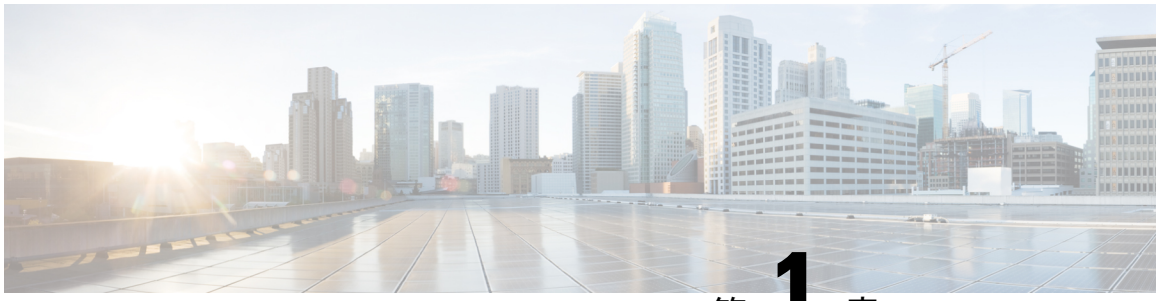
Cisco ISE リリース 2.4 管理者ガイド

初版：2019 年 6 月 13 日

最終更新：2019 年 6 月 13 日

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

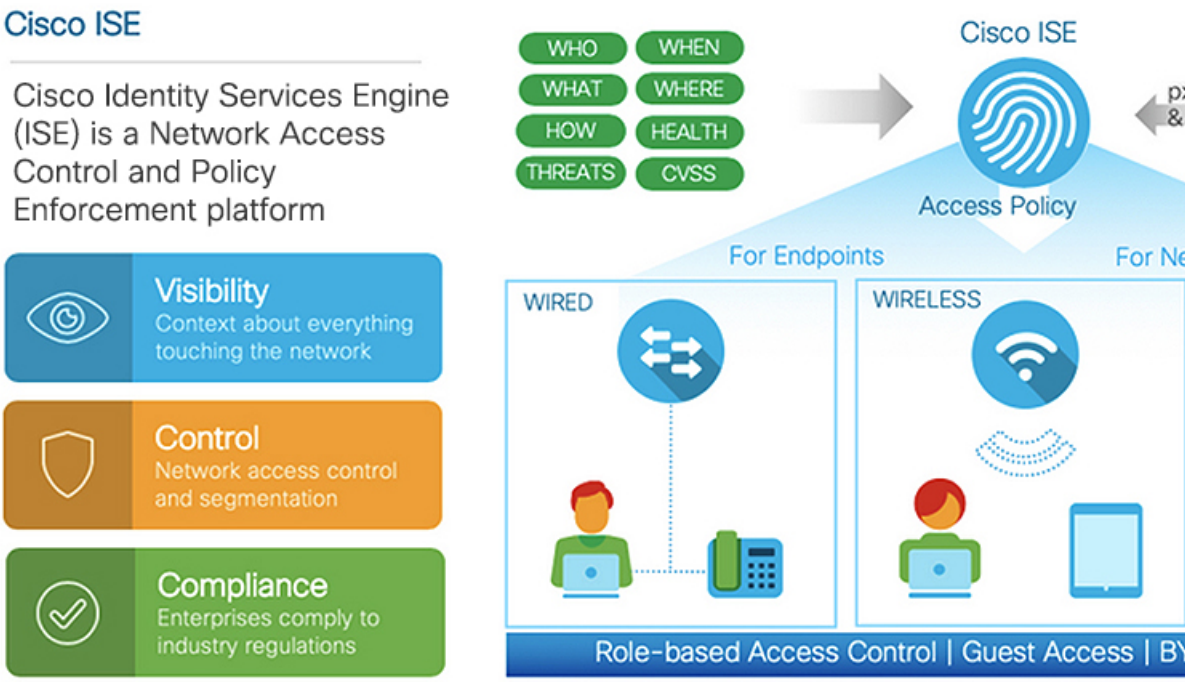
目 次



第 1 章

概要

Cisco ISE の概要



Cisco Identity Services Engine（ISE）は、アイデンティティベースのネットワーク アクセス コントロールおよびポリシー適用システムです。企業におけるエンドポイントのアクセスコント

ロールとネットワークデバイスの管理を可能にする共通のポリシーエンジンとして機能します。

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

Cisco ISE 管理者は、ユーザ/ユーザグループ（誰が）、デバイスタイプ（何を）、アクセス時間（いつ）、アクセスロケーション（どこで）、アクセスタイプ（有線、ワイヤレス、またはVPN）（どのように）、ネットワークの脅威と脆弱性といった、ネットワークのリアルタイムのコンテキストデータを収集できます。

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

Cisco ISE の機能

Cisco ISE は、次の機能を備えています。

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

これには、802.1X、RADIUS、MAB、Web ベース、EasyConnect、および外部エージェント対応の認証方式が含まれます（これらに限定されない）。

- **セグメンテーション**：Cisco ISE は、ネットワークデバイスとエンドポイントに関するコンテキストデータを使用して、ネットワークセグメンテーションを容易にします。Cisco ISE がセキュアなネットワークセグメンテーションを実現する方法には、セキュリティグループタグ、アクセスコントロールリスト、ネットワークアクセスプロトコル、ポリシーセット（認可、アクセス、認証を定義）などがあります。
- **ポスチャまたはコンプライアンス**：Cisco ISE を使用すると、エンドポイントにネットワークへの接続を許可する前に、そのエンドポイントのコンプライアンス（ポスチャとも呼ばれる）をチェックすることができます。エンドポイントがポスチャサービスに適したポスチャエージェントを確実に受け取るようにすることができます。
- **脅威の封じ込め**：Cisco ISE がエンドポイントから脅威または脆弱性の属性を検出すると、適応型ネットワーク制御ポリシーが送信され、エンドポイントのアクセスレベルが動的に変更されます。脅威または脆弱性が評価され、対処されると、エンドポイントは元のアクセスポリシーに戻されます。
- **セキュリティエコシステム統合**：pxGrid 機能により、Cisco ISE は、接続されたネットワークデバイス、サードパーティベンダー、またはシスコパートナーシステムと、コンテキスト依存情報、ポリシー、設定データなどを安全に共有できます。

Cisco ISE 管理者

管理者は、次の目的で管理者ポータルを使用できます。

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

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

セットアップ時に設定したユーザ名とパスワードは、CLI への管理アクセスにのみ使用されます。このロールは、CLI 管理ユーザ（CLI 管理者）と見なされます。デフォルトでは、CLI 管理ユーザのユーザ名は admin、パスワードはセットアップで定義したパスワードです。デフォルトのパスワードはありません。この CLI 管理ユーザはデフォルトの admin ユーザであり、このユーザアカウントは削除できません。ただし、このアカウントのパスワードを有効化、無効化、または変更するオプションなど、他の管理者によって編集できます。

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

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

管理者は、1 つ以上の管理者グループに割り当てられます。

関連トピック

Cisco ISE 管理者グループ （5 ページ）

CLI 管理者と Web ベースの管理者の権限の比較

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

新しい管理者の作成

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

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザ（Admin Users）] > [追加（Add）]** を選択します。

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

- **管理者ユーザの作成**

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

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

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

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

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

関連トピック

読み取り専用管理ポリシー （24 ページ）
内部読み取り専用管理者の作成 （549 ページ）
読み取り専用管理者のメニュー アクセスのカスタマイズ （25 ページ）
外部グループを読み取り専用管理者グループにマッピング （549 ページ）

Cisco ISE 管理者グループ

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

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

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

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

表 *1 : Cisco ISE* 管理者グループ、アクセス レベル、権限、および制約事項

管理者グループロール	アクセス レベル	権限	制約事項
カスタマイズ管理者	スポンサー、ゲスト、およびパーソナルデバイスポータルの管理。	• ゲストおよびスポンサー アクセスの設定。 • ゲスト アクセス設定の管理。 • エンドユーザ Web ポータルの管理。	• Cisco ISE のすべてのポリシー管理、ID 管理、またはシステムレベルの設定タスクを実行できません。 • レポートを表示できません。

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

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

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

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

管理者グループロール	アクセス レベル	権限	制約事項
読み取り専用管理者	ISE GUI への読み取り専用アクセス。		

管理者グループロール	アクセス レベル	権限	制約事項
		• データのフィルタリング、クエリーの実行、オプションの保存、印刷、データのエクスポートなど、ダッシュボード、レポート、およびライブログまたはセッションの機能の表示および使用。 • 自分のアカウントのパスワードの変更。 • グローバル検索、レポート、およびライブログまたはセッションを使用した ISE への照会。 • 属性に基づいたデータのフィルタリングと保存。 • 認証ポリシー、プロファイル ポリシー、ユーザ、エンドポイント、ネットワーク デバイス、ネットワーク デバイス グループ、ID（グループを含む）、およびその他の構成に関するデータのエクスポート。 • レポート クエリのカスタマイズ、保存、印刷、およびエクスポート。	• 許可ポリシー、認証ポリシー、ポスチャポリシー、プロファイラポリシー、エンドポイント、ユーザなど、オブジェクトの作成、更新、削除、インポート、検疫、およびモバイルデバイス管理（MDM）アクションなどの構成変更の実行。 • バックアップおよび復元、ノードの登録または登録解除、ノードの同期化、ノードグループの作成、編集、削除、またはパッチのアップグレードおよびインストールなどのシステム操作の実行。 • ポリシー、ネットワーク デバイス、ネットワーク デバイス グループ、ID（グループを含む）、およびその他の設定に関するデータのインポート。 • CoA、エンドポイントのデバッグ、収集フィルタの変更、ライブセッションデータの抑止のバイパス、PAN-HA フェールオーバー設定の変

管理者グループロール	アクセス レベル	権限	制約事項
		• カスタム レポート クエリの生成、結果の保存、印刷、またはエクスポート。 • 今後の参照用に UI 設定の保存。 • **[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[ログのダウンロード（Download Logs）]** ウィンドウから ise-psc-log などのログのダウンロード。	更、Cisco ISE ノードのペルソナまたはサービスの編集などの操作の実行。 • パフォーマンスに重大な影響を与える可能性のあるコマンドの実行。たとえば、**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般的なツール（General Tools）]** ウィンドウの TCP ダンプへのアクセスは制限されています。 • サポート バンドルの生成。

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

管理者グループロール	アクセス レベル	権限	制約事項
システム管理者	すべての Cisco ISE 設定およびメンテナンスのタスク。		Cisco ISE のすべてのポリシー管理またはシステムレベルの設定タスクを実行できません。

管理者グループロール	アクセス レベル	権限	制約事項
		[操作（Operations）] タブの下のすべてのアクティビティを実行するためのフルアクセス（読み取りおよび書き込み権限）、および [管理（Administration）] タブの下のいくつかのメニュー項目への部分的なアクセス。 • 管理者アカウント設定および管理者グループ設定に対する読み取り権限。 • RBAC ポリシー ウィンドウに加えて、管理者アクセスおよびデータアクセス権限に対する読み取り権限。 • **[管理（Administration）]> [システム（System）]** のすべてのオプションに対する読み取りおよび書き込み権限。 • 認証の詳細の表示。 • エンドポイント保護サービス適応型ネットワーク制御の有効化/無効化 • アラームの作成、編集、および削除、レポートの生成と表示、Cisco	

管理者グループロール	アクセス レベル	権限	制約事項
		ISE を使用したネットワーク内の問題のトラブルシューティング。 • デバイス管理：TACACS グローバルプロトコル設定を有効にする権限。	
外部 RESTful サービス（ERS）管理者	GET、POST、DELETE、PUT など、すべての ERS API 要求へのフル アクセス	• ERS API 要求の作成、読み取り、更新、および削除。	ロールは、内部ユーザ、ID グループ、エンドポイント、エンドポイントグループ、および SGT をサポートする ERS 許可のみを対象としています
外部 RESTful サービス（ERS）オペレータ	ERS API への読み取り専用アクセス、GET のみ	• ERS API 要求の読み取りのみ可能	ロールは、内部ユーザ、ID グループ、エンドポイント、エンドポイントグループ、および SGT をサポートする ERS 許可のみを対象としています。
TACACS+ Admin	フル アクセス	アクセス先： • デバイス管理ワーク センター。 • 展開（Deployment）：TACACS+ サービスを有効にします。 • 外部 ID ストア。 • **[操作（Operations）]** > **[TACACSライブログ（TACACS Live Logs）]** ウィンドウ。	—

関連トピック

Cisco ISE 管理者 （3 ページ）

管理者グループの作成

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

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]** を選択します。

ステップ 2 [追加（Add）] をクリックして名前と説明を入力します。

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

ステップ 3 設定する管理者グループのタイプを次のように指定します。

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

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

ステップ 4 [メンバーユーザ（Member Users）] エリアの [追加（Add）] をクリックして、ユーザをこの管理者グループに追加します。

ステップ 5 [送信（Submit）] をクリックします。

ユーザを管理者グループから削除するには、削除するユーザに対応するチェックボックスをオンにして、[削除（Remove）] をクリックします。

Cisco ISE への管理アクセス

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

Cisco ISE では、次のオプションによって Web インターフェイスへの管理アクセスを制御することができます。

管理アクセスの方法

Cisco ISE サーバには、いくつかの方法で接続することができます。管理者ポータルは PAN によって運用されます。ログインには管理者パスワードが必要です。CLI を実行できる SSH またはコンソールを使用すると、他の ISE ペルソナサーバにアクセスできます。ここでは、各接続タイプで利用可能なプロセスとパスワードのオプションについて説明します。

- [管理者パスワード（Admin password）]：インストール時に作成した Cisco ISE 管理者ユーザのタイムアウトは、デフォルトで 45 日間です。**[管理（Administration）]** > **[システム（System）]** > **[管理者設定（Admin Settings）]** でパスワードの有効期間をオフにすると、これを回避することができます。[パスワードポリシー（Password Policy）] タブをクリックし、[パスワードの有効期間（Password Lifetime）] で [管理パスワードの有効期限（Administrative passwords expire）] をオフにします。

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

- [CLI パスワード（CLI password）]：CLI パスワードはインストール時に指定する必要があります。無効なパスワードが原因で CLI へのログインに問題がある場合は、CLI パスワードをリセットできます。コンソールに接続し、**password** CLI コマンドを実行して、パスワードをリセットします。詳細については、「*ISE CLI* リファレンス」を参照してください。

- CLIへのSSHアクセス（SSH access to the CLI）：インストール中またはインストール後に **service sshd** コマンドを使用して、SSH アクセスを有効にすることができます。また、SSH 接続でキーを使用するように強制することもできます。この場合、すべてのネットワークデバイスとの SSH 接続でも、このキーが使用されることに注意してください。を参照してくださいSSH キーの検証 （1149 ページ）。SSH キーで Diffie-Hellman アルゴリズムの使用を強制できます。ECDSA キーは、SSH キーではサポートされないことに注意してください。

Cisco ISE でのロールベースの管理者アクセス コントロール

Cisco ISE では、管理権限を制限することでセキュリティを確保するロールベース アクセス コントロール（RBAC）ポリシーが提供されます。RBAC ポリシーは、ロールおよび権限を定義

するためにデフォルトの管理者グループに関連付けられています。標準的な権限セット（メニューおよびデータ アクセス）が、事前定義された管理者グループそれぞれとペアになっており、それによって、関連付けられたロールおよび職務機能と整合性がとられています。

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

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

（注） SuperAdmin または ReadOnlyAdmin の権限を持つシステム定義の管理者ユーザのみが、ユーザグループに含まれていない ID ベースのユーザを表示できます。これらの権限なしで作成した管理者は、それぞれのユーザを表示することはできません。

ロールベースの権限

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

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

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

RBAC ポリシー

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

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

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

デフォルトのメニュー アクセス権限

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

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

メニュー アクセス権限の設定

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [権限（Permissions）] > [メニュー アクセス（Menu Access）]** を選択します。

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

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

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

ステップ 3 [送信（Submit）] をクリックします。

データ アクセス権限を付与するための前提条件

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

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

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

デフォルトのデータ アクセス権限

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

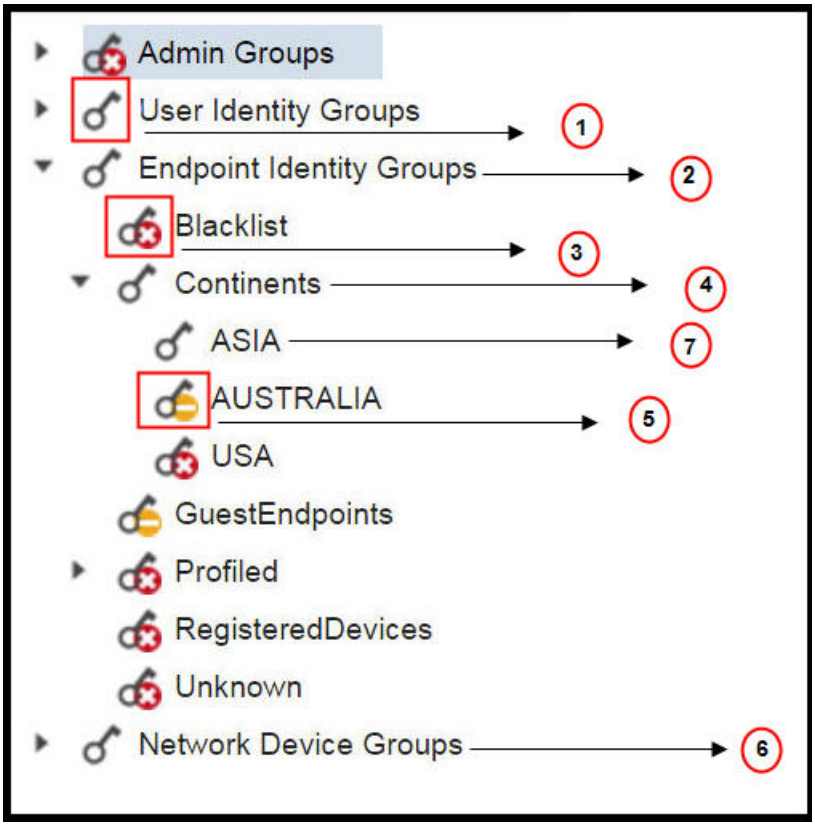
管理者グループに付与することができる、フルアクセス、アクセスなし、読み取り専用という名前の 3 つのデータアクセス権限があります。

読み取り専用権限は次の管理者グループに付与できます。

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

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

図 *1* : 以下の図に、さまざまな ***RBAC*** グループのための追加のサブメニューまたはオプションを含む *2* 番目または *3* 番目のレベルのメニューに、データアクセス権限がどのように適用されるかを示します。



ラベル	説明
1	[ユーザ ID グループ（User Identity Groups）] データ タイプのフル アクセスが示されています。
2	[エンドポイントIDグループ（Endpoint Identity Groups）] が、その子（Asia）に付与されている最大の権限（フルアクセス）を得ていることが示されています。
3	オブジェクト（Blacklist）のアクセス権限がないことが示されています。
4	親（Continents）が、その子（Asia）に付与されている最大のアクセス権限を得ていることが示されています。
5	オブジェクト（Australia）の読み取り専用アクセスが示されています。

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

データ アクセス権限の設定

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [権限（Permissions）]** を選択します。

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

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

a) 管理者グループをクリックして展開し、目的の管理者グループを選択します。

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

ステップ 4 [**保存（Save）**] をクリックします。

読み取り専用管理ポリシー

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

（注） デフォルトの読み取り専用ポリシーは、読み取り専用管理者グループに割り当てられます。読み取り専用管理者グループを使用してカスタムRBACポリシーを作成することはできません。

読み取り専用管理者のメニュー アクセスのカスタマイズ

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

ステップ 1 管理者用ポータルにネットワーク管理者としてログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authorization）] > [権限（Permissions）] > [メニュー アクセス（Menu Access）]** ページに移動します。

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

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

ステップ 5 [送信（Submit）] をクリックします。
カスタム メニュー アクセス権限は、[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authorization）] > [ポリシー（Policy）] ページに表示される、読み取り専用管理ポリシーに対応する [権限（Permissions）] ドロップダウンに表示されます。

ステップ 6 [管理（Administration）]> [システム（System）]> [管理者アクセス（Admin Access）]> [許可（Authorization）] > [RBAC]> [ポリシー（Policy）] ページに移動します。

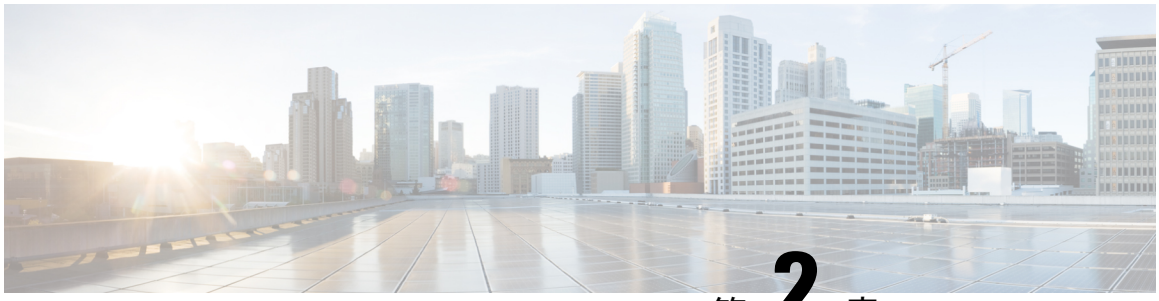
ステップ 7 **読み取り専用管理ポリシー**に対応する [権限（Permissions）] ドロップダウンをクリックします。

ステップ 8 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authorization）] > [権限（Permissions）] > [メニュー アクセス（Menu Access）]** ページで作成したデフォルト（MnT 管理者メニュー アクセス権）またはカスタム メニュー アクセス権限（MyMenu）を選択します。

ステップ 9 [保存（Save）] をクリックします。

読み取り専用管理者ポリシーにデータ アクセス権限を選択すると、エラーが発生します。

（注） 読み取り専用管理者用ポータルにログインすると、画面上部に読み取り専用のアイコンが表示され、指定したメニュー オプションのみを表示（データ アクセスなし）できます。



第 2 章

展開

Cisco ISE 展開の用語

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

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

分散 Cisco ISE 展開のペルソナ

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

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

- ハイ アベイラビリティ用のプライマリ管理ノードとセカンダリ管理ノード
- 自動フェールオーバー用の管理ノードのヘルス チェック用の非管理ノードの 1 つまたはペア
- プライマリ管理ノード（PAN）自動フェールオーバー用のヘルス チェック ノードのペアまたは単一のヘルス チェック ノード
- セッション フェールオーバー用の 1 つ以上のポリシー サービス ノード（PSN）

Cisco ISE ノードの設定

Cisco ISE ノードをインストールすると、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナによって提供されるすべてのデフォルト サービスがそのノードで実行されます。このノードはスタンドアロン状態となります。Cisco ISE ノードの管理者ポータルにログインして設定する必要があります。スタンドアロン Cisco ISE ノードのペルソナまたはサービスは編集できません。ただし、プライマリおよびセカンダリ Cisco ISE ノードのペルソナおよびサービスは編集できます。最初にプライマリ ISE ノードを設定し、その後、セカンダリ ISE ノードをプライマリ ISE ノードに登録する必要があります。

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

設定済みの Cisco ISE または本番環境では、ホスト名とドメイン名を変更しないことを推奨します。これが必要な場合は、初期展開時にアプライアンスのイメージを再作成し、変更を加え、詳細を設定します。

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

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

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

プライマリ PAN の設定

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

当初は [登録（Register）] ボタンが無効になっています。このボタンを有効にするには、プライマリ PAN を設定する必要があります。

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

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

ステップ 4 [保存（Save）] をクリックしてノード設定を保存します。

次のタスク

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

セカンダリ Cisco ISE ノードの登録

ISE ノードをプライマリ PAN に登録して、マルチノード展開を形成することができます。プライマリ PAN 以外の展開内のノードは、セカンダリ ノードと呼ばれます。ノードを登録する際に、ノード上で有効にする必要があるペルソナとサービスを選択できます。登録されたノード

は、プライマリ PANから管理することができます（たとえば、ノードのペルソナ、サービス、証明書、ライセンス、パッチの適用などの管理）。

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

始める前に

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

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

セッション サービスが有効になっているノード（ネットワーク アクセス、ゲスト、ポスチャなど）を登録する場合は、それをノード グループに追加できます。詳細についてはポリシー サービス ノード グループの作成 （87 ページ）を参照してください。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

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

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

ステップ 5 [ユーザ名（Username）] フィールドおよび [パスワード（Password）] フィールドに、セカンダリ ノードの UI ベースの管理者クレデンシャルを入力します。

ステップ 6 [Next] をクリックします。

プライマリ PAN は、登録されているノードを使用して TLS 通信を（初めて）確立しようとします。

- ノードが信頼できる証明書を使用している場合は、手順 7 に進むことができます。
- ノードが信頼されていない自己署名証明書を使用している場合は、証明書の警告メッセージが表示されます。証明書の警告メッセージには、ノード上の実際の証明書と照合できる証明書に関する詳細（発行先、発行元、シリアル番号など）が表示されます。[証明書のインポートと続行（Import Certificate and Proceed）] オプションを選択して、この証明書を信頼し、登録を続行することができます。Cisco ISE は、そのノードのデフォルトの自己署名証明書をプライマリ PAN の信頼できる証明書ストアにインポートします。デフォルトの自己署名証明書を使用しない場合は、[登録のキャンセル（Cancel

Registration）] をクリックし、そのノードの関連する証明書チェーンをプライマリ PAN の信頼できる証明書ストアに手動でインポートします。信頼できる証明書ストアにセカンダリ ノードの証明書をインポートする場合は、セカンダリ ノードの証明書を検証するように PAN の [ISE 内の認証用に信頼する（Trust for Authentication within ISE）] チェックボックスをオンにします。

- ノードが CA 署名付き証明書を使用する場合は、証明書の信頼が設定されるまで登録を続行できないというエラー メッセージが表示されます。

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

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

次のタスク

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

  参照先 Cisco ISE CA 証明書およびキーのバックアップと復元 （211 ページ）

複数の展開シナリオのサポート

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

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

Cisco ISE ノードは、1 つ以上の管理ペルソナ、モニタリング ペルソナ、およびポリシー サービス ペルソナとして展開できます。各ペルソナは、ネットワーク ポリシー管理トポロジ内の異なる部分で重要な役割を担います。Cisco ISE を管理ペルソナとしてインストールすると、集中型ポータルからネットワークを設定および管理することによって、効率と使いやすさを向上させることができます。

Cisco ISE 分散展開

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

Cisco ISE 展開の設定

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

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

分散展開内にモニタリング ノードが少なくとも 1 つ存在する必要があります。プライマリ PAN の設定時に、モニタリング ペルソナを有効にする必要があります。展開内のモニタリング ノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリング ペルソナを無効にしたりできます。

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

1 つの Cisco ISE ノードをセカンダリ ノードとして登録すると、Cisco ISE はプライマリ ノードからセカンダリ ノードへのデータ レプリケーション チャネルをすぐに作成し、複製のプロセスを開始します。複製は、プライマリ ノードからセカンダリ ノードに Cisco ISE 設定データを共有するプロセスです。複製によって、展開を構成するすべての Cisco ISE ノードの設定データの整合性を確実に維持できます。

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

れが完了すると、ノード ステータスは、セカンダリ ノードが PAN と同期されたことを示す緑に変わります。

Cisco ISE ノードの登録解除

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

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

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

（注） プライマリ PAN は登録解除できません。

分散展開を設定する場合のガイドライン

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

- ノードタイプ、ISE ノード、を選択します。管理、ポリシー サービス、およびモニタリング機能の場合は、ISE ノードを選択する必要があります。
- すべてのノードで、同じ Network Time Protocol（NTP）サーバを選択します。ノード間のタイムゾーンの問題を回避するには、各ノードのセットアップ中に同じ NTP サーバ名を指定する必要があります。この設定で、展開内にあるさまざまなノードからのレポートとログが常にタイムスタンプで同期されるようになります。
- Cisco ISE のインストール時に Cisco ISE 管理パスワードを設定します。以前の Cisco ISE 管理のデフォルトのログイン クレデンシャル（admin/cisco）は無効になっています。初期セットアップ中に作成したユーザ名とパスワードを使用するか、または後でパスワードを変更した場合はそのパスワードを使用します。
- ドメイン ネーム システム（DNS）サーバを設定します。DNS サーバに、分散展開に含まれるすべての Cisco ISE ノードの IP アドレスと完全修飾ドメイン名（FQDN）を入力します。解決できない場合は、ノード登録が失敗します。
- DNS サーバに、分散展開のすべての Cisco ISE ノードの逆引き DNS ルックアップを設定します。設定しなかった場合、Cisco ISE ノードの登録時および再起動時に、展開に関する問

題が発生することがあります。すべてのノードで逆引き DNS ルックアップが設定されていない場合、パフォーマンスが低下する可能性があります。

- （任意）プライマリ PAN からセカンダリ Cisco ISE ノードを登録解除して、Cisco ISE をアンインストールします。
- プライマリ モニタリング ノードをバックアップし、新しいセカンダリ モニタリング ノードにデータを復元します。これにより、新しい変更内容が複製されるため、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期状態となります。
- プライマリ PAN と、セカンダリ ノードとして登録しようとしているスタンドアロン ノードで、同じバージョンの Cisco ISE が実行されていることを確認します。
- 新しいノードを展開に追加する際に、ワイルドカード証明書の発行元証明書チェーンが新しいノードの信頼できる証明書に含まれていることを確認します。新しいノードが展開に追加されると、ワイルドカード証明書が新しいノードに複製されます。

プライマリ ノードおよびセカンダリ ノードで使用可能なメニュー オプション

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

1 つのノードが、ポリシー サービス ペルソナとアクティブ ロールのモニタリング ペルソナを担当するなど、複数のペルソナを担当する場合、ポリシー サービス ノードおよびアクティブ モニタリング ノードにリストされているメニュー オプションがそのノードで使用可能となります。

次の表に、さまざまなペルソナとなる Cisco ISE ノードで使用可能なメニュー オプションを示します。

表 *2 : Cisco ISE* ノードおよび使用可能なメニュー オプション

Cisco ISE ノード	使用可能なメニュー オプション
すべてのノード	• システム時刻と NTP サーバ設定の表示および設定。 • サーバ証明書のインストール、証明書署名要求の管理。すべてのサーバ証明書を一元的に管理するプライマリ PAN 経由で、展開内のすべてのノードに対し、サーバ証明書の操作を実行できます。 （注） 秘密キーは、ローカル データベースに格納されず、関連ノードからコピーされません。秘密キーは、ローカル ファイル システムに格納されます。
プライマリ PAN	すべてのメニューおよびサブメニュー。
アクティブ モニタリング ノード	• モニタリング データにアクセスします（プライマリ モニタリング ノードとアクティブ モニタリング ノードの両方から）。 （注） [操作（Operations）] メニューはプライマリ PAN からのみ表示できます。Cisco ISE 2.1 以降では、[操作（Operations）] メニューはモニタリング ノードに表示されません。
ポリシー サービス ノード	Active Directory 接続への参加、脱退、およびテストを行うオプション。各ポリシー サービス ノードが別個に Active Directory ドメインに参加している必要があります。最初にドメイン情報を定義し、PAN を Active Directory ドメインに参加させる必要があります。次に、他のポリシー サービス ノードを Active Directory ドメインに個別に参加させます。

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

展開とノードの設定

展開とノードの設定

[展開ノード（Deployment Nodes）] ページを使用すると、Cisco ISE（管理、ポリシー サービス、およびモニタリング）ノードを設定し、展開を設定することができます。

展開ノードリストウィンドウ

次の表に、展開内の Cisco ISE ノードを設定するために使用できる [展開のノードリスト（Deployment Nodes List）] ページのフィールドを示します。このページへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** です。

フィールド名	使用上のガイドライン
ホスト名（**Hostname**）	ノードのホスト名を表示します。
ノード タイプ（**Node Type**）	ノード タイプを表示します。次のいずれかを設定できます。 • Cisco ISE（管理、ポリシー サービス、およびモニタリング）ノード
ペルソナ（**Personas**）	（ノード タイプが Cisco ISE の場合にのみ表示）Cisco ISE ノードが担当してきたペルソナがリストされます。[管理（Administration）]、[ポリシー サービス（Policy Service）] などがあります。

フィールド名	使用上のガイドライン
ロール（**Role**）	このノードで管理ペルソナまたはモニタリング ペルソナが有効になっている場合、これらのペルソナが担当しているロール（プライマリ、セカンダリ、またはスタンドアロン）が示されます。ロールは、次のうちの 1 つまたは複数にできます。 • [PRI（A）] : プライマリ PAN を意味します • [SEC（A）] : セカンダリ PAN を意味します • [PRI（M）] : プライマリ モニタリング ノードを意味します • [SEC（M）] : セカンダリ モニタリング ノードを意味します
Services	（ポリシー サービス ペルソナが有効な場合にのみ表示）この Cisco ISE ノードで実行されているサービスがリストされます。サービスは次のいずれか 1 つとなります。 • セッション（Session） • プロファイリング • すべて（All）

フィールド名	使用上のガイドライン
ノード ステータス（**Node Status**）	データ レプリケーション用の展開内の各 ISE ノードのステータスを示します。 • [緑（接続）（Green（Connected））]：すでに展開に登録されている ISE ノードがプライマリ PAN と同期していることを示します。 • [赤（切断）（Red（Disconnected））]：ISE ノードに到達できないか、ISE ノードがダウンしているか、またはデータレプリケーションが行われていないことを示します。 • [オレンジ（進行中）（Orange（In Progress））]：ISE ノードがプライマリ PAN に新規に登録されているか、手動同期操作を実行したか、または ISE ノードがプライマリ PAN と同期していないことを示します。 詳細については、[ノード ステータス（Node Status）] カラムで各 ISE ノードのクイック ビュー アイコンをクリックします。

関連トピック

Cisco ISE 分散展開 （32 ページ）
Cisco ISE 展開の用語 （27 ページ）
Cisco ISE ノードの設定 （28 ページ）
セカンダリ Cisco ISE ノードの登録

ノードの一般設定

次の表で、Cisco ISE ノードの [全般設定 (General Settings)] ウィンドウのフィールドについて説明します。このウィンドウでは、ペルソナをノードに割り当て、そのサービスを実行するように設定できます。このタブのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [展開ノード（Deployment Node）] > [編集（Edit）] > [全般設定（General Settings）]** です。

*表 **3**: ノードの一般設定*

フィールド名	使用上のガイドライン
ホスト名（**Hostname**）	Cisco ISE ノードのホスト名を表示します。

フィールド名	使用上のガイドライン
FQDN	Cisco ISE ノードの完全修飾ドメイン名を表示します。たとえば、ise1.cisco.com などです。
IP アドレス	Cisco ISE ノードの IP アドレスを表示します。
ノード タイプ（Node Type）	ノード タイプを表示します。
ペルソナ（Personas）	
管理（Administration）	Cisco ISE ノードに管理ペルソナを担当させる場合は、このチェックボックスをオンにします。管理ペルソナは、管理サービスを提供するようライセンスされているノードでのみ有効にできます。 ロール（Role）：管理ペルソナが展開で担当しているロールを表示します。[スタンドアロン（Standalone）]、[プライマリ（Primary）]、[セカンダリ（Secondary）] のいずれかの値になります。 プライマリにする（Make Primary）：ノードをプライマリ Cisco ISE ノードにする場合にこのボタンをクリックします。展開では 1 つのプライマリ Cisco ISE ノードのみを使用できます。このページのその他のオプションは、ノードをプライマリにした後にのみアクティブになります。展開では 2 つの管理ノードのみを使用できます。ノードにスタンドアロン ロールが割り当てられている場合、[プライマリにする（Make Primary）] ボタンがノードの横に表示されます。ノードにセカンダリ ロールが割り当てられている場合、[プライマリに昇格（Promote to Primary）] ボタンがノードの横に表示されます。ノードにプライマリ ロールがあり、そのノードを使用して登録されている他のノードがない場合は、ノードの横に[スタンドアロンにする（Make Standalone）] ボタンが表示されます。このボタンをクリックすると、プライマリ ノードをスタンドアロン ノードにすることができます。

フィールド名	使用上のガイドライン
モニタリング	

フィールド名	使用上のガイドライン
	Cisco ISE ノードにモニタリング ペルソナを担当させ、ログ コレクタとして機能させる場合は、このチェックボックスをオンにします。分散展開内にモニタリング ノードが少なくとも 1 つ存在する必要があります。プライマリ PAN の設定時に、モニタリング ペルソナを有効にする必要があります。展開内のセカンダリ モニタリング ノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリング ペルソナを無効にしたりできます。 VMware プラットフォームで Cisco ISE ノードをログ コレクタとして設定するには、次のガイドラインに従って最低限必要なディスク領域を決定します。1 日あたりネットワーク内のエンドポイント 1 つにつき 180 KB、1 日あたりネットワーク内の Cisco ISE ノード 1 つにつき 2.5 MB となります。 モニタリング ノードに何ヵ月分のデータを格納するかに応じて、必要な最大ディスク領域を計算します。展開にモニタリング ノードが 1 つしかない場合は、スタンドアロン ロールを担当します。展開に2つのモニタリング ノードがある場合は、Cisco ISE に、プライマリ-セカンダリ ロールを設定する他のモニタリング ノードの名前が表示されます。これらのロールを設定するには、次のいずれかを選択します。 • プライマリ（Primary）：現在のノードをプライマリ モニタリング ノードにする場合。 • セカンダリ（Secondary）：現在のノードをセカンダリ モニタリング ノードにする場合。 • なし（None）：モニタリングノードにプライマリ/セカンダリ ロールを担当させない場合。 モニタリング ノードの 1 つをプライマリまたはセカンダリとして設定すると、もう一方のモニタリング ノードが自動的にそれぞれセカンダリ ノードまたはプライマリ ノードになります。プライマリ モニタリング ノードおよび

フィールド名	使用上のガイドライン
	セカンダリ モニタリング ノードは、管理ログおよびポリシー サービス ログを受信します。1 つのモニタリングノードのロールを [なし（None）]に変更した場合、他方のモニタリングノードのロールも同様に [なし（None）] になり、それによって高可用性ペアがキャンセルされます。モニタリングノードとしてノードを指定すると、そのノードが **[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]** >**[リモートロギングターゲット（Remote Logging Targets）]** ウィンドウで syslog ターゲットとして表示されます。

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

フィールド名	使用上のガイドライン
	次のサービスの 1 つまたはすべてを有効にするには、このチェックボックスをオンにします。 • [セッションサービスの有効化（Enable Session Services）] : ネットワーク アクセス サービス、ポスチャサービス、ゲスト サービス、およびクライアント プロビジョニング サービスを有効にするには、このチェックボックスをオンにします。このポリシー サービス ノードが属するグループを、[ノードをノード グループに含める（Include Node in Node Group）] ドロップダウン リストから選択します。CA サービスと EST サービスは、セッション サービスが有効になっているポリシーサービスノードでのみ実行できることに注意してください。 [ノードをノードグループに含める（Include Node in Node Group）] については、このポリシーサービスモードをどのグループにも含めない場合は [なし（None）] を選択します。 同じノード グループ内のすべてのノードが、ネットワーク アクセス デバイス（NAD）で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノード グループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロード バランサを使用していない場合、ノード グループ内のノードは、NAD で設定されている RADIUS サーバおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバとしても設定できます。 多数の ISE ノード（RADIUS サーバおよび動的許可クライアントとして）を持つ単一の NAD を設定できますが、すべてのノードが同じノード グループに属している必要はありません。

フィールド名	使用上のガイドライン
	ノード グループのメンバーは、ギガビット イーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノード グループのメンバーは L2 隣接関係である必要はありませんが、十分な帯域幅と到達可能性を確保するには L2 隣接関係が強く推奨されます。詳細については、『』の「ポリシー サービス ノード グループの作成」のセクションポリシー サービス ノード グループの作成（87 ページ）を参照してください。 • プロファイリング サービスの有効化（Enable Profiling Service）：プロファイラ サービスを有効にするには、このチェックボックスをオンにします。プロファイリング サービスを有効にする場合は、[Profiling Configuration（プロファイリング設定）] タブをクリックし、必要に応じて詳細を入力する必要があります。ポリシー サービス ノードで実行されるサービスを有効または無効にしたり、このノードを変更したりする場合は、そのサービスが実行されるアプリケーション サーバ プロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。ノードでアプリケーション サーバがいつ再起動したかを確認するには、CLI で show application status ise コマンドを使用します。 • 脅威中心型NACサービスの有効化（Enable Threat Centric NAC Service）：脅威中心型ネットワーク アクセス コントロール（TC-NAC）機能を有効にするには、このチェックボックスをオンにします。この機能では、脅威と脆弱性のアダプタから受信した脅威と脆弱性の属性に基づいて認証ポリシーを作成することができます。脅威の重大度レベルと脆弱性評価の結果は、エンドポイントまたはユーザのアクセス レベルを動的に制御するために使用できます。

フィールド名	使用上のガイドライン
	• SXPサービスの有効化（Enable SXP Service）：ノードで SXP サービスを有効にするには、このチェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。 NIC ボンディングまたはチーミングを設定している場合は、ボンディングされたインターフェイスも物理インターフェイスとともに [使用インターフェイス（Use Interface）] ドロップダウン リストに表示されます。 • デバイス管理サービスの有効化（Enable Device Admin Service）：TACACS ポリシーセット、ポリシー結果などを作成し、ネットワークデバイスの設定を制御および監査するには、このチェックボックスをオンにします。 • パッシブIDサービスの有効化（Enable Passive Identity Service）：ID マッピング機能を有効にするには、このチェックボックスをオンにします。この機能を使用すると、Cisco ISE ではなくドメイン コントローラ（DC）で認証されるユーザをモニタすることができます。Cisco ISE がユーザのネットワーク アクセスをアクティブには認証しないネットワークでは、ID マッピング機能を使用して、Active Directory（AD）ドメイン コントローラからユーザ認証情報を収集することができます。

フィールド名	使用上のガイドライン
pxGrid	pxGridペルソナを有効にするには、このチェック ボックスをオンにします。Cisco pxGridは、Cisco ISE セッション ディレクトリから Cisco Adaptive Security Appliance（ASA）などの他のポリシー ネットワーク システムへコンテキスト依存情報を共有するために使用されます。pxGrid フレームワークは、ポリシー データや設定データをノード間で交換するためにも使用できます（たとえば、ISEとサードパーティ ベンダー間でのタグやポリシー オブジェクトの共有）。また、脅威情報など、非 ISE 関連情報の交換用にも使用できます。

関連トピック

分散 Cisco ISE 展開のペルソナ （28 ページ）
管理ノード （59 ページ）
ポリシー サービス ノード （69 ページ）
モニタリング ノード （70 ページ）
pxGrid ノード （77 ページ）
プライマリおよびセカンダリの Cisco ISE ノードの同期 （86 ページ）
ポリシー サービス ノード グループの作成 （87 ページ）
ISE pxGrid ノードの展開 （80 ページ）
ノード ペルソナとサービスの変更 （86 ページ）
自動フェールオーバー用のモニタリング ノードの設定 （76 ページ）

プロファイリング ノードの設定

次の表では、プロファイラ サービスのプローブの設定に使用できる [プロファイリング設定（Profiling Configuration）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [ISE ノード（ISE Node）] > [編集（Edit）] > [プロファイリング設定（Profiling Configuration）]** です。

表 *4:* プロファイリング ノードの設定

フィールド名	使用上のガイドライン
NetFlow	ルータから送信された NetFlow パケットを受信および解析するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに NetFlow を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。 • [インターフェイス（Interface）]：ISE ノード上のインターフェイスを選択します。 • [ポート（Port）]：NetFlow エクスポートがルータから受信した NetFlow リスナー ポート番号を入力します。デフォルト ポートは 9996 です。
DHCP	IP ヘルパーから DHCP パケットをリッスンするために、ポリシーサービスペルソナを担当した Cisco ISE ノードごとに DHCP を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。 • [ポート（Port）]：DHCP サーバの UDP ポート番号を入力します。デフォルト ポートは 67 です。 • [インターフェイス（Interface）]：ISE ノード上のインターフェイスを選択します。 • [ポート（Port）]：DHCP サーバの UDP ポート番号を入力します。デフォルト ポートは 67 です。
DHCP SPAN	DHCP パケットを収集するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに DHCP SPAN を有効にする場合は、このチェックボックスをオンにします。 • [インターフェイス（Interface）]：ISE ノード上のインターフェイスを選択します。

フィールド名	使用上のガイドライン
HTTP	HTTPパケットを受信および解析するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとにHTTP を有効にする場合は、このチェックボックスをオンにします。 • [インターフェイス（Interface）] : ISE ノード上のインターフェイスを選択します。
『**RADIUS**』	IOS センサー対応デバイスから RADIUS セッション属性、さらに CDP 属性と LLDP 属性を収集するために、ポリシー サービス ペルソナを担当した ISE ノードごとに RADIUS を有効にする場合は、このチェックボックスをオンにします。
ネットワーク スキャン（**NMAP**）（**Network Scan (NMAP)**）	NMAP プローブをイネーブルにするには、このボックスをオンにします。
DNS	FQDN の DNS ルックアップを実行するために、ポリシー サービス ペルソナを担当した ISE ノードごとに DNS を有効にする場合は、このチェックボックスをオンにします。秒単位でタイムアウト時間を入力します。 （注） DNSプローブを分散展開内の特定のCisco ISE ノードで動作させるには、DHCP、DHCP SPAN、HTTP、RADIUS、SNMPのいずれかのプローブを有効にする必要があります。DNSルックアップの場合、上記のいずれかのプローブを DNS プローブとともに起動する必要があります。

フィールド名	使用上のガイドライン
SNMP クエリ（SNMP Query）	指定した間隔でネットワーク デバイスをポーリングするために、ポリシー サービス ペルソナを担当したISEノードごとにSNMPクエリーを有効にする場合は、このチェックボックスをオンにします。[再試行（Retries）]、[タイムアウト（Timeout）]、[イベント タイムアウト（Event Timeout）]、任意の [説明（Description）] の各フィールドに値を入力します。 （注） SNMPクエリープローブの設定に加えて、[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] の場所にある他のSNMP設定も行う必要があります。ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスでシスコ デバイス プロトコル（CDP）およびLink Layer Discovery Protocol（LLDP）をグローバルに有効にしていることを確認します。

フィールド名	使用上のガイドライン
SNMP トラップ（SNMP Trap）	ネットワーク デバイスから linkUp、linkDown、MAC 通知トラップを受信するために、ポリシー サービス ペルソナを担当した ISE ノードごとに SNMP トラップ プローブを有効にする場合は、このチェックボックスをオンにします。次のいずれかを選択します。 • [リンクトラップクエリ（Link Trap Query）]：SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、このチェックボックスをオンにします。 • [MAC トラップクエリ（MAC Trap Query）]：SNMP トラップを介して受信する MAC 通知を受信して解釈するには、このチェックボックスをオンにします。 • [インターフェイス（Interface）]：ISE ノードのインターフェイスを選択します。 • [ポート（Port）]：使用するホストの UDP ポートを入力します。デフォルト ポートは 162 です。
Active Directory	定義された Active Directory サーバをスキャンして、Windows ユーザに関する情報を探します。
pxGrid	ISE で pxGrid を介してエンドポイント属性を収集（プロファイリング）できるようになります。

関連トピック

Cisco ISE プロファイリング サービス （748 ページ）
プロファイリング サービスによって使用されるネットワーク プローブ （751 ページ）
Cisco ISE ノードでのプロファイリング サービスの設定 （750 ページ）

ロギングの設定

次の各ページでは、デバッグ ログの重大度の設定、外部ログ ターゲットの作成が可能です。また、Cisco ISE がこれらの外部ログ ターゲットにログ メッセージを送信できるようにできます。

リモート ロギング ターゲットの設定

次の表では、外部の場所（syslogサーバ）を作成してロギングメッセージを保存するために使用できる [リモート ロギング ターゲット（Remote Logging Targets）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** です。

表 *5:* リモート ロギング ターゲットの設定

フィールド	使用上のガイドライン
名前（Name）	新しいターゲットの名前を入力します。
ターゲット タイプ（Target Type）	ターゲット タイプを選択します。デフォルトでは、[UDP Syslog] に設定されます。
説明	新しいターゲットの簡単な説明を入力します。
[IPアドレス（IP Address）]	ログを格納する宛先マシンの IP アドレスまたはホスト名を入力します。
[ポート（Port）]	宛先マシンのポート番号を入力します。
ファシリティ コード（Facility Code）	ロギングに使用する syslog ファシリティ コードを選択します。有効なオプションは、Local0 ～ Local7 です。
最大長（Maximum Length）	リモートログターゲットメッセージの最大長を入力します。有効なオプションは200～1024バイトです。
サーバダウン時のバッファ メッセージ（Buffer Message When Server Down）	TCP syslog ターゲットおよびセキュア syslog ターゲットが使用できないときに Cisco ISE に syslog メッセージをバッファするには、このチェックボックスをオンにします。ISEは、接続が再開されるとターゲットへのメッセージの送信を再試行します。接続が再開された後、メッセージは古いものから順に送信され、バッファ内のメッセージは常に新しいメッセージの前に送信されます。バッファがいっぱいになると、古いメッセージが廃棄されます。
バッファ サイズ（MB）（Buffer Size (MB)）	各ターゲットのバッファサイズを設定します。デフォルトでは、100 MB に設定されます。バッファ サイズを変更するとバッファがクリアされ、特定のターゲットのバッファリングされた既存のすべてのメッセージが失われます。

フィールド	使用上のガイドライン
再接続タイムアウト（秒）（Reconnect Timeout (Sec)）	サーバがダウンしている場合に TCP およびセキュア syslog を廃棄する前に保持する期間を秒単位で指定します。
CA 証明書の選択（Select CA Certificate）	クライアント証明書を選択します。
サーバ証明書有効性を無視（Ignore Server Certificate validation）	ISE でサーバ証明書認証が無視されるようにして、syslog サーバを許可するには、このチェックボックスをオンにします。デフォルトでは、このオプションが無効になっているときにシステムが FIPS モードでない限り、このオプションはオフに設定されます。

関連トピック

Cisco ISE ロギング メカニズム （291 ページ）
Cisco ISE システム ログ （292 ページ）
リモート syslog メッセージの形式
Cisco ISE メッセージ カタログ （295 ページ）
収集フィルタ （298 ページ）
イベント抑制バイパス フィルタ （298 ページ）
リモート syslog 収集場所の設定 （293 ページ）
収集フィルタの設定 （298 ページ）

ロギング カテゴリの設定

次の表では、[ロギング カテゴリ（Logging Categories）]ページのフィールドについて説明します。これらのフィールドを使用して、ログの重大度レベルを設定し、選択したカテゴリのログが保存されるロギング ターゲットを選択できます。このページへのナビゲーション パスは、[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギングカテゴリ（Logging Categories）] です。

表 *6:* ロギング カテゴリの設定

フィールド	使用上のガイドライン
名前（Name）	ロギング カテゴリの名前を表示します。

フィールド	使用上のガイドライン
ログの重大度レベル（Log Severity Level）	次のオプションから、診断ロギング カテゴリの重大度レベルを選択できます。 • [重大（FATAL）]：緊急事態。 このオプションは、Cisco ISE が使用できないため、緊急措置が必要であることを意味します • [エラー（ERROR）]：このオプションは深刻な状態またはエラー状態を示します。 • [警告（WARN）]：このオプションは、通常の状態ではあるが重大な状態を示します。 これがデフォルトの条件です。 • [情報（INFO）]：このオプションは、情報メッセージを示します。 • [デバッグ（DEBUG）]：このオプションは、診断バグ メッセージを示します。
ローカル ロギング（Local Logging）	ローカル ノードで上のこのカテゴリのロギング イベントを有効にするには、このチェックボックスをオンにします。
ターゲット（Target）	左アイコンと右アイコンを使用して[使用可能（Available）]と[選択済み（Selected）]のボックス間でターゲットを移動することによって、カテゴリのターゲットを変更できます。[使用可能（Available）]ボックスには、論理（事前定義済み）と外部（ユーザ定義）という両方の既存のロギング ターゲットが含まれています。最初は空の[選択済み（Selected）]ボックスには、特定のカテゴリの選択済みターゲットが含まれます。

関連トピック

リモート syslog メッセージの形式

Cisco ISE メッセージ コード （294 ページ）
リモート syslog 収集場所の設定 （293 ページ）
メッセージ コードの重大度レベルの設定 （294 ページ）

管理者アクセスの設定

これらのページにより、管理者のアクセス設定を行うことができます。

管理者パスワード ポリシーの設定

次の表に、管理者パスワードが満たす必要のある基準を定義するために使用できる [管理者パスワードポリシー（Administrator Password Policy）] ページのフィールドを示します。このページのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理アクセス（Admin Access）]** > **[認証（Authentication）]** > **[パスワード ポリシー（Password Policy）]** です。

表 *7:* 管理者パスワード ポリシーの設定

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

フィールド	使用上のガイドライン
パスワードに使用できない文字（Password may not contain）	[管理者名またはその文字の逆順は使用できません（Admin name or its characters in reverse order）]：このチェックボックスをオンにして、管理者ユーザ名またはその文字の逆順での使用を制限します。
	[「cisco」またはその文字の逆順は使用できません（"cisco" or its characters in reverse order）]：このチェックボックスをオンにして、単語「cisco」またはその文字の逆順での使用を制限します。
	[この単語またはその文字の逆順は使用できません（This word or its characters in reverse order）]：このチェックボックスをオンにして、定義したすべての単語またはその文字の逆順での使用を制限します。
	[4 回以上連続する繰り返し文字は使用できません（Repeated characters four or more times consecutively）]：このチェックボックスをオンにして、4回以上連続する繰り返し文字の使用を制限します。

フィールド	使用上のガイドライン
	[辞書の単語、その文字の逆順、または文字の置き換えは使用できません（Dictionary words, their characters in reverse order or their letters replaced with other characters]：辞書の単語、単語の文字の逆順での使用、単語の文字の置き換えでの使用を制限します。 「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば Pa$$w0rd などです。 • [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。 デフォルトでは、このオプションが選択されています。 • [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択（Choose File）] をクリックし、カスタム辞書ファイルを選択します。このテキスト ファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。
必須の文字（Required Characters）	管理者パスワードに、次の選択肢から選択したタイプの文字が少なくとも 1 つ含まれている必要があることを指定します。 • 小文字の英文字 • 大文字の英文字 • 数字（Numeric characters） • 英数字以外の文字（Non-alphanumeric characters）

フィールド	使用上のガイドライン
パスワード履歴（Password History）	同じパスワードが繰り返し使用されるのを防ぐために、新しいパスワードと異なっている必要がある以前のパスワードの数を指定します。 また、以前のパスワードと異なる必要がある文字数を指定します。 ユーザがパスワードを再使用できない日数を入力します。
パスワードライフタイム（Password Lifetime）	次のオプションを指定して、指定した期間後にパスワードを変更するようユーザに強制します。 • パスワードが変更されなかった場合に管理者アカウントを無効にするまでの時間（日数）（Time (in days) before the administrator account is disabled if the password is not changed.）（使用可能な範囲は 0 ～ 2,147,483,647 日です）。 • 管理者アカウントが無効になるまでのリマインダ（日数）。（Reminder (in days) before the administrator account is disabled.）
ネットワーク デバイスの機密データの表示	
管理者パスワードが必要（Require Admin Password）	共有秘密やパスワードなどのネットワーク デバイスの機密データを表示するために管理者ユーザがログイン パスワードを入力するようにする場合には、このチェックボックスにマークを付けます。
パスワードのキャッシュ期間（Password cached for）	管理者ユーザによって入力されたパスワードは、この期間キャッシュされます。管理者ユーザはこの間、ネットワークデバイスの機密データを表示するためにパスワードの再入力を求められることはありません。有効な範囲は 1 ～ 60 分です。

関連トピック

Cisco ISE 管理者 （3 ページ）
新しい管理者の作成 （4 ページ）

セッション タイムアウトおよびセッション情報の設定

次の表では、セッションタイムアウトを定義し、アクティブな管理セッションを終了するために使用できる[セッション（Session）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** です。

表 *8*：セッション タイムアウトおよびセッション情報の設定

フィールド	使用上のガイドライン
セッションのタイムアウト（Session Timeout）	
セッション アイドル タイムアウト（Session Idle Timeout）	アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。
セッション情報（Session Info）	
無効化（Invalidate）	終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。

関連トピック

管理者アクセスの設定 （243 ページ）
管理者のセッション タイムアウトの設定 （247 ページ）
アクティブな管理セッションの終了 （247 ページ）

管理ノード

管理ペルソナの Cisco ISE ノードは、Cisco ISE のすべての管理操作を実行することができます。認証、許可、監査などの機能に関連したすべてのシステム関連設定を処理します。分散環境では、最大 2 つの管理ペルソナを実行するノードを実行できます。管理ペルソナは、スタンドアロン、プライマリ、またはセカンダリのロールのいずれかを担当できます。

管理ノードのハイ アベイラビリティ

ハイ アベイラビリティ構成では、プライマリ管理ノード（PAN）がアクティブな状態です。セカンダリ PAN（バックアップ PAN）はスタンバイ状態です。これは、セカンダリ PAN がプライマリ PAN からすべての設定更新を受信するものの、ISE ネットワークではアクティブではないことを意味します。

Cisco ISE は、手動および自動フェールオーバーをサポートします。自動フェールオーバーでは、プライマリ PAN がダウンした場合にセカンダリ PAN の自動プロモーションが開始されま

す。自動フェールオーバーでは、ヘルス チェック ノードと呼ばれる非管理セカンダリ ノードが必要です。ヘルス チェック ノードは、プライマリ PAN の正常性を確認します。プライマリ PAN がダウンまたは到達不能であることが検出された場合、ヘルス チェック ノードがセカンダリ PAN のプロモーションを開始して、プライマリ ロールが引き継がれます。

自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルス チェック ノードとして機能します。ヘルス チェック ノードは非管理ノードで、ポリシー サービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルス チェック ノードが必要です。

次の表に、プライマリ PAN がダウンし、セカンダリ PAN がまだ引き継がれていない場合に影響を受ける機能を示します。

機能	プライマリ PAN のダウン時に使用できるかどうか（可/不可）
既存の内部ユーザの RADIUS 認証	可
既存または新しい AD ユーザの RADIUS 認証	可
プロファイル変更がない既存のエンドポイント	可
プロファイル変更がある既存のエンドポイント	不可
プロファイリングで学習した新しいエンドポイント	不可
既存のゲスト：LWA	可
既存のゲスト：CWA	可（自動デバイス登録機能を持つホットスポット、BYOD、CWA などのデバイス登録に有効なフローを除く）
ゲストのパスワード変更	不可
ゲスト：AUP	不可
ゲスト：ログイン失敗の最大回数の適用	不可
新しいゲスト（Sponsored-Guest またはアカウント登録）	不可
ポスチャ	可
内部 CA による BYOD	不可
登録済みの既存のデバイス	可

機能	プライマリ PAN のダウン時に使用できるかどうか（可/不可）
MDM オンボーディング	不可
pxGrid サービス	不可
セカンダリ ノードの GUI にログインします	はい（ログインプロセスは、PAN へのコールのブロックが最後のログイン詳細を更新しようとしたときに遅延します。ログインは、コールタイムアウト後に 1 回進みます）

内部認証局による証明書のプロビジョニングをサポートするには、プロモーションの後に、元のプライマリ PAN のルート証明書とそのキーを新しいプライマリ ノードにインポートする必要があります。セカンダリ ノードからプライマリ PAN へのプロモーションの後に追加された PSN ノードでは、自動フェールオーバー後に証明書のプロビジョニングが機能しません。

ハイ アベイラビリティのヘルス チェック ノード

プライマリ PAN のヘルス チェック ノードをアクティブ ヘルス チェック ノードと呼びます。セカンダリ PAN のヘルス チェック ノードをパッシブ ヘルス チェック ノードと呼びます。アクティブ ヘルス チェック ノードは、プライマリ PAN のステータスを検査し、管理ノードの自動フェールオーバーを管理します。ヘルス チェック ノードとして 2 つの非管理 ISE ノードを使用することをお勧めします。1 つはプライマリ PAN、もう 1 つはセカンダリ PAN です。1 つだけヘルス チェック ノードを使用する場合、そのノードがダウンすると、自動フェールオーバーは発生しません。

両方の PAN が同じデータセンターにある場合、1 つの非管理 ISE ノードをプライマリ PAN とセカンダリ PAN の両方のヘルス チェック ノードとして使用できます。単一のヘルス チェック ノードがプライマリ PAN とセカンダリ PAN の両方の状態を検査する場合、そのノードはアクティブ/パッシブ両方の役割を担います。

ヘルス チェック ノードは非管理ノードです。つまり、ポリシー サービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。管理ノードと同じデータセンター内の PSN ノードをヘルス チェック ノードとして指定することをお勧めします。ただし、2つの管理ノードが同じ場所（LANまたはデータセンター）にない小規模または一元化された展開では、管理ペルソナを持っていないノード（PSN/pxGrid/MnT）をヘルス チェック ノードとして使用できます。

自動フェールオーバーを無効にし、プライマリ PAN の障害発生時に手動でセカンダリ ノードを昇格させることを選択した場合には、チェック ノードは不要です。

セカンダリ PAN のヘルス チェック ノード

セカンダリ PAN のヘルス チェック ノードはパッシブ モニタです。セカンダリ PAN がプライマリ PAN として昇格するまで、このノードはアクションを実行しません。セカンダリ PAN がプライマリ ロールを引き継ぐと、関連するヘルス チェック ノードは管理ノードの自動フェールオーバーを管理するアクティブ ロールを担います。以前のプライマリ PAN のヘルス チェッ

ク ノードはセカンダリ PAN のヘルス チェック ノードになり、受動的にモニタリングを行います。

ヘルス チェックの無効化と再起動

ノードがヘルス チェック ロールから削除された場合、または自動フェールオーバー設定が無効な場合、ヘルス チェック サービスはそのノードで停止します。自動フェールオーバー設定が指定されたハイアベイラビリティ ヘルス チェック ノードでイネーブルになると、ノードは管理ノードの正常性のチェックを再度開始します。ノードでハイアベイラビリティ ヘルス チェック ロールを指定または削除しても、そのノードのいずれのアプリケーションが再起動されることはありません。ヘルス チェック アクティビティのみが開始または停止します。

ハイアベイラビリティのヘルス チェック ノードを再起動すると、プライマリ PAN の以前のダウンタイムが無視され、再びヘルス ステータスのチェックが開始されます。

ヘルス チェック ノード

アクティブなヘルス チェック ノードは、設定したポーリング間隔でプライマリ PAN のヘルス ステータスをチェックします。ヘルス チェック ノードはプライマリ PAN に要求を送信し、それに対する応答が設定内容に一致する場合は、プライマリ PAN が良好な状態であると見なします。そうでなければ、ヘルス チェック ノードはプライマリ PAN が不良な状態であると見なします。プライマリ PAN の状態が設定済みフェールオーバー期間を超えて継続的に不良である場合、ヘルス チェック ノードはセカンダリ PAN へのフェールオーバーを開始します。

ヘルス チェックの任意の時点で、フェールオーバー期間中に不良と報告されたヘルス ステータスがその後で良好になったことが検出されると、ヘルス チェック ノードはプライマリ PAN のステータスを良好としてマークし、ヘルス チェック サイクルをリセットします。

プライマリ PAN ヘルス チェックからの応答は、そのヘルス チェック ノードで使用可能な設定値に照らして検証されます。応答が一致しない場合、アラームが発生します。ただし、プロモーション要求はセカンダリ PAN に行われます。

ヘルス ノードの変更

ヘルス チェックに使用している ISE ノードを変更できますが、考慮すべき点がいくつかあります。

たとえば、ヘルス チェック ノード（H1）が非同期になり、他のノード（H2）がプライマリ PAN のヘルス チェック ノードになったとします。この場合、プライマリ PAN がダウンした時点で、同じプライマリ PAN を検査している別のノード（H2）があることを N1 が認識する方法はありません。その後、H2 がダウンしたりネットワークから切断されたりした場合に、実際のフェールオーバーが必要になります。しかし、セカンダリ PAN はプロモーション要求を拒否する権限を保持します。したがって、セカンダリ PAN がプライマリ ロールに昇格すると、H2 からのプロモーション要求が拒否されてエラーが発生します。プライマリ PAN のヘルス チェック ノードは、非同期になった場合でもプライマリ PAN の状態を引き続き検査します。

セカンダリ PAN への自動フェールオーバー

プライマリ PAN が使用できなくなったときにセカンダリ PAN を自動的に昇格させるように ISE を設定できます。この設定は、**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** ページのプライマリ管理ノード（プライマリ PAN）で行うことができます。フェールオーバー時間は、「**フェールオーバーの前に障害が発生したポール数（Number of Failure Polls before Failover**）」で設定された回数と「**ポーリング間隔（Polling Interval**）」で設定された秒数をかけて得られる値として定義されます。デフォルト設定では、この時間は10分です。セカンダリ PAN からプライマリへの昇格には、さらに 10 分かかります。つまりデフォルトでは、プライマリ PAN の障害発生からセカンダリ PAN の動作開始までの時間は 20 分です。

セカンダリ PAN がフェールオーバー コールを受信すると、実際のフェールオーバーに進む前に、次の検証が行われます。

- ネットワークでプライマリ PAN が使用不能になっている。
- 有効なヘルス チェック ノードからフェールオーバー要求が受信された。
- この PAN に関するフェールオーバー要求である。

すべての検証に合格すると、セカンダリ PAN はプライマリ ロールに自身を昇格させます。

次に、セカンダリ PAN の自動フェールオーバーが試行されるシナリオのサンプルを示します（ただしこれに限定されません）。

- ポーリング期間中に、プライマリ PAN の正常性が「フェールオーバーの前に障害が発生したポール数（Number of failure polls before failover）」の値に対して一貫して良好でない。
- プライマリ PAN 上の Cisco ISE サービスが手動で停止され、フェールオーバー時間にわたって停止状態のままである。
- ソフト停止またはリブート オプションを使ってプライマリ PAN がシャットダウンされ、設定済みのフェールオーバー時間にわたってシャットダウン状態のままである。
- プライマリ PAN が突然ダウン（電源オフ）し、フェールオーバー時間にわたってダウン状態のままである。
- プライマリ PAN のネットワーク インターフェイスがダウンした（ネットワークポートが閉じた、またはネットワークサービスがダウンした）、あるいは他の理由でヘルスチェックノードから到達不能になり、設定済みのフェールオーバー時間にわたってダウン状態のままである。

ヘルス チェック ノードの再起動

再起動すると、ハイアベイラビリティのヘルスチェックノードでは、プライマリ PAN の以前のダウンタイムが無視され、再びヘルスステータスがチェックされます。

セカンダリ PAN への自動フェールオーバーの場合の個人所有デバイスの持ち込み

プライマリ PAN がダウンしている場合、プライマリ PAN ルート CA チェーンによってすでに発行された証明書が存在するエンドポイントに対して認証が中断されることはありません。これは、展開内のすべてのノードに、信頼と検証のための証明書チェーン全体が含まれているためです。

ただし、セカンダリ PAN がプライマリに昇格されるまで、新しい BYOD デバイスはオンボードされません。BYOD のオンボードには、アクティブなプライマリ PAN が必要です。

元のプライマリ PAN が復帰するか、セカンダリ PAN が昇格すると、新しい BYOD エンドポイントは問題なくオンボードされます。

障害が発生したプライマリ PAN をプライマリ PAN として再結合できない場合は、新たに昇格したプライマリ PAN（元のセカンダリ PAN）でルート CA 証明書を再生成します。

既存の証明書チェーンの場合、新しいルート CA 証明書をトリガーすると、下位 CA 証明書が自動的に生成されます。新しい下位証明書が生成された場合でも、以前のチェーンによって生成されたエンドポイント証明書は引き続き有効です。

自動フェールオーバーが回避された場合のシナリオ例

次に、ヘルス チェック ノードによる自動フェールオーバーが回避された場合、またはセカンダリ ノードへのプロモーション要求が拒否された場合を表すシナリオの例を示します。

- プロモーション要求を受信するノードがセカンダリ ノードでない。
- プロモーション要求に正しいプライマリ PAN の情報がない。
- プロモーション要求が不正なヘルス チェック ノードから受信された。
- プロモーション要求が受信されたが、プライマリ PAN が起動していて良好な状態である。
- プロモーション要求を受信するノードが同期していない。

PAN 自動フェールオーバー機能の影響を受ける機能

次の表に、PAN の自動フェールオーバーの設定が展開でイネーブルの場合にブロックされる機能、または追加の設定変更を必要とする機能を示します。

機能	影響の詳細
ブロックされる操作	

機能	影響の詳細
アップグレード	CLI によるアップグレードがブロックされます。 PAN の自動フェールオーバー機能は、Cisco ISE の以前のバージョンからリリース 1.4 にアップグレードした後の構成で使用できます。デフォルトでは、この機能は無効になっています。 自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルス チェック ノードとして機能します。ヘルス チェック ノードは非管理ノードで、ポリシー サービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルス チェック ノードが必要です。
バックアップの復元	CLI による復元およびユーザ インターフェイスがブロックされます。 PAN の自動フェールオーバーの設定が復元前にイネーブルであった場合は、正常に復元した後に再設定する必要があります。
ノード ペルソナの変更	ユーザ インターフェイスによる次のノード ペルソナの変更がブロックされます。 • 両方の管理ノード内の管理ペルソナ。 • PAN のペルソナ。 • PAN の自動フェールオーバー機能をイネーブルにした後の、ヘルス チェック ノードの登録解除。

機能	影響の詳細
その他の CLI 操作	CLIによる次の管理操作がブロックされます。 • パッチのインストールおよびロールバック • DNS サーバの変更 • eth1、eth2、およびeth3インターフェイスの IP アドレスの変更 • eth1、eth2、およびeth3インターフェイスのホスト エイリアスの変更 • タイムゾーンの変更
他の管理ポータル操作	ユーザ インターフェイスによる次の管理操作がブロックされます。 • パッチのインストールおよびロールバック • HTTPS 証明書の変更。 • 管理者認証タイプの変更（パスワードベースの認証から証明書ベースの認証へ、およびその逆）。
すでに最大数のデバイスに接続しているユーザは接続できません。	障害の発生したPANに一部のセッションデータが格納されていため、PSN によってこれを更新できません。
PAN の自動フェールオーバーをディセーブルにする必要がある操作	
CLI の操作	PAN の自動フェールオーバーの設定がイネーブルの場合、CLI による次の管理操作では警告メッセージが表示されます。サービス/システムがフェールオーバー ウィンドウ内で再起動されない場合、これらの操作によって自動フェールオーバーが起動する場合があります。そのため、以下の操作の実行時には、PAN の自動フェールオーバーの設定を無効にすることを推奨します。 • 手動による ISE サービスの停止 • 管理 CLI を使用したソフト リロード（リブート）

