [ユーザー情報（User Info）] 属性。
- SAML ID プロバイダーの設定 （1188 ページ） の手順 8。

- [プログラムによるインターフェイス（Guest REST API）を使用した Cisco ISE ゲストアカウントへのアクセス（Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)）]：スポンサーは、自分が管理できるゲストアカウントについて、Guest REST API プログラミングインターフェイスを使用してゲストアカウントにアクセスできます。

エンドユーザー ポータル

Cisco ISE では、Web ベースのポータルをエンドユーザーの 3 つのプライマリ セットに対して提供しています。

- ゲストポータル（ホットスポットとクレデンシャルを持つゲストポータル）を使用して企業ネットワークに一時的にアクセスする必要があるゲスト。
- スポンサー ポータルを使用してゲスト アカウントを作成および管理できるスポンサーとして指定されている従業員。
- 個人所有デバイスの持ち込み（BYOD）、モバイル デバイス管理（MDM）、デバイス ポータルなどのさまざまな非ゲスト ポータルを使用して、企業ネットワークでパーソナル デバイスを使用している従業員。

エンドユーザー Web ポータルのカスタマイズ

さらにポータルを編集、複製、作成できます。ポータルの外観を完全にカスタマイズし、その結果として、ポータルのエクスペリエンスをカスタマイズすることもできます。他のポータルへの影響なく、各ポータルを個別にカスタマイズできます。

ポータル全体またはポータルの特定のページに適用される、次のようなポータル インターフェイスのさまざまな側面をカスタマイズできます。

- テーマ、イメージ、色、バナー、およびフッター
- ポータル テキスト、エラー メッセージ、および通知の表示に使用される言語
- タイトル、コンテンツ、手順、およびフィールドとボタンのラベル
- 電子メール、SMS、およびプリンタでゲストに送信される通知（アカウント登録ゲスト ポータルとスポンサー ポータルにのみ該当）
- ユーザーに表示されるエラー メッセージと情報メッセージ
- アカウント登録ゲストポータルとスポンサーポータルの場合は、カスタムフィールドを作成して必要に応じた固有のゲスト情報を収集できます。

> ISE コミュニティ リソース
>
> Web ポータルのカスタマイズの詳細については、「ISE Portal Builder」および「HowTo: ISE Web Portal Customization Options」を参照してください。

カスタマイズ方法

エンドユーザーのポータルページをカスタマイズする方法は複数あり、それぞれ異なるレベルの知識が必要です。

- **基本**：ポータルの [カスタマイズ（Customization）] ページを変更できます。
  - バナーとロゴのアップロード
  - 一部の色の変更（ボタンを除く）
  - 画面のテキスト、およびポータル全体で使用される言語の変更
- **中間**
  - ミニエディタを使用した HTML および Javascript の追加。

（注） ミニエディタにHTMLを入力する前に、[HTML]アイコンをクリックします。

  - jQuery mobile theme roller を使用したすべてのページ要素の色の変更
- **詳細設定**
  - プロパティおよび CSS ファイルの手動による変更。

ポータルをカスタマイズした後、それを複製して（同じタイプの）複数のポータルを作成できます。たとえば、1つの業務エンティティのホットスポット ゲスト ポータルをカスタマイズした場合、それを複製し、少し変更して他の業務エンティティのカスタム ホットスポット ゲスト ポータルを作成することができます。

ミニ エディタを使用してポータルをカスタマイズするためのヒント

- ミニエディタのボックス内のワードが長いと、ポータルの画面領域のスクロールがオフになる場合があります。HTML 段落属性 style="word-wrap: break-word" を使用して改行します。次に例を示します。

```
<p style="word-wrap:break-word">

thisisaverylonglineoftextthatwillexceedthewidthoftheplacethatyouwanttoputitsousethisstructure

</p>
```

- HTML または javascript を使用してポータル ページをカスタマイズする場合は、必ず有効な構文を使用してください。Cisco ISE は、ミニエディタに入力したタグやコードを検証しません。無効な構文が原因でポータル フロー時に問題が発生する場合があります。

ポータル コンテンツのタイプ

Cisco ISE では、「そのまま」使用するか、または新しいカスタム ファイルを作成するためのモデルとして既存の CSS ファイルを使用することでカスタマイズできる、ポータル テーマの

デフォルト セットが提供されます。ただし、カスタマイズされた CSS ファイルを使用しないでポータルの外観を変更することもできます。

たとえば、独自の企業ロゴやバナーイメージを使用する場合は、単にこれらの新しいイメージファイルをアップロードして使用することができます。ポータルのさまざまな要素および領域の色を変更することによって、デフォルトのカラースキームをカスタマイズできます。カスタム変更時に、カスタム変更を表示する言語を選択することもできます。

ロゴおよびバナーを置き換えるための画像を設計するときは、画像のサイズを次のピクセルサイズに可能な限り近づけてください。

バナー	1724 X 133
デスクトップのロゴ	86 X 45
モバイルのロゴ	80 X 35

ISE はポータルに合わせて画像のサイズを変更しますが、画像が小さすぎるとサイズ変更後に正しく表示されない場合があります。

高度なカスタマイズ（ページ レイアウトの変更、ポータル ページへのビデオ クリップや広告の追加など）を行うには、独自のカスタム CSS ファイルを使用できます。

特定のポータルでのこのようなタイプの変更は、そのポータルのすべてのページにグローバルに適用されます。ページ レイアウトの変更は、ポータル内にグローバルに、または特定の 1 ページのみに適用することができます。

ポータル ページのタイトル、コンテンツ、およびラベル

エンドユーザー Web ポータル ページでゲストに表示されるタイトル、テキスト ボックス、手順、フィールドとボタンのラベル、その他の視覚要素をカスタマイズすることができます。ページをカスタマイズするときには、ページ設定を動的に編集することができます。

これらの変更は、カスタマイズしている特定のページにのみ適用されます。

ポータルの基本的なカスタマイズ

ニーズに最適な事前定義済みテーマを選択し、デフォルト設定のほとんどを使用します。その後、次のような基本的なカスタマイズが可能です。

- ポータルのテーマ カラーの変更 （931 ページ）
- ポータルのアイコン、イメージ、およびロゴの変更 （932 ページ）
- ポータルのバナーおよびフッター要素の更新 （933 ページ）
- ポータルの表示言語の変更 （932 ページ）
- タイトル、手順、ボタン、およびラベル テキストの変更 （934 ページ）
- テキスト ボックスの内容のフォーマットおよびスタイル （934 ページ）

ヒント　更新するときに、カスタマイズの参照 （940 ページ）を行うことができます。

ポータルのテーマ カラーの変更

デフォルト ポータル テーマのデフォルト カラー スキームをカスタマイズして、ポータルのさまざまな要素と領域の色を変更できます。これらの変更は、カスタマイズしているポータル全体に適用されます。

ポータルの色を変更する場合は、次のことに注意してください。

- このオプションを使用して、このポータルで使用するためにインポートしたカスタム ポータル テーマのカラー スキームを変更することはできません。その色の設定を変更するには、カスタム テーマ CSS ファイルを編集する必要があります。
- ポータルのテーマ カラーを変更した後で、[ポータル テーマ（Portal Theme）] ドロップダウン メニューから別のポータルのテーマを選択した場合、元のポータル テーマの変更は失われ、デフォルト カラーに戻ります。
- 変更済みのカラー スキームを使用してポータルのテーマ カラーを調整し、保存する前に色をリセットした場合、カラー スキームはデフォルト カラーに戻り、前の変更はすべて失われます。

ステップ 1　次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[設定（Configure）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2　[ポータル テーマ（Portal Theme）] ドロップダウン リストからデフォルト テーマの 1 つを選択します。

ステップ 3　[調整（Tweaks）] をクリックして、選択したデフォルト ポータル テーマの色の設定の一部を上書きします。

a) バナーとページ背景、テキスト、およびラベルの色の設定を変更します。
b) テーマのデフォルト カラー スキームに戻す場合は、[色のリセット（Reset Colors）] をクリックします。
c) [プレビュー（Preview）] で色の変更を確認する場合は、[OK] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

ポータルの表示言語の変更

カスタム変更を加えるときに、変更内容を表示する言語を選択できます。この変更は、カスタマイズしているポータル全体に適用されます。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[グローバルなカスタマイズ（Global Customization）]** を選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Sponsor Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[グローバルなカスタマイズ（Global Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > （任意のポータル） > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[グローバルなカスタマイズ（Global Customization）]** の順に選択します。

ステップ 2 [表示（View In）] ドロップダウン リストから、ページをカスタマイズするときにテキストを表示する言語を選択します。

ドロップダウン リストには、特定のポータルに関連付けられた言語ファイルにあるすべての言語が含まれています。

次のタスク

ポータルページをカスタマイズするときに選択した言語に加えた変更が、サポート対象のすべての言語プロパティ ファイルで更新されていることを確認します。

ポータルのアイコン、イメージ、およびロゴの変更

独自の企業ロゴ、アイコン、およびバナー イメージを使用する場合は、カスタム イメージをアップロードするだけで既存のイメージを置き換えることができます。サポートされている画像形式は、.gif、.jpg、.jpeg、.png です。これらの変更は、カスタマイズしているポータル全体に適用されます。

始める前に

ポータルのフッター（たとえば、アドバタイズメント）にイメージを含めるには、そのイメージがある外部サーバーにアクセスできる必要があります。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]**>**[ゲストアクセス（Guest Access）]**>**[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[設定（Configure）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]**>**[デバイスポータル管理（Device Portal Management）]**>（任意のポータル）> **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [イメージ（Images）] で、ロゴ、アイコン、イメージのボタンをクリックし、カスタム イメージをアップロードします。

ステップ 3 [保存（Save）] をクリックします。

ポータルのバナーおよびフッター要素の更新

ポータルの各ページのバナーおよびフッターセクションに表示される情報をカスタマイズできます。これらの変更は、カスタマイズしているポータル全体に適用されます。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]**>**[ゲストアクセス（Guest Access）]**>**[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]**>**[デバイスポータル管理（Device Portal Management）]**>（任意のポータル）> **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 各ポータル ページに表示される [バナー タイトル（Banner title）] を変更します。

ステップ 3 ポータルを使用するゲスト用に次のリンクを含めます。

- [ヘルプ（Help）]：オンライン ヘルプ（スポンサーおよびデバイス ポータルにのみ提供します）。
- [連絡先（Contact）]：テクニカルサポート（このことができるようにするには、[サポート情報（Support Information）] ページを設定します）。

ステップ 4 各ポータル ページの下部に表示される [フッター要素（Footer Elements）] に利用規約または著作権表示を追加します。

ステップ 5 [保存（Save）] をクリックします。

タイトル、手順、ボタン、およびラベル テキストの変更

ポータルに表示されるすべてのテキストを更新できます。カスタマイズするページの各 UI 要素に、入力できる文字数の最小範囲および最大範囲があります。テキストブロックの一部が使用可能な場合、ミニエディタを使用して表示スタイルをテキストに適用できます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。これらのページ要素は、電子メール、SMS、印刷通知ごとに異なります。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[設定（Configure）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** >（任意のポータル）> **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [ページ（Pages）] で、変更するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、表示された UI 要素を更新します。すべてのページに [ブラウザ ページ タイトル（Browser Page Title）]、[コンテンツ タイトル（Content Title）]、[説明テキスト（Instructional Text）]、[コンテンツ（Content）]、および 2 つの [任意のコンテンツ（Optional Content）] の各テキスト ブロックが含まれています。[コンテンツ（Content）] 領域のフィールドはすべてのページに固有です。

テキスト ボックスの内容のフォーマットおよびスタイル

テキストの基本的な書式設定を行うには、[説明テキスト（Instructional Text）]、[オプションの内容 1（Optional Content 1）]、および [オプションの内容 2（Optional Content 2）] テキスト ボッ

クスにあるミニエディタを使用します。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え（Toggle Full Screen）] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [ページ（Pages）] で、変更するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] の、[説明テキスト（Instructional Text）] および [オプションの内容（Optional Content）] テキスト ボックスで、次の操作を実行できます。

- テキストのフォント、色、サイズを変更します。
- テキストに太字、イタリック体、下線のスタイルを設定します。
- 箇条書きおよび番号付きリストを作成します。

（注） ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え（Toggle HTML Source）] ボタンを使用できます。[HTML ソース（HTML Source）] ビューでテキストを編集する場合は、[ポータルページのカスタマイズ（Portal Page Customization）] ウィンドウで変更を保存する前に、[HTML ソースの切り替え（Toggle HTML Source）] ボタンをもう一度クリックします。

ポータル ページのカスタマイズ用の変数

これらのポータル ページ テキスト ボックスへのナビゲーション パス:

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** の順に選択します。

- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]**>**[ゲストアクセス（Guest Access）]**>**[ポータルとコンポーネント（Portals & Components）]**>**[スポンサーポータル（Guest Portals）]**>**[編集（Edit）]**>**[ポータルページのカスタマイズ（Portal Page Customization）]**>**[ページ（Pages）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]**>**[デバイスポータル管理（Device Portal Management）]**>**（任意のポータル）**>**[編集（Edit）]**>**[ポータルページのカスタマイズ（Portal Page Customization）]**>**[ページ（Pages）]** の順に選択します。

ポータルユーザー（ゲスト、スポンサーおよび従業員）に表示される情報の一貫性を維持するために、ポータルコンテンツおよびゲスト通知用のテンプレートを作成するときにこれらの変数を使用します。[説明テキスト（Instructional Text）]、[オプション コンテンツ 1（Optional Content 1）]、および [オプション コンテンツ 2（Optional Content 2）] テキスト ボックスで、各ポータルのテキストを次に示す変数名と置き換えます。

表 *52*：ゲスト ポータルの変数のリスト

表示名	変数名による代替
アクセスコード（Access code） 電子メール、テキストまたは印刷物の通知を使用して、ゲストにアクセスコードを提供するために使用します。	ui_access_code
BYOD IOS SSID デュアルSSIDフローに入った後にデバイスが接続する必要があるネットワークを指定するために使用します。	ui_byod_success_ios_ssid
クライアントプロビジョニングエージェントのタイプ（Client Provisioning Agent Type） クライアントプロビジョニングポリシーに現在設定されているエージェントを指定するために使用します。	ui_client_provision_agent_type
クライアントプロビジョニングエージェントの URL（Client Provisioning Agent URL） ポスチャエージェントのダウンロードURLを指定するために使用します。	ui_client_provision_agent_url

表示名	変数名による代替
クライアントプロビジョニングエージェントインストール分数（Client Provisioning agent install minutes） ゲストに、[クライアント プロビジョニング（Client Provisioning）] ウィンドウでインストール手順を完了する必要がある制限時間（修復タイマーにより設定）を通知するために使用します。タイマーが時間切れになる前にゲストがインストール手順を完了しなかった場合、ゲストはブラウザ ページをリフレッシュして、ログイン プロセスをやり直す必要があります。	ui_client_provision_install_agent_mins
会社（Company）	ui_company
電子メール アドレス（Email address）	ui_email_address
終了日時（End date and time）	ui_end_date_time
名（First name）	ui_first_name
姓（Last name）	ui_last_name
ロケーション名（Location name）	ui_location_name
最大登録デバイス数（Maximum registered devices）	ui_max_reg_devices
最大同時ログイン数（Maximum simultaneous logins）	ui_max_siml_login
パスワード（Password）	ui_password
訪問先担当者（電子メール）（Person being visited (email)）	ui_person_visited
電話番号（Phone number）	ui_phone_number
訪問の理由（Reason for visit）	ui_reason_visit
SMS プロバイダー（SMS Provider）	ui_sms_provider
SSID ゲストがネットワークに接続するために使用できるワイヤレス ネットワークを指定するために使用します。	ui_ssid

表示名	変数名による代替
開始日時（Start date and time）	ui_start_date_time
残り時間（Time left）	ui_time_left
ユーザー名（Username）	ui_user_name

表 *53 :* スポンサー ポータルの変数のリスト

表示名	変数名による代替
ゲスト - 会社（Guest - Company）	ui_guest_company
ゲスト - 電子メール アドレス（Guest - Email address）	ui_guest_email_address
ゲスト- 終了日時（Guest - End date and time）	ui_guest_end_date_time
ゲスト - 名（Guest - First name）	ui_guest_first_name
ゲスト - 姓（Guest - Last name）	ui_guest_last_name
ゲスト - ロケーション名（Guest - Location name）	ui_guest_location_name
ゲスト - 最大登録デバイス数（Guest - Maximum registered devices）	ui_guest_max_reg_devices
ゲスト - 最大同時ログイン数（Guest - Maximum simultaneous logins）	ui_guest_max_siml_login
ゲスト - パスワード（Guest - Password）	ui_guest_password
ゲスト - 訪問先担当者（電子メール）（Guest - Person being visited (email)）	ui_guest_person_visited
ゲスト - 電話番号（Guest - Phone number）	ui_guest_phone_number
ゲスト - 訪問の理由（Guest - Reason for visit）	ui_guest_reason_visit
ゲスト - SMS プロバイダー（Guest - SMS Provider）	ui_guest_sms_provider
ゲスト - SSID（Guest - SSID） ゲストがネットワークに接続するために使用できるワイヤレス ネットワークを指定するために使用します。	ui_guest_ssid
ゲスト - 開始日時（Guest - Start date and time）	ui_guest_start_date_time

表示名	変数名による代替
ゲスト - 残り時間（Guest - Time left）	ui_guest_time_left
ゲスト - ユーザー名（Guest - Username）	ui_guest_user_name
ユーザー名（Username） ポータルにログインしたユーザーのユーザー名を指定するために使用します。	ui_sponsor_user_name
[ゲストアクセス情報（Guest Access Information）] ウィンドウに [これ以降（From）] を表示するために使用します。	ui_from_label
[ゲストアクセス情報（Guest Access Information）] ウィンドウに [初回ログイン（First Login）] を表示するために使用します。	ui_first_login_text
初回ログイン時にアクセス時間が開始すると、ゲスト アカウントの通知メッセージを表示するために使用します。	ui_notification_first_login_text
電子メール通知のアカウントの有効期間を示す動的変数。	ui_access_duration
利用できなくなったアカウントを表示する動的変数。[開始/終了（Start-End）] アカウントでは日付は終了日で、[初回ログインから（From-First-Login）] アカウントでは日付はアカウントの作成日に消去期間日数を足したものです。	ui_account_purge_date
ゲスト ユーザーが少なくとも一度以前ログインしたことがある場合、スポンサーが、ゲストのタイプを [初回ログインから（From-First-Login）] から [開始/終了（Start-End）] に変更、または逆に変更することを制限するために使用します。一般的なスポンサー ポータル メッセージに表示されます。	ui_guest_type_change_ffl_startend_not_allowed_error ui_guest_type_change_ startend_ffl_not_allowed_error

表 *54 : MDM* ポータルの変数のリスト

表示名	変数名による代替
MDM - ベンダー名（MDM - Vendor Name）	ui_mdm_vendor_name

表 *55:* デバイス ポータルの変数のリスト

表示名	変数名による代替
デバイス - ログイン失敗の頻度制限（MyDevices - Login Failure Rate Limit）	$user_login_failure_rate_limit$
デバイス - 最大登録デバイス数（MyDevices - Max Devices to Register）	ui_max_register_devices
デバイス - ユーザー名（MyDevices - User Name） ポータルにログインしたユーザーのユーザー名を指定するために使用します。	$session_username$

カスタマイズの参照

カスタマイズがポータルユーザー（ゲスト、スポンサー、従業員）にどのように表示されるかを確認できます。

ステップ 1 [ポータルテストURL（Portal test URL）] をクリックして、変更を表示します。

ステップ 2 （オプション）変更がさまざまなデバイスでどのように表示されるかを動的に確認するには、[プレビュー（Preview）] をクリックします。

- モバイルデバイス：[プレビュー（Preview）] で変更を表示します。
- デスクトップデバイス：[プレビュー（Preview）] をクリックし、[デスクトッププレビュー（Desktop Preview）] をクリックします。

  変更が表示されない場合は、[プレビューのリフレッシュ（Refresh Preview）] をクリックします。表示されるポータルは、変更を確認するためだけのものです。ボタンをクリックしたり、データを入力したりすることはできません。

（注） テストポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

カスタム ポータル ファイル

カスタム ポータル ファイル メニューでは、ISE サーバーに独自のファイルをアップロードすることができ、（管理者ポータルを除く）ユーザーがアクセスできるすべてのポータルのカス

タマイズに使用できます。アップロードしたファイルは PSN に保存され、すべての PSN に同期されます。

サポートされるファイル タイプは次のとおりです。

- .png、.gif、.jpg、.jpeg、ico：背景、お知らせ、および広告用
- .htm、.html、.js、.json、.css、.m4a、.m4v、.mp3、.mp4、.mpeg、.ogg、.wav：高度なカスタマイズ用（ポータルビルダーなど）

ファイルのサイズは限定されます。

- ファイルあたり 20 MB
- すべてのファイルの合計が 200 MB

ファイルのリストのパス列には、このサーバー上のファイルのURLが表示されます。このURLは、ミニエディタ外部でそのファイルを参照する場合に使用できます。イメージファイルの場合、リンクをクリックすると、新しいウィンドウが開き、イメージが表示されます。

アップロードされたファイルは、[ポータルページのカスタマイズ（Portal Page Customization）]の下にあるミニエディタで、管理者用ポータルを除くすべてのポータルタイプにより参照できます。ミニエディタにファイルを挿入するには、ツールバーの [ファイルを挿入（insert file）]ボタンをクリックします。[HTML ソース（HTML Source）] ビューに切り替えます。挿入されたファイルが適切な HTML タグで囲まれていることがわかります。

テストのために、表示可能なアップロードファイルをISEの外部からブラウザで表示することもできます。URL は https://*ise_ip*:8443/portal/customFiles/*filename* です。

ポータルの高度なカスタマイズ

Cisco ISE から提供されるデフォルトのポータル テーマの 1 つを使用しない場合、ニーズに合わせてポータルをカスタマイズできます。そのためには、CSS および Javascript ファイルと jQuery Mobile ThemeRoller アプリケーションの使用経験が必要です。

デフォルトのポータル テーマを変更することはできませんが、次の操作を実行できます。

- ポータルのデフォルト テーマ CSS ファイルのエクスポート（946 ページ）、カスタムポータルテーマを作成する基本として使用できます。
- カスタム ポータル テーマ CSS ファイルの作成（947 ページ）、デフォルトのポータルテーマを編集し、新規ファイルとして保存することによって可能になります。
- カスタム ポータル テーマ CSS ファイルのインポート（958 ページ）、ポータルに適用できます。

専門知識と要件に基づいて、さまざまなタイプの高度なカスタマイズを実行できます。事前定義済み変数を使用して、表示される情報の整合性の実現、ポータルページへのアドバタイズメントの追加、HTML、CSS、およびJavascriptコードを使用した内容のカスタマイズ、ポータルページのレイアウト変更が可能になります。

ポータルを変更するには、各ポータルの [ポータルページのカスタマイズ（Portal Page Customization）] タブのコンテンツボックスに HTML、CSS、および Javascript を追加します。このドキュメントでは、HTML と CSS を使用したカスタマイズの例について説明します。Javascript を使用した例は、ISE コミュニティ（http://cs.co/ise-community）で紹介されています。さらに多くの HTML、CSS、および Javascript の例については、ISE コミュニティ https://community.cisco.com/t5/security-documents/how-to-ise-web-portal-customization-options/ta-p/3619042 を参照してください。

（注） TAC では、Javascript での Cisco ISE ポータルのカスタマイズをサポートしていません。Javascript でのカスタマイズに関する問題が発生した場合は、ISE コミュニティ https://community.cisco.com/t5/identity-services-engine-ise/bd-p/5301j-disc-ise に質問を投稿してください。

ポータル テーマと構造 CSS ファイル

CSS ファイルの使用に関する経験がある場合、デフォルトのポータル テーマ CSS ファイルをカスタマイズして、ポータル プレゼンテーションを変更し、ページ レイアウト、色、フォントなどの要素を操作できます。CSS ファイルをカスタマイズすると、プレゼンテーションの特性の指定における柔軟性と制御が向上し、複数のページでフォーマットを共有することが可能になり、構造化されたコンテンツの複雑さと繰り返しが削減されます。

Cisco ISE エンドユーザー ポータルは、種類が異なる 2 つの CSS ファイル（structure.css および *theme*.css）を使用します。ポータルテーマごとに独自の *theme*.css ファイルがありますが、ポータル タイプにつき structure.css ファイルは 1 つのみです（例：ゲスト ポータルの場合は guest.structure.css、スポンサー ポータルの場合は sponsor.structure.css、デバイス ポータルの場合は mydevices.structure.css）。

structure.css では、ページ レイアウトと構造のスタイルを指定しています。これには各ページの要素の位置が定義され、jQuery Mobile 構造のスタイルも含まれています。structure.css ファイルは表示のみ可能で、編集することはできません。ただし、*theme*.css ファイル内のページ レイアウトを変更し、これらのファイルをポータルにインポートして適用すると、最新の変更が structure.css のスタイルよりも優先されます。

theme.css ファイルは、フォント、ボタンの色、ヘッダーの背景などのスタイルを指定します。*theme*.css ファイルをエクスポートし、テーマ設定を変更してインポートし、ポータルのカスタム テーマとして使用できます。*theme*.css ファイルに対するページ レイアウト スタイルの変更は、structure.css ファイルで定義されるスタイルよりも優先されます。

シスコが提供するデフォルトのポータル *theme*.css ファイルは変更できません。ただし、ファイル内の設定を編集して、新しいカスタム *theme*.css ファイルに保存できます。カスタム *theme*.css ファイルをさらに編集することはできますが、Cisco ISE に再度インポートする場合は、最初に使用されていたのと同じテーマ名にしてください。同じ *theme*.css ファイルに 2 つの異なるテーマ名を使用することはできません。

たとえば、デフォルトの *green theme.css* ファイルを使用して新しいカスタム *blue theme.css* ファイルを作成し、*Blue* と名付けることができます。その後、*blue theme.css* ファイルを編集できま

すが、これを再度インポートする場合は、同じテーマ名の *Blue* を再利用する必要があります。Cisco ISE はファイル名やその名前とテーマ名の一意性の関係を確認するため、そのファイルを *Red* という名前にすることはできません。ただし、*blue theme.css* ファイルを編集し、*red theme.css* として保存し、新規ファイルをインポートして *Red* と名付けることは可能です。

jQuery Mobile によるテーマカラーの変更

シスコのエンドユーザー ポータルのカラー スキームは、jQuery ThemeRoller と互換性があります。ThemeRoller Web サイトを使用して、ポータル全体の色を簡単に編集できます。

ThemeRoller の色の「見本」には独自のカラースキームがあります。それらのスキームによって、主要 UI 要素（ツールバー、コンテンツブロック、ボタン、リスト項目、フォントのテキストシャドウなど）の色、テクスチャ、フォントの設定が定義されます。さらに、ボタンのさまざまな操作状態（通常時、マウスオーバー時、押された時）の設定も定義されます。

シスコでは、次の 3 つの見本が使用されます。

- スイッチ A：デフォルトのスイッチ。
- スイッチ B：強調する要素を定義します（例：[承認（Accept）] ボタンなど）。
- スイッチ C：重要な要素を定義します（例：アラート、エラー メッセージ、無効な入力フィールド、削除ボタンなど）。

スイッチを新たに追加して適用する場合は、そのスイッチを使用する要素を含む HTML コードを（オプション コンテンツなどに）追加しない限り、追加したスイッチを適用できません。

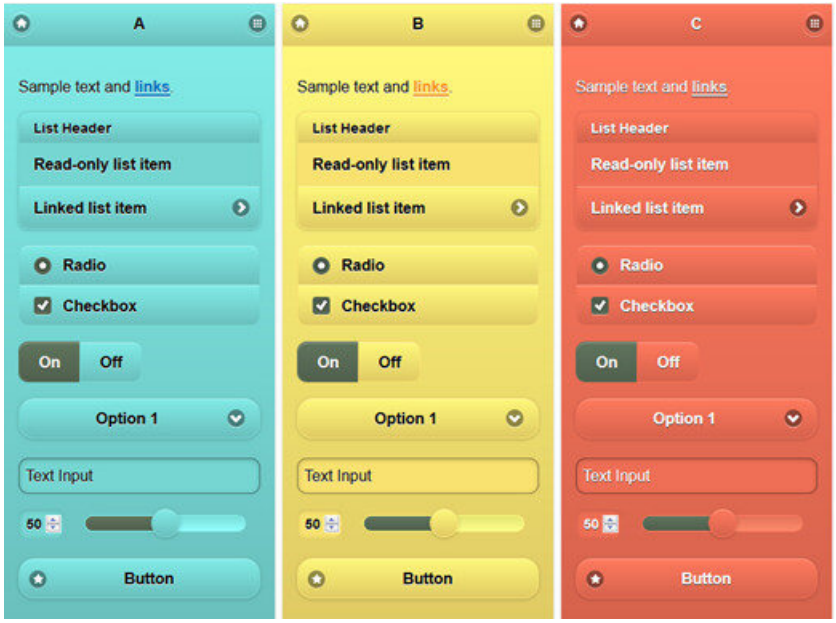
シスコ提供のデフォルトの CSS ファイルを編集するか、またはデフォルトのテーマに定義されている CSS クラスおよび構造に基づいて新しいファイルを作成するには、jQuery Mobile ThemeRoller（リリース 1.3.2）の必要なバージョンを使用してください。

jQuery Mobile ThemeRoller のスウォッチおよびテーマの詳細情報については、『Creating a Custom Theme with ThemeRoller』の「Theming Overview」を参照してください。jQuery Mobile ThemeRoller のオンライン ヘルプを使用して、カスタム テーマをダウンロード、インポート、および共有する方法を学習します。

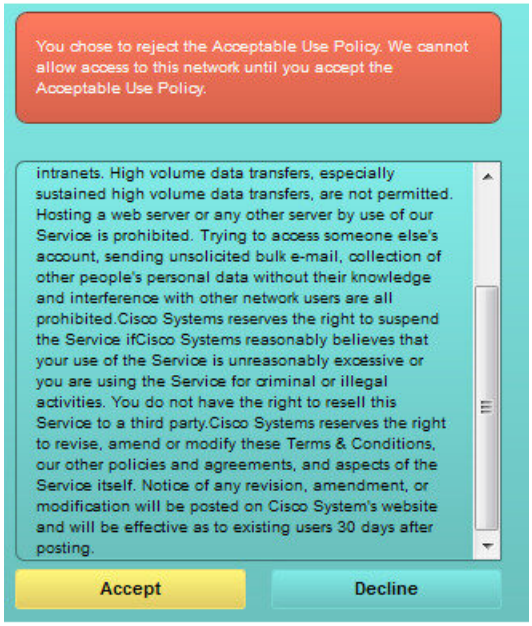
HTML、CSS、および Javascript コードを使用して、ポータルページに表示されるテキストおよびコンテンツをカスタマイズする方法のチュートリアルについては、Codecademy にアクセスしてください。

シスコの見本を示すテーマの例

見本がどのように使用されるかを示すために、ゲスト ポータルのデフォルト テーマが色の違いを示すように ThemeRoller で編集されました。



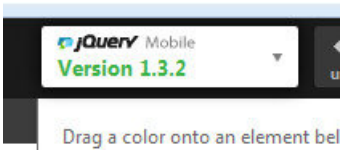
次の画面は、ユーザー（見本B）からのアクションを取るボタンとともにゲストポータルのログイン エラー（見本 C）を示し、画面の残りは見本 A です。



jQuery Mobile によるテーマ カラーの変更

始める前に

jQuery Mobile ThemeRoller のバージョン 1.3.2 を使用していることを確認します。ご使用のバージョンが次のように画面の左上隅に表示されます。



ステップ 1 ポータルで [構成（Configuration）] タブをクリックして、ポータルから変更する既存のテーマをエクスポートします。

ステップ 2 **[高度なカスタマイズ（Advanced Customization）] > [テーマのエクスポート/インポート（Export/Import Themes）]** を選択します。

ステップ 3 [カスタムテーマ（Custom Theming）] ダイアログで、更新するテーマをエクスポートします。

ステップ 4 テキスト エディタでそのテーマを開き、すべてを選択してコピーします。

ステップ 5 jQuery Web サイトの [テーマのインポート（Import Theme）] フィールドにテキスト（CSS）を貼り付けます。

ステップ 6 jQuery Mobil Web ベースのアプリケーションで変更を行います。

ステップ 7 jQuery Web サイトから更新されたテーマをエクスポートします（エクスポート形式は zip）。

ステップ 8 更新されたテーマを解凍し、テーマ フォルダ内の更新されたテーマを PC に展開します。テーマの名前は、jQuery Web サイトで指定した名前です。

ステップ 9 ポータル構成ページの [カスタムテーマ（Custom Theming）] ダイアログで、展開した CSS テーマファイルをポータルにインポートします。

[ポータル構成（Portal Configuration）] ウィンドウの [ポータルテーマ（Portal Theme）] ドロップダウンをクリックすることで、古いテーマと新しいテーマを切替えることができます。

ロケーションに基づくカスタマイズ

ゲスト アカウントが作成されるときに、それらをロケーションに関連付けて Service Set Identifier（SSID）属性を指定することできます。ロケーションと SSID のどちらも、CSS クラスとして使用することができます。これを使用すると、ゲストのロケーションと SSID に基づいて、それぞれ異なる CSS スタイルをポータル ページに適用できます。

次に例を示します。

- ゲスト ロケーション：ロケーションとして *San Jose* または *Boston* を持つアカウント付きゲストがクレデンシャルを持つゲスト ポータルにログインした場合、**guest-location-san-jose** または **guest-location-boston** のいずれかのクラスをすべてのポータル ページで使用できます。
- ゲスト SSID：*Coffee Shop Wireless* という名前の SSID の場合、すべてのポータル ページで **guest-ssid-coffee-shop-wireless** という CSS クラスを使用できます。この SSID は、ゲスト アカウントに指定した SSID であり、ログイン時にゲストが接続した SSID ではありません。

（注） この情報は、クレデンシャルを持つゲスト ポータルにのみ、ゲストがログインした後に適用されます。

スイッチやワイヤレス LAN コントローラ（WLC）などのデバイスをネットワークに追加するときに、ロケーションも指定できます。このロケーションも CSS クラスとして使用することができ、これを使用すると、ネットワーク デバイスのロケーションに応じて、それぞれ異なる CSS スタイルをポータル ページに適用できます。

たとえば、WLC が *Seattle* に割り当てられ、ゲストが Seattle-WLC から Cisco ISE にリダイレクトされた場合、すべてのポータル ページで **device-location-my-locations-usa-seattle** という CSS クラスを使用できます。

関連トピック

ゲスト ロケーションに基づいたグリーティングのカスタマイズ （954 ページ）

ユーザー デバイス タイプに基づくカスタマイズ

Cisco ISE は、クライアント デバイスのタイプ（ゲスト、スポンサー、または従業員）を検出し、企業のネットワークまたはエンドユーザー Web ポータル（ゲスト、スポンサーおよびデバイス）にアクセスします。タイプは、モバイル デバイス（Android、iOS など）またはデスクトップ デバイス（Windows、MacOS など）のいずれかとして検出されます。デバイス タイプは、CSS クラスとして利用できます。このクラスは、ユーザーのデバイス タイプに基づいてポータル ページに異なる CSS スタイルを適用するために使用できます。

ユーザーは Cisco ISE のエンドユーザー Web ポータルにログインすると、それらのポータル ページで **cisco-ise-mobile** クラスまたは **cisco-ise-desktop** クラスを使用できます。

関連トピック

ユーザー デバイス タイプに基づいたグリーティングのカスタマイズ （955 ページ）

ポータルのデフォルト テーマ CSS ファイルのエクスポート

シスコが提供するデフォルトのポータルテーマをダウンロードし、ニーズに合わせてカスタマイズできます。それを高度なカスタマイズを実行するための基本として使用できます。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント**

（**Portals & Components**）] > [スポンサーポータル（**Guest Portals**）] > [編集（**Edit**）] > [ポータルページのカスタマイズ（**Portal Page Customization**）] > [ページ（**Pages**）] の順に選択します。

- デバイスポータルの場合、[メニュー（**Menu**）] アイコン（☰）をクリックして次を選択します。[管理（**Administration**）] > [デバイスポータル管理（**Device Portal Management**）] > （任意のポータル） > [編集（**Edit**）] > [ポータルページのカスタマイズ（**Portal Page Customization**）] > [ページ（**Pages**）] の順に選択します。

ステップ 2 [高度なカスタマイズ（Advanced Customization）] ドロップダウン リストから [テーマのエクスポート/インポート（Export/Import Themes）] を選択します。

ステップ 3 [カスタム テーマ（Custom Theming）] ダイアログボックスで、ドロップダウン リストを使用してカスタマイズするテーマを選択します。

ステップ 4 [テーマ CSS のエクスポート（Export Theme CSS）] をクリックして、カスタマイズするデフォルトの *theme.css* ファイルをダウンロードします。

ステップ 5 [保存（Save）] をクリックしてファイルをデスクトップに保存します。

カスタム ポータル テーマ CSS ファイルの作成

カスタム ポータル テーマを作成するには、既存のデフォルト ポータル テーマをカスタマイズして、新規ポータルの *theme*.css ファイルに変更を保存します。デフォルト テーマの設定および見本を変更して、選択したポータルへのグローバルな変更を行うことができます。

始める前に

- カスタマイズするポータルから *theme*.css ファイルをデスクトップにダウンロードします。
- このタスクには、HTML、CSS、および Javascript コードの使用経験が必要です。
- jQuery Mobile ThemeRoller のリリース 1.3.2 を使用します。

ステップ 1 ダウンロードしたポータルの *theme*.css ファイルのコンテンツを jQuery Mobile ThemeRoller ツールにインポートします。

ヒント 変更時に、カスタマイズの参照 （959 ページ） を行うことができます。

ステップ 2 （任意） ポータル コンテンツに組み込まれたリンク （948 ページ）

ステップ 3 （任意） 動的なテキスト更新の変数の挿入 （949 ページ）

ステップ 4 （任意） テキストをフォーマットし、リンクを含めるソース コードの使用 （950 ページ）

ステップ 5 （任意） アドバタイズメントとしてのイメージの追加 （951 ページ）

ステップ 6 （任意） ゲスト ロケーションに基づいたグリーティングのカスタマイズ （954 ページ）

ステップ 7 （任意） ユーザー デバイス タイプに基づいたグリーティングのカスタマイズ （955 ページ）

ステップ 8 （任意） カルーセル アドバタイジングの設定 （952 ページ）

ステップ 9 （任意） ポータル ページのレイアウトの変更 （956 ページ）

ステップ 10 カスタマイズされたファイルを新しい *theme*.css ファイルとして保存します。

（注） デフォルト CSS テーマ ファイルに編集内容を保存することはできません。編集を使用して新しいカスタム ファイルを作成することのみができます。

ステップ 11 新しい *theme*.css ファイルは、準備を整えた後、Cisco ISE にインポートできます。

ポータル コンテンツに組み込まれたリンク

リンクを追加して、ゲストがポータル ページからさまざまな Web サイトにアクセスできるようにすることができます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。

[全画面表示の切り替え（Toggle Full Screen）] オプションを使用して、作業しているフィールドのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals and Components]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals and Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- 証明書プロビジョニングポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[証明書プロビジョニング（Certificate Provisioning）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[オプションの内容（Optional Content）] テキスト ブロックで提供されるミニエディタを使用して、ポータル ページへのリンクを追加します。

ステップ 4 [リンクの作成（Create Link）] ボタンをクリックします。
[リンクのプロパティ（Link Properties）] ダイアログボックスが表示されます。

ステップ 5 [URL] の [説明（Description）] ウィンドウに、ハイパーリンクする **URL** およびテキストを入力します。

リンクが正しく機能するように、URL にプロトコル識別子を含めます。たとえば、www.cisco.com ではなく http://www.cisco.com を使用します。

ステップ 6 [設定（Set）] をクリックし、[保存（Save）] をクリックします。

ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え（Toggle HTML Source）] オプションを使用できます。

動的なテキスト更新の変数の挿入

内容を動的に更新する事前定義済みの変数（$variable$）を代わりに使用することによって、ポータルに表示されるテキストのテンプレートを作成することもできます。これにより、ゲストに表示するテキストと情報の一貫性が維持されます。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え（Toggle Full Screen）] オプションを使用して、作業しているフィールドのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals and Components]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals and Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[説明テキスト（Instructional Text）]、[オプションの内容 1（Optional Content 1）]、および [オプションの内容 2（Optional Content 2）] フィールドで提供されるミニエディタを使用して、ポータルページのテキストテンプレートを作成します。

たとえば、複数のゲスト用に単一の初期メッセージ テンプレートを作成し、正常にログインしてネットワークに接続した後にゲストに表示するメッセージをカスタマイズできます。

ステップ 4 通常どおりに情報をフィールドに入力します。

たとえば、ポータル用の初期メッセージを入力することができます。

```
Welcome to our company's Guest portal,
```

ステップ 5 テキストの代わりに変数を使用する箇所では、[変数の挿入（Insert Variable）] ボタンをクリックします。変数のリストがポップアップ メニューに表示されます。

ステップ 6 テキストの代わりに使用する変数を選択します。

たとえば、初期メッセージに各ゲストの名を表示する [名（First name）] を選択します。変数 **ui_first_name** がカーソル位置に挿入されます。

```
Welcome to our company's Guest portal,$ui_first_name$.
```

これは John という名のゲストのポータルの初期ページに表示される初期メッセージです。**当社のゲストポータルへようこそ、John（Welcome to our company's Guest portal, John）**。

ステップ 7 テキスト ボックスに情報を入力し終えるまで、必要に応じて続けて変数のリストを使用します。

ステップ 8 [保存（Save）] をクリックします。

ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え（Toggle HTML Source）] オプションを使用できます。

テキストをフォーマットし、リンクを含めるソース コードの使用

ミニエディタのフォーマットとプレーンテキスト付きリンクアイコンの使用に加えて、HTML、CSS、および Javascript コードを使用して、ポータル ページに表示されるテキストをカスタマイズすることもできます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。

[全画面表示の切り替え（Toggle Full Screen）] オプションを使用して、作業しているテキストボックスのサイズを拡大および縮小します。

始める前に

[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [ポータルのカスタマイズ（Portal Customization）] で [HTML を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML）] がデフォルトで有効になっていることを確認します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Guest Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > （任意のポータル） > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[説明テキスト（Instructional Text）]、[任意のコンテンツ1（Optional Content 1）]、および [任意のコンテンツ2（Optional Content 2）] の各フィールドで提供されるミニエディタを使用して、ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] をクリックします。

ステップ 5 ソース コードを入力します。

たとえば、テキストに下線を引くには、次のように入力します。

```
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

たとえば、HTML コードを使用してリンクを含めるには、次のように入力します。

```
<a href="http://www.cisco.com">Cisco</a>
```

重要 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対（全体的な）URL パスを入力することを確認します。

ステップ 6 [保存（Save）] をクリックします。

アドバタイズメントとしてのイメージの追加

ポータルページの特定の領域に表示されるイメージおよびアドバタイズメントを含めることができます。

[全画面表示の切り替え（Toggle Full Screen）] オプションを使用して、作業しているテキストボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[説明テキスト（Instructional Text）]、[任意のコンテンツ1（Optional Content 1）]、および [任意のコンテンツ2（Optional Content 2）] の各フィールドで提供されるミニエディタを使用して、ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] をクリックします。

ステップ 5 ソース コードを入力します。

たとえば、ホットスポット ゲスト ポータル ポスト アクセス バナーに HTML コードを使用して製品アドバタイズメントおよびそのイメージを含めるには、このコードを [ポスト アクセス バナー（Post-Access Banner）] ページの [任意のコンテンツ 1（Optional Content 1）] テキスト ボックスに入力します。

```
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p>
<img  src="http://www.static-cisco.com/assets/prod/root/catalyst_6800.jpg" width="100%" />
```

（注） 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対（全体的な）URL パスを入力することを確認します。

ステップ 6 [保存（Save）] をクリックします。

カルーセル アドバタイジングの設定

カルーセルアドバタイジングは、複数の製品イメージまたは説明テキストが表示され、バナー内で循環して繰り返されるアドバタイズメントの形式です。ゲスト ポータルでカルーセル アドバタイジングを使用して、複数の関連製品や、会社が提供するさまざまな製品を宣伝します。

[全画面表示の切り替え（Toggle Full Screen）] オプションを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

始める前に

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [ポータルのカスタマイズ（Portal Customization）]** を選択し、[HTML と Javascript を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML and Javascript）] をオンにします。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Guest Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > （任意のポータル） > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[説明テキスト（Instructional Text）]、[任意のコンテンツ1（Optional Content 1）]、および [任意のコンテンツ2（Optional Content 2）] の各フィールドで提供されるミニエディタを使用して、ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] をクリックします。

ステップ 5 ソース コードを入力します。

たとえば、ゲストポータルで製品イメージを使用してカルーセルアドバタイジングを導入するには、[ポストアクセスバナー（Post-Access Banner）]（ホットスポットポータルの場合）または [ポストログインバナー（Post Login Banner）]（ログイン情報を持つゲストポータルの場合）ウィンドウの [任意のコンテンツ1（Optional Content 1）] フィールドに次の HTML および Javascript コードを入力します。

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 5000);

function changeBanner(){
var bannersArray = ["<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' width='100%'/>",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_0/
n21v1DrawerContainer.img.jpg/1400748629549.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_1/
n21v1DrawerContainer.img.jpg/1376556883237.jpg' width='100%'/>"

];
  var div = document.getElementById("image-ads");
  if(div){
     currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
      div.innerHTML = bannersArray[currentIndex];
   }
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
</style>
<div class="grey" id="image-ads">
<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout- overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg'/>
</div>
```

たとえば、ゲストポータルでテキスト製品説明を使用してカルーセルアドバタイジングを導入するには、[ポストアクセスバナー（Post-Access Banner）]（ホットスポットポータルの場合）または [ポストログインバナー（Post Login Banner）]（ログイン情報を持つゲストポータルの場合）ウィンドウの [任意のコンテンツ2（Optional Content 2）] フィールドに次の HTML および Javascript コードを入力します。

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 2000);

function changeBanner(){
var bannersArray = ["Optimize branch services on a single platform while delivering an optimal
application experience across branch and WAN infrastructure", "Transform your Network Edge to
```

```
deliver high-performance, highly secure, and reliable services to unite campus, data center,
and branch networks",  "Differentiate your service portfolio and increase revenues by delivering
end-to-end scalable solutions and subscriber-aware services"];

var colorsArray = ["grey", "blue",  "green"];
  var div = document.getElementById("text-ads");
  if(div){
     currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
      div.innerHTML = bannersArray[currentIndex];
               div.className = colorsArray[currentIndex];
   }
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
.blue{
color: black;
background-color: lightblue;
}
.green{
color: black;
background-color: lightgreen;
}
</style>
<div class="grey" id="text-ads">
Optimize branch services on a single platform while delivering an optimal application
experience across branch and WAN infrastructure
</div>
```

（注） 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対（全体的な）URL パスを入力する必要があります。

ステップ 6 [保存（Save）] をクリックします。

ゲスト ロケーションに基づいたグリーティングのカスタマイズ

次の例に、ゲストがクレデンシャルを持つゲストポータル（ホットスポットではない）にログインした後に表示される正常なログインメッセージを、ゲストタイプに設定されたロケーションに基づいてカスタマイズする方法を示します。

[全画面表示の切り替え（Toggle Full Screen）] オプションを使用して、作業しているフィールドのサイズを拡大および縮小します。

ステップ 1 次のポータルのいずれかに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント**

（**Portals & Components**）] > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [ページ（Pages）] で、[認証成功（Authentication Success）] をクリックします。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[任意のコンテンツ1（Optional Content 1）] フィールドで提供されるミニエディタを使用して、HTML ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] をクリックします。

ステップ 5 ソース コードを入力します。

たとえば、ロケーションベースのグリーティングを含めるには、[任意のコンテンツ1（Optional Content 1）] に次のコードを入力します。

```
<style>
    .custom-greeting {
        display: none;
    }
    .guest-location-san-jose .custom-san-jose-greeting {
        display: block;
    }
    .guest-location-boston .custom-boston-greeting {
        display: block;
    }
</style>
<div class="custom-greeting custom-san-jose-greeting">
    Welcome to The Golden State!
</div>
<div class="custom-greeting custom-boston-greeting">
    Welcome to The Bay State!
</div>
```

正常なログイン後に、特定のロケーションに応じて異なるメッセージがゲストに表示されます。

ユーザー デバイス タイプに基づいたグリーティングのカスタマイズ

ユーザーが Cisco ISE エンドユーザー Web ポータル（ゲスト、スポンサーおよびデバイス）のいずれかにログインした後に、ユーザーに送信するグリーティングを、クライアントデバイスタイプ（モバイルまたはデスクトップ）に基づいてカスタマイズできます。

[全画面表示の切り替え（Toggle Full Screen）] オプションを使用して、作業しているフィールドのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[オプションコンテンツ 1（Optional Content 1）] フィールドで提供されるミニエディタを使用して、HTML ソースコードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] をクリックします。

ステップ 5 ソース コードを入力します。

たとえば、[AUP] ページでデバイスタイプベースのメッセージを含めるには、[AUP] ウィンドウの [オプションコンテンツ 1（Optional Content 1）] フィールドにこの値を入力します。

```
<style>
    .custom-greeting {
        display: none;
    }
    .cisco-ise-desktop .custom-desktop-greeting {
        display: block;
    }
    .cisco-ise-mobile .custom-mobile-greeting {
        display: block;
    }
</style>
<div class="custom-greeting custom-mobile-greeting">
    Try our New Dark French Roast! Perfect on the Go!
</div>
<div class="custom-greeting custom-desktop-greeting">
    We brough back our Triple Chocolate Muffin!
    Grab a seat and dig in!
</div>
```

ユーザーがネットワークまたはポータルへのアクセスを取得するために使用したデバイスに応じて、[AUP] ページに異なるグリーティングが表示されます。

ポータル ページのレイアウトの変更

ページの全体的なレイアウトを操作できます。たとえば、追加情報や情報へのリンクを提供するサイドバーを AUP ページに追加できます。

ステップ 1 作成し、ポータルに適用するカスタム *theme*.css ファイルの末尾に次の CSS コードを追加します。これにより、AUP ページのレイアウトが変更されます。[任意のコンテンツ1（Optional Content 1）] フィールドは、デスクトップおよびモバイルデバイスモードでサイドバーとして表示されます。

```
#page-aup .cisco-ise-optional-content-1 {
        margin-bottom: 5px;
}
@media all and ( min-width: 60em ) {
        #page-aup .cisco-ise-optional-content-1 {
                float: left;
                margin-right: 5px;
                width: 150px;
        }
```

```
        #page-aup .cisco-ise-main-content {
                float: left;
                width: 800px;
        }
        #page-aup .cisco-ise-main-content h1,
        #page-aup .cisco-ise-main-content p {
                margin-right: auto;
                margin-left: -200px;
        }
}
```

次に、ポータルの AUP ウィンドウの [任意のコンテンツ1（Optional Content 1）] フィールドで HTML コードを使用して、リンクを追加できます。

ステップ 2 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portal & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portal & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 3 [ページ（Pages）] で、サイド バーを追加するページを選択します。

ステップ 4 [ページのカスタマイズ（Page Customizations）] で、[任意のコンテンツ1（Optional Content 1）] フィールドで提供されるミニエディタを使用して、 ソースコードを入力および表示します。

ステップ 5 [HTML ソースの切り替え（Toggle HTML Source）] をクリックします。

ステップ 6 ソース コードを入力します。

たとえば、AUP ウィンドウにサイドバーを含めるには、AUP ウィンドウの [任意のコンテンツ1（Optional Content 1）] フィールドにこのコードを入力します。

```
<ul data-role="listview">
    <li>Rent a Car</li>
    <li>Top 10 Hotels</li>
    <li>Free Massage</li>
    <li>Zumba Classes</li>
</ul>
```

ステップ 7 [保存（Save）] をクリックします。

次のタスク

[任意のコンテンツ（Optional Content）] フィールドに別のテキストまたは HTML コードを入力して、他のページをカスタマイズできます。

カスタム ポータル テーマ CSS ファイルのインポート

作成したカスタム *theme*.css ファイルをアップロードし、エンドユーザー ポータルに適用できます。これらの変更は、カスタマイズしているポータル全体に適用されます。

カスタム *theme*.css ファイルを編集し、Cisco ISE に再度インポートする場合は、最初に使用したテーマ名を使用するように注意してください。同じ *theme*.css ファイルに 2 つの異なるテーマ名を使用することはできません。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[設定（Configure）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > （任意のポータル） > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [高度なカスタマイズ（Advanced Customization）] ドロップダウン リストから [テーマのエクスポート/インポート（Export/Import Themes）] を選択します。

ステップ 3 [カスタム テーマ（Custom Theming）] ダイアログボックスで、新しい *theme*.css ファイルを検索するには、[参照（Browse）] をクリックします。

ステップ 4 新しいファイルの [テーマ名（Theme Name）] を入力します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

カスタマイズするポータルにこのカスタム ポータル テーマを適用できます。

1. ポータル全体に適用する更新されたテーマを [ポータル テーマ（Portal Themes）] ドロップダウン リストから選択します。
2. [保存（Save）] をクリックします。

カスタム ポータル テーマの削除

Cisco ISE にインポートしたカスタム ポータル テーマは、いずれかのポータルで使用されていない場合に削除できます。Cisco ISE によって提供されているデフォルトのテーマを削除することはできません。

始める前に

他のポータルで使用されているポータル テーマを削除することはできません。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** の順に選択します。

ステップ 2 [高度なカスタマイズ（Advanced Customization）] ドロップダウン リストから [テーマの削除（Delete Themes）] を選択します。

ステップ 3 [テーマ名（Theme Name）] ドロップダウン リストから削除するポータル テーマを選択します。

ステップ 4 [削除（Delete）] をクリックし、[保存（Save）] をクリックします。

カスタマイズの参照

カスタマイズがポータルユーザー（ゲスト、スポンサー、従業員）にどのように表示されるかを確認できます。

ステップ 1 [ポータルテストURL（Portal test URL）] をクリックして、変更を表示します。

ステップ 2 （オプション）変更がさまざまなデバイスでどのように表示されるかを動的に確認するには、[プレビュー（Preview）] をクリックします。

- モバイルデバイス：[プレビュー（Preview）] で変更を表示します。
- デスクトップデバイス：[プレビュー（Preview）] をクリックし、[デスクトッププレビュー（Desktop Preview）] をクリックします。

  変更が表示されない場合は、[プレビューのリフレッシュ（Refresh Preview）] をクリックします。表示されるポータルは、変更を確認するためだけのものです。ボタンをクリックしたり、データを入力したりすることはできません。

（注） テストポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

ポータル言語のカスタマイズ

ゲスト、スポンサー、デバイスおよびクライアントプロビジョニングの各ポータルは、サポートされているすべての言語およびロケールにローカライズされています。ローカライズには、テキスト ラベル、メッセージ、フィールド名およびボタン ラベルが含まれます。クライアント ブラウザが Cisco ISE テンプレートにマッピングされていないロケールを要求した場合、ポータルは英語のテンプレートを使用して内容を表示します。

管理者ポータルを使用して、各言語のゲスト、スポンサー、デバイスの各ポータルで使用されるフィールドを個別に変更できます。また、言語を追加することも可能です。現在、クライアントプロビジョニング ポータルについては、これらのフィールドはカスタマイズできません。

デフォルトでは、各タイプのポータルでは 15 言語がサポートされています。[ポータルページのカスタマイズ（Portal Page Customization）] ウィンドウで、ポータルで使用する言語を選択し、オプションで選択した言語でページのコンテンツを更新します。ある言語に合わせてページのフォントとコンテンツを変更しても、他の言語へこの変更は反映されません。[ポータルページのカスタマイズ（Portal Page Customization）] ウィンドウで行った変更は、次回に言語ファイルをエクスポートするときに組み込まれます。

サポート対象の言語は次のとおりです。

- 中国語（簡体字）
- 中国語（繁体字）
- チェコ語
- オランダ語
- 英語
- フランス語
- ドイツ語
- ハンガリー語
- イタリア語
- 日本語
- 韓国語
- ポーランド語

- ポルトガル語
- ロシア語
- スペイン語
- ウクライナ語

ポータルで使用する言語の編集

1. 編集するポータルを開きます。
2. [ポータルページのカスタマイズ（Portal Page Customization] タブで、[表示（view in）] ドロップダウンから、編集する言語を選択します。
3. 必要に応じてコンテンツ、ヘッダー、フォントを変更します。
4. ポータル構成を保存し、更新する他の言語でこのフローを繰り返します。

言語ファイルを編集するには

各 [ポータルページのカスタマイズ（Portal Page Customization）] ウィンドウでは言語ファイルも提供されます。言語ファイルとは、属性ファイルが含まれている ZIP です。これらの属性ファイルは、ポータルフローの一部であるテキストやヘッダーのカスタマイズには使用できますが、[ポータルページのカスタマイズ（Portal Page Customization）] ウィンドウのカスタマイズには使用できません。

言語ファイルには、特定のブラウザロケール設定へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザー Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザ ロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイス ポータルにも適用されます。

zip 形式の言語ファイルをエクスポートし、新規言語の追加や不要な既存言語の削除などを行って更新することができます。

言語ファイルの更新手順については、次を参照してください。

- 言語ファイルのエクスポート （961 ページ）
- 言語ファイルでの言語の追加または削除 （962 ページ）
- 更新された言語ファイルのインポート （963 ページ）

言語ファイルのエクスポート

各ポータルタイプに使用できる言語ファイルをエクスポートして、そのファイルで指定された既存の値を編集およびカスタマイズし、言語を追加または削除できます。

（注） 言語プロパティ ファイル内の一部のディクショナリ キーだけが値（テキスト）で HTML をサポートしています。

ステップ 1 次のポータルに移動します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[編集（Edit）]** を選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[設定（Configure）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Sponsor Portals]** > **[編集（Edit）]** を選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** の順に選択します。

ステップ 2 [言語ファイル（Language File）] をクリックし、ドロップダウン リストから [エクスポート（Export）] を選択します。

ステップ 3 zip 形式の言語ファイルをデスクトップに保存します。

言語ファイルでの言語の追加または削除

ポータル タイプに使用したい言語が言語ファイルにない場合は、新しい言語プロパティ ファイルを作成し、zip 形式の言語ファイルに追加できます。不要な言語がある場合、その言語プロパティ ファイルを削除できます。

始める前に

言語プロパティ ファイルを追加または削除するには、各ポータル タイプで使用可能な zip 形式の言語ファイルをエクスポートします。

ステップ 1 UTF-8 を表示するエディタ（Notepad ++ など）を使用して、言語を追加または削除するポータル タイプ用の定義済み言語ファイルを開きます。

複数のポータル タイプの言語を追加または削除するには、該当するすべてのポータル プロパティ ファイルを使用します。

ステップ 2 新しい言語を追加するには、既存の言語プロパティ ファイルを他のファイルと同じ命名規則を使用する新しい言語プロパティ ファイルとして zip 形式の言語ファイルに保存します。たとえば、新しい日本語の言語プロパティ ファイルを作成するには、ファイルを Japanese.properties（*LanguageName*.properties）として保存します。

ステップ 3 新しい言語プロパティ ファイルの最初の行にブラウザ ロケール値を指定して、ブラウザ ロケールに新しい言語を関連付けます。たとえば、LocaleKeys= ja,ja-jp（LocaleKeys=*browser locale value*）を Japanese.properties ファイルの最初の行に入力する必要があります。

ステップ 4 新しい言語プロパティ ファイルでディクショナリ キーのすべての値（テキスト）を更新します。

ディクショナリキーは変更できません。それらの値のみを更新できます。

（注） 一部のディクショナリ キーだけが、値（テキスト）に HTML をサポートしています。

次のタスク

1. すべてのプロパティ ファイル（新規および既存）を zip 形式で圧縮し、新しい zip 形式の言語ファイルを作成します。フォルダやディレクトリは含めないでください。

（注） Mac を使用する場合は、ZIP ファイルを抽出すると、DS ストアが生成されます。編集後に言語ファイルを圧縮する場合は、DS ストアに ZIP を含めないでください。DS ストアの抽出方法については、https://superuser.com/questions/198569/compressing-folders-on-a-mac-without-the-ds-store を参照してください。

2. zip 形式の言語ファイルには新しい名前または元の名前を使用します。
3. エクスポート元の特定のポータルに zip 形式の言語ファイルをインポートします。

更新された言語ファイルのインポート

言語プロパティ ファイルを追加または削除したり、既存のプロパティ ファイルのテキストを更新してカスタマイズした編集済み言語ファイルをインポートできます。

（注） Word ファイルからカスタマイズした内容をコピーして貼り付けることはできません。代わりに [ファイル（File）] > [名前を付けて保存（Save As）] を選択し、Word ファイルを HTML 形式で保存します。その後、この HTML ファイルからカスタマイズした内容をコピーして貼り付けることができます。

ステップ 1 次のポータルに移動します。

- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Sponsor Portals）]** > **[編集（Edit）]** の順に選択します。

- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** の順に選択します。

ステップ 2 [言語ファイル（Language）] をクリックし、ドロップダウン リストから [インポート（Import）] を選択します。

ステップ 3 デスクトップを参照して新しい zip 形式の言語ファイルを見つけます。

ステップ 4 エクスポートしたポータル タイプに再度インポートします。

次のタスク

変更したテキストまたは追加した新しい言語を表示するには、[表示（View In）] ドロップダウン リストから特定の言語を選択します。

ゲスト通知、承認、およびエラー メッセージのカスタマイズ

各ポータルで内で、ゲストが電子メール、SMS テキスト メッセージ、および印刷物で通知を受け取る方法をカスタマイズできます。これらの通知を使用して、次の場合にログイン クレデンシャルを電子メール送信、テキスト送信、または印刷します。

- ゲストがアカウント登録ゲスト ポータルを使用し、自分自身の登録に成功した場合。
- スポンサーがゲスト アカウントを作成し、ゲストに詳細を提供する場合。スポンサー グループ作成時にスポンサーによる SMS 通知の使用を許可するかどうかを指定できます。これらの機能を利用できる場合は、常に電子メール通知および印刷通知を使用できます。

ネットワークにアクセスしようとするアカウント登録ゲストを承認するよう要求するスポンサー宛電子メール通知をカスタマイズすることもできます。また、ゲストとスポンサーに表示されるデフォルトのエラー メッセージをカスタマイズできます。

電子メールでの通知のカスタマイズ

電子メールでゲストに送信される情報をカスタマイズできます。

始める前に

- 電子メールでの通知を有効にするように SMTP サーバーを設定します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[SMTP サーバー（SMTP Server）]** を選択します。
- ゲストへの電子メールでの通知のサポートを設定します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work**

Centers）] > [ゲストアクセス（Guest Access）] > [設定（Settings）] > [ゲスト電子メールの設定（Guest Email Settings）] を選択します。[ゲストへの電子メール通知を有効にする（Enable email notifications to guests）] をオンにします。

- **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [ポータルのカスタマイズ（Portal Customization）]** で [HTML を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML）] がデフォルトで有効になっていることを確認します。

ステップ 1 自己登録スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [ゲストへの通知（Notify Guests）] > [電子メール通知（Email Notification）]** を選択します。

ステップ 2 [グローバル ページのカスタマイズ（Global Page Customizations）] で指定されたデフォルトの [ロゴ（電子メール）（Logo (Email)）] を変更できます。

ステップ 3 [件名（Subject）] および [電子メール本文（Email body）] を指定します。電子メール メッセージに含まれる、ゲスト アカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。

ステップ 4 [設定（Settings）] では、次のことが可能です。

- 異なる電子メールで [ユーザー名とパスワードを個別に送信する（Send username and password separately）]。このオプションを選択すると、**ユーザー名電子メール通知**と**パスワード電子メール通知**をカスタマイズするための 2 つのタブが [ページのカスタマイズ（Page Customizations）] に表示されます。
- 電子メール アドレスへの [テスト電子メールの送信（Send Test Email）]。すべてのデバイスでカスタマイズをプレビューし、適切に表示されることを確認します。

ステップ 5 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

SMS テキスト メッセージ通知のカスタマイズ

SMS テキスト メッセージでゲストに送信される情報をカスタマイズできます。

始める前に

- SMS ゲートウェイに電子メールを送信して、SMS テキスト メッセージを配信するために使用される SMTP サーバーを設定します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]>[システム（System）]> [設定（Settings）] > [SMTP サーバー（SMTP Server）]** を選択します。
- SMS テキスト通知をサポートするようにスポンサー グループを設定します。

- サードパーティ SMS ゲートウェイでアカウントを設定します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（Systems）]** > **[設定（Settings）]** > **[SMS ゲートウェイ（SMS Gateway）]** を選択します。Cisco ISE では、テキスト メッセージが電子メールとしてゲートウェイに送信され、SMS プロバイダー経由で指定したユーザーにメッセージが転送されます。
- **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[ポータルのカスタマイズ（Portal Customization）]** で [HTML を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML）] がデフォルトで有効になっていることを確認します。

ステップ 1 アカウント登録ゲストポータルおよびスポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータルまたはスポンサーポータル（Guest or Sponsor Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[SMS 受信または SMS 通知（SMS Receipt or SMS Notification）]** を選択します。

ステップ 2 [メッセージ テキスト（Message Text）] をカスタマイズするには、ミニエディタと HTML タグを使用します。SMS テキスト メッセージに含まれる、ゲスト アカウント情報を指定するには、事前定義済みの変数を使用します。

ステップ 3 [設定（Settings）] では、次のことが可能です。

- 異なるテキスト メッセージで [ユーザー名とパスワードを個別に送信する（Send username and password separately）]。このオプションを選択すると、**ユーザー名メッセージ**と**パスワード メッセージ**をカスタマイズするための 2 つのタブが [ページのカスタマイズ（Page Customizations）] に表示されます。
- 携帯電話への [テスト メッセージの送信（Send Test Message）]。カスタマイズをプレビューし、情報が適切に表示されることを確認します。

ステップ 4 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

印刷通知のカスタマイズ

ゲスト用に印刷される情報をカスタマイズできます。

（注） 各ポータル内では、印刷通知ロゴは、電子メール通知ロゴの設定から継承されます。

始める前に

[管理（Administration）] > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[ポータルのカスタマイズ（Portal Customization）]** で [HTML を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML）] がデフォルトで有効になっていることを確認します。

ステップ 1 アカウント登録ゲストポータルおよびスポンサーポータルの場合、**[メニュー（Menu）]**アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]**>**[ゲストポータルまたはスポンサーポータル（Guest or Sponsor Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[印刷受け取りまたは印刷通知（Print Receipt or Print Notification）]** を選択します。

ステップ 2 [印刷説明テキスト（Print Introduction Text）] を指定します。電子メール メッセージに含まれる、ゲスト アカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。

ステップ 3 サムネールで、または [印刷プレビュー（Print Preview）] をクリックして、カスタマイズをプレビューします。サムネールでは、HTML のカスタマイズを表示できません。
[印刷プレビュー（Print Preview）] オプションを選択した場合、アカウントの詳細を印刷できるウィンドウが表示され、そこで適切に表示されることを確認します。

ステップ 4 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

承認要求の電子メールでの通知のカスタマイズ

アカウント登録ゲストのアカウントが作成され、そのゲストがログインクレデンシャルを取得する前に、アカウント登録ゲストを承認するようスポンサーに要求できます。電子メールでスポンサーに送信される、承認を要求する情報をカスタマイズできます。この通知は、ネットワーク アクセスを許可する前にアカウント登録ゲスト ポータルを使用するアカウント登録ゲストを承認する必要があると指定した場合にのみ表示されます。

始める前に

- 電子メールでの通知を有効にするように SMTP サーバーを設定します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]**>**[システム（System）]**>**[設定（Settings）]**>**[SMTP サーバー（SMTP Server）]** を選択します。
- ゲストへの電子メールでの通知のサポートを設定します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[設定（Settings）]** > **[ゲスト電子メールの設定（Guest Email Settings）]** を選択します。[ゲストへの電子メール通知を有効にする（Enable email notifications to guests）] をオンにします。
- スポンサーに自己登録アカウントの要求を承認させるには、[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブの [アカウント登録ページの設定（Self-Registration Page Settings）] で、[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] をオンにします。それによって、[ポータルページのカスタマイズ（Portal Page Customization）] の [通知（Notifications）] の下の [承認要求の電子メール（Approval Request Email）] タブが有効になり、スポンサーに送られる電子メールをカスタマイズできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [設定（Configure）] > [アカウント登録ゲストポータル（Self-Registered Guest Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [承認要求電子メール（Approval Request Email）]** を選択します。ここでは次を実行できます。

ステップ 2 次の手順を実行します。

a) [グローバル ページのカスタマイズ（Global Page Customizations）] で指定されたデフォルトの [ロゴ（Logo）] を変更します。

b) [件名（Subject）] および [電子メール本文（Email body）] を指定します。電子メール メッセージに含まれる、ゲスト アカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。たとえば、リクエスト承認の電子メールにスポンサーポータルへのリンクを含めるには、[リンクを作成（Create a Link）] をクリックして、スポンサーポータルに FQDN を追加します。

c) [テスト電子メールの送信（Send Test Email）] を使用してすべてのデバイスでカスタマイズをプレビューし、適切に表示されることを確認します。

d) [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

ステップ 3 スポンサーが送信する承認電子メールの内容をカスタマイズします。

a) **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）]** を選択します。

b) [ポータルページのカスタマイズ（Portal Page Customizations）] をクリックします。

c) [電子メール通知（Email Notification）] タブをクリックし、詳細を入力します。

エラー メッセージの編集

ゲスト、スポンサー、および従業員に表示される [失敗（Failure）] ページに表示されるエラーメッセージを完全にカスタマイズできます。[失敗（Failure）] ページは、[ブロック済みリスト（Blocked List）] ポータルを除くすべてのエンドユーザー Web ポータルで利用可能です。

ステップ 1 次のいずれかを実行します。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [メッセージ（Messages）] > [エラーメッセージ（Error Messages）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [メッセージ（Messages）] > [エラーメッセージ（Error Messages）]** の順に選択します。

- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[メッセージ（Messages）]** > **[エラーメッセージ（Error Messages）]** の順に選択します。

ステップ 2 [表示言語（View In）] ドロップダウンから、メッセージのカスタマイズ時にテキストを表示する言語を選択します。

このドロップダウン リストには、特定のポータルに関連付けられた言語ファイルのすべての言語が含まれています。ポータルページのカスタマイズ時に行った変更でサポート対象の言語プロパティ ファイルを更新します。

ステップ 3 エラー メッセージ テキストを更新します。特定のエラー メッセージを検索するには、エラー メッセージに関連付けられた AUP を検索する **aup** などのキーワードを入力します。

ステップ 4 **[保存（Save）]** > **[閉じる（Close）]** の順に選択します。

ポータル ページのタイトル、コンテンツおよびラベルの文字数制限

[ポータル ページのカスタマイズ（Portal Page Customization）] タブのタイトル、テキスト ボックス、手順、フィールド、ボタン ラベル、およびその他の視覚的な要素に入力できる文字数には上限および下限があります。

ポータル ページのタイトル、コンテンツおよびラベルの文字数制限

ポータル ページの UI 要素へのナビゲーション パスは、次のとおりです。

- ゲストポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲストポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** の順に選択します。
- スポンサーポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** の順に選択します。
- デバイスポータルの場合、**[メニュー（Menu）]** アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** の順に選択します。

タイトル、テキストボックス、手順、フィールドとボタンのラベル、およびカスタマイズしているポータルページのその他のビジュアル要素のコンテンツを入力する際に、この情報を使用します。これらの更新は、カスタマイズしている特定のページにのみ適用されます。

（注） シングルバイト文字とマルチバイト文字のどちらを入力するかにかかわらず、識別される最大文字数のみをフィールドに入力できます。マルチバイト文字は文字数制限には影響しません。

フィールドのカテゴリ	フィールド	フィールド ラベル：最小文字数	フィールド ラベル：最大文字数	フィールドの入力値：最小文字数	フィールドの入力値：最大文字数
共通のページ要素	バナー タイトル				256
	フッター要素			0	2000
	ブラウザ ページのタイトル			0	256
	説明テキスト			0	2000
	コンテンツ タイトル			0	256
	オプション コンテンツ 1			0	2000
	オプション コンテンツ 2			0	2000
	ボタン ラベル	0	64		
	チェック ボックス ラベル	0	64		
	タブ ラベル	0	64		
	リンク ラベル	0	256		

フィールドのカテゴリ	フィールド	フィールド ラベル：最小文字数	フィールド ラベル：最大文字数	フィールドの入力値：最小文字数	フィールドの入力値：最大文字数
AUP	AUP テキスト			0	50,000
メッセージ テキスト	メッセージ テキスト（ページに表示）			0	2000
	メッセージ テキスト（ポップアップ ウィンドウに表示）			0	256
フィールド ラベル	すべての フィールド ラベル	0	256		
フィールド入力（一般）	一般的な フィールド入力（次の特別な場合を参照）			0	256
フィールド入力（特別な場合）	[アクセス コード（Access Code）] フィールド			1	20
	[登録コード（Registration Code）] フィールド			1	20
	[ユーザー名（Username）] フィールド			1	64
	[パスワード（Password）] フィールド			1	256

フィールドのカテゴリ	フィールド	フィールド ラベル：最小文字数	フィールド ラベル：最大文字数	フィールドの入力値：最小文字数	フィールドの入力値：最大文字数
	[電話番号（Phone Number）] フィールド			0	64
	[デバイス ID（Device ID）] フィールド			12	17

ポータルのカスタマイズ

エンドユーザー Web ポータルおよびゲスト エクスペリエンスの外観をカスタマイズできます。カスケーディング スタイル シート（CSS）言語と Javascript の使用経験がある場合、ポータル ページのレイアウトを変更することで、jQuery Mobile ThemeRoller アプリケーションを使用してポータルのテーマをカスタマイズできます。

必要なポータル ページから CSS テーマまたは言語プロパティをエクスポートすることで、すべてのフィールドを表示できます。詳細については、「ポータルのデフォルト テーマ CSS ファイルのエクスポート」を参照してください。

エンドユーザー ポータルのページ レイアウトの CSS クラスと説明

Cisco ISE エンドユーザー Web ポータルのページ レイアウトを定義および変更するには、次の CSS クラスを使用します。

CSS クラス名	説明
cisco-ise-banner	ロゴ、バナー イメージ、およびバナー テキストが含まれます。 スポンサー ポータルおよびデバイス ポータルでは、このクラスにコンテキスト メニューをアクティブ化できるボタンも含まれます。たとえば、このメニューで [ログアウト（Log Out）]、[パスワードの変更（Change Password）] などのオプションが含まれるポップアップ ウィンドウを表示できます。
cisco-ise-body	バナーの一部ではないすべてのページの要素が含まれます。

CSS クラス名	説明
cisco-ise-optional-content-1	デフォルトでは空です。テキスト、リンク、および HTML コードと JavaScript コードを追加できます。
cisco-ise-main-content	説明テキスト、操作ボタン、および cisco-ise-footer コンテナなど、ポータル ページのメイン コンテンツが含まれます。
cisco-ise-optional-content-2	デフォルトでは空です。テキスト、リンク、および HTML コードと JavaScript コードを追加できます。
cisco-ise-footer	フッターの一部です。**サポートへの問い合わせ**やオンライン **ヘルプ**などのリンクのプレースホルダーです。
cisco-ise-footer-text	デフォルトでは空です。著作権表示または免責事項など、ポータル ページの下部に表示するもののプレースホルダーです。

ポータル言語ファイルの HTML サポート

各ポータルの圧縮済み言語ファイルには、そのポータルのデフォルト言語プロパティ ファイルが含まれます。各プロパティ ファイルには、ポータルに表示される内容を定義するディクショナリ キーが含まれます。

[説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[オプションコンテンツ 1（Optional Content 1）]、[オプションコンテンツ 2（Optional Content 2）] の各フィールドの内容など、ポータルに表示されるテキストをカスタマイズすることができます。これらのフィールドには、デフォルトのコンテンツがあるものと空白のものがあります。

これらのフィールドに関連付けられたディクショナリキーの一部でのみ、その値（テキスト）で HTML がサポートされます。

ブロック済みリストポータル言語ファイルの HTML サポート

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [ブロック済みリストポータル（Blocked List Portal）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]**。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.blacklist.ui_reject_message

個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[BYOD ポータル（BYOD Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** です。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_contact_instruction_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_byod_reg_limit_message
- key.guest.ui_byod_reg_content_message
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_byod_welcome_aup_text
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1

- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_error_instruction_message

証明書プロビジョニング ポータルの言語ファイルの HTML サポート

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[証明書プロビジョニングポータル（Certificate Provisioning Portal）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** です。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.manualcertprov.ui_login_instruction_message
- key.manualcertprov.ui_aup_instruction_message
- key.manualcertprov.ui_changepwd_instruction_message
- key.manualcertprov.ui_post_access_instruction_message
- key.manualcertprov.ui_status_csv_invalid_instruction_message
- key.manualcertprov.ui_login_optional_content_1
- key.manualcertprov.ui_login_optional_content_2
- key.manualcertprov.ui_aup_optional_content_1

- key.manualcertprov.ui_aup_optional_content_2
- key.manualcertprov.ui_changepwd_optional_content_1
- key.manualcertprov.ui_changepwd_optional_content_2
- key.manualcertprov.ui_post_access_optional_content_1
- key.manualcertprov.ui_post_access_optional_content_2
- key.manualcertprov.ui_landing_instruction_message
- key.manualcertprov.ui_status_page_single_generated_content
- key.manualcertprov.ui_status_generated_content

クライアント プロビジョニング ポータルの言語ファイルの HTML サポート

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[クライアント プロビジョニング ポータル（Client Provisioning Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** です。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1

- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

クレデンシャル ゲスト ポータルの言語ファイルの HTML サポート

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_contact_instruction_message
- key.guest.ui_login_optional_content_1
- key.guest.ui_login_optional_content_2
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_device_reg_optional_content_2
- key.guest.ui_device_reg_optional_content_1

- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_max_devices_instruction_message
- key.guest.ui_max_devices_optional_content_1
- key.guest.ui_self_reg_results_instruction_message
- key.guest.notification_credentials_email_body
- key.guest.ui_max_devices_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_changepwd_instruction_message
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_aup_instruction_message
- key.guest.ui_changepwd_optional_content_2
- key.guest.ui_changepwd_optional_content_1
- key.guest.ui_self_reg_results_optional_content_2
- key.guest.ui_self_reg_results_optional_content_1
- key.guest.ui_device_reg_instruction_message
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_vlan_execute_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_device_reg_max_reached_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_aup_employee_text

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_success_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_self_reg_optional_content_2
- key.guest.ui_self_reg_optional_content_1
- key.guest.ui_byod_reg_limit_message
- key.guest.notification_credentials_print_body
- key.guest.ui_byod_reg_content_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_aup_guest_text
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_self_reg_aup_text
- key.guest.ui_login_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_self_reg_results_aup_text
- key.guest.ui_device_reg_register_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_self_reg_instruction_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message

- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_client_provision_posture_agent_scan_message

ホットスポット ゲスト ポータルの言語ファイルの HTML サポート

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_success_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_vlan_unsupported_error_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_aup_instruction_message
- key.guest.ui_aup_hotspot_text
- key.guest.ui_vlan_execute_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1

- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1

モバイル デバイス管理ポータルの言語ファイルの HTML サポート

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [MDM ポータル（MDM Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

- key.mdm.ui_contact_instruction_message
- key.mdm.ui_mdm_enrollment_after_message
- key.mdm.ui_error_optional_content_2
- key.mdm.ui_error_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_2
- key.mdm.ui_mdm_enroll_instruction_message
- key.mdm.ui_error_instruction_message
- key.mdm.ui_mdm_enrollment_link_message
- key.mdm.ui_mdm_not_reachable_message
- key.mdm.ui_contact_optional_content_2
- key.mdm.ui_mdm_continue_message
- key.mdm.ui_contact_optional_content_1

デバイス ポータルの言語ファイルの HTML サポート

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [編集（Edit）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.mydevices.ui_add_optional_content_1
- key.mydevices.ui_add_optional_content_2
- key.mydevices.ui_post_access_instruction_message
- key.mydevices.ui_edit_instruction_message
- key.mydevices.ui_contact_optional_content_2
- key.mydevices.ui_contact_optional_content_1
- key.mydevices.ui_changepwd_optional_content_1
- key.mydevices.ui_changepwd_optional_content_2
- key.mydevices.ui_post_access_message
- key.mydevices.ui_home_instruction_message
- key.mydevices.ui_edit_optional_content_1
- key.mydevices.ui_edit_optional_content_2
- key.mydevices.ui_add_instruction_message
- key.mydevices.ui_post_access_optional_content_2
- key.mydevices.ui_post_access_optional_content_1
- key.mydevices.ui_error_instruction_message
- key.mydevices.ui_actions_instruction_message
- key.mydevices.ui_home_optional_content_2
- key.mydevices.ui_aup_optional_content_1
- key.mydevices.ui_aup_optional_content_2
- key.mydevices.ui_home_optional_content_1
- key.mydevices.ui_changepwd_instruction_message
- key.mydevices.ui_contact_instruction_message
- key.mydevices.ui_aup_employee_text
- key.mydevices.ui_login_optional_content_2
- key.mydevices.ui_login_optional_content_1
- key.mydevices.ui_login_instruction_message

- key.mydevices.ui_error_optional_content_1
- key.mydevices.ui_error_optional_content_2
- key.mydevices.ui_aup_instruction_message

スポンサー ポータルの言語ファイルの HTML サポート

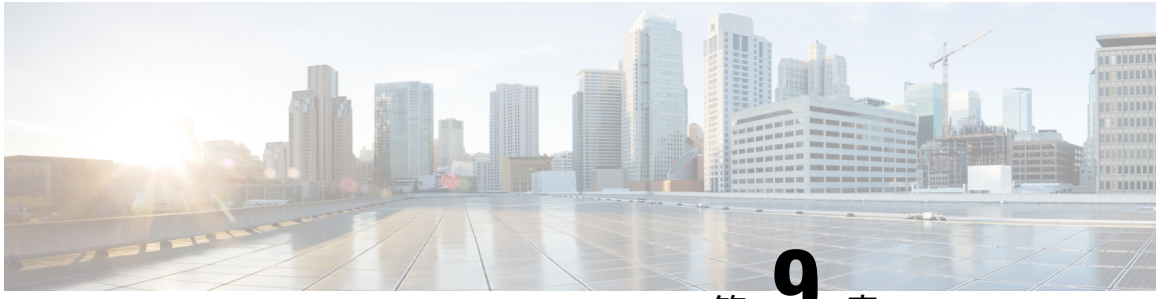
このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Sponsor Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（ Portal Page Customization）]** > **[ページ（（Pages）]** です。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.sponsor.ui_aup_instruction_message
- key.sponsor.ui_create_random_instruction_message
- key.sponsor.ui_home_instruction_message
- key.sponsor.ui_post_access_instruction_message
- key.sponsor.notification_credentials_print_body
- key.sponsor.ui_aup_sponsor_text
- key.sponsor.ui_create_accounts_access_info_instruction_message
- key.sponsor.ui_login_instruction_message
- key.sponsor.notification_credentials_email_body
- key.sponsor.ui_create_known_instruction_message
- key.sponsor.ui_create_import_instruction_message
- key.sponsor.ui_suspend_account_instruction_message
- key.sponsor.ui_post_access_message
- key.sponsor.ui_login_optional_content_2
- key.sponsor.ui_login_optional_content_1
- key.sponsor.notification_credentials_email_password_body
- key.sponsor.ui_contact_optional_content_2
- key.sponsor.ui_contact_optional_content_1

- key.sponsor.ui_login_aup_text
- key.sponsor.ui_changepwd_instruction_message
- key.sponsor.ui_create_accounts_guest_type_instruction_message
- key.sponsor.ui_changepwd_optional_content_1
- key.sponsor.ui_changepwd_optional_content_2
- key.sponsor.notification_credentials_email_username_body
- key.sponsor.ui_aup_optional_content_1
- key.sponsor.ui_aup_optional_content_2
- key.sponsor.ui_post_access_optional_content_1
- key.sponsor.ui_post_access_optional_content_2
- key.sponsor.ui_contact_instruction_message



第 9 章

アセットの可視性

- 外部 ID ストアを使用した Cisco ISE への管理アクセス （987 ページ）
- 外部 ID ソース （992 ページ）
- Cisco ISE ユーザー （1004 ページ）
- 内部 ID ソースと外部 ID ソース （1023 ページ）
- 証明書認証プロファイル （1027 ページ）
- 外部 ID ソースとしての Active Directory （1028 ページ）
- Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件 （1068 ページ）
- Easy Connect （1077 ページ）
- PassiveID ワーク センター （1083 ページ）
- LDAP （1142 ページ）
- ODBC ID ソース （1160 ページ）
- RADIUS トークン ID ソース （1169 ページ）
- RSA ID ソース （1176 ページ）
- 外部 ID ソースとしての SAMLv2 ID プロバイダー （1185 ページ）
- Cisco pxGrid Direct （1195 ページ）
- ID ソース順序 （1206 ページ）
- レポートでの ID ソースの詳細 （1208 ページ）
- ネットワークのプロファイリングされたエンドポイント （1208 ページ）
- プロファイラ条件の設定 （1209 ページ）
- Cisco ISE プロファイリング サービス （1210 ページ）
- プロファイラフォワーダ永続キュー （1212 ページ）
- Cisco ISE ノードでのプロファイリング サービスの設定 （1213 ページ）
- プロファイリング サービスによって使用されるネットワーク プローブ （1213 ページ）
- Cisco ISE ノードごとのプローブの設定 （1226 ページ）
- CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定 （1227 ページ）
- ISE データベースの持続性とパフォーマンスの属性フィルタ （1232 ページ）
- Cisco IOS センサー組み込みスイッチからの属性の収集 （1235 ページ）
- ISE プロファイラによる Cisco IND コントローラのサポート （1237 ページ）

- MUD の Cisco ISE サポート （1239 ページ）
- 多要素分類による拡張エンドポイントの可視化 （1242 ページ）
- AI 分析によって実現されるサービス （1245 ページ）
- プロファイラ条件 （1250 ページ）
- プロファイリング ネットワーク スキャン アクション （1250 ページ）
- プロファイラ条件の作成 （1267 ページ）
- エンドポイント プロファイリング ポリシー ルール （1267 ページ）
- エンドポイント プロファイリング ポリシーの設定 （1269 ページ）
- エンドポイント プロファイリング ポリシーの作成 （1274 ページ）
- 事前定義されたエンドポイント プロファイリング ポリシー （1278 ページ）
- Cisco Catalyst 9800 ワイヤレス LAN コントローラからの Wi-Fi デバイス分析データ （1282 ページ）
- エンドポイント プロファイリング ポリシーの論理プロファイルによるグループ化 （1284 ページ）
- プロファイリング例外アクション （1285 ページ）
- ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 （1286 ページ）
- 識別されたエンドポイント （1292 ページ）
- エンドポイント ID グループの作成 （1294 ページ）
- エニーキャストおよびプロファイラサービス （1298 ページ）
- プロファイラ フィード サービス （1298 ページ）
- プロファイラ レポート （1303 ページ）
- エンドポイントの異常な動作の検出 （1304 ページ）
- クライアント マシン上のエージェントのダウンロードの問題 （1306 ページ）
- エンドポイント （1307 ページ）
- IF-MIB （1321 ページ）
- SNMPv2-MIB （1321 ページ）
- IP-MIB （1322 ページ）
- CISCO-CDP-MIB （1322 ページ）
- CISCO-VTP-MIB （1323 ページ）
- CISCO-STACK-MIB （1323 ページ）
- BRIDGE-MIB （1323 ページ）
- OLD-CISCO-INTERFACE-MIB （1324 ページ）
- CISCO-LWAPP-AP-MIB （1324 ページ）
- CISCO-LWAPP-DOT11-CLIENT-MIB （1325 ページ）
- CISCO-AUTH-FRAMEWORK-MIB （1326 ページ）
- EEE8021-PAE-MIB: RFC IEEE 802.1X （1326 ページ）
- HOST-RESOURCES-MIB （1327 ページ）
- LLDP-MIB （1327 ページ）
- エンドポイントのセッションのトレース （1327 ページ）
- エンドポイントのグローバル検索 （1329 ページ）

外部 ID ストアを使用した Cisco ISE への管理アクセス

Cisco ISE では、Active Directory、LDAP、RSA SecureID などの外部 ID ストアを介して管理者を認証できます。外部 ID ストアを介した認証の提供に使用できる次の 2 つのモデルがあります。

- 外部認証および許可：管理者に関してローカル Cisco ISE データベースで指定されたクレデンシャルはなく、許可は、外部 ID ストア グループ メンバーシップのみに基づきます。このモデルは、Active Directory および LDAP 認証で使用されます。
- 外部認証および内部許可：管理者の認証クレデンシャルは外部 ID ソースから取得され、許可および管理者ロール割り当てはローカル Cisco ISE データベースを使用して行われます。このモデルは、RSA SecurID 認証で使用されます。この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザー名を設定する必要があります。

認証プロセス時、Cisco ISE は、外部 ID ストアとの通信が確立されなかった場合や失敗した場合はフォールバックし、内部 ID データベースから認証の実行を試行するように設計されています。さらに、外部認証が設定されている管理者には、ブラウザを起動してログインセッションを開始するたびに、ログインダイアログボックスの [ID ストア（Identity Store）] ドロップダウンリストから [内部（Internal）] を選択すると Cisco ISE のローカルデータベースを介した認証を要求するオプションが依然として表示されます。

ネットワーク管理者グループに所属する管理者と、外部 ID ストアを使用して認証および認可するように設定されている管理者は、CLI（コマンドラインインターフェイス）アクセス用に外部 ID ストアを使用して認証することもできます。

（注） 外部管理者認証を提供するこの方法は、管理者ポータルを介してのみ設定できます。Cisco ISE CLI では、これらの機能は設定されません。

ネットワークに既存の外部 ID ストアがまだない場合は、必要な外部 ID ストアをインストールし、これらの ID ストアにアクセスするように Cisco ISE が設定されていることを確認します。

外部認証および許可

デフォルトでは、Cisco ISE によって内部管理者認証が提供されます。外部認証を設定するには、外部 ID ストアで定義している外部管理者アカウントのパスワード ポリシーを作成する必要があります。次に、結果的に外部管理者 RBAC ポリシーの一部となるこのポリシーを外部管理者グループに適用できます。

外部認証を設定するには、次の手順を実行する必要があります。

- 外部 ID ストアを使用してパスワード ベースの認証を設定します。
- 外部管理者グループを作成します。
- 外部管理者グループ用のメニュー アクセスとデータ アクセスの権限を設定します。

- 外部管理者認証の RBAC ポリシーを作成します。

ネットワークでは、外部 ID ストア経由の認証を提供するほかに、Common Access Card（CAC）認証デバイスを使用する必要もある場合があります。

外部 ID ストアを使用したパスワード ベースの認証の設定

最初に、Active Directory や LDAP などの外部 ID ストアを使用して認証を行う管理者のためのパスワード ベースの認証を設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]** を選択します。

ステップ 2 [認証方式（Authentication Method）] タブで、[パスワードベース（Password Based）] をクリックし、すでに設定されている外部 ID ソースの 1 つを選択します。たとえば、作成した Active Directory インスタンスを選択します。

ステップ 3 外部 ID ストアを使用して認証を行う管理者のためのその他の特定のパスワード ポリシーを設定します。

ステップ 4 [保存（Save）] をクリックします。

外部管理者グループの作成

外部 Active Directory または LDAP 管理者グループを作成する必要があります。これにより、Cisco ISE は外部 Active Directory または LDAP ID ストアで定義されているユーザー名を使用して、ログイン時に入力した管理者ユーザー名とパスワードを検証します。

Cisco ISE は、外部リソースから Active Directory または LDAP グループ情報をインポートし、それをディクショナリ属性として保存します。次に、この属性を、外部管理者認証方式用の RBAC ポリシーを設定するときのポリシー要素の 1 つとして指定できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]** を選択します。

[マッピングされた外部グループ（External Groups Mapped）] 列には、内部 RBAC ロールにマップされている外部グループの数が表示されます。管理者ロールに対応する番号をクリックすると、外部グループを表示できます（たとえば、[ネットワーク管理者（Super Admin）] に対して表示されている 2 をクリックすると、2 つの外部グループの名前が表示されます）。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 名前とオプションの説明を入力します。

ステップ 4 [外部（External）] をクリックします。

Active Directory ドメインに接続し、参加している場合は、Active Directory インスタンス名が [名前（Name）] フィールドに表示されます。

ステップ 5 [外部グループ（External Groups）] ドロップダウン リスト ボックスから、この外部管理者グループにマッピングする Active Directory グループを選択します。

追加の Active Directory グループをこの外部管理者グループにマッピングするために「+」記号をクリックします。

ステップ 6 [保存（Save）] をクリックします。

内部読み取り専用管理者の作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）]** を選択します。

ステップ 2 [追加（Add）] をクリックして、[管理ユーザーの作成（Create An Admin User）] を選択します。

ステップ 3 [読み取り専用（Read Only）] チェックボックスをオンにして読み取り専用管理者を作成します。

外部グループを読み取り専用管理者グループにマッピング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択して、外部認証ソースを設定します。

ステップ 2 必要な外部 ID ソース（Active Directory や LDAP など）をクリックし、選択した ID ソースからグループを取得します。

ステップ 3 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] を選択して、管理者アクセスの認証方式を ID ソースとマッピングします。

ステップ 4 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）] を選択し、[読み取り専用管理者（Read Only Admin）] グループを選択します。

ステップ 5 [外部（External）]チェックボックスをオンにして、読み取り専用権限を提供する必要のある外部グループを選択します。

ステップ 6 [保存（Save）] をクリックします。

読み取り専用管理者グループにマップされている外部グループは、他の管理者グループに割り当てることはできません。

外部管理者グループのメニューアクセス権限とデータアクセス権限の設定

外部管理者グループに割り当てることができるメニュー アクセス権限とデータ アクセス権限を設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [権限（Permissions）]** を選択します。

ステップ 2 次のいずれかをクリックします。

- **[メニューアクセス（Menu Access）]**：外部管理者グループに属するすべての管理者に、メニューまたはサブメニューレベルでの権限を付与することができます。メニュー アクセス権限によって、アクセスできるサブメニューまたはメニューが決定されます。
- **[データアクセス（Data Access）]**：外部管理者グループに属するすべての管理者に、データレベルでの権限を付与することができます。データ アクセス権限によって、アクセスできるデータが決定されます。

ステップ 3 外部管理者グループのメニュー アクセス権限とデータ アクセス権限を指定します。

ステップ 4 [保存（Save）] をクリックします。

外部管理者認証の RBAC ポリシーの作成

外部 ID ストアを使用して管理者を認証し、カスタムメニューアクセス権限とデータアクセス権限を指定するには、新しいRBACポリシーを設定する必要があります。このポリシーには、認証用の外部管理者グループ、および外部認証と許可を管理するための Cisco ISE メニュー アクセス権限とデータ アクセス権限が存在している必要があります。

（注） これらの新しい外部属性を指定するように既存（システムプリセット）のRBACポリシーを変更することはできません。テンプレートとして使用する既存のポリシーがある場合は、そのポリシーを複製し、名前を変更してから、新しい属性を割り当てる必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [RBACポリシー（RBAC Policy）]** を選択します。

ステップ 2 ルール名、外部管理者グループ、および権限を指定します。

適切な外部管理者グループが正しい管理者ユーザーIDに割り当てられている必要があることに注意してください。管理者が正しい外部管理者グループに関連付けられていることを確認します。

ステップ 3 [保存（Save）] をクリックします。

管理者としてログインした場合、Cisco ISE RBAC ポリシーが管理者 ID を認証できないと、Cisco ISE では、「認証されていない」ことを示すメッセージが表示され、管理者ポータルにアクセスできません。

内部許可を伴う認証に対する外部IDストアを使用した管理アクセスの設定

この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザー名を設定する必要があります。外部 RSA SecurID ID ストアを使用して管理者認証を提供するように Cisco ISE を設定している場合、管理者のクレデンシャル認証が RSA ID ストアによって実行されます。ただし、許可（ポリシー アプリケーション）は、依然として Cisco ISE 内部データベースに従って行われます。また、外部認証と許可とは異なる、留意する必要がある次の2つの重要な要素があります。

- 管理者の特定の外部管理者グループを指定する必要はありません。
- 外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザー名を設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）]** を選択します。

ステップ 2 外部 RSA ID ストアの管理者ユーザー名が Cisco ISE にも存在することを確認します。[パスワード（Password）] の下の [外部（External）] オプションをクリックします。

（注） 外部管理者ユーザー ID のパスワードを指定する必要はなく、特別に設定されている外部管理者グループを関連付けられている RBAC ポリシーに適用する必要もありません。

ステップ 3 [保存（Save）] をクリックします。

外部認証のプロセス フロー

管理者がログインすると、ログインセッションはそのプロセスにおいて次の手順で処理されます。

1. 管理者が RSA SecurID チャレンジを送信します。
2. RSA SecurID は、チャレンジ応答を返します。
3. 管理者は、ユーザー ID とパスワードを入力する場合と同様に、ユーザー名および RSA SecurID チャレンジ応答を Cisco ISE ログイン ダイアログに入力します。
4. 管理者は、指定した ID ストアが外部 RSA SecurID リソースであることを確認します。
5. 管理者は、[ログイン（Login）] をクリックします。

ログイン時、管理者には、RBAC ポリシーで指定されたメニュー アクセス項目とデータ アクセス項目のみが表示されます。

外部 ID ソース

これらのウィンドウでは、Cisco ISE が認証および認可に使用するユーザーデータが含まれている外部 ID ソースを設定および管理することができます。

LDAP ID ソースの設定

次の表では、[LDAP ID ソース（LDAP Identity Sources）] ウィンドウのフィールドについて説明します。これらのフィールドを使用してLDAPインスタンスを作成し、これに接続します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[LDAP]** です。

LDAP 一般設定

以下の表では、[一般（General）] タブのフィールドについて説明します。

表 *56 : LDAP* 一般設定

フィールド名	使用上のガイドライン
名前（**Name**）	LDAP インスタンスの名前を入力します。この値は、サブジェクト DN および属性を取得するために検索で使用されます。この値は string 型で、最大長は 64 文字です。
説明（**Description**）	LDAP インスタンスの説明を入力します。この値は string 型で、最大長は 1024 文字です。
スキーマ（**Schema**）	次の組み込みのスキーマ タイプのいずれかを選択するか、カスタム スキーマを作成できます。 • Active Directory • Sun Directory Server • Novell eDirectory [スキーマ（Schema）] の隣の矢印をクリックすると、スキーマの詳細を表示できます。 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。
（注） 次のフィールドは、カスタム スキーマを選択した場合にのみ編集できます。	

フィールド名	使用上のガイドライン
サブジェクト オブジェクト クラス（**Subject Objectclass**）	サブジェクト DN および属性を取得するために検索で使用する値を入力します。この値は string 型で、最大長は 256 文字です。
サブジェクト名属性（**Subject Name Attribute**）	要求内のユーザー名を含む属性の名前を入力します。この値はstring型で、最大長は 256 文字です。 （注） 構成されているサブジェクト名属性は、外部 ID ストア内のインデックス付きのものである必要があります。
グループ名属性（**Group Name Attribute**）	• CN：共通名に基づいて LDAP ID ストアグループを取得します。 • DN：識別名に基づいて LDAP ID ストアグループを取得します。
証明書属性（**Certificate Attribute**）	証明書定義を含む属性を入力します。証明書ベースの認証の場合、クライアントによって提示された証明書を検証するために、これらの定義が使用されます。
グループ オブジェクト クラス（**Group Objectclass**）	グループとして認識されるオブジェクトを指定するために、検索に使用する値を入力します。この値は string 型で、最大長は 256 文字です。
グループ マップ属性（**Group Map Attribute**）	マッピング情報を含む属性を指定します。この属性は、選択した参照方向に基づいて、ユーザーまたはグループ属性を指定できます。
サブジェクト オブジェクトにグループへの参照が含まれる（**Subject Objects Contain Reference To Groups**）	所属するグループを指定する属性がサブジェクトオブジェクトに含まれている場合は、このオプションをクリックします。
グループ オブジェクトにサブジェクトへの参照が含まれる（**Group Objects Contain Reference To Subjects**）	サブジェクトを指定する属性がグループオブジェクトに含まれている場合は、このオプションをクリックします。この値はデフォルト値です。

フィールド名	使用上のガイドライン
グループ内のサブジェクトをメンバー属性に保存（**Subjects In Groups Are Stored In Member Attribute As**）	[グループオブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）] オプションを有効にした場合に限り使用可能）グループメンバー属性にメンバーが供給される方法を指定します（デフォルトは DN）。
ユーザー情報属性（**User Info Attributes**）	デフォルトでは、事前設定された属性が次の組み込みのスキーマタイプのユーザー情報（名、姓、電子メール、電話、地域など）を収集するために使用されます。 • Active Directory • Sun Directory Server • Novell eDirectory 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。 [スキーマ（Schema）] ドロップダウン リストから [カスタム（Custom）] オプションを選択し、要件に基づいてユーザー情報の属性を編集することもできます。

（注） 構成されているサブジェクト名属性は、外部 ID ストア内のインデックス付きのものである必要があります。

LDAP の接続設定

以下の表では、[接続設定（Connection Settings）] タブのフィールドについて説明します。

表 *57 : LDAP* の接続設定

フィールド名	使用上のガイドライン
セカンダリ サーバーの有効化（**Enable Secondary Server**）	プライマリ LDAP サーバーに障害が発生した場合にバックアップとして使用するセカンダリ LDAP サーバーを有効にする場合は、このオプションをオンにします。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバーの設定パラメータを入力する必要があります。
プライマリ サーバーとセカンダリ サーバー（**Primary and Secondary Servers**）	

フィールド名	使用上のガイドライン
ホスト名/IP（Hostname/IP）	LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。
ポート（Port）	LDAP サーバーがリッスンしている TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバーの管理者からポート番号を取得できます。
各 ISE ノードのサーバーの指定（Specify server for each ISE node）	プライマリおよびセカンダリ LDAP サーバーの hostnames/IP および各 PSN のポートを設定するには、このチェック ボックスをオンにします。 このオプションを有効にすると、導入のすべてのノードを表示するテーブルが表示されます。ノードを選択し、プライマリおよびセカンダリ LDAP サーバーの hostname/IP および選択したノードのポートを設定する必要があります。
アクセス（Access）	**[匿名アクセス（Anonymous Access）]**：LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバーではクライアントが区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへの、クライアント読み取りアクセスが許可されます。認証情報をサーバーに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。 **[認証されたアクセス（Authenticated Access）]**：LDAP ディレクトリの検索が管理者のログイン情報によって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。
管理者 DN（Admin DN）	管理者の DN を入力します。管理者 DN は、[ユーザー ディレクトリ サブツリー（User Directory Subtree）] 下のすべての必要なユーザーの検索およびグループの検索を行う権限を持つ LDAP アカウントです。指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、該当 LDAP サーバーで認証されたユーザーのグループ マッピングは失敗します。
パスワード（Password）	LDAP 管理者アカウントのパスワードを入力します。
セキュアな認証（Secure Authentication）	SSL を使用して Cisco ISE とプライマリ LDAP サーバー間の通信を暗号化する場合にクリックします。[ポート（Port）] フィールドに LDAP サーバーでの SSL に使用されるポート番号が入力されていることを確認します。このオプションを有効にした場合は、ルート CA を選択する必要があります。

フィールド名	使用上のガイドライン
LDAP サーバーのルート CA（LDAP Server Root CA）	ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証を有効にします。
サーバー タイムアウト（Server timeout）	プライマリ LDAP サーバーでの接続または認証が失敗したと判断する前に Cisco ISE がプライマリ LDAP サーバーからの応答を待つ秒数を入力します。有効な値は 1 ～ 99 です。デフォルトは 10 です。
最大管理接続（Max. Admin Connections）	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、ユーザー ディレクトリ サブツリーおよびグループ ディレクトリ サブツリーの下にあるユーザーおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です。デフォルトは 20 です。
N 秒ごとに再接続（Force reconnect every N seconds）	このチェックボックスをオンにし、[秒（Seconds）] フィールドに、サーバーを指定された間隔で LDAP 接続を更新するための適切な値を入力します。有効な範囲は 1 ～ 60 分です。
サーバーへのバインドをテスト（Test Bind To Server）	LDAP サーバーの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバーの詳細を編集して再テストします。
フェールオーバー（Failover）	
常にプライマリ サーバーに最初にアクセスする（Always Access Primary Server First）	Cisco ISE の認証と認可のために常にプライマリ LDAP サーバーに最初にアクセスするように設定するには、このオプションをクリックします。
経過後にプライマリ サーバーにフェールバック（Failback to Primary Server After）	Cisco ISE で接続しようとしたプライマリ LDAP サーバーが到達不可能な場合、Cisco ISE はセカンダリ LDAP サーバーへの接続を試行します。Cisco ISE に再びプライマリ LDAP サーバーを使用するように設定するには、このオプションをクリックし、テキスト ボックスに値を入力します。

[LDAP] の [ディレクトリ構成（Directory Organization）] タブ

次の表では、[ディレクトリ構成（Directory Organization）] タブのフィールドについて説明します。

表 *58 : [LDAP]* の *[*ディレクトリ構成（*Directory Organization*）*]* タブ

フィールド名	使用上のガイドライン
サブジェクト検索ベース（Subject Search Base）	すべてのサブジェクトを含むサブツリーの DN を入力します。次に例を示します。 o=corporation.com サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。
グループ検索ベース（Group Search Base）	すべてのグループを含むサブツリーの DN を入力します。次に例を示します。 ou = 組織ユニット、ou = 次の組織ユニット、o = corporation.com グループを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。
形式での MAC アドレスの検索（Search for MAC Address in Format）	LDAP データベースでの検索に使用する、Cisco ISE の MAC アドレス形式を入力します。内部 ID ソースの MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で供給されます。LDAP データベースの MAC アドレスは、異なる形式で供給できます。ただし、Cisco ISE でホスト ルックアップ要求が受信されると、MAC アドレスは内部形式からこのフィールドで指定した形式に変換されます。 ドロップダウン リストを使用して、特定の形式での MAC アドレスの検索を有効にします。<*format*> は次のいずれかです。 • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 選択する形式は、LDAP サーバーに供給されている MAC アドレスの形式と一致している必要があります。

フィールド名	使用上のガイドライン
サブジェクト名の先頭から最後に出現する区切り文字まで削除（Strip start of subject name up to the last occurrence of the separator）	ユーザー名からドメインプレフィックスを削除するための適切なテキストを入力します。 ユーザー名の中でこのフィールドに指定した区切り文字が Cisco ISE で検出されると、そのユーザー名の初めから区切り文字までのすべての文字が削除されます。ユーザー名に、<start_string> ボックスに指定した文字が複数含まれている場合は、Cisco ISE によって最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザー名が DOMAIN\user1 である場合、Cisco ISE によって user1 が LDAP サーバーに送信されます。 （注） <start_string> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザー名にこれらの文字を使用できません。
最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip end of subject name from the first occurrence of the separator）	ユーザー名からドメインサフィックスを削除するための適切なテキストを入力します。 ユーザー名の中でこのフィールドに指定した区切り文字が Cisco ISE で検出されると、その区切り文字からユーザー名の末尾までのすべての文字が削除されます。ユーザー名に、このフィールドに指定した文字が複数含まれている場合は、Cisco ISE によって最初の区切り文字から文字が削除されます。たとえば、区切り文字が@で、ユーザー名が *user1@domain* であれば、Cisco ISE は *user1* を LDAP サーバーに送信します。 （注） <*end_string*> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザー名にこれらの文字を使用できません。

LDAP グループ設定

表 *59 : LDAP* グループ設定

フィールド名	使用上のガイドライン
追加（**Add**）	[追加（Add）] > [グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）]>[ディレクトリからグループを選択（Select Groups From Directory）] を選択して LDAP ディレクトリからグループを選択します。 グループの追加を選択した場合は、新しいグループの名前を入力します。ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。選択したグループが [グループ（Groups）] ウィンドウに表示されます。

LDAP 属性設定

表 *60 : LDAP* 属性設定

フィールド名	使用上のガイドライン
追加（**Add** ）	[追加（Add）] > [属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）]>[ディレクトリから属性を選択（Select Attributes From Directory）] を選択して LDAP サーバーから属性を選択します。 属性を追加する場合は、新しい属性の名前を入力します。ディレクトリから選択する場合は、ユーザー名を入力し、[属性の取得（Retrieve Attributes）] をクリックして属性を取得します。選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

LDAP 詳細設定

以下の表では、[詳細設定（Advanced Settings）] タブのフィールドについて説明します。

表 *61 : LDAP* 詳細設定

フィールド名	使用上のガイドライン
パスワードの変更を有効にする（**Enable password change**）	デバイス管理に PAP プロトコルを使用し、ネットワーク アクセスに RADIUS EAP-GTC プロトコルを使用している場合に、パスワードが期限切れになるか、またはパスワードがリセットされるときに、ユーザーがパスワードを変更できるようにするには、このチェックボックスをオンにします。サポートされていないプロトコルでは、ユーザー認証が失敗します。このオプションでは、ユーザーが次回のログイン時にパスワードを変更できるようにすることもできます。

関連トピック

LDAP ディレクトリ サービス （1142 ページ）
LDAP ユーザー認証 （1143 ページ）
LDAP ユーザー ルックアップ （1147 ページ）
LDAP ID ソースの追加 （1148 ページ）

RADIUS トークン ID ソースの設定

次の表では、RADIUS 外部 ID ソースを設定し、それに接続するために使用できる [RADIUS トークン ID ソース（RADIUS Token Identity Sources）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）]** です。

表 *62 : RADIUS* トークン *ID* ソースの設定

フィールド名	使用上のガイドライン
名前（**Name**）	RADIUS トークン サーバーの名前を入力します。許容最大文字数は 64 文字です。
説明（**Description**）	RADIUS トークン サーバーの説明を入力します。最大文字数は 1024 です。
SafeWord サーバー（SafeWord Server）	RADIUS ID ソースが SafeWord サーバーである場合はこのチェックボックスをオンにします。
セカンダリ サーバーの有効化（Enable Secondary Server）	プライマリに障害が発生した場合にバックアップとして使用する Cisco ISE のセカンダリ RADIUS トークン サーバーを有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにする場合は、セカンダリ RADIUS トークン サーバーを設定する必要があります。
常にプライマリ サーバーに最初にアクセスする（Always Access Primary Server First）	Cisco ISE が常にプライマリ サーバーに最初にアクセスするように設定するには、このオプションをクリックします。
経過後にプライマリ サーバーにフォールバック（Fallback to Primary Server after）	プライマリ サーバーに到達できない場合に Cisco ISE がセカンダリ RADIUS トークンサーバーを使用して認証できる時間（分単位）を指定するには、このオプションをクリックします。この時間を過ぎると、Cisco ISE はプライマリ サーバーに対する認証を再試行します。
プライマリ サーバー（**Primary Server**）	

フィールド名	使用上のガイドライン
ホスト名/アドレス（Host IP）	プライマリ RADIUS トークン サーバーの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。
共有秘密鍵（Shared Secret）	この接続のプライマリ RADIUS トークン サーバーで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	プライマリ RADIUS トークン サーバーが受信しているポート番号を入力します。
サーバー タイムアウト（Server timeout）	プライマリ サーバーがダウンしていると判断する前に Cisco ISE がプライマリ RADIUS トークン サーバーからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	セカンダリ サーバー（定義されている場合）に移動する前、またはセカンダリ サーバーが定義されていない場合は要求をドロップする前に、Cisco ISE がプライマリ サーバーへの再接続を試行する回数を指定します。
セカンダリ サーバー（Secondary Server）	
ホスト名/アドレス（Host IP）	セカンダリ RADIUS トークン サーバーの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。
共有秘密鍵（Shared Secret）	この接続のセカンダリ RADIUS トークン サーバーで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	セカンダリ RADIUS トークン サーバーが受信しているポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは 1812 です。
サーバー タイムアウト（Server timeout）	セカンダリ サーバーがダウンしていると判断する前に Cisco ISE がセカンダリ RADIUS トークン サーバーからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	要求をドロップする前に Cisco ISE がセカンダリ サーバーへの再接続を試行する回数を指定します。

関連トピック

RADIUS トークン ID ソース （1169 ページ）
RADIUS トークン サーバーの追加 （1174 ページ）

RSA SecurID ID ソースの設定

次の表では、RSA SecurID ID ソースを作成し、それに接続するために使用できる [RSA SecurID ID ソース（RSA SecurID Identity Sources）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID]**。

RSA プロンプトの設定

次の表では、[RSA プロンプト（RSA Prompts）] タブ内のフィールドについて説明します。

表 *63 : RSA* プロンプトの設定

フィールド名	使用上のガイドライン
パスコード プロンプトの入力（Enter Passcode Prompt）	パス コードを取得するテキスト文字列を入力します。
次のトークン コードの入力（Enter Next Token Code）	次のトークンを要求するテキスト文字列を入力します。
PIN タイプの選択（Choose PIN Type）	PIN タイプを要求するテキスト文字列を入力します。
システム PIN の受け入れ（Accept System PIN）	システム生成の PIN を受け付けるテキスト文字列を入力します。
英数字 PIN の入力（Enter Alphanumeric PIN）	英数字 PIN を要求するテキスト文字列を入力します。
数値 PIN の入力（Enter Numeric PIN）	数値 PIN を要求するテキスト文字列を入力します。
PIN の再入力（Re-enter PIN）	ユーザーに PIN の再入力を要求するテキスト文字列を入力します。

RSA メッセージ設定

次の表では、[RSA メッセージ（RSA Messages）] タブ内のフィールドについて説明します。

表 *64 : RSA* メッセージ設定

フィールド名	使用上のガイドライン
システム PIN メッセージの表示（Display System PIN Message）	システム PIN メッセージのラベルにするテキスト文字列を入力します。
システム PIN 通知の表示（Display System PIN Reminder）	ユーザーに新しいPINを覚えるように通知するテキスト文字列を入力します。
数字を入力する必要があるエラー（Must Enter Numeric Error）	PIN には数字のみを入力するようにユーザーに指示するメッセージを入力します。
英数字を入力する必要があるエラー（Must Enter Alpha Error）	PIN には英数字のみを入力するようにユーザーに指示するメッセージを入力します。
PIN 受け入れメッセージ（PIN Accepted Message）	ユーザーのPINがシステムによって受け入れられたときに表示されるメッセージを入力します。
PIN 拒否メッセージ（PIN Rejected Message）	ユーザーのPINがシステムによって拒否されたときに表示されるメッセージを入力します。
ユーザーの PIN が異なるエラー（User Pins Differ Error）	ユーザーが不正なPINを入力したときに表示されるメッセージを入力します。
システム PIN 受け入れメッセージ（System PIN Accepted Message）	ユーザーのPINがシステムによって受け入れられたときに表示されるメッセージを入力します。
不正パスワード長エラー（Bad Password Length Error）	ユーザーが指定した PIN が、PIN 長ポリシーで指定されている範囲に収まらない場合に表示されるメッセージを入力します。

関連トピック

RSA ID ソース （1176 ページ）

Cisco ISE と RSA SecurID サーバーの統合 （1177 ページ）
RSA ID ソースの追加 （1181 ページ）

Cisco ISE ユーザー

このトピックで使用するユーザーという用語は、ネットワークに定期的にアクセスする従業員と請負業者に加え、スポンサーユーザーおよびゲストユーザーを指します。スポンサーユーザーは、ある組織の従業員または請負業者で、スポンサーポータルからゲストユーザーアカウントを作成および管理する人のことです。ゲストユーザーは、一定期間、ある組織のネットワークリソースへのアクセスを必要とする外部ビジターのことです。

Cisco ISE ネットワーク上のリソースとサービスにアクセスするすべてのユーザーのアカウントを作成する必要があります。従業員、請負業者、およびスポンサーユーザーは、管理者ポータルから作成するのが望ましいです。

[有効化日（Date Enabled）] 列（**[設定（Settings）] > [列（Columns）] > [有効化日（Date Enabled）]**）と [パスワードの有効期限までの日数（Days Until Password Expires）] 列（**[設定（Settings）] > [列（Columns）] > [パスワードの有効期限までの日数（Days Until Password Expires）]**）を [ネットワーク アクセス ユーザー（Network Access User ）] ウィンドウ（**[管理（Administration）] > [アイデンティティ管理（Identity Management）] > [アイデンティティ（Identities）] > [ユーザー（Users）]**）の [ネットワーク アクセス ユーザー（Network Access User）] テーブルに追加することを選択できます。この操作は、ネットワーク アクセス ユーザーをパスワードの期限切れに関する情報でソートするのに役立ちます。[有効化日（Date Enabled）] フィールドと [パスワードの有効期限までの日数（Days Until Password Expires）] フィールドは、デフォルトでは追加されません。ウィンドウのカスタマイズオプションを使用して、[ネットワーク アクセス ユーザー（Network Access User）] テーブルにそれらを追加できます。

Cisco ISE リリース 3.3 から、[作成日（Date Created）] 列（**[設定（Settings）] > [列（Columns）] > [作成日（Date Created）]**）と [変更日（Date Modified）] 列（**[設定（Settings）] > [列（Columns）] > [変更日（Date Modified）]**）を [ネットワーク アクセス ユーザー（Network Access User）] テーブルに追加できます。この操作は、[ネットワーク アクセス ユーザー（Network Access User）] ウィンドウ（**[管理（Administration）] > [アイデンティティ管理（Identity Management）] > [アイデンティティ（Identities）] > [ユーザー（Users）]**）で、この情報を使用してネットワークアクセスユーザーをソートするのに役立ちます。[作成日（Date Created）] 列にはいつユーザーが作成されたのかが表示され、[変更日（Date Modified）] 列にはいつユーザーの詳細が最後に変更されたのかが表示されます。これらのフィールドは、デフォルトでは追加されません。[ネットワーク アクセス ユーザー（Network Access Users）] ウィンドウのカスタマイズ オプションを使用して、ユーザーを [ネットワーク アクセス ユーザー（Network Access User）] テーブルに追加できます。これらの列は、昇順および降順でソートすることもできます。

（注） Cisco ISE リリース 3.3 にアップグレードすると、[作成日（Date Created）] フィールドと [変更日（Date Modified）] フィールドが [該当なし（N/A）] とマークされます。したがって、エクスポートされた CSV ファイルでは、これらのユーザーの [作成日（Date Created）] 列と [変更日（Date Modified）]列に空白のセルが含まれます。これらのユーザーの詳細が変更されると、[変更日（Date Modified）] フィールドが更新され、変更日が表示されます。

内部ユーザー（ネットワーク アクセス ユーザーおよび管理ユーザー）のパスワードは、8文字以上にすることを推奨しています。

ユーザー ID

ユーザーIDは、ユーザーに関する情報を保持するコンテナに似ており、ユーザーのネットワーク アクセス クレデンシャルを形成します。各ユーザーの ID はデータにより定義され、ユーザー名、電子メールアドレス、パスワード、アカウントの説明、関連付けられている管理者グループ、ユーザー グループ、ロールなどが含まれます。

ユーザー グループ

ユーザー グループは、特定の一連の Cisco ISE サービスおよび機能へのアクセスを許可する共通の権限セットを共有する個々のユーザーの集合です。

ユーザー ID グループ

ユーザーのグループ ID は、同じグループに属している特定のユーザー グループを識別および説明する要素で構成されています。グループ名は、このグループのメンバーが持っている機能ロールの説明です。グループは、そのグループに属しているユーザーのリストです。

デフォルト ユーザー ID グループ

Cisco ISE には、次の事前定義されたユーザー ID グループが用意されています。

- All_Accounts
- Employee
- Group_Accounts
- GuestType_Contractor
- GuestType_Daily
- GuestType_SocialLogin
- GuestType_Weekly
- Own_Accounts

ユーザー ロール

ユーザー ロールは、ユーザーが Cisco ISE ネットワークで実行できるタスクやアクセスできるサービスを決定する権限セットです。ユーザー ロールは、ユーザー グループに関連付けられています（ネットワーク アクセス ユーザーなど）。

ユーザー アカウントのカスタム属性

Cisco ISE では、ネットワーク アクセス ユーザーと管理者の両方に対して、ユーザー属性に基づいてネットワーク アクセスを制限することができます。Cisco ISE では、一連の事前定義されたユーザー属性が用意されており、カスタム属性を作成することもできます。両方のタイプの属性が認証ポリシーを定義する条件で使用できます。パスワードが指定された基準を満たすように、ユーザー アカウントのパスワード ポリシーも定義できます。

カスタム ユーザー属性

[ユーザーのカスタム属性（User Custom Attributes）] ウィンドウ（[管理（Administration）] > [ID 管理（Identity Management）] > [設定（Settings）] > [ユーザーのカスタム属性（User Custom Attributes）]）で、追加のユーザー アカウント属性を設定できます。このウィンドウに事前に定義済みのユーザー属性のリストを表示することもできます。事前定義済みユーザー属性を編集することはできません。

新しいカスタム属性を追加するには、[ユーザーのカスタム属性（User Custom Attributes）] ペインに必要な詳細を入力します。[ユーザーのカスタム属性（User Custom Attributes）] ウィンドウに追加するカスタム属性とデフォルト値が、ネットワークアクセスユーザー（[管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [追加（Add）] / [編集（Edit）]）または管理者ユーザー（[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）] > [追加（Add）]/[編集（Edit）]）の追加または編集時に表示されます。これらのデフォルト値は、ネットワーク アクセスまたは管理者ユーザーの追加または編集時に変更できます。

ユーザーが [ユーザーのカスタム属性（User Custom Attributes）] ウィンドウで、カスタム属性に対し次のデータ型を選択できます。

- [文字列（String）]：文字列の最大長（文字列属性値の最大許容長）を指定できます。
- [整数（Integer）]：最小値と最大値を設定できます（最小、最大の許容可能な整数値を指定します）。
- [Enum]：各パラメータに次の値を指定できます。
  - 内部値
  - 表示値

  デフォルト パラメータを指定することもできます。ネットワーク アクセスまたは管理者ユーザーの追加または編集時に、[表示（Display）] フィールドに追加する値が表示されます。

- [浮動小数点数（Float）]
- [パスワード（Password）]：最大文字列の長さを指定できます。
- [Long 型（Long）]：最小値と最大値を設定できます。
- [IP]：デフォルトの IPv4 アドレスまたは IPv6 アドレスを指定できます。
- [ブール値（Boolean）]：デフォルト値として True または False を設定できます。
- [日付（Date）]：カレンダーから日付を選択し、デフォルト値として設定できます。日付は yyyy-mm-dd 形式で表示されます。

ネットワーク アクセスまたは管理者ユーザーの追加または編集時、これを必須属性とする場合は、[必須（Mandatory）] チェックボックスをオンにします。カスタム属性のデフォルト値を設定することもできます。

カスタム属性は、認証ポリシーで使用できます。カスタム属性に設定するデータ型と許容範囲は、ポリシー条件のカスタム属性の値に適用されます。

メモ　一部の文字は、属性名と属性値では無効と見なされます。属性名と属性値に次の文字を使用することは制限されています。

- 属性値：@、=、+、または -（これらの文字を属性名または値の先頭に使用しないでください）
- 属性名：^、=、\、"、`、|、：（これらの文字は文字列のどこにも使用しないでください）

ユーザー認証の設定

すべての外部 ID ストアで、ネットワーク アクセス ユーザーが自分のパスワードを変更できるわけではありません。詳細については、各 ID ソースのセクションを参照してください。

ネットワーク使用パスワードルールは、**[管理（Administration）] > [IDの管理（Identity Management）] > [設定（Settings）] > [ユーザー認証設定（User Authentication Settings）]** で設定されます。

[パスワードポリシー（Password Policy）] タブの一部のフィールドに関する追加情報を次のセクションに示します。

- [必須の文字（Required Characters）]：大文字または小文字が必要なユーザーパスワードポリシーを設定するときに、ユーザーの言語でこれらの文字がサポートされていない場合、ユーザーはパスワードを設定できません。UTF-8 文字をサポートするには、次のチェックボックスをオフにします。
  - **小文字の英文字**
  - **大文字の英文字**

- [パスワード変更差分（Password Change Delta）]：現在のパスワードを新しいパスワードに変更するときに変更する必要がある最小文字数を指定します。Cisco ISE 3.2 以降、パスワードの範囲が 1 ～ 20 に変更されました。Cisco ISE では、文字の位置を変更することは変更とみなされません。たとえば、パスワードの差分が 3 で、現在のパスワードが「?Aa1234?」の場合、「?Aa1567?」（「5」、「6」、「7」は 3 つの新しい文字です）は有効な新しいパスワードです。「?Aa1562?」は、「?」、「2」、および「?」の文字が現在のパスワードに含まれているため無効です。文字位置が変更された場合でも、同じ文字が現在のパスワードに含まれているため、「Aa1234??」は無効になります。

  また、パスワード変更差分では、以前の X パスワードが考慮されます。この X は、[パスワードは前のバージョンと異なっている必要があります（Password must be different from the previous versions）] の値です。パスワードの差分が 3 で、パスワードの履歴が 2 である場合は、過去 2 つのパスワードの一部ではない 4 文字を変更する必要があります。

- [辞書の単語（Dictionary words）]：辞書の単語、辞書の単語の逆順での使用、単語内の文字を別の文字で置き換えた単語の使用を制限する場合は、このチェックボックスをオンにします。

  「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば、「Pa$$w0rd」です。

  - [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。
  - [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択（Choose File）] をクリックし、カスタム辞書ファイルを選択します。このテキストファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。

- [パスワードの有効期間（Password Lifetime）]セクションを使用して、パスワードのリセット間隔と通知を更新できます。パスワードの有効期間を設定するには、[パスワードを__日ごとに変更する（有効範囲は1～3650）（Change password every __ days (valid range 1 to 3650)）]チェックボックスをオンにし、入力フィールドに日数を入力します。[ユーザーアカウントを無効にする（Disable User Account）] オプションを選択して、指定された時間内にユーザーがパスワードを変更しなかった場合にユーザーアカウントを無効にすることができます。[次回のログイン時にパスワードの変更が必要（Require password change on next login）] を選択して、次回 Cisco ISE にログインするときにパスワードを変更するようにユーザーに求めます。

  パスワードをリセットするためのリマインダ電子メールを送信するには、[パスワード有効期限の __ 日前にリマインダを表示する（Display Reminder __ Days Before to Password Expiration）] チェックボックスをオンにし、ネットワークアクセスユーザーに設定された電子メールアドレスにリマインダ電子メールを送信するまでの日数を入力します。ネットワークアクセスユーザーを作成するときに、[管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [ネットワークアクセスユーザーの追加（Add Network Access User）] ウィンドウで電子メールアドレスを追加して、パスワードのリセットに関する電子メール通知を送信できます。

（注）

- リマインダ電子メールは、iseadminportal@<ISE-Primary-FQDN> から送信されます。この送信者のアクセスを明示的に許可する必要があります。
- デフォルトでは、リマインダ電子メールには次の内容が含まれています。ネットワークアクセスパスワードは、*<password expiry date and time>* に失効します。「システム管理者に連絡して支援を受けてください（Please contact your system administrator for assistance）」

  Cisco ISE リリース 3.2 以降では、電子メール通知の「システム管理者に連絡して支援を受けてください（Please contact your system administrator for assistance）」の部分の後の電子メールの内容をカスタマイズできます。
- Cisco ISE リリース 3.2 以降では、[パスワードの有効期間（Password Lifetime）] フィールド（**[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [ユーザー認証の設定（User Authentication Settings）] > [パスワードポリシー（Password Policy）] > [パスワードの有効期間（Password Lifetime）]**）で [パスワードの変更（Change Password）] チェックボックスがオンになっていない場合、[ネットワークアクセスユーザー（Network Access Users）] ウィンドウにこのユーザーの [パスワードの有効期間（Password Lifetime）] フィールドが表示されません。

- [不正なログイン試行によるアカウントのロック/一時停止（Lock/Suspend Account with Incorrect Login Attempts）]：このオプションを使用して、ログイン試行が指定した回数失敗した場合にアカウントを一時停止またはロックできます。有効な範囲は、3 ～ 20 です。
- [アカウント無効化ポリシー（Account Disable Policy）]：既存のユーザーアカウントを無効にするタイミングに関するルールを設定できます。詳細については、「グローバルにユーザー アカウントを無効化」を参照してください。

関連トピック

ユーザー アカウントのカスタム属性 （1006 ページ）
ユーザーの追加方法 （1010 ページ）

ユーザーおよび管理者用の自動パスワードの生成

ユーザーおよび管理者の作成ウィンドウで [パスワードの生成（Generate Password）] オプションを使用して、Cisco ISE パスワードポリシーに従うインスタントパスワードを生成します。これにより、ユーザーまたは管理者は設定する安全なパスワードを考えるために時間を費やすことなく、Cisco ISE によって生成されたパスワードを使用することができます。

[パスワードの生成（Generate Password）] オプションは、次のウィンドウで使用できます。

- [管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]。
- [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）]。
- [設定（Settings）] > [アカウント設定（Account Settings）] > [パスワードの変更（Change Password）]。

内部ユーザー操作

ユーザーの追加方法

Cisco ISE では、Cisco ISE ユーザーの属性を表示、作成、編集、複製、削除、ステータス変更、インポート、エクスポート、または検索できます。

Cisco ISE 内部データベースを使用する場合、Cisco ISE ネットワークのリソースまたはサービスへのアクセスを必要とするすべての新規ユーザーのアカウントを作成する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** を選択します。

[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ID（Identities）] > [ユーザー（Users）] ウィンドウにアクセスすることによって、ユーザーを作成することもできます。

ステップ 2 新しいユーザーを作成するには、[追加（Add）]（+）をクリックします。

ステップ 3 すべてのフィールドに値を入力します。

（注） !、%、:、;、[、{、|、}、]、`、?、=、<、>、\、および制御文字をユーザー名に使用しないでください。スペースのみのユーザー名も許可されません。BYOD 用に Cisco ISE 内部認証局（CA）を使用する場合、ここに入力したユーザー名がエンドポイント証明書の共通名として使用されます。Cisco ISE 内部 CA は、「+」または「*」の文字を [共通名（Common Name）] フィールドでサポートしていません。

Cisco ISE リリース 3.2 から、Cisco ISE の内部ユーザーとして、次の操作を実行できます。

1. [アカウント名のエイリアス（Account Name Alias）] フィールドでアカウント名にエイリアスを追加します。アカウント名のエイリアスは、パスワードの有効期限に関する電子メール通知を送信するために使用されます。複数の内部ユーザーが同じ電子メールアドレスを使用している場合、エイリアスを追加すると、電子メールの受信者を区別するのに役立ちます。この通知メールの内容は、[ユーザー認証の設定（User Authentication Settings）] ウィンドウ（**[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [ユーザー認証の設定（User Authentication Settings）]**）で編集できます。
2. [パスワードの有効期間（Password Lifetime）] フィールドを使用して、ユーザーのログインパスワードとイネーブルパスワードの有効期間を入力します。

- [期限あり（With Expiration）] オプションボタンをクリックして、有効期限のあるパスワードを設定します。このフィールドの下に、パスワードの有効期限が切れるまでの残りの日数が表示されます。

  パスワードの有効期限が切れた後にアカウントが自動的に無効化されないようにするには、[ユーザー認証の設定（User Authentication Settings）] ウィンドウで [パスワードの有効期間（Password Lifetime）] の設定を変更します。この設定は、[ユーザー認証の設定（User Authentication Settings）] ウィンドウ（**[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [ユーザー認証の設定（User Authentication Settings）]**）で明示的に [無期限（Never Expires）] に設定されていない限り、イネーブルパスワードにも適用されます。

- [無期限（Never Expires）] オプションボタンをクリックして、ユーザーのログインパスワードとイネーブルパスワードが期限切れにならないようにします。この操作の結果として、グローバルパスワード設定が上書きされ、ユーザーアカウントが無効になることはなくなります。このフィールドは、Cisco ISE 管理ユーザーには適用されません。

  （注）
  - 管理者でもある Cisco ISE 管理ユーザーが [パスワードの有効期間（Password Lifetime）] フィールドを使用することはできません。[ネットワークアクセスユーザー（Network Access User）] テーブルの管理者でもある Cisco ISE ユーザーには、緑色のチェックマーク記号が表示されます。
  - [パスワードの有効期間（Password Lifetime）] フィールドは、[パスワードタイプ（Password Type）] として [内部ユーザー（Internal Users）] が選択されている場合にのみ使用できます。
  - [パスワードの有効期間（Password Lifetime）] フィールド（**[管理（Administration）] > [ID管理（Identity Management）] > [設定（Settings）] > [ユーザー認証の設定（User Authentication Settings）] > [パスワードポリシー（Password Policy）] > [パスワードの有効期間（Password Lifetime）]**）で [パスワードの変更（Change Password）] チェックボックスがオフのままになっている場合、[ネットワークアクセスユーザー（Network Access Users）] ウィンドウの [パスワード（Passwords）] セクションに [パスワードの有効期間（Password Lifetime）] オプションが表示されません。

ステップ 4 [送信（Submit）] をクリックして、Cisco ISE 内部データベースに新しいユーザーを作成します。

Cisco ISE ユーザー データのエクスポート

Cisco ISE 内部データベースからユーザーデータをエクスポートできます。Cisco ISE では、パスワード保護された CSV ファイル形式でユーザーデータをエクスポートできます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** を選択します。

ステップ 2 データをエクスポートするユーザーに対応するチェックボックスをオンにします。

ステップ 3 [選択済みをエクスポート（Export Selected）] をクリックします。

ステップ 4 [キー（Key）] フィールドに、パスワードを暗号化するためのキーを入力します。

ステップ 5 [エクスポート開始（Start Export）] をクリックして、users.csv ファイルを作成します。

ステップ 6 [OK] をクリックして、users.csv ファイルをエクスポートします。

Cisco ISE リリース 3.3 にアップグレードすると、[作成日（Date Created）] フィールドと [変更日（Date Modified）] フィールドが [該当なし（N/A）] とマークされます。したがって、エクスポートされた CSV ファイルでは、これらのユーザーの [作成日（Date Created）] 列と [変更日（Date Modified）] 列に空白のセルが含まれます。

Cisco ISE 内部ユーザーのインポート

新しい内部アカウントを作成するために、CSV ファイルを使用して新しいユーザーデータを Cisco ISE にインポートできます。ユーザーアカウントのインポート中にテンプレートの CSV ファイルをダウンロードに使用できます。スポンサーはスポンサーポータルでユーザーをインポートできます。スポンサーゲストアカウントが使用する情報タイプの設定に関する情報については、スポンサーアカウント作成のためのアカウントコンテンツの設定（867ページ）を参照してください。

（注） CSV ファイルにカスタム属性が含まれている場合、カスタム属性に設定するデータタイプと許容範囲は、インポート時にカスタム属性の値に適用されます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** を選択します。

ステップ 2 [インポート（Import）] をクリックして、カンマ区切りテキスト ファイルからユーザーをインポートします。

カンマ区切りテキストファイルがない場合は、[テンプレートの生成（Generate a Template）] をクリックし、ヘッダー行に値が取り込まれている CSV ファイルを作成します。

ステップ 3 [ファイル（File）] フィールドに、インポートするユーザー名が含まれたファイル名を入力するか、[参照（Browse）] をクリックして、ファイルがある場所に移動します。

ステップ 4 新しいユーザーを作成して既存のユーザーの詳細を更新する場合は、[新しいユーザーの作成と新しいデータでの既存ユーザーの更新（Create new user(s) and update existing user(s) with new data）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

すべてのネットワーク アクセス ユーザーを一度に削除しないことを推奨します。一度に削除すると、特に非常に大規模なデータベースを使用している場合は、CPU スパイクとサービスのクラッシュにつながる場合があるためです。

インポート日は、インポートした Cisco ISE 内部ユーザーの作成日と見なされます。

エンドポイント設定

次の表では、エンドポイントを作成し、エンドポイントにポリシーを割り当てるために使用できる [エンドポイント（Endpoints）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]**。

表 *65 :* エンドポイント設定

フィールド名	使用上のガイドライン
MACアドレス（MAC Address）	エンドポイントを静的に作成するには、MAC アドレスを 16 進数形式で入力します。 MAC アドレスは、Cisco ISE 対応のネットワークに接続するインターフェイスのデバイス ID です。
スタティック割り当て（Static Assignment）	[エンドポイント（Endpoints）] ウィンドウでエンドポイントを静的に作成する場合このチェックボックスをオンにすると、静的割り当てのステータスが static に設定されます。 エンドポイントのスタティック割り当てのステータスを静的から動的に、または動的から静的に切り替えできます。
ポリシー割り当て（Policy Assignment）	（[スタティック割り当て（Static Assignment）] が選択されていない限り、デフォルトで無効）[ポリシー割り当て（Policy Assignment）] ドロップダウンリストから一致するエンドポイントポリシーを選択します。 次のいずれかを実行できます。 • 一致するエンドポイントポリシーを選択しないで、デフォルトのエンドポイントポリシーである不明を使用する場合、スタティック割り当てステータスはエンドポイントに対して動的に設定され、それにより、エンドポイントの動的プロファイリングが可能になります。 • [不明（Unknown）] ではなく、一致するエンドポイントポリシーを選択する場合、スタティック割り当てのステータスはそのエンドポイントに対して静的に設定され、[スタティック割り当て（Static Assignment）] チェックボックスが自動的にオンになります。

フィールド名	使用上のガイドライン
スタティックグループ割り当て（Static Group Assignment）	エンドポイントをIDグループに静的に割り当てる場合はこのチェックボックスをオンにします。 このチェックボックスをオンにした場合、プロファイリングサービスは、前に他のエンドポイントID グループに動的に割り当てられたエンドポイントの次のエンドポイント ポリシーの評価時に、そのエンドポイントID グループを変更しません。 このチェックボックスをオフにした場合、エンドポイントIDグループは、ポリシー設定に基づいてISE プロファイラにより割り当てられたダイナミック グループです。[スタティック グループ割り当て（Static Group Assignment）] オプションを選択しない場合、エンドポイントは、エンドポイント ポリシーの次回評価時に一致するID グループに自動的に割り当てられます。
IDグループ割り当て（Identity Group Assignment）	エンドポイントを割り当てるエンドポイントID グループを選択します。 エンドポイントを静的に作成する場合、またはエンドポイントのエンドポイントポリシーの評価時に [一致するID グループの作成（Create Matching Identity Group）] オプションを使用しない場合は、エンドポイントをID グループに割り当てることができます。 Cisco ISE には、次のシステムによって作成された次のエンドポイントID グループがあります。 • ブロック済みリスト • GuestEndpoints • プロファイル済み • Cisco IP-Phone • ワークステーション • RegisteredDevices • 不明

Cisco ISEによる不要な処理の回避と、潜在的なサービス拒否（DoS）攻撃からの保護のため、RADIUS認証が同じ理由で繰り返し失敗するActive Directoryユーザーエンドポイントは、一定の期間、自動的に拒否されます。

拒否されたエンドポイントのリストを表示するには、[操作（Operations）] > [レポート（Reports）] > [拒否されたエンドポイント（Rejected Endpoints）] の順に選択します。このレポートのデータは、Advantage ライセンスがインストールされている場合にのみ使用および表示可能です。

（注） 次の 2 つのエラーメッセージが表示されて RADIUS 認証に失敗した AD ユーザーエンドポイントは拒否されません。

22063 - WRONG_PASSWORD

24408 - ACTIVE_DIRECTORY_USER_WRONG_PASSWORD

関連トピック

識別されたエンドポイント （1292 ページ）
ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 （1286 ページ）

エンドポイントの LDAP からのインポートの設定

次の表では、LDAP サーバーからのエンドポイントのインポートに使用できる [LDAP からのインポート（Import from LDAP）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]**。

表 *66 :* エンドポイントの、*LDAP* からのインポートの設定

フィールド名	使用上のガイドライン
接続の設定	
ホスト（Host）	LDAP サーバーのホスト名または IP アドレスを入力します。
ポート（Port）	LDAP サーバーのポート番号を入力します。デフォルト ポート 389 を使用して LDAP サーバーからインポートするか、デフォルト ポート 636 を使用して SSL を介して LDAP サーバーからインポートできます。 （注） Cisco ISE では、任意の設定済みポート番号をサポートします。設定済みの値は、LDAP サーバー接続詳細に一致する必要があります。
セキュア接続を有効にする（Enable Secure Connection）	SSL を介して LDAP サーバーからインポートするには、[セキュア接続を有効にする（Enable Secure Connection）] チェックボックスをオンにします。
ルートCA証明書名（Root CA Certificate Name）	ドロップダウン矢印をクリックして、信頼できる CA 証明書を表示します。 ルート CA 証明書名は、LDAP サーバーに接続する場合に必要となる信頼できる CA 証明書を指します。Cisco ISE 内の CA 証明書は、追加（インポート）、編集、削除、およびエクスポートが可能です。

フィールド名	使用上のガイドライン
匿名バインド（Anonymous Bind）	[匿名バインド（Anonymous Bind）] チェックボックスをオンにするか、または slapd.conf コンフィギュレーション ファイルの LDAP 管理者クレデンシャルを入力する必要があります。
管理者DN（Admin DN）	slapd.conf コンフィギュレーション ファイルで LDAP 管理者に設定されている識別名（DN）を入力します。 管理者 DN フォーマット例：cn=Admin, dc=cisco.com, dc=com
パスワード（Password）	LDAP 管理者に設定されたパスワードを slapd.conf コンフィギュレーション ファイルに入力します。
ベースDN（Base DN）	親エントリの認定者名を入力します。 ベース DN フォーマット例：dc=cisco.com, dc=com
クエリ設定	
MACアドレス objectClass（MAC Address objectClass）	MAC アドレスのインポートに使用されるクエリフィルタ（ieee802Device など）を入力します。
MACアドレス属性名（MAC Address Attribute Name）	インポートに対して返される属性名（macAddress など）を入力します。
プロファイル属性名（Profile Attribute Name）	LDAP 属性の名前を入力します。この属性は、LDAP サーバーで定義されている各エンドポイント エントリのポリシー名を保持します。 [プロファイル属性名（Profile Attribute Name）] フィールドを設定する場合は、次の点を考慮してください。 • [プロファイル属性名（Profile Attribute Name）] フィールドでこの LDAP 属性を指定しない場合、またはこの属性を誤って設定した場合、インポート操作時にエンドポイントは [不明（Unknown）] としてマークされ、これらのエンドポイントは一致するエンドポイント プロファイリング ポリシーに個別にプロファイリングされます。 • [プロファイル属性名（Profile Attribute Name）] フィールドで LDAP 属性を設定した場合、その属性値は、エンドポイント ポリシーが Cisco ISE 内の既存のポリシーに一致することを確認するために検証され、エンドポイントがインポートされます。エンドポイント ポリシーが既存のポリシーと一致しない場合、それらのエンドポイントはインポートされません。

フィールド名	使用上のガイドライン
タイムアウト（Time Out）	時間は秒数で入力します。有効な範囲は 1 ～ 60 秒です。

関連トピック

識別されたエンドポイント （1292 ページ）

LDAP サーバーからのエンドポイントのインポート （1290 ページ）

ID グループ操作

ユーザー ID グループの作成

ユーザー ID グループを追加する前に、ユーザー ID グループを作成する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [アイデンティティ グループ（Identity Groups）] > [ユーザー ID グループ（User Identity Groups）] > [追加（Add）]** を選択します。

[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ユーザーIDグループ（User Identity Groups）] > [アイデンティティグループ（Identity Groups）] > [ユーザーIDグループ（User Identity Groups）] > [追加（Add）] ページにアクセスして、ユーザー ID グループを作成することもできます。

ステップ 2 [名前（Name）] フィールドおよび [説明（Description）] フィールドに値を入力します。[名前（Name）] フィールドでサポートされる文字は、スペース、# $ & ‘ ( ) * + - . / @ _ です。

ステップ 3 [送信（Submit）] をクリックします。

関連トピック

ユーザー ID グループ （1005 ページ）

ユーザー ID グループのエクスポート

Cisco ISE では、ローカルに設定されたユーザー ID グループを csv ファイル形式でエクスポートすることができます。

ステップ 1 [管理（Administration）] > [ID 管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザー ID グループ（User Identity Groups）] を選択します。

ステップ 2 エクスポートするユーザー ID グループに対応するチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 **[OK]** をクリックします。

ユーザー ID グループのインポート

Cisco ISE では、ユーザー ID グループを csv ファイル形式でインポートすることができます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザー ID グループ（User Identity Groups）]** を選択します。

ステップ 2 インポートファイルに使用するテンプレートを取得するには、[テンプレートの生成（Generate a Template）] をクリックします。

ステップ 3 [インポート（Import）] をクリックして、カンマ区切りテキストファイルからネットワーク アクセス ユーザーをインポートします。

ステップ 4 新しいユーザー ID グループの追加、および既存のユーザー ID グループの更新の両方を実行する必要がある場合は、[新しいデータで既存のデータを上書き（Overwrite existing data with new data）] チェックボックスをオンにします。

ステップ 5 [インポート（Import）] をクリックします。

ステップ 6 Cisco ISE データベースに変更を保存するには、[保存（Save）] をクリックします。

エンドポイント ID グループの設定

次の表に、エンドポイントグループを作成するために使用できる [エンドポイント ID グループ（Endpoint Identity Groups）] ウィンドウのフィールドを示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** です。

表 *67 :* エンドポイント *ID* グループの設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するエンドポイント ID グループの名前を入力します。
説明（**Description**）	作成するエンドポイント ID グループの説明を入力します。
親グループ（**Parent Group**）	新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを、[親グループ（Parent Group）] ドロップダウンリストから選択します。

関連トピック

識別されたエンドポイントの、エンドポイント ID グループでのグループ化（1295 ページ）
エンドポイント ID グループの作成（1294 ページ）

最大同時セッション数の設定

最適なパフォーマンスを得るために、同時ユーザー セッション数を制限できます。ユーザー レベルまたはグループ レベルで制限を設定できます。最大ユーザー セッションの設定に応じて、セッション カウントはユーザーに適用されます。

ISE ノードごとに各ユーザーの同時セッションの最大数を設定できます。この制限を超えるセッションは拒否されます。

ステップ 1 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [最大セッション数（Max Sessions）] > [ユーザー（User）] を選択します。

ステップ 2 次のいずれかを実行します。

- 各ユーザーに許可される同時セッションの最大数を、[ユーザーごとの最大セッション数（Maximum Sessions per User）] フィールドに入力します。
- ユーザーのセッション数を無制限にするには、[セッション数無制限（Unlimited Sessions）] チェックボックスをオンにします。このオプションは、デフォルトで選択されます。

ステップ 3 [保存（Save）] をクリックします。

セッションの最大数がユーザー レベルとグループ レベルの両方で設定されている場合、小さい方の値が優先されます。たとえば、ユーザーの最大セッション値が 10 に設定されていて、ユーザーが属するグループの最大セッション値が 5 に設定されている場合、ユーザーは最大で 5 つのセッションのみを持つことができます。

（注） 最大同時セッション数は、設定されている PSN によって管理されます。このカウントは PSN 間で同期されません。ユーザーまたはグループごとの最大同時セッション数が設定されている Cisco ISE で認証が行われ、別のプロキシサーバーで許可が行われる場合、最大同時セッション制限は Cisco ISE にのみ適用され、プロキシサーバーには適用されません。

最大同時セッション数はランタイムプロセスで実装され、データはメモリにのみ保存されます。PSN が再起動されると、最大同時セッションカウンタがリセットされます。

最大同時セッション数は、使用されるネットワーク アクセス デバイスに関係なく、ユーザー名に関して大文字と小文字を区別しません（同じ PSN ノードが使用されている場合）。

グループの最大同時セッション数

ID グループの最大同時セッション数を設定できます。

グループ内の少人数のユーザーによってすべてのセッションが使用される場合があります。他のユーザーからの新しいセッションの作成要求は、セッション数がすでに最大設定値に達しているため、拒否されます。Cisco ISE では、グループ内の各ユーザーに最大セッション制限を設定できます。特定の ID グループに所属する各ユーザーは、同じグループの他のユーザーが

開いているセッション数に関係なく、制限以上はセッションを開くことができません。特定のユーザーのセッション制限を計算する場合は、ユーザー1人あたりのグローバルセッション制限、ユーザーが所属する ID グループあたりのセッション制限、グループ内のユーザー 1 人あたりのセッション制限のいずれかの最小設定値が優先されます。

ID グループの同時セッションの最大数を設定するには、次の手順に従います。

ステップ 1 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [最大セッション数（Max Sessions）] > [グループ（Group）] の順に選択します。

設定した ID グループがすべて一覧表示されます。

ステップ 2 編集するグループの横にある [編集（Edit）] アイコンをクリックして、次の値を入力します。

- そのグループに許可される同時セッションの最大数。グループのセッションの最大数を 100 に設定した場合、グループのすべてのメンバーによって確立されたすべてのセッションの総数は 100 を超えることはできません。

  （注） グループ階層に基づいてグループ レベルのセッションが適用されます。

- そのグループの各ユーザーに許可される同時セッションの最大数。このオプションは、グループの最大セッション数を上書きします。

グループの同時セッションの最大数、またはグループ内のユーザーの同時セッションの最大数を [無制限（Unlimited）] に設定するには、[グループの最大セッション数/グループ内のユーザーの最大セッション数（Max Sessions for User in Group/Max Sessions for User in Group）] フィールドを空白にし、ティック アイコンをクリックし、[保存（Save）] をクリックします。デフォルトでは、両方の値が [無制限（Unlimited）] に設定されています。

ステップ 3 [保存（Save）] をクリックします。

カウンタの時間制限の設定

同時ユーザー セッションのタイムアウトを設定できます。

ステップ 1 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [最大セッション数（Max Sessions）] > [カウンタの時間制限（Counter Time Limit）] の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- [無制限（Unlimited）]：セッションのタイムアウトまたは時間制限を設定しない場合は、このチェックボックスをオンにします。
- [経過後にセッションを削除（Delete sessions after）]：日、時間、分の単位で同時セッションのタイムアウト値を入力できます。セッションが時間制限を超えると、Cisco ISE はカウンタからセッションを削除してセッション数を更新するため、新しいセッションが許可されます。ユーザーは、セッションの時間制限を超えた場合、ログアウトされません。

ステップ 3 [保存（Save）] をクリックします。

[RADIUS ライブログ（RADIUS Live Logs）] ウィンドウでセッションカウントをリセットできます。[ID（Identity）]、[ID グループ（Identity Group）]、[サーバー（Server）] 列に表示される [アクション（Actions）] アイコンをクリックして、セッション カウントをリセットします。セッションをリセットすると、セッションはカウンタから削除されます（これにより、新しいセッションが許可されます）。ユーザーのセッションがカウンタから削除されても、ユーザーの接続は切断されません。

アカウントの無効化ポリシー

ユーザーまたは管理者の認証または問い合わせ時に、Cisco ISE は **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザー認証設定（User Authentication Settings）]** でグローバルアカウント無効化ポリシー設定を確認し、その構成に基づいて認証または結果を返します。

Cisco ISE は、次の 3 つのポリシーを確認します。

- [指定した日付（yyyy-mm-dd）を超えたらユーザーアカウントを無効にする（Disable user accounts that exceed a specified date (yyyy-mm-dd)）]：設定された日付にユーザーアカウントを無効にします。ただし、[管理（Administration）] > [IDの管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [アカウント無効化ポリシー（Account Disable Policy）] で設定された個々のネットワーク アクセス ユーザーのアカウント無効化ポリシー設定はグローバル設定よりも優先されます。
- [アカウント作成時または最後の有効化から*n*日後にユーザーアカウントを無効にする（Disable user account after n days of account creation or last enable）]：アカウントの作成またはアカウントが有効になった最後の日から指定した日数後にユーザーアカウントを無効にします。[管理（Administration）] > [IDの管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [ステータス（Status）] でユーザーのステータスを確認できます。
- [非アクティブになってから*n*日後にアカウントを無効にする（Disable accounts after n days of inactivity）]：設定した連続日数、認証されなかった管理者およびユーザーアカウントを無効化します。[非アクティブになってから*n*日後にアカウントを無効にする（disable accounts after n days of inactivity）] オプションは、内部パスワードを使用する Cisco ISE 内部ユーザーにのみ適用されます。

Cisco Secure ACS から Cisco ISE に移行する際、Cisco Secure ACS ではネットワーク アクセス ユーザー用に指定したアカウント無効化ポリシーの設定は Cisco ISE に移行されます。

（注） 任意の [フィルタタイプ（Filter Type）] に設定された収集フィルタは、モニタリングノードに送信される認証 syslog メッセージを除外します。詳細については、『Cisco ISE Administration Guide』の「Maintain and Monitor」の章にある「収集フィルタ」を参照してください。

任意の [属性（Attribute）] および [ファイルタイプ（Filter Type）] に対して収集フィルタ（**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [収集フィルタ（Collection Filter）]**）を設定していて、[非アクティブになってからn日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックス（**[管理（Administration）] > [IDの管理（Identity Management）] > [ユーザー認証の設定（User Authentication Settings）] > [アカウントの無効化ポリシー（Disable Account Policy）]**）をオンにしている場合、認証成功のsyslogメッセージがモニタリングノードにリレーされない結果、アカウントが無効になる可能性があります。

個別のユーザー アカウントの無効化

Cisco ISE では、アカウントの無効日が管理者ユーザーによって指定された日付を超えた場合は、各個人ユーザーのユーザー アカウントを無効にすることができます。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] の順に選択します。

ステップ 2 [追加（Add）] をクリックして新しいユーザーを作成するか、既存のユーザーの横のチェックボックスをオンにして [編集（Edit）] をクリックして既存のユーザーの詳細を編集します。

ステップ 3 [日付を超えたらアカウントを無効化する（Disable account if the date exceeds）] チェックボックスをオンにして、日付を選択します。

このオプションによって、ユーザー レベルで設定した日付を超えたときに、ユーザー アカウントをディセーブルにすることができます。必要に応じて、異なるユーザーに異なる失効日を設定できます。このオプションは、個々のユーザーのグローバル コンフィギュレーションを無効にします。日付には、現在のシステム日付または将来の日付を設定できます。

（注） 現在のシステム日付よりも古い日付は入力できません。

ステップ 4 [送信（Submit）] をクリックして、個々のユーザーのアカウント無効化ポリシーを設定します。

グローバルにユーザー アカウントを無効化

特定の日付、アカウントの作成日または最終アクセス日から数日後、およびアカウントが非アクティブになってから数日後に、ユーザー アカウントを無効にすることができます。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザー認証設定（User Authentication Settings）] > [アカウント無効化ポリシー（Account Disable Policy）] を選択します。

ステップ 2 次のいずれかの操作を実行します。

- [日付を超えるとアカウントを無効にする（Disable account if date exceeds）] チェック ボックスをオンにして、yyyy-mm-dd形式の適切な日付を選択します。このオプションによって、設定した日付の後、ユーザー アカウントを無効にすることができます。ユーザー レベルでの [日付を超えるとアカウントを無効にする（Disable account if date exceeds）] オプションは、このグローバル設定よりも優先されます。
- [アカウントの作成または最後に有効になってから n 日後にアカウントを無効にする（Disable account after n days of account creation or last enable）] チェック ボックスをオンにして、日数を入力します。このオプションは、アカウントの作成日または最終アクセス日が指定した日数を超えたときにユーザー アカウントを無効にします。管理者は、無効化されたユーザー アカウントを手動で有効にでき、有効にすると、日数の数はリセットされます。
- [非アクティブになってから n 日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオンにして、日数を入力します。このオプションは、アカウントが指定した日数非アクティブのときにユーザー アカウントを無効にします。

ステップ 3 [送信（Submit）] をクリックし、グローバル アカウント無効化ポリシーを設定します。

（注） [非アクティブ状態で n 日経過後のアカウントを無効化（Disable account after n days of inactivity）] オプションを使用して、Cisco ISE の非アクティブユーザーを無効にすると、デバイスポータルにログインしたエンドポイントのアクティブな日数はリセットされません。これは、デバイスポータルがプロファイリングの更新やアカウンティング情報を送信しないためです。

内部 ID ソースと外部 ID ソース

アイデンティティ ソースは、ユーザー情報を保存するデータベースです。Cisco ISE は、アイデンティティ ソースのユーザー情報を使用して、認証時にユーザー クレデンシャルを検証します。ユーザー情報には、グループ情報と、そのユーザーに関連付けられているその他の属性が含まれます。ID ソースに対してユーザー情報の追加、編集、および削除を行うことができます。

Cisco ISE では内部 ID ソースと外部 ID ソースがサポートされます。スポンサーとゲストユーザーの認証に両方のソースを使用できます。

内部 ID ソース

Cisco ISE には、ユーザー情報を保存できる内部ユーザー データベースがあります。内部ユーザー データベースのユーザーは、内部ユーザーと呼ばれます。Cisco ISE には、Cisco ISE に接

続するすべてのデバイスおよびエンドポイントに関する情報を格納する内部エンドポイントデータベースもあります。

外部 ID ソース

Cisco ISE では、ユーザー情報を含む外部 ID ソースを設定することができます。Cisco ISE は外部 ID ソースに接続して、認証用のユーザー情報を取得します。外部 ID ソースには、Cisco ISE サーバーおよび証明書認証プロファイルの証明書情報も含まれます。Cisco ISE は外部 ID ソースとの通信に認証プロトコルを使用します。

内部ユーザーのポリシーを設定する際は、次の点に注意してください。

- 内部 ID ストアに対して内部ユーザーを認証するための認証ポリシーを設定します。
- 次のオプションを選択して、内部ユーザー グループの許可ポリシーを設定します。

  `Identitygroup.Name EQUALS User Identity Groups: Group_Name`

次の表に、認証プロトコルおよびサポートされる外部 ID ソースを示します。

表 *68 :* 認証プロトコルとサポートされている外部 *ID* ソース

プロトコル（認証タイプ）	内部データベース	Active Directory	LDAP	RADIUS トークン サーバーまたは RSA	REST	ODBC
EAP-GTC、PAP（プレーン テキスト パスワード）	はい	はい	はい	はい	はい	はい
MS-CHAP パスワード ハッシュ： MSCHAPv1/v2 EAP-MSCHAPv2（PEAP、EAP-FAST、EAP-TTLS、または TEAP の内部メソッドとして） LEAP	はい	はい	いいえ	いいえ	いいえ	はい

プロトコル（認証タイプ）	内部データベース	Active Directory	LDAP	RADIUS トークン サーバーまたは RSA	REST	ODBC
EAP-MD5 CHAP	はい	いいえ	いいえ	いいえ	いいえ	はい
EAP-TLS PEAP-TLS （証明書取得） （注） TLS 認証（EAP-TLS と PEAP-TLS）に ID ソースは必須ではありませんが、許可ポリシー条件のために任意で追加できます。	いいえ	はい	はい	いいえ	いいえ	いいえ

クレデンシャルを保存する方法は、外部データ ソースの接続タイプと使用される機能に応じて異なります。

- Active Directory ドメイン（パッシブ ID 用ではない）に参加する場合、参加に使用されるクレデンシャルは保存されません。Cisco ISE は、AD コンピュータ アカウントが存在しない場合はそのアカウントを作成し、そのアカウントを使用してユーザーを認証します。
- LDAP およびパッシブ ID の場合、外部データ ソースへの接続に使用されるクレデンシャルは、ユーザーの認証にも使用されます。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバーなどの外部 ID ソースに接続して、認証/許可のユーザー情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザー ID を受信して共有できるようにするパッシブ ID サービスを使用するには、その他の パッシブ ID サービス プロバイダー （1094 ページ）を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。
- Active Directory：外部 ID ソースとして Active Directory に接続する場合。詳細については、外部 ID ソースとしての Active Directory （1028 ページ）を参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、LDAP（1142 ページ）を参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバーを追加する場合。詳細については、RADIUS トークン ID ソース （1169 ページ）を参照してください。
- RSA SecurID：RSA SecurID サーバーを追加する場合。詳細については、RSA ID ソース （1176 ページ）を参照してください。
- SAML IDプロバイダー（SAML Id Providers）：Oracle Access Manager などの ID プロバイダー（IdP）を追加する場合。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダー （1185 ページ）を参照してください。
- ソーシャルログイン（Social Login）：Facebook などのソーシャルログインを外部 ID ソースとして追加する場合。詳細については、アカウント登録ゲストのソーシャル ログイン （834 ページ）を参照してください。

外部 ID ストアパスワードに対する内部ユーザーの認証

Cisco ISE では、外部 ID ストア パスワードに対して内部ユーザーを認証できます。Cisco ISE では、[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] ウィンドウから、内部ユーザーのパスワード ID ストアを選択するオプションが提供されます。管理者は、Cisco ISE の外部 ID ソースのリストから ID ストアを選択することができ、[ユーザー（Users）] ウィンドウでユーザーを追加するか、または編集します。内部ユーザーのデフォルトのパスワード ID ストアは内部 ID ストアです。Cisco Secure ACS ユーザーは、Cisco Secure ACS から Cisco ISE への移行中および移行後、同じパスワード ID ストアを維持します。

Cisco ISE はパスワード タイプに対し次の外部 ID ストアをサポートします。

- Active Directory
- LDAP
- ODBC
- RADIUS トークン サーバー
- RSA SecurID サーバー

（注） 現在の設計では、外部 ID ストアに対して認証が行われる場合、内部ユーザー ID グループ名は認証ポリシー内に設定できません。許可に内部ユーザー ID グループを使用するには、内部ユーザー ID ストアに対して認証するように認証ポリシーを設定する必要があります。また、ユーザー設定でパスワードタイプ（内部または外部）を選択する必要があります。

証明書認証プロファイル

プロファイルごとに、プリンシパルユーザー名として使用する証明書フィールドと、証明書のバイナリ比較を行うかどうかを指定する必要があります。

証明書認証プロファイルの追加

Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）証明書ベースの認証方式を使用する場合は、証明書認証プロファイルを作成する必要があります。従来のユーザー名とパスワードの方法で認証する代わりに、Cisco ISE はクライアントから受信した証明書をサーバー内の証明書と比較してユーザーの信頼性を確認します。

始める前に

スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [証明書認証プロファイル（Certificate Authentication Profile）] > [追加（Add）]** を選択します。

ステップ 2 証明書認証プロファイルの名前と説明（任意）を入力します。

ステップ 3 ドロップダウン リストから ID ストアを選択します。

基本証明書のチェックは ID ソースを必要としません。証明書にバイナリ比較チェックが必要な場合は、ID ソースを選択する必要があります。ID ソースとして Active Directory を選択した場合は、サブジェクト名、一般名、およびサブジェクト代替名（すべての値）を使用してユーザーを検索できます。

ステップ 4 [証明書属性（Certificate Attribute）] または [証明書の任意のサブジェクトまたは代替名属性（Any Subject or Alternative Name Attributes in the Certificate）] から ID の使用を選択します。これは、ログで検索のために使用されます。

[証明書の任意のサブジェクトまたは代替名属性（Any Subject or Alternative Name Attributes in the Certificate）] を選択すると、Active Directory UPN がログ用のユーザー名として使用され、証明書のすべてのサブジェクト名および代替名がユーザーの検索に試行されます。このオプションは、ID ソースとして Active Directory を選択した場合にのみ使用できます。

ステップ 5 [クライアント証明書をIDストアの証明書と照合（Match Client Certificate Against Certificate In Identity Store）] の場合に選択します。この場合、ID ソース（LDAP または Active Directory）を選択する必要があります。

[Active Directory] を選択した場合は、ID のあいまいさを解決するためにのみ証明書を照合することを選択できます。

- [なし（Never）]：このオプションは、バイナリ比較を実行しません。
- [ID のあいまいさを解決する目的のみ（Only to resolve identity ambiguity）]：このオプションは、あいまいさが見つかった場合にのみ、クライアント証明書と Active Directory のアカウントの証明書とのバイナリ比較を実行します。たとえば、複数の Active Directory アカウントが証明書の識別名に一致することがあります。
- [常にバイナリ比較を実行する（Always perform binary comparison）]：このオプションは、クライアント証明書と ID ストア（Active Directory または LDAP）内のアカウントの証明書とのバイナリ比較を常に実行します。

ステップ 6 [送信（Submit）] をクリックして、証明書認証プロファイルを追加するか、変更を保存します。

外部 ID ソースとしての Active Directory

Cisco ISE は、ユーザー、マシン、グループ、属性などのリソースにアクセスするために、Microsoft Active Directory を外部 ID ソースとして使用します。Active Directory でのユーザーとマシンの認証では、Active Directory にリストされているユーザーとデバイスに対してのみネットワーク アクセスを許可します。

Cisco ISE ノードが Active Directory に参加すると、そのノードは Active Directory 内で認証されたユーザーグループのメンバーになります。認証されたユーザーグループは、デフォルトで Windows 2000 以前のグループのメンバーです。Windows 2000 以前のグループを無効にするか、Windows 2000 以前のグループから認証されたユーザーを削除すると、認証エラーが発生します。

Windows 2000 以前のグループを無効にしないことを推奨します。ただし、何らかの理由でこのグループを無効にする必要がある場合は、関連するユーザーまたはユーザーのフォルダに対して、AD の Cisco ISE に [リモートアクセス情報の読み取り（Read Remote Access Information）] 権限を付与します。

ISE コミュニティ リソース

ISE Administrative Portal Access with AD Credentials Configuration Example

Active Directory でサポートされる認証プロトコルおよび機能

Active Directory は、いくつかのプロトコルを使用した、ユーザーおよびマシン認証や Active Directory ユーザー パスワード変更などの機能をサポートします。次の表に、Active Directory でサポートされる認証プロトコルおよびそれぞれの機能を示します。

表 *69 : Active Directory* でサポートされる認証プロトコル

認証プロトコル	機能
EAP-FAST およびパスワード ベースの Protected Extensible Authentication Protocol（PEAP）	MS-CHAPv2 および EAP-GTC の内部方式で EAP-FAST と PEAP を使用するパスワード変更機能を備えたユーザーとマシンの認証
Password Authentication Protocol（PAP）	ユーザーおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol Version 1（MS-CHAPv1）	ユーザーおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）	ユーザーおよびマシン認証
Extensible Authentication Protocol-Generic Token Card（EAP-GTC）	ユーザーおよびマシン認証
Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）	• ユーザーおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling-Transport Layer Security（EAP-FAST-TLS）	• ユーザーおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較

認証プロトコル	機能
Protected Extensible Authentication Protocol-Transport Layer Security（PEAP-TLS）	• ユーザーおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Lightweight Extensible Authentication Protocol（LEAP）	ユーザー認証

許可ポリシーで使用する Active Directory 属性およびグループの取得

Cisco ISE は、許可ポリシー ルールで使用するために Active Directory からユーザーまたはマシンの属性およびグループを取得します。これらの属性は Cisco ISE ポリシーで使用され、ユーザーまたはマシンの承認レベルを決定します。Cisco ISE は、認証が成功した後にユーザーおよびマシンの Active Directory 属性を取得します。認証とは別に、許可のために属性を取得することもできます。

Cisco ISE は、外部 ID ストア内のグループを使用してユーザーまたはコンピュータに権限を割り当てることがあります（たとえば、ユーザーをスポンサー グループにマップします）。Active Directory のグループ メンバーシップの次の制限事項に注意してください。

- ポリシー ルール条件は、ユーザーまたはコンピュータのプライマリ グループ、ユーザーまたはコンピュータが直接メンバーであるグループ、または間接的な（ネストされた）グループのいずれかを参照します。
- ユーザーまたはコンピュータのアカウント ドメイン外のドメイン ローカル グループはサポートされません。

（注） Active Directory 属性の値 msRadiusFramedIPAddress を IP アドレスとして使用できます。この IP アドレスは、許可プロファイルのネットワーク アクセス サーバー（NAS）に送信できます。msRADIUSFramedIPAddress 属性は IPv4 アドレスだけをサポートします。ユーザー認証では、ユーザーに対し取得された msRadiusFramedIPAddress 属性値が IP アドレス形式に変換されます。

属性およびグループは、参加ポイントごとに取得され、管理されます。これらは許可ポリシーで使用されます（まず参加ポイントを選択し、次に属性を選択します）。許可範囲ごとに属性またはグループを定義することはできませんが、認証ポリシーに範囲を使用できます。認証ポリシーで範囲を使用する場合、ユーザーは1つの参加ポイントで認証されますが、ユーザーのアカウント ドメインへの信頼できるパスがある別の参加ポイント経由で属性またはグループを

取得することができます。認証ドメインを使用して、1 つの範囲内にある 2 つの参加ポイントで認証ドメインが重複しないようにすることができます。

マルチ参加ポイント設定の許可プロセス時に、Cisco ISE は、特定のユーザーが見つかるまで、認証ポリシーに記載されている順序で参加ポイントを検索します。ユーザーが見つかると、参加ポイント内のユーザーに割り当てられた属性とグループが、認証ポリシーを評価するために使用されます。

複数参加ポイント設定で、各参加ポイントからの同じ ID に対して個別に認証が成功する場合、ID ソース順序 "All_AD_Join_Points" に対して認証が行われると、この認証は失敗します。

複数参加ポイント設定で、各参加ポイントからの同じ ID に対して個別に Active Directory グループ取得が成功する場合、Active Directory グループ取得は次の場合に失敗します。

- 異なる参加ポイントが認証と承認に使用される。
- 認証でバイナリ比較なしの EAP-TLS が使用されていて（[証明書認証プロファイル（Certificate Authentication Profile）] で [クライアント証明書をIDストアの証明書と照合（Match Client Certificate Against Certificate In Identity Store）] が [なし（Never）] に設定されている）、一致認証ルールの前に、異なる参加ポイントを持つ不一致認証ルールがある。
- 認証でバイナリ比較なしの EAP-TLS が使用されていて（[証明書認証プロファイル（Certificate Authentication Profile）] で [クライアント証明書をIDストアの証明書と照合（Match Client Certificate Against Certificate In Identity Store）] が [なし（Never）] に設定されている）、マシンアクセス制限（MAR）が、現在の一致認証ルールの参加ポイントとは別の MAR 期間内の参加ポイントを使用してエンドポイントで有効になっている。

（注） 複数参加ポイント設定で、Active Directory グループ取得は各参加ポイントに対して個別に成功しますが、"All_AD_Join_Points" を含む ID ソース順序で認証ルールが設定されている場合は失敗します。承認と認証に異なる参加ポイントが使用されている場合も、Active Directory グループ取得は失敗します。

使用可能な Active Directory グループの最大数については、Microsoft の制限を参照してください。http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

ルールに、/、!、@、\、#、$、%、^、&、*、(、)、_、+、または~のような特殊文字を使用した Active Directory グループ名が含まれる場合、許可ポリシーは失敗します。

管理者ユーザー名に $ という文字が含まれている場合、Active Directory を介した管理者ユーザーのログインが失敗することがあります。

明示的な UPN の使用

ユーザー情報と Active Directory のユーザー プリンシパル名（UPN）属性を照合する場合の不確実性を減らすため、明示的な UPN を使用するように Active Directory を設定する必要があります。2 人のユーザーが同じ値 *sAMAccountName* を使用した場合、暗示的な UPN を使用すると、あいまいな結果が生成されます。

Active Directory で明示的な UPN を設定するには、[高度な調整（Advanced Tuning）] ページを開いて、属性 *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* を 1 に設定します。

ブール属性のサポート

Cisco ISE は、Active Directory および LDAP ID ストアからのブール属性の取得をサポートしています。

Active Directory または LDAP のディレクトリ属性を設定する際に、ブール属性を設定できます。これらの属性は、Active Directory または LDAP による認証時に取得されます。

ブール属性は、ポリシー ルール条件の設定に使用できます。

ブール属性値は、文字列型として Active Directory または LDAP サーバーから取得されます。Cisco ISE は、次のブール属性値をサポートしています。

ブール属性	サポートされる値
はい（True）	t、T、true、TRUE、True、1
いいえ（False）	f、F、false、FALSE、False、0

（注） 属性置換はブール属性ではサポートされません。

文字列型としてブール属性（たとえば、msTSAllowLogon）を設定すると、Active Directory または LDAP サーバーの属性のブール値は Cisco ISE の文字列属性に設定されます。属性タイプをブール型に変更したり、ブール型として属性を手動で追加できます。

証明書ベース認証の Active Directory 証明書の取得

Cisco ISE では、EAP-TLS プロトコルを使用するユーザーまたはマシン認証のための証明書取得がサポートされています。Active Directory 上のユーザーまたはマシン レコードには、バイナリ データ型の証明書属性が含まれています。この証明書属性に 1 つ以上の証明書を含めることができます。Cisco ISE ではこの属性は userCertificate として識別され、この属性に対して他の名前を設定することはできません。Cisco ISE はこの証明書を取得し、バイナリ比較の実行に使用します。

証明書認証プロファイルは、証明書の取得に使用する Active Directory のユーザーを検索するためにユーザー名を取得するフィールド（たとえば、サブジェクト代替名（SAN）または一般名）を決定します。Cisco ISE は、証明書を取得した後、この証明書とクライアント証明書とのバイナリ比較を実行します。複数の証明書が受信された場合、Cisco ISE は、いずれかが一致するかどうかをチェックするために証明書を比較します。一致が見つかった場合、ユーザーまたはマシン認証に合格します。

Active Directory ユーザー認証プロセス フロー

ユーザーの認証または問い合わせ時に、Cisco ISE は次のことをチェックします。

- MS-CHAP および PAP 認証では、ユーザーが無効かどうか、ロックアウトされているかどうか、期限切れかどうか、またはログイン時間外かどうかを確認します。これらの条件のいずれかが true の場合、認証が失敗します。
- EAP-TLS 認証では、ユーザーが無効かどうか、ロックアウトされているかどうかを確認します。これらの条件のいずれかが一致する場合、認証が失敗します。

Microsoft Entra ID の Cisco ISE への接続

Cisco ISE リリース 3.1 以降、Cisco ISE は Microsoft Entra ID によるエンドポイントの認証と承認をサポートします。Cisco ISE リリース 3.1 は、リソース オーナー パスワード クレデンシャル（ROPC）方式のみをサポートします。Cisco ISE リリース 3.2 は、ROPC フローに加えて、EAP-TLS および TEAP 方式をサポートします。

Entra ID でユーザーを認証するためのリソース オーナー パスワード クレデンシャル フローの設定

⚠

注意 Cisco ISE のリソースオーナーのパスワードクレデンシャル（ROPC）フローは、制御された導入機能です。この機能を実稼働環境で使用する前に、テスト環境で十分にテストすることを推奨します。

リソースオーナーのパスワードクレデンシャル（ROPC）は、クラウドベースの ID プロバイダーとのネットワークで Cisco ISE が認証と許可を実行できるようにする OAuth 2.0 付与タイプです。

ROPC フローを使用して、Cisco ISE はクラウドベースの ID ソースでユーザーのログイン情報を検証します。ROPC フローは、プレーンテキスト認証プロトコルをサポートしています。

Cisco ISE は現在、ROPC フローを介して Microsoft Entra ID をサポートしています。

Microsoft Entra ID でのリソース オーナー パスワード クレデンシャル フロー用アプリケーションの設定

ステップ 1 Azure ポータルにログインします。

ステップ 2 上部のナビゲーションバーで [ディレクトリ + アプリケーション（Directory+Application）] フィルタアイコンをクリックします。ROPC 対応アプリケーションの追加が必要な Microsoft Entra ID テナントを選択します。

ステップ 3 検索バーを使用し、[アプリケーションの登録（App Registrations）] を見つけて選択します。

ステップ 4 [+ 新規登録（+ New Registration）] をクリックします。

ステップ 5 表示される [アプリケーションの登録（Register an Application）] ウィンドウで、[名前（Name）] フィールドにこのアプリケーションのわかりやすい名前を入力します。

ステップ 6 [サポートされているアカウントタイプ（Supported account types）] 領域で、[この組織ディレクトリ内のみのアカウント（Accounts in this organization directory only）] をクリックします。

ステップ 7 [登録（Register）] をクリックします。

ステップ 8 表示される新しいウィンドウで、左側のメニューペインから [証明書と秘密（Certificates & Secrets）] をクリックします。

ステップ 9 [クライアントの秘密（Client Secrets）] 領域で、[+ 新しいクライアントの秘密（+ New Client Secret）] をクリックします。

ステップ 10 表示される [クライアントの秘密の追加（Add a Client Secret）] ダイアログボックスで、[説明（Description）] フィールドに説明を入力します。

ステップ 11 [有効期限（Expiry）] 領域で、[なし（Never）] をクリックします。

ステップ 12 [追加（Add）] をクリックします。

ステップ 13 [クリップボードにコピー（Copy to Clipboard）] アイコンをクリックして共有秘密をコピーします。この値は、Cisco ISE で ROPC フローを設定するときに必要になります。

ステップ 14 左側のメニューペインで [概要（Overview）] をクリックし、ROPC フローの設定時に Cisco ISE で使用する次の値をコピーします。

- アプリケーション（クライアント）ID。
- ディレクトリ（テナント）ID。

ステップ 15 このアプリケーションの ROPC フローを有効にするには、左側のメニューペインで [認証（Authentication）] をクリックします。[高度な設定（Advanced Settings）] 領域で、トグルボタンが [はい（Yes）] に設定されていることを確認します。

このアプリケーションを EAP-TLS または TEAP ワークフローのみに使用する場合は、手順 15 を実行しないでください。

ステップ 16 グループ要求をアプリケーションに追加するには、左側のメニューペインで [トークンの設定（Token Configuration）] をクリックします。

ステップ 17 [+ グループ要求の追加（+ Add Groups Claim）] をクリックします。

ステップ 18 [グループ要求の編集（Edit Groups Claim）] ダイアログボックスで、[セキュリティグループ（Security groups）] チェックボックスをオンにします。

ステップ 19 [保存（Save）]をクリックします。

ステップ 20 API の使用を有効にするには、左側のメニューペインで [API のアクセス権（API Permissions）] をクリックします。

ステップ 21 [+ アクセス権の追加（+ Add A Permission）] をクリックします。

ステップ 22 [Microsoft の API（Microsoft APIs）] 領域で、[Microsoft Graph] をクリックします。

ステップ 23 [アプリケーションのアクセス権（Application Permissions）] をクリックします。

ステップ 24 [グループ（Group）] ドロップダウン領域で、[Group.Read.All] チェックボックスをオンにします。

このアプリケーションを EAP-TLS または TEAP ワークフローに使用するには、[User.Read] および [User.Read.All] チェックボックスもオンにします。

ステップ 25 [権限の追加（Add Permissions）] をクリックします。

ステップ 26 [次のユーザーに管理者の合意を付与（Grant Admin Consent for <user>）] をクリックし、[はい（Yes）] をクリックします。

Cisco ISE でのリソースオーナーパスワードクレデンシャルフローの設定

始める前に

Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します。**[システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）]**。[DigiCert Global Root G2] が信頼できる証明書のリストに表示されているかどうかを確認します。

この証明書が信頼できる証明書ストアにない場合は、PEM 形式のパブリックルート証明書 DigiCert Global Root G2 をCisco ISE の信頼できる証明書ストアにインポートします。

https://www.digicert.com/kb/digicert-root-certificates.htm を参照してください。

ステップ 1 Cisco ISE の GUIで、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [設定（Settings）] > [REST IDストア設定（REST ID Store Settings）]**。

ステップ 2 [有効（Enabled）] をクリックし、次に [送信（Submit）] をクリックします。

サービスが有効になっている間は「**サーバーを起動しています。これには数分かかる場合があります。（The service is starting. This may take a few minutes.）**」というメッセージがウィンドウに表示されます。「サービスは有効になっています（The service is enabled）」というメッセージがウィンドウに表示され、サービスがアクティブであることを示します。

ステップ 3 Cisco ISE の GUIで、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [ID 管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [REST]** を選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 表示される新しいウィンドウの [全般（General）] タブで、[名前（Name）] フィールドに値を入力します。

ステップ 6 [REST ID プロバイダー（REST Identity Provider）] ドロップダウンリストから、設定する ID ソースを選択します。

ステップ 7 前のタスクで Microsoft Entra ID を設定するときに保存した情報から、[クライアントID（Client ID）]、[クライアントシークレット（Client Secret）]、および [テナントID（Tenant ID）] の各フィールドに必要な値を入力します。

ステップ 8 [接続のテスト（Test Connection）] をクリックして、Cisco ISE が選択した ID ソースに接続できるかどうかを確認します。

ステップ 9 [送信（Submit）] をクリックします。

ステップ 10 REST ID ストアグループを追加するには、[グループ（Groups）] タブを選択し、[追加（Add）] をクリックします。

[グループの取得（Retrieve Groups）] をクリックして、接続された ID ソースからユーザーグループをインポートします。選択するグループの隣にあるチェックボックスをオンにし、[保存（Save）] をクリックします。必要に応じて、すべてのグループを選択することもできます。選択したグループが[グループ（Groups）] タブに一覧表示されます。

フィルタオプションを使用して結果をフィルタ処理できます。

ユーザーグループを削除するには、削除するグループの隣にあるチェックボックスをオンにして、[削除（Delete）] をクリックします。

ステップ 11 （オプション）[ユーザー名サフィックス（Username Suffix）] フィールドに値を入力し、Microsoft Entra ID テナントのユーザーをユーザー名で認証します。

たとえば、ユーザーの Azure Active Directory ユーザープライベート名（UPN）が *example@myTest.onMicrosoft.com* の場合、サフィックスが区切り文字で、ドメイン名は *@myTest.onMicrosoft.com* です。

ステップ 12 [送信（Submit）] をクリックします。

Microsoft Entra ID を使用した EAP-TLS および TEAP 認証

Cisco ISE は、証明書ベースの認証と Microsoft Entra ID 認証をサポートしています。証明書ベースの認証は、内部方式として EAP-TLS または EAP-TLS を使用した TEAP のいずれかです。次に、Microsoft Entra ID から属性を選択し、それらを Cisco ISE ディクショナリに追加できます。これらの属性は、認証に使用できます。

ステップ 1 タスク「Microsoft Entra ID でのリソース オーナー パスワード クレデンシャル フロー用アプリケーションの設定（1033 ページ）」の手順に従って、Cisco ISE 用の Microsoft Entra ID アプリケーションを設定します。手順 15 は実行しないでください。

ステップ 2 タスク「Cisco ISE でのリソースオーナーパスワードクレデンシャルフローの設定（1035 ページ）」の手順に従って、Microsoft Entra ID アプリケーションを Cisco ISE に接続します。

ステップ 3 Microsoft Entra ID 統合のために Cisco ISE ディクショナリに追加する属性を選択するには、[ユーザー属性（User attributes）] タブ（**[管理（Administration）] > [ID管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [REST]**）に移動します。REST ID ソース統合のリストから、属性を選択する統合をクリックします。

ステップ 4 [ユーザー属性（User attributes）] タブで、[追加（Add）] をクリックします。Cisco ISE ディクショナリに追加する属性の横にあるチェックボックスをオンにします。その後、ポリシーセットの作成でディクショナリの属性を使用できます。

Active Directory マルチドメイン フォレストのサポート

Cisco ISE では、マルチドメイン フォレストの Active Directory がサポートされます。各フォレスト内で、Cisco ISE は単一のドメインに接続しますが、Cisco ISE が接続されているドメインと他のドメイン間に信頼関係が確立されている場合は、Active Directory フォレストの他のドメインからリソースにアクセスできます。

Active Directory サービスをサポートする Windows サーバー オペレーティング システムのリストについては、『Release Notes for Cisco Identity Services Engine』を参照してください。

（注） Cisco ISE は、ネットワーク アドレス トランスレータの背後にあり、ネットワーク アドレス変換（NAT）アドレスを持つ Microsoft Active Directory サーバーをサポートしません。

Active Directory と Cisco ISE の統合の前提条件

この項では、Cisco ISE と統合する Active Directory を設定するために必要な手動での作業手順について説明します。ただしほとんどの場合、Cisco ISE が Active Directory を自動的に設定するようにできます。次に、Cisco ISE と Active Directory を統合するための前提条件を示します。

- AD ドメイン設定の変更に必要な Active Directory ドメイン管理者クレデンシャルがあることを確認します。
- Cisco ISE でのネットワーク管理者またはシステム管理者の権限があることを確認します。
- Cisco ISE サーバーと Active Directory 間の時間を同期するために Network Time Protocol（NTP）サーバー設定を使用します。Cisco ISE CLI で NTP を設定できます。
- Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。特定の参加ポイントから他のドメインを照会する場合は、参加ポイントと、アクセスする必要があるユーザー情報およびマシン情報があるその他のドメインの間に信頼関係が確立されていることを確認します。信頼関係が確立されていない場合は、信頼できないドメインへの別の参加ポイントを作成する必要があります。信頼関係の確立の詳細については、Microsoft Active Directory のドキュメントを参照してください。
- Cisco ISE の参加先ドメインでは、少なくとも 1 つのグローバル カタログ サーバーが動作し、Cisco ISE からアクセス可能である必要があります。

さまざまな操作の実行に必要な Active Directory アカウント権限

参加操作	脱退処理	Cisco ISE マシン アカウント
参加操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシンアカウントがあるかどうかの確認） • ドメインに Cisco ISE マシンアカウントを作成する権限（マシンアカウントが存在しない場合） • 新しいマシンアカウントに属性を設定する権限（Cisco ISE マシンアカウント パスワード、SPN、dnsHostname など）	脱退操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシンアカウントがあるかどうかの確認） • ドメインから Cisco ISE マシンアカウントを削除する権限 強制脱退（パスワードなしの脱退）を実行する場合、ドメインからマシンアカウントは削除されません。	Active Directory 接続と通信する Cisco ISE マシン アカウントには、次の権限が必要です。 • パスワードを変更する権限 • 認証されるユーザーおよびマシンに対応するユーザーおよびマシンオブジェクトを読み取る権限 • 情報を取得するために Active Directory をクエリする権限（信頼ドメイン、代替の UPN サフィックスなど） • tokenGroups 属性を読み取る権限 Active Directory でマシン アカウントを事前に作成できます。SAM の名前が Cisco ISE アプライアンスのホスト名と一致する場合は、参加操作中に検索して再利用します。 複数の参加操作が実行される場合、参加ごとに複数のマシンアカウントが Cisco ISE 内で保持されます。

（注） 参加操作または脱退操作に使用するクレデンシャルは Cisco ISE に保存されません。新規作成された Cisco ISE マシンアカウントのログイン情報のみが保存されます。

Microsoft Active Directory のセキュリティポリシー「**ネットワーク アクセス：SAM へのリモートの呼び出しを許可するクライアントを制限する**」が改訂されました。このため、Cisco ISE は 15 日ごとにマシンアカウントのパスワードを更新できない場合があります。マシンアカウントのパスワードが更新されない場合、Cisco ISE は Microsoft Active Directory を介してユーザーを認証しません。このイベントを通知するために、Cisco ISE ダッシュボードに [AD：ISE アカウントパスワードの更新に失敗（AD: ISE account password update failed）] アラームが表示されます。

（注） この問題は、Windows Server 2016 Active Directory 以降および Windows 10 バージョン 1607 の制限により発生します。この制限を克服するには、Windows Server 2016 Active Directory 以降または Windows 10 バージョン 1607 を Cisco ISE と統合する場合、レジストリ：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam のレジストリ値を non-zero から空白に設定して、すべてにアクセスを提供する必要があります。これにより、Cisco ISE がそのマシンのアカウントパスワードを更新できるようになります。

セキュリティポリシーにより、ユーザーはローカル セキュリティ アカウント マネージャ（SAM）データベース内と Microsoft Active Directory 内のユーザーとグループを列挙できます。Cisco ISE がマシンアカウントのパスワードを更新できるようにするには、Microsoft Active Directory の設定が正しいことを確認します。影響を受ける Windows オペレーティングシステムと Windows Server のバージョン、ネットワークにおけるこのセキュリティポリシーの意味、必要な変更の詳細については、以下を参照してください。

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

通信用に開放するネットワークポート

プロトコル	ポート（リモート ローカル）	ターゲット	認証	注記
DNS（TCP/UDP）	49152 以上の乱数	DNS サーバー/AD ドメイン コントローラ	なし	—
MSRPC	445	ドメイン コントローラ	あり	—
Kerberos（TCP/UDP）	88	ドメイン コントローラ	あり（Kerberos）	MS AD/KDC
LDAP（TCP/UDP）	389	ドメイン コントローラ	あり	—
LDAP（GC）	3268	グローバル カタログ サーバー	あり	—
NTP	123	NTP サーバー/ドメイン コントローラ	なし	—
IPC	80	展開内の他の ISE ノード	あり（RBAC クレデンシャルを使用）	—

DNS サーバー

DNS サーバーを設定する場合は、次の処理を実行します。

- Cisco ISE に設定されている DNS サーバーで、使用するドメインのすべての正引きおよび逆引き DNS クエリを解決できるようにする必要があります。
- DNS 再帰によって遅延が発生してパフォーマンスが重大な悪影響を受ける可能性があるので、権威 DNS サーバーで Active Directory レコードを解決することをお勧めします。
- すべての DNS サーバーで、追加サイト情報の有無に関係なく、DC、GC、および KDC の SRV クエリに回答できるようにする必要があります。
- パフォーマンスを向上させるために、SRV 応答にサーバー IP アドレスを追加することを推奨します。
- パブリック インターネットでクエリを実行する DNS サーバーを使用しないでください。不明な名前を解決する必要がある場合に、ネットワークの情報が漏洩する可能性があります。

外部 ID ソースとしての Active Directory の設定

Easy Connect や PassiveID ワーク センターなどの機能を設定する際に、Active Directory を外部 ID ソースとして設定します。これらの機能の詳細については、Easy Connect （1077 ページ）と PassiveID ワーク センター （1083 ページ）を参照してください。

外部 ID ソースとして Active Directory を設定する前に、次のことを確認します。

- Microsoft Active Directory サーバーがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないこと。
- 参加操作用の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更（Change Password on Next Login）] を使用して設定されていないこと。
- ISE のスーパー管理者またはシステム管理者の権限があること。

（注） Cisco ISE が Active Directory に接続されているときに操作に関する問題がある場合は、**[操作（Operations）] > [レポート（Reports）]** で AD コネクタ操作レポートを参照してください。

外部 ID ソースとして Active Directory を設定するには、次のタスクを実行する必要があります。

1. Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （1041 ページ）
2. 認証ドメインの設定 （1048 ページ）
3. Active Directory ユーザー グループの設定 （1049 ページ）

4. Active Directory ユーザーとマシンの属性の設定 （1050 ページ）
5. （省略可）パスワード変更、マシン認証、およびマシンアクセス制限の設定の変更 （1050 ページ）

Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加

始める前に

Cisco ISE ノードが、NTP サーバー、DNS サーバー、ドメインコントローラ、グローバルカタログサーバーが配置されているネットワークと通信できることを確認します。ドメイン診断ツールを実行して、これらのパラメータをチェックできます。

Active Directory と、パッシブ ID ワーク センターのエージェント、syslog、SPAN、およびエンドポイントの各プローブを使用するには、参加ポイントを作成する必要があります。

Active Directory と統合する際に IPv6 を使用する場合は、関連する ISE ノードで IPv6 アドレスが設定されていることを確認する必要があります。

Google Chrome ブラウザを使用し、広告ブロックソフトウェアを有効にしている場合は、広告ブロッカーを無効にする必要があります。このタスクには、広告ブロッカーの影響を受ける Cisco ISE GUI 要素が含まれています。または、Google Chrome シークレットブラウザでこのタスクを実行できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [追加（Add）] をクリックして、[Active Directory 参加ポイント名（Active Directory Join Point Name）] の設定のドメイン名と ID ストア名を入力します。

ステップ 3 [送信（Submit）] をクリックします。

新しく作成された参加ポイントをドメインに参加させるかどうかを確認するポップアップ ウィンドウが表示されます。すぐに参加させる場合は [はい（Yes）] をクリックします。

[いいえ（No）] をクリックした場合、設定を保存すると、Active Directory ドメインの設定が（プライマリおよびセカンダリのポリシー サービス ノードに）グローバルに保存されますが、いずれの Cisco ISE ノードもまだドメインに参加しません。

ステップ 4 作成した新しい Active Directory 参加ポイントの横にあるチェックボックスをオンにして [編集（Edit）] をクリックするか、または左側のナビゲーションウィンドウから新しい Active Directory 参加ポイントをクリックします。展開の参加/脱退テーブルに、すべての Cisco ISE ノード、ノードのロール、およびそのステータスが表示されます。

ステップ 5 参加ポイントがステップ 3 の間にドメインに参加しなかった場合は、関連する Cisco ISE ノードの横にあるチェックボックスをオンにし、[参加（Join）] をクリックして Active Directory ドメインに Cisco ISE ノードを参加させます。

設定を保存した場合も、これを明示的に実行する必要があります。1 回の操作で複数の Cisco ISE ノードをドメインに参加させるには、使用するアカウントのユーザー名とパスワードがすべての参加操作で同じで

ある必要があります。各 Cisco ISE ノードを追加するために異なるユーザー名とパスワードが必要な場合は、Cisco ISE ノードごとに参加操作を個別に実行する必要があります。

ステップ 6 [ドメインへの参加（Join Domain）] ダイアログボックスで Active Directory のユーザー名とパスワードを入力します。

[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメインコントローラ（DC）に使用されます。

参加操作に使用するユーザーは、ドメイン自体に存在する必要があります。ユーザーが異なるドメインまたはサブドメインに存在する場合、ユーザー名は jdoe@acme.com のように、UPN 表記で表記する必要があります。

ステップ 7 （任意） [組織ユニットの指定（Specify Organizational Unit）] チェックボックスをオンにします。

このチェックボックスは、Cisco ISE ノードのマシンアカウントを CN=Computers,DC=someDomain,DC=someTLD 以外の特定の組織ユニットに配置する場合に、オンにする必要があります。Cisco ISE は、指定された組織ユニットの下にマシンアカウントを作成するか、またはマシン アカウントがすでにある場合は、この場所に移動します。組織ユニットが指定されない場合、Cisco ISE はデフォルトの場所を使用します。値は完全識別名（DN）形式で指定する必要があります。構文は、Microsoft のガイドラインに準拠する必要があります。特別な予約文字（/'+,;=<> など）、改行、スペース、およびキャリッジ リターンは、バックスラッシュ（\）によってエスケープする必要があります。たとえば、OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ や Workstations,DC=someDomain,DC=someTLD のようにします。マシンアカウントがすでに作成されている場合、このチェックボックスをオンにする必要はありません。Active Directory ドメインに参加したマシン アカウントのロケーションを後で変更することもできます。

ステップ 8 [OK] をクリックします。

Active Directory ドメインに参加する複数のノードを選択できます。

参加操作に失敗した場合、失敗メッセージが表示されます。各ノードの失敗メッセージをクリックして、そのノードの詳細なログを表示します。

参加ポイントを設定する際は、次の点に注意してください。

- 複数の参加ポイントを使用する場合、代替 UPN サフィックスが単一の参加ポイントまたはドメインに対してのみ設定されている場合、アイデンティティルックアップはその参加ポイントまたはドメインでのみ実行されます。このような場合、認証が失敗する可能性があります。回避策として、すべての参加ポイントまたはドメインに代替 UPN サフィックスを設定できます。
- ISE には最大 200 のドメイン コントローラのみを追加できます。制限を超えると、「エラー発生 <DC FQDN> - DC の数が最大許容数である 200 を超えています（Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200）」というエラーが表示されます。展開用のドメインコントローラのテスト済みスケール制限の詳細については、『Performance and Scalability Guide for Cisco Identity Services Engine』を参照してください。

- 参加が完了すると、Cisco ISE によりその AD グループと対応するセキュリティ識別子（SID）が更新されます。Cisco ISE は自動的に SID の更新プロセスを開始します。このプロセスを完了できるようにする必要があります。
- DNS サービス（SRV）レコードが欠落している（参加しようとしているドメインに対し、ドメインコントローラが SRV レコードをアドバタイズしない）場合は、Active Directory ドメインに Cisco ISE を参加させることができない可能性があります。
- （[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory] > [高度なツール（Advanced Tools）] > [高度なチューニング（Advanced Tuning）] を選択して）AD コネクタを再起動することをお勧めします。これにより、AD キャッシュが最新の更新内容で更新されます。
- 作成される AD マシンアカウント名は、ホスト名が 15 文字を超える場合、Cisco ISE ホスト名と一致しません。この場合、マシンアカウント名は次の形式で作成されます。

  first_8_characters_of(hostname) + "-" + 6 random characters + "$"

  マシンアカウント名とホスト名を一致させるには、ホスト名を 15 文字以下にする必要があります。
- Cisco ISE および AD の参加に使用された AD クレデンシャルが無効になった場合でも、Cisco ISE と AD 間の参加ポイントは変更されません。

ドメイン コントローラの追加

ステップ 1 **[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）]** を選択し、左側のパネルから **[Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 （注） パッシブ ID サービスの新しいドメイン コントローラ（DC）を追加するには、その DC のログイン クレデンシャルが必要です。

[PassiveID] タブに移動し、[DC の追加（Add DCs）] をクリックします。

ステップ 4 モニター対象として参加ポイントに追加するドメイン コントローラの隣にあるチェックボックスをオンにし、[OK] をクリックします。
ドメイン コントローラが [PassiveID] タブの [ドメイン コントローラ（Domain Controllers）] リストに表示されます。

ステップ 5 ドメイン コントローラを設定します。

a) ドメイン コントローラをオンにし、[編集（Edit）] をクリックします。[アイテムの編集（Edit Item）] 画面が表示されます。

b) 必要に応じて、各種ドメイン コントローラ フィールドを編集します。

DC フェールオーバー メカニズムは DC 優先順位リストに基づいて管理されます。このリストは、フェールオーバーの発生時に DC が選択される順序を決定します。ある DC がオフラインであるか、何らかのエラーのため到達不能な場合には、優先順位リストにおける優先順位が下がります。DC がオンラインに戻ると、優先順位リストにおけるその優先順位が適宜調整されます（上がります）。

Cisco ISE リリース 3.4 以降では、Cisco ISE の内部優先順位リストをオーバーライドし、フェールオーバー時に次に優先される DC が選択される順序を決定することができます。詳細については、「優先順位によるドメインコントローラの選択の強制（1065 ページ）」を参照してください。

パッシブ ID の MSRPC プロトコル

Cisco ISE リリース 3.0 以降では、パッシブ ID に MS-Eventing API または Microsoft Remote Procedure Call（MSRPC）プロトコルを使用できます。MSRPC プロトコルは、ノード通信を確立し、Cisco ISE のノード間のハートビートをモニターするために使用されます。

MSRPC プロトコルは、Cisco ISE または Cisco ISE-PIC が複数のドメインコントローラからイベントを収集またはモニターするときに、信頼性の高いメカニズムを促進します。また、ドメインコントローラのユーザーログオンイベントの遅延も減少します。

Cisco ISE 3.0 以降では、MSRPC がデフォルトのプロトコルです。プライマリエージェントがインストールされたサーバーで障害が発生した場合にセカンダリエージェントがアクティブになり、ドメインコントローラをモニターできるように、プライマリエージェントとセカンダリエージェントで MSPRC のハイアベイラビリティ機能を有効にすることを推奨します。

また、エージェントの作成時に MSPRC のスタンドアロンオプションを使用することもできます。ただし、エージェントに障害が発生し、ドメイン コントローラ イベントをモニターできない場合、スタンドアロンエージェントはセカンダリエージェントによってバックアップされません。

Cisco ISE 2.x から 3.0 バージョンへのアップグレード中に、メンバーサーバーが既存のエージェントで更新された場合、エージェントバージョンは [エージェント（Agents）] ウィンドウの [バージョン（Version）] 列に 2.0.0.1 と表示されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [パッシブ ID（Passive ID）] > [プロバイダー（Providers）] > [エージェント（Agents）]**。

エージェントがドメインコントローラに直接インストールされている場合は、モニタリング ユーザーがイベント ログ リーダー グループのメンバーであることを確認してください。

エージェントが AD ドメインメンバーサーバーにインストールされている場合は、次の手順を実行する必要があります。

- モニタリングユーザーがイベント ログ リーダー グループのメンバーであることを確認します。
- 高可用性を設定した場合は、サーバーペア間のファイアウォールで UDP ポート 9095 を開きます。

- Cisco ISE に設定されている DNS サーバーが Windows メンバーサーバーの順方向（A）レコードおよび逆方向（PTR）レコードを解決できることを確認します。必要な詳細を追加する必要があります（不足している場合）。

エージェントがサーバーに直接インストールされているか、メンバーサーバーにインストールされているかに関係なく、ドメインコントローラのリモートイベントログ管理グループの次のファイアウォールルールを有効にして、サーバーがドメインコントローラのイベントログにアクセスできるようにします。

- リモートイベントログ管理（NP-in）
- リモートイベントログ管理（RPC）
- リモートイベントログ管理（RPC-EPMAP）

エージェントのインストール後にこの手順を実行する場合は、サーバーでエージェントサービスを再起動する必要があります。

MSRPC のエージェントの展開

始める前に

パッシブ ID サービスを有効にする必要があります。手順は、次のとおりです。

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** をクリックし、展開ノードの横にあるチェックボックスをオンにします。[編集（Edit）] をクリックします。[ノードの編集（Edit Node）] ウィンドウで、[パッシブ ID サービスの有効化（Enable Passive Identity Service）] チェックボックスをオンにして、[保存（Save）] をクリックします。

Cisco ISE-PIC の GUI で、**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択し、展開ノードの横にあるチェックボックスをオンにします。[編集（Edit）] をクリックします。[ノードの編集（Edit Node）] ウィンドウで、[パッシブ ID サービスの有効化（Enable Passive Identity Service）] チェックボックスをオンにして、[保存（Save）] をクリックします。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [パッシブ ID（Passive ID）] > [プロバイダー（Providers）] > [エージェント（Agents）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 新しいエージェントを展開する場合は、[エージェント（Agents）] ウィンドウで [新しいエージェントの展開（Deploy New Agent）] をクリックします。既存のエージェントを登録する場合は、[既存のエージェントの登録（Register Existing Agents）] をクリックします。

[既存のエージェントの登録（Register Existing Agent）] オプションを選択した場合、サポートされている登録済みのクライアントからの要求が、サポートされていないプロトコルが原因でドロップされることがあります。このようなイベントでは、サポートされているプロトコルで Cisco ISE クライアントを設定する必要があります。

ステップ 4 [名前（Name）] フィールドに名前を入力します。

ステップ 5 [ホスト FQDN（Host FQDN）] フィールドにホスト FQDN URL を入力します。

ステップ 6 [ユーザー名（User Name）] と [パスワード（Password）] に入力します。

ユーザーアカウントには、PIC エージェントをインストールするためにリモートで接続する権限が必要です。

ステップ 7 [プロトコル（Protocol）] ドロップダウンリストから、[MSRPC] を選択します。

ステップ 8 [ハイアベイラビリティ設定（High Availability Settings）] セクションで [プライマリ（Primary）] をクリックします。

プライマリエージェントが正常に展開されたら、上記の手順を繰り返して（[ハイアベイラビリティ設定（High Availability Settings）] セクションで [セカンダリ（Secondary）] オプションを選択）セカンダリエージェントを展開します。セカンダリエージェントの展開中に、[プライマリエージェント（Primary Agent）] ドロップダウンリストから設定済みのプライマリエージェントを選択します。

ステップ 9 [展開（Deploy）] をクリックします。

ドメインコントローラとプライマリエージェントのマッピング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [Active Directory]** を選択します。

ステップ 2 [Active Directory] ウィンドウで、[追加（Add）] をクリックします。

ステップ 3 [接続（Connection）] セクションで、ドメインコントローラの [参加ポイント名（Join Point Name）] と [Active Directoryドメイン（Active Directory Domain）] を入力します。

ステップ 4 [送信（Submit）] をクリックします。

次のメッセージが表示されます。

```
Would you like to Join all ISE Nodes to this Active Directory Domain?
```

ステップ 5 [はい（Yes）] をクリックして、すべての ISE ノードに参加します。

ステップ 6 [ドメインに参加（Join Domain）] ポップアップウィンドウで、[ADユーザー名（AD User name）] と [パスワード（Password）] を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [PassiveID] タブをクリックします。

ステップ 9 [PassiveIDドメインコントローラ（PassiveID Domain Controllers）] ウィンドウで、マッピングする ISE ドメインの横にあるチェックボックスをクリックします。

複数の DC マッピングの場合は、[既存のエージェントを使用（Use Existing Agent）] オプションから既存のエージェントを選択できます。

ステップ 10 [編集（Edit）] をクリックします。

ステップ 11 [ホストFQDN（Host FQDN）] フィールドにホスト FQDN URL を入力します。

ステップ 12 [ADユーザー名（AD User Name）] フィールドと [パスワード（Password）] フィールドに AD クレデンシャルを入力します。ユーザーアカウントにドメインコントローラのセキュリティイベントを読み取る権限が付与されている必要があります。

ステップ 13 [プロトコル（Protocol）] ドロップダウンリストから、[エージェント（Agent）] を選択します。

ステップ 14 [エージェント（Agent）] ドロップダウンリストから、対応するエージェント（高可用性のためには [プライマリ（Primary）]、または [スタンドアロン（Standalone）]）を選択します。

ステップ 15 [保存（Save）]をクリックします。

[ダッシュボード（Dashboard）] で、エージェントマッピングステータス、ドメインコントローラを監視しているエージェント、およびエージェントの役割を確認できます。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[PassiveID]** > **[概要（Overview）]**を選択します。

ドメインコントローラのイベントログを表示するには、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[運用（Operations）]** > **[RADIUS]** > **[ライブセッション（Live Sessions）]** を選択します。

Active Directory ドメインの脱退

この Active Directory ドメインまたはこの参加ポイントからユーザーとマシンを認証する必要がない場合は、Active Directory ドメインを脱退できます。

コマンドライン インターフェイスから Cisco ISE アプリケーション設定をリセットする場合、またはバックアップやアップグレードの後に設定を復元する場合、脱退操作が実行され、Cisco ISE ノードがすでに参加している場合は、Active Directory ドメインから切断されます。ただし、Cisco ISE ノードのアカウントは、Active Directory ドメインから削除されません。脱退操作では Active Directory ドメインからノード アカウントも削除されるため、脱退操作は管理者ポータルから Active Directory クレデンシャルを使用して実行することを推奨します。これは、Cisco ISE ホスト名を変更する場合にも推奨されます。

始める前に

Active Directory ドメインを脱退したが、認証の ID ソースとして（直接または ID ソース順序の一部として）Active Directory を使用している場合、認証が失敗する可能性があります。

ステップ 1 **[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 Cisco ISE ノードの隣にあるチェックボックスをオンにして [脱退（Leave）] をクリックします。

ステップ 4 Active Directory のユーザー名とパスワードを入力し、[OK] をクリックしてドメインを脱退し、Cisco ISE データベースからマシン アカウントを削除します。

Active Directory クレデンシャルを入力すると、Cisco ISE ノードは Active Directory ドメインを脱退し、Active Directory データベースから Cisco ISE マシン アカウントが削除されます。

（注） Active Directory データベースから Cisco ISE マシン アカウントを削除するには、ここに入力する Active Directory クレデンシャルに、ドメインからマシン アカウントを削除する権限がなければなりません。

ステップ 5 Active Directory クレデンシャルがない場合は、[使用可能なクレデンシャルなし（No Credentials Available）] チェックボックスをオンにして、[OK] をクリックします。

[クレデンシャルなしでドメインを脱退（Leave domain without credentials）] チェックボックスをオンにすると、プライマリ Cisco ISE ノードが Active Directory ドメインから脱退します。参加時に Active Directory で作成されたマシン アカウントは、Active Directory 管理者が手動で削除する必要があります。

認証ドメインの設定

Cisco ISE が参加しているドメインは、信頼関係を持つ他のドメインに対して可視性があります。デフォルトでは、Cisco ISE はこれらすべての信頼ドメインに対する認証を許可するように設定されます。認証ドメインのサブセットに対して、Active Directory 展開との相互作用を制限できます。ドメイン認証を設定することにより、接続ポイントごとに特定のドメインを選択して、選択されたドメインに対してのみ認証が実行されるようにできます。認証ドメインでは、接続ポイントから信頼されたすべてのドメインではなく、選択されたドメインのユーザーのみを認証するように Cisco ISE に指示するため、セキュリティが向上します。また、認証ドメインでは検索範囲（着信したユーザー名または ID に一致するアカウントの検索）が制限されるため、認証要求処理のパフォーマンスと遅延が改善されます。これは、着信ユーザー名または ID にドメイン マークアップ（プレフィクスまたはサフィックス）が含まれていない場合に特に重要です。これらの理由から、認証ドメインを設定することをベストプラクティスとして強く推奨します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 **Active Directory** の参加ポイントをクリックします。

ステップ 3 [認証ドメイン（Authentication Domains）] タブをクリックします。

表に、信頼ドメインのリストが表示されます。デフォルトでは、Cisco ISE はすべての信頼ドメインに対する認証を許可します。

ステップ 4 指定したドメインのみを許可するには、[認証にすべての Active Directory ドメインを使用する（Use all Active Directory domains for authentication）] チェックボックスをオフにします。

ステップ 5 認証を許可するドメインの隣にあるチェックボックスをオンにし、[選択対象の有効化（Enable Selected）] をクリックします。[認証（Authenticate）] カラムで、このドメインのステータスが [はい（Yes）] に変わります。

また、選択したドメインを無効にすることもできます。

ステップ 6 [使用できないドメインを表示（Show Unusable Domains）] をクリックして、使用できないドメインのリストを表示します。使用できないドメインは、単方向の信頼や選択的な認証などの理由により、Cisco ISE が認証に使用できないドメインです。

次のタスク

Active Directory ユーザー グループを設定します。

Active Directory ユーザー グループの設定

Active Directory ユーザー グループを許可ポリシーで使用できるように設定する必要があります。内部的には、Cisco ISE はグループ名のあいまいさの問題を解決し、グループ マッピングを向上させるためにセキュリティ ID（SID）を使用します。SID により、グループ割り当てが正確に一致します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [グループ（Groups）] タブをクリックします。

ステップ 3 次のいずれかを実行します。

a) **[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）]** を選択して、既存のグループを選択します。

b) **[追加（Add）] > [グループの追加（Add Group）]** を選択して、グループを手動で追加します。グループ名と SID の両方を指定するか、またはグループ名のみを指定し、[SID を取得（Fetch SID）] を押します。

ユーザー インターフェイス ログインのグループ名に二重引用符（"）を使用しないでください。

ステップ 4 グループを手動で選択する場合は、フィルタを使用してグループを検索できます。たとえば、**admin*** をフィルタ基準として入力し、[グループの取得（Retrieve Groups）] をクリックすると、admin で始まるユーザー グループが表示されます。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。一度に取得できるのは 500 グループのみです。

ステップ 5 許可ポリシーで使用可能にするグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 グループを手動で追加する場合は、新しいグループの名前と SID を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

（注） グループを削除し、そのグループと同じ名前で新しいグループを作成する場合は、[SID 値の更新（Update SID Values）] をクリックして、新しく作成したグループに新しい SID を割り当てる必要があります。アップグレードすると、最初の参加の後に SID が自動的に更新されます。

次のタスク

Active Directory のユーザー属性を設定します。

Active Directory ユーザーとマシンの属性の設定

許可ポリシーの条件で使用できるようにActive Directoryユーザーとマシンの属性を設定する必要があります。

ステップ 1 **[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > [Active Directory] を選択します。

ステップ 2 [属性（Attributes）] タブをクリックします。

ステップ 3 **[追加（Add）]** > **[属性の追加（Add Attribute）]** を選択して属性を手動で追加するか、**[追加（Add）]** > **[ディレクトリから属性を選択（Select Attributes From Directory）]** を選択してディレクトリから属性のリストを選択します。

Cisco ISE では、属性タイプ IP を手動で追加するときに、ユーザー認証に IPv4 または IPv6 アドレスを使用して AD を設定できます。

ステップ 4 ディレクトリからの属性の追加を選択した場合、ユーザーの名前を [サンプル ユーザー（Sample User）] フィールドまたは [マシン アカウント（Machine Account）] フィールドに入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザーの属性のリストを取得します。たとえば、管理者属性のリストを取得するには **administrator** を入力します。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。

（注） ユーザー名の例を入力する場合、Cisco ISE が接続されているアクティブな Active Directory ドメインからユーザーを選択します。マシン属性を取得するマシンの例を選択する場合、マシン名のプレフィックスとして「host/」を追加するか、SAM$ 形式を使用してください。たとえば、host/myhost を使用します。属性の取得時に表示される値の例は説明のみを目的としており、保存されません。

ステップ 5 選択する Active Directory の属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 属性を手動で追加する場合は、新しい属性の名前を入力します。

ステップ 7 [保存（Save）] をクリックします。

パスワード変更、マシン認証、およびマシン アクセス制限の設定の変更

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。詳細については、Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （1041 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 該当する Cisco ISE ノードの隣にあるチェックボックスをオンにして [編集（Edit）] をクリックします。

ステップ 3 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 4 必要に応じて、パスワード変更、マシン認証、およびマシンアクセス制限（MAR）の設定を変更します。

ステップ 5 [ダイヤルイン チェックを有効にする（Enable dial-in check）] チェックボックスをオンにして、認証中またはクエリ中にユーザーのダイヤルインアクセス権をチェックします。ダイヤルインアクセス権が拒否されている場合は、チェックの結果により認証拒否の原因になります。

ステップ 6 認証中またはクエリ中にサーバーからユーザーにコールバックするようにするには、[ダイヤルイン クライアントのコールバック チェックを有効にする（Enable callback check for dial-in clients）] チェックボックスをオンにします。サーバーによって使用される IP アドレスまたは電話番号は、発信者またはネットワーク管理者によって設定されます。チェックの結果は、RADIUS 応答でデバイスに返されます。

ステップ 7 プレーン テキスト認証に Kerberos を使用する場合は、[プレーン テキスト認証に Kerberos を使用（Use Kerberos for Plain Text Authentications）] チェックボックスをオンにします。デフォルトの推奨オプションは MS-RPC です。

Active Directory アカウントに対するパスワードの最大試行回数の設定

Cisco ISE 管理者には、不正なパスワードの試行が多すぎることによる Active Directory アカウントのロックアウトを防ぐメカニズムが必要です。ロックアウトを防ぐために、badPwdCount 属性を設定できます。Cisco ISE は、Active Directory に認証を送信する前に、十分な試行回数が残っているか確認する必要があります。

Cisco ISE は、ユーザーを認証する前に、Cisco ISE で設定されている不正なパスワードの最大試行回数を Active Directory における badPwdCount 属性の現在の値と比較します。Cisco ISE で設定された不正なパスワードの最大試行回数が badPwdCount 属性の値と等しい場合、認証はドロップされ、Active Directory に送信されません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]**。

ステップ 2 該当する Cisco ISE ノードの隣にあるチェックボックスをオンにして [編集（Edit）] をクリックします。

ステップ 3 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 4 [Active Directoryユーザーのロックアウトを防ぐ（Prevent Active Directly User Lockout）] セクションで、[失敗した認証の保護を有効にする（Enable Failed Authentication Protection）] チェックボックスをオンにします。

ステップ 5 不正なパスワードの最大試行回数を入力します。

（注） ここでのパスワードの最大試行回数は、Active Directory の badPwdCount 属性の値として設定されている不正なパスワードの最大試行回数よりも少なくする必要があります。

ステップ 6 認証のための接続要求ごとに [有線（Wired）] および [ワイヤレス（Wireless）] チェックボックスをオンにします。

（注） 接続タイプ（有線またはワイヤレス）は、RADIUS NAS-port-type 属性から取得されます。NAD は、この機能が機能するために、この Radius 属性の正しい値を Access-request メッセージに含める必要があります。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** > **[デフォルト（Default）]** > **[認証ポリシー（Authentication Policy）]**。

ステップ 9 必要な**ルール名**については、ID ソースとして設定された Active Directory **を使用します**。

（注） ID シーケンス範囲または Active Directory 範囲は機能しません。特定の Active Directory 参加ポイントを使用していることを確認します。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 ゲストポータルも同じように設定できます。

ステップ 12 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ID（Identities）]** > **[IDソース順序（Identity Source Sequences）]** > **[追加（Add）]**。

ステップ 13 ID ソース順序の [名前（Name）] を入力します。

ステップ 14 [認証検索リスト（Authentication Search List）] セクションで、[>] ボタンを使用して ID ソースを [使用可能（Available）] ペインから [選択済み（Selected）] ペインに移動します。

（注） ID シーケンス範囲や Active Directory 範囲は機能しません。特定の Active Directory 参加ポイントを使用していることを確認します。この機能が有効になっている最初の Active Directory 参加ポイントのみが使用されます。この機能が複数の参加ポイントで有効になっている場合は、リストの最初の参加ポイントだけがチェックされます。

ステップ 15 [送信（Submit）] をクリックします。

トラブルシューティング

問題 1：Active Directory でユーザーがロックされている。

解決策：Active Directory で該当ユーザーの badPwdCount 属性をリセットするようにネットワーク管理者に依頼します。

問題 2：ユーザーが Active Directory に対する認証に失敗したが、その Active Directory に対してロックアウト防止が有効になっている。

解決策：次の手順を実行します。

- ユーザーアカウントが Active Directory に存在することを確認します。
- Active Directory のユーザーアカウントに対する badPwdCount 属性値は、Cisco ISE で設定されている不正パスワード最大試行回数未満である必要があります。

- 選択されていない接続タイプを使用して認証します。ロックアウト防止が [ワイヤレス（Wireless）] に設定されている場合は、有線接続を使用して認証を試みます。その逆も同様です。認証に成功すると、Active Directory の badPwdCount 属性がリセットされます。
- Active Directory で該当ユーザーの badPwdCount 属性をリセットするようにネットワーク管理者に依頼します。

問題 3：Active Directory のロックアウト防止が有効になっている場合でも、ユーザーがロックアウトされる。

解決策：Cisco ISE で設定されている不正なパスワードの最大試行回数が、Active Directory で設定されている badPwdCount 属性の値未満であることを確認します。

問題 4：ポータルフローにおいてユーザーが Active Directory に対する認証に失敗したが、その Active Directory に対してロックアウト防止が有効になっている。

解決策：次の手順を実行します。

- 関連する Active Directory インスタンスが、そのポータルフローに使用される ID ストア（シーケンスではない）の一部であることを確認します。
- ユーザーアカウントが Active Directory に存在することを確認します。
- Active Directory のユーザーアカウントに対する badPwdCount 属性値は、Cisco ISE で設定されている不正パスワード最大試行回数未満である必要があります。
- 選択されていない接続タイプを使用して認証を試行します。ロックアウト防止が [ワイヤレス（Wireless）] に設定されている場合は、有線接続を使用して認証を試みます。その逆も同様です。認証に成功すると、Active Directory の badPwdCount 属性がリセットされます。
- Active Directory で該当ユーザーの badPwdCount 属性をリセットするようにネットワーク管理者に依頼します。

マシンアクセス制限キャッシュ

アプリケーションサービスを手動で停止すると、Cisco ISE はマシンアクセス制限（MAR）キャッシュコンテンツ、calling-station-ID リスト、および対応するタイムスタンプをローカルディスクのファイルに保存します。アプリケーションサービスを誤って再起動した場合、Cisco ISE はインスタンスの MAR キャッシュ エントリを保存しません。アプリケーション サービスが再起動すると、Cisco ISE はキャッシュエントリの存続時間に基づいて、ローカルディスクのファイルから MAR キャッシュエントリを読み取ります。再起動後にアプリケーションサービスが起動すると、Cisco ISE はそのインスタンスの現在の時刻と MAR キャッシュエントリの時刻を比較します。現在の時刻と MAR エントリの時刻の差が MAR キャッシュ エントリの存続時間よりも大きい場合は、Cisco ISE はディスクからそのエントリを取得しません。それ以外の場合、Cisco ISE は MAR キャッシュ エントリを取得し、MAR キャッシュ エントリ存続時間を更新します。

MAR キャッシュを設定するには、次の手順を実行します。

外部 ID に ソースで定義されている Active Directory の [詳細設定（Advanced Settings）] タブで、次のオプションがオンになっていることを確認します。

- [マシン認証の有効化（Enable Machine Authentication）]：マシン認証を有効にします。
- [マシンアクセス制限の有効化（Enable Machine Access Restriction）]：承認前にユーザーとマシン認証を組み合わせます。

認証で MAR キャッシュを使用するには、次の手順を実行します。

認証ポリシーで `WasMachineAuthenticated is True` を使用します。このルールとクレデンシャルルールを使用すると、デュアル認証を行うことができます。マシン認証は、AD クレデンシャルの前に実行する必要があります。

[システム（System）] > [展開（Deployment）] ページでノードグループを作成した場合は、MAR のキャッシュ配布を有効にします。MAR のキャッシュ配布は、同じノードグループ内のすべての PSN に MAR キャッシュを複製します。

詳細については、次の Cisco ISE コミュニティのページを参照してください。

- https://community.cisco.com/t5/policy-and-access/mar-why-is-it-useful/td-p/3213527
- https://community.cisco.com/t5/policy-and-access/ise-2-1-mar-aging-time-eap-tls/td-p/3209628

関連トピック

外部 ID ソースとしての Active Directory の設定 （1040 ページ）

カスタム スキーマの設定

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 参加ポイントを選択します。

ステップ 3 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 4 [スキーマ（Schema）]セクションの[スキーマ（Schema）] ドロップダウンリストから[カスタム（Custom）] オプションを選択します。必要に応じて、ユーザー情報の属性を更新できます。これらの属性は、ユーザー情報（名、姓、電子メール、電話番号、地域など）の収集に使用されます。

事前設定された属性は、Active Directory スキーマ（組み込みのスキーマ）に使用されます。事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。

Active Directory の複数参加設定のサポート

Cisco ISE では、Active Directory ドメインへの複数参加がサポートされます。Cisco ISE では、50 までの Active Directory 参加がサポートされます。Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。Active Directory の複数ドメイン参加は、各参加の独自のグループ、属性、および許可ポリシーを持つ個別の Active Directory ドメインのセットで構成されます。

同じフォレストに複数回参加できます。つまり、必要に応じて、同じフォレスト内の複数のドメインに参加できます。

Cisco ISE は、単方向の信頼があるドメインに参加できます。このオプションで、単方向の信頼によって生じる権限の問題を回避できます。いずれかの信頼ドメインに参加できるため、両方のドメインを確認できます。

- [参加ポイント（Join Point）]：Cisco ISE では、Active Directory ドメインへの個別参加は、参加ポイントと呼ばれます。Active Directory の参加ポイントは、Cisco ISE の ID ストアであり、認証ポリシーで使用できます。属性およびグループの関連ディクショナリがあり、許可条件で使用できます。

- [スコープ（Scope）]：グループ化された Active Directory の参加ポイントのサブセットは、スコープと呼ばれます。単一参加ポイントの代わりに、認証結果として認証ポリシーでスコープを使用できます。スコープは、複数の参加ポイントに対してユーザーを認証するために使用されます。各参加ポイントに複数のルールを使用する代わりにスコープを使用すると、単一のルールで同じポリシーを作成することができ、Cisco ISE で要求の処理やパフォーマンスの向上にかかる時間を短縮できます。参加ポイントには、複数のスコープが含まれる場合があります。スコープは、ID ソース順序に含まれる場合があります。スコープには関連するディクショナリがないため、許可ポリシー条件にスコープを使用することはできません。

  新しい Cisco ISE のインストールを実行する場合、デフォルトでスコープは存在しません。これは、ノー スコープ モードと呼ばれます。スコープを追加すると、Cisco ISE はマルチスコープモードになります。必要に応じて、ノースコープモードに戻すことができます。すべての参加ポイントは [Active Directory] フォルダに移動されます。

  - Initial_Scope は、ノー スコープ モードで追加された Active Directory 参加ポイントの格納に使用される暗黙のスコープです。マルチスコープモードを有効にすると、すべての Active Directory 参加ポイントが自動作成された Initial_Scope に移動します。Initial_Scope の名前を変更できます。

  - All_AD_Instances は組み込み型の疑似スコープで、Active Directory 設定には表示されません。これは、認証結果としてポリシーおよび ID 順序にのみ示されます。Cisco ISE で設定されたすべての Active Directory 参加ポイントを選択する場合は、このスコープを選択できます。

Active Directory 参加ポイントを追加する新しいスコープの作成

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [スコープモード（Scope Mode）] をクリックします。
Initial_Scope と呼ばれるデフォルトのスコープが作成され、現在のすべての参加ポイントがこのスコープに配置されます。

ステップ 3 より多くのスコープを作成するには、[追加（Add）] をクリックします。

ステップ 4 新しいスコープの名前と説明を入力します。

ステップ 5 [送信（Submit）] をクリックします。

ID 書き換え

ID 書き換えは、外部 Active Directory システムに渡される前に ID を操作するよう Cisco ISE に指示する拡張機能です。ID を必要な形式（任意のドメイン プレフィクスやサフィックスまたはその他の追加マークアップを含むまたは除く）に変更するためのルールを作成できます。

ID 書き換えルールは、サブジェクト検索、認証クエリー、許可クエリーなどの操作のために、クライアントから受信したユーザー名またはホスト名に対して Active Directory に渡される前に適用されます。Cisco ISE は条件のトークンを照合し、最初の 1 つが一致するとポリシーの処理を停止して、結果に応じて ID 文字列を書き換えます。

書き換え時、角カッコ [ ] で囲まれている（[IDENTITY] など）内容はすべて、評価側では評価されず、代わりに文字列内のその場所に一致する文字列が付加される変数です。角カッコなしはすべて、ルールの評価側と書き換え側の両方で、固定文字列として評価されます。

次に、ユーザーによって入力された ID が ACME\jdoe であるとした場合の ID 書き換えの例を示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**[IDENTITY]** に書き換えます。

  結果は jdoe です。このルールは、ACME プレフィクスを持つすべてのユーザー名を削除するよう Cisco ISE に指示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**[IDENTITY]@ACME.com** に書き換えます。

  結果は jdoe@ACME.com です。このルールは、形式をプレフィクス表記からサフィックス表記に、または NetBIOS 形式から UPN 形式に変更するよう Cisco ISE に指示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**ACME2\[IDENTITY]** に書き換えます。

  結果は ACME2\jdoe です。このルールは、特定のプレフィクスを持つすべてのユーザー名を代替プレフィクスに変更するよう Cisco ISE に指示します。

- ID が **[ACME]\jdoe.USA** と一致する場合、**[IDENTITY]@[ACME].com** に書き換えます。

結果は jdoe\ACME.com です。このルールは、ドットの後の領域を削除するよう Cisco ISE に指示します。この場合は国名で、正しいドメインに置き換えられます。

- ID が **E=[IDENTITY]** と一致する場合、**[IDENTITY]** に書き換えます。

  結果は jdoe です。これは、ID が証明書から取得され、フィールドが電子メール アドレスで、Active Directory がサブジェクトで検索するように設定されている場合に作成可能なルールの例です。このルールは、「E=」を削除するように Cisco ISE に指示します。

- ID が **E=[EMAIL],[DN]** と一致する場合、**[DN]** に書き換えます。

  このルールは、証明書サブジェクトを、E=jdoe@acme.com、CN=jdoe、DC=acme、DC=com から単なる DN、CN=jdoe、DC=acme、DC=com に変換します。これは、ID が証明書サブジェクトから取得され、Active Directory が DN でユーザー検索するように設定されている場合に作成可能なルールの例です。このルールは、電子メール プレフィクスを削除し、DN を生成するよう Cisco ISE に指示します。

次に、ID 書き換えルールを記述する際によくある間違いを示します。

- ID が **[DOMAIN]\[IDENTITY]** と一致する場合、**[IDENTITY]@DOMAIN.com** に書き換えます。

  結果は jdoe@DOMAIN.com です。このルールは、ルールの書き換え側の角カッコ [ ] に [DOMAIN] がありません。

- ID が **DOMAIN\[IDENTITY]** と一致する場合、**[IDENTITY]@[DOMAIN].com** に書き換えます。

  この場合も、結果は jdoe@DOMAIN.com です。このルールは、ルールの評価側の角カッコ [ ] に [DOMAIN] がありません。

ID 書き換えルールは、常に、Active Directory 参加ポイントのコンテキスト内で適用されます。認証ポリシーの結果としてスコープが選択されている場合でも、書き換えルールは、各 Active Directory 参加ポイントに適用されます。EAP-TLS が使用されている場合、これらの書き換えルールは、証明書から取得される ID にも適用されます。

ID 書き換えの有効化

（注） この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 3 [ID 書き換え（Identity Rewrite）] セクションで、ユーザー名を変更する書き換えルールを適用するかどうかを選択します。

ステップ 4 一致条件および書き換え結果を入力します。表示されるデフォルトルールを削除し、要件に応じてルールを入力できます。Cisco ISE は順番にポリシーを処理し、要求ユーザー名に一致する最初の条件が適用されます。一致トークン（角カッコ内に含まれるテキスト）を使用して、元のユーザー名の要素を結果に転送できます。いずれのルールにも一致しない場合、識別名は変更されません。[テスト開始（Launch Test）] ボタンをクリックして、書き換え処理をプレビューできます。

ID 解決の設定

一部のタイプの ID には、プレフィクスまたはサフィックスのようなドメイン マークアップが含まれます。たとえば、ACME\jdoe などの NetBIOS ID では、「ACME」がドメイン マークアップのプレフィクスで、同様に jdoe@acme.com などの UPN ID では、「acme.com」がドメイン マークアップのサフィックスです。ドメイン プレフィクスは、組織内の Active Directory ドメインの NetBIOS（NTLM）名に一致し、ドメイン サフィックスは、組織内の Active Directory ドメインの DNS 名または代替 UPN サフィックスに一致する必要があります。たとえば、jdoe@gmail.com は、gmail.com が Active Directory ドメインの DNS 名でないため、ドメイン マークアップなしとして処理されます。

ID 解決の設定によって、重要な設定を構成して、Active Directory 導入環境に対応するようにセキュリティおよびパフォーマンス バランスを調整することができます。これらの設定を使用して、ドメイン マークアップのないユーザー名およびホスト名の認証を調整できます。Cisco ISE でユーザーのドメインを認識できない場合、すべての認証ドメインでユーザーを検索するように設定できます。ユーザーが 1 つのドメインで見つかった場合でも、Cisco ISE は ID のあいまいさがないことを確実にするために、すべての応答を待ちます。この処理は、ドメインの数、ネットワークの遅延、負荷などに応じて、時間がかかる場合があります。

ID 解決問題の回避

認証時にユーザーおよびホストの完全修飾名（つまり、ドメインマークアップ付き名前）を使用することを強く推奨します。たとえば、ユーザーの UPN と NetBIOS 名、およびホストの FQDN SPN です。複数の Active Directory アカウントが着信ユーザー名と一致する（たとえば、jdoe が jdoe@emea.acme.com および jdoe@amer.acme.com と一致する）などのあいまいエラーが頻繁に発生する場合には、このことが特に重要になります。場合によっては、完全修飾名を使用することが、問題を解決する唯一の方法になります。また、ユーザーのパスワードが一意であることを保証するのみで十分な場合もあります。したがって、一意の ID を最初から使用すると、効率が向上し、パスワード ロックアウトの問題が減少します。

ID 解決の設定

（注） この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE ノードを参加させる必要があります。

ステップ 1 **[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[Active Directory]** を選択します。

ステップ 2 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 3 [ID 解決（Identity Resolution）] セクションで、ユーザー名またはマシン名の ID 解決についての次の設定を定義します。この設定によって、ユーザーの検索と認証を詳細に制御できます。

最初に、マークアップなしの ID に対する設定を行います。このような場合、次のオプションのいずれかを選択できます。

- [要求を拒否する（Reject the request）]：このオプションを使用すると、SAM 名などのドメインマークアップがないユーザーの認証は失敗します。このことは、複数参加ドメインで、Cisco ISE がすべての参加グローバル カタログの ID を検索する必要があることによって、安全性が低下する可能性がある場合に役立ちます。このオプションによって、ドメイン マークアップを含むユーザー名を使用することがユーザーに対して強制されます。
- [結合されたフォレストの「認証ドメイン」のみで検索する（Only search in the “Authentication Domains” from the joined forest）]：このオプションを使用すると、認証ドメインのセクションで指定した、結合ポイントのフォレスト内のドメイン内のみで ID が検索されます。これはデフォルトオプションです。
- [すべての「認証ドメイン」セクションで検索する（Search in all the “Authentication Domains” sections）]：このオプションを使用すると、すべての信頼できるフォレストのすべての認証ドメイン内で ID が検索されます。これにより、遅延が増加し、パフォーマンスに影響する可能性があります。

Cisco ISE で認証ドメインがどのように設定されているかに基づいて選択します。特定の認証ドメインのみを選択した場合は、それらのドメインのみが検索されます（「結合されたフォレスト」と「すべてのフォレスト」のいずれを選択した場合も）。

2 番目の設定は、Cisco ISE が、[認証ドメイン（Authentication Domains）] セクションで指定された設定に準拠するために必要となるすべてのグローバルカタログ（GC）と通信できない場合に使用します。このような場合、次のオプションのいずれかを選択できます。

- [使用可能なドメインで続行する（Proceed with available domains）]：このオプションを使用すると、使用可能ないずれかのドメインで一致が見つかった場合に認証が続行されます。
- [要求をドロップする（Drop the request）]：このオプションを使用すると、ID 解決で到達不能または使用できないドメインが検出された場合に認証要求がドロップされます。

Active Directory 認証のためのユーザーのテスト

Active Directory からユーザー認証を検証するには、[ユーザーのテスト（Test User）] ツールを使用できます。グループおよび属性を取得して調査することもできます。単一の参加ポイントまたはスコープのテストを実行できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- すべての参加ポイントのテストを実行するには、**[拡張ツール（Advanced Tools）] > [すべての参加ポイントのユーザーをテスト（Test User for All Join Points）]** を選択します。
- 特定の参加ポイントのテストを実行するには、参加ポイントを選択し、[編集（Edit）] をクリックします。Cisco ISE ノードを選択し、[ユーザーのテスト（Test User）] をクリックします。

ステップ 3 Active Directory のユーザー（またはホスト）のユーザー名とパスワードを入力します。

ステップ 4 認証タイプを選択します。ステップ 3 のパスワード入力は、ルックアップ オプションを選択する場合には必要ありません。

ステップ 5 すべての参加ポイントに対してこのテストを実行する場合は、このテストを実行する Cisco ISE ノードを選択します。

ステップ 6 Active Directory からグループおよび属性を取得するには、[グループの取得（Retrieve Groups）] および [属性の取得（Retrieve Attributes）] チェックボックスをオンにします。

ステップ 7 [テスト（Test）] をクリックします。
テスト操作の結果と手順が表示されます。手順で失敗の原因を特定し、トラブルシューティングできます。

また、Active Directory がそれぞれの処理手順（認証、参照、グループおよび属性の取得）を実行するのに要する時間（ミリ秒単位）を表示することもできます。操作にかかる時間がしきい値を超えると、Cisco ISE に警告メッセージが表示されます。

Active Directory の設定の削除

Active Directory を外部 ID ソースとして使用しない場合は、Active Directory の設定を削除する必要があります。別の Active Directory ドメインに参加する場合は、設定を削除しないでください。現在参加しているドメインから脱退し、新しいドメインに参加できます。

始める前に

Active Directory ドメインが残っていることを確認します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 設定された Active Directory の横のチェックボックスをオンにします。

ステップ 3 [ローカル ノード ステータス（Local Node Status）] が [参加していない（Not Joined）] としてリストされていることを確認します。

ステップ 4 [削除（Delete）] をクリックします。

Active Directory データベースから設定を削除しました。後で Active Directory を使用する場合は、有効な Active Directory の設定を再送信できます。

ノードの Active Directory の参加の表示

特定の Cisco ISE ノードのすべての Active Directory 参加ポイントのステータスまたはすべての Cisco ISE ノードのすべての参加ポイントのリストを表示するには、[Active Directory] ページの [ノード ビュー（Node View）] ボタンを使用できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [ノード ビュー（Node View）] をクリックします。

ステップ 3 [ISE Node（ISE ノード）] ドロップダウン リストからノードを選択します。
テーブルに、Active Directory のステータスがノード別に一覧されます。展開に複数の参加ポイントと複数の Cisco ISE ノードがある場合、このテーブルが更新されるまでに数分かかる場合があります。

ステップ 4 その Active Directory 参加ポイントのページに移動し、その他の特定のアクションを実行するには、参加ポイントの [名前（Name）] リンクをクリックします。

ステップ 5 [診断ツール（Diagnostic Tools）] ページに移動して特定の問題のトラブルシューティングを行うには、[診断概要（Diagnostic Summary）] 列のリンクをクリックします。診断ツールでは、ノードごとに各参加ポイントの最新の診断結果が表示されます。

Active Directory の問題の診断

診断ツールは、各 Cisco ISE ノードで実行されるサービスです。診断ツールを使用して、Active Directory 展開を自動的にテストおよび診断したり、Cisco ISE によって Active Directory が使用される場合に機能やパフォーマンスの障害の原因となる可能性がある問題を検出するための一連のテストを実行したりすることができます。

Cisco ISE が Active Directory に参加できない、または Active Directory に対して認証できない理由は、複数あります。このツールは、Cisco ISE を Active Directory に接続するための前提条件が正しく設定されていることを確認するのに役立ちます。また、ネットワーク、ファイアウォール設定、クロック同期、ユーザー認証などの問題の検出に役立ちます。このツールは、手順をステップごとに説明したガイドとして機能し、必要に応じて、中間の各レイヤの問題の修正を支援します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [拡張ツール（Advanced Tools）] ドロップダウン リストをクリックし、[診断ツール（Diagnostic Tools）] を選択します。

ステップ 3 診断を実行する Cisco ISE ノードを選択します。

Cisco ISE ノードを選択しない場合は、すべてのノードでテストが実行されます。

ステップ 4 特定の Active Directory 参加ポイントを選択します。

Active Directory 参加ポイントを選択しない場合は、すべての参加ポイントでテストが実行されます。

ステップ 5 オンデマンドで、またはスケジュールに基づいて診断テストを実行できます。

- テストをすぐに実行するには、[テストを今すぐ実行（Run Tests Now）] を選択します。
- スケジュールした間隔でテストを実行するには、[スケジュールしたテストを実行する（Run Scheduled Tests）] チェックボックスをオンにし、開始時刻とテストの実行間隔（時、日、週単位）を指定します。このオプションを有効にすると、すべての診断テストがすべてのノードとインスタンスに対して実行され、[ホーム（Home）] ダッシュボードの [アラーム（Alarms）] ダッシュレットに障害が報告されます。

ステップ 6 警告ステータスまたは失敗ステータスのテストの詳細を確認するには、[テストの詳細の表示（View Test Details）] をクリックします。
このテーブルを使用して、特定のテストの再実行、実行中のテストの停止、特定のテストのレポートの表示を行うことができます。

Active Directory デバッグ ログの有効化

Active Directory デバッグ ログはデフォルトでは記録されません。展開でポリシー サービス ペルソナを担当する Cisco ISE ノードでこのオプションを有効にする必要があります。Active Directory のデバッグ ログを有効にすると、ISE のパフォーマンスに影響する場合があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログの設定（Debug Log Configuration）]** を選択します。

ステップ 2 Active Directory のデバッグ情報を取得する Cisco ISE ポリシー サービス ノードの隣のオプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 3 [Active Directory] オプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 4 [Active Directory] の隣にあるドロップダウン リストから [DEBUG] を選択します。これにはエラー、警告、および verbose ログが含まれます。完全なログを取得するには、[TRACE] を選択します。

ステップ 5 [保存（Save）] をクリックします。

トラブルシューティング用の Active Directory ログ ファイルの入手

可能性がある問題をトラブルシューティングするには、Active Directory のデバッグ ログをダウンロードし、表示します。

始める前に

Active Directory のデバッグ ロギングを有効にする必要があります。

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）]** を選択します。

ステップ 2 Active Directory のデバッグ ログ ファイルを取得するノードをクリックします。

ステップ 3 [デバッグ ログ（Debug Logs）] タブをクリックします。

ステップ 4 このページを下にスクロールして ad_agent.log ファイルを見つけます。このファイルをクリックしてダウンロードします。

Active Directory のアラームおよびレポート

Cisco ISE は、Active Directory に関連するアクティビティをモニタリングし、トラブルシューティングを実行するためのさまざまなアラームおよびレポートを提供します。

アラーム

Active Directory のエラーおよび問題に対して、次のアラームがトリガーされます。

- 設定したネームサーバーが使用できない
- 参加したドメインが使用できない
- 認証ドメインが使用できない
- Active Directory フォレストが使用できない
- AD コネクタを再起動する必要があった
- AD：ISE アカウントパスワードの更新に失敗
- AD：マシン TGT のリフレッシュに失敗

レポート

次の 2 つのレポートで Active Directory に関連するアクティビティをモニターできます。

- [RADIUS認証レポート（RADIUS Authentications report）]：このレポートは、Active Directory の認証および許可の詳細な手順を示します。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] > [RADIUS 認証（RADIUS Authentications）]** にあります。

- [ADコネクタ操作レポート（AD Connector Operations report）]：[ADコネクタ操作レポート（AD Connector Operations Report）] は、AD コネクタが実行するバックグラウンド操作（Cisco ISE サーバーパスワードの更新、Kerberos チケットの管理、DNS クエリ、DC 検出、LDAP、および RPC 接続管理など）のログを提供します。Active Directory の障害が発生した場合は、考えられる原因を特定するために、このレポートで詳細を確認できます。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [診断（Diagnostics）] > [AD コネクタ操作（AD Connector Operations）]** にあります。

Active Directory の高度な調整

高度な調整機能ではノード固有の設定が可能です。この設定は、システムのパラメータの詳細な調整を伴う、シスコのサポート担当者の指示に基づくサポートアクションに使用します。これらの設定は、通常の管理フローを対象としていません。ガイダンスに従って使用する必要があります。

優先ドメインコントローラの設定

ドメインフェールオーバーの場合に使用するドメインコントローラを指定できます。ドメインが失敗した場合、Cisco ISE は優先リストに追加されたドメインコントローラの優先順位スコアを比較し、優先順位スコアが最も高いドメインコントローラを選択します。そのドメインコントローラがオフラインであるか、何らかの問題により到達不能である場合、優先リスト内で優先順位スコアが次に高いドメインコントローラが使用されます。優先リスト内のすべてのドメインコントローラがダウンしている場合は、優先順位スコアに基づいてリスト外のドメインコントローラが選択されます。フェールオーバーの前に使用されていたドメインコントローラが復元されると、Cisco ISE はそのドメインコントローラに戻ります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory] > [高度なツール（Advanced Tools）] > [高度なチューニング（Advanced Tuning）] を選択します。

ステップ 2 [ISEノード（ISE Node）] ドロップダウンリストから、設定する Cisco ISE ノードを選択します。

ステップ 3 [名前（Name）] フィールドに次のレジストリキーを入力します。

REGISTRY.Services\lsass\Parameters\Providers\Active Directory\PreferredDCs\<Domain Name>

ステップ 4 [値（Value）] フィールドで、優先リストに追加するドメインコントローラをスペースで区切って指定します。次に例を示します。`dc01.domain.com dc03.domain.com dc05.domain.com`

ステップ 5 （オプション）[コメント（Comment）] フィールドに、優先リストに関する説明を入力します。

ステップ 6 [値の更新（Update Value）] をクリックします。

ステップ 7 [Active Directory Connectorの再起動（Restart Active Directory Connector）] をクリックします。

ステップ 8 パラメータを追加するには、この手順を繰り返します。

優先リストを使用しない場合は、[パラメータを工場出荷時のデフォルトにリセット（Reset Parameter to Factory Default）] をクリックします。

優先順位によるドメインコントローラの選択の強制

Cisco ISE リリース 3.4 以降では、優先ドメインコントローラのフェールオーバーが発生した場合に、Cisco ISE のドメインコントローラ選択をオーバーライドすることを選択できます。これを行うには、[名前（Name）] フィールドに **REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\PreferredDcAndGc\Priority\Enabled** レジストリキーを入力し、[値（Value）] フィールドに **1** を入力します。これにより、フェールオーバーの発生時に、Cisco ISE は既存の優先順位値をオーバーライドし、左から右への入力順序で優先リスト内の次のドメインコントローラを選択します。このレジストリキーの値は、デフォルトで **0** に設定されています。

REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\PreferredDcAndGc\Priority\Enabled レジストリキーが有効になっている場合は、フェールバック間隔（秒単位）を設定することもできます。これは、Cisco ISE が左から右への入力順序で優先ドメインコントローラへのフェールバックを試行する前に待機する時間です。フェールバック間隔を設定するには、**REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\PreferredDcAndGc\Failback\Interval** レジストリキーを [名前（Name）] フィールドに入力し、対応するフェールバック間隔の値を [値（Value）] フィールドに入力します。フェールバック間隔の値は 60 ～ 86400 です。デフォルトのフェールバック間隔は 180 秒です。

（注） この機能は、ドメインコントローラが設定された直接ドメインに対してのみ機能し、信頼関係ドメインに対しては機能しません。

ドメインコントローラのフェールバックおよびフェールオーバーアクティビティをモニターするには、**[操作（Operations）] > [レポート（Reports）] > [レポート（Reports）] > [診断（Diagnostics）] > [ADコネクタ操作（AD Connector Operations）]** の順に選択します。

Active Directory アイデンティティ検索属性

Cisco ISE は、SAM と CN のいずれか、または両方の属性を使用してユーザーを識別します。Cisco ISE では、sAMAccountName 属性がデフォルトの属性として使用されます。

実際の環境で必要に応じて、SAM と CN のいずれか、または両方を使用するように Cisco ISE を設定できます。SAM および CN が使用される場合、SAMAccountName 属性の値が一意でないと、Cisco ISE は CN 属性値も比較します。

（注） このデフォルトの動作を変更するには、「Active Directory アイデンティティ検索の属性の設定」のセクションで説明しているように「IdentityLookupField」フラグの値を変更します。

Active Directory アイデンティティ検索の属性の設定

1. **[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]** を選択します。
2. [Active Directory] ウィンドウで、[拡張ツール（Advanced Tools）] をクリックし、[高度な調整（Advanced Tuning）] を選択します。次の詳細を入力します。
   - [ISE ノード（ISE Node）]：Active Directory に接続される ISE ノードを選択します。
   - [名前（Name）]：変更するレジストリキーを入力します。Active Directory 検索属性を変更するには、`REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField` と入力します。
   - [値（Value）]：ユーザーを識別するために ISE で使用する属性を入力します。
     - SAM：クエリで SAM のみを使用します（このオプションがデフォルトです）。
     - CN：クエリで CN のみを使用します。
     - SAMCN：クエリで CN と SAM を使用します。
   - [コメント（Comment）]：変更内容を記述します（「デフォルト動作を SAM および CN に変更」など）。
3. [値の更新（Update Value）] をクリックしてレジストリを更新します。

   ポップアップウィンドウが表示されます。メッセージを読み取り、変更を受け入れます。ISE の AD コネクタサービスが再起動します。

検索文字列の例

次の例では、ユーザー名が *userd2only* であると想定します。

- SAM 検索文字列：

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(|(cn=userd2only)(sAMAccountName=userd2only)))]
```