自動フェールオーバー用のプライマリ PAN の設定

始める前に

自動フェールオーバー機能を展開するには、少なくとも 3 つのノードが必要です。このうち 2 つのノードが管理ペルソナとなり、1 つのノードはヘルス チェック ノードとして機能します。ヘルス チェック ノードは非管理ノードで、ポリシー サービス ノード、モニタリング ノード、または pxGrid ノード、あるいはそれらの組み合わせにできます。これらの PAN が異なるデータセンターにある場合、それぞれの PAN にヘルス チェック ノードが必要です。

ステップ 1 プライマリ PAN のユーザ インターフェイスにログインします。

ステップ 2 **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** > **[PAN のフェールオーバー（PAN Failover）]** の順に選択します。

ステップ 3 プライマリ PAN の自動フェールオーバーをイネーブルにするには、[PAN の自動フェールオーバーを有効にする（Enable PAN Auto Failover）] チェックボックスをオンにします。

セカンダリ PAN をプライマリ PAN に昇格させることしかできません。ポリシー サービス ペルソナ、モニタリング ペルソナ、または pxGrid ペルソナ、あるいはそれらの組み合わせのみを担当する Cisco ISE ノードはプライマリ PAN に昇格できません。

ステップ 4 使用可能なすべてのセカンダリ ノードを含む [プライマリ ヘルス チェック ノード（Primary Health Check Node）] ドロップダウン リストから、プライマリ PAN のヘルス チェック ノードを選択します。

このノードは、プライマリ PAN と同じロケーションまたはデータセンターに置くことを推奨します。

ステップ 5 使用可能なすべてのセカンダリ ノードを含む [セカンダリ ヘルス チェック ノード（Secondary Health Check Node）] ドロップダウン リストから、セカンダリ PAN のヘルス チェック ノードを選択します。

このノードは、セカンダリ PAN と同じロケーションまたはデータセンターに置くことを推奨します。

ステップ 6 管理ノードのステータスがチェックされるまでの [ポーリング間隔（Polling Interval）] 時間を指定します。有効な範囲は 30 ～ 300 秒です。

ステップ 7 [フェールオーバーの前に障害が発生したポール数（Number of Failure Polls before Failover）] の数を指定します。

フェールオーバーは、管理ノードのステータスが障害が発生したポール数として指定された数に対して良好でない場合に発生します。有効な範囲は 2 ～ 60 です。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

セカンダリ PAN のプライマリ PAN へのプロモーション後に、次の操作を実行します。

- 手動で古いプライマリ PAN を同期して、展開内に戻します。
- 手動で同期されていない他のセカンダリ ノードを同期して、展開内に戻します。

セカンダリ PAN のプライマリへの手動昇格

プライマリ PAN が失敗し、PAN の自動フェールオーバーを設定していないした場合は、セカンダリ PAN を新しいプライマリ PAN に手動で昇格させる必要があります。

始める前に

プライマリ PAN に昇格するように管理ペルソナで設定された 2 番目の Cisco ISE ノードがあることを確認します。

ステップ 1 セカンダリ PAN のユーザ インターフェイスにログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 3 [ノードの編集（Edit Node）] ページで、[プライマリに昇格（Promote to Primary）] をクリックします。

セカンダリ PAN をプライマリ PAN に昇格させることしかできません。ポリシー サービス ペルソナまたはモニタリング ペルソナ、あるいはその両方のみを担当する Cisco ISE ノードはプライマリ PAN に昇格できません。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

元はプライマリ PAN であったノードが復帰した場合は、自動的にレベル下げされ、セカンダリ PAN になります。このノード（元のプライマリ PAN）で手動で同期を実行し、ノードを展開に戻す必要があります。

セカンダリ ノードの [ノードの編集（Edit Node）] ページでは、オプションが無効なためペルソナまたはサービスを変更できません。変更を加えるには、管理者ポータルにログインする必要があります。

プライマリ PAN にサービスを復元する

Cisco ISE は、元のプライマリ PAN への自動フォールバックをサポートしていません。セカンダリ PAN への自動フェールオーバーが開始された後、元のプライマリ PAN をネットワークに戻す場合には、それをセカンダリ PAN として設定する必要があります。

管理ノードの自動フェールオーバーのサポート

Cisco ISE は、管理ペルソナの自動フェールオーバーをサポートしています。自動フェールオーバー機能をイネーブルにするには、分散セットアップで少なくとも 2 つのノードが管理ペルソナを引き継ぎ、1 つのノードが非管理ペルソナを引き継ぐ必要があります。プライマリ管理ノード（PAN）がダウンした場合は、セカンダリ管理ノードの自動プロモーションが開始されます。この場合、非管理セカンダリ ノードが各管理ノードのヘルス チェック ノードとして指定

されます。ヘルス チェック ノードは、設定された間隔で PAN の正常性を確認します。PAN の正常性について受信されたヘルス チェック応答がダウンまたは到達不能により良好でない場合、ヘルス チェック ノードは、設定されたしきい値まで待機した後、プライマリ ロールを引き継ぐようにセカンダリ管理ノードのプロモーションを開始します。セカンダリ管理ノードの自動フェールオーバー後に使用できなくなる機能がいくつかあります。Cisco ISE は、元の PAN へのフォールバックをサポートしていません。詳細については、「管理ノードのハイ アベイラビリティ」の項を参照してください。

ポリシー サービス ノード

ポリシーサービスモード（PSN）は Cisco ISE ノードであり、ポリシーサービスペルソナを使用して、ネットワークアクセス、ポスチャ、ゲストアクセス、クライアント プロビジョニング、およびプロファイリングの各サービスを提供します。

分散セットアップでは、少なくとも 1 つのノードがポリシー サービス ペルソナを担当する必要があります。このペルソナはポリシーを評価し、すべての決定を行います。通常、1 つの分散デプロイメントに複数のポリシー サービス ノードが存在します。

同じ高速ローカル エリア ネットワーク（LAN）またはロード バランサの背後に存在するポリシー サービス ノードはすべて、グループ化してノード グループを形成することができます。ノード グループのいずれかのノードで障害が発生した場合、その他のノードは障害を検出し、URL にリダイレクトされたセッションをリセットします。

ポリシー サービス ノードのハイ アベイラビリティ

ノード障害を検出し、障害が発生したノードで URL がリダイレクトされたすべてのセッションをリセットするために、2 つ以上のポリシー サービス ノードを同じノード グループに配置できます。ノード グループに属しているノードがダウンすると、同じノード グループの別のノードが、障害が発生したノードで URL がリダイレクトされたすべてのセッションに関する許可変更（CoA）を発行します。

同じノード グループ内のすべてのノードが、ネットワーク アクセス デバイス（NAD）で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノード グループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロード バランサを使用していない場合、ノード グループ内のノードは、NAD で設定されている RADIUS サーバおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバとしても設定できます。

多数の ISE ノード（RADIUS サーバおよび動的許可クライアントとして）を持つ単一の NAD を設定できますが、すべてのノードが同じノード グループに属している必要はありません。

ノード グループのメンバーは、ギガビット イーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノード グループのメンバーは L2 隣接関係である必要はありませんが、十分な帯域幅と到達可能性を確保するには L2 隣接関係が強く推奨されます。詳細については、「ポリシー サービス ノード グループの作成 （87 ページ）」を参照してください。

PSN 間で均等に要求を分散するためのロード バランサ

展開内に複数のポリシー サービス ノードがある場合、ロード バランサを使用して要求を均等に分散できます。ロードバランサは、その背後にある機能ノードに要求を分散します。ロードバランサの背後に PSN を展開する詳細とベスト プラクティスについては、『Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP』を参照してください。

ポリシー サービス ノードでのセッション フェールオーバー

アクティブな URL にリダイレクトされたセッションがあるポリシー サービス ノードがダウンすると、エンドポイントが中間状態となります。リダイレクトエンドポイントが通信していたポリシー サービス ノードのダウンを検出した場合でも、許可を再開することはできません。

ポリシー サービス ノードがノード グループに属している場合は、ノード グループ内のノード間でハートビートメッセージが交換され、ノードの障害が検出されます。ノードに障害が発生した場合、ノードグループのピアの 1 つによって、障害が発生したノードのアクティブな URL にリダイレクトされたセッションが学習され、それらのセッションへの接続を解除するための CoA が発行されます。

その結果、同じノードグループで使用可能な別のポリシーサービス ノードによって、セッションが処理されます。セッション フェールオーバーでは、ダウンしたポリシー サービス ノードから使用可能なポリシー サービス ノードにセッションが自動的に移動しませんが、セッションを移動するための CoA が発行されます。

ポリシー サービス ノード グループ内のノード数

ノード グループに含めることができるノードの数は、展開要件によって異なります。ノード グループを使用すると、確実に、ノードの障害が検出され、許可されたがポスチャされていないセッションに関する CoA がピアによって発行されます。ノード グループのサイズはあまり大きくする必要はありません。

ノードグループのサイズが増加すると、ノード間で交換されるメッセージおよびハートビートの数が大幅に増加します。その結果、トラフィックも増加します。ノードグループ内のノードの数を少なくすることで、トラフィックを削減でき、同時にポリシー サービス ノードの障害を検出するのに十分な冗長性が提供されます。

ノード グループ クラスタに含めることができるポリシー サービス ノードの数にはハード制限はありません。

モニタリング ノード

モニタリング ペルソナの機能を持つ Cisco ISE ノードがログ コレクタとして動作し、ネットワーク内のすべての管理およびポリシーサービス ノードからのログメッセージを保存します。このペルソナは、ネットワークとリソースを効果的に管理するために使用できる高度な監視お

よびトラブルシューティング ツールを提供します。このペルソナのノードは、収集するデータを集約して関連付けて、意味のある情報をレポートの形で提供します。

Cisco ISE では、プライマリ ロールまたはセカンダリ ロールを担うことができるこのペルソナを持つノードを最大 2 つ使用してハイ アベイラビリティを実現できます。プライマリ モニタリング ノードおよびセカンダリ モニタリング ノードの両方で、ログ メッセージを収集します。プライマリ モニタリング ノードがダウンした場合、プライマリ PAN はモニタリング データを収集するセカンダリ ノードを指定します。ただし、セカンダリ ノードがプライマリに自動的に昇格されることはありません。このためには、MnT ロールの手動変更必要があります。

分散セットアップでは、少なくとも 1 つのノードが監視ペルソナを担当する必要があります。同じ Cisco ISE ノードで、モニタリング ペルソナとポリシー サービス ペルソナを有効にしないことを推奨します。最適なパフォーマンスを実現するために、ノードをモニタリング専用とすることを推奨します。

展開内の PANから [モニタリング（Monitoring）] メニューにアクセスできます。

MnT ロールの手動変更

プライマリ PAN から MnT ロールを手動で変更できます（プライマリからセカンダリとセカンダリからプライマリの両方）。

ステップ 1 プライマリ PAN のユーザ インターフェイスにログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 3 ロールを変更する MnT ノードをノード リストから選択します。

ステップ 4 [編集（Edit）] をクリックします。

ステップ 5 [モニタリング（Monitoring）] セクションで、[プライマリ/セカンダリ（Primary/ Secondary）] にロールを変更します。

ステップ 6 [保存（Save）] をクリックします。

（注） そのノードで有効になっている他のすべてのペルソナおよびサービスを無効にする場合は、[専用MnT（Dedicated MnT）]オプションを有効にします。このオプションを有効にすると、設定データ レプリケーション プロセスがそのノードで停止します。これにより、モニタリング ノードのパフォーマンスが向上します。このオプションを無効にすると、手動同期がトリガーされます。

モニタリング ノードでの自動フェールオーバー

モニタリング ノードはハイ アベイラビリティを提供しませんが、アクティブ スタンバイを提供します。ポリシー サービス ノード（PSN）は、プライマリ モニタリング ノードとセカンダリ モニタリング ノードの両方に操作監査データをコピーします。

自動フェールオーバー プロセス

プライマリ モニタリング ノードがダウンした場合は、セカンダリ モニタリング ノードがすべてのモニタリング情報およびトラブルシューティング情報を引き継ぎます。

セカンダリ モニタリング ノードをプライマリ ノードに手動で変換するために、MnT ロールの手動変更。セカンダリ ノードが昇格された後にプライマリ ノードが復旧した場合、プライマリ ノードはセカンダリ ロールを担当します。セカンダリ ノードが昇格されなかった場合、プライマリ モニタリング ノードは、復旧後にプライマリ ロールを再開します。

注意 プライマリ ノードがフェールオーバー後に復旧すると、セカンダリのバックアップを取得してデータを復元し、プライマリ ノードを最新の状態にします。

モニタリング ノードのアクティブ/スタンバイ ペアを設定するためのガイドライン

ISE ネットワークでは 2 つのモニタリング ノードを指定して、アクティブ/スタンバイ ペアを設定できます。プライマリ モニタリング ノードをバックアップし、新しいセカンダリ モニタリング ノードにデータを復元することを推奨します。これにより、プライマリが新しいデータを複製するため、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期されます。アクティブ/スタンバイ ペアには、次のルールが適用されます。

- すべての変更は、プライマリ モニタリング ノードに記録されます。セカンダリ ノードは読み取り専用です。
- プライマリ ノードで行った変更は、セカンダリ ノードに自動的に複製されます。
- プライマリ ノードとセカンダリ ノードは両方とも、他のノードがログを送信するログ コレクタとしてリストされます。
- Cisco ISE ダッシュボードは、モニタリングおよびトラブルシューティングの主要なエントリ ポイントとなります。PAN からのモニタリング情報は、ダッシュボードに表示されます。プライマリ ノードがダウンした場合、セカンダリ ノードでモニタリング情報が利用できます。
- モニタリング データのバックアップおよび消去は、標準 Cisco ISE ノードのバックアップ プロセスでは行われません。プライマリ モニタリング ノードとセカンダリ モニタリング ノードの両方でバックアップとデータ消去用のリポジトリを設定し、それぞれに同じリポジトリを使用する必要があります。

モニタリング ノードのフェールオーバー シナリオ

次のシナリオは、モニタリング ノード数に応じてアクティブ/スタンバイまたは単一ノード構成に適用されます。

- モニタリング ノードのアクティブ/スタンバイ構成では、プライマリ管理ノード（PAN）は、常にプライマリ モニタリング ノードに接続してモニタリング データを収集します。プライマリ モニタリング ノードに障害が発生した後に、PAN はスタンバイ モニタリング スタンバイ ノードに接続します。プライマリ モニタリング ノードからスタンバイ モニタ

リング ノードへのフェールオーバーは、プライマリ モニタリング ノードのダウンから 5 分以上経過した後に行われます。

ただし、プライマリ ノードに障害が発生した後、スタンバイ ノードはプライマリ ノードになりません。プライマリ ノードが復旧すると、管理ノードは再開されたプライマリ ノードからのモニタリング データの収集を再び開始します。

- プライマリ モニタリング ノードがダウンしたときに、スタンバイ モニタリング ノードをアクティブ ステータスに昇格する場合は、MnT ロールの手動変更、既存のプライマリ モニタリング ノードを登録解除して、スタンバイ モニタリング ノードをプライマリに昇格することができます。既存のプライマリ モニタリング ノードを登録解除すると、スタンバイ ノードがプライマリ モニタリング ノードになり、PAN は新しく昇格されたプライマリ ノードに自動的に接続します。
- アクティブ/スタンバイ ペアで、セカンダリ モニタリング ノードを登録解除するか、またはセカンダリ モニタリング ノードがダウンした場合、既存のプライマリ モニタリング ノードが現在のプライマリ ノードのままになります。
- ISE 展開内にモニタリング ノードが 1 つだけ存在する場合、そのノードはプライマリ モニタリング ノードとして機能し、PAN にモニタリング データを提供します。ただし、新しいモニタリング ノードを登録して展開内でプライマリ ノードにすると、既存のプライマリ モニタリング ノードは自動的にスタンバイ ノードになります。PAN は、新しく登録されたプライマリ モニタリング ノードに接続し、モニタリング データを収集します。

モニタリング データベース

モニタリング機能によって利用されるデータ レートおよびデータ量には、これらの目的専用のノード上に別のデータベースが必要です。

ポリシー サービスと同様に、モニタリングには専用のデータベースがあり、この項で説明するトピックのようなメンテナンス タスクを実行する必要があります。

モニタリング データベースのバックアップと復元

モニタリングデータベースは、大量のデータを処理します。時間が経つにつれ、モニタリング ノードのパフォーマンスと効率は、そのデータをどう管理するかによって変わってきます。効率を高めるために、データを定期的にバックアップして、それをリモートのリポジトリに転送することを推奨します。このタスクは、自動バックアップをスケジュールすることによって自動化できます。

（注） 消去操作の実行中には、バックアップを実行しないでください。消去操作の実行中にバックアップが開始されると、消去操作が停止または失敗します。

セカンダリ モニタリング ノードを登録する場合は、最初にプライマリ モニタリング ノードをバックアップしてから、新しいセカンダリ モニタリング ノードにデータを復元することを推奨します。これにより、新しい変更内容が複製されるため、プライマリ モニタリング ノードの履歴が新しいセカンダリ ノードと同期状態となります。

モニタリング データベースの消去

消去プロセスでは、消去時にデータを保持する月数を指定することで、モニタリング データベースのサイズを管理できます。デフォルトは3ヵ月間です。この値は、消去用のディスク領域使用率しきい値（ディスク領域のパーセンテージ）に達したときに使用されます。このオプションでは、各月は 30 日で構成されます。デフォルトの 3 ヵ月は 90 日間です。

モニタリング データベースの消去に関するガイドライン

次に、モニタリングデータベースのディスク使用に関連して従うべきガイドラインをいくつか示します。

- モニタリング データベースのディスク使用量がしきい値設定の 80% を超えた場合、データベース サイズが割り当てられたディスク サイズを超過したことを示すクリティカル アラームが生成されます。ディスク使用量が 90% より大きい場合は、別のアラームが生成されます。

  消去プロセスが実行され、ステータス履歴レポートが作成されます。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [展開ステータス（Deployment Status）] > [データ消去の監査（Data Purging Audit）]** を選択して表示できます。消去の完了時に情報（INFO）アラームが生成されます。

- 消去は、データベースの使用済みディスク領域のパーセンテージにも基づきます。モニタリング データベースの使用済みディスク領域がしきい値（デフォルトは 80%）以上になると、消去プロセスが開始されます。このプロセスは、管理者ポータルの設定に関係なく、過去 7 日間のモニタリング データのみを削除します。ディスク領域が 80% 未満になるまで繰り返しプロセスを続行します。消去では、処理の前にモニタリングデータベースのディスク領域制限が常にチェックされます。

運用データの消去

ISE MnT 運用（OPS）データベースには、ISE レポートに生成される情報が含まれています。最近の ISE リリースでは、ISE admin CLI コマンド **application configure ise** を実行した後に、[M&T運用データを消去（Purge M&T Operational Data）] と [M&Tデータベースをリセット（Reset M&T Database）] のオプションを使用します。

パージオプションは、データのクリーンアップに使用します。また、保持する日数を尋ねるプロンプトを表示します。リセットオプションを使用すると、データベースが工場出荷時の初期状態にリセットされるため、バックアップされているすべてのデータが完全に削除されます。ファイルがファイルシステム領域を過度に消費している場合、データベースをリセットすることができます。

（注） リセットオプションを使用すると、再起動するまで、ISEサービスが一時的に利用できなくなります。

[運用データの消去（Operational Data Purging）] ページ（[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [運用データの消去（Operational Data Purging）]）には、[データベースの使用状況（Database Utilization）] 領域と [データを今すぐ消去（Purge Data Now）] 領域があります。[データベースの使用状況（Database Utilization）] 領域には、使用可能なデータベース容量の合計と、保存されている RADIUS および TACACS データが表示されます。ステータスバーをマウスオーバーすると、利用可能なディスク容量と、データベースに既存データが保存されている日数が表示されます。RADIUS データと TACACS データを保持できる期間を [データ保存期間（Data Retention Period）] 領域に指定できます。データは毎朝午前4時に消去されます。また、保存日数を指定して、消去前にデータをリポジトリにエクスポートするように設定できます。[リポジトリのエクスポートを有効にする（Enable Export Repository）] チェックボックスをオンにして、リポジトリを選択して作成し、暗号キーを指定できます。

[データを今すぐ消去（Purge Data Now）] 領域では、すべての RADIUS および TACACS データを消去するか、またはデータ消去までに保存できる日数を指定できます。

（注） 消去前にリポジトリにエクスポートできるテーブルは、RADIUS 認証およびアカウンティング、TACACS 認証およびアカウンティング、RADIUS エラー、および設定が誤っているサプリカントの各テーブルです。

関連トピック

古い運用データの消去 （75 ページ）

古い運用データの消去

運用データはサーバに一定期間集められています。すぐに削除することも、定期的に削除することもできます。データ消去の監査レポートを表示して、データ消去が成功したかどうかを確認できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [運用データの消去（Operational Data Purging）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [データ保持期間（Data Retention Period ）] 領域で次の操作を行います。

1. RADIUS または TACACS データを保持する期間を日単位で指定します。指定した期間より前のデータはすべてリポジトリにエクスポートされます。
2. [リポジトリ（Repository）] 領域で、[リポジトリのエクスポートを有効にする（Enable Export Repository）] チェックボックスをオンにし、データを保存するリポジトリを選択します。詳細については、「リポジトリの作成」の項を参照してください。
3. [暗号キー（Encryption Key）] テキスト ボックスに必要なパスワードを入力します。
4. [保存（Save）] をクリックします。

（注） 設定した保持期間が診断データに対応する既存の保持しきい値未満の場合、設定値は既存のしきい値を上書きします。たとえば、保持期間を 3 日に設定し、この値が診断テーブルの既存のしきい値（たとえば、5 日のデフォルト）未満の場合、データはこのページで設定した値（3 日）に従って消去されます。

- [データを今すぐ消去（Purge Data Now）] 領域で、次の操作を行います。

1. すべてのデータを消去するか、または指定された日数よりも古いデータを消去します。データはリポジトリに保存されません。
2. [消去（Purge）] をクリックします。

自動フェールオーバー用のモニタリング ノードの設定

展開に 2 つのモニタリング ISE ノードがある場合は、自動フェールオーバーのプライマリ-セカンダリ ペアを設定して、Cisco ISE モニタリング サービスのダウンタイムを回避します。プライマリ-セカンダリ ペアによって、プライマリ ノードに障害が発生した場合に、セカンダリ モニタリング ノードが自動的にモニタリングを提供します。

始める前に

- 自動フェールオーバー用のモニタリング ノードを設定するには、モニタリング ノードが Cisco ISE ノードとして登録されている必要があります。
- 両方のノードでモニタリング ロールおよびサービスを設定し、必要に応じてこれらのノードにプライマリ ロールおよびセカンダリ ロールの名前を付けます。
- プライマリ モニタリング ノードとセカンダリ モニタリング ノードの両方でバックアップとデータ消去用のリポジトリを設定します。バックアップおよび消去を正しく動作させるには、両方のノードに同じリポジトリを使用します。消去は、冗長ペアのプライマリ ノードおよびセカンダリ ノードの両方で行われます。たとえば、プライマリ モニタリング ノードでバックアップおよび消去用に 2 つのリポジトリが使用されている場合、同じリポジトリをセカンダリ ノードに指定する必要があります。

システム CLI の **repository** コマンドを使用してモニタリング ノードのデータ リポジトリを設定します。

注意 スケジュールバックアップと消去をモニタリング冗長ペアのノードで正しく動作させるには、CLI を使用して、プライマリ ノードとセカンダリ ノードの両方で同じリポジトリを設定します。リポジトリは、2 つのノードの間で自動的に同期されません。

Cisco ISE ダッシュボードで、モニタリング ノードの準備ができていることを確認します。[システム概要（System Summary）] ダッシュレットに、サービスが準備完了の場合は左側に緑色のチェック マークが付いたモニタリング ノードが表示されます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 [展開ノード（Deployment Nodes）] ページで、アクティブとして指定するモニタリング ノードの隣にあるチェックボックスをオンにし、**Edit** をクリックします。

ステップ 3 [全般設定（General Settings）] タブをクリックし、[ロール（Role）] ドロップダウン リストから [プライマリ（Primary）] を選択します。

1 つのモニタリング ノードをプライマリとして選択すると、もう 1 つのモニタリング ノードが自動的にセカンダリとなります。スタンドアロン展開の場合、プライマリおよびセカンダリのロール設定は無効になります。

ステップ 4 **Save** をクリックします。アクティブ ノードおよびスタンバイ ノードが再起動します。

pxGrid ノード

Cisco pxGrid を使用すると、Cisco ISE セッション ディレクトリからの状況依存情報を、ISE エコ システムのパートナー システムなどの他のネットワーク システムや他のシスコ プラットフォームと共有できます。また、pxGrid フレームワークは、Cisco ISE とサード パーティのベンダー間でのタグおよびポリシー オブジェクトの共有のように、ノード間でのポリシーおよび設定データの交換に使用でき、その他の情報交換にも使用できます。また、pxGrid では、サードパーティ システムが適応型ネットワーク制御アクション（EPS）を起動して、ネットワーク イベントまたはセキュリティ イベントに応答してユーザ/デバイスを隔離できます。タグ定義、値、および説明のような TrustSec 情報は、TrustSec トピックを通して Cisco ISE から別のネットワークに渡すことができます。完全修飾名（FQN）を持つエンドポイント プロファイルは、エンドポイント プロファイル メタ トピックを通して Cisco ISE から他のネットワークに渡すことができます。Cisco pxGrid は、タグおよびエンドポイント プロファイルの一括ダウンロードもサポートしています。

pxGrid経由でSXPバインディング（IP-SGTマッピング）を発行および受信登録できます。SXPバインディングの詳細については、セキュリティ グループ タグの交換プロトコル （1157ページ）を参照してください。

ハイ アベイラビリティ設定で、Cisco pxGrid サーバは、PAN を通してノード間で情報を複製します。PAN がダウンすると、pxGrid サーバは、クライアントの登録およびサブスクリプション処理を停止します。pxGrid サーバの PAN をアクティブにするには、手動で昇格する必要があります。[pxGrid サービス（pxGrid Services）] ページ（[管理（Administration）] > [pxGrid サービス（pxGrid Services）]）を調べ、pxGrid ノードが現在アクティブであるか、スタンバイ状態であるかを確認できます。

XMPP（Extensible Messaging and Presence Protocol）クライアントの場合、pxGrid ノードはアクティブ/スタンバイの高可用性モードで動作します。つまり、pxGridサービスはアクティブ ノード上では「実行中」状態で、スタンバイ ノードでは「無効」状態です。

セカンダリ pxGrid ノードへの自動フェールオーバーが開始された後、元のプライマリ pxGrid ノードがネットワークに戻された場合、元のプライマリ pxGrid ノードは引き続きセカンダリ ロールを持ち、現在のプライマリ ノードがダウンしない限り、プライマリ ロールに昇格されません。

（注） 時々、元のプライマリ pxGrid ノードがプライマリ ロールに自動的に昇格されることがあります。

ハイ アベイラビリティ展開では、プライマリ pxGrid ノードがダウンすると、セカンダリ pxGrid ノードに切り替えるのに約 3 ～ 5 分かかることがあります。プライマリ pxGrid ノードに障害が発生した場合は、キャッシュ データを消去する前に、クライアントはスイッチオーバーが完了するまで待機することを推奨します。

pxGrid ノードでは、次のログを使用できます。

- pxgrid.log：状態変更通知。
- pxgrid-cm.log：パブリッシャ/サブスクライバおよびクライアントとサーバ間のデータ交換アクティビティの更新。
- pxgrid-controller.log：クライアント機能、グループ、およびクライアント許可の詳細を表示します。
- pxgrid-jabberd.log：システムの状態と認証に関連するすべてのログ。
- pxgrid-pubsub.log：パブリッシャとサブスクライバのイベントに関する情報。

（注） ノードで pxGrid サービスが無効になっている場合、ポート 5222 はダウンしますが、（Web クライアントで使用される）ポート 8910 は機能し、引き続き要求に応答します。

（注） Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。また、 のアップグレード ライセンスを最近インストールしている場合には、Base インストールで特定の拡張 pxGrid サービスが使用可能である可能性があります。

（注） パッシブ ID ワーク センターを使用するには pxGrid を定義する必要があります。詳細については、 PassiveID ワークセンター （637 ページ）を参照してください。

pxGrid クライアントおよび機能の管理

Cisco ISE に接続するクライアントは、pxGrid サービスを使用する前に、アカウントを登録し、承認を受ける必要があります。pxGrid クライアントは、クライアントになるために pxGrid SDK を介してシスコから利用可能な pxGrid クライアントライブラリを使用します。Cisco ISE は、自動および手動承認の両方をサポートします。クライアントは、一意の名前と証明書ベースの相互認証を使用して pxGrid にログインできます。スイッチの AAA 設定と同様に、クライアントは設定された pxGrid サーバのホスト名または IP アドレスに接続できます。

pxGrid の「機能」は、クライアントの pxGrid 上の情報トピックまたはチャネルであり、これらは公開および登録されます。Cisco ISE では、ID、適応型ネットワーク制御、SGA などの機能のみがサポートされます。クライアントが新しい機能を作成すると、その機能は **[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [機能別に表示（View by Capabilities）]** に表示されます。機能は個別に有効または無効にできます。機能情報は、発行、ダイレクト クエリー、または一括ダウンロード クエリーでパブリッシャから入手してください。

（注） pxGrid セッション グループが EPS グループの一部であるため、EPS ユーザ グループに割り当てられたユーザはセッション グループで操作を実行できます。ユーザが EPS グループに割り当てられると、ユーザは pxGrid クライアントのセッションのグループに加入できます。

関連トピック

pxGrid 証明書の生成 （82 ページ）

pxGrid クライアントの有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。

- パッシブ ID サービスを有効にします。**[管理（Administration）]** > **[展開（Deployment）]** を選択し、必要なノードにチェックマークを付け、[編集（Edit）] をクリックします。設定画面で [パッシブ ID サービスを有効にする（Enable Passive Identity Service）] をオンにします。

ステップ 1 **[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** を選択します。
ステップ 2 クライアントの隣にあるチェックボックスをオンにして [承認（Approve）] をクリックします。
ステップ 3 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

pxGrid 機能の有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- pxGrid クライアントをイネーブルにします。

ステップ 1 **[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** を選択します。
ステップ 2 右上の [機能別に表示（View by Capabilities）] をクリックします。
ステップ 3 有効にする機能を選択し、[有効（Enable）] をクリックします。
ステップ 4 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

ISE pxGrid ノードの展開

スタンドアロン ノードと分散展開ノードの両方で、Cisco pxGrid ペルソナを有効にできます。

始める前に

- Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。
- Cisco pxGrid サービスは、Cisco ISE SNS 3415/3495 アプライアンス上または VMware で実行されます。
- すべてのノードは、pxGrid 用に CA 証明書を使用するように設定されています。アップグレード前にデフォルトの証明書を pxGrid に使用する場合、アップグレード後にこの証明書は内部 CA 証明書に置き換えられます。
- 分散展開を使用しているか、または Cisco ISE 1.2 からアップグレードする場合は、証明書で [pxGrid 使用（pxGrid Usage）] オプションを有効にする必要があります。[pxGrid 使用（pxGrid Usage）] オプションを有効にするには、**[管理（Administration）]** > **[証明書（Certificates）]** > **[システム証明書（Certificates）]** に移動します。展開に使用される証明

書を選択し、[編集（Edit）] をクリックします。pxGrid を確認します。[pxGrid コントローラ（pxGrid Controller）] チェックボックスの証明書を使用します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 [展開ノード（Deployment Nodes）] ページで、pxGrid サービスを有効にするノードの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 [全般設定（General Settings）] タブをクリックし、[pxGrid] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

以前のバージョンからアップグレードするとき、[保存（Save）] オプションが無効になる場合があります。このことは、ブラウザ キャッシュが旧バージョンの Cisco ISE の古いファイルを参照する場合に発生します。[保存（Save）] オプションを有効にするには、ブラウザ キャッシュを消去します。

Cisco pxGrid ライブ ログ

[ライブ ログ（Live Logs）] ページには、すべての pxGrid 管理イベントが表示されます。イベント情報には、クライアント名と機能名、およびイベント タイプとタイムスタンプが含まれています。

[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [ライブ ログ（Live Log）] の順に移動して、イベント リストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

pxGrid の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）] を選択します。

ステップ 2 必要に応じて、次のオプションを選択します。

- 新しいアカウントの自動承認（Automatically Approve New Accounts）：このチェック ボックスにマークを付けると、新しい pxGrid クライアントからの接続要求が自動的に承認されます。
- パスワード ベースのアカウント作成の許可（Allow Password Based Account Creation）：このチェックボックスにマークを付けると、pxGrid クライアントのユーザ名/パスワードベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

  pxGrid クライアントは、REST API を介してユーザ名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

ステップ 3 [保存（Save）] をクリックします。

[pxGrid の設定（pxGrid Settings ）] ページで [テスト（Test）] オプションを使用して、pxGrid ノードでヘルス チェックを実行します。pxgrid/pxgrid-test.log ファイルで詳細を確認できます。

pxGrid 証明書の生成

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- pxGrid 証明書はプライマリ PAN から生成する必要があります。
- PxGrid 証明書がサブジェクト代替名（SAN）の拡張を使用する場合、DNS 名のエントリとしてサブジェクト ID の FQDN が含まれるようにします。

ステップ 1 [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）] の順に選択します。

ステップ 2 [処理の選択（I want to）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- 単一の証明書の生成（証明書署名要求なし）（Generate a single certificate without a certificate signing request）：このオプションを選択すると、コモン ネーム（CN）を入力する必要があります。
- 単一の証明書の生成（証明書署名要求あり）（Generate a single certificate with a certificate signing request）：このオプションを選択すると、証明書署名要求の詳細を入力する必要があります。
- 一括証明書の生成（Generate bulk certificates）：必要な詳細を含む CSV ファイルをアップロードすることができます。
- ルート証明書チェーンのダウンロード（Download root certificate chain）：ルート証明書をダウンロードして、信頼できる証明書ストアに追加できます。ホスト名と証明書のダウンロード形式を指定する必要があります。

[証明書テンプレート（Certificate Templates）] リンクから証明書テンプレートをダウンロードし、必要に応じて、テンプレートを編集できます。

ステップ 3 （[単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）] オプションを選択した場合は必須）pxGrid クライアントの FQDN を入力します。

ステップ 4 （オプション）この証明書の説明を入力できます。

ステップ 5 サブジェクト代替名（SAN）を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- IP アドレス（IP address）：この証明書に関連付ける pxGrid クライアントの IP アドレスを入力します。
- FQDN：pxGrid の完全修飾ドメイン名を入力します。

（注） このフィールドは、[一括証明書の生成（Generate bulk certificates）] オプションを選択している場合には表示されません。

ステップ 6 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- Private Enhanced Electronic Mail（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY----」タグで終わります。
- PKCS12 形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル）：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンドエンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成（Create）] をクリックします。

作成した証明書は、ISE の **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [発行された証明書（Issued Certificates）]** に表示され、ブラウザのダウンロード ディレクトリにダウンロードされます。

pxGrid クライアントの権限の制御

pxGrid クライアントの権限を制御するために、pxGrid 許可ルールを作成できます。これらのルールを使用して、pxGrid クライアントに提供されるサービスを制御します。

さまざまな種類のグループを作成し、pxGrid クライアントに提供されるサービスをこれらのグループにマッピングできます。[権限（Permissions）] ウィンドウの [グループの管理（Manage Groups）] オプションを使用して、新しいグループを追加します。[権限（Permissions）] ウィンドウで、事前定義されたグループ（EPS や ANC など）を使用する事前定義された許可ルールを表示できます。事前定義されたルールでは [操作（Operations）] フィールドだけを更新できることに注意してください。

pxGrid クライアントの許可ルールを作成するには、以下の手順を実行します。

ステップ 1 [管理（Administration）] タブから、[pxGridサービス（pxGrid Services）] > [権限（Permissions）] を選択します。

ステップ 2 [サービス（Service）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**

- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

ステップ 3 [操作（Operations）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **<ANY>**
- **パブリッシュ**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**

（注） このオプションを選択すると、カスタム操作を指定できます。

ステップ 4 [グループ（Groups）] ドロップダウン リストから、このサービスにマッピングするグループを選択します。

（EPS や ANC などの）事前定義されたグループ、および（[権限（Permissions）] ウィンドウの [グループの管理（Manage Groups）] オプションを使用して）手動で追加されたグループが、このドロップダウン リストに表示されます。

展開内のノードの表示

[展開ノード（Deployment Nodes）] ページで、展開を構成するすべての Cisco ISE ノード、プライマリ ノードおよびセカンダリ ノードを表示できます。

ステップ 1 プライマリ Cisco ISE 管理者ポータルにログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 3 左側のナビゲーション ペインで、 [展開（Deployment）] をクリックします。

展開を構成するすべての Cisco ISE ノードが表示されます。

モニタリングノードからのエンドポイント統計データのダウンロード

モニタリング ノードからネットワークに接続するエンドポイントの統計データをダウンロードできます。ロード、CPU使用率、認証トラフィックデータを含む主要パフォーマンスメトリック（KPM）が使用可能で、ネットワークの問題の監視およびトラブルシューティングに使用できます。日次 KPM 統計情報または過去 8 週間の KPM 統計情報をそれぞれダウンロードするには、Cisco ISE コマンドライン インターフェイス（CLI）から、**application configure ise** コマンドを使用し、オプション 12 または 13 を使用します。

このコマンドの出力では、エンドポイントに関する次のデータが提供されます。

- ネットワーク上のエンドポイントの総数
- 正常な接続を確立したエンドポイントの数
- 認証に失敗したエンドポイントの数。
- 毎日の接続済みの新しいエンドポイントの総数
- 毎日のオンボーディングしたエンドポイントの総数

出力には、タイムスタンプの詳細、展開内の各ポリシー サービス ノード（PSN）を介して接続したエンドポイントの総数、エンドポイントの総数、アクティブエンドポイント、負荷、および認証トラフィックの詳細も含まれています。

このコマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

データベースのクラッシュまたはファイルの破損の問題

Cisco ISE は、データ損失が発生する停電またはその他の理由により、Oracle データベース ファイルが破損している場合にクラッシュすることがあります。インシデントに応じて、データ損失から回復するには、次の手順を実行します。

- 展開で PAN が破損した場合は、セカンダリ PAN をプライマリ PAN に昇格する必要があります。
- 小規模な展開またはその他の理由により、SPAN を昇格できない場合は、利用可能な最新のバックアップを復元します。
- PSN が破損した場合は、次の手順を実行して、登録解除、設定のリセット、ノードの再登録を行います。
- スタンドアロン ボックスの場合、利用可能な最新のバックアップを復元します。

（注） 最新の設定変更が失われないようにするために、スタンドアロンボックスからバックアップを定期的に取得します。

モニタリングのためのデバイス設定

モニタリングノードにより、ネットワーク上のデバイスからのデータが受信および使用されて、ダッシュボードに表示されます。モニタリングノードとネットワークデバイス間の通信を有効にするには、スイッチと NAD を正しく設定する必要があります。

プライマリおよびセカンダリの Cisco ISE ノードの同期

Cisco ISE の設定に変更を加えることができるのは、プライマリ PAN からのみです。設定変更はすべてのセカンダリ ノードに複製されます。何らかの理由でこの複製が正しく実行されない場合は、プライマリ PAN に手動でセカンダリ PAN を同期できます。

始める前に

[同期ステータス（Sync Status）] が [同期していない（Out of Sync）] に設定されている場合や [複製ステータス（Replication Status）] が [失敗（Failed）] または [無効（Disabled）] の場合は、[同期を更新（Syncup）] ボタンをクリックして完全複製を強制的に実行する必要があります。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 3 プライマリ PAN と同期させるノードの横にあるチェックボックスをオンにし、[同期を更新（Syncup）] をクリックして完全データベース複製を強制的に実行します。

ノード ペルソナとサービスの変更

Cisco ISE ノードの設定を編集して、そのノードで実行されているペルソナおよびサービスを変更できます。

始める前に

- ポリシーサービス ノードで実行されるサービスを有効または無効にしたり、ポリシーサービス ノードを変更したりする場合は、そのサービスが実行されるアプリケーション サーバ プロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。

- このサービスの再起動の遅延により、自動フェールオーバーが開始される場合があります（展開内で有効になっている場合）。これを回避するには、自動フェールオーバー設定がオフになっていることを確認します。

ステップ 1 プライマリ PAN にログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 3 ペルソナまたはサービスを変更するノードの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 4 必要なサービスおよびペルソナを選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 プライマリ PAN でアラームの受信を確認して、ペルソナまたはサービスの変更を確認します。ペルソナまたはサービスの変更が正常に保存されなかった場合、アラームは生成されません。

Cisco ISE でのノードの変更による影響

Cisco ISE ISE で次のいずれかの変更を行うと、そのノードが再起動するため、遅延が発生します。

- ノードの登録（スタンドアロンからセカンダリへ）
- ノードの登録解除（セカンダリからスタンドアロンへ）
- プライマリ ノードからスタンドアロンへの変更（他のノードが登録されていない場合は、プライマリからスタンドアロンに変更されます）
- 管理ノードの昇格（セカンダリからプライマリへ）
- ペルソナの変更（ノードからポリシー サービスまたは監視ペルソナを割り当てたり、削除したりする場合）
- ポリシー サービス ノードでのサービスの変更（セッションとプロファイラ サービスを有効または無効にします）
- プライマリでのバックアップの復元（同期操作がトリガーされ、プライマリ ノードからセカンダリ ノードにデータが複製されます）

ポリシー サービス ノード グループの作成

2 つ以上のポリシー サービス ノード（PSN）が同じ高速ローカル エリア ネットワーク（LAN）に接続されている場合は、同じノード グループに配置することを推奨します。この設計は、グループにローカルの重要度が低い属性を保持し、ネットワークのリモート ノードに複製される情報を減らすことによって、エンドポイント プロファイリング データのレプリケーションを

最適化します。ノード グループ メンバーは、ピア グループ メンバーの可用性もチェックします。グループがメンバーに障害が発生したことを検出すると、障害が発生したノードの URL にリダイレクトされたすべてのセッションをリセットし、回復することを試行します。

（注） すべての PSN を同じノード グループの同じローカル ネットワークの部分に置くことを推奨します。PSN は、同じノード グループに参加するために負荷分散クラスタの一部である必要はありません。ただし、負荷分散クラスタの各ローカル PSN は通常同じノード グループに属している必要があります。

ノード グループにメンバーとして PSN を追加する前に、最初にノード グループを作成する必要があります。管理者ポータルの [展開（Deployment）] ページで、ポリシー サービス ノード グループを作成、編集、および削除できます。

始める前に

ノード グループ メンバーは TCP/7800 を使用して通信できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 [アクション（action）] アイコンをクリックし、[ノード グループの作成（Create Node Group）] をクリックします。

ステップ 3 ノード グループに付ける一意の名前を入力します。

ステップ 4 （任意）ノード グループの説明を入力します。

ステップ 5 （任意）[MAR キャッシュ分散の有効化（Enable MAR Cache Distribution）] チェックボックスをオンにし、その他のオプションを入力します。このオプションを有効にする前に、[Active Directory] ページで MAR が有効になっていることを確認してください。

ステップ 6 [送信（Submit）] をクリックして、ノード グループを保存します。

ノードグループを保存すると、左側のナビゲーション ペインにそのグループが表示されます。左側のペインにノードグループが表示されていない場合、そのグループは非表示になっている可能性があります。非表示オブジェクトを表示するには、ナビゲーション ペインで [展開（Expand）] ボタンをクリックします。

次のタスク

ノード グループにノードを追加します。ノードを編集するには、[ノード グループのメンバー（Member of Node Group）] ドロップダウン リストからノード グループを選択します。

展開からのノードの削除

展開からノードを削除するには、ノードの登録を解除する必要があります。登録解除されたノードは、スタンドアロン Cisco ISE ノードになります。

これはプライマリ PAN から受信した最後の設定を保持し、管理、ポリシー サービス、およびモニタリングであるスタンドアロン ノードのデフォルトのペルソナを担当します。モニタリング ノードを登録解除した場合、このノードは syslog ターゲットではなくなります。

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

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

プライマリ PAN の [展開（Deployment）] ページからこれらの変更を表示できます。ただし、変更が反映され、[展開（Deployment）] ページに表示されるには 5 分間の遅延が生じます。

始める前に

展開からセカンダリ ノードを削除する前に、必要に応じて後で復元できる Cisco ISE 設定のバックアップを実行します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 削除するセカンダリ ノードの隣のチェックボックスをオンにして、[登録解除（Deregister）] をクリックします。

ステップ 3 [OK] をクリックします。

ステップ 4 プライマリ PAN のアラームの受信を確認し、セカンダリ ノードが正常に登録解除されたことを確認します。セカンダリ ノードのプライマリ PAN からの登録解除が失敗した場合は、このアラームは生成されません。

ISE ノードのシャットダウン

halt コマンドを実行する前に、Cisco ISE アプリケーション サービスを停止し、バックアップ、復元、インストール、アップグレード、または削除操作を実行中でないことを確認します。Cisco ISE がこれらのいずれかの操作を行っている間に halt コマンドを実行すると、次のいずれかの警告メッセージが表示されます。

```
WARNING: A backup or restore is currently in progress! Continue with halt?

WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

halt コマンドの使用時に他のプロセスが実行されていない場合、または表示される警告メッセージに応じて [はい（Yes）] をクリックした場合は、次の質問に応答する必要があります。

```
Do you want to save the current configuration?
```

[はい（Yes）] をクリックして既存の Cisco ISE 設定を保存すると、次のメッセージが表示されます。