- SAM および CN 検索文字列：

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=userd2only))]
```

Active Directory が構成された Cisco ISE をセットアップするための補足情報

Active Directory が構成された Cisco ISE を設定するには、グループ ポリシーを設定し、マシン認証のサプリカントを設定する必要があります。

Active Directory のグループ ポリシーの設定

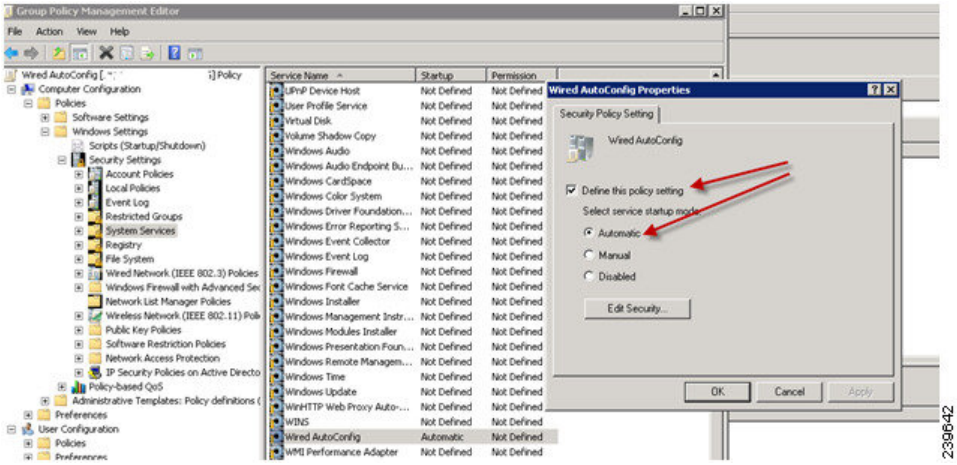
グループ ポリシー管理エディタにアクセスする方法の詳細については、Microsoft Active Directory のマニュアルを参照してください。

ステップ 1 次の図に示すように、グループ ポリシー管理エディタを開きます。

ステップ 2 新しいポリシーを作成し、その説明的な名前を入力するか、既存のドメイン ポリシーに追加します。

次の例では、ポリシー名に Wired Autoconfiguration を使用しています。

ステップ 3 次の図に示すように、[このポリシー設定を定義する（Define this policy setting）] チェックボックスをオンにして、サービス起動モードの [自動（Automatic）] オプション ボタンをクリックします。



ステップ 4 目的の組織ユニットまたはドメイン Active Directory レベルでポリシーを適用します。

Active Directory に対する EAP-TLS マシン認証のための Odyssey 5.X サプリカントの設定

Active Directory に対する EAP-TLS マシン認証に Odyssey 5.x サプリカントを使用している場合は、サプリカントで次の設定を行う必要があります。

ステップ 1 Odyssey アクセス クライアントを起動します。

ステップ 2 [ツール（Tools）] メニューから [Odyssey アクセス クライアント管理者（Odyssey Access Client Administrator）] を選択します。

ステップ 3 [マシン アカウント（Machine Account）] アイコンをダブルクリックします。

ステップ 4 [マシンアカウント（Machine Account）] ウィンドウから、EAP-TLS 認証のプロファイルを設定する必要があります。

a) **[設定（Configuration）] > [プロファイル（Profiles）]** を選択します。
b) EAP-TLS プロファイルの名前を入力します。
c) [認証（Authentication）] タブで、認証方式として [EAP-TLS] を選択します。
d) [証明書（Certificate）] タブで、[証明書を使用したログインを許可（Permit login using my certificate）] チェックボックスをオンにして、サプリカント マシンの証明書を選択します。
e) [ユーザー情報（User Info）] タブで、[マシン クレデンシャルを使用（Use machine credentials）] チェックボックスをオンにします。

このオプションが有効になっている場合、Odyssey サプリカントは host\<*machine_name*> の形式でマシン名を送信します。Active Directory は要求をマシンから送信されていると識別し、認証を実行するコンピュータ オブジェクトを検索します。このオプションが無効になっている場合、Odyssey サプリカントは host\ プレフィクスなしでマシン名を送信します。Active Directory はユーザー オブジェクトを検索し、認証は失敗します。

マシン認証のためのエージェントの設定

マシン認証のために エージェントを設定する場合、次のいずれかを実行できます。

- デフォルトのマシン ホスト名（プレフィクス「host/」を含む）を使用する。
- 新しいプロファイルを設定する。その場合、マシン名の前にプレフィクス「host/」を付加する必要があります。

Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件

Easy Connect および パッシブ ID サービスでは、Active Directory ドメイン コントローラによって生成される Active Directory ログイン監査イベントを利用して、ユーザー ログイン情報を収集します。ISE ユーザーが接続を行い、ユーザー ログイン情報を取得することができるように、Active Directory サーバーを適切に設定する必要があります。ここでは、Easy Connect および パッシブ ID サービス をサポートするように Active Directory ドメインコントローラを設定する方法（Active Directory 側からの設定）について説明します。

Easy Connect およびパッシブ ID サービスをサポートするように Active Directory ドメインコントローラを設定するには（Active Directory 側からの設定）、次の手順に従います。

（注） すべてのドメインのすべてのドメインコントローラを設定する必要があります。

1. ISE から Active Directory の参加ポイントとドメインコントローラを設定します（Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （1041 ページ）を参照）。
2. Active Directory で次の操作を実行します。
   - パッシブ ID サービス の Active Directory の設定 （1069 ページ）
   - Windows 監査ポリシーの設定 （1072 ページ）
3. （オプション）Active Directory で ISE により実行された自動設定のトラブルシューティングを行うには、次の操作を実行します。
   - Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定 （1073 ページ）
   - ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限 （1073 ページ）
   - ドメイン コントローラで DCOM を使用するための権限 （1075 ページ）

パッシブ ID サービス の Active Directory の設定

ISE Easy Connect およびパッシブ ID サービスでは、ユーザー ログイン情報を収集するため、Active Directory ドメイン コントローラにより生成される Active Directory ログイン監査イベントが使用されます。ISE は Active Directory に接続し、ユーザー ログイン情報を取得します。

次の手順は、Active Directory ドメイン コントローラから実行する必要があります。

ステップ 1 該当する Microsoft のパッチが Active Directory ドメイン コントローラにインストールされていることを確認します。

ステップ 2 Active Directory がユーザー ログイン イベントを Windows セキュリティ ログに記録するのを確認します。

[監査ポリシー（Audit Policy）]の設定（[グループポリシー管理（Group Policy Management）] の設定の一部）が、正常なログインによって Windows セキュリティログに必要なイベントが生成されるように設定されていることを確認します（これはデフォルトの Windows 設定ですが、この設定が適切であることを明示的に確認する必要があります）。

ステップ 3 ISE が Active Directory に接続するための十分な権限を持つ Active Directory ユーザーを設定する必要があります。次の手順では、管理ドメイン グループのユーザー、または管理ドメイン グループではないユーザーに対して権限を定義する方法を示します。

- Active Directory ユーザーがドメイン管理グループのメンバーである場合に必要な権限
- Active Directory ユーザーがドメイン管理グループのメンバーでない場合に必要な権限

ステップ 4 ISE によって使用される Active Directory ユーザーは、NT Lan Manager（NTLM）v1 または v2 のいずれかによって認証を受けることができます。ISE と Active Directory ドメイン コントローラ間の正常な認証済み接

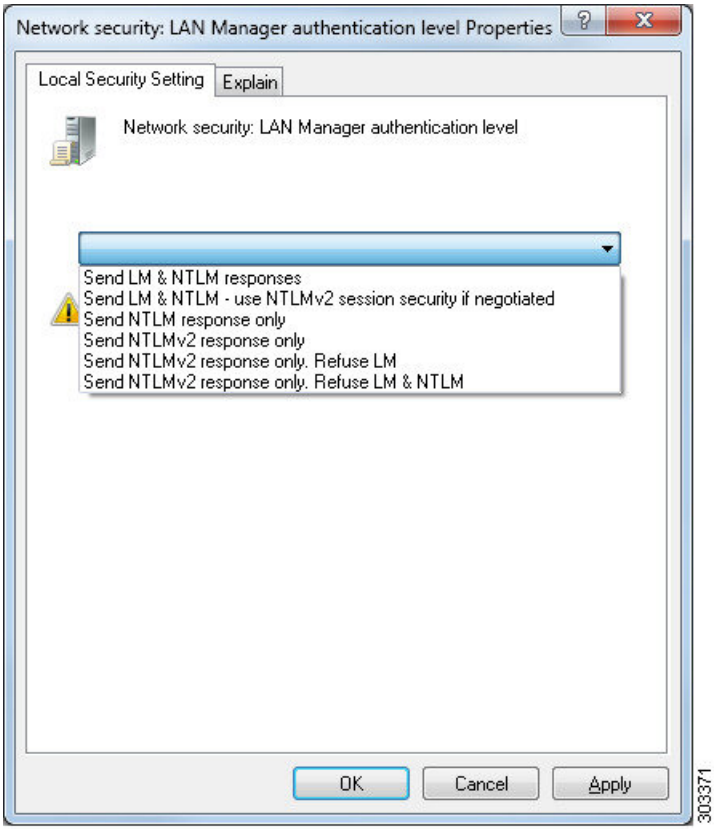
続を確実に行うために、Active Directory NTLM の設定が ISE NTLM の設定と合っていることを確認する必要があります。次の表に、すべての Microsoft NTLM オプションと、サポート対象の ISE NTLM アクションを示します。ISE が NTLMv2 に設定される場合、記載されている 6 つのオプションがすべてサポートされます。NTLMv1 をサポートするように ISE が設定されている場合、最初の 5 つのオプションだけがサポートされます。

表 *70 : ISE* と *AD NTLM* のバージョン設定に基づいてサポートされる認証タイプ

ISE NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション（NTLMv1 NTLMv2）	**NTLMv1**	**NTLMv2**
LM & NTLM応答を送信接続を許可接続を許可（Send LM & NTLM responses connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
LM & NTLMを送信：ネゴシエートされた接続が許可された場合にNTLMv2セッションセキュリティを使用接続を許可（Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみNTLM応答を送信接続を許可（Send NTLM response only connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみNTLMv2応答を送信接続を許可（Send NTLMv2 response only connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
NTLMv2応答のみを送信（Send NTLMv2 response only）。LMを拒否接続を許可接続を許可（Refuse LM connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます

ISE NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション（NTLMv1 NTLMv2）	NTLMv1	NTLMv2
NTLMv2応答のみを送信（Send NTLMv2 response only）。LM &NTLMを拒否接続を拒否接続を許可（Refuse LM & NTLM connection is refused connection is allowed）	接続は拒否されます	接続が受け入れられます

図 *15 : MS NTLM* 認証タイプのオプション



ステップ 5 Active Directory ドメイン コントローラで `dllhost.exe` へのトラフィックを許可するファイアウォール ルールを作成していることを確認します。

ファイアウォールをオフにするか、または次のポートへの特定の IP（ISE IP アドレス）のアクセスを許可することができます。

- TCP 135：一般的な RPC ポート。非同期 RPC 発信をすると、このポートでリスニングしているサービスが、クライアントに、この要求を処理できるコンポーネントが使用しているポートを通知します。
- UDP 137：NetBIOS 名前解決

- UDP 138：NetBIOS データグラム サービス
- TCP 139：NetBIOS セッション サービス
- TCP 445：SMB

数値の大きいポートは動的に割り当てられ、手動で設定できます。ターゲットとして %SystemRoot%\System32\dllhost.exe を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォール ルールを、特定の IP アドレス（ISE IP）に割り当てることができます。

Windows 監査ポリシーの設定

監査ポリシー（**グループポリシー管理**設定の一部）が正常なログインを許可していることを確認します。これには、AD ドメイン コントローラ マシンの Windows セキュリティ ログに必要なイベントを生成する必要があります。これはデフォルトの Windows 設定ですが、この設定が正しいことを確認する必要があります。

ステップ 1 **[スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [グループポリシー管理（Group Policy Management）]** を選択します。

ステップ 2 [ドメイン（Domains）] で関連するドメインに移動し、ナビゲーション ツリーを展開します。

ステップ 3 [デフォルトのドメインコントローラポリシー（Default Domain Controllers Policy）] を選択し、右クリックして、[編集（Edit）] を選択します。

グループ ポリシー管理エディターが表示されます。

ステップ 4 **[デフォルトのドメイン コントローラ ポリシー（Default Domain Controllers Policy）] > [コンピュータ設定（Computer Configuration）] > [ポリシー（Policies）] > [Windows 設定（Windows Settings）] > [セキュリティ設定（Security Settings）]** の順に選択します。

- Windows Server 2003 または Windows Server 2008（R2 以外）の場合は **[Local Policies]** > **[Audit Policy]** の順に選択します。2 つのポリシー項目（[Audit Account Logon Events] と [Audit Logon Events]）で、対応する [Policy Setting] に [Success] 状態が直接的または間接的に含まれていることを確認します。[Success] 状況を間接的に含めるには、[Policy Setting] に [Not Defined] を設定します。この場合、上位ドメインから有効値が継承されるため、[Success] 状態を明示的に含めるようにその上位ドメインの [Policy Setting] を設定する必要があります。
- Windows Server 2008 R2 および Windows 2012 の場合、**[Advanced Audit Policy Configuration]** > **[Audit Policies]** > **[Account Logon]** を選択します。2 つのポリシー項目（[Audit Kerberos Authentication Service] と [Audit Kerberos Service Ticket Operations]）に対応する [Policy Setting] に、前述のように [Success] 状態が直接または間接的に含まれていることを確認します。

（注） Active Directory ドメイン コントローラの設定で RC4 暗号が無効になっている場合を除き、Cisco ISE は Active Directory との通信に Kerberos プロトコルで RC4 暗号を使用します。Active Directory で [ネットワークセキュリティ：Kerberosで許可される暗号タイプを設定（Network Security: Configure Encryption Types Allowed for Kerberos）] オプションを使用すると、Kerberos プロトコルで許可される暗号タイプを設定できます。

ステップ 5 [監査ポリシー（Audit Policy）] の項目設定が変更されている場合は、`gpupdate /force` を実行して新しい設定を強制的に有効にする必要があります。

Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows Server 2012 および Windows Server 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティングシステムの特定のレジストリ キーを完全に制御することはできません。Microsoft Active Directory の管理者は、Microsoft Active Directory ユーザーに次のレジストリキーに対する完全制御権限を提供する必要があります。

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

次の Microsoft Active Directory バージョンでは、レジストリを変更する必要はありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、まず Microsoft Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーアイコンを右クリックし、[所有者（Owner）] タブを選択します。
ステップ 2 [アクセス許可（Permissions）] をクリックします。
ステップ 3 [詳細設定（Advanced）] をクリックします。

ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限

Windows 2012 R2 の場合は、Microsoft AD ユーザーに次のレジストリキーに対する完全制御権限を提供します。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

Windows PowerShell で次のコマンドを使用して、レジストリキーに完全な権限が付与されているかどうかを確認します。

- get-acl -path "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list
- get-acl -path "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list

Microsoft AD ユーザーがドメイン管理者グループではなく、ドメインユーザーグループに所属している場合は、次の権限が必要です。

- Cisco ISE がドメインコントローラに接続できるようにするには、レジストリキーを追加します。
- ドメイン コントローラで DCOM を使用するための権限 （1075 ページ）
- WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （1441 ページ）

これらの権限は、次のバージョンの Microsoft AD でのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ドメインコントローラへの Cisco ISE の接続を許可するためにレジストリキーを追加

Cisco ISE がドメインユーザーとして接続し、ログイン認証イベントを取得できるようにするには、ドメインコントローラにいくつかのレジストリ キーを手動で追加する必要があります。エージェントはドメインコントローラまたはドメイン内のマシンには必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキスト ファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
```

```
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

DllSurrogate キーの値には、2 つのスペースが含まれていることを確認します。レジストリを手動で更新する場合は、2つのスペースのみを含める必要があり、引用符は含めないでください。レジストリを手動で更新する際は、AppID、DllSurrogate、およびその値に引用符が含まれていないことを確認してください。

前述のスクリプトに示すように、ファイルの末尾の空の行を含めて、空の行は保持します。

Windows コマンドプロンプトで次のコマンドを使用して、レジストリキーが作成され、正しい値が設定されているかどうかを確認します。

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

ドメイン コントローラで DCOM を使用するための権限

Cisco ISE パッシブ ID サービスに使用される Microsoft Active Directory ユーザーには、ドメイン コントローラ サーバーでDCOM を使用する権限が必要です。**dcomcnfg** コマンドラインツールを使用して権限を設定します。

ステップ 1 コマンド ラインから **dcomcnfg** ツールを実行します。

ステップ 2 [コンポーネントサービス（Component Services）] を展開します。

ステップ 3 **[コンピュータ（Computers）] > [マイコンピュータ（My Computer）]** を展開します。

ステップ 4 メニューバーで [アクション（Action）] を選択し、[プロパティ（Properties）] をクリックして [COM セキュリティ（COM Security）] をクリックします。

ステップ 5 Cisco ISE がアクセスと起動の両方に使用するアカウントには許可権限が必要です。4 つのオプション（[アクセス権限（Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対する [制限の編集（Edit Limits）] と [デフォルトの編集（Edit Default）]）のすべてに Microsoft Active Directory ユーザーを追加します。

ステップ 6 [アクセス権限（Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対してローカルアクセスとリモートアクセスをすべて許可します。

図 ***16 : [***アクセス権限（***Access Permissions***）***]***に対するローカルアクアセスとリモートアクセス

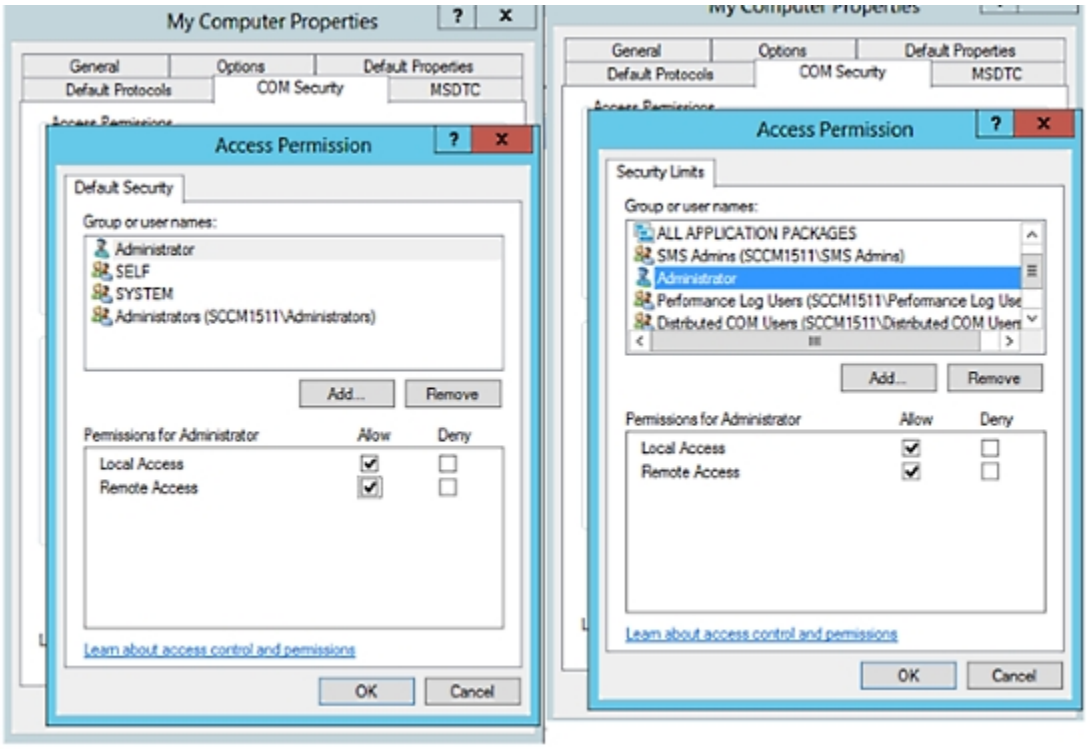
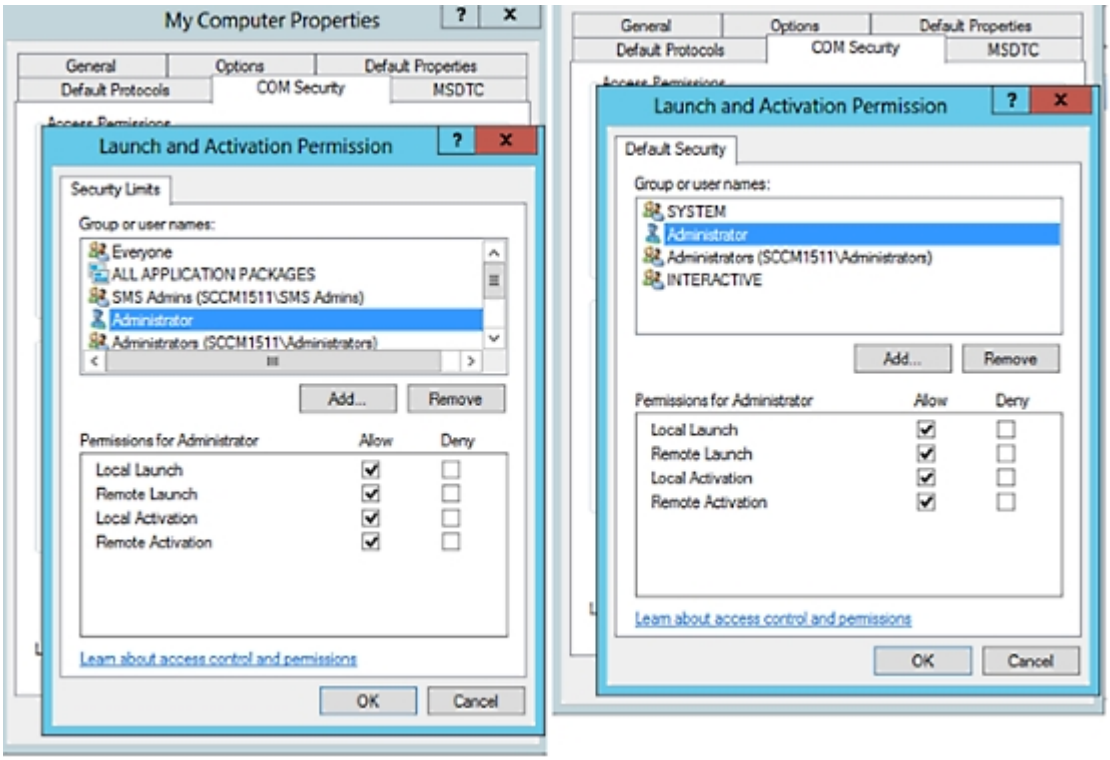


図 *17 : [*起動およびアクティブ化の権限（***Launch and Activation Permissions***）*]* のローカルアクセスとリモートアクセス



Easy Connect

Easy Connect により、セキュアな方法で有線接続されたエンドポイントからネットワークにユーザーを簡単に接続し、Cisco ISE ではなく Active Directory ドメイン コントローラからユーザーを認証することで、それらのユーザーをモニターすることができます。Easy Connect により、Cisco ISE は Active Directory ドメインコントローラからユーザー認証情報を収集します。Easy Connect は MS WMI インターフェイスを使用して Windows システム（Active Directory）に接続し、Windows イベントメッセージからのログにクエリを行うため、現在は Windows がインストールされているエンドポイントのみをサポートしています。Easy Connect は MAB を使用した有線接続をサポートし、これは 802.1X よりもずっと設定が容易です。802.1X とは異なり、Easy Connect と MAB では、

- サプリカントを設定する必要がありません
- PKI を設定する必要がありません
- ISE は外部サーバー（AD）がユーザーを認証した後に CoA を発行します

Easy Connect は次の動作モードをサポートしています。

- 適用モード：ISEがユーザークレデンシャルに基づいて、適用のために認証ポリシーをネットワークデバイスにアクティブにダウンロードします。
- 可視性モード：Cisco ISE がセッションマージをパブリッシュし、情報を pxGrid に送信するために NAD デバイスセンサーから受信した情報をアカウンティングします。

どちらの場合も、Active Directory（AD）で認証されたユーザーは、Cisco ISE のライブセッション ビューに表示され、サードパーティ製アプリケーションによる Cisco pxGrid インターフェイスを使用してセッションディレクトリからクエリすることができます。既知の情報としては、ユーザー名、IP アドレス、AD DC ホスト名と AD DC NetBIOS 名があります。pxGrid の詳細については、Cisco pxGrid ノード （464 ページ）を参照してください。

Easy Connect のセットアップが完了したら、ユーザーの名前または IP アドレスに基づいて特定ユーザーをフィルタリングできます。たとえば IT サービスの管理者が、そのエンドポイントの標準ユーザーを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して [ライブ セッション（Live Sessions）] に表示されないようにし、そのエンドポイントの標準ユーザーだけが表示されるようにできます。パッシブ ID サービスをフィルタリングするには、パッシブ ID サービスのフィルタリング （1134 ページ）を参照してください。

Easy Connect の制限

- MAC 認証バイパス（MAB）は Easy Connect をサポートします。MAB と 802.1X の両方を同じポートで設定できますが、各サービス用に異なる ISE ポリシーが必要です。
- 現在は MAB 接続のみがサポートされています。許可ポリシーで定義されている Easy Connect 条件によって接続が許可され、権限が付与されるため、接続についての独自の認証ポリシーは不要です。
- Easy Connect はハイ アベイラビリティ モードでサポートされます。パッシブ ID を使用して、複数のノードを定義して有効にすることができます。ISE はその後自動的に 1 つの PSN を有効にしますが、その他のノードはスタンバイ状態のままです。
- シスコのネットワーク アクセス デバイス（NAD）のみがサポートされています。
- IPv6 はサポートされていません。
- ワイヤレス接続は現在サポートされていません。
- Kerberos 認証イベントのみが追跡されるため、Easy Connect はユーザー認証のみを有効にし、マシン認証をサポートしません。

Easy Connect は ISE で設定する必要があり、Active Directory ドメイン サーバーには Microsoft によって発行された指示とガイドラインに基づいた適切なパッチと設定が必要です。Cisco ISE の Active Directory ドメインコントローラの設定については、次の項を参照してください。
Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件 （1068 ページ）

Easy Connect 適用モード

Easy Connect により、ユーザーは MAC アドレス バイパス（MAB）プロトコルを使用し、認証のための Active Directory（AD）にアクセスすることで、Windows オペレーティング システムを備えた有線接続されたエンドポイント（通常は PC）からセキュアなネットワークにログオンすることができます。Easy Connect は、認証されるユーザーに関する情報のために Active Directory サーバーからの Windows Management Instrumentation（WMI）イベントをリッスンします。AD がユーザーを認証すると、ドメインコントローラがユーザーに割り当てられたユーザー名と IP アドレスを含むイベント ログを生成します。Cisco ISE が AD からログインの通知を受信し、RADIUS の認可変更（CoA）を発行します。

（注） RADIUS サービス タイプが call-check に設定されている場合、MAC アドレス ルックアップは MAB 要求のために行われません。そのため、この要求への応答は access-accept です。これはデフォルトの設定です。

Easy Connect 適用モードのプロセス フロー

Easy Connect 適用モードのプロセスは次のとおりです。

1. ユーザーが有線接続されたエンドポイント（PC など）から NAD に接続します。
2. NAD（MAB 用に設定）はアクセス要求を Cisco ISE に送信します。Cisco ISE がアクセスに応答し、ユーザー設定に基づいて、ユーザーに AD へのアクセスを許可します。設定では、少なくとも DNS、DHCP、および AD へのアクセスを許可する必要があります。
3. ユーザーがドメインにログインし、セキュリティ監査イベントが Cisco ISE に送信されます。
4. ISE は RADIUS から MAC アドレスを収集し、セキュリティ監査イベントから IP アドレス、ドメイン名、ユーザーに関するアカウンティング情報（ログイン情報）を収集します。
5. セッションディレクトリですべてのデータが収集されてマージされると、（ポリシーサービスノードで管理されている適切なポリシーに基づいて）Cisco ISE が NAD に CoA を発行し、そのポリシーに基づいて NAD によりユーザーにネットワークへのアクセスが提供されます。

図 *18 : Easy Connect* 適用モードの基本フロー

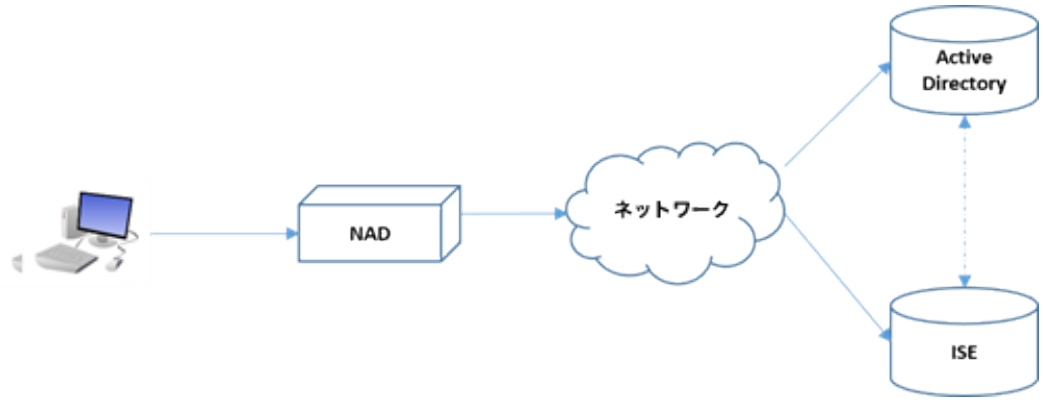
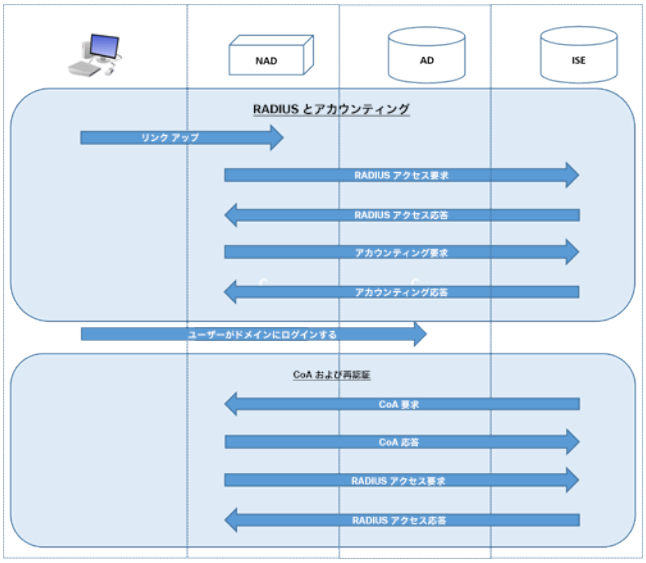


図 *19 : Easy Connect* 適用モードの詳細フロー

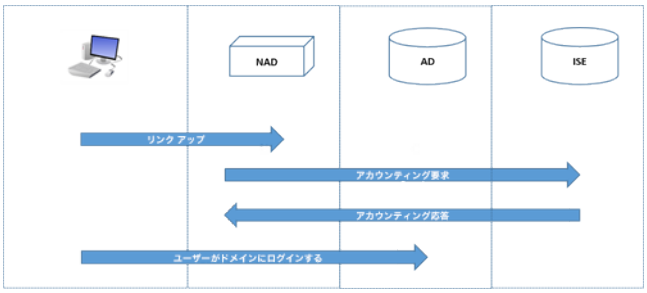


適用モードの設定の詳細については、Easy Connect 適用モードの設定（1081 ページ）を参照してください。

Easy Connect 可視性モード

可視性モードでは、Cisco ISE は RADIUS からのアカウンティング情報のみをモニターし（NAD のデバイスセンサー機能の一部）、認証は行いません。Easy Connect は RADIUS アカウンティングと WMI イベントをリッスンし、ログとレポート（およびオプションで pxGrid）にその情報をパブリッシュします。pxGrid が設定されている場合、Active Directory を使用したユーザーログイン中に RADIUS のアカウンティング開始とセッション終了の両方が pxGrid にパブリッシュされます。

図 *20 : Easy Connect* 可視性モードのフロー



Easy Connect 可視性モードの設定の詳細については、Easy Connect 可視性モードの設定 （1082 ページ）を参照してください。

Easy Connect 適用モードの設定

始める前に

- 最適なパフォーマンスを得るには、WMI イベントを受け取るための専用の PSN を導入します。
- AD ログイン イベントを受け取る、WMI ノードの Active Directory ドメイン コントローラのリストを作成します。
- Active Directory からユーザーグループを取得するために Cisco ISE が参加する必要がある Microsoft ドメインを決定します。
- 認証ポリシーでリファレンスとして使用される Active Directory グループを決定します。
- pxGrid を使用してネットワーク デバイスからのセッション データを他の pxGrid 対応システムと共有する場合は、導入内で pxGrid ペルソナを定義します。pxGrid の詳細については、次を参照してください。 Cisco pxGridノード （464 ページ）
- MAB が成功した後、NAD は、そのポートのユーザーが Active Directory サーバーにアクセスできるようにする、制限付きアクセスプロファイルを提供する必要があります。

（注） パッシブ ID サービスは複数のノードで有効にできますが、Easy Connect は一度に 1 つのノードでのみ操作できます。複数のノードのサービスを有効にすると、ISE はアクティブな Easy Connect セッションのために使用するノードを自動的に決定します。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択してノードを開き、[全般設定（General Settings）] で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] を有効にします。

ステップ 2 Easy Connect が使用する Active Directory 参加ポイントとドメイン コントローラを設定します。詳細については、Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件 （1068 ページ）を参照してください。

ステップ 3 （オプション）**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。[グループ（Groups）] タブをクリックし、認証ポリシーで使用する Active Directory グループを追加します。
ドメイン コントローラ用にマッピングした Active Directory グループは PassiveID ディクショナリで動的に更新され、ポリシー条件ルールを設定するときに使用することができます。

ステップ 4 （注） Easy Connect プロセスが適切に実行され、ISE が有効にされて CoA が発行できるように、Easy Connect 認証に使用されるすべてのプロファイルで [パッシブ ID 追跡（Passive Identity Tracking）] を有効にする必要があります。

[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）] を選択します。Easy Connect によって使用されるプロファイルについて、プロファイルを開いて [パッシブ ID 追跡（Passive Identify Tracking）] を有効にします。

ステップ 5 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）] > [単純条件（Simple Conditions）]** を選択し、Easy Connect 用のルールを作成します。[追加（Add）] をクリックして条件を定義します。

a) 名前と説明を入力します。
b) [属性（Attribute）] から PassiveID ディクショナリに移動し、PassiveID_Groups を選択してドメイン コントローラ グループ用の条件を作成するか、PassiveID_user を選択して個々のユーザー用の条件を作成します。
c) 正しい操作を入力します。
d) ポリシーに含めるユーザー名またはグループ名を入力します。

ステップ 6 [送信（Submit）] をクリックします。

Easy Connect 可視性モードの設定

始める前に

- 最適なパフォーマンスを得るには、WMI イベントを受け取るための専用の PSN を導入します。
- AD ログイン イベントを受け取る、WMI ノードの Active Directory ドメイン コントローラのリストを作成します。
- Active Directory からユーザーグループを取得するために Cisco ISE が参加する必要がある Microsoft ドメインを決定します。
- pxGrid を使用してネットワーク デバイスからのセッション データを他の pxGrid 対応システムと共有する場合は、導入内で pxGrid ペルソナを定義します。pxGrid の詳細については、次を参照してください。 Cisco pxGridノード （464 ページ）

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択してノードを開き、[全般設定（General Settings）] で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] を有効にします。

ステップ 2 Easy Connect が使用する Active Directory 参加ポイントとドメイン コントローラを設定します。詳細については、Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件 （1068 ページ） を参照してください。

PassiveID ワーク センター

パッシブ ID コネクタ（PassiveID ワーク センター）は一元的なワンストップ インストールおよび実装を提供します。これにより、ユーザー ID 情報を受信してさまざまなセキュリティ製品（Cisco Firepower Management Center（FMC）や Stealthwatch など）のサブスクライバと共有するように、ネットワークを容易に設定できます。パッシブ ID の完全なブローカとして、PassiveID ワーク センター はさまざまなプロバイダー ソース（Active Directory ドメイン コントローラ（AD DC）など）からユーザー ID を収集し、ユーザー ログイン情報を使用中の該当する IP アドレスにマッピングし、そのマッピング情報を、設定されているサブスクライバ セキュリティ製品と共有します。

（注） ISE で検証されている FMC および Stealthwatch のリリースについては、『Cisco Identity Services Engine Network Component Compatibility』を参照してください。

パッシブ ID について

認証、許可、およびアカウンティング（AAA）サーバーを提供し、802.1X や Web 認証などのテクノロジーを使用する Cisco Identity Services Engine（ISE）で提供される標準フローは、ユーザーまたはエンドポイントと直接通信し、ネットワークへのアクセスを要求し、ログイン クレデンシャルを使用して ID を検証およびアクティブに認証します。

パッシブ ID サービスはユーザーを直接認証するのではなく、プロバイダーと呼ばれる Active Directory などの外部認証サーバーからユーザー ID および IP アドレスを収集し、サブスクライバとこの情報を共有します。まず初めに、PassiveID ワーク センターは、通常、ユーザーのログインとパスワードに基づいてプロバイダーからユーザー ID 情報を受信し、ユーザー ID および関連する IP アドレスを照合するために必要な確認とサービスを実行し、認証済み IP アドレスをサブスクライバに提供します。

Passive Identity Connector（PassiveID ワーク センター）のフロー

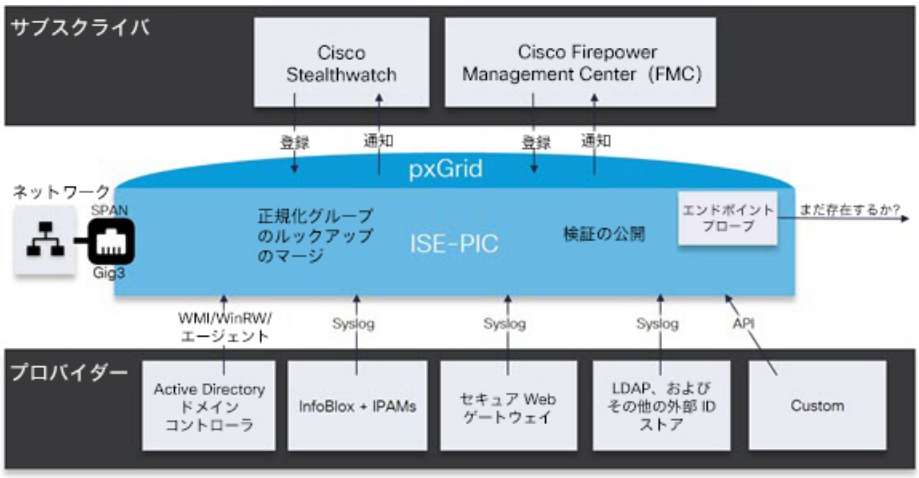
PassiveID ワーク センター のフローは次のとおりです。

1. プロバイダーがユーザーまたはエンドポイントの認証を実行します。
2. プロバイダーが認証済みのユーザー情報を Cisco ISE に送信します。

3. Cisco ISE によりユーザー情報の正規化、ルックアップ、マージ、解析、および IP アドレスへのマッピングが行われ、マッピングされた詳細情報が pxGrid に対して公開されます。
4. pxGrid サブスクライバはマッピングされたユーザーの詳細情報を受信します。

次の図に、Cisco ISE の全体的なフローを示します。

図 *21* : 全体的なフロー



初期セットアップと設定

Cisco PassiveID ワーク センターをすぐに使用できるようにするには、次のフローに従います。

1. DNS サーバーを適切に設定していることを確認します。これには、Cisco ISE からのクライアントマシンの逆引きの設定も含まれます。詳細については、DNS サーバー（1040 ページ）を参照してください。
2. いずれかのパッシブ ID サービスに使用する専用ポリシーサーバー（PSN）で、パッシブ ID サービスと pxGrid サービスを有効にします。**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択して該当するノードを開き、[全般設定（General Settings）] で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] と [pxGrid] を有効にします。
3. NTP サーバーのクロック設定を同期します。
4. ISE パッシブ ID セットアップで、最初のプロバイダーを設定します。詳細については、PassiveID セットアップの使用を開始（1086 ページ）を参照してください。
5. 1 つまたは複数のサブスクライバを設定します。

最初のプロバイダーとサブスクライバのセットアップが完了したら、追加のプロバイダーを容易に作成でき（その他の パッシブ ID サービス プロバイダー（1094 ページ）を参照）、また PassiveID ワーク センターで異なるプロバイダーのパッシブ ID を管理できます。

PassiveID ワーク センター ダッシュボード

Cisco PassiveID ワーク センター ダッシュボードには、効果的なモニタリングおよびトラブルシューティングに必要不可欠な、統合され、関連付けられた概要と統計データが表示されます。ダッシュボードはリアルタイムに更新されます。特に指定がない限り、ダッシュレットには過去 24 時間のアクティビティが表示されます。ダッシュボードにアクセスするには、**[ワークセンター（Work Centers）] > [PassiveID]** を選択し、左側のパネルで [ダッシュボード（Dashboard）] を選択します。Cisco PassiveID ワーク センター ダッシュボードはプライマリ管理ノード（PAN）でのみ表示できます。

- [メイン（Main）] ビューには、線形の [メトリクス（Metrics）] ダッシュボード、チャートダッシュレット、およびリストダッシュレットが含まれています。PassiveID ワーク センターでは、ダッシュレットは設定できません。使用可能なダッシュレットには次のものがあります。
  - [パッシブ ID メトリック（Passive Identity Metrics）] では、現在追跡中の固有のライブセッションの総数、システムに設定されている ID プロバイダーの総数、ID データをアクティブに配信しているエージェントの総数、および現在設定されているサブスクライバの総数が表示されます。
  - [プロバイダー（Providers）]：プロバイダーはユーザー ID 情報を PassiveID ワーク センターに提供します。ISE プローブ(特定のソースからデータを収集するメカニズム）を設定します。プローブを介してプロバイダー ソースからの情報を受信します。たとえば、Active Directory（AD）プローブとエージェント プローブはいずれも ISE-PIC による AD からのデータ収集を支援しますが、syslog プローブは、syslog メッセージを読み取るパーサーからデータを収集します。
  - [サブスクライバ（Subscribers）]：サブスクライバは ISE に接続し、ユーザー ID 情報を取得します。
  - [OS タイプ（OS Types）]：表示できる唯一の OS タイプは Windows です。Windows のタイプが Windows バージョン別に表示されます。プロバイダーは OS タイプを報告しませんが、ISE はこの情報を取得するため Active Directory を照会できます。ダッシュレットに表示できるエントリの最大数は 1000 です。
  - [アラーム（Alarms）]：ユーザー ID 関連のアラーム。

プローブおよびプロバイダーとしての Active Directory

Active Directory（AD）は、ユーザー ID 情報（ユーザー名、IP アドレス、ドメイン名など）の取得元である安全性が高く正確なソースです。

Active Directory プローブを設定すると、次の（ソースとして Active Directory を使用する）その他のプローブも迅速に設定して有効にできます。

- Active Directory エージェント （1098 ページ）

（注） Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。

- SPAN （1108 ページ）
- エンドポイント プローブ （1134 ページ）

また、ユーザー情報の収集時に AD ユーザー グループを使用するために Active Directory プローブを設定します。AD、エージェント、SPAN、および syslog プローブで AD ユーザーグループを使用できます。AD グループの詳細については、Active Directory ユーザー グループの設定（1049 ページ）を参照してください。

PassiveID セットアップの使用を開始

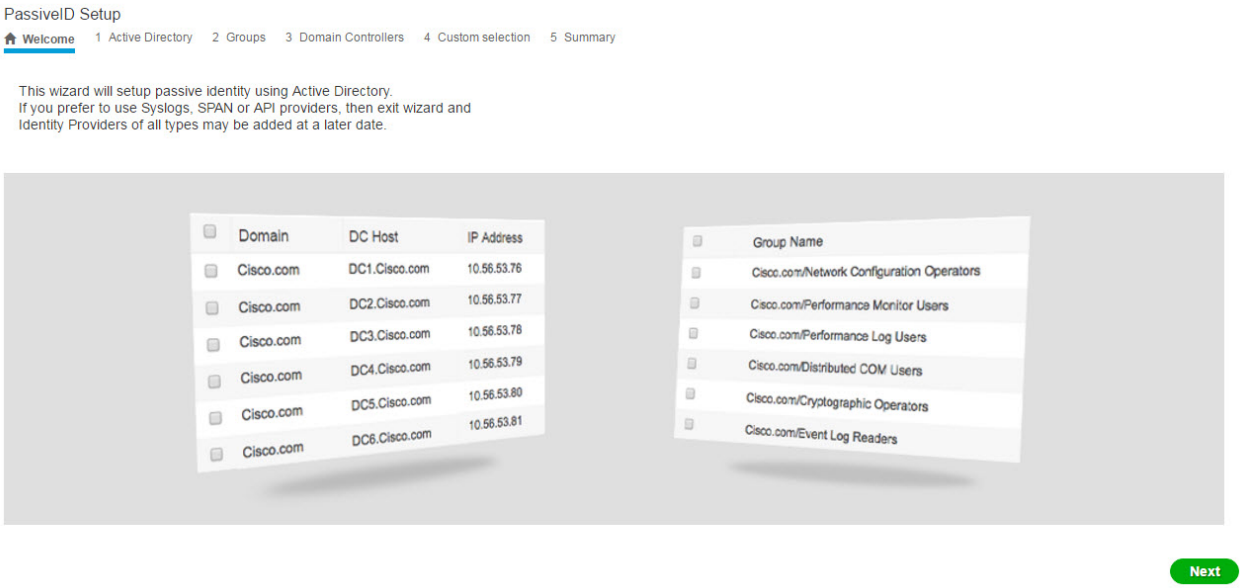
ISE-PIC には、Active Directory からユーザー ID を受信するために、Active Directory を最初のユーザー ID プロバイダーとして容易に設定できるウィザードがあります。ISE-PIC に Active Directory を設定することで、後でその他のプロバイダー タイプを設定するプロセスも簡素化されます。Active Directory を設定したら、ユーザーデータを受信するクライアントを定義するため、サブスクライバ（Cisco Firepower Management Center（FMC）や Stealthwatch など）を設定する必要があります。

始める前に

- Microsoft Active Directory サーバーがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないことを確認します。
- 参加操作用の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更（Change Password on Next Login）] を使用して設定されていないことを確認します。
- ISE でのスーパー管理者またはシステム管理者の権限があることを確認します。
- いずれかのパッシブ ID サービスに使用する専用ポリシーサーバー（PSN）で、パッシブ ID サービスと pxGrid サービスを有効にします。**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択して該当するノードを開き、[全般設定（General Settings）] で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] と [pxGrid] を有効にします。
- ISE のエントリがドメイン ネーム サーバー（DNS）にあることを確認します。ISE からのクライアントマシンの逆引き参照を適切に設定していることを確認します。詳細については、DNS サーバー （1040 ページ）を参照してください。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** を選択します。[パッシブ ID コネクタの概要（Passive Identity Connector Overview）] 画面で [パッシブ ID ウィザード（Passive Identity Wizard）] をクリックします。

図 *22 : [PassiveID* セットアップ（*PassiveID Setup*）*]*



ステップ 2 [次へ（Next）] をクリックしてウィザードを開始します。

ステップ 3 この Active Directory の参加ポイントの一意の名前を入力します。このノードが接続されている Active Directory ドメインのドメイン名を入力し、Active Directory 管理者のユーザー名とパスワードを入力します。

[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメインコントローラ（DC）に使用されます。

ステップ 4 [次へ（Next）] をクリックし、Active Directory グループを定義し、追加してモニターするユーザー グループをすべてオンにします。

前のステップで設定した Active Directory 参加ポイントに基づいて Active Directory ユーザー グループが自動的に表示されます。

ステップ 5 [次へ（Next）] をクリックします。モニターする DC を選択します。[カスタム（Custom）] を選択した場合は、次の画面でモニターする特定の DC を選択します。完了したら、[次へ（Next）] をクリックします。

ステップ 6 [終了（Exit）] をクリックして、ウィザードを終了します。

次のタスク

最初のプロバイダーとして Active Directory の設定を完了したら、追加のプロバイダー タイプも容易に設定できます。詳細については、その他のパッシブ ID サービス プロバイダー（1094 ページ）を参照してください。さらに、定義したいずれかのプロバイダーが収集したユーザー ID 情報を受信するためのサブスクライバも設定できるようになりました。

Active Directory プロバイダーの管理

Active Directory 参加ポイントの作成と設定が完了したら、次の作業を行い Active Directory プローブを管理します。

- Active Directory 認証のためのユーザーのテスト （1060 ページ）
- ノードの Active Directory の参加の表示 （1061 ページ）
- Active Directory の問題の診断 （1061 ページ）
- Active Directory ドメインの脱退 （1047 ページ）
- Active Directory の設定の削除 （1060 ページ）
- Active Directory デバッグ ログの有効化 （1062 ページ）

Active Directory の設定

Active Directory（AD）は、安全性が高く正確なソースであり、ここからユーザー情報（ユーザー名、IP アドレスなど）が取得されます。

参加ポイントを作成、編集することで Active Directory のプローブを作成し、管理するには、**[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [Active Directory]** を選択します。

詳細については、Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （1041 ページ）を参照してください。

表 *71 : Active Directory* 参加ポイント名の設定と *[*ドメインへの参加（*Join Domain*）*]* ウィンドウ

フィールド名	説明
参加ポイント名（Join Point Name）	設定したこの参加ポイントを容易に区別できる一意の名前。
Active Directory ドメイン（Active Directory Domain）	このノードが接続している Active Directory ドメインのドメイン名。
ドメイン管理者（Domain Administrator）	管理者権限を持つ Active Directory ユーザーのユーザー プリンシパル名またはユーザー アカウント名。
パスワード（Password）	Active Directory で設定されているドメイン管理者のパスワード。
組織単位の指定（Specifiy Organizational Unit）	管理者の組織単位の情報を入力します。

フィールド名	説明
クレデンシャルの保存（Store Credentials）	[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。 エンドポイント プローブの場合は、[クレデンシャルの保存（Store Credentials）] を選択する必要があります。

表 *72 : [Active Directory* 参加/脱退（*Active Directory Join/Leave*）*]* ウィンドウ

フィールド名	説明
ISEノード（ISE Node）	インストール環境での特定のノードの URL。
ISE ノードのロール（ISE Node Role）	インストール環境でそのノードがプライマリ ノードまたはセカンダリ ノードのいずれであるかを指定します。
ステータス（Status）	ノードが Active Directory ドメインにアクティブに参加しているかどうかを示します。
ドメインコントローラ（Domain Controller）	Active Directory に参加しているノードの場合、この列には Active Directory ドメインでノードが接続している特定のドメイン コントローラが示されます。
サイト（Site）	Active Directory フォレストが ISE に参加する場合、このフィールドには、[Active Directory サイトとサービス（Active Directory Sites and Services）] 領域に示されるフォレスト内の特定の Active Directory サイトが示されます。

表 *73 : [*パッシブ *ID* ドメイン コントローラ（*DC*）（*Passive ID Domain Controllers (DC)*）*]* リスト

フィールド	説明
ドメイン（Domain ）	ドメイン コントローラが存在しているサーバーの完全修飾ドメイン名。
DCホスト（DC Host）	ドメイン コントローラが存在しているホスト。
サイト（Site）	Active Directory フォレストが ISE に参加する場合、このフィールドには、[Active Directory サイトとサービス（Active Directory Sites and Services）] 領域に示されるフォレスト内の特定の Active Directory サイトが示されます。
IPアドレス（IP Address）	ドメイン コントローラの IP アドレス。

フィールド	説明
モニター方法（Monitor Using）	次のいずれかの方法で、ユーザー ID 情報を取得するため Active Directory ドメイン コントローラをモニターします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニターします。 • [エージェント名（Agent name）]：ユーザー情報を取得するために Active Directory をモニターするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウンリストから使用するエージェントを選択します。エージェントの詳細については、Active Directory エージェント （1098 ページ） を参照してください。

表 *74 : [*パッシブ *ID* ドメインコントローラ（*DC*）（*Passive ID Domain Controllers (DC)*）*]* 編集ウィンドウ

フィールド名	説明
ホストFQDN（Host FQDN）	ドメインコントローラが存在しているサーバーの完全修飾ドメイン名を入力します。
説明（Description）	このドメインコントローラを容易に特定できるように、一意の説明を入力します。
ユーザー名（User Name）	Active Directory にアクセスするための管理者のユーザー名。
パスワード（Password）	Active Directory にアクセスするための管理者のパスワード。
プロトコル（Protocol）	次のいずれかの方法で、ユーザー ID 情報を取得するため Active Directory ドメイン コントローラをモニターします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニターします。 • [エージェント名（Agent name）]：ユーザー情報を取得するために Active Directory をモニターするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウンリストから使用するエージェントを選択します。エージェントの詳細については、Active Directory エージェント （1098 ページ） を参照してください。

Active Directory グループは Active Directory から定義および管理されます。このノードに参加している Active Directory のグループは、このタブで確認できます。Active Directory の詳細については、https://msdn.microsoft.com/en-us/library/bb742437.aspxを参照してください。

表 *75 : Active Directory* の詳細設定

フィールド名	説明
履歴期間（History interval）	すでに発生したユーザー ログインの情報をパッシブ ID サービスが読み取る期間。これは、パッシブ ID サービスの起動時または再起動時に、このサービスが使用不可であった間に生成されたイベントを確認するために必要となります。エンドポイント プローブがアクティブな場合、この期間の頻度が維持されます。
ユーザー セッションのエージング タイム（User session aging time）	ユーザーがログインできる時間です。パッシブ ID サービスでは、DC からの新しいユーザー ログイン イベントが識別されますが、DC はユーザーがログオフする時点を報告しません。エージング タイムを使用すると、Cisco ISE で、ユーザーがログインする時間間隔を決定できます。
NTLM プロトコル設定（NTLM Protocol settings）	Cisco ISE と DC の間の通信プロトコルとして [NTLMv1] または [NTLMv2] を選択できます。推奨されるデフォルトは [NTLMv2] です。

フィールド名	説明
認証フロー（**Authorization Flow**）	

フィールド名	説明
	PassiveID ログインユーザーの認証ポリシーを設定するには、このチェックボックスをオンにします。 Active Directory グループメンバーシップに基づいて SGT をユーザーに割り当てる認証ポリシーを設定できます。設定すると、PassiveID 認証に対しても TrustSec ポリシールールを作成できるようになります。 [PassiveID] ディクショナリの [PassiveID_Provider]、[PassiveID_Username]、または [PassiveID_Groups] 属性を使用して、PassiveID ログインユーザーの認証ルールを作成できます。[PassiveID_Provider] 属性には、次の値を設定できます。 • **API** • **エージェント** • **SPAN** • **Syslog** • **WMI** • **その他** PassiveID ログインユーザーの IP-SGT マッピングと Active Directory グループの詳細は、セッショントピックに含まれています。これらの詳細は、pxGrid、pxGrid クラウド、または SXP を使用して公開できます。 認証ポリシーのステータスと SGT の詳細は、[RADIUSライブログ（RADIUS Live Logs）] ウィンドウ（[操作（Operations）] > [RADIUS] > [ライブログ（Live Logs）]）および [RADIUSライブセッション（RADIUS Live Sessions）] ウィンドウ（[操作（Operations）] > [RADIUS] > [ライブセッション（Live Sessions）]）で表示できます。 （注） • PassiveID、pxGrid、pxGrid クラウド、および SXP サービスがノードで有効になっていることを確認します。これらのサービスを有効にするには、[管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。 • [SXP設定（SXP Settings）] ウィンドウ（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [SXP設定（SXP Settings）]）で [SXP IP SGTマッピングテーブルにRADIUSおよびPassiveIDマッピングを追加する（Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping）] オプションを有効にして、SXP マッピングに PassiveID マッピングを含める必要があります。 • API プロバイダーを使用して認証された PassiveID ログインユーザーの SGT の詳細は、SXP を使用して公開するこ

フィールド名	説明
	とはできません。ただし、これらのユーザーの SGT の詳細は、pxGrid および pxGrid Cloud を介して公開できます。

その他の パッシブ ID サービス プロバイダー

ISE が ID 情報（パッシブ ID サービス）を、サービスをサブスクライブするコンシューマ（サブスクライバ）に提供できるようにするため、最初に ISE プローブを設定する必要があります。このプローブは ID プロバイダーに接続します。

次の表に、ISE で使用可能なすべてのプロバイダーとプローブタイプの詳細を示します。Active Directory の詳細については、プローブおよびプロバイダーとしての Active Directory（1085 ページ）を参照してください。

定義できるプロバイダー タイプを次に示します。

表 *76* : プロバイダー タイプ

プロバイダー タイプ（プローブ）	説明	送信元システム（プロバイダー）	テクノロジー	収集される ユーザー ID 情報	ドキュメント リンク
Active Directory（AD）	ユーザー情報の取得元である安全性が高く正確で最も一般的なソース。 プローブとして機能する場合、AD は WMI テクノロジーを使用して認証済みユーザー ID を送信します。 また AD 自体が、プローブではなく、その他のプローブがユーザーデータを取得するソース システム（プロバイダー）として機能します。	Active Directory ドメイン コントローラ	WMI	• ユーザー名 • IP アドレス • ドメイン	プローブおよびプロバイダーとしての Active Directory（1085 ページ）
エージェント（Agents）			ドメイン コントローラまたはメンバー サーバーにインストールされているエージェント。	• ユーザー名 • IP アドレス • ドメイン	Active Directory エージェント（1098ページ）

プロバイダー タイプ（プローブ）	説明	送信元システム（プロバイダー）	テクノロジー	収集される ユーザー ID 情報	ドキュメント リンク
	Active Directory ドメイン コントローラまたはメンバー サーバーにインストールされているネイティブ 32 ビット アプリケーション。エージェント プローブは、ユーザー ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。				
エンドポイント（Endpoint）	設定されているその他のプローブに加えて、ユーザーが接続しているかどうかを確認するため、常にバックグラウンドで実行されます。		WMI	ユーザーが接続しているかどうか	エンドポイント プローブ（1134ページ）
SPAN			SPAN（スイッチにインストール）と Kerberos メッセージ	• ユーザー名 • IP アドレス • ドメイン	SPAN（1108ページ）

プロバイダータイプ（プローブ）	説明	送信元システム（プロバイダー）	テクノロジー	収集されるユーザー ID 情報	ドキュメントリンク
	ネットワークトラフィックをリッスンし、Active Directory データに基づいてユーザー ID 情報を抽出するため、ネットワーク スイッチに導入されています。				
APIプロバイダー（API providers）	ISE が提供する RESTful API サービスを使用して、RESTful API クライアントと通信するようにプログラミングされている任意のシステムから、ユーザー ID 情報を収集します。	REST API クライアントと通信するようにプログラミングされている任意のシステム。	RESTful API。JSON 形式でサブスクライバに送信されるユーザー ID。	• ユーザー名 • IP アドレス • ポート範囲 • ドメイン	API プロバイダー（1103 ページ）
Syslog	syslog メッセージを解析し、ユーザー ID（MAC アドレスを含む）を取得します。	• 標準 syslog メッセージ プロバイダー • DHCP サーバー	syslog メッセージ	• ユーザー名 • IP アドレス • MAC アドレス • ドメイン	syslog プロバイダー（1110 ページ）

（注） pxGrid は、セッショントピックに対して 1 秒あたり 200 イベントを送信して、クライアントのオーバーロードを回避します。パブリッシャが 200 を超えるイベントを送信すると、追加のイベントはキューに入り、次のバッチで送信されます。

pxGrid が長時間にわたって 1 秒あたり 200 を超えるイベントを継続的に受信する場合、バックログイベントを保存するために通常よりも多くのメモリが消費される可能性があり、pxGrid のパフォーマンスに影響を与える場合があります。

Active Directory エージェント

パッシブ ID サービス ワーク センターから、ネイティブ 32 ビット アプリケーション、ドメイン コントローラ（DC）エージェントを、（設定に応じて）Active Directory（AD）ドメイン コントローラ（DC）またはメンバー サーバー上の任意の場所にインストールし、AD からユーザー ID 情報を取得して、設定したサブスクライバにこれらの ID を送信します。エージェント プローブは、ユーザー ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。エージェントは個別のドメインまたは AD ドメインにインストールできます。インストールされたエージェントは、1 分ごとに ISE にステータス更新情報を提供します。

エージェントは ISE が自動的にインストールおよび設定するか、またはユーザーが手動でインストールすることができます。インストールが完了すると、次のようになります。

- エージェントとその関連ファイルはパス **Program Files/Cisco/Cisco ISE PassiveID Agent** にインストールされています。
- エージェントのロギング レベルを指定する **PICAgent.exe.config** という設定ファイルがインストールされます。この設定ファイル内でロギング レベルを手動で変更できます。
- CiscoISEPICAgent.log ファイルにはすべてのロギング メッセージが保存されます。
- nodes.txt ファイルには、展開内でエージェントが通信できるすべてのノードのリストが含まれています。エージェントはリストの最初のノードと通信します。このノードと通信できない場合、エージェントはリストのノード順序に従ってノードとの通信を試行します。手動でのインストールの場合、このファイルを開き、ノード IP アドレスを入力する必要があります。（手動または自動での）インストールの完了後にこのファイルを変更するには、このファイルを手動で更新する必要があります。ファイルを開き、ノード IP アドレスを必要に応じて追加、変更、または削除します。
- Cisco ISE PassiveID Agent サービスはマシン上で稼働します。このサービスは [Windows サービス（Windows Services）] ダイアログボックスから管理できます。
- Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。エージェントをインストールできない場合、パッシブ ID サービスには Active Directory プローブを使用します。詳細については、プローブおよびプロバイダーとしての Active Directory（1085 ページ）を参照してください。

（注） メンバーサーバーで AD エージェントを実行している場合でも、Active Directory にログイン要求を問い合わせます。

Active Directory エージェントの自動インストールおよび展開

ユーザー ID についてドメイン コントローラをモニターするようにエージェント プロバイダーを設定するときには、エージェントがメンバー サーバーまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE が自動的にインストールするか、またはユーザーが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニターするように設定する必要があります。このプロセスでは、自動インストールを有効にし、ドメイン コントローラをモニターするようにエージェントを設定する方法について説明します。

始める前に

始める前に：

- サーバー側からの関連 DNS サーバーの逆引き参照を設定します。ISE の DNS サーバー設定要件の詳細については、DNS サーバー （1040 ページ）を参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/framework を参照してください。
- アクティブなパッシブ ID および pxGrid サービス。詳細については、初期セットアップと設定 （1084 ページ）を参照してください。
- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダーとしての Active Directory （1085 ページ）を参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザー グループを使用します。AD グループの詳細については、Active Directory ユーザー グループの設定 （1049 ページ）を参照してください。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [エージェント（Agents）] を選択します。

ステップ 2 新しいエージェントを追加するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 新しいエージェントを作成し、この設定で指定するホストに自動的にインストールするには、[新規エージェントの展開（Deploy New Agent）] を選択します。

ステップ 4 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、「Active Directory エージェントの設定 （1102 ページ）」を参照してください。

ステップ 5 [展開（Deploy）] をクリックします。

設定で指定したドメインに基づいてエージェントが自動的にホストにインストールされ、設定が保存されます。エージェントは [エージェント（Agents）] テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 6 **[ワーク センター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）]** を選択し、左側のパネルから [Active Directory] を選択して、現在設定されているすべての参加ポイントを表示します。

ステップ 7 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 8 前提条件の一部として追加したドメインコントローラを設定するには、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 9 作成したエージェントを使用してモニターするドメインコントローラを選択し、[編集（Edit）] をクリックします。

ステップ 10 [プロトコル（Protocol）] ドロップダウンリストから [エージェント（Agent）] を選択します。

ステップ 11 作成したエージェントを [エージェント（Agent）] ドロップダウンリストから選択します。作成したエージェントのユーザー名とパスワードのログイン情報を入力し、[保存（Save）] をクリックします。

ユーザー名とパスワードのログイン情報は、ドメインコントローラにエージェントをインストールするために使用されます。最後に、[展開する（Deploy）] をクリックすると、*picagent.exe* が */opt/pbis/bin* から指定した Windows マシンにコピーされます。

Active Directory エージェントの手動インストールおよび展開

ユーザー ID についてドメイン コントローラをモニターするようにエージェント プロバイダーを設定するときには、エージェントがメンバー サーバーまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE が自動的にインストールするか、またはユーザーが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニターするように設定する必要があります。このプロセスでは、エージェントを手動でインストールし、ドメイン コントローラをモニターするように設定する方法について説明します。

始める前に

始める前に：

- サーバー側からの関連 DNS サーバーの逆引き参照を設定します。ISE の DNS サーバー設定要件の詳細については、DNS サーバー （1040 ページ）を参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/framework を参照してください。
- アクティブなパッシブ ID および pxGrid サービス。詳細については、初期セットアップと設定 （1084 ページ）を参照してください。

- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダーとしての Active Directory （1085 ページ）を参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザー グループを使用します。AD グループの詳細については、Active Directory ユーザー グループの設定 （1049 ページ）を参照してください。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [エージェント（Agents）] を選択します。

ステップ 2 [エージェントのダウンロード（Download Agent）] をクリックし、手動でインストールするための **`picagent-installer.zip`** ファイルをダウンロードします。
このファイルは Windows の標準ダウンロード フォルダにダウンロードされます。

ステップ 3 ZIP ファイルを指定のホスト マシンに保存してインストールを実行します。

ステップ 4 ISE GUI から **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** をもう一度選択し、左側のパネルから [エージェント（Agents）] を選択します。

ステップ 5 新しいエージェントを設定するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 6 すでにホストマシンにインストールしているエージェントを設定するには、[既存のエージェントの登録（Register Existing Agent）] を選択します。

ステップ 7 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、Active Directory エージェントの設定 （1102 ページ）を参照してください。

ステップ 8 [保存（Save）] をクリックします。
エージェント設定が保存されます。エージェントは[エージェント（Agents）]テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 9 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [Active Directory] を選択して、現在設定されているすべての参加ポイントを表示します。

ステップ 10 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 11 前提条件の一部として追加したドメインコントローラを設定するには、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 12 作成したエージェントを使用してモニターするドメインコントローラを選択し、[編集（Edit）]をクリックします。

ステップ 13 [プロトコル（Protocol）] ドロップダウンリストから [エージェント（Agent）] を選択します。

ステップ 14 作成したエージェントを[エージェント（Agent）] ドロップダウンリストから選択します。エージェントに接続するためのユーザー名とパスワードを入力し、[保存（Save）] をクリックします。

ユーザーアカウントには、セキュリティイベントを読み取るために必要な権限が必要です。WMI ベースのエージェントのユーザーアカウントには、WMI/DCOM 権限が必要です。

エージェントのアンインストール

自動または手動でインストールされたエージェントは、Windowsから直接（手動で）簡単にアンインストールできます。

ステップ1 [Windows] ダイアログで [プログラムと機能（Programs and Features）] に移動します。

ステップ2 インストールされているプログラムのリストで [Cisco ISE PassiveID エージェント（Cisco ISE PassiveID Agent）] を見つけて選択します。

ステップ3 [アンインストール（Uninstall）] をクリックします。

Active Directory エージェントの設定

ISEが、さまざまなドメイン コントローラ（DC）からユーザー ID 情報を取得し、その情報をパッシブ ID サービス サブスクライバに配信するために、ネットワーク内の指定されたホストにエージェントを自動的にインストールすることを許可します。

エージェントを作成および管理するには、**[プロバイダー（Providers）]** > **[エージェント（Agents）]** を選択します。Active Directoryエージェントの自動インストールおよび展開 （1099ページ）を参照してください。

表 *77* : *[エージェント（Agents）]* ウィンドウ

フィールド名	説明
名前（Name）	設定したエージェント名。
ホスト（Host）	エージェントがインストールされているホストの完全修飾ドメイン名。
モニターリング（Monitoring）	指定されたエージェントがモニターするドメイン コントローラのカンマ区切りリストです。

表 *78* : 新規エージェント（*Agents New*）

フィールド	説明
新規エージェントの展開（Deploy New Agent）または既存のエージェントの登録（Register Existing Agent）	• 新規エージェントの展開（Deploy New Agent）：指定されたホストに新規エージェントをインストールします。 （注） 指定されたホストにエージェントを展開するには、ユーザーはドメインユーザーおよびドメイン管理者権限を持っている必要があります。 • 既存のエージェントの登録（Register Existing Agent）：ホストにエージェントを手動でインストールし、パッシブ ID サービス がサービスを有効にできるようにするため、この画面でそのエージェントを設定します。

フィールド	説明
名前（Name）	エージェントを容易に把握できる名前を入力します。
説明（Description）	エージェントを容易に把握できる説明を入力します。
ホスト FQDN（Host FQDN）	エージェントがインストールされているホスト(既存のエージェントの登録の場合）またはインストールされるホスト（自動展開の場合）の完全修飾ドメイン名です。
ユーザー名（User Name）	エージェントをインストールするホストにアクセスするためのユーザー名を入力します。パッシブ ID サービスはこれらのクレデンシャルを使用してエージェントを自動的にインストールします。 ユーザーアカウントには、リモートで接続して PIC エージェントをインストールするための権限が必要です。
パスワード（Password）	エージェントをインストールするホストにアクセスするためのパスワードを入力します。パッシブ ID サービスはこれらのクレデンシャルを使用してエージェントを自動的にインストールします。

API プロバイダー

Cisco ISE の API プロバイダー機能では、カスタマイズしたプログラムまたはターミナル サーバー（TS）エージェントから組み込み ISE パッシブ ID サービス REST API サービスにユーザー ID 情報をプッシュできます。これにより、ネットワークからプログラミング可能なクライアントをカスタマイズして、任意のネットワーク アクセス制御（NAC）システムから収集されたユーザー ID をこのサービスに送信するようにできます。さらに Cisco ISE API プロバイダーにより、すべてのユーザーの IP アドレスが同一であるが、各ユーザーに固有のポートが割り当てられるネットワーク アプリケーション（Citrix サーバーの TS-Agent など）と対話できます。

たとえば、Active Directory（AD）サーバーに対して認証されたユーザーの ID マッピングを提供する Citrix サーバーで稼働するエージェントは、新しいユーザーがログインまたはログオフするたびに、ユーザー セッションを追加または削除する REST 要求を ISE に送信できます。ISE は、クライアントから送信されたユーザー ID 情報（IP アドレス、割り当てられたポートなど）を取得し、事前に設定されているサブスクライバ（Cisco Firepower Management Center（FMC）など）に送信します。

ISE REST API フレームワークは、HTTPS プロトコルを介した REST サービスを実装し（クライアント証明書の検証は不要）、ユーザー ID 情報が JSON（JavaScript Object Notation）形式で送信されます。JSON の詳細については、http://www.json.org/ を参照してください。

ISE REST API サービスは、1 つのシステムに同時にログインしている複数のユーザーを区別するため、ユーザー ID を解析し、その情報をポート範囲にマッピングします。ポートがユーザーに割り当てられるたびに、API がメッセージを ISE に送信します。

REST API プロバイダーのフロー

カスタマイズしたクライアントをISEのプロバイダーとして宣言し、そのカスタマイズした特定のプログラム（クライアント）が RESTful 要求を送信できるようにして、ISE からカスタマイズしたクライアントへのブリッジを設定している場合、ISE REST サービスは次のように機能します。

1. Cisco ISE はクライアント認証のために認証トークンを必要とします。通信開始時と、ISE から以前のトークンの期限が切れたことが通知されるたびに、クライアントマシンのカスタマイズしたプログラムから認証トークンを求める要求が送信されます。この要求への応答としてトークンが返されます。これによりクライアントと ISE サービス間の継続的な通信が可能になります。
2. ユーザーがネットワークにログインすると、クライアントはユーザー ID 情報を取得し、API Add コマンドを使用してこの情報を ISE REST サービスに送信します。
3. Cisco ISE はユーザー ID 情報を受信してマッピングします。
4. Cisco ISE はマッピングされたユーザー ID 情報をサブスクライバに送信します。
5. 必要な場合は常に、カスタマイズされたマシンはユーザー情報削除要求を送信できます。このためには、Remove API コールを送信し、Add コールの送信時に応答として受信したユーザー ID を含めます。

ISE での REST API プロバイダーの操作

ISE で REST サービスをアクティブにするには、次の手順に従います。

1. クライアント側を設定します。詳細については、クライアント ユーザー マニュアルを参照してください。
2. パッシブ ID サービスと pxGrid サービスをアクティブにします。詳細については、初期セットアップと設定 （1084 ページ）を参照してください。
3. DNS サーバーを適切に設定していることを確認します。これには、ISE からのクライアント マシンの逆引きの設定も含まれます。 の DNS サーバー設定要件の詳細については、DNS サーバー （1040 ページ）を参照してください。
4. パッシブ ID サービス の ISE REST サービスへのブリッジの設定 （1105 ページ）を参照してください。

（注） TS-Agent と連携するように API プロバイダーを設定するには、ISE からそのエージェントへのブリッジの作成時に TS-Agent 情報を追加します。その後、TS-Agent のマニュアルで API コールの送信について確認してください。

5. 認証トークンを生成し、追加要求と削除要求を API サービスに送信します。

パッシブ ID サービス の ISE REST サービスへのブリッジの設定

ISE REST API サービスが特定のクライアントから情報を受信できるようにするには、まず Cisco ISE でその特定のクライアントを定義する必要があります。異なる IP アドレスを使用して複数の REST API クライアントを定義できます。

始める前に

始める前に：

- パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。詳細については、初期セットアップと設定 （1084 ページ）を参照してください。
- DNS サーバーを適切に設定していることを確認します。これには、Cisco ISE からのクライアントマシンの逆引きの設定も含まれます。Cisco ISE の DNS サーバー設定要件の詳細については、DNS サーバー （1040 ページ）を参照してください。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、次に左側のパネルから [API プロバイダー（API Providers）] を選択します。
[API プロバイダー（API Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しいクライアントを追加するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、「API プロバイダーの設定 （1106 ページ）」を参照してください。

ステップ 4 [送信（Submit）] をクリックします。
クライアント設定が保存され、更新された [API プロバイダー（API Providers）] テーブルが画面に表示されます。これで、クライアントは ISE REST サービスにポストを送信できるようになりました。

次のタスク

認証トークンとユーザー ID を ISE REST サービスに送信するように、カスタマイズしたクライアントをセットアップします。「パッシブ ID REST サービスへの API コールの送信 （1105 ページ）」を参照してください。

パッシブ ID REST サービスへの API コールの送信

始める前に

パッシブ ID サービス の ISE REST サービスへのブリッジの設定 （1105 ページ）

ステップ 1 Cisco ISE URL をブラウザのアドレス バーに入力します（たとえば *https://<ise hostname or ip address>/admin/*）。

ステップ 2 [API プロバイダー（API Providers）] ウィンドウで指定および設定したユーザー名とパスワードを入力します。詳細については、パッシブ ID サービスの ISE REST サービスへのブリッジの設定（1105 ページ）を参照してください。

ステップ 3 Enter キーを押します。

ステップ 4 ターゲットノードの [URL アドレス（URL Address）] フィールドに API コールを入力します。

ステップ 5 [送信（Send）] をクリックして API コールを発行します。

次のタスク

さまざまな API コールとそのスキーマおよび結果の詳細については、API コール（1107 ページ）を参照してください。

API プロバイダーの設定

（注） 次のようにリクエスト コールを使用して完全な API 定義とオブジェクト スキーマを取得できます。

- 完全な API の指定（wadl）：https://YOUR_ISE:9094/application.wadl
- API モデルとオブジェクト スキーマ：https://YOUR_ISE:9094/application.wadl/xsd0.xsd

表 *79 : API* プロバイダーの設定

フィールド	説明
名前（Name）	このクライアントを他のクライアントから容易に区別できる一意の名前を入力します。
説明（Description）	このクライアントのわかりやすい説明を入力します。
ステータス（Status）	設定完了後すぐにクライアントが REST サービスとやりとりできるようにするには、[有効（Enabled）] を選択します。
ホスト/IP（Host/IP）	クライアント ホスト マシンの IP アドレスを入力します。DNS サーバーを適切に設定していることを確認します。これには、ISE からのクライアント マシンの逆引きの設定も含まれます。
ユーザー名（User name）	REST サービスへの送信時に使用する一意のユーザー名を作成します。
パスワード（Password）	REST サービスへの送信時に使用する一意のパスワードを作成します。

API コール

Cisco ISE で パッシブ ID サービスのユーザー ID イベントを管理するには、次の API コールを使用します。

目的：認証トークンの生成

- **要求**

  POST

  https://<PIC IP アドレス>:9094/api/fmi_platform/v1/identityauth/generatetoken

  要求には BasicAuth 認証ヘッダーが含まれている必要があります。ISE-PIC GUI から以前に作成した API プロバイダーのログイン情報を入力します。詳細については、API プロバイダーの設定 （1106 ページ）を参照してください。

- **応答ヘッダー**

  このヘッダーには X-auth-access-token が含まれています。これは、追加の REST 要求を送信するときに使用するトークンです。

- **応答本文**

  HTTP 204 No Content

目的：ユーザーの追加

- **要求**

  POST

  https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity

  POST 要求のヘッダーに X-auth-access-token を追加します（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）。

- **応答ヘッダー**

  201 Created

- **応答本文**

  {

  "user": "<ユーザー名>",

  "srcPatRange": {

  "userPatStart": <ユーザー PAT 開始値>,

  "userPatEnd": <ユーザー PAT 終了値>,

  "patRangeStart": <PAT 範囲開始値>

  },

  "srcIpAddress": "<src IP アドレス>",

"agentInfo": "<エージェント名>",

"timestamp": "<ISO_8601 形式、例：“YYYY-MM-DDTHH:MM:SSZ" >",

"domain": "<ドメイン>"

}

- **注記**
  - 上記の JSON で 1 つの IP ユーザー バインディングを作成するには srcPatRange を削除します。
  - 応答本文には「ID」（作成されたユーザーセッションバインディングの固有識別子）が含まれています。削除するユーザーを指定する DELETE 要求を送信するときに、この ID を使用してください。
  - この応答には、新たに作成されたユーザー セッション バインディングの URL であるセルフ リンクも含まれています。

目的：ユーザーの削除

- **要求**

  DELETE

  https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity/<id>

  <id> に、Add 応答で受信した ID を入力します。

  DELETE 要求のヘッダーに X-auth-access-token を追加します（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）。

- **応答ヘッダー**

  200 OK

- **応答本文**

  応答本文には、削除されたユーザーセッションバインディングの詳細が含まれています。

SPAN

SPAN は、Cisco ISE がネットワークをリッスンし、ユーザー情報を取得できるようにユーザーが容易に設定できるようにする、パッシブ ID サービスです。このとき、Active Directory が Cisco ISE と直接連携するように設定する必要はありません。SPAN はネットワーク トラフィックをスニフィングし、特に Kerberos メッセージを調べ、Active Directory により保存されているユーザー ID 情報を抽出し、その情報を ISE に送信します。ISE は次にその情報を解析し、最終的にはユーザー名、IP アドレス、およびドメイン名を、ISE からすでに設定しているサブスクライバに送信します。

SPAN がネットワークをリッスンし、Active Directory ユーザー情報を抽出できるようにするには、ISE と Active Directory の両方がネットワーク上の同一スイッチに接続している必要があり

ます。これにより、SPAN は Active Directory からすべてのユーザー ID データをコピーおよびミラーリングできます。

SPAN により、ユーザー情報は次のように取得されます。

1. ユーザーエンドポイントがネットワークにログインします。
2. ログイン データとユーザー データは Kerberos メッセージに保存されます。
3. ユーザーがログインし、ユーザーデータがスイッチを通過すると、SPAN がネットワークデータをミラーリングします。
4. Cisco ISE は、ユーザー情報を取得するためネットワークをリッスンし、ミラーリングされたデータをスイッチから取得します。
5. Cisco ISE はユーザー情報を解析し、パッシブ ID マッピングを更新します。
6. Cisco ISE は解析後のユーザー情報をサブスクライバに送信します。

SPAN の使用

始める前に

ISE がネットワーク スイッチから SPAN トラフィックを受信できるようにするには、最初にそのスイッチをリッスンするノードとノードインターフェイスを定義する必要があります。インストールされている複数の ISE ノードをリッスンするには、SPAN を設定します。ネットワークをリッスンするように設定できるインターフェイスは、ノードごとに 1 つのみです。また、リッスンするために使用するインターフェイスは SPAN 専用である必要があります。

開始する前に、パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。SPAN の設定に使用可能なインターフェイスのリストには、パッシブ ID が有効なノードだけが表示されます。詳細については、初期セットアップと設定（1084 ページ）を参照してください。

また、次の操作を行う必要があります。

- ネットワークで Active Directory が設定されていることを確認します。
- スイッチが ISE と通信できることを確認するために、Active Directory に接続しているネットワーク上のスイッチで CLI を実行します。
- AD からネットワークをミラーリングするようにスイッチを設定します。
- SPAN 専用の ISE ネットワーク インターフェイス カード（NIC）を設定します。この NIC は SPAN トラフィック専用で使用されます。
- SPAN 専用の NIC が、コマンドライン インターフェイスからアクティブにされていることを確認します。
- Kerberos トラフィックのみを SPAN ポートに送信する VACL を作成します。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、次に左側のパネルから [SPAN] を選択して SPAN を設定します。

ステップ 2 （注） GigabitEthernet0 ネットワーク インターフェイス カード（NIC）は使用可能なままにし、SPAN の設定には使用可能な別の NIC を選択することを推奨します。GigabitEthernet0 は、システム管理の目的で使用されます。

わかりやすい説明を入力し（オプション）、[有効（Enabled）] ステータスを選択し、ネットワーク スイッチのリッスンに使用する関連 NIC とノードを選択します。詳細については、SPAN 設定 （1110 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックします。
SPAN 設定が保存され、ISE-PIC ISE がネットワーク トラフィックをアクティブにリッスンします。

SPAN 設定

SPAN をクライアント ネットワークにインストールすることで、展開した各ノードから、 ISE がユーザー ID を受信することを簡単に設定できます。

表 *80 : SPAN* 設定

フィールド	説明
説明（Description）	現在有効なノードとインターフェイスがわかる固有の説明を入力します。
ステータス（Status）	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。
インターフェイス NIC（Interface NIC）	ISE にインストールされている 1 つ以上のノードを選択してから、選択したノードごとに、ネットワークをリッスンして情報を得るノードインターフェイスを選択します。 （注） GigabitEthernet0 NIC を引き続き使用可能にし、SPAN の設定には他の使用可能な NIC を選択することを推奨します。GigabitEthernet0 は、システム管理の目的で使用されます。

syslog プロバイダー

パッシブ ID サービス は syslog メッセージを配信する任意のクライアント（ID データプロバイダー）からの syslog メッセージを解析し、MAC アドレスなどのユーザー ID 情報を送信します。syslog メッセージには、通常の syslog メッセージ（InfoBlox、Blue Coat、BlueCat、Lucent などのプロバイダーからのメッセージ）と DHCP syslog メッセージがあります。このマッピングされたユーザー ID データがサブスクライバに配信されます。

ユーザー ID データを受信する syslog クライアントを指定できます（syslog クライアントの設定 （1111 ページ）を参照）。プロバイダーの設定時に、接続方法（TCP または UDP）および解析に使用する syslog テンプレートを指定する必要があります。

（注） 設定されている接続タイプが TCP であり、メッセージヘッダーに問題があるためにホスト名を解析できない場合、 ISE はパケットで受信した IP アドレスを、ISE で設定されている syslog メッセージのプロバイダーリストにあるすべてのプロバイダーの IP アドレスと照合しようとします。このリストを表示するには、**[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] > [syslog プロバイダー（Syslog Providers）]** を選択します。メッセージヘッダーを確認し、必要に応じて、解析が正常に実行されるようにカスタマイズすることをお勧めします。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （1117 ページ） を参照してください。

syslog プローブが受信した syslog メッセージを ISE パーサーに送信します。パーサーはユーザー ID 情報をマッピングし、その情報を ISE に公開します。次に ISE が、解析およびマッピングされたユーザー ID 情報を パッシブ ID サービス サブスクライバに配信します。

ISE-PIC ISE からの syslog メッセージを解析してユーザー ID を取得するには、次の手順を実行します。

- ユーザー ID データの送信元 syslog クライアントを設定します。syslog クライアントの設定 （1111 ページ）を参照してください。
- 1 つのメッセージヘッダーをカスタマイズします。syslog ヘッダーのカスタマイズ （1117 ページ）を参照してください。
- テンプレートを作成してメッセージ本文をカスタマイズします。syslog メッセージ本文のカスタマイズ （1116 ページ）を参照してください。
- 解析に使用するメッセージテンプレートとして syslog クライアントを設定する場合には、ISE で事前に定義されているメッセージテンプレートを使用します。あるいは、これらの事前に定義されたテンプレートに基づいてヘッダーまたは本文のテンプレートをカスタマイズします。「Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）」を参照してください。

syslog クライアントの設定

Cisco ISE が特定のクライアントからの syslog メッセージをリッスンできるようにするには、最初に Cisco ISE でそのクライアントを定義する必要があります。異なる IP アドレスを使用して複数のプロバイダーを定義できます。

始める前に

開始する前に、パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。詳細については、初期セットアップと設定 （1084 ページ）を参照してください。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、次に左側のパネルから [Syslogプロバイダー（Syslog Providers）] を選択します。
[syslog プロバイダー（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを設定するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドを入力し（詳細についてはSyslog の設定（1112ページ）を参照）、必要に応じてメッセージテンプレートを作成します（詳細についてはsyslog メッセージ本文のカスタマイズ （1116 ページ）を参照）。

ステップ 4 [送信（Submit）] をクリックします。

Syslog の設定

特定のクライアントからの syslog メッセージを介してユーザー ID（MAC アドレスを含む）を受信するように Cisco ISE を設定します。異なる IP アドレスを使用して複数のプロバイダーを定義できます。

表 81 : syslog プロバイダー

フィールド名	説明
名前（Name）	設定したこのクライアントを容易に区別できる一意の名前を入力します。
説明（Description）	この syslog プロバイダーのわかりやすい説明。
ステータス（Status）	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。
ホスト（Host）	ホスト マシンの FQDN を入力します。
接続タイプ（Connection Type）	ISE が syslog メッセージをリッスンするチャネルを指定するため、UDP または TCP を入力します。 （注） TCP が設定されている接続タイプである場合で、メッセージヘッダーとホスト名が解析できない問題がある場合は、Cisco ISE は syslog メッセージに設定されているプロバイダーのリストにあるいずれかのプロバイダーの IP アドレス宛のパケットで受信した IP アドレスと照合しようとします。 このリストを表示するには、**[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** > **[syslog プロバイダー（Syslog Providers）]** を選択します。メッセージヘッダーを確認し、必要に応じて、解析が正常に実行されるようにカスタマイズすることをお勧めします。ヘッダーのカスタマイズの詳細については、syslogヘッダーのカスタマイズ（1117ページ） を参照してください。

フィールド名	説明
テンプレート **(Template)**	

フィールド名	説明
	テンプレートにより正確な本文メッセージ構造が指定されます。これにより、パーサーはsyslogメッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。 たとえば、テンプレートでは正確なユーザー名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザー名を検出できます。 このフィールドでは、syslog メッセージを認識して正しく解析するために使用される（syslog メッセージの本文の）テンプレートを指定します。 事前定義のドロップダウンリストから選択するか、または [新規（New）] をクリックして独自のカスタムテンプレートを作成します。新しいテンプレートの作成の詳細については、syslog メッセージ本文のカスタマイズ（1116ページ）を参照してください。ほとんどの事前定義テンプレートでは正規表現が使用されています。カスタムテンプレートでも正規表現を使用する必要があります。 （注） 編集または削除できるのはカスタムテンプレートだけであり、ドロップダウンの事前定義システム テンプレートは変更できません。 現在 ISE に含まれている事前定義 DHCP プロバイダー テンプレートを次に示します。 • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP （注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより Cisco ISE は ユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合しようとします。 DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。 Cisco ISE には次の事前定義の標準 syslog プロバイダーテンプレートがあります。

フィールド名	説明
	• ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN テンプレートについては、Syslog 事前定義メッセージテンプレートの使用（1122 ページ）を参照してください。
デフォルト ドメイン（Default Domain）	syslog メッセージで特定のユーザーに対してドメインが指定されていない場合、このデフォルト ドメインが自動的にそのユーザーに割り当てられます。これにより、すべてのユーザーにドメインが割り当てられます。 デフォルト ドメインまたはメッセージから解析されたドメインにユーザー名が付加され、username@domain となります。したがって、ユーザーとユーザーグループに関する詳細情報を取得するためには、ドメインを含めます。

syslog メッセージ構造のカスタマイズ（テンプレート）

テンプレートは正確なメッセージ構造を指定します。これにより、パーサーはsyslogメッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。たとえば、テンプレートでは正確なユーザー名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザー名を検出できます。テンプレートにより、新規マッピングメッセージとマッピング削除メッセージの両方に対応する構造が決定します。

Cisco ISE では、パッシブ ID パーサーが使用する 1 つのメッセージ ヘッダーと複数の本文構造をカスタマイズできます。

パッシブ ID パーサーが、メッセージがユーザー ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザーの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザー名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

メッセージテンプレートをカスタマイズするときに、事前定義オプションで使用されている正規表現とメッセージ構造を調べ、ISE-PICISE の事前定義メッセージ テンプレートに基づいてカスタマイズを行うかどうかを決定できます。事前定義テンプレートの正規表現、メッセージ構造、例などの詳細については、Syslog 事前定義メッセージテンプレートの使用 （1122ページ）を参照してください。

次の内容をカスタマイズできます。

- 1 つのメッセージ ヘッダー：syslog ヘッダーのカスタマイズ （1117 ページ）
- 複数のメッセージ本文：syslog メッセージ本文のカスタマイズ （1116 ページ）。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより Cisco ISE は ユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合しようとします。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

DHCP メッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCP メッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義の DHCP テンプレートを使用してください。

syslog メッセージ本文のカスタマイズ

Cisco ISE では、パッシブ ID パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます（メッセージ本文のカスタマイズ）。テンプレートには、ユーザー名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE は ユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

DHCP メッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCP メッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義の DHCP テンプレートを使用してください。

syslog クライアント設定画面から、syslog メッセージ本文テンプレートを作成および編集します。

（注） 各自でカスタマイズしたテンプレートだけを編集できます。システムに用意されている事前定義テンプレートは変更できません。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、次に左側のパネルから [Syslogプロバイダー（Syslog Providers）] を選択します。
[syslog プロバイダー（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを追加するには [追加（Add）] をクリックし、すでに設定されているクライアントを更新するには [編集（Edit）] をクリックします。syslog クライアントの設定と更新については、syslog クライアントの設定 （1111 ページ）を参照してください。

ステップ 3 [syslog プロバイダー（Syslog Providers）] ウィンドウで、[新規（New）] をクリックして新しいメッセージテンプレートを作成します。既存のテンプレートを編集するには、ドロップダウンリストからテンプレートを選択して [編集（Edit）] をクリックします。

ステップ 4 必須フィールドをすべて指定します。

値を正しく入力する方法の詳細については、syslog カスタマイズテンプレートの設定と例 （1119 ページ）を参照してください。

ステップ 5 [テスト（Test）] をクリックして、入力した文字列に基づいてメッセージが正しく解析されていることを確認します。

ステップ 6 [保存（Save）] をクリックします。

syslog ヘッダーのカスタマイズ

syslog ヘッダーには、メッセージの送信元のホスト名も含まれています。syslog メッセージが Cisco ISE メッセージパーサーで認識されない場合は、ホスト名の後に続く区切り文字を設定し、Cisco ISE がホスト名を認識してメッセージを正しく解析できるようにすることで、メッセージヘッダーをカスタマイズする必要がある場合があります。この画面のフィールドの詳細については、syslog カスタマイズテンプレートの設定と例（1119 ページ）を参照してください。カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダー タイプにこの設定が追加されます。

（注） 1 つのヘッダーだけをカスタマイズできます。ヘッダーをカスタマイズした後、[カスタムヘッダー（Custom Header）] をクリックしてテンプレートを作成すると、最新の設定のみが保存されます。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、次に左側のパネルから [Syslogプロバイダー（Syslog Providers）] を選択します。
[syslog プロバイダー（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 [カスタム ヘッダー（Custom Header）] をクリックして [syslog カスタム ヘッダー（Syslog Custom Header）] 画面を開きます。

ステップ 3 [サンプル syslog を貼り付ける（Paste sample syslog）] に、syslog メッセージのヘッダー形式の例を入力します。たとえば、メッセージの 1 つからヘッダー **<181>Oct 10 15:14:08 Cisco.com** をコピーして貼り付けます。

ステップ 4 [区切り文字（Separator）] フィールドで、単語をスペースとタブのいずれで区切るかを指定します。

ステップ 5 [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドで、ヘッダーのどの位置がホスト名であるかを指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。

[ホスト名（Hostname）] フィールドに、最初の 3 つのフィールドに示される詳細情報に基づいてホスト名が表示されます。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。

<181>Oct 10 15:14:08 Cisco.com

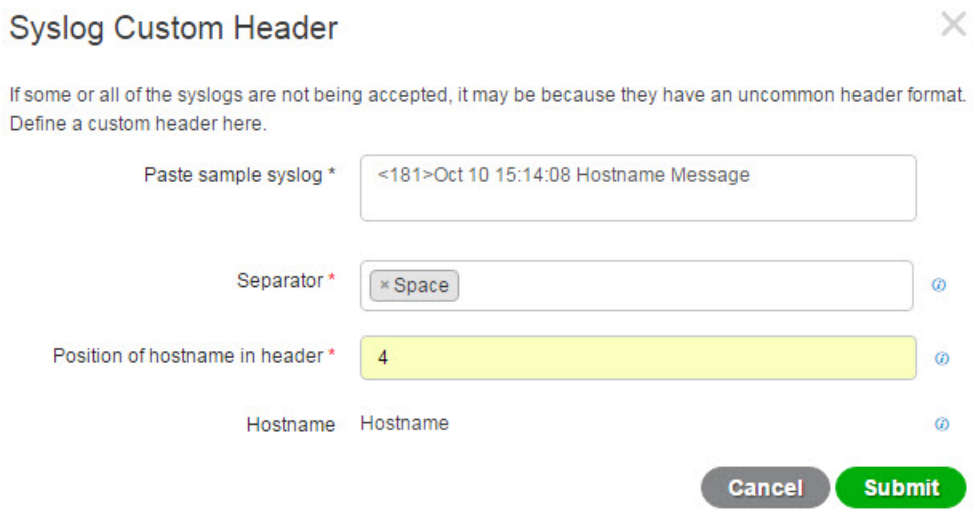
区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。

[ホスト名（Hostname）] には自動的に Cisco.com と表示されます。これは、[syslog の例を貼り付ける（Paste sample syslog）] フィールドに貼り付けたヘッダー フレーズの 4 番目の単語です。

ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

この例を次のスクリーン キャプチャに示します。

図 *23 : syslog* ヘッダーのカスタマイズ



ステップ 6 [送信（Submit）] をクリックします。
カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダータイプにこの設定が追加されます。

syslog カスタマイズ テンプレートの設定と例

Cisco ISE では、パッシブ ID パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます。カスタマイズされたテンプレートは、新規マッピング メッセージとマッピング削除メッセージの両方に対応する構造を決定します。パッシブ ID パーサーが、メッセージがユーザー ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザーの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザー名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されます。カスタマイズテンプレートでも正規表現を使用してください。

syslog ヘッダーの各部分

ホスト名の後に続く区切り文字を設定することで、syslog プローブが認識する単一ヘッダーをカスタマイズできます。

次の表に、カスタム syslog ヘッダーに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 84 : カスタマイズ テンプレートの正規表現（1121 ページ）を参照してください。

表 *82 : syslog* カスタム ヘッダー

フィールド	説明
syslog の例を貼り付ける（Paste sample syslog）	syslog メッセージにヘッダー形式の例を入力します。たとえば、次のヘッダーをコピーして貼り付けます。 `<181>Oct 10 15:14:08 Hostname Message`
区切り文字（Separator）	単語をスペースまたはタブのいずれで区切るかを指定します。
ヘッダーのホスト名の位置（Position of hostname in header）	ヘッダーでのホスト名の位置を指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。

フィールド	説明
ホスト名（Hostname）	最初の 3 つのフィールドに示される詳細情報に基づいて、ホスト名を表示します。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。 <181>Oct 10 15:14:08 Hostname Message 区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。 [ホスト名（Hostname）] には Hostname が自動的に表示されます。 ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

メッセージ本文の syslog テンプレートの各部分と説明

次の表に、カスタマイズ syslog メッセージ テンプレートに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 84 : カスタマイズテンプレートの正規表現（1121 ページ）を参照してください。

表 *83 : syslog* テンプレート

パート	フィールド	説明
	名前	このテンプレートの目的がわかる一意の名前。
マッピング操作	新規マッピング	新しいユーザーを追加するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、F5 VPN にログインした新しいユーザーを示すには、このフィールドに「logged on from」と入力します。
	削除されたマッピング	ユーザーを削除するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、削除する必要がある ASA VPN のユーザーを示すには、このフィールドに「session disconnect」と入力します。

パート	フィールド	説明
ユーザー データ	IPアドレス	キャプチャする IP アドレスを示す正規表現。 たとえば Bluecat メッセージの場合、この IP アドレス範囲内のユーザーの ID をキャプチャするには、次のように入力します。 (?:\b(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))
	ユーザー名	キャプチャするユーザー名形式を示す正規表現。
	ドメイン	キャプチャするドメインを示す正規表現。
	MAC アドレス	キャプチャする MAC アドレスの形式を示す正規表現。

正規表現の例

メッセージを解析するため、正規表現を使用します。ここでは、IPアドレス、ユーザー名、およびマッピング追加メッセージを解析する正規表現の例を示します。

たとえば、正規表現を使用して次のメッセージを解析します。

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

次の表に、正規表現の定義を示します。

表 *84*：カスタマイズ テンプレートの正規表現

パート	正規表現
IPアドレス（IP address）	Address <([^\s]+)>|address ([^\s]+)
ユーザー名（User name）	User <([^\s]+)>| Username = ([^\s]+)
マッピング追加メッセージ（Add mapping message）	(%ASA-4-722051|%ASA-6-713228)

Syslog 事前定義メッセージテンプレートの使用

syslog メッセージには、ヘッダーとメッセージ本文を含む標準構造があります。

ここでは、メッセージの送信元に基づいてサポートされているヘッダーの内容の詳細や、サポートされている本文の構造など、Cisco ISE が提供する事前定義テンプレートについて説明します。

また、システムで事前に定義されていないソース用に、カスタマイズした本文コンテンツを使用した独自のテンプレートも作成できます。ここでは、カスタムテンプレートでサポートされる構造について説明します。メッセージの解析時には、システムで事前定義されているヘッダーに加えて、使用する 1 つのカスタマイズヘッダーを設定できます。また、メッセージ本文には、複数のカスタマイズテンプレートを設定できます。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ（1117 ページ）を参照してください。本文のカスタマイズの詳細については、syslog メッセージ本文のカスタマイズ（1116 ページ）を参照してください。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されており、カスタマイズテンプレートでも正規表現を使用する必要があります。

メッセージ ヘッダー

パーサーで認識されるヘッダータイプには、すべてのクライアントマシンのすべてのメッセージタイプ（新規および削除）について認識される 2 つのタイプがあります。これらのヘッダーは次のとおりです。

- <171>Host message
- <171>Oct 10 15:14:08 Host message

受信されたヘッダーはホスト名を検出するため解析されます。ホスト名は、IP アドレス、ホスト名、または完全 FQDN のいずれかです。

ヘッダーもカスタマイズできます。ヘッダーをカスタマイズするには、syslog ヘッダーのカスタマイズ（1117 ページ）を参照してください。

syslog ASA VPN 事前定義テンプレート

ASA VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用（1122 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

本文メッセージ	解析例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPsec: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	

本文メッセージ	解析例
%ASA-6-113039 Group group User UserA IP 10.0.0.11 agent parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] （注） このメッセージ タイプから解析される IP アドレスは、メッセージに示されているようにプライベート IP アドレスです。
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] （注） このメッセージ タイプから解析された IP アドレスは IPv4 アドレスです。

マッピング削除本文メッセージ

ここではパーサーで ASA VPN のためにサポートされている マッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,10.1.1.1]

本文メッセージ
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number

本文メッセージ
%ASA-6-602304 IPsec: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: Agent not enabled or invalid agent image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

syslog Bluecat 事前定義テンプレート

Bluecat でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）を参照）。

新規マッピング本文メッセージ

ここでは、Bluecat syslog で新規マッピングとしてサポートされるメッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

本文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

マッピング削除メッセージ

Bluecat のマッピング削除メッセージはありません。

syslog F5 VPN 事前定義テンプレート

F5 VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな F5 VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[user=UserA,ip=172.16.0.12]

本文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

マッピング削除メッセージ

現在、F5 VPN でサポートされている削除メッセージはありません。

syslog Infoblox 事前定義テンプレート

Infoblox でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

本文メッセージ
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

マッピング削除メッセージ

受信された本文が解析され、次のようにユーザーの詳細が判明します。

- MAC アドレスが含まれている場合：

  [00:0c:29:a2:18:34,10.0.10.100]

- MAC アドレスが含まれていない場合：

  [10.0.10.100]

本文メッセージ
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

syslog Linux DHCPd3 事前定義テンプレート

Linux DHCPd3 でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）を参照）。

新規マッピング メッセージ

次の表では、パーサーが認識するさまざまな Linux DHCPd3 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

マッピング削除本文メッセージ

ここではパーサーで Linux DHCPd3 のためにサポートされているマッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[00:0c:29:a2:18:34 ,10.0.10.100]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

syslog MS DHCP 事前定義テンプレート

MS DHCP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな MS DHCP 本文メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0

マッピング削除本文メッセージ

ここではパーサーで MS DHCP のためにサポートされているマッピング削除メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

syslog SafeConnect NAC 事前定義テンプレート

SafeConnect NAC でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな SafeConnect NAC 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

本文メッセージ
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

マッピング削除メッセージ

現在、Safe Connect でサポートされている削除メッセージはありません。

syslog Aerohive 事前定義テンプレート

Aerohive でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Aerohive 本文メッセージについて説明します。

本文で解析される詳細には、ユーザー名と IP アドレスがあります。解析に使用される正規表現の例を次に示します。

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,10.5.50.52]

本文メッセージ
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

マッピング削除メッセージ

現在、Aerohive からのマッピング削除メッセージはサポートされていません。

syslog Blue Coat 事前定義テンプレート：Main Proxy、Proxy SG、Squid Web Proxy

Blue Coat の次のメッセージ タイプがサポートされています。

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

BlueCoat メッセージでサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Blue Coat 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,192.168.10.24]

本文メッセージ（この例は、**BlueCoat プロキシ SG** メッセージからの引用です）
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

次の表では、新規マッピング メッセージに使用されるクライアント別の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})|(?:(?:[a-zA-Z0-9]{1,4}\:{1,2}){1,7}[a-zA-Z0-9]{1,4}))\s** ユーザー名 **\s\-\s([a-zA-Z0-9_]+)\s\-\s**

クライアント	正規表現
BlueCoat Proxy SG	新規マッピング **(\-\sPROXIED){1}** IP **\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})|(?:(?:[a-zA-Z0-9]{1,4}\:{1,2}){1,7}[a-zA-Z0-9]{1,4}))\s[a-zA-Z0-9_]+\s\-** ユーザー名 **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid Web Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})|(?:(?:[a-zA-Z0-9]{1,4}\:{1,2}){1,7}[a-zA-Z0-9]{1,4}))\sTCP** ユーザー名 **\s([a-zA-Z0-9\._]+)\s\-\/**

マッピング削除メッセージ

Blue Coat クライアントではマッピング削除メッセージがサポートされていますが、現在利用できる例はありません。

次の表では、マッピング削除メッセージに使用されるクライアント別の既知の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	現在利用できる例はありません。
BlueCoat Squid Web Proxy	**(TCP_MISS|TCP_NC_MISS){1}**

syslog ISE および ACS 事前定義テンプレート

パーサーは ISE または ACS クライアントをリッスンするときに、次のメッセージ タイプを受信します。

- 認証成功：ユーザーが ISE または ACS により認証されると、認証が成功したことを通知し、ユーザーの詳細情報を記述した認証成功メッセージが発行されます。このメッセージが解析され、このメッセージのユーザーの詳細とセッション ID が保存されます。
- アカウンティング開始およびアカウンティング更新メッセージ（新規マッピング）：アカウンティング開始メッセージまたはアカウンティング更新メッセージは、認証成功メッ

セージから保存されたユーザーの詳細とセッション ID を使用して解析され、ユーザーがマッピングされます。

- アカウンティング終了（マッピング削除）：システムからユーザーマッピングが削除されます。

ISE および ACS でサポートされる syslog メッセージの形式とタイプについて説明します。

認証成功メッセージ

認証成功メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- **解析例**

  ユーザー名とセッション ID だけが解析されます。

  [UserA,5]

アカウンティング開始/更新（新規マッピング）メッセージ

新規マッピング メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザー名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

マッピング削除メッセージ

マッピング削除では次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザー名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

syslog Lucent QIP 事前定義テンプレート

Lucent QIP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （1122 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまなLucent QIP本文メッセージについて説明します。

これらのメッセージの正規表現構造を次に示します。

DHCP_GrantLease|:DHCP_RenewLease

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[00:0C:29:91:2E:5D,10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

マッピング削除本文メッセージ

これらのメッセージの正規表現構造を次に示します。

Delete Lease:|DHCP Auto Release:

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

パッシブ ID サービスのフィルタリング

特定のユーザーを名前や IP アドレスに基づいてフィルタリングできます。たとえば IT サービスの管理者が、そのエンドポイントの標準ユーザーを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して[ライブセッション（Live Sessions）]に表示されないようにし、そのエンドポイントの標準ユーザーだけが表示されるようにできます。[ライブ セッション（Live Session）] には、マッピング フィルタでフィルタリングされていないパッシブ ID サービス コンポーネントが表示されます。フィルタは必要なだけ追加できます。「OR」論理演算子をフィルタの間に適用します。両方のフィールドを 1 つのフィルタで指定する場合は、「AND」論理演算子をこれらのフィールドの間に適用します。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [マッピング フィルタ（Mapping Filters）] を選択します。

ステップ 2 **[プロバイダー（Providers）]** > **[マッピング フィルタ（Mapping Filters）]** を選択します。

ステップ 3 [追加（Add）] をクリックし、フィルタするユーザーのユーザー名や IP アドレスを入力して、[送信（Submit）] をクリックします。

ステップ 4 現在モニタリングセッションディレクトリにログインしているフィルタリングされていないユーザーを表示するには、**[操作（Operations）]** > **[RADIUSライブログ（RADIUS Livelog）]** を選択します。

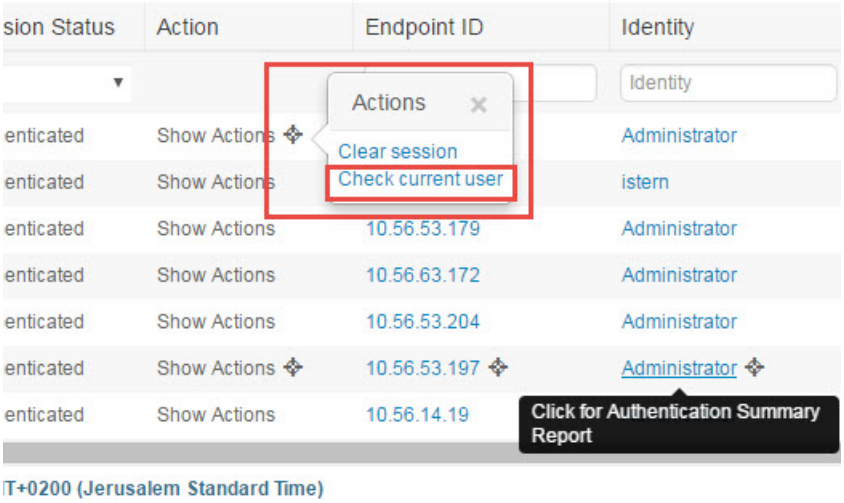
エンドポイント プローブ

設定可能なカスタム プロバイダーの他に、パッシブ ID サービス がアクティブになると ISE でエンドポイント プローブが有効になります。エンドポイント プローブは、特定の各ユーザーがまだシステムにログインしているかどうかを定期的にチェックします。

（注） エンドポイントがバックグラウンドで実行されることを確認するには、まず最初の Active Directory 参加ポイントを設定し、[クレデンシャルの保存（Store Credentials）] を選択していることを確認します。エンドポイントプローブの設定の詳細については、エンドポイントプローブの使用 （1136 ページ）を参照してください。

エンドポイントのステータスを手動で確認するには、[アクション（Actions）] 列から [ライブセッション（Live Sessions）] に移動し、[アクションを表示（Show Actions）] をクリックし、次の図に示すように [現在のユーザーを確認（Check current user）] を選択します。

図 *24* : 現在のユーザーを確認（*Check current user*）



エンドポイントユーザーのステータスと手動でのチェックの実行の詳細については、RADIUS ライブ セッション （778 ページ）を参照してください。

エンドポイントプローブはユーザーが接続していることを認識します。特定のエンドポイントのセッションが最後に更新された時点から 4 時間経過している場合には、ユーザーがまだログインしているかどうかを確認し、次のデータを収集します。

- MAC アドレス
- オペレーティング システムのバージョン

このチェックに基づいてプローブは次の操作を実行します。

- ユーザーがまだログインしている場合、プローブは Cisco ISE を [アクティブユーザー（Active User）] ステータスで更新します。
- ユーザーがログアウトしている場合、セッション状態は [終了（Terminated）] に更新され、15 分経過後にユーザーはセッション ディレクトリから削除されます。

- ユーザーと通信できない場合、たとえばファイアウォールによって通信が防止されているか、エンドポイントがシャットダウンしている場合などには、ステータスが [到達不可能（Unreachable）] として更新され、サブスクライバポリシーによってユーザーセッションの処理方法が決定します。エンドポイントは引き続きセッション ディレクトリに残ります。

エンドポイント プローブの使用

始める前に

サブネット範囲に基づいてエンドポイント プローブを作成および有効にできます。PSN ごとに1つのエンドポイントプローブを作成できます。エンドポイントプローブを使用するには、次のように設定していることを確認してください。

- エンドポイントはポート 445 とのネットワーク接続が必要です。
- ISE から 1 番目の Active Directory 参加ポイントを設定し、プロンプトが表示されたら [クレデンシャルの選択（Select Credentials）] を選択してください。参加ポイントの詳細については、プローブおよびプロバイダーとしての Active Directory （1085 ページ）を参照してください。

（注） エンドポイントがバックグラウンドで実行するようにするため、最初に 1 番目の Active Directory 参加ポイントを設定する必要があります。これにより、Active Directory プローブが完全に設定されていない場合でもエンドポイントプローブを実行できるようになります。

ステップ 1 **[ワーク センター（Work Centers）] > [パッシブ ID（Passive ID）] > [プロバイダー（Providers）]** を選択し、[エンドポイント プローブ（Endpoint Probes）] を選択します。

ステップ 2 新しいエンドポイント プローブを作成するには、[追加（Add）] をクリックします。

ステップ 3 必須フィールドに入力し、[ステータス（Status）] フィールドで [有効化（Enable）] を選択していることを確認してから、[送信（Submit）] をクリックします。詳細については、エンドポイントプローブ設定 （1136 ページ）を参照してください。

エンドポイント プローブ設定

サブネット範囲に基づいて PSN ごとに 1 つのエンドポイント プローブを作成します。展開で複数の PSN を使用している場合は、個別のサブネットのセットに各 PSN を割り当てることができます。

表 *85 :* エンドポイント プローブ設定

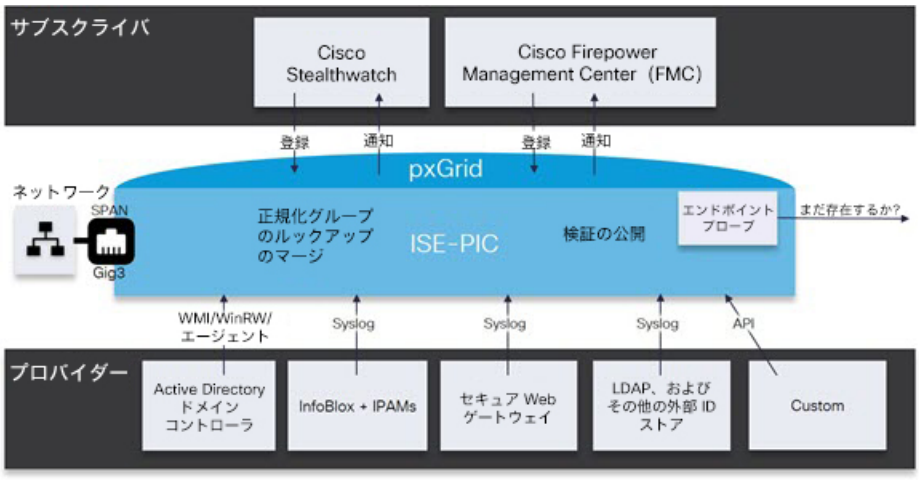
フィールド名	説明
名前（**Name**）	このプローブの用途を示す一意の名前を入力します。
説明（**Description**）	このプローブの用途を示す一意の説明を入力します。
ステータス（**Status**）	このプローブをアクティブにするには [有効化（Enable）] を選択します。
ホスト名（**Host Name**）	展開で使用可能な PSN のリストから、このプローブの PSN を選択します。
サブネット（**Subnets**）	このプローブがチェックする必要があるエンドポイントのグループのサブネット範囲を入力します。標準のサブネット マスク範囲と、カンマで区切ったサブネット アドレスを使用します。 例：10.56.14.111/32,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 各範囲は一意である必要があり、相互に重複していてはなりません。たとえば、範囲 2.2.2.0/16,2.2.3.0/16 は相互に重複しているため、同一プローブに対して入力できません。

サブスクライバ

パッシブ ID サービス は、さまざまなプロバイダーから収集し、Cisco ISE セッション ディレクトリにより保存された認証済みユーザー ID を、Cisco Stealthwatch や Cisco Firepower Management Center（FMC）などのその他のネットワーク システムに送信するため、Cisco pxGrid サービスを使用します。

次の図では、pxGrid ノードが外部プロバイダーからユーザー ID を収集しています。これらの ID は解析、マッピング、およびフォーマットされます。pxGrid はこれらのフォーマット済みのユーザー ID を取得し、パッシブ ID サービス サブスクライバに送信します。

図 *25 :* パッシブ *ID* サービス フロー



Cisco ISE に接続するサブスクライバは、pxGrid サービスの使用を登録する必要があります。サブスクライバは、クライアントになるために pxGrid SDK を介してシスコから使用可能な pxGrid クライアント ライブラリを採用する必要があります。サブスクライバは、一意の名前と証明書ベースの相互認証を使用して pxGrid にログインできます。Cisco pxGrid サブスクライバは、有効な証明書を送信すると、ISE により自動的に承認されます。

サブスクライバは設定されている pxGrid サーバーのホスト名または IP アドレスのいずれかに接続できます。不必要なエラーが発生することを防ぎ、DNS クエリが適切に機能するようにするため、ホスト名を使用することが推奨されます。公開および登録するためにサブスクライバの pxGrid で作成される、情報トピックまたはチャネル機能があります。Cisco ISE では SessionDirectory と IdentityGroup だけがサポートされています。機能情報は、公開、ダイレクトクエリ、または一括ダウンロードクエリによりパブリッシャから取得でき、[機能（Capabilities）] タブの [サブスクライバ（Subscribers）] で確認できます。

サブスクライバが ISE から情報を受信できるようにするには、次の操作を行います。

1. 必要に応じて、サブスクライバ側から証明書を生成します。
2. PassiveID ワーク センターからサブスクライバの pxGrid 証明書の生成 （1138 ページ）を参照してください。
3. サブスクライバの有効化 （1140 ページ）。サブスクライバが ISE からユーザー ID を受信できるようにするため、このステップを実行するか、承認を自動的に有効にします。サブスクライバの設定 （1141 ページ）を参照してください。

サブスクライバの pxGrid 証明書の生成

始める前に

pxGrid とサブスクライバの間の相互信頼を保証するため、pxGrid サブスクライバの証明書を生成できます。これにより、ISE からサブスクライバにユーザー ID を渡すことが可能になりま

す。次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[サブスクライバ（Subscribers）]** を選択し、[証明書（Certificates）] タブに移動します。

ステップ 2 [処理の選択（I want to）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- [単一の証明書の生成（証明書署名要求なし）（Generate a single certificate without a certificate signing request）]：このオプションを選択した場合は、共通名（CN）を入力する必要があります。[コモンネーム（Common Name）] フィールドに、pxGrid をプレフィックスとして含む pxGrid FQDN を入力します。たとえば www.pxgrid-ise.ise.net です。あるいはワイルドカードを使用します。たとえば *.ise.net です。
- [単一の証明書の生成（証明書署名要求あり）（Generate a single certificate with a certificate signing request）]：このオプションを選択した場合は、証明書署名要求の詳細を入力する必要があります。
- [一括証明書の生成（Generate bulk certificates）]：必要な詳細を含む CSV ファイルをアップロードすることができます。
- [ルート証明書チェーンのダウンロード（Download root certificate chain）]：pxGrid クライアントの信頼できる証明書ストアに追加するために、ISE 公開ルート証明書をダウンロードします。ISE pxGrid ノードは、新規に署名された pxGrid クライアント証明書だけを信頼します（あるいはこの逆）。これにより、外部の認証局を使用する必要がなくなります。

ステップ 3 （オプション）この証明書の説明を入力できます。

ステップ 4 この証明書のベースとなる pxGrid 証明書テンプレートを表示または編集します。証明書テンプレートには、そのテンプレートに基づいて認証局（CA）によって発行されたすべての証明書に共通のプロパティが含まれています。証明書テンプレートは、件名、サブジェクト代替名（SAN）、キー タイプ、キー サイズ、使用する必要がある SCEP RA プロファイル、証明書の有効期間、証明書がクライアントまたはサーバーの認証またはその両方に使用される必要があるかどうかを指定した拡張キーの使用状況（EKU）を定義します。内部 Cisco ISE CA（ISE CA）は、証明書テンプレートを使用し、そのテンプレートに基づいて証明書を発行します。このテンプレートを編集するには、**[管理（Administration）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[証明書テンプレート（Certificate Templates）]** を選択します。

ステップ 5 サブジェクト代替名（SAN）を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- [FQDN]：ISE ノードの完全修飾ドメイン名を入力します。たとえば www.isepic.ise.net です。あるいは FQDN にワイルドカードを使用します。たとえば *.ise.net です。

  pxGrid FQDN も入力できる追加の行を FQDN に追加できます。これは [コモンネーム（Common Name）] フィールドで使用する FQDN と同一である必要があります。

- [IP アドレス（IP address）]：この証明書に関連付ける ISE ノードの IP アドレスを入力します。サブスクライバが FQDN ではなく IP アドレスを使用する場合には、この情報を入力する必要があります。

（注） このフィールドは、[一括証明書の生成（Generate bulk certificates）] オプションを選択している場合には表示されません。

ステップ 6 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- [Private Enhanced Electronic Mail（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）（Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)）]：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY----」タグで終わります。
- [PKCS12 形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル）（PKCS12 format (including certificate chain; one file for both the certificate chain and key)）]：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンドエンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成（Create）] をクリックします。

サブスクライバの有効化

サブスクライバが Cisco ISE からユーザー ID を受信できるようにするため、このタスクを実行するか、または承認を自動的に有効にする必要があります。サブスクライバの設定（1141 ページ）を参照してください。

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- パッシブ ID サービスを有効にします。詳細については、Easy Connect（1077 ページ）を参照してください。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[サブスクライバ（Subscribers）]** を選択し、[クライアント（Clients）] タブが表示されることを確認します。

ステップ 2 サブスクライバの隣にあるチェックボックスをオンにして [承認（Approve）] をクリックします。

ステップ 3 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

ライブ ログからのサブスクライバ イベントの表示

[ライブ ログ（Live Logs）] ページにはすべてのサブスクライバ イベントが表示されます。イベント情報には、イベント タイプ、タイムスタンプ、サブスクライバ名、機能名が含まれています。

[サブスクライバ（Subscribers）] に移動し、[ライブ ログ（Live Log）] タブを選択し、イベント リストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

サブスクライバの設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** > **[設定（Settings）]** を選択します。

ステップ 2 必要に応じて、次のオプションを選択します。

- [新しいアカウントの自動承認（Automatically Approve New Accounts）]：このチェックボックスをオンにすると、新しい pxGrid クライアントからの接続要求が自動的に承認されます。
- [パスワードベースのアカウント作成の許可（Allow Password Based Account Creation）]：このチェックボックスをオンにすると、pxGrid クライアントのユーザー名/パスワードベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

  pxGrid クライアントは、REST API を介してユーザー名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

ステップ 3 [保存（Save）] をクリックします。

PassiveID ワーク センター でのサービスのモニタリングとトラブルシューティング

モニタリング、トラブルシューティング、およびレポーティングの各ツールを使用して PassiveID ワーク センター を管理する方法について説明します。

- RADIUS ライブ セッション （778 ページ）
- 『』の「レポート」のセクションを参照してください。
- 着信トラフィックを検証する TCP ダンプユーティリティ （2020 ページ）

LDAP

Lightweight Directory Access Protocol（LDAP）は、RFC 2251 で定義されている、TCP/IP 上で動作するディレクトリ サービスの問い合わせおよび変更のためのネットワーキング プロトコルです。LDAP は、X.500 ベースのディレクトリ サーバーにアクセスするためのライトウェイト メカニズムです。

Cisco ISE は、LDAP プロトコルを使用して LDAP 外部データベース（ID ソースとも呼ばれる）と統合します。

LDAP ディレクトリ サービス

LDAP ディレクトリ サービスは、クライアント/サーバー モデルに基づきます。クライアントは、LDAP サーバーに接続し、操作要求をサーバーに送信することで、LDAP セッションを開始します。サーバーは、応答を送信します。1 台以上の LDAP サーバーに、LDAP ディレクトリ ツリーまたは LDAP バックエンド データベースからのデータが含まれています。

ディレクトリ サービスは、情報を保持するデータベースであるディレクトリを管理します。ディレクトリ サービスは、情報を保存するために分散モデルを使用します。その情報は、通常はディレクトリ サーバー間で複製されます。

LDAP ディレクトリは、単純なツリー階層で編成されており、数多くのサーバー間で分散できます。各サーバーには、定期的に同期化されるディレクトリ全体の複製バージョンを配置できます。

ツリーのエントリには属性のセットが含まれており、各属性には名前（属性タイプまたは属性の説明）と 1 つ以上の値があります。属性はスキーマに定義されます。

各エントリには、固有識別情報、つまり識別名（DN）があります。この名前には、エントリ内の属性で構成されている相対識別名（RDN）と、それに続く親エントリの DN が含まれています。DN は完全なファイル名、RDN はフォルダ内の相対ファイル名と考えることができます。

複数の LDAP インスタンス

IP アドレスまたはポートの設定が異なる複数の LDAP インスタンスを作成することにより、異なる LDAP サーバーを使用するか、または同じ LDAP サーバー上の異なるデータベースを使用して認証を行うように、Cisco ISE を設定できます。プライマリ サーバーの各 IP アドレスおよびポートの設定は、セカンダリ サーバーの IP アドレスおよびポートの設定とともに、Cisco ISE LDAP ID ソース インスタンスに対応する LDAP インスタンスを形成します。

Cisco ISE では、個々の LDAP インスタンスが一意の LDAP データベースに対応している必要はありません。複数の LDAP インスタンスを、同一のデータベースにアクセスするように設定できます。この方法は、LDAP データベースにユーザーまたはグループのサブツリーが複数含まれている場合に役立ちます。各 LDAP インスタンスでは、ユーザーとグループに対してそれぞれ単一のサブツリー ディレクトリだけをサポートするため、Cisco ISE が認証要求を送信す

るユーザー ディレクトリとグループ ディレクトリのサブツリーの組み合わせごとに、別々の LDAP インスタンスを設定する必要があるからです。

LDAP フェールオーバー

Cisco ISE は、プライマリ LDAP サーバーとセカンダリ LDAP サーバー間でのフェールオーバーをサポートします。フェールオーバーは、LDAP サーバーがダウンしているかまたは到達不可能なために Cisco ISE で LDAP サーバーに接続できないことが原因で認証要求が失敗した場合に発生します。

フェールオーバー設定が指定され、Cisco ISE で接続しようとした最初の LDAP サーバーが到達不可能な場合、Cisco ISE は常に 2 番目の LDAP サーバーへの接続を試行します。再度、Cisco ISE で最初の LDAP サーバーを使用する場合は、[フェールバック再試行の遅延（Failback Retry Delay）] テキスト ボックスに値を入力する必要があります。

（注） Cisco ISE では、常にプライマリ LDAP サーバーを使用して、認証ポリシーで使用するグループと属性を管理者ポータルから取得します。このため、プライマリ LDAP サーバーはこれらの項目を設定するときにアクセス可能である必要があります。Cisco ISE では、フェールオーバーの設定に従って、実行時に認証と許可にのみセカンダリ LDAP サーバーを使用します。

LDAP 接続管理

Cisco ISE では、複数の同時 LDAP 接続がサポートされます。接続は、最初の LDAP 認証時にオンデマンドで開かれます。最大接続数は、LDAP サーバーごとに設定されます。事前に接続を開いておくと、認証時間が短縮されます。同時バインディング接続に使用する最大接続数を設定できます。開かれる接続の数は、LDAP サーバー（プライマリまたはセカンダリ）ごとに異なる場合があり、サーバーごとに設定される最大管理接続数に基づいて決まります。

Cisco ISE は、Cisco ISE で設定されている LDAP サーバーごとに、開いている LDAP 接続（バインディング情報を含む）のリストを保持します。認証プロセス中に、Connection Manager は開いている接続をプールから検索しようとします。開いている接続が存在しない場合、新しい接続が開かれます。

LDAP サーバーが接続を閉じた場合、Connection Manager はディレクトリを検索する最初のコールでエラーをレポートし、接続を更新しようとします。認証プロセスが完了した後、Connection Manager は接続を解放します。

LDAP ユーザー認証

LDAP を外部 ID ストアとして設定できます。Cisco ISE はプレーン パスワード認証を使用します。ユーザー認証には次の処理が含まれます。

- LDAP サーバーでの、要求のユーザー名に一致するエントリの検索
- ユーザー パスワードと、LDAP サーバーで見つかったパスワードとの照合

- ポリシーで使用するグループ メンバーシップ情報の取得
- ポリシーおよび許可プロファイルで使用するように指定された属性の値の取得

ユーザーを認証するために、Cisco ISE は LDAP サーバーにバインド要求を送信します。バインド要求には、ユーザーの DN およびユーザー パスワードがクリア テキストで含まれています。ユーザーの DN およびパスワードが LDAP ディレクトリ内のユーザー名およびパスワードと一致した場合に、ユーザーは認証されます。

Active Directory が LDAP として使用されている場合は、UPN 名がユーザー認証に使用されます。Sun ONE Directory Server が LDAP として使用されている場合は、SAM 名がユーザー認証に使用されます。

（注）
- Cisco ISE は、ユーザー認証ごとに 2 つの searchRequest メッセージを送信します。これは、Cisco ISE の許可またはネットワークのパフォーマンスに影響しません。2 番目の LDAP 要求では、Cisco ISE が正しい ID と通信していることを確認します。
- DNS クライアントとしての Cisco ISE は、DNS 応答で返された最初の IP のみを使用して、LDAP バインドを実行します。

Secure Sockets Layer（SSL）を使用して LDAP サーバーへの接続を保護することを推奨します。

（注） パスワードの変更は、パスワードの有効期限が切れた後にアカウントの残りの猶予ログインがあるときにのみ、LDAP でサポートされます。パスワードが正常に変更された場合、LDAP サーバーの bindResponse は LDAP_SUCCESS であり、bindResponse メッセージに残りの猶予ログインの制御フィールドが含まれます。bindResponse メッセージにさらなる制御フィールド（残りの猶予ログイン以外）が含まれる場合は、Cisco ISE がメッセージを復号できない可能性があります。

許可ポリシーで使用する LDAP グループおよび属性の取得

Cisco ISE は、ディレクトリ サーバーでバインド操作を実行し、サブジェクトを検索および認証することによって、LDAP ID ソースに対してサブジェクト（ユーザーまたはホスト）を認証できます。認証が成功した後、Cisco ISE は、要求された場合、常にサブジェクトに所属するグループおよび属性を取得できます。Cisco ISE 管理者ポータルで取得されるように属性を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[LDAP]** を選択します。Cisco ISE は、これらのグループおよび属性を使用してサブジェクトを許可できます。

ユーザーの認証または LDAP ID ソースの問い合わせを行うために、Cisco ISE は LDAP サーバーに接続し、接続プールを保持します。

Active Directory が LDAP ストアとして設定されている場合は、グループ メンバーシップに関する次の制限事項に注意する必要があります。

- ユーザーまたはコンピュータは、ポリシー条件でポリシールールに一致するように定義されたグループの直接的なメンバーである必要があります。
- 定義されたグループは、ユーザーまたはコンピュータのプライマリ グループではない可能性があります。この制限は、Active Directory が LDAP ストアとして設定されている場合にのみ適用されます。

LDAP グループ メンバーシップ情報の取得

ユーザー認証、ユーザー ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからグループ メンバーシップ情報を取得する必要があります。LDAP サーバーは、サブジェクト（ユーザーまたはホスト）とグループ間の関連付けを次の方法のいずれかで表します。

- [グループがサブジェクトを参照（Groups Refer to Subjects）]：グループオブジェクトには、サブジェクトを指定する属性が含まれています。サブジェクトの識別子は、次のものとしてグループに供給できます。
  - 識別名
  - プレーン ユーザー名
- [サブジェクトがグループを参照（Subjects Refer to Groups）]：サブジェクトオブジェクトには、所属するグループを指定する属性が含まれています。

LDAP ID ソースには、グループ メンバーシップ情報の取得のために次のパラメータが含まれています。

- [参照方向（Reference direction）]：このパラメータは、グループメンバーシップを決定するときに使用する方法を指定します（グループからサブジェクトへまたはサブジェクトからグループへ）。
- [グループマップ属性（Group Map Attribute）]：このパラメータは、グループメンバーシップ情報を含む属性を示します。
- [グループオブジェクトクラス（Group Object Class）]：このパラメータは、特定のオブジェクトがグループとして認識されることを決定します。
- [グループ検索サブツリー（Group Search Subtree）]：このパラメータは、グループ検索の検索ベースを示します。
- [メンバータイプオプション（Member Type Option）]：このパラメータは、グループメンバー属性にメンバーが保存される方法を指定します（DN またはプレーンユーザー名のいずれかとして）。

LDAP 属性の取得

ユーザー認証、ユーザー ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからサブジェクト属性を取得する必要があります。LDAP ID ソース

のインスタンスごとに、ID ソース ディクショナリが作成されます。これらのディレクトリでは、次のデータ型の属性がサポートされています。

- 文字列
- 符号なし 32 ビット整数
- IPv4 アドレス

符号なし整数および IPv4 属性の場合、Cisco ISE は取得した文字列を対応するデータ型に変換します。変換が失敗した場合、または属性の値が取得されなかった場合、Cisco ISE ではデバッグ メッセージをロギングしますが、認証またはルックアップ プロセスは失敗しません。

変換が失敗した場合、または Cisco ISE で属性の値が取得されない場合に、Cisco ISE で使用できるデフォルトの属性値を任意で設定できます。

LDAP 証明書の取得

ユーザー ルックアップの一部として証明書取得を設定した場合、Cisco ISE は証明書属性の値を LDAP から取得する必要があります。証明書属性の値を LDAP から取得するには、LDAP ID ソースの設定時に、アクセスする属性のリストで証明書属性をあらかじめ設定しておく必要があります。

LDAP サーバーによって返されるエラー

次のエラーが認証プロセス中に発生する可能性があります。

- 認証エラー：Cisco ISE は、認証エラーを Cisco ISE ログ ファイルに記録します。

  LDAP サーバーがバインディング（認証）エラーを返す理由で考えられるのは、次のとおりです。

  - パラメータ エラー：無効なパラメータが入力された
  - ユーザーアカウントが制限されている（無効、ロックアウト、期限切れ、パスワード期限切れなど）
  - 初期化エラー：LDAP サーバーのタイムアウト設定を使用して、LDAP サーバーでの接続または認証が失敗したと判断する前に Cisco ISE が LDAP サーバーからの応答を待つ秒数を設定します。

    LDAP サーバーが初期化エラーを返す理由で考えられるのは、次のとおりです。

    - LDAP がサポートされていない。
    - サーバーがダウンしている。
    - サーバーがメモリ不足である。
    - ユーザーに特権がない。
    - 間違った管理者クレデンシャルが設定されている。

外部リソースエラーとして次のエラーがロギングされ、LDAPサーバーで考えられる問題が示されます。

- 接続エラーが発生した
- タイムアウトが期限切れになった
- サーバーがダウンしている
- サーバーがメモリ不足である

未知ユーザー エラーとして次のエラーがロギングされます。

- データベースにユーザーが存在しない

ユーザーは存在するが送信されたパスワードが無効である場合、無効パスワードエラーとして次のエラーがロギングされます。

- 無効なパスワードが入力された

LDAP ユーザー ルックアップ

Cisco ISE は LDAP サーバーを使用したユーザー ルックアップ機能をサポートしています。この機能を使用すると、認証なしでLDAPデータベース内のユーザーを検索し、情報を取得できます。ユーザー ルックアップ プロセスには次のアクションが含まれます。

- LDAP サーバーでの、要求のユーザー名に一致するエントリの検索
- ポリシーで使用するユーザー グループ メンバーシップ情報の取得
- ポリシーおよび許可プロファイルで使用するように指定された属性の値の取得

LDAP MAC アドレス ルックアップ

Cisco ISE はMACアドレス ルックアップ機能をサポートしています。この機能を使用すると、認証なしで LDAP データベース内の MAC アドレスを検索し、情報を取得できます。MAC アドレス ルックアップ プロセスには次のアクションが含まれます。

- デバイスの MAC アドレスと一致するエントリの LDAP サーバーの検索
- ポリシーで使用するデバイスの MAC アドレス グループ情報の取得
- ポリシーで使用する指定された属性の値の取得

LDAP ID ソースの追加

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- Cisco ISE は、許可ポリシーで使用するグループおよび属性を取得するためにプライマリ LDAP サーバーを常に使用します。このため、プライマリ LDAP サーバーはこれらの項目を設定するときに到達可能である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [LDAP] > [追加（Add）]** を選択します。

ステップ 2 値を入力します。

ステップ 3 [送信（Submit）] をクリックして、LDAP インスタンスを作成します。

LDAP ID ソースの設定

次の表では、[LDAP ID ソース（LDAP Identity Sources）] ウィンドウのフィールドについて説明します。これらのフィールドを使用して LDAP インスタンスを作成し、これに接続します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** です。

LDAP 一般設定

以下の表では、[一般（General）] タブのフィールドについて説明します。

表 *86 : LDAP* 一般設定

フィールド名	使用上のガイドライン
名前（**Name**）	LDAP インスタンスの名前を入力します。この値は、サブジェクト DN および属性を取得するために検索で使用されます。この値は string 型で、最大長は 64 文字です。
説明（**Description**）	LDAP インスタンスの説明を入力します。この値は string 型で、最大長は 1024 文字です。

フィールド名	使用上のガイドライン
スキーマ（**Schema**）	次の組み込みのスキーマ タイプのいずれかを選択するか、カスタム スキーマを作成できます。 • Active Directory • Sun Directory Server • Novell eDirectory [スキーマ（Schema）]の隣の矢印をクリックすると、スキーマの詳細を表示できます。 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。
（注） 次のフィールドは、カスタム スキーマを選択した場合にのみ編集できます。	
サブジェクト オブジェクト クラス（**Subject Objectclass**）	サブジェクト DN および属性を取得するために検索で使用する値を入力します。この値は string 型で、最大長は 256 文字です。
サブジェクト名属性（**Subject Name Attribute**）	要求内のユーザー名を含む属性の名前を入力します。この値は string 型で、最大長は 256 文字です。 （注） 構成されているサブジェクト名属性は、外部 ID ストア内のインデックス付きのものである必要があります。
グループ名属性（**Group Name Attribute**）	• CN：共通名に基づいて LDAP ID ストアグループを取得します。 • DN：識別名に基づいて LDAP ID ストアグループを取得します。
証明書属性（**Certificate Attribute**）	証明書定義を含む属性を入力します。証明書ベースの認証の場合、クライアントによって提示された証明書を検証するために、これらの定義が使用されます。
グループ オブジェクト クラス（**Group Objectclass**）	グループとして認識されるオブジェクトを指定するために、検索に使用する値を入力します。この値は string 型で、最大長は 256 文字です。
グループ マップ属性（**Group Map Attribute**）	マッピング情報を含む属性を指定します。この属性は、選択した参照方向に基づいて、ユーザーまたはグループ属性を指定できます。

フィールド名	使用上のガイドライン
サブジェクト オブジェクトにグループへの参照が含まれる（**Subject Objects Contain Reference To Groups**）	所属するグループを指定する属性がサブジェクトオブジェクトに含まれている場合は、このオプションをクリックします。
グループ オブジェクトにサブジェクトへの参照が含まれる（**Group Objects Contain Reference To Subjects**）	サブジェクトを指定する属性がグループオブジェクトに含まれている場合は、このオプションをクリックします。この値はデフォルト値です。
グループ内のサブジェクトをメンバー属性に保存（**Subjects In Groups Are Stored In Member Attribute As**）	[グループオブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）] オプションを有効にした場合に限り使用可能）グループメンバー属性にメンバーが供給される方法を指定します（デフォルトは DN）。
ユーザー情報属性（**User Info Attributes**）	デフォルトでは、事前設定された属性が次の組み込みのスキーマ タイプのユーザー情報（名、姓、電子メール、電話、地域など）を収集するために使用されます。 • Active Directory • Sun Directory Server • Novell eDirectory 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。 [スキーマ（Schema）] ドロップダウン リストから [カスタム（Custom）] オプションを選択し、要件に基づいてユーザー情報の属性を編集することもできます。

（注） 構成されているサブジェクト名属性は、外部 ID ストア内のインデックス付きのものである必要があります。

LDAP の接続設定

以下の表では、[接続設定（Connection Settings）] タブのフィールドについて説明します。

表 *87 : LDAP* の接続設定

フィールド名	使用上のガイドライン
セカンダリ サーバーの有効化（**Enable Secondary Server**）	プライマリ LDAP サーバーに障害が発生した場合にバックアップとして使用するセカンダリ LDAP サーバーを有効にする場合は、このオプションをオンにします。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバーの設定パラメータを入力する必要があります。
プライマリ サーバーとセカンダリ サーバー（**Primary and Secondary Servers**）	
ホスト名/IP（**Hostname/IP**）	LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。
ポート（**Port**）	LDAP サーバーがリッスンしている TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバーの管理者からポート番号を取得できます。
各 ISE ノードのサーバーの指定（**Specify server for each ISE node**）	プライマリおよびセカンダリ LDAP サーバーの hostnames/IP および各 PSN のポートを設定するには、このチェック ボックスをオンにします。 このオプションを有効にすると、導入のすべてのノードを表示するテーブルが表示されます。ノードを選択し、プライマリおよびセカンダリ LDAP サーバーの hostname/IP および選択したノードのポートを設定する必要があります。
アクセス（**Access**）	**[匿名アクセス（Anonymous Access）]** : LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバーではクライアントが区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへの、クライアント読み取りアクセスが許可されます。認証情報をサーバーに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。 **[認証されたアクセス（Authenticated Access）]** : LDAP ディレクトリの検索が管理者のログイン情報によって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。

フィールド名	使用上のガイドライン
管理者 DN（**Admin DN**）	管理者の DN を入力します。管理者 DN は、[ユーザー ディレクトリ サブツリー（User Directory Subtree）] 下のすべての必要なユーザーの検索およびグループの検索を行う権限を持つLDAPアカウントです。指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、該当 LDAP サーバーで認証されたユーザーのグループ マッピングは失敗します。
パスワード（**Password**）	LDAP 管理者アカウントのパスワードを入力します。
セキュアな認証（**Secure Authentication**）	SSL を使用して Cisco ISE とプライマリ LDAP サーバー間の通信を暗号化する場合にクリックします。[ポート（Port）] フィールドにLDAPサーバーでのSSLに使用されるポート番号が入力されていることを確認します。このオプションを有効にした場合は、ルート CA を選択する必要があります。
LDAPサーバーのルート CA（**LDAP Server Root CA**）	ドロップダウンリストボックスから信頼できるルート認証局を選択して、証明書による安全な認証を有効にします。
サーバー タイムアウト（**Server timeout**）	プライマリLDAPサーバーでの接続または認証が失敗したと判断する前に Cisco ISE がプライマリ LDAP サーバーからの応答を待つ秒数を入力します。有効な値は 1 ～ 99 です。デフォルトは 10 です。
最大管理接続（**Max. Admin Connections**）	特定のLDAP設定に対して実行できるLDAP管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、ユーザー ディレクトリ サブツリーおよびグループ ディレクトリ サブツリーの下にあるユーザーおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です。デフォルトは 20 です。
N秒ごとに再接続（**Force reconnect every N seconds**）	このチェックボックスをオンにし、[秒（Seconds）] フィールドに、サーバーを指定された間隔でLDAP接続を更新するための適切な値を入力します。有効な範囲は 1 ～ 60 分です。
サーバーへのバインドをテスト（**Test Bind To Server**）	LDAP サーバーの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバーの詳細を編集して再テストします。
フェールオーバー（**Failover**）	

フィールド名	使用上のガイドライン
常にプライマリ サーバーに最初にアクセスする（**Always Access Primary Server First**）	Cisco ISE の認証と認可のために常にプライマリ LDAP サーバーに最初にアクセスするように設定するには、このオプションをクリックします。
経過後にプライマリ サーバーにフェールバック（**Failback to Primary Server After**）	Cisco ISE で接続しようとしたプライマリ LDAP サーバーが到達不可能な場合、Cisco ISE はセカンダリ LDAP サーバーへの接続を試行します。Cisco ISE に再びプライマリ LDAP サーバーを使用するように設定するには、このオプションをクリックし、テキスト ボックスに値を入力します。

[LDAP] の [ディレクトリ構成（Directory Organization）] タブ

次の表では、[ディレクトリ構成（Directory Organization）] タブのフィールドについて説明します。

表 *88 : [LDAP]* の *[*ディレクトリ構成（*Directory Organization*）*]* タブ

フィールド名	使用上のガイドライン
サブジェクト検索ベース（**Subject Search Base**）	すべてのサブジェクトを含むサブツリーの DN を入力します。次に例を示します。 o=corporation.com サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

フィールド名	使用上のガイドライン
グループ検索ベース（Group Search Base）	すべてのグループを含むサブツリーの DN を入力します。次に例を示します。 ou = 組織ユニット、ou = 次の組織ユニット、o = corporation.com グループを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。
形式での MAC アドレスの検索（Search for MAC Address in Format）	LDAP データベースでの検索に使用する、Cisco ISE の MAC アドレス形式を入力します。内部 ID ソースの MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で供給されます。LDAP データベースの MAC アドレスは、異なる形式で供給できます。ただし、Cisco ISE でホスト ルックアップ要求が受信されると、MAC アドレスは内部形式からこのフィールドで指定した形式に変換されます。 ドロップダウン リストを使用して、特定の形式での MAC アドレスの検索を有効にします。<*format*> は次のいずれかです。 • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 選択する形式は、LDAP サーバーに供給されている MAC アドレスの形式と一致している必要があります。

フィールド名	使用上のガイドライン
サブジェクト名の先頭から最後に出現する区切り文字まで削除（Strip start of subject name up to the last occurrence of the separator）	ユーザー名からドメインプレフィックスを削除するための適切なテキストを入力します。 ユーザー名の中でこのフィールドに指定した区切り文字が Cisco ISE で検出されると、そのユーザー名の初めから区切り文字までのすべての文字が削除されます。ユーザー名に、<start_string> ボックスに指定した文字が複数含まれている場合は、Cisco ISE によって最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザー名が DOMAIN\user1 である場合、Cisco ISE によって user1 が LDAP サーバーに送信されます。 （注） <start_string> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザー名にこれらの文字を使用できません。
最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip end of subject name from the first occurrence of the separator）	ユーザー名からドメインサフィックスを削除するための適切なテキストを入力します。 ユーザー名の中でこのフィールドに指定した区切り文字が Cisco ISE で検出されると、その区切り文字からユーザー名の末尾までのすべての文字が削除されます。ユーザー名に、このフィールドに指定した文字が複数含まれている場合は、Cisco ISE によって最初の区切り文字から文字が削除されます。たとえば、区切り文字が@で、ユーザー名が *user1@domain* であれば、Cisco ISE は *user1* を LDAP サーバーに送信します。 （注） <*end_string*> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザー名にこれらの文字を使用できません。

LDAP グループ設定

表 *89 : LDAP* グループ設定

フィールド名	使用上のガイドライン
追加（**Add**）	[追加（Add）] > [グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）]>[ディレクトリからグループを選択（Select Groups From Directory）] を選択して LDAP ディレクトリからグループを選択します。 グループの追加を選択した場合は、新しいグループの名前を入力します。ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。選択したグループが [グループ（Groups）] ウィンドウに表示されます。

LDAP 属性設定

表 *90 : LDAP* 属性設定

フィールド名	使用上のガイドライン
追加（**Add** ）	[追加（Add）] > [属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）]>[ディレクトリから属性を選択（Select Attributes From Directory）] を選択して LDAP サーバーから属性を選択します。 属性を追加する場合は、新しい属性の名前を入力します。ディレクトリから選択する場合は、ユーザー名を入力し、[属性の取得（Retrieve Attributes）] をクリックして属性を取得します。選択する属性の隣にあるチェック ボックスをオンにし、[OK] をクリックします。

LDAP 詳細設定

以下の表では、[詳細設定（Advanced Settings）] タブのフィールドについて説明します。

表 *91 : LDAP* 詳細設定

フィールド名	使用上のガイドライン
パスワードの変更を有効にする（**Enable password change**）	デバイス管理に PAP プロトコルを使用し、ネットワーク アクセスに RADIUS EAP-GTC プロトコルを使用している場合に、パスワードが期限切れになるか、またはパスワードがリセットされるときに、ユーザーがパスワードを変更できるようにするには、このチェック ボックスをオンにします。サポートされていないプロトコルでは、ユーザー認証が失敗します。このオプションでは、ユーザーが次回のログイン時にパスワードを変更できるようにすることもできます。

関連トピック

LDAP ディレクトリ サービス （1142 ページ）
LDAP ユーザー認証 （1143 ページ）
LDAP ユーザー ルックアップ （1147 ページ）
LDAP ID ソースの追加 （1148 ページ）

LDAP スキーマの設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] を選択します。

ステップ 2 LDAP インスタンスを選択します。

ステップ 3 [全般（General）] タブをクリックします。

ステップ 4 [スキーマ（Schema）] オプションの近くにあるドロップダウン矢印をクリックします。

ステップ 5 [スキーマ（Schema）] ドロップダウン リストから必要なスキーマを選択します。[カスタム（Custom）] オプションを選択して、要件に基づいて属性を更新できます。

事前定義属性は、組み込みスキーマ（Active Directory、Sun directory Server、Novell eDirectory など）に使用されます。事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。

プライマリおよびセカンダリ LDAP サーバーの設定

LDAP インスタンスを作成したら、プライマリ LDAP サーバーに対する接続を設定する必要があります。セカンダリ LDAP サーバーの設定は、オプションです。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 [接続（Connection）] タブをクリックして、プライマリおよびセカンダリ サーバーを設定します。

ステップ 4 「LDAP ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 [送信（Submit）] をクリックして接続パラメータを保存します。

LDAP サーバーからの属性を取得するための Cisco ISE の有効化

Cisco ISE で LDAP サーバーからユーザーとグループのデータを取得するには、Cisco ISE で LDAP ディレクトリの詳細を設定する必要があります。LDAP ID ソースでは、次の 3 つの検索が適用されます。

- 管理のためのグループ サブツリーのすべてのグループの検索
- ユーザーを特定するためのサブジェクト サブツリーのユーザーの検索
- ユーザーが所属するグループの検索

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 [ディレクトリ構成（Directory Organization）] タブをクリックします。

ステップ 4 「LDAP ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 [送信（Submit）] をクリックして設定を保存します。

LDAP サーバーからのグループ メンバーシップ詳細の取得

新しいグループを追加するか、LDAP ディレクトリからグループを選択できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 [グループ（Groups）] タブをクリックします。

ステップ 4 **[追加（Add）]>[グループの追加（Add Group）]** を選択して新しいグループを追加するか、**[追加（Add）]> [ディレクトリからグループを選択（Select Groups From Directory）]** を選択して LDAP ディレクトリからグループを選択します。

a) グループの追加を選択した場合は、新しいグループの名前を入力します。

b) ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。検索条件には、アスタリスク（*）ワイルドカード文字を含めることができます。

ステップ 5 選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

選択したグループが [グループ（Groups）] ページに表示されます。

ステップ 6 グループ選択を保存するには、[送信（Submit）] をクリックします。

（注） Active Directory の組み込みグループは、Active Directory が Cisco ISE の LDAP ID ストアとして設定されているときにはサポートされません。

LDAP サーバーからのユーザー属性の取得

許可ポリシーで使用する LDAP サーバーからユーザー属性を取得できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 [属性（Attributes）] タブをクリックします。

ステップ 4 **[追加（Add）] > [属性の追加（Add Attribute）]** を選択して新しい属性を追加するか、**[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）]** を選択して LDAP サーバーから属性を選択します。

a) 属性を追加する場合は、新しい属性の名前を入力します。

b) ディレクトリから選択する場合は、例のユーザーを入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザーの属性を取得します。アスタリスク（*）ワイルドカード文字を使用できます。

Cisco ISE では、属性タイプ IP を手動で追加するときに、ユーザー認証に IPv4 または IPv6 アドレスを使用して LDAP サーバーを設定できます。

ステップ 5 選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 属性選択を保存するには、[送信（Submit）] をクリックします。

LDAP ID ソースによるセキュア認証の有効化

LDAP 設定ページで [セキュア認証（Secure Authentication）] オプションを選択すると、Cisco ISE は LDAP ID ソースとのセキュアな通信に SSL を使用します。LDAP ID ソースへのセキュアな接続は以下を使用して確立されます。

- SSL トンネル：SSL v3 または TLS v1（LDAP サーバーでサポートされる最も強力なバージョン）を使用
- サーバー認証（LDAP サーバーの認証）：証明書ベース
- クライアント認証（Cisco ISE の認証）：なし（管理者のバインドは SSL トンネル内で使用されます）
- 暗号スイート：Cisco ISE でサポートされるすべての暗号スイート

最も強力な暗号化と Cisco ISE がサポートする暗号方式を備えている TLS v1 を使用することを推奨します。

Cisco ISE が LDAP ID ソースと安全に通信できるようにするには、次の手順を実行します。

始める前に

- Cisco ISE は、LDAP サーバーに接続する必要があります

• TCP ポート 636 を開く必要があります

ステップ 1 LDAP サーバーにサーバー証明書を発行した CA の認証局（CA）チェーン全体を Cisco ISE にインポートします（**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]**）。

完全な CA チェーンは、ルート CA 証明書および中間 CA 証明書を参照し、LDAP サーバー証明書は参照しません。

ステップ 2 LDAP ID ソースとの通信時にセキュア認証を使用するように Cisco ISE を設定します（**[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[LDAP]**。[接続設定（Connection Settings）] タブで [セキュア認証（Secure Authentication）] チェックボックスを必ずオンにしてください）。

ステップ 3 LDAP ID ストアでルート CA 証明書を選択します。

LDAP アイデンティティ送信元がスポンサーポータルにアクセスするためのアイデンティティ送信元の順序として使用される場合、LDAP グループ内のユーザーは、スポンサーグループの権限に基づいてスポンサーポータルにアクセスできます。スポンサーポータルへのアクセスを制限するには、アイデンティティ送信元の順序として LDAP アイデンティティ送信元を使用しないでください。

ODBC ID ソース

オープン データベース コネクティビティ（ODBC）準拠データベースは、ユーザーとエンドポイントを認証する外部 ID ソースとして使用できます。ODBC ID ストアは、ID ストアの順序で、ゲストおよびスポンサーの認証に使用できます。また、BYOD フローにも使用できます。

サポートされているデータベース エンジンは次のとおりです。

- MySQL
- Oracle
- PostgreSQL
- Microsoft SQL Server
- Sybase

ODBC 準拠データベースに対して認証するように Cisco ISE を設定しても、データベースの設定には影響を与えません。データベースを管理するには、データベースのマニュアルを参照してください。

（注） Cisco ISE は ODBC による暗号化をサポートしていません。したがって、ODBC 接続は保護されていません。

ODBC データベースのクレデンシャルチェック

Cisco ISE は、ODBC データベースに対する 3 つの異なるタイプのクレデンシャルチェックをサポートしています。それぞれのクレデンシャル チェック タイプに適切な SQL ストアドプロシージャを設定する必要があります。ストアドプロシージャは、ODBCデータベースで適切なテーブルをクエリし、ODBCデータベースから出力パラメータやレコードセットを受信するために使用されます。データベースは、ODBCクエリに応答してレコードセットまたは名前付きパラメータのセットを返すことができます。

パスワードは、クリアテキストまたは暗号化形式でODBCデータベースに保存できます。Cisco ISEによって呼び出された場合は、ストアドプロシージャでパスワードをクリアテキストに復号化できます。

クレデンシャルチェック タイプ	ODBC 入力パラメータ	ODBC 出力パラメータ	クレデンシャルチェック	認証プロトコル
ODBCデータベースのプレーンテキストパスワード認証	ユーザー名 パスワード	結果 グループ アカウント情報 エラー文字列	ユーザー名とパスワードが一致すると、関連するユーザー情報が返されます。	PAP EAP-GTC（PEAP またはEAP-FAST の内部メソッドとして） TACACS
ODBCデータベースから取得したプレーンテキストパスワード	ユーザー名	結果 グループ アカウント情報 エラー文字列 パスワード	ユーザー名が見つかった場合、そのパスワードと関連するユーザー情報がストアドプロシージャによって返されます。Cisco ISEは、認証方式に基づいてパスワードハッシュを計算し、クライアントから受信したものと比較します。	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2（PEAP または EAP-FAST の内部メソッドとして） TACACS
ルックアップ	ユーザー名	結果 グループ アカウント情報 エラー文字列	ユーザー名が見つかった場合、該当するユーザー情報が返されます。	MAB PEAP、EAP-FAST、EAP-TTLS の高速再接続

（注） 承認の参照元としてODBC を使用する場合は、ODBC データベースと着信要求 MAB 形式が同じであることを確認します。

出力パラメータで返されるグループは、Cisco ISE では使用されません。グループの取得ストアドプロシージャによって取得されたグループのみが Cisco ISE で使用されます。アカウント情報は、認証の監査ログにのみ含まれています。

次の表に、ODBC データベース ストアドプロシージャと Cisco ISE 認証結果コードによって返される、結果コード間のマッピングを示します。

（ストアドプロシージャによって返される）結果コード	説明	Cisco ISE 認証結果コード
0	CODE_SUCCESS	NA (authentication passed)
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	Failed
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	Error
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired

（注） Cisco ISE は、このマッピングされた認証結果コードに基づいて実際の認証またはルックアップ操作を実行します。

ODBC データベースからグループと属性を取得するためにストアドプロシージャを使用できます。

次は、プレーンテキストパスワード認証用のレコードセットを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset]
        @username varchar(64), @password varchar(255)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

次は、プレーンテキストパスワード取得用のレコードセットを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset]
        @username varchar(64)
AS
```

```
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error',password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

次は、ルックアップ用のレコードセットを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

次は、プレーンテキストパスワード認証用のパラメータを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters]
        @username varchar(64), @password varchar(255), @result INT OUTPUT, @group
varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc',  @errorString='ODBC Authen Error'
END
```

次は、プレーンテキストパスワード取得用のパラメータを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters]
       @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
 varchar(255) OUTPUT, @errorString varchar(255) OUTPUT, @password varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error', @password=password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
```

```
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

次は、ルックアップ用のパラメータを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters]
       @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
 varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

次は、Microsoft SQL Server からグループを取得するサンプルのプロシージャです。

```
CREATE PROCEDURE [dbo].[ISEGroupsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                select 'accountants', 'engineers', 'sales','test_group2'
        end
        else
                set @result = 1
END
```

次は、ユーザー名が「*」の場合にすべてのユーザーの全グループを取得するサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
ALTER PROCEDURE [dbo].[ISEGroupsH]
                @username varchar(64), @result int output
AS
BEGIN
                if @username = '*'
                begin
                                -- if username is equal to '*' then return all existing
 groups
                                set @result = 0
                                select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4'
                end
                else
                if exists (select * from NetworkUsers where username = @username)
                begin
                                set @result = 0
                                select 'accountants'
                end
                else
                                set @result = 1
END
```

次は、Microsoft SQL Server から属性を取得するサンプルのプロシージャです。

```
CREATE PROCEDURE [dbo].[ISEAttrsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                                select phone as phone, username as username, department
 as department, floor as floor, memberOf as memberOf, isManager as isManager from
NetworkUsers where username = @username
        end
        else
                set @result = 1
END
```

ODBC 設定のその他の例

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/211581-Configure-ODBC-on-ISE-2-3-with-Oracle-Da.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200644-Configure-ODBC-on-ISE-2-1-with-PostgreSQ.html

ODBC ID ソースの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 [ODBC] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [一般（General）] タブで、ODBC ID ソースの名前と説明を入力します。

ステップ 5 [接続（Connection）] タブで、次の詳細情報を入力します。

- ODBC データベースのホスト名または IP アドレス。データベースに非標準 TCP ポートが使用されている場合は、「ホスト名または IP アドレス:ポート」の形式でポート番号を指定できます。
- ODBC データベースの名前
- 管理者のユーザー名およびパスワード（Cisco ISE がこれらのクレデンシャルを使用してデータベースに接続します）
- 秒単位のサーバーのタイムアウト（デフォルトは 5 秒）
- 接続の試行（デフォルトは 1）
- データベースタイプ。次のいずれかを実行します。
  - **MySQL**

- **Oracle**
- **PostgreSQL**
- **Microsoft SQL Server**
- **Sybase**

ステップ 6 ステップ 5 でデータベースタイプとして **MySQL** を選択した場合は、[セキュアな接続（Secure Connection）] 領域が表示されます。ODBC 接続を確立してログイン情報を保護するには、[セキュアな接続の有効化（Enable Secure Connection）] チェックボックスをオンにします。

[セキュアな接続の有効化（Enable Secure Connection）] オプションを選択すると、[サーバー ID のチェックを要求（Require Server Identity Check）] チェックボックスをオンにできます。このオプションは Cisco ISE に対し、ODBC サーバー証明書の CN および SAN フィールドをチェックして、その情報が設定した FQDN または IP アドレスと一致するかどうか確認するよう求めます。情報が一致した場合にのみ接続が確立されます。

ステップ 7 [テスト接続（Test Connection）] をクリックして ODBC データベースとの接続を確認し、設定された使用例用のストアドプロシージャの存在を確認します。

ステップ 8 [ストアドプロシージャ（Stored Procedures）] タブで、次の詳細情報を入力します。

- [ストアドプロシージャのタイプ（Stored Procedure Type）]：データベースが提供する出力のタイプを選択します。
  - [レコードセットを返す（Returns Recordset）]：データベースは、ODBC クエリに応じてレコードセットを返します。
  - [パラメータを返す（Returns Parameters）]：データベースは、ODBC クエリに応じて名前付きパラメータのセットを返します。
- [プレーンテキストパスワード認証（Plain Text Password Authentication）]：プレーンテキストパスワード認証のために ODBC サーバー上で実行するストアドプロシージャの名前を入力します。PAP、EAP-GTC 内部メソッド、TACACS 用に使用されます。
- [プレーンテキストパスワードの取得（Plain Text Password Fetching）]：プレーンテキストパスワードの取得のために ODBC サーバー上で実行するストアドプロシージャの名前を入力します。CHAP、MS-CHAPv1/v2、LEAP、EAP-MD5、EAP-MSCHAPv2 内部メソッド、TACACS 用に使用されます。
- [ユーザー名またはマシンの存在を確認する（Check username or machine exists）]：ユーザー/MAC アドレスルックアップのために ODBC サーバー上で実行するストアドプロシージャの名前を入力します。MAB、および PEAP、EAP-FAST、EAP-TTLS の高速再接続用に使用されます。
- [グループの取得（Fetch Groups）]：ODBC データベースからグループを取得するストアドプロシージャの名前を入力します。
- [属性の取得（Fetch Attributes）]：ODBC データベースから属性とその値を取得するストアドプロシージャの名前を入力します。

- [詳細設定（Advanced Settings）]：次のディクショナリの属性を、（ユーザー名とパスワードに加えて）[属性の取得（Fetch Attributes）] のストアドプロシージャの入力パラメータとして使用するには、このオプションをクリックします。
  - **RADIUS**
  - **Device**
  - **Network Access**

（注） [ネットワークアクセス（Network Access）]ディクショナリでは、[AuthenticationMethod]、[デバイスの IP アドレス（Device IP Address）]、[EapAuthentication]、[EapTunnel]、[ISE ホスト名（ISE Host Name）]、[プロトコル（Protocol）]、[ユーザー名（UserName）]、[VN]、および [WasMachineAuthenticated] の属性のみを使用できます。

[ストアドプロシージャの属性名（Attribute Name in Stored Procedure）] フィールドで、ストアドプロシージャで使用される属性名を指定します。

ODBC データベースから次の出力パラメータを取得するようにストアドプロシージャを設定できます。

- ACL
- セキュリティグループ
- VLAN（名前または番号）
- Web リダイレクト ACL
- Web リダイレクトポータル名

これらの属性を使用して、認証プロファイルを設定できます。これらの属性は、[認証プロファイル（Authorization Profile）] ウィンドウ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）]）の [共通タスク（Common Tasks）] セクションに表示されます。次に、これらの属性を使用できるいくつかの使用例を示します。

- 認証プロファイルごとに VLAN を手動で指定するのではなく、指定された入力属性（MAC アドレス、ユーザー名、着信側ステーション ID、デバイスロケーション）に基づいて ODBC データベースから返された VLAN を使用するように認証プロファイルを設定する場合。
- ODBC ID ストアでブロックされている発信側ステーション ID のアクセスをブロックするように認証プロファイルを設定する場合。
- MAC アドレス、ユーザー名、着信側ステーション ID、またはデバイスロケーションに基づいて、ODBC データベースから Web リダイレクト ACL または Web リダイレクトポータル名を取得するように認証プロファイルを設定する場合。

認証ポリシーの設定時に、[ポリシーセット（Policy Sets）] ウィンドウで ODBC データベースから取得したセキュリティグループを選択できます。

（注） [詳細設定（Advanced Settings）] オプションを使用すると、user_attributes_detail という名前の新しいテーブルが ODBC データベースに作成され、追加の詳細が保存されます。すべての出力パラメータのデータ型を VARCHAR2 として設定する必要があります。そうしないと、ユニオンおよびコンパイルプロセス中にストアドプロシージャが失敗する可能性があります。たとえば、SGTNAME が VARCHAR2 として設定され、VLANNUMBER が NUMBER として設定されている場合、次のストアドプロシージャのコンパイルは失敗することがあります。

```
select  ATTR_NAME, value from ATTRIBUTES where user_id=userid
          union
          select 'SGTNAME', SGTNAME from user_attributes_detail where USER_ID =
userid and user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE
          union
         select 'VLANNUMBER', VLANNUMBER from user_attributes_detail where USER_ID
 = userid and user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE;
```

- [この形式の MAC アドレスを検索（Search for MAC Address in Format）]：着信 MAC アドレスは、選択した MAC 形式に基づいて正規化されます。

ステップ 9 [属性（Attributes）] タブに必要な属性を追加します。属性の追加時に、属性名が認証ポリシールールでどのように表示されるかを指定できます。

ODBC データベースから属性を取得することもできます。これらの属性は、認証ポリシーで使用できます。

ステップ 10 [グループ（Groups）] タブにユーザーグループを追加します。また、ユーザー名または MAC アドレスを指定して ODBC データベースからグループを取得することもできます。これらのグループは、認証ポリシーで使用できます。

グループおよび属性の名前を変更できます。デフォルトでは、[ISE の名前（Name in ISE）] フィールドに表示される名前は ODBC データベースの名前と同じですが、この名前は変更できます。この名前が認証ポリシーで使用されます。

ステップ 11 [送信（Submit）] をクリックします。

ODBC ID ソースの設定方法の詳細については、次のリンクを参照してください。

- Oracle データベースを用いた Cisco ISE での ODBC の設定
- ODBC を使用した MS SQL を用いた Cisco ISE の設定
- PostgreSQL を用いた Cisco ISE での ODBC の設定
- MySQL サーバーと統合するための Cisco ISE の設定

（注） 入力属性を設定した場合は、ODBC ID ストアを複製するときに次の手順を実行する必要があります。保存しない場合は、複製した ODBC ID ストアで入力パラメータが失われる可能性があります。

1. [詳細設定（Advance Settings）] をクリックします。
2. 入力パラメータが正しく設定されているかどうかを確認します。
3. [OK] をクリックして、複製した ODBC ID ストアにこれらの入力パラメータを保存します。

RADIUS トークン ID ソース

RADIUS プロトコルをサポートし、ユーザーおよびデバイスに認証、許可、アカウンティング（AAA）サービスを提供するサーバーは、RADIUS サーバーと呼ばれます。RADIUS ID ソースは、サブジェクトとそのクレデンシャルの集合を含み、通信に RADIUS プロトコルを使用する外部 ID ソースです。たとえば、Safeword トークン サーバーは、複数のユーザーおよびそのクレデンシャルをワンタイム パスワードとして含めることができる ID ソースであり、Safeword トークン サーバーによって提供されるインターフェイスでは、RADIUS プロトコルを使用して問い合わせることができます。

Cisco ISE では、RADIUS RFC 2865 準拠のいずれかのサーバーが外部 ID ソースとしてサポートされています。Cisco ISE では、複数の RADIUS トークン サーバー ID がサポートされています。たとえば、RSA SecurID サーバーや SafeWord サーバーなどです。RADIUS ID ソースは、ユーザーを認証するために使用される任意の RADIUS トークン サーバーと連携できます。

（注） MAB 認証では、プロセス ホスト ルックアップ オプションを有効にする必要があります。MAB 認証を使用するデバイスは OTP または RADIUS トークン（RADIUS トークン サーバー認証に必要）を生成できないため、MAB 認証用に外部 ID ソースとして使用される RADIUS トークン サーバーを設定しないことをお勧めします。そのため、認証は失敗します。MAB 要求の処理には、外部 RADIUS サーバー オプションを使用できます。

RADIUS トークンサーバーでサポートされる認証プロトコル

Cisco ISE では、RADIUS ID ソースに対して次の認証プロトコルがサポートされています。

- RADIUS PAP
- 内部拡張認証プロトコル汎用トークン カード（EAP-GTC）を含む保護拡張認証プロトコル（PEAP）
- 内部 EAP-GTC を含む EAP-FAST

RADIUS トークンサーバーで通信に使用されるポート

RADIUS ID トークン サーバーでは、認証セッションに UDP ポートが使用されます。このポートはすべての RADIUS 通信に使用されます。Cisco ISE で RADIUS ワンタイム パスワード（OTP）メッセージを RADIUS 対応トークン サーバーに送信するには、Cisco ISE と RADIUS 対応トークン サーバーの間のゲートウェイ デバイスが、UDP ポートを介した通信を許可するように設定されている必要があります。UDP ポートは、管理者ポータルを介して設定できます。

RADIUS 共有秘密

Cisco ISE で RADIUS ID ソースを設定するときに、共有秘密を指定する必要があります。この共有秘密情報は、RADIUS トークン サーバー上で設定されている共有秘密情報と同一である必要があります。

RADIUS トークン サーバーでのフェールオーバー

Cisco ISE では、複数の RADIUS ID ソースを設定できます。各 RADIUS ID ソースには、プライマリとセカンダリの RADIUS サーバーを指定できます。Cisco ISE からプライマリ サーバーに接続できない場合は、セカンダリ サーバーが使用されます。

RADIUS トークン サーバーの設定可能なパスワード プロンプト

RADIUS ID ソースでは、パスワード プロンプトを設定できます。パスワード プロンプトは、管理者ポータルを介して設定できます。

RADIUS トークン サーバーのユーザー認証

Cisco ISE は、ユーザー クレデンシャル（ユーザー名とパスコード）を取得し、RADIUS トークン サーバーに渡します。また、Cisco ISE は RADIUS トークン サーバー認証処理の結果をユーザーに中継します。

RADIUS トークン サーバーのユーザー属性キャッシュ

RADIUS トークン サーバーでは、デフォルトではユーザー ルックアップはサポートされていません。ただし、ユーザー ルックアップは次の Cisco ISE 機能に不可欠です。

- PEAP セッション再開：この機能によって、認証の成功後、EAP セッションの確立中に PEAP セッションを再開できます。
- EAP/FAST 高速再接続：この機能によって、認証の成功後、EAP セッションの確立中に高速再接続が可能になります。
- TACACS+ 許可：TACACS+ 認証に成功すると発生します。

Cisco ISE では、これらの機能のユーザー ルックアップ要求を処理するために、成功した認証の結果がキャッシュされます。成功した認証すべてについて、認証されたユーザーの名前と取得された属性がキャッシュされます。失敗した認証はキャッシュに書き込まれません。

キャッシュは、実行時にメモリで使用可能であり、分散展開の Cisco ISE ノード間で複製されません。管理者ポータルを介してキャッシュの存続可能時間（TTL）制限を設定できます。ISE 2.6 以降、ID キャッシング オプションを有効にして、エージング タイムを分単位で設定する場合があります。デフォルトでは、このオプションは無効です。有効にすると、指定した期間、メモリでキャッシュが使用できるようになります。

ID 順序での RADIUS ID ソース

ID ソース順序で認証順序用の RADIUS ID ソースを追加できます。ただし、属性取得順序用の RADIUS ID ソースを追加することはできません。これは、認証しないで RADIUS ID ソースを問い合わせることはできないためです。RADIUS サーバーによる認証中、Cisco ISE では異なるエラーを区別できません。すべてのエラーに対して RADIUS サーバーから Access-Reject メッセージが返されます。たとえば、RADIUS サーバーでユーザーが見つからない場合、RADIUS サーバーからは User Unknown ステータスの代わりに Access-Reject メッセージが返されます。

RADIUS サーバーがすべてのエラーに対して同じメッセージを返す

RADIUS サーバーでユーザーが見つからない場合、RADIUS サーバーからは Access-Reject メッセージが返されます。Cisco ISE では、管理者ポータルを使用してこのメッセージを [認証失敗（Authentication Failed）] メッセージまたは [ユーザーが見つからない（User Not Found）] メッセージとして設定するためのオプションを使用できます。ただし、このオプションを使用すると、ユーザーが未知の状況だけでなく、すべての失敗状況に対して「ユーザーが見つからない（User Not Found）」メッセージが返されます。

次の表は、RADIUS ID サーバーで発生するさまざまな失敗状況を示しています。

表 *92 :* エラー処理

失敗状況	失敗の理由
認証に失敗	• ユーザーが未知である。 • ユーザーが不正なパスコードでログインしようとしている。 • ユーザー ログイン時間が期限切れになった。
プロセスの失敗	• RADIUS サーバーが Cisco ISE で正しく設定されていない。 • RADIUS サーバーが使用できない。 • RADIUS パケットが偽装として検出されている。 • RADIUS サーバーとのパケットの送受信の問題。 • タイムアウト。

失敗状況	失敗の理由
不明なユーザー	認証が失敗し、[拒否で失敗（Fail on Reject）] オプションが false に設定されている。

Safeword サーバーでサポートされる特別なユーザー名の形式

Safeword トークン サーバーでは、次のユーザー名フォーマットでの認証がサポートされています。

ユーザー名：Username, OTP

Cisco ISE では、認証要求を受信するとすぐにユーザー名が解析され、次のユーザー名に変換されます。

ユーザー名：Username

Safeword トークン サーバーでは、これらの両方のフォーマットがサポートされています。Cisco ISE はさまざまなトークン サーバーと連携します。SafeWord サーバーを設定する場合、Cisco ISE でユーザー名を解析して指定のフォーマットに変換するには、管理者ポータルで [SafeWord サーバー（SafeWord Server）] チェックボックスをオンにする必要があります。この変換は、要求が RADIUS トークン サーバーに送信される前に、RADIUS トークン サーバー ID ソースで実行されます。

RADIUS トークン サーバーでの認証要求と応答

Cisco ISE が RADIUS 対応トークン サーバーに認証要求を転送する場合、RADIUS 認証要求には次の属性が含まれます。

- User-Name（RADIUS 属性 1）
- User-Password（RADIUS 属性 2）
- NAS-IP-Address（RADIUS 属性 4）

Cisco ISE は次の応答のいずれかを受信すると想定されます。

- [Access-Accept]：属性は必要ありませんが、応答には RADIUS トークンサーバーの設定に基づいてさまざまな属性が含まれる場合があります。
- [Access-Reject]：属性は必要ありません。
- [Access-Challenge]：RADIUS RFC ごとに必要な属性は次のとおりです。
  - State（RADIUS 属性 24）
  - Reply-Message（RADIUS 属性 18）
  - 次の 1 つ以上の属性：Vendor-Specific、Idle-Timeout（RADIUS 属性 28）、Session-Timeout（RADIUS 属性 27）、Proxy-State（RADIUS 属性 33）

Access-Challenge ではそれ以外の属性は使用できません。

RADIUS トークン ID ソースの設定

次の表では、RADIUS 外部 ID ソースを設定し、それに接続するために使用できる [RADIUS トークン ID ソース（RADIUS Token Identity Sources）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）]** です。

表 *93 : RADIUS* トークン *ID* ソースの設定

フィールド名	使用上のガイドライン
名前（Name）	RADIUS トークン サーバーの名前を入力します。許容最大文字数は 64 文字です。
説明（Description）	RADIUS トークンサーバーの説明を入力します。最大文字数は 1024 です。
SafeWord サーバー（SafeWord Server）	RADIUS ID ソースが SafeWord サーバーである場合はこのチェックボックスをオンにします。
セカンダリ サーバーの有効化（Enable Secondary Server）	プライマリに障害が発生した場合にバックアップとして使用する Cisco ISE のセカンダリ RADIUS トークン サーバーを有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにする場合は、セカンダリ RADIUS トークン サーバーを設定する必要があります。
常にプライマリ サーバーに最初にアクセスする（Always Access Primary Server First）	Cisco ISE が常にプライマリサーバーに最初にアクセスするように設定するには、このオプションをクリックします。
経過後にプライマリ サーバーにフォールバック（Fallback to Primary Server after）	プライマリサーバーに到達できない場合に Cisco ISE がセカンダリ RADIUS トークンサーバーを使用して認証できる時間（分単位）を指定するには、このオプションをクリックします。この時間を過ぎると、Cisco ISE はプライマリ サーバーに対する認証を再試行します。
プライマリ サーバー（Primary Server）	
ホスト名/アドレス（Host IP）	プライマリ RADIUS トークン サーバーの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。

フィールド名	使用上のガイドライン
共有秘密鍵（Shared Secret）	この接続のプライマリ RADIUS トークン サーバーで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	プライマリ RADIUS トークン サーバーが受信しているポート番号を入力します。
サーバー タイムアウト（Server timeout）	プライマリ サーバーがダウンしていると判断する前に Cisco ISE がプライマリ RADIUS トークン サーバーからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	セカンダリ サーバー（定義されている場合）に移動する前、またはセカンダリ サーバーが定義されていない場合は要求をドロップする前に、Cisco ISE がプライマリ サーバーへの再接続を試行する回数を指定します。
セカンダリ サーバー（Secondary Server）	
ホスト名/アドレス（Host IP）	セカンダリ RADIUS トークン サーバーの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。
共有秘密鍵（Shared Secret）	この接続のセカンダリ RADIUS トークン サーバーで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	セカンダリ RADIUS トークン サーバーが受信しているポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは 1812 です。
サーバー タイムアウト（Server timeout）	セカンダリ サーバーがダウンしていると判断する前に Cisco ISE がセカンダリ RADIUS トークン サーバーからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	要求をドロップする前に Cisco ISE がセカンダリ サーバーへの再接続を試行する回数を指定します。

関連トピック

RADIUS トークン ID ソース （1169 ページ）
RADIUS トークン サーバーの追加 （1174 ページ）

RADIUS トークン サーバーの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）] > [追加（Add）]** を選択します。

ステップ 2 [一般（General）] タブおよび [接続（Connection）] タブに値を入力します。

ステップ 3 [認証（Authentication）] タブをクリックします。

このタブでは、RADIUS トークン サーバーからの Access-Reject メッセージへの応答を制御できます。この応答は、クレデンシャルが無効であること、またはユーザーが不明であることのいずれかを意味する場合があります。Cisco ISE は、認証失敗か、またはユーザーが見つからないかのいずれかの応答を受け入れます。このタブでは、ID キャッシングを有効にし、キャッシュのエージング タイムを設定することもできます。パスワードを要求するプロンプトを設定することもできます。

a) RADIUS トークン サーバーからの Access-Reject 応答を認証失敗として処理する場合は、[拒否を「認証失敗」として処理（Treat Rejects as 'authentication failed'）] オプション ボタンをクリックします。

b) RADIUS トークン サーバーからの Access-Reject 応答を未知ユーザー エラーとして処理する場合は、[拒否を「ユーザーが見つからない」として処理（Treat Rejects as 'user not found'）] オプション ボタンをクリックします。

ステップ 4 RADIUS トークン サーバーとの最初の認証の成功の後、Cisco ISE でキャッシュにパスコードを保存し、設定された期間内に発生した後続の認証に対しキャッシュされたユーザーのクレデンシャルを使用する場合、[パスコード キャッシングの有効化（Enable Passcode Caching）] チェック ボックスをオンにします。

パスコードをキャッシュ内に保存する必要がある秒数を [エージング タイム（Aging Time）] フィールドに入力します。この期間内にユーザーは同じパスコードで複数回の認証を行うことができます。デフォルト値は 30 秒です。有効な範囲は 1 ～ 900 秒です。

（注） Cisco ISE は、認証が初めて失敗した後でキャッシュをクリアします。ユーザーは新しい有効なパスコードを入力する必要があります。

キャッシュは、実行時にメモリで使用可能であり、分散展開の Cisco ISE ノード間で複製されません。

（注） EAP-FAST-GTC などの、パスコードの暗号化をサポートするプロトコルを使用する場合にのみこのオプションを有効にすることを強く推奨します。RADIUS トークン サーバーでサポートされている認証プロトコルについては、次を参照してください。 RADIUS トークンサーバーでサポートされる認証プロトコル （1169 ページ）

ステップ 5 サーバーに対する認証を実行しない要求の処理を許可する場合は、[ID キャッシングの有効化（Enable Identity Caching）] チェックボックスをオンにします。

ID キャッシング オプションを有効にし、エージング タイムを分単位で設定できます。デフォルト値は 120 分です。有効な範囲は、1 ～ 1440 分です。最後に成功した認証から取得された結果と属性が、指定された時間、キャッシュ内に保持されます。

このオプションは、デフォルトで無効です。

ステップ 6 [許可（Authorization）] タブをクリックします。

このタブでは、Cisco ISE への Access-Accept 応答を送信中に RADIUS トークン サーバーによって返されるこの属性に対して表示される名前を設定できます。この属性は、許可ポリシー条件で使用できます。デフォルト値は CiscoSecure-Group-Id です。

（注） 外部 ID ソースから Access-Accept で属性を送信する場合、外部 ID ソースは属性名および値として <ciscoavpair> を ACS 形式（<attrname>=<attrvalue>）で送信する必要があります。<attrname> は [許可（Authorization）] タブで設定します。

ステップ 7 [送信（Submit）] をクリックします。

RADIUS トークン サーバーの削除

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ID ソース順序に含まれる RADIUS トークン サーバーを選択していないことを確認します。ID ソース順序に含まれる RADIUS トークン サーバーを削除用に選択した場合、削除操作は失敗します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）]** を選択します。

ステップ 2 削除する RADIUS トークン サーバーの隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして、選択した RADIUS トークン サーバーを削除します。

削除する RADIUS トークン サーバーを複数選択し、その 1 つが ID ソース順序で使用されている場合、削除操作は失敗し、いずれの RADIUS トークン サーバーも削除されません。

RSA ID ソース

Cisco ISE では、外部データベースとして RSA SecurID サーバーがサポートされています。RSA SecurID の 2 要素認証は、ユーザーの PIN と、タイム コード アルゴリズムに基づいて使い捨てのトークン コードを生成する個別に登録された RSA SecurID トークンで構成されます。異なるトークン コードが固定間隔（通常は 30 または 60 秒ごと）で生成されます。RSA SecurID サーバーでは、この動的な認証コードが検証されます。各 RSA SecurID トークンは固有であり、過去のトークンに基づいて将来のトークンの値を予測することはできません。そのため、正しいトークン コードが PIN とともに提示された場合、その人が有効なユーザーである確実

性が高くなります。したがって、RSA SecurID サーバーでは、従来の再利用可能なパスワードよりも信頼性の高い認証メカニズムが提供されます。

Cisco ISE では、次の RSA ID ソースがサポートされています。

- RSA ACE/Server 6.x シリーズ
- RSA Authentication Manager 7.x および 8.0 シリーズ

次のいずれかの方法で、RSA SecurID 認証テクノロジーと統合できます。

- RSA SecurID エージェントの使用：ユーザーは、RSA のネイティブプロトコルによってユーザー名とパスコードで認証されます。
- RADIUS プロトコルの使用：ユーザーは、RADIUS プロトコルによってユーザー名とパスコードで認証されます。

Cisco ISE の RSA SecurID トークン サーバーは、RSA SecurID 認証テクノロジーと RSA SecurID エージェントを使用して接続します。

Cisco ISE では、1 つの RSA 領域だけがサポートされています。

Cisco ISE と RSA SecurID サーバーの統合

Cisco ISE と RSA SecurID サーバーを接続するには、次の 2 つの管理ロールが必要です。

- RSA サーバー管理者：RSA システムおよび統合を設定および維持します。
- Cisco ISE 管理者：Cisco ISE を RSA SecurID サーバーに接続するように設定し、設定を維持します。

ここでは、Cisco ISE に RSA SecurID サーバーを外部 ID ソースとして接続するために必要なプロセスについて説明します。RSA サーバーについての詳細は、RSA に関するドキュメントを参照してください。

Cisco ISE の RSA 設定

RSA 管理システムでは sdconf.rec ファイルが生成されます。このファイルは RSA システム管理者によって提供されます。このファイルを使用すると、Cisco ISE サーバーを領域内の RSA SecurID エージェントとして追加できます。このファイルを参照して Cisco ISE に追加する必要があります。プライマリ Cisco ISE サーバーは、複製のプロセスによってこのファイルをすべてのセカンダリ サーバーに配布します。

RSA SecurID サーバーに対する RSA エージェント認証

sdconf.rec ファイルがすべての Cisco ISE サーバーにインストールされると、RSA エージェントモジュールが初期化され、RSA 生成のクレデンシャルによる認証が各 Cisco ISE サーバーで実行されます。展開内の各 Cisco ISE サーバー上のエージェントが正常に認証されると、RSA サーバーとエージェント モジュールは securid ファイルをダウンロードします。このファイルは

Cisco ISE ファイル システムに存在し、RSA エージェントによって定義された既知の場所にあります。

分散 Cisco ISE 環境の RSA ID ソース

分散 Cisco ISE 環境で RSA ID ソースを管理するには、次の操作が必要です。

- sdconf.rec および sdopts.rec ファイルのプライマリ サーバーからセカンダリ サーバーへの配布。
- securid および sdstatus.12 ファイルの削除。

Cisco ISE 展開の RSA サーバーの更新

Cisco ISE で sdconf.rec ファイルを追加した後、RSA サーバーを廃止する場合、または新しい RSA セカンダリ サーバーを追加する場合、RSA SecurID 管理者は sdconf.rec ファイルを更新することがあります。更新されたファイルは RSA SecurID 管理者によって提供されます。更新されたファイルによって Cisco ISE を再設定できます。Cisco ISE では、更新されたファイルが複製プロセスによって展開内のセカンダリ Cisco ISE サーバーに配布されます。Cisco ISE では、まずファイル システムのファイルを更新し、RSA エージェント モジュールに合わせて調整して再起動プロセスを適切に段階的に行います。sdconf.rec ファイルが更新されると、sdstatus.12 および securid ファイルがリセット（削除）されます。

自動 RSA ルーティングの上書き

領域内に複数の RSA サーバーを持つことができます。sdopts.rec ファイルはロード バランサの役割を果たします。Cisco ISE サーバーと RSA SecurID サーバーはエージェント モジュールを介して動作します。Cisco ISE に存在するエージェント モジュールは、領域内の RSA サーバーを最大限に利用するためにコストベースのルーティング テーブルを保持します。ただし、領域の各 Cisco ISE サーバーの手動設定を使用してこのルーティングを上書きするには、管理者ポータルで sdopts.rec と呼ばれるテキスト ファイルを使用します。このファイルの作成方法については、RSA に関するドキュメントを参照してください。

RSA ノード秘密リセット

securid ファイルは秘密ノード キー ファイルです。RSA が最初に設定されると、RSA では秘密を使用してエージェントが検証されます。Cisco ISE に存在する RSA エージェントが RSA サーバーに対して初めて正常に認証されると、securid と呼ばれるファイルがクライアント マシン上に作成され、このファイルを使用して、マシン間で交換されるデータが有効であることが確認されます。展開内の特定の Cisco ISE サーバーまたはサーバーのグループから securid ファイルを削除する必要がある場合があります（たとえば、RSA サーバーでのキーのリセット後など）。領域に対する Cisco ISE サーバーからこのファイルを削除するには、Cisco ISE 管理者ポータルを使用できます。Cisco ISE の RSA エージェントが次回正常に認証されたとき、新しい securid ファイルが作成されます。

（注） Cisco ISE の最新リリースへのアップグレード後に認証が失敗した場合は、RSA 秘密をリセットします。

RSA の自動可用性のリセット

sdstatus.12 ファイルは、領域内の RSA サーバーのアベイラビリティに関する情報を提供します。たとえば、いずれのサーバーがアクティブで、いずれのサーバーがダウンしているかに関する情報を提供します。エージェント モジュールは領域内の RSA サーバーと連携して、このアベイラビリティ ステータスを維持します。この情報は、sdstatus.12 ファイルに連続的に表示されます。このファイルは、Cisco ISE ファイル システムの既知の場所に供給されます。このファイルは古くなり、現在のステータスが反映されていないことがあります。その場合、現在のステータスが反映されるように、このファイルを削除する必要があります。特定の領域に対する固有の Cisco ISE サーバーからファイルを削除するには、管理者ポータルを使用できます。Cisco ISE は RSA エージェントに合わせて調整して、再起動が正しく段階的に行われるようにします。

sdstatus.12 ファイルは、securid ファイルがリセットされるか、あるいは sdconf.rec ファイルまたは sdopts.rec ファイルが更新されるたびに削除されます。

RSA SecurID ID ソースの設定

次の表では、RSA SecurID ID ソースを作成し、それに接続するために使用できる [RSA SecurID ID ソース（RSA SecurID Identity Sources）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID]**。

RSA プロンプトの設定

次の表では、[RSA プロンプト（RSA Prompts）] タブ内のフィールドについて説明します。

表 *94 : RSA* プロンプトの設定

フィールド名	使用上のガイドライン
パスコード プロンプトの入力（Enter Passcode Prompt）	パス コードを取得するテキスト文字列を入力します。
次のトークン コードの入力（Enter Next Token Code）	次のトークンを要求するテキスト文字列を入力します。

フィールド名	使用上のガイドライン
PIN タイプの選択（Choose PIN Type）	PIN タイプを要求するテキスト文字列を入力します。
システム PIN の受け入れ（Accept System PIN）	システム生成の PIN を受け付けるテキスト文字列を入力します。
英数字 PIN の入力（Enter Alphanumeric PIN）	英数字 PIN を要求するテキスト文字列を入力します。
数値 PIN の入力（Enter Numeric PIN）	数値 PIN を要求するテキスト文字列を入力します。
PIN の再入力（Re-enter PIN）	ユーザーに PIN の再入力を要求するテキスト文字列を入力します。

RSA メッセージ設定

次の表では、[RSA メッセージ（RSA Messages）] タブ内のフィールドについて説明します。

表 *95 : RSA* メッセージ設定

フィールド名	使用上のガイドライン
システム PIN メッセージの表示（Display System PIN Message）	システム PIN メッセージのラベルにするテキスト文字列を入力します。
システム PIN 通知の表示（Display System PIN Reminder）	ユーザーに新しいPINを覚えるように通知するテキスト文字列を入力します。
数字を入力する必要があるエラー（Must Enter Numeric Error）	PIN には数字のみを入力するようにユーザーに指示するメッセージを入力します。
英数字を入力する必要があるエラー（Must Enter Alpha Error）	PIN には英数字のみを入力するようにユーザーに指示するメッセージを入力します。

フィールド名	使用上のガイドライン
PIN 受け入れメッセージ（PIN Accepted Message）	ユーザーの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
PIN 拒否メッセージ（PIN Rejected Message）	ユーザーの PIN がシステムによって拒否されたときに表示されるメッセージを入力します。
ユーザーの PIN が異なるエラー（User Pins Differ Error）	ユーザーが不正な PIN を入力したときに表示されるメッセージを入力します。
システム PIN 受け入れメッセージ（System PIN Accepted Message）	ユーザーの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
不正パスワード長エラー（Bad Password Length Error）	ユーザーが指定した PIN が、PIN 長ポリシーで指定されている範囲に収まらない場合に表示されるメッセージを入力します。

関連トピック

RSA ID ソース （1176 ページ）
Cisco ISE と RSA SecurID サーバーの統合 （1177 ページ）
RSA ID ソースの追加 （1181 ページ）

RSA ID ソースの追加

RSA ID ソースを作成するには、RSA コンフィギュレーション ファイル（sdconf.rec）をインポートする必要があります。RSA 管理者から sdconf.rec ファイルを取得する必要があります。このタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

RSA ID ソースを追加するには、次のタスクを実行します。

RSA コンフィギュレーション ファイルのインポート

Cisco ISE に RSA ID ソースを追加するには、RSA コンフィギュレーション ファイルをインポートする必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）]** を選択します。

ステップ 2 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから新しい sdconf.rec ファイルまたは更新された sdconf.rec ファイルを選択します。

初めて RSA ID ソースを作成する場合、[新しい sdconf.rec ファイルのインポート（Import new sdconf.rec file）] フィールドは必須フィールドです。これ以降は、既存の sdconf.rec ファイルを更新されたファイルで置き換えることができますが、既存のファイルの置き換えは任意です。

ステップ 3 サーバーのタイムアウト値を秒単位で入力します。Cisco ISE はタイムアウトになる前に、指定された秒数 RSA サーバーからの応答を待ちます。この値には、1 ～ 199 の任意の整数を指定できます。デフォルト値は 30 秒です。

ステップ 4 PIN が変更された場合に強制的に再認証するには、[変更 PIN で再認証（Reauthenticate on Change PIN）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

Cisco ISE は、次のシナリオもサポートします。

- Cisco ISE サーバーのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット。
- RSA ID ソースの認証制御オプションの設定。

Cisco ISE サーバーのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット

ステップ 1 Cisco ISE サーバーにログインします。

ステップ 2 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）]** を選択します。

ステップ 3 [RSA インスタンス ファイル（RSA Instance Files）] タブをクリックします。

このページには、展開内のすべての Cisco ISE サーバーの sdopts.rec servers ファイルが一覧表示されます。

ユーザーが RSA SecurID トークン サーバーに対して認証されると、ノードのシークレット ステータスは [作成済み（Created）] と表示されます。ノードのシークレット ステータスは、[作成済み（Created）] または [未作成（Not Created）] のどちらかになります。消去されると、ノードのシークレット ステータスは [未作成（Not Created）] と表示されます。

ステップ 4 特定の Cisco ISE サーバーの sdopts.rec ファイルの横にあるオプション ボタンをクリックし、[オプション ファイルの更新（Update Options File）] をクリックします。

[現在のファイル（Current File）] 領域に既存のファイルが表示されます。

ステップ 5 次のいずれかを実行します。

- [RSA エージェントが保持する自動ロード バランシング ステータスを使用（Use the Automatic Load Balancing status maintained by the RSA agent）]：RSA エージェントでロード バランシングを自動的に管理する場合は、このオプションを選択します。
- [次で選択された sdopts.rec ファイルで自動ロード バランシング ステータスを上書き（Override the Automatic Load Balancing status with the sdopts.rec file selected below）]：特定のニーズに基づいて手動でロードバランシングを設定する場合は、このオプションを選択します。このオプションを選択する場合は、[参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから新しい sdopts.rec ファイルを選択する必要があります。

ステップ 6 [OK] をクリックします。

ステップ 7 Cisco ISE サーバーに対応する行をクリックして、そのサーバーの securid および sdstatus.12 ファイルをリセットします。

a) ドロップダウン矢印をクリックし、[securid ファイルのリセット（Reset securid File）] 列と [sdstatus.12 ファイルのリセット（Reset sdstatus.12 File）] 列の [送信で削除（Remove on Submit）] を選択します。

（注） [sdstatus.12 ファイルのリセット（Reset sdstatus.12 File）] フィールドはユーザーのビューから非表示になっています。このフィールドを表示するには、最も内側のフレームで垂直および水平スクロール バーを使用して、下にスクロールし、次に右にスクロールします。

b) この行で [保存（Save）] をクリックして変更を保存します。

ステップ 8 [保存（Save）] をクリックします。

RSA ID ソースの認証制御オプションの設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）]** を選択します。

ステップ 2 [認証制御（Authentication Control）] タブをクリックします。

ステップ 3 次のいずれかを実行します。

- [拒否を「認証失敗」として処理（Treat Rejects as "authentication failed"）]：拒否された要求を認証失敗として処理する場合は、このオプションを選択します。
- [拒否を「ユーザーが見つからない」として処理（Treat Rejects as "user not found"）]：拒否された要求をユーザーが見つからないエラーとして処理する場合は、このオプションを選択します。

ステップ 4 最初に認証が成功した後に Cisco ISE がキャッシュにパスコードを保存し、設定された期間内に認証が行われた場合にキャッシュされたユーザー クレデンシャルを後続の認証のために使用するようにする場合は、[パスコード キャッシュの有効化（Enable Passcode Caching）] チェック ボックスにマークを付けます。

パスコードをキャッシュ内に保存する必要がある秒数を [エージング タイム（Aging Time）] フィールドに入力します。この期間内にユーザーは同じパスコードで複数回の認証を行うことができます。デフォルト値は 30 秒です。有効な範囲は 1 ～ 300 秒です。

（注） Cisco ISE は、認証が初めて失敗した後でキャッシュをクリアします。ユーザーは新しい有効なパスコードを入力する必要があります。

（注） EAP-FAST-GTC などの、パスコードの暗号化をサポートするプロトコルを使用する場合にのみこのオプションを有効にすることを強く推奨します。

ステップ 5 サーバーに対する認証を実行しない要求の処理を許可する場合は、[ID キャッシングの有効化（Enable Identity Caching）] チェックボックスをオンにします。

ID キャッシング オプションを有効にし、エージング タイムを分単位で設定できます。デフォルト値は 120 分です。有効な範囲は、1 ～ 1440 分です。最後に成功した認証から取得された結果と属性が、指定された時間、キャッシュ内に保持されます。

このオプションは、デフォルトで無効です。

ステップ 6 [保存（Save）] をクリックして、設定を保存します。

RSA プロンプトの設定

Cisco ISE では、RSA SecurID サーバーに送信される要求の処理中にユーザーに表示される RSA プロンプトを設定できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID]** を選択します。

ステップ 2 [プロンプト（Prompts）] をクリックします。

ステップ 3 「RSA SecurID ID ソースの設定」の説明に従って、値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

RSA メッセージの設定

Cisco ISE では、RSA SecurID サーバーに送信される要求の処理中にユーザーに表示されるメッセージを設定できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID]** を選択します。

ステップ 2 [プロンプト（Prompts）] をクリックします。

ステップ 3 [メッセージ（Messages）] タブをクリックします。

ステップ 4 「RSA SecurID ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 [送信（Submit）] をクリックします。

外部 ID ソースとしての SAMLv2 ID プロバイダー

Security Assertion Markup Language（SAML）は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のアプリケーションにシームレスにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。SAML により、ID プロバイダー（IdP）とサービス プロバイダー（この場合は ISE）の間で、セキュリティ認証情報を交換できます。

SAML シングル サインオン（SSO）は、IdP とサービス プロバイダーの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。サービス プロバイダーは IdP のユーザー情報を信頼して、さまざまなサービスやアプリケーションにアクセスできるようにします。

SAML SSO を有効にすると、次のようないくつかの利点が得られます。

- 異なるユーザー名とパスワードの組み合わせを入力する必要がなくなるため、パスワードの劣化が軽減します。
- 同じ ID に資格情報を再入力する時間が省けるため、生産性が向上します。
- アプリケーションをホストしているお使いのシステムからサードパーティのシステムに、認証を転送します。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

IdP は、ユーザー、システム、またはサービスの ID 情報を作成、維持、管理する認証モジュールです。IdP は、ユーザー クレデンシャルを保管、検証し、ユーザーがサービス プロバイダーの保護リソースにアクセスできる SAML 応答を生成します。

（注） IdP サービスをよく理解している必要があります。現在インストールされていて、操作可能であることを確認してください。

SAML SSO は次のポータルでサポートされます。

- ゲスト ポータル（スポンサー付きおよびアカウント登録）
- スポンサー ポータル
- デバイス ポータル
- 証明書プロビジョニング ポータル

BYOD ポータルでは外部 ID ソースとして IdP を選択できませんが、ゲスト ポータルでは IdP を選択し、BYOD フローをイネーブルにできます。

Cisco ISE は SAMLv2 に準拠しており、Base64 でエンコードされた証明書を使用するすべての SAMLv2 準拠 IdP をサポートしています。次に示す IdP が Cisco ISE でテストされました。

- Oracle Access Manager（OAM）
- Oracle Identity Federation（OIF）
- SecureAuth
- PingOne
- PingFederate
- Microsoft Entra ID

IdP は、ID ソース順序に追加できません。

指定された時間（デフォルトでは5分）にアクティビティがない場合は、SSOセッションが終了し、セッション タイムアウトのエラー メッセージが表示されます。

ポータルの [エラー（Error）] ページに [再度サインオン（Sign On Again）] ボタンを追加する場合は、[ポータルエラー（Portal Error）] ページの [オプションコンテンツ（Optional Content）] フィールドに次の JavaScript を追加します。

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'"
type="button">SignOn Again</button>
```

セッションサービスの有効化

始める前に

セッションサービスは、SAML SSO を有効にするノードで有効にする必要があります。このオプションを有効にするには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 ノードを選択して、[編集（Edit）] をクリックします。

ステップ 3 [全般設定（General Settings）] タブで [ポリシーサービス（Policy Service）] トグルボタンを有効にします。

ステップ 4 [セッションサービスの有効化（Enable Session Services）] チェックボックスをオンにして、[保存（Save）] をクリックします。

Cisco ISE での SAML ID プロバイダーの設定

Cisco ISE で SAML ID プロバイダーを設定するには、次の手順を実行します。

- Cisco ISE のネットワーク管理者またはシステム管理者である必要があります。
- 使用する証明書が ID プロバイダー（IdP）で自己署名されていない場合は、信頼できる証明書ストアに認証局（CA）証明書をインポートします。
- 設定している IdP ポータルへの管理者アクセス権が必要です。次のタスクには、IdP ポータルで実行する複数の手順が含まれます。

Cisco ISE で SAML ID プロバイダーを設定するには、次の手順を実行します。

1. Cisco ISE に SAML ID プロバイダーを追加します。
2. ポータルの認証方式として SAML ID プロバイダーを追加します。
3. SAML ID プロバイダーを設定します。

Cisco ISE への SAML ID プロバイダーの追加

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [外部 ID ソース（External Identity Sources）] > [SAML ID プロバイダー（SAML Id Providers）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 表示される [SAML ID プロバイダー（SAML Identity Provider）] ウィンドウで [全般（General）] タブの [ID プロバイダー名（Id Provider Name）] と [説明（Description）] に入力します。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 [ID プロバイダー設定（Identity Provider Config）] タブで、関連する metadata.xml ファイルをインポートし、[送信（Submit）] をクリックします。

Cisco ISE リリース 3.3 では、インポートしたメタデータファイルに自己署名証明書が含まれている場合、その証明書は Cisco ISE の信頼できる証明書ストアに自動的に追加されます。その後は、信頼できる証明書ストアでその証明書にアクセスできます。

（注） [認証要求に署名（Want Authentication Requests Signed）] チェックボックスは読み取り専用です。オプションの選択または非選択は、アップロードするメタデータ XML ファイルの情報に基づいて自動的に行われます。

認証要求に署名する必要があるかどうかを選択するには、[詳細設定（Advanced Settings）] タブの [認証要求の署名（Sign Authentication Request）] チェックボックスを使用します。認証要求の署名の実行が優先されます。

ポータルの認証方式としての SAML ID プロバイダの追加

作成した SAML ID プロバイダーを次のポータルに追加できます。

1. アカウント登録ゲストポータルとスポンサーゲストポータル（**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > ポータルとコンポーネント（Portals and Components）]**）
2. 証明書プロビジョニングポータル（**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisoning）] > [証明書プロビジョニングポータル（デフォルト）（Certificate Provisioning Portal）]**）

ステップ 1 設定するポータルの [ポータルのカスタマイズ（Portal Customization）] ウィンドウで、[ポータル設定（Portal Settings）] ボタンをクリックします。

ステップ 2 表示されるドロップダウンセクションで、[認証方式（Authentication Method）] セクションに移動し、メニューを使用して追加した SAML IP プロバイダーを選択します。

ステップ 3 [保存（Save）] をクリックします。

SAML ID プロバイダーの設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [外部 ID ソース（External Identity Sources）] > [SAML ID プロバイダー（SAML Id Providers）]** を選択します。ポータルにリンクする IdP を選択し、[編集（Edit）] をクリックします。

ステップ 2 （オプション）ロードバランサを使用して Cisco ISE ノードの負荷を最適化する場合は、[サービスプロバイダー情報（Service Provider Info）] タブにロードバランサの詳細を追加して、IdP の設定を簡素化できます。ソフトウェアまたはハードウェアのロードバランサを追加できます。

ロードバランサは、[ポータル設定（Portal Settings）] ウィンドウで指定されたポートを使用して、展開内の Cisco ISE ノードに要求を転送できる必要があります。

ロードバランサを追加すると、そのロードバランサの URL だけがサービスプロバイダーのメタデータファイルで提供されます。ロードバランサが存在しない場合は、複数の AssertionConsumerService URL がサービス プロバイダーのメタデータファイルに含まれます。

（注） ポータル FQND 設定でロード バランサに同じ IP アドレスを使用しないようにすることが推奨されます。

ステップ 3 [サービスプロバイダー情報（Service Provider Info）] タブで、[エクスポート（Export）] をクリックして、サービス プロバイダーのメタデータ ファイルをエクスポートします。エクスポートされたメタデータには、Cisco ISE の署名証明書が含まれており、これは選択したポータルの証明書と同一です。

エクスポートされたメタデータの ZIP フォルダには、各 IdP（Microsoft Entra ID、PingOne、PingFederate、SecureAuth、OAM など）の設定に関する基本的な説明を含む Readme ファイルが含まれています。

次の内容に変更がある場合は、サービスプロバイダーのメタデータを再エクスポートする必要があります。

- 新しい Cisco ISE ノードの登録。
- ノードのホスト名または IP アドレス。
- デバイス、スポンサー、または証明書プロビジョニングポータルの完全修飾ドメイン名（FQDN）。
- ポートおよびインターフェイスの設定。
- 関連するロードバランサ。

更新されたメタデータが再エクスポートされない場合、 IdP でユーザー認証要求が拒否される可能性があります。

ステップ 4 IdP ポータルに移動し、管理者ユーザーとしてログインし、Cisco ISE からエクスポートしたサービスプロバイダーのメタデータファイルをインポートします。最初に、エクスポートしたフォルダとメタデータファイルをポータルの名前で解凍する必要があります。メタデータ ファイルには、プロバイダー ID とバインディング URI が含まれています。

ステップ 5 Cisco ISE ポータルに戻ります。

ステップ 6 （オプション）[SAML ID プロバイダー（SAML Identity Provider）] ウィンドウの [グループ（Groups）] タブで、必要なユーザーグループを追加します。

[グループ メンバーシップ属性（Group Membership Attribute）] フィールドにユーザーのグループ メンバーシップを指定するアサーション属性を入力します。

ステップ 7 （オプション）[属性（Attributes）] タブでユーザー属性を追加し、IdP から返されるアサーションでの属性の表示方法を指定します。

[ISE の名前（Name in ISE）] フィールドに指定した名前はポリシー ルールに表示されます。

属性でサポートされているのは、次のデータ型です。

- 文字列
- 整数
- IPv4
- ブール値

ステップ 8 [詳細設定（Advanced Settings）] タブで、次のオプションを設定します。

オプション	説明
ID属性	表示されるオプションのオプションボタンをクリックして、認証されているユーザーの ID を指定する属性を選択します。 （注） Cisco ISE は、件名（NameID）が一時的なまたは永続的な形式で含まれる SAML IdP 応答をサポートしていません。このような方法が使用され、認証が失敗する場合、Cisco ISE は SAML IdP 応答からユーザー名属性アサーションを取得できません。
メール属性	ドロップダウンリストから、ユーザーの電子メールアドレスを返すアサーション属性を選択します。スポンサー付きゲストのリストが 1 人のスポンサーによって承認されるようにフィルタ処理（制限）する場合は、電子メール属性を設定する必要があります。
複数値属性	次のいずれかを選択します。 • [個別の XML 要素で各値（Each value in a separate XML element）]：IdP が個別の XML 要素で同じ属性の複数の値を返す場合は、このオプションをクリックします。 • [単一の XML 要素で複数の値（Multiple values in a single XML element）]：IdP が単一の XML 要素で複数の値を返す場合は、このオプションをクリックします。テキストボックスにデリミタを指定します。
認証設定	Cisco ISE では、定義された証明書を使用して認証要求に署名されます。SAML 署名要求の場合、SAML 署名証明書を適切に定義する必要があります。 **1. 要求** • [署名認証要求（Sign Authentication Request）]：外部 ID プロバイダに署名付き要求が必要な場合は、このチェックボックスをオンにします。PingFederate などの一部の ID プロバイダには、署名付き認証要求が必要です。 • [証明書情報を含める（Include Certificate Info）]：認証要求に特定の証明書に関する情報を含めるには、このチェックボックスをオンにします。 **2. 応答の署名** （注） デフォルトでは、Cisco ISE には少なくとも 1 つの署名付き SAML 応答または署名付き SAML アサーションが必要です。Cisco ISE では、[SAML 署名付き応答が必要（Require SAML Signed Response）] チェックボックスと [署名付きアサーションが必要（Require Assertions Signed）] チェックボックスがオフになっている場合でも必要になります。 適切なチェックボックスをオンにして、次のオプションから特定の署名を選択できます。 • [SAML 署名付き応答が必要（Require SAML Signed Response）]：このオプションを選択すると、Cisco ISE は署名付き SAML 応答のみを受け入れます。

オプション	説明
	• [署名付きアサーションが必要（Require Assertions Signed）]：このオプションを選択すると、Cisco ISE は署名付き SAML アサーションを含む SAML 応答のみを受け入れます。 **3. アサーションの暗号化** • [暗号化されたアサーションが必要（Require Assertions Encrypted）]：このオプションを選択すると、Cisco ISE は暗号化された SAML アサーションのみを受け入れます。
ログアウト設定	[ログアウト要求の署名（Sign Logout Requests）]：ログアウト要求に署名する場合は、このチェックボックスをオンにします。このオプションは、設定されている IdP が Oracle Access Manager または Oracle Identity Federation の場合は表示されません。 （注） SecureAuth は SAML ログアウトをサポートしていません。 次のオプションは、Oracle Access Manager または Oracle Identity Federation IdP を設定していて、ロードバランサが設定されていない場合にのみ表示されます。 • [ログアウト URL（Logout URL）]：ユーザーがスポンサーまたはデバイスポータルからログアウトするときに、SSO セッションを終了するためにリダイレクトされるページの URL を入力します。 • [リダイレクトパラメータ名（Redirect Parameter Name）]：SSO セッションが終了すると、ユーザーは IdP のログインページに戻ります。リダイレクトパラメータ名は、end_url や returnURL など、IdP によって異なる場合があります。このフィールドは大文字と小文字が区別されます。 ログアウトが正常に機能しない場合は、IdP のマニュアルで、ログアウト URL およびリダイレクトパラメータ名の使用に関する詳細を確認してください。
認証コンテキスト	このセクションを使用して、SAML IdP 認証コンテキストクラス参照を編集します。Cisco ISE SAML 要求では、通常、SAML 要求ヘッダーで **PasswordProtectedTransport** 認証方式が使用されます。この結果、多要素認証が使用されている場合に認証が失敗します。 これを回避するには、**AuthnContextClassRef SAML Element** セクションを使用して認証方式を指定します。使用する認証方式が不明な場合は、認証の失敗を防ぐために、このセクションを空白のままにすることを推奨します。

ステップ 9 [送信（Submit）] をクリックします。

ID プロバイダーの削除

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

削除する IdP がいずれのポータルにもリンクされていないことを確認します。IdP がポータルにリンクされている場合、削除操作は失敗します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [外部 ID ソース（External Identity Sources）] > [SAML ID プロバイダー（SAML Id Providers）]**を選択します。

ステップ 2 削除する IdP の隣のチェックボックスをオンにして、[削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして、選択した IdP を削除します。

SAML ベースの管理者ログイン

SAML ベースのログインでは、SAML 2.0 標準規格を使用してシングルサインオン（SSO）機能を Cisco ISE に追加します。Okta などの外部 ID プロバイダ（IdP）や、SAML 2.0 標準を実装するその他の IdP を使用できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [SAML Idプロバイダー（SAML Id Providers）] > [追加（Add）] > [一般（General）]** の順に選択します。

ステップ 2 [アイデンティティ プロバイダー名（Id Provider Name）] フィールドに値を入力します。

ステップ 3 [送信（Submit）] をクリックします。

ステップ 4 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [System（システム）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [認証方式（Authentication Method）]** を選択します。

ステップ 5 [パスワードベース（Password Based）] オプションボタンをクリックします。

ステップ 6 [ID ソース（Identity Source）] ドロップダウンリストから、前の手順で作成した IdP 名を選択します。

ステップ 7 **[保存（Save）]**をクリックします。

ステップ 8 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [SAML Idプロバイダー（SAML Id Providers）]** の順に選択します。

ステップ 9 前の手順で作成した IdP の横にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 10 [サービスプロバイダー情報（Service Provider Info）] タブで、[エクスポート（Export）] をクリックして、サービスプロバイダーのメタデータをダウンロードします。Cisco ISE メタデータは .xml ファイルとしてエクスポートされます。このメタデータ XML ファイルには、展開内のすべてのノードの **entityID** や

AssertionConsumerService URL などの情報が含まれています。この情報を使用して、外部 ID プロバイダーのノードを設定できます。

ステップ 11 メタデータファイルを開きます。

ステップ 12 外部 ID プロバイダーでプライマリ PAN の URL を設定します。Cisco ISE 管理者は、SAML を使用してアクセスできるすべての Cisco ISE ノードを外部 ID プロバイダーに登録する必要があります。

ステップ 13 外部 ID プロバイダで、エクスポートされたメタデータの [AssertionConsumerService] URL と [entityID] を使用します。

ステップ 14 ID プロバイダーでグループ属性を設定します。

ステップ 15 ID プロバイダーのメタデータをエクスポートします。

ステップ 16 [アイデンティティ プロバイダーの設定（Identity Provider Config）] タブで、[ファイルの選択（Choose File）] をクリックしてアイデンティティ プロバイダーのメタデータをアップロードします。

（注） Cisco ISE 管理者ポータルでは、専用の IdP を使用する必要があります。ゲストポータルなどの他のポータル用に作成された IdP は再利用しないでください。

ステップ 17 [グループ（Groups）] タブで、[グループメンバーシップ属性（Group Membership Attribute）] フィールドに必要な値を入力します。ID プロバイダで使用されていたグループ属性名を使用します。

ステップ 18 [追加（Add）] をクリックします。

ステップ 19 [アサーションの名前（Name in Assertion）] に ID プロバイダで設定されているグループ名を入力します。

ステップ 20 [ISE の名前（Name in ISE）] ドロップダウンリストで、管理者グループを選択します。

ステップ 21 [追加（Add）] をクリックします。

ステップ 22 [保存（Save）] をクリックします。

ステップ 23 変更された Cisco ISE ログインページが表示されます。[SAML でログイン（Log in With SAML）] をクリックして、認証のためにアイデンティティ プロバイダーにリダイレクトします。

（注） マルチノード展開の場合は、IP アドレスの代わりに FQDN を使用してログインします。

重要 Microsoft Entra ID が IdP として使用されているときに、ユーザーが 150 以上のグループのメンバーである場合、ログインアクセスは拒否されます。これを回避するには、次のいずれかを行います。

- 管理者がメンバーであるグループの数を 150 未満に制限します。
- エンタープライズアプリケーション SSO 設定のグループ要求にフィルタを設定し、管理者アクセスに必要なグループのみを抽出して含めます。

これは Microsoft Entra ID の制限です。詳細については、Microsoft Entra ID ドキュメントに含まれる Microsoft のページを参照してください。

認証失敗ログ

SAML ID ストアに対する認証が失敗し、IdP がユーザーを ISE ポータルに（SAML 応答を通じて）リダイレクトすると、ISE は認証ログに障害の理由を報告します。ゲスト ポータルで（BYOD フローの有効無効に関係なく）、認証の失敗の原因を知るために、RADIUS Livelog（[操作（Operations）] > [RADIUS] > [ライブ ログ（Live Logs）]）を確認できます。ポータルおよびスポンサー ポータル認証失敗の原因を把握するためには、デバイス ポータルおよびスポンサー ポータルで、デバイス ログイン/監査レポートとスポンサー ログイン/監査レポート（[操作（Operations）] > [レポート（Reports）] > [ゲスト（Guest）]）を確認できます。

ログアウトで障害が発生した場合、My Devices、スポンサーおよびゲスト ポータルの障害の原因を知るためにレポートおよびログを確認することができます。

認証が失敗する原因には次のものが考えられます。

- SAML 応答の解析エラー
- SAML 応答の検証エラー（不正な発行者など）
- SAML アサーションの検証エラー（誤った対象者など）
- SAML 応答署名の検証エラー（不正な署名など）
- IdP 署名証明書のエラー（失効した証明書など）

（注） Cisco ISE は、暗号化されたアサーションを含む SAML 応答をサポートしていません。IdP で設定すると、ISE に次のエラー メッセージが表示されます：`FailureReason=24803 Unable to find 'username' attribute assertion`。

認証に失敗した場合は、認証ログの「DetailedInfo」属性を確認することを推奨します。この属性では、障害理由に関する追加情報が提供されます。

Cisco pxGrid Direct

（注） Cisco ISE リリース 3.2 パッチ 2 以降では、pxGrid Direct は制御された新規導入（ベータ）機能ではなくなりました。このドキュメントでは、Cisco ISE リリース 3.2 パッチ 2 以降で提供されている pxGrid Direct について説明します。

Cisco ISE リリース 3.2 または 3.2 パッチ 13.2 パッチ 2 以降にアップグレードする前に、設定済みのすべての pxGrid Direct コネクタと、pxGrid Direct コネクタからのデータを使用する認証プロファイルおよび認証ポリシーを削除することを推奨します。Cisco ISE リリース 3.3 にアップグレードした後、pxGrid Direct コネクタを再設定してください。設定済みの pxGrid Direct コネクタを削除しない場合、コネクタはアップグレード中に自動的に削除されます。この削除により、編集も使用も不可能な認証プロファイルと認証ポリシーが作成されます。これらを削除して新しいものに置き換える必要があります。

pxGrid Direct コネクタを作成、編集、有効化、および無効化するには、Advantage ライセンスが必要です。

Cisco pxGrid Direct は、エンドポイント属性の JSON データを提供し、このデータを Cisco ISE データベースに取得させる外部 REST API に接続できるようにすることで、エンドポイントをより迅速に評価および承認するのに役立ちます。この機能により、エンドポイントを承認する必要があるたびにエンドポイント属性データをクエリする必要がなくなります。その後、取得したデータを認証ポリシーで使用できます。

Cisco pxGrid の詳細については、『Cisco ISE Administrator Guide』の「Cisco pxGridノード」の章を参照してください。

pxGrid Direct は、pxGrid Direct 構成で指定した属性に基づいてデータを収集するのに役立ちます。関連データの取得には、一意の識別子と相関識別子と呼ばれる 2 つの必須フィールドが使用されます。コネクタにこれらのフィールドのいずれかの値が含まれていない場合、コネクタからのデータの取得と保存が誤っている可能性があります。

pxGrid Direct の特徴は次のとおりです。

- ポリシーセットで構成する pxGrid Direct 属性の数に比例して、ポリシー実行の実行時間（1 秒あたりのトランザクション数）が増加します。
- 10 個を超えるコネクタを追加すると、パフォーマンスが低下する可能性があります。

pxGrid Direct は PAN で実行され、取得されたデータがすべての PSN で使用可能になり、認証ポリシーで使用されます。

設定されたコネクタと取得されたエンドポイントデータの詳細は、**[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [pxGrid Directコネクタ（pxGrid Direct Connectors）]**および**[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [pxGrid Directエンドポイント（pxGrid Direct Endpoints）]** ウィンドウで確認できます。

[pxGrid Directエンドポイント（pxGrid Direct Endpoints）] ウィンドウで、エンドポイントをクリックして、スライドインペインに詳細を表示します。

[操作（Operations）] > [レポート（Reports）] > [監査（Audit）] > [変更設定監査（Change Configuration Audit）]ウィンドウで、オブジェクトタイプ名が [pxGrid Directコネクタ操作（pxGrid Direct Connector Operation）] の関連ログを表示できます。

[操作（Operations）] > [トラブルシュート（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグログの設定（Debug Log Configuration）]ウィンドウで、pxGrid Direct デバッグログを設定します。

pxGrid Direct Open API または GUI を使用して、pxGrid Direct コネクタを作成できます。コネクタの作成方法の手順については、「オープン API を使用したコネクタの作成（1200ページ）」または「GUI を使用したコネクタの作成 （1201 ページ）」を参照してください。

pxGrid Direct コネクタは、コネクタにマッピングされた属性に基づいて外部 REST API からデータを取得し、Cisco ISE データベースのエンドポイントテーブルにデータを保存します。コネクタでマッピングされた属性は、認証プロファイルのディクショナリ属性として使用できます。

ディクショナリ属性値に基づいて条件を作成し、エンドポイントが Cisco ISE 環境にアクセスするときに Cisco ISE が実行する必要がある一連のアクションを定義できます。

次のログファイルは、pxGrid Direct コネクタに関連する情報を提供します。

- pxgriddirect.log：取得したエンドポイントデータが受信され、Cisco ISE データベースに保存されたかどうかに関連するログが含まれています。
- pxgriddirect-connector.log：pxGrid Direct コネクタが Cisco ISE に正常に追加されたかどうかを示すログが含まれています。

以下は、Open API GET /api/v1/pxgrid-direct/connector-config/<connector-name> を使用したときに受け取る pxGrid Direct コネクタ設定の応答の例です。pxGrid Direct Open API は、Cisco ISE API - pxGrid Direct のドキュメントにリストされています。

```
{
    "connector": {
      "connectorName": "SNOW_CMDBconnectorfetch",
      "description": "description",
      "connectorType": "urlfetcher",
      "skipCertificateValidations": true,
      "enabled": true,
      "url": {
        "bulkUrl": "https://cmdbhostname.domain/cmdb-random/1",
        "authenticationType": "basic",
        "userName": "BASIC_USER_NAME",
        "password": "BASIC_PASSWORD"
      },
      "fullsyncSchedule": {
        "intervalUnit": "days",
        "interval": 1,
        "startDate": "2022-05-30T09:00:00"
      },
      "attributes": {
        "topLevelObject": "result",
        "uniqueIdentifier": "mac_address",
        "bulkUniqueIdentifier": "mac_address",
```

```
        "attributeMapping": [
          {
            "includeInDictionary": true,
            "jsonAttribute": "group_tag",
            "dictionaryAttribute": "securityTag"
          }
        ]
      }
    }
  }
```

次の例は、`result` に最上位レベルのオブジェクトを含む pxGrid Direct コネクタからの JSON 応答を示しています。上記の GET API のキー **bulkUrl** に記載されている URL を使用すると、次の結果の例が表示されます。

```
{
  "result": [
    {
      "mac_manufacturer": "Example, Incorporated",
      "operational_status": "Operational",
      "sys_updated_on": "2022-03-31 17:27:41",
      "sys_updated_by": "admin",
      "sys_created_on": "2022-01-20 12:23:40",
      "sys_created_by": "admin",
      "cmdb_ci": "Computer1",
      "install_status": "Installed",
      "name": "NetworkAdapter",
      "sys_id": "00abc11xyz",
      "mac_address": "00:00:xx:00:xx:xx",
      "group_tag": "0123"
    }
  ]
}
```

`group_tag` と `mac_address` の属性は、この JSON 応答から選択されます。これらの属性は、pxGrid Direct が外部 REST API に接続するときに、この JSON 応答を識別するために pxGrid Direct コネクタによって使用されます。

一括固有識別子と固有識別子は、`mac_address` として定義されます。

最上位オブジェクトは `result` として定義されます。

コネクタの名前は `SNOW_CMDBconnectorfetch` です。

コネクタタイプは `urlfetcher` として定義されます。これは `bulkurl` および `incrementalurl` で定義された URL からデータを取得します。現在、`authenticationType` は `basic` のみに制限されています。

データ同期スケジュールは、データ同期間隔とともに `deltasyncSchedule` と `fullsyncSchedule` で定義されます。`bulkUrl` に記載されている URL は、データの完全同期に使用されます。`IncrementalUrl` に記載されている URL は、データの増分同期に使用されます。

データ同期の間隔

pxGrid Direct コネクタを追加する構成手順には、完全同期および部分同期をスケジュールするオプションが含まれています。

完全同期は一括データ収集に使用されます（たとえば、最初に外部 REST API に接続してデータを収集する際など）。

外部 REST API から Cisco ISE データベースへの大量のデータ転送によるパフォーマンスの問題を回避するために、営業時間後に完全同期をスケジュールします。

完全同期では、必要に応じて定期的なバルクデータ収集も可能です。

増分同期は、完全同期を使用してすでにデータを収集した外部 REST API からのデータを更新する必要がある場合に使用されます。

Cisco ISE リリース 3.4、Cisco ISE リリース 3.3 パッチ 2 および Cisco ISE リリース 3.2 パッチ 5 以降、[pxGrid Direct Connectors] ウィンドウで同期ステータス、同期時間、およびオブジェクトの合計を表示できます。

インスタンス	インターバル（**Interval**）
完全同期のスケジュール	デフォルト：1 週間 最短：12 時間 最長：1 ヵ月
増分同期のスケジュール	デフォルト：1 日 最短：1 時間 最長：1 週間

「今すぐ同期」を使用したオンデマンドの pxGrid 直接データ同期

Cisco ISE リリース 3.4、、 以降では、「**今すぐ同期**」機能を使用して、pxGrid Direct コネクタのデータのオンデマンド同期を実行できます。

pxGrid Direct コネクタを作成、編集、有効化、および無効化するには、Advantage ライセンスが必要です。ただし、pxGrid Direct コネクタが作成された後は、コネクタが編集されるまで、ライセンスステータスに関係なくデータの同期が続行されます。pxGrid Direct コネクタがすでに作成されている場合は、Essentials ライセンスを使用して「今すぐ同期」機能を使用できます。

オンデマンド同期は、完全同期と増分同期の両方でサポートされています。pxGrid Direct コネクタを個別に同期することも、pxGrid Direct コネクタを一括で同期することも可能です。「**今すぐ同期**」 を使用したオンデマンドのデータ同期は、Cisco ISE GUI または OpenAPI を使用して実行できます。現在、コネクタの一括同期は、Cisco ISE GUI を介してのみサポートされています。スケジュールされたデータ同期がコネクタに対して進行中の場合、そのコネクタに対して「**今すぐ同期**」オプションを使用することはできません。同期（スケジュールされた同期または今すぐ同期）の進行中にコネクタを無効にしても、コネクタは進行中のサーバーからのデータ取得を最後まで実行して、Cisco ISE データベースにデータをアップロードします。進行中のデータ取得の後のデータ取得は無効になります。

Cisco ISE GUI の [pxGrid Direct Connectors] ウィンドウの [Sync Now] 列を使用して、1 つ以上の pxGrid Direct コネクタのデータの完全同期または増分同期をオンデマンドで実行できます。（最初にスケジュールされた完全同期の前に）「今すぐ同期」オプションを使用して新しく追加されたコネクタのデータを同期する場合は、**完全同期**を選択することをお勧めします。

- **1 つの pxGrid コネクタを今すぐ同期**：1 つの pxGrid Direct コネクタを同期するには、データ同期要件に応じて、[Sync Now] 列で [Full] または [Incremental] をクリックします。
- **多数の pxGrid コネクタを今すぐ同期**：「今すぐ同期」操作のために選択する pxGrid Direct コネクタの横にあるチェックボックスをオンにします。[Sync Now] ドロップダウンリストから、データ同期要件に応じて [Incremental Sync] または [Full Sync] をクリックします。

（注）
- 一度に同期できる pxGrid Direct コネクタは 5 つだけです。
- 6 つ以上の pxGrid Direct コネクタが選択されている場合、それらはすべてキューに入れられますが、一度に同期されるのはそのうちの 5 つだけです。1 つのコネクタが [Completed] ステータスに移行すると、キュー内の次のコネクタの同期が開始されます。

選択した pxGrid Direct コネクタの最新の同期ステータスを表示するには、[pxGrid Direct Connectors] ウィンドウのテーブルの上部にある [Refresh] をクリックします。[Sync Status] 列に、pxGrid Direct コネクタの同期ステータスが表示されます。同期ステータスは次のとおりです。

同期ステータス	説明
Queued	pxGrid Direct コネクタは、データ同期のためにキューに入っています。
Submitted	pxGrid Direct コネクタのデータ同期が開始されました。このステータスでは、データは外部サーバーから取得されます。
InProgress	pxGrid Direct コネクタのデータ同期が進行中です。このステータスでは、データは外部サーバーから取得され、Cisco ISE に保存されます。 （注） 「今すぐ同期」操作の進行中にスケジュールされた同期サイクルがトリガーされた場合、スケジュールされた同期サイクルはスキップされ、監査ログに記録されます。
Completed	pxGrid Direct コネクタのデータ同期が完了しました。 データはプライマリ PAN に保存され、PSN へのデータの複製はまだ進行中です。
Errored	データの同期中にエラーが発生しました。エラーの詳細については、監査ログを参照してください。

同期ステータス	説明
Cancelled	フェールオーバー中、アップグレード中、または復元操作中に、進行中の同期をキャンセルできます。「今すぐ同期」操作を使用してその pxGrid Direct コネクタのデータ同期を手動でトリガーするか、次の定期的な同期スケジュールを待つことができます。

（注） キューに入れられている同期をキャンセルするには、[Sync Now] 列の [Cancel Sync] をクリックします。同期は、[Queued] 状態の場合にのみキャンセルできます。同期が [InProgress] または [Submitted] 状態に進行した場合、同期をキャンセルすることはできません。

[Last Sync] 列には、pxGrid Direct コネクタの最新のデータ同期の時刻が表示されます。

[Total Objects] 列には、最新の同期後の各 pxGrid Direct コネクタについて Cisco ISE データベースに保存されたオブジェクトの合計数が表示されます。[Refresh] をクリックして同期のステータスを表示すると、列のカウントが変更されます。

（注） コネクタの同期の進行中に PAN フェールオーバーが発生した場合、進行中のデータ同期は自動的に中断し、ステータスは [Canceled] と表示されます。同期を再度手動でトリガーする必要があります。

オープン API を使用したコネクタの作成

始める前に

- プロキシなしで外部サーバーに到達できない場合は、プロキシ接続を設定します。
- 設定する URL で証明書の検証が必要な場合は、必要な証明書を信頼できる証明書ストアにアップロードします。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [API設定（API Settings）]** を選択します。

ステップ 2 [API設定（API Settings）] ウィンドウで、[Swagger API] リンクをクリックします。

ステップ 3 [Cisco ISE API] ウィンドウで、[定義の選択（Select a Definition）] ドロップダウンリストから [pxGrid Direct] を選択します。

ステップ 4 [pxGrid Direct] をクリックします。

ステップ 5 [POST /api/v1/pxgrid-direct/connector-config Configure connnectorconfig information] をクリックします。

ステップ 6 [試してみる（Try it Out）] をクリックします。

ステップ 7 [要求本文（Request Body）] フィールドに、次の詳細を入力します。入力時に入力内容は検証されないことに注意してください。誤ったフィールド名と値を入力すると、Cisco ISE 管理ポータルの設定済みコネクタのリストにコネクタが表示されている場合でも、設定済みコネクタからエンドポイントデータを取得できません。

- ディクショナリ属性
- ディクショナリに含める
- JSON 属性
- 一括固有識別子
- 最上位オブジェクト
- 固有識別子
- 相関識別子
- バージョン ID
- コネクタ名（コネクタ名は 50 文字以内にする必要があります）
- コネクタタイプ
- 差分同期スケジュール
- 完全同期のスケジュール
- プロトコル
- 認証タイプ
- 一括 URL
- 増分 URL

ステップ 8 [実行（Execute）] をクリックします。

GUI を使用したコネクタの作成

Cisco ISE GUI を使用して、pxGrid Direct コネクタを作成できます。pxGrid Direct コネクタタイプには、[URLフェッチャ（URL Fetcher）] と [URLプッシャ（URL Pusher）] の 2 種類があります。Cisco ISE リリース 3.4 以降では、[URLフェッチャ（URL Fetcher）] の pxGrid Direct コネクタタイプまたは [URLプッシャ（URL Pusher）] の pxGrid Direct コネクタタイプのいずれかを選択できます。適切な手順に従って、必要な pxGrid Direct コネクタを作成してください。

- URL プッシャコネクタタイプの作成 （1202 ページ）
- URL フェッチャコネクタタイプの作成 （1203 ページ）

URL プッシャコネクタタイプの作成

ステップ 1 Cisco ISE 管理ポータルで、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [pxGrid Directコネクタ（pxGrid Direct Connectors）]** を選択します。

ステップ 2 [pxGrid Directコネクタ（pxGrid Direct Connectors）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 3 [pxGrid Directコネクタの追加（Add pxGrid Direct Connector）] ウィザードで、[それでは実行しましょう（Let's Do It）] をクリックします。

ステップ 4 [コネクタの定義（Connector Definition）] ウィンドウで、コネクタの名前と説明を入力します。

ステップ 5 ラジオボタンをクリックして、[コネクタタイプ（Connector Type）] として [URLプッシャ（URL Pusher）] を選択します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [管理者グループの権限（Admin Groups' Permissions）] ウィンドウで、管理者グループに付与する権限を選択します。これらの権限は、Cisco ISE 内部ユーザーにのみ付与できます。

- [権限の拒否（Deny Permissions）]：権限を拒否された内部ユーザーは、API を使用して pxGrid Direct データを送受信することができません。
- [読み取り権限（Read Permissions）]：読み取り権限のみを持つ内部ユーザーは、API を使用して pxGrid Direct データを送受信するための制限されたアクセス権を持ちます（GET 操作のみを使用できます）。
- [読み取りおよび書き込み権限（Read and Write Permissions）]：読み取りおよび書き込み権限を持つ内部ユーザーは、API を使用して pxGrid Direct データを送受信できます。少なくとも 1 つの管理者グループに読み取りおよび書き込み権限が必要です。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 （オプション）[サンプルJSON（Sample JSON）] ウィンドウで、属性の選択とディクショナリ項目の設定に必要な属性を取得するためのサンプル JSON を入力します。

参考のために、[サンプルJSON（Sample JSON）] ウィンドウにサンプル JSON の例が示されています。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [属性の選択ディクショナリ項目の設定（Select Attributes Configure Dictionary Items）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 12 [外部名（External Name）] フィールドに、外部 REST API に存在する属性の名前を入力します。

ステップ 13 [ディクショナリに含める（Include in Dictionary）] をクリックして、この外部 REST API 属性を pxGrid Direct コネクタのディクショナリに追加します。

ステップ 14 [ディクショナリでの名前（Name in Dictionary）] フィールドにこの属性の名前を入力します。

ステップ 15 [次へ（Next）] をクリックします。

ステップ 16 [識別子（Identifiers）] ウィンドウの [固有識別子（Unique Identifier）] ドロップダウンリストから、エンドポイントに固有の属性を選択します。

ステップ 17 [相関ID（Correlation ID）] ドロップダウンリストから、Cisco ISE がエンドポイントを認証ポリシーと照合するときに使用する属性を選択します。

ステップ 18 （オプション）[バージョン識別子（Version Identifier）] ドロップダウンリストから、エンドポイントデータのバージョンを記録するのに役立つ属性を選択します。

ステップ 19 [次へ（Next）] をクリックします。

ステップ 20 [設定の概要（Configuration Summary）] ウィンドウで、設定を確認します。続行するには、[完了（Done）] をクリックします。
新しいコネクタが [pxGrid Directコネクタ（pxGrid Direct Connectors）] ウィンドウに表示されます。

[pxGrid Directコネクタ（pxGrid Direct Connectors）] ウィンドウで、pxGrid Direct コネクタを編集、更新、または削除できます。

- pxGrid Direct コネクタを編集するには、編集するコネクタの隣のチェックボックスをオンにして、[編集（Edit）] をクリックします。必要な詳細を更新して、[保存（Save）] をクリックします。
- pxGrid Direct プッシュ API を使用して、エンドポイントデータを Cisco ISE にプッシュすることもできます。pxGrid Direct プッシュ API の詳細については、『Cisco ISE API Reference Guide』を参照してください。

ステップ 21 コネクタが作成されているかどうかを確認するには、次の手順を実行します。

1. Cisco ISE 管理ポータルで、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）]** を選択します
2. [システムディクショナリ（System Dictionaries）] ウィンドウで、コネクタの作成時に指定したコネクタ名をクリックします。
3. [ディクショナリの表示（View Dictionary）] ウィンドウで、[ディクショナリ属性（Dictionary Attributes）] をクリックして、コネクタの作成時に追加したディクショナリ属性を表示します。

URL フェッチャコネクタタイプの作成

始める前に

- プロキシなしで外部サーバーに到達できない場合は、プロキシ接続を設定します。
- 設定する URL で証明書の検証が必要な場合は、必要な証明書を信頼できる証明書ストアにアップロードします。

ステップ 1 Cisco ISE 管理ポータルで、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [pxGrid Directコネクタ（pxGrid Direct Connectors）]** を選択します。

ステップ 2 [pxGrid Directコネクタ（pxGrid Direct Connectors）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 3 [pxGrid Directコネクタの追加（Add pxGrid Direct Connector）] ウィザードで、[それでは実行しましょう（Let's Do It）] をクリックします。

ステップ 4 [コネクタの定義（Connector Definition）] ウィンドウで、コネクタの名前と説明を入力します。

ステップ 5 ラジオボタンをクリックして、[コネクタタイプ（Connector Type）] として [URLフェッチャ（URL Fetcher）] を選択します。

ステップ 6 （オプション）[証明書の検証（Certificate Validations）] の下にある [証明書の検証（Validate Certificate）] チェックボックスをオンにして、証明書を検証します。証明書の検証をスキップする場合は、[証明書の検証（Validate Certificate）] チェックボックスをオフにします。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [URLの追加（Add URL）] ウィンドウで、完全同期のためにデータを取得する必要がある URL を [URL] フィールドに入力します。

ステップ 9 （オプション）[URLの追加（Add URL）] ウィンドウで、増分同期のためにデータを取得する URL を [増分URL（Incremental URL）] フィールドに入力します。Cisco ISE リリース 3.2 パッチ 2 以降では、増分 URL に最新バージョンのコンポーネントを含めることができます。

増分同期 URL の例：
https://<hostname>/api/now/table/test_adapter?sysparm_limit=5&sysparm_query=sys_updated_on>=javascript:gs.dateGenerate('{{LATEST_VERSION}}').