```
Saved the running configuration to startup successfully.
```

（注） アプライアンスを再起動する前に、アプリケーション プロセスを停止することをお勧めします。

これは、ISE の再起動にも適用されます。詳細については、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

スタンドアロン Cisco ISE ノードのホスト名または IP アドレスの変更

スタンドアロン Cisco ISE ノードのホスト名、IP アドレス、またはドメイン名を変更できます。ノードのホスト名として「localhost」を使用することはできません。

始める前に

Cisco ISE ノードが分散展開の一部である場合、展開から削除し、スタンドアロン ノードであることを確認する必要があります。

ステップ 1 Cisco ISE CLI から **hostname**、**ip address**、、または **ip domain-name** の各コマンドを使用して Cisco ISE ノードのホスト名または IP アドレスを変更します。

ステップ 2 すべてのサービスを再起動するために、Cisco ISE CLI から **application stop ise** コマンドを使用して Cisco ISE アプリケーション設定をリセットします。

ステップ 3 Cisco ISE ノードは、分散 展開の一部である場合、プライマリ PAN に登録します。

（注） Cisco ISE ノードの登録時にホスト名を使用する場合、登録するスタンドアロン ノードの完全修飾ドメイン名（FQDN）（たとえば、*abc.xyz.com*）は、プライマリ PAN から DNS を使用して解決できる必要があります。解決できない場合は、ノード登録が失敗します。DNS サーバに、分散展開の一部である Cisco ISE ノードの IP アドレスと FQDN を入力する必要があります。

セカンダリ ノードとして Cisco ISE ノードを登録した後、プライマリ PAN は IP アドレス、ホスト名、またはドメイン名への変更を展開内の他の Cisco ISE ノードに複製します。

Cisco ISE 展開のアップグレード

Cisco ISE では、管理者ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードプロセスはさらに簡素化され、アップグレードの進行状況およびノードのステータスが画面に表示されます。アップグレード前およびアップグレード後のタスクのリストについては、『*Cisco Identity Services Engine Upgrade Guide*』を参照してください。

[アップグレードの概要（Upgrade Overview）]ページには、展開内のすべてのノード、そのノードで有効なペルソナ、インストールされている ISE のバージョン、およびノードのステータス（ノードがアクティブか非アクティブか）がリストされます。ノードがアクティブな状態である場合にのみアップグレードを開始できます。

さまざまなタイプの展開

- スタンドアロンノード：管理、ポリシーサービスおよびモニタリングのペルソナを担当する単一の Cisco ISE ノード
- マルチノード展開：複数の ISE ノードによる分散展開。分散展開をアップグレードする手順については、次の参照先で説明しています。

ISE コミュニティ リソース

ネットワークが ISE 展開への準備ができているかどうかを評価する方法については、ISE Deployment Assistant（IDA）を参照してください。

分散展開のアップグレード

リリース 2.0 以降の管理者ポータルを使用して Cisco ISE 展開環境のすべてのノードをアップグレードすることもできます。また、Cisco ISE 2.0 以降の限定的な可用性リリースを一般的な可用性リリースにアップグレードすることもできます。

始める前に

（注） Cisco ISE STANDALONE ノードをアップグレードする場合、または既存の展開からノードを登録解除していて STANDALONE のアップグレードを実行する場合は、アップグレードを開始する前に、「/opt/oracle/base/admin/cpm10/dpdump」のパスにあるすべての upgradedb_*.properties ファイルを削除する必要があります。

上記のファイルを削除するにはルート権限が必要なため、Cisco TAC にお問い合わせください。詳細については CSCvi87302 を参照してください。

上記の回避策は、2018 年 4 月 13 日より前にアップグレードファイル（ise-upgradebundle-2.0.x-2.3.x-to-2.4.0.357.SPA.x86_64.tar.gz）をダウンロードした場合のみ必要です。

アップグレードする前に、次の作業が完了していることを確認します。

- ISE の設定および運用データのバックアップを取得します。
- システムログのバックアップを取得します。
- スケジュールしたバックアップを無効にします。展開のアップグレードが完了したら、バックアップスケジュールを再設定します。
- 証明書および秘密キーをエクスポートします。
- リポジトリを設定します。アップグレードバンドルをダウンロードし、このリポジトリに格納します。
- Active Directory の参加クレデンシャルと RSA SecurID ノード秘密のメモを取ります（該当する場合）。この情報は、アップグレード後に Active Directory または RSA SecurID サーバに接続するために必要です。
- アップグレードのパフォーマンスを向上させるために、運用データを消去します。
- リポジトリとのインターネット接続が良好であることを確認します。

（注） リポジトリからノードにアップグレードバンドルをダウンロードする場合、ダウンロードが完了するまでに 35 分以上かかるとダウンロードがタイムアウトします。この問題は、インターネットの帯域幅が不十分なために発生します。

ステップ 1 管理者ポータルの [アップグレード（Upgrade）] タブをクリックします。

ステップ 2 [続行（Proceed）] をクリックします。

[レビューチェックリスト（Review Checklist）] ウィンドウが表示されます。表示された手順を確認してください。

ステップ 3 [チェックリストを確認済み（I have reviewed the checklist）] チェックボックスをオンにし、[続行（Continue）] をクリックします。

[バンドルのノードへのダウンロード（Download Bundle to Nodes）] ウィンドウが表示されます。

ステップ 4 リポジトリからノードにアップグレードバンドルをダウンロードします。

a) アップグレードバンドルをダウンロードするノードの隣のチェックボックスをオンにします。

b) [ダウンロード（Download）] をクリックします。

[リポジトリおよびバンドルの選択（Select Repository and Bundle）] ウィンドウが表示されます。

c) リポジトリを選択します。

異なるノードで同じリポジトリまたは異なるリポジトリを選択できますが、すべてのノードで同じアップグレードバンドルを選択する必要があります。

d) アップグレードに使用するバンドルの隣にあるチェックボックスをオンにします。

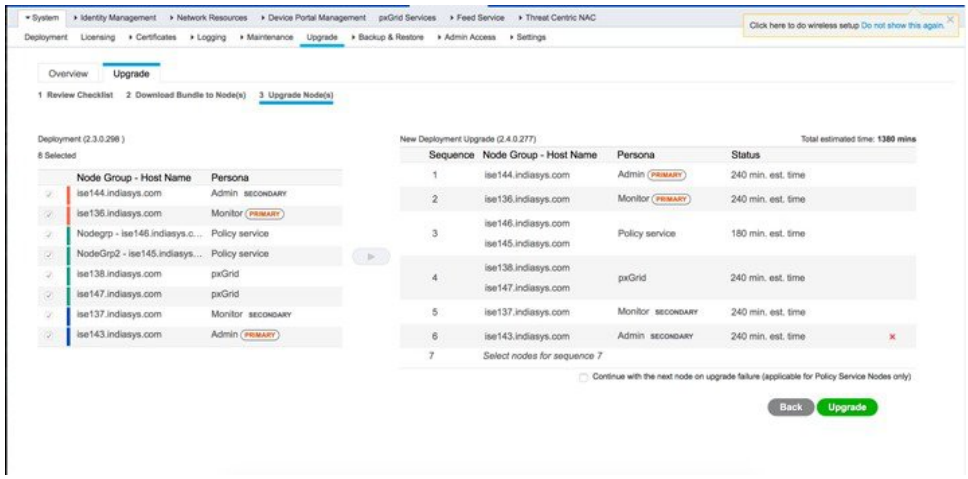
e) [確認（Confirm）] をクリックします。

バンドルがノードにダウンロードされると、ノードステータスが [アップグレードの準備が整いました（Ready for Upgrade）] に変わります。

ステップ 5 [続行（Continue）] をクリックします。

[ノードのアップグレード（Upgrade Nodes）] ウィンドウが表示されます。

図 2 : 現在の展開と新しい展開を表示する *[アップグレード（Upgrade）]* ウィンドウ



ステップ 6 アップグレード順序を選択します。

ノードを新しい展開に移動すると、アップグレードの推定所要時間が [ノードのアップグレード（Upgrade Nodes）] ウィンドウに表示されます。この情報を使用して、アップグレードを計画し、ダウンタイムを最小化できます。管理ノードとモニタリングノードのペアおよび複数のポリシーサービスノードがある場合は、以下の手順に従います。

a) デフォルトでは、セカンダリ管理ノードは、アップグレード順序の最初にリストされています。アップグレード後に、このノードは新しい展開でプライマリ管理ノードになります。

b) プライマリモニタリングノードは、次に新しい展開にアップグレードされるノードです。
c) ポリシーサービスノードを選択し、新しい展開に移動します。ポリシーサービスノードをアップグレードする順序を変更できます。

ポリシーサービスノードは、順番にまたは並行してアップグレードできます。ポリシーサービスノードのセットを選択し、並行してアップグレードできます。

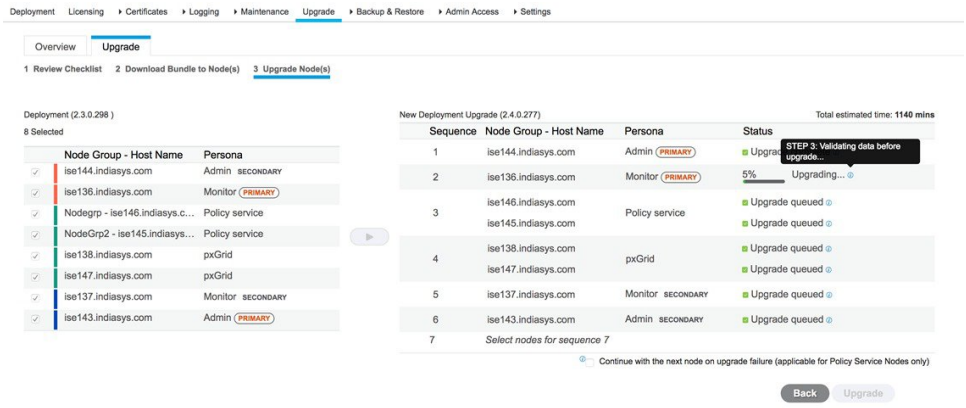
d) セカンダリ モニタリング ノードを選択し、新しい展開に移動します。
e) 最後に、プライマリ管理ノードを選択し、新しい展開に移動します。

ステップ 7 アップグレードがアップグレード順序のいずれかのポリシーサービスノードで失敗した場合でもアップグレードを続行するには、[失敗時でもアップグレードを続行する（Continue with upgrade on failure）] チェックボックスをオンにします。

このオプションは、セカンダリ管理ノードおよびプライマリ モニタリング ノードには適用されません。これらのノードのいずれかに障害が発生すると、アップグレードプロセスはロールバックされます。ポリシーサービスノードのいずれかが失敗すると、セカンダリ モニタリング ノードおよびプライマリ管理ノードはアップグレードされず、古い展開内に残ります。

ステップ 8 [アップグレード（Upgrade）] をクリックして、展開のアップグレードを開始します。

図 *3:* アップグレードの進行状況を表示する *[*アップグレード（*Upgrade*）*]* ウィンドウ



各ノードのアップグレードの進行状況が表示されます。正常に完了すると、ノードのステータスが[アップグレード完了（Upgrade Complete）] に変わります。

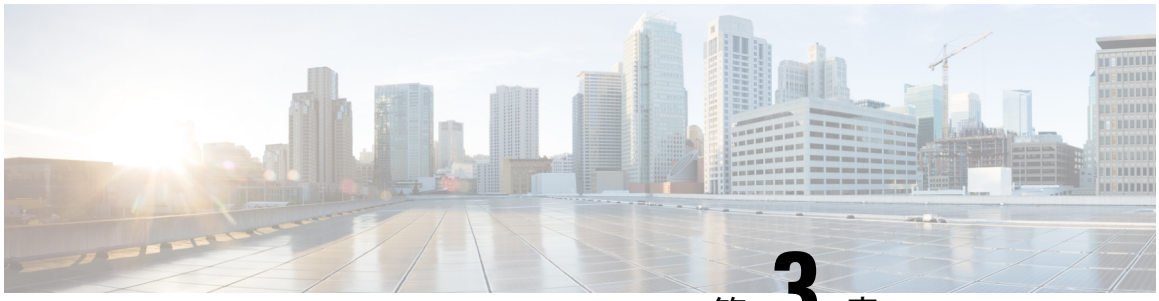
（注） 管理者ポータルからノードをアップグレードするときに、ステータスが長時間変化しない場合（80% のままの場合）は、CLI からアップグレードログをチェックするか、コンソールからアップグレードのステータスをチェックできます。アップグレードの進行状況を表示するには、CLI にログインするか、Cisco ISE ノードのコンソールを表示します。**show logging application** コマンドを使用すると、*upgrade-uibackend-cliconsole.log* および *upgrade-postosupgrade-yyyymmdd-xxxxxx.log* を表示できます。

show logging application コマンドを使用すると、CLI から次のアップグレードログを表示できます。

- DB データのアップグレードログ
- DB スキーマログ
- Post OS アップグレードログ

警告メッセージ「**The node has been reverted back to its pre-upgrade state**」が表示された場合は、**[アップグレード（Upgrade）]**ウィンドウに移動し、**[詳細（Details）]** リンクをクリックします。[アップグレードの失敗の詳細（Upgrade Failure Details）] ウィンドウに記載されている問題を解決します。すべての問題を解決した後、[アップグレード（Upgrade）] をクリックして、アップグレードを再起動します。

（注） 新しい展開のプライマリ管理ノードでポスチャデータの更新処理が実行している場合、プライマリ管理ノードにノードを登録できません。ポスチャ更新プロセスが終了するまで待つか（約20分かかることがあります）、またはアップグレードまたはノードの新しい展開への登録中に、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）] ページから、ポスチャの自動更新機能を無効にすることができます。

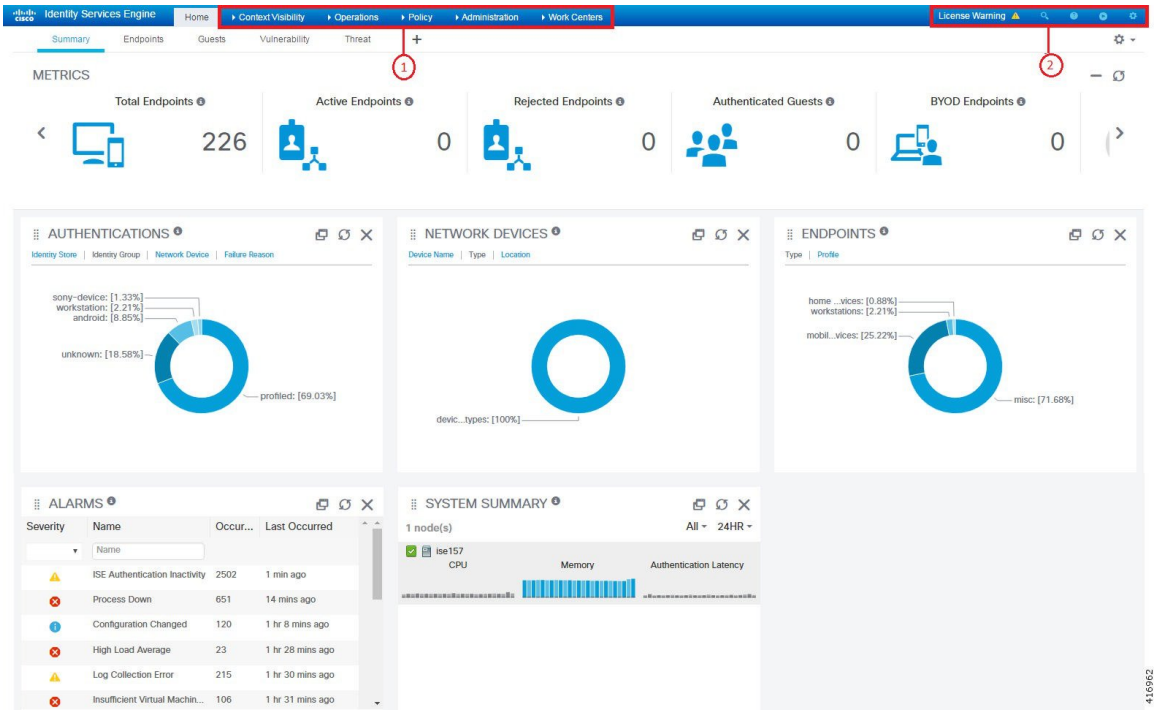


第 3 章

基本的なセットアップ

管理者ポータル

管理者ポータルでは、ISE の設定およびレポートにアクセスできます。次の図に、このポータルのメニュー バーの主な要素を示します。



1	メニューのドロップダウン	• [コンテキストの可視性（Context Visibility）]：これらのメニューでは、エンドポイント、ユーザ、NAD に関する情報が表示されます。情報は、ライセンスに応じて、機能、アプリケーション、BYOD、その他のカテゴリ別にセグメント化できます。コンテキスト メニューは中央データベースを使用して、データベース テーブル、キャッシュ、およびバッファから情報を収集し、それにより、コンテキストダッシュレットおよびリストの内容が非常に高速に更新されます。コンテキスト メニューは上部のダッシュレットおよび下部の情報のリストから構成されます。リストのカラム属性を変更することによってデータをフィルタすると、変更したコンテンツを示すためにダッシュレットが更新されます。 • [ポリシー（Policy）]：認証、許可、プロファイリング、ポスチャ、クライアントプロビジョニングの領域でネットワーク セキュリティを管理するためのツールにアクセスします。 • [管理（Administration）]：Cisco ISE ノード、ライセンス、証明書、ネットワーク デバイス、ユーザ、エンドポイント、およびゲスト サービスを管理するためのツールにアクセスします。

2	右上のメニュー	

- 

  エンドポイントを検索し、プロファイル、障害、IDストア、ロケーション、デバイス タイプ別にそれらの分布を表示します。

- 

  現在表示されているページ、ISE コミュニティへのリンク、ポータル ビルダーなどのオンライン ヘルプにアクセスします。

- 

  次のオプションにアクセスします。

  - [PassiveIDセットアップ（PassiveID Setup）]：[PassiveIDセットアップ（PassiveID Setup）]オプションでは、Active Directory を使用してパッシブ ID をセットアップする [PassiveIDセットアップ（PassiveID Setup）] ウィザードが起動されます。外部認証サーバからユーザ ID と IP アドレスを収集し、認証済み IP アドレスを対応するサブスクライバに配信するように、サーバを設定することができます。

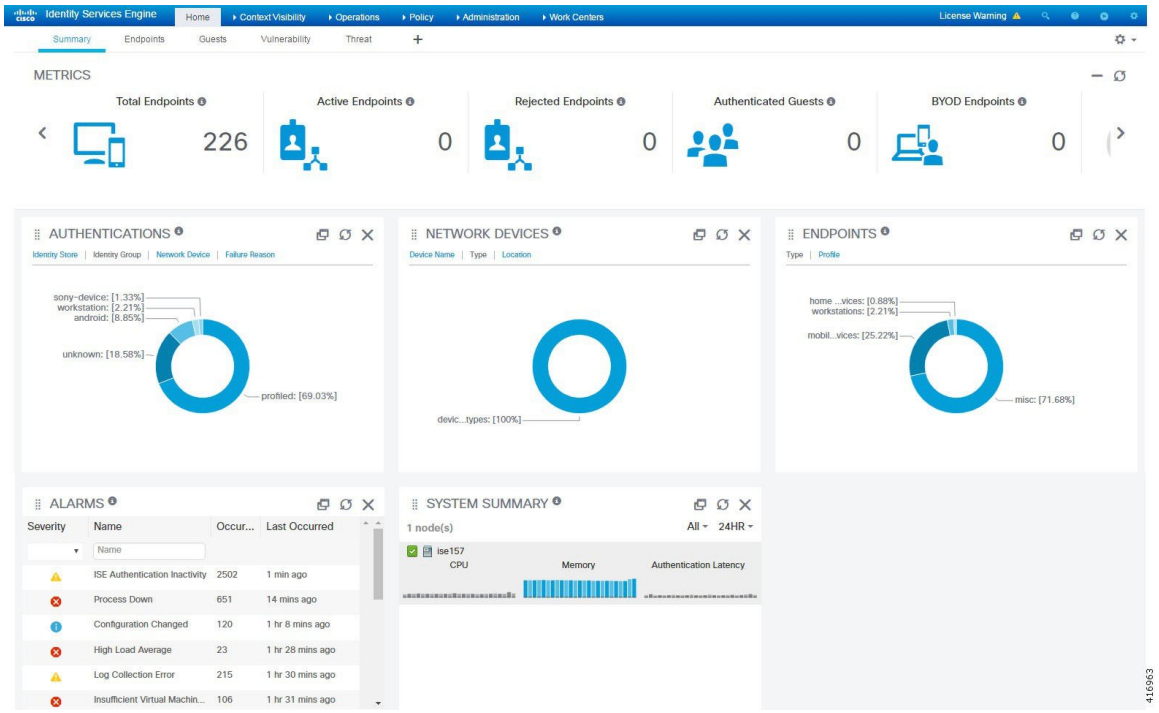
  - [可視性セットアップ（Visibility Setup）]：[可視性セットアップ（Visibility Setup）]オプションは、アプリケーション、ハードウェアインベントリ、USB ステータス、ファイアウォール ステータス、Windows エンドポイントの全般的なコンプライアンス ステータスなどのエンドポイント データを収集して Cisco ISE に送信する、価値の実証（PoV）サービスです。ISE の [可視性セットアップ（Visibility Setup）] ウィザードを起動すると、IP アドレス範囲を指定して、ネットワークの特定セグメントまたはエンドポイント グループに対してエンドポイント検出を実行できます。

    PoV サービスは Cisco Stealth Temporal エージェントを使用して、エンドポイント ポスチャ データを収集します。Cisco ISE は、管理者アカウント タイプで Windows を実行しているコンピュータに Cisco Stealth Temporal エージェントをプッシュし、一時的な実行可能ファイルを自動実行してコンテキストを収集し、エージェントが自動的に削除されます。Cisco Stealth Temporal エージェントのオプション デバッグ機能を使用するには、[エンドポイントロギング（Endpoint Logging）]チェックボックス（[可視性セットアップ（Visibility Setup）] > [ポスチャ（Posture）]）をチェックして、1 つまたは複数のエンド

		ポイントにデバッグ ログを保存します。ログは、次のいずれかの場所で参照できます。 • C:\WINDOWS\syswow64\config\systemprofile\（64 ビット オペレーティング システム） • C:\WINDOWS\system32\config\systemprofile\（32 ビット オペレーティング システム） • [ワイヤレスのセットアップ（ベータ）（Wireless Setup（BETA））] : [ワイヤレスのセットアップ（ベータ）（Wireless Setup（BETA））] オプションでは、802.1x、ゲスト、および個人所有デバイス持ち込み（BYOD）のワイヤレス フローを容易にセットアップできます。また、このオプションには、ゲストおよび BYOD 向けの各ポータルを設定してカスタマイズするためのワークフローも用意されています。 •  オンライン ヘルプの起動とアカウント設定の指定を含む、システム アクティビティ。

ISE ホーム ダッシュボード

Cisco ISE ダッシュボードには、効果的なモニタリングおよびトラブルシューティングに必要不可欠な、統合された相関性のあるライブ統計データが表示されます。特に指定がない限り、ダッシュボード要素によってアクティビティは 24 時間表示されます。次の図に、Cisco ISE ダッシュボードで使用できる情報の一部を示します。Cisco ISE ダッシュボード データはプライマリ管理ノード（PAN）でのみ表示されます。



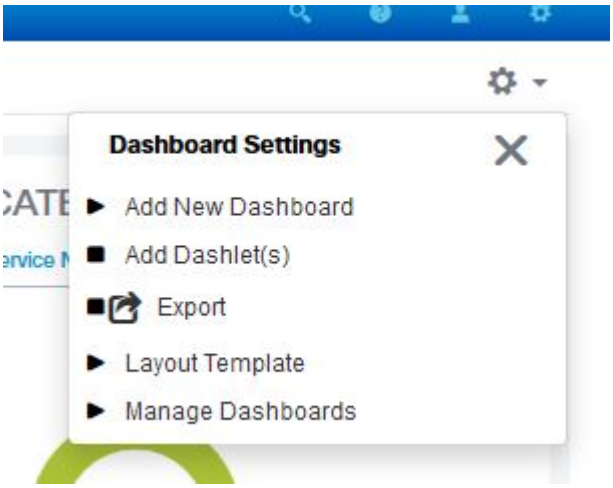
[ホーム（Home）]ページには、ISEデータのビューを表示する5つのデフォルトダッシュボードがあります。

- [概要（Summary）]：このビューには、線形の[メトリック（Metrics）]ダッシュレット、円グラフ ダッシュレット、およびリスト ダッシュレットが表示されます。[メトリック（Metrics）]ダッシュレットは設定できません。
- [エンドポイント（Endpoints）]：ステータス、エンドポイント、エンドポイント カテゴリ、ネットワーク デバイス。
- [ゲスト（Guests）]：ゲスト ユーザ タイプ、ログイン失敗、ロケーション。
- [脆弱性（Vulnerability）]：脆弱性サーバにより ISE に報告される情報。
- [脅威（Threat）]：脅威サーバにより ISE に報告される情報。

これらの各ダッシュボードには、複数の事前定義ダッシュレットがあります。たとえば[概要（Summary）]ダッシュボードには[ステータス（Status）]、[エンドポイント（Endpoints）]、[エンドポイント カテゴリ（Endpoint Categories）]、および[ネットワーク デバイス（Network Devices）]があります。

ホーム ダッシュボードの設定

ホーム ページ ダッシュボードをカスタマイズするには、ページの右上隅にある歯車アイコンをクリックします。



- [エクスポート（Export）] は、現在選択されているホーム ビューを PDF に保存します。
- [レイアウト テンプレート（Layout Template）] は、このビューに表示される列の数を設定します。
- [ダッシュボードの管理（Manage Dashboards）] では、現在のダッシュボードをデフォルト（[ホーム（Home）] を選択すると表示されるダッシュボード）に設定するか、またはすべてのダッシュボードをリセットする（すべてのホーム ダッシュボードの設定を削除する）ことができます。

[コンテキストの可視性（Context Visibility）] のビュー

[コンテキストの可視性（Context Visibility）] ページの構造はホーム ページに似ていますが、[コンテキストの可視性（Context Visibility）] ページでは次の点が異なります。

- 表示データをフィルタリングするときに、現在のコンテキストを維持する（ブラウザ ウィンドウ）。
- より細かなカスタマイズが可能である
- エンドポイント データを中心としている

コンテキストの可視性データはプライマリ管理ノード（PAN）にのみ表示されます。

[コンテキスト（Context）] ページのダッシュレットには、エンドポイントと、エンドポイントからNADへの接続に関する情報が表示されます。現在表示されている情報は、各ページのダッシュレットの下にあるデータ リストの内容に基づいています。各ページには、タブの名前に基づいてエンドポイント データのビューが表示されます。データをフィルタリングすると、リストとダッシュレットの両方が更新されます。データをフィルタリングするには、1 つ以上の円グラフの特定部分をクリックするか、表で行をフィルタリングするか、またはこれらの操作を組み合わせて実行します。複数のフィルタを選択した場合、フィルタ結果は加算的になります。これはカスケード フィルタと呼ばれます。これにより、ドリルダウンして特定のデータを

見つけることができます。また、リストでエンドポイントをクリックして、そのエンドポイントの詳細ビューを表示することもできます。

[コンテキストの可視性（Context Visibility）] には 4 つのメイン ビューがあります。

- [エンドポイント（Endpoints）]：デバイス タイプ、コンプライアンス ステータス、認証タイプ、ハードウェア インベントリなどに基づいて表示するエンドポイントを選択できます。詳細については、「ハードウェア ダッシュボード（108 ページ）」の項を参照してください。

（注） アカウンティングの開始および更新情報が Cisco ISE に確実に送信されるように、NAD でアカウンティングの設定を有効にすることを推奨します。

Cisco ISE では、アカウンティングが有効な場合にのみ、最新の IP アドレス、セッションのステータス（接続 [Connected]、切断 [Disconnected]、または拒否 [Rejected]）、エンドポイントの非アクティブな日数などのアカウンティング情報を収集できます。この情報は、[ライブ ログ（Live Logs）]、[ライブ セッション（Live Sessions）] および [コンテキストの可視性（Context Visibility）] ページに表示されます。NAD でアカウンティングが無効にされている場合、[ライブ セッション（Live Sessions）]、[ライブ ログ（Live Logs）] および [コンテキストの可視性（Context Visibility）] ページ間でアカウンティング情報が欠落しているか、間違っているか、一致していない可能性があります。

（注） [可視性セットアップ（Visibility Setup）] ウィザードでは、エンドポイントを検出するため IP アドレス範囲のリストを追加できます。このウィザードの設定後に、Cisco ISE はエンドポイントを認証しますが、設定された IP アドレス範囲に含まれないエンドポイントは、[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] タブと、[エンドポイント（Endpoints）] リスト ページ（[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）] の下）には表示されません。

- [ユーザベース（User-Based）]：ユーザ ID ソースからのユーザ情報を表示します。

  このビューを使用する際には次の点に注意してください。

  1. ユーザ名属性またはパスワード属性が変更されると、認証ステータスが変更された時点でこのページに変更が即時に反映されます。
  2. Active Directory でユーザ名以外の属性が変更されると、再認証から 24 時間後に、更新された属性が表示されます。

3. Active Directory でユーザ名とその他の属性が変更されると、再認証後即時に最新の変更が表示されます。

- [ネットワーク デバイス（Network Devices）]：エンドポイントに接続している NAD のリスト。NAD のエンドポイント数（右端の列）をクリックすると、その NAD に基づいてフィルタリングされたすべてのデバイスが [コンテキストの可視性（Context Visibility）] 画面にリストされます。

（注） ネットワーク デバイスに SNMPv3 パラメータを設定した場合、モニタリング サービス（[操作（Operations）]>[レポート（Reports）]>[カタログ（Catalog）]>[ネットワーク デバイス（Network Device）]>[セッション ステータス概要（Session Status Summary）]）によって提供されるネットワーク デバイス セッション ステータス概要レポートを生成できません。ネットワーク デバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。

- [アプリケーション（Application）]：[アプリケーション（Application）] ビューは、指定されたアプリケーションがインストールされているエンドポイントの数を識別するために使用されます。結果は、グラフ形式と表形式で表示されます。グラフ表示は、比較分析に役立ちます。たとえば、Google Chrome ソフトウェアを使用してエンドポイントの数をバージョン、ベンダー、カテゴリ（フィッシング詐欺対策、ブラウザなど）と共に、表や棒グラフで確認することができます。詳細については、「アプリケーション ダッシュボード」の項を参照してください。

フィルタリング処理を追加する目的で、[コンテキストの可視性（Context Visibility）] の下に新しいビューを作成し、カスタム リストを作成できます。このリリースでは、カスタム ビューでダッシュレットがサポートされていません。

ダッシュレットの円グラフの特定部分をクリックすると、新しいページが開き、そのダッシュレットからフィルタリングされたデータが [コンテキストの可視性（Context Visibility）] モードで表示されます。この新しいページから、表示されているデータをさらにフィルタリングできます。これについては「ビューに表示するデータのフィルタリング （111 ページ）」で説明します。

[コンテキストの可視性（Context Visibility）] を使用してエンドポイント データを検索する方法の詳細については、Cisco YouTube ビデオを参照してください。このビデオでは ISE 2.1 https://www.youtube.com/watch?v=HvonGhrydfg を使用しています。

関連トピック

ハードウェア ダッシュボード （108 ページ）

コンテキストの可視性の属性

コンテキストの可視性の属性を提供するシステムとサービスでは、同じ属性名に異なる値を使用していることがよくあります。次にいくつかの例を示します。

オペレーティング システム

- *OperatingSystem*：ポスチャ オペレーティング システム
- *operating-system*：NMAP オペレーティング システム
- *operating-system-result*：プロファイラ統合オペレーティング システム

（注） Cisco ISE のエンドポイントに複数のプローブが有効になっている場合、[コンテキストの可視性（Context Visibility）] ページに表示されるエンドポイントのオペレーティングシステムのデータにいくつかの不一致が生じることがあります。

ポータル名

- *Portal.Name*：デバイス登録が有効な場合のゲスト ポータル名。
- *PortalName*：デバイス登録が無効な場合のゲスト ポータル名。

ポータル ユーザ

- *User-Name*：RADIUS 認証のユーザ名
- *GuestUserName*：ゲスト ユーザ
- *PortalUser*：ポータル ユーザ

アプリケーション ダッシュボード

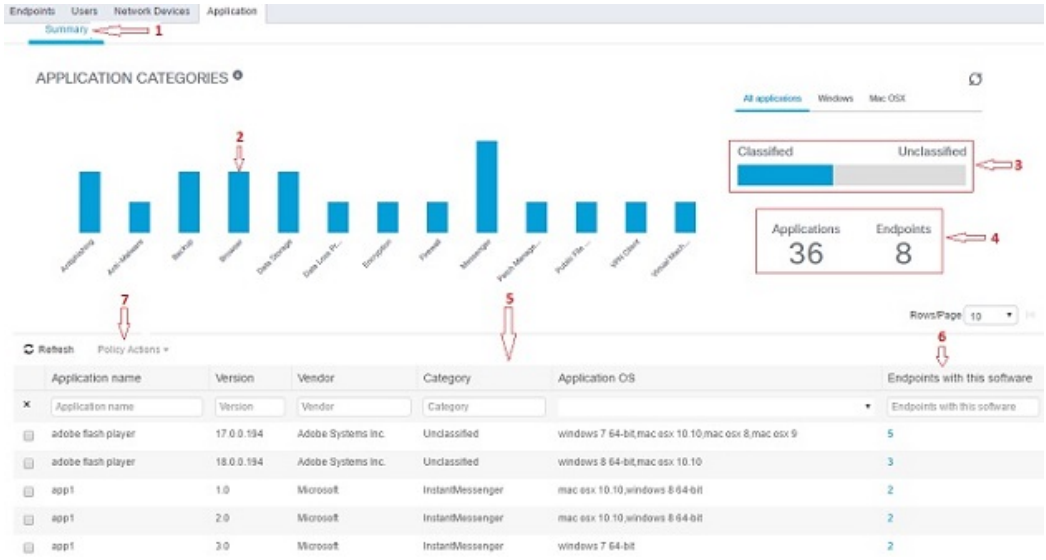
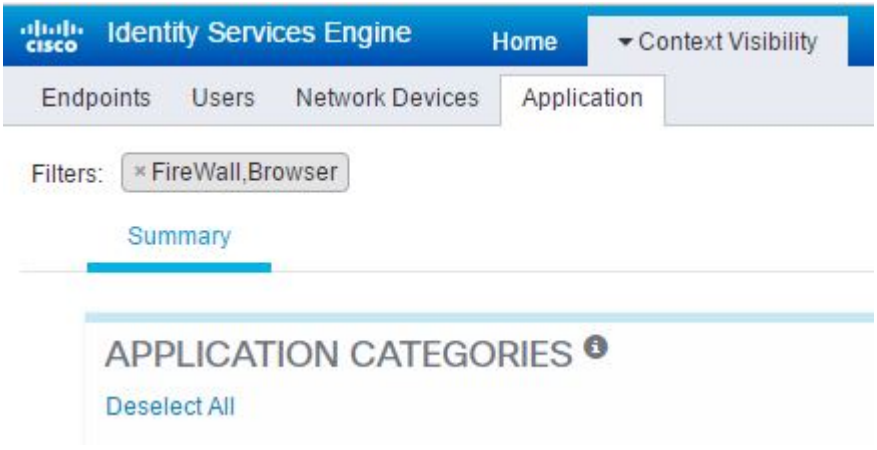


表 *9*:アプリケーション ダッシュボードの説明

ラベル	説明
1	デフォルトで[概要（Summary）]タブが選択されています。棒グラフを含む[アプリケーション カテゴリ（Application Categories）]ダッシュレットが表示されます。アプリケーションは13のカテゴリに分類されます。これらのカテゴリに属さないアプリケーションは、「未分類（Unclassified）」と呼ばれます。 利用可能なカテゴリは、[マルウェア対策（Anti-Malware）]、[フィッシング対策（Antiphishing）]、[バックアップ（Backup）]、[ブラウザ（Browser）]、[データ漏洩防止（Data Loss Prevention）]、[データ ストレージ（Data Storage）]、[暗号化（Encryption）]、[ファイアウォール（Firewall）]、[メッセンジャ（Messenger）]、[パッチ管理（Patch Management）]、[パブリック ファイル共有（Public File Sharing）]、[仮想マシン（Virtual Machine）]、[VPN クライアント（VPN Client）]です。
2	各バーは、分類されたカテゴリに対応します。各バーの上にマウスを置くと、選択したアプリケーション カテゴリに対応するアプリケーションとエンドポイントの合計数を表示できます。
3	分類されたカテゴリに該当するアプリケーションとエンドポイントは青色で表示されます。未分類のアプリケーションとエンドポイントはグレーで表示されます。分類されたカテゴリ バーまたは分類されていないカテゴリ バーの上にマウスを置くと、そのカテゴリに属するアプリケーションとエンドポイントの合計数を表示できます。[分類済み（Classified）]をクリックして、棒グラフと表（5）で結果を表示できます。[未分類（Unclassified）]をクリックすると、棒グラフが無効になり（グレー表示）、結果が表（5）に表示されます。
4	アプリケーションとエンドポイントは、選択されたフィルタに基づいて表示されます。異なるフィルタをクリックすると、パンくずリストを表示できます。[すべて選択解除（Deselect All）]をクリックして、すべてのフィルタを削除できます。 

<table>
<tr><th>ラベル</th><th>説明</th></tr>
<tr><td>5</td><td>複数のバーをクリックすると、対応する分類されたアプリケーションとエンドポイントが表に表示されます。たとえば、[マルウェア対策（Antimalware）]および[パッチ管理（Patch Management）] カテゴリを選択すると、次の結果が表示されます。
<table>
<tr><th>アプリケーション</th><th>バージョン</th><th>Vendor</th><th>カテゴリ</th><th>アプリケーション OS</th><th>このソフトウェアで使用するエンドポイント</th></tr>
<tr><td>Gatekeeper</td><td>9.9.5</td><td>Apple Inc.</td><td>マルウェア対策</td><td>windows 7 64 ビット、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
<tr><td>Gatekeeper</td><td>10.9.5</td><td>Apple Inc.</td><td>マルウェア対策</td><td>windows 8 64 ビット、mac osx 10.10</td><td>3</td></tr>
<tr><td>ソフトウェア更新</td><td>2.3</td><td>Apple Inc.</td><td>パッチ管理</td><td>windows 7 64 ビット、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
</table></td></tr>
<tr><td>6</td><td>表の [このソフトウェアで使用するエンドポイント（Endpoints With This Software）] 列のエンドポイントをクリックして、Mac アドレス、NAD IP アドレス、NAD ポート ID/SSID、IPv4 アドレスなどのエンドポイントの詳細を表示します。</td></tr>
<tr><td>7</td><td>アプリケーションのコンプライアンス条件と修復を作成するには、アプリケーション名を選択し、[ポリシー アクション（Policy Actions）] ドロップダウンリストから [アプリケーション コンプライアンスの作成（Create App Compliance）] オプションを選択します。</td></tr>
</table>

ハードウェア ダッシュボード

[コンテキストの可視性（context visibility）] の下の [エンドポイント ハードウェア（endpoint hardware）] タブは、短期間にエンドポイント ハードウェア インベントリ情報を収集、分析、およびレポートするのに役立ちます。メモリ容量が小さいエンドポイントの検出や、エンドポイントのBIOSモデル/バージョンの検出など、情報を収集することができます。これらの結果に基づいて、メモリ容量を増やしたり、BIOS バージョンをアップグレードすることができます。アセットの購入を計画する前に、要件を評価することができます。リソースを適時に交換することができます。モジュールをインストールしたりエンドポイントとやりとりすることなく、この情報を収集できます。要約すると、アセットのライフサイクルを効果的に管理できます。

[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [ハードウェア（Hardware）] ページには、[製造者（Manufacturers）] および [エンドポイント使用率（Endpoint Utilizations）] ダッシュレットが表示されます。これらのダッシュレットは、選択されたフィルタに基づく変更を反映します。[製造者（Manufacturers）] ダッシュレットには、Windows および Mac OS が搭載されたエンドポイントのハードウェア インベントリの詳細が表示されます。[エンドポイント使用率（Endpoint Utilizations）] ダッシュレットには、エンドポイントの CPU、メモリ、およびディスク使用率が表示されます。3 つのオプションのいずれかを選択すると、利用率をパーセンテージで表示できます。

- [CPU 使用率が n% を超えるデバイス（Devices With Over n% CPU Usage）]
- [メモリ使用率が n% を超えるデバイス（Devices With Over n% Memory Usage）]
- [ディスク使用率が n% を超えるデバイス（Devices With Over n% Disk Usage）]

（注） ハードウェア インベントリ データは、ISE GUI に表示されるまでに 120 秒かかります。ハードウェア インベントリ データは、ポスチャ準拠および非準拠の状態について収集されます。

エンドポイントとその接続された外部デバイスのハードウェア属性は表形式で表示されます。次のハードウェア属性が表示されます。

- MAC アドレス
- BIOS 製造元
- BIOS シリアル番号
- BIOS モデル
- 接続デバイス
- CPU 名
- CPU 速度（GHz）
- CPU 使用率（%）
- コア数
- プロセッサ数
- メモリ サイズ（GB）
- メモリ使用率（%）
- 内部ディスクの合計サイズ（GB）
- 内部ディスクの合計フリー サイズ（GB）
- 内部ディスクの合計使用率（%）
- 内部ディスク数

- NAD ポート ID
- ステータス
- ネットワークデバイス名
- 参照先
- UDID
- IPv4 アドレス
- ユーザ名
- ホストネーム
- OS タイプ
- 異常な動作
- エンドポイント プロファイル
- 説明
- エンドポイント タイプ
- ID グループ
- 登録日
- ID ストア
- 許可プロファイル

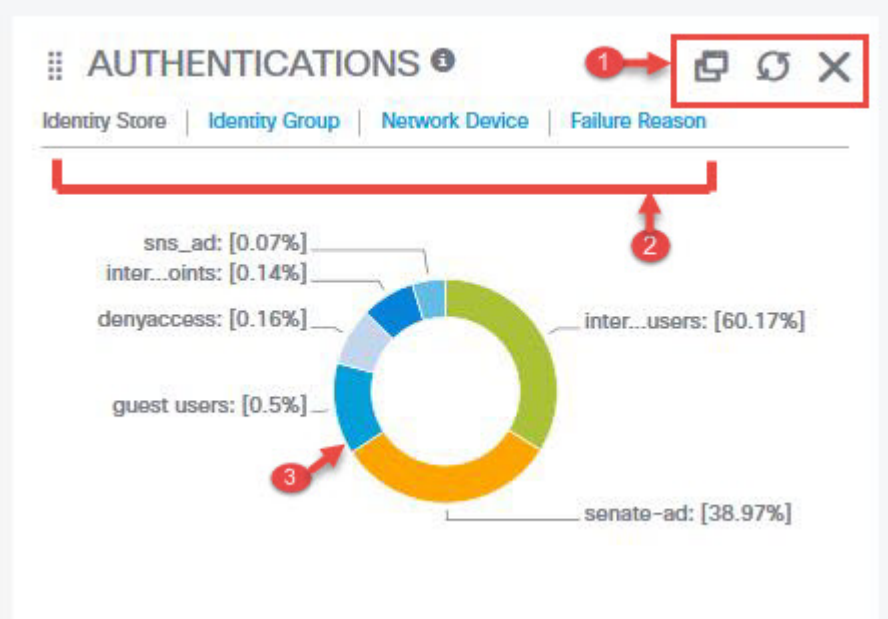
エンドポイントに対応する [接続デバイス（Attached Devices）] 列の番号をクリックすると、現在エンドポイントに接続されている USB デバイスの名前、カテゴリ、製造元、タイプ、製品 ID、およびベンダー ID を表示できます。

（注） Cisco ISE はクライアントのシステムのハードウェア属性をプロファイリングしますが、Cisco ISE がプロファイリングしないハードウェア属性がいくつか存在することがあります。これらのハードウェア属性は、[ハードウェア コンテキストの可視性（Hardware Context Visibility）] ページに表示されないことがあります。

ハードウェア インベントリ データの収集間隔は、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** ページで制御できます。デフォルトの間隔は 5 分です。

ダッシュレット

次に、ダッシュレットの例を示します。



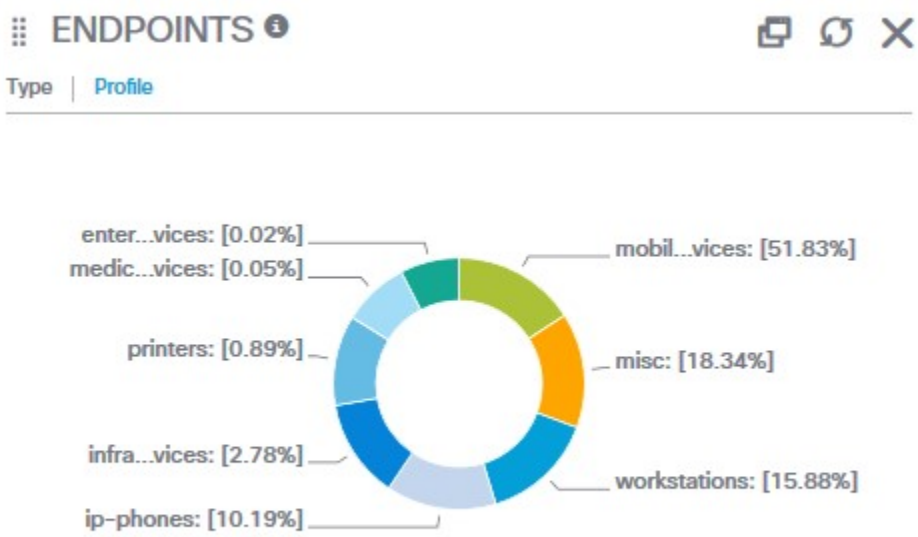
1. ウィンドウが重なり合ったシンボルは、このダッシュレットを「切り離し」ます。つまり、新しいブラウザ ウィンドウでこのダッシュレットを開きます。円形のシンボルは更新を実行します。Xはこのダッシュレットを削除します。このシンボルはホームページでのみ使用可能です。[コンテキストの可視性（Context Visibility）] でダッシュレットを削除するには、画面右上隅にある歯車のシンボルを使用します。
2. 一部のダッシュレットには異なるカテゴリのデータが表示されます。リンクをクリックすると、そのデータ セットの円グラフが表示されます。
3. 円グラフには、選択したデータが表示されます。円グラフの 1 つのセグメントをクリックすると、[コンテキストの可視性（Context Visibility）] で新しいタブが開き、円グラフ セグメントに基づいてフィルタリングされたデータが表示されます。

ホーム ダッシュボードで円グラフのセクションをクリックすると、新しいブラウザ ウィンドウが開き、円グラフでクリックしたセクションに基づいてフィルタリングされたデータが表示されます。

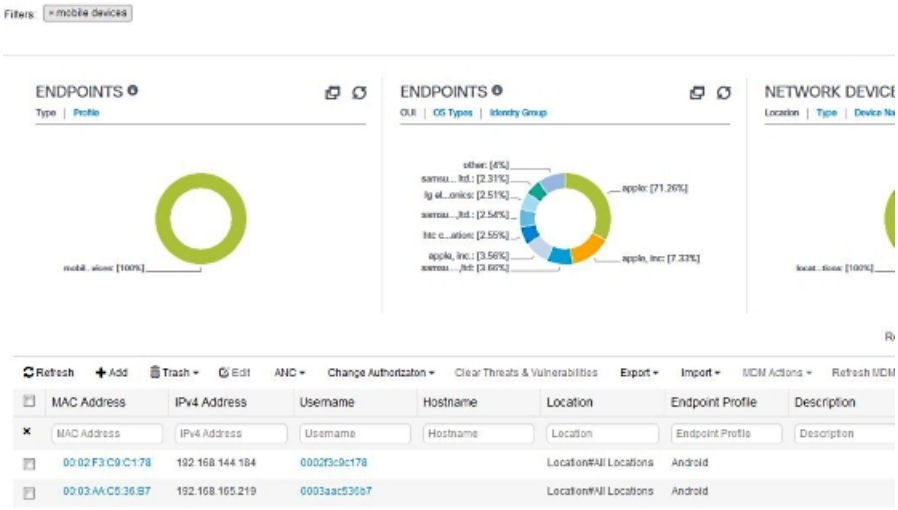
[コンテキスト（Context）] ビューで円グラフのセクションをクリックすると、表示されているデータがフィルタリングされますが、コンテキストは変更されず、フィルタリングされたデータは同じブラウザ ウィンドウに表示されます。

ビューに表示するデータのフィルタリング

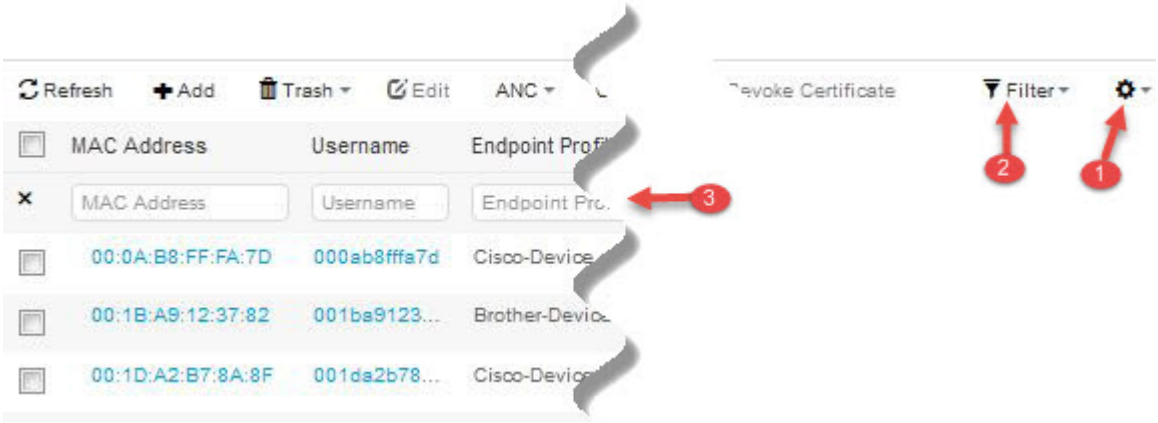
[コンテキストの可視性（Context Visibility）] ページでいずれかのダッシュレットをクリックすると、クリックしたアイテムに基づいて表示されるデータ（円グラフの一部分など）がフィルタリングされます。



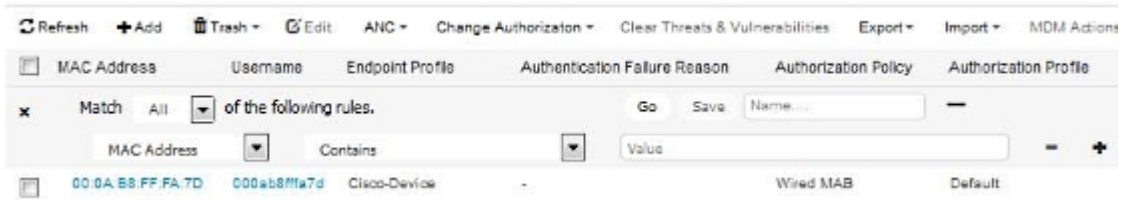
[エンドポイント（Endpoints）] ダッシュレットで [mobil…vices] をクリックすると、ページが再表示され、2 つの [エンドポイント（Endpoints）] ダッシュレット、[ネットワークデバイス（Network Devices）] ダッシュレット、およびデータのリストが表示されます。次の例に示すように、ダッシュレットとリストにはモバイル デバイスのデータが表示されます。



さらにデータをフィルタリングするには、円グラフの他のセクションをクリックするか、またはデータ リストのコントロールを使用します。



1. 歯車アイコンにより、表示列がフィルタリングされます。ドロップダウンでは、このダッシュボードのリストに表示する列を選択できます。
2. デフォルトではクイック フィルタが表示されます。ボックス（ラベル番号 3）に文字を入力すると、結果に基づいてリストがフィルタリングされます。カスタムフィルタでは、次に示すようにより細かく設定できるフィルタが表示されます。



カスタム フィルタは保存できます。

カスタム フィルタの作成

カスタムフィルタを作成および保存し、プリセットフィルタでフィルタ条件を変更できます。カスタム フィルタは Cisco ISE データベースに保存されません。カスタム フィルタにアクセスするには、そのフィルタの作成に使用した同じコンピュータおよびブラウザを使用する必要があります。

ステップ 1 [表示（Show）] ドロップダウン リストをクリックし、[拡張フィルタ（Advanced Filter）] を選択します。
ステップ 2 [フィルタ（Filter）] メニューからフィールド、演算子、値などの検索属性を指定します。
ステップ 3 [+] をクリックして、その他の条件を追加します。
ステップ 4 [実行（Go）] をクリックして、指定された属性に一致するエントリを表示します。
ステップ 5 [保存（Save）] アイコンをクリックしてフィルタを保存します。
ステップ 6 名前を入力し、[Save（保存）] をクリックします。フィルタが [表示（Show）] ドロップダウン リストに表示されます。

拡張フィルタを使用した条件によるデータのフィルタリング

拡張フィルタを使用して、指定した条件（名 = Mike、ユーザ グループ = 従業員など）に基づいて情報をフィルタリングできます。複数の条件を指定できます。

ステップ 1 [表示（Show）] ドロップダウン リストをクリックし、[拡張フィルタ（Advanced Filter）] を選択します。

ステップ 2 [フィルタ（Filter）] メニューから検索および検索属性（フィールド、演算子、値など）を指定します。

ステップ 3 [+] をクリックして、その他の条件を追加します。

ステップ 4 [実行（Go）] をクリックして、指定された属性に一致するエントリを表示します。

クイックフィルタを使用したフィールド属性によるデータのフィルタリング

クイック フィルタを使用して、リストページに表示されるフィールド属性の値を入力し、ページをリフレッシュすることで、フィルタ基準に一致するレコードのみを一覧表示できます。

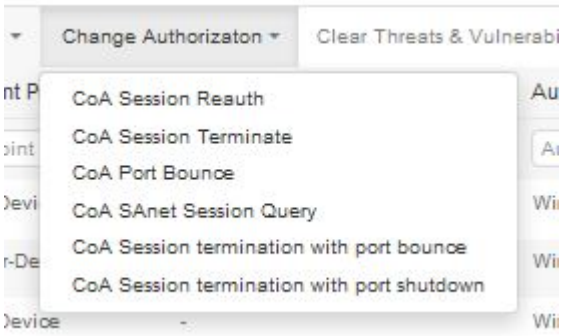
ステップ 1 [表示（Show）] ドロップダウン リストをクリックし、[クイック フィルタ（Quick Filter）] を選択します。

ステップ 2 属性フィールドの 1 つ以上に検索条件を入力すると、指定した属性に一致するエントリが自動的に表示されます。

ビューのリストでのエンドポイント アクション

リスト上部にあるツールバーから、リストで選択したエンドポイントに対してアクションを実行できます。すべてのリストですべてのアクションが有効になっているわけではありません。一部のアクションは、使用可能な機能に基づいています。次のリストに、使用する前にISEで有効にする必要がある 2 つのエンドポイント アクションを示します。

- 適応型ネットワーク制御（ANC）が有効な場合、リストでエンドポイントを選択して、ネットワーク アクセスを割り当てるかまたは取り消すことができます。認可変更（CoA）も発行できます。



ANC（エンドポイント保護サービス）は、ISE の [管理（Administration）] > [システム（System）] > [設定（Settings）] > [エンドポイント保護サービス（Endpoint Protection Service）] > [適応型ネットワーク制御（Adaptive Network Control）] で有効にします。詳細については、の「Cisco ISE での適応型ネットワーク制御の有効化」のセクションを参照してくださいCisco ISE での適応型ネットワーク制御の有効化 （255 ページ）。

- MDM がインストールされている場合は、選択したエンドポイントに対して MDM アクションを実行できます。

Cisco ISE ダッシュボード

Cisco ISE ダッシュボードまたはホームページ（[ホーム（Home）] > [概要（Summary）]）は、Cisco ISE 管理コンソールにログインすると表示されるランディング ページです。ダッシュボードは、ウィンドウの上部に沿って表示されるメトリック メーターと下にあるダッシュレットで構成された、集中化された管理コンソールです。デフォルトのダッシュボードは、[概要（Summary）]、[エンドポイント（Endpoints）]、[ゲスト（Guests）]、[脆弱性（Vulnerability）]、[脅威（Threat）] です。詳細については、ISE ホーム ダッシュボード （101 ページ）の項を参照してください。

（注） ダッシュボード データはプライマリ PAN にのみ表示されます。

ダッシュボードのリアルタイムデータによって、ネットワークにアクセスしているデバイスおよびユーザの一目で確認できるステータスと、システムの正常性の概要が示されます。

2 番目のレベルのメニューバーにある歯車アイコンをクリックして、ダッシュボード設定のドロップダウンリストを表示します。次の表に、[ダッシュボード設定（Dashboard Settings）] で使用可能なオプションに関する情報を示します。

オプション	説明
新しいダッシュボードの追加（Add New Dashboard）	5 つのデフォルトのダッシュボードを含めて、最大で 20 個のダッシュボードを設定できます。

オプション	説明
ダッシュボードの名前の変更	ダッシュボードの名前を変更するには、次の手順を実行します（カスタム ダッシュボードに対してのみ使用可能）。 **1.** [ダッシュボードの名前の変更（Rename Dashboard）] をクリックします。 **2.** 新しい名前を指定します。 **3.** [適用（Apply）] をクリックします。
ダッシュレットの追加（**Add Dashlet**）	ホームページダッシュボードにダッシュレットを追加するには、次の手順を実行します。 **1.** [Add Dashlet(s)] をクリックします。 **2.** [ダッシュレットの追加（Add Dashlets）] ウィンドウで、追加するダッシュレットの横にある [追加（Add）] をクリックします。 **3.** [保存（Save）] をクリックします。 （注） ダッシュボードごとに最大で 9 個のダッシュレットを追加できます。

オプション	説明
エクスポート	ダッシュレットデータをPDFまたはCSVファイルとしてエクスポートできます。 手順は次のとおりです。 **1.** Cisco ISE ホーム ページから、[サマリー（Summary）] など、対応するダッシュボードを選択します。 **2.** [ダッシュボード設定（Dashboard Settings）] > [エクスポート（Export）] の順に選択します。 **3.** [エクスポート（Export）] ダイアログボックスで、次のいずれかのファイル形式を選択します。 • 選択したダッシュレットのスナップショットを表示するには、 PDF 形式を選択します。 • 選択したダッシュボードデータをZIPファイルとしてダウンロードするには、CSV 形式を選択します。 **4.** [ダッシュレット（Dashlets）] セクションで必要なダッシュレットを選択します。 **5.** [エクスポート（Export）] をクリックします。 ZIP ファイルには、選択したダッシュボードの個々のダッシュレット CSV ファイルが含まれています。ダッシュレットの各タブに関連するデータは、対応するダッシュレット CSV ファイルで個別のセクションとして示されます。 カスタム ダッシュボードをエクスポートする場合、ZIPファイルは同じ名前でエクスポートされます。たとえば、MyDashboard という名前のカスタム ダッシュボードをエクスポートすると、エクスポートされたファイルの名前は MyDashboard.zip となります。

オプション	説明
レイアウト テンプレート（**Layout Template**）	ダッシュレットが表示されるテンプレートのレイアウトを変更できます。 レイアウトを変更するには、次の手順を実行します。 **1.** [ダッシュボード設定（Dashboard Settings）] > [レイアウト テンプレート（Layout Template）] の順に選択します。 **2.** 使用可能なオプションから必要なレイアウトを選択します。
ダッシュボードの管理	[ダッシュボードの管理（Manage Dashboards）] では次のオプションを使用できます。 • [デフォルトのダッシュボードにする（Mark as Default Dashboard）]：ダッシュボードをデフォルト ダッシュボード（ホーム ページ）として設定するには、このオプションを使用します • [すべてのダッシュボードのリセット（Reset all Dashboards）]：すべてのダッシュボードを元の設定にリセットするには、このオプションを使用します

対応するカスタム ダッシュボードの横にある閉じる（**x**）アイコンをクリックすることで作成したダッシュボードを削除できます。

（注） デフォルト ダッシュボードの名前を変更したり、削除することはできません。

すべてのダッシュレットには右上にツールバーがあり、次のオプションが含まれています。

- [分離（Detach）]：別のウィンドウにダッシュレットを表示します。
- [更新（Refresh）]：ダッシュレットを更新します。
- [削除（Remove）]：ダッシュボードからダッシュレットを削除します。

ダッシュレットの左上隅にあるグリッパ アイコンを使用して、ダッシュレットをドラッグ アンド ドロップできます。

[アラーム（Alarms）] ダッシュレットのクイック フィルタ：[重大（Critical）]、[警告（Warning）]、[情報（Info）] などの重大度に基づいてアラームをフィルタリングできます。

[アラーム（Alarms）] ダッシュレットはホーム ページにあり、クイック フィルタ オプションがある [フィルタ（Filter）] ドロップダウン リストが含まれています。

Cisco ISE 国際化およびローカリゼーション

Cisco ISE 国際化では、サポートされる言語にユーザ インターフェイスを合わせます。ユーザ インターフェイスのローカリゼーションでは、ロケール固有のコンポーネントおよび翻訳されたテキストが組み込まれます。Windows、MAC OSX、および Android デバイスの場合、ネイティブ サプリカント プロビジョニング ウィザードは、次のサポートされている言語のいずれかで使用できます。

Cisco ISE の国際化およびローカリゼーションのサポートでは、ポータルに接するエンドユーザに対して UTF-8 符号化で英語以外のテキストをサポートすること、および管理者ポータルの選択的フィールドに重点を置いています。

サポートされる言語

Cisco ISE では、次の言語とブラウザ ロケールのローカリゼーションおよび国際化がサポートされます。

言語	ブラウザ ロケール
中国語（繁体字）	zh-tw
中国語（簡体字）	zh-cn
チェコ語	cs-cz
オランダ語	nl-nl
英語	en
フランス語	fr-fr
ドイツ語	de-de
ハンガリー語	hu-hu
イタリア語	it-it
日本語	ja-jp
韓国語	ko-kr
ポーランド語	pl-pl
ポルトガル語（ブラジル）	pt-br
ロシア語	ru-ru

言語	ブラウザ ロケール
スペイン語	es-es

エンドユーザ Web ポータルのローカリゼーション

ゲスト、スポンサー、デバイスおよびクライアントプロビジョニングの各ポータルは、サポートされているすべての言語およびロケールにローカライズされています。ローカライズには、テキスト ラベル、メッセージ、フィールド名およびボタン ラベルが含まれます。クライアント ブラウザが Cisco ISE テンプレートにマッピングされていないロケールを要求した場合、ポータルは英語のテンプレートを使用して内容を表示します。

管理者ポータルを使用して、各言語のゲスト、スポンサー、デバイスの各ポータルで使用されるフィールドを個別に変更できます。また、言語を追加することも可能です。現在、クライアントプロビジョニング ポータルについては、これらのフィールドはカスタマイズできません。

HTML ページを Cisco ISE にアップロードすることによって、ゲスト ポータルを詳細にカスタマイズできます。カスタマイズしたページをアップロードする場合は、展開に対する適切なローカリゼーション サポートに責任を負います。Cisco ISE では、サンプル HTML ページを含むローカリゼーション サポート例が提供されており、これをガイドとして使用できます。Cisco ISE には、国際化されたカスタム HTML ページをアップロード、格納、および表示する機能があります。

（注） NAC および MAC エージェントのインストーラおよび WebAgent ページはローカライズされていません。

UTF-8 文字データ エントリのサポート

エンドユーザに（Cisco クライアントエージェントまたはサプリカント、あるいはスポンサー、ゲスト、デバイス、クライアント プロビジョニングの各ポータルを介して）公開される Cisco ISE フィールドは、すべての言語の UTF-8 文字セットをサポートします。UTF-8 は、Unicode 文字セット用のマルチバイト文字エンコーディングであり、ヘブライ語、サンスクリット語、アラビア語など、多数の異なる言語文字セットがあります。

文字の値は、管理設定データベースに UTF-8 で格納され、UTF-8 文字はレポートおよびユーザ インターフェイス コンポーネントで正しく表示されます。

UTF-8 クレデンシャル認証

ネットワーク アクセス認証では、UTF-8 ユーザ名およびパスワードのクレデンシャルがサポートされます。これには、RADIUS、EAP、RADIUS プロキシ、RADIUS トークン、ゲストおよび管理ポータルのログイン認証からの Web 認証が含まれます。ユーザ名とパスワードの UTF-8 サポートは、ローカル ID ストアおよび外部 ID ストアに対する認証に適用されます。

UTF-8認証は、ネットワーク ログインに使用されるクライアント サプリカントに依存します。一部のWindowsネイティブ サプリカントでは、UTF-8クレデンシャルはサポートされません。

（注） RSA では UTF-8 ユーザはサポートされないため、RSA を使用した UTF-8 認証はサポートされません。同様に、Cisco ISE と互換性がある RSA サーバでも UTF-8 がサポートされません。

UTF-8 ポリシーおよびポスチャ評価

属性値に基づいて決定される Cisco ISE のポリシー ルールに、UTF-8 テキストが含まれている場合があります。UTF-8属性値はルール評価でサポートされます。また、管理ポータルでUTF-8の値を使用して条件を設定できます。

ポスチャ要件を、UTF-8 文字セットに基づくファイル、アプリケーション、およびサービス条件として変更できます。

サプリカントに送信されるメッセージの UTF-8 サポート

RSA プロンプトおよびメッセージは、RADIUS 属性 REPLY-MESSAGE を使用して、または EAP データ内で、サプリカントに転送されます。テキストに UTF-8 データが含まれている場合は、サプリカントによって、クライアントのローカル オペレーティング システムの言語サポートに基づいて表示されます。一部の Windows ネイティブ サプリカントでは、UTF-8 クレデンシャルはサポートされません。

Cisco ISE プロンプトおよびメッセージは、サプリカントが実行されているクライアントのオペレーティング システムのロケールと同期していない場合があります。エンドユーザのサプリカントのロケールを Cisco ISE によってサポートされている言語に合わせる必要があります。

レポートおよびアラートの UTF-8 サポート

モニタリングおよびトラブルシューティングのレポートおよびアラートでは、Cisco ISE でサポートされる言語について、次のように関連属性の UTF-8 の値がサポートされます。

- ライブ認証の表示
- レポート レコードの詳細ページの表示
- レポートのエクスポートと保存
- Cisco ISE ダッシュボードの表示
- アラート情報の表示
- tcpdump データの表示

ポータルでの UTF-8 文字のサポート

Cisco ISE フィールド（UTF-8）では、ポータルおよびエンドユーザ メッセージでローカリゼーション用に現在サポートされているよりも、多くの文字セットがサポートされます。たとえ

ば、Cisco ISE では、ヘブライ語やアラビア語などの右から左へ記述する言語はサポートされていません（文字セット自体はサポートされています）。

次の表に、データの入力および表示にUTF-8 文字をサポートする管理者ポータルおよびエンドユーザ ポータルのフィールドを示します。次の制限があります。

- Cisco ISE では、UTF-8 文字を使用したゲストのユーザ名とパスワードはサポートされません。
- Cisco ISE では、証明書で UTF-8 文字を使用することはできません。

表 *10 :* 管理者ポータルの *UTF-8* 文字フィールド

管理者ポータル要素	UTF-8 フィールド
ネットワーク アクセスのユーザ設定	• [ユーザ名（User name）] ユーザ名には、大文字と小文字、数字、スペース、特殊文字（`、%、^、;、:、[、{、|、}、]、\、‘、“、=、<、>、?、!、制御文字を除く）を自由に組み合わせて使用できます。スペースのみのユーザ名も許可されません。 • [名（First name）] • [姓（Last name）] • [電子メール（e-mail）]
ユーザ リスト	• すべてのフィルタ フィールド • [ユーザ リスト（User List）] ページに表示される値 • 左側のナビゲーション クイック ビューに表示される値

管理者ポータル要素	UTF-8 フィールド
ユーザ パスワード ポリシー	パスワードには、大文字と小文字、数字、特殊文字（「!」、「@」、「#」、「$」、「%」、「^」、「&」、「*」、「(」、「)」など）を自由に組み合わせて使用できます。[パスワード（Password）] フィールドでは、UTF-8 文字を含むあらゆる文字を使用できますが、制御文字は使用できません。 言語の中には大文字または小文字のアルファベットがないものがあります。ユーザパスワード ポリシーでユーザに大文字または小文字でパスワードを入力することを求め、ユーザの言語がこれらの文字をサポートしていない場合、ユーザはパスワードを設定できません。ユーザパスワードフィールドでUTF-8 文字をサポートするには、ユーザ パスワード ポリシー ページ（**[管理（Administration）] > [IDの管理（Identity Management）] > [設定（Settings）] > [ユーザ パスワード ポリシー（User Password Policy）]**）で次のオプションをオフにする必要があります。 • 小文字の英文字 • 大文字の英文字
管理者リスト	• すべてのフィルタ フィールド • [管理者リスト（Administrator List）] ページに表示される値 • 左側のナビゲーション クイック ビューに表示される値
管理者ログイン ページ	• [ユーザ名（User name）]
RSA	• メッセージ • プロンプト
RADIUS トークン	• [認証（Authentication）] タブ > [プロンプト（Prompt）]

管理者ポータル要素	UTF-8 フィールド
ポスチャ要件	• [名前（Name）] • [修復アクション（Remediation action）] > エージェント ユーザに表示されるメッセージ • 要件リスト表示
ポスチャ条件	• [ファイル条件（File condition）] > [ファイル パス（File path）] • [アプリケーション条件（Application condition）] > [プロセス名（Process name）] • [サービス条件（Service condition）] > [サービス名（Service name）] • 条件リスト表示
ゲストおよびデバイスの設定	• [スポンサー（Sponsor）] > [言語テンプレート（Language Template）] : サポートされているすべての言語、すべてのフィールド • [ゲスト（Guest）] > [言語テンプレート（Language Template）] : サポートされているすべての言語、すべてのフィールド • [デバイス（My Devices）] > [言語テンプレート（Language Template）] : サポートされているすべての言語、すべてのフィールド
システム設定	• [SMTP サーバ（SMTP Server）] > [デフォルトの電子メールアドレス（Default e-mail address）]
[操作（Operations）] > [アラーム（Alarms）] > [ルール（Rule）]	• [基準（Criteria）] > [ユーザ（User）] • [通知（Notification）] > [電子メール通知ユーザ リスト（e-mail Notification user list）]

管理者ポータル要素	UTF-8 フィールド
[操作（Operations）] > [レポート（Reports）]	• [操作（Operations）] > [ライブ認証（Live Authentications）] > [フィルタ（Filter）] フィールド • [操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] > [レポートフィルタ（Report filter）] フィールド
[操作（Operations）] > [トラブルシューティング（Troubleshoot）]	• [一般ツール（General Tools）] > [RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）] > [ユーザ名（Username）]
ポリシー	• [認証（Authentication）] > ポリシー条件内での av 式の値 • [許可（Authorization）]/[ポスチャ（Posture）]/[クライアント プロビジョニング（Client Provisioning）] > [その他の条件（Other Conditions）] > ポリシー条件内での av 式の値

管理者ポータル要素	UTF-8 フィールド
ポリシー ライブラリ条件の属性値	• [認証（Authentication）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > av 式の値 • [認証（Authentication）] > 単純条件リスト表示 • [認証（Authentication）] > 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [許可（Authorization）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > av 式の値 • [許可（Authorization）] > 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [ポスチャ（Posture）] > [ディクショナリ単純条件/ディクショナリ複合条件（Dictionary Simple Condition/Dictionary Compound Condition）] > av 式の値 • [ゲスト（Guest）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > av 式の値

ユーザ インターフェイス外での UTF-8 サポート

この項では、Cisco ISE ユーザ インターフェイス外で UTF-8 がサポートされる領域について説明します。

デバッグ ログおよび CLI 関連の UTF-8 サポート

一部のデバッグ ログには、属性値およびポスチャ条件の詳細が表示されます。そのため、すべてのデバッグ ログで UTF-8 の値が受け入れられます。raw UTF-8 データを含むデバッグ ログをダウンロードして、UTF-8 対応ビューアで表示できます。

ACS 移行の UTF-8 サポート

Cisco ISE では、ACS UTF-8 設定オブジェクトおよび値の移行が可能です。一部の UTF-8 オブジェクトの移行は、Cisco ISE UTF-8 言語でサポートされない場合があります。そのため、移行中に提供される UTF-8 データの一部は、管理ポータルまたはレポート方式を使用して読み取れない表示になる場合があります。（ACS から移行された）読み取り不可能な UTF-8 値は ASCII

テキストに変換する必要があります。ACS から ISE への移行についての詳細は、お使いの ISE バージョンの『Cisco Secure ACS to Cisco ISE Migration Tool』を参照してください。

UTF-8 の値のインポートおよびエクスポートのサポート

管理者ポータルおよびスポンサー ポータルは、ユーザ アカウントの詳細をインポートするときに使用される UTF-8 値のプレーン テキストおよび .csv ファイルをサポートします。エクスポートされたファイルは csv ファイルとして提供されます。

REST での UTF-8 サポート

UTF-8 の値は、外部 REST 通信でサポートされます。これは、admin 認証を除き、Cisco ISE ユーザ インターフェイスの UTF-8 がサポートされる設定可能項目に適用されます。REST での admin 認証には、ログインのために ASCII テキスト クレデンシャルが必要です。

ID ストアの許可データの UTF-8 サポート

Cisco ISE では、Active Directory および LDAP がポリシー処理のために許可ポリシーで UTF- 8 データを使用できます。

MAC アドレスの正規化

ISE は次のいずれかの形式で入力された MAC アドレスの正規化をサポートします。

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

次の ISE ウィンドウでは、完全または部分的な MAC アドレスを指定できます。

- [ポリシー（Policy）] > [ポリシー セット（Policy Sets）]
- [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）]
- [認証（Authentications）] > [フィルタ（Filters）]（エンドポイント カラムおよび ID カラム）
- [グローバル検索（Global Search）]
- [操作（Operations）] > [レポート（Reports）] > [レポート フィルタ（Reports Filters）]
- [操作（Operations）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [エンドポイントのデバッグ（Endpoint Debug）]

次の ISE ウィンドウでは、完全な MAC アドレスを指定する必要があります（「:」または「-」または「.」で区切られた 6 オクテット）。

- [操作（Operations）] > [エンドポイント保護サービス（Endpoint Protection Services）適応型ネットワーク制御（Adaptive Network Control）]
- [操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）]
- [操作（Operations）] > [トラブルシューティング（Troubleshooting）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ポスチャのトラブルシューティング（Posture Troubleshooting）]
- [管理（Administration）] > [ID（Identities）] > [エンドポイント（Endpoints）]
- [管理（Administration）] > [システム（System）] > [展開（Deployment）]
- [管理（Administration）] > [ロギング（Logging）] > [収集フィルタ（Collection Filter）]

REST API でも、完全な MAC アドレスの正規化がサポートされます。

有効なオクテットには 0 ～ 9、a ～ f、または A ～ F のみ含めることができます。

Cisco ISE 展開のアップグレード

Cisco ISE では、管理者ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードプロセスはさらに簡素化され、アップグレードの進行状況およびノードのステータスが画面に表示されます。アップグレード前およびアップグレード後のタスクのリストについては、『*Cisco Identity Services Engine Upgrade Guide*』を参照してください。

[アップグレードの概要（Upgrade Overview）]ページには、展開内のすべてのノード、そのノードで有効なペルソナ、インストールされている ISE のバージョン、およびノードのステータス（ノードがアクティブか非アクティブか）がリストされます。ノードがアクティブな状態である場合にのみアップグレードを開始できます。

管理者アクセス コンソール

次の手順では、管理ポータルにログインする方法について説明します。

ステップ 1 Cisco ISE URL をブラウザのアドレス バーに入力します（たとえば https://<ise hostname or ip address>/admin/）。

ステップ 2 ユーザ名と、Cisco ISE の初期セットアップで指定して設定した大文字と小文字が区別されるパスワードを入力します。

ステップ 3 [ログイン（Login）] をクリックするか、Enter を押します。

ログインに失敗した場合は、[ログイン（Login）]ページの[ログインで問題が発生する場合（Problem logging in?）] リンクをクリックして、手順に従ってください。

管理者ログイン ブラウザのサポート

Cisco ISE 管理者ポータルは次の HTTPS 対応ブラウザをサポートしています。

- Mozilla Firefox 72 以前のバージョン
- Mozilla Firefox ESR 60.9 以前のバージョン
- Google Chrome 80 以前のバージョン
- Microsoft Edge ベータ 77 以前のバージョン
- Microsoft Internet Explorer 10.*x* および 11.*x*

  Internet Explorer 10.x を使用する場合は、TLS 1.1 と TLS 1.2 をイネーブルにし、SSL 3.0 と TLS 1.0 をディセーブルにします（[インターネット オプション（Internet Options）] > [詳細設定（Advanced）]）。

ISE コミュニティ リソース

ISE Pages Fail to Fully Load When Adblock Plus is Used

ログインの試行に失敗した後の管理者のロックアウト

管理者ユーザ ID に対して誤ったパスワードを何度も入力すると、アカウントは指定された時間一時停止されるか、またはロックアウトされます（設定による）。ロックアウトすることを選択した場合は、管理者ポータルによってシステムの「ロックアウト」が表示されます。Cisco ISE は、サーバ管理者ログイン レポートにログ エントリを追加し、その管理者 ID のクレデンシャルを一時停止します。その管理者 ID のパスワードをリセットするには、『Cisco Identity Services Engine Installation Guide』の「Reset a Disabled Password Due to Administrator Lockout」のセクションでの説明に従います。管理者アカウントが無効になるまでに失敗できる回数は設定可能です。詳細は、『*Cisco Identity Services Engine Administrator Guide*』の「Cisco ISE への管理アクセス （18 ページ）」のセクションを参照してください。管理者ユーザ アカウントがロックアウトされると、そのように設定されている場合、Cisco ISE からその管理者ユーザに電子メールが送信されます。

無効になったシステム管理者のステータスは、Active Directory ユーザを含むすべてのスーパー管理者が有効にできます。

Cisco ISE でのプロキシ設定の指定

既存のネットワーク トポロジにおいて、外部リソース（たとえば、クライアント プロビジョニングやポスチャ関連のリソースが存在するリモート ダウンロード サイト）にアクセスするために、Cisco ISE に対してプロキシを使用することが要求されている場合は、管理者ポータルを使用してプロキシのプロパティを指定できます。

プロキシ設定は次の Cisco ISE 機能に影響します。

- パートナー モバイル管理
- エンドポイント プロファイラ フィード サービスの更新
- エンドポイント ポスチャの更新
- エンドポイント ポスチャ エージェント リソースのダウンロード
- CRL（証明書失効リスト）のダウンロード
- ゲスト通知
- SMS メッセージの送信
- [Social Login]

Cisco ISE プロキシ設定はプロキシ サーバの基本認証をサポートします。NT LAN Manager（NTLM）認証はサポートされていません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）]** を選択します。

ステップ 2 プロキシの IP アドレスまたは DNS 解決可能ホスト名を入力し、Cisco ISE との間のプロキシトラフィックを通過させるポートを [プロキシホストサーバ：ポート（Proxy host server : port）] で指定します。

ステップ 3 必要に応じて、[パスワード必須（Password required）] チェックボックスをオンにします。

ステップ 4 [ユーザ名（User Name）] および [パスワード（Password）] フィールドに、プロキシ サーバへの認証に使用するユーザ名とパスワードを入力します。

ステップ 5 [次のホストとドメインに対するプロキシをバイパス（Bypass proxy for these hosts and domain）] に、バイパスするホストまたはドメインの IP アドレスまたはアドレス範囲を入力します。

ステップ 6 [保存（Save）] をクリックします。

管理者ポータルで使用されるポート

管理者ポータルは HTTP ポート 80 および HTTPS ポート 443 を使用するように設定され、これらの設定は変更できません。Cisco ISE はまた、あらゆるエンドユーザ ポータルが同じポートを使用することを禁止して、管理者ポータルへのリスクを減らすようになっています。

外部 RESTful サービス API の有効化

外部 RESTful サービス API は HTTPS プロトコルおよび REST 方法論に基づいており、ポート 9060 を使用します。

外部 RESTful サービス API は、基本認証をサポートしています。認証クレデンシャルは、暗号化され、要求ヘッダーの一部となっています。

JAVA、curl Linux コマンド、Python などの REST クライアントやその他のクライアントを使用して、外部 RESTful サービス API コールを呼び出すことができます。

ISE 管理者は、外部 RESTful サービス API を使用して操作を実行するための特権をユーザに割り当てる必要があります。外部 RESTful サービス API（ゲスト API を除く）を使用して操作を実行するには、次の管理者グループのいずれかにユーザを割り当て、Cisco ISE の内部データベース（内部管理者ユーザ）に保存されているクレデンシャルに対して認証する必要があります。

- 外部 RESTful サービス管理者：すべての ERS API へのフル アクセス（GET、POST、DELETE、PUT）。このユーザは、ERS API 要求を作成、読み取り、更新、および削除できます。
- 外部 RESTful サービス オペレータ：読み取り専用アクセス（GET 要求のみ）。

（注） ネットワーク管理者ユーザは、すべての ERS API にアクセスできます。

外部 RESTful サービス API は、デフォルトではイネーブルになっていません。それらをイネーブルにする前に外部 RESTful サービス API コールを呼び出そうとすると、エラー応答を受信します。Cisco ISE REST API 用に開発されたアプリケーションから Cisco ISE にアクセスできるようにするには、Cisco ISE REST API をイネーブルにする必要があります。Cisco REST API は HTTPS ポート 9060 を使用します。このポートはデフォルトでは閉じられています。Cisco ISE REST API が Cisco ISE 管理用サーバでイネーブルになっていない場合、クライアント アプリケーションは、サーバから Guest REST API 要求に対するタイムアウト エラーを受信します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ERS 設定（ERS Settings）]** を選択します。

ステップ 2 プライマリ管理ノードの [読み取り/書き込み用に ERS をイネーブル化（Enable ERS for Read/Write）] を選択します。

ステップ 3 セカンダリ ノードがある場合は、[その他すべてのノードの読み取り用に ERS をイネーブル化（Enable ERS for Read for All Other Nodes）] を選択します。

すべてのタイプの外部 RESTful サービス要求はプライマリ ISE ノードに限り有効です。セカンダリ ノードは読み取りアクセス（GET 要求）に対応します。

ステップ 4 次のオプションのいずれかを選択します。

- [セキュリティ強化に CSRF チェックを使用（Use CSRF Check for Enhanced Security）]：このオプションを有効にすると、ERS クライアントは Cisco ISE から Cross-Site Request Forgery（CSRF）トークンを取得する GET 要求を送信し、Cisco ISE に送信される要求に CSRF トークンを含める必要があります。Cisco ISE は、ERS クライアントからの要求を受信すると、CSRF トークンを検証します。Cisco ISE は、トークンが有効な場合にのみ要求を処理します。このオプションは、ISE 2.3 以前のクライアントには適用されません。
- [ERS 要求に対して CSRF を無効にする（Disable CSRF for ERS Request）]：このオプションを有効にすると、CSRF 検証は実行されません。このオプションは、ISE 2.3 以前のクライアントに使用できます。

ステップ 5 [保存（**Save**）] をクリックします。

すべての REST 操作が監査され、ログがシステム ログに記録されます。外部 RESTful サービス API にはデバッグ ロギング カテゴリがあります。このカテゴリは、Cisco ISE GUI のデバッグ ログ ページからイネーブルにすることができます。

Cisco ISE で外部 RESTful サービスを無効にすると、ポート 9060 は開いたままになりますが、ポート経由の通信は許可されません。

関連トピック

外部 RESTful サービス SDK （132 ページ）

外部 RESTful サービス SDK

外部 RESTful サービス SDK を使用して、独自ツールの構築を開始できます。次の URL から外部 RESTful サービス SDK にアクセスできます。https://<ISE-ADMIN-NODE>:9060/ers/sdk 外部 RESTful サービス SDK には、外部 RESTful サービス管理ユーザのみがアクセスできます。

SDK は、次のコンポーネントで構成されています。

- クイック リファレンス API マニュアル
- すべての利用可能な API 操作の完全なリスト
- ダウンロード可能なスキーマ ファイル
- ダウンロード可能な Java のサンプル アプリケーション
- cURL スクリプト形式の使用例
- python スクリプト形式の使用例
- Chrome POSTMAN の使用方法

システム時刻と NTP サーバ設定の指定

Cisco ISE では、Network Time Protocol（NTP）サーバを 3 台まで設定することができます。NTP サーバを使用すると、正確な時刻を維持でき、複数のタイムゾーンの間で時刻を同期できます。また、認証済みの NTP サーバのみを Cisco ISE で使用するかどうかを指定することもでき、そのための認証キーを入力できます。

シスコは、すべての Cisco ISE ノードを協定世界時（UTC）の時間帯に設定することを推奨します（特に Cisco ISE ノードが分散展開されてインストールされている場合）。この手順では、展開内にあるさまざまなノードからのレポートとログのタイムスタンプが常に同期されます。

Cisco ISE は、NTP サーバの公開キー認証もサポートしています。NTPv4 は、対称キー暗号化を使用し、公開キー暗号化に基づく新しい Autokey 方式も提供します。公開キー暗号化は、一般に、各サーバによって生成され公開されない非公開の値に基づいているため、対称キー暗号化よりも安全であると考えられます。Autokey では、すべてのキー配布および管理機能には公開値のみが含まれているため、キーの配布と保管が大幅に簡素化されます。

コンフィギュレーション モードで Cisco ISE CLI から NTP サーバに Autokey を設定できます。IFF（identify Friend または Foe）識別方式は最も広く使用されている方式なので、この方式を使用することを推奨します。

始める前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

プライマリおよびセカンダリの両方の Cisco ISE ノードがある場合は、セカンダリ ノードのユーザ インターフェイスにログインし、展開内の各 Cisco ISE ノードのシステム時間と NTP サーバ設定を個別に設定する必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [システム時刻（System Time）]** を選択します。

ステップ 2 NTP サーバに一意の IP アドレス（IPv4/IPv6/FQDN）を入力します。

ステップ 3 システムおよびネットワーク時間の維持に認証済みの NTP サーバだけを使用するように Cisco ISE を制限する場合は、[認証済みの NTP サーバのみ可能（Only allow authenticated NTP servers）] チェックボックスをオンにします。

ステップ 4 （オプション）秘密キーを使用して NTP サーバを認証する場合に、指定したサーバのいずれかが認証キーによる認証を必要とする場合は、[NTP 認証キー（NTP Authentication Keys）] タブをクリックし、1 つ以上の認証キーを次のように指定します。

a) [追加（Add）] をクリックします。

b) 必要な [キー ID（Key ID）] と [キー値（Key Value）] を入力します。 [信頼できるキー（Trusted Key）] オプションをアクティブにするか、または非アクティブにすることによって、そのキーが信頼できるかどうかを指定し、[OK] をクリックします。[キー ID（Key ID）] フィールドは 1 ～ 65535 の数値をサポートし、[キー値（Key Value）] フィールドは最大 15 文字の英数字をサポートします。

c) NTP サーバの認証キーの入力が終了したら、[NTP サーバ設定（NTP Server Configuration）] タブに戻ります。

ステップ 5 （オプション）公開キー認証を使用して NTP サーバを認証する場合は、コマンドライン インターフェイス（CLI）から Cisco ISE で Autokey を設定します。詳細については、ご使用のリリースの ISE の『Cisco Identity Services Engine CLI Reference Guide』で **ntp server** および **crypto** コマンドを参照してください。

ステップ 6 [保存（**Save**）] をクリックします。

システムの時間帯の変更

一度設定すると、管理者ポータルからの時間帯の編集はできません。時間帯設定を変更するには、Cisco ISE CLI で次のコマンドを入力します。

clock timezone タイムゾーン

（注） Cisco ISE は、タイム ゾーン名と出力の省略形に POSIX スタイルの記号を使用します。そのため、グリニッジの西にあるゾーンはプラス記号を持ち、グリニッジの東にあるゾーンはマイナス記号を持ちます。たとえば、TZ='Etc/GMT+4' はグリニッジ標準時（UT）の 4 時間遅れに対応します。

注意 インストール後に Cisco ISE アプライアンスでタイム ゾーンを変更するには、ISE サービスをその特定のノードで再起動する必要があります。そのため、メンテナンス ウィンドウ内でこのような変更を行うことを推奨します。また、単一 ISE 展開内のすべてのノードが同じタイム ゾーンに設定されていることが重要です。複数の ISE ノードが異なる地理的な場所やタイム ゾーンにある場合は、すべての ISE ノードで UTC などのグローバルなタイム ゾーンを使用する必要があります。

clock timezone コマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

通知をサポートするための SMTP サーバの設定

アラームの電子メール通知を送信したり、スポンサーがゲストにログイン クレデンシャルやパスワードのリセット指示の電子メール通知を送信できるようにしたり、ゲストがアカウント登録に成功した後、自動的にログイン クレデンシャルを受信したり、ゲスト アカウントの期限が切れる前に実行するアクションを受信したりできるようにするには、Simple Mail Transfer Protocol（SMTP）サーバを設定します。

電子メールを送信する ISE ノード

次のリストは、電子メールを送信する分散 ISE 環境のノードを示しています。

電子メールの目的	電子メールを送信するノード
ゲストの有効期限	プライマリ PAN
アラーム	アクティブな MnT
ゲストとスポンサーのポータルからのスポンサーとゲストの通知	PSN
パスワードの有効期限	プライマリ PAN

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[SMTP サーバ（SMTP Server）]** を選択します。

ステップ 2 **[設定（Settings）]** > **[SMTPサーバ（SMTP Server）]** を選択します。

ステップ 3 [SMTPサーバ（SMTP Server）] フィールドにアウトバウンド SMTP サーバのホスト名を入力します。この SMTP ホスト サーバは Cisco ISE サーバからアクセス可能である必要があります。このフィールドの最大長は 60 文字です。

ステップ 4 次のオプションのいずれかを選択します。

- スポンサーの電子メールアドレスからゲスト通知メールを送信するには、[スポンサーの電子メールアドレスを使用（Use email address from Sponsor）] を選択して、[通知の有効化（Enable Notifications）] を選択します。
- すべてのゲスト通知の送信元となる電子メールアドレスを指定するには、[デフォルトの電子メールアドレスを使用（Use Default email address）] を選択して、それを [デフォルトの電子メールアドレス（Default email address）] フィールドに入力します。

ステップ 5 [保存（Save）] をクリックします。

アラーム通知の受信者は、[電子メールにシステムアラームを含む（Include system alarms in emails）] オプションが有効になっている内部管理者ユーザです。アラーム通知を送信する送信者の電子メール アドレスは、ise@<hostname> としてハード コードされています。

FIPS モードのサポート

ISE FIPS 140 モードでは、FIPS 140-2 モードに対して Cisco FIPS オブジェクト モジュールの暗号化モジュールを初期化します。Cisco Identity Services Engine には、FIPS 140-2 の検証済み暗号化モジュールが組み込まれています。FIPS コンプライアンスの要求の詳細については、『FIPS Compliance Letter』を参照してください。

FIPS モードを有効にすると、Cisco ISE 管理者インターフェイスのページの右上隅のノード名の左側に FIPS モード アイコンが表示されます。

Cisco ISE は、FIPS 140-2 標準でサポートされないプロトコルまたは証明書の使用を検出すると、準拠していないプロトコルまたは証明書の名前とともに警告を表示し、FIPSモードは有効になりません。必ず FIPS に準拠したプロトコルのみを選択し、FIPS モードを有効にする前に FIPS に非準拠の証明書を交換してください。

FIPS 標準では特定のアルゴリズムの使用について制限が設けられています。Cisco ISE による FIPS 140-2 準拠の有効化の手段として、RADIUS の共有秘密とキー管理が使用されます。FIPS モードが有効になると、FIPS 非準拠アルゴリズムを使用する機能はすべて失敗します。

Cisco ISE にインストールされている証明書で使用されている暗号化方式が FIPS でサポートされていない場合には、証明書を再発行する必要があります。

FIPS モードを有効にすると、次の機能が影響を受けます。

- IEEE 802.1X 環境
  - EAP-Flexible Authentication via Secure Tunneling（EAP-FAST）
  - EAP-Transport Layer Security（EAP-TLS）
  - PEAP
  - RADIUS
- Lightweight Directory Access Protocol（LDAP）over Secure Sockets Layer（SSL）
- Cisco ISE による FIPS 140-2 準拠の有効化の手段として、RADIUS の共有秘密とキー管理が使用されます。FIPS モードが有効になると、FIPS 非準拠アルゴリズムを使用する機能はすべて失敗します。

FIPS モードを有効にすると、展開内のすべてのノードが自動的に再起動されます。Cisco ISE はローリング再起動を実行します。具体的には、最初にプライマリ PAN を再起動し、その後でセカンダリ ノードを 1 つずつ再起動します。そのため、設定を変更する前にダウンタイムを計画することをお勧めします。

ヒント　データベース移行プロセスを行う場合は、移行が完了してから FIPS モードを有効にすることを推奨します。

Cisco ISE での FIPS モードの有効化

FIPS モードを有効にする場合：

ステップ 1　**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[FIPSモード（FIPS Mode）]** の順に選択します。

ステップ 2　[FIPSモード（FIPS Mode）] ドロップダウン リストで [有効（Enabled）] オプションを選択します。

ステップ 3 [保存（Save）] をクリックして、マシンを再起動します。

次のタスク

FIPS モードを有効にしたら、次の FIPS 140-2 準拠機能を有効にして設定します。

- 自己署名証明書の生成 （162 ページ）
- 証明書署名要求の作成と認証局への CSR の送信 （185 ページ）
- 『』の「ネットワーク デバイス定義の設定」のセクションを参照してください。
- ネットワーク デバイス定義の設定 （1429 ページ）で RADIUS 認証を設定します。

また、Common Access Card（CAC）機能を使用して管理者アカウントの許可を有効にすることもできます。許可のために CAC 機能を使用することは、厳密には FIPS 140-2 の要件ではありませんが、セキュア アクセスの手法としてよく知られており、多くの環境で FIPS 140-2 準拠を強化するために使用されています。

管理者 CAC 認証のための Cisco ISE の設定

始める前に

設定を始める前に、次の手順を実行してください。

- （任意）FIPS モードを有効にします。FIPS モードは証明書ベースの認証には必要ありませんが、この 2 つのセキュリティ手段は多くの場合、組み合わせて使用されます。Cisco ISE を FIPS 140-2 準拠の環境に展開する予定があり、CAC 証明書ベース許可も使用する場合は、必ず FIPS モードを有効にするとともに、適切な秘密キーと暗号化/復号化設定を最初に指定してください。
- Cisco ISE のドメイン ネーム サーバ（DNS）が Active Directory に設定されていることを確認します。
- Active Directory のユーザとユーザ グループ メンバーシップが、管理者証明書ごとに定義されていることを確認します。

Cisco ISE による管理者の認証と許可を、ブラウザから送信された CAC ベースのクライアント証明書に基づいて実行できるようにするには、次の設定が完了していることを確認してください。

- 外部 ID ソース（次の例では Active Directory）
- 管理者が属する Active Directory のユーザ グループ
- ユーザのアイデンティティを証明書の中で見つける方法
- Active Directory ユーザ グループから Cisco ISE RBAC 権限へのマッピング
- クライアント証明書に署名する認証局（信頼）証明書

- クライアント証明書がすでに CA によって失効させられたかどうかを判断する方法

Cisco ISE にログインする場合、クレデンシャルを認証するために Common Access Card（CAC）を使用できます。

ステップ 1 FIPS モードを有効にします。FIPS モードを有効にすると、システムを再起動するように促されます。CA 証明書もインポートする場合は、再起動を遅らせることができます。

ステップ 2 Cisco ISE の Active Directory ID ソースを設定し、Active Directory にすべての Cisco ISE ノードを追加します。

ステップ 3 ガイドラインに従って証明書認証プロファイルを設定します。

[プリンシパル名 X.509 属性（Principal Name X.509 Attribute）] フィールドでは、証明書内で管理者ユーザ名が格納されている属性を選択します。（CAC カードの場合は、カード上の署名証明書が通常は Active Directory でのユーザの検索に使用されます。プリンシパル名は、この証明書の「サブジェクトの別名（Subject Alternative Name）」拡張情報の中にあります。具体的には、この拡張情報の「別の名前（Other Name）」というフィールドです。したがって、ここで選択する属性は「Subject Alternative Name - Other Name」となります。）

ユーザの AD レコードにユーザの証明書が格納されている場合に、ブラウザから受信した証明書を AD の証明書と比較するには、[証明書のバイナリ比較（Binary Certificate Comparison）] チェックボックスをオンにして、以前に指定した Active Directory インスタンス名を選択します。

ステップ 4 パスワードベースの admin 認証用の Active Directory を有効にします。Cisco ISE に接続し結合された Active Directory インスタンス名を選択します。

（注） その他の設定が完了するまでは、パスワードベースの認証を使用します。この手順の最後に、認証タイプをクライアント証明書ベースに変更できます。

ステップ 5 外部管理者グループを作成して、Active Directory グループにマッピングします。**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[管理者（Administrators）]** > **[管理グループ（Admin Groups）]** を選択します。外部システム管理者グループを作成します。

ステップ 6 外部管理グループに RBAC 権限を割り当てる管理者許可ポリシーを設定します。

注意 外部スーパー管理者グループを作成して Active Directory グループにマッピングし、スーパー管理者権限を持つ管理者許可ポリシー（メニュー アクセスおよびデータ アクセス）を設定し、Active Directory グループに少なくとも 1 人のユーザを作成することを強く推奨します。このマッピングにより、クライアント証明書ベースの認証が有効になると、少なくとも 1 人の外部管理者がスーパー管理者権限を持つことが保証されます。これができないと、Cisco ISE 管理者が管理者ポータルの重要な機能から締め出される状況になる可能性があります。

ステップ 7 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書ストア（Certificate Store）]** を選択して、認証局証明書を Cisco ISE 証明書信頼ストアにインポートします。

Cisco ISE がクライアント証明書を受け入れるには、そのクライアント証明書の信頼チェーンの CA 証明書が Cisco ISE 証明書ストアの中にあることが条件となります。Cisco ISE 証明書ストアには適切な CA 証明書をインポートする必要があります。

a) [参照（Browse）] をクリックして証明書を選択します。
b) [クライアント認証を信頼（Trust for client authentication）] チェックボックスをオンにします。
c) [送信（Submit）] をクリックします。

Cisco ISE は、証明書をインポートしたら展開内のすべてのノードを再起動することを促します。すべての証明書をインポートするまで、再起動を遅らせることができます。ただし、すべての証明書をインポートしたら、次に進む前に Cisco ISE を再起動する必要があります。

ステップ 8 失効ステータス確認のための認証局証明書を設定します。

a) **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [OSCP サービス（OSCP Services）]** を選択します。
b) OSCP サーバの名前、説明（任意）、サーバの URL を入力します。
c) **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書ストア（Certificate Store）]** を選択します。
d) クライアント証明書に署名できる CA 証明書のそれぞれについて、その CA の失効ステータス チェックを行う方法を指定する必要があります。リストから CA 証明書を選択して [編集（Edit）] をクリックします。編集ページで、OCSP または CRL 検証の一方あるいは両方を選択します。OCSP を選択した場合は、CA に使用する OCSP サービスを選択します。CRL を選択した場合は、CRL Distribution URL などの設定パラメータを指定します。

ステップ 9 クライアント証明書ベースの認証を有効にします。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]** を選択します。

a) [認証方式（Authentication Method）] タブの [クライアント証明書ベース（Client Certificate Based）] 認証タイプを選択します。
b) 設定済みの証明書認証プロファイルを選択します。
c) Active Directory のインスタンス名を選択します。
d) [保存（Save）] をクリックします。

ここで、パスワード ベースの認証からクライアント証明書ベースの認証に切り替えます。設定済みの証明書認証プロファイルにより、管理者による証明書の認証方法を指定します。管理者は外部 ID ソースを使用して許可されます。この例では、Active Directory です。

Active Directory での管理者の検索には、証明書認証プロファイルからのプリンシパル名属性が使用されます。

Cisco ISE は、管理者 CAC 認証に設定されています。

サポートされる Common Access Card 標準

Cisco ISE は、Common Access Card（CAC）認証デバイスを使用して自身を認証する米国政府ユーザをサポートします。CAC は特定の従業員を識別する一連の X.509 クライアント証明書を含む電子チップの認識票です。CAC によるアクセスには、カードを挿入し PIN を入力するカードリーダーが必要です。カードからの証明書が Windows の証明書ストアに転送されます。Windows の証明書ストアは、Cisco ISE などのローカル ブラウザで実行されているアプリケーションで使用可能です。

Windows Internet Explorer バージョン 8 または 9 を Windows 7 オペレーティング システムで使用している場合は、ActiveIdentity の ActivClient バージョン 6.2.0.133 をインストールする必要があります。このミドルウェアは、Cisco ISE を CAC とともに相互運用するためのサードパーティ製品です。ActiveIdentity セキュリティ クライアント製品の詳細については、ActivID ActivClient Security Software Datasheet を参照してください。

Cisco ISE での共通アクセス カードの動作

管理者ポータルは、クライアント証明書を使用してのみ Cisco ISE との認証が許可されるように設定できます。ユーザ ID とパスワードなどのクレデンシャル ベースの認証はできません。クライアント証明書認証では、共通アクセス カード（CAC）カードを挿入して PIN を入力してから、ブラウザのアドレス フィールドに Cisco ISE 管理者ポータルの URL を入力します。ブラウザによって証明書が Cisco ISE に転送され、Cisco ISE はログイン セッションを証明書の内容に基づいて認証および許可します。このプロセスが完了すると、[Cisco ISE モニタリングおよびトラブルシューティング（Cisco ISE Monitoring and Troubleshooting）] ホーム ページに表示され、適切な RBAC 権限が与えられます。

Diffie-Hellman アルゴリズムを使用した SSH キー交換の保護

Diffie-Hellman-Group14-SHA1 SSH キー交換しか許可しないように Cisco ISE を設定することができます。このためには、Cisco ISE コマンドライン インターフェイス（CLI）のコンフィギュレーション モードから次のコマンドを入力します。

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

次に例を示します。

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

セキュア syslog 送信のための Cisco ISE の設定

Cisco ISE ノード間で、およびモニタリング ノードに対して、TLS 保護されたセキュア syslog のみを送信するように Cisco ISE を設定するには、次の手順を実行します。

始める前に

- 展開内のすべての Cisco ISE ノードに適切なサーバ証明書が設定されていることを確認します。 FIPS 140-2 準拠にセットアップする場合は、証明書キーは 2,048 ビット以上のキーサイズが必要です。
- 管理者ポータルの FIPS モードを有効にします。

- デフォルト ネットワーク アクセス認証ポリシーが、あらゆるバージョンの SSL プロトコルを許可しないことを確認します。FIPS 認定アルゴリズムとともに、FIPS モードで TLS プロトコルを使用します。
- 展開内のすべてのノードがプライマリ PAN に登録されていることを確認します。また、展開の少なくとも 1 つのノードに、セキュア syslog レシーバ（TLS サーバ）としての動作が有効になっているモニタリング ペルソナが含まれることも確認します。

ステップ 1 セキュア syslog リモート ロギング ターゲットを設定します。

ステップ 2 セキュア syslog リモート ロギング ターゲットに監査可能なイベントを送信するロギング カテゴリを有効にします。

ステップ 3 TCP syslog および UDP syslog コレクタを無効にします。TLS 保護された syslog コレクタのみを有効にします。

セキュア syslog リモート ロギング ターゲットの設定

Cisco ISE システム ログは、さまざまな目的のために、ログ コレクタによって収集され保存されます。セキュア syslog ターゲットを設定するためには、ログ コレクタとして Cisco ISE モニタリング ノードを選択する必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 **[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[リモート ロギング ターゲット（Remote Logging Targets）]** を選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 セキュア syslog サーバの名前を入力します。

ステップ 5 [ターゲット タイプ（Target Type）] ドロップダウン リストからセキュア syslog を選択します。

ステップ 6 [ステータス（Status）] ドロップダウン リストで [有効化（Enabled）] を選択します。

ステップ 7 展開の Cisco ISE モニタリング ノードの IP アドレスを入力します。

ステップ 8 ポート番号として 6514 を入力します。セキュア syslog レシーバは TCP ポート 6514 をリッスンします。

ステップ 9 syslog ファシリティ コードを選択します。デフォルトは LOCAL6 です。

ステップ 10 [サーバ ダウンの場合はバッファ メッセージ（Buffer Messages When Server is Down）] チェックボックスをオンにします。このオプションがオンの場合、Cisco ISE は、セキュア syslog レシーバが到達不能な場合にはログを格納し、セキュア syslog レシーバを定期的に検査し、セキュア syslog レシーバが起動すると転送します。

a) バッファ サイズを入力します。

b) 定期的にセキュア syslog レシーバを検査するように、Cisco ISE の再接続タイムアウトを秒単位で入力します。

ステップ 11 Cisco ISE がセキュア syslog サーバに提示する CA 証明書を選択します。

ステップ 12 [サーバ証明書有効性を無視（Ignore Server Certificate validation）] チェックボックスをオフにします。このオプションをオンにしてはいけません。

ステップ 13 [送信（Submit）] をクリックします。

リモート ロギング ターゲットの設定

次の表では、外部の場所（syslogサーバ）を作成してロギングメッセージを保存するために使用できる [リモート ロギング ターゲット（Remote Logging Targets）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** です。

表 *11* : リモート ロギング ターゲットの設定

フィールド	使用上のガイドライン
名前（Name）	新しいターゲットの名前を入力します。
ターゲット タイプ（Target Type）	ターゲット タイプを選択します。デフォルトでは、[UDP Syslog] に設定されます。
説明	新しいターゲットの簡単な説明を入力します。
[IPアドレス（IP Address）]	ログを格納する宛先マシンの IP アドレスまたはホスト名を入力します。
[ポート（Port）]	宛先マシンのポート番号を入力します。
ファシリティ コード（Facility Code）	ロギングに使用する syslog ファシリティ コードを選択します。有効なオプションは、Local0 ～ Local7 です。
最大長（Maximum Length）	リモートログターゲットメッセージの最大長を入力します。有効なオプションは200～1024バイトです。
サーバダウン時のバッファ メッセージ（Buffer Message When Server Down）	TCP syslog ターゲットおよびセキュア syslog ターゲットが使用できないときに Cisco ISE に syslog メッセージをバッファするには、このチェックボックスをオンにします。ISEは、接続が再開されるとターゲットへのメッセージの送信を再試行します。接続が再開された後、メッセージは古いものから順に送信され、バッファ内のメッセージは常に新しいメッセージの前に送信されます。バッファがいっぱいになると、古いメッセージが廃棄されます。

フィールド	使用上のガイドライン
バッファ サイズ（MB）（Buffer Size (MB)）	各ターゲットのバッファ サイズを設定します。デフォルトでは、100 MB に設定されます。バッファ サイズを変更するとバッファがクリアされ、特定のターゲットのバッファリングされた既存のすべてのメッセージが失われます。
再接続タイムアウト（秒）（Reconnect Timeout (Sec)）	サーバがダウンしている場合に TCP およびセキュア syslog を廃棄する前に保持する期間を秒単位で指定します。
CA 証明書の選択（Select CA Certificate）	クライアント証明書を選択します。
サーバ証明書有効性を無視（Ignore Server Certificate validation）	ISE でサーバ証明書認証が無視されるようにして、syslog サーバを許可するには、このチェックボックスをオンにします。デフォルトでは、このオプションが無効になっているときにシステムが FIPS モードでない限り、このオプションはオフに設定されます。

関連トピック

Cisco ISE ロギング メカニズム （291 ページ）
Cisco ISE システム ログ （292 ページ）
リモート syslog メッセージの形式
Cisco ISE メッセージ カタログ （295 ページ）
収集フィルタ （298 ページ）
イベント抑制バイパス フィルタ （298 ページ）
リモート syslog 収集場所の設定 （293 ページ）
収集フィルタの設定 （298 ページ）

セキュア syslog ターゲットに監査可能なイベントを送信するためのロギング カテゴリの有効化

Cisco ISE によってセキュア syslog ターゲットに監査可能なイベントが送信されるようにするには、ロギング カテゴリを有効にする必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択します。

ステップ 3 [管理および運用の監査（Administrative and Operational Audit）] ロギングカテゴリの横にあるオプション ボタンをクリックし、次に [編集（Edit）] をクリックします。

ステップ 4 [ログ重大度レベル（Log Severity Level）] ドロップダウンリストから [警告（WARN）] を選択します。

ステップ 5 [ターゲット（Targets）] フィールドで、以前に作成したセキュアな syslog リモート ロギング ターゲットを、[選択済み（Selected）] ボックスに移動します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 次のロギング カテゴリを有効にする場合は、この手順を繰り返し行います。

- [AAA 監査（AAA Audit）]

  [情報（INFO）] はこのカテゴリのデフォルトのログ重大度レベルであり、編集できないことに注意してください。

- [ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）]

ロギング カテゴリの設定

次の表では、[ロギング カテゴリ（Logging Categories）] ページのフィールドについて説明します。これらのフィールドを使用して、ログの重大度レベルを設定し、選択したカテゴリのログが保存されるロギング ターゲットを選択できます。このページへのナビゲーション パスは、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）] です。

表 *12 :* ロギング カテゴリの設定

フィールド	使用上のガイドライン
名前（Name）	ロギング カテゴリの名前を表示します。

フィールド	使用上のガイドライン
ログの重大度レベル（Log Severity Level）	次のオプションから、診断ロギング カテゴリの重大度レベルを選択できます。 • [重大（FATAL）]：緊急事態。 このオプションは、Cisco ISE が使用できないため、緊急措置が必要であることを意味します • [エラー（ERROR）]：このオプションは深刻な状態またはエラー状態を示します。 • [警告（WARN）]：このオプションは、通常の状態ではあるが重大な状態を示します。 これがデフォルトの条件です。 • [情報（INFO）]：このオプションは、情報メッセージを示します。 • [デバッグ（DEBUG）]：このオプションは、診断バグ メッセージを示します。
ローカル ロギング（Local Logging）	ローカル ノードで上のこのカテゴリのロギング イベントを有効にするには、このチェックボックスをオンにします。
ターゲット（Target）	左アイコンと右アイコンを使用して[使用可能（Available）]と [選択済み（Selected）]のボックス間でターゲットを移動することによって、カテゴリのターゲットを変更できます。[使用可能（Available）]ボックスには、論理（事前定義済み）と外部（ユーザ定義）という両方の既存のロギング ターゲットが含まれています。最初は空の[選択済み（Selected）]ボックスには、特定のカテゴリの選択済みターゲットが含まれます。

関連トピック

リモート syslog メッセージの形式

Cisco ISE メッセージ コード （294 ページ）

リモート syslog 収集場所の設定 （293 ページ）

メッセージ コードの重大度レベルの設定 （294 ページ）

TCP syslog および UDP syslog コレクタの無効化

Cisco ISE が ISE ノード間でセキュアな syslog のみを送信するには、TCP および UDP syslog コレクタを無効にして、セキュアな syslog コレクタのみを有効にする必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** を選択します。

ステップ 3 TCP または UDP syslog コレクタの横にあるオプション ボタンをクリックします。

ステップ 4 [編集（Edit）] をクリックします。

ステップ 5 [ステータス（Status）] ドロップダウン リストから [無効化（Disabled）] を選択します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 すべての TCP または UDP syslog コレクタが無効になるまで、このプロセスを繰り返します。

デフォルトのセキュア syslog コレクタ

Cisco ISE には、MnT ノード用のデフォルトのセキュア syslog コレクタがあります。デフォルトでは、これらのデフォルト セキュア syslog コレクタにはロギング カテゴリはマッピングされません。デフォルト セキュア syslog コレクタの名前は次のとおりです。

- プライマリ MnT ノード：SecureSyslogCollector
- セカンダリ MnT ノード：SecureSyslogCollector2

[リモート ロギング ターゲット（Remote Logging Targets）] ページ（[管理（Administration）] > [システム（System）] > [ロギング（Logging）]）でこの情報を確認できます。デフォルトの syslog コレクタは削除できません。また、デフォルト syslog コレクタの [名前（Name）]、[ターゲット タイプ（Target Type）]、[IP/ホスト アドレス（IP/Host address）]、および [ポート（Port）] フィールドは更新できません。

Cisco ISE の新規インストール中に、システムから「デフォルトの自己署名サーバ証明書（Default Self-signed Server Certificate）」が信頼ストアに追加され、「クライアン認証および syslog 用の信頼（Trust for Client authentication and Syslog）」目的で使用されるものとしてマークされます。これにより、この証明書はセキュア syslog に使用できるようになります。展開を設定する場合または証明書を更新する場合には、関連する証明書をセキュア syslog ターゲットに割り当てる必要があります。

アップグレード中に、ポート 6514 で MnT ノードを指し示している既存のセキュア syslog ターゲットがある場合、同じ名前と設定が維持されますが、アップグレード完了後にこれらの syslog ターゲットを削除すること、および [名前（Name）]、[ターゲット タイプ（Target Type）]、[IP/ホスト アドレス（IP/Host address）]、および [ポート（Port）] フィールドを編集することはできません。アップグレードの時点でこのようなターゲットが存在しない場合、新規インストールの場合と同様にデフォルト セキュア syslog ターゲットが作成されますが、証明書のマッ

ピングは行われません。これらの syslog ターゲットに関連証明書を割り当てることができます。どの証明書にもマッピングされていないセキュア syslog ターゲットをロギング カテゴリにマッピングしようとすると、次のメッセージが表示されます。

log_target_name □□□□□□□□□□□□□□□□Please configure the certificate for log_target_name□

オフライン メンテナンス

メンテナンス時間が 1 時間未満の場合、ISE ノードをオフラインにしてメンテナンス作業を行います。ノードをオンラインに戻すと、メンテナンス時間内に行われたすべての変更が PAN により自動的に同期されます。変更が自動的に同期されない場合は、PAN を使用して手動で同期できます。

メンテナンス時間が 1 時間を超える場合は、メンテナンスの時点でノードを登録解除し、ノードを展開に再び追加するときにノードを再登録します。

処理があまり行われていない時間帯にメンテナンスをスケジュールすることが推奨されます。

（注）

1. キューに格納されているメッセージの数が 1,000,000 を超える場合、または ISE ノードが 6 時間を超えてオフラインになっている場合には、データの複製の問題が発生している可能性があります。
2. プライマリ MnT ノードでメンテナンスを行う予定の場合は、メンテナンス アクティビティを実行する前に、MnT ノードの操作バックアップを作成しておくことを推奨します。

Cisco ISE での証明書の管理

証明書は、個人、サーバ、会社、またはその他のエンティティを識別し、そのエンティティを公開キーに関連付ける電子文書です。自己署名証明書は、独自の作成者によって署名されます。証明書は、自己署名したり、外部の認証局（CA）がデジタルで署名したりできます。CA 署名付きデジタル証明書は、業界標準であり、よりセキュアです。

証明書は、ネットワークに対するセキュアなアクセスを提供するために使用されます。Cisco ISE は、ノード間通信、および syslog サーバ、フィード サーバ、すべてのエンドユーザ ポータル（ゲスト、スポンサーおよびパーソナル デバイス ポータル）などの外部サーバとの通信に証明書を使用します。証明書は、エンドポイントに対して Cisco ISE ノードを識別し、そのエンドポイントと Cisco ISE ノード間の通信を保護します。

展開内のすべてのノードの証明書を管理するには、管理者ポータルを使用できます。

Cisco ISE によるセキュアなアクセスの提供を可能にする証明書

Cisco Identity Services Engine（ISE）は、公開キー インフラストラクチャ（PKI）に依存して、エンドポイントおよび管理者の両方とのセキュアな通信、そしてマルチノード展開内の複数の Cisco ISE ノード間のセキュアな通信を実現しています。PKI は X.509 デジタル証明書に依存して、メッセージの暗号化と復号化のための公開キーの転送、およびユーザとデバイスを表す他の証明書の信頼性の検証を行います。Cisco ISE には、次の 2 つの X.509 証明書のカテゴリを管理する、管理者ポータルが用意されています。

- システム証明書：これらはクライアント アプリケーションに対して Cisco ISE ノードを識別するサーバ証明書です。各 Cisco ISE ノードには独自のシステム証明書があり、それぞれの証明書は対応する秘密キーとともにノードに格納されています。
- 信頼できる証明書：この証明書は、ユーザおよびデバイスから受信した公開キーの信頼を確立するために使用される認証局（CA）証明書です。信頼できる証明書ストアには、Simple Certificate Enrollment Protocol（SCEP）から配信された証明書も含まれます。これにより、モバイルデバイスを企業ネットワークに登録できるようになります。信頼できる証明書ストア内の証明書はプライマリ管理ノード（PAN）で管理され、Cisco ISE 展開内の他のすべてのノードに自動的に複製されます。

分散展開では、証明書を PAN の証明書信頼リスト（CTL）のみにインポートする必要があります。この証明書はセカンダリ ノードに複製されます。

一般に、Cisco ISE での証明書認証が、証明書による認証機能のわずかな違いの影響を受けないようにするために、ネットワークに展開されているすべての Cisco ISE ノードには小文字のホスト名を使用してください。

証明書の使用

Cisco ISE に証明書を追加またはインポートする場合、証明書の使用目的を指定する必要があります。

- 管理者：ノード間通信および管理者ポータルの認証
- EAP：TLS ベースの EAP 認証
- RADIUS DTLS： RADIUS DTLS サーバ認証用
- ポータル：すべての Cisco ISE エンドユーザ ポータルとの通信
- xGrid：pxGrid コントローラとの通信

管理者ポータル（管理者）、pxGrid コントローラ（xGrid）との通信および TLS ベースの EAP 認証（EAP）に、各ノードから異なる証明書を関連付けることができます。ただし、これらの各目的に各ノードから関連付けることができる証明書は 1 つのみです。

Web ポータル要求を処理できる展開に複数のポリシー サービス ノード（PSN）がある場合、Cisco ISE には一意の ID が必要です。この ID で、ポータルの通信に使用する必要がある証明書を識別します。ポータルでの使用に指定された証明書を追加またはインポートする場合、証

明書グループ タグを定義して、それを展開内の各ノードの対応する証明書に関連付ける必要があります。この証明書グループ タグを対応するエンドユーザ ポータル（ゲスト、スポンサー、およびパーソナル デバイス ポータル）に関連付ける必要があります。この証明書グループ タグは一意の ID で、Cisco ISE が各ポータルと通信する際に使用する必要がある証明書を識別する場合に役立ちます。ポータルごとに各ノードから 1 つの証明書を指定できます。

（注） EAP-TLS クライアント証明書では、以下の暗号に対し、KeyUsage=Key Agreement および ExtendedKeyUsage=Client Authentication が必要です。

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS クライアント証明書では、以下の暗号に対し、KeyUsage=Key Encipherment および ExtendedKeyUsage=Client Authentication が必要です。

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

Cisco ISE の証明書の一致

展開内で Cisco ISE ノードをセットアップすると、2 つのノードが相互に通信します。システムは各 ISE ノードの FQDN を調べ、FQDN が一致することを確認します（たとえば ise1.cisco.com と ise2.cisco.com、またはワイルドカード証明書を使用している場合は *.cisco.com）。また、外部マシンから ISE サーバに証明書が提示される場合、認証のために提示される外部証明書が、ISE サーバの証明書と照合されます。2 つの証明書が一致すると、認証は成功します。

では、 ノード間（2 ノードの場合）、または と pxGrid の間で照合が実行されます。

Cisco ISE は、サブジェクト名の一致を次のようにして確認します。

1. Cisco ISE により証明書のサブジェクト代替名（SAN）の拡張が確認されます。SAN に 1 つ以上の DNS 名が含まれている場合は、それらの DNS 名の 1 つが Cisco ISE ノードの FQDN に一致している必要があります。ワイルドカード証明書が使用されている場合、ワイルドカード ドメイン名は Cisco ISE ノードの FQDN ドメインに一致している必要があります。
2. SAN に DNS 名が存在しない場合、または SAN 全体が欠落している場合は、証明書の [サブジェクト（Subject）] フィールドの一般名（CN）または証明書の [サブジェクト（Subject）] フィールドのワイルドカード ドメインが、ノードの FQDN に一致している必要があります。
3. 一致しない場合、証明書は拒否されます。

（注） Cisco ISE にインポートされる X.509 証明書は、Privacy Enhanced Mail（PEM）または Distinguished Encoding Rules（DER）形式である必要があります。証明書チェーン（システム証明書、およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。

X.509 証明書の有効性

X.509 証明書が有効なのは、指定された特定の日付までのみです。システム証明書が期限切れになった場合、その証明書に依存する Cisco ISE 機能が影響を受けます。Cisco ISE は、有効期限が 90 日以内になると、システム証明書の有効期間の残りについて通知します。この通知は、いくつかの方法で表示されます。

- 配色された有効期限の状態アイコンが、[システム証明書（System Certificates）] ページに表示されます。
- 期限切れメッセージが Cisco ISE システム診断レポートに表示されます。
- 有効期限のアラームは、有効期限の 90 日前、60 日前に生成され、有効期限前の最後の 30 日間には毎日生成されます。

失効した証明書が自己署名証明書の場合は、この証明書を編集して有効期限を延長できます。CA 署名付き証明書の場合は、CA から新しい証明書を取得するのに十分な期間を確保する必要があります。

Cisco ISE での PKI の有効化

公開キーインフラストラクチャ（PKI）は、セキュアな通信を可能にし、デジタル署名を使用してユーザの ID を確認する暗号化技術です。

ステップ 1 EAP-TLS などの TLS 対応認証プロトコル、管理者ポータルの認証、Cisco ISE Web ポータルにアクセスするブラウザおよび REST クライアント、および pxGrid コントローラ向けのシステム証明書を各展開ノードで確立します。

デフォルトで、Cisco ISE ノードには EAP 認証、管理者用ポータル、ポータル、pxGrid コントローラに使用される自己署名証明書があらかじめインストールされています。一般的な企業環境では、この証明書は、信頼された CA によって署名されたサーバ証明書に置き換えられます。

ステップ 2 信頼できる証明書ストアに、ユーザとの信頼を確立するために必要な CA 証明書と、Cisco ISE に提示されるデバイス証明書を配置します。

ルート CA 証明書と 1 つ以上の中間 CA 証明書で構成されている証明書チェーンでユーザまたはデバイス証明書の信頼性を確認するには、次の手順を実行します。

- ルート CA の [信頼性（Trust）] オプションを有効にします。

  Cisco ISE の GUI から、**[管理（Administration）] > [システム（System）]** > [証明書（Certificate）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted certificates）] を選択します。このウィンドウで、ルート CA 証明書を選択し、[編集（Edit）] をクリックします。[使用方法（Usage）] タブで、[信頼先（Trusted For）] セクションのチェックボックスをオンにします。

- ルート CA の [信頼（Trust）] オプションを有効にしない場合は、CA 証明書チェーン全体を信頼できる証明書ストアにインポートします。

ノード間の通信では、Cisco ISE 展開内の各ノードに属する管理者システム証明書を検証するために必要な信頼された証明書を、信頼できる証明書ストアに配置する必要があります。ノード間の通信にデフォルトの自己署名証明書を使用する場合は、各 Cisco ISE ノードの [システム証明書（System Certificates）] ページからこの証明書をエクスポートし、信頼できる証明書ストアにインポートする必要があります。自己署名証明書を CA 署名証明書で置き換える場合に必要なのは、適切なルート CA 証明書および中間 CA 証明書を信頼できる証明書ストアに配置することだけです。この手順を完了するまでは、ノードを Cisco ISE 展開に登録できないことに注意してください。

展開内でクライアントと PSN の間のセキュアな通信に自己署名証明書を使用する場合、BYOD ユーザがある場所から別の場所に移動すると、EAP-TLS ユーザ認証は失敗します。一部の PSN 間で提供される必要があるこのような認証要求の場合、外部で署名された CA 証明書を使用してクライアントと PSN の間の通信を保護するか、または外部の CA によって署名されたワイルドカード証明書を使用する必要があります。

パブリック署名証明書を取得する場合、または Cisco ISE 展開が FIPS モードで動作する場合は、すべてのシステム証明書および信頼できる証明書が FIPS 準拠であることを確認する必要があります。つまり、各証明書のキー サイズが 2048 バイト以上であり、SHA-1 または SHA-256 暗号化を使用する必要があります。

（注） スタンドアロンの Cisco ISE または PAN からバックアップを取得した後に、展開内の 1 つ以上のノードの証明書設定を変更する場合は、データを復元するために別のバックアップを取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。

ワイルドカード証明書

ワイルドカード証明書はワイルドカード表記（ドメイン名の前にアスタリスクとピリオドの形式）を使用し、組織の複数のホスト間で証明書を共有できるようにします。たとえば、証明書サブジェクトの CN 値は aaa.ise.local などの汎用ホスト名であり、SAN フィールドには、同じ汎用ホスト名と DNS.1=aaa.ise.local および DNS.2=*.ise.local などのワイルドカード表記が含まれます。

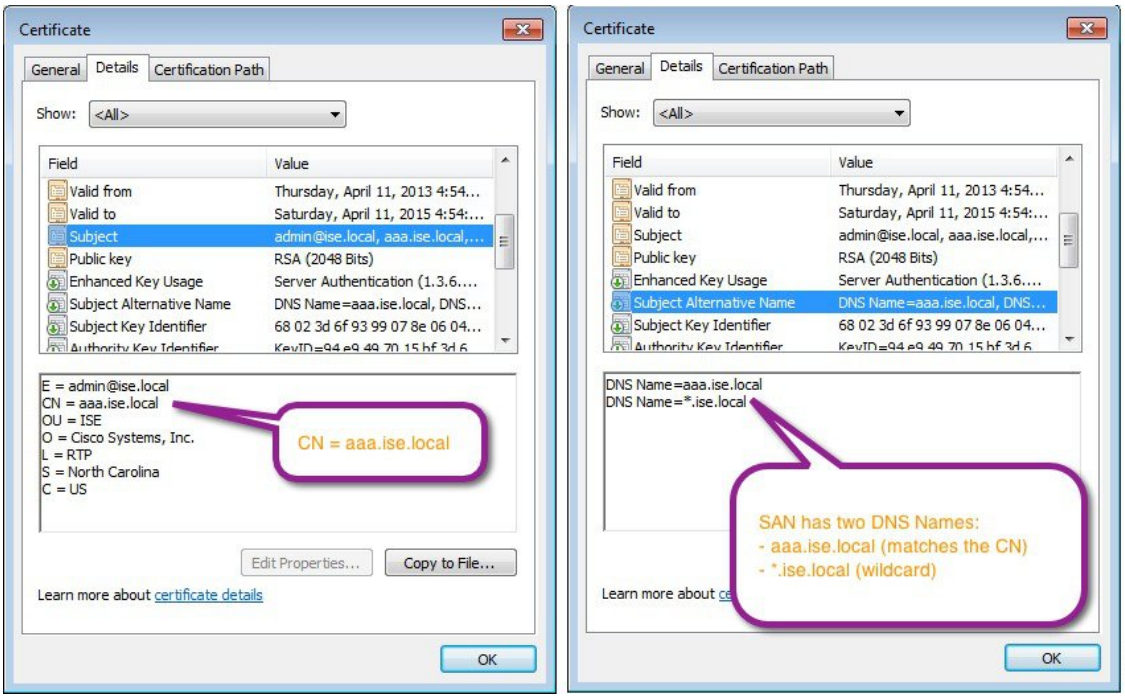
のように *.ise.local を使用してワイルドカード証明書を設定すると、その同じ証明書を使用して、次のような DNS 名が「.ise.local」で終了する他のすべてのホストを保護することができます。：

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

ワイルドカード証明書は通常の証明書と同じ方法で通信を保護し、要求は同じ検証方式を使用して処理されます。

次の図に、Web サイトの保護に使用されるワイルドカード証明書の例を示します。

図 *4:* ワイルドカード証明書の例



Cisco ISE のワイルドカード証明書のサポート

Cisco ISE はワイルドカード証明書をサポートしています。以前のリリースの Cisco ISE では、HTTPS に対して有効になったすべての証明書を検証し、CN フィールドがホストの完全修飾（FQDN）と正確に一致することを確認していました。フィールドが一致しない場合、その証明書は HTTPS 通信に使用できませんでした。

以前のリリースの Cisco ISE では、CN 値を使用して、url-redirect A-V pair 文字列の変数を置き換えていました。この CN 値は、すべての Centralized Web Authentication（CWA）、オンボーディング、ポスチャ リダイレクションなどに使用されました。

Cisco ISE は CN として ISE ノードのホスト名を使用します。

HTTPS および EAP 通信用のワイルドカード証明書

SSL/TLS トンネリングを使用する Admin（Web ベースのサービス）および EAP プロトコルに対して、Cisco ISE でワイルドカード サーバ証明書を使用できます。ワイルドカード証明書を使用することにより、各 Cisco ISE ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用すると、展開内の複数のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバ証明書を割り当てる場合よりも安全性が低いと見なされます。

ゲスト ポータルにパブリック ワイルドカード証明書を割り当て、ルート CA 証明書を使用してサブ CA をインポートする場合、ISE サービスが再起動されるまで証明書チェーンは送信されません。

（注） ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、重大なセキュリティ問題が発生する可能性があります。

ワイルドカード証明書では、ドメイン名の前にアスタリスク（*）およびピリオドが使用されます。たとえば、証明書のサブジェクト名の CN 値は aaa.ise.local などの汎用ホスト名になり、SAN フィールドには *.ise.local のようなワイルドカード文字が入力されます。Cisco ISE は、ワイルドカード証明書（提示される ID の一番左の文字がワイルドカード文字（*））をサポートします。たとえば、*.example.com または *.ind.example.com です。提示される ID に追加の文字とワイルドカード文字が含まれた証明書はサポートされません。たとえば、abc*.example.com、a*b.example.com、または *abc.example.com です。

URL リダイレクションの完全修飾ドメイン名

Cisco ISE が許可プロファイル リダイレクトを構築（中央集中型 Web 認証、デバイス登録 Web 認証、ネイティブ サプリカントのプロビジョニング、モバイル デバイス管理、およびクライアントのプロビジョニングとポスチャ サービスに対して）する場合、結果の cisco-av-pair ペアには、次のような文字列が含まれます。

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

この要求を処理するときに、Cisco ISE は文字列の一部のキーワードを実際の値で置き換えます。たとえば、SessionIdValue は、要求の実際のセッション ID に置き換えられます。eth0 インターフェイスの場合、Cisco ISE は URL 内の IP を Cisco ISE ノードの FQDN で置き換えます。eth0 以外のインターフェイスの場合、Cisco ISE は URL 内の IP アドレスを使用します。インターフェイス eth1 から eth3 にはホストのエイリアス（名前）を割り当てることができます。このエイリアスは Cisco ISE が URL リダイレクション中に IP アドレスの代わりに置き換えることができます。

これを行うために、次のように、Cisco ISE CLI の ISE /admin(config)# プロンプトからコンフィギュレーション モードで **ip host** コマンドを使用できます。

ip host *IP_address host-alias FQDN-string*

ここで、IP_address はネットワーク インターフェイス（eth1 または eth2 または eth3）の IP アドレスで、host-alias はネットワーク インターフェイスに割り当てる名前です。FQDN-string は、ネットワーク インターフェイスの完全修飾ドメイン名です。このコマンドを使用して、ネットワーク インターフェイスに host-alias または FQDN-string あるいはその両方を割り当てることができます。

ip host コマンドの使用例：ip host a.b.c.d sales sales.amerxyz.com

eth0 以外のインターフェイスにホストのエイリアスを割り当てたら、**application start ise** コマンドを使用して Cisco ISE でアプリケーション サービスを再起動する必要があります。

このホスト エイリアスのネットワーク インターフェイスとの関連付けを削除するには、次のようにこのコマンドの no 形式を使用します。

no ip host *IP_address host-alias FQDN-string*

ホストのエイリアスの定義を表示するには、**show running-config** コマンドを使用します。

FQDN 文字列を指定している場合は、その FQDN で URL 内の IP アドレスが置き換えられます。ホストのエイリアスのみを指定した場合は、そのホスト エイリアスと設定された IP ドメイン名を結合して完全な FQDN が結合され、URL 内の IP アドレスがその FQDN で置き換えられます。ネットワーク インターフェイスをホストのエイリアスにマッピングしない場合は、URL 内のネットワーク インターフェイスの IP アドレスが使用されます。

クライアントのプロビジョニング、ネイティブ サプリカント、またはゲスト フローに対して eth0 以外のインターフェイスを使用する場合は、eth0 以外のインターフェイスの IP アドレスまたはホスト エイリアスがポリシー サービス ノードの証明書の SAN フィールドに適切に設定されていることを確認する必要があります。

ワイルドカード証明書を使用する利点

- コスト削減。サードパーティの認証局によって署名された証明書には高額な費用がかかります（特にサーバ数が多い場合）。ワイルドカード証明書は、Cisco ISE 展開内の複数ノードで使用できます。
- 運用の効率化。ワイルドカード証明書は、すべてのポリシー サービス ノード（PSN）EAP および Web サービスが同じ証明書を共有することを可能にします。証明書を 1 回作成して、すべての PSN に適用することにより、コストを大幅に削減できるだけでなく、証明書の管理も簡素化されます。
- 認証エラーの低減。ワイルドカード証明書は、クライアントがプロファイル内に信頼された証明書を保存しており、そのクライアントが iOS のキーチェーン（署名ルートが信頼されている）に従っていない Apple iOS デバイスで発生する問題に対処します。iOS クライアントが最初に PSN と通信する際、このクライアントはその PSN の証明書を（信頼された認証局が署名している場合でも）明示的に信頼しません。ワイルドカード証明書を使用すると、この証明書がすべての PSN で同一になるため、ユーザは証明書の受け入れを 1 回行えばよく、その後の異なる PSN に対する認証はエラーやプロンプトが表示されることなく進行します。
- 簡素化されたサプリカントの設定。たとえば、PEAP-MSCHAPv2 およびサーバ証明書の信頼が有効になっている Microsoft Windows サプリカントで、各サーバ証明書を信頼するように指定することが必要とされており、そのように指定されていない場合、そのクライアントが別の PSN を使用して接続を行うと、各 PSN 証明書を信用するように、ユーザにプロンプトが出される可能性があります。ワイルドカード証明書を使用すると、各 PSN の個別の証明書ではなく、単一のサーバ証明書を信頼するだけで済みます。
- ワイルドカード証明書を使用すると、プロンプトの提示が減り、よりシームレスな接続が実現されることにより、ユーザ エクスペリエンスが改善されます。

ワイルドカード証明書を使用することの欠点

次に、ワイルドカード証明書に関連するセキュリティ上の考慮事項の一部を説明します。

- 監査性と否認防止性の低下
- 秘密キーの露出の増加
- 一般的ではなく、管理者により理解されていない

ワイルドカード証明書はISEノードごとの固有のサーバ証明書よりも安全性が低いと見なされています。ただし、コスト、およびその他の運用関連の要因がセキュリティリスクに勝っています。

ASA などのセキュリティ デバイスも、ワイルドカード証明書をサポートしています。

ワイルドカード証明書を展開する場合には注意が必要です。たとえば、*.company.local を使用して証明書を作成したとします。該当の秘密キーを攻撃者が回復できた場合、攻撃者は company.local ドメイン内のすべてのサーバをスプーフィングすることができます。したがって、このタイプの危険を回避するために、ドメイン領域を分割することがベストプラクティスと見なされています。

この想定される問題に対処し、利用範囲を制限するために、ワイルドカード証明書を使用して組織の特定のサブドメインを保護することもできます。ワイルドカードを指定する一般名のサブドメイン領域に、アスタリスク（*）を追加します。

たとえば、*.ise.company.localに対してワイルドカード証明書を設定すると、その証明書は次のような、DNS 名が「.ise.company.local」で終わるすべてのホストを保護するために使用できます。

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

ワイルドカード証明書の互換性

ワイルドカード証明書は通常、証明書サブジェクトの一般名（CN）としてリストされているワイルドカードを使用して作成されます。Cisco ISEは、このタイプの作成をサポートします。ただし、すべてのエンドポイントサプリカントが証明書サブジェクトのワイルドカード文字をサポートするわけではありません。

テスト済みのすべての Microsoft ネイティブ サプリカント（Windows Mobile を含む）の一部は、証明書のサブジェクトのワイルドカード文字をサポートしていません。

Cisco AnyConnect Network Access Manager（NAM）など、[サブジェクト（Subject）] フィールドでのワイルドカード文字の使用をサポートできる他のサプリカントを使用することができます。

また、DigiCert の Wildcard Plus など、証明書のサブジェクト代替名に特定のサブドメインを含めることで、互換性のないデバイスを使用するように設計された、特別なワイルドカード証明書を使用することもできます。

Microsoftサプリカントの制限はワイルドカード証明書の使用にとって妨げになるように見えますが、Microsoft のネイティブ サプリカントを含む、セキュアなアクセスについてテスト済みのすべてのデバイスを使用できるようにする代替の方法があります。

このためには、サブジェクトにワイルドカードを使用する代わりに、[Subject Alterative Name (SAN)] フィールドでワイルドカード文字を使用します。SAN フィールドはドメイン名（DNS 名）を検査するように設計された拡張を保持します。詳細については、RFC 6125 および 2128 を参照してください。

証明書階層

管理者ポータルから、すべてのエンドポイント、システム、および信頼できる証明書の証明書階層または信頼書トラストチェーンを表示できます。証明書階層には、証明書、すべての中間認証局（CA）の証明書、およびルート証明書が含まれています。たとえば、管理者ポータルからシステム証明書を表示すると、デフォルトでは該当するシステム証明書の詳細が表示されます。証明書階層は、証明書の上部に表示されます。詳細を表示するには、その階層で証明書をクリックします。自己署名証明書には階層または信頼チェーンがありません。

証明書のリスト ページで、[ステータス（Status）] 列に次のアイコンのいずれかが表示されます。

- 緑色のアイコン：有効な証明書（有効な信頼チェーン）を示します
- 赤色のアイコン：エラーを示します（たとえば、信頼証明書の欠落または期限切れ）
- 黄色のアイコン：証明書が期限切れ間近であることを警告し、更新処理を求めます

システム証明書

Cisco ISE システム証明書は、展開内のその他のノードおよびクライアント アプリケーションに対して Cisco ISE ノードを識別するサーバ証明書です。システム証明書の用途は次のとおりです。

- Cisco ISE 展開でノード間通信に使用されます。この証明書の場合、[使用方法（Usage）] フィールドで [管理（Admin）] オプションを選択します。
- Cisco ISE Web ポータルに接続するブラウザおよび REST クライアントで使用されます。この証明書の場合、[使用方法（Usage）] フィールドで [ポータル（Portal）] オプションを選択します。
- PEAP および EAP-FAST を使用する外部 TLS トンネルを形成するために使用されます。EAP-TLS、PEAP、および EAP-FAST の相互認証の場合、[使用方法（Usage）] フィールドで [EAP] オプションを選択します。
- RADIUS DTLS サーバ認証に使用されます。
- SAML IDプロバイダー（IdP）との通信に使用されます。この証明書の [使用方法（Usage）] フィールドで [SAML] オプションを選択します。[SAML] オプションを選択すると、その他のサービスにこの証明書を使用することはできません。

- pxGrid コントローラとの通信に使用されます。この証明書の場合、[使用方法（Usage）] フィールドで [pxGrid] オプションを選択します。

Cisco ISE 展開で、各ノードで有効なシステム証明書をインストールする必要があります。デフォルトでは、インストール時に Cisco ISE ノードに 2 つの自己署名証明書と、内部 Cisco ISE CA により署名された 1 つの証明書が作成されます。

- [EAP]、[管理（Admin）]、[ポータル（Portal）]、および [RADIUS DTLS] のための自己署名サーバ証明書（キー サイズは 2048 で 1 年間有効です）。
- SAML IdP との安全な通信に使用できる自己署名 SAML サーバ証明書（キーサイズは 2048 で 1 年間有効です）。
- pxGrid クライアントとの安全な通信に使用できる内部 Cisco ISE CA 署名付きサーバ証明書（キー サイズは 4096 で 1 年間有効です）。

展開をセットアップし、セカンダリ ノードを登録すると、pxGrid コントローラ用の証明書が自動的にプライマリ ノードの CA 署名付き証明書に置き換わります。したがってすべての pxGrid 証明書が同一 PKI トラスト階層の一部となります。

（注） ワイルドカードシステム証明書をエクスポートして、（ノード間通信用に）他のノードにインポートする場合は、必ず証明書と秘密キーをエクスポートして、暗号化パスワードを指定してください。インポート時は、証明書、秘密キー、および暗号化パスワードが必要です。

（注） お使いのリリースでサポートされているキーと暗号情報を確認するには、適切なバージョンの『Cisco Identity Services Engine Network Component Compatibility』ガイドを参照してください。

セキュリティを強化するために、自己署名証明書を CA 署名付き証明書で置き換えることを推奨します。CA 署名付き証明書を取得するには、以下を行う必要があります。

1. 証明書署名要求の作成と認証局への CSR の送信 （185 ページ）
2. 信頼できる証明書ストアへのルート証明書のインポート （177 ページ）
3. CSR への CA 署名付き証明書のバインド （185 ページ）

ISE コミュニティ リソース

How To: Implement ISE Server-Side Certificates

Certificate Renewal on Cisco Identity Services Engine Configuration Guide

システム証明書の表示

[システム証明書（System Certificate）] ページに、Cisco ISE に追加されたすべてのシステム証明書が一覧表示されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

[システム証明書（System Certificate）] ページが表示されます。このページには、システム証明書に関する次の情報が表示されています。

- [フレンドリ名（Friendly Name）]：証明書の名前。
- [使用者（Used By）]：この証明書が使用されるサービス。
- [ポータル グループ タグ（Portal group tag）]：ポータルを使用するように指定された証明書に対してのみ適用できます。どの証明書をポータルに使用しなければならないかを指定します。
- [発行先（Issued To）]：証明書のサブジェクトの一般名。
- [発行元（Issued By）]：証明書発行者の一般名
- [有効期限の開始（Valid From）]：証明書の作成日付（Not Before 証明書属性）。
- [期限日（Expiration Date）]：証明書の有効期限（Not After 証明書属性）。証明書の有効期限を示します。ここには、アイコンが関連付けられた 5 つのカテゴリがあります。
  - [91 日以上で期限切れ（Expiring in more than 90 days）]（緑のアイコン）
  - [90 日以内に期限切れ（Expiring in 90 days or less）]（青のアイコン）
  - [60 日以内に期限切れ（Expiring in 60 days or less）]（黄色のアイコン）
  - [30 日以内に期限切れ（Expiring in 30 days or less）]（オレンジのアイコン）
  - [期限切れ（Expired）]（赤のアイコン）

ステップ 2 証明書を選択し、[表示（View）] を選択して証明書の詳細を表示します。

システム証明書のインポート

管理者ポータルから、任意の Cisco ISE ノードのシステム証明書をインポートできます。

（注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。プライマリ管理ノード（PAN）の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

始める前に

- クライアント ブラウザを実行しているシステムに、システム証明書と秘密キー ファイルがあることを確認します。
- インポートするシステム証明書が外部 CA によって署名されている場合は、関連するルート CA および中間 CA の証明書を信頼できる証明書ストアにインポートします（[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]）。
- SHA-256 より大きいハッシュアルゴリズムで署名されたサーバ証明書はインポートしないでください。
- インポートするシステム証明書に、CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、およびkeyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。
[サーバ証明書のインポート（Import Server Certificate）] 画面が表示されます。

ステップ 3 インポートする証明書の値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

システム証明書のインポート設定

次の表では、サーバ証明書をインポートするために使用できる [システム証明書のインポート（Import System Certificate）] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理（Administration）]** > > > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** > **[インポート（Import）]** です。

表 *13 :* システム証明書のインポート設定

フィールド名	説明
ノードの選択（Select Node）	（必須）システム証明書をインポートする Cisco ISE ノードを選択します。
証明書ファイル（Certificate file）	（必須）[参照（Browse）] をクリックして、ローカル システムから証明書ファイルを選択します。

フィールド名	説明
秘密キー ファイル（Private key file）	（必須）[参照（Browse）] をクリックして、秘密キー ファイルを選択します。
[パスワード（Password）]	（必須）秘密キー ファイルを復号化するためのパスワードを入力します。
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ワイルドカード証明書の許可（Allow Wildcard Certificates）	ワイルドカード証明書（サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク（*）が含まれている証明書）をインポートする場合は、このチェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。このチェックボックスをオンにすると、Cisco ISE は展開内の他のすべてのノードにこの証明書をインポートします。
証明書の拡張の検証（Validate Certificate Extensions）	Cisco ISE に証明書の拡張の検証を許可する場合は、このチェックボックスをオンにします。このチェックボックスをオンにし、かつインポートする証明書に CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。
Usage	このシステム証明書を使用する必要があるサービスを選択します。 • [管理者（Admin）]：管理者ポータルとの通信および展開内の ISE ノード間の通信の保護に使用されるサーバ証明書 （注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。 • [EAP 認証（EAP Authentication）]：SSL/TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバ証明書 • [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバ証明書 • [pxGrid]：pxGrid クライアントとサーバの間の通信を保護するクライアントおよびサーバ証明書 • [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバ証明書

関連トピック

システム証明書 （157 ページ）
システム証明書の表示 （158 ページ）
システム証明書のインポート （159 ページ）

自己署名証明書の生成

自己署名証明書を生成することにより、新しいローカル証明書を追加できます。自己署名証明書は、内部テストと評価のニーズに対してのみ使用することを推奨します。実稼働環境にCisco ISE を展開することを計画している場合は、可能な限り CA 署名付き証明書を使用して、実稼働ネットワーク全体でより均一な受け入れが行われるようにします。

（注） 自己署名証明書を使用しており、Cisco ISE ノードのホスト名を変更する必要がある場合は、Cisco ISE ノードの管理者用ポータルにログインし、古いホスト名が使用された自己署名証明書を削除し、新しい自己署名証明書を生成します。そうしないと、Cisco ISE は古いホスト名が使用された自己署名証明書を引き続き使用します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

セカンダリ ノードから自己署名証明書を生成するには、**[管理（Administration）] > [システム（System）] > [サーバ証明書（Server Certificate）]** を選択します。

ステップ 2 [自己署名証明書の生成（Generate Self Signed Certificate）] をクリックし、[自己署名証明書の生成（Generate Self Signed Certificate）] ページに詳細を入力します。

ステップ 3 自己署名したワイルドカード証明書（サブジェクトの任意の一般名またはサブジェクト代替名のDNS名、またはその両方にアスタリスク（*）が含まれている証明書）を生成する場合は、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] チェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。

ステップ 4 この証明書を使用するサービスに基づいて [使用方法（Usage）] 領域のチェックボックスをオンにします。

ステップ 5 証明書を生成するには、[送信（Submit）] をクリックします。

CLI からセカンダリ ノードを再起動するには、指定された順序で次のコマンドを入力します。

a) **application stop ise**
b) **application start ise**

自己署名証明書の設定

次の表では、[自己署名証明書の生成（Generate Self Signed Certificate）] ページのフィールドについて説明します。このページでは、ノード間通信、EAP-TLS 認証、Cisco ISE Web ポータル、および pxGrid コントローラとの通信用のシステム証明書を作成できます。このページのナビゲーションパスは、**[管理（Administration）]**>**[システム（System）]**>**[証明書（Certificates）]**> **[システム証明書（System Certificates）]** > **[自己署名証明書の生成（Generate Self Signed Certificate）]** です。

表 *14 :* 自己署名証明書の設定

フィールド名	使用上のガイドライン
ノードの選択（Select Node）	（必須）システム証明書を生成するノード。
Common Name（CN）	（SAN を指定しない場合に必須）デフォルトでは、一般名は自己署名証明書を生成する ISE ノードの完全修飾ドメイン名です。
Organizational Unit（OU）	組織ユニット名。Engineering など。
組織（Organization）（O）	組織名。Cisco など。
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。
Country（C）	国名。2 文字の ISO 国番号を入力する必要があります。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	証明書に関連付けられた IP アドレス、DNS 名、または Uniform Resource Identifier（URI）。
キー タイプ	RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。

フィールド名	使用上のガイドライン
キーの長さ（**Key Length**）	公開キーのビット サイズを指定します。RSA には、次のオプションを使用できます。 • 512 • 1024 • 2048 • 4096 ECDSA には、次のオプションを使用できます。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。 パブリック CA 署名付き証明書を取得する場合、または FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は、2048 を選択します。
署名するダイジェスト（**Digest to Sign With**）	ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。
証明書ポリシー（**Certificate Policies**）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。
TTL 有効期限（**Expiration TTL**）	証明書が失効するまでの日数を指定します。
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ワイルドカード証明書の許可（**Allow Wildcard Certificates**）	自己署名したワイルドカード証明書（サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク（*）が含まれている証明書）を生成する場合は、このチェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。

フィールド名	使用上のガイドライン
Usage	このシステム証明書を使用する必要があるサービスを選択します。 • [管理者（Admin）]：管理者ポータルとの通信および展開内の ISE ノード間の通信の保護に使用されるサーバ証明書 • [EAP 認証（EAP Authentication）]：SSL/TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバ証明書 • [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバ証明書 • [pxGrid]：pxGrid クライアントとサーバの間の通信を保護するクライアントおよびサーバ証明書 • [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバ証明書

関連トピック

システム証明書 （157 ページ）
システム証明書の表示 （158 ページ）
自己署名証明書の生成 （162 ページ）

システム証明書の編集

このページを使用して、システム証明書を編集し、自己署名証明書を更新できます。ワイルドカード証明書を編集すると、変更が展開内のすべてのノードに複製されます。ワイルドカード証明書を削除した場合、そのワイルドカード証明書は展開内のすべてのノードから削除されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 自己署名証明書を更新するには、[更新期間（Renewal Period）] チェックボックスをオンにして、有効期限 TTL（存続可能時間）を日、週、月、または年単位で入力します。

ステップ 4 [Save（保存）] をクリックして変更内容を保存します。

[管理者（Admin）] チェックボックスがオンになっている場合、Cisco ISE ノードのアプリケーション サーバが再起動されます。また、その Cisco ISE ノードが展開の PAN である場合は、展開内のその他すべてのノードでもアプリケーション サーバが再起動されます。プライマリ管理ノード（PAN）の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

（注） Chrome 65 以上を使用して ISE を起動すると、URL が正しくリダイレクトされたにもかかわらず、BYOD ポータルまたはゲスト ポータルがブラウザで起動に失敗することがあります。これは、すべての [サブジェクトの別名（Subject Alternative Name）] フィールドに証明書を必要とする、Google で導入された新しいセキュリティ機能が原因です。ISE 2.4 以降のリリースの場合、[サブジェクトの別名（Subject Alternative Name）] フィールドを入力する必要があります。

Chrome 65 以上で起動するには、次の手順に従います。

1. [サブジェクトの別名（Subject Alternative Name）] フィールドに入力することで、ISE GUI から新しい自己署名証明書を生成します。DNS と IP アドレスの両方を入力する必要があります。

2. ISE サービスが再起動します。

3. Chrome ブラウザでポータルにリダイレクトされます。

4. ブラウザで [証明書の表示（View Certificate）] > [詳細（Details）] > [コピー（Copy）] の順に選択し、base-64 エンコードを選択して、証明書をコピーします。

5. 高信頼パスで証明書をインストールします。

6. Chrome ブラウザを終了し、ポータルのリダイレクトを試みます。

（注） Win RS4 または RS5 のオペレーティング システムでブラウザ Firefox 64 以降のワイヤレス BYODセットアップを設定する場合は、証明書の例外を追加することができない場合があります。この現象は Firefox 64 以降の新規インストール時に発生することがあります。以前のバージョンから Firefox 64 以降にアップグレードした場合は発生しません。次の手順では、このような場合でも証明書の例外を追加することができます。

1. BYOD フローのシングル/デュアル PEAP または TLS を設定します。

2. Windows のすべてのオプションで CP ポリシーを設定します。

3. エンド クライアント Windows RS4/RS5 で Dot1.x/MAB SSID に接続します。

4. ゲスト/BYOD ポータルにリダイレクトするために、FF64 ブラウザに 1.1.1.1 と入力します。

5.**[例外を追加（Add Exception）]** > **[証明書を追加できない（Unable to add certificate）]** をクリックし、フローを続行します。

これを回避するには、**[オプション（Options）]**>**[プライバシーと設定（Privacy & Settings）]**> **[証明書の表示（View certificates）]** > **[サーバ（Servers）]** > **[例外を追加（Add Exception）]** に移動して、Firefox 64 に証明書を手動で追加する必要があります。

システム証明書の削除

今後使用しないシステム証明書を削除できます。

システム証明書ストアから複数の証明書を一度に削除できますが、管理および EAP 認証に使用できる証明書を少なくとも 1 つ所有する必要があります。また、管理、EAP 認証、ポータル、または pxGrid コントローラに使用される証明書は削除できません。ただし、サービスがディセーブルの場合は、pxGrid 証明書を削除できます。

ワイルドカード証明書を削除することを選択した場合、証明書は展開内のすべてのノードから削除されます。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。

ステップ 3 [はい（Yes）] をクリックして、証明書を削除します。

システム証明書のエクスポート

選択したシステム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 エクスポートする証明書の横にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント　値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカードシステム証明書をエクスポートしてノード間通信用に他のノードにインポートする場合）は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE ノードにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート（Export）] をクリックして、クライアント ブラウザを実行しているファイル システムに証明書を保存します。

証明書のみをエクスポートする場合、証明書は Privacy Enhanced Mail 形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書は Privacy Enhanced Mail 形式の証明書と暗号化された秘密キーファイルを含む .zip ファイルとしてエクスポートされます。

信頼できる証明書ストア

信頼できる証明書ストアには、信頼に使用される、Simple Certificate Enrollment Protocol（SCEP）用の X.509 証明書が含まれています。

信頼できる証明書ストア内の証明書は PAN で管理され、Cisco ISE 展開内の他のすべてのノードに複製されます。Cisco ISE はワイルドカード証明書をサポートしています。

Cisco ISE は、次の目的で信頼できる証明書を使用します。

- エンドポイントによる認証と、証明書ベースの管理者認証を使用してISE-PIC管理者ポータルにアクセスする Cisco ISE 管理者による認証に使用するクライアント証明書を確認するため。
- 展開内の Cisco ISE ノード間のセキュアな通信を可能にするため。信頼できる証明書ストアには、展開内の各ノードのシステム証明書との信頼を確立するために必要な CA 証明書のチェーンが含まれている必要があります。
  - 自己署名証明書をシステム証明書に使用する場合は、各ノードの自己署名証明書を PAN の信頼できる証明書ストアに配置する必要があります。

- CA 署名付き証明書をシステム証明書に使用する場合は、CA ルート証明書だけでなく、信頼チェーン内のすべての中間証明書も PAN の信頼できる証明書ストアに配置する必要があります。

- セキュア LDAP 認証を有効にするには、SSL を経由してアクセスされる LDAP ID ソースを定義するときに、証明書ストアから証明書を選択する必要があります。
- パーソナル デバイス ポータルを使用してネットワークへの登録を準備しているパーソナル デバイスに配信するため。Cisco ISE は、パーソナル デバイス登録をサポートするために、ポリシー サービス ノード（PSN）での SCEP を実装しています。登録するデバイスは、SCEP プロトコルを使用して PSN からクライアント証明書を要求します。PSN には中継の役割を果たす登録局（RA）があります。RA は、登録するデバイスからの要求を受信して検証し、その後クライアント証明書を発行する外部 CA または内部 Cisco ISE CA にその要求を転送します。CA は RA に証明書を返し、RA が証明書をデバイスに返します。

  Cisco ISE によって使用される各 SCEP CA は、SCEP RA プロファイルによって定義されます。SCEP RA のプロファイルが作成されると、次の 2 つの証明書が信頼できる証明書ストアに自動的に追加されます。

  - CA 証明書（自己署名証明書）
  - CA によって署名された RA 証明書（証明書要求のエージェントの証明書）。

  SCEP プロトコルでは、これらの 2 つの証明書が RA によって登録デバイスに提供されている必要があります。信頼できる証明書ストアにこの 2 つの証明書を配置すると、これらのノードの RA が使用するために、証明書がすべての PSN ノードに複製されます。

（注） SCEP RA プロファイルが削除されると、関連付けられている CA チェーンが信頼できる証明書ストアからも削除されます。ただし、セキュアな syslog、LDAP、システム、または信頼証明書によって同じ証明書が参照されている場合は、SCEP プロファイルだけが削除されます。

（注）

- Cisco ISE にインポートされる X.509 証明書は、Privacy Enhanced Mail（PEM）または Distinguished Encoding Rules（DER）形式である必要があります。証明書チェーン（システム証明書、およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。
- ゲスト ポータルにパブリック ワイルドカード証明書を割り当て、ルート CA 証明書を使用してサブ CA をインポートする場合、ISE サービスが再起動されるまで証明書チェーンは送信されません。

ISE コミュニティ リソース

Install a Third-Party CA Certificate in ISE 2.0

信頼できる証明書ストアの証明書

信頼できる証明書ストアは、次の信頼できる証明書で事前設定されています。製造業者証明書、ルート証明書、その他の信頼できる証明書。ルート証明書（Cisco Root CA）は、製造業者（Cisco CA Manufacturing）証明書に署名します。これらの証明書は、デフォルトでは無効になっています。展開でエンドポイントとして Cisco IP Phone を使用している場合は、これら 2 つの証明書を有効にして、この電話用にシスコが署名した証明書の認証ができるようにします。

[信頼できる証明書ストア（Trusted Certificate Store）] ページ

次の表では、管理ノードに追加された証明書を表示するために使用できる [信頼できる証明書ストア（Trusted Certificates Store）] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** です。

表 *15 :* 信頼できる証明書ページ

フィールド名	使用上のガイドライン
フレンドリ名（**Friendly Name**）	証明書の名前を表示します。
Status（ステータス）	有効または無効にします。[無効（Disabled）] の場合、ISE は信頼を確立するために証明書を使用しません。
信頼対象（**Trusted for**）	証明書を使用するサービスを表示します。
発行先（**Issued To**）	証明書のサブジェクトの一般名（CN）。
発行元（**Issued By**）	証明書の発行元の一般名（CN）。
有効期限の開始（**Valid From**）	「Not Before」証明書属性。
Expiration Date	「Not After」証明書属性。
有効期限ステータス（**Expiration Status**）	証明書の有効期限のステータスに関する情報です。このコラムに表示される情報メッセージには 5 つのアイコンとカテゴリがあります。 • **緑色**：期限切れまで 91 日以上 • **青色**：期限切れまで 90 日以内 • **黄色**：期限切れまで 60 日以内 • **オレンジ色**：期限切れまで 30 日以内 • **赤色**: 期限切れ

関連トピック

信頼できる証明書ストア （168 ページ）
信頼できるストア証明書の表示 （172 ページ）
信頼できる証明書ストアの証明書のステータス変更 （172 ページ）
信頼できる証明書ストアへの証明書の追加 （173 ページ）

信頼できる証明書の命名の制約

CTL の信頼できる証明書には名前の制約の拡張が含まれている場合があります。この拡張は、証明書チェーンの後続のすべての証明書のサブジェクト名とサブジェクト代替名フィールドの値の名前空間を定義します。Cisco ISE は、ルート証明書で指定された制約を検査しません。

次の名前の制約がサポートされています。

- ディレクトリ名

  ディレクトリ名の制限は、サブジェクト/SAN のディレクトリ名のプレフィクスです。次の例を参考にしてください。

  - 正しいサブジェクト プレフィクス：

    CA 証明書の名前の制約：Permitted: O=Cisco

    クライアント証明書のサブジェクト：O=Cisco,CN=Salomon

  - 不正なサブジェクト プレフィクス：

    CA 証明書の名前の制約：Permitted: O=Cisco

    クライアント証明書のサブジェクト：CN=Salomon,O=Cisco

- DNS
- E-mail
- URI（URI の制約は、http://、https://、ftp://、または ldap:// のような URI プレフィクスで始まる必要があります）。

次の名前の制約はサポートされていません。

- IP アドレス
- Othername

信頼できる証明書にサポートされていない制約が含まれており、検証中の証明書に該当のフィールドが含まれていない場合は、Cisco ISE がサポートされない制約を検証できないため、その証明書は拒否されます。

信頼できる証明書内の名前の制約の定義例を次に示します。

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
```

```
    email:.abcde.be
    email:.abcde.bg
    email:.abcde.by
    DNS:.dir
    DirName: DC = dir, DC = emea
    DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
    DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
    DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
   DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100

    URI:.dir
    IP:172.23.0.171/255.255.255.255
  Excluded:
    DNS:.dir
    URI:.dir
```