最新バージョン識別子として sys_updated_on を使用する場合、増分同期は、前回のコネクタからのデータフェッチに記載された最新の sys_updated_on 値から開始してエンドポイントデータを取得します。

（注） [同期スケジュールの設定（Set Up Synchronization Schedule）] ウィンドウで増分同期スケジュールを設定するオプションは、[増分URL（Incremental URL）] フィールドに URL を入力した場合にのみ有効になります。

最新バージョンのコンポーネントは、Cisco ISE リリース 3.2 パッチ 1 以前ではサポートされていません。

ステップ 10 [認証（Authentication）] フィールドにログイン情報を入力します。

ステップ 11 [テスト接続（Test Connection）] をクリックして、追加された URL にアクセスできるかどうかを確認します。

ステップ 5 で [証明書の検証（Validate Certificate）] チェックボックスをオンにしておらず、必要な URL 検証証明書が Cisco ISE の信頼できる証明書ストアにアップロードされていない場合は、エラーメッセージが表示されます。必要な証明書を信頼できる証明書ストアにインポートし、証明書の [シスコサービスの認証を信頼する（Trust for Authentication of Cisco Services）] チェックボックスをオンにする必要があります。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 13 [同期スケジュールの設定（Set Up Synchronization Schedule）] ウィンドウで、次のいずれかのオプションを選択します。

- [完全（Full）]：外部 REST API から全データを抽出する場合は、このオプションを選択します。
- [完全および増分（Full and Incremental）]：外部 REST API から全データを抽出し、Cisco ISE データベースのデータを定期的に更新する場合は、このオプションを選択します。

（注） スケジュールは、常に PAN のシステム時刻に基づいて設定されます。

ステップ 14 [完全同期のスケジュール（Schedule Full Sync）] フィールドに、完全同期の期間、開始日、および開始時刻を入力します。

ステップ 15 [増分同期のスケジュール（Schedule Incremental Sync）] フィールドに、増分同期の期間、開始日、および開始時刻を入力します。

（注） このフィールドは、手順 12 で [完全および増分（Full and Incremental）] オプションを選択した場合にのみ表示されます。

ステップ 16 [次へ（Next）] をクリックします。

ステップ 17 [親オブジェクト（Parent Object）] ウィンドウで、残りの属性がクエリされる外部 REST API に存在する JSON ファイルを識別するために必要な [親オブジェクト（Parent Object）] の名前を入力します。

ステップ 18 [次へ（Next）] をクリックします。

ステップ 19 [属性の選択ディクショナリ項目の設定（Select Attributes Configure Dictionary Items）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 20 [外部名（External Name）] フィールドに、外部 REST API に存在する属性の名前を入力します。

ステップ 21 [ディクショナリに含める（Include in Dictionary）] をクリックして、この外部 REST API 属性を pxGrid Direct コネクタのディクショナリに追加します。

ステップ 22 [ディクショナリでの名前（Name in Dictionary）] フィールドにこの属性の名前を入力します。

ステップ 23 [次へ（Next）] をクリックします。

ステップ 24 [識別子（Identifiers）] ウィンドウの [固有識別子（Unique Identifier）] ドロップダウンリストから、エンドポイントに固有の属性を選択します。

ステップ 25 [相関ID（Correlation ID）] ドロップダウンリストから、Cisco ISE がエンドポイントを認証ポリシーと照合するときに使用する属性を選択します。

ステップ 26 （オプション）[バージョン識別子（Version Identifier）] ドロップダウンリストから、エンドポイントデータのバージョンを記録するのに役立つ属性を選択します。

注意 URL フェッチャコネクタタイプを作成するときは、バージョン識別子を使用しないことを推奨します。一括ダウンロード操作中にバージョン識別子を使用すると、コネクタ内の既存のデータが失われます。

ステップ 27 [次へ（Next）] をクリックします。

ステップ 28 [設定の概要（Configuration Summary）] ウィンドウで、設定を確認します。続行するには、[完了（Done）] をクリックします。
新しいコネクタが [pxGrid Directコネクタ（pxGrid Direct Connectors）] ウィンドウに表示されます。

[pxGrid Directコネクタ（pxGrid Direct Connectors）] ウィンドウで、pxGrid Direct コネクタを編集、更新、または削除できます。pxGrid Direct コネクタの [スケジュール設定（Scheduling）] オプションを有効または無効にすることもできます。

- pxGrid Direct コネクタを編集するには、編集するコネクタの隣のチェックボックスをオンにして、[編集（Edit）] をクリックします。必要な詳細を更新して、[保存（Save）] をクリックします。
- コネクタで定義されているように外部 REST API からデータを取得する場合は、コネクタを有効にすることができます。
- 外部 REST API からデータを取得しない場合は、コネクタを無効にすることができます。コネクタを無効にすると、すでに取得しているエンドポイントデータは、Cisco ISE の [pxGridダイレクトコネ

クタ（pxGrid Direct Connectors）] ウィンドウに保持されます。コネクタは、無効になると取得を試行しません。

ステップ 29 コネクタが作成されているかどうかを確認するには、次の手順を実行します。

1. Cisco ISE 管理ポータルで、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** を選択します
2. [システムディクショナリ（System Dictionaries）] ウィンドウで、コネクタの作成時に指定したコネクタ名をクリックします。
3. [ディクショナリの表示（View Dictionary）] ウィンドウで、[ディクショナリ属性（Dictionary Attributes）] をクリックして、コネクタの作成時に追加したディクショナリ属性を表示します。

コネクタ属性を使用した認証プロファイルの設定

ステップ 1 Cisco ISE 管理ポータルで、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** を選択します。

ステップ 2 **[認証（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** を選択します。

ステップ 3 [標準認証プロファイル（Standard Authorization Profiles）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 4 [認証プロファイル（Authorization Profile）] ウィンドウで、認証プロファイルの名前を入力します。

ステップ 5 [詳細な属性の設定（Advanced Attributes Setting）] セクションで、[ディクショナリ（Dictionaries）] ドロップダウンリストから [cisco-av-pair] を選択します。

ステップ 6 [属性値（Attribute Values）] ドロップダウンリストから、必要なディクショナリ属性を選択します。

ステップ 7 [送信（Submit）] をクリックします。

ID ソース順序

ID ソース順序は、Cisco ISE がそれぞれ異なるデータベース内でユーザー クレデンシャルを検索する順序を定義します。

Cisco ISE に接続されている 2 つ以上のデータベースにユーザー情報がある場合、Cisco ISE でこれらの ID ソース内の情報を検索する順序を定義できます。一致が見つかると、Cisco ISE はそれ以上の検索を行いませんが、クレデンシャルを評価し、ユーザーに結果を返します。このポリシーは最初の一致ポリシーです。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲストユーザーがローカル WebAuth を使用して認証できるようにするには、ゲストポータル認証ソースと ID ソース順序の両方に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）]** を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リストフィールドの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストフィールドのデータベースを並べ替えます。

ステップ 6 選択したアイデンティティストアに認証のためにアクセスできない場合は、[高度な検索リスト（Advanced Search List）] 領域で次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus属性をProcessErrorに設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]
- [ユーザーが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]

  Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストフィールドに Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

ID ソース順序の削除

ポリシーで今後使用しない ID ソース順序を削除できます。

始める前に

- 削除する ID ソース順序がいずれの認証ポリシーでも使用されていないことを確認してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]** を選択します。

ステップ 2 削除する ID ソース順序の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして ID ソース順序を削除します。

レポートでの ID ソースの詳細

Cisco ISE は認証ダッシュレットおよび ID ソース レポートで ID ソースに関する情報を提供します。

[認証（Authentications）] ダッシュレット

[認証（Authentications）] ダッシュレットから、障害の理由などの詳細情報にドリルダウンできます。

[操作（Operations）] > [RADIUS ライブログ（RADIUS Livelog）] の順に選択して、リアルタイムで認証の概要を表示します。RADIUS ライブ ログの詳細については、RADIUS ライブ ログ（774 ページ）を参照してください。

ID ソース レポート

Cisco ISE は ID ソースに関する情報を含むさまざまなレポートを提供します。これらのレポートの詳細については、「使用可能なレポート」の項を参照してください。

ネットワークのプロファイリングされたエンドポイント

プロファイラ サービスは、ネットワーク上にあるすべてのエンドポイントの機能（Cisco ISE では ID とも呼ばれる）を、デバイス タイプにかかわらず識別、検索、および特定して、企業ネットワークへの適切なアクセスを保証および維持するのに役立ちます。Cisco ISE プロファイラ機能では、さまざまなプローブを使用して、ネットワーク上にあるすべてのエンドポイントの属性を収集し、それらを既知のエンドポイントが関連ポリシーおよび ID グループに従って分類されるプロファイラ アナライザに渡します。

プロファイラ フィード サービスによって、管理者は、新規および更新されたエンドポイント プロファイリング ポリシーや更新された OUI データベースを、指定された Cisco フィード サーバーからの、サブスクリプションを介した Cisco ISE へのフィードとして取得できます。

プロファイラ条件の設定

次の表では、[プロファイラ条件（Profiler Condition）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[プロファイリング（Profiling）]** です。

表 *96* : プロファイラ条件の設定

フィールド名	使用上のガイドライン
名前（Name）	プロファイラ条件の名前。
説明（Description）	プロファイラ条件の説明。
タイプ（Type）	事前定義済みタイプのいずれかを選択します。
属性名（Attribute Name）	プロファイラ条件が基づく属性を選択します。
演算子（Operator）	演算子を選択します。
属性値（Attribute Value）	選択した属性の値を入力します。事前定義された属性値を含む属性名の場合、事前定義された値のドロップダウン リストが表示され、値を選択できます。
システム タイプ（System Type）	プロファイリング条件は、次のいずれかのタイプになります。 • [シスコ提供（Cisco Provided）] : シスコ提供として識別され、展開時に Cisco ISE によって提供されるプロファイリング条件。システムから編集したり削除したりすることはできません。 • [管理者作成（Administrator Created）] : 管理者作成として識別され、Cisco ISE の管理者として作成したプロファイリング条件。

関連トピック

Cisco ISE プロファイリング サービス （1210 ページ）
プロファイラ条件 （1250 ページ）
プロファイラ フィード サービス （1298 ページ）
プロファイラ条件の作成 （1267 ページ）

Cisco ISE プロファイリング サービス

Cisco Identity Services Engine（ISE）のプロファイリング サービスは、ネットワークに接続されているデバイスおよびその場所を識別します。エンドポイントは Cisco ISE に設定されたエンドポイント プロファイリング ポリシーに基づいてプロファイリングされます。次に、Cisco ISE では、ポリシー評価の結果に基づいてネットワークのリソースにアクセスする権限がエンドポイントに付与されます。

プロファイリング サービス：

- IEEE 規格 802.1X ポートベースの認証アクセス コントロール、MAC 認証バイパス（MAB）認証、およびネットワーク アドミッション コントロール（NAC）をさまざまな規模および複雑度の企業ネットワークに使用して、認証の効率的かつ効果的な展開および継続的な管理を容易にします。
- デバイス タイプにかかわらず、接続されたすべてのネットワーク エンドポイントの機能を特定、検索、および決定します。
- 一部のエンドポイントへのアクセスを誤って拒否しないようにします。

ISE Community Resource

ISE Endpoint Profiles

How To: ISE Profiling Design Guide

プロファイラ ワーク センター

[プロファイラ ワーク センター（Profiler Work Center）] メニュー（[ワーク センター（Work Centers）]>[プロファイラ（Profiler）]）には、すべてのプロファイラ ページが含まれ、ISE の管理者向けの単一の窓口として機能します。[プロファイラ ワーク センター（Profiler Work Center）] メニューには次のオプションがあります：[概要（Overview）]、[外部 ID ストア（Ext ID Stores）]、[ネットワーク デバイス（Network Devices）]、[エンドポイント分類（Endpoint Classification）]、[ノード設定（Node Config）]、[フィード（Feeds）]、[手動スキャン（Manual Scans）]、[ポリシー要素（ポリシーの要素）]、[プロファイリング ポリシー（Profiling Policies）]、[許可ポリシー（Authorization Policy）]、[トラブルシューティング（Troubleshoot）]、[レポート（Reports）]、[設定（Settings）] および [ディクショナリ（Dictionaries）]。

[プロファイラ（Profiler）] ダッシュボード

[プロファイラ（Profiler）] ダッシュボード（[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [エンドポイント分類（Endpoint Classification）]）は、ネットワーク内のプロファイル、エンドポイント、アセットの集中型モニタリング ツールです。このダッシュボードには、グラフと表の形式でデータが表示されます。[プロファイル（Profiles）] ダッシュレットには、ネットワークで現在アクティブな論理プロファイルとエンドポイント プロファイルが表示されます。[エンドポイント（Endpoints）] ダッシュレットには、ネットワークに接続するエ

ンドポイントのIDグループ、PSN、OSタイプが表示されます。[アセット（Assets）]ダッシュレットには、ゲスト、BYOD、企業などのフローが表示されます。表には接続されたさまざまなエンドポイントが表示され、新しいエンドポイントを追加することもできます。

プロファイリング サービスを使用したエンドポイント インベントリ

プロファイリングサービスを使用して、ネットワークに接続されたすべてのエンドポイントの機能を検出、特定、および決定することができます。デバイスのタイプに関係なく、エンドポイントの企業ネットワークへの適切なアクセスを、保障し、保持できます。

プロファイリングサービスでは、エンドポイントの属性をネットワークデバイスとネットワークから収集し、エンドポイントをそのプロファイルに従って特定のグループに分類します。一致したプロファイルを持つエンドポイントがCisco ISEデータベースに保存されます。プロファイリング サービスで処理されるすべての属性は、プロファイラ ディクショナリに定義されている必要があります。

プロファイリングサービスは、ネットワークの各エンドポイントを識別し、そのプロファイルに従ってシステム内の既存のエンドポイントのIDグループ、またはシステム内で作成できる新しいグループにそれらのエンドポイントをグループ化します。エンドポイントをグループ化して既存のIDグループにエンドポイント プロファイリング ポリシーを適用することで、エンドポイントと対応するエンドポイント プロファイリング ポリシーのマッピングを決定できます。

Cisco ISE プロファイラ キュー制限の設定

Cisco ISE プロファイラは、ネットワークから大量のエンドポイント データを短時間で収集します。それにより、一部の遅い Cisco ISE コンポーネントがプロファイラによって生成されるデータを処理するときにバックログが蓄積されるため、Java仮想マシン（JVM）のメモリ使用率が増大し、パフォーマンスの低下および安定性の問題が生じます。

プロファイラが JVM メモリ使用率を増やさず、また、JVM がメモリ不足になり、再起動しないように、プロファイラの次の内部コンポーネントに制限が適用されます。

- エンドポイントキャッシュ：内部キャッシュのサイズは制限され、サイズが制限を超えると定期的に消去する必要があります（最長時間未使用方式に基づく）。
- フォワーダ：プロファイラによって収集されたエンドポイント情報のメイン入力キュー。
- イベントハンドラ：高速コンポーネントを接続解除する内部キューで、（通常、データベースクエリーに関連する）低速処理コンポーネントにデータを提供します。

エンドポイント キャッシュ

- maxEndPointsInLocalDb = 100000（キャッシュ内のエンドポイント オブジェクト）
- endPointsPurgeIntervalSec = 300（秒単位のエンドポイント キャッシュ消去スレッド間隔）
- numberOfProfilingThreads = 8（スレッド数）

制限は、すべてのプロファイラ内部イベント ハンドラに適用されます。キュー サイズ制限に達すると、モニタリング アラームがトリガーされます。

Cisco ISE プロファイラのキュー サイズの制限

- forwarderQueueSize = 5000（エンドポイント収集イベント）
- eventHandlerQueueSize = 10000（イベント）

イベント ハンドラ

- NetworkDeviceEventHandler：すでにキャッシュされているネットワーク アクセス デバイス（NAD）の重複 IP アドレスのフィルタリングのほか、ネットワークデバイスのイベント用。
- ARPCacheEventHandler：ARP キャッシュのイベント用。

Martian IP アドレス

Martian IP アドレスは、RADIUS パーサーがプロファイリングサービスに到達する前にそのようなアドレスを削除するため、**[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** と **[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[エンドポイントの分類（Endpoint Classification）]** ウィンドウには表示されません。Martian IP アドレスは攻撃に対して脆弱であるため、セキュリティ上の懸念事項です。ただし、Martian IP アドレスは監査目的で MnT ログに表示されます。この動作は、マルチキャスト IP アドレスの場合にも当てはまります。Martian IP アドレスの詳細については、https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/250/index.html#page/tesla_250_olh/martian_addresses.html を参照してください。

プロファイラフォワーダ永続キュー

プロファイラ フォワーダ永続キューは、イベントがさらなる処理のためにプロファイラ モジュールに送信される前に、それらのイベントを保存します。さらに、キューイングキャパシティも増加し、イベント処理の増加をサポートしています。これにより、イベント数が急激に増加したために失われるイベントの数が減少します。これにより、キューが最大制限に達したときに発生するアラームが減少します。

この機能はデフォルトでイネーブルになっています。必要な場合、この機能を無効にして元のメカニズムにフォールバックすることができます。その場合、イベントは直接プロファイラモジュールに送信されます。この機能を有効または無効にするには、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロファイリング（Profiling）]** を選択し、[プロファイラフォワーダ永続キューの有効化（Enable Profiler Forwarder Persistence Queue）] チェックボックスをオンまたはオフにします。

Cisco ISE ノードでのプロファイリング サービスの設定

Cisco ISE 対応のネットワークでネットワーク リソースを使用しているすべてのエンドポイントのコンテキスト インベントリを提供するプロファイリング サービスを設定できます。

デフォルトですべての管理、モニタリング、およびポリシー サービスのペルソナを担当する単一の Cisco ISE ノードで実行されるようにプロファイリング サービスを設定できます。

分散展開では、プロファイリング サービスは、ポリシー サービス ペルソナを担当する Cisco ISE ノードでのみ実行され、管理ペルソナとモニタリング ペルソナを担当する他の Cisco ISE ノードでは実行されません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 2 ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。

ステップ 3 [展開ノード（Deployment Nodes）] ページで [編集（Edit）] をクリックします。

ステップ 4 [全般設定（General Settings）] タブで [ポリシー サービス（Policy Service）] チェックボックスをオンにします。[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 次の作業を実行します。

a) [セッション サービスの有効化（Enable Session Services）] チェックボックスをオンにして、ネットワーク アクセス セッション サービス、ポスチャ セッション サービス、ゲスト セッション サービス、およびクライアント プロビジョニング セッション サービスを実行します。

b) [プロファイリング サービスの有効化（Enable Profiling Service）] チェックボックスをオンにして、プロファイリング サービスを実行します。

c) デバイス管理サービスを実行し、企業のネットワーク デバイスを制御および監査するには、[デバイス管理サービスの有効化（Enable Device Admin Service）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックしてノード設定を保存します。

プロファイリング サービスによって使用されるネットワーク プローブ

ネットワーク プローブは、ネットワーク上のエンドポイントから属性を収集するために使用される方法です。プローブを使用して、エンドポイントを Cisco ISE データベース内の一致するプロファイルで作成または更新できます。

Cisco ISE では、ネットワーク デバイスの動作を分析してデバイス タイプを決定する多数のネットワーク プローブを使用して、デバイスをプロファイリングすることができます。ネットワーク プローブは、ネットワーク可視性の向上に役立ちます。

IP アドレスと MAC アドレスのバインディング

エンドポイントを作成または更新するには、企業ネットワークの MAC アドレスのみを使用できます。ARP キャッシュにエントリが見つからない場合は、Cisco ISE で HTTP パケットの L2 MAC アドレスと NetFlow パケットの IN_SRC_MAC を使用してエンドポイントを作成または更新できます。エンドポイントが 1 ホップだけ離れている場合、プロファイリング サービスは L2 隣接関係に依存します。エンドポイントに L2 隣接関係がある場合、エンドポイントの IP アドレスと MAC アドレスはすでにマッピングされているため、IP-MAC キャッシュ マッピングは必要ありません。

エンドポイントに L2 隣接関係が存在せず、エンドポイントが複数ホップ離れている場合、マッピングは信頼できない場合があります。収集する NetFlow パケットの既知の属性には、PROTOCOL、L4_SRC_PORT、IPV4_SRC_ADDR、L4_DST_PORT、IPV4_DST_ADDR、IN_SRC_MAC、OUT_DST_MAC、IN_SRC_MAC、OUT_SRC_MAC などがあります。エンドポイントに L2 隣接関係が存在せず、L3 ホップに関して複数ホップ離れている場合は、IN_SRC_MAC 属性で L3 ネットワーク デバイスの MAC アドレスのみが伝送されます。Cisco ISE で HTTP プローブが有効になっている場合は、HTTP 要求メッセージによってペイロード データでエンドポイントの IP アドレスと MAC アドレスが伝送されないため、HTTP パケットの MAC アドレスを使用してのみエンドポイントを作成できます。

Cisco ISE では、プロファイリング サービスで ARP キャッシュが実装されるため、エンドポイントの IP アドレスと MAC アドレスを確実にマッピングできます。ARP キャッシュを機能させるには、DHCP プローブまたは RADIUS プローブを有効にする必要があります。DHCP プローブと RADIUS プローブは、ペイロード データでエンドポイントの IP アドレスと MAC アドレスを伝送します。DHCP プローブの dhcp-requested address 属性と RADIUS プローブの Framed-IP-address 属性によって、エンドポイントの IP アドレスがその MAC アドレスとともに伝送されます。これらのアドレスは、マッピングして ARP キャッシュに格納できます。

NetFlow プローブ

Cisco ISE プロファイラは Cisco IOS NetFlow Version 9 を実装しています。NetFlow Version 9 には、Cisco ISE プロファイリング サービスをサポートするためのプロファイラの拡張に必要な追加機能があるため、これを使用することを推奨します。

NetFlow Version 9 の属性を NetFlow 対応のネットワーク アクセス デバイスから収集して、エンドポイントを作成したり、Cisco ISE データベース内の既存のエンドポイントを更新できます。NetFlow Version 9 は、エンドポイントの送信元 MAC アドレスと宛先 MAC アドレスを割り当てて、更新するように設定できます。NetFlow 属性のディクショナリを作成して NetFlow ベースのプロファイリングに対応することもできます。

NetFlow Version 9 レコード フォーマットの詳細については、『NetFlow Version 9 Flow-Record Format』マニュアルの表 6「NetFlow Version 9 Field Type Definitions」を参照してください。

さらに、Cisco ISE は Version 5 以前の NetFlow バージョンをサポートします。ネットワークで NetFlow Version 5 を使用する場合は、Version 5 をアクセス レイヤのプライマリ ネットワーク アクセス デバイス（NAD）でのみ使用できます。他のデバイスでは動作しません。

Cisco IOS NetFlow Version 5 パケットには、エンドポイントの MAC アドレスが含まれません。NetFlow Version 5 から収集された属性は、Cisco ISE データベースに直接追加できません。IP アドレスを使用してエンドポイントを検出し、エンドポイントに NetFlow Version 5 の属性を付加できます。このことは、ネットワーク アクセス デバイスの IP アドレスと NetFlow Version 5 属性から抽出される IP アドレスを組み合わせることによって実行できます。ただし、これらのエンドポイントを RADIUS または SNMP プローブで事前に検出しておく必要があります。

NetFlow Version 5 以前のバージョンでは、MAC アドレスは IP フローの一部ではありません。このため、エンドポイントのキャッシュにあるネットワーク アクセス デバイスから収集された属性情報を関連付けることにより、エンドポイントの IP アドレスをプロファイリングすることが必要となります。

NetFlow Version 5 レコード フォーマットの詳細については、『NetFlow Services Solutions Guide』の表 2「Cisco IOS NetFlow Flow Record and Export Format Content Information」を参照してください。

DHCP プローブ

Cisco ISE 展開内のダイナミック ホスト コンフィギュレーション プロトコル プローブを使用すると、Cisco ISE プロファイリングサービスで INIT-REBOOT および SELECTING のメッセージタイプの新しい要求だけに基づいてエンドポイントを再プロファイリングできます。RENEWING や REBINDING などの他の DHCP メッセージ タイプは処理されますが、エンドポイントのプロファイリングには使用されません。DHCP パケットから解析された属性は、エンドポイント属性にマッピングされます。

Cisco ISE リリース 3.3 以降、IPv6 は DHCP プローブでサポートされます。

INIT-REBOOT 状態中に生成された DHCPREQUEST メッセージ

DHCP クライアントが前に割り当てられてキャッシュされた設定を確認する場合、クライアントはサーバー識別子（server-ip）オプションを入力できません。代わりに、前に割り当てられた IP アドレスを要求された IP アドレス（requested-ip）オプションに入力する必要があります。また、DHCPREQUEST メッセージの Client IP Address（ciaddr）フィールドをゼロで埋める必要があります。要求された IP アドレスが正しくない場合、またはクライアントが誤ったネットワークに配置されている場合、DHCP サーバーは DHCPNAK メッセージをクライアントに送信します。

SELECTING 状態中に生成された DHCPREQUEST メッセージ

DHCP クライアントは、サーバー識別子（server-ip）オプションで選択された DHCP サーバーの IP アドレスを挿入し、要求された IP アドレス（requested-ip）オプションにクライアントによって選択された DHCPOFFER の Your IP Address（yiaddr）フィールドの値を入力します。また、「ciaddr」フィールドをゼロで埋めます。

表 *97:* さまざまな状態からの *DHCP* クライアント メッセージ

—	INIT-REBOOT	SELECTING	RENEWING	REBINDING
broadcast/unicast	broadcast	broadcast	unicast	broadcast
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP address	IP address

DHCP ブリッジ モードのワイヤレス LAN コントローラ設定

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）ブリッジ モードでワイヤレス LAN コントローラ（WLC）を設定することを推奨します。このモードでは、ワイヤレス クライアントから Cisco ISE にすべての DHCP パケットを転送できます。WLC Web インターフェイスの **[コントローラ（Controller）]** > **[詳細設定（Advanced）]** > **[DHCPマスターコントローラモード（DHCP Master Controller Mode）]** > **[DHCPパラメータ（DHCP Parameters）]** で使用可能な [DHCPプロキシの有効化（Enable DHCP Proxy）] チェックボックスをオフにする必要があります。DHCP IP ヘルパー コマンドが Cisco ISE ポリシー サービス ノードを指していることも確認する必要があります。

DHCP SPAN プローブ

DHCP スイッチド ポート アナライザ（SPAN）プローブは、Cisco ISE ノードで初期化されると、特定インターフェイス上のネットワーク アクセスデバイスからのネットワーク トラフィックをリッスンします。DHCP SPAN パケットを DHCP サーバーから Cisco ISE プロファイラに転送するようにネットワーク アクセス デバイスを設定する必要があります。プロファイラはこれらの DHCP SPAN パケットを受信して解析し、エンドポイントのプロファイリングに使用できるエンドポイント属性を取得します。

次に例を示します。

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

HTTP プローブ

HTTP プローブでは、識別文字列が HTTP 要求ヘッダー フィールド User-Agent を使って転送されます。このフィールドは、IP タイプのプロファイリング条件の作成、および Web ブラウザ情報の確認に使用される属性です。プロファイラは Web ブラウザ情報を User-Agent 属性および要求メッセージの他の HTTP 属性から取得し、エンドポイント属性のリストに追加します。

Cisco ISE はポート 80 およびポート 8080 で Web ブラウザからの通信をリッスンします。Cisco ISE には、多くのデフォルト プロファイルが用意されています。これらのプロファイルはシステムに組み込まれ、User-Agent 属性に基づいてエンドポイントを識別します。

HTTP はデフォルトで有効になっています。CWA、Hotspot、BYOD、MDM、およびポスチャなどの複数の ISE サービスは、クライアントの Web ブラウザの URL リダイレクトに依存しています。リダイレクトされるトラフィックには、接続されたエンドポイントの RADIUS セッション ID が含まれています。PSN でこれらの URL リダイレクトフローを終端すると、復号化された HTTPS データが可視化されます。HTTP プローブが PSN で無効になっている場合でも、ノードは Web トラフィックからブラウザのユーザーエージェント文字列を解析し、関連付けられたセッション ID に基づいてエンドポイントにデータを関連付けます。この方法でブラウザ文字列が収集されると、データのソースが HTTP プローブではなく、ゲストポータルまたは CP（クライアント プロビジョニング）としてリストされます。

Cisco ISE リリース 3.3 以降では、HTTP プローブで IPv6 がサポートされます。

HTTP SPAN プローブ

Cisco ISE 展開の HTTP プローブをスイッチド ポート アナライザ（SPAN）プローブとともに有効にすると、プロファイラは指定されたインターフェイスからの HTTP パケットをキャプチャできます。SPAN 機能は、Cisco ISE サーバーが Web ブラウザからの通信をリッスンするポート 80 で使用できます。

HTTP SPAN は、HTTP 要求ヘッダー メッセージの HTTP 属性を IP ヘッダー（L3 ヘッダー）の IP アドレスとともに収集し、L2 ヘッダーのエンドポイントの MAC アドレスに基づいてエンドポイントに関連付けることができます。この情報は、Apple デバイスやさまざまなオペレーティング システムのコンピュータなどの各種モバイルおよびポータブル IP 対応デバイスを識別するのに役立ちます。ゲスト ログインまたはクライアント プロビジョニング ダウンロード時に Cisco ISE サーバーでキャプチャをリダイレクトするため、各種モバイルおよびポータブル IP 対応デバイスの識別の信頼性が向上しました。これにより、プロファイラは User-Agent 属性とその他の HTTP 属性を要求メッセージから取得し、Apple デバイスなどのデバイスを識別できます。

VMware で実行中の Cisco ISE の HTTP 属性の収集の無効化

Cisco ISE を ESX サーバー（VMware）に展開している場合、Cisco ISE プロファイラはダイナミック ホスト コンフィギュレーション プロトコル トラフィックを収集しますが、vSphere クライアント上の設定の問題により HTTP トラフィックを収集しません。VMware セットアップで HTTP トラフィックを収集するには、Cisco ISE プロファイラのために作成する仮想スイッチの無差別モードを Accept から Reject（デフォルト）に変更して、セキュリティを設定します。DHCP および HTTP のスイッチド ポート アナライザ（SPAN）プローブが有効になっている場合は、Cisco ISE プロファイラによって DHCP トラフィックと HTTP トラフィックの両方が収集されます。

pxGrid プローブ

PxGrid プローブは、外部ソースからエンドポイントコンテキストを受信するために Cisco pxGrid を利用します。Cisco ISE 2.4 より前は、Cisco ISE はパブリッシャおよび共有されたさまざまなコンテキスト情報（セッション id、グループ情報、外部サブスクライバへの設定要素など）のみを提供していました。Cisco ISE 2.4 での pxGrid プローブの導入により、パブリッシャおよび

Cisco ISE ポリシーサービスノードがサブスクライバになるという他のソリューションが提供されます。

pxGrid プローブは、エンドポイントアセットのトピック /topic/com.cisco.endpoint.asset、サービス名 com.cisco.endpoint.asset を使用する pxGrid v2 仕様に基づいています。次の表に、プレフィックス asset が先行するすべてのトピック属性を示します。

表 *98 :* エンドポイントアセットのトピック

属性名	タイプ	説明
assetId	長整数型	アセット ID
assetName	文字列	アセット名
assetIpAddress	文字列	IP アドレス
assetMacAddress	文字列	MAC アドレス
assetVendor	文字列	製造元
assetProductId	文字列	製品コード
assetSerialNumber	文字列	シリアル番号
assetDeviceType	文字列	デバイスタイプ
assetSwRevision	文字列	S/W リビジョン番号
assetHwRevision	文字列	H/W リビジョン番号
assetProtocol	文字列	プロトコル
assetConnectedLinks	配列	ネットワーク リンク オブジェクトの配列
assetCustomAttributes	配列	カスタム名と値のペアの配列

デバイスの MAC アドレス（assetMacAddress）や IP アドレス（assetIpAddress）などのネットワーク資産を追跡するために一般的に使用される属性に加えて、このトピックでは、ベンダーが固有のエンドポイント情報をカスタム属性（assetCustomAttributes）として公開することができます。Cisco ISE でエンドポイントカスタム属性を使用すると、pxGrid で共有される一意のベンダー属性セットごとにスキーマの更新を必要とせずに、さまざまな使用例に関するトピックを拡張できます。

RADIUS プローブ

Cisco ISE で認証に RADIUS を使用するように設定し、クライアント サーバー トランザクションで使用できる共有秘密を定義できます。RADIUS サーバーから RADIUS 要求および応答メッセージを受信すると、プロファイラはエンドポイントのプロファイリングに使用できる RADIUS 属性を収集できます。

Cisco ISE は RADIUS サーバーおよび他の RADIUS サーバーに対する RADIUS プロキシ クライアントとして動作できます。プロキシ クライアントとして動作する場合は、外部の RADIUS サーバーを使用して RADIUS 要求および応答メッセージを処理します。

また、RADIUS プローブは、デバイスセンサーによって RADIUS アカウンティングパケットで送信された属性も収集します。詳細については、Cisco IOS センサー組み込みスイッチからの属性の収集 （1235 ページ）およびCisco IOS センサー組み込みネットワーク アクセス デバイスの設定チェックリスト （1235 ページ）を参照してください。

RADIUS プローブは、プロファイルサービス用に設定されていないシステムであっても、デフォルトで実行し、ISE がコンテキスト可視性サービスで使用するエンドポイント認証および認可の詳細を追跡できるようにします。

また、RADIUS プローブサービスおよびプロファイリングサービスは、消去操作のために登録されたエンドポイントの作成および更新の時間を追跡するためにも使用されます。

Cisco ISE リリース 3.3 以降、IPv6 は RADIUS プローブでサポートされます。

表 *99 : RADIUS* プローブを使用して収集した共通属性

ユーザー名	発信側ステーションID	着信側ステーションID	フレーム IP アドレス
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
デバイスタイプ（NAD）	ロケーション（NAD）	認証ポリシー	許可ポリシー

（注） Cisco ISE がアカウンティング終了を受信すると、エンドポイントが最初に IP アドレスでプロファイルされた場合、対応するエンドポイントを再プロファイルするように Cisco ISE がトリガーされます。したがって、IP アドレスを使用してプロファイルされたエンドポイントのカスタムプロファイルがある場合、これらのプロファイルの確実度係数の合計を満たす唯一の方法は、プロファイルが対応する IP アドレスで一致することです。

ネットワーク スキャン（NMAP）プローブ

Cisco ISE では、NMAP セキュリティ スキャナを使用して、サブネット内のデバイスを検出できます。プロファイリング サービスの実行が有効になっているポリシー サービス ノードで NMAP プローブをイネーブルにします。エンドポイント プロファイリング ポリシーでそのプローブからの結果を使用します。

NMAP スキャンは、不明プロファイルに一致して IP アドレスが割り当てられているエンドポイントデバイス、またはプロファイリングポリシーの NMAP 条件に一致するエンドポイントデバイスに対して自動的に実行されます。この自動 NMAP スキャンは、不明なエンドポイントとネットワーク スキャン アクションの一致の両方に対して、3 回のみ実行されます。さらにスキャンが必要な場合は、手動スキャンを実行するか、コンテキストの可視性からエンドポイントデバイスを削除することができます。

NMAP の各手動サブネット スキャンには、エンドポイント ソース情報をそのスキャン ID で更新するために使用される一意の数値 ID があります。エンドポイント検出時に、エンドポイント ソース情報を更新して、ネットワーク スキャン プローブで検出されたことを示すこともできます。

NMAP の手動サブネット スキャンは、静的な IP アドレスが割り当てられたプリンタなど、常に Cisco ISE ネットワークに接続されているために、他のプローブで検出できないデバイスを検出する場合に便利です。

NMAP スキャンの制限

サブネットのスキャンには非常に多くのリソースを消費します。サブネットのスキャンは時間のかかるプロセスです。これは、サブネットのサイズや密度によって異なります。アクティブなスキャンの数は常に 1 つに制限されるため、同時にスキャンできるサブネットは 1 つだけです。また、サブネット スキャンの進行中にいつでもサブネット スキャンをキャンセルできます。[クリック（Click）] を使用して、最新のスキャン結果のリンクを表示できます。これにより、**[ワーク センター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[手動スキャン（Manual Scans）]** > **[手動 NMAP スキャンの結果（Manual NMAP Scan Results）]** に保存されている最新のネットワーク スキャン結果を表示できます。

手動 NMAP スキャン

次の NMAP コマンドを使用すると、サブネットがスキャンされ、nmapSubnet.log に出力が送信されます。

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

表 *100 :* 手動サブネット スキャンの *NMAP* コマンド

-O	OS 検出の有効化
-sU	UDP スキャン
-p <port ranges>	特定のポートのみスキャンします。たとえば、U:161, 162 と指定します。
oN	通常の出力
oX	XML 出力

NMAP の手動サブネット スキャンの SNMP 読み取り専用コミュニティ ストリング

NMAP の手動サブネット スキャンは、エンドポイントで UDP ポート 161 が開かれ、その結果、より多くの属性が収集されることを検出したときには、SNMP クエリーで拡張されます。NMAP 手動サブネット スキャン中は、ネットワーク スキャン プローブによって、デバイスで SNMP ポート 161 が開いているかどうかが検出されます。ポートが開いている場合は、SNMP バージョン 2c のデフォルトのコミュニティ ストリング（public）を使用して SNMP クエリがトリガーされます。

デバイスで SNMP がサポートされ、デフォルトの読み取り専用コミュニティ ストリングが public に設定されている場合は、デバイスの MAC アドレスを MIB 値「ifPhysAddress」から取得できます。

さらに、[プロファイラ設定（Profiler Configuration）] ウィンドウでは、NMAP の手動ネットワークスキャン用として、カンマで区切られた追加の SNMP 読み取り専用コミュニティ文字列を設定できます。また、SNMP バージョン 1 および 2c の SNMP MIB ウォーク用に新しい読み取り専用コミュニティ文字列を指定できます。SNMP 読み取り専用コミュニティ文字列の設定については、CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定 （1227 ページ）を参照してください。

手動 NMAP スキャンの結果

最新のネットワーク スキャン結果は、[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャンの結果（Manual NMAP Scan Results）] に保存されます。[手動 NMAP スキャンの結果（Manual NMAP Scan Results）] ページには、任意のサブネットに対して手動でのネットワーク スキャンを実行し、その結果として検出された最新のエンドポイントのみが、関連付けられたエンドポイント プロファイル、MAC アドレス、およびスタティック割り当てステータスとともに表示されます。このページでは、必要に応じて、エンドポイント サブネットで検出されたポイントをより適切に分類するために編集できます。

Cisco ISE を使用すると、プロファイリング サービスの実行が有効になっている [ポリシー サービス（Policy Service）] ノードで手動でのネットワーク スキャンを実行できます。展開内のプライマリ管理 ISE ノード ユーザー インターフェイスでポリシー サービス ノードを選択し、そのポリシー サービス ノードで手動でのネットワーク スキャンを実行する必要があります。任意のサブネットに対する手動でのネットワーク スキャン時に、ネットワーク スキャン プローブにより、指定されたサブネット上のエンドポイントとそのオペレーティング システムが検出され、SNMP サービス用の UDP ポート 161 および 162 がチェックされます。

手動での NMAP スキャンの結果に関する追加情報を以下に示します。

- 不明なエンドポイントを検出するには、NMAP が NMAP スキャンまたはサポートする SNMP スキャンを介して IP/MAC バインディングを学習できる必要があります。
- ISE は、RADIUS 認証または DHCP プロファイリングを使用して、既知のエンドポイントの IP/MAC バインディングを学習します。
- IP/MAC バインディングは、展開内の PSN ノード間で複製されません。したがって、ローカル データベースに IP/MAC バインディングがある PSN（たとえば、MAC アドレスが最後に認証された PSN）から手動スキャンを開始する必要があります。
- NMAP スキャンの結果には、手動または自動にかかわらず、NMAP が以前にスキャンしたエンドポイントに関する情報は表示されません。

DNS プローブ

Cisco ISE 展開のドメイン ネーム サーバー（DNS）プローブを使用すると、プロファイラはエンドポイントを検索し、完全修飾名（FQDN）を取得できます。Cisco ISE 対応のネットワークでエンドポイントが検出されたら、エンドポイント属性のリストが NetFlow、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP プローブから収集されます。

Cisco ISE をスタンドアロンで展開する場合、または初めて分散環境に展開する場合は、セットアップ ユーティリティを実行して Cisco ISE アプライアンスを設定するように求められます。セットアップ ユーティリティを実行するときに、ドメイン ネーム システム（DNS）ドメインとプライマリ ネームサーバー（プライマリ DNS サーバー）を設定します。設定時には、1 つ以上のネームサーバーを設定できます。Cisco ISE の展開後に、CLI コマンドを使用して DNS ネームサーバーを変更または追加することもできます。

DNS FQDN ルックアップ

DNS ルックアップを実行する前に、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP のいずれかのプローブを DNS プローブとともに起動する必要があります。これにより、プロファイラの DNS プローブは、Cisco ISE 展開に定義されている、指定されたネームサーバーに対して逆引き DNS ルックアップ（FQDN ルックアップ）を実行できます。新しい属性がエンドポイントの属性リストに追加され、エンドポイント プロファイリング ポリシーの評価に使用できます。FQDN は、システム IP ディクショナリに存在する新しい属性です。エンドポイント プロファイリング条件を作成して、FQDN 属性およびそのプロファイリング用の値を検証できます。次は、DNS ルックアップ、およびこれらの属性を収集するプローブに必要な特定のエンドポイント属性です。

- dhcp-requested-address 属性：DHCP プローブと DHCP SPAN プローブによって収集される属性
- SourceIP 属性：HTTP プローブによって収集される属性
- Framed-IP-Address 属性：RADIUS プローブによって収集される属性
- cdpCacheAddress 属性：SNMP プローブによって収集される属性

WLC Web インターフェイスでの呼出端末 ID タイプの設定

WLC Web インターフェイスを使用して、呼出端末 ID タイプ情報を設定できます。WLC Web インターフェイスの [セキュリティ（Security）] タブに移動すると、[RADIUS RADIUS 認証サーバー（Authentication Servers）] ページで発信側ステーション ID を設定できます。[MAC デリミタ（MAC Delimiter）] フィールドは、WLC ユーザーインターフェイスのデフォルトでは、[コロン（Colon）] に設定されます。

WLC Web インターフェイスで設定する方法の詳細については、『Cisco Wireless LAN Controller Configuration Guide, Release 7.2』の第 6 章「Configuring Security Solutions」を参照してください。

config radius callStationIdType コマンドを使用して WLC CLI で設定する方法の詳細については、『Cisco Wireless LAN Controller Command Reference Guide, Release 7.2』の第 2 章「Controller Commands」を参照してください。

ステップ 1 ワイヤレス LAN コントローラのユーザー インターフェイスにログインします。

ステップ 2 [セキュリティ（Security）] をクリックします。

ステップ 3 [AAA] を展開して、**[RADIUS]** > **[認証（Authentication）]** を選択します。

ステップ 4 [呼出端末 ID タイプ（Call Station ID Type）] ドロップダウン リストから [システム MAC アドレス（System MAC Address）] を選択します。

ステップ 5 FIPS モードで Cisco ISE を実行する場合は、[AES キー ラップ（AES Key Wrap）] チェックボックスをオンにします。

ステップ 6 [MAC 区切り文字（MAC Delimiter）] ドロップダウン リストから [コロン（Colon）] を選択します。

SNMP クエリ プローブ

[ノードの編集（Edit Node）] ページでの SNMP クエリー プローブの設定に加えて、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス（Network Devices）]** でその他の Simple Management Protocol 設定を行う必要があります。

[ネットワーク デバイス（Network Devices）] リスト ページで新しいネットワーク アクセス デバイス（NAD）の SNMP 設定を行うことができます。ネットワーク アクセス デバイスの SNMP クエリー プローブまたは SNMP 設定に指定したポーリング間隔で、NAD に定期的にクエリーを実行します。

次の設定に基づいて、特定の NAD の SNMP クエリーをオンおよびオフにすることができます。

- [リンクアップ時に SNMP クエリー（SNMP Query on Link up）] および [新しい MAC の通知（New MAC notification）] のオンまたはオフ
- Cisco Discovery Protocol 情報の [リンクアップ時に SNMP クエリー（SNMP Query on Link up）] および [新しい MAC の通知（New MAC notification）] のオンまたはオフ
- SNMP クエリー タイマーをデフォルトでスイッチごとに 1 時間に 1 回

iDevice および SNMP をサポートしないその他のモバイル デバイスでは、ARP テーブルによって MAC アドレスを検出でき、SNMP クエリー プローブによってネットワーク アクセス デバイスからクエリーを実行できます。

SNMP クエリに関する Cisco Discovery Protocol のサポート

ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスのすべてのポートで Cisco Discovery Protocol を有効（デフォルト）にする必要があります。ネットワーク デバイスのいずれかのポートで Cisco Discovery Protocol を無効にすると、接続されているすべてのエンドポイントの Cisco Discovery Protocol 情報が失われるため、正しくプロファイリングを実行

できなくなる可能性があります。ネットワーク デバイスで cdp run コマンドを使用して Cisco Discovery Protocol をグローバルに有効にし、ネットワーク アクセス デバイスのインターフェイスで cdp enable コマンドを使用して Cisco Discovery Protocol を有効にします。ネットワーク デバイスとインターフェイスで Cisco Discovery Protocol を無効にするには、コマンドの先頭に no キーワードを使用します。

SNMP クエリに関する Link Layer Discovery Protocol のサポート

Cisco ISE プロファイラは LLDP の属性を収集するために SNMP クエリを使用します。RADIUS プローブを使用して、ネットワーク デバイスに組み込まれている Cisco IOS センサーから LLDP 属性を収集することもできます。次に、ネットワーク アクセス デバイスでの LLDP グローバル コンフィギュレーション コマンドと LLDP インターフェイス コンフィギュレーション コマンドの設定に使用できるデフォルトの LLDP 構成設定を示します。

表 *101* : デフォルトの *LLDP* 設定

属性	設定
LLDP グローバル ステート	無効
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	有効（すべての TLV の送受信が可能）
LLDP インターフェイス ステート	有効
LLDP 受信	有効
LLDP 転送	有効
LLDP med-tlv-select	有効（すべての LLDP-MED TLV の送信が可能）

単一文字で表示される CDP および LLDP の機能コード

エンドポイントの属性リストには、lldpCacheCapabilities 属性と lldpCapabilitiesMapSupported 属性の 1 文字の値が表示されます。値は、CDP と LLDP を実行するネットワーク アクセス デバイスに対して表示される機能コードです。

例 1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

例 2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

例 3

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

SNMP トラップ プローブ

SNMP トラップは、MAC 通知、linkup、linkdown、および informs をサポートする特定のネットワーク アクセス デバイスから情報を受信します。SNMP トラップ プローブは、ポートが起動するかダウンし、エンドポイントがネットワークから切断されるかネットワークに接続すると、特定のネットワーク アクセス デバイスから情報を受信します。

SNMP トラップを完全に機能させ、エンドポイントを作成するには、トラップを受信したときに SNMP クエリー プローブがネットワーク アクセス デバイスの特定のポートでポーリング イベントをトリガーするように SNMP クエリーを有効にする必要があります。この機能を完全に動作させるには、ネットワーク アクセス デバイスと SNMP トラップを設定する必要があります。

（注） Cisco ISE では、ワイヤレス LAN コントローラ（WLC）とアクセス ポイント（AP）から受信した SNMP トラップはサポートされません。

Active Directory プローブ

Active Directory（AD）のプローブは以下を実現します。

- Windows エンドポイントの OS 情報の明瞭度を向上させます。Microsoft AD はバージョンとサービス パックのレベルを含む、AD に参加しているコンピュータの OS の詳細情報を追跡します。AD のプローブは、AD のランタイム コネクタを使用してこの情報を直接取得し、クライアント OS 情報の信頼性の高いソースを提供します。
- 社内および社外の資産を区別するのに役立ちます。AD のプローブで使用される基本的ですが重要な属性は、エンドポイントが AD にあるかどうかです。この情報は AD に含まれるエンドポイントを管理対象デバイスまたは企業資産として分類するために使用できます。

[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [プロファイリング設定（Profiling Configuration）] で AD プローブを有効化できます。このプローブを有効にすると、Cisco ISE はホスト名を受信するとすぐに、新しいエンドポイントの AD 属性を取得します。ホスト名は通常 DHCP または DNS プローブから正常に学習されます。正常に取得すると、ISE は再スキャンがタイムアウトになるまで、同じエンドポイントに対し AD を再度問い合わせようとはしません。これにより属性の問い合わせに対する AD の負荷が制限されます。再スキャン タイマーは、[再スキャンまでの日数（Days Before Rescan）] フィールド（[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [プロファイリング設定（Profiling Configuration）] > [Active Directory] ）で設定できます。エンドポイントでの追加のプロファイリング アクティビティがあれば、AD はもう一度クエリーされます。

次の AD プローブの属性は ACTIVEDIRECTORY 条件を使用して、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [プロファイリング（Profiling）]** でマッチングさせることができます。AD のプローブを使用して集められた AD 属性は、[コンテキストの可視性（Context Visibility）]>[エンドポイント（Endpoints）] ウィンドウのエンドポイントの詳細にプレフィックス「AD」が付いて表示されます。

- AD-Host-Exists
- AD-Join-Point
- AD-Operating-System
- AD-OS-Version
- AD-Service-Pack

Cisco ISE ノードごとのプローブの設定

ポリシー サービス ペルソナを担当する展開の Cisco ISE ノードごとに、[プロファイリング設定（Profiling Configuration）] タブで次のプローブを 1 つ以上設定できます。

- [スタンドアロンノード（A standalone node）] : デフォルトですべての管理、モニタリング、およびポリシー サービスのペルソナを担当する単一のノードに Cisco ISE を展開した場合。

- [複数ノード（Multiple nodes）]：展開でポリシーサービスペルソナを担当するノードを複数登録した場合。

（注） デフォルトでは、すべてのプローブが有効になっているわけではありません。一部のプローブは、チェックマークで明示的に有効にされていない場合でも部分的に有効になります。プロファイリングの設定は、現在、各 PSN に固有です。展開内の各 PSN は、同一のプロファイラ構成設定を使用して設定することを推奨します。

始める前に

Cisco ISE ノードごとのプローブは、管理ノードからのみ設定できます。管理ノードは、分散展開のセカンダリ管理ノードで使用できません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 2 ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。

ステップ 3 [展開ノード（Deployment Nodes）] ページで [編集（Edit）] をクリックします。

ステップ 4 [全般設定（General Settings）] タブで [ポリシー サービス（Policy Service）] チェックボックスをオンにします。[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 [プロファイリング サービスの有効化（Enable Profiling Service）] チェックボックスをオンにします。

ステップ 6 [プロファイリング設定（Profiling Configuration）] タブをクリックします。

ステップ 7 各プローブの値を設定します。

ステップ 8 [保存（Save）] をクリックしてプローブ設定を保存します。

CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定

Cisco ISE では、グローバル コンフィギュレーションで、[プロファイラ設定（Profiler Configuration）] ページで許可変更（CoA）を発行し、プロファイリング サービスを有効にしてすでに認証されているエンドポイントに対する制御を拡張することができます。

さらに、[プロファイラ設定（Profiler Configuration）] ページでは、NMAP の手動でのネットワーク スキャンのために、カンマで区切られた追加の SNMP 読み取り専用コミュニティ ストリングを設定できます。SNMP RO コミュニティ ストリングは、[現在のカスタム SNMP コミュニティ ストリング（Current custom SNMP community strings）] フィールドに表示されるのと同じ順序で使用されます。

[プロファイラ設定（Profiler Configuration）] ページでは、エンドポイント属性のフィルタリングを設定することもできます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）]** を選択します。

ステップ 2 次のいずれかの設定を選択して、CoA タイプを設定します。

- [CoA なし（No CoA）]（デフォルト）：このオプションを使用して、CoA のグローバル コンフィギュレーションを無効にできます。この設定は、エンドポイント プロファイリング ポリシーごとに設定された CoA を上書きします。目的が可視性のみの場合は、デフォルト値 の [CoA なし（No CoA）] のままにします。
- [ポート バウンス（Port Bounce）]：スイッチ ポートのセッションが 1 つだけである場合は、このオプションを使用できます。ポートに複数のセッションがある場合は、[再認証（Reauth）] オプションを使用します。プロファイルの変更に基づいてアクセスポリシーをすぐに更新することが目的の場合は、[ポートバウンス（Port Bounce）] オプションを選択します。これにより、クライアントレス エンドポイントが再認可され、必要に応じて、IP アドレスが更新されます。
- [再認証（Reauth）]：このオプションを使用して、すでに認証されているエンドポイントをプロファイリング時に再認証できます。 現在のセッションの再認可に従った VLAN またはアドレスの変更が予期されていない場合は、[再認証（Reauth）] オプションを選択します。

（注） 1 つのポートに複数のアクティブなセッションがある場合は、CoA に [ポートバウンス（Port Bounce）] オプションを設定しても、プロファイリングサービスによって [再認証（Reauth）] オプションが指定された CoA が発行されます。この機能を使用すると、[ポート バウンス（Port Bounce）] オプションの場合のように他のセッションが切断されるのを回避できます。

ステップ 3 NMAP の手動でのネットワークスキャンのために、カンマで区切られた新しい SNMP コミュニティ文字列を [カスタム SNMP コミュニティ文字列の変更（Change Custom SNMP Community Strings）] フィールドに入力し、[カスタム SNMP コミュニティ文字列の確認（Confirm Custom SNMP Community Strings）] フィールドに文字列を再入力します。

デフォルトの SNMP コミュニティ文字列は「public」です。これを確認するには、[現在のカスタム SNMP コミュニティ文字列（Current Custom SNMP Community Strings）] セクションの [表示（Show）] をクリックします。

ステップ 4 [エンドポイント属性フィルタ（Endpoint Attribute Filter）] チェックボックスをオンにして、エンドポイント属性のフィルタリングを有効にします。

[エンドポイント属性フィルタ（Endpoint Attribute Filter）] を有効にすると、Cisco ISE プロファイラは、許可された属性のみを保持し、その他の属性をすべて廃棄します。詳細については、エンドポイント属性をフィルタリングするグローバル設定（1232 ページ）およびISE データベースの持続性とパフォーマンスの属性フィルタ（1232 ページ）の項を参照してください。ベストプラクティスとして、実稼働展開では [エンドポイント属性フィルタ（Endpoint Attribute Filter）] を有効にすることを推奨します。

ステップ 5 [プローブデータパブリッシャの有効化（Enable Probe Data Publisher）] チェックボックスをオンにして、Cisco ISE でエンドポイント プローブ データを、ISE でのエンドポイント オンボーディングの分類にこのデータが必要な pxGrid サブスクライバにパブリッシュします。PxGrid サブスクライバは、初期導入フェーズ中に一括ダウンロードを使用して、Cisco ISE からエンドポイントレコードをプルできます。Cisco ISE は、PAN で更新されるたびに、エンドポイントレコードを pxGrid サブスクライバに送信します。このオプションはデフォルトでは無効になっています。

このオプションを有効にする場合は、導入環境で pxGrid ペルソナが有効になっていることを確認します。

ステップ 6 [保存（Save）] をクリックします。

認証されたエンドポイントに対する許可変更のグローバル設定

デフォルトの [CoA なし（No CoA）] オプションを使用して認可変更（CoA）を無効にするか、またはポートバウンスと再認証オプションを使用して CoA を有効にするグローバル コンフィギュレーション機能を使用できます。Cisco ISE の CoA でポート バウンスを設定している場合は、「CoA 免除」の項で説明されているように、プロファイリング サービスにより他の CoA が発行されることがあります。

選択したグローバルコンフィギュレーションでは、より具体的な設定がない場合のみ、デフォルトの CoA 動作が規定されます。エンドポイント プロファイリング ポリシーごとの認可変更の設定 （1275 ページ）を参照してください。

RADIUS プローブまたはモニタリング ペルソナの REST API を使用して、エンドポイントの認証できます。RADIUS プローブを有効にして、パフォーマンスを向上させることができます。CoA を有効にした場合は、Cisco ISE アプリケーションで CoA 設定と合わせて RADIUS プローブを有効にしてパフォーマンスを向上させることを推奨します。これにより、プロファイリング サービスは収集された RADIUS 属性を使用して、エンドポイントに適切な CoA を発行できます。

Cisco ISE アプリケーションで RADIUS プローブを無効にした場合は、モニタリング ペルソナの REST API を使用して CoA を発行できます。これにより、プロファイリング サービスは幅広いエンドポイントをサポートできます。分散展開では、モニタリング ペルソナの REST API を使用して CoA を発行するために、モニタリング ペルソナを担当する Cisco ISE ノードがネットワークに少なくとも 1 つ存在している必要があります。

プライマリおよびセカンダリ モニタリング ノードは同一のセッション ディレクトリ情報を持つため、Cisco ISE は、分散展開内の REST クエリーのデフォルトの宛先としてプライマリおよびセカンダリ モニタリング ノードを適宜指定します。

許可変更の発行の使用例

次の場合に、プロファイリング サービスによって許可変更が発行されます。

- エンドポイントが削除される：エンドポイントが [エンドポイント（Endpoints）] ページから削除され、そのエンドポイントがネットワークから接続解除または排除された場合。

- 例外アクションが設定される：エンドポイントに異常または許容できないイベントをもたらす例外アクションがプロファイルごとに設定されている場合。プロファイリング サービスは、CoA を発行して対応するスタティック プロファイルにエンドポイントを移動します。
- エンドポイントが初めてプロファイリングされる：エンドポイントがスタティックに割り当てられておらず、初めてプロファイリングされる場合（たとえば、プロファイルが不明プロファイルから既知のプロファイルに変更された場合）。
  - エンドポイント ID グループが変更される：エンドポイントが認証ポリシーで使用されるエンドポイント ID グループに対して追加または削除された場合。

    エンドポイント ID グループが変更され、エンドポイント ID グループが次のために許可ポリシーで使用されている場合、プロファイリング サービスは CoA を発行します。
    - 動的にプロファイリングされる場合のエンドポイントに対するエンドポイント ID グループの変更
    - ダイナミック エンドポイントに対してスタティック割り当てフラグが true に設定されている場合のエンドポイント ID グループの変更
- エンドポイント プロファイリングのポリシーが変更され、ポリシーが認証ポリシーで使用される：エンドポイント プロファイリング ポリシーが変更され、認証ポリシーで使用される論理的なプロファイルにそのポリシーが含まれる場合。エンドポイント プロファイリング ポリシーは、プロファイリング ポリシーの一致のため、または、エンドポイントが論理的なプロファイルに関連付けられたエンドポイント プロファイリング ポリシーにスタティックに割り当てられるときに、変更される場合があります。両方の場合で、エンドポイント プロファイリング ポリシーが許可ポリシーで使用される場合のみ、プロファイリング サービスは CoA を発行します。

許可変更の発行の免除

エンドポイント ID グループが変更され、スタティック割り当てがすでに true の場合、プロファイリング サービスは CoA を発行しません。

Cisco ISE は次の理由で CoA を発行しません。

- エンドポイントがネットワークから切断されている：ネットワークから切断されているエンドポイントが検出された場合。
- 有線（Extensible Authentication Protocol）EAP 対応エンドポイントが認証された：認証された有線 EAP 対応エンドポイントが検出された場合。
- ポートごとに複数のアクティブ セッション：1 つのポートに複数のアクティブなセッションがある場合は、CoA に [ポート バウンス（Port Bounce）] オプションを設定しても、プロファイリング サービスによって [再認証（Reauth）] オプションが指定された CoA が発行されます。

- ワイヤレス エンドポイント検出時のパケット オブ ディスコネクト CoA（セッションの終了）：エンドポイントがワイヤレスとして検出されて、パケットオブディスコネクトCoA（セッション終了）がポート バウンス CoA の代わりに送信された場合。この変更の利点は、ワイヤレス LAN コントローラ（WLC）CoA がサポートされていることです。
- プロファイラ CoA は、許可プロファイルで設定された論理プロファイルに対して、[論理プロファイルでエンドポイントのプロファイラCoAを抑制する（Suppress Profiler CoA for endpoints in Logical Profile）] オプションを使用すると抑制されます。デフォルトでは、プロファイラ CoA は他のすべてのエンドポイントに対してトリガーされます。
- グローバルな [CoA なし（No CoA）] 設定がポリシー CoA を上書きする：グローバルな [CoA なし（No CoA）] は、エンドポイント プロファイリング ポリシーのすべての構成設定を上書きします。エンドポイント プロファイリングポリシーごとに設定された CoA に関係なく、Cisco ISE で CoA が発行されないためです。

（注） [CoA なし（No CoA）] および [再認証（Reauth）] CoA 設定は影響を受けません。また、プロファイラ サービスは有線およびワイヤレス エンドポイントに同じ CoA の設定を適用します。

CoA 設定の各タイプに発行される許可変更

表 *102 : CoA* 設定の各タイプに発行される許可変更

シナリオ	CoA なし設定	ポート バウンス設定	再認証設定	その他の情報
Cisco ISE における CoA グローバル コンフィギュレーション（一般的な設定）	CoA なし（No CoA）	ポートバウンス（Port Bounce）	再認証	—
エンドポイントがネットワークで検出された場合	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	許可変更は、RADIUS 属性の Acct -Status -Type 値 Stop で判別されます。
同じスイッチ ポートで複数のアクティブ セッションと有線接続	CoA なし（No CoA）	再認証	再認証	再認証は、他のセッションの切断を回避します。

シナリオ	CoA なし設定	ポート バウンス設定	再認証設定	その他の情報
ワイヤレス エンドポイント	CoA なし（No CoA）	切断パケット CoA（セッション終了）	再認証	ワイヤレス LAN コントローラに対するサポート。
不完全な CoA データ	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	原因は RADIUS 属性の欠落。

ISE データベースの持続性とパフォーマンスの属性フィルタ

Cisco ISE は、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP ヘルパーと DHCP SPAN の両方）、HTTP、RADIUS、およびシンプル ネットワーク管理プロトコルの各プローブのフィルタを実装しています。ただし、パフォーマンスの低下に対処するために NetFlow は除外されています。各プローブ フィルタには、一時的でエンドポイント プロファイルとは関係のない属性のリストが含まれ、これらの属性はプローブによって収集された属性から削除されます。

isebootstrap ログ（isebootstrap-yyyymmdd-xxxxxx.log）には、辞書からの属性がフィルタリングされた状態で、辞書の作成を処理するメッセージが含まれます。エンドポイントがフィルタリング フェーズを通過するときに、フィルタリングが行われたことを示すデバッグ メッセージをログに記録するように設定することもできます。

Cisco ISE プロファイラは、次のエンドポイント属性フィルタを呼び出します。

- DHCP ヘルパーと DHCP SPAN の両方の DHCP フィルタには、不要なすべての属性が含まれ、これらの属性は DHCP パケットの解析後に削除されます。フィルタリング後の属性は、エンドポイントのエンドポイント キャッシュ内にある既存の属性とマージされます。
- HTTP フィルタは、HTTP パケットからの属性のフィルタリングに使用され、フィルタリング後の属性セットに大幅な変更はありません。
- RADIUS フィルタは、syslog 解析が完了すると使用され、エンドポイント属性がプロファイリングのためにエンドポイント キャッシュにマージされます。
- SNMP クエリー用の SNMP フィルタには、CDP および LLDP フィルタが含まれています。これらのフィルタはすべて SNMP クエリー プローブに使用されます。

エンドポイント属性をフィルタリングするグローバル設定

収集ポイントで頻繁には変わらないエンドポイント属性の数を減らして、永続性イベントおよび複製イベントの数を減らすことができます。[エンドポイント属性フィルタ（EndPoint Attribute

Filter）]を有効にすると、Cisco ISE プロファイラは許可された属性のみを保持し、その他の属性をすべて廃棄します。

[エンドポイント属性フィルタ（EndPoint Attribute Filter）]を有効にするには、CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定（1227ページ）の項を参照してください。

許可されたリストは、カスタム エンドポイント プロファイリング ポリシー内でエンドポイントのプロファイリングに使用される属性のセットであり、認可変更（CoA）、Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）、デバイス登録 WebAuth（DRW）などが Cisco ISE で期待どおりに機能するために不可欠です。許可されたリストは、無効になっている場合でも、エンドポイントの所有権が変わった場合に（属性が複数のポリシーのサービスノードによって収集されている場合）、常に基準として使用されます。

デフォルトでは許可されたリストは無効で、属性は、属性フィルタが有効になっている場合にのみドロップされます。許可されたリストは、フィードからの変更など、エンドポイントプロファイリングポリシーが変更されると、プロファイリングポリシーに新しい属性を含めるように、動的に更新されます。許可されたリストにない属性は収集時に即座にドロップされ、属性はプロファイリングエンドポイントには使用されません。バッファリングと組み合わせると、永続性イベントの数を減らすことができます。

許可されたリストに次の2つのソースから決定された属性のセットが含まれていることを確認する必要があります。

- エンドポイントをプロファイルに適合させるためにデフォルトプロファイルで使用される属性のセット。
- 許可変更（CoA）、個人所有デバイスの持ち込み（BYOD）、デバイス登録 WebAuth（DRW）などが Cisco ISE で期待どおりに機能するために不可欠な属性のセット。

（注） 許可されたリストに新しい属性を追加するには、管理者がその属性を使用する新しいプロファイラ条件とポリシーを作成する必要があります。この新しい属性は、保存された属性と複製された属性の許可されたリストに自動的に追加されます。

表 *103* : 許可属性

AAA-Server	BYODRegistration
Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	Description
DestinationIPAddress	Device Identifier
Device Name	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID

EndPointProfilerServer	EndPointSource
[FQDN]	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	Product
RegistrationTimeStamp	—
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

Cisco IOS センサー組み込みスイッチからの属性の収集

Cisco IOS センサーの統合により、スイッチから送信された任意またはすべての属性を Cisco ISE ランタイムと Cisco ISE プロファイラで収集できます。RADIUS プロトコルを使用して、DHCP、CDP、および LLDP 属性をスイッチから直接収集できます。DHCP、CDP、および LLDP について収集された属性は、解析され、（**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]**）にあるプロファイラディクショナリの属性にマッピングされます。

デバイス センサー用にサポートされている Catalyst プラットフォームについては、https://communities.cisco.com/docs/DOC-72932 を参照してください。

Cisco IOS センサー組み込みネットワーク アクセス デバイス

Cisco IOS センサー組み込みネットワーク アクセス デバイスと Cisco ISE の統合では、次のコンポーネントが含まれます。

- Cisco IOS センサー
- DHCP、CDP および LLDP のデータを収集するためにネットワーク アクセス デバイス（スイッチ）に組み込まれているデータ コレクタ
- データを処理し、エンドポイントのデバイス タイプを決定するアナライザ

  アナライザを展開するには次の 2 つの方法がありますが、2 つを組み合わせて使用することは想定されていません。

  - アナライザを Cisco ISE に展開する
  - アナライザをセンサーとしてスイッチに組み込む

Cisco IOS センサー組み込みネットワーク アクセス デバイスの設定チェックリスト

ここでは、スイッチから直接 DHCP、CDP、および LLDP の属性を収集するために、Cisco IOS センサー対応スイッチと Cisco ISE で設定する必要がある作業のリストの概要について説明します。

- RADIUS プローブが Cisco ISE で有効になっていることを確認します。
- ネットワーク アクセス デバイスで DHCP、CDP、および LLDP 情報を収集するための IOS センサーがサポートされていることを確認します。
- ネットワーク アクセス デバイスで、エンドポイントから CDP 情報と LLDP 情報を取得するために次の CDP コマンドと LLDP コマンドが実行されていることを確認します。

```
cdp enable
lldp run
```

- 標準の AAA コマンドと RADIUS コマンドを使用して、セッション アカウンティングが個別に有効になっていることを確認します。

  コマンドの使用例を示します。

```
aaa new-model
aaa accounting dot1x default start-stop group radius

radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
radius-server vsa send accounting
```

- IOS センサー固有のコマンドを実行していることを確認します。
  - アカウンティング拡張の有効化

    ネットワーク アクセス デバイスで Cisco IOS センサープロトコルデータを RADIUS アカウンティングメッセージに追加したり、新しいセンサープロトコルデータの検出時に追加のアカウンティングイベントを生成したりできるようにする必要があります。つまり、RADIUS アカウンティング メッセージには、すべての CDP、LLDP、および DHCP 属性が含まれている必要があります。

    次のグローバル コマンドを入力します。

    device-sensor accounting

  - アカウンティング拡張の無効化

    （アカウンティング機能がグローバルに有効になっている場合）（アカウンティング）ネットワーク アクセス デバイスで、特定のポートでホストされているセッションについて Cisco IOS センサープロトコルデータを RADIUS アカウンティングメッセージに追加できないようにするには、適切なポートで次のコマンドを入力します。

    no device-sensor accounting

  - TLV 変更のトラッキング

    デフォルトでは、サポートされている各ピアプロトコルでクライアント通知とアカウンティングイベントが生成されるのは、特定のセッションのコンテキストで前に受信したことのないタイプ、長さ、値（TLV）が着信パケットに含まれている場合だけです。

    新しい TLV が存在するか、または前に受信した TLV の値が異なる場合は、すべての TLV 変更に対するクライアント通知とアカウンティング イベントを有効にする必要があります。次のコマンドを入力します。

    device-sensor notify all-changes

- ネットワーク アクセス デバイスで Cisco IOS Device Classifier（ローカルアナライザ）が無効になっていることを確認します。

  次のコマンドを入力します。

```
no macro auto monitor
```

（注） このコマンドにより、ネットワーク アクセス デバイスは変更ごとに2つの同じRADIUSアカウンティング メッセージを送信できなくなります。

ISE プロファイラによる Cisco IND コントローラのサポート

Cisco ISE は、Cisco Industrial Network Director（IND）に接続されたデバイスの状態をプロファイル化して表示できます。PxGrid は、Cisco ISE と Cisco Industrial Network Director を接続してエンドポイント（IoT）データの通信を行います。Cisco ISE の pxGrid は Cisco IND イベントを消費し、Cisco IND に照会してエンドポイント タイプを更新します。

Cisco ISE プロファイラには、IoT デバイス用のディクショナリ属性があります。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** を選択し、システムディクショナリのリストから *IOTASSET* を選択してディクショナリ属性を確認します。

ガイドラインと推奨事項

プロファイル用に複数の ISE ノードが設定されている場合、1 つのノードのみで IND の Cisco pxGrid を有効にすることを推奨します。

複数の Cisco IND デバイスを単一の ISE に接続できます。

複数のパブリッシャ（Cisco IND）から同じエンドポイントを受信した場合、Cisco ISE は最後のパブリッシャのデータのみをそのエンドポイント用に保持します。

Cisco ISE は pxGrid のサービス名 *com.cisco.endpoint.asset* と */topic/com.cisco.endpoint.asset* から Cisco IND データを受け取ります。

Cisco IND プロファイリング プロセス フロー

Cisco IND アセットディスカバリでは IoT デバイスを検出し、そのデバイスのエンドポイントデータを pxGrid にパブリッシュします。Cisco ISE は、pxGrid 上のイベントを認識し、エンドポイントデータを取得します。Cisco ISE のプロファイラポリシーは、ISE プロファイラ ディクショナリ内の属性にデバイスデータを割り当て、これらの属性を Cisco ISE のエンドポイントに適用します。

Cisco ISE の既存の属性を満たさない IoT エンドポイントデータは保存されません。ただし、Cisco ISE でさらに属性を作成して Cisco IND に登録することができます。

Cisco ISE は、pxGrid を介した Cisco IND への接続が最初に確立されるときにエンドポイントの一括ダウンロードを行います。ネットワークに障害があると、Cisco ISE は蓄積されたエンドポイント変更を再び一括ダウンロードします。

IND プロファイル用の Cisco ISE と Cisco IND の設定

（注） Cisco INDで pxGrid をアクティブ化する前に、Cisco IND に Cisco ISE 証明書をインストールし、ISE に Cisco IND 証明書をインストールする必要があります。

1. **[管理（Administration）]** > **[展開（Deployment）]** を選択します。pxGrid コンシューマとして使用する予定の PSN を編集し、pxGrid を有効にします。この PSN は、Cisco IND およびプロファイリングによってパブリッシュされた pxGrid データからエンドポイントを作成します。
2. **[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** を選択して pxGrid が実行していることを確認します。次に [証明書（Certificates）] タブをクリックし、証明書フィールドに入力します。[作成（Create）] をクリックして証明書を発行し、その証明書をダウンロードします。
   - [処理の選択（I want to）] では [単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）] を選択し、接続する Cisco IND の名前を入力します。
   - [証明書のダウンロード形式（Certificate Download Format）] では、**`PKS12 format`**を選択します。
   - [証明書のパスワード（Certificate Password）] では、パスワードを作成します。

（注） ISE 内部 CA を有効にする必要があります。ご使用のブラウザでポップアップをブロックしている場合は、証明書をダウンロードできません。証明書を解凍して、この次の手順で PEM ファイルを使用できるようにします。

3. Cisco INDで、**[設定（Settings）]** > **[pxGrid]** を選択し、[.pem IND 証明書のダウンロード（Download .pem IND certificate）] をクリックします。このウィンドウを開いたままにします。
4. Cisco ISE で、**[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** > **[すべてのクライアント（All Clients）]** を選択します。Cisco IND pxGrid クライアントが表示されたら、それを承認します。
5. Cisco IND でスライダを移動して pxGrid を有効にします。別の画面が開き、そこで ISE ノードの場所、ISE で pxGrid サーバー用に入力した証明書の名前、指定したパスワードを定義します。[証明書のアップロード（Upload Certificate）] をクリックして、ISE pxGrid PEM ファイルを検索します。

6. ISE で、**[管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。[インポート（Import）] をクリックし、Cisco IND から取得した証明書へのパスを入力します。
7. Cisco INDで、[アクティブ化（Activate）] をクリックします。
8. Cisco ISEで、[管理（Adminstration）] > [展開（Deployment）]を選択します。Cisco IND 接続に使用する PSN を選択し、[プロファイリング（Profiling）] ウィンドウを選択して pxGrid プローブを有効にします。
9. ISE と Cisco IND の間の pxGrid 接続がアクティブになりました。それを確認するには、Cisco IND が検出した IoT エンドポイントを表示します。

IND プロファイリング用の属性の追加

Cisco IND は、ISE ディクショナリに含まれていない属性を返す場合があります。Cisco ISE に属性をさらに追加することによって、その IoT デバイスをより正確にプロファイルすることができます。新しい属性を追加するには、Cisco ISE でカスタム属性を作成し、pxGrid を介してその属性を Cisco IND に送信します。

1. **[管理（Administration）] > [ID 管理（Identity Management）] > [設定（Settings）] > [エンドポイントカスタム属性（Endpoint Custom Attributes）]** を選択します。属性のエンドポイント属性を作成します。
2. これで、プロファイラポリシーでこの属性を使用して、新しい属性でアセットを識別できるようになります。**[ポリシー（Policy）] > [プロファイリング（Profiling）]** を選択し、新しいプロファイラポリシーを作成します。[ルール（Rule）] セクションで、新しいルールを作成します。**属性/値**を追加した場合は、**CUSTOMATTRIBUTE** フォルダを選択し、作成したカスタム属性を選択します。

MUD の Cisco ISE サポート

製造元使用率記述子（MUD）は IETF 標準で、オンボード IoT デバイスに対する方法を定義します。IoT デバイスのシームレスな可視化とセグメンテーションの自動化を提供します。MUD は IETF プロセスで承認されており、RFC8520 としてリリースされています。詳細については、https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/ を参照してください。

Cisco ISE リリース 2.6 以降では、IoT デバイスの識別がサポートされています。Cisco ISE は、プロファイリングポリシーとエンドポイント ID グループを自動的に作成します。MUD は、IoT デバイスのプロファイリング、プロファイリングポリシーの動的作成、ポリシーとエンドポイント ID グループの作成プロセス全体の自動化をサポートします。管理者はこれらのプロファイリングポリシーを使用して、許可ポリシーおよびプロファイルを手動で作成できます。DHCP と LLDP のパケットで MUD URL を送信する IoT デバイスは、これらのプロファイルとポリシーを使用して登録されています。

Cisco ISE は IoT デバイスを符号なしで分類します。Cisco ISE は MUD 属性を保存しません。属性は現在のセッションのみで使用されます。[コンテキストと可視性（Context and Visibility）]

>[エンドポイント（Endpoints）] ウィンドウの [エンドポイントプロファイル（Endpoint Profile）] フィールドで、IoT デバイスをフィルタリングできます。

次のデバイスは、Cisco ISE への MUD データの送信をサポートしています。

- Cisco IOS XE バージョン 16.9.1 と 16.9.2 を実行している Cisco Catalyst 3850 シリーズ スイッチ
- Cisco IOS バージョン 15.2(6)E2 を実行している Cisco Catalyst デジタル ビルディング シリーズ スイッチ
- Cisco IOS バージョン 15.2(6)E2 を実行している Cisco Industrial Ethernet 4000 シリーズ スイッチ
- MUD 機能が組み込まれた Internet of Things（IoT）デバイス

Cisco ISE は、次のプロファイリングプロトコルおよびプロファイリングプローブをサポートします。

- LLDP と Radius - TLV 127
- DHCP - オプション 161

両方のフィールドが IOS デバイスセンサーで Cisco ISE に送信できます。

MUD での ISE の設定

1. **[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [プロファイラの設定（Profiler Settings）]** を選択し、[MUD のプロファイリングの有効化（Enable profiling for MUD）] チェックボックスをオンにします。
2. MUD URI を送信可能なネットワーク アクセス デバイスを ISE に追加します。ネットワークデバイスを追加するには、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** を選択します。
3. MUD-URL 接続が機能していることを確認します。
    1. **[コンテキストの可視性（Visibility）] > [エンドポイント（Endpoints）]** を選択し、ISE が正常に分類されている IoT エンドポイントを見つけます。IoT デバイスはエンドポイントプロファイル名でフィルタリングできます。**`IOT-MUD`** から始まります。
    2. いずれかの IoT デバイスのエンドポイント MAC アドレスをクリックし、属性タグを選択します。属性のリストに mud-url があることを確認します。
    3. **[ポリシー（Policy）] > [プロファイリング（Profiling）]** を選択し、[システムタイプ（System Type）] に [作成した IOT（IOT Created）] を選択してリストをフィルタ処理します。
4. 必要に応じて、新しい IoT デバイスのデバッグ ロギングを設定します。
    1. **[システム（System）] > [ロギング（Logging）] > [デバッグログの設定（Debug Log Configuration）]** を選択し、MUD が設定された ISE ノードを選択します。

2. 左側のメニューで [デバッグログの設定（Debug Log Configuration）] を選択し、プロファイラを選択します。

分類する IoT デバイスが増えると、同じ MUD-URL を持つ同じカテゴリまたはグループ内のすべてのデバイスが同じエンドポイントグループに割り当てられます。たとえば、Molex ライトを接続し、分類すると、この Molex ライトにプロファイラグループが作成されます。同じタイプの（同じ MUD-URL を持つ）Molex ライトが増え、分類されると、同じ分類またはエンドポイント ID グループを継承します。

ISE とスイッチで MUD トラフィックフローを確認

1. IoT デバイスをオンにする前に、ポートを接続するか、インターフェイスのシャットダウンを解除します。
    1. ISE でパケットキャプチャを開始します。
    2. スイッチポートでパケットキャプチャを開始します。
2. スイッチに関する次のコマンドの出力を確認します。
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**
3. IoT デバイスをオンにします。
4. 1 分ごとに次のコマンドを繰り返し実行します。
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**
5. ISE のすべてのデバイスが表示されるまで 3 ～ 5 分間待機します。
6. ISE とスイッチパケットの両方のキャプチャを停止します。
7. 1 分ごとに次のコマンドを繰り返し実行します。
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**

多要素分類による拡張エンドポイントの可視化

ネットワークに接続しているエンドポイントからの4つの特定の属性を使用して、微妙な認証ポリシーを作成できます。多要素分類（MFC）プロファイラは、さまざまなプロファイリングプローブを使用して、Cisco ISE 認証ポリシー作成ワークフローに次の 4 つの新しいエンドポイント属性を取得します。

- MFC エンドポイントタイプ（ワークステーション、プリンタ、ネットワークデバイスなど）
- MFC ハードウェア製造元（Xerox Corporation、Google, Inc.、TP-LINK TECHNOLOGIES CO.,LTD など）
- MFC ハードウェアモード（Xerox-Printer-Phaser3250、TP-LINK-Device など）
- MFC オペレーティングシステム（Windows、Lexmark-OS など）

多要素分類エンドポイント属性を受信するには、次のプローブを有効にすることをお勧めします。

- Active Directory
- DHCP
- DHCP SPAN
- DNS
- HTTP
- NetFlow
- ネットワーク スキャン（NMAP）
- RADIUS
- SNMP トラップ
- SNMP クエリ

多要素分類では、エンドポイント属性として4つの新しいラベルが追加され、エンドポイントの可視性を強化する効果的な認証ポリシーを作成できます。多要素分類ラベルと収集したデータは、レポートとしてエクスポートできます。

多要素分類属性を表示して使用するには、Cisco ISE 展開に Advantage ライセンスが必要です。

多要素分類プロファイラは、Cisco ISE リリース 3.3 ではデフォルトで有効になっており、ポリシーサービスノード（PSN）およびプライマリポリシー管理ノード（PAN）で実行されます。

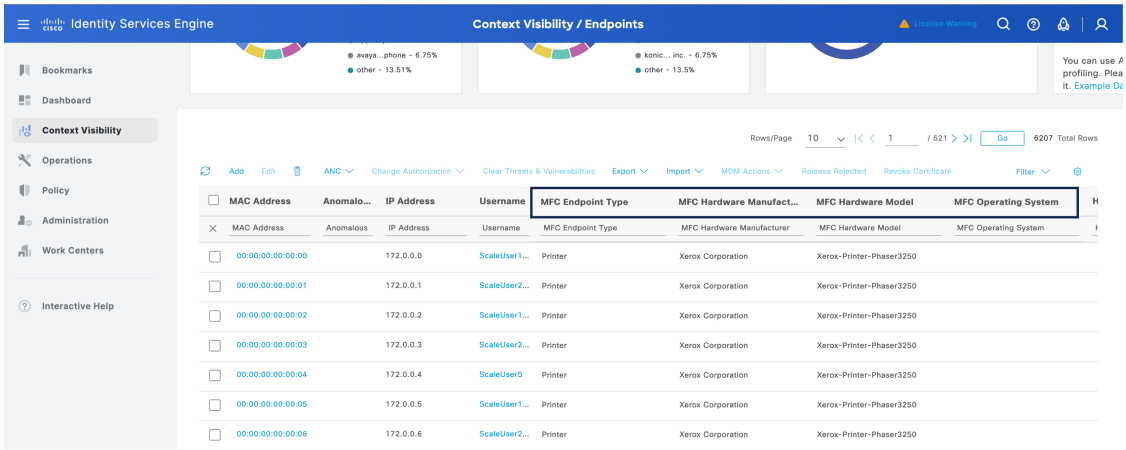
多要素分類を無効にするには、Cisco ISE 管理ポータルで、[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）] > [プロファイラ設定（Profiler Settings）] の順に選択します。[MFCプロファイリング（MFC Profiling）] 領域で、[MFCプロファイリングとAIルール（MFC Profiling and AI Rules）] チェックボックスをオフにします。

MFC プロファイリングを無効にすると、すべての Cisco ISE PSN で多要素分類機能が停止します。無効化の時点までのデータ収集は Cisco ISE に保持されます。**[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[認証（Authentication）]** ウィンドウでは古いデータが引き続き表示される場合があります。

[MFCプロファイリングとAIルール（MFC Profiling and AI Rules）] チェックボックスをオフにすると、エンドポイントプロファイリングに対する Cisco AI-ML ルール提案は機能しません。

多要素分類機能によって取得した属性データは、**[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[認証（Authentication）]** ウィンドウに表示されます。4 つの新しい列には、エンドポイント属性データ（**MFC エンドポイントタイプ**、**MFC ハードウェア製造元**、**MFC ハードウェアモデル**、**MFC オペレーティングシステム**）が表示されます。

図 *26 : [*コンテキストの可視性（*Context Visibility***）*] > [*エンドポイント（***Endpoints***）*] ウィンドウの多要素分類エンドポイント属性**



ルールの優先順位付け

プロファイリングルールには、多要素分類において以下のような変更できない優先順位があり、最初のルールが最も高い優先順位を持ちます。

1. システム規則
    1. シスコが管理するダイレクトマッピング属性値。ディクショナリルックアップの順序は、MDM、Wi-Fi デバイス分析、IOT-Assets、ポスチャ、ACIDEXです。
    2. シスコが管理する MFC ルール：多要素分類ラベルを生成する Cisco ISE の既存のプロファイリングポリシー。
2. AI-ML ルール：これらは多要素分類ラベルを生成する、ユーザーが承認する AI-ML プロファイリングポリシーです。
3. システムライブラリルール：シスコが管理するユーザーエージェントおよびOUIルール。

MFC ラベルが優先順位の高いルールによって提供されている場合、そのラベルが優先順位の低いルールによって上書きされることはありません。システムルールがエンドポイントのハードウェア製造元ラベルを提供するシナリオを考えてみましょう。4 つのラベルすべてを含むエ

ンドポイントに AI-ML ルールが存在する場合、システムルールのハードウェア製造元の値が保持されます。他の 3 つのラベルのみが AI-ML ルールから取得されます。

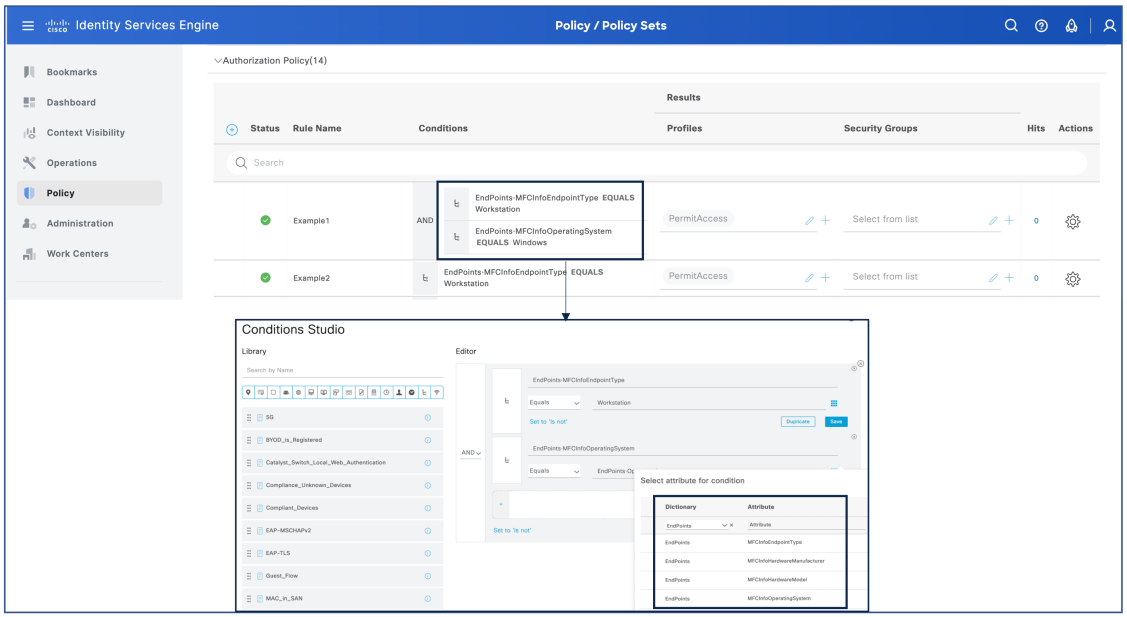
多要素分類属性を使用した認証ポリシーセットの作成

[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] > [デフォルト（Default）] > [認証ポリシー（Authorization Policy）] ウィンドウで、多要素分類属性を使用して認証ポリシーセットを作成できます。

多要素分類属性は、**エンドポイントディクショナリ**に自動的に追加されます。新しいポリシーを作成する、または既存のポリシーを更新するときに、4 つの **MFC** プレフィックス属性から選択して、それらの詳細を活用し、焦点を絞った認証ポリシーを定義できます。

次の画像は、条件スタジオで使用できる 4 つの多要素分類属性と、多要素分類エンドポイント属性を使用する完全なポリシーセットの例を示しています。

図 *27 :* 多要素分類属性を使用する条件付きの認証ポリシー



[認証ポリシー（Authorization Policy）] 領域のポリシーセットの順序は重要です。エンドポイントは、一致する最初のポリシーセットに従ってプロファイリングされます。この微妙なエンドポイント情報を効果的に使用するために、多要素分類属性条件を含むポリシーセットを他のポリシーセットよりも前に配置することをお勧めします。

これらのポリシーセットに一致したエンドポイントを表示するには、**[操作（Operations）] > [RADIUS] > [ライブログ（Live Logs）]** ウィンドウに移動します。新しく定義されたポリシーによってエンドポイントのプロファイリングに変更がある場合、CoA が自動的にトリガーされます。

多要素分類のトラブルシューティング

多要素分類機能のトラブルシューティングのログを表示するには、サポートバンドルをダウンロードします。

1. **[操作（Operations）] > [トラブルシュート（Troubleshoot）] > [ログのダウンロード（Download Logs）]** を選択します。
2. 左側のペインで、サポートバンドルを生成するノードをクリックします。
3. [デバッグログ（Debug Logs）] タブで、[pi-profiler] セクションと [プロファイラ（profiler）] セクションから必要なログを選択します。
4. [サポートバンドル（Support Bundle）] タブで、[デバッグログを含める（Include debug logs）] チェックボックスをオンにします。
5. [サポート バンドルの作成（Create Support Bundle）] をクリックします。

多要素分類機能に関連するログのシビラティ（重大度）レベルは、[操作（Operations）] > [トラブルシュート（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグプロファイルの設定（Debug Profile Configuration）] ウィンドウで設定できます。

1. [プロファイリング（Profiling）] をクリックします。
2. コンポーネントの **MFC プロファイラ**について、[ログレベル（Log Level）] ドロップダウンリストから、目的のシビラティ（重大度）レベルを選択します。
3. [保存（Save）] をクリックします。

AI 分析によって実現されるサービス

Cisco AI Analytics の有効化

Cisco AI Analytics エージェントは、Cisco ISE からエンドポイントのデータに対してクエリを実行し、定期的に機械学習（ML）クラウドに送信します。このエージェントは、pxGrid REST API を使用して Cisco ISE からエンドポイントの情報にアクセスします。

Cisco ISE 3.2 以降の Cisco ISE リリースでは、AI と ML を使用して、AI ベースのエンドポイントグループ化、自動化されたカスタム プロファイリング ルール、クラウドソーシングされたエンドポイントラベルを提供することにより、ネットワーク内の不明なエンドポイントの数を減らすことができます。

始める前に

- Cisco ISE 展開のノードの少なくとも 1 つで pxGrid ペルソナを有効にします。pxGrid サービスに使用されるシステム証明書には、[サブジェクト代替名（SAN）（Subject Alternative Name (SAN)）] フィールドに DNS 名が含まれている必要があります。

- この機能を使用するには、スマートライセンスを有効にする必要があり、Advantage ライセンスが必要です。スマートライセンスの詳細については、スマートライセンスの登録とアクティブ化を参照してください。
- SSM オンプレミスサーバーおよび特定のライセンス予約（SLR）ライセンス方式はサポートされていません。
- HTTPS（TCP ポート 443）を介した api.prd.kairos.ciscolabs.com へのネットワーク接続が必要です。必要に応じて、Cisco ISE でプロキシの設定を行います。
- Cisco AI Analytics は、組み込みの評価ライセンスではサポートされていません。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[ワークセンター（Work Center）]** > **[プロファイラ（Profiler）]** > **[設定（Settings）]** > **[Cisco AI Analytics]**の順に選択します。

ステップ 2 [構成（Configure）] をクリックします。

ステップ 3 [構成方法の選択（Choose Configuration Method）] セクションで、次のいずれかを実行します。

- 新しい構成の場合は、[新しい構成（New Configuration）] をクリックします。
- 以前に保存した構成ファイルから既存の顧客構成を復元するには、[構成ファイルから回復（Recover from a config file）] をクリックします。

（注） 保存された構成ファイルから回復すると、バックアップ JSON 構成ファイルを使用して以前の AI Analytics 設定がインポートされます。AI Analytics バックアップファイルには、プライベート暗号化キー、クラウドの場所、顧客 ID 情報が含まれています。インポート後、AI Analytics は以前の構成設定を復元します。

ステップ 4 チェックボックスをオンにして、一般条件とシスコプライバシーポリシーを読んで同意したことを確認します。

（注） 貴社とその関連会社に義務を負わせる権限がない場合、またはユニバーサルクラウド契約の条件に同意しない場合は、チェックボックスをオンにしないでください。

ステップ 5 [地域の選択（Choose Region）] ドロップダウンリストから必要な地域を選択します。

ステップ 6 [有効（Enable）] をクリックします。

エージェントが有効になると、AI Analytics が正常にオンボーディングされたことを示す [成功（Success）] ダイアログボックスが表示されます。また、構成ファイルをダウンロードするように求められます。この設定を使用して、同じ AI Analytics クラウドインスタンスへの接続を復元し、履歴データにアクセスすることができます。

ステップ 7 [OK] をクリック

ステップ 8 [構成ファイルのダウンロード（Download configuration file）] をクリックして構成ファイルをダウンロードします。

（注） 構成ファイルには機密情報が含まれているため、安全な場所に保存する必要があります。構成ファイルへのアクセスを制御する必要があります。Cisco AI Analytics 構成を有効または無効にすると、監査が生成されます。監査の詳細を表示するには、[メニュー（Menu）]アイコン（☰）をクリックし、**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[監査（Audit）]** > **[変更設定監査（Change Configuration Audit）]** を選択します。

Cisco ISE GUI の [デバッグログの設定（Debug Log Configuration）] ウィンドウで **ai-analytics** ログを表示して、エンドポイントのデータが Cisco ISE からクラウドに転送されたかどうかを確認できます。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックし、**[操作（Operations）]** > **[トラブルシュート（Troubleshoot）]** > **[デバッグウィザード（Degug Wizard）]** > **[デバッグログの設定（Debug Log Configuration）]** を選択します。

AI Analytics に関連する問題をトラブルシューティングするには、[デバッグログの設定（Debug Log Configuration）] ウィンドウで **ai-analytics** コンポーネントの [ログレベル（Log Level）] を [デバッグ（DEBUG）] に設定します。

ログは、[ログのダウンロード（Download Logs）] ウィンドウからダウンロードできますこのウィンドウを表示するには、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[操作（Operations）]** > **[トラブルシュート（Troubleshoot）]** > **[ログのダウンロード（Download Logs）]** を選択します。

エンドポイント プロファイリングに対する Cisco AI-ML ルール提案

Cisco ISE は、ネットワーク全体の継続的な学習に基づいてプロファイリングの提案を行い、エンドポイントプロファイリングと管理を強化するのに役立ちます。このような提案を使用して、ネットワーク内の不明なエンドポイントやプロファイリングされていないエンドポイントの数を減らすことができます。

機械学習を利用したプロファイリングの提案を受け取るには、Cisco AI Analytics を有効にして、Cisco ISE と Cisco AI Analytics システム間で情報を共有できるようにする必要があります。

Cisco AI Analytics には、次の前提条件が適用されます。

- 登録済みの Advantage ライセンスでスマートライセンスを有効にしておく必要があります。
- ライセンス方式の SSM オンプレミスサーバーと特定のライセンス予約（SLR）は使用されていません。
- 少なくとも 1 つの Cisco ISE ノードで pxGrid サービスを有効にしておく必要があります。

AI プロポーザルを受信するには、**[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[設定（Settings）]** > **[プロファイラ設定（Profiler Settings）]** ウィンドウで多要素分類による拡張エンドポイントの可視化を有効にする必要があります。この機能は、Cisco ISE ではデフォルトで有効になっています。

Cisco AI 分析機能と MFC プロファイリング機能の両方が有効になっている場合、少なくとも2つのエンドポイント属性値を持つエンドポイントに対してAIプロポーザルが期待できます。AI プロポーザルエンジンの次のソースを有効にすることをお勧めします。

- Active Directory
- DHCP
- DHCP SPAN
- DNS
- HTTP
- NetFlow
- ネットワーク スキャン（NMAP）
- RADIUS
- SNMP トラップ
- SNMP クエリ

AIプロポーザルエンジンは、IPアドレスやMACアドレスなどの一意のエンドポイント識別子を処理しません。

[コンテキスト可視性（Context Visibility）] > **[エンドポイント（Endpoints）]** > **[エンドポイント分類（Endpoint Classification）]** ウィンドウでAIプロポーザルを表示、確認、および適用できます。

Cisco ISE は、新規または変更されたエンドポイント情報を AI プロポーザルと合わせて 12 時間ごとに共有します。過去7日間に収集されたエンドポイントデータは、24時間ごとに分析され、ML モデリングとルール提案の作成に活かされます。

AI プロポーザルを使用してネットワーク内の不明点を減らす

[コンテキスト可視性（Context Visibility）] > **[エンドポイント（Endpoints）]** > **[エンドポイント分類（Endpoint Classification）]** ウィンドウの **[AIプロポーザル（AI Proposals）]** ダッシュレットで、[確認（Review）] をクリックして、Cisco ISE 用に生成された AI プロポーザルを表示します。

AI プロポーザルは、ネットワーク全体の継続的な学習に基づいて、ネットワーク内の不明なエンドポイントの分類ルールとラベルを提示します。各エンドポイントは、1 つのプロポーザルグループにのみ属します。

各プロポーザルグループには、次のエンドポイントが含まれます。

- システムルールによってプロファイリングされている場合とされていない場合があります
- [多要素分類（Multi-Factor Classification）] フィールドのラベルの提案がある場合とない場合があります。

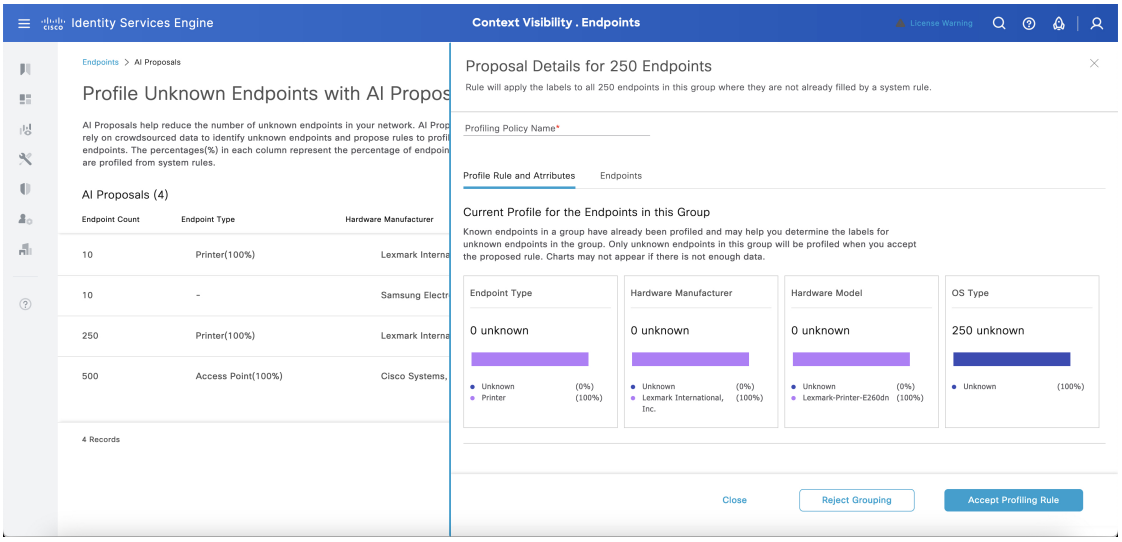
AI によって提案されたルールを適用すると、提案グループの一部である不明なエンドポイントとプロファイリングされていないエンドポイントのみが影響を受けます。既存のシステム

ルールによってすでにプロファイリングされているエンドポイントは、再プロファイリングされず、いかなる影響も受けません。

[AIプロポーザル（AI Proposals）] ウィンドウには、多要素分類（MFC）プロファイラからのエンドポイント属性が表示されます。各列には、推奨されるラベルと、すでにプロファイリングされているグループ内のエンドポイントの割合が表示されます。

確認するエンドポイントグループの [プロポーザルの表示（View Proposals）] をクリックします。

図 *28 :* エンドポイントグループに対する *AI* プロポーザル



スライドインペインにルールの提案が表示されるので、必要に応じてプロファイリングポリシーに名前を付け、ラベル値を更新できます。[プロファイルルールと属性（Profile Rule and Attributes）] タブには、グループ内の不明なエンドポイントの数と、AI プロポーザル通知済みの属性情報が表示されます。このタブには、エンドポイントとして最も最近知られるようになったネットワーク アクセス デバイスも表示されます。

[エンドポイント（Endpoints）] タブには、選択したプロポーザルグループのエンドポイントのリストが表示されます。

必要に応じてラベルを編集し、AI プロポーザルの詳細を確認した後、ペインの最後にある関連ボタンをクリックして、プロポーザルを受け入れるか拒否するかを選択できます。プロポーザルのルール条件は変更できません。プロファイリングルールを受け入れると、選択したエンドポイントグループ内の不明なエンドポイントにプロポーザルが適用されます。

グループ化を拒否すると、プロポーザルは Cisco ISE から削除され、再度表示されなくなります。

プロファイラ条件

プロファイラ条件はポリシー要素であり、他の条件とほとんど同じです。ただし、認証、許可、およびゲスト条件とは異なり、プロファイリング条件は限られた数の属性に基づいています。[プロファイラ条件（Profiler Conditions）] ページに Cisco ISE で使用できる属性とその説明が表示されます。

プロファイラ条件は次のとおりです。

- シスコ提供：Cisco ISE には展開時に事前定義されたプロファイリング条件が含まれており、[プロファイラ条件（Profiler Conditions）] ウィンドウでシスコ提供の条件として識別されます。シスコ提供のプロファイリング条件を削除することはできません。

  [ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[ディクショナリ（Dictionaries）]>[システム（System）]からアクセスできる場所にあるシステムプロファイラディクショナリにもシスコ提供条件があります。

  たとえば、MAC ディクショナリです。一部の製品では、OUI（固有識別子情報）がデバイスの製造組織を識別するために最初に使用できる固有属性です。これはデバイスの MAC アドレスのコンポーネントです。MAC ディクショナリには、MACAddress および OUI 属性が含まれています。

- 管理者作成：ユーザーが Cisco ISE の管理者として作成するプロファイラ条件、複製された事前定義済みのプロファイリング条件は管理者作成として識別されます。[プロファイラ条件（Profiler Conditions）] ウィンドウでプロファイラディクショナリを使用して、DHCP、MAC、SNMP、IP、RADIUS、NetFlow、CDP、LLDP、および NMAP タイプのプロファイラ条件を作成できます。

プロファイリング ポリシーの数の推奨上限は 1000 ですが、最高 2000 までプロファイリング ポリシーを拡張できます。

プロファイリング ネットワーク スキャン アクション

エンドポイント スキャン アクションは、エンドポイント プロファイリング ポリシーで参照できる設定可能なアクションであり、ネットワーク スキャン アクションに関連付けられている条件が満たされるとトリガーされます。

Cisco ISE システムにおけるリソース使用量を制限するために、エンドポイントをスキャンする場合はエンドポイント スキャンが使用されます。ネットワーク スキャン アクションでは、リソースを大量に消費するネットワーク スキャンとは異なり、1 つのエンドポイントをスキャンします。これにより、エンドポイントの全体的な分類が向上し、エンドポイントのエンドポイント プロファイルが再定義されます。エンドポイント スキャンは、1 度に 1 つずつしか処理できません。

1 つのネットワーク スキャン アクションをエンドポイント プロファイリング ポリシーに関連付けることができます。Cisco ISE には、ネットワーク スキャン アクションに 3 つの走査方式

が事前定義されています。たとえば、OS-scan、SNMPPortsAndOS-scan、および CommonPortsAndOS-scan といった 3 つの走査方式のいずれか、またはすべてを含めることができます。OS-scan、SNMPPortsAndOS-scan、および CommonPortsAndOS-scans を編集または削除できません。これらは、Cisco ISE の事前定義済みネットワーク スキャン アクションです。独自の新しいネットワーク スキャン アクションを作成することもできます。

エンドポイントを適切にプロファイリングしたら、設定済みのネットワーク スキャンアクションをエンドポイントに対して使用できません。たとえば、Apple-Device をスキャンすると、スキャンされたエンドポイントを Apple デバイスに分類できます。OS-scan によってエンドポイントで実行されているオペレーティング システムが特定されたら、Apple-Device プロファイルに一致しなくなりますが、Apple デバイスの適切なプロファイルに一致します。

新しいネットワーク スキャン アクションの作成

エンドポイント プロファイリング ポリシーに関連付けられたネットワーク スキャン アクションでは、エンドポイントのオペレーティング システム、簡易ネットワーク管理プロトコル（SNMP）ポート、および一般ポートがスキャンされます。シスコでは、最も一般的な NMAP スキャンのためのネットワーク スキャン アクションを提供していますが、独自のものを作成することもできます。

新しいネットワーク スキャンを作成する場合は、NMAP プローブがスキャンする情報のタイプを定義します。

始める前に

ネットワーク スキャン（NMAP）プローブは、ネットワーク スキャン アクションをトリガーするルールを定義する前にイネーブルにする必要があります。その手順は、「Cisco ISE ノードごとのプローブの設定」で説明します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）]** を選択します。または、**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシー要素（Policy Elements）] > [NMAPスキャンアクション（NMAP Scan Actions）]** を選択することもできます。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するネットワーク スキャン アクションの名前と説明を入力します。

ステップ 4 次のエンドポイントをスキャンする場合、1 つ以上のチェックボックスをオンにします。

- [OSのスキャン（Scan OS）]：オペレーティングシステムをスキャンする場合。
- [SNMP ポートのスキャン（Scan SNMP Port）]：SNMP ポート（161、162）をスキャンする場合。
- [一般ポートのスキャン（Scan Common Port）]：一般ポートをスキャンする場合。
- [カスタムポートのスキャン（Scan Custom Ports）]：カスタムポートをスキャンする場合。
- [サービスバージョン情報を含むスキャン（Scan Include Service Version Information）]：デバイスの詳細な説明を含むことがあるバージョン情報をスキャンする場合。

- [SMB 検出スクリプトの実行（Run SMB Discovery Script）]：SMB ポート（445 および 139）をスキャンして、OS やコンピュータ名などの情報を取得する場合。
- [NMAP ホスト検出のスキップ（Skip NMAP Host Discovery）]：NMAP スキャンの最初のホスト検出ステージをスキップする場合。

（注） [NMAP ホスト検出のスキップ（Skip NMAP Host Discovery）] オプションは自動 NMAP スキャンではデフォルトでオンになっていますが、手動 NMAP スキャンを実行する場合は選択する必要があります。

ステップ 5 [送信（Submit）] をクリックします。

NMAP オペレーティング システム スキャン

オペレーティング システム スキャン（OS-scan）タイプでは、エンドポイントで実行されているオペレーティング システム（および OS バージョン）がスキャンされます。これはリソースを大量に消費するスキャンです。

NMAP ツールには、信頼できない結果をまねく可能性がある OS-scan 上の制限があります。たとえば、スイッチやルータなどのネットワーク デバイスのオペレーティング システムをスキャンすると、NMAP OS-scan から、それらのデバイスについて正しくない operating-system 属性が返されることがあります。Cisco ISE は精度が 100% ではない場合でも、operating-system 属性を表示します。

ルールで NMAP operating-system 属性を使用するエンドポイント プロファイリング ポリシーに低い確実度値の条件（確実度係数の値）を設定する必要があります。NMAP:operating-system 属性に基づいてエンドポイント プロファイリング ポリシーを作成するときは、NMAP からの不正な結果をフィルタリングする AND 条件を含めることを推奨します。

[OS のスキャン（Scan OS）] をエンドポイント プロファイリング ポリシーに関連付けた場合、次の NMAP コマンドはオペレーティング システムをスキャンします。

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

次の NMAP コマンドを使用すると、サブネットがスキャンされ、nmapSubnet.log に出力が送信されます。

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

表 *104* : 手動サブネット スキャンの *NMAP* コマンド

-O	OS 検出の有効化
-sU	UDP スキャン
-p <port ranges>	特定のポートのみスキャンします。たとえば、U:161, 162 と指定します。
oN	通常の出力

oX	XML 出力

オペレーティング システム ポート

次の表に、NMAP が OS のスキャンに使用する TCP ポートを示します。また、NMAP は ICMP および UDP ポート 51824 を使用します。

1	3	4	6	7	9	13	17	19
20	21	22	23	24	25	26	30	32
33	37	54	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
1000	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040 ～ 1100
1102	1104	1105	1106	1107	1108	1110	1111	1112
1113	1114	1117	1119	1121	1122	1123	1124	1126
1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199

1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720
1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972	1974	1984	1998 ～ 2010	2013	2020	2021
2022	2030	2033	2034	2035	2038	2040 ～ 2043	2045 ～ 2049	2065
2068	2099	2100	2103	2105 ～ 2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381 ～ 2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000 ～ 4006	4045	4111	4125	4126	4129	4224	4242

4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000 ～ 5004	5009	5030
5033	5050	5051	5054	[5060]	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900 ～ 5907	5910	5911	5915	5922	5925	5950	5952	5959
5960 ～ 5963	5987 ～ 5989	5998 ～ 6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565 ～ 6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080 ～ 8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9,000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876

9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616
10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774
32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389
50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

NMAP SNMP ポート スキャン

SNMP ポート（161 および 162）が開いている場合、SNMPPortsAndOS-scan タイプは、エンドポイントが実行中のオペレーティングシステム（およびOSバージョン）をスキャンし、SNMP クエリーをトリガーします。さらに分類するために、識別されて不明プロファイルと最初に一致したエンドポイントに使用できます。

[SNMP ポートのスキャン（Scan SNMP Port）] をエンドポイント プロファイリング ポリシーに関連付けた場合、次の NMAP コマンドは SNMP ポート（UDP 161 と 162）をスキャンします。

nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>

表 *105 :* エンドポイントの *SNMP* ポート スキャンの *NMAP* コマンド

-sU	UDP スキャン。
-p <port-ranges>	特定のポートのみスキャンします。たとえば、UDP ポート 161 と 16.2 をスキャンします
oN	通常の出力。
oX	XML 出力。
IP-address	スキャン対象のエンドポイントの IP アドレス。

NMAP 一般ポート スキャン

CommonPortsAndOS-scan タイプでは、エンドポイントで実行されているオペレーティングシステム（および OS バージョン）がスキャンされ、SNMP ポートではなく共通ポート（TCP と UDP）もスキャンされます。[一般ポートのスキャン（Scan Common Port）] をエンドポイント プロファイリング ポリシーに関連付けると、次の NMAP コマンドが一般ポートをスキャンします。nmap -sTU -pT:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>

表 *106 :* エンドポイントの一般ポート スキャンの *NMAP* コマンド

-sTU	TCP 接続スキャンと UDP スキャンの両方。
-p <port ranges>	TCP ポート 21、22、23、25、53、80、110、135、139、143、443、445、3306、3389、8080、および UDP ポート 53、67、68、123、135、137、138、139、161、445、500、520、631、1434、1900 をスキャンします。
oN	通常の出力。
oX	XML 出力。
IP アドレス	スキャン対象のエンドポイントの IP アドレス。

一般ポート

次の表に、NMAP がスキャンのために使用する一般的なポートを示します。

表 *107 :* 一般ポート

TCP ポート		**UDP ポート**	
ポート	サービス	ポート	サービス
21/tcp	FTP	53/udp	domain
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp

TCP ポート		UDP ポート	
ポート	サービス	ポート	サービス
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

NMAP カスタム ポート スキャン

一般的なポートに加えて、カスタム ポートを使用して（**[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[ポリシー要素（Policy Elements）]** > **[NMAP スキャン アクション（NMAP Scan Actions）]** または **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[プロファイリング（Profiling）]** > **[ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）]**）、自動および手動 NMAP スキャン動作を指定できます。NMAP プローブが、指定した開いているカスタム ポートを通じてエンドポイントから属性を収集します。これらの属性は、[ISE ID（ISE Identity）] ページのエンドポイントの属性で更新されます（**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]**）。各スキャン動作に、最大で 10 個の UDP および 10 個の TCP ポートを指定することができます。一般ポートとして指定されているものと同じポート番号を使用できません。詳細については、「McAfee ePolicy Orchestrator を使用したプロファイリング ポリシーの設定」を参照してください。

サービス バージョン情報を含む NMAP スキャン

サービス バージョン情報を含む NMAP プローブは、デバイスで実行されているサービスに関する情報を収集することによる、より優れた分類のためにエンドポイントを自動的にスキャンします。このサービス バージョン オプションは、一般ポートまたはカスタム ポートと組み合わせることができます。

例：

CLI コマンド：nmap -sV -p T:8083 172.21.75.217

出力：

ポート	ステータス	サービス	バージョン
8083/tcp	open	http	McAfee ePolicy Orchestrator Agent 4.8.0.1500 (ePOServerName: WIN2008EPO, AgentGuid: {[illegible]})

NMAP SMB 検出スキャン

NMAP SMB 検出スキャンにより、Windows バージョンを区別し、よりよいエンドポイントのプロファイリングが得られます。NMAP が提供する SMB 検出スクリプトを実行するように NMAP スキャン アクションを設定できます。

NMAP スキャン アクションは Windows のデフォルト ポリシーに組み込まれ、エンドポイントがポリシーおよびスキャン ルールに一致すると、そのエンドポイントでスキャンされ、結果は、正確な Windows バージョンの決定に役立ちます。さらに、ポリシーは、フィード サービスで設定され、新しい事前定義済 NMAP スキャンが SMB の検出オプションで作成されます。

NMAP スキャン アクションは Microsoft ワークステーション ポリシーにより呼び出され、スキャンの結果は、オペレーティング システムの属性の下のエンドポイントに保存され、Windows ポリシーに活用されます。また、サブネットの手動スキャンの SMB 検出スクリプト オプションも用意されています。

（注） SMB 検出では、エンドポイントで Windows ファイル共有オプションを有効にしてください。

SMB 検出属性

SMB 検出スクリプトがエンドポイントで実行されるときに、新しい SMB 検出属性（SMB.Operating-system など）がエンドポイントに追加されます。これらの属性は、フィード サービスの Windows エンドポイント プロファイリング ポリシーの更新に対して考慮されます。SMB 検出スクリプトが実行されるときに、SMB 検出属性には SMB.operating-system、SMB.lanmanager、SMB.server、SMB.fqdn、SMB.domain、SMB.workgroup、SMB.cpe などのように、SMB が前に追加されます。

NMAP ホスト検出のスキップ

それぞれの IP アドレスのすべてのポートをスキャンすることは時間のかかるプロセスです。スキャンの目的によって、アクティブなエンドポイントの NMAP ホストの検出を省略できます。

NMAP スキャンがエンドポイントの分類の後にトリガーされると、プロファイラはエンドポイントのホストの検出を常にスキップします。ただし、手動スキャン アクションが NMAP ホスト検出のスキップ スキャンを有効にした後でトリガーされると、ホストの検出がスキップされます。

NMAP スキャン ワークフロー

NMAP スキャンを実行するための手順：

始める前に

NMAP SMB 検出スクリプトを実行するには、そのシステムでファイル共有を有効にする必要があります。例については、「NMAP SMB 検出スクリプトを実行するためのファイル共有の有効化」トピックを参照してください。

ステップ 1 SMB スキャン アクションの作成。

ステップ 2 SMB スキャン アクションを使用したプロファイラ ポリシーの設定。

ステップ 3 SMB 属性を使用した新しい条件の追加。

SMB スキャン アクションの作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[プロファイリング（Profiling）]** > **[ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）]** を選択します。

ステップ 2 [アクション名（Action Name）] と [説明（Description）] に入力します。

ステップ 3 [SMB 検出スクリプトの実行（Run SMB Discovery Script）] チェックボックスをオンにします。

ステップ 4 [追加（Add）] をクリックして、ネットワーク アクセス ユーザーを作成します。

次のタスク

SMB スキャン アクションを使用してプロファイラ ポリシーを設定する必要があります。

SMB スキャン アクションを使用したプロファイラ ポリシーの設定

始める前に

SMB スキャン アクションを使用してエンドポイントをスキャンするための新しいプロファイラ ポリシーを作成する必要があります。たとえば、DHCP クラス ID に MSFT 属性が含まれている場合にネットワーク アクションを実行する必要があるルールを指定して、Microsoft Workstation をスキャンすることができます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[追加（Add）]** の順に選択します。

ステップ 2 [名前（Name）] と [説明（Description）] に入力します。

ステップ 3 ドロップダウンで、作成したスキャン アクション（SMBScanAction など）を選択します。

次のタスク

SMB 属性を使用して新しい条件を追加する必要があります。

SMB 属性を使用した新しい条件の追加

始める前に

エンドポイントのバージョンをスキャンするには新しいプロファイラ ポリシーを作成する必要があります。たとえば、Microsoft ワークステーション親ポリシーの下で Windows 7 をスキャンできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[追加（Add）]** の順に選択します。

ステップ 2 [名前（Name）]（たとえば Windows-7Workstation）と [説明（Description）] を入力します。

ステップ 3 [ネットワーク スキャン（NMAP）アクション（Network Scan（NMAP）Action）] ドロップダウンでは [なし（None）] を選択します。

ステップ 4 [親ポリシー（Parent Policy）] ドロップダウンでは Microsoft ワークステーション ポリシーを選択します。

NMAP SMB 検出スクリプトを実行するためのファイル共有の有効化

NMAP SMB 検出スクリプトを実行するために、Windows OS バージョン 7 のファイル共有を有効にする例を次に示します。

ステップ 1 [コントロールパネル（Control Panel）] > [ネットワークとインターネット（Network and Internet）] の順に選択します。

ステップ 2 [ネットワークと共有センター（Network and Sharing Center）] をクリックします。

ステップ 3 [共有の詳細設定の変更（Change Advanced Sharing Settings）] をクリックします。

ステップ 4 [ファイルとプリンタを共有する（Turn on File and Printer Sharing）] をクリックします。

ステップ 5 [40 ビット暗号化または 56 ビット暗号化を使用するデバイスのファイル共有を有効にする（Enable File Sharing for Devices That Use 40- or 56-bit Encryption）] オプションと [パスワード保護共有を有効にする（Turn on Password Protected Sharing）] オプションを有効にします。

ステップ 6 [変更の保存（Save Changes）]をクリックします。

ステップ 7 ファイアウォール設定を設定します。

a) コントロール パネルで、**[システムとセキュリティ]** > **[Windows ファイアウォール]** > **[Windows ファイアウォールによるプログラムの許可]** の順に選択します。

b) [ファイルとプリンターの共有（File and Printer Sharing）] チェックボックスをオンにします。

c) [OK] をクリックします。

ステップ 8 共有フォルダを設定します。

a) 接続先フォルダを右クリックし、[プロパティ（Properties）] を選択します。

b) [共有（Sharing）] タブをクリックし、[共有（Share）] をクリックします。
c) [ファイルの共有（File Sharing）] ダイアログボックスで、必要な名前を追加して、[共有（Share）] をクリックします。
d) 選択したフォルダを共有した後で、[完了（Done）] をクリックします。
e) [詳細な共有（Advanced Sharing）] をクリックし、[このフォルダーの共有（Share This Folders）] チェックボックスをオンにします。
f) [アクセス許可（Permissions）] をクリックします。
g) [スキャンのアクセス許可（Permissions for Scans）] ダイアログボックスで、[全員（Everyone）] を選択し、[フル コントロール（Full Control）] チェックボックスをオンにします。
h) **[OK]** をクリックします。

NMAP スキャンからのサブネットの除外

エンドポイントの OS または SNMP ポートを特定するために NMAP スキャンを実行できます。

NMAP スキャンを実行するときに、NMAP でスキャンしないサブネット全体または IP 範囲を除外できます。**[NMAP スキャンサブネット除外（NMAP Scan Subnet Exclusions）]** ウィンドウ（**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）] > [NMAP スキャンサブネット除外（NMAP Scan Subnet Exclusions）]**）でサブネットまたは IP 範囲を設定できます。これにより、ネットワークの負荷が制限され、相当の時間を節約できます。

手動 NMAP スキャンの場合は、**[手動 NMAP スキャンの実行（Run Manual NMAP Scan）]** ウィンドウ（**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャン（Manual NMAP Scan）] > [NMAP スキャンサブネット除外の設定（Configure NMAP Scan Subnet Exclusions At）]**）を使用してサブネットまたは IP 範囲を指定できます。

手動 NMAP スキャンの設定

自動 NMAP スキャンに使用可能なオプションを使用して手動 NMAP スキャン（**[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャン（Manual NMAP Scan）]**）を実行できます。スキャン オプションまたは事前定義されているオプションを選択できます。

表 *108* : 手動 *NMAP* スキャンの設定

フィールド名	使用上のガイドライン
ノード（**Node**）	NMAP スキャンが実行する ISE ノードを選択します。
サブネットの手動スキャン（**Manual Scan Subnet**）	NMAP スキャンを実行するエンドポイントのサブネットの IP アドレスの範囲を入力します。

フィールド名	使用上のガイドライン
NMAP スキャン サブネット除外の設定（Configure NMAP Scan Subnet Exclusions At）	**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）] > [NMAP スキャンサブネット除外（NMAP Scan Subnet Exclusions）]** ウィンドウに誘導されます。除外する IP アドレスとサブネット マスクを指定します。一致が見つかると、NMAP スキャンは実行されません。
NMAP スキャン サブネット（NMAP Scan Subnet）	次のいずれかを実行できます。 • スキャン オプションの指定 • 既存の NMAP スキャンを選択します
スキャン オプションの指定（Specify Scan Options）	必要なスキャン オプションを選択します（OS、SNMP ポート、共通ポート、カスタム ポート、サービス バージョン情報を含む、SMB 検出スクリプトの実行、NMAP ホスト検出のスキップ）。詳細については、「新しいネットワーク スキャン アクションの作成」を参照してください。
既存の NMAP スキャンを選択（Select an Existijng NMAP Scan）	[既存の NMAP スキャンアクション（Existing NMAP Scan Actions）] ドロップダウンリストが表示され、デフォルトのプロファイラ NMAP スキャン アクションが表示されます。
デフォルトのスキャン オプションにリセット（Reset to Default Scan Options）	このボタンをクリックしてデフォルト設定を復元します（すべてのスキャンオプションをオンにします）。
名前を付けて NMAP スキャン アクションを保存（Save as NMAP Scan Action）	アクション名と説明を入力します。

手動 NMAP スキャンの実行

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャン（Manual NMAP Scan）]** の順に選択します。

ステップ 2 [ノード（Node）] ドロップダウンリストで、NMAP スキャンを実行する予定の ISE ノードを選択します。

ステップ 3 [サブネットの手動スキャン（Manual Scan Subnet）] テキスト ボックスに、オープン ポートをチェックする予定のエンドポイントのサブネット アドレスを入力します。

ステップ 4 次のいずれかを選択します。

a) [スキャン オプションの指定（Specify Scan Options）] を選択し、ページの右側で、必要なスキャン オプションを選択します。詳細については、「新しいネットワーク スキャン アクションの作成」ページを参照してください。

b) [既存の NMAP スキャンアクションの選択（Select An Existing NMAP Scan Action）] を選択し、MCAFeeEPOOrchestratorClientScan などのデフォルトの NMAP アクションを選択します。

ステップ 5 [スキャンの実行（Run Scan）] をクリックします。

McAfee ePolicy Orchestrator を使用したプロファイリング ポリシーの設定

サービスのプロファイリングを行うCisco ISEは、McAfee ePolicy Orchestrator （McAfee ePO）クライアントをエンドポイントに登録するかどうかが検出されます。これにより、特定のエンドポイントが組織に属しているかどうかを確認する上で役立ちます。

このプロセスに関与するエンティティは、次のとおりです。

- ISEサーバー
- McAfee ePOサーバー
- McAfee ePO Agent

Cisco ISEは、オンボードNMAPスキャン動作（）をMCAFeeEPOOrchestratorClientscan McAfeeのエージェントが設定されているポート上でNMAP McAfeeのスクリプトを使用して、エンドポイントで実行されているかどうかを確認できます。また、カスタム ポートマップを使用して新しいNMAPスキャン オプション作成できます（たとえば、8082）。McAfee ePOソフトウェアを使用して、次の手順に従って、新しいNMAPスキャン動作を設定可能です。

ステップ 1 McAfee ePo NMAP スキャン アクションの設定。

ステップ 2 McAfee ePO Agent の設定。

ステップ 3 McAfee ePO NMAP スキャン アクションを使用したプロファイラ ポリシーの設定。

McAfee ePo NMAP スキャン アクションの設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシー要素（Policy Elements）] > [ネットワーク スキャン（NMAP）アクション（Network Scan（NMAP）Actions）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [アクション名（Action Name）] と [説明（Description）] に入力します。

ステップ 4 [スキャンオプション（Scan Options）] では、[カスタムポート（Custom Ports）] を選択します。

ステップ 5 [カスタム ポート（Custom Ports）] ダイアログボックスで、必要な TCP ポートを追加します。TCP ポート 8080 は、McAfee ePO に対してデフォルトで有効になっています。

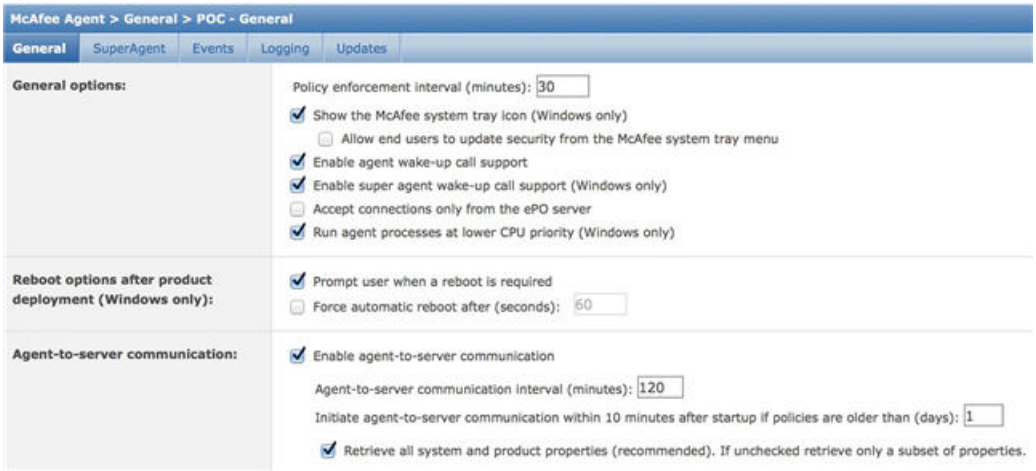
ステップ 6 [サービス バージョン情報を含む（Include Service Version Information）] チェック ボックスをオンにします。

ステップ 7 [送信（Submit）] をクリックします。

McAfee ePO Agent の設定

ステップ 1 McAfee ePO サーバーで、McAfee ePO Agent と ISE サーバー間の通信を容易にするために推奨される設定を確認します。

図 *29 : McAfee ePO Agent* の推奨されるオプション



ステップ 2 [ePO サーバーからのみ接続を受け入れる（Accept Connections Only From The ePO Server）] のマークが外されていることを確認します。

McAfee ePO NMAP スキャン アクションを使用したプロファイラ ポリシーの設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[追加（Add）]** の順に選択します。

ステップ 2 [名前（Name）] と [説明（Description）] に入力します。

ステップ 3 [ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Action）] ドロップダウンで、必要なアクション（MCAFeeEPOOrchestratorClientscan など）を選択します。

ステップ 4 親プロファイラ ポリシー（DHCP クラス ID に MSFT 属性が含まれているかどうかを確認するルールを含む Microsoft-Workstation など）を作成します。

ステップ 5 McAfee ePO Agent がエンドポイントにインストールされているかどうかを確認するために、親 NMAP McAfee ePO ポリシー（Microsoft-Workstation など）内に新しいポリシー（CorporateDevice など）を作成します。

条件を満たすエンドポイントが会社のデバイスとしてプロファイルされます。このポリシーを使用して、McAfee ePO Agent によってプロファイルされたエンドポイントを新しい VLAN に移動することができます。

プロファイラ エンドポイント カスタム属性

エンドポイントがプローブから収集する属性に加えて、他の属性をエンドポイントに割り当てるには、**[管理（Administration）] > [ID 管理（Identity Management）] > [設定（Settings）] > [エンドポイントカスタム属性（Endpoint Custom Attributes）]** を選択します。エンドポイントのカスタム属性は、認可ポリシーでエンドポイントのプロファイルを作成するために使用できます。

最大100個のエンドポイントのカスタム属性を作成できます。サポートされるエンドポイントのカスタム属性の型は次のとおりです：Int、String、Long、Boolean および Float。

[コンテキストディレクトリ（Context Directory）] > [エンドポイント（Endpoints）] > [エンドポイント分類（Endpoint Classification）] ウィンドウで、エンドポイントのカスタム属性の値を追加できます。

エンドポイントのカスタム属性に対する使用例には、特定の属性に基づくデバイスの許可またはブロック、あるいは認証に基づく特定の権限の割り当てが含まれています。

認証ポリシーでのエンドポイント カスタム属性の使用

[エンドポイントカスタム属性（Endpoint Custom Attributes）] セクションを使用すると、追加の属性を設定できます。各定義は属性とタイプ（String、Int、Boolean、Float、Long）で構成されます。エンドポイントカスタム属性を使用して、デバイスのプロファイリングを行うことができます。

（注） エンドポイントにカスタム属性を追加するには、Cisco ISE Advantage のライセンスが必要です。

エンドポイント カスタム属性を使用して許可ポリシーを作成する手順を以下に示します。

ステップ 1 エンドポイント カスタム属性を作成し、値を割り当てます。

a) **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント カスタム属性（Endpoint Custom Attributes）]** の順に選択します。

b) [エンドポイント カスタム属性（Endpoint Custom Attributes）] 領域で、[属性名（Attribute Name）]（たとえば、deviceType）と [データ型（Data Type）]（たとえば、String）とパラメータを入力します。

c) [保存（Save）] をクリックします。

d) **[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [概要（Summary）]** の順に選択します。

e) カスタム属性値を割り当てます。

- 必要な MAC アドレスのチェックボックスをオンにし、[編集（Edit）] をクリックします。
- または、必要な MAC アドレスをクリックして、[エンドポイント（Endpoints）] ページで、[編集（Edit）] をクリックします。

f) [エンドポイントの編集（Edit Endpoint）] ダイアログボックスの [カスタム属性（Custom Attribute）] 領域に、必須の属性値（たとえば、deviceType = Apple-iPhone）を入力します。

g) [保存（Save）] をクリックします。

ステップ 2 カスタム属性と値を使用して許可ポリシーを作成します。

a) **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]** を選択します。

b) エンドポイントの辞書からカスタム属性を選択することで、許可ポリシーを作成します（たとえば、Rule Name: Corporate Devices, Conditions:EndPoints:deviceType Contains Apple-iPhone, Permissions: then PermitAccess）。

c) [保存（Save）] をクリックします。

関連トピック

プロファイラ エンドポイント カスタム属性 （1266 ページ）

プロファイラ条件の作成

Cisco ISE のエンドポイント プロファイリング ポリシーを使用すると、ネットワーク上で検出されたエンドポイントを分類し、特定のエンドポイント ID グループに割り当てることができます。これらのエンドポイント プロファイリング ポリシーは、エンドポイントを分類し、グループ化するために Cisco ISE が評価するプロファイリング条件から構成されます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [プロファイリング（Profiling）] > [追加（Add）]** を選択します。

ステップ 2 エンドポイントプロファイリングポリシーの設定 （1269ページ）の説明に従って、フィールドに値を入力します。

ステップ 3 [送信（Submit）] をクリックして、プロファイラ条件を保存します。

ステップ 4 さらに多くの条件を作成するには、この手順を繰り返します。

エンドポイント プロファイリング ポリシー ルール

ルールを定義すると、すでにポリシー要素ライブラリに作成および保存されているライブラリから 1 つ以上のプロファイリング条件を選択し、確実度係数の整数値を各条件に関連付けるか、例外アクションまたはネットワーク スキャン アクションをその条件に関連付けることができます。例外アクションまたはネットワーク スキャン アクションは、Cisco ISE がエンドポイントの分類全体に関するプロファイリング ポリシーを評価しているときに、設定可能なアクションをトリガーするために使用します。

特定のポリシー内のルールがOR演算子で個別に評価されると、各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。エンドポイント プロファイリング ポリシーのルールが一致した場合、そのプロファイリングポリシーおよび一致するポリシーは、それらがネットワーク上で動的に検出された場合のエンドポイントと同じです。

プロファイリングポリシーの分類の優先順位

Cisco ISEは、シスコ提供の、または管理者が作成したプロファイリングポリシーに基づいて、ネットワーク内のデバイスを分類します、Cisco ISE リリース 3.3 からは、デバイスの分類に使用するプロファイリングポリシーのカテゴリの優先順位を設定できます。

[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [プロファイリングポリシー（Profiling Policies）] ページには、シスコ提供のプロファイリングポリシーと管理者が作成したプロファイリングポリシーの両方が表示されます。

プロファイリング ポリシー タイプに優先順位を付けるには、**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）] > [プロファイラ設定（Profiler Settings）]** の順に進みます。[重複する分類の優先順位（Overlapping Classification Priority）] ドロップダウンメニューから、[管理者優先（Admin First）] または [シスコ優先（Cisco First）] を選択します。この設定のデフォルト値では、管理者が作成したポリシーが優先になっています。

シスコ提供のプロファイリングポリシーと管理者が作成したプロファイリングポリシーがあり、どちらもエンドポイントに一致する場合、このプライオリティ設定によって、プロファイリング ワークフローで適用されるプロファイルが決まります。プライオリティ設定の値だけで、重複するポリシーの確実性要因に関係なく、エンドポイントと一致するポリシーが決定されます。

たとえば、確実度係数 10 の Cisco ポリシー A と確実度係数 5 の管理者ポリシー B がエンドポイントで使用可能な場合に、[管理者優先（Admin First）] が優先して選択されていたら、管理者ポリシー B がエンドポイントに割り当てられます。

設定した優先順位は、Endpoints:EndpointPolicy や Endpoints:LogicalProfile など、使用する AuthZ 条件に基づくエンドポイントの認証にも影響を及ぼします。

ルール内で論理的にグループ化される条件

エンドポイントプロファイリング ポリシー（プロファイル）には、単一の条件またはAND演算子やOR演算子を使用して論理的に結合された複数の単一条件の組み合わせが含まれ、これらの条件と照合して、ポリシー内の特定のルールについてエンドポイントをチェック、分類、およびグループ化することができます。

条件は、収集されたエンドポイント属性値をエンドポイントの条件に指定されている値と照合するために使用されます。複数の属性をマッピングする場合は、条件を論理的にグループ化して、ネットワーク上のエンドポイントの分類に使用できます。ルールで対応する確実度メトリック（定義済みの整数値）が関連付けられている1つ以上の条件とエンドポイントを照合するか、または、条件に関連付けられた例外アクション、または条件に関連付けられたネットワーク スキャン アクションをトリガーすることができます。

確実度係数

プロファイリングポリシーの最小確実度メトリックは、エンドポイントの一致するプロファイルを評価します。エンドポイント プロファイリング ポリシーの各ルールには、プロファイリング条件に関連付けられた最小確実度メトリック（整数値）があります。確実度メトリックは、エンドポイント プロファイリング ポリシー内のすべての有効ルールに対して追加される尺度で、エンドポイント プロファイリング ポリシー内の各条件がエンドポイントの全体的な分類の改善にどの程度役立つかを測定します。

各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。すべての有効なルールの確実度メトリックが合計され、照合の確実度が求められます。この値は、エンドポイントプロファイリング ポリシーに定義されている最小の確実度係数を超えている必要があります。デフォルトでは、すべての新しいプロファイリング ポリシー ルールおよび事前に定義されたプロファイリング ポリシーで、最小の確実度係数は 10 です。

エンドポイント プロファイリング ポリシーの設定

次の表では、[エンドポイントポリシー（Endpoint Policies）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[プロファイリング ポリシー（Profiling Policies）]**。

表 *109* : エンドポイント プロファイリング ポリシーの設定

フィールド名	使用上のガイドライン
名前（Name）	作成するエンドポイントプロファイリングポリシーの名前を入力します。
説明（Description）	作成するエンドポイントプロファイリングポリシーの説明を入力します。
ポリシー有効（Policy Enabled）	デフォルトでは [ポリシー有効（Policy Enabled）] チェックボックスはオンになっており、エンドポイントのプロファイリング時に、一致するプロファイリング ポリシーが関連付けられます。 オフになっている場合、エンドポイントのプロファイリング時に、エンドポイント プロファイリング ポリシーは除外されます。
最小確実度計数（Minimum Certainty Factor）	プロファイリングポリシーに関連付ける最小値を入力します。デフォルト値は 10 です。

フィールド名	使用上のガイドライン
例外アクション（Exception Action）	プロファイリング ポリシー内のルールを定義するときに条件に関連付ける例外アクションを選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[結果（Results）]>[プロファイリング（Profiling）]>[例外アクション（Exception Actions）] で定義されます。
ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Action）	必要に応じて、プロファイリング ポリシー内のルールを定義するときに条件に関連付けるネットワーク スキャン アクションをリストから選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[結果（Results）]>[プロファイリング（Profiling）]>[ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Actions）] で定義されます。
ポリシーの ID グループの作成（Create an Identity Group for the policy）	エンドポイント ID グループを作成するには、次のオプションのいずれかをオンにします。 • **はい、一致する ID グループを作成します（Yes, create matching Identity Group）** • **いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）**
はい、一致する ID グループを作成します（Yes, create matching Identity Group）	既存のプロファイリング ポリシーを使用する場合、このオプションを選択します。 このオプションは、これらのエンドポイントの一致する ID グループを作成します。エンドポイント プロファイルが既存のプロファイリング ポリシーと一致した場合に、ID グループは Profiled エンドポイント ID グループの子になります。 たとえば、ネットワーク上で検出されたエンドポイントが Xerox-Device プロファイルに一致する場合は、[エンドポイント ID グループ（Endpoint Identity Groups）] ページで Xerox-Device エンドポイント ID グループが作成されます。

フィールド名	使用上のガイドライン
いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）	プロファイリング ポリシーおよび ID グループの階層構造を使用して、一致する親エンドポイント ID グループにエンドポイントを割り当てるには、このチェックボックスをオンにします。 このオプションを使用すると、エンドポイントプロファイリングポリシー階層を利用することができ、エンドポイントはいずれかの一致する親エンドポイント ID グループ、さらに、親 ID グループに関連付けられたエンドポイント ID グループに割り当てられます。 たとえば、既存のプロファイルに一致するエンドポイントは、適切な親エンドポイント ID グループの下にグループ化されます。ここで、不明プロファイルに一致するエンドポイントは、[不明（Unknown）] の下にグループ化され、既存のプロファイルに一致するエンドポイントは、プロファイリングされたエンドポイント ID グループの下にグループ化されます。次の例を参考にしてください。 • エンドポイントが Cisco-IP-Phone プロファイルに一致する場合、これらのエンドポイントは Cisco-IP-Phone エンドポイント ID グループの下でグループ化されます。 • エンドポイントが Workstation プロファイルに一致する場合、これらのエンドポイントは、Workstation エンドポイント ID グループの下でグループ化されます。 Cisco-IP-Phone および Workstation エンドポイント ID グループは、システム内の Profiled エンドポイント ID グループに関連付けられます。
親ポリシー（Parent Policy）	新しいエンドポイント プロファイリング ポリシーを関連付ける、システムで定義されている親プロファイリング ポリシーを選択します。 子にルールと条件を継承できる親プロファイリングポリシーを選択できます。
関連 CoA タイプ（Associated CoA Type）	エンドポイント プロファイリング ポリシーと関連付ける次のいずれかの CoA タイプを選択します。 • CoA なし（No CoA） • ポートバウンス（Port Bounce） • 再認証（Reauth） • [グローバル設定（Global Settings）] : [管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロファイリング（Profiling）] で設定されたプロファイラ設定から適用されます。

フィールド名	使用上のガイドライン
ルール（**Rule**）	エンドポイント プロファイリング ポリシーで定義された 1 つ以上のルールにより、エンドポイントの一致するプロファイリング ポリシーが決定されます。これにより、プロファイルに応じたエンドポイントのグループ化が可能になります。 ポリシー要素ライブラリからの 1 つ以上のプロファイリング条件がルールに使用され、エンドポイント属性およびその値が、全体的な分類用に検証されます。
条件（**Conditions**）	プラス（+）記号をクリックして、条件の固定オーバーレイを展開します。マイナス（-）記号をクリックするか、固定オーバーレイの外側をクリックして条件を閉じます。 [既存の条件をライブラリから選択（Select Existing Condition from Library）] または [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] をクリックします。 [既存の条件をライブラリから選択（Select Existing Condition from Library）]：ポリシー要素ライブラリからシスコによって事前定義された条件を選択して、式を定義できます。 [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）]：さまざまなシステム辞書またはユーザー定義辞書から属性を選択して、式を定義できます。 プロファイリング条件と次のいずれかとを関連付けることができます。 • 各条件の確実度係数の整数値 • その条件の例外アクションまたはネットワーク スキャン アクション プロファイリング条件と関連付ける、次のいずれかの定義済み設定を選択します。 • [確実度計数が増加する（Certainty Factor Increases）]：各ルールの確実度値を入力します。この値は、全体的な分類に関するすべての一致ルールに対して追加されます。 • [例外の操作を行う（Take Exception Action）]：このエンドポイント プロファイリング ポリシーの [例外アクション（Exception Action）] フィールドで設定された例外アクションがトリガーされます。 • [ネットワークスキャンを行う（Take Network Scan Action）]：このエンドポイント プロファイリング ポリシーの [ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Action）] フィールドで設定されたネットワーク スキャン アクションがトリガーされます。

フィールド名	使用上のガイドライン
既存の条件をライブラリから選択（Select Existing Condition from Library）	次を実行できます。 • ポリシー要素ライブラリに存在するシスコによって事前定義された条件を選択できます。AND またはOR 演算子を使用して複数の条件を追加できます。 • [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。 • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます • [複製（Duplicate）]：選択した条件のコピーを作成します • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます • [削除（delete）]：選択した条件を削除します。
新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）	次を実行できます。 • 式にアドホック属性/値の組み合わせを追加し、AND または OR 演算子を使用すると、複数の条件を追加できます。 • [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。 • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます • [複製（Duplicate）]：選択した条件のコピーを作成します • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます • [削除（delete）]：選択した条件を削除します。 AND または OR 演算子を使用できます

関連トピック

Cisco ISE プロファイリング サービス （1210 ページ）

エンドポイント プロファイリング ポリシーの作成 （1274 ページ）
UDID 属性を使用するエンドポイント コンテキストの可視性 （1317 ページ）

エンドポイント プロファイリング ポリシーの作成

新しいプロファイリングポリシーを作成して、エンドポイントをプロファイリングするには、[新しいプロファイラ ポリシー（New Profiler Policy）]ページで次のオプションを使用します。

- ポリシー有効（Policy Enabled）
- [ID グループの作成（Create an Identity Group）]：一致するエンドポイント ID グループを作成するか、またはエンドポイント ID グループ階層を使用するポリシーの場合
- 親ポリシー（Parent Policy）
- 関連 CoA タイプ（Associated CoA Type）

（注） [プロファイリングポリシー（Profiling Policies）] ウィンドウでエンドポイントポリシーを作成する場合は、Web ブラウザの停止ボタンを使用しないでください。このアクションによって、[新しいプロファイラポリシー（New Profiler Policy）] ウィンドウでのロードが停止され、アクセス時にリストページ内のその他のリストページおよびメニューがロードされ、リストページ内のフィルタメニュー以外のすべてのメニューでの操作を実行できなくなります。リストページ内ですべてのメニューの操作を実行するには、Cisco ISE からログアウトし、再度ログインする必要がある場合があります。

類似した特性のプロファイリングポリシーを作成するには、すべての条件を再定義して新しいプロファイリングポリシーを作成するのではなく、エンドポイントプロファイリングポリシーを複製して変更することができます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[プロファイリングポリシー（Profiling Policies）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成する新しいエンドポイント ポリシーの名前と説明を入力します。[ポリシー有効（Policy Enabled）] チェックボックスはデフォルトでオンになっており、エンドポイントのプロファイリング時に検証するエンドポイント プロファイリング ポリシーが含まれます。

ステップ 4 有効範囲 1 ～ 65535 の最小の確実度係数の値を入力します。

（注） カスタム プロファイリング ポリシーを作成する場合は、次の事項を考慮する必要があります。

- カスタムポリシーで設定された同じ属性が、デフォルトのプロファイリングポリシーによって評価されるようにすでに設定されている場合、およびデフォルトのプロファイリングポリシーの確実度係数（CF）がカスタムポリシーの CF よりも大きい場合、カスタムプロファイリングポリシーはどのエンドポイントにも割り当てられません。これは、CF の増加が大きいプロファイリングポリシーが、CF の増加が小さい他のポリシーよりも優先されるためです。
- 多くのデフォルトのプロファイリングポリシーは、増分 CF が 10、20、および 30 ずつ増加するように設定されています。

ステップ 5 [例外アクション（Exception Action）] ドロップダウン リストの隣にある矢印をクリックして、例外アクションを関連付けるか、[ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）] ドロップダウン リストの隣にある矢印をクリックして、ネットワーク スキャン アクションを関連付けます。

ステップ 6 [ポリシーの ID グループの作成（Create an Identity Group for the policy）] で次のオプションのいずれか 1 つを選択します。

- **はい、一致する ID グループを作成します（Yes, create matching Identity Group）**
- **いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）**

ステップ 7 [親ポリシー（Parent Policy）] ドロップダウン リストの隣の矢印をクリックして、新しいエンドポイント ポリシーに親ポリシーを関連付けます。

ステップ 8 [関連付ける CoA タイプ（Associated CoA Type）] ドロップダウン リストで、関連付ける CoA タイプを選択します。

ステップ 9 ルールをクリックし、条件を追加して、各条件の確実度係数の整数値を関連付けるか、エンドポイントの全体的な分類のその条件の例外アクションまたはネットワーク スキャン アクションを関連付けます。

ステップ 10 [送信（Submit）] をクリックしてエンドポイント ポリシーを追加するか、または [新しいプロファイラ ポリシー（New Profiler Policy）] ページの [プロファイラ ポリシー リスト（Profiler Policy List）] リンクをクリックして [プロファイリング ポリシー（Profiling Policies）] ページに戻ります。

エンドポイント プロファイリング ポリシーごとの認可変更の設定

Cisco ISE の許可変更（CoA）タイプのグローバル コンフィギュレーションに加えて、各エンドポイント プロファイリング ポリシーに関連付けられた特定のタイプの CoA も発行するように設定できます。

グローバル CoA なしタイプの設定は、エンドポイント プロファイリング ポリシーで設定された各 CoA タイプを上書きします。グローバル CoA タイプが CoA なしタイプ以外に設定されている場合、各エンドポイント プロファイリング ポリシーはグローバル CoA の設定を上書きできます。

CoA がトリガーされると、各エンドポイント プロファイリング ポリシーは、次のように実際の CoA タイプを決定できます。

- [全般設定（General Settings）]：これは、グローバル コンフィギュレーションごとに CoA を発行するすべてのエンドポイントプロファイリングポリシーのデフォルトの設定です。
- [CoA なし（No CoA）]：この設定はグローバル コンフィギュレーションを上書きし、そのプロファイルの CoA を無効にします。
- [ポート バウンス（Port Bounce）]：この設定は、グローバル ポート バウンスおよび再認証設定タイプを上書きし、ポート バウンス CoA を発行します。
- [再認証（Reauth）]：この設定は、グローバルポートバウンスおよび再認証設定タイプを上書きし、再認証 CoA を排出します。

（注） プロファイラ グローバル CoA 設定がポート バウンス（または再認証）に設定されている場合は、モバイル デバイスの BYOD フローが切断されないように、対応するエンドポイントプロファイリング ポリシーを [CoA なし（No CoA）]、[ポリシーごとの CoA（per-policy CoA）] オプションを指定して設定していることを確認します。

グローバルおよびエンドポイント プロファイリング ポリシー設定に基づいて各場合に発行されたすべての CoA タイプと実際の CoA タイプが組み合わされた設定については、次の概要を参照してください。

表 *110*：設定のさまざまな組み合わせに発行された *CoA* タイプ

グローバル **CoA** タイプ	ポリシーごとに設定されたデフォルトの **CoA** タイプ	ポリシーごとの **CoA** なしタイプ	ポリシーごとのポート バウンス タイプ	ポリシーごとの再認証タイプ
CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）
ポートバウンス（Port Bounce）	ポートバウンス（Port Bounce）	CoA なし（No CoA）	ポートバウンス（Port Bounce）	再認証（Re-Auth）
再認証（Reauth）	再認証（Reauth）	CoA なし（No CoA）	ポートバウンス（Port Bounce）	再認証（Re-Auth）

エンドポイント プロファイリング ポリシーのインポート

エクスポート機能で作成できる同じ形式を使用して、XML ファイルからエンドポイント プロファイリング ポリシーをインポートできます。親ポリシーが関連付けられている、新しく作成

されたプロファイリング ポリシーをインポートする場合は、子ポリシーを定義する前に親ポリシーを定義しておく必要があります。

インポート ファイルでは、エンドポイント プロファイリング ポリシーが階層構造になっており、最初に親ポリシー、次にポリシーに定義されているルールとチェックとともにインポートしたプロファイルが含まれます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]**>**[プロファイリング（Profiling）]**>**[プロファイリング（Profiling）]**>**[プロファイリングポリシー（Profiling Policies）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、前にエクスポートしてこれからインポートするファイルを特定します。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 [プロファイリングポリシー（Profiling Policies）] ウィンドウに戻るには、[プロファイラポリシーリスト（Profiler Policy List）] リンクをクリックします。

エンドポイント プロファイリング ポリシーのエクスポート

他の Cisco ISE 展開にエンドポイント プロファイリング ポリシーをエクスポートできます。または、XML ファイルを独自のポリシーを作成するためのテンプレートとして使用してインポートできます。ファイルをシステムのデフォルトの場所にダウンロードして、後でインポートに使用することもできます。

エンドポイント プロファイリング ポリシーをエクスポートする際にダイアログが表示され、適切なアプリケーションで profiler_policies.xml を開くか、保存するように要求されます。これは XML 形式のファイルで、Web ブラウザまたは他の適切なアプリケーションで開くことができます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]**>**[プロファイリング（Profiling）]**>**[プロファイリング（Profiling）]**>**[プロファイリングポリシー（Profiling Policies）]** を選択します。

ステップ 2 [エクスポート（Export）] を選択し、次のいずれかを選択します。

- [選択済みをエクスポート（Export Selected）]：[プロファイリングポリシー（Profiling Policies）] ウィンドウでは、選択済みのエンドポイント プロファイリングのポリシーだけをエクスポートできます。
- [選択済みとエンドポイントをエクスポート（Export Selected with Endpoints）]：選択済みのエンドポイントプロファイリング ポリシーと、選択済みのエンドポイントプロファイリング ポリシーでプロファイリングされたエンドポイントをエクスポートできます。
- [すべてエクスポート（Export All）]：デフォルトでは、[プロファイリングポリシー（Profiling Policies）] ウィンドウのすべてのプロファイリングポリシーをエクスポートできます。

ステップ 3 [OK] をクリックして、profiler_policies.xml ファイルのエンドポイント プロファイリング ポリシーをエクスポートします。

事前定義されたエンドポイント プロファイリング ポリシー

Cisco ISE を展開するとき、Cisco ISE には事前定義されたデフォルトのプロファイリング ポリシーが含められます。その階層構造を使用して、ネットワーク上の識別されたエンドポイントを分類し、それらを一致するエンドポイント ID グループに割り当てることができます。エンドポイント プロファイリング ポリシーは階層的であるため、[プロファイリング ポリシー（Profiling Policies）] ウィンドウにはデバイスの汎用（親）ポリシーと、それらの親ポリシーが [プロファイリング ポリシー（Profiling Policies）] リストウィンドウに関連付けられている子ポリシーが表示されます。

[プロファイリング ポリシー（Profiling Policies）] ウィンドウには、エンドポイント プロファイリングポリシーとともに、その名前、タイプ、説明、およびステータス（検証が有効になっているかどうか）が表示されます。

エンドポイント プロファイリング ポリシー タイプは、次のように分類されます。

- シスコ提供：Cisco ISE で事前に定義されたエンドポイント プロファイリング ポリシーはシスコ提供タイプとして識別されます。
    - 管理者による変更：事前に定義されたエンドポイント プロファイリング ポリシーを変更したときに、エンドポイント プロファイリング ポリシーは管理者による変更タイプとして識別されます。Cisco ISE では、事前定義されたエンドポイント プロファイリング ポリシーに行った変更がアップグレード時に上書きされます。
- 管理者作成：作成したエンドポイント プロファイリング ポリシー、またはシスコ提供のエンドポイント プロファイリング ポリシーを複製したときのエンドポイント プロファイリング ポリシーは、管理者作成タイプとして識別されます。

一連のエンドポイントの一般的なポリシー（親）を作成して、その子がルールと条件を継承できるようにすることを推奨します。エンドポイントを分類する必要がある場合は、エンドポイントをプロファイリングするときに、まずエンドポイントプロファイルを親ポリシーと、次にその子孫（子）ポリシーと照合する必要があります。

たとえば、Cisco-Device は、すべてのシスコ デバイスの一般的なエンドポイント プロファイリングのポリシーであり、シスコ デバイスの他のポリシーは、Cisco-Device の子です。エンドポイントを Cisco-IP-Phone 7960 として分類する必要がある場合は、まずこのエンドポイントのエンドポイント プロファイルを親の Cisco-Device ポリシー、その子の Cisco-IP-Phone ポリシーと照合する必要があり、その後さらに分類するために Cisco-IP-Phone 7960 プロファイリング ポリシーと照合します。

（注） Cisco ISE では、管理者によって変更されたポリシーや子ポリシーは、シスコ提供のラベルが付いていても上書きされません。管理者が変更したポリシーが削除されると、以前のシスコ提供のポリシーに戻ります。次にフィードの更新が発生すると、すべての子ポリシーが更新されます。

アップグレード中に上書きされる事前定義されたエンドポイントプロファイリング ポリシー

[プロファイリング ポリシー（Profiling Policies）] ページで既存のエンドポイント プロファイリング ポリシーを編集できます。また、事前定義されたエンドポイント プロファイリング ポリシーを変更するときは、事前定義されたエンドポイントプロファイルのコピーにすべての設定を保存する必要があります。

アップグレード時に、事前定義されたエンドポイントプロファイルに保存した設定が上書きされます。

エンドポイント プロファイリング ポリシーを削除できない

[プロファイリングポリシー（Profiling Policies）] ウィンドウで選択したエンドポイント プロファイリング ポリシーまたはすべてのエンドポイント プロファイリング ポリシーを削除できます。デフォルトでは、[プロファイリングポリシー（Profiling Policies）] ウィンドウからすべてのエンドポイント プロファイリング ポリシーを削除できます。[プロファイリングポリシー（Profiling Policies）] ウィンドウですべてのエンドポイントプロファイリング ポリシーを選択して削除しようとしても、エンドポイント プロファイリング ポリシーが他のエンドポイントプロファイリングポリシーにマッピングされるか、または認証ポリシーにマッピングされる場合、そのエンドポイント プロファイリング ポリシーは削除できません。

- シスコ提供のエンドポイント プロファイリング ポリシーは削除できません。
- エンドポイントプロファイルが他のエンドポイントプロファイルの親として定義されている場合は、[プロファイリングポリシー（Profiling Policies）] ウィンドウで親プロファイルを削除できません。たとえば、Cisco-Device は、シスコデバイスの他のエンドポイントプロファイリング ポリシーの親です。
- 許可ポリシーにマッピングされているエンドポイントプロファイルは削除できません。たとえば、Cisco-IP-Phone は Profiled Cisco IP Phones 許可ポリシーにマッピングされ、Cisco IP Phone の他のエンドポイント プロファイリング ポリシーの親です。

Draeger 医療機器用の事前定義済みプロファイリング ポリシー

Cisco ISE のデフォルトのエンドポイント プロファイルには、Draeger 医療機器用の一般的なポリシー、Draeger-Delta 医療機器用のポリシー、および Draeger-M300 医療機器用のポリシーが

含まれます。両方の医療機器にポート 2050 と 2150 があるため、デフォルトの Draeger エンドポイント プロファイリング ポリシーを使用しても、Draeger-Delta 医療機器と Draeger-M300 医療機器を分類できません。

使用中の環境では、これらの Draeger デバイスにポート 2050 と 2150 があるため、デフォルトの Draeger-Delta and Draeger-M300 エンドポイント プロファイリング ポリシーでデバイスの宛先 IP アドレスのチェックに加えて、これらの医療機器を区別できるようにルールを追加する必要があります。

Cisco ISE には、Draeger 医療機器のエンドポイント プロファイリング ポリシーで使用される次のプロファイリング条件があります。

- ポート 2000 が含まれる Draeger-Delta-PortCheck1
- ポート 2050 が含まれる Draeger-Delta-PortCheck2
- ポート 2100 が含まれる Draeger-Delta-PortCheck3
- ポート 2150 が含まれる Draeger-Delta-PortCheck4
- ポート 1950 が含まれる Draeger-M300PortCheck1
- ポート 2050 が含まれる Draeger-M300PortCheck2
- ポート 2150 が含まれる Draeger-M300PortCheck3

不明なエンドポイントのエンドポイント プロファイリング ポリシー

既存のプロファイルに一致せず、Cisco ISE でプロファイリングできないエンドポイントは、不明なエンドポイントです。不明プロファイルは、エンドポイントについて収集された属性が Cisco ISE の既存のプロファイルと一致しない場合にそのエンドポイントに割り当てられるデフォルトのシステム プロファイリング ポリシーです。

不明プロファイルは次のシナリオで割り当てられます。

- エンドポイントが Cisco ISE で動的に検出され、そのエンドポイントに一致するエンドポイント プロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。
- エンドポイントが Cisco ISE で静的に追加され、静的に追加されたエンドポイントに一致するエンドポイント プロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。

  ネットワークにエンドポイントを静的に追加した場合、そのエンドポイントは Cisco ISE のプロファイリング サービスによってプロファイリングされません。不明プロファイルを適切なプロファイルに後で変更できます。割り当てたプロファイリング ポリシーは、Cisco ISE によって再プロファイリングされることはありません。

静的に追加されたエンドポイントのエンドポイントプロファイリングポリシー

静的に追加されたエンドポイントをプロファイリングするために、プロファイリングサービスは、新しい MATCHEDPROFILE 属性をエンドポイントに追加することによって、エンドポイントのプロファイルを計算します。計算されたプロファイルは、そのエンドポイントが動的にプロファイリングされるときのエンドポイントの実際のプロファイルです。これにより、静的に追加されたエンドポイントの計算されたプロファイルと動的にプロファイリングされたエンドポイントに一致するプロファイルの間の不一致を見つけることができます。

スタティックIPデバイスのエンドポイントプロファイリングポリシー

静的に割り当てられた IP アドレスを持つエンドポイントがある場合、そのスタティック IP デバイスのプロファイルを作成できます。

スタティック IP アドレスが割り当てられているエンドポイントをプロファイリングするには、RADIUS プローブまたは SNMP クエリー プローブと SNMP トラップ プローブを有効にする必要があります。

エンドポイント プロファイリング ポリシーの一致

1 つ以上のルールで定義されているプロファイリング条件がプロファイリング ポリシーに一致する場合、Cisco ISE は、エンドポイント用に選択されたポリシーを、評価されたポリシーではなく、一致したポリシーであると常に見なします。ここで、そのエンドポイントのスタティック割り当てのステータスがシステムで false に設定されます。ただし、エンドポイントの編集時にスタティック割り当て機能を使用して、システム内の既存のプロファイリング ポリシーに静的に再割り当てした後は、true に設定されることがあります。

次は、エンドポイントの一致したポリシーに適用されます。

- スタティックに割り当てられたエンドポイントでは、プロファイリング サービスは MATCHEDPROFILE を計算します。
- 動的に割り当てられたエンドポイントでは、MATCHEDPROFILE は一致するエンドポイント プロファイルと同じです。

ダイナミック エンドポイントに一致するプロファイリング ポリシーは、プロファイリング ポリシーで定義された 1 つ以上のルールを使用して特定できます。また、分類のために、必要に応じてエンドポイント ID グループを割り当てることができます。

エンドポイントが既存のポリシーにマッピングされる場合、プロファイリング サービスは、一連のポリシーが一致する最も近い親プロファイルをプロファイリング ポリシーの階層で検索し、エンドポイントを適切なエンドポイント ポリシーに割り当てます。

許可に使用するエンドポイント プロファイリング ポリシー

許可ルールにエンドポイント プロファイリング ポリシーを使用できます。このとき、エンドポイント プロファイリング ポリシーのチェックを含めるように属性として新しい条件を作成できます。属性値は、エンドポイント プロファイリング ポリシーの名前になります。エンドポイント プロファイリング ポリシーを、エンドポイント辞書から選択できます。エンドポイント プロファイリング ポリシーには、属性 PostureApplicable、EndPointPolicy、LogicalProfile および BYODRegistration が含まれています。

PostureApplicable の属性値は、オペレーティング システムに基づいて自動設定されます。この値は、IOS および Android デバイスでは *[*なし（*No*）*]* に設定されます。これらのプラットフォームでは、ポスチャを実行するための エージェントがサポートされていないためです。この値は、Mac OSX および Windows デバイスでは [はい（Yes）] に設定されます。

EndPointPolicy、BYODRegistration および ID グループの組み合わせを含む許可ルールを定義できます。

Cisco Catalyst 9800 ワイヤレス LAN コントローラからの Wi-Fi デバイス分析データ

Cisco ISE に統合されたシスコ ワイヤレス LAN コントローラからのデバイス分析データを使用して、Apple、Intel、および Samsung のエンドポイントのプロファイリングポリシー、許可条件、および認証条件と認証ポリシーを作成できます。コントローラは、デバイス分析を使用して、一連のエンドポイントからモデル番号、オペレーティングシステムのバージョン、その他の情報などのエンドポイント属性を学習します。収集したデータはその後 Cisco ISE と共有します。

Cisco ISE では、受信したデータは Wi-Fi Device Analytics という名前の新しいディクショナリに追加されます。

2 つのシステム間でデバイス属性データを交換できるようにするには、次の条件が満たされていることを確認する必要があります。

シスコ ワイヤレス LAN コントローラの場合

- ネットワークデバイスが、Cisco IOS XE 17.10.1 以降のバージョンを実行し、802.11ac Wave2 および 802.11ax（Wi-Fi 6/6E）アクセスポイントを搭載した Cisco Catalyst 9800 シリーズのワイヤレスコントローラである。
- Cisco Catalyst 9800 ワイヤレスコントローラの場合

  1. 以下が有効になるようにポリシープロファイルを設定します。
     - RADIUS Profiling
     - HTTP TLV Caching
     - DHCP TLV Caching

- Dot11-tlv-accounting（CLI を介してのみ設定）。

2. Apple iOS の分析には、PSK または 802.1X のいずれかを使用したセキュアな WLAN が必要です。
3. Samsung の分析には、WPA、WPA2、または WPA3 ポリシーを使用したセキュアな WLAN が必要です。
4. Intel の分析には、保護された管理フレーム（PMF）がオプションまたは必須に設定されたセキュアな WLAN が必要です。

- コントローラで RADIUS アカウンティングを有効にする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのデバイスの設定方法の詳細については、お使いのデバイスの設定ガイドを参照してください。

シスコワイヤレス LAN コントローラからデバイス分析データを受信するには、Cisco ISE 管理ポータルで次の手順を実行します。

1. **[管理（Administration）]**>**[システム（System）]**>**[展開（Deployment）]**>**[ノード（Node）]** を選択します。
2. ノードのホスト名をクリックします。
3. [ノードの編集（Edit Node）] ウィンドウの [プロファイリング設定（Profiling Configuration）] タブで、**RADIUS** オプションが有効になっていることを確認します。
4. **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** の順に選択します。必要な Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのデバイスが Cisco ISE と統合されていることを確認します。これらのデバイスを Cisco ISE に追加する方法については、Cisco ISE でのネットワークデバイスの追加 （648 ページ） を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのデバイスと Cisco ISE が 2 つのシステム間でデバイス属性を共有できるように設定すると、**[コンテキストの可視性 > エンドポイント（Context Visibility Endpoints）]** ウィンドウでデバイス属性を表示できます。 エンドポイントの MAC アドレスをクリックすると、詳細には名前が DEVICE_INFO_< 属性名 > の形式の新しい属性が示されます。

シスコワイヤレス LAN コントローラでは、次の 7 つのデバイス情報属性を使用できます。

- モデル番号
- ファームウェアバージョン
- OS のバージョン
- 製造業者名
- モデル名

- ハードウェア モデル
- ベンダータイプ

エンドポイント プロファイリング ポリシーの論理プロファイルによるグループ化

論理プロファイルは、エンドポイント プロファイリング ポリシーがシスコ提供か、管理者作成かに関係なく、プロファイルまたは関連付けられているプロファイルのカテゴリのコンテナです。エンドポイント プロファイリング ポリシーは、複数の論理プロファイルに関連付けることができます。

許可ポリシー条件で論理プロファイルを使用して、プロファイルのカテゴリでネットワーク全体のアクセス ポリシーの作成に役立てることができます。許可の単純条件を作成して、許可ルールに含めることができます。許可条件で使用できる属性と値のペアは、論理プロファイル（属性）および論理プロファイルの名前（値）であり、エンドポイント システム ディクショナリ内にあります。

たとえば、カテゴリに一致するエンドポイント プロファイリング ポリシーを論理プロファイルに割り当てることによって、Android、Apple iPhone、Blackberry などのすべてのモバイル デバイスの論理プロファイルを作成できます。Cisco ISE には、すべての IP フォンのデフォルトの論理プロファイルである IP-Phone が含まれ、IP-Phone には、IP-Phone、Cisco IP-Phone、Nortel-IP-Phone-2000-Series、および Avaya-IP-Phone プロファイルが含まれます。

論理プロファイルの作成

エンドポイント プロファイリング ポリシーのカテゴリをグループ化するために使用できる論理プロファイルを作成でき、それにより、プロファイルまたは関連付けられているプロファイルのカテゴリ全体を作成できます。エンドポイント プロファイリング ポリシーを割り当てられたセットから削除して、使用可能なセットに戻すこともできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[プロファイリング（Profiling）]** > **[論理プロファイル（Logical Profiles）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] のテキスト ボックスに新しい論理プロファイルの名前と説明を入力します。

ステップ 4 [使用可能なポリシー（Available Policies）] からエンドポイント プロファイリング ポリシーを選択して、論理プロファイルに割り当てます。

ステップ 5 右矢印をクリックして、選択したエンドポイント プロファイリング ポリシーを [割り当てられたポリシー（Assigned Policies）] に移動します。

ステップ 6 [Submit] をクリックします。

プロファイリング例外アクション

例外アクションは、エンドポイント プロファイリング ポリシーで参照できる単一の設定可能なアクションであり、アクションに関連付けられている例外条件が満たされるとトリガーされます。

例外アクションのタイプは次のいずれかになります。

- シスコ提供：シスコ提供の例外アクションは削除できません。Cisco ISE では、Cisco ISE のエンドポイントをプロファイリングするときに、次の編集不能なプロファイリング例外アクションがトリガーされます。
  - 許可変更：エンドポイントが許可ポリシーで使用されるエンドポイント ID グループに対して追加または削除される場合、プロファイリング サービスは許可変更を発行します。
  - エンドポイント削除：エンドポイントが [エンドポイント（Endpoints）] ページでシステムから削除されるか、Cisco ISE ネットワーク上で編集ページから不明プロファイルに再割り当てされると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。
  - FirstTimeProfiled：エンドポイントが Cisco ISE で初めてプロファイリングされ、そのエンドポイントのプロファイルが不明プロファイルから既存のプロファイルに変更されて、そのエンドポイントが Cisco ISE ネットワーク上で認証に失敗すると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。
- 管理者作成：Cisco ISE では、作成したプロファイリング例外アクションがトリガーされます。

例外アクションの作成

1 つ以上の例外ルールを定義し、1 つのプロファイリング ポリシーに関連付けることができます。この関連付けにより、Cisco ISE でエンドポイントをプロファイリングする際にプロファイリング ポリシーが一致し、少なくとも 1 つの例外ルールが一致する場合、例外アクション（単一の設定可能なアクション）がトリガーされます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[プロファイリング（Profiling）]** > **[例外アクション（Exception Actions）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ3 [名前（Name）] と [説明（Description）] のテキスト ボックスに例外アクションの名前と説明を入力します。

ステップ4 [CoA アクション（CoA Action）] チェックボックスをオンにします。

ステップ5 [ポリシー割り当て（Policy Assignment）] ドロップダウン リストをクリックしてエンドポイント ポリシーを選択します。

ステップ6 [Submit] をクリックします。

ポリシーおよびIDグループのスタティック割り当てによるエンドポイントの作成

[エンドポイント（Endpoints）] ページでエンドポイントの MAC アドレスを使用して、新しいエンドポイントを静的に作成できます。また、スタティック割り当ての [エンドポイント（Endpoints）] ページで、エンドポイント プロファイリング ポリシーおよび ID グループを選択できます。

通常のモバイルデバイス（MDM）エンドポイントは、[エンドポイントID（Endpoints Identities）] リストに表示されます。リストページには、[ホスト名（Hostname）]、[デバイスタイプ（Device Type）]、[デバイス ID（Device ID）] など、MDM エンドポイントの属性のカラムが表示されます。[スタティック割り当て（Static Assignment）]、[スタティック グループ割り当て（Static Group Assignment）] などのその他のカラムは、デフォルトでは表示されません。

（注） このページを使用して、MDM エンドポイントを追加、編集、削除、インポートまたはエクスポートすることはできません。

ステップ1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

ステップ2 [追加（Add）] をクリックします。

ステップ3 エンドポイントの MAC アドレスをコロンで区切られた 16 進表記で入力します。

ステップ4 [ポリシー割り当て（Policy Assignment）] ドロップダウン リストから一致するエンドポイント ポリシーを選択して、スタティック割り当てステータスをダイナミックからスタティックに変更します。

ステップ5 [スタティック割り当て（Static Assignment）] チェックボックスをオンにして、エンドポイントに割り当てられたスタティック割り当てのステータスをダイナミックからスタティックに変更します。

ステップ6 [ID グループ割り当て（Identity Group Assignment）] ドロップダウン リストから、新しく作成されたエンドポイントを割り当てるエンドポイント ID グループを選択します。

ステップ7 エンドポイントID グループのダイナミック割り当てをスタティックに変更するには、[スタティック グループ割り当て（Static Group Assignment）] チェックボックスをオンにします。

ステップ 8 [送信（Submit）] をクリックします。

CSV ファイルを使用したエンドポイントのインポート

Cisco ISE テンプレートから作成した CSV ファイルからエンドポイントをインポートし、エンドポイントの詳細を使用して更新することができます。Cisco ISE からエクスポートされたエンドポイントには約 90 個の属性が含まれているため、別の ISE 展開に直接インポートすることはできません。インポートが許可されていない列が CSV ファイルにある場合は、インポートできない属性のリストを含むメッセージが表示されます。ファイルを再度インポートする前に、指定された列を削除する必要があります。

CSV ファイルを変更せずに Cisco ISE にインポートできる属性のみをエクスポートする場合は、[エンドポイントのエクスポート（Export Endpoints）] ダイアログボックスで、[インポート可能のみ（Importable Only）] チェックボックスをオンにします。このオプションを使用すると、Cisco ISE にインポートする前に、エクスポートされた CSV ファイルの列またはメタデータを変更する必要がなくなります。

インポートできる属性は約 31 個あります。このリストには、MACAddress、EndPointPolicy、IdentityGroup が含まれています。オプション属性は次のとおりです。

説明	PortalUser	LastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	Device Type	host-name
PortalUser.GuestStatus	StaticAssignment	Location
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<custom attribute name>	—	—

ファイル ヘッダーは、デフォルトのインポート テンプレートで指定されている形式にして、エンドポイントのリストが次の順序で表示されるようにする必要があります。MACAddress、EndpointPolicy、IdentityGroup、<オプション属性として上に記載されている属性のリスト>。次のファイル テンプレートを作成できます。

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup

- MACAddress, EndPointPolicy, IdentityGroup, <オプション属性として上に記載されている属性のリスト>

MAC アドレスを除くすべての属性値は、CSV ファイルからエンドポイントをインポートする際に省略可能です。特定の値のないエンドポイントをインポートする場合も、値はカンマで区切られます。次の例を参考にしてください。

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser, など

CSV ファイルを使用してエンドポイントをインポートするには、次の手順を実行します。

ステップ 1 **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** の順に選択します。

ステップ 2 [ファイルからインポート（Import from File）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、作成済みの CSV ファイルを見つけます。

ステップ 4 [送信（Submit）] をクリックします。

エンドポイントのカスタム属性をインポートするには、正しいデータタイプを使用して **[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[設定（Settings）]** > **[エンドポイントカスタム属性（Endpoint Custom Attributes）]** ウィンドウで CSV ファイルと同じカスタム属性を作成する必要があります。それらの属性には、CUSTOM というプレフィックスを付けてエンドポイント属性と区別する必要があります。

エンドポイントで使用可能なデフォルトのインポート テンプレート

エンドポイントのインポートに使用できるエンドポイントを更新できるテンプレートを生成できます。デフォルトで、[テンプレートの生成（Generate a Template）] リンクを使用して、Microsoft Office Excel アプリケーションで CSV ファイルを作成し、このファイルをシステム上にローカルに保存できます。ファイルは **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** > **[ファイルからインポート（Import from File）]** にあります。[テンプレートの生成（Generate a Template）] リンクを使用してテンプレートを作成でき、Cisco ISE サーバーは、[template.csv を開く（Opening template.csv）] ダイアログを表示します。このダイアログを使用すると、デフォルトの template.csv ファイルを開いたり、template.csv ファイルをシステム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルは Microsoft Office Excel アプリケーションで開かれます。デフォルトの template.csv ファイルには、MAC アドレス、エンドポイント ポリシー、エンドポイント ID グループ、およびその他のオプション属性が表示されるヘッダー行が含まれています。

エンドポイントの MAC アドレス、エンドポイント プロファイリング ポリシー、エンドポイント ID グループを、インポートするオプションの属性値とともに更新し、新しいファイル名を使用してファイルを保存します。このファイルをエンドポイントのインポートのために使用できます。[テンプレートの生成（Generate a Template）] リンクを使用したときに作成される template.csv ファイルのヘッダー行を参照してください。

表 *111 : CSV* テンプレート ファイル

MAC	EndPointPolicy	IdentityGroup	その他のオプションの属性
11:11:11:11:11:11	Android	プロファイル済み	<Empty>/<Value>

インポート中の不明なエンドポイントの再プロファイリング

インポートに使用するファイルに、MAC アドレスを持つエンドポイントがあり、それらに割り当てられているエンドポイントプロファイリングポリシーが不明プロファイルである場合、これらのエンドポイントはインポート中に Cisco ISE でただちに一致するエンドポイント プロファイリングポリシーに再プロファイリングされます。ただし、不明プロファイルに静的に割り当てられることはありません。エンドポイントに割り当てられているエンドポイント プロファイリング ポリシーが CSV ファイルにない場合、これらのエンドポイントは不明プロファイルに割り当てられ、一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。次に、Cisco ISE が、インポート中に Xerox_Device プロファイルに一致する不明プロファイルをどのように再プロファイリングするか、および割り当てられていないエンドポイントをどのように再プロファイリングするかを示します。

表 *112 :* 不明プロファイル：ファイルからのインポート

MAC アドレス	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:02	不明	Xerox-Device
00:00:00:00:01:03	不明	Xerox-Device
00:00:00:00:01:04	不明	Xerox-Device
00:00:00:00:01:05	プロファイルがエンドポイントに割り当てられていない場合、そのエンドポイントは不明プロファイルに割り当てられ、一致するプロファイルに再プロファイリングされます。	Xerox-Device

インポートされない無効な属性を持つエンドポイント

CSV ファイルに存在するエンドポイントのいずれかに無効な属性がある場合、エンドポイントはインポートされず、エラー メッセージが表示されます。

たとえば、エンドポイントがインポートに使用されるファイル内で無効なプロファイルに割り当てられている場合、それらのエンドポイントは、Cisco ISE には一致するプロファイルがないためインポートされません。エンドポイントが CSV ファイル内の無効なプロファイルに割り当てられている場合、それらのエンドポイントがインポートされない仕組みを下に示します。

表 *113 :* 無効なプロファイル：ファイルからのインポート

MAC アドレス	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:02	不明	Xerox-Device
00:00:00:00:01:05	00:00:00:00:01:05 などのエンドポイントが Cisco ISE 使用可能なプロファイル以外の無効なプロファイルに割り当てられている場合、Cisco ISE では、ポリシー名が無効で、エンドポイントがインポートされないことを示す警告メッセージが表示されます。	エンドポイントは、Cisco ISE 内に一致するプロファイルがないためインポートされません。

LDAP サーバーからのエンドポイントのインポート

エンドポイントの MAC アドレス、関連するプロファイル、およびエンドポイント ID グループを LDAP サーバーからセキュアにインポートできます。

始める前に

エンドポイントをインポートする前に、LDAP サーバーがインストールされていることを確認します。

LDAP サーバーからインポートするには、接続設定値およびクエリー設定値を設定する必要があります。接続設定値またはクエリー設定値が Cisco ISE で間違って設定されていると、「LDAP インポートが失敗：（LDAP import failed:）」エラー メッセージが表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [インポート（Import）] > [LDAP からのインポート（Import From LDAP）]** の順に選択します。

ステップ 2 接続設定の値を入力します。

ステップ 3 クエリ設定の値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

CSV ファイルを使用したエンドポイントのエクスポート

CSV ファイルを使用して、すべてのエンドポイントまたは選択したエンドポイントのみをエクスポートできます。エンドポイントは MAC アドレス、エンドポイント プロファイリング ポリシー、およびエンドポイント ID グループと、約 90 属性とともに一覧表示されます。カスタム属性は、CSV ファイルにもエクスポートされ、CUSTOM というプレフィクスが付けられて、他のエンドポイント属性と区別されます。

（注） 1 つの展開からエクスポートされたエンドポイントのカスタム属性を別の展開にインポートするには、**[管理（Administration）] > [ID 管理（Identity Management）] > [設定（Settings）] > [エンドポイントカスタム属性（Endpoint Custom Attributes）]** ウィンドウで同じカスタム属性を作成し、元の展開で指定したのと同じデータタイプを使用する必要があります。

CSV ファイルを使用してエンドポイントをエクスポートするには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]** を選択します。

ステップ 2 [エクスポート（Export）] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [すべてエクスポート（Export All）] : [エンドポイント（Endpoints）] ウィンドウにリストされているすべてのエンドポイントをエクスポートするには、このオプションを選択します。
- [選択済みのエクスポート（Export Selected）] : 選択したエンドポイントのみをエクスポートするには、このオプションを選択します。
- [フィルタ済みのエクスポート（Export Filtered）] : フィルタ済みのエンドポイントのみをエクスポートするには、[クイックフィルタ（Quick Filter）] オプションまたは [高度なフィルタ（Advanced Filter）] オプションを使用しているときにこのオプションを選択します。

ステップ 3 CSV ファイルを変更せずに Cisco ISE にインポートできる属性のみをエクスポートする場合は、[エンドポイントのエクスポート（Export Endpoints）] ダイアログボックスで、[インポート可能のみ（Importable Only）] チェックボックスをオンにします。このオプションを使用すると、Cisco ISE にインポートする前に、エクスポートされた CSV ファイルの列またはメタデータを変更する必要がなくなります。

ステップ 4 [OK] をクリックして CSV ファイルを保存します。

エクスポートされたスプレッドシート内の属性のほとんどはシンプルなものです。属性の説明は次のとおりです。

- *UpdateTime*：エンドポイント属性の変更により、プロファイラがエンドポイントを最後に更新した時間。エンドポイント セッションの開始以降、更新がない場合、値は 0 です。更新中、一時的に空白になります。
- *InactivityTime*：エンドポイントがアクティブになってからの時間。

識別されたエンドポイント

Cisco ISE では、ネットワークに接続してネットワーク リソースを使用する識別されたエンドポイントが、[エンドポイント（Endpoints）] ウィンドウに表示されます。エンドポイントは、通常、有線および無線のネットワーク アクセス デバイスと VPN を介してネットワークに接続するネットワーク対応デバイスです。エンドポイントとして、パーソナル コンピュータ、ラップトップ、IP Phone、スマートフォン、ゲーム コンソール、プリンタ、ファクス機などがあります。

16 進数形式で表したエンドポイントの MAC アドレスは、常にエンドポイントの一意の表現ですが、それらに関連付けられた属性と値のさまざまなセット（属性と値のペアと呼ばれる）でエンドポイントを識別することもできます。エンドポイントの属性のさまざまなセットは、エンドポイント機能、ネットワーク アクセス デバイスの機能と設定、およびこれらの属性の収集に使用する方法（プローブ）に基づいて収集できます。

動的にプロファイリングされるエンドポイント

エンドポイントは、ネットワークで検出されると、設定されているプロファイリング エンドポイントのプロファイリング ポリシーに基づいて動的にプロファイリングされ、プロファイルに応じて一致するエンドポイント ID グループに割り当てられます。

静的にプロファイリングされるエンドポイント

MAC アドレスを使用してエンドポイントを作成し、Cisco ISE のエンドポイント ID グループとともにプロファイルをそのエンドポイントに割り当てると、エンドポイントを静的にプロファイリングすることができます。Cisco ISE では、静的に割り当てられたエンドポイントに対して、プロファイリング ポリシーおよび ID グループを再割り当てしません。

不明なエンドポイント

エンドポイントに対して一致するプロファイリング ポリシーがない場合、不明なプロファイリング ポリシー（「不明」）を割り当てることで、エンドポイントを不明としてプロファイリングできます。不明なエンドポイント ポリシーにプロファイリングされたエンドポイントの場合、そのエンドポイントに対して収集された属性または属性セットを使用してプロファイルを

作成する必要があります。いずれのプロファイルにも一致しないエンドポイントは、不明なエンドポイント ID グループにグループ化されます。

識別されたエンドポイントの、ポリシー サービス ノード データベースへのローカル保存

Cisco ISE は識別されたエンドポイントをポリシー サービス ノードのデータベースにローカルに書き込みます。エンドポイントをデータベースにローカル保存した後は、それらのエンドポイントは、重要な属性がエンドポイントで変更され、他のポリシーサービス ノードデータベースに複製されているときにのみ、管理ノードデータベースで使用できる（リモート書き込み）ようになります。重要な属性とは、Cisco ISE システムによって使用される属性またはエンドポイント プロファイリング ポリシーやルールで明確に使用される属性です。

重要な属性は次のとおりです。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

Cisco ISE でエンドポイント プロファイル定義を変更した場合、すべてのエンドポイントを再プロファイリングする必要があります。エンドポイント属性を収集するポリシーサービス ノードが、これらのエンドポイントの再プロファイリングを担当します。

あるポリシー サービス ノードが、最初は別のポリシー サービス ノードによって属性が収集されていたエンドポイントに関する属性を収集し始めると、エンドポイントの所有権が現在のポリシー サービス ノードに移ります。新しいポリシー サービス ノードは、前のポリシー サービス ノードから最新の属性を取得して、すでに収集されている属性と調整します。

重要な属性がエンドポイントで変更されると、エンドポイントの属性は管理ノードデータベースに自動的に保存され、エンドポイントの最新の重要な変更を使用できます。エンドポイントを所有するポリシー サービス ノードが何らかの理由で使用できない場合、管理 ISE ノードが所有者を失ったエンドポイントを再プロファイリングします。また、このようなエンドポイントに対して新しいポリシー サービス ノードを設定する必要があります。

クラスタのポリシー サービス ノード

Cisco ISE では、ポリシー サービス ノード グループをクラスタとして使用するため、クラスタ内の複数のノードが同じエンドポイントの属性を収集するときに、エンドポイント属性を交換できます。1 つのロード バランサの背後に存在する、すべてのポリシー サービス ノードに対するクラスタを作成することを推奨します。

現在のオーナー以外の別のノードが同じエンドポイントの属性を受信した場合、属性をマージし、所有権の変更が必要かどうかを決定するために、現在のオーナーから最新の属性を要求するメッセージをクラスタ全体に送信します。Cisco ISE でノード グループを定義していない場合は、すべてのノードが 1 つのクラスタ内にあると想定されます。

Cisco ISE でエンドポイントの作成と複製への変更は行われません。エンドポイントの所有権の変更のみが、プロファイリングに使用される、静的属性と動的属性で構成される属性の許可されたリストに基づいて決定されます。

次のいずれかの属性が変更された場合、後続の属性の収集時に、エンドポイントは管理ノードで更新されます。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

エンドポイントが管理ノードで編集および保存されている場合、この属性はエンドポイントの現在のオーナーから取得されます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイントIDグループ（Endpoint Identity Groups）] ウィンドウでは、追加のエンドポイント ID グループも作成できます。作成したエンドポイント ID グループを編集または削除できます。システムで定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集または削除することはできません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するエンドポイント ID グループの [名前（Name）] に入力します（エンドポイント ID グループの名前にはスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの [説明（Description）] に入力します。

ステップ 5 [親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

識別されたエンドポイントの、エンドポイントIDグループでのグループ化

Cisco ISE では、エンドポイント プロファイリング ポリシーに基づいて、検出されたエンドポイントを対応するエンドポイント ID グループにグループ化します。プロファイリング ポリシーは階層構造になっており、Cisco ISE のエンドポイント ID グループ レベルで適用されます。エンドポイントをエンドポイント ID グループにグループ化し、プロファイリング ポリシーをエンドポイント ID グループに適用すると、Cisco ISE により、対応するエンドポイント プロファイリング ポリシーを確認してエンドポイント プロファイルへのエンドポイントのマッピングを決定できます。

Cisco ISE によってエンドポイント ID グループのセットがデフォルトで作成され、これを使用して、エンドポイントを動的または静的に割り当てできる独自の ID グループを作成できます。エンドポイント ID グループを作成し、システムが作成した ID グループの 1 つにその ID グループを関連付けることができます。また、自分が作成したエンドポイントをシステム内のいずれかの ID グループに静的に割り当てることができ、ID グループがプロファイリング サービスで再割り当てされることはありません。

エンドポイントに対して作成されるデフォルトのエンドポイントIDグループ

Cisco ISE は次のエンドポイント ID グループを作成します。

- [ブロックリスト（Blocked List）]：このエンドポイント ID グループには、Cisco ISE でこのグループに静的に割り当てられたエンドポイント、およびデバイス登録ポータルでブロックされたエンドポイントが含まれます。許可プロファイルを Cisco ISE で定義して、このグループのエンドポイントへのネットワーク アクセスを許可または拒否できます。
- [GuestEndpoints]：このエンドポイント ID グループには、ゲストユーザーが使用するエンドポイントが含まれます。

- [プロファイル済み（Profiled）]：このエンドポイント ID グループには、Cisco ISE の Cisco IP 電話およびワークステーションを除くエンドポイント プロファイリング ポリシーに一致するエンドポイントが含まれます。
- [RegisteredDevices]：このエンドポイント ID グループには、デバイス登録ポータルを介して従業員が追加した登録済みデバイスであるエンドポイントが含まれます。プロファイリング サービスは通常、これらのデバイスがこのグループに割り当てられている場合、これらのデバイスを引き続きプロファイリングします。エンドポイントは Cisco ISE のこのグループに静的に割り当てられ、プロファイリング サービスがこれらのエンドポイントを他の ID グループに割り当てることはできません。これらのデバイスは、エンドポイント リストの他のエンドポイントと同様に表示されます。デバイス登録ポータルを介して追加されたこれらのデバイスは、Cisco ISE の [エンドポイント（Endpoints）] ウィンドウのエンドポイントリストで編集、削除、およびブロックできます。デバイス登録ポータルでブロックされているデバイスは、[ブロックリスト（Blocked List）]エンドポイント ID グループに割り当てられ、Cisco ISE に存在する認証プロファイルは、ブロックされたデバイスを URL（「無許可ネットワークアクセス」と表示される、ブロックされたデバイスのデフォルトポータルページ）にリダイレクトします。
- 不明：このエンドポイント ID グループには、Cisco ISE のプロファイルに一致しないエンドポイントが含まれます。

上記のシステムで作成されたエンドポイント ID グループに加えて、Cisco ISE ではプロファイル済み（親）ID グループに関連付けられる次のエンドポイント ID グループが作成されます。親グループは、システムに存在するデフォルトの ID グループです。

- [Cisco-IP-Phone]：ネットワーク上のすべてのプロファイル済み Cisco IP 電話 が含まれる ID グループです。
- [ワークステーション（Workstation）]：ネットワーク上のすべてのプロファイル済みワークステーションが含まれる ID グループです。

一致するエンドポイント プロファイリング ポリシーに対して作成されるエンドポイント ID グループ

既存のポリシーと一致するエンドポイント ポリシーがある場合、プロファイリング サービスは一致するエンドポイント ID グループを作成できます。この ID グループは、プロファイル済みエンドポイント ID グループの子になります。エンドポイント ポリシーを作成する場合、[プロファリング ポリシー（Profiling Policies）] ページの [一致する ID グループの作成（Create Matching Identity Group）] チェックボックスをオンにして、一致するエンドポイント ID グループを作成できます。プロファイルのマッピングが削除されない限り、一致する ID グループは削除できません。

エンドポイント ID グループでの静的なエンドポイントの追加

エンドポイント ID グループの静的に追加されたエンドポイントを追加または削除できます。

[エンドポイント（Endpoints）] ウィジェットのエンドポイントのみを特定の ID グループに追加できます。エンドポイントを特定のエンドポイント ID グループに追加した場合、そのエンドポイントは、前に動的にグループ化されたエンドポイント ID グループから移動されます。

エンドポイントを最近追加したエンドポイント ID グループから削除すると、そのエンドポイントは、適切な ID グループに再プロファイリングされます。エンドポイントは、システムから削除されませんが、エンドポイントの ID グループからのみ削除されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 エンドポイント ID グループを選択して [編集（Edit）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [エンドポイント（Endpoints）] ウィジェットでエンドポイントを選択して、選択したエンドポイントをエンドポイント ID グループに追加します。

ステップ 5 [エンドポイント グループ リスト（Endpoint Group List）] リンクをクリックして、[エンドポイント ID グループ（Endpoint Identity Groups）] ページに戻ります。

ダイナミックエンドポイントの、IDグループへの追加または削除後の再プロファイリング

エンドポイント ID グループが静的に割り当てられていない場合、エンドポイント ID グループに追加した、またはエンドポイント ID グループから削除したエンドポイントは、再プロファイリングされます。ISE プロファイラにより動的に識別されたエンドポイントは、適切なエンドポイント ID グループに表示されます。動的に追加されたエンドポイントをエンドポイント ID グループから削除した場合、Cisco ISE では、エンドポイント ID グループからエンドポイントを正常に削除したが、それらのエンドポイントをエンドポイント ID グループに再プロファイリングして戻すことを示すメッセージが表示されます。

許可ルールで使用されるエンドポイント ID グループ

エンドポイント ID グループを許可ポリシーで効率的に使用して、検出されたエンドポイントに適切なネットワーク アクセス権限を付与することができます。たとえば、すべてのタイプの Cisco IP Phone 用の許可ルールが、デフォルトで、Cisco ISE の **[ポリシー セット（Policy Sets）] > [デフォルト（Default）] > [許可ポリシー（Authorization Policy）]** で使用できます。

エンドポイント プロファイリング ポリシーがスタンドアロン ポリシー（他のエンドポイント プロファイリング ポリシーの親でない）であるか、またはエンドポイント プロファイリング ポリシーの親ポリシーが無効でないことを確認する必要があります。

エニーキャストおよびプロファイラサービス

エニーキャストは、同じ IP アドレスが 2 つ以上のホストに割り当てられ、データを受信する最適なターゲットを決定するためにルーティングが許可されるネットワーキング技術です。データをプロファイリングする単一のターゲット（RADIUS、DHCP リレー、SNMP トラップ、および NetFlow）を提供するロードバランサの使用例と同様に、エニーキャストでは、複数の宛先に同じデータを送信しないように、単一の IP ターゲットで送信元を設定できます。

エニーキャスト IP アドレスを実際の PSN インターフェイス IP アドレスまたはロードバランサの仮想 IP アドレスに割り当てて、データセンター間の冗長性をサポートできます。エニーキャスト IP アドレスを ISE ギガビットイーサネット 0 管理インターフェイスに割り当てないでください。

エニーキャストに使用されるインターフェイスは、プロファイラプローブで使用される専用インターフェイスである必要があります。エニーキャスト IP アドレスがロードバランサの仮想 IP アドレスに割り当てられている場合、同じ要件は適用されません。

エニーキャストを使用する場合、ノード障害が自動的に検出され、障害が発生したノードまでの該当するルートがルーティングテーブルから削除されることが不可欠です。エニーキャストのターゲットがリンクまたは VLAN の唯一のホストの場合、障害が発生するとルートを自動的に削除できます。

IP エニーキャストを展開する場合、各ターゲットまでのルートメトリックに有意な重み付けやバイアスを確実に持たせることがきわめて重要になります。エニーキャストターゲットまでのルートがフラッピングする場合や、結果的に等コストマルチパス（ECMP）ルーティングのシナリオになる場合、所定のサービス（RADIUS AAA、DHCP または SNMP トラッププロファイリング、HTTPS ポータル）に関するトラフィックが各ターゲットに分散されることがあります。その場合、過剰なトラフィックやサービスの障害が発生したり（RADIUS AAA および HTTPS ポータル）、最適とは言えないプロファイリングやデータベース レプリケーションになります（プロファイリングサービス）。

IP エニーキャストの主要な利点は、アクセス デバイス、プロファイル データ ソース、DNS の設定が大幅に簡単になることです。また、特定のエンドポイントに関するデータのみ単一の PSN に送信されることが保証されるため、ISE プロファイリングが最適化されます。追加のルート設定を慎重に計画し、適切なモニタリングによって管理する必要があります。ただし、明確なサブネットワークおよび IP アドレスが使用されないため、トラブルシューティングも困難になります。

プロファイラ フィード サービス

プロファイラ条件、例外アクション、および NMAP スキャン アクションは、シスコ提供または管理者作成として分類され、システム タイプ属性に表示されます。エンドポイント プロファイリング ポリシーは、シスコ提供、管理者作成、または管理者による変更として分類されます。これらの分類は、システム タイプ属性に表示されます。

システム タイプ属性によって、プロファイラ条件、例外アクション、NMAP スキャン アクション、およびエンドポイント プロファイリング ポリシーに対して異なる操作を実行できます。シスコ提供の条件、例外アクション、NMAP スキャン アクションは編集または削除できません。シスコが提供するエンドポイント ポリシーは削除できません。ポリシーを編集すると、管理者による変更と見なされます。フィード サービスによってポリシーが更新されると、管理者によって変更されたポリシーは、それが基づいていたシスコ提供ポリシーの最新のバージョンに置き換えられます。

新規および更新されたエンドポイント プロファイリング ポリシーと更新された OUI データベースは、Cisco フィード サーバーから取得できます。Cisco ISE へのサブスクリプションが必要です。また、適用、成功、および失敗のメッセージに関する電子メール通知を受信することもできます。シスコによるフィード サービスの改善のため、フィード サービス アクションに関する匿名の情報をシスコに返信することができます。

OUI データベースには、ベンダーに割り当てられた MAC OUI が含まれています。OUI リストは、次の URL から入手できます。 http://standards.ieee.org/develop/regauth/oui/oui.txt

Cisco ISE は毎日ローカル Cisco ISE サーバーのタイム ゾーンの午前 1:00 にポリシーと OUI データベースの更新をダウンロードします。Cisco ISE は、これらのダウンロードされたフィード サーバー ポリシーを自動的に適用し、また、以前の状態に復元できるように変更内容を保存します。以前の状態に復元すると、新しいエンドポイント プロファイリング ポリシーは削除され、更新されたエンドポイント プロファイリング ポリシーは以前の状態に復元されます。さらに、プロファイラ フィード サービスは自動的に無効になります。

また、オフライン モードで手動でフィード サービスを更新することもできます。ISE 展開をシスコ フィード サービスに接続できない場合には、このオプションを使用して更新プログラムを手動でダウンロードすることができます。

（注） 60 日間のうち、ライセンスがコンプライアンス外（OOC）となっている日数が 45 日間に達すると、フィード サービスからの更新が許可されなくなります。ライセンスがコンプライアンス外になるのは、ライセンスの有効期限が切れるか、または使用が許可されているセッション数を超えた時点です。

プロファイラ フィード サービスの設定

プロファイラ フィード サービスは、Cisco フィード サーバーから新規および更新されたエンドポイント プロファイリング ポリシーと MAC OUI データベース更新を取得します。フィード サービスが使用できない場合、またはその他のエラーが発生した場合は、操作監査レポートで報告されます。

匿名のフィード サービス使用レポートをシスコに返信するように Cisco ISE を設定できます。そのレポートでは、次の情報がシスコに送信されます。

- Hostname：Cisco ISE のホスト名
- MaxCount：エンドポイントの合計数

- ProfiledCount：プロファイリングされたエンドポイントの数
- UnknownCount：不明なエンドポイントの数
- MatchSystemProfilesCount：シスコ提供のプロファイルの数
- UserCreatedProfiles：ユーザーが作成したプロファイルの数

シスコから提供されるプロファイリング ポリシーの CoA タイプを変更できます。フィード サービスがそのポリシーを更新すると、CoA タイプは変更されませんが、そのポリシーの残りの属性は引き続き更新されます。

Cisco ISE リリース 2.7 以降では、ポリシー更新をダウンロードせずに OUI 更新を手動でダウンロードできます。一部のプロファイラ条件をカスタマイズして CoA タイプ以外も変更している場合は、プロファイラ フィードによってそれらの条件が置き換えられることが望ましくない場合があります。それでも OUI の更新は必要である場合のため、製造者が新しいデバイスを追加したときにはプロファイラがそれを特定できるようになっています。OUI のみをダウンロードするオプションは、フィード サービス ポータルから利用できます。

始める前に

分散展開またはスタンドアロン ISE ノードでは、Cisco ISE 管理者ポータルからのみプロファイラ フィード サービスを設定できます。

フィード更新について管理者ポータルから電子メール通知を送信する場合は、Simple Mail Transfer Protocol（SMTP）サーバーを設定します（**[管理（Administration）] > [システム（System）] > [設定（Settings）]**）。

フィード サービスをオンラインで更新するには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** の順に選択し、[QuoVadis Root CA 2] が有効になっているか確認します。

ステップ 2 **[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [フィード（Feeds）]** の順に選択します。
[管理（Administration）] > [フィードサービス（FeedService）] > [プロファイラ（Profiler）] ページでこのオプションにアクセスすることもできます。

ステップ 3 [オンライン サブスクリプションの更新（Online Subscription Update）] タブをクリックします。

ステップ 4 [フィードサービス接続のテスト（Test Feed Service Connection）] ボタンをクリックして、Cisco フィード サービスへの接続があり、証明書が有効であることを確認します。

ステップ 5 [オンライン サブスクリプション更新の有効化（Enable Online Subscription Update）] チェック ボックスをオンにします。

ステップ 6 HH:MM 形式で時刻（Cisco ISE サーバーのローカル タイム ゾーン）を入力します。デフォルトでは、Cisco ISE フィード サービスは毎日午前 1 時にスケジュールされます。

ステップ 7 [ダウンロードが行われたら管理者に通知（Notify administrator when download occurs）] チェック ボックスをオンにして、[管理者の電子メール アドレス（Administrator email address）] テキスト ボックスに電子メール アドレスを入力します。Cisco ISE が非機密情報（今後のリリースでよりよいサービスと追加機能を提供するために使用される）を収集することを許可する場合、[プロファイリング精度を上げるために Cisco 匿

名情報を提供する（Provide Cisco anonymous information to help improve profiling accuracy）] チェック ボックスをオンにします。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 [今すぐ更新（Update Now）] をクリックします。

最後のフィード サービス更新以降に作成された新規および更新されたプロファイルをチェックするために Cisco フィード サーバーに連絡するように Cisco ISE に指示します。これによりシステム内のすべてのエンドポイントが再プロファイリングされ、システム負荷が増加する可能性があります。エンドポイント プロファイリング ポリシーの更新のため、現在 Cisco ISE に接続している一部のエンドポイントの許可ポリシーが変更される場合があります。

最後のフィード サービス以降に作成された新規および更新されたプロファイルを更新すると [今すぐ更新（Update Now）] ボタンは無効になり、ダウンロードの完了後にのみ有効になります。[プロファイラ フィード サービス設定（Profiler Feed Service Configuration）] ウィンドウから別の場所に移動し、このウィンドウに戻る必要があります。

関連トピック

オフラインでのプロファイラ フィード サービスの設定 （1301 ページ）

オフラインでのプロファイラ フィード サービスの設定

Cisco ISE と Cisco フィード サーバーが直接接続されていないときに、フィード サービスをオフラインで更新できます。Cisco フィード サーバーからオフライン更新プログラム パッケージをダウンロードし、Cisco ISE にオフライン フィード更新プログラムを使用してアップロードできます。またフィード サーバーに追加される新しいポリシーに関する電子メール通知を設定することもできます。

オフラインでのプロファイラ フィード サービス設定には、次のタスクが含まれます。

1. オフライン更新プログラム パッケージのダウンロード
2. オフライン フィード更新の適用

オフライン更新プログラム パッケージのダウンロード

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[フィード（Feeds）]** の順に選択します。
[管理（Administration）] > **[フィードサービス（FeedService）]** > **[プロファイラ（Profiler）]** ページでこのオプションにアクセスすることもできます。

ステップ 2 [オフライン手動更新（Offline Manual Update）] タブをクリックします。

ステップ 3 [更新されているプロファイル ポリシーのダウンロード（Download Updated Profile Policies）] リンクをクリックします。フィード サービス パートナー ポータルにリダイレクトされます。
また、ブラウザから https://ise.cisco.com/partner/ にアクセスして、フィード サービス パートナー ポータルに直接アクセスすることもできます。

ステップ 4 初めてのユーザーは、各種条件および契約に同意します。
要求を承認するフィードサービス管理者に電子メールが送信されます。承認されると、確認用の電子メールが届きます

ステップ 5 Cisco.com のクレデンシャルを使用してパートナー ポータルにログインします。

ステップ 6 [オフライン フィード（Offline Feed）] > [パッケージのダウンロード（Download Package）] の順に選択します。

ステップ 7 [パッケージの生成（Generate Package）] をクリックします。

ステップ 8 [オフライン 更新プログラム パッケージの内容を表示するにはクリックしてください（Click to View the Offline Update Package contents）] リンクをクリックして、生成したパッケージに含まれるすべてのプロファイルと OUI を表示します。

- [フィード プロファイラ 1（Feed Profiler 1）] と [フィード OUI（Feed OUI）] の下のポリシーは Cisco ISE の全バージョンにダウンロードされます。
- [フィード プロファイラ 2（Feed Profiler 2）] の下のポリシーは Cisco ISE リリース 1.3 以降のみにダウンロードされます。
- [フィード プロファイラ 3（Feed Profiler 2）] の下のポリシーは Cisco ISE リリース 2.1 以降のみにダウンロードされます。

ステップ 9 [パッケージのダウンロード（Download Package）] をクリックして、ローカル システムにファイルを保存します。
保存したファイルを Cisco ISE サーバーにアップロードして、ダウンロードしたパッケージのフィード更新プログラムを適用できます。

オフライン フィード更新の適用

始める前に

フィード更新を適用する前に、オフライン更新プログラム パッケージをダウンロードしている必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [フィード（Feeds）]** を選択します。
[管理（Administration）] > [フィードサービス（FeedService）] > [プロファイラ（Profiler）] ウィンドウでこのオプションにアクセスすることもできます。

ステップ 2 [オフライン手動更新（Offline Manual Update）] タブをクリックします。

ステップ 3 [参照（Browse）] をクリックして、ダウンロードしたプロファイラ フィード パッケージを選択します。

ステップ 4 [更新の適用（Apply Update）] をクリックします。

プロファイルと OUI の更新に関する電子メール通知の設定

プロファイルと OUI の更新通知を受信する電子メール アドレスを設定できます。

ステップ 1 「オフライン更新プログラム パッケージのダウンロード」セクションの手順 1 ～ 5 を実行し、フィード サービス パートナー ポータルに移動します。

ステップ 2 [オフライン フィード（Offline Feed）] > [電子メール設定（Email Preferences）] を選択します。

ステップ 3 通知を受信するには、[通知の有効化（Enable Notifications）] チェック ボックスをオンにします。

ステップ 4 新しい更新通知を受信する頻度を設定するには、[日数（days）] ドロップダウン リストから日数を選択します。

ステップ 5 電子メール アドレスまたはアドレスを入力し、[保存（Save）] をクリックします。

フィード更新の取り消し

前回の更新で更新されたエンドポイント プロファイリング ポリシーに戻り、プロファイラ フィード サービスの前回の更新により新しく追加されたが、エンドポイント プロファイリング ポリシーおよび OUI を削除できます。

エンドポイント プロファイリング ポリシーは、フィード サーバーからの更新後に変更された場合、システムで変更されません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [フィード（Feeds）]** を選択します。

ステップ 2 変更設定監査レポートで設定変更を表示する場合は、[更新レポート ページに移動（Go to Update Report Page）] をクリックします。

ステップ 3 [最新を元に戻す（Undo Latest）] をクリックします。

プロファイラ レポート

Cisco ISE には、エンドポイント プロファイリングに関するさまざまなレポートと、ネットワークの管理に使用できるトラブルシューティング ツールが用意されています。現在のデータに加えて履歴のレポートを生成できます。レポートの一部をドリルダウンして詳細を表示できます。大規模なレポートの場合、レポートをスケジュールし、さまざまな形式でダウンロードすることもできます。

[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] からエンドポイントに関する次のレポートを実行できます。

- エンドポイント セッション履歴
- プロファイリングされたエンドポイントの概要

- エンドポイント プロファイルの変更
- エンドポイントによる上位承認
- 登録済みエンドポイント

エンドポイントの異常な動作の検出

Cisco ISE により、不正な MAC アドレスの使用からネットワークが保護されます。Cisco ISE は MAC アドレススプーフィングに関与しているエンドポイントを検出し、疑わしいエンドポイントの権限を制限できます。

プロファイラ設定ページには、異常な動作に関する次の 2 つのオプションがあります。

- 異常な動作の検出を有効にする（Enable Anomalous Behavior Detection）
- 異常な動作の適用を有効にする（Enable Anomalous Behavior Enforcement）

異常な動作の検出を有効にすると、Cisco ISE はデータを調査し、NAS ポート タイプ、DHCP クラス ID、およびエンドポイント ポリシーに関連する属性の変更について、既存のデータとの矛盾がないかどうかを確認します。該当する場合、**AnomalousBehavior** 属性が True に設定され、エンドポイントに追加されます。これは、[可視性のコンテキスト（Visibility Context）] ページでエンドポイントをフィルタリングおよび表示する際に役立ちます。該当する MAC アドレスの監査ログも生成されます。

異常な動作の検出を有効にすると、Cisco ISE は、既存のエンドポイントの次の属性が変更されたかどうかを検査します。

1. ポートタイプ—エンドポイントのアクセス方式が変更されたかどうかを判断します。これは、有線 Dot1x 経由で接続したものと同じ MAC アドレスがワイヤレス Dot1x にも使用されていた場合（およびその逆の場合）に適用されます。
2. DHCP クラス ID—エンドポイントのクライアントまたはベンダーのタイプが変更されたかどうかを判断します。これは、DHCP クラス ID 属性に特定の値が入力された後で別の値に変更された場合にのみ当てはまります。エンドポイントが静的 IP アドレスで構成されている場合、Cisco ISE での DHCP クラス ID 属性は空です。後で別のデバイスがこのエンドポイントの MAC アドレスをスプーフィングして DHCP を使用すると、クラス ID が空の値から特定の文字列に変更されます。これによって異常な動作の検出がトリガーされることはありません。
3. エンドポイント ポリシー—重要なプロファイル変更があったかどうかを判断します。これは、エンドポイントのプロファイルが [電話（Phone）] または [プリンタ（Printer）] から [ワークステーション（Workstation）] に変更されたときに適用されます。

[異常な動作の適用（Anomalous Behavior Enforcement）] を有効にすると、異常な動作が検出された時点で CoA が発行されます。これは、[プロファイラ設定（Profiler Configuration）] ウィンドウで設定した許可ルールに基づいて、疑わしいエンドポイントを再許可するために使用できます。

異常な動作が発生しているエンドポイントに関する許可ポリシールールの設定

異常な動作が発生しているエンドポイントに対して実行するアクションを選択するには、[許可ポリシー（Authorization Policy）] ページで対応するルールを設定します。

ステップ 1 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択します。

ステップ 2 デフォルト ポリシーに対応する [表示（View）] 列から矢印アイコン をクリックすると、[設定（Set）] ビュー画面が開き、デフォルト許可ポリシーを表示および管理できます。

ステップ 3 いずれかの行の [アクション（Actions）] 列から、歯車アイコンをクリックし、ドロップダウン リストから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して新しい認証ルールを挿入します。
[ポリシー セット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 4 [ルール名（Rule Name）] に入力します。

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性を選択します（たとえば、Endpoints.AnomalousBehaviorEqualsTrue）。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップすることもできます。

ステップ 7 [使用（Use）] をクリックして、異常な動作を伴うエンドポイントの許可ポリシー ルールを設定します。

ステップ 8 [完了（Done）] をクリックします。

異常な動作が発生しているエンドポイントの表示

次のいずれかのオプションを使用して、異常な動作が発生しているエンドポイントを表示できます。

- [ホーム（Home）] > [概要（Summary）] > [メトリック（Metrics）] から [異常な動作（Anomalous Behavior）] をクリックします。この操作により、ウィンドウ下部のペインに [異常な動作（Anomalous Behavior）] 列がある新しいタブが表示されます。
- [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [エンドポイントの分類（Endpoint Classification）] を選択します。ウィンドウ下部のペインで [異常な動作（Anomalous Behavior）] 列を表示できます。
- 次の手順で説明するように、[コンテキストの可視性（Context Visibility）] ウィンドウの [認証（Authentication）] ビューまたは [侵害されたエンドポイント（Compromised Endpoints）] ビューで新しい [異常な動作（Anomalous Behavior）] 列を作成できます。

ステップ 1 [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [認証（Authentication）] または [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [侵害されたエンドポイント（Compromised Endpoints）] を選択します。

ステップ 2 ウィンドウ下部のペインにある [設定（Settings）] アイコンをクリックし、[異常な動作（ Anomalous Behavior）] チェックボックスをオンにします。

ステップ 3 [移動（Go）] をクリックします。
[認証（Authentication）] ビューまたは [侵害されたエンドポイント（Compromised Endpoints）] ビューで [異常な動作（Anomalous Behavior）] 列を表示できます。

クライアントマシン上のエージェントのダウンロードの問題

問題

ユーザーの認証と許可の後、クライアント マシン ブラウザに「ポリシーが一致しません（no policy matched）」のエラー メッセージが表示されます。この問題は、認証のクライアント プロビジョニング フェーズ中のユーザー セッションに該当します。

考えられる原因

クライアント プロビジョニング ポリシーに必要な設定が欠落している可能性があります。

ポスチャ エージェントのダウンロードの問題

ポスチャエージェントのインストーラをダウンロードするには、次のものが必要があることに注意してください。

- エージェントを初めてクライアントマシンにインストールする場合、ユーザーはブラウザセッションでActiveXインストーラを許可する必要がありますクライアントプロビジョニング ダウンロード ページで、この情報の指定を求められます。
- クライアント マシンには、インターネット アクセスが必要です。

解像度

- クライアント プロビジョニング ポリシーが Cisco ISE に存在することを確認します。存在する場合は、ポリシー内に定義されているポリシー ID グループ、条件およびエージェントのタイプを確認します。また、すべてのデフォルト値のプロファイルも含め、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）] > > > [エージェント ポスチャ プロファイル（Agent Posture Profile）]** で設定されたエージェントプロファイルが存在するかどうかについても確認します。

- アクセス スイッチのポートをバウンスすることにより、クライアント マシンの再認証を試行します。

エンドポイント

これらのウィンドウでは、ネットワークに接続するエンドポイントを設定および管理することができます。

エンドポイント設定

次の表では、エンドポイントを作成し、エンドポイントにポリシーを割り当てるために使用できる [エンドポイント（Endpoints）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]**。

表 *114* : エンドポイント設定

フィールド名	使用上のガイドライン
MACアドレス（MAC Address）	エンドポイントを静的に作成するには、MAC アドレスを 16 進数形式で入力します。 MAC アドレスは、Cisco ISE 対応のネットワークに接続するインターフェイスのデバイス ID です。
スタティック割り当て（Static Assignment）	[エンドポイント（Endpoints）] ウィンドウでエンドポイントを静的に作成する場合このチェックボックスをオンにすると、静的割り当てのステータスが static に設定されます。 エンドポイントのスタティック割り当てのステータスを静的から動的に、または動的から静的に切り替えできます。

フィールド名	使用上のガイドライン
ポリシー割り当て（Policy Assignment）	（[スタティック割り当て（Static Assignment）] が選択されていない限り、デフォルトで無効）[ポリシー割り当て（Policy Assignment）] ドロップダウンリストから一致するエンドポイントポリシーを選択します。 次のいずれかを実行できます。 • 一致するエンドポイントポリシーを選択しないで、デフォルトのエンドポイントポリシーである不明を使用する場合、スタティック割り当てステータスはエンドポイントに対して動的に設定され、それにより、エンドポイントの動的プロファイリングが可能になります。 • [不明（Unknown）] ではなく、一致するエンドポイントポリシーを選択する場合、スタティック割り当てのステータスはそのエンドポイントに対して静的に設定され、[スタティック割り当て（Static Assignment）] チェックボックスが自動的にオンになります。
スタティックグループ割り当て（Static Group Assignment）	エンドポイントをIDグループに静的に割り当てる場合はこのチェックボックスをオンにします。 このチェックボックスをオンにした場合、プロファイリングサービスは、前に他のエンドポイントID グループに動的に割り当てられたエンドポイントの次のエンドポイント ポリシーの評価時に、そのエンドポイントID グループを変更しません。 このチェックボックスをオフにした場合、エンドポイントIDグループは、ポリシー設定に基づいてISE プロファイラにより割り当てられたダイナミック グループです。[スタティック グループ割り当て（Static Group Assignment）] オプションを選択しない場合、エンドポイントは、エンドポイント ポリシーの次回評価時に一致するID グループに自動的に割り当てられます。

フィールド名	使用上のガイドライン
IDグループ割り当て（Identity Group Assignment）	エンドポイントを割り当てるエンドポイント ID グループを選択します。 エンドポイントを静的に作成する場合、またはエンドポイントのエンドポイントポリシーの評価時に [一致する ID グループの作成（Create Matching Identity Group）] オプションを使用しない場合は、エンドポイントを ID グループに割り当てることができます。 Cisco ISE には、次のシステムによって作成された次のエンドポイント ID グループがあります。 • ブロック済みリスト • GuestEndpoints • プロファイル済み • Cisco IP-Phone • ワークステーション • RegisteredDevices • 不明

Cisco ISEによる不要な処理の回避と、潜在的なサービス拒否（DoS）攻撃からの保護のため、RADIUS認証が同じ理由で繰り返し失敗するActive Directoryユーザーエンドポイントは、一定の期間、自動的に拒否されます。

拒否されたエンドポイントのリストを表示するには、[操作（Operations）] > [レポート（Reports）] > [拒否されたエンドポイント（Rejected Endpoints）] の順に選択します。このレポートのデータは、Advantage ライセンスがインストールされている場合にのみ使用および表示可能です。

（注） 次の 2 つのエラーメッセージが表示されて RADIUS 認証に失敗した AD ユーザーエンドポイントは拒否されません。

22063 - WRONG_PASSWORD

24408 - ACTIVE_DIRECTORY_USER_WRONG_PASSWORD

関連トピック

識別されたエンドポイント （1292 ページ）
ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 （1286 ページ）

エンドポイントの LDAP からのインポートの設定

次の表では、LDAP サーバーからのエンドポイントのインポートに使用できる [LDAP からのインポート（Import from LDAP）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]**。

表 *115 :* エンドポイントの、*LDAP* からのインポートの設定

フィールド名	使用上のガイドライン
接続の設定	
ホスト（Host）	LDAP サーバーのホスト名または IP アドレスを入力します。
ポート（Port）	LDAP サーバーのポート番号を入力します。デフォルト ポート 389 を使用して LDAP サーバーからインポートするか、デフォルト ポート 636 を使用して SSL を介して LDAP サーバーからインポートできます。 （注） Cisco ISE では、任意の設定済みポート番号をサポートします。設定済みの値は、LDAP サーバー接続詳細に一致する必要があります。
セキュア接続を有効にする（Enable Secure Connection）	SSL を介して LDAP サーバーからインポートするには、[セキュア接続を有効にする（Enable Secure Connection）] チェックボックスをオンにします。
ルートCA証明書名（Root CA Certificate Name）	ドロップダウン矢印をクリックして、信頼できる CA 証明書を表示します。 ルート CA 証明書名は、LDAP サーバーに接続する場合に必要となる信頼できる CA 証明書を指します。Cisco ISE 内の CA 証明書は、追加（インポート）、編集、削除、およびエクスポートが可能です。
匿名バインド（Anonymous Bind）	[匿名バインド（Anonymous Bind）] チェックボックスをオンにするか、または slapd.conf コンフィギュレーション ファイルの LDAP 管理者クレデンシャルを入力する必要があります。
管理者DN（Admin DN）	slapd.conf コンフィギュレーション ファイルで LDAP 管理者に設定されている識別名（DN）を入力します。 管理者 DN フォーマット例：cn=Admin, dc=cisco.com, dc=com
パスワード（Password）	LDAP 管理者に設定されたパスワードを slapd.conf コンフィギュレーション ファイルに入力します。

フィールド名	使用上のガイドライン
ベースDN（Base DN）	親エントリの認定者名を入力します。 ベース DN フォーマット例：dc=cisco.com, dc=com
クエリ設定	
MACアドレス objectClass（MAC Address objectClass）	MAC アドレスのインポートに使用されるクエリフィルタ（ieee802Device など）を入力します。
MACアドレス属性名（MAC Address Attribute Name）	インポートに対して返される属性名（macAddress など）を入力します。
プロファイル属性名（Profile Attribute Name）	LDAP 属性の名前を入力します。この属性は、LDAP サーバーで定義されている各エンドポイント エントリのポリシー名を保持します。 [プロファイル属性名（Profile Attribute Name）] フィールドを設定する場合は、次の点を考慮してください。 • [プロファイル属性名（Profile Attribute Name）] フィールドでこの LDAP 属性を指定しない場合、またはこの属性を誤って設定した場合、インポート操作時にエンドポイントは [不明（Unknown）] としてマークされ、これらのエンドポイントは一致するエンドポイント プロファイリング ポリシーに個別にプロファイリングされます。 • [プロファイル属性名（Profile Attribute Name）] フィールドで LDAP 属性を設定した場合、その属性値は、エンドポイント ポリシーが Cisco ISE 内の既存のポリシーに一致することを確認するために検証され、エンドポイントがインポートされます。エンドポイント ポリシーが既存のポリシーと一致しない場合、それらのエンドポイントはインポートされません。
タイムアウト（Time Out）	時間は秒数で入力します。有効な範囲は 1 ～ 60 秒です。

関連トピック

識別されたエンドポイント （1292 ページ）
LDAP サーバーからのエンドポイントのインポート （1290 ページ）

エンドポイント プロファイリング ポリシーの設定

次の表では、[エンドポイント ポリシー（Endpoint Policies）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリッ

クして次を選択します。**[ポリシー（Policy）]>[プロファイリング（Profiling）]>[プロファイリング ポリシー（Profiling Policies）]**。

表 *116 :* エンドポイント プロファイリング ポリシーの設定

フィールド名	使用上のガイドライン
名前（Name）	作成するエンドポイントプロファイリングポリシーの名前を入力します。
説明（Description）	作成するエンドポイントプロファイリングポリシーの説明を入力します。
ポリシー有効（Policy Enabled）	デフォルトでは [ポリシー有効（Policy Enabled）] チェックボックスはオンになっており、エンドポイントのプロファイリング時に、一致するプロファイリング ポリシーが関連付けられます。 オフになっている場合、エンドポイントのプロファイリング時に、エンドポイント プロファイリング ポリシーは除外されます。
最小確実度計数（Minimum Certainty Factor）	プロファイリングポリシーに関連付ける最小値を入力します。デフォルト値は 10 です。
例外アクション（Exception Action）	プロファイリングポリシー内のルールを定義するときに条件に関連付ける例外アクションを選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[結果（Results）]>[プロファイリング（Profiling）]>[例外アクション（Exception Actions）] で定義されます。
ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Action）	必要に応じて、プロファイリングポリシー内のルールを定義するときに条件に関連付けるネットワーク スキャン アクションをリストから選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[結果（Results）]>[プロファイリング（Profiling）]>[ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Actions）] で定義されます。
ポリシーの ID グループの作成（Create an Identity Group for the policy）	エンドポイント ID グループを作成するには、次のオプションのいずれかをオンにします。 • **はい、一致する ID グループを作成します（Yes, create matching Identity Group）** • **いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）**

フィールド名	使用上のガイドライン
はい、一致する ID グループを作成します（Yes, create matching Identity Group）	既存のプロファイリングポリシーを使用する場合、このオプションを選択します。 このオプションは、これらのエンドポイントの一致する ID グループを作成します。エンドポイント プロファイルが既存のプロファイリング ポリシーと一致した場合に、ID グループは Profiled エンドポイント ID グループの子になります。 たとえば、ネットワーク上で検出されたエンドポイントが Xerox-Device プロファイルに一致する場合は、[エンドポイント ID グループ（Endpoint Identity Groups）] ページで Xerox-Device エンドポイント ID グループが作成されます。
いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）	プロファイリング ポリシーおよび ID グループの階層構造を使用して、一致する親エンドポイント ID グループにエンドポイントを割り当てるには、このチェックボックスをオンにします。 このオプションを使用すると、エンドポイントプロファイリングポリシー階層を利用することができ、エンドポイントはいずれかの一致する親エンドポイント ID グループ、さらに、親 ID グループに関連付けられたエンドポイント ID グループに割り当てられます。 たとえば、既存のプロファイルに一致するエンドポイントは、適切な親エンドポイント ID グループの下にグループ化されます。ここで、不明プロファイルに一致するエンドポイントは、[不明（Unknown）] の下にグループ化され、既存のプロファイルに一致するエンドポイントは、プロファイリングされたエンドポイント ID グループの下にグループ化されます。次の例を参考にしてください。 • エンドポイントが Cisco-IP-Phone プロファイルに一致する場合、これらのエンドポイントは Cisco-IP-Phone エンドポイント ID グループの下でグループ化されます。 • エンドポイントが Workstation プロファイルに一致する場合、これらのエンドポイントは、Workstation エンドポイント ID グループの下でグループ化されます。 Cisco-IP-Phone および Workstation エンドポイント ID グループは、システム内の Profiled エンドポイント ID グループに関連付けられます。
親ポリシー（Parent Policy）	新しいエンドポイント プロファイリング ポリシーを関連付ける、システムで定義されている親プロファイリング ポリシーを選択します。 子にルールと条件を継承できる親プロファイリングポリシーを選択できます。

フィールド名	使用上のガイドライン
関連 CoA タイプ（Associated CoA Type）	エンドポイント プロファイリング ポリシーと関連付ける次のいずれかの CoA タイプを選択します。 • CoA なし（No CoA） • ポートバウンス（Port Bounce） • 再認証（Reauth） • [グローバル設定（Global Settings）] : [管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロファイリング（Profiling）] で設定されたプロファイラ設定から適用されます。
ルール（Rule）	エンドポイント プロファイリング ポリシーで定義された 1 つ以上のルールにより、エンドポイントの一致するプロファイリング ポリシーが決定されます。これにより、プロファイルに応じたエンドポイントのグループ化が可能になります。 ポリシー要素ライブラリからの 1 つ以上のプロファイリング条件がルールに使用され、エンドポイント属性およびその値が、全体的な分類用に検証されます。

フィールド名	使用上のガイドライン
条件（**Conditions**）	プラス（+）記号をクリックして、条件の固定オーバーレイを展開します。マイナス（-）記号をクリックするか、固定オーバーレイの外側をクリックして条件を閉じます。 [既存の条件をライブラリから選択（Select Existing Condition from Library）] または [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] をクリックします。 [既存の条件をライブラリから選択（Select Existing Condition from Library）]：ポリシー要素ライブラリからシスコによって事前定義された条件を選択して、式を定義できます。 [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）]：さまざまなシステム辞書またはユーザー定義辞書から属性を選択して、式を定義できます。 プロファイリング条件と次のいずれかとを関連付けることができます。 • 各条件の確実度係数の整数値 • その条件の例外アクションまたはネットワーク スキャン アクション プロファイリング条件と関連付ける、次のいずれかの定義済み設定を選択します。 • [確実度計数が増加する（Certainty Factor Increases）]：各ルールの確実度値を入力します。この値は、全体的な分類に関するすべての一致ルールに対して追加されます。 • [例外の操作を行う（Take Exception Action）]：このエンドポイント プロファイリング ポリシーの [例外アクション（Exception Action）] フィールドで設定された例外アクションがトリガーされます。 • [ネットワークスキャンを行う（Take Network Scan Action）]：このエンドポイント プロファイリング ポリシーの [ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Action）] フィールドで設定されたネットワーク スキャン アクションがトリガーされます。

フィールド名	使用上のガイドライン
既存の条件をライブラリから選択（Select Existing Condition from Library）	次を実行できます。 • ポリシー要素ライブラリに存在するシスコによって事前定義された条件を選択できます。ANDまたはOR演算子を使用して複数の条件を追加できます。 • [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。 • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます • [複製（Duplicate）]：選択した条件のコピーを作成します • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます • [削除（delete）]：選択した条件を削除します。
新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）	次を実行できます。 • 式にアドホック属性/値の組み合わせを追加し、AND または OR 演算子を使用すると、複数の条件を追加できます。 • [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。 • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます • [複製（Duplicate）]：選択した条件のコピーを作成します • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます • [削除（delete）]：選択した条件を削除します。 AND または OR 演算子を使用できます

関連トピック

Cisco ISE プロファイリング サービス （1210 ページ）

エンドポイント プロファイリング ポリシーの作成 （1274 ページ）
UDID 属性を使用するエンドポイント コンテキストの可視性 （1317 ページ）

UDID 属性を使用するエンドポイント コンテキストの可視性

固有識別子（UDID）は、特定のエンドポイントの MAC アドレスを識別するエンドポイント属性です。エンドポイントは複数の MAC アドレスを持つことがあります。たとえば、有線インターフェイスに 1 つ、ワイヤレスインターフェイス用にもう 1 つの MAC アドレスがある場合があります。エージェントはそのエンドポイントの UDID を生成し、それをエンドポイント属性として保存します。UDID は承認クエリ内に使用できます。エンドポイントの UDID は一定であり、エージェントのインストールまたはアンインストールに伴って変更されることはありません。UDID を使用すると、[コンテキストの可視性（Context Visibility）] ウィンドウ（[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [コンプライアンス（Compliance）]）では、複数の NIC が装着されているエンドポイントの場合は複数のエントリではなく 1 つのエントリが表示されます。MAC アドレスではなく特定のエンドポイントに対してポスチャ制御を行うことができます。

（注） UDID を作成するには、エンドポイントの AnyConnect が 4.7 以上である必要があります。

エンドポイントコンテキストの可視性ウィンドウの GUID を持つエンドポイントの単一エントリ

ランダムな MAC アドレスを使用するエンドポイントが Cisco ISE に接続し、次の条件を満たす場合、[エンドポイントコンテキストの可視性（Endpoint Context Visibility）] ウィンドウには、エンドポイントの最新の MAC アドレスのみが表示されます。

- エンドポイントは、証明書ベースの認証方法（EAP-TLS など）を介して Cisco ISE に接続します。
- エンドポイントは、MDM サーバーを介して Cisco ISE に接続します。

上記の条件を満たすエンドポイントは、MAC アドレスではなく GUID と呼ばれる一意の属性によって識別されます。Cisco ISE GUI の **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** ウィンドウで、GUID を持つエンドポイントは、最新のランダム MAC アドレスとともに 1 回だけリストされます。

[MDM-GUID] 列には、エンドポイントに割り当てられている一貫性のある GUID が表示されます。

以前の MAC アドレスエントリで使用できたすべてのエンドポイントデータは、新しいエントリに引き継がれます。

Windows および MacOS エンドポイント用のエンドポイント スクリプト ウィザード

エンドポイント スクリプト ウィザードを使用すると、接続されているエンドポイントでスクリプトを実行して、組織の要件に準拠した管理タスクを実行できます。これには、使用されていないソフトウェアのアンインストール、プロセスやアプリケーションの開始または終了、特定のサービスの有効化または無効化などのタスクが含まれます。

エンドポイントスクリプトは、エンドポイント スクリプト ウィザードを使用して Windows と MacOS のエンドポイントで実行できます。

始める前に

- ネットワーク管理者のユーザーロールが必要です。
- 管理権限で MacOS と Windows のエンドポイントにアクセスするための Cisco ISE のログインクレデンシャルを設定します。

  Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [エンドポイントログイン設定（Endpoint Login Configuration）]** を選択し、次を設定します。

  - Cisco ISE がエンドポイントにログインできるドメインクレデンシャル。
  - Cisco ISE がローカルユーザーとしてエンドポイントにログインできる Windows と MacOS のローカルユーザーのクレデンシャル。

    ドメインユーザーはローカルユーザーよりも優先されます。両方を設定し、ローカルユーザーのクレデンシャルを使用してスクリプトを実行する必要がある場合は、ドメインのクレデンシャルを削除する必要があります。

- Windows のエンドポイントには、Windows PowerShell バージョン 5.1 以降がインストールされている必要があります。PowerShell のリモート処理を有効にする必要があります。
- MacOS のエンドポイントには Bash がインストールされている必要があります。
- Windows と MacOS の両方のエンドポイントに cURL バージョン 7.34 以降がインストールされている必要があります。
- Windows と MacOS のエンドポイントは、ネットワークに接続され、Cisco ISE にアクティブなセッションがある必要があります。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]** を選択します。

ステップ 2 ウィンドウの右上隅にあるリンクアイコンをクリックし、ドロップダウンリストから [エンドポイントスクリプトの実行（Run Endpoint Scripts）] を選択します。

[ようこそ（Welcome）] タブには、ログインクレデンシャルが設定されていない場合にこれを行うための [エンドポイントのログイン設定（Endpoint Login Configuration）] ウィンドウへのリンクが含まれています。ログインクレデンシャルが設定されている場合にのみ、このタブの右下隅にある [開始（Start）] ボタンをクリックできます。

ステップ 3 [カテゴリの選択（Select Category）] タブでは、オペレーティングシステムまたはそれらで使用可能なアプリケーションのいずれかに基づいてエンドポイントを選択できます。[OS別（By OS）] または [アプリケーション別（By Application）] のオプションボタンをクリックして選択します。[次へ（Next）] をクリックして次に進みます。

ステップ 4 [エンドポイントの選択（Select Endpoints）] ウィンドウのダッシュレットには、適用可能な OS タイプまたはアプリケーションに使用できるフィルタが表示されます。ダッシュレットで、適用するフィルタをクリックすると、そのフィルタのすべてのエンドポイントがテーブルに表示されます。

- 選択したフィルタのすべてのエンドポイントを選択するには、テーブルのタイトル行のチェックボックスをオンにします。
- 特定のエンドポイントを選択するには、テーブル内のそのエントリのチェックボックスをオンにします。テーブルから特定のエンドポイントを検索するには、テーブルの上の [フィルタ（Filter）] ボタンをクリックし、[クイックフィルタ（Quick Filter）] を選択します。表示される任意のパラメータでフィルタ処理して、必要なエンドポイントを見つけることができます。

（注） [カテゴリの選択（Select Categories）] のステップで [アプリケーション別（By Application）] を選択した場合は、このステップで同じ OS タイプに所属するエンドポイントを選択してください。アプリケーションベースのスクリプトの場合は、OS タイプごとにスクリプトを作成し、エンドポイント スクリプト ウィザードで OS タイプごとに個別のジョブを設定します。

ステップ 5 スクリプトを実行するエンドポイントを選択したら、[次へ（Next）] をクリックします。

ステップ 6 [スクリプトの選択（Select Scripts）] タブで、[追加（Add）] をクリックします。

ステップ 7 [スクリプトの追加（Add Script）] をクリックして、システムからスクリプトを選択します。[アップロードの開始（Start Upload）] をクリックして、[スクリプトの選択（Select Scripts）] タブにスクリプトを追加します。

ステップ 8 実行するスクリプトのチェックボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 9 [サマリー（Summary）] タブには、選択したエンドポイントと選択したスクリプトが表示されます。ここで選択内容を確認し、[戻る（Back）] をクリックして詳細を変更します。[終了（Finish）] をクリックして、スクリプトの実行を開始します。

[エンドポイント スクリプト レポート（Endpoints Script Report）] という名前のポップアップウィンドウが表示され、このタスクの**ジョブ ID** が示されます。このタスクと詳細とともにウィンドウにリダイレクトする [エンドポイント スクリプト プロビジョニング レポート（Endpoint Scripts provisioning report）] をクリックします。

エンドポイント スクリプト ウィザードで実行されたジョブのレポートを表示するには、**[操作（Operations）] > [レポート（Reports）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] > [エンドポイントスクリプトのプロビジョニングのサマリー（Endpoint Scripts Provisioning Summary）]** を選択します。

エンドポイントスクリプトのプロビジョニングのサマリーレポート

Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[エンドポイントとユーザー（Endpoints and Users）]** > **[エンドポイントスクリプトのプロビジョニングの概要（Endpoint Scripts Provisioning Summary）]** を選択します。

[エンドポイントスクリプトのプロビジョニングの概要（Endpoint Scripts Provisioning Summary）] ウィンドウには、過去 30 日間にエンドポイント スクリプト ウィザードで実行されたジョブの詳細が表示されます。レポートのエクスポートをスケジュールし、古いレポートを追跡するには、ウィンドウの右上隅にある [スケジュール（Schedule）] をクリックします。

[エクスポート先（Export To）] をクリックし、ドロップダウンリストからオプションを選択して、レポートの CSV または PDF バージョンをリポジトリまたはローカルの接続先に保存します。

[エンドポイントスクリプトプロビジョニングの概要（Endpoint Scripts Provisioning Summary）] ウィンドウには、デフォルトで次の列を含むテーブルが表示されます。

列の名前	表示される情報
ログ記録	ジョブ送信のタイムスタンプ。
ジョブ ID	このエントリの詳細を表示するには、[ジョブ ID（Job ID）] エントリをクリックします。[エンドポイントスクリプトのプロビジョニングの詳細（Endpoint Scripts Provisioning Details）] が表示された新しいタブが開き、タイムスタンプ、選択したエンドポイントの MAC アドレス、各エンドポイントのスクリプトのステータスとスクリプトのプロビジョニングステータス、ジョブをプロビジョニングする PSN の名前、ジョブ ID が表示されます。 （注） **注**：スクリプト実行の詳細な手順については、MAC アドレスをクリックします。
管理者名	ジョブを送信した管理者の名前。
オペレーティング システム	選択したスクリプトが実行されたオペレーティングシステム。
合計/成功/失敗/進行中のエンドポイント	• 選択されたエンドポイントの合計数。 • スクリプトが正常に実行されたエンドポイントの数。 • スクリプトの実行に失敗したエンドポイントの数。

列の名前	表示される情報
	• スクリプトが実行中のエンドポイントの数。
スクリプト名	ジョブに含まれるスクリプトの名前。

IF-MIB

オブジェクト	OID
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

SNMPv2-MIB

オブジェクト	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

IP-MIB

オブジェクト	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToPhysicalPhysAddress	1.3.6.1.2.1.4.35.1.4

CISCO-CDP-MIB

オブジェクト	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17

オブジェクト	OID
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

CISCO-VTP-MIB

オブジェクト	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

CISCO-STACK-MIB

オブジェクト	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

BRIDGE-MIB

オブジェクト	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

OLD-CISCO-INTERFACE-MIB

オブジェクト	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

CISCO-LWAPP-AP-MIB

オブジェクト	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.2
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.9
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.11
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.20

オブジェクト	OID
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

CISCO-LWAPP-DOT11-CLIENT-MIB

オブジェクト	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10

オブジェクト	OID
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

CISCO-AUTH-FRAMEWORK-MIB

オブジェクト	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

EEE8021-PAE-MIB: RFC IEEE 802.1X

オブジェクト	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

HOST-RESOURCES-MIB

オブジェクト	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

LLDP-MIB

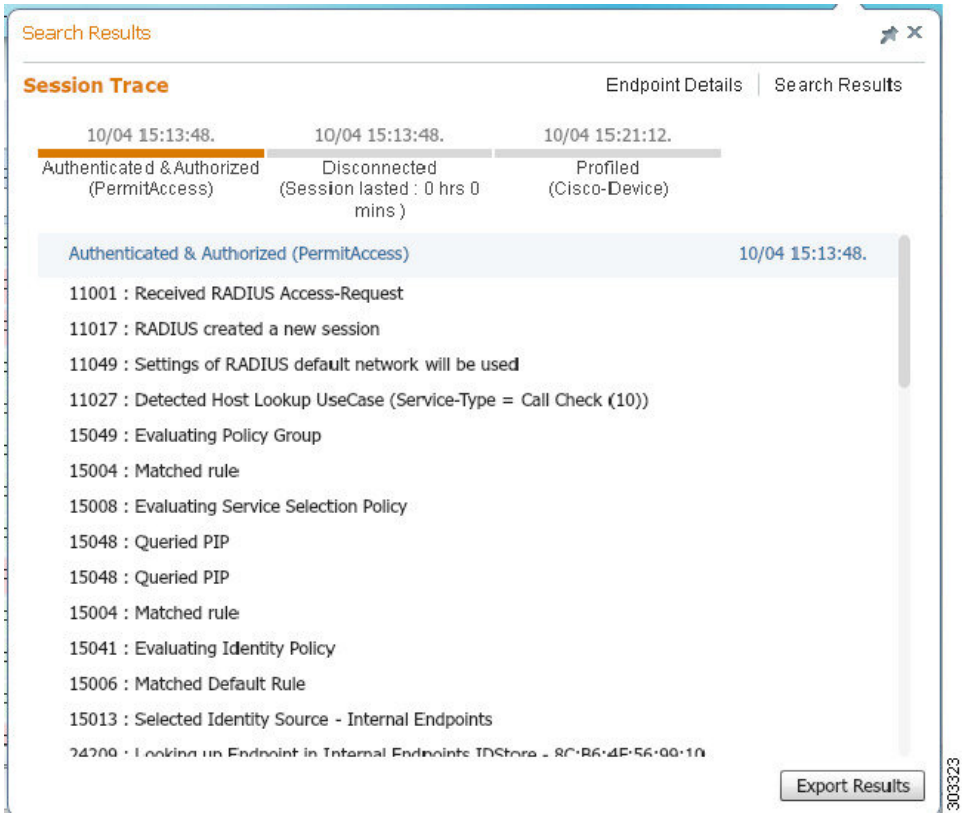
オブジェクト	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
lldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

エンドポイントのセッションのトレース

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用して、特定のエンドポイントのセッション情報を取得できます。基準に基づいて検索する場合は、エンドポイントのリストを取得します。エンドポイントのセッション トレース情報を表示するには、そのエンドポイントをクリックします。次の図に、エンドポイントに表示されるセッション トレース情報の例を示します。

（注） 検索に使用されるデータ セットは、インデックスとしてのエンドポイント ID に基づいています。したがって、認証が行われる場合、検索結果セットにそれらを含めるには、認証にエンドポイントのエンドポイント ID が必要です。

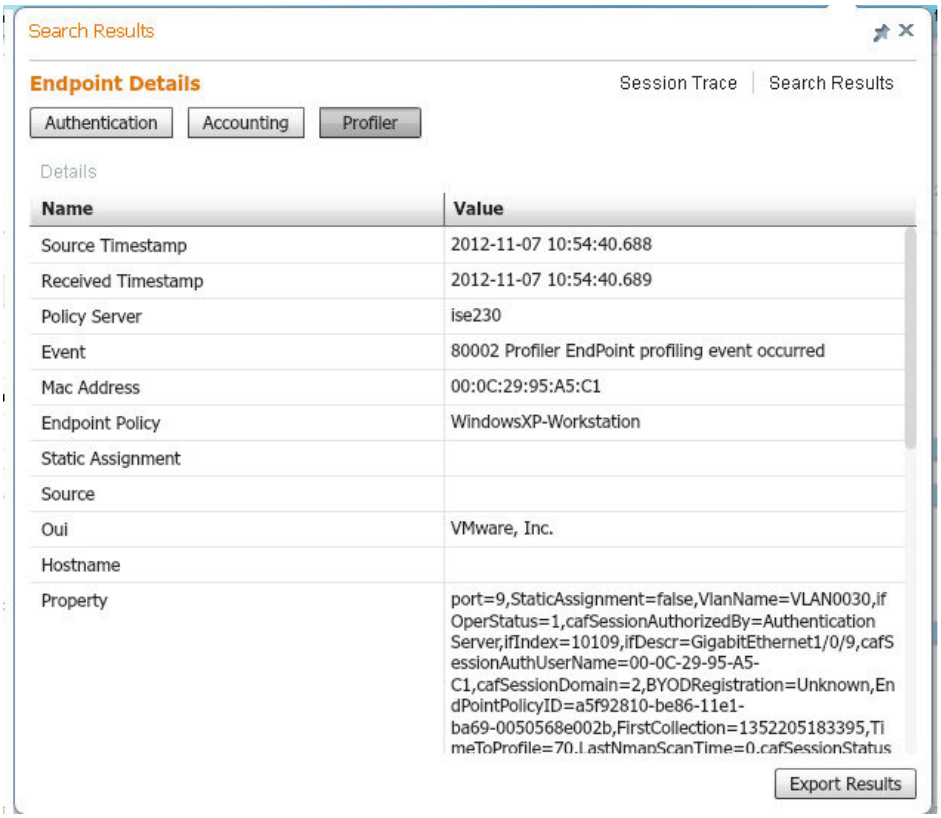
図 *30* : エンドポイントのセッションのトレース



上部にあるクリック可能なタイムラインを使用すると、主な許可の遷移を確認できます。[結果のエクスポート（Export Results）] オプションを使用して、.csv 形式で結果をエクスポートすることもできます。レポートはブラウザにダウンロードされます。

特定のエンドポイントの認証、アカウンティング、およびプロファイラの詳細情報を表示するには、[エンドポイントの詳細（Endpoint Details）] リンクをクリックします。次の図に、エンドポイントに対して表示されたエンドポイントの詳細情報の例を示します。

図 *31* : エンドポイントの詳細



ディレクトリからのセッションの削除

次のように、セッションが、モニタリングおよびトラブルシューティング ノード上のセッション ディレクトリから削除されます。

- 終了したセッションは、終了後 15 分で削除されます。
- 認証はあるがアカウンティングがない場合、このようなセッションは 1 時間後に削除されます。
- すべての非アクティブ セッションは 5 日後に消去されます。

エンドポイントのグローバル検索

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用して、エンドポイントを検索できます。次の条件を使用してエンドポイントを検索できます。

- ユーザー名
- MAC アドレス

- IP アドレス
- 許可プロファイル
- エンドポイント プロファイル
- 失敗の理由
- ID グループ
- ID ストア
- ネットワーク デバイス名
- ネットワーク デバイス タイプ
- オペレーティング システム
- ポスチャ ステータス
- ロケーション
- セキュリティ グループ
- ユーザー タイプ

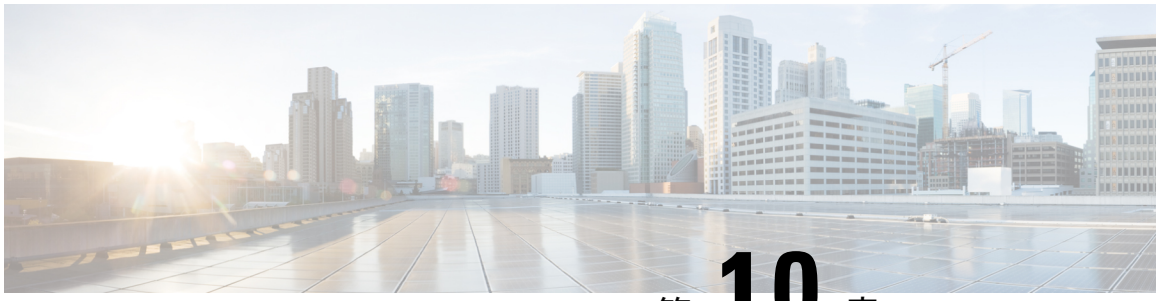
データを表示するには、[検索（Search）] フィールドに任意の検索条件の少なくとも 3 文字以上を入力する必要があります。

（注） エンドポイントが Cisco ISE によって認証された場合、またはそのアカウンティングの更新が受信された場合は、グローバル検索で確認できます。手動で追加され、Cisco ISE による認証または考慮がされていないエンドポイントは、検索結果に表示されません。

検索結果には、エンドポイントの現在のステータスに関する詳細および概要の情報が表示され、これをトラブルシューティングに使用することができます。検索結果には、上位 25 のエントリのみが表示されます。結果を絞り込むためにフィルタを使用できます。

左パネルの任意のプロパティを使用して、結果をフィルタリングします。エンドポイントをクリックして、エンドポイントに関する次のような詳細情報を表示することもできます。

- セッションのトレース
- 認証の詳細
- アカウンティングの詳細
- ポスチャの詳細
- プロファイラの詳細
- クライアント プロビジョニングの詳細
- ゲスト アカウンティングおよびアクティビティ



第 10 章

個人所有デバイスの持ち込み（BYOD）

- 企業ネットワークのパーソナル デバイス（BYOD） （1331 ページ）
- パーソナル デバイス ポータル （1332 ページ）
- ネイティブ サプリカントを使用したデバイス登録のサポート （1341 ページ）
- デバイス ポータルの設定タスク （1342 ページ）
- 従業員が追加するパーソナル デバイスの管理 （1360 ページ）
- デバイス ポータルおよびエンドポイント アクティビティのモニター （1362 ページ）

企業ネットワークのパーソナル デバイス（BYOD）

企業ネットワーク上のパーソナルデバイスをサポートする場合は、ユーザー（従業員、請負業者、およびゲスト）とそのデバイスを認証および許可することで、ネットワーク サービスおよび企業データを保護する必要があります。Cisco ISE は、従業員が企業ネットワーク上でパーソナル デバイスを安全に使用できるようにするために必要なツールを提供します。

ゲストは、ゲストポータルへのログイン時に、自動的に自分のデバイスを登録することができます。ゲストは、ゲストタイプに定義されている最大数まで追加デバイスを登録できます。これらのデバイスは、ポータル構成に基づいてエンドポイント ID グループに登録されます。

ゲストは、ネイティブ サプリカント プロビジョニング（Network Setup Assistant）を実行するか、またはデバイスを [デバイス（My Devices）] ポータルに追加して、パーソナル デバイスをネットワークに追加できます。オペレーティング システムに基づいて、使用する適切なネイティブ サプリカント プロビジョニング ウィザードを決定するネイティブ サプリカント プロファイルを作成できます。

ネイティブ サプリカント プロファイルはすべてのデバイスで使用できるわけではないため、ユーザーはデバイス ポータルを使用してこれらのデバイスを手動で追加することができます。または、これらのデバイスを登録するように BYOD ルールを設定できます。

Cisco ISE コミュニティ リソース

分散環境のエンドユーザーのデバイス ポータル

Cisco ISE のエンドユーザー Web ポータルは、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナに基づき、設定、セッション サポート、およびレポート作成を提供します。

- [ポリシー管理ノード（PAN）（Policy Administration node (PAN)）]：ユーザー、デバイス、およびエンドユーザーポータルが PAN に書き込まれる構成の変更。
- [ポリシーサービスノード（PSN）（Policy Service node (PSN)）]：エンドユーザーポータルは PSN で実行する必要があります。ここでは、ネットワークアクセス、クライアントプロビジョニング、ゲストサービス、ポスチャ、およびプロファイリングを含むすべてのセッショントラフィックが処理されます。PSN がノードグループに含まれる場合、1 つのノードで障害が発生すると、他のノードが障害を検出し、保留中のセッションをリセットします。
- [モニタリングノード（MnT ノード）（Monitoring node (MnT node)）]：MnT ノードは、デバイスポータル、スポンサーポータル、およびゲストポータルでのエンドユーザーおよびデバイスのアクティビティについて、データを収集、集約、およびレポートします。プライマリ MnT ノードに障害が発生すると、セカンダリ MnT ノードが自動的にプライマリ MonT ノードになります。

デバイス ポータルのグローバル設定

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータルの管理（Device Portal Management）] > [設定（Settings）]** を選択します。

BYOD ポータルおよびデバイス ポータルの次の一般設定を設定できます。

- [従業員が登録したデバイス（Employee Registered Devices）]：[従業員を制限（Restrict employees to）] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は **5** デバイスに設定されています。
- [再試行 URL（Retry URL）]：デバイスを Cisco ISE にリダイレクトするために使用できる URL を [オンボードのための再試行 URL（Retry URL for onboarding）] に入力します。

これらの一般的な設定値を設定したら、これらの設定は会社に設定したすべて BYOD ポータルおよびデバイス ポータルに適用されます。

パーソナル デバイス ポータル

Cisco ISE では、従業員が所有するパーソナル デバイスをサポートするために複数の Web ベース ポータルが提供されています。これらのデバイスポータルは、ゲストポータルのフローまたはスポンサー ポータルのフローには関与しません。

- **ブロック済みリストポータル**：ブロックリストに掲載されており、ネットワークへのアクセスには使用できないパーソナルデバイスに関する情報が表示されます。
- **BYOD ポータル**：従業員がネイティブ サプリカント プロビジョニング機能を使用して自分のパーソナルデバイスを登録できるようにします。
- **証明書プロビジョニングポータル**：管理者や従業員が BYOD フローを通過できないデバイスについてユーザー証明書やデバイス証明書を要求できるようにします。
- **クライアント プロビジョニング ポータル**：コンプライアンスをチェックするポスチャエージェントを自分のデバイスにダウンロードするよう従業員に強制します。
- **MDM ポータル**：従業員が外部のモバイルデバイス管理（MDM）システムに自分のモバイルデバイスを登録できるようにします。
- **デバイスポータル**：従業員がパーソナルデバイス（ネイティブ サプリカント プロビジョニングをサポートしないデバイスを含む）を追加および登録し、管理できるようにします。

Cisco ISE には、事前定義済みのデフォルト ポータルのセットを含む複数のデバイス ポータルを Cisco ISE サーバーでホストする機能が用意されています。デフォルトのポータルテーマには、管理者ポータル（[管理（Administration）] > [デバイスポータル管理（Device Portal Management）]）を通じて管理できる標準的なシスコのブランディングが適用されています。組織に固有のイメージ、ロゴ、およびカスケーディング スタイル シート（CSS）ファイルをアップロードして、ポータルをさらにカスタマイズすることもできます。

デバイス ポータルへのアクセス

次のように、Cisco ISE GUI から任意のパーソナルデバイスポータルにアクセスできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）]** を選択します。

ステップ 2 設定する特定のデバイス ポータルを選択します。

ブロックリスト ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

従業員が自分のパーソナルデバイスを紛失したり、盗まれたりした場合、[デバイス（My Devices）] ポータルでデバイスのステータスを更新して、ブロック済みリストのエンドポイント ID グループにデバイスを追加できます。これにより、不正なネットワーク アクセスにデバイスが使用されることを防ぎます。誰かがこれらのデバイスの 1 つを使用してネットワークに接続しようとすると、ブロック済みリストポータルにリダイレクトされ、デバイスのネットワークアクセスが拒否されることが通知されます。デバイスが見つかった場合、従業員はデバ

イス ポータルでデバイスを復元し、デバイスを再登録せずにネットワーク アクセスを回復できます。デバイスの盗難か紛失かによっては、デバイスをネットワークに接続する前に、追加のプロビジョニングが必要になる場合があります。

ブロック済みリストポータルのポート設定（デフォルトはポート8444）を設定できます。ポート番号を変更する場合は、別のエンドユーザーポータルで使用されていないことを確認してください。

ブロック済みリストポータルの設定については、ブロックリスト ポータルの編集 （1347 ページ）を参照してください。

証明書プロビジョニング ポータル

従業員は、証明書プロビジョニング ポータルに直接アクセスできます。

証明書プロビジョニング ポータルでは、従業員はオンボーディング フローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスは、BYOD フローを通過できず、証明書を手動で発行する必要があります。証明書プロビジョニング ポータルで、権限のある一連のユーザーは、そのようなデバイスに対する証明書要求をアップロードし、キーペアを生成し（必要に応じて）、証明書をダウンロードできます。

従業員は、このポータルにアクセスして、1 つの証明書について要求を行うか、または CSV ファイルを使用して一括証明書要求を行うことができます。

ISE コミュニティ リソース

Cisco ISE 証明書プロビジョニングポータルの機能と構成については、「ISE 2.0: Certificate Provisioning Portal」を参照してください。

個人所有デバイスの持ち込みポータル

従業員は、このポータルに直接アクセスしません。

従業員は、ネイティブ サプリカントを使用してパーソナル デバイスを登録すると、個人所有デバイスの持ち込み（BYOD）ポータルにリダイレクトされます。従業員がパーソナルデバイスを使用して初めてネットワークにアクセスを試みると、手動でNetwork Setup Assistant（NSA）ウィザードをダウンロードして起動するように求められ、ネイティブ サプリカントの登録およびインストールに進む場合があります。デバイスを登録すると、デバイス ポータルを使用して、それを管理できます。

NSA およびエージェントウィザードをダウンロードするための Web ブラウザとして Microsoft Edge 93 または Microsoft Edge 94 を使用している場合は、**リダイレクトされた URL** または**ダウンロードリンク**をコピーして新しいタブに貼り付け、キーボードの **Enter** を押します。

あるいは、Microsoft Edge 93 または Microsoft Edge 94 ブラウザで、**[ダウンロード（Download）] アイコン** > **[ダウンロードしたファイルを右クリック（right click on downloaded file）]** > **[ファイルの保持（Keep file）]** をクリックします。

Network Setup Assistant（NSA）およびエージェントウィザードをダウンロードするために Web ブラウザとして Google Chrome 93 または Google Chrome 95 を使用している場合は、ダウンロード通知の [保持（Keep）] オプションをクリックして、システムに NSA および エージェント パッケージを保持してインストールします。

（注）

- BYOD フローは、デバイスが Network Access Manager（NAM）を使用してネットワークに接続すると、サポートされません。
- Android デバイスに BYOD フローを使用している場合は、WLAN 設定で Android 11 にアップグレードするか、[ブロードキャスト SSID（Broadcast SSID）] オプションを有効にします。

関連トピック

BYOD ポータルの作成 （1350 ページ）
企業ネットワークのパーソナル デバイス（BYOD） （1331 ページ）

クライアント プロビジョニング ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

クライアント プロビジョニング システムでは、企業ネットワークにアクセスしようとしているデバイスのポスチャ評価および修復を行います。従業員がデバイスを使用してネットワークアクセスを要求したときに、クライアント プロビジョニング ポータルにルーティングして、最初にポスチャ エージェントをダウンロードするように要求できます。ポスチャ エージェントは、デバイスにアンチウイルス ソフトウェアがインストールされていることや、オペレーティング システムがサポートされていることの確認など、コンプライアンスに関するデバイスのスキャンを行います。

関連トピック

クライアント プロビジョニング ポータルの作成 （1353 ページ）

モバイル デバイス管理ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

数多くの会社で、従業員のモバイル デバイスを管理するために、モバイル デバイス管理（MDM）システムを使用しています。

Cisco ISE では外部 MDM システムとの統合が許可されており、従業員はこれを使用して、モバイルデバイスを登録し、企業ネットワークにアクセスすることができます。シスコでは、従業員がデバイスを登録し、ネットワークに接続するために使用できる外部MDMインターフェイスを提供しています。

MDM ポータルを使用することで、従業員は外部 MDM システムに登録できます。

従業員は、デバイス ポータルを使用して、PIN コードでのデバイスのロック、工場出荷時のデフォルト設定へのデバイスのリセット、デバイス登録時にインストールされていたアプリケーションおよび設定の削除など、モバイル デバイスの管理を行うことができます。

Cisco ISE では、すべての外部 MDM システム用に単一の MDM ポータルを、または個々の MDM システムごとに 1 つのポータルを使用できます。

MDM サーバーを Cisco ISE とともに動作するように設定する方法については、MDM ポータルの作成 （1355 ページ）を参照してください。

デバイス ポータル

従業員は、デバイス ポータルに直接アクセスできます。

ネットワーク アクセスが必要な一部のネットワーク デバイスは、ネイティブ サプリカント プロビジョニングでサポートされていないため、BYOD ポータルを使用して登録することができません。ただし、従業員は、オペレーティングシステムがサポートされていないか、または Web ブラウザが搭載されていないパーソナルデバイス（プリンタ、インターネットラジオ、その他のデバイスなど）を、[デバイス（My Devices）] ポータルを使用して追加および登録することができます。

従業員は、デバイスの MAC アドレスを入力して、新しいデバイスを追加および管理できます。従業員が [デバイス（My Devices）] ポータルを使用してデバイスを追加すると、Cisco ISE はそのデバイスを [登録済みデバイス（RegisteredDevices）] エンドポイント ID グループのメンバーとして [エンドポイント（Endpoints）] ウィンドウ（**[管理（Administration）] > [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]**）に追加します（別のエンドポイント ID グループに静的に割り当てられている場合を除く）。デバイスは、Cisco ISE の他のエンドポイントと同様にプロファイリングされ、ネットワーク アクセスのための登録プロセスが行われます。

1 つのデバイスからの 2 つの MAC アドレスがユーザーにより [デバイス（My Devices）] ポータルに入力されると、それらが同じホスト名を持ち、Cisco ISE で 1 つのエントリとして統合されていることがプロファイリングによって設定されます。たとえば、ユーザーは有線および無線のアドレスでラップトップを登録します。そのデバイス上での削除などの操作は、両方のアドレスで機能します。

登録済みデバイスがポータルから削除されると、[デバイス登録ステータス（DeviceRegistrationStatus）] と [BYOD 登録状態（BYODRegistration）] の属性はそれぞれ [未登録（NotRegistered）] と [いいえ（No）] に変更されます。ただし、これらの属性は、従業員のデバイス登録時にのみ使用される BYOD 属性であるため、ゲスト（従業員以外）がクレデンシャルを持つゲストポータルの [ゲストデバイス登録（Guest Device Registration）] ウィンドウを使用してデバイスを登録した場合は、変更されずそのままになります。

従業員は、BYOD またはデバイス ポータルを使用して自分のデバイスを登録しているかどうかに関係なく、デバイス ポータルを使用してそれらを管理できます。

（注） 管理者ポータルがダウンしている場合、デバイス ポータルは使用できません。

エンドポイントが [コンテキストの可視性（Context Visibility）] からインポートされても、BYODユーザーアカウントに自動的にリンクされません。デバイスポータルに追加するには、通常の BYOD 登録プロセスに従う必要があります。

関連トピック

デバイス ポータルの作成 （1357 ページ）

BYOD の展開オプションとステータス ワークフロー

パーソナルデバイスをサポートするBYOD展開フローは、次の要因によって若干異なります。

- シングルまたはデュアル SSID：シングル SSID の場合は、同じワイヤレス ローカル エリア ネットワーク（WLAN）が証明書の登録、プロビジョニング、およびネットワークアクセスに使用されます。デュアル SSID 展開では、2 つの SSID があります。1 つは登録およびプロビジョニングを提供し、もう 1 つはセキュアなネットワーク アクセスを提供します。
- Windows、MacOS、iOS、またはAndroidデバイス：ネイティブサプリカントのフローは、サポートされているパーソナルデバイスを利用する従業員を BYOD ポータルにリダイレクトしてこれらのデバイス情報を確認することによって、デバイスのタイプに関係なく、同様に開始します。プロセスはデバイス タイプに応じて分岐します。

Cisco ISE リリースを使用していて、シングルまたはデュアル SSID BYOD フローの場合、iOS デバイスを持つ BYOD ユーザーはエンタープライズ ネットワークに接続する前に、次の手順を実行する必要があります。

1. **[設定（Settings）]** > **[Safari]**の順に移動します。
2. **[履歴と Web サイトデータを消去（Clear History and Website Data）]** をタップします。

[管理（Administration）] > **[管理（Administration）]** > **[証明書（Certificate）]** > **[システム証明書（System Certificates）]** > **[デフォルト自己署名証明書（Default Self-Signed Certificate）]**ウィンドウの、BYOD 証明書の [サブジェクト代替名（Subject Alternative Name）] フィールドには、DNS 名と IP アドレスの両方を含める必要があります。

従業員がネットワークに接続する

1. Cisco ISE は、会社の Active Directory または会社の他の ID ストアを照合して従業員のクレデンシャルを認証し、認証ポリシーを提供します。
2. デバイスが BYOD ポータルにリダイレクトされます。デバイスの [MAC アドレス（MAC address）] フィールドは事前に設定されています。ユーザーはデバイス名と説明を追加できます。

3. ネイティブサプリカント（MacOS、Windows、iOS、Android）が設定されますが、プロセスはデバイスによって異なります。

   • MacOS デバイスと Windows デバイス：従業員が BYOD ポータルで [登録（Register）] をクリックし、サプリカントプロビジョニング ウィザード（Network Setup Assistant）をダウンロードしてインストールします。このウィザードではサプリカントが設定され、EAP-TLS 証明書ベース認証に使用する証明書が（必要に応じて）提供されます。デバイスの MAC アドレスと従業員のユーザー名が発行済み証明書に組み込まれます。

   MacOS 10.15 以降では、ユーザーはサプリカントプロビジョニング ウィザード（SPW）のダウンロードを許可する必要があります。ユーザーのデバイスに、Cisco ISE サーバーからのダウンロードを許可または拒否するように求めるウィンドウが表示されます。

（注） Network Setup Assistant は、そのデバイスのユーザーが管理者権限を持っていない限り、Windows デバイスにダウンロードすることはできません。エンドユーザーに管理者権限を与えることができない場合は、BYOD フローを使用するのではなく、グループ ポリシー オブジェクト（GPO）を使用して証明書をユーザーのデバイスにプッシュします。

   • iOS デバイス：Cisco ISE ポリシーサーバーは Apple の iOS ワイヤレス機能を使用して新しいプロファイルを iOS デバイスに送信します。このプロファイルには次の情報が含まれます。

     • 発行済み証明書（設定されている場合）には iOS デバイスの MAC アドレスと従業員のユーザー名が組み込まれます。

     • 802.1X 認証の EAP-TLS の使用を強制できる Wi-Fi サプリカント プロファイル。追加のプロファイルをエンドポイントデバイスにインストールして、Over-The-Air（OTA）通信を保護できます。

   [ターゲットネットワークが非表示になっている場合は有効にする（Enable if Target Network is Hidden）] チェックボックスをオンにするのは、実際の Wi-Fi ネットワークが非表示の場合に限ります。そうしないと、特にシングル SSID フロー（同じ Wi-Fi ネットワークまたは SSID がオンボーディングと接続の両方に使用されている）の特定の iOS デバイスに対して Wi-Fi ネットワーク設定が適切にプロビジョニングされない場合があります。

   • Android デバイス：Cisco ISE は、従業員に Google Play ストアから Network Setup Assistant（NSA）をダウンロードするように要求し、ルーティングします。アプリケーションのインストール後に、従業員は NSA を開いてセットアップウィザードを開始できます。このウィザードでは、サプリカントの設定と、デバイスの設定に使用される発行済み証明書が生成されます。

4. ユーザーがオンボーディングフローを完了すると、Cisco ISE は認可変更（CoA）を開始します。これにより、MacOS、Windows、および Android デバイスはセキュアな 802.1X ネットワークに再接続します。シングル SSID の場合、iOS デバイスも自動的に接続されますが、デュアル SSID の場合、ウィザードは iOS ユーザーに手動で新しいネットワークに接続するように要求します。

サプリカントを使用しない BYOD フローを設定できます。詳細については、Cisco ISE コミュニティリソースに関するドキュメント [英語] を参照してください。

（注） このフローでは、Mac のランダム化は有効ではありません。

Android 10 は新しい接続プロファイルが作成されるたびにランダムな MAC アドレスを生成するため、BYOD フローが Android クライアントで動作するためには、デフォルトルールを変更して、認証プロファイルから *BYOD_is_Registered* および *MAC_in_SAN* 条件を削除する必要があります。

BYOD セッション エンドポイント属性

エンドポイント属性 *BYODRegistration* の状態は、BYOD フローにおいて次の状態に変化します。

- *Unknown*：デバイスは BYOD フローを完了していません。
- *Yes*：デバイスは BYOD フローを通過し、登録されました。
- *No*：デバイスは BYOD フローを完了しましたが、登録されていません。つまり、デバイスは削除されています。

デバイス登録ステータスのエンドポイント属性

エンドポイント属性 *DeviceRegistrationStatus* の状態は、デバイス登録中に次の状態に変化します。

- *Registered*：デバイスは BYOD フローを完了し、登録されました。この属性が Pending から Registered になるまでに 20 分の遅れがあります。
- *Pending*：デバイスは BYOD フローを完了し、登録されています。ただし、Cisco ISE はネットワーク上でそれを認識していません。
- *Not Registered*：デバイスは BYOD フローを完了していません。*Not Registered* は、*DeviceRegistrationStatus* 属性のデフォルトの状態です。
- *Stolen*：ユーザーが [デバイス（My Devices）] ポータルにログインし、現在オンボーディングされているデバイスを Stolen としてマークしました。次のようになります。
  - 証明書とプロファイルをプロビジョニングしてデバイスのオンボーディングが行われた場合、Cisco ISE はそのデバイスに対してプロビジョニングされた証明書を失効さ

せ、デバイスの MAC アドレスを ブロック済みリストのエンドポイント ID グループに割り当てます。そのデバイスはネットワークにアクセスできなくなります。

- （証明書は含めず）プロファイルのみをプロビジョニングしてデバイスのオンボーディングが行われた場合、Cisco ISE はそのデバイスを ブロック済みリストのエンドポイント ID グループに割り当てます。この状況に対応する認証ポリシーを作成していない場合は、デバイスは引き続きネットワークにアクセスできます。たとえば、**エンドポイント ID グループがブロック済みリストであり、BYOD_is_Registered の場合は DenyAccess となります。**

管理者は、さまざまなデバイスに対してネットワークアクセスを無効にするアクション（証明書の削除や失効など）を実行します。

ユーザーが盗まれたデバイスを復元すると、ステータスは *Not Registered* に戻ります。ユーザーはそのデバイスを削除してからもう一度追加する必要があります。これにより、オンボーディングプロセスが開始されます。

- *Lost*：ユーザーが [デバイス（My Devices）] ポータルにログオンし、現在オンボーディングされているデバイスを *Lost* としてマークしたため、次のアクションが実行されます。
  - そのデバイスは ブロック済みリストの ID グループに割り当てられます。
  - デバイスに対してプロビジョニングされた証明書は失効します。
  - デバイスのステータスが *Lost* に更新されます。
  - *BYODRegistration* ステータスが *No* に更新されます。

紛失デバイスをブロックする許可ポリシーを作成していない場合、紛失デバイスは引き続きネットワークにアクセスできます。ルールで ブロック済みリストの ID グループまたはルールで *endpoint:BYODRegistration* 属性を使用できます。たとえば、**エンドポイント ID グループがブロック済みリストで EndPoints:BYODRegistrations が No の場合は BYOD** になります。きめ細かなアクセスを設定するには、*NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST" , InternalUser:IdentityGroup Equals <<group>>* をルールの IF 部分に追加することもできます。

従業員が登録するパーソナル デバイス数の制限

従業員が 1 ～ 999 のパーソナル デバイスを登録できるようにすることができます。従業員がパーソナルデバイスの登録に使用したポータルに関係なく、この設定では、すべてのポータルにわたって登録されるデバイスの最大数を定義します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）]** を選択します。

ステップ 2 [従業員を制限（Restrict employees to）] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は **5** デバイスに設定されています。

ステップ 3 [保存（Save）]をクリックします。設定の更新を保存しない場合は、[リセット（Reset）]をクリックして、最後に保存した値に戻します。

ネイティブ サプリカントを使用したデバイス登録のサポート

ネイティブ サプリカント プロファイルを作成して、Cisco ISE ネットワークでパーソナル デバイスをサポートできます。ユーザーの許可要件に関連付けるプロファイルに基づいて、Cisco ISE はネットワークにアクセスするユーザーのパーソナル デバイスをセットアップするために必要なサプリカント プロビジョニング ウィザードを提供します。

従業員がパーソナルデバイスを使用して初めてネットワークへのアクセスを試みると、登録とサプリカントの設定の手順が自動的に示されます。デバイスを登録した後、デバイス ポータルを使用してデバイスを管理できます。

ネイティブ サプリカントがサポートするオペレーティング システム

ネイティブ サプリカントは、次のオペレーティング システムでサポートされます。

- Android（Amazon Kindle、B&N Nook を除く）
- MacOS（Apple Mac コンピュータの場合）
- Apple iOS デバイス（Apple iPod、iPhone、および iPad）
- Microsoft Windows 7、8（RT を除く）、Vista、および 10

クレデンシャルを持つゲスト ポータルを使用したパーソナル デバイスの登録を従業員に許可

クレデンシャルを持つゲスト ポータルを利用している従業員は、自分のパーソナル デバイスを登録できます。BYOD ポータルによって提供されるセルフ プロビジョニング フローにより、従業員は Windows、MacOS、iOS および Android デバイスで使用可能なネイティブ サプリカントを使用してネットワークにデバイスを直接接続できます。

始める前に

ネイティブ サプリカント プロファイルを作成する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Center）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）]** を選択します。

ステップ 2 従業員がネイティブ サプリカントを使用して自分のデバイスを登録するために使用できるクレデンシャルを持つゲスト ポータルを選択し、[編集（Edit）] をクリックします。

ステップ 3 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 4 [BYOD 設定（BYOD Settings）] で [従業員にネットワークでのパーソナルデバイスの使用を許可する（Allow employees to use personal devices on the network）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

BYOD 登録に再接続する URL の提供

BYOD ポータルを使用してパーソナル デバイスを登録中に問題が発生した従業員に、登録プロセスへの再接続を可能にする情報を提供できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [再試行 URL（Retry URL）]** を選択します。

ステップ 2 [オンボードのための再試行 URL（Retry URL for onboarding）] フィールドに、デバイスを Cisco ISE にリダイレクトするために使用できる URL を入力します。

登録プロセス中にデバイスに問題が発生した場合、デバイスはインターネットに自動的に再接続しようとします。この時点で、このフィールドに入力した URL を使用してデバイスが Cisco ISE にリダイレクトされ、オンボーディングプロセスが再開されます。デフォルト値は 192.0.2.123 です。

ステップ 3 [保存（Save）] をクリックします。

設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

デバイス ポータルの設定タスク

デフォルト ポータルと、証明書、エンドポイント ID グループ、ID ソース順序、ポータル テーマ、イメージ、および Cisco ISE によって提供されるその他の詳細などのデフォルト設定を使用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

新しいポータルを作成したり、デフォルト ポータルを編集した後は、ポータルの使用を承認する必要があります。いったんポータルの使用を承認すると、後続の設定変更はただちに有効になります。

デバイス ポータルを使用するための許可は必要ありません。

ポータルを削除する場合は、関連付けられている許可ポリシー ルールおよび許可プロファイルを先に削除するか、別のポータルを使用するように変更する必要があります。

この表を使用して、異なるデバイス ポータルの設定に関連するタスクを確認できます。

タスク	ブロックリスト ポータル	BYOD ポータル	クライアント プロビジョニング ポータル	MDM ポータル	デバイス ポータル
ポリシー サービスの有効化（1344ページ）	必須	必須	必須	必須	必須
デバイス ポータルへの証明書の追加（1344ページ）	必須	必須	必須	必須	必須
外部 ID ソースの作成（1345ページ）	不要	不要	不要	不要	必須
ID ソース順序の作成（1346ページ）	不要	不要	不要	不要	必須
エンドポイント ID グループの作成（1346ページ）	不要	必須	不要	必須	必須
ブロックリスト ポータルの編集	必須	N/A	N/A	N/A	N/A
BYOD ポータルの作成（1350ページ）	N/A	必須	N/A	N/A	N/A
クライアント プロビジョニング ポータルの作成（1353ページ）	N/A	N/A	必須	N/A	N/A
MDM ポータルの作成（1355ページ）	N/A	N/A	N/A	必須	N/A
デバイス ポータルの作成（1357ページ）	N/A	N/A	N/A	N/A	必須

タスク	ブロックリスト ポータル	BYOD ポータル	クライアント プロビジョニング ポータル	MDM ポータル	デバイス ポータル
許可プロファイルの作成（1358ページ）	N/A	必須	必須	必須	不要
デバイス ポータルのカスタマイズ（1360ページ）	オプション	オプション	オプション	オプション	オプション

ポリシー サービスの有効化

Cisco ISE エンドユーザー Web ポータルをサポートするには、ホストするノードでポータルポリシーサービスを有効にする必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 2 ノードをクリックして、[編集（Edit）] をクリックします。

ステップ 3 [全般設定（General Settings）] タブで [ポリシーサービス（Policy Service）] トグルボタンを有効にします。

ステップ 4 [セッションサービスの有効化（Enable Session Services）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

デバイス ポータルへの証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループ タグに割り当てることができます。すべてのエンドユーザー Web ポータルに使用されるデフォルトの証明書グループタグは [デフォルトポータル証明書グループ（Default Portal Certificate Group）] です。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。

この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。

ステップ 3 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータルの管理（Device Portal Management）] >（任意のポータル）> [作成または編集（Create or Edit）] > [ポータル設定（Portal Settings）]** を選択します。

ステップ 4 新しく追加された証明書に関連付けられた [証明書グループ タグ（Certificate Group Tag）] ドロップダウン リストから特定の証明書グループ タグを選択します。

（注）
- BYOD は長さが 3 つの証明書を超える証明書チェーンをサポートしていません。
- BYOD オンボーディング時に、iOS デバイスに対して証明書が 2 回発行されます。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバーなどの外部 ID ソースに接続して、認証/許可のユーザー情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザー ID を受信して共有できるようにするパッシブ ID サービスを使用するには、その他の パッシブ ID サービス プロバイダー （1094 ページ）を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。
- Active Directory：外部 ID ソースとして Active Directory に接続する場合。詳細については、外部 ID ソースとしての Active Directory （1028 ページ）を参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、LDAP（1142 ページ）を参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバーを追加する場合。詳細については、RADIUS トークン ID ソース （1169 ページ）を参照してください。
- RSA SecurID：RSA SecurID サーバーを追加する場合。詳細については、RSA ID ソース （1176 ページ）を参照してください。
- SAML IDプロバイダー（SAML Id Providers）：Oracle Access Manager などの ID プロバイダー（IdP）を追加する場合。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダー （1185 ページ）を参照してください。
- ソーシャルログイン（Social Login）：Facebook などのソーシャルログインを外部 ID ソースとして追加する場合。詳細については、アカウント登録ゲストのソーシャル ログイン （834 ページ）を参照してください。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲストユーザーがローカル WebAuth を使用して認証できるようにするには、ゲストポータル認証ソースと ID ソース順序の両方に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）]** を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リストフィールドの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストフィールドのデータベースを並べ替えます。

ステップ 6 選択したアイデンティティストアに認証のためにアクセスできない場合は、[高度な検索リスト（Advanced Search List）] 領域で次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus属性をProcessErrorに設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]
- [ユーザーが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]

  Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストフィールドに Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイントIDグループ（Endpoint Identity Groups）] ウィンドウでは、追加のエンドポイント ID グループも作成できます。作成したエンドポイント ID グループを編

集または削除できます。システムで定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集または削除することはできません。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するエンドポイント ID グループの [名前（Name）] に入力します（エンドポイント ID グループの名前にはスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの [説明（Description）] に入力します。

ステップ 5 [親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

ブロックリスト ポータルの編集

Cisco ISE では、Cisco ISE でブロックリストに登録されている、紛失したり、盗難にあったりしたデバイスが企業のネットワークへのアクセスを試行した場合に、情報が表示される単一のブロックリストポータルが提供されます。

デフォルトのポータル設定を編集し、ポータルについて表示されるデフォルトのメッセージをカスタマイズすることのみができます。新しいブロックリストポータルを作成することはできず、デフォルトポータルを複製または削除することもできません。

始める前に

このポータルで使用するために、必要な証明書が設定されていることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [ブロックリストポータル（Blocked List Portal）] > [編集（Edit）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザー ポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルテストURL（Portal test URL）] リンクをクリックすると、このポータルの URL を表示する新しいブラウザタブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

（注） テストポータルはRADIUSセッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYODおよびクライアント プロビジョニングはRADIUSセッションに依存するポータルの例です。たとえば、外部URLへのリダイレクションは機能しません。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで 8443 です。ただし、ブロックリストポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアント プロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

  （注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポート

を探します。異なるサブネット上のIPアドレスを使用してイーサネットインターフェイスを設定する必要があります。

これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべてのPSNがゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
- ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらくは、そのPSNでボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- NIC チーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理NICと対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンドセットアップがなかったことが原因である可能性があるので、PSNは物理インターフェイスでポータルを開始しようとします。

- [証明書グループタグ（Certificate Group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループタグを選択します。
- **表示言語**
  - [ブラウザのロケールを使用する（Use Browser Locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語（Fallback Language）] が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback Language）]：ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。

- [常に使用（Always Use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する（User Browser Locale）] オプションを上書きします。

ステップ 6 [ポータル ページのカスタマイズ（Portal Page Customization）] タブで、許可されていないデバイスがネットワークへのアクセスの取得を試行した場合にポータルに表示されるページタイトルおよびメッセージテキストをカスタマイズします。

ステップ 7 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

BYOD ポータルの作成

Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）ポータルを提供して、ネットワークへのアクセスの許可の前に登録とサプリカント構成を行うことができるように、従業員がパーソナルデバイスを登録できるようにすることができます。

新しいBYODポータルを作成するか、既存のものを編集または複製できます。Cisco ISEによって提供されているデフォルトのポータルを含むすべての BYOD ポータルを削除できます。

[ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] タブのしたにある [ポータルとページの設定（Portal & Page Settings）] に加えた変更は、デバイスポータルフロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ウィンドウなどのウィンドウを有効にすると、そのウィンドウがフローに表示され、従業員はポータルで使用できるようになります。ウィンドウを無効にすると、フローから削除されます。

始める前に

このポータル内で使用するために、必要な証明書とエンドポイント ID グループが設定されていることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [BYOD] > [作成（Create）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザーポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 [サポート情報ページの設定（Support Information Page Settings）] を展開します。ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、ここで必要な情報を更新します。

ステップ 7 [ポータルページのカスタマイズ（Portal Page Customizations）] タブをクリックします。次のエンドユーザーポータル ウィンドウをカスタマイズするには、[ページのカスタマイズ（Page Customizations）] 領域までスクロールします。左側のメニューにある [ページ（Pages）] にリストされている対応するオプションをクリックして、カスタマイズするポータルウィンドウを選択します。

- **[BYOD ようこそ（BYOD Welcome）]**：
  - **[デバイス構成が必要（Device Configuration Required）]**：デバイスが BYOD ポータルに初めてリダイレクトされ、証明書のプロビジョニングが必要な場合、表示される内容を入力します。
  - **[証明書の更新が必要（Certificate Needs Renewal）]**：前の証明書が更新される必要がある場合、表示される内容を入力します。
- **[BYOD デバイス情報（BYOD Device Information）]**：
  - **[最大デバイス数に到達（Maximum Devices Reached）]**：従業員が登録できるデバイスの最大数に到達した場合、表示される内容を入力します。
  - **[必要なデバイス情報（Required Device Information）]**：従業員がデバイスを登録できるようにするために必要なデバイス情報を要求している場合、表示される内容を入力します。
- **[BYOD インストール（BYOD Installation）]**：
  - **[デスクトップインストール（Desktop Installation）]**：デスクトップデバイス用のインストール情報を提供する場合、表示される内容を入力します。
  - **[iOS インストール（iOS Installation）]**：iOS モバイルデバイス用のインストールの指示を提供する場合、表示される内容を入力します。
  - **[Android インストール（Android Installation）]**：Android モバイルデバイス用のインストールの指示を提供する場合、表示される内容を入力します。
- **[BYOD成功（BYOD Success）]**：
  - **[成功（Success）]**：デバイスが設定され、自動的にネットワークに接続される場合、表示される内容を入力します。
  - **[成功：手動手順（Success: Manual Instructions）]**：デバイスが正常に設定され、従業員がネットワークに手動で接続する必要がある場合、表示される内容を入力します。
  - **[成功：サポート対象外のデバイス（Success: Unsupported Device）]**：サポート対象外のデバイスがネットワークに接続できる場合、表示される内容を入力します。

ステップ 8 [保存（Save）] をクリックして、さらに [閉じる（Close）] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

クライアント プロビジョニング ポータルの作成

Cisco ISE では証明書プロビジョニング ポータルが提供され、そこではオンボーディング フローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスがあります。1つの証明書について要求を行うか、またはCSVファイルを使用して一括証明書要求を行うことができます。

デフォルトのポータル設定を編集し、ポータルに表示されるメッセージをカスタマイズすることができます。また、証明書プロビジョニング ポータルを作成、複製、および削除することもできます。

証明書プロビジョニング ポータルにアクセスできるユーザーには 2 つのタイプがあります。

- 管理者権限を持つ内部または外部のユーザー：自分自身と他人に対し証明書を生成できます。
- 他のすべてのユーザー：自身の証明書のみを生成できます。

スーパー管理ロールまたは ERS 管理ロールを割り当てられたユーザー（ネットワーク アクセス ユーザー）はこのポータルにアクセスでき、他人のために証明書を要求できます。ただし、新しい内部管理ユーザーを作成し、スーパー管理ロールまたは ERS 管理ロールを割り当てると、内部管理ユーザーはこのポータルにアクセスできません。最初にネットワーク アクセス ユーザーを作成し、それからユーザーをスーパー管理グループまたは ERS 管理グループに追加する必要があります。スーパー管理グループまたは ERS 管理グループに追加されている既存のネットワーク アクセス ユーザーは、このポータルにアクセスできます。

他のユーザーがポータルにアクセスして自身の証明書を生成できるようにするには、[証明書プロビジョニングポータルの設定（Certificate Provisioning Portal Settings）] を設定します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）] > [編集（Edit）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]**。[認証方式（Authentication Method）] で適切な ID ソースまたは ID ソース順序を選択し、[承認済みグループの設定（Configure Authorized Groups）] でユーザー グループを選択します。選択したグループに属するすべてのユーザーが、ポータルにアクセスし、自分自身の証明書を生成できるようになります。

始める前に

このポータルで使用するために、必要な証明書が設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）]** > [作成（Create）]Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。。

ここで使用するポータル名が他のエンドユーザー ポータルに使用されていないことを確認します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 [ポータルページのカスタマイズ（Portal Page Customizations）] タブをクリックします。ポータルに表示されるページのタイトルとメッセージのテキストをカスタマイズします。

ステップ 7 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

クライアント プロビジョニング ポータルの作成

クライアント プロビジョニング ポータルを提供して、ネットワークへのアクセスを許可する前に、デバイスのポスチャ遵守を確認する エージェントのポスチャコンポーネント を従業員がダウンロードできるようにすることが可能です。

新しいクライアント プロビジョニング ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのクライアント プロビジョニング ポータルを削除できます。

スーパー管理ロールまたは ERS 管理ロールを割り当てられたユーザー（ネットワーク アクセス ユーザー）はこのポータルにアクセスできます。ただし、新しい内部管理ユーザーを作成し、スーパー管理ロールまたはERS管理ロールを割り当てると、内部管理ユーザーはこのポータルにアクセスできません。最初にネットワーク アクセス ユーザーを作成し、それからユーザーをスーパー管理グループまたは ERS 管理グループに追加する必要があります。スーパー管理グループまたは ERS 管理グループに追加されている既存のネットワーク アクセス ユーザーは、このポータルにアクセスできます。

他のユーザーがポータルにアクセスして自身の証明書を生成できるようにするには、[証明書プロビジョニングポータルの設定（Certificate Provisioning Portal Settings）] を設定します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [クライアントプロビジョニング（Client Provisioning）] > [編集（Edit）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です。[認証方式（Authentication Method）] で適切な ID ソースまたは ID ソース順序を選択し、[承認済みグループの設定（Configure Authorized Groups）] でユーザー グループを選択します。選択したグループに属するすべてのユーザーが、ポータルにアクセスし、自分自身の証明書を生成できるようになります。

[ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] タブのしたにある [ポータルとページの設定（Portal & Page Settings）] に加えた変更は、デバイスポータルフロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ウィンドウなどのウィンドウを有効にすると、そのウィンドウがフローに表示され、従業員はポータルで使用できるようになります。ウィンドウを無効にすると、フローから削除されます。

始める前に

このポータルで使用するために設定されている必要な証明書とクライアントプロビジョニングポリシーがあることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータルの管理（Device Portal Management）] > [クライアントプロビジョニング（Client Provisioning）] > [作成（Create）** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザーポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 [サポート情報ページの設定（Support Information Page Settings）] を展開します。ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、ここで必要な情報を更新します。

ステップ 7 [ポータルページのカスタマイズ（Portal Page Customizations）] タブをクリックします。次のエンドユーザーポータル ウィンドウをカスタマイズするには、[ページのカスタマイズ（Page Customizations）] 領域までスクロールします。左側のメニューにある [ページ（Pages）] にリストされている対応するオプションをクリックして、カスタマイズするポータルウィンドウを選択します。

- **[クライアントプロビジョニングポータル（Client Provisioning Portals）]**：
  - **[不明なエージェント（Agent Unknown）]**：エージェントが不明な場合に表示される内容を入力します。
  - **[確認（Checking）]、[スキャン（Scanning）]、[準拠（Compliant）]**：ポスチャエージェントが正常にインストールされ、デバイスがポスチャ要件に準拠していることを確認、スキャン、および検証する場合に表示される内容を入力します。
  - **[非準拠（Non-compliant）]**:ポスチャエージェントが、デバイスがポスチャ要件に準拠していないと判断した場合に表示される内容を入力します。
- **[クライアントプロビジョニング（エージェント未検出）（Client Provisioning (Agent Not Found)）]**：
  - **[エージェントが見つかりませんでした（Agent Not Found）]**：ポスチャエージェントがデバイスで検出されない場合に表示される内容を入力します。
  - **[手動インストールの手順（Manual Installation Instructions）]**：デバイスに Java または Active X ソフトウェアがインストールされていない場合に表示される内容、ポスチャエージェントを手動でダウンロードし、インストールする方法の手順を入力します。
  - **[インストール、Java/ActiveX なし（Install, No Java/ActiveX）]**：デバイスに Java または Active X ソフトウェアがインストールされていない場合に表示される内容、手動で Java プラグインをダウンロードしてインストールする方法の手順を入力します。

- **[エージェントインストール済み（Agent Installed）]**：ポスチャエージェントがデバイスで検出された場合に表示される内容、ポスチャエージェントを開始する方法の手順を入力します。ポスチャエージェントにより、デバイスがポスチャ要件に準拠するかどうかが確認されます。

ステップ 8 [保存（Save）] をクリックして、さらに [閉じる（Close）] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

関連トピック

ポータルの許可 （856 ページ）
デバイス ポータルのカスタマイズ （1360 ページ）

MDM ポータルの作成

モバイル デバイス管理（MDM）ポータルを提供して、従業員が、企業ネットワークでの使用のために登録されたモバイル デバイスを管理できるようにすることができます。

新しい MDM ポータルを作成するか、既存のものを編集または複製できます。すべての MDM システムに対して 1 つの MDM ポータルを設定できます。または、各システムに対し 1 つのポータルを作成できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべての MDM ポータルを削除できます。デフォルトのポータルは、サードパーティの MDM プロバイダー用です。

新しいMDMポータルを作成するか、既存のものを編集または複製できます。Cisco ISEによって提供されているデフォルトのポータルを含むすべての MDM ポータルを削除できます。デフォルトのポータルは、サードパーティの MDM プロバイダー用です。

[ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] タブのしたにある [ポータルとページの設定（Portal & Page Settings）] に加えた変更は、デバイスポータルフロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ウィンドウなどのウィンドウを有効にすると、そのウィンドウがフローに表示され、従業員はポータルで使用できるようになります。ウィンドウを無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書とエンドポイント ID グループが設定されていることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[モバイルデバイス管理（Mobile Device Management）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザーポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 [ポータル設定（Portal Settings）] を展開します。ポート、証明書グループタグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 [従業員のモバイルデバイス管理設定（Employee Mobile Device Management Settings）] を展開します。サードパーティの MDM プロバイダーを設定するために提供されているリンクにアクセスし、MDM ポータルを使用して従業員の受信ポリシーによる動作を定義します。

ステップ 7 [サポート情報ページの設定（Support Information Page Settings）] を展開します。ネットワークアクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、ここで必要な情報を更新します。

ステップ 8 [ポータルページのカスタマイズ（Portal Page Customizations）] タブをクリックします。

ステップ 9 デバイス登録プロセス時に MDM ポータルに表示される [コンテンツ領域（Content Area）] メッセージをカスタマイズします。

- **[到達不能（Unreachable）]**：選択された MDM システムにアクセスできない場合に表示される内容を入力します。
- **[非準拠（Non-compliant）]**：登録されるデバイスが MDM システムの要件に準拠していない場合に表示される内容を入力します。
- **[続行（Continue）]**：接続に問題があるケースで、デバイスがネットワークへの接続を試行する必要がある場合に表示される内容を入力します。
- **[登録（Enroll）]**：デバイスが MDM エージェントを必要とし、かつそのデバイスを MDM システムに登録する必要がある場合に表示される内容を入力します。

ステップ 10 [保存（Save）] をクリックして、さらに [閉じる（Close）] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。また、次のトピックを参照してください。

- デバイス ポータルへの証明書の追加 （1344 ページ）
- エンドポイント ID グループの作成 （1346 ページ）
- 許可プロファイルの作成 （1358 ページ）
- デバイス ポータルのカスタマイズ （1360 ページ）

デバイス ポータルの作成

デバイス ポータルを提供して、従業員が、ネイティブ サプリカントをサポートせず、個人所有デバイスの持ち込み（BYOD）を使用して追加できないパーソナルデバイスを追加および登録できるようにすることができます。デバイスポータルを使用して、いずれかのポータルを使用して追加されたすべてのデバイスを管理できます。

新しいデバイス ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのデバイス ポータルを削除できます。

[ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] タブのしたにある [ポータルとページの設定（Portal & Page Settings）] に加えた変更は、デバイスポータルフロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ウィンドウなどのウィンドウを有効にすると、そのウィンドウがフローに表示され、従業員はポータルで使用できるようになります。ウィンドウを無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書、外部 ID ストア、ID ソース順序、およびエンドポイント ID グループが設定されていることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[デバイス（My Devices）]** > **[作成（Create）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザーポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウンリストから、ポータルで使用する言語ファイルをインポートまたはエクスポートする目的のアクションを選択します。

ステップ 4 [ポータルの動作とフロー設定（Portal Behavior and Flow Settings）] タブをクリックします。

ステップ 5 ポート、証明書グループタグ、エンドポイントIDグループなどのデフォルト値を更新して、ポータル全体に適用する動作を定義するには、[ポータルの設定（Portal Settings）] を展開します。

ステップ 6 従業員のログイン情報およびログインガイドラインを指定するには、[ログインページの設定（Login Page Settings）] を展開します。

ステップ 7 別の AUP ページを追加し、従業員のアクセプタブル ユース ポリシーの動作を定義するには、[アクセプタブルユースポリシー（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）] を展開します。

ステップ 8 ポータルへのログイン後に、従業員に追加情報を通知するには、[ポストログインバナーページの設定（Post-Login Banner Page Settings）] を展開します。

ステップ 9 従業員の自身のパスワードの変更を許可するには、[従業員のパスワード変更の設定（Employee Change Password Settings）] を展開します。このオプションは、従業員が内部ユーザーデータベースの一部である場合にのみ有効になります。

ステップ 10 [ポータル ページのカスタマイズ（Portal Page Customization）] タブで、登録および管理時にデバイス ポータルに表示される次の情報をカスタマイズします。

- タイトル、コンテンツ、フィールド、およびボタン ラベル
- **エラーメッセージ**および**通知メッセージ**

ステップ 11 [保存（Save）] をクリックして、さらに [閉じる（Close）] をクリックします。

次のタスク

ポータルの外観を変更する場合は、ポータルをカスタマイズできます。

関連トピック

デバイス ポータルのカスタマイズ （1360 ページ）
デバイス ポータル （1336 ページ）
従業員が追加したデバイスの表示 （1360 ページ）

許可プロファイルの作成

ポータルを許可するときは、ネットワーク アクセス用のネットワーク許可プロファイルおよびルールを設定します。

始める前に

ポータルを許可する前にポータルを作成する必要があります。

ステップ 1 ポータルの特別な許可プロファイルを設定します。
ステップ 2 プロファイルの許可ポリシー ルールを作成します。

許可プロファイルの作成

各ポータルには、特別な許可プロファイルを設定する必要があります。

始める前に

デフォルトのポータルを使用しない場合は、許可プロファイルとポータル名を関連付けることができるように、最初にポータルを作成する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** を選択します。
ステップ 2 使用を許可するポータル名を使用して許可プロファイルを作成します。

次のタスク

新しく作成される許可プロファイルを使用するポータル許可ポリシー ルールを作成する必要があります。

許可ポリシー ルールの作成

ユーザー（ゲスト、スポンサー、従業員）のアクセス要求への応答に使用するポータルのリダイレクション URL を設定するには、そのポータル用の許可ポリシー ルールを定義します。

url-redirect は、ポータル タイプに基づいて次の形式になります。

ip:port ：IP アドレスとポート番号

PortalID：一意のポータル名

ホットスポット ゲスト ポータル：
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

モバイル デバイス管理（MDM）ポータル：
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]**> **[ポリシーセット（Policy Sets）]** を選択して、[標準（Standard）] ポリシーで新しい認証ポリシールールを作成します。

ステップ 2 [条件（Conditions）] には、ポータルの検証に使用するエンドポイント ID グループを選択します。たとえば、ホットスポット ゲスト ポータルの場合は、デフォルトの [GuestEndpoints] エンドポイント ID グループを選択し、MDM、ポータルの場合は、デフォルトの [RegisteredDevices] エンドポイント ID グループを選択します。

（注） Reauthenticate および Terminate CoA タイプは、ホットスポット ゲスト ポータルでサポートされています。ホットスポット ゲスト ポータルで Reauthentication CoA タイプが選択されている場合のみ、ホットスポットゲスト認証ポリシーの検証条件の 1 つとして [ネットワークアクセス：ユースケースEQUALSゲストフロー（Network Access:UseCase EQUALS Guest Flow）] を使用できます。

ステップ 3 [権限（Permissions）] には、作成したポータル許可プロファイルを選択します。

（注） RADIUS.Calling-Station-ID など、MAC オプションが有効になっているディクショナリ属性を使用して許可条件を作成する場合は、さまざまな MAC 形式をサポートするために Mac 演算子（Mac_equals など）を使用する必要があります。

デバイス ポータルのカスタマイズ

ポータルの外観およびユーザー（必要に応じてゲスト、スポンサー、または従業員）エクスペリエンスをカスタマイズするには、ポータルテーマをカスタマイズし、ポータルページの UI 要素を変更して、ユーザーに表示されるエラーメッセージと通知を編集します。ポータルのカスタマイズの詳細については、エンドユーザー Web ポータルのカスタマイズ （928 ページ）を参照してください。

従業員が追加するパーソナル デバイスの管理

従業員が Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）またはデバイスポータルを使用してデバイスを登録すると、登録済みデバイスは[エンドポイント（Endpoints）]リストに表示されます。従業員はデバイスを削除して自分のアカウントからデバイスを切り離すことができますが、デバイスは Cisco ISE データベースに残ります。この結果、従業員は、デバイスの使用時に発生するエラーの解決に管理者の支援を必要とする場合があります。

従業員が追加したデバイスの表示

[エンドポイント（Endpoints）] リストページに表示される [ポータルユーザー（Portal User）] フィールドを使用して、特定の従業員が追加したデバイスを特定できます。これは、特定のユーザーが登録したデバイスを削除する必要がある場合に役立つことがあります。デフォルトでは、このフィールドは表示されないため、検索する前に最初に有効にする必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

ステップ 2 エンドポイントリストの右上隅でダッシュレットの下にある [設定（Settings）] アイコンをクリックします。

ステップ 3 [ポータルユーザー（Portal User）] チェックボックスをオンにして、[ポータルユーザー（Portal User）] トグルボタンを有効にして、エンドポイントリストにこの情報を表示します。

ステップ 4 [実行（Go）] をクリックします。

ステップ 5 [フィルタ（Filter）] ドロップダウンリストをクリックし、[クイック フィルタ（Quick Filter）] を選択します。

ステップ 6 [ポータル ユーザー（Portal User）] フィールドにユーザーの名前を入力して、その特定のユーザーに割り当てられたエンドポイントのみを表示します。

デバイスをデバイス ポータルに追加するときのエラー

従業員は、別の従業員がすでに追加したサービスを追加することはできません。デバイスは引き続きエンドポイント データベースに含まれます。

Cisco ISE データベースにすでに存在しているデバイスを従業員が追加しようとした場合：

- デバイスがネイティブサプリカントのプロビジョニングをサポートしている場合は、BYOD ポータルからデバイスを追加することを推奨します。この場合、デバイスがネットワークに最初に追加されたときに作成された登録詳細がすべて上書きされます。
- デバイスがプリンタなどのMAC認証バイパス（MAB）デバイスである場合は、デバイスの所有権を最初に解決する必要があります。必要に応じて、管理者のポータルを使用してエンドポイントデータベースからデバイスを削除できます。これにより、新しい所有者は、マイデバイスポータルを使用して正常にデバイスを追加できます。

（注） 管理者ポータルがダウンしている場合、デバイス ポータルは使用できません。

デバイス ポータルから削除されたデバイスはエンドポイント データベースに残っている

従業員が [デバイス（My Devices）] ポータルからデバイスを削除すると、そのデバイスは従業員の登録済みデバイスのリストから削除されますが、Cisco ISE エンドポイントデータベースには残っており、[エンドポイント（Endpoints）] のリストに表示されます。

[エンドポイント（Endpoints）] ウィンドウからデバイスを完全に削除できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** です。

従業員が登録するパーソナル デバイス数の制限

従業員が 1 ～ 999 のパーソナル デバイスを登録できるようにすることができます。従業員がパーソナルデバイスの登録に使用したポータルに関係なく、この設定では、すべてのポータルにわたって登録されるデバイスの最大数を定義します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）]** を選択します。

ステップ 2 [従業員を制限（Restrict employees to）] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は **5** デバイスに設定されています。

ステップ 3 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

デバイス ポータルおよびエンドポイント アクティビティのモニター

Cisco ISE は、エンドポイントおよびユーザー管理情報、およびゲストとスポンサーのアクティビティを参照できるさまざまなレポートとログを提供します。

オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]**。

ステップ 2 [ゲスト（Guest）] または [エンドポイントとユーザー（Endpoints and Users）] を選択して、さまざまなゲスト、スポンサー、およびエンドポイント関連のレポートを表示します。

ステップ 3 [フィルタ（Filters）] ドロップダウンリストを使用して検索するデータを選択します。

ステップ 4 データを表示する [時間範囲（Time Range）] を選択します。

ステップ 5 [実行（Run）] をクリックします。

デバイス ログインおよび監査レポート

[デバイスログインと監査（My Devices Login and Audit）] レポートは、次を追跡する統合レポートです。

- [デバイス（My Devices）] ポータルでの従業員によるログイン アクティビティ。
- [デバイス（My Devices）] ポータルで従業員が実行したデバイス関連の操作。

このレポートは、**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[ゲスト（Guest）]** > **[デバイスログインと監査（My Devices Login and Audit）]** で使用できます。

登録済みエンドポイント レポート

[登録済みエンドポイント（Registered Endpoints）] のレポートには、従業員によって登録されたすべてのエンドポイントに関する情報が表示されます。このレポートは、**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート(Reports)]** > **[エンドポイントとユーザー（Endpoints and Users）]** > **[登録済みエンドポイント（Registered Endpoints）]** で使用できます。[ID（Identity）]、[エンドポイント ID（Endpoint ID）]、[ID グループ（Identity Group）]、[エンドポイントプロファイル（Endpoint Profile）] などの属性でフィルタ処理してレポートを生成できます。

[登録済みデバイス（Registered Devices）] エンドポイント ID グループに割り当てられているエンドポイントについて、エンドポイントデータベースに照会できます。また、[ポータルユー

ザー（Portal User）] 属性がヌル以外の値に設定されている特定のユーザーについてはレポートを生成することもできます。

[登録済みエンドポイント（Registered Endpoints）] のレポートには、特定のユーザーによって指定の期間内にデバイス登録ポータルから登録されたエンドポイントのリストに関する情報が表示されます。

第 11 章

セキュアなアクセス

- Cisco ISE でのネットワークデバイスの定義 （1365 ページ）
- Cisco ISE でのサードパーティ ネットワーク デバイスのサポート （1389 ページ）
- ネットワーク デバイス グループの管理 （1398 ページ）
- ネットワーク デバイス グループ （1400 ページ）
- Cisco ISE でのテンプレートのインポート （1404 ページ）
- Cisco ISE と NAD 間の通信を保護する IPSec セキュリティ （1409 ページ）
- Mobile Device Manager と Cisco ISE との相互運用性 （1416 ページ）
- Cisco ISE を使用したモバイルデバイス管理サーバーのセットアップ （1426 ページ）
- サービスとしての Cisco Private 5G の設定 （1449 ページ）
- サービスとしての Cisco Private 5G の設定 （1453 ページ）

Cisco ISE でのネットワークデバイスの定義

スイッチやルータなどのネットワークデバイスは、認証、許可、およびアカウンティング（AAA）クライアントであり、Cisco ISE に AAA サービス要求を送信します。Cisco ISE でネットワークデバイスを定義すると、Cisco ISE とネットワークデバイス間の連携動作が有効になります。

ネットワークデバイスを RADIUS または TACACS AAA に設定したり、プロファイリングサービスでプロファイリング エンドポイントの Cisco Discovery Protocol 属性および Link Layer Discovery Protocol（LLDP）属性を収集するための Simple Network Management Protocol（SNMP）を設定したり、Cisco TrustSec デバイスの TrustSec 属性を設定したりします。Cisco ISE に定義されていないネットワーク デバイスは、Cisco ISE から AAA サービスを受信できません。

Cisco ISE のメインメニューで、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** を選択し、[追加（Add）] をクリックします。表示される [新しいネットワークデバイス（New Network Device）] ウィンドウで、次の詳細を入力してネットワークデバイスを定義します。

- ネットワークデバイスに応じたベンダープロファイルを選択します。プロファイルには、URL リダイレクトや許可変更の設定などの、デバイスに事前に定義された設定が含まれています。

- RADIUS 認証用の RADIUS プロトコルを設定します。Cisco ISE はネットワークデバイスから RADIUS 要求を受信すると、対応するデバイス定義を探して設定されている共有秘密を取得します。Cisco ISE はデバイス定義を検出すると、デバイスに設定されている共有秘密を取得し、それを要求内の共有秘密と照合してアクセスを認証します。共有秘密が一致すると、RADIUS サーバーは、ポリシーと設定に基づいて要求をさらに処理します。共有秘密が一致しない場合は、拒否応答がネットワークデバイスに送信されます。失敗した認証レポートが生成され、失敗の理由が示されます。
- TACACS+ 認証用の TACACS+ プロトコルを設定します。Cisco ISE はネットワーク デバイスから TACACS+ 要求を受信すると、対応するデバイス定義を探して設定されている共有秘密を取得します。デバイス定義が見つかった場合、デバイスに設定されている共有秘密を取得し、それを要求内の共有秘密と照合してアクセスを認証します。共有秘密が一致すると、TACACS+ サーバーは、ポリシーと設定に基づいて要求をさらに処理します。一致しない場合は、拒否応答がネットワーク デバイスに送信されます。失敗した認証レポートが生成され、失敗の理由が示されます。
- プロファイリング サービスがネットワーク デバイスと通信し、ネットワーク デバイスに接続されているエンドポイントをプロファイリングするように、ネットワーク デバイス定義で簡易ネットワーク管理プロトコル（SNMP）を設定できます。
- Cisco TrustSec ソリューションの一部となる可能性がある TrustSec 対応デバイスからの要求を処理するには、Cisco ISE 内に Cisco TrustSec 対応デバイスを定義する必要があります。Cisco TrustSec ソリューションをサポートするスイッチはすべて Cisco TrustSec 対応デバイスです。

  Cisco TrustSec デバイスでは IP アドレスは使用されません。代わりに、Cisco TrustSec デバイスが Cisco ISE と通信できるように、その他の設定を定義する必要があります。

  Cisco TrustSec 対応デバイスは Cisco ISE との通信に TrustSec 属性を使用します。Cisco Nexus 7000 シリーズ スイッチ、Cisco Catalyst 6000 シリーズ スイッチ、Cisco Catalyst 4000 シリーズ スイッチ、Cisco Catalyst 3000 シリーズ スイッチなどの Cisco TrustSec 対応デバイスは、Cisco TrustSec デバイスの追加時に定義した Cisco TrustSec 属性を使用して認証されます。

（注） Cisco ISE でネットワークデバイスを設定する際には、共有秘密の一部としてバックスラッシュ（\）を含めないことをお勧めします。これは、Cisco ISE をアップグレードすると、共有秘密にバックスラッシュが表示されなくなるためです。ただし、Cisco ISE をアップグレードせずに再イメージ化すると、共有秘密にバックスラッシュが表示されます。

Cisco ISE でのデフォルト ネットワーク デバイスの定義

Cisco ISE では、RADIUS および TACACS 認証のデフォルトのデバイス定義がサポートされています。特定の IP アドレスのデバイス定義が見つからない場合、Cisco ISE で使用できるデフォルトのネットワーク デバイスを定義することができます。この機能を使用すると、新しくプロビジョニングされたデバイスのデフォルトの RADIUS または TACACS 共有秘密とアクセス レベルを定義できます。

（注） 基本的な RADIUS および TACACS 認証のみにデフォルトのデバイス定義を追加することを推奨します。高度なフローについては、ネットワークデバイスごとに個別のデバイス定義を追加する必要があります。

Cisco ISE は、ネットワーク デバイスから RADIUS または TACACS 要求を受信すると、対応するデバイス定義を検索して、ネットワーク デバイス定義に設定されている共有秘密を取得します。

RADIUS または TACACS 要求が受信されると、Cisco ISE は次の手順を実行します。

1. 要求内の IP アドレスに一致する特定の IP アドレスを探します。
2. 範囲を調べて、要求内の IP アドレスが指定された範囲内にあるかどうかを確認します。
3. ステップ 1 と 2 の両方が失敗すると、要求の処理にデフォルトのデバイス定義（定義されている場合）が使用されます。

Cisco ISE は、そのデバイスのデバイス定義に設定されている共有秘密を取得し、それを RADIUS または TACACS 要求内の共有秘密と照合してアクセスを認証します。デバイス定義が見つからない場合、Cisco ISE はデフォルトのネットワーク デバイス定義から共有秘密を取得し、RADIUS または TACACS 要求を処理します。

ネットワーク デバイス

後続の項で説明されているウィンドウを使用して、Cisco ISE でネットワークデバイスを追加および管理できます。

ネットワーク デバイス定義の設定

次の表では、Cisco ISE のネットワーク アクセス デバイスを設定するために使用できる [ネットワークデバイス（Network Devices）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** で、**[追加（Add）]** をクリックします。

ネットワーク デバイスの設定

次の表では、**[新しいネットワークデバイス（New Network Devices）]** ウィンドウのフィールドについて説明します。

表 *117*：ネットワーク デバイスの設定

フィールド名	説明
名前（**Name**）	ネットワークデバイスの名前を入力します。 ネットワークデバイスに、デバイスのホスト名とは異なるわかりやすい名前を指定できます。デバイス名は論理識別子です。 （注）　必要に応じて、設定後にデバイスの名前を変更できます。
説明（**Description**）	このデバイスの説明を入力します。
IP アドレス（IP Address）または **IP 範囲（IP Range）**	ドロップダウンリストから次のいずれかを選択し、表示されるフィールドに必要な値を入力します。 • [IP アドレス（IP Address）]：単一の IP アドレス（IPv4 または IPv6 アドレス）とサブネットマスクを入力します。 • [IP 範囲（IP Ranges）]：必要な IPv4 アドレスの範囲を入力します。認証時に IP アドレスを除外するには、[除外（Exclude）] フィールドに IP アドレスまたは IP アドレスの範囲を入力します。 IP アドレスとサブネットマスクまたは IP アドレスの範囲を定義するためのガイドラインを次に示します。 • 特定の IP アドレスを定義するか、サブネットマスクを使用して IP 範囲を定義できます。デバイス A の IP アドレス範囲が定義されている場合、デバイス A に定義されている範囲の個別のアドレスを別のデバイス B に設定できます。 • すべてのオクテットの IP アドレス範囲を定義できます。IP アドレスの範囲を指定するときに、ハイフン（-）またはアスタリスク（*）をワイルドカードとして使用できます。たとえば、*.*.*.*、1-10.1-10.1-10.1-10 または 10-11.*.5.10-15 などです。 • サブセットがすでに追加されている場合は、設定された範囲からその IP アドレス範囲のサブセットを除外できます。例：10.197.65.*/10.197.65.1 または 10.197.65.* exclude 10.197.65.1。 • ネットワークデバイスごとに最大 40 の IP アドレス、または IP 範囲を設定できます。 • 同じ IP アドレスを持つ 2 台のデバイスを定義することはできません。 • 同じ IP 範囲を持つ 2 台のデバイスを定義することはできません。IP 範囲は、一部または全部が重複することはできません。 • IP アドレスを除外する場合は、重複する IP 範囲を使用しないでください。代わりに、独立した IP 範囲を除外してください。

フィールド名	説明
デバイスプロファイル（Device Profile）	ドロップダウンリストから、ネットワークデバイスのベンダーを選択します。 選択したベンダーのネットワークデバイスがサポートしているフローおよびサービスを表示するには、ドロップダウンリストの横にあるツールのヒントを使用します。ツールのヒントには、デバイスが使用する URL リダイレクトの RADIUS 認可変更（CoA）ポートとタイプも表示されます。これらの属性は、デバイス タイプのネットワーク デバイス プロファイルで定義されます。
モデル名（Model Name）	ドロップダウンリストからデバイスのモデルを選択します。 モデル名は、ルールベースのポリシーの条件をチェックするときに、パラメータの1つとして使用します。この属性は、デバイスディクショナリにあります。
ソフトウェアバージョン（Software Version）	ドロップダウンリストから、ネットワークデバイスで実行するソフトウェアのバージョンを選択します。 ソフトウェア バージョンは、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性は、デバイスディクショナリにあります。
ネットワーク デバイス グループ（Network Device Group）	[ネットワークデバイスグループ（Network Device Group）]領域で、[ロケーション（Location）]、**[IPSec]**、および[デバイスタイプ（Device Type）]ドロップダウンリストから必要な値を選択します。 グループに明確にデバイスを割り当てないと、そのグループはデフォルトのデバイスグループ（ルート ネットワーク デバイス グループ）に含まれます。これにより、ロケーションは [すべてのロケーション（All Locations）]、デバイスタイプは [すべてのデバイスタイプ（All Device Types）] となります。

（注） フィルタを使用して Cisco ISE 展開からネットワーク アクセス デバイス（NAD）を選択して削除する場合は、ブラウザのキャッシュをクリアして、選択した NAD のみが削除されるようにします。

RADIUS 認証設定

次の表では、[RADIUS 認証設定（RADIUS Authentication Settings）] 領域のフィールドについて説明します。

表 *118 : [RADIUS* 認証設定（*RADIUS Authentication Settings*）*]* 領域

フィールド名	使用上のガイドライン
RADIUS UDP の設定	
プロトコル（**Protocol**）	選択したプロトコルとして **RADIUS** を表示します。
共有秘密鍵（**Shared Secret**）	ネットワーク デバイスの共有秘密鍵を入力します。 共有秘密鍵は、**pac** オプションを指定した **radius-host** コマンドを使用してネットワークデバイスに設定したキーです。 （注） 共有秘密鍵の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ウィンドウ（[管理（Administration）]>[ネットワークリソース（Network Resources）]>[ネットワークデバイス（Network Devices）]>[デバイスセキュリティ設定（Device Security Settings）]）の [RADIUS 共有秘密鍵の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります。 RADIUS サーバーでのベストプラクティスは、22 文字にすることです。新規インストールおよびアップグレードされた展開の場合、共有秘密鍵の長さはデフォルトで4 文字です。この値は [デバイスセキュリティ設定（Device Security Settings）] ウィンドウで変更できます。

フィールド名	使用上のガイドライン
2 番目の共有秘密の使用（Use Second Shared Secret）	ネットワークデバイスと Cisco ISE で使用される 2 番目の共有秘密鍵を指定します。 （注） Cisco TrustSec デバイスには、デュアル共有秘密（鍵）の利点がありますが、Cisco ISE により送信される Cisco TrustSec CoA パケットは常に最初の共有秘密（鍵）を使用します。2 番目の共有秘密鍵の使用を有効にするには、Cisco TrustSec CoA パケットを Cisco TrustSec デバイスに送信する Cisco ISE ノードを選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources }] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [高度な TrustSec 設定（Advanced Trustsec Settings）]** ウィンドウの [送信元（Send From）] ドロップダウンリストで、このタスクに使用する Cisco ISE ノードを設定します。プライマリ管理ノード（PAN）またはポリシーサービスノード（PSN）を選択できます。選択した PSN ノードがダウンしている場合、PAN は Cisco TrustSec デバイスに Cisco TrustSec CoA パケットを送信します。 （注） RADIUS アクセス要求の 2 番目の共有秘密機能は、[Message-Authenticator] フィールドを含むパケットに対してのみ機能します。
CoA ポート（CoA Port）	RADIUS CoA に使用するポートを指定します。 デバイスのデフォルトの CoA ポートは、ネットワークデバイス用に設定されたネットワーク デバイス プロファイルで定義されます（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）]**）。デフォルト CoA ポートを使用するには、[デフォルトに設定（Set To Default）] をクリックします。 （注） [RADIUS 認証設定（RADIUS Authentication Settings）] の **[ネットワークデバイス（Network Devices）]** ウィンドウ（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]**）で指定した CoA ポートを変更する場合は、**[ネットワークデバイスプロファイル（Network Device Profile）]** ウィンドウ（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）]**）で対応するプロファイルに同じ CoA ポートを指定します。
RADIUS DTLS の設定	

フィールド名	使用上のガイドライン
必要な DTLS（DTLS Required）	[必要な DTLS（DTLS Required）] チェックボックスをオンにすると、Cisco ISE ではこのデバイスからの DTLS 要求のみが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS はセキュアソケットレイヤ（SSL）トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、Message Digest 5（MD5）完全性チェックを計算するために使用されます。
CoA ポート（CoA Port）	RADIUS DTLS CoA に使用するポートを指定します。
CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）	ドロップダウンリストから RADIUS DTLS CoA に使用する認証局を選択します。
DNS 名（DNS Name）	ネットワーク デバイスの DNS 名を入力します。[RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification）] オプションが [RADIUS 設定（RADIUS Settings）] ウィンドウ（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[RADIUS]**）で有効になっている場合、Cisco ISE はこの DNS 名とクライアント証明書で指定されている DNS 名を比較して、ネットワークデバイスの ID を確認します。
全般設定	
KeyWrap の有効化（Enable KeyWrap）	KeyWrap アルゴリズムがネットワークデバイスでサポートされている場合にのみ、[KeyWrap の有効化（Enable KeyWrap）] チェックボックスをオンにします。ネットワークデバイスは、AES KeyWrap RFC（RFC 3394）と互換性がある必要があります。 このオプションは、AES KeyWrap アルゴリズムを介して RADIUS セキュリティを強化するために使用されます。
キー暗号キー（Key Encryption Key）	セッションの暗号化（秘密）に使用される暗号キーを入力します。

フィールド名	使用上のガイドライン
メッセージ オーセンティケータ コード キー（**Message Authenticator Code Key**）	RADIUS メッセージに対するキー付きハッシュメッセージ認証コード（HMAC）の計算に使用されるキーを入力します。
キー入力形式（**Key Input Format**）	次のいずれかのオプション ボタンをクリックします。 • [ASCII]：[キー暗号キー（Key Encryption Key）] フィールドに入力する値の長さは16文字（バイト）、[メッセージ認証コードキー（Message Authenticator Code Key）] フィールドに入力する値の長さは 20 文字（バイト）にする必要があります。 • [16 進数（Hexadecimal）]：[キー暗号キー（Key Encryption Key）] フィールドに入力する値の長さは 32 文字（バイト）、[メッセージ認証コードキー（Message Authenticator Code Key）] フィールドに入力する値の長さは 40 文字（バイト）にする必要があります。 ネットワークデバイスの設定と一致するように、キー暗号キーおよびメッセージ認証コードキーの入力に使用するキー入力形式を指定できます。指定する値はキーの正しい（全体の）長さにする必要があり、それよりも短い値は許可されません。

TACACS 認証設定

表 *119 : [TACACS* 認証設定（*TACACS Authentication Settings*）*]* 領域のフィールド

フィールド名	使用上のガイドライン
共有秘密鍵（**Shared Secret**）	TACACS+ プロトコルが有効のときにネットワークデバイスに割り当てられたテキストの文字列。ユーザーは、ネットワークデバイスによってユーザー名およびパスワードが認証される前にテキストを入力する必要があります。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。
廃止された共有秘密がアクティブです（**Retired Shared Secret is Active**）	リタイアメント期間がアクティブな場合に表示されます。
廃止（**Retire**）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、ダイアログボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。

フィールド名	使用上のガイドライン
残りの廃止期間（Remaining Retired Period）	（[廃止（Retire）] ダイアログボックスで [はい（Yes）] を選択した場合にのみ利用可能）**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[設定（Settings）]** > **[接続設定（Connection Settings）]** > **[デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]** で指定されたデフォルト値が表示されます。必要に応じて、デフォルト値を変更できます。 古い共有秘密は、指定された日数の間はアクティブなままになります。
終了（End）	（[廃止（Retire）] ダイアログボックスで [はい（Yes）] をクリックした場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。
シングル接続モードを有効にする（Enable Single Connect Mode）	[シングル接続モードを有効にする（Enable Single Connect Mode）] チェックボックスは、ネットワークデバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかのオプションボタンをクリックします。 • **[レガシーシスコデバイス（Legacy Cisco Devices）]** • **[TACACS ドラフトコンプライアンスシングル接続のサポート（TACACS Draft Compliance Single Connect Support）]** （注） [シングル接続モード（Single Connect Mode）] を無効にすると、Cisco ISE はすべての TACACS 要求に対して新しい TCP 接続を使用します。

SNMP 設定

次の表では、[SNMP 設定（SNMP Settings）] セクションのフィールドについて説明します。

表 *120 : [SNMP*設定（*SNMP Settings*）*]* 領域のフィールド

フィールド名	使用上のガイドライン
SNMP バージョン（SNMP Version）	[SNMP バージョン（SNMP Version）] ドロップダウンリストから、次のいずれかのオプションを選択します。 • **1**：SNMPv1 は informs をサポートしていません。 • **2c** • 3：SNMPv3 は、[セキュリティ レベル（Security Level）] フィールドで [Priv] を選択した場合にパケットの暗号化が可能であるため、最もセキュアなモデルです。 （注） ネットワークデバイスに SNMPv3 パラメータを設定した場合、モニタリングサービス（**[操作（Operations）]** > **（[レポート（Reports）]** > **[診断（Diagnostics）]** > **[ネットワークデバイスセッションステータス（Network Device Session Status）]**）によって提供される [ネットワーク デバイス セッション ステータス（Network Device Session Status）] 概要レポートを生成できません。ネットワークデバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。
SNMP RO コミュニティ（SNMP RO Community）	（SNMP バージョン 1 および 2c にのみ適用可能）Cisco ISE にデバイスへの特定タイプのアクセスを提供する読み取り専用コミュニティ文字列を入力します。 （注） キャレット記号（曲折アクセント付き^）は使用できません。
SNMP ユーザー名（SNMP Username）	（SNMP バージョン 3 の場合のみ）SNMP ユーザー名を入力します。
セキュリティ レベル（Security Level）	（SNMP バージョン 3 の場合のみ）[セキュリティ レベル（Security Level）] ドロップダウンリストから次のオプションのいずれかを選択します。 • **[Auth]**：MD5 またはセキュア ハッシュ アルゴリズム（SHA）パケットの認証を有効にします。 • **[No Auth]**：認証なし、プライバシーなしのセキュリティ レベル。 • **[Priv]**：Data Encryption Standard（DES; データ暗号規格）パケットの暗号化を有効にします。

フィールド名	使用上のガイドライン
認証プロトコル（**Auth Protocol**）	（SNMP バージョン 3 でセキュリティレベル [Auth] または [Priv] を選択した場合のみ）[認証プロトコル（Auth Protocol）] ドロップダウンリストから、ネットワークデバイスで使用する認証プロトコルを選択します。 • **[MD5]** • **[SHA]**
認証パスワード（**Auth Password**）	（SNMP バージョン 3 で [Auth] および [Priv] セキュリティレベルを選択した場合のみ）認証キーを入力します。8 文字以上の長さにする必要があります。 デバイスにすでに設定されている認証パスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き^）を使用することはできません。
プライバシー プロトコル（**Privacy Protocol**）	（SNMP バージョン 3 で [Priv] セキュリティレベルを選択した場合のみ）[プライバシープロトコル（Privacy Protocol）] ドロップダウンリストから次のいずれかのオプションを選択します。 • **DES** • **AES128** • **AES192** • **AES256** • **3DES**
プライバシー パスワード（**Privacy Password**）	（SNMP バージョン 3 で [Priv] セキュリティレベルを選択した場合のみ）プライバシーキーを入力します。 デバイスにすでに設定されているプライバシーパスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き^）を使用することはできません。
ポーリング間隔（**Polling Interval**）	ポーリング間隔を秒単位で入力します。デフォルト値は 3600 です。
リンク トラップ クエリー（**Link Trap Query**）	SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、[リンクトラップクエリ（Link Trap Query）] チェックボックスをオンにします。

フィールド名	使用上のガイドライン
MAC トラップ クエリ（MAC Trap Query）	SNMP トラップを介して受信する MAC 通知を受信して解釈するには、[MAC トラップクエリ（MAC Trap Query）] チェックボックスをオンにします。
送信元ポリシー サービス ノード（Originating Policy Services Node）	[送信元ポリシーサービスノード（Originating Policy Services Node）] ドロップダウンリストから、SNMP データのポーリングに使用する Cisco ISE サーバーを選択します。このフィールドのデフォルト値は [自動（Auto）] です。ドロップダウンリストから特定の値を選択して、設定を上書きします。

高度な TrustSec 設定

次の表は、[高度なTrustSec設定（Advanced TrustSec Settings）] セクションのフィールドについて説明しています。

表 *121 : [*高度な *TrustSec* 設定（*Advanced TrustSec Settings*）*]* 領域のフィールド

フィールド名	使用上のガイドライン
デバイスの認証設定	
TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）	[デバイスID（Device ID）] フィールドにデバイス ID としてデバイス名をリストするには、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスをオンにします。
デバイスID（Device ID）	このフィールドは、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスがオフになっている場合にのみ使用できます。
パスワード（Password）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
HTTP REST API の設定	
HTTP REST API の有効化（Enable HTTP REST API）	HTTP REST API を使用して、ネットワークデバイスに必要な Cisco TrustSec 情報を提供するには、[HTTP REST API の有効化（Enable HTTP REST API）]チェックボックスをオンにします。これにより、効率性と能力が向上し、RADIUS プロトコルと比較して、短時間で大規模な設定をダウンロードできます。また、UDP を介した TCP を使用することで、信頼性が向上します。

フィールド名	使用上のガイドライン
ユーザー名（**Username**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したユーザー名を入力します。ユーザー名にスペース、!%^:;、[{}] ' "=<>? を含めることはできません
パスワード（**Password**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。
TrustSec デバイスの通知および更新	
デバイスID（**Device ID**）	このフィールドは、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスがオフになっている場合にのみ使用できます。
パスワード（**Password**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
環境データのダウンロード間隔 <...>（**Download Environment Data Every <...>**）	この領域のドロップダウンリストから必要な値を選択して、デバイスが Cisco ISE から環境データをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で選択できます。デフォルト値は 1 日です。
ピア許可ポリシーのダウンロード間隔 <...>（**Download Peer Authorization Policy Every <...>**）	デバイスが Cisco ISE からピア認証ポリシーをダウンロードする必要がある時間間隔を、この領域のドロップダウンリストから必要な値を選択して指定します。時間間隔を秒、分、時、日数、または週数で指定できます。デフォルト値は 1 日です。
再認証間隔 <...>（**Reauthentication Every <...>**）	この領域のドロップダウンリストから必要な値を選択して、最初の認証後、デバイスが Cisco ISE に対して自身を再認証する時間間隔を指定します。時間間隔は秒、分、時、日、または週で設定できます。たとえば 1000 秒と入力すると、デバイスは 1000 秒ごとに Cisco ISE に対して自身を認証します。デフォルト値は 1 日です。
SGACL リストのダウンロード間隔 <...>（**Download SGACL Lists Every <...>**）	この領域のドロップダウンリストから必要な値を選択して、デバイスが Cisco ISE から SGACL リストをダウンロードする時間間隔を指定します。時間間隔は秒、分、時、日、または週で設定できます。デフォルト値は 1 日です。

フィールド名	使用上のガイドライン
その他の TrustSec デバイスでこのデバイスを信頼する（信頼できる TrustSec）（Other TrustSec Devices to Trust This Device (TrustSec Trusted)）	すべてのピアデバイスがこの Cisco TrustSec デバイスを信頼できるようにするには、[このデバイスを信頼する他の TrustSec デバイス（Other TrustSec Devices to Trust This Device）] チェックボックスをオンにします。このチェックボックスをオフにした場合、ピアデバイスはこのデバイスを信頼せず、このデバイスから到着したすべてのパケットが適宜色付けまたはタグ付けされます。
設定変更のデバイスへの送信（Send Configuration Changes to Device）	Cisco ISE で CoA または CLI（SSH）を使用して Cisco TrustSec 構成変更を Cisco TrustSec デバイスに送信する場合は、[構成変更のデバイスへの送信（Send Configuration Changes to Device）] チェックボックスをオンにします。必要に応じて、[CoA] または [CLI（SSH）（CLI (SSH)）] オプションボタンをクリックします。 Cisco ISE で CoA を使用して設定変更を Cisco TrustSec デバイスに送信する場合は、[CoA] オプションボタンをクリックします。 Cisco ISE で CLI を使用（SSH 接続を使用）して設定変更を Cisco TrustSec デバイスに送信するには、[CLI（SSH）（CLI (SSH)）] オプションボタンをクリックします。詳細については、非 CoA サポート デバイスへの設定変更のプッシュ（1647 ページ）を参照してください。
送信元（Send From）	ドロップダウンリストから、設定変更を Cisco TrustSec デバイスに送信する必要がある送信元 Cisco ISE ノードを選択します。PAN または PSN を選択できます。選択した PSN がダウンした場合、PSN を使用して Cisco TrustSec デバイスに設定変更が送信されます。
テスト接続（Test Connection）	Cisco TrustSec デバイスと選択した Cisco ISE ノード（PAN または PSN ノード）の間の接続をテストするには、このオプションを使用できます。
SSH キー（SSH Key）	この機能を使用するには、Cisco ISE からネットワーク デバイスへの SSHv2 トンネルを開き、デバイスの CLI を使用して SSH キーを取得します。確認のために、このキーをコピーして [SSHキー（SSH Key）] フィールドに貼り付ける必要があります。詳細については、SSH キーの検証（1647 ページ）を参照してください。
デバイス構成の展開	

フィールド名	使用上のガイドライン
セキュリティ グループ タグ マッピングの展開時にこのデバイスを含める（**Include this device when deploying Security Group Tag Mapping Updates**）	Cisco TrustSec デバイスがデバイスインターフェイスのログイン情報を使用して IP-SGT マッピングを取得するには、[セキュリティ グループ タグ マッピングの更新の展開時にこのデバイスを含める（Include this device when deploying Security Group Tag Mapping Updates）] チェックボックスをオンにします。
EXEC モード ユーザー名（EXEC Mode Username）	Cisco TrustSec デバイスへのログインに使用するユーザー名を入力します。
EXEC モード パスワード（EXEC Mode Password）	デバイス パスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。 （注） セキュリティの脆弱性を回避するために、EXEC モードやイネーブルモードのパスワードを含むパスワードの文字に % を使用しないことを推奨します。
有効モード パスワード（Enable Mode Password）	（任意）特権 EXEC モードで Cisco TrustSec デバイスの設定を編集するために使用する有効なパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
アウトオブバンドTrustSec PAC	
発行日（Issue Date）	この Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の発行日を表示します。
期限日（Expiration Date）	この Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の期限日を表示します。
発行元（Issued By）	このデバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行者（Cisco TrustSec 管理者）の名前を表示します。
PAC の生成（Generate PAC）	Cisco TrustSec デバイスのアウトオブバンド Cisco TrustSec PAC を生成するには、[PACの生成（Generate PAC）] ボタンをクリックします。

デフォルトのネットワーク デバイス定義の設定

次の表では、Cisco ISE が RADIUS または TACACS+ 認証に使用できる、デフォルトのネットワークデバイスを設定できるようにする [デフォルトのネットワークデバイス（Default Network device）] ウィンドウのフィールドについて説明します。次のナビゲーションパスのいずれかを選択します。

- **[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デフォルトのデバイス（Default Devices）]**
- **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク ソース（Network Resources）] > [デフォルトのデバイス（Default Devices）]**

表 *122 : [*デフォルトのネットワークデバイス（***Default Network Device***）*]* ウィンドウのフィールド

フィールド名	使用上のガイドライン
デフォルトのネットワーク デバイスのステータス（Default Network Device Status）	デフォルトのネットワークデバイスの定義を有効にするには、[デフォルトのネットワークデバイスのステータス（Default Network Device Status）] ドロップダウンリストから [有効化（Enable）] を選択します。 （注） デフォルトのデバイスが有効になっている場合は、ウィンドウ内の関連するチェックボックスをオンにすることで、RADIUS または TACACS+ の認証設定を有効にする必要があります。
デバイス プロファイル（Device Profile）	デフォルトのデバイスベンダーとして [シスコ（Cisco）] が表示されます。
RADIUS 認証設定	
RADIUS の有効化（Enable RADIUS）	デバイスの RADIUS 認証を有効にするには、[RADIUS の有効化（Enable RADIUS）] チェックボックスをオンにします。
RADIUS UDP の設定	

フィールド名	使用上のガイドライン
共有秘密鍵（Shared Secret）	共有秘密を入力します。共有秘密情報の長さは、最大 127 文字です。 共有秘密鍵は、pac キーワードを指定した radius-host コマンドを使用してネットワークデバイスに設定したキーです。 （注） 共有秘密の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ウィンドウ（**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** > **[デバイスのセキュリティ設定（Device Security Settings）]**）の [RADIUS 共有秘密の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります。デフォルトでは、この値は新規インストールとアップグレードされた展開の場合は4文字です。RADIUS サーバーでのベストプラクティスは、22 文字にすることです。
RADIUS DTLS の設定	
必要な DTLS（DTLS Required）	[必要な DTLS（DTLS Required）] チェックボックスをオンにすると、Cisco ISE ではこのデバイスからの DTLS 要求のみが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。
CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）	RADIUS DTLS CoA に使用する認証局を [CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）] ドロップダウンリストから選択します。
全般設定	
KeyWrap の有効化（Enable KeyWrap）	（任意）KeyWrap アルゴリズムがネットワークデバイスでサポートされている場合にのみ [KeyWrap の有効化（Enable KeyWrap）] チェックボックスをオンにします。これにより AES KeyWrap アルゴリズムを介した RADIUS のセキュリティが強化されます。
キー暗号キー（Key Encryption Key）	KeyWrap を有効にした場合は、セッションの暗号化（秘密）に使用する暗号キーを入力します。

フィールド名	使用上のガイドライン
メッセージ オーセンティケータ コード キー（**Message Authenticator Code Key**）	KeyWrapを有効にしているときに、RADIUSメッセージに対するキー付きHashed Message Authentication Code（HMAC）の計算に使用されるキーを入力します。
キー入力形式（**Key Input Format**）	対応するオプションボタンをクリックして次のいずれかの形式を選択し、[キー暗号化キー（Key Encryption Key）]フィールドと[メッセージ認証コードキー（Message Authenticator Code Key）]フィールドに値を入力します。 • [ASCII]：**キー暗号化キー**の長さは16文字（バイト）、**メッセージ オーセンティケータ コード キー**の長さは20文字（バイト）である必要があります。 • [16進数（Hexadecimal）]：キー暗号化キーの長さは32バイト、メッセージオーセンティケータ コードキーの長さは40バイトである必要があります。 ネットワークデバイスの設定と一致するように、キー暗号キーおよびメッセージ認証コードキーの入力に使用するキー入力形式を指定します。指定する値はキーの正しい（全体の）長さにする必要があります。それよりも短い値は許可されません。
TACACS 認証設定	
共有秘密鍵（**Shared Secret**）	TACACS+プロトコルが有効のときにネットワークデバイスに割り当てるテキスト文字列を入力します。ユーザーはネットワークデバイスによってユーザー名およびパスワードが認証される前にテキストを入力する必要があることに注意してください。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。
廃止された共有秘密がアクティブです（**Retired Shared Secret is Active**）	リタイアメント期間がアクティブな場合に表示されます。
廃止（**Retire**）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）]をクリックすると、ダイアログボックスが表示されます。[はい（Yes）]または[いいえ（No）]をクリックします。

フィールド名	使用上のガイドライン
残りの廃止期間（Remaining Retired Period）	（任意）[廃止（Retire）] ダイアログボックスで [はい（Yes）] をクリックした場合にのみ使用できます。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[設定（Settings）]** > **[接続設定（Connection Settings）]** > **[デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]** ウィンドウで指定されたデフォルト値が表示されます。デフォルト値は変更することができます。 これにより、新しい共有秘密を入力できます。古い共有秘密は、指定された日数の間はアクティブなままになります。
終了（End）	（任意）[残りの廃止期間（Remaining Retired Period）] ダイアログボックスで [はい（Yes）] を選択した場合にのみ使用できます。廃止期間が終了し、古い共有秘密の設定は解除されます。
シングル接続モードを有効にする（Enable Single Connect Mode）	[シングル接続モードを有効にする（Enable Single Connect Mode）] チェックボックスは、ネットワークデバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかのオプションボタンをクリックします。 • [レガシーシスコデバイス（Legacy Cisco Devices）] • [TACACS ドラフト コンプライアンス シングル接続のサポート（TACACS Draft Compliance Single Connect Support）] （注） このフィールドを無効にすると、Cisco ISE はすべての TACACS+ 要求に新しい TCP 接続を使用します。

ネットワーク デバイスのインポート設定

次の表では、ネットワークデバイスの詳細を Cisco ISE にインポートするために使用できる [ネットワークデバイスのインポート（Import Network Devices）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]**。[ネットワークデバイス（Network Devices）] ウィンドウで、[インポート（Import）] をクリックします。

表 *123 :* ネットワークデバイスのインポート設定

フィールド名	使用上のガイドライン
テンプレートの生成（Generate a Template）	カンマ区切りの値（CSV）テンプレートファイルを作成するには、[テンプレートの生成（Generate a Template）] をクリックします。 CSV形式のネットワークデバイス情報でテンプレートを更新し、ローカルに保存します。次に、編集したテンプレートを使用して、Cisco ISE展開にネットワークデバイスをインポートします。

フィールド名	使用上のガイドライン
ファイル（**File**）	最近作成したか、または Cisco ISE 展開から以前にエクスポートした CSV ファイルを選択するには、**[ファイルの選択（Choose File）]** をクリックします。 [インポート（Import）] オプションを使用して、新規および更新されたネットワークデバイスの情報を含む別の Cisco ISE 展開にネットワークデバイスをインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワークデバイスをインポートファイル内のデバイスに置き換えるには、[既存のデータを新しいデータで上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポート ファイル内の新しいネットワーク デバイス定義がネットワーク デバイス リポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生したときに Cisco ISE にインポートを中止する場合は、[最初のエラー時にインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。Cisco ISE は、エラーが発生するまでネットワークデバイスをインポートします。 このチェックボックスがオンになっておらず、エラーが発生した場合は、エラーが報告され、Cisco ISE は残りのデバイスを引き続きインポートします。

Cisco ISE でのネットワークデバイスの追加

Cisco ISE でネットワークデバイスを追加したり、デフォルトのネットワークデバイスを使用したりできます。

[ネットワークデバイス（Network Devices）]（**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]**）ウィンドウでもネットワークデバイスを追加できます。

始める前に

追加するネットワークデバイスで AAA 機能を有効にする必要があります。AAA 機能を有効にするコマンド （1944 ページ）を参照してください。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Device）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）]、[説明（Description）]、および [IP アドレス（IP Address）] の各フィールドに対応する値を入力します。

ステップ 4 [デバイスプロファイル（Device Profile）]、[モデル名（Model Name）]、[ソフトウェアバージョン（Software Version）]、および [ネットワーク デバイス グループ（Network Device Group）] ドロップダウンリストから必要な値を選択します。

ステップ 5 （任意）[RADIUS 認証設定（RADIUS Authentication Settings）] チェックボックスをオンにして、RADIUS プロトコル認証を設定します。

ステップ 6 （任意）[TACACS 認証設定（TACACS Authentication Settings）] チェックボックスをオンにして、TACACS プロトコル認証を設定します。

ステップ 7 （オプション）[SNMP の設定（SNMP Settings）] チェックボックスをオンにして、ネットワークデバイスから情報を収集するように Cisco ISE プロファイリングサービスに SNMP を設定します。

ステップ 8 （オプション）TrustSec 対応デバイスを設定するには [高度なTrustSec 設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 9 [送信（Submit）] をクリックします。

Cisco ISE へのネットワーク デバイスのインポート

Cisco ISE がネットワークデバイスと通信できるようにするには、Cisco ISE でネットワークデバイスのデバイス定義を追加する必要があります。**[ネットワークデバイス（Network Devices）]** ウィンドウ（メインメニューから、**[管理（Administration）]**>**[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]**）で、ネットワークデバイスのデバイス定義を Cisco ISE にインポートします。

カンマ区切り形式（CSV）ファイルを使用して、Cisco ISE ノードにデバイス定義のリストをインポートします。[ネットワークデバイス（Network Devices）] ウィンドウで [インポート（Import）] をクリックすると、CSV テンプレートファイルを使用できます。このファイルをダウンロードし、必要なデバイス定義を入力してから、[インポート（Import）] ウィンドウで編集したファイルをアップロードします。

同じリソースタイプの複数のインポートを同時に実行できません。たとえば、2 つの異なるインポート ファイルから同時にネットワーク デバイスをインポートできません。

デバイス定義の CSV ファイルをインポートする場合、新しいレコードを作成するか、[既存のデータを新しいデータで上書きする（Overwrite Existing Data with New Data）] オプションをクリックして既存のレコードを更新できます。

インポートテンプレートは、Cisco ISE ごとに異なる場合があります。異なる Cisco ISE リリースからエクスポートしたネットワークデバイスの CSV ファイルをインポートしないでください。リリースの CSV テンプレートファイルにネットワークデバイスの詳細を入力し、このファイルを Cisco ISE にインポートします。

（注） すべてのオクテットで IP 範囲を持つネットワーク デバイスをインポートできます。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Device）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 表示された [ネットワークデバイスのインポート（Import Network Devices）] ウィンドウで、[テンプレートの生成（Generate A Template）] をクリックして、編集可能な CSV ファイルをダウンロードし、必要な詳細情報とともに Cisco ISE にインポートします。

ステップ 4 [ファイルの選択（Choose Files）] をクリックして、クライアントブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 5 （オプション）必要に応じて、[新しいデータで既存のデータを上書き（Overwrite Existing Data with New Data）] および [最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 6 [インポート（Import）] をクリックします。

ファイルのインポートが完了すると、Cisco ISE には概要メッセージが表示されます。このメッセージには、インポートのステータス（成功または失敗）、発生したエラーの数（ある場合）、およびファイルインポートプロセスにかかった合計処理時間が含まれます。

Cisco ISE からのネットワーク デバイスのエクスポート

Cisco ISE ノードで使用可能なネットワークデバイスのデバイス定義を CSV ファイル形式でエクスポートします。その後、この CSV ファイルを別の Cisco ISE ノードにインポートして必要な Cisco ISE ノードでデバイス定義を使用できるようにします。

（注） すべてのオクテットで IP 範囲を持つネットワーク デバイスをエクスポートできます。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Device）]** を選択します。

ステップ 2 [エクスポート（Export）] をクリックします。

ステップ 3 次のいずれかのアクションを実行して、Cisco ISE ノードに追加されたネットワークデバイスのデバイス定義をエクスポートします。

- エクスポートするデバイスの横にあるチェックボックスをオンにし、[エクスポート（Export）] ドロップダウンリストから [選択済みをエクスポート（Export Selected）] を選択します。
- [エクスポート（Export）] ドロップダウンリストから [すべてエクスポート（Export All）] を選択して、Cisco ISE ノードに追加されたすべてのネットワークデバイスをエクスポートします。

ステップ 4 どちらの場合も、デバイス定義の CSV ファイルがシステムにダウンロードされます。

ネットワーク デバイス設定の問題のトラブルシューティング

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [設定バリデータの評価（Evaluate Configuration Validator）]** を選択します。

ステップ 2 評価するネットワークデバイスの IP アドレスを、[ネットワークデバイス IP（Network Device IP）] フィールドに入力します。

ステップ 3 チェックボックスをオンにして、推奨テンプレートと比較する設定オプションの横にあるオプションボタンをクリックします。

ステップ 4 [実行（Run）] をクリックします。

ステップ 5 [進行状況の詳細…（Progress Details ...）] 領域で、[ここをクリックしてログイン情報を入力（Click Here to Enter Credentials）] をクリックします。

ステップ 6 [ログイン情報ウィンドウ（Credentials Window）] ダイアログボックスで、ネットワークデバイスとの接続を確立するために必要な接続パラメータとログイン情報を入力します。

ステップ 7 [送信 (Submit)] をクリックします。

ステップ 8 （オプション）ワークフローをキャンセルするには、[進行状況の詳細（Progress Details ...）] ウィンドウで [ここをクリックして実行中のワークフローをキャンセル（Click Here to Cancel the Running Workflow）] をクリックします。

ステップ 9 （オプション）分析するインターフェイスの隣にあるチェックボックスをオンにして、[送信（Submit）] をクリックします。

ステップ 10 （オプション）設定の評価の詳細については、[結果概要の表示（Show Results Summary）] をクリックします。

Execute Network Device Command 診断ツール

Execute Network Device Command 診断ツールを使用すると、ネットワーク デバイスに対して **show** コマンドを実行することができます。

表示される結果は、コンソールに表示されるものと同じです。ツールにより、デバイス構成の問題（ある場合）を特定できます。

このツールは、ネットワークデバイスの構成を検証するか、またはネットワークデバイスの設定方法を確認する場合に使用します。

Execute Network Device Command 診断ツールにアクセスするには、次のナビゲーションパスのいずれかを選択します。

1. Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[操作（Operations）] > [トラブルシュート（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [ネットワークデバイスコマンドの実行（Execute Network Device Command）]** を選択します。Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[ワークセンター（Work**

Centers）] > [**プロファイラ**（**Profiler**）] > [**トラブルシュート**（**Troubleshoot**）] > [**ネットワークデバイスコマンドの実行**（**Execute Network Device Command**）] を選択します。

2. 表示される [ネットワークデバイスコマンドの実行（Execute Network Device Command）] ウィンドウで、ネットワークデバイスの IP アドレスと実行する **show** コマンドを対応するフィールドに入力します。
3. [実行（Run）] をクリックします。

Cisco ISE でのサードパーティ ネットワーク デバイスのサポート

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、サードパーティ製ネットワーク アクセスデバイス（NAD）をサポートします。NAD プロファイルは、ベンダー側の導入に関係なく、シンプルなポリシー構成でサードパーティデバイスの機能を定義します。ネットワーク デバイス プロファイルには、次のものが含まれています。

- RADIUS、TACACS+、Cisco TrustSec などの、ネットワークデバイスがサポートするプロトコル。ネットワークデバイスに存在するベンダー固有の RADIUS ディクショナリを Cisco ISE にインポートできます。
- デバイスが有線 MAB、802.1X などのさまざまな認証フローに使用する属性および値。これらの属性と値により、Cisco ISE は、ネットワークデバイスが使用する属性に従って、デバイスに適した認証フローを検出できます。
- ネットワークデバイスの認可変更（CoA）機能。RADIUS プロトコル RFC 5176 では CoA 要求が定義されていますが、CoA 要求で使用される属性はネットワークデバイスによって異なります。RFC 5176 サポート付きのほとんどのシスコ以外のデバイスは、「プッシュ」および「切断」機能をサポートします。RADIUS CoA タイプをサポートしていないデバイスについては、Cisco ISE も SNMP CoA をサポートします。
- ネットワークデバイスが MAB フローに使用する属性およびプロトコル。さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。
- デバイスで使用される VLAN および ACL の権限。プロファイルを保存すると、Cisco ISE は設定された各権限に対し認証プロファイルを自動的に生成します。
- URL リダイレクション技術情報。URL リダイレクションは、個人所有デバイスの持ち込み（BYOD）、ゲストアクセス、ポスチャサービスなどの高度なフローに必要です。ネットワークデバイス内で見つかる URL リダイレクションには、静的と動的の 2 つのタイプがあります。静的 URL リダイレクションの場合は、Cisco ISE ポータル URL をコピーして構成に貼り付けることができます。動的 URL リダイレクションの場合、Cisco ISE は RADIUS 属性を使用して、リダイレクト先をネットワークデバイスに伝えます。

  ネットワークデバイスが動的および静的 URL リダイレクトのいずれもサポートしない場合、Cisco ISE は URL リダイレクトをシミュレートすることにより認証 VLAN 構成を提供

します。認証 VLAN 構成は、Cisco ISE で実行されている DHCP および DNS サービスに基づいています。

Cisco ISE でネットワークデバイスを定義したら、これらのデバイスプロファイルを設定するか、Cisco ISE によって提供された事前設定済みデバイスプロファイルを使用して、Cisco ISE が基本認証フローや、プロファイラ、ゲスト、BYOD、MAB、ポスチャなどの高度なフローを有効にするために使用する機能を定義します。

URL リダイレクト メカニズムと認証 VLAN

ネットワークでサードパーティデバイスが使用されていて、デバイスがダイナミックまたはスタティック URL リダイレクトをサポートしていない場合、Cisco ISE が URL リダイレクトフローをシミュレートします。このようなデバイスの URL リダイレクト シミュレーション フローは、Cisco ISE で DHCP または DNS サービスを実行することによって動作します。

次に、認証 VLAN フローの例を示します。

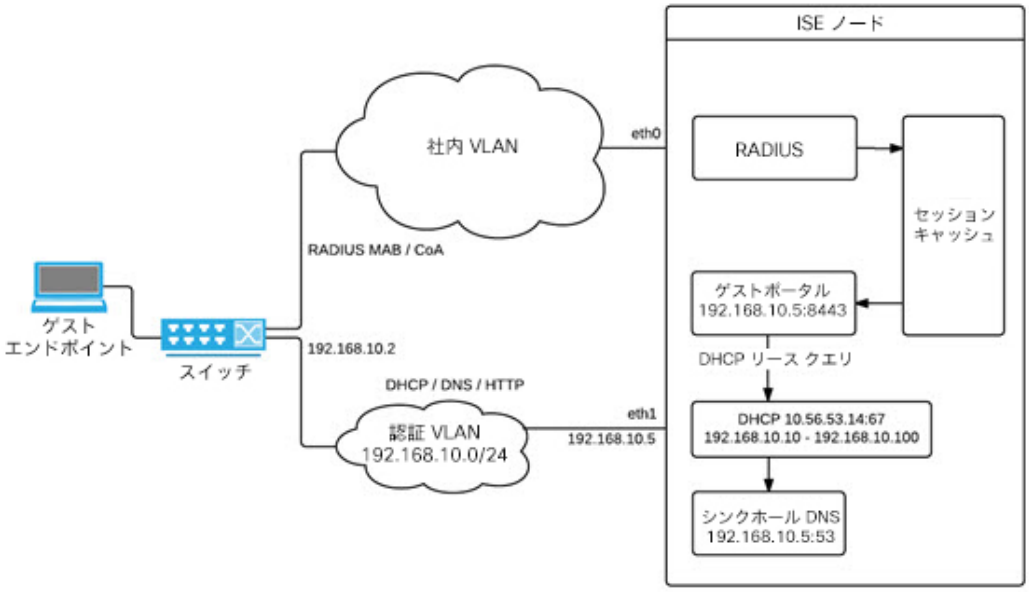
1. ゲスト エンドポイントが NAD に接続します。
2. ネットワークデバイスは、RADIUS 要求または MAB 要求を Cisco ISE に送信します。
3. ISE が認証ポリシーと許可ポリシーを実行し、ユーザーアカウンティング情報を保存します。
4. Cisco ISE が認証 VLAN ID を含む RADIUS アクセス承認メッセージを送信します。
5. ゲスト エンドポイントがネットワーク アクセスを受け取ります。
6. エンドポイントが DHCP 要求を送信し、Cisco ISE DHCP サービスからクライアント IP アドレスと Cisco ISE DNS シンクホール IP アドレスを取得します。
7. ゲストエンドポイントは、DNS クエリを送信して Cisco ISE IP アドレスを受け取るブラウザを開きます。
8. エンドポイントの HTTP 要求と HTTPS 要求は Cisco ISE に転送されます。
9. Cisco ISE は、ゲストポータル URL を含む **HTTP 301 Moved** メッセージで応答します。エンドポイントブラウザがゲストポータルウィンドウにリダイレクトされます。
10. ゲスト エンドポイント ユーザーが認証のためにログインします。
11. Cisco ISE はエンドポイントコンプライアンスを検証してから、NAD に応答します。Cisco ISE は CoA を送信し、エンドポイントを許可して、シンクホールをバイパスします。
12. ゲストユーザーは CoA に基づいて適切なアクセスを受け、エンドポイントが企業 DHCP から IP アドレスを受信します。これで、ゲストユーザーはネットワークを使用できます。

エンドポイントが認証を通過する前にゲストエンドポイントによって不正なネットワークアクセスが行われないように、認証 VLAN を企業のネットワークから分離することができます。認証 VLAN IP ヘルパーを設定して Cisco ISE マシンを示すか、いずれかの Cisco ISE ネットワーク インターフェイスを認証 VLAN に接続します。

NAD 設定から VLAN IP ヘルパーを設定することで、複数の VLAN を 1 つのネットワーク インターフェイス カードに接続することができます。IP ヘルパーの設定の詳細については、ネットワークデバイス用のアドミニストレーション ガイドの指示を参照してください。IP ヘルパーを持つ VLAN を含むゲストアクセスフローの場合、ゲストポータルを定義し、MAB 許可にバインドされた認証プロファイルでそのポータルを選択します。ゲスト ポータルの詳細については、Cisco ISE ゲスト サービス （811 ページ）を参照してください。

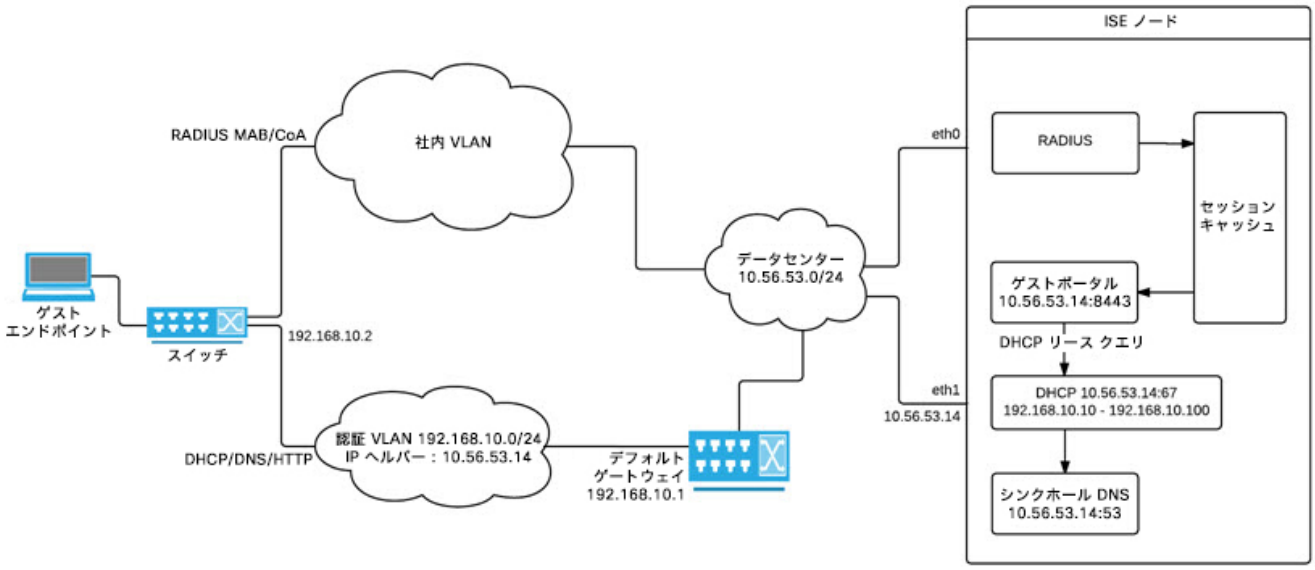
次の図に、認証 VLAN が定義されているときの基本的なネットワーク設定を示します（認証 VLAN が Cisco ISE ノードに直接接続されています）。

図 *32 : Cisco ISE* ノードに接続された認証 *VLAN*



次の図に、認証 VLAN と IP ヘルパーを備えたネットワークを示します。

図 *33 : IP* ヘルパーを備えた認証 *VLAN* 構成



CoA タイプ

Cisco ISE は、RADIUS と SNMP の両方の CoA タイプをサポートします。RADIUS または SNMP CoA タイプのサポートは、基本的なフローでは必須ではありませんが、NAD が複雑なフローで機能するために必要です。

Cisco ISE で NAD を設定するときに、ネットワークデバイスがサポートする RADIUS および SNMP 設定を定義します。NAD プロファイルを設定するときに、特定のフローに使用する CoA タイプを指定します。NAD のプロトコルの定義の詳細については、ネットワーク デバイス定義の設定（1367 ページ）を参照してください。Cisco ISE でデバイスと NAD のプロファイルを作成する前に、NAD でどの CoA タイプがサポートされているかをサードパーティサプライヤに確認してください。

ネットワーク デバイス プロファイル

Cisco ISE は、ネットワーク デバイス プロファイルを使用してサードパーティ製の NAD をサポートしています。これらのプロファイルによって、基本フローと、ゲスト、BYOD、MAB、ポスチャなどの高度なフローを有効にするために Cisco ISE が使用する機能が定義されます。

Cisco ISE には、いくつかのベンダーからのネットワーク デバイスの定義済みプロファイルが含まれています。Cisco ISE 2.1 以降のリリースは、次の表に記載されているネットワークデバイスでテストされています。

表 *124 : Cisco ISE 2.1* 以降のリリースでテスト済みのベンダーデバイス

デバイスタイプ	ベンダー	CoA タイプ	URL リダイレクトタイプ	サポートされる使用例または検証済みの使用例				
				802.1X フローと MAB フロー	CoA のないプロファイラ	CoA があるプロファイラ	ポスチャ	ゲストと BYOD
ワイヤレス	Aruba 7000、InstantAP	RADIUS	スタティック URL	はい	はい	はい	はい	はい
	Motorola RFS 4000	RADIUS	ダイナミック URL	はい	はい	はい	はい	はい
	HP 830	RADIUS	スタティック URL	はい	はい	はい	はい	はい
	Ruckus ZD 1200	RADIUS	—	はい	はい	はい	はい	はい
有線	HP A5500	RADIUS	ISE が提供する認証 VLAN	はい	はい	はい	はい	はい
	HP 3800 および 2920（ProCurve）	RADIUS	ISE が提供する認証 VLAN	はい	はい	はい	はい	はい
	Alcatel 6850	SNMP	ダイナミック URL	はい	はい	はい	はい	はい
	Brocade ICX 6610	RADIUS	ISE が提供する認証 VLAN	はい	はい	はい	はい	はい
	Juniper EX3300-24p	RADIUS	ISE が提供する認証 VLAN	はい	はい	はい	はい	はい

その他のサードパーティ製 NAD の場合は、デバイスのプロパティおよび機能を識別し、Cisco ISE でカスタム NAD プロファイルを作成する必要があります。	はい	はい	CoA サポートが必要	CoA サポートが必要です。 有線デバイスが URL リダイレクトをサポートしていない場合、Cisco ISE は認証 VLAN を使用します。ワイヤレスデバイスは認証 VLAN でテストされていません。

定義済みプロファイルがないその他のサードパーティ製ネットワークデバイス用のカスタム NAD プロファイルを作成する必要があります。ゲスト、BYOD、ポスチャなどの高度なワークフローについては、ネットワークデバイスは、これらのフローの CoA サポートに関連する RADIUS プロトコル RFC 5176をサポートしている必要があります。Cisco ISE でネットワークデバイスプロファイルを作成するために必要な属性については、デバイスのアドミニストレーション ガイドを参照してください。

ISE コミュニティ リソース

サードパーティ製 NAD プロファイルについては、「ISE Third-Party NAD Profiles and Configs」を参照してください。

Cisco ISE でのサードパーティ製ネットワークデバイスの設定

Cisco ISE は、ネットワーク デバイス プロファイルを使用してサードパーティ製の NAD をサポートしています。これらのプロファイルによって、ゲスト、BYOD、MAB、ポスチャなどのフローを有効にするために Cisco ISE が使用する機能が定義されます。

始める前に

ネットワーク デバイス プロファイル （1392 ページ）を参照してください。

ステップ 1 Cisco ISE へサードパーティ製ネットワークデバイスを追加します（Cisco ISE へのネットワーク デバイスのインポート（1386ページ）を参照）。ゲスト、BYOD またはポスチャのワークフローを設定している場合、CoA が定義され、NAD の URL リダイレクトメカニズムが、関連する Cisco ISE ポータルをポイントするように設定されていることを確認します。URL リダイレクトを設定するには、ポータルのランディングページから Cisco ISE ポータルの URL をコピーします。Cisco ISE の NAD の CoA タイプと URL リダイレクトの設定に関する詳細については、ネットワークデバイス定義の設定（1367ページ）を参照してください。さらに、手順については、サードパーティデバイスのアドミニストレーションガイドを参照してください。

ステップ 2 デバイスに適切な NAD プロファイルが Cisco ISE で利用できることを確認します。既存のプロファイルを表示するには、**[管理（Administration）]>[ネットワークリソース（Network Resources）]>[ネットワークデバイスプロファイル（Network Device Profiles）]** を選択します。適切なプロファイルが Cisco ISE に存在

しない場合は、カスタムプロファイルを作成します。カスタム プロファイルの作成方法の詳細については、ネットワーク デバイス プロファイルの作成 （1395 ページ）を参照してください。

ステップ 3 設定する NAD に NAD プロファイルを割り当てます。Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Device）]** を選択します。プロファイルを割り当てるデバイスを開き、**[デバイスプロファイル（Device Profile）]** ドロップダウンリストから割り当てるプロファイルを選択します。

ステップ 4 ポリシールールを設定する場合は、許可プロファイルをステップ 1 で NAD プロファイルに設定します。または、VLAN または ACL を使用するだけの場合、あるいはネットワークに異なるベンダーからのさまざまなデバイスがある場合は、[いずれか（Any）] に設定します。許可プロファイルの NAD プロファイルを設定するには、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。関連する認証プロファイルを開き、**[ネットワーク デバイス プロファイル（Network Device Profiles）]** ドロップダウンリストから関連する NAD プロファイルを選択します。ゲストフロー用に認証 VLAN を使用する場合、通常のゲストフローと同様に、ゲストポータルを定義し、MAB 認証にバインドされた認証プロファイルでそのポータルを選択する必要があります。ゲストポータルの詳細については、「Cisco ISE ゲストサービス」のセクションを参照してくださいCisco ISE ゲスト サービス （811 ページ） を参照してください。

ネットワーク デバイス プロファイルの作成

始める前に

- ほとんどの NAD には、標準の IETF RADIUS 属性に加えてベンダー固有のいくつかの属性を提供する、ベンダー固有の RADIUS ディクショナリが備わっています。ネットワークデバイスにベンダー固有の RADIUS ディクショナリがある場合は、それを Cisco ISE にインポートします。RADIUS ディクショナリが必要な手順については、サードパーティ製デバイスの管理ガイドを参照してください。Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[システム（System）]** > **[Radius]** > **[RADIUSベンダー（RADIUS Vendors）]**。RADIUS ディクショナリをインポートするには、RADIUS ベンダー ディクショナリの作成 （1499 ページ）を参照してください。
- ゲストやポスチャなどの複雑なフローの場合、ネットワークデバイスはRFC 5176で定義されている CoA タイプサポートしている必要があります
- ネットワークデバイスのプロファイルを作成するためのフィールドと可能な値の詳細については、ネットワーク デバイス プロファイル設定 （1896 ページ）を参照してください。

ステップ 1 Cisco ISE のGUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワーク デバイス プロファイル（Network Device Profiles）]** 。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 表示される [新しいネットワークデバイスのプロファイル（New Network Device Profile）] ウィンドウで、ネットワークデバイスの [名前（Name）] フィールドと [説明（Description）] フィールドに対応する値を入力します。

ステップ 4 [ベンダー（Vendor）] ドロップダウンリストから、ネットワークデバイスのベンダーを選択します。

ステップ 5 [アイコン（Icon）] 領域で、[アイコンの変更...（Change Icon ...）] をクリックして、システムからネットワークデバイスのアイコンをアップロードします。

または、[アイコン（Icon）] 領域で [デフォルトに設定（Set To Default）] をクリックして、Cisco ISE が提供するデフォルトのアイコンを使用します。

ステップ 6 [サポートされているプロトコル（Supported Protocols）] 領域で、デバイスがサポートするプロトコルのチェックボックスをオンにします。実際に使用するプロトコルのチェックボックスのみをオンにします。ネットワークデバイスが RADIUS プロトコルをサポートしている場合は、デバイスで使用する RADIUS ディクショナリを [RADIUSディクショナリ（RADIUS Dictionaries）] ドロップダウンリストから選択します。

ステップ 7 [テンプレート（Templates）] 領域で、関連する詳細情報を入力します。

a) [認証/許可（Authentication/Authorization）] をクリックし、フロータイプ、属性エイリアシング、およびホストルックアップに関するネットワークデバイスのデフォルト設定を行います。表示される新しい [フロータイプ条件（Flow Type Conditions）] 領域で、デバイスがさまざまな認証と許可フロー（有線 MAB や 802.1X など）に使用する属性と値を入力します。これにより、Cisco ISE は使用される属性に従ってデバイスに適切なフロータイプを検出できます。MAB 用の IETF 標準がないため、ベンダーごとに異なる値が [サービスタイプ（Service Type）] に使用されています。正しい設定を判断するには、デバイスのユーザーガイドを参照するか、またはMAB認証のスニファトレースを使用してください。[属性エイリアシング（Attribute Aliasing）] 領域で、デバイス固有の属性名を共通名にマップして、ポリシールールを簡素化します。現在、サービスセット識別子（SSID）のみが定義されています。ネットワークデバイスにワイヤレスSSIDの概念がある場合には、使用される属性に対してこれを設定します。Cisco ISE は、これを正規化された RADIUS ディクショナリの SSID という属性にマッピングします。これは、1 つのルール内で SSID を参照でき、基盤となる属性が異なっていても複数のデバイスで動作するので、ポリシールールの設定を簡素化します。[ホストルックアップ（Host Lookup）] 領域で、[ホストルックアップの処理（Process Host Lookup）] チェックボックスをオンにし、サードパーティデバイス ベンダーが提供する指示に基づき、関連する MAB プロトコルと属性を選択します。

b) [権限（Permissions）] から、VLAN と ACL に関するネットワークデバイスのデフォルト設定を行います。これらは、Cisco ISE で作成した認証プロファイルに基づいて自動的にマッピングされます。

c) [認可変更（CoA）（Change of Authorization (CoA)）] をクリックし、ネットワークデバイスの CoA 機能を設定します。

[次によるCoA（CoA By）] ドロップダウンリストから [RADIUS] を選択した場合は、表示される設定領域で、スタティック属性のみを選択する必要があります。ダイナミック属性はサポートされていません。

d) [リダイレクト（Redirect）] をクリックし、ネットワークデバイスのURLリダイレクト機能を設定します。URL リダイレクションは、ゲスト、BYOD およびポスチャサービスに必要です。

ステップ 8 [送信（Submit）] をクリックします。

関連トピック

Cisco ISE ネットワーク アクセス デバイス プロファイルの作成方法

Cisco ISE からのネットワーク デバイス プロファイルのエクスポート

Cisco ISE で設定された単一または複数のネットワーク デバイス プロファイルを XML ファイルの形式でエクスポートします。XML ファイルを編集し、新しいネットワークプロファイルとして Cisco ISE ファイルにインポートできます。

始める前に

「How to Create ISE Network Access Device Profiles」を参照してください。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Device）]** を選択します。

ステップ 2 エクスポートするデバイスの隣にあるチェックボックスをオンにし、[選択済みをエクスポート（Export Selected）] をクリックします。

ステップ 3 **DeviceProfiles.xml** という名前のファイルがローカルハードディスクにダウンロードされます。

Cisco ISE へのネットワーク デバイス プロファイルのインポート

Cisco ISE XML 構造を備えた単一の XML ファイルを使用して、Cisco ISE に単一または複数のネットワーク デバイス プロファイルをインポートします。複数のインポート ファイルから同時にネットワーク デバイス プロファイルをインポートすることはできません。

通常は、まずテンプレートとして使用するために Cisco ISE 管理者ポータルから既存のプロファイルをエクスポートする必要があります。デバイスプロファイルの詳細をファイルに入力し、XML ファイルとして保存します。次に、編集したファイルを Cisco ISE に再度インポートします。複数のネットワーク デバイス プロファイルを扱うには、単一の XML ファイルとして一緒に構造化された複数のプロファイルをエクスポートし、ファイルを編集してからプロファイルを一緒にインポートして、Cisco ISE で複数のプロファイルを作成します。

ネットワーク デバイス プロファイルのインポート時は、新しいレコードの作成のみができます。既存のプロファイルは上書きできません。既存のネットワーク デバイス プロファイルを更新するには、Cisco ISE から既存のプロファイルをエクスポートし、Cisco ISE からプロファイルを削除してから、必要に応じてプロファイルを編集した後にそのプロファイルをインポートします。

始める前に

「How to Create ISE Network Access Device Profiles」を参照してください。

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイスプロファイル（Network Device Profiles）]**。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 **[ファイルの選択（Choose Files）]** をクリックして、クライアントブラウザを実行しているシステムから XML ファイルを選択します。

ステップ 4 [インポート（Import）] をクリックします。

ネットワーク デバイス グループの管理

次のウィンドウを使用すると、ネットワークデバイスグループを設定し、管理することができます。

ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用する [ネットワークデバイスグループ（Network Device Groups）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[すべてのグループ（All Groups）]**。

ネットワーク デバイス グループは、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[すべてのグループ（All Groups）]** ウィンドウでも作成できます。

表 *125 : [ネットワーク デバイス グループ（Network Device Group）] ウィンドウのフィールド*

フィールド名	使用上のガイドライン
名前（Name）	ルート ネットワーク デバイス グループの名前を入力します。このルート ネットワーク デバイス グループに追加される後続のすべての子ネットワーク デバイス グループに対して、新たに作成したこのネットワーク デバイス グループの名前を入力します。 ネットワーク デバイス グループ階層内には、ルートノードを含めて、最大で 6 つのノードを含めることができます。各ネットワーク デバイス グループの名前には最大で 32 文字を使用できます。
説明（Description）	ルートまたは子のネットワーク デバイス グループの説明を入力します。

フィールド名	使用上のガイドライン
ネットワークデバイスの数（No. of Network Devices）	ネットワークグループ内のネットワークデバイスの数がこの列に表示されます。

ネットワーク デバイス グループのインポート設定

次の表では、[ネットワークデバイスグループ（Network Device Group）] ウィンドウの [インポート（Import）] ダイアログボックスのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）]**。

表 *126 : [*ネットワーク デバイス グループのインポート（***Network Device Groups Import***）*]* ウィンドウのフィールド

フィールド名	使用上のガイドライン
テンプレートの生成（Generate a Template）	CSV テンプレートファイルをダウンロードするには、このリンクをクリックします。 同じ形式のネットワーク デバイス グループ情報でテンプレートを更新します。そのテンプレートをローカルに保存し、ネットワーク デバイス グループを Cisco ISE 展開にインポートします。
ファイル（File）	**[ファイルの選択（Choose File）]** をクリックして、アップロードする CSV ファイルの場所に移動します。そのファイルは、新規ファイル、または別の Cisco ISE 展開からエクスポートされたファイルである可能性があります。 更新されたネットワーク デバイス グループ情報を使用して、ある Cisco ISE 展開から別の展開にネットワーク デバイス グループをインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワーク デバイス グループをインポートファイル内のデバイスグループに置き換える場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポートファイル内の新しいネットワーク デバイス グループのみがネットワーク デバイス グループ リポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生した最初のインスタンスでインポートを中止するには、このチェックボックスをオンにします。 このチェックボックスをオンにしていないためにエラーが発生した場合は、Cisco ISE はエラーを報告し、残りのデバイスグループを引き続きインポートします。

ネットワーク デバイス グループ

Cisco ISE では、階層型ネットワーク デバイス グループ（NDG）を作成できます。ネットワーク デバイス グループを使用し、地理的な場所、デバイスタイプ、またはネットワーク内の相対的な位置（アクセスレイヤやデータセンターなど）に基づいて、ネットワークデバイスを論理的にグループ化します。

[ネットワーク デバイス グループ（Network Device Groups）] ウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）]** を選択します。

たとえば、地理的な場所に基づいてネットワークデバイスを編成するには、大陸、地域、または国でグループ化します。

- **[アフリカ（Africa）] > [南部（Southern）] > [ナミビア（Namibia）]**
- **[アフリカ（Africa）] > [南部（Southern）] > [南アフリカ（South Africa）]**
- **[アフリカ（Africa）] > [南部（Southern）] > [ボツワナ（Botswana）]**

デバイスタイプに基づいてネットワークデバイスをグループ化します。

- **[アフリカ（Africa）] > [南部（Southern）] > [ボツワナ（Botswana）] > [ファイアウォール（Firewalls）]**
- **[アフリカ（Africa）] > [南部（Southern）] > [ボツワナ（Botswana）] > [ルータ（Routers）]**
- **[アフリカ（Africa）] > [南部（Southern）] > [ボツワナ（Botswana）] > [スイッチ（Switches）]**

ネットワークデバイスを 1 つ以上の階層型ネットワーク デバイス グループに割り当てます。Cisco ISE が、設定されたネットワーク デバイス グループの順序リストを処理して特定のデバイスに割り当てる適切なグループを決定する場合、同じデバイスプロファイルが複数のデバイスグループに適用されることがわかることがあります。この場合、Cisco ISE は最初に一致したデバイスグループを適用します。

作成できるネットワーク デバイス グループの最大数に制限はありません。ネットワーク デバイス グループの階層レベル（親グループを含む）は最大 6 レベルまで作成できます。

デバイスグループ階層は、[ツリーテーブル（Tree Table）] と [フラットテーブル（Flat Table）] の 2 つのビューに表示されます。ネットワーク デバイス グループのリストの上にある [ツリーテーブル（Tree Table）] または [フラットテーブル（Flat Table）] をクリックして、リストを対応するビューに編成します。

[ツリーテーブル（Tree Table）] ビューで、ルートノードはツリーの最上位に表示され、その後に子グループが階層順で続きます。各ルートグループのすべてのデバイスを表示するには、[すべて展開（Expand All）] をクリックします。ルートグループのみのリストを表示するには、[すべて折りたたむ（Collapse All）] をクリックします。

[フラットテーブル（Flat Table）] ビューでは、各デバイスグループの階層が [グループ階層（Group Hierarchy）] 列に表示されます。

両方のビューで、各子グループに割り当てられているネットワークデバイスの数が、対応する [ネットワークデバイスの数（No. of Network Devices）] 列に表示されます。デバイスグループに割り当てられているすべてのネットワークデバイスのリストを表示するダイアログボックスをクリックするには、この数字をクリックします。表示されるダイアログボックスには、ネットワークデバイスをあるグループから別のグループに移動するための2つのボタンも含まれています。現在のグループから別のグループにネットワークデバイスを移動するには、[デバイスを別のグループに移動（Move Devices to Another Group）] をクリックします。選択したネットワーク デバイス グループにネットワークデバイスを移動するには、[デバイスをグループに追加（Add Devices to Group）] をクリックします。

[ネットワークデバイスグループ（Network Device Groups）] ウィンドウでネットワーク デバイス グループを追加するには、[追加（Add）] をクリックします。[親グループ（Parent Group）] ドロップダウンリストで、ネットワーク デバイス グループを追加する必要がある親グループを選択するか、または [ルートグループとして追加（Add As Root Group）] オプションを選択して、新しいネットワーク デバイス グループを親グループとして追加します。

（注） デバイスが割り当てられているデバイス グループは削除できません。デバイスグループを削除する前に、すべての既存のデバイスを別のデバイスグループに移動する必要があります。

ルート ネットワーク デバイス グループ

Cisco ISE には、[すべてのデバイスタイプ（All Device Types）] と [すべてのロケーション（All Locations）] という 2 つの事前に定義されたルート ネットワーク デバイス グループが含まれています。これらの事前に定義されたネットワーク デバイス グループを編集、複製、または削除することはできませんが、それらの下に新しいデバイスグループを追加することはできます。

ルート ネットワーク デバイス グループ（ネットワーク デバイス グループ）を作成した後に、すでに説明したように、[ネットワークデバイスグループ（Network Device Groups）] ウィンドウでルートグループの下に子ネットワーク デバイス グループを作成できます。

ポリシー評価で Cisco ISE が使用するネットワークデバイスの属性

新しいネットワーク デバイス グループを作成すると、新しいネットワークデバイス属性が**システムディクショナリ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）]**）内の**デバイス**ディクショナリに追加されます。追加されたデバイス属性は、ポリシー定義で使用されます。

Cisco ISE では、デバイスタイプ、ロケーション、モデル名、またはネットワークデバイス上で実行しているソフトウェアバージョンなどの**デバイス**ディクショナリ属性を使用して、認証ポリシーと許可ポリシーを設定できます。

Cisco ISE へのネットワーク デバイス グループのインポート

カンマ区切り形式（CSV）ファイルを使用して Cisco ISE ノードにネットワーク デバイス グループをインポートできます。2 つの異なるインポートファイルから同時にネットワーク デバイス グループをインポートできません。

Cisco ISE 管理者ポータルから CSV テンプレートをダウンロードします。そのテンプレートにネットワーク デバイス グループの詳細を入力して CSV ファイルとして保存した後、編集したファイルを Cisco ISE にインポートします。

デバイスグループのインポート中に、新しいレコードを作成するか、または既存のレコードを更新できます。デバイス グループをインポートする場合、Cisco ISE で最初のエラーが発生した場合、既存のデバイス グループを新しいグループで上書きするか、またはインポート プロセスを停止するかを定義できます。

ステップ 1 Cisco ISE の GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）]**。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 ダイアログボックスで、**[ファイルの選択（Choose Files）]** をクリックし、クライアントブラウザを実行しているシステムから CSV ファイルを選択します。

ネットワーク デバイス グループを追加するための CSV テンプレートファイルをダウンロードするには、[テンプレートの生成（Generate a Template）] をクリックします。

ステップ 4 既存のネットワークデバイス グループを上書きするには、[既存のデータを新しいデータで上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。

ステップ 5 [最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 6 [インポート（Import）] をクリックします。

Cisco ISE からのネットワーク デバイス グループのエクスポート

Cisco ISE で設定されたネットワーク デバイス グループは、CSV ファイルの形式でエクスポートできます。その後で、これらのネットワーク デバイス グループを別の Cisco ISE ノードにインポートできます。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] > [すべてのグループ（All Groups）]**

ステップ 2 ネットワーク デバイス グループをエクスポートするには、次のいずれかを行うことができます。

- エクスポートするデバイスグループの横にあるチェックボックスをオンにし、**[エクスポート（Export）] > [選択済みをエクスポート（Export Selected）]** を選択します。

- **[エクスポート（Export）]** > **[すべてエクスポート（Export All）]** を選択して、定義されたネットワーク デバイス グループをすべてエクスポートします。

CSV ファイルがローカルハードディスクにダウンロードされます。

ネットワーク デバイス グループの管理

次のウィンドウを使用すると、ネットワークデバイスグループを設定し、管理することができます。

ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用する [ネットワークデバイスグループ（Network Device Groups）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[すべてのグループ（All Groups）]**。

ネットワーク デバイス グループは、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[すべてのグループ（All Groups）]** ウィンドウでも作成できます。

表 *127 : [*ネットワーク デバイス グループ（***Network Device Group***）*]* ウィンドウのフィールド

フィールド名	使用上のガイドライン
名前（Name）	ルート ネットワーク デバイス グループの名前を入力します。このルート ネットワークデバイス グループに追加される後続のすべての子ネットワーク デバイス グループに対して、新たに作成したこのネットワーク デバイス グループの名前を入力します。 ネットワーク デバイス グループ階層内には、ルートノードを含めて、最大で 6 つのノードを含めることができます。各ネットワーク デバイス グループの名前には最大で 32 文字を使用できます。
説明（Description）	ルートまたは子のネットワーク デバイス グループの説明を入力します。
ネットワークデバイスの数（No. of Network Devices）	ネットワークグループ内のネットワークデバイスの数がこの列に表示されます。

ネットワーク デバイス グループのインポート設定

次の表では、[ネットワークデバイスグループ（Network Device Group）] ウィンドウの [インポート（Import）] ダイアログボックスのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）]**。

表 *128 : [*ネットワーク デバイス グループのインポート（***Network Device Groups Import***）*]* ウィンドウのフィールド

フィールド名	使用上のガイドライン
テンプレートの生成（Generate a Template）	CSVテンプレートファイルをダウンロードするには、このリンクをクリックします。 同じ形式のネットワーク デバイス グループ情報でテンプレートを更新します。そのテンプレートをローカルに保存し、ネットワーク デバイス グループを Cisco ISE 展開にインポートします。
ファイル（File）	**[ファイルの選択（Choose File）]** をクリックして、アップロードする CSV ファイルの場所に移動します。そのファイルは、新規ファイル、または別の Cisco ISE 展開からエクスポートされたファイルである可能性があります。 更新されたネットワーク デバイス グループ情報を使用して、ある Cisco ISE展開から別の展開にネットワークデバイスグループをインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワーク デバイス グループをインポートファイル内のデバイスグループに置き換える場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポートファイル内の新しいネットワーク デバイス グループのみがネットワーク デバイス グループリポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生した最初のインスタンスでインポートを中止するには、このチェックボックスをオンにします。 このチェックボックスをオンにしていないためにエラーが発生した場合は、Cisco ISE はエラーを報告し、残りのデバイスグループを引き続きインポートします。

Cisco ISE でのテンプレートのインポート

Cisco ISE では、CSV ファイルを使用して大量のネットワークデバイスやネットワーク デバイス グループをインポートできます。テンプレートには、フィールドのフォーマットを定義するヘッダー行が含まれます。次の表に記載されている列を追加する場合を除き、このヘッダー行は編集しないでください。

ネットワークデバイスやネットワーク デバイス グループに関連するインポートフロー内で[テンプレートの生成（Generate a Template）] リンクを使用して CSV ファイルをローカルシステムにダウンロードします。

ネットワーク デバイスのインポート テンプレート形式

次の表は、インポート ネットワーク デバイスの CSV テンプレートファイルのフィールドのリストと説明です。

表 *129* : ネットワークデバイスの *CSV* テンプレートのフィールドと説明

フィールド	使用上のガイドライン
Name:String(32)	ネットワークデバイスの名前を入力します。name には、最大 32 字の英数字を指定できます。
Description:String(256)	（オプション）最大256 文字でネットワークデバイスの説明を入力します。
IP Address:Subnets(a.b.c.d/m|...)	ネットワークデバイスの IP アドレスおよびサブネットマスクを入力します。パイプ記号（|）で区切って複数の値を指定できます。 IPv4 および IPv6 アドレスは、ネットワークデバイス（TACACS および RADIUS）構成および外部 RADIUS サーバー構成でサポートされています。 IPv4アドレスを入力する場合は、範囲とサブネットマスクを使用できます。 IPv6 では、範囲がサポートされていません。
Model Name:String(32)	ネットワークデバイスの機種名を最大 32 文字で入力します。
Software Version:String(32)	ネットワークデバイスのソフトウェアバージョンを最大 32 文字で入力します。
Network Device Groups:String(100)	既存のネットワーク デバイス グループの名前を入力します。サブグループの場合は、親グループとサブグループの両方をスペースで区切って含める必要があります。最大 100 文字の文字列（たとえば、*Location>All Location>US*）です。
Authentication:Protocol:String(6)	使用する認証プロトコルを入力します。有効な値は **RADIUS** のみです（大文字と小文字は区別されません）。
Authentication:Shared Secret:String(128)	（[Authentication:Protocol:String(6)] のフィールドの値を入力した場合に限り必須）最大 128 文字の文字列を入力します。

フィールド	使用上のガイドライン
PasswordEncrypted:Boolean(true|false)	この列に必要なフィールド値はありません。 Cisco ISE リリース 3.3 パッチ 1 以前のリリースからネットワークデバイスをインポートする場合は、インポートする前に、このヘッダーを含む新しい列を [Authentication:Shared Secret:String(128)] 列の右側に追加する必要があります。この列が追加されていない場合は、エラーメッセージが表示され、ファイルをインポートできません。 インポート時にパスワードを復号するための有効なキーが指定されていない場合、暗号化されたパスワードを持つネットワークデバイスは拒否されます。
EnableKeyWrap:Boolean(true|false)	このフィールドは、KeyWrap がネットワークデバイスでサポートされている場合に限り有効です。**true** または **false** を入力します。
EncryptionKey:String(ascii:16|hexa:32)	（KeyWrap を有効にした場合は必須）セッションの暗号化に使用される暗号キーを入力します。 ASCII 値：16 文字（バイト）の長さ。 16 進数値：32 文字（バイト）の長さ。
AuthenticationKey:String(ascii:20|hexa:40)	（KeyWrap を有効にした場合は必須）RADIUS メッセージに対するキー付きハッシュメッセージ認証コード（HMAC）の計算を入力します。 ASCII 値：20 文字（バイト）の長さ。 16 進数値：40 文字（バイト）の長さ。
InputFormat:String(32)	暗号化キーと認証キーの入力形式を入力します。ASCII 値および 16 進数値を使用できます。
SNMP:Version:Enumeration (|2c|3)	プロファイラサービスが使用する必要のある SNMP プロトコルのバージョンを入力します（1、2c、または 3）。
SNMP:RO Community:String(32)	（[SNMP:Version:Enumeration (|2c|3)] のフィールドに値を入力する場合は必須）。読み取り専用コミュニティの文字列を最大 32 文字で入力します。
SNMP:RW Community:String(32)	（[SNMP:Version:Enumeration (|2c|3)] のフィールドに値を入力する場合は必須）。読み取り書き込みコミュニティの文字列を最大 32 文字で入力します。
SNMP:Username:String(32)	最大 32 文字の文字列を入力します。
	（[SNMP:Version:Enumeration (|2c|3)] のフィールドに SNMP バージョン 3 を入力した場合は必須）[Auth]、[No Auth]、または [Priv] を入力します。

フィールド	使用上のガイドライン
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	（SNMP セキュリティレベルで [Auth] または [Priv] を入力した場合は必須）[MD5] または [SHA] を入力します。
SNMP:Authentication Password:String(32)	（[SNMP:Security Level:Enumeration(Auth|No Auth|Priv)] のフィールドに [Auth] を入力した場合は必須）最大 32 文字の文字列を入力します。
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	（[SNMP:Security Level:Enumeration(Auth|No Auth|Priv)] のフィールドに [Priv] を入力した場合は必須）[DES]、[AES128]、[AES192]、[AES256]、または [3DES] を入力します。
SNMP:Privacy Password:String(32)	（[SNMP:Security Level:Enumeration(Auth|No Auth|Priv)] のフィールドに [Priv] を入力した場合は必須）最大 32 文字の文字列を入力します。
SNMP:Polling Interval:Integer:600-86400 seconds	SNMP ポーリング間隔を秒単位で入力します。有効な値は 600 ー 86400 の整数です。
SNMP:Is Link Trap Query:Boolean(true|false)	**true** または **false** を入力して、SNMP リンクトラップを有効または無効にします。
SNMP:Is MAC Trap Query:Boolean(true|false)	**true** または **false** を入力して、SNMP MAC トラップを有効または無効にします。
SNMP:Originating Policy Services Node:String(32)	SNMP データのポーリングに使用される Cisco ISE サーバーを示します。デフォルトでは自動ですが、このフィールドに別の値を割り当てて設定を上書きできます。
Trustsec:Device Id:String(32)	Cisco Trustsec デバイス ID を、最大 32 文字の文字列で入力します。
Trustsec:Device Password:String(256)	（Cisco TrustSec デバイス ID を入力した場合は必須）Cisco TrustSec デバイスのパスワードを、最大 256 文字の文字列で入力します。
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds	TrustSec 環境データのダウンロード間隔を入力します。有効な値は 1 ー 2147040000 の整数です。
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds	TrustSec のピア許可ポリシーのダウンロード間隔を入力します。有効な値は 1 ー 2147040000 の整数です。
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds	TrustSec の再認証間隔を入力します。有効な値は 1 ー 2147040000 の整数です。
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds	Cisco TrustSec セキュリティグループ ACL リストのダウンロード間隔を入力します。有効な値は 1 ー 2147040000 の整数です。
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true|false)	**true** または **false** を入力して、Cisco TrustSec デバイスが信頼できるかどうかを示します。

フィールド	使用上のガイドライン
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL|DISABLE_ALL)	**ENABLE_ALL** または **DISABLE_ALL** を入力して、Cisco TrustSec の構成変更を Cisco TrustSec デバイスに通知します。
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)	**true** または **false** を入力して、Cisco TrustSec デバイスがセキュリティグループタグに含まれているかどうかを示します。
Deployment:Execution Mode Username:String(32)	ネットワークデバイス設定を編集する権限を持っているユーザー名を入力します。これは、最大 32 文字の文字列です。
Deployment:Execution Mode Password:String(32)	デバイスのパスワードを、最大 32 文字の文字列で入力します。
Deployment:Enable Mode Password:String(32)	デバイスの構成を編集するためのデバイスのパスワードを入力します。これは、最大 32 文字の文字列です。
Trustsec:PAC issue date:Date	Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の発行日を入力します。
Trustsec:PAC expiration date:Date	Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の期限日を入力します。
Trustsec:PAC issued by:String	Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の発行者（Cisco TrustSec 管理者）の名前を入力します。文字列値である必要があります。

ネットワーク デバイス グループのインポート テンプレート形式

次の表に、テンプレート ヘッダーのフィールドとネットワーク デバイス グループの CSV ファイルにおけるこれらのフィールドの説明を示します。

表 *130 :* ネットワーク デバイス グループの *CSV* テンプレートのフィールドと説明

フィールド	説明
Name:String(100):	（必須）このフィールドはネットワーク デバイス グループの名前です。最大 100 文字の文字列です。NDG の完全な名前の長さは、最大 100 文字です。たとえば、[グローバル（Global）] >[アジア（Asia）] という親グループの下に [インド（India）] というサブグループを作成する場合、作成する NDG の完全な名前は Global#Asia#India になります。完全な名前の長さは 100 文字以内でなければなりません。NDG の完全な名前の長さが 100 文字を超えた場合、NDG の作成は失敗します。
Description:String(1024)	これはオプションのフィールドです。これは、最大 1024 文字の文字列です。

フィールド	説明
Type:String(64):	（必須）このフィールドはネットワーク デバイス グループのタイプです。これは、最大 64 文字の文字列です。
Is Root:Boolean(true|false):	（必須）これは、特定のネットワーク デバイス グループがルート グループかどうかを示すフィールドです。有効な値は true または false です。

Cisco ISE と NAD 間の通信を保護する IPSec セキュリティ

IPSec は、IP にセキュリティを実装するプロトコルのセットです。RADIUS および TACACS+ のプロトコルでは MD5 ハッシュアルゴリズムを使用します。セキュリティを強化するため、Cisco ISE には IPsec 機能があります。IPsec は、送信者を認証し、送信中のデータ変更を検出し、送信されたデータを暗号化することで通信を保護します。

Cisco ISE は、トンネルモードとトランスポートモードで IPSec をサポートしています。Cisco ISE インターフェイスで IPsec を有効にし、ピアを設定すると、通信を保護するため Cisco ISE と NAD の間に IPsec トンネルが作成されます。

事前共有キーを定義するか、または IPsec 認証に X.509 証明書を使用できます。IPsec は、ギガビット イーサネット 1 ～ 5 のインターフェイスで有効にできます。IPsec は PSN あたり 1 つの Cisco ISE インターフェイスでのみ設定できます。

（注） IPSec は、ボンド 1 およびボンド 2 インターフェイスでのみサポートされています。ギガビットイーサネット 0 とボンド 0（ギガビットイーサネット 0 と ギガビットイーサネット 1 インターフェイスがボンディングされている場合）は、Cisco ISE CLI の管理インターフェイスです。IPSec はギガビットイーサネット 0 と ボンド 0 ではサポートされていません。ボンドインターフェイスに関する情報は、Cisco ISE GUI の [IPSec] ページには表示されません。

IPSec は Cisco ISE リリース 2.2 以降でサポートされています。

IPSec の設定、制限、およびサポートの詳細については、『Security Configuration Guide, Cisco IOS XE Cupertino 17.7.x (Catalyst 9300 Switches)』を参照してください。

Cisco ISE リリース 3.4、 以降では、ネイティブ IPSec のみを使用して Cisco ISE PSN ノードで IPSec を設定できます。ネイティブ IPSec の設定方法の詳細については、「Cisco ISE でのネイティブ IPSec の設定」を参照してください。

レガシー IPSec（ESR）からネイティブ IPSec に移行する方法については、『Cisco ISE Administrator Guide』のCisco ISE でのレガシー IPSec からネイティブ IPSec への移行 （1413 ページ）を参照してください。

Cisco ISE でのネイティブ IPSec の設定

ネイティブ IPSec 設定を使用すると、IKEv1 および IKEv2 プロトコルを使用して、IPSec トンネルを介した Cisco ISE PSN と NAD 間のセキュリティ アソシエーションを確立できます。

（注）
- Cisco ISE PSN と NAD の IPSec 設定が同じであることを確認します。
- PSN ごとに 150 の IPSec トンネル（VTI を含む）をサポートできます。

始める前に

Cisco ISE でネイティブ IPSec を設定するには、次が必要です。

Cisco ISE で、次の手順を実行します。

- Cisco ISE Essentials ライセンスがあることを確認します。
- （オプション）[X.509証明書（X.509 Certificates）] オプションを使用している場合は、ネイティブ IPSec 接続を確立する PSN ごとに IPSec のシステム証明書をアップロードします。[システム証明書（System Certificates）] ウィンドウの [IPSec：ネイティブIPSecの証明書の使用（IPSec: Use certificate for Native IPSec）] チェックボックスをオンにします。また、Cisco ISE IPSec システム証明書と NAD 証明書用の CA 証明書を信頼ストアにアップロードする必要があります。[信頼できる証明書（Trusted Certificates）] ウィンドウで、[CA IPSecの信頼できる証明書（CA IPSec Trusted Certificate）] の [ISE内で認証を信頼する（Trust for authentication within ISE）] チェックボックスをオンにします。

重要 Cisco ISE 3.3 パッチ 2 以降では、関連付けられたすべてのピアおよび中間 CA 証明書に Authority Information Access（AIA）OCSP URL または crlDistributionPoint URL、あるいはその両方が含まれている場合にのみ、[X.509証明書（X.509 Certificates）] オプションを使用して IPSec トンネルを確立できます。このオプションを引き続き使用できるようにするには、既存の証明書を更新して、AIA OCSP URL または crlDistributionPoint URL、あるいはその両方を含める必要があります。AIA または crlDistributionPoint の情報が証明書に存在しない場合は、[事前共有キー（Pre-shared Keys）] オプションのみを使用して IPSec トンネルを確立できます。

- [ネットワークデバイス（Network Devices）] ウィンドウで、特定の IP アドレスを持つ NAD を追加します。
- NAD で IPSec を設定します。Cisco ISE PSN と NAD の IPSec 設定は同じである必要があります。

ステップ 1 Cisco ISE GUI で、[管理（Administration）] にカーソルを合わせ、**[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[IPSec]** > **[ネイティブIPSec（Native IPSec）]** に移動します。

ステップ 2 [追加（Add）] をクリックして、Cisco ISE PSNとNAD間のセキュリティアソシエーションを設定します。

ステップ 3 [ノード固有の設定（Node-Specific Settings）] セクションで、次の詳細情報を入力します。

a) [ノードの選択（Select Node）] ドロップダウンリストから、必要な Cisco ISE PSN を選択します。

b) **[NAD IPアドレス（NAD IP Address）]** フィールドに、対応する値を入力します。

c) **[ネイティブIPSecインターフェイス（Native IPSec Interface）]** ドロップダウンリストから、必要なネイティブ IPSec トラフィック インターフェイスを選択します。

d) （オプション）[VTIの設定（Configure VTI）] チェックボックスをオンにして、仮想トンネルインターフェイス（VTI）を設定します。

- [リモートトンネルIPアドレス（Remote Tunnel IP address）] フィールドに、対応する値を入力します。
- [ローカルトンネルIPアドレス（Local Tunnel IP address）] フィールドに、対応する値を入力します。

（注） Cisco ISE リリース 3.4 へのアップグレード後は、すべての IPSec 接続を無効にしてから Cisco ISE GUI で再度有効にし、既存のすべての VTI トンネルがアクティブであることを確認する必要があります。

ステップ 4 [認証設定（Authentication Settings）] セクションでオプションボタンをクリックして、選択した Cisco ISE PSN ノードに対し、次の認証タイプのいずれかを選択します。

a) [事前共有キー（Pre-shared Key）]：このオプションを選択した場合は、事前共有キーを入力し、ネットワークデバイスで同じキーを設定する必要があります。事前共有キーには英数字を使用してください。特殊文字はサポートされていません。ネットワークデバイスで事前共有キーを設定する方法については、ネットワークデバイスのマニュアルを参照してください。

b) [X.509証明書（X.509 Certificates）]：[X.509証明書（X.509 Certificates）] ドロップダウンリストから、IPSec トンネルに必要な X.509 証明書を選択します。

（注） [X.509証明書（X.509 Certificates）] オプションを選択する前に、必要な証明書（IPSec システム証明書および CA IPSec 信頼証明書）を設定します。証明書には、SAN（サブジェクト代替名）拡張子と DNS が含まれている必要があります。

相関するネイティブ IPSec 設定が行われた後に証明書が追加または変更された場合は、ネイティブ IPSec 設定を再度保存する必要があります。

ステップ 5 [全般設定（General Settings）] セクションで、以下の詳細を入力します。

a) [IKEバージョン（IKE Version）] ドロップダウンリストから、必要な IKE バージョンを選択します。

b) [モード（Mode）] ドロップダウンリストから、必要なモードを選択します。

VTI を設定する場合は、トンネルモードのみがサポートされます。

c) [ESP/AHプロトコル（ESP/AH Protocol）] ドロップダウンリストから、必要なプロトコルを選択します。

d) （オプション）[IKE再認証時間（IKE Reauth Time）] フィールドに、対応する値を入力します。

[IKE再認証時間（IKE Reauth Time）] の値の範囲は 0 ～ 86,400 です。このフィールドに値 0 を入力すると、[IKE再認証時間（IKE Reauth Time）] フィールドを無効にできます。

ステップ 6 [フェーズ1の設定（Phase One Settings）] セクションで、IKE セキュリティ アソシエーション構成のセキュリティ設定を行うと、2つの IKE デーモン間の通信を保護できます。

a) [暗号化アルゴリズム（Encryption Algorithm）] ドロップダウンリストから必要な暗号化アルゴリズムを選択します。

b) [ハッシュアルゴリズム（Hash Algorithm）] ドロップダウンリストから、必要なハッシュアルゴリズムを選択します。

c) [DHグループ（DH Group）] ドロップダウンリストから、必要な DH グループを選択します。

d) （オプション）[キー再生成時間（Re-key Time）] フィールドに、対応する値を入力します。

[キー再生成時間（Re-key Time）] の値の範囲は 0 ～ 86,400 です。このフィールドに値 0 を入力すると、[キー再生成時間（Re-key Time）] フィールドを無効にできます。

ステップ 7 [フェーズ2の設定（Phase Two Settings）] セクションでは、2 つのエンドポイント間の IP トラフィックを保護するために、ネイティブ IPSec セキュリティ アソシエーション構成のセキュリティ設定を行えます。次の詳細を入力します。

a) [暗号化アルゴリズム（Encryption Algorithm）] ドロップダウンリストから必要な暗号化アルゴリズムを選択します。

b) [ハッシュアルゴリズム（Hash Algorithm）] ドロップダウンリストから、必要なハッシュアルゴリズムを選択します。

c) （オプション）[DHグループ（DH Group）] ドロップダウンリストから、必要な DH グループを選択します。

d) （オプション）[キー再生成時間（Re-key Time）] フィールドに、対応する値を入力します。

[キー再生成時間（Re-key Time）] の値の範囲は 0 ～ 2,592,000 です。このフィールドに値 0 を入力すると、[キー再生成時間（Re-key Time）] フィールドを無効にできます。

ステップ 8 [保存（Save）] をクリックして、選択した Cisco ISE PSN ノードでネイティブ IPSec をアクティブにします。

（注）

- ネイティブ IPSec の設定中は、複数の Cisco ISE インターフェイスを同じ IP サブネットに設定しないでください。
- 既存の IPSec トンネルインターフェイスで IP アドレスが変更された場合は、既存のトンネル設定を再度有効にして、IP アドレスの変更を反映する必要があります。
- IPSec トンネルの既存のインターフェイスがシャットダウンされた場合、そのトンネルの IPSec ステータスは、次のキー再生成または再認証が行われるまで、[確立済み（Established）] と表示されます。
- ネイティブ IPSec に関連した監査レポートを表示するには、**[操作（Operations）] > [レポート（Reports）] > [監査（Audit）] > [変更設定監査（Change Configuration Audit）]** の順に選択します。

Cisco ISE で [ネイティブIPSec設定（Native IPsec Configuration）] を表示して修正

[ネイティブIPSec設定（Native IPsec Configuration）] ウィンドウのネイティブ IPsec 設定を使用して、Cisco ISE PSN と NAD の間に確立されたセキュリティ アソシエーションを追加、表示、編集、複製、無効化、および削除できます。

クイックフィルタを使用して、ネイティブ IPsec 設定をフィルタリングできます。

[ネイティブIPSec設定（Native IPsec Configuration）] テーブルには、さらに列を追加できます。[ネイティブIPSec設定（Native IPsec Configuration）] テーブルの右上にある歯車アイコンをクリックし、[フェーズ1暗号化アルゴリズム（Phase-one Encryption Algorithm）]、[フェーズ2暗号化アルゴリズム（Phase-two Encryption Algorithm）]、[フェーズ1ハッシュアルゴリズム（Phase-one Hash Algorithm）] などの列から希望する列を選択し、[実行（Go）] をクリックして、選択した列を [ネイティブIPSec設定（Native IPsec Configuration）] テーブルに追加します。

Cisco ISE でのレガシー IPSec からネイティブ IPSec への移行

Cisco ISE リリース 3.4 以降、レガシー IPSec（ESR）は Cisco ISE でサポートされません。Cisco ISE のすべての IPSec 設定が、ネイティブ IPSec 設定になります。トンネルとトンネルの設定が失われないように、Cisco ISE リリース 3.4 にアップグレードする前に、レガシー IPSec（ESR）からネイティブ IPSec に移行することをお勧めします。

始める前に

Cisco ISE でレガシー IPSec からネイティブ IPSec に移行するには、次が必要です。

- レガシー IPSec（ESR）設定のバックアップ
- レガシー IPSec（ESR）のキーと証明書

ステップ 1 レガシー IPSec（ESR）の設定をバックアップします。

a) Cisco ISE CLI ESR シェルにログインし、実行中の設定をブートフラッシュのファイルに保存します。
b) SCP または FTP を使用して、その実行中の設定ファイルをコンピュータにエクスポートします。この保存した ESR 設定ファイルを ESR 設定のバックアップとして使用できます。

ステップ 2 IPSec の設定をエクスポートします。

a) レガシー IPSec（ESR）からキーと証明書をエクスポートします。Cisco ISE でのキーと証明書のエクスポートの詳細については、「Cisco ISE の CA 証明書とキーのバックアップと復元」を参照してください。
b) Cisco ISE CLI ESR シェルから、**show runnning config** コマンドを実行し、実行中の設定と暗号化設定を表示します。
c) レガシー IPSec（ESR）で設定された暗号化設定を、表 131 : レガシー IPSec 設定とネイティブ IPSec 設定の比較：フェーズ 1 の設定および表 132 : レガシー IPSec 設定とネイティブ IPSec 設定の比較：フェーズ 2 の設定に記載されている参照と比較します。

表 131 : レガシー IPSec 設定とネイティブ IPSec 設定の比較：フェーズ 1 の設定および表 132 : レガシー IPSec 設定とネイティブ IPSec 設定の比較：フェーズ 2 の設定は、レガシー IPSec（ESR）の CLI コマンドと、Cisco ISE GUI のネイティブ IPSec 設定でそれらに対応するコマンドとの直接比較を示しています。レガシー IPSec（ESR）の設定情報を使用して、Cisco ISE でネイティブ IPSec を設定できます。

表 *131* : レガシー *IPSec* 設定とネイティブ *IPSec* 設定の比較：フェーズ *1* の設定

レガシー IPSec（ESR）の show running config コマンド	Cisco ISE GUI でのネイティブ IPSec 設定

• **crypto isakmp policy 10**
• **encr aes**
• **hash sha256**
• **authentication pre-share**
• **group 14**
• **crypto isakmp key cisco123 address 0.0.0.0**
	• **認証設定**：事前共有
	• **事前共有キー**：cisco123
	• **IKE バージョン**：IKEv1
	• **フェーズ 1 の設定**
	  • **暗号化アルゴリズム**：AES-128
	  • **ハッシュアルゴリズム**：SHA-256
	  • **DH グループ**：グループ 14

表 *132 :* レガシー *IPSec* 設定とネイティブ *IPSec* 設定の比較：フェーズ *2* の設定

レガシー IPSec（ESR）の show running config コマンド	Cisco ISE GUI でのネイティブ IPSec 設定

• **crypto IPsec transform-set IPsec-ts esp-aes esp-sha256-hmac mode tunnel**
• **crypto map IPsec-crypto-map 10 IPsec-isakmp**
• **set peer 192.168.10.1**
• **set transform-set IPsec-ts**
• **set pfs group14**
• **match address 100**
	• **ESP/AHプロトコル**：ESP
	• **モード**：トンネル
	• **フェーズ 2 の設定**
	  • **暗号化アルゴリズム**：AES-128
	  • **ハッシュアルゴリズム**：SHA-256
	  • **DH グループ**：グループ 14

ステップ 3 レガシー IPSec（ESR）を無効にします。

a) Cisco ISE GUI で、[管理（Administration）] にカーソルを合わせ、**[システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [IPSec] > [レガシーIPSec（ESR）（Legacy IPSec (ESR)）]** に移動します。

b) レガシー IPSec（ESR）を無効にする必要がある Cisco ISE ノードを選択するには、チェックボックスをオンにします。

c) [選択したノードのIPSecの有効化/無効化（Enable/Disable IPSec for Selected Nodes）] フィールドの [無効化（Disable）] オプションボタンをクリックします。

これにより、選択したノードの IPSec が無効になり、Cisco ISE が再起動します。

d) Cisco ISE 管理 CLI から **ISE/admin#show esr status** コマンドを実行して、選択した Cisco ISE ノードの ESR ステータスが無効になっていることを確認します。次の出力が表示されます。

% ESR 5921 は無効です。

e) （オプション）Cisco ISE 管理 CLI から **ISE/admin#esr** コマンドを実行して、ESR シェルが無効になっているかどうかを確認します。

f) Cisco ISE 管理 CLI から **ISE/admin#show interface** コマンドを実行して、Cisco ISE インターフェイスで IP アドレスが復元されているかどうかを確認します。次の出力が表示されます。

GigabitEthernet 1 flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.10.11 netmask 255.255.255.0 broadcast 192.168.10.255 inet6 fe80::250:56ff:fe92:5f13 prefixlen 64 scopeid 0x20<link>.

ステップ 4 ネイティブ IPSec を有効化します。

a) Cisco ISE GUI で、[管理（Administration）] にカーソルを合わせ、**[ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]**に移動します。

b) レガシー IPSec（ESR）設定で以前に選択された NAD を、ネイティブ IPSec 設定でも選択します。

c) [編集（Edit）] をクリックして、NAD の IPSec の詳細を編集します。

d) [ネットワークデバイスグループ（Network Device Group）]セクションの [レガシーIPSec（ESR）（Legacy IPSec (ESR)）] ドロップダウンリストから、[いいえ（No）] を選択します。

e) [保存（Save）] をクリックします。
f) IKEv1 および IKEv2 プロトコルを使用し、IPSec トンネルを介して Cisco ISE PSN と選択した NAD 間のセキュリティ アソシエーションを確立するように、ネイティブ IPSec を設定します。ネイティブ IPSec の設定方法の詳細については、Cisco ISE でのネイティブ IPSec の設定（1410 ページ）を参照してください。

Mobile Device Manager と Cisco ISE との相互運用性

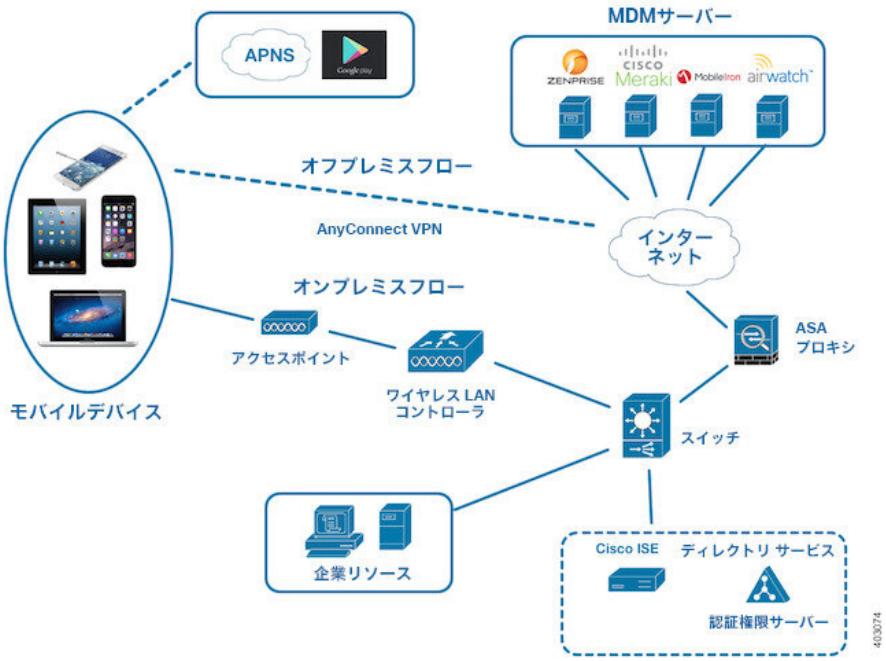
モバイルデバイス管理（MDM）サーバーはモバイル事業者、サービスプロバイダ、および企業に展開されたモバイルデバイスの保護、モニター、管理、およびサポートを行います。従来、MDM サーバーはモバイルデバイスのみをサポートしていました。一部の MDM サーバーは、ネットワーク内のすべてのタイプのデバイス（携帯電話、タブレット、ラップトップ、デスクトップ）を管理するようになり、統合エンドポイント管理（UEM）サーバーと呼ばれています。MDM サーバーはポリシーサーバーとして機能し、ポリシーサーバーは展開環境のモバイルデバイスにある一部のアプリケーション（電子メールアプリケーションなど）の使用を制御します。Cisco ISE は、ネットワーク認証ポリシーの作成に使用できるさまざまな属性に関する情報について、接続された MDM サーバーにクエリします。

さまざまなベンダーの複数のアクティブな MDM サーバーをネットワークで実行できます。これにより、ロケーションやデバイス タイプなどのデバイスの要因に基づいて、異なる MDM サーバーに異なるエンドポイントをルーティングすることができます。

また、Cisco ISE は、Cisco MDM Server Info API バージョン 2 以降を使用して MDM サーバーと統合し、Cisco AnyConnect 4.1 およびシスコの適応型セキュリティアプライアンス 9.3.2 以降を介して VPN 経由でデバイスがネットワークにアクセスできるようにします。

次の図では、Cisco ISE が適用ポイントで、MDM ポリシーサーバーがポリシー情報ポイントです。Cisco ISE は、MDM サーバーからデータを取得して、完全なソリューションを提供します。

図 *34 : MDM* の *Cisco ISE* との相互運用性



1 台以上の外部 MDM サーバーと相互運用するように Cisco ISE を設定します。サードパーティのこのタイプの接続を設定することによって、MDM データベースにある詳細情報を使用できます。Cisco ISE は REST API コールを使用して、外部 MDM サーバーから情報を取得します。Cisco ISE はスイッチ、アクセスルータ、ワイヤレスアクセスポイント、その他のネットワークアクセスポイントに適切なアクセス コントロール ポリシーを適用しています。ポリシーにより、Cisco ISE 対応ネットワークにアクセスしているリモートデバイスが強化されます。

Cisco ISE でサポートされる MDM ベンダーのリストについては、サポートされている統合エンドポイント管理およびモバイルデバイス管理サーバー（1421 ページ）を参照してください。

サポートされているモバイルデバイス管理の使用例

Cisco ISE は外部 MDM サーバーを使用して次の機能を実行します。

- デバイス登録の管理：ネットワークにアクセスする未登録のエンドポイントは、MDM サーバー上でホストされている登録ページにリダイレクトされます。デバイス登録には、ユーザーロール、デバイスタイプなどが含まれます。
- デバイスの修復の処理：修復中のエンドポイントには制限付きアクセス権が付与されます。
- エンドポイントデータの増加：Cisco ISE プロファイリングサービスを使用して収集できない MDM サーバーの情報でエンドポイントデータベースを更新します。Cisco ISE では、[エンドポイント（Endpoints）]ページに表示できる複数のデバイス属性が使用されます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックし、**[ワークセンター**

（**Work Centers**）] > **[ネットワークアクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]** を選択します。

次に、使用可能なデバイス属性の例を示します。

- MDMImei: xx xxxxxx xxxxxx x
- MDMManufacturer: Apple
- MDMModel: iPhone
- MDMOSVersion: iOS 6.0.0
- MDMPhoneNumber: 5550100
- MDMSerialNumber: DNPGQZGUDTFx

- 4 時間に 1 回 MDM サーバーをポーリングし、デバイス コンプライアンス データを確認します。[外部MDMサーバー（External MDM Servers）] ページでポーリング間隔を設定します。（このページを表示するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ネットワークリソース（Network Resources）]** > **[外部MDMサーバー（External MDM Servers）]** を選択します。）
- MDM サーバーを介したデバイス手順の発行：Cisco ISE は、MDM サーバーを介してユーザーのデバイスに対するリモートアクションを発行します。[エンドポイント（Endpoints）] ページを使用して、Cisco ISE 管理ポータルからリモートアクションを開始します。このページを表示するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** を選択します。MDM サーバーの横にあるチェックボックスをオンにし、[MDMアクション（MDM Actions）] をクリックします。表示されるドロップダウンリストから必要なアクションを選択します。

ベンダー MDM 属性

Cisco ISE で MDM サーバーを設定すると、Cisco ISE は MDM サーバーにデバイス属性情報をクエリし、その情報を MDM システムディクショナリに追加します。次の属性は登録ステータスで使用され、MDM ベンダーで一般的にサポートされています。

Cisco ISE は API を使用して、MDM サーバーに必要なデバイス属性をクエリします。Cisco ISE リリース 3.1 以降のリリースでは、MDM API バージョン 3 がサポートされています。バージョン 3 の API には、MAC アドレスのランダム化を使用するエンドポイントを識別するのに役立つデバイス属性について、Cisco ISE が MDM サーバーにクエリを送信できる API が含まれています。Cisco ISE は MDM サーバーに次の属性をクエリします。

- GUID：MAC アドレスを使用してデバイスを識別する固有のデバイス識別子。
- MAC アドレス：UEM または MDM サーバーが特定のデバイス用に記録した MAC アドレスのリスト。1 つのデバイスで最大 5 つの MAC アドレスが共有されます。

MDM サーバーから必須属性の値が提供されない場合、Cisco ISE により次の表に示すデフォルト値が属性フィールドに入力されます。

表 *133 : MDM* 属性と値

属性名	属性ディクショナリ	デフォルト値	UEM または MDM サーバーから予期されるデータ	Microsoft SCCM サーバーから予期されるデータ
DaysSinceLastCheckin MDM API バージョン 3 以降でサポート	MDM	なし	ユーザーが UEM または MDM サーバーとデバイスを最後にチェックインまたは同期してからの日数。有効な範囲は 1 ～ 365 日です。	ユーザーが SCCM サーバーとデバイスを最後にチェックインまたは同期してからの日数。有効な範囲は 1 ～ 365 日です。
DeviceCompliantStatus	MDM	非準拠（NonCompliant）	[準拠（Compliant）] または [非準拠（NonCompliant）]。	[準拠（Compliant）] または [非準拠（NonCompliant）]。
DeviceRegisterStatus	MDM	登録済み（Registered）	[登録済み（Registered）] または [未登録（UnRegistered）]。	[登録済み（Registered）] または [未登録（UnRegistered）]。
DiskEncryptionStatus	MDM	オフ（Off）	[オン（On）] または [オフ（Off）]。	[オン（On）] または [オフ（Off）]。
IMEI	MDM	なし	デバイスの IMEI 番号。	適用なし
JailBrokenStatus	MDM	完全（Unbroken）	[到達可能（Reachable）] または [到達不能（UnReachable）]。	[到達可能（Reachable）] または [到達不能（UnReachable）]。
MDMFailureReason	MDM	なし	デバイス障害の理由。	デバイス障害の理由。
MDMServerName	MDM	なし	サーバの名前。	サーバの名前。
MDMServerReachable	MDM	到達可能（Reachable）	[到達可能（Reachable）] または [到達不能（UnReachable）]。	[到達可能（Reachable）] または [到達不能（UnReachable）]。
MEID	MDM	なし	デバイスの MEID 値。	適用なし
Manufacturer	MDM	なし	デバイスの製造元の名前。	適用なし

属性名	属性ディクショナリ	デフォルト値	UEM または MDM サーバーから予期されるデータ	Microsoft SCCM サーバーから予期されるデータ
Model	MDM	なし	デバイスモデルの名前。	適用なし
OsVersion	MDM	なし	デバイスのオペレーティングシステムのバージョン。	適用なし
PhoneNumber	MDM	なし	デバイスの電話番号。	適用なし
PinLockStatus	MDM	オフ（Off）	[オン（On）] または [オフ（Off）]。	適用なし
SerialNumber	MDM	なし	デバイスのシリアル番号。	適用なし
server-type	MDM	なし	Mobile Device Manager サーバーの MDM。 デスクトップデバイスマネージャ サーバーの DM。	デスクトップデバイスマネージャ サーバーの DM。
UDID	MDM	なし	デバイスの UDID 番号。	適用なし
UserNotified	MDM	なし（No）	[あり（Yes）] または [なし（No）]	適用なし
GUID MDM API バージョン 3 以降でサポート	ディクショナリ属性ではない	なし	GUID は、デバイスの MAC アドレス、UDID、MEID、または IMEI 値の代わりにデバイスを識別するために使用される固有のデバイス識別子です。GUID テンプレートは **ID:MDMServer:GUID:{{DeviceId}}** です GUID 値は、Cisco ISE ではなく MDM サーバーによって生成されて提供されます。	適用なし

属性名	属性ディクショナリ	デフォルト値	UEM または MDM サーバーから予期されるデータ	Microsoft SCCM サーバーから予期されるデータ
Macaddresses MDM API バージョン 3 以降でサポート	ディクショナリ属性ではない	なし	UEM または MDM サーバーが特定のデバイス用に記録した MAC アドレスのリスト。1 つのデバイスで最大 5 つの MAC アドレスを共有できます。 Macaddresses 値は、Cisco ISE ではなく、MDM サーバーによって生成されて提供されます。	適用なし

ベンダー固有の属性はサポートされていませんが、ERS API を使用してベンダー固有の属性を交換できる場合があります。サポートされている ERS API については、ベンダーのマニュアルを参照してください。

新しい MDM ディクショナリ属性は認証ポリシーで使用可能です。

サポートされている統合エンドポイント管理およびモバイルデバイス管理サーバー

サポートされる MDM サーバーは、次のベンダーの製品です。

- Absolute
- Blackberry：BES
- Blackberry：Good Secure EMM
- Cisco Meraki Systems Manager
- Citrix XenMobile 10.x（オンプレミス）
- Globo
- IBM MaaS360
- Ivanti（以前の MobileIron UEM）、コアおよびクラウド UEM サービス

  Cisco ISE 3.1 におけるランダムおよび変更 MAC アドレスの処理に関するユースケースでは、MobileIron Core 11.3.0.0 ビルド 24 以降のリリースを統合し、GUID 値を受け取る必要があります。

（注） 一部のバージョンの MobileIron は Cisco ISE では動作しません。MobileIron はこの問題を認識しており、修正があります。詳細については、MobileIron 社までお問い合わせください。

- JAMF Casper Suite
- Microsoft Endpoint Configuration Manager
- Microsoft Endpoint Manager Intune
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE（以前の AirWatch）
- 42Gears

サーバーを Cisco ISE と統合するためにエンドポイント管理サーバーで実行する必要がある設定については、「Integrate UEM and MDM Servers With Cisco ISE」を参照してください。

ISE コミュニティ リソース

How To: Meraki EMM / MDM Integration with ISE

モバイルデバイス管理サーバーで使用されるポート

次の表に、相互に通信ができるように Cisco ISE と MDM サーバー間で開く必要のあるポートを示します。MDM エージェントとサーバーで開く必要があるポートのリストについては、MDM ベンダーのドキュメントを参照してください。

表 *134 : MDM* サーバーにより使用されるポート

MDM サーバー	ポート
MobileIron	443
Citrix XenMobile 10.x（オンプレミス）	443
Blackberry：Good Secure EMM	19005

MDM サーバー	ポート
VMware Workspace ONE（以前の AirWatch）	443
SAP Afaria	443
IBM MaaS360	443
Cisco Meraki	443
Microsoft Intune	80 および 443
Microsoft SCCM	80 および 443

モバイルデバイス管理の統合プロセスフロー

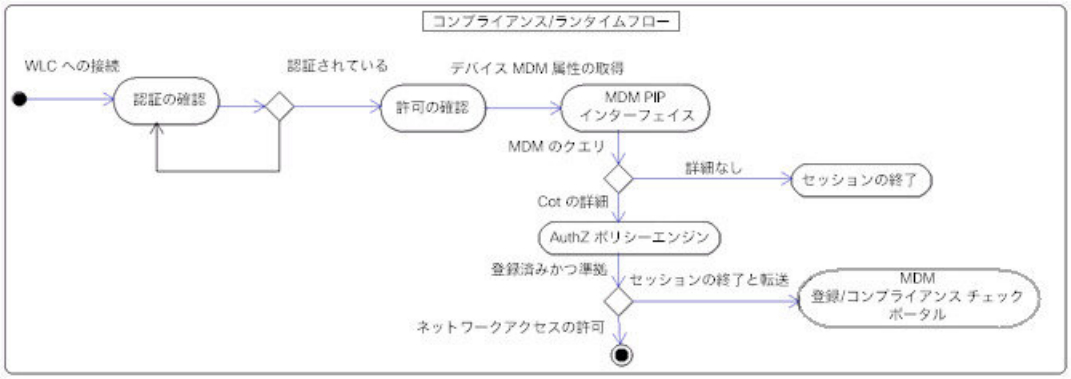
1. ユーザーはデバイスを SSID に関連付けます。
2. Cisco ISE は、MDM サーバーに対して API コールを実行します。
3. この API コールは、ユーザーのデバイスとデバイスのポスチャステータスのリストを戻します。

（注） 入力パラメータは、エンドポイントデバイスの MAC アドレスです。オフプレミスの Apple iOS デバイス（VPN 経由で Cisco ISE に接続するデバイス）の場合、入力パラメータは UDID です。

4. ユーザーのデバイスがこのリストにない場合、デバイスが登録されていないことを意味します。Cisco ISE は、Cisco ISE にリダイレクトされる許可要求を NAD に送信します。ユーザーが MDM サーバーページに表示されます。
5. Cisco ISE は、MDM を使用してデバイスをプロビジョニングし、デバイスを登録するための適切なウィンドウをユーザーに表示します。
6. ユーザーは MDM サーバーにデバイスを登録し、MDM サーバーは自動リダイレクションまたは手動のブラウザリフレッシュによって Cisco ISE に要求をリダイレクトします。
7. Cisco ISE は MDM サーバーに対して再度ポスチャ ステータスのクエリーを実行します。
8. ユーザーのデバイスが MDM サーバーで設定されているポスチャ（コンプライアンス）ポリシーに準拠していない場合、デバイスがポリシーに準拠していないことがユーザーに通知されます。ユーザーは、デバイスがポリシーに準拠していることを確認するために必要なアクションを実行する必要があります。

9. ユーザーのデバイスがポリシーに準拠すると、MDM のサーバーは内部テーブルのデバイスのステータスを更新します。
10. ここでユーザーがブラウザをリフレッシュすると、制御が Cisco ISE に返されます。
11. Cisco ISE はコンプライアンス情報を取得するために MDM サーバーを 4 時間ごとにポーリングし、適切な認可変更（CoA）を発行します。ポーリング間隔を設定できます。また、Cisco ISE は 5 分ごとに MDM サーバーをチェックして使用できるかどうかを確認します。

図 *35 : Cisco ISE* での *MDM* プロセスフロー



（注） 一度に 1 つの MDM サーバーに登録できるデバイスは 1 台のみです。別のベンダーから MDM サービスに同じデバイスを登録する場合、デバイスから前のベンダーのプロファイルを削除する必要があります。MDM サービスは通常、「企業ワイプ」を提供し、これはデバイスからベンダーの設定のみを削除します（デバイス全体ではありません）。ユーザーはこのファイルを削除することもできます。たとえば、iOS デバイスで、**[設定（Settings）]**>**[全般（General）]**>**[デバイス管理（Device management）]** ウィンドウの順に移動し、[削除の管理（Remove Management）] をクリックすることができます。または、Cisco ISE の MyDevices ポータルに移動し、[企業ワイプ（Corporate Wipe）] をクリックすることができます。

モバイルデバイス管理サーバーを使用した、ランダムで変化するMAC アドレスの処理

ランダムで変化する MAC アドレスの使用に起因する問題を回避するために、MAC アドレスではなく一意のデバイス識別子を使用して MDM サーバーに接続されているエンドポイントを識別するように Cisco ISE を設定します。プライバシー対策として、モバイルデバイスは接続先の SSID ごとにランダムで変化する MAC アドレスを使用することが増えています。一部のデスクトップ オペレーティング システムでは、ユーザーが定期的に MAC アドレスをランダム化する機能も提供しています。これは、エンドポイントが MDM サーバーと Cisco ISE に異なる MAC アドレスを提示することを意味します。その結果、MDM サーバーと Cisco ISE が統

合され、エンドポイントに対してアクションが開始されると、2 つのシステムでエンドポイント ID が異なるために問題が発生します。

この問題を回避するために、MAC アドレスではなく固有のデバイス識別子を使用するように Cisco ISE を設定できます。エンドポイントが MDM サーバーに登録されると、GUID 値を含む証明書が MDM サーバーからエンドポイントに送信されます。エンドポイントは、Cisco ISE での認証にこの証明書を使用します。Cisco ISE は、証明書からエンドポイントの GUID を受信します。Cisco ISE と MDM サーバー間のすべての通信は、GUID を使用してエンドポイントを識別し、2 つのシステム間の精度と一貫性を確保します。

GUID は、証明書ベースの認証方式でのみ使用できることに注意してください。SAN URI または CN フィールドに GUID を含めるには、MDM または UEM サーバーによって発行された証明書を設定する必要があります。GUID の SAN URI フィールドを設定することを推奨します。Active Directory に接続されたエンドポイントの認証に同じ証明書が使用される場合、CN フィールドに GUID が存在すると問題が発生する可能性があります。

ユーザー名とパスワードのみを使用する基本認証方式では、GUID ベースのソリューションを利用できません。

EAP-TLS プロトコルを介した MAC アドレスと GUID によるエンドポイントの再認証の場合、コンテキスト可視性サービスを更新するための 1 秒あたりのトランザクション（TPS）は、1 秒あたり 12 ～ 15 エンドポイントです。

GUID データの収集と管理を容易にするために、Cisco ISE MDM API（Cisco ISE MDM API バージョン3）が更新されました。

接続された MDM サーバーの GUID の設定

Cisco ISE にすでに接続している MDM サーバーが最新の Cisco ISE MDM API をサポートし、GUID 情報を送信できるかどうかを確認するには、次の手順を実行します。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [外部MDM（External MDM）]**。
2. [MDM サーバー（MDM Servers）] ウィンドウで、更新する MDM サーバーのチェックボックスをオンにし、[編集（Edit）] をクリックします。
3. [テスト接続（Test Connection）] をクリックします。
4. MDM サーバーが Cisco ISE MDM API バージョン 3 をサポートしている場合は、[デバイス識別子（Device Identifiers）] という新しいセクションが表示されます。

   次のオプションのうち有効にする 1 つ以上のチェックボックスをオンにします。

   - **証明書：SAN URI、GUID**
   - **証明書：CN、GUID**
   - **レガシー MAC アドレス**

   オプションをドラッグアンドドロップして、優先順に並べ替えることができます。たとえば、[証明書：SAN URI、GUID（Cert - SAN URI, GUID）] を最初に配置し、次に [証明書：

CN、GUID（Cert - CN, GUID）] を配置すると、Cisco ISE は最初にエンドポイントの SAN URI 属性と GUID 属性について MDM サーバーにクエリします。要求された属性が使用できない場合、Cisco ISE はエンドポイントの共通名と GUID 属性をクエリします。

5. [保存（Save）] をクリックします。

pxGrid による GUID の共有

Cisco ISE は、pxGrid を介してこの GUID 情報を他のシスコのソリューションと共有できます。たとえば、MDM サーバーから受信した GUID は、pxGrid トピックを使用して展開内の Catalyst Center と共有できます。

Cisco ISE を使用したモバイルデバイス管理サーバーのセットアップ

Cisco ISE で MDM サーバーを設定するには、次の高レベル タスクを実行します。

ステップ 1 Azure にポリシー管理ノード（PAN）の証明書をインポートする Intune を除き、Cisco ISE に MDM のサーバー証明書をインポートします。

ステップ 2 Mobile Device Manager の定義を作成します。

ステップ 3 Cisco WLC で ACL を設定します。

ステップ 4 MDM サーバーに未登録のデバイスをリダイレクトする認証プロファイルを設定します。

ステップ 5 ネットワークに複数の MDM サーバーがある場合は、ベンダーごとに個別の認証プロファイルを設定します。

ステップ 6 MDM 使用例の許可ポリシー ルールを設定します。

Cisco ISE へのモバイルデバイス管理サーバー証明書のインポート

Cisco ISE を MDM サーバーに接続するには、Cisco ISE 信頼できる証明書ストアに MDM サーバー証明書をインポートする必要があります。MDM サーバーに CA 署名付き証明書がある場合は、Cisco ISE 信頼できる証明書ストアにルート証明書をインポートする必要があります。

（注） Microsoft Azure の場合は、Cisco ISE 証明書を Azure にインポートします。「Cisco ISE へのモバイルデバイス管理サーバーとしての Microsoft Intune の接続」を参照してください。

ステップ 1 MDM サーバー証明書を MDM サーバーからエクスポートして、ローカル マシンに保存します。

ステップ 2 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** を選択します。

ステップ 3 [証明書ストアへの新しい証明書のインポート（Import a new Certificate into the Certificate Store）] ウィンドウで、**[ファイルの選択（Choose File）]** をクリックして、MDM サーバーから取得した MDM サーバー証明書を選択します。

ステップ 4 [フレンドリ名（Friendly Name）] フィールドに証明書の名前を入力します。

ステップ 5 [ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにします。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 [証明書ストア（Certificate Store）] ウィンドウに新たに追加した MDM サーバー証明書のリストが表示されることを確認します。

Cisco ISE でのデバイス管理サーバーの定義

Cisco ISE が必要なサーバーと通信できるように、Cisco ISE でモバイルデバイス管理サーバーとデスクトップデバイス管理サーバーを定義します。サーバーとの通信に使用される認証タイプ、Cisco ISE がデバイス管理サーバーのデバイス情報を要求する頻度などを設定できます。

モバイル管理サーバーを定義するには、Cisco ISE でのモバイルデバイス管理サーバーの設定（1427 ページ）を参照してください。

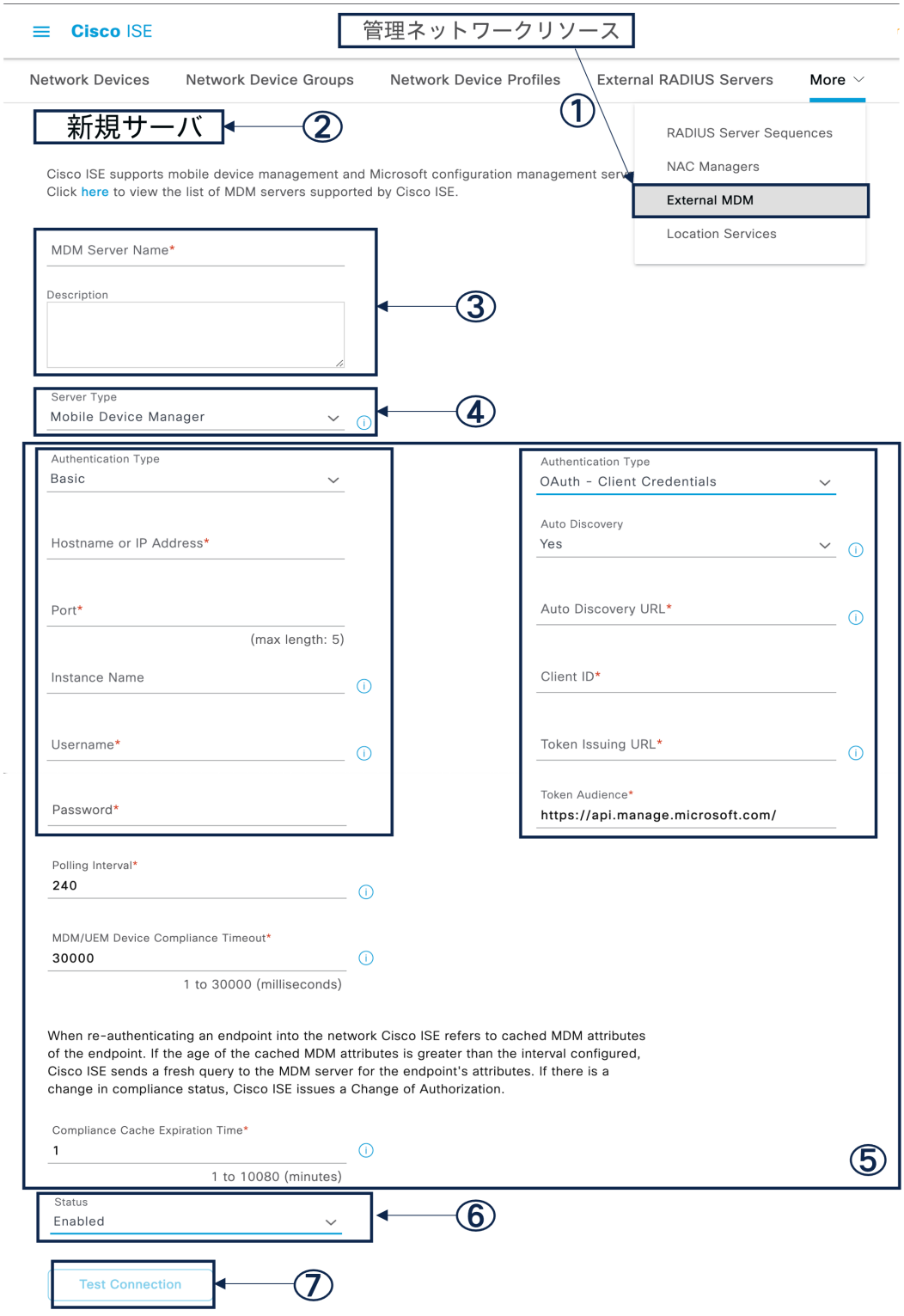
Microsoft System Center Configuration Manager（SCCM）サーバーを定義するには、「デスクトップ デバイス マネージャ サーバーでのエンドポイント コンプライアンスの設定基準ポリシーの選択」を参照してください。

Cisco ISE でのモバイルデバイス管理サーバーの設定

Cisco ISE にエンドポイントの情報を提供する最初の MDM サーバーは、[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] ウィンドウのエンドポイント情報に表示されます。エンドポイントが別の MDM サーバーに接続しても、MDM サーバー情報は自動的に更新されません。[コンテキストの可視性（Context Visibility）] ウィンドウからエンドポイントを削除してから、[コンテキストの可視性（Context Visibility）] ウィンドウに更新された情報を表示するためには、エンドポイントを MDM サーバーに再接続する必要があります。

次の画像は、このタスク中に操作する必要がある Cisco ISE GUI フィールドを示しています。画像中の番号は、次のタスクに含まれる手順の番号に対応しています。

図 *36 : Cisco ISE* での *MDM* サーバーの追加



ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [ネットワークリソース（Network Resources）] > [外部 MDM（External MDM）]**。

ステップ 2 **[MDM/UEM統合（MDM / UEM Integrations）]** ウィンドウで、[追加（Add）] をクリックします。

ステップ 3 追加する MDM サーバーの名前と説明を対応するフィールドに入力します。

ステップ 4 [サーバータイプ（Server Type）] ドロップダウンリストから [Mobile Device Manager] を選択します。

ステップ 5 [認証タイプ（Authentication Type）] ドロップダウンリストから、[基本（Basic）] または [OAuth：クライアントのクレデンシャル（OAuth - Client Credentials）] のいずれかを選択します。

[基本（Basic）] 認証タイプを選択すると、次のフィールドが表示されます。

- [ホスト名/IPアドレス（Host Name/IP Address）]：MDM サーバーのホスト名または IP アドレスを入力します。
- [ポート（Port）]：MDM サーバーとの接続に使用するポートを指定します。通常は 443 です。
- [インスタンス名（Instance Name）]：この MDM サーバーに複数のインスタンスがある場合に、接続するインスタンスを入力します。
- [ユーザー名（Username）]：MDM サーバーへの接続に使用する必要があるユーザー名を入力します。
- [パスワード（Password）]：MDM サーバーへの接続に使用するパスワードを入力します。

[OAuth：クライアントクレデンシャル（OAuth - Client Credentials）] 認証タイプを選択すると、次のフィールドが表示されます。

- [自動検出（Auto Discovery）] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。
- [自動検出URL（Auto Discovery URL）]：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph API Endpoint] の値を入力します。この URL は、アプリケーションが Graph API を使用して Microsoft Entra ID のデータに直接アクセスできるエンドポイントです。詳細については、『MDM および UEM サーバーと Cisco ISE の統合』を参照してください。
- [クライアント ID（Client ID）]：アプリケーションの固有識別子。アプリケーションが Microsoft Azure AD Graph API、Microsoft Intune API などの他のアプリケーションのデータにアクセスする場合に、この属性を使用します。
- [トークン発行URL（Token Issuing URL）]：[OAuth2.0認証エンドポイント（Oauth2.0 Authorization Endpoint）] の値を入力します。これは、Cisco ISE が OAuth2.0 を使用してアクセストークンを取得するエンドポイントです。
- [トークン対象者（Token Audience）]：トークンが対象とする受信者リソースであり、公開されている既知の Microsoft Intune API の **APP ID URL** です。

[ポーリング間隔（Polling Interval）]：Cisco ISE が MDM サーバーをポーリングして非準拠エンドポイントを確認するためのポーリング間隔（分単位）を入力します。MDM サーバー上のポーリング間隔に一致するようにこの値を設定します。有効な範囲は 15 ～ 1440 分です。デフォルト値は 240 分です。多数の非準

拠エンドポイントが原因で発生する可能性のあるパフォーマンスへの影響を最小限に抑えるために、運用環境ではポーリング間隔を 60 分より長く設定することをお勧めします。

ISE は、MAC アドレス/GUID ベースの非準拠 API コールを介して非準拠デバイス情報のリストを取得します（例：）

これは一括取得APIであるため、ISEはMDMサーバーによって提供されるページング情報を使用します。

ISEは、非準拠API応答に基づいてエンドポイントレコードの準拠に関する情報を更新します。ISEは、これらの非準拠デバイスでアクティブセッションを検出すると、再認証します。

ISE は、非準拠 API コールを最大で 200 の要求または 20,000 のエンドポイントレコードのいずれか早い方に制限します。

ポーリング間隔を 0 に設定すると、Cisco ISE は MDM サーバーへのポーリングを無効にします。

（注） Cisco ISE は、非準拠エンドポイントからの API コールを 200 に制限します。外部 MDM サーバーが 20000 を超える非準拠エンドポイントから要求を受信した場合、外部 MDM サーバーのポーリング間隔は自動的に 0 に設定されます。また、Cisco ISE に次のアラームが表示されます。

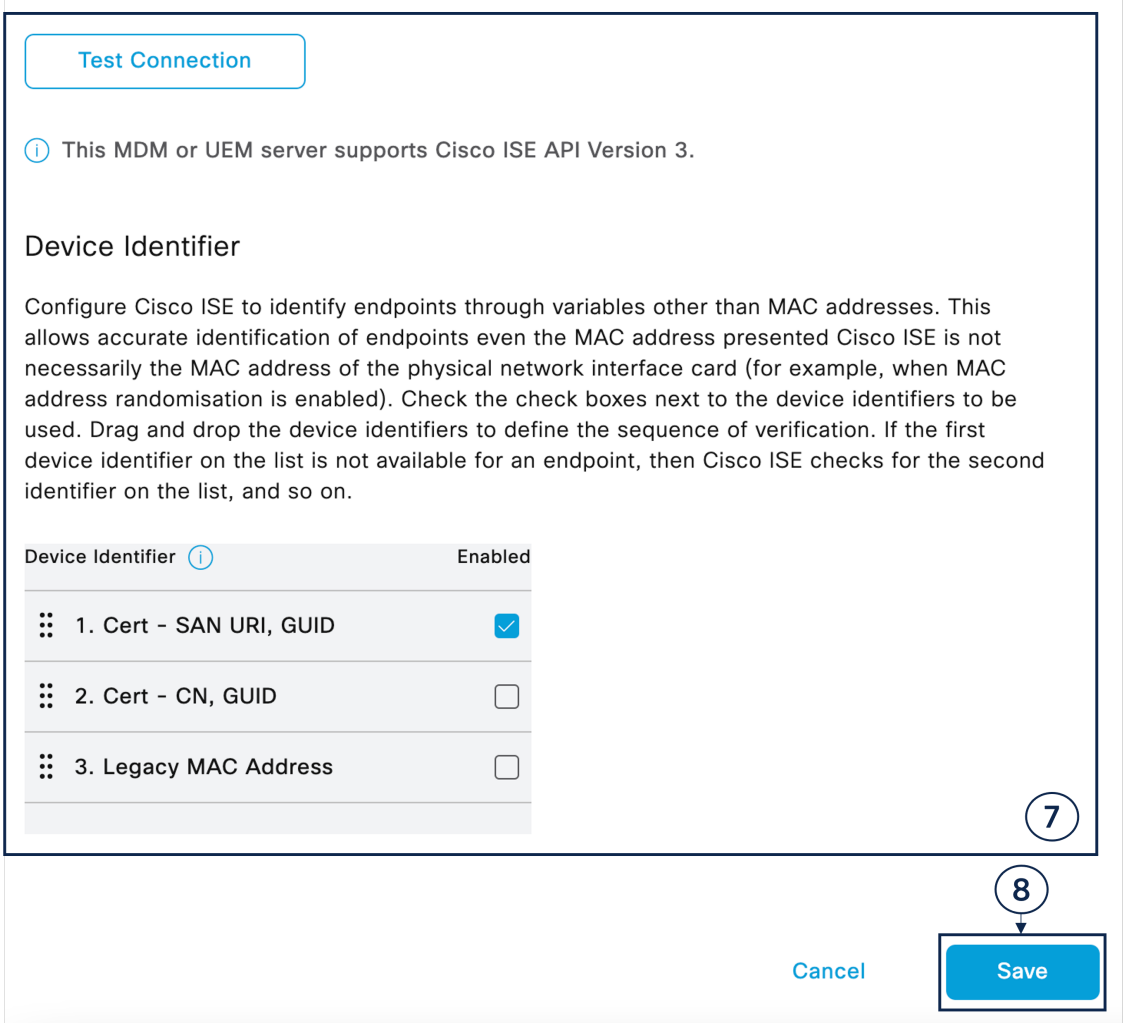
MDM コンプライアンスポーリングが無効：定期的なコンプライアンスポーリングで、膨大な非準拠デバイス情報を受信しました（MDM Compliance Polling Disabled: Reason is Periodic Compliance Polling received huge non-compliance device information）。

[MDM/UEMデバイス コンプライアンス タイムアウト（MDM / UEM Device Compliance Timeout）]：Cisco ISE が MDM または UEM サーバーへのクエリ後に MDM または UEM サーバーからの応答を待機するタイムアウト期間をミリ秒単位で入力します。デフォルト値は 30000 ミリ秒です。1 台の MDM サーバーまたは UEM サーバーのみにクエリを実行する場合は、1 ～ 30000 ミリ秒の値を設定できます。デバイスのコンプライアンス API を使用して複数の MDM サーバーまたは UEM サーバーにクエリを実行する場合は、300 ミリ秒未満の値を設定して、システムパフォーマンスへの影響を回避する必要があります。

ステップ 6 [ステータス（Status）] ドロップダウンリストから [有効（Enabled）] を選択します。

ステップ 7 MDM サーバーが Cisco ISE に接続されているかどうかを確認するには、[接続のテスト（Test Connection）] をクリックします。[接続のテスト（Test Connection）]は、すべての使用例（ベースラインの取得、デバイス情報の取得など）の権限を確認するためのものではないことに注意してください。これらは、サーバーが Cisco ISE に追加されるときに検証されます。

図 *37 : Cisco ISE* での *MDM* サーバーの追加



設定する MDM サーバーが Cisco ISE MDM API バージョン 3 をサポートしており、属性 GUID を Cisco ISE と共有できる場合は、[デバイス識別子（Device Identifiers）] 領域が表示されます。詳細については、モバイルデバイス管理サーバーを使用した、ランダムで変化する MAC アドレスの処理（1424 ページ）を参照してください。

有効にする次のオプションの 1 つ以上のチェックボックスをオンにし、各オプションを適切な場所にドラッグアンドドロップして、優先順に配置します。

- **証明書：SAN URI、GUID**
- **証明書：CN、GUID**
- **レガシー MAC アドレス**

ステップ 8 [保存（Save）] をクリックします。

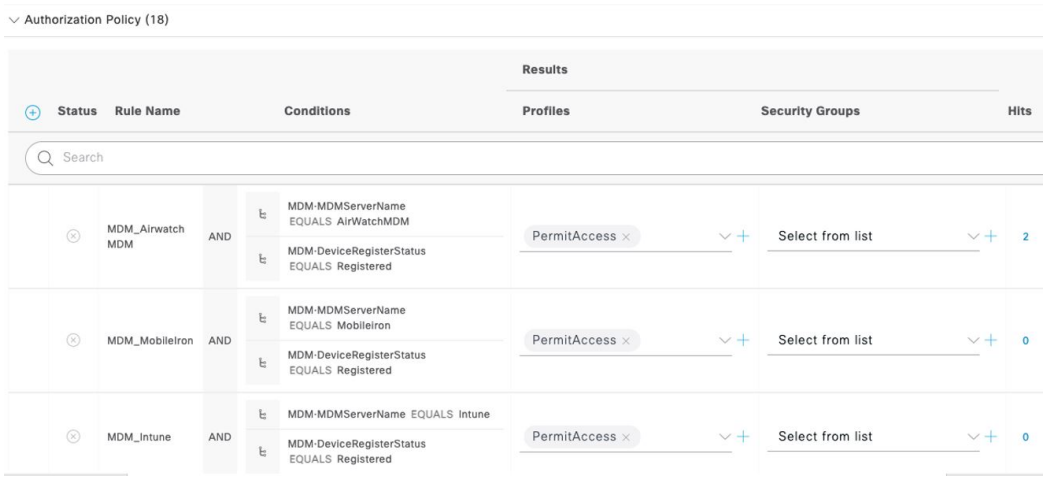
全般的な MDM 設定または UEM 設定の構成

Cisco ISE が複数の MDM サーバーまたは UEM サーバーを照会し、エンドポイントが接続されている MDM サーバーまたは UEM サーバーを識別できるように MDM 設定または UEM 設定を構成します。

たとえば、新しいエンドポイントが Intune に登録されている場合、Cisco ISE でエンドポイントの Intune を評価するには、認証ポリシーにデバイスタイプやユーザータイプといったいくつかの条件が必要になります。

[複数のMDM/UEM統合のクエリ（Query Multiple MDM / UEM Integrations）] オプションを有効にすると、Cisco ISE は認証ポリシーにリストされているすべての MDM サーバーにクエリを実行し、エンドポイントが登録されているサーバーを識別します。

図 *38* : 複数の *MDM* サーバーを含む認証ポリシーの例



ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [全般的なMDM/UEM設定（General MDM / UEM Settings）]** を選択します。

ステップ 2 [全般的な MDM/UEM 設定（General MDM / UEM Settings）] ウィンドウで、[複数の MDM/UEM 統合のクエリ（Query Multiple MDM / UEM Integrations）] をクリックします。

（注） デフォルトでは、[複数の MDM/UEM 統合のクエリ（Query Multiple MDM / UEM Integrations）] オプションは無効になっています。

ステップ 3 次のいずれかのオプションを選択します。

- [エンドポイントが構成済みのプライマリMDM/UEMサーバーに登録されていない（Endpoint is not Registered with the Configured Primary MDM/UEM Server）]：次のシナリオで、Cisco ISE が認証ポリシーで指定されたすべての MDM または UEM サーバーからコンプライアンス情報を取得するようにする場合は、このオプションを選択します。
  - エンドポイントの登録情報がプライマリ MDM または UEM サーバーに存在しない。

- エンドポイントが初めてネットワークにアクセスしている。
- エンドポイントが Cisco ISE に保存されていない。
- エンドポイントが登録されている MDM または UEM サーバーがわからない。

MDM サーバーとのエンドポイントの関連付けは、認証ポリシーの MDM サーバー名の条件に基づいてチェックされます。

- [プライマリMDM/UEMサーバーがエラー/例外応答を送信する（Primary MDM/UEM Server Sends Error/exception Response）]：プライマリ MDM または UEM サーバーがエラーメッセージを送信した場合、または到達不能な場合に、Cisco ISE が認証ポリシーで指定された他の MDM または UEM サーバーにクエリを実行するようにする場合は、このオプションを選択します。

ステップ 4 [保存（Save）] をクリックします。

MDM または UEM サーバーのタイムアウトの設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [外部 MDM（External MDM）]** を選択します。

ステップ 2 [MDM/UEM統合（MDM / UEM Integrations）] ウィンドウで、タイムアウト値を変更する MDM サーバーまたは UEM サーバーの横のチェックボックスをオンにします。

ステップ 3 [タイムアウトの変更（Change Timeout）] をクリックします。これは [MDM/UEMデバイスコンプライアンスタイムアウト（MDM / UEM Device Compliance Timeout）] で、Cisco ISE が MDM または UEM サーバーへのクエリ後に MDM または UEM サーバーからの応答を待機する期間です。

ステップ 4 [接続タイムアウト（ミリ秒）（Connection Timeout (milliseconds)）] フィールドにタイムアウト値を入力します。

（注） MDM サーバーまたは UEM サーバーのデフォルトのタイムアウトは、30000 ミリ秒です。

ステップ 5 [変更（Change）] をクリックします。

Microsoft Intune と Microsoft SCCM 用の Cisco ISE MDM サポート

- **Microsoft Intune**：Cisco ISE は、モバイルデバイスを管理するパートナー MDM サーバーとして Microsoft Intune のデバイス管理をサポートしています。

  Microsoft Intune サーバーの管理モバイルデバイスの OAuth 2.0 クライアント アプリケーションとして Cisco ISE を設定します。Cisco ISE は、Azure からトークンを取得し、Cisco ISE Intune アプリケーションとのセッションを確立します。

Microsoft Intune がクライアントアプリケーションとどのように通信するかの詳細については、https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx を参照してください。

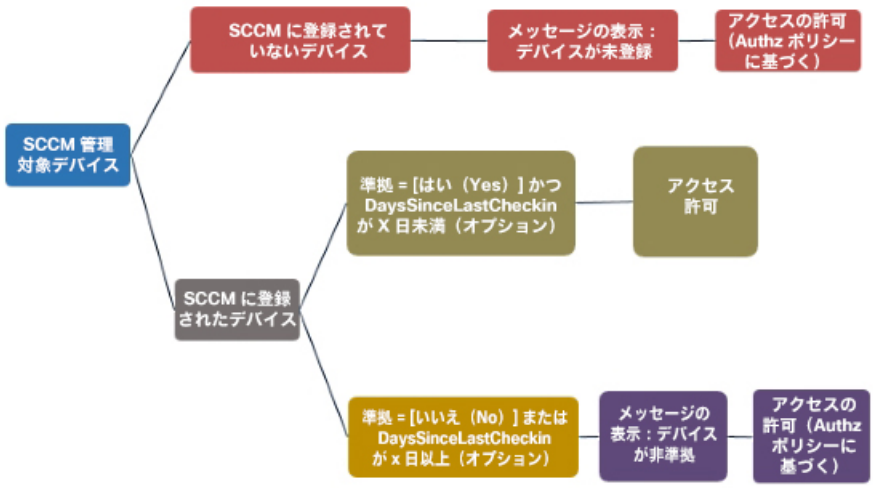
- **デスクトップ デバイス マネージャ（Microsoft SCCM）**：Cisco ISE は Microsoft System Center Configuration Manager（SCCM）を Windows コンピュータの管理用パートナー MDM サーバーとしてサポートしています。

  Microsoft SCCM 統合のパフォーマンスとスケーラビリティの情報については、「Size and Scale Numbers for Configuration Manager」を参照してください。Microsoft は、コンポーネント オブジェクト モデル（COM）に基づく Windows Management Instrumentation（WMI）インターフェイスを使用しているため、スケーラビリティに制限があります。

Microsoft SCCM のワークフロー

Cisco ISE はデバイスが登録されているかどうかについて、Microsoft SCCM サーバーから情報を取得します。エンドポイントが登録されている場合、Cisco ISE はその準拠のステータスをチェックします。次の図に、Microsoft SCCM により管理されるデバイスのワークフローを示します。

図 *39 : SCCM* のワークフロー



デバイスをネットワークに接続し、Microsoft SCCM ポリシーが一致すると、Cisco ISE はコンプライアンスと最終ログイン（チェックイン）時間を取得するために、関連する SCCM サーバーを照会します。この情報を使用して、Cisco ISE は [エンドポイント（Endpoints）] のリストのデバイスのコンプライアンス ステータスと lastCheckinTimeStamp を更新します。

デバイスが準拠していないか、または Microsoft SCCM サーバーに登録されていない場合にリダイレクトプロファイルが認証ポリシーで使用されている場合、デバイスが準拠していないか、または Microsoft SCCM に登録されていないというメッセージがユーザーに表示されます。ユーザーがメッセージを受け取った後、Cisco ISE は Microsoft SCCM 登録サイトへ CoA を発行できます。認証ポリシーとプロファイルに基づいてユーザーにアクセスを許可します。

Microsoft SCCM サーバー接続の監視

Microsoft SCCM のポーリング間隔は設定できません。

Cisco ISE は、Microsoft SCCM サーバーとの接続を検証し、Cisco ISE が Microsoft SCCM サーバーへの接続を失うと MDM ハートビートジョブを実行し、アラームを発生させます。ハートビートジョブの間隔は設定できません。

Microsoft System Center Configuration Manager のポリシー設定例

Microsoft SCCM をサポートするために次の新しいディクショナリエントリを使用します。

- **MDM.DaysSinceLastCheckin**：ユーザーが最後に確認するか、または Microsoft SCCM とデバイスを同期してからの日数。値は 1 ～ 365 日の範囲になります。
- **MDM.UserNotified**：有効な値は **Y** または **N** です。この値は、デバイスが登録されていないことをユーザーに通知したかどうかを示します。その後で、ユーザーにネットワークへの制限付きアクセスを許可してから、登録ポータルにリダイレクトしたり、ユーザーによるネットワークへのアクセスを拒否したりできます。
- **MDM.ServerType**：有効な値は、MDM サーバーの場合は **MDM**、デスクトップデバイス管理の場合は **DM** です。

次に、Microsoft SCCM をサポートするポリシーセットの例を示します。

ポリシー名	条件	結果
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess

ポリシー名	条件	結果
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCMRedirect
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCMRedirect
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

Cisco ISE 用の Microsoft System Center Configuration Manager サーバーの設定

Cisco ISE は、Windows Management Instrumentation（WMI）を使用して Microsoft SCCM サーバーと通信します。Microsoft SCCM を実行している Windows サーバーで WMI を設定します。

（注） Cisco ISE 統合に使用するユーザーアカウントは、次のいずれかの条件を満たしている必要があります。

- SMS 管理ユーザーグループのメンバーである。
- WMI 名前空間で SMS オブジェクトと同じアクセス許可がある。

  `root\sms\site_<sitecode>`

  サイトコードは Microsoft SCCM サイトです。

Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows Server 2012 および Windows Server 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティングシステムの特定のレジストリ キーを完全に制御することはできません。Microsoft Active Directory の管理者は、Microsoft Active Directory ユーザーに次のレジストリキーに対する完全制御権限を提供する必要があります。

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

次の Microsoft Active Directory バージョンでは、レジストリを変更する必要はありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、まず Microsoft Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーアイコンを右クリックし、[所有者（Owner）] タブを選択します。
ステップ 2 [アクセス許可（Permissions）] をクリックします。
ステップ 3 [詳細設定（Advanced）] をクリックします。

ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限

Windows 2012 R2 の場合は、Microsoft AD ユーザーに次のレジストリキーに対する完全制御権限を提供します。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell で次のコマンドを使用して、レジストリキーに完全な権限が付与されているかどうかを確認します。

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

Microsoft AD ユーザーがドメイン管理者グループではなく、ドメインユーザーグループに所属している場合は、次の権限が必要です。

- Cisco ISE がドメインコントローラに接続できるようにするには、レジストリキーを追加します。
- ドメイン コントローラで DCOM を使用するための権限 （1075 ページ）
- WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （1441 ページ）

これらの権限は、次のバージョンの Microsoft AD でのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ドメインコントローラへの Cisco ISE の接続を許可するためにレジストリキーを追加

Cisco ISE がドメインユーザーとして接続し、ログイン認証イベントを取得できるようにするには、ドメインコントローラにいくつかのレジストリ キーを手動で追加する必要があります。エージェントはドメインコントローラまたはドメイン内のマシンには必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

DllSurrogate キーの値には、2 つのスペースが含まれていることを確認します。レジストリを手動で更新する場合は、2 つのスペースのみを含める必要があり、引用符は含めないでください。レジストリを手動で更新する際は、AppID、DllSurrogate、およびその値に引用符が含まれていないことを確認してください。

前述のスクリプトに示すように、ファイルの末尾の空の行を含めて、空の行は保持します。

Windows コマンドプロンプトで次のコマンドを使用して、レジストリキーが作成され、正しい値が設定されているかどうかを確認します。

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

ドメイン コントローラで DCOM を使用するための権限

Cisco ISE パッシブ ID サービスに使用される Microsoft Active Directory ユーザーには、ドメイン コントローラ サーバーでDCOMを使用する権限が必要です。**dcomcnfg** コマンドラインツールを使用して権限を設定します。

ステップ 1 コマンド ラインから **dcomcnfg** ツールを実行します。

ステップ 2 [コンポーネントサービス（Component Services）] を展開します。

ステップ 3 **[コンピュータ（Computers）]** > **[マイコンピュータ（My Computer）]** を展開します。

ステップ 4 メニューバーで[アクション（Action）]を選択し、[プロパティ（Properties）]をクリックして[COMセキュリティ（COM Security）] をクリックします。

ステップ 5 Cisco ISEがアクセスと起動の両方に使用するアカウントには許可権限が必要です。4つのオプション（[アクセス権限（Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対する [制限の編集（Edit Limits）] と [デフォルトの編集（Edit Default）]）のすべてに Microsoft Active Directory ユーザーを追加します。

ステップ 6 [アクセス権限（Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対してローカルアクセスとリモートアクセスをすべて許可します。

図 ***40 : [***アクセス権限（***Access Permissions***）***]***に対するローカルアクアセスとリモートアクセス

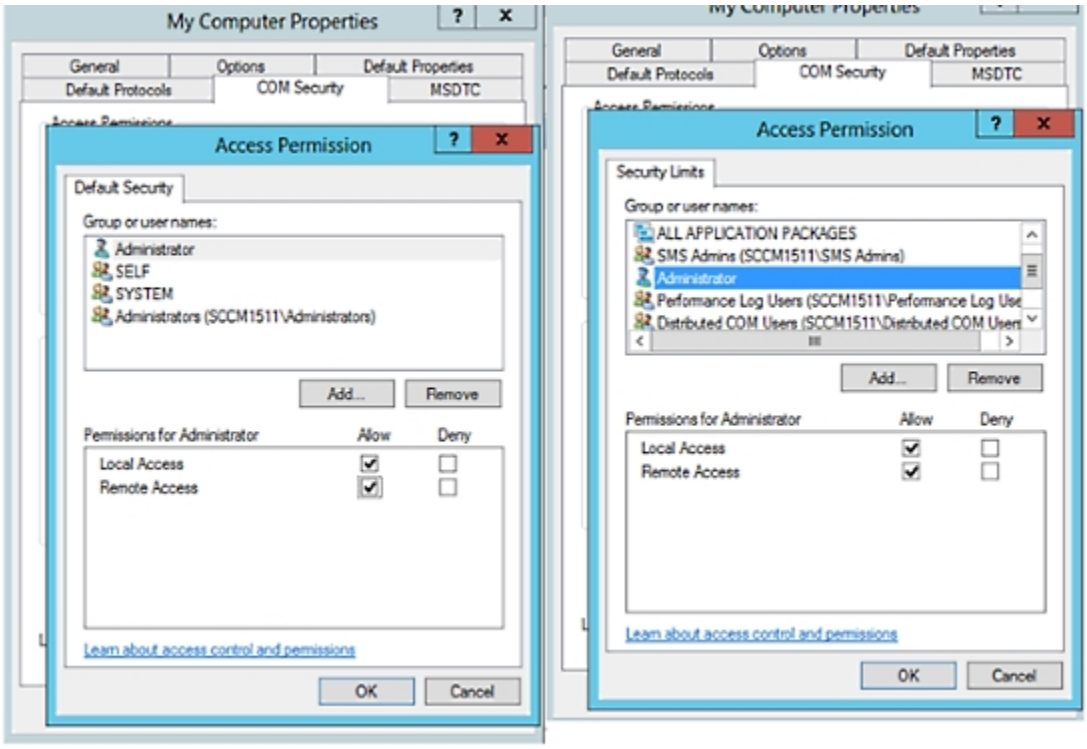
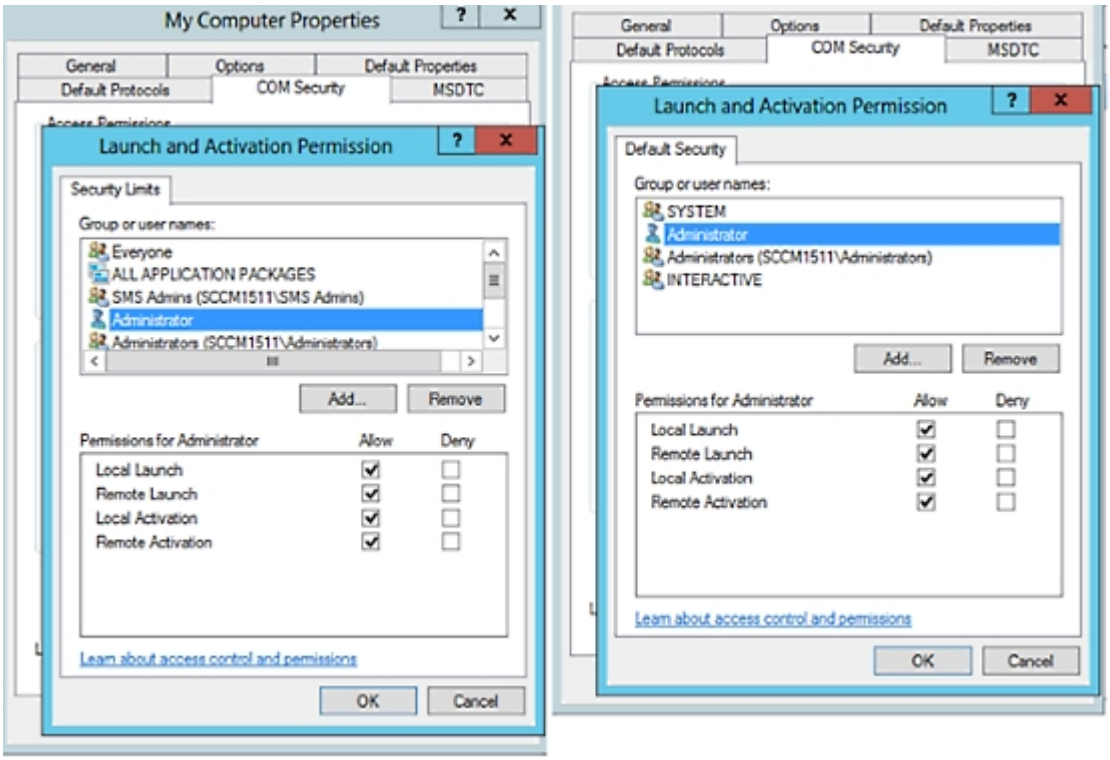


図 *41 : [*起動およびアクティブ化の権限（***Launch and Activation Permissions***）*]* のローカルアクセスとリモートアクセス



WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Microsoft Active Directory ユーザーには実行メソッドおよびリモートの有効化のための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

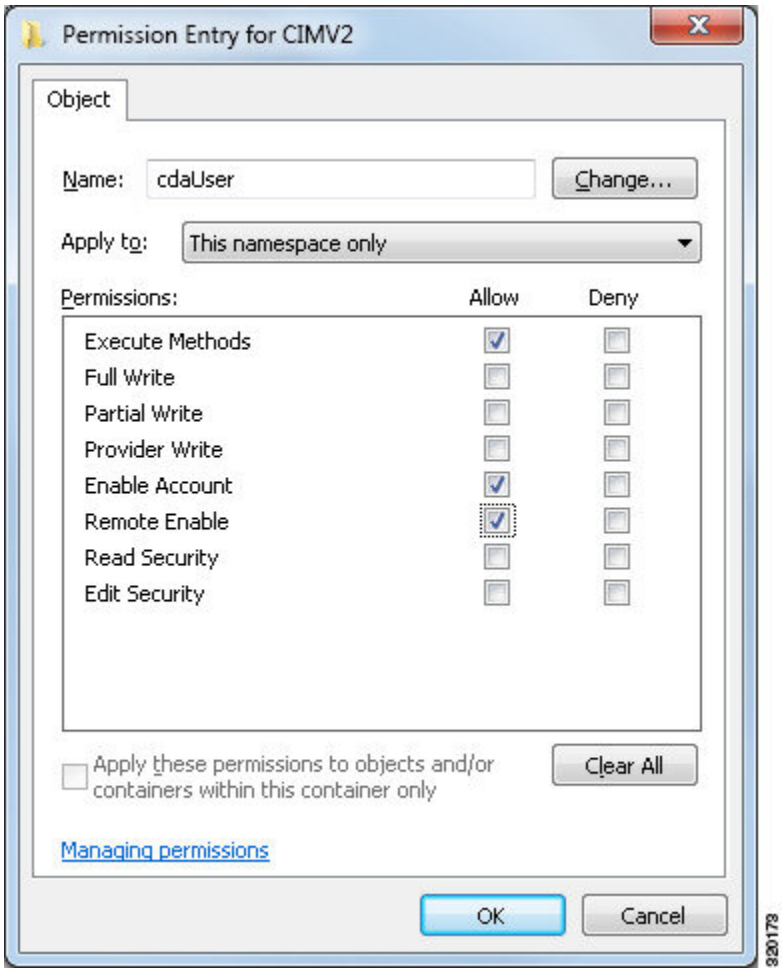
ステップ 1 **[スタート（Start）]** > **[実行（Run）]** を選択し、`wmimgmt.msc` と入力します。

ステップ 2 [WMIコントロール（WMI Control）] を右クリックし、[プロパティ（Properties）] をクリックします。

ステップ 3 [セキュリティ（Security）] タブで、[ルート（Root）] を展開し、[CIMV2] を選択します。

ステップ 4 [セキュリティ（Security）] をクリックします。

ステップ 5 次のイメージに示すように、Microsoft Active Directory ユーザーを追加し、必要な権限を設定します。



WMI アクセス用にファイアウォール ポートを開く

Microsoft Active Directory ドメインコントローラのファイアウォール ソフトウェアは、WMI へのアクセスをブロックすることがあります。ファイアウォールをオフにするか、または次のポートへの特定の IP アドレス（Cisco ISE の IP アドレス）のアクセスを許可することができます。

- TCP 135：一般的な RPC ポート。非同期 RPC コールを実行すると、このポートでリスニングしているサービスが、この要求を処理できるコンポーネントが使用しているポートをクライアントに通知します。
- UDP 138：NetBIOS データグラムサービス
- TCP 139：NetBIOS セッションサービス
- TCP 445：サーバーメッセージブロック（SMB）

（注） Cisco ISE は SMB 2.0 をサポートしています。

数値の大きいポートは動的に割り当てられるか、または手動で設定できます。ターゲットとして *%SystemRoot%\System32\dllhost.exe* を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォールルールを、特定の IP アドレス（Cisco ISE の IP）に割り当てることができます。

デスクトップ デバイス マネージャ サーバーでのエンドポイント コンプライアンスの設定基準ポリシーの選択

Cisco ISE に追加されたデスクトップ デバイス マネージャ サーバー（Microsoft SCCM サーバーなど）で使用可能な基準ポリシーを表示し、ネットワークアクセスのエンドポイントコンプライアンスを確認するための特定の基準ポリシーを選択できます。デスクトップデバイスマネージャ サーバーで有効化および展開された設定基準ポリシーは、Cisco ISE 管理ポータルで確認できます。

（注） デスクトップデバイス管理サーバーで自分のユーザー権限を確認し、基準ポリシーとコンプライアンス情報を Cisco ISE に送信するために必要なセキュリティ権限があることを確認します。デスクトップデバイスマネージャの [セキュリティ（Security）]>[管理者ユーザー（Administrator Users）] フォルダに管理者を追加する必要があります。

Cisco ISE GUI でデスクトップ デバイス マネージャ サーバーの基準ポリシーを表示するには、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[外部 MDM（External MDM）]** > **[MDM サーバー（MDM Servers）]** を選択します。

新しいデスクトップ デバイス マネージャ サーバーを Cisco ISE に追加し、構成基準ポリシーを選択します。

1. [MDMサーバー（MDM Servers）] ウィンドウで、[追加（Add）] をクリックします。
2. [サーバータイプ（Server Type）] ドロップダウンリストから、[デスクトップデバイスマネージャ（Desktop Device Manager）] を選択します。
3. 次のフィールドに必要な詳細情報を入力します。
   - **[ホスト名/IP アドレス（Host Name / IP Address）]**：Microsoft SCCM サーバーのホスト名または IP アドレスを入力します。
   - **[インスタンス名（Instance Name）]**：Microsoft SCCM サーバーに複数のインスタンスがある場合、接続するインスタンスを入力します。

- **[ユーザー名（Username）]**：Microsoft SCCM サーバーへの接続に使用する必要があるユーザー名を入力します。
- **[パスワード（Password）]**：Microsoft SCCM サーバーへの接続に使用する必要があるパスワードを入力します。
- **[準拠デバイス再認証クエリの時間間隔（Time Interval For Compliance Device ReAuth Query）]**：エンドポイントが認証または再認証されるときに、Cisco ISE はそのエンドポイントの MDM 変数を取得するのにキャッシュを使用します。キャッシュされた値の経過時間がこのフィールドで設定された値よりも大きい場合、Cisco ISE は新しい値を取得するために MDM サーバーに新しいデバイスクエリを送信します。準拠ステータスが変更されると、Cisco ISE は適切な CoA をトリガーします。

  有効な範囲は 1 ～ 10080 分です。デフォルト値は 1 分です。

4. [ステータス（Status）] ドロップダウンリストで [有効化（Enabled）] を選択します。

サーバーが Cisco ISE に接続されていることを確認するには、[テスト接続（Test Connection）] ボタンをクリックします。このサーバーで使用可能な設定基準ポリシーを表示するには、[保存して続行（Save & Continue）] をクリックします。新しいウィンドウが開き、基準ポリシーの名前と ID のリストが表示されます。

既存のデスクトップ デバイス マネージャ サーバーから構成基準ポリシーを選択

[MDM サーバー（MDM Servers）] ウィンドウで、目的のサーバーのチェックボックスをオンにし、[編集（Edit）] をクリックします。このサーバーで使用可能な基準ポリシーのリストを表示するには、[設定基準（Configuration Baselines）] タブをクリックします。

デフォルトでは、すべての基準ポリシーが選択されています。[名前（Name）] の横にあるチェックボックスをオフにして、すべての基準ポリシーの選択を解除します。ポリシーの名前の横にあるチェックボックスをオンにして、必要な基準ポリシーを選択します。[保存（Save）] をクリックします。

エンドポイントのコンプライアンスは、選択した設定基準ポリシーに基づいてチェックされます。

デスクトップ デバイス マネージャ サーバーの設定基準ポリシーに変更がある場合は、Cisco ISE で更新する変更に対して [設定基準（Configuration Baselines）] タブの [今すぐ更新（Update Now）] ボタンをクリックします。

Windows エンドポイントのデバイス識別子の設定

デスクトップ デバイス マネージャ サーバーは、特定の属性を識別子として使用して、ネットワークに接続するエンドポイントを確認します。エンドポイントの MAC アドレスは、最も一般的に使用される識別子です。ただし、ドングル、ドッキングステーション、または MAC アドレスのランダム化技術が使用されている場合、MAC アドレスは最も信頼性の高い識別子ではありません。

ホスト名を識別子として使用するように選択できるようになりました。ホスト名は、証明書で使用可能な共通名（CN）または SAN-DNS 属性から取得されます。エンドポイントの証明書

ベースの認証は、ホスト名を使用して基準ポリシーのコンプライアンスをチェックするために必須です。

デスクトップデバイスマネージャサーバーのデバイス識別子を設定するには、[サーバー設定（Server Configuration）]タブに移動します。メインメニューから、**[管理（Administration）]**>**[ネットワークリソース（Network Resources）]**>**[外部 MDM（External MDM）]**>**[MDM サーバー（MDM Servers）]**>**[編集（Edit）]**を選択します。

[デバイス識別子の設定（Device Identifier Configurations）]セクションでは、次の順序で識別子がデフォルトで有効になっています。

1. **レガシーMACアドレス**
2. **Cert**：**CN、ホスト名**
3. **Cert**：**SAN-DNS、ホスト名**

識別子の選択を解除するには、その識別子のチェックボックスをオフにします。属性をドラッグして、検証のためにサーバーで使用される順序を並べ替えることができます。

デバイス識別子の設定の確認

ホスト名が検証に使用される場合、GUID は Cisco ISE によってエンドポイントに割り当てられます。[ライブログ（Live Logs）]ウィンドウを表示し（Cisco ISE GUI で、[メニュー（Menu）]アイコン（☰）をクリックし、**[操作（Operations）]**>**[RADIUS]**>**[ライブログ（Live Logs）]**を選択して、GUID エントリの詳細を確認します。

未登録のデバイスのリダイレクトのための許可プロファイルの設定

各外部MDMサーバーの未登録のデバイスをリダイレクトするには、Cisco ISEで許可プロファイルを設定する必要があります。

始める前に

- Cisco ISE でMDMサーバー定義を作成したことを確認します。Cisco ISE をMDMサーバーと正常に統合できてはじめて、MDM ディクショナリは読み込まれます。その後、MDM ディクショナリ属性を使用して許可ポリシーを作成できます。
- 未登録のデバイスをリダイレクトするために、Cisco WLC の ACL を設定します。
- インターネット接続にプロキシを使用していて、MDM サーバーが内部ネットワークの一部である場合は、プロキシバイパスリストに MDM サーバー名または IP アドレスを追加する必要があります。Cisco ISE GUI で、[メニュー（Menu）]アイコン（☰）をクリックし、**[管理（Administration）]**>**[システム（System）]**>**[設定（Settings）]**>**[プロキシ（Proxy）]**を選択して、このアクションを実行します。

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）] > [追加（Add）]** を選択します。

ステップ 2 準拠していないまたは登録されていない未登録デバイスをリダイレクトするための許可プロファイル作成します。

ステップ 3 MDM サーバー名と一致する認証プロファイルの名前を [名前（Name）] フィールドに入力します。

ステップ 4 [アクセスタイプ（Access Type）] ドロップダウンリストから [ACCESS_ACCEPT] を選択します。

ステップ 5 [共通タスク（Common Tasks）] セクションで、[Web リダイレクション（Web Redirection）] チェックボックスをオンにし、ドロップダウンリストから [MDM リダイレクト（MDM Redirect）] を選択します。

ステップ 6 ワイヤレス LAN コントローラ上で設定した ACL の名前を [ACL] ドロップダウンリストから選択します。

ステップ 7 [値（Value）] ドロップダウンリストから MDM ポータルを選択します。

ステップ 8 使用する MDM サーバーを [MDM サーバー（MDM Server）] ドロップダウンリストから選択します。

ステップ 9 [送信（Submit）] をクリックします。

次のタスク

MDM 使用例の許可ポリシー ルールの設定。

MDM 使用例の許可ポリシー ルールの設定

MDM 設定を完了するには、Cisco ISE で認証ポリシールールを設定します。

始める前に

- Cisco ISE 証明書ストアに MDM サーバー証明書を追加します。
- Cisco ISE で MDM サーバー定義を作成したことを確認します。正常に MDM サーバーと Cisco ISE を統合した後にのみ、MDM ディクショナリが入力され、MDM ディクショナリ属性を使用して認証ポリシーを作成できます。
- 未登録または非準拠のデバイスをリダイレクトするために、Cisco WLC の ACL を設定します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu） アイコン（☰）をクリックし、**[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]** を選択し、認証ポリシールールを表示するポリシーセットを展開します。

ステップ 2 次のルールを追加します。

- [MDM_Un_Registered_Non_Compliant]：MDM サーバーに登録されていないか、MDM ポリシーに準拠していないデバイスの場合。要求がこのルールに一致すると、ユーザーに Cisco ISE MDM ウィンドウが表示され、MDM サーバーでのデバイスの登録に関する情報が示されます。

（注） このポリシーでは、**MDM.MDMServerName** 条件を使用しないでください。この条件を使用すると、エンドポイントが MDM サーバーに登録されている場合にのみ、エンドポイントはポリシーに一致します。

- [PERMIT]：デバイスが Cisco ISE と MDM に登録されており、Cisco ISE と MDM のポリシーに準拠している場合、Cisco ISE で設定されたアクセス コントロール ポリシーに基づいてネットワークへのアクセス権が付与されます。

ステップ 3 [保存（Save）] をクリックします。

MDM 相互運用性のためのワイヤレス LAN コントローラでの ACL の設定

未登録のデバイスおよび証明書プロビジョニングをリダイレクトするために認証ポリシーで使用する ACL をワイヤレスコントローラで設定します。ACL は次の順序にする必要があります。

ステップ 1 サーバーからクライアントへのすべての発信トラフィックを許可します。

ステップ 2 （任意）トラブルシューティングのためにクライアントからサーバーへの ICMP 着信トラフィックを許可します。

ステップ 3 未登録および非準拠のデバイスが MDM エージェントをダウンロードし、コンプライアンスチェックに進むように MDM サーバーへのアクセスを許可します。

ステップ 4 Web ポータルおよびサプリカント用 Cisco ISE、および証明書プロビジョニングフローに対するクライアントからサーバーへのすべての着信トラフィックを許可します。

ステップ 5 名前解決のためにクライアントからサーバーへの着信ドメインネームシステム（DNS）トラフィックを許可します。

ステップ 6 IP アドレスのためにクライアントからサーバーへの着信 DHCP トラフィックを許可します。

ステップ 7 Cisco ISE へのリダイレクションのための、クライアントからサーバーへの企業リソースに対するすべての着信トラフィックを（会社のポリシーに応じて）拒否します。

ステップ 8 （任意）残りのトラフィックを許可します。

例

次の例では、未登録のデバイスを BYOD フローにリダイレクトするための ACL を示しています。この例では、Cisco ISE IP アドレスは 10.35.50.165 で、企業のネットワークの IP アドレスは 192.168.0.0 および 172.16.0.0（リダイレクト用）で、MDM サーバーサブネットは 204.8.168.0 です。

図 *42* : 登録されていないデバイスをリダイレクトするための *ACL*

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

デバイスのワイプまたはロック

Cisco ISE では、紛失したデバイスのワイプや PIN ロックの有効化ができます。この操作は、[エンドポイント（Endpoints）] ウィンドウで設定できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックし、**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]** の順にクリックします。

ステップ 2 ワイプまたはロックするデバイスの横にあるチェックボックスをオンにします。

ステップ 3 [MDM アクセス（MDM Access）] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [完全ワイプ（Full Wipe）]：このオプションを使用すると、MDM ベンダーに応じて、企業アプリケーションが削除されるか、またはデバイスが工場出荷時の設定にリセットされます。
- [企業ワイプ（Corporate Wipe）]：このオプションを使用すると、MDM サーバーポリシーで設定したアプリケーションが削除されます。
- [PIN ロック（PIN Lock）]：このオプションを使用すると、デバイスがロックされます。

ステップ 4 [はい（Yes）] をクリックして、デバイスをワイプまたはロックします。

モバイルデバイス管理レポートの表示

Cisco ISE では、MDM サーバー定義のすべての追加、更新、および削除を記録します。これらのイベントは、選択された期間での任意のシステム管理者によるすべての設定変更を表示する [変更設定監査（Change Configuration Audit）] レポートに表示できます。

Cisco ISE の GUIで、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[監査（Audit）]** > **[変更設定監査（Change Configuration Audit）]** を選択します。確認する MDM サーバーの [オブジェクトタイプ（Object Type）] 列と [オブジェクト名（Object Name）] 列のエントリを確認し、対応する [イベント（Event）] の値をクリックして設定イベントの詳細を表示します。

モバイルデバイス管理ログの表示

[デバッグウィザード（Debug Wizard）] ウィンドウを使用して、モバイルデバイス管理のログメッセージを表示できます。Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）]** > **[トラブルシュート（Troubleshoot）]** > **[デバッグウィザード（Degug Wizard）]** > **[デバッグログの構成（Debug Log Configuration）]** を選択します。Cisco ISE ノードの横にあるオプションボタンをクリックし、[編集（Edit）] をクリックします。表示された新しいウィンドウで、コンポーネント名 **external-mdm** の横にあるオプションボタンをクリックし、[編集（Edit）] をクリックします。デフォルトのレベルは [情報（INFO）] です。対応する [ログレベル（Log Level）] ドロップダウンリストから [デバッグ（DEBUG）] または [トレース（TRACE）] を選択し、[保存（Save）] をクリックします。

サービスとしての Cisco Private 5G の設定

Cisco ISE リリース 3.2 以降、Cisco ISE は Cisco Private 5G およびセッション管理機能（SMF）ソフトウェアをサポートします。Cisco ISE は、RADIUS 認証のみおよびアカウンティングフローで実装される 5G 認証のポリシー設定を提供します。SMF との通信は、RADIUS プロトコルを使用して行われます。Cisco ISE と Cisco Private 5G 間の通信は、OpenAPI および ERS API を使用して行われます。

始める前に

Cisco ISE でサービスとして有効化する前に、ネットワークで Cisco Private 5G を展開しておく必要があります。

ステップ 1 Cisco Private 5G オンプレミス Cisco ISE プロキシで Cisco ISE を RADIUS サーバーとして設定します。

ステップ 2 ERS と Open API を有効にします。

ERS と Open API を有効にすると、API を使用するか、Cisco ISE GUI から、後続の手順を実行できます。

ステップ 3 Cisco ISE で 5G を有効にします。

a) Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authentication）]** > **[許可されるプロトコル（Allowed Protocols）]** を選択します。

b) 新しい**許可されるプロトコル**サービスを追加するか、既存のサービスを変更します。

（注） 新しいサービスを作成することは必須ではありません。5G エンドポイントにも既存の**デフォルト ネットワーク アクセス** サービスを使用できます。

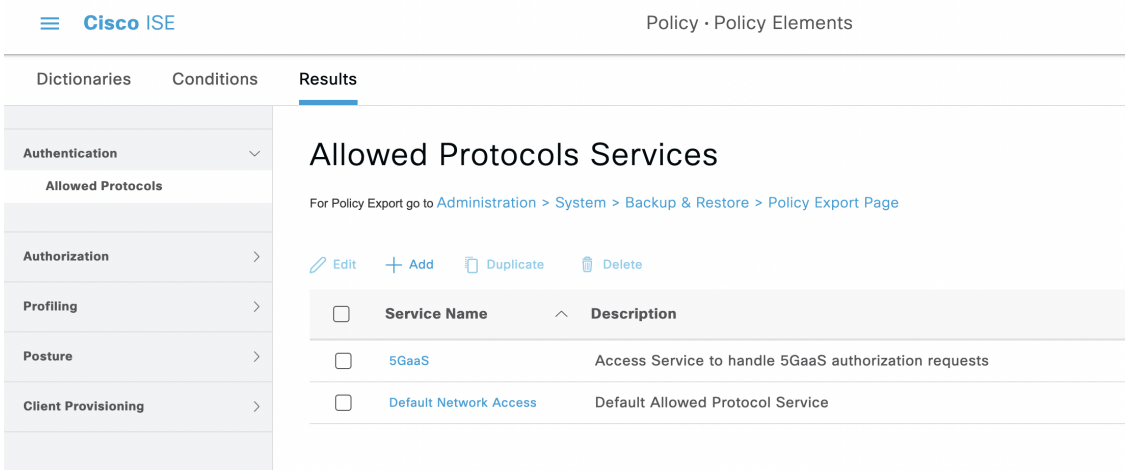
c) ネットワーク要件に従って設定を変更します。

d) [5G] チェックボックスをオンにします。

e) [保存（Save）] をクリックします。

たとえば、次の図に示す**許可されるプロトコルサービス**を作成して、5G トラフィックに一致させることができます。

図 *43 : 5G* の許可されるプロトコルサービス



ステップ 4 Cisco ISE で SMF をネットワークデバイスとして設定します。

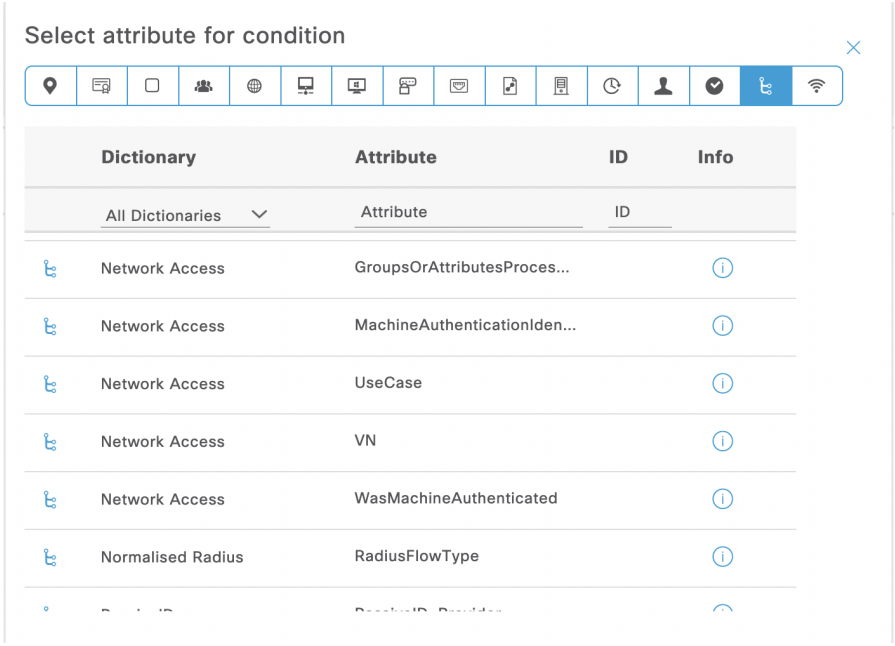
ステップ 5 新しい ID グループを作成するか、既存の ID グループを使用します。5G ユーザーは、Cisco ISE 内部データベースにサブスクライバとして保存されます。

ステップ 6 ユーザー ID グループを作成するか、Cisco ISE のデフォルトのユーザー ID グループから選択します。

ステップ 7 新しいポリシーセットを作成するか、既存のポリシーを使用します。

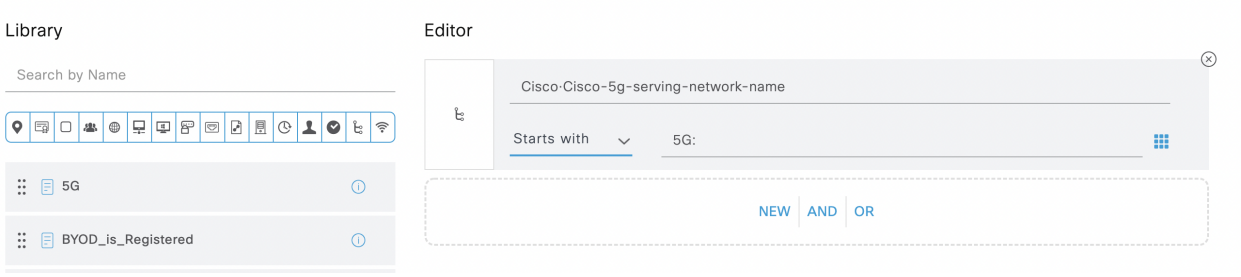
Conditions Studio の **Network Access.UseCase** 属性に、新しい値 **FiveG** が入力されます。**UseCase** 属性にも基づいてポリシーを作成できるようになりました。

図 *44* : 条件ライブラリの *UseCase* 属性の場所



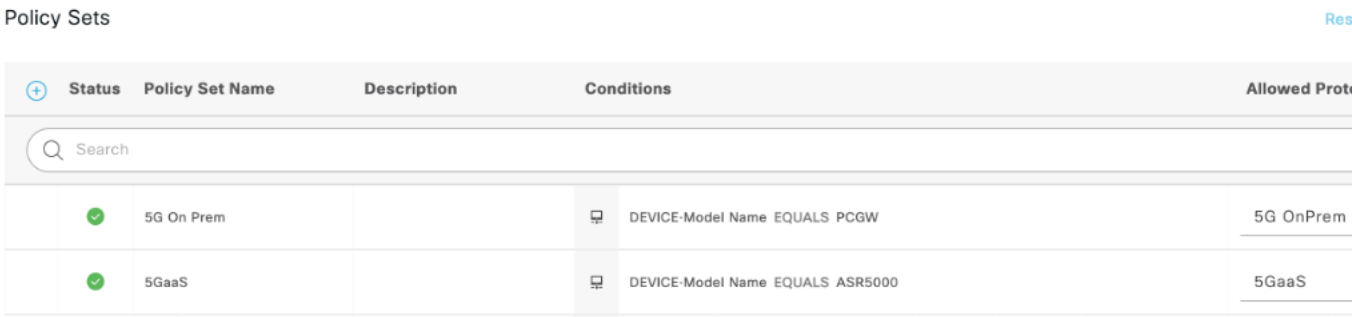
新しい組み込み条件である **5G** は、**Conditions Studio** の**ライブラリ**でも利用できます。この条件では、5G エンドポイントの照合に使用できる **Cisco·Cisco-5g-serving-network-name** 属性を使用します。

図 *45* : *5G* の条件



このポリシーには、以前に作成した、許可されるプロトコルサービスプロファイルをプッシュできます。

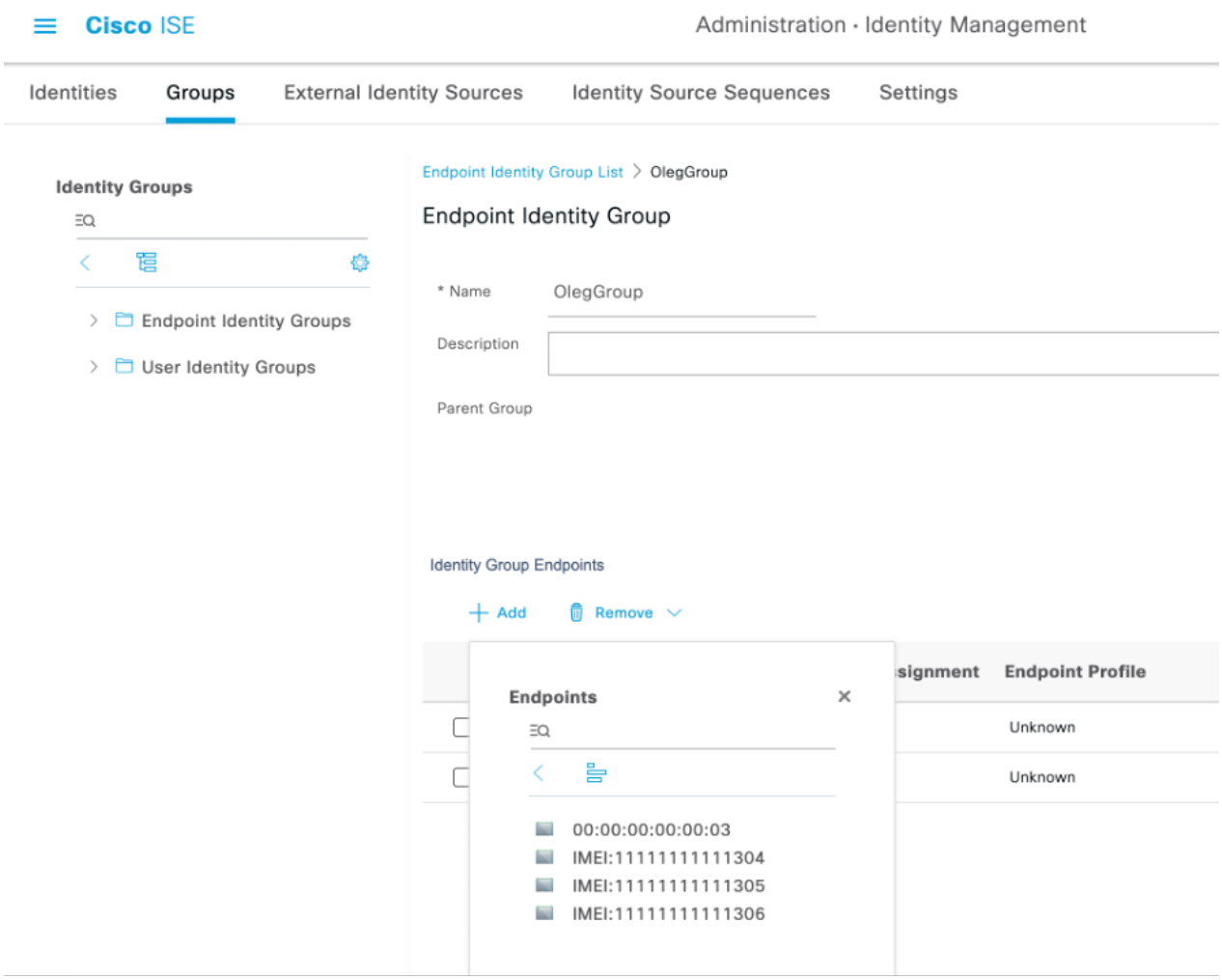
図 *46* : *5G* のポリシーセット



ステップ 8 Cisco Private 5G は、5GaaS API を使用して、サブスクライバ（セルラーユーザー）とユーザー機器（モバイルデバイス）を Cisco ISE に追加します。

たとえば、次の図に示すように、エンドポイント ID グループには追加されたサブスクライバが表示されます。

図 *47 : 5G* サブスクライバのエンドポイント *ID* グループ



ライブログと**ライブセッション**をチェックして、5G セッションログを表示し、必要に応じてトラブルシューティングを行うことができます。**ライブセッション**には、**ユースケース**（デフォルトでは無効）という新しい列があり、**5G** フィルタを使用して 5G エンドポイントをフィルタ処理できます。**エンドポイント**列でプレフィックス **IMEI:** を使用して、5G エンドポイントをフィルタ処理することもできます。

図 *48 : 5G* ライブログ

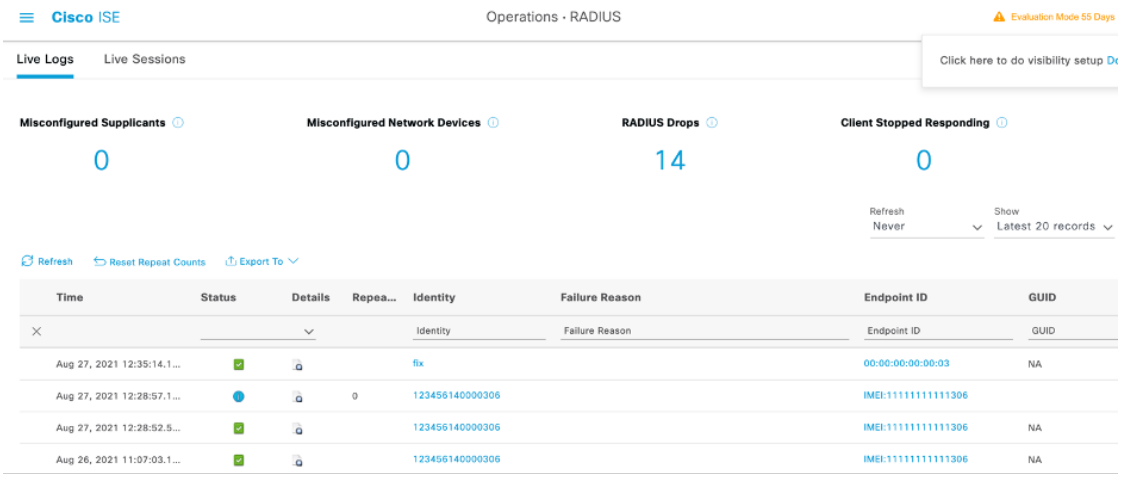
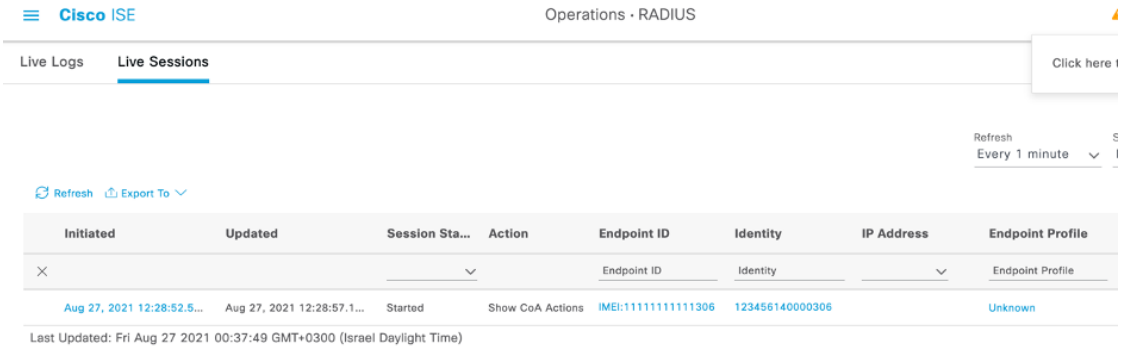


図 *49 : 5G* ライブセッション



サービスとしての Cisco Private 5G の設定

Cisco ISE リリース 3.2 以降、Cisco ISE は Cisco Private 5G およびセッション管理機能（SMF）ソフトウェアをサポートします。Cisco ISE は、RADIUS 認証のみおよびアカウンティングフローで実装される 5G 認証のポリシー設定を提供します。SMF との通信は、RADIUS プロトコルを使用して行われます。Cisco ISE と Cisco Private 5G 間の通信は、OpenAPI および ERS API を使用して行われます。

始める前に

Cisco ISE でサービスとして有効化する前に、ネットワークで Cisco Private 5G を展開しておく必要があります。

ステップ 1 Cisco Private 5G オンプレミス Cisco ISE プロキシで Cisco ISE を RADIUS サーバーとして設定します。

ステップ 2 ERS と Open API を有効にします。

ERS と Open API を有効にすると、API を使用するか、Cisco ISE GUI から、後続の手順を実行できます。

ステップ 3 Cisco ISE で 5G を有効にします。

a) Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authentication）]** > **[許可されるプロトコル（Allowed Protocols）]** を選択します。

b) 新しい**許可されるプロトコル**サービスを追加するか、既存のサービスを変更します。

（注） 新しいサービスを作成することは必須ではありません。5G エンドポイントにも既存の**デフォルト ネットワーク アクセス** サービスを使用できます。

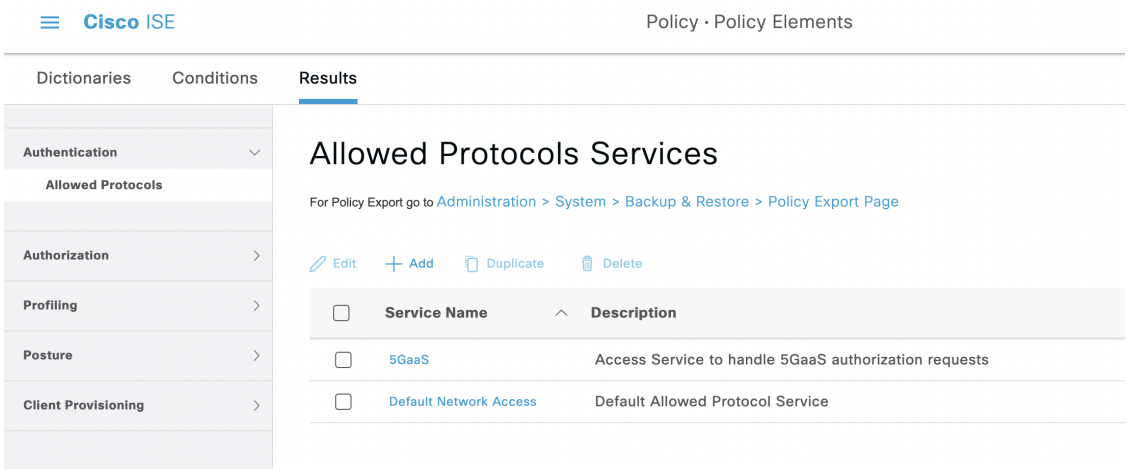
c) ネットワーク要件に従って設定を変更します。

d) [5G] チェックボックスをオンにします。

e) [保存（Save）] をクリックします。

たとえば、次の図に示す**許可されるプロトコルサービス**を作成して、5G トラフィックに一致させることができます。

図 *50 : 5G* の許可されるプロトコルサービス



ステップ 4 Cisco ISE で SMF をネットワークデバイスとして設定します。

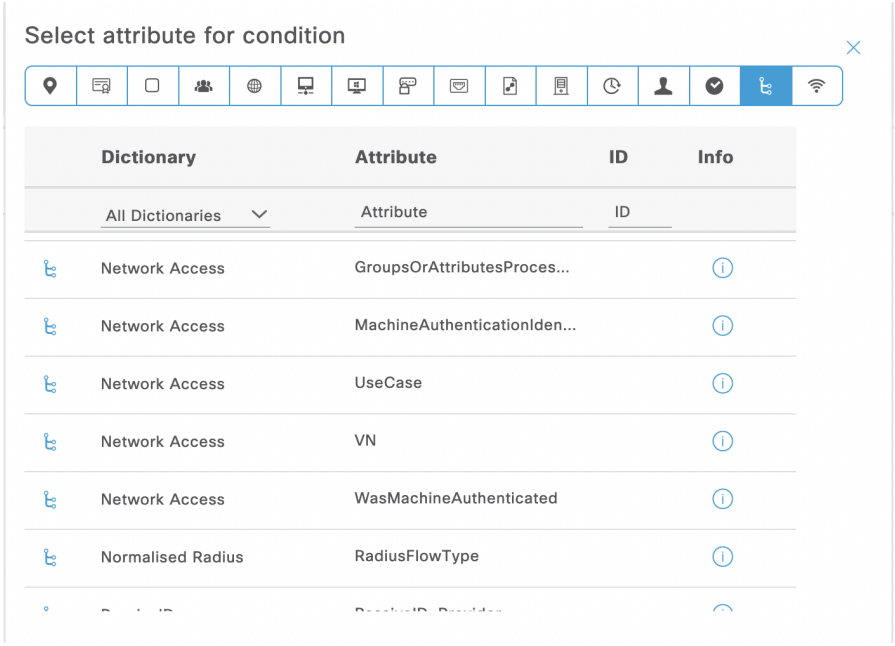
ステップ 5 新しい ID グループを作成するか、既存の ID グループを使用します。5G ユーザーは、Cisco ISE 内部データベースにサブスクライバとして保存されます。

ステップ 6 ユーザー ID グループを作成するか、Cisco ISE のデフォルトのユーザー ID グループから選択します。

ステップ 7 新しいポリシーセットを作成するか、既存のポリシーを使用します。

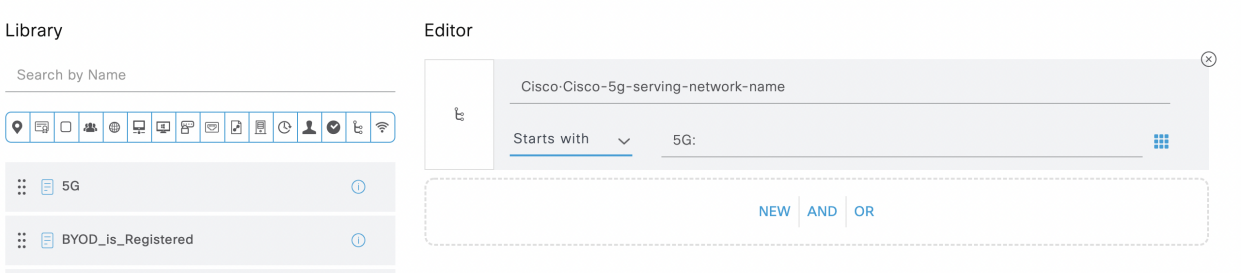
Conditions Studio の **Network Access.UseCase** 属性に、新しい値 **FiveG** が入力されます。**UseCase** 属性にも基づいてポリシーを作成できるようになりました。

図 *51* : 条件ライブラリの *UseCase* 属性の場所



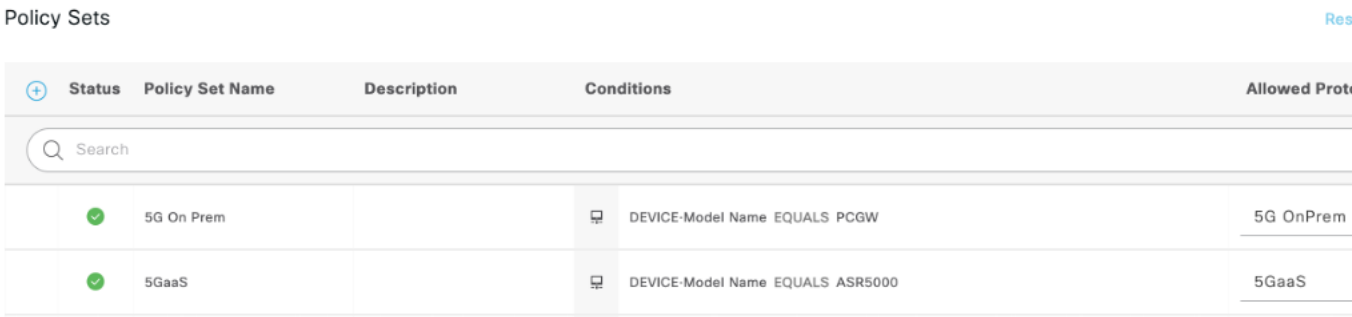
新しい組み込み条件である **5G** は、**Conditions Studio** の**ライブラリ**でも利用できます。この条件では、5G エンドポイントの照合に使用できる **Cisco·Cisco-5g-serving-network-name** 属性を使用します。

図 *52* : *5G* の条件



このポリシーには、以前に作成した、許可されるプロトコルサービスプロファイルをプッシュできます。

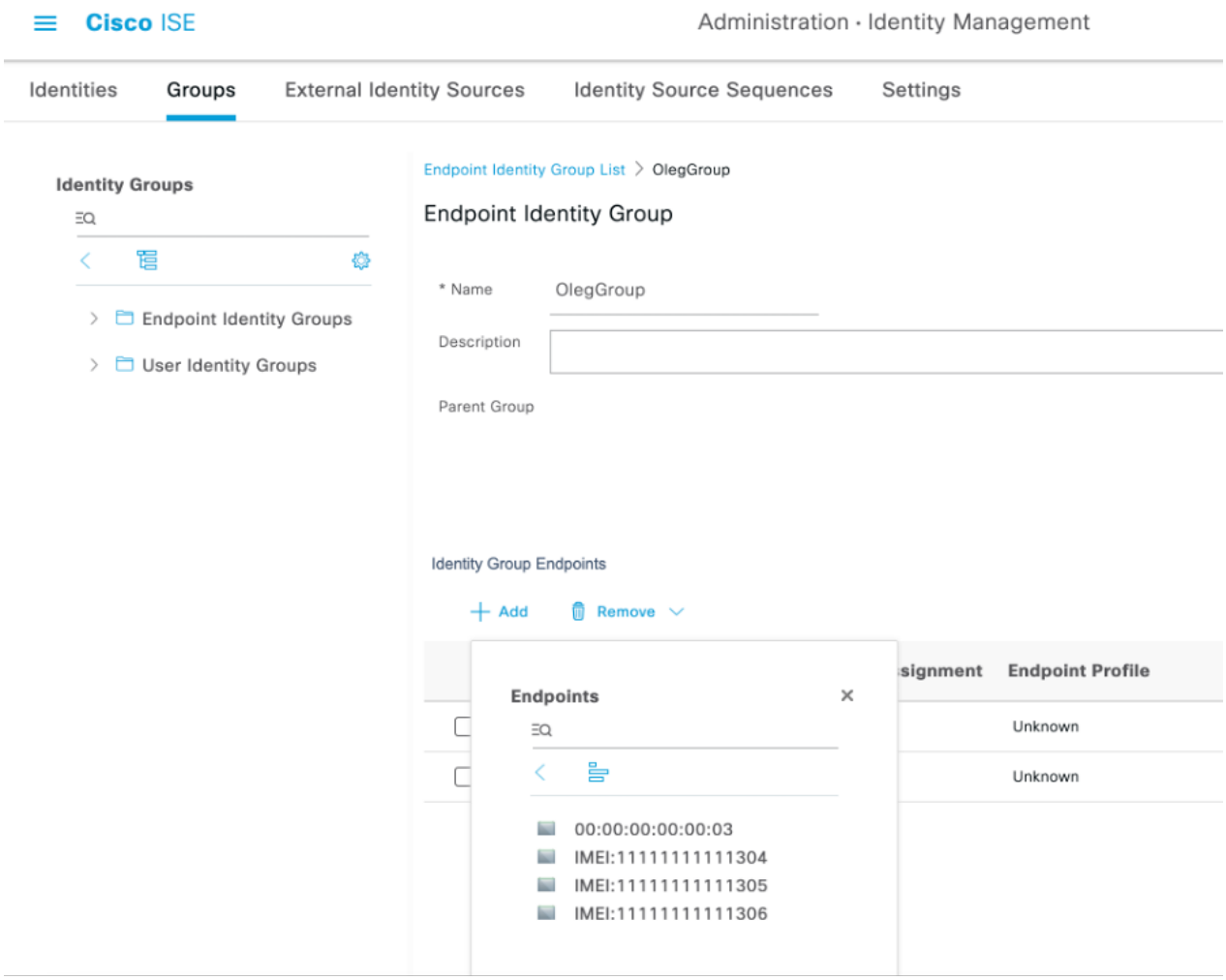
図 *53* : *5G* のポリシーセット



ステップ 8 Cisco Private 5G は、5GaaS API を使用して、サブスクライバ（セルラーユーザー）とユーザー機器（モバイルデバイス）を Cisco ISE に追加します。

たとえば、次の図に示すように、エンドポイント ID グループには追加されたサブスクライバが表示されます。

図 *54 : 5G* サブスクライバのエンドポイント *ID* グループ



ライブログと**ライブセッション**をチェックして、5G セッションログを表示し、必要に応じてトラブルシューティングを行うことができます。**ライブセッション**には、**ユースケース**（デフォルトでは無効）という新しい列があり、**5G** フィルタを使用して 5G エンドポイントをフィルタ処理できます。**エンドポイント**列でプレフィックス **IMEI:** を使用して、5G エンドポイントをフィルタ処理することもできます。

図 *55 : 5G* ライブログ

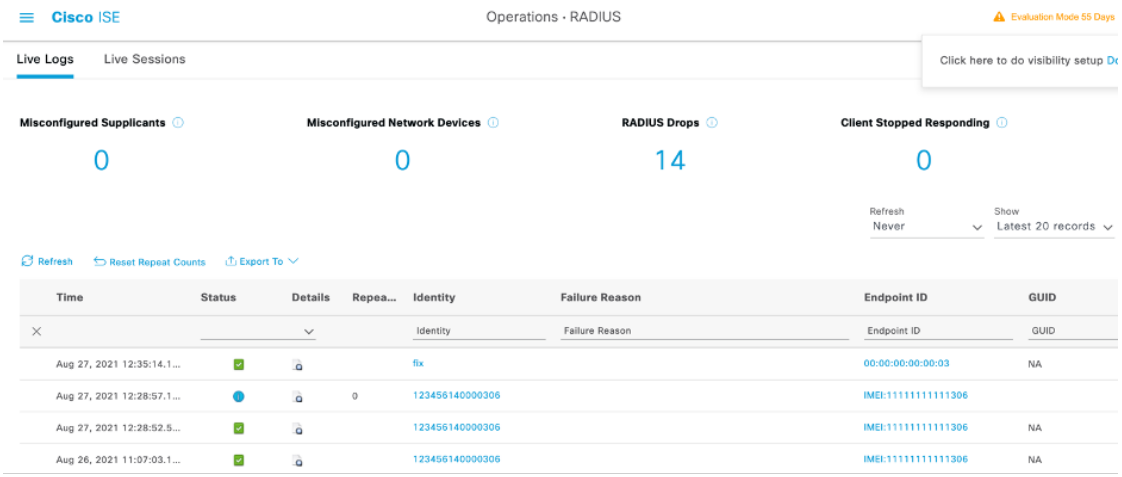
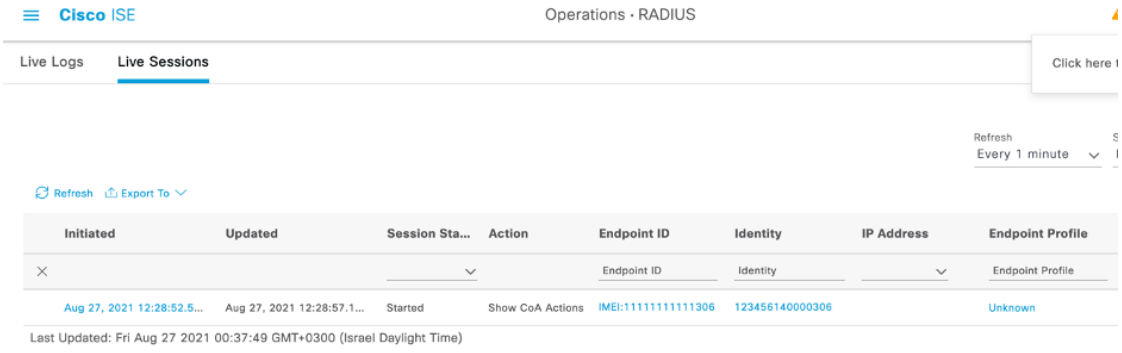
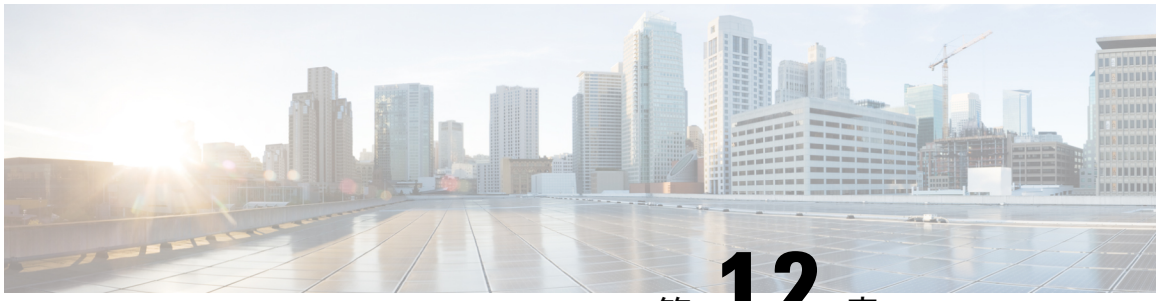


図 *56 : 5G* ライブセッション





第 12 章

セグメンテーション

- ポリシー セット （1460 ページ）
- ポリシー セットの構成時の設定 （1461 ページ）
- 認証ポリシー （1463 ページ）
- 許可ポリシー （1474 ページ）
- ポリシー条件 （1490 ページ）
- 特別なネットワーク アクセス条件 （1513 ページ）
- ポリシー セット プロトコルの設定 （1518 ページ）
- シスコ以外のデバイスからの MAB の有効化 （1585 ページ）
- シスコ デバイスからの MAB の有効化 （1586 ページ）
- TrustSec アーキテクチャ （1588 ページ）
- Cisco Catalyst Center との統合 （1592 ページ）
- TrustSec ダッシュボード （1594 ページ）
- TrustSec のグローバル設定 （1598 ページ）
- TrustSec マトリックスの設定 （1602 ページ）
- TrustSec デバイスの設定 （1605 ページ）
- Cisco TrustSec AAA サーバーの設定 （1608 ページ）
- TrustSec HTTPS サーバー （1609 ページ）
- セキュリティ グループの設定 （1612 ページ）
- 出力ポリシー （1620 ページ）
- SGT の割り当て （1643 ページ）
- TrustSec の設定およびポリシー プッシュ （1646 ページ）
- セキュリティ グループ タグの交換プロトコル （1656 ページ）
- SGT ドメインフィルタの追加 （1659 ページ）
- SXP の設定 （1660 ページ）
- Cisco ISE でのシスコ アプリケーション セントリック インフラストラクチャ接続 （1661 ページ）
- Cisco ACI 接続の追加 （1663 ページ）
- インバウンドおよびアウトバウンド SGT ドメインルールの追加 （1666 ページ）
- SGT ドメインの作成 （1667 ページ）

- SGTバインディング （1668 ページ）
- Cisco ACI 統合の互換性マトリックス （1668 ページ）
- ACI コネクタのデバッグログ （1669 ページ）
- Cisco ACI 統合で発生するアラーム （1669 ページ）
- レガシー ACI 統合から新しい ACI 接続ワークフローへの移行 （1670 ページ）
- 仮想ネットワーク認識による Cisco ACI と Cisco SD-Access の統合 （1670 ページ）
- ユーザー レポート別上位 N 個の RBACL ドロップの実行 （1681 ページ）
- Cisco Meraki ダッシュボードと Cisco ISE の接続 （1682 ページ）

ポリシー セット

Cisco ISE はポリシーベースのネットワークアクセス制御ソリューションで、ネットワーク アクセスポリシーセットを提供し、ワイヤレス、有線、ゲスト、およびクライアントプロビジョニングなど、さまざまなネットワーク アクセスの使用例を管理できます。ポリシー セット（ネットワーク アクセスとデバイス管理の両方のセット）を使用すると、認証および許可ポリシーを論理的に同じセットにグループ化することができます。ロケーション、アクセスタイプ、類似パラメータに基づくポリシーセットなどの領域に基づいて、複数のポリシーセットを作成できます。Cisco ISE をインストールすると、デフォルトのポリシーセットであるポリシーセットが常に 1 つ定義され、デフォルトのポリシーセットには、事前定義されたデフォルトの認証、許可、および例外のポリシー規則が含まれています。

ポリシーセットを作成するときは、ネットワーク アクセス サービスはポリシーセット レベルで、ID ソースは認証ポリシー レベルで、ネットワーク許可は許可ポリシー レベルで選択するように、（条件および結果で設定された）これらのルールを設定できます。さまざまなベンダーに対し、Cisco ISE 対応ディクショナリからの属性のいずれかを使用して、1 つまたは複数の条件を定義できます。Cisco ISE では、再利用可能な個別のポリシー要素として条件を作成できます。

ネットワーク デバイスと通信するためにポリシー セットごとに使用されるネットワーク アクセス サービスは、そのポリシー セットの最上位レベルで定義されます。ネットワーク アクセス サービスには次のものがあります。

- 許可されたプロトコル：初期要求とプロトコルネゴシエーションを処理するように設定されたプロトコル
- プロキシサービス：処理のために外部 RADIUS サーバーに要求を送信します

（注） **[ワークセンター（Work Centers）]>[デバイス管理（Device Administration）]**から、ポリシーセットに関連する TACACS サーバー順序を選択することもできます。TACACS サーバー順序を使用して、一連の TACACS プロキシ サーバーを処理用に設定します。

[ポリシーセット（Policy Set）]テーブルから確認できるポリシーセットの最上位レベルのルールが、セット全体に適用され、残りのポリシーと例外のルールの前に一致している場合、ポリ

シーセットは階層的に構成されています。その後、セットのルールが次の順序で適用されます。

1. 認証ポリシー ルール
2. ローカル ポリシー例外
3. グローバル ポリシー例外
4. 許可ポリシー ルール

（注） ポリシーセットの機能は、ネットワークアクセスとデバイス管理ポリシーの場合と同じです。この章で説明するすべてのプロセスは、[ネットワークアクセス（Network Access）]および[デバイス管理（Device Administration）] ワークセンターの両方で作業する場合に適用できます。この章では、[ネットワーク アクセス（Network Access）] ワーク センターのポリシーセットについて具体的に説明します。**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）]**Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [ネットワークアクセス（Policy Sets）] > [ポリシーセット（Policy Sets）]**。

ISE コミュニティ リソース

WLC からの RADIUS 結果の使用については、「WLC Called-Station-ID（RADIUS 認証とアカウンティングの設定）（WLC Called-Station-ID (Radius Authentication and Accounting Config)）」を参照してください。

ポリシー セットの構成時の設定

次の表では、[ポリシーセット（Policy Sets）] ウィンドウのフィールドについて説明します。このフィールドから、認証、例外、および許可ポリシーを含むポリシーセットを設定できます。ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）]** を選択します。ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）]** を選択します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。デバイス管理ポリシーの場合は、**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]** Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

表 *135 :* ポリシー セットの構成時の設定

フィールド名	使用上のガイドライン
ステータス（**Status**）	このポリシーのステータスを選択します。次のいずれかを設定できます。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニターのみ（Monitor Only）]：このポリシー条件は評価されません。
ポリシーセット名（**Policy Set Name**）	このポリシー セットの一意の名前を入力します。
条件（**Conditions**）	新しいポリシー行から、プラス（+）アイコンをクリックするか、既存のポリシー行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
説明（**Description**）	ポリシーの一意の説明を入力します。
許可されているプロトコルまたはサーバー順序（**Allowed Protocols or Server Sequence**）	すでに作成した許可されているプロトコルを選択するか、または（+）記号をクリックして [新しい許可されているプロトコルを作成（Create a New Allowed Protocol）] するか、[新しい RADIUS 順序を作成（Create a New Radius Sequence）] するか、または [TACACS 順序を作成（Create a TACACS Sequence）] します。
条件（**Conditions**）	新しい例外行から、プラス（+）アイコンをクリックするか、既存の例外行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
ヒット数（**Hits**）	ヒット数は、条件が一致した回数を示す診断ツールです。このアイコンが最後に更新された時刻を表示し、ゼロにリセットし、更新の頻度を表示するには、アイコンにカーソルを合わせます。

フィールド名	使用上のガイドライン
アクション（**Actions**）	さまざまなアクションを表示して選択するには、[アクション（Actions）] 列の歯車アイコン をクリックします。 • [上に新しい行を挿入（Insert new row above）] : [アクション（Actions）] メニューを開いたポリシーの上に新しいポリシーを挿入します。 • [下に新しい行を挿入（Insert new row below）] : [アクション（Actions）] メニューを開いたポリシーの下に新しいポリシーを挿入します。 • [上に複製（Duplicate above）] : 元のセットの上に、[アクション（Actions）] メニューを開いたポリシーの上に複製ポリシーを挿入します。 • [下に複製（Duplicate below）] : 元のセットの下に、[アクション（Actions）] メニューを開いたポリシーの下に複製ポリシーを挿入します。 • [削除（Delete）] : ポリシーセットを削除します。
表示（**View**）	矢印アイコンをクリックすると、特定のポリシーセットの [設定（Set）] ビューが開き、認証、例外、および許可のサブポリシーが表示されます。

認証ポリシー

各ポリシーセットには、そのセットの認証ポリシーを表す複数の認証ルールを含めることができます。認証ポリシーの優先順位は、（[認証ポリシー（Authentication Policy）] 領域の [設定（Set）] ビュー ページから）ポリシー セット自体に表示されるポリシーに対する順序に基づいて決定されます。