受け入れ可能なクライアント証明書のサブジェクトは、次のように上記の定義に一致します。

```
          Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

信頼できるストア証明書の表示

[信頼できる証明書（Trusted Certificates）] ページに、Cisco ISE に追加されたすべての信頼できる証明書が一覧表示されます。信頼できる証明書を表示するには、スーパー管理者またはシステム管理者である必要があります。

すべての証明書を表示するには、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。[信頼できる証明書（Trusted Certificates）] ページが表示され、すべての信頼できる証明書が一覧表示されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

信頼できる証明書ストアの証明書のステータス変更

証明書のステータスが有効になっている必要があります。これにより、Cisco ISE が信頼の確立にこの証明書を使用できるようになります。証明書が信頼できる証明書ストアにインポートされると、この証明書は自動的に有効になります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 有効または無効にする証明書の隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 ステータスを変更します。

ステップ 4 [保存（Save）] をクリックします。

信頼できる証明書ストアへの証明書の追加

[証明書ストア（Certificate Store）] ページを使用して、Cisco ISE に CA 証明書を追加することができます。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ブラウザを実行しているコンピュータのファイル システムに、証明書ストアの証明書が存在することを確認します。証明書は PEM または DER 形式である必要があります。
- Admin 認証または EAP 認証に証明書を使用する場合は、基本制約が証明書に定義され、CA フラグが true に設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 必要に応じてフィールドの値を設定します。

EAP認証用または証明書ベースの管理者認証用に証明書チェーンにサブCA証明書を使用する場合は、ルート CA までに証明書チェーンにすべての証明書をインポートする際に [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）] チェックボックスを必ずオンにしてください。CISCO ISE 2.4 パッチ 8 以降、同じサブジェクト名を持つ複数の CA 証明書をインポートできます。証明書ベースの管理者認証の場合は、信頼できる証明書を追加する際に、[証明書ベースの管理者認証用に信頼する（Trust for certificate based admin authentication）] チェックボックスをオンにします。

パスワードベースの認証から証明書ベースの認証に認証タイプを変更すると、Cisco ISE は展開内の各ノードでアプリケーション サーバを再起動します。PAN のアプリケーション サーバから開始され、その後に各追加ノードが 1 つずつ続きます。

信頼できる証明書の編集

証明書を信頼できる証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 必要に応じて編集可能なフィールドを変更します。

ステップ 4 [保存（Save）] をクリックして、証明書ストアに対して行った変更を保存します。

証明書設定の編集

次の表では、認証局（CA）証明書属性を編集するために使用できる [証明書ストアの証明書編集（Certificate Store Edit Certificate）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [証明書（Certificate）] > [編集（Edit）]** です。

表 *16 :* 証明書ストア編集設定

フィールド名	使用上のガイドライン
証明書発行元（Certificate Issuer）	
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。
Status（ステータス）	[有効（Enabled）] または [無効（Disabled）] を選択します。[無効（Disabled）]の場合、ISE は信頼を確立するために証明書を使用しません。
説明	任意で説明を入力します。
使用方法	
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書で（他の ISE ノードまたは LDAP サーバから）サーバ証明書を検証する場合は、このチェックボックスをオンにします。
クライアント認証および syslog 用に信頼する（**Trust for client authentication and Syslog**）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した ISE に接続するエンドポイントの認証 • syslog サーバの信頼
シスコ サービスの認証用に信頼する（**Trust for authentication of Cisco Services**）	フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
証明書ステータスの検証（Certificate Status Validation）	ISEは、特定のCAが発行するクライアントまたはサーバ証明書の失効ステータスをチェックする2とおりの方法をサポートしています。1つは、Online Certificate Status Protocol（OCSP）を使用して証明書を検証することです（OCSPは、CAによって保持されるOCSPサービスに要求を行います）。もう1つは、ISEにCAからダウンロードした証明書失効リスト（CRL）に対して証明書を検証することです。両方の方法は、OCSPを最初に使用し、ステータスを判断できないときに限りCRLを使用する場合に使用できます。
OCSPサービスに対して検証する（Validate Against OCSP Service）	OCSPサービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まずOCSPサービスを作成する必要があります。
OCSPが不明なステータスを返した場合は要求を拒否する（Reject the request if OCSP returns UNKNOWN status）	認証ステータスがOCSPによって判別されなかった場合に要求を拒否するには、このチェックボックスをオンにします。このチェックボックスをオンにした場合、OCSPサービスによって不明のステータス値が返されると、ISEは現在評価されているクライアントまたはサーバ証明書を拒否します。
OCSP応答側が到達不能な場合は要求を拒否する（Reject the request if OCSP Responder is unreachable）	OCSP応答側が到達不能な場合にISEが要求を拒否するには、このチェックボックスをオンにします。
CRLのダウンロード（Download CRL）	Cisco ISEでCRLをダウンロードするには、このチェックボックスをオンにします。
CRL配信URL（CRL Distribution URL）	CAからCRLをダウンロードするためのURLを入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URLは「http」、「https」、または「ldap」で始まる必要があります。
CRLの取得（Retrieve CRL）	CRLは、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。
ダウンロードが失敗した場合は待機する（If download failed, wait）	Cisco ISEがCRLを再度ダウンロードするまでに待機する時間間隔を設定します。

フィールド名	使用上のガイドライン
CRL を受信しない場合 CRL 検証をバイパスする（Bypass CRL Verification if CRL is not Received）	このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。
CRL がまだ有効でないか、または期限切れの場合は無視する（Ignore that CRL is not yet valid or expired）	Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。 Cisco ISE で [有効日（Effective Date）] フィールドの開始日と [次の更新（Next Update）] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRL がまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。

関連トピック

信頼できる証明書ストア （168 ページ）
信頼できる証明書の編集 （173 ページ）

信頼できる証明書の削除

今後使用しない信頼できる証明書を削除できます。ただし、ISE 内部 CA（認証局）の証明書は削除しないでください。ISE 内部 CA 証明書を削除できるのは、展開全体の ISE ルート証明書チェーンを置き換える場合のみです。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。ISE 内部 CA 証明書を削除することを選択した場合は、次のとおりにクリックします。

- [削除（Delete）]：ISE 内部 CA 証明書を削除する場合。ISE 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークにアクセスできません。エンドポイントをネットワークで再度有効にするには、信頼できる証明書ストアに同じ ISE 内部 CA 証明書をインポートします。

- [削除および取消（Delete & Revoke）]：ISE 内部 CA 証明書を削除して取り消します。ISE 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークにアクセスできません。この操作は取り消すことができません。展開全体の ISE ルート証明書チェーンを置き換える必要があります。

ステップ 3 [はい（Yes）] をクリックして、証明書を削除します。

信頼できる証明書ストアからの証明書のエクスポート

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

（注） 内部 CA から証明書をエクスポートし、そのエクスポートを使用してバックアップから復元する場合は、CLI コマンド `application configure ise` を使用する必要があります。詳細については、Cisco ISE CA 証明書およびキーのエクスポート （212 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**。.

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 3 クライアント ブラウザを実行しているファイル システムに Privacy Enhanced Mail ファイルを保存します。

信頼できる証明書ストアへのルート証明書のインポート

ルート CA 証明書および中間 CA 証明書をインポートするとき、信頼できる CA 証明書を使用する対象のサービスを指定できます。

始める前に

CSR に署名し、デジタルで署名された CA 証明書を返した認証局のルート証明書および他の中間証明書が必要です。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 表示された [証明書ストアへの新しい証明書のインポート（Import a new Certificate into the Certificate Store）] ウィンドウで、[ファイルの選択（Choose File）] をクリックし、CA によって署名され、返されたルート CA 証明書を選択します。

ステップ 4 **わかりやすい名前**を入力します。

わかりやすい名前を入力しないと、Cisco ISE により、このフィールドには、*common-name#issuer#nnnnn* 形式（、*nnnnn* は一意の番号）で名前が自動的に入力されます。再度証明書を編集して、**わかりやすい名前**を変更できます。

ステップ 5 この信頼できる証明書を使用するサービスの横にあるチェックボックスをオンにします。

ステップ 6 （任意）[説明（Description）] フィールドに証明書の説明を入力します。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

信頼できる証明書ストアに中間 CA 証明書をインポートします（該当する場合）。

信頼できる証明書のインポート設定

次の表では、認証局（CA）証明書を Cisco ISE に追加するために使用できる [信頼できる証明書のインポート（Trusted Certificate Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** です。

表 *17 :* 信頼できる証明書のインポート設定

フィールド	説明
証明書ファイル（Certificate file）	[参照（Browse）] をクリックして、ブラウザを実行しているコンピュータから証明書ファイルを選択します。
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE により <common name>#<issuer>#<nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書を（他の ISE ノードまたは LDAP サーバから）サーバ証明書の検証に使用する場合は、このチェックボックスをオンにします。

フィールド	説明
クライアント認証および syslog 用に信頼する（**Trust for client authentication and Syslog**）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した ISE に接続するエンドポイントの認証 • syslog サーバの信頼
シスコ サービスの認証用に信頼する（**Trust for authentication of Cisco Services**）	フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書の拡張の検証（**Validate Certificate Extensions**）	（[クライアント認証用に信頼する（Trust for client authentication）] オプションと [証明書拡張の検証を有効にする（Enable Validation of Certificate Extensions）] オプションの両方をオンにした場合のみ）「keyUsage」拡張が存在し、「keyCertSign」ビットが設定されていることと、CA フラグが true に設定された基本制約拡張が存在することを確認します。
説明	任意で説明を入力します。

関連トピック

信頼できる証明書ストア （168 ページ）
証明書チェーンのインポート （179 ページ）
信頼できる証明書ストアへのルート証明書のインポート （177 ページ）

証明書チェーンのインポート

証明書ストアから受信した証明書チェーンを含む単一のファイルから、複数の証明書をインポートすることができます。ファイル内のすべての証明書は Privacy-Enhanced Mail（PEM）の形式であり、証明書は次の順序に並べられている必要があります。

- ファイル内の最後の証明書は、CA によって発行されたクライアントまたはサーバ証明書である必要があります。
- 前にあるすべての証明書は、ルート CA 証明書と、発行された証明書の署名のチェーンにあるすべて中間 CA 証明書である必要があります。

証明書チェーンのインポートは、次の 2 ステップのプロセスです。

1. 管理者ポータルで信頼できる証明書ストアに証明書チェーン ファイルをインポートします。この操作により、信頼できる証明書ストアにある最後の 1 つを除き、すべての証明書がファイルからインポートされます。
2. CA 署名付き証明書のバインド操作を使用して証明書チェーン ファイルをインポートします。この操作により、最後の証明書がローカル証明書としてファイルからインポートされます。

Cisco ISE ノード間通信の信頼できる証明書のインストール

展開をセットアップする場合、セカンダリ ノードを登録する前に、セカンダリ ノードの管理者証明書の検証に使用される適切な CA 証明書を PAN の証明書信頼リスト（CTL）に配置する必要があります。PAN の CTL に入力する手順は、シナリオに応じて異なります。

- セカンダリ ノードが管理者ポータルとの通信に CA 署名付き証明書を使用する場合は、セカンダリ ノードの CA 署名付き証明書、関連する中間証明書（ある場合）、および（セカンダリ ノードの証明書に署名した CA の）ルート CA 証明書を PAN の CTL にインポートする必要があります。
- セカンダリ ノードが管理者ポータルとの通信に自己署名証明書を使用する場合は、PAN の CTL にセカンダリ ノードの自己署名証明書をインポートできます。

（注）
- 登録されたセカンダリ ノードの管理者証明書を変更する場合は、セカンダリ ノードの管理者証明書の検証に使用できる適切な CA 証明書を取得し、PAN の CTL にインポートする必要があります。
- 展開内でクライアントと PSN の間のセキュアな通信に自己署名証明書を使用する場合、BYOD ユーザがある場所から別の場所に移動すると、EAP-TLS ユーザ認証は失敗します。一部の PSN 間で提供される必要があるこのような認証要求の場合、外部で署名された CA 証明書を使用してクライアントと PSN の間の通信を保護するか、または外部の CA によって署名されたワイルドカード証明書を使用する必要があります。

外部 CA から発行された証明書に基本制約が定義されており、CA フラグが true に設定されていることを確認します。ノード間通信用の CA 署名付き証明書のインストール：

ステップ 1 証明書署名要求の作成と認証局への CSR の送信 （185 ページ）
ステップ 2 信頼できる証明書ストアへのルート証明書のインポート （177 ページ）
ステップ 3 CSR への CA 署名付き証明書のバインド （185 ページ）

Cisco ISE でのデフォルトの信頼できる証明書

Cisco ISE の信頼できる証明書ストア（**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**）には、デフォルトで使用可能な証明書がいくつか含まれています。これらの証明書は、セキュリティ要件を満たすためにストアに自動的にインポートされます。ただし、これらすべてを使用する必要はありません。次の表に記載されている場合を除き、すでに使用可能になっている証明書ではなく、自分で選択した証明書を使用できます。

表 *18 :*

信頼できる証明書の名前	シリアル番号（Serial Number）	証明書の目的	証明書を含む Cisco ISE リリース
Baltimore CyberTrust Root CA	02 00 00 B9	この証明書は、一部の地域で cisco.com が使用する CA チェーン内のルート CA 証明書として機能することができます。また、この証明書は、https://s3.amazonaws.com でホストされている ISE 2.4 のポスチャ/CP 更新 XML ファイルでも使用されていました。	リリース 2.4 以降。
DST Root CA X3 Certificate Authority	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	この証明書は、cisco.com が使用する CA チェーンのルート CA 証明書として機能することができます。	リリース 2.4 以降。
Thawte Primary Root CA	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	この証明書は、cisco.com と perfigo.com が使用する CA チェーンのルート CA 証明書として機能することができます。	リリース 2.4 以降。

信頼できる証明書の名前	シリアル番号（Serial Number）	証明書の目的	証明書を含む Cisco ISE リリース
VeriSign Class 3 Public Primary Certification Authority	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	この証明書は、VeriSign Class 3 Secure Server CA-G3 のルート CA 証明書として機能します。 Cisco ISE でプロファイラ フィード サービスを設定する場合は、この証明書を使用する必要があります。	リリース 2.4 以降。
VeriSign Class 3 Secure Server CA - G3	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	これは、2020 年 2 月 7 日に期限切れになる中間 CA 証明書です。この証明書を更新する必要はありません。 証明書を削除するには、下記のタスクを実行します。	リリース 2.4 以降。
Cisco CA Manufacturing	6A 69 67 B3 00 00 00 00 00 03	この証明書は、Cisco ISE に接続している特定のシスコデバイスが使用する場合があります。この証明書はデフォルトでは無効になっています。	リリース 2.4 および 2.6。
Cisco Manufacturing CA SHA2	02	この証明書は、管理者認証、エンドポイント認証、および展開インフラストラクチャフローの CA チェーン内で使用できます。	リリース 2.4 以降。
Cisco Root CA 2048	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	この証明書は、Cisco ISE に接続している特定のシスコデバイスが使用することができます。この証明書はデフォルトでは無効になっています。	リリース 2.4 以降。

信頼できる証明書の名前	シリアル番号（Serial Number）	証明書の目的	証明書を含むCisco ISEリリース
Cisco Root CA M2	01	この証明書は、管理者認証、エンドポイント認証、および展開インフラストラクチャフローのCAチェーン内で使用できます。	リリース2.4以降。
DigiCert Root CA	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	Facebookを使用したゲストログインを使用しているフローには、この証明書を使用する必要があります。	リリース2.4以降。
DigiCert SHA2 High Assurance Server CA	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	Facebookを使用したゲストログインを使用しているフローには、この証明書を使用する必要があります。	リリース2.4以降。
HydrantID SSL ICA G2	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	シスコサービスで信頼されています。	リリース2.4および2.6。
QuoVadis Root CA 2	05 09	この証明書は、プロファイラ、ポスチャ、およびクライアントプロビジョニングフロー内で使用する必要があります。	リリース2.4以降。
Cisco ECC Root CA	01	この証明書は、Cisco ISEで使用されるシスコの信頼ルートストアバンドルの一部です。	リリース2.6。
Cisco Licensing Root CA	01	この証明書は、Cisco ISEで使用されるシスコの信頼ルートストアバンドルの一部です。	リリース2.6以降。
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	この証明書は、Cisco ISEで使用されるシスコの信頼ルートストアバンドルの一部です。	リリース2.6以降。

信頼できる証明書の名前	シリアル番号（Serial Number）	証明書の目的	証明書を含む Cisco ISE リリース
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
Cisco RXC-R2	01	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。
Cisco ECC Root CA 2099	03	この証明書は、Cisco ISE で使用されるシスコの信頼ルートストアバンドルの一部です。	リリース 2.6 以降。

Cisco ISE からのデフォルトの信頼できる証明書の削除

- すべての信頼できる証明書を表示するには、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** に移動します。
- 削除する証明書をエクスポートして保存します。これにより、必要に応じて再度インポートできるようになります。

  エクスポートする証明書のチェックボックスをクリックし、上にあるメニューバーの [エクスポート（Export）] をクリックします。キーチェーンがシステムにダウンロードされます。
- 証明書を削除します。削除する証明書のチェックボックスをクリックし、上にあるメニューバーの [削除（Delete）] をクリックします。CA チェーン、セキュアな syslog、またはセキュアな LDAP によって使用されている場合は、その証明書を削除することはできません。
- CA チェーン、セキュアな syslog、および それが含まれている syslog から証明書を削除するために必要な設定変更を行ってから、証明書を削除します。
- 証明書が削除されたら、関連するサービス（証明書の目的を参照）が予想どおりに動作していることを確認します。

証明書署名要求

認証局（CA）が署名付き証明書を発行するためには、証明書署名要求（CSR）を作成してCAに送信する必要があります。

自分が作成した証明書署名要求（CSR）のリストは、[証明書署名要求（Certificate Signing Requests）]ページで使用できます。認証局（CA）から署名を取得するには、CSRをエクスポートし、その証明書をCAに送信する必要があります。証明書はCAによって署名され、返されます。

管理者ポータルから証明書を一元的に管理できます。展開内のすべてのノードのCSRを作成およびエクスポートできます。その後、CSRをCAに送信し、CAからCA署名付き証明書を取得し、CAによって返されたルートおよび中間CA証明書を信頼できる証明書ストアにインポートし、CSRにCA署名付き証明書をバインドする必要があります。

証明書署名要求の作成と認証局へのCSRの送信

証明書署名要求（CSR）を生成して、展開内のノードのCA署名付き証明書を取得できます。展開の選択ノードまたは展開のすべてのノード用のCSRを生成できます。

ステップ1 **[管理（Administration）]>[システム（System）]>[証明書（Certificates）]>[証明書署名要求（Certificate Signing Requests）]**を選択します。

ステップ2 CSRを生成するための値を入力します。各フィールドの詳細については、「証明書署名要求の設定」を参照してください。

ステップ3 [Generate（生成）]をクリックしてCSRを生成します。

CSRが生成されます。

ステップ4 [Export（エクスポート）]をクリックして、メモ帳でCSRを開きます。

ステップ5 「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」までのすべてのテキストをコピーします。

ステップ6 選択したCAの証明書要求に、このCSRの内容を貼ってください。

ステップ7 署名済みの証明書をダウンロードする。

CAによっては、署名付き証明書が電子メールで送信される場合があります。署名付き証明書は、zipファイルの形式で、Cisco ISEの信頼された証明書ストアに追加する必要がある、新規発行の証明書とCAのパブリック署名証明書が含まれています。デジタル署名されたCA証明書、ルートCA証明書、および他の中間CA証明書（該当する場合）がクライアントブラウザを実行するローカルシステムにダウンロードされます。

CSRへのCA署名付き証明書のバインド

CAからデジタル署名付き証明書を受け取った後、それを証明書署名要求（CSR）にバインドする必要があります。管理者ポータルから展開内のすべてのノードに対してバインド操作を実行できます。

始める前に

- デジタル署名付き証明書、および関連するルート中間 CA 証明書を CA から受け取る必要があります。
- 関連するルートおよび中間CA証明書を信頼できる証明書ストアにインポートします（**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**）。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]** を選択します。

CA 署名付き証明書に CSR をバインドするノードの隣にあるチェックボックスをオンにします。

ステップ 2 [バインド（Bind）] をクリックします。

ステップ 3 [参照（Browse）] をクリックし、CA 署名付き証明書を選択します。

ステップ 4 証明書の [フレンドリ名（Friendly Name）] を指定します。

ステップ 5 Cisco ISE に証明書の拡張の検証を許可する場合は、[証明書の拡張の検証（Validate Certificate Extensions）] チェックボックスをオンにします。

[証明書の拡張の検証（Validate Certificate Extensions）] オプションが有効になっており、インポートする証明書にCA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。

（注） ISE では、EAP-TLS クライアント証明書にデジタル署名キー使用拡張を使用する必要があります。

ステップ 6 この証明書が使用領域で使用されるサービスを確認します。

この情報は、CSR の生成時に [使用方法（Usage）] オプションを有効にした場合は自動入力されます。 証明書のバインディング時に使用方法を指定しない場合は、[使用方法（Usage）] オプションをオフにします。後で証明書を編集し、使用方法を指定できます。

（注） プライマリ PAN の管理者ロール証明書の証明書を変更すると、他のすべてのノードのサービスが再起動します。

プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。プライマリ管理ノード（PAN）の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

ステップ 7 [送信（Submit）] をクリックし、CA 署名付き証明書をバインドします。

Cisco ISE ノード間通信にこの証明書を使用するように選択した場合、Cisco ISE ノードでアプリケーションサーバが再起動されます。

他のノードで CA 署名付き証明書に CSR をバインドするために、このプロセスを繰り返します。

次のタスク

信頼できる証明書ストアへのルート証明書のインポート （177 ページ）

証明書署名要求のエクスポート

このページを使用して、証明書署名要求をエクスポートすることができます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 [OK] をクリックして、クライアントブラウザを実行しているファイルシステムにファイルを保存します。

証明書署名要求の設定

Cisco ISE では、1 つの要求で、管理者ポータルから展開内のすべてのノードの CSR を生成することができます。また、展開内の単一ノードまたは複数両方のノードのどちらの CSR を生成するのか選択することもできます。単一ノードの CSR を生成する場合、ISE は証明書サブジェクトの [CN=] フィールドの特定ノードの完全修飾ドメイン名（FQDN）を自動的に置き換えます。証明書の [サブジェクト代替名（Subject Alternative Name (SAN)）] フィールドにエントリを含めることを選択した場合、他の SAN 属性に加えて ISE ノードの FQDN を入力する必要があります。展開内のすべてのノードの CSR を生成することを選択した場合は、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] チェックボックスをオンにして、[SAN] フィールド（DNS 名）にワイルドカード表記で FQDN を入力します（*.amer.example.com など）。EAP 認証に証明書を使用する場合は、[CN=] フィールドにワイルドカード値を入力しないでください。

ワイルドカード証明書を使用することにより、各 Cisco ISE ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用すると、展開内の複数の両方のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバ証明書を割り当てる場合よりも安全性が低いと見なされます。

次の表に、認証局（CA）が署名可能な証明書署名要求（CSR）の生成に使用できる [証明書署名要求（Certificate Signing Request）] ページのフィールドを示します。このページのナビゲーション パスは **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書管理（Certificate Management）]** > **[証明書署名要求（Certificate Signing Request）]** です。

表 *19 :* 証明書署名要求の設定

フィールド	使用上のガイドライン
証明書の用途（**Certificate(s) will be used for**）	

フィールド	使用上のガイドライン
	証明書を使用するサービスを選択します。 **Cisco ISE ID 証明書** • [複数使用（Multi-Use）]：複数のサービス（管理者、EAP-TLS 認証、pxGrid、およびポータル）に使用されます。複数使用の証明書は、クライアントとサーバ両方のキーの用途を使用します。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [管理者（Admin）]：サーバ認証に使用されます（管理者ポータルとの通信および展開内の ISE ノード間の通信を保護するため）。署名 CA の証明書テンプレートは、Web サーバ証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） • [EAP 認証（EAP Authentication）]：サーバ認証に使用されます。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） （注） EAP-TLS クライアント証明書にデジタル署名キー使用法を使用する必要があります。 • [RADIUS DTLS]：RADIUS DTLS サーバの認証に使用されます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） • [ポータル（Portal）]：サーバ認証に使用されます（すべての ISE Web

フィールド	使用上のガイドライン
	ポータルとの通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） • [pxGrid]：クライアント認証とサーバ認証の両方に使用されます（pxGrid クライアントとサーバ間の通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） （注） 拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用しないことをお勧めします。拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用する場合、証明書は無効と見なされ、次のエラー メッセージが表示されます。 `source=local ; type=fatal ; message="unsupported certificate"` **Cisco ISE 認証局証明書**

フィールド	使用上のガイドライン
	• [ISE ルート CA（ISE Root CA）]：（内部 CA サービスにのみ適用可能）プライマリ PAN のルート CA および PSN の下位 CA を含む内部 CA 証明書チェーン全体を再生成するために使用されます。 • [ISE 中間 CA（ISE Intermediate）]：（ISE が外部 PKI の中間 CA として機能する場合に内部 CA サービスにのみ適用可能）プライマリ PAN の中間 CA 証明書および PSN の下位 CA 証明書の生成に使用されます。署名 CA の証明書テンプレートは、下位認証局と呼ばれます。このテンプレートには、次のプロパティがあります。 • [基本制約（Basic Constraints）]：重要、認証局 • [キーの用途（Key Usage）]：証明書の署名、デジタル署名 • [キーの拡張用途（Extended Key Usage）]：OCSP 署名（1.3.6.1.5.5.7.3.9） • [ISE OCSP 応答側証明書の更新（Renew ISE OCSP Responder Certificates）]：（内部 CA サービスにのみ適用可能）展開全体の ISE OCSP 応答側証明書の更新に使用されます（証明書署名要求ではありません）。セキュリティ上の理由から、ISE OCSP 応答側証明書を 6 ヵ月ごとに更新することを推奨します。
ワイルドカード証明書の許可（Allow Wildcard Certificates）	証明書の [SAN] フィールドの CN/DNS 名にワイルドカード文字（*）を使用するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、展開内のすべてのノードが自動的に選択されます。左端のラベルの位置にアスタリスク（*）ワイルドカード文字を使用する必要があります。ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、セキュリティ問題が発生する可能性があります。
これらのノードの CSR の生成（Generate CSRs for these Nodes）	証明書を生成するノードの隣のチェックボックスをオンにします。展開内の選択されたノードの CSR を生成するには、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオフにします。
Common Name（CN）	デフォルトでは、一般名は CSR を生成する ISE ノードの FQDN です。$FQDN$ は ISE ノードの FQDN を意味します。展開内の複数ノードの CSR を生成すると、CSR の [一般名（Common Name）] フィールドは各 ISE ノードの FQDN に置き換えられます。
Organizational Unit（OU）	組織ユニット名。Engineering など。
Organization（O）	組織名。Cisco など。

フィールド	使用上のガイドライン
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。
Country（C）	国名。2 文字の ISO 国番号を入力する必要があります。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	証明書に関連付けられている IP アドレス、DNS 名、Uniform Resource Identifier（URI）、またはディレクトリ名。 • [DNS 名（DNS Name）]：DNS 名を選択した場合は、ISE ノードの完全修飾ドメイン名を入力します。[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオンにした場合は、ワイルドカード表記（ドメイン名の前にアスタリスクとピリオドを入力）を指定します。*.amer.example.com など。 • [IP アドレス（IP Address）]：証明書に関連付けられる ISE ノードの IP アドレス。 • [Uniform Resource Identifier]：証明書に関連付ける URI。 • [ディレクトリ名（Directory Name）]：RFC 2253 に従って定義される識別名（DN）の文字列表現。DN 間はカンマ（,）で区切ります。「dnQualifier」RDN の場合は、カンマをエスケープし、区切り文字としてバックスラッシュ カンマ「\,」を使用します。たとえば、CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL などです。
キー タイプ	RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。

フィールド	使用上のガイドライン
キーの長さ（Key Length）	公開キーのビット サイズを指定します。 RSA には、次のオプションを使用できます。 • 512 • 1024 • 2048 • 4096 ECDSA には、次のオプションを使用できます。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。 パブリック CA の署名付き証明書を取得するか、FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は 2048 以上を選択します。
署名するダイジェスト（Digest to Sign With）	ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。
証明書ポリシー（Certificate Policies）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。

関連トピック

証明書署名要求 （185 ページ）
証明書署名要求の作成と認証局への CSR の送信 （185 ページ）
CSR への CA 署名付き証明書のバインド （185 ページ）

ポータルで使用する証明書のセットアップ

Web ポータル要求を処理できる展開に複数のポリシー サービス ノード（PSN）がある場合、Cisco ISE には一意の ID が必要です。この ID で、ポータルの通信に使用する必要がある証明書を識別します。ポータルでの使用に指定された証明書を追加またはインポートする場合、証明書グループ タグを定義して、それを展開内の各ノードの対応する証明書に関連付ける必要があります。この証明書グループ タグを対応するエンドユーザ ポータル（ゲスト、スポンサー、およびパーソナル デバイス ポータル）に関連付ける必要があります。この証明書グループ タグは一意の ID で、Cisco ISE が各ポータルと通信する際に使用する必要がある証明書を識別する場合に役立ちます。ポータルごとに各ノードから 1 つの証明書を指定できます。

（注） Cisco ISE は TCP ポート 8443（またはポータルが使用するように設定したポート）でポータル証明書を提示します。

ステップ 1 証明書署名要求の作成と認証局への CSR の送信 （185 ページ）。

すでに定義済みの証明書グループ タグを選択するか、ポータル用に新しく作成する必要があります。たとえば、mydevicesportal などです。

ステップ 2 信頼できる証明書ストアへのルート証明書のインポート （177 ページ）。

ステップ 3 CSR への CA 署名付き証明書のバインド （185 ページ）。

CA 署名付き証明書へのデフォルトのポータル証明書グループ タグの再割り当て

デフォルトでは、すべての Cisco ISE ポータルは自己署名証明書を使用します。ポータルに CA 署名付き証明書を使用する場合は、デフォルトのポータル証明書グループ タグを CA 署名付き証明書に割り当てることができます。既存の CA 署名付き証明書を使用するか、または CSR を生成して、ポータルに使用する新しい CA 署名付き証明書を取得できます。1 つの証明書から別の証明書にポータル グループ タグを再割り当てすることができます。

（注） 既存の証明書を編集する場合、証明書に関連付けられているポータル タグ（ゲスト）がいずれかのポータルですでに使用されている場合は、デフォルトのポータル証明書グループ タグまたは他のポータル グループ タグをこの証明書に再割り当てすることはできません。「ゲスト」ポータル タグを使用しているポータルのリストが表示されます。

次に、CA 署名付き証明書にデフォルトのポータル証明書グループ タグを再割り当てする手順について説明します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

このタグを使用するポータルのリストを表示するには、デフォルトのポータル証明書グループ タグの横にある i アイコンにマウス ポインタを合わせます。このタグが割り当てられているポータル証明書がある展開内の ISE ノードを表示することもできます。

ステップ 2 ポータルに使用する CA 署名付き証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

いずれのポータルでも使用されていない CA 署名付き証明書を選択してください。

ステップ 3 [使用方法（Usage）] 領域で、[ポータル（Portal）] チェックボックスをオンにして、デフォルトのポータル証明書グループ タグを選択します。

ステップ 4 [保存（Save）] をクリックします。

警告メッセージが表示されます。

ステップ 5 [はい（Yes）] をクリックして、CA 署名付き証明書にデフォルトのポータル証明書グループ タグを再割り当てします。

ノードの登録前のポータル証明書タグの関連付け

展開内のすべてのポータルに「デフォルト ポータル証明書グループ」タグを使用する場合は、新しい ISE ノードを登録する前に、関連する CA 署名付き証明書をインポートし、サービスとして「ポータル」を選択し、この証明書に「デフォルト ポータル証明書グループ」タグを関連付けます。

展開に新しいノードを追加すると、デフォルトの自己署名証明書が「デフォルト ポータル証明書グループ」タグに関連付けられ、このタグを使用するようにポータルが設定されます。

新しいノードの登録後、証明書グループ タグの関連付けは変更できません。したがって、展開にノードを登録する前に、次を実行してください。

ステップ 1 自己署名証明書を作成し、サービスとして「ポータル」を選択し、別の証明書グループ タグ（たとえば、tempportaltag）を割り当てます。

ステップ 2 新しく作成した証明書グループ タグ（tempportaltag）を使用するようにポータル設定を変更します。

ステップ 3 デフォルト自己署名証明書を編集し、ポータル ロールを削除します。

このオプションは、デフォルト ポータル証明書グループ タグとデフォルト自己署名証明書との関連付けを削除します。

ステップ 4 次のいずれかを実行します。

オプション	説明
CSR の生成	CSR を生成するときは、次を実行します。 **1.** この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。 **2.** CSR を CA に送信し、署名付きの証明書を取得します。 **3.** 信頼できる証明書ストアに証明書に署名した CA のルートおよび他の中間証明書をインポートします。 **4.** CSR に CA 署名付き証明書をバインドします。
秘密キーと CA 署名付き証明書のインポート	CA 署名付き証明書をインポートするときは、次を実行します。 **1.** この証明書を使用する「ポータル」をサービスとして選択し、「デフォルト ポータル証明書グループ」タグを関連付けます。

オプション	説明
	2. 信頼できる証明書ストアに証明書に署名した CA のルートおよび他の中間証明書をインポートします。
既存の CA 署名付き証明書の編集	既存の CA 署名付き証明書を編集するときは、次を実行します。 この証明書を使用する「ポータル」をサービスとして選択し、「デフォルトポータル証明書グループ」タグを関連付けます。

ステップ 5 展開に ISE ノードを登録します。
展開内のポータル構成は「デフォルト ポータル証明書グループ」タグに設定され、ポータルは新しいノードの「デフォルト ポータル証明書グループ」タグに関連付けられた CA 署名付き証明書を使用するように設定されます。

ユーザおよびエンドポイントの証明書の更新

デフォルトでは、Cisco ISE は証明書が期限切れになったデバイスからの要求を拒否します。ただし、このデフォルト動作を変更し、このような要求を処理し、ユーザに証明書の更新を求めるように ISE を設定できます。

ユーザが証明書を更新することを許可する場合は、要求をさらに処理する前に証明書が更新されたかどうかを判断する許可ポリシールールを設定することを推奨します。証明書が期限切れになったデバイスからの要求を処理することで、潜在的なセキュリティ脅威が発生する可能性があります。組織のセキュリティが侵害されていないことを保証するには、適切な許可プロファイルおよびルールを設定する必要があります。

あるデバイスは有効期限の前後に証明書を更新できます。ただし、Windows デバイスでは、期限切れになる前にだけ証明書を更新できます。Apple iOS、Mac OSX、および Android デバイスでは、有効期限の前または後に証明書を更新できます。

ポリシー条件で証明書更新に使用されるディクショナリ属性

Cisco ISE 証明書ディクショナリには、ユーザに証明書更新を許可するポリシー条件で使用される次の属性が含まれます。

- [有効期限までの日数（Days to Expiry）]：この属性は、証明書が有効な日数を指定します。この属性を使用して、許可ポリシーで使用できる条件を作成できます。この属性には、0 ～ 15 の値を指定できます。0 の値は、証明書の有効期限がすでに切れていることを示します。1 の値は、証明書の有効期限が切れるまで 1 日未満であることを示します。
- [有効期限切れ（Is Expired）]：このブール属性は、証明書が有効期限切れかどうかを示します。証明書の有効期限が近く、有効期限切れではない場合にのみ証明書更新を許可する場合は、許可ポリシー条件でこの属性を使用します。

証明書更新用の許可ポリシー条件

許可ポリシーでCertRenewalRequiredの単純条件（デフォルトで使用可能）を使用すると、Cisco ISE が要求を処理する前に証明書（有効期限切れまたはまもなく有効期限が切れる）を更新できます。

証明書を更新するための CWA リダイレクト

ユーザ証明書が期限切れになる前に失効している場合、Cisco ISE は、CA がパブリッシュした CRL をチェックして認証要求を拒否します。失効した証明書の期限が切れている場合は、CA が CRL でこの証明書をパブリッシュしない可能性があります。このシナリオでは、失効した証明書が Cisco ISE によって更新される可能性があります。このことを避けるために、証明書を更新する前に、要求が中央 Web 認証（CWA）にリダイレクトされ、完全認証が実行されるようにします。CWA のユーザをリダイレクトするには、許可プロファイルを作成する必要があります。

ユーザによる証明書の更新を許可する Cisco ISE の設定

ユーザが証明書を更新できるように Cisco ISE を設定するには、この手順で示すタスクを実行する必要があります。

始める前に

WLC で制限されたアクセス ACL を設定して、CWA 要求をリダイレクトします。

ステップ 1 許可されるプロトコルの設定の更新 （197 ページ）

ステップ 2 CWA リダイレクションの許可ポリシー プロファイルの作成 （198 ページ）

ステップ 3 証明書を更新する許可ポリシー ルールの作成 （199 ページ）

ステップ 4 ゲスト ポータルでの BYOD 設定の有効化 （199 ページ）

許可されるプロトコルの設定の更新

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）] > [デフォルト ネットワーク アクセス（Default Network Access）]** を選択します。

ステップ 2 PEAP および EAP-FAST プロトコルの EAP-TLS プロトコルおよび EAP-TLS 内部方式の下の [許可ポリシーの証明書更新を可能にするために失効した証明書の認証を許可（Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy）] チェックボックスをオンにします。

EAP-TLS プロトコルを使用する要求が NSP フローを通過します。

PEAP および EAP-FAST プロトコルについては、要求を処理するように Cisco ISE 向け Cisco AnyConnect を手動で設定する必要があります。

ステップ 3 [送信（Submit）] をクリックします。

次のタスク

CWA リダイレクションの許可ポリシー プロファイルの作成 （198 ページ）

CWA リダイレクションの許可ポリシー プロファイルの作成

始める前に

WLC で制限されたアクセス ACL が設定されていることを確認します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 許可プロファイルの名前を入力します。たとえば、CertRenewal_CWA です。

ステップ 4 [共通タスク（Common Tasks）] 領域の [Web リダイレクション（CWA、DRW、MDM、NSP、CPP）（Web Redirection (CWA, DRW, MDM, NSP, CPP)）] チェックボックスをオンにします。

ステップ 5 ドロップダウン リストの [中央集中 Web 認証（Centralized Web Auth）] および制限されたアクセス ACL を選択します。

ステップ 6 [証明書更新メッセージの表示（Display Certificates Renewal Message）] チェックボックスをオンにします。

url-redirect 属性値が変更され、この値に証明書が有効である日数が含まれます。

ステップ 7 [送信（Submit）] をクリックします。

（注） Cisco ISE 1.2 で無線デバイスの次のデバイス登録 WebAuth（DRW）ポリシーを設定している場合：

- 条件 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) およびプロファイル = Wireless-drw-redirect を含む DRW-Redirect ポリシー
- 条件 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) およびプロファイル = Wireless-Permit を含む DRW-Allow ポリシー

ISE 1.3 以上のバージョンにアップグレードした後は、DRW-Allow ポリシー条件を次のように更新する必要があります。

- 条件 = (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow) およびプロファイル = Wireless-Permit

次のタスク

証明書を更新する許可ポリシー ルールの作成 （199 ページ）

証明書を更新する許可ポリシー ルールの作成

始める前に

中央 Web 認証リダイレクションの許可プロファイルが作成されていることを確認します。

[管理（Administration）]>[システム（System）]>[設定（Settings）]>[ポリシーセット（Policy Sets）] でポリシー セットを有効にします。

ステップ 1 **[ワーク センター（Work Centers）]>[デバイス管理（Device Administration）]>[ポリシー セット（Policy Sets）]** を選択します。

ステップ 2 [上を作成（Create Above）] をクリックします。

ステップ 3 新しいルールの名前を入力します。

ステップ 4 次の単純条件と結果を選択します。

CertRenewalRequired EQUALS True の場合は、権限用に以前に作成した許可プロファイル（CertRenewal_CWA）を選択します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

証明書が期限切れになったデバイスを持つ企業ネットワークにアクセスした場合は、[更新（Renew）] をクリックして、デバイスを再設定します。

ゲスト ポータルでの BYOD 設定の有効化

ユーザがパーソナル デバイス証明書を更新できるようにするには、選択したゲスト ポータルで BYOD 設定を有効にする必要があります。

ステップ 1 **[ワークセンター（Work Center）]>[ゲストアクセス（Guest Access）]>[ポータルとコンポーネント（Portals & Components）]>[ゲストポータル（Guest Portals）]** を選択します。

a) 目的の CWA ポータルを選択して、[編集（Edit）] をクリックします。

ステップ 2 [BYOD 設定（BYOD Settings）] から [従業員にネットワークでのパーソナルデバイスの使用を許可する（Allow employees to use personal devices on the network）] チェックボックスをオンにします。

ステップ 3 **[保存（Save）]** をクリックします。

Apple iOS デバイスの証明書更新の失敗

ISE を使用して Apple iOS デバイスのエンドポイント証明書を更新する場合、「プロファイル済みでインストールできませんでした（Profiled Failed to Install）」エラー メッセージが表示される場合があります。このエラー メッセージは、同じポリシー サービス ノード（PSN）または別の PSN で、期限切れ間近または期限切れのネットワーク プロファイルが更新のプロセス時に使用されるものとは異なる管理者 HTTPS 証明書によって署名されている場合に表示されます。

回避策としては、展開内のすべての PSN で管理者 HTTPS 用にマルチドメイン SSL 証明書（通称 Unified Communications Certificates（UCC））またはワイルドカード証明書を使用します。

証明書のステータス（OCSP または CRL）を確認します。

Cisco ISE は、証明書失効リスト（CRL）を定期的にチェックします。このページを使用して、自動的にダウンロードされた CRL に対して進行中のセッションをチェックするように Cisco ISE を設定できます。OCSP または CRL のチェックを毎日開始する時刻と、OCSP サーバまたは CRL を再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定できます。

次の表では、[証明書定期チェックの設定（Certificate Periodic Check Settings）] ページのフィールドについて説明します。このページを使用して、証明書（OCSP または CRL）のステータスをチェックする時間間隔を指定できます。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [証明書定期チェックの設定（Certificate Periodic Check Settings）]** です。

表 ***20 :*** **証明書定期チェックの設定**

フィールド名	使用上のガイドライン
証明書チェックの設定	
自動的に取得されたCRLに対する進行中のセッションのチェック（Check ongoing sessions against automatically retrieved CRL）	Cisco ISE が自動的にダウンロードされた CRL に対する進行中のセッションをチェックするようにするには、このチェックボックスをオンにします。
CRL/OCSP の定期的な証明書チェック	
最初のチェック時刻（First check at）	CRL または OCSP のチェックを毎日開始する時刻を指定します。00:00 ～ 23:59 の時間範囲の値を入力します。
チェック間隔（Check every）	CRL または OCSP サーバを再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定します。

関連トピック

OCSP サービス （235 ページ）
OCSP クライアント プロファイルの追加 （237 ページ）

Cisco ISE CA サービス

証明書は、自己署名したり、外部の認証局（CA）がデジタルで署名したりできます。Cisco ISE 内部認証局（ISE CA）は、従業員が企業ネットワークでパーソナル デバイスを使用できるように、一元的なコンソールからエンドポイントのデジタル証明書を発行し、管理します。CA 署名付きデジタル証明書は、業界標準であり、よりセキュアです。プライマリ PAN は、ルート CA です。ポリシー サービス ノード（PSN）は、プライマリ PAN の下位 CA です（SCEP RA）。ISE CA には次の機能があります。

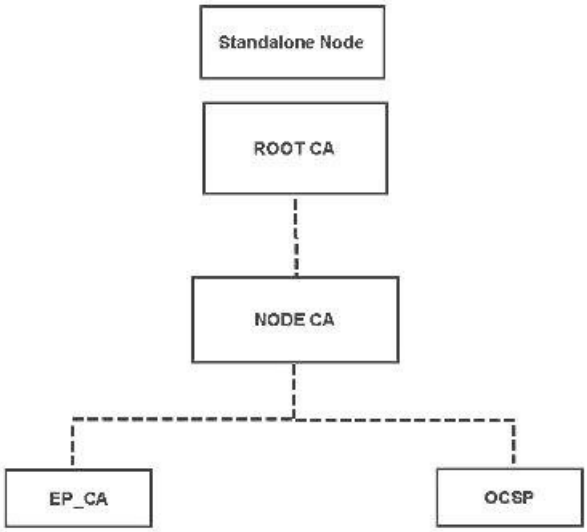
- 証明書の発行：ネットワークに接続するエンドポイントの証明書署名要求（CSR）を検証し、署名します。
- キー管理：PAN ノードと PSN ノードの両方でキーと証明書を生成し、セキュアに保存します。
- 証明書ストレージ：ユーザやデバイスに発行された証明書を保存します。
- Online Certificate Status Protocol（OCSP）サポート：OCSP 応答側に証明書の有効性を確認する手段を提供します。

CA サービスがプライマリ管理ノードで無効になっている場合でも、CA サービスはセカンダリ管理ノードの CLI で実行中として表示されます。理想的には、CA サービスは無効として表示される必要があります。これは、Cisco ISE の既知の問題です。

管理ノードとポリシー サービス ノードでプロビジョニングされる ISE CA 証明書

インストール後に、Cisco ISE ノードはルート CA 証明書およびノード CA 証明書でプロビジョニングされ、エンドポイントの証明書が管理されます。

図 *5:* スタンドアロン ノードでプロビジョニングされる *ISE CA* 証明書

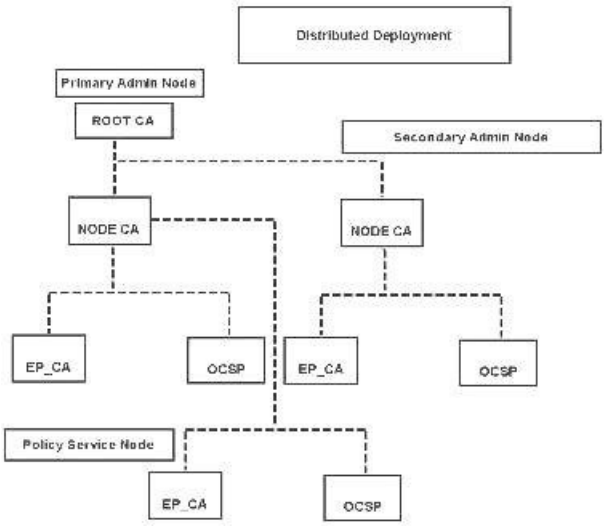


展開をセットアップすると、プライマリ管理ノード（PAN）として指定したノードがルート CA になります。PAN には、ルート CA 証明書と、ルート CA によって署名されたノード CA 証明書があります。

PAN にセカンダリ管理ノードを登録すると、ノード CA 証明書が生成され、プライマリ管理ノードでルート CA によって署名されます。

PAN に登録したポリシー サービス ノード（PSN）には、エンドポイント CA と、PAN のノード CA によって署名された OCSP 証明書がプロビジョニングされます。ポリシー サービス ノード（PSN）は、PAN の下位 CA です。ISE CA を使用すると、PSN のエンドポイント CA によってネットワークにアクセスするエンドポイントに証明書が発行されます。

図 *6:* 展開内の管理ノードおよびポリシー サービス ノードでプロビジョニングされる *ISE CA* 証明書



ISE CA チェーンの再生成

Cisco ISE CA チェーンを再生成すると、ルート CA、ノード CA、およびエンドポイント CA 証明書を含むすべての証明書が再生成されます。PAN または PSN のドメイン名またはホスト名を変更すると、ISE CA チェーンを再生する必要があります。以前のリリースから 2.0 以降にアップグレードするときには、2 つのルート階層から 1 つのルート階層に移行するように ISE CA チェーンを再生成することをお勧めします。

楕円曲線暗号化証明書のサポート

Cisco ISE CA サービスが、楕円曲線暗号化（ECC）アルゴリズムに基づく証明書をサポートするようになりました。ECC は、より小さいキー サイズを使用している場合でも、他の暗号化アルゴリズムよりも高いセキュリティとパフォーマンスを提供します。

次の表では、ECC および RSA のキー サイズとセキュリティ強度を比較しています。

ECC のキー サイズ（ビット単位）	RSA のキー サイズ（ビット単位）
160	1024
224	2048
256	3072
384	7680
521	15360

キー サイズが小さいため、暗号化が迅速になります。

Cisco ISE では、次の ECC 曲線タイプがサポートされています。曲線タイプまたはキー サイズが大きくなると、セキュリティが強化されます。

- P-192
- P-256
- P-384
- P-521

ISE は、証明書の EC 部分の明示的なパラメータをサポートしていません。明示的なパラメータで証明書をインポートしようとすると、「証明書の検証に失敗しました」というエラーが表示されます。名前付き ECParameters のみがサポートされています。

Cisco ISE CA サービスは、BYOD フローを介して接続するデバイスの ECC 証明書をサポートします。また、証明書プロビジョニング ポータルから ECC 証明書を生成することもできます。

（注） 次の表に、ECC をサポートしているオペレーティング システムおよびバージョンと、サポートされている曲線タイプを示します。デバイスがサポートされているオペレーティング システムを実行していない場合、またはサポートされているバージョンでない場合には、代わりに RSA ベースの証明書を使用することもできます。

オペレーティング システム（Operating System）	サポートされるバージョン	サポートされる曲線タイプ
Windows	8 以降	P-256、P-384、P-521
Android	4.4 以降 （注） Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ（P-192 曲線タイプをサポートしていない Android 6.0 を除く）。

Windows 7 と Apple iOS は、EAP-TLS を介した認証用の ECC をネイティブでサポートしていません。Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

Enrollment over Secure Transport（EST）プロトコルを備えた BYOD フローが適切に機能しない場合は、次のことを確認します。

- 証明書サービス エンドポイント サブ CA 証明書チェーンが完全であること。証明書チェーンが完全かどうかを確認するには：
  1. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）] の順に選択します。
  2. 確認する証明書の横にあるチェック ボックスをオンにして、[表示（View）]をクリックします。
- CA および EST サービスが起動し、実行されていることを確認します。サービスが実行されていない場合は、[管理（Administration）]>[システム（System）]>[証明書（Certificates）] > [認証局（Certificate Authority）] > [内部CAの設定（Internal CA Settings）] に移動して CA サービスを有効にします。
- 2.0 以前の ISE バージョンから Cisco ISE 2.x にアップグレードしている場合は、アップグレード後に ISE ルート CA 証明書チェーンを置き換えます。手順は次のとおりです。
  1. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書署名要求（Certificate Signing Requests）] の順に選択します。

2. [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。
3. [1つ以上の証明書の使用先（one or more Certificates will be used for）] ドロップダウンリストから ISE ルート CA を選択します。
4. [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA Certificate Chain）] をクリックします。

（注） Cisco ISE のこのリリースでは、EST クライアントが Cisco ISE に存在する EST サーバに対して直接認証を行うことはサポートされていません。

Android または Windows エンドポイントでのオンボーディング時に、要求が ECC ベースの証明書用である場合には、ISE が EST フローをトリガーします。

Cisco ISE 認証局証明書

[認証局（CA）証明書（Certificate Authority (CA) Certificates）] ページには、内部 Cisco ISE CA に関連するすべての証明書が表示されます。以前のリリースでは、これらの CA 証明書は信頼できる証明書ストアにありましたが、現在は [CA 証明書（CA Certificates）] ページに移動しています。これらの証明書は、このページにノード方式で表示されます。ノードを展開して、その特定のノードの ISE CA 証明書をすべて表示することができます。プライマリおよびセカンダリ管理ノードには、ルート CA、ノード CA、下位 CA、OCSP レスポンダ証明書があります。展開内の他のノードには、エンドポイント下位 CA および OCSP 証明書があります。

Cisco ISE CA サービスを有効にすると、すべてのノードでこれらの証明書が自動的に生成され、インストールされます。また、ISE ルート CA チェーン全体を置き換えると、すべてのノードでこれらの証明書が自動的に再生成され、インストールされます。手動による介入は必要ありません。

Cisco ISE CA 証明書は **Certificate Services** <**エンドポイント サブ *CA*/ノード *CA*/ルート *CA*/*OCSP* レスポンダ**>-<ノードのホスト名>**#**証明書番号という命名規則に従います。

[CA 証明書（CA Certificates）] ページで Cisco ISE CA 証明書を編集、インポート、エクスポート、削除、表示できます。

Cisco ISE CA 証明書の編集

証明書を Cisco ISE CA 証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。.

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 必要に応じて編集可能なフィールドを変更します。フィールドの説明については、「証明書設定の編集」を参照してください。

ステップ 4 [保存（Save）] をクリックして、証明書ストアに対して行った変更を保存します。

Cisco ISE CA 証明書のエクスポート

Cisco ISE ルート CA およびノード CA 証明書をエクスポートするには、次の手順を実行します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 3 クライアント ブラウザを実行しているファイル システムに Privacy Enhanced Mail ファイルを保存します。

Cisco ISE CA 証明書のインポート

エンドポイントが別の展開の Cisco ISE CA によって発行された証明書を使用してネットワークへの認証を試みる場合、Cisco ISE ルート CA、ノード CA、エンドポイント サブ CA 証明書をその展開から Cisco ISE の信頼できる証明書ストアにインポートする必要があります。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ISE ルート CA、ノード CA、エンドポイント サブ CA 証明書を、エンドポイント証明書が署名されている展開からエクスポートし、ブラウザが実行されているコンピュータのファイル システムに保存します。

ステップ 1 エンドポイントが認証されている展開の管理者用ポータルにログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 3 [インポート（Import）] をクリックします。

ステップ 4 必要に応じてフィールドの値を設定します。詳細については、「信頼できる証明書のインポート設定」を参照してください。

クライアント証明書ベースの認証が有効である場合は、Cisco ISE により展開内の各ノードのアプリケーション サーバが再起動されます（最初に PAN のアプリケーション サーバが再起動され、続いて追加のノードのアプリケーション サーバが 1 つずつ再起動されます）。

証明書テンプレート

証明書テンプレートには、そのテンプレートに基づいて認証局（CA）によって発行されたすべての証明書に共通のプロパティが含まれています。証明書テンプレートは、件名、サブジェクト代替名（SAN）、キー タイプ、キー サイズ、使用する必要がある SCEP RA プロファイル、証明書の有効期間、証明書がクライアントまたはサーバの認証またはその両方に使用される必要があるかどうかを指定した拡張キーの使用状況（EKU）を定義します。内部 Cisco ISE CA（ISE CA）は、証明書テンプレートを使用し、そのテンプレートに基づいて証明書を発行します。

Cisco ISE には、次の ISE CA のデフォルトの証明書テンプレートが付属しています。必要に応じて、追加の証明書テンプレートを作成できます。デフォルトの証明書テンプレートは次のとおりです。

- CA_SERVICE_Certificate_Template：Cisco ISE を認証局として使用するその他のネットワーク サービス用。たとえば、ASA VPN ユーザに対し証明書を発行するには、ISE の設定時にこの証明書テンプレートを使用します。この証明書テンプレートでは、有効期間のみを変更できます。
- EAP_Authentication_Certificate_Template：EAP 認証用。
- pxGrid_Certificate_Template：証明書プロビジョニング ポータルから証明書を生成するときの pxGrid コントローラ用。

証明書テンプレート名の拡張子

Cisco ISE の内部 CA には、エンドポイント証明書を作成するために使用された証明書テンプレートを表す拡張子が含まれています。内部 CA によって発行されたすべてのエンドポイント証明書には、証明書テンプレート名の拡張子が含まれています。この拡張子は、そのエンドポイント証明書を作成するために使用された証明書テンプレートを表します。拡張子の ID は 1.3.6.1.4.1.9.21.2.5 です。CERTIFICATE: テンプレート名属性を許可ポリシーの条件に使用して、評価の結果に基づいて適切なアクセス権限を割り当てることができます。

許可ポリシー条件での証明書テンプレート名の使用

許可ポリシー ルールで証明書テンプレート名の拡張子を使用できます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー セット（Policy Sets）]** を選択し、許可ポリシー ルールを表示するデフォルトのポリシー セットを展開します。

ステップ 2 新しいルールを追加するか、既存のルールを編集します。次に、Compliant_Device_Access ルールを編集する例を示します。

a) Compliant_Device_Access ルールを編集します。
b) [属性/値の追加（Add Attribute/Value）] を選択します。
c) ディクショナリから、**CERTIFICATE: Template Name** 属性と **Equals** 演算子を選択します。
d) 証明書テンプレート名の値を入力します。たとえば、EAP_Authentication_Certificate_Template などです。

ステップ 3 [保存（Save）] をクリックします。

pxGrid コントローラ用の Cisco ISE CA 証明書の展開

Cisco ISE CA は、証明書プロビジョニング ポータルから証明書を生成するための pxGrid コントローラの証明書テンプレートを提供します。

始める前に

pxGrid クライアントの証明書署名要求（CSR）を生成し、CSR の内容をクリップボードにコピーします。

ステップ 1 ネットワーク アクセス ユーザ アカウントを作成します（[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] > [追加（Add）]）。

ユーザが割り当てられているユーザ グループをメモします。

ステップ 2 証明書プロビジョニング ポータルの設定を編集します（[管理（Administration）]>[デバイス ポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）]）。

a) 証明書プロビジョニング ポータルを選択して、[編集（Edit）] をクリックします。
b) [ポータル設定（Portal Settings）] ドロップダウン リストをクリックします。[承認済みグループの設定（Configure authorized groups）] の選択可能なリストから、ネットワーク アクセス ユーザが属すユーザ グループを選択して、選択済みリストに移動します。
c) [証明書プロビジョニング ポータル設定（Certificate Provisioning Portal Settings）] ドロップダウン リストをクリックします。[pxGrid_Certificate_Template] を選択します。詳細については、「証明書プロビジョニング ポータルのポータル設定」を参照してください。
d) ポータル設定を保存します。

ステップ 3 証明書プロビジョニング ポータルを起動します。[ポータル テスト URL（Portal test URL）] リンクをクリックします。

a) 手順 1 で作成したユーザ アカウントを使用して証明書プロビジョニング ポータルにログインします。
b) AUP を受け入れ、[続行（Continue）] をクリックします。

c) [処理の選択（I want to）] ドロップダウン リストから、[単一の証明書の生成（証明書署名要求あり）（Generate a single certificate (with certificate signing request)）] を選択します。
d) [証明書署名要求の詳細（Certificate Signing Request Details）] フィールドに、クリップボードから CSR の内容を貼り付けます。
e) [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、[PKCS8 形式（PKCS8 format）] を選択します。

（注） [PKCS12 形式（PKCS12 format）] を選択する場合は、1 つの証明書ファイルを証明書ファイルとキー ファイルに分けて変換する必要があります。Cisco ISE にインポートする前に、証明書とキー ファイルはバイナリ DER エンコードまたは PEM 形式にする必要があります。

f) [証明書テンプレートの選択（Choose Certificate Template）] ドロップダウン リストから、[pxGrid_Certificate_Template] を選択します。
g) 証明書のパスワードを入力します。
h) [生成（Generate）] をクリックします。

証明書が生成されます。

i) 証明書をエクスポートします。

証明書チェーンとともに証明書がエクスポートされます。

ステップ 4 pxGrid クライアントの信頼できる証明書ストアに Cisco ISE CA チェーンをインポートします。

Simple Certificate Enrollment Protocol プロファイル

ユーザがネットワークで登録できるさまざまなモバイルデバイスの証明書のプロビジョニング機能を有効にするために、1 つ以上の Simple Certificate Enrollment Protocol（SCEP）認証局（CA）プロファイル（Cisco ISE 外部 CA 設定と呼ばれます）を設定して、Cisco ISE に複数の CA の場所を指定できます。複数のプロファイルを使用できる利点は、ハイアベイラビリティを実現し、指定した CA の場所の間でロード バランシングを実行できることです。特定の SCEP CA への要求に 3 回連続して応答がなかった場合、Cisco ISE は特定のサーバが使用不能であると宣言し、次に負荷が小さく応答時間が短い既知の CA に自動的に移動し、サーバがオンラインに復帰するまで、定期的なポーリングを開始します。

Microsoft SCEP サーバを Cisco ISE と相互運用するように設定する方法については、次を参照してください。

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf

発行された証明書

管理者ポータルには、内部 ISE CA によってエンドポイントに対して発行されたすべての証明書のリストが示されます（[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [エンドポイント証明書（Endpoint Certificates）]）。[発行された証明書（Issued Certificates）] ページでは、証明書ステータスを一目で確認できます。証明書が失効している場

合は、[ステータス（Status）] 列の上にマウス カーソルを移動すると、失効の理由を確認できます。[証明書テンプレート（Certificate Template）] 列の上にマウス カーソルを移動すると、キー タイプ、キー サイズ、曲線タイプ、サブジェクト、サブジェクト代替名（SAN）、証明書の有効性などの詳細情報を表示できます。エンドポイント証明書クリックして、証明書を表示できます。

ISE CA によって発行されたすべての証明書（BYOD フローを介して自動的にプロビジョニングされた証明書と証明書プロビジョニング ポータルから取得された証明書）は、[エンドポイント証明書（Endpoint Certificates）] ページにリストされます。このページからこれらの証明書を管理できます。

たとえばuser7に発行された証明書を確認する場合は、[フレンドリ名（Friendly Name）] フィールドの下に表示されるテキスト ボックスに 「user7」 と入力します。このユーザに Cisco ISE によって発行されたすべての証明書が表示されます。フィルタをキャンセルするには、テキスト ボックスから検索語を削除します。また、[拡張フィルタ（Advanced Filter）] オプションを使用して、さまざまな検索基準に基づいてレコードを表示することもできます。

この [エンドポイント証明書（Endpoint Certificates）] ページには、必要に応じてエンドポイント証明書を取り消すためのオプションもあります。

[証明書管理概要（Certificate Management Overview）] ページには、展開内の各 PSN ノードによって発行されたエンドポイント証明書の合計数が表示されます。また、失効した証明書の合計数と失敗した証明書の合計数をノードごとに確認することもできます。このページのデータは任意の属性に基づいてフィルタリングできます。

発行および失効した証明書

次の表で、[発行および失効した証明書の概要（Overview of Issued and Revoked Certificates）] ページのフィールドについて説明します。展開内の PSN ノードがエンドポイントに証明書を発行します。このページでは、展開内の各 PSN ノードが発行するエンドポイント証明書に関する情報を示します。このページへのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[概要（Overview）]** です。

表 *21 :* 発行された証明書と失効した証明書

フィールド	使用上のガイドライン
ノード名	証明書を発行したポリシー サービス ノード（PSN）の名前。
[発行された証明書（Certificates Issued）]	PSN ノードが発行したエンドポイント証明書の数。
[取り消された証明書（Certificates Revoked）]	失効したエンドポイント証明書（PSN ノードが発行した証明書）の数。

フィールド	使用上のガイドライン
[証明書要求（Certificates Requests）]	PSN ノードが処理した証明書ベースの認証要求の数。
[失敗した証明書（Certificates Failed）]	PSN ノードが処理する失敗した認証要求の数。

関連トピック

発行された証明書 （209 ページ）
ユーザおよびエンドポイントの証明書の更新 （196 ページ）
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 （214 ページ）
ユーザによる証明書の更新を許可する Cisco ISE の設定 （197 ページ）
エンドポイント証明書の失効 （235 ページ）

Cisco ISE CA 証明書およびキーのバックアップと復元

PPAN に障害が発生し、セカンダリ管理ノードを外部 PKI のルート CA または中間 CA として機能させるために昇格する場合に備え、Cisco ISE CA 証明書およびキーをセキュアにバックアップして、セカンダリ管理ノードにこれらを復元できるようにする必要があります。Cisco ISE 設定のバックアップには、CA 証明書とキーは含まれていません。CA 証明書およびキーをリポジトリにエクスポートおよびインポートするには、代わりにコマンドラインインターフェイス（CLI）を使用する必要があります。**application configure ise** コマンドには、CA 証明書およびキーのバックアップと復元のためのエクスポートおよびインポートのオプションが含まれています。

信頼できる証明書ストアからの次の証明書が、セカンダリ管理ノードで復元されます。

- Cisco ISE ルート CA 証明書
- Cisco ISE サブ CA 証明書
- Cisco ISE エンドポイント RA 証明書
- Cisco ISE OCSP 応答側証明書

次の場合、Cisco ISE CA 証明書およびキーのバックアップおよび復元が必要となります。

- 展開内にセカンダリ管理ノードが存在する
- Cisco ISE CA ルート チェーン全体を置き換える
- 外部 PKI の下位 CA として機能するように Cisco ISE ルート CA を設定する
- リリース 1.2 からそれ以降のリリースにアップグレードする

- 設定のバックアップからデータを復元する。この場合、最初にCisco ISE CAルートチェーンを再生成し、次に ISE CA 証明書およびキーのバックアップと復元を行う必要があります。

Cisco ISE CA 証明書およびキーのエクスポート

CA 証明書およびキーを PAN からエクスポートし、セカンダリ管理ノードでインポートする必要があります。このオプションでは、PANがダウンした場合にセカンダリ管理ノードでエンドポイントの証明書を発行および管理し、セカンダリ管理ノードを PAN に昇格させることができます。

始める前に

CA 証明書およびキーを格納するためのリポジトリを作成したことを確認します。

ステップ 1 Cisco ISE CLI から、**application configure ise** コマンドを入力します。

ステップ 2 7 を入力して、証明書およびキーをエクスポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 暗号キーを入力します。

エクスポートされた証明書のリスト、件名、発行者、およびシリアル番号とともに成功メッセージが表示されます。

例：

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Cisco ISE CA 証明書およびキーのインポート

セカンダリ管理ノードを登録したら、PAN から CA 証明書およびキーをエクスポートし、セカンダリ管理ノードにインポートします。

ステップ 1 Cisco ISE CLI から、**application configure ise** コマンドを入力します。

ステップ 2 8 を入力して、CA 証明書およびキーをインポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 インポートするファイルの名前を入力します。ファイル名は **ise_ca_key_pairs_of_<vm hostname>** 形式である必要があります。

ステップ 5 ファイルを復号化するための暗号キーを入力します。

処理が正常に完了したことを知らせるメッセージが表示されます。

例：

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

プライマリ PAN および PSN でのルート CA および下位 CA の生成

展開をセットアップする場合、Cisco ISE は、プライマリ PAN でルート CA を生成し、ポリシーサービス ノード（PSN）で Cisco ISE CA サービスに対する下位 CA 証明書を生成します。ただし、プライマリ PAN または PSN のドメイン名またはホスト名を変更する場合は、プライマリ PAN でルート CA、PSN で下位 CA をそれぞれ再生成する必要があります。

PSN のホスト名を変更する場合は、プライマリ PAN および PSN でそれぞれルート CA と下位 CA を再生成する代わりに、ホスト名を変更する前に PSN を登録解除し、再登録できます。新しい下位証明書は PSN 上で自動的にプロビジョニングされます。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用先（Certificate(s) will be used for）] ドロップダウン リストから ISE ルート CA を選択します。

ステップ 4 [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA Certificate chain）] をクリックします。

ルート CA と下位 CA 証明書が、展開内のすべてのノードに対して生成されます。

次のタスク

展開にセカンダリ PAN がある場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN がルート CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

外部 PKI の下位 CA としての Cisco ISE ルート CA の設定

外部 PKI の下位 CA として機能するプライマリ PAN のルート CA が必要な場合は、ISE 中間 CA 証明書署名要求を生成して、外部 CA に送信し、ルートおよび CA 署名付き証明書を入手して、ルート CA 証明書を信頼できる証明書ストアにインポートし、CA 署名付き証明書を CSR にバインドします。この場合、外部 CA はルート CA、プライマリ PAN は外部 CA の下位 CA、PSN はプライマリ PAN の下位 CA です。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用目的（Certificate(s) will be used for）] ドロップダウン リストから [ISE 中間 CA（ISE Intermediate CA）] を選択します。

ステップ 4 [生成（Generate）] をクリックします。

ステップ 5 CSR をエクスポートし、外部 CA に送信して、CA 署名付き証明書を取得します。

ステップ 6 信頼できる証明書ストアに外部 CA のルート CA 証明書をインポートします。

ステップ 7 CSR に CA 署名付き証明書をバインドします。

次のタスク

展開にセカンダリ PAN がある場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN が外部 PKI の下位 CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定

ネットワークに接続するエンドポイント（パーソナルデバイス）の証明書を発行し、管理するように Cisco ISE を設定できます。内部 Cisco ISE 認証局（CA）サービスを使用して、エンド

ポイントから証明書署名要求（CSR）に署名したり、外部 CA に CSR を転送したりすることができます。

始める前に

- プライマリ PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、ディザスタ リカバリのため、安全な場所に保管してください。
- 展開にセカンダリ PAN がある場合は、プライマリ PAN から Cisco ISE CA 証明書およびキーをバックアップし、セカンダリ PAN で復元します。

ステップ 1 Employee ユーザ グループへのユーザの追加 （215 ページ）
内部 ID ストアまたは Active Directory などの外部 ID ストアにユーザを追加できます。

ステップ 2 TLS ベース認証の証明書認証プロファイルの作成 （216 ページ）

ステップ 3 TLS ベース認証の ID ソース順序の作成 （216 ページ）

ステップ 4 クライアント プロビジョニング ポリシーを作成します。

a) 認証局の設定 （217 ページ）
b) CA テンプレートの作成 （219 ページ）
c) クライアント プロビジョニング ポリシーで使用されるネイティブ サプリカント プロファイルの作成 （221 ページ）
d) Cisco サイトからの Windows および Mac OS X オペレーティング システムのエージェント リソースのダウンロード （222 ページ）
e) Apple iOS、Android および MACOSX デバイスのクライアント プロビジョニング ポリシー ルールの作成 （223 ページ）

ステップ 5 TLS ベース認証の Dot1X 認証ポリシー ルールの設定 （224 ページ）

ステップ 6 TLS ベース認証用の許可ポリシー ルールを設定します。

a) 中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成 （224 ページ）
b) 許可ポリシー ルールの作成 （225 ページ）

パーソナル デバイスからワイヤレス SSID に接続するときに ECC RSA ベースの証明書を使用すると、2 回目のパスワード入力を行うよう求められます。

Employee ユーザ グループへのユーザの追加

次の手順では、Cisco ISE ID ストアの Employee ユーザ グループにユーザを追加する方法について説明します。外部 ID ストアを使用した場合でも、ユーザを追加できる Employee ユーザ グループがあることを確認します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ユーザの詳細情報を入力します。

ステップ 4 [パスワード（Passwords）] セクションで、[ログインパスワード（Login Password）] と [TACACS+イネーブルパスワード（TACACS+ Enable Password）] を選択し、ネットワーク デバイスにアクセス レベルを設定します。

ステップ 5 [ユーザ グループ（User Group）] ドロップダウン リストから [従業員（Employee）] を選択します。

Employee ユーザ グループに属するすべてのユーザが同じ権限セットを共有します。

ステップ 6 [送信（Submit）] をクリックします。

次のタスク

TLS ベース認証の証明書認証プロファイルの作成 （216 ページ）

TLS ベース認証の証明書認証プロファイルの作成

ネットワークに接続するエンドポイントの認証に証明書を使用するには、Cisco ISE で証明書認証プロファイルを定義するか、またはデフォルトの Preloaded_Certificate_Profile を編集する必要があります。証明書認証プロファイルには、プリンシパルユーザ名として使用する必要がある証明書フィールドが含まれています。たとえば、ユーザ名が [一般名（Common Name）] フィールドにある場合は、証明書認証プロファイルを [プリンシパル ユーザ名（Principal Username）] が [サブジェクト - 一般名（Subject - Common Name）] であるとして定義できます。これは ID ストアに照らして確認できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [証明書認証プロファイル（Certificate Authentication Profile）]** を選択します。

ステップ 2 証明書認証プロファイルの名前を入力します。たとえば、CAP となります。

ステップ 3 [サブジェクト - 一般名（Subject - Common Name）] に [プリンシパル ユーザ名 X509 属性（Principal Username X509 Attribute）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

TLS ベース認証の ID ソース順序の作成 （216 ページ）

TLS ベース認証の ID ソース順序の作成

証明書認証プロファイルを作成したら、Cisco ISE が証明書の属性を取得し、定義した ID ソースを ID ソース順序で照合できるように、証明書認証プロファイルを ID ソース順序に追加します。

始める前に

次のタスクが完了していることを確認します。

- Employee ユーザ グループへのユーザの追加。
- 証明書ベースの認証の証明書認証プロファイルの作成。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ID ソース順序の名前を入力します。たとえば、Dot1X となります。

ステップ 4 [証明書認証プロファイルの選択（Select Certificate Authentication Profile）] チェックボックスをオンにし、作成した証明書認証プロファイル、つまり CAP を選択します。

ステップ 5 ユーザ情報を含む ID ソースを [認証検索リスト（Authentication Search List）] 領域の [選択済み（Selected）] リスト ボックスに移動します。

追加の ID ソースを追加すると、一致が見つかるまで Cisco ISE は、これらのデータ ストアを順に検索します。

ステップ 6 [ユーザが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）] オプション ボタンをクリックします。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

認証局の設定 （217 ページ）

認証局の設定

CSR への署名に外部 CA を使用する場合、外部 CA を設定する必要があります。外部 CA 設定は Cisco ISE の以前のリリースでは、SCEP RA プロファイルと呼ばれていました。Cisco ISE CA を使用する場合、CA 設定を明示的に設定する必要はありません。[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [内部 CA 設定（Internal CA Settings）] で、内部 CA 設定を確認できます。

ユーザのデバイスが検証済みの証明書を受信すると、証明書はデバイス上の次の表の場所に置かれます。

表 *22 :* デバイス証明書の場所