Cisco ISE は、ポリシー セット レベルで設定された設定に基づいて、ネットワーク アクセス サービス（許可されたプロトコルまたはサーバー順序のいずれか）を動的に選択し、その後、認証ポリシー レベルおよび許可ポリシー レベルから ID ソースおよび結果をチェックします。複数の条件を、Cisco ISE ディクショナリ内の任意の属性を使用して定義できます。Cisco ISE

では、個々のポリシー要素として条件を作成し、ライブラリに保存してから、他のルールベースのポリシーに再利用することができます。

認証ポリシーの結果である ID 特定方法は、次のいずれかになります。

- アクセスを拒否：ユーザーへのアクセスは拒否され、認証は実行されません。
- ID データベース：次のいずれかの単一の ID データベース。
  - 内部ユーザー
  - ゲスト ユーザー
  - 内部エンドポイント
  - Active Directory
  - Lightweight Directory Access Protocol（LDAP）データベース
  - RADIUS トークン サーバー（RSA または SafeWord サーバー）
  - 証明書認証プロファイル
- ID ソース順序：認証に使用する ID データベースの順序。

最初の Cisco ISE インストール時に実装されるデフォルト ポリシー セットには、デフォルトの ISE 認証ルールおよび許可ルールが含まれています。デフォルト ポリシー セットには、認証と許可のための追加の柔軟な組み込みルール（デフォルトではない）も含まれています。これらのポリシーにルールを追加して、組み込みルールを削除および変更できますが、デフォルト ルールを削除することはできず、デフォルト ポリシー セットを削除することはできません。

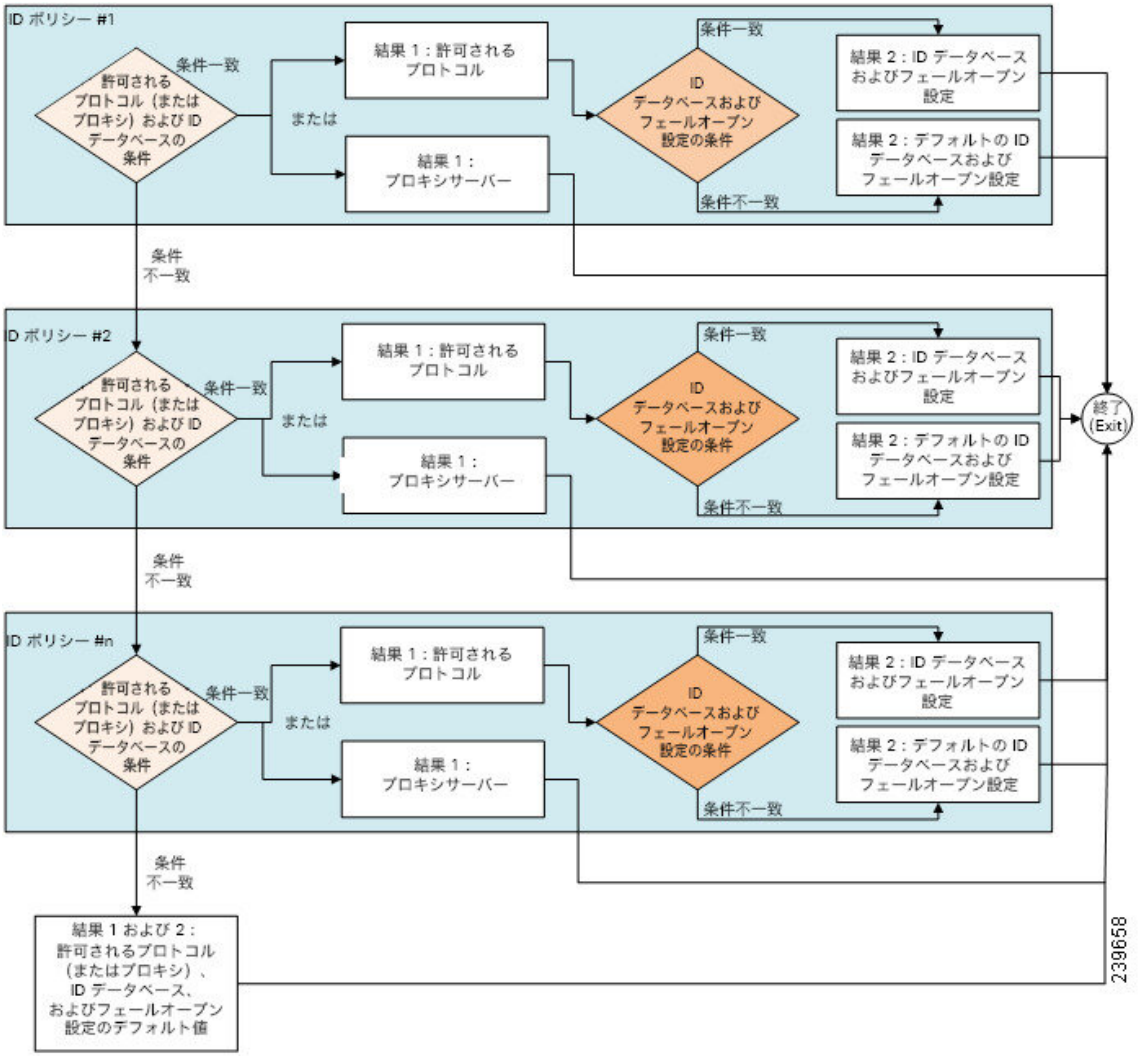
認証ポリシーのフロー

認証ポリシーでは、条件と結果で構成される複数のルールを定義できます。ISE は、指定された条件を評価し、評価結果に基づいて対応する結果を割り当てます。ID データベースは、基準に一致する最初のルールに基づいて選択されます。

異なるデータベースで構成される ID ソース順序を定義することもできます。Cisco ISE がデータベースを検索する順序を定義できます。Cisco ISE は、認証が成功するまで指定された順序でこれらのデータベースにアクセスします。1 つの外部データベースに同一ユーザーの複数のインスタンスが存在する場合、認証は失敗します。1 つの ID ソース内で、ユーザー レコードは重複できません。

ID ソース順序には、3 つのデータベース、または多くとも 4 つのデータベースを使用することを推奨します。

図 *57 :* 認証ポリシーのフロー



認証失敗：ポリシー結果オプション

識別方法としてアクセス拒否を選択した場合、要求への応答として拒否メッセージが送信されます。ID データベースまたは ID ソース順序を選択して、認証が成功した場合、処理は同じポリシーセットに対して設定された許可ポリシーに対して続行されます。一部の認証は失敗し、その場合次のように分類されます。

- 認証の失敗：クレデンシャルが正しくない、無効なユーザーであることなどが原因で認証が失敗したことを示す明確な応答を受信します。アクションのデフォルト コースは拒否です。
- ユーザーが見つからない：どの ID データベースでもこのユーザーが見つかりませんでした。アクションのデフォルト コースは拒否です。

- 処理の失敗：ID データベース（複数の場合もある）にアクセスできません。アクションのデフォルト コースはドロップです。

Cisco ISE では、認証失敗に対して次のアクションのコースのいずれかを設定することができます。

- [拒否（Reject）]：拒否応答が送信されます。
- [ドロップ（Drop）]：応答は送信されません。
- [続行（Continue）]：許可ポリシーに従って Cisco ISE を継続します。

[続行（Continue）] オプションを選択した場合でも、使用されているプロトコルの制限により Cisco ISE が要求の処理を実行できない場合があります。PEAP、LEAP、EAP-FAST、EAP-TLS、または RADIUS MSCHAP を使用した認証では、認証に失敗したり、ユーザーが見つからなかったときには、要求の処理を続行することはできません。

認証に失敗した場合、PAP/ASCII または MAC 認証バイパス（MAB またはホスト ルックアップ）の許可ポリシーの処理を続行できます。その他のすべての認証プロトコルの場合、認証に失敗すると、次のいずれかの状態となります。

- 認証の失敗：拒否応答が送信されます。
- ユーザーまたはホストが見つからない：拒否応答が送信されます。
- 処理に問題が発生：応答は送信されず、要求はドロップされます。

認証失敗時の一連のアクションとして [続行（Continue）] を使用するユースケース

[続行（Continue）] オプションを選択すると、次の場合に Cisco ISE は認証をスキップして認証ポリシーの評価に進みます。

- ルックアップ（MAB）：「ユーザーが見つかりませんでした（User not found）」という結果が表示された場合でも、Cisco ISE は認証ポリシーの評価を続行します。
- PAP または ASCII
- CHAP
- EAP-MD5
- EAP-TLS：AD または LDAP でユーザーまたは証明書の検証が失敗した場合でも、Cisco ISE は認証ポリシーの評価を続行します。
- PEAP（EAP-TLS）：AD または LDAP でユーザーまたは証明書の検証が失敗した場合でも、Cisco ISE は認証ポリシーの評価を続行します。
- TEAP（EAP-TLS）：AD または LDAP でユーザーまたは証明書の検証が失敗した場合でも、Cisco ISE は認証ポリシーの評価を続行します。
- EAP-FAST（EAP-TLS）：AD または LDAP でユーザーまたは証明書の検証が失敗した場合でも、Cisco ISE は認証ポリシーの評価を続行します。

- EAP チェーン TEAP（EAP-TLS、EAP-MS-CHAPv2）：AD または LDAP でユーザーまたは証明書の検証が失敗した場合でも、Cisco ISE は認証ポリシーの評価を続行します。[続行（Continue）] オプションは、EAP-TLS 内部方式にのみ適用されることに注意してください。

次の認証プロトコルで認証が失敗した場合、選択したすべての [詳細設定（Advanced）] オプションが無視され、Cisco ISE は **Access-Reject** 応答を送信します。

- MS-CHAPv1
- MS-CHAPv2
- LEAP
- PEAP（EAP-MS-CHAPv2）
- TEAP（EAP-MS-CHAPv2）
- EAP-FAST（EAP-MS-CHAPv2）
- EAP-TTLS（PAP\ASCII）
- EAP-TTLS（MS-CHAPv1）
- EAP-TTLS（MS-CHAPv2）
- EAP-TTLS（EAP-MD5）
- EAP-TTLS（CHAP）
- EAP-TTLS（EAP-MS-CHAPv2）
- EAP-FAST（EAP-GTC）
- PEAP（EAP-GTC）

認証ポリシーの設定

必要に応じて、複数の認証ルールを設定および管理することによって、ポリシーセットごとに認証ポリシーを定義します。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 ネットワーク アクセス ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

ステップ 2 認証ポリシーを追加または更新するポリシーセットの行から、ポリシーセットの詳細のすべてにアクセスし、認証および許可ポリシーとポリシー例外を作成するために、[ポリシーセット（Policy Sets）]テーブルの [表示（View）] 列から をクリックします。

ステップ 3 ページの認証ポリシー部分の横にある矢印アイコンをクリックして、テーブル内のすべての認証ポリシールールを展開して表示します。

ステップ 4 いずれかの行の[アクション（Actions）]列から、歯車アイコンをクリックします。ドロップダウンメニューから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して、新しい認証ポリシールールを挿入します。
[認証ポリシー（Authentication Policy）] テーブルに新しい行が表示されます。

ステップ 5 [ステータス（Status）] 列から、現在の [ステータス（Status）] アイコンをクリックし、ドロップダウンリストから必要に応じてポリシーセットのステータスを更新します。[ステータス（Status）] の詳細については、認証ポリシーの構成設定 （1468 ページ）を参照してください。

ステップ 6 テーブル内のルールの場合は、[ルール名（Rule Name）] または [説明（Description）] のセルをクリックして、フリーテキストを変更します。

ステップ 7 条件を追加または変更するには、[条件（Conditions）] 列のセルにカーソルを合わせ、 をクリックします。[条件スタジオ（Conditions Studio）] が開きます。詳細については、特別なネットワーク アクセス条件（1513 ページ）を参照してください。

選択するすべての属性に「Equals」、「Not Equals」、「In」、「Not In」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現（REGEX）をサポートし、使用します。

（注） 単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数値属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。リストの場合、「in」演算子は、特定の値がリスト内に存在するかどうかをチェックします。単一文字列の場合、「in」演算子は、文字列が「equals」演算子などと同じかどうかをチェックします。

ステップ 8 チェックして一致させる順序に従って、テーブル内のポリシーを編成します。ルールの順序を変更するには、行をドラッグして正しい位置にドロップします。

ステップ 9 [保存（Save）] をクリックすると、変更内容が保存されて実装されます。

次のタスク

1. 許可ポリシーの設定

認証ポリシーの構成設定

次の表では、[ポリシーセット（Policy Sets）] ウィンドウの [認証ポリシー（Authentication Policy）]セクションのフィールドについて説明します。これらのフィールドから、認証サブポリシーをポリシーセットの一部として構成できます。Cisco ISE GUI で [メニュー（Menu）] ア

イコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]**（ネットワーク アクセス ポリシーの場合）。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]**（デバイス管理ポリシーの場合）。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシーセット（Policy Sets）]** > **[表示（View）]** > **[認証ポリシー（Authentication Policy）]**。

表 *136 :* 認証ポリシーの構成設定

フィールド名	使用上のガイドライン
ステータス（Status）	このポリシーのステータスを選択します。次のいずれかを設定できます。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニターのみ（Monitor Only）]：このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証（Live Log authentication）] ページでこのポリシー条件の結果を照会できます。ここでは、モニターされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加する場合に、条件がもたらす結果が正しいかどうかを判断できないことがあります。この場合、モニター モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。
ルール名（Rule Name）	この認証ポリシーの名前を入力します。
条件（Conditions）	新しいポリシー行から、プラス（+）アイコンをクリックするか、または既存のポリシー行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。

フィールド名	使用上のガイドライン
使用（**Use**）	認証に使用する ID ソースを選択します。ID ソース順序が設定済みである場合、これを選択することも可能です。 デフォルトの ID ソースを編集して、このルールで定義されたいずれの ID ソースも要求に一致しない場合に Cisco ISE が使用する ID ソースを指定できます。
オプション（**Options**）	認証失敗、ユーザーが見つからない、プロセス障害、の各イベントに対する今後のアクションのコースを定義します。次のいずれかのオプションを選択できます。 • [拒否（Reject）]：拒否応答が送信されます。 • [ドロップ（Drop）]：応答は送信されません。 • [続行（Continue）]：Cisco ISE は認証ポリシーの処理を続行します。
ヒット数（**Hits**）	ヒット数は、条件が一致した回数を示す診断ツールです。

フィールド名	使用上のガイドライン
アクション（**Actions**）	さまざまなアクションを表示して選択するには、[アクション（Actions）] 列の歯車アイコン をクリックします。 • [上に新しい行を挿入（Insert new row above）] : [アクション（Actions）] メニューを開いたポリシーの上に新しい認証ポリシーを挿入します。 • [下に新しい行を挿入（Insert new row below）] : [アクション（Actions）] メニューを開いたポリシーの下に新しい認証ポリシーを挿入します。 • [上に複製（Duplicate above）] : 元のセットの上に、[アクション（Actions）] メニューを開いたポリシーの上に複製認証ポリシーを挿入します。 • [下に複製（Duplicate below）] : 元のセットの下に、[アクション（Actions）] メニューを開いたポリシーの下に複製認証ポリシーを挿入します。 • [削除（Delete）] : ポリシーセットを削除します。

パスワード ベースの認証

認証とは、ユーザー情報を検証してユーザー ID を確認することです。従来の認証方式では、名前とある決まったパスワードが使用されていました。これは、最も一般的かつ単純で、低コストの認証方式です。この方式の欠点は、ユーザー名やパスワードの情報が簡単に第三者に伝えられたり、推測または不正に取得されたりする可能性がある点です。単純な暗号化されていないユーザー名とパスワードを使用する方法は、強力な認証方式とは考えられていませんが、インターネットアクセスなど、許可または特権レベルが低い場合は十分に要件を満たす可能性があります。

暗号化されたパスワードと暗号化技術を使用したセキュアな認証

ネットワーク上でパスワードが不正に取得される危険性を低減するには、暗号化を使用する必要があります。RADIUS などのクライアント/サーバー アクセス コントロール プロトコルでは、パスワードを暗号化することにより、ネットワーク内でパスワードが不正に取得される事態を防止します。ただし、RADIUS は認証、許可、およびアカウンティング（AAA）クライアントと Cisco ISE との間でだけ動作します。認証プロセスでは、このポイントの前で、許可さ

れていないユーザーが次のような例で暗号化されていないパスワードを入手する可能性があります。

- 電話回線を介してダイヤルアップ接続を行うエンドユーザークライアントとの間の通信
- ネットワークアクセスサーバーで終了する ISDN 回線
- エンドユーザー クライアントとホスティング デバイスの間の Telnet セッションを介して行われる通信

さらに安全な方式では、チャレンジハンドシェイク認証プロトコル（CHAP）、ワンタイムパスワード（OTP）、および高度な EAP ベースのプロトコルの内部で使用されるような暗号化技術を使用します。Cisco ISE は、これらのさまざまな認証方式をサポートしています。

認証方式と許可特権

認証と許可には基本的な暗黙の関係があります。ユーザーに与えられる許可特権が多くなればなるほど、それに応じて認証を強化する必要があります。Cisco ISE では、さまざまな認証方式を提供することにより、この関係がサポートされています。

認証ダッシュレット

Cisco ISE のダッシュボードには、ネットワークとデバイスに対し行われたすべての認証の概要が表示されます。これには、[認証（Authentication）] ダッシュレットにある認証および許可の失敗についての概要情報が表示されます。

[RADIUS 認証（RADIUS Authentication）] ダッシュレットには、Cisco ISE が処理した認証に関する次の統計情報が表示されます。

- 認証成功、認証失敗、同一ユーザーによる同時ログインなど、Cisco ISE が処理した RADIUS 認証要求の総数。
- Cisco ISE が処理した、失敗した RADIUS 認証要求の総数。

また、TACACS+ 認証の概要を表示することもできます。TACACS+ 認証ダッシュレットには、デバイス認証の統計情報が表示されます。

デバイス管理認証の詳細については、TACACS ライブ ログ （783 ページ）を参照してください。RADIUS ライブ ログ設定の詳細については、RADIUS ライブ ログ （774 ページ）を参照してください。

> ISE コミュニティ リソース
>
> 認証と許可の失敗のトラブルシューティング方法については、「How To: Troubleshoot ISE Failed Authentications & Authorizations」を参照してください。

認証結果の表示

Cisco ISE にはリアルタイムで認証の概要を表示するさまざまな方法があります。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 ネットワーク認証（RADIUS）の場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）] > [RADIUS] > [ライブログ（Live Logs）]**。リアルタイム認証のサマリーを表示する場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）] > [TACACS] > [ライブログ（Live Logs）]**。

ステップ 2 認証の概要を表示するには、次のような方法があります。

- [ステータス（Status）] アイコンの上にマウス カーソルを移動すると、認証の結果と概要を表示できます。ステータスの詳細とともにポップアップが表示されます。
- 結果をフィルタリングするには、リストの最上部に表示される 1 つ以上の任意のテキスト ボックスに検索条件を入力して **Enter** を押します。
- 詳細なレポートを表示するには、[詳細（Details）] の虫眼鏡アイコンをクリックします。

（注） [認証概要（Authentication Summary）] レポートまたはダッシュボードが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。

認証レポートおよびトラブルシューティング ツール

認証の詳細の他に、Cisco ISE では、ネットワークの効率的な管理に使用できるさまざまなレポートおよびトラブルシューティング ツールが提供されます。

ネットワーク内の認証の傾向およびトラフィックを把握するために実行できるさまざまなレポートがあります。現在のデータに加えて履歴のレポートを生成できます。認証レポートのリストは次のとおりです。

- AAA の診断
- RADIUS アカウンティング
- RADIUS 認証
- 認証概要

（注） Cisco Catalyst 4000 シリーズ スイッチで IPv6 スヌーピングを有効にする必要があります、有効にしないと、IPv6 アドレスが認証セッションにマッピングされず、show の出力に表示されません。IPv6 スヌーピングを有効にするには、次のコマンドを使用します。

```
vlan config <vlan-number>
 ipv6 snooping
 end
ipv6 nd raguard policy router
 device-role router
interface <access-interface>
  ipv6 nd raguard
interface <uplink-interface>
  ipv6 nd raguard attach-policy router
  end
```

許可ポリシー

許可ポリシーは、Cisco ISE ネットワーク許可サービスのコンポーネントです。このサービスを使用して、ネットワーク リソースにアクセスする特定のユーザーおよびグループの許可ポリシーを定義し、許可プロファイルを設定することができます。

許可ポリシーには条件付きの要件を含めることができ、この要件では、1つ以上の許可プロファイルを返すことができる許可チェックを含む複合条件を使用して、1 つ以上の ID グループを組み合わせます。さらに、条件付きの要件は、特定の ID グループの使用とは別に存在することがあります。

許可プロファイルは、Cisco ISE で許可ポリシーを作成するときに使用されます。許可ポリシーは許可ルールで構成されます。許可ルールには、名前、属性、および権限の3つの要素があります。権限要素は、許可プロファイルにマッピングされます。

Cisco ISE の許可プロファイル

許可ポリシーは、特定のユーザーおよびグループの ID にルールを関連付け、対応するプロファイルを作成します。これらのルールが設定された属性と一致する場合は、常に、権限を付与する、対応する許可プロファイルがポリシーによって返され、ネットワーク アクセスがこれに応じて許可されます。

たとえば、許可プロファイルには、次のタイプに含まれるさまざまな権限を含めることができます。

- 標準プロファイル
- 例外プロファイル
- デバイスベースのプロファイル

プロファイルは、利用可能なベンダー ディクショナリのいずれかに保存されているリソースセットから選択された属性で構成され、特定の許可ポリシーの条件が一致したときに返されま

す。許可ポリシーには単一のネットワーク サービス ルールにマッピングする条件を含めることができるため、許可チェックのリストを含めることもできます。

許可確認は、返される許可プロファイルに準拠する必要があります。許可確認は、通常、ライブラリに追加できるユーザー定義名を含む1つ以上の条件から構成され、他の許可ポリシーで再利用できます。

許可プロファイルの権限

許可プロファイルの権限設定を開始する前に、以下を確認します。

- 認証ポリシーおよび認証プロファイル間の関係を理解している。
- [認証プロファイル（Authorization Profile）] ページをよく理解している。
- ポリシーおよびプロファイルを設定する場合に必要な基本ガイドラインを知っている。
- 認証プロファイルの権限の構成を理解している。

認証プロファイルを使用するには、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** を選択します。左側のメニューから、**[許可（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** を選択します。

ネットワークでさまざまなタイプの認証プロファイルのポリシー要素権限を表示、作成、変更、削除、複製、または検索するプロセスの開始点として [結果（Results）] ナビゲーション ウィンドウを使用します。[結果（Results）] ペインには、最初 [認証（Authentication）]、[許可（Authorization）]、[プロファイリング（Profiling）]、[ポスチャ（Posture）]、[クライアント プロビジョニング（Client Provisioning）]、および [TrustSec] のオプションが表示されています。

許可プロファイルでは、RADIUS 要求が受け入れられたときに返される属性を選択できます。Cisco ISE では、[共通タスク（Common Tasks）] 設定を設定して共通に使用される属性をサポートできるメカニズムが提供されます。Cisco ISE が基盤となる RADIUS 値に変換する [共通タスク属性（Common Tasks Attributes）] の値を入力する必要があります。

> ISE コミュニティ リソース
>
> 802.1x サプリカント（Cisco AnyConnect Mobile Security）とオーセンティケータ（スイッチ）間の Media Access Control Security（MACsec）暗号化を設定する方法の例については、「MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example」を参照してください。

ダウンロード可能 ACL

アクセス コントロール リスト（ACL）はアクセス コントロール エントリ（ACE）のリストで、ポリシー適用ポイント（スイッチなど）によってリソースに適用できます。各 ACE は、読み取り、書き込み、実行など、このオブジェクトに対してユーザーごとに許可された権限を識別します。たとえば、1人のユーザーに読み取りおよび書き込み権限を許可する ACE と、もう 1 人のユーザーに読み取り専用権限のみを許可する別の ACE を使用して、ネットワークの販売領域の 2 人のユーザーに対して ACL を設定できます。

Cisco ISE の場合、ダウンロード可能な ACL（DACL）は、さまざまなユーザーおよびユーザーグループがネットワークにアクセスする方法を制御するために許可ポリシーで設定および実装できます。DACL は、カスタムユーザー属性と AD 属性を使用して設定することもできます。

（注） アイデンティティ プロバイダー（IdP）の認証ポリシーで使用されている DACL が空の場合、認証は失敗します。

Cisco ISE でネットワーク認証ポリシーに DACL を実装するには、次の手順を実行します。

1. **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ダウンロード可能ACL（Downloadable ACLs）]** から新規または既存の DACL を設定します。詳細については、ダウンロード可能 ACL に対する権限の設定 （1476 ページ）を参照してください。
2. 設定済みの DACL を使用して、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）]** から新規または既存の許可プロファイルを設定します。
3. **[ポリシー（Policy）] > [ポリシーセット（Policy Sets]** から新規および既存のポリシー セットを作成および設定する場合は、設定済みの許可プロファイルを実装します。

（注） ユーザーごとの動的アクセス制御リストを使用して認証プロファイルを評価するときに、DACL が Cisco ISE 設定に存在しない場合、認証は失敗し、Cisco ISE はそのユーザーに Access-Reject 応答を送信します。この情報は、[ライブログの詳細（Live Log Details）] ページと [AAA診断（AAA Diagnostics）] レポートで確認できます。Cisco ISE リリース 3.4 以降では、Cisco ISE ダッシュボードの [アラーム（Alarms）] ダッシュレットにも認証失敗アラームが表示されます。

RADIUS プロトコルの場合、送信元と宛先の IP アドレス、トランスポート プロトコル、および他のパラメータをフィルタリングして、ACL は許可を付与します。スタティック ACL がスイッチに存在し、スイッチから直接設定され、ISE GUI から認証ポリシーに適用できます。

ダウンロード可能 ACL に対する権限の設定

デフォルト許可 DACL は、次のデフォルト プロファイルを含む ISE のインストール時に使用できます。

- DENY_ALL_IPV4_TRAFFIC
- PERMIT_ALL_IPV4_TRAFFIC
- DENY_ALL_IPV6_TRAFFIC
- PERMIT_ALL_IPV6_TRAFFIC

DACL を使用する場合、これらのデフォルトは設定できませんが、他の同じような DACL を作成するために複製することはできます。

必要な DACL を設定した後に、ネットワーク上で関連する認証ポリシーにその DACL を適用できます。認証ポリシーで使用されている DACL は、編集または削除できません。その DACL を編集または削除するには、まずその DACL を認証ポリシーから削除する必要があります。DACL を更新した後に、必要に応じて、同じ DACL を認証ポリシーに再適用できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[ダウンロード可能ACL（Downloadable ACLs）]** を選択します。

ステップ 2 [ダウンロード可能ACL（Downloadable ACLs）] テーブル上部の [追加（Add）] をクリックするか、既存の DACL を選択し、テーブル上部の [複製（Duplicate）] をクリックします。

ステップ 3 次のルールに留意しながら、DACL に適切な値を入力または編集します。

- [名前（Name）] フィールドのサポート対象の文字：英数字、ハイフン（-）、ドット（.）、アンダースコア（_）
- 次の DACL タイプを選択すると、IP 形式は選択した IP バージョンに基づいて処理されます。
  - IPv4 の法的な ACE のみを検証する [IPv4]。有効な IPv4 形式を入力する必要があります。
  - IPv6 の法的な ACE のみを検証する [IPv6]。有効な IPv6 形式を入力する必要があります。
  - 以前のリリースからリリース 2.6 にアップグレードされた DACL では、[IP バージョン（IP Version）] フィールドに DACL タイプとして [非依存（Agnostic）] オプションが表示されます。必要に応じて形式を入力します。シスコでサポートされていないデバイスの DACL を作成するには、[非依存（Agnostic）] を使用します。[非依存（Agnostic）] を選択すると、形式は検証されないため、DACL 構文をチェックすることはできません。
- キーワード **Any** が DACL のすべての ACE のソースである必要があります。DACL がプッシュされると、ソースの **Any** がスイッチに接続されているクライアントの IP アドレスで置き換えられます。

（注） [IP バージョン（IP Version）] フィールドは、DACL がいずれかの認証プロファイルにマッピングされている場合は編集できません。この場合、[認証プロファイル（Authorization Profiles）] から DACL 参照を削除し、IP バージョンを編集して、[認証プロファイル（Authorization Profiles）] の DACL を再マッピングします。

ステップ 4 必要に応じて、ACE のすべてのリストの作成が完了したら、[DACL構文のチェック（Check DACL Syntax）] をクリックしてリストを検証します。検証エラーが発生した場合、自動的に表示されるウィンドウで無効な構文を識別する特定の指示が返されます。

ステップ 5 [送信（Submit）] をクリックします。

Active Directory ユーザー許可のためのマシン アクセス制限

Cisco ISE には、Microsoft Active Directory 認証ユーザーの許可を制御する追加の方法を提供する、マシンアクセス制限（MAR）コンポーネントが含まれています。この形式の許可は、Cisco ISE ネットワークにアクセスするために使用されるコンピュータのマシン認証に基づきます。

成功したマシン認証ごとに、Cisco ISE は、RADIUS Calling-Station-ID 属性（属性 31）で受信した値を、成功したマシン認証の証拠としてキャッシュします。

Cisco ISE は、[Active Directory の設定（Active Directory Settings）] ページの [存続可能時間（Time to Live）] パラメータで設定された時間が失効になるまで各 Calling-Station-ID 属性値をキャッシュに保持します。失効したパラメータは、Cisco ISE によってキャッシュから削除されます。

ユーザーをエンドユーザー クライアントから認証する場合、Cisco ISE は、成功したマシン認証の Calling-Station-ID 値のキャッシュを検索して、ユーザー認証要求で受信した Calling-Station-ID 値を見つけようとします。Cisco ISE が一致するユーザー認証 Calling-Station-ID 値をキャッシュで見つけた場合、これは、次の方法で認証を要求するユーザーに Cisco ISE が権限を割り当てる方法に影響します。

- Calling-Station-ID 値が Cisco ISE キャッシュで見つかった値と一致する場合、成功した許可の許可プロファイルを割り当てます。
- Calling-Station-ID 値が Cisco ISE キャッシュの値と一致しないことがわかった場合、マシン認証のない成功したユーザー認証の許可プロファイルを割り当てます。

許可ポリシーおよびプロファイルの設定のガイドライン

許可ポリシーおよびプロファイルを管理または運用する場合、次のガイドラインに従ってください。

- 作成するルール名は、サポートされている次の文字のみを使用する必要があります。
  - 記号：プラス（+）、ハイフン（-）、アンダースコア（_）、ピリオド（.）、およびスペース（ ）。
  - アルファベット文字：A ～ Z、a ～ z。
  - 数字：0 ～ 9。
- ID グループのデフォルトは「Any」です（このグローバル デフォルトを使用してすべてのユーザーに適用できます）。
- 条件では、1 つ以上のポリシー値を設定することが許可されています。ただし、条件はオプションであり、許可ポリシーを作成する場合に必須ではありません。次に、条件を作成する 2 つの方法を示します。
  - 選択肢の対応するディクショナリから既存の条件または属性を選択します。
  - 推奨値を選択またはテキストボックスを使用してカスタム値を入力できるカスタム条件を作成します。
- 作成する条件名は、サポートされている次の文字のみを使用する必要があります。
  - 記号：ハイフン（-）、アンダースコア（_）、およびピリオド（.）。
  - アルファベット文字：A ～ Z、a ～ z。

- 数字：0 ～ 9。

- 認証プロファイルを作成または編集するときに、[クライアント プロビジョニング（ポリシー）（Client Provisioning (Policy)）] 以外のオプションで [Webリダイレクション（CWA、MDM、NSP、CPP）（Web Redirection (CWA, MDM, NSP, CPP)）] を有効にする場合、IPv6 アドレスをその許可ポリシーの [スタティックIP/ホスト名/FQDN（Static IP/Host name/FQDN）] として設定することはできません。これは、IPv6 のスタティック IP/ホスト名/FQDN が中央 Web 認証（CWA）、モバイル デバイス管理（MDM）リダイレクト、およびネイティブ サプリカント プロトコル（NSP）でサポートされていないためです。
- 権限は、ポリシーに使用する許可プロファイルを選択するときに重要です。権限は、特定のリソースへのアクセス権を付与したり、特定のタスクの実行を可能にしたりできます。たとえば、あるユーザーが特定の ID グループ（デバイス管理者など）に属しており、そのユーザーが定義済みの条件（サイトがボストンにあるなど）を満たしている場合、このユーザーは、そのグループに関連付けられた権限（特定のネットワーク リソースのセットへのアクセス権、デバイスへの特定の操作を実行する権限など）を付与されます。
- 認可条件で **radius** 属性 **Tunnel-Private-Group-ID** を使用する場合、**EQUALS** 演算子を使用するときに、条件にタグと値の両方を指定する必要があります。次に例を示します。

```
Tunnel-Private-Group-ID EQUALS (tag=0) 77
```

許可ポリシーの設定

[ポリシー（Policy）] メニューから許可ポリシーの属性および構成要素を作成したら、[ポリシーセット（Policy Sets）] メニューからポリシー セット内で許可ポリシーを作成します。

（注） Cisco ISE リリース 3.4 以降では、ディクショナリ属性として配列とともに pxGrid Direct コネクタのデータを使用して、認証ポリシーを設定することもできます。ポリシーの設定時には、“Contains” または “Matches” の演算子（正規表現の場合）を使用する必要があります。配列がある場合、”Equals” と “In” の演算子は機能しません。"AND" または "OR" 条件を使用して、複数の属性をネストできます。

始める前に

この手順を開始する前に、ID グループと条件など、許可ポリシーの作成に使用されるさまざまなビルディング ブロックについて基本を理解しておく必要があります。

ステップ 1 ネットワーク アクセス ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

ステップ 2 [表示（View）]列から、 をクリックしてすべてのポリシーセットの詳細にアクセスし、認証および許可ポリシーとポリシー例外を作成します。

ステップ 3 ページの許可ポリシー部分の横にある矢印アイコンをクリックして、[許可ポリシー（Authorization Policy）]テーブルを展開して表示します。

ステップ 4 いずれかの行の [アクション（Actions）] 列から、歯車アイコンをクリックします。ドロップダウン メニューから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して、新しい許可ポリシー ルールを挿入します。
[許可ポリシー（Authorization Policy）] テーブルに新しい行が表示されます。

ステップ 5 ポリシーのステータスを設定するには、現在の[ステータス（Status）]アイコンをクリックし、ドロップダウンリストの[ステータス（Status）]列から必要なステータスを選択します。ステータスの詳細については、許可ポリシーの設定 （1482 ページ） を参照してください。

ステップ 6 テーブル内のポリシーの場合は、[ルール名（Rule Name）]のセルをクリックしてフリーテキストを変更し、一意のルール名を作成します。

ステップ 7 条件を追加または変更するには、[条件（Conditions）] 列のセルにカーソルを合わせ、 をクリックします。[条件スタジオ（Conditions Studio）]が開きます。詳細については、ポリシー条件 （1490 ページ）を参照してください。

選択するすべての属性に「Equals」、「Not Equals」、「In」、「Not In」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現（REGEX）をサポートし、使用します。

（注） 単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数値属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。リストの場合、「in」演算子は、特定の値がリスト内に存在するかどうかをチェックします。単一文字列の場合、「in」演算子は、文字列が「equals」演算子などと同じかどうかをチェックします。

ステップ 8 ネットワーク アクセス結果プロファイルの場合は、[結果プロファイル（Results Profiles）] ドロップダウンリストから関連する許可プロファイルを選択するか、または を選択またはクリックして、[新しい許可プロファイルの作成（Create a New Authorization Profile）] を選択し、[新しい標準プロファイルの追加（Add New Standard Profile）] 画面が開いたら、次の手順を実行します。

a) 必要に応じて値を入力して、新しい許可プロファイルを設定します。次の点を考慮してください。

- [名前（name）] フィールドでサポートされる文字は次のとおりです：スペース、! # $ % & ‘ ( ) * + , - . / ; = ? @ _ {。
- [共通タスク（Common Tasks）]の場合、DACL を入力し、次の関連する [DACL名（DACL Name）] オプションを選択して、動的なドロップダウン リストから必要な DACL を選択します。
  - IPv4 DACL を使用するには、[DACL名（DACL Name）] をオンにします。
  - IPv6 DACL を入力するには、[IPv6 DACL名（IPv6 DACL Name）] をオンにします。

- 他の DACL 構文を入力するには、いずれかのオプションをオンにします。IPv4 と IPv6 の両方のドロップダウン リストに依存しない DACL が表示されます。

  （注） [DACL名（DACL Name）] を選択すると、DACL 自身が非依存でも、AVP タイプは IPv4 です。[IPv6 DACL名（IPv6 DACL Name）] の DACL を選択すると、DACL 自身が非依存でも、AVP タイプは IPv6 です。

- （注） ポリシーに ACL を使用する場合は、デバイスとこの機能に互換性があることを確認します。詳細については、『Cisco Identity Services Engine Compatibility Guide』を参照してください。

[共通タスク（Common Tasks）]の場合、ACL を入力するには、次のように関連する [ACL（フィルタID）（ACL (Filter-ID)）] オプションを選択し、フィールドに ACL 名を入力します。

- IPv4 ACL を使用するには、[ACL（フィルタID）（ACL (Filter-ID)）] をオンにします。
- IPv6 ACL を入力するには、[ACL IPv6（フィルタID）（ACL IPv6 (Filter-ID)）] をオンにします。

- Airespace デバイスで ACL を使用するには、必要に応じて [Airespace ACL名（Airespace ACL Name）] または [Airespace IPv6 ACL名（Airespace IPv6 ACL Name）] をオンにして、フィールドに ACL 名を入力します。
- 画面下部に動的に表示される [属性詳細（Attributes Details）] から許可プロファイル RADIUS 構文をダブルチェックできます。

b) [保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、許可プロファイルを作成します。

c) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）]** で [ポリシーセット（Policy Sets）] 領域外のプロファイルを作成、管理、編集、および削除します。

ステップ 9 ネットワーク アクセス結果のセキュリティ グループの場合は、[結果のセキュリティ グループ（Results Security Groups）] ドロップダウンリストから関連するセキュリティ グループを選択するか、または ➕ をクリックして、[新しいセキュリティ グループの作成（Create a New Security Group）] を選択し、[新しいセキュリティ グループの作成（Create New Security Group）] 画面が開いたら、次の手順を実行します。

a) 新規セキュリティ グループの名前と説明（オプション）を入力します。

b) タグ値を入力します。タグ値は、手動で入力したり、自動生成されるようにしたり設定できます。また SGT の範囲を予約できます。これは、から設定できます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSec の全般設定（General TrustSec Settings）]**

c) [送信（Submit）] をクリックします。

詳細については、セキュリティ グループの設定 （1612 ページ）を参照してください。

ステップ 10 TACACS+ の結果については、[結果（Results）] ドロップダウンリストから関連するコマンド セットとシェル プロファイルを選択するか、または [コマンド セット（Command Sets）] または [シェル プロファ

イル（Shell Profiles）] 列で ➕ をクリックして、[コマンドの追加（Add Commands）] 画面または [シェルプロファイルの追加（Add Shell Profile）] をそれぞれ開きます。[新しいコマンドセットの作成（Create a New Command Set）] または [新しいシェルプロファイルの作成（Create a New Shell Profile）] を選択し、フィールドに入力します。

ステップ 11 テーブル内でポリシーをチェックして一致させる順序を編成します。

ステップ 12 [保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、この新しい許可ポリシーを作成します。

許可ポリシーの設定

次の表では、[ポリシーセット（Policy Sets）] ウィンドウの [許可ポリシー（Authorization Policy）] セクションのフィールドについて説明します。このフィールドから、許可ポリシーをポリシーセットの一部として構成できます。ネットワーク アクセス ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

表 *137 :* 許可ポリシーの構成時の設定

フィールド名	使用上のガイドライン
ステータス（**Status**）	このポリシーのステータスを選択します。次のいずれかを設定できます。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニターのみ（Monitor Only）]：このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証（Live Log authentication）]ページでこのポリシー条件の結果を照会できます。ここでは、モニターされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加する場合に、条件がもたらす結果が正しいかどうかを判断できないことがあります。この場合、モニター モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。
ルール名（**Rule Name**）	このポリシーの一意の名前を入力します。
条件（**Conditions**）	新しいポリシー行から、プラス（+）アイコンをクリックするか、既存のポリシー行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
結果またはプロファイル（**Results or Profiles**）	関連する許可プロファイルを選択します。これにより、構成されたセキュリティ グループに提供される権限のそれぞれのレベルが決まります。関連する許可プロファイルをまだ設定していない場合は、インラインで行うことができます。
結果またはセキュリティグループ（**Results or Security Groups**）	関連するセキュリティグループを選択します。これにより、特定のルールに関連するユーザーのグループが決まります。関連するセキュリティ グループをまだ設定していない場合は、インラインで行うことができます。

フィールド名	使用上のガイドライン
結果またはコマンドセット（**Results or Command Sets**）	コマンド セットは、デバイス管理者が実行できるコマンドの指定されたリストを適用します。デバイス管理者がネットワーク デバイスに対して操作コマンドを発行すると、その管理者がこれらのコマンドの発行を認可されているかどうかを判定する問い合わせが ISE に行われます。これは、コマンド認可とも呼ばれます。
結果またはシェルプロファイル（**Results or Shell Profiles**）	TACACS+ シェル プロファイルは、デバイス管理者の最初のログイン セッションを制御します。
ヒット数（**Hits**）	ヒット数は、条件が一致した回数を示す診断ツールです。
アクション（**Actions**）	さまざまなアクションを表示して選択するには、[アクション（Actions）] 列の歯車アイコン をクリックします。 • [上に新しい行を挿入（Insert new row above）] : [アクション（Actions）] メニューを開いたルールの上に新しい許可ルールを挿入します。 • [下に新しい行を挿入（Insert new row below）] : [アクション（Actions）] メニューを開いたルールの下に新しい許可ルールを挿入します。 • [上に複製（Duplicate above）] : 元のセットの上に、[アクション（Actions）] メニューを開いたルールの上に複製許可ルールを挿入します。 • [下に複製（Duplicate below）] : 元のセットの下に、[アクション（Actions）] メニューを開いたルールの下に複製許可ルールを挿入します。 • [削除（Delete）] : ルールを削除します。

許可プロファイルの設定

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Authorization）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]**を選択し、[認証プロファイル（Authorization Profiles）] ウィンドウでは、ネットワークアクセスの属性を定義します。

（注） シスコ以外のデバイスで Cisco ISE 2.x リリースから Cisco ISE 3.x リリースにアップグレードする場合、認証プロファイルに ACL 値が設定されたネットワーク デバイス プロファイルが含まれていると、アップグレードが失敗する可能性があります。これは、ネットワーク デバイス プロファイルが ACL を設定するようになっていないためです。

この問題を回避するには、値を手動で削除するか、該当する認証プロファイル自体を削除します。

許可プロファイルの設定

- [名前（Name）]：この新しい認証プロファイルの名前を入力します。
- [説明（Description）]：許可プロファイルの説明を入力します。
- [アクセスタイプ（Access Type）]：アクセスタイプ（[ACCESS_ACCEPT] または [ACCESS_REJECT]）を選択します。
- [サービステンプレート（Service Template）]：SAnet 対応デバイスとのセッションをサポートするには、このオプションを有効にします。Cisco ISE は、許可プロファイルを「サービステンプレート」互換としてマークする特別なフラグを使用して、許可プロファイルにサービステンプレートを実装します。サービステンプレートは許可プロファイルでもあるため、SAnet デバイスと非 SAnet デバイスの両方をサポートする単一のポリシーとして機能します。
- [移動の追跡（Track Movement）]：Cisco Mobility Services Engine（MSE）を使用してユーザーの場所を追跡するには、このオプションを有効にします。

（注） このオプションは、Cisco ISE のパフォーマンスに影響を与える可能性があります。これは、セキュリティレベルの高い場所を対象としています。

- [Passive Identityトラッキング（Passive Identity Tracking）]：ポリシーの適用とユーザートラッキングのために Passive Identity の Easy Connect 機能を使用するには、このオプションを有効にします。

一般的なタスク

一般的なタスクは、ネットワークアクセスに適用される特定の権限とアクションです。

- [DACL名（DACL Name）]：ダウンロード可能なACLを使用するには、このオプションを有効にします。デフォルト値（**PERMIT_ALL_IPV4_TRAFFIC**、**PERMIT_ALL_IPV6_TRAFFIC**、**DENY_ALL_IPV4_TRAFFIC**、**DENY_ALL_IPV6_TRAFFIC**）を使用するか、次のディクショナリから属性を選択することができます。
  - 外部 ID ストア（属性）（External identity store (attributes)）
  - エンドポイント
  - 内部ユーザー
  - 内部エンドポイント

  DACLの追加、または既存のDACLの編集および管理の詳細については、ダウンロード可能 ACL （1475 ページ）を参照してください。

- [ACL（フィルタID）（ACL（Filter-ID））]：RADIUS フィルタ ID 属性を設定するには、このオプションを有効にします。フィルタ ID は、NAD の ACL を指定します。フィルタ ID は [属性の詳細（Attributes Details）] ペインに表示されます。[ACL IPv6（フィルタID）（ACL IPv6（Filter-ID））] は、NAD への IPv6 接続と同じ方法で動作します。

（注） Cisco ISE 3.0 以降では、テキストを入力するか、[ACLフィルタID（ACL Filter-ID）] の [属性値（Attribute Values）] ドロップダウンリストから必要な属性を選択できます。[ACLフィルタID（ACL Filter-ID）] のテキストを入力する場合は、シスコデバイスのサフィックス「.in」を追加する必要があります。

- [セキュリティグループ（Security group）]：認証の一部としてセキュリティグループ（SGT）を割り当てるには、このオプションを有効にします。

  Cisco ISE 3.2 以降では、セキュリティグループを選択するときに、仮想ネットワークを任意で指定できます。その場合、ドロップダウンリストから選択するか、必要なテキストを入力します。任意で VLAN 名を指定することもできます。

  セキュリティグループタスクには、セキュリティグループとオプションのVNが含まれています。セキュリティグループを設定する場合、別個に VLAN を設定することはできません。エンドポイントデバイスは、1 つの仮想ネットワークにのみ割り当てることができます。

- [VLAN]：仮想LAN（VLAN）IDを指定するには、このオプションを有効にします。VLAN ID には、整数または文字列値を入力できます。このエントリの形式は、Tunnel-Private-Group-ID:VLANnumber です。

- [音声ドメイン権限（Voice Domain Permission）]：ダウンロード可能な ACL を使用するには、このオプションを有効にします。`cisco-av-pair` のベンダー固有属性（VSA）を `device-traffic-class=voice` の値と関連付けます。複数ドメインの許可モードでは、ネットワークスイッチがこの VSA を受信した場合、エンドポイントは、許可後に音声ドメインに接続されます。
- [Webリダイレクション（CWA、DRW、MDM、NSP、CPP）（Web Redirection（CWA, DRW, MDM, NSP, CPP））]：認証後に Web リダイレクションを有効にするには、このオプションを有効にします。
  - リダイレクションのタイプを選択します。選択した Web リダイレクションのタイプには、次で説明する追加のオプションが表示されます。
  - Cisco ISE が NAD に送信するリダイレクションをサポートするための ACL を入力します。

    NAD に送信するために入力する ACL は、cisco-av ペアとして [属性の詳細（Attributes Details）] ペインに表示されます。たとえば、**acl119** と入力した場合、これは [属性の詳細（Attributes Details）] ペインには `cisco-av-pair = url-redirect-acl = acl119` と表示されます。
  - 選択した Web リダイレクションタイプのその他の設定を選択します。

  次のタイプの Web リダイレクションのいずれかを選択します。
  - [中央集中Web認証（Centralized Web Auth）]：[値（Value）] ドロップダウンから選択したポータルにリダイレクトします。
  - [クライアント プロビジョニング（ポスチャ）（Client Provisioning (Posture)）]：クライアントでポスチャを有効にするため、[値（Value）] ドロップダウンから選択したクライアント プロビジョニング ポータルにリダイレクトします。
  - [ホットスポット: リダイレクト（Hot Spot: Redirect）]：[値（Value）] ドロップダウンから選択したホットスポットポータルにリダイレクトします。
  - [MDM リダイレクト（MDM Redirect）]：指定した MDM サーバーの MDM ポータルにリダイレクトします。
  - [ネイティブサプリカントのプロビジョニング（Native Supplicant Provisioning）]：[値（Value）] ドロップダウンから選択した BYOD にリダイレクトします。

  Web リダイレクションタイプを選択し、必要なパラメータを入力したら、次のオプションを設定します。
  - [証明書更新メッセージの表示（Display Certificates Renewal Message）]：証明書更新メッセージを表示するには、このオプションを有効にします。url-redirect 属性値が変更され、この値に証明書が有効である日数が含まれます。このオプションは、中央集中型 Web 認証のみに使用できます。
  - [スタティックIP/ホスト名/FQDN（Static IP/Host Name/FQDN）]：ユーザーを別の PSN にリダイレクトするには、このオプションを有効にします。ターゲット IP アドレス、

ホスト名、またはFQDNを入力します。このオプションを設定しない場合、ユーザーはこの要求を受信したポリシーサービスノードの FQDN にリダイレクトされます。

- [論理プロファイルでエンドポイントのプロファイラCoAを抑制する（Suppress Profiler CoA for endpoints in Logical Profile）]：特定のタイプのエンドポイントデバイスのリダイレクトをキャンセルするには、このオプションを有効にします。

- [自動スマートポート（Auto smartport）]：自動スマートポート機能を使用するには、このオプションを有効にします。イベント名を入力します。これにより、この値を持つ VSA の cisco-av-pair が `auto-smart-port=event_name` として作成されます。この値は、[属性詳細（Attributes Details）] ペインに表示されます。

- [アクセスの脆弱性（Access Vulnerabilities）]：このオプションを有効にすると、このエンドポイントでの脅威中心型 NAC 脆弱性評価を許可の一環として実行できます。アダプタを選択し、スキャンを実行するタイミングを選択します。

- [再認証（Reauthentication）]：再認証中にエンドポイントを接続したままにするには、このオプションを有効にします。 [RADIUS要求（RADIUS-Request）]（1）を使用することを選択して、再認証中に接続を維持することを選択します。 デフォルトの [RADIUS要求（RADIUS-Request）]（0）では、既存のセッションを切断します。非アクティビティタイマーを設定することもできます。

- [MACSec ポリシー（MACSec Policy）]：MACSec 対応クライアントが Cisco ISE に接続するたびにMACSec暗号化ポリシーを使用するには、このオプションを有効にします。次のオプションのいずれかを選択します。[must-secure]、[should-secure]、または [must-not-secure]。 設定は [属性詳細（Attributes Details）] ペインに `cisco-av-pair = linksec-policy=must-secure` と表示されます。

- [NEAT]：ネットワーク間の ID 認識を拡張するネットワーク エッジ アクセス トポロジ（NEAT）を使用するには、このオプションを有効にします。このチェックボックスをオンにすると、[属性の詳細（Attributes Details）] ペインに、`cisco-av-pair = device-traffic-class=switch` と表示されます。

- [Web認証（ローカルWeb認証）（Web Authentication（Local Web Auth））]：この許可プロファイルのローカル Web 認証を使用するには、このオプションを有効にします。この値では、Cisco ISE が DACL とともに VSA を送信することによって Web 認証の許可をスイッチが認識できます。VSA は `cisco-av-pair = priv-lvl=15` で、これは [属性の詳細（Attributes Details）] ペインに表示されます。

- [Airespace ACL名（Airespace ACL Name）]：Cisco Airespace ワイヤレスコントローラに ACL 名を送信するには、このオプションを有効にします。Airespace VSA はこの ACL を使用して、ローカルで定義された WLC 上の接続への ACL を許可します。たとえば、**rsa-1188** と入力した場合、これは [属性の詳細（Attributes Details）] ペインに `Airespace-ACL-Name = rsa-1188` と表示されます。

- [ASA VPN]：適応型セキュリティアプライアンス（ASA）VPN グループポリシーを割り当てるには、このオプションを有効にします。ドロップダウンリストから、VPN グループポリシーを選択します。

- [AVCプロファイル名（AVC Profile Name）]：このエンドポイントでアプリケーションの可視性を実行するには、このオプションを有効にします。使用する AVC プロファイルを入力します。
- [UPNルックアップ（UPN Lookup）]：未定

高度な属性設定（Advanced Attributes Settings）

- [ディクショナリ（Dictionaries）]：下矢印アイコンをクリックし、[ディクショナリ（Dictionaries）] ウィンドウに選択可能なオプションを表示します。最初のフィールドで設定する必要があるディクショナリと属性を選択します。
- [属性値（Attribute Values）]：下矢印アイコンをクリックし、[属性値（Attribute Values）] ウィンドウに選択可能なオプションを表示します。目的の属性グループと属性値を選択します。この値は、最初のフィールドで選択した値と一致します。設定する [高度な属性（Advanced Attributes）] が [属性の詳細（Attribute Details）] パネルに表示されます。
- [属性の詳細（Attributes Details）]：このペインには、[共通タスク（Common Tasks）] および [高度な属性（Advanced Attributes）] に設定した設定済みの属性値が表示されます。

  [属性の詳細（Attributes Details）] ペインに表示される値は読み取り専用です。

（注） [属性の詳細（Attributes Details）] ペインに表示される読み取り専用の値を変更または削除するには、対応する [共通タスク（Common Tasks）] フィールド、または [高度な属性設定（Advanced Attributes Settings）] ペインの [属性値（Attribute Values）] で選択した属性でこれらの値を変更または削除します。

関連トピック

Cisco ISE の許可プロファイル （1474 ページ）
許可プロファイルの権限 （1475 ページ）
未登録のデバイスのリダイレクトのための許可プロファイルの設定 （1445 ページ）
許可プロファイルの作成 （856 ページ）

許可ポリシーの例外

各ポリシーセット内では、通常の認証ポリシーの他に、ローカルの例外ルール（各ポリシーセットの [設定（Set）] ビューの [認証ポリシーのローカル例外（Authorization Policy Local Exceptions）] パートから定義される）およびグローバル例外ルール（各ポリシーセットの [設定（Set）] ビューの [認証ポリシーのグローバル例外（Authorization Policy Global Exceptions）] パートから定義される）も定義できます。

グローバル許可例外ポリシーを使用すると、すべてのポリシーセット内のすべての許可ルールを上書きするルールを定義できます。グローバル許可例外ポリシーを設定すると、すべてのポリシーセットに追加されます。グローバル許可例外ポリシーは、現在設定されているポリシー

セットのいずれかから更新できます。グローバル許可例外ポリシーを更新するたびに、それらの更新がすべてのポリシー セットに適用されます。

ローカル許可例外ルールは、グローバル例外ルールを上書きします。許可ルールは、許可ポリシーのローカル例外規則、グローバル例外規則、通常ルールの順番で処理されます。

認証例外ポリシールールは、認証ポリシールールと同じように設定されます。認証ポリシーについては、許可ポリシーの設定 （1479 ページ）を参照してください。

（注） Cisco ISE では、認証ポリシーで % 文字を使用してセキュリティ問題を回避することはサポートできません。

ローカル例外およびグローバル例外の構成時の設定

ネットワーク アクセス ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシーセット（Policy Sets）]** > **[表示（View）]** > **[ローカル例外ポリシー（Local Exceptions Policy）]** または **[グローバル例外ポリシー（Global Exceptions Policy）]** を選択します。

許可例外設定は、許可ポリシー設定と同じで、許可ポリシーの設定 （1482 ページ） で説明されています。

ポリシー条件

Cisco ISE はルールベースのポリシーを使用してネットワーク アクセスを提供します。ポリシーは、ルールが条件で構成されているルールと結果のセットです。Cisco ISE では、個々のポリシー要素として条件を作成し、システム ライブラリに保存してから、[条件スタジオ（Conditions Studio）] の他のルールベースのポリシーに再利用することができます。

条件では演算子（等しい、等しくない、より大きい、など）と値を使用し、必要に応じて単純にすることも、複雑にすることもできます。また、複数の属性、演算子、複雑な階層を含めることもできます。実行時に、Cisco ISE はポリシー条件を評価し、ポリシー評価が true または false 値のどちらを返すかに応じて、定義された結果を適用します。

条件を作成して一意の名前を割り当てた後、この条件を [条件スタジオ ライブラリ（Conditions Studio Library）] から選択することで、さまざまなルールとポリシーにわたって複数回再利用することができます。例を次に示します。

```
Network Conditions.MyNetworkCondition EQUALS true
```

ポリシーで使用されているか、または別の条件の一部である条件は[条件スタジオ（Conditions Studio）] から削除できません。

各条件は、オブジェクトのリストを定義します。このリストはポリシー条件に含めることができ、これにより、要求で示される定義と照合される定義セットになります。

演算子 `EQUALS true` を使用して、ネットワーク条件が true であるかどうか（要求に指定されている値がネットワーク条件の1つ以上のエントリと一致しているかどうか）を確認するか、または`EQUALS false` を使用して、ネットワーク条件が false であるかどうか（ネットワーク条件のどのエントリとも一致しないかどうか）を確認することができます。

Cisco ISE には、事前定義されたスマート条件も用意されています。この条件は、ポリシーで個別に使用したり、独自のカスタマイズされた条件で構成要素として使用でき、必要に応じて更新および変更できます。

次の固有のネットワーク条件を作成してネットワークへのアクセスを制限することができます。

- エンドステーション ネットワーク条件（Endstation Network Conditions）：接続が開始および終了されるエンドステーションに基づきます。

  Cisco ISE はリモート アドレスの [TO] フィールド（TACACS+ 要求または RADIUS 要求であるかに基づいて取得）を評価し、これがエンドポイントの IP アドレス、MAC アドレス、発信側回線ID（CLI）、または着信番号識別サービス（DNIS）のいずれであるかを確認します。

  RADIUS 要求では、この ID は属性 31（Calling-Station-Id）で使用できます。

  TACACS+ 要求では、リモート アドレスにスラッシュ（/）が含まれている場合、スラッシュより前の部分は [FROM] の値として見なされ、スラッシュより後の部分は [TO] 値として見なされます。たとえば、要求に CLI/DNIS と指定されている場合、CLI は [FROM] の値と見なされ、DNIS は [TO] の値と見なされます。スラッシュが含まれていない場合は、リモート アドレス全体が [FROM] の値として見なされます（IP アドレス、MAC アドレス、CLI いずれの場合でも）。

- デバイス ネットワーク条件（Device Network Conditions）：要求を処理する AAA クライアントに基づきます。

  ネットワーク デバイスは、IP アドレス、ネットワーク デバイス リポジトリで定義されているデバイス名、またはネットワーク デバイス グループによって識別されます。

  RADIUS 要求では、属性 4（NAS-IP-Address）が指定されている場合、Cisco ISE はこの属性から IP アドレスを取得します。属性 32（NAS-Identifier）が存在する場合、Cisco ISE は属性 32 から IP アドレスを取得します。これらの属性が存在しない場合は、受信したパケットから IP アドレスを取得します。

  デバイス ディクショナリ（NDG ディクショナリ）にはネットワーク デバイス グループ属性（Location、Device Type、または NDG を表すその他の動的に作成された属性など）が含まれています。これらの属性には、現在のデバイスに関連するグループが含まれています。

- デバイス ポート ネットワーク条件（Device Port Network Conditions）：デバイスの IP アドレス、名前、NDG、およびポート（エンドポイントが接続しているデバイスの物理ポート）に基づきます。

  RADIUS 要求では、属性 5（NAS-Port）が要求内に存在する場合、Cisco ISE はこの属性から値を取得します。属性 87（NAS-Port-Id）が要求内に存在する場合、Cisco ISE は属性 87 から要求を取得します。

  TACACS+ 要求では、Cisco ISE はその ID を（すべてのフェーズの）開始要求のポート フィールドから取得します。

これらの固有条件の詳細については、特別なネットワーク アクセス条件 （1513 ページ） を参照してください。

ディクショナリおよびディクショナリ属性

ディクショナリは、ドメインのアクセス ポリシーの定義に使用できる属性と許容値のドメイン固有カタログです。個々のディクショナリは、属性タイプの同種の集合です。ディクショナリで定義された属性は同じ属性タイプを持ち、タイプは特定の属性のソースまたはコンテキストを示します。

属性タイプは次のいずれかになります。

- MSG_ATTR
- ENTITY_ATTR
- PIP_ATTR

属性と許容値に加えて、ディクショナリには名前と説明、データ型、デフォルト値などの属性に関する情報が含まれます。属性は、次のいずれかのデータ型となります。BOOLEAN、FLOAT、INTEGER、IPv4、IPv6、OCTET_STRING、STRING、UNIT32、および UNIT64。

Cisco ISE ではインストール中にシステム ディクショナリが作成され、ユーザー ディクショナリを作成できます。

属性は、異なるシステム ディクショナリに格納されます。属性を使用して、条件を構成します。属性は、複数の条件で再利用できます。

ポリシー条件を作成するときに、有効な属性を再利用するには、サポートされている属性を含むディクショナリから選択します。たとえば、Cisco ISE は、AuthenticationIdentityStore という属性を提供しています。これは NetworkAccess ディクショナリにあります。この属性は、ユーザーの認証中にアクセスされた最後の ID ソースを識別します。

- 認証中に単一の ID ソースが使用されると、この属性には認証が成功した ID ストアの名前が含まれます。
- 認証中に ID ソース順序を使用する場合、この属性にはアクセスされた最後の ID ソースの名前が含まれます。

AuthenticationStatus 属性を AuthenticationIdentityStore 属性と組み合わせて使用し、ユーザーが正常に認証された ID ソースを識別する条件を定義できます。たとえば、許可ポリシーで LDAP ディレクトリ（LDAP13）を使用してユーザーが認証された条件をチェックするために、次の再利用可能な条件を定義できます。

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

（注） AuthenticationIdentityStore は、条件にデータを入力できるテキストフィールドを表します。このフィールドには、名前を必ず正しく入力またはコピーします。ID ソースの名前が変更された場合は、ID ソースの変更と一致するように、この条件を変更する必要があります。

以前認証されたエンドポイント ID グループに基づく条件を定義するために、Cisco ISE では、エンドポイント ID グループ 802.1X 認証ステータスの間に定義された許可をサポートしています。Cisco ISE では、802.1X 認証を実行するとき、RADIUS 要求の「Calling-Station-ID」フィールドから MAC アドレスを抽出し、この値を使用して、デバイスのエンドポイント ID グループ（endpointIDgroup 属性として定義）のセッション キャッシュを検索して読み込みます。このプロセスによって、許可ポリシー条件の作成に endpointIDgroup 属性を使用できるようになり、ユーザー情報に加えてこの属性を使用して、エンドポイント ID グループ情報に基づく許可ポリシーを定義できます。

エンドポイント ID グループの条件は、[許可ポリシー設定（authorization policy configuration）] ページの [ID グループ（ID Groups）] カラムで定義できます。ユーザー関連情報に基づく条件は、許可ポリシーの [その他の条件（Other Conditions）] のセクションで定義する必要があります。ユーザー情報が内部ユーザー属性に基づいている場合は、内部ユーザーディクショナリの ID グループ属性を使用します。たとえば、「User Identity Group:Employee:US」のような値を使用して、ID グループに完全な値のパスを入力できます。

ネットワーク アクセス ポリシーでサポートされるディクショナリ

Cisco ISE は、認証ポリシーと許可ポリシーの条件とルールを構築する際に必要なさまざまな属性を含む次のシステム格納ディクショナリをサポートしています。

- システム定義されたディクショナリ
  - CERTIFICATE
  - DEVICE
  - RADIUS
- RADIUS ベンダー ディクショナリ
  - Airespace
  - Cisco
  - Cisco-BBSM
  - Cisco-VPN3000

- Microsoft
- Network Access

許可ポリシータイプの場合、条件で設定された検証は、戻される許可プロファイルに従う必要があります。

確認には、通常、ライブラリに追加して他のポリシーで再利用できるユーザー定義名を含む 1 つ以上の条件が含まれます。

以下の項では、条件の設定に使用できるサポートされている属性とディクショナリについて説明します。

ディクショナリによってサポートされる属性

表に、ディクショナリでサポートされる固定属性を示します。これらの属性をポリシー条件内で使用できます。作成する条件のタイプによっては、使用できない属性もあります。

たとえば、認証ポリシー内でアクセス サービスを選択する条件を作成する場合、使用できるネットワーク アクセス属性は、Device IP Address、ISE Host Name、Network Device Name、Protocol、および Use Case のみです。

次の表に示す属性をポリシー条件に使用できます。

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
Device	Device Type（定義済みのネットワーク デバイス グループ）	はい	はい
	Device Location（定義済みのネットワーク デバイス グループ）		
	Other Custom Network Device Group		
	Software Version		
	Model Name		
RADIUS	すべての属性	はい	はい

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
Network Access	ISE Host Name	はい	はい
	AuthenticationMethod	いいえ	はい
	AuthenticationStatus	いいえ	いいえ
	CTSDeviceID	いいえ	いいえ
	Device IP Address	はい	はい
	EapAuthentication（マシンのユーザーの認証時に使用される EAP 方式）	いいえ	はい
	EapTunnel（トンネルの確立に使用される EAP 方式）	いいえ	はい
	Protocol	はい	はい
	UseCase	はい	はい
	UserName	いいえ	はい
	WasMachineAuthenticated	いいえ	いいえ

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
Certificate	Common Name	いいえ	はい
	Country		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	Issuer		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
	Issuer - Street Address		
	Issuer - Domain Component		
	Issuer - User ID		

システム定義のディクショナリとディクショナリ属性

Cisco ISE は、インストール中にシステム ディクショナリを作成します。これは、[システム ディクショナリ（System Dictionaries）] ページで確認できます。システム定義のディクショナリ属性は、読み取り専用の属性です。その特性のため、既存のシステム定義のディクショナリは表示することのみができます。システム定義の値またはシステムディクショナリ内の属性を作成、編集、削除することはできません。

システム定義のディクショナリ属性は、属性の記述名、ドメインによって認識される内部名、および許容値とともに表示されます。

また、Cisco ISE は Internet Engineering Task Force（IETF）で定義され、システム定義のディクショナリにも含まれる IETF RADIUS 属性セット用にディクショナリ デフォルトを作成します。ID を除くすべてのフリー IETF RADIUS 属性フィールドを編集できます。

システム ディクショナリおよびディクショナリ属性の表示

システムディクショナリ内のシステム定義の属性を作成、変更、削除することはできません。システム定義された属性は表示することのみができます。ディクショナリの名前と説明に基づくクイック検索またはユーザー定義の検索ルールに基づく高度な検索を実行できます。

ステップ 1

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[システム（System）]** を選択します。

ステップ 3 [システム ディクショナリ（System Dictionaries）] ページからシステム ディクショナリを選択して [表示（View）] をクリックします。

ステップ 4 [ディクショナリ属性（Dictionary Attributes）] をクリックします。

ステップ 5 リストからシステム ディクショナリを選択して [表示（View）] をクリックします。

ステップ 6 [システム ディクショナリ（System Dictionaries）] ページに戻るには、[ディクショナリ（Dictionaries）] リンクをクリックします。

ユーザー定義のディクショナリとディクショナリ属性

Cisco ISE では、[ユーザー ディクショナリ（User Dictionary）] ページで作成したユーザー定義ディクショナリが表示されます。システムで作成され、保存された既存のユーザーディクショナリの [ディクショナリ名（Dictionary Name）] または [ディクショナリ タイプ（Dictionary Type）] の値は変更できません。

[ユーザー ディクショナリ（User Dictionaries）] ページでは、次の操作を実行できます。

- ユーザー ディクショナリを編集および削除します。
- 名前および説明に基づいてユーザー ディクショナリを検索します。

- ユーザーディクショナリのユーザー定義のディクショナリ属性を追加、編集、および削除します。
- NMAP スキャン機能を使って、NMAP 拡張ディクショナリの属性を削除します。カスタム ポートが [NMAP スキャン アクション（NMAP Scan Actions）] ページで追加または削除されると、対応するカスタム ポート属性がディクショナリで追加、削除または更新されます。
- ディクショナリ属性の許容値を追加または削除します。

ユーザー定義のディクショナリの作成

ユーザー定義のディクショナリを作成、編集、または削除できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[ユーザー（User）]**

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ユーザー ディクショナリの名前、オプションの説明、およびバージョンを入力します。

ステップ 4 [ディクショナリ属性タイプ（Dictionary Attribute Type）] ドロップダウン リストから属性タイプを選択します。

ステップ 5 [送信（Submit）] をクリックします。

ユーザー定義のディクショナリ属性の作成

ユーザーディクショナリの、ユーザー定義のディクショナリ属性を追加、編集および削除したり、ディクショナリ属性に使用できる値を追加または削除したりすることができます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[ユーザー（User）]**

ステップ 2 [ユーザーディクショナリ（User Dictionaries）] ページからユーザーディクショナリを選択して [編集（Edit）] をクリックします。

ステップ 3 [ディクショナリ属性（Dictionary Attributes）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 ディクショナリ属性の属性名、オプションの説明、および内部名を入力します。

ステップ 6 [データ型（Data Type）] ドロップダウン リストからデータ型を選択します。

ステップ 7 [追加（Add）] をクリックして、[使用できる値（Allowed Values）] テーブルで名前、使用できる値、およびデフォルト ステータスを設定します。

ステップ 8 [送信（Submit）] をクリックします。

RADIUS ベンダー ディクショナリ

Cisco ISE では、一連の RADIUS ベンダー ディクショナリを定義したり、それぞれの一連の属性を定義したりできます。リスト内の各ベンダー定義には、ベンダー名、ベンダー ID、および簡単な説明が含まれています。

Cisco ISE では、次の RADIUS ベンダー ディクショナリがデフォルトで提供されます。

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

RADIUS プロトコルは、これらのベンダーディクショナリと、許可プロファイルとポリシー条件で使用できるベンダー固有属性をサポートします。

RADIUS ベンダー ディクショナリの作成

RADIUS ベンダーディクショナリを作成、編集、削除、エクスポート、およびインポートすることもできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[システム（System）]** > **[Radius（Radius）]** > **[Radiusベンダー（Radius Vendors）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 RADIUS ベンダーの Internet Assigned Numbers Authority（IANA）で承認されている RADIUS ベンダー ディクショナリの名前、オプションの説明、およびベンダーIDを入力します。ベンダーIDはグローバルIANAベンダーリスト全体で一意にする必要があり、既存のベンダーが使用することはできません。

ステップ 4 属性値から取得したバイト数を選択して、[ベンダー属性タイプ フィールド長（Vendor Attribute Type Field Length）] ドロップダウン リストから属性タイプを指定します。有効な値は、1、2、および4です。デフォルト値は 1 です。

ステップ 5 属性値から取得したバイト数を選択して、[ベンダー属性サイズ フィールド長（Vendor Attribute Size Field Length）] ドロップダウン リストから属性長を指定します。有効な値は 0 と 1 です。デフォルト値は 1 です。

ステップ 6 [送信（Submit）] をクリックします。

RADIUS ベンダー ディクショナリ属性の作成

Cisco ISE がサポートする RADIUS ベンダー属性を作成、編集、および削除できます。各 RADIUS ベンダー属性には、名前、データ型、説明、および方向（要求のみに関連する、応答のみに関連する、または両方に関連するかどうかを指定）が含まれています。

ステップ 1 次のとおり選択します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [Radius（Radius）] > [Radiusベンダー（Radius Vendors）]**

ステップ 2 RADIUS ベンダーディクショナリ リストから RADIUS ベンダーディクショナリを選択して [編集（Edit）] をクリックします。

ステップ 3 [ディクショナリ属性（Dictionary Attributes）] をクリックし、[追加（Add）] をクリックします。

ステップ 4 RADIUS ベンダー属性の属性名とオプションの説明を入力します。

ステップ 5 [データ型（Data Type）] ドロップダウン リストからデータ型を選択します。

ステップ 6 [MAC オプションの有効化（Enable MAC option）] チェックボックスを選択します。

ステップ 7 RADIUS 要求のみ、RADIUS 応答のみ、またはその両方に適用される方向を [方向（Direction）] ドロップダウン リストから選択します。

ステップ 8 [ID] フィールドにベンダー属性 ID を入力します。

ステップ 9 [タグ付けの許可（Allow Tagging）] チェックボックスをオンにします。

ステップ 10 [プロファイルのこの属性の複数インスタンスを許可する（Allow multiple instances of this attribute in a profile）] チェックボックスをオンにします。

ステップ 11 [追加（Add）] をクリックして、[使用できる値（Allowed Values）] テーブルにベンダー属性の使用できる値を追加します。

ステップ 12 [送信（Submit）] をクリックします。

HP RADIUS IETF サービス タイプ属性

Cisco ISE では、RADIUS IETF サービス タイプ属性に 2 つの新しい値が導入されました。RADIUS IETF サービスタイプ属性は、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [RADIUS] > [IETF]Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [RADIUS] > [IETF] で使用できます。ポリシーの条件で次の 2 つの値を使用できます。これら 2 つの値は、特に HP のデバイスがユーザーの権限を理解できるように設計されています。

列挙名	列挙値
HP-Oper	252
HP-User	255

RADIUS ベンダー ディクショナリ属性の設定

ここでは、Cisco ISE で使用される RADIUS ベンダーのディクショナリについて説明します。

次の表に、RADIUS ベンダーのディクショナリ属性を設定できるようにする RADIUS ベンダーの [ディクショナリ（Dictionary）] ウィンドウのフィールドを示します。Cisco ISE GUI で [メ

ニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[システム（System）]** > **[RADIUS]** > **[RADIUS ベンダー（RADIUS Vendors）]**。

表 *138 : RADIUS* ベンダー ディクショナリ属性の設定

フィールド名	使用上のガイドライン
属性名（Attribute Name）	選択した RADIUS ベンダーのベンダー固有属性名を入力します。
説明（Description）	ベンダー固有属性のオプションの説明を入力します。
内部名（Internal Name ）	内部のデータベースで表されるベンダー固有属性の名前を入力します。
データタイプ（Data Type）	ベンダー固有属性に対して、次のデータ型のいずれかを選択します。 • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4 • IPV6
MAC を有効にするオプション（Enable MAC option）	MAC アドレスとしての RADIUS 属性の比較を有効にするには、このチェックボックスをオンにします。デフォルトで、RADIUS 属性 Calling-Station-ID に対して、このオプションは有効とマークされ、無効にできません。RADIUSベンダーディクショナリ内の別のディクショナリ属性（文字列型）の場合は、このオプションを有効または無効にできます。 このオプションを有効にした場合、認証および許可条件の設定中に、テキスト オプションを選択して比較をクリアな文字列にするか、またはMACアドレスオプションを選択して比較をMACアドレスにするかを定義できます。
方向（Direction）	RADIUS メッセージに適用するいずれかのオプションを選択します。

フィールド名	使用上のガイドライン
ID	ベンダー属性 ID を入力します。有効な範囲は 0 ～ 255 です。
タギングの許可（Allow Tagging）	RFC2868 で定義するように、タグを持つことが許可されるものとして属性をマークするには、このチェック ボックスをオンにします。タグの目的は、トンネル化されたユーザーの属性のグループ化を許可することです。詳細については、RFC2868 を参照してください。 タグ付けされた属性のサポートでは、特定のトンネルに関するすべての属性のそれぞれのタグ フィールドに同じ値が含まれ、各セットに Tunnel-Preference 属性の適切に評価されたインスタンスが含まれていることが保証されます。これは、マルチベンダー ネットワーク環境に使用すべきトンネル属性に適合しているため、複数のベンダーで製造されたネットワーク アクセス サーバー（NAS）間の相互運用性の問題を解決します。
プロファイルでこの属性の複数のインスタンスを許可する（Allow Multiple Instances of this Attribute in a Profile）	プロファイルでこの RADIUS ベンダー固有属性の複数のインスタンスが必要な場合は、このチェックボックスをオンにします。

関連トピック

システム定義のディクショナリとディクショナリ属性 （1497 ページ）
ユーザー定義のディクショナリとディクショナリ属性 （1497 ページ）
RADIUS ベンダー ディクショナリ （1499 ページ）
RADIUS ベンダー ディクショナリの作成 （1499 ページ）

[条件スタジオ（Conditions Studio）] の操作

[条件スタジオ（Conditions Studio）] は、条件の作成、管理、および再利用に使用します。条件には複数のルールを含めることができ、1 つのみのレベルまたは複数の階層レベルを含む任意の複雑度で構築できます。[条件スタジオ（Conditions Studio）] を使用して新しい条件を作成する場合は、[ライブラリ（Library）] にすでに保存している条件ブロックを使用することができ、それらの保存された条件ブロックを更新および変更することもできます。後で条件を作成および管理する際に、クイック カテゴリ フィルタなどを使用して、必要なブロックと属性を簡単に見つけることができます。

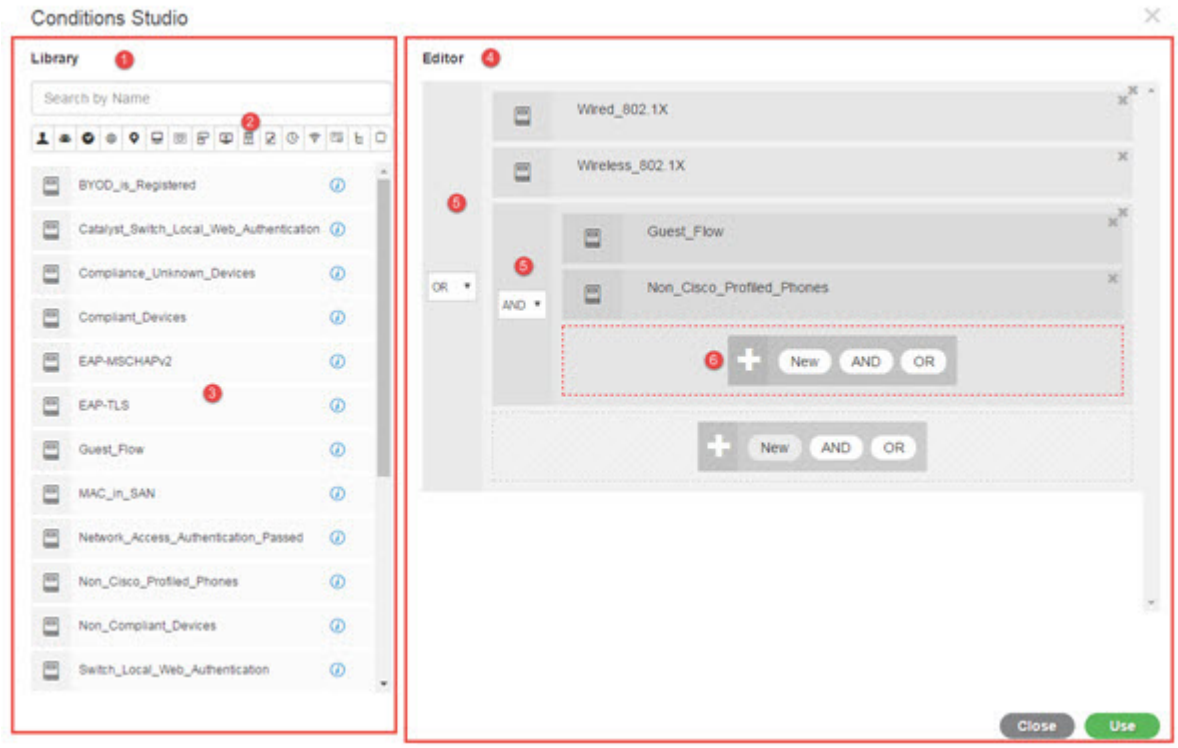
ネットワーク アクセス ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理

ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

いずれかのポリシーセットの特定のルールにすでに適用されている条件を編集または変更するには、[条件（Conditions）] 列のセルにカーソルを合わせ をクリックするか、または新しい条件を作成するには [ポリシーセット（Policy Set）] テーブルの [条件（Conditions）] 列のプラス記号 ✚ をクリックします。その条件は、すぐに同じポリシーセットに適用することができます。または、後で使用するために [ライブラリ（Library）] に保存することもできます。

次の図に、[条件スタジオ（Conditions Studio）] の主な要素を示します。

図 *58 : [条件スタジオ（Conditions Studio）]*



[条件スタジオ（Conditions Studio）] は、[ライブラリ（Library）] と [エディタ（Editor）] の 2 つの主要部分に分かれています。[ライブラリ（Library）] には再使用のために条件ブロックが保存され、[エディタ（Editor）] では保存されたブロックを編集したり新しいブロックを作成できます。

次の表では、[条件スタジオ（Conditions Studio）] のさまざまな部分について説明します。

フィールド	使用上のガイドライン
ライブラリ（Library）	再利用のために ISE データベースで作成され保存されたすべての条件ブロックのリストを表示します。これらの条件ブロックを現在編集している条件の一部として使用するには、それらを [ライブラリ（Library）] から [エディタ（Editor）] の関連レベルにドラッグ アンド ドロップし、必要に応じて演算子を更新します。 条件は複数のカテゴリに関連付けることができるため、[ライブラリ（Library）] に保存されている条件はすべて [ライブラリ（Library）] アイコン  で表されます。 また、[ライブラリ（Library）] の各条件の横には、iアイコンがあります。このアイコンの上にカーソルを置くと、条件の完全な説明や、関連付けられているカテゴリが表示され、また、ライブラリから条件を完全に削除できます。ポリシーで使用されている条件は削除できません。 ライブラリ条件のいずれかを [エディタ（Editor）] にドラッグ アンド ドロップして、現在編集されているポリシーに単独で使用するか、または現在のポリシーで使用されるさらに複雑な条件の構成要素として使用するか、あるいは [ライブラリ（Library）] に新しい条件として保存します。[エディタ（Editor）] に条件をドラッグ アンド ドロップしてその条件を変更し、[ライブラリ（Library）] に同じ名前または新しい名前で保存することもできます。 インストール時には事前定義された条件もあります。これらの条件は、変更および削除することもできます。

フィールド	使用上のガイドライン
検索およびフィルタ（Search and filter）	名前で条件を検索したり、カテゴリ別にフィルタリングしたりできます。同様に、[エディタ（Editor）] の [クリックして属性を追加する（Click to add an attribute）] フィールドから属性を検索およびフィルタリングすることもできます。ツールバー上のアイコンは、件名や住所などの異なる属性カテゴリを表します。アイコンをクリックすると、特定のカテゴリに関連する属性が表示されます。カテゴリ ツールバーの強調表示されたアイコンをクリックすると、そのカテゴリが選択解除され、フィルタが削除されます。
条件リスト（Conditions List）	[ライブラリ（Library）] 内のすべての条件の完全なリスト、または検索またはフィルタの結果に基づく [ライブラリ（Library）] 内の条件のリスト。
エディタ（Editor）	すぐに使用する新しい条件を作成するだけでなく、今後使用するためにシステム ライブラリに条件を保存したり、既存の条件を編集して、即座に使用したり今後使用するためにその変更を [ライブラリ（Library）] に保存します。 新しい条件を作成するために [条件スタジオ（Conditions Studio）] を開くと（ポリシー セット テーブルのいずれかのプラス記号をクリック）、最初のルールを追加できる空白の行が 1 つだけ表示されます。 [エディタ（Editor）] が空のフィールドとともに表示される場合は、演算子アイコンは表示されません。

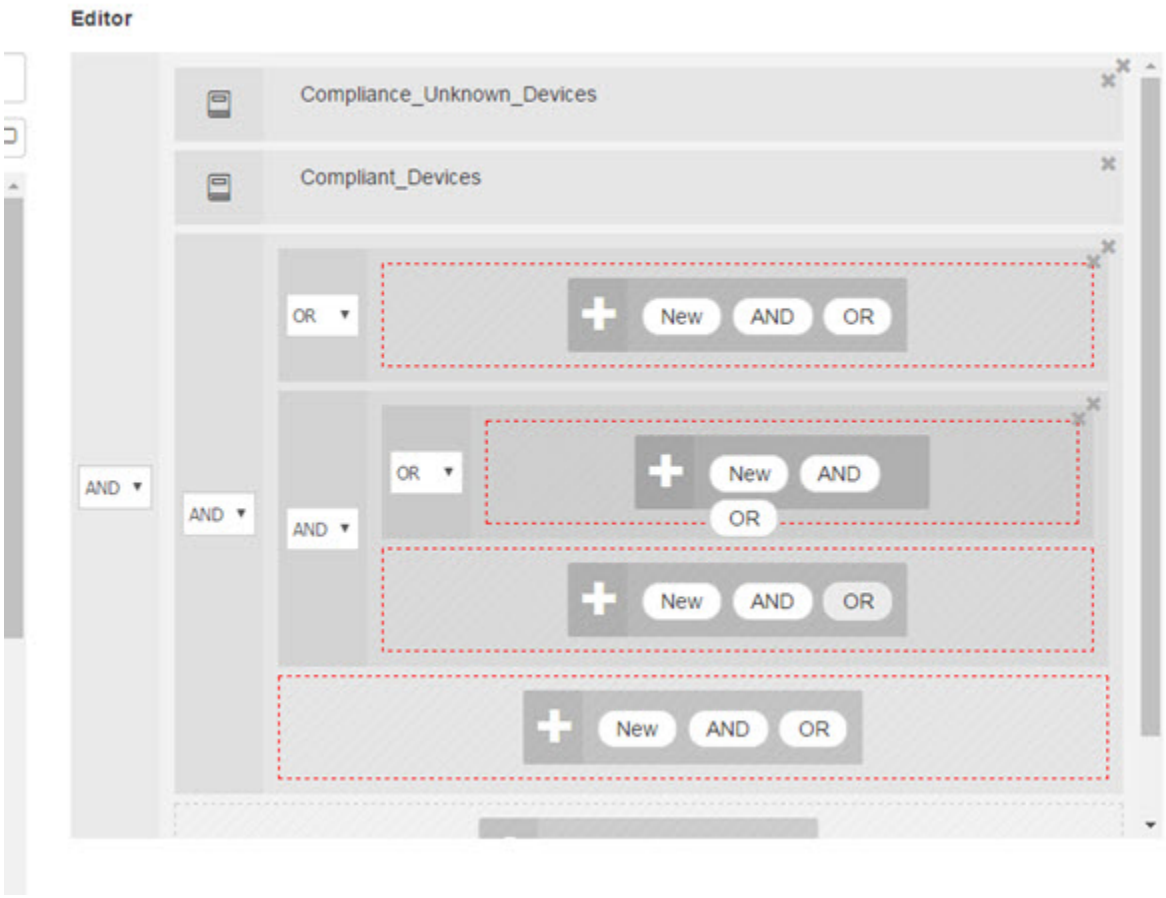
フィールド	使用上のガイドライン
	[エディタ（Editor）] は、さまざまな仮想列と行に分かれています。 列は異なる階層レベルを表し、各列は階層内の位置に基づいてインデントされます。行は個々のルールを表します。レベルごとに 1 つまたは複数のルールを作成し、複数のレベルを含めることができます。 上記のイメージの例は、構築または編集中の条件を示しており、ルールの階層を含んでいます。図の第 1 レベルと第 2 レベルの両方に番号 5 が付けられています。上位親レベルのルールは、演算子 OR を使用します。 演算子を選択して階層レベルを作成した後で演算子を変更するには、この列に表示されているドロップダウンリストから該当するオプションを選択するだけです。 演算子のドロップダウンリストに加えて、各ルールにはこの列に関連するアイコンがあり、そのルールが属するカテゴリが示されています。アイコンの上にカーソルを置くと、ツールチップにカテゴリの名前が示されます。 ライブラリに保存されると、すべての条件ブロックに [ライブラリ（Library）] アイコンが割り当てられ、[エディタ（Editor）] に表示されたカテゴリ アイコンが置き換えられます。 最後に、関連するすべての一致項目を**除外する**ルールが設定されている場合、Is-Not インジケータもこの列に表示されます。たとえば、London という値を持つロケーション属性が Is-Not に設定されている場合、ロンドンからのすべてのデバイスはアクセスが拒否されます。

フィールド	使用上のガイドライン
	この領域には、階層レベルで作業するときに使用できるオプションと、条件内の複数のルールが表示されます。 任意の列または行にカーソルを置くと、関連するアクションが表示されます。アクションを選択すると、そのアクションがそのセクションとすべての子セクションに適用されます。たとえば、階層 A の 5 つのレベルで、第 3 レベルの任意のルールから AND を選択すると、元のルールの下に新しい階層 B が作成され、元のルールが階層 B の親ルールになるように階層 A に埋め込まれます。 新しい条件を最初から作成するために [条件スタジオ（Condition Studio）] を最初に開くと、[エディタ（Editor）] 領域には、設定可能な単一ルールの 1 行のみと、関連する演算子を選択するオプション、または関連条件を [ライブラリ（Library）] からドラッグ アンド ドロップするオプションが含まれています。 **AND** および **OR** 演算子オプションを使用して、条件にレベルを追加できます。オプションをクリックしたときと同じレベルで新しいルールを作成するには、[新規（New）] を選択します。[新規（New）] オプションは、階層の最上位レベルに少なくとも 1 つのルールを設定した場合にのみ表示されます。

ポリシー条件の設定、編集および管理

[条件スタジオ（Conditions Studio）] は、条件の作成、管理、および再利用に使用します。条件には複数のルールを含めることができ、1 つのみのレベルまたは複数の階層レベルを含む任意の複雑度で構築できます。次の図のように、[条件スタジオ（Conditions Studio）] の [エディタ（Editor）] 側から条件階層を管理します。

図 *59 : [*エディタ（*Editor*）*]* : 条件階層



新しい条件を作成する場合は、[ライブラリ（Library）]にすでに保存している条件ブロックを使用することができ、それらの保存された条件ブロックを更新および変更することもできます。条件を作成および管理する際に、クイック カテゴリ フィルタなどを使用して、必要なブロックと属性を簡単に見つけることができます。

条件ルールを作成および管理する場合は、属性、演算子、および値を使用します。

Cisco ISE には、最も一般的な使用例の一部に関する事前定義された条件ブロックも含まれています。これらの事前定義された条件を要件に合わせて編集できます。設定済みブロックを含む、再使用のために保存された条件は、このタスクで説明するように、[条件スタジオ（Conditions Studio）] の [ライブラリ（Library）] に保存されます。

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]**

ステップ 2 [条件スタジオ（Conditions Studio）] にアクセスして新しい条件を作成したり、既存の条件ブロックを編集して、特定のポリシー セット（および関連するポリシーとルール）のために設定したルールの一部としてそれらの条件を使用したり、今後使用するために [ライブラリ（Library）] に保存します。

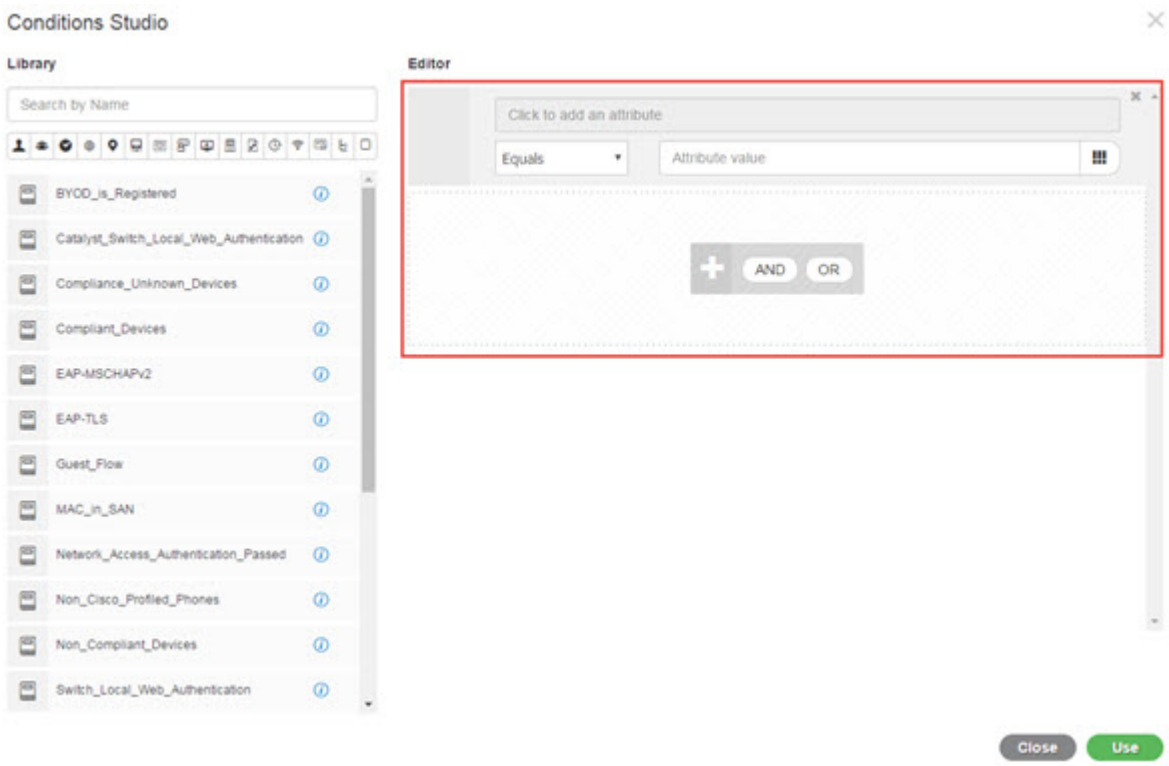
a) ポリシー セット全体（認証ポリシー ルールに照合する前にチェックされる条件）に関連する条件を作成するには、メインの [ポリシー セット（Policy Set）] ページで [ポリシー セット（Policy Set）] テーブルの [条件（Conditions）] 列から ✚ をクリックします。

b) または、認証および許可のすべてのルールを含む [設定（Set）] ビューを表示するには、特定のポリシー セットの行から › をクリックします。[設定（Set）] ビューから、ルールの表のいずれかの [条件（Conditions）] 列のセルにカーソルを合わせ、✚ をクリックして [条件スタジオ（Conditions Studio）] を開きます。

c) すでにポリシー セットに適用されている条件を編集する場合は、✎ をクリックして [条件スタジオ（Conditions Studio）] にアクセスします。

[条件スタジオ（Conditions Studio）] が開きます。新しい条件を作成するために開いた場合は、次の画像のように表示されます。フィールドの説明と、ポリシー セットに既に適用されている条件を編集するために開いた場合の [条件スタジオ（Conditions Studio）] の例を参照するには、[条件スタジオ（Conditions Studio）] の操作 （1502 ページ） を参照してください。

図 *60 : [条件スタジオ（Conditions Studio）]*：新しい条件の作成



ステップ 3 [ライブラリ（Library）] からの既存の条件ブロックを、作成または編集している条件のルールとして使用します。

a) [ライブラリ（Library）] のカテゴリ ツールバーから関連するカテゴリを選択してフィルタリングすると、選択したカテゴリの属性を含むすべてのブロックが表示されます。複数のルールを含むが、それらのルールの少なくとも 1 つに対して選択したカテゴリの属性を使用している条件ブロックも表示されます。追加のフィルタが追加されている場合、表示される結果には、特定のフィルタからの条件ブロックのみが含まれ、含まれている他のフィルタも照合されます。たとえば、ツールバーから [ポート（Ports）] カテゴリを選択し、[名前で検索（Search by Name）] フィールドにフリー テキストとして「auth」と入力すると、名前に「auth」が含まれているポートに関連するすべてのブロックが表示されます。カテゴリ ツールバーの強調表示されたアイコンを再度クリックすると選択解除され、そのフィルタが削除されます。

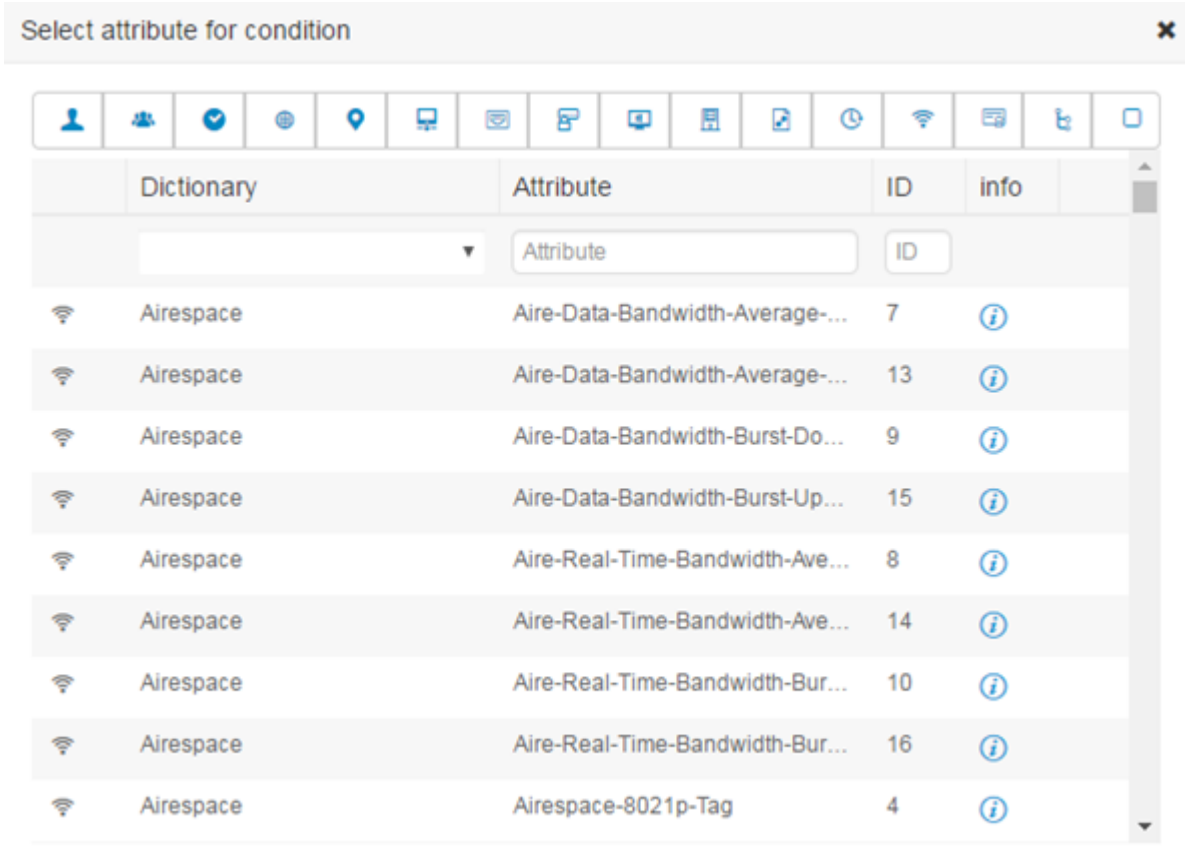
b) フリーテキストで条件ブロックを検索するには、検索しているブロックの名前に表示される [名前で検索（Search by Name）] フリー テキスト フィールドに、任意の用語または用語の一部を入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。カテゴリが選択されていない場合（いずれのアイコンも強調表示されていない場合）、結果にはすべてのカテゴリの条件ブロックが含まれます。カテゴリ アイコンがすでに選択されている場合（表示されているリストがすでにフィルタされている場合）、表示される結果には、特定のテキストを使用する特定のカテゴリのブロックのみが含まれます。

c) 条件ブロックを見つけたら、それを [エディタ（Editor）] にドラッグし、作成しているブロックの正しいレベルにドロップします。間違った場所にドロップした場合は、正しく配置されるまで [エディタ（Editor）] 内から再度ドラッグ アンド ドロップできます。

d) 作業中の条件に関連する変更を加えるには、[エディタ（Editor）] からブロックにカーソルを合わせ、[編集（Edit）] をクリックしてルールを変更し、[ライブラリ（Library）] のルールをその変更で上書きしたり、ルールを新しいブロックとして [ライブラリ（Library）] に保存します。
[エディタ（Editor）] にドロップされたときに読み込み専用であったブロックを編集できるようになりました。そのブロックには、[エディタ（Editor）] 内の他のすべてのカスタマイズされたルールと同じフィールド、構造、リスト、アクションがあります。このルールの編集の詳細については、次の手順に進みます。

ステップ 4 同じレベルでルールを追加するには、現在のレベルに演算子を追加します。[AND]、[OR]、または ['Is not' に設定（Set to 'Is not'）] を選択します。['Is not' に設定（Set to 'Is not'）] は、個々のルールにも適用できます。

ステップ 5 属性ディクショナリを使用してルールを作成および編集するには、[クリックして属性を追加する（Click to add an attribute）] フィールドをクリックします。次の画像のように、属性セレクタが開きます。



属性セレクタの要素を次の表で説明します。

フィールド	使用上のガイドライン
[属性カテゴリ（Attribute Category）] ツールバー	異なる属性カテゴリごとに固有のアイコンが含まれています。カテゴリ別に表示をフィルタ処理するには任意の属性カテゴリ アイコンを選択します。 強調表示されたアイコンをクリックすると選択解除され、フィルタが削除されます。
ディクショナリ（Dictionary）	属性が格納されているディクショナリの名前を示します。ベンダー ディクショナリ別に属性をフィルタリングするには、ドロップダウンから特定のディクショナリを選択します。
属性（Attribute）	属性の名前を示します。属性をフィルタリングするには、使用可能なフィールドに属性名のフリー テキストを入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。

フィールド	使用上のガイドライン
ID	一意の属性 ID 番号を示します。属性をフィルタリングするには、使用可能なフィールドに ID 番号を入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。
情報（Info）	属性に関する詳細を表示するには、関連する属性の行にある情報アイコンの上にカーソルを置きます。

a) 属性セレクタ検索で、必要な属性をフィルタリングして検索します。属性セレクタの任意の部分でフリー テキストをフィルタリングまたは入力すると、他のフィルタがアクティブ化されていない場合、結果には選択されたフィルタのみに関連するすべての属性が含まれます。複数のフィルタを使用すると、表示される検索結果はすべてのフィルタに一致します。たとえば、ツールバーの [ポート（Port）] アイコンをクリックし、[属性（Attribute）] 列に「auth」と入力すると、名前に「auth」が含まれる [ポート（Ports）] カテゴリの属性のみが表示されます。カテゴリを選択すると、ツールバーのアイコンが青色で強調表示され、フィルタリングされたリストが表示されます。カテゴリ ツールバーの強調表示されたアイコンを再度クリックすると選択解除され、そのフィルタが削除されます。

b) 関連する属性をルールに追加するには、その属性を選択します。
属性セレクタが閉じ、選択した属性が [クリックして属性を追加する（Click to add an attribute）] フィールドに追加されます。

c) [等しい（Equals）] ドロップダウンリストから、関連する演算子を選択します。

選択するすべての属性に「Equals」、「Not Equals」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現（REGEX）をサポートし、使用します。

単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数値属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。

d) [属性値（Attribute value）] フィールドから、次のいずれかを実行します。

- フィールドにフリー テキスト値を入力します。
- リストから動的にロードする値を選択します（関連する場合は、前の手順で選択した属性によって異なります）。
- 条件ルールの値として別の属性を使用します。フィールドの横にあるテーブル アイコンを選択して、属性セレクタを開き、関連する属性を検索、フィルタリング、および選択します。属性セレクタが閉じ、選択した属性が [属性値（Attribute value）] フィールドに追加されます。

ステップ 6 条件ブロックとして [ライブラリ（Library）] にルールを保存します。

a) [ライブラリ（Library）] にブロックとして保存するルールまたはルールの階層の上にマウス カーソルを置きます。[重複（Duplicate）] ボタンと [保存（Save）] ボタンは、単一の条件ブロックとして保存できるルールまたはルールのグループに対して表示されます。ルールのグループをブロックとし

て保存する場合は、階層全体のブロックされた領域内の階層全体の下部からアクション ボタンを選択します。

b) [保存（Save）] をクリックします。[保存（Save）] 条件画面が表示されます。

c) 次のどちらかを選択します。

- [既存のライブラリ条件に保存（Save to Existing Library Condition）] : [ライブラリ（Library）] 内の既存の条件ブロックを作成した新しいルールで上書きし、[リストから選択（Select from list）] ドロップダウンリストから上書きする条件ブロックを選択するには、このオプションを選択します。
- [新しいライブラリ条件として保存（Save as a new Library Condition）] : [条件名（Condition Name）] フィールドにブロックの一意の名前を入力します。

d) 必要に応じて、[説明（Description）] フィールドに説明を入力します。この説明は、[ライブラリ（Library）]内の任意の条件ブロックの情報アイコン上にマウスを置いた場合に表示され、さまざまな条件ブロックとその用途をすばやく識別できます。

e) [保存（Save）] をクリックして、条件ブロックを [ライブラリ（Library）] に保存します。

ステップ 7 新しい子レベルに新しいルールを作成するには、[AND] または [OR] をクリックして、既存の親階層と作成している子階層の間に正しい演算子を適用します。選択した演算子を使用して、演算子を選択したルールまたは階層の子として、エディタ階層に新しいセクションが追加されます。

ステップ 8 現在の既存のレベルで新しいルールを作成するには、該当するレベルから [新規（New）] をクリックします。新しいルールの新しい空の行が、開始したレベルと同じレベルで表示されます。

ステップ 9 [X] をクリックして、[エディタ（Editor）] とそのすべての子から条件を削除します。

ステップ 10 [重複（Duplicate）] をクリックすると、階層内の特定の条件が自動的にコピー アンド ペーストされ、同じレベルで追加の同一の子が作成されます。[重複（Duplicate）]ボタンをクリックしたレベルに応じて、子の有無にかかわらず個々のルールを複製できます。

ステップ 11 ページ下部の [使用（Use）] をクリックして、[エディタ（Editor）] で作成した条件を保存し、その条件をポリシー セットに実装します。

（注） いずれかのポリシーセットで AD 属性が必要な場合は、対応する AD 条件を設定する必要があります。

特別なネットワーク アクセス条件

この項では、ポリシーセットを作成するときに役立つ固有条件について説明します。これらの条件は、[条件スタジオ（Conditions Studio）]から作成することはできず、独自のプロセスがあります。

デバイス ネットワーク条件の設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [デバイスポートネットワーク条件（Device Port Network Conditions）]**

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IPアドレス（IP Addresses）：IP アドレスまたはサブネットの一覧を、1 行に 1 つ追加できます。IP アドレス/サブネットは IPv4 または Ipv6 形式で指定できます。
- デバイス名（Device Name）：デバイス名の一覧を、1 行に 1 つ追加することができます。ネットワーク デバイス オブジェクトで設定されているものと同じデバイス名を入力する必要があります。
- デバイスグループ（Device Groups）：ルート NDG、カンマ、（ルート NDG 配下の）NDG の順でタプル一覧を追加できます。タプルは、1 行に 1 つにする必要があります。

ステップ 5 [送信（Submit）] をクリックします。

デバイス ポート ネットワーク条件の設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [デバイス ポート ネットワーク条件（Device Port Network Conditions）]**

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IPアドレス（IP Addresses）：次の順序で詳細を入力します。IP アドレスまたはサブネット、カンマ、（デバイスによって使用される）ポート。タプルは、1 行に 1 つにする必要があります。
- デバイス（Devices）：次の順序で詳細を入力します。デバイス名、カンマ、ポート。タプルは、1 行に 1 つにする必要があります。ネットワーク デバイス オブジェクトで設定されているものと同じデバイス名を入力する必要があります。
- デバイスグループ（Device Groups）：次の順序で詳細を入力します。ルート NDG、カンマ、（ルート下の）NDG、ポート。タプルは、1 行に 1 つにする必要があります。

ステップ 5 [送信（Submit）] をクリックします。

エンドステーション ネットワーク条件の設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [エンドステーションネットワーク条件（Endstation Network Conditions）] の順に選択します。**

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IPアドレス（IP Addresses）：IP アドレスまたはサブネットの一覧を、1 行に 1 つ追加できます。IP アドレス/サブネットは IPv4 または Ipv6 形式で指定できます。
- MAC アドレス：カンマ区切りのエンドステーション MAC アドレスと宛先 MAC アドレスの一覧を入力できます。各 MAC アドレスには 12 桁の 16 進数を含め、次の形式のいずれかで指定してください。nn:nn:nn:nn:nn:nn、nn-nn-nn-nn-nn-nn、nnnn.nnnn.nnnn、nnnnnnnnnnnn。

  エンドステーション MAC または宛先 MAC が必要でない場合は、代わりにトークン「-ANY-」を使用します。
- CLI/DNIS：カンマ区切りの発信者 ID（CLI）および受信者 ID（DNIS）の一覧を追加できます。発信者 ID（CLI）または受信者 ID（DNIS）が必要でない場合は、代わりにトークン「-ANY-」を使用します。

ステップ 5 [送信（Submit）] をクリックします。

時刻と日付の条件の作成

[ポリシー要素条件（Policy Elements Conditions）] ページを使用して、時刻と日付のポリシー要素条件を表示、作成、変更、削除、複製、および検索します。ポリシー要素は、設定した特定の時刻と日付の属性設定に基づく条件を定義する共有オブジェクトです。

時刻と日付の条件を使用すると、Cisco ISE システム リソースにアクセスする権限を、作成した属性設定で指定された特定の時刻と日付に設定または制限できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [共通（Common）] > [時刻と日付（Time and Date）] > [追加（Add）]**。

ステップ 2 フィールドに適切な値を入力します。

- [標準設定（Standard Settings）] 領域で、アクセスを提供する日時を指定します。

• [例外（Exceptions）] 領域で、アクセスを制限する日時の範囲を指定します。

ステップ 3 [送信（Submit）] をクリックします。

許可ポリシーで IPv6 条件属性を使用

Cisco ISE では、エンドポイントからの IPv6 トラフィックを検出、管理、保護できます。

IPv6 対応エンドポイントが Cisco ISE ネットワークに接続すると、IPv6 ネットワーク経由でネットワーク アクセス デバイス（NAD）と通信します。NAD は、アカウンティングおよびプロファイリングの情報をエンドポイント（IPv6 値を含む）から Cisco ISE に IPv4 ネットワークを介して伝達します。ルール条件で IPv6 属性を使用して、IPv6 対応エンドポイントからのそのような要求を処理し、エンドポイントが準拠していることを保証するための、認証プロファイルおよびポリシーを Cisco ISE で設定できます。

ワイルドカード文字は、IPv6 プレフィックスと IPv6 インターフェイスの値で使用できます。たとえば、2001:db8:1234::/48 です。

サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記：コロンで区切られた 4 つの 16 進数桁の 8 つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。
- 短縮表記：1 つのグループ内にある先行ゼロは除きます。ゼロのグループを 2 つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切りの 4 つの表記（IPv4 対応付けおよび IPv4 互換性 IPv6 アドレス）：たとえば、::ffff:192.0.2.128 です。

サポートされている IPv6 属性は次のとおりです。

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address
- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

サポートされるシスコの属性と値のペアおよび対応する IETF 属性を次の表に示します。

シスコの属性と値のペア	IETF 属性
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

[RADIUS ライブログ（RADIUS Live Logs）] ページ、RADIUS 認証レポート、RADIUS アカウンティングレポート、現在アクティブなセッションレポート、RADIUS エラーレポート、設定が誤っている NAS レポート、適応型ネットワーク制御の監査および設定が誤っているサプリカントレポートは、IPv6 アドレスをサポートしています。[RADIUS ライブログ（RADIUS Live Logs）] ページ、またはこれらのレポートのいずれかから、これらのセッションの詳細を表示できます。IPv4、IPv6、または MAC アドレスでレコードをフィルタリングできます。

（注） IPv6 対応の DHCPv6 ネットワークに Android デバイスを接続すると、そのデバイスは DHCP サーバーからリンクローカルの IPv6 アドレスのみを受信します。したがって、[ライブログ（Live Log）] と [エンドポイント（Endpoints）] ページ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]**）にはグローバル IPv6 アドレスは表示されません。

次の手順は、許可ポリシーに IPv6 属性を設定する方法を説明します。

始める前に

展開内の NAD が IPv6 による AAA をサポートしていることを確認します。NAD で IPv6 の AAA サポートをイネーブルにする方法については、『**AAA Support for IPv6**』を参照してください。

ステップ 1 ネットワーク アクセス ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

ステップ 2 許可ルールを作成します。

ステップ 3 許可ルールを作成するときは、[条件スタジオ（Conditions Studio）] から条件を作成します。[条件スタジオ（Conditions Studio）] で、RADIUS ディクショナリから、RADIUS IPv6 属性、演算子、および値を選択します。

ステップ 4 **[保存（Save）]** をクリックして、許可ルールをポリシーセットに保存します。

ポリシー セット プロトコルの設定

これらのプロトコルを使用してポリシー セットを作成、保存、実装する前に、Cisco ISE でグローバル プロトコル設定を定義する必要があります。[プロトコル設定（Protocol Settings）] ページを使用して、ネットワーク内の他のデバイスと通信する Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）、Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）、および Protected Extensible Authentication Protocol（PEAP）の各プロトコルのグローバル オプションを定義できます。

サポートされているネットワーク アクセス ポリシー セット プロトコル

ネットワーク アクセス ポリシー セット ポリシーの定義時に選択可能なプロトコルを次に示します。

- Password Authentication Protocol（PAP）
- Protected Extensible Authentication Protocol（PEAP）
- Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）
- Extensible Authentication Protocol-Message Digest 5（EAP-MD5）
- Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）
- Extensible Authentication Protocol-Tunneled Transport Layer Security（EAP-TTLS; 拡張認証プロトコル - トンネル方式トランスポート層セキュリティ）
- Protected Extensible Authentication Protocol-Transport Layer Security（PEAP-TLS）

プロトコルとして EAP-FAST を使用するためのガイドライン

EAP-FAST を認証プロトコルとして使用する場合は、次のガイドラインに従ってください。

- EAP-FAST 受信クライアント証明書が認証されたプロビジョニングで有効な場合は、EAP-TLS 内部方式を有効にすることを強く推奨します。認証されたプロビジョニングの EAP-FAST 受信クライアント証明書は別の認証方式ではなく、ユーザーを認証するのと同じ証明書のクレデンシャルのタイプを使用した略式のクライアント証明書認証ですが、内部方式を実行する必要がありません。

- PAC なしの完全なハンドシェイクおよび認定 PAC プロビジョニングとの認証プロビジョニング作業に対するクライアント証明書を受け入れます。PACなしのセッション再開、匿名 PAC プロビジョニング、PAC ベース認証には動作しません。
- EAP 属性は、認証の順序とは関係なく、ID ごとにモニタリング ツールの認証詳細に、まずユーザー順、次にマシン順に表示されます（したがって EAP チェーニングは 2 回表示されます）。
- EAP-FAST 認可 PAC が使用される場合、ライブ ログに表示される EAP 認証方式は完全認証に使用される認証方式と同じ（PEAPでのように）であり、参照としてではありません。
- EAP チェーン モードでは、トンネル PAC が期限切れになると、ISE がプロビジョニングにフォールバックし、AC 要求ユーザーおよびマシン認可 PAC（マシン許可 PAC）はプロビジョニングできません。後続の PAC ベースの認証通信で AC が要求したときにプロビジョニングされます。
- Cisco ISE がチェーンに、AC がシングル モードに設定されている場合は、AC は IdentityType TLV で ISE に応答します。ただし、2 番目の ID 認証は失敗します。この通信から、クライアントのチェーニング実行は適切であるが、現在はシングル モードで構成されていることがわかります。
- Cisco ISE は AD にのみチェーンしている EAP-FAST のマシンとユーザーの両方の属性およびグループをサポートします。LDAP および内部 DB ISE に対しては、最新の ID 属性のみを使用します。

（注） High Sierra、Mojave、または Catalina MAC OSX デバイスに EAP-FAST 認証プロトコルを使用すると、「EAP-FAST 暗号化バインドの検証に失敗しました（EAP-FAST cryptobinding verification failed）」というメッセージが表示される場合があります。これらの MAC OSX デバイスに EAP-FAST を使用する代わりに PEAP または EAP-TLS を使用するよう、[許可プロトコル（Allowed Protocols）] ページの [優先EAPプロトコル（Preferred EAP Protocol）] フィールドを設定することをお勧めします。

EAP-FAST の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [EAP-FAST の設定（EAP-FAST Settings）]** を選択します。

ステップ 2 EAP-FAST プロトコルの定義に必要な詳細を入力します。

ステップ 3 以前に生成されたプライマリキーと PAC をすべて失効させるには、[失効（Revoke）] をクリックします。

ステップ 4 EAP-FAST 設定を保存するには、[保存（Save）] をクリックします。

EAP-FAST の PAC の生成

Cisco ISE の [PAC の生成（Generate PAC）] オプションを使用して、EAP-FAST プロトコルのトンネル PAC またはマシン PAC を生成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）]** を選択します。
ステップ 2 左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。
ステップ 3 **[EAP-FAST] > [PAC の生成（Generate PAC）]** を選択します。
ステップ 4 EAP-FAST プロトコルのマシン PAC を生成する場合に必要な詳細を入力します。
ステップ 5 [PAC の生成（Generate PAC）] をクリックします。

EAP-FAST 設定

次の表に、EAP-FAST、EAP-TLS、およびPEAPプロトコルを設定するために使用できる [プロトコル設定（Protocol Settings）] ウィンドウのフィールドを示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [EAP-FAST 設定（EAP-FAST Settings）]**。

表 *139 : EAP-FAST* の設定

フィールド名	使用上のガイドライン
機関識別情報の説明（Authority Identity Info Description）	クレデンシャルをクライアントに送信する Cisco ISE ノードを説明したわかりやすい文字列を入力します。クライアントは、この文字列をタイプ、長さ、および値（TLV）の Protected Access Credentials（PAC）情報で認識できます。デフォルト値は、Identity Services Engine です。
マスター キー生成期間（Master Key Generation Period）	プライマリキー生成期間を、秒、分、時間、日、または週単位で指定します。値は、1 ～ 2147040000 秒の正の整数である必要があります。デフォルトは 604800 秒で、これは 1 週間と同等です。

フィールド名	使用上のガイドライン
すべてのマスター キーおよび PAC の失効（Revoke all master keys and PACs）	すべてのプライマリキーと PAC を失効させるには、[失効（Revoke）] をクリックします。
PAC なしセッション再開の有効化（Enable PAC-less Session Resume）	PAC ファイルなしで EAP-FAST を使用する場合は、このチェックボックスをオンにします。
PAC なしセッションのタイムアウト（PAC-less Session Timeout）	PAC なしセッションの再開がタイムアウトするまでの時間を秒単位で指定します。デフォルトは 7200 秒です。

関連トピック

ポリシー セット プロトコルの設定 （1518 ページ）
プロトコルとして EAP-FAST を使用するためのガイドライン （1518 ページ）
EAP-FAST の利点 （1584 ページ）
EAP-FAST の設定 （1519 ページ）

PAC の設定

次の表では、[PAC の生成（Generate PAC）] ウィンドウ上のフィールドについて説明します。これらのフィールドを使用して、EAP-FAST 認証用の Protected Access Credentials を設定します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [PAC の生成（Generate PAC）]** です。

表 *140 : EAP-FAST* の *PAC* の生成の設定

フィールド名	使用上のガイドライン
トンネル PAC（Tunnel PAC）	トンネル PAC を生成するには、このオプション ボタンをクリックします。
マシン PAC（Machine PAC）	マシン PAC を生成するには、このオプション ボタンをクリックします。
TrustSec PAC	TrustSec PAC を生成するには、このオプション ボタンをクリックします。

フィールド名	使用上のガイドライン
ID（Identity）	（トンネル PAC およびマシン PAC 用）EAP-FAST プロトコルによって「内部ユーザー名」として示されるユーザー名またはマシン名を指定します。ID 文字列がそのユーザー名と一致しない場合、認証は失敗します。 これは、適応型セキュリティ アプライアンス（ASA）で定義されているホスト名です。ID 文字列は、ASA ホスト名に一致する必要があります。一致しない場合、ASA は生成された PAC ファイルをインポートできません。 TrustSec PAC を生成する場合、[ID（Identity）] フィールドにより TrustSec ネットワーク デバイスのデバイス ID が指定され、EAP-FAST プロトコルによりイニシエータ ID とともに提供されます。ここに入力した ID 文字列がそのデバイス ID に一致しない場合、認証は失敗します。
PAC 存続可能時間（PAC Time To Live）	（トンネル PAC およびマシン PAC 用）PAC の有効期限を指定する値を秒単位で入力します。デフォルトは 604800 秒で、これは 1 週間と同等です。この値は、1 ～ 157680000 秒の正の整数である必要があります。TrustSec PAC に対しては、日、週、月、または年単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。
暗号化キー（Encryption Key）	暗号キーを入力します。キーの長さは 8 ～ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。
期限日（Expiration Date）	（TrustSec PAC のみ）有効期限は、PAC 存続可能時間に基づいて計算されます。

関連トピック

ポリシー セット プロトコルの設定 （1518 ページ）
プロトコルとして EAP-FAST を使用するためのガイドライン （1518 ページ）
EAP-FAST の PAC の生成 （1520 ページ）

認証プロトコルとしての EAP-TTLS の使用

EAP-TTLS は、EAP-TLS プロトコルの機能を拡張する 2 フェーズ プロトコルです。フェーズ 1 では、セキュアなトンネルを構築し、フェーズ 2 で使用するセッション キーを導出し、サーバーとクライアント間で属性および内部方式データを安全にトンネリングします。フェーズ 2 中では、トンネリングされた属性を使用して、多数のさまざまなメカニズムを使用する追加認証を実行できます。

Cisco ISE は、次のようなさまざまな TTLS サプリカントから認証を処理できます。

- Windows 上の Network Access Manager（NAM）
- Windows 8.1 ネイティブ サプリカント
- セキュア W2（MultiOS で JoinNow とも呼ばれます）
- MAC OS X ネイティブ サプリカント
- IOS ネイティブ サプリカント
- Android ベースのネイティブ サプリカント
- Linux WPA サプリカント

（注） 暗号化バインドが必要な場合は、内部方式として EAP-FAST を使用する必要があります。

EAP-TLS の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-TTLS]**

ステップ 2 [EAP-TTLS設定（EAP-TTLS Settings）] ページに必要な詳細を入力します。

ステップ 3 [保存（Save）] をクリックします。

EAP-TTLS 設定

次の表では、[EAP-TTLS 設定（EAP-TTLS Settings）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-TTLS]

表 *141 : EAP-TTLS* 設定

フィールド名	使用上のガイドライン
EAP-TTLSセッションの再開を有効にする（Enable EAP-TTLS Session Resume）	このチェックボックスをオンにすると、Cisco ISE はユーザーが EAP-TTLS 認証のフェーズ 2 で正常に認証された場合に限り、EAP-TTLS 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザーが再接続しようとする場合、元の EAP-TTLS セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、EAP-TTLS のパフォーマンスが向上し、AAA サーバーの負荷が軽減されます。 （注） EAP-TTLS セッションが再開されると、内部方式はスキップされます。
EAP-TTLSセッションタイムアウト（EAP-TTLS Session Timeout）	EAP-TTLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。

関連トピック

ポリシー セット プロトコルの設定 （1518 ページ）
認証プロトコルとしての EAP-TTLS の使用 （1523 ページ）
EAP-TLS の設定 （1523 ページ）

EAP-TLS の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-TLS]** を選択します。

ステップ 2 EAP-TLS プロトコルの定義に必要な詳細を入力します。

ステップ 3 EAP-TLS 設定を保存するには、[保存（Save）] をクリックします。

EAP-TLS 設定

次の表では、EAP-TLS プロトコル設定を行うために使用できる [EAP-TLS 設定（EAP-TLS Settings）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-TLS]**。

表 *142 : EAP-TLS* 設定

フィールド	使用上のガイドライン
EAP-TLSセッションの再開を有効にする（Enable EAP-TLS Session Resume）	完全なEAP-TLS認証に成功したユーザーの簡略化された再認証をサポートする場合にオンにします。この機能により、Secure Sockets Layer（SSL）ハンドシェイクのみでユーザーの再認証が可能となり、証明書の適用が不要になります。EAP-TLS セッションは、タイムアウトしていない限り動作を再開します。
EAP-TLSセッションタイムアウト（EAP-TLS Session Timeout）	EAP-TLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。
ステートレスセッション再開（Stateless Session Resume）	
マスターキー生成期間（Master Key Generation Period）	プライマリキー再生成までの時間を入力します。この値により、プライマリキーがアクティブである期間が決定します。この値は秒、分、時、日数、または週数で入力できます。
取り消し（Revoke）	これまでに生成されたすべてのプライマリキーとチケットをキャンセルするには、[取り消し（Revoke）] をクリックします。このオプションは、セカンダリ ノードでは無効です。

EAP-TLS プロトコルを介した MAC アドレスと GUID によるエンドポイントの再認証の場合、コンテキスト可視性サービスを更新するための 1 秒あたりのトランザクション（TPS）は、1 秒あたり 12 ～ 15 エンドポイントです。

関連トピック

ポリシー セット プロトコルの設定 （1518 ページ）
EAP-TLS の設定 （1524 ページ）

PEAP の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）]** を選択します。
ステップ 2 左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。
ステップ 3 [PEAP] を選択します。
ステップ 4 PEAP プロトコルの定義に必要な詳細を入力します。
ステップ 5 PEAP 設定を保存するには、[保存（Save）] をクリックします。

PEAP 設定

次の表では、PEAP プロトコル設定を行うために使用できる [PEAP 設定（PEAP Settings）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [PEAP]** です。

表 *143 : PEAP* 設定

フィールド名	使用上のガイドライン
PEAP セッションの再開を有効にする（Enable PEAP Session Resume）	このチェックボックスをオンにすると、Cisco ISE はユーザーが PEAP 認証のフェーズ 2 で正常に認証された場合に限り、PEAP 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザーが再接続しようとする場合、元の PEAP セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、PEAP のパフォーマンスが向上し、AAA サーバーの負荷が軽減されます。PEAP セッション再開機能を動作させるには、PEAP セッション タイムアウト値を指定する必要があります。
PEAP セッション タイムアウト（PEAP Session Timeout）	PEAP セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。

フィールド名	使用上のガイドライン
高速再接続を有効にする（**Enable Fast Reconnect**）	このチェックボックスをオンにすると、セッション再開機能が有効な場合に、ユーザー クレデンシャルを確認しないで PEAP セッションが Cisco ISE で再開することが許可されます。

関連トピック

ポリシー セット プロトコルの設定 （1518 ページ）
PEAP の設定 （1526 ページ）
PEAP の使用の利点 （1583 ページ）
PEAP プロトコルでサポートされているサプリカント （1583 ページ）
PEAP プロトコルのフロー （1583 ページ）

RADIUS の設定

認証に失敗、または認証成功のレポートの繰り返しの抑制に失敗したクライアントを検出するように RADIUS 設定を設定することができます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）]** を選択します。

ステップ 2 [設定（Settings）] ナビゲーション ペインで [プロトコル（Protocols）] をクリックします。

ステップ 3 [RADIUS] を選択します。

ステップ 4 RADIUS 設定の定義に必要な詳細を入力します。

ステップ 5 [保存（Save）] をクリックして、設定を保存します。

RADIUS 設定

次の表に、[RADIUS 設定（RADIUS Settings）] ページにある各フィールドの説明を示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS]** です。

[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）] オプションを有効にすると、認証が繰り返し失敗するクライアントは監査ログに出力されず、指定された期間にわたってこれらのクライアントからの要求が自動的に拒否されます。また、認証失敗回数を指定できます。失敗回数がこの回数を超えると、これらのクライアントからの要求は拒否されます。たとえばこの値を 5 に設定すると、クライアント認証が 5 回失敗した場合、指定された期間にわたってそのクライアントから受信する要求はすべて拒否されます。

（注）

- エンドポイント認証失敗の原因が誤ったパスワードの入力であり、ユーザータイプが内部ユーザーである場合、エンドポイントは抑制され、拒否モードになります。ただし、Active Directoryユーザーの場合に誤ったパスワードが検出された場合、エンドポイントは抑制されますが、拒否モードにはなりません。
- Cisco ISE でのクライアント抑制は、クライアントの発信側ステーションアイデンティティに関連付けられた MAC アドレスがある場合にのみ機能します。

[繰り返し失敗したクライアントからのRADIUS要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] 設定で指定された時間が経過すると、エンドポイントの拒否モードが解除されます。

[繰り返し失敗したクライアントからのRADIUS要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] 設定よりも早く拒否されたエンドポイントを解除するには、次の手順を実行します。

- Cisco ISE 管理ポータルで、**[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** ページに移動します。解除するエンドポイントの横にあるチェックボックスをオンにして、エンドポイントテーブルの上部にある [削除（Remove）] をクリックします。
- ERS API PUT /ers/config/endpoint/{id}/releaserejectedendpoint を使用して、エンドポイントを解除します。

（注） RADIUS 障害の抑制を設定すると、RADIUS ログの抑制を設定した後も、「`5440 Endpoint Abandoned EAP Session and started a new one`」というエラーを受信することがあります。詳細については、次の ISE コミュニティの投稿を参照してください。

https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944

表 *144 : RADIUS* 設定

フィールド名	使用上のガイドライン
抑制とレポート（Suppression and Reports）	
繰り返し失敗したクライアントと繰り返されるアカウンティングの抑制（Suppress Repeated Failed Clients and Repeated Accounting）	

フィールド名	使用上のガイドライン
繰り返し失敗したクライアントと繰り返されるアカウンティングの抑制（Suppress Repeated Failed Clients and repeated accounting）	同じ理由で繰り返し認証に失敗するクライアントを抑止するには、このチェックボックスをオンにします。これらのクライアントは監査ログに出力されず、また [繰り返し失敗したクライアントからのRADIUS要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] オプションが有効な場合には、指定された期間にわたってこれらのクライアントからの要求が拒否されます。 （注） CTS 関連のログは、このオプションが有効になっている場合でも抑制されず、常にライブログに含まれます。
2回の失敗を検出する期間（Detect Two Failures Within）	分単位で時間間隔を入力します。クライアントがこの期間内に同じ理由で 2 回認証に失敗すると、監査ログに出力されず、また [繰り返し失敗したクライアントからのRADIUS要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] オプションが有効な場合には、このクライアントからの要求が拒否されます。デフォルト値は 5 分です。有効な範囲は 5 ～ 30 分です。
失敗を報告する間隔（Report Failures Once Every）	報告対象の認証失敗の時間間隔を分単位で入力します。デフォルト値は 15 分です。有効な範囲は 15 ～ 60 分です。 たとえば、この値を 15 分に設定すると、繰り返し認証に失敗するクライアントが 15 分に 1 回だけ監査ログに報告されるため、報告の重複が防止されます。
繰り返し発生するアカウンティング更新を無視する期間（Ignore Repeated Accounting Updates Within）	この期間内に繰り返し発生するアカウンティング更新は無視されます。デフォルト値は300秒です。有効な範囲は 1 ～ 86400 秒です。

フィールド名	使用上のガイドライン
メモ	• [繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）] チェックボックスがオンになっていて、[2回の失敗を検出する期間（Detect Two Failures Within）] フィールドで指定された時間**内**に 2 回の失敗が発生した場合、エンドポイントの設定に誤りがあると見なされます。設定に誤りがあるエンドポイントでは、認証を成功させるために管理者の介入が必要です。エンドポイントが最初の認証に失敗すると、関連情報が管理者のダッシュボードに表示されます。同じ理由の後続の認証失敗には、管理者のための追加情報は含まれません。そのため、[失敗を報告する間隔（Report Failures Once Every）] フィールドで指定された期間中に特定の理由でエンドポイントの認証失敗が繰り返されても、監査ログには報告されません。 [失敗を報告する間隔（Report Failures Once Every）] フィールドで指定された期間が経過した後に、設定に誤りがあるエンドポイントに関する **TotalFailedAttempts** と **TotalFailedTime** の情報がモニタリングノードに報告されます。 • [繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）] チェックボックスがオンになっていて、[2回の失敗を検出する期間（Detect Two Failures Within）] フィールドで指定した時間が経過した後に 2 回の失敗が発生した場合、エンドポイントの失敗した認証試行は、認証失敗の理由が同じであっても、監査ログに別個のインスタンスとして報告されます。 • エンドポイントはさまざまなサプリカントプロファイルを持てるため、Cisco ISE ではエンドポイントがさまざまな失敗理由で複数回連続して失敗することが許容されます。そのため、エンドポイントが異なる失敗理由のために認証に複数回失敗した場合、Cisco ISE は各失敗理由を個別にカウントします。
繰り返し失敗したクライアントからのRADIUS要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）	認証が繰り返し失敗するクライアントからの RADIUS 要求を自動的に拒否するには、このチェックボックスをオンにします。Cisco ISE による不要な処理を防ぎ、Denial of Service（DoS）攻撃から防御するには、このオプションを有効にします。

フィールド名	使用上のガイドライン
メモ	• [繰り返し失敗したクライアントからのRADIUS要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] チェックボックスがオンになっていて、エンドポイントで [自動拒否前の失敗回数（Failures Prior to Automatic Rejection）] フィールドに示されている回数と同じ回数の認証失敗が発生した場合、エンドポイントの設定に誤りがあると見なされて拒否されます。Cisco ISE はこのエンドポイントからの認証要求が含まれている最初の RADIUS メッセージをただちに拒否するため、エンドポイントは認証を完了できません。エンドポイントの監査ログは生成されません。エンドポイントは、[要求を拒否する期間（Continue Rejecting Requests for）] フィールドで指定された期間、拒否されたままになります。エンドポイントは、[要求を拒否する期間（Continue Rejecting Requests for）] で指定された期間が経過した後に認証要求を送信できます。認証が成功すると、エンドポイントが設定されます。 • 拒否されたエンドポイントは、[コンテキストの可視性（Context Visibility）]（**[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]**）ページで表示およびリリースすることができます。拒否されたエンドポイントを選択し、[拒否のリリース（Release Rejected）] をクリックして、拒否されたエンドポイントをリリースします。リリースされたエンドポイントの監査ログがモニタリングノードに送信されます。 • 設定に誤りがあるエンドポイントからのアクティビティが 6 時間ない場合、そのエンドポイントは設定に誤りがあると見なされなくなります。
自動拒否前の失敗回数（Failures Prior to Automatic Rejection）	認証失敗回数を入力します。認証失敗回数がこの値を超えると、繰り返し失敗するクライアントからの要求は自動的に拒否されます。設定されている期間（[要求を拒否する期間（Continue Rejecting Requests for）] で指定）にわたり、これらのクライアントから受信する要求はすべて自動的に拒否されます。この期間が経過した後では、これらのクライアントからの認証要求が処理されます。デフォルト値は 5 です。有効な範囲は 2 ～ 100 です。
要求を拒否する期間（Continue Rejecting Requests for）	繰り返し失敗するクライアントからの要求を拒否する時間間隔を分単位で入力します。デフォルト値は 5 分です。有効な範囲は 5 ～ 180 分です。
成功レポートの抑制（Suppress Successful Reports）	

フィールド名	使用上のガイドライン
繰り返される認証成功の抑制（Suppress Repeated Successful Authentications）	直近の 24 時間で、ID、ネットワーク デバイス、および許可のコンテキストに変更がない認証要求成功が繰り返し報告されないようにするには、このチェックボックスをオンにします。
認証の詳細（Authentications Details）	
次よりも長いステップを強調表示（Highlight Steps Longer Than）	ミリ秒単位で時間間隔を入力します。1つのステップの実行が指定のしきい値を超えると、認証詳細ページでそのステップがクロック アイコンでマークされます。デフォルト値は、1000 ミリ秒です。有効な範囲は 500 ～ 10,000 ミリ秒です。
高レートなRADIUS要求を検出する（Detect High Rate of RADIUS Requests）	
高レートなRadius要求を検出する（Detect High Rate of Radius Requests）	[RADIUS要求の期間（Duration of RADIUS requests）] および [RADIUS要求の合計数（Total number of RADIUS requests）] フィールドで指定した上限を超える場合に、高レートな RADIUS 要求負荷のアラームを発生させるには、このチェックボックスをオンにします。
RADIUS要求の期間（Duration of RADIUS Requests）	RADIUS のレートを計算するために使用する期間（秒単位）を入力します。デフォルト値は 60 秒です。有効な範囲は 20 ～ 86400 秒です。
RADIUS要求の合計数（Total Number of RADIUS Requests）	RADIUS のレートを計算するために使用される要求の上限を入力します。デフォルトの要求数は 72000 です。要求数の有効な範囲は 24000 ～ 103680000 で d す。
UDPポート（UDP Ports）	
認証ポート（Authentication Port）	RADIUS UDP の認証フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1812 とポート 1645 が使用されます。値の範囲は 1024 ～ 65535 です。

フィールド名	使用上のガイドライン
アカウンティングポート（Accounting Port）	RADIUS UDP のアカウンティング フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1813 とポート 1646 が使用されます。値の範囲は 1024 ～ 65535 です。 （注） これらのポートが他のサービスにより使用されていないことを確認します。
DTLS	
認証およびアカウンティングポート（Authentication and Accounting Port）	RADIUS DTLS の認証およびアカウンティング フローに使用するポートを指定します。デフォルトでは、ポート 2083 が使用されます。値の範囲は 1024 ～ 65535 です。 （注） このポートが他のサービスにより使用されていないことを確認します。
アイドルタイムアウト（Idle Timeout）	パケットがネットワーク デバイスから届かなかったら、TLS セッションを終了する前に、Cisco ISE を待機する時間を秒単位で入力します。デフォルト値は 120 秒です。有効な範囲は 60 ～ 600 秒です。

フィールド名	使用上のガイドライン
RADIUS/DTLSクライアントID検証の有効化（Enable RADIUS/DTLS Client Identity Verification）	Cisco ISE が DTLS ハンドシェイク中に RADIUS/DTLS クライアントの ID を確認するようにする場合は、このチェックボックスをオンにします。クライアント ID が有効でない場合、Cisco ISE はハンドシェイクに失敗します。デフォルトのネットワーク デバイスが設定されている場合、ID チェックはスキップされます。ID チェックは次の順序で実行されます。 1. クライアント証明書にサブジェクト代替名（SAN）属性が含まれている場合： • SAN に DNS 名が含まれている場合、証明書に指定されている DNS 名が Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。 • SAN に IP アドレスが含まれていて（DNS 名が含まれていない場合）、証明書で指定された IP アドレスが Cisco ISE で設定されているすべてのデバイス IP アドレスと比較されます。 2. 証明書に SAN が含まれていない場合、サブジェクト CN は Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。不一致の場合、Cisco ISE はハンドシェイクに失敗します。

関連トピック

ポリシー セット プロトコルの設定 （1518 ページ）
Cisco ISE の RADIUS プロトコルのサポート （1545 ページ）
RADIUS の設定 （1527 ページ）

セキュリティ設定の構成

始める前に

次の手順を実行して、セキュリティ設定を構成します。

ステップ 1 Cisco ISE GUI で、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[セキュリティ（Security Settings）]**を選択します。

ステップ 2 [TLSバージョン設定（TLS Versions Settings）] セクションで、1 つまたは連続する TLS バージョンの範囲を選択します。有効にする TLS バージョンの横にあるチェックボックスをオンにします。

（注）
- TLS 設定を変更すると、ノードが再起動します。
- TLS 1.2 はデフォルトで有効になっており、無効にすることはできません。複数の TLS バージョンを選択する場合は、連続するバージョンを選択する必要があります。たとえば、TLS 1.0 を選択すると、TLS 1.1 が自動的に有効になります。
- TLS 1.2 は、EAP-TLS が EAP-FAST、TEAP、および PEAP プロトコルの内部方式として使用される場合にサポートされる最新の TLS バージョンです。

- **[TLS 1.0を許可（Allow TLS 1.0）]**：次のワークフローについて、レガシーピアとの通信に TLS 1.0 を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
  - Cisco ISE は、セキュアな ODBC クライアントとして設定されます
  - Cisco ISE は、ERS サーバーとして設定されます

  また、次の Cisco ISE コンポーネントとの通信用に TLS 1.0 を許可します。
  - すべてのポータル
  - 認証局
  - MDM クライアント
  - pxGrid
  - PassiveID エージェント

  （注） セキュリティを強化するために、TLS の後続バージョンを使用するようにクライアントとサーバーでネゴシエートすることをお勧めします。

- **[TLS 1.1を許可（Allow TLS 1.1）]**：次のワークフローについて、レガシーピアとの通信に TLS 1.1 を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます

- Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- Cisco ISE は、セキュアな ODBC クライアントとして設定されます
- Cisco ISE は、ERS サーバーとして設定されます

また、次の Cisco ISE コンポーネントとの通信用に TLS 1.1 を許可します。

- すべてのポータル
- 認証局
- ERS
- MDM クライアント
- pxGrid

（注） セキュリティを強化するために、TLS の後続バージョンを使用するようにクライアントとサーバーでネゴシエートすることをお勧めします。

- **[TLS 1.2を許可（Allow TLS 1.2）]**：次のワークフローについて、レガシーピアとの通信に TLS 1.2 を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
  - Cisco ISE は、セキュアな ODBC クライアントとして設定されます
  - Cisco ISE は、ERS サーバーとして設定されます

  また、次の Cisco ISE コンポーネントとの通信用に TLS 1.2 を許可します。
  - Cisco ISE Admin GUI
  - すべてのポータル
  - 認証局
  - ポート 443 で有効になっている API（Open API、ERS、MnT）
  - MDM クライアント
  - pxGrid

  （注） TLS 1.2 は、TLS を使用するすべての Cisco ISE 機能のデフォルトです。

- **[Allow TLS 1.3]**：次のワークフローについて、ピアとの通信に TLS 1.3 を許可します。
  - Cisco ISE は、EAP-TLS サーバーとして設定されます

- Cisco ISE は、TEAP サーバーとして設定されます

  注目　Cisco ISE リリース 3.4 の時点では、TEAP TLS 1.3 は使用可能なクライアント OS でサポートされていないため、TEAP サーバーとして設定された Cisco ISE の TLS 1.3 サポートは、内部テスト条件下でテストされています。

- Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます

ポート 443 を介した次の管理者 HTTPS アクセスに対して TLS 1.3 を許可します。

- Cisco ISE Admin GUI
- ポート 443 で有効になっている API（Open API、ERS、MnT）

ステップ 3　[暗号方式とセキュリティ設定（Ciphers and Security Settings）] ウィンドウで、次の必須オプションを選択します。

- **[SHA-1暗号方式を許可（Allow SHA-1 Ciphers）]**：次のワークフローでのピアとの通信に SHA-1 暗号方式を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
  - Cisco ISE は、セキュアな ODBC クライアントとして設定されます

  また、次の Cisco ISE コンポーネントとの通信用に SHA-1 暗号化を許可します。

  - 管理アクセス GUI
  - すべてのポータル
  - ERS
  - OpenAPI
  - pxGrid

  上記にリストアップされたコンポーネントの通信には、次のポートが使用されます。

  - 管理者アクセス：443
  - Cisco ISE ポータル：9002、8443、8444、8445、8449
  - ERS：9060、9061、9063
  - pxGrid：8910

（注） [SHA-1暗号方式を許可（Allow SHA-1 Ciphers）] オプションは、デフォルトでは無効になっています。

[SHA-1暗号化を許可（Allow SHA-1 Ciphers）] オプションを有効または無効にした後、展開内のすべてのノードを再起動する必要があります。再起動に失敗すると、設定の変更は適用されません。このようなシナリオでは、次のコマンド（管理 CLI）を使用して、すべてのノードを手動で再起動する必要があります。

application stop ise および **application start ise**。

[SHA-1暗号方式を許可（Allow SHA-1 Ciphers）] オプションが無効になっている場合、SHA-1 暗号方式のみを使用するクライアントがCisco ISEに接続しようとすると、ハンドシェイクが失敗し、クライアントのブラウザにエラーメッセージが表示されます。

レガシーピアとの通信用にSHA-1暗号方式を許可する際、次のオプションのいずれかを選択します。

- **[すべてのSHA-1暗号方式を許可（Allow all SHA-1 Ciphers）]**：レガシーピアとの通信にすべてのSHA-1 暗号方式を許可します。
- **[TLS_RSA_WITH_AES_128_CBC_SHAのみを許可（Allow only TLS_RSA_WITH_AES_128_CBC_SHA）]**：レガシーピアとの通信に、TLS_RSA_WITH_AES_128_CBC_SHA 暗号方式のみを許可します。

（注） セキュリティを強化するために、SHA-256またはSHA-384暗号化を使用することを推奨します。

- **[ECDHE-RSA暗号方式を許可（Allow ECDHE-RSA Ciphers）]**：次のワークフローでのピアとの通信に ECDHE-RSA 暗号方式を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- **[3DES暗号方式を許可（Allow 3DES ciphers）]**：次のワークフローでのピアとの通信に3DES暗号方式を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます

- Cisco ISE は、セキュアな LDAP クライアントとして設定されます

- **[目的の検証なしで証明書を受け入れる（Accept Certificates without Validating Purpose）]**：Cisco ISE が EAP または RADIUS DTLS サーバーとして機能している場合、クライアント証明書は次のことを確認せずに受け入れられます。
  - Key Usage 拡張に、ECDHE-ECDSA 暗号方式の keyAgreement ビットまたは他の暗号方式の keyEncipherment ビットが含まれている
  - Extended Key Usage の属性値は ClientAuth である

  このオプションを無効にすると、Cisco ISE により、すべてのクライアント証明書の目的が検証されます。証明書は、次のいずれかの条件が満たされた場合にのみ有効と見なされます。
  - Extended Key Usage 拡張が存在しない場合：
    - cipherGroup が ECDHE-ECDSA の場合、Key Usage 拡張には KeyAgreement 値が含まれている必要があります。
    - cipherGroup が ECDHE-ECDSA 以外の場合、Key Usage 拡張には keyEncipherment 値と DigitalSignature 値が含まれている必要があります。
  - Extended Key Usage の属性値が ClientAuth の場合：
    - cipherGroup が ECDHE-ECDSA の場合、Key Usage 拡張には KeyAgreement 値が含まれている必要があります。
    - cipherGroup が ECDHE-ECDSA 以外の場合、Key Usage 拡張には keyEncipherment 値と DigitalSignature 値が含まれている必要があります。

  上記の条件のいずれも満たされない場合、証明書の検証は失敗します。
- **[ISEのDSS暗号方式をクライアントとして許可（Allow DSS ciphers for ISE as a client）]**：次のワークフローにおいて、Cisco ISE がクライアントとして機能する場合、サーバーとの通信に DSS 暗号方式を許可します。
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- **[ISEの従来の安全でないTLS再ネゴシエーションをクライアントとして許可（Allow Legacy Unsafe TLS Renegotiation for ISE as a Client）]**：次のワークフローについて、安全な TLS 再ネゴシエーションをサポートしていない従来の TLS サーバーとの通信を許可します。
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます

- Cisco ISE は、セキュアな LDAP クライアントとして設定されます

- **[無効なユーザー名を開示する（Disclose invalid usernamess）]**：デフォルトでは、ユーザー名が正しくないために認証が失敗した場合に、Cisco ISE は `invalid` メッセージを表示します。デバッグをサポートするために、このオプションでは `invalid` メッセージの代わりに、Cisco ISE がレポートにユーザー名を表示するように強制します。ユーザー名が正しくないという理由以外で認証に失敗した場合、ユーザー名は常に表示されることに注意してください。

  この機能は、Active Directory、内部ユーザー、LDAP、および ODBC ID ソースでサポートされます。RADIUS トークン、RSA、または SAML など、他のアイデンティティ送信元ではサポートされません。

- **[サードパーティベンダーとの通信にFQDNベースの証明書を使用する（Use FQDN-based certificates for communication with third party vendors (TC-NAC)）]**：FQDN ベースの証明書は、次のルールに準拠する必要があります。

  - 証明書の SAN および CN フィールドには、FQDN 値が含まれている必要があります。ホスト名とIPアドレスはサポートされません。
  - ワイルドカード証明書には、左端のフラグメントにのみワイルドカード文字が含まれている必要があります。
  - 証明書で提供される FQDN は、DNS で解決可能である必要があります。

- [Show Password in Plaintext]：このオプションを無効にすると、編集中に次のフィールド値の [Show] ボタンが非表示になり、パスワードをプレーンテキストで表示できません。

  - **[管理（Administration）]**>**[ネットワークリソース（Network Resources）]**>**[ネットワークデバイス（Network Devices）]**>**[ネットワークデバイスリスト（Network Devices List）]**>**[編集（Edit）]** ページ：
    - RADIUS共有秘密（RADIUS Shared Secret）
    - RADIUSの2番目の共有秘密（RADIUS Second Shared Secret）
  - **[管理（Administration）]**>**[システム（System）]**>**[設定（Settings）]**>**[プロトコル（Protocols）]**>[IPSec]**[ネイティブ（Native）]**[IPsec]**[編集（Edit）]** ページ：
    - **Pre-shared Key**

  このオプションは、Cisco ISE ではデフォルトで有効になっています。[パスワードをプレーンテキストで表示（Show Password in Plaintext）] オプションが有効になっている場合、いずれかのページで [表示（Show）] ボタンをクリックすると、監査ログが生成され、サーバーの opt/CSCOcpm/logs/localStore/iseLocalStore.log フォルダに保存されます。

ステップ 4 次の Cisco ISE コンポーネント（管理 UI、ERS、OpenAPI、セキュア ODBC、ポータル、および pxGrid）との通信用に暗号方式を手動で設定する場合は、[暗号方式リストの手動設定（Manually Configure Ciphers List）] チェックボックスをオンにします。

許可された暗号方式がすでに選択された状態で暗号方式リストが表示されます。たとえば、[SHA1暗号方式を許可（Allow SHA1 Ciphers）] オプションが有効になっている場合、このリストの SHA1 暗号方式が有効になります。[TLS_RSA_With_AES_128_CBC_SHAのみを許可（Allow Only TLS_RSA_WITH_AES_128_CBC_SHA）] オプションが選択されている場合、このリストのこの SHA1 暗号方式のみが有効になります。[SHA1暗号方式を許可（Allow SHA1 Ciphers）] オプションが無効になっている場合、このリストの SHA1 暗号方式はどれも有効にできません。

（注）
- 無効にする暗号方式リストを編集すると、アプリケーションサーバーがすべての Cisco ISE ノードで再起動します。
- FIPS モードを有効または無効にすると、すべてのノードのアプリケーションサーバーが再起動され、大幅なシステムダウンタイムが発生します。[手動で暗号方式リストを設定（Manually Configure Ciphers List）] オプションを使用して何らかの暗号方式を無効にした場合は、アプリケーションサーバーの再起動後に、無効な暗号方式のリストを確認します。無効な暗号方式リストには、FIPS モードの移行による変更が含まれる場合があります。

ステップ 5 [保存（Save）] をクリックします。

サポートされる暗号スイート

Cisco ISE は、TLS バージョン 1.0、1.1、1.2、および 1.3 をサポートしています。

Cisco ISE リリース 3.3 以降では、TLS 1.3 によるポート 443 を介した管理 HTTPS アクセスで、次の暗号がサポートされています。

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Cisco ISE は、RSA および ECDSA サーバー証明書をサポートしています。次の楕円曲線をサポートしています。

- secp256r1
- secp384r1
- secp521r1

次の表に、サポートされている暗号スイートが表示されています。

暗号スイート	**Cisco ISE が EAP サーバーとして設定されている場合** **Cisco ISE が RADIUS DTLS サーバーとして設定されている場合**	**Cisco ISE が、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードする場合** **Cisco ISE がセキュアな LDAP クライアントとして設定されている場合** **Cisco ISE が CoA の RADIUS DTLS クライアントとして設定されている場合**
TLS 1.0 のサポート	TLS 1.0 が許可されている場合 （DTLS サーバーは DTLS 1.2 のみをサポート） Cisco ISE 2.3 以上では、[TLS 1.0を許可（Allow TLS 1.0）] オプションがデフォルトで無効になっています。このオプションが無効の場合、TLS 1.0 では、TLS ベースの EAP 認証方式（EAP-TLS、EAP-FAST/TLS）および 802.1 X サプリカントがサポートされません。TLS ベースの EAP 認証方式を TLS 1.0 で使用するには、[セキュリティ設定（Security Settings）] ウィンドウの [TLS 1.0 を許可（Allow TLS 1.0）] チェックボックスをオンにします。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [セキュリティ設定（Security Settings）]**。	TLS 1.0 が許可されている場合 （DTLS クライアントは DTLS 1.2 のみをサポート）
TLS 1.1 のサポート	TLS 1.1 が許可されている場合	TLS 1.1 が許可されている場合

ECC DSA 暗号方式		
ECDHE-ECDSA-AES256-GCM-SHA384	はい	はい
ECDHE-ECDSA-AES128-GCM-SHA256	はい	はい
ECDHE-ECDSA-AES256-SHA384	はい	はい
ECDHE-ECDSA-AES128-SHA256	はい	はい
ECDHE-ECDSA-AES256-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
ECDHE-ECDSA-AES128-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
ECC RSA 暗号方式		
ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES256-SHA384	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES128-SHA256	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES256-SHA	ECDHE-RSA/SHA-1 が許可されている場合	ECDHE-RSA/SHA-1 が許可されている場合
ECDHE-RSA-AES128-SHA	ECDHE-RSA/SHA-1 が許可されている場合	ECDHE-RSA/SHA-1 が許可されている場合
DHE RSA 暗号方式		
DHE-RSA-AES256-SHA256	いいえ	はい
DHE-RSA-AES128-SHA256	いいえ	はい
DHE-RSA-AES256-SHA	いいえ	SHA-1 が許可されている場合
DHE-RSA-AES128-SHA	いいえ	SHA-1 が許可されている場合
RSA 暗号方式		

AES256-SHA256	はい	はい
AES128-SHA256	はい	はい
AES256-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
AES128-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
3DES 暗号方式		
DES-CBC3-SHA	3DES/SHA-1 が許可されている場合	3DES/DSS および SHA-1 が有効になっている場合
DSS 暗号方式		
DHE-DSS-AES256-SHA	いいえ	3DES/DSS および SHA-1 が有効になっている場合
DHE-DSS-AES128-SHA	いいえ	3DES/DSS および SHA-1 が有効になっている場合
EDH-DSS-DES-CBC3-SHA	いいえ	3DES/DSS および SHA-1 が有効になっている場合
弱い RC4 暗号方式		
RC4-SHA	[許可されているプロトコル（Allowed Protocols）] ページで [脆弱な暗号を許可（Allow weak ciphers）] オプションが有効になっていて、SHA-1 が許可されている場合	いいえ
RC4-MD5	[許可されているプロトコル（Allowed Protocols）] ページで [脆弱な暗号を許可（Allow weak ciphers）] オプションが有効になっている場合	いいえ
EAP-FAST 匿名プロビジョニングのみの場合： ADH-AES-128-SHA	はい	いいえ
ピア証明書の制限		

KeyUsage の検証	クライアント証明書では、以下の暗号に対し、KeyUsage=Key Agreement および ExtendedKeyUsage=Client Authentication が必要です。 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
ExtendedKeyUsage の検証	クライアント証明書では、以下の暗号に対し、KeyUsage=Key Encipherment および ExtendedKeyUsage=Client Authentication が必要です。 • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	サーバー証明書では ExtendedKeyUsage=Server Authentication が必要です

Cisco ISE の RADIUS プロトコルのサポート

RADIUS は、クライアント/サーバー プロトコルです。リモート アクセス サーバーは、このプロトコルを使用して中央サーバーと通信してダイヤルインユーザーを認証し、要求されたシステムまたはサービスへのアクセスを許可します。RADIUS を使用すると、すべてのリモート サーバーが共有できる中央データベースでユーザープロファイルを管理できます。このプロトコルはセキュリティを向上させます。また、このプロトコルを使用して、単一の管理ネットワーク ポイントで適用されるポリシーを設定できます。

RADIUS は、Cisco ISE の RADIUS クライアントとしても機能し、リモート RADIUS サーバーへの要求をプロキシ処理します。また、アクティブセッション中に許可変更（CoA）アクティビティを提供します。

Cisco ISE では、RFC 2865 と、その仕様および拡張仕様に記載されているすべての一般的な RADIUS 属性の包括的なサポートに従って、RADIUS プロトコルのフローがサポートされます。Cisco ISE では、Cisco ISE ディクショナリで定義されているベンダーだけを対象に、ベンダー固有属性の解析がサポートされます。

RADIUS インターフェイスでは、RFC 2865 で定義されている次の属性データ型がサポートされます。

- テキスト（Unicode Transformation Format（UTF））
- 文字列（バイナリ）
- アドレス（IP）
- 整数
- 時刻

ISE コミュニティ リソース

Cisco ISE でサポートされるネットワーク アクセス属性については、「ISE Network Access Attributes」を参照してください。

許可されるプロトコル

次の表に、認証中に使用するプロトコルを設定できるようにする [許可されるプロトコル（Allowed Protocols）] ウィンドウのフィールドを示します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）]**。

表 *145 :* 許可されるプロトコル

フィールド名	使用上のガイドライン
[許可されているプロトコル（Allowed Protocols）] > [認証バイパス（Authentication Bypass）]	

フィールド名	使用上のガイドライン
ホスト ルックアップの処理（**Process Host Lookup**）	Cisco ISE がホスト ルックアップ要求を処理できるようにするには、このチェックボックスをオンにします。ホスト ルックアップ要求は、RADIUS Service-Type が 10（Call-Check）に等しく、ユーザー名が Calling-Station-ID に等しい場合は PAP/CHAP プロトコルに対して処理されます。ホスト ルックアップ要求は、Service-Type が 1（Framed）に等しく、ユーザー名が Calling-Station-ID に等しい場合は EAP-MD5 プロトコルに対して処理されます。Cisco ISE でホスト ルックアップ要求を無視し、認証にシステム ユーザー名属性の元の値を使用するには、このチェックボックスをオフにします。オフにすると、メッセージ処理はプロトコル（たとえばPAP）に従って行われます。 （注） このオプションを無効にすると、既存のMAB認証で障害が発生する可能性があります。
[許可されているプロトコル（Allowed Protocols）] > [認証プロトコル（Authentication Protocols）]	
PAP/ASCII を許可（Allow PAP/ASCII）	このオプションによって、PAP/ASCII が有効になります。PAP は、平文パスワード（つまり暗号化されていないパスワード）を使用する最も安全性の低い認証プロトコルです。
CHAP を許可（Allow CHAP）	このオプションによって、CHAP 認証が有効になります。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。
MS-CHAPv1 を許可（Allow MS-CHAPv1）	MS-CHAPv1 を有効にするには、このチェックボックスをオンにします。
MS-CHAPv2 を許可（Allow MS-CHAPv2）	MS-CHAPv2 を有効にするには、このチェックボックスをオンにします。
EAP-MD5 を許可（Allow EAP-MD5）	EAP ベースの MD5 パスワード ハッシュ認証を有効にするには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
EAP-TLS を許可（Allow EAP-TLS）	

フィールド名	使用上のガイドライン
	EAP-TLS 認証プロトコルを有効にする場合、および EAP-TLS 設定値を設定する場合は、このチェックボックスをオンにします。エンドユーザー クライアントからの EAP Identity 応答で提示されたユーザー ID を Cisco ISE が確認する方法を指定できます。ユーザーIDは、エンドユーザー クライアントによって提示された証明書の情報に照らして確認されます。この比較は、Cisco ISE とエンドユーザー クライアントとの間に EAP-TLS トンネルが確立された後に行われます。 （注） EAP-TLS は、証明書ベースの認証プロトコルです。EAP-TLS 認証が行われるのは、証明書の設定に必要な手順を完了した場合に限られます。 • [期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）]：ユーザーが証明書を更新できるようにする場合は、このチェックボックスをオンにします。このチェックボックスをオンにすると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。 • [ステートレスセッション再開を有効にする（Enable Stateless Session Resume）]：セッション状態をサーバーに保存する必要なしで EAP-TLS セッションを再開できるようにするには、このチェックボックスをオンにします。Cisco ISE では RFC 5077 で記述されているセッション チケット拡張もサポートされます。Cisco ISE はチケットを作成して EAP-TLS クライアントにそのチケットを送信します。クライアントはセッションを再開するためにそのチケットを ISE に提示します。 • [プロアクティブセッションチケット更新（Proactive Session Ticket update）]：セッションチケットが更新される前に経過する必要がある存続可能時間（TTL）の量を示すパーセント値を入力します。たとえば、値に 60 を入力すると、セッション チケットは TTL の 60 パーセントが経過した後で更新されます。 • [セッションチケットの存続時間（Session ticket Time to Live）]：セッションチケットが期限切れになるまでの時間を入力します。この値は、セッション チケッ

フィールド名	使用上のガイドライン
	トがアクティブである期間を決定します。この値は秒、分、時、日数、または週数で入力できます。
LEAP を許可（Allow LEAP）	Lightweight Extensible Authentication Protocol（LEAP）認証を有効にするには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
PEAP を許可（Allow PEAP）	

フィールド名	使用上のガイドライン
	PEAP 認証プロトコルおよび PEAP 設定値を有効にする場合は、このチェックボックスをオンにします。デフォルトの内部方式は、MS-CHAPv2 です。 [PEAP を許可（Allow PEAP）] チェックボックスをオンにすると、次の PEAP 内部方式を設定できます。 • [EAP-MS-CHAPv2を許可（Allow EAP-MS-CHAPv2）]：内部方式として EAP-MS-CHAPv2 を使用する場合は、このチェックボックスをオンにします。 • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザークレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。 • [EAP-GTCを許可（Allow EAP-GTC）]：内部方式として EAP-GTC を使用する場合は、このチェックボックスをオンにします。 • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザークレデンシャルを要求する回数を指定します。有効範囲は 0 ～ 3 です。 • [EAP-TLSを許可（Allow EAP-TLS）]：内部方式として EAP-TLS を使用する場合は、このチェックボックスをオンにします。 ユーザーによる証明書の更新を許可する場合は、[期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）] チェックボックスをオンにします。このチェックボックスをオンにすると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。 • [暗号化バインドTLVを要求（Require cryptobinding TLV）]：EAP ピアと EAP サーバーの両方が PEAP 認

フィールド名	使用上のガイドライン
	証の内部および外部 EAP 認証に参加する場合、このチェックボックスをオンにします。 • [レガシークライアントにのみPEAPv0を許可（Allow PEAPv0 only for legacy clients）]：PEAP サプリカントがPEAPv0を使用してネゴシエーションできるようにするには、このチェックボックスをオンにします。一部のレガシークライアントはPEAPv1プロトコル規格に準拠しません。そのようなPEAPカンバセーションがドロップされないようにするには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
EAP-FAST を許可（Allow EAP-FAST）	

フィールド名	使用上のガイドライン
	EAP-FAST 認証プロトコルおよびEAP-FAST 設定を有効にする場合は、このチェックボックスをオンにします。EAP-FASTプロトコルは、同じサーバー上の複数の内部プロトコルをサポートできます。デフォルトの内部方式は、MS-CHAPv2 です。 [EAP-FAST を許可（Allow EAP-FAST）] チェックボックスをオンにすると、EAP-FAST を内部方式として設定できます。 • **EAP-MS-CHAPv2 を許可（Allow EAP-MS-CHAPv2）** • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザークレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。 • **EAP-GTC を許可（Allow EAP-GTC）** [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザークレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。 • [PACの使用（Use PACs）]：EAP-FAST クライアントに認可 Protected Access Credentials（PAC）をプロビジョニングするように Cisco ISE を設定する場合にこのオプションを選択します。追加の PAC オプションが表示されます。 • [PACを使用しない（Don’t use PACs）]：トンネルまたはマシン PAC を発行したり受け入れたりしないで EAP-FAST を使用するように Cisco ISE を設定する場合にこのオプションを選択します。PACのすべての要求は無視され、Cisco ISE は PAC を含まない Success-TLV で応答します。 このオプションを選択すると、マシン認証を実行するように Cisco ISE を設定できます。 • [EAP-TLSを許可（Allow EAP-TLS）]：内部方式として EAP-TLS を使用する場合は、このチェックボック

フィールド名	使用上のガイドライン
	スをオンにします。 ユーザーによる証明書の更新を許可する場合は、[期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）] チェックボックスをオンにします。このチェックボックスをオンにすると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。

フィールド名	使用上のガイドライン
	• [EAPチェーンを有効化（Enable EAP Chaining）]：EAP チェーンを有効にするには、このチェックボックスをオンにします。 EAP チェーンによって、Cisco ISE はユーザー認証とマシン認証の結果を関連付け、EAPChainingResult 属性を使用して適切な許可ポリシーを適用することができます。 EAP チェーンには、クライアント デバイスで EAP チェーンをサポートするサプリカントが必要です。サプリカントで [ユーザー認証およびマシン認証（User and Machine Authentication）] オプションを選択します。 EAP チェーンは、EAP-FAST プロトコル（PAC ベース モードおよび PAC レス モードの両方）を選択するときに使用できます。 PAC ベースの認証では、ユーザー認可 PAC またはマシン認可 PAC のいずれかを使用するか、両方を使用して内部方式をスキップすることができます。 証明書ベースの認証では、（許可されるプロトコル サービスの）EAP-FAST プロトコルに対して [プロビジョニングの受信クライアント証明書（Accept Client Certificate for Provisioning）] オプションが有効な場合、およびエンドポイント（エージェント）がトンネル内のユーザー証明書を送信するように設定されている場合、トンネルの確立中に、ISE が証明書を使用してユーザーを認証し（内部方式はスキップされます）、マシン認証は内部方式によって実行されます。これらのオプションが設定されていない場合、EAP-TLS が内部方式としてユーザー認証に使用されます。 EAP チェーンを有効にした後、許可ポリシーを更新し、NetworkAccess:EapChainingResult 属性を使用して条件を追加し、適切な権限を割り当てます。

フィールド名	使用上のガイドライン

EAP-TTLSを許可（Allow EAP-TTLS）	EAP-TTLSプロトコルを有効にする場合に、このチェックボックスをオンにします。
	
	次の内部方式を設定できます。
	
	• [PAP/ASCIIを許可（Allow PAP/ASCII）]：内部方式としてPAP/ASCIIを使用する場合は、このチェックボックスをオンにします。EAP-TTLS PAPは、トークンおよびOTPベースの認証で使用できます。
	
	• [CHAPを許可（Allow CHAP）]：内部方式としてCHAPを使用する場合は、このチェックボックスをオンにします。CHAPは、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAPは、Microsoft Active Directoryでは使用できません。
	
	• [MS-CHAPv1を許可（Allow MS-CHAPv1）]：内部方式としてMS-CHAPv1を使用する場合は、このチェックボックスをオンにします。
	
	• [MS-CHAPv2を許可（Allow MS-CHAPv2）]：内部方式としてMS-CHAPv2を使用する場合は、このチェックボックスをオンにします。
	
	• [EAP-MD5を許可（Allow EAP-MD5）]：内部方式としてEAP-MD5を使用する場合は、このチェックボックスをオンにします。
	
	• [EAP-MS-CHAPv2を許可（Allow EAP-MS-CHAPv2）]：内部方式としてEAP-MS-CHAPv2を使用する場合は、このチェックボックスをオンにします。
	
	  • [パスワード変更の許可（Allow Password Change）]：Cisco ISEでパスワード変更をサポートする場合は、このチェックボックスをオンにします。
	
	  • [再試行（Retry Attempts）]：Cisco ISEでログイン失敗を返す前にユーザークレデンシャルを要求する回数を指定します。有効な値は0 ～ 3です。

フィールド名	使用上のガイドライン
TEAP を許可（**Allow TEAP**）	

フィールド名	使用上のガイドライン
	Tunnel Extensible Authentication Protocol（TEAP）を有効にしてTEAPを設定するには、このチェックボックスをオンにします。TEAPは、トンネルを確立するためにTransport Layer Security（TLS）プロトコルを使用して、サーバーとピア間のセキュアな通信を可能にする、トンネルベースのEAP方式です。TEAPトンネル内では、EAPピアとEAPサーバー間の認証関連データを伝送するために、Type-Length-Value（TLV）オブジェクトが使用されます。 TEAPに次の内部方式を設定できます。 • [EAP-MS-CHAPv2を許可（Allow EAP-MS-CHAPv2）]：内部方式としてEAP-MS-CHAPv2を使用する場合は、このチェックボックスをオンにします。 • [パスワード変更の許可（Allow Password Change）]：Cisco ISEでパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行回数（Retries）]：ログイン失敗メッセージを返す前に、Cisco ISEがログイン情報の入力を許可する回数を入力します。有効範囲は0～3です。 • [EAP-TLSを許可（Allow EAP-TLS）]：内部方式としてEAP-TLSを使用する場合は、このチェックボックスをオンにします。 • [期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）]：ユーザーが証明書を更新できるようにする場合は、このチェックボックスをオンにします。このオプションを有効にすると、認証要求をさらに処理する前に証明書が更新されたかどうかを確認するように適切な許可ポリシールールを設定します。 • [MSKへのダウングレードの許可（Allow Downgrade to MSK）]：内部方式が拡張マスターセッションキー（EMSK）をサポートしているが、クライアントデバイスがマスターセッションキー（MSK）のみを提供している場合は、このチェックボックスをオンにします。EMSKはMSKよりも安全ですが、一部のクライアントデバイスではEMSKがサポートされていない

フィールド名	使用上のガイドライン
	可能性があることに注意してください。 • [トンネル確立中のクライアント証明書の承認（Accept Client Certificate during Tunnel Establishment）]：TEAP トンネルの確立時に Cisco ISE がクライアント証明書を要求するようにするには、このチェックボックスをオンにします。証明書が指定されていない場合、Cisco ISE は設定された内部方式を認証に使用します。 • [EAPチェーンを有効化（Enable EAP Chaining）]：EAP チェーンを有効にするには、このチェックボックスをオンにします。EAP チェーンを使用すると、Cisco ISE は、同じ TEAP トンネル内でユーザーとマシンの両方の認証の内部方式を実行できます。これにより、Cisco ISE は認証の結果を関連付け、EAPChainingResult 属性を使用して適切な許可ポリシーを適用することができます。 EAP チェーンを有効にした後、許可ポリシーを更新し、NetworkAccess:EapChainingResult 属性を使用して条件を追加し、適切な権限を割り当てます。 （注） EAP チェーンが有効になっていて、ユーザーとマシンの両方の認証を実行する場合は、ユーザーとマシンの証明書がサプリカントにコピーされていることを確認します。 （注） • Cisco ISE で EAP チェーンが有効になっている場合は、プライマリとセカンダリの両方の認証方式が Microsoft サプリカント用に設定されている必要があります。 • Cisco ISE で EAP チェーンが無効になっている場合は、プライマリの認証方式のみが Microsoft サプリカント用に設定されている必要があります。 • プライマリとセカンダリの両方の認証方式が [なし（None）] に設定されている場合、EAP ネゴシエーションが失敗し、次のメッセージが表示されることがあります。 `Supplicant stopped responding to ISE`

フィールド名	使用上のガイドライン
優先 EAP プロトコル（Preferred EAP protocol）	EAP-FAST、PEAP、LEAP、EAP-TLS、EAP-TTLS、および EAP-MD5 から任意の優先 EAP プロトコルを選択するには、このチェックボックスをオンにします。優先プロトコルを指定しない場合、EAP-TLS がデフォルトで使用されます。
EAP-TLS L ビット（EAP-TLS L-bit）	デフォルトで、ISE からの TLS Change Cipher Spec メッセージと暗号化ハンドシェイクメッセージの長さの含まれるフラグ（L ビットフラグ）を予測するレガシー EAP サプリカントをサポートするには、このチェックボックスをオンにします。 （注） このフラグを必要とするサプリカントに対してのみ、このオプションを有効にします。Windows ネイティブサプリカントは、PEAP、TEAP、EAP-FAST などのトンネル EAP プロトコルでこのフラグをサポートしません。このオプションが有効になっていて、サプリカントがこのオプションをサポートせず、トンネル EAP プロトコルが使用されている場合、ISE は TLS トンネルを確立した後にアプリケーションデータでこのフラグを有効にします。その後、サプリカントは EAP セッションを破棄し、トンネルの内部方式の EAP 認証を完了せず、「エンドポイントが EAP セッションを放棄して新しいセッションを開始しました（Endpoint abandoned EAP session and started new）」という失敗理由で認証が失敗します。
EAP の脆弱な暗号の許可（Allow Weak Ciphers for EAP）	このオプションを有効にすると、レガシー クライアントが脆弱な暗号（RSA_RC4_128_SHA、RSA_RC4_128_MD5 など）を使用してネゴシエートすることができます。レガシー クライアントが脆弱な暗号化だけをサポートしている場合に限り、このオプションを有効にすることを推奨します。 このオプションはデフォルトでは無効になっています。 （注） Cisco ISE は、EDH_RSA_DES_64_CBC_SHA および EDH_DSS_DES_64_CBC_SHA をサポートしていません。

フィールド名	使用上のガイドライン
すべての RADIUS 要求にメッセージ オーセンティケータが必要（Require Message Authenticator for all RADIUS Requests）	このオプションを有効にすると、Cisco ISE は、RADIUS メッセージ オーセンティケータ属性が RADIUS メッセージがあるかどうかを検証します。メッセージオーセンティケータ属性がない場合、RADIUS メッセージは破棄されます。 このオプションを有効にすると、スプーフィングされたアクセス要求メッセージおよび RADIUS メッセージの改ざんに対する保護が提供されます。 RADIUS メッセージオーセンティケータ属性は、RADIUS メッセージ全体の Message Digest 5（MD5）ハッシュです。 （注） EAP はメッセージ オーセンティケータ属性をデフォルトで使用するので、これを有効にする必要はありません。
5G を許可する（Allow 5G）	Cisco ISE での Cisco Private 5G を有効にするには、このチェックボックスをオンにします。 （注） Cisco ISE で 5G as a Service（5GaaS）を有効にする前に、ネットワークに Cisco Private 5G を展開しておく必要があります

関連トピック

TACACS+ デバイス管理を許可された FIPS および非 FIPS モードのプロトコル （797 ページ）
ネットワーク アクセスの許可されるプロトコルの定義 （1577 ページ）

PAC オプション

次の表では、[許可されるプロトコルサービスリスト（Allowed Protocols Services List）] ウィンドウで [PACを使用（Use PAC）] を選択した後のフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）]** です。

表 *146 : PAC* オプション

フィールド名	使用上のガイドライン
PAC を使用（Use PAC）	

フィールド名	使用上のガイドライン
	• [トンネルPACの存続可能時間（Tunnel PAC Time To Live）]：存続可能時間（TTL）の値によって PAC のライフタイムが制限されます。ライフタイム値と単位を指定します。デフォルトは 90 日です。範囲は 1 ～ 1825 日です。 • [プロアクティブPAC更新の条件：<n%>のPAC TTLが残っている場合（Proactive PAC Update When: <n%> of PAC TTL is Left）]：Update 値により、クライアントに有効な PAC が保持されます。Cisco ISE は、最初に認証が成功してから TTL によって設定された有効期限までに更新を開始します。update 値は、TTL の残り時間のパーセンテージです。デフォルトは90% です。 • [匿名インバンドPACプロビジョニングを許可（Allow Anonymous In-band PAC Provisioning）]：Cisco ISE でクライアントとのセキュアな匿名 TLS ハンドシェイクを確立し、クライアントに PAC をプロビジョニングする場合にこのチェックボックスをオンにします。その際、EAP-FAST のフェーズ 0 と EAP-MSCHAPv2 が使用されます。匿名 PAC プロビジョニングを有効にするには、内部方式として EAP-MSCHAPv2 と EAP-GTC の両方を選択する必要があります。 • [認証付きインバンドPACプロビジョニングを許可（Allow Authenticated In-band PAC Provisioning）]：Cisco ISE は SSL サーバー側の認証を使用して、EAP-FAST のフェーズ 0 中にクライアントに PAC をプロビジョニングします。このオプションは匿名プロビジョニングよりもセキュアですが、サーバー証明書および信頼できるルート CA が Cisco ISE にインストールされている必要があります。 このオプションをオンにすると、認証された PAC プロビジョニングの成功後に Access-Accept メッセージをクライアントに返すように Cisco ISE を設定できます。 • [認証されたプロビジョニングの後にサーバーからAccess-Acceptを返す（Server Returns Access Accept After Authenticated Provisioning）]：認証された PAC プロビジョニングの後に Cisco ISE から access-accept パッケージを返す場合にこのチェックボックスをオンにします。 •

フィールド名	使用上のガイドライン
	[マシン認証を許可（Allow Machine Authentication）]：Cisco ISE でエンドユーザークライアントにマシン PAC をプロビジョニングし、（マシンクレデンシャルを持たないエンドユーザークライアントに対して）マシン認証を実行する場合にこのチェックボックスをオンにします。マシン PAC は、要求（インバンド）によって、または管理者（アウトオブバンド）によって、クライアントにプロビジョニングできます。Cisco ISE がエンドユーザークライアントから有効なマシン PAC を受信すると、その PAC からマシン ID の詳細が抽出され、Cisco ISE 外部 ID ソースで確認されます。マシン認証の外部 ID ソースとして Cisco ISE によってサポートされるのは、Active Directory だけです。その詳細が正しいことが確認されると、その後の認証は実行されません。 このオプションをオンにすると、マシン PAC を使用するために受け入れることができる期間の値を入力できます。Cisco ISE は、期限切れのマシン PAC を受け取ると、（エンドユーザー クライアントからの新規マシン PAC 要求を待たずに）エンドユーザー クライアントに新規マシン PAC を自動的に再プロビジョニングします。 • [ステートレスセッション再開の有効化（Enable Stateless Session Resume）]：Cisco ISE で EAP-FAST クライアントに認可 PAC をプロビジョニングし、EAP-FAST のフェーズ 2 をスキップする場合にこのチェックボックスをオンにします（デフォルトはオン）。 このチェックボックスは次の場合にオフにします。 • Cisco ISE が EAP-FAST クライアントに認可 PAC をプロビジョニングしないようにする場合 • EAP-FAST のフェーズ 2 を常に実行する場合 このオプションをオンにすると、ユーザー認可 PAC の認可期間を入力できます。この期間の終了後、PAC は期限切れになります。Cisco ISE は期限切れの認可 PAC を受信すると、EAP-FAST 認証のフェーズ 2 を実行します。

関連トピック

OOB TrustSec PAC （1606 ページ）

EAP-FAST の PAC の生成 （1520 ページ）

RADIUS プロキシ サーバーとして機能する Cisco ISE

Cisco ISE は、RADIUS サーバーおよび RADIUS プロキシ サーバーとして機能できます。プロキシ サーバーとして機能する場合、Cisco ISE はネットワーク アクセス サーバー（NAS）から認証要求およびアカウンティング要求を受信し、これらの要求を外部 RADIUS サーバーに転送します。Cisco ISE は要求の結果を受け取り、NAS に返します。

Cisco ISE は、同時に複数の外部 RADIUS サーバーへのプロキシ サーバーとして動作できます。RADIUS サーバー順序で設定した外部 RADIUS サーバーを使用できます。次に説明する [外部 RADIUS サーバー（External RADIUS Server）] ページには、Cisco ISE で定義した外部 RADIUS サーバーがすべて表示されます。フィルタ オプションを使用して、名前または説明、またはその両方に基づいて特定の RADIUS サーバーを検索することができます。単純な認証ポリシーとルールベースの認証ポリシーの両方で、RADIUS サーバー順序を使用して要求を RADIUS サーバーにプロキシできます。

RADIUS サーバー順序は、RADIUS-Username 属性からドメイン名を抜き取り（ストリッピング）、RADIUS 認証に使用します。このドメイン ストリッピングは EAP 認証には使用できません。EAP 認証では EAP-Identity 属性が使用されます。RADIUS プロキシ サーバーは RADIUS-Username 属性からユーザー名を取得し、RADIUS サーバー順序の設定時に指定した文字列からユーザー名を抜き取ります。EAP 認証の場合は、RADIUS プロキシ サーバーはユーザー名を EAP-Identity 属性から取得します。RADIUS サーバー順序を使用する EAP 認証は、EAP-Identity 値と RADIUS-Username 値が同一である場合のみ成功します。

外部 RADIUS サーバーの設定

Cisco ISE で外部 RADIUS サーバーを設定して、要求を外部 RADIUS サーバーに送信できるようにする必要があります。タイムアウト時間および接続試行回数を定義できます。

始める前に

- この項で作成した外部 RADIUS サーバーは、それだけでは使用できません。RADIUS サーバー順序を作成して、この項で作成した RADIUS サーバーを使用するように設定する必要があります。これにより、RADIUS サーバー順序を認証ポリシーで使用できるようになります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [外部 RADIUS サーバー（External RADIUS Servers）]** を選択します。

[RADIUS サーバー（RADIUS Servers）] ページが表示され、Cisco ISE で定義された外部 RADIUS サーバーのリストが示されます。

ステップ 2 外部 RADIUS サーバーを追加するには、[追加（Add）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信（Submit）] をクリックして、外部 RADIUS サーバーの設定を保存します。

RADIUS サーバー順序の定義

Cisco ISE の RADIUS サーバー順序を使用すると、NAD からの要求を外部 RADIUS サーバーにプロキシできます。外部 RADIUS サーバーは要求を処理して結果を Cisco ISE に返し、Cisco ISE はその応答を NAD に転送します。

[RADIUS サーバー順序（RADIUS Server Sequences）] ページに、Cisco ISE で定義したすべての RADIUS サーバーの順序が表示されます。このページを使用して、RADIUS サーバーの作成、編集、または複製が可能です。

始める前に

- この手順を開始する前に、プロキシサービスの基本を理解し、関連リンクの最初のエントリのタスクを正常に完了している必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [RADIUS サーバー順序（RADIUS Server Sequences）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信（Submit）] をクリックして、ポリシーに使用する RADIUS サーバー順序を保存します。

TACACS+ プロキシ クライアントとして機能する Cisco ISE

Cisco ISE は、外部 TACACS+ サーバーへのプロキシ クライアントとして機能できます。プロキシ クライアントとして機能する場合、Cisco ISE はネットワーク アクセス サーバー（NAS）から認証要求、許可要求およびアカウンティング要求を受信し、これらの要求を外部 TACACS+ サーバーに転送します。Cisco ISE は要求の結果を受け取り、NAS に返します。

[TACACS+外部サーバー（TACACS+ External Servers）] ページには、Cisco ISE で定義した外部 TACACS+ サーバーがすべて表示されます。フィルタ オプションを使用して、名前または説明、またはその両方に基づいて特定の TACACS+ サーバーを検索することができます。

Cisco ISE は、同時に複数の外部 TACACS+ サーバーへのプロキシ クライアントとして動作できます。複数の外部サーバーを設定するには、[TACACS+サーバーの順序（TACACS+ server

sequence）]ページを使用できます。詳細については、「TACACS+ サーバー順序の設定」ページを参照してください。

外部 TACACS+ サーバーの設定

Cisco ISE で外部 TACACS サーバーを設定して、要求を外部 TACACS サーバーに送信できるようにする必要があります。タイムアウト時間および接続試行回数を定義できます。

始める前に

- この項で作成した外部 TACACS サーバーは、ポリシーに直接使用できません。TACACS サーバー順序を作成して、この項で作成した TACACS サーバーを使用するように設定する必要があります。これにより、TACACS サーバー順序をポリシー セットで使用できるようになります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[TACACS外部サーバー（TACACS External Servers）]** の順に選択します。
[TACACS外部サーバー（TACACS External Servers）] ページが表示され、Cisco ISE で定義された外部 TACACS サーバーのリストが示されます。

ステップ 2 外部 TACACS サーバーを追加するには、[追加（Add）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信（Submit）] をクリックして、外部 TACACS サーバーの設定を保存します。

TACACS+ 外部サーバーの設定

次の表では、[TACACS外部サーバー（TACACS External Servers）] ページのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[TACACS 外部サーバー（TACACS External Servers）]**。

表 *147 : TACACS+* 外部サーバーの設定

フィールド	使用上のガイドライン
名前（Name）	TACACS+ 外部サーバーの名前を入力します。
説明（Description）	TACACS+ 外部サーバー設定の説明を入力します。

フィールド	使用上のガイドライン
ホスト名/アドレス（Host IP）	リモート TACACS+ 外部サーバーの IP アドレス（IPv4 または IPv6 アドレス）を入力します。
接続ポート（Connection Port）	リモート TACACS+ 外部サーバーのポート番号を入力します。ポート番号は 49 です。
タイムアウト（Timeout）	ISE が外部 TACACS+ サーバーからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は 1 ～ 120 です。
共有秘密鍵（Shared Secret）	TACACS+外部サーバーとの接続を保護するのに使用するテキスト文字列。正しく設定されていない場合、接続はTACACS+外部サーバーによって拒否されます。
シングル接続を使用（Use Single Connect）	TACACS プロトコルは、接続にセッションを関連付けるための 2 つのモード、シングル接続と非シングル接続をサポートしています。シングル接続モードは、クライアントが開始する可能性がある多数の TACACS+ セッションに対し、単一の TCP 接続を再使用します。非シングル接続では、クライアントが開始するすべての TACACS+ セッションに対し、新しい TCP 接続が開かれます。TCP 接続は、各セッションの後に閉じられます。 トラフィックが多い環境では、[シングル接続を使用（Use Single Connect）]チェックボックスをオンにし、トラフィックが少ない環境ではオフにできます。

TACACS+ サーバー順序の定義

Cisco ISE の TACACS+ サーバー順序を使用すると、NAD からの要求を外部 TACACS+ サーバーにプロキシできます。外部 TACACS+ サーバーは要求を処理して結果を Cisco ISE に返し、Cisco ISE はその応答を NAD に転送します。[TACACS+サーバー順序（TACACS+ Server Sequences）] ページに、Cisco ISE で定義したすべての TACACS+ サーバーの順序が表示されます。このページを使用して、TACACS+ サーバー順序の作成、編集、または複製が可能です。

始める前に

- プロキシ サービス、Cisco ISE 管理者グループ、アクセス レベル、権限、および制限の基本を理解している必要があります。

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- TACACS+ サーバー順序で使用する外部 TACACS+ サーバーがすでに定義されていることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[TACACS外部サーバー順序（TACACS External Server Sequence）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 必要な値を入力します。

ステップ 4 [送信（Submit）] をクリックして、ポリシーに使用する TACACS+ サーバー順序を保存します。

TACACS+ サーバー順序の設定

次の表では、[TACACSサーバー順序（TACACS Server Sequence）] ページのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[TACACS外部サーバー順序（TACACS External Server Sequence）]**。

表 *148 : TACACS+* サーバー順序の設定

フィールド	使用上のガイドライン
名前（Name）	TACACS プロキシ サーバー順序の名前を入力します。
説明（Description）	TACACS プロキシ サーバー順序の説明を入力します。
サーバー リスト（Server List）	[使用可能（Available）] リストから必要な TACACS プロキシ サーバーを選択します。[使用可能（Available）] リストには、[TACACS外部サービス（TACACS External Services）] ページで設定されている TACACS プロキシ サーバーのリストが含まれています。

フィールド	使用上のガイドライン
ロギング制御（Logging Control）	ロギング制御を有効にするにはオンにします。 • ローカル アカウンティング：アカウンティング メッセージは、デバイスからの要求を処理するサーバーによってログに記録されます。 • リモート アカウンティング：アカウンティング メッセージは、デバイスからの要求を処理するプロキシ サーバーによってログに記録されます。
ユーザー名の除去（Username Stripping）	ユーザー名のプレフィックス/サフィックスの除去 • [プレフィックスの除去（Prefix Strip）]：プレフィックスからユーザー名を取り除く場合にオンにします。たとえば、サブジェクト名が acme\smith、区切り文字が \ の場合、ユーザー名は smith になります。デフォルトの区切り文字は \ です。 • [サフィックスの除去（Suffix Strip）]：サフィックスからユーザー名を取り除く場合にオンにします。たとえば、サブジェクト名が smith@acme.com、区切り文字が @ の場合、ユーザー名は smith になります。デフォルトの区切り文字は @ です。

多要素認証のための Cisco Duo と Cisco ISE の統合

（注） Cisco Duo と Cisco ISE の統合は、制御された導入（ベータ）機能です。この機能を実稼働環境で使用する前に、テスト環境で十分にテストすることを推奨します。

Cisco ISE リリース 3.3 パッチ 1 以降では、多要素認証（MFA）ワークフローの外部 ID ソースとして Cisco Duo を直接統合できます。Cisco ISE の以前のリリースでは、Cisco Duo は外部 RADIUS プロキシサーバーとしてサポートされていましたが、この設定は引き続きサポートされます。

この統合機能を使用すると、Cisco Duo に直接接続できます。次に、MFA 認証ポリシーを作成して、Cisco ISE がプライマリ認証を実行した後のセカンダリ認証のために、エンドポイント認証が Cisco Duo に送信される条件を定義します。

この Cisco Duo 統合では、次の多要素認証のユースケースがサポートされています。

- VPN ユーザー認証
- TACACS+ 管理者アクセス認証

現在、次の認証方式がサポートされています。

- Duo モバイルプッシュ
- 電話

この統合により、Active Directory と Cisco Duo の間でユーザーデータが同期されます。次のデータが Active Directory と Cisco Duo の間で同期され、Active Directory から取得されたデータが Cisco Duo に保存されます。

データ型	Cisco Duo フィールド名	Active Directory フィールド名	値の例
First Name	firstname	givenName	*Test*
Last Name	lastname	sn	*User*
Display Name	realname	displayName	*Test A. User*
Email Address	email	mail	*testuser@example.com*
User Name	username	sAMAccountName	*testuser*

Active Directory と Cisco Duo 間のユーザーデータ同期に関する既知の制限事項：

- グループ名は同期されません。
- 大規模な展開の TACACS+ の場合、サポートされる認証レートは 1 秒あたり 20 認証であり、小規模な展開ではこのレートが低くなります。

  RADIUS プロトコルの認証レートに関する詳細については、『Performance and Scalability Guide for Cisco Identity Services Engine』を参照してください。

始める前に

Cisco Duo を MFA ID ソースとして統合するには、次の前提条件が適用されます。

1. Cisco ISE Advantage ライセンスが必要です。Cisco ISE ライセンスについては、『Cisco ISE Licensing Guide』を参照してください。
2. この統合には、Cisco Duo Essentials、Advantage、または Premier プランが必要です。Cisco Duo プランの詳細については、「Cisco Duo Editions & Pricing」を参照してください。
3. Microsoft Active Directory Domain Services を Cisco ISE と統合し、必要なユーザーグループをインポートします。

4. インターネットとプロキシサーバーの設定を確認して、Cisco ISE が保護された Cisco Duo アプリケーションに到達できることを確認します。
5. OpenAPI を有効にして、アイデンティティ同期ステータスを取得または更新します。

Duo 管理パネルで次の手順を実行します。

1. Cisco ISE Admin API と Cisco ISE Auth API 用の保護されたアプリケーションを作成します。所有者ロールを持つ管理者のみが、Duo Admin Panel で Cisco ISE Admin API アプリケーションを作成または変更できます。
2. Cisco ISE Admin API の [リソースの読み取りを付与（Grant read resource）] 権限と [リソースの書き込みを付与（Grant write resource）] 権限を有効にします。
3. 両方のアプリケーションについて、一意の統合キー（iKey）および秘密キー（sKey）の値と、API ホスト名の値をメモします。これらの値は、Cisco ISE 統合ウィザードで Cisco Duo との接続を設定するために必要です。

ステップ 1 Cisco ISE で Duo 統合を初めて設定する場合は、次の手順を実行します。2 回目以降の Duo 接続の設定は、ステップ 2 から開始します。

1. Cisco ISE 管理ポータルで、**[Administration]** > **[Identity Management]** > **[Settings]** > **[External Identity Management Settings]** の順に選択します。
2. [Multi-Factor Authentication] 領域で [MFA] トグルボタンをクリックして、Cisco ISE でこの機能を有効にします。

ステップ 2 **[Administration]** > **[Identity Management]** > **[External Identity Sources]** > **[MFA]** を選択します。

ステップ 3 [Add] をクリックします。

セットアップウィザードが起動します。

ステップ 4 [Connector Definition] ページで、Duo 接続の名前と説明を入力します。

これは、**[External Identity Sources]** > **[MFA]** ページの MFA 接続のリストに表示される名前です。接続名をクリックすると、Duo の統合が完了した後で、いつでも接続設定を編集できます。

ステップ 5 [Account Configurations] ページで、次の詳細を入力します。

1. API ホスト名
2. Cisco ISE Admin API の iKey および sKey の値
3. Cisco ISE Auth API の iKey および sKey の値

ステップ 6 [Test Connection] をクリックして、Duo アカウントで接続を確立できることを確認します。接続が成功した場合にのみ、次の手順に進むことができます。

ステップ 7 [Next] をクリックします。

ステップ 8 [アイデンティティ同期（Identity Sync）] ページで、同期の名前を入力します。

ここで入力した同期名は、**[外部IDソース（External Identity Sources）]** > **[アイデンティティ同期（Identity Sync）]** ページに表示されます。

Active Directory と Duo 間のユーザーデータ同期を今すぐ設定しない場合は、[スキップ（Skip）] をクリックします。[サマリー（Summary）] ページに直接移動します。

Duo 接続を作成した後は、いつでもアイデンティティ同期設定を追加できます。

ステップ 9 表示される Active Directory 名のリストから、Cisco ISE と Duo 間でデータ同期を設定するディレクトリの横にあるチェックボックスをオンにします。少なくとも 1 つのディレクトリを選択して、次の手順に進みます。

Duo 統合が完了した後は、**[External Identity Sources]** > **[Identity Sync]** ページでいつでも同期の選択を編集できます。

ステップ 10 [Next] をクリックします。

ステップ 11 [ADグループ（AD Groups）] ページで、表示された Active Directory グループのリストから、Cisco ISE と Duo 間のデータ同期を設定するグループの横にあるチェックボックスをオンにします。少なくとも 1 つのグループを選択して、次の手順に進みます。

Duo 統合が完了した後は、**[外部IDソース（External Identity Sources）]** > **[アイデンティティ同期（Identity Sync）]** ページでいつでも AD グループの選択を編集できます。

ステップ 12 [Next] をクリックします。

ステップ 13 [Summary] ページで設定を確認します。[Edit] をクリックして設定を変更し、[Done] をクリックして Duo 統合を保存します。

[Done] をクリックすると、アイデンティティの同期が自動的に開始されます。

次のタスク

Duo アカウントを Cisco ISE に接続した後、エンドポイントの多要素認証を有効にするための MFA ポリシーを作成する必要があります。

- VPN ユーザー認証の場合は、**[Policy]** > **[Policy Sets]** > **[Default]** > **[MFA Policy]** ページで RADIUS 認証ポリシーを作成します。
- TACACS+ 管理者アクセス認証の場合は、 > **[Work Centers]** > **[Device Administration]** > **[Device Admin Policy Sets > Default]** > **[MFA Policy]** ページでデバイス管理ポリシーを作成します。

Duo 接続に関するアクティビティログは、デバッグファイル ise-duo.log で確認できます。

Duo 接続へのアイデンティティ同期の追加

Duo 接続へアイデンティティ同期を追加するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [アイデンティティ同期（Identity Sync）]。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [それでは実行しましょう（Let's Do It）] をクリックします。

[アイデンティティ同期（Identity Sync）] ページが表示されます。

ステップ 4 アイデンティティ同期の名前を入力します。

ステップ 5 [MFA接続（MFA Connection）] ドロップダウンリストから、アイデンティティ同期を設定する Duo 接続を選択します。

ステップ 6 [次へ（Next）] をクリックします。

[Active Directory] ページが表示されます。

ステップ 7 Cisco ISE と Duo 間でデータ同期を設定する Active Directory の横にあるチェックボックスをオンにします。少なくとも 1 つの Active Directory を選択して、次の手順に進みます。

ステップ 8 [次へ（Next）] をクリックします。

[ADグループ（AD Groups）] ページが表示されます。

ステップ 9 Cisco ISE と Duo 間でデータ同期を設定する Active Directory グループの横にあるチェックボックスをオンにします。少なくとも 1 つのグループを選択して、次の手順に進みます。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [サマリー（Summary）] ページで設定を確認します。

[編集（Edit）] をクリックして設定を変更し、[完了（Done）] をクリックして Duo 統合を保存します。

[完了（Done）] をクリックすると、アイデンティティの同期が自動的に開始されます。

設定されたアイデンティティ同期は、[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [MFA] ページで確認できます。

アイデンティティ同期の設定を編集するには、次の手順を実行します。

1. **[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [アイデンティティ同期（Identity Sync）]** の順に選択します。
2. アイデンティティ同期名を選択し、[編集（Edit）] をクリックします。

（注） [アイデンティティ同期（Identity Sync）] ページからアイデンティティ同期を削除すると、対応する Duo 接続も自動的に削除されます。

Cisco ISE と Duo 接続間のデータ同期をトリガーするには、[アイデンティティ同期（Identity Sync）] ページでアイデンティティ同期名を選択し、[同期（Sync）] をクリックします。

ネットワーク アクセス サービス

ネットワーク アクセス サービスには、要求に対する認証ポリシー条件が含まれています。たとえば有線 802.1X や有線 MAB など、さまざまな用途向けに個別のネットワーク アクセス サービスを作成することができます。ネットワーク アクセス サービスを作成するには、許可されているプロトコルまたはサーバー順序を設定します。その後、ネットワーク アクセス ポリシーのネットワーク アクセス サービスが [ポリシー セット（Policy Sets）] ページから構成されます。

ネットワーク アクセスの許可されるプロトコルの定義

許可されるプロトコルは、ネットワーク リソースへのアクセスを要求するデバイスとの通信に Cisco ISE が使用できるプロトコルのセットを定義します。許可されるプロトコル アクセス サービスは、認証ポリシーを設定する前に作成する必要がある独立したエントリです。許可されるプロトコル アクセス サービスは、特定の使用例に対して選択されたプロトコルが含まれているオブジェクトです。

[許可されるプロトコル サービス（Allowed Protocols Services）] ページには、作成した許可されるプロトコル サービスがすべて表示されます。Cisco ISE で事前に定義されたデフォルトのネットワーク アクセス サービスが存在します。

始める前に

この手順を開始する前に、認証に使用するプロトコル サービスの基本を理解している必要があります。

- この章の「Cisco ISE 認証ポリシー」の項を参照して、さまざまなデータベースでサポートされる認証タイプおよびプロトコルについて理解します。
- 「PAC オプション」を確認して、各プロトコル サービスの機能とオプションを理解し、使用しているネットワークに最適な選択ができるようにしてください。
- 手順を進める前に、グローバル プロトコル設定を必ず定義してください。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）]** を選択します。

Cisco ISE が FIPS モードで動作するように設定されている場合は、一部のプロトコルがデフォルトで無効になり、それらのプロトコルを設定できません。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 必要な情報を入力します。

ステップ 4 ネットワークに適切な認証プロトコルとオプションを選択します。

ステップ 5 PAC の使用を選択した場合、適切な選択を行います。

匿名 PAC プロビジョニングを有効にするには、内部方式として EAP-MSCHAPv2 と Extensible Authentication Protocol-Generic Token Card（EAP-GTC）の両方を選択する必要があります。また Cisco ISE では、マシン認証の外部 ID ソースとしては Active Directory だけがサポートされる点に注意してください。

ステップ 6 [送信（Submit）] をクリックして、許可されるプロトコル サービスを保存します。

許可されるプロトコル サービスは、単純な認証ポリシーおよびルールベースの認証ポリシーのページで独立したオブジェクトとして表示されます。このオブジェクトは異なるルールに使用できます。

これで、単純な認証ポリシーおよびルールベースの認証ポリシーを作成できるようになります。

内部方式として EAP-MSCHAP を無効にし、PEAP または EAP-FAST の EAP-GTC と EAP-TLS 内部方式を有効にすると、ISE は内部方式のネゴシエーション中に EAP-GTC 内部方式を開始します。最初の EAP-GTC メッセージがクライアントに送信される前に、ISE は ID 選択のポリシーを実行して、ID ストアから GTC パスワードを取得します。このポリシーの実行中、EAP 認証は EAP-GTC と同じです。EAP-GTC 内部方式がクライアントによって拒否され、EAP-TLS がネゴシエートされても、ID ストア ポリシーが再び実行されることはありません。ID ストア ポリシーが EAP 認証属性に基づいている場合、本当の EAP 認証は EAP-TLS でありながら ID ポリシー評価後に設定されたため、予期しない結果になることがあります。

ユーザーのネットワーク アクセス

ネットワーク アクセスでは、ホストはネットワーク デバイスに接続し、ネットワーク リソースの使用を要求します。ネットワーク デバイスは、新しく接続されたホストを識別し、転送方式として RADIUS プロトコルを使用して、ユーザーの認証および許可を Cisco ISE に要求します。

Cisco ISE では、RADIUS プロトコルを使用して転送されるプロトコルに応じて、ネットワーク アクセス フローがサポートされます。

EAP を使用しない RADIUS ベースのプロトコル

EAP を含まない RADIUS ベースのプロトコルは、次のとおりです。

- Password Authentication Protocol（PAP）
- CHAP
- Microsoft Challenge Handshake Authentication Protocol version 1（MS-CHAPv1）
- MS-CHAP version 2（MS-CHAPv2）

RADIUS-Based Non-EAP 認証フロー

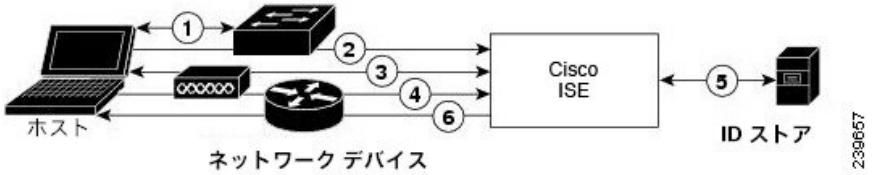
ここでは、EAP 認証を使用しない RADIUS ベースのフローについて説明します。PAP 認証を使用する RADIUS ベースのフローは、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。

2. ネットワーク デバイスが RADIUS 要求（Access-Request）を Cisco ISE に送信します。この要求には、使用する特定のプロトコル（PAP、CHAP、MS-CHAPv1、または MS-CHAPv2）に適した RADIUS 属性が含まれます。
3. Cisco ISE では、ID ストアを使用してユーザー クレデンシャルを検証します。
4. RADIUS 応答（Access-Accept または Access-Reject）が、決定を適用するネットワーク デバイスに送信されます。

次の図は、EAP を使用しない RADIUS ベースの認証を示しています。

図 *61 : EAP* を使用しない *RADIUS* ベースの認証



Cisco ISE でサポートされる非 EAP プロトコルは次のとおりです。

パスワード認証プロトコル

PAP では、ユーザーが双方向ハンドシェイクを使用して ID を確立できる単純な方法が提供されます。PAP パスワードは共有秘密を使用して暗号化されるため、最もセキュリティ レベルの低い認証プロトコルです。PAP は、反復的な試行錯誤攻撃に対する保護がほとんどないため、確実な認証方式ではありません。

Cisco ISE の *RADIUS-Based PAP* 認証

Cisco ISE では、ID ストアに対してユーザー名とパスワードのペアをチェックし、最終的にその認証を確認するか、接続を終了します。

Cisco ISE では、異なるセキュリティ レベルを同時に使用して、さまざまな要件に対応できます。PAP は双方向ハンドシェイク手順を適用します。認証に成功した場合、Cisco ISE は確認応答を返します。認証に失敗した場合、Cisco ISE は接続を終了するか、認証の要求元にもう一度チャンスを与えます。

認証の要求元が、試行の頻度とタイミングを総合的に制御します。したがって、より強力な認証方式を使用できるサーバーは、PAP よりも前にその方式のネゴシエーションを提案します。PAP は RFC 1334 で定義されています。

Cisco ISE では、RADIUS UserPassword 属性に基づく標準の RADIUS PAP 認証がサポートされます。RADIUS PAP 認証は、すべての ID ストアと互換性があります。

PAP 認証フローを使用する RADIUS には、試行の成功と失敗のロギングが含まれます。

チャレンジ ハンドシェイク認証プロトコル

CHAPは、応答時に一方向の暗号化を使用するチャレンジ/レスポンス方式です。CHAPを使用することで、Cisco ISE は、セキュリティ レベルの高い順からセキュリティ暗号化方式をネゴシエートし、プロセス中に伝送されるパスワードを保護します。CHAPパスワードは再利用が可能です。Cisco ISE 内部データベースを認証に使用する場合は、PAP または CHAP のどちらかを使用できます。CHAPは、Microsoftユーザー データベースでは使用できません。RADIUS PAP と比較した場合、エンドユーザー クライアントから AAA クライアントに通信するときに CHAPを使用すると、パスワードが暗号化されるため、高いセキュリティ レベルを確保できます。

Cisco ISE では、RADIUS ChapPassword 属性に基づく標準の RADIUS CHAP 認証がサポートされます。Cisco ISE では、外部 ID ストアを使用した RADIUS CHAP 認証だけがサポートされます。

Microsoft Challenge Handshake Authentication Protocol Version 1

Cisco ISE では、RADIUS MS-CHAPv1 認証およびパスワード変更機能がサポートされます。RADIUS MS-CHAPv1 には、Change-Password-V1 と Change-Password-V2 の 2 つのバージョンのパスワード変更機能が含まれます。Cisco ISE は RADIUS MS-CHAP-CPW-1 属性に基づいた Change-Password-V1 パスワード変更をサポートせず、MS-CHAP-CPW-2 属性に基づいた Change-Password-V2 のみをサポートします。RADIUS MS-CHAPv1 認証およびパスワード変更機能は、次の ID ソースを使用してサポートされます。

- 内部 ID ストア
- Microsoft Active Directory ID ストア

Microsoft Challenge Handshake Authentication Protocol Version 2

RADIUS MS-CHAPv2 認証およびパスワード変更機能は、次の ID ソースでサポートされます。

- 内部 ID ストア
- Microsoft Active Directory ID ストア

RADIUS ベースの EAP プロトコル

EAPでは、さまざまな認証タイプをサポートする拡張可能なフレームワークが提供されます。ここでは、Cisco ISE でサポートされる EAP 方式について説明します。次のトピックを扱います。

単純な EAP 方式

- EAP-Message Digest 5
- Lightweight EAP

認証に Cisco ISE サーバー証明書を使用する EAP 方式

- PEAP/EAP-MS-CHAPv2

- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

上記にリストした方式とは別に、サーバー認証とクライアント認証の両方に証明書を使用する EAP 方式があります。

RADIUS-Based EAP 認証フロー

認証プロセスで EAP が使用される場合は常に、そのプロセスよりも、具体的にどの EAP 方式（および該当する場合は内部方式）を使用する必要があるかを決定するネゴシエーションフェーズが先行します。EAP ベースの認証は、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが EAP 要求をホストに送信します。
3. ホストは、EAP 応答によって、ネットワーク デバイスに応答します。
4. ネットワーク デバイスは、ホストから受信した EAP 応答を RADIUS Access-Request 内に（EAP-Message RADIUS 属性を使用して）カプセル化し、RADIUS Access-Request を Cisco ISE に送信します。
5. Cisco ISE は、RADIUS パケットから EAP 応答を抽出して新しい EAP 要求を作成し、この EAP 要求を RADIUS Access-Challenge 内に（この場合も EAP-Message RADIUS 属性を使用して）カプセル化し、ネットワーク デバイスに送信します。
6. ネットワーク デバイスは、EAP 要求を抽出し、ホストへ送信します。

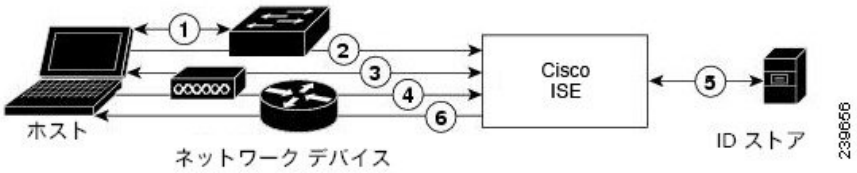
この方法で、ホストと Cisco ISE は間接的に EAP メッセージを交換します（EAP メッセージは、RADIUS を使用して転送され、ネットワーク デバイスを介して渡されます）。この方法で交換される EAP メッセージの最初のセットによって、特定の EAP 方式がネゴシエートされます。その後、認証を実行する場合に、この EAP 方式が使用されます。

その後交換される EAP メッセージは、実際の認証の実行に必要なデータを伝送するために使用されます。ネゴシエートされた特定の EAP 認証方式で必要な場合、Cisco ISE では ID ストアを使用してユーザー クレデンシャルを検証します。

Cisco ISE では、認証が成功か失敗かを決定した後、EAP-Success または EAP-Failure メッセージを、RADIUS Access-Accept または Access-Reject メッセージ内にカプセル化された状態で、ネットワーク デバイスに（最終的にはホストにも）送信します。

次の図は、EAP を使用する RADIUS ベースの認証を示しています。

図 *62 : EAP* を使用する *RADIUS* ベースの認証



Extensible Authentication Protocol-Message Digest 5

Extensible Authentication Protocol-Message Digest 5（EAP-MD5）では、一方向のクライアント認証が提供されます。サーバーは、クライアントにランダムチャレンジを送信します。クライアントは、チャレンジとそのパスワードをMD5で暗号化することによって、応答でそのIDを証明します。中間者がチャレンジと応答を見ることができるため、EAP-MD5は、公開メディアで使用される場合にはディクショナリ攻撃に対して脆弱です。サーバー認証が行われないため、スプーフィングに対しても脆弱です。Cisco ISE では、Cisco ISE 内部 ID ストアに対するEAP-MD5認証がサポートされます。EAP-MD5プロトコルを使用している場合は、ホストルックアップもサポートされます。

Lightweight Extensible Authentication Protocol

Cisco ISE では現在、Lightweight Extensible Authentication Protocol（LEAP）を Cisco Aironet ワイヤレス ネットワーキングに対してだけ使用します。このオプションを有効にしないと、LEAP認証を実行するように設定された Cisco Aironet エンドユーザー クライアントは、ネットワークにアクセスできなくなります。Cisco Aironetエンドユーザークライアントすべてが Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）などの異なる認証プロトコルを使用する場合は、このオプションを無効にすることを推奨します。

（注） [ネットワーク デバイス（Network Devices）] セクションで RADIUS（Cisco Aironet）デバイスとして定義された AAA クライアントを使用してユーザーがネットワークにアクセスする場合は、LEAP、EAP-TLS、またはその両方を有効にする必要があります。これ以外の場合、Cisco Aironet ユーザーは認証を受けることができません。

保護拡張認証プロトコル

保護拡張認証プロトコル（PEAP）では、相互認証が提供され、脆弱なユーザー クレデンシャルの機密性と整合性が保証されます。またこのプロトコルでは、自身をパッシブ（盗聴）およびアクティブ（中間者）攻撃から保護し、セキュアに暗号キー関連情報を生成します。PEAPは、IEEE 802.1X標準およびRADIUSプロトコルと互換性があります。Cisco ISE では、Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol（EAP-MS-CHAP）、Extensible Authentication Protocol-Generic Token Card（EAP-GTC）、およびEAP-TLS内部方式でPEAP バージョン 0（PEAPv0）と PEAP バージョン 1（PEAPv1）がサポートされます。Cisco Secure Services Client（SSC）サプリカントでは、Cisco ISE でサポートされるすべての PEAPv1内部方式がサポートされます。

PEAP の使用の利点

PEAP を使用すると、次のような利点があります。PEAP は、広く実装されセキュリティが細部にわたって確認された TLS に基づいています。キーを生成しない方式に対しては、キーを確立します。トンネル内でIDを送信します。内部方式の交換と結果メッセージを保護します。フラグメンテーションがサポートされます。

PEAP プロトコルでサポートされているサプリカント

PEAP では、次のサプリカントがサポートされます。

- Microsoft Built-In Clients 802.1X XP
- Microsoft Built-In Clients 802.1X Vista
- Cisco Secure Services Client（SSC）リリース 4.0
- Cisco SSC リリース 5.1
- Funk Odyssey Access Client リリース 4.72
- Intel リリース 12.4.0.0

PEAP プロトコルのフロー

PEAP カンバセーションは、次の 3 つの部分に分かれます。

1. Cisco ISE とピアが TLS トンネルを構築します。Cisco ISE は自身の証明書を提示しますが、ピアは提示しません。ピアと Cisco ISE はキーを作成して、トンネル内のデータを暗号化します。
2. 内部方式によって、次のようにトンネル内のフローが決定されます。
   - EAP-MS-CHAPv2 内部方式：EAP-MS-CHAPv2 パケットは、ヘッダーなしでトンネル内を移動します。ヘッダーの先頭のバイトにタイプ フィールドが含まれます。EAP-MS-CHAPv2 内部方式では、パスワード変更機能がサポートされます。ユーザーが管理者ポータルでパスワードの変更を試行できる回数を設定できます。ユーザー認証の試行回数はこの数値によって制限されます。
   - EAP-GTC 内部方式：PEAPv0 と PEAPv1 の両方で、EAP-GTC 内部方式がサポートされます。サポートされるサプリカントでは、EAP-GTC 内部方式を使用する PEAPv0 はサポートされません。EAP-GTC では、パスワード変更機能がサポートされます。ユーザーが管理者ポータルでパスワードの変更を試行できる回数を設定できます。ユーザー認証の試行回数はこの数値によって制限されます。
   - EAP-TLS 内部方式：Windows 組み込みサプリカントでは、トンネルが確立された後のメッセージのフラグメンテーションはサポートされず、このことは EAP-TLS 内部方式に影響を与えます。Cisco ISE では、トンネルが確立された後の外部 PEAP メッセージのフラグメンテーションはサポートされません。トンネルの確立中、フラグメンテーションは PEAP のマニュアルで指定されているとおりに動作します。PEAPv0 では EAP-TLS パケットのヘッダーが削除され、PEAPv1 では EAP-TLS パケットがそのまま送信されます。

- Extensible Authentication Protocol-type, length, value（EAP-TLV）拡張：EAP-TLV パケットはそのまま送信されます。EAP-TLV パケットは、トンネル内をヘッダー付きで移動します。

3. カンバセーションが内部方式に到達した場合、保護された成功と失敗の確認応答があります。

   クライアント EAP メッセージは常に RADIUS Access-Request メッセージで送信され、サーバー EAP メッセージは常に RADIUS Access-Challenge メッセージで送信されます。EAP-Success メッセージは、常に RADIUS Access-Accept メッセージで送信されます。EAP-Failure メッセージは、常に RADIUS Access-Reject メッセージで送信されます。クライアント PEAP メッセージをドロップすると、RADIUS クライアント メッセージがドロップされます。

（注） Cisco ISE は、PEAPv1 通信中に EAP-Success または EAP-Failure メッセージの確認を要求します。ピアは、成功または失敗メッセージの受信を確認するために空の TLS データ フィールドを含む PEAP パケットを返送する必要があります。

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）は、相互認証を提供する認証プロトコルであり、共有秘密を使用してトンネルを確立します。このトンネルは、パスワードに基づく弱い認証方式を保護するために使用されます。Protected Access Credentials（PAC）キーと呼ばれる共有秘密は、トンネルのセキュリティを確保するときにクライアントとサーバーを相互認証するために使用されます。

EAP-FAST の利点

EAP-FAST は、他の認証プロトコルに比べて次の利点があります。

- 相互認証：EAP サーバーはピアの ID と信頼性を確認できる必要があり、ピアは EAP サーバーの信頼性を確認できる必要があります。
- パッシブ ディクショナリ攻撃に対する耐性：多くの認証プロトコルでは、ピアから EAP サーバーにパスワードがクリアテキストまたはハッシュとして明示的に提供される必要があります。
- 中間者攻撃に対する耐性：相互認証された保護トンネルの確立時に、プロトコルは、ピアと EAP サーバーとの間のカンバセーションに攻撃者が情報を挿入することを防ぐ必要があります。
- MS-CHAPv2 や汎用トークン カード（GTC）などの多くの異なるパスワード認証インターフェイスをサポートできる柔軟性：EAP-FAST は、同じサーバーで複数の内部プロトコルをサポートできる拡張可能なフレームワークです。
- 効率性：無線メディアを使用する場合、ピアは計算資源と電源リソースを制限されます。EAP-FAST では、ネットワーク アクセス通信の計算を軽量化できます。
- 認証サーバーのユーザーごとの認証状態要件の最小化：大規模な展開では、通常、多くのサーバーが多くのピアに対する認証サーバーとして機能する必要があります。ユーザー名

とパスワードを使用してネットワークにアクセスするのと同じように、ピアが同じ共有秘密を使用してトンネルのセキュリティを確保することも強く推奨されます。EAP-FAST により、サーバーでキャッシュおよび管理する必要があるユーザーごとおよびデバイスごとの状態を最小にすることができ、ピアによる強力な単一共有秘密の使用が容易になります。

EAP-FAST フロー

EAP-FAST プロトコルのフローは常に、次のフェーズを組み合わせたものになります。

1. プロビジョニング フェーズ：これは EAP-FAST のフェーズ 0 です。このフェーズでは、Cisco ISE とピアとの間で共有される、PAC と呼ばれる一意の強力な秘密を使用して、ピアがプロビジョニングされます。
2. トンネル確立フェーズ：PAC を使用して新しいトンネル キーを確立することによって、クライアントとサーバーを相互認証します。トンネル キーはその後、残りのカンバセーションを保護するために使用され、メッセージの機密性と信頼性を提供します。
3. 認証フェーズ：認証がトンネル内で処理され、セッション キーの生成と保護された終了が行われます。Cisco ISE では、EAP-FAST バージョン 1 および 1a がサポートされます。

シスコ以外のデバイスからの MAB の有効化

次の設定を順番に設定して、シスコ以外のデバイスから MAB を設定します。

ステップ 1 認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。プロファイラ サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。

ステップ 2 シスコ以外のデバイス（PAP、CHAP、EAP-MD5）で使用される MAC 認証のタイプに基づいて、ネットワーク デバイス プロファイルを作成します。

a) [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス プロファイル（Network Device Profiles）] の順に選択します。
b) [追加（Add）] をクリックします。
c) ネットワーク デバイス プロファイルの名前と説明を入力します。
d) [ベンダー（Vendor）] ドロップダウン リストからベンダー名を選択します。
e) デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスが RADIUS をサポートする場合は、ネットワーク デバイスで使用する RADIUS ディクショナリを選択します。
f) [認証/許可（Authentication/Authorization）] セクションを展開し、フロー タイプ、属性エイリアシング、およびホスト ルックアップに関するデバイスのデフォルト設定を行います。
g) [ホスト ルックアップ（MAB）（Host Lookup (MAB)）] セクションで、次を実行します。

- [ホスト ルックアップの処理（Process Host Lookup）]：ネットワーク デバイス プロファイルで使用されるホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。

さまざまなベンダーからのネットワーク デバイスは、MAB認証を異なる方法で実行します。デバイス タイプに応じて、使用しているプロトコルの [パスワードを確認（Check Password）] チェック ボックスまたは [Calling-Station-Id が MAC アドレスと等しいかを確認（Checking Calling-Station-Id equals MAC Address）] チェック ボックス、またはその両方をオンにします。

- [PAP/ASCII 経由（Via PAP/ASCII）]：ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。
- [CHAP 経由（Via CHAP）]：ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。
- [EAP-MD5 経由（Via EAP-MD5）]：ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。

h) [アクセス許可（Permissions）]、[認可変更（CoA）（Change of Authorization (CoA)）]、[リダイレクト（Redirect）] のセクションで必要な詳細を入力して、[送信（Submit）] をクリックします。

カスタム NAD プロファイルを作成する方法については、『Network Access Device Profiles with Cisco Identity Services Engine』を参照してください。

ステップ 3 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）][ネットワークリソース（Network Resources）][ネットワークデバイス（Network Devices）]** を選択します。

ステップ 4 MAB を有効にするデバイスを選択して、[編集（Edit）] をクリックします。

ステップ 5 [ネットワーク デバイス（Network Device）] ページの [デバイス プロファイル（Device Profile）] ドロップダウン リストから、手順 2 で作成したネットワーク デバイス プロファイルを選択します。

ステップ 6 [保存（Save）] をクリックします。

（注） Cisco NAD では、MAB および Web/ユーザー認証に使用する Service-Type 値は異なります。これにより、Cisco NAD を使用する場合に、ISE は MAB と Web 認証を区別できます。シスコ以外の一部の NAD では、MAB と Web/ユーザー認証に同じ値の Service-Type 属性を使用しています。この場合、アクセスポリシーでセキュリティ上の問題につながる場合があります。シスコ以外のデバイスで MAB を使用する場合は、ネットワーク セキュリティが侵害されないように、追加の許可ポリシー ルールを設定することを推奨します。たとえば、プリンタで MAB を使用する場合は、ACL のプリンタ プロトコル ポートに制限する許可ポリシー ルールを設定できます。

シスコ デバイスからの MAB の有効化

次の設定を順番に設定して、シスコ デバイスから MAB を設定します。

ステップ 1 認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。プロファイラ サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。

ステップ 2 シスコ デバイス（PAP、CHAP、EAP-MD5）で使用される MAC 認証のタイプに基づいて、ネットワーク デバイス プロファイルを作成します。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[管理（Administration）]>[ネットワークリソース（Network Resources）]>[ネットワーク デバイス プロファイル（Network Device Profiles）] を 選択します。

b) [追加（Add）] をクリックします。

c) ネットワーク デバイス プロファイルの名前と説明を入力します。

d) デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスが RADIUS をサポートする場合は、ネットワーク デバイスで使用する RADIUS ディクショナリを選択します。

e) [認証/許可（Authentication/Authorization）] セクションを展開し、フロータイプ、属性エイリアシング、およびホスト ルックアップに関するデバイスのデフォルト設定を行います。

f) [ホスト ルックアップ（MAB）（Host Lookup (MAB)）] セクションで、次を実行します。

- [ホスト ルックアップの処理（Process Host Lookup）]：ネットワーク デバイス プロファイルで使用されるホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。

  デバイス タイプに応じて、使用しているプロトコルの [パスワードを確認（Check Password）] チェックボックスまたは [Calling-Station-Id が MAC アドレスと等しいかを確認（Checking Calling-Station-Id equals MAC Address）] チェックボックス、またはその両方をオンにします。

- [PAP/ASCII 経由（Via PAP/ASCII）]：ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。

- [CHAP 経由（Via CHAP）]：ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。

- [EAP-MD5 経由（Via EAP-MD5）]：ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。

g) [アクセス許可（Permissions）]、[認可変更（CoA）（Change of Authorization (CoA)）]、[リダイレクト（Redirect）] のセクションで必要な詳細を入力して、[送信（Submit）] をクリックします。

カスタム NAD プロファイルを作成する方法については、『Network Access Device Profiles with Cisco Identity Services Engine』を参照してください。

ステップ 3 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）][ネットワークリソース（Network Resources）][ネットワークデバイス（Network Devices）]** を選択します。

ステップ 4 MAB を有効にするデバイスを選択して、[編集（Edit）] をクリックします。

ステップ 5 [ネットワーク デバイス（Network Device）] ページの [デバイス プロファイル（Device Profile）] ドロップダウン リストから、手順 2 で作成したネットワーク デバイス プロファイルを選択します。

ステップ 6 [保存（Save）] をクリックします。

ISE コミュニティ リソース

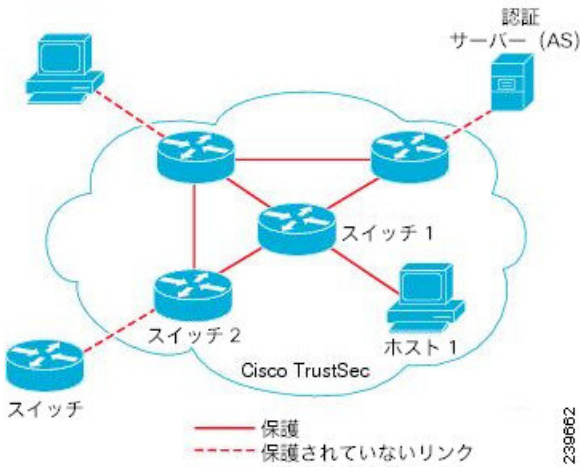
IP フォンの認証機能については、「Phone Authentication Capabilities」を参照してください。

TrustSec アーキテクチャ

Cisco TrustSec ソリューションでは、信頼ネットワーク デバイスのクラウドを確立して、セキュアなネットワークを構築します。Cisco TrustSec クラウド内の個々のデバイスは、そのネイバー（ピア）によって認証されます。TrustSec クラウド内のデバイス間の通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。TrustSec ソリューションでは、認証中に取得したデバイスおよびユーザー ID 情報を使用して、ネットワークに入ってきたパケットを分類（色付け）します。このパケット分類は、パケットが TrustSec ネットワークに入ってきたときに、そのパケットにタグ付けすることによって維持されます。これにより、パケットはデータ パス全体で正しく識別され、セキュリティおよびその他のポリシー基準が適用されるようになります。このタグは、セキュリティ グループ タグ（SGT）と呼ばれることもあります。エンドポイント デバイスで SGT に応じてトラフィックをフィルタリングできるようにすることにより、Cisco ISE でアクセス コントロール ポリシーを適用できるようになります。

次の図に、TrustSec ネットワーク クラウドの例を示します。

図 *63 : TrustSec* アーキテクチャ



ISE コミュニティ リソース

Cisco TrustSec を使用してネットワーク セグメンテーションを簡素化、セキュリティを強化する方法については、「Simplify Network Segmentation with Cisco TrustSec」と「Policy-Based Software Defined Segmentation and Cisco TrustSec Improve Security White Paper」を参照してください。

Cisco TrustSec プラットフォーム サポート マトリックスのリストについては、「Cisco TrustSec Platform Support Matrix」を参照してください。

利用可能な TrustSec のサポート ドキュメントのリストについては、「Cisco TrustSec」を参照してください。

TrustSec コミュニティ リソースのリストについては、「TrustSec Community」を参照してください。

TrustSec のコンポーネント

主な TrustSec のコンポーネント：

- ネットワーク デバイス アドミッション コントロール（NDAC）：信頼ネットワークでは、認証中に、TrustSec クラウド内にある各ネットワーク デバイス（イーサネット スイッチなど）のクレデンシャルおよび信頼性が、そのピア デバイスによって検証されます。NDAC は IEEE 802.1X ポートベース認証を使用し、その拡張認証プロトコル（EAP）方式として Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）を使用します。NDAC プロセスの認証および許可が成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションが実行されます。Cisco ISE では、IOS XE 17.1 以降のスイッチング プラットフォームおよび IOS XE 17.6 以降のルーティング プラットフォームのための CTS プロビジョニング（EAP-FAST）TLSv1.2 のサポートが用意されています。
- エンドポイント アドミッション コントロール（EAC）：TrustSec クラウドに接続しているエンドポイント ユーザーまたはデバイスの認証プロセス。EAC は一般的にアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可が成功すると、ユーザーまたはデバイスに対する SGT 割り当てが実行されます。認証および許可の EAC アクセス方法には次のものがあります。
  - 802.1X ポートベースの認証
  - MAC 認証バイパス（MAB）
  - Web 認証（WebAuth）
- セキュリティ グループ（SG）：アクセス コントロール ポリシーを共有するユーザー、エンドポイント デバイス、およびリソースのグループ。SG は、管理者が Cisco ISE で定義します。新規ユーザーおよびデバイスが TrustSec ドメインに追加されると、Cisco ISE では、これらの新規エントリを適切なセキュリティ グループに割り当てます。

- セキュリティ グループ タグ（SGT）：TrustSec サービスは各セキュリティ グループに、その範囲が TrustSec ドメイン内でグローバルな一意のセキュリティ グループ番号（16 ビット）を割り当てます。スイッチ内のセキュリティ グループの数は、認証されたネットワーク エンティティの数に制限されます。セキュリティ グループ番号を手動で設定する必要はありません。これらは自動的に生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。
- セキュリティ グループ アクセス コントロール リスト（SGACL）：SGACL では、割り当てられている SGT に基づいてアクセスおよび権限を制御できます。権限をロールにまとめることにより、セキュリティ ポリシーの管理が容易になります。デバイスを追加するときに、1 つ以上のセキュリティ グループを割り当てるだけで、即座に適切な権限が付与されます。セキュリティ グループを変更することにより、新しい権限を追加したり、現在の権限を制限することもできます。
- セキュリティ交換プロトコル（SXP）：SGT 交換プロトコル（SXP）は、TrustSec サービス用に開発されたプロトコルで、SGT 対応ハードウェアをサポートしていないネットワーク デバイス間で、SGT/SGACL をサポートしているハードウェアに IP-SGT バインディングを伝播します。
- 環境データのダウンロード：TrustSec デバイスは、初めて信頼ネットワークに参加するときに、その環境データを Cisco ISE から取得します。デバイス上の一部のデータは、手動で設定することもできます。デバイスでは、期限切れになる前に環境データを更新する必要があります。TrustSec デバイスは、次の環境データを Cisco ISE から取得します。
  - サーバー リスト：クライアントがその後の RADIUS 要求に使用できるサーバーのリスト（認証および許可の両方）
  - デバイス SG：そのデバイス自体が属しているセキュリティ グループ
  - 有効期間：TrustSec デバイスが環境データをダウンロードまたはリフレッシュする頻度を制御する期間
- ID とポートとのマッピング：エンドポイントの接続先のポートでスイッチが ID を定義するための方法で、この ID を使用して Cisco ISE サーバー内の特定の SGT 値が検索されます。

TrustSec の用語

次の表は、TrustSec ソリューションで使用される一般的な用語の一部と、TrustSec 環境でのその意味を示しています。

表 *149 : TrustSec* の用語

用語	意味
サプリカント	信頼ネットワークへの参加を試行するデバイス。

用語	意味
認証	信頼ネットワークへの参加を許可する前に、各デバイスの ID を検証するプロセス。
許可	信頼ネットワーク上のリソースへのアクセスを要求しているデバイスに対し、デバイスの認証IDに基づいてアクセスのレベルを決定するプロセス。
アクセス コントロール	各パケットに割り当てられている SGT に基づいて、パケットごとにアクセス コントロールを適用するプロセス。
セキュアな通信	信頼ネットワーク内の各リンクを経由して流れるパケットをセキュリティで保護するための、暗号化、整合性、データパス リプレイ保護のプロセス。
TrustSec デバイス	TrustSec ソリューションをサポートする Cisco Catalyst 6000 シリーズまたは Cisco Nexus 7000 シリーズのスイッチ。
TrustSec 対応デバイス	TrustSec 対応デバイスは、TrustSec 対応のハードウェアとソフトウェアを備えています。たとえば、Nexus オペレーティング システムを搭載した Nexus 7000 シリーズ スイッチなどです。
TrustSec シード デバイス	Cisco ISE サーバーに対して直接認証を行う TrustSec デバイス。オーセンティケータとサプリカントの両方として機能します。
受信側	Cisco TrustSec ソリューションが有効になっているネットワーク内の TrustSec 対応デバイスにパケットが初めて到達すると、SGT を使用してパケットにタグが付けられます。この信頼ネットワークへの入り口点を入力と呼びます。
送信側	Cisco TrustSec ソリューションが有効になっているネットワーク内の最後の TrustSec 対応デバイスをパケットが通過すると、タグが解除されます。この信頼ネットワークからの出口点を出力と呼びます。

TrustSec のサポートされるスイッチと必要なコンポーネント

Cisco TrustSec ソリューションが有効になった Cisco ISE ネットワークを設定するには、TrustSec ソリューションおよび他のコンポーネントをサポートするスイッチが必要です。スイッチ以外に、IEEE 802.1X プロトコルを使用した ID ベースのユーザー アクセス コントロールには、その他のコンポーネントも必要です。TrustSec をサポートするシスコ スイッチのプラットフォームおよび必要なコンポーネントの完全な最新のリストについては、「Cisco TrustSec-Enabled Infrastructure」を参照してください。

Cisco Catalyst Center との統合

Catalyst Center は、Cisco ISE との信頼された通信リンクを作成するメカニズムを備えており、Cisco ISE と安全な方法でデータを共有できます。Cisco ISE が Catalyst Center に登録されると、Catalyst Center が検出したすべてのデバイスが、関連する設定やその他のデータとともに Cisco ISE にプッシュされます。Catalyst Center を使用してデバイスを検出し、Catalyst Center と Cisco ISE の両方の機能を検出されたデバイスに適用できます。これは、検出されたデバイスが両方のアプリケーションに表示されるためです。Catalyst Center デバイスと Cisco ISE デバイスは、すべてそのデバイス名で一意に識別されます。

Cisco ISE への Catalyst Center の接続

Cisco ISE 用の Catalyst Center の設定の詳細については、『Cisco Catalyst Center Installation Guide』を参照してください。

このセクションでは、Catalyst Center 向けの Cisco ISE 設定に関する追加情報について説明します。

- パスワード：Catalyst Center は、Cisco ISE に接続するときに、Cisco ISE 管理者のユーザー名とパスワードを使用します。システムパスワードの詳細については、Cisco ISE への管理アクセス （22 ページ）を参照してください。

（注） 2.2.1.0 より前の Catalyst Center バージョンでは、Cisco ISE CLI を使用して初期統合手順を実行していたため、Cisco ISE CLI と管理者のユーザー名およびパスワードは同じである必要がありました。Catalyst Center リリース 2.2.1.0 以降では、Cisco ISE CLI の使用が廃止されているため、Cisco ISE CLI と管理者のユーザー名およびパスワードを同じにする必要はありません。

- API：Cisco ISE で外部 RESTful サービス（ERS）API を有効にする必要があります。Cisco ISE で [セキュリティの強化に CSRF チェックを使用する（Use CSRF Check for Enhanced Security）] オプションが無効になっていることを確認してください。
- pxGrid：Cisco ISE は pxGrid コントローラで、Catalyst Center はサブスクライバです。Cisco ISE と Catalyst Center の両方で、SGT と SGACL 情報が含まれる Trustsec（SD-Access）コ

ンテンツをモニターします。Cisco ISE と Catalyst Center 間でシステムクロックを同期してください。Cisco ISE の pxGrid の詳細については、Cisco pxGridノード （464 ページ）を参照してください。

（注） Cisco ISE 2.4 以降では、pxGrid 2.0 および pxGrid 1.0 がサポートされています。pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Catalyst Center は現在 2 つを超える pxGrid ノードをサポートしていません。

- Cisco ISE IP アドレス：Cisco ISE PAN と Catalyst Center 間は直接接続する必要があります。プロキシ、ロードバランサ、または仮想 IP アドレスを使用することはできません。

  Cisco ISE がプロキシを使用していないことを確認します。使用している場合は、プロキシから Catalyst Center の IP を除外してください。

- SXP：Catalyst Center に SXP は必要ありません。Cisco ISE と Catalyst Center 管理対象ネットワークを接続する場合に SXP を有効にすると、Cisco ISE は Trustsec（SD-Access）がハードウェアでサポートされないネットワークデバイスと通信できます。

（注） TrustSec をサポートするように Cisco ISE 展開を設定する場合、または Cisco ISE が Catalyst Center と統合されている場合は、ポリシーサービスノードを SXP 専用として設定しないでください。SXP は、TrustSec デバイスと非 Trustsec デバイス間のインターフェイスです。TrustSec 対応ネットワークデバイスとは通信しません。

- Cisco ISE との接続用の証明書：
  - Cisco ISE 管理証明書では、件名または SAN に Cisco ISE IP または FQDN を含める必要があります。
  - ECDSA は、SSH キー、ISE SSH アクセス、または Catalyst Center と Cisco ISE の接続用の証明書ではサポートされません。
  - Catalyst Centerの自己署名証明書では、cA:TRUE (RFC5280 section-4.2.19) の Basic Constraints 拡張を使用する必要があります。

（注） 2.2.1.0 より前の Catalyst Center リリースでは、SSH を有効にする必要がありました。Catalyst Center リリース 2.2.1.0 以降、SSH の使用は廃止されたため、SSH を有効にする必要はありません。

TrustSec ダッシュボード

TrustSec ダッシュボードは、TrustSec ネットワークの一元化されたモニタリング ツールです。

TrustSec ダッシュボードには次のダッシュレットが含まれています。

- **[メトリック（Metrics）]**：[メトリック（Metrics）] ダッシュレットには、TrustSec ネットワークの動作に関する統計情報が表示されます。
- **[アクティブなSGTセッション（Active SGT Sessions）]**：[アクティブなSGTセッション（Active SGT Sessions）] ダッシュレットには、ネットワークで現在アクティブな SGT セッションが表示されます。[アラーム（Alarms）] ダッシュレットには、TrustSec セッション関連のアラームが表示されます。
- **[アラーム（Alarms）]**
- **[NAD/SGT/ACIクイックビュー（NAD / SGT/ACI Quick View）]**：[クイックビュー（Quick View）] ダッシュレットには、NAD および SGT の TrustSec 関連情報が表示されます。
- **[TrustSecセッション/NADアクティビティ/ACIエンドポイントアクティビティライブログ（TrustSec Sessions / NAD Activity/ACI endpoint Activity Livelog）]**：アクティブな TrustSec セッションを表示するには、[ライブログ（Livelog）] ドロップダウンリストから [TrustSec セッション（TrustSec Sessions）] を選択します。また、[NADアクティビティ（NAD Activity）] または [ACIエンドポイントアクティビティ（ACI endpoint Activity）] を選択して、NAD から Cisco ISE への TrustSec プロトコルデータ要求と応答に関する情報を表示することもできます。

メトリック

このセクションには、TrustSec ネットワークの動作に関する統計情報が表示されます。タイムフレーム（たとえば、過去 2 時間、過去 2 日 など）とチャート タイプ（たとえば、棒、折れ線、スプラインなど）を選択できます。

最新のバー値がグラフに表示されます。また、前のバーからのパーセンテージの変化も表示されます。バー値に増加がある場合、プラス記号付きの緑色で表示されます。値に減少がある場合、マイナス記号付きの赤色で表示されます。

値が計算された時刻とその正確な値を <Value:xxxx Date/Time: xxx> 形式で表示するには、グラフのバーにカーソルを置きます。

次のメトリックを表示できます。

SGTセッション（SGT sessions）	選択された時間内に作成された SGT セッションの総数が表示されます。 （注） SGTセッションは、認証フローの一部として SGT を受信したユーザー セッションです。

使用中のSGT（SGTs in use）	選択された時間内に使用された固有の SGT の総数が表示されます。たとえば、1 時間で 200 の TrustSec セッションがあったが、ISE が認証応答で 6 つのタイプの SGT でしか応答しなかった場合、グラフにはこの時間に値 6 が表示されます。
アラーム（Alarms）	選択された時間内に発生したアラームおよびエラーの総数が表示されます。エラーは赤色で表示され、アラームは黄色で表示されます。
使用中のNAD（NADs in use）	選択された時間内に TrustSec 認証に参加した固有の NAD の数が表示されます。

現在のネットワーク ステータス

このダッシュボードの中間部分には、TrustSec ネットワークの現在のステータスに関する情報が表示されます。グラフに表示される値は、ページがロードされると更新され、[ダッシュボードの更新（Refresh Dashboard）] オプションを使用して更新できます。

アクティブな SGT セッション

このダッシュレットには、ネットワークで現在アクティブなSGTセッションが表示されます。上位 10 個の最もよく使用されている SGT または最も使用頻度の低い SGT を表示できます。X 軸には SGT 使用率が表示され、Y 軸には SGT の名前が表示されます。

SGT の TrustSec セッションの詳細を表示するには、その SGT に対応するバーをクリックします。その SGT に関連する TrustSec セッションの詳細が [ライブログ（Live Log）] ダッシュレットに表示されます。

アラーム

このダッシュレットには、TrustSec セッション関連のアラームが表示されます。次の詳細情報を表示できます。

- [アラームのシビラティ（重大度）（Alarm Severity）]：アラームのシビラティ（重大度）レベルを示すアイコンが表示されます。
  - [高（High）]：TrustSec ネットワーク内の障害を示すアラームが含まれます（たとえば、PAC の更新が失敗したデバイスなど）。赤色のアイコンが付いています。
  - [中（Medium）]：ネットワーク デバイスの誤った設定を示す警告が含まれます（たとえば、CoA メッセージの受け入れを失敗したデバイスなど）。黄色でマークされます。
  - [低（Low）]：ネットワーク動作の一般情報および更新が含まれます（たとえば、TrustSec の設定変更など）。青色でマークされます。

- アラームの説明
- このアラーム カウンタが最後にリセットされてからアラームが発生した回数。
- アラームが最後に発生した時刻

クイック ビュー

[クイックビュー（Quick View）] ダッシュレットには、NAD の TrustSec 関連情報が表示されます。SGT の TrustSec 関連情報を表示することもできます。

NAD クイック ビュー

[検索（Search）] ボックスに詳細を表示する TrustSec ネットワーク デバイスの名前を入力し、**Enter** を押します。検索ボックスには自動入力機能があり、ユーザーがテキストボックスに入力すると、ドロップダウンに一致するデバイス名がフィルタされ表示されます。

次の情報がこのダッシュレットに表示されます。

- **[NDG（NDGs）]**：このネットワークデバイスが属するネットワーク デバイス グループ（NDG）がリストされます。
- **[IPアドレス（IP Address）]**：ネットワークデバイスの IP アドレスを表示します。[ライブ ログ（Live Logs）] ダッシュレットに NAD アクティビティの詳細を表示するには、このリンクをクリックします。
- **[アクティブセッション（Active sessions）]**：このデバイスに接続されているアクティブな TrustSec セッションの数がリストされます。
- **[PACの有効期限（PAC expiry）]**：PAC の失効日が表示されます。
- **[最後のポリシー更新（Last Policy Refresh）]**：ポリシーを最後にダウンロードした日付が表示されます。
- **[最後の認証（Last Authentication）]**：このデバイスの最後の認証レポートのタイムスタンプを表示します。が表示されます。
- **[アクティブSGT（Active SGTs）]**：このネットワークデバイスに関連するアクティブセッションで使用されている SGT がリストされます。カッコ内に表示される数字は、現在この SGT を使用しているセッションの数を示します。[ライブ ログ（Live Log）] ダッシュレットに TrustSec セッションの詳細を表示するには、SGT のリンクをクリックします。

[最新ログの表示（Show Latest Logs）] オプションを使用して、デバイスの NAD アクティビティのライブ ログを表示できます。

SGT クイック ビュー

[検索（Search）] ボックスに詳細を表示する SGT の名前を入力し、**Enter** を押します。

次の情報がこのダッシュレットに表示されます。

- **[値（Value）]**：SGT 値（10 進数と 16 進数の両方）が表示されます。

- **[アイコン（Icon）]**：この SGT に割り当てられているアイコンが表示されます。
- **[アクティブセッション（Active sessions）]**：現在この SGT を使用しているアクティブなセッションの数がリストされます。
- **[固有ユーザー（Unique users）]**：この SGT をアクティブセッションに保持する固有ユーザー名の数がリストされます。
- **[更新されたNAD（Updated NADs）]**：この SGT のポリシーをダウンロードした NAD の数がリストされます。

ACI クイックビュー

次の情報がこのダッシュレットに表示されます。

- **[SDA SGT（SDA SGTs）**：Cisco ISE が Cisco SD-Access に送信した SGT の数がリストされます。
- **[ACI EPG（ACI EPGs）]**：Cisco ISE が Cisco ACI から学習した EPG の数がリストされます。
- **[SDAバインディング（SDA Bindings）]**：Cisco ISE が Cisco SD-Access に送信したバインディングの数がリストされます。
- **[ACIバインディング（ACI Bindings）]**：Cisco ISE が Cisco ACI から学習したバインディングの数がリストされます。
- **[SDA VN（SDA VNs）]**：Cisco ISE が Cisco SD-Access から学習した仮想ネットワークの数がリストされます。
- **[ACI VN（ACI VNs）**：Cisco ISE が Cisco ACI から学習した仮想ネットワークの数がリストされます。
- **[SDA拡張VN（SDA Extended VNs）]**：Cisco SD-Access ドメインから Cisco ACI ドメインに送信された拡張仮想ネットワークの数がリストされます。
- **[SDAテナント（SDA Tenant）]**：Cisco ISE で Cisco SD-Access によって共有されるテナントの名前が表示されます。
- **[ACIテナント（ACI Tenants）]**：Cisco ACI が Cisco SD-Access と共有するテナントの数がリストされます。
- **[SDAドメインID（SDA Domain ID）]**：Cisco SD-Access のドメイン ID 番号が表示されます。
- **[ACIドメインID（ACI Domain ID）]**：Cisco ACI のドメイン ID 番号が表示されます。
- **[ピアリング状態（Peering State）]**：Cisco SD-Access ドメインと Cisco ACI ドメイン間のピアリング関係の現在の状態が表示されます。

ライブログ

[ライブログ（Livelog）] ドロップダウンリストの次のオプションから選択して、関連情報を表示します。

- アクティブな TrustSec セッション（応答の一部として SGT があるセッション）を表示するには、[Trustsecセッション（Trustsec Sessions）]。
- NAD から Cisco ISE への TrustSec プロトコルデータ要求と応答に関する情報を表示するには、[NADアクティビティ（NAD Activity）]。
- Cisco ISE が Cisco ACI から学習した IP-SGT 情報を表示するには、[ACIエンドポイントアクティビティ（ACI endpoint Activity）]。

TrustSec のグローバル設定

Cisco ISE が TrustSec サーバーとして機能して TrustSec サービスを提供するには、いくつかのグローバル TrustSec 設定を定義する必要があります。

始める前に

- TrustSec グローバル設定を設定する前に、グローバル EAP-FAST 設定が定義されていることを確認します（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [EAP-FAST 設定（EAP-FAST Settings）]** を選択）。

  [機関識別情報の説明（Authority Identity Info Description）] を Cisco ISE サーバー名に変更することができます。この説明は、クレデンシャルをエンドポイントクライアントに送信する Cisco ISE サーバーを説明したわかりやすい文字列にします。Cisco TrustSec アーキテクチャのクライアントには、IEEE 802.1X 認証の EAP 方式として EAP-FAST を実行するエンドポイント、または Network Device Access Control（NDAC）を実行するサプリカントネットワークデバイスのいずれも使用できます。クライアントは、この文字列を Protected Access Credentials（PAC）Type-Length-Value（TLV）情報で認識できます。デフォルト値は、Identity Services Engine です。NDAC 認証時に、ネットワーク デバイスで Cisco ISE PAC 情報が一意に識別されるように、この値を変更する必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSec の全般設定（General TrustSec Settings）]**

ステップ 2 フィールドに値を入力します。フィールドの詳細については、次を参照してください。一般 TrustSec の設定 （1599 ページ）

ステップ 3 [保存（Save）] をクリックします。

次のタスク

- TrustSec デバイスの設定 （1605 ページ）

一般 TrustSec の設定

Cisco ISE が TrustSec サーバーとして機能したり、TrustSec サービスを提供したりするには、グローバル TrustSec 設定を定義します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）]>[TrustSec] > [設定（Settings）] > [TrustSec の全般設定（General TrustSec Settings）]。

TrustSec 展開の確認

このオプションを選択すると、すべてのネットワークデバイスに最新の TrustSec ポリシーが展開されているかどうかを確認できます。Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合は [アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] および [ホーム（Home）] > [サマリ（Summary）]）にアラームが表示されます。TrustSec ダッシュ ボードに、以下のアラームが表示されます。

- 検証プロセスが開始または完了するたびに、[情報（Info）] アイコンとともにアラームが表示されます。
- 新しい展開要求により検証プロセスがキャンセルされた場合は、[情報（Info）] アイコンとともにアラームが表示されます。
- 検証プロセスがエラーで失敗した場合は、[警告（Warning）] アイコンとともにアラームが表示されます。たとえば、ネットワーク デバイスとの SSH 接続を開けない場合やネットワーク デバイスが使用できない場合、あるいは Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合などです。

[展開の検証（Verify Deployment）] オプションは、次のウィンドウでも使用できます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。：

- **[ワーク センター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティ グループ（Security Groups）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ ACL（Security Group ACLs）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [送信元ツリー（Source Tree）]**

- **[ワーク センター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [宛先ツリー（Destination Tree）]**

[すべての展開後に自動検証（Automatic Verification After Every Deploy）]：それぞれの展開後に、Cisco ISE ですべてのネットワーク デバイス上の更新を検証するには、このチェックボックスをオンにします。展開プロセスが完了したら、[展開プロセス後の時間（Time after Deploy Process）] フィールドに指定した時間が経過した後に、検証プロセスが開始されます。

[展開プロセス後の時間（Time after Deploy Process）]：展開プロセスが完了した後、検証プロセスを開始する前に Cisco ISE に待機させる時間を指定します。有効な範囲は、10 ～ 60 分です。

待機期間中に新しい展開が要求された場合や別の検証が進行中の場合は、現在の検証プロセスはキャンセルされます。

[今すぐ検証（Verify Now）]：検証プロセスをすぐに開始するには、このオプションをクリックします。

Protected Access Credential（PAC）

- [トンネル PAC の存続可能時間（Tunnel PAC Time to Live）]：

  PAC の有効期限を指定します。トンネル PAC は EAP-FAST プロトコル用のトンネルを生成します。時間を秒、分、時、日数、または週数で指定できます。デフォルト値は 90 日です。有効な範囲は次のとおりです。

  - 1 ～ 157680000 秒
  - 1 ～ 2628000 分
  - 1 ～ 43800 時間
  - 1 ～ 1825 日
  - 1 ～ 260 週間

- [プロアクティブ PAC 更新を次の後に実行する（Proactive PAC Update Will Occur After）]：Cisco ISE は、認証に成功した後、設定したパーセンテージのトンネル PAC TTL が残っているときに、新しい PAC をクライアントに予防的に提供します。PAC の期限が切れる前に最初の認証が正常に行われると、サーバーはトンネル PAC の更新を開始します。このメカニズムにより、有効な PAC でクライアントが更新されます。デフォルト値は 10% です。

セキュリティグループタグ番号の割り当て

- [システムで SGT 番号を割り当てる（System will Assign SGT Numbers）]：Cisco ISE に SGT 番号を自動生成させる場合は、このオプションを選択します。

- [範囲内の番号を除外する（Except Numbers In range）]：手動設定用に SGT 番号の範囲を予約する場合は、このオプションを選択します。Cisco ISE は、SGT の生成時にこの範囲の数値を使用しません。
- [ユーザーが手動で SGT 番号を入力する（User Must Enter SGT Numbers Manually）]：SGT 番号を手動で定義する場合は、このオプションを選択します。

APIC EPGのセキュリティグループタグのナンバリング（Security Group Tag Numbering for APIC EPGs）

[APIC EPGのセキュリティグループタグのナンバリング（Security Group Tag Numbering for APIC EPGs）]：APIC から学習した EPG に基づいて SGT を作成する場合は、このチェックボックスをオンにし、使用する番号の範囲を指定します。

セキュリティグループの自動作成

[認証ルールを作成するときにセキュリティグループを自動作成する（Auto Create Security Groups When Creating Authorization Rules）]：認証ポリシーのルールを作成する際に SGT を自動的に作成する場合は、このチェックボックスをオンにします。

このオプションを選択した場合は、[認証ポリシー（Authorization Policy）] ウィンドウの上部に、`Auto Security Group Creation is On` というメッセージが表示されます。

自動作成された SGT は、ルール属性に基づいて命名されます。

（注） 自動作成された SGT は、それに対応する認可ポリシールールを削除しても削除されません。

デフォルトでは、新規インストールまたはアップグレードの後でこのオプションが無効になります。

- [自動命名オプション（Automatic Naming Options）]：自動作成される SGT の命名規則を定義するには、このオプションを使用します。

  （必須）[名前に次が含まれます（Name Will Include）]：次のオプションのいずれかを選択します。

  - **ルール名（Rule name）**
  - **SGT番号（SGT number）**
  - **ルール名およびSGT番号（Rule name and SGT number）**

  デフォルトでは、[ルール名（Rule name）] オプションが選択されます。

  オプションで、SGT 名に以下の情報を追加できます。

  - **ポリシーセット名（Policy Set Name）**（このオプションは [ポリシーセット（Policy Sets）] が有効な場合にのみ使用可能です）
  - **プレフィックス（Prefix）**（8 文字まで）

- **サフィックス（Suffix）**（8 文字まで）

Cisco ISE は、選択内容に応じて [サンプル名（Example Name）] フィールドにサンプル SGT 名を表示します。

同じ名前の SGT が存在している場合、ISE は SGT 名に「_*x*」を付け加えます。*x* は（現在の名前に 1 が使用されていない場合は）1 から始まる最初の値です。新しい名前が 32 文字より長い場合、Cisco ISE によって最初の 32 文字に切り捨てられます。