Device	証明書ストレージの場所	アクセス方式
iPhone/iPad	標準の証明書ストア	[設定（Settings）] > [一般（General）] > [プロファイル（Profile）]

Device	証明書ストレージの場所	アクセス方式
Android	暗号化された証明書ストア	エンドユーザに不可視です。 （注） 証明書は、[設定（Settings）] > [ロケーションおよびセキュリティ（Location & Security）] > [ストレージのクリア（Clear Storage）] を使用して削除できます。
Windows	標準の証明書ストア	**/cmd** プロンプトから mmc.exe を起動するか、または証明書スナップインで表示します。
Mac	標準の証明書ストア	[アプリケーション（Application）] > [ユーティリティ（Utilities）] > [キーチェーン アクセス（Keychain Access）]

始める前に

証明書署名要求（CSR）への署名に外部認証局（CA）を使用する場合は、外部 CA の URL が必要となります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [外部 CA 設定（External CA Settings）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 外部 CA 設定の名前を入力します。たとえば、EXTERNAL_SCEP などです。

ステップ 4 [URL] テキスト ボックスに、外部 CA サーバの URL を入力します。

外部 CA が到達可能かどうかを確認するには、[テスト接続（Test Connection）] をクリックします。追加 CA サーバの URL を入力するには、[+] ボタンをクリックします。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

CA テンプレートの作成 （219 ページ）

CA テンプレートの作成

証明書テンプレートは、（内部または外部 CA のために）使用する必要がある SCEP RA プロファイル、キー タイプ、キー サイズ、曲線タイプ、サブジェクト、サブジェクト代替名（SAN）、証明書の有効期間、拡張キーの使用状況を定義します。この例では、内部 Cisco ISE CA を使用すると想定します。外部 CA テンプレートの場合、有効期間は外部 CA によって決定され、指定することはできません。

新しい CA テンプレートを作成するか、デフォルトの証明書テンプレート EAP_Authentication_Certificate_Template を編集できます。

デフォルトでは、次の CA テンプレートが Cisco ISE で使用できます。

- CA_SERVICE_Certificate_Template：ISE CA を使用する他のネットワーク サービス用。たとえば、ASA VPN ユーザに対し証明書を発行するには、ISE の設定時にこの証明書テンプレートを使用します。
- EAP_Authentication_Certificate_Template：EAP 認証用。
- pxGrid_Certificate_Template：証明書プロビジョニング ポータルから証明書を生成する際の pxGrid コントローラ用。

（注） ECC キー タイプを使用する証明書テンプレートは、内部 Cisco ISE CA とのみ使用することができます。

始める前に

CA が設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [CA サービス（CA Service）] > [内部 CA 証明書テンプレート（Internal CA Certificate Template）]** を選択します。

ステップ 2 内部 CA テンプレートの名前を入力します。たとえば、Internal_CA_Template とします。

ステップ 3 （オプション）[組織単位（Organizational Unit）]、[組織（Organization）]、[市（City）]、[州/都道府県（State）]、[国（Country）] フィールドに値を入力します。

証明書テンプレート フィールド（[組織ユニット（Organizational Unit）]、[組織（Organization）]、[都市（City）]、[州（State）]、および [国（Country）]）の UTF-8 文字はサポートしていません。UTF-8 文字を証明書テンプレートで使用すると、証明書プロビジョニングが失敗します。

証明書を生成する内部ユーザのユーザ名が、証明書の共通名として使用されます。Cisco ISE 内部 CA は、「+」または「*」の文字を [共通名（Common Name）] フィールドでサポートしていません。ユーザ名に「+」または「*」の特殊文字が含まれていないことを確認してください。

ステップ 4 サブジェクト代替名（SAN）および証明書の有効期間を指定します。

ステップ 5 キー タイプを指定します。RSA または ECC を選択します。

次の表に、ECC をサポートしているオペレーティング システムおよびバージョンと、サポートされている曲線タイプを示します。デバイスがサポートされているオペレーティング システムを実行していない場合、またはサポートされているバージョンでない場合には、代わりに RSA ベースの証明書を使用することもできます。

オペレーティング システム（Operating System）	サポートされるバージョン	サポートされる曲線タイプ
Windows	8 以降	P-256、P-384、P-521
Android	4.4 以降 （注） Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ（P-192 曲線タイプをサポートしていない Android 6.0 を除く）。

Windows 7 と Apple iOS は、EAP-TLS 認証用の ECC をネイティブでサポートしていません。Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

ネットワークのデバイスがサポートされていないオペレーティング システム（Windows 7、MAC OS X、Apple iOS）を実行する場合は、キー タイプとして RSA を選択することを推奨します。

ステップ 6 （RSA キー タイプを選択する場合に適用）キー サイズを指定します。1024 以上のキー サイズを選択する必要があります。

ステップ 7 （ECC キー タイプを選択する場合にのみ適用）曲線タイプを指定します。デフォルトは P-384 です。

ステップ 8 ISE 内部 CA を SCEP RA プロファイルとして選択します。

ステップ 9 有効期間を日数単位で入力します。デフォルトは 730 日です。有効な範囲は 1 ～ 730 です。

ステップ 10 拡張キーの使用状況を指定します。証明書をクライアント認証に使用する場合は、[クライアント認証（Client Authentication）] チェック ボックスにマークを付けます。証明書をサーバ認証に使用する場合は、[サーバ認証（Server Authentication）] チェック ボックスにマークを付けます。

ステップ 11 [送信（Submit）] をクリックします。

内部 CA 証明書テンプレートが作成され、クライアント プロビジョニング ポリシーによって使用されます。

次のタスク

クライアント プロビジョニング ポリシーで使用されるネイティブ サプリカント プロファイルの作成 （221 ページ）

内部 CA の設定

次の表では、内部 CA の設定ページのフィールドについて説明します。内部 CA の設定を表示し、このページから内部 CA サービスを無効にできます。このページへのナビゲーションパス

は、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [内部 CA の設定（Internal CA Settings）]** です。

表 *23 :* 内部 *CA* の設定

フィールド名	使用上のガイドライン
認証局の無効化（Disable Certificate Authority）	内部 CA サービスを無効にするには、このボタンをクリックします。
ホスト名（Host Name）	CA サービスを実行している Cisco ISE ノードのホスト名。
ペルソナ（Personas）	CA サービスを実行しているノードで有効な Cisco ISE ノードのペルソナ。たとえば、管理、ポリシー サービスなどです。
ロール（Role(s)）	CA サービスを実行する Cisco ISE ノードが担当するロール。たとえば、スタンドアロンまたはプライマリまたはセカンダリです。
CA、EST、および OCSP 応答側のステータス（CA, EST & OCSP Responder Status）	有効または無効
OCSP 応答側 URL（OCSP Responder URL）	OCSP サーバにアクセスするための Cisco ISE ノードの URL。
SCEP URL	SCEP サーバにアクセスするための Cisco ISE ノードの URL。

関連トピック

Cisco ISE CA サービス （201 ページ）
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 （214 ページ）

クライアントプロビジョニングポリシーで使用されるネイティブサプリカントプロファイルの作成

ネイティブ サプリカント プロファイルを作成して、ユーザがパーソナル デバイスを企業ネットワークに含めることができます。Cisco ISE では、異なるオペレーティング システムごとに異なるポリシー ルールを使用します。各クライアント プロビジョニング ポリシー ルールには、どのオペレーティング システムにどのプロビジョニング ウィザードを使用するかを指定するネイティブ サプリカント プロファイルが含まれています。

始める前に

- Cisco ISE で CA 証明書テンプレートを設定します。
- TCP ポート 8905 および UDP ポート 8905 を開き、クライアントエージェントとサプリカントのプロビジョニングウィザードのインストールを有効にします。ポートの使用法の詳細については、『*Cisco Identity Services Engine Hardware Installation Guide*』の付録「Cisco ISE Appliance Ports Reference」を参照してください。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [ネイティブ サプリカント プロファイル（Native Supplicant Profile）]** を選択します。

ステップ 3 ネイティブ サプリカント プロファイルの名前を入力します。たとえば、EAP_TLS_INTERNAL となります。

ステップ 4 [オペレーティング システム（Operating System）] ドロップダウン リストから [すべて（ALL）] を選択します。

（注） MAC OS バージョン 10.10 のユーザは、デュアル SSID PEAP フローに対してプロビジョニングされた SSID に手動で接続する必要があります。

ステップ 5 [有線（Wired）] または [無線（Wireless）] チェックボックスをオンにします。

ステップ 6 [許可されるプロトコル（Allowed Protocol）] ドロップダウン リストから [TLS] を選択します。

ステップ 7 以前に作成した CA 証明書テンプレートを選択します。

ステップ 8 [送信（Submit）] をクリックします。

次のタスク

Cisco サイトからの Windows および Mac OS X オペレーティング システムのエージェント リソースのダウンロード （222 ページ）

Cisco サイトからの Windows および Mac OS X オペレーティング システムのエージェント リソースのダウンロード

Windows および Mac OS X オペレーティング システムでは、Cisco サイトからリモート リソースをダウンロードする必要があります。

始める前に

ネットワークのプロキシ設定が正しく設定されていることを確認し、適切なリモート ロケーションにアクセスして、クライアント プロビジョニング リソースを Cisco ISE にダウンロードできることを確認します。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[リソース（Resources）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）]** > **[Cisco サイトのエージェント リソース（Agent resources from Cisco site）]** を選択します。

ステップ 3 [Windows] および [MAC OS X] パッケージの隣にあるチェックボックスをオンにします。必ず最新バージョンを含めます。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

Apple iOS、Android および MACOSX デバイスのクライアント プロビジョニング ポリシー ルールの作成 （223 ページ）

Apple iOS、Android および MACOSX デバイスのクライアント プロビジョニング ポリシー ルールの作成

クライアント プロビジョニング リソース ポリシーは、どのユーザがリソース（エージェント、エージェント コンプライアンス モジュール、エージェント カスタマイズ パッケージ/プロファイル）のどのバージョン（または複数のバージョン）をログイン時およびユーザ セッション開始時に Cisco ISE から受信するかを決定します。

エージェント コンプライアンス モジュールをダウンロードすると、システムで使用している既存のモジュールがあれば常にそれが上書きされます。

従業員が iOS、Android、および MACOSX デバイスを持ち込むことができるようにするには、[クライアント プロビジョニング ポリシー（Client Provisioning Policy）] ページでこれらの各デバイスのポリシー ルールを作成する必要があります。

始める前に

必要なネイティブ サプリカント プロファイルを設定し、[クライアント プロビジョニング ポリシー（Client Provisioning Policy）] ページから必要なエージェントをダウンロードしておく必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 Apple iOS、Android および MACOSX デバイスのクライアント プロビジョニング ポリシー ルールを作成します。

ステップ 3 [保存（Save）] をクリックします。

次のタスク

TLS ベース認証の Dot1X 認証ポリシー ルールの設定 （224 ページ）

TLS ベース認証の Dot1X 認証ポリシー ルールの設定

このタスクは、TLS ベース認証の Dot1X 認証ポリシー ルールを更新する方法を示します。

始める前に

TLS ベース認証用に作成された証明書認証プロファイルが存在することを確認します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー セット（Policy Sets）]** を選択します。

ステップ 2 [表示（View）] 列から矢印アイコン › をクリックすると、[設定（Set）] ビュー画面が開き、認証ポリシーを表示、管理、および更新できます。

デフォルトのルールベースの認証ポリシーには、Dot1X 認証用のルールが含まれます。

ステップ 3 Dot1X 認証ポリシー ルールの条件を編集するには、[条件（Conditions）] 列のセルにカーソルを合わせ、 をクリックします。[条件スタジオ（Conditions Studio）] が開きます。

ステップ 4 Dot1X ポリシー ルールの [アクション（Actions）] 列で、歯車アイコンをクリックし、必要に応じてドロップダウンメニューから、挿入または複製オプションのいずれかを選択して新しいポリシー セットを挿入します。
[ポリシー セット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 5 ルールの名前を入力します。たとえば、eap-tls と入力します。

ステップ 6 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 7 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性（たとえば、Network Access:UserName Equals User1）を選択します。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 8 [使用（Use）] をクリックします。

ステップ 9 デフォルト ルールは、そのままにします。

ステップ 10 **[保存（Save）]** をクリックします。

次のタスク

中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成 （224 ページ）

中央 Web 認証とサプリカント プロビジョニング フローの許可プロファイルの作成

許可プロファイルを定義して、証明書ベースの認証の成功後にユーザに付与するアクセスを決定します。

始める前に

ワイヤレス LAN コントローラ（WLC）に必要なアクセス コントロール リスト（ACL）が設定されていることを確認します。WLC での ACL の作成方法については、『*TrustSec How-To Guide: Using Certificates for Differentiated Access*』を参照してください。

この例では、WLC で次の ACL が作成されていると仮定します。

- NSP-ACL：ネイティブ サプリカント プロビジョニング用
- BLACKHOLE：ブラックリストに登録されているデバイスへのアクセスの制限
- NSP-ACL-Google：Android デバイスのプロビジョニング

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 新しい許可プロファイルを作成するには、[追加（Add）] をクリックします。

ステップ 3 許可プロファイルの名前を入力します。

ステップ 4 [アクセス タイプ（Access Type）] ドロップダウン リストから、[ACCESS_ACCEPT] を選択します。

ステップ 5 中央 Web 認証、Google Play の中央 Web 認証、ネイティブ サプリカント プロビジョニング、および Google のネイティブ サプリカント プロビジョニングの許可プロファイルを追加するには、[追加（Add）] をクリックします。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

許可ポリシー ルールの作成 （225 ページ）

許可ポリシー ルールの作成

Cisco ISE は、許可ポリシー ルールを評価し、ポリシー ルールで指定された許可プロファイルに基づいてネットワーク リソースへのアクセス権をユーザに付与します。

始める前に

必要な許可プロファイルを作成済みであることを確認します。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択し、許可ポリシー ルールを表示するポリシー セットを展開します。

ステップ 2 デフォルトのルールの上に追加のポリシー ルールを挿入します。

ステップ 3 **[保存（Save）]** をクリックします。

CA サービス ポリシーのリファレンス

ここでは、Cisco ISE CA サービスを有効にする前に作成する必要がある許可ポリシー ルールおよびクライアント プロビジョニング ポリシー ルールの詳細情報について説明します。

証明書サービスのクライアント プロビジョニング ポリシー ルール

ここでは、Cisco ISE 証明書サービスを使用している場合に作成する必要があるクライアント プロビジョニング ポリシー ルールについて説明します。次の表に詳細を示します。

ルール名	ID グループ	オペレーティング システム	その他の条件	結果
iOS	任意（Any）	Apple iOS すべて	条件	EAP_TLS_INTERNAL（以前に作成したネイティブ サプリカント プロファイル）。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカント プロファイルを選択します。
Android	任意（Any）	Android	条件	EAP_TLS_INTERNAL（以前に作成したネイティブ サプリカント プロファイル）。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカント プロファイルを選択します。

ルール名	ID グループ	オペレーティング システム	その他の条件	結果
MACOSX	任意（Any）	MACOSX	条件	ネイティブ サプリカントの設定で、次を指定してください。 1. 構成ウィザード：シスコのサイトからダウンロードした MACOSX サプリカントのウィザードを選択します。 2. ウィザードのプロファイル：以前作成した EAP_TLS_INTERNAL ネイティブ サプリカントのプロファイルを選択します。外部 CA を使用している場合は、外部 CA 用に作成したネイティブ サプリカント プロファイルを選択します。

証明書サービスの許可プロファイル

ここでは、Cisco ISE で証明書ベースの認証を有効にするために作成する必要がある許可プロファイルについて説明します。ワイヤレス LAN コントローラ（WLC）の ACL（NSP-ACL および NSP-ACL-Google）がすでに作成されている必要があります。

- CWA：このプロファイルは、中央 Web 認証フローを使用するデバイス用です。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [中央集中（Centralized）] を選択し、ACL テキスト ボックスに NSP-ACL を入力します。

- CWA_GooglePlay：このプロファイルは、中央 Web 認証フローを使用する Android デバイス用です。このプロファイルによって、Android デバイスは Google Play ストアにアクセスし、Cisco Network Setup Assistant をダウンロードできます。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [中央集中（Centralized）] を選択し、ACL テキスト ボックスに NSP-ACL-Google を入力します。
- NSP：このプロファイルは、サプリカント プロビジョニング フローを使用する非 Android デバイス用です。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [サプリカント プロビジョニング（Supplicant Provisioning）] を選択し、ACL テキスト ボックスに NSP-ACL を入力します。
- NSP-Google：このプロファイルは、サプリカント プロビジョニング フローを使用する Android デバイス用です。[Web 認証（Web Authentication）] チェックボックスをオンにして、ドロップダウン リストから [サプリカント プロビジョニング（Supplicant Provisioning）] を選択し、ACL テキスト ボックスに NSP-ACL-Google を入力します。

デフォルトの Blackhole_Wireless_Access 許可プロファイルを確認します。高度な属性設定を次のように設定する必要があります。

- Cisco:cisco-av-pair = url-redirect=https://*ip:port*/blacklistportal/gateway?portal=*PortalID*
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

証明書サービスの許可ポリシー ルール

ここでは、Cisco ISE CA サービスを有効にするときに作成する必要がある許可ポリシー ルールについて説明します。

- 企業資産：このルールは、802.1X および MSCHAPV2 プロトコルを使用して企業のワイヤレス SSID に接続する企業のデバイス用です。
- Android_SingleSSID：このルールは、Google Play ストアにアクセスして、プロビジョニングのために Cisco Network Setup Assistant をダウンロードする Android デバイス用です。このルールは、シングル SSID 設定に固有です。
- Android_DualSSID：このルールは、Google Play ストアにアクセスして、プロビジョニングのために Cisco Network Setup Assistant をダウンロードする Android デバイス用です。このルールは、デュアル SSID 設定に固有です。
- CWA：このルールは、中央 Web 認証フローを使用するデバイス用です。
- NSP：このルールは、EAP-TLS 認証の証明書を使用するネイティブ サプリカント プロビジョニング フローを使用するデバイス用です。
- EAP-TLS：このルールは、サプリカント プロビジョニング フローを完了したデバイスおよび証明書でプロビジョニングされるデバイス用です。デバイスには、ネットワークへのアクセス権限が付与されます。

次の表に、Cisco ISE CA サービスの許可ポリシー ルールを設定するときに選択する必要がある属性および値を示します。この例では、Cisco ISE で対応する許可プロファイルも設定しているものと想定します。

ルール名	条件（Conditions）	権限（適用される許可プロファイル）
企業資産	Corp_Assets AND（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2）	PermitAccess
Android_SingleSSID	（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android）	NSP_Google
Android_DualSSID	（Wireless_MAB AND Session:Device-OS EQUALS Android）	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2）	NSP
EAP-TLS	（Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI	PermitAccess

ISE CA による ASA VPN ユーザへの証明書の発行

ISE CA は、ASA VPN 経由で接続しているクライアント マシンに証明書を発行します。この機能を使用して、ASA VPN 経由で接続しているエンド デバイスに証明書を自動的にプロビジョニングできます。

Cisco ISE は、Simple Certificate Enrollment Protocol（SCEP）を使用して登録を行い、証明書をクライアント マシンにプロビジョニングします。AnyConnect クライアントは、HTTPS 接続で ASA に SCEP 要求を送信します。ASA は、Cisco ISE と ASA の間に確立された HTTP 接続を介して Cisco ISE に要求を中継する前に、要求を評価し、ポリシーを適用します。Cisco ISE CA からの応答はクライアントに中継されます。ASA は、SCEP メッセージの内容を読み取ることはできず、Cisco ISE CA のプロキシとして機能します。Cisco ISE CA は、クライアントからの SCEP メッセージを復号化し、暗号化された形式で応答を送信します。

ISE CA SCEP URL は http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe です。ISE ノードの FQDN を使用する場合は、ASA に接続されている DNS サーバが FQDN を解決できる必要があります。

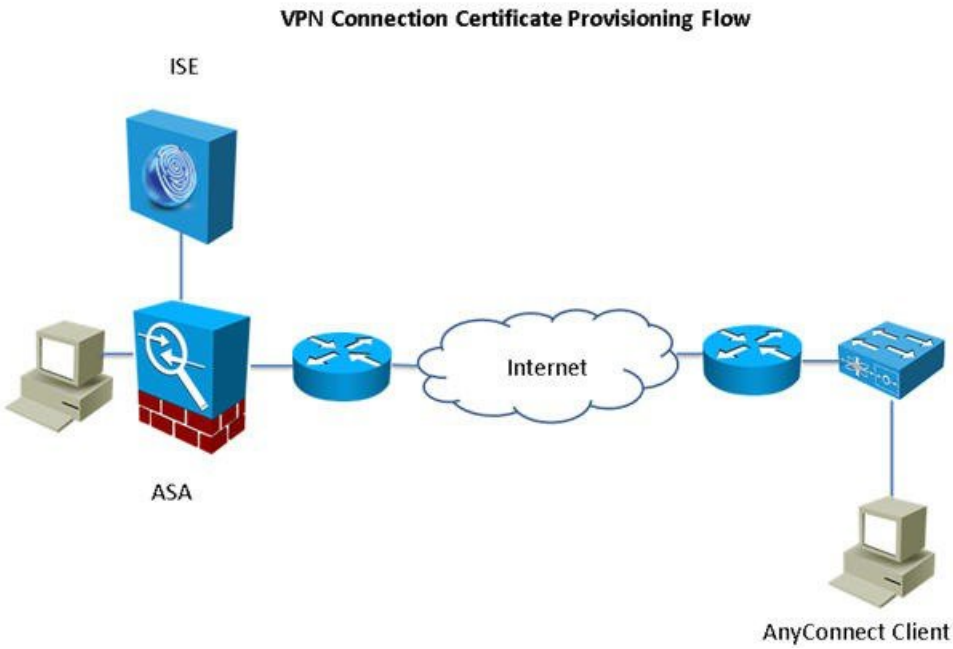
AnyConnect クライアント プロファイルの期限が切れる前に、証明書の更新を設定できます。証明書がすでに期限切れの場合、更新フローは新規登録と同様です。

サポートされているバージョンは次のとおりです。

- ソフトウェア バージョン 8.x を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco AnyConnect VPN バージョン 2.4 以降

VPN 接続の証明書プロビジョニング フロー

図 *7: ASA VPN* ユーザの証明書プロビジョニング



1. ユーザが VPN 接続を開始します。
2. AnyConnect クライアントは、クライアント マシンをスキャンし、固有デバイス識別子（たとえば IMEI）などの属性を ASA に送信します。
3. ASA はクライアントからの証明書ベースの認証を要求します。証明書がないため、認証は失敗します。
4. ASA は、ユーザ名/パスワードを使用してプライマリ ユーザ認証（AAA）に進み、情報を認証サーバ（ISE）に渡します。
    1. 認証が失敗すると、接続はただちに終了します。
    2. 認証が成功すると、制限付きアクセスが許可されます。aaa.cisco.sceprequired 属性を使用して証明書を要求するクライアント マシンでダイナミック アクセス ポリシー（DAP）を設定できます。この属性の値を「true」に設定し、ACL および Web ACL を適用できます。

5. VPN 接続は、関連するポリシーと ACL が適用された後に確立されます。クライアントは、AAA 認証が成功し、VPN 接続が確立された後にのみ、SCEP のキー生成を開始します。
6. クライアントは、SCEP 登録を開始し、HTTP を介して ASA に SCEP 要求を送信します。
7. ASA は、要求のセッション情報を検索し、セッションが登録を許可されている場合は、ISE CA に要求をリレーします。
8. ASA は ISE CA からの応答をクライアントにリレー バックします。
9. 登録が成功すると、クライアントにユーザに対する設定可能メッセージが表示され、VPN セッションが接続解除されます。
10. ユーザは証明書を使用して再度認証を行うことができ、正常な VPN 接続が確立されます。

ASA VPN ユーザに証明書を発行する Cisco ISE CA の設定

ASA VPN ユーザに証明書をプロビジョニングするには、Cisco ISE および ASA で次の設定を行う必要があります。

始める前に

- VPN ユーザ アカウントが Cisco ISE の内部または外部の ID ソースに存在することを確認します。
- ASA および Cisco ISE のポリシー サービス ノードが同じ NTP サーバを使用して同期されていることを確認します。

ステップ 1 Cisco ISE で ASA をネットワーク アクセス デバイスとして定義します。ネットワーク デバイスとして ASA を追加する方法については、Cisco ISE でのネットワークデバイスの追加 （231 ページ） を参照してください。

ステップ 2 ASA でのグループ ポリシーの設定 （232 ページ）。

ステップ 3 SCEP 登録用の AnyConnect 接続プロファイルの設定 （233 ページ）。

ステップ 4 ASDM での VPN クライアント プロファイルの設定 （233 ページ）。

ステップ 5 ASA への Cisco ISE CA 証明書のインポート。

Cisco ISE でのネットワークデバイスの追加

Cisco ISE でネットワークデバイスを追加したり、デフォルトのネットワークデバイスを使用したりできます。

また、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** ページで、ネットワーク デバイスを作成することもできます。

始める前に

ネットワークデバイスで AAA 機能が有効になっていることを確認します。詳細については、を参照してくださいAAA 機能を有効にするコマンド （1518 ページ）

ステップ 1 **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ネットワークデバイスの [名前（Name）] を入力します。

ステップ 4 （注） IPv4 および IPv6 は、ネットワーク デバイス（TACACS および RADIUS）設定および外部 RADIUS サーバ設定でサポートされるようになりました。IPv4 アドレスを入力する場合は、範囲とサブネット マスクを使用できます。IPv6 では、範囲がサポートされていません。

IP アドレスを入力します。

ステップ 5 （任意）[RADIUS 認証設定（RADIUS Authentication Settings）] チェックボックスをオンにして、RADIUS プロトコル認証を設定します。

ステップ 6 （任意）[TACACS 認証設定（TACACS Authentication Settings）] チェックボックスをオンにして、TACACS プロトコル認証を設定します。

ステップ 7 （任意）[SNMP の設定（SNMP Settings）] チェックボックスをオンにして、デバイス情報を収集するプロファイリング サービスの簡易ネットワーク管理プロトコルを設定します。

ステップ 8 （任意）TrustSec 対応デバイスを設定するには [高度なTrustSec設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 9 [送信（Submit）] をクリックします。

ASA でのグループ ポリシーの設定

ASA でグループ ポリシーを設定し、SCEP 登録要求を転送するための AnyConnect 用の ISE CA URL を定義します。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN（Remote Access VPN）] ナビゲーション ペインから、[グループポリシー（Group Policies）] をクリックします。

ステップ 3 [追加（Add）] をクリックして、グループ ポリシーを作成します。

ステップ 4 グループ ポリシーの名前を入力します。たとえば、ISE_CA_SCEP のようになります。

ステップ 5 [SCEP転送URL（SCEP forwarding URL）] フィールドで、[継承（Inherit）] チェックボックスをオフにして、ポート番号を含む ISE SCEP URL を入力します。

ISE ノードの FQDN を使用する場合は、ASA に接続されている DNS サーバが ISE ノードの FQDN を解決できる必要があります。

例：

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.

ステップ 6 [OK] をクリックして、グループ ポリシーを保存します。

SCEP 登録用の AnyConnect 接続プロファイルの設定

ISE CA サーバ、認証方式、および ISE CA SCEP URL を指定するには、ASA で AnyConnect 接続プロファイルを設定します。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN（Remote Access VPN）] ナビゲーション ペインから、[AnyConnect接続プロファイル（AnyConnect Connection Profiles）] をクリックします。

ステップ 3 [追加（Add）] をクリックして、接続プロファイルを作成します。

ステップ 4 接続プロファイルの名前を入力します。たとえば、Cert-Group と入力します。

ステップ 5 （オプション）[エイリアス（Aliases）]フィールドに接続プロファイルの説明を入力します。たとえば、SCEP-Call-ASA とします。

ステップ 6 [認証（Authentication）] 領域で、次の情報を指定します。

- [方式（Method）] : [両方（Both）] オプション ボタンをクリックします
- [AAAサーバグループ（AAA Server Group）] : [管理（Manage）] をクリックして ISE サーバを選択します

ステップ 7 [クライアントアドレスの割り当て（Client Address Assignment）] 領域で、使用する DHCP サーバおよびクライアント アドレス プールを選択します。

ステップ 8 [デフォルトグループポリシー（Default Group Policy）] 領域で、[管理（Manage）] をクリックし、ISE SCEP URL とポート番号で作成したグループ ポリシーを選択します。

例：

たとえば、ISE_CA_SCEP のようになります。

ステップ 9 **[詳細設定（Advanced）]**>**[一般（General）]** を選択し、この接続プロファイルに対して [Simple Certificate Enrollment Protocolを有効にする（Enable Simple Certificate Enrollment Protocol）] チェックボックスをオンにします。

ステップ 10 [OK] をクリックします。
AnyConnect 接続プロファイルが作成されます。

次のタスク

ASDM での VPN クライアント プロファイルの設定

SCEP 登録用に AnyConnect で VPN クライアント プロファイルを設定します。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセスVPN（Remote Access VPN）] ナビゲーション ペインから、[AnyConnectクライアントプロファイル（AnyConnect Client Profile）] をクリックします。

ステップ 3 使用するクライアント プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 4 左側の [プロファイル（Profile）] ナビゲーション ペインで、[証明書の登録（Certificate Enrollment）] をクリックします。

ステップ 5 [証明書の登録（Certificate Enrollment）] チェックボックスをオンにします。

ステップ 6 次のフィールドに値を入力します。

- [証明書失効しきい値（Certificate Expiration Threshold）]：AnyConnect がユーザに対して証明書の失効が近づいていることを証明書の有効期限の何日前に警告するか（SCEP が有効な場合はサポートされません）。デフォルトは 0（警告は表示しない）です。値の範囲は 0 ～ 180 日です。
- [自動SCEPホスト（Automatic SCEP Host）]：SCEP 証明書取得が設定されている ASA のホスト名および接続プロファイル（トンネル グループ）を入力します。ASA の完全修飾ドメイン名（FQDN）または接続プロファイル名を入力してください。たとえば、ホスト名 asa.cisco.com、接続プロファイル名 Cert_Group などです。
- [CA URL]：SCEP CA サーバを識別します。ISE サーバの FQDN または IP アドレスを入力します。たとえば、http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe などです。

ステップ 7 証明書の内容をクライアントが要求する方法を定義する値を [証明書の内容（Certificate Contents）] に入力します。

ステップ 8 [OK] をクリックします。
AnyConnect クライアント プロファイルが作成されます。詳細については、お使いのバージョンの AnyConnect の『Cisco AnyConnect Secure Mobility Client』を参照してください。

ASA への Cisco ISE CA 証明書のインポート

Cisco ISE 内部 CA 証明書を ASA にインポートします。

始める前に

Cisco ISE 内部 CA 証明書をエクスポートします。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** に移動します。[証明書サービスノードCA（Certificate Services Node CA）] および [証明書サービスルートCA（Certificate Services Root CA）] 証明書の横にあるチェックボックスをオンにして、これらの証明書を一度に 1 つずつエクスポートします。

ステップ 1 Cisco ASA ASDM にログインします。

ステップ 2 左側の [リモートアクセス VPN（Remote Access VPN）] ナビゲーション ペインから、**[証明書管理（Certificate Management）] > [CA 証明書（CA Certificates）]** を選択します。

ステップ 3 [追加（Add）] をクリックして Cisco ISE 内部 CA 証明書を選択し、ASA にインポートします。

エンドポイント証明書の失効

従業員のパーソナル デバイスに対して発行された証明書を取り消す必要がある場合は、[エンドポイント証明書（Endpoint Certificates）] ページから取り消すことができます。たとえば、従業員のデバイスが盗難されたり、紛失したりした場合には、Cisco ISE 管理者ポータルにログインし、そのデバイスに発行された証明書を [エンドポイント証明書（Endpoint Certificates）] ページから取り消すことができます。フレンドリ名、デバイスの一意の ID、シリアル番号に基づいて、このページのデータをフィルタリングできます。

PSN（サブ CA）が侵害された場合は、[エンドポイント証明書（Endpoint Certificates）] ページの [発行元（Issued By）] フィールドでフィルタリングすることによって、その PSN によって発行されたすべての証明書を取り消すことができます。

従業員に対して発行された証明書を取り消すときに、アクティブなセッション（その証明書を使用して認証された）がある場合、セッションは即座に終了します。証明書を取り消すと、その直後に、許可されていないユーザはリソースにアクセスできなくなります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [発行された証明書（Issued Certificates）]** を選択します。

ステップ 2 取り消すエンドポイント証明書の隣にあるチェックボックスをオンにし、[失効（Revoke）] をクリックします。

フレンドリ名とデバイス タイプに基づいて証明書を検索できます。

ステップ 3 証明書を取り消す理由を入力します。

ステップ 4 [Yes] をクリックします。

OCSP サービス

Online Certificate Status Protocol（OCSP）は、x.509 デジタル証明書のステータスのチェックに使用されるプロトコルです。このプロトコルは証明書失効リスト（CRL）に代わるものであり、CRL の処理が必要となる問題に対処します。

Cisco ISE には HTTP を介して OCSP サーバと通信し、認証で証明書のステータスを検証する機能があります。OCSP のコンフィギュレーションは、Cisco ISE で設定されるいずれかの認証局（CA）証明書から参照できる再利用可能な設定オブジェクトで設定されます。

CRL 検証と OCSP 検証の両方または一方を CA ごとに設定できます。両方を選択すると、Cisco ISE では最初に OCSP を介した検証が実行されます。プライマリ OCSP サーバとセカンダリ OCSP サーバの両方で通信の問題が検出された場合、または特定の証明書に対して不明のステータスが返された場合、Cisco ISE は CRL チェックの実行に切り替えます。

Cisco ISE CA サービスの Online Certificate Status Protocol レスポンダ

Cisco ISE CA OCSP 応答側は、OCSP クライアントと通信するサーバです。Cisco ISE CA の OCSP クライアントには、Cisco ISE の内部 OCSP クライアントと適応型セキュリティ アプライアンス（ASA）の OCSP クライアントがあります。OCSP クライアントは、RFC 2560、5019 で定義されている OCSP 要求/応答構造を使用して、OCSP 応答側と通信する必要があります。

Cisco ISE CA は、OCSP 応答側に証明書を発行します。OCSP 応答側は、着信要求をポート 2560 でリッスンします。このポートは、OCSP トラフィックのみを許可するように設定されています。

OCSP 応答側は RFC 2560、5019 で規定された構造に従って要求を受け入れます。OCSP 要求ではナンス拡張がサポートされます。OCSP 応答側は証明書のステータスを取得し、OCSP 応答を作成して署名します。OCSP 応答は、OCSP 応答側ではキャッシュされませんが、クライアントでは最大 24 時間 OCSP 応答をキャッシュすることができます。OCSP クライアントでは、OCSP 応答の署名を検証する必要があります。

PAN 上の自己署名 CA 証明書（ISE が外部 CA の中間 CA として機能する場合は、中間 CA 証明書）によって、OCSP 応答側証明書が発行されます。PAN 上のこの CA 証明書によって、PAN および PSN の OCSP 証明書が発行されます。この自己署名 CA 証明書は、展開全体に対するルート証明書でもあります。展開全体のすべての OCSP 証明書が、これらの証明書を使用して署名された応答を ISE で検証するために、信頼できる証明書ストアに格納されます。

OCSP 証明書のステータスの値

OCSP サービスでは、所定の証明書要求に対して次の値が返されます。

- [良好（Good）]：ステータスの問い合わせへの肯定的な応答を示します。証明書が失効していないこと、および状態が次の時間間隔（存続可能時間）値までは良好であることを示します。
- [失効（Revoked）]：証明書は失効しています。
- [不明（Unknown）]：証明書のステータスは不明です。この OCSP 応答側の CA で証明書が発行されなかった場合、OCSP サービスはこの値を返します。
- [エラー（ERROR）]：OCSP 要求に対する応答を受信しませんでした。

OCSP ハイ アベイラビリティ

Cisco ISE では CA ごとに最大 2 つの OCSP サーバを設定でき、それらのサーバはプライマリおよびセカンダリ OCSP サーバと呼ばれます。各 OCSP サーバ設定には、次のパラメータが含まれます。

- [URL]：OCSP サーバの URL。
- [ナンス（Nonce）]：要求で送信される乱数。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。

• [応答の検証（Validate Response）]：Cisco ISE は OCSP サーバから受信した応答の署名を検証します。

Cisco ISE がプライマリ OCSP サーバと通信しているときに、タイムアウト（5 秒）が発生した場合、Cisco ISE はセカンダリ OCSP サーバに切り替えます。

Cisco ISE はプライマリ サーバの再使用を試行する前に、設定可能な期間セカンダリ OCSP サーバを使用します。

OCSP の障害

3 つの一般的な OCSP 障害のシナリオは次のとおりです。

• OCSP キャッシュまたは OCSP クライアント側（Cisco ISE）の失敗による障害。

• 失敗した OCSP 応答側のシナリオ。例：

最初のプライマリ OCSP 応答側が応答せず、セカンダリ OCSP 応答側が Cisco ISE OCSP 要求に応答します。

Cisco ISE OCSP 要求からエラーまたは応答が受信されません。

OCSP 応答側が、Cisco ISE OCSP 要求への応答を提供しないか、失敗の OCSP 応答のステータスを返している可能性があります。OCSP 応答のステータス値は次のようになります。

• tryLater

• signRequired

• unauthorized

• internalError

• malformedRequest

OCSP 要求には、多数の日時チェック、署名の有効性チェックなどがあります。詳細については、エラー状態を含むすべての可能性のある状態について説明している『*RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*』を参照してください。

• 失敗した OCSP レポート

OCSP クライアント プロファイルの追加

[OCSP クライアント プロファイル（OCSP Client Profile）] ページを使用して、Cisco ISE に新しい OCSP クライアント プロファイルを追加できます。

始める前に

認証局（CA）が非標準ポート（80 または 443 以外）で OCSP サービスを実行している場合は、そのポートで Cisco ISE と CA 間の通信を可能にするためにスイッチで ACL を設定する必要があります。次に例を示します。

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP* ポート番号 >

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] >** [OCSP クライアント プロファイル（OCSP Client Profile）] を選択します。

ステップ 2 OCSP クライアント プロファイルを追加するための値を入力します。

ステップ 3 [送信（Submit）] をクリックします。

OCSP クライアント プロファイル設定

次の表では、OCSP クライアント プロファイル設定を行うために使用できる [OCSP クライアント プロファイル（OCSP Client Profile）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [OCSP クライアント プロファイル（OCSP Client Profile）]** です。

表 *24 : OCSP* クライアント プロファイル設定

フィールド名	使用上のガイドライン
名前（**Name**）	OCSP クライアント プロファイル名。
説明	任意で説明を入力します。
OCSP応答側の設定（Configure OCSP Responder）	
セカンダリ サーバの有効化（**Enable Secondary Server**）	ハイ アベイラビリティのセカンダリ OCSP サーバを有効にするには、このチェックボックスをオンにします。
常にプライマリ サーバに最初にアクセスする（**Always Access Primary Server First**）	このオプションは、セカンダリ サーバへの移動を試行する前にプライマリ サーバをチェックする場合に使用します。プライマリが以前にチェックされ、応答しないことがわかっている場合にも、Cisco ISE はセカンダリ サーバに移動する前にプライマリ サーバへの要求の送信を試行します。
[n 分経過後にプライマリ サーバにフォールバック（Fallback to Primary Server After Interval *n* Minutes）]	このオプションは、Cisco ISE がセカンダリ サーバに移動してから、再度プライマリ サーバにフォールバックする場合に使用します。この場合、その他の要求はすべてスキップされ、テキスト ボックスで設定した時間セカンダリ サーバが使用されます。許可される時間の範囲は 1 ～ 999 分です。

フィールド名	使用上のガイドライン
プライマリ サーバとセカンダリ サーバ（**Primary and Secondary Servers**）	
URL	プライマリおよびセカンダリ OCSP サーバの URL を入力します。
ナンス拡張サポートの有効化（**Enable Nonce Extension Support**）	ナンスが OCSP 要求の一部として送信されるように設定できます。ナンスには、OCSP 要求の疑似乱数が含まれます。応答で受信される数値は要求に含まれる数値と同じであることが検証されています。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。
応答の署名の検証（**Validate Response Signature**）	OCSP レスポンダは、次のいずれかの証明書を使用して応答に署名します。 • CA 証明書 • CA 証明書とは別の証明書 Cisco ISE が応答の署名を検証するためには、OCSP 応答側が応答を証明書とともに送信する必要があります。そうでない場合、応答の検証は失敗し、証明書のステータスは利用できません。RFC に従い、OCSP は異なる証明書を使用して応答に署名できます。このことは、OCSP が Cisco ISE による検証用に応答に署名した証明書を送信する限り当てはまります。OCSP が Cisco ISE で設定されているものとは異なる証明書を使用して応答に署名した場合、応答の検証は失敗します。
Authority Information Access（**AIA**）に指定された**OCSP URL**を使用する（**Use OCSP URLs specified in Authority Information Access (AIA)**）	Authority Information Access の拡張で指定されている OCSP URL を使用するには、オプション ボタンをクリックします。
応答キャッシュ（**Response Cache**）	

フィールド名	使用上のガイドライン
[キャッシュ エントリの存続可能時間 n 分(Cache Entry Time To Live *n* Minutes)]	キャッシュ エントリが期限切れになる時間を分単位で入力します。OCSP サーバからの各応答には nextUpdate 値が含まれています。この値は、証明書のステータスがサーバで次にいつ更新されるかを示します。OCSP 応答がキャッシュされるとき、2 つの値（1 つは設定から、もう 1 つは応答から）が比較され、この 2 つの最小値の時間だけ応答がキャッシュされます。nextUpdate 値が 0 の場合、応答はまったくキャッシュされません。Cisco ISE は設定された時間 OCSP 応答をキャッシュします。キャッシュは複製されず、永続的でもないため、Cisco ISE が再起動するとキャッシュはクリアされます。次の理由により、OCSP キャッシュは OCSP 応答を保持するために使用されます。 • 既知の証明書に関する OCSP サーバからのネットワークトラフィックと負荷を低減するため • 既知の証明書のステータスをキャッシュすることによって Cisco ISE のパフォーマンスを向上させるため デフォルトでは、キャッシュは内部 CA OCSP クライアントプロファイルに対し 2 分に設定されています。エンドポイントが最初の認証から 2 分以内にもう一度認証すると、OCSP のキャッシュが使用され、OCSP レスポンダには問い合わせされません。エンドポイントの証明書がキャッシュ期間内に失効した場合、以前の OCSP のステータス [良好（Good）] が使用され、認証は成功します。キャッシュを 0 分に設定すると、応答はキャッシュされません。このオプションでは、セキュリティは向上しますが、認証のパフォーマンスは低下します。
キャッシュのクリア（Clear Cache）	OCSP サービスに接続されているすべての認証局のエントリをクリアするには、[キャッシュのクリア（Clear Cache）] をクリックします。 展開内で、[キャッシュのクリア（Clear Cache）] はすべてのノードと相互作用して、処理を実行します。このメカニズムでは、展開内のすべてのノードが更新されます。

関連トピック

OCSP サービス （235 ページ）
Cisco ISE CA サービスの Online Certificate Status Protocol レスポンダ （236 ページ）
OCSP 証明書のステータスの値 （236 ページ）
OCSP ハイ アベイラビリティ （236 ページ）
OCSP の障害 （237 ページ）
OCSP 統計情報カウンタ （241 ページ）

OCSP クライアント プロファイルの追加 （237 ページ）

OCSP 統計情報カウンタ

Cisco ISE では、OCSP カウンタを使用して、OCSP サーバのデータと健全性をロギングおよびモニタリングします。ロギングは 5 分ごとに実行されます。Cisco ISE はモニタリング ノードに syslog メッセージを送信し、それはローカル ストアに保持されます。ローカル ストアには過去 5 分のデータが含まれています。Cisco ISE が syslog メッセージを送信した後、カウンタは次の間隔について再計算されます。つまり、5 分後に、新しい 5 分間の間隔が再度開始されます。

次の表に、OCSP syslog メッセージとその説明を示します。

表 *25 : OCSP Syslog* メッセージ

メッセージ	説明
OCSPPrimaryNotResponsiveCount	応答のないプライマリ要求の数
OCSPSecondaryNotResponsiveCount	応答のないセカンダリ要求の数
OCSPPrimaryCertsGoodCount	プライマリ OCSP サーバを使用して返された所定の CA の「良好な」証明書の数
OCSPSecondaryCertsGoodCount	プライマリ OCSP サーバを使用して返された所定の CA の「良好な」ステータスの数
OCSPPrimaryCertsRevokedCount	プライマリ OCSP サーバを使用して返された所定の CA の「失効した」ステータスの数
OCSPSecondaryCertsRevokedCount	セカンダリ OCSP サーバを使用して返された所定の CA の「失効した」ステータスの数
OCSPPrimaryCertsUnknownCount	プライマリ OCSP サーバを使用して返された所定の CA の「不明の」ステータスの数
OCSPSecondaryCertsUnknownCount	セカンダリ OCSP サーバを使用して返された所定の CA の「不明の」ステータスの数
OCSPPrimaryCertsFoundCount	プライマリの送信元からのキャッシュ内に見つかった証明書の数
OCSPSecondaryCertsFoundCount	セカンダリの送信元からのキャッシュ内に見つかった証明書の数
ClearCacheInvokedCount	一定間隔の後にキャッシュのクリアがトリガーされた回数

メッセージ	説明
OCSPCertsCleanedUpCount	t 間隔の後にクリーンアップされたキャッシュ エントリの数
NumOfCertsFoundInCache	キャッシュから実行された要求の数
OCSPCacheCertsCount	OCSP キャッシュ内に見つかった証明書の数

管理者のアクセス ポリシーの設定

管理者アクセス（RBAC）ポリシーは if-then 形式で表され、ここで if は RBAC 管理者グループの値、および then は RBAC 権限の値になります。

[RBACポリシー（RBAC policies）] ページ（[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] >[RBAC] > [ポリシー（Policy）]）には、デフォルトポリシーのリストが含まれています。これらのデフォルト ポリシーは編集または削除できません。ただし、読み取り専用管理ポリシーのデータ アクセス許可は編集できます。[RBAC ポリシー（RBAC policies）] ページでは、特に職場の管理者グループ用にカスタム RBAC ポリシーを作成し、パーソナライズされた管理者グループに適用できます。

制限付きメニュー アクセスを割り当てるときには、データ アクセス権限により、指定されているメニューを使用するために必要なデータに管理者がアクセスできることを確認してください。たとえばデバイス ポータルへのメニュー アクセスを付与するが、エンドポイント ID グループへのデータ アクセスを許可しないと、管理者はポータルを変更できません。

（注） 管理者ユーザは、エンドポイントの MAC アドレスを、読み取り専用アクセス権を持つエンドポイント ID グループから、フルアクセス権を持つエンドポイント ID グループに移動できます。その逆はできません。

始める前に

- RBAC ポリシーを定義するすべての管理者グループを作成していることを確認します。
- これらの管理者グループが、個々の管理者ユーザにマッピングされていることを確認します。
- メニュー アクセス権限やデータ アクセス権限など、RBAC 権限を設定していることを確認します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [ポリシー（Policy）]** を選択します。

[RBAC ポリシー（RBAC Policies）] ページには、デフォルトの管理者グループ用にすぐに使用できる定義済みの一連のポリシーが含まれています。これらのデフォルト ポリシーは編集または削除できません。ただし、デフォルトの読み取り専用管理ポリシーのデータ アクセス許可は編集できます。

ステップ 2 デフォルト RBAC ポリシー ルールのいずれかの隣にある [操作（Action）] をクリックします。

ここでは、新しい RBAC ポリシーを挿入し、既存の RBAC ポリシーを複製し、既存の RBAC ポリシーを削除できます。

ステップ 3 [新しいポリシーの挿入（Insert New Policy）] をクリックします。

ステップ 4 [ルール名（Rule Name）]、[RBAC グループ（RBAC Group(s)）]、および [権限（Permissions）] フィールドに値を入力します。

RBAC ポリシーの作成時に、複数のメニュー アクセス権限とデータ アクセス権限を選択することはできません。

ステップ 5 [**保存（Save**）] をクリックします。

管理者アクセスの設定

Cisco ISE では、セキュリティ強化のために管理者アカウントにルールを定義できます。管理インターフェイスへのアクセスを制限したり、強力なパスワードの使用やパスワードの定期的な変更を管理者に強制することができます。Cisco ISE の [管理者アカウントの設定（Administrator Account Settings）] で定義するパスワード ポリシーは、すべての管理者アカウントに適用されます。

Cisco ISE では、管理者パスワードでの UTF-8 文字の使用はサポートされていません。

同時管理セッションとログイン バナーの最大数の設定

同時管理 GUI または CLI（SSH）セッションの最大数、および管理 Web または CLI インターフェイスにアクセスする管理者を手助け、ガイドするログイン バナーを設定できます。管理者のログイン前後に表示されるログイン バナーを設定できます。デフォルトでは、これらのログイン バナーは無効になっています。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [アクセス（Access）] > [セッション（Session）]** を選択します。

ステップ 2 GUI および CLI インターフェイスを介した同時管理セッションの、許可する最大数を入力します。同時管理 GUI セッションの有効範囲は 1 ～ 20 です。同時管理 CLI セッションの有効範囲は 1 ～ 10 です。

ステップ 3 Cisco ISE で管理者がログインする前にメッセージを表示する場合は、[プリログイン バナー（Pre-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

ステップ 4 Cisco ISE で管理者がログインした後にメッセージを表示する場合は、[ポストログイン バナー（Post-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

ステップ 5 [保存（**Save**）] をクリックします。

関連トピック

IP アドレスの選択からの Cisco ISE への管理アクセスの許可 （244 ページ）

IP アドレスの選択からの Cisco ISE への管理アクセスの許可

Cisco ISE では、管理者が Cisco ISE 管理インターフェイスにアクセスできる IP アドレスのリストを設定することができます。

管理者アクセス コントロール設定は、管理ペルソナ、ポリシー サービス ペルソナ、またはモニタリング ペルソナを担う Cisco ISE ノードに対してのみ適用できます。これらの制限は、プライマリ ノードからセカンダリ ノードに複製されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[アクセス（Access）]** > **[IP アクセス（IP Access）]** を選択します。

ステップ 2 [リストにある IP アドレスだけに接続を許可（Allow only listed IP addresses to connect）] を選択します。

（注） 管理アクセスにはポート 161（SNMP）の接続を使用します。ただし、IP アクセス制限が設定されている場合は、実行元のノードで管理アクセスが設定されていないと snmpwalk が失敗します。

ステップ 3 [アクセス制限の IP リストの設定（Configure IP List for Access Restriction）] 領域で、[追加（Add）] をクリックします。

ステップ 4 [IP アドレス（IP Address）] フィールドに IP アドレスをクラスレス ドメイン間ルーティング（CIDR）形式で入力します。

（注） この IP アドレスの範囲は IPv4 から IPv6 です。ISE ノードに複数の IPv6 アドレスを設定できるようになりました。

ステップ 5 [CIDR 形式のネットマスク（Netmask in CIDR format）] フィールドにサブネット マスクを入力します。

ステップ 6 [OK] をクリックします。このプロセスを繰り返して、他の IP アドレス範囲をこのリストに追加します。

ステップ 7 [保存（Save）] をクリックして、変更内容を保存します。

ステップ 8 [IPアクセス（IP Access）] ページを更新するには、[リセット（Reset）] をクリックします。

管理者アカウントのパスワード ポリシーの設定

Cisco ISE では、セキュリティ向上のために管理者アカウントにパスワード ポリシーを作成することもできます。必要な管理者認証がパスワードベースか、クライアント証明書ベースかを定義できます。ここで定義したパスワード ポリシーは、Cisco ISE のすべての管理者アカウントに適用されます。

（注）

- 内部管理者ユーザの電子メール通知は root@host に送信されます。電子メール アドレスは設定できません。多くの SMTP サーバがこの電子メールを拒否します。

  未解決の不具合 CSCui5583 を確認できます。これは、電子メール アドレスの変更を許可する拡張機能です。

- Cisco ISE では、管理者パスワードでの UTF-8 文字の使用はサポートされていません。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- 自動フェールオーバー設定が展開でイネーブルになっている場合はオフにします。認証方式を変更すると、アプリケーション サーバ プロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ管理ノードの自動フェールオーバーが開始される場合があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]** を選択します。

ステップ 2 次の認証方式のいずれかを選択します。

- パスワードベース：管理者ログインで標準のユーザ ID およびパスワード クレデンシャルを使用する場合は、[パスワードベース（Password Based）] オプションを選択し、[内部（Internal）] または [外部（External）] のいずれかの認証タイプを指定します。

  （注） LDAP などの外部 ID ストアを設定しており、それを認証ソースとして使用して管理者ユーザにアクセス権を付与する場合は、その ID ソースを [ID ソース（Identity Source）] リスト ボックスから選択する必要があります。

- [クライアント証明書ベース（Client Certificate Based）]：証明書ベースのポリシーを指定する場合は、[クライアント証明書ベース（Client Certificate Based）] オプションを選択し、既存の証明書認証プロファイルを選択します。

ステップ 3 [パスワード ポリシー（Password Policy）] タブをクリックし、値を入力します。

ステップ 4 [保存（Save）] をクリックして、管理者パスワード ポリシーを保存します。

（注） 外部IDストアを使用してログイン時に管理者を認証する場合は、管理者プロファイルに適用されるパスワード ポリシーにこの設定値が設定されている場合でも、外部 ID ストアが依然として管理者のユーザ名とパスワードを認証することに留意してください。

関連トピック

管理者パスワード ポリシーの設定 （55 ページ）
管理者アカウントのアカウント無効化ポリシーの設定 （246 ページ）
管理者アカウントのロック設定または一時停止設定 （246 ページ）

管理者アカウントのアカウント無効化ポリシーの設定

Cisco ISE では、設定した連続日数の間に管理者アカウントが認証されなかった場合は、管理者アカウントを無効にすることができます。

ステップ 1 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [アカウント無効化ポリシー（Account Disable Policy）] の順に選択します。

ステップ 2 [非アクティブになってから n 日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオンにして、日数を入力します。

このオプションでは、管理者アカウントが連続する日数非アクティブだった場合に管理者アカウントを無効にすることができます。ただし、[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理ユーザ（Admin Users）] の [非アクティブアカウントを無効化しない（Inactive Account Never Disabled）] オプションを使用して、このアカウント無効化ポリシーから個々の管理者アカウントを除外することができます。

ステップ 3 [保存（Save）] をクリックして、管理者のグローバル アカウント無効化ポリシーを設定します。

管理者アカウントのロック設定または一時停止設定

Cisco ISE では、指定されたログイン試行失敗回数を超えた管理者アカウント（パスワードベースの内部管理者アカウントと証明書ベースの管理者アカウントを含む）をロックまたは一時停止できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] > [ロック/一時停止設定（Lock/Suspend Settings）]** を選択します。

ステップ 2 [ログイン試行が間違っているアカウントを一時停止またはロックする（Suspend or Lock Account With Incorrect Login Attempts）] チェックボックスをオンにして、アクションを実行するまでの試行失敗の回数を入力します。有効な範囲は、3 ～ 20 です。

- [n 分間アカウントを一時停止（Suspend Account For n Minutes）]：指定した間違ったログイン試行回数を超えるアカウントを一時停止するには、このオプションを選択します。有効な範囲は、15 ～ 1440 です。
- [アカウントのロック（Lock Account）]：指定した間違ったログイン試行回数を超えるアカウントをロックするには、このオプションを選択します。

エンドユーザにヘルプデスクに連絡してアカウントのロックを解除するよう要求するなどの、修復を依頼するカスタムの電子メール メッセージを入力することができます。

（注） ロックまたは一時停止設定は、Cisco ISE の以前のリリースでは [パスワード ポリシー（Password Policy）] タブで利用できました。

管理者のセッション タイムアウトの設定

Cisco ISE を使用すると、管理 GUI セッションが非アクティブであっても依然として接続状態である時間を決定できます。分単位の時間を指定することができ、その時間が経過すると Cisco ISE は管理者をログアウトします。セッションのタイムアウト後、管理者は、Cisco ISE 管理者ポータルにアクセスするには再びログインする必要があります。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** > **[セッションのタイムアウト（Session Timeout）]** を選択します。

ステップ 2 アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。

ステップ 3 [**保存（Save）**] をクリックします。

アクティブな管理セッションの終了

Cisco ISE では、すべてのアクティブな管理セッションが表示され、そこからセッションを選択し、必要が生じた場合はいつでも終了できます。同時管理 GUI セッションの最大数は 20 です。GUI セッションの最大数に達した場合、スーパー管理者グループに属する管理者がログインして一部のセッションを終了できます。

始める前に

次のタスクを実行するには、スーパー管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** > **[セッション情報（Session Info）]** を選択します。

ステップ 2 終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。

管理者の名前の変更

Cisco ISE では GUI からユーザ名を変更できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 Cisco ISE UI の右上にリンクとして表示されるユーザ名をクリックします。

ステップ 3 表示される [管理者ユーザ（Admin User）] ページに新しいユーザ名を入力します。

ステップ 4 変更するアカウントに関するその他の詳細を編集します。

ステップ 5 [保存（Save）] をクリックします。

管理者アクセスの設定

これらのページにより、管理者のアクセス設定を行うことができます。

管理者パスワード ポリシーの設定

次の表に、管理者パスワードが満たす必要のある基準を定義するために使用できる [管理者パスワード ポリシー（Administrator Password Policy）] ページのフィールドを示します。このページのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理アクセス（Admin Access）]** > **[認証（Authentication）]** > **[パスワード ポリシー（Password Policy）]** です。

表 *26 :* 管理者パスワード ポリシーの設定

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

フィールド	使用上のガイドライン
パスワードに使用できない文字（Password may not contain）	[管理者名またはその文字の逆順は使用できません（Admin name or its characters in reverse order）]：このチェックボックスをオンにして、管理者ユーザ名またはその文字の逆順での使用を制限します。
	[「cisco」またはその文字の逆順は使用できません（"cisco" or its characters in reverse order）]：このチェックボックスをオンにして、単語「cisco」またはその文字の逆順での使用を制限します。
	[この単語またはその文字の逆順は使用できません（This word or its characters in reverse order）]：このチェックボックスをオンにして、定義したすべての単語またはその文字の逆順での使用を制限します。
	[4 回以上連続する繰り返し文字は使用できません（Repeated characters four or more times consecutively）]：このチェックボックスをオンにして、4回以上連続する繰り返し文字の使用を制限します。

フィールド	使用上のガイドライン
	[辞書の単語、その文字の逆順、または文字の置き換えは使用できません（Dictionary words, their characters in reverse order or their letters replaced with other characters]：辞書の単語、単語の文字の逆順での使用、単語の文字の置き換えでの使用を制限します。 「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば Pa$$w0rd などです。 • [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。 デフォルトでは、このオプションが選択されています。 • [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択（Choose File）] をクリックし、カスタム辞書ファイルを選択します。このテキスト ファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。
必須の文字（Required Characters）	管理者パスワードに、次の選択肢から選択したタイプの文字が少なくとも 1 つ含まれている必要があることを指定します。 • 小文字の英文字 • 大文字の英文字 • 数字（Numeric characters） • 英数字以外の文字（Non-alphanumeric characters）

フィールド	使用上のガイドライン
パスワード履歴（Password History）	同じパスワードが繰り返し使用されるのを防ぐために、新しいパスワードと異なっている必要がある以前のパスワードの数を指定します。 また、以前のパスワードと異なる必要がある文字数を指定します。 ユーザがパスワードを再使用できない日数を入力します。
パスワードライフタイム（Password Lifetime）	次のオプションを指定して、指定した期間後にパスワードを変更するようユーザに強制します。 • パスワードが変更されなかった場合に管理者アカウントを無効にするまでの時間（日数）（Time (in days) before the administrator account is disabled if the password is not changed.）（使用可能な範囲は 0 ～ 2,147,483,647 日です）。 • 管理者アカウントが無効になるまでのリマインダ（日数）。（Reminder (in days) before the administrator account is disabled.）
ネットワーク デバイスの機密データの表示	
管理者パスワードが必要（Require Admin Password）	共有秘密やパスワードなどのネットワーク デバイスの機密データを表示するために管理者ユーザがログイン パスワードを入力するようにする場合には、このチェックボックスにマークを付けます。
パスワードのキャッシュ期間（Password cached for）	管理者ユーザによって入力されたパスワードは、この期間キャッシュされます。管理者ユーザはこの間、ネットワークデバイスの機密データを表示するためにパスワードの再入力を求められることはありません。有効な範囲は 1 ～ 60 分です。

関連トピック

Cisco ISE 管理者 （3 ページ）
新しい管理者の作成 （4 ページ）

セッション タイムアウトおよびセッション情報の設定

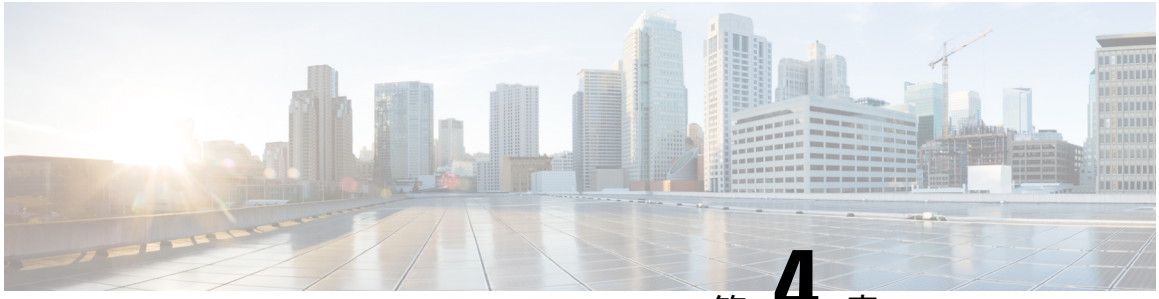
次の表では、セッションタイムアウトを定義し、アクティブな管理セッションを終了するために使用できる[セッション（Session）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** です。

表 *27*：セッション タイムアウトおよびセッション情報の設定

フィールド	使用上のガイドライン
セッションのタイムアウト（Session Timeout）	
セッション アイドル タイムアウト（Session Idle Timeout）	アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。
セッション情報（Session Info）	
無効化（Invalidate）	終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。

関連トピック

管理者アクセスの設定 （243 ページ）
管理者のセッション タイムアウトの設定 （247 ページ）
アクティブな管理セッションの終了 （247 ページ）



第 4 章

メンテナンスとモニタ

適応型ネットワーク制御

適応型ネットワーク制御（ANC）は、管理ノードで実行されるサービスで、エンドポイントのネットワーク アクセスのモニタリングと制御に使用できます。 ANC は、ISE 管理者が管理 GUI で呼び出すことも、サード パーティ システムから pxGrid を介して呼び出すこともできます。ANC は有線展開とワイヤレス展開をサポートし、Plus ライセンスが必要です。

ANC を使用すると、システムの許可ポリシー全体を変更することなく許可状態を変更できます。 ANC を使用すると、 ANCPolicy を確認してネットワーク アクセスを制限または拒否するように許可ポリシーが定義されている場合、確立された許可ポリシーの結果としてエンドポイントを隔離するときの許可状態を設定することができます。エンドポイントを隔離解除して、フル ネットワーク アクセスを可能にできます。ネットワークからエンドポイントを接続解除する Network Attached System（NAS）上のポートをシャットダウンすることもできます。

一度に隔離できるユーザの数に制限はなく、また隔離期間の長さにも制限はありません。

ANC によってネットワーク アクセスをモニタおよび制御するには、次の操作を実行できます。

- 隔離：例外ポリシー（許可ポリシー）を使用して、ネットワークへのエンドポイント アクセスを制限または拒否することができます。 ANCPolicy に応じて異なる許可プロファイル（権限）を割り当てるために、例外ポリシーを作成する必要があります。隔離状態に設定すると、基本的に、デフォルトの VLAN から指定した隔離 VLAN にエンドポイントが移動します。エンドポイントと同じ NAS でサポートされる隔離 VLAN を事前に定義する必要があります。

- 隔離解除：エンドポイントのネットワークへのフル アクセスを許可し、エンドポイントを元の VLAN に戻す隔離ステータスを反転することができます。

- シャットダウン：NAS 上のポートを非アクティブ化し、ネットワークからエンドポイントを接続解除することができます。エンドポイントが接続されている NAS 上のポートがシャットダウンされた後、エンドポイントがネットワークに接続できるようにするには、

NAS 上のポートを手動で再度リセットする必要があります。このことは無線展開では実行できません。

アクティブ エンドポイントに対する隔離および隔離解除操作は、セッション ディレクトリ レポートからトリガーできます。

（注） 隔離されていたセッションが隔離解除された場合、新たに隔離解除されたセッションの開始方法は、スイッチ設定で指定されている認証方法によって決まります。

Cisco ISE での適応型ネットワーク制御の有効化

ANC は、デフォルトで無効になっています。pxGrid が有効にされた場合にのみ有効になり、管理者ポータルでサービスを手動で無効にするまで有効のままになります。

ネットワーク アクセスの設定

ANC によって、ネットワーク アクセス ステータスをリセットして、ポートを隔離、隔離解除、またはシャットダウンすることができます。これにより、ネットワーク アクセス ステータスに応じたネットワークへの許可が定義されます。

エンドポイントの隔離や隔離解除、またはエンドポイントが接続されているネットワーク アクセス サーバ（NAS）ポートのシャットダウンを行うには、エンドポイントの IP アドレスまたは MAC アドレスを使用します。同時に実行しない限り、同じエンドポイントに複数回、隔離操作および隔離解除操作を実行できます。ネットワーク上に悪意のあるエンドポイントを見つけた場合は、 ANC を使用してそのエンドポイントのアクセスをシャットダウンし、NAS ポートを閉じることができます。

ANC ポリシーをエンドポイントに割り当てるには、次の手順を実行します。

始める前に

- ANC を有効にする必要があります。
- ANC の許可プロファイルおよび例外タイプの許可ポリシーを作成する必要があります。

ステップ 1 **[操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）] > [ポリシーリスト（Policy List）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ANC ポリシーの名前を入力し、ANC アクションを指定します。次のオプションを使用できます。

- 検疫（Quarantine）
- シャットダウン（Shut_Down）

- ポートバウンス（Port_Bounce）

1 つまたは複数のアクションを選択できますが、[シャットダウン（Shut_Down）] および [ポート バウンス（Port_Bounce）] を他の ANC アクションと組み合わせることはできません。

ステップ 4 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択して、ポリシー セットを展開します。

ステップ 5 ANCPolicy 属性を使用して ANC ポリシーを対応する許可ポリシーに関連付けます。

ステップ 6 [操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）] > [エンドポイント割り当て（Endpoint Assignment）] の順に選択します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 エンドポイントの IP アドレスまたは MAC アドレスを入力し、[ポリシー割り当て（Policy Assignment）] ドロップダウン リストからポリシーを選択します。

ステップ 9 [送信（Submit）] をクリックします。

ANC によるネットワーク アクセスの許可プロファイルの作成

ANC に使用する許可プロファイルを作成する必要があります。許可プロファイルは、標準許可プロファイルのリストに表示されます。エンドポイントはネットワークで認証および許可されますが、ネットワークへのアクセスが制限されています。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 許可プロファイルの一意の名前と説明を入力し、[アクセス タイプ（Access Type）] は [ACCESS_ACCEPT] のままにします。

ステップ 4 [DACL 名（DACL Name）] チェックボックスをオンにし、ドロップダウン リストから [DENY_ALL_TRAFFIC] を選択します。

ステップ 5 [送信（Submit）] をクリックします。

例外許可ポリシーは、特別な条件や権限、または緊急の要件を満たすために制限付きアクセスを許可することを目的としています。ANC 許可用に、すべての標準許可ポリシーの前に処理される隔離例外ポリシーを作成する必要があります。次の条件で例外ルールを作成する必要があります：Session:ANCPolicy EQUALS Quarantine

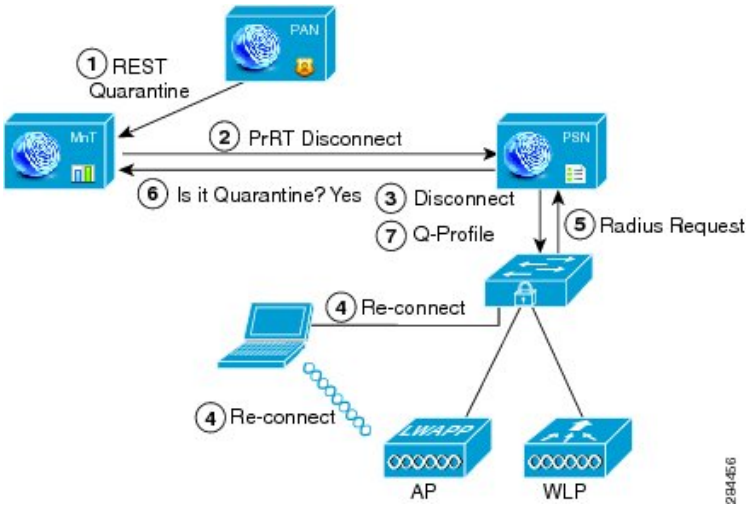
ANC 隔離と隔離解除フロー

選択したエンドポイントのネットワークへのアクセスを制限するために、 ANC を使用してこれらを隔離できます。エンドポイントを隔離し、ステータスに応じて異なる許可プロファイルを割り当てる例外許可ポリシーを確立できます。許可プロファイルは許可ポリシーで定義され

る権限のコンテナとして機能し、許可ポリシーによって特定のネットワーク サービスへのアクセスが許可されます。許可が完了すると、ネットワーク アクセス要求に権限が付与されます。エンドポイントの妥当性が認められた場合には、エンドポイントの隔離を解除してネットワークへのフル アクセスを許可できます。

この図は、隔離フローを示しています。許可ルールが設定され、 ANC セッションが確立されていることを前提としています。

図 *8 : ANC* 隔離フロー



1. クライアント デバイスがワイヤレス デバイス（WLC）を通じてネットワークにログインし、隔離の REST API コールが管理ノード（PAP）からモニタリング ノード（MnT）に発行されます。
2. 続いて、モニタリング ノードは、ポリシー サービス ISE ノード（PDP）を通じて PrRT をコールし、CoA を呼び出します。
3. クライアント デバイスが切断されます。
4. 続いて、クライアント デバイスが再認証および再接続されます。
5. クライアント デバイスに対する RADIUS 要求が、モニタリング ノードに返送されます。
6. チェックが行われている間、クライアント デバイスは隔離されます。
7. Q プロファイル許可ポリシーが適用され、クライアント デバイスの妥当性が確認されます。
8. クライアント デバイスの隔離が解除され、ネットワークにフル アクセスできるようになります。

ANC NAS ポートのシャットダウン フロー

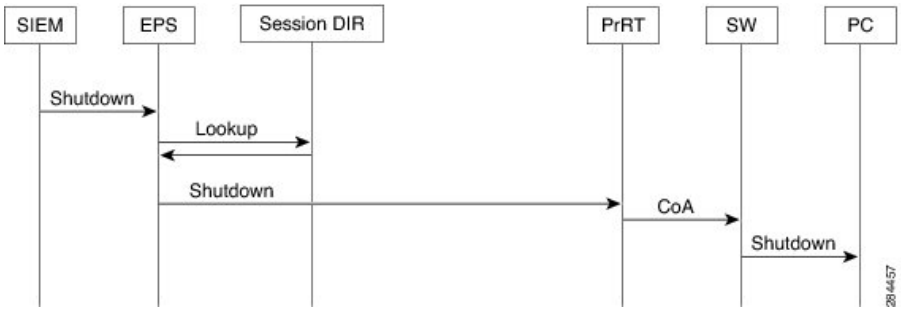
エンドポイントのIPアドレスまたはMACアドレスを使用して、エンドポイントの接続先NASポートをシャット ダウンできます。

シャットダウンでは、MAC アドレスに対して指定された IP アドレスに基づいて NAS ポートを閉じることが可能です。また、手動でポートを復元して、エンドポイントをネットワークに戻す必要があります。これは、有線メディアで接続されたエンドポイントのみに有効です。

シャットダウンはすべてのデバイスでサポートされているわけではありません。ただし、大部分のスイッチでシャットダウン コマンドがサポートされています。getResult() コマンドを使用すると、シャットダウンが正常に実行されたかどうかを確認できます。

この図は、 ANC のシャットダウンのフローを示しています。図のクライアント デバイスでは、このクライアント デバイスがネットワークにアクセスするために使用する NAS でシャットダウン操作が実行されます。

図 *9: ANC* のシャットダウン フロー



エンドポイントの消去の設定

[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント消去（Endpoint Purge）] を使用して、ID グループおよび他の条件に基づいて、設定ルールによってエンドポイント パージ ポリシーを定義できます。指定したエンドポイントを消去しないことや、選択したプロファイリング条件に基づいてエンドポイントを消去することを選択できます。

エンドポイント消去ジョブをスケジュールできます。このエンドポイント消去スケジュールはデフォルトで有効です。Cisco ISE はデフォルトで、30 日よりも古い登録デバイスとエンドポイントを削除します。消去ジョブは、プライマリ PAN で設定された時間帯に基づいて毎日午前 1 時に実行されます。

エンドポイントの消去では、3 分ごとに 5000 エンドポイントが削除されます。

次に、エンドポイントの消去に使用できる条件と例の一部を示します。

- InactivityDays：エンドポイントでの最後のプロファイリング アクティビティまたは更新からの日数。

- この条件によって、時間の経過に伴って蓄積した古いデバイス（一般的には一時的なゲストやパーソナルデバイス）、または廃止されたデバイスが消去されます。これらのエンドポイントは、ネットワーク上でアクティブでないか、近い将来に使用される可能性が低いため、ほとんどの展開でノイズを表す傾向があります。それらが再度接続した場合は、必要に応じて再検出、プロファイリング、登録などが行われます。
- エンドポイントから更新が発生すると、InactivityDaysはプロファイリングが有効である場合にのみ0にリセットされます。

- ElapsedDays：オブジェクトが作成されてからの日数。
  - この条件は、ゲストまたは請負業者のエンドポイント、ネットワーク アクセスにWebAuthを利用する従業員などの、未認証アクセスまたは条件付きアクセスが一定期間認められたエンドポイントに使用できます。許可された接続猶予期間が経過した後、それらは完全に再認証および登録される必要があります。

- PurgeDate：エンドポイントを消去する日付。
  - このオプションは、作成または開始時間に関係なく一定期間のアクセスを許可する、特別なイベントやグループに使用できます。このオプションでは、すべてのエンドポイントを同時に消去できます。たとえば、展示会、会議、または毎週メンバーが入れ替わる週ごとのトレーニング クラスでは、絶対的な日/週/月ではなく、特定の週や月にアクセスを許可する場合に使用します。

隔離済みエンドポイントがポリシー変更の後に認証を更新しない

問題

ポリシー変更またはIDの追加後に認証が失敗し、再認証が行われません。認証が失敗するか、問題のエンドポイントがネットワークに接続できなくなります。この問題は、ユーザロールに割り当てられるポスチャ ポリシーごとのポスチャ評価に失敗するクライアント マシンで頻繁に発生します。

考えられる原因

クライアントマシンで認証タイマーが正しく設定されていないか、またはスイッチ上で認証間隔が正しく設定されていません。

ソリューション

この問題には、解決策がいくつか考えられます。

1. Cisco ISE で、指定された NAD またはスイッチの Session Status Summary レポートを検査し、インターフェイスに適切な認証間隔が設定されていることを確認します。

2. NAD/スイッチ上で "show running configuration" と入力し、適切な「authentication timer restart」設定でインターフェイスが設定されていることを確認します（たとえば、「authentication timer restart 15」および「authentication timer reauthenticate 15」）。
3. NAD/スイッチ上で "interface shutdown" および "no shutdown" と入力してポートをバウンスし、Cisco ISE で変更があったと考えられる場合には再認証を適用します。

（注） CoA は MAC アドレスまたはセッション ID を必要とするので、Network Device SNMP レポートに表示されるポートをバウンスしないように推奨しています。

ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する

エンドポイントで実行する ANC 操作は、そのエンドポイントのアクティブなセッションに IP アドレスに関する情報が含まれていない場合に失敗します。このことは、そのエンドポイントの MAC アドレスおよびセッション ID にも適用されます。

（注） ANC を介してエンドポイントの許可状態を変更する場合は、エンドポイントの IP アドレスまたは MAC アドレスを指定する必要があります。IP アドレスまたは MAC アドレスがエンドポイントのアクティブなセッションで見つからない場合、「この MAC アドレス、IP アドレスまたはセッション ID のアクティブなセッションが見つかりません。（No active session found for this MAC address, IP Address or Session ID.）」というエラー メッセージが表示されます。

外部認証された管理者が ANC 操作を実行できない

外部認証された管理者がライブ セッションから CoA 隔離を発行しようとすると、Cisco ISE は次のエラー メッセージを返します。

「xx: xx: xx: xx: xx: xx に対する隔離の CoA アクションを開始できません。（CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated.）原因：内部でユーザが見つかりません。（Cause:User not found internally.）サポートされていない外部認証されたユーザを使用している可能性があります（Possible use of unsupported externally authenticated user）」

外部認証された管理者が、エンドポイントの IP アドレスまたは MAC アドレスを使用して、Cisco ISE 管理者ポータル内の [操作（Operations）]>[適応型ネットワーク制御（Adaptive Network Control）] から ANC 操作を実行すると、Cisco ISE は次のエラー メッセージを返します。

「サーバ障害：内部でユーザが見つかりません。（Server failure: User not found internally.）サポートされていない外部認証されたユーザを使用している可能性があります（Possible use of unsupported externally authenticated user）」

Cisco ISE ソフトウェアパッチ

Cisco ISE ソフトウェアパッチは通常累積されます。Cisco ISE では、パッチのインストールおよびロールバックを CLI または GUI から実行できます。

展開内の Cisco ISE サーバにパッチをインストールする作業は、プライマリ PAN から行うことができます。プライマリ PAN からパッチをインストールするには、Cisco.com からクライアントブラウザを実行しているシステムにパッチをダウンロードします。

GUI からパッチをインストールする場合、パッチは最初にプライマリ PAN に自動的にインストールされます。その後、システムは、GUI にリストされている順序で、展開内の他のノードにパッチをインストールします。ノードが更新される順序を制御することはできません。また、GUI の [管理者（Administrator）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）] ウィンドウから、手動でパッチバージョンをインストール、ロールバック、および表示することもできます。

CLI からパッチをインストールする場合は、ノードの更新順序を制御できます。ただし、最初にプライマリ PAN にパッチをインストールすることを推奨します。

展開全体をアップグレードする前にいくつかのノードでパッチを検証する場合、CLI を使用すると、選択したノードでパッチをインストールできます。パッチをインストールするには、次の CLI コマンドを使用します。

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

詳細については、『Cisco Identity Services Engine CLI Reference Guide』の「Cisco ISE CLI Commands in EXEC Mode」の章にある「install Patch」の項を参照してください。

必要なパッチバージョンを直接インストールすることができます。たとえば、Cisco ISE 2.x を使用していて、Cisco ISE 2.x パッチ 5 をインストールする場合、以前のパッチ（Cisco ISE 2.x パッチ 1 ～ 4 など）をインストールしなくても、Cisco ISE 2.x パッチ 5 を直接インストールできます。CLI でパッチバージョンを表示するには、次の CLI コマンドを使用します。