ホスト名の IP SGT 静的マッピング（IP SGT Static Mapping of Hostnames）

[ホスト名の IP SGT 静的マッピング（IP SGT Static Mapping of Hostnames）]：FQDN とホスト名が使用される場合、Cisco ISE はマッピングを展開して展開状態を検査する際に、PAN および PSN ノード内の対応する IP アドレスを検索します。DNS クエリによって返される IP アドレス用に作成されるマッピングの数を指定する場合は、このオプションを使用します。次のいずれかのオプションを選択できます。

- **DNS クエリによって返されるすべての IP アドレスに対してマッピングを作成する（Create mappings for all IP addresses returned by a DNS query）**
- **DNSクエリによって返される最初のIPv4アドレスおよび最初のIPv6アドレスに対してのみマッピングを作成する（Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query）**

ネットワークデバイス用TrustSec HTTPサービス

- [HTTP サービスを有効化（Enable HTTP Service）]：HTTPを使用して、ポート 9063 経由で TrustSec データをネットワークデバイスに転送します。
- [応答ペイロード本文を監査に含める（Include entire response payload body in Audit）]：監査ログに TrustSec HTTP 応答ペイロード本文全体を表示する場合は、このオプションを有効にします。このオプションを選択すると、パフォーマンスが大幅に低下する可能性があります。このオプションを無効にすると、HTTP ヘッダー、ステータス、および認証情報のみがログに記録されます。

関連トピック

TrustSec アーキテクチャ （1588 ページ）
TrustSec のコンポーネント （1589 ページ）
TrustSec のグローバル設定 （1598 ページ）

TrustSec マトリックスの設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSecマトリックスの設定（TrustSec Matrix Settings）] の順に選択します。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSecマトリックスの設定（TrustSec Matrix Settings）]**。

ステップ 3 [TrustSecマトリックスの設定（TrustSec Matrix Settings）] ページに必要な詳細を入力します。

ステップ 4 [保存（Save）] をクリックします。

TrustSec マトリックスの設定

次の表では、[TrustSec マトリックスの設定（TrustSec Matrix Settings）] ウィンドウにある各フィールドの説明を示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSec マトリックスの設定（TrustSec Matrix Settings）]**。

表 *150 : TrustSec* マトリックスの設定

フィールド名	使用上のガイドライン
複数のSGACLを許可（Allow Multiple SGACLs）	セル内で複数の SGACL を許可するには、このチェックボックスをオンにします。このオプションが選択されていない場合、Cisco ISE はセル 1 つあたり 1 つの SGACL のみを許可します。 デフォルトでは、新たにインストールすると、このオプションはディセーブルになります。 アップグレード後、Cisco ISE は出力セルをスキャンし、複数の SGACL が割り当てられたセルを少なくとも 1 つ特定した場合、管理者に複数の SGACL をセルに追加することを許可します。それ以外の場合は、セル 1 つあたり 1 つの SGACL のみを許可します。 （注） 複数の SGACL を無効にする前に、複数の SGACL を含むセルを 1 つの SGACL のみを含めるように編集する必要があります。

フィールド名	使用上のガイドライン
モニタリングの許可（Allow Monitoring）	マトリクス内のすべてのセルのモニタリングをイネーブルにする場合は、このチェックボックスをオンにします。モニタリングがディセーブルの場合、[セルの編集（Edit Cell）] ダイアログで、[すべてをモニター（Monitor All）] アイコンはグレー表示され、[モニター（Monitor）] オプションはディセーブルになります。 デフォルトでは、新たにインストールすると、モニタリングはディセーブルになります。 （注） マトリクス レベルでモニタリングをディセーブルにする前に、現在モニターされているセルのモニタリングをディセーブルにする必要があります。
SGT番号の表示（Show SGT Numbers）	マトリクス セルの SGT 値（10 進数および 16 進数の両方）を表示または非表示にするには、このオプションを使用します。 デフォルトでは、SGT 値はセルに表示されます。
アピアランス設定（Appearance Settings）	次のオプションを使用できます。 • [カスタム設定（Custom settings）] : デフォルトのテーマ（パターンなしの色）が最初に表示されます。独自の色とパターンを設定できます。 • [デフォルト設定（Default settings）] : パターンなしの色の事前に定義されたリスト（編集不可）。 • [アクセシビリティ設定（Accessibility settings）] : パターンありの色の事前に定義されたリスト（編集不可）。

フィールド名	使用上のガイドライン
色/パターン（Color/Pattern）	マトリックスを読み取りやすくするために、セルの内容に基づいて、マトリックス セルに色とパターンを適用できます。 使用可能な表示タイプは、次のとおりです。 • [IP を許可/IP ログを許可（Permit IP/Permit IP Log）]：セル内に設定されます。 • [IP を拒否/IP ログを拒否（Deny IP/Deny IP Log）]：セル内に設定されます。 • [SGACL（SGACLs）]：セル内に設定されている SGACL の場合。 • [IP を許可/IP ログを許可（継承）（Permit IP/Permit IP Log (Inherited)）]：デフォルト ポリシーから取得されます（設定されていないセルの場合）。 • [IP を拒否/IP ログを拒否（継承）（Deny IP/Deny IP Log (Inherited)）]：デフォルト ポリシーから取得されます（設定されていないセルの場合）。 • [SGACL（継承）（SGACLs (Inherited)）]：デフォルトポリシーから取得されます（設定されていないセルの場合）。

関連トピック

出力ポリシー （1620 ページ）
マトリクス ビュー （1621 ページ）
TrustSec マトリックスの設定 （1602 ページ）

TrustSec デバイスの設定

Cisco ISE で TrustSec 対応デバイスからの要求を処理するには、これらの TrustSec 対応デバイスを Cisco ISE で定義しておく必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）]**

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ネットワーク デバイス（Network Devices）] セクションで、必要な情報を入力します。

ステップ 4 TrustSec 対応デバイスを設定するために [高度な TrustSec 設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 5 [送信（Submit）] をクリックします。

OOB TrustSec PAC

すべての TrustSec ネットワーク デバイスで、EAP-FAST プロトコルの一部として TrustSec PAC が保持されています。これはセキュアな RADIUS プロトコルでも使用され、ここでは RADIUS 共有秘密が PAC で伝送されるパラメータから作成されます。これらのパラメータの 1 つである発信側 ID には、TrustSec ネットワーク デバイス ID、つまりデバイス ID が保持されます。

デバイスが TrustSec PAC を使用して識別される場合、Cisco ISE でそのデバイス用に設定されているデバイス ID と、PAC の発信側 ID が一致していない場合、認証に失敗します。

一部の TrustSec デバイス（Cisco ASA ファイアウォールなど）では EAP-FAST プロトコルをサポートしていません。したがって、Cisco ISE ではこれらのデバイスを EAP-FAST を介した TrustSec PAC でプロビジョニングできません。代わりに、TrustSec PAC は Cisco ISE 上で生成され、手動でデバイスにコピーされます。そのため、これをアウトオブバンド（OOB）TrustSec PAC 生成と呼びます。

Cisco ISE で PAC を生成すると、暗号キーで暗号化された PAC ファイルが生成されます。

ここでは、次の内容について説明します。

[設定（Settings）] 画面からの TrustSec PAC の生成

[設定（Settings）] 画面から TrustSec PAC を生成できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）]** を選択します。

ステップ 2 左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。

ステップ 3 **[EAP-FAST] > [PAC の生成（Generate PAC）]** を選択します。

ステップ 4 TrustSec PAC を生成します。

[ネットワーク デバイス（Network Devices）] 画面からの TrustSec PAC の生成

[ネットワーク デバイス（Network Devices）] 画面から TrustSec PAC を生成できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）]**

ステップ 2 [追加（Add）] をクリックします。[ネットワーク デバイス（Network Devices）] ナビゲーション ペインのアクション アイコンから [新規デバイスの追加（Add new device）] をクリックすることもできます。

ステップ 3 新規デバイスを追加する場合は、デバイス名を入力します。

ステップ 4 TrustSec デバイスを設定するために [高度な TrustSec 設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 5 [アウトオブバンド（OOB）TrustSec PAC（Out of Band (OOB) TrustSec PAC）] サブ セクションで、[PAC の生成（Generate PAC）] をクリックします。

ステップ 6 次の詳細事項を入力します。

- [PAC 存続可能時間（PAC Time to Live）]：日、週、月、および年の単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。
- [暗号化キー（Encryption Key）]：暗号キーを入力します。キーの長さは 8 ～ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。

  暗号キーを使用して、生成されるファイルの PAC が暗号化されます。このキーは、デバイスで PAC ファイルを復号化する場合にも使用されます。したがって、後で使用できるように管理者が暗号キーを保存しておくことを推奨します。

  [ID（Identity）] フィールドは TrustSec ネットワーク デバイスのデバイス ID を示し、このフィールドには EAP-FAST プロトコルによって発信側 ID が提供されます。ここに入力した ID 文字列がネットワーク デバイスの作成ページの [TrustSec] セクションで定義されたデバイス ID と一致しない場合、認証は失敗します。

  有効期限は、PAC 存続可能時間に基づいて計算されます。

ステップ 7 [PAC の生成（Generate PAC）] をクリックします。

[ネットワーク デバイス リスト（Network Devices List）] 画面からの TrustSec PAC の生成

[ネットワーク デバイス リスト（Network Devices list）] 画面から TrustSec PAC を生成できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）]**

ステップ 2 [ネットワーク デバイス（Network Devices）] をクリックします。

ステップ 3 TrustSec PAC を生成するデバイスの隣にあるチェックボックスをオンにし、[PAC の生成（Generate PAC）] をクリックします。

ステップ 4 フィールドで詳細を提供します。

ステップ 5 [PAC の生成（Generate PAC）] をクリックします。

[プッシュ（Push）] ボタン

出力ポリシーの [プッシュ（Push）] オプションは CoA 通知を開始します。この通知は、Cisco ISE からの出力ポリシー設定変更に関する更新を、ただちに要求するよう TrustSec デバイスに伝えます。

Cisco TrustSec AAA サーバーの設定

AAA サーバーリスト内に、Cisco Trustsec が有効になっている Cisco ISE サーバーのリストを設定すると、Cisco TrustSec デバイスの認証が、これらのサーバーのいずれに対しても実行されます。[プッシュ（Push）] をクリックすると、このリスト内の新しいサーバーが TrustSec デバイスにダウンロードされます。Cisco TrustSec デバイスは、認証を試行するときに、このリストから Cisco ISE サーバーを選択します。最初のサーバーがダウン状態またはビジー状態の場合、Cisco TrustSec デバイスはこのリストにある別の任意のサーバーに対してデバイス自体を認証できます。デフォルトでは、プライマリ Cisco ISE サーバーが Cisco TrustSec AAA サーバーです。より信頼性の高い Cisco TrustSec 環境を構築するために、より多くの Cisco ISE サーバーを設定することをお勧めします。

（注） Cisco ISE プライマリ PAN は、Amazon Web Services（AWS）の Amazon マシンイメージ（AMI）を介して設定されている場合、既知の制限により、不正なホスト名と IP アドレスを持つ Cisco TrustSec AAA サーバーとして自動的に追加されます。[TrustSec AAA サーバー（TrustSec AAA Servers）] ウィンドウで、正しいホスト名と IP アドレスの詳細を入力して Cisco ISE サーバーを追加します。次に、自動的に追加されたサーバーの横にあるチェックボックスをオンにし、[削除（Delete）] をクリックして、[TrustSec AAA サーバー（TrustSec AAA Servers）] ウィンドウから該当サーバーを削除します。AWS を介して設定された Cisco ISE サーバーの詳細については、『Cisco ISE Installation Guide, Release 3.1』の「Install Cisco ISE with Amazon Web Services」の章を参照してください。

このページには、展開内の Cisco TrustSec AAA サーバーとして設定した Cisco ISE サーバーが一覧表示されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [TrustSec AAA サーバー（TrustSec AAA Servers）]**

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 説明に従って値を入力します。

- [名前（Name）]：この AAA サーバーリスト内で Cisco ISE サーバーに割り当てる名前。この名前は、Cisco ISE サーバーのホスト名と異なっていてもかまいません。
- [説明（Description）]：任意の説明。
- [IP]：AAA サーバーリストに追加する Cisco ISE サーバーの IP アドレス。
- [ポート（Port）]：Cisco TrustSec デバイスとサーバー間の通信が行われるポート。デフォルトは 1812 です。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 表示される [AAA サーバー（AAA Servers）] ウィンドウで、[プッシュ（Push）] をクリックします。

次のタスク

セキュリティ グループを設定します。

TrustSec HTTPS サーバー

デフォルトでは、Cisco ISE が RADIUS を使用して Cisco ISE と TrustSec NAD 間で TrustSec 環境データを交換します。HTTPS を使用するように Cisco ISE を設定できます。これにより、RADIUS より高速で信頼性が高くなります。Cisco ISE は、REST API を使用して HTTP 転送を実装します。

HTTPS 転送には次が必要です。

- HTTPS サーバーと TrustSec ネットワークデバイス間でポート 9603 が開いていること。
- PSN に接続するすべてのネットワークデバイス上の HTTPS サーバーのクレデンシャルが一意であること。
- シスコのスイッチがバージョン16.12.2、17.1.1 以降を実行していること。

HTTPS 転送を設定するには、次の手順を実行します。

1. 各ネットワークデバイスで HTTP ファイル転送を有効にし、クレデンシャルを要求します。
2. Cisco ISE で、[TrustSec の全般設定（General TrustSec Settings）] で [ネットワークデバイスの TrustSec REST API サービス] を有効にします。
3. Cisco ISE で、各 PSN のネットワークデバイス定義を編集し、[HTTP REST API を有効にする（Enable HTTP REST API）] をオンにし、ネットワークデバイスの HTTP サーバーへのクレデンシャルを入力します。
4. Cisco ISE で、[TrustSec] > [コンポーネント（Components）] の下でそのネットワークデバイスを TrustSec HTTPs サーバーとして追加します。

（注） HTTPS に対して設定したノードが 1 つのみの場合は、HTTPS 用に設定されていない TrustSec サーバーは [TrustSec サーバー（TrustSec Servers）] リストに表示されません。展開内の他のすべての TrustSec 対応ノードを HTTPS 用に設定する必要があります。HTTPS 用に PSN が設定されていない場合は RADIUS が使用され、すべての Cisco ISE がこの TrustSec 展開のすべての PSN ノードをリストします。

設定が完了すると、Cisco ISE は [TrustSec] > [ネットワークデバイス（Network Devices）] で TrustSec 環境データに設定されているサーバーのリストを返します。

デバッグ

デバッグでの ERS を有効にします。この設定により、すべての ERS トラフィックがログに記録されます。ログファイルのオーバーロードを回避するために、この設定は 30 分以上有効にしたままにしないでください。

追加の監査情報を有効にするには、[TrustSec]>[設定（Settings）]>[TrustSec の全般設定（General TrustSec Settings）] の [ネットワークデバイス用 TrustSec REST API サービス（TrustSec REST API Service for Network Devices）] の下にある [要求ペイロードの本文を含める（Include request payload body）] をオンにします。一般 TrustSec の設定

Cisco ISE TrustSec HTTPS サーバーへの外部サーバーの追加

HTTPS サーバーリストに 1 つ以上の外部サーバーを追加することで、HTTPS TrustSec サービスのロードバランシングを実現できます。

外部サーバーは、次のいずれかの方法でロードバランサとして機能できます。

- **SSL 終了**

  このセットアップでは、外部サーバーは、TrustSec 対応ネットワークデバイスによって開始された SSL 接続のターミネーションポイントです。同時に、サーバーは PSN ノードとの独自の SSL セッションを確立し、ネットワークデバイスと特定の PSN ノードの間で情報をリレーするプロキシとして機能します。したがって外部サーバーは、その IP アドレス、FQDN、またはその両方を含む証明書をホストする必要があります。この証明書は、ネットワークデバイスによって信頼されている必要があります。

  外部サーバーと PSN ノード間の SSL セッションの場合、外部サーバーは PSN ノードからの証明書を信頼する必要があります。この信頼の確立は、この目的で使用される製品に応じて、外部サーバーのデバイス固有の設定側面になります。

- **SSL パススルー**

  このセットアップでは、外部サーバーは IP アドレス変換デバイスとして機能し、ネットワークデバイスと PSN ノード間の通信を通過させるだけです。結果として外部サーバーには証明書が存在しないため、ネットワークデバイスと PSN ノードの間で証明書の信頼を確立させる必要があります。

ネットワークデバイスは外部サーバーの IP アドレスを使用して SSL セッションを確立するため、この目的で PSN ノードが使用する証明書には、外部サーバーの IP アドレスが含まれている必要があります。これは、ワイルドカード証明書またはユニバーサル証明書を使用することで実現できます。ユニバーサル証明書のSANエントリとして、複数のFQDN、IP アドレス、またはその両方を追加できます。

選択した展開オプションに関係なく、外部サーバーがネットワークデバイスから特定の PSN ノードへの通信を行う際は常に、その接続の永続性を確保する必要があります。つまり、その通信のすべてを、そのネットワークデバイスとその特定の PSN ノード間のみで行う必要があります。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [TrustSecサーバー（TrustSec Servers）] > [HTTPSサーバー（HTTPS Servers）]**

ステップ 2 [外部サーバーの追加（Add External Server）] をクリックします。

ステップ 3 次の詳細を入力します。

- **名前**：Cisco ISE HTTPS サーバーリストに追加する外部サーバーの名前。
- **ホスト名（FQDN）**：外部サーバーのホスト名。

  （注） 外部サーバーのホスト名またはIPアドレスのどちらを指定するか選択できます。

- **説明**：任意の説明。
- **ポート**：Cisco TrustSec デバイスと外部サーバー間の通信が行われるポート。
- **IPアドレス**：Cisco ISE HTTPS サーバーリストに追加する外部サーバーの IP アドレス。

ステップ 4 [証明書の追加（Add Certificate）] をクリックします。

外部サーバーでロードバランシング操作とセキュア通信を有効にするには、SSL 証明書が必要です。ルート証明書から始まる信頼チェーンの順序に従って、証明書を追加します。

ステップ 5 [証明書名（Certificate name）] フィールドに名前を入力します。

ステップ 6 [証明書（Certificate）] フィールドに SSL 証明書を追加します。これを行うには、ファイルを添付するか、クリップボードから証明書を貼り付けます。

ステップ 7 [保存（Save）] をクリックします。

通知バーに、次のメッセージを含むダイアログボックスが表示されます。

ネットワークデバイスに通知されていない TrustSec 設定の変更があります。関連するネットワークデバイスにこれらの変更について通知するには、[プッシュ（Push）] ボタンをクリックします。

ステップ 8 [プッシュ（Push）] をクリックします。

関連するネットワークデバイスに、これらの設定変更が通知されます。

これで、Cisco ISE HTTPS サーバーリストにその外部サーバーが表示されるようになります。

セキュリティ グループの設定

セキュリティ グループ（SG）またはセキュリティ グループ タグ（SGT）は、TrustSec ポリシー設定で使用される要素です。SGT は、パケットが信頼ネットワーク内を移動する場合に付加されます。これらのパケットは、信頼ネットワークに入ったとき（入力）にタグ付けされ、信頼ネットワークから離れるとき（出力）にタグ解除されます。

SGT は順次的な方法で生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。Cisco ISE は、SGT の生成時に予約済みの番号をスキップします。

TrustSec サービスはこれらの SGT を使用して、出力時に TrustSec ポリシーを適用します。

管理者ポータルで次のページからセキュリティ グループを設定できます。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワーク センター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティ グループ（Security Groups）]**
- **[設定（Configure）] > [新規セキュリティ グループの作成（Create New Security Group）]** の出力ポリシーページから直接。

[プッシュ（Push）] ボタンをクリックすると、複数の SGT を更新した後に、環境 CoA 通知を開始できます。この環境 CoA 通知はすべての TrustSec ネットワーク デバイスに送信され、ポリシー/データ リフレッシュ要求を開始することを強制します。

（注） [プッシュ（Push）] または [展開（Deploy）] ボタンを頻繁に使用することは推奨されません。マトリックスまたは SGACL に変更がある場合、次の展開操作を実行する前に、保留中の展開要求の通知バーを確認します。

Cisco ISE でのセキュリティグループの管理

前提条件

セキュリティグループを作成、編集、または削除するには、ネットワーク管理者またはシステム管理者である必要があります。

セキュリティグループの追加

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）]** を選択します。
2. [追加（Add）] をクリックして新規セキュリティ グループを追加します。
3. 新規セキュリティ グループの名前と説明（オプション）を入力します。
4. タグ値を入力します。タグ値は、手動で入力したり、自動生成されるようにしたり設定できます。またSGTの範囲を予約できます。これは、から設定できます。[一般TrustSecの設定（General TrustSec Settings）] ページ（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）]）。
5. [保存（Save）] をクリックします。

セキュリティグループの削除

送信元または宛先で使用中のセキュリティグループは削除できません。Cisco ISEの機能にマッピングされるデフォルトグループも削除できません。

- BYOD
- ゲスト
- TrustSec デバイス
- 不明

Cisco ISE へのセキュリティ グループのインポート

カンマ区切り形式（CSV）ファイルを使用して Cisco ISE ノードにセキュリティ グループをインポートできます。Cisco ISE にセキュリティ グループをインポートする前に、テンプレートを更新する必要があります。同じリソースタイプのインポートを同時に実行できません。たとえば、2つの異なるインポートファイルから同時にセキュリティグループをインポートできません。

管理者ポータルからCSVテンプレートをダウンロードし、テンプレートにセキュリティグループの詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

セキュリティ グループのインポート中、Cisco ISE で最初のエラーが発生した場合、インポート プロセスを停止できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 5 [インポート（Import）] をクリックします。

Cisco ISE からのセキュリティ グループのエクスポート

Cisco ISE で設定されたセキュリティ グループを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのセキュリティ グループをインポートできます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）] を選択します。

ステップ 2 [エクスポート（Export）] をクリックします。

ステップ 3 セキュリティ グループをエクスポートするには、次のいずれかを実行できます。

- エクスポートするグループの隣にあるチェックボックスをオンにし、**[エクスポート（Export）]** > **[選択済みをエクスポート（Export Selected）]** を選択します。
- **[エクスポート（Export）]** > **[すべてエクスポート（Export All）]** を選択して、定義されたすべてのセキュリティ グループをエクスポートします。

ステップ 4 ローカル ハード ディスクに export.csv ファイルを保存します。

IP SGT スタティック マッピングの追加

IP-SGT スタティックマッピングを使用して、TrustSec デバイスと SGT ドメインに統一された方法でマッピングを展開することができます。新しい IP-SGT スタティックマッピングを作成するときに、このマッピングを展開する SGT ドメインとデバイスを指定できます。また、IP-SGT マッピングをマッピング グループに関連付けることもできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[TrustSec]** > **[コンポーネント（Components）]** > **[IP SGT スタティックマッピング（IP SGT Static Mapping）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 表示される [新規（New）] 領域で、ドロップダウンリストから [IP アドレス（IP Address）] または [ホスト名（Hostname）] を選択し、その横のフィールドに対応する値を入力します。

次の手順の [SGTに個別にマッピング（Map to SGT individually）] オプションで、マッピング先の SGT ドメインを指定できます。ただし、この手順で[ホスト名（Hostname）]を選択した場合、[SGTドメインに送信（Send to SGT Domain）] フィールドにはアクセスできません。次の手順で SGT ドメインを追加するには、ここで [IPアドレス（IP Address）] を選択する必要があります。

ステップ 4 既存のマッピング グループを使用する場合は、[マッピング グループに追加（Add to a Mapping Group）] をクリックして、[マッピング グループ（Mapping Group）] ドロップダウン リストから必要なグループを選択します。

この IP アドレス/ホスト名を SGT に個別にマッピングする場合は、[SGT に個別にマッピング（Map to SGT Individually）] をクリックして以下を実行します。

- [SGT] ドロップダウン リストから SGT を選択します。
- ドロップダウンリストからマッピングするための仮想ネットワークを選択します。
- マッピングを展開する必要がある SXP VPN グループを選択します。
- このマッピングを展開するデバイスを指定します。すべての TrustSec デバイス、選択されたネットワーク デバイス グループ、または選択されたネットワーク デバイスにマッピングを展開できます。

ステップ 5 [保存（Save）] をクリックします。

IP SGT スタティック マッピングの展開

マッピングを追加した後、[展開（Deploy）] オプションを使用して、対象のネットワーク デバイスでこのマッピングを展開します。マッピングをすでに保存している場合でも、これを明示的に行う必要があります。デバイスの展開ステータスを確認するには、[ステータスを確認（Check Status）] をクリックします。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）] の順に選択します。**

ステップ 2 展開するマッピングの近くにあるチェックボックスをオンにします。すべてのマッピングを展開する場合は、一番上のチェックボックスをオンにします。

ステップ 3 [展開（Deploy）] をクリックします。

すべての TrustSec デバイスが [IP SGTスタティックマッピングの展開（Deploy IP SGT Static Mapping）] ウィンドウにリストされます。

ステップ 4 選択したマッピングの展開先となる適切なデバイスまたはデバイス グループの横にあるチェックボックスをオンにします。

- すべてのデバイスを選択する場合は、一番上のチェックボックスをオンにします。
- フィルタリング オプションを使用して、特定のデバイスを検索します。
- デバイスを何も選択しない場合は、選択したマッピングがすべての TrustSec デバイスに展開されます。
- 新しいマッピングを展開するデバイスを選択すると、新しいマッピングの影響を受ける**すべて**のデバイスが ISE によって選択されます。

ステップ 5 [展開（Deploy）] をクリックします。[展開（Deploy）] ボタンをクリックすると、新しいマップによって影響を受けるすべてのデバイスのマッピングが更新されます。

[展開ステータス（Deployment Status）] ウィンドウに、デバイスが更新される順序と、エラーのために（またはデバイスが到達不能なために）更新されないデバイスが示されます。展開が完了すると、このウィンドウに、正常に更新されたデバイスの合計数と更新されないデバイスの数が表示されます。

[IP SGTスタティックマッピング（IP SGT Static Mapping）] ページの [ステータスを確認（Check Status）] オプションを使用して、特定のデバイスの同じ IP アドレスに複数の異なる SGT が割り当てられているかどうかを確認します。このオプションを使用すると、競合するマッピングがあるデバイス、複数の SGT にマッピングされている IP アドレス、および同じ IP アドレスに割り当てられている複数の SGT を見つけることができます。展開でデバイス グループ、FQDN、ホスト名、または IPv6 アドレスが使用される場合でも、[ステータスを確認（Check Status）] オプションを使用できます。競合するマッピングを展開する前に、それらのマッピングを削除するか、展開の範囲を変更する必要があります。

IP SGT 静的マッピングでではIPv6 アドレスを使用できます。SSH または SXP を使用して、特定のネットワーク デバイスまたはネットワーク デバイス グループにこれらのマッピングを伝達できます。

FQDN とホスト名が使用される場合、Cisco ISE はマッピングを展開して展開ステータスを検査する際に、PAN および PSN ノード内の対応する IP アドレスを検索します。

[一般TrustSecの設定（General TrustSec Settings）] ウィンドウの [ホスト名のIP SGTスタティックマッピング（IP SGT Static Mapping of Hostnames）] オプションを使用して、DNS クエリによって返される IP アドレス用に作成されるマッピング数を指定します。次のオプションのいずれかを選択します。

- DNSクエリによって返されるすべてのIPアドレスに対してマッピングを作成する（Create mappings for all IP addresses returned by a DNS query）。
- DNSクエリによって返される最初のIPv4アドレスおよび最初のIPv6アドレスに対してのみマッピングを作成する（Create mappings only for the first IPv4 address and the first IPv6 address returned by a DNS query）。

Cisco ISE への IP SGT スタティック マッピングのインポート

CSV ファイルを使用して IP SGT マッピングをインポートできます。

また、管理者ポータルからCSVテンプレートをダウンロードし、マッピングの詳細を入力し、CSV ファイルとしてテンプレートを保存して、Cisco ISE にインポートすることができます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）] の順に選択します。**

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [アップロード（Upload）] をクリックします。

Cisco ISE からの IP SGT スタティック マッピングのエクスポート

IP SGT マッピングを CSV ファイルの形式でエクスポートできます。このファイルを使用して、これらのマッピングを別の Cisco ISE ノードにインポートできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）]** の順に選択します。

ステップ 2 次のいずれかを実行します。

- エクスポートするマッピングの隣にあるチェックボックスをオンにし、[エクスポート（Export）]>[選択済み（Selected）] を選択します。
- [エクスポート（Export）]>[すべて（All）] を選択して、すべてのマッピングをエクスポートします。

ステップ 3 ローカル ハード ディスクに mappings.csv ファイルを保存します。

SGT マッピング グループの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGT スタティックマッピング（IP SGT Static Mapping）] > [グループ管理（Manage Groups）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 マッピング グループの名前と説明を入力します。

ステップ 4 次の手順を実行します。

- [SGT] ドロップダウン リストから SGT を選択します。
- ドロップダウンリストからマッピングを行う仮想ネットワークを選択します。
- マッピングを展開する必要がある SXP VPN グループを選択します。
- マッピングを展開するデバイスを指定します。すべての TrustSec デバイス、選択されたネットワーク デバイス グループ、または選択されたネットワーク デバイスにマッピングを展開できます。

ステップ 5 [保存（Save）] をクリックします。

あるマッピング グループから別のマッピング グループに IP SGT マッピングを移動できます。

また、マッピングおよびマッピング グループを更新または削除できます。マッピングまたはマッピング グループを更新するには、更新するマッピングまたはマッピング グループの横にあるチェック ボックスにマークを付けてから、[編集（Edit）] をクリックします。マッピングまたはマッピング グループを削除するには、削除するマッピングまたはマッピング グループの横にあるチェック ボックスにマークを付けてから、[ごみ箱（Trash）]>[選択済み（Selected）] の順にクリックします。マッピング グループが削除されると、そのグループ内の IP SGT マッピングも削除されます。

セキュリティ グループ アクセス コントロール リストの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループACL（Security Group ACLs）]** を選択します。

ステップ 2 [追加（Add）] をクリックして新規セキュリティ グループ ACL を作成します。

ステップ 3 次の情報を入力します。

- [名前（Name）]：SGACL の名前
- [説明（Description）]：SGACL の説明（任意）
- [IP バージョン（IP Version）]：この SGACL でサポートされる IP バージョン：
  - [IPv4]：IP バージョン 4（IPv4）がサポートされます
  - [IPv6]：IP バージョン 6（IPv6）がサポートされます
  - [非認識（Agnostic）]：IPv4 と IPv6 の両方がサポートされます
- セキュリティ グループ ACL の内容：アクセス コントロール リスト（ACL）コマンド。次に例を示します。

  permit icmp

  deny ip

  ISE 内では SGACL 入力の構文が検査されません。スイッチ、ルータ、アクセス ポイントをエラーなく適用できるように、正しい構文を確実に使用してください。デフォルト ポリシーを **permit IP**、**permit ip log**、**deny ip**、または **deny ip log** として設定できます。TrustSec ネットワーク デバイスでは、デフォルト ポリシーを特定セルのポリシーの最後に付加します。

参考用に SGACL の 2 つの例を示します。どちらにも最終的な catch-all ルールが含まれています。最初の例では、最終的な catch-all ルールとして拒否し、2 番目の例では許可します。

Permit_Web_SGACL

```
permit tcp dst eq 80
permit tcp dst eq 443
deny ip
```

Deny_JumpHost_Protocols

```
deny tcp dst eq 23
deny tcp dst eq 23
deny tcp dst eq 3389
permit ip
```

次の表に、IOS、IOS XE、NS OS オペレーティング システム用の SGACL の構文を示します。

SGACL CLI と ACE	**IOS、IOS XE、NX OS で共通の構文**
config acl	deny、exit、no、permit
deny permit	ahp、eigrp、gre、icmp、igmp、ip、nos、ospf、pcp、pim、tcp、udp
deny tcp deny tcp src deny tcp dst	dst、log、src
deny tcp dst eq deny tcp src eq	range 0 65535
deny udp deny udp src deny udp dest	Dst、log、src
deny tcp dst eq www deny tcp src eq www	range 0 65535

（注） Hypens は一部のシスコのスイッチでは許可されていません。したがって、`permit dst eq 32767-65535` は有効ではありません。`permit dst eq range 32767 65535` を使用します。一部の Cisco スイッチでは、コマンド構文に eq を含める必要がありません。したがって、それらのスイッチでは permit dst eq 32767-65535 は無効です。代わりに、permit dst 32767-65535 または permit dst range 32767 65535 を使用します。

ステップ 4 [プッシュ（Push）] をクリックします。
[プッシュ（Push）] オプションは CoA 通知を開始します。この通知は、Cisco ISE からの設定変更に関する更新をただちに要求するよう TrustSec デバイスに伝えます。

（注） Cisco ISE では次の事前定義済み SGACL を使用します：許可 IP、許可 IP ログ、拒否 IP、または拒否 IP ログ。これらの SGACL で GUI または ERS API を使用すると、TrustSec マトリックスを設定できます。これらの SGACL は GUI のセキュリティ グループ ACL リストのページに表示されませんが、ERS API を使用して利用可能な SGACL（ERS getAll 呼び出し）を表示すると表示されます。

出力ポリシー

出力テーブルには、送信元 SGT および宛先 SGT が、予約済みのものもそうでないものもあわせてリストされます。また、このページでは、出力テーブルをフィルタリングして特定のポリシーを表示することや、これらのプリセットフィルタを保存することもできます。送信元SGTから宛先SGTに到達しようとすると、TrustSec対応デバイスは、出力ポリシーで定義されているTrustSecポリシーに基づいてSGACLを適用します。Cisco ISEはポリシーを作成してプロビジョニングします。

TrustSecポリシーの作成に必要な基本的構築ブロックであるSGTおよびSGACLを作成した後に、SGACLを送信元SGTおよび宛先SGTに割り当てることによって、それらの関係を確立できます。

送信元 SGT と宛先 SGT のそれぞれの組み合わせが、出力ポリシーのセルになります。

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] の順に選択します。**

それぞれ異なる 3 つの方法で出力ポリシーを表示できます。

- 送信元ツリー ビュー
- 宛先ツリー ビュー
- マトリクス ビュー

送信元ツリー ビュー

送信元ツリー ビューには、簡潔で組織化された送信元 SGT のビューが折りたたまれた状態で表示されます。送信元 SGT を展開すると、選択した送信元 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、宛先 SGT にマッピングされている送信元 SGT のみが表示されます。特定の送信元 SGT を展開すると、この送信元 SGT にマッピングされているすべての宛先 SGT とその対応するポリシー（SGACL）がテーブルに表示されます。

一部のフィールドの横には、3 つのドット（...）が表示されます。これは、セルにより多くの情報が含まれていることを示しています。カーソルを 3 個のドットの上に置くと、クイック ビュー ポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上

に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

宛先ツリー ビュー

宛先ツリー ビューには、簡潔で組織化された宛先 SGT のビューが折りたたまれた状態で表示されます。宛先 SGT を展開すると、選択した宛先 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、送信元 SGT にマッピングされている宛先 SGT のみが表示されます。特定の宛先 SGT を展開すると、この宛先 SGT にマッピングされているすべての送信元 SGT と対応するポリシー（SGACL）が表に示されます。

一部のフィールドの横には、3 つのドット（...）が表示されます。これは、セルにより多くの情報が含まれていることを示しています。カーソルを 3 個のドットの上に置くと、クイック ビュー ポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

マトリクス ビュー

出力ポリシーのマトリクス ビューは、スプレッドシートに似ています。ここには2つの軸があります。

- 送信元軸：垂直軸にはすべての送信元 SGT がリストされます。
- 宛先軸：水平軸にはすべての宛先 SGT がリストされます。

送信元 SGT と宛先 SGT のマッピングが、セルとして示されます。セルにデータが含まれている場合、対応する送信元 SGT と宛先 SGT 間にマッピングがあるということになります。マトリクス ビューには 2 つのタイプのセルがあります。

- マッピングされたセル：送信元SGTと宛先SGTのペアが、順序付けされたSGACLのセットに関連付けられ、特定のステータスになっている場合。
- マッピングされていないセル：送信元 SGT と宛先 SGT のペアが、SGACL に関連付けられてなく、特定のステータスになっていない場合。

出力ポリシー セルには、送信元 SGT、宛先 SGT、最終的な catch-all ルールが 1 つのリストとして SGACL の下にカンマで区切られて表示されます。最終的な catch-all ルールは、[なし（None）] に設定されている場合には表示されません。マトリクス内の空のセルは、マッピングされていないセルを示します。

出力ポリシーのマトリクス ビューでは、マトリクスをスクロールして目的のセルのセットを表示できます。ブラウザがマトリクスデータ全体を一度にロードすることはありません。ブラウザは、ユーザーがスクロールした領域に移入されるデータをサーバーに要求します。これにより、メモリのオーバーフローとパフォーマンスの問題が回避されます。

[表示（View）] ドロップダウン リストで次のオプションを使用して、マトリックス ビューを変更できます。

- [SGACL名ありで簡易設定（Condensed with SGACL names）]：このオプションを選択すると、空のセルは非表示になり、SGACL 名がセルに表示されます。
- [SGACL名なしで簡易設定（Condensed without SGACL names）]：空のセルは非表示になり、SGACL 名はセルに表示されません。このビューは、より多くのマトリックス セルを表示し、色、パターンおよびアイコン（セルのステータス）を使用して、セルの内容を区別する場合に便利です。
- [SGACL名ありでフル（Full with SGACL names）]：このオプションを選択すると、左側と上側のメニューは非表示になり、SGACL 名がセルに表示されます。
- [SGACL名なしでフル（Full without SGACL names）]：このオプションを選択すると、マトリックスは全画面モードで表示され、SGACL 名はセルに表示されません。

ISE では、カスタム ビューを作成し、名前を付け、保存できます。カスタム ビューを作成するには、[表示（Show）] > [カスタムビューの作成（Create Custom View）] の順に選択します。また、ビューの条件を更新したり、未使用のビューを削除することもできます。

[マトリックス（Matrix）] ビューは、[ソース（Source）] ビューおよび [送信先（Destination）] ビューと同じ GUI 要素を持っています。ただし、次の追加要素を含みます。

マトリクスの次元

次元ビューの [次元（Dimension）] ドロップダウン リストでは、マトリクスの次元を設定することができます。

カスタム ビューの作成

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [マトリックスビュー（Matrix View）] ページで、[表示（Show）] ドロップダウン リストから [カスタム ビューの作成（Create Custom View）] オプションを選択します。

ステップ 2 [ビューの編集（Edit View）] ダイアログボックスで、次の詳細情報を入力します。

- [ビュー名（View Name）]：カスタム ビューの名前を入力します。
- [送信元セキュリティグループ（Source Security Groups）]：カスタム ビューに含める SGT を [表示（Show）] 転送ボックスに移動します。
- [宛先関連の表示（Show Relevant for Destination）]：[送信元セキュリティグループの表示（Source Security Group Show）] 転送ボックス内での選択内容を上書きして、[宛先セキュリティグループの非表示（Destination Security Group Hide）] 転送ボックス内のすべてのエントリをコピーするには、このチェックボックスをオンにします。200 を超えるエントリがある場合、データはコピーされず、警告メッセージが表示されます。
- [着信先セキュリティグループ（Destination Security Groups）]：カスタム ビューに含める SGT を [表示（Show）] 転送ボックスに移動します。

- [送信元関連の表示（Show Relevant for Source）]：[宛先セキュリティグループの表示（Destination Security Group Show）] 転送ボックス内での選択内容を上書きして、[送信元セキュリティグループの非表示（Source Security Group Hide）] 転送ボックス内のすべてのエントリをコピーするには、このチェックボックスをオンにします。
- [次によってマトリックスをソートする（Sort Matrix By）]：次のいずれかのオプションを選択します。
  - 手動順序（Manual Order）
  - タグ番号（Tag Number）
  - SGT名（SGT Name）

ステップ 3 [保存（Save）] をクリックします。

マトリクス操作

マトリクスでの移動

カーソルでマトリクス コンテンツ領域をドラッグするか、または水平および垂直スクロールバーを使用して、マトリクス内を移動できます。セルをクリックしたままにし、マトリクス コンテンツ全体を任意の方向にドラッグできます。送信元および宛先のバーがセルと一緒に移動します。セルを選択すると、マトリクス ビューによってそのセルと対応する行（送信元 SGT）およびカラム（宛先 SGT）が強調表示されます。選択したセルの座標（送信元 SGT および宛先 SGT）がマトリクス コンテンツ領域の下に表示されます。

マトリクスでのセルの選択

マトリクス ビューでセルを選択するには、該当のセルをクリックします。選択したセルが別の色で表示され、送信元 SGT および宛先 SGT が強調表示されます。セルをもう一度クリックするか、または別のセルを選択することで、セルの選択を解除できます。複数セルの選択は、マトリクス ビューでは許可されていません。セルをダブルクリックして、セルの設定を編集します。

出力ポリシーの SGACL の設定

[出力ポリシー（Egress Policy）] ページでセキュリティ グループ ACL を直接作成できます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] の順に選択します。

ステップ 2 [送信元ツリービュー（Source Tree View）] または [宛先ツリービュー（Destination Tree View）] ページから、[設定（Configure）] > [新しいセキュリティグループACLの作成（Create New Security Group ACL）] を選択します。

ステップ 3 必要な詳細を入力し、[送信（Submit）] をクリックします。

ワーク プロセスの設定

始める前に

次のタスクを実行するには、スーパー管理者である必要があります。

ステップ 1 [ワーク センター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ワーク プロセスの設定（Work Process Settings）] の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 単一マトリックス（Single Matrix）：TrustSec ネットワーク上のすべてのデバイスに対してポリシー マトリックスを 1 つのみ作成するには、このオプションを選択します。
- 複数マトリックス（Multiple Matrices）：さまざまなシナリオで複数のポリシー マトリックスを作成できるようにします。これらのマトリックスを使用して、さまざまなネットワーク デバイスに異なるポリシーを展開できます。

  （注） マトリックスは独立していて、各ネットワーク デバイスを 1 つのマトリックスのみに割り当てることができます。

- 承認プロセス付き実稼働およびステージング マトリックス（Production and Staging Matrices with Approval Process）：ワークフロー モードを有効にするには、このオプションを選択します。エディタ ロールおよび承認者ロールに割り当てられるユーザーを選択します。ユーザーは、ポリシー管理者グループおよびスーパー管理者グループからのみ選択できます。ユーザーはエディタ ロールおよび承認者ロールの両方に割り当てることはできません。

  エディタまたは承認者ロールが割り当てられたユーザーの電子メール アドレスが設定されていることを確認します。設定されていないと、ワークフロー プロセスに関する電子メール通知がこれらのユーザーに送信されません。

  ワークフロー モードを有効にすると、エディタのロールが割り当てられたユーザーは、ステージング マトリックスを作成し、ステージング ポリシーを展開するデバイスを選択して、承認者に承認を求めるステージング ポリシーを送信できます。承認者ロールが割り当てられたユーザーは、ステージング ポリシーを確認し、要求を承認または拒否することができます。ステージング ポリシーが承認者によって確認され、承認された後でのみ、ステージング ポリシーを選択したネットワーク デバイスに展開できます。

ステップ 3 DEFCON マトリックスを作成する場合は、[DEFCON を使用する（Use DEFCONS）] チェックボックスをオンにします。

DEFCONS マトリックスは、ネットワーク セキュリティ侵害の発生時に簡単に展開できるスタンバイ ポリシー マトリックスです。

シビラティ（重大度）レベル [重大（Critical）]、[深刻（Severe）]、[実質的（Substantial）]、および [適度（Moderate）] の DEFCON マトリックスを作成できます。

DEFCONマトリックスがアクティブになると、対応するDEFCONポリシーがすべてのTrustSecネットワーク デバイスにすぐに展開されます。ネットワーク デバイスからDEFCONポリシーを削除するには、非アクティブ化オプションを使用できます。

ステップ4 **[保存（Save）]** をクリックします。

[マトリックス登録（Matrices Listing）] ページ

TrustSecポリシーマトリックスとDEFCONマトリックスは、[マトリックス登録（Matrices Listing）] ページに表示されます。Cisco ISE GUIで [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス登録（Matrices List）]** を選択します。各マトリックスに割り当てられているデバイスの数を確認することもできます。

（注） [マトリックス登録（Matrices Listing）] ページは、単一マトリックス モードが有効であり、DEFCONマトリックス オプションが無効な場合は表示されません。

[マトリックス登録（Matrices Listing）] ページからは、次のことが行えます。

- 新しいマトリックスの追加
- 既存のマトリックスの編集
- マトリックスの削除
- 既存のマトリックスの複製
- マトリックスへのNADの割り当て

[NADの割り当て（Assign NADs）] オプションを使用して、マトリックスにNADを割り当てることができます。手順は次のとおりです。

1. [ネットワーク デバイスの割り当て（Assign Network Devices）] ウィンドウで、マトリックスに割り当てるネットワーク デバイスを選択します。フィルタ オプションを使用してネットワーク デバイスを選択することもできます。
2. [マトリックス（Matrix）] ドロップダウン リストから、マトリックスを選択します。既存のすべてのマトリックスとデフォルトのマトリックスがこのドロップダウン リストに表示されます。

デバイスをマトリックスに割り当てたら、[プッシュ（Push）] をクリックし、TrustSecの設定変更を該当するネットワーク デバイスに通知します。

[マトリックス登録（Matrices Listing）] ページで作業を行うときは、次の点に注意してください。

- デフォルトのマトリックスを編集、削除、名前変更することはできません。
- 新しいマトリックスを作成する際は、空のマトリックスから開始することや、既存のマトリックスからポリシーをコピーすることができます。
- マトリックスを削除すると、そのマトリックスに割り当てられている NAD が自動的にデフォルトのマトリックスに移動します。
- 既存のマトリックスをコピーするとマトリックスのコピーが作成されますが、デバイスはコピーされたマトリックスに自動的に割り当てられません。
- 複数マトリックスモードでは、すべてのデバイスが初期段階でデフォルトのマトリックスに割り当てられます。
- 複数マトリックス モードでは、一部の SGACL がマトリックス間で共有されることがあります。この場合、SGACL コンテンツを変更すると、セルにその SGACL が含まれているすべてのマトリックスに影響します。
- 複数マトリックスは、ステージングが進行中のときに有効にすることはできません。
- 複数マトリックス モードから単一マトリックス モードに変更すると、すべての NAD が自動的にデフォルトのマトリックスに割り当てられます。
- 現在有効になっている場合は、DEFCON マトリックスを削除することはできません。

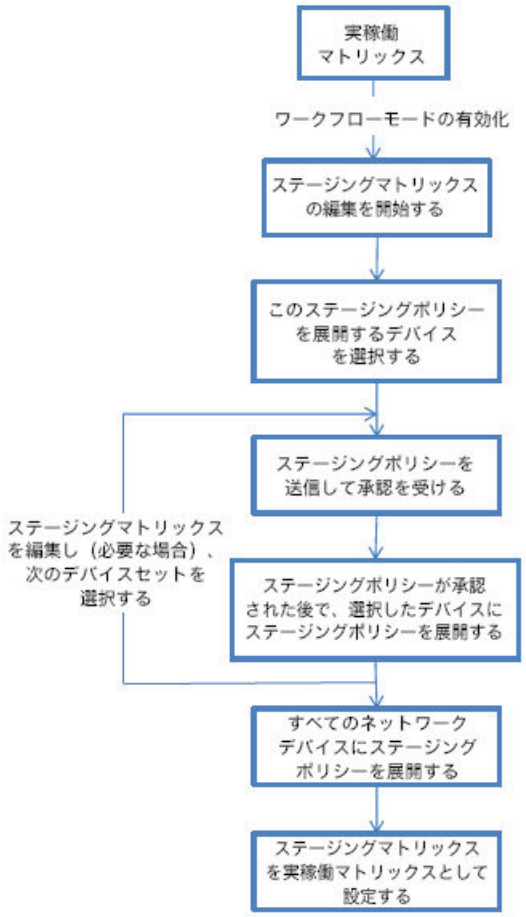
TrustSec マトリックス ワークフロー プロセス

マトリクスのワークフロー機能は、すべてのネットワーク デバイスにポリシーを導入する前に、このマトリックスのドラフト版（ステージング マトリックスとも呼ばれます）を使用して、デバイスの制限されたセットで新しいポリシーをテストできます。承認のためのステージング ポリシーを送信し、承認されると、選択したネットワーク デバイスにステージング ポリシーを導入できます。この機能により、必要に応じて、デバイスの制限されたセットへの新しいポリシーの導入、適切に機能しているかの確認、変更を行うことができます。次の一連のデバイスまたはすべてのデバイスにポリシーを適用し続けることもできます。ステージング ポリシーがすべてのネットワーク デバイスに導入されると、ステージング マトリックスは新たな実稼働マトリックスとして設定できます。

ワークフロー モードを有効にすると、エディタ ロールに割り当てられたユーザーは、ステージングマトリクスを作成し、マトリクスセルを編集できます。ステージングマトリックスは、TrustSec ネットワークに現在展開されている実稼働マトリックスのコピーです。エディタは、ステージング ポリシーを展開し、承認のために承認者にステージング ポリシーを送信するデバイスを選択できます。承認者ロールが割り当てられたユーザーは、ステージング ポリシーを確認し、要求を承認または拒否することができます。ステージング ポリシーが承認者によって確認され、承認された後でのみ、ステージング ポリシーを選択したネットワーク デバイスに展開できます。

次の図で、ワークフロー プロセスについて説明します。

図 *64 :* マトリックス ワークフロー プロセス



ネットワーク管理者ユーザーは、[ワークフロープロセス（Workflow Process）] ページで、エディタおよび承認者ロールに割り当てられたユーザーを選択できます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ワークフロープロセス（Workflow Process）]** の順に選択します。

ステージング ポリシーが選択されたデバイスに導入された後では、SGT および SGACL を編集できませんが、マトリクスセルは編集できます。設定の差分レポートを使用して、実稼働マトリックスとステージングマトリックスの違いを追跡できます。また、ステージング処理中にそのセルへの変更を表示するには、セルで [デルタ（Delta）] アイコンをクリックします。

次の表では、ワークフローのさまざまな段階を説明します。

ステージ	説明
ステージングを編集中（Staging in Edit）	エディタがステージング マトリックスの編集を開始すると、マトリックスは[ステージングを編集中（Staging in Edit）] 状態に移行します。ステージングマトリックスを編集したら、エディタは、新しいステージング ポリシーを導入するデバイスを選択できます。
ステージングの承認待ち（Staging Awaiting Approval）	マトリックスの編集後、エディタは確認および承認を受けるために承認者にステージング マトリックスを送信します。 承認のためにステージング マトリックスを送信する時に、エディタは承認者に送信される電子メールにコメントを追加できます。 承認者は、ステージング ポリシーを確認し、要求を承認または拒否することができます。承認者は、選択したネットワーク デバイスと設定の差分レポートを表示できます。要求の承認または拒否時に、承認者はエディタに送信される電子メールにコメントを追加できます。 エディタはステージング ポリシーがどのネットワーク デバイスにも導入されていなければ承認リクエストをキャンセルできます。
展開の承認取得済み（Deploy Approved）	承認者が要求を承認すると、ステージング マトリックスは [展開の承認取得済み（Deploy Approved）] 状態に移行します。要求が拒否された場合、マトリックスは[ステージングを編集中（Staging in Edit）] 状態に戻されます。 エディタはステージング ポリシーが承認者によって承認された後でのみ、ステージング ポリシーを選択したネットワーク デバイスに導入できます。

ステージ	説明
一部展開済み（Partially deployed）	ステージング マトリックスが選択したデバイスに展開された後、マトリックスは[一部展開済み（Partially deployed）] 状態に移行します。マトリックスは、ステージング ポリシーがすべてのネットワーク デバイスに導入されるまで、[一部展開済み（Partially deployed）] ステージのままです。 このステージでは、SGT および SGACL を編集できませんが、マトリクス セルは編集できます。 最新のポリシーが導入されていないデバイス（同期していないデバイス）は、[ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウにオレンジ色（イタリック体）で表示されます。このステータスは、導入の進捗状況のステータス バーにも表示されます。エディタはこれらのデバイスを選択し、さまざまな導入サイクルで更新されたデバイスを同期するように承認を要求できます。
完全に展開済み（Fully deployed）	上記の手順は、ステージング ポリシーがすべてのネットワーク デバイスに展開されるまで繰り返されます。ステージング マトリックスをすべてのネットワーク デバイスに展開する場合、承認者はステージング マトリックスを実稼働マトリックスとして設定できます。 実稼働マトリックスをステージング マトリックスに置き換えた後では、実稼働マトリックスの以前のバージョンへのロールバックはできないため、新たな実稼働マトリクスとしてステージング マトリクスを設定する前に実稼働マトリクスのコピーを取得しておくことをお勧めします。

[ワークフロー（Workflow）] ドロップダウン リストに表示されるオプションは、ワークフローの状態とユーザー ロール（エディタまたは承認者）によって異なります。次の表に、エディタおよび承認者に表示されるメニュー オプションを示します。

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
ステージングを編集中（Staging in Edit）		• ネットワークデバイスの表示（View network devices） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	• ネットワークデバイスの選択（Select network devices） 次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • 選択したデバイスの承認要求（Request approval for selected devices） • すべての/フィルタリングされたステージングリストの承認要求（Request approval for all/filtered Staging list） • すべての/フィルタリングされた実稼働リストの承認要求（Request approval for all/filtered Production list） • すべての/フィルタリングされたデバイスの承認要	

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	求（Request approval for all/filtered devices） • 選択したデバイスの承認要求（Request approval for selected devices） • ステージングの破棄（Discard staging） • デルタの表示（View deltas）	
ステージングの承認待ち（Staging Awaiting Approval）	• 承認要求のキャンセル（Cancel approval request） • ネットワークデバイスの表示（View network devices） 次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • 承認要求のキャンセル（Cancel approval request） • デルタの表示（View deltas）	• 展開の承認（Approve deploy） • 展開の拒否（Reject deploy） • ネットワークデバイスの表示（View network devices） 次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • 展開の承認（Approve deploy） • 展開の拒否（Reject deploy） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー

承認済み：展開の準備完了（Approved - ready to deploy）	• 展開（Deploy）
	• 承認要求のキャンセル（Cancel approval request）
	• ネットワークデバイスの表示（View network devices）
	次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。
	  • 展開（Deploy）
	  • 承認要求のキャンセル（Cancel approval request）
	• デルタの表示（View deltas）
		• 展開の拒否（Reject deploy）
		• ネットワークデバイスの表示（View network devices）
		次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。
		  • 展開の拒否（Reject deploy）
		• デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
一部展開済み（Partially deployed）		• ネットワークデバイスの表示（View network devices） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	• ネットワークデバイスの選択（Select network devices） 次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • 選択したデバイスの承認要求（Request approval for selected devices） • すべての/フィルタリングされたステージングリストの承認要求（Request approval for all/filtered Staging list） • すべての/フィルタリングされた実稼働リストの承認要求（Request approval for all/filtered Production list） • すべての/フィルタリングされたデバイスの承認要	

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	求（Request approval for all/filtered devices） • 選択したデバイスの承認要求（Request approval for selected devices） • デルタの表示（View deltas）	

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
完全に展開済み（Fully deployed）		• 実稼働として設定（Set as production） • ネットワークデバイスの表示（View network devices） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	• ネットワークデバイスの選択（Select network devices） 次のオプションが[ネットワーク デバイスの導入（Network Device Deployment）]ウィンドウで使用できます。 • 選択したデバイスの承認要求（Request approval for selected devices） • すべての/フィルタリングされたステージングリストの承認要求（Request approval for all/filtered Staging list） • すべての/フィルタリングされた実稼働リストの承認要求（Request approval for all/filtered Production list） • すべての/フィルタリングされたデバイスの承認要	

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	求（Request approval for all/filtered devices） • 選択したデバイスの承認要求（Request approval for selected devices） • デルタの表示（View deltas）	

ワークフロー オプションは、[送信元ツリービュー（Source Tree View）] と [宛先ツリービュー（Destination Tree View）] でも使用できます。

TrustSec ポリシーのダウンロード レポート（[ワーク センター（Work Centers）] > [TrustSec] > [レポート（Reports）]）を使用して、ステージング/実稼働ポリシーをダウンロードしたデバイスのリストを表示できます。TrustSec ポリシーのダウンロードは、ポリシー（SGT/SGACL）のダウンロードのために、ネットワーク デバイスによって送信された要求と ISE によって送信された詳細を示します。ワークフローモードを有効にしている場合、要求を実稼働マトリックスまたはステージング マトリックスに対してフィルタ処理することができます。

出力ポリシー テーブル セルの設定

Cisco ISE では、ツールバーで使用可能なさまざまなオプションを使用して、セルを設定できます。Cisco ISE では、選択した送信元 SGT および宛先 SGT がマッピングされたセルと同一である場合には、セルを設定できません。

出力ポリシー セルのマッピングの追加

[ポリシー（Policy）] ページから出力ポリシーのマッピング セルを追加できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [イーグレスポリシー（Egress Policy）]** の順に選択します。

ステップ 2 マトリクス セルを選択するには、次の手順を実行します。

- マトリクス ビューで、セルをクリックして選択します。
- 送信元ツリー ビューおよび宛先ツリー ビューで、内部テーブル内の行のチェックボックスをオンにして選択します。

ステップ 3 新しいマッピング セルを追加するには [追加（Add）] をクリックします。

ステップ 4 次の項目について適切な値を選択します。

- 送信元セキュリティ グループ（Source Security Group）
- 宛先セキュリティグループ（Destination Security Group）
- ステータス（Status）、セキュリティ グループ ACL（Security Group ACLs）
- 最終的な catch-all ルール（Final Catch All Rule）

ステップ 5 [保存（Save）] をクリックします。

出力ポリシーのエクスポート

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [エクスポート（Export）] を選択します。

ステップ 2 エクスポートしたファイルに空のセル（SGACL が設定されていないセル）を含める場合は、[空のセルを含める（Include Empty Cells）] チェック ボックスにマークを付けます。

このオプションが有効になっている場合、マトリックス全体がエクスポートされ、空のセルは[SGACL]列に「空（Empty）」キーワードでマークされます。

（注） エクスポートされたファイルに 500000 を超える行が含まれていないことを確認してください。そうでない場合、エクスポートが失敗する場合があります。

ステップ 3 次のオプションのいずれかを選択します。

- [ローカルディスク（Local Disk）]：コンピュータのローカルドライブにファイルをエクスポートする場合は、このオプションを選択します。
- [リポジトリ（Repository）]：リモート リポジトリにファイルをエクスポートする場合は、このオプションを選択します。

  ファイルをエクスポートする前にリポジトリを設定する必要があります。リポジトリを設定するには、[管理（Administration）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）] の順に選択します。読み取りおよび書き込みアクセス権が選択したリポジトリに提供されていることを確認します。

  暗号キーを使用してエクスポートされたファイルを暗号化できます。

  ファイル名は変更することができます。ファイル名は、50 文字以内でなければなりません。デフォルトでは、ファイル名には現在の時刻が含まれていますが、同じファイル名がリモート リポジトリに存在する場合は、ファイルが上書きされます。

ステップ 4 [エクスポート（Export）] をクリックします。

出力ポリシーのインポート

出力ポリシーをオフラインで作成し、Cisco ISE にインポートすることができます。セキュリティ グループ タグの数が多い場合、セキュリティ グループ ACL マッピングを 1 つずつ作成すると、時間がかかることがあります。代わりに、出力ポリシーをオフラインで作成し、Cisco ISE にインポートすることにより、時間を節約できます。インポート中、Cisco ISE は CSV ファイルのエントリを出力ポリシー マトリクスに追加し、データは上書きしません。

次の場合、出力ポリシーのインポートは失敗します。

- 送信元または宛先 SGT が存在しない
- SGACL が存在しない
- モニター ステータスが、そのセルについて Cisco ISE で現在設定されているものと異なる

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [インポート（Import）] を選択します。

ステップ 2 [テンプレートの生成（Generate a Template）] をクリックします。

ステップ 3 [出力ポリシー（Egress Policy）] ページからテンプレート（CSV ファイル）をダウンロードし、CSV ファイルに次の情報を入力します。

- 送信元 SGT
- 宛先 SGT
- SGACL
- モニター ステータス（有効、無効、またはモニター対象）

ステップ 4 インポートするポリシーで既存のポリシーが上書きされるようにする場合は、[新しいデータで既存のデータを上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。空セル（「Empty」キーワードでマークされた、[SGACL] 列のセル）がインポートされたファイルに含まれていると、対応するマトリックスのセルの既存のポリシーが削除されます。

イーグレス ポリシーをエクスポートする際に空セルを含めるには、[空のセルを含める（Include Empty Cells）] チェックボックスをオンにします。詳細については、出力ポリシーのエクスポート （1640 ページ）を参照してください。

ステップ 5 [ファイルの検証（Validate File）] をクリックして、インポートされたファイルを検証します。Cisco ISE は、ファイルをインポートする前に CSV 構造、SGT 名、SGACL、およびファイル サイズを検証します。

ステップ 6 エラーが発生した場合に Cisco ISE でインポートを取り消すには、[最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 7 [インポート（Import）] をクリックします。

出力ポリシーの SGT の設定

[出力ポリシー（Egress Policy）] ページでセキュリティ グループを直接作成できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [イーグレスポリシー（Egress Policy）]** の順に選択します。

ステップ 2 [送信元ツリービュー（Source Tree View）] または [宛先ツリービュー（Destination Tree View）] ページから、[設定（Configure）] > [新しいセキュリティグループの作成（Create New Security Group）] を選択します。

ステップ 3 必要な詳細を入力し、[送信（Submit）] をクリックします。

モニター モード

出力ポリシーの [すべてをモニター（Monitor All）] オプションを使用すると、出力ポリシー設定ステータス全体を 1 回のクリックでモニターモードに変更できます。[出力ポリシー（egress policy）] ページの [すべてをモニター（Monitor All）] チェックボックスをオンにして、すべてのセルの出力ポリシー設定ステータスをモニター モードに変更します。[すべてをモニター（Monitor All）] チェックボックスをオンにすると、設定ステータスが次のように変更されます。

- ステータスが [有効（Enabled）] であるセルはモニター対象として動作しますが、有効であるかのように表示されます。
- ステータスが [無効（Disabled）] であるセルは何も影響を受けません。
- ステータスが [モニター（Monitor）] であるセルは、[モニター対象（Monitored）] のままになります。

[すべてをモニター（Monitor All）] チェックボックスをオフにすると、元の設定ステータスに戻ります。データベース内の実際のセルのステータスは変更されません。[すべてをモニター（Monitor All）] をオフにすると、出力ポリシーのそれぞれのセルが元の設定ステータスに戻ります。

モニター モードの機能

モニター モードのモニタリング機能は次の操作に役立ちます。

- フィルタリングされているけれども、モニターモードではモニターされているトラフィックの量の確認
- SGT-DGT ペアがモニター モードであるか強制モードであるかの確認と、ネットワーク内で異常なパケット ドロップが発生していないかどうかの観察
- SGACL ドロップが実際に強制モードによって強制されているのか、またはモニター モードによって許可されているのかの確認

- モードのタイプ（モニター、強制、または両方）に基づいたカスタム レポートの作成
- NAD に適用されている SGACL、および表示の不一致（ある場合）の識別

不明セキュリティ グループ

不明セキュリティ グループは事前に設定されているセキュリティ グループで、変更不可能であり、タグ値 0 の TrustSec を表します。

Cisco セキュリティ グループのネットワーク デバイスは、送信元または宛先のいずれかの SGT がない場合に不明 SGT を参照するセルを要求します。送信元のみが不明の場合、要求は <不明, 宛先 SGT> セルに適用されます。宛先のみが不明の場合、要求は <source SGT, unknown> セルに適用されます。送信元および宛先の両方が不明の場合、要求は<不明, 不明> セルに適用されます。

デフォルト ポリシー

デフォルト ポリシーは、<ANY,ANY> セルを参照します。任意の送信元 SGT が任意の宛先 SGT にマッピングされています。ここでは、ANY SGT は変更不可能であり、送信元 SGT にも宛先 SGT にも表示されません。ANY SGT は ANY SGT とのみペアにできます。他の SGT とはペアにできません。TrustSec ネットワーク デバイスでは、デフォルト ポリシーを特定セルのポリシーの最後に付加します。

- つまり、セルが空白の場合は、デフォルト ポリシーのみが含まれることになります。
- セルにポリシーが含まれる場合、結果のポリシーは、セル固有のポリシーとその後に続くデフォルト ポリシーの組み合わせになります。

Cisco ISE では、セル ポリシーおよびデフォルト ポリシーは 2 つの別々の SGACL セットになり、デバイスは 2 つの別々のポリシー クエリーの応答としてこれらのセットを取得します。

デフォルト ポリシーの設定は、他のセルと次の点で異なります。

- ステータスは [有効（Enabled）] または [モニター対象（Monitored）] の 2 つの値しかとることができません。
- セキュリティ グループ ACL は、デフォルト ポリシーでは任意のフィールドであるため、空白のままにできます。
- 最終的な catch-all ルールは次のいずれかになります。許可 IP、拒否 IP、許可 IP ログ、または拒否 IP ログ。デフォルト ポリシーを上回る安全策はないため、ここで [なし（None）] オプションを使用できないことは明らかです。

SGT の割り当て

Cisco ISE では、デバイスのホスト名または IP アドレスがわかっている場合に、TrustSec デバイスに SGT を割り当てることができます。特定のホスト名または IP アドレスを持つデバイスがネットワークに参加すると、Cisco ISE によって認証前に SGT が割り当てられます。

次の SGT がデフォルトで作成されています。

- SGT_TrustSecDevices
- SGT_NetworkServices
- SGT_Employee
- SGT_Contractor
- SGT_Guest
- SGT_ProductionUser
- SGT_Developer
- SGT_Auditor
- SGT_PointofSale
- SGT_ProductionServers
- SGT_DevelopmentServers
- SGT_TestServers
- SGT_PCIServers
- SGT_BYOD
- SGT_Quarantine

セキュリティ グループ タグをエンドポイントにマップするようにデバイスを手動で設定する必要がある場合もあります。このマッピングは [セキュリティ グループ マッピング（Security Group Mappings）] ページから作成できます。この操作を実行する前に、SGT の範囲が予約済みであることを確認します。

ISE では、最大 10,000 の IP-to-SGT マッピングを作成できます。IP-to-SGT マッピング グループを作成して、このような大規模なマッピングを論理的にグループ化することができます。各 IP-to-SGT マッピング グループには、IP アドレスのリスト、マップ先の単一のセキュリティ グループ、およびこれらのマッピングの展開対象であるネットワーク デバイスまたはネットワーク デバイス グループが含まれています。

NDAC 許可

デバイスに SGT を割り当てることで TrustSec ポリシーを設定できます。TrustSec デバイスの ID 属性に基づいて、デバイスにセキュリティ グループを割り当てることができます。

NDAC 許可の設定

始める前に

- ポリシーで使用するためのセキュリティ グループを作成します。

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [ネットワークデバイス認証（Network Device Authorization）] を選択します。

ステップ 2 [デフォルト ルール（Default Rule）] 行の右側にある [操作（Action）] アイコンをクリックし、[新規行を上に挿入（Insert New Row Above）] をクリックします。

ステップ 3 このルールの名前を入力します。

ステップ 4 [条件（Conditions）] の隣にあるプラス記号（+）をクリックして、ポリシー条件を追加します。

ステップ 5 [新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）] をクリックすると、新しい条件を作成できます。

ステップ 6 [セキュリティ グループ（Security Group）] ドロップダウン リストから、この条件の評価が true になった場合に割り当てる SGT を選択します。

ステップ 7 この行の [操作（Action）] アイコンをクリックして、現在のルールの上または下に、デバイス属性に基づいた別のルールを追加します。このプロセスを繰り返して、TrustSec ポリシーに必要なすべてのルールを作成できます。ルールをドラッグ アンド ドロップし、  アイコンをクリックすることでこれらの順序を変更できます。既存の条件を複製することもできますが、ポリシー名は必ず変更してください。

評価が true になる最初のルールによって、評価の結果が決まります。いずれのルールも一致しなかった場合、デフォルト ルールが適用されます。デフォルト ルールを編集して、いずれのルールも一致しなかった場合にデバイスに適用される SGT を指定できます。

ステップ 8 [保存（Save）] をクリックして TrustSec ポリシーを保存します。

ネットワーク デバイス ポリシーを設定した後に、TrustSec デバイスで認証を行おうとすると、デバイスはその SGT およびそのピアの SGT を取得し、関連するすべての詳細をダウンロードできるようになります。

（注） デフォルトでは、デフォルトの [ネットワークデバイス認証（Network Device Authorization）] ポリシーの結果は [TrustSec_Devices] に設定されます。

エンドユーザーの許可の設定

Cisco ISE では、許可ポリシー評価の結果としてセキュリティ グループを割り当てることができます。このオプションを使用すると、ユーザーおよびエンドポイントにセキュリティ グループを割り当てることができます。

始める前に

- 許可ポリシーについての情報を参照してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）] > [TrustSec] > [認証ポリシー（Authorization Policy）] を選択します。

ステップ 2 新しい許可ポリシーを作成します。

ステップ 3 権限のセキュリティ グループを選択します。

あるユーザーまたはエンドポイントについて、この許可ポリシーで指定した条件が true の場合、このセキュリティ グループがそのユーザーまたはエンドポイントに割り当てられ、このユーザーまたはエンドポイントによって送信されたすべてのデータ パケットにこの特定の SGT でタグが付けられます。

TrustSec の設定およびポリシー プッシュ

Cisco ISE では、許可変更（CoA）がサポートされています。これを使用すると、Cisco ISE で TrustSec の設定およびポリシーの変更を TrustSec デバイスに通知でき、デバイスでは関連データの取得要求でこれに応答できるようになります。

CoA 通知では、TrustSec ネットワーク デバイスをトリガーし、環境 CoA またはポリシー CoA のいずれかを送信できます。

また、基本的に TrustSec CoA 機能をサポートしないデバイスに設定変更をプッシュできます。

CoA でサポートされるネットワーク デバイス

Cisco ISE は次のネットワーク デバイスに CoA 通知を送信します。

- 単一の IP アドレスを持つネットワーク デバイス（サブネットはサポートされません）
- TrustSec デバイスとして設定されているネットワーク デバイス
- CoA サポート対象として設定されているネットワーク デバイス

複数のセカンダリが存在する分散環境に Cisco ISE が展開されており、これらのセカンダリがそれぞれ異なるデバイス セットと相互運用している場合、CoA 要求は Cisco ISE プライマリ ノードからすべてのネットワーク デバイスに送信されます。そのため、TrustSec ネットワーク デバイスは、Cisco ISE プライマリ ノードで CoA クライアントとして設定されている必要があります。

デバイスは、Cisco ISE プライマリ ノードに CoA NAK または ACK を返します。ただし、ネットワーク デバイスからの次の TrustSec セッションは、ネットワーク デバイスが他の AAA 要求

をすべて送信する Cisco ISE ノードに送信され、必ずしもプライマリ ノードに送信されるわけではありません。

非 CoA サポート デバイスへの設定変更のプッシュ

一部のプラットフォームでは、許可変更（CoA）について Cisco ISE の「プッシュ」機能はサポートされていません。例：Nexus ネットワーク デバイスの一部のバージョン。この場合、ISE はネットワーク デバイスに接続し、ISE に対して更新された設定要求をデバイスがトリガーするようにします。これを行うために、ISE はネットワーク デバイスへの SSHv2 トンネルを開き、TrustSec ポリシーマトリクスのリフレッシュをトリガーするコマンドを送信します。この方法は、CoA プッシュをサポートするネットワーク プラットフォームでも実行できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** の順に選択します。

ステップ 2 必要なネットワーク デバイスの横にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ネットワーク デバイスの名前、IP アドレス、RADIUS および TrustSec 設定が正しく設定されていることを確認します。

ステップ 3 [高度な TrustSec 設定（Advanced TrustSec Settings）] まで下にスクロールし、[TrustSec 通知および更新（TrustSec Notifications and Updates）] セクションで、[デバイスに設定変更を送信（Send configuration changes to device）] チェックボックスをオンにして [CLI（SSH）（CLI (SSH)）] オプション ボタンをクリックします。

ステップ 4 （任意） SSH キーを指定します。

ステップ 5 デバイス インターフェイスのクレデンシャルを使用して IP-SGT マッピングを取得するには、この SGA デバイスに対して [セキュリティ グループ タグ マッピングの展開時にこのデバイスを含める（Include This Device When Deploying Security Group Tag Mapping Updates）] チェックボックスをオンにします。

ステップ 6 EXEC モードでデバイス設定を編集する権限を持つユーザーのユーザー名とパスワードを入力します。

ステップ 7 （任意） 設定を編集できるデバイスの EXEC モード パスワードを有効にするためのパスワードを入力します。[表示（Show）] をクリックして、このデバイスにすでに設定されている EXEC モード パスワードを表示できます。

ステップ 8 ページの下部にある [送信（Submit）] をクリックします。

ネットワーク デバイスは、TrustSec の変更をプッシュするように設定されました。Cisco ISE ポリシーを変更した後で、ネットワーク デバイスに新規設定を反映させるには、[プッシュ（Push）] をクリックします。

SSH キーの検証

SSH キーを使用してセキュリティを強化することもできます。Cisco ISE では、SSH キー検証機能によってこれをサポートします。

この機能を使用するには、Cisco ISE からネットワーク デバイスに SSHv2 トンネルを開いて、ネットワーク デバイスの独自の CLI を使用して SSH キーを取得します。このキーをコピーし、検証のために Cisco ISE に貼り付けます。SSH キーが誤っている場合、Cisco ISE は接続を終了します。

制限：現在、Cisco ISE が検証できるのは 1 つの IP のみです（IP の範囲、または IP 内のサブネットは検証できません）

始める前に

次のものが必要です。

- ログイン クレデンシャル
- SSH キーを取得する CLI コマンド

（Cisco ISE とセキュアに通信できるようにするネットワーク デバイスのもの）

ステップ 1 ネットワーク デバイス上：

a) Cisco ISE が SSH キー検証を使用して通信するネットワーク デバイスにログインします。

b) デバイスの CLI を使用して SSH キーを表示します。

例：

Catalyst デバイスの場合、コマンドは次のとおりです。`sho ip ssh`。

c) 表示された SSH キーをコピーします。

ステップ 2 Cisco ISE ユーザー インターフェイスから、次の手順を実行します。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** を選択し、必要なネットワーク デバイス名、IP アドレス、RADIUS および TrustSec 設定が正しく設定されていることを確認します。

b) [高度な TrustSec 設定（Advanced TrustSec Settings）] まで下にスクロールし、[TrustSec 通知および更新（TrustSec Notifications and Updates）] セクションで、[デバイスに設定変更を送信（Send configuration changes to device）] チェックボックスをオンにして [CLI（SSH）（CLI (SSH)）] オプション ボタンをクリックします。

c) [SSH キー（SSH Key）] フィールドに、ネットワーク デバイスから取得した SSH キーを貼り付けます。

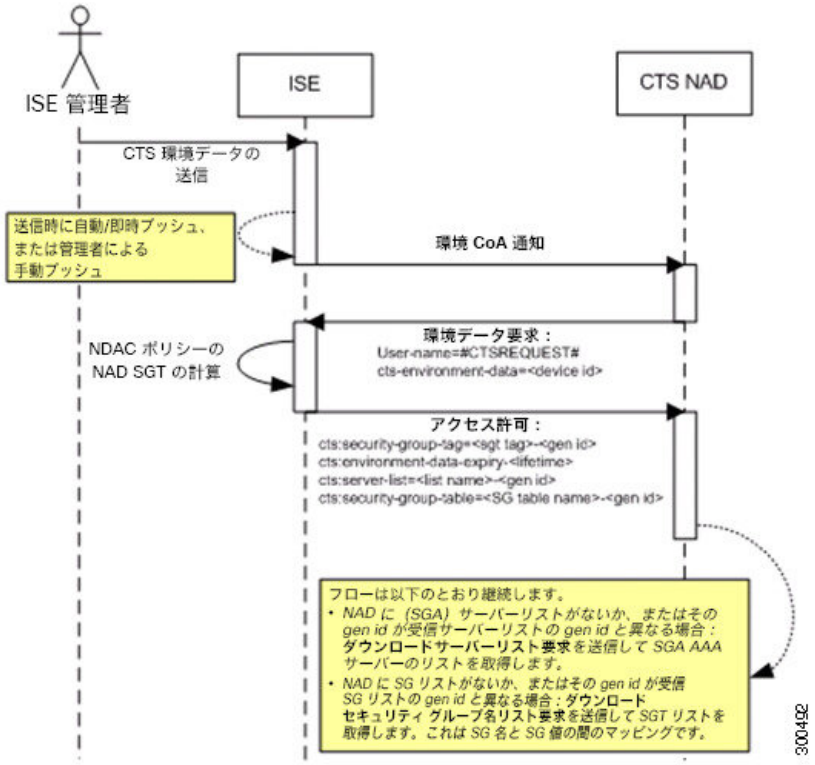
d) ページの下部にある [送信（Submit）] をクリックします。

ネットワーク デバイスは、SSH キー検証を使用して Cisco ISE と通信するようになりました。

環境 CoA 通知のフロー

次の図は、環境 CoA 通知のフローを示しています。

図 *65 :* 環境 *CoA* 通知のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに環境 CoA 通知を送信します。
2. デバイスは、環境データ要求を返します。
3. 環境データ要求への応答で、Cisco ISE は次の情報を返します。

   要求を送信したデバイスの環境データ：これには、（NDAC ポリシーから推測される）TrustSec デバイスの SGT およびダウンロード環境 TTL が含まれます。

   TrustSec AAA サーバー リストの名前および生成 ID。

   （複数の可能性がある）SGT テーブルの名前および生成 ID：これらのテーブルには SGT 名と SGT 値がリストされ、一緒に SGT の完全リストも保持されます。
4. デバイスが TrustSec AAA サーバー リストを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、AAA サーバー リストの内容を取得します。
5. デバイスが応答にリストされている SGT テーブルを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、その SGT テーブルの内容を取得します。

環境 CoA トリガー

環境 CoA は次のものに関して開始できます。

- ネットワーク デバイス
- セキュリティ グループ
- AAA サーバー

ネットワーク デバイスの環境 CoA のトリガー

ネットワーク デバイスに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 ネットワーク デバイスを追加または編集します。

ステップ 3 [高度な TrustSec 設定（Advanced TrustSec Settings）] セクションで、[TrustSec 通知および更新（TrustSec Notifications and Updates）] パラメータを更新します。

環境属性の変更は、変更が発生した特定の TrustSec ネットワーク デバイスにのみ通知されます。

単一のデバイスのみが影響を受けるため、環境CoA通知は送信直後に送信されます。結果として、そのデバイスの環境属性が更新されます。

セキュリティ グループの環境 CoA のトリガー

セキュリティ グループに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）]**。

ステップ 2 [セキュリティ グループ（Security Group）] ページで、SGT の名前を変更します。これにより、その SGT のマッピング値の名前が変更されます。これで環境変更がトリガーされます。

ステップ 3 複数の SGT の名前を変更した後、[プッシュ（Push）] ボタンをクリックして、環境 CoA 通知を開始します。この環境CoA通知は、すべてのTrustSecネットワークデバイスに送信され、変更されたすべてのSGTの更新が提供されます。

TrustSec AAA サーバーの環境 CoA のトリガー

TrustSec AAA サーバーに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [TrustSec AAA サーバー（TrustSec AAA Servers）]** を選択します。

ステップ 2 [TrustSec AAA サーバー（TrustSec AAA Servers）] ページで、TrustSec AAA サーバーの設定を作成、削除、または更新します。これで環境変更がトリガーされます。

ステップ 3 複数の TrustSec AAA サーバーを設定した後、[プッシュ（Push）] ボタンをクリックして、環境 CoA 通知を開始します。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、変更されたすべての TrustSec AAA サーバーの更新を提供します。

NDAC ポリシーの環境 CoA のトリガー

NDAC ポリシーに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [ワークセンター（Work Centers）]>[TrustSec]>[ポリシー（Policy）]>[ネットワークデバイス許可（Network Device Authorization）] の順に選択します。

[NDAC ポリシー（NDAC policy）] ページで、NDAC ポリシーのルールを作成、削除、または更新できます。これらの環境変更は、すべてのネットワーク デバイスに通知されます。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）]>[TrustSec]>[TrustSec ポリシー（TrustSec Policy）]>[ネットワークデバイス認証（Network Device Authorization）] を選択します。

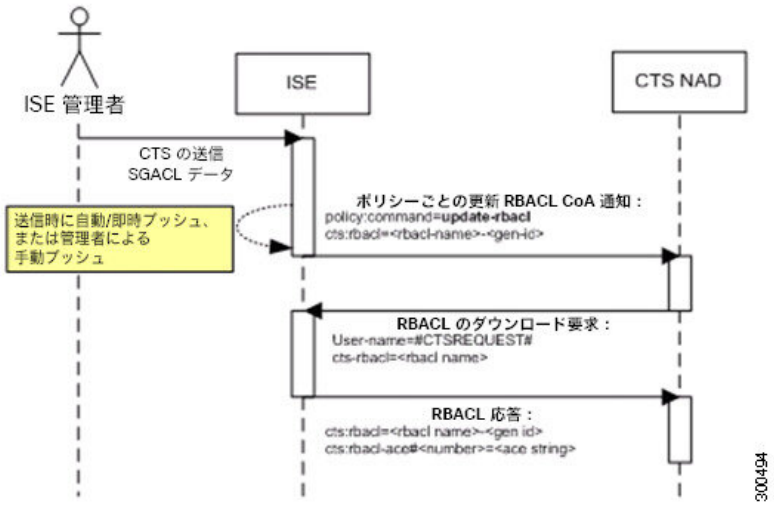
[NDAC ポリシー（NDAC policy）] ページで、NDAC ポリシーのルールを作成、削除、または更新できます。これらの環境変更は、すべてのネットワーク デバイスに通知されます。

ステップ 3 [NDAC ポリシー（NDAC policy）] ページで [プッシュ（Push）] ボタンをクリックすることで、環境 CoA 通知を開始できます。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、ネットワーク デバイス自体の SGT の更新を提供します。

SGACL コンテンツ更新のフロー

次の図に、SGACL コンテンツ更新のフローを示します。

図 *66 : SGACL* コンテンツ更新のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに SGACL 名前付きリストの更新 CoA 通知を送信します。通知には、SGACL 名と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGACL データ要求で応答できます。

   SGACL が、デバイスが保持する出力セルに含まれている場合。デバイスには出力ポリシー データのサブセットが保持されます。これらは、そのネイバーデバイスおよびエンドポイントの SGT に関連するセルです（選択した宛先 SGT の出力ポリシー カラム）。

   CoA 通知内の生成 ID が、この SGACL 用にデバイスが保持している生成 ID と異なっている。
3. SGACL データ要求への応答で、Cisco ISE は SGACL のコンテンツ（ACE）を返します。

SGACL 名前付きリストの更新 CoA の開始

SGACL 名前付きリストの更新 CoA をトリガーするには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループACL（Security Group ACLs）]** を選択します。

ステップ 2 SGACL のコンテンツを変更します。SGACL を送信すると、SGACL の生成 ID が変更されます。

ステップ 3 複数の SGACL のコンテンツを変更した後、[プッシュ（Push）] ボタンをクリックして、SGACL 名前付きリストの更新 CoA 通知を開始します。この通知は、すべての TrustSec ネットワーク デバイスに送信され、関連するデバイスのその SGACL コンテンツの更新が提供されます。

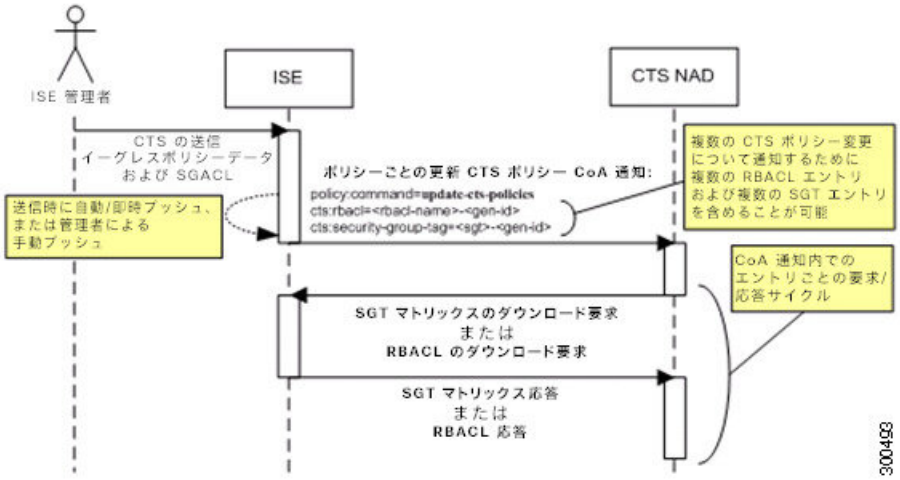
SGACL の名前または IP バージョンを変更しても、その生成 ID は変更されません。そのため、SGACL 名前付きリストの更新 CoA 通知を送信する必要はありません。

ただし、出力ポリシーで使用中の SGACL の名前または IP バージョンを変更することは、その SGACL を含むセルが変更されることを意味するため、この変更でそのセルの宛先 SGT の生成 ID が変更されます。

ポリシーの更新 CoA 通知のフロー

次の図に、ポリシーの CoA 通知のフローを示します。

図 *67 :* ポリシーの *CoA* 通知のフロー

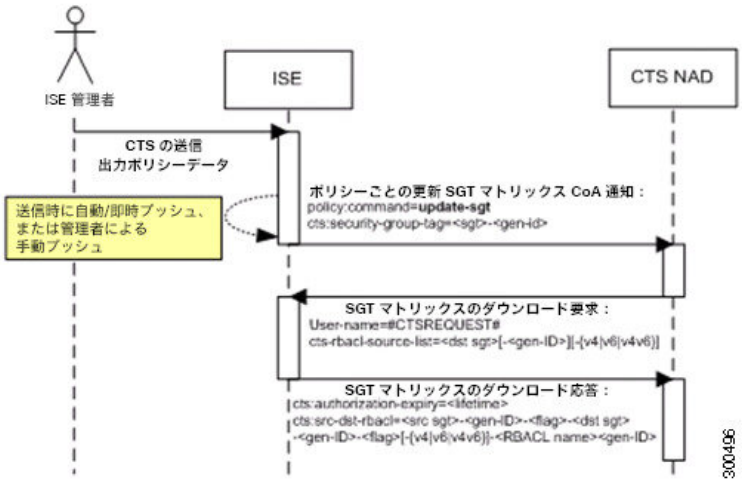


1. Cisco ISE は、TrustSec ネットワーク デバイスにポリシーの更新 CoA 通知を送信します。通知には、複数の SGACL 名とその生成 ID、および複数の SGT 値とその生成 ID が含まれることがあります。
2. デバイスは、複数の SGACL データ要求か複数の SGT データ、またはその両方で応答できます。
3. 各 SGACL データ要求または SGT データ要求に対する応答で、Cisco ISE は関連するデータを返します。

SGT マトリクスの更新 CoA のフロー

次の図に、SGT マトリクスの更新 CoA のフローを示します。

図 *68 : SGT* マトリクスの更新 *CoA* のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに SGT マトリクスの更新 CoA 通知を送信します。通知には、SGT 値と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGT データ要求で応答できます。

   SGT がネイバーデバイスまたはエンドポイントの SGT である場合。デバイスは、ネイバーデバイスおよびエンドポイントの SGT に関連するセルをダウンロードして保持します（宛先 SGT）。

   CoA 通知内の生成 ID が、この SGT 用にデバイスが保持している生成 ID と異なっている。
3. SGT データ要求に対する応答で、Cisco ISE は、送信元および宛先 SGT、セルのステータス、そのセルに設定されている SGACL 名の順序リストなど、すべての出力セルのデータを返します。

出力ポリシーからの、SGT マトリクスの更新 CoA の開始

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [イーグレスポリシー（Egress Policy）]** の順に選択します。

ステップ 2 [出力ポリシー（Egress Policy）] ページで、セルの内容（ステータス、SGACL）を変更します。

ステップ 3 変更を送信すると、そのセルの宛先 SGT の生成 ID が変更されます。

ステップ 4 複数の出力セルの内容を変更した後、[プッシュ（Push）] ボタンをクリックして、SGT マトリクスの更新 CoA 通知を開始します。この通知は、すべての TrustSec ネットワーク デバイスに送信され、関連するデバイスのセルの内容の更新が提供されます。

TrustSec CoA の概要

次の表に、TrustSec CoA の開始を要求するさまざまなシナリオ、各シナリオで使用される CoA のタイプ、および関連する UI ページの概要を示します。

表 *151 : TrustSec CoA* の概要

UI ページ	CoA をトリガーする操作	トリガー方法	CoA タイプ	送信先
ネットワーク デバイス（Network Device）	ページの [TrustSec] セクションでの環境 TTL の変更	TrustSec ネットワーク デバイスで正常に送信が行われたとき	環境	特定のネットワーク デバイス
TrustSec AAA サーバー（TrustSec AAA Server）	TrustSec AAA サーバーの変更（作成、更新、削除、順序変更）	[TrustSec AAA サーバー（TrustSec AAA servers）] リストページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス
セキュリティ グループ（Security Group）	SGT の変更（作成、名前変更、削除）	[SGT] リストページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス
NDAC ポリシー（NDAC Policy）	NDAC ポリシーの変更（作成、更新、削除）	[NDAC ポリシー（NDAC policy）] ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス

UI ページ	CoA をトリガーする操作	トリガー方法	CoA タイプ	送信先
SGACL	SGACL ACE の変更	[SGACL] リストページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	RBACL 名前付きリストの更新	すべての TrustSec ネットワーク デバイス
	SGACL 名または IP バージョンの変更	[SGACL] リストページの [プッシュ（Push）] ボタンまたは出力テーブルのポリシー プッシュ ボタンをクリックすると、累積された変更をプッシュできます。	更新 SGT マトリクス	すべての TrustSec ネットワーク デバイス
出力ポリシー（Egress Policy）	SGT の生成 ID を変更するすべての操作	[出力ポリシー（egress policy）] ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	更新 SGT マトリクス	すべての TrustSec ネットワーク デバイス

セキュリティ グループ タグの交換プロトコル

セキュリティ グループ タグ（SGT）の交換プロトコル（SXP）は、TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播するために使用されます。SXP は、ある SGT 対応ネットワーク デバイスから別のデバイスに IP アドレスとともにエンドポイントの SGT を転送するために使用されます。SXP が転送するデータは、IP-SGT マッピングと呼ばれます。エンドポイントが属する SGT は静的または動的に割り当てることができ、SGT はネットワーク ポリシーで分類子として使用できます。

ノードで SXP サービスをイネーブルにするには、[ノードの一般設定（General Node Settings）] ページで [SXPサービスの有効化（Enable SXP Service）] チェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。

SXP はトランスポート プロトコルとして TCP を使用して、2 つの個別のネットワーク デバイス間に SXP 接続をセットアップします。各 SXP 接続には、SXP スピーカーとして指定されたピアと、SXP リスナーとして指定されたピアがあります。ピアは双方向モードで設定することもでき、そのモードでは、それぞれがスピーカーとリスナーの両方として機能します。接続はいずれかのピアによって開始できますが、マッピング情報は常にスピーカーからリスナーに伝播されます。

（注） セッションのバインディングは常にデフォルトの SGT ドメインに伝播されます。

次の表には、SXP 環境で使用される一般的な用語のいくつかを示しています。

IP-SGT マッピング	SXP 接続を介して交換される SGT マッピングへの IP アドレス。 SXP デバイスで学習されたすべてのマッピング（スタティックマッピングおよびセッションマッピングを含む）を表示するには、**[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SGTバインディング（SGT Bindings）]** の順に選択します。
SXP スピーカー	SXP 接続を介して IP-SGT マッピングを送信するピア。
SXP リスナー	SXP 接続を介して IP-SGT マッピングを受信するピア。

Cisco ISE に追加された SXP ピア デバイスを表示するには、[ワークセンター（Work centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）] の順に選択します。

（注） SXP サービスはスタンドアロン ノードで実行することを推奨します。

SXP サービスを使用する際は、次の点に注意してください。

- アップグレード、ノード障害、またはノード設定の更新の場合は、接続されたPSNの詳細を使用してSXPデバイス設定を更新する必要があります。
- セッションベースのマッピングは、展開内のすべての SXP ノードに伝播され、適切な SGT ドメインのすべての SXP リスナーに送信されます。SXP ベースのマッピングは、展開内のすべての SXP ノードに伝播されません。これらのマッピングは、すべてのノードではなく、マッピングを受信した PSN の SXP リスナーとのみ共有されます。
- SXP ノードを登録解除して、既存の展開に再登録すると、そのノードに接続されている SXP デバイスが展開から削除されます。これらのデバイスは、**[SXPデバイス（SXP Devices）]** ウィンドウ（**[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデ**

バイス（**SXP Devices**）]）には表示されません。SXP ノードを展開に再登録した後、これらのデバイスを手動で再追加する必要があります。ただし、SXP ノードの SXP サービスが無効になっている場合、SXP デバイスは削除されません。

- Cisco ISE は、同じ IP アドレスを持つ複数の SXP セッション バインディングをサポートしていません。
- RADIUS アカウンティング更新の頻度が高すぎる（数秒に約 6 から 8 のアカウンティング更新）場合、アカウンティング更新パケットがドロップされる可能性があり、SXP が IP-SGT バインディングを受信できないことがあります。
- 以前のバージョンの ISE からアップグレードした後は、SXP は自動的に起動しません。アップグレード後に、SXP パスワードを変更し、SXP プロセスを再起動する必要があります。

SXP デバイスの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 デバイスの詳細を入力します。

- CSV ファイルを使用して SXP デバイスを追加するには、[CSVファイルからアップロード（Upload from a CSV file）] をクリックします。CSV ファイルを参照して選択し、[アップロード（Upload）] をクリックします。

  また、CSV テンプレート ファイルをダウンロードして、追加するデバイスの詳細を入力し、CSV ファイルをアップロードすることもできます。

- 各 SXP デバイスの詳細を手動で追加するには、[単一デバイスの追加（Add Single Device）] をクリックします。

  ピア デバイスの名前、IP アドレス、SXP ロール（リスナー、スピーカー、または両方）、パスワード タイプ、SXP バージョン、および接続されている PSN を入力します。また、ピア デバイスが接続されている SGT ドメインも指定する必要があります。

ステップ 4 （任意）[詳細設定（Advanced Settings）] をクリックし、次の詳細を入力します。

- [最小許容ホールドタイマー（Minimum Acceptable Hold Timer）]：スピーカーが接続状態を保持するためにキープアライブ メッセージを送信する時間を秒単位で指定します。値の範囲は 1 ～ 65534 です。

- [キープアライブタイマー（Keep Alive Timer）]：アップデート メッセージによって他の情報がエクスポートされないインターバル期間にキープアライブ メッセージのディスパッチをトリガーするためにスピーカーによって使用されます。値の範囲は 0 ～ 64000 です。

ステップ 5 [保存（Save）] をクリックします。

SGT ドメインフィルタの追加

SXP デバイスで学習されたすべてのマッピング（スタティックマッピングおよびセッションマッピングを含む）を表示できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SGTバインディング（SGT Bindings）]**。

デフォルトでは、ネットワークデバイスから学習したセッションマッピングは、デフォルトの VPN グループ（デフォルトと呼ばれる）にのみ送信されます。SGT ドメインフィルタを作成して、異なる SGT ドメイン（VPN）にマッピングを送信できます。

ネットワークデバイス用の仮想ネットワークが指定されていない場合、Cisco ISE はそのバインディングをデフォルトの仮想ネットワーク（DEFAULT_VN と呼ばれる）に割り当てます。SXP フィルタには、「DEFAULT_VN」を「デフォルト」VPN に回送する内部ルールがあります。

Catalyst Center で新しい仮想ネットワークが作成されるか、仮想ネットワーク作成 ERS 要求を受信すると、Cisco ISE で新しい VPN が作成されます。たとえば、Catalyst Center で VN1 が作成されると、Cisco ISE で新しい VPN（SDA_VN1）が作成されます。さらに、新しい SXP フィルタルール（VN1 を SDA_VN1 に回送）が Cisco ISE で内部的に作成されます。VN1 からのバインディングを SDA_VN1 に伝播する場合は、SDA_VN1 をそれらの SXP デバイスに割り当てる必要があります。

仮想ネットワークは認証プロファイルに割り当てることができます。認証要求（Access-Request）が受け入れられると、Cisco ISE は SGT、仮想ネットワーク、および VLAN の詳細をその応答（Access-Accept）に追加します。NAD はその後の accounting-start や accounting-interim などの要求で、以下に示すように Cisco AV ペアと同じ SGT および仮想ネットワークを送信する必要があります。

- cisco-av-pair=cts:security-group-tag
- cisco-av-pair=cts:vn

（注） Cisco ISE 3.0 以降では、ネットワークデバイスを複数の SGT ドメインに含めることができます。

SGT ドメインフィルタを追加するには、次の手順を実行します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SGTバインディング（SGT Bindings）]**。

ステップ 2 [SGTドメインフィルタの追加（Add SGT Domain Filter）] をクリックします。

ステップ 3 次の手順を実行します。

- サブネットの詳細を入力します。このサブネットからの IP アドレスを持つネットワークデバイスのセッションマッピングは、[SGTドメイン（SGT Domain）] フィールドで選択された SGT ドメイン（VPN）に送信されます。
- [SGT] ドロップダウンリストから SGT を選択します。この SGT に関連するセッションマッピングは、[SGTドメイン（SGT Domain）] フィールドで選択された SGT ドメインに送信されます。

  サブネットと SGT の両方を指定した場合、このフィルタに一致するセッションマッピングは、[SGTドメイン（SGT Domain）] フィールドで選択された SGT ドメインに送信されます。
- **[VN]** フィールドで仮想ネットワークを指定します。この仮想ネットワークに関連するセッションマッピングは、[SGTドメイン（SGT Domain）] フィールドで選択された SGT ドメインに送信されます。
- マッピングを送信する必要がある SGT ドメインを選択します。

ステップ 4 [保存（Save）] をクリックします。

SGT ドメインフィルタを更新または削除することもできます。フィルタを更新するには、[SGTドメインフィルタの管理（Manage SGT Domain Filter）] をクリックし、更新するフィルタの横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。フィルタを削除するには、削除するフィルタの横にあるチェックボックスをオンにして、[ごみ箱（Trash）]>[選択済み（Selected）] をクリックします。

SXP の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [SXP 設定（SXP Settings）] を選択します。

ステップ 2 次のチェック ボックスをオンにします。

- **pxGrid の SXP バインディングを公開する**
- **SXP IP SGT マッピングテーブルに Radius および PassiveID マッピングを追加する**

[SXPバインディングをPxGridで公開（Publish SXP Bindings on PxGrid）] チェックボックスをオフにすると、IP-SGT マッピングは pxGrid SXP トピックに公開されません。

ステップ 3 [SXP設定（SXP Settings）] ページに必要な詳細を入力します。

ステップ 4 [保存（Save）] をクリックします。

（注）
- SXP 設定が変更されると、SXP サービスが再起動されます。
- アップグレード、ノード障害、またはノード設定の更新の場合は、接続されたPSNの詳細を使用してSXPデバイス設定を更新する必要があります。

Cisco ISE でのシスコ アプリケーション セントリック インフラストラクチャ接続

（注） 複数の Cisco Application Infrastructure（Cisco ACI）コネクタに対するサポートは、制御された導入（ベータ）機能です。この機能を実稼働環境で使用する前に、テスト環境で十分にテストすることを推奨します。このベータ機能を最大限に活用するには、このホットパッチをインストールします。

Cisco ISEを使用すると、複数のドメイン間で一貫したアクセスポリシーを作成して適用できます。Cisco ISE は、SGT および IP-SGT バインディングを Cisco ACI と共有し、Cisco ACI からエンドポイントグループ（EPG）、エンドポイント セキュリティ グループ（ESG）、およびエンドポイント設定情報を受信できます。

Cisco ISE に複数の Cisco ACI 接続を追加できます。各接続を使用して、異なる ACI ファブリックに接続できます。Cisco ISE は、個々の Cisco ACI ファブリックおよびマルチポッド Cisco ACI ファブリックと統合できます。Cisco ISE は、Cisco ACI マルチテナントおよび Multi-Virtual Routing and Forwarding（VRF）の展開をサポートしています。

Cisco ISE で学習したコンテキストを管理し、Cisco ISE コネクタと Cisco ACI コネクタ間のコンテキストフローを最適化するルールを設定できます。

以下は、この統合を説明する際に一般的に使用される用語です。

- エンドポイントグループ（EPG）：Cisco ACI で使用されます。EPG は、エンドポイントの集合を含む論理エンティティです。EPG は単一のブリッジドメインに関連付けられ、ブリッジドメイン内のセキュリティゾーンを定義するために使用されます。

- エンドポイント セキュリティ グループ（ESG）：Cisco ACI で使用されます。ESG は、物理または仮想ネットワークエンドポイントの収集を含む論理エンティティです。ESG は、ブリッジドメインではなく単一の VRF インスタンスに関連付けられます。
- インバウンド SGT ドメインルール：SGT バインディングを特定の SGT ドメインにマッピングするために Cisco ISE で使用されるルール。
- アウトバウンド SGT ドメインルール：特定の SGT バインディングのターゲット宛先を指定するために Cisco ISE で使用されるルール。

Cisco ISE は、EPG と ESG を同期し、関連する SGT を作成することで、Cisco ACI ドメインから TrustSec ドメインに着信するパケットをサポートします。これらの SGT は、Cisco ACI に設定されたエンドポイントをマッピングし、Cisco ISE で関連する SGT バインディングを作成します。

Cisco ACI は、SGT を同期し、関連する EEPG を作成することで、TrustSec ドメインから Cisco ACI ドメインに送信されるパケットをサポートします。Cisco ACI は、Cisco ISE からの SGT バインディングに基づいて EEPG でサブネットを作成します。これらのサブネットは、対応する SGT バインディングが Cisco ISE で削除されるときに、Cisco ACI から削除されます。

EPG または ESG が Cisco ACI で削除されると、同期された EPG リストが Cisco ISE で更新されます。EPG または ESG がインバウンドまたはアウトバウンド SGT ドメインルールで使用されていない場合、Cisco ISE で削除されます。EPG または ESG が削除されると、その EPG または ESG から学習された IP-SGT バインディングも Cisco ISE から削除され、対応する IP-SGT 削除イベントが pxGrid SXP トピックを介して送信されます。

EPG または ESG がインバウンドまたはアウトバウンド SGT ドメインルールで使用されている場合、これらは削除されません。その EPG または ESG を手動で削除する必要があります。どちらの場合もアラームが発生します。

Cisco ISE で SGT がアウトバウンド SGT ドメインルールに追加されると、EEPG が Cisco ACI に作成されます。SGT がアウトバウンド SGT ドメインルールから削除されると、対応する EEPG が Cisco ACI で削除されます。

（注） 2 つのエンドポイントの IP アドレスが同じ場合、最新のエンドポイント バインディング イベントによって、その ACI 接続から学習された既存の IP-SGT バインディングが上書きされます。

Cisco ACI サーバーとの接続が失われると、接続が再確立されるときに、Cisco ISE でデータが再同期されます。

Cisco ISE リリース 3.4 では、次の用語が変更されています。

Cisco ISE リリース 3.3 以前	**Cisco ISE リリース 3.4**
SXPマッピング	SGT バインディング
SXP ドメイン	SGT ドメイン

Cisco ACI 接続の追加

始める前に

- [管理（Administration）]>[システム（System）]>[展開（Deployment）]ページで、pxGrid および SXP サービスが有効になっていることを確認します。
- Cisco ACI が Cisco ISE pxGrid ノードの FQDN を解決できるように、Cisco ACI の DNS 設定を更新します。
- この統合には、Advantage、Premier、または 90 日間の評価ライセンスが必要です。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [ワークセンター（Work Centers）] > [TrustSec] > [統合（Integrations）] > [ACI] > [ACI接続（ACI Connections）]。

ステップ 2 [Add Connection] をクリックします。

ステップ 3 [それでは実行しましょう（Let's Do It）] をクリックします。

ステップ 4 [ACI接続の作成（Create ACI Connection）] ページで、次の詳細を入力します。

- [ACI接続名（ACI Connection Name）]：接続の名前を入力します。
- [FQDNまたはIPアドレス（FQDN or IP Address）]：Cisco ACI サーバーの IP アドレスまたは FQDN を入力します。
- [ACIユーザー名（ACI Username）]：Cisco ACI 管理者ユーザーのユーザー名を入力します。
- [ACIパスワード（ACI Password）]：Cisco ACI 管理者ユーザーのパスワードを入力します。
- [ACI証明書の検証（Validate ACI Certificate）]：このオプションを有効にすると、Cisco ISE は、信頼できる証明書ストア内の ACI コントローラの証明書を必要とするようになります。このオプションを無効にすると、Cisco ISE で ACI 証明書が検証されません。このオプションは、実稼働環境で有効にすることをお勧めします。Cisco ISE の信頼できる証明書ストアに証明書をインポートする方法については、信頼できる証明書ストアへのルート証明書のインポート（587 ページ）を参照してください。

  [テスト接続（Test Connection）] をクリックして、Cisco ACI サーバーとの接続性を確認します。

  このコントローラに接続すると、Cisco ISE は、同じ Cisco Application Policy Infrastructure Controller（APIC）サイトに接続されている他のコントローラの FQDN と IP アドレスを自動的に取得します。

  接続が確認されたら、[次へ（Next）] をクリックします。

ステップ 5 [命名規則（Naming Convention）] ページで、接続された Cisco ACI コントローラから受信した EPG および ESG から作成される SGT の命名規則を設定します。

次の種類の命名規則を使用して、最大 64 文字の SGT 名を作成できます。

- [ACI属性値を使用（Use ACI Attribute Values）]：新しく作成された SGT の名前を構成するために値を組み合わせる必要がある EPG または ESG 属性を選択します。これらの属性は、新しく作成された SGT 名のサフィックスに追加されます。次の属性の中から選択できます。
  - **接続名**
  - **テナント**
  - **VRF**
  - **アプリケーション プロファイル**
  - **エンドポイント グループ タイプ**

  デフォルトの属性値を使用するか、カスタム値を作成できます。

- [プレフィックスまたはサフィックスの追加（Append Prefix or Suffix）]：EPG または ESG の既存の名前に追加されるプレフィックスまたはサフィックスを入力します。

（注）
- 2.3.7.7 より前の Cisco Catalyst Center バージョンを使用している場合、SGT 名の文字数の上限は 32 です。
- 統合アプリケーションのいずれかが 32 文字を超える文字をサポートしていない場合は、Cisco ISE で SGT 名の命名規則を設定するときにこの制限を考慮する必要があります。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [EPG/ESGの選択（Select EPG/ESGs）] ページで、Cisco ISE に取得して SGT に変換する必要がある EPG または ESG を選択します。

初期セットアップ時に [すべて選択（Select All）] オプションを使用できます。SGT 番号範囲を設定した後は、リストされた EPG/ESG の数が設定された番号範囲より大きいと [すべて選択（Select All）] オプションを選択できません。

接続から入力されたセキュリティグループ名が Cisco ISE データベースにすでに存在する場合、SGT に新しい番号は割り当てられません。セキュリティグループ名が Cisco ISE データベースに存在しない場合は、導出された名前で新しいセキュリティグループが作成され、使用可能な SGT 範囲から SGT が割り当てられます。

この接続の編集中に、インバウンドまたはアウトバウンド SGT ドメインルールで使用されている EPG の選択を解除することはできません。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 （オプション）[SGT番号範囲の設定（Set SGT Numbering Range）] ページで [EPG/ESGへのSGT番号範囲の設定（Set SGT Numbering Range for EPG/ESGs）] オプションを有効にし、新しく作成された SGT の番号範囲を手動で設定します。

番号範囲の設定中も、既存の EPG と ESG、および予想される EPG と ESG を考慮します。

このオプションを無効にすると、Cisco ISE は、他の SGT で予約または使用されていない番号範囲の番号を SGT に自動的に割り当てます。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [サマリー（Summary）] ページで入力した詳細を確認します。必要に応じて、対応するセクションの [編集（Edit）] をクリックして詳細を更新できます。

ステップ 12 [作成（Create）] をクリックします。

Cisco ACI 接続が正常に作成されたかどうかを確認するには、次の手順を実行します。

- [ワークセンター（Work Centers）] > [TrustSec] > [統合（Integrations）] > [ACI] > [ACI接続（ACI Connections）] ページで、接続のステータスを確認します。
- **手順 7** で選択した EPG と ESG が、[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）] ページで、セキュリティグループに変換されているかどうかを確認します。
- **手順 7** で選択した EPG と ESG のバインディングが、[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SGTバインディング（SGT Bindings）] ページに表示されているかどうかを確認します。

[ワークセンター（Work Centers）] > [TrustSec] > [統合（Integrations）] > [ACI] > [ACI接続（ACI Connections）] ページから、接続の接続、一時停止、または削除を行うことができます。

接続に関連付けられているすべての SGT が削除されると、接続は [一時停止（Suspended）] 状態に移行します。接続が [一時停止（Suspended）] 状態の場合：

- その接続に関連するすべての SXP バインディングと MnT セッションデータが削除されます。
- ACI 接続サブスクリプションが一時停止されます。

（注）

- 名前変換ルールの変更は、この Cisco ACI 接続ですでに学習された EPG または ESG に自動的に適用されません。変更された名前の変換ルールを適用するには、最初に [同期されたEPG/ESG（Synced EPG/ESGs）] タブから以前に学習した EPG または ESG の選択を解除し、変更を保存する必要があります。その後、接続を再度編集して必要な EPG または ESG を選択し、変更を再度保存する必要があります。
- PSN が再起動された場合は、ACI 接続を一時停止して再接続し、ACI 接続の詳細を再入力する必要があります。
- 複数の ACI 接続を使用している場合は、同じ NAD をリッスンするように SXP ノードを同じように設定する必要があります。

インバウンドおよびアウトバウンド SGT ドメインルールの追加

Cisco ISE と Cisco ACI の間で共有されるデータを定義および管理するための、インバウンドおよびアウトバウンド SGT ドメインルールを作成できます。

インバウンド SGT ドメインルールを作成して、SGT バインディングを特定の SGT ドメインにマッピングできます。ルールが定義されていない場合、Cisco ACI から受信したバインディングはデフォルトの SGT ドメインに送信されます。

アウトバウンド SGT ドメインルールを作成して、特定の SGT バインディングのターゲット宛先を指定できます。

インバウンドまたはアウトバウンド SGT ドメインルールを作成するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [インバウンドおよびアウトバウンドSGTドメインルール（Inbound & Outbound SGT Domain Rules）]。

ステップ 2 インバウンド SGT ドメインルールを作成するには、次の手順を実行します。

a) [インバウンドSGTドメインルール（Inbound SGT Domain Rules）] タブで、[インバウンドルールの追加（Add Inbound Rule）] をクリックします。

b) [ルール設定（Rule Settings）] 領域に、インバウンド SGT ドメインルールの名前を入力します。

c) [有効（Enabled）] をクリックします。

d) [宛先（Destination）] ドロップダウンリストから、バインディングの送信先となる SGT ドメインを選択します。

[SGTドメインの作成（Create SGT Domain）] オプションを使用して新しい SGT ドメインを作成し、宛先リストに追加します。

e) [ルール設定（Rule Configuration）] 領域で、次の属性を使用してインバウンド SGT ドメインルールの条件を設定します。

- **EPG**
- **SGT名（SGT Name）**
- **ソース（Source）**
- **テナント（Tenant）**
- **VRF**

要件に基づいて AND または OR 条件を追加することもできます。

f) [追加（Add）] をクリックします。

g) [保存（Save）] をクリックします。

ステップ 3 アウトバウンド SGT ドメインルールを作成するには、次の手順を実行します。

a) [アウトバウンドSGTドメインルール（Outbound SGT Domain Rules）] タブで、[アウトバウンドルールの追加（Add Outbound Rule）] をクリックします。

b) [ルール設定（Rule Settings）] 領域に、アウトバウンド SGT ドメインルールの名前を入力します。

c) [有効（Enabled）] をクリックします。

d) [宛先（Destination）] ドロップダウンリストから、SGT の送信先となる Cisco ACI 接続とレイヤ 3 アウト（L3Outs）を選択します。

e) [ルール設定（Rule Configuration）] 領域で、次の属性を使用してアウトバウンド SGT ドメインルールの条件を設定します。

- **SGTドメイン（SGT Domains）**
- **SGT名（SGT Name）**

要件に基づいて AND または OR 条件を追加することもできます。

f) （オプション）[コントラクトの設定（Contract Configuration）] 領域で、共有セキュリティグループで使用および提供されるコントラクトを割り当てます。

g) [追加（Add）] をクリックします。

h) [保存（Save）] をクリックします。
アウトバウンドSGT ドメインルールを作成したら、[管理（Administration）]>[pxGridサービス（pxGrid Services）] > [診断（Diagnostics）] > [WebSocket] > [トピック（Topics）] ページで ACI コンシューマのステータスを確認できます。

インバウンドおよびアウトバウンドSGT ドメインルールは、[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [インバウンドおよびアウトバウンドSGTドメインルール（Inbound & Outbound SGT Domain Rules）] ページで確認できます。特定のフィルタ処理に使用する SGT バインディングテーブルを表示するには、その SGT バインディングの番号をクリックします。

SGTドメインの作成

SGT バインディングの配信を管理する SGT ドメインを作成できます。デフォルトでは、すべてのバインディングがデフォルト SGT ドメインに送信されます。

SGT ドメインを作成するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SGTドメイン（SGT Domains）]。

ステップ 2 [SGTドメインの作成（Create SGT domain）] をクリックします。

ステップ 3 [SGTドメイン名（SGT Domain Name）] フィールドに、SGT ドメインの名前を入力します。

ステップ 4 [保存（Save）] をクリックします。

各 SGT ドメインにマッピングされている SXP デバイスと SGT バインディングは、[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SGTドメイン（SGT Domains）] ページで表示できます。

ACI 接続および SGT ドメインルールに関連するオープン API は、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [API設定（API Settings）] ページの [TrustSec] カテゴリに表示されます。

SGTバインディング

[SGTバインディング（SGT Bindings）] ページで、Cisco ISE から Cisco ACI へ、およびその逆に送信されたすべてのバインディングを表示できます。[学習元（Learned From）]列には、Cisco ACI サーバーの IP アドレスと関連する PSN が表示されます。[学習者（Learned By）]列には、セッション、ローカル、SXP などのバインディングのタイプが表示されます。

SGT ドメインフィルタを作成して、異なる SGT ドメインにマッピングを送信できます。SGT ドメインフィルタを追加するには、次の手順を実行します。

1. [ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SGTバインディング（SGT Bindings）] の順に選択します。
2. [SGTドメインフィルタの追加（Add SGT Domain Filter）] をクリックします。
3. 次の手順を実行します。
   - サブネットの詳細を入力するか、[プライマリSGT（Primary SGT）] ドロップダウンリストから SGT を選択します。

     サブネットと SGT の両方を指定することもできます。
   - （オプション）[VN] フィールドで仮想ネットワークを指定します。
   - バインディングを送信する必要がある SGT ドメインを選択します。
4. [保存（Save）] をクリックします。

フィルタを更新するには、[SGTドメインフィルタの管理（Manage SGT Domain Filter）] をクリックします。

（注） インバウンド SGT ドメインルールによって割り当てられた SGT ドメインは、SGT ドメインフィルタによって上書きされます。

Cisco ACI 統合の互換性マトリックス

新しい ACI 接続ワークフローには、次のバージョンが必要です。

製品	バージョン
Cisco ISE	3.4 以降
Cisco ACI	6.1.1 以降
SD-WAN	20.12.2（検証済みバージョン）
Cisco Catalyst Center	2.3.7.7 以降
Cisco Firepower Management Center	7.2.5（検証済みバージョン）

ACI コネクタのデバッグログ

ACI コネクタでのデバッグログのシビラティ（重大度）レベルは、[操作（Operations）] > [トラブルシュート（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグプロファイルの設定（Debug Profile Configuration）] ページで設定できます。PAN、SXP、および pxGrid ノードの [ACIコネクタ（ACI Connector）] コンポーネントに対応するログレベルを [DEBUG] に設定する必要があります。

ACI コネクタでは、次のログファイルを使用できます（/opt/CSCOcpm/logs の下）。

- workloads.log
- aciconn/aciconn.log
- api-service.log
- ise-psc.log
- pxgriddirect-service.log
- sxp_appserver/sxp.log

Cisco ACI 統合で発生するアラーム

ACI 統合に対して次のアラームが生成されます。

- EPG、ESG、または L3Out が Cisco ACI で削除されると、対応するオブジェクトが Cisco ISE で削除されます。これらのオブジェクトのいずれかがインバウンドルールまたはアウトバウンドルールに含まれている場合、アラームが発生してユーザーに通知されます。
- Cisco ACI で mdpConn オブジェクトが削除されると、Cisco ISE は設定変更を学習し、同じ状態に対してアラームを生成します。
- Cisco ACI で EEPG が削除されると、Cisco ISE は設定変更を学習し、同じ状態に対してアラームを生成します。

- Cisco ISE で ACI 接続を削除するときに、プロセスが学習した SGT と SGT 範囲の削除に失敗すると、アラームが発生します。
- Cisco ACI イベントをリッスンしている Cisco ISE リスナーが Cisco ACI から切断されると、アラームが発生します。これは、ACI パスワードの変更、証明書の有効期限、またはネットワーク接続の問題が原因で発生する可能性があります。

レガシー ACI 統合から新しい ACI 接続ワークフローへの移行

レガシー ACI 統合から新しい ACI 接続ワークフローに移行するには、次の手順を実行します。

1. [ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ACI の設定（ACI Settings）] の順に選択します。
2. [ACI統合の有効化（Enable ACI Integration）] チェックボックスをオフにします。
3. [ワークセンター（Work Centers）] > [TrustSec] > [統合（Integrations）] > [ACI] > [ACI接続（ACI Connections）] ページを使用して、新しい Cisco ACI 接続を追加します。詳細については、「Cisco ACI 接続の追加 （1663 ページ）」を参照してください。

（注）

- Cisco ISE との既存の ACI 統合を削除すると、この統合を通じて学習されたすべてのデータが Cisco ISE と Cisco ACI の両方から削除されます。
- 移行中にポリシーの適用が中断される可能性があるため、この移行はメンテナンス期間中に実行することをお勧めします。

仮想ネットワーク認識による Cisco ACI と Cisco SD-Access の統合

Cisco ISE リリース 3.0 では、Cisco Software-Defined Access（SD-Access）ファブリックと Cisco ACI インフラストラクチャの情報交換とクロスドメイン自動化の変換が強化されています。この実装では、次の機能がサポートされています。

- EPG 情報と SGT 情報の交換と変換
- Cisco ACI ファブリックへの Cisco SD-Access 仮想ネットワークの拡張
- Cisco SD-Access と Cisco ACI ファブリックデータプレーンの自動化
- IP-SGT バインディングの交換

- pxGrid ドメインと SGT ドメインへのバインディングの送信

Cisco ISE は、RADIUS バインディングまたは Cisco ACI バインディングから仮想ネットワーク情報を学習し、特定の仮想ネットワークのローカルスタティックマッピングを提供します。仮想ネットワークを使用して SXP フィルタロジックを強化できます。このロジックは、Cisco ACI との IP-SGT バインディングの共有を調整するためにも活用されます。Cisco ACI まで拡張されている仮想ネットワークは Cisco ACI との IP-SGT バインディングを共有する唯一の構造であるという点で、SGT ドメインと仮想ネットワークが密接にリンクされています。そのため、特定の SGT ドメイン（SD-Access- プレフィックスで示される）は Cisco ISE で同等な仮想ネットワーク（SD-Access- プレフィックスなしの SGT ドメイン）にマッピングされます。

Cisco SD-Access ボーダーノードが Cisco ACI バインディングを認識できるようにするために、Cisco ACI バインディングは、SXP フィルタロジックを介して送信される前に、すべての拡張仮想ネットワークから発信されたものとして複製されます。たとえば、Cisco SD-Access 仮想ネットワーク 1、仮想ネットワーク 2、および仮想ネットワーク 3 が Cisco ACI に拡張されている場合、Cisco ACI から元の Cisco ACI 仮想ネットワークへのバインディングは SXP フィルタを介して 4 回送信されます。これとまったく同じバインディングがフィルタを通過して、4 つすべての仮想ネットワークに送信されます。フィルタは、特定の展開要件に従って変更およびカスタマイズできます。ただし、複製は常にすべての拡張仮想ネットワークに対して行われます。

Cisco ISE は、可能な場合は常に Cisco ACI から IP-SGT、EPG バインディングを学習します。ただし、Cisco ISE は Cisco ACI にバインディングを強制的に学習させることはできません。Cisco ACI は、Cisco ISE からのバインディングを明示的に要求する必要があります。

次の表に、Cisco ISE での IP-SGT または IP-EPG バインディングで考えられる送信元と宛先の組み合わせを示します。

送信元ドメイン	宛先ドメイン	送信元グループ	宛先グループ	注記
Cisco ACI	SXP	Cisco ACI 仮想ネットワーク	SGT ドメイン	Cisco ACI 仮想ネットワークは、1 つ以上の SGT ドメインとバインディングを共有する SXP フィルタのキーとして使用できます。
Cisco ACI	pxGrid	Cisco ACI 仮想ネットワーク	pxGrid の SXP トピックに対する VPN	Cisco ACI 仮想ネットワークを SXP フィルタのキーとして使用して、pxGrid 上の 1 つ以上の SXP VPN とバインディングを共有できます。

Cisco ACI	Cisco SD-Access ボーダーノード	Cisco SD-Access 拡張仮想ネットワーク	SGT ドメイン	Cisco ACI バインディングは、ボーダーノード仮想ネットワークの情報交換用に自動作成されるすべての SGT ドメイン（“SD-Access-“ プレフィックス付きドメイン）と共有されます。
Cisco ISE スタティックマッピング	SXP	Cisco SD-Access 仮想ネットワークまたは既存の SGT ドメイン	SGT ドメイン	スタティックバインディングは、SGT ドメインに直接送信するか（スタティックマッピングで SGT ドメインを指定）、または SXP フィルタを介して（仮想ネットワーク情報とともに）送信できます。仮想ネットワークが指定されていない場合、SXP フィルタは仮想ネットワークに DEFAULT_VN を使用します。

Cisco ISE スタティックマッピング	pxGrid	Cisco SD-Access 仮想ネットワーク	SGT ドメイン	スタティックバインディングは、SGT ドメインに直接送信するか（スタティックマッピングで SGT ドメインを指定）、または SXP フィルタを介して（仮想ネットワーク情報とともに）送信できます。仮想ネットワークが指定されていない場合、SXP フィルタは仮想ネットワークに DEFAULT_VN を使用します。
Cisco ISE スタティックマッピング	Cisco ACI	Cisco SD-Access 仮想ネットワーク	Cisco SD-Access 仮想ネットワーク	Cisco SD-Access 仮想ネットワークは Cisco ACI（mdpExtendvirtualnetworkReq）に拡張する必要があります。バインディングは SXP フィルタ内の仮想ネットワークを使用し、仮想ネットワークにマッピングした SGT ドメインとのバインディングを Cisco ACI に送信します。
SXP	pxGrid	SGT ドメイン	SGT ドメイン	SGT ドメインは pxGrid の SXP トピック内に VPN として表示されます。

SXP	Cisco ACI	SGT ドメイン	Cisco SD-Access 仮想ネットワーク	SGT ドメイン共有は、Cisco ACI 設定で選択されます。 Cisco SD-Access 仮想ネットワークによって自動作成された SGT ドメイン（仮想ネットワークに相当する SGT ドメイン）のみが共有されます。 仮想ネットワークがバインディングを共有できるようにするには、Cisco SD-Access 仮想ネットワークを Cisco ACI に拡張する必要があります。 バインディングは、Cisco ACI がエンドポイントデータを要求するコンシューマサービスの一部である必要があります。
SXP	SXP	SGT ドメイン	SGT ドメイン	優先順位付けによって行われる SXP バインディングは共有されます。

RADIUS バインディング	Cisco ACI	Cisco SD-Access 仮想ネットワーク	Cisco SD-Access 仮想ネットワーク	RADIUS バインディングは SXP フィルタを介して（仮想ネットワーク情報とともに）送信されます。バインディングに仮想ネットワークが指定されていない場合、SXPフィルタは仮想ネットワークに DEFAULT_VN を使用します。
RADIUS バインディング	pxGrid	Cisco SD-Access 仮想ネットワーク	Cisco SD-Access 仮想ネットワーク	RADIUS バインディングは、トピックに仮想ネットワークフィールドが追加された pxGrid 上のセッションディレクトリ トピックになります。
RADIUS バインディング	SXP	Cisco SD-Access 仮想ネットワーク	SGT ドメイン	Cisco SD-Access 仮想ネットワークを SXP フィルタのキーとして使用して、バインディングを共有する SGT ドメインを選択できます。

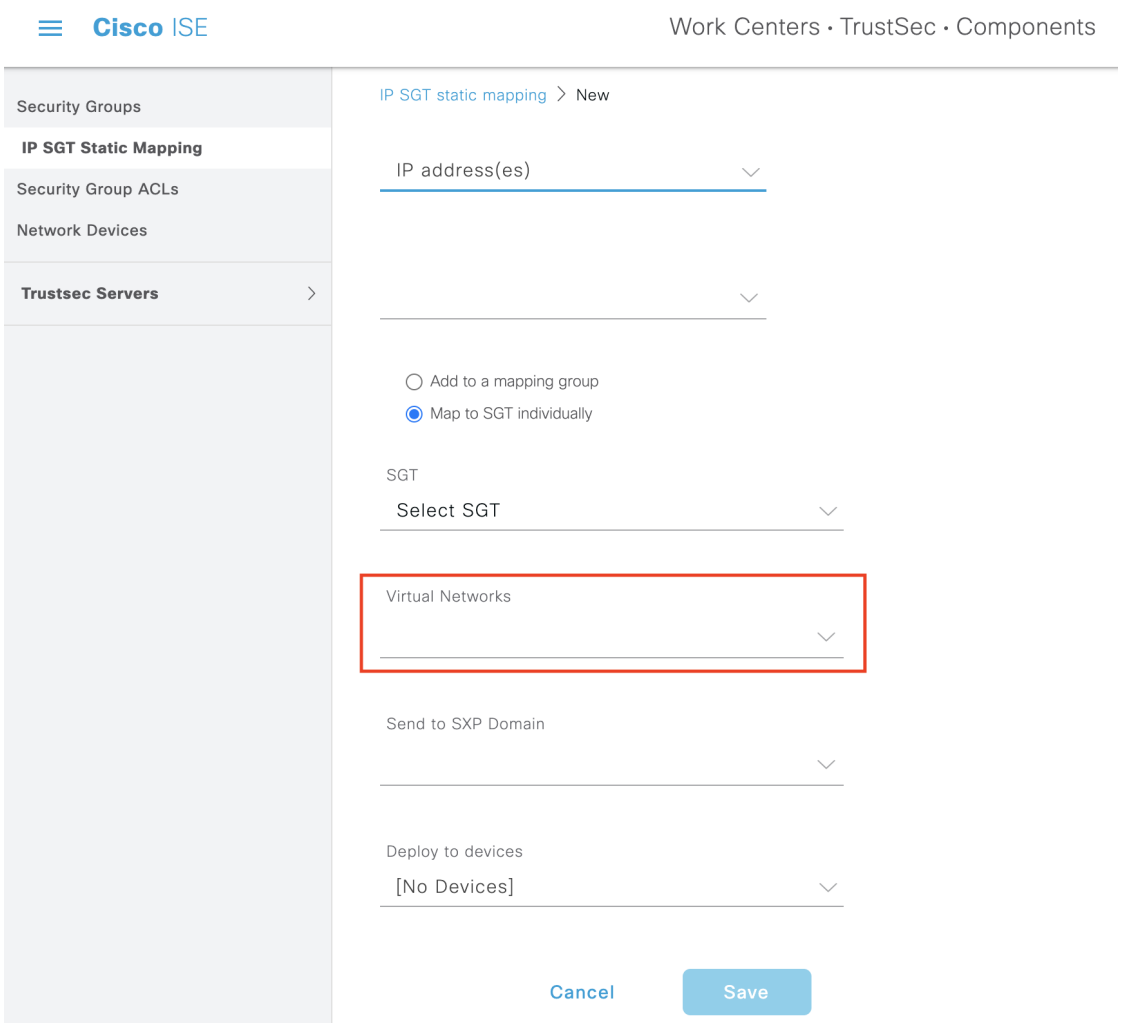
クロスドメインサポートを促進するには、1 つのポリシードメインまたはポリシードメイン内の転送ドメインから別のポリシードメインへ（およびその逆に）さまざまなネットワーク転送ドメイン（ IP アドレス、サブネットマスク、セキュリティグループタグ、EPG、仮想ネットワーク、Virtual Route Forwarding（VRF）など、）を交換したり、フィルタ処理を行ったりできる必要があります。これは、ポリシードメイン（Cisco SD-Access、ACI、SD-WAN、CPC、Meraki など）に複数の転送ドメインがある場合に特に重要です。

ポリシードメインのネットワーク固有の転送ドメインと、他のポリシードメインから学習したすべてのセッションやバインディングのドメイン固有の属性を識別、キャプチャ、および保存できます。これらの情報は、特定の SGT ドメインへのセッションとバインディングをフィルタ処理するためにポリシー管理者によって使用されます。また、管理者は、ある転送ドメインから別の転送ドメインへの特定のバインディングのみをマッピングまたはフィルタ処理するポリシーを作成できます。

Cisco ISE 3.0 以降では、Catalyst Center の Cisco ISE によって学習されたすべての仮想ネットワークを使用して、[SXPデバイス（SXP Devices）] ウィンドウに SXP フィルタと SGT ドメインが自動的に作成されます。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXP デバイス（SXP Devices）]**。それらの SGT ドメインは、Cisco ACI と共有されるバインディングに仮想ネットワークを設定するために使用されます。

[IP-SGTスタティックマッピング（IP-SGT Static Mapping）] ウィンドウで、IP-SGT スタティックマッピングへの仮想ネットワークを追加および編集できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）]**。[追加（Add）] をクリックして新しいマッピングを追加するか、または [編集（Edit）] をクリックして既存のマッピングを変更します。

図 *69 : IP SGT* スタティックマッピングでの仮想ネットワークの追加



Cisco ACI と Cisco SD-Access の統合のための Cisco ISE の設定

このタスクは、Cisco ACI と Cisco SD-Access の統合をサポートするように Cisco ISE を設定するのに役立ちます。

始める前に

Cisco ISE が Catalyst Center の最新バージョンと統合されていて、使用されている APIC バージョンが 5.1 以降であることを確認します。

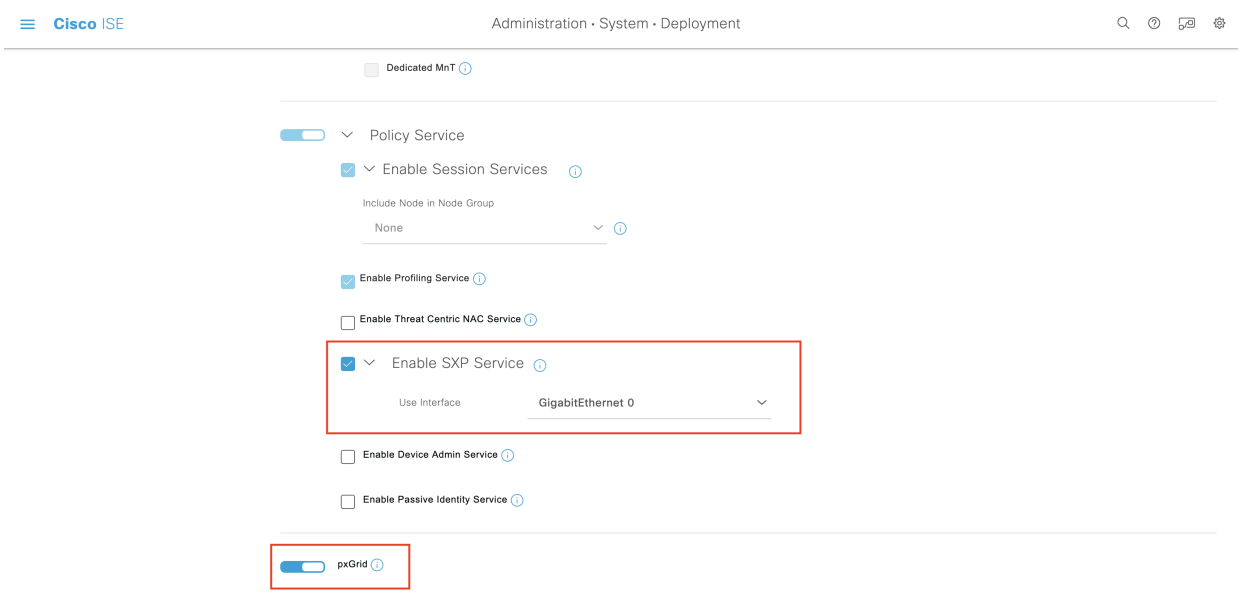
ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 ノードリストから、SXP および pxGrid サービスを有効にするノードの横にあるチェックボックスをオンにします。

ステップ 3 次の図に示すように、[ポリシーサービス（Policy Service）] セクションまでスクロールし、pxGrid および SXP サービスを有効にします。

Cisco ISE で複数のインターフェイスを有効にしている場合は、[SXP サービスの有効化（Enable SXP Service）] 領域で、SXP 接続を保持するインターフェイスを指定します。

図 *70 : SXP* および *pxGrid* サービスの有効化



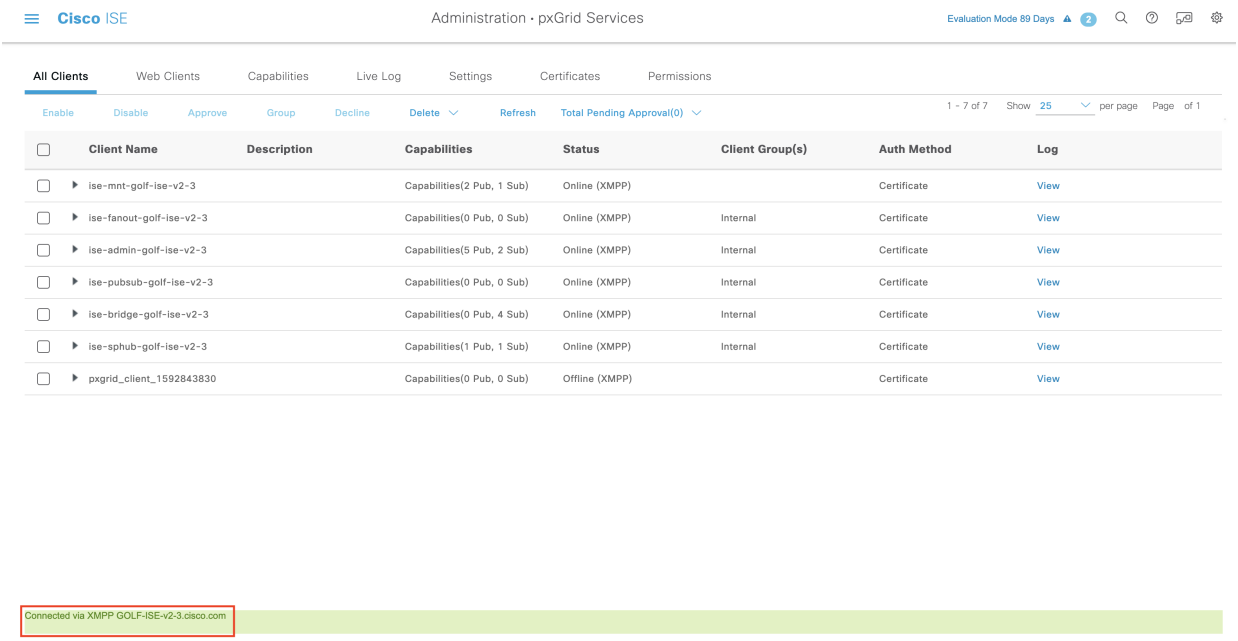
ステップ 4 [保存（Save）] をクリックします。

ステップ 5 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [すべてのクライアント（All Clients）]** を選択します。

ステップ 6 pxGrid サービスが稼働しているかどうかを確認します。

次の図に示すように、接続が成功したことを示す通知がウィンドウの左下隅に表示されます。

図 *71 : pxGrid* サービスへの接続の確認



ステップ 7 APIC コントローラブラウザから APIC 証明書をダウンロードします。証明書を表示して PEM ファイルとしてダウンロードするには、ブラウザのアドレスバーにあるロックアイコンをクリックします。

ステップ 8 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 9 [信頼できる証明書（Trusted Certificates）] ウィンドウで、ダウンロードした APIC 証明書ファイルをインポートします。

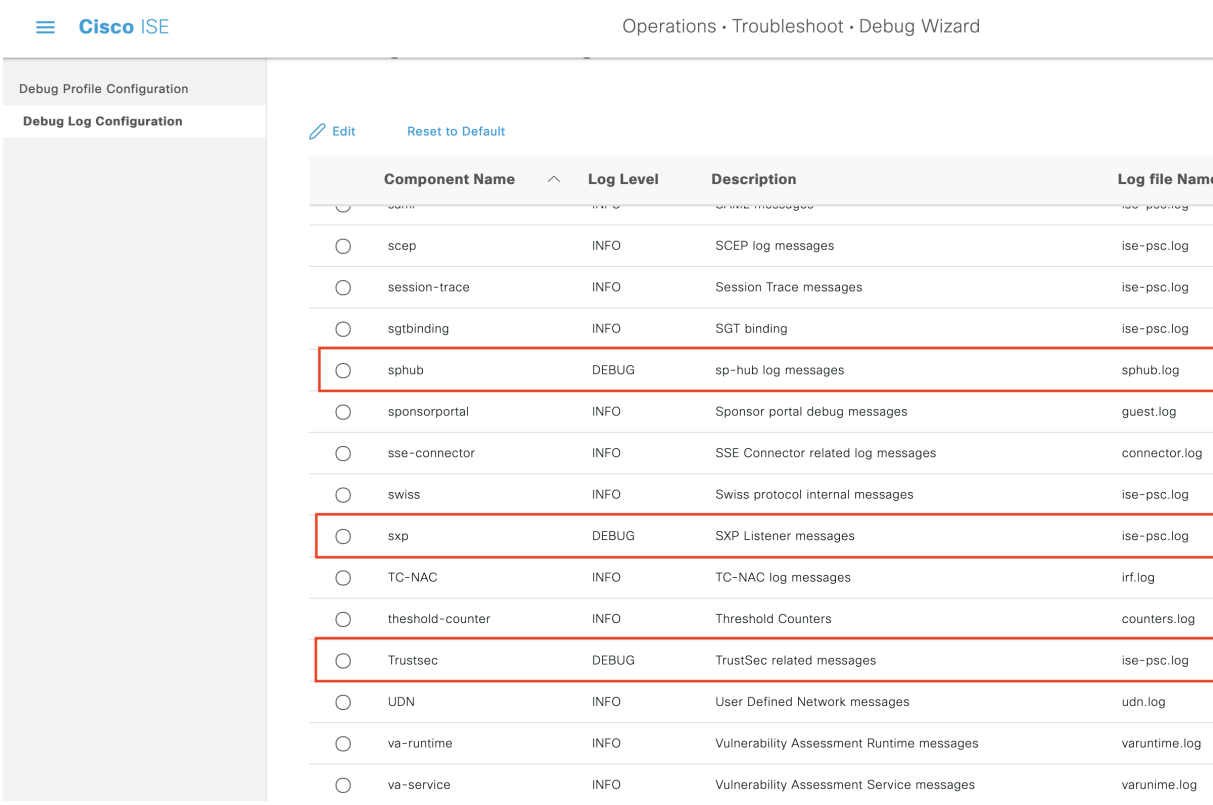
ステップ 10 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ACI 設定（ACI Settings）]** を選択します。

ステップ 11 必要に応じて ACI 設定を設定します。

Cisco ACI と Cisco SD-Access の統合の確認

Cisco ACI と Cisco SD-Access 接続間の詳細情報を取得するには、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグログの設定（Debug Log Configuration）]** を選択します。SXP サービスと pxGrid サービスが有効になっている Cisco ISEノードを選択し、[編集（Edit）] をクリックします。次の図に示すように、[spbhub]、[sxp]、および [TrustSec] の各コンポーネントのログレベルを [デバッグ（DEBUG）] に設定します。

図 *72* : デバッグログの有効化



ログは [ログのダウンロード（Dowload Logs）] ウィンドウからダウンロードできます（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]>[トラブルシューティング（Troubleshoot）]>[ログのダウンロード（Download Logs）]**）。[サポートバンドル（Support Bundle）] タブからサポートバンドルをダウンロードするか、または [デバッグログ（Debug Logs）] タブから特定のデバッグログをダウンロードするかを選択できます。

さらに、TrustSec ダッシュボード（1594 ページ）は、Cisco ACI の統合から学習した情報で強化されています。これは、Cisco ACI 関連の問題のトラブルシューティングに役立ちます。

Catalyst Center がドメインアドバタイズメントを送信した後、Cisco ISE の [信頼できる証明書（Trusted Certificates）] ウィンドウと [システム証明書（System Certificates）] ウィンドウの両方で APIC 証明書が APIC ドメインマネージャから取得されているかどうかを確認します。

図 *73 : [*システム証明書（***System Certificates***）*]* ウィンドウでの証明書の確認

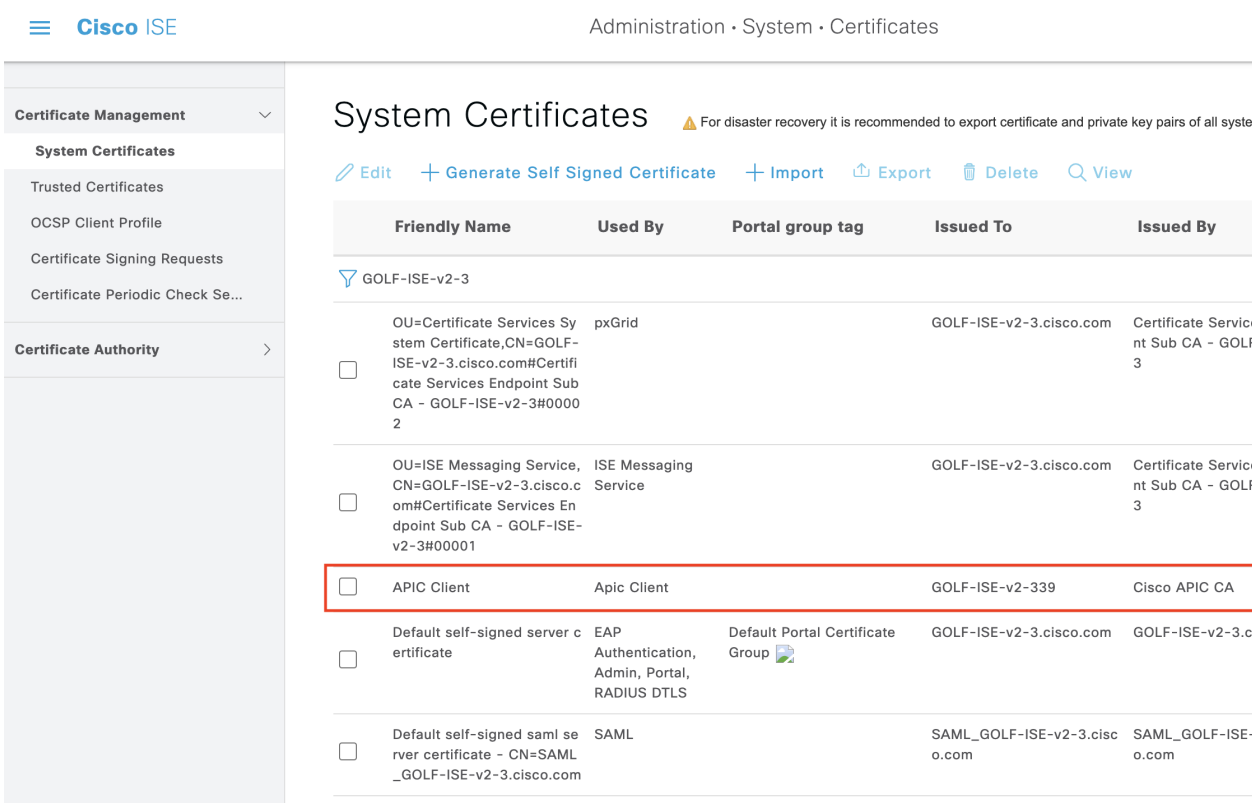
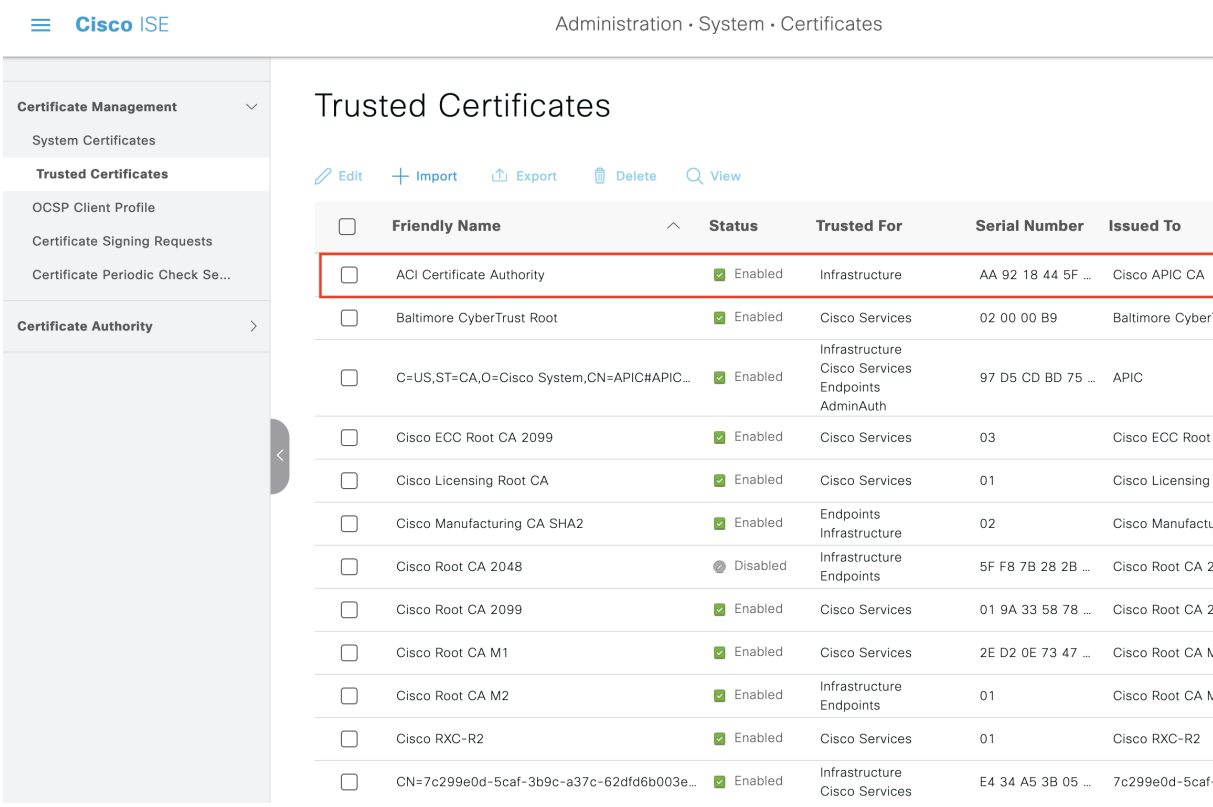


図 *74 : [*信頼できる証明書（***Trusted Certificates***）*]* ウィンドウでの証明書の確認



ユーザー レポート別上位 N 個の RBACL ドロップの実行

ユーザー レポート別上位 N 個の RBACL ドロップを実行して、特定のユーザーによるポリシー違反（パケット ドロップに基づく）を表示できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [レポート（Reports）] > [TrustSec]** を選択します。

ステップ 2 [ユーザー別上位 N 個の RBACL ドロップ（Top N RBACL Drops by User）] をクリックします。

ステップ 3 [フィルタ（Filters）] ドロップダウン メニューから、必要なモニター モードを追加します。

ステップ 4 選択したパラメータの値をこれに応じて入力します。[強制モード（Enforcement mode）] ドロップダウン リストから、[強制（Enforce）]、[モニター（Monitor）]、または [両方（Both）] としてモードを指定できます。

ステップ 5 [時間範囲（Time Range）] ドロップダウン メニューから、レポート データを収集する期間を選択します。

ステップ 6 [実行（Run）] をクリックして、選択したパラメータとともに特定の期間のレポートを実行します。

Cisco Meraki ダッシュボードと Cisco ISE の接続

Cisco ISE およびクラウドベースの Cisco Meraki は、TrustSec ポリシーのポリシー管理ポイントである TrustSec 対応システムです。Cisco と Meraki の両方のネットワークデバイスを使用している場合、1 つ以上の Cisco Meraki ダッシュボードを Cisco ISE に接続して、TrustSec ポリシーおよび要素を Cisco ISE から各組織に属する Cisco Meraki ネットワークに複製できます。

Cisco Meraki の TrustSec 統合は、プライマリ PAN で実行されるオンプレミスサービスです。フェールオーバーが発生した場合、統合サービスは、新しく昇格したプライマリ PAN で引き続き機能します。Cisco Meraki サービスの TrustSec 統合は、次の機能を実行します。

- 指定された Cisco Meraki 組織で、選択された Cisco ISE TrustSec ポリシーとその構成要素であるセキュリティグループ ACL（SGACL）およびセキュリティグループタグ（SGT）を複製します。

  Meraki 適応型ポリシーでサポートされている形式に準拠する TrustSec ポリシーのみを選択できます。SGACL などのポリシー要素の形式要件については、「Cisco Meraki Dashboard Organizational Structure」を参照してください。

- 既存の情報が編集された場合、既存の TrustSec ポリシーまたはポリシー要素を新しいバージョンで上書きします。上書きは、Cisco ISE ポリシーが完全である場合にのみ発生します。空または不完全なポリシーは同期されません。

  Cisco ISE と Cisco Meraki ダッシュボードを接続するときに、同じ送信元と宛先に対して設定された異なる TrustSec ポリシーが 2 つのシステムにある場合、Cisco ISE TrustSec ポリシーが Cisco Meraki の TrustSec ポリシーに置き換わります。

（注） Cisco Meraki 適応型ポリシーを Cisco ISE に転送することはできません。

- 複製されたポリシーを Cisco ISE で編集すると、Cisco Meraki でも同じように更新されます。たとえば、Cisco Meraki に複製された Cisco ISE TrustSec ポリシーに SGACL を追加すると、その SGACL は、Cisco Meraki ダッシュボードの対応するポリシーにも自動的に表示されます。

- Cisco Meraki の TrustSec 統合では、Cisco Meraki のポリシーまたはポリシー要素は削除されません。Cisco ISE でポリシーまたはポリシー要素を削除するときは、Cisco Meraki でもそれらを削除する必要があります。

Cisco ISE は、設定された同期間隔（5 ～ 30 分）で、選択された TrustSec イーグレスポリシーを接続先の Cisco Meraki ダッシュボードと同期します。ただし、TrustSec ポリシーを Cisco Meraki に直接追加し、必要に応じていつでも手動同期をトリガーすることもできます。Cisco Meraki API は、Meraki ダッシュボードから受信した応答を使用して同期のスケール制限を決定するために使用されます。Cisco Meraki のスケール制限の詳細については、『Cisco Meraki Adaptive Policy Configuration Guide』を参照してください。

Cisco ISE は、同期するイーグレスポリシーの選択時に Meraki のスケール制限を超えないようにします。

（注） Cisco ISE ユーザーがダウングレードすると、ユーザーが Cisco ISE と Cisco Meraki 間で同期した既存のポリシー、ダッシュボード、および組織はアクティブなままになります。ただし、ユーザーはポリシーを追加したり、ダッシュボードと組織に設定変更を加えたりすることはできません。

Cisco ISE は、設定された Cisco Meraki ダッシュボード接続に対し、クラウドごとに 1 つの接続のみをサポートします。同じ情報がすべての Cisco Meraki 組織に転送されます。

始める前に

Cisco ISE を Cisco Meraki ダッシュボードに接続し、TrustSec ポリシーおよびポリシー要素を共有するワークフローでは、次の情報が必要になります。

Cisco ISE で、次の手順を実行します。

- Cisco ISE Advantage ライセンス
- 同期する TrustSec イーグレスポリシー
- 同期する SGACL
- 同期する SGT

イーグレスポリシーの詳細については、「出力ポリシー（1620ページ）」を参照してください。

SGACL および SGT の詳細については、「TrustSec のコンポーネント（1589 ページ）」を参照してください。

Cisco Meraki：

- Cisco ISE と同期するすべての Cisco Meraki 組織にアクセスする権限のある Cisco Meraki アカウントが必要です。このアカウントから、Cisco ISE で Cisco Meraki ダッシュボードにアクセスするために使用できる API キーを生成する必要があります。
- Cisco Meraki ポータルで、Cisco ISE に接続する各組織の Meraki ダッシュボード API アクセスも有効にする必要があります。

組織、API ホスト名とキー、ダッシュボード API アクセスなどの概念については、「Cisco Meraki Dashboard Organizational Structure」を参照してください。

ステップ 1 Cisco ISE 管理ポータルで、**[ワークセンター（Work Centers）]** > **[TrustSec]** > **[統合（Integrations）]** > **[Meraki]** > **[概要（Overview）]** を選択します。

ステップ 2 [Merakiの接続（Connect Meraki）] をクリックして、Cisco Meraki ダッシュボードと組織を Cisco ISE に接続するワークフローを開始します。

ステップ 3 [ようこそ（Welcome）] ウィンドウで、[始める（Let's do it）] をクリックします。

ステップ 4 [接続の追加（Add Connections）] ウィンドウで、[Cisco Merakiダッシュボード API ホスト名（Cisco Meraki dashboard API hostname）] ドロップダウンリストから、必要なオプションを選択します。

ステップ 5 [APIキー（API Key）] フィールドに、対応する値を入力します。API キーの詳細については、「Cisco Meraki Dashboard API」を参照してください。

ステップ 6 [接続（Connect）] をクリックして、選択した Cisco Meraki ダッシュボードを Cisco ISE と統合します。

ステップ 7 接続が完了すると、選択した API キーに接続されているすべての組織が [Meraki組織の選択（Choose Meraki Organization）] ドロップダウンリストに表示されます。このリストを使用して、Cisco ISE と同期する組織を選択できます。

ステップ 8 （任意）[+] アイコンをクリックして、その他の Cisco Meraki ダッシュボードを Cisco ISE に追加します。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [同期間隔の設定（Set Up Sync Interval）] ウィンドウの [同期間隔（Sync Interval）] フィールドに、5 ～ 30 の値を入力します。この値は、接続された Cisco ISE システムと Cisco Meraki システム間の同期頻度を定義します。デフォルトの同期間隔は 12 分です。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [イーグレスポリシーの選択（Select Egress Policy）] ウィンドウで、Cisco Meraki と同期する TrustSec イーグレスポリシーの横にあるチェックボックスをオンにします。

Meraki 適応型ポリシーでサポートされている形式に準拠していないイーグレスポリシーは選択できません。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 14 [追加のSGACLの選択（Select Additional SGACLs）] ウィンドウでは、[イーグレスポリシーの選択（Select Egress Policy）] ウィンドウで選択したイーグレスポリシーに関連付けられている SGACL があらかじめ選択されています。同期する SGACL をさらに選択するには、対応する SGACL の横にあるチェックボックスをオンにします。

Meraki 適応型ポリシーでサポートされている形式に準拠していない SGACL は選択できません。

ステップ 15 [次へ（Next）] をクリックします。

ステップ 16 [追加のSGTの選択（Select Additional SGTs）] ウィンドウでは、[イーグレスポリシーの選択（Select Egress Policy）] ウィンドウで選択したイーグレスポリシーに関連付けられている SGT があらかじめ選択されています。同期する SGT をさらに選択するには、対応する SGT の横にあるチェックボックスをオンにします。

ステップ 17 [次へ（Next）] をクリックします。

ステップ 18 [概要（Summary）] ウィンドウで、ワークフローで定義したすべての構成を確認し、[完了（Finish）] をクリックします。

ワークフローが完了すると、最初の同期サイクルが実行され、この最初の同期の結果が [同期ステータス（Sync Status）] ページに表示されます。

Cisco ISE での Cisco Meraki 接続の表示と変更

Cisco Meraki を Cisco ISE に接続した後、[同期ステータス（Sync Status）]、[接続（Connections）]、および [同期の選択（Sync Selections）] ウィンドウで接続構成を監視および編集できます。

同期ステータス（Sync Status）

[同期ステータス（Sync Status）] ウィンドウには、最新の同期サイクルに関連する情報が、[イーグレスポリシー（Egress Policies）]、[ACL（ACLs）]、および [SGT（SGTs）] タブにグループ化されて表示されます。

[同期ステータス（Sync Status）]ページの左上隅には、選択したイーグレスポリシー、SGACL、およびセキュリティグループのうち、すべての Cisco Meraki 組織に正常に同期された数が表示されます。選択したイーグレスポリシー、SGACL、およびセキュリティグループのすべてまたは一部を受信した、あるいはいずれも受信していない Cisco Meraki 組織の数に関する情報も表示されます。

Cisco ISE で特定の項目を正常に同期できない場合は、[同期ステータス（Sync Status）] ページの下部に表示される 3 つのタブで、選択したイーグレスポリシー、SGACL、およびセキュリティグループに関するこの情報を確認できます。

同期ステータステーブルの [組織（Organizations）] 列の数字をクリックして、個々の組織の特定の項目の同期ステータスを表示します。同期に失敗した場合は、その理由と修復方法が表示されます。

[同期ステータス（Sync Status）] ペインの右上隅には、次の情報が含まれています。

- [同期間隔（Sync Interval）]：現在適用されている同期間隔が表示されます。同期間隔の値をクリックして、ドロップダウンリストから別の間隔を選択できます。
- [データ同期までの時間（Data Sync In）]：次にスケジュールされている同期までのカウントダウンタイマーが表示されます。
- [今すぐ同期化（Sync Now）]：[今すぐ同期化（Sync Now）] をクリックすると、すぐに同期を開始できます。
- [同期の一時停止（Pause Sync）]：[同期の一時停止（Pause Sync）] をクリックすると、同期スケジュールを一時停止できます。[同期の一時停止（Pause Sync）] オプションに代わって表示される [同期の再開（Resume Sync）] をクリックするまで、同期スケジュールは一時停止されます。

  同期を再開すると、すぐに同期サイクルがトリガーされて同期スケジュールが新たに開始されます。

接続（Connections）

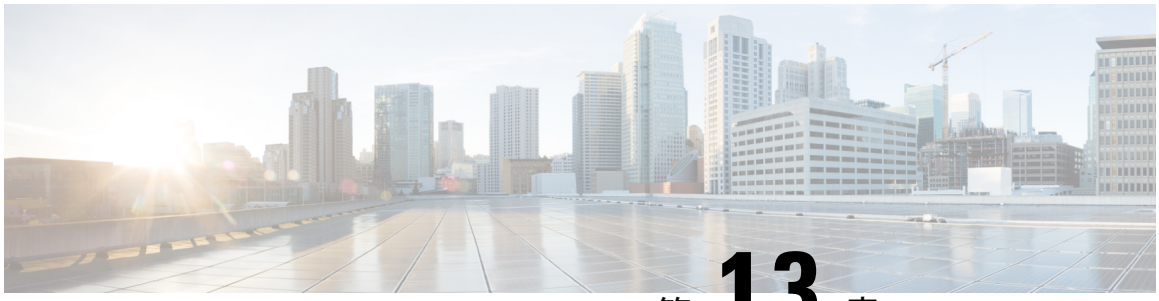
[接続（Connections）] ウィンドウで、Cisco Meraki 接続を表示および変更できます。Cisco ISE に接続した Cisco Meraki ダッシュボードのリストがこのウィンドウに表示されます。

Cisco Meraki 組織を追加および削除できます。組織が削除されると、Cisco ISE はその組織との同期を行わなくなりますが、以前に同期されていた Cisco ISE ポリシーは削除された組織に残ります。

同期の選択（Sync Selections）

[同期の選択（Sync Selections）] ウィンドウでは、接続された Cisco Meraki ダッシュボードと共有するように設定されている TrustSec ポリシーとポリシー要素を表示および変更できます。項目の選択を解除すると、Cisco ISE はその項目の同期を行わなくなりますが、その項目は組織から削除されません。

（注） Cisco ISE の TrustSec ポリシーを Cisco Meraki ダッシュボードと同期するためのモニタリングログ（meraki-connector.log および meraki-sync-service.log）は、Meraki コネクタで維持されるデバッグログで確認できます。



第 13 章

コンプライアンス

- ポスチャ タイプ （1688 ページ）
- エージェントレス ポスチャ （1690 ページ）
- エージェントレスポスチャのトラブルシューティング （1695 ページ）
- ポスチャ管理の設定 （1696 ページ）
- ポスチャの全般設定 （1705 ページ）
- Cisco ISE へのポスチャ更新のダウンロード （1706 ページ）
- ポスチャの利用規定の構成設定 （1709 ページ）
- ポスチャ評価の利用規定の設定 （1711 ページ）
- ポスチャ条件 （1711 ページ）
- コンプライアンス モジュール （1717 ページ）
- ポスチャ コンプライアンスのチェック （1718 ページ）
- パッチ管理条件の作成 （1718 ページ）
- ディスク暗号化条件の作成 （1719 ページ）
- ポスチャ条件の設定 （1720 ページ）
- スクリプト条件の追加 （1751 ページ）
- ポスチャ ポリシーの設定 （1755 ページ）
- エージェントのワークフローの設定 （1758 ページ）
- 証明書ベースの条件のための前提条件 （1759 ページ）
- デフォルトのポスチャ ポリシー （1760 ページ）
- クライアント ポスチャ評価 （1762 ページ）
- ポスチャ評価オプション （1762 ページ）
- ポスチャ修復オプション （1763 ページ）
- ポスチャのカスタム条件 （1764 ページ）
- ポスチャ エンドポイント カスタム属性 （1765 ページ）
- エンドポイント カスタム属性を使用したポスチャ ポリシーの作成 （1765 ページ）
- カスタム ポスチャ修復アクション （1766 ページ）
- ポスチャ評価要件 （1773 ページ）
- ポスチャ再評価の構成設定 （1777 ページ）
- ポスチャのカスタム権限 （1779 ページ）

- 標準許可ポリシーの設定 （1780 ページ）
- ポスチャとネットワーク ドライブ マッピングのベスト プラクティス （1781 ページ）
- エージェントステルスモードのワークフローの設定 （1781 ページ）
- エージェントステルスモード通知の有効化 （1786 ページ）
- Cisco Temporal Agent のワークフローの設定 （1787 ページ）
- ポスチャのトラブルシューティング ツール （1789 ページ）
- エンドポイント ログイン クレデンシャルの設定 （1790 ページ）
- エンドポイントスクリプト設定 （1790 ページ）
- Cisco ISE でのクライアント プロビジョニングの設定 （1791 ページ）
- クライアント プロビジョニン リソース （1792 ページ）
- ネイティブ サプリカント プロファイルの作成 （1799 ページ）
- 各種ネットワークでの URL リダイレクトなしでのクライアント プロビジョニング （1802 ページ）
- AMP イネーブラ プロファイルの設定 （1804 ページ）
- Cisco ISE の Chromebook デバイスのオンボーディングのサポート （1808 ページ）
- Cisco Secure クライアント （1822 ページ）
- ポスチャステータスの同期 （1829 ページ）
- Cisco Web Agent （1832 ページ）
- クライアント プロビジョニング リソース ポリシーの設定 （1832 ページ）
- クライアント プロビジョニング レポート （1835 ページ）
- クライアント プロビジョニング イベント ログ （1836 ページ）
- クライアント プロビジョニング ポータルのポータル設定 （1836 ページ）
- クライアントプロビジョニングポータルの言語ファイルのHTMLサポート （1840ページ）

ポスチャ タイプ

次のポスチャエージェントは、Cisco ISE ポスチャポリシーをモニターおよび適用します。

- **[エージェント（Agent）]**：エージェントを展開し、クライアントによるデータのやり取りが必要な Cisco ISE ポスチャポリシーを監視し、適用します。エージェントはクライアントに残ります。Cisco ISE でのエージェントの使用に関する詳細については、「Cisco Secure クライアント （1822 ページ）」を参照してください。

- **[エージェントステルス（Agent Stealth）]**：ユーザーインターフェイスなしで、サービスとしてポスチャを実行します。エージェントはクライアント上に残ります。

  ポスチャ要件でエージェントステルスポスチャタイプを選択すると、一部の条件、修復、または条件内の属性が無効になります（灰色表示）。たとえば、手動修復ではクライアント側のやりとりが必要となるため、エージェントステルス要件を有効にすると、[手動修復タイプ（Manual Remediation Type）] が無効になります（灰色表示）。

  エージェントステルスモードの展開で、ポスチャプロファイルをエージェント設定にマッピングし、エージェント設定を [クライアント プロビジョニング（Client Provisioning）] ウィンドウにマッピングする場合、次の処理がサポートされます。

- エージェントはポスチャプロファイルを読み取り、必要なモードを設定することができます。
- エージェントは初回ポスチャ要求時に選択したモードに関する情報を Cisco ISE へ送信できます。
- Cisco ISE は、モードおよびその他の要因（ID グループ、OS、コンプライアンスモジュールなど）に基づいて正しいポリシーを照合します。

（注） エージェントステルスモードを使用するには、AnyConnect バージョン 4.4 以降が必要です。

Cisco ISE でのエージェントステルスの設定の詳細については、エージェントステルスモードのワークフローの設定 （1781 ページ）を参照してください。

- [一時エージェント（Temporal Agent）]：クライアントが信頼できるネットワークにアクセスしようとすると、Cisco ISE は [クライアント プロビジョニング（Client Provisioning）] ポータルを開きます。ポータルから、エージェントをダウンロードしてインストールし、エージェントを実行するようにユーザーに指示が出されます。一時エージェントはコンプライアンスステータスを確認し、そのステータスを Cisco ISE に送信します。Cisco ISE は結果に基づいて動作します。コンプライアンス処理が完了すると、クライアントから一時エージェント自体が削除されます。一時エージェントは、カスタム修復をサポートしていません。デフォルトの修復では、メッセージ テキストのみがサポートされます。

  一時エージェントは、次の条件をサポートしていません。

  - サービス条件 MAC：システム デーモン チェック
  - サービス条件 MAC：デーモンまたはユーザー エージェント チェック
  - PM：最新チェック
  - PM：有効化チェック
  - DE：暗号化チェック
  - [ポスチャタイプ（Posture Types）]、[Temporal Agent]、[コンプライアンスモジュール 4.x 以降（Compliance Module 4.x or later）] 使用した、ポスチャポリシーの設定。コンプライアンスモジュールを **3.x 以前**または**任意のバージョン**として設定しないでください。
  - 一時エージェントの場合は、[要件（Requirements）] ウィンドウで [インストール（Installation）] チェックタイプを含むパッチ管理条件のみを表示できます。
  - Cisco ISE は、MacOS 向け一時エージェントを使用した VLAN 制御ポスチャをサポートしていません。ネットワークアクセスを既存の VLAN から新しい VLAN に変更すると、VLAN が変更される前にユーザーの IP アドレスが解放されます。ユーザーが新しい VLAN に接続すると、クライアントは DHCP によって新しい IP アドレスを取

得します。新しいIPアドレスを認識するにはルート権限が必要ですが、一時エージェントはユーザープロセスとして実行します。

- Cisco ISE は、エンドポイント IP アドレスの更新を必要としない ACL 制御のポスチャ環境をサポートしています。
- Cisco ISE での Temporal Agent の設定の詳細については、Cisco Temporal Agent のワークフローの設定 （1787 ページ）を参照してください。

- [AMP イネーブラ（AMP Enabler）]：AMP イネーブラによって、社内でローカルにホストされているサーバーからエンドポイントのサブセットに AMP for Endpoints ソフトウェアがプッシュされ、AMP サービスが既存のユーザーベースにインストールされます。
- [エージェントレスポスチャ（Agentless Posture）]：エージェントレスポスチャは、クライアントからのポスチャ情報を提供し、終了時に完全に削除します。エンドユーザーによる操作は不要です。Temporal Agent とは異なり、エージェントレスポスチャは管理者ユーザーとしてクライアントに接続します。Cisco ISE でのエージェントレスポスチャの使用の詳細については、エージェントレス ポスチャ （1690 ページ）を参照してください。

[クライアントプロビジョニング（Client Provisioning）] ウィンドウ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]）と [ポスチャ要件（Posture Requirements）] ウィンドウ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]）でポスチャタイプを選択できます。ベストプラクティスは、[クライアント プロビジョニング（Client Provisioning）] ウィンドウでポスチャプロファイルをプロビジョニングすることです。

関連トピック

エージェントステルスモードのワークフローの設定 （1781 ページ）
Cisco Temporal Agent のワークフローの設定 （1787 ページ）

エージェントレス ポスチャ

エージェントレスポスチャは、クライアントからのポスチャ情報を提供し、完了後、Cisco ISE によって再度呼び出されるまでそれ自体を完全に削除します。エンドユーザーによる操作は不要です。

エージェントレス ポスチャ パッケージは、デフォルトの Cisco ISE クライアント プロビジョニング リソースの一部として使用できます。クライアント プロビジョニング ポリシーに使用するエージェントの設定を作成するときに、このパッケージを選択できます。

前提条件：

- クライアントは IPv4 または IPv6 アドレスを介して到達可能である必要があり、その IP アドレスは RADIUS アカウンティングで使用可能である必要があります。
- Windows クライアントと Mac クライアントが現在サポートされています。

- Windows クライアントの場合、クライアントの PowerShell にアクセスするにはポート 5985 が開いている必要があります。PowerShell はバージョン 7.1 以降である必要があります。クライアントには、cURL v7.34 以降が必要です。
- Mac OS クライアントの場合、クライアントにアクセスするには SSH にアクセスするポート 22 が開いている必要があります。クライアントには、cURL v7.34 以降が必要です。

- シェルログイン用のクライアントログイン情報には、ローカル管理者権限が必要です。
- 設定手順の説明に従って、ポスチャフィードの更新を実行して最新のクライアントを取得します。
- エンドポイントでの証明書のインストールが失敗しないようにするため、次のエントリが sudoers ファイルで更新されていることを確認します。

```
<macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript
```

- Mac OS の場合、設定するユーザーアカウントは管理者のアカウントである必要があります。Mac OS のエージェントレスポスチャは、より多くの権限が付与されているとしても、他のアカウントタイプでは機能しません。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）] > [ログイン設定（Login Configuration）] > [MAC ローカルユーザー（MAC Local User）]**。
- Microsoft からの更新により Windows クライアントのポート関連のアクティビティが変更された場合は、Windows クライアントのエージェントレスポスチャ設定ワークフローを再設定する必要がある場合があります。

サポートされているポスチャ条件

- ファイル条件（USER_DESKTOP および USER_PROFILE ファイルパスを使用する条件を除く）
- サービス条件（MacOS のシステムデーモンとデーモンまたはユーザーエージェントのチェックを除く）
- アプリケーション条件
- 外部データソース条件
- 複合条件
- マルウェア対策条件
- パッチ管理条件（**Enabled** および **Up To Date** 条件チェックを除く）
- ファイアウォール条件
- ディスク暗号化条件（暗号化ロケーションベースの条件チェックを除く）
- レジストリ条件（ルートキーとして HCSK を使用する条件を除く）

（注） エージェントレスポスチャフローの認証にデュアルスタックプロトコルを使用する場合、NADも同じプロトコルを使用する必要があります。

サポートされていないポスチャ条件

- 修復
- 猶予期間
- 定期的再評価
- 利用規定

サポート対象のクライアント オペレーティング システム

- Microsoft Windows のバージョン：10、11
- MacOS のバージョン：10.13、10.14、10.15、13.x、14

エージェントレス ポスチャ プロセス フロー

1. クライアントがネットワークに接続します。
2. Cisco ISEが、クライアントが使用する認証プロファイルでエージェントレスポスチャが有効になっているかどうかを検出します。
3. 有効になっている場合、Cisco ISE がエージェントレス ポスチャ ジョブ要求を Cisco ISE メッセージングキューに送信します。
4. Cisco ISE は、メッセージングキューからジョブを取得し、エージェントレス ポスチャ フローを開始します。
5. Cisco ISE が PowerShell または SSH を介してクライアントに接続します。
6. 証明書がクライアントの信頼できる認証局ストアにない場合、Cisco ISEが証明書をプッシュします。
7. Cisco ISE がクライアント プロビジョニング ポリシーを実行します。
8. Cisco ISEが、エージェントレスプラグインをクライアントにプッシュし、プラグインを起動します。
9. ポスチャ アセスメントがクライアントで実行され、ステータスが Cisco ISE に送信されます。
10. Cisco ISEが、クライアントからエージェントレスプラグインを削除します。ポスチャフローのログは、24 時間、またはクライアントが削除するまで、クライアントに残ります。

エージェントレスポスチャ設定

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）] を選択し、**エージェントレスポスチャを使用して要件を特定する 1 つ以上のポスチャ要件を作成します。

2. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャポリシー（Posture Policy）] を選択し、**そのポスチャ要件にエージェントレスポスチャを使用する 1 つ以上のサポートされているポスチャポリシールールを作成します。使用する予定のルールを複製し、ポスチャタイプを [エージェントレス（Agentless）] に変更できます。

3. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）] を選択し、**エージェントレスポスチャからの結果を評価する認証プロファイルを作成します。

   - 認証プロファイルでエージェントレスポスチャを有効にします。
   - このプロファイルは、エージェントレスポスチャにのみ使用します。他のポスチャタイプには使用しないでください。
   - エージェントレスポスチャには CWA とリダイレクト ACL は必要ありません。VLAN、DACL、または ACL をセグメンテーションルールの一部として使用できます。

4. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）] に移動し、**クライアント プロビジョニング ポリシーを追加します。Cisco Agent の設定の場合は、設定したオペレーティングシステムのエージェントレスプラグインを選択します。Windows の場合、プラグインは CiscoAgentlessWindows 4.9.01095 です。MacOS の場合、プラグインは CiscoAgentlessOSX 4.9.01095 です。このルールが確認するポスチャ条件を選択します。Active Directory を使用している場合は、ポリシーで Active Directory グループを使用できます。

（注） MACOSX 10.14 バージョンと10.15 バージョンのエージェントレスポスチャ設定は、ポスチャフィードを更新するまで使用できません。ポスチャフィードを実行する前に、ポスチャフィードの URL を更新します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアの更新（Software Updates）] > [ポスチャの更新（Posture Updates）]**。[ポスチャの更新（Posture Updates）] ウィンドウで、[フィードの URL の更新（Update Feed URL）] フィールドに URL（https://www.cisco.com/web/secure/spa/posture-update.xml）を入力し、[今すぐ更新（Update Now）] をクリックします。

5. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] を選択し、**[認証ポリシー（Authorization Policy）] を展開します。次の 3 つの認証ポリシーを有効にし、設定します。

- **Unknown_Compliance_Redirect**：結果をエージェントレスポスチャとして Network_Access_Authentication_Passed 条件と Compliance_Unknown_Devices 条件を設定します。
- **NonCompliant_Devices_Redirect**：結果を DenyAccess として Network_Access_Authentication_Passed 条件と Non_Compliant_Devices 条件を設定します。
- **Compliant_Devices_Access**：結果を PermitAccess として Network_Access_Authentication_Passed 条件と Compliant_Devices 条件を設定します。

6. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）] > [エンドポイントログインの設定（Endpoint Login Configuration）]** をクリックし、クライアントにログオンするためのクライアント資格情報を構成します。これらの同じログイン情報がエンドポイントスクリプトで使用されます。
7. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [設定（Settings）] > [エンドポイントスクリプト（Endpoint Scripts）] > [設定（Settings）] を選択し、**[OS 識別の最大再試行回数（Max retry attempts for OS identification）] と [OS 識別の再試行間の遅延（Delay between retries for OS identification）] を設定します。これらの設定によって、接続の問題をどれだけ迅速に確認できるかが決まります。たとえば、PowerShell ポートが開いていないというエラーがログに表示されるのは、再試行がすべては実行されなかった後のみです。
8. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）] を選択し、**エージェントレスポスチャを設定します。
9. クライアントがエージェントレスポスチャに接続すると、ライブログでクライアントを確認できます。

デバッグおよびトラブルシューティング

次のデバッグログレベルを有効にします。

- インフラストラクチャ
- クライアント プロビジョニング
- ポスチャ

デバッグログは *ise-psc.log* にあります

エージェントレスポスチャのトラブルシューティングは、次の場所で使用できます。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [ライブログ（Live Logs）]**：[ポスチャステータス（Posture Status）] 列の下にある3つのドットをクリックすると、エージェントレスポスチャのトラブルシューティングが開きます。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断（Diagnostics）] > [一般ツール（General Tools）]**

エージェントレスポスチャのトラブルシューティング

エージェントレス ポスチャ レポートは、エージェントレスポスチャが想定どおりに動作しない場合に使用する主要なトラブルシューティングツールです。このレポートには、スクリプトアップロードの完了、スクリプトアップロードの失敗、スクリプト実行の完了などのイベントを含む、エージェントレスフローの段階が既知の失敗の理由（ある場合）とともに表示されます。

（注） エージェントレス ポスチャ スクリプトは自身を検証できませんが、スクリプトの実行後に、Cisco ISE から受信したデータを検証します。

エージェントレスポスチャのトラブルシューティングには、次の2つの場所からアクセスできます。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[操作（Operations）] > [ライブログ（Live Logs）] を選択し、トラブルシューティングするクライアントの [ポスチャステータス（Posture Status）] 列にある縦に並んだ 3 つのドットをクリックします。
- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断（Diagnostics）] > [一般ツール（General Tools）] > [エージェントレスポスチャのトラブルシューティング（Agentless Posture Troubleshooting）]**。

エージェントレスポスチャのトラブルシューティング ツールは、指定されたクライアントのエージェントレスポスチャ アクティビティを収集します。[エージェントレス ポスチャ フロー（Agentless Posture Flow）] はポスチャを開始し、現在アクティブなクライアントと Cisco ISE 間のすべてのデータのやり取りを表示します。[クライアントログのみをダウンロード（Only Download Client Logs）] は、クライアントからの最大 24 時間分のポスチャフローを含むログを作成します。クライアントはいつでもログを削除できます。収集が完了したら、ログの ZIP ファイルをエクスポートできます。

レポート

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [操作（Operations）] > [レポート（Reports）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] > [エージェントレスポスチャ（Agentless Posture）] を選択すると、エージェントレスポスチャを実行したすべてのエンドポイントが表示されます。

ポスチャ管理の設定

ポスチャ サービス用の管理者ポータルをグローバルに設定できます。シスコから Web 経由で自動的に Cisco ISE サーバーに更新をダウンロードできます。また、オフラインで、後で、Cisco ISE を手動で更新することもできます。さらに、クライアントに Cisco Secure ClientWeb Agent などのエージェントがインストールされていると、クライアントにポスチャアセスメントおよび修復サービスが提供されます。クライアント エージェントは、Cisco ISE に対してクライアントのコンプライアンス ステータスを定期的に更新します。ログインおよびポスチャの要件アセスメントが正常に完了した後、ネットワーク使用の利用規約への準拠をエンドユーザーに求めるリンクが示されたダイアログがクライアントエージェントに表示されます。このリンクを使用して、エンドユーザーがネットワークへのアクセス権を取得する前に同意する、企業ネットワークのネットワーク使用情報を定義できます。

ポスチャワークフローでの未検証のオペレーティングシステムリリースのサポートの強化

Cisco ISE リリース 3.3 以降、Cisco ISE は、エージェントベースおよびエージェントレスのポスチャワークフローで、オペレーティングシステムの未検証バージョンをサポートしています。Cisco ISE の以前のリリースでは、検証済みのオペレーティングシステムを実行するエンドポイントのみがポスチャ エージェント ポリシーを正常に満たしていました。

その結果、未検証のオペレーティングシステムを実行しているエンドポイントは、「**The operating system is not supported by the server**」というエラー メッセージが表示され、ポスチャ エージェント ワークフローに失敗します。

サポートされるオペレーティングシステムの詳細については、お使いの Cisco ISE リリースの「Compatibility Matrix」を参照してください。

たとえば、オペレーティング システム バージョン Windows 10 IoT Enterprise LTSC または Mac 14 を実行しているエンドポイントのポスチャエージェントフローは、これらのオペレーティングシステムのバージョンが検証されていない間は失敗しました。Cisco ISE がこれらのバージョンを検証し、オペレーティングシステムのデータがフィードサービスにパブリッシュされると、ポスチャエージェントはこれらのエンドポイントを正常に照合しました。

Cisco ISE 管理ポータルの**[管理（Administration）]** > **[システム（System）]** > **[ポスチャ（Posture）]** > **[更新（Updates）]**ページの [フィードサービス（Feed Service）] から Cisco ISE に最新のオペレーティングシステムのデータをダウンロードできます。

Cisco ISE リリース 3.3 から、未検証のオペレーティングシステムは、Cisco ISE 管理ポータルの [ポリシー（Policy）] ページ（[ポスチャ（Posture）]、[要件（Requirements）]、[条件（Conditions）]ページ）にリストされている既知のオペレーティングシステムと照合されるため、ポスチャ エージェント ワークフローを正常に完了できます。たとえば、Mac xx が検証されず、エンドポイントがそれを実行している場合、ポスチャエージェントはエンドポイントを MacOSX と照合できるようになりました。Mac xx が検証され、フィードサービスに公開され、ポスチャエージェントがエンドポイントで再度実行されると、エンドポイントは Mac xx と照

合されます。ポスチャレポートには、エンドポイントが一致するオペレーティングシステムが表示されます。

Cisco ISE リリース 3.3 でサポートされているすべてのポスチャエージェントが、この変更の影響を受けます。BYOD などの他の Cisco ISE 機能は影響を受けません。

クライアントのポスチャ要件

ポスチャの要件を作成するには、次の手順を実行します。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）] を選択します。
2. 要件行の末尾にある [編集（Edit）] ドロップダウンリストから、[新しい要件の挿入（Insert New Requirement）] を選択します。
3. 必要な詳細を入力し、[完了（Done）] をクリックします。

次の表に、[クライアントのポスチャ要件（Client Posture Requirements）] ウィンドウのフィールドを示します。

表 *152* : ポスチャ要件

フィールド名	使用上のガイドライン
名前	要件の名前を入力します。
オペレーティングシステム	オペレーティング システムを選択します。 プラス記号 [+] をクリックして、複数のオペレーティング システムをポリシーに関連付けます。 マイナス記号 [-] をクリックして、ポリシーからオペレーティング システムを削除します。
コンプライアンスモジュール	[準拠モジュール（Compliance Module）] ドロップダウンリストから必要な準拠モジュールを選択します。 • [4.x 以降（4.x or Later）]：マルウェア対策、ディスク暗号化、Patch Management、および USB の各種条件をサポートします。 • [3.x 以前（3.x or Earlier）]：ウイルス対策、スパイウェア対策、ディスク暗号化、および Patch Management の各種条件をサポートします。 • [すべてのバージョン（Any Version）]：ファイル、サービス、レジストリ、アプリケーション、および複合の各種条件をサポートします。 コンプライアンスモジュールの詳細については、コンプライアンスモジュール （1717 ページ）を参照してください。

フィールド名	使用上のガイドライン
ポスチャタイプ	[ポスチャタイプ（Posture Type）] ドロップダウンリストから、必要なポスチャタイプを選択します。 • [エージェント（Agent）]： エージェントを展開し、クライアントとのやり取りが必要な Cisco ISE ポリシーを監視し、適用します。 • [エージェントステルス（AnyConnect Agent Stealth）]：エージェントを展開し、クライアントとやり取りしない Cisco ISE ポスチャポリシーを監視し、適用します。 • [一時エージェント（Temporal Agent）]：準拠のステータスを確認するためにクライアント上で実行される一時実行ファイル。
条件	リストから条件を選択します。 [操作（Action）] アイコンをクリックして、ユーザー定義の条件を作成して、要件に関連付けることもできます。ユーザー定義の条件を作成中に関連する親オペレーティング システムは編集できません。 pr_WSUSRule は、Windows Server Update Services（WSUS）修復が関連付けられているポスチャ要件で使用される、ダミーの複合条件です。関連 WSUS 修復アクションは、シビラティ（重大度）レベル オプションを使用して Windows Updates を検証するように設定する必要があります。この要件が欠けていると、Windows クライアントのエージェントは、WSUS 修復で定義した重大度レベルに基づいて WSUS 修復アクションを適用します。 pr_WSUSRule は複合条件のリスト ページには表示できません。条件ウィジェットからのみ pr_WSUSRule を選択できます。
修復アクション	リストから修復を選択します。 修復アクションを作成して、要件に関連付けることもできます。 エージェントユーザーとの通信に使用できるすべての修復タイプ用のテキストボックスがあります。修復アクションに加えて、クライアントの非準拠に関してメッセージでエージェントユーザーと通信することができます。 [メッセージテキストのみ（Message Text Only）] オプションで、エージェントユーザーに非準拠について通知します。また、詳細情報を得るためにヘルプ デスクに連絡したり、クライアントを手動で修復したりするオプションの手順がユーザーに提供されています。このシナリオでは、エージェントは修復アクションをトリガーしません。

関連トピック

ポスチャ評価の利用規定の設定 （1711 ページ）
クライアントのポスチャ要件の作成 （1775 ページ）

クライアントのタイマー設定

ユーザーが修復するためのタイマー、あるステータスから別のステータスに移行するためのタイマー、およびログイン成功画面を制御するためのタイマーをセットアップできます。

エージェントプロファイルを設定して、修復タイマー、ネットワーク遷移遅延タイマー、およびクライアントマシン上でログイン成功画面を制御するために使用するタイマーを設定し、これらの設定がポリシーベースになるようにすることを推奨します。**[エージェントポスチャプロファイル（Agent Posture Profile）]** ウィンドウ（**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアントのプロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** > **[追加（Add）]** > **[エージェントポスチャプロファイル（Agent Posture Profile）]**）のクライアントのプロビジョニングリソースのエージェントに対してすべてのタイマーを設定できます。

ただし、クライアント プロビジョニング ポリシーに一致するように設定されたエージェントプロファイルがない場合、[全般設定（General Settings）] ウィンドウ（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]**）の設定を使用できます。

指定した時間内で修復するためのクライアントの修復タイマーの設定

指定した時間内にクライアントを修復するためのタイマーを設定できます。最初の評価時にクライアントが設定されたポスチャ ポリシーを満たすことに失敗した場合、エージェントは修復タイマーに設定された時間内にクライアントが修復するのを待ちます。クライアントがこの指定時間内の修復に失敗すると、クライアント エージェントはポスチャ ランタイム サービスにレポートを送信します。その後、クライアントは非準拠ステートに移行されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]**。

ステップ 2 [修復タイマー（Remediation Timer）] フィールドに、分単位で時間の値を入力します。

デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。

ステップ 3 [保存（Save）] をクリックします。

クライアントの遷移のためのネットワーク遷移遅延タイマーの設定

ネットワーク遷移遅延タイマーを使用して、指定した時間内に、クライアントがある状態から別の状態に遷移するためのタイマーを設定できます。これは、許可変更（CoA）が完了するために必要となります。ポスチャの成功時と失敗時にクライアントが新しい VLAN の IP アドレスを取得するための時間がかかる場合は、より長い遅延時間が必要になることがあります。クライアントが正常にポスチャされると、Cisco ISE は、ネットワーク遷移遅延タイマーで指定された時間内に未知から準拠モードへ移行することを許可します。ポスチャに失敗すると、Cisco ISE は、タイマーで指定された時間内にクライアントが未知から非準拠モードへ移行することを許可します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]**。

ステップ 2 [ネットワーク遷移遅延（Network Transition Delay）] フィールドに時間値を秒単位で入力します。

デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。

ステップ 3 [保存（Save）] をクリックします。

ログイン成功ウィンドウを自動的に閉じる設定

ポスチャ評価が正常に完了した後、クライアント エージェントは一時的なネットワーク アクセス画面を表示します。ユーザーはログイン ウィンドウで [OK] ボタンをクリックして、この画面を閉じる必要があります。指定した時間の経過後にこのログイン画面を自動的に閉じるタイマーを設定できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]**。

ステップ 2 [経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）] チェックボックスをオンにします。

ステップ 3 [経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）] チェックボックスの横のフィールドに時間値を秒単位で入力します。

有効な値の範囲は 0 ～ 300 秒です。時間をゼロに設定すると、エージェントはログイン成功画面を表示しません。

ステップ 4 [保存（Save）] をクリックします。

非エージェント デバイスへのポスチャ ステータスの設定

非エージェントデバイスで実行されるエンドポイントのポスチャステータスを設定できます。Android デバイスや iPod、iPhone、iPad などの Apple のデバイスが Cisco ISE 対応ネットワークに接続されている場合、これらのデバイスはデフォルトのポスチャステータスの設定を引き継ぎます。

これらの設定は、エンドポイントがクライアント プロビジョニング ポータルにリダイレクトされている間、ポスチャのランタイム中に一致するクライアント プロビジョニング ポリシーが見つからない場合、Windows および MacOS オペレーティングシステムで実行されるエンドポイントにも適用できます。

始める前に

エンドポイントにポリシーを適用するには、対応するクライアントプロビジョニングポリシー（エージェントのインストールパッケージ）を設定する必要があります。そうしないと、エンドポイントのポスチャ ステータスは自動的にデフォルト設定が反映されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]**。

ステップ 2 [デフォルトポスチャステータス（Default Posture Status）] ドロップダウン リストから、オプションに [準拠（Compliant）] または [非準拠（Noncompliant）] を選択します。

ステップ 3 [保存（Save）] をクリックします。

ポスチャのリース

ユーザーがネットワークにログインするたびにポスチャ評価を実行したり、指定した間隔でポスチャ評価を実行したりするよう Cisco ISE を設定できます。有効な範囲は 1 ～ 365 日です。

この設定は、ポスチャアセスメントにエージェントを使用するユーザーだけに適用されます。

ポスチャ リースがアクティブな場合、Cisco ISE は最新の既知のポスチャを使用しますが、コンプライアンスの確認のためにエンドポイントに接続しません。ただし、ポスチャ リースが期限切れになると、Cisco ISE はエンドポイントの再認証またはポスチャ再評価を自動的にトリガーしません。同じセッションが使用されているため、エンドポイントは同じコンプライアンス状態のままになります。エンドポイントが再認証されると、ポスチャが実行され、ポスチャ リース時間がリセットされます。

使用例のシナリオ

- ユーザーはエンドポイントにログオンし、1 日に設定されているポスチャ リースにポスチャ準拠させます。
- ユーザーは4時間後にエンドポイントからログオフします（この時点で、ポスチャ リースは 20 時間残っています）。
- ユーザーは 1 時間後に再度ログオンします。この時点で、ポスチャ リースは 19 時間残っています。最新の既知のポスチャ状態は準拠状態でした。したがって、エンドポイントでポスチャが実行されることなく、ユーザーにアクセス権が付与されます。
- ユーザーは 4 時間後にログオフします（この時点で、ポスチャ リースは 15 時間残っています）。
- ユーザーは 14 時間後にログオンします。ポスチャ リースは 1 時間残っています。最新の既知のポスチャ状態は準拠状態でした。エンドポイントでポスチャが実行されることなく、ユーザーにアクセス権が付与されます。

- 1 時間後、ポスチャ リースは期限切れになります。同じユーザーセッションが使用されているため、ユーザーは引き続きネットワークに接続されています。
- 1 時間後、ユーザーはログオフします（セッションはユーザーに関連付けられていますが、マシンには関連付けられていないため、マシンはネットワーク上に留まることができます）。
- 1 時間後、ユーザーはログオンします。ポスチャ リースが期限切れになり、新しいユーザー セッションが開始されるため、マシンはポスチャ アセスメントを実行し、その結果が Cisco ISE に送信され、ポスチャ リース時間が 1 日にリセットされます（この使用例の場合）。

定期的再評価

定期的再評価（PRA）は、コンプライアンスについてすでに適切にポスチャされているクライアントにのみ実行できます。PRAは、クライアントがネットワーク上で準拠していない場合には実行されません。

PRAは、エンドポイントが準拠ステートになっている場合にのみ有効であり、適用可能です。ポリシー サービス ノードは関連するポリシーを調べ、設定で定義されているクライアント ロールに応じて要件をコンパイルし、PRA を適用します。PRA 設定の一致が見つかった場合、ポリシー サービス ノードは、クライアントのPRA設定で定義されているPRA属性を使用して、クライアント エージェントに応答してから、CoA 要求を発行します。クライアント エージェントは、設定に指定された間隔に基づいて定期的に PRA 要求を送信します。PRA が成功した場合、または、PRA設定に指定されているアクションが続行になっている場合、クライアントは準拠ステートのままになります。クライアントが PRA を満たしていない場合、準拠ステートから非準拠ステートに移行します。

PostureStatus属性は、ポスチャ再評価要求の場合でも、PRA要求で現在のポスチャ ステータスを不明ではなく準拠と示します。PostureStatus はモニタリング レポートでも更新されます。

ポスチャのリースが有効期限内の場合、アクセス コントロール リスト（ACL）に基づいてエンドポイントが準拠し、PRA が開始されます。PRA が失敗すると、エンドポイントが非準拠になり、ポスチャのリースがリセットされます。

（注） PRA は、PSN フェールオーバー中はサポートされません。PSN フェールオーバー後、クライアントで再スキャンを有効にするか、ポスチャリースを有効にする必要があります。

定期的再評価の設定

コンプライアンスに対してすでに正常にポスチャされているクライアントだけの定期的な再評価を設定できます。システムで定義されているユーザー ID グループに各 PRA を設定できます。

始める前に

- 各定期的再評価（PRA）構成に、設定に割り当てられている一意のグループ、またはユーザー ID グループの一意の組み合わせがあることを確認します。
- 2 つの一意のロールである role_test_1 および role_test_2 を PRA 設定に割り当てることができます。論理演算子とこれら 2 つのロールを組み合わせ、2 つのロールの一意の組み合わせとして PRA 設定に割り当てることができます。たとえば、role_test_1 OR role_test_2 とします。
- 2 つの PRA 設定に共通のユーザー ID グループがないことを確認します。
- PRA 構成がユーザー ID グループ *Any* にすでに存在する場合、次のことを実行しないと、他の PRA 設定を作成できません。
  - *Any* 以外のユーザー ID グループを反映するように、任意のユーザー ID グループで既存の PRA 設定を更新します。
  - ユーザー ID グループ「*Any*」の既存の PRA 設定を削除します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 新しい PRA を作成するには、[新規再評価の構成（New Reassessment Configuration）] ウィンドウで値を変更します。

ステップ 4 [送信（Submit）] をクリックして、PRA 設定を作成します。

ポスチャのトラブルシューティングの設定

次の表では、ネットワーク内のポスチャ問題の検出と解決に使用する [ポスチャのトラブルシューティング（Posture troubleshooting）] ウィンドウのフィールドについて説明します。 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ポスチャのトラブルシューティング（Posture Troubleshooting）]**。

表 *153* : ポスチャのトラブルシューティングの設定

フィールド名	使用上のガイドライン
トラブルシューティングが必要なポスチャ イベントの検索と選択	
ユーザー名（Username）	フィルタリング基準として使用するユーザー名を入力します。

フィールド名	使用上のガイドライン
MACアドレス（MAC Address）	フィルタリング基準として使用する MAC アドレスを、xx-xx-xx-xx-xx-xx 形式で入力します。
ポスチャ ステータス（Posture Status）	フィルタリング基準として使用する認証ステータスを選択します。
失敗の理由（Failure Reason）	失敗理由を入力するか、または [選択（Select）] をクリックしてリストから失敗理由を選択します。失敗理由をクリアするには、[クリア（Clear）] をクリックします。
時間範囲（Time Range）	時間範囲を選択します。この時間範囲に作成された RADIUS 認証レコードが使用されます。
開始日時：（Start Date-Time:）	（[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合にのみ使用可能）開始日時を入力するか、またはカレンダ アイコンをクリックして開始日時を選択します。日付は *mm/dd/yyyy* 形式、時刻は *hh:mm* 形式である必要があります。
終了日時：（End Date-Time:）	（[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合にのみ使用可能）終了日時を入力するか、またはカレンダ アイコンをクリックして終了日時を選択します。日付は *mm/dd/yyyy* 形式、時刻は *hh:mm* 形式である必要があります。
レコード数の取得（Fetch Number of Records）	表示するレコードの数を選択します。10、20、50、100、200、または 500 を選択できます。
検索結果	
時刻（Time）	イベントの時刻
ステータス（Status）	ポスチャ ステータス
ユーザー名（Username	イベントに関連付けられたユーザー名
MACアドレス（MAC Address）	システムの MAC アドレス
失敗の理由（Failure Reason）	イベントの障害理由

関連トピック

ポスチャのトラブルシューティング ツール （1789 ページ）

ポスチャの全般設定

次の表では、修復時間およびポスチャ ステータスなどの一般的なポスチャ設定を行うために使用できる [ポスチャの全般設定（Posture General Settings）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]**。

これらの設定はポスチャのデフォルト設定であり、ポスチャプロファイルによって上書きできます。

全般的なポスチャの設定

- [修復タイマー（Remediation Timer）]：修復を開始する前に待機する時間を入力します。デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。
- [ネットワーク遷移遅延（Network Transition Delay）]：時間値を秒単位で入力します。デフォルト値は 3 秒です。有効な範囲は 2 ～ 30 秒です。
- [デフォルト ポスチャ ステータス（Default Posture Status）]：[準拠（Compliant）] または [非準拠（Noncompliant）] を選択します。非エージェントデバイスは、ネットワークに接続している間はこのステータスを想定します。
- [経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）]：このチェックボックスをオンにすると、指定された時間後に、ログイン成功画面が自動的に閉じます。ログイン画面が自動的に閉じるようにタイマーを設定できます。有効な範囲は 0 ～ 300 秒です。時間をゼロに設定した場合は、クライアント上のエージェントはログイン成功画面を表示しません。
- [連続モニタリング間隔（Continuous Monitoring Interval）]：エージェントがモニタリングデータの送信を開始するまでの時間間隔を指定します。アプリケーションおよびハードウェア条件の場合、Cisco ISE 3.2 以降では、デフォルト値は 15 分です。

（注） Cisco ISE のパフォーマンスへの影響を避けるために、ポスチャ対象のネットワーク内の 3,000 エンドポイントごとに、連続モニタリング間隔を 1 分以上に設定することをお勧めします。たとえば、30,000 のエンドポイントがポスチャされている環境では、間隔を 10 分以上に設定します。

- [エージェントレス ポスチャ クライアントのタイムアウト（Agentless posture client timeout）]：ポスチャチェックが失敗したと見なされるまでの待機時間を指定します。

- [毎回の実行後にエージェントレスプラグインを削除する（Remove Agentless Plugin after each run）]：この設定を有効にすると、エージェントレスポスチャの実行後にクライアントからエージェントが削除されます。新しいバージョンが使用可能になるまで、ダウンロードしたプラグインを再利用できるように、これを無効のままにしておくことを強くお勧めします。これを無効のままにすると、ネットワークトラフィックを削減できます。
- [ステルスモードでのアクセプタブル ユース ポリシー（Acceptable Use Policy in Stealth Mode）]：会社のネットワークの利用規約が満たされていない場合、ステルスモードで[ブロック（Block）]を選択して、クライアントを非準拠ポスチャステータスに移行します。

ポスチャのリース

- [ユーザーがネットワークに接続するたびにポスチャアセスメントを行う（Perform posture assessment every time a user connects to the network）]：ユーザーがネットワークに接続するたびにポスチャアセスメントを開始するには、このオプションを選択します。
- [n 日おきにポスチャアセスメントを行う（Perform posture assessment every n days）]：クライアントがすでにポスチャ準拠である場合でも、指定された日数が経過したらポスチャアセスメントを開始するには、このオプションを選択します。
- [最後の既知のポスチャ準拠ステータスをキャッシュする（Cache Last Known Posture Compliant Status）]：ポスチャアセスメントの結果をキャッシュするには、Cisco ISE のこのチェックボックスをオンにします。デフォルトでは、このフィールドは無効です。
- [最後の既知のポスチャ準拠ステータス（Last Known Posture Compliant Status）]：この設定は、[最後の既知のポスチャ準拠ステータスをキャッシュする（Cache Last Known Posture Compliant Status）] をオンにした場合にのみ適用されます。Cisco ISE は、このフィールドに指定された時間、ポスチャアセスメントの結果をキャッシュします。有効な値は、1 ～ 30 日、1 ～ 720 時間、または 1 ～ 43200 分です。

関連トピック

ポスチャ管理の設定 （1696 ページ）
ポスチャのリース （1701 ページ）
指定した時間内で修復するためのクライアントの修復タイマーの設定 （1699 ページ）
クライアントの遷移のためのネットワーク遷移遅延タイマーの設定 （1699 ページ）
ログイン成功ウィンドウを自動的に閉じる設定 （1700 ページ）
非エージェント デバイスへのポスチャ ステータスの設定 （1700 ページ）

Cisco ISE へのポスチャ更新のダウンロード

ポスチャ更新には、Windows および MacOS オペレーティングシステムの両方のウイルス対策とスパイウェア対策の一連の事前定義済みのチェック、ルール、サポート表、およびシスコでサポートされるオペレーティングシステム情報が含まれます。また、ローカル ファイル システムの更新の最新のアーカイブを含むファイルから Cisco ISE をオフラインで更新することもできます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。通常、このプロセスには約 20 分かかります。初回ダウンロード後に、差分更新が自動的にダウンロードされるように Cisco ISE を設定できます。

Cisco ISE では、初回ポスチャ更新時に 1 回のみ、デフォルトのポスチャ ポリシー、要件、および修復を作成します。それらを削除した場合、Cisco ISE は後続の手動またはスケジュールされた更新中にこれらを再作成しません。

始める前に

ポスチャリソースを Cisco ISE にダウンロードできる適切なリモートロケーションにアクセスできるようにするには、「Cisco ISE でのプロキシ設定の指定」の説明に従ってネットワークにプロキシが正しく設定されていることを確認する必要がある場合があります。

[ポスチャ更新（Posture Update）] ウィンドウを使用して、Web から更新を動的にダウンロードできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]**。

ステップ 2 [Web] オプションを選択して、更新を動的にダウンロードします。

ステップ 3 [デフォルトに設定（Set to Default）] をクリックして、[フィードURLの更新（Update Feed URL）] フィールドにシスコのデフォルト値を設定します。

ネットワークで URL リダイレクション機能（プロキシ サーバー経由など）を制限しているために、上記の URL へのアクセスに問題がある場合は、Cisco ISE で関連トピックの代替 URL を指定してください。

ステップ 4 [ポスチャ更新（Posture Updates）] ウィンドウの値を変更します。

ステップ 5 シスコからの更新をダウンロードするには、[今すぐ更新（Update Now）] をクリックします。

更新された後、[ポスチャ更新（Posture Updates）] ウィンドウに、[ポスチャ更新（Posture Updates）] ウィンドウの [更新情報（Update Information）] セクションの更新の確認として現在のシスコ更新のバージョン情報が表示されます。

ステップ 6 [はい（Yes）] をクリックして続行します。

Cisco ISE オフライン更新

このオフライン更新オプションを使用すると、Cisco ISE を使用してデバイスから Cisco.com にインターネット経由で直接アクセスできない場合、またはセキュリティポリシーによって許可されていない場合に、クライアントプロビジョニングおよびポスチャ更新をダウンロードできます。

オフラインのクライアント プロビジョニング リソースをアップロードするには、次の手順を実行します。

ステップ 1 https://software.cisco.com/download/home/283801620/type/283802505/release/3.0.0に進みます。

ステップ 2 ログインクレデンシャルを入力します。

ステップ 3 Cisco Identity Services Engine のダウンロードウィンドウに移動し、リリースを選択します。

次のオフライン インストール パッケージをダウンロードできます。

- **win_spw-**<*version*>**-isebundle.zip**：Windows 向けのオフライン SPW インストールパッケージ
- **mac-spw-**<*version*>**.zip**：Mac OS X 向けのオフライン SPW インストールパッケージ
- **compliancemodule-**<*version*>**-isebundle.zip**：オフライン コンプライアンス モジュール インストール パッケージ
- **macagent-**<*version*>**-isebundle.zip**：オフライン Mac エージェント インストール パッケージ
- **webagent-**<*version*>**-isebundle.zip**：オフライン Web エージェント インストール パッケージ

ステップ 4 [ダウンロード（Download）] または [カートに追加（Add to Cart）] のいずれかをクリックします。

ダウンロードしたインストールパッケージを Cisco ISE に追加する方法については、『Cisco Identity Services EngineAdministrator Guide』の「Add ClientProvisioning Resources from a Local Machine」のセクションを参照してください。

ポスチャ更新を使用して、ローカルシステムのアーカイブから Windows および Mac オペレーティングシステムのチェック、オペレーティングシステム情報、ウイルス対策とスパイウェア対策サポート表を更新できます。

オフライン更新の場合は、アーカイブファイルのバージョンが設定ファイルのバージョンと一致していることを確認します。Cisco ISE を設定した後にオフラインでポスチャ更新を使用し、ポスチャポリシーサービスの動的更新を有効にします。

オフラインのポスチャ更新をダウンロードするには、次のようにします。

ステップ 1 https://www.cisco.com/web/secure/spa/posture-offline.htmlに進みます。

ステップ 2 ローカルシステムに **posture-offline.zip** ファイルを保存します。このファイルを使用すると、Windows および Mac オペレーティングシステムのオペレーティングシステム情報、チェック、ルール、ウイルス対策とスパイウェア対策サポート表が更新されます。

ステップ 3 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[管理（Administration）]>[システム（System）]>[設定（Settings）]>[ポスチャ（Posture）]の順に選択します。

ステップ 4 矢印をクリックすると、ポスチャの設定が表示されます。

ステップ 5 [更新（Updates）] をクリックします。
[ポスチャ更新（Posture Updates）] ウィンドウが表示されます。

ステップ 6 [オフライン（Offline）] オプションをクリックします。

ステップ 7 [参照（Browse）]をクリックし、システムのローカルフォルダからアーカイブファイル（posture-offline.zip）を検索します。

（注） [更新するファイル（File to Update）]フィールドは必須フィールドです。適切なファイルを含むアーカイブファイル（.zip）を 1 つだけ選択できます。.zip、.tar、.gz 以外のアーカイブファイルはサポートされていません。

ステップ 8 [今すぐ更新（Update Now）] をクリックします。

ポスチャ更新の自動ダウンロード

最初の更新後に、更新を確認し、自動的にダウンロードするようにCisco ISE を設定できます。

始める前に

- 最初にポスチャ更新をダウンロードして、更新を確認し、自動的にダウンロードするように Cisco ISE を設定しておく必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]**。

ステップ 2 [ポスチャ更新（Posture Updates）] ウィンドウで [初期遅延から開始される更新の自動確認（Automatically check for updates starting from initial delay）] チェックボックスをオンにします。

ステップ 3 初期遅延時間を hh:mm:ss の形式で入力します。

Cisco ISE は、初期遅延時間の終了後に確認を開始します。

ステップ 4 時間間隔を時間単位で入力します。

Cisco ISE は初期遅延時間から指定した間隔で、展開に更新をダウンロードします。

ステップ 5 [保存（Save）] をクリックします。

ポスチャの利用規定の構成設定

次の表では、ポスチャのアクセプタブルユースポリシーを設定するために使用できるポスチャの [アクセプタブルユースポリシー構成（Acceptable Use Policy Configurations）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]>[システム（System）]>[設定（Settings）] > [ポスチャ（Posture）] > [アクセプタブルユースポリシー（Acceptable Use Policy）]** です。

表 *154 :* ポスチャ *AUP* の設定

フィールド名	使用上のガイドライン
構成名（Configuration Name）	ユーザーが作成する AUP 設定の名前を入力します。
設定の説明（Configuration Description）	ユーザーが作成する AUP 設定の説明を入力します。
エージェントユーザーへの AUP の表示（Windows の場合のみ）	選択した場合、認証およびポスチャアセスメントが成功すると、ネットワークのネットワーク使用の利用規約へのリンクがユーザーに表示されます。
AUP メッセージの URL を使用（Use URL for AUP message）	選択した場合、AUP メッセージの URL を [AUP URL] フィールドに入力する必要があります。
AUP メッセージのファイルを使用（Use file for AUP message）	選択した場合、場所を参照し、ジップ形式のファイルをアップロードします。このファイルには、最上位レベルに index.html を含める必要があります。 .zip ファイルには、index.html ファイルに加えて、他のファイルおよびサブディレクトリを含めることができます。これらのファイルは、HTML タグを使用して相互に参照できます。
AUP URL	ユーザーが認証およびポスチャアセスメントに成功した際にアクセスする AUP の URL を入力します。
AUP ファイル（AUP File）	ファイルを参照し、Cisco ISE サーバーにアップロードします。これは zip 形式のファイルで、最上位レベルに index.html ファイルを含める必要があります。
ユーザー ID グループの選択（Select User Identity Groups）	AUP 構成の一意のユーザー ID グループまたはユーザー ID グループの一意の組み合わせを選択します。 AUP 設定を作成する場合は、次の点に注意してください。 • ポスチャ AUP は、ゲスト フローには適用できません。 • 2 つの設定が共通のユーザー ID グループを持つことはできません。 • ユーザー ID グループ「Any」で AUP 設定を作成する場合は、まず他のすべての AUP 設定を削除します。 • ユーザー ID グループ「Any」を使用して AUP 構成を作成した場合、一意のユーザー ID グループ、または複数のユーザー ID グループを使用して他の AUP 構成を作成することはできません。Any 以外のユーザー ID グループを使用して AUP 構成を作成するには、最初にユーザー ID グループ「Any」を使用した既存の AUP 構成を削除するか、ユーザー ID グループ「Any」を使用した既存の AUP 構成を一意のユーザー ID グループまたは複数のユーザーの ID グループを使用して更新します。

フィールド名	使用上のガイドライン
利用規定設定 - 設定リスト（Acceptable use policy configurations—Configurations list）	既存の AUP 設定と AUP 設定に関連付けられたエンドユーザー ID グループを一覧表示します。

関連トピック

ポスチャ評価の利用規定の設定 （1711 ページ）

ポスチャ評価の利用規定の設定

ログインし、クライアントのポスチャ評価が成功すると、クライアントエージェントにより一時的なネットワーク アクセス画面が表示されます。この画面には、利用規定（AUP）へのリンクが含まれています。ユーザーがリンクをクリックすると、ネットワーク使用の利用規約を表示するページにリダイレクトされます。その条件を読み、同意する必要があります。

各利用規定設定には、一意のユーザー ID グループ、またはユーザー ID グループの一意の組み合わせが必要です。Cisco ISE は最初に一致したユーザー ID グループの AUP を見つけ、AUP を表示するクライアント エージェントと通信します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [アクセプタブル ユース ポリシー（Acceptable Use Policy）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [アクセプタブルユースポリシー構成（New Acceptable Use Policy Configuration）] ウィンドウで値を変更します。

ステップ 4 [送信（Submit）] をクリックします。

ポスチャ条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの 1 つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。このプロセスは、初期ポスチャ更新と呼ばれます。

初期ポスチャ更新の後、Cisco ISE はシスコ定義の単純および複合条件も作成します。シスコ定義の単純条件はプレフィクスとして pc_ が付けられ、複合条件はプレフィクスとして pr_ が付けられています。

ダイナミック ポスチャ更新の結果としてシスコ定義の条件を Web を介してダウンロードするように Cisco ISE を設定することもできます。シスコ定義のポスチャ条件を削除または編集することはできません。

ユーザー定義の条件やシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

単純ポスチャ条件

[ポスチャナビゲーション（Posture Navigation）] ペインを使用して、次の単純条件を管理できます。

- ファイル条件：ファイルの存在、ファイルの日付、およびクライアントのファイルバージョンを確認する条件。
- レジストリ条件：レジストリキーの存在またはクライアント上のレジストリ キーの値を確認する条件。
- アプリケーション条件：アプリケーションまたはプロセスがクライアント上で実行されているかどうかを確認する条件。

（注） プロセスがインストールされ実行されている場合、ユーザーは準拠します。ただし、アプリケーション条件が逆ロジックで動作している場合は、アプリケーションがインストールされておらず実行されていなくも、エンドユーザーは準拠します。アプリケーションがインストールされ実行されている場合、エンドユーザーは準拠しません。

- サービス条件：サービスがクライアント上で実行されているかどうかを確認する条件。
- ディクショナリ条件：ディクショナリ属性と値を確認する条件。
- USB 条件：USB マスストレージデバイスの有無をチェックする条件。

単純ポスチャ条件の作成

ポスチャ ポリシーまたは他の複合条件で使用できる、ファイル、レジストリ、アプリケーション、サービス、およびディクショナリ単純条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]**。

ステップ 2 [ファイル（File）]、[レジストリ（Registry）]、[アプリケーション（Application）]、[サービス（Service）]、または [ディクショナリ単純条件（Dictionary Simple Condition）] のいずれかを選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 フィールドに適切な値を入力します。

ステップ 5 [送信（Submit）] をクリックします。

複合ポスチャ条件

複合条件は、1 つ以上の単純条件、または複合条件で構成されます。ポスチャ ポリシーを定義する場合、次の複合条件を使用できます。

- 複合条件：1 つ以上の単純条件、またはタイプがファイル、レジストリ、アプリケーション、またはサービス条件の複合条件が含まれます。
- ウイルス対策複合条件：1 つ以上の AV 条件、または AV 複合条件が含まれます。
- スパイウェア対策複合条件：1 つ以上の AS 条件、または AS 複合条件が含まれます。
- ディクショナリ複合条件：1 つ以上のディクショナリ単純条件またはディクショナリ複合条件が含まれます。
- マルウェア対策条件：1 つ以上の AM 条件が含まれます。

複合ポスチャ条件の作成

ポスチャ評価と検証のポスチャ ポリシーで使用できる複合条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[複合条件（Compound Conditions）]** > **[追加（Add）]**。

ステップ 2 フィールドに適切な値を入力します。

ステップ 3 条件を検証するために [式の確認（Validate Expression）] をクリックします。

ステップ 4 [送信（Submit）] をクリックします。

ディクショナリ複合条件の設定

表 *155 :* ディクショナリ複合条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するディクショナリ複合条件の名前を入力します。
説明（**Description**）	作成するディクショナリ複合条件の説明を入力します。
既存の条件をライブラリから選択（**Select Existing Condition from Library**）	ポリシー要素ライブラリから事前定義済みの条件を選択して式を定義するか、または後のステップでアドホック属性/値のペアを式に追加します。
条件名（**Condition Name**）	ポリシー要素ライブラリからすでに作成しているディクショナリ単純条件を選択します。
式（**Expression**）	[条件名（Condition Name）] ドロップダウン リストでの選択に基づいて式が更新されます。
AND または OR 演算子（**AND or OR operator**）	ライブラリから追加できるディクショナリ単純条件を論理的に組み合わせるには、AND または OR 演算子を選択します。 次の操作を行うには、[操作（Action）] アイコンをクリックします。 • 属性/値の追加（Add Attribute/Value） • ライブラリから条件を追加（Add Condition from Library） • 削除（Delete） Cisco ISE は、複合条件の各 OR 条件を順番に処理します。たとえば、複合条件が A OR B をチェックする場合、Cisco ISE は最初に A をチェックし、次に B をチェックします。条件 A または B のいずれかが合格すると、全体の結果は合格とマークされます。 条件 A が失敗し、条件 B が成功した場合、全体の結果は合格とマークされます。この場合、ポスチャレポートでは、条件 A は不合格とマークされ、条件 B は合格とマークされます。 条件 A が成功した場合、Cisco ISE は条件 B をスキップし、全体の結果を合格とマークします。ポスチャレポートでは、条件 A は合格とマークされ、条件 B はスキップされたとマークされ、全体の結果は合格とマークされます。

フィールド名	使用上のガイドライン
新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）	さまざまなシステムディクショナリまたはユーザー定義ディクショナリから属性を選択します。 後のステップで事前定義された条件をポリシー要素ライブラリから追加することもできます。
条件名（Condition Name）	すでに作成したディクショナリ単純条件を選択します。
式（Expression）	[式（Expression）] ドロップダウン リストから、ディクショナリ単純条件を作成できます。
演算子（Operator）	属性に値を関連付ける演算子を選択します。
値（Value）	ディクショナリ属性に関連付ける値を入力するか、またはドロップダウンリストから値を選択します。

関連トピック

複合ポスチャ条件 （1713 ページ）
複合ポスチャ条件の作成 （1713 ページ）

Windowsクライアントでの自動アップデートを有効にするための事前定義の条件

pr_AutoUpdateCheck_Ruleはシスコによって事前定義された条件であり、[複合条件（Compound Conditions）] ウィンドウにダウンロードされます。この条件を使用すると、Windowsクライアント上で自動アップデート機能が有効になっているかどうかを確認することができます。Windows クライアントがこの要件を満たさない場合、ネットワーク アクセス コントロール（NAC）エージェントによって、Windowsクライアントの自動アップデート機能が強制的に有効になります（修復）。この修復後、Windowsクライアントはポスチャ準拠になります。自動アップデート機能がWindowsクライアント上で有効になっていない場合は、ポスチャ ポリシーで関連付けた Windows Update 修復で Windows 管理者設定を上書きします。

事前設定済みアンチウイルスおよびアンチスパイウェア条件

Cisco ISE の [AV複合条件（AV Compound Condition）] および [AS複合条件（AS Compound Conditions）] ウィンドウには、ウイルス対策とスパイウェア対策の事前設定済みの複合条件がロードされます。これらの条件は、Windows および MacOS オペレーティングシステムのアンチウイルスおよびアンチスパイウェアサポート表で定義されます。これらの複合条件では、指定されたアンチウイルスとアンチスパイウェア製品がすべてのクライアント上に存在するかど

うかを確認できます。Cisco ISE で新しいアンチウイルスとアンチスパイウェアの複合条件を作成することもできます。

アンチウイルスとアンチスパイウェア サポート表

Cisco ISE は、各ベンダー製品の最新バージョンおよび定義ファイルの日付を提供するアンチウイルスとアンチスパイウェア サポート表を使用します。ユーザーは頻繁にアンチウイルスとアンチスパイウェア サポート表をポーリングする必要があります。アンチウイルスとアンチスパイウェアのベンダーはアンチウイルスとアンチスパイウェア定義ファイルを頻繁に更新するため、各ベンダー製品の最新バージョンおよび定義ファイルの日付を検索します。

新しいアンチウイルスとアンチスパイウェアのベンダー、製品、リリースのサポートを反映するようにアンチウイルスとアンチスパイウェアサポート表が更新されるたびに、エージェントは新しいアンチウイルスおよびアンチスパイウェア ライブラリを受け取ります。これは、エージェントがより新しい追加機能をサポートするのに役立ちます。エージェントがこのサポート情報を取得すると、定期的に更新される se-checks.xml ファイル（se-templates.tar.gz アーカイブで se-rules.xml ファイルとともに公開される）で最新の定義情報をチェックし、クライアントがポスチャポリシーに準拠しているかどうかを確認します。特定のアンチウイルスまたはアンチスパイウェア製品のアンチウイルスおよびアンチスパイウェア ライブラリによってサポートされている機能に応じて、適切な要件がエージェントに送信され、ポスチャ検証中にクライアント上でそれらの存在、および特定のアンチウイルスおよびアンチスパイウェア製品のステータスが検証されます。

ISE ポスチャエージェントでサポートされているウイルス対策およびマルウェア対策製品の詳細については、『Cisco ISE Compatibility Guide』の Cisco ISE ポスチャのサポート表を参照してください。

マルウェア対策のポスチャ条件を作成する際に、コンプライアンスモジュールの最小バージョンを確認できます。ポスチャフィードが更新されたら、[ワークセンター（Work Centers）]>[ポスチャ（Posture）]>[ポリシー要素（Policy Elements）]>[マルウェア対策条件（Anti-Malware Condition）] を選択し、[オペレーティングシステム（Operating System）] と [ベンダー（Vendor）] を選択してサポート表を表示します。

（注） マルウェア対策のエンドポイントセキュリティ ソリューション（FireEye、Cisco AMP、Sophos など）の一部には、それぞれの集中型サービスへネットワークを通じてアクセスしないと機能しないものがあります。このような製品の場合、ISE の章（または OESIS ライブラリ）は、エンドポイントがインターネットに接続されていることを想定しています。このようなエンドポイントについては、これらのオンラインエージェントのための事前ポスチャ（オフライン検出が有効になっていない場合）時にインターネットアクセスを許可することを推奨します。このような場合には、署名定義の条件が適用されないことがあります。

コンプライアンス モジュール

コンプライアンス モジュールには、ベンダー名、製品バージョン、製品名、および Cisco ISE のポスチャ条件をサポートする OPSWAT が提供する属性などのフィールドのリストが含まれています。

コンプライアンス モジュールは、Cisco.com で入手可能です。

次の表に、ISE ポスチャ ポリシーをサポートするまたはしない OPSWAT API バージョンを示します。バージョン 3 および 4 をサポートするエージェントごとに異なるポリシー ルールがあります。

表 *156 : OPSWAT API* バージョン

ポスチャ条件	コンプライアンス モジュールのバージョン
OPSWAT	
アンチウイルス	3.x 以前
スパイウェア対策	3.x 以前
マルウェア対策	4.x 以降
ディスク暗号化	3.x 以前および 4.x 以降
パッチ管理	3.x 以前および 4.x 以降
USB	4.x 以降
非 OPSWAT	
ファイル	すべてのバージョン
アプリケーション	すべてのバージョン
複合	すべてのバージョン
レジストリ	すべてのバージョン
サービス	すべてのバージョン

（注）

- 上記のバージョンのいずれかがインストールされた可能性のあるクライアントを予測して、バージョン 3.x 以前およびバージョン 4.x 以降用に別個のポスチャ ポリシーを作成する必要があります。
- OESIS バージョン 4 のサポートはコンプライアンス モジュール 4.x および Cisco AnyConnect 4.3 以降に提供されます。しかし、AnyConnect 4.3 は OESIS バージョン 3 とバージョン 4 のポリシーの両方をサポートします。
- バージョン 4 コンプライアンス モジュールは、ISE 2.1 以降でサポートされています。

ポスチャ コンプライアンスのチェック

ステップ 1 Cisco ISE にログインし、ダッシュボードにアクセスします。

ステップ 2 [ポスチャ コンプライアンス（Posture Compliance）] ダッシュレットで、カーソルを積み上げ棒またはスパークラインに合わせます。

ツール チップに詳細情報が示されます。

ステップ 3 データ カテゴリを展開すると、詳細を参照できます。

ステップ 4 [ポスチャ コンプライアンス（Posture Compliance）] ダッシュレットを大きくします。

詳細なリアルタイムレポートが表示されます。

（注） [コンテキストの可視性（Context Visibility ）] ウィンドウにポスチャ コンプライアンス レポートを表示できます。[コンテキストの可視性（Context Visibility）]>[エンドポイント（Endpoints）] > [コンプライアンス（Compliance）] に移動します。このウィンドウには、コンプライアンス ステータス、場所、エンドポイント、およびカテゴリ別のアプリケーションに基づいてさまざまなチャートが表示されます。

アクティブなセッションがないエンドポイントのポスチャ ステータスが表示される場合があります。たとえば、エンドポイントの最新の既知のポスチャ ステータスが準拠の場合、エンドポイントセッションが終了していても、エンドポイントで次の更新を受信するまで、[コンテキストの可視性（Context Visibility）] ウィンドウのステータスは準拠のままになります。ポスチャ ステータスは、このエンドポイントが削除または消去されるまで、[コンテキストの可視性（Context Visibility）] ウィンドウで保持されます。

パッチ管理条件の作成

選択したベンダーのパッチ管理製品のステータスを確認するポリシーを作成できます。

たとえば、Microsoft System Center Configuration Manager（SCCM）、クライアント バージョン 4.x ソフトウェア製品がエンドポイントにインストールされているかどうかを確認する条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[パッチ管理条件（Patch Management Condition）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）] フィールドに条件名を入力し、[説明（Description）] フィールドにその説明を入力します。

ステップ 4 [オペレーティングシステム（Operating System）] ドロップダウン フィールドから、適切なオペレーティング システムを選択します。

ステップ 5 ドロップダウン リストから [コンプライアンスモジュール（Compliance Module）] を選択します。

ステップ 6 ドロップダウン リストから [ベンダー名（Vendor Name）] を選択します。

ステップ 7 [チェックタイプ（Check Type）] を選択します。

ステップ 8 [インストール済みパッチの確認（Check Patches Installed）] ドロップダウン リストから適切なパッチを選択します。

ステップ 9 [送信（Submit）] をクリックします。

関連トピック

パッチ管理条件の設定 （1746 ページ）
パッチ管理修復の追加 （1772 ページ）

ディスク暗号化条件の作成

エンドポイントが指定されたデータ暗号化ソフトウェアに準拠しているかどうかを確認するポリシーを作成できます。

たとえば、C: ドライブがエンド ポイントで暗号化されているかどうかを確認する条件を作成できます。C: ドライブが暗号化されていない場合、エンド ポイントはコンプライアンス違反通知を受信し、ISE はメッセージをログに記録します。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。ISE ポスチャエージェントを使用している場合にのみ、ポスチャ要件とディスク暗号化条件を関連付けることができます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Condition）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ディスク暗号化条件（Disk Encryption Condition）] ウィンドウで、フィールドに適切な値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

ポスチャ条件の設定

ここでは、ポスチャに使用される単純条件および複合条件について説明します。

ファイル条件の設定

次の表では、[ファイル条件（File Conditions）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ファイル条件（File Conditions）]** です。

表 *157 :* ファイル条件の設定

フィールド名	Windows OS での使用ガイドライン	MacOS での使用ガイドライン	Linux OS での使用ガイドライン
名前（Name）	ファイル条件の名前を入力します。	ファイル条件の名前を入力します。	ファイル条件の名前を入力します。
説明（Description）	ファイル条件の説明を入力します。	ファイル条件の説明を入力します。	ファイル条件の説明を入力します。
オペレーティングシステム（Operating System）	ファイル条件が適用される Windows オペレーティングシステムを選択します。	ファイル条件が適用される MacOS を選択します。	ファイル条件が適用される Linux OS（Ubuntu、Red Hat、または SUSE）を選択します。OS のサポート情報については、お使いの Cisco ISE リリースの「Compatibility Matrix」を参照してください。

フィールド名	**Windows OS** での使用ガイドライン	**MacOS** での使用ガイドライン	**Linux OS** での使用ガイドライン
ファイル タイプ（File Type）	次のいずれかのオプションを選択します。 • FileDate：特定のファイル作成日またはファイル更新日のファイルがシステムに存在するかどうかをチェックします。 • FileExistence：システムにファイルが存在するかどうかをチェックします。 • FileVersion：特定のバージョンのファイルがシステムに存在するかどうかをチェックします。 • CRC32：チェックサム関数を使用してファイルのデータ整合性をチェックします。 • SHA-256：ハッシュ関数を使用してファイルのデータ整合性をチェックします。	次のいずれかのオプションを選択します。 • FileDate：特定のファイル作成日またはファイル更新日のファイルがシステムに存在するかどうかをチェックします。 • FileExistence：システムにファイルが存在するかどうかをチェックします。 • CRC32：チェックサム関数を使用してファイルのデータ整合性をチェックします。 • SHA-256：ハッシュ関数を使用してファイルのデータ整合性をチェックします。 • PropertyList：loginwindow.plist などの plist ファイルのプロパティ値をチェックします。	次のいずれかのオプションを選択します。 • FileDate：特定のファイル作成日またはファイル更新日のファイルがシステムに存在するかどうかをチェックします。 • FileExistence：システムにファイルが存在するかどうかをチェックします。 • CRC32：チェックサム関数を使用してファイルのデータ整合性をチェックします。 • SHA-256：ハッシュ関数を使用してファイルのデータ整合性をチェックします。

フィールド名	**Windows OS** での使用ガイドライン	**MacOS**での使用ガイドライン	**Linux OS** での使用ガイドライン
データ型と演算子（**Data Type and Operator**）	該当なし		該当なし

フィールド名	Windows OS での使用ガイドライン	MacOS での使用ガイドライン	Linux OS での使用ガイドライン
		（ファイルタイプとして [PropertyList] を選択した場合に限り使用可能）plist ファイル内で検索するデータ型またはキーの値を選択します。各データ型には、一連の演算子が含まれています。 • 未指定（Unspecified）：指定したキーの存在をチェックします。 演算子（Exists、DoesNotExist）を入力します。 • 番号（Number）：指定した番号データ型のキーをチェックします。 演算子（equals、does not equal、greater than、less than、greater than または equal to、less than または equal to）と値を入力します。 • 文字列（String）：指定した文字列データ型のキーをチェックします。 演算子（equals、does not equal、equals (ignore case)、starts with、does not start with、contains、does not	

フィールド名	**Windows OS** での使用ガイドライン	**MacOS**での使用ガイドライン	**Linux OS** での使用ガイドライン
		contain、ends with、does not end with）と値を入力します。 • バージョン（Version）：バージョン文字列で指定したキーの値をチェックします。演算子（earlier than、later than、same as）と値を入力します。	
プロパティ名（**Property Name**）	該当なし	（ファイルタイプとして [PropertyList] を選択した場合に限り使用可能）キーの名前（たとえば BuildVersionStampAsNumber）を入力します	該当なし

フィールド名	**Windows OS** での使用ガイドライン	**MacOS**での使用ガイドライン	**Linux OS** での使用ガイドライン
ファイル パス（File Path）		次のいずれかのオプションを選択します。 • ルート（Root）：ルート（/）ディレクトリ内のファイルをチェックします。 ファイルのパスを入力します。 • ホーム（Home）：ホーム（~）ディレクトリ内のファイルをチェックします。 ファイルのパスを入力します。	次のいずれかのオプションを選択します。 • ルート（Root）：ルート（/）ディレクトリ内のファイルをチェックします。 ファイルのパスを入力します。 • ホーム（Home）：ホーム（~）ディレクトリ内のファイルをチェックします。 ファイルのパスを入力します。

フィールド名	Windows OS での使用ガイドライン	MacOSでの使用ガイドライン	Linux OS での使用ガイドライン
	次のいずれかのオプションを選択します。 • ABSOLUTE_PATH：ファイルの完全修飾パスのファイルをチェックします。 例：C:\<directory>\file name。その他の設定では、ファイル名のみを入力します。 • SYSTEM_32：C:\WINDOWS\system32 ディレクトリ内のファイルをチェックします。 ファイル名を入力します。 • SYSTEM_DRIVE：C:\ ドライブ内のファイルをチェックします。ファイル名を入力します。 • SYSTEM_PROGRAMS：C:\Program Files 内のファイルをチェックします。ファイル名を入力します。 • SYSTEM_ROOT：Windows システムのルートパス内のファイルをチェックします。ファイル名を入力します。 • USER_DESKTOP：		

フィールド名	**Windows OS** での使用ガイドライン	**MacOS** での使用ガイドライン	**Linux OS** での使用ガイドライン
	指定したファイルが Windows ユーザーのデスクトップにあるかどうかをチェックします。ファイル名を入力します。 • USER_PROFILE：ファイルが Windows ユーザーのローカル プロファイル ディレクトリにあるかどうかをチェックします。ファイルのパスを入力します。		
ファイル日付タイプ（**File Date Type**）	（ファイルタイプとして [FileDate] を選択した場合に限り使用可能）[作成日（Creation Date）] または [変更日（Modification Date）] を選択します。	（ファイルタイプとして [FileDate] を選択した場合に限り使用可能）[作成日（Creation Date）] または [変更日（Modification Date）] を選択します。	（ファイルタイプとして [FileDate] を選択した場合に限り使用可能）[作成日（Creation Date）] または [変更日（Modification Date）] を選択します。

フィールド名	**Windows OS** での使用ガイドライン	**MacOS**での使用ガイドライン	**Linux OS** での使用ガイドライン
ファイル演算子（**File Operator**）	[File Operator] オプションは、[File Type] で選択した設定に応じて変化します。次の設定を適切に選択します。 **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • [Within]：最後の n 日。有効な範囲は 1 ～ 300 です。 **FileExistence** • **Exists** • **DoesNotExist** **FileVersion** • **EarlierThan** • **LaterThan** • **EqualTo**	[File Operator] オプションは、[File Type] で選択した設定に応じて変化します。次の設定を適切に選択します。 **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • [Within]：最後の n 日。有効な範囲は 1 ～ 300 です。 **FileExistence** • **Exists** • **DoesNotExist**	[File Operator] オプションは、[File Type] で選択した設定に応じて変化します。次の設定を適切に選択します。 **FileDate** • **EarlierThan** • **LaterThan** • **EqualTo** • [Within]：最後の n 日。有効な範囲は 1 ～ 300 です。 **FileExistence** • **Exists** • **DoesNotExist**
ファイルの **CRC** データ（**File CRC Data**）	（[File Type] として [CRC32] を選択した場合のみ使用可能） チェックサムの値（たとえば0x3c37fec3）を入力してファイルの整合性をチェックできます。チェックサム値は 16 進数の整数 0x で始まる必要があります。	（[File Type] として [CRC32] を選択した場合のみ使用可能） チェックサムの値（たとえば0x3c37fec3）を入力してファイルの整合性をチェックできます。チェックサム値は 16 進数の整数 0x で始まる必要があります。	（[File Type] として [CRC32] を選択した場合のみ使用可能） チェックサムの値（たとえば0x3c37fec3）を入力してファイルの整合性をチェックできます。チェックサム値は 16 進数の整数 0x で始まる必要があります。

フィールド名	Windows OS での使用ガイドライン	MacOS での使用ガイドライン	Linux OS での使用ガイドライン
ファイルのSHA-256データ（File SHA-256 Data）	（[File Type] として [SHA-256] を選択した場合のみ使用可能）64 バイトの 16 進数のハッシュ値を入力してファイルの整合性をチェックできます。	（[File Type] として [SHA-256] を選択した場合のみ使用可能）64 バイトの 16 進数のハッシュ値を入力してファイルの整合性をチェックできます。	（[File Type] として [SHA-256] を選択した場合のみ使用可能）64 バイトの 16 進数のハッシュ値を入力してファイルの整合性をチェックできます。
日付および時刻（Date and Time）	（[File Type] として [FileDate] を選択した場合のみ使用可能）クライアントシステムの日付と時刻を、mm/dd/yyyy 形式と hh:mm:ss 形式で入力します。	（[File Type] として [FileDate] を選択した場合のみ使用可能）クライアントシステムの日付と時刻を、mm/dd/yyyy 形式と hh:mm:ss 形式で入力します。	（[File Type] として [FileDate] を選択した場合のみ使用可能）クライアントシステムの日付と時刻を、mm/dd/yyyy 形式と hh:mm:ss 形式で入力します。

関連トピック

単純ポスチャ条件 （1712 ページ）
複合ポスチャ条件 （1713 ページ）
ポスチャ条件の作成 （1784 ページ）

ファイアウォール条件の設定

ファイアウォール条件により、特定のファイアウォール製品がエンドポイントで稼働しているかどうかがチェックされます。サポートされているファイアウォール製品のリストは、OPSWAT サポート チャートに基づいています。初回ポスチャと定期的再評価（PRA）の実行中にポリシーを適用できます。

Cisco ISE は、Windows および MacOS のデフォルトのファイアウォール条件を提示します。これらの条件は、デフォルトで無効になっています。

フィールド名	使用上のガイドライン
名前（Name）	ファイアウォール条件の名前を入力します。
説明（Description）	ファイアウォール条件の説明を入力します。

フィールド名	使用上のガイドライン
コンプライアンス モジュール（**Compliance Module**）	必要なコンプライアンス モジュールを選択します。 • 4.x 以降 • 3.x 以降 • 任意のバージョン
オペレーティング システム（**Operating System**）	必要なファイアウォール製品がエンドポイントにインストールされているかどうかを確認します。Windows OS または MacOS を選択できます。
ベンダー（**Vendor**）	ドロップダウン リストからベンダー名を選択します。ベンダーのファイアウォール製品とそれらのチェック タイプが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。テーブル内のリストは、選択したオペレーティング システムによって変わります。
チェックタイプ（**Check Type**）	[有効（Enabled）]：特定のファイアウォールがエンドポイントで稼働しているかどうかをチェックします。ベンダーの製品が選択したチェック タイプをサポートしているかどうかを [選択したベンダーの製品（Products for Selected Vendor）] リストを参照することで確認します。

レジストリ条件の設定

次の表では、[レジストリ条件（Registry Conditions）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[レジストリ条件（Registry Conditions）]** です。

表 ***158*** : レジストリ条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	レジストリ条件の名前を入力します。
説明（**Description**）	レジストリ条件の説明を入力します。
レジストリ タイプ（**Registry Type**）	レジストリ タイプとして事前定義済み設定の 1 つを選択します。
レジストリ ルート キー（**Registry Root Key**）	レジストリ ルート キーとして事前定義済み設定の 1 つを選択します。

フィールド名	使用上のガイドライン
サブ キー（Sub Key）	レジストリ ルート キーに指定されたパスのレジストリ キーをチェックするには、バックスラッシュ（「\」）なしでサブ キーを入力します。 たとえば、SOFTWARE\Symantec\Norton AntiVirus\version によって、次のパスのキーがチェックされます。 HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
値の名前（Value Name）	（[レジストリ タイプ（Registry Type）] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能）[RegistryValue] をチェックするレジストリ キー値の名前を入力します。 これは [RegistryValueDefault] のデフォルト フィールドです。
値データ型（Value Data Type）	（[レジストリ タイプ（Registry Type）] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能）次の設定の 1 つを選択します。 • [未指定（Unspecified）]：レジストリ キー値があるかどうかをチェックします。このオプションは、[RegistryValue] の場合にのみ使用できます。 • [数字（Number）]：レジストリ キー値の指定された数字をチェックします • [文字列（String）]：レジストリ キー値の文字列をチェックします • [バージョン（Version）]：レジストリ キー値のバージョンをチェックします
値演算子（Value Operator）	設定を適切に選択します。
値データ（Value Data）	（[レジストリ タイプ（Registry Type）] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能）[値データ型（Value Data Type）] で選択したデータ型に応じてレジストリ キーの値を入力します。
オペレーティング システム（Operating System）	レジストリ条件を適用する必要のあるオペレーティング システムを選択します。

関連トピック

単純ポスチャ条件 （1712 ページ）
複合ポスチャ条件 （1713 ページ）

継続的なエンドポイント属性モニタリング

エージェントを使用して、さまざまなエンドポイント属性を継続的にモニターし、エンドポイントの全体的な可視性を向上させることができます。エージェントは、エンドポイントにインストールされ実行されているアプリケーションをモニターします。この機能をオンまたはオフにできます。また、データのモニター頻度を設定できます。デフォルトでは、データは5分間隔で収集され、データベースに保存されます。エージェントは初回ポスチャ時に、実行中のアプリケーションと搭載アプリケーションの一覧を報告します。初回ポスチャの後に、エージェントはX分間隔でアプリケーションをスキャンし、最終スキャンでの差異をサーバーに送信します。サーバーはすべての実行中アプリケーションとインストールされているアプリケーションのリストを表示します。

アプリケーション条件の設定

エンドポイントにインストールされているアプリケーションに対するアプリケーション条件クエリ。これにより、エンドポイントで配信されているソフトウェアの集約された可視性を確認できます。

次の表に、[アプリケーション条件（Application Conditions）] ウィンドウのフィールドを示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [アプリケーション条件（Application Condition）] > [追加（Add）]**。

フィールド名	使用上のガイドライン
名前（Name）	アプリケーションの条件の名前を入力します。
説明（Description）	アプリケーション条件の説明を入力します。
オペレーティングシステム（Operating System）	アプリケーション条件が適用されるオペレーティング システムを選択します。次のオプションを使用できます。 • **Windows** • **Mac OSX** • **Linux**
コンプライアンスモジュール（Compliance Module）	次のいずれかのオプションを選択します。 • **4.x 以降** • **3.x 以前** • **任意のバージョン（Any Version）**

フィールド名	使用上のガイドライン
次を確認（**Check By**）	次のいずれかのオプションを選択します。 • [Process]：エンドポイントでプロセスが実行されているかどうかを確認するには、このオプションをオンにします。 • [Application]：エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションをオンにします。 （注） Linux OS の場合は、[Process] オプションのみが表示されます。
プロセス名（**Process Name**）	（[Check By] オプションで [Process] を選択した場合のみ使用可能）必要なプロセス名を入力します。
アプリケーション演算子（**Application Operator**）	（[Check By] オプションで [Process] を選択した場合のみ使用可能）次のいずれかを選択します。 • [Running]：エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションをオンにします。 • [Not Running]：エンドポイントでアプリケーションが実行されていないかどうかを確認するには、このオプションをオンにします。
アプリケーションの状態（**Application State**）	（[Check By] オプションで [Application] を選択した場合のみ使用可能）次のいずれかのオプションを選択します。 • [Installed]：クライアントに悪質なアプリケーションがインストールされているかどうかを確認するには、このオプションをオンにします。悪意のあるアプリケーションがある場合は、修復アクションがトリガーされます。 • [Running]：エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションをオンにします。

フィールド名	使用上のガイドライン
次をプロビジョニング（**Provision By**）	（[Check By] オプションで [Application] を選択した場合のみ使用可能）次のいずれかのオプションを選択します。 • [すべて（Everything）] : [ブラウザ（Browser）]、[パッチ管理（Patch Management）] など、リストされているすべてのカテゴリを選択できます。 • [名前（Name）] : 1 つ以上のカテゴリを選択します。 たとえば [ブラウザ（Browser）] カテゴリを選択すると、[ベンダー（Vendor）] ドロップダウン リストに対応するベンダーが表示されます。 • [カテゴリ（Category）] : 1 つ以上のカテゴリ（[マルウェア対策（Anti-Malware）]、[バックアップ（Backup）]、[ブラウザ（Browser）]、[データストレージ（Data Storage）] など）をオンにできます。 （注） カテゴリは OPSWAT ライブラリから動的に更新されます。

[コンテキストの可視性（Context Visibility）] > **[エンドポイント（Endpoints）]** > **[コンプライアンス（Compliance）]** ウィンドウで、各エンドポイントでインストールされているアプリケーションと実行中のアプリケーションの数を確認できます。

[ホーム（Home）] > **[概要（Summary）]** > **[コンプライアンス（Compliance）]** ウィンドウに、ポスチャアセスメント対象であり準拠しているエンドポイントのパーセンテージが表示されます。

サービス条件の設定

次の表では、[サービス条件（Service Conditions）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[サービス条件（Service Condition）]**。

表 *159* : サービス条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	サービス条件の名前を入力します。
説明（**Description**）	サービス条件の説明を入力します。

フィールド名	使用上のガイドライン
オペレーティング システム（Operating Systems）	サービス条件を適用する必要のあるオペレーティングシステムを選択します。Windows OS または MacOS のさまざまなバージョンを選択できます。
サービス名（Service Name）	ルートとして動作するデーモンまたはユーザー エージェント サービスの名前を入力します（たとえば com.apple.geod）。エージェントは、コマンド **sudo launchctl list** を使用してサービス条件を確認します。
サービス タイプ（Service Type）	クライアントのコンプライアンスを確実にするためにエージェントが調べる必要があるタイプオブサービスを選択します。 • [デーモン（Daemon）]：マルウェアに対するクライアントデバイスのスキャンなど、指定したサービスがクライアントのデーモンサービスの指定されたリストにあるかどうかをチェックします。 • [ユーザーエージェント（User Agent）]：マルウェアが検出された場合に実行するサービスなど、指定したサービスがクライアントのユーザーサービスの指定されたリストにあるかどうかをチェックします。 • [デーモンまたはユーザーエージェント（Daemon or User Agent）]：指定したサービスがデーモンまたはユーザーエージェントのサービスリストにあるかどうかをチェックします。
サービス オペレータ（Service Operator）	クライアントでチェックするサービス ステータスを選択します。 • [Windows OS]：サービスが [実行している（Running）] か、または [実行していない（Not Running）] かをチェックします。 • [Mac OSX]：サービスが [ロード済み（Loaded）] か、[ロードされていない（Not Loaded）] か、[ロード済みで実行している（Loaded and Running）] か、[終了コード付きでロード済み（Loaded with Exit Code）] か、[ロード済みで実行しているまたは終了コードが付いている（Loaded & running or with Exit code）] かどうかをチェックします。

関連トピック

単純ポスチャ条件 （1712 ページ）
複合ポスチャ条件 （1713 ページ）

ポスチャ複合条件の設定

次の表に、[複合条件（Compound Conditions）] ウィンドウのフィールドを示します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[複合条件（Compound Conditions）]** です。

表 *160* : ポスチャ複合条件の設定

フィールド名	使用上のガイドライン
名前	作成する複合条件の名前を入力します。
説明	作成する複合条件の説明を入力します。
オペレーティングシステム	1 つ以上の Windows オペレーティング システムを選択します。これにより、条件が適用される Windows オペレーティングシステムを関連付けることができます。
カッコ ( )	ファイル、レジストリ、アプリケーション、サービス条件という単純な条件タイプから 2 つの単純条件を組み合わせるには、カッコをクリックします。
（&）：AND 演算子（AND 演算子には「&」を使用します）	複合条件内には AND 演算子（アンパサンド（&））を使用できます。たとえば、**Condition1 & Condition2** と入力します。
（|）：OR 演算子（OR 演算子には「|」を使用します）	複合条件内には OR 演算子（縦線「|」）を使用できます。たとえば、**Condition1 & Condition2** と入力します。
（!）：NOT 演算子（NOT 演算子には「!」を使用します）	複合条件内には NOT 演算子（感嘆符（!））を使用できます。たとえば、**Condition1 & Condition2** と入力します。
単純条件	ファイル、レジストリ、アプリケーション、サービス条件という単純条件のリストから選択します。 また、オブジェクトセレクタからファイル、レジストリ、アプリケーション、サービス条件という単純条件を作成できます。 ファイル、レジストリ、アプリケーション、サービス条件という単純条件を作成するには、[操作（Action）] ボタンのクイック ピッカー（下向き矢印）をクリックします。

関連トピック

ポスチャ条件 （1711 ページ）
複合ポスチャ条件の作成 （1713 ページ）

ウイルス対策条件の設定

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ウイルス対策条件（Anti-Virus Condition）]**。

フィールド名	使用上のガイドライン
名前（Name）	作成するウイルス対策条件の名前を入力します。
説明（Description）	作成するウイルス対策条件の説明を入力します。
オペレーティングシステム（Operating System）	オペレーティングシステムを選択して、クライアント上のウイルス対策プログラムのインストールを確認するか、または条件が適用される最新のウイルス対策定義ファイルの更新を確認します。
ベンダー（Vendor）	ドロップダウン リストからベンダーを選択します。ベンダーを選択すると、アンチウイルス製品およびバージョンが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。
チェックタイプ（Check Type）	クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするかを選択します。
インストール（Installation）	クライアント上のアンチウイルス プログラムのインストールのみをチェックする場合に選択します。
定義（Definition）	クライアント上のアンチウイルス製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。

選択したベンダーの製品（Products for Selected Vendor）

テーブルからアンチウイルス製品を選択します。[新しいアンチウイルス条件（New Anti-virus Compound Condition）] ページで選択したベンダーに基づいて、テーブルは、アンチウイルス製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。

テーブルから製品を選択すると、アンチウイルス プログラムのインストールをチェックしたり、最新のアンチウイルス定義ファイルの日付および最新バージョンをチェックしたりできます。

（注） [ベースライン条件（Baseline Condition）] または [高度な条件（Advance Condition）] のいずれかから、各ウイルス対策製品に対して 1 つの条件のみを設定できます。

ベースライン条件

フィールド名	ガイドライン
最小バージョン	（オペレーティングシステムとベンダーを更新する場合にのみ使用可能）ドロップダウンリストからウイルス対策の最小バージョンを選択します。 このチェックにより、ネットワーク上のすべてのエンドポイントにネットワークポリシーが適用され、ウイルス対策の最小バージョンに準拠します。
最大バージョン	ウイルス対策の最大バージョンは、ポスチャフィードを更新すると自動的に改訂されます。
最小準拠モジュールバージョン	最小準拠モジュールバージョンはエージェントから更新されます。

高度な条件

フィールド名	ガイドライン
最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）（**Check against latest AV definition file version, if available**）	（[定義（Definition）] チェック タイプを選択した場合にのみ使用可能）クライアントのアンチウイルス定義ファイルのバージョンをチェックする場合に選択します。Cisco ISE でのポスチャ更新の結果として、最新のアンチウイルス定義ファイルのバージョンを使用できるときには、そのバージョンに対するチェックが行われます。それ以外の場合、このオプションを使用すると、クライアント上の定義ファイルの日付を、Cisco ISE の最新の定義ファイルの日付に対してチェックできます。

フィールド名	ガイドライン
ウイルス定義ファイルを（有効）にすることを許可する（**Allow virus definition file to be (Enabled)**）	（定義チェック タイプを選択した場合のみ使用可能）アンチウイルス定義ファイルのバージョンと、クライアント上の最新のアンチウイルス定義ファイルの日付をチェックする場合に選択します。最新の定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付から、次のフィールド（[より古い日数（days older than）] フィールド）で定義した日数よりも古いことは許容されません。 オフにした場合、[最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。（Check against latest AV definition file version, if available.）] オプションを使用してアンチウイルス定義ファイルのバージョンのみをチェックすることができます。
より古い日数（**Days Older Than**）	クライアント上の最新のアンチウイルス定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。
最新のファイルの日付（**Latest File Date**）	[より古い日数（days older than）] クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のアンチウイルス定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付よりも古いことは許容されません。
現在のシステム日付（**Current System Date**）	[より古い日数（days older than）] クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のアンチウイルス定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。

関連トピック

複合ポスチャ条件 （1713 ページ）
事前設定済みアンチウイルスおよびアンチスパイウェア条件 （1715 ページ）
アンチウイルスとアンチスパイウェア サポート表 （1716 ページ）

アンチスパイウェア複合条件の設定

次の表に、[AS複合条件（AS Compound Conditions）] ウィンドウのフィールドを示します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [AS 複合条件（AS Compound Condition）]**。

表 *161* : アンチスパイウェア複合条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するアンチスパイウェア複合条件の名前を入力します。
説明（**Description**）	作成するアンチスパイウェア複合条件の説明を入力します。
オペレーティングシステム（**Operating System**）	オペレーティングシステムを選択すると、クライアント上のスパイウェア対策プログラムのインストールをチェックするか、または条件が適用される最新のスパイウェア対策定義ファイルの更新をチェックすることができます。
ベンダー（**Vendor**）	ドロップダウン リストからベンダーを選択します。ベンダーを選択すると、アンチスパイウェア製品およびバージョンが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。
チェック タイプ（**Check Type**）	クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするか、いずれかのタイプを選択します。
インストール（**Installation**）	クライアント上のアンチスパイウェア プログラムのインストールのみをチェックする場合に選択します。
定義（**Definition**）	クライアント上のアンチスパイウェア製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。