```
show version
```

関連トピック

ソフトウェア パッチ インストールのガイドライン （261 ページ）
ソフトウェア パッチ ロールバックのガイドライン （264 ページ）
ソフトウェアパッチのインストール （262 ページ）
ソフトウェアパッチのロールバック （263 ページ）

ソフトウェア パッチ インストールのガイドライン

ISE ノードにパッチをインストールすると、インストールの完了後にノードが再起動されます。再びログインできる状態になるまで、数分かかることがあります。メンテナンスウィンドウ中

にパッチをインストールするようにスケジュール設定し、一時的な機能停止を回避することができます。

インストールするパッチが、ネットワーク内に展開されている Cisco ISE のバージョンに適用されるものであることを確認してください。Cisco ISE はパッチファイルのバージョンの不一致とあらゆるエラーをレポートします。

Cisco ISE に現在インストールされているパッチよりも低いバージョンのパッチをインストールできません。同様に、あるバージョンのパッチの変更をロールバックしようとしたときに、それよりも高いバージョンのパッチがその時点でCisco ISEにインストール済みの場合は、ロールバックはできません。たとえば、パッチ3がCisco ISEサーバにインストール済みの場合に、パッチ1または2をインストールしたり、パッチ1または2にロールバックすることはできません。

分散展開の一部であるプライマリ PAN からパッチのインストールを実行するときは、Cisco ISEによってそのパッチが展開内のプライマリノードとすべてのセカンダリノードにインストールされます。パッチのインストールがプライマリ PAN で成功すると、Cisco ISE はセカンダリノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリノードに進みません。ただし、何らかの理由でセカンダリノードのいずれかでインストールに失敗した場合は、処理が続行され、展開内の次のセカンダリノードでインストールが実行されます。

2 ノード展開の一部であるプライマリ PAN からパッチのインストールを実行するときは、Ciscoによってそのパッチが展開内のプライマリノードとセカンダリノードにインストールされます。パッチのインストールがプライマリ PAN で成功すると、Cisco はセカンダリノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリノードに進みません。

ソフトウェアパッチのインストール

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。
- **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** > **[PANのフェールオーバー（PAN Failover）]** に移動し、[PANの自動フェールオーバーを有効にする（Enable PAN Auto Failover）] チェックボックスがオフになっていることを確認します。このタスクの期間中は、PAN の自動フェールオーバー設定を無効にする必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[メンテナンス（Maintenance）]** > **[パッチ管理（Patch Management）]** > [インストール（Install）] を選択します。

ステップ 2 [参照（Browse）] をクリックし、Cisco.com からダウンロードしたパッチを選択します。

ステップ 3 [インストール（Install）] をクリックしてパッチをインストールします。

PAN でのパッチのインストールが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

（注） パッチインストールの進行中は、[パッチ管理（Patch Management）]ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。

ステップ 4 **[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** を選択して、[パッチのインストール（Patch Installation）] ページに戻ります。

ステップ 5 セカンダリノードにインストールしたパッチの横のオプションボタンをクリックし、[ノードステータスを表示（Show Node Status）] をクリックしてインストールが完了したことを確認します。

次のタスク

1 つ以上のセカンダリノードでパッチをインストールする必要がある場合は、ノードが動作中であることを確認し、プロセスを繰り返して残りのノードにパッチをインストールします。

ソフトウェアパッチのロールバック

複数のノードの展開の一部である PAN からパッチのロールバックを実行するときは、Cisco ISE によってそのパッチが展開内のプライマリノードとすべてのセカンダリノードにロールバックされます。

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** を選択します。

ステップ 2 変更をロールバックするパッチバージョンのオプションボタンをクリックしてから、[ロールバック（Rollback）] をクリックします。

（注） パッチのロールバックの進行中は、[パッチ管理（Patch Management）]ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。

PAN からのパッチのロールバックが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

ステップ 3 ログイン後に、ページの一番下にある [アラーム（Alarms）] リンクをクリックしてロールバック操作のステータスを表示します。

ステップ 4 **[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** を選択します。

ステップ 5 パッチのロールバックの進行状況を表示するには、[パッチ管理（Patch Management）] ページでパッチを選択し、[ノードステータスを表示（Show Node Status）] をクリックします。

ステップ 6 パッチのオプションボタンをクリックし、セカンダリノード上で [ノードステータスを表示（Show Node Status）] をクリックして、そのパッチが展開内のすべてのノードからロールバックされたことを確認します。

そのパッチがロールバックされていないセカンダリノードがある場合は、そのノードが稼働中であることを確認してから、プロセスをもう一度実行して残りのノードから変更をロールバックしてください。Cisco ISE は、このバージョンのパッチがインストールされているノードからのみパッチをロールバックします。

ソフトウェア パッチ ロールバックのガイドライン

展開の Cisco ISE ノードからパッチをロールバックするには、最初に PAN から変更をロールバックします。これに成功すると、セカンダリノードからパッチがロールバックされます。PAN でロールバックプロセスが失敗した場合は、セカンダリノードからのパッチロールバックは行われません。ただし、いずれかのセカンダリノードでパッチのロールバックが失敗しても、展開内の次のセカンダリノードからのパッチのロールバックは継続されます。

Cisco ISE によるセカンダリノードからのパッチロールバックが進行中のときも、引き続き PAN GUI から他のタスクを実行できます。セカンダリノードは、ロールバック後に再起動されます。

パッチのインストールおよびロールバックの変更の表示

インストールされているパッチに関連するレポートを表示するには、次の手順を実行します。

始める前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。**[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** ページで、パッチをインストールまたはロールバックできます。展開内の各ノードで特定のパッチのステータス（[インストール済み（installed）]、[処理中（in-progress）]、[未インストール（not installed）]）を確認できます。このためには、特定のパッチを選択し、[ノードステータスを表示（Show Node Status）] ボタンをクリックします。

ステップ 1 **[操作（Operations）] > [レポート（Reports）] > [監査（Audit）] > [操作監査（Operations Audit）]** を選択します。デフォルトでは、過去 7 日間のレコードが表示されます。

ステップ 2 [フィルタ（Filter）] ドロップダウンをクリックして [クイックフィルタ（Quick Filter）] または [高度なフィルタ（Advanced Filter）] を選択し、必要なキーワード（例：patch install iniated）を使用して、インストール済みのパッチを示すレポートを生成します。

バックアップ データのタイプ

Cisco ISE では、プライマリ PAN とモニタリング ノードからデータをバックアップすることができます。バックアップは CLI またはユーザ インターフェイスから実行できます。

Cisco ISE では次のタイプのデータのバックアップが可能です。

- 設定データ：アプリケーション固有および Cisco ADE オペレーティング システム両方の設定データが含まれます。バックアップは、GUI または CLI を使用してプライマリ PAN を介して実行できます。
- 運用データ：モニタリングおよびトラブルシューティング データが含まれます。バックアップは、プライマリ PAN GUI を介して、またはモニタリング ノードの場合は CLI を使用して実行できます。

Cisco ISE が VMware で実行されている場合、ISE データをバックアップするのに、VMware スナップショットはサポートされていません。

（注） Cisco ISE は、ISE データのバックアップ用の VMware スナップショットをサポートしていません。これは、VMware スナップショットが特定の時点で VM のステータスを保存するためです。マルチノード Cisco ISE 環境では、すべてのノードのデータは、現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。シスコは、データのバックアップおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。

VMware スナップショットまたはサードパーティのバックアップを使用して ISE データをバックアップすると、Cisco ISE サービスが停止します。バックアップが VMware または CommVault SAN レベルのバックアップのようなサードパーティによって開始された場合、ファイル システムを休止してクラッシュ整合を維持するため、ISE のフリーズを引き起こします。ISE のサービスを再開するには再起動が必要です。

例：VM スナップショット、CommVault SAN レベルのバックアップなど。

復元操作は、以前のバージョンの Cisco ISE のバックアップ ファイルを使用して実行でき、以降のバージョンで復元できます。たとえば、Cisco ISE リリース 1.3 または 1.4 からの ISE ノードのバックアップがある場合、そのバックアップを Cisco ISE リリース 2.1 で復元できます。

Cisco ISE リリース 2.4 は、リリース 2.0 以降から取得したバックアップからの復元をサポートしています。

バックアップ/復元リポジトリ

Cisco ISE では管理者ポータルを使用してリポジトリを作成および削除することができます。次のタイプのリポジトリを作成できます。

- ディスク（DISK）
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

（注） リポジトリは、各デバイスに対してローカルです。

どのタイプの展開（小規模、中規模、大規模）であっても、最低でも 100 GB のリポジトリ サイズを用意することを推奨します。

リポジトリの作成

リポジトリを作成するには、CLI と GUI を使用できます。次の理由により、GUI を使用することを推奨します。

- CLI で作成されたリポジトリはローカルに保存され、他の展開ノードに複製されません。これらのリポジトリは、GUI のリポジトリ ページに表示されません。
- プライマリ PAN で作成されたリポジトリは、他の展開ノードに複製されます。

キーはプライマリ PAN でのみ GUI で生成されます。このためアップグレード時に、新しいプライマリ管理ノードの GUI でキーを再生成して、SFTP サーバにエクスポートする必要があります。展開からノードを除去する場合、非管理ノードの GUI でキーを生成し、SFTP サーバにエクスポートする必要があります。

RSA 公開キー認証を使用する Cisco ISE の SFTP リポジトリを設定できます。データベースとログを暗号化するために管理者が作成したパスワードを使用する代わりに、セキュア キーを使用する RSA 公開キー認証を選択できます。RSA 公開キーを使用して作成された SFTP リポジトリの場合、GUI から作成されたリポジトリは CLI では複製されず、CLI から作成されたリポジトリは GUI では複製されません。CLI と GUI で同じリポジトリを設定するには、CLI と GUI の両方で RSA 公開キーを生成し、この両方のキーを SFTP サーバにエクスポートします。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- RSA 公開キー認証を使用する SFTP リポジトリを作成する場合は、次を実行してください。

- SFTP リポジトリの RSA 公開キー認証を有効にします。
- **crypto host_key add** コマンドを使用して Cisco ISE CLI から SFTP サーバのホスト キーを入力します。ホスト キー文字列は、リポジトリの設定ページで、[パス（Path）] フィールドに入力したホスト名と一致する必要があります。
- GUI でキーペアを生成し、ローカル システムに公開キーをエクスポートします。Cisco ISE CLI から **crypto key generate rsa passphrase***test123* コマンドを使用してキー ペアを生成し（この場合パスフレーズは 5 文字以上でなければなりません）、キーを任意のリポジトリ（ローカルディスクまたは設定されているその他のリポジトリ）にエクスポートします。
- エクスポートした RSA 公開キーを PKI 対応の SFTP サーバにコピーし、「authorized_keys」ファイルに追加します。

ステップ 1 [管理（Administration）]>[システム（System）]>[メンテナンス（Maintenance）]>[リポジトリ（Repository）] を選択します。

ステップ 2 [追加（Add）] をクリックして、新しいリポジトリを追加します。

ステップ 3 新しいリポジトリのセットアップの必要に応じて値を入力します。フィールドの説明については、リポジトリの設定 （268 ページ）を参照してください。

ステップ 4 [送信（Submit）] をクリックしてリポジトリを作成します。

ステップ 5 左側の [操作（Operations）] ナビゲーション ペインで [リポジトリ（Repository）] をクリックするか、このページ上部の [リポジトリ リスト（Repository List）] リンクをクリックして、リポジトリのリスト ページに移動して、リポジトリが正常に作成されていることを確認します。

次のタスク

- 作成したリポジトリが有効であることを確認します。これは、リポジトリのリストページから行います。リポジトリを選択し、[確認（Validate）] をクリックします。また、Cisco ISE コマンドライン インターフェイスから次のコマンドを実行することもできます。

  show repository *repository_name*

  ここで、*repository_name* は作成したリポジトリの名前です。

  （注） リポジトリの作成時に指定したパスが存在しない場合、「%無効なディレクトリです（%Invalid Directory）」というエラーが表示されます。

- オンデマンド バックアップを実行するかバックアップのスケジュールを設定します。

リポジトリの設定

次の表では、リポジトリを作成してバックアップ ファイルを保存するために使用できる [リポジトリ リスト（Repository List）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[メンテナンス（Maintenance）]** > **[リポジトリ（Repository）]** です。

表 *28 :* リポジトリの設定

フィールド	使用上のガイドライン
リポジトリ（Repository）	リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。
プロトコル	使用する使用可能なプロトコルの 1 つを選択します。
サーバ名（Server Name）	（TFTP、HTTP、HTTPS、FTP、SFTP、および NFS で必須）リポジトリの作成先サーバのホスト名または IPv4 アドレスを入力します。 （注） IPv6 アドレスを使用してリポジトリを追加する場合は、IPv6 アドレスを使用して ISE eth0 インターフェイスが設定されていることを確認します。
パス	リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。 この値は、サーバのルート ディレクトリを示す 2 つのスラッシュ（//）または単一のスラッシュ（/）で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ（/）はルート ディレクトリではなく FTP ユーザのホーム ディレクトリを示します。
PKI 認証を有効にします。	（オプション：SFTP リポジトリにのみ適用）SFTP リポジトリで RSA 公開キー認証を有効にするには、このチェック ボックスをオンにします。
ユーザ名（User Name）	（FTP、SFTP、および NFS で必須）指定されたサーバに対する書き込み権限を持つユーザ名を入力します。使用できる文字は英数字のみです。

フィールド	使用上のガイドライン
[パスワード（Password）]	（FTP、SFTP、および NFS で必須）指定されたサーバへのアクセスに使用するパスワードを入力します。パスワードに使用できる文字は、0 ～ 9、a ～ z、A ～ Z、-、.、|、@、#、$、%、^、&、*、,、+、および = です。

関連トピック

バックアップ/復元リポジトリ （265 ページ）
リポジトリの作成 （266 ページ）

SFTP リポジトリでの RSA 公開キー認証の有効化

SFTP サーバでは、各ノードに 2 つの RSA 公開キー（CLI 用と GUI 用にそれぞれ 1 つずつ）が必要です。SFTP リポジトリの RSA 公開キー認証を有効にするには、以下のステップに従います。

ステップ 1 */Etc/ssh/sshd_config.file* を編集する権限を持つアカウントで SFTP サーバにログインします。

（注） *sshd_config* ファイルのロケーションは、インストールされているオペレーティング システムによって異なる可能性があります。

ステップ 2 **vi etc/ssh/sshd_config** コマンドを入力します。

Sshd_config ファイルの内容がリストされます。

ステップ 3 RSA 公開キー認証を有効にするには、以下の行の「#」記号を削除します。

- RSAAuthentication yes
- PubkeyAuthentication yes

（注） Public Auth Key が no の場合は yes に変更してください。

- AuthorizedKeysFile ~/.ssh/authorized_keys

オンデマンドおよびスケジュール バックアップ

プライマリ PAN およびプライマリ モニタリング ノードのオンデマンドバックアップを設定できます。バックアップデータがすぐに必要な場合にオンデマンドバックアップを実行します。

システムレベルのバックアップは、1 回のみ、毎日、毎週、または毎月実行するようにスケジュールできます。バックアップ操作は長時間かかる場合がありますが、スケジュールできる

ため中断が発生することはありません。管理者ポータルからバックアップをスケジュールできます。

（注） 内部 CA を使用している場合は、CLI を使用して証明書とキーをエクスポートする必要があります。管理ポータルのバックアップでは、CA チェーンはバックアップされません。

詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Basic Setup」の章にある「Export Cisco ISE CA Certificates and Keys」の項を参照してください。

関連トピック

メンテナンスの設定 （1373 ページ）

オンデマンド バックアップの実行

オンデマンドバックアップを実行して、即座に設定データまたはモニタリング（運用）データをバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。

重要 バックアップと復元を行う場合、復元によって、ターゲット システムの信頼できる証明書のリストがソース システムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  長所：ソース システムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲット システムによって発行された新しい証明書は、同じキーによって署名されます。

  短所：復元機能を使用する前にターゲット システムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  長所：このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソース システムによって発行された証明書は引き続き信頼されます。

  短所：復元機能を使用する前にターゲット システムによって発行された証明書は信頼されないため、再発行する必要があります。

始める前に

- この作業を実行する前に、Cisco ISE のバックアップ データのタイプの基本を理解している必要があります。
- バックアップファイルを格納するリポジトリを作成したことを確認します。
- ローカルリポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- バックアップを取得する前に、すべての証明書関連の変更を実行します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

（注） バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。バックアップを復元するには、リポジトリを選択し、[復元（Restore）] をクリックします。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 バックアップのタイプ [設定（Configuration）] または [動作中（Operational）] を選択します。

ステップ 3 [すぐにバックアップ（Backup Now）] をクリックします。

ステップ 4 バックアップを実行するために必要な値を入力します。

ステップ 5 [OK][バックアップ（Backup）]をクリックします。

ステップ 6 バックアップが正常に完了したことを確認します。

Cisco ISE はタイムスタンプを持つバックアップ ファイル名を付け、指定されたリポジトリにファイルを保存します。タイムスタンプに加えて、Cisco ISE は設定バックアップには CFG タグ、操作バックアップには OPS タグを追加します。バックアップファイルが指定リポジトリにあることを確認します。

分散展開では、バックアップの実行中にノードのロールを変更したり、ノードの設定を行ったりすることはできません。バックアップの実行中にノードのロールを変更すると、すべてのプロセスがシャットダウンし、データに不一致が生じる場合があります。ノードのロールを変更する際は、バックアップが完了するまで待機してください。

バックアップの実行中はノードを昇格しないでください。これによりすべてのプロセスがシャットダウンし、バックアップを同時に実行中の場合はデータに不一致が生じる場合があります。ノードを変更する際は、バックアップが完了するまで待ってください。

（注） バックアップが実行されているときに、高いCPU使用率が観察されたり、[負荷平均が高い（High Load Average）] アラームが表示されたりする可能性があります。バックアップが完了すると、CPU 使用率は通常に戻ります。

関連トピック

Cisco ISE 復元操作 （278 ページ）
認証および許可ポリシー設定のエクスポート （285 ページ）

オンデマンド バックアップの設定

次の表では、バックアップを任意の時点で取得するために使用できる [オンデマンド バックアップ（On-Demand Backup）] ページのフィールドについて説明します。このページへのナビ

ゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup & Restore）]** です。

表 *29* : オンデマンド バックアップの設定

フィールド	使用上のガイドライン
バックアップ名（Backup Name）	バックアップ ファイルの名前を入力します。
リポジトリ名（Repository Name）	バックアップファイルを保存するリポジトリ。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（Encryption Key）	このキーは、バックアップ ファイルの暗号化および解読に使用されます。

関連トピック

バックアップ データのタイプ （265 ページ）
オンデマンドおよびスケジュール バックアップ （269 ページ）
バックアップ履歴 （277 ページ）
バックアップの失敗 （277 ページ）
Cisco ISE 復元操作 （278 ページ）
認証および許可ポリシー設定のエクスポート （285 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （286 ページ）
オンデマンド バックアップの実行 （270 ページ）

バックアップのスケジュール

オンデマンドバックアップを実行して、即座に設定データまたはモニタリング（運用）データをバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。

重要 バックアップと復元を行う場合、復元によって、ターゲットシステムの信頼できる証明書のリストがソースシステムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  長所：ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲットシステムによって発行された新しい証明書は、同じキーによって署名されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  長所：このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソースシステムによって発行された証明書は引き続き信頼されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

始める前に

- この作業を実行する前に、Cisco ISE のバックアップ データのタイプの基本を理解している必要があります。
- リポジトリを設定していることを確認します。
- ローカル リポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- Cisco ISE 1.1 以前のリリースから Cisco ISE 1.2 にアップグレードする場合、バックアップのスケジュールを再設定する必要があります。『*Cisco Identity Services Engine Upgrade Guide, Release 1.2*』の「Known Upgrade Issues」の項を参照してください。

（注） バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 [作成（Create）][スケジュール（Schedule）]をクリックして、設定または操作バックアップをスケジュールします。

ステップ 3 必要に応じてバックアップをスケジュールするための値を入力します。

ステップ 4 [保存（Save）] をクリックして、バックアップをスケジュールします。

ステップ 5 次のいずれかの操作を実行します。

- [リポジトリの選択（Select Repository）] ドロップダウンリストから、必要なリポジトリを選択します。
- [リポジトリの追加（Add Repository）] リンクをクリックして新しいリポジトリを追加します。

ステップ 6 [更新（Refresh）] リンクをクリックして、スケジュール バックアップのリストを表示します。

作成できる設定または操作バックアップのスケジュールは 1 回に 1 つだけです。スケジュール バックアップは有効化または無効化できますが、削除はできません。

スケジュール バックアップの設定

次の表では、フル バックアップまたは差分バックアップの復元に使用できる [スケジュール バックアップ（Scheduled Backup）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** です。

表 *30 :* スケジュール バックアップの設定

フィールド	使用上のガイドライン
名前（Name）	バックアップ ファイルの名前を入力します。任意の説明的な名前を入力できます。Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加して、ファイルをリポジトリに格納します。一連のバックアップを設定しても、バックアップ ファイル名は一意になります。[スケジュール バックアップ（Scheduled Backup）] リスト ページでは、ファイルが **kron** occurrence ジョブであることを示すために、バックアップ ファイル名に「backup_occur」が付加されます。 .
説明	バックアップの説明を入力します。
リポジトリ名（Repository Name）	バックアップ ファイルを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（Encryption Key）	バックアップ ファイルを暗号化および復号化するためのキーを入力します。
スケジューリング オプション（Schedule Options）	スケジュール バックアップの頻度を選択し、適宜他のオプションに入力します。

関連トピック

バックアップ データのタイプ （265 ページ）
オンデマンドおよびスケジュール バックアップ （269 ページ）
バックアップ履歴 （277 ページ）
バックアップの失敗 （277 ページ）
Cisco ISE 復元操作 （278 ページ）
認証および許可ポリシー設定のエクスポート （285 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （286 ページ）
CLI を使用したバックアップ （277 ページ）
バックアップのスケジュール （273 ページ）

CLI を使用したバックアップ

CLI と GUI の両方からバックアップをスケジュールできますが、GUI から実行することを推奨します。ただし、セカンダリ モニタリング ノードの操作バックアップは、CLI からのみ実行できます。

バックアップ履歴

バックアップ履歴は、スケジュールまたはオンデマンドバックアップに関する基本情報です。バックアップ履歴には、バックアップ名、バックアップ ファイルのサイズ、バックアップが保存されているリポジトリ、バックアップが取られたタイム スタンプを表示します。この情報は、操作監査レポートまたは、履歴テーブルの [バックアップ/復元（Backup and Restore）] ページから入手できます。

バックアップが失敗すると、Cisco ISE がアラームをトリガーします。バックアップ履歴ページに失敗の原因が表示されます。障害の原因は操作監査レポートにも記載されます。障害の原因が欠落しているか明確でない場合は、Cisco ISE CLI から **backup-logs** コマンドを実行し、ADE.log でより詳細な情報を確認できます。

バックアップ操作の実行中は、**show backup status** CLI コマンドを使用して、バックアップ操作の進行状況を確認することができます。

バックアップ履歴は、Cisco ADE オペレーティング システムの設定データとともに保存されています。つまり、アプリケーションのアップグレード後もそこに残っており、PAN のイメージを再作成した場合にのみ削除されます。

バックアップの失敗

バックアップが失敗した場合は、次を確認してください。

-
- 他のバックアップが同時に実行されていないことを確認します。
- 設定したリポジトリの使用可能なディスク領域を確認します。
    - （操作）バックアップのモニタリングは、モニタリング データがモニタリング データベースに割り当てられたサイズの 75% を超えると失敗します。たとえばモニタリング ノードに 600 GB 割り当てられており、モニタリング データがストレージの 450 GB を超える領域を消費すると、モニタリングのバックアップは失敗します。
    - データベースのディスク使用量が 90% を超える場合、消去が発生してデータベースを割り当てられたサイズの 75% 以下のサイズにします。
- 消去が進行中かどうかを確認します。消去の進行中はバックアップ/復元操作は動作しません。
- リポジトリが正しく設定されていることを確認します。

Cisco ISE 復元操作

プライマリまたはスタンドアロン 管理ノードで設定データを復元できます。プライマリ PAN にデータを復元したら、手動でセカンダリ ノードをプライマリ PAN と同期する必要があります。

運用データを復元するプロセスは、展開のタイプによって異なります。

（注） Cisco ISE の新しいバックアップ/復元ユーザ インターフェイスでは、バックアップ ファイル名にメタデータが使用されます。したがって、バックアップが完了後に、バックアップ ファイル名を手動で変更しないでください。バックアップ ファイルの名前を手動で変更すると、Cisco ISE バックアップ/復元ユーザ インターフェイスがそのバックアップ ファイルを認識できなくなります。バックアップ ファイル名を変更しなければならない場合は、バックアップの復元に Cisco ISE CLI を使用する必要があります。

データの復元に関するガイドライン

次は、Cisco ISE バックアップ データを復元する場合に従うべきガイドラインです。

- Cisco ISE では、ある ISE ノード（A）からバックアップを取得して、別の ISE ノード（B）に復元することができます。両方のノードは同じホスト名（IP アドレスは異なる）です。ただし、ノード B 上のバックアップを復元した後は、証明書とポータル グループ タグの問題が生じる可能性があるため、ノード B のホスト名を変更することはできません。
- あるタイムゾーン内のプライマリ PAN からバックアップを取得して、別のタイムゾーン内の別の Cisco ISE ノードに復元する場合、復元プロセスが失敗することがあります。この問題は、バックアップ ファイルのタイムスタンプが、バックアップが復元される Cisco ISE ノードのシステム時刻より新しい場合に発生します。同じバックアップを、取得後 1 日経過してから復元すると、バックアップ ファイルのタイムスタンプが過去のものになり、復元プロセスは成功します。
- バックアップを取得したホスト名と別のホスト名を持つプライマリ PAN にバックアップを復元すると、プライマリ PAN はスタンドアロン ノードになります。展開が切断し、セカンダリ ノードは機能しなくなります。スタンドアロン ノードをプライマリ ノードにし、セカンダリ ノードの設定をリセットしてプライマリ ノードに再登録する必要があります。Cisco ISE ノードの設定をリセットするには、Cisco ISE CLI から次のコマンドを入力してください。
  - **application reset-config ise**
- システムのタイムゾーンは、最初の Cisco ISE インストールおよびセットアップ後に変更しないことを推奨します。

- 展開の 1 つ以上のノードの証明書設定を変更した場合は、データを復元するための別のバックアップをスタンドアロン Cisco ISE ノードまたはプライマリ PAN から取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。
- プライマリ PAN 上で設定バックアップを復元した後に、以前にエクスポートした Cisco ISE CA 証明書およびキーをインポートできます。

（注） Cisco ISE CA 証明書およびキーをエクスポートしなかった場合は、プライマリ PAN 上で設定バックアップを復元した後に、プライマリ PAN およびポリシー サービス ノード（PSN）でルート CA および下位 CA を生成します。

- 適切な FQDN（プラチナ データベースの FQDN）を使用せずにプラチナ データベースを復元する場合は、CA 証明書を再生成する必要があります。（[管理（Administration）]>[証明書（Certificates）]>[証明書署名要求（Certificate Signing Requests）]>[ISEルートCA証明書チェーンの置き換え（Replace ISE Root CA certificate chain）] を選択します）。ただし、適切な FQDN でプラチナ データベースを復元する場合は、CA 証明書が自動的に再生成されます。
- Cisco ISE がバックアップ ファイルを格納するデータ リポジトリが必要です。オンデマンドまたはスケジュール設定されたバックアップを実行する前に、リポジトリを作成する必要があります。
- スタンドアロン管理ノードに障害が発生した場合、設定バックアップを実行して復元する必要があります。プライマリ PAN で障害が発生した場合、分散セットアップを使用してセカンダリ管理ノードをプライマリに昇格できます。その後、新しいプライマリ PAN にデータを復元できます。

（注） Cisco ISE では、**backup-logs** CLI コマンドも使用できます。このコマンドを使用して、ログやコンフィギュレーション ファイルの収集を行い、これらをトラブルシューティングに利用できます。

CLI からの設定またはモニタリング（操作）バックアップの復元

Cisco ISE CLI から設定データを復元するには、EXEC モードで **restore** コマンドを使用します。設定または操作バックアップからデータを復元するには、次のコマンドを使用します。

restore *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

構文の説明

restore	設定または操作バックアップからデータを復元するには、このコマンドを入力します。
filename	リポジトリに存在するバックアップ ファイルのファイル名。最大 120 文字の英数字をサポートします。 （注） ファイル名の後に、tar.gpg という拡張子を付ける必要があります（myfile.tar.gpg など）。
repository	バックアップを含むリポジトリを指定します。
repository-name	バックアップを復元するリポジトリの名前。
encryption-key	（オプション）バックアップを復元するユーザ定義の暗号キーを指定します。
hash	バックアップを復元するためのハッシュされた暗号キー。使用する暗号化された（ハッシュ化された）暗号化キーを指定します。40 文字までで指定します。
plain	バックアップを復元するためのプレーン テキストの暗号キー。使用する暗号化されたプレーンテキストの暗号化キーを指定します。15 文字までで指定します。
encryption-key name	暗号キーを入力します。
include-adeos	（オプション、設定バックアップのみに該当）設定バックアップから ADE-OS 設定を復元する場合に、このコマンド オペレータ パラメータを入力します。設定バックアップを復元する場合にこのパラメータを含めないと、Cisco ISE は Cisco ISE アプリケーション設定データのみを復元します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

使用上のガイドライン

Cisco ISE で restore コマンドを使用すると、Cisco ISE サーバが自動的に再起動します。

データの復元処理で、暗号キーはオプションです。暗号キーを指定しなかった以前のバックアップの復元をサポートするために、暗号キーなしで **restore** コマンドを使用できます。

例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

関連コマンド

	Description
backup	バックアップ（Cisco ISE と Cisco ADE OS）を実行して、そのバックアップをリポジトリに保存します。
backup-logs	システム ログをバックアップします。
repository	バックアップ設定のリポジトリ サブモードを入力します。
show repository	特定のリポジトリにある使用可能なバックアップ ファイルを表示します。
show backup history	システムのバックアップ履歴を表示します。
show backup status	バックアップ操作のステータスを表示します。
show restore status	復元操作のステータスを表示します。

いずれかのセカンダリ ノードでアプリケーション復元後の同期ステータスおよび複製ステータスが [非同期（Out of Sync）] になっている場合、該当セカンダリ ノードの証明書をプライマリ PAN に再インポートして、手動同期を実行する必要があります。

GUI からの設定バックアップの復元

管理者ポータルで設定バックアップを復元できます。GUI には現在のリリースから取得されたバックアップのみが表示されます。このリリースより前のバックアップを復元するには、CLI から restore コマンドを使用します。

始める前に

プライマリ PAN の自動フェールオーバー設定が展開でイネーブルになっている場合はオフにします。設定バックアップを復元すると、アプリケーション サーバ プロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ PAN の自動フェールオーバーが開始される場合があります。

（注） コンフィギュレーション データベースのバックアップを復元し、プライマリ PAN でのみルート CA を再生成することができます。ただし、登録済みの PAN でコンフィギュレーションデータベースのバックアップは復元できません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 バックアップの名前を設定バックアップのリストから選択し、[復元（Restore）] をクリックします。

ステップ 3 バックアップ時に使用した暗号キーを入力します。

ステップ 4 [復元（Restore）] をクリックします。

次のタスク

Cisco ISE CA サービスを使用する場合は、次のことを実行する必要があります。

1. Cisco ISE CA ルート チェーン全体を再生成します。
2. Cisco ISE CA 証明書およびキーのバックアップをプライマリ PAN から取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN が外部 PKI のルート CA または下位 CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

モニタリング データベースの復元

モニタリングデータベースを復元するプロセスは、展開のタイプによって異なります。次の項では、スタンドアロンおよび分散展開でモニタリングデータベースを復元する方法について説明します。

Cisco ISE の以前のリリースからのオンデマンド モニタリング データベースのバックアップを復元するには、CLI を使用する必要があります。Cisco ISE リリース間でのスケジュール バックアップの復元はサポートされていません。

（注） データが取得されたノードとは別のノードにデータを復元しようとする場合、新しいノードを指すロギング ターゲット設定を設定する必要があります。これにより、モニタリング syslog が正しいノードに送信されるようになります。

スタンドアロン環境でのモニタリング（運用）バックアップの復元

GUIには現在のリリースから取得されたバックアップのみが表示されます。前のリリースから取得されたバックアップを復元するには、CLI から restore コマンドを使用します。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 バックアップの名前を操作バックアップのリストから選択し、[復元（Restore）] をクリックします。

ステップ 3 バックアップ時に使用した暗号キーを入力します。

ステップ 4 [復元（Restore）] をクリックします。

管理およびモニタリングペルソナによるモニタリング バックアップの復元

管理およびモニタリング ペルソナを使用して、分散環境でのモニタリング バックアップを復元することができます。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 プライマリとセカンダリ PAN を使用している場合は、PAN と同期します。

PAN と同期する場合、アクティブなプライマリに昇格するように PAN を選択する必要があります。

ステップ 2 モニタリング ノードを登録解除する前に、モニタリング ペルソナを展開内の別のノードに割り当てます。

展開ごとに、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 3 バックアップされるモニタリング ノードを登録解除します。

ステップ 4 新しく登録解除されたノードにモニタリング バックアップを復元します。

ステップ 5 現在の管理ノードにより新たに復元されたノードを登録します。

ステップ 6 新たに復元されて登録されたノードをアクティブなモニタリング ノードに昇格します。

モニタリング ペルソナによるモニタリング バックアップの復元

分散環境のモニタリング バックアップは、モニタリング ペルソナによってのみ復元できます。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 復元されるノードを登録解除する準備を行います。そのためには、モニタリング ペルソナを展開内の別のノードに割り当てます。

展開内に、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 2 復元されるノードを登録解除します。

（注） 登録解除が完了するのを待機してから、復元に進みます。復元を続行する前に、ノードがスタンドアロン状態になっている必要があります。

ステップ 3 新しく登録解除されたノードにモニタリング バックアップを復元します。

ステップ 4 現在の管理ノードにより新たに復元されたノードを登録します。

ステップ 5 新たに復元されて登録されたノードを PAN に昇格します。

復元履歴

操作監査レポートからは、すべての復元操作、ログイベント、ステータスに関する情報を取得することができます。

（注） ただし操作監査レポートには、前回の復元操作に対応する開始時間に関する情報はありません。

トラブルシューティング情報を入手するには、Cisco ISE CLI から **backup-logs** コマンドを実行して、ADE.log ファイルを調べる必要があります。

復元操作の進行中は、すべての Cisco ISE サービスは停止します。**show restore status** CLI コマンドを使用して、復元操作の進行状況を確認できます。

認証および許可ポリシー設定のエクスポート

認証および許可ポリシー設定を XML ファイルの形式でエクスポートし、これをオフラインで読み取って設定エラーを特定し、トラブルシューティングのために使用できます。この XML ファイルには認証および許可ポリシー ルール、単純および複合ポリシー条件、dACL、および許可プロファイルが含まれます。XML ファイルを電子メールで送信するか、ローカル システムに保存することを選択できます。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup & Restore）]** を選択します。

ステップ 2 [ポリシーのエクスポート（Policy Export）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [エクスポート（Export）] をクリックします。

XML ファイルの内容を表示するには、ワードパッドなどのテキスト エディタを使用します。

ポリシーのエクスポート設定のスケジュール

次の表では、[ポリシーのエクスポートのスケジュール（Schedule Policy Export）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup and Restore）]** > **[ポリシーのエクスポート（Policy Export）]** です。

表 *31* : ポリシーのエクスポート設定のスケジュール

フィールド	使用上のガイドライン
暗号化（Encryption）	

フィールド	使用上のガイドライン
暗号化キー（Encryption Key）	エクスポート データを暗号化および復号化するためのキーを入力します。このフィールドは、[暗号キーを使用したエクスポート（Export with Encryption Key）] オプションを選択した場合にのみ有効になります。
[接続先（Destination）]	
ローカルコンピュータにファイルをダウンロード（Download file to local computer）	ポリシー エクスポート ファイルをローカル システムにダウンロードできます。
[ファイルをメールで送信（Email file to）]	複数の電子メール アドレスをカンマで区切って入力します。
リポジトリ（Repository）	エクスポート データを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。ポリシーのエクスポートのスケジュールを設定する前に、リポジトリを作成してください。
今すぐエクスポート（Export Now）	指定したリポジトリにデータをすぐにエクスポートするには、このオプションをクリックします。
スケジュール	
スケジューリング オプション（Schedule Options）	エクスポートのスケジュールの頻度を選択し、それに応じてその他の詳細を入力します。

分散環境でのプライマリノードとセカンダリノードの同期

分散環境では、PANのバックアップファイルの復元後に、プライマリおよびセカンダリノードの Cisco ISE データベースが自動的に同期されないことがあります。この場合には、PAN からセカンダリ ISE ノードへの完全複製を手動で強制実行できます。強制同期は、PANからセカンダリ ノードにのみ可能です。同期操作中は、設定を変更することはできません。Cisco ISE では、同期が完全に完了した後にのみ、他の Cisco ISE 管理者ポータル ページに移動して設定変更を行うことができます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 非同期レプリケーション ステータスのセカンダリ ISE ノードの横にあるチェックボックスをオンにします。

ステップ 3 [同期を更新（Syncup）] をクリックし、ノードが PAN と同期されるまで待ちます。Cisco ISE 管理者ポータルへのアクセスは、このプロセスが完了するのを待たなければなりません。

スタンドアロンおよび分散展開での失われたノードの復元

この項では、スタンドアロンおよび分散展開での失われたノードの復元に使用できるトラブルシューティング情報を提供します。次の使用例の一部では、失われたデータの復旧にバックアップと復元機能を使用し、その他の使用例では、複製機能を使用しています。

分散展開での既存IPアドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。復元後に、既存 IP アドレスとホストネームを使用します。

たとえば、2 つのノード、N1（プライマリ ポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリ ポリシー管理ノードすなわちセカンダリ PAN）があります。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。

前提

展開内のすべての Cisco ISE ノードが破壊されました同じホスト名と IP アドレスを使用して、新しいハードウェアのイメージが作成されました。

解決手順（Resolution Steps）

1. N1 および N2 ノードの両方を置き換える必要があります。N1 および N2 ノードはスタンドアロン構成になりました。
2. N1 と N2 のノードの UDI を使用してライセンスを取得し、N1 ノードにインストールします。

3. 置き換えたN1ノードでバックアップを復元する必要があります。復元スクリプトはN2にデータを同期しようとしますが、N2 はスタンドアロン ノードであるため同期は失敗します。N1 のデータは時刻 T1 にリセットされます。
4. N1 の管理者ポータルにログインして、N2 ノードを削除して再登録する必要があります。これで、N1 および N2 ノードのデータが時刻 T1 にリセットされます。

分散展開の新IPアドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。新しいハードウェアのイメージが新しい場所で再作成され、新しい IP アドレスとホスト名が必要です。

たとえば、2 つの ISE ノード N1（プライマリ ポリシー管理ノード（プライマリ PAN））と N2（セカンダリ ポリシー サービス ノード）があります。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。Cisco ISE ノードが新しいロケーションで置き換えられ、新しいホスト名は N1A（プライマリ PAN）および N2A（セカンダリ ポリシー サービス ノード）です。N1A および N2A はこの時点ではスタンドアロン ノードです。

前提条件

展開内のすべての Cisco ISE ノードが破壊されました新しいハードウェアのイメージが、異なるホスト名と IP アドレスを使用して異なる場所で作成されました。

解決手順（Resolution Steps）

1. N1 のバックアップを入手し、これを N1A 上で復元します。復元スクリプトは、ホスト名とドメイン名の変更を認識し、現在のホスト名に基づいて展開設定内のホスト名とドメイン名を更新します。
2. 新しい自己署名証明書を生成する必要があります。
3. N1A で Cisco ISE 管理者ポータルにログインし、**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択して、次の操作を行う必要があります。

   古い N2 ノードを削除します。

   新しい N2A ノードをセカンダリ ノードとして登録します。N1A ノードのデータが N2A ノードに複製されます。

スタンドアロン展開の既存IPアドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノードN1があったとします。N1データベースのバックアップは、時刻 T1 に取得されました。物理的な障害により N1 ノードがダウンし、イメージの再作成または新しいハードウェアが必要です。N1 ノードを、同じ IP アドレスとホスト名を使用して回復させる必要があります。

前提条件

この展開はスタンドアロン展開であり、新規またはイメージを再作成したハードウェアは、同じ IP アドレスとホスト名を持ちます。

解決手順（Resolution Steps）

イメージの再作成後、または同一 IP アドレスとホスト名で新しい Cisco ISE ノードを導入した後に N1 ノードが起動したら、古い N1 ノードから取得したバックアップを復元する必要があります。ロールを変更する必要はありません。

スタンドアロン展開の新 IP アドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノード N1 があったとします。時刻 T1 に取得された N1 データベースのバックアップが利用可能です。物理的な障害により N1 ノードがダウンし、異なる IP アドレスとホスト名を使用した新しいハードウェアに別のロケーションで置き換えられます。

前提条件

これはスタンドアロン展開であり、置き換えられたハードウェアは、異なる IP アドレスとホスト名を持ちます。

解決手順（Resolution Steps）

1. 新しいハードウェアで N1 ノードを置き換えます。このノードはスタンドアロン状態となり、ホスト名は N1B です。
2. バックアップを N1B ノード上で復元できます。ロールを変更する必要はありません。

設定のロール バック

問題

意図せずに設定を変更してしまい、後でそれが正しくないことがわかる場合があります。たとえば、いくつかの NAD を削除したり、一部の RADIUS 属性を誤って修正したりして、数時間後にこの問題に気付く場合があります。この場合、変更を行う前に取得したバックアップを復元することにより、元の設定に戻すことができます。

考えられる原因

N1（プライマリ ポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリ ポリシー管理ノードすなわちセカンダリ PAN）の 2 つのノードがあり、N1 ノードのバックアップを使用できます。N1 上で誤った変更をいくつか行い、変更を元に戻す必要があります。

ソリューション

誤った設定変更を行う前に取得したN1ノードのバックアップを入手します。N1ノード上でこのバックアップを復元します。復元スクリプトにより、N1 のデータで N2 が同期されます。

分散展開での障害発生時のプライマリ ノードの復元

シナリオ

マルチノード展開内で、PAN に障害が発生しました。

たとえば、2 つの Cisco ISE ノード、N1（PAN）と N2（セカンダリ管理ノード）があります。ハードウェアの問題で N1 に障害が発生します。

前提条件

分散展開内のプライマリ ノードのみに障害が発生します。

解決手順（Resolution Steps）

1. N2 管理者ポータルにログインします。**[管理（Administration）]**>**[システム（System）]**>**[展開（Deployment）]** を選択して、N2 をプライマリ ノードとして設定します。

   N1 ノードが新しいハードウェアで置き換えられ、イメージが再作成され、スタンドアロン状態となります。

2. N2 管理者ポータルで、セカンダリ ノードとして新しい N1 ノードを登録します。

   これで、N2 ノードがプライマリ ノードになり、N1 ノードがセカンダリ ノードになります。

N1 ノードを再びプライマリ ノードにするには、N1 の管理者ポータルにログインして、このノードをプライマリ ノードに設定します。N2 は、自動的にセカンダリ サーバとなります。データが失われることはありません。

分散展開での障害発生時のセカンダリ ノードの復元

シナリオ

マルチノード展開で、1台のセカンダリ ノードに障害が発生しました。復元の必要はありません。

たとえば、N1（プライマリ PAN）、N2（セカンダリ PAN）、N3（セカンダリ ポリシー サービス ノード）、N4（セカンダリ ポリシーサービス ノード）の複数のノードが存在します。セカンダリノードの 1 つである N3 に障害が発生しました。

解決手順（Resolution Steps）

1. 新しいN3A ノードのイメージを再作成して、デフォルトのスタンドアロン状態にします。
2. N1 の管理者ポータルにログインし、N3 ノードを削除します。
3. N3A ノードを登録します。

   N1 から N3A へ、データが複製されます。復元の必要はありません。

Cisco ISE ロギング メカニズム

Cisco ISE には、監査、障害管理、およびトラブルシューティングに使用されるロギング メカニズムが備わっています。このロギング メカニズムは、展開されたサービスの障害状態を識別したり、問題のトラブルシューティングを効率的に行う場合に役立ちます。また、プライマリ ノードのモニタリングおよびトラブルシューティングのロギング出力が一貫した形式で生成されます。

仮想ループバック アドレスを使用してローカル システムにログを収集するように Cisco ISE ノードを設定できます。ログを外部に収集するには、ターゲットと呼ばれる外部syslogサーバを設定します。ログは事前定義された各種のカテゴリに分類されます。ターゲット、重大度レベルなどに応じてカテゴリを編集することにより、ロギング出力をカスタマイズできます。

ベストプラクティスとして、Cisco ISEのモニタリングおよびトラブルシューティング（MnT）ノードに syslog を送信するようにネットワーク デバイスを設定しないでください。これは、一部のネットワーク アクセス デバイス（NAD）の syslog が失われる可能性があるほか、MnT サーバが過負荷になりロードの問題が発生するためです。

（注） モニタリング ノードがネットワーク デバイスの syslog サーバとして設定されている場合、ロギング ソースが次の形式で正しいネットワーク アクセス サーバ（NAS）の IP アドレスを送信することを確認してください。

<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

そうしないと、これは NAS の IP アドレスに依存する機能に影響を及ぼすことがあります。

syslog の消去の設定

このプロセスを使用して、ローカル ログ格納期間を設定し、特定の期間後にローカル ログを削除します。

ステップ 1 **[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ローカルログ設定（Local Log Settings）]** を選択します。

ステップ 2 [ローカル ログ格納期間（Local Log Storage Period）] フィールドに、設定ソースでログ エントリを保持する最大日数を入力します。

localStore フォルダのサイズが 97 GB に達した場合、ログは設定された [ローカルログの保存期間（Local Log Storage Period）] よりも前に削除されることがあります。

ステップ 3 格納期間が経過する前に既存のログ ファイルを削除するには、[今すぐログを削除（Delete Logs Now）] をクリックします。

ステップ 4 **[保存（Save）]** をクリックします。

Cisco ISE システム ログ

Cisco ISE では、システム ログはロギング ターゲットと呼ばれる場所で収集されます。ターゲットは、ログを収集して格納するサーバの IP アドレスを参照します。ログをローカルで生成して格納することも、FTP ファシリティを使用して外部サーバに転送することもできます。Cisco ISE には、次のデフォルト ターゲットがあり、これらはローカル システムのループバック アドレスに動的に設定されます。

- LogCollector：ログ コレクタのデフォルトの syslog ターゲット。
- ProfilerRadiusProbe：プロファイラ Radius プローブのデフォルトの syslog ターゲット。

デフォルトでは、AAA 診断サブカテゴリとシステム診断サブカテゴリのロギング ターゲットは、ディスク領域を減らすために、新規 Cisco ISE インストールまたはアップグレード時に無効になります。これらのサブカテゴリのロギング ターゲットを手動で設定できますが、これらのサブカテゴリのローカル ロギングは常に有効です。

Cisco ISE インストールの最後にローカルに設定されるデフォルトのロギング ターゲットを使用するか、またはログを保存する外部ターゲットを作成することができます。

（注） syslog サーバが分散展開で設定されている場合、syslog メッセージは MnT ノードではなく認証 PSN から syslog サーバへ直接送信されます。

関連トピック

Cisco ISE メッセージ コード （294 ページ）

リモート syslog 収集場所の設定

Web インターフェイスを使用して、システム ログ メッセージの送信先になるリモート syslog サーバ ターゲットを作成できます。ログ メッセージは、syslog プロトコル標準（RFC-3164 を参照）に従ってリモート syslog サーバ ターゲットに送信されます。syslog プロトコルはセキュアでない UDP です。

メッセージは、イベントが発生したときに生成されます。イベントは、プログラムの終了時に表示されるメッセージやアラームなどのステータスを表示するものである場合があります。カーネル、メール、ユーザ レベルなど、異なるファシリティから生成されたさまざまなタイプのイベント メッセージがあります。イベント メッセージは重大度レベルに関連付けられており、管理者はメッセージをフィルタリングし、優先度付けできます。数値コードはファシリティおよび重大度レベルに割り当てられます。syslog サーバはイベント メッセージ コレクタで、これらのファシリティからイベント メッセージを収集します。管理者は、重大度レベルに基づいて、メッセージを転送するイベント メッセージ コレクタを選択できます。

UDP syslog（ログ コレクタ）はデフォルトのリモート ロギング ターゲットです。このロギング ターゲットは、無効にすると、ログ コレクタとして動作しなくなり、[ロギング カテゴリ（Logging Categories）] ページから削除されます。このロギング ターゲットを有効にした場合は、[ロギング カテゴリ（Logging Categories）] ページのログ コレクタになります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 次の必須詳細情報を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リモート ロギング ターゲット（Remote Logging Targets）] ページに移動し、新しいターゲットが作成されたことを確認します。

その後、ロギング ターゲットを、以下のそれぞれのロギング カテゴリにマッピングできます。PSN ノードは、それらのノードで有効になっているサービスに応じて、該当するログをリモート ロギング ターゲットに送信します。

- AAA 監査
- AAA の診断
- アカウンティング（Accounting）
- 外部 MDM
- パッシブ ID
- ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）
- ポスチャおよびクライアント プロビジョニングの診断（Posture and Client Provisioning Diagnostics）

- プロファイラ

展開内のすべてのノードによって、次のカテゴリのログがロギング ターゲットに送信されます。

- 管理および操作の監査（Administrative and Operational Audit）
- システム診断
- システム統計

Cisco ISE メッセージ コード

ロギング カテゴリは、ACS の機能、フロー、または使用例を説明するメッセージ コードのバンドルです。Cisco ISE では、各ログにはログ メッセージの内容に従ってロギング カテゴリにバンドルされているメッセージ コードが関連付けられています。ロギング カテゴリは、含まれているメッセージの内容を説明する場合に役立ちます。

ロギング カテゴリはロギング設定で役立ちます。各カテゴリには、アプリケーションの要件に応じて設定可能な名前、ターゲット、および重大度レベルがあります。

Cisco ISE では、サービスに対して事前定義されたロギング カテゴリ（[ポスチャ（Posture）]、[プロファイラ（Profiler）]、[ゲスト（Guest）]、[AAA（認証、許可、アカウンティング）（AAA (authentication, authorization, and accounting)）] など）が提供されており、これらにログ ターゲットを割り当てることができます。

ロギングカテゴリが [成功した認証（Passed Authentications）] の場合、ローカルロギングを許可するオプションは、デフォルトでは無効になっています。このカテゴリのローカルロギングを有効にすると、運用スペースの使用率が高くなり、iseLocalStore.log とともに prrt-server.log がいっぱいになります。

[成功した認証（Passed Authentications）] のローカルロギングを有効にする場合は、**[管理（Administration）] > [システム（System）] > [ロギング（logging）] > [ロギングカテゴリ（logging Categories）]** に移動し、[カテゴリ（category）] セクションから [成功した認証（Passed Authentications）] をクリックして、[ローカルロギング（Local Logging）] のチェックボックスをオンにします。

関連トピック

メッセージ コードの重大度レベルの設定 （294 ページ）

メッセージ コードの重大度レベルの設定

ログの重大度レベルを設定し、選択したカテゴリのログが格納されるロギング ターゲットを選択できます。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギング カテゴリ（Logging Categories）]** を選択します。

ステップ 2 編集するカテゴリの隣のオプション ボタンをクリックにして、[編集（Edit）] をクリックします。

ステップ 3 必須フィールドの値を変更します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [ロギング カテゴリ（Logging Categories）] ページに移動し、特定のカテゴリに対して行われた設定の変更内容を確認します。

Cisco ISE メッセージ カタログ

可能性があるすべてのログ メッセージと説明を表示するために、[メッセージカタログ（Message Catalog）] ページを使用できます。**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[メッセージ カタログ（Message Catalog）]** を選択します。

[ログ メッセージ カタログ（Log Message Catalog）] ページが表示されます。このページでは、ログ ファイルに記録される可能性があるすべてのログ メッセージを表示できます。すべての Syslog メッセージを CSV ファイル形式でエクスポートするには、[エクスポート（Export）] を選択します。

Cisco ISE から送信される syslog メッセージの包括的なリスト、syslog メッセージの意味、ローカルおよびリモート ターゲットでの syslog メッセージの記録方法については、『Cisco ISE Syslogs』ドキュメントを参照することもできます。

デバッグ ログ

デバッグ ログにより、ブートストラップ、アプリケーション設定、ランタイム、展開、モニタリングとレポート、および公開キー インフラストラクチャ（PKI）に関する情報が取得されます。過去 30 日間の重大アラームと警告アラーム、および過去 7 日間の情報アラームがデバッグ ログに含まれます。

個々のコンポーネントのデバッグ ログ重大度レベルを設定できます。

ノードまたはコンポーネントで [デフォルトにリセット（Reset to Default）] オプションを使用して、ログ レベルを出荷時のデフォルト値に戻すことができます。

ローカル サーバにデバッグ ログを保存できます。

（注） デバッグ ログの設定は、システムをバックアップから復元した場合やアップグレードした場合には保存されません。

関連トピック

デバッグ ログの重大度レベルの設定 （296 ページ）

ノードのロギング コンポーネントの表示

ステップ 1 [管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログ設定（Debug Log Configuration）] を選択します。

ステップ 2 ロギング コンポーネントを表示するノードを選択し、[編集（Edit）] をクリックします。

[デバッグ レベルの設定（Debug Level Configuration）] ページが表示されます。次の詳細情報を表示できます。

- 選択したノードで実行中のサービスに基づくロギング コンポーネントのリスト
- 各コンポーネントの説明
- 個々のコンポーネントに設定されている現在のログ レベル

デバッグ ログの重大度レベルの設定

デバッグ ログの重大度レベルを設定できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログの設定（Debug Log Configuration）]** を選択します。

ステップ 2 ノードを選択して、[編集（Edit）] をクリックします。

[デバッグログの設定（Debug Log Configuration）] ページには、選択したノードで実行されているサービス、および個別のコンポーネントに対して設定されている現在のログ レベルに基づいたコンポーネントのリストが表示されます。

ノードまたはコンポーネントで [デフォルトにリセット（Reset to Default）] オプションを使用して、ログ レベルを出荷時のデフォルト値に戻すことができます。

ステップ 3 ログ重大度レベルを設定するコンポーネントを選択し、[編集（Edit）] をクリックします。[ログレベル（Log Level）] ドロップダウン リストから目的のログ重大度レベルを選択し、[保存（Save）] をクリックします。

（注） runtime-AAA コンポーネントのログ重大度レベルを変更すると、サブコンポーネント prrt-JNI のログ レベルも変更されます。サブコンポーネントのログ レベルを変更しても、その親コンポーネントには影響はありません。

関連トピック

Cisco ISE デバッグ ログ （1589 ページ）

エンドポイントのデバッグ ログ コレクタ

特定のエンドポイントの問題をトラブルシューティングするために、IP アドレスまたは MAC アドレスに基づいて、特定のエンドポイントのデバッグ ログをダウンロードできます。その特定のエンドポイント固有のログが、展開内のさまざまなノードから 1 つのファイルに収集されるため、迅速かつ効率的に問題をトラブルシューティングできます。このトラブルシューティング ツールは、一度に 1 つのエンドポイントに対してのみ実行できます。ログ ファイルが GUI に表示されます。1 つのノードまたは展開内のすべてのノードからエンドポイントのログをダウンロードできます。

特定のエンドポイントのデバッグ ログのダウンロード

ネットワーク内の特定のエンドポイントの問題をトラブルシューティングするには、管理者ポータルからデバッグ エンドポイント ツールを使用できます。または、このツールを [認証（Authentications）] ページから実行できます。[認証（Authentications）] ページの [エンドポイント ID（Endpoint ID）] を右クリックして、[エンドポイント デバッグ（Endpoint Debug）] をクリックします。このツールでは、単一ファイルの特定のエンドポイントに関連するすべてのサービスに関するすべてのデバッグ情報が提供されます。

始める前に

デバッグ ログを収集するエンドポイントの IP アドレスまたは MAC アドレスが必要です。

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [エンドポイント デバッグ（Endpoint Debug）]** を選択します。

ステップ 2 [MAC アドレス（MAC Address）] または [IP] オプション ボタンをクリックし、エンドポイントの MAC または IP アドレスを入力します。

ステップ 3 一定の時間が経過した後にログ収集を停止する場合は、[*n* 分後に自動的に無効化（Automatic disable after n Minutes）] チェックボックスをオンにします。このチェックボックスをオンにする場合は、1 ～ 60 分の時間を入力する必要があります。

次のメッセージが表示されます。「エンドポイント デバッグによって、展開のパフォーマンスが低下します。続行しますか?（Endpoint Debug degrades the deployment performance. Would you like to continue?）」

ステップ 4 ログを収集するには、[続行（Continue）] をクリックします。

ステップ 5 手動でログの収集を中止する場合は、[停止（Stop）] をクリックします。

関連トピック

エンドポイントのデバッグ ログ コレクタ （297 ページ）

収集フィルタ

収集フィルタを設定して、モニタリング サーバおよび外部サーバに送信される syslog メッセージを抑制できます。抑制は、異なる属性タイプに基づいてポリシー サービス ノード レベルで実行できます。特定の属性タイプおよび対応する値を使用して複数のフィルタを定義できます。

モニタリング ノードまたは外部サーバに syslog メッセージを送信する前に、Cisco ISE は送信する syslog メッセージのフィールドとそれらの値を比較します。一致が見つかった場合、対応するメッセージは送信されません。

収集フィルタの設定

さまざまな属性のタイプに基づいて複数の収集フィルタを設定できます。フィルタ数を 20 に制限することを推奨します。収集フィルタを追加、編集、または削除できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [収集フィルタ（Collection Filters）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 次のリストから**フィルタ タイプ**を選択します。

- ユーザ名（User Name）
- MAC アドレス（MAC Address）
- ポリシー セット名
- NAS IP アドレス
- Device IP Address（デバイス IP アドレス）

ステップ 4 選択したフィルタ タイプの対応する**値**を入力します。

ステップ 5 ドロップダウン リストから**結果**を選択します。結果は、[すべて（All）]、[成功（Passed）]、または [失敗（Failed）] になります。

ステップ 6 [送信（Submit）] をクリックします。

関連トピック

収集フィルタ （298 ページ）
イベント抑制バイパス フィルタ （298 ページ）

イベント抑制バイパス フィルタ

Cisco ISE では、フィルタを設定し、収集フィルタを使用して、一部の syslog メッセージがモニタリング ノードおよび他の外部サーバに送信されることを抑制できます。場合によっては、

これらの抑制されたログ メッセージにアクセスすることが必要になります。Cisco ISE は、設定可能な時間について、ユーザ名などの属性に基づいてイベント抑制をバイパスするオプションを提供します。デフォルトは 50 分ですが、5 分から 480 分（8 時間）の期間を設定できます。イベント抑制バイパスは、設定した後すぐに有効になります。設定した期間が経過すると、バイパス抑制フィルタは失効します。

抑制バイパス フィルタは、Cisco ISE ユーザ インターフェイスの [収集フィルタ（Collection Filters）] ページから設定できます。この機能を使用して、特定の ID（ユーザ）のすべてのログを表示し、その ID の問題をリアルタイムでトラブルシューティングできます。

フィルタは有効または無効にできます。バイパス イベント フィルタで設定した期間が経過すると、フィルタは再度有効にするまで自動的に無効になります。

Cisco ISE は設定変更監査レポートでこれらの設定変更を取得します。このレポートは、イベント抑制またはバイパス抑制を設定したユーザ、およびイベントが抑制された期間または抑制がバイパスされた期間に関する情報を提供します。

Cisco ISE レポート

モニタリング機能およびトラブルシューティング機能とともに Cisco Identity Services Engine（ISE）レポートを使用して、集中管理する場所からのトレンドの分析、システム パフォーマンスおよびネットワーク アクティビティのモニタリングを行います。

Cisco ISE はネットワーク全体からログおよび設定データを収集します。その後、表示と分析のために、データがレポートに集約されます。Cisco ISE には、使用可能な事前定義されたレポートが用意されており、必要に応じてカスタマイズできます。

Cisco ISE レポートは事前設定されており、認証、セッション トラフィック、デバイス管理、設定と管理、およびトラブルシューティングに関する情報の論理カテゴリにグループ化されます。

関連トピック

レポートの実行および表示 （301 ページ）
レポートのエクスポート （302 ページ）
使用可能なレポート （306 ページ）

レポート フィルタ

レポートには、シングルセクション レポートとマルチセクション レポートの 2 種類があります。シングルセクション レポートには 1 つのグリッドが含まれており（RADIUS 認証レポート）、マルチセクション レポートには複数のグリッドが含まれており（認証概要レポート）、データがグラフと表の形式で示されます。シングルセクション レポートの [フィルタ（Filter）] ドロップダウン メニューには、[クイック フィルタ（Quick Filter）] と [拡張フィルタ（Advanced Filter）] があります。マルチセクション レポートでは、拡張フィルタだけを指定できます。

マルチセクション レポートには、入力が必要な必須拡張フィルタが1つ以上含まれていることがあります。たとえば、健全性の概要レポート（[操作（Operations）]>[レポート（Reports）]>[診断（Diagnostics）]ページ）をクリックすると、2つの必須拡張フィルタ（[サーバ（Server）]と [時間範囲（Time Range）]）が表示されます。レポートを生成するには、この両方のフィルタで演算子コマンド、サーバ名、必要な値を指定し、[実行（Go）]をクリックする必要があります。プラス記号（+）をクリックして新しい拡張フィルタを追加できます。マルチセクション レポートはPDF形式でのみエクスポートできます。特定の時刻または時間間隔でCisco ISEマルチセクション レポートを実行または再実行するようにスケジュールすることはできません。

（注） レポートをクリックすると、デフォルトでは最新のデータが生成されます。ただし一部のマルチセクション レポートでは、時間範囲以外にもユーザが入力する必要のある項目があります。

シングルセクション レポートでは、デフォルトでクイック フィルタが1番目の行として表示されます。フィールドには、検索基準を選択できるドロップダウン リストまたはテキスト ボックスが含まれています。

拡張フィルタには、1つ以上の内部条件を含む外部条件が含まれています。外部条件では、検索で指定された内部条件すべてに一致する必要があるか、またはいずれかに一致する必要があるかを指定します。内部条件には、カテゴリ（[エンドポイントID（Endpoint ID）]、[IDグループ（Identity Group）]）、メソッド（Contains、Does Not Containなどの演算子コマンド）、および時間範囲を条件として指定するために使用される1つ以上の条件が含まれています。

[クイックフィルタ（Quick Filter）]を使用すると、[記録日時（Logged At）]ドロップダウン リストから日付または時刻を選択し、過去30日以内にログインしたデータ セットのレポートを生成できます。30日より前の日付または時刻のレポートを生成する場合は、[高度なフィルタ（Advanced Filters）]を使用して、ドロップダウン リストの[カスタム（Custom）]オプションの[開始日（From）]と[終了日（To）]のフィールドに必要な時間枠を設定します。

クイック フィルタ条件の作成

ここでは、クイック フィルタ条件の作成方法を説明します。クイック フィルタ条件はシングルセクション レポートでのみ作成できます。

ステップ1 **[操作（Operations）]>[レポート（Reports）]**を選択し、必要なレポートをクリックします。

ステップ2 [設定（Settings）]ドロップダウンリストから必須フィールドを選択します。

ステップ3 データをフィルタリングするため、必須フィールドでドロップダウンリストから選択するか、または特定の文字を入力できます。検索ではContains演算子コマンドが使用されます。たとえば、「K」で始まるテキストをフィルタリングするにはKと入力し、テキスト内の任意の位置に「geo」が含まれているテキストをフィルタリングするにはgeoと入力します。また、アスタリスク（*）を使用することもできます。たとえば、*abcで始まり*defで終わる正規表現などです。

クイック フィルタで使用される条件には、contains、starts with、ends with、starts with or ends with、および OR 演算子で結合する複数の値があります。

ステップ 4 Enter キーを押します。

拡張フィルタ条件の作成

ここでは、拡張フィルタ条件の作成方法を説明します。拡張フィルタは、シングルセクション レポートとマルチセクション レポートで作成できます。シングルセクション レポートの [フィルタ（Filter）] ドロップダウン メニューには、[クイック フィルタ（Quick Filter）] と [拡張フィルタ（Advanced Filter）] があります。マルチセクション レポートでは、拡張フィルタだけを指定できます。

ステップ 1 **[操作（Operations）] > [レポート（Reports）]** を選択し、必要なレポートをクリックします。

ステップ 2 [フィルタ（Filters）] セクションで [一致（Match）] ドロップダウン リストから次のいずれかのオプションを選択します。

a) 指定したすべての条件に一致する必要がある場合は、[すべて（All）] を選択します。

b) 指定したいずれか 1 つの条件に一致すればよい場合は、[いずれか（Any）] を選択します。

ステップ 3 [時間範囲（Time Range）] ドロップダウンリストから必要なカテゴリを選択します。

ステップ 4 [演算子コマンド（Operator Commands）] ドロップダウンリストから、必要なコマンドを選択します。たとえば、特定の文字で始まるテキストや（[次の文字で始まる（Begin With）] を使用）、テキスト内の任意の位置に特定の文字が含まれているテキスト（[次の文字を含む（Contains）] を使用）をフィルタリングできます。あるいは、[ログに記録された時刻（Logged Time）] と対応する [カスタム（Custom）] オプションを選択し、カレンダーからデータをフィルタリングする期間の開始日時と終了日時を指定します。

ステップ 5 [時間範囲（Time Range）] ドロップダウンリストから必要なオプションを選択します。

ステップ 6 [移動（Go）] をクリックします。

今後の参照のために、フィルタリングされたレポートを保存し、[フィルタ（Filter）] ドロップダウンリストから取得することができます。