フィールド名	使用上のガイドライン
ウイルス定義ファイルを（有効）にすることを許可する（Allow Virus Definition File to be (Enabled)）	このチェックボックスは、アンチスパイウェア定義チェック タイプを作成するときはオンにし、アンチスパイウェア インストール チェック タイプを作成するときはオフにします。 オンにすると、その選択により、クライアント上のアンチスパイウェア定義ファイルのバージョンおよび最新のアンチスパイウェア定義ファイルの日付をチェックできます。最新の定義ファイルの日付が、現在のシステム日付から、[より古い日数（days older than）] フィールドで定義した日数より古いことは許容されません。 オフの場合、その選択により、[ウイルス定義ファイルを（有効）にすることを許可する（Allow virus definition file to be (Enabled)）] チェックボックスがオフのときに、アンチスパイウェア定義ファイルのバージョンのみをチェックすることができます。
より古い日数（Days Older Than）	クライアント上の最新のアンチスパイウェア定義ファイルの日付が、現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。
現在のシステム日付（Current System Date）	[より古い日数（days older than）] クライアント上のアンチスパイウェア定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のアンチスパイウェア定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。
選択したベンダーの製品（Products for Selected Vendor）	テーブルからアンチスパイウェア製品を選択します。[新しいアンチスパイウェア複合条件（New Anti-spyware Compound Condition）] ページで選択したベンダーに基づいて、テーブルは、アンチスパイウェア製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。 テーブルから製品を選択すると、アンチスパイウェア プログラムのインストールをチェックしたり、最新のアンチスパイウェア定義ファイルの日付および最新バージョンをチェックしたりできます。

関連トピック

複合ポスチャ条件 （1713 ページ）
事前設定済みアンチウイルスおよびアンチスパイウェア条件 （1715 ページ）
アンチウイルスとアンチスパイウェア サポート表 （1716 ページ）

マルウェア対策条件の設定

マルウェア対策条件はスパイウェア対策条件とウイルス対策条件の組み合わせで、OESIS バージョン 4.x 以降のコンプライアンス モジュールでサポートされています。

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[マルウェア対策条件（Antimalware Condition）]**。

（注） 最新の定義が適用されるようにインストールしたマルウェア対策製品を手動で1回以上更新することをお勧めします。更新しないと、マルウェア対策定義のエージェントを使用したポスチャチェックが失敗する場合があります。

フィールド名	使用上のガイドライン
名前（Name）	マルウェア対策条件の名前を入力します。
説明（Description）	マルウェア対策条件の説明を入力します。
オペレーティングシステム（Operating System）	オペレーティングシステムを選択して、クライアント上のマルウェア対策プログラムのインストールを確認するか、または条件が適用される最新のマルウェア対策定義ファイルの更新を確認します。。Windows、MacOS、および Linux オペレーティングシステムをサポートしています。
ベンダー（Vendor）	ドロップダウンリストからベンダーを選択します。選択したベンダーのマルウェア対策製品、バージョン、最新の定義日、最新の定義バージョン、最小コンプライアンスモジュールバージョンが [Products for Selected Vendor] テーブルに表示されます。
チェックタイプ（Check Type）	次のいずれかのオプションを選択します。 • [Install]：クライアント上のマルウェア対策プログラムのインストールのみを確認する場合にこのオプションを選択します。 • [Definition]：クライアント上のマルウェア対策製品の、最新の定義ファイルの更新のみを確認する場合にこのオプションを選択します。
最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）（Check Against Latest AV Definition File Version, if Available）	（[Definition] チェックタイプを選択した場合のみ使用可能）クライアント上のマルウェア対策定義ファイルのバージョンを確認する場合に選択します。Cisco ISE でのポスチャ更新の結果として、最新のマルウェア対策定義ファイルのバージョンを使用できるときには、そのバージョンに対するチェックが行われます。それ以外の場合、このオプションを使用すると、クライアント上の定義ファイルの日付を、Cisco ISE の最新の定義ファイルの日付に対してチェックできます。 このチェックは、選択した製品の [Latest Definition Date] または [Latest Definition Version] フィールドの Cisco ISE に値が記載されている場合にのみ機能します。そうでない場合は、[Current System Date] フィールドを使用する必要があります。

フィールド名	使用上のガイドライン
次のウイルス定義ファイルを許可します（Allow Virus Definition File to be）	（[Definition] チェックタイプを選択した場合のみ使用可能）マルウェア対策定義ファイルのバージョンと、クライアント上の最新のマルウェア対策定義ファイルの日付を確認する場合にこのオプションを選択します。最新の定義ファイルの日付を [Days Older Than] フィールドで定義した値よりも前にすることはできません。 オフにした場合、Cisco ISE では [Check against latest AV definition file version] オプションを使用するマルウェア対策定義ファイルのバージョンのみをチェックできます。
より古い日数（Days Older Than）	クライアント上の最新のマルウェア対策定義ファイルの日付を、製品の最新のマルウェア対策定義ファイルの日付または現在のシステム日付よりも前にできる日数を定義します。デフォルト値は 0 です。
最新のファイルの日付（Latest File Date）	クライアント上の最新のマルウェア対策定義ファイルの日付を製品の最新のマルウェア対策定義ファイルの日付よりも前にできる日数を定義するには、このオプションを選択します。 日数をデフォルト値に設定する場合、クライアント上のマルウェア対策定義ファイルの日付を、製品の最新のマルウェア対策定義ファイルの日付よりも前にすることは許容されません。 このチェックは、選択した製品の [Latest Definition Date] フィールドの Cisco ISE に値が記載されている場合にのみ機能します。そうでない場合は、[Current System Date] フィールドを使用する必要があります。
現在のシステム日付（Current System Date）	クライアント上の最新のマルウェア対策定義ファイルの日付が現在のシステム日付よりも前にできる日数を定義するには、このオプションを選択します。 日数をデフォルト値に設定すると、クライアント上のマルウェア対策定義ファイルの日付が現在のシステム日付よりも前にすることはできません。

Mac OS での Carbon Black Cloud 3.x のマルウェア対策条件が成功するには、次の要件を条件的に満たしている必要があります。

- コンプライアンスモジュールは 4.3.2741 よりも大きい必要があります。
- 条件は、ベンダーの VMware, Inc. に関連付けられている必要があります。

ある Cisco ISE リリースから、事前設定された Carbon Black Cloud 3.x 条件付きの別のリリースにアップグレードする場合、ポスチャフィードの更新後、2 つの Carbon Black Cloud 3.x 条件が [マルウェア対策条件（Anti-Malware Condition）] ウィンドウの [詳細条件（Advanced Conditions）] 領域にリストされます。Cisco ISE リリース 3.3 では、以前のリリースからアップグレードした場合にのみ 2 つの条件が表示されます。

ベンダーの Carbon Black, Inc. に関連付けられている Carbon Black Cloud 3.x 条件を削除する必要があります。Carbon Black, Inc.のCarbon Black Cloud 3.x を使用する既存のマルウェア対策条件を再設定して、ベンダー VMware, Inc の条件を使用する必要があります。

関連トピック

複合ポスチャ条件 （1713 ページ）

ディクショナリ単純条件の設定

次の表に、[ディクショナリ単純条件（Dictionary Simple Conditions）] ウィンドウのフィールドを示します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディクショナリ単純条件（Dictionary Simple Conditions）]**。

表 *162 :* ディクショナリ単純条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するディクショナリ単純条件の名前を入力します。
説明（**Description**）	作成するディクショナリ単純条件の説明を入力します。
属性（**Attribute**）	ディクショナリから属性を選択します。
演算子（**Operator**）	選択した属性に値を関連付ける演算子を選択します。
値（**Value**）	ディクショナリ属性に関連付ける値を入力するか、またはドロップダウンリストから事前定義済みの値を選択します。

関連トピック

単純ポスチャ条件 （1712 ページ）
単純ポスチャ条件の作成 （1712 ページ）

ディクショナリ複合条件の設定

表 *163 :* ディクショナリ複合条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するディクショナリ複合条件の名前を入力します。
説明（**Description**）	作成するディクショナリ複合条件の説明を入力します。

フィールド名	使用上のガイドライン
既存の条件をライブラリから選択（Select Existing Condition from Library）	ポリシー要素ライブラリから事前定義済みの条件を選択して式を定義するか、または後のステップでアドホック属性/値のペアを式に追加します。
条件名（Condition Name）	ポリシー要素ライブラリからすでに作成しているディクショナリ単純条件を選択します。
式（Expression）	[条件名（Condition Name）] ドロップダウン リストでの選択に基づいて式が更新されます。
AND または OR 演算子（AND or OR operator）	ライブラリから追加できるディクショナリ単純条件を論理的に組み合わせるには、AND または OR 演算子を選択します。 次の操作を行うには、[操作（Action）] アイコンをクリックします。 • 属性/値の追加（Add Attribute/Value） • ライブラリから条件を追加（Add Condition from Library） • 削除（Delete） Cisco ISE は、複合条件の各 OR 条件を順番に処理します。たとえば、複合条件が A OR B をチェックする場合、Cisco ISE は最初に A をチェックし、次に B をチェックします。条件 A または B のいずれかが合格すると、全体の結果は合格とマークされます。 条件 A が失敗し、条件 B が成功した場合、全体の結果は合格とマークされます。この場合、ポスチャレポートでは、条件 A は不合格とマークされ、条件 B は合格とマークされます。 条件 A が成功した場合、Cisco ISE は条件 B をスキップし、全体の結果を合格とマークします。ポスチャレポートでは、条件 A は合格とマークされ、条件 B はスキップされたとマークされ、全体の結果は合格とマークされます。
新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）	さまざまなシステムディクショナリまたはユーザー定義ディクショナリから属性を選択します。 後のステップで事前定義された条件をポリシー要素ライブラリから追加することもできます。
条件名（Condition Name）	すでに作成したディクショナリ単純条件を選択します。

フィールド名	使用上のガイドライン
式（Expression）	[式（Expression）] ドロップダウン リストから、ディクショナリ単純条件を作成できます。
演算子（Operator）	属性に値を関連付ける演算子を選択します。
値（Value）	ディクショナリ属性に関連付ける値を入力するか、またはドロップダウン リストから値を選択します。

関連トピック

複合ポスチャ条件 （1713 ページ）
複合ポスチャ条件の作成 （1713 ページ）

パッチ管理条件の設定

次の表に、[パッチ管理条件（Patch Management Conditions）] ウィンドウのフィールドを示します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[パッチ管理条件（Patch Management Conditions）]** です。

表 *164* : パッチ管理条件

フィールド名	使用上のガイドライン
名前（Name）	パッチ管理条件の名前を入力します。
説明（Description）	パッチ管理条件の説明を入力します。
オペレーティング システム（Operating System）	オペレーティングシステムを選択して、エンドポイント上のパッチ管理ソフトウェアのインストールを確認するか、または条件が適用される最新のパッチ管理定義ファイルの更新を確認します。Windows、MacOS、または Linux OS を選択できます。また、パッチ管理条件を作成する複数のオペレーティング システムのバージョンを選択することもできます。
ベンダー名（Vendor Name）	[ベンダー名（Vendor Name）] ドロップダウンリストからベンダーを選択します。選択したベンダーとパッチ管理製品およびそれらのサポート対象のバージョンに基づいて、チェックタイプ、最小対応モジュールのサポートの詳細が [選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。テーブル内のリストは、選択したオペレーティングシステムによって変わります。

フィールド名	使用上のガイドライン
チェックタイプ（**Check Type**）	次のいずれかのオプションを選択します。 • [インストール（Installation）]：選択した製品がエンドポイントにインストールされているかどうかを確認します。このチェックタイプは、すべてのベンダーでサポートされています。 （注） Cisco Temporal Agent の場合は、[要件（Requirements）] ウィンドウで [インストール（Installation）] チェックタイプを含むパッチ管理条件のみを表示できます。 • [有効（Enabled）]：選択した製品がエンドポイントで有効かどうかを確認します。 ベンダーの製品が選択したチェック タイプをサポートしているかどうかを [選択したベンダーの製品（Products for Selected Vendor）] リストを参照することで確認します。 • [最新（Up to Date）]：選択した製品に欠けているパッチがないかどうかを確認します。ベンダーの製品が選択したチェックタイプをサポートしているかどうかを [選択したベンダーの製品（Products for Selected Vendor）] リストを参照することで確認します。 [ベンダー名（Vendor Name）] フィールドで指定したベンダーがサポートする製品のリストを表示するには、[選択したベンダー製品（Products for Selected Vendor）] ドロップダウンリストをクリックします。たとえば、製品 1 と 製品 2 の 2 つの製品を持つベンダー A を選択したとします。製品 1 は [有効（Enabled）] オプションをサポートしているが、製品 2 はサポートしていない場合があります。または、製品 1 がチェックタイプのいずれもサポートしていない場合は、グレー表示されます。

フィールド名	使用上のガイドライン
インストール済みパッチの確認（Check Patches Installed）	（[Up To Date] チェックタイプを選択した場合のみ使用可能）欠落しているパッチのシビラティ（重大度）レベルを設定し、シビラティ（重大度）に基づいて展開することができます。次のいずれかのオプションを選択します。 • [Critical Only]：クリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [Important and Critical]：重要かつクリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [Moderate, Important, and Critical]：中程度、重要およびクリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [Low To Critical]：低程度、中程度、重要、およびクリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [All]：すべてのシビラティ（重大度）レベルの欠落しているパッチをインストールします。

関連トピック

パッチ管理条件の作成 （1718 ページ）

ディスク暗号化条件の設定

次の表では、[ディスク暗号化条件（Disk Encryption Condition）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Condition）] です。

表 *165 :* ディスク暗号化条件の設定

フィールド名	使用上のガイドライン
名前（Name）	作成するディスク暗号化条件の名前を入力します。
説明（Description）	ディスク暗号化条件の説明を入力します。
オペレーティングシステム（Operating System）	ディスクを暗号化のためにチェックするエンドポイントのオペレーティング システムを選択します。Windows OS または MacOS を選択できます。また、ディスク暗号化条件を作成するための複数のバージョンのオペレーティング システムを選択することもできます。

フィールド名	使用上のガイドライン
ベンダー名（**Vendor Name**）	ドロップダウンリストからベンダー名を選択します。ベンダーのデータ暗号化製品およびそれらのサポート対象バージョン、暗号化状態チェック、および最小対応モジュール サポートが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されますテーブル内のリストは、選択したオペレーティング システムによって変わります。
ロケーション（**Location**）	オプションが [選択したベンダーの製品（Products for Selected Vendor）] セクションでオンになっている場合にのみ有効です。次のオプションのいずれかを選択します。 • [特定のロケーション（Specific Location）]：指定したディスクドライブがエンドポイントで暗号化されているか（たとえば Windows OS の場合はC:）、または指定したボリュームラベルが暗号化されているか（たとえば、MacOS の場合は Mackintosh HD）を確認します。 • [システムロケーション（System Location）]：デフォルトの Windows OS のシステムドライブまたは MacOS のハードドライブがエンドポイントで暗号化されているかを確認します。 • [すべての内部ドライブ（All Internal Drives）]：内部のドライブを確認します。マウントおよび暗号化されたすべてのハードディスクと、すべての内部パーティションが含まれます。読み取りのみのドライブ、システム リカバリ ディスク/パーティション、ブート パーティション、ネットワーク パーティション、およびエンドポイント外のさまざまな物理ディスク ドライブ（USB およびサンダーボルトを介して接続されたディスク ドライブを含むがこれに限定されない）は除外されます。検証済みの暗号化ソフトウェア製品には次のものがあります。 • Bit-locker-6.x/10.x • Windows 7 上の Checkpoint 80.x
暗号化状態（**Encryption State**）	[暗号化状態（Encryption State）] チェックボックスは、選択した製品が暗号化状態チェックをサポートしていない場合はディセーブルになっています。リピータは、チェックボックスがオンになっている場合のみ表示されます。[完全に暗号化済み（Fully Encrypted）] オプションを選択して、クライアントのディスク ドライブが完全に暗号化されているかどうかを確認できます。 たとえば TrendMicro に対し条件を作成し、2 つのベンダー（一方のベンダーの [暗号化状態（Encryption State）] は「はい（Yes）」でもう一方の [暗号化状態（Encryption State）] は「いいえ（No）」）を選択した場合、ベンダーの暗号化状態の一方が「いいえ（No）」になっているので [暗号化状態（Encryption State）] は無効になります。 （注） リピータをクリックすることで追加のロケーションを追加でき、各ロケーション間の関係は論理 AND 演算子です。

関連トピック

ディスク暗号化条件の作成 （1719 ページ）

USB 条件の設定

次の表では、[USB条件（USB Condition）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [USB]**。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [USB 条件（USB Condition）]**

USB チェックは事前に定義された条件で、Windows OS のみをサポートしています。

表 *166 : USB* 条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	USB_Check
説明（**Description**）	シスコの事前定義チェック
オペレーティングシステム（**Operating System**）	Windows
コンプライアンスモジュール（**Compliance Module**）	バージョン 4.x 以降向けの、ISE のポスチャ準拠モジュールの表示専用フィールドのサポート。

関連トピック

単純ポスチャ条件 （1712 ページ）

ハードウェア属性条件の設定

[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ハードウェア属性条件（Hardware Attributes Condition）]Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ハードウェア属性条件（Hardware Attributes Condition）] ウィンドウにアクセスします。次の表では、[ハードウェア属性条件（Hardware Attributes Condition）] ウィンドウのフィールドについて説明します。

フィールド名	使用上のガイドライン
名前（**Name**）	Hardware_Attributes_Check：条件に割り当てられたデフォルトの名前。

フィールド名	使用上のガイドライン
説明（**Description**）	クライアントからハードウェア属性を収集するシスコの事前に定義されたチェック。
オペレーティングシステム（**Operating System**）	Windows すべてまたは Mac OS
コンプライアンスモジュール（**Compliance Module**）	4.x 以降

ポスチャ外部データソース条件

エンドポイント UDID と外部データソースが一致する条件を設定できます。現在、Active Directory のみがサポートされています。ポスチャ エージェントで必要な、UDID を Active Directory に送信するスクリプトは、ISE に含まれていません。

スクリプト条件の追加

ポスチャ条件スクリプトを作成し、アップロードして、エンドポイントのコンプライアンスステータスを確認できます。ファイルが存在するかどうかを確認する Linux スクリプトの例を次に示します。

```
#!/bin/bash
TESTFILE=/tmp/sample.log
if [ -f $TESTFILE ]
then
    echo "Success: File $TESTFILE exist."
    exit 0
else
    echo "Failed: File $TESTFILE does not exist."
    exit 1
fi
```

次のプラットフォームとスクリプトタイプがサポートされています。

プラットフォーム	サポートされるスクリプトタイプ
Windows	PowerShell スクリプト（.ps1）
macOS	シェルスクリプト（.sh）
Linux	シェルスクリプト（.sh）

始める前に

- エンドポイントでスクリプトを実行するための信頼を確立します。詳細については、スクリプト条件を実行するために信頼を確立 （1753 ページ）を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [スクリプト（Script）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 スクリプトの名前と説明を入力します。

ステップ 4 [オペレーティングシステム（Operating System）] ドロップダウンリストから、必要なオペレーティングシステムを選択します。

[Windows] オペレーティングシステムを選択した場合は、[スクリプトタイプ（Script Type）] と [Windows PowerShell実行ポリシー（Windows PowerShell Execution Policy）] フィールドが表示されます。

[スクリプトタイプ（Script Type）] で、次のオプションのいずれかを選択します。

- **PowerShell**
- **PowerShell Core**

（注） [スクリプトタイプ（Script Type）] は、macOS および Linux オペレーティングシステムの場合、デフォルトで [シェルスクリプト（Shell Script）] に設定されています。

[Windows PowerShell実行ポリシー（Windows PowerShell Execution Policy）] で、次のオプションのいずれかを選択します。

- [バイパス（Bypass）]：エンドポイントで設定済みの他のポリシーでデジタル署名か署名済みの PowerShell スクリプトが必須になっていても、スクリプトを実行するのにデジタル署名は必要ありません。
- [AllSigned]：エンドポイントで設定済みの他のポリシーでデジタル署名が必須になっていない場合でも、スクリプトを実行するにはデジタル署名が必要です。
- [なし（None）]：スクリプトは、エンドポイントの既存のスクリプト実行ポリシーに従って実行されます。Cisco ISE によってスクリプトの実行ポリシーは定義されません。

[AllSigned] オプションを選択して署名済みの Powershell スクリプトを実行する場合は、ルート証明書がエンドポイントの信頼できるルート認証局ストアに配置されていることを確認してください。スクリプトの署名に使用される証明書は信頼できる発行元ストアに配置する必要があり、中間証明書は中間認証局ストアに配置する必要があります。[AllSigned] では、スクリプトが信頼できる発行元によって署名されている必要があります。信頼できるルート認証局ストアにルート証明書があるだけでは十分ではありません。

ステップ 5 [ファイルの選択（Choose File）] をクリックし、ローカルシステムからアップロードするスクリプトを選択します。

ステップ 6 [タイムアウト（Timeout）] フィールドに、スクリプトのタイムアウト期間（秒単位）を入力します。

有効な範囲は 1 ～ 300 秒です。

スクリプトの実行時間が設定されたタイムアウト期間を超えると、エージェントはスクリプトを停止し、[スクリプト条件の実行失敗またはタイムアウト（Script Condition Execution Failure or Timeout）] フィールドで選択されたオプションに基づいて条件をマークします。

ステップ 7 [スクリプト条件の実行失敗またはタイムアウト（Script Condition Execution Failure or Timeout）] で、設定されたタイムアウトの前にスクリプトが終了しない場合、またはスクリプトの実行が失敗した場合に、条件がどうなるかを指定します。

- [合格（Pass）] を選択すると、条件は満たされているとマークされます。
- [失敗（Fail）] を選択すると、条件は満たされていないとマークされます。

ステップ 8 スクリプトを管理者として実行するには、[管理者/ルート（Administrator/Root）] オプションボタンをクリックします。ログインユーザーとしてスクリプトを実行するには、[ログインユーザー（Logged-in User）] オプションボタンをクリックします。

（注） エージェントレス ポスチャ ワークフローは、このスクリプトに関して選択したユーザー権限に関係なく、管理者権限を使用し、一時エージェントはログインユーザー権限を使用します。

ステップ 9 [送信（Submit）] をクリックします。

スクリプト条件を実行するために信頼を確立

エンドポイントでスクリプトを実行し、Cisco ISE サーバーが侵害されていないことを確認するには、信頼を確立する必要があります。Cisco ISE 環境では、1 つ以上の PSN を設定できます。すべての PSN には有効な証明書チェーンがあります。証明書チェーンは任意の証明書で始まり、中間証明書またはルート CA 証明書が続きます。フィンガープリントの検証では、証明書チェーン内のすべての証明書を使用できます。

AnyConnectLocalPolicy のプロファイルエディタの証明書チェーン内に任意の証明書の SHA-256 フィンガープリントを設定できます。たとえば、次のコマンドは、input.cer という名前の証明書の SHA-256 フィンガープリントを生成します

```
openssl x509 -inform DER -in <input.cer> -out <output.crt>
openssl x509 -in <output.crt> -fingerprint -noout -sha256
```

次に、出力の例を示します。

```
openssl x509 -in 535-pos.crt -fingerprint -noout -sha256
SHA256
Fingerprint=B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5
```

次の例は、AnyConnectLocalPolicy.xml の新しいタグを示しています。

```
<TrustedISECertFingerprints>
<fingerprint>
<algorithm>SHA-256</algorithm>
<hash>B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5</hash>
</fingerprint>
</TrustedISECertFingerprints>
```

（注） SHA-256 フィンガープリントは、コロンの有無にかかわらず追加できます。次のいずれかの形式でフィンガープリントを追加できます。
`B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5` または
`B9427F8509183040060BDB9C4836F0609075ABD3E983AB1ABF018F6EF0119AB5`。フィンガープリントでは大文字と小文字は区別されません。

エージェントは、Cisco ISE 証明書のフィンガープリントと信頼できる証明書のフィンガープリント（AnyConnectLocalPolicy.xml に存在）を照合します。エンドポイントに有効な証明書フィンガープリントがない場合、スクリプトはエンドポイントで実行されません。

（注） AnyConnectLocalPolicy.xml でフィンガープリントが設定されている場合、すべてのフローの Cisco ISE 信頼を検証するためにそれらのフィンガープリントが使用されます。証明書が信頼できない場合、またはフィンガープリントの不一致がある場合、エラーメッセージは表示されません。ただし、次のエラーメッセージが [ポスチャスクリプト条件（Posture Script Condition）] レポートに含まれています（[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）]）。

`条件スクリプト証明書の検証に失敗しました。クライアントが、Cisco ISE よって提示されたサーバー証明書を検証できませんでした。`

スクリプト終了コード

スクリプトには、条件が合格したか失敗したかを判断するための明示的な終了コードが必要です。スクリプトがゼロで終了した場合、条件は合格とマークされます。終了コードがゼロより大きい場合、条件は失敗とマークされます。

スクリプトの実行前にエラー（スクリプトのダウンロードの失敗やハッシュ検証エラーなど）が発生した場合、条件は失敗とマークされます。

設定されたタイムアウト時間内にスクリプトが終了しなかった場合、スクリプトは終了し、終了コードが適切に設定されます。

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] > [ポスチャスクリプト条件（Posture Script Condition）]** を選択し、スクリプトの実行ステータスを確認します。

次のステータスのいずれかが表示されます。

- 0 – 条件スクリプトの実行に成功しました。
- > 0 – 条件スクリプトが実行され、そのスクリプトは失敗コードと共に終了しました。
- -1 – 条件スクリプトは試行されませんでした。

- -2 – 条件スクリプトは実行されませんでした。ポリシーは整合性チェックに失敗しました。
- -3 – 条件スクリプトは実行されませんでした。クライアントがスクリプトのダウンロードに失敗しました。
- -4 – 条件スクリプトは実行されませんでした。スクリプトは整合性チェックに失敗しました。
- -5 – 条件スクリプトが失敗しました。スクリプトは実行されましたが、時間内に終了しませんでした（タイムアウト）。
- -6 – 条件スクリプトが失敗しました。一般的な内部システム障害が発生しました。
- -7 – 条件スクリプトは実行されませんでした。スクリプトタイプがサポートされていません。
- -8 – 条件スクリプトが失敗しました。スクリプトの起動に失敗しました。
- -9 – 条件スクリプト証明書の検証に失敗しました。クライアントは、Cisco ISE によって提示されたサーバー証明書を確認できませんでした。

スクリプトのダウンロード

ポスチャエージェントは、ポスチャポリシーに含まれる HTTPS URL からスクリプトをダウンロードします。スクリプトは、次の条件が満たされた場合にのみダウンロードされます。

- 信頼できる証明書のフィンガープリントが AnyConnectLocalPolicy.xml に存在する。
- HTTPS URL によって提示されるフィンガープリントが、AnyConnectLocalPolicy.xml に存在している信頼できる証明書フィンガープリントと一致している。

（注）

- フィンガープリント検証は、テンポラルエージェントおよびエージェントレス ポスチャ フローでは実行されません。
- テンポラルエージェントおよびエージェントレス ポスチャ フローでは、ポリシーの整合性チェックがバイパスされます。

ポスチャ ポリシーの設定

ポスチャ ポリシーは 1 つ以上の ID グループおよびオペレーティング システムに関連付けられたポスチャ要件の集合です。ディクショナリ属性は、デバイスの異なるポリシーを定義する、ID グループおよびオペレーティング システムと組み合わされたオプションの条件です。

Cisco ISE には、適合しないデバイスの猶予時間を設定するオプションが用意されています。デバイスが適合していないことが判明した場合、Cisco ISE はポスチャ評価結果キャッシュ内で以前の正常な状態を検索し、デバイスに猶予時間を与えます。デバイスには、猶予期間中にネットワークへのアクセス権が付与されます。分、時、または日単位（最大 30 日）で猶予期間を設定できます。

詳細については、『ISE Posture Prescriptive Deployment Guide』の「Posture Policy」の項を参照してください。

（注） 「エンドポイントポリシー」と「論理プロファイル」の両方が **[ポリシー（Policy）]** > **[ポスチャ（Posture）]** の [その他の条件（Other Conditions）] で設定されている場合、プロファイラポリシー評価は機能しません。

（注）

- 猶予期間が延長または短縮されると、デバイスがポスチャ フローを再び通過した場合（たとえば、[遅延通知（Delayed Notification）] オプションが有効で、[再スキャン（Re-Scan）] オプションが選択されている場合、デバイスとネットワークの切断や再接続が行われます）、新しい猶予期間および遅延通知が適用されます。
- 猶予期間は Temporal Agent には適用されません。
- 猶予期間は Linux エージェントではサポートされません。
- （それぞれ異なる猶予期間を設定した）複数のポスチャ ポリシーにデバイスが一致する場合、それらの異なるポリシーで設定された最大の猶予期間がデバイスに与えられます。
- デバイスが猶予期間になると、アクセプタブル ユース ポリシー（AUP）は表示されません。

始める前に

- アクセプタブル ユース ポリシー（AUP）について理解している必要があります。
- 定期的再評価（PRA）について理解している必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）]** > **[ポスチャ（Posture）]** または **[ワークセンター（Work Centers）]** > **[ポスチャ（Posture）]** > **[ポスチャポリシー（Posture Policy）]**。

ステップ 2 ドロップダウンの矢印を使用して新しいポリシーを追加します。

ステップ 3 プロファイルを編集するには、ポリシーをダブルクリックするか、または行の末尾にある [編集（Edit）] をクリックします。

ステップ 4 [ルールステータス（Rule Status）] ドロップダウン リストで [有効（Enabled）] または [無効（Disabled）] を選択します。

ステップ 5 [ポリシーオプション（Policy Options）] でドロップダウンを選択し、[猶予期間の設定（Grace Period Settings）] を分単位、時間単位、日単位で指定します。

有効な値は次のとおりです。

- 1 ー 90 日
- 1 ー 2,160 時間
- 1 ー 129,600 分

デフォルトでは、この設定は無効です。

（注） ポスチャ評価の結果が適合しない場合でも、デバイスが以前に準拠しており、キャッシュの期限がまだ切れていなければ、[猶予期間の設定（Grace Period Settings）] で指定された時間にわたり、デバイスにアクセス権が付与されます。

ステップ 6 （オプション）[遅延通知（Delayed Notification）] という名前のスライダをドラッグし、猶予期間の特定の割合が過ぎるまで、猶予期間プロンプトがユーザーに遅れて表示されるようにします。たとえば、通知遅延期間が 50 % に設定され、設定されている猶予期間が 10 分の場合、Cisco ISE は 5 分後にポスチャステータスをチェックし、エンドポイントが準拠していないと判断した場合は猶予期間通知を表示します。エンドポイントのステータスが準拠している場合、猶予期間通知は表示されません。通知遅延期間が 0 % に設定されている場合は、猶予期間の開始時に直ちに問題の解決を促すメッセージが表示されます。ただし、エンドポイントは、猶予期間の有効期限が切れるまで、アクセス権が付与されます。このフィールドのデフォルト値は 0% です。有効な範囲は 0 ～ 95% です。

ステップ 7 [ルール名（Rule Name）] フィールドに、ポリシーの名前を入力します。

（注） 予期しない結果を回避するためのベストプラクティスは、各要件でポスチャ ポリシーを個別のルールとして設定することです。

ステップ 8 [IDグループ（Identity Groups）] 列から任意の ID グループを選択します。

ユーザーまたはエンドポイントの ID グループに基づいて、ポスチャ ポリシーを作成することができます。

ステップ 9 [オペレーティングシステム（Operating Systems）] 列からオペレーティング システムを選択します。

ステップ 10 [準拠モジュール（Compliance Module）] 列から必要な準拠モジュールを選択します。

- [4.x 以降（4.x or Later）]：マルウェア対策、ディスク暗号化、パッチ管理、および USB の各種条件をサポートします。
- [3.x 以前（3.x or Earlier）]：ウイルス対策、スパイウェア対策、ディスク暗号化、およびパッチ管理の各種条件をサポートします。
- [すべてのバージョン（Any Version）]：ファイル、サービス、レジストリ、アプリケーション、および複合の各種条件をサポートします。

ステップ 11 [ポスチャタイプ（Posture Type）] 列から、[ポスチャタイプ（Posture Type）] を選択します。

- **[エージェント（Agent）]**：エージェントを展開し、クライアントとのやりとりが必要なCisco ISEポリシーを監視し、適用します。
- **[エージェントステルス（Agent Stealth）]**：エージェントを展開し、クライアントとやりとりしないCisco ISE ポスチャポリシーを監視し、適用します。
- [一時エージェント（Temporal Agent）]：準拠のステータスを確認するためにクライアント上で実行される一時実行可能ファイル。

ステップ 12 [その他の条件（Other Conditions）]では、1つ以上のディクショナリ属性を追加し、単純条件または複合条件としてディクショナリに保存できます。

（注） [ポスチャポリシー（Posture Policy）]ウィンドウで作成したディクショナリ単純条件とディクショナリ複合条件は、許可ポリシーを設定するときには表示されません。

ステップ 13 [要件（Requirements）]フィールドに要件を指定します。

ステップ 14 [保存（Save）]をクリックします。

エージェントのワークフローの設定

エージェントを設定するには、Cisco ISE で次の手順を実行します。

ステップ 1 エージェントプロファイルを作成します。

ステップ 2 エージェントパッケージのエージェント設定を作成します。

ステップ 3 クライアント プロビジョニング ポリシーを作成します。

ステップ 4 （任意）カスタムポスチャを作成します。

ステップ 5 （任意）カスタム修復アクションを作成します。

ステップ 6 （任意）カスタムポスチャの要件を作成します。

ステップ 7 ポスチャポリシーを作成します。

ステップ 8 クライアント プロビジョニング ポリシーを設定します。

ステップ 9 認証プロファイルを作成します。

ステップ 10 認証ポリシーを設定します。

ステップ 11 エージェントをダウンロードして起動します。

a) SSID に接続します。
b) ブラウザを起動すると、クライアント プロビジョニング ポータルにリダイレクトされます。
c) [開始（Start）]をクリックします。これにより、エージェントがインストールされ、動作しているかどうかがチェックされます。
d) [ここに初めて来ました（This Is My First Time Here）]をクリックします。
e) **[エージェントをダウンロードして起動するにはここをクリック（Click Here to Download and Launch Agent）]**を選択します。

f) Windows または MacOS 用の エージェントの .exe または .dmg ファイルをそれぞれ保存します。Windows の場合は .exe ファイルを実行し、MacOS の場合は .dmg ファイルをダブルクリックして、アプリケーションを実行します。

証明書ベースの条件のための前提条件

クライアント プロビジョニングおよびポスチャ ポリシーのルールに、証明書の属性に基づく条件を含めることができます。クライアントプロビジョニングまたはポスチャポリシーのいずれかにおける証明書ベースの条件では、同じ証明書属性に基づいて一致する認証ポリシールールが存在することが前提条件になります。

たとえば、図に示されているように同じ属性を使用する必要があります。[発行者 - 共通名（Issuer – Common Name）] 属性が、クライアント プロビジョニングまたはポスチャと許可ポリシーの両方で使用されています。

図 *75 : Cisco* のプロビジョニング ポリシー

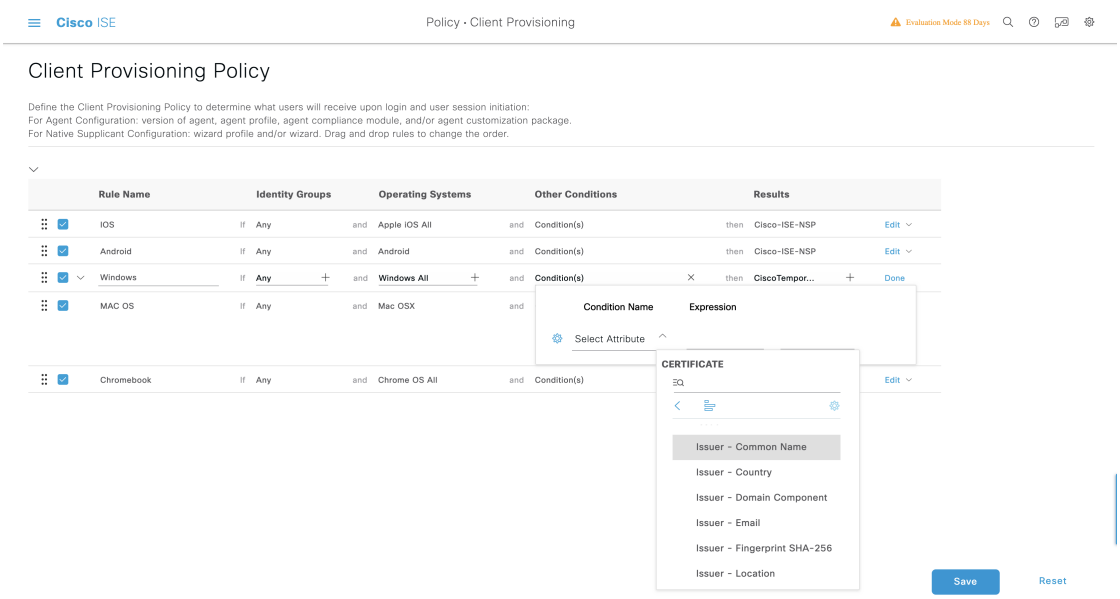
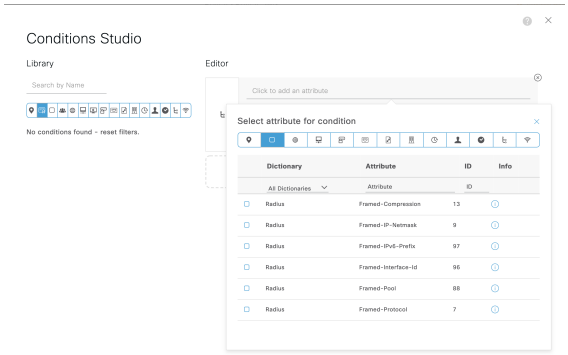


図 *76 : [*条件スタジオ（***Conditions Studio***）*]*



（注） ISE サーバー証明書は、AnyConnect 4.6 MR2 以降のシステム証明書ストアで信頼できる必要があります。昇格権限を必要とするポスチャ チェックおよび修復は、サーバーが信頼されていない場合は機能しません。

- Windows OS：サーバー証明書をシステム証明書ストアに追加する必要があります。
- MAC OS：サーバー証明書をシステムキーチェーンに追加する必要があります。コマンドライン ユーティリティを使用して証明書を信頼することをお勧めします。キーチェーン アクセス アプリケーションを使用してシステム キーチェーンに証明書を追加しても、ログイン キーチェーンにすでに存在する場合は機能しないことがあります。

デフォルトのポスチャ ポリシー

Cisco ISE ソフトウェアには、ポスチャポリシーとプロファイルの作成を容易にする、事前に設定されたポスチャポリシーが多数用意されています。これらのポリシーは、デフォルトで無効になっています。要件に基づいて、これらのポリシーを有効にできます。次に、デフォルトのいくつかのデフォルトのポスチャポリシーを示します。

ルール名	説明	要件
Default_Antimalware_Policy_Mac	エンドポイントに、サポートされているベンダーのマルウェア対策ソフトウェア（エージェントで認識されているもの）がインストールされ、デバイスで実行されているかどうかを確認します。	Any_AM_Installation

ルール名	説明	要件
Default_Antimalware_Policy_Win	エンドポイントに、サポートされているベンダーのマルウェア対策ソフトウェア（エージェントで認識されているもの）がインストールされ、デバイスで実行されているかどうかを確認します。	Any_AM_Installation_Win
Default_AppVis_Policy_Mac	情報を収集し、特定のエンドポイントにインストールされているすべてのアプリケーションを報告します。	Default_AppVis_Requirement_Mac
Default_AppVis_Policy_Win	情報を収集し、特定のエンドポイントにインストールされているすべてのアプリケーションを報告します。	Default_AppVis_Requirement_Win
Default_Firewall_Policy_Mac	エンドポイントに、サポートされているベンダーのファイアウォールプログラム（エージェントで認識されているもの）がインストールされているかどうかを確認します。	Default_Firewall_Requirement_Mac
Default_Firewall_Policy_Win	エンドポイントに、サポートされているベンダーのファイアウォールプログラム（エージェントで認識されているもの）がインストールされているかどうかを確認します。	Default_Firewall_Requirement_Win
Default_USB_Block_Win	エンドポイントデバイスにUSB ストレージ デバイスが接続されていないことを確認します。	USB_Block

クライアント ポスチャ評価

Cisco ISE を使用すると、適用されたネットワーク セキュリティ対策の適切さと効果を維持するために、保護されたネットワークにアクセスする任意のクライアントマシンに対してセキュリティ機能を検証し、そのメンテナンスを行うことができます。Cisco ISE 管理者は、クライアントマシンで最新のセキュリティ設定またはアプリケーションを使用できるよう設計されたポスチャポリシーを使用することによって、どのクライアントマシンでも、エンタープライズネットワークへのアクセスについて定義されたセキュリティ標準を満たし、その状態を継続することを保証できます。ポスチャ コンプライアンス レポートによって、ユーザーがログインしたとき、および定期的再評価が行われるたびに、クライアント マシンのコンプライアンス レベルのスナップショットが Cisco ISE に提供されます。

ポスチャ評価オプション

次の表に、Windows および MacOS の Cisco ISE Posture Agent、および Windows の Web Agent でサポートされるポスチャアセスメント（ポスチャ条件）オプションのリストを示します。

表 *167 :* ポスチャ評価オプション

Windows 用 ISE ポスチャ エージェント	Windows 用 Cisco Temporal エージェント	MacOS 用 ISE ポスチャ エージェント	MacOS 用 Cisco Temporal エージェント
オペレーティングシステム/サービス パック/ホットフィックス	—	—	—
サービス チェック	サービスチェック（Temporal エージェント 4.5）	サービスチェック	デーモンチェックはサポートされていません
レジストリ チェック	レジストリチェック（Temporal エージェント 4.5）	—	—
ファイル チェック	ファイルチェック（Temporal エージェント 4.5）	ファイルチェック	ファイルチェック（Temporal エージェント 4.5）
アプリケーション チェック	アプリケーション チェック（Temporal エージェント 4.5）	アプリケーション チェック	アプリケーション チェック（Temporal エージェント 4.5）
アンチウイルスのインストール	マルウェア対策のインストール	アンチウイルスのインストール	マルウェア対策のインストール

Windows 用 ISE ポスチャ エージェント	Windows 用 Cisco Temporal エージェント	MacOS 用 ISE ポスチャ エージェント	MacOS 用 Cisco Temporal エージェント
アンチウイルス バージョン/アンチウイルス定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチウイルス バージョン/アンチウイルス定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
アンチスパイウェアのインストール	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチスパイウェアのインストール	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
アンチスパイウェア バージョン/アンチスパイウェア定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチスパイウェア バージョン/アンチスパイウェア定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
パッチ管理チェック	パッチ管理のインストールのみチェック	パッチ管理チェック	—
実行中の Windows Update	—	—	—
Windows Update の設定	—	—	—
WSUS のコンプライアンス設定	—	—	—

ポスチャ修復オプション

次の表に、Windows および MacOS の Cisco ISE ポスチャエージェント、および Windows の Web エージェントでサポートされている修復オプション（ポスチャ条件）のリストを示します。

表 *168 :* ポスチャ修復オプション

ISE ポスチャ エージェント **Windows**	**ISE ポスチャ エージェント** **MacOS**
メッセージ テキスト（ローカル チェック）	メッセージ テキスト（ローカル チェック）
URL リンク（リンク分散）	URL リンク（リンク分散）
ファイル配布	—
プログラム起動	—
アンチウイルス定義更新	アンチウイルス ライブ更新
アンチスパイウェア定義更新	アンチスパイウェア ライブ更新
パッチ管理修復	—
Windows Update	—
WSUS	—

ISE Community Resource

Cisco ISE と SCCM の統合ワークフロー

ポスチャのカスタム条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの 1 つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

最初のポスチャ更新の後に、Cisco ISE もシスコ定義の単純条件と複合条件を作成します。シスコ定義の単純条件では pc_ as が使用され、複合条件では pr_ as が使用されます。

ユーザー定義の条件またはシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

ポスチャ サービスは、アンチウイルスおよびアンチスパイウェア（AV/AS）複合条件に基づいた内部チェックを使用します。このため、ポスチャ レポートは、作成した正確な AV/AS 複合条件名を反映しません。レポートには、AV/AS 複合条件の内部チェックの名前だけが表示されます。

たとえば、任意のベンダーおよび製品をチェックする「MyCondition_AV_Check」という名前の AV 複合条件を作成した場合、ポスチャ レポートには、条件名として、「MyCondition_AV_Check」ではなく、内部チェック「av_def_ANY」が表示されます。

ポスチャ エンドポイント カスタム属性

ポスチャ エンドポイントのカスタム属性を使用して、クライアント プロビジョニングおよびポスチャ ポリシーを作成できます。最大100個のエンドポイントのカスタム属性を作成できます。以下のタイプのエンドポイントカスタム属性がサポートされています：Int、String、Long、Boolean、Float、IP、および Date。

エンドポイントカスタム属性は、特定の属性に基づいてデバイスを許可またはブロックするために使用することも、ポスチャまたはクライアント プロビジョニング ポリシーに基づいて特定の権限を割り当てるために使用することもできます。

エンドポイント カスタム属性を使用したポスチャ ポリシーの作成

エンドポイント カスタム属性を使用してポスチャ ポリシーを作成するには、次の手順を実行します。

ステップ 1 エンドポイント カスタム属性を作成します。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイントカスタム属性（Endpoint Custom Attributes）]** の順に選択します。

b) [エンドポイント カスタム属性（Endpoint Custom Attributes）] 領域に、[属性名（Attribute Name）]（たとえば、deviceType）と [データ型（Data Type）]（たとえば、String）を入力します。

c) [保存（Save）] をクリックします。

ステップ 2 カスタム属性に値を割り当てます。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] の順に選択します。

b) カスタム属性値を割り当てます。

- 必要な MAC アドレスのチェックボックスをオンにし、[編集（Edit）] をクリックします。
- または、必要なMACアドレスをクリックし、[エンドポイント（Endpoints）]ページで[編集（Edit）] をクリックします。

c) 作成したカスタム属性が、[エンドポイントの編集（Edit Endpoint）] ダイアログボックスの [カスタム属性（Custom Attributes）] 領域に表示されていることを確認します。

d) [編集（Edit）] をクリックし、必要な属性値を入力します（たとえば、deviceType = Apple-iPhone）。

e) [保存（Save）] をクリックします。

ステップ 3 カスタム属性と値を使用してポスチャ ポリシーを作成します。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャポリシー（Posture Policy）]** を選択します。

b) 必要なポリシーを作成します。[その他の条件（Other Conditions）] をクリックしてカスタム属性を選択し、必要なディクショナリを選択します（たとえば、ステップ 1 で作成したカスタム属性である [エンドポイント（Endpoints）] > [deviceType] を選択します）。詳細については、「Cisco Temporal Agent のワークフローの設定 （1787 ページ）」を参照してください。

c) [保存（Save）] をクリックします。

エンドポイント カスタム属性を使用してクライアント プロビジョニング ポリシーを作成するには、次の手順を実行します。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [クライアントプロビジョニング（Client Provisioning）] > [クライアントプロビジョニングポリシー（Client Provisioning Policy）]** を選択します。
2. 必要なポリシーを作成します。
   - 必要なルールを作成します（たとえば、Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。
   - [その他の条件（Other Conditions）] をクリックして必要なディクショナリを選択して、カスタム属性を選択します。

カスタム ポスチャ修復アクション

カスタムポスチャ修復アクションは、ファイル、リンク、アンチウイルスまたはアンチスパイウェア定義の更新、プログラムの起動、Windows Update、Windows Server Update Services（WSUS）の修復タイプです。

アンチスパイウェア修復の追加

アンチスパイウェア修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AS 修復（AS Remediations）] ウィンドウには、すべてのウイルス対策修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [AS 修復（AS Remediations）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 AS 修復（New AS Remediation）] ウィンドウで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

アンチウイルス修復の追加

アンチウイルス修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AV 修復（AV Remediations）] ウィンドウには、すべてのウイルス対策修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [AV 修復（AV Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 AV 修復（New AV Remediation）] ウィンドウで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

ファイル修復の追加

ファイル修復により、クライアントはコンプライアンスに必要なファイルのバージョンをダウンロードできます。クライアントエージェントは、コンプライアンスのためにクライアントが必要とするファイルを使用してエンドポイントを修復します。

[ファイル修復（File Remediations）] ウィンドウではファイル修復をフィルタリング、表示、追加、または削除することはできますが、ファイル修復を編集することはできません。[ファイル修復（File Remediations）] ウィンドウには、すべてのファイル修復がそれらの名前と説明、および修復に必要なファイルとともに表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [ファイル修復（File Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [名前（Name）] フィールドに名前を入力し、[説明（Description）] フィールドにファイル修復の説明を入力します。

ステップ 6 [新規ファイル修復（New File Remediation）] ウィンドウで値を変更します。

ステップ 7 [送信（Submit）] をクリックします。

スクリプト修復の追加

ポスチャ修復スクリプトを作成して Cisco ISE にアップロードし、エンドポイントのコンプライアンス違反の問題を解決できます。

始める前に

- ポスチャポリシーを取得するための信頼を確立します。詳細については、「スクリプト条件を実行するために信頼を確立 （1753 ページ）」を参照してください。
- スクリプトをダウンロードします。詳細については、「スクリプトのダウンロード（1770 ページ）」を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）]**。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [スクリプト修復（Script Remediations）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 スクリプトの [名前（Name）] と [説明（Description）] に入力します。

ステップ 6 対応するドロップダウンリストから [オペレーティングシステム（Operating System）] と [修復タイプ（Remediation Type）] を選択します。

[Windows] オペレーティングシステムを選択した場合は、[スクリプトタイプ（Script Type）] と [Windows PowerShell 実行ポリシー（Windows PowerShell Execution）] フィールドが表示されます。対応するオプションボタンをクリックして、必要なスクリプトタイプと実行ポリシーを選択します。

ステップ 7 [修復タイプ（Remediation Type）] ドロップダウンリストから、[自動（Automatic）] または [手動（Manual）] を選択します。

（注）
- Linux エージェントでは、自動修復のみがサポートされます。手動修復はサポートされていません。
- Linux エージェントでは、シェルスクリプトのみがサポートされます。

ステップ 8 [間隔（Interval）] と [再試行回数（Retry Count）] に値を入力します。有効な範囲は 0 ～ 999 です。

ステップ 9 [アップロードするファイル（File To Upload）] の隣にある [ファイルの選択（Choose File）] をクリックし、ローカルシステムからアップロードするスクリプトを選択します。

ステップ 10 スクリプトを管理者として実行するには、[管理者/ルート（Administrator/Root）] オプションボタンをクリックします。ログインユーザーとしてスクリプトを実行するには、[ログインユーザー（Logged-in User）] オプションボタンをクリックします。

ステップ 11 [送信（Submit）] をクリックします。

ステップ 12 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[運用（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] > [ポスチャスクリプト修復（Posture Script Remediation）]**、修復スクリプトの実行ステータスを確認します。

次のいずれかのステータスが表示されます。

- 修復スクリプトの実行に成功しました。
- 修復が試行され、スクリプトは失敗して終了しました。
- 修復は試行されませんでした（デフォルト）。
- 修復の試行に失敗しました。含まれているポリシーが改ざんされている可能性があるため、スクリプトは整合性チェックに失敗しました。
- 修復の試行に失敗しました。クライアントがスクリプトのダウンロードに失敗しました。
- 修復の試行に失敗しました。スクリプトが破損しているか、改ざんされている可能性があるため、スクリプトは整合性テストに失敗しました。
- 修復の試行に失敗しました。スクリプトは実行されましたが、時間内に終了しませんでした（タイムアウト）。
- 修復の試行に失敗しました。一般的な内部システム障害が発生しました。
- 修復の試行に失敗しました。スクリプトタイプはサポートされていません。
- 修復の試行に失敗しました。スクリプトの起動に失敗しました。
- 証明書の確認に失敗しました。クライアントは、Cisco ISE によって提示されたサーバー証明書を確認できませんでした。

スクリプト条件を実行するために信頼を確立

エンドポイントでスクリプトを実行し、Cisco ISE サーバーが侵害されていないことを確認するには、信頼を確立する必要があります。Cisco ISE 環境では、1 つ以上の PSN を設定できます。すべての PSN には有効な証明書チェーンがあります。証明書チェーンは任意の証明書で始まり、中間証明書またはルート CA 証明書が続きます。フィンガープリントの検証では、証明書チェーン内のすべての証明書を使用できます。

AnyConnectLocalPolicy のプロファイルエディタの証明書チェーン内に任意の証明書の SHA-256 フィンガープリントを設定できます。たとえば、次のコマンドは、input.cer という名前の証明書の SHA-256 フィンガープリントを生成します

```
openssl x509 -inform DER -in <input.cer> -out <output.crt>
openssl x509 -in <output.crt> -fingerprint -noout -sha256
```

次に、出力の例を示します。

```
openssl x509 -in 535-pos.crt -fingerprint -noout -sha256
SHA256
Fingerprint=B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5
```

次の例は、AnyConnectLocalPolicy.xml の新しいタグを示しています。

```
<TrustedISECertFingerprints>
<fingerprint>
<algorithm>SHA-256</algorithm>
<hash>B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5</hash>
</fingerprint>
</TrustedISECertFingerprints>
```

（注） SHA-256 フィンガープリントは、コロンの有無にかかわらず追加できます。次のいずれかの形式でフィンガープリントを追加できます。
`B9:42:7F:85:09:18:30:40:06:0B:DB:9C:48:36:F0:60:90:75:AB:D3:E9:83:AB:1A:BF:01:8F:6E:F0:11:9A:B5` または
`B9427F8509183040060BDB9C4836F0609075ABD3E983AB1ABF018F6EF0119AB5`。フィンガープリントでは大文字と小文字は区別されません。

エージェントは、Cisco ISE 証明書のフィンガープリントと信頼できる証明書のフィンガープリント（AnyConnectLocalPolicy.xml に存在）を照合します。エンドポイントに有効な証明書フィンガープリントがない場合、スクリプトはエンドポイントで実行されません。

（注） AnyConnectLocalPolicy.xml でフィンガープリントが設定されている場合、すべてのフローの Cisco ISE 信頼を検証するためにそれらのフィンガープリントが使用されます。証明書が信頼できない場合、またはフィンガープリントの不一致がある場合、エラーメッセージは表示されません。ただし、次のエラーメッセージが [ポスチャスクリプト条件（Posture Script Condition）] レポートに含まれています（[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）]）。

条件スクリプト証明書の検証に失敗しました。クライアントが、Cisco ISE よって提示されたサーバー証明書を検証できませんでした。

スクリプトのダウンロード

ポスチャチェックが失敗し、関連する修復アクションがトリガーされると、エージェントはポスチャポリシーで設定された HTTPS URL からスクリプトをダウンロードします。スクリプトをダウンロードするには、次の条件を満たしている必要があります。

- 信頼できるフィンガープリントが AnyConnectLocalPolicy.xml に存在している。
- HTTPS URL によって提示されるフィンガープリントが、AnyConnectLocalPolicy.xml に存在している信頼できる証明書フィンガープリントと一致している。

プログラム修復起動の追加

コンプライアンスのために、クライアントエージェントが1つ以上のアプリケーションを起動してクライアントを修復するプログラム修復起動を作成できます。

[プログラム修復起動（Launch Program Remediations）] ページには、すべてのプログラム修復起動がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [プログラム起動修復（Launch Program Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規プログラム修復起動（New Launch Program Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

プログラム修復起動のトラブルシューティング

問題

プログラム修復起動を使用して、アプリケーションを修復として起動すると、アプリケーションは正常に開始されます（Windows Task Manager で観察されます）が、アプリケーション UI は表示されません。

ソリューション

プログラム起動 UI アプリケーションはシステム権限で実行され、[インタラクティブサービス検出（ISD）（Interactive Service Detection (ISD)）] ウィンドウに表示されます。プログラム起動 UI アプリケーションを表示するには、次の OS で ISD をイネーブルにする必要があります。

- Windows Vista：ISD はデフォルトで停止状態になっています。services.msc で ISD サービスを起動して、ISD をイネーブルにします。
- Windows 7：ISD サービスはデフォルトでイネーブルになっています。
- Windows 8/8.1：レジストリ \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows で「NoInteractiveServices」を 1 から 0 に変更することで ISD をイネーブルにします。

リンク修復の追加

リンク修復により、クライアントは修復ウィンドウまたはリソースにアクセスするための URL をクリックできます。クライアントエージェントはリンクを使用してブラウザを開き、クライアントはコンプライアンスのために自身を修復できます。

[リンク修復（Link Remediation）] ウィンドウには、すべてのリンク修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [リンク修復（Link Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規リンク修復（New Link Remediation）] ウィンドウで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

パッチ管理修復の追加

パッチ管理修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[パッチ管理修復（Patch Management Remediation）] ウィンドウには、修復タイプ、パッチ管理ベンダーの名前、およびさまざまな修復オプションが表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [パッチ管理修復（Patch Management Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [パッチ管理修復（Patch Management Remediation）] ウィンドウで値を変更します。

ステップ 6 [送信（Submit）] をクリックして、[パッチ管理修復（Patch Management Remediation）] ウィンドウに修復アクションを追加します。

Windows Server Update Services 修復の追加

コンプライアンスのためにローカルに管理されているか、または Microsoft で管理されている WSUS サーバーから最新の WSUS 更新を受信するように Windows クライアントを設定できます。Windows Server Update Services（WSUS）修復は、ローカルに管理されている WSUS サーバーまたは Microsoft で管理されている WSUS サーバーから最新の Windows サービス パック、ホット フィックス、およびパッチをインストールします。

クライアント エージェントをローカルの WSUS Agent と統合して、エンドポイントの WSUS 更新が最新かどうかをチェックする WSUS 修復を作成できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]**。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [Windows Server Update Service 修復（Windows Server Update Services Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 Windows Server Update Service 修復（New Windows Server Update Services Remediation）] ウィンドウの値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

Windows Update 修復の追加

[Windows Update 修復（Windows update remediations）] ページには、すべての Windows Update 修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > > **[ポスチャ（Posture）]**。.

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [Windows Update 修復（Windows Update Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 Windows Update 修復（New Windows Update Remediation）] ウィンドウで値を変更します。

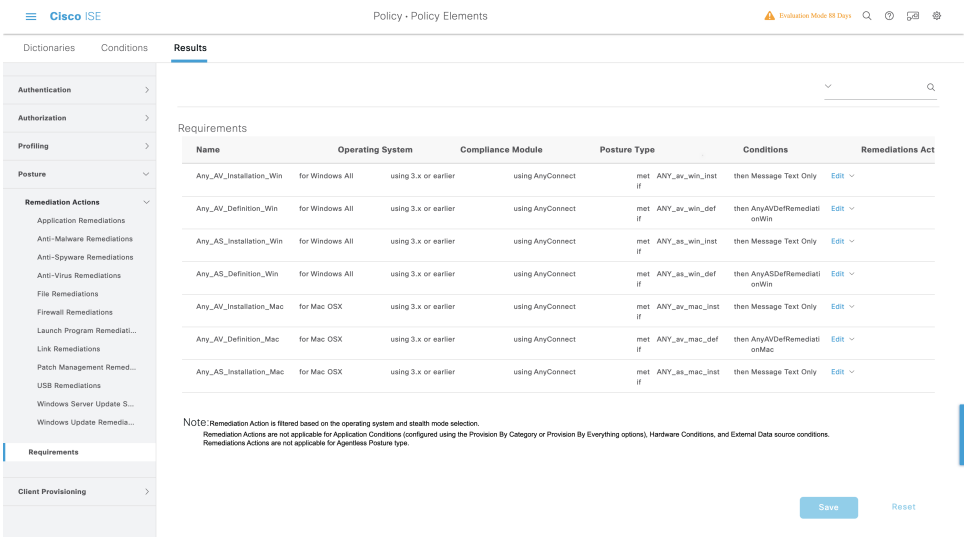
ステップ 6 [送信（Submit）] をクリックします。

ポスチャ評価要件

ポスチャ要件は、ロールおよびオペレーティングシステムとリンクできる修復アクションを伴う一連の複合条件です。ネットワークに接続しているすべてのクライアントは、ネットワークで適合ホストになるためにはポスチャ評価中に必須要件を満たす必要があります。

ポスチャ ポリシー要件は、ポスチャ ポリシーの必須、オプション、または監査タイプに設定できます。要件がオプションで、クライアントがこれらの要件を満たさない場合、クライアントにはエンドポイントのポスチャ評価中に続行するオプションがあります。

図 77：ポスチャ ポリシーの要件タイプ



必須要件

ポリシーの評価時に、エージェントはポスチャ ポリシーに定義されている必須要件を満たすことができないクライアントに修復オプションを提供します。エンドユーザーは、修復タイマー設定で指定された時間内に要件を満たすように修復する必要があります。

たとえば、絶対パス内に C:\temp\text.file があるかをチェックするために、ユーザー定義の条件を含む必須要件を指定したとします。ファイルがない場合、必須要件は失敗し、ユーザーは [非準拠（Non-Compliant）] 状態になります。

オプション要件

ポリシーの評価時に、クライアントがポスチャ ポリシーに指定されたオプション要件を満たすことができない場合に、エージェントは続行するためのオプションをクライアントに提供します。エンドユーザーは、指定されたオプション要件をスキップすることができます。

たとえば、Calc.exe などのクライアント マシンで実行するアプリケーションをチェックするために、ユーザー定義の条件を含むオプション要件を指定したとします。クライアントが条件を満たすことができない場合、オプション要件がスキップされ、エンドユーザーが [準拠（Compliant）] 状態になるように、さらに続行するためのオプションがエージェントによって促されます。

監査要件

監査要件は内部用に指定され、エージェントはポリシー評価時の合格または失敗のステータスに関係なく、メッセージやエンドユーザーからの入力を促しません。

たとえば、エンドユーザーにアンチウイルス プログラムの最新バージョンがあるかどうかを確認するために、必須のポリシー条件を作成中だとします。ポリシー条件として実際に適用する前に非準拠のエンドユーザーを見つける場合は、その条件を監査要件として指定できます。

可視性要件

ポリシーの評価時に、エージェントが可視性要件のコンプライアンスデータを 5 ～ 10 分ごとに報告します。

非準拠ステートでスタックしたクライアント システム

クライアント マシンが必須要件を修復できない場合、ポスチャ ステータスは「非準拠」に変更され、エージェント セッションは隔離されます。クライアント マシンを「非準拠」状態から移行するには、エージェントがクライアントマシン上でポスチャ評価を再び開始するようにポスチャ セッションを再起動する必要があります。次のようにポスチャ セッションを再起動できます。

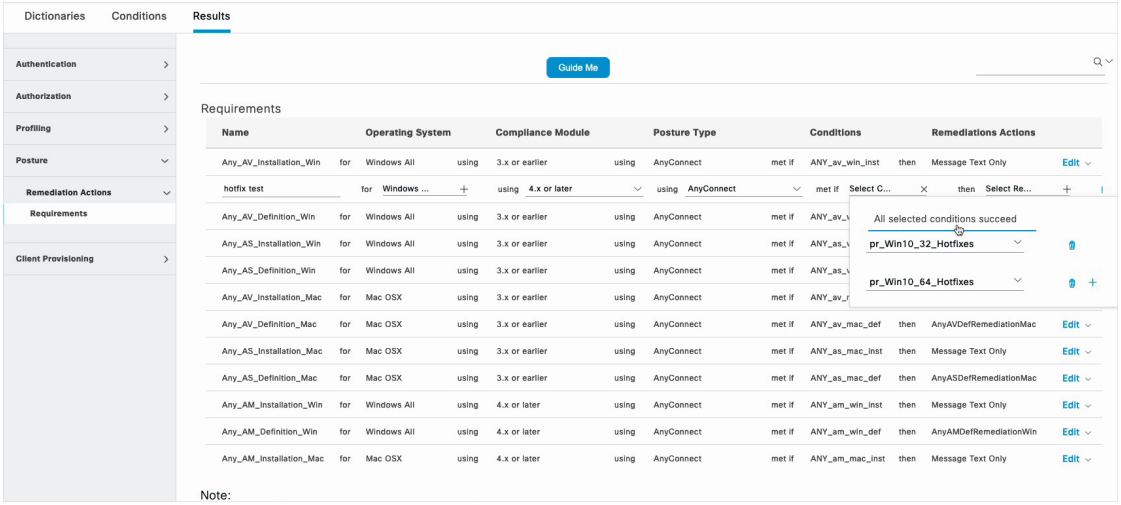
- 802.1X 環境での有線およびワイヤレス許可変更（CoA）：
  - [新しい許可プロファイル（New Authorization Profiles）] ウィンドウで新しい許可プロファイルを作成するときに、特定の許可ポリシーの再認証タイマーを設定できます。
  - 有線ユーザーは、ネットワークの接続を切断して再接続すると、隔離状態から移行できます。ワイヤレス環境では、ユーザーは、ワイヤレス LAN コントローラ（WLC）から切断し、ユーザーのアイドルタイムアウト時間が過ぎるまで待機してから、ネットワークへの再接続を試行する必要があります。
- VPN 環境：VPN トンネルを切断し、再接続します。

クライアントのポスチャ要件の作成

[要件（Requirements）] ウィンドウでは、ユーザー定義の条件とシスコ定義の条件、および修復アクションを関連付けて要件を作成できます。[要件（Requirements）] ウィンドウで作成および保存されたユーザー定義の条件および修復アクションは、それぞれのリストウィンドウに表示されます。

（注） 環境内のすべての Windows 10 ホットフィックスを検証するポスチャ要件を作成するには、要件の [条件（Conditions）] 領域に pr_Win10_32_Hotfixes と pr_Win10_64_Hotfixes の両方を含めるように設定する必要があります。条件の上部で、[選択したすべての条件が成功する（All selected conditions succeed）] が選択されていることを確認します。設定が成功すると、**pr_Win10_32_Hotfixes と pr_Win10_64_Hotfixes** が表示されます。エンドポイントの検証済み条件の詳細を表示するには、メインメニューから**[運用（Operations）]>[レポート（Reports）]>[レポート（Reports）]>[エンドポイントとユーザー（Endpoints and Users）]>[エンドポイントによるポスチャアセスメント（Posture Assessment by Endpoints）]**を選択します。エンドポイントをクリックして、対応するポスチャの詳細を表示します。

図 *78 : Windows 10* でのポスチャ要件の検証



始める前に

- ポスチャの利用規定（AUP）について理解している必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[結果（Results）]>[ポスチャ（Posture）]>[要件（Requirements）]**。

ステップ 2 [要件（Requirements）] ウィンドウに値を入力します。

ステップ 3 読み取り専用モードでポスチャ要件を保存するには、[完了（Done）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

ポスチャ再評価の構成設定

次の表では、ポスチャ再評価の設定に使用できる [ポスチャ再評価構成（Posture Reassessment Configurations）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]** です。

表 *169 :* ポスチャ再評価の構成設定

フィールド名	使用上のガイドライン
構成名（Configuration Name）	PRA 設定の名前を入力します。
設定の説明（Configuration Description）	PRA 設定の説明を入力します。
再評価適用を使用?（Use Reassessment Enforcement?）	ユーザー ID グループの PRA 設定を適用するには、チェックボックスをオンにします。

フィールド名	使用上のガイドライン
適用タイプ（**Enforcement Type**）	適用する次のアクションを選択します。 • [続行（Continue）]：ユーザーはポスチャ要件に関係なくクライアントを修復できるようにユーザー介入なしの特権アクセスが引き続き提供されます。 • [ログオフ（Logoff）]：クライアントが非準拠の場合、ユーザーを強制的にネットワークからログオフします。クライアントが再度ログインしたときのコンプライアンス ステータスは不明です。 • [修復（Remediate）]：クライアントが非準拠の場合、エージェントは修復のために指定の期間待機します。クライアントが修復された後、エージェントはポリシー サービス ノードに PRA レポートを送信します。修復がクライアントで無視された場合、エージェントはクライアントにネットワークからログオフすることを強制するために、ポリシー サービス ノードにログオフ要求を送信します。 ポスチャ要件が [必須（mandatory）] に設定されている場合、RADIUS セッションは PRA 障害アクションの結果としてクリアされ、クライアントを再びポスチャするには新しいRADIUSセッションを開始する必要があります。 ポスチャ要件が [任意（Optional）] に設定されている場合、クライアント上のエージェントではユーザーがエージェントから [続行（Continue）] オプションをクリックできます。ユーザーは、制限なしで現在のネットワークにとどまることができます。
インターバル（**Interval**）	最初のログイン成功後にクライアントで PRA を開始する間隔を分単位で入力します。 デフォルト値は 240 分です。最小値は 60 分、最大値は 1440 分です。
猶予時間（**Grace time**）	クライアントが修復を完了することのできる時間間隔を分単位で入力します。猶予時間をゼロにすることはできません。また、PRA 間隔より大きくする必要があります。デフォルトの最小間隔（5 分）から最小 PRA 間隔までの範囲にすることができます。 最小値は 5 分、最大値は 60 分です。 （注） 猶予時間は、クライアントがポスチャの再評価に失敗した後、適用タイプが修復アクションに設定されている場合にだけ有効です。
ユーザー ID グループの選択（**Select User Identity Groups**）	PRA 設定に対して一意のグループまたはグループの一意の組み合わせを選択します。

フィールド名	使用上のガイドライン
PRA の設定（PRA configurations）	既存の PRA 設定と PRA 設定に関連付けられたユーザー ID グループを表示します。

関連トピック

ポスチャのリース （1701 ページ）
定期的再評価 （1702 ページ）
ポスチャ評価オプション （1762 ページ）
ポスチャ修復オプション （1763 ページ）
ポスチャのカスタム条件 （1764 ページ）
カスタム ポスチャ修復アクション （1766 ページ）
定期的再評価の設定 （1702 ページ）

ポスチャのカスタム権限

カスタム権限は、Cisco ISE で定義する標準許可プロファイルです。標準許可プロファイルは、エンドポイントの一致するコンプライアンス ステータスに基づいてアクセス権を設定します。ポスチャ サービスでは、ポスチャは大きく不明プロファイル、準拠プロファイル、および非準拠プロファイルに分類されます。ポスチャ ポリシーおよびポスチャ要件によって、エンドポイントのコンプライアンス ステータスが決まります。

VLAN、DACL および他の属性値ペアの異なるセットを持つことができるエンドポイントの不明、準拠、および非準拠のポスチャステータスに対して 3 つの異なる認証プロファイルを作成する必要があります。これらのプロファイルは、3 つの異なる許可ポリシーに関連付けることができます。これらの許可ポリシーを区別するために、Session:PostureStatus 属性を他の条件とともに使用できます。

不明プロファイル

エンドポイントに一致するポスチャ ポリシーが定義されていない場合、そのエンドポイントのポスチャ コンプライアンス ステータスは不明に設定されることがあります。不明のポスチャ コンプライアンス ステータスは、一致するポスチャ ポリシーが有効であるが、エンドポイントに対してポスチャ評価がまだ行われておらず、従ってクライアント エージェントによってコンプライアンス レポートが提供されていないエンドポイントにも適用できます。

（注） すべてのシスコのネットワーク アクセス デバイスに、リダイレクトベースのポスチャを使用することを推奨します。

準拠プロファイル

エンドポイントに一致するポスチャ ポリシーが定義されている場合、そのエンドポイントのポスチャ コンプライアンス ステータスは準拠に設定されます。ポスチャ評価が行われると、エンドポイントは、一致するポスチャ ポリシー内に定義されているすべての必須要件を満たします。準拠とポスチャされているエンドポイントには、ネットワークに対する特権ネットワーク アクセスを付与できます。

非準拠プロファイル

エンドポイントのポスチャ コンプライアンス ステータスが非準拠に設定されるのは、そのエンドポイントに対して一致するポスチャ ポリシーが定義されているが、ポスチャ評価の実行中にすべての必須要件を満たすことができない場合です。非準拠としてポスチャされたエンドポイントは、修復アクションを含むポスチャ要件に一致し、自らを修復するために修復リソースへ制限付きのネットワーク アクセスが付与される必要があります。

標準許可ポリシーの設定

[認証ポリシー（Authorization Policy）] ウィンドウでは、標準認証ポリシーと例外認証ポリシーの2種類の認証ポリシーを定義できます。ポスチャに固有の標準許可ポリシーは、エンドポイントのコンプライアンス ステータスに基づいて、ポリシー決定を行うために使用されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]**。

ステップ 2 [ビュー（View）] 列で、対応するデフォルトポリシーに隣接する矢印アイコンをクリックします。

ステップ 3 [アクション（Actions）] 列で、歯車アイコンをクリックし、ドロップダウンリストから新しい認証ポリシーを選択します
[ポリシーセット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 4 着信サービス名を入力します。

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性を選択します。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 7 [使用（Use）] をクリックして、読み取り専用モードで新しい標準許可ポリシーを作成します。

ステップ 8 [保存（Save）] をクリックします。

ポスチャとネットワーク ドライブ マッピングのベスト プラクティス

Windows エンドポイントのポスチャ アセスメント実行中に、エンドポイント ユーザーがデスクトップへのアクセスするときに遅延が生じることがあります。これは、Windows でユーザーがデスクトップにアクセスできるようにする前に、ファイル サーバーのドライブ文字のマッピングを復元しようとすることが原因で発生する場合があります。ポスチャ実行中の遅延を防ぐためのベスト プラクティスを次に示します。

- ファイル サーバー ドライブ文字をマッピングするときには AD にアクセスする必要があるため、エンドポイントは Active Directory サーバーにアクセスできる必要があります。（ISE ポスチャエージェントを使用した）ポスチャがトリガーされると、AD へのアクセスがブロックされ、これが原因でログインが遅延します。ポスチャが完了する前に、ポスチャ修復 ACL を使用して AD サーバーへのアクセスを提供します。
- ポスチャ完了までのログイン スクリプトの遅延を設定し、その後 Persistence 属性を NO に設定する必要があります。Windows はログイン中にすべてのネットワークドライブへの再接続を試行しますが、ISE ポスチャエージェントが完全なネットワークアクセスを得るまでは、この操作を完了できません。

エージェントステルスモードのワークフローの設定

ステルスモードでのエージェントの設定プロセスには、一連の手順があります。Cisco ISE で次の手順を実行する必要があります。

ステップ 1 エージェントプロファイルを作成します。「エージェントプロファイルの作成」を参照してください。

ステップ 2 エージェントパッケージのエージェント設定を作成します。「エージェントパッケージのエージェント設定の作成」を参照してください。

ステップ 3 Cisco ISE でオープン DNS プロファイルをアップロードします。「Cisco ISE へのオープン DNS プロファイルのアップロード」を参照してください。

ステップ 4 クライアント プロビジョニング ポリシーを作成します。「クライアント プロビジョニング ポリシーの作成」を参照してください。

ステップ 5 ポスチャ条件を作成します。「ポスチャ条件の作成」を参照してください。

ステップ 6 ポスチャ修復を作成します。「ポスチャ修復の作成」を参照してください。

ステップ 7 クライアントレス モードでポスチャ要件を作成します。「ステルス モードでのポスチャ要件の作成」を参照してください。

ステップ 8 ポスチャ ポリシーを作成します。「ポスチャ ポリシーの作成」を参照してください。

ステップ 9 認証プロファイルを設定します。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]** を選択します。

b) [追加（Add）] をクリックして、プロファイルの [名前（Name）] に入力します。

c) [共通タスク（Common Tasks）] で、[Web リダイレクション（CWA、MDM、NSP、CPP）（Web Redirection (CWA, MDM, NSP, CPP)）] を有効にし、ドロップダウンリストから [クライアント プロビジョニング（ポスチャ）（Client provisioning (Posture)）] を選択し、リダイレクト [ACL] の名前を入力して、[クライアント プロビジョニング ポータル（Client Provisioning Portal）] 値を選択します。新しいクライアント プロビジョニング ポータルは、**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [クライアント プロビジョニング（Client Provisioning）] > [クライアント プロビジョニング ポータル（Client Provisioning Portal）]** で編集または作成できます。

ステップ 10 許可ポリシーを設定します。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]** を選択します。

b) [>] をクリックして [認可ポリシー（Authorization Policy）] を選択し、[+] アイコンをクリックして **Session:Posture Status EQUALS Unknown** と以前に設定した認証プロファイルが備わっている新しいルールを作成します。

c) 以前のルールの上に、**Session:Posture Status EQUALS NonCompliant** 条件を備えた新しい認証ルールと、**Session:Posture Status EQUALS Compliant** 条件を備えた別の新しい認証ルールを作成します

エージェントプロファイルの作成

始める前に

Mac および Windows OS 用の エージェントパッケージおよび準拠モジュールをアップロードする必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]**。

ステップ 2 [追加（Add）] ドロップダウンリストから、**[エージェントポスチャプロファイル（Agent Posture Profile）]** を選択します。

ステップ 3 [ポスチャエージェントプロファイルの設定（Posture Agent Profile Settings）] ドロップダウンリストから **[エージェント（Agent）]** を選択します。

ステップ 4 [名前（Name）] フィールドに、目的の名前（たとえば、AC_Agent_Profile）を入力します。

ステップ 5 [エージェントの動作（Agent Behavior）] セクションでは、[ステルスモード（Stealth Mode）] パラメータで **[有効（Enabled）]** を選択します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

エージェントパッケージのエージェント設定を作成する必要があります。

エージェントパッケージのエージェント 設定の作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]**。

ステップ 2 [追加（Add）] ドロップダウンリストから、**[エージェントの設定（Agent Configuration）]** を選択します。

ステップ 3 **[エージェントパッケージの選択（Select Agent Package）]** ドロップダウンリストから、必要なエージェントパッケージを選択します。

ステップ 4 [設定名（Configuration Name）] テキストボックスに、必要な名前を入力します。

ステップ 5 [コンプライアンスモジュール（Compliance Module）] ドロップダウンリストで、必要なコンプライアンスモジュールを選択します。

ステップ 6 **[エージェントモジュール選択（Agent Module Selection）]** セクションで、[ISEポスチャ（ISE Posture）] と [ネットワークアクセスマネージャ（Network Access Manager）] チェックボックスをオンにします。

ステップ 7 [プロファイル選択（Profile Selection）] セクションの [ISEポスチャ（ISE Posture）] ドロップダウンリストで、エージェントプロファイルを選択します。

ステップ 8 [ネットワークアクセスマネージャ（Network Access Manager）] ドロップダウンリストから、必要なエージェントプロファイルを選択します。

次のタスク

クライアントにプッシュされるオープン DNS プロファイルをアップロードする必要があります。

Cisco ISE へのオープン DNS プロファイルのアップロード

オープン DNS プロファイルがクライアントにプッシュされます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]**。

ステップ 2 [追加（Add）] ドロップダウン リストから、[ローカルディスクのエージェント リソース（Agent Resources From Local Disk）] を選択します。

ステップ 3 [カテゴリ（Category）] ドロップダウン リストから [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 4 [タイプ（Type）] ドロップダウンリストから、**[エージェントプロファイル（Agent Profile）]** を選択します。

ステップ 5 [名前（Name）] テキスト ボックスに、目的の名前（たとえば、OpenDNS）を入力します。
ステップ 6 [参照（Browse）] をクリックして、ローカル ディスクから JSON ファイルを見つけます。
ステップ 7 [送信（Submit）] をクリックします。

次のタスク

クライアント プロビジョニング ポリシーを作成する必要があります。

クライアント プロビジョニング ポリシーの作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]**。
ステップ 2 必要なルールを作成します（たとえば、Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。

次のタスク

ポスチャ条件を作成する必要があります。

ポスチャ条件の作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[ファイル条件（File Condition）]**。
ステップ 2 必要な名前を入力します（filechk など）。
ステップ 3 [オペレーティング システム（Operating Systems）] ドロップダウン リストから、[Windows 7（すべて）（Windows 7 (All)）] を選択します。
ステップ 4 [ファイル タイプ（File Type）] ドロップダウン リストから、[FileExistence] を選択します。
ステップ 5 [ファイル パス（File Path）] ドロップダウン リストから、[ABSOLUTE_PATH C:\test.txt] を選択します。
ステップ 6 [ファイル演算子（File Operator）] ドロップダウン リストから、[DoesNotExist] を選択します。

次のタスク

ポスチャ修復を作成する必要があります。

ポスチャ修復の作成

ファイル条件により、test.txt ファイルがエンドポイントに存在するかどうかが確認されます。存在しない場合の修復は、USB ポートをブロックし、USB デバイスを使用したファイルのインストールを防止することです。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[修復アクション（Remediation Actions）]** > **[USB 修復（USB Remediations）]**。

ステップ 2 必要な名前を入力します（clientless_mode_block など）。

ステップ 3 [送信（Submit）] をクリックします。

次のタスク

ポスチャ要件を作成する必要があります。

ステルス モードでのポスチャ要件の作成

[要件（Requirements）] ページから修復アクションを作成する際は、ステルス モードに適した次の修復だけが表示されます：[マルウェア対策（Anti-Malware）]、[プログラム起動（Launch Program）]、[パッチ管理（Patch Management）]、[USB]、[Windows Server Update Services]、および [Windows Update]。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]**。

ステップ 2 ポスチャの必須要件を作成します（たとえば、Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=Agent Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block）。

次のタスク

ポスチャ ポリシーを作成する必要があります。

ポスチャ ポリシーの作成

始める前に

ポスチャ ポリシーの要件およびポリシーがクライアントレス モードで作成されていることを確認してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポスチャ（Posture）]**

ステップ 2 必要なルールを作成します。たとえば、if Identity Groups=Any and Operating Systems=Windows 7(All) and Compliance Module=4.x or later and Posture Type=Agent Stealth then Requirements=win7Req です。

（注） URL リダイレクションのないクライアント プロビジョニングの場合、ネットワーク アクセスまたは RADIUS に固有の属性を使用して条件を設定しても条件は機能せず、Cisco ISE サーバーで特定ユーザーのセッション情報が使用可能ではないことが原因で、クライアント プロビジョニング ポリシーの照合が失敗することがあります。ただし、Cisco ISE では外部で追加された ID グループに対して条件を設定できます。

エージェントステルスモード通知の有効化

Cisco ISE ではエージェントステルスモード展開に対し、いくつかの新しい障害の発生通知を提供します。ステルス モードでの障害の発生通知を有効にすると、有線、ワイヤレスまたは VPN 接続で問題を特定できます。ステルス モードでの通知を有効にするには、次のようにします。

（注） AnyConnect バージョン 4.5.0.3040 以降は、ステルスモードでの通知をサポートします。

始める前に

ステルスモードでエージェントを設定します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] を選択します。

ステップ 2 **[追加（Add）]** > **[エージェントポスチャプロファイル（Agent Posture Profile）]** を選択します。

ステップ 3 [カテゴリの選択（Select a Category）] ドロップダウンリストから **[エージェント（Agent）]** を選択します。

ステップ 4 [エージェントの動作（Agent Behavior）] セクションで、[ステルスモードで通知を有効にする（Enable notifications in stealth mode）] オプションに [有効（Enabled）] を選択します。

Cisco Temporal Agent のワークフローの設定

Cisco temporal agent を設定するプロセスには、一連の手順があります。Cisco ISE で次の手順を実行する必要があります。

ステップ 1 ポスチャ条件の作成

ステップ 2 ポスチャ要件の作成

ステップ 3 ポスチャ ポリシーの作成

ステップ 4 クライアント プロビジョニング ポリシーの設定

ステップ 5 認証プロファイルを設定します。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）]**。

b) [追加（Add）] をクリックして、プロファイルの [名前（Name）] に入力します。

c) [共通タスク（Common Tasks）] で、[Web リダイレクション（CWA、MDM、NSP、CPP）（Web Redirection (CWA, MDM, NSP, CPP)）] を有効にし、ドロップダウンリストから [クライアント プロビジョニング（ポスチャ）（Client provisioning (Posture)）] を選択し、リダイレクト [ACL] の名前を入力して、[クライアント プロビジョニング ポータル（Client Provisioning Portal）] 値を選択します。新しいクライアント プロビジョニング ポータルは、**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [クライアント プロビジョニング（Client Provisioning）] > [クライアント プロビジョニング ポータル（Client Provisioning Portal）]** で編集または作成できます。

ステップ 6 許可ポリシーを設定します。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]**。

b) [>] をクリックして [認可ポリシー（Authorization Policy）] を選択し、[+] アイコンをクリックして **Session:Posture Status EQUALS Unknown** と以前に設定した認証プロファイルが備わっている新しいルールを作成します。

c) 以前のルールの上に、**Session:Posture Status EQUALS NonCompliant** 条件を備えた新しい認証ルールと、**Session:Posture Status EQUALS Compliant** 条件を備えた別の新しい認証ルールを作成します

ステップ 7 Cisco Temporal Agent のダウンロードと起動

ポスチャ条件の作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ファイル条件（File Condition）]**。

ステップ 2 必要な名前を入力します（filecondwin など）。

ステップ 3 [オペレーティング システム（Operating Systems）] ドロップダウン リストから、[Windows 7（すべて）（Windows 7 (All)）] を選択します。

ステップ 4 [ファイル タイプ（File Type）] ドロップダウン リストから、[FileExistence] を選択します。

ステップ 5 [ファイル パス（File Path）] ドロップダウン リストから、[ABSOLUTE_PATH C:\test.txt] を選択します。

ステップ 6 [ファイル演算子（File Operator）] ドロップダウン リストから、[DoesNotExist] を選択します。

ポスチャ要件の作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]** > **[要件（Requirements）]**。

ステップ 2 [編集（Edit）] ドロップダウンリストから、[新しい要件の挿入（Insert New Requirement）] を選択します。

ステップ 3 [名前（Name）]、[オペレーティング システム（Operating Systems）]、および [コンプライアンス モジュール（Compliance Module）] を入力します（たとえば、Name filereqwin、Operating Systems Windows All、Compliance Module 4.x or later）。

ステップ 4 [ポスチャ タイプ（Posture Type）] ドロップダウンで、[一時エージェント（Temporal Agent）] を選択します。

ステップ 5 必要な条件（たとえば、filecondwin）を選択します。

（注） Cisco Temporal Agent の場合は、[要件（Requirements）] ページで [インストール（Installation）] チェック タイプを含むパッチ管理条件のみを表示できます。

ステップ 6 [メッセージ テキストのみ（Message Text Only）] 修復アクションを選択します。

（注） 一時エージェントは、AnyConnect 4.x 以降でサポートされています。

ポスチャ ポリシーの作成

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポスチャ（Posture）]**。

ステップ 2 必要なルールを作成します（たとえば、Name=filepolicywin、Identity Groups=Any、Operating Systems=Windows All、Compliance Module=4.x or later、Posture Type=Temporal Agent、および Requirements=filereqwin）。

クライアント プロビジョニング ポリシーの設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]**> **[クライアント プロビジョニング（Client Provisioning）]**。

ステップ 2 必要なルールを作成します（たとえば、Rule Name=Win、Identity Groups=Any、Operating Systems=Windows All、Other Conditions=Conditions、Results=CiscoTemporalAgentWindows4.5）。

Cisco Temporal Agent のダウンロードと起動

ステップ 1 SSID に接続します。

ステップ 2 ブラウザを起動すると、クライアント プロビジョニング ポータルにリダイレクトされます。

ステップ 3 [開始（Start）] をクリックします。これにより、Cisco Temporal Agent がインストールされ、動作しているかどうかがチェックされます。

ステップ 4 [ここに初めて来ました（This Is My First Time Here）] をクリックします。

ステップ 5 [Cisco Temporal Agent をダウンロードして起動するにはここをクリック（Click Here to Download and Launch Cisco Temporal Agent）] を選択します。

ステップ 6 Windows または MacOS 用の Cisco Temporal Agent .exe または .dmg ファイルをそれぞれ保存します。Windows の場合は .exe ファイルを実行し、MacOS の場合は .dmg ファイルをダブルクリックして、acisetempagent アプリケーションを実行します。
Cisco Temporal Agent はクライアントをスキャンし、結果（非準拠を示す赤い十字マークなど）を表示します。

ポスチャのトラブルシューティング ツール

[ポスチャのトラブルシューティング（Posture Troubleshooting）] ツールは、ポスチャ チェック エラーの原因を見つけ、次のことを識別するのに役立ちます。

- どのエンドポイントがポスチャに成功し、どのエンドポイントが成功しなかったか。
- エンドポイントがポスチャに失敗した場合、ポスチャ プロセスのどの手順が失敗したか。
- どの必須および任意のチェックが成功および失敗したか。

ユーザー名、MAC アドレス、ポスチャ ステータスなどのパラメータに基づいて要求をフィルタリングすることによって、この情報を特定します。

エンドポイント ログイン クレデンシャルの設定

[エンドポイントログイン設定（Endpoint Login Configuration）] ウィンドウでは、Cisco ISE がクライアントにログインできるようにログインクレデンシャルを設定します。このウィンドウで設定されたログインクレデンシャルは、次の Cisco ISE 機能で使用されます。

Cisco ISE の GUIで、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[エンドポイントスクリプト（Endpoint Scripts）]** > **[設定（Settings）]** を選択します。

次のタブが表示されます。

- [Windowsドメインユーザー（Windows Domain User）]：Cisco ISE が SSH 経由でクライアントにログインするために使用する必要があるドメインクレデンシャルを設定します。[+（Plus）] アイコンをクリックして、必要な数の Windows ログインを入力します。ドメインごとに、[ドメイン（Domain）]、[ユーザー名（Username）]、および [パスワード（Password）] の各フィールドに必要な値を入力します。ドメインクレデンシャルを設定すると、[Windowsローカルユーザー（Windows Local User）] タブで設定されたローカルユーザー クレデンシャルは無視されます。
- [Windowsローカルユーザー（Windows Local User）]：Cisco ISE が SSH 経由でクライアントにアクセスするために使用するローカルアカウントを設定します。このローカルアカウントで、PowerShell および PowerShell リモートを実行できる必要があります。
- [MACローカルユーザー（MAC Local User）]：Cisco ISE が SSH 経由でクライアントにアクセスするために使用するローカルアカウントを設定します。このローカルアカウントで、PowerShell および PowerShell リモートを実行できる必要があります。[ユーザー名（Username）] フィールドに、ローカルアカウントのアカウント名を入力します。Mac OS アカウント名を表示するには、ターミナルで次のコマンドを実行します。

  ```
  whoami
  ```

エンドポイントスクリプト設定

このページでは、エンドポイントスクリプトとエージェントレスポスチャのオプションを設定します。

- [ISEへのエンドポイントスクリプト実行ログのアップロード（Upload endpoint script execution logs to ISE）]：デフォルトで有効になっている場合、エンドポイントスクリプトを Cisco ISE にアップロードできます。これを無効にすると、エンドポイントスクリプトが無効になり、エンドポイントスクリプトをアップロードまたは実行できなくなります。
- [エンドポイントスクリプト実行の冗長ロギング（Endpoint script execution verbose logging）]：デバッグの冗長ロギングを有効にします。
- [エンドポイントプロセッサのバッチサイズ（Endpoints processor batch size）]：ネットワークの負荷とシステムのパフォーマンスに対応するように調整できます。

- **MAC の同時エンドポイント処理**
- **Windows の同時エンドポイント処理**
- **OS 識別の最大再試行回数**
- **OS 識別の再試行間の遅延（ミリ秒）**
- **エンドポイントページネーションのバッチサイズ**
- **エンドポイントのログ保持期間（日）**
- **接続タイムアウト（秒）**
- **接続の最大再試行回数**
- [Powershell接続のポート番号（Port Number for Powershell）]：非標準のポート番号を使用するには。これを変更します。
- [SSH接続のポート番号（Port Number for SSH Connection）]：非標準のポート番号を使用するには、これを変更します。

Cisco ISE でのクライアント プロビジョニングの設定

クライアント プロビジョニングを有効にして、ユーザーがクライアント プロビジョニング リソースをダウンロードし、エージェント プロファイルを設定できるようにします。Linux クライアント、 Windows クライアント、Mac OS X クライアント、および Linux クライアント、とパーソナルデバイスのネイティブ サプリカント プロファイルのエージェントプロファイルを設定できます。クライアントプロビジョニングを無効にすると、ネットワークにアクセスしようとするユーザーには、クライアント プロビジョニング リソースをダウンロードできないことを示す警告メッセージが表示されます。

始める前に

プロキシを使用していて、クライアント プロビジョニング リソースをリモートシステムでホストしている場合は、プロキシがクライアントにそのリモートの場所へのアクセスを許可していることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアント プロビジョニング（Client Provisioning）]**または **[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアの更新（Software Updates）] > [クライアント プロビジョニング（Client Provisioning）]**。

ステップ 2 [プロビジョニングの有効化（Enable Provisioning）] ドロップダウンリストから、[有効（Enable）] または [無効（Disable）] を選択します。

ステップ 3 [自動ダウンロードの有効化（Enable Automatic Download）] ドロップダウンリストから、[有効（Enable）] を選択します。

フィードのダウンロードには、使用可能なすべてのクライアント プロビジョニング リソースが含まれます。これらのリソースの一部は、展開に関係していない場合があります。シスコでは、このオプションを設定する代わりに可能な限りリソースを手動でダウンロードすることを推奨します。

ステップ 4 [フィードURLの更新（Update Feed URL）]テキストボックスに、Cisco ISEで検索するシステムアップデートのURLを指定します。たとえば、クライアント プロビジョニング リソースをダウンロードするためのデフォルト URL は https://www.cisco.com/web/secure/spa/provisioning-update.xml. です。

ステップ 5 デバイスのクライアントプロビジョニング リソースがない場合は、次のいずれかのオプションを選択します。

- [ネットワークアクセスの許可（Allow Network Access）]：ユーザーは、ネイティブ サプリカント ウィザードをインストールおよび起動せずに、デバイスをネットワークに登録することを許可されます。
- [定義済みの認証ポリシーの適用（Apply Defined Authorization Policy）]：ユーザーは、標準認証および（ネイティブ サプリカント プロビジョニング プロセスではない）認証ポリシーを適用して Cisco ISE ネットワークへのアクセスを試みる必要があります。このオプションを有効にすると、ユーザー デバイスに対して、ユーザーの ID に適用されたすべてのクライアント プロビジョニング ポリシーに従った標準登録が行われます。ユーザーのデバイスがCisco ISEネットワークにアクセスするための証明書を必要とする場合、ユーザーに表示されるカスタマイズ可能なテキストフィールドを使用して、有効な証明書を取得し、適用する方法を説明する詳細指示をユーザーに提供する必要があります。

ステップ 6 [保存（Save）]をクリックします。

（注） ISE 証明書がエンドポイントの HTTP Strict Transport Security（HSTS）ストアにキャッシュされている場合、クライアントプロビジョニング ポータル リダイレクションが失敗し、次のエラーメッセージが表示されることがあります。

```
Web サイトで HSTS が使用されているため、現在 hostname.domain.com にアクセスできません。ネットワークエラーと攻撃は一時的なものであるため、このページは後で機能する可能性があります。
```

この問題を解決するには、エンドポイントのブラウザのキャッシュを削除するか、chrome://net-internals/#hsts に移動して自己署名 ISE 証明書を削除します。

次のタスク

クライアント プロビジョニング リソース ポリシーを設定します。

クライアント プロビジョニン リソース

クライアント プロビジョニング リソースは、エンドポイントがネットワークに接続した後にエンドポイントにダウンロードされます。クライアント プロビジョニング リソースは、デスクトップの場合はコンプライアンスとポスチャ エージェントで構成され、電話およびタブレットの場合はネイティブ サプリカント プロファイルで構成されます。クライアント プロビジョ

ニング ポリシーによって、これらのプロビジョニング リソースがエンドポイントに割り当てられ、ネットワーク セッションが開始します。

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]**。次のリソース タイプは、[追加（Add）] ボタンをクリックすることでリストに追加できます。

- **[Ciscoサイトのエージェントリソース（Agent resources from Cisco Site）]**：クライアント プロビジョニング ポリシーで使用できるようにするエージェントおよび [サプリカントプロビジョニング（Supplicant Provisioning）] ウィザードを選択します。シスコは、新しいリソースを追加したり既存のリソースを更新することで、定期的にこのリソースのリストを更新します。すべてのシスコのリソースおよびリソースの更新を自動的にダウンロードするように ISE を設定することもできます。詳細については、Cisco ISE でのクライアント プロビジョニングの設定 （1791 ページ） を参照してください。
- **[ローカルディスクのエージェントリソース（Agent resources from local disk）]**：ISE にアップロードする PC 上のリソースを選択します。ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加 （1795 ページ） を参照してください。
- **[エージェント設定（Agent Configuration）]**：クライアント プロビジョニングで使用できるようにするエージェントクライアントを選択します。詳細については、「エージェント設定の作成」を参照してください。
- **[ネイティブ サプリカント プロファイル（Native Supplicant Profile）]**：ネットワークの設定が含まれている電話とタブレット用のサプリカントプロファイルを設定します。詳細については、「ネイティブ サプリカント プロファイルの作成」を参照してください。
- **[エージェントポスチャプロファイル（Agent Posture Profile）]**：エージェント XML プロファイルを作成および配布しない場合は、エージェント ISE ポスチャを設定します。。

クライアント プロビジョニング リソースを作成した後、エンドポイントにクライアント プロビジョニング リソースを適用するクライアントプロビジョニング ポリシーを作成します。「クライアントプロビジョニング リソース ポリシーの設定（1832ページ）」を参照してください。

関連トピック

Cisco ISE でのクライアント プロビジョニングの設定 （1791 ページ）
シスコからのクライアント プロビジョニング リソースの追加 （1793 ページ）
ローカルマシンからのシスコ提供のクライアントプロビジョニング リソースの追加 （1795 ページ）
ローカルマシンからのエージェント用の顧客作成リソースの追加 （1796 ページ）

シスコからのクライアント プロビジョニング リソースの追加

Cisco Web エージェント、エージェント Windows、MacOS、および Linux クライアントの場合は、Cisco.com からクライアント プロビジョニング リソースを追加できます。選択したリソースおよび利用できるネットワーク帯域幅によっては、Cisco ISE にクライアント プロビジョニング リソースをダウンロードするのに数分かかることがあります。

始める前に

- Cisco ISE で正しいプロキシ設定が設定されていることを確認します。
- Cisco ISE でクライアント プロビジョニングを有効にします。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]**。

ステップ 2 **[追加（Add）]** > **[Cisco サイトのエージェント リソース（Agent resources from Cisco site）]** を選択します。

ステップ 3 [リモートリソースのダウンロード（Download Remote Resources）] ダイアログボックスで選択可能なリストから必要なクライアント プロビジョニング リソースを 1 つ以上選択します。

ステップ 4 [保存（Save）] をクリックします。

Linux エージェントをインストールする際は、次の点に注意してください。

- 自己署名証明書を使用している場合：
  - ISE 証明書を Linux エージェントにコピーするには、SSH エージェントを有効にする必要があります。
    - RHEL の場合
      1. Cisco ISE の GUI から証明書をエクスポートします。

注目 Red Hat Linux の場合、自己署名証明書の SAN フィールドに IP アドレスを追加する必要があります。

      2. <certificate>.pem を /etc/pki/ca-trust/source/anchors/ にコピーし、ファイルの名前を <certificate>.crt に変更します。
      3. コマンド **sudo update-ca-trust extract** を実行します。
      4. /etc/pki/tls/certs/ に移動します。
      5. コマンド **openssl x509 -in ca-bundle.crt -text -noout** を実行します。
    - Ubuntu の場合は、次の手順を実行します。
      1. Cisco ISE の GUI から証明書をエクスポートします。
      2. <certificate>.pem を /usr/local/share/ca-certificates/ に移動し、名前を <certificate>.crt に変更します。
      3. コマンド **sudo update-ca-certificates** を実行します。

CA 証明書が正しくインストールされているかどうかを確認するには、/etc/ssl/certs/ca-certificates.crt に移動し、このファイルに証明書あることを確認します。

（注） ISE 証明書が信頼できる CA によって発行されている場合、証明書のインポートは必要ありません。

- dot1x リダイレクトフローまたは非リダイレクトフローを開始します。
- RHEL を使用している場合は、yum がサブスクリプションマネージャで更新されていることを確認します。Ubuntu を使用している場合は、apt-get を更新します。

  Linux エージェントのシステム要件の詳細については、『Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.9』を参照してください。

次のタスク

Cisco ISE に正常にクライアント プロビジョニング リソースを追加したら、クライアント プロビジョニング リソース ポリシーの設定を開始します。

ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加

シスコから以前にダウンロードしたクライアント プロビジョニング リソースをローカルディスクから追加できます。

始める前に

Cisco ISE には、必ず現行のサポートされているリソースのみをアップロードしてください。サポートされていない古いリソースでは、クライアントアクセスに重大な問題が発生する可能性があります。

Cisco.com からリソースファイルを手動でダウンロードする場合は、「Cisco ISE Release Notes」の「Cisco ISE Offline Updates」の項を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）]** > **[ローカルディスクのエージェントリソース（Agent resources from local disk）]** を選択します。

ステップ 3 [カテゴリ（Category）] ドロップダウンから [シスコ提供パッケージ（Cisco Provided Packages）] を選択します。

ステップ 4 [参照（Browse）] をクリックし、Cisco ISE にダウンロードするリソース ファイルがあるローカル マシン上のディレクトリに移動します。

以前に Cisco からローカルマシンにダウンロードしたエージェントまたは Cisco Web Agent のリソースを追加できます。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

Cisco ISE に正常にクライアント プロビジョニング リソースを追加したら、クライアント プロビジョニング リソース ポリシーの設定できます。

ローカルマシンからのエージェント用の顧客作成リソースの追加

エージェントカスタマイゼーションおよびローカリゼーションパッケージ、エージェントプロファイルなどの顧客作成リソースをローカルマシンから Cisco ISE に追加します。

始める前に

エージェントの顧客作成リソースがローカルディスクに zip 形式のファイルで使用可能であることを確認します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]**。

ステップ 2 [追加（Add）] > [ローカルディスクのエージェントリソース（Agent resources from local disk）] を選択します。

ステップ 3 [カテゴリ（Category）] ドロップダウンから [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 4 エージェントリソースの名前と説明を入力します。

ステップ 5 [参照（Browse）] をクリックし、Cisco ISE にダウンロードするリソース ファイルがあるローカル マシン上のディレクトリに移動します。

ステップ 6 Cisco ISE にアップロードする次のエージェントリソースを選択します。

- エージェントカスタマイゼーション バンドル
- エージェントローカリゼーションバンドル
- エージェントプロファイル
- 高度なマルウェア防御（AMP）イネーブラ プロファイル

ステップ 7 [送信（Submit）] をクリックします。

[アップロードされたエージェントリソース（Uploaded Agent Resources）] 表に、Cisco ISE に追加するエージェントリソースが表示されます。

次のタスク

エージェント設定の作成

ARM64バージョンのエージェントに対するクライアントプロビジョニング ポリシーの設定

Cisco ISE リリース 3.3 から、ポスチャポリシーとクライアント プロビジョニング ポリシーは ARM64 エンドポイントでサポートされます。ARM64 エンドポイント用の ARM64 バージョンのエージェントをアップロードできます。

ARM64 クライアント プロビジョニング ポリシーを設定する際は、次の点に注意してください。

- ARM64 ポスチャポリシーは、Windows エージェントでサポートされています。

  Windows ポリシーは、ARM64 アーキテクチャとインテルアーキテクチャで別のパッケージを実行します。Windows Temporal と Windows Agentless は、ARM64 アーキテクチャではサポートされていませんが、インテルアーキテクチャではサポートされています。

  macOS ポリシーは、両方のアーキテクチャで同じパッケージを実行します。

- ARM64 パッケージは、Cisco AnyConnect VPN および Cisco Secure Client でサポートされています。

（注） Cisco Secure Client 5.0.4xxx 以降のバージョンは、ARM64 エンドポイントのポスチャおよびクライアント プロビジョニング ポリシーをサポートしています。

ARM64 準拠モジュール 4.3.3583.8192 以降のバージョンは、Cisco Secure Client 5.0.4xxx 以降のバージョンと、ARM64 エンドポイント用の Cisco ISE 3.3 以降のバージョンで使用できます。コンプライアンスモジュールは、ソフトウェア ダウンロード センターからダウンロードできます。

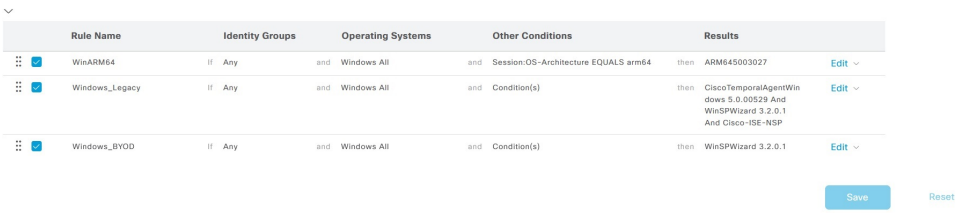
- ARM64エージェントの自動アップグレードとコンプライアンスモジュールのアップグレードがサポートされています。

- Google Chrome および Microsoft Edge 89 以降のバージョンでは、arm64、64 ビット、32 ビットなどの OS アーキテクチャ条件のクライアント プロビジョニング ポータルがサポートされています。

  Firefox ブラウザは、arm64、64 ビット、32 ビットなどの OS アーキテクチャ条件のクライアント プロビジョニング ポータルをサポートしていません。Firefox ブラウザを使用すると、次のメッセージが表示されます。

ARM64 エンドポイントは Firefox ブラウザをサポートしていないため、このエージェントのダウンロードを続行すると互換性の問題が発生する可能性があります。代わりに Chrome または Microsoft Edge ブラウザを使用することをお勧めします。

- BYOD と ARM64 クライアント プロビジョニング ポリシーを組み合わせることはできません。
- ARM64 条件ポリシーが条件リストの一番上にあることを確認します（ARM64 条件のないポリシーの上に表示されます）。これは、エンドポイントが [クライアント プロビジョニング ポリシー（Client Provisioning Policy）] ウィンドウに一覧表示されているポリシーと順を追って照合されるためです。



ARM64 クライアント プロビジョニング ポリシーを設定するには、次の手順を実行します。

ステップ 1 Cisco フィードサーバーからオフライン更新パッケージをダウンロードし、オフラインフィード更新を使用して Cisco ISE にアップロードできます。詳細については、「オフラインでのプロファイラ フィード サービスの設定 （1301 ページ）」を参照してください。

ステップ 2 ARM64 パッケージとコンプライアンスモジュールをアップロードします。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]。

b) **[追加（Add）] > [シスコサイトのエージェントリソース（Agent resources from Cisco site）]** を選択します。

c) [リモートリソースのダウンロード（Download Remote Resources）] ダイアログボックスのリストから、必要な ARM64 パッケージとコンプライアンスモジュールを選択します。

d) [保存（Save）]をクリックします。

ステップ 3 ARM64 エージェントパッケージを設定します。

a) **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

b) **[追加（Add）] > [エージェント設定（Agent Configuration）]** の順に選択します。

c) [エージェントパッケージの選択（Select Agent Package）] ドロップダウンリストから、ARM64 エージェントパッケージを選択します。

d) [コンプライアンスモジュール（Compliance Module）] ドロップダウンリストから、ARM64 コンプライアンス モジュール パッケージを選択します。

ステップ 4 ARM64 クライアント プロビジョニング ポリシーを設定します。

a) **[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]** を選択します。

b) 次の手順を実行します。

1. [オペレーティングシステム（Operating System）] 列で、[すべてのウィンドウ（Windows All）] を選択します。
2. [その他の条件（Other Conditions）] 列で、**Session:OS-Architecture Equalsarm64** または **cisco-av-pair Equals mdm-tlv=device-platform=win-arm64** を選択します。
3. [結果（Results）] 列で、[エージェント設定ARM（Agent Configuration-ARM）] を選択します。
4. [保存（Save）]をクリックします。

（注）

- ISE 証明書が ARM64 エンドポイントの HTTP Strict Transport Security（HSTS）ストアにキャッシュされている場合、クライアント プロビジョニング ポータル リダイレクションが失敗し、次のエラーメッセージが表示されることがあります。

  `Web サイトで HSTS が使用されているため、現在 hostname.domain.com にアクセスできません。ネットワークエラーと攻撃は一時的なものであるため、このページは後で機能する可能性があります。`

  この問題を解決するには、エンドポイントのブラウザのキャッシュを削除するか、chrome://net-internals/#hsts に移動して自己署名 ISE 証明書を削除します。

- ARM64 バージョンは、USB 修復を除くすべてのタイプの修復をサポートしています。さまざまなタイプのポスチャ修復の詳細については、カスタムポスチャ修復アクション（1766ページ） を参照してください。

ネイティブ サプリカント プロファイルの作成

ネイティブ サプリカント プロファイルを作成して、ユーザーが独自のデバイスを Cisco ISE ネットワークに含めることができます。ユーザーがサインインすると、Cisco ISE は、ユーザーの承認要件に関連付けられたプロファイルを使用して、必要なサプリカント プロビジョニング ウィザードを選択します。ウィザードは、ユーザーのパーソナルデバイスを起動して設定し、ネットワークにアクセスします。

（注） プロビジョニング ウィザードは、アクティブなインターフェイスのみを設定します。このため、有線接続ユーザーと無線接続ユーザーは、どちらもアクティブになっている場合を除き、両方のインターフェイスにはプロビジョニングされません。

始める前に

- TCP ポート 8905 を開き、Cisco Agent、Cisco Web Agent、およびサプリカント プロビジョニング ウィザードのインストールを有効にします。ポートの使用法の詳細については、

『Cisco Identity Services Engine Hardware Installation Guide』の付録「Cisco ISE Appliance Ports Reference」を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]**。

ステップ 2 **[追加（Add）] > [ネイティブ サプリカント プロファイル（Native Supplicant Profile）]** を選択します。

ステップ 3 ネイティブ サプリカント プロファイルの設定（1800 ページ）で説明されている手順を使用して、プロファイルを作成します。

次のタスク

「複数ゲスト ポータルのサポート」の項の説明に従って、従業員が自分のパーソナル デバイスをネットワークに直接接続できるようにセルフ プロビジョニング機能を有効にします。

ネイティブ サプリカント プロファイルの設定

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）] > [ネイティブサプリカントプロファイル（Native Supplicant Profile）]**。以下の設定が表示されます。

- [名前（Name）]：作成するネイティブ サプリカント プロファイルの名前を入力します。
- [オペレーティングシステム（Operating System）]：このプロファイルを適用するオペレーティングシステムをドロップダウンリストから選択します。

各プロファイルでは、Cisco ISE がクライアントのネイティブサプリカントに適用するネットワーク接続の設定を定義します。

ワイヤレスプロファイル

クライアントで使用可能にする SSID ごとにワイヤレスプロファイルを 1 つ設定します。

- [SSID 名（SSID Name）]：クライアントが接続する SSID の名前。
- [プロキシ自動コンフィギュレーション ファイルの URL（Proxy Auto-Config File URL）]：サプリカントのネットワーク設定を取得するためにクライアントがプロキシに接続する場合は、そのプロキシサーバーの URL を入力します。
- [プロキシホスト/IP（Proxy Host/IP）]：サプリカントのネットワーク設定を取得するためにクライアントがプロキシに接続する場合は、そのプロキシサーバーのホスト/IP を入力します。
- [プロキシポート（Proxy Port）]：サプリカントのネットワーク設定を取得するためにクライアントがプロキシに接続する場合は、そのプロキシサーバーのポートを入力します。

- [セキュリティ（Security）]：[WPA] または [WPA2] を選択します。
- [許可されたプロトコル（Allowed Procotol）]：[PEAP] または [EAP-TLS] を選択します。
- [証明書テンプレート（Certificate Template）]：TLS の場合は、いずれかの証明書テンプレートを選択します。証明書テンプレートは、**[管理（Administration）]** > **[システム証明書（System Certificates）]** > **[認証局（Certificate Authority）]** > **[証明書テンプレート（Certificate Templates）]** で定義されています。

オプションの設定

[オプション（Optional）] を展開すると、次のフィールドが表示されます。

Windows の設定

- [認証モード（Authentication Mode）]：認証のためのログイン情報として、[ユーザー（User）]、[マシン（Machine）]、または両方を選択します。
- [新規サーバーまたは信頼された証明機関の承認をユーザーに求めない（Do not prompt user to authorize new servers or trusted certification authorities）]：このオプションを有効にすると、ユーザーは承認を求められません。ユーザー証明書は自動的に受け入れられます。
- [接続に別のユーザー名を使用（Use a different user name for the connection）]：ワイヤレスプロファイルにのみ適用されます。接続に別のユーザー名を使用します。
- [ネットワークが名前（SSID）をブロードキャストしていなくても接続する（Connect even if the network is not broadcasting its name (SSID)）]：ワイヤレスプロファイルにのみ適用されます。SSID がブロードキャストされていない場合でも、ネットワークに接続します。

iOS 設定

- [ターゲットネットワークが非表示になっている場合は有効にする（Enable if target network is hidden）]：ターゲットネットワークが非表示になっている場合は、このチェックボックスをオンにします。

Android の設定

- [証明書登録プロトコル（Certificate Enrollment Protocol）]：いすれかのオプションボタンをクリックして、証明書登録プロトコル（[Enrollment over Secure Transport（EST）] または [Simple Certificate Enrollment Protocol（SCEP）]）を選択します。ESTプロトコルを選択した場合、Cisco ISEは、証明書の発行時にAndroidユーザーに対して追加のパスワードの入力を要求します。

有線プロファイル

- [許可されたプロトコル（Allowed Procotol）]：[PEAP] または [EAP-TLS] を選択します。
- [証明書テンプレート（Certificate Template）]：TLS の場合は、いずれかの証明書テンプレートを選択します。証明書テンプレートは、**[管理（Administration）]** > **[システム証明**

書（**System Certificates**）] > **[認証局（Certificate Authority**）] > **[証明書テンプレート（Certificate Templates**）] で定義されています。

オプションの設定

[オプション（Optional）] を展開すると、Windows クライアントの場合は次のフィールドも使用できます。

- [認証モード（Authentication Mode）]：認証のためのログイン情報として、[ユーザー（User）]、[マシン（Machine）]、または両方を選択します。
- [自動的にログイン名とパスワード（およびもしあればドメイン）を使用する（Automatically use logon name and password (and domain if any)）]：[認証モード（Authentication Mode）] で [ユーザー（User）] を選択すると、ユーザーにプロンプトを表示することなくログインおよびパスワード情報が使用されます（これらの情報が使用可能な場合）。
- [高速再接続を有効にする（Enable Fast Reconnect）]：セッションの再開機能が PEAP プロトコルオプションで有効になっている場合（これは、**[管理（Administration**）] > **[システム（System**）] > **[設定（Settings**）] > **[プロトコル（Protocols**）] > **[PEAP]** で設定）、PEAP セッションはユーザークレデンシャルをチェックすることなく再開できます。
- [隔離チェックを有効にする（Enable Quarantine Checks）]：クライアントが隔離されたかどうかを確認します。
- [サーバーが暗号化バインドTLVを示さない場合に切断する（Disconnect if server does not present cryptobinding TLV）]：暗号化バインド TLV がネットワーク接続でサポートされていない場合に切断します。
- [新規サーバーまたは信頼できる証明機関の承認をユーザーに求めない（Do not prompt user to authorize new servers or trusted certification authorities）]：自動的にユーザー証明書を受け入れ、ユーザーにプロンプトを表示しません。

各種ネットワークでの URL リダイレクトなしでのクライアント プロビジョニング

URL リダイレクトなしのクライアント プロビジョニングは、サードパーティの NAC で CoA がサポートされていない場合に必要です。クライアント プロビジョニングは、URL リダイレクトの有無にかかわらず実行できます。

（注） URL リダイレクションを使用するクライアント プロビジョニングの場合、クライアント マシンにプロキシ設定が構成されている場合は、ブラウザ設定の例外リストに Cisco ISE を追加してください。この設定は、URL リダイレクションを使用するすべてのフロー、BYOD、MDM、ゲスト、およびポスチャに適用されます。たとえば、Windows マシンでは、次の手順を実行します。

1. コントロール パネルから、[インターネットプロパティ（Internet Properties）] をクリックします。
2. [接続（Connections）] タブを選択します。
3. [LAN設定（LAN settings）] をクリックします。
4. [プロキシサーバー（Proxy server）] 領域から、[詳細設定（Advanced）] をクリックします。
5. [例外（Exceptions）] ボックスに Cisco ISE ノードの IP アドレスを入力します。
6. [OK] をクリックします。

各種ネットワークでリダイレクトなしでエンドポイントをプロビジョニングする手順を次に示します。

Dot1X EAP-TLS

1. プロビジョニングされた認証を使用して Cisco ISE ネットワークに接続する。
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザー、AD、LDAP、または SAML を介して CP ポータルにログインする。

   エージェントがポスチャを実行します。エンドポイントがポスチャ コンプライアンスに基づいて正しいネットワークに移動する。

Dot1X PEAP

1. NSP 経由でユーザー名とパスワードを使用して Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザー、AD、LDAP、または SAML を介して CP ポータルにログインする

   エージェントがポスチャを実行します。エンドポイントがポスチャ コンプライアンスに基づいて正しいネットワークに移動する。

MAB（有線ネットワーク）

1. Cisco ISE ネットワークに接続する。
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザー、AD、LDAP、または SAML を介して CP ポータルにログインする。

エージェントがポスチャを実行します。エンドポイントがポスチャ コンプライアンスに基づいて正しいネットワークに移動する。

MAB（ワイヤレス ネットワーク）

1. Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザー、AD、LDAP、または SAML を介して CP ポータルにログインする。

   エージェントがポスチャを実行します。ポスチャはワイヤレス 802.1X の場合にのみ開始する。

AMP イネーブラ プロファイルの設定

次の表に、[Cisco Advanced Malware Protection（AMP）イネーブラプロファイル（Advanced Malware Protection (AMP) Enabler Profile）] ウィンドウのフィールドを示します。Cisco ISE GUI で[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** です。

[追加（Add）] ドロップダウン矢印をクリックし、[AMPイネーブラプロファイル（AMP Enabler Profile）] を選択します。

表 *170 : [AMPイネーブラプロファイル（AMP Enabler Profile）]* ページ

フィールド名	使用上のガイドライン
名前（Name）	ユーザーが作成する AMP イネーブラ プロファイルの名前を入力します。
説明（Description）	AMP イネーブラ プロファイルの説明を入力します。
AMPイネーブラのインストール（Install AMP Enabler）	• [Windows インストーラ（Windows Installer）]：Windows OS ソフトウェアの AMP をホストするローカルサーバーの URL を指定します。エージェントモジュールはこの URL を使用して、エンドポイントに .exe ファイルをダウンロードします。ファイル サイズは約 25 MB です。 • [Macインストーラ（Mac Installer）]：MacOS ソフトウェアの AMP をホストするローカルサーバーの URL を指定します。エージェントモジュールはこの URL を使用して、エンドポイントに .pkg ファイルをダウンロードします。ファイル サイズは約 6 MB です。 [オン（Check）] ボタンは、サーバーと通信を行って URL が有効かどうかを確認します。URL が有効の場合は、「ファイルが見つかりました（File found）」メッセージが表示され、有効でない場合はエラー メッセージが表示されます。

フィールド名	使用上のガイドライン
AMPイネーブラのアンインストール（Uninstall AMP Enabler）	エンドポイントからエンドポイント ソフトウェアの AMP をアンインストールします。
開始メニューへの追加（Add to Start Menu）	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントの [開始（Start）] メニューにエンドポイント ソフトウェアの AMP のショートカットを追加します。
デスクトップへの追加（Add to Desktop）	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントのデスクトップにエンドポイント ソフトウェアの AMP のショートカットを追加します。
コンテキストメニューへの追加（Add to Context Menu）	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントの右クリック コンテキスト メニューに [今すぐスキャン（Scan Now）] オプションを追加します。

組み込みプロファイル エディタを使用した AMP イネーブラ プロファイルの作成

（注） AMP イネーブラは、AnyConnect を使用するクライアントにのみ適用できます。Cisco Secure Client には、代わりに Secure Endpoint が含まれています。Cisco Secure Client で Secure Endpoint を使用する方法については、『Cisco Secure Client Administrator Guide』を参照してください。

Cisco ISE 埋め込みプロファイルエディタまたはスタンドアロンエディタを使用して、AMP イネーブラプロファイルを作成できます。

Cisco ISE 埋め込みプロファイルエディタを使用して AMP 有効化プロファイルを作成するには、次の手順を実行します。

始める前に

- SOURCEfire ポータルからエンドポイント ソフトウェアの AMP をダウンロードし、ローカル サーバーでホスティングします。
- エンドポイントのソフトウェアの AMP をホストするサーバーの証明書を ISE 証明書ストアにインポートします。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**。

- [AMPイネーブラ（AMP Enabler）] オプションが **[エージェント設定（Agent Configuration）]** ウィンドウ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client provisioning）] > [リソース（Resources）] > [追加（Add）] > **[エージェント設定（Agent Configuration）]** > **[エージェントパッケージの選択（Select Agent Package）]**）の **[エージェントモジュールの選択（Agent Module Selection）]** および [プロファイルの選択（Profile Selection）] セクションで選択されていることを確認します。
- SOURCEfire ポータルにログインして、エンドポイント グループのポリシーを作成し、エンドポイント ソフトウェアの AMP をダウンロードする必要があります。ソフトウェアには、選択したポリシーが事前設定されています。2 つのイメージ、すなわち Windows OS の場合はエンドポイントソフトウェアの AMP、MacOS の場合はエンドポイントソフトウェアの AMP の再配布可能なバージョンをダウンロードする必要があります。ダウンロードされたソフトウェアは、エンタープライズネットワークからアクセスできるサーバーでホストされます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client Provision）]** > **[リソース（Resources）]** の順に選択します。

ステップ 2 [追加（Add）] ドロップダウンをクリックします。

ステップ 3 [AMPイネーブラプロファイル（AMP Enabler Profile）] を選択して、新しい AMP イネーブラ プロファイルを作成します。

ステップ 4 フィールドに適切な値を入力します。

スタンドアロン エディタを使用した AMP イネーブラ プロファイルの作成

エージェントスタンドアロンエディタを使用して、AMP イネーブラプロファイルを作成するには、次の手順を実行します。

始める前に

AnyConnect 4.1 スタンドアロン エディタを使用して、XML 形式のプロファイルをアップロードして AMP イネーブラ プロファイルを作成できます。

- Cisco.com から Windows および Mac OS のエージェント スタンドアロン プロファイル エディタをダウンロードします。
- スタンドアロン プロファイル エディタを起動し、[AMPイネーブラプロファイルの設定（AMP Enabler Profile Settings）]AMP イネーブラ プロファイルの設定 （1804 ページ） で指定されているようにフィールドに入力します。
- プロファイルを XML ファイルとしてローカル ディスクに保存します。

- [AMPイネーブラ（AMP Enabler）]オプションが**[エージェント設定（Agent Configuration）]**ウィンドウ（[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[結果（Results）]>[クライアントプロビジョニング（Client provisioning）]>[リソース（Resources）]>[追加（Add）]>**[エージェント設定（Agent Configuration）]**>**[エージェントパッケージの選択（Select Agent Package）]**）の**[エージェントモジュールの選択（Agent Module Selection）]**および[プロファイルの選択（Profile Selection）]セクションで選択されていることを確認します。

ステップ 1 Cisco ISE GUIで[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]**>**[結果（Results）]**>**[クライアント プロビジョニング（Client Provisioning）]**>**[リソース（Resources）]**。

ステップ 2 [追加（Add）]をクリックします。

ステップ 3 [ローカルディスクのエージェントリソース（Agent resources from local disk）]を選択します。

ステップ 4 [カテゴリ（Category）]ドロップダウンから[顧客作成のパッケージ（Customer Created Packages）]を選択します。

ステップ 5 [タイプ（Type）]ドロップダウンから[AMPイネーブラプロファイル（AMP Enabler Profile）]を選択します。

ステップ 6 [名前（Name）]と[説明（Description）]に入力します。

ステップ 7 [参照（Browse）]をクリックして、ローカル ディスクから保存済みプロファイル（XML ファイル）を選択します。次に、カスタマイズされたインストール ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Install>
 <WindowsConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</WindowsConnectorLocation>
 <MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
 <StartMenu>true</StartMenu>
 <DesktopIcon>false</DesktopIcon>
 <ContextIcon>true</ContextIcon>
 </Install>
 </FAConfiguration>
</FAProfile>
```

次に、カスタマイズされたアンインストール ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Uninstall>
 </Uninstall>
 </FAConfiguration>
</FAProfile>
```

ステップ 8 [送信（Submit）]をクリックします。

新しく作成された AMP イネーブラ プロファイルが [リソース（Resources）] ページに表示されます。

一般的な AMP イネーブラ インストール エラーのトラブルシューティング

[Windowsインストーラ（Windows Installer）] または [MACインストーラ（MAC Installer）] テキスト ボックスに SOURCEfire URL を入力して [オン（Check）] をクリックすると、次のエラーのいずれかが発生する場合があります。

- エラー メッセージ：「MacまたはWindowsのインストーラファイルを含むサーバーの証明書がISEによって信頼されていません。（The certificate for the server containing the Mac/Windows installer file is not trusted by ISE.）信頼証明書を [管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] に追加します。（Add a trust certificate to **Administration** > **Certificates** > **Trusted Certificates**.）」

  このエラー メッセージは、Cisco ISE 証明書ストアに SOURCEfire の信頼できる証明書をインポートしていない場合に表示されます。SOURCEfire の信頼できる証明書を入手し、Cisco ISE の信頼できる証明書ストア（[管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]）にインポートします。

- エラー メッセージ：「インストーラファイルがこの場所で見つかりません。接続の問題である可能性があります。（The installer file is not found at this location, this may be due to a connection issue.）有効なパスを [インストーラ（Installer）] テキスト ボックスに入力するか、または接続を確認します。（Enter a valid path in the Installer text box or check your connection.）」

  このエラー メッセージは、エンドポイント ソフトウェアの AMP をホストしているサーバーがダウンした場合、または [Windowsインストーラ（Windows Installer）] または [MACインストーラ（MAC Installer）] テキストボックスに入力ミスがある場合に表示されます。

- エラー メッセージ：「[Windowsインストーラ（Windows Installer）]または[MACインストーラ（MAC Installer）]テキスト ボックスに有効なURLが含まれていません。（The Windows/Mac installer text box does not contain a valid URL.）」

  このエラーメッセージは、構文的に正しくないURL形式を入力した場合に表示されます。

Cisco ISE の Chromebook デバイスのオンボーディングのサポート

Chromebookデバイスは他のデバイス（Apple、Windows、Android）とは異なり管理型デバイス（Google ドメインによって管理）で、オンボーディング サポートが制限されています。Cisco ISE はネットワークでの Chromebook デバイスのオンボーディングをサポートしています。オンボーディングとは、Cisco ISE による認証の後にネットワークに安全に接続できるように、

エンドポイントに必要な設定とファイルを配送するプロセスのことです。このプロセスには、証明書のプロビジョニングやネイティブサプリカントのプロビジョニングが含まれています。ただし、Chromebookデバイスでは、証明書のプロビジョニングのみが実行できます。ネイティブ サプリカントのプロビジョニングは、Google 管理コンソールで実行されます。

管理されていない Chromebook デバイスは、安全なネットワークへのオンボーディングができません。

Chromebook オンボーディング プロセスに関与するエンティティは次のとおりです。

- Google 管理者
- ISE 管理者
- Chromebook ユーザー/デバイス
- Google 管理コンソール（Google 管理者が管理）

Google 管理者：

- 次のライセンスの安全性を確保します。
  1. Google 管理コンソール設定のための Google Apps 管理者ライセンス。URL：https://admin.google.com。Google管理コンソールを使用して、管理者は組織内の人間のための Google サービスを管理できます。
  2. Chromebook のデバイス管理ライセンス。URL：https://support.google.com/chrome/a/answer/2717664?hl=en。Chromebook のデバイス管理ライセンスは、特定の Chromebook デバイスに対して設定を行い、ポリシーを適用するために使用されます。ユーザーアクセスの制御、機能のカスタマイズ、ネットワーク アクセスの設定などのためのデバイス設定への Google 管理者アクセス権を提供します。
- Googleデバイス ライセンスによるChromebookデバイスのプロビジョニングと登録を促進します。
- Google 管理コンソールを通じて Chromebook デバイスを管理します。
- 各 Chromebook ユーザーの Wi-Fi ネットワーク設定のセットアップと管理を行います。
- Chromebook デバイスでアプリケーションの設定と強制されている拡張機能のインストールを行い、Chromebookデバイスを管理します。Chromebookデバイスのオンボーディングには、Chromebook デバイスに Cisco Network Setup Assistant 拡張機能がインストールされている必要があります。これにより、Chromebook デバイスが Cisco ISE に接続し、ISE 証明書をインストールできるようになります。証明書のインストールの操作は管理対象デバイスにのみ許可されるため、この拡張機能は強制的にインストールされます。
- サーバーの検証と安全な接続を実現するために、Cisco ISE 証明書が Google 管理コンソールにインストールされていることを確認します。Google管理者が、証明書がデバイスに対して生成されるか、ユーザーに対して生成されるかを決定します。CiscoISEには次のオプションがあります。
  - Chromebook デバイスを共有しない単一のユーザー用に証明書を生成します。

- 複数のユーザーで共有される Chromebook デバイス用に証明書を生成します。必要な追加設定については、「Google 管理コンソールでのネットワークの設定と拡張機能の強制」セクションの手順 5 を参照してください。

ISE が Chromebook デバイスで証明書のプロビジョニングを実行するために信頼され、EAP-TLS 証明書ベースの認証が許可されるように、Google 管理者が ISE サーバー証明書をインストールします。Google Chrome バージョン 37 以降は、Chromebook デバイスの証明書ベースの認証をサポートしています。Google 管理者は Google 管理コンソールで ISE プロビジョニング アプリケーションをロードし、ISE から証明書を取得するために Chromebook デバイスで使用できるようにする必要があります。

- 推奨される Google ホスト名が、SSL の安全な接続のために WLC で設定された ACL 定義リストで許可されていることを確認します。Google サポートページの推奨および許可されているホスト名を参照してください。

ISE 管理者：

- 証明書テンプレートの構造を含む、Chromebook OS のネイティブ サプリカント プロファイルを定義します。
- Chromebook ユーザーの Cisco ISE で必要な認証ルールとクライアント プロビジョニング ポリシーを作成します。

Chromebook ユーザー：

- Chromebook デバイスを消去し、Google ドメインに登録して、Google 管理者によって定義された適用ポリシーを保護します。
- Chromebook デバイス ポリシーと、Google 管理コンソールによってインストールされた、強制されている Cisco Network Setup Assistant 拡張機能を受信します。
- Google 管理者によって定義されているとおりにプロビジョニングされた SSID に接続して、ブラウザを開いて BYOD ページを表示し、オンボーディング プロセスを開始します。
- Cisco Network Setup Assistant が Chromebook デバイスにクライアント証明書をインストールし、これによりデバイスが EAP-TLS 証明書ベースの認証を行えるようになります。

Google 管理コンソール：

Google 管理コンソールは Chromebook デバイス管理をサポートし、安全なネットワークの設定と、Chromebook への Cisco Network Setup Assistant 証明書管理拡張機能のプッシュができます。この拡張機能は SCEP 要求を Cisco ISE に送信し、クライアント証明書をインストールして、安全な接続とネットワークへのアクセスを可能にします。

共有環境での Chromebook デバイスの使用のベスト プラクティス

Chromebook デバイスが学校や図書館などの共有環境で使用される場合、Chromebook デバイスはさまざまなユーザーによって共有されます。シスコが推奨するベスト プラクティスの一部は、次のとおりです。

- 特定のユーザー（学生または教授）の名前で Chromebook デバイスをオンボーディングする場合、ユーザーの名前が証明書の [件名（Subject）] フィールドの [共通名（CN）（Common Name (CN)）] に入力されます。また、共有 Chromebook がその特定のユーザーの My Devices ポータルに表示されます。そのため、共有デバイスではオンボーディング時に共有クレデンシャルを使用し、特定のユーザーの My Devices ポータルのリストにのみデバイスが表示されるようにすることを推奨します。共有アカウントは、個別のアカウントとして管理者または教授が管理し、共有デバイスを制御することができます。
- Cisco ISE 管理者は、共有 Chromebook デバイス用のカスタム証明書テンプレートを作成し、ポリシーで使用することができます。たとえば、[件名-共通名（CN）（Subject-Common Name (CN)）] 値に一致する標準の証明書テンプレートを使用する代わりに、証明書の名前（chrome-shared-grp1 など）を指定して同じ名前を Chromebook デバイスに割り当てることができます。ポリシーは、Chromebook デバイスへのアクセスを許可または拒否するために、名前で一致させるように設計できます。
- Cisco ISE 管理者は、（アクセスが制限される必要があるデバイスの）Chromebook オンボーディングを経る必要があるすべての Chromebook デバイスの MAC アドレスを備えたエンドポイントグループを作成できます。認証ルールは、デバイス タイプ Chromebook とともにこれを呼び出す必要があります。これにより、アクセスが NSP にリダイレクトされます。

Chromebook オンボーディング プロセス

Chromebook オンボーディング プロセスは、次の一連のステップを実行します。

ステップ 1 Google 管理コンソールでのネットワークの設定と拡張機能の強制 。
ステップ 2 Chromebook オンボーディング用の Cisco ISE の設定。
ステップ 3 Chromebook デバイスのワイプ。
ステップ 4 Google 管理コンソールへの Chromebook の登録。
ステップ 5 BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続。

Google 管理コンソールでのネットワークの設定と拡張機能の強制

Google 管理者は、次の手順を実行します。

ステップ 1 Google 管理コンソールにログインします。

a) ブラウザで URL https://admin.google.com を入力します。
b) 必要なユーザー名とパスワードを入力します。
c) [管理コンソールへようこそ（Welcome to Admin Console）] ウィンドウで、[デバイス管理（Device Management）] をクリックします。
d) [デバイス管理（Device Management）] ウィンドウで、[ネットワーク（Network）] をクリックします。

ステップ 2 管理対象デバイスの Wi-Fi ネットワークをセットアップします。

a) [ネットワーク（Networks）] ページで、[Wi-Fi] をクリックします。

b) [Add Wi-Fi] をクリックして、必要な SSID を追加します。詳細については、「Google 管理コンソール：Wi-Fi ネットワーク設定」を参照してください。

MAB フローについては、2 つの SSID を作成し、1 つをオープン ネットワーク用、もう 1 つを証明書認証用にします。ユーザーがオープン ネットワークに接続すると、Cisco ISE ACL は、認証のために、ユーザーをクレデンシャルを持つゲスト ポータルにリダイレクトします。認証が成功すると、ACL はユーザーを BYOD ポータルにリダイレクトします。

ISE 証明書が中間 CA によって発行された場合は、ルート CA ではなく、中間証明書を「サーバー認証局」にマッピングする必要があります。

c) [追加（Add）] をクリックします。

ステップ 3 強制拡張機能を作成します。

a) [デバイス管理（Device Management）] ウィンドウの [デバイス設定（Device Settings）] の下にある [Chrome 管理（Chrome Management）] をクリックします。

b) [ユーザー設定（User Settings）] をクリックします。

c) 下にスクロールして、[アプリケーションと拡張機能（Apps and Extensions）] セクションの [強制的にインストールされたアプリケーションと拡張機能（Force-Installed Apps and Extensions）] オプションで、[強制的にインストールされたアプリケーションの管理（Manage Force-Installed Apps）] をクリックします。

ステップ 4 強制拡張機能をインストールします。

a) [強制的にインストールされたアプリケーションと拡張機能（Force-Installed Apps and Extensions）] ウィンドウで、[Chrome Web ストア（Chrome Web Store）] をクリックします。

b) [検索（Search）] テキスト ボックスに「Cisco Network Setup Assistant」と入力して、拡張機能を見つけます。

Chromebook デバイスの Cisco Network Setup Assistant 拡張機能は、Cisco ISE の証明書を要求し、Chromebook デバイスに ISE の証明書をインストールします。証明書のインストールは管理対象デバイスに対してのみ許可されるため、この拡張機能は、強制的にインストールされるように設定する必要があります。登録プロセス中にこの拡張機能がインストールされていない場合は、Cisco ISE の証明書をインストールすることはできません。

c) [追加（Add）] をクリックして、強制的にアプリをインストールします。

d) [保存（Save）] をクリックします。

ステップ 5 （オプション）複数のユーザーに共有されている Chromebook デバイスに証明書をインストールするには、コンフィギュレーション ファイルを定義します。

a) メモ帳ファイルに次のコードをコピー アンド ペーストして、ローカル ディスクに保存します。

```
{
  "certType": {
    "Value": "system"
  }
}
```

b) **[デバイス管理（Device Management）]** > **[Chromebook管理（ Chromebook Management）]** > **[アプリケーション管理（App Management）]** の順に選択します。
c) [Cisco Network Setup Assistant] 拡張機能をクリックします。
d) [ユーザー設定（User Settings）] をクリックし、ドメインを選択します。
e) [設定ファイルのアップロード（Upload Configuration File）] をクリックし、ローカルディスクに保存した .txt ファイルを選択します。

（注） Cisco Network Setup Assistant で複数のユーザーが共有するデバイスの証明書を作成するには、このメモ帳ファイルを Google 管理コンソールに追加する必要があります。追加しないと、Cisco NSA はシングル ユーザー用の証明書を作成します。

f) [保存（Save）] をクリックします。

ステップ 6 （オプション）Chromebook を共有しないシングル ユーザーの証明書をインストールします。

a) **[デバイス管理（Device Management）]** > **[ネットワーク（Network）]** > **[証明書（Certificates）]** の順に選択します。
b) [証明書（Certificates）] ウィンドウで、[証明書の追加（Add Certificate）] をクリックして、Cisco ISE の証明書ファイルをアップロードします。

次のタスク

Chromebook オンボードのための Cisco ISE の設定

Chromebook オンボーディング用の Cisco ISE の設定

始める前に

Cisco ISE 管理者は、必要なポリシーを作成する必要があります。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**(ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** ウィンドウを選択します。

認証ポリシーの例を次に示します。

Rule Name: Full_Access_After_Onboarding, Conditions: If RegisteredDevices AND Wireless_802.1x AND Endpoints:BYODRegistration EQUALS Yes AND Certificate: Subject Alternative Name Equals RadiusCalling-Station-ID AND Network Access: EAP-Authentication EQUALS EAP-TLS Then CompliantNetworkAccess.

CompliantNetworkAccess は、設定された認証結果です。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** ウィンドウを選択します。

ステップ 1 Cisco ISE でネイティブ サプリカント プロファイル（NSP）を設定します。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアントプロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** を選択します。

Chromebook デバイスが新規 Cisco ISE インストールの [クライアント プロビジョニング（Client Provisioning）] ページに表示されます。ただし、アップグレードの場合は、ポスチャの更新プログラムをダウンロードする必要があります。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）][システム（System）][設定（Settings）][ポスチャ（Posture）][更新（Updates）]** ウィンドウを選択します。

b) **[追加（Add）]** > **[ネイティブ サプリカント プロファイル（Native Supplicant Profile）]** の順にクリックします。

c) [名前（Name）] と [説明（Description）] に入力します。

d) [オペレーティング システム（Operating System）] フィールドで、[Chrome OS すべて（Chrome OS All）] を選択します。

e) [証明書テンプレート（Certificate Template）] フィールドで、必要な証明書テンプレートを選択します。

f) [送信（Submit）] をクリックします。SSID が Google 管理コンソールからプロビジョニングされていて、ネイティブ サプリカント プロビジョニング フローからではないことを確認します。

ステップ 2 [クライアント プロビジョニング（Client Provisioning）] ページで NSP をマッピングします。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[クライアントプロビジョニング（Client Provisioning）]** を選択します。

b) 結果を定義します。

- クライアント プロビジョニング ポリシーの [結果（Results）] で組み込みのネイティブ サプリカント設定（Cisco-ISE-Chrome-NSP）を選択します。
- または、新しいルールを作成し、Chromebook デバイス用に作成された [結果（Result）] が選択されていることを確認します。

Chromebook デバイスのワイプ

Chromebook デバイスは、Google 管理コンソールが Google 管理者により設定された後でワイプされる必要があります。Chromebook ユーザーはデバイスをワイプする必要があり、これは拡張を強制し、ネットワークを設定する一度だけの処理です。詳細については、次の URL https://support.google.com/chrome/a/answer/1360642を参照してください。

Chromebook ユーザーは次の手順を実行します。

ステップ 1 **Esc + Refresh + Power** キーの組み合わせを押します。画面に黄色い感嘆符（!）が表示されます。

ステップ 2 開発モードを開始するには、**Ctrl + D** キーの組み合わせを押してから、**Enter** キーを押します。画面に赤い感嘆符が表示されます。

ステップ 3 **Ctrl + D** キーの組み合わせを押します。Chromebook はローカルデータを削除して、初期状態に戻ります。この削除には約 15 分かかります。

ステップ 4 移行が完了したら、**Space** キーを押してから **Enter** キーを押して、確認モードに戻ります。

ステップ 5 サインインする前に Chromebook を登録します。

次のタスク

Google 管理コンソールに Chromebook を登録します。

Google 管理コンソールへの Chromebook の登録

Chromebook のデバイスをプロビジョニングするには、Chromebook ユーザーは最初に Google 管理コンソール ページに登録し、デバイス ポリシーおよび強制拡張を受信する必要があります。

ステップ 1 Chromebook のデバイスの電源を入れ、サインオン画面が表示されるまで、画面上の指示に従います。まだサインインしないでください。

ステップ 2 Chromebook のデバイスにサインインする前に、**Ctrl + Alt + E** のキーの組み合わせを押します。[エンタープライズ登録（Enterprise Enrolment）] 画面が表示されます。

ステップ 3 E メールアドレスを入力し、[次へ（Next）] をクリックします。
次のメッセージが表示されます：「デバイスは企業管理用に正しく登録されています（Your device has successfully been enrolled for enterprise management.）」。

ステップ 4 [完了（Done）] をクリックします。

ステップ 5 Google 管理のようこそレターからのユーザー名とパスワード、または登録資格があるアカウントの既存の Google アプリケーション ユーザーのユーザー名とパスワードを入力します。

ステップ 6 [デバイスの登録（Enroll Device）] をクリックします。デバイスが正常に登録されると、確認メッセージが表示されます。

Chromebook の登録の処理は一度だけであることに注意してください。

BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続

デュアル SSID 用の手順：EAP-TLS プロトコルを使用して 802.x ネットワークに接続する場合、Chromebook ユーザーは次の手順を実行します。

（注） デュアル SSID を使用している場合：802.x PEAP から EAP-TLS ネットワークに接続するときは、ネットワーク サプリカント（Webブラウザではなく）にクレデンシャルを入力して、ネットワークに接続してください。

ステップ 1 Chromebook で [設定（Settings）] をクリックします。

ステップ 2 [インターネット接続（Internet Connection）] セクションで、[Wi-Fi ネットワークをプロビジョニングする（Provisioning Wi-Fi Network）] をクリックしてから、該当するネットワークをクリックします。

ステップ 3 クレデンシャルを持つゲスト ポータルが開きます。

1. [サインオン（Sign On）] ページで、[ユーザー名（Username）] と [パスワード（Password）] を入力します。
2. [サインオン（Sign-on）] をクリックします。

ステップ 4 BYOD のウェルカム ページで、[開始（Start）] をクリックします。

ステップ 5 [デバイス情報（Device Information）] フィールドにデバイスの名前と説明を入力します。たとえば、「パーソナル デバイス：学校で使用するジェーンの Chromebook、または共有デバイス：ライブラリ Chromebook #1 または教室 1 Chromebook #1」と入力します。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 [Cisco Network Setup Assistant] ダイアログ ボックスで [はい（Yes）] をクリックして、セキュアなネットワークにアクセスするための証明書をインストールします。

Google 管理者がセキュアな Wi-Fi を設定した場合、ネットワーク接続は自動的に行われます。そうでない場合は、使用可能なネットワークのリストからセキュアな SSID を選択します。

すでにドメインに登録され、Cisco Network Setup Assistant の拡張を取得済みの Chromebook ユーザーは、自動更新を待たずに、拡張を更新できます。次の手順を実行して、拡張を手動で更新します。

1. Chromebook で、ブラウザを開き、次の URL を入力してください。**chrome://Extensions**
2. [開発者モード（Developer Mode）] チェック ボックスをオンにします。
3. [今すぐ拡張を更新（Update Extensions Now）] をクリックします。
4. Cisco Network Setup Assistant の拡張バージョンが 2.1.0.35 以上であることを確認します。

Google 管理コンソール：Wi-Fi ネットワーク設定

Wi-Fi ネットワークの設定を使用して、顧客ネットワークの SSID を設定するか、または証明書属性（EAP-TLS 用）を使用して証明書を照合します。証明書が Chromebook にインストールされるときに、Google管理設定と同期されます。接続は、定義された証明書属性のいずれかが SSID 設定と一致したときのみ確立されます。

以下に、EAP-TLS、PEAPおよびオープン ネットワーク フローに特有な必須フィールドを示します。これらは、Google 管理コンソール ページで各 Chromebook ユーザーに対し、Wi-Fi ネットワークを設定するように Google 管理者が設定します。（[デバイス管理（Device Administration）] > [ネットワーク（Network ）] > [Wi-Fi] > [Wi-Fi の追加（Add Wi-Fi）]）。

フィールド	EAP-TLS	PEAP	オープン
名前	ネットワーク接続の名前を入力します。	ネットワーク接続の名前を入力します。	ネットワーク接続の名前を入力します。
サービスセット識別子（SSID）	SSID（たとえば、tls_ssid）を入力します。	SSID（たとえば、tls_ssid）を入力します。	SSID（たとえば、tls_ssid）を入力します。
この SSID はブロードキャストされません	オプションを選択します。	オプションを選択します。	オプションを選択します。
自動的に接続	オプションを選択します。	オプションを選択します。	オプションを選択します。
セキュリティ タイプ	WPA/WPA2 Enterprise（802.1x）	WPA/WPA2 Enterprise（802.1x）	オープン
拡張認証プロトコル	EAP-TLS	PEAP	—
内部プロトコル	—	• 自動 • MSCHAP v2（オプションを選択） • MD5 • PAP • MSCHAP • GTC	—
外部 ID	—	—	—
ユーザー名	必要に応じて、固定値を設定するか、またはユーザーログインから変数を使用します：${LOGIN_ ID} または ${LOGIN_EMAIL}。	ISE（内部 ISE ユーザー / AD / その他の ISE ID）とパスワード フィールドに対し認証する PEAP クレデンシャルを入力します。	—

フィールド	EAP-TLS	PEAP	オープン
サーバー認証局	ISE 証明書を選択します（[デバイス管理（Device Administration）] > [ネットワーク（Network ）] > [証明書（Certificates）] からインポートされます）。	ISE 証明書を選択します（[デバイス管理（Device Administration）] > [ネットワーク（Network ）] > [証明書（Certificates）] からインポートされます）。	—
プラットフォームによるこの Wi-Fi ネットワークへのアクセス制限	• モバイル デバイスを選択します。 • Chromebooks を選択します。	• モバイル デバイスを選択します。 • Chromebooks を選択します。	—
クライアントの登録 URL	登録されていないユーザーに対して Chromebook デバイスのブラウザがリダイレクトされる先の URL を入力します。未登録のユーザーをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。	—	—

フィールド	EAP-TLS	PEAP	オープン
発行者パターン	証明書属性。少なくとも1つの属性を、インストールされた証明書属性に一致する、発行者パターンまたはサブジェクトパターンから選択してください。証明書を受け入れるように Chromebook デバイスに一致する証明書属性を指定します。 • 共通名：証明書のサブジェクトフィールド、またはノードのFQDNと一致している必要がある証明書のサブジェクトフィールドのワイルドカード ドメインを参照します。 • 地域：証明書のサブジェクトに関連するテスト地域（市）を参照してください。 • 組織：証明書のサブジェクトに関連する組織名を参照します。 • 組織単位：証明書のサブジェクトに関連する組織単位の名前を参照します。	—	—

フィールド	EAP-TLS	PEAP	オープン
サブジェクトパターン	証明書属性。少なくとも1つの属性を、インストールされた証明書属性に一致する、発行者パターンまたはサブジェクトパターンから選択してください。証明書を受け入れるように Chromebook デバイスに一致する証明書属性を指定します。 • 共通名：証明書のサブジェクトフィールド、またはノードのFQDNと一致している必要がある証明書のサブジェクトフィールドのワイルドカード ドメインを参照します。 • 地域：証明書のサブジェクトに関連するテスト地域（市）を参照してください。 • 組織：証明書のサブジェクトに関連する組織名を参照します。 • 組織単位：証明書のサブジェクトに関連する組織単位の名前を参照します。	—	—

フィールド	EAP-TLS	PEAP	オープン
プロキシの設定	• インターネットへの直接接続（選択済み） • 手動でのプロキシ設定 • 自動でのプロキシ設定	• インターネットへの直接接続（選択済み） • 手動でのプロキシ設定 • 自動でのプロキシ設定	—
ネットワークの適用	By User	By User	—

Cisco ISE での Chromebook デバイス アクティビティのモニター

Cisco ISE は Chromebook のデバイスの認証と認可に関する情報を表示するさまざまなレポートとログを提供します。オンデマンドまたは定期的にこれらのレポートを実行できます。認証方式（たとえば、802.1x）と認証プロトコル（たとえば、EAP-TLS）を表示することができます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）] > [RADIUS] > [ライブログ（Live Logs）]** ウィンドウを選択します。また、Chromebook デバイスとして分類されるエンドポイントの数を特定することもできます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** ウィンドウを選択します。

オンボーディング中の Chromebook デバイスのトラブルシューティング

このセクションでは、Chromebook デバイスのオンボーディング中に発生する可能性のある問題について説明します。

- エラー：webstore から拡張をインストールできない：webstore から拡張をインストールできません。これは、ネットワーク管理者によって Chromebook デバイスに自動的にインストールされます。
- エラー：証明書のインストールを完了したが、セキュアなネットワークに接続できない：管理コンソールで、インストールした証明書が定義された発行者とサブジェクトの属性パターンと一致していることを確認します。以下からインストールされた証明書に関する情報を得ることができます。chrome://settings/certificates
- エラー：Chromebook でセキュアなネットワークに手動で接続しようとして、「ネットワーク証明書の取得（Obtain Network Certificate）」のエラー メッセージが表示される：[新しい証明書の取得（Get New Certificate）] をクリックしてブラウザを開き、証明書をインストールする ISE BYOD にリダイレクトされます。ただし、セキュアなネットワークに接続

できない場合は、管理コンソールで、インストールされた証明書が定義された発行者とサブジェクトの属性パターンと一致していることを確認します。

- エラー：[新しい証明書の取得（Get New Certificate）] をクリックしたが、www.cisco.com に転送される：ユーザーはISEにリダイレクトされ、証明書のインストールプロセスを開始するために、プロビジョニングする SSID に接続する必要があります。適切なアクセスリストがこのネットワーク用に定義されていることを確認します。
- エラー：エラーメッセージ「管理対象デバイスのみがこの拡張を使用できます。ヘルプデスクまたはネットワーク管理者にお問い合わせください（Only managed devices can use this extension. Contact helpdesk or network administrator）」が表示される：Chromebook は管理対象デバイスであり、デバイスで証明書をインストールするには、拡張は、Chrome OS API にアクセスするために強制インストールとして設定する必要があります。拡張は、Google Web ストアからダウンロードして手動でインストールすることもできますが、登録されていない Chromebook ユーザーは証明書をインストールすることはできません。

  登録されていないChromebookデバイスは、ユーザーがドメインユーザー グループに属する場合に証明書を保護できます。拡張はデバイスのドメインユーザーを追跡します。ただし、ドメインユーザーは登録されていないデバイスのユーザー単位の認証キーを生成できます。
- エラー：Google の管理コンソールで SSID が接続された順番が不明：
  - いくつかの SSID（PEAP、および EAP-TLS）が Google の管理コンソールで設定された場合、証明書がインストールされ、属性が一致すると、Chrome OS は SSID が設定された順序にかかわらず、証明書ベースの認証を使用して SSID に自動的に接続します。
  - 2つのEAP-TLS SSIDが同じ属性で一致した場合、接続は、信号強度や他のネットワーク レベルの信号などの、ユーザーまたは管理者で制御できないその他の要因に依存します。
  - 複数のEAP-TLSの証明書がChromebookデバイスにインストールされ、そのすべてが管理コンソールで設定された証明書パターンと一致した場合、一番新しい証明書が接続に使用されます。

Cisco Secure クライアント

Cisco ISE は、Cisco ISE ポスチャ要件の Cisco セキュアクライアントで統合モジュールを使用します。

（注） Cisco ISE 2.7 パッチ 8 以降、Cisco ISE 3.0 パッチ 7 以降、Cisco ISE 3.1 パッチ 5 以降、Cisco ISE 3.2 パッチ 1 以降、および Cisco ISE 3.3 以降のリリースは、Windows、macOS、および Linux オペレーティングシステム用の AnyConnect と Cisco Secure Client の両方をサポートします。これらのオペレーティングシステムでは、次の Cisco Secure Client バージョンがサポートされています。

- Windows：Cisco Secure Client バージョン 5.00529 以降
- MacOS：Cisco Secure Client バージョン 5.00556 以降
- Linux：Cisco Secure Client バージョン 5.00556 以降

これらのオペレーティングシステムではエンドポイントに対して AnyConnect と Cisco Secure Client の両方を構成できますが、エンドポイントでの実行時に考慮されるのは 1 つのポリシーのみです。いずれの場合も、エンドポイントが Cisco ISE 管理対象ネットワークデバイスに接続しない場合、TCP ポート 8905 およびクライアント プロビジョニング ポータル ポートのエンドポイントからすべての Cisco ISE PSN への HTTP プローブをブロックする必要があります。デフォルトのクライアント プロビジョニング ポータル ポートは TCP ポート 8443 です。

Cisco ISE をエージェントと統合すると、Cisco ISE は次のように機能します。

- Cisco セキュアクライアントを展開するためのステージングサーバーとして機能する
- Cisco ISE ポスチャ要件のエージェントポスチャコンポーネントとやり取りする
- エージェントプロファイル、カスタマイズおよび言語パッケージ、ならびに の OPSWAT のライブラリ更新の展開をサポートする

（注） ネットワークのメディアを切り替えるときに、ポスチャモジュールが変更後のネットワークを検出し、クライアントを再評価するように、デフォルトのゲートウェイを変更する必要があります。

エージェント設定の作成

エージェント設定には、エージェントソフトウェアおよび関連するコンフィギュレーション ファイルが含まれます。この設定は、ユーザーがクライアントでエージェントリソースをダウンロードしてインストールできるクライアント プロビジョニング ポリシーで使用できます。ISE と ASA の両方を使用してエージェントを展開する場合は、両方のヘッドエンドで設定が一致している必要があります。

VPN に接続するときに ISE ポスチャモジュールをプッシュするには、シスコの Adaptive Security Device Manager（ASDM）GUI ツールを使用する Cisco 適応型セキュリティアプライアンス（ASA）を使用してエージェントをインストールすることをお勧めします。ASA は、VPN ダウンローダを使用してインストールを行います。ダウンロードでは、ISE ポスチャ プロファイ

ルは ASA によってプッシュされ、後続のプロファイルのプロビジョニングに必要なホスト検出が利用可能になってから、ISE ポスチャ モジュールが ISE に接続します。その一方、ISE では、ISE ポスチャ モジュールは ISE が検出された後にのみプロファイルを取得し、これがエラーの原因になることがあります。したがって、VPN に接続するとき ASA を ISE ポスチャ モジュールにプッシュすることを推奨します。

（注） Cisco ISE が ASA と統合されている場合は、ASA でアカウンティングモードが [シングル（Single）] に設定されていることを確認します。アカウンティングデータは、シングルモードでは 1 つのアカウンティングサーバーにのみ送信されます。

始める前に

エージェント設定オブジェクトを設定する前に、次の手順を実行する必要があります。

1. Cisco ソフトウェアのダウンロードページからエージェントヘッドエンド展開パッケージとコンプライアンスモジュールをダウンロードします。
2. これらのリソースを Cisco ISE にアップロードします（ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加 （1795 ページ）を参照）。
3. （任意）カスタマイズおよびローカライズのバンドルを追加します（ローカルマシンからのエージェント用の顧客作成リソースの追加 （1796 ページ）を参照）。
4. ポスチャ エージェント プロファイルを設定します（ポスチャ エージェント プロファイルの作成 （1825 ページ）を参照）。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provision）] > [リソース（Resources）]**の順に選択します。

ステップ 2 **[追加（Add）]** をクリックして、エージェント設定を作成します。

ステップ 3 **[エージェントの設定（Agent Configuration）]** を選択します。

ステップ 4 以前にアップロードしたエージェントパッケージを選択します。たとえば、cisco-secure-client-win-xxxxxxx-webdeploy-k9.pkg などです。

ステップ 5 現在のエージェント設定の名前を入力します。たとえば、AC Config xxx.x.xxxxx.x とします。

ステップ 6 以前にアップロードしたコンプライアンス モジュールを選択します。たとえば、cisco-secure-client-win-xxxxxxx-isecompliance-predeploy-k9.msi などです。

ステップ 7 1つ以上のエージェントモジュールのチェックボックスをオンにします。たとえば、ISEポスチャ、VPN、ネットワーク アクセス マネージャ、Web セキュリティ、AMP イネーブラ、ASA ポスチャ、Start Before Log on（Windows OS のみ）、Diagnostic and Reporting Tool の中から、1 つ以上のモジュールを選択します。

（注） [エージェントモジュール選択（Agent Module Selection）] で VPN モジュールをオフにしても、プロビジョニングされたクライアントの VPN タイルは無効になりません。エージェント GUI の VPN タイルを無効にするには、VPNDisable_ServiceProfile.xml を設定する必要があります。エージェントがデフォルトの場所にインストールされているシステムでは、このファイルは C:\Program Files\Cisco にあります。エージェントが別の場所にインストールされている場合、このファイルは <エージェントがインストールされているパス>\Cisco にあります。

ステップ 8 選択した エージェントモジュール用のエージェントプロファイルを選択します。たとえば、ISE ポスチャ、VPN、NAM および Web セキュリティを選択します。

ステップ 9 エージェントカスタマイゼーション バンドルおよびローカリゼーションバンドルを選択します。

ステップ 10 [送信（Submit）] をクリックします。

ポスチャ エージェント プロファイルの作成

ポスチャのエージェントプロファイルを作成するには、次の手順を実行します。このプロファイルでは、ポスチャプロトコルのエージェントの動作を定義するパラメータを指定できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 **[エージェントポスチャプロファイル（Agent Posture Profile）]** を選択します。

ステップ 4 プロファイルの [名前（Name）] に入力します。

ステップ 5 次のパラメータを設定します。

- Cisco ISE ポスチャ エージェントの動作
- クライアント IP アドレスの変更
- Cisco ISE ポスチャ プロトコル

ステップ 6 [送信（Submit）] をクリックします。

クライアント IP アドレスのリフレッシュ設定

次の表に、VLAN の変更後に IP アドレスをリフレッシュするようにクライアントのパラメータを設定できる [エージェントポスチャプロファイル（Agent Posture Profile）] ウィンドウのフィールドを示します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアントプロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** > **[追加（Add）]** > **[エージェントポスチャプロファイル（Agent Posture Profile）]** 。

フィールド名	デフォルト値	使用上のガイドライン
VLAN 検出間隔（VLAN detection interval）	0、5	この設定は、エージェントが VLAN 変更をチェックする間隔です。 Mac OS X エージェントの場合、デフォルト値は 5 です。Mac OS X のデフォルトでは、認証 VLAN 変更機能へのアクセスは、VlanDetectInteval を 5 秒として有効になっています。有効な範囲は 5 ～ 900 秒です。 0：認証 VLAN 変更機能へのアクセスは無効化されます。 1～5：エージェントはインターネット制御メッセージ プロトコル（ICMP）またはアドレス解決プロトコル（ARP）クエリーを 5 秒ごとに送信します。 6 ～ 900：ICMP/ARP クエリーが x 秒ごとに送信されます。
UI なしの VLAN 検出の有効化（Enable VLAN detection without UI）（Mac OS X クライアントには適用できません）	No	この設定は、ユーザーがログインしていないときでも VLAN 検出を有効または無効にします。 No：VLAN 検出機能は無効です。 Yes：VLAN 検出機能が有効です。
再試行検出数（Retry detection count）	3	インターネット制御メッセージプロトコル（ICMP）またはアドレス解決プロトコル（ARP）ポーリングが失敗する場合、この設定で、クライアント IP アドレスをリフレッシュする前に x 回再試行するようにエージェントを設定します。
Ping または ARP（Ping or ARP）	0 有効な範囲は 0 ～ 2 です。	この設定は、クライアント IP アドレスの変更を検出するために使用する方式を指定します。 0：ICMP を使用してポーリング 1：ARP を使用してポーリング 2：最初に ICMP を使用し、（ICMP が失敗した場合は）ARP を使用してポーリング

フィールド名	デフォルト値	使用上のガイドライン
ping の最大タイムアウト（Maximum timeout for ping）	1 有効な値の範囲は 1 ～ 10 秒です。	ICMP を使用してポーリングし、指定した時間内に応答がない場合は、ICMP ポーリングの失敗を宣言します。
エージェント IP のリフレッシュの有効化（Enable agent IP refresh）	Yes（デフォルト）	この設定は、スイッチ（または WLC）が各スイッチポートでクライアントのログイン セッション用 VLAN を変更した後にクライアントマシンが IP アドレスをリフレッシュするかどうかを指定します。
DHCP 更新遅延（DHCP renew delay）	0 有効な値の範囲は 0 ～ 60 秒です。	この設定は、ネットワーク DHCP サーバーからの新しい IP アドレスの要求を試行する前に、クライアントマシンが待機するように指定します。
DHCP リリース遅延（DHCP release delay）	0 有効な値の範囲は 0 ～ 60 秒です。	この設定は、現在の IP アドレスをリリースする前にクライアントマシンが待機するように指定します。

（注） パラメータ値は、既存のエージェントプロファイル設定とマージするか、または上書きして、Windows および Mac OS X クライアントで適切に IP アドレスがリフレッシュされるように設定します。

ポスチャ プロトコル設定

次の表に、エージェントのポスチャプロトコル設定を設定できる [エージェントポスチャプロファイル（AnyConnect Agent Posture Profile）] ウィンドウのフィールドを示します。詳細については、ご使用のバージョンのエージェントの『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

フィールド名	デフォルト値	使用上のガイドライン
PRA 再送信時間	120 秒	パッシブ再アセスメントで通信障害がある場合のエージェントの再試行期間です。
再送遅延	60 秒	再試行までに待つ時間(秒)。

フィールド名	デフォルト値	使用上のガイドライン
再送の制限	4	メッセージに対して許可される再試行回数。
ホストの検出	—	NADを介してルーティングされる任意のIPアドレスまたはFQDNを入力します。NADはそのHTTPトラフィックを検出し、クライアントプロビジョニングポータルにリダイレクトします。
バックアップ サーバー リストの検出	—	ドロップダウンリストからPSNを選択します。エージェントは、このサーバーリストをプローブして、ポスチャを実行する必要があるPSNノードを見つけます。PSNを選択しない場合、ノードグループまたはクラスタ内のすべてのPSNがバックアップサーバーリストとしてエージェントに送信されます。
サーバー名ルール	—	エージェントが接続できるサーバーを定義する、ワイルドカード対応のカンマで区切られた名前のリスト。
Call Home リスト	—	IPアドレスとポートをコロンで結んだカンマ区切りリストを入力します。
バックオフ タイマー	30秒	この設定により、エージェントは最大時間制限に達するまでディスカバリパケットを送信することで、ディスカバリターゲット（リダイレクションターゲットおよび以前に接続していたPSN）に継続的に到達できます。有効な範囲は10～600秒です。

継続的なエンドポイント属性モニタリング

エージェントを使用して、さまざまなエンドポイント属性を継続的にモニターし、エンドポイントの全体的な可視性を向上させることができます。エージェントは、エンドポイントにインストールされ実行されているアプリケーションをモニターします。この機能をオンまたはオフにできます。また、データのモニター頻度を設定できます。デフォルトでは、データは5分間隔で収集され、データベースに保存されます。エージェントは初回ポスチャ時に、実行中のア

プリケーションと搭載アプリケーションの一覧を報告します。初回ポスチャの後に、エージェントはX分間隔でアプリケーションをスキャンし、最終スキャンでの差異をサーバーに送信します。サーバーはすべての実行中アプリケーションとインストールされているアプリケーションのリストを表示します。

ポスチャステータスの同期

ネットワーク設定の変更により、Cisco ISE がクライアントまたはエンドポイントを「保留（Pending）」状態に移行する場合があります。ただし、エージェントはこの変更を検出できず、クライアントまたはエンドポイントを「準拠（Compliant）」状態で維持します。したがって、ポスチャステータスに不一致があり、理想的には、このシナリオで正しいポスチャステータスを取得するために Cisco ISE がプローブされる必要があります。指定された間隔で Cisco ISEをプローブするようにエージェントを設定することで、これを実行できます。それにより、Cisco ISEでクライアントまたはエンドポイントのポスチャステータスが保留状態の場合、プローブによってクライアントまたはエンドポイントが保留状態のままになるのを防ぐことができます。

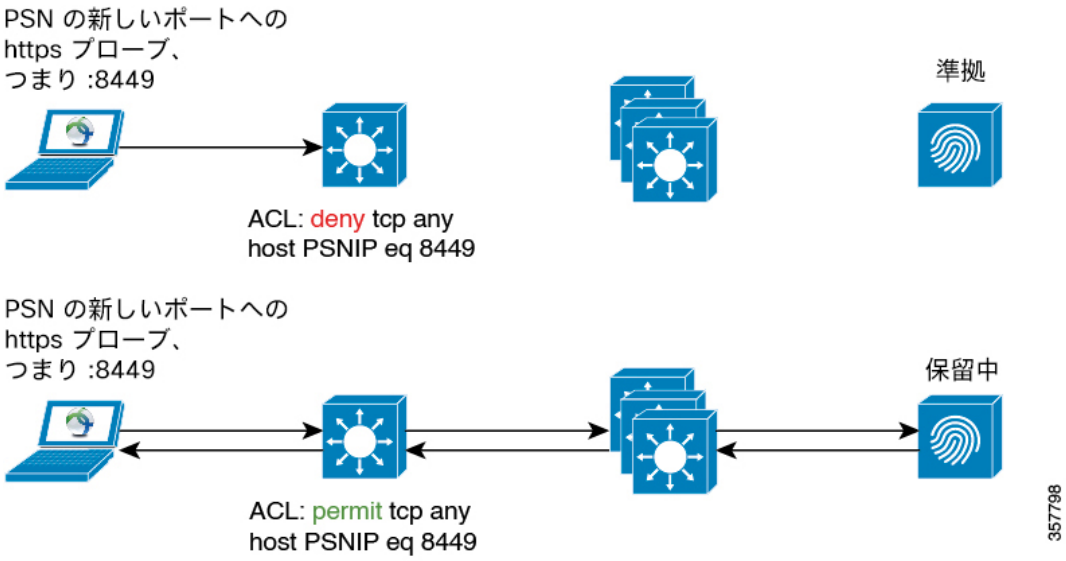
ポスチャステータスの同期は、Windows、Linux、および MacOS クライアントでサポートされています。

ポスチャステータスの同期には、次の手順が含まれます。

1. クライアントがネットワークへの接続を試行します。
2. PSNはポスチャフローを実行します。クライアントがポスチャポリシーに準拠している場合、エンドポイントは準拠状態に移行します。
3. エージェントが、Cisco ISEから[ポスチャプロービングバックアップリスト（Posture Probing Backup List）] および [ポスチャ状態同期間隔（Posture State Synchronization Interval）] の設定の詳細を受信します。
4. エージェントが、指定された間隔で Cisco ISE のプローブを開始します。

   たとえば、Cisco ISE はポスチャステータスを [保留（Pending）] と表示し、エージェントはポスチャステータスを [準拠（Compliant）] と表示します。エージェントが Cisco ISE をプローブし、新しい状態を学習すると、再評価がトリガーされます。

図 *79* : ポスチャステータスの同期



（注） 何らかの理由でクライアントのステータスが「**保留（Pending）**」に移行した場合、エージェントはクライアントからプローブ要求を受け取ります。これにより、正しいクライアント状態を調べて Cisco ISE から受信し、クライアントを正しい状態に移行します。

ポスチャ状態の同期の設定

ステップ 1 **[エージェントポスチャプロファイル（Agent Posture Profile）]** で [ポスチャプロービングバックアップリスト（Posture Probing Backup List）] と [ポスチャ状態同期間隔（Posture State Synchronization Interval）] を設定します。手順は次のとおりです。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]。

b) [追加（Add）] ドロップダウンリストから、**[エージェントポスチャプロファイル（Agent Posture Profile）]** を選択します。

c) [エージェントの動作（Agent Behavior）] 領域で、次の設定を行います。

- **[ポスチャプロービングバックアップリスト（Posture Probing Backup List）]** : エージェントがエンドポイントのポスチャ コンプライアンス ステータスをプローブする必要がある PSN を選択します。最大 6 つの PSN を選択できます。

エージェントは、これらの PSN にプローブを送信して、エンドポイントのポスチャ コンプライアンス ステータスがまだ有効かどうかを確認します。PSN を選択しない場合、接続された PSN と任意の 2 台のバックアップサーバーがポスチャ状態同期のバックアップとして使用されます。

- **[ポスチャ状態同期間隔（Posture State Synchronization Interval）]**：エージェントがポスチャステータスを Cisco ISE と同期する頻度を定義します。有効な範囲は 0 ～ 300 です。0 を入力すると、ポスチャステート同期プローブが無効になります。この値が 0 より大きい場合は、ポスチャステート同期ポートを準拠認証プロファイルに対してブロックする必要があります。

ステップ 2 ポート 8449 を双方向通信用に設定します。手順は次のとおりです。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [クライアントプロビジョニングポータル（Client Provisioning Portals）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]。

b) [ポータル設定（Portal Settings）] をクリックします。

c) [双方向ポート（Bidirectional Port）] フィールドで、ポート 8449 が双方向通信用に設定されていることを確認します。

デフォルトでは、ポート 8449 は双方向通信に使用されます。

ステップ 3 クライアント ポスチャ ステータスが準拠している場合、ポスチャ状態同期プローブが Cisco ISE に到達しないように ACL を設定します。手順は次のとおりです。

a) Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能ACL（Downloadable ACLs）] を選択します。

b) ACLを設定します。

保留状態のクライアントのみが、双方向ポートを介して設定済みの PSN に到達できることを確認します。これにより、準拠状態のクライアントからの不要なトラフィックが回避されます。次に、ACL の例を示します。

```
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
deny tcp any host <ip address> eq 8449
permit ip any any
```

ACL が設定されていない場合、Cisco ISE ダッシュボードで、ポスチャ設定検出アラームがトリガーされます。ACL は、問題のあるポリシー セットでのみ設定する必要があります。このアラームの主な目的は、Cisco ISE への大量のトラフィックを防ぐことです。

（注） クライアントが保留状態のときに、対応するポートの通信がファイアウォールによってブロックされないようにします。

Cisco Web Agent

Cisco Web Agent では、クライアント マシンのための一時的なポスチャ評価を提供します。

ユーザーはCisco Web Agent実行ファイルを起動することができ、ActiveX コントロールまたは Java アプレットによって、クライアント マシンの一時ディレクトリに Web Agent ファイルがインストールされます。

Cisco Web Agent は、ユーザーがログインすると、ユーザー ロールまたはオペレーティング システムに設定された要件を Cisco ISE サーバーから取得し、必要なパッケージのホスト レジストリ、プロセス、アプリケーション、およびサービスをチェックし、レポートをCisco ISEサーバーに送信します。クライアントマシンに関する要件が満たされている場合、ユーザーはネットワークにアクセスできます。要件が満たされていない場合、Web Agent は満たされていない要件ごとに、ユーザーにダイアログを表示します。ダイアログにより、クライアントマシンの要件を満たすための手順および対処法が提供されます。あるいは、指定された要件が満たされない場合は、ユーザー ログイン ロールの要件を満たすようにクライアント システムの修復試行中は制限付きのネットワーク アクセスを受け入れるという選択もできます。

（注） ActiveX は 32 ビット版の Internet Explorer でのみサポートされます。Firefox Web ブラウザまたは 64 ビット版の Internet Explorer のバージョンでは、ActiveX をインストールできません。

クライアント プロビジョニング リソース ポリシーの設定

クライアントの場合、クライアント プロビジョニング リソースのポリシーによって、ログイン時とユーザーセッション開始時にどのユーザーがどのバージョンのリソース（エージェント、エージェント対応モジュール、およびエージェント カスタマイゼーション パッケージまたはプロファイル）を Cisco ISE から受信するかが決まります。

エージェントの場合、[クライアントプロビジョニング リソース（Client Provisioning Resources）] ウィンドウからリソースを選択して、[クライアント プロビジョニング ポリシー（Client Provisioning Policy）] ウィンドウで使用できる エージェント設定を作成できます。エージェント設定では、エージェントソフトウェアとさまざまなコンフィギュレーションファイルとの関連付けを指定します。ファイルには、 Windows クライアント、MacOS クライアント、および Linux クライアントの エージェント バイナリ パッケージ、コンプライアンスモジュール、モジュールプロファイル、カスタマイズパッケージ、および言語パッケージなどがあります。

始める前に

- 有効なクライアント プロビジョニング リソース ポリシーを作成する前に、Cisco ISE にリソースを追加したことを確認します。エージェント コンプライアンス モジュールをダウ

ンロードすると、システムで使用している既存のモジュールがあれば常にそれが上書きされます。

- クライアント プロビジョニング ポリシーで使用されているネイティブのサプリカント プロファイルをチェックして、ワイヤレス SSID が正しいことを確認します。iOS デバイスの場合、接続対象ネットワークが非表示の場合は、[iOSの設定（iOS Settings）] 領域で [ターゲットネットワーク非表示時にイネーブルにする（Enable if target network is hidden）] チェックボックスをオンにします。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]**。

ステップ 2 [動作（Behavior）] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [有効化（Enable）]：ユーザーがネットワークにログインし、クライアントプロビジョニング ポリシーのガイドラインに従っている場合に、Cisco ISE がこのポリシーを使用して、クライアントプロビジョニング機能を果たすようにします。
- [無効化（Disable）]：Cisco ISE は、指定されたリソースポリシーを使用せずにクライアント プロビジョニング機能を果たします。
- [モニター（Monitor）]：ポリシーを無効にし、クライアントプロビジョニングセッション要求を「監視」し、Cisco ISE が「モニター対象」のポリシーに基づいて起動しようとした回数を確認します。

ステップ 3 [ルール名（Rule Name）] テキストボックスに新しいリソースポリシーの名前を入力します。

ステップ 4 Cisco ISE にログインするユーザーが属する ID グループを 1 つ以上指定します。

設定した既存の ID グループのリストから、[任意（Any）] ID タイプを指定することも、1 つ以上のグループを選択することもできます。

ステップ 5 [オペレーティングシステム（Operating Systems）] フィールドを使用して、ユーザーが Cisco ISE にログインする際に使用するクライアントマシンまたはデバイスで動作している 1 つ以上のオペレーティングシステムを指定します。

（注） Cisco ISE の GUI の [クライアント プロビジョニング（Client Provisioning）] ウィンドウには MacOS 10.6、10.7、および 10.8 を選択するオプションはありますが、エージェントはこれらのバージョンをサポートしていません。

ステップ 6 [その他の条件（Other Conditions）] フィールドで、この特定のリソースポリシー用に作成する新しい式を指定します。

ステップ 7 クライアントマシンの場合は、[エージェント設定（Agent Configuration）] オプションを使用して、クライアントマシンで利用可能にし、プロビジョニングするエージェントタイプ、コンプライアンスモジュール、エージェント カスタマイズ パッケージ、およびプロファイルを指定します。

クライアントマシンでエージェントがポップアップできるようにするには、クライアントプロビジョニング URL を認証ポリシーに含める必要があります。これにより、ランダムなクライアントからの要求が回避され、適切なリダイレクト URL を持つクライアントのみがポスチャ評価を要求できるようになります。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

1 つ以上のクライアント プロビジョニング リソース ポリシーを正常に設定したら、ログイン中にクライアントマシンのポスチャアセスメントを実行するように Cisco ISE の設定を開始できます。

クライアント プロビジョニング ポリシーの Cisco ISE ポスチャ エージェントの設定

クライアントマシンについては、エージェントタイプ、コンプライアンスモジュール、エージェント カスタマイズ パッケージ/プロファイルを、ユーザーがクライアントマシンにダウンロードおよびインストールできるように設定します。

始める前に

Cisco ISE のエージェントのクライアント プロビジョニング リソースを追加している必要があります。

ステップ 1 **Agent** ドロップダウン リストから使用可能なエージェントを選択し、ここで定義したエージェントのアップグレード（ダウンロード）がクライアント マシンに対して必須かどうかを、**Is Upgrade Mandatory** オプションを必要に応じて有効または無効にすることによって指定します。

Is Upgrade Mandatory 設定は、エージェントのダウンロードにのみ適用されます。エージェントプロファイル、コンプライアンスモジュール、およびエージェント カスタマイズ パッケージの更新は常に必須です。

ステップ 2 **Profile** ドロップダウン リストから既存のエージェント プロファイルを選択します。

ステップ 3 **Compliance Module** ドロップダウン リストを使用して使用可能なコンプライアンス モジュールを選択し、クライアント マシンにダウンロードします。

ステップ 4 **Agent Customization Package** ドロップダウン リストから、クライアント マシンに使用可能なエージェント カスタマイズ パッケージを選択します。

パーソナル デバイスのネイティブ サプリカントの設定

従業員は、Windows、Mac OS、iOS、および Android デバイスで使用可能なネイティブ サプリカントを使用して、ネットワークに自分のパーソナルデバイスを直接接続できます。パーソナル デバイスに関して、登録されているパーソナル デバイスで使用可能にし、プロビジョニングするネイティブ サプリカントの設定を指定します。

始める前に

ユーザーがログインするとき、そのユーザーの許可要件と関連付けるプロファイルに基づいて、Cisco ISE が、ユーザーのパーソナルデバイスを設定するために必要なサプリカント プロビジョニング ウィザードを提供して、ネットワークにアクセスするように、ネイティブ サプリカント プロファイルを作成します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 動作のドロップダウンリストから **Enable**、**Disable**、または **Monitor** を選択します。

ステップ 3 [ルール名（Rule Name）] テキスト ボックスに、新しいリソース ポリシーの名前を入力します。

ステップ 4 次を指定します。

- [IDグループ（Identity Groups）] フィールドを使用して、Cisco ISE にログインするユーザーが属する ID グループを 1 つ以上指定します。
- [オペレーティングシステム（Operating System）] フィールドを使用して、ユーザーが Cisco ISE にログインする際に使用するパーソナルデバイスで動作している 1 つ以上のオペレーティングシステムを指定します。
- [その他の条件（Other Conditions）] フィールドを使用して、この特定のリソースポリシー用に作成する新しい式を指定します。

ステップ 5 パーソナル デバイスの場合、[ネイティブサプリカントの設定（Native Supplicant Configuration）] を使用し、特定の**Configuration Wizard**を選択して、パーソナル デバイスに配信します。

ステップ 6 指定されたパーソナル デバイス タイプに適用可能な **Wizard Profile** を指定します。

ステップ 7 [保存（Save）] をクリックします。

クライアント プロビジョニング レポート

Cisco ISE のモニタリングおよびトラブルシューティング機能にアクセスし、ユーザー ログインセッションの成功または失敗の全体のトレンドをチェックし、特定の期間にネットワークにログインしたクライアントマシンの数およびタイプに関する統計情報を収集し、また、クライアント プロビジョニング リソースでの最近の設定変更をチェックすることができます。

クライアント プロビジョニングの要求

[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [エンドポイントおよびユーザー（Endpoints and Users）] > [クライアント プロビジョニング（Client Provisioning）] レポートには、クライアントプロビジョニング要求の成功および失敗に関する統計情報が表示されます。**Run** を選択していずれかのプリセット期間を指定すると、Cisco ISE によってデータベースが調べられ、生成されたクライアント プロビジョニング データが表示されます。

サプリカント プロビジョニングの要求

[操作（Operations）] > **[レポート（Reports）]** > **[ISE レポート（ISE Reports）]** > **[エンドポイントおよびユーザー（Endpoints and Users）]** > **[サプリカント プロビジョニング（Supplicant Provisioning）]** ウィンドウには、最近の成功および失敗したユーザーデバイス登録およびサプリカント プロビジョニング要求に関する情報が表示されます。**Run** を選択していずれかのプリセット期間を指定すると、Cisco ISE によってデータベースが調べられ、生成されたサプリカント プロビジョニング データが表示されます。

サプリカント プロビジョニング レポートは、特定の期間にデバイス登録ポータルから登録されたエンドポイントのリストに関する情報が提供されます。これには、ログイン日時、ID（ユーザー ID）、IP アドレス、MAC アドレス（エンドポイント ID）、サーバー プロファイル、エンドポイント オペレーティング システム、SPW バージョン、障害理由（ある場合）、登録のステータスなどのデータが含まれます。

クライアント プロビジョニング イベント ログ

クライアントの動作の問題の診断に役立つイベント ログ エントリを検索できます。たとえば、ネットワーク上のクライアント マシンがログイン時にクライアント プロビジョニング リソースの更新を取得できないという問題の原因を特定する必要がある場合があります。ポスチャおよびクライアントプロビジョニングの監査、ポスチャおよびクライアントプロビジョニングの診断のロギング エントリを使用できます。

クライアントプロビジョニング ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[クライアントプロビジョニングポータル（Client Provisioning Portals）]** > **[作成、編集、複製または削除（Create, Edit, Duplicate, or Delete）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** です。

ポータル設定

- **[HTTPS ポート（HTTPS Port）]**：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで 8443 です。ただし、**[ブロックリスト（Blocked List）]** ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合、この制限に従うようにポート設定を変更する必要があります。
- **[使用可能インターフェイス（Allowed interfaces）]**：ポータルを実行できる PSN インターフェイスを選択します。PSN で使用可能なインターフェイスを備えた PSN のみがポータルを作成できます。物理およびボンディングされたインターフェイスの任意の組み合わせを設定できます。これは PSN 全体の設定です。すべてのポータルはこれらのインターフェイスでのみ動作し、このインターフェイス設定はすべての PSN に適用されます。

- 異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
- ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
- ポータルの証明書のサブジェクト名とサブジェクトの代替名は、インターフェイス IP に解決される必要があります。
- ISE CLI の ip host x.x.x.x yyy.domain.com をセカンダリ インターフェイス IP と FQDN をマッピングするように設定します。これは証明書のサブジェクト名/サブジェクトの代替名を一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディング インターフェイスの設定を試みます。これが成功しない場合、その PSN にボンドセットがなかったことが原因である可能性があるので、PSN はエラーを記録して終了します。物理インターフェイスでポータルを開始しようとはしません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- **[証明書グループタグ（Certificate group tag）]**：ポータルの HTTPS トラフィックに使用する証明書グループのグループタグを選択します。
- **[認証方式（Authentication Method）]**：ユーザー認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザー クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザー、内部ユーザー、Active Directory、LDAP などがあります。

  Cisco ISE には、クライアント プロビジョニング ポータル用のデフォルトのクライアント プロビジョニング ID ソース順序 Certificate_Portal_Sequence が含まれています。
- **[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]**：クライアント プロビジョニング ポータル用に少なくとも 1 つの一意の FQDN、ホスト名、またはその両方を入力します。たとえば、「provisionportal.yourcompany.com」と入力した場合、ユーザーはこれらのいずれかをブラウザに入力して証明書プロビジョニング ポータルに到達できます。

- DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに確実に解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
- 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバー証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

（注） URL リダイレクトなしのクライアント プロビジョニングの場合、[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）] フィールドに入力するポータル名は、DNS 設定で設定されている必要があります。URL リダイレクトなしのクライアント プロビジョニングを有効にするため、この URL をユーザーに通知する必要があります。

- **[アイドルタイムアウト（Idle timeout）]**：ポータルでアクティビティがない場合にユーザーをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

（注） クライアント プロビジョニング ポータルではポート番号と証明書を定義できます。これにより、ホストはクライアント プロビジョニングとポスチャに同じ証明書をダウンロードすることを許可します。ポータル証明書が正式な認証局により署名されている場合、セキュリティ警告は表示されません。自己署名証明書の場合、ポータルと Cisco エージェント ポスチャ コンポーネントの両方でセキュリティ警告を受け取ります。

ログイン ページの設定（Login Page Settings）

- [ログインの有効化（Enable Login）]：クライアント プロビジョニング ポータルのログイン手順を有効にするには、このチェックボックスを選択します
- [レート制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：単一のブラウザセッションからのログイン試行失敗回数を指定します。この回数を超過すると、Cisco ISE はログイン試行を実行できる頻度を意図的に低下させて、追加のログイン試行を防ぎます。ログイン失敗がこの回数に達した後のログイン試行の間隔は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で指定されます。
- [頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）]：[レート制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザーが再度ログインを試行するまでに待機する必要がある時間を分単位で設定します。

- [AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）]：会社のネットワーク使用の契約条件を、現在ユーザーに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
- [同意が必要（Require acceptance）]：ポータルにアクセスする前にユーザーが AUP を受け入れることを要求します。[ログイン（Login）] ボタンは、ユーザーが AUP を受け入れない場合は有効になりません。AUP を受け入れないユーザーは、ポータルにアクセスできません。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。

利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP を含める（Include an AUP）]：会社のネットワーク使用の契約条件を、別のページでユーザーに表示します。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：ユーザーが AUP を完全に読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。
- [初回のログインのみ（On first login only）]：ユーザーがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
- [ログインごと（On every login）]：ユーザーがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [_ 日ごと（初回のログインから）（Every _____ days (starting at first login)）]：ネットワークやポータルにユーザーが初めてログインした後は、AUP を定期的に表示します。

ポストログイン バナー ページ設定（Post-Login Banner Page Settings）

[ポストログインバナーページを含める（Include a Post-Login Banner page）]：ユーザーが正常にログインした後、ネットワークアクセスを付与される前に追加情報を表示します。

パスワード変更設定（Change Password Settings）

[内部ユーザーに自身のパスワードの変更を許可する（Allow internal users to change their own passwords）]：従業員がクライアントプロビジョニング ポータルにログインして、自分のパスワードを変更できるようにします。これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

クライアントプロビジョニングポータルの言語ファイルの HTML サポート

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[クライアント プロビジョニング ポータル（Client Provisioning Portals）]** > **[編集（Edit）]** > **[ポータルページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** です。ミニエディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2

- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

第 14 章

脅威の封じ込め

- 脅威中心型 NAC サービス （1843 ページ）
- 信頼できる証明書の設定 （1865 ページ）
- メンテナンスの設定 （1868 ページ）
- 一般 TrustSec の設定 （1873 ページ）
- ネットワーク リソース （1876 ページ）
- デバイス ポータルの管理 （1907 ページ）

脅威中心型 NAC サービス

脅威中心型ネットワーク アクセス コントロール（TC-NAC）機能により、脅威および脆弱性のアダプタから受信する脅威と脆弱性の属性に基づいて、許可ポリシーを作成できます。

脅威のシビラティ（重大度）レベルと脆弱性評価の結果は、エンドポイントまたはユーザーのアクセス レベルを動的に制御するために使用できます。

忠実度の高い侵害の兆候（IoC）、脅威検出イベント、およびCVSS スコアを Cisco ISE に送信するように脆弱性および脅威のアダプタを設定できます。これにより、エンドポイントの権限とコンテキストを適宜変更するための脅威中心型アクセスポリシーを作成できます。

Cisco ISE では次のアダプタがサポートされています。

- SourceFire FireAMP（現在の Cisco Secure Endpoint）
- Cognitive Threat Analytics（CTA）アダプタ
- Qualys

（注） TC-NAC フローで現在サポートされているのは Qualys Enterprise Edition のみです。

- Rapid7 Nexpose
- Tenable Security Center

エンドポイントの脅威イベントが検出されたら、[侵害されたエンドポイント（Compromised Endpoints）] ウィンドウでエンドポイントの MAC アドレスを選択して ANC ポリシー（Quarantine など）を適用できます。Cisco ISE は、そのエンドポイントに対して CoA をトリガーし、対応する ANC ポリシーを適用します。ANC ポリシーが使用可能ではない場合、Cisco ISE はそのエンドポイントに対して CoA をトリガーし、元の許可ポリシーを適用します。[侵害されたエンドポイント（Compromised Endpoints）] ウィンドウの [脅威と脆弱性のクリア（Clear Threat and Vulnerabilities）] オプションを使用して、（Cisco ISE システムデータベースから）エンドポイントに関連付けられている脅威と脆弱性をクリアできます。

脅威ディクショナリには次の属性がリストされます。

- CTA-Course_Of_Action（値は Internal Blocking、Eradication、または Monitoring です。）
- Qualys-CVSS_Base_Score
- Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

Base Score 属性と Temporal Score 属性の有効な範囲は 0 ~ 10 です。

脆弱性イベントがエンドポイントに受信されると、Cisco ISE はそのエンドポイントの CoA をトリガーします。ただし、脅威イベントの受信時には CoA はトリガーされません。

脆弱性属性を使用して、属性の値に基づいて脆弱なエンドポイントを自動的に隔離する許可ポリシーを作成できます。次に例を示します。

```
Any Identity Group & Threat:Qualys-CVSS_Base_Score > 7.0 -> Quarantine
```

CoA イベント中に自動的に隔離されているエンドポイントのログを表示するには、**[操作（Operations）] > [脅威中心型NACのライブログ（Threat-Centric NAC Live Logs）]** を選択します。手動で隔離されているエンドポイントのログを表示するには、**[操作（Operations）] > [レポート（Reports）] > [監査（Audit）] > [変更構成監査（Change Configuration Audit）]** を選択します。

脅威中心型 NAC サービスを有効にする際には、次の点に注意してください。

- 脅威中心型 NAC サービスを使用するには、Cisco ISE Premier ライセンスが必要です。
- 脅威中心型 NAC サービスは、展開内の 1 つのノードでのみ有効にできます。
- 脆弱性アセスメント サービスでは、ベンダーあたり 1 つのアダプタ インスタンスだけを追加できます。ただし、FireAMP アダプタ インスタンスは複数追加できます。
- 設定を失わずにアダプタを停止、再開できます。アダプタの設定後は、任意の時点でアダプタを停止できます。ISE サービスの再起動時でもアダプタはこの状態のままになります。アダプタを再起動するには、アダプタを選択して [再起動（Restart）] をクリックします。

（注） アダプタが [停止（Stopped）] 状態の場合、アダプタ インスタンスの名前だけを編集できます。アダプタ設定や詳細設定は編集できません。

エンドポイントの脅威情報は次に示すページで確認できます。

- **[ホーム（Home）] ページ > [脅威（Threat）] ダッシュボード**
- **[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [侵害されたエンドポイント（Compromised Endpoints）]**

脅威中心型 NAC サービスによりトリガーされるアラームを次に示します。

- Adapter not reachable（syslog ID：91002）：アダプタに到達できないことを示します。
- Adapter Connection Failed（syslog ID：91018）：アダプタに到達できるが、アダプタとソースサーバーの間の接続がダウンしていることを示します。
- Adapter Stopped Due to Error（syslog ID：91006）：このアラームは、アダプタが必要な状態になっていない場合にトリガーされます。このアラームが表示されたら、アダプタ設定とサーバー接続を調べてください。詳細については、アダプタ ログを参照してください。
- Adapter Error（syslog ID：91009）：Qualys アダプタが Qualys サイトとの接続を確立できないか、またはこのサイトから情報をダウンロードできないことを示します。

脅威中心型 NAC サービスで使用できるレポートを次に示します。

- **[アダプタのステータス（Adapter Status）]**：アダプタのステータスレポートには、脅威と脆弱性のアダプタのステータスが表示されます。
- **[COA イベント（COA Events）]**：エンドポイントの脆弱性イベントを受信すると、Cisco ISE はそのエンドポイントについて CoA をトリガーします。CoA イベント レポートには、これらの CoA イベントのステータスが表示されます。また、これらのエンドポイントの新旧の認証ルールとプロファイルの詳細が表示されます。
- **[脅威イベント（Threat Events）]**：脅威イベントレポートには、設定したさまざまなアダプタから Cisco ISE が受信した脅威イベントがすべて表示されます。脆弱性アセスメントのイベントは、このレポートには含まれません。
- **[脆弱性アセスメント（Vulnerability Assessment）]**：脆弱性アセスメントレポートには、エンドポイントで実行中のアセスメントに関する情報が示されます。このレポートを表示して、設定されたポリシーに基づいてアセスメントが行われているかどうかを確認することができます。

[操作（Operations）] > [レポート（Reports）] > [診断（Diagnostics）] > [ISE カウンタ（ISE Counters）] > [しきい値カウンタのトレンド（Threshold Counter Trends）] で、次の情報を確認できます。

- 受信したイベントの総数

- 脅威イベントの総数
- 脆弱性イベントの総数
- （PSN に対して）発行された CoA の総数

これらの属性の値は 5 分おきに収集されるため、この値は直近 5 分間の数を表します。

[脅威（Threat）] ダッシュボードには次のダッシュレットが表示されます。

- [侵害されたエンドポイントの総数（Total Compromised Endpoints）] ダッシュレットには、ネットワーク上で現在影響を受けているエンドポイント（接続エンドポイントと切断エンドポイントの両方）の総数が表示されます。
- [特定期間における侵害されたエンドポイント（Compromised Endpoints Over Time）] ダッシュレットには、指定された期間におけるエンドポイントへの影響の履歴ビューが表示されます。
- [上位の脅威（Top Threats）] ダッシュレットには、影響を受けるエンドポイントの数と脅威のシビラティ（重大度）に基づく上位の脅威が表示されます。
- [脅威ウォッチリスト（Threats Watchlist）] ダッシュレットを使用して、選択したイベントのトレンドを分析できます。

[上位の脅威（Top Threats）] ダッシュレットでは、バブルのサイズが影響を受けるエンドポイントの数を示し、薄い影が付いている領域が切断されているエンドポイントの数を示します。色と縦方向の目盛りで脅威のシビラティ（重大度）を示します。脅威には、インディケータとインシデントという 2 つのカテゴリがあります。インディケータのシビラティ（重大度）属性は「Likely_Impact」、インシデントのシビラティ（重大度）属性は「Impact_Qualification」です。

[侵害されたエンドポイント（Compromised Endpoint）] ウィンドウには、影響を受けるエンドポイントのマトリックスビューと、各脅威カテゴリの影響のシビラティ（重大度）が示されます。エンドポイントの詳細な脅威情報を表示するには、デバイス リンクをクリックします。

[実行されたアクション（Course Of Action）] チャートには、CTA アダプタから受信した CTA-Course_Of_Action 属性に基づき、脅威インシデントに対して実行されたアクション（[内部ブロック（Internal Blocking）]、[撲滅（Eradication）]、または [モニタリング（Monitoring）]）が表示されます。

[ホーム（Home）] ページの [脆弱性（Vulnerability）] ダッシュボードには、次のダッシュレットが表示されます。

- [脆弱なエンドポイントの総数（Total Vulnerable Endpoints）] ダッシュレットには、指定された値よりも大きい CVSS スコアを持つエンドポイントの総数が表示されます。また、CVSS スコアが指定された値よりも大きい接続エンドポイントと切断エンドポイントの総数も表示されます。
- [上位の脆弱性（Top Vulnerability）] ダッシュレットには、影響を受けるエンドポイントの数または脆弱性のシビラティ（重大度）に基づく上位の脅威が表示されます。[上位の脆弱性（Top Vulnerability）] ダッシュレットでは、バブルのサイズが影響を受けるエンドポ

イントの数を示し、薄い影が付いている領域が切断されているエンドポイントの数を示します。色と縦方向の目盛りで脆弱性のシビラティ（重大度）を示します。

- [脆弱性ウォッチリスト（Vulnerability Watchlist）] ダッシュレットを使用して、一定期間にわたる選択した脆弱性のトレンドを分析できます。ダッシュレットで検索アイコンをクリックし、ベンダー固有の ID（Qualys の ID 番号の場合は「qid」）を入力して、その ID 番号の傾向を選択して表示します。
- [特定期間における脆弱なエンドポイント（Vulnerable Endpoints Over Time）] ダッシュレットには、一定期間におけるエンドポイントへの影響の履歴ビューが表示されます。

[脆弱なエンドポイント（Vulnerable Endpoints）] ウィンドウの [CVSS 別エンドポイント数（Endpoint Count By CVSS）] グラフには、影響を受けるエンドポイントの数とその CVSS スコアが表示されます。[脆弱なエンドポイント（Vulnerable Endpoints）] ウィンドウでは、影響を受けるエンドポイントのリストも表示されます。各エンドポイントの詳細な脆弱性情報を表示するには、デバイスリンクをクリックします。

脅威中心型 NAC サービスログはサポートバンドルに含まれています。脅威中心型 NAC サービスログは support/logs/TC-NAC/ にあります。

（注） Cisco ISE は、エンドポイントでのクレデンシャルを使用したオンデマンドスキャンをサポートしていません。

脅威中心型 NAC サービスの有効化

脆弱性と脅威のアダプタを設定するには、まず脅威中心型 NAC サービスを有効にする必要があります。このサービスは、導入内の 1 つのポリシーサービス ノードでのみ有効にできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 脅威中心型 NAC サービスを有効にする PSN の隣にあるチェック ボックスにマークを付けて、[編集（Edit）] をクリックします。

ステップ 3 [脅威中心型 NAC サービスの有効化（Enable Threat Centric NAC Service）] チェック ボックスにマークを付けます。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

SourceFire FireAMP アダプタの追加 （1848 ページ）
Cognitive Threat Analytics アダプタの追加 （1849 ページ）
CTA アダプタの許可プロファイルの設定 （1851 ページ）
Course of Action 属性を使用した許可ポリシーの設定 （1851 ページ）
脅威中心型 NAC サービス （1843 ページ）

SourceFire FireAMP アダプタの追加

始める前に

- SourceFire FireAMP のアカウントが必要です。
- すべてのエンドポイントの FireAMP クライアントを導入する必要があります。
- 脅威中心型 NAC サービスを展開ノードで有効にする必要があります（脅威中心型 NAC サービスの有効化 （1847 ページ）を参照）。
- FireAMP アダプタは REST API コール（AMP クラウドへ）、およびイベントを受信する AMQP に SSL を使用します。また、プロキシの使用をサポートしています。FireAMP アダプタは通信にポート 443 を使用します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから [AMP：脅威（AMP：Threat）] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ベンダーインスタンスのリストウィンドウを更新します。ベンダーインスタンスのリストウィンドウでアダプタのステータスが [設定準備完了（Ready to Configure）] に変更された後でのみ、アダプタを設定できます。

ステップ 7 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 8 （オプション）すべてのトラフィックをルーティングするように SOCKS プロキシ サーバーを設定した場合、プロキシ サーバーのホスト名とポート番号を入力します。

ステップ 9 接続するクラウドを選択します。US クラウドまたは EU クラウドを選択できます。

ステップ 10 サブスクライブするイベント ソースを選択します。次のオプションを使用できます。

- **[AMP イベントのみ（AMP events only）]**
- **[CTA イベントのみ（CTA events only）]**
- **[CTA と AMP のイベント（CTA and AMP events）]**

ステップ 11 FireAMP リンクをクリックし、admin として FireAMP にログインします。[アプリケーション（Applications）] ペインの [許可（Allow）] をクリックして、ストリーミング イベント エクスポート要求を許可します。
Cisco ISE にリダイレクトします。

ステップ 12 監視するイベントを選択します（たとえば、不審なダウンロード、疑わしいドメインへの接続、実行されたマルウェア、Java 侵害）。

詳細設定の変更またはアダプタの再設定時に、AMPクラウドに新しいイベントが追加されている場合、これらのイベントも [イベントリスト（Events Listing）] ウィンドウに表示されます。

アダプタ用のログ レベルを選択できます。選択可能なオプションは、[エラー（Error）]、[情報（Info）]、[デバッグ（Debug）] です。

アダプタインスタンスの設定の要約が [設定サマリー（Configuration Summary）] ウィンドウに表示されます。

Cognitive Threat Analytics アダプタの追加

始める前に

- 脅威中心型 NAC サービスを展開ノードで有効にする必要があります（脅威中心型 NAC サービスの有効化 （1847 ページ）を参照）。
- http://cognitive.cisco.com/login から Cisco Cognitive Threat Analytics（CTA）ポータルにログインし、CTA STIX/TAXII サービスを要求します。詳細については、『Cisco ScanCenter Administrator Guide』を参照してください。
- Cognitive Threat Analytics（CTA）アダプタは、SSL とともに TAXII プロトコルを使用して、CTA クラウドをポーリングし、検出された脅威を確認します。また、プロキシの使用をサポートしています。
- 信頼できる証明書ストアにアダプタ証明書をインポートします。[管理（Administration）] >[システム（System）]>[証明書（Certificates）]>[信頼できる証明書（Trusted Certificates）] > [インポート（Import）] の順に選択し、証明書をインポートします。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [脅威中心型NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから [CTA：脅威（CTA：Threat）] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ベンダー インスタンスのリスト ページを更新します。ベンダー インスタンスのリスト ページでアダプタのステータスが [設定準備完了（Ready to Configure）] に変更された後でのみ、アダプタを設定できます。

ステップ 7 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 8 次の詳細を入力します。

- [CTA STIX/TAXII サービスの URL（CTA STIX/TAXII service URL）]：CTA クラウドサービスの URL。デフォルトでは URL https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService/ が使用されます。
- [CTA フィード名（CTA feed name）]：CTA クラウドサービスのフィード名を入力します。
- [CTA ユーザー名とパスワード（CTA username and password）]：CTA クラウドサービスのユーザー名とパスワードを入力します。
- [プロキシホストとポート（Proxy host and port）]（オプション）：すべてのトラフィックをルーティングするようにプロキシサーバーを設定した場合、そのプロキシ サーバーのホスト名とポート番号を入力します。
- [ポーリング間隔（Polling interval）]：各ポーリング間の時間間隔。デフォルト値は 30 分です。
- [最初のポーリング期間（時間数）（First Poll Duration in hours）]：最初のポーリングで取得されるデータの経過時間。デフォルト値は 2 時間です。最大値は 12 時間です。
- [インシデントタイプ（Incident Type）]：次のオプションを使用できます。
  - **[CTA イベントのみ（CTA events only）]**
  - **[AMP イベントのみ（AMP events only）]**
  - **[CTA と AMP のイベント（CTA and AMP events）]**

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 次のオプションを設定するには、[詳細設定（Advanced Settings）] をクリックします。

- [影響の指定（Impact Qualification）]：ポーリングするインシデントのシビラティ（重大度）レベルを選択します。次のオプションを使用できます。
  - **[1 - 影響なし（1 - Insignificant）]**
  - **[2 - 妨害（2 - Distracting）]**
  - **[3 - 困難（3 - Painful）]**
  - **[4 - 損害発生（4 - Damaging）]**
  - **[5 - 壊滅的（5 - Catastrophic）]**

  [3 - 困難（3 - Painful）] を選択した場合、シビラティ（重大度）レベルが [3 - 困難（3 - Painful）] またはそれ以上（この場合 [4 - 損害発生（4 - Damaging）] と [5 - 壊滅的（5 - Catastrophic）]）のインシデントがポーリングされます。
- [ロギングレベル（Logging Level）]：アダプタのログ レベルを選択します。選択可能なオプションは、[エラー（Error）]、[情報（Info）]、[デバッグ（Debug）] です。

ステップ 11 [終了（Finish）] をクリックします。

（注） CTA は Web プロキシ ログに IP アドレスまたはユーザー名としてリストされているユーザー ID を処理します。具体的には、IP アドレスの場合、プロキシ ログで使用可能なデバイスの IP アドレスが、内部ネットワークの別のデバイスの IP アドレスと競合する可能性があります。たとえばエージェント経由で接続するローミングユーザーと、インターネットに直接接続するスプリットトンネルが獲得するローカル IP 範囲アドレス（例：10.0.0.X）が、内部ネットワークで使用されている重複するプライベート IP 範囲のアドレスと競合することがあります。不一致のデバイスに隔離アクションが適用されることを防ぐポリシーを定義するときには、論理ネットワーク アーキテクチャを考慮することが推奨されます。

CTA アダプタの許可プロファイルの設定

脅威イベントごとに、CTA アダプタは Course of Action 属性の値「Internal Blocking」、「Monitoring」、または「Eradication」のいずれかを返します。これらの値に基づいて許可プロファイルを作成できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 許可プロファイルの名前および説明を入力します。

ステップ 4 アクセス タイプを選択します。

ステップ 5 必要な詳細を入力し、[送信（Submit）] をクリックします。

Course of Action 属性を使用した許可ポリシーの設定

脅威イベントが報告されたエンドポイントに対して許可ポリシーを設定するには、CTA-Course_Of_Action 属性を使用できます。この属性は [脅威（Threat）] ディレクトリで使用できます。

また、CTA-Course_Of_Action 属性に基づいて例外ルールを作成することもできます。

ステップ 1 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択します。
脅威イベントが発生したエンドポイントについて、既存のポリシー ルールを編集するか、または新しい例外ルールを作成することができます。

ステップ 2 CTA-Course_Of_Action 属性値を検査するための条件を作成し、適切な許可プロファイルを割り当てます。次に例を示します。

Network_Access_Authentication_Passed AND ThreatCTA-Course_Of_Action CONTAINS Internal Blocking then blocking (authorization profile)

（注） 「Internal Blocking」はエンドポイントの隔離に使用することが推奨される Course of Action 属性です。

ステップ 3 [保存（Save）] をクリックします。

エンドポイントの脅威イベントを受信すると、Cisco ISE は、そのエンドポイントに一致する許可ポリシーがあるかどうかを調べ、エンドポイントがアクティブな場合にのみ CoA をトリガーします。エンドポイントがオフラインの場合、脅威イベントの詳細が脅威イベント レポートに追加されます（[操作（Operations）] > [レポート（Reports）] > [脅威中心型 NAC（Threat Centric NAC] > [脅威イベント（Threat Events）]）。

（注） CTA が 1 つのインシデントで複数のリスクとそれらに関連付けられている Course of Action 属性を送信することがあります。たとえば 1 つのインシデントで「Internal Blocking」と「Monitoring」（Course of Action 属性）を送信することがあります。この場合、「equals」演算子を使用してエンドポイントを隔離する許可ポリシーが設定されていると、エンドポイントは隔離されません。次に例を示します。

```
CTA-Course_Of_Action EQUALS Internal Blocking then Quarantine_Systems (authorization
profile)
```

この場合、エンドポイントを隔離するには許可ポリシーで「contains」演算子を使用する必要があります。次に例を示します。

```
CTA-Course_Of_Action CONTAINS Internal Blocking then Quarantine_Systems
```

Cisco ISE での脆弱性アセスメントのサポート

Cisco ISE は次の脆弱性アセスメント（VA）エコシステムパートナーと連携し、Cisco ISE ネットワークに接続するエンドポイントの脆弱性アセスメント結果を取得します。

- Qualys：Qualysは、ネットワークに導入されているスキャナアプライアンスを使用するクラウドベースの評価システムです。Cisco ISE では、Qualys と通信して VA 結果を取得するアダプタを設定できます。管理者ポータルからアダプタを設定できます。アダプタを設定するには、スーパー管理者権限を持つ Cisco ISE 管理者アカウントが必要です。Qualys アダプタは、Qualys クラウド サービスとの通信に REST API を使用します。REST API にアクセスするには、Qualys でマネージャ権限が付与されたユーザー アカウントが必要です。Cisco ISE は次の Qualys REST API を使用します。
  - [ホスト検出リストAPI（Host Detection List API）]：エンドポイントの最新スキャン結果を確認します。
  - [Scan API]：エンドポイントのオンデマンドスキャンをトリガーします。

  Qualys により、サブスクライブ ユーザーが実行できる API コールの数に制限が適用されます。デフォルトのレート制限カウントは、24 時間あたり 300 です。Cisco ISE は Qualys

API バージョン 2.0 を使用して Qualys に接続します。これらの API 機能の詳細については、『Qualys API V2 User Guide』を参照してください。

- [Rapid7 Nexpose]：Cisco ISE は脆弱性管理ソリューションである Rapid 7 Nexpose と連携して、脆弱性の検出を促進します。これにより、このような脅威に迅速に対応できるようになります。Cisco ISE は Nexpose から脆弱性データを受信し、ISE で設定したポリシーに基づいて、影響を受けるエンドポイントを隔離します。Cisco ISE ダッシュボードから、影響を受けるエンドポイントを確認し、適切なアクションを実行できます。

  Cisco ISE は Nexpose リリース 6.4.1 でテスト済みです。

- [Tenable SecurityCenter（Nessus スキャナ）（Tenable SecurityCenter (Nessus scanner)）]：Cisco ISE は Tenable SecurityCenter と連携し、（Tenable SecurityCenter により管理される）Tenable Nessus スキャナから脆弱性データを受信します。また、ISE で設定したポリシーに基づいて、影響を受けるエンドポイントを隔離します。Cisco ISE ダッシュボードから、影響を受けるエンドポイントを確認し、適切なアクションを実行できます。

  Cisco ISE リリース 3.4 は、Tenable SecurityCenter 6.4 で検証されます。

エコシステム パートナーからの結果は Structured Threat Information Expression（STIX）表現に変換され、この値に基づき、必要に応じて認可変更（CoA）がトリガーされ、適切なアクセスレベルがエンドポイントに付与されます。

エンドポイントの脆弱性に関する評価にかかる時間は、さまざまな要因に基づいて異なるため、VA をリアルタイムで実行することはできません。エンドポイントの脆弱性に関する評価にかかる時間に影響する要因を次に示します。

- 脆弱性アセスメント エコシステム
- スキャン対象の脆弱性のタイプ
- 有効なスキャンのタイプ
- エコシステムによりスキャナ アプライアンスに割り当てられるネットワーク リソースとシステム リソース

このリリースの Cisco ISE では、IPv4 アドレスを持つエンドポイントのみが脆弱性を評価できます。

脆弱性アセスメント サービスの有効化と設定

Cisco ISE で脆弱性アセスメント サービスを有効にして設定するには、次の作業を行います。

ステップ 1 脅威中心型 NAC サービスの有効化 （1847 ページ）。

ステップ 2 次の設定を行います。

- Qualys アダプタ（Qualys アダプタの設定 （1854 ページ）を参照）。
- Nexpose アダプタ（Nexpose アダプタの設定 （1858 ページ）を参照）。
- Tenable アダプタ（Tenable アダプタの設定 （1860 ページ）を参照）。

ステップ 3 認可プロファイルの設定 （1863 ページ）。

ステップ 4 脆弱なエンドポイントを隔離する例外ルールの設定 （1864 ページ）。

脅威中心型 NAC サービスの有効化

脆弱性と脅威のアダプタを設定するには、まず脅威中心型 NAC サービスを有効にする必要があります。このサービスは、導入内の 1 つのポリシー サービス ノードでのみ有効にできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 脅威中心型NACサービスを有効にするPSNの隣にあるチェック ボックスにマークを付けて、[編集（Edit）] をクリックします。

ステップ 3 [脅威中心型 NAC サービスの有効化（Enable Threat Centric NAC Service）] チェック ボックスにマークを付けます。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

SourceFire FireAMP アダプタの追加 （1848 ページ）
Cognitive Threat Analytics アダプタの追加 （1849 ページ）
CTA アダプタの許可プロファイルの設定 （1851 ページ）
Course of Action 属性を使用した許可ポリシーの設定 （1851 ページ）
脅威中心型 NAC サービス （1843 ページ）

Qualys アダプタの設定

Cisco ISE は、Qualys 脆弱性アセスメント エコシステムをサポートしています。Cisco ISE 用の Qualys アダプタを作成して、Qualys と通信し、VA 結果を取得する必要があります。

始める前に

- 次のユーザー アカウントを準備する必要があります。
  - ベンダー アダプタを設定できる、スーパー管理者権限を持つ Cisco ISE の管理者ユーザー アカウント。
  - 管理者権限を持つ Qualys のユーザー アカウント
- 適切な Qualys ライセンス サブスクリプションがあることを確認します。Qualys レポート センター、ナレッジベース（KBX）、APIにアクセスする必要があります。詳細については、Qualys アカウント マネージャにお問い合わせください。
- Cisco ISE の信頼できる証明書ストアに Qualys サーバー証明書をインポートします（[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]）。適切なルートと中

間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている（または存在する）ことを確認します。

- Qualys API ガイドの次の設定を参照してください。
  - Qualys で CVSS スコアが有効になっていることを確認します（[レポート（Reports）] > [設定（Setup）] > [CVSS スコア（CVSS Scoring）] > [CVSS スコアの有効化（Enable CVSS Scoring）]）。
  - Qualys にエンドポイントの IP アドレスとサブネットマスクが追加されていることを確認します（[アセット（Assets）] > [ホストアセット（Host Assets）]）。
  - Qualys オプションプロファイルの名前があることを確認します。オプションプロファイルは、Qualys がスキャンのために使用するスキャナ テンプレートです。認証されたスキャンを含むオプション プロファイルを使用することを推奨します（このオプションは、エンドポイントの MAC アドレスも確認します）。
- HTTPS/SSL（ポート 443）を介して Qualys と通信する Cisco ISE。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから、[Qualys:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば、Qualys_Instance などです。

設定されているアダプタインスタンスのリストを含むリストウィンドウが表示されます。

ステップ 5 ベンダーインスタンスのリストウィンドウを更新します。新しく追加された Qualys_Instance アダプタのステータスが、[設定準備完了（Ready to Configure）] に変化します。

ステップ 6 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 7 Qualys の設定画面で次の値を入力し、[次へ（Next）] をクリックします。

フィールド名	説明
REST API ホスト（REST API Host）	Qualys クラウドをホストするサーバーのホスト名です。この情報については、Qualys の担当者にお問い合わせください。
REST API ポート（REST API Port）	443
ユーザー名（Username）	管理者権限を持つ Qualys のユーザー アカウントです。
パスワード（Password）	Qualys ユーザー アカウントのパスワードです。

フィールド名	説明
HTTP プロキシ ホスト（HTTP Proxy Host）	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバーがある場合は、プロキシ サーバーのホスト名を入力します。
HTTP プロキシ ポート（HTTP Proxy Port）	プロキシ サーバーが使用するポート番号を入力します。

Qualys サーバーへの接続が確立されると、Qualys スキャナのリストを含む [スキャナマッピング（Scanner Mappings）] ウィンドウが表示されます。ネットワークからの Qualys スキャナがこのウィンドウに表示されます。

ステップ 8 Cisco ISE がオンデマンド スキャンに使用するデフォルトのスキャナを選択します。

ステップ 9 [スキャナマッピングに対する PSN（PSN to Scanner Mapping）] 領域で、PSN ノードに対して 1 つ以上の Qualys スキャナアプライアンスを選択し、[次へ（Next）] をクリックします。

[詳細設定（Advanced Settings）] ポップアップウィンドウが表示されます。

ステップ 10 [詳細設定（Advanced Settings）] ウィンドウに次の値を入力します。このウィンドウの設定は、オンデマンドスキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド名	説明
オプション プロファイル（Option Profile）	Qualys がエンドポイントのスキャンのために使用するオプションプロファイルを選択します。デフォルト オプション プロファイルである、[初期オプション（Initial Options）] を選択できます。
最後のスキャン結果 - チェック設定	
分単位の最後のスキャン結果のチェック間隔（Last scan results check interval in minutes）	（ホスト検出リスト API のアクセス レートに影響します）経過後に最後のスキャン結果を再度チェックする必要がある、分単位の時間間隔です。有効な範囲は 1 ～ 2880 です。
最後のスキャン結果がチェックされる前の最大結果数（Maximum results before last scan results are checked）	（ホスト検出リスト API のアクセス レートに影響します）キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[分単位の最後のスキャン結果のチェック間隔（Last scan results check interval in minutes）] フィールドで指定された時間間隔の前に最後のスキャン結果がチェックされます。有効な範囲は 1 ～ 1000 です。

フィールド名	説明
MAC アドレスの確認（Verify MAC address）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Qualys からの最後のスキャン結果はエンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
分単位のスキャン トリガー間隔（Scan trigger interval in minutes）	（スキャン API のアクセス レートに影響します）経過後にオンデマンドスキャンがトリガーされる、分単位の時間間隔です。有効な範囲は 1 ～ 2880 です。
スキャンがトリガーされる前の最大要求数（Maximum requests before scan is triggered）	（スキャン API のアクセス レートに影響します）キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[分単位のスキャン トリガー間隔（Scan trigger interval in minutes）] フィールドで指定された時間間隔の前にオンデマンド スキャンがトリガーされます。有効な範囲は 1 ～ 1000 です。
分単位のスキャン ステータスのチェック間隔（Scan status check interval in minutes）	経過後に Cisco ISE が Qualys と通信してスキャンのステータスをチェックする、分単位の時間間隔です。有効な範囲は 1 ～ 60 です。
同時にトリガーできるスキャン数（Number of scans that can be triggered concurrently）	（このオプションは、[スキャナ マッピング（Scanner Mappings）] 画面で各 PSN にマッピングされているスキャナの数に依存しています）各スキャナは同時に 1 つの要求のみを処理できます。PSN に複数のスキャナをマッピングしている場合は、選択したスキャナの数に基づいてこの値を増やすことができます。有効な範囲は 1 ～ 200 です。
分単位のスキャン タイムアウト（Scan timeout in minutes）	経過後にスキャン要求がタイムアウトする、分単位の時間です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は 20 ～ 1440 です。
スキャナごとの送信される IP アドレスの最大数（Maximum number of IP addresses to be submitted per scanner）	処理のために Qualys に送信される単一の要求にキュー登録できる要求の数を示します。有効な範囲は 1 ～ 1000 です。
アダプタ ログ ファイル用のログ レベルの選択（Choose the log level for adapter log files）	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー（ERROR）]、[情報（INFO）]、[デバッグ（DEBUG）]、[トレース（TRACE）] です。

ステップ 11 [次へ（Next）] をクリックして、構成設定を確認します。

ステップ 12 [完了（Finish）] をクリックします。

Nexpose アダプタの設定

Cisco ISE 用の Nexpose アダプタを作成して、Nexpose と通信し、VA 結果を取得する必要があります。

始める前に

- Cisco ISE で脅威中心型 NAC サービスを有効にしていることを確認します。
- Nexpose Security Console にログインし、ユーザーアカウントを作成して次の権限をこのアカウントに付与します。
  - サイトの管理
  - レポートの作成
- Cisco ISE の信頼できる証明書ストアに Nexpose サーバー証明書をインポートします（**[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]**）。適切なルートと中間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている（または存在する）ことを確認します。
- HTTPS/SSL（ポート 3780）を介して Nexpose と通信する Cisco ISE。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウンリストから [Rapid7 Nexpose:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば Nexpose と入力します。

設定されているアダプタインスタンスのリストを含むリストウィンドウが表示されます。

ステップ 5 ベンダーインスタンスのリストウィンドウを更新します。新しく追加された Nexpose アダプタのステータスが、[設定準備完了（Ready to Configure）] に変化します。

ステップ 6 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 7 Nexpose の設定画面で次の値を入力し、[次へ（Next）] をクリックします。

フィールド名	説明
Nexpose ホスト（Nexpose Host）	Nexpose サーバーのホスト名。
Nexpose ポート（Nexpose Port）	3780。

フィールド名	説明
ユーザー名（**Username**）	Nexpose 管理者ユーザー アカウント。
パスワード（**Password**）	Nexpose管理者ユーザーアカウントのパスワード。
HTTP プロキシ ホスト（HTTP Proxy Host）	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバーがある場合は、プロキシ サーバーのホスト名を入力します。
HTTP プロキシ ポート（HTTP Proxy Port）	プロキシ サーバーが使用するポート番号を入力します。

ステップ 8 [次へ（Next）] をクリックして拡張設定を設定します。

ステップ 9 [詳細設定（Advanced Settings）] ウィンドウに次の値を入力します。このウィンドウの設定は、オンデマンドスキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド名	説明
最新スキャン結果のチェックの設定	
最新スキャン結果をチェックする間隔（分単位）（**Interval between checking the latest scan results in minutes**）	最新スキャン結果を再度確認するまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。
最新スキャン結果を確認するトリガーとなる保留要求数（**Number of pending requests that can trigger checking the latest scan results**）	[最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）] フィールドに指定した期間が経過していない場合でも、キューに登録されたスキャン要求の数がここで指定する最大数を超えると、最新スキャン結果が確認されます。有効な範囲は 1 ～ 1000 です。
MAC アドレスの確認（**Verify MAC address**）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Nexpose からの最後のスキャン結果はエンドポイントのMACアドレスを含む場合にのみ使用されます。
スキャンの設定	
各サイトのスキャン トリガー間隔（分単位）（**Scan trigger interval for each site in minutes**）	スキャンがトリガーされるまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。

フィールド名	説明
最新スキャン結果のチェックの設定	
各サイトのスキャンのトリガーとなる保留要求の数（**Number of pending requests before a scan is triggered for each site**）	キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[スキャン トリガー間隔（分単位）（Scan trigger interval in minutes）] フィールドで指定された時間間隔が経過する前にスキャンがトリガーされます。有効な範囲は1～1000です。
分単位のスキャン タイムアウト（**Scan timeout in minutes**）	経過後にスキャン要求がタイムアウトする、分単位の時間です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は20～1440です。
スキャンを同時にトリガーできるサイトの数（**Number of sites for which scans could be triggered concurrently**）	スキャンを同時に実行できるサイトの数。有効な範囲は 1 ～ 200 です。
タイムゾーン（**Timezone**）	Nexposeサーバーで設定されているタイム ゾーンに基づいてタイム ゾーンを選択します。
HTTP タイムアウト（秒単位）（Http timeout in seconds）	Cisco ISE が Nexpose からの応答を待機する時間間隔。有効な範囲は 5 ～ 1200 です。
アダプタ ログ ファイル用のログ レベルの選択（**Choose the log level for adapter log files**）	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー（ERROR）]、[情報（INFO）]、[デバッグ（DEBUG）]、[トレース（TRACE）] です。

ステップ 10 [次へ（Next）] をクリックして、構成設定を確認します。

ステップ 11 [完了（Finish）] をクリックします。

Tenable アダプタの設定

Cisco ISE が Tenable SecurityCenter（Nessus スキャナ）と通信し、VA 結果を取得するためには、Tenable アダプタを作成する必要があります。

始める前に

Cisco ISE で Tenable Adapter を設定する前に、Tenable SecurityCenter で次の項目を設定する必要があります。これらの設定については、Tenable SecurityCenter のマニュアルを参照してください。

- Tenable Security Center と Tenable Nessus Vulnerability Scanner がインストールされている必要があります。Tenable Nessus スキャナの登録時に、[登録（Registration）] フィールドで [SecurityCenter で管理（Managed by SecurityCenter）] を必ず選択します。
- Tenable SecurityCenter で Security Manager 権限を持つユーザー アカウントを作成します。
- SecurityCenter でリポジトリを作成します（管理者ログイン情報を使用して Tenable SecurityCenter にログインし、**[リポジトリ（Repository）] > [追加（Add）]** を選択します）。
- リポジトリにスキャン対象のエンドポイント IP 範囲を追加します。
- Nessus スキャナを追加します。
- スキャン ゾーンを作成し、作成したスキャン ゾーンと、これらのスキャン ゾーンにマッピングされているスキャナに、IP アドレスを割り当てます。
- ISE のスキャン ポリシーを作成します。
- アクティブなスキャンを追加し、ISE スキャン ポリシーに関連付けます。設定項目とターゲット（IP/DNS 名）を設定します。
- システム証明書とルート証明書を Tenable SecurityCenter からエクスポートし、Cisco ISE の信頼できる証明書ストアにインポートします（**[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]**）。適切なルートと中間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている（または存在する）ことを確認します。
- Tenable SecurityCenter 6.4 以降のリリースでは、**SCAN_DEFAULT_SCAN_TIMEOUT** パラメータ値（/opt/sc/src/ の下）を 43200 に設定する必要があります。

（注） HTTPS/SSL（ポート 443）を介して Tenable SecurityCenter と通信する Cisco ISE。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから、[Tenable Security Center:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば、Tenable。

設定されているアダプタインスタンスのリストを含むリストウィンドウが表示されます。

ステップ 5 ベンダーインスタンスのリストウィンドウを更新します。新しく追加された Tenable アダプタのステータスが、[設定準備完了（Ready to Configure）] に変化します。

ステップ 6 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 7 Tenable SecurityCenter の設定画面で次の値を入力し、[次へ（Next）] をクリックします。

フィールド名	説明
Tenable SecurityCenter ホスト（Tenable SecurityCenter Host）	Tenable SecurityCenter のホスト名。
Tenable SecurityCenter ポート（Tenable SecurityCenter Port）	443
ユーザー名（Username）	Tenable SecurityCenter でセキュリティ マネージャ権限を持つユーザー アカウントのユーザー名。
パスワード（Password）	Tenable SecurityCenter でセキュリティ マネージャ権限を持つユーザー アカウントのパスワード。
HTTP プロキシ ホスト（HTTP Proxy Host）	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバーがある場合は、プロキシ サーバーのホスト名を入力します。
HTTP プロキシ ポート（HTTP Proxy Port）	プロキシ サーバーが使用するポート番号を入力します。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [詳細設定（Advanced Settings）] ウィンドウに次の値を入力します。このウィンドウの設定は、オンデマンドスキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド名	説明
リポジトリ（Repository）	Tenable SecurityCenter で作成したリポジトリを選択します。
スキャン ポリシー（Scan Policy）	Tenable SecurityCenter で、ISE 用に作成したスキャン ポリシーを選択します。
最新スキャン結果のチェックの設定	
最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）	最新スキャン結果を再度確認するまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。
最新スキャン結果を確認するトリガーとなる保留要求数（Number of pending requests that can trigger checking the latest scan results）	[最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）] フィールドに指定した期間が経過していない場合でも、キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、最新スキャン結果が確認されます。有効な範囲は 1 ～ 1000 です。デフォルトは 10 です。

フィールド名	説明
MAC アドレスの確認（Verify MAC address）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Tenable SecurityCenter からの最新スキャン結果は、エンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
各サイトのスキャン トリガー間隔（分単位）（Scan trigger interval for each site in minutes）	オンデマンド スキャンがトリガーされるまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。
スキャンのトリガーとなる保留要求の数（Number of pending requests before a scan is triggered）	キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[スキャン トリガー間隔（分単位）（Scan trigger interval in minutes）] フィールドで指定された時間間隔が経過する前にオンデマンド スキャンがトリガーされます。有効な範囲は 1 ～ 1000 です。
分単位のスキャン タイムアウト（Scan timeout in minutes）	経過後にスキャン要求がタイムアウトする期間（分単位）です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は 20 ～ 1440 です。
並列実行可能なスキャンの数（Number of scans that could run in parallel）	同時に実行できるスキャンの数。有効な範囲は 1 ～ 200 です。
HTTP タイムアウト（秒単位）（Http timeout in seconds）	Cisco ISE が Tenable SecurityCenter からの応答を待機する時間間隔。有効な範囲は 5 ～ 1200 です。
アダプタ ログ ファイル用のログ レベルの選択（Choose the log level for adapter log files）	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー（ERROR）]、[情報（INFO）]、[デバッグ（DEBUG）]、[トレース（TRACE）] です。

ステップ 10 [次へ（Next）] をクリックして、構成設定を確認します。

ステップ 11 [完了（Finish）] をクリックします。

認可プロファイルの設定

Cisco ISE の許可プロファイルに、脆弱性がないかエンドポイントをスキャンするオプションが含まれるようになりました。スキャンの定期的な実行を選択できます。また、これらのスキャンの時間間隔を指定することもできます。許可プロファイルを定義した後、既存の認可ポリシー ルールに適用するか、または新しい認可ポリシー ルールを作成できます。

始める前に

脅威中心型 NAC サービスを有効にし、ベンダー アダプタを設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[許可（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 新規の許可プロファイルを作成するか、既存のプロファイルを編集します。

ステップ 3 [共通タスク（Common Tasks）] 領域で、[脆弱性を評価する（Assess Vulnerabilities）] チェックボックスをオンにします。

ステップ 4 [アダプタ インスタンス（Adapter Instance）] ドロップダウン リストから、設定したベンダー アダプタを選択します。たとえば、Qualys_Instance などです。

ステップ 5 最後のスキャンからの時間がテキスト ボックスよりも大きい場合は、トリガー スキャンのスキャン間隔を時間単位で入力します。有効な範囲は 1 ～ 9999 です。

ステップ 6 [上の間隔を使用して定期的に評価する（Assess periodically using above interval）] チェックボックスをオンにします。

ステップ 7 [送信（Submit）] をクリックします。

脆弱なエンドポイントを隔離する例外ルールの設定

例外ルールを設定し、脆弱なエンドポイントへのアクセスを制限するには、次の脆弱性アセスメント属性を使用できます。

- Threat:Qualys-CVSS_Base_Score
- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

これらの属性は [脅威（Threat）] ディレクトリで使用できます。有効な値の範囲は 0 ～ 10 です。

エンドポイントの隔離、アクセスの制限（別のポータルへのリダイレクト）、または要求の拒否のいずれかを選択できます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択します。
既存のポリシー ルールを編集するか、または VA 属性のチェックについて新しい例外ルールを作成します。

ステップ 2 Qualys スコアを確認して適切な許可プロファイルを割り当てるための条件を作成します。次に例を示します。

Any Identity Group & Threat:Qualys-CVSS_Base_Score > 5 -> Quarantine (authorization profile)

ステップ 3 [保存（Save）] をクリックします。

脆弱性アセスメント ログ

Cisco ISE には、VA サービスのトラブルシューティングのための次のログがあります。

- vaservice.log：VA コア情報が含まれており、TC-NAC サービスを実行しているノードで使用可能です。
- varuntime.log：エンドポイントと VA フローに関する情報が含まれており、モニタリングノードと、TC-NAC サービスを実行しているノードで使用可能です。
- vaaggregation.log：1 時間ごとに収集されるエンドポイントの脆弱性に関する情報が含まれており、プライマリ管理ノードで使用可能です。

信頼できる証明書の設定

次の表では、信頼できる証明書の [編集（Edit）] ウィンドウのフィールドについて説明します。このウィンドウで CA 証明書の属性を編集します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** です。編集する信頼できる証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

表 *171* : 信頼できる証明書の編集設定

フィールド名	使用上のガイドライン
証明書発行元（Certificate Issuer）	
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。これはオプションのフィールドです。フレンドリ名を入力しない場合は、次の形式でデフォルト名が生成されます。 *common-name#issuer#nnnnn*
ステータス（Status）	ドロップダウンリストから [有効（Enabled）] または [無効（Disabled）] を選択します。証明書が無効の場合、Cisco ISE は信頼を確立するために証明書を使用しません。
説明（Description）	（任意）説明を入力します。
使用方法（Usage）	

フィールド名	使用上のガイドライン
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書で（他の Cisco ISE ノードまたは LDAP サーバーからの）サーバー証明書を確認する場合は、このチェックボックスをオンにします。
クライアント認証および syslog 用に信頼する（Trust for client authentication and Syslog）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した Cisco ISE に接続するエンドポイントを認証します。 • syslog サーバーを信頼します。
証明書ベースの管理者認証用に信頼する（Trust for certificate based admin authentication）	このチェックボックスをオンにできるのは、[クライアント認証および Syslog 用に信頼する（Trust for client authentication and Syslog）] が選択されている場合のみです。 管理者アクセスの証明書ベースの認証の使用を有効にするには、このチェックボックスをオンにします。信頼できる証明書ストアに必要な証明書チェーンをインポートします。
シスコ サービスの認証用に信頼する（Trust for authentication of Cisco Services）	フィードサービスなどの外部シスコサービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書ステータスの検証（Certificate Status Validation）	Cisco ISE は、特定の CA が発行するクライアントまたはサーバー証明書の失効ステータスをチェックする 2 とおりの方法をサポートしています。1 つめの方法は、Online Certificate Status Protocol（OCSP）を使用して証明書を検証することです（OCSP は、CA によって保持される OCSP サービスに要求を行います）。2 つめの方法は、Cisco ISE に CA からダウンロードした証明書失効リスト（CRL）と照合して証明書を検証することです。どちらの方法も、OCSP を最初に使用してステータスを判断できないときに限り CRL を使用する場合に使用できます。
OCSP サービスに対して検証する（Validate Against OCSP Service）	OCSP サービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まず OCSP サービスを作成する必要があります。

フィールド名	使用上のガイドライン
OCSP が不明なステータスを返した場合は要求を拒否する（Reject the request if OCSP returns UNKNOWN status）	証明書ステータスがOCSPサービスによって判断されなかった場合に要求を拒否するには、このチェックボックスをオンにします。このチェックボックスをオンにした場合、OCSP サービスによって不明なステータス値が返されると、Cisco ISEは現在評価しているクライアントまたはサーバー証明書を拒否します。
OCSP応答側が到達不能な場合は要求を拒否する（Reject the request if OCSP Responder is unreachable）	OCSP 応答側が到達不能な場合に Cisco ISE が要求を拒否するには、このチェックボックスをオンにします。
CRL のダウンロード（Download CRL）	Cisco ISE で CRL をダウンロードするには、このチェックボックスをオンにします。
CRL 配信 URL（CRL Distribution URL）	CA から CRL をダウンロードするための URL を入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URL は「http」、「https」、または「ldap」で始まる必要があります。
CRL の取得（Retrieve CRL）	CRLは、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。
ダウンロードが失敗した場合は待機する（If download failed, wait）	Cisco ISE が CRL を再度ダウンロードするまでに Cisco ISE に必要な試行を待機する必要がある時間間隔を設定します。
CRL を受信しない場合 CRL 検証をバイパスする（Bypass CRL Verification if CRL is not Received）	このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。

フィールド名	使用上のガイドライン
CRL がまだ有効でないか、または期限切れの場合は無視する（Ignore that CRL is not yet valid or expired）	Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。 Cisco ISE で [有効日（Effective Date）] フィールドの開始日と [次の更新（Next Update）] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRL がまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。

関連トピック

信頼できる証明書ストア （577 ページ）
信頼できる証明書の編集 （583 ページ）

メンテナンスの設定

これらのウィンドウでは、バックアップ、復元、およびデータ消去の機能を使用してデータを管理できます。

リポジトリの設定

次の表では、リポジトリを作成してバックアップ ファイルを保存するために使用できる [リポジトリリスト（Repository List）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）]**。

表 *172 :* リポジトリの設定

フィールド	使用上のガイドライン
リポジトリ（Repository）	リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。
プロトコル（Protocol）	使用する使用可能なプロトコルの 1 つを選択します。
サーバー名（Server Name）	（TFTP、HTTP、HTTPS、FTP、SFTP、および NFS で必須）リポジトリの作成先サーバーのホスト名または IP アドレス（IPv4 または IPv6）を入力します。 （注） IPv6 アドレスを使用してリポジトリを追加する場合は、IPv6 アドレスを使用して ISE eth0 インターフェイスが設定されていることを確認します。

フィールド	使用上のガイドライン
パス（**Path**）	リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。 この値は、サーバーのルート ディレクトリを示す 2 つのスラッシュ（//）または単一のスラッシュ（/）で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ（/）はルートディレクトリではなく、ローカル デバイス ホーム ディレクトリの FTP を示します。
PKI認証の有効化（Enable PKI authentication）	（オプション：SFTP リポジトリにのみ適用）SFTP リポジトリで RSA 公開キー認証を有効にするには、このチェック ボックスをオンにします。
ユーザー名（**User Name**）	（FTP、SFTP で必須）指定されたサーバーに対する書き込み権限を持つユーザー名を入力します。ユーザー名には、英数字と _-. /@\$ 文字を含めることができます。
パスワード（**Password**）	（FTP、SFTP で必須）指定されたサーバーへのアクセスに使用するパスワードを入力します。パスワードに使用できる文字は、0 ～ 9、a ～ z、A ～ Z、-、.、|、@、#、$、^、&、*、,、+、および = です。 !、?、~ のような一部の特殊文字（上記のリストには含まれていません）は、GUI を介した FTP および SFTP パスワード設定で許可されていることに注意してください。ただし、これらの特殊文字は、CLI または Open API による設定には使用できません。

関連トピック

バックアップ/復元リポジトリ （681 ページ）
リポジトリの作成 （683 ページ）

オンデマンド バックアップの設定

次の表では、バックアップを任意の時点で取得するために使用できる [オンデマンドバックアップ（On-Demand Backup）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup & Restore）]** です。

表 *173* : オンデマンド バックアップの設定

フィールド名	使用上のガイドライン
タイプ（**Type**）	次のいずれかを実行します。 • **[設定データのバックアップ（Configuration Data Backup）]**：アプリケーション固有およびCisco ADE オペレーティングシステム両方の構成データが含まれます。 • **[運用データのバックアップ（Operational Data Backup）]**：モニタリングおよびトラブルシューティング データが含まれます。
バックアップ名（**Backup Name**）	バックアップ ファイルの名前を入力します。
リポジトリ名（**Repository Name**）	バックアップファイルを保存するリポジトリ。ここにリポジトリ名を入力することはできません。ドロップダウンリストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（**Encryption Key**）	このキーは、バックアップ ファイルの暗号化および解読に使用されます。

関連トピック

バックアップ データのタイプ （680 ページ）
オンデマンドおよびスケジュール バックアップ （687 ページ）
バックアップ履歴 （693 ページ）
バックアップの失敗 （694 ページ）
Cisco ISE 復元操作 （694 ページ）
認証および許可ポリシー設定のエクスポート （702 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （703 ページ）
オンデマンド バックアップの実行 （688 ページ）

スケジュール バックアップの設定

次の表では、フルバックアップまたは増分バックアップの復元に使用できる[スケジュールバックアップ（Scheduled Backup）]ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup and Restore）]** です。

表 *174* : スケジュール バックアップの設定

フィールド名	使用上のガイドライン
タイプ（**Type**）	次のいずれかを実行します。 • **[設定データのバックアップ（Configuration Data Backup）]**：アプリケーション固有およびCisco ADE オペレーティングシステム両方の構成データが含まれます。 • **[運用データのバックアップ（Operational Data Backup）]**：モニタリングおよびトラブルシューティング データが含まれます。
名前（**Name**）	バックアップ ファイルの名前を入力します。任意のわかりやすい名前を入力できます。Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加して、ファイルをリポジトリに格納します。複数のバックアップを作成するように設定しても、一意なバックアップ ファイル名を得ることができます。[スケジュールバックアップ（Scheduled Backup）] リストウィンドウで、ファイル名の先頭に「backup_occur」が追加され、このファイルが **kron** ジョブであることを示します。
説明（**Description**）	バックアップの説明を入力します。
リポジトリ名（**Repository Name**）	バックアップ ファイルを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウンリストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（**Encryption Key**）	バックアップ ファイルを暗号化および復号化するためのキーを入力します。
スケジューリング オプション（**Schedule Options**）	スケジュール バックアップの頻度を選択し、適宜他のオプションに入力します。

関連トピック

バックアップ データのタイプ （680 ページ）
オンデマンドおよびスケジュール バックアップ （687 ページ）
バックアップ履歴 （693 ページ）
バックアップの失敗 （694 ページ）
Cisco ISE 復元操作 （694 ページ）
認証および許可ポリシー設定のエクスポート （702 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （703 ページ）
CLI を使用したバックアップ （693 ページ）

バックアップのスケジュール （691 ページ）

ポリシーのエクスポート設定のスケジュール

次の表では、[ポリシーのエクスポートのスケジュール（Schedule Policy Export）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]>[システム（System）]>[バックアップ/復元（Backup and Restore）] > [ポリシーのエクスポート（Policy Export）]** です。

表 *175 :* ポリシーのエクスポート設定のスケジュール

フィールド名	使用上のガイドライン
暗号化（Encryption）	
暗号キー（Encryption Key）	エクスポートデータを暗号化および復号化するためのキーを入力します。このフィールドは、[暗号キーを使用したエクスポート（Export with Encryption Key）] オプションを選択した場合にのみ有効になります。
宛先（Destination）	
ローカル コンピュータにファイルをダウンロード（Download file to local computer）	ポリシー エクスポート ファイルをローカル システムにダウンロードできます。
ファイルをメールで送信（Email file to）	複数の電子メールアドレスは、カンマで区切ることで入力できます。
リポジトリ（Repository）	ポリシーデータをエクスポートするリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウンリストから利用可能なリポジトリのみを選択できます。ポリシーのエクスポートのスケジュールを設定する前に、リポジトリを作成してください。
今すぐエクスポート（Export Now）	データをローカルコンピュータにエクスポートするか、電子メールの添付ファイルとして送信するには、このオプションをクリックします。リポジトリにエクスポートすることはできません。リポジトリのエクスポートのみをスケジュールできます。
スケジュール（Schedule）	
スケジューリング オプション（Schedule Options）	エクスポートのスケジュールの頻度を選択し、それに応じてその他の詳細を入力します。

一般 TrustSec の設定

Cisco ISE が TrustSec サーバーとして機能したり、TrustSec サービスを提供したりするには、グローバル TrustSec 設定を定義します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSec の全般設定（General TrustSec Settings）]。

TrustSec 展開の確認

このオプションを選択すると、すべてのネットワークデバイスに最新の TrustSec ポリシーが展開されているかどうかを確認できます。Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合は [アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] および [ホーム（Home）] > [サマリ（Summary）]）にアラームが表示されます。TrustSec ダッシュ ボードに、以下のアラームが表示されます。

- 検証プロセスが開始または完了するたびに、[情報（Info）] アイコンとともにアラームが表示されます。
- 新しい展開要求により検証プロセスがキャンセルされた場合は、[情報（Info）] アイコンとともにアラームが表示されます。
- 検証プロセスがエラーで失敗した場合は、[警告（Warning）] アイコンとともにアラームが表示されます。たとえば、ネットワーク デバイスとの SSH 接続を開けない場合やネットワーク デバイスが使用できない場合、あるいは Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合などです。

[展開の検証（Verify Deployment）] オプションは、次のウィンドウでも使用できます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。：

- **[ワーク センター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティ グループ（Security Groups）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ ACL（Security Group ACLs）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [送信元ツリー（Source Tree）]**
- **[ワーク センター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [宛先ツリー（Destination Tree）]**

[すべての展開後に自動検証（Automatic Verification After Every Deploy）]：それぞれの展開後に、Cisco ISE ですべてのネットワーク デバイス上の更新を検証するには、このチェックボッ

クスをオンにします。展開プロセスが完了したら、[展開プロセス後の時間（Time after Deploy Process）] フィールドに指定した時間が経過した後に、検証プロセスが開始されます。

[展開プロセス後の時間（Time after Deploy Process）]：展開プロセスが完了した後、検証プロセスを開始する前に Cisco ISE に待機させる時間を指定します。有効な範囲は、10 ～ 60 分です。

待機期間中に新しい展開が要求された場合や別の検証が進行中の場合は、現在の検証プロセスはキャンセルされます。

[今すぐ検証（Verify Now）]：検証プロセスをすぐに開始するには、このオプションをクリックします。

Protected Access Credential（PAC）

- [トンネル PAC の存続可能時間（Tunnel PAC Time to Live）]：

  PAC の有効期限を指定します。トンネル PAC は EAP-FAST プロトコル用のトンネルを生成します。時間を秒、分、時、日数、または週数で指定できます。デフォルト値は 90 日です。有効な範囲は次のとおりです。

  - 1 ～ 157680000 秒
  - 1 ～ 2628000 分
  - 1 ～ 43800 時間
  - 1 ～ 1825 日
  - 1 ～ 260 週間

- [プロアクティブ PAC 更新を次の後に実行する（Proactive PAC Update Will Occur After）]：Cisco ISE は、認証に成功した後、設定したパーセンテージのトンネル PAC TTL が残っているときに、新しい PAC をクライアントに予防的に提供します。PAC の期限が切れる前に最初の認証が正常に行われると、サーバーはトンネル PAC の更新を開始します。このメカニズムにより、有効な PAC でクライアントが更新されます。デフォルト値は 10% です。

セキュリティグループタグ番号の割り当て

- [システムで SGT 番号を割り当てる（System will Assign SGT Numbers）]：Cisco ISE に SGT 番号を自動生成させる場合は、このオプションを選択します。
- [範囲内の番号を除外する（Except Numbers In range）]：手動設定用に SGT 番号の範囲を予約する場合は、このオプションを選択します。Cisco ISE は、SGT の生成時にこの範囲の数値を使用しません。
- [ユーザーが手動で SGT 番号を入力する（User Must Enter SGT Numbers Manually）]：SGT 番号を手動で定義する場合は、このオプションを選択します。

APIC EPGのセキュリティグループタグのナンバリング（Security Group Tag Numbering for APIC EPGs）

[APIC EPGのセキュリティグループタグのナンバリング（Security Group Tag Numbering for APIC EPGs）]：APIC から学習した EPG に基づいて SGT を作成する場合は、このチェックボックスをオンにし、使用する番号の範囲を指定します。

セキュリティグループの自動作成

[認証ルールを作成するときにセキュリティグループを自動作成する（Auto Create Security Groups When Creating Authorization Rules）]：認証ポリシーのルールを作成する際に SGT を自動的に作成する場合は、このチェックボックスをオンにします。

このオプションを選択した場合は、[認証ポリシー（Authorization Policy）] ウィンドウの上部に、`Auto Security Group Creation is On` というメッセージが表示されます。

自動作成された SGT は、ルール属性に基づいて命名されます。

（注） 自動作成された SGT は、それに対応する認可ポリシールールを削除しても削除されません。

デフォルトでは、新規インストールまたはアップグレードの後でこのオプションが無効になります。

- [自動命名オプション（Automatic Naming Options）]：自動作成される SGT の命名規則を定義するには、このオプションを使用します。

  （必須）[名前に次が含まれます（Name Will Include）]：次のオプションのいずれかを選択します。

  - **ルール名（Rule name）**
  - **SGT番号（SGT number）**
  - **ルール名およびSGT番号（Rule name and SGT number）**

  デフォルトでは、[ルール名（Rule name）] オプションが選択されます。

  オプションで、SGT 名に以下の情報を追加できます。

  - **ポリシーセット名（Policy Set Name）**（このオプションは [ポリシーセット（Policy Sets）] が有効な場合にのみ使用可能です）
  - **プレフィックス（Prefix）**（8 文字まで）
  - **サフィックス（Suffix）**（8 文字まで）

  Cisco ISE は、選択内容に応じて [サンプル名（Example Name）] フィールドにサンプル SGT 名を表示します。

同じ名前の SGT が存在している場合、ISE は SGT 名に「_x」を付け加えます。x は（現在の名前に 1 が使用されていない場合は）1 から始まる最初の値です。新しい名前が 32 文字より長い場合、Cisco ISE によって最初の 32 文字に切り捨てられます。

ホスト名の IP SGT 静的マッピング（IP SGT Static Mapping of Hostnames）

[ホスト名の IP SGT 静的マッピング（IP SGT Static Mapping of Hostnames）]：FQDN とホスト名が使用される場合、Cisco ISE はマッピングを展開して展開状態を検査する際に、PAN および PSN ノード内の対応する IP アドレスを検索します。DNS クエリによって返される IP アドレス用に作成されるマッピングの数を指定する場合は、このオプションを使用します。次のいずれかのオプションを選択できます。

- **DNS クエリによって返されるすべての IP アドレスに対してマッピングを作成する（Create mappings for all IP addresses returned by a DNS query）**
- **DNSクエリによって返される最初のIPv4アドレスおよび最初のIPv6アドレスに対してのみマッピングを作成する（Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query）**

ネットワークデバイス用TrustSec HTTPサービス

- [HTTP サービスを有効化（Enable HTTP Service）]：HTTPを使用して、ポート 9063 経由で TrustSec データをネットワークデバイスに転送します。
- [応答ペイロード本文を監査に含める（Include entire response payload body in Audit）]：監査ログに TrustSec HTTP 応答ペイロード本文全体を表示する場合は、このオプションを有効にします。このオプションを選択すると、パフォーマンスが大幅に低下する可能性があります。このオプションを無効にすると、HTTP ヘッダー、ステータス、および認証情報のみがログに記録されます。

関連トピック

TrustSec アーキテクチャ （1588 ページ）
TrustSec のコンポーネント （1589 ページ）
TrustSec のグローバル設定 （1598 ページ）

ネットワーク リソース

セッション認識型ネットワーク（SAnet）のサポート

Cisco ISE は、セッション認識型ネットワーキング（SAnet）に対する限定的なサポートを提供します。SAnet は、多くのシスコスイッチで実行するセッション管理フレームワークです。SAnet は、可視性、認証、認可などのアクセスセッションを管理します。SAnet は、RADIUS 認可属性が含まれているサービステンプレートを使用します。Cisco ISE には、認証プロファイル内にサービステンプレートが含まれています。Cisco ISE は、プロファイルを「サービス

テンプレート」互換として識別するフラグを使用して認証プロファイルのサービステンプレートを識別します。

Cisco ISE 認証プロファイルには、属性のリストに変換される RADIUS 認可属性が含まれています。また、SAnet サービステンプレートには、RADIUS 認可属性も含まれていますが、これらの属性はリストに変換されません。

SAnetデバイスの場合、Cisco ISEはサービステンプレートの名前を送信します。キャッシュ内にそのコンテンツか、または静的に定義された設定が存在しない限り、デバイスはサービステンプレートのコンテンツをダウンロードします。サービステンプレートによってRADIUS属性が変更されると、Cisco ISE はデバイスに CoA 通知を送信します。

ネットワーク デバイス

後続の項で説明されているウィンドウを使用して、Cisco ISE でネットワークデバイスを追加および管理できます。

ネットワーク デバイス定義の設定

次の表では、Cisco ISE のネットワーク アクセス デバイスを設定するために使用できる [ネットワークデバイス（Network Devices）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** で、**[追加（Add）]** をクリックします。

ネットワーク デバイスの設定

次の表では、**[新しいネットワークデバイス（New Network Devices）]** ウィンドウのフィールドについて説明します。

表 *176 :* ネットワーク デバイスの設定

フィールド名	説明
名前（Name）	ネットワークデバイスの名前を入力します。 ネットワークデバイスに、デバイスのホスト名とは異なるわかりやすい名前を指定できます。デバイス名は論理識別子です。 （注）　必要に応じて、設定後にデバイスの名前を変更できます。
説明（Description）	このデバイスの説明を入力します。

フィールド名	説明
IP アドレス（IP Address）または **IP 範囲（IP Range）**	ドロップダウンリストから次のいずれかを選択し、表示されるフィールドに必要な値を入力します。 • [IP アドレス（IP Address）]：単一の IP アドレス（IPv4 または IPv6 アドレス）とサブネットマスクを入力します。 • [IP 範囲（IP Ranges）]：必要な IPv4 アドレスの範囲を入力します。認証時に IP アドレスを除外するには、[除外（Exclude）] フィールドに IP アドレスまたは IP アドレスの範囲を入力します。 IP アドレスとサブネットマスクまたは IP アドレスの範囲を定義するためのガイドラインを次に示します。 • 特定の IP アドレスを定義するか、サブネットマスクを使用して IP 範囲を定義できます。デバイス A の IP アドレス範囲が定義されている場合、デバイス A に定義されている範囲の個別のアドレスを別のデバイス B に設定できます。 • すべてのオクテットの IP アドレス範囲を定義できます。IP アドレスの範囲を指定するときに、ハイフン（-）またはアスタリスク（*）をワイルドカードとして使用できます。たとえば、*.*.*.*、1-10.1-10.1-10.1-10 または 10-11.*.5.10-15 などです。 • サブセットがすでに追加されている場合は、設定された範囲からその IP アドレス範囲のサブセットを除外できます。例：10.197.65.*/10.197.65.1 または 10.197.65.* exclude 10.197.65.1。 • ネットワークデバイスごとに最大 40 の IP アドレス、または IP 範囲を設定できます。 • 同じ IP アドレスを持つ 2 台のデバイスを定義することはできません。 • 同じ IP 範囲を持つ 2 台のデバイスを定義することはできません。IP 範囲は、一部または全部が重複することはできません。 • IP アドレスを除外する場合は、重複する IP 範囲を使用しないでください。代わりに、独立した IP 範囲を除外してください。
デバイスプロファイル（Device Profile）	ドロップダウンリストから、ネットワークデバイスのベンダーを選択します。 選択したベンダーのネットワークデバイスがサポートしているフローおよびサービスを表示するには、ドロップダウンリストの横にあるツールのヒントを使用します。ツールのヒントには、デバイスが使用する URL リダイレクトの RADIUS 認可変更（CoA）ポートとタイプも表示されます。これらの属性は、デバイス タイプのネットワーク デバイス プロファイルで定義されます。

フィールド名	説明
モデル名（**Model Name**）	ドロップダウンリストからデバイスのモデルを選択します。 モデル名は、ルールベースのポリシーの条件をチェックするときに、パラメータの1つとして使用します。この属性は、デバイスディクショナリにあります。
ソフトウェアバージョン（**Software Version**）	ドロップダウンリストから、ネットワークデバイスで実行するソフトウェアのバージョンを選択します。 ソフトウェアバージョンは、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性は、デバイスディクショナリにあります。
ネットワーク デバイス グループ（**Network Device Group**）	[ネットワークデバイスグループ（Network Device Group）] 領域で、[ロケーション（Location）]、**[IPSec]**、および [デバイスタイプ（Device Type）] ドロップダウンリストから必要な値を選択します。 グループに明確にデバイスを割り当てないと、そのグループはデフォルトのデバイスグループ（ルート ネットワーク デバイス グループ）に含まれます。これにより、ロケーションは [すべてのロケーション（All Locations）]、デバイスタイプは [すべてのデバイスタイプ（All Device Types）] となります。

（注） フィルタを使用して Cisco ISE 展開からネットワーク アクセス デバイス（NAD）を選択して削除する場合は、ブラウザのキャッシュをクリアして、選択した NAD のみが削除されるようにします。

RADIUS 認証設定

次の表では、[RADIUS 認証設定（RADIUS Authentication Settings）] 領域のフィールドについて説明します。

表 *177 : [RADIUS* 認証設定（*RADIUS Authentication Settings***）*]* 領域**

フィールド名	使用上のガイドライン
RADIUS UDP の設定	
プロトコル（**Protocol**）	選択したプロトコルとして **RADIUS** を表示します。

フィールド名	使用上のガイドライン
共有秘密鍵（Shared Secret）	ネットワーク デバイスの共有秘密鍵を入力します。 共有秘密鍵は、**pac** オプションを指定した **radius-host** コマンドを使用してネットワークデバイスに設定したキーです。 （注） 共有秘密鍵の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ウィンドウ（[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デバイスセキュリティ設定（Device Security Settings）]）の [RADIUS 共有秘密鍵の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります。 RADIUS サーバーでのベストプラクティスは、22 文字にすることです。新規インストールおよびアップグレードされた展開の場合、共有秘密鍵の長さはデフォルトで 4 文字です。この値は [デバイスセキュリティ設定（Device Security Settings）] ウィンドウで変更できます。
2 番目の共有秘密の使用（Use Second Shared Secret）	ネットワークデバイスと Cisco ISE で使用される 2 番目の共有秘密鍵を指定します。 （注） Cisco TrustSec デバイスには、デュアル共有秘密（鍵）の利点がありますが、Cisco ISE により送信される Cisco TrustSec CoA パケットは常に最初の共有秘密（鍵）を使用します。2 番目の共有秘密鍵の使用を有効にするには、Cisco TrustSec CoA パケットを Cisco TrustSec デバイスに送信する Cisco ISE ノードを選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources }] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [高度な TrustSec 設定（Advanced Trustsec Settings）]** ウィンドウの [送信元（Send From）] ドロップダウンリストで、このタスクに使用する Cisco ISE ノードを設定します。プライマリ管理ノード（PAN）またはポリシーサービスノード（PSN）を選択できます。選択した PSN ノードがダウンしている場合、PAN は Cisco TrustSec デバイスに Cisco TrustSec CoA パケットを送信します。 （注） RADIUS アクセス要求の 2 番目の共有秘密機能は、[Message-Authenticator] フィールドを含むパケットに対してのみ機能します。

フィールド名	使用上のガイドライン
CoA ポート（CoA Port）	RADIUS CoA に使用するポートを指定します。 デバイスのデフォルトの CoA ポートは、ネットワークデバイス用に設定されたネットワーク デバイス プロファイルで定義されます（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）]**）。デフォルト CoA ポートを使用するには、[デフォルトに設定（Set To Default）] をクリックします。 （注） [RADIUS 認証設定（RADIUS Authentication Settings）] の **[ネットワークデバイス（Network Devices）]** ウィンドウ（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]**）で指定した CoA ポートを変更する場合は、**[ネットワークデバイスプロファイル（Network Device Profile）]** ウィンドウ（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）]**）で対応するプロファイルに同じ CoA ポートを指定します。
RADIUS DTLS の設定	
必要な DTLS（DTLS Required）	[必要な DTLS（DTLS Required）] チェックボックスをオンにすると、Cisco ISE ではこのデバイスからの DTLS 要求のみが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS はセキュアソケットレイヤ（SSL）トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、Message Digest 5（MD5）完全性チェックを計算するために使用されます。
CoA ポート（CoA Port）	RADIUS DTLS CoA に使用するポートを指定します。
CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）	ドロップダウンリストから RADIUS DTLS CoA に使用する認証局を選択します。

フィールド名	使用上のガイドライン
DNS 名（DNS Name）	ネットワーク デバイスの DNS 名を入力します。[RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification）] オプションが [RADIUS 設定（RADIUS Settings）] ウィンドウ（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[RADIUS]**）で有効になっている場合、Cisco ISE はこの DNS 名とクライアント証明書で指定されている DNS 名を比較して、ネットワークデバイスの ID を確認します。
全般設定	
KeyWrap の有効化（Enable KeyWrap）	KeyWrap アルゴリズムがネットワークデバイスでサポートされている場合にのみ、[KeyWrap の有効化（Enable KeyWrap）] チェックボックスをオンにします。ネットワークデバイスは、AES KeyWrap RFC（RFC 3394）と互換性がある必要があります。 このオプションは、AES KeyWrap アルゴリズムを介して RADIUS セキュリティを強化するために使用されます。
キー暗号キー（Key Encryption Key）	セッションの暗号化（秘密）に使用される暗号キーを入力します。
メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）	RADIUS メッセージに対するキー付きハッシュメッセージ認証コード（HMAC）の計算に使用されるキーを入力します。
キー入力形式（Key Input Format）	次のいずれかのオプション ボタンをクリックします。 • [ASCII] : [キー暗号キー（Key Encryption Key）] フィールドに入力する値の長さは16 文字（バイト）、[メッセージ認証コードキー（Message Authenticator Code Key）] フィールドに入力する値の長さは 20 文字（バイト）にする必要があります。 • [16 進数（Hexadecimal）] : [キー暗号キー（Key Encryption Key）] フィールドに入力する値の長さは 32 文字（バイト）、[メッセージ認証コードキー（Message Authenticator Code Key）] フィールドに入力する値の長さは 40 文字（バイト）にする必要があります。 ネットワークデバイスの設定と一致するように、キー暗号キーおよびメッセージ認証コードキーの入力に使用するキー入力形式を指定できます。指定する値はキーの正しい（全体の）長さにする必要があり、それよりも短い値は許可されません。

TACACS 認証設定

表 *178 : [TACACS* 認証設定（*TACACS Authentication Settings*）*]* 領域のフィールド

フィールド名	使用上のガイドライン
共有秘密鍵（**Shared Secret**）	TACACS+ プロトコルが有効のときにネットワークデバイスに割り当てられたテキストの文字列。ユーザーは、ネットワークデバイスによってユーザー名およびパスワードが認証される前にテキストを入力する必要があります。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。
廃止された共有秘密がアクティブです（**Retired Shared Secret is Active**）	リタイアメント期間がアクティブな場合に表示されます。
廃止（**Retire**）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、ダイアログボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。
残りの廃止期間（**Remaining Retired Period**）	（[廃止（Retire）] ダイアログボックスで [はい（Yes）] を選択した場合にのみ利用可能）**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[設定（Settings）]** > **[接続設定（Connection Settings）]** > **[デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]** で指定されたデフォルト値が表示されます。必要に応じて、デフォルト値を変更できます。 古い共有秘密は、指定された日数の間はアクティブなままになります。
終了（**End**）	（[廃止（Retire）] ダイアログボックスで [はい（Yes）] をクリックした場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。
シングル接続モードを有効にする（**Enable Single Connect Mode**）	[シングル接続モードを有効にする（Enable Single Connect Mode）] チェックボックスは、ネットワークデバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかのオプションボタンをクリックします。 • **[レガシーシスコデバイス（Legacy Cisco Devices）]** • **[TACACS ドラフトコンプライアンスシングル接続のサポート（TACACS Draft Compliance Single Connect Support）]** （注） [シングル接続モード（Single Connect Mode）] を無効にすると、Cisco ISE はすべての TACACS 要求に対して新しい TCP 接続を使用します。

SNMP 設定

次の表では、[SNMP 設定（SNMP Settings）] セクションのフィールドについて説明します。

表 *179 : [SNMP*設定（***SNMP Settings***）*]* 領域のフィールド

フィールド名	使用上のガイドライン
SNMP バージョン（SNMP Version）	[SNMP バージョン（SNMP Version）] ドロップダウンリストから、次のいずれかのオプションを選択します。 • **1**：SNMPv1 は informs をサポートしていません。 • **2c** • 3：SNMPv3 は、[セキュリティレベル（Security Level）] フィールドで [Priv] を選択した場合にパケットの暗号化が可能であるため、最もセキュアなモデルです。 （注） ネットワークデバイスに SNMPv3 パラメータを設定した場合、モニタリングサービス（**[操作（Operations）] > （[レポート（Reports）] > [診断（Diagnostics）] > [ネットワークデバイスセッションステータス（Network Device Session Status）]**）によって提供される [ネットワーク デバイス セッション ステータス（Network Device Session Status）] 概要レポートを生成できません。ネットワークデバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。
SNMP RO コミュニティ（SNMP RO Community）	（SNMP バージョン 1 および 2c にのみ適用可能）Cisco ISE にデバイスへの特定タイプのアクセスを提供する読み取り専用コミュニティ文字列を入力します。 （注） キャレット記号（曲折アクセント付き^）は使用できません。
SNMP ユーザー名（SNMP Username）	（SNMP バージョン 3 の場合のみ）SNMP ユーザー名を入力します。
セキュリティ レベル（Security Level）	（SNMP バージョン 3 の場合のみ）[セキュリティレベル（Security Level）] ドロップダウンリストから次のオプションのいずれかを選択します。 • **[Auth]**：MD5 またはセキュア ハッシュ アルゴリズム（SHA）パケットの認証を有効にします。 • **[No Auth]**：認証なし、プライバシーなしのセキュリティレベル。 • **[Priv]**：Data Encryption Standard（DES; データ暗号規格）パケットの暗号化を有効にします。

フィールド名	使用上のガイドライン
認証プロトコル（**Auth Protocol**）	（SNMP バージョン 3 でセキュリティレベル [Auth] または [Priv] を選択した場合のみ）[認証プロトコル（Auth Protocol）] ドロップダウンリストから、ネットワークデバイスで使用する認証プロトコルを選択します。 • **[MD5]** • **[SHA]**
認証パスワード（**Auth Password**）	（SNMP バージョン 3 で [Auth] および [Priv] セキュリティレベルを選択した場合のみ）認証キーを入力します。8 文字以上の長さにする必要があります。 デバイスにすでに設定されている認証パスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き^）を使用することはできません。
プライバシー プロトコル（**Privacy Protocol**）	（SNMP バージョン 3 で [Priv] セキュリティレベルを選択した場合のみ）[プライバシープロトコル（Privacy Protocol）] ドロップダウンリストから次のいずれかのオプションを選択します。 • **DES** • **AES128** • **AES192** • **AES256** • **3DES**
プライバシー パスワード（**Privacy Password**）	（SNMP バージョン 3 で [Priv] セキュリティレベルを選択した場合のみ）プライバシーキーを入力します。 デバイスにすでに設定されているプライバシーパスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き^）を使用することはできません。
ポーリング間隔（**Polling Interval**）	ポーリング間隔を秒単位で入力します。デフォルト値は 3600 です。
リンク トラップ クエリー（**Link Trap Query**）	SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、[リンクトラップクエリ（Link Trap Query）] チェックボックスをオンにします。

フィールド名	使用上のガイドライン
MAC トラップ クエリ（MAC Trap Query）	SNMP トラップを介して受信する MAC 通知を受信して解釈するには、[MAC トラップクエリ（MAC Trap Query）] チェックボックスをオンにします。
送信元ポリシー サービス ノード（Originating Policy Services Node）	[送信元ポリシーサービスノード（Originating Policy Services Node）] ドロップダウンリストから、SNMP データのポーリングに使用する Cisco ISE サーバーを選択します。このフィールドのデフォルト値は [自動（Auto）] です。ドロップダウンリストから特定の値を選択して、設定を上書きします。

高度な TrustSec 設定

次の表は、[高度なTrustSec設定（Advanced TrustSec Settings）] セクションのフィールドについて説明しています。

表 *180 : [*高度な *TrustSec* 設定（*Advanced TrustSec Settings*）*]* 領域のフィールド

フィールド名	使用上のガイドライン
デバイスの認証設定	
TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）	[デバイスID（Device ID）] フィールドにデバイス ID としてデバイス名をリストするには、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスをオンにします。
デバイスID（Device ID）	このフィールドは、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスがオフになっている場合にのみ使用できます。
パスワード（Password）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
HTTP REST API の設定	
HTTP REST API の有効化（Enable HTTP REST API）	HTTP REST API を使用して、ネットワークデバイスに必要な Cisco TrustSec 情報を提供するには、[HTTP REST API の有効化（Enable HTTP REST API）]チェックボックスをオンにします。これにより、効率性と能力が向上し、RADIUS プロトコルと比較して、短時間で大規模な設定をダウンロードできます。また、UDP を介した TCP を使用することで、信頼性が向上します。

フィールド名	使用上のガイドライン
ユーザー名（**Username**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したユーザー名を入力します。ユーザー名にスペース、!%^:;、[{|}] ' "= <>? を含めることはできません
パスワード（**Password**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。
TrustSec デバイスの通知および更新	
デバイスID（**Device ID**）	このフィールドは、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスがオフになっている場合にのみ使用できます。
パスワード（**Password**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
環境データのダウンロード間隔 <...>（**Download Environment Data Every <...>**）	この領域のドロップダウンリストから必要な値を選択して、デバイスが Cisco ISE から環境データをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で選択できます。デフォルト値は 1 日です。
ピア許可ポリシーのダウンロード間隔 <...>（**Download Peer Authorization Policy Every <...>**）	デバイスが Cisco ISE からピア認証ポリシーをダウンロードする必要がある時間間隔を、この領域のドロップダウンリストから必要な値を選択して指定します。時間間隔を秒、分、時、日数、または週数で指定できます。デフォルト値は 1 日です。
再認証間隔 <...>（**Reauthentication Every <...>**）	この領域のドロップダウンリストから必要な値を選択して、最初の認証後、デバイスが Cisco ISE に対して自身を再認証する時間間隔を指定します。時間間隔は秒、分、時、日、または週で設定できます。たとえば 1000 秒と入力すると、デバイスは 1000 秒ごとに Cisco ISE に対して自身を認証します。デフォルト値は 1 日です。
SGACL リストのダウンロード間隔 <...>（**Download SGACL Lists Every <...>**）	この領域のドロップダウンリストから必要な値を選択して、デバイスが Cisco ISE から SGACL リストをダウンロードする時間間隔を指定します。時間間隔は秒、分、時、日、または週で設定できます。デフォルト値は 1 日です。

フィールド名	使用上のガイドライン
その他の TrustSec デバイスでこのデバイスを信頼する（信頼できる TrustSec）（Other TrustSec Devices to Trust This Device (TrustSec Trusted)）	すべてのピアデバイスがこの Cisco TrustSec デバイスを信頼できるようにするには、[このデバイスを信頼する他の TrustSec デバイス（Other TrustSec Devices to Trust This Device）] チェックボックスをオンにします。このチェックボックスをオフにした場合、ピアデバイスはこのデバイスを信頼せず、このデバイスから到着したすべてのパケットが適宜色付けまたはタグ付けされます。
設定変更のデバイスへの送信（Send Configuration Changes to Device）	Cisco ISE で CoA または CLI（SSH）を使用して Cisco TrustSec 構成変更を Cisco TrustSec デバイスに送信する場合は、[構成変更のデバイスへの送信（Send Configuration Changes to Device）] チェックボックスをオンにします。必要に応じて、[CoA] または [CLI（SSH）（CLI (SSH)）] オプションボタンをクリックします。 Cisco ISE で CoA を使用して設定変更を Cisco TrustSec デバイスに送信する場合は、[CoA] オプションボタンをクリックします。 Cisco ISE で CLI を使用（SSH 接続を使用）して設定変更を Cisco TrustSec デバイスに送信するには、[CLI（SSH）（CLI (SSH)）] オプションボタンをクリックします。詳細については、非 CoA サポート デバイスへの設定変更のプッシュ （1647 ページ）を参照してください。
送信元（Send From）	ドロップダウンリストから、設定変更を Cisco TrustSec デバイスに送信する必要がある送信元 Cisco ISE ノードを選択します。PAN または PSN を選択できます。選択した PSN がダウンした場合、PSN を使用して Cisco TrustSec デバイスに設定変更が送信されます。
テスト接続（Test Connection）	Cisco TrustSec デバイスと選択した Cisco ISE ノード（PAN または PSN ノード）の間の接続をテストするには、このオプションを使用できます。
SSH キー（SSH Key）	この機能を使用するには、Cisco ISE からネットワーク デバイスへの SSHv2 トンネルを開き、デバイスの CLI を使用して SSH キーを取得します。確認のために、このキーをコピーして [SSHキー（SSH Key）] フィールドに貼り付ける必要があります。詳細については、SSH キーの検証（1647 ページ）を参照してください。
デバイス構成の展開	

フィールド名	使用上のガイドライン
セキュリティ グループ タグ マッピングの展開時にこのデバイスを含める（**Include this device when deploying Security Group Tag Mapping Updates**）	Cisco TrustSec デバイスがデバイスインターフェイスのログイン情報を使用して IP-SGT マッピングを取得するには、[セキュリティ グループ タグ マッピングの更新の展開時にこのデバイスを含める（Include this device when deploying Security Group Tag Mapping Updates）] チェックボックスをオンにします。
EXEC モード ユーザー名（EXEC Mode Username）	Cisco TrustSec デバイスへのログインに使用するユーザー名を入力します。
EXEC モード パスワード（EXEC Mode Password）	デバイス パスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。 （注） セキュリティの脆弱性を回避するために、EXEC モードやイネーブルモードのパスワードを含むパスワードの文字に % を使用しないことを推奨します。
有効モード パスワード（Enable Mode Password）	（任意）特権 EXEC モードで Cisco TrustSec デバイスの設定を編集するために使用する有効なパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
アウトオブバンドTrustSec PAC	
発行日（Issue Date）	この Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の発行日を表示します。
期限日（Expiration Date）	この Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の期限日を表示します。
発行元（Issued By）	このデバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行者（Cisco TrustSec 管理者）の名前を表示します。
PAC の生成（Generate PAC）	Cisco TrustSec デバイスのアウトオブバンド Cisco TrustSec PAC を生成するには、[PACの生成（Generate PAC）] ボタンをクリックします。

デフォルトのネットワーク デバイス定義の設定

次の表では、Cisco ISE が RADIUS または TACACS+ 認証に使用できる、デフォルトのネットワークデバイスを設定できるようにする [デフォルトのネットワークデバイス（Default Network device）] ウィンドウのフィールドについて説明します。次のナビゲーションパスのいずれかを選択します。

- **[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デフォルトのデバイス（Default Devices）]**
- **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク ソース（Network Resources）] > [デフォルトのデバイス（Default Devices）]**

表 ***181 : [***デフォルトのネットワークデバイス（***Default Network Device***）***]*** ウィンドウのフィールド

フィールド名	使用上のガイドライン
デフォルトのネットワーク デバイスのステータス（Default Network Device Status）	デフォルトのネットワークデバイスの定義を有効にするには、[デフォルトのネットワークデバイスのステータス（Default Network Device Status）] ドロップダウンリストから [有効化（Enable）] を選択します。 （注） デフォルトのデバイスが有効になっている場合は、ウィンドウ内の関連するチェックボックスをオンにすることで、RADIUS または TACACS+ の認証設定を有効にする必要があります。
デバイス プロファイル（Device Profile）	デフォルトのデバイスベンダーとして [シスコ（Cisco）] が表示されます。
RADIUS 認証設定	
RADIUS の有効化（Enable RADIUS）	デバイスの RADIUS 認証を有効にするには、[RADIUS の有効化（Enable RADIUS）] チェックボックスをオンにします。
RADIUS UDP の設定	

フィールド名	使用上のガイドライン
共有秘密鍵（Shared Secret）	共有秘密を入力します。共有秘密情報の長さは、最大 127 文字です。 共有秘密鍵は、pac キーワードを指定した radius-host コマンドを使用してネットワークデバイスに設定したキーです。 （注） 共有秘密の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ウィンドウ（**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** > **[デバイスのセキュリティ設定（Device Security Settings）]**）の [RADIUS 共有秘密の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります。デフォルトでは、この値は新規インストールとアップグレードされた展開の場合は 4 文字です。RADIUS サーバーでのベストプラクティスは、22 文字にすることです。
RADIUS DTLS の設定	
必要な DTLS（DTLS Required）	[必要な DTLS（DTLS Required）] チェックボックスをオンにすると、Cisco ISE ではこのデバイスからの DTLS 要求のみが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。
CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）	RADIUS DTLS CoA に使用する認証局を [CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）] ドロップダウンリストから選択します。
全般設定	
KeyWrap の有効化（Enable KeyWrap）	（任意）KeyWrap アルゴリズムがネットワークデバイスでサポートされている場合にのみ [KeyWrap の有効化（Enable KeyWrap）] チェックボックスをオンにします。これにより AES KeyWrap アルゴリズムを介した RADIUS のセキュリティが強化されます。
キー暗号キー（Key Encryption Key）	KeyWrap を有効にした場合は、セッションの暗号化（秘密）に使用する暗号キーを入力します。

フィールド名	使用上のガイドライン
メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）	KeyWrapを有効にしているときに、RADIUSメッセージに対するキー付きHashed Message Authentication Code（HMAC）の計算に使用されるキーを入力します。
キー入力形式（Key Input Format）	対応するオプションボタンをクリックして次のいずれかの形式を選択し、[キー暗号化キー（Key Encryption Key）]フィールドと[メッセージ認証コードキー（Message Authenticator Code Key）]フィールドに値を入力します。 • [ASCII]：**キー暗号化キー**の長さは16文字（バイト）、**メッセージ オーセンティケータ コード キー**の長さは20文字（バイト）である必要があります。 • [16進数（Hexadecimal）]：キー暗号化キーの長さは32バイト、メッセージ オーセンティケータ コード キーの長さは40バイトである必要があります。 ネットワークデバイスの設定と一致するように、キー暗号キーおよびメッセージ認証コードキーの入力に使用するキー入力形式を指定します。指定する値はキーの正しい（全体の）長さにする必要があります。それよりも短い値は許可されません。
TACACS 認証設定	
共有秘密鍵（Shared Secret）	TACACS+プロトコルが有効のときにネットワークデバイスに割り当てるテキスト文字列を入力します。ユーザーはネットワークデバイスによってユーザー名およびパスワードが認証される前にテキストを入力する必要があることに注意してください。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。
廃止された共有秘密がアクティブです（Retired Shared Secret is Active）	リタイアメント期間がアクティブな場合に表示されます。
廃止（Retire）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）]をクリックすると、ダイアログボックスが表示されます。[はい（Yes）]または[いいえ（No）]をクリックします。

フィールド名	使用上のガイドライン
残りの廃止期間（Remaining Retired Period）	（任意）[廃止（Retire）] ダイアログボックスで [はい（Yes）] をクリックした場合にのみ使用できます。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）] > [接続設定（Connection Settings）] > [デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]** ウィンドウで指定されたデフォルト値が表示されます。デフォルト値は変更することができます。 これにより、新しい共有秘密を入力できます。古い共有秘密は、指定された日数の間はアクティブなままになります。
終了（End）	（任意）[残りの廃止期間（Remaining Retired Period）] ダイアログボックスで [はい（Yes）] を選択した場合にのみ使用できます。廃止期間が終了し、古い共有秘密の設定は解除されます。
シングル接続モードを有効にする（Enable Single Connect Mode）	[シングル接続モードを有効にする（Enable Single Connect Mode）] チェックボックスは、ネットワークデバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかのオプションボタンをクリックします。 • [レガシーシスコデバイス（Legacy Cisco Devices）] • [TACACS ドラフト コンプライアンス シングル接続のサポート（TACACS Draft Compliance Single Connect Support）] （注） このフィールドを無効にすると、Cisco ISE はすべての TACACS+ 要求に新しい TCP 接続を使用します。

デバイス セキュリティ設定

RADIUS 共有秘密の最小長を指定します。新規インストールとアップグレードした展開の場合、デフォルトではこの値は 4 文字になります。RADIUS サーバーでのベスト プラクティスは、22 文字にすることです。

（注） [ネットワーク デバイス（Network Devices）] ページに入力した共有秘密の長さは、[デバイス セキュリティ設定（Device Security Settings）] ページの [RADIUS 共有秘密の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定した値以上でなければなりません。

関連トピック

ネットワーク デバイス定義の設定 （1367 ページ）

ネットワーク デバイスのインポート設定

次の表では、ネットワークデバイスの詳細を Cisco ISE にインポートするために使用できる [ネットワークデバイスのインポート（Import Network Devices）] ウィンドウのフィールドにつ

いて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]**。[ネットワークデバイス（Network Devices）] ウィンドウで、[インポート（Import）] をクリックします。

表 *182 :* ネットワークデバイスのインポート設定

フィールド名	使用上のガイドライン
テンプレートの生成（Generate a Template）	カンマ区切りの値（CSV）テンプレートファイルを作成するには、[テンプレートの生成（Generate a Template）] をクリックします。 CSV形式のネットワークデバイス情報でテンプレートを更新し、ローカルに保存します。次に、編集したテンプレートを使用して、Cisco ISE展開にネットワークデバイスをインポートします。
ファイル（File）	最近作成したか、またはCisco ISE 展開から以前にエクスポートしたCSVファイルを選択するには、**[ファイルの選択（Choose File）]** をクリックします。 [インポート（Import）]オプションを使用して、新規および更新されたネットワークデバイスの情報を含む別のCisco ISE 展開にネットワークデバイスをインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワークデバイスをインポートファイル内のデバイスに置き換えるには、[既存のデータを新しいデータで上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポートファイル内の新しいネットワーク デバイス定義がネットワーク デバイス リポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生したときにCisco ISE にインポートを中止する場合は、[最初のエラー時にインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。Cisco ISE は、エラーが発生するまでネットワークデバイスをインポートします。 このチェックボックスがオンになっておらず、エラーが発生した場合は、エラーが報告され、Cisco ISEは残りのデバイスを引き続きインポートします。

ネットワーク デバイス グループの管理

次のウィンドウを使用すると、ネットワークデバイスグループを設定し、管理することができます。

ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用する [ネットワークデバイスグループ（Network Device Groups）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] > [すべてのグループ（All Groups）]**。

ネットワーク デバイス グループは、**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] > [すべてのグループ（All Groups）]** ウィンドウでも作成できます。

表 *183 : [ネットワーク デバイス グループ（Network Device Group）] ウィンドウのフィールド*

フィールド名	使用上のガイドライン
名前（Name）	ルート ネットワーク デバイス グループの名前を入力します。このルート ネットワークデバイス グループに追加される後続のすべての子ネットワーク デバイス グループに対して、新たに作成したこのネットワーク デバイス グループの名前を入力します。 ネットワーク デバイス グループ階層内には、ルートノードを含めて、最大で 6 つのノードを含めることができます。各ネットワーク デバイス グループの名前には最大で 32 文字を使用できます。
説明（Description）	ルートまたは子のネットワーク デバイス グループの説明を入力します。
ネットワークデバイスの数（No. of Network Devices）	ネットワークグループ内のネットワークデバイスの数がこの列に表示されます。

ネットワーク デバイス グループのインポート設定

次の表では、[ネットワークデバイスグループ（Network Device Group）] ウィンドウの [インポート（Import）] ダイアログボックスのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）]**。

表 *184 : [*ネットワーク デバイス グループのインポート（***Network Device Groups Import***）*]* ウィンドウのフィールド

フィールド名	使用上のガイドライン
テンプレートの生成（Generate a Template）	CSVテンプレートファイルをダウンロードするには、このリンクをクリックします。 同じ形式のネットワーク デバイス グループ情報でテンプレートを更新します。そのテンプレートをローカルに保存し、ネットワーク デバイス グループを Cisco ISE 展開にインポートします。
ファイル（File）	**[ファイルの選択（Choose File）]** をクリックして、アップロードするCSVファイルの場所に移動します。そのファイルは、新規ファイル、または別の Cisco ISE 展開からエクスポートされたファイルである可能性があります。 更新されたネットワーク デバイス グループ情報を使用して、ある Cisco ISE展開から別の展開にネットワークデバイスグループをインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワーク デバイス グループをインポートファイル内のデバイスグループに置き換える場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポートファイル内の新しいネットワーク デバイス グループのみがネットワーク デバイス グループリポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生した最初のインスタンスでインポートを中止するには、このチェックボックスをオンにします。 このチェックボックスをオンにしていないためにエラーが発生した場合は、Cisco ISE はエラーを報告し、残りのデバイスグループを引き続きインポートします。

ネットワーク デバイス プロファイル設定

次の表は、[ネットワークデバイスプロファイル（Network Device Profiles）] ウィンドウのフィールドについての説明です。このページを使用して、プロトコル、リダイレクトURLおよびCoA設定に対するデバイスのサポートなど、特定のベンダーからのネットワークデバイスのタイプに対するデフォルト設定を構成することができます。その後、プロファイルを使用して特定のネットワーク デバイスを定義します。

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイスプロファイル（Network Device Profiles）]** です。

ネットワーク デバイス プロファイルの設定

次の表は、[ネットワーク デバイス プロファイル（Network Device Profile）] セクションのフィールドについての説明です。

表 *185*：ネットワーク デバイス プロファイルの設定

フィールド名	説明
名前（**Name**）	ネットワーク デバイス プロファイルの名前を入力します。
説明（**Description**）	ネットワーク デバイス プロファイルの説明を入力します。
アイコン（**Icon**）	ネットワーク デバイス プロファイルに使用するアイコンを選択します。このアイコンには、選択したベンダーのアイコンがデフォルトで設定されます。 選択するアイコンは 16 X 16 の PNG ファイルである必要があります。
ベンダー（**Vendor**）	ネットワーク デバイス プロファイルのベンダーを選択します。
サポートされるプロトコル	
RADIUS	このネットワーク デバイス プロファイルが RADIUS をサポートしている場合は、このチェックボックスをオンにします。
TACACS+	このネットワーク デバイス プロファイルが TACACS+ をサポートしている場合は、このチェックボックスをオンにします。
TrustSec	このネットワーク デバイス プロファイルが TrustSec をサポートしている場合は、このチェックボックスをオンにします。
RADIUS ディクショナリ（RADIUS Dictionaries）	このプロファイルでサポートされる 1 つ以上の RADIUS ディクショナリを選択します。プロファイルを作成する前に、ベンダー固有の RADIUS ディクショナリをインポートします。

認証/許可テンプレートの設定

次の表は、[認証/許可（Authentication/Authorization）] セクションのフィールドについての説明です。

表 *186 :* 認証/許可の設定

フィールド名	説明
フロータイプの条件（**Flow Type Conditions**）	Cisco ISE では、802.1X、MAC 認証バイパス（MAB）、およびブラウザベースの Web 認証ログインが、有線ネットワークと無線ネットワークの両方を介した基本的なユーザー認証およびアクセスでサポートされます。 このタイプのネットワーク デバイスがサポートする認証ログインのチェックボックスをオンにします。次の 1 つ以上の項目を指定できます。 • 有線 MAC 認証バイパス（MAB）（Wired MAC authentication bypass (MAB)） • 無線 MAB（Wireless MAB） • 有線 802.1x（Wired 802.1X） • 無線 802.1x（Wireless 802.1X） • 有線 Web 認証（Wired Web Authentication） • 無線 Web 認証（Wireless Web Authentication） ネットワーク デバイス プロファイルでサポートされる認証ログインをオンにした後、ログインの条件を指定します。
属性エイリアシング（**Attribute Aliasing**）	ポリシー ルールのフレンドリ名としてデバイスのサービス セット識別子（SSID）を使用する場合は、[SSID]チェックボックスをオンにします。これにより、ポリシールールで使用する一貫した名前を作成できます。
ホスト ルックアップ（**MAB**）	
ホスト ルックアップの処理（**Process Host Lookup**）	ネットワーク デバイス プロファイルで使用されるホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。 さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。デバイスタイプに応じて、使用しているプロトコルの[パスワードを確認（Check Password）] チェックボックス、または[Calling-Station-IdがMACアドレスと等しいかを確認（Checking Calling-Station-Id equals MAC Address）] チェックボックス、あるいはその両方をオンにします。
PAP/ASCII 経由（**Via PAP/ASCII**）	ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。

フィールド名	説明
CHAP 経由（Via CHAP）	ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。 このオプションによって、CHAP 認証が有効になります。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。
EAP-MD5 経由（EAP-MD5）	ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。

権限

このネットワーク デバイス プロファイルに使用される VLAN および ACL の権限を定義できます。プロファイルを保存すると、Cisco ISE は設定された各権限に対し許可プロファイルを自動的に生成します。

表 *187 :* 権限

フィールド名	説明
VLAN の設定（Set VLAN）	このネットワーク デバイス プロファイルに VLAN 権限を設定するには、このチェックボックスをオンにします。次のいずれかのオプションを選択します。 • IETF 802.1X 属性（IETF 802.1X Attributes）：Internet Engineering Task Force で定義されたデフォルトの RADIUS 属性のセットです。 • 一意の属性（Unique Attributes）：複数の RADIUS 属性値のペアを指定できます。
ACL の設定（Set ACL）	RADIUS 属性をネットワーク デバイス プロファイルの ACL に設定する場合は、このチェックボックスをオンにします。

許可変更（CoA）テンプレートの設定

このテンプレートは、CoA がこのタイプのネットワーク デバイスにどのように送信されるかを定義します。次の表は、[許可変更（CoA）（Change of Authorization (CoA)）] セクションのフィールドについての説明です。

表 *188 :* 許可変更（*CoA*）の設定

フィールド名	定義
次による CoA（CoA by）	次のオプションのいずれかを選択します。 • RADIUS • SNMP • サポート対象外
RADIUS による CoA（CoA by RADIUS）	
デフォルトの CoA ポート（Default CoA Port）	RADIUS CoA を送信するポート。シスコ デバイスのデフォルト ポートは 1700 で、他のベンダーのデバイスでは 3799 です。 [ネットワークデバイス（Network Device）] ウィンドウでこれを上書きできます。
タイムアウト間隔（Timeout Interval）	CoA の送信後に Cisco ISE が応答を待機する秒数。
再試行回数（Retry Count）	最初のタイムアウト後に Cisco ISE が CoA の送信を試行する回数。
切断（Disconnect）	これらのデバイスに接続解除要求を送信する方法を選択します。 • **[RFC 5176]**：標準のセッション終了の場合はこのチェックボックスをオンにし、RFC 5176 に従って定義されているように、ポートを新しいセッション用に残しておきます。 • **[ポートバウンス（Port Bounce）]**：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。 • **[ポートのシャットダウン（Port Shutdown）]**：セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。
再認証（Re-authenticate）	ネットワーク デバイスに再認証要求を送信する方法を選択します。これは現在、シスコ デバイスのみでサポートされています。 • **[基本（Basic）]**：標準のセッション再認証の場合はこのチェックボックスをオンにします。 • **[再実行（Rerun）]**：認証方式によって最初から実行する場合は、このチェックボックスをオンにします。 • **[最後（Last）]**：最後に成功した認証方式をセッションに使用します。

フィールド名	定義
CoA プッシュ（CoA Push）	ネットワーク デバイスがシスコの TrustSec CoA 機能をサポートしない場合は、このオプションを選択して、Cisco ISE が設定の変更をデバイスにプッシュできるようにします。
SNMP による CoA（CoA by SNMP）	
タイムアウト間隔（Timeout Interval）	CoA の送信後に Cisco ISE が応答を待機する秒数。
再試行回数（Retry Count）	Cisco ISE が CoA の送信を試行する回数。
NAD ポートの検出（NAD Port Detection）	関連する RADIUS 属性は、現時点での唯一のオプションです。
関連する RADIUS 属性	NAD ポートを検出する方法を選択します。 • Nas-Port • Nas-Port-ID
切断（Disconnect）	これらのデバイスに接続解除要求を送信する方法を選択します。 • **[再認証（Reauthenticate）]**：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。 • **[ポートバウンス（Port Bounce）]**：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。 • **[ポートのシャットダウン（Port Shutdown）]**：セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。

リダイレクト テンプレートの設定

ネットワーク デバイスは、許可プロファイルで設定されている場合、クライアントの HTTP 要求をリダイレクトできます。このテンプレートは、このネットワーク デバイス プロファイルが URL リダイレクトをサポートするかどうかを指定します。デバイス タイプに固有の URL パラメータ名を使用します。

次の表は、[リダイレクト（Redirect）] セクションのフィールドについての説明です。

表 *189 :* リダイレクトの設定

フィールド名	定義
タイプ（**Type**）	ネットワーク デバイス プロファイルが静的または動的 URL リダイレクトをサポートするかを選択します。 デバイスがどちらもサポートしていない場合、[未サポート（Not Supported）] を選択し、**[設定（Settings）] > [DHCPおよびDNSサービス（DHCP & DNS Services）]** から VLAN を設定します。
リダイレクト URL パラメータ名	
クライアントIPアドレス（**Client IP Address**）	ネットワーク デバイスがクライアントの IP アドレスに使用するパラメータ名を入力します。
クライアントMACアドレス（**Client MAC Address**）	ネットワーク デバイスがクライアントの MAC アドレスに使用するパラメータ名を入力します。
元の URL（**Originating URL**）	ネットワーク デバイスが元の URL に使用するパラメータ名を入力します。
セッションID（**Session ID**）	ネットワーク デバイスがセッション ID に使用するパラメータ名を入力します。
SSID	ネットワーク デバイスがサービス セット識別子（SSID）に使用するパラメータ名を入力します。
ダイナミック URL パラメータ	
パラメータ（**Parameter**）	動的 URL リダイレクトを選択する場合は、これらのネットワーク デバイスがリダイレクト URL を作成する方法を指定する必要があります。また、リダイレクト URL がセッション ID またはクライアントの MAC アドレスを使用するかを指定できます。

詳細設定（Advanced Settings）

ネットワーク デバイス プロファイルを使用して、ネットワーク デバイスをポリシー ルールで使いやすくするために、多数のポリシー要素を生成できます。これらの要素には、複合条件、許可プロファイル、および許可されているプロトコルが含まれています。

これらの要素を作成するには、[ポリシー要素の作成（Generate Policy Elements）] をクリックします。

外部 RADIUS サーバーの設定

次の表では、[外部 RADIUS サーバー（External RADIUS Server）] ウィンドウのフィールドについて説明します。これらのフィールドを使用して、RADIUS サーバーを設定できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [外部 RADIUS サーバー（External RADIUS Servers）]**。

表 *190* : 外部 *RADIUS* サーバーの設定

フィールド名	使用上のガイドライン
名前（**Name**）	外部 RADIUS サーバーの名前を入力します。
説明（**Description**）	外部 RADIUS サーバーの説明を入力します。
ホスト名/アドレス（**Host IP**）	外部 RADIUS サーバーの IP アドレスを入力します。IPv4 アドレスを入力する場合は、範囲とサブネット マスクを使用できます。IPv6 では、範囲がサポートされていません。
共有秘密鍵（**Shared Secret**）	外部 RADIUS サーバーの認証に使用される、Cisco ISE と外部 RADIUS サーバーの間の共有秘密を入力します。共有秘密情報は、予期されるテキスト文字列です。ユーザーは、ネットワーク デバイスによってユーザー名およびパスワードが認証されるようにこれらの情報を提示する必要があります。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。共有秘密情報の長さは、最大 128 文字です。
KeyWrap の有効化（**Enable KeyWrap**）	このオプションを有効にすると、AES KeyWrap アルゴリズムにより RADIUS プロトコルのセキュリティが強化され、Cisco ISE で FIPS 140 に準拠可能になります。
キー暗号キー（**Key Encryption Key**）	（[keyWrap を有効にする（Enable keyWrap）] チェックボックスをオンにした場合のみ）セッション暗号化（秘密）に使用される暗号キーを入力します。
メッセージ オーセンティケータ コード キー（**Message Authenticator Code Key**）	（[keyWrap を有効にする（Enable keyWrap）] チェックボックスをオンにした場合のみ）RADIUS メッセージ上のキー付き HMAC 計算に使用されるキーを入力します。

フィールド名	使用上のガイドライン
キー入力形式（**Key Input Format**）	Cisco ISE 暗号キーの入力に使用する形式を指定します。これは、WLAN コントローラ上の設定と一致する必要があります。指定する値の長さは、次に定義されているキーの（最大の）長さと正確に一致している必要があります。これより短い値は許可されません。 • [ASCII]：キー暗号キーの長さは 16 文字（バイト）、メッセージ オーセンティケータ コード キーの長さは 20 文字（バイト）である必要があります。 • [16 進数（Hexadecimal）]：キー暗号キーの長さは 32 バイトであり、メッセージ オーセンティケータ コード キーの長さは 40 バイトである必要があります。
認証ポート（**Authentication Port**）	RADIUS 認証のポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1812 です。
アカウンティング ポート（**Accounting Port**）	RADIUS アカウンティングのポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1813 です。
サーバー タイムアウト（**Server timeout**）	Cisco ISE が外部 RADIUS サーバーからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は 5 ～ 120 です。
接続試行回数（**Connection Attempts**）	Cisco ISE が外部 RADIUS サーバーへの接続を試行する回数を入力します。デフォルトは 3 回に設定されています。有効な値は 1 ～ 9 です。
RADIUS プロキシ フェールオーバーの有効期限（RADIUS Proxy Failover Expiration）	接続に失敗してから、このサーバーに再び接続を試みるまでの経過時間を入力します。有効な範囲は 1 ～ 600 です。 サーバータイムアウトをスキップし、フェールオーバーに直接移動するには、このパラメータを設定します。

RADIUS サーバー順序

次の表では、RADIUS サーバー順序を作成するために使用する [RADIUS サーバー順序（RADIUS Server Sequences）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[RADIUSサーバー順序（RADIUS Server Sequences）]** > [追加（Add）]。

表 *191 : RADIUS* サーバー順序

フィールド名	使用上のガイドライン
名前（**Name**）	RADIUS サーバー順序の名前を入力します。
説明（**Description**）	任意で説明を入力します。
ホスト名/アドレス（**Host IP**）	外部 RADIUS サーバーの IP アドレスを入力します。
ユーザーが選択したサービス タイプ（**User Selected Service Type**）	[使用可能（Available）] リスト ボックスで、ポリシー サーバーとして使用する外部 RADIUS サーバーを選択し、選択した外部 RADIUS サーバーを [選択済み（Selected）] リスト ボックスに移動します。
リモート アカウンティング（**Remote Accounting**）	リモート ポリシー サーバーでアカウンティングを有効にするには、このチェックボックスをオンにします。
ローカル アカウンティング（**Local Accounting**）	Cisco ISE でのアカウンティングを有効にするには、このチェックボックスをオンにします。
高度な属性設定（**Advanced Attributes Settings**）	
サブジェクト名の先頭から最後に出現する区切り文字まで削除（**Strip Start of Subject Name up to the First Occurrence of the Separator**）	プレフィクスからユーザー名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が acme\userA、区切り文字が \ の場合、ユーザー名は userA になります。

フィールド名	使用上のガイドライン
最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip End of Subject Name from the Last Occurrence of the Separator）	サフィックスからユーザー名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が userA@abc.com、区切り文字が @ の場合、ユーザー名は userA になります。 • NetBIOS または User Principle Name（UPN）フォーマットのユーザー名（user@domain.com または /domain/user）からユーザー名を抽出するには、これらのストリップオプションを有効にする必要があります。RADIUS サーバーでユーザーを認証するために、ユーザー名だけが RADIUS サーバーに渡されるためです。 • \ および @ の両方のストリップ機能をアクティブ化し、エージェントを使用している場合、Cisco ISE は最初に出現する \ を文字列から正確に取り除くことができません。ただし、各ストリップ機能は、エージェントを考慮して設計されているため、個別に使用する場合は動作します。
外部 RADIUS サーバーへの要求に含まれる属性を変更する（Modify Attributes in the Request to the External RADIUS Server）	認証済みの RADIUS サーバーとの間で送受信する属性の操作を Cisco ISE に許可するには、このチェックボックスをオンにします。 次の属性操作が可能です。 • [追加（Add）]：RADIUS 要求/応答全体に属性を追加します。 • [更新（Update）]：属性値（固定または静的）を変更します。または属性を別の属性値（動的）で置き換えます。 • [削除（Remove）]：属性または属性と値のペアを削除します。 • [すべて削除（RemoveAny）]：存在するすべての属性を削除します。
認証ポリシーに進む（Continue to Authorization Policy）	ID ストア グループおよび属性の取得に基づいて、プロキシ フローを許可ポリシーの実行に誘導して、より詳細な意思決定を行うには、このチェックボックスをオンにします。このオプションを有効にすると、外部RADIUS サーバーからの応答に含まれる属性が、認証ポリシーの選択に使用されます。このコンテキストの既存の属性は、AAA サーバーの受け入れ応答属性の適切な値で更新されます。
Access-Accept の送信前に属性を変更する（Modify Attributes before send an Access-Accept）	応答をデバイスに返送する直前に属性を変更するには、このチェックボックスをオンにします。

デバイス ポータルの管理

デバイス ポータルの設定

デバイス ポータルのポータル ID 設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータルの管理（Device Portal Managment）] > [ブロックリストポータル（Blocked List Portal）]/[クライアントプロビジョニングポータル（Client Provisioning Portals）]/[BYOD ポータル（BYOD Portals）]/[MDM ポータル（MDM Portals）]/[デバイスポータル（My Device Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの設定およびカスタマイズ（Portals Settings and Customization）]** です。

- [ポータル名（Portal Name）]：このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル（[ブロック済みリスト（Blocked List）]、[個人所有デバイス持ち込み（BYOD）（Bring Your Own Device (BYOD)）]、[クライアント プロビジョニング（Client Provisioning）]、[モバイルデバイス管理（MDM）（Mobile Device Management (MDM)）]、または [デバイス（My Devices）] の各ポータル）に使用しないでください。

  この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- [説明（Description）]：オプションです。

- [ポータルテスト URL（Portal test URL）]：[保存（Save）] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

  リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

（注） テストポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアントプロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

- [言語ファイル（Language File）]：各ポータルタイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

  言語ファイルには、特定のブラウザロケール設定へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。1つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

  1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザー Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイスポータルにも適用されます。

  [ポータルページのカスタマイズ（Portal Page Customizations）] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に1つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

BYOD と MDM ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [BYOD ポータルまたは MDM ポータル（BYOD Portals or MDM Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]**。

これらを設定して、ポータル ページの動作を定義します。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで8443です。ただし、ブロックリストポータルは8444です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート8905および8909も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

  同じHTTPSポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートと

インターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。

- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされたNICのみが選択されている場合は、PSNはポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- NICチーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方のNICは、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSNは物理インターフェイスでポータルを開始しようとします。

- [証明書グループタグ（Certificate Group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループタグを選択します。
- [エンドポイント ID グループ（Endpoint Identity Group）]：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。
- **表示言語**
  - [ブラウザのロケールを使用する（Use Browser Locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語（Fallback Language）] が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback Language）]：ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。

- [常に使用（Always Use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する（User Browser Locale）] オプションを上書きします。

BYOD ポータルの BYOD 設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [BYOD ポータル（BYOD Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [BYOD 設定（BYOD Settings）]**。

この設定を使用して、パーソナル デバイスを使用する従業員の個人所有デバイスの持ち込み（BYOD）機能を有効にし、企業ネットワークにアクセスできるようにします。

フィールド名	使用上のガイドライン
AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）	会社のネットワーク使用の諸条件を、現在ユーザーに表示されているウィンドウ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
同意が必要（Require Acceptance）	ユーザーのアカウントが完全に有効になる前に、ユーザーは AUP に同意する必要があります。[ログイン（Login）] ボタンは、ユーザーが AUP を受け入れない場合は有効になりません。ユーザーが AUP に同意しない場合、ネットワークにアクセスできません。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	このオプションは、[AUP をページに含める（Include an AUP on page）] が有効である場合のみ表示されます。 ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールすると有効になります。
登録時にデバイス ID フィールドを表示する（Display Device ID Field During Registration）	登録プロセス中に、デバイス ID をユーザーに表示します。これは、デバイス ID が事前設定されており、BYOD ポータルを使用しているときに変更できない場合も含みます。

フィールド名	使用上のガイドライン
元の URL（Originating URL）	ネットワークへの認証に成功すると、可能な場合はユーザーのブラウザを、ユーザーがアクセスしようとしていた元の Web サイトにリダイレクトします。使用できない場合は、[認証成功（Authentication Success）] ウィンドウが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の Cisco ISE で設定された認証プロファイルにより、PSN のポート 8443 で動作することを確認します。 Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザード アプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS（dot1X）およびサポート対象外のデバイス（ネットワーク アクセスが許可されている）では、この URL にリダイレクトされます。
成功ページ（Success page）	デバイスの登録が成功したことを示すページを表示します。
URL	ネットワークへの認証に成功すると、ユーザーのブラウザを指定された URL（会社の Web サイトなど）にリダイレクトします。

（注） 認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。

証明書プロビジョニング ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニング ポータル（Certificate Provisioning Portal）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]**。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで 8443 です。ただし、ブロックリストポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。こ

れは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。

- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- NIC チーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループタグ（Certificate Group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループタグを選択します。
- **[認証方式（AuthenticationMethod）]**：ユーザー認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ID ソース順序は、ユーザークレデンシャルを確認するために順番に検索される ID ストアのリストです。

  Cisco ISE には、スポンサーポータル Sponsor_Portal_Sequence 用のデフォルトの ID ソース順序が含まれています。

  IdP を設定するには、**[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

  ID ソース順序を設定するには、[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] を選択します。
- [承認済みグループの設定（Configure Authorized Groups）]：証明書を生成してそれを [選択済み（Chosen）] ボックスに移動するための権限を付与するユーザー ID グループを選択します。
- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：[スポンサー（Sponsor）] ポータルまたは [デバイス（MyDevices）] ポータルの固有の FQDN またはホスト名を 1 つの以上入力します。たとえば、

sponsorportal.yourcompany.com,sponsor と入力することで、ユーザーはブラウザにこれらのいずれかを入力すると、が表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

デフォルトの FQDN を変更する場合は、次を実行します。

- DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
- 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカルサーバー証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。[Kerberos SSO を許可（Allow Kerberos SSO）] オプションがスポンサーポータルで有効になっている場合は、ポータルで使用されるローカルサーバー証明書の SAN 属性に Cisco ISE PSN の FQDN またはワイルドカードを含める必要があります。

- [アイドルタイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザーをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

ログイン ページの設定（Login Page Settings）

- [レート制限までの最大ログイン試行失敗数（Maximum Failed Login Attempts Before Rate Limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [AUP を含める（Include an AUP）]：フローにアクセプタブル ユース ポリシー ウィンドウを追加します。AUP をウィンドウに追加したり、別のウィンドウへのリンクを設定することができます。

利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP ページを含める（Include an AUP Page）]：会社のネットワーク使用諸条件を、別のページでユーザーに表示します。
- [従業員に別の AUP を使用する（Use Different AUP for Employees）]：従業員専用に別の AUP およびネットワーク使用諸条件を表示します。このオプションを選択すると、[従業員用の AUP をスキップ（Skip AUP for employees）] は選択できません。
- [従業員用の AUP をスキップ（Skip AUP for Employees）]：従業員は、ネットワークにアクセスする前に AUP に同意する必要はありません。このオプションを選択すると、[従業員に別の AUP を使用する（Use different AUP for employees）] は選択できません。
- [同意が必要（Require Acceptance）]：ユーザーのアカウントが完全に有効になる前に、ユーザーは AUP に同意する必要があります。[ログイン（Login）] ボタンは、ユーザーが AUP

を受け入れない場合は有効になりません。ユーザーがAUPに同意しない場合、ネットワークにアクセスできません。

- [AUP の最後までのスクロールが必要（Require Scrolling to End of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。

  ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。AUP がユーザーに表示された場合に設定します。

  - [初回のログインのみ（On First Login only）]：ユーザーが初めてネットワークまたはポータルにログインしたときに AUP を表示します。
  - [ログインごと（On Every Login）]：ユーザーがネットワークまたはポータルにログインするごとに、AUP を表示します。
  - [__ 日ごと（初回のログインから）（Every __ Days (starting at first login)）]：ネットワークやポータルにユーザーが初めてログインした後は、AUP を定期的に表示します。

クライアント プロビジョニング ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[クライアントプロビジョニングポータル（Client Provisioning Portals）]** > **[作成、編集、複製または削除（Create, Edit, Duplicate, or Delete）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** です。

ポータル設定

- **[HTTPS ポート（HTTPS Port）]**：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで 8443 です。ただし、**[ブロックリスト（Blocked List）]** ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合、この制限に従うようにポート設定を変更する必要があります。
- **[使用可能インターフェイス（Allowed interfaces）]**：ポータルを実行できる PSN インターフェイスを選択します。PSN で使用可能なインターフェイスを備えた PSN のみがポータルを作成できます。物理およびボンディングされたインターフェイスの任意の組み合わせを設定できます。これはPSN全体の設定です。すべてのポータルはこれらのインターフェイスでのみ動作し、このインターフェイス設定はすべての PSN に適用されます。
  - 異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときのVMベースのものを含む、すべてのPSNで使用できるものでなければなりません。こ

れは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。

- ポータルの証明書のサブジェクト名とサブジェクトの代替名は、インターフェイス IP に解決される必要があります。
- ISE CLI の ip host x.x.x.x yyy.domain.com をセカンダリ インターフェイス IP と FQDN をマッピングするように設定します。これは証明書のサブジェクト名/サブジェクトの代替名を一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディング インターフェイスの設定を試みます。これが成功しない場合、その PSN にボンドセットがなかったことが原因である可能性があるので、PSN はエラーを記録して終了します。物理インターフェイスでポータルを開始しようとはしません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- **[証明書グループタグ（Certificate group tag）]**：ポータルの HTTPS トラフィックに使用する証明書グループのグループタグを選択します。
- **[認証方式（Authentication Method）]**：ユーザー認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザー クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザー、内部ユーザー、Active Directory、LDAP などがあります。

  Cisco ISE には、クライアント プロビジョニング ポータル用のデフォルトのクライアント プロビジョニング ID ソース順序 Certificate_Portal_Sequence が含まれています。
- **[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]**：クライアント プロビジョニング ポータル用に少なくとも 1 つの一意の FQDN、ホスト名、またはその両方を入力します。たとえば、「provisionportal.yourcompany.com」と入力した場合、ユーザーはこれらのいずれかをブラウザに入力して証明書プロビジョニング ポータルに到達できます。
  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに確実に解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。

- 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバー証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

（注） URL リダイレクトなしのクライアント プロビジョニングの場合、[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）] フィールドに入力するポータル名は、DNS 設定で設定されている必要があります。URL リダイレクトなしのクライアント プロビジョニングを有効にするため、この URL をユーザーに通知する必要があります。

- **[アイドルタイムアウト（Idle timeout）]**：ポータルでアクティビティがない場合にユーザーをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

（注） クライアント プロビジョニング ポータルではポート番号と証明書を定義できます。これにより、ホストはクライアント プロビジョニングとポスチャに同じ証明書をダウンロードすることを許可します。ポータル証明書が正式な認証局により署名されている場合、セキュリティ警告は表示されません。自己署名証明書の場合、ポータルと Cisco エージェント ポスチャ コンポーネントの両方でセキュリティ警告を受け取ります。

ログイン ページの設定（Login Page Settings）

- [ログインの有効化（Enable Login）]：クライアント プロビジョニング ポータルのログイン手順を有効にするには、このチェックボックスを選択します
- [レート制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：単一のブラウザセッションからのログイン試行失敗回数を指定します。この回数を超過すると、Cisco ISE はログイン試行を実行できる頻度を意図的に低下させて、追加のログイン試行を防ぎます。ログイン失敗がこの回数に達した後のログイン試行の間隔は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で指定されます。
- [頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）]：[レート制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザーが再度ログインを試行するまでに待機する必要がある時間を分単位で設定します。
- [AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）]：会社のネットワーク使用の契約条件を、現在ユーザーに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。

- [同意が必要（Require acceptance）]：ポータルにアクセスする前にユーザーが AUP を受け入れることを要求します。[ログイン（Login）] ボタンは、ユーザーが AUP を受け入れない場合は有効になりません。AUP を受け入れないユーザーは、ポータルにアクセスできません。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。

利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP を含める（Include an AUP）]：会社のネットワーク使用の契約条件を、別のページでユーザーに表示します。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：ユーザーが AUP を完全に読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。
- [初回のログインのみ（On first login only）]：ユーザーがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
- [ログインごと（On every login）]：ユーザーがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [_ 日ごと（初回のログインから）（Every _____ days (starting at first login)）]：ネットワークやポータルにユーザーが初めてログインした後は、AUP を定期的に表示します。

ポストログイン バナー ページ設定（Post-Login Banner Page Settings）

[ポストログインバナーページを含める（Include a Post-Login Banner page）]：ユーザーが正常にログインした後、ネットワークアクセスを付与される前に追加情報を表示します。

パスワード変更設定（Change Password Settings）

[内部ユーザーに自身のパスワードの変更を許可する（Allow internal users to change their own passwords）]：従業員がクライアントプロビジョニング ポータルにログインして、自分のパスワードを変更できるようにします。これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

MDM ポータルの従業員のモバイル デバイス管理設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [MDM ポータル（MDM Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] > [従業員のモバイル デバイス管理設定（Employee Mobile Device Management Settings）]**。

これらの設定を使用して、MDMポータルを使用する従業員のモバイルデバイス管理（MDM）機能を有効にし、AUP エクスペリエンスを定義します。

フィールド名	使用上のガイドライン
AUPをページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）	会社のネットワーク使用の諸条件を、現在ユーザーに表示されているウィンドウ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
同意が必要（Require Acceptance）	ユーザーのアカウントが完全に有効になる前に、ユーザーは AUP に同意する必要があります。[ログイン（Login）] ボタンは、ユーザーが AUP を受け入れない場合は有効になりません。ユーザーが AUP に同意しない場合、ネットワークにアクセスできません。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	このオプションは、[AUP をページに含める（Include an AUP on page）] が有効である場合のみ表示されます。 ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールすると有効になります。

デバイス ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]**。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで8443です。ただし、ブロックリストポータルは8444です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート8905および8909も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

  同じHTTPSポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。

- スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
- スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
- スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**

- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。

- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされたNICのみが選択されている場合は、PSNはポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- NICチーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方のNICは、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSNは物理インターフェイスでポータルを開始しようとします。

- [証明書グループタグ（Certificate Group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループタグを選択します。
- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：[スポンサー（Sponsor）] ポータルまたは [デバイス（MyDevices）] ポータルの固有の FQDN またはホスト名を 1 つの以上入力します。たとえば、**sponsorportal.yourcompany.com,sponsor** と入力することで、ユーザーはブラウザにこれらのいずれかを入力すると、が表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

  デフォルトの FQDN を変更する場合は、次を実行します。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバー証明書のサブジェクト代替名（SAN）属性に、カスタマイズされたURLの FQDN またはワイルドカードを含めます。[Kerberos SSO を許可（Allow Kerberos SSO）] オプションがスポンサーポータルで有効になっている場合は、ポータルで使用されるローカルサーバー証明書の SAN 属性に Cisco ISE PSN の FQDN またはワイルドカードを含める必要があります。

- **[認証方式（AuthenticationMethod）]**：ユーザー認証に使用する ID ソース順序（ISS）またはIDプロバイダー（IdP）を選択します。ID ソース順序は、ユーザー クレデンシャルを確認するために順番に検索される ID ストアのリストです。

  Cisco ISE には、スポンサーポータル Sponsor_Portal_Sequence 用のデフォルトの ID ソース順序が含まれています。

IdP を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

ID ソース順序を設定するには、[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] を選択します。

- [エンドポイント ID グループ（Endpoint Identity Group）]：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

- [__日に達した場合にこの ID グループ内のエンドポイントを消去する（Purge Endpoints in this Identity Group when they Reach __ Days）]：Cisco ISE データベースからデバイスが消去されるまでの日数を指定します。消去は毎日実行され、消去アクティビティは全体的な消去タイミングと同期されます。変更は、このエンドポイント ID グループ全体に適用されます。

  その他のポリシー条件に基づいてエンドポイント消去ポリシーに変更が加えられた場合、この設定は使用できなくなります。

- [アイドルタイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザーをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

- **表示言語**

  - [ブラウザのロケールを使用する（Use Browser Locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語（Fallback Language）] が言語ポータルとして使用されます。

  - [フォールバック言語（Fallback Language）]：ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。

  - [常に使用（Always Use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する（User Browser Locale）] オプションを上書きします。

デバイス ポータルのログイン ページ設定

- [レート制限までの最大ログイン試行失敗数（Maximum Failed Login Attempts Before Rate Limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッ

ションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。

- [レート制限までの最大ログイン試行失敗数（Maximum Failed Login Attempts Before Rate Limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [AUP を含める（Include an AUP）]：フローにアクセプタブル ユース ポリシー ウィンドウを追加します。AUPをウィンドウに追加したり、別のウィンドウへのリンクを設定することができます。

デバイス ポータルの利用規定ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [アクセプタブルユースポリシー（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]** です。

これらの設定を使用して、ユーザー（状況に応じてゲスト、スポンサーまたは従業員）に対して AUP エクスペリエンスを定義します。

フィールド	使用上のガイドライン
AUP ページを含める（Include AUP Page）	会社のネットワーク使用諸条件を、別のページでユーザーに表示します。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールすると有効になります。
初回ログイン時のみ（On First Login only）	ユーザーがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
ログインごと（On Every Login）	ユーザーがネットワークまたはポータルにログインするごとに、AUP を表示します。

フィールド	使用上のガイドライン
__日ごと（初回のログインから）（Every __ Days (starting at first login)）	ユーザーがネットワークまたはポータルに初めてログインした後に、定期的に AUP を表示します。

デバイス ポータルのポストログイン バナー ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポストログイン バナー ページ設定（Post-Login Banner Page Settings）]**。

これらの設定を使用して、正常なログイン後にユーザー（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

フィールド名	使用上のガイドライン
ポストログインバナーページを含める（Include a Post-Login Banner page）	ユーザーが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

デバイス ポータルの従業員によるパスワード変更の設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [従業員のパスワード変更設定（Employee Change Password Settings）]**。これらの設定を使用して、デバイス ポータルを使用している従業員のパスワード要件を定義します。

従業員のパスワードポリシーを設定するには、**[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザー名パスワード ポリシー（Username Password Policy）]** を選択します。

フィールド名	使用上のガイドライン
内部ユーザーにパスワードの変更を許可する（Allow internal users to change password）	従業員が、デバイス ポータルにログインした後で、自分のパスワードを変更することを許可します。 これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

デバイス ポータルのデバイス管理設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [マイデバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [デバイスの管理（Manage Device）]**。

[ページのカスタマイズ（Page Customizations）] で、マイデバイスポータルの [アカウントの管理（Manage Accounts）] タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

[設定（Settings）] では、このポータルを使用する従業員が各自の登録されたパーソナルデバイスで実行可能なアクションを指定できます。

表 *192* : デバイス ポータルのデバイス管理設定

フィールド名	使用上のガイドライン
紛失（Lost）	デバイスを紛失したことを従業員が示すことができるようにします。このアクションは、マイデバイスポータルのデバイスのステータスを [紛失（Lost）] に更新し、ブロック済みリストのエンドポイントの ID グループにそのデバイスを追加します。
復元（Reinstate）	このアクションでは、ブロックリストに記載されているか、紛失したか、または盗難されたデバイスを復元し、そのステータスを最後の既知の値にリセットします。このアクションでは、ネットワークに接続する前に追加プロビジョニングを実行する必要があるため、盗難デバイスのステータスを [未登録（Not Registered）] にリセットします。 ブロックリストに記載されているデバイスを従業員が復元できないようにする場合は、デバイスポータルでこのオプションを有効にしないでください。
削除（Delete）	登録済みデバイスの最大数に到達した場合、従業員が、登録されたデバイスをデバイスポータルから削除したり、未使用のデバイスを削除して新しいデバイスを追加したりできるようにします。このアクションによって、デバイス ポータルに表示されるデバイス リストからデバイスが削除されますが、デバイスは Cisco ISE データベースに残り、エンドポイントのリストに表示されます。 BYOD またはマイデバイスポータルを使用して従業員が登録できるパーソナルデバイスの最大数を定義するには、**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員登録済みデバイス（Employee Registered Devices）]** を選択します。 Cisco ISE データベースからデバイスを完全に削除するには、**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

フィールド名	使用上のガイドライン
盗難（**Stolen**）	デバイスが盗まれたことを従業員が示すことができるようにします。このアクションは、マイデバイスポータルのデバイスのステータスを [盗難（Stolen）] に更新し、ブロック済みリストのエンドポイントの ID グループにそのデバイスを追加し、証明書を削除します。
デバイスロック（**Device lock**）	MDM 登録デバイスのみ。 デバイスの紛失または盗難が発生した場合、従業員がすぐにデバイス ポータルからリモートでデバイスをロックできるようにします。このアクションによって、デバイスの不正使用が防止されます。 ただし、デバイス ポータルでは PIN を設定できないため、従業員が事前にモバイル デバイスに設定しておく必要があります。
登録解除（**Unenroll**）	MDM 登録デバイスのみ。 職場でデバイスを使用する必要がなくなった場合に、従業員がこのオプションを選択できるようにします。このアクションでは、会社がインストールしているアプリケーションと設定のみが削除され、従業員のモバイル デバイス上の他のアプリケーションおよびデータは維持されます。
完全消去（**Full wipe**）	MDM 登録デバイスのみ。 デバイスを紛失したり、新しいものに交換したりした場合に、従業員がこのオプションを選択できるようにします。このアクションでは、従業員のモバイル デバイスを工場出荷時のデフォルト設定にリセットし、インストール済みのアプリケーションとデータを削除します。

デバイス ポータルのデバイス カスタマイズの追加、編集、および検索

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [デバイスの追加、デバイスの編集またはデバイスの検索（Add Devices, Edit Devices or Locate Devices）]** です。

[ページのカスタマイズ（Page Customizations）] で、デバイス ポータルの [追加（Add）]、[編集（Edit）]、および [検索（Locate）] の各タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

デバイス ポータルのサポート情報ページの設定

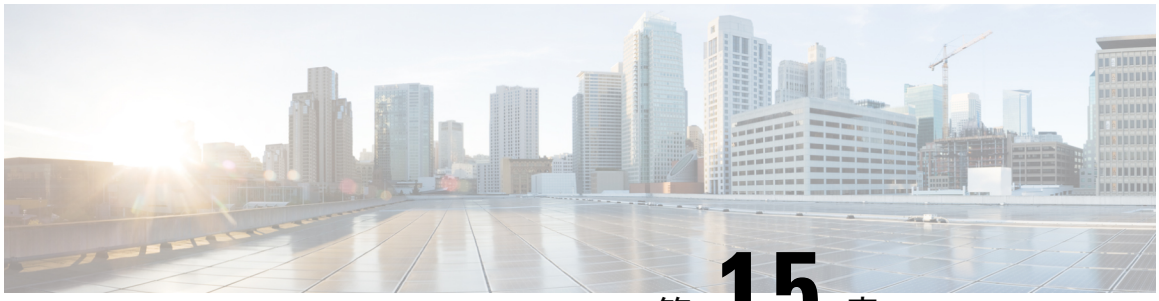
このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [BYOD ポータル（BYOD Portals）]/[クライアントプロビジョニングポータル（Client Provisioning Portals）]/[MDM ポータル（MDM Portals）]/[デバイスポータル（My Device Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフ**

ローの設定（Portal Behavior and Flow Settings）] > [サポート情報ページの設定（Support Information Page Settings）] です。

これらの設定を使用して、ヘルプデスクがユーザー（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

フィールド名	使用上のガイドライン
サポート情報ページを含める（Include a Support Information Page）	該当ポータルのすべての有効なページ上で、[問い合わせ先（Contact Us）] などの情報へのリンクを表示します。
MAC アドレス（MAC Address）	[サポート情報（Support Information）] ウィンドウにデバイスの MAC アドレスを含めます。
IP アドレス（IP Address）	[サポート情報（Support Information）] ウィンドウにデバイスの IP アドレスを含めます。
ブラウザのユーザーエージェント（Browser User Agent）	[サポート情報（Support Information）] ページに、要求の発信元の製品名とバージョン、レイアウトエンジン、ユーザーエージェントのバージョンなど、ブラウザの詳細を含めます。
ポリシーサーバー（Policy Server）	[サポート情報（Support Information）] ウィンドウに、このポータルを提供している ISE ポリシーサービスノード（PSN）の IP アドレスを含めます。
障害コード（Failure code）	可能な場合は、ログ メッセージ カタログ内の対応する番号を含めます。メッセージカタログを表示するには、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージカタログ（Message Catalog）]** を選択します。
フィールドを非表示にする（Hide Field）	含める情報が存在しない場合、[サポート情報（Support Information）] ウィンドウ上の該当するフィールドのラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード（Failure Code）] は、選択されている場合でも表示されません。
値のないラベルを表示（Display label with no value）	含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを [サポート情報（Support Information）] ウィンドウに表示します。たとえば、障害コードが不明な場合、[障害コード（Failure Code）] は空白であっても表示されます。

フィールド名	使用上のガイドライン
デフォルト値でラベルを表示（**Display Label with Default Value**）	含める情報が存在しない場合、[サポート情報（Support Information）] ウィンドウ上の選択されているすべてのフィールドにこのテキストが表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード（Failure code）] に [使用できません（Not Available）] と表示されます。



第 15 章

Cisco pxGrid

• Cisco pxGrid と ISE （1931 ページ）

Cisco pxGrid と ISE

（注） Cisco ISE リリース 3.1 以降、すべての pxGrid 接続は pxGrid 2.0 に基づく必要があります。pxGrid 1.0 ベース（XMPP ベース）の統合は、リリース 3.1 以降の Cisco ISE では動作しなくなります。

WebSocket に基づく pxGrid バージョン 2.0 は、Cisco ISE リリース 2.4 で導入されました。統合の中断を防ぐために、他のシステムを計画して pxGrid 2.0 準拠バージョンにアップグレードすることをお勧めします。

Cisco Platform Exchange Grid（pxGrid）は、オープンで拡張性のある Security Product Integration Framework であり、双方向のエニーツーエニー パートナー プラットフォーム統合を可能にします。

pxGrid 2.0 は REST および WebSocket インターフェイスを使用します。クライアントは、制御メッセージ、クエリ、アプリケーションデータに REST を使用し、イベントをプッシュするために Websocket を使用します。pxGrid 2.0 の詳細については、『Welcome to Learning Cisco Platform Exchange Grid (pxGrid)』を参照してください。

Cisco pxGrid Direct の詳細については、Cisco pxGrid Direct （1195 ページ）を参照してください。

pxGrid は次のことができます。

- Cisco ISE セッションディレクトリからの状況依存情報を、Cisco ISE エコシステムのパートナーシステムなどの他のネットワークシステムや他のシスコプラットフォームと共有する。
- サードパーティシステムが適応型のネットワーク制御アクションを呼び出し、ネットワークまたはセキュリティイベントに応じてユーザーおよびデバイスを検疫できるようにする。タグ定義、値、説明などの TrustSec 情報を、TrustSec トピックを介して Cisco ISE から別のネットワークに渡す。

- 完全修飾名（FQN）を持つエンドポイントプロファイルを、エンドポイントプロファイルメタ トピックを通して Cisco ISE から他のネットワークに渡す。
- タグおよびエンドポイントプロファイルを一括ダウンロードする。
- pxGrid 経由で SXP バインディング（IP-SGT マッピング）を発行および登録する。SXP バインディングの詳細については、『Cisco ISE Administrators Guide』の「Segmentation」章の「Security Group Tag Exchange Protocol」セクションを参照してください。
- Cisco pxGrid Context-in を使用すると、エコシステムパートナーはトピック情報を Cisco ISE に公開できます。これにより、Cisco ISE は、エコシステムで特定された資産に基づいてアクションを実行できます。Cisco pxGrid Context-in の詳細については、「pxGrid Context-In」を参照してください。

pxGrid の概要

pxGrid には次のコンポーネントがあります。

- コントローラ：検出、認証、および許可を処理します。
- プロバイダー：クエリ結果を返すか、または発行します。
- Pubsub：プロバイダーとコンシューマに pxGrid サービスを提供します。
- サブスクライバ：サブスクライバは、承認されると、登録しているトピックからコンテキスト情報とアラートを取得します。

pxGrid には次の機能があります。

- 検出：サービス名に基づいてサービスプロパティを検出します。フローは、プロバイダーが pxGrid コントローラで「サービスの登録」を要求したときに開始されます。登録後、コンシューマは「ルックアップサービス」を使用してプロバイダーの場所を検出します。
- 認証：pxGrid コントローラは、サービスにアクセスするために pxGrid クライアントを認証します。ログイン情報は、ユーザー名とパスワード、または証明書（推奨）です。
- 許可：pxGrid は操作要求を取得すると、pxGrid コントローラに問い合わせて要求を許可し、クライアントを事前定義されたグループに割り当てます。

pxGrid 2.0 のハイアベイラビリティ

pxGrid 2.0 ノードはアクティブ/アクティブ構成で動作します。ハイアベイラビリティを実現するには、導入環境に少なくとも 2 つの pxGrid ノードが必要です。大規模な導入では、拡張性と冗長性を高めるために最大4つのノードを使用できます。あるノードがダウンした場合に、そのノードのクライアントが動作中のノードに接続できるように、すべてのノードの IP アドレスを設定することをお勧めします。PAN がダウンすると、pxGrid サーバーは、アクティブ化処理を停止します。pxGrid サーバーをアクティブにするには、PAN を手動で昇格させます。pxGrid の展開の詳細については、『**ISE Performance & Scale**』を参照してください。

すべての pxGrid サービスプロバイダーのクライアントは、7.5 分以内に pxGrid コントローラに定期的に再登録します。クライアントが再登録しない場合、PAN ノードは非アクティブである

と見なし、そのクライアントを削除します。PAN ノードが 7.5 分を超えてダウンした場合、再度起動すると、タイムスタンプ値が 7.5 分よりも古いすべてのクライアントが削除されます。これらのクライアントはすべて、pxGrid コントローラに再度登録する必要があります。

pxGrid 2.0 クライアントでは、PubSub やクエリに WebSocket および REST ベースの API を使用しています。これらの API は、ポート 8910 で ISE アプリケーションサーバーによって提供されます。`show logging application pxgrid` を実行して表示される pxGrid プロセスは、pxGrid 2.0 には適用されません。

（注） GUI および CLI で pxGrid 1.0 プロセスへのすべての参照が削除されました。

損失検出

Cisco ISE 3.0 では、pxGrid トピックにシーケンス ID が追加されました。送信に中断がある場合、サブスクライバは ID のシーケンスのギャップをチェックすることで中断を認識できます。サブスクライバはトピックシーケンス ID の変更に気付き、最後のシーケンス番号の日付に基づいてデータを要求します。パブリッシャがダウンして復帰した場合、トピックシーケンスは 0 から始まります。サブスクライバはシーケンス 0 を確認したら、キャッシュをクリアして一括ダウンロードを開始する必要があります。サブスクライバがダウンした場合、パブリッシャはシーケンス ID を割り当て続けます。サブスクライバが再接続し、シーケンス ID にギャップがある場合、サブスクライバは最後のシーケンス番号の時刻からデータを要求します。損失検出は、セッションディレクトリおよび TrustSec 構成で機能します。セッションディレクトリを使用している場合、損失を検出したクライアントは、キャッシュをクリアして一括ダウンロードを開始する必要があります。

シーケンス ID を使用しない既存のアプリケーションがある場合は、シーケンス ID を使用する必要はありません。ただし、シーケンス ID を使用すると、損失検出と損失からの回復という利点を得られます。

セッションディレクトリのセッションは、`/topic/com.cisco.ise.session` への通知間隔ごとに MnT によって非同期的にバッチ処理され、公開されます。

TrustSec セキュリティグループへの変更
は、`/topic/com.cisco.ise.config.trustsec.security.group` に公開されます。

損失検出は pxGrid 2.0 でのみサポートされ、デフォルトで有効になっています。

損失検出を使用したコード例、https://github.com/cisco-pxgrid/pxgrid-rest-ws/tree/master/java/src/main/java/com/cisco/pxgrid/samples/ise を参照してください。

モニタリングとデバッグ

pxGrid では、次のログを使用できます。

- pxgrid-server.log：pxGrid 2.0 のアクティビティとエラー

[ログ（Logs）] ページには、すべての pxGrid 2.0 管理イベントが表示されます。イベント情報には、クライアント名と機能名、およびイベントタイプとタイムスタンプが含まれています。

[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [診断（Diagnostics）] > [ログ（Log）]の順に移動して、イベントリストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

pxGrid フェールオーバーとリカバリ

プライマリ pxGrid ノードとセカンダリ pxGrid ノードがそれぞれ少なくとも 1 つ含まれたマルチ pxGrid ノードでの展開で、さまざまなフェールオーバーシナリオにおける pxGrid のリカバリにかかる時間は、ダウンして復帰するノードやその他の特定の変数によって異なります。そのうちの一部の詳細について、以下に示します。

以下に、4 つの異なる pxGrid フェールオーバーおよびリカバリのシナリオと、各ケースで内部的にトリガーされるワークフローを示します。

- **プライマリ pxGrid ノードがダウンする**

  セカンダリ pxGrid ノード MnT は、引き続きセッションデータのパブリッシャとなります。Firewall Management Center（FMC）がプライマリノードに接続されている場合、再試行に数回失敗すると、セカンダリノードに接続して登録されます。中断が発生したため、FMC で一括ダウンロードを実行します。

  FMC がすでにセカンダリ pxGrid ノードに登録されている場合、リカバリはさらにスムーズになります。中断がないため、FMC で一括ダウンロードを実行する必要はありません。したがって、リカバリがさらにスムーズになります。このシナリオでのリカバリの所要時間は 2 分程度です。

- **プライマリ pxGrid ノードが復旧する**

  FMC は引き続きセカンダリ pxGrid ノードに接続され、セカンダリノードでセッションデータの公開が継続されるため、中断は少なくなります。この場合、一括ダウンロードは不要であるため、前のシナリオの場合と同様にリカバリがスムーズになります。

  すべてのファンアウトが再確立され、データベースの同期が完了した後にのみ、FMC で pxGrid との接続が再確立され、プライマリ pxGrid ノードに接続できます。

- **セカンダリ pxGrid ノードがダウンする**

  FMC がプライマリノード pxGrid に接続されている場合は、引き続き同じ場所に接続されます。ただし、これまではセカンダリ MnT ノードがセッショントピックデータのパブリッシャであったため、中断が発生します。プライマリ MnT ノードでセカンダリ MnT ノードがダウンしていることを認識するまでには時間がかかりますが、認識されると、プライマリノードからセッショントピックデータの公開が開始されます。

  FMC がセカンダリノードの pxGrid に接続されている場合は接続を再試行し、失敗した場合はプライマリ PxGrid ノードに接続して登録されます。これは、前の手順と並行して行われます。セカンダリ pxGrid ノードとの再接続が成功すると、FMC は一括ダウンロードを実行します。

- **セカンダリ pxGrid ノードが復旧する**

  これは、リカバリに最も時間がかかるシナリオです。セカンダリノードがダウンしている間に pxGrid 関連のデータベースに変更があった場合、データベースの同期操作が完了す

るまで pxGrid が機能しない可能性があります。データベースの同期にかかる時間は、コンフィギュレーション データベースのサイズによって異なります。

セカンダリ pxGrid ノードは、セッションデータのパブリッシャに戻ります。

更新された展開の通知がすべてのモジュールに送信され、pxgrid モジュールがこの通知を受信すると、データの内部配布に使用されるすべてのファンアウトが再確立されます。これが完了するまで、pxGrid は完全には機能しません。

FMC を再接続する必要がある場合、再接続に成功すると FMC で一括ダウンロードが実行されます。

pxGrid のフィルタリング

Cisco ISE リリース 3.4 以降、pxGrid はクライアントの特定の要件に基づいた情報のフィルタリングをサポートします。現在、pxGrid フィルタリングは次のトピックでサポートされています。

- TrustSec SXP
- セッションディレクトリ - セッショントピック
- セッションディレクトリ - グループトピック

Cisco ISE 3.3 より前のリリースでは、pxGrid はパブリッシャから受信したすべての情報をクライアントにパブリッシュしていました。pxGrid フィルタリング機能を使用すると、クライアントは各サブスクリプションのパブリッシャから関連情報のみを受信できます。pxGrid 情報は、次の 2 つの時点で適用されたフィルタに基づいてフィルタリングされます。

1. 一括ダウンロードの前
2. ライブデータをクライアントにパブリッシュする前

サブスクリプション中に一括ダウンロードとライブデータのフィルタを使用する方法の詳細と作業例については、pxGrid GitHub ページおよび『Cisco pxGrid API Reference Guide』を参照してください。

pxGrid の概要ページ

pxGrid の [概要（Summary）] ページには、現在の pxGrid 2.0 環境の統計情報が表示されます。

- [現在の接続（Current Connections）]：コントローラへの接続のリストが表示されます。
- [制御メッセージ（Control Messages）]：認証、認可、およびサービスディスカバリ。
- [REST API]：WebSocket または XMPP を使用して接続したクライアントの数。
- [PubSub スループット（Pubsub Throughput）]：クライアントにパブリッシュされたデータの量。
- [クライアント（Clients）]：REST または WebSocket によって接続されたクライアント。

- [エラー（Errors）]：クライアントがデータ転送の再開を要求する原因となった送信エラーの数。

pxGrid クライアント管理

クライアントは、Cisco ISEで pxGrid サービスを使用するためにアカウントを登録して承認を受ける必要があります。クライアントは、登録するために pxGrid SDK を介して pxGrid クライアントライブラリを使用します。Cisco ISE は、自動と手動両方の登録をサポートします。

- [クライアント（Clients）]：[管理（Administration）]>[pxGridサービス（pxGrid Services）]>[クライアント管理（Client Management）]>[クライアント（Clients）]を選択して、このウィンドウを表示します。pxGrid 2.0 の外部クライアントアカウントが一覧表示されます。
- [pxGridポリシー（pxGrid Policy）]：[管理（Administration）]>[pxGridサービス（pxGrid Services）]>[クライアント管理（Client Management）]>[pxGridポリシー（pxGrid Policy）]を選択して、このウィンドウを表示します。クライアントが登録できる使用可能なサービスのリストが表示されます。ポリシーを編集して、そのポリシーにアクセスできるグループを変更できます。まだポリシーがないサービスに新しいポリシーを作成することもできます。
- [グループ（Groups）]：[管理（Administration）]>[pxGridサービス（pxGrid Services）]>[クライアント管理（Client Management）]>[グループ（Groups）]を選択して、このウィンドウを表示します。ANC は事前定義されたグループです。他のグループを追加し、それらのグループを使用してサービスへのアクセスを制限できます。

  pxGrid クライアントは、REST API を介してユーザー名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。
- [証明書（Certificates）]：[管理（Administration）]>[pxGridサービス（pxGrid Services）]>[クライアント管理（Client Management）]>[証明書（Certificates）]を選択して、このウィンドウを表示します。Cisco ISE 内部認証局を使用する新しい証明書を生成できます。

  pxGrid の証明書の作成方法については、次を参照してください。
  - Deploying Certificates with Cisco pxGrid - Using Self-Signed Certificates Updates to Cisco ISE 2.0/2.1/2.2
  - Deploying Certificates with Cisco pxGrid - Using External CA with updates to Cisco ISE 2.0/2.1/2.2

pxGrid ポリシーの制御

pxGrid クライアントがアクセスできるサービスへのアクセスを制御する pxGrid 認証ポリシーを作成できます。これらのポリシーは、pxGrid クライアントで使用できるサービスを制御します。

さまざまなタイプのグループを作成して、pxGrid クライアントで使用可能なサービスをこれらのグループにマッピングできます。[クライアント管理（Client Management）]>[グループ

（Groups）] ウィンドウの [グループの管理（Manage Groups）] オプションを使用して、新しいグループを追加します。**[クライアント管理（Client Management）] > [ポリシー（Policies）]** ウィンドウでは、許可ルールの例を表示できます。

pxGrid クライアントの認証ポリシーを作成するには、次の手順を実行します。

ステップ 1 [管理（Administration）] > [pxGridサービス（pxGrid Services）] > [クライアント管理（Client Management）] > [ポリシー（Policy）] を選択し、[追加（Add）] をクリックします。

ステップ 2 [サービス（Service）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- com.cisco.ise.radius
- come.cisco.ise.sxp
- com.cisco.ise.trustsec
- com.cisco.ise.session
- com.cisco.ise.system
- com.cisco.ise.mdm
- com.cisco.ise.config.trustsec
- com.cisco.ise.config.profiler
- com.cisco.ise.pxgrid.admin
- com.cisco.ise.config.deployment.node
- com.cisco.ise.endpoint
- com.cisco.ise.config.anc
- com.cisco.ise.dnac
- com.cisco.ise.config.upn
- com.cisco.ise.pubsub

ステップ 3 [操作（Operations）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- <ANY>
- publish
- publish /topic/com.cisco.ise.session
- publish /topic/com.cisco.ise.session.group
- publish /topic/com.cisco.ise.anc
- <CUSTOM>：このオプションを選択すると、カスタム操作を指定できます。

ステップ 4 [グループ（Groups）] ドロップダウン リストから、このサービスにマッピングするグループを選択します。

（EPSやANCなどの）事前定義されたグループ、および手動で追加したグループがこのドロップダウンリストに表示されます。

（注） ポリシーに含まれるグループの一部であるクライアントのみが、そのポリシーで指定されたサービスに登録できます。

ステップ 5 [送信（Submit）] をクリックします。

pxGridサービスの有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）]**。

ステップ 2 クライアントの隣にあるチェックボックスをオンにして [承認（Approve）] をクリックします。

ステップ 3 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

ステップ 4 有効にする機能を選択し、[有効（Enable）] をクリックします。

ステップ 5 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

pxGrid 診断

- [WebSocket] : [管理（Administration）] > [pxGridサービス（pxGrid Services）] > [診断（Diagnostics）] > [WebSocket] ウィンドウには、pxGrid 2.0 クライアント（外部および内部）のリストが表示されます。また、使用可能な pxGrid 2.0 トピック、および各トピックを公開または登録するクライアントのリストも表示されます。
- [ログ（Log）] : [管理（Administration）] > [pxGridサービス（pxGrid Services）] > [診断（Diagnostics）] > [ライブログ（Live Logs）] ウィンドウに管理イベントのリストが表示されます。
- [テスト（Tests）] : [管理（Administration）] > [pxGridサービス（pxGrid Services）] > [診断（Diagnostics）] > [テスト（Tests）] > [ヘルスモニタリングテスト（Health Monitoring test）] を選択し、[テストの開始（Start Test）] をクリックして、クライアントがセッションディレクトリ サービスにアクセスできることを確認します。テストが完了すると、テストアクティビティのログを表示できます。

pxGrid 設定

[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [設定（Settings）] ウィンドウで、次のオプションのいずれかを選択します。

- [新しい証明書ベースのアカウントを自動的に承認する（Automatically approve new certificate-based accounts）]：このオプションはデフォルトで無効になっています。これにより、pxGrid サーバーへの接続を制御できます。環境内のすべてのクライアントを信頼している場合にのみ、このオプションを有効にします。
- [パスワードベースのアカウント作成の許可（Allow password based account creation）]：このチェックボックスをオンにすると、pxGrid クライアントのユーザー名/パスワードベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

Cisco pxGrid 証明書の生成

始める前に

- Cisco ISE pxGrid サーバーと pxGrid クライアントに同じ証明書を使用しないでください。pxGrid クライアントにはクライアント証明書を使用する必要があります。クライアント証明書を生成するには、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）]** を選択します。
- Cisco ISE の一部のバージョンには NetscapeCertType を使用する Cisco pxGrid の証明書があります。新しい証明書を生成することを推奨します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- pxGrid 証明書はプライマリ PAN から生成する必要があります。
- Cisco pxGrid 証明書がサブジェクト代替名（SAN）の拡張を使用する場合、DNS 名のエントリとしてサブジェクト ID の FQDN が含まれるようにします。
- デジタル署名を使用して証明書テンプレートを作成し、新しい Cisco pxGrid 証明書を生成します。

（注） FIPS モードが有効になっている場合、pxGrid 証明書テンプレートの RSA 秘密キーのサイズは 2048 ビット以上である必要があります。それ以外の場合、pxGrid 証明書を生成しようとするとエラーが表示されます。証明書テンプレートの秘密キーサイズを変更するには、pxGrid 証明書テンプレートのキーサイズの変更（1941 ページ） を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [クライアント管理（Client Management）] > [証明書（Certificates）]**。

ステップ 2 [処理の選択（I want to）] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）]：このオプションを選択した場合は、共通名（CN）を入力する必要があります。
- [単一の証明書の生成（証明書署名要求あり）（Generate a single certificate (with a certificate signing request)）]：このオプションを選択した場合は、証明書署名要求の詳細を入力する必要があります。

ステップ 3 （オプション）この証明書の説明を入力します。

ステップ 4 [pxGrig_Certificate_Template] のリンクをクリックして証明書テンプレートをダウンロードし、必要に応じて編集します。

ステップ 5 [サブジェクト代替名（SAN）（Subject Alternative Name (SAN)）] を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- [IPアドレス（IP address）]：この証明書に関連付ける Cisco pxGrid クライアントの IP アドレスを入力します。
- [FQDN]：pxGrid クライアントの FQDN を入力します。

ステップ 6 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウンリストから、以下のいずれかのオプションを選択します。

- [Private Enhanced Electronic Mail（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）（Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)）]：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「`-------BEGIN CERTIFICATE-----`」タグで始まり、「`-----END CERTIFICATE----`」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「`-----BEGIN ENCRYPTED PRIVATE KEY----`」タグで始まり、「`-----END ENCRYPTED PRIVATE KEY----`」タグで終わります。
- [PKCS12形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で1ファイル）（PKCS12 format (including certificate chain; one file for both the certificate chain and key)）]：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンドエンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成（Create）] をクリックします。

作成した証明書は、[発行された証明書（Issued Certificates）] ウィンドウに表示されます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [発行された証明書（Issued Certificates）]**。

（注） Cisco ISE 2.4 パッチ 13 以降、pxGrid サービスの証明書要件がより厳格になりました。pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、Cisco ISE 2.4 パッチ 13 以降の適用後に証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の以前のバージョンに、**SSL サーバー**として指定された **Netscape Cert Type** 拡張があるためです。これは現在は失敗するようになっています（現在はクライアント証明書も必要）。

非準拠の証明書を持つクライアントは、Cisco ISE と統合できません。内部 CA によって発行された証明書を使用するか、適切な使用拡張で新しい証明書を生成します。

- 証明書の [キーの使用方法（Key Usage）] の拡張には、[デジタル署名（Digital Signature）] フィールドと [キー暗号化（Key Encipherment）] フィールドが含まれている必要があります。
- 証明書の [拡張キーの使用方法（Extended Key Usage）] の拡張には、[クライアント承認（Client Authentication）] フィールドと [サーバー承認（Server Authentication）] フィールドが含まれている必要があります。
- 証明書に [Netscape証明書タイプ（Nestscape Certificate Type）] の拡張は必要ありません。その拡張を含める場合は、[SSLクライアント（SSL Client）] と [SSLサーバー（SSL Server）] の両方を拡張に追加します。
- 自己署名証明書を使用している場合は、[基本制約CA（Basic Constraints CA）] フィールドを **TRUE** にし、[キーの使用方法（Key Usage）] の拡張に [キー証明書署名（Key Cert Sign）] フィールドを含める必要があります。

pxGrid証明書の生成における既知の制限

Cisco ISE での pxGrid 証明書の生成は、次に説明する表形式のロジックに従います。

シリアル番号	システム証明書（EAP）	発行元証明書	pxGrid 形式	サポート
1	複数の共通名	単一の共通名	PKCS8、PKCS12	サポート対象
2	複数の共通名	複数の共通名	PKCS12	サポート対象
3	複数の共通名	複数の共通名	PKCS8	サポート対象外

pxGrid 証明書テンプレートのキーサイズの変更

次のタスクは、pxGrid 証明書テンプレートのキーサイズを変更するのに役立ちます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[証明書テンプレート（Certificate Templates）]** を選択します。

ステップ 2 テンプレート **pxGrid_Certificate_Template** の横にあるチェックボックスをオンにします。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 [キーサイズ（Key Size）] ドロップダウンリストから、[2048] を選択します。

ステップ 5 [保存（Save）] をクリックします。

第 16 章

統合

次のセクションでは、Cisco ISE 機能をサポートするためにスイッチおよびワイヤレスコントローラで必要な構成について説明します。

- スイッチでの標準 Web 認証のサポートの有効化 （1944 ページ）
- 代理 RADIUS トランザクション用のローカルユーザー名とパスワードの定義 （1944 ページ）
- ログとアカウンティングのタイムスタンプの正確性を保証するための NTP サーバー設定 （1944 ページ）
- AAA 機能を有効にするコマンド （1944 ページ）
- スイッチ上の RADIUS サーバーの設定 （1945 ページ）
- RADIUS 認可変更（CoA）を処理するスイッチの有効化 （1946 ページ）
- スイッチポートでのデバイストラッキングと DHCP スヌーピングの有効化 （1946 ページ）
- スイッチポート用 802.1X ポートベースの認証の有効化 （1947 ページ）
- クリティカルな認証に対する EAP の有効化 （1947 ページ）
- リカバリの遅延を使用した AAA 要求のスロットリング （1947 ページ）
- 適用状態に基づく VLAN の定義 （1947 ページ）
- スイッチでのローカル（デフォルト）アクセスリスト（ACL）の定義 （1948 ページ）
- 802.1X および MAB のスイッチ ポートの有効化 （1949 ページ）
- Identity-Based Network Services に基づいて 802.1X を有効にするコマンド （1951 ページ）
- EPM ロギングの有効化 （1952 ページ）
- SNMP トラップを受信するためのスイッチの有効化 （1953 ページ）
- プロファイリング用の SNMP v3 クエリーの有効化 （1953 ページ）
- プロファイラによる収集を可能にするための MAC 通知トラップの有効化 （1953 ページ）
- スイッチ上での RADIUS アイドルタイムアウトの設定 （1954 ページ）
- iOS サプリカントのプロビジョニング用のワイヤレスコントローラの構成 （1954 ページ）
- MDM 相互運用性のためのワイヤレス LAN コントローラでの ACL の設定 （1955 ページ）

スイッチでの標準 Web 認証のサポートの有効化

認証時の URL リダイレクションのプロビジョニングなど、Cisco ISE 用の標準 Web 認証機能を有効にするには、次のコマンドをスイッチの構成に含めます。

```
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443
ip http secure-server
```

代理 RADIUS トランザクション用のローカルユーザー名とパスワードの定義

スイッチがこのネットワーク セグメントの RADIUS サーバーであるかのように Cisco ISE ノードと通信するには、次のコマンドを入力します。

```
username test-radius password 0 abcde123
```

ログとアカウンティングのタイムスタンプの正確性を保証するための NTP サーバー設定

次のコマンドを入力して、Cisco ISE で設定したものと同じ NTP サーバーをスイッチ上に指定していることを確認します。

```
ntp server <IP_address>|<domain_name>
```

AAA 機能を有効にするコマンド

802.1X および MAB 認証機能など、スイッチと Cisco ISE との間でさまざまな AAA 機能を有効にするには、スイッチ上で次のコマンドを入力します。

```
aaa new-model
! Creates an 802.1X port-based authentication method list
aaa authentication dot1x default group radius
```

```
! Required for VLAN/ACL assignment
aaa authorization network default group radius
! Authentication & authorization for webauth transactions
aaa authorization auth-proxy default group radius
! Enables accounting for 802.1X and MAB authentications
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
!
aaa accounting update periodic 1440
! Update AAA accounting information periodically every 1440 minutes
aaa accounting system default start-stop group radius
!
```

スイッチ上の RADIUS サーバーの設定

Cisco ISE とやり取りし、RADIUS ソース サーバーとして動作するようスイッチを設定するには、次のコマンドを入力します。

```
!
radius-server <ISE Name>
! ISE Name is the name of the ISE PSN
address ipv4 <ip address> auth-port 1812 acct-port 1813
! IP address is the address of the PSN. This example uses the standard RADIUS ports.
key <passwd>
! passwd is the secret password confiugured in Cisco ISE
exit
```

（注） 3 回の再試行を含む 30 秒のデッド基準時間を設定し、Active Directory を認証に使用する RADIUS 要求に対して、より長い応答時間を提供することを推奨します。

RADIUS 認可変更（CoA）を処理するスイッチの有効化

スイッチが Cisco ISE で RADIUS CoA の動作と関連するポスチャ機能を適切に処理できるように設定を指定するには、次のコマンドを入力します。

aaa server radius dynamic-author client *<ISE-IP>* **server-key 0** *abcde123*

（注）

- Cisco ISE では、RFC の CoA 用デフォルト ポート 3799 に対して、ポート 1700（Cisco IOS ソフトウェアのデフォルト）を使用します。既存の Cisco Secure ACS 5.x ユーザーは、既存の ACS の実装の一部として CoA を使用している場合、すでにこれをポート 3799 に設定している可能性があります。
- 秘密キーは、ネットワークデバイスの追加時に Cisco ISE で設定したものと同じである必要があり、IP アドレスは PSN IP アドレスである必要があります。

スイッチポートでのデバイストラッキングと DHCP スヌーピングの有効化

セキュリティに関連する Cisco ISE のオプション機能を提供できるようにするには、次のコマンドを入力することによって、スイッチポートのダイナミック ACL 内での IP 置換に関して、デバイストラッキングと DHCP スヌーピングを有効化します。

```
! Optional
 ip dhcp snooping

! Required!

! Configure Device Tracking Policy!device-tracking policy <DT_POLICY_NAME>no
protocol ndp tracking enable

! Bind it to interface!interface <interface_id>device-tracking
attach-policy<DT_POLICY_NAME>
```

RADIUS アカウンティングでは、DHCP スヌーピングが有効になっていても、DHCP 属性は IOS センサーによって Cisco ISE に送信されません。このような場合、DHCP スヌーピングを VLAN で有効にして DHCP をアクティブにする必要があります。

VLAN で DHCP スヌーピングを有効にするには、次のコマンドを使用します。

ip dhcp snooping

ip dhcp snooping vlan 1-100

スイッチポート用 802.1X ポートベースの認証の有効化

スイッチポートに対してグローバルに 802.1X 認証を有効にするには、次のコマンドを入力します。

```
dot1x system-auth-control
```

クリティカルな認証に対する EAP の有効化

サプリカントによる LAN 経由での認証要求をサポートするには、次のコマンドを入力することによって、EAP をクリティカルな認証（アクセスできない認証バイパス）に対して有効にします。

```
dot1x critical eapol
```

リカバリの遅延を使用した AAA 要求のスロットリング

クリティカルな認証リカバリの場合は、自動的に認証遅延（秒単位）を発生させるようにスイッチを設定し、リカバリ後に Cisco ISE が再びサービスを開始できるようにします。次のコマンドを使用します。

```
authentication critical recovery delay 1000
```

適用状態に基づく VLAN の定義

ネットワーク内の既知の適用状態に基づいて VLAN 名、番号、およびスイッチ仮想インターフェイス（SVI）を定義するには、次のコマンドを入力します。ネットワーク間のルーティングを有効にするには、それぞれの VLAN インターフェイスを作成します。これは特に、エンドポイントがネットワークに接続するときに経由するエンドポイント（PC やラップトップ）と IP 電話の両方からの同じネットワークセグメントを経由して渡される複数のソースからのトラフィックを処理する場合に役立ちます。次に例を示します。

```
vlan <VLAN_number>
name ACCESS!
vlan <VLAN_number>
name VOICE

!
interface <VLAN_number>
description ACCESS
ip address 10.1.2.3 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
ip helper-address <Cisco_ISE_IP_address>
```

```
!
interface <VLAN_number>
description VOICE
ip address 10.2.3.4 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
```

スイッチでのローカル（デフォルト）アクセスリスト（ACL）の定義

このような機能を古いバージョンのスイッチ（Cisco IOS ソフトウェア リリースのバージョンが 12.2(55)SE よりも前）で有効にし、Cisco ISE が認証と許可に必要なダイナミック ACL の更新を実行できるようにするには、次のコマンドを入力します。

```
ip access-list extended ACL-ALLOW

 permit ip any any

!

ip access-list extended ACL-DEFAULT

  remark DHCP

  permit udp any eq bootpc any eq bootps

  remark DNS

  permit udp any any eq domain

  remark Ping

  permit icmp any any

  remark Ping

  permit icmp any any

  remark PXE / TFTP

  permit udp any any eq tftp

  remark Allow HTTP/S to ISE and WebAuth portal
permit tcp any host <Cisco_ISE_IP_address> eq www

permit tcp any host <Cisco_ISE_IP_address> eq 443

permit tcp any host <Cisco_ISE_IP_address> eq 8443
```

```
permit tcp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8906

permit tcp any host <Cisco_ISE_IP_address> eq 8080

permit udp any host <Cisco_ISE_IP_address> eq 9996

remark Drop all the rest

  deny ip any any log

!

! The ACL to allow URL-redirection for WebAuth
 ip access-list extended ACL-WEBAUTH-REDIRECT

 permit tcp any any eq www

 permit tcp any any eq 443
```

（注） ワイヤレスコントローラでこの設定を行うと、CPU使用率が増加し、システムが不安定になるリスクが高まります。これは IOS の問題で、Cisco ISE は悪影響を受けません。

802.1X および MAB のスイッチ ポートの有効化

802.1X および MAB のスイッチ ポートを有効にするには、以下の手順を実行します。

ステップ 1 すべてのアクセススイッチポートのインターフェイス コンフィギュレーション モードを開始します。
interface range FastEthernet0/1-8

ステップ 2 次のように、（トランク モードではなく）アクセス モードのスイッチ ポートを有効にします。
switchport mode access

ステップ 3 静的にアクセス VLAN を設定します。アクセス VLAN のローカル プロビジョニングを提供するこの手順は、オープンモード認証に必要となります。
switchport access vlan <*VLAN_number*>

ステップ 4 静的に音声 VLAN を設定します。
switchport voice vlan <*VLAN_number*>

ステップ 5 オープン モード認証を有効にします。オープンモードを使用すると、認証が完了する前に、トラフィックをデータおよび音声 VLAN 上にブリッジングできます。実稼働環境では、ポートベースの ACL を使用して不正アクセスを防ぐことを強く推奨します。

オープンモード認証を有効にすると、ポート ACL に従って AAA サーバー応答の前に事前認証アクセスも可能になります。

authentication open

ステップ 6 ポートベースの ACL を適用して、認証されていないエンドポイントからアクセス VLAN 上にデフォルトでどのトラフィックをブリッジングするかを決定します。最初にすべてのアクセスを許可してからポリシーを適用する必要があるため、ACL-ALLOW を適用して、スイッチ ポートを通過するすべてのトラフィックを許可する必要があります。すでに現時点のすべてのトラフィックを許可するデフォルトの Cisco ISE 許可を作成しましたが、この理由は、完全な可視性を実現し、既存のエンドユーザー環境にはまだ影響を与えないようにするためです。

ACL は AAA サーバーから動的 ACL の前に追加されるように設定する必要があります。

ip access-group ACL-ALLOW in

（注） DSBU スイッチ上に Cisco IOS Release 12.2(55)SE ソフトウェアを用意する前に、RADIUS AAA サーバーからのダイナミック ACL を適用するためのポート ACL が必要です。デフォルトの ACL を用意できなかった場合、割り当てられた動的 ACL はスイッチによって無視されます。Cisco IOS ソフトウェアのリリース 12.2(55)SE では、デフォルトの ACL が自動的に生成および適用されます。

（注） テストの現段階では、ポートベースの 802.1X 認証を有効にし、さらに既存のネットワークに対する影響を避けるために、ACL-ALLOW を使用しています。今後のテストでは、実稼働環境に必要のないトラフィックをブロックする、異なる ACL-DEFAULT を適用する予定です。

ステップ 7 マルチ認証ホストモードを有効にします。マルチ認証は、基本的には複数ドメイン認証（MDA）のスーパーセットです。MDA では、データ ドメイン内の単一のエンドポイントだけが許可されます。マルチ認証を設定すると、音声ドメイン内では認証された単一の電話が（MDA の場合と同じように）許可されますが、データ ドメイン内では認証できるデータ デバイスの数に制限がありません。

同じ物理アクセスポート上の音声と複数のエンドポイントが許可されます。

authentication host-mode multi-auth

（注） IP 電話の背後で複数のデータ デバイス（仮想デバイスであるかハブに接続されている物理デバイスであるかにかかわらず）を使用すると、アクセス ポートの物理リンクステート認識度が低下する可能性があります。

ステップ 8 次のコマンドを使用して、さまざまな認証方式オプションを有効にします。

次のように、再認証を有効にします。

authentication periodic

次のように、RADIUS セッションタイムアウトを介して再認証を有効にします。

authentication timer reauthenticate server

authentication event fail action next-method

デッドサーバーの場合は、次のようにクリティカル認証 VLAN 方式を設定します。

authentication event server dead action reinitialize vlan *<VLAN_number>*

authentication event server alive action reinitialize

次のように、802.1X と MAB の IOS Flex-Auth 認証を設定します。

authentication order dot1x mab
authentication priority dot1x mab

ステップ 9 次のように、スイッチ ポートで 802.1X ポート制御を有効にします。
authentication port-control auto
authentication violation restrict

ステップ 10 次のように、MAC 認証バイパス（MAB）を有効にします。
mab

ステップ 11 次のように、スイッチポート上で 802.1X を有効にします。
dot1x pae authenticator

ステップ 12 次のように、再送信時間を 10 秒に設定します。
dot1x timeout tx-period *10*

（注） 802.1X tx-period のタイムアウトは 10 秒に設定する必要があります。この値を変更する場合は、その影響を理解したうえで行ってください。

ステップ 13 次のように、PortFast 機能を有効にします。
spanning-tree portfast

Identity-Based Network Services に基づいて 802.1X を有効にするコマンド

次の例は、802.1X、MAB、および Web 認証を使用する連続認証方式を許可するように設定されている制御ポリシーを示しています。

```
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
!


policy-map type control subscriber DOT1XMAB
 event session-started match-all
```

```
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
   30 authorize
  40 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
!
```

次の例は、MAB、802.1X、および Web 認証を使用する連続認証方式を許可するように設定されている制御ポリシーを示しています。

```
policy-map type control subscriber MABDOT1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
   20 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class ALL_FAILED do-until-failure
   10 authentication-restart 60
 event authentication-success match-all
  10 class DOT1X do-until-failure
   10 terminate mab
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
```

サービスポリシーをインターフェイスに適用します。

```
interface GigabitEthernet1/0/4
 switchport mode access
 device-tracking attach-policy pol1
 ip access-group sample in
 authentication timer reauthenticate server
 access-session port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 dot1x timeout auth-period 10
 spanning-tree portfast
 service-policy type control subscriber DOT1XMAB
```

EPM ロギングの有効化

Cisco ISE の機能について発生する可能性があるトラブルシューティングや記録をサポートするには、スイッチに標準のロギング機能を次のように設定します。

epm logging

SNMP トラップを受信するためのスイッチの有効化

次のように、スイッチがこのネットワークセグメント内の適切なVLANを経由して、Cisco ISEからSNMP トラップ送信を受信できるようにします。

```
snmp-server community public RO
snmp-server trap-source <VLAN_number>
```

プロファイリング用の SNMP v3 クエリーの有効化

SNMP v3 ポーリングが正常に実行され、Cisco ISE プロファイリングサービスがサポートされるように、次のコマンドを使用してスイッチを設定します。その前に、SNMP設定をCisco ISEのGUIの **[SNMP設定（SNMP Settings）]** ウィンドウで設定します。 このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** > **[追加 | 編集（Add | Edit）]** > **[SNMP 設定（SNMP Settings）]**。

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
snmp-server group  <group> v3 priv
snmp-server group <group> v3 priv contextvlan-1
```

（注） **snmp-server group** <*group*> **v3 priv context** *vlan-1* コマンドは、コンテキストごとに設定する必要があります。**snmp show context** コマンドでは、すべてのコンテキスト情報がリストされます。

SNMP要求がタイムアウトになり、接続の問題が発生していない場合は、タイムアウト値を増加させることができます。

プロファイラによる収集を可能にするためのMAC通知トラップの有効化

次のように、適切な MAC 通知トラップを送信するようスイッチを設定し、Cisco ISE のプロファイラ機能がネットワークエンドポイントで情報を収集できるようにします。

```
mac address-table notification change
mac address-table notification mac-move
snmp trap mac-notification change added
snmp trap mac-notification change removed
```

スイッチ上での RADIUS アイドルタイムアウトの設定

スイッチに RADIUS Idle-timeout を設定するには、次のコマンドを使用します。

```
Switch(config-if)# authentication timer inactivity
```

ここで、*inactivity* は、クライアントアクティビティが不正と見なされるまでの非アクティブ間隔を秒単位で表したものです。

Cisco ISE では、そのようなセッション非アクティブタイマーを適用する認証ポリシーに対してこのオプションを有効にできます。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Authorization）]** > **[承認（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Policy Elements）]** > **[結果（Authorization）]** > **[承認（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** を選択します。

iOS サプリカントのプロビジョニング用のワイヤレスコントローラの構成

シングル SSID の場合

同じワイヤレスアクセスポイントで、Apple iOS ベースのデバイス（iPhone または iPad）が、ある SSID から別の SSID に切り替えることができるようにするには、**FAST SSID change**機能を有効にするようワイヤレスコントローラを設定します。この機能によって、iOS ベースのデバイスが SSID 間の切り替えを迅速に行えるようにします。

デュアル SSID BYOD の場合

デュアル SSID BYOD をサポートするには、Fast SSID が有効になっている必要があります。ワイヤレスコントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間を高速で移動できます。高速 SSID が有効になっている場合、クライアントエントリがクリアされず、遅延は適用されません。シスコ ワイヤレス コントローラでの高速 SSID の構成に関する詳細については、『Cisco Wireless Controller Configuration Guide』を参照してください。

ワイヤレスコントローラの構成例

```
WLC (config)# FAST SSID change
```

一部の Apple iOS ベースのデバイスでは、ワイヤレス ネットワークに接続しようとすると、次のエラー メッセージが表示される場合があります。

```
Could not scan for Wireless Networks.
```

デバイス認証に影響しないため、このエラー メッセージは無視できます。

MDM 相互運用性のためのワイヤレス LAN コントローラでの ACL の設定

未登録のデバイスおよび証明書プロビジョニングをリダイレクトするために認証ポリシーで使用する ACL をワイヤレスコントローラで設定します。ACL は次の順序にする必要があります。

ステップ 1 サーバーからクライアントへのすべての発信トラフィックを許可します。

ステップ 2 （任意）トラブルシューティングのためにクライアントからサーバーへの ICMP 着信トラフィックを許可します。

ステップ 3 未登録および非準拠のデバイスが MDM エージェントをダウンロードし、コンプライアンスチェックに進むように MDM サーバーへのアクセスを許可します。

ステップ 4 Web ポータルおよびサプリカント用 Cisco ISE、および証明書プロビジョニングフローに対するクライアントからサーバーへのすべての着信トラフィックを許可します。

ステップ 5 名前解決のためにクライアントからサーバーへの着信ドメインネームシステム（DNS）トラフィックを許可します。

ステップ 6 IP アドレスのためにクライアントからサーバーへの着信 DHCP トラフィックを許可します。

ステップ 7 Cisco ISE へのリダイレクションのための、クライアントからサーバーへの企業リソースに対するすべての着信トラフィックを（会社のポリシーに応じて）拒否します。

ステップ 8 （任意）残りのトラフィックを許可します。

例

次の例では、未登録のデバイスを BYOD フローにリダイレクトするための ACL を示しています。この例では、Cisco ISE IP アドレスは 10.35.50.165 で、企業のネットワークの IP アドレスは 192.168.0.0 および 172.16.0.0（リダイレクト用）で、MDM サーバーサブネットは 204.8.168.0 です。

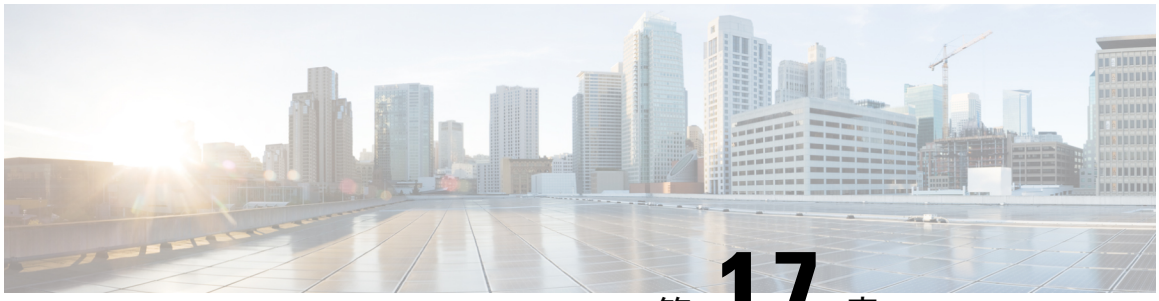
図 *80* : 登録されていないデバイスをリダイレクトするための *ACL*

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819



第 17 章

トラブルシューティング

- Cisco ISE のモニタリングとトラブルシューティング サービス （1957 ページ）
- Cisco ISE テレメトリ （1963 ページ）
- テレメトリが収集する情報 （1963 ページ）
- Cisco ISE をモニターする SNMP トラップ （1966 ページ）
- Cisco ISE アラーム （1970 ページ）
- ログ収集 （1995 ページ）
- RADIUS ライブ ログ （1996 ページ）
- TACACS ライブ ログ （2000 ページ）
- ライブ認証 （2002 ページ）
- RADIUS ライブ セッション （2004 ページ）
- エクスポート サマリ （2009 ページ）
- 認証概要レポート （2011 ページ）
- 展開およびサポート情報のための Cisco Support Diagnostics （2012 ページ）
- Cisco Support Diagnostics Connector を使用した構成バックアップの取得 （2014 ページ）
- 診断トラブルシューティング ツール （2014 ページ）
- セッション トレース テスト ケース （2019 ページ）
- 着信トラフィックを検証する TCP ダンプユーティリティ （2020 ページ）
- その他のトラブルシューティング情報の入手 （2025 ページ）

Cisco ISE のモニタリングとトラブルシューティング サービス

モニタリングおよびトラブルシューティング（MnT）サービスは、すべての Cisco ISE 実行時サービスを対象とした包括的なアイデンティティ ソリューションです。[操作（Operations）] メニューには次のコンポーネントが表示されます。このメニューはプライマリポリシー管理ノード（PAN）からのみ表示できます。[操作（Operations）] メニューはプライマリ モニタリング ノードに表示されないことに注意してください。

- モニタリング：ネットワーク上のアクセスアクティビティの状態を表す意味のあるデータをリアルタイムに表示します。これを把握することにより、操作の状態を簡単に解釈し、監視できます。
- トラブルシューティング：ネットワーク上のアクセスの問題を解決するための状況に応じたガイダンスを提供します。また、ユーザーの懸念に対応してタイムリーに解決策を提供できます。
- レポート：トレンドを分析し、システムパフォーマンスおよびネットワークアクティビティをモニターするために使用できる、標準レポートのカタログを提供します。レポートをさまざまな方法でカスタマイズし、今後使用するために保存できます。[ID（Identity）]、[エンドポイントID（Endpoint ID）]、および [ISE ノード（ISE Node）]（正常性の概要レポートは除く）のすべてのレポートで、ワイルドカードおよび複数値を使用してレコードを検索できます。

ISE コミュニティ リソース

トラブルシューティングに関するテクニカル ノートのリストについては、「ISE Troubleshooting TechNotes」を参照してください。

TAC サポートケースのオープン

Cisco ISE を介して TAC サポートケースをオープンして、Cisco ISE の展開に関する問題のサポートを要求できるようになりました。TAC サポートケース機能を使用すると、問題が発生した特定のノードのサポートケースを簡単に作成できます。Support Case Manager（SCM）で提示されるフォームに入力する情報とともに、ノードのシリアル番号や使用中の Cisco ISE バージョンなどの情報も Cisco TAC に送信されます。

（注） Cisco ISE がエアギャップ環境に展開されている場合、Support Case Manager（SCM）機能は機能しないため、

ステップ 1 Cisco ISE ポータルのホームページで、右上隅にある疑問符アイコンをクリックします。

ステップ 2 表示される [インタラクティブヘルプ（Interactive Help）] メニューの [リソース（Resources）] ドロップダウンリストから [TAC サポートケース（TAC Support Cases）] を選択します。

ステップ 3 [TAC サポートケース（TAC Support Cases）] ウィンドウの [ノードリスト（Node List）] ドロップダウンリストから、ケースをオープンする最大 4 つのノードを選択します。デフォルトでは、プライマリ PAN および MnT ノードが選択されています。

ステップ 4 [ケースをオープン（Open A Case）] をクリックします。Support Case Manager が新しいタブで開きます。

（オプション）Support Case Manager で作成された TAC ケースのステータスを表示するには、[ケースリスト（Cases List）] をクリックします。

ステップ 5 Support Case Manager の [SSO 認証（SSO Authentication）] ウィンドウで、cisco.com ログイン情報を使用してログインします。ログインできない場合は、シスコのカスタマーサポートにお問い合わせください。

ステップ 6 必要な詳細情報を入力し、SCM で Cisco ISE 展開に関する新しい TAC サポートケースを開きます。Support Case Manager（SCM）で TAC サポートケースを開く手順を使用して、支援とトラブルシューティングを得ることをお勧めします。

ヘルス チェック

Cisco ISE には、Cisco ISE 展開内のすべてのノードを診断するオンデマンドのヘルスチェックオプションがあります。運用前にすべてのノードのヘルスチェックを実行すると、ダウンタイムを短縮でき、重大な問題（ある場合）を特定することで Cisco ISE システムの機能全体を向上できます。ヘルスチェックでは、コンポーネントの動作ステータスが示され、展開内の問題（ある場合）に関するトラブルシューティングの推奨事項が表示されます。

表 *193*：ヘルスチェックの展開

展開タイプ	説明
プラットフォーム サポート チェック	展開でサポートされているプラットフォームを確認します。推奨要件の仕様を満たしていないプラットフォームは、パフォーマンスの問題を引き起こす可能性があります。 34xx およびその他のサポートされていないプラットフォームの詳細を確認し、システムに最低でも 12 コアの CPU、300 GB のハードディスク、16 GB のメモリが搭載されていることを確認します。
展開の検証	展開のノードの状態（同期しているか進行中か）を確認します
DNS の解決可能性	ホスト名と IP アドレスの正引きと逆引きを確認します。 展開の正常性チェックが適切に機能するためには、DNS 解決を正引きと逆引きの両方で行うことが推奨されます。
信頼ストア証明書の検証	信頼ストア証明書が有効か、期限切れかを確認します。 最適な Cisco ISE 機能を確保するために、未使用または期限切れの証明書を削除または更新します。
システム証明書の検証	各ノードのシステム証明書の検証を確認します。 最適な Cisco ISE 機能を確保するために、未使用または期限切れの証明書を削除または更新します。
ディスク容量チェック	プラットフォーム サポート チェックにあるハードディスクと、アップグレード手順のために使用可能なディスクの空き容量をチェックします。 パフォーマンスの問題を回避するために、アップグレード操作を開始する前にディスク容量チェックを実行することをお勧めします。

展開タイプ	説明
NTP の到達可能性と時刻源の確認	システムで設定されている NTP をチェックし、時刻源が NTP サーバーかどうかを確認します。 NTP 同期は、AD 操作、アップグレードワークフローなどの Cisco ISE サービスに不可欠です。
負荷平均チェック	指定した間隔でシステムの負荷を確認します。有効な間隔の設定は、1、5、および 15 分です。 負荷平均チェックの失敗は、Cisco ISE のパフォーマンスの問題につながる可能性があります。
MDM の検証	設定された MDM サーバーと Cisco ISE PSN サーバー間の接続を確認します。 MDM でサポートされる機能を Cisco ISE で使用するには、MDM 検証チェックが成功する必要があります。
ライセンスの検証	スマートライセンスが設定されていて、有効であるかどうかを確認します。スマートライセンスが設定されていないか有効でない場合、ライセンスを設定して検証するように求める警告が Cisco ISE GUI に表示されます。 Cisco ISE リリース 3.0 以降のリリースでは、スマートライセンスのみがサポートされます。Cisco ISE リリース 3.0 以降のリリースにアップグレードする前に、従来のライセンスをスマートライセンスに変換します。
サービスまたはプロセスの失敗	サービスまたはアプリケーションのステータスが実行中か、障害状態かを確認します。
I/O 帯域幅のパフォーマンスチェック	Cisco ISE のパフォーマンスの問題を回避するために、ディスクの読み取りおよび書き込み速度をチェックします。

（注） 展開の横にある数字は、ノードの数とそのヘルスチェックの詳細を示します。例：展開に 0/2 がある場合、0 は失敗/進行中/完了状態のノードの数を示し、2 は展開内のノードの数を示します。ヘルスチェック中に、いずれかのノードが 15 分間応答を返さない場合、そのノードのヘルスチェックはタイムアウトになります。

ヘルスチェックの実行

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [正常性チェック（Health Checks）]** を選択します。

ステップ 2 **[正常性チェックの確認（Start health checks）]** をクリックします。

情報ポップアップウィンドウに次のメッセージが表示されます。

```
Health Checks triggered.
```

ステップ 3 **[Ok]** をクリックすると、ステータスが表示されます。

ステップ 4 **[正常性チェック（Health Checks）]** ウィンドウで、各コンポーネントの正常性ステータスを表示できます。次の色は、対応する Cisco ISE コンポーネントのヘルスステータスを示します。

カラー	正常性ステータス	アクション
赤	不良	トラブルシューティングの推奨事項を表示するには、ドロップダウンオプションをクリックします。 アップグレードワークフローなどの操作は、これらの問題が解決されるまで続行できないため、問題を解決することをお勧めします。
オレンジ	良好	ボックスで使用可能なトラブルシューティングの推奨事項を表示するには、ドロップダウンオプションをクリックします。 コンポーネントのヘルスステータスは操作の実行に適しているため、アップグレードワークフローを続行できますが、これらの問題も Cisco ISE の機能に影響する可能性があるため、続行する前にオレンジ色で示されている問題を解決することを推奨します。
グリーン	良好	アクションは不要です。
青色	良好	機能に関する重要な情報を表示するには、情報アイコンをクリックします。

ステップ 5 **[レポートのダウンロード（Download）]** をクリックします。

HealthChecksReport.json ファイルは、Cisco ISE 展開の詳細な正常性ステータス情報とともにローカルシステムに保存されます。

正常性チェックがトリガーされると、ステータスは **[正常性チェック（Health Check）]** ウィンドウに 3 時間保持されます。[ヘルスチェック（Health Checks）] ウィンドウが更新されるか期限切れになるまで、ヘルスチェックを実行できません。

Network Privilege Framework のイベントフロープロセス

Network Privilege Framework（NPF）認証および許可イベント フローでは、次の表に記載されているプロセスが使用されます。

プロセス ステージ	説明
1	ネットワーク アクセスデバイス（NAD）によって通常の許可またはフレックス許可のいずれかが実行されます。
2	未知のエージェントレス ID が Web 許可を使用してプロファイリングされます。
3	RADIUS サーバーによって ID が認証および許可されます。
4	許可がポートでアイデンティティに対してプロビジョニングされます。
5	許可されないエンドポイント トラフィックはドロップされます。

モニタリングおよびトラブルシューティング機能のユーザーロールと権限

モニタリングおよびトラブルシューティング機能は、デフォルトのユーザー ロールに関連付けられます。実行を許可されるタスクは、割り当てられているユーザー ロールに直接関係します。

各ユーザーロールに設定されている権限と制約事項については、Cisco ISE 管理者グループ （12 ページ）を参照してください。

（注） Cisco TAC の指示がないルートシェルを使用した Cisco ISE へのアクセスはサポート対象外のため、その結果として生じる可能性があるサービスの中断については、シスコは責任を負いません。

モニタリングデータベースに格納されているデータ

Cisco ISE モニタリング サービスでは、データが収集され、特化したモニタリング データベースに格納されます。ネットワーク機能のモニタリングに使用されるデータのレートおよび量によっては、モニタリング専用のノードが必要な場合があります。Cisco ISE ネットワークによって、ポリシーサービスノードまたはネットワークデバイスからロギングデータが高いレートで収集される場合は、モニタリング専用の Cisco ISE ノードを推奨します。

モニタリングデータベースに格納される情報を管理するには、データベースの完全バックアップおよび差分バックアップを実行します。これには、不要なデータの消去とデータベースの復元が含まれます。

Cisco ISE テレメトリ

テレメトリは、ネットワーク内のシステムとデバイスを監視し、ユーザーの製品使用方法に関する情報をシスコにフィードバックします。シスコでは、この情報を使用して製品を改善します。

Cisco ISE テレメトリデータ通信は、https://connectdna.cisco.com/ のポート 443 を介した HTTPS トラフィックとして行われます。

テレメトリはデフォルトで有効になっています。この機能を無効にするには、次の手順に従ってください。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [Network Success Diagnostics] > [テレメトリ（Telemetry）]** を選択します。
2. [テレメトリの有効化（Enable Telemetry）] チェックボックスをオフにし、テレメトリを無効にします。

   • [シスコアカウント（Cisco Account）]：テレメトリからの電子メールを受信できるようにシスコアカウントのログイン情報を入力します。この ID は、Cisco ISE 展開に影響する可能性がある重大な問題がテレメトリによって発見された場合の連絡にも使用されることがあります。

テレメトリが収集する情報

テレメトリは、シスコに次の情報を送信します。

ノード：

各ポリシー管理ノード（PAN）については、次のとおりです。

- ポスチャされたエンドポイントの現在の数
- pxGrid クライアントの現在の数
- MDM によって管理されるエンドポイントの現在の数
- 現在のゲストユーザーの数
- このテレメトリレコードの開始日と終了日
- FIPS ステータス

各ポリシーサービスノード（PSN）については、次のとおりです。

- プロファイラプローブの数
- ノードサービスタイプ

- 使用されているパッシブ ID

すべてのノードの場合

- アクティブな NAD と NAD の総数
- CPU コア数
- VM 利用可能なディスク容量
- VM メモリと CPU の設定
- システム名
- シリアル番号
- VID と PID
- アップタイム
- 最後の CLI ログイン

MnT ノード数

pxGrid ノード数

ライセンス

- ライセンスの有効期限が切れていますか?
- 使用可能な Cisco ISE Essentials ライセンスの数、これまでに使用された最大数
- 使用可能な Cisco ISE Advantage ライセンスの数、これまでに使用された最大数
- 使用可能な Cisco ISE Premier ライセンスの数、これまでに使用された最大数
- 評価ライセンスを使用していますか?
- スマートアカウントの名前
- TACACS デバイスの数
- 有効期限、残りの日数、ライセンス期間
- サービスタイプ、プライマリ UDI およびセカンダリ UDI

ポスチャ

- 非アクティブなポリシーの数
- 最後のポスチャフィード更新
- アクティブなポリシーの数
- ポスチャフィードの更新

ゲスト ユーザー

- 当日の認証されたゲストの最大数
- 当日のアクティブゲストの最大数
- 当日の BYOD ユーザーの最大数
- 認証済みゲストの外部 ID 情報

ネットワーク アクセス デバイス（NAD）

- 認証：アクティブ化された ACL、VLAN、ポリシーサイズ
- NDG マップと NAD 階層
- 認証：
  - RADIUS、RSA ID、LDAP、ODBC、およびアクティブディレクトリ ID ストアの数
  - ローカル（管理者以外の）ユーザーの数
  - NDG マップと NAD マップ
  - ポリシーの行数

認証用のアクティブ VLAN、ポリシー数、アクティブ化された ACL の数：

- ステータス、VID、PT
- 平均負荷、メモリ使用率
- PAP、MnT、pxGrid、および PIC ノードの数
- 名前、プロファイル名、プロファイル ID

NAD プロファイル

各 NAD プロファイルに関する情報：

- 名前と ID
- シスコ デバイス
- TACACS サポート
- RADIUS サポート
- TrustSec サポート
- デフォルトのプロファイル

プロファイラ

- フィードの最終更新日
- 自動更新を有効にしますか。

- プロファイルされたエンドポイント、エンドポイントの種類、不明なエンドポイント、不明なパーセンテージ、および合計エンドポイント数
- カスタムプロファイルの数
- シリアル番号、範囲、エンドポイントタイプ、カスタムプロファイル

モバイル デバイス管理（MDM）

- MDM ノードのリスト
- 日付範囲内における、現在の MDM エンドポイント数、現在のゲストユーザー数、現在のポスチャ済みユーザー数
- pxGrid クライアント数
- ノード数

パッチおよびホットパッチ

- ノード FQDN
- Cisco ISE バージョン
- パッチとホットパッチの名前とインストールステータス

Cisco ISE をモニターする SNMP トラップ

SNMP トラップは、Cisco ISE のステータスをモニターできます。Cisco ISE サーバーにアクセスせずに Cisco ISE をモニターする場合は、Cisco ISE の SNMP ホストとして MIB ブラウザを設定できます。その後、MIB ブラウザから Cisco ISE のステータスをモニターすることもできます。

snmp-server host および **snmp-server trap** コマンドの詳細については、『Cisco Identity Services Engine CLI リファレンス ガイド』を参照してください。

Cisco ISE は、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。

CLI から SNMP ホストを設定した場合は、Cisco ISE は次の汎用システム トラップを送信します。

- Cold start：デバイスをリブートする場合。
- Linkup：イーサネット インターフェイスがアップしている場合。
- Linkdown：イーサネット インターフェイスがダウンしている場合。
- Authentication failure：コミュニティストリングが一致しない場合。

次の表に、Cisco ISE でデフォルトで生成される汎用 SNMP トラップを示します。

OID	説明	トラップの例
.1.3.6.1.4.1.8072.4.0.3 \n NET SNMP エージェント MIB::nsNotifyRestart	エージェントが再起動されたことを示します。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.4.1.8072.4.0.2 \n NET SNMP エージェント MIB::nsNotifyShutdown	エージェントがシャットダウン中であることを示します。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.6.3.1.1.5.4 \n IF-MIB::linkUp	エージェントロールで動作している SNMP エンティティで、いずれかの通信リンクの ifOperStatus オブジェクトが、ダウン状態から（notPresent 状態以外の）他の状態に遷移したことが検出されたことを示します。この他の状態は、ifOperStatus に含まれる値によって示されています。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.3 \n IF-MIB::linkDown	エージェントロールで動作している SNMP エンティティで、いずれかの通信リンクの ifOperStatus オブジェクトが、（notPresent 状態以外の）他の状態からダウン状態に遷移しようとしていることが検出されたことを示します。この他の状態は、ifOperStatus に含まれる値によって示されています。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

OID	説明	トラップの例
.1.3.6.1.6.3.1.1.5.1 \n SNMPv2-MIB::coldStart	通知発信元アプリケーションをサポートする SNMP エンティティが再初期化され、このエンティティの設定が変更された可能性があることを示します。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

Cisco ISE のプロセスモニタリング SNMP トラップ

Cisco ISE では、Cisco ISE CLI から SNMP ホストを設定する場合、Cisco ISE プロセス ステータスの hrSWRunName トラップを SNMP マネージャに送信できます。Cisco ISE は cron ジョブを使用してこれらのトラップをトリガーします。cron ジョブは Cisco ISE プロセスステータスを Monit から取得します。CLI から **SNMP-Server Host** コマンドを設定した後、5 分ごとに cron ジョブを実行して Cisco ISE をモニターします。

（注） 管理者が ISE プロセスを手動で停止した場合は、プロセスの Monit が停止しても、SNMP マネージャにトラップは送信されません。プロセス停止 SNMP トラップは、プロセスが不意にシャットダウンし、自動的に復活しない場合のみ SNMP マネージャに送信されます。

次に、Cisco ISE のプロセスモニタリング SNMP トラップのリストを示します。

OID	説明	トラップの例
.1.3.6.1.2.1.25.4.2.1.2 \n HOST-RESOURCES-MIB::hrSWRunName	製造元、リビジョン、一般に知られている名前など、この実行中のソフトウェアの説明テキストです。このソフトウェアがローカルにインストールされている場合は、対応する hrSWInstalledName で使用されているものと同じ文字列である必要があります。検討する必要のあるサービスは、app-server、rsyslog、redis-server、ad-connector、mnt-collector、mnt-processor、ca-server est-server、および elasticsearch です。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (63692139) 7 days, 8:55:21.39 SNMPv2-MIB::snmpTrapOID.0 = OID: HOSTRESOURCES- MIB::hrSWRunName HOSTRESOURCES- MIB::hrSWRunName = STRING: "redis-server:Running"

Cisco ISE は、次のステータスのトラップを設定済みの SNMP サーバーに送信します。

- Process Start（監視状態）
- Process Stop（監視されていない状態）
- Execution Failed：プロセスの状態が「Monitored」から「Execution failed」に変わるとトラップが送信されます。
- Does Not Exists：プロセスの状態が「Monitored」から「Does Not Exists」に変わるとトラップが送信されます。

SNMP サーバーで、すべてのオブジェクトについて一意のオブジェクト ID（OID）が生成され、値が OID に割り当てられます。SNMP サーバーの OID 値でオブジェクトを検索できます。

実行中のトラップの OID 値は running で、監視されないトラップ、存在しないトラップ、実行に失敗したトラップの OID 値は stopped です。

Cisco ISE は、HOST-RESOURCES MIB に属している hrSWRunName の OID を使用してトラップを送信し、< PROCESS NAME > - < PROCESS STATUS > として OID 値を設定します。たとえば、runtime - running として設定します。

Cisco ISE が SNMP トラップを SNMP サーバーに送信するのを停止させるには、Cisco ISE CLI から SNMP 設定を削除します。この操作によって、SNMP トラップの送信と、SNMP マネージャからのポーリングが停止されます。

Cisco ISE のディスク使用状況 SNMP トラップ

Cisco ISE のパーティションのディスク使用率がしきい値に到達し、設定された空きディスク領域の量に達すると、ディスク使用状況トラップが送信されます。

次の表に、Cisco ISE で設定可能なディスク使用状況 SNMP トラップのリストを示します。

OID	説明	トラップの例
.1.3.6.1.4.1.2021.9.1.9 \n UCD-SNMP-MIB::dskPercent	使用されているディスク容量の割合。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198297) 13 days, 16:19:42.97 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPercent UCD-SNMP-MIB::dskPercent = INTEGER: 13
.1.3.6.1.4.1.2021.9.1.2 \n UCD-SNMP-MIB::dskPath	ディスクがマウントされている場所のパス。 dskPath は、ISE 管理コマンド **show disks** の出力ですべてのマウントポイントのトラップを送信できます。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198304) 13 days, 16:19:43.04 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPath UCD-SNMP-MIB::dskPath = STRING: /opt

Cisco ISE アラーム

アラームは、ネットワークの重大な状態を通知し、[アラーム（Alarms）] ダッシュレットに表示されます。データ消去イベントなど、システムアクティビティの情報も提供されます。システムアクティビティの通知方法を設定したり、システムアクティビティを完全に無効にしたりできます。また、特定のアラームのしきい値を設定できます。

大半のアラームには関連付けられているスケジュールがなく、イベント発生後即時に送信されます。その時点で最新の 15,000 件のアラームのみが保持されます。

イベントが繰り返し発生する場合、同じアラームは約 1 時間抑制されます。イベントが繰り返し発生する間、トリガーによっては、アラームが再び表示されるまでに約 1 時間かかる場合があります。

アラーム名、カテゴリ、シビラティ（重大度）、またはステータスに基づいて、表示するアラームをフィルタリングできます。複数のフィルタを選択した場合、フィルタ結果は加算的になります。これはカスケード フィルタと呼ばれます。これにより、ドリルダウンして特定のデータを見つけることができます。

クイックフィルタを使用すれば、リストページに表示されるフィールド属性の値を入力し、ページをリフレッシュすることで、フィルタ基準に一致するレコードのみを一覧表示できます。

拡張フィルタを使用すれば、アラーム名に *TrustSec* を含むなど、指定した条件に基づいて情報をフィルタリングできます。複数の条件を指定できます。

自分だけがアクセスできるユーザー固有のカスタムフィルタを作成して保存できます。

[すべてのフィルタをクリア（Clear All Filters）] をクリックして、すべての適用されたフィルタを削除します。

次の表に、すべての Cisco ISE アラームおよびその説明と解決方法を示します。

表 *194 : Cisco ISE* アラーム

アラーム名	アラームの説明	アラームの解決方法
管理および操作の監査の管理		
過剰な RADIUS ネットワークデバイス通信（Excessive RADIUS Network Device Communication）	Cisco ISE で、4 時間の間に各 RADIUS 認証 syslog に対する RADIUS アカウンティング syslog を予想よりも多く受信しています。 このアラームは、Cisco ISE で 4 時間以内に各 RADIUS 認証 syslog に対して 6 つを超える RADIUS アカウンティング syslog を受信した場合にトリガーされます。	シスコのベストプラクティスの推奨事項に従ってNADが設定されていることを確認します。 詳細については、『Performance and Scalability Guide for Cisco Identity Services Engine』を参照してください。
過剰なエンドポイント通信（Excessive Endpoint Communication）	Cisco ISE で、4 時間の間にエンドポイントから予想よりも多くの RADIUS 通信メッセージを受信しています。 このアラームは、Cisco ISE で 4 時間以内にワイヤレスエンドポイントから 48 件を超える RADIUS 通信メッセージを受信した場合、または有線エンドポイントから 4 件を超える RADIUS 通信メッセージを受信した場合にトリガーされます。	エンドポイントがシスコのベストプラクティスの推奨事項に従って設定されていることを確認します。 詳細については、『Performance and Scalability Guide for Cisco Identity Services Engine』を参照してください。

アラーム名	アラームの説明	アラームの解決方法
管理証明書制御による再起動（Admin Certificate Controlled Restart）	プライマリ PAN で管理証明書が置き換えられました。設定に基づいてすべてのノードが再起動します。	設定された時間またはその前に、次のノードを再起動します。
管理証明書制御による再起動（Admin Certificate Controlled Restart）	次のノードは 5 日後に再起動します。	設定された時間またはその前に、次のノードを再起動します。
管理証明書制御による再起動（Admin Certificate Controlled Restart）	次のノードの再起動に失敗しました。イベントの詳細を確認し、必要に応じて手動で再起動します。	設定された時間またはその前に、次のノードを再起動します。
展開のアップグレードの失敗（Deployment Upgrade Failure）	ISE ノードでアップグレードに失敗しました。	アップグレードが失敗した原因と修正処置について、失敗したノードの ADE.log を確認します。
アップグレードバンドルのダウンロードの失敗（Upgrade Bundle Download failure）	アップグレードバンドルのダウンロードが ISE ノードで失敗しました。	アップグレードが失敗した原因と修正処置について、失敗したノードの ADE.log を確認します。
SXP 接続障害（SXP Connection Failure）	SXP 接続に失敗しました。	SXP サービスが実行していることを確認します。ピアに互換性があることを確認します。
シスコ プロファイルの全デバイスへの適用（Cisco profile applied to all devices）	ネットワーク デバイス プロファイルによって、MAB、Dot1X、CoA、Web リダイレクトなどのネットワーク アクセス デバイスの機能が定義されます。	シスコ以外のネットワーク デバイスの設定を必要に応じて編集し、適切なプロファイルを割り当てます。
CRL で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続（Secure LDAP connection reconnect due to CRL found revoked certificate）	CRL チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。LDAP サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバーにインストールします。
OCSP で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続（Secure LDAP connection reconnect due to OCSP found revoked certificate）	OCSP チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。LDAP サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバーにインストールします。

アラーム名	アラームの説明	アラームの解決方法
CRL で失効した証明書が見つかったことによるセキュア syslog 接続の再接続（Secure syslog connection reconnect due to CRL found revoked certificate）	CRL チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。syslog サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバーにインストールします。
OCSP で失効した証明書が見つかったことによるセキュアな syslog 接続の再接続（Secure syslog connection reconnect due to OCSP found revoked certificate）	OCSP チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。syslog サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバーにインストールします。
管理者アカウントがロック/無効（Administrator account Locked/Disabled）	パスワードの失効または不正なログイン試行のために、管理者アカウントがロックされているか、または無効になっています。詳細については、管理者パスワードポリシーを参照してください。	管理者パスワードは、GUI または CLI を使用して、他の管理者によってリセットできます。
ERS が非推奨の URL を検出（ERS identified deprecated URL）	ERS が廃止 URL を検出しました。	要求された URL は廃止されているため、使用しないでください。
ERS が古い URL を検出（ERS identified out-dated URL）	ERS が古い URL を検出しました。	要求された URL は古いため、新しい URL を使用してください。古い URL は今後のリリースで削除されません。
ERS 要求 Content-Type ヘッダーが古い（ERS request content-type header is outdated）	ERS 要求 Content-Type ヘッダーが最新ではありません。	要求 Content-Type ヘッダーで指定された要求のリソースバージョンが最新ではありません。これはリソーススキーマが変更されたことを意味します。いくつかの属性が追加または削除された可能性があります。古いスキーマをこのまま処理するために、ERS エンジンでデフォルト値が使用されます。
ERS XML 入力が XSS またはインジェクション攻撃の原因です（ERS XML input is a suspect for XSS or Injection attack）	ERS XML 入力が XSS またはインジェクション攻撃の原因になっています。	XML 入力を確認してください。

アラーム名	アラームの説明	アラームの解決方法
バックアップに失敗（Backup Failed）	ISE バックアップ操作に失敗しました。	Cisco ISE とリポジトリ間のネットワーク接続を確認します。次の点を確認します。 • リポジトリに使用しているログイン情報が正しいこと。 • リポジトリに十分なディスク領域があること。 • リポジトリユーザーが書き込み特権を持っていること。
CA サーバーがダウン（CA Server is down）	CA サーバーがダウンしています。	CA サービスが CA サーバーで稼働中であることを確認します。
CA サーバーが稼働中（CA Server is Up）	CA サーバーは稼働中です。	CA サーバーが稼働中であることを知らせる通知が管理者に送信されます。
証明書の有効期限（Certificate Expiration）	この証明書はまもなく有効期限が切れます。これが失効すると、Cisco ISE がクライアントとのセキュアな通信を確立しないようにします。	証明書を交換します。信頼できる証明書の場合、発行元の認証局（CA）にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書が失効（Certificate Revoked）	内部 CA がエンドポイントに発行した証明書を管理者が取り消しました。	もう一度 BYOD フローに従って最初から新しい証明書を使用してプロビジョニングします。
証明書プロビジョニング初期化エラー（Certificate Provisioning Initialization Error）	証明書プロビジョニングの初期化に失敗しました。	複数の証明書でサブジェクトの CN（CommonName）属性が同じ値になっています。証明書チェーンを構築できません。SCEP（Simple Certificate Enrollment Protocol）サーバーからの証明書を含め、システム内のすべての証明書を確認します。
証明書の複製に失敗（Certificate Replication Failed）	セカンダリノードへの証明書の複製に失敗しました。	証明書がセカンダリ ノードで無効であるか、他の永続的なエラー状態があります。セカンダリ ノードに矛盾する証明書が存在しないかどうかを確認します。存在する場合は、セカンダリノードに存在する証明書を削除し、プライマリノードの新しい証明書をエクスポートしてから削除し、その後インポートして複製を再試行します。

アラーム名	アラームの説明	アラームの解決方法
証明書の複製に一時的に失敗（Certificate Replication Temporarily Failed）	セカンダリノードへの証明書の複製に一時的に失敗しました。	証明書は、ネットワークの停止などの一時的な状態によりセカンダリノードに複製されませんでした。複製は、成功するまで再試行されます。
証明書が失効（Certificate Expired）	この証明書の期限が切れています。Cisco ISE がクライアントとのセキュアな通信を確立しないようにします。ノードツーノード通信も影響を受ける場合があります。	証明書を交換します。信頼できる証明書の場合、発行元の認証局（CA）にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書要求転送に失敗（Certificate Request Forwarding Failed）	証明書要求転送に失敗しました。	受信する証明書要求が送信者の属性に一致することを確認します。
設定が変更（Configuration Changed）	Cisco ISE 設定が更新されています。このアラームは、ユーザーとエンドポイントに設定変更があってもトリガーされません。	設定変更が想定どおりであるかどうかを確認します。
CRL の取得に失敗（CRL Retrieval Failed）	サーバーから CRL を取得できません。これは、指定した CRL が使用できない場合に発生します。	ダウンロード URL が正しく、サービスに使用可能であることを確認します。
DNS 解決に失敗（DNS Resolution Failure）	ノードで DNS 解決に失敗しました。	**ip name-server** コマンドで設定した DNS サーバーが到達可能であるか確認します。 **DNS Resolution failed for CNAME <hostname of the node>** というアラームが表示された場合は、各 Cisco ISE ノードの A レコードとともに CNAME RR を作成していることを確認します。
ファームウェアの更新が必要（Firmware Update Required）	このホスト上でファームウェアの更新が必要です。	ファームウェアの更新の入手方法については、Cisco TAC にお問い合わせください。
仮想マシン リソースが不十分（Insufficient Virtual Machine Resources）	このホストには、CPU、RAM、ディスク容量、IOPS（1 秒当たりの入出力処理）などの仮想マシン（VM）リソースが不足しています。	Cisco ISE ハードウェア設置ガイド [英語] に指定されている VM ホストの最小要件を確認します。

アラーム名	アラームの説明	アラームの解決方法
NTP サービスの障害（NTP Service Failure）	NTP サービスがこのノードでダウンしています。	これは、NTP サーバーと Cisco ISE ノードとの間に大きな時間差（1000 秒以上）があるために発生することがあります。NTP サーバーが正しく動作していることを確認し、**ntp server** <*servername*> CLI コマンドを使用して NTP サービスを再起動して、時間のずれを修正します。
NTP 同期に失敗（NTP Sync Failure）	このノードに構成されているすべての NTP サーバーが到達不能です。	CLI で **show ntp** コマンドを実行してトラブルシューティングします。Cisco ISE から NTP サーバーに到達可能であることを確認します。NTP 認証が設定されている場合、キー ID と値がサーバーの対応する値に一致することを確認します。
スケジュールされた設定バックアップなし（No Configuration Backup Scheduled）	Cisco ISE 設定バックアップがスケジュールされていません。	設定バックアップのスケジュールを作成します。
操作 DB 消去に失敗（Operations DB Purge Failed）	操作データベースから古いデータを消去できません。これは、MnT ノードがビジーの場合に発生します。	[データ消去の監査（Data Purging Audit）] レポートをチェックし、使用済みスペースがしきい値スペースより少ないことを確認します。CLI を使用して MnT ノードにログインし、消去操作を手動で実行します。
プロファイラ SNMP 要求に失敗（Profiler SNMP Request Failure）	SNMP 要求がタイム アウトしたか、あるいは SNMP コミュニティまたはユーザー認証データが不正です。	SNMP が NAD で動作していることを確認し、Cisco ISE の SNMP 設定が NAD に一致していることを確認します。
復元に失敗（Restore Failed）	Cisco ISE 復元操作に失敗しました。	Cisco ISE とリポジトリ間のネットワーク接続を確認します。リポジトリに使用するクレデンシャルが正しいことを確認します。バックアップファイルが破損していないことも確認します。CLI で **reset-config** コマンドを実行して、正常な既知の最終バックアップを復元します。
パッチに失敗（Patch Failure）	パッチ プロセスがサーバーで失敗しました。	サーバーにパッチプロセスを再インストールします。
パッチに成功（Patch Success）	パッチ プロセスがサーバーで成功しました。	—

アラーム名	アラームの説明	アラームの解決方法
外部 MDM サーバー API バージョンが不一致（External MDM Server API Version Mismatch）	外部 MDM サーバー API バージョンが Cisco ISE に設定されたものと一致しません。	MDM サーバー API バージョンが Cisco ISE に設定されたものと同じであることを確認します。Cisco ISE MDM サーバー設定を更新します（必要な場合）。
外部 MDM サーバー接続に失敗（External MDM Server Connection Failure）	外部 MDM サーバーへの接続に失敗しました。	MDM サーバーが稼働し、Cisco ISE-MDM API サービスが MDM サーバーで稼働していることを確認します。
外部 MDM サーバー応答エラー（External MDM Server Response Error）	外部 MDM サーバー応答エラーです。	Cisco ISE-MDM API サービスが MDM サーバーで適切に動作していることを確認します。
MDM コンプライアンスポーリングが無効（MDM Compliance Polling Disabled）	定期的なコンプライアンスポーリングで、膨大な非準拠デバイス情報を受信しました。	MDM サーバーに到達する非準拠デバイス要求の数を 20000 未満に維持します。
エンドポイント証明書が期限切れ（Endpoint certificates expired）	エンドポイント証明書が日次スケジュールジョブで期限切れとマークされました。	エンドポイントデバイスを再登録して新しいエンドポイント証明書を取得します。
エンドポイント証明書が消去（Endpoint certificates purged）	期限切れのエンドポイント証明書が日次スケジュールジョブによって消去されました。	特に対処は必要ありません。これは、管理者が開始したクリーンアップ操作です。
エンドポイントのアクティビティ消去（Endpoints Purge Activities）	過去 24 時間のエンドポイントのアクティビティを消去します。このアラームは、午前 0 時にトリガーされます。	**[操作（Operations）]** > **[レポート（Reports）]** > **[エンドポイントとユーザー（Endpoints and Users）]** > **[エンドポイントのアクティビティ消去（Endpoints Purge Activities）]** を選択して、消去アクティビティを確認します。
PAN 自動フェールオーバー：フェールオーバーが失敗しました（PAN Auto Failover - Failover Failed）	セカンダリ管理ノードへのプロモーション要求が失敗しました。	解決方法については、アラームの詳細を参照してください。
PAN 自動フェールオーバー：フェールオーバーがトリガーされました（PAN Auto Failover - Failover Triggered）	プライマリロールにセカンダリ管理ノードのフェールオーバーが正常にトリガーされました。	セカンダリ PAN のプロモーションが完了するまで待機し、古いプライマリ PAN を起動します。
PAN 自動フェールオーバー：ヘルスチェックの非アクティビティ（PAN Auto Failover - Health Check Inactivity）	PAN がモニタリングノードからヘルスチェックのモニタリング要求を受け取りませんでした。	報告されたモニタリングノードがダウンしているか、または同期していないか確認し、必要に応じて、手動同期をトリガーします。

アラーム名	アラームの説明	アラームの解決方法
PAN 自動フェールオーバー：無効なヘルスチェック（PAN Auto Failover - Invalid Health Check）	自動フェールオーバーで無効なヘルスチェックモニタリング要求が受信されました。	ヘルス チェック モニタリング ノードが同期していることを確認し、必要な場合は手動で同期をトリガーします。
PAN 自動フェールオーバー：プライマリ管理ノードのダウン（PAN Auto Failover - Primary Administration Node Down）	PAN がダウンしているか、またはモニタリングノードから到達不能です。	PAN を起動するか、またはフェールオーバーが発生するまで待機します。
PAN 自動フェールオーバー：フェールオーバーの試行が拒否されました（PAN Auto Failover - Rejected Failover Attempt）	ヘルス チェック モニター ノードによって行われたプロモーション要求をセカンダリ管理ノードが拒否しました。	解決方法については、アラームの詳細を参照してください。
EST サービスの停止（EST Service is down）	EST サービスが停止しています。	CA および EST サービスが稼働しており、証明書サービスのエンドポイントサブ CA 証明書チェーンが完了していることを確認します。
EST サービスの稼働（EST Service is up）	EST サービスが稼働しています。	EST サービスが稼働中であることを知らせる通知が管理者に送信されます。
Smart Call Home の通信障害（Smart Call Home Communication Failure）	Smart Call Home メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間にネットワーク接続があることを確認します。
テレメトリ メッセージの障害（Telemetry Communication Failure）	テレメトリ メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間にネットワーク接続があることを確認します。
アダプタに接続できない（Adapter not reachable）	Cisco ISE は、アダプタに接続できません。	エラーの詳細はアダプタ ログを確認してください。
アダプタのエラー（Adapter Error）	アダプタにエラーが生じています。	アラームの説明を確認してください。
アダプタ接続の失敗（Adapter Connection Failed）	アダプタは、送信元のサーバーに接続できません。	送信元のサーバーがアクセス可能であることを確認します。
エラーによるアダプタの停止（Adapter Stopped Due to Error）	アダプタにエラーが発生し、望ましい状態ではありません。	アダプタの設定が正しく、送信元サーバーがアクセス可能であることを確認してください。エラーの詳細については、アダプタログを確認してください。
サービス コンポーネントのエラー（Service Component Error）	サービス コンポーネントにエラーが生じています。	アラームの説明を確認してください。
サービス コンポーネントの情報（Service Component Info）	サービス コンポーネントが情報を送信しました。	なし。

アラーム名	アラームの説明	アラームの解決方法
ISE サービス		
過剰な TACACS 認証試行（Excessive TACACS Authentication Attempts）	ISE ポリシーサービスノードで TACACS 認証の割合が想定よりも多くなっています。	• ネットワーク デバイスの再認証タイマーをチェックします。 • ISEインフラストラクチャのネットワーク接続を確認します。
過剰なTACACS認証の失敗した試行（Excessive TACACS Authentication Failed Attempts）	ISE ポリシーサービスノードで失敗したTACACS認証の割合が想定よりも多くなっています。	• 根本原因を特定するために認証手順を確認します。 • ID と秘密の不一致がないか、ISE または NAD の設定を確認します。
AD コネクタを再起動する必要があった（AD Connector had to be restarted）	AD コネクタが突然シャットダウンし、再起動が必要となりました。	問題が解決しない場合は、Cisco TAC にお問い合わせください。
Active Directory フォレストが使用不可（Active Directory Forest is unavailable）	Active Directory フォレスト グローバル カタログが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
認証ドメインが使用不可（Authentication domain is unavailable）	認証ドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
承認結果（Authorization Result）	承認結果とアクティブセッションをモニターします。「認証結果アラームの設定（1991 ページ）」を参照してください。	矛盾がないか、ネットワークまたは Cisco ISE の設定変更を確認します。
ISE の認証非アクティビティ（ISE Authentication Inactivity）	Cisco ISE ポリシー サービス ノードは、ネットワーク デバイスから認証要求を受け取っていません。	• Cisco ISE および NAD の設定を確認します。 • Cisco ISE および NAD インフラストラクチャのネットワーク接続を確認します。
IDマッピングの認証非アクティビティ（ID Map. Authentication Inactivity）	過去 15 分間、ユーザー認証イベントが IDマッピングサービスによって収集されませんでした。	ユーザー認証が想定される時間（勤務時間など）である場合は、Active Directory ドメインコントローラへの接続を確認します。
CoA 失敗（COA Failed）	ネットワークデバイスが、Cisco ISEポリシーサービスノードによって発行された認可変更（CoA）要求を拒否しました。	そのネットワークデバイスが Cisco ISE からの CoA を受け入れるように設定されていることを確認します。CoA が有効なセッションに対して発行されているか確認します。

アラーム名	アラームの説明	アラームの解決方法
設定されたネームサーバーがダウン（Configured nameserver is down）	設定されたネームサーバーがダウンしているか、使用できません。	DNS 設定とネットワーク接続を確認します。
サプリカントが応答停止（Supplicant Stopped Responding）	Cisco ISE がクライアントに最後のメッセージを 120 秒前に送信しましたが、クライアントから応答がありません。	• サプリカントが Cisco ISE との完全な EAP カンバセーションを行えるように適切に設定されていることを確認します。 • サプリカントとの間で EAP メッセージを転送するように NAS が正しく設定されていることを確認します。 • サプリカントまたは NAS で、EAP カンバセーションのタイムアウトが短くないことを確認します。
過剰な認証試行（Excessive Authentication Attempts）	Cisco ISE ポリシー サービス ノードで認証の割合が想定よりも多くなっています。	ネットワークデバイスの再認証タイマーをチェックします。Cisco ISE インフラストラクチャのネットワーク接続を確認します。 しきい値が満たされた場合、[過剰な認証試行（Excessive Authentication Attempts）] および [過剰な失敗試行（Excessive Failed Attempts）] アラームがトリガーされます。[説明（Description）] 列の横に表示される数値は、過去 15 分間に Cisco ISE に対して成功または失敗した認証の総数です。
過剰な失敗試行（Excessive Failed Attempts）	Cisco ISE ポリシー サービス ノードで認証失敗の割合が想定よりも多くなっています。	根本原因を特定するために認証手順を確認します。ID と秘密の不一致がないか、Cisco ISE または NAD の設定を確認します。 しきい値が満たされた場合、[過剰な認証試行（Excessive Authentication Attempts）] および [過剰な失敗試行（Excessive Failed Attempts）] アラームがトリガーされます。[説明（Description）] 列の横に表示される数値は、過去 15 分間に Cisco ISE に対して成功または失敗した認証の総数です。
AD：マシン TGT の更新に失敗（AD: Machine TGT refresh failed）	ISE サーバーのチケット認可チケット（TGT）の更新に失敗しました。TGT は、Active Directory 接続とサービスに使用されます。	ISE マシン アカウントが存在し、有効であることを確認します。また、クロックスキュー、複製、ケルベロスの設定、またはネットワークエラー、あるいはこれらすべてを確認します。

アラーム名	アラームの説明	アラームの解決方法
AD：ISE アカウント パスワードの更新に失敗（AD: ISE account password update failed）	ISE サーバーは、AD マシン アカウント パスワードを更新できませんでした。	ISE マシン アカウント パスワードが変更されていないことと、マシン アカウントが無効でなく制限もされていないことを確認します。KDC への接続を確認します。
参加しているドメインが使用不可（Joined domain is unavailable）	参加しているドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
ID ストアが使用不可（Identity Store Unavailable）	Cisco ISE ポリシー サービス ノードは設定された ID ストアに到達できません。	Cisco ISE と ID ストア間のネットワーク接続を確認します。
正しく設定されていないネットワーク デバイスを検出（Misconfigured Network Device Detected）	Cisco ISE が、NAS からの過剰な RADIUS アカウンティング情報を検出しました。 このアラームは、デフォルトではディセーブルに設定されています。このアラームを有効にするには、「アラームの有効化および設定」を参照してください。	非常に多くの重複する RADIUS アカウンティング情報が、NAS から ISE に送信されました。正確なアカウンティング頻度で NAS を設定します。
正しく設定されていないサプリカントを検出（Misconfigured Supplicant Detected）	Cisco ISE が、ネットワーク上で正しく設定されていないサプリカントを検出しました。 このアラームは、デフォルトではディセーブルに設定されています。このアラームを有効にするには、「アラームの有効化および設定」を参照してください。	サプリカントの設定が正しいことを確認します。
アカウンティングの開始なし（No Accounting Start）	Cisco ISE ポリシーサービスノードではセッションを許可していますが、ネットワークデバイスからアカウンティングの開始を受信しませんでした。	RADIUS アカウンティングがネットワーク デバイス上に設定されていることを確認します。ローカル許可に対するネットワーク デバイス設定を確認します。
不明な NAD（Unknown NAD）	Cisco ISE ポリシー サービス ノードは、Cisco ISE に設定されていないネットワーク デバイスから認証要求を受信しています。	ネットワーク デバイスが正規の要求であるかどうかを確認してから、それを設定に追加します。シークレットが一致することを確認します。

アラーム名	アラームの説明	アラームの解決方法
SGACL がドロップ（SGACL Drops）	セキュリティ グループ アクセス（SGACL）ドロップが発生しました。これは、SGACL ポリシーの違反により、TrustSec 対応デバイスがパケットをドロップすると発生します。	RBACL ドロップ概要レポートを実行し、SGACL ドロップを引き起こしているソースを確認します。攻撃ソースに CoA を発行してセッションを再許可または切断します。
RADIUS 要求がドロップ（RADIUS Request Dropped）	NAD からの認証およびアカウンティング要求がサイレントに破棄されています。これは、NAD が不明であるか、共有秘密が不一致であるか、RFC ごとのパケット内容が無効であるために発生することがあります。 このアラームは、デフォルトではディセーブルに設定されています。このアラームを有効にするには、「アラームの有効化および設定」を参照してください。	NAD/AAA クライアントについて Cisco ISE に有効な設定があることを確認します。 NAD/AAA クライアントと Cisco ISE の共有秘密が一致しているかどうかを確認します。AAA クライアントとネットワーク デバイスにハードウェアの問題または RADIUS 互換性の問題がないことを確認します。また、Cisco ISE にデバイスを接続するネットワークにハードウェア上の問題がないことを確認します。
EAP セッションの割り当てに失敗（EAP Session Allocation Failed）	RADIUS 要求は EAP セッションの制限に達したためにドロップされました。この状態の原因として、並列 EAP 認証要求が多すぎることが考えられます。	新しい EAP セッションで別の RADIUS 要求を呼び出す前に数秒間待ちます。システムのオーバーロードが解消しない場合は、ISE サーバーの再起動を試してください。
RADIUS コンテキストの割り当てに失敗（RADIUS Context Allocation Failed）	RADIUS 要求はシステムのオーバーロードのためにドロップされました。この状態の原因として、並列認証要求が多すぎることが考えられます。	新しい RADIUS 要求を呼び出す前に数秒間待ちます。システムのオーバーロードが解消しない場合は、ISE サーバーの再起動を試してください。
AD：ISE のマシン アカウントにグループを取得するために必要な権限がない（AD: ISE machine account does not have the required privileges to fetch groups）	Cisco ISE のマシン アカウントにグループを取得するために必要な権限がありません。	Cisco ISE のマシンアカウントに Active Directory のユーザーグループを取得する権限があるか確認します。
ポスチャ設定の検出（Posture Configuration Detection）	ポスチャ状態同期ポートは、準拠する認証プロファイルに対してブロックされません。	クライアント ポスチャ ステータスが準拠している場合、ポスチャ状態同期プローブが Cisco ISE に到達しないように ACL を設定します。
MnT ルックアップに対するポスチャクエリが高い（Posture Query to MnT Lookup is High）	1 時間あたりの MnT セッション ルックアップに対するポスチャクエリが高くなっています。	ネットワーク設定を確認し、ISE ネットワーク外のクライアントから PSN に到達できないことを確認します。

アラーム名	アラームの説明	アラームの解決方法
ノードの複製		
複製低速情報（Slow Replication Info）	保留中のメッセージ数が 10,000 件を超えるか、メッセージの複製にかかる時間が 1 時間を超えると、低速またはスタックした複製が検出されます。	ノードが到達可能であり、展開の一部であることを確認し、負荷が高い場合は検証します。
複製低速警告（Slow Replication Warning）	保留中のメッセージ数が 20,000 件を超えるか、メッセージの複製にかかる時間が 3 時間を超えると、低速またはスタックした複製が検出されます。	ノードが到達可能であり、展開の一部であることを確認し、負荷が高い場合は検証します。
複製低速エラー（Slow Replication Error）	保留中のメッセージ数が 40,000 件を超えるか、メッセージの複製にかかる時間が 5 時間を超えると、低速またはスタックした複製が検出されます。	ノードが到達可能であり、展開の一部であることを確認し、負荷が高い場合は検証します。
複製に失敗（Replication Failed）	セカンダリ ノードは複製されたメッセージを消費できませんでした。	Cisco ISE GUI にログインし、[展開（Deployment）] ウィンドウから手動同期を実行するか、または影響を受けた Cisco ISE ノードを登録解除してから登録します。
複製が停止（Replication Stopped）	Cisco ISE ノードで PAN から設定データを複製できませんでした。	Cisco ISE GUI にログインし、[展開（Deployment）] ウィンドウから手動同期を実行するか、または影響を受けた Cisco ISE ノードを登録解除してから必須フィールドを指定して登録します。
システムの状態（System Health）		
ディスク I/O 使用率が高い（High Disk I/O Utilization）	Cisco ISE システムは、ディスク I/O 使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラアクティビティを確認します。負荷を分散するためのサーバーを追加します。
ディスク領域の使用率が高い（High Disk Space Utilization）	Cisco ISE システムは、ディスク領域の使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラアクティビティを確認します。負荷を分散するためのサーバーを追加します。

アラーム名	アラームの説明	アラームの解決方法
負荷平均が高い（High Load Average）	Cisco ISE システムは、不可平均が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラアクティビティを確認します。負荷を分散するためのサーバーを追加します。 サードパーティツールを使用してシングルCPUコアの負荷平均を確認しないでください。このメトリックにはシステム全体の負荷が反映されないためです。システム負荷の累積ビューには、Cisco ISE CLI で **tech top** コマンドを使用することをお勧めします。 プライマリおよびセカンダリ MnT ノードの 2:00 a.m. タイムスタンプに対して [負荷平均が高い（High Load Average）] アラームが表示される場合、この時刻に実行している DBMS 統計が原因で CPU 使用率が高くなっている可能性があります。DBMS統計が完了すると、CPU使用率は通常に戻ります。 [負荷平均が高い（High Load Average）] アラームは、毎週日曜日の午前 1 時に、毎週のメンテナンスタスクによってトリガーされます。このメンテナンスタスクによって、1 GB 以上の領域を占有するすべてのインデックスが再構築されます。このアラームは無視できます。

アラーム名	アラームの説明	アラームの解決方法
メモリ使用率が高い（High Memory Utilization）	Cisco ISE システムは、メモリ使用率が高くなっています。 このアラームは、メモリ使用率がしきい値に達するとトリガーされます。デフォルトのしきい値は 90%（MEMORY_UTILIZATION=90）です。これは設定できますが、デフォルトのしきい値を変更しないことを推奨します。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラアクティビティを確認します。負荷を分散するためのサーバーを追加します。 Cisco ISE CLI で **show memory** コマンドを使用して、メモリ使用率を確認することをお勧めします。 Cisco ISE ノードでは、オペレーティングシステムによってメモリ使用率が管理されます。メモリ使用率のより信頼できる測定値を得るには、（空きメモリではなく）使用可能なメモリのメトリックを確認する必要があります。 オペレーティングシステムは、バッファまたはキャッシュ内のほとんどのメモリをセグメント化することに注意してください。合計メモリの 90% 未満が使用済みとして表示され、スワップメモリに実質的な増加がない場合、Cisco ISE のメモリ使用率は安定していると見なすことができます。
操作 DB の使用率が高い（High Operations DB Usage）	ノードをモニターする Cisco ISE は、syslog データの量が想定よりも多くなっています。	操作データの消去設定ウィンドウを確認して削減します。
認証待ち時間が長い（High Authentication Latency）	Cisco ISE システムは、認証待ち時間が長くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラアクティビティを確認します。負荷を分散するためのサーバーを追加します。
ヘルス ステータスが使用不可（Health Status Unavailable）	モニタリングノードが Cisco ISE ノードからヘルスステータスを受信しませんでした。	Cisco ISE ノードが稼働していて、モニタリングノードと通信できることを確認します。
プロセスがダウン（Process Down）	Cisco ISE プロセスの 1 つが動作していません。	Cisco ISE アプリケーションを再起動します。
プロファイラ キューサイズの制限に到達（Profiler Queue Size Limit Reached）	ISE プロファイラキューサイズの制限に到達しました。キューサイズの制限に達した後に受信されたイベントはドロップされます。	システムに十分なリソースがあることを確認し、エンドポイント属性フィルタが有効になっていることを確認します。

アラーム名	アラームの説明	アラームの解決方法
OCSP トランザクションしきい値に到達（OCSP Transaction Threshold Reached）	OCSP トランザクションしきい値に到達しました。このアラームは、内部 OCSP サービスのトランザクション数がそのしきい値に到達するとトリガーされます。	システムに十分なリソースがあるかどうかを確認します。
ライセンシング		
ライセンスがまもなく期限切れ（License About to Expire）	Cisco ISE ノードにインストールされたライセンスがまもなく期限切れになります。	Cisco ISE の [ライセンス（Licensing）] ウィンドウを参照してライセンスの使用状況を確認します。
ライセンスが期限切れ（License Expired）	Cisco ISE ノードにインストールされたライセンスの期限が切れました。	シスコアカウントチームに問い合わせて、新しいライセンスを購入してください。
ライセンス違反（License Violation）	Cisco ISE ノードが、許可されたライセンス数を超過しているか、まもなく超過することを検出しました。	シスコアカウントチームに問い合わせて、追加のライセンスを購入してください。
スマートライセンスの認証の期限切れ（Smart Licensing Authorization Expired）	スマートライセンスの認証の有効期限が切れました。	[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照して、手動でスマートライセンスの登録を更新するか、Cisco Smart Software Manager とのネットワーク接続を確認してください。問題が続くようであれば、シスコ パートナーまでお問い合わせください。
スマートライセンスの認証の更新の失敗（Smart Licensing Authorization Renewal Failure）	Cisco Smart Software Manager を使用した認証の更新に失敗しました。	[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照し、[ライセンス（Licenses）] テーブルの [更新（Refresh）] ボタンを使用して、Cisco Smart Software Manager で認証を手動で更新します。問題が続くようであれば、シスコ パートナーまでお問い合わせください。
スマートライセンスの認証の更新の成功（Smart Licensing Authorization Renewal Success）	Cisco Smart Software Manager を使用した認証の更新に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の認証の更新が成功したことを知らせる通知が送信されます。
スマートライセンスの通信障害（Smart Licensing Communication Failure）	Cisco Smart Software Manager と Cisco ISE の通信が失敗しました。	Cisco Smart Software Manager とのネットワーク接続を確認します。問題が続く場合は、Cisco Smart Software Manager にログインするか、またはシスコパートナーまでお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
復元されたスマートライセンスの通信（Smart Licensing Communication Restored）	Cisco Smart Software Manager と Cisco ISE の通信が復元されました。	Cisco Smart Software Manager とのネットワーク接続が復元されたことを知らせる通知が送信されます。
スマートライセンスの登録解除の障害（Smart Licensing De-Registration Failure）	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に失敗しました。	詳細については、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。問題が続く場合は、Cisco Smart Software Manager にログインするか、またはシスコパートナーまでお問い合わせください。
スマートライセンスの登録解除の成功（Smart Licensing De-Registration Success）	Cisco Smart Software Manager を使用した Cisco ISE の登録に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に成功したことを知らせる通知が送信されます。
スマート ライセンスの無効化（Smart Licensing Disabled）	スマートライセンスは Cisco ISE で無効になっており、従来のライセンスが使用されています。	スマートライセンスを再度有効にするには、[ライセンスの管理（License Administration）] ウィンドウを参照してください。Cisco ISE のスマートライセンスの使用方法の詳細については、Cisco ISE 管理者ガイド [英語] を参照するか、シスコパートナーにお問い合わせください。
スマートライセンスの評価期間の期限切れ（Smart Licensing Evaluation Period Expired）	スマートライセンスの評価期間が終了しました。	Cisco Smart Software Manager を使用して Cisco ISE を登録するには、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。
スマート ライセンスの HA 役割の変更（Smart Licensing HA Role changed）	スマートライセンスの使用中に、ハイアベイラビリティの役割が変更されました。	Cisco ISE の HA ロールが変わったことを知らせる通知が送信されます。
スマート ライセンス ID 証明書の期限切れ（Smart Licensing Id Certificate Expired）	スマートライセンス証明書の期限が切れました。	手動でスマートライセンスの登録を更新するには、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。問題が続くようであれば、シスコ パートナーまでお問い合わせください。
スマート ライセンス ID 証明書の更新の失敗（Smart Licensing Id Certificate Renewal Failure）	Cisco Smart Software Manager を使用したスマートライセンスの登録の更新が失敗しました。	手動でスマートライセンスの登録を更新するには、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。問題が続くようであれば、シスコ パートナーまでお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
スマート ライセンス ID 証明書の更新の成功（Smart Licensing Id Certificate Renewal Success）	Cisco Smart Software Manager を使用したスマートライセンスの登録の更新が成功しました。	Cisco Smart Software Manager を使用した登録の更新が成功したことを知らせる通知が送信されます。
スマートライセンスの無効な要求（Smart Licensing Invalid Request）	無効な要求が Cisco Smart Software Manager に送信されました。	詳細については、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ウィンドウを参照してください。問題が続く場合は、Cisco Smart Software Manager にログインするか、またはシスコパートナーまでお問い合わせください。
コンプライアンスに準拠していないスマート ライセンス（Smart Licensing Out of Compliance）	Cisco ISE ライセンスがコンプライアンスに準拠していません。	詳細については、[ISE ライセンス管理（ISE License Administration）] ウィンドウを参照してください。新しいライセンスを購入するには、パートナーまたはシスコ アカウント チームにお問い合わせください。
スマートライセンスの登録の障害（Smart Licensing Registration Failure）	Cisco Smart Software Manager を使用した Cisco ISE の登録が失敗しました。	詳細については、[ISE ライセンス管理（ISE License Administration）] ウィンドウを参照してください。問題が続く場合は、Cisco Smart Software Manager にログインするか、またはシスコパートナーまでお問い合わせください。
スマートライセンスの登録の成功（Smart Licensing Registration Successful）	Cisco Smart Software Manager を使用した Cisco ISE の登録に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の登録に成功したことを知らせる通知が送信されます。
システム エラー		
ログ収集エラー（Log Collection Error）	コレクタプロセスをモニターする Cisco ISE が、ポリシーサービス ノードから生成された監査ログを使用して処理を継続できません。	これは、ポリシー サービス ノードの実際の機能に影響を与えません。その後の解決については、Cisco TAC にお問い合わせください。
スケジュールされているレポートのエクスポートに失敗（Scheduled Report Export Failure）	設定されたリポジトリにエクスポートされたレポート（CSV ファイル）をコピーできません。	設定されたリポジトリを確認します。それが削除されていた場合は、再度追加します。リポジトリが使用できないか、リポジトリに到達できない場合は、リポジトリを再設定して有効にします。
TrustSec		
不明な SGT のプロビジョニング（Unknown SGT was provisioned）	不明な SGT がプロビジョニングされました。	ISE は承認フローの一部として不明な SGT をプロビジョニングしました。不明な SGT は既知のフローの一部として割り当てることはできません。

アラーム名	アラームの説明	アラームの解決方法
一部の TrustSec ネットワーク デバイスに最新の ISE IP-SGT マッピング設定がありません（Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration）	一部の TrustSec ネットワーク デバイスに最新の ISE IP-SGT マッピング設定がありません。	ISE が異なる IP-SGT マッピング セットを持ついくつかのネットワーク デバイスを検出しました。[IP-SGT マッピング展開（IP-SGT Mapping Deploy）] オプションを使用してデバイスを更新します。
TrustSec SSH 接続の失敗（TrustSec SSH connection failed）	TrustSec SSH 接続に失敗しました。	ISE がネットワーク デバイスへの SSH 接続を確立できませんでした。[ネットワークデバイス（Network Device）] ウィンドウでネットワークデバイスの SSH ログイン情報がネットワークデバイス上のログイン情報と類似していることを確認します。ネットワークデバイスで ISE（IP アドレス）からの SSH 接続が有効になっていることを確認します。
TrustSec で識別された ISE が 1.0 以外の TLS バージョンで動作するよう設定されている（TrustSec identified ISE was set to work with TLS versions other than 1.0）	TrustSec で識別された ISE は 1.0 以外の TLS バージョンで動作するよう設定されています。	TrustSec は TLS バージョン 1.0 のみをサポートします。
TrustSec PAC の検証の失敗（Trustsec PAC validation failed）	TrustSec PAC の検証に失敗しました。	ISE がネットワークデバイスから送信された PAC を検証できませんでした。[ネットワークデバイス（Network Device）] ウィンドウとデバイスの CLI で、TrustSec デバイスのログイン情報を確認します。デバイスが ISE サーバーによってプロビジョニングされた有効な PAC を使用していることを確認します。
TrustSec 環境データのダウンロードの失敗（Trustsec environment data download failed）	TrustSec 環境データのダウンロードに失敗しました。	Cisco ISE は不正な環境データ要求を受信しました。 次のことを確認してください。 • 要求に PAC が存在し有効である。 • すべての属性が要求に存在している。
TrustSec CoA メッセージの無視（TrustSec CoA message ignored）	TrustSec CoA メッセージが無視されました。	Cisco ISE は、TrustSec CoA メッセージを送信し、応答を受信しませんでした。ネットワーク デバイスが CoA 対応であることを確認してください。ネットワーク デバイス設定を確認してください。

アラーム名	アラームの説明	アラームの解決方法
TrustSec のデフォルトの出力ポリシーの変更（TrustSec default egress policy was modified）	TrustSec のデフォルトの出力ポリシーが変更されました。	セキュリティ ポリシーに合致していることを確認します。

（注） アラームは、Cisco ISE にユーザーまたはエンドポイントを追加する場合にはトリガーされません。

アラーム設定

次の表では、[アラーム設定（Alarm Settings）] ウィンドウ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarm Settings）] > [アラームの設定（Alarm Configuration）] > [追加（Add）]**）のフィールドについて説明します。

フィールド名	説明
アラーム タイプ（Alarm Type）	アラームタイプ。
アラーム名（Alarm Name）	アラームの名前。
説明（Description）	アラームの説明。
推奨されるアクション（Suggested Actions）	アラームがトリガーされたときに実行されるアクション。
ステータス（Status）	アラームルールの有効化または無効化。
シビラティ（重大度）（Severity）	アラームのシビラティ（重大度）レベルを選択します。有効なオプションは次のとおりです。 • [重大（Critical）]：重大なエラーの条件を示します。 • [警告（Warning）]：正常ではあるものの重要な状態を示します。これがデフォルトの条件です。 • [情報（Info）]：情報メッセージを示します。

フィールド名	説明
syslog メッセージを送信（Send Syslog Message）	Cisco ISE で生成される各システムアラームの syslog メッセージを送信します。
複数の電子メールアドレスをカンマで区切って入力（Enter multiple e-mails separated with comma）	電子メールアドレスまたは ISE 管理者名あるいはその両方のリスト。
電子メールのメモ（0 ～ 4,000 文字）（Notes in Email (0 to 4000 characters)）	システムアラームに関連付けるカスタムテキストメッセージ。

認証結果アラームの設定

認証ポリシーの結果に基づいてアラームを設定できます。これにより、エンドポイント認証に対するネットワーキング、インフラストラクチャ、またはアプリケーションの変更の影響をモニターできます。特定のネットワーク デバイス グループ（NDG）を選択して、アラームの範囲を定義できます。選択した NDG ごとに、新しい認証結果アラームが作成されます。

特定の認証プロファイルとセキュリティグループタグ（SGT）を選択することで、このアラームでモニターする認証ログをフィルタ処理できます。指定された認証プロファイルおよびSGTを持つ認証ポリシーセットを満たしているエンドポイントのみがアラームによってモニターされます。

このアラームには、次のいずれかのしきい値を定義できます。

- 現在のアクティブセッションの総数。
- アクティブセッションの総数と比較した、選択された認証プロファイル、SGT、または両方を持つアクティブセッションの割合。
- 定義された期間に発生した、選択された認証プロファイル、SGT、または両方を持つエンドポイント認証の数。
- 定義された期間に生成された認証ログの総数と比較した、選択された認証プロファイル、SGT、または両方を持つエンドポイント認証の割合。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [アラーム設定（Alarm Settings）]**。

ステップ 2 アラームのリストから、[認証結果（Authorization Result）] の横にあるオプションボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 3 表示された新しいウィンドウの [アラーム設定（Alarm Configuration）] タブで、[しきい値（Thresholds）] 領域の次のフィールドを設定します。

a) [しきい値の対象（Threshold On）]：ドロップダウンリストから [アクティブセッション（Active Sessions）] または [設定された期間内の認証（Authorizations in Configured Time Period）] を選択します。

[アクティブセッション（Threshold On）]：アクティブセッションに基づいてアラームを定義します。

[設定された期間内の認証（Authorizations in Configured Time Period）]：定義された期間内のエンドポイント認証に基づいてアラームを定義します。

b) [しきい値タイプ（Threshold Type）]：ドロップダウンリストから [数（Number）] または [割合（Percentage）] を選択します。

c) [しきい値演算子（Threshold Operator）]：ドロップダウンリストから [次の値より大きい（Greater Than）] または [次の値より小さい（Less Than）] を選択します。

d) [しきい値（Threshold Value）]：テキストフィールドに、しきい値を入力します。有効な範囲は、[しきい値タイプ（Threshold Type）] が [数（Number）] の場合は 0 ー 999999、[しきい値タイプ（Threshold Type）] が [割合（Percentage）] の場合は 0 ー100 です。

e) [最後のデータを含む（分）（Include Data of Last (Minutes)）]：このフィールドは、[しきい値の対象（Threshold On）] ドロップダウンリストで [設定された期間内の認証（Authorizations in Configured Time Period）] を選択した場合にのみ表示されます。ドロップダウンリストから必要な値を選択します。

f) [実行間隔（Run Every）]：ドロップダウンリストからアラームのポーリング間隔を分単位で選択します。

ステップ 4 [フィルタ（Filters）] 領域で、このアラームに対してポーリングされる認証ログのフィルタを定義します。[認証プロファイル（Authorization Profile）] および [SGT] ドロップダウンリストから必要なオプションを選択します。

このアラームを正しく設定するには、[フィルタ（Filters）] 領域、認証プロファイル、または SGT でオプションを少なくとも 1 つ選択する必要があります。各フィルタで複数のオプションを選択できます。

ステップ 5 [範囲（Scope）] 領域でアラームの範囲を定義します。特定の NDG に関連するエンドポイント認証ログのみをポーリングするには、対応するドロップダウンリストから特定の NDG を選択します。選択した NDG ごとに、個別のアラームが作成されます。各 NDG のログを個別に表示および確認できます。ドロップダウンリストからオプションを選択しない場合、Cisco ISE のすべての NDG がこのアラームの範囲に含まれます。

ステップ 6 このアラームのアクティビティに関連する syslog メッセージを受信するには、[Syslogメッセージの送信（Send Syslog Message）] チェックボックスをオンにします。

syslog の送信先となる電子メールアドレスを、[複数の電子メールをカンマで区切って入力（Enter multiple e-mails separated with comma）] フィールドに入力します。syslog 電子メールに特定のメッセージを含めるには、[電子メールのメモ（Notes in Email）] フィールドにメッセージを入力します。

ステップ 7 [送信（Submit）] をクリックして設定を保存します。

ステップ 8 [アラーム通知（Alarm Notification）] タブで、アラーム通知の送信先となる電子メールアドレスを入力します。[複数の電子メールアドレスをカンマで区切って入力（Enter multiple e-mails separated with comma）]

フィールドに、受信者の電子メールアドレスを入力します。送信者の電子メールアドレスを[送信者の電子メールを入力（Enter sender e-mail）] フィールドに入力します。

ステップ 9 [保存（Save）] をクリックします。

認証結果アラームは、Cisco ISE の [ダッシュボード（Dashboard）] の [アラーム（Alarms）] ダッシュレットに表示されます。このアラームの詳細には、フィルタとして選択された認証プロファイルまたはSGTを含む各認証ポリシーのヒットカウントが含まれます。その後、特定の認証ポリシーを確認して、エンドポイントの認証に影響を与えるネットワーク、インフラストラクチャ、またはアプリケーションの変更を特定できます。

カスタム アラームの追加

Cisco ISE には [メモリ使用率が高い（High Memory Utilization）]、[設定変更（Configuration Change）] など 12 種類のデフォルト アラームがあります。シスコ定義のシステムアラームは [アラーム設定（Alarms Settings）] ウィンドウ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [管理（(Administration)）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarms Settings）]）に表示されます。システム アラームだけを編集できます。

既存のシステムアラームに加えて、既存のアラームタイプでカスタムアラームを追加、編集、削除できます。

アラームタイプごとに、最大 5 つのアラームを作成できます。アラームの総数は 200 に制限されます。

[アラーム設定（Alarm Settings）] ウィンドウの [アラーム設定（Alarm Configuration）] タブの [条件（Conditions）] 列に、[認証待ち時間が長い（High Authentication Latency）]、[ディスク I/O 使用率が高い（High Disk I/O Utilization）]、[ディスク領域の使用率が高い（High Disk Space Utilization）]、[メモリ使用率が高い（High Memory Utilization）] の 4 つのアラームの詳細が表示されます。これらのアラームには、設定可能なしきい値があります。ただし、[条件（Conditions）]列には、しきい値が設定された後でも詳細が表示されないことがあります。表示されない場合は、そのアラームの関連するしきい値フィールドを再編集して、[条件（Conditions）] 列に詳細を表示します。

アラームを追加するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarm Settings）]**

ステップ 2 [アラームの設定（Alarm Configuration）] タブで、[追加（Add）] をクリックします。

ステップ 3 次の必須詳細情報を入力します。詳細については、「アラーム設定」の項を参照してください。

アラームタイプに基づいて（[メモリ使用率が高い（High Memory Utilization）]、[過剰な RADIUS 認証試行（Excessive RADIUS Authentication Attempts）]、[過剰な TACACS 認証試行（Excessive TACACS Authentication Attempts）] など）、追加の属性が [アラーム設定（Alarm Configuration）] ウィンドウに表示されます。たとえば、設定変更アラームには、[オブジェクト名（Object Name）]、[オブジェクトタイプ（Object Types）]

および[管理者名（Admin Name）]フィールドが表示されます。さまざまな基準で同じアラームの複数のインスタンスを追加できます。

ステップ 4 [Submit] をクリックします。

Cisco ISE アラーム通知およびしきい値

Cisco ISE アラームを有効または無効にし、重大な状態を通知するようにアラーム通知動作を設定できます。特定のアラームに対して、過剰な失敗試行アラームの最大失敗試行数、または高ディスク使用量アラームの最大ディスク使用量などのしきい値を設定できます。

通知の設定はアラームベースで設定し、アラームごとに通知する必要があるユーザーの電子メール ID を入力できます（システム定義アラームとユーザー定義アラームの両方）。

（注） アラーム ルール レベルで指定された受信者の電子メール アドレスは、グローバルの受信者の電子メール アドレスより優先されます。

アラームの有効化および設定

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarm Settings）]**

ステップ 2 オプションボタンをクリックして、デフォルトアラームのリストからアラームを選択し [編集（Edit）] をクリックします。

ステップ 3 [ステータス（Status）] ドロップダウンリストから [有効（Enable）] または [無効（Disable）] を選択します。

ステップ 4 アラームしきい値を必要に応じて設定します。

ステップ 5 [送信（Submit）] をクリックします。

モニタリング用の Cisco ISE アラーム

Cisco ISE は、重大なシステム状態が発生するたびに通知するシステムアラームを提供します。Cisco ISE によって生成されたアラームは [アラーム（Alarm）] ダッシュレットに表示されます。これらの通知は、自動的に [アラーム（Alarm）] ダッシュレットに表示されます。

[アラーム（Alarm）] ダッシュレットには、最近のアラームのリストが表示されます。このリストから、表示するアラームの詳細を選択できます。電子メールおよびsyslogメッセージを介してアラームの通知を受信することもできます。

モニタリング アラームの表示

ステップ 1 Cisco ISE **ダッシュボード**に進みます。

ステップ 2 [アラーム（Alarm）] ダッシュレットでアラームをクリックします。アラームの詳細および推奨アクションを含むダイアログボックスが開きます。

ステップ 3 アラームをリフレッシュするには、[リフレッシュ（Refresh）] をクリックします。

ステップ 4 確認応答アラームは、アラームを既読としてマークすることで、アラームカウンタ（アラームの発生回数）を削減します。タイムスタンプの横にあるチェックボックスをオンにして、確認するアラームを選択します。

[確認応答（Acknowledge）] ドロップダウンリストから [選択済みの確認応答（Acknowledge Selected）] を選択して、ウィンドウに現在表示されているすべてのアラームを既読としてマークします。デフォルトでは、100 行がウィンドウに表示されます。[行/ページ（Rows/Page）] ドロップダウンリストから値を選択することで、表示する別の行数を選択できます。

[確認応答（Acknowledge）] ドロップダウンリストから **[すべての確認応答（Acknowledge All）]** を選択して、ウィンドウに現在表示されているかどうかに関係なく、リストにあるすべてのアラームを既読としてマークします。

（注） タイトル行の [タイムスタンプ（Time Stamp）] の隣にあるチェックボックスをオンにすると、ウィンドウに表示されているすべてのアラームが選択されます。ただし、選択した 1 つ以上のアラームのチェックボックスをオフにすると、全選択機能が無効になります。この時点で、[タイムスタンプ（Time Stamp）] の隣にあるチェックボックスがオフになっていることがわかります。

ステップ 5 選択したアラームに対応する [詳細（Details）] リンクをクリックします。選択したアラームに対応する詳細を含むダイアログボックスが開きます。

（注） ペルソナの変更前に生成されたアラームに対応する [詳細（Details）] リンクには、データは表示されません。

ログ収集

モニタリング サービスはログと設定データを収集し、そのデータを保存してから、レポートおよびアラームを生成するために処理します。展開内の任意のサーバーから収集されたログの詳細を表示できます。

アラーム syslog 収集場所

システム アラーム通知を syslog メッセージとして送信するようにモニタリング機能を設定した場合は、通知を受信する syslog ターゲットが必要です。アラーム syslog ターゲットは、アラーム syslog メッセージが送信される宛先です。

（注） Cisco ISE モニタリングでは、logging-source interface の設定にネットワーク アクセス サーバー（NAS）の IP アドレスを使う必要があります。Cisco ISE モニタリング用のスイッチを設定する必要があります。

syslog メッセージを受信するには、syslog サーバーとして設定されたシステムも必要です。アラーム syslog ターゲットを作成、編集、および削除できます。

リモートロギングターゲットをアラームターゲットとして設定するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモートロギングターゲット（Remote Logging Targets）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [新しいロギングターゲット（New Logging Target）] ウィンドウで、ロギングターゲットに必要な詳細を送信し、[このターゲットのアラームを含める（Include Alarms for this Target）] チェックボックスをオンにします。

RADIUS ライブ ログ

次の表では、最近の RADIUS 認証を表示する [ライブログ（Live Logs）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [RADIUS] > [ライブログ（Live Logs）]**を選択します。RADIUS ライブログはプライマリ PAN でのみ確認できます。

表 *195 : RADIUS* ライブ ログ

フィールド名	説明
時刻（Time）	モニタリングおよびトラブルシューティング収集エージェントがログを受信した時刻を表示します。このカラムは必須です。選択解除することはできません。
ステータス（Status）	認証の成功/失敗を表示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。

フィールド名	説明
詳細（**Details**）	そのセッションのアカウンティングイベントが処理された場合、[詳細（Details）] 列の下にあるアイコンをクリックすると、[アカウンティングの詳細（Accounting Detail）] レポートが開きます。セッションが認証済みの状態である場合、[詳細（Details）] 列の下にあるアイコンをクリックすると、[認証の詳細（Authentication Detail）] レポートが表示されます。 [認証の詳細（Authentication Detail）] レポートの [応答時間（Response Time）] は、Cisco ISE で認証フローを処理するのにかかった合計時間です。たとえば、認証が 3 つのラウンドトリップメッセージで構成されている場合（最初のメッセージは 300 ミリ秒、次のメッセージは 150 ミリ秒、最後のメッセージは 100 ミリ秒）、[応答時間（Response Time）] は、300 + 150 + 100 = 550 ミリ秒になります。 （注） 7 日を超えてアクティブになっているエンドポイントの詳細を表示することはできません。7 日を超えてアクティブになっているエンドポイントの [詳細（Details）] アイコンをクリックすると、次のメッセージがウィンドウに表示されます。`No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.`
繰り返し回数（**Repeat Count**）	ID、ネットワークデバイス、および許可のコンテキストで変更がなく、直近の 24 時間で認証要求が繰り返された回数を表示します。
ID（**Identity**）	ログイン済みの認証に関連付けられているユーザー名を示します。 ユーザー名が ID ストアに存在しない場合は、`INVALID` と表示されます。その他の原因で認証に失敗した場合は、`USERNAME` と表示されます。 （注） これはユーザーにのみ適用されます。これは MAC アドレスには適用されません。 デバッグをサポートするために、無効なユーザー名の開示を ISE に強制できます。これを行うには、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]** で [無効なユーザー名を開示する（Disclose invalid usernames）] チェックボックスをオンにします。また、[無効なユーザー名を開示する（Disclose Invalid Usernames）] オプションを設定して、タイムアウトを設定し、手動でオフにする必要をなくすこともできます。
エンドポイント ID（**Endpoint ID**）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。

フィールド名	説明
エンドポイントプロファイル（Endpoint Profile）	プロファイリングされるエンドポイントのタイプを示します（たとえば、iPhone、Android、MacBook、Xbox になるようにプロファイリングされます）。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（Authorization Policy）	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル（Authorization Profiles）	認証に使用された認証プロファイルを表示します。
IP アドレス（IP Address）	エンドポイントデバイスの IP アドレスを表示します。
ネットワークデバイス（Network Device）	ネットワーク アクセス デバイスの IP アドレスを表示します。
デバイスポート（Device Port）	エンドポイントが接続されているポート番号を表示します。
ID グループ（Identity Group）	ログの生成対象となるユーザーまたはエンドポイントに割り当てられる ID グループを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
サーバー（Server）	ログの生成元になったポリシーサービスが示されます。
MDMサーバー名（MDM Server Name）	MDM サーバーの名前を表示します。
イベント（Event）	イベントステータスを表示します。

フィールド名	説明
失敗の理由（**Failure Reason**）	認証が失敗した場合、失敗の詳細な理由を表示します。
認証方式（**Auth Method**）	Microsoft チャレンジハンドシェイク認証プロトコルバージョン 2（MS-CHAPv2）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（**Authentication Protocol**）	Protected Extensible Authentication Protocol（PEAP）や Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）など、使用される認証プロトコルを表示します。
セキュリティグループ（**Security Group**）	認証ログによって識別されるグループを表示します。
セッション ID（**Session ID**）	セッション ID を表示します。

（注） [RADIUS ライブログ（RADIUS Live Logs）] と [TACACS+ ライブログ（TACACS+ Live Logs）] ウィンドウでは、各ポリシーの認証ルールに対する最初の属性として [クエリ済み PIP（Queried PIP）] エントリが表示されます。認証ルール内のすべての属性が、以前のルールについてすでにクエリされているディクショナリに関連している場合、追加の [クエリ済み PIP（Queried PIP）] エントリは表示されません。

[RADIUS ライブログ（RADIUS Live Logs）] ウィンドウでは、次の操作を実行できます。

- データを CSV または PDF 形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタ処理します。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） ユーザーのカスタマイズはすべて、ユーザー設定として保存されます。

TACACS ライブ ログ

次の表では、TACACS+ AAA の詳細を表示する [TACACS ライブログ（TACACS Live Logs）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]**>**[TACACS]**>**[ライブログ（Live Logs）]**。TACACS ライブ ログはプライマリ PAN だけで表示されます。

表 *196 : TACACS* ライブ ログ

フィールド名	使用上のガイドライン
生成日時（Generated Time）	特定のイベントがトリガーされた時点に基づいて、syslog の生成日時を示します。
ログに記録された時刻（Logged Time）	syslog がモニタリング ノードによって処理され、保存された時刻を示します。このカラムは必須です。選択解除することはできません。
ステータス（Status）	認証の成功/失敗を表示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細（Details）	虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。
セッションキー（Session Key）	ISE によってネットワーク デバイスに返される（EAP の成功メッセージまたはEAP の失敗メッセージにある）セッション キーを示します。
ユーザー名（Username）	デバイス管理者のユーザー名を示します。このカラムは必須です。選択解除することはできません。
タイプ（Type）	[認証（Authentication）] および [承認（Authorization）] の 2 つのタイプで構成されます。認証、承認、または両方を通過または失敗したユーザー名を表示します。このカラムは必須です。選択解除することはできません。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（Authorization Policy）	特定の許可に選択されているポリシーの名前を表示します。
ISEノード（ISE Node）	アクセス要求が処理される ISE ノードの名前を表示します。

フィールド名	使用上のガイドライン
ネットワークデバイス名（**Network Device Name**）	ネットワーク デバイスの名前を示します。
ネットワークデバイスIP（**Network Device IP**）	アクセス要求を処理するネットワーク デバイスのIPアドレスを示します。
ネットワークデバイスグループ（**Network Device Groups**）	ネットワークデバイスが属する対応するネットワーク デバイス グループの名前を表示します。
デバイスタイプ（**Device Type**）	異なるネットワークデバイスからのアクセス要求の処理に使用されるデバイスタイプポリシーを示します。
ロケーション（**Location**）	ネットワークデバイスからのアクセス要求の処理に使用されるロケーションベースのポリシーを示します。
デバイスポート（**Device Port**）	アクセス要求が行われるデバイスのポート番号を示します。
失敗の理由（**Failure Reason**）	ネットワークデバイスによって行われたアクセス要求を拒否した理由を示します。
リモートアドレス（**Remote Address**）	エンドステーションを一意に識別するIPアドレス、MACアドレス、またはその他の任意の文字列を示します。
一致したコマンドセット（**Matched Command Set**）	MatchedCommandSet 属性値が存在する場合はその値を表示し、MatchedCommandSet属性値が空の場合、または属性自体がsyslogに存在しない場合は空の値を表示します。
シェルプロファイル（**Shell Profile**）	ネットワークデバイスでコマンドを実行するためのデバイス管理者に付与された権限を示します。

[TACACSライブログ（TACACS Live Logs）] ウィンドウで、次の手順を実行できます。

- データを CSV または PDF 形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタ処理します。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。

- 列の値をソートします。

（注） ユーザーのカスタマイズはすべて、ユーザー設定として保存されます。

ライブ認証

[ライブ認証（Live Authentications）] ウィンドウから、最新の RADIUS 認証を発生時に監視できます。このウィンドウには、直近の 24 時間における上位 10 件の RADIUS 認証が表示されます。ここでは、[ライブ認証（Live Authentications）] ウィンドウの機能について説明します。

[ライブ認証（Live Authentications）] ウィンドウには、認証イベントの発生時に、その認証イベントに対応するライブ認証エントリが表示されます。このウィンドウには、認証エントリに加えて、そのイベントに対応するライブセッションエントリも表示されます。また、表示するセッションをドリルダウンして、そのセッションに対応する詳細レポートを表示できます。

[ライブ認証（Live Authentications）] ウィンドウには、最近の RADIUS 認証が発生順に表形式で表示されます。[ライブ認証（Live Authentications）] ウィンドウの下部に表示される最終更新には、サーバー日付、時刻、およびタイムゾーンが示されます。

（注） アクセス要求パケット内のパスワード属性が空の場合、エラーメッセージがトリガーされ、アクセス要求は失敗します。

1 つのエンドポイントが正常に認証されると、2 つのエントリが [ライブ認証（Live Authentications）] ウィンドウに表示されます。1 つのエントリは認証レコードに対応し、もう 1 つのエントリは（セッションライブビューからプルされた）セッショレコードに対応しています。その後、デバイスで別の認証が正常に実行されると、セッション レコードに対応する繰り返しカウンタの数が増えます。[ライブ認証（Live Authentications）] ウィンドウに表示される繰り返しカウンタには、抑制されている重複した RADIUS 認証成功メッセージの数が示されます。

デフォルトで表示されるライブ認証データカテゴリを参照してください。各カテゴリついては、「最近の RADIUS 認証」を参照してください。

すべての列を表示するか、選択したデータ列のみ表示することを選択できます。表示する列を選択した後で、選択内容を保存できます。

ライブ認証のモニター

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[RADIUS]** > **[ライブログ（Live Logs）]**

ステップ 2 データリフレッシュレートを変更するには、[更新（Refresh）] ドロップダウンリストから時間間隔を選択します。

ステップ 3 データを手動で更新するには、[更新（Refresh）] アイコンをクリックします。

ステップ 4 表示されるレコードの数を変更するには、[表示（Show）] ドロップダウンリストからオプションを選択します。

ステップ 5 時間間隔を指定するには、[次の範囲内（Within）] ドロップダウンリストからオプションを選択します。

ステップ 6 表示される列を変更するには、[列の追加または削除（Add or Remove Columns）] をクリックし、ドロップダウンリストからオプションを選択します。

ステップ 7 ウィンドウの下部にある [保存（Save）] をクリックして、変更を保存します。

ステップ 8 ライブ RADIUS セッションを表示するには、[ライブセッションの表示（Show Live Sessions）] をクリックします。

アクティブな RADIUS セッションを動的に制御できるライブセッションに対して動的な認可変更（CoA）機能を使用できます。ネットワーク アクセス デバイス（NAD）に再認証または接続解除要求を送信できます。

[ライブ認証（Live Authentications）] ページでのデータのフィルタ処理

[ライブ認証（Live Authentications）] ウィンドウのフィルタを使用して、必要な情報をフィルタ処理し、ネットワーク認証の問題を迅速にトラブルシューティングできます。[認証ライブログ（Authentication live logs）] ウィンドウのレコードをフィルタ処理して、目的のレコードのみを表示できます。認証ログには多数の詳細が含まれており、特定のユーザーまたはロケーションから認証をフィルタリングすることで、データをすばやくスキャンできます。[ライブ認証（Live Authentications）] ウィンドウで使用できる複数の演算子を使用し、次のような検索条件に基づいてレコードをフィルタ処理できます。

- 'abc'：「abc」を含む
- '!abc'：「abc」を含まない
- '{}'：空である
- '!{}'：空ではない
- 'abc*'：「abc」で始まる
- '*abc'：「abc」で終わる
- '\!'、'*'、'\{'、'\\'：エスケープ

エスケープオプションを使用すると、特殊文字を含むテキストをフィルタリングできます（フィルタとして使用される特殊文字を含む）。特殊文字の前にバック スラッシュ（\）を付ける必要があります。たとえば、「Employee!」という ID を持つユーザーの認証レコードを確認する場合は、[ID フィルタ（Identity Filter）] フィールドに「Employee\!」と入力します。この例では、Cisco ISE は感嘆符（!）を特殊文字ではなくリテラル文字と見なします。

また、[ステータス（Status）] フィールドでは、成功した認証レコード、失敗した認証、ライブセッションなどのみをフィルタ処理できます。緑色のチェックマークは以前発生したすべての成功した認証をフィルタ処理します。赤い十字マークはすべての失敗した認証をフィルタリングします。青い [i] アイコンはすべてのライブセッションをフィルタ処理します。これらのオプションの組み合わせを表示することも選択できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[RADIUS]** > **[ライブログ（Live Logs）]**。

ステップ 2 [ライブ認証の表示（Show Live Authentications）] ウィンドウのいずれかのフィールドに基づいてデータをフィルタ処理します。

成功または失敗した認証、あるいはライブ セッションに基づいて結果をフィルタリングできます。

RADIUS ライブ セッション

次の表では、ライブ認証が表示される [RADIUSライブセッション（RADIUS Live Sessions）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。RADIUS ライブ セッションはプライマリ PAN だけで表示されます。

表 *197 : RADIUS* ライブ セッション

フィールド名	説明
開始（Initiated）	セッション開始時のタイムスタンプを表示します。
更新済み（Updated）	変更のためにセッションが最後に更新された時点のタイムスタンプを表示します。
アカウント セッション時間（Account Session Time）	ユーザー セッションの期間（秒単位）を表示します。
セッション ステータス（Session Status）	エンドポイントデバイスの現在のステータスを表示します。
アクション（Action）	アクティブなRADIUSセッションを再認証または切断するには、[アクション（Actions）] アイコンをクリックします。
繰り返し回数（Repeat Count）	ユーザーまたはエンドポイントの再認証回数を表示します。

フィールド名	説明
エンドポイント ID（Endpoint ID）	エンドポイントの一意の識別子を表示します。通常はMACまたはIPアドレスです。
ID（Identity）	エンドポイントデバイスのユーザー名を表示します。
IP アドレス（IP Address）	エンドポイントデバイスの IP アドレスを表示します。
監査セッション ID（Audit Session ID）	固有のセッション ID を表示します。
アカウント セッション ID（Account Session ID）	ネットワークデバイスから提供される一意の ID を表示します。
エンドポイント プロファイル（Endpoint Profile）	デバイスのエンドポイントプロファイルを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
セキュリティ グループ（Security Group）	認証ログによって識別されるグループを表示します。
サーバー（Server）	ログを生成したポリシー サービス ノードを示します。
認証方式（Auth Method）	パスワード認証プロトコル（PAP）、チャレンジハンドシェイク認証プロトコル（CHAP）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（Authentication Protocol）	Protected Extensible Authentication Protocol（PEAP）や Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）など、使用される認証プロトコルを表示します。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。

フィールド名	説明
許可ポリシー（**Authorization Policy**）	特定の許可に選択されているポリシーの名前を表示します。
許可プロファイル（**Authorization Profiles**）	認証に使用された許可プロファイルを表示します。
NAS IP アドレス（**NAS IP Address**）	ネットワークデバイスの IP アドレスを表示します。
デバイス ポート（**Device Port**）	ネットワークデバイスに接続されたポートを表示します。
PRA アクション（**PRA Action**）	ネットワークでのコンプライアンスのためにクライアントが正常にポスチャされた後、そのクライアントで実行される定期的な再評価アクションを表示します。
ANCステータス（**ANC Status**）	デバイスの適応型ネットワーク制御のステータス（[隔離（Quarantine）]、[隔離解除（Unquarantine）]、または[シャットダウン（Shutdown）]）を表示します。
WLC ローミング（**WLC Roam**）	ローミング中にエンドポイントがワイヤレス LAN コントローラ（WLC）間でハンドオフされたことを追跡するために使用されるブール値（Y/N）を表示します。cisco-av-pair=nas-update の値は Y または N です。 （注） Cisco ISE では、セッションの状態がローミングであるかの判定を WLC の nas-update=true 属性に依存して行っています。元の WLC が nas-update=true のアカウンティング停止属性を送信する場合、再認証を回避するために ISE のセッションは削除されません。ローミングが失敗する場合、ISE は 5 日間非アクティブだった場合にセッションを消去します。
パケット入力（**Packets In**）	受信したパケットの数を表示します。
パケット出力（**Packets Out**）	送信したパケットの数を表示します。
受信バイト数（**Bytes In**）	受信したバイト数を表示します。
送信バイト数（**Bytes Out**）	送信したバイト数を表示します。

フィールド名	説明
セッション送信元（Session Source）	RADIUS セッションであるか、パッシブ ID セッションであるかを示します。
ユーザードメイン名（User Domain Name）	ユーザーの登録済み DNS 名を示します。
ホストドメイン名（Host Domain Name）	ホストの登録済み DNS 名を示します。
ユーザーNetBIOS名（User NetBIOS Name）	ユーザーの NetBIOS 名を示します。
ホストNetBIOS名（Host NetBIOS Name）	ホストの NetBIOS 名を示します。
ライセンスのタイプ（License Type）	使用されているライセンスのタイプ（Base、Plus、Apex、または Plus と Apex）を表示します。
ライセンスの詳細（License Details）	ライセンスの詳細を表示します。

フィールド名	説明
プロバイダー（Provider）	エンドポイントイベントはさまざまなsyslogソースから学習されます。これらのsyslogソースはプロバイダーと呼ばれます。 • Windows Management Instrumentation（WMI）：WMIは、オペレーティングシステム、デバイス、アプリケーション、およびサービスに関する管理情報にアクセスするための共通インターフェイスとオブジェクトモデルを提供するWindowsサービスです。 • エージェント：クライアントまたは別のプログラムの代わりにクライアントで実行されるプログラム。 • syslog：クライアントがイベントメッセージを送信するロギングサーバー。 • REST：クライアントはターミナルサーバーで認証されます。このsyslogソースの場合、[TSエージェントID（TS Agent ID）]、[開始送信元ポート（Source Port Start）]、[終了送信元ポート（Source Port End）]、[最初の送信元ポート（Source First Port）]の値が表示されます。 • SPAN：ネットワーク情報はSPANプローブを使用して検出されます。 • DHCP：DHCPイベント。 • エンドポイント （注） 異なるプロバイダの2つのイベントがエンドポイントセッションから学習または取得されると、それらのプロバイダは[ライブセッション（Live Sessions）]ウィンドウにカンマ区切り値として表示されます。
MACアドレス（MAC Address）	クライアントのMACアドレスを表示します。
エンドポイントチェック時刻（Endpoint Check Time）	エンドポイントプローブによってエンドポイントが最後にチェックされた時刻を表示します。
エンドポイントチェック結果（Endpoint Check Result）	エンドポイントプローブの結果が表示されます。設定可能な値は次のとおりです。 • [到達不要（Unreachable）] • [ユーザー ログアウト（User Logout）] • [アクティブ ユーザー（Active User）]

フィールド名	説明
送信元ポートの開始（Source Port Start）	（REST プロバイダーの場合にのみ値が表示されます。）ポート範囲の最初のポートの番号を示します。
送信元ポートの終了（Source Port End）	（REST プロバイダーの場合にのみ値が表示されます。）ポート範囲の最後のポート番号を示します。
最初の送信元ポート（Source First Port）	（REST プロバイダーの場合にのみ値が表示されます）ターミナル サーバー エージェントによって割り当てられた最初のポートを示します。 ターミナルサーバーとは、複数のエンドポイントがモデムまたはネットワーク インターフェイスなしで接続でき、複数のエンドポイントが LAN ネットワークに接続できるようにするサーバーまたはネットワークデバイスを指します。複数のエンドポイントに同一 IP アドレスが割り当てられている場合、特定ユーザーの IP アドレスの識別が困難になります。このため、特定ユーザーを識別する目的でターミナル サーバー エージェントがサーバーにインストールされ、各ユーザーにポート範囲が割り当てられます。これにより、IP アドレス - ポート - ユーザーのマッピングが作成されます。
TS エージェント ID（TS Agent ID）	（REST プロバイダーの場合にのみ値が表示されます）エンドポイントにインストールされているターミナル サーバー エージェントの一意の ID を表示します。
AD ユーザー解決 ID（AD User Resolved Identities）	（AD ユーザーの場合にのみ値が表示されます。）一致したアカウントの候補が表示されます。
AD ユーザー解決 DN（AD User Resolved DNs）	（AD ユーザーの場合にのみ値が表示されます。）AD ユーザーの識別名（例：CN=chris,CN=Users,DC=R1,DC=com）を表示します。

エクスポート サマリ

過去7日間にすべてのユーザーによってエクスポートされたレポートの詳細をステータスとともに表示できます。エクスポートサマリには、手動レポートとスケジュールされたレポートの両方が含まれます。[エクスポートの概要（Export Summary）] ウィンドウは、2 分ごとに自動的に更新されます。[更新（Refresh）]アイコンをクリックすると、[エクスポートの概要（Export Summary）] ウィンドウが手動で更新されます。

ネットワーク管理者は、[進行中（In-Progess）] または [キュー登録済み（Queued）] 状態のエクスポートを取り消すことができます。他のユーザーは、自分が開始したエクスポートプロセスをキャンセルすることのみが許可されています。

デフォルトでは、任意の時点で3つのレポートの手動エクスポートのみを実行でき、残りのトリガーされたレポートの手動エクスポートはキューに入れられます。スケジュールされたレポートのエクスポートには、このような制限はありません。

（注） キューに入れられた状態のすべてのレポートが再度スケジューリングされ、Cisco ISE サーバーの再起動時に [進行中（In-progress）] または [キャンセル処理中（Cancellation-in-progress）] 状態のレポートには [失敗しました（failed）] とマークがつきます。プライマリ MnT ノードがダウンしている場合、スケジュールされたレポートエクスポートジョブはセカンダリ MnT ノードで実行されます。

次の表では、[エクスポートの概要（Export Summary）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）] > [レポート（Reports）] > [エクスポートの概要（Export Summary）]**。

表 *198* : エクスポート サマリ

フィールド名	説明
エクスポートされたレポート（Report Exported）	レポートの名前を表示します。
エクスポート実行ユーザー（Exported By）	エクスポート プロセスを開始したユーザーのロールを示します。
スケジュール済み（Scheduled）	レポートのエクスポートが予定されているものであるかどうかを示します。
トリガー時刻（Triggered On）	システムでエクスポートプロセスがトリガーされた時刻を示します。
リポジトリ（Repository）	エクスポートされたデータを格納するリポジトリの名前を表示します。
フィルタ パラメータ（Filter Parameters）	レポートのエクスポート中に選択されたフィルタパラメータを示します。

フィールド名	説明
ステータス（**Status**）	エクスポートされたレポートのステータスを示します。次のいずれかを設定できます。 • キュー（Queued） • 進行中（In-progress） • 完了（Completed） • キャンセル処理中（Cancellation-in-progress） • キャンセル済み（Cancelled） • 失敗しました（Failed） • 省略（Skipped） （注） [失敗しました（Failed）] ステータスは、失敗の理由を示します。[省略（Skipped）] ステータスは、プライマリ MnT ノードがダウンしているため、スケジュールされたレポートのエクスポートが省略されることを示します。

[エクスポートの概要（Export Summary）] ウィンドウで次の操作を実行できます。

- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。

認証概要レポート

認証要求に関連する属性に基づいて、特定のユーザー、デバイス、または検索条件についてネットワークアクセスをトラブルシューティングできます。このトラブルシューティングは、[認証概要（Authentication Summary）] レポートを実行して行います。

（注） 過去 30 日間の認証概要レポートのみを生成できます。

ネットワーク アクセスの問題のトラブルシューティング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[デバイス管理（Device Administration）]** > **[認証の要約レポート（Authentication Summary Report）]**。

ステップ 2 [失敗の理由（Failure Reasons）] でレポートをフィルタリングします。

ステップ 3 レポートの [失敗の理由別の認証（Authentication by Failure Reasons）] セクションのデータを確認し、ネットワークアクセスの問題をトラブルシューティングします。

（注） [認証の要約レポート（Authentication Summary Report ）] には失敗または成功した認証に対応する最新データが収集されて表示されるため、レポートの内容は数分遅れて表示されます。

展開およびサポート情報のための Cisco Support Diagnostics

概要

Cisco Support Diagnostics Connector は、Cisco Technical Assistance Center（TAC）とシスコサポートエンジニアがプライマリ管理ノードから展開の情報を取得するのに役立つ新機能です。TAC は、展開内の特定のノードのサポート情報を取得するのにコネクタを使用します。このデータにより、より迅速でより多くの情報を得たうえでのトラブルシューティングが可能になります。

Cisco Support Diagnostics Connector は、Cisco ISE 管理ポータルを使用して有効化します。この機能を使用すると、セキュリティサービス交換（SSE）クラウドポータルを活用して、展開内のプライマリポリシー管理ノードと Cisco Support Diagnostics の間の双方向接続が可能になります。

前提条件

- Cisco Support Diagnostics を有効または無効にするには、Super Admin または System Admin ロールが必要です。

Cisco Support Diagnostics Connector の設定

Cisco Support Diagnostics 機能を有効にするには、次の手順を実行します。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[Network Success Diagnostics]** > **[Cisco Support Diagnostics]** > **[Cisco Support Diagnostics 設定（Cisco Support Diagnostics Setting）]** を選択します。
- この機能は、デフォルトで無効にされています。有効になっていない場合は、[Cisco Support Diagnostics の有効化（Enable Cisco Support Diagnostics）] チェックボックスをオンにして、Cisco Support Diagnostics を有効にします。

Cisco Support Diagnostics の双方向接続の確認

Cisco ISE が Cisco Support Diagnostics に正常に登録されていることと、双方向接続がセキュリティサービス交換ポータルを介して確立されていることを確認するには、次の手順を実行します。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[監査（Audit）]** > **[変更構成監査（Change Configuration Audit）]** を選択します。
- 次の状態を確認してください。
  1. Cisco Support Diagnostics が有効化されています。
  2. ISE サーバーは Cisco Support Diagnostics に登録されています。
  3. ISE SSE サービスが Cisco Support Diagnostics に登録されています。
  4. Cisco Support Diagnostics の双方向接続は有効になっています。
- サービスの詳細（有効または無効、登録済みまたは未登録、Cisco Support Diagnostics の一部として登録または未登録）については、[操作監査（Operations Audit）] ウィンドウ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** > **[監査（Audit）]** > **[操作監査（Operations Audit）]**）でも確認できます。

トラブルシューティング情報

Cisco Support Diagnostics の双方向接続が切断されていると考えられる場合は、次のことを確認します。

- [スマートライセンス（Smart Licensing）]：スマートライセンスを無効にすると、Cisco Support Diagnostics は自動的に無効になります。スマート ライセンスを再度有効にしてコネクタを有効にします。
- [セキュリティサービス交換クラウドへの接続（Connectivity to Security Services Exchange cloud）]：Cisco Support Diagnostics が有効になっている場合、Cisco ISE はセキュリティサービス交換ポータルとの間で確立された永続的な接続を継続的にチェックします。この接続が切断されていることが判明した場合は、重大なアラーム「アラーム：Cisco Support Diagnostics の双方向接続が切断されています（Alarms: The Cisco Support Diagnostics bi-directional connectivity is broken）」がトリガーされます。前述の構成手順を使用して、機能を再度有効にします。

関連情報

管理者は、これらの特定のタスクを実行するために、ERS API を使用できます。

- 特定のノードのサポート情報をトリガーします。
- トリガーされたサポート バンドルのステータスを取得します。
- サポート バンドルをダウンロードします。
- 展開の情報を取得します。

使用方法やその他の情報については、ERS SDK のページを参照してください。

Cisco Support Diagnostics Connector を使用した構成バックアップの取得

この機能により、Cisco Technical Assistance Center（TAC）およびシスコのサポートエンジニアは、設定のバックアップをトリガーし、バックアップファイルを Cisco Support Diagnostics フォルダにアップロードできます。Cisco Support Diagnostics フォルダにアップロードしたバックアップファイルは、Cisco ISE ローカルディスクから削除できます。

この機能を使用するには、Cisco ISE でスマートライセンスと Cisco Support Diagnostics を有効にする必要があります。Cisco Support Diagnostics を有効にするには、次の手順を実行します。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[管理（Administration）] > [システム（System）] > [設定（Settings）] > [Network Success Diagnostics] > [Cisco Support Diagnostics] > [Cisco Support Diagnostics設定（Cisco Support Diagnostics Setting）] を選択します。
2. [Cisco Support Diagnosticsの有効化（Enable Cisco Support Diagnostics）] チェックボックスをオンにして、Cisco Support Diagnostics を有効にします。

次の方法を使用して、設定のバックアップをトリガーし、バックアップファイルを Cisco Support Diagnostics フォルダにアップロードします。

1. REST API は、ISE 統合会社名の組織 ID を取得するために使用されます。
2. デバイスのリストを取得するには、REST API の組織 ID を使用します。
3. REST API を使用してサービス ID を取得します。
4. サービス ID と組織 ID は、JSON Web トークン（JWT）の生成に使用されます。
5. REST API は、デバイス ID をパスパラメータとして使用して、デバイスで使用可能なサービスを確認するために使用されます。
6. REST API は、Cisco ISE から Cisco Support Diagnostics フォルダにバックアップファイルをアップロードするために使用されます。バックアップファイルのアップロードステータスを確認できます。ファイルが Cisco Support Diagnostics フォルダにアップロードされていない場合は、404 エラーが表示されます。

診断トラブルシューティング ツール

診断ツールは、Cisco ISE ネットワークの問題の診断およびトラブルシューティングに役立ち、問題解決方法の詳細な手順が提供されます。これらのツールを使用して、認証をトラブルシューティングし、TrustSec デバイスなど、ネットワーク上のネットワークデバイスの設定を評価できます。

RADIUS 認証のトラブルシューティング ツール

このツールを使用すると、予期せぬ認証結果がある場合に、RADIUS 認証または RADIUS 認証に関連する Active Directory を検索および選択して、トラブルシューティングを実行できます。認証が成功すると予想していたのに失敗した場合、または特定の権限レベルが付与されていると予想していたユーザーやマシンにそれらの権限が付与されていなかった場合に、このツールを使用します。

- トラブルシューティングのために、ユーザー名、エンドポイント ID、ネットワーク アクセス サービス（NAS）の IP アドレス、および認証失敗理由に基づいて RADIUS 認証を検索すると、Cisco ISE はシステム（現在）の日付の認証だけを表示します。
- トラブルシューティングのために NAS ポートに基づいて RADIUS 認証を検索すると、Cisco ISE は前月の初めから現在までのすべての NAS ポート値を表示します。

（注） NAS IP アドレスおよび [エンドポイント ID（Endpoint ID）] フィールドに基づいて RADIUS 認証を検索する場合、検索はまず運用データベースで実行されてから、構成データベースで実行されます。

予期せぬ RADIUS 認証結果のトラブルシューティング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[トラブルシューティング（Troubleshooting）]** > **[診断ツール（Diagnostic Tools）]** > **[一般ツール（General Tools）]** > **[RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）]** を選択します。

ステップ 2 必要に応じてフィールドに検索条件を指定します。

ステップ 3 [検索（Search）] をクリックして、検索条件に一致する RADIUS 認証を表示します。

Active Directory 関連の認証を検索する際に、展開に Active Directory サーバーが設定されていない場合は、「AD が設定されていない」ことを示すメッセージが表示されます。

ステップ 4 テーブルから RADIUS 認証レコードを選択し、[トラブルシューティング（Troubleshoot）] をクリックします。

Active Directory 関連の認証をトラブルシューティングするには、[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] > [AD ノード（AD node）] で、診断ツールにアクセスします。

ステップ 5 [ユーザー入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更して、[送信（Submit）] をクリックします。

ステップ 6 [完了（Done）] をクリックします。

ステップ 7 トラブルシューティングが完了したら、[結果概要の表示（Show Results Summary）] をクリックします。

ステップ 8 （任意）診断、問題を解決するための手順、およびトラブルシューティングの概要を表示するには、[完了（Done）] をクリックします。

Execute Network Device Command 診断ツール

Execute Network Device Command 診断ツールを使用すると、ネットワーク デバイスに対して **show** コマンドを実行することができます。

表示される結果は、コンソールに表示されるものと同じです。ツールにより、デバイス構成の問題（ある場合）を特定できます。

このツールは、ネットワークデバイスの構成を検証するか、またはネットワークデバイスの設定方法を確認する場合に使用します。

Execute Network Device Command 診断ツールにアクセスするには、次のナビゲーションパスのいずれかを選択します。

1. Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[操作（Operations）]** > **[トラブルシュート（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[ネットワークデバイスコマンドの実行（Execute Network Device Command）]** を選択します。Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[トラブルシュート（Troubleshoot）]** > **[ネットワークデバイスコマンドの実行（Execute Network Device Command）]** を選択します。
2. 表示される [ネットワークデバイスコマンドの実行（Execute Network Device Command）] ウィンドウで、ネットワークデバイスの IP アドレスと実行する **show** コマンドを対応するフィールドに入力します。
3. [実行（Run）] をクリックします。

設定を確認する Cisco IOS show コマンドの実行

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般ツール（General Tools）]** > **[ネットワーク デバイス コマンドの実行（Execute Network Device Command）]**。

ステップ 2 該当するフィールドに情報を入力します。

ステップ 3 [実行（Run）] をクリックして、指定したネットワーク デバイスでコマンドを実行します。

ステップ 4 [ユーザー入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更します。

ステップ 5 [送信（Submit）] をクリックして、ネットワーク デバイス上でコマンドを実行し、出力を表示します。

設定バリデータの評価ツール

この診断ツールを使用して、ネットワークデバイスの設定を評価し、設定の問題（ある場合）を特定できます。Expert Troubleshooterによって、デバイスの設定が標準設定と比較されます。

エージェントレスポスチャのトラブルシューティング

エージェントレス ポスチャ レポートは、エージェントレスポスチャが想定どおりに動作しない場合に使用する主要なトラブルシューティングツールです。このレポートには、スクリプトアップロードの完了、スクリプトアップロードの失敗、スクリプト実行の完了などのイベントを含む、エージェントレスフローの段階が既知の失敗の理由（ある場合）とともに表示されます。

（注） エージェントレス ポスチャ スクリプトは自身を検証できませんが、スクリプトの実行後に、Cisco ISE から受信したデータを検証します。

エージェントレスポスチャのトラブルシューティングには、次の2つの場所からアクセスできます。

- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[操作（Operations）]>[ライブログ（Live Logs）] を選択し、トラブルシューティングするクライアントの [ポスチャステータス（Posture Status）] 列にある縦に並んだ 3 つのドットをクリックします。
- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断（Diagnostics）] > [一般ツール（General Tools）] > [エージェントレスポスチャのトラブルシューティング（Agentless Posture Troubleshooting）]**。

エージェントレスポスチャのトラブルシューティング ツールは、指定されたクライアントのエージェントレスポスチャアクティビティを収集します。[エージェントレス ポスチャ フロー（Agentless Posture Flow）] はポスチャを開始し、現在アクティブなクライアントと Cisco ISE 間のすべてのデータのやり取りを表示します。[クライアントログのみをダウンロード（Only Download Client Logs）] は、クライアントからの最大 24 時間分のポスチャフローを含むログを作成します。クライアントはいつでもログを削除できます。収集が完了したら、ログの ZIP ファイルをエクスポートできます。

レポート

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [操作（Operations）] > [レポート（Reports）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] > [エージェントレスポスチャ（Agentless Posture）] を選択すると、エージェントレスポスチャを実行したすべてのエンドポイントが表示されます。

ネットワーク デバイス設定の問題のトラブルシューティング

ステップ 1 Cisco ISE GUI で、[メニュー（Menu）] アイコン（☰）をクリックし、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [設定バリデータの評価（Evaluate Configuration Validator）]** を選択します。

ステップ 2 評価するネットワークデバイスの IP アドレスを、[ネットワークデバイス IP（Network Device IP）] フィールドに入力します。

ステップ 3 チェックボックスをオンにして、推奨テンプレートと比較する設定オプションの横にあるオプションボタンをクリックします。

ステップ 4 [実行（Run）] をクリックします。

ステップ 5 [進行状況の詳細…（Progress Details ...）] 領域で、[ここをクリックしてログイン情報を入力（Click Here to Enter Credentials）] をクリックします。

ステップ 6 [ログイン情報ウィンドウ（Credentials Window）] ダイアログボックスで、ネットワークデバイスとの接続を確立するために必要な接続パラメータとログイン情報を入力します。

ステップ 7 [送信 (Submit)] をクリックします。

ステップ 8 （オプション）ワークフローをキャンセルするには、[進行状況の詳細（Progress Details ...）] ウィンドウで [ここをクリックして実行中のワークフローをキャンセル（Click Here to Cancel the Running Workflow）] をクリックします。

ステップ 9 （オプション）分析するインターフェイスの隣にあるチェックボックスをオンにして、[送信（Submit）] をクリックします。

ステップ 10 （オプション）設定の評価の詳細については、[結果概要の表示（Show Results Summary）] をクリックします。

エンドポイント ポスチャの障害のトラブルシューティング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ポスチャのトラブルシューティング（Posture Troubleshooting）]**。

ステップ 2 該当するフィールドに情報を入力します。

ステップ 3 [検索（Search）] をクリックします。

ステップ 4 説明を見つけ、イベントの解決策を決定するには、リストでイベントを選択し、[トラブルシューティング（Troubleshoot）] をクリックします。

セッション トレース テスト ケース

このツールを使用すると、予測できる方法でポリシーフローをテストし、実際のトラフィックを実際のデバイスから発信することなく、ポリシーの設定方法を確認、検証できます。

テストケースで使用する属性と値のリストを設定できます。これらの詳細情報を使用して、ポリシーシステムとのデータのやり取りが行われ、実行時のポリシー呼び出しがシミュレートされます。

属性はディクショナリを使用して設定できます。[属性（Attributes）] フィールドに、単純な RADIUS 認証で使用可能なディクショナリがすべて示されます。

（注） 単純な RADIUS 認証のテストケースのみを設定できます。

セッション トレース テスト ケースの設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [セッション トレース テスト ケース（Session Trace Test Cases）]。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [テストの詳細（Test Details）] タブで、テストケースの名前と説明を入力します。

ステップ 4 事前定義テストケースを 1 つ選択するか、または必須属性と属性の値を設定します。使用可能な事前定義テスト ケースを次に示します。

- [基本認証済みアクセス（Basic Authenticated Access）]
- [プロファイリングされている Cisco Phone（Profiled Cisco Phones）]
- [準拠デバイス アクセス（Compliant Devices Access）]
- [Wi-Fi ゲスト（リダイレクト）（Wi-Fi Guest (Redirect)）]
- [Wi-Fi ゲスト（アクセス）（Wi-Fi Guest (Access)）]

事前定義テストケースを選択すると、Cisco ISE によりそのテストケースの関連する属性に自動的に値が取り込まれます。これらの属性のデフォルト値を使用するか、または表示されるオプションから値を選択できます。テストケースにカスタム属性を追加することもできます。

テストケースに追加する属性と値は、（[カスタム属性（Custom Attributes）] フィールドの下の）[テキスト（Text）] フィールドに表示されます。[テキスト（Text）] フィールドの内容を編集すると、Cisco ISE により更新後の内容の有効性と構文がチェックされます。

[テストの詳細（Test Details）] ウィンドウの下部で、すべての属性の概要を確認できます。

ステップ 5 [送信（Submit）] をクリックします。

Cisco ISE はテストの詳細を保存する前に、属性と属性の値を検証してエラーがある場合はエラーを表示します。

ステップ 6 [テスト ビジュアライザ（Test Visualizer）] タブで、このテスト ケースを実行するノードを選択します。

（注） [ISE ノード（ISE Node）] ドロップダウン リストには、ポリシー サービス ペルソナを担当するノードだけが表示されます。

[ユーザー グループ/属性（User Groups/Attributes）] をクリックして、外部 ID ストアからユーザーのグループと属性を取得します。

ステップ 7 [実行（Execute）] をクリックします。

Cisco ISE がテストケースを実行し、テストケースのステップごとの結果が表形式で表示されます。ポリシー ステージ、一致ルール、結果オブジェクトが表示されます。緑色のアイコンをクリックして各ステップの詳細を表示します。

ステップ 8 （任意）[以前のテスト実行（Previous Test Executions）] タブをクリックし、以前のテストの実行結果を表示します。2 つのテストケースを選択して比較することもできます。Cisco ISE では、各テストケースの属性の比較ビューが表形式で表示されます。

ステップ 9 [RADIUS ライブログ（RADIUS Live Logs）] ウィンドウから [セッション トレース テスト ケース（Session Trace Test Case）] ツールを起動できます。[セッション トレース テスト ケース（Session Trace Test Case）] ツールを起動するには、[ライブログ（Live Logs）] ウィンドウでエントリを選択し、（[詳細（Details）] 列の）[アクション（Actions）] アイコンをクリックします。Cisco ISE により、対応するログエントリから関連する属性と値が抽出されます。必要に応じてそれらの属性と値を変更してから、テストケースを実行できます。

着信トラフィックを検証する TCP ダンプユーティリティ

パケットをスニッフィング する TCP ダンプユーティリティを使用して、予定していたパケットがノードに到達したかどうかを確認できます。たとえば、レポートに示されている着信認証またはログがない場合、着信トラフィックがない、または着信トラフィックが Cisco ISE に到達できないのではないかと疑うことがあります。このような場合、検証するためにこのツールを実行できます。

TCP ダンプオプションを設定し、ネットワークトラフィックからデータを収集して、ネットワークの問題をトラブルシューティングできます。

ネットワーク トラフィックのモニタリングでの TCP ダンプの使用

[TCP ダンプ（TCP Dump）] ウィンドウには、作成した TCP ダンププロセスファイルが一覧表示されます。目的に応じて異なるファイルを作成し、必要に応じて実行し、不要になったら削除できます。

収集するデータは、サイズ、ファイル数、プロセスの実行時間を指定することによって制御できます。制限時間内にプロセスが終了し、ファイルが最大サイズ未満で、複数のファイルを有効にしている場合、プロセスは続行され、別のダンプファイルが作成されます。

ボンディングされたインターフェイスを含む、複数のインターフェイスで TCP ダンプを実行できます。

（注） 可読形式のオプションはなくなり、ダンプファイルは常に RAW 形式になります。

シスコは、リポジトリへの IPv6 接続をサポートしています。

始める前に

[TCP ダンプ（TCP Dump）] ウィンドウの [ネットワーク インターフェイス（Network Interface）] ドロップダウンリストには、IPv4 または IPv6 アドレスが設定されているネットワーク インターフェイス カード（NIC）のみが表示されます。VMware のデフォルトでは、すべての NIC が接続されるため、すべての NIC に IPv6 アドレスが設定されて、[ネットワーク インターフェイス（Network Interface）] ドロップダウンリストに表示されます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [TCP ダンプ（TCP Dump）]**。

ステップ 2 [ホスト名（Host Name）] ドロップダウンリストから、TCP ダンプユーティリティのソースを選択します。

ステップ 3 [ネットワーク インターフェイス（Network Interface）] ドロップダウンリストから、モニターするインターフェイスを選択します。

ステップ 4 [フィルタ（Filter）] フィールドに、フィルタ処理のもとになるブール式を入力します。

サポートされている標準 TCP ダンプフィルタ式は、次のとおりです。

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 and not 10.77.122.119

ステップ 5 この TCP ダンププロセスの [ファイル名（File Name）] を入力します。

ステップ 6 [リポジトリ（Repository）] ドロップダウンリストから、TCP ダンプログファイルを保存するリポジトリを選択します。

ステップ 7 [ファイルサイズ（File Size）] ドロップダウンリストから、最大ファイルサイズを選択します。

ダンプがこのファイルサイズを超えると、新しいファイルが開いてダンプが続行されます。新しいファイルに変わるまでダンプを続行できる回数は、[制限（Limit to）] 設定によって制限されます。

ステップ 8 [制限（Limit to）] オプションを使用すると、ダンプを拡張できるファイルの数を制限できます。

ステップ 9 [時間制限（Time Limit）] オプションを使用すると、ダンプが終了するまでの実行時間を設定できます。

ステップ 10 [オン（On）] または [オフ（Off）] をクリックして無差別モードを設定します。デフォルトは [オン（On）] です。

無差別モードは、ネットワーク インターフェイスがシステムの CPU にすべてのトラフィックを渡すデフォルト パケット スニッフィング モードです。[オン（On）] のままにしておくことを推奨します。

TCP ダンプ ファイルの保存

始める前に

「ネットワークトラフィックのモニタリングでの TCP ダンプの使用」の項の説明に従って、タスクを完了しておく必要があります。

（注） Cisco ISE CLI を使用して TCP ダンプにアクセスすることもできます。詳細については、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [TCP ダンプ（TCP Dump）]**。

ステップ 2 [ダウンロード（Download）] をクリックし、目的の場所に移動して、[保存（Save）] をクリックします。

ステップ 3 （任意）以前のダンプファイルを保存せずに削除するには、[削除（Delete）] をクリックします。

エンドポイントまたはユーザーの予期しない SGACL の比較

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [TrustSec ツール（TrustSec Tools）] > [出力（SGACL）ポリシー（Egress (SGACL) Policy）]** を選択します。

ステップ 2 SGACL ポリシーを比較する TrustSec デバイスのネットワークデバイス IP アドレスを入力します。

ステップ 3 [実行（Run）] をクリックします。

ステップ 4 [ユーザー入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更します。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 [結果概要の表示（Show Results Summary）] をクリックして、診断および推奨される解決手順を表示します。

出力ポリシー診断フロー

出力ポリシー診断ツールでは、次の表に示すプロセスが使用されます。

プロセス ステージ	説明
1	指定した IP アドレスを使用してデバイスに接続し、送信元 SGT と宛先 SGT の各ペアに対するアクセスコントロールリスト（ACL）を取得します。
2	Cisco ISE に設定された出力ポリシーをチェックし、送信元 SGT と宛先 SGT の各ペアに対する ACL を取得します。
3	ネットワーク デバイスから取得された SGACL ポリシーと、Cisco ISE から取得された SGACL ポリシーを比較します。
4	ポリシーが一致しない送信元 SGT と宛先 SGT のペアを表示します。また、追加情報として、一致するエントリも表示します。

SXP-IP マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[TrustSec ツール（TrustSec Tools）]** > **[SXP-IP マッピング（SXP-IP Mappings）]**。

ステップ 2 ネットワーク デバイスの IP アドレスを入力します。

ステップ 3 [選択（Select）] をクリックします。

ステップ 4 [実行（Run）] をクリックします。

Expert Troubleshooter によって、ネットワークデバイスから TrustSec SXP 接続が取得されて、ピア SXP デバイスを選択するように要求するプロンプトが再表示されます。

ステップ 5 [ユーザー入力必須（User Input Required）] をクリックし、必要な情報をフィールドに入力します。

ステップ 6 SXP マッピングを比較するピア SXP デバイスのチェックボックスをオンにして、共通接続パラメータを入力します。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 [結果概要の表示（Show Results Summary）] をクリックして、診断および解決手順を表示します。

IP-SGT マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[TrustSec ツール（TrustSec Tools）]** > **[IP ユーザー SGT（IP User SGT）]** を選択します。

ステップ 2 必要に応じてフィールドに情報を入力します。

ステップ 3 [実行（Run）] をクリックします。

追加入力が要求されます。

ステップ 4 [ユーザー入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更します。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 [結果概要の表示（Show Results Summary）] をクリックして、診断および解決手順を表示します。

デバイス SGT ツール

TrustSec ソリューションが有効なデバイスの場合、RADIUS 認証によって各ネットワークデバイスに SGT 値が割り当てられます。デバイス SGT 診断ツールは、（提供された IP アドレスを使用して）ネットワーク デバイスに接続し、ネットワーク デバイス SGT 値を取得します。次に RADIUS 認証レコードをチェックして、割り当てられた最新の SGT 値を特定します。最後に、デバイス SGT ペアを表形式で表示して、SGT 値が同じであるかどうかを特定します。

デバイス SGT マッピングの比較による TrustSec 対応ネットワークの接続問題のトラブルシューティング

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[TrustSec ツール（Trustsec Tools）]** > **[デバイス SGT（Device SGT）]**。

ステップ 2 必要に応じてフィールドに情報を入力します。

デフォルトのポート番号は、Telnet は 23、SSH は 22 です。

ステップ 3 [実行（Run）] をクリックします。

ステップ 4 [結果概要の表示（Show Results Summary）] をクリックして、デバイス SGT 比較の結果を表示します。

その他のトラブルシューティング情報の入手

Cisco ISE を使用すると、管理者ポータルから、サポートおよびトラブルシューティング情報をダウンロードできます。サポートバンドルを使用して、Cisco Technical Assistance Center（TAC）が Cisco ISE の問題をトラブルシューティングするための診断情報を準備できます。

（注） サポート バンドルおよびデバッグ ログにより、高度なトラブルシューティング情報が TAC に提供されます。サポート バンドルおよびデバッグ ログは解釈が困難です。Cisco ISE で提供されるさまざまなレポートおよびトラブルシューティング ツールを使用して、ネットワークで直面している問題を診断およびトラブルシューティングできます。

Cisco ISE のサポート バンドル

サポートバンドルに含めるログを設定できます。たとえば、特定のサービスのログをデバッグログに含めるように設定できます。また、日付に基づいてログをフィルタリングできます。

ダウンロードできるログは、次のように分類されます。

- 完全な設定データベース：Cisco ISE 設定データベースは、可読の XML 形式です。問題をトラブルシューティングする場合、このデータベース設定を別の Cisco ISE ノードにインポートして、シナリオを再現できます。
- デバッグログ：ブートストラップ、アプリケーション設定、ランタイム、展開、公開キーインフラストラクチャ（PKI）情報、およびモニタリングとレポートがキャプチャされます。

  デバッグ ログによって、特定の Cisco ISE コンポーネントのトラブルシューティング情報が提供されます。デバッグログを有効にするには、「Logging」の第 11 章を参照してください。デバッグ ログを有効にしない場合、情報メッセージ（INFO）はすべてサポート バンドルに含まれます。詳細については、Cisco ISE デバッグ ログ （2027 ページ）を参照してください。
- ローカルログ：Cisco ISE で実行されるさまざまなプロセスの syslog メッセージが含まれています。
- コアファイル：クラッシュの原因の特定に役立つ重要な情報が含まれています。これらのログは、アプリケーションがクラッシュし、アプリケーションにヒープダンプが含まれている場合に作成されます。
- モニタリングおよびレポートログ：アラートおよびレポートに関する情報が含まれています。
- システムログ：Cisco Application Deployment Engine（ADE）関連の情報が含まれています。
- ポリシー設定：Cisco ISE で設定されたポリシーが可読形式で含まれます。

これらのログは、Cisco ISE CLI から **backup-logs** コマンドを使用してダウンロードできます。詳細については、『Cisco Identity Services Engine CLI リファレンスガイド』を参照してください。

（注） インラインポスチャノードの場合、管理者ポータルからサポートバンドルをダウンロードできません。**backup-logs** コマンドは、Cisco ISE CLI から使用する必要があります。

これらのログを管理者ポータルからダウンロードすることを選択した場合、次の操作を実行できます。

- デバッグログやシステムログなどのログタイプに基づいて、ログのサブセットのみをダウンロードします。
- 選択したログタイプの最新の n 個のファイルのみをダウンロードします。このオプションによって、サポート バンドルのサイズとダウンロードにかかる時間を制御できます。

モニタリングログによって、モニタリング、レポート、およびトラブルシューティング機能に関する情報が提供されます。ログのダウンロードの詳細については、Cisco ISE ログ ファイルのダウンロード （2026 ページ）を参照してください。

サポート バンドル

サポート バンドルは、単純な tar.gpg ファイルとしてローカル コンピュータにダウンロードできます。サポート バンドルは、日付とタイム スタンプを使用して、ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg という形式で名前が付けられます。ブラウザに、適切な場所にサポートバンドルを保存するように要求するプロンプトが表示されます。サポートバンドルの内容を抽出し、README.TXT ファイルを表示できます。このファイルには、サポートバンドルの内容と、ISE データベースがサポートバンドルに含まれている場合はその内容をインポートする方法が示されています。

Cisco ISE ログ ファイルのダウンロード

ネットワークでの問題のトラブルシューティング時に、Cisco ISE ログ ファイルをダウンロードして、詳細情報を確認できます。

インストールとアップグレードに関する問題のトラブルシューティングを行うには、ADE-OS やその他のログファイルを含む、システムログをダウンロードすることもできます。

サポートバンドルをダウンロードする際、暗号キーを手動で入力する代わりに、暗号化用の公開キーを使用することを選択できます。このオプションを選択すると、Cisco PKI はサポートバンドルの暗号化および復号化に使用されます。Cisco TAC は、公開キーと秘密キーを保持します。Cisco ISE はサポート バンドルの暗号化に公開キーを使用します。Cisco TAC は、秘密キーを使用してサポートバンドルを復号化できます。このオプションは、トラブルシューティング用に Cisco TAC にサポート バンドルを提供する場合に使用します。オンプレミスの問題をトラブルシューティングしている場合、共有キー暗号化を使用します。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者の権限が必要です。
- デバッグログとデバッグログレベルを設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[ログのダウンロード（Download Logs）]** > **[アプライアンス ノードリスト（Appliance Node List）]**。

ステップ 2 サポート バンドルをダウンロードするノードをクリックします。

ステップ 3 [サポートバンドル（Support Bundle）] タブでは、サポートバンドルに入力するパラメータを選択します。

すべてのログを含めると、サポート バンドルが大きくなりすぎて、ダウンロードに時間がかかります。ダウンロード プロセスを最適化するには、最新の *n* ファイルのみをダウンロードするように選択します。

ステップ 4 サポートバンドルを生成する [開始日（From date）] と [終了日（To date）] を入力します。

ステップ 5 次のいずれかを実行します。

- [公開キー暗号化（Public Key Encryption）]：トラブルシューティング用に Cisco TAC にサポートバンドルを提供する場合は、このオプションを選択します。
- [共有キー暗号化（Shared Key Encryption）]：オンプレミスでローカルに問題をトラブルシューティングする場合は、このオプションを選択します。このオプションを選択すると、サポート バンドル用の暗号キーを入力する必要があります。

ステップ 6 サポート バンドルの暗号キーを入力し、再入力します。

ステップ 7 [サポート バンドルの作成（Create Support Bundle）] をクリックします。

ステップ 8 [ダウンロード（Download）] をクリックして、新しく作成されたサポート バンドルをダウンロードします。

サポート バンドルは、アプリケーション ブラウザを実行しているクライアント システムにダウンロードされる tar.gpg ファイルです。

次のタスク

特定のコンポーネントのデバッグログをダウンロードします。

Cisco ISE デバッグ ログ

デバッグ ログには、さまざまな Cisco ISE コンポーネントのトラブルシューティング情報が含まれています。デバッグログには、過去30日間に生成された重大なアラームと警告アラーム、過去7日間に生成された情報アラームが含まれています。問題を報告しているときに、これらのデバッグ ログを有効にして、問題の診断と解決のためにこれらのログを送信するよう求められる場合があります。

（注） 高負荷のデバッグログ（モニタリングデバッグログなど）を有効にすると、高負荷に関するアラームが生成されます。

デバッグ ログの入手

ステップ 1 デバッグログを入手するコンポーネントを設定します。「Cisco ISE コンポーネントおよび対応するデバッグ ログ （2029 ページ）」を参照してください。

ステップ 2 デバッグ ログのダウンロード。

デバッグログの設定

各デバッグログコンポーネントに許可される最大ファイルサイズと最大ファイル数を設定できます。

（注） 通常の操作ではデフォルト設定を使用し、問題のデバッグ時にのみデバッグログファイルのサイズ、ファイル数、またはその両方を増やすことを推奨します。

ステップ 1 [操作（Operations）] > [デバッグウィザード（Debug Wizard）] > [デバッグログの設定（Debug Log Configuration）] の順に選択します。

ステップ 2 [ノードリスト（Node List）] ウィンドウで、ノードを選択し、[編集（Edit）] をクリックします。

ステップ 3 [デバッグレベルの設定（Debug Level Configuration）] ウィンドウで、設定するコンポーネントの横にあるオプションボタンをクリックします。

ステップ 4 [デバッグログの設定（Debug Log Settings）] をクリックします。

ステップ 5 [デバッグログの設定（Debug Log Settings）] ウィンドウに次の詳細を入力します。

- [最大ファイルサイズ（Max File Size）]：このコンポーネントの最大ファイルサイズを MB 単位で入力します。有効な範囲は 1 ～ 100 です。
- [ファイル数（File Count）]：そのコンポーネントで許可される最大ファイル数を指定します。

  [デバッグレベルの設定（Debug Level Configuration）] ウィンドウの [合計ディスク容量（Total Disk Space）]使用率表示バーには、現在のディスク容量の使用率と、[最大ファイルサイズ（Max File Size）] と [ファイル数（File Count）] に設定された値に基づいた容量の使用率の推定値が表示されます。

  （注） デバッグログに使用できる最大ディスク容量は 60 GB です。

- [デフォルトにリセットする日付/時刻の指定（Specify Date/Time to Reset to Default）]：（オプション）このチェックボックスをオンにして、これらの値が自動的にデフォルトに設定される日時を指定します。

[デバッグログの設定（Debug Log Configuration）] ウィンドウの [デフォルトにリセット（Reset to Default）] オプションを使用して、これらの値をデフォルトにリセットすることもできます。

（注） [最大ファイルサイズ（Max File Size）] と [ファイル数（File Count）] のデフォルト値は、選択したコンポーネントによって異なります。

ステップ 6 [保存（Save）] をクリックします。

（注） [Active Directory]、[runtime-AAA]、[runtime-config]、および [runtime-logging] コンポーネントの [最大ファイルサイズ（Max File Size）] と [ファイル数（File Count）] は更新できません。

Cisco ISE コンポーネントおよび対応するデバッグ ログ

表 *199 :* コンポーネントおよび対応するデバッグ ログ

コンポーネント	デバッグ ログ
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
License	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cellular-config	ise-psc.log
cellular-config-api	api-service.log
cellular-config-ui	ise-psc.log
cellular-mnt	collector.log
cisco-mnt	ise-psc.log
client	ise-psc.log

コンポーネント	デバッグ ログ
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
Guest Access Admin	guest.log
Guest Access	guest.log
MyDevices	guest.log
Portal	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
IPSec	ise-psc.log
ipsec-api	api-service.log
ipsec-ui	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log

コンポーネント	デバッグ ログ
profiler	profiler.log
provisioning	ise-psc.log
policy-engine	ise-psc.log
policy-engine-timelog	policy-eval-time.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log
telemetry	sch.log

機能別のデバッグウィザードの設定

デバッグウィザードには、Cisco ISE ノードの問題のトラブルシューティングに使用できるデバッグテンプレートが含まれています。デバッグプロファイルとデバッグログを設定できます。

[デバッグプロファイルの設定（Debug Profile Configuration）] ウィンドウでは、テンプレート内にある個々のコンポーネントのデバッグログのシビラティ（重大度）レベルを設定できます。

[デバッグログの設定（Debug Log Configuration）] ウィンドウでは、デバッグログのシビラティ（重大度）レベルを設定できます。デバッグログにより、ブートストラップ、アプリケーション設定、ランタイム、展開、モニタリングとレポート、および公開キーインフラストラクチャ（PKI）に関する情報が取得されます。

（注）
- ノードごとのログレベルが、デバッグウィザードのプロファイルよりも優先されます。
- 同じコンポーネントを編集する複数のプロファイルを有効にすると、トレースの優先順位が最も高いログレベルが優先されます。

ステップ 1 デバッグプロファイルを設定するには、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[デバッグウィザード（Debug Wizard）]** > **[デバッグプロファイルの設定（Debug Profile Configuration）]** を選択します。

ステップ 2 新しいプロファイルを作成するには、[追加（Add）] をクリックします。

ステップ 3 新しいプロファイルの**名前**と**説明**を入力します。

ステップ 4 プロファイルに含めるコンポーネントの横にあるチェックボックスをオンにし、各コンポーネントに対応する [ログレベル（Log Level）] を設定します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ISE ノードをただちに有効にするには、[有効化（Enable）] をクリックします。それ以外の場合は、[後で実行（Do it Later）] をクリックします。

ステップ 7 [有効化（Enable）] をクリックした場合は、プロファイルを有効にする ISE ノードの横にあるチェックボックスをオンにします。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 デバッグログを設定するには、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [デバッグウィザード（Debug Wizard）] > [デバッグログの設定（Debug Log Configuration）]** を選択します。

ステップ 10 オプションボタンをクリックしてノードを選択します。

ステップ 11 オプションボタンをクリックしてコンポーネントを選択します。

ステップ 12 [編集（Edit）] をクリックして、コンポーネントの [コンポーネント名（Component Name）]、[ログレベル（Log Level）]、[説明（Description）]、[ログファイル名（Log File Name）] を変更します。

ステップ 13 [保存（Save）] をクリックします。

デバッグ ログのダウンロード

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）] > [アプライアンスノードリスト（Appliance Node List）]**。

ステップ 2 [アプライアンスノードリスト（Appliance node list）] で、デバッグログをダウンロードするノードをクリックします。

ステップ 3 [デバッグ ログ（Debug Logs）] タブをクリックします。

デバッグ ログ タイプとデバッグ ログのリストが表示されます。このリストは、デバッグ ログの設定に基づいています。

ステップ 4 ダウンロードするログ ファイルをクリックし、クライアントブラウザを実行しているシステムに保存します。

必要に応じて、このプロセスを繰り返して他のログファイルをダウンロードできます。次に、[デバッグログ（Debug Logs）] ウィンドウからダウンロードできるその他のデバッグログを示します。

- isebootstrap.log：ブートストラップ ログ メッセージを提供します。
- monit.log：ウォッチドッグメッセージを提供します。

- pki.log：サードパーティの暗号ライブラリログを提供します。
- iseLocalStore.log：ローカルストアファイルに関するログを提供します。
- ad_agent.log：Microsoft Active Directory サードパーティ ライブラリ ログを提供します。
- catalina.log：サードパーティログを提供します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。