レポートの実行および表示

ここでは、Reports View を使用してレポートを実行、表示、およびナビゲートする方法について説明します。デフォルトでは、レポートをクリックすると過去 7 日間のデータが生成されます。各レポートでは、ページごとに 500 行のデータが表示されます。レポートにデータを表示する時間の増分を指定できます。

ステップ 1 **[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）]** を選択します。

また、各ワークセンターの[レポート（Reports）]リンクに移動して、ワークセンター固有の一連のレポートを確認することもできます。

ステップ 2 使用可能な**レポート** カテゴリからレポートをクリックします。

ステップ 3 レポートを実行する 1 つ以上のフィルタを選択します。各レポートに、異なるフィルタを使用できます。フィルタの一部は必須で一部は任意選択です。

ステップ 4 フィルタに適切な値を入力します。

ステップ 5 [移動（Go）] をクリックします。

関連トピック

レポートのエクスポート （302 ページ）
使用可能なレポート （306 ページ）

レポートのナビゲーション

レポート出力から詳細情報を取得できます。たとえば、5 ヵ月の期間に 1 つのレポートを生成した場合、グラフと表には月単位の目盛りでレポートの集約データが表示されます。

表内の特定の値をクリックすると、この特定のフィールドに関連する別のレポートを表示できます。たとえば、認証概要レポートには、ユーザまたはユーザ グループの失敗したカウントが表示されます。失敗したカウントをクリックすると、その特定の失敗したカウントについての認証概要レポートが開きます。

レポートのエクスポート

次のファイル形式でレポート データをエクスポートできます。

- カンマ区切り値（.csv）ファイルとしての Excel スプレッドシート。データをエクスポートすると、レポートの場所を詳細に示した電子メールを受信します。
- ローカル ディスクに保存できる Microsoft Excel のカンマ区切り値（.csv）ファイル。
- ローカル ディスクに保存できる Adobe Acrobat Document（.pdf）ファイル。

（注） Microsoft Excel 形式の場合、エクスポートできるのは 5000 レコードです。PDF ファイル形式の場合、エクスポートできるのは 1000 レコードです。

次のレポートは PDF ファイル形式でののみエクスポートできます。

- 認証概要（Authentication Summary）
- 健全性の概要

- RBACL ドロップ概要

（注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。

- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス

（注） レポートをエクスポートした後で英語以外の文字を正しく表示するには、UTF-8 文字エンコーディングを有効にして Microsoft Excel にファイルをインポートする必要があります。UTF-8 文字エンコーディングを有効にしないで、エクスポートした .csv ファイルを Microsoft Excel で直接開いた場合、レポートの英語以外の文字は文字化けした状態で表示されます。

（注） レポート データは、プライマリ PAN からのみ .csv 形式にエクスポートできます。

ステップ 1 「レポートの実行と表示」の項の説明に従ってレポートを実行します。

ステップ 2 レポート サマリー ページの右上隅にある [エクスポート（Export）][エクスポート先（Export To）] をクリックします。

ステップ 3 エクスポートするデータ カラムを指定します。

ステップ 4 ドロップダウン リストからリポジトリを選択します。

ステップ 5 [エクスポート（Export）] をクリックします。

Cisco ISE レポートのスケジュールと保存

レポートをカスタマイズし、変更内容を新しいレポートとして保存するか、またはレポート サマリー ページの右上隅にある [マイ レポート（My Reports）] でデフォルトのレポート設定を復元できます。

Cisco ISE レポートをカスタマイズおよびスケジュールして、特定の時間または時間間隔で実行および再実行することもできます。生成されたレポートに関する電子メール通知を送受信することもできます。

時間単位の頻度でレポートをスケジュールする場合は、レポートを複数の日にわたって実行することはできますが、日をまたぐ時間枠を設定することはできません。

たとえば、時間単位のレポートを 2019 年 5 月 4 日から 5 月 8 日までスケジューリングする場合は、時間間隔を各日の午前 6 時から午後 11 時までに設定することはできますが、ある日の午後 6 時から翌日の午前 11 時までに設定することはできません。後者の場合、Cisco ISE は、時間範囲が無効であることを示すエラー メッセージを表示します。

（注） 外部の管理者（Active Directory の管理者など）が電子メール ID フィールドを指定せずにスケジュール設定されたレポートを作成すると、電子メール通知は送信されません。

次のレポートはスケジュールできません。

- 認証概要（Authentication Summary）
- 健全性の概要
- RBACL ドロップ概要
- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス

（注） Cisco ISE レポートの保存またはスケジューリング（カスタマイズ）は、PAN からのみ実行できます。

ステップ 1 「レポートの実行と表示」の項の説明に従ってレポートを実行します。

ステップ 2 レポート サマリー ページの右上隅の [マイ レポート（My Reports）] をクリックします。

ステップ 3 ダイアログボックスに必要な詳細を入力します。

ステップ 4 [新規として保存（Save as New）] をクリックします。

保存済みレポートに戻ると、すべてのフィルタ オプションがデフォルトでオンになります。使用しないフィルタはオフにします。

[マイレポート（My Reports）] カテゴリから、保存したレポートを削除することもできます。

Cisco ISE のアクティブな RADIUS セッション

Cisco ISE では、ライブ セッション用の動的な許可変更（CoA）機能が提供されます。この機能を使用すると、アクティブな RADIUS セッションを動的に制御できます。次のタスクを実行するために再認証または接続解除要求をネットワーク アクセス デバイス（NAD）に送信できます。

- 認証に関連する問題のトラブルシューティング：[セッション再認証（Session reauthentication）] オプションを使用して、再認証を試みることができます。ただし、アクセスを制限するためにこのオプションを使用しないでください。アクセスを制限するには、シャットダウン オプションを使用します。
- 問題のあるホストのブロック：[ポート シャットダウンによるセッション終了（Session termination with port shutdown）] オプションを使用して、ネットワークに大量のトラフィックを送信する、ウイルスなどに感染したホストをブロックできます。ただし、RADIUS プロトコルでは、シャットダウンされたポートを再度有効にするための方法は現在サポートされていません。
- エンドポイントでの IP アドレス再取得の強制：サプリカントまたはクライアントを持たないエンドポイントに対して [ポート バウンスでのセッション終了（Session termination with port bounce）] オプションを使用し、VLAN 変更後に DHCP 要求を生成できます。
- エンドポイントへの更新された許可ポリシーのプッシュ：[セッション再認証（Session reauthentication）] オプションを使用して、管理者の裁量に基づいた既存のセッションの許可ポリシーの変更などの、更新されたポリシー設定を適用できます。たとえば、ポスチャ確認が有効である場合にエンドポイントが最初にアクセスを許可されると、通常、エンドポイントは隔離されます。エンドポイントのアイデンティティおよびポスチャが確認された後、Session reauthentication コマンドをエンドポイントに送信して、エンドポイントがそのポスチャに基づいて実際の許可ポリシーを取得できるようにすることが可能です。

デバイスによって CoA コマンドが認識されるためには、適切にオプションを設定することが重要です。

CoA が適切に動作するには、動的な許可変更を必要とする各デバイスの共有秘密情報を設定する必要があります。Cisco ISE では、デバイスからのアクセス要求、およびデバイスへの CoA コマンドの発行において、共有秘密情報設定が使用されます。

（注） このリリースの Cisco ISE では、表示可能な認証されたエンドポイント セッションの最大数が 100,000 に制限されています。

関連トピック

RADIUS セッションの許可の変更 （305 ページ）

RADIUS セッションの許可の変更

ネットワークの一部のネットワーク アクセス デバイスでは、リロード後にアカウンティング停止パケットまたはアカウンティング オフ パケットが送信されないことがあります。このため、[セッション ディレクトリ（Session Directory）] の下のレポートでは、有効なセッションと期限切れのセッションの 2 つのセッションが表示される場合があります。

アクティブな RADIUS セッションの許可を動的に変更する場合や、アクティブな RADIUS セッションの接続を解除する場合には、最新のセッションを選択する必要があります。

ステップ 1 **[操作（Operations）]** > **[RADIUSライブログ（RADIUS Livelog）]** の順に選択します。

ステップ 2 [ライブ セッションの表示（Show Live Session）] にビューを切り替えてください。

ステップ 3 CoA を発行する RADIUS セッションの CoA リンクをクリックし、次のいずれかのオプションを選択します。

- [SAnet セッション クエリー（SAnet Session Query）]：SAnet でサポートされるデバイスからのセッションに関する情報をクエリーするために使用します。
- [セッション再認証（Session reauthentication）]：セッションを再認証します。CoA をサポートする ASA デバイスに確立されるセッションにこのオプションを選択すると、セッションポリシープッシュ CoA が呼び出されます。
- [最後の方式でのセッション再認証（Session reauthentication with last）]：そのセッションに対して、最後に成功した認証方式を使用します。
- [再実行によるセッション再認証（Session reauthentication with rerun）]：設定されている認証方式を最初から実行します。

  （注） [最後の方式でのセッション再認証（Session reauthentication with last）] オプションおよび [再実行によるセッション再認証（Session reauthentication with rerun）] オプションは、Cisco IOS ソフトウェアで現在サポートされていません。

- [セッション終了（Session termination）]：単にセッションを終了します。スイッチは、異なるセッションでクライアントを再認証します。
- [ポート バウンスでのセッション終了（Session termination with port bounce）]：セッションを終了し、ポートを再起動します。
- [ポート シャットダウンによるセッション終了（Session termination with port shut down）]：セッションを終了し、ポートをシャットダウンします。

ステップ 4 [実行（Run）] をクリックして、選択した再認証または終了オプションとともに CoA を発行します。

CoA に失敗した場合は、次の理由が考えられます。

- デバイスで CoA がサポートされていない。
- アイデンティティまたは許可ポリシーに変更があった。
- 共有秘密が一致しない。

使用可能なレポート

次の表に、事前設定済みレポートをカテゴリ別に分類して示します。また、レポートの機能およびロギング カテゴリについても説明します。

レポート名	説明	ロギング カテゴリ
Audit		
適応型ネットワーク制御の監査	適応型ネットワーク制御の監査レポートは、RADIUS アカウンティングに基づきます。つまり、エンドポイントごとにすべてのネットワーク セッションの履歴レポートを表示します。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択し、[成功した認証（Passed Authentications）] および [RADIUS アカウンティング（RADIUS Accounting）] を選択します。
管理者ログイン	管理者ログイン レポートには、GUI ベースの管理者ログイン イベントと成功した CLI ログイン イベントに関する情報が提供されます。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。
変更設定監査	変更設定監査レポートは、指定した期間内の設定変更の詳細を提供します。機能をトラブルシューティングする必要がある場合、このレポートは、最新の設定変更が問題の原因となったかどうかを決定するのに役立ちます。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。

レポート名	説明	ロギング カテゴリ
データ消去の監査	データ消去の監査レポートは、ロギング データが消去されている時間を記録します。 このレポートは、データ消去の 2 つのソースを反映します。 毎日午前 4 時に、Cisco ISE は、[管理（Administration）]>[メンテナンス（Maintenance）]>[データ消去（Data Purging）] ページで設定した基準に一致するロギング ファイルがあるかどうかを確認します。あった場合は、ファイルが削除され、このレポートに記録されます。さらに、Cisco ISE は、常にログ ファイルに使用される記憶域を最大 80% に維持します。1 時間ごとに、Cisco ISE はこの割合を確認し、80% のしきい値に再び到達するまで、最も古いデータが削除されます。この情報もこのレポートに記録されます。 高いディスク容量使用率がある場合、しきい値の 80% で「ISE モニタ ノードはもうすぐ割り当てられている最大量を超えます（ISE Monitor node(s) is about to exceed the maximum amount allocated）」という警告メッセージが表示されます。その後、しきい値の 90% で「ISE モニタ ノードは割り当てられている最大量を超えました（ISE Monitor node(s) has exceeded the maximum amount allocated）」という警告メッセージが表示されます。	—

レポート名	説明	ロギング カテゴリ
エンドポイントのアクティビティ消去	エンドポイントのアクティビティ消去レポートを使用すると、エンドポイントのアクティビティ消去の履歴を確認できます。このレポートは、プロファイラ ロギング カテゴリが有効である必要があります。デフォルトでは有効になっています。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択し、[プロファイラ（Profiler）] を選択します。
内部管理者の概要	内部管理者の概要レポートを使用すると、管理者ユーザのエンタイトルメントを確認できます。このレポートから、管理者ログイン レポートおよび変更設定監査レポートにもアクセスでき、それにより、管理者ごとにこれらの詳細を表示できます。	—
操作監査	操作監査レポートは、次のような操作の変更に関する詳細を提供します。バックアップの実行、Cisco ISE ノードの登録、またはアプリケーションの再起動。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。

レポート名	説明	ロギング カテゴリ
pxGrid 管理者の監査	pxGrid 管理者の監査レポートは、プライマリ PAN でのクライアントの登録、クライアントの登録解除、クライアントの承認、トピックの作成、トピックの削除、パブリッシャとサブスクライバの追加、およびパブリッシャとサブスクライバの削除など、pxGrid の管理処理の詳細を提供します。 すべてのレコードに、ノードで処理を実行した管理者の名前が示されます。 管理者およびメッセージの基準に基づいて、pxGrid 管理者の監査レポートをフィルタできます。	—
セキュアな通信の監査	セキュアな通信の監査レポートには、認証の失敗、ブレークインの可能性がある試み、SSH ログイン、失敗したパスワード、SSH ログアウト、無効なユーザ アカウントなどが含まれる、Cisco ISE 管理 CLI のセキュリティ関連イベントに関する監査の詳細が提供されます。	—
User Change Password Audit	User Change Password Audit レポートは、従業員のパスワード変更に関する検証を表示します。	管理および操作の監査（Administrative and Operational audit）
デバイス管理		
認証概要（Authentication Summary）	[TACACS 認証概要（TACACS Authentication Summary）] レポートには、最も一般的な認証および認証失敗の理由の詳細が示されています。	

レポート名	説明	ロギング カテゴリ
TACACS アカウンティング	TACACS アカウンティング レポートは、デバイス セッションのアカウンティングの詳細を提供します。ユーザおよびデバイスの生成された時刻およびログに記録された時刻に関する情報が表示されます。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[TACACSアカウンティング（TACACS Accounting）] を選択します。
失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）	[失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）] レポートには、選択したパラメータに基づいて、特定の期間における失敗の理由別の認証の合計数が表示されます。	—
ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）	[ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）] レポートには、選択されたパラメータに基づいて、特定の期間におけるネットワーク デバイス名ごとの合格および不合格の認証数が表示されます。	—
ユーザ別上位 N の認証（Top N Authentication by User）	[ユーザ別上位 N の認証（Top N Authentication by User）] レポートには、選択したパラメータに基づいて、特定の期間におけるユーザ名ごとの合格および不合格の認証数が表示されます。	—
診断		

レポート名	説明	ロギング カテゴリ
AAA の診断	AAA の診断レポートは、Cisco ISE とユーザ間のすべてのネットワーク セッションの詳細を提供します。ユーザがネットワークにアクセスできない場合、トレンドを識別し、問題が特定のユーザに隔離されているか、またはより広範囲の問題を示しているかを識別するために、このレポートを確認できます。	**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギング カテゴリ（Logging Categories）]** を選択し、次のロギング カテゴリを選択します。[ポリシー診断（Policy Diagnostics）]、[ID ストア診断（Identity Stores Diagnostics）]、[認証フロー診断（Authentication Flow Diagnostics）]、および [RADIUS 診断（RADIUS Diagnostics）]。
AD コネクタ操作	AD コネクタ操作レポートは、Cisco ISE サーバのパスワードのリフレッシュ、Kerberos チケットの管理、DNS クエリ、DC 検出、LDAP、および RPC 接続管理など、AD コネクタが実行する操作のログを提供します。 AD の障害がいくつか発生している場合、このレポートで詳細を確認して考えられる原因を特定できます。	**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギング カテゴリ（Logging Categories）]** を選択し、[AD コネクタ（AD Connector）] を選択します。
エンドポイント プロファイルの変更	エンドポイント（MAC アドレス）別上位認証レポートは、ネットワークにアクセスするために各エンドポイントの MAC アドレスが Cisco ISE によって許可された回数を表示します。	成功した認証、失敗した試行（Passed Authentications, Failed Attempts）

レポート名	説明	ロギング カテゴリ
健全性の概要	健全性の概要レポートは、ダッシュボードのような詳細を提供します。ただし、ダッシュボードは過去 24 時間のデータしか表示しませんが、このレポートを使用するとより多くの履歴データを確認できます。 データの一貫したパターンを調べるためにこのデータを評価できます。たとえば、大多数の従業員が就業時間を開始するときに、非常に高い CPU 使用率が予想されます。これらのトレンドの不整合がわかれば、潜在的な問題を識別できます。 [CPU 使用率（CPU Usage）] テーブルには、各種 Cisco ISE 機能の CPU 使用率（%）が表示されます。**show cpu usage** CLI コマンドの出力がこのテーブルに表示されるため、これらの値を、展開内で発生している問題と関連付け、原因を特定することができます。	—

レポート名	説明	ロギング カテゴリ
ISE カウンタ	ISE カウンタ レポートには、さまざまな属性のしきい値が示されます。各種属性の値の収集間隔は異なり、またデータは表形式で表示されます。5 分間隔で収集される属性と 5 分よりも長い間隔で収集される属性があります。 このデータを評価してトレンドを確認し、しきい値よりも高い値を検出した場合には、展開内で発生している問題にこの情報を関連付け、考えられる原因を特定できます。 Cisco ISE はデフォルトでこれらの属性の値を収集します。このデータ収集を無効にするには、Cisco ISE CLI で **application configure ise** コマンドを使用します。カウンタ属性の収集を有効または無効にするには、オプション 14 を選択します。	—
主要パフォーマンス測定指標	主要パフォーマンス測定指標レポートには、展開に接続しているエンドポイントの数と、1 時間あたりに各 PAN が処理する RADIUS 要求の数に関する統計情報が表示されます。このレポートには、サーバの平均負荷、要求あたりの平均遅延、および平均トランザクション数/秒が示されます。	—

レポート名	説明	ロギング カテゴリ
設定が誤っている NAS	設定が誤っているNASレポートは、通常、アカウンティング情報を頻繁に送信するときに、アカウンティング頻度が不正確なNADに関する一般情報を提供します。修正処置を行い、設定が誤っているNADを修正すると、レポートはレポートに修正済み確認を表示します。 （注） レポートを実行するには、RADIUS 抑制を有効にする必要があります。	—
設定が誤っているサプリカント	設定が誤っているサプリカントのレポートは、特定のサプリカントが実行した失敗試行のため、設定が誤っているサプリカントの一覧および統計情報を提供します。修正処置を行い、設定が誤っているサプリカントを修正すると、レポートはレポートに修正済み確認を表示します。 （注） レポートを実行するには、RADIUS 抑制を有効にする必要があります。	—

レポート名	説明	ロギング カテゴリ
ネットワーク デバイスのセッション ステータス	ネットワーク デバイスのセッション ステータス概要レポートを使用すると、直接スイッチにログインせずにスイッチ設定を表示することができます。 Cisco ISE は SNMP クエリを使用してこれらの詳細にアクセスするので、ネットワーク デバイスは SNMP v1/v2c を使用して設定されている必要があります。 ユーザにネットワークの問題が発生している場合に、このレポートは、問題が Cisco ISE ではなくスイッチの設定に関連しているかどうかを識別するのに役立ちます。	—
OCSP Monitoring	OCSP モニタリング レポートは、Online Certificate Status Protocol（OCSP）サービスのステータスを指定します。Cisco ISE が正常に証明書サーバに連絡し、証明書ステータス監査を提供できるかどうかを識別します。Cisco ISE によって実行されたすべての OCSP 証明書検証操作の概要が提供されます。適切な/失効したプライマリ/セカンダリ証明書に関連する情報を OCSP サーバから取得します。Cisco ISE は、応答をキャッシュし、後続の OCSP モニタリング レポートの生成に使用します。キャッシュがクリアされる場合は、OCSP サーバから情報を取得します。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギング カテゴリ（Logging Categories）]** を選択し、[システム診断（System Diagnostics）] を選択します。

レポート名	説明	ロギング カテゴリ
RADIUS エラー	RADIUS エラー レポートを使用すると、ドロップされた RADIUS 要求（未知のネットワーク アクセス デバイスからの廃棄された認証/アカウンティング要求）、EAP 接続タイムアウトおよび未知の NAD をチェックできます。 （注） ISE は、ユーザ認証が進行中のときにエンドポイントのアカウンティング停止要求をサイレントにドロップする場合があります。ただし、ISE はユーザ認証が完了すると、すべてのアカウンティング要求の認識を開始します。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択し、[失敗した試行（Failed Attempts）] を選択します。
システム診断	システム診断レポートは Cisco ISE ノードのステータスの詳細を提供します。Cisco ISE ノードが登録できない場合、このレポートを確認して問題をトラブルシューティングすることができます。 このレポートでは、最初に複数の診断ロギング カテゴリを有効にする必要があります。これらのログを収集すると、Cisco ISE パフォーマンスに悪影響を及ぼすことがあります。したがって、これらのカテゴリはデフォルトで有効ではなく、データを収集するのに十分な時間だけ有効にする必要があります。そうでない場合は、30 分後に自動的に無効になります。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択し、次のロギング カテゴリを選択します。[内部操作診断（Internal Operations Diagnostics）]、[分散管理（Distributed Management）]、および [管理者の認証と許可（Administrator Authentication and Authorization）]。
エンドポイントとユーザ		

レポート名	説明	ロギング カテゴリ
認証概要	認証概要レポートは、RADIUS認証に基づいています。それにより、最も一般的な認証および認証失敗の原因を特定することができます。たとえば、あるCisco ISEサーバが他のサーバよりもはるかに多くの認証を処理している場合、負荷を適切に分散するためにユーザを別のCisco ISEサーバに再割り当てする場合があります。 （注） 認証概要レポートまたはダッシュボードが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。	—

レポート名	説明	ロギング カテゴリ
クライアント プロビジョニング	クライアント プロビジョニング レポートは、特定のエンドポイントに適用されるクライアント プロビジョニング エージェントについて示します。このレポートを使用すると、各エンドポイントに適用されるポリシーを確認してエンドポイントが正しくプロビジョニングされたことを確認することができます。 （注） エンドポイントが ISE に接続されない（セッションが確立されない）場合、またはネットワーク アドレス変換（NAT）アドレスがセッションで使用される場合、エンドポイントの MAC アドレスは [エンドポイントID（Endpoint ID）] 列に表示されません。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択し、[ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）] および [ポスチャおよびクライアント プロビジョニングの診断（Audit and Posture and Client Provisioning Diagnostics）] を選択します。
現在のアクティブなセッション	現在アクティブなセッション レポートを使用すると、指定の期間内のその時点でネットワーク上に存在していた者に関する詳細を含むレポートをエクスポートできます。 ユーザがネットワークにアクセスできない場合、セッションが認証または終了されているかどうか、またはセッションに別の問題があるかどうかを確認できます。	—

レポート名	説明	ロギング カテゴリ
外部モバイル デバイス管理	外部モバイル デバイス管理レポートは、Cisco ISE と外部モバイルデバイス管理（MDM）サーバ間の統合に関する詳細を提供します。 このレポートを使用すると、MDM サーバに直接ログインせずに、MDM サーバによってプロビジョニングされたエンドポイントを確認することができます。また、登録および MDM コンプライアンス ステータスなどの情報が表示されます。	**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギング カテゴリ（Logging Categories）]** を選択し、[MDM] を選択します。
パッシブ ID	パッシブ ID レポートでは、ドメイン コントローラへの WMI 接続の状態をモニタし、関連する統計情報（受信した通知の数、1 秒あたりのユーザ ログイン/ログアウト回数など）を収集することができます。 （注） この方法で認証されたセッションには、レポートの認証の詳細がありません。	**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギング カテゴリ（Logging Categories）]** を選択し、[ID マッピング（Identity Mapping）] を選択します。
手動証明書プロビジョニング	手動証明書プロビジョニング レポートには、証明書プロビジョニング ポータル経由で手動でプロビジョニングされたすべての証明書がリストされます。	—
条件によるポスチャ アセスメント	条件によるポスチャ アセスメント レポートでは、ISE に設定されたポスチャ ポリシー条件に基づいてレコードを表示し、最新のセキュリティ設定またはアプリケーションがクライアント マシンで利用可能かどうかを確認できます。	—

レポート名	説明	ロギング カテゴリ
エンドポイントによるポスチャ アセスメント	[エンドポイントによるポスチャ アセスメント（Posture Assessment by Endpoint）] レポートには、エンドポイントの時間、ステータス、PRA アクションなどの詳細な情報が提供されます。[詳細（Details）]をクリックして、エンドポイントの詳細情報を表示することができます。 （注） [エンドポイントによるポスチャアセスメント（Posture Assessment by Endpoint）] レポートでは、エンドポイントのアプリケーションおよびハードウェア属性のポスチャポリシーの詳細は提供されません。[コンテキストの可視性（Context Visibility）] ページでのみこの情報を確認できます。	—
プロファイリングされたエンドポイントの概要	プロファイリングされたエンドポイントの概要レポートは、ネットワークにアクセスしているエンドポイントに関するプロファイリングの詳細を提供します。 （注） Cisco IP Phone など、セッション時間を登録しないエンドポイントの場合、[エンドポイント（Endpoint）] セッション時間フィールドに、[該当なし（Not Applicable）] と表示されます。	**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギング カテゴリ（Logging Categories）]** を選択し、[プロファイラ（Profiler）] を選択します。

レポート名	説明	ロギング カテゴリ
RADIUS アカウンティング（RADIUS Accounting）	RADIUS アカウンティング レポートは、ユーザがネットワーク上に存在した時間を識別します。ユーザがネットワークにアクセスできない場合、Cisco ISE がネットワーク接続問題の原因であるかどうか、このレポートを使用して識別できます。 （注） 暫定アップデートに、指定されたセッションの IPv4 または IPv6 アドレスの変更に関する情報が含まれている場合、Radius アカウンティング暫定アップデートは [RADIUS アカウンティング（RADIUS Accounting）] レポートに含まれています。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギング カテゴリ（Logging Categories）]** を選択し、[RADIUS アカウンティング（RADIUS Accounting）] を選択します。
RADIUS 認証	RADIUS 認証レポートを使用すると、認証失敗および成功の履歴を確認できます。ユーザがネットワークにアクセスできない場合、このレポートの詳細を確認して考えられる原因を識別できます。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギング カテゴリ（Logging Categories）]** を選択し、次のロギング カテゴリを選択します。[成功した認証（Passed Authentications）] および [失敗した試行（Failed Attempts）]。
登録済みエンドポイント	登録済みエンドポイント レポートは、従業員によって登録されているすべてのパーソナル デバイスを表示します。	—

レポート名	説明	ロギング カテゴリ
拒否エンドポイント	拒否エンドポイント レポートには、従業員が登録したパーソナル デバイスのうち、拒否されたデバイスまたはリリースされたデバイスがすべて表示されます。このレポートのデータは、Plus ライセンスをインストールしている場合にのみ使用可能です。	—
サプリカント プロビジョニング	サプリカント プロビジョニング レポートは、従業員のパーソナル デバイスにプロビジョニングされたサプリカントに関する詳細を提供します。	ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）
エンドポイントによる上位承認	エンドポイント（MACアドレス）別上位認証レポートは、ネットワークにアクセスするために各エンドポイントのMAC アドレスが Cisco ISE によって許可された回数を表示します。	成功した認証、失敗した試行（Passed Authentications, Failed Attempts）
ユーザ別上位認証	ユーザ別上位認証レポートは、ネットワークにアクセスするために各ユーザが Cisco ISEによって許可された回数を表示します。	成功した認証、失敗した試行（Passed Authentications, Failed Attempts）
アクセス サービス別上位 N の認証（Top N Authentication by Access Service）	[アクセス サービス別上位 N の認証（Top N Authentication by Access Service）] レポートには、選択されたパラメータに基づいて、特定の期間におけるアクセス サービス タイプごとの合格および不合格の認証数が表示されます。	—

レポート名	説明	ロギング カテゴリ
失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）	[失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）] レポートには、選択したパラメータに基づいて、特定の期間における失敗の理由別の認証の合計数が表示されます。	—
ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）	[ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）] レポートには、選択されたパラメータに基づいて、特定の期間におけるネットワーク デバイス名ごとの合格および不合格の認証数が表示されます。	—
ユーザ別上位 N の認証（Top N Authentication by User）	[ユーザ別上位 N の認証（Top N Authentication by User）] レポートには、選択したパラメータに基づいて、特定の期間におけるユーザ名ごとの合格および不合格の認証数が表示されます。	—
ゲスト		
AUP 受け入れステータス	AUP 受け入れステータス レポートには、すべてのゲスト ポータルからの AUP 承認の詳細が示されます。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギング カテゴリ（Logging Categories）]** を選択し、[ゲスト（Guest）] を選択します。
ゲスト アカウンティング	ゲスト アカウンティング レポートは、RADIUS アカウンティング レポートのサブセットです。アクティブなゲストまたはゲスト ID グループに割り当てられたすべてのユーザがこのレポートに表示されます。	—

レポート名	説明	ロギング カテゴリ
マスター ゲスト レポート		**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギング カテゴリ（Logging Categories）]** を選択して、[成功した認証（Passed Authentications）] を選択します。

レポート名	説明	ロギング カテゴリ
	マスター ゲスト レポートは、さまざまなゲスト アクセス レポートからデータを結合し、異なるレポート ソースからデータをエクスポートできるようにします。マスター ゲスト レポートは、ゲスト ユーザがアクセスしている Web サイトに関する詳細も提供します。このレポートは、セキュリティ監査の目的で使用し、ゲスト ユーザがネットワークにアクセスした時間、およびそこで行った操作を示すことができます。 また、ゲスト トラフィックに使用するネットワーク アクセス デバイス（NAD）の HTTP インスペクションを有効にする必要もあります。この情報は、NAD によって Cisco ISE に返送されます。 クライアントが最大同時セッションの制限数に到達した時期を確認するには、管理者ポータルから、[管理（Administration）]>[システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）] の順に選択し、次を実行します。 **1.** 「認証フロー診断」のロギング カテゴリのログ レベルを [警告（WARN）] から [情報（INFO）] に上げます。 **2.** AAA 診断の [ロギングカテゴリ（Logging Category）] の下で [LogCollectorターゲット	

レポート名	説明	ロギング カテゴリ
	（LogCollector Target）] を [使用可能（Available）] から [選択済み（Selected）] に変更します。	
デバイスのログインおよび監査	デバイスのログインおよび監査レポートは、デバイス ポータルのデバイスでユーザが実行するログイン アクティビティと操作についての詳細を提供します。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択し、[デバイス（My Devices）] を選択します。
スポンサーのログインおよび監査	スポンサーのログインおよび監査レポートは、スポンサー ポータルでのゲスト ユーザのログイン、追加、削除、有効化、一時停止、および更新操作の詳細、ならびにスポンサーのログイン アクティビティの詳細を提供します。 ゲスト ユーザを一括で追加すると、[ゲスト ユーザ（Guest Users）] カラムの下に表示されます。このカラムは、デフォルトでは非表示です。エクスポート時に、これらの一括処理されたユーザもエクスポート ファイルに存在します。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択し、[ゲスト（Guest）] を選択します。
SXP		
SXP バインディング	SXP バインディング レポートは、SXP 接続を介して交換される IP-SGT バインディングに関する情報を提供します。	—
SXP 接続	このレポートを使用して、SXP 接続のステータスをモニタしたり、ピア IP、SXP ノード IP、VPN 名、SXP モードなど、その接続に関連する情報を収集できます。	—

レポート名	説明	ロギング カテゴリ
TrustSec		
RBACL ドロップ概要	RBACL ドロップ概要レポートは、拡張 Cisco ISE ライセンスのみで使用できる TrustSec 機能に固有です。 また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。 ユーザが特定のポリシーまたはアクセスに違反した場合、パケットがドロップされ、このレポートに示されます。 （注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズスイッチでのみ使用できます。	—

レポート名	説明	ロギング カテゴリ
ユーザ別上位 N 個の RBACL ドロップ	ユーザ別上位 N 個の RBACL ドロップ レポートは、拡張 Cisco ISE ライセンスのみで使用できる TrustSec 機能に固有です。 また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。 このレポートは、特定のユーザ別にポリシー違反（パケット ドロップに基づく）を表示します。 （注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズスイッチでのみ使用できます。	—
TrustSec ACI	このレポートには、IEPG、EEPG、エンドポイント、APIC のサブネット設定と同期された SGT および SXP のマッピングが一覧表示されます。これらの詳細は、TrustSec APIC 統合機能が有効になっている場合にのみ表示されます。	—

レポート名	説明	ロギング カテゴリ
TrustSec 展開の検証		—

レポート名	説明	ロギング カテゴリ
	このレポートを使用すると、最新の TrustSec ポリシーがすべてのネットワーク デバイスで展開されているかどうか、Cisco ISE とネットワーク デバイスで設定されたポリシーに不一致があるかどうかを確認できます。 検証プロセスの結果を表示するには、[詳細（Details）] アイコンをクリックします。次の詳細情報を表示できます。 • 検証プロセスの開始時期と終了時期 • 最新の TrustSec ポリシーがネットワーク デバイスで正常に展開されているかどうか。また、最新の TrustSec ポリシーを展開するネットワーク デバイスの名前および IP アドレスを表示することもできます。 • Cisco ISE とネットワーク デバイスで設定されたポリシーに不一致があるかどうか。デバイス名、IP アドレス、および各ポリシーの違いの対応するエラー メッセージが表示されます。 [アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] と [ホーム（Home）] > [サマリー（Summary）]）で、TrustSec 展開の検証アラームを表示できます。	

レポート名	説明	ロギング カテゴリ
	（注） • レポート作成にかかる時間は、展開内のネットワーク デバイスと TrustSec グループの数に応じて異なります。 • TrustSec 展開の検証レポートのエラー メッセージの長さは、現在 480 文字に制限されています。480 文字を超えるエラー メッセージは切り捨てられます。最初から 480 文字のみがレポートに表示されます。	
TrustSec ポリシーのダウンロード	このレポートには、ポリシー（SGT/SGACL）のダウンロードのためにネットワーク デバイスによって送信された要求と、ISE によって送信された詳細が一覧表示されます。ワークフロー モードを有効にしている場合、要求を実稼働マトリックスまたはステージング マトリックスに対してフィルタ処理することができます。	このレポートを表示するには、次の手順を実行する必要があります。 1. **[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択します。 2. **[AAA 診断（AAA Diagnostics）]** > **[RADIUS 診断（RADIUS Diagnostics）]** を選択します。 3. RADIUS 診断の [ログ重大度レベル（Log Severity Level）] を DEBUG に設定します。

レポート名	説明	ロギング カテゴリ
脅威中心型 NAC サービス		
アダプタのステータス	アダプタのステータス レポートには、脅威および脆弱性のアダプタのステータスが表示されます。	—
COA イベント	脆弱性イベントがエンドポイントに受信されると、Cisco ISE はそのエンドポイントの CoA をトリガーします。CoA イベント レポートには、これらの CoA イベントのステータスが表示されます。また、これらのエンドポイントの新旧の認証ルールとプロファイルの詳細が表示されます。	—
脅威イベント	脅威イベント レポートには、設定したさまざまなアダプタから Cisco ISE が受信した脅威イベントがすべて表示されます。	—
脆弱性アセスメント	脆弱性アセスメント レポートには、エンドポイントで行われているアセスメントに関する情報が提供されます。このレポートを表示して、設定されたポリシーに基づいてアセスメントが行われているかどうかを確認することができます。	—

RADIUS ライブ ログ

次の表では、最近の RADIUS 認証を表示する [RADIUS ライブ ログ（RADIUS Live Logs）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [RADIUS] > [ライブ ログ（Live Logs）]** です。RADIUS ライブ ログはプライマリ PAN だけで表示されます。

表 *32 : RADIUS* ライブ ログ

オプション	使用上のガイドライン
時刻（Time）	モニタリングおよび収集エージェントがログを受信した時刻を表示します。このカラムは必須です。選択解除することはできません。
ステータス（Status）	認証が成功したか失敗したかを示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細（Details）	[詳細（Details）] 列の下にあるアイコンをクリックすると、新しいブラウザウィンドウに [認証詳細レポート（Authentication Detail Report）] が表示されます。このレポートには、認証と関連属性のほか、認証フローに関する情報が記載されています。[認証の詳細（Authentications Details）] ボックスの [応答時間（Response Time）] には、Cisco ISE で認証フローを処理するのにかかった合計時間が示されます。たとえば、認証が 3 つのラウンドトリップメッセージで構成されている場合（最初のメッセージには300ミリ秒、次のメッセージには150ミリ秒、最後のメッセージには100ミリ秒かかる）、応答時間は、300＋150＋100 = 550 750 ミリ秒になります。 （注） 48時間を超えるアクティブになっているエンドポイントの詳細を表示することはできません。48時間を超えるアクティブになっているエンドポイントの詳細アイコンをクリックすると、次のメッセージがページに表示される場合があります：`No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.`

オプション	使用上のガイドライン
繰り返し回数（Repeat Count）	ID、ネットワークデバイス、および許可のコンテキストで変更がなく、直近の24時間で認証要求が繰り返された回数を表示します。
ID（Identity）	ログイン済みの認証に関連付けられているユーザ名を示します。 ユーザ名が ID ストアに存在しない場合は、「無効（INVALID）」と表示されます。その他の原因で認証に失敗した場合は、「ユーザ名（USERNAME）」と表示されます。 デバッグをサポートするために、無効なユーザ名の開示をISEに強制することもできます。[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS] > [抑制とレポート（Suppression & Reports）] > [認証の詳細（Authentication Details）] で [無効なユーザ名を開示する（Disclose invalid usernames）] チェックボックスをオンにします。このオプションは、30分後に自動的に無効になります。
エンドポイント ID（Endpoint ID）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。
エンドポイント プロファイル（Endpoint Profile）	プロファイリングされるエンドポイントのタイプを示します（たとえば、iPhone、Android、MacBook、Xbox になるようにプロファイリングされます）。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（Authorization Policy）	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル（Authorization Profiles）	認証に使用された許可プロファイルを表示します。
IP アドレス（IP Address）	エンドポイントデバイスの IP アドレスを表示します。
ネットワークデバイス（Network Device）	ネットワーク アクセス デバイスの IP アドレスを表示します。

オプション	使用上のガイドライン
デバイスポート（Device Port）	エンドポイントが接続されているポート番号を表示します。
ID グループ（Identity Group）	ログの生成対象となるユーザまたはエンドポイントに割り当てられるIDグループを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
サーバ（Server）	ログの生成元になったポリシーサービスが示されます。
MDMサーバ名（MDM Server Name）	MDM サーバの名前を表示します。
イベント（Event）	イベントステータスを表示します。
失敗の理由（Failure Reason）	認証が失敗した場合、その失敗の詳細な理由を表示します。
認証方式（Auth Method）	Microsoft チャレンジハンドシェイク認証プロトコルバージョン 2（MS-CHAPv2）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（Authentication Protocol）	Protected Extensible Authentication Protocol（PEAP）や拡張認証プロトコル（EAP）など、使用される認証プロトコルを表示します。
セキュリティ グループ（Security Group）	認証ログによって識別されるグループを表示します。
セッション ID（Session ID）	セッション ID を表示します。

（注） [RADIUS ライブ ログ（RADIUS Live Logs）] と [TACACS+ ライブ ログ（TACACS+ Live Logs）] 詳細ペインでは、各ポリシー許可ルールの 1 番目の属性として [照会済み PIP（Queried PIP）] が表示されます。許可ルール内のすべての属性が、以前のルールについてすでに照会されているディクショナリに関連している場合、これ以外に [照会済み PIP（Queried PIP）] エントリは表示されません。

[RADIUS ライブ ログ（RADIUS Live Logs）] ページで、次を実行できます。

- データを csv または pdf ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。

- 簡易またはカスタム フィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） すべてのユーザのカスタマイズは、ユーザ設定として保存されます。

関連トピック

ライブ認証のモニタ （1570 ページ）
ライブ認証 （1569 ページ）

RADIUS ライブ セッション

次の表では、ライブ認証が表示される [RADIUS ライブ セッション（RADIUS live sessions）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）]** > **[RADIUS]** > **[ライブセッション（Live Sessions）]** です。RADIUS ライブ セッションはプライマリ PAN だけで表示されます。

表 *33 : RADIUS* ライブ セッション

フィールド	説明
開始（Initiated）	セッション開始時のタイムスタンプを表示します。
更新しました	何らかの変更のためにセッションが最後に更新された時点のタイムスタンプを表示します。
アカウント セッション時間（Account Session Time）	ユーザ セッションの期間（秒単位）を表示します。
セッション ステータス（Session Status）	エンドポイント デバイスの現在のステータスを表示します。
アクション（CoA Action）	アクティブな RADIUS セッションを再認証するか、またはアクティブな RADIUS セッションを切断するには、[アクション（Actions）] アイコンをクリックします。
繰り返し回数（Repeat Count）	ユーザまたはエンドポイントの再認証回数を示します。

フィールド	説明
エンドポイント ID（Endpoint ID）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。
ID（Identity）	エンドポイント デバイスのユーザ名を表示します。
[IPアドレス（IP Address）]	エンドポイントデバイスのIPアドレスを表示します。
監査セッション ID（Audit Session ID）	固有のセッション ID を表示します。
アカウント セッション ID（Account Session ID）	ネットワーク デバイスから提供された固有IDを表示します。
エンドポイント プロファイル（Endpoint Profile）	デバイスのエンドポイント プロファイルを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
セキュリティ グループ（Security Group）	認証ログによって識別されるグループを表示します。
サーバ	ログを生成したポリシー サービス ノードを示します。
認証方式（Auth Method）	パスワード認証プロトコル（PAP）、チャレンジ ハンドシェイク認証プロトコル（CHAP）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（Authentication Protocol）	Protected Extensible Authentication Protocol（PEAP）や拡張認証プロトコル（EAP）など、使用される認証プロトコルを表示します。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル	認証に使用された許可プロファイルを表示します。
NAS IP アドレス	ネットワーク デバイスのIPアドレスを表示します。

フィールド	説明
デバイス ポート（Device Port）	ネットワーク デバイスに接続されたポートを表示します。
PRA アクション（PRA Action）	ネットワークでのコンプライアンスのためにクライアントが正常にポスチャされた後、そのクライアントで実行される定期的な再評価アクションを表示します。
ANCステータス（ANC Status）	[隔離（Quarantine）]、[隔離解除（Unquarantine）]、または [シャットダウン（Shutdown）] としてデバイスの適応型ネットワーク制御のステータスを表示します。
WLC ローミング（WLC Roam）	エンドポイントがローミング中にWLC間でハンドオフされたことを追跡するために使用されるブール値（Y/N）を表示します。cisco-av-pair=nas-update の値は Y または N です。 （注） セッションの状態がローミングであるかどうかを判断する場合、Cisco ISE は WLC の nas-update=true 属性に依存しています。元の WLC が nas-update=true のアカウンティング停止属性を送信する場合、再認証を回避するために ISE のセッションは削除されません。何らかの理由でローミングが失敗する場合、ISE は何も操作しない期間が 5 日経過するとセッションを消去します。
パケット入力	受信したパケットの数を表示します。
パケット出力	送信したパケットの数を表示します。
受信バイト数（Bytes In）	受信したバイト数を表示します。
送信バイト数（Bytes Out）	送信したバイト数を表示します。
セッション送信元（Session Source）	RADIUS セッションまたは PassiveID セッションのいずれであるかを示します。
ユーザドメイン名（User Domain Name）	ユーザの登録済み DNS 名を示します。
ホストドメイン名（Host Domain Name）	ホストの登録済み DNS 名を示します。
ユーザNetBIOS名（User NetBIOS Name）	ユーザの NetBIOS 名を示します。

フィールド	説明
ホストNetBIOS名（Host NetBIOS Name）	ホストの NetBIOS 名を示します。
ライセンスのタイプ（License Type）	使用されているライセンスのタイプ（Base、Plus、Apex、または Plus and Apex）を表示します。
ライセンスの詳細（License Details）	ライセンスの詳細を表示します。
プロバイダー	エンドポイント イベントはさまざまな syslog ソースから学習されます。これらの syslog ソースはプロバイダーと呼ばれます。 • Windows Management Instrumentation（WMI）：WMI は、オペレーティング システム、デバイス、アプリケーション、およびサービスに関する管理情報にアクセスするための共通インターフェイスとオブジェクト モデルを提供する Windows サービスです。 • エージェント：クライアントまたは別のプログラムの代わりにクライアントで実行されるプログラム。 • syslog：クライアントがイベント メッセージを送信するロギング サーバ。 • REST：クライアントはターミナル サーバで認証されます。この syslog ソースの場合、[TS エージェント ID（TS Agent ID）]、[開始送信元ポート（Source Port Start）]、[終了送信元ポート（Source Port End）]、[最初の送信元ポート（Source First Port）] の値が表示されます。 • SPAN：ネットワーク情報は SPAN プローブを使用して検出されます。 • DHCP：DHCP イベント。 • エンドポイント（Endpoint） 異なるプロバイダーからの 2 つのイベントがエンドポイントセッションから学習されると、ライブ セッション ページにこれらのプロバイダーがカンマ区切り値として表示されます。
MAC アドレス	クライアントの MAC アドレスを表示します。

フィールド	説明
[エンドポイントチェック時刻（Endpoint Check Time）]	エンドポイント プローブによってエンドポイントが最後にチェックされた時刻を表示します。
[エンドポイントチェック結果（Endpoint Check Result）]	エンドポイント プローブの結果が表示されます。設定可能な値は次のとおりです。 • 到達不要 • [ユーザ ログアウト（User Logout）] • [アクティブ ユーザ（Active User）]
[送信元ポートの開始（Source Port Start）]	（RESTプロバイダーの場合にのみ値が表示されます。）ポート範囲の最初のポートの番号を示します。
[送信元ポートの終了（Source Port End）]	（RESTプロバイダーの場合にのみ値が表示されます。）ポート範囲の最後のポート番号を示します。
[最初の送信元ポート（Source First Port）]	（RESTプロバイダーの場合にのみ値が表示されます。）ターミナルサーバ（TS）エージェントにより割り当てられた最初のポートを示します。 ターミナルサーバ（TS）は、複数のエンドポイントがモデムまたはネットワーク インターフェイスなしで接続でき、複数エンドポイントがLANネットワークに接続できるようにするサーバまたはネットワーク デバイスです。複数のエンドポイントに同一 IP アドレスが割り当てられている場合は、特定ユーザの IP アドレスを識別することが困難になります。このため、特定ユーザを識別する目的でTSエージェントがサーバにインストールされ、各ユーザにポート範囲が割り当てられます。これにより、IP アドレス - ポート - ユーザのマッピングが作成されます。
[TS エージェント ID（TS Agent ID）]	（RESTプロバイダーの場合にのみ値が表示されます。）エンドポイントにインストールされているターミナルサーバ（TS）エージェントの一意の ID を表示します。

フィールド	説明
[AD ユーザ解決 ID（AD User Resolved Identities）]	（AD ユーザの場合にのみ値が表示されます。）一致したアカウントの候補が表示されます。
[AD ユーザ解決 DN（AD User Resolved DNs）]	（AD ユーザの場合にのみ値が表示されます。）AD ユーザの識別名（例：CN=chris,CN=Users,DC=R1,DC=com）を表示します。

関連トピック

RADIUS セッションの許可の変更 （305 ページ）
Cisco ISE のアクティブな RADIUS セッション （304 ページ）

TACACS ライブ ログ

次の表では、TACACS+ AAA の詳細を表示する [TACACS ライブ ログ（TACACS Live Logs）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [TACACS ライブ ログ（TACACS Live Logs）]** です。TACACS ライブ ログはプライマリ PAN だけで表示されます。

表 34 : TACACS ライブ ログ

フィールド	使用上のガイドライン
生成日時（Generated Time）	特定のイベントがトリガーされた時点に基づいて、syslog の生成日時を示します。
ログに記録された時刻（Logged Time）	syslog がモニタリング ノードによって処理され、保存された時刻を示します。このカラムは必須です。選択解除することはできません。
ステータス	認証が成功したか失敗したかを示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細（Details）	虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。

フィールド	使用上のガイドライン
セッションキー（Session Key）	ISE によってネットワーク デバイスに返される（EAP の成功メッセージまたはEAP の失敗メッセージにある）セッション キーを示します。
[ユーザ名（Username）]	デバイス管理者のユーザ名を示します。このカラムは必須です。選択解除することはできません。
タイプ（Type）	[認証（Authentication）] および [承認（Authorization）] の 2 つのタイプで構成されます。認証、承認、またはその両方を通過または失敗したユーザ名を示します。このカラムは必須です。選択解除することはできません。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー	特定の許可に選択されているポリシーの名前を表示します。
ISEノード（ISE Node）	アクセス要求が処理される ISE ノードの名前を示します。
ネットワークデバイス名（Network Device Name）	ネットワーク デバイスの名前を示します。
ネットワーク デバイス IP（Network Device IP）	アクセス要求を処理するネットワーク デバイスの IP アドレスを示します。
ネットワーク デバイス グループ（Network Device Groups）	ネットワーク デバイスが属する対応するネットワーク デバイス グループの名前を示します。
デバイスタイプ（Device Type）	異なるネットワーク デバイスからのアクセス要求の処理に使用されるデバイス タイプ ポリシーを示します。
参照先	ネットワーク デバイスからのアクセス要求の処理に使用されるロケーション ベースのポリシーを示します。
デバイス ポート（Device Port）	アクセス要求が行われるデバイスのポート番号を示します。

フィールド	使用上のガイドライン
失敗の理由（Failure Reason）	ネットワーク デバイスによって行われたアクセス要求を拒否した理由を示します。
リモート アドレス（Remote Address）	エンドステーションを一意に識別するIPアドレス、MACアドレス、またはその他の任意の文字列を示します。
一致したコマンドセット（Matched Command Set）	MatchedCommandSet 属性値が存在する場合はその値を示し、MatchedCommandSet 属性値が空の場合、または属性自体が syslog に存在しない場合は空の値を示します。
シェルプロファイル（Shell Profile）	ネットワーク デバイスでコマンドを実行するためのデバイス管理者に付与された権限を示します。

[TACACS ライブログ（TACACS Live Logs）] ページで、次を実行できます。

- データを csv または pdf ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） すべてのユーザのカスタマイズは、ユーザ設定として保存されます。

関連トピック

TACACS+ デバイス管理

TACACS+ のグローバル設定 （363 ページ）

エクスポート サマリ

過去7日間のすべてのユーザによってエクスポートされたレポートの詳細をステータスとともに表示できます。エクスポート サマリには、手動レポートとスケジュールされたレポートの両方が含まれます。[エクスポート サマリ（export summary）] ページは、2 分ごとに自動的に更新されます。[更新（Refresh）] アイコンをクリックすると、[エクスポート サマリ（export summary）] ページが手動で更新されます。

ネットワーク管理者は、進行中またはキューに入れられた状態のエクスポートを取り消すことができます。他のユーザは、自分が開始したエクスポートプロセスをキャンセルすることのみが許可されています。

デフォルトでは、任意の時点で3つのレポートの手動エクスポートのみを実行でき、残りのトリガーされたレポートの手動エクスポートはキューに入れられます。スケジュールされたレポートのエクスポートには、このような制限はありません。

（注） キューに入れられた状態のすべてのレポートが再度スケジューリングされ、Cisco ISE サーバの再起動時に [進行中（In-progress）] または [キャンセル処理中（Cancellation-in-progress）] 状態のレポートには [失敗しました（failed）] とマークがつきます。

（注） プライマリ MnT ノードがダウンしている場合、スケジュールされたレポート エクスポート ジョブはセカンダリ MnT ノードで実行されます。

次の表では、[エクスポート サマリ（Export Summary）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [レポート（Reports）] > [エクスポート サマリ（Export Summary）]** です。

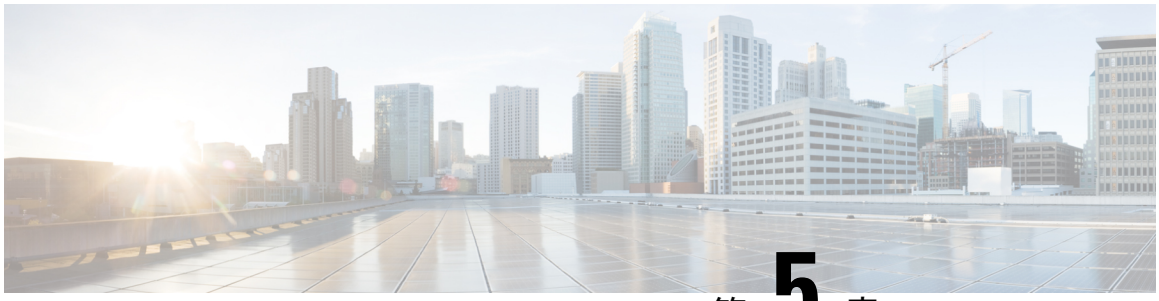
表 *35* : エクスポート サマリ

フィールド	説明
エクスポートされたレポート（Report Exported）	レポートの名前を表示します。
エクスポート実行ユーザ（Exported By）	エクスポートプロセスを開始したユーザのロールを示します。
スケジュール済み（Scheduled）	レポートのエクスポートが予定されているものであるかどうかを示します。
トリガー時刻（Triggered On）	システムでエクスポート処理がトリガーされた時刻を示します。
リポジトリ（Repository）	エクスポートされたデータを格納するリポジトリの名前を表示します。
フィルタ パラメータ（Filter Parameters）	レポートのエクスポート中に選択されたフィルタ パラメータを示します。

フィールド	説明
ステータス	エクスポートされたレポートのステータスを示します。次のいずれかを設定できます。 • キュー（Queued） • 進行中（In-progress） • 完了 • キャンセル処理中（Cancellation-in-progress） • キャンセル • 失敗しました（Failed） • 省略（Skipped） （注） [失敗しました（Failed）] ステータスは、失敗の理由を示します。スキップされたステータスは、プライマリ MnT ノードがダウンしているため、スケジュールされたレポートのエクスポートがスキップされることを示します。

[エクスポート サマリ（Export Summary）] ページでは、次の操作を実行できます。

- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタム フィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。



第 5 章

デバイス管理

TACACS+ デバイス管理

Cisco ISE は、ネットワーク デバイスの設定を制御および監査するための Terminal Access Controller Access-Control System（TACACS+）のセキュリティ プロトコルを使用したデバイス管理をサポートしています。ネットワーク デバイスは、デバイス管理者の操作の認証および認可のために ISE にクエリを行うために設定され、ISE のアカウンティング メッセージを送信して操作をログに記録します。これによって、どのネットワーク デバイスに誰がアクセスできて関連するネットワーク設定を変更できるかについて、きめ細かい制御が容易になります。ISE 管理者は、コマンド セットやシェル プロファイルなどの TACACS 結果をデバイス管理アクセス サービスの許可ポリシー ルールで選択できるようにするポリシー セットを作成できます。ISE モニタリング ノードでは、デバイス管理に関する高度なレポートが提供されます。[ワークセンター（Work Center）] メニューには、すべてのデバイス管理ページが含まれており、ISE 管理者の単一の始点として機能します。

ISE には、TACACS+ を使用するためのデバイス管理ライセンスが必要です。

デバイス管理については 2 つのタイプの管理者がいます。

- デバイス管理者

- ISE 管理者

デバイス管理者は、管理対象デバイスの設定と保守を実行するために、（通常は SSH を介して）スイッチ、ワイヤレス アクセス ポイント、ルータ、ゲートウェイなどのネットワーク デバイスにログインするユーザです。ISE 管理者は、デバイス管理者がログインするデバイスの設定と調整のために ISE にログインします。

ISE にログインしてデバイス管理者の操作を制御する設定を行う ISE 管理者がこのドキュメントの対象読者です。ISE 管理者は、デバイス管理機能（[ワーク センター（Work centers）]>[デバイス管理（Device Administration）]）を使用して、ネットワーク デバイスの設定を制御および監査します。デバイスは、Terminal Access Controller Access-Control System（TACACS）のセキュリティ プロトコルを使用して ISE サーバにクエリを行うように設定できます。ISE モニタリング ノードでは、デバイス管理に関する高度なレポートが提供されます。ISE 管理者は、次のタスクを実行できます。

- TACACS+ の詳細（共有秘密）によるネットワーク デバイスの設定。
- 内部ユーザとしてのデバイス管理者の追加、および必要に応じてイネーブル パスワードの設定。
- コマンド セットやシェル プロファイルなどの TACACS 結果をデバイス管理アクセス サービスの許可ポリシー ルールで選択できるようにするポリシー セットの作成。
- デバイス管理者がポリシーセットに基づいてデバイスにアクセスできるようにするための ISE での TACACS サーバの設定。

デバイス管理者は、ISE サーバと通信するためのデバイスの設定タスクを実行します。デバイス管理者がデバイスにログインすると、デバイスは ISE サーバにクエリを行い、次に内部または外部の ID ストアにクエリを行い、デバイス管理者の詳細を検証します。検証が ISE サーバによって行われると、デバイスは、アカウンティングと監査の目的で、各セッションまたはコマンド許可操作の最終結果を ISE サーバに通知します。

ISE 管理者は、TACACS および Cisco ISE 2.0 以降のリリースを使用してデバイスを管理できます。デバイス管理に関連する設定は、Cisco Secure Access Control System（ACS）サーバのバージョン 5.5、5.6、5.7 および 5.8 から移行することもできます。これ以前のバージョンの場合は、移行の前に 5.5 または 5.6 にアップグレードする必要があります。

（注） TACACS+ の操作をイネーブルにするには、[管理（Administration）]>[システム（System）]>[展開（Deployment）]>[全般設定（General Settings）] ページの [デバイス管理サービスの有効化（Enable Device Admin Service）] チェックボックスをオンにする必要があります。このオプションは展開内の各 PSN で必ず有効にしてください。

（注） Cisco ISE では、既存の基本またはモビリティ ライセンスに加えて TACACS+ サービスを使用するには、デバイス管理ライセンスが必要です。デバイス管理ライセンスは永久ライセンスです。以前のリリースから Cisco ISE リリース 2.0 以降にアップグレードして、TACACS+ サービスを有効にするには、個別のアドオン ライセンスとしてデバイス管理ライセンスを発注する必要があります。Device Administration ライセンスの数は、展開内のデバイス管理ノード数と同じである必要があります。

ISE コミュニティ リソース

デバイス管理属性については、「ISE Device Administration Attributes」を参照してください。

ワイヤレス LAN コントローラ、IOS ネットワーク デバイス、Cisco NX-OS ネットワーク デバイス、およびネットワーク デバイスの TACACS+ 設定については、「ISE Device Administration (TACACS+)」を参照してください。

デバイス管理ワーク センター

[ワークセンター（Work Center）] メニューには、すべてのデバイス管理ページが含まれており、ISE 管理者の単一の始点として機能します。ただし、ユーザ、ユーザ ID グループ、ネットワーク デバイス、デフォルト ネットワーク デバイス、ネットワーク デバイス グループ、認証および許可条件などのデバイス管理に固有ではないページは、[管理（Administration）] などの元のメニュー オプションから、アクセスすることができます。[ワークセンター（Work Centers）] オプションは、正しい TACACS+ ライセンスが取得され、インストールされている場合にのみ使用できます。

[デバイス管理（Device Administration）] メニューには、次のメニュー オプションが含まれています。[概要（Overview）]、[ID（Identities）]、[ユーザ ID グループ（User Identity Groups）]、[外部 ID ストア（Ext ID Stores）]、[ネットワーク リソース（Network Resources）]、[ネットワーク デバイス グループ（Network Device Groups）]、[ポリシー要素（Policy Elements）]、[デバイス管理ポリシーセット（Device Admin Policy Sets）]、[レポート（Reports）] および [設定（Settings）]。

デバイス管理の展開設定

[デバイス管理の展開（Device Administration Deployment）] ページ（**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）] > [展開（Deployment）]**）では、ISE 管理者は [展開（deployment）] セクションで各ノードを参照する必要なく、デバイス管理システムを一元的に表示できます。

[デバイス管理の展開（Device Administration Deployment）] ページには、展開内の PSN が一覧表示されます。これにより、展開内の各 PSN でデバイス管理サービスを個別に有効にする作

業が簡単になります。次のオプションを選択することで、多くの PSN に対するデバイス管理サービスを集合的にイネーブルにできます。

オプション	説明
なし（None）	デフォルトでは、デバイス管理サービスはすべてのノードで無効になっています。
すべてのポリシーサービスノード（All Policy Service Nodes）	すべての PSN でデバイス管理サービスを有効にします。このオプションを使用すると、新しい PSN はデバイス管理のために追加されるときに自動的に有効になります。
特定のノード（Specific Nodes）	展開内のすべての PSN をリストしている [ISE ノード（ISE Nodes）] セクションが表示されます。デバイス管理サービスをイネーブルにする必要があるノードを選択できます。

（注） 展開に TACACS+ のライセンスがない場合、上記のオプションはディセーブルになります。

[TACACSポート（TACACS Ports）] フィールドでは、最大 4 つの TCP ポートをカンマ区切りで入力できます。ポート値の範囲は 1 ～ 65535 です。Cisco ISE ノードおよびそのインターフェイスは指定されたポートで TACACS+ 要求をリッスンします。指定されたポートが他のサービスで使用されないようにする必要があります。デフォルトの TACACS+ ポート値は 49 です。

[保存（Save）] をクリックすると、変更が **[管理（Administration）]** > **[システム（System）]** > **[展開のリスト（Deployment Listing）]** ページで指定されたノードと同期されます。

デバイス管理ポリシー セット

[デバイス管理ポリシーセット（Device Admin Policy Sets）] ページ（[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]）には、ISE 管理者が TACACS+ デバイス管理者の認証と許可を制御するために管理するポリシーセットのリストが含まれています。各ポリシーでは、[通常（Regular）] および [プロキシシーケンス（Proxy Sequence）] の 2 つのモードのいずれかを使用できます。

通常のポリシー セットは認証ルール テーブルおよび許可ルール テーブルから成ります。認証ルール テーブルには、ネットワーク デバイスの認証に必要なアクションを選択する一連のルールが含まれています。

許可ルール テーブルは、承認ビジネス モデルを実装するために必要な特定の承認結果を選択するための一連のルールが含まれています。各許可ルールは、連動するようにルールに一致する必要がある 1 つ以上の条件と、許可プロセスを制御するために選択される一連のコマンド セット、および/またはシェル プロファイルで構成されます。各ルール テーブルには、特定の

状況のルールを上書きするために使用できる例外ポリシーがあり、多くの場合、例外テーブルは一時的な状況に使用されます。

プロキシ シーケンス ポリシー セットには、単一の選択されたプロキシ シーケンスが含まれています。ポリシー セットがこのモードの場合、リモート プロキシ サーバが要求の処理に使用されます（しかし、ローカル アカウンティングがプロキシ シーケンスで設定されている場合があります）。

デバイス管理ポリシー セットの作成

デバイス管理ポリシー セットを作成するには、次の手順を実行します。

始める前に

- [ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）] > [展開（Deployment）] ページで、デバイス管理が TACACS+ 操作に対し有効になっていることを確認します。
- ポリシーに必要なユーザ ID グループ（たとえば、System_Admin、Helpdesk）が作成されていることを確認します。（[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ユーザ ID グループ（User Identity Groups）] > ページ）。メンバー ユーザ（たとえば、ABC、XYZ）が対応するグループに割り当てられていることを確認します。（[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ID（Identities）] > [ユーザ（Users）] ページ）。
- 管理が必要なデバイスで TACACS 設定を行います。（デバイスが ISE にクエリを行いやすいようにするために、[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [TACACS認証設定（TACACS Authentication Settings）] チェックボックスがイネーブルで、TACACS およびデバイスの共有秘密が同一になっています）
- デバイス タイプとロケーションに基づいたネットワーク デバイス グループが作成されていることを確認します。（[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークデバイスグループ（Network Device Groups）] ページ）

ステップ 1 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシー セット（Device Admin Policy Sets）]** の順に選択します。

ステップ 2 いずれかの行の [アクション（Actions）] 列から、歯車アイコンをクリックし、ドロップダウン メニューから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して新しいポリシー セットを挿入します。
[ポリシー セット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 3 ポリシー セットの名前と説明を入力します。

ステップ 4 必要に応じて、[許可されているプロトコル/サーバ順序（Allowed Protocols/Server Sequence）] 列から、（+）記号をクリックし、次のいずれかを選択します。

a) 新しい許可されているプロトコルを作成（Create a New Allowed Protocol）

b) TACACS サーバ順序を作成（Create a TACACS Server Sequence）

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性（たとえば、Device-Location Equals Europe）を選択します。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 7 [使用（Use）] をクリックします。

ステップ 8 [表示（View）] 列から、 をクリックしてすべてのポリシー セットの詳細にアクセスし、認証および許可ポリシーとポリシー例外を作成します。

ステップ 9 必要な認証ポリシーを作成します（たとえば、Rule Name: ATN_Internal_Users、Conditions: DEVICE:Location EQUALS Location #All Locations#Europe：このポリシーは、ヨーロッパ内にあるデバイスにのみ一致します）。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 必要な許可ポリシーを作成します。

例 1：ルール名：Sys_Admin_rule、条件：if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8。この例で、ポリシーはユーザ名 ABC のシステム管理者を照合し、指定されたコマンドの実行を許可し、特権レベル 8 を割り当てます。

例 2：ルール名：HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1。この例で、ポリシーはユーザ名 XYZ のシステム管理者を照合し、指定されたコマンドの実行を許可し、特権レベル 1 を割り当てます。

上記の例で、

- コマンド セット cmd_Sys_Admin および cmd_HDesk は、[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS コマンド セット（TACACS Command Sets）] > [追加（Add）] ページで作成されます。
- TACACS プロファイル Profile_Priv_1 および Profile_priv_8 は、[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）] > [追加（Add）] ページで作成されます。

（注） 認証および許可ポリシーで使用される条件で、デバイス IP アドレス属性に IPv4 または IPv6 の単一アドレスを追加できます。

ステップ 12 [保存（Save）] をクリックします。

TACACS+ 認証設定と共有秘密

次の表では、ネットワーク デバイスの TACACS+ 認証を設定するために使用できる [ネットワークデバイス（Network Devices）] ページのフィールドについて説明します。ナビゲーション パスは次のとおりです。

- （ネットワーク デバイスの場合）**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [TACACS認証設定（TACACS Authentication Settings）]**。
- （デフォルトのデバイスの場合）**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [デフォルトのデバイス（Default Devices）] > [TACACS認証設定（TACACS Authentication Settings）]**。詳細については、「Cisco ISE でのデフォルト ネットワーク デバイスの定義」を参照してください。

フィールド	使用上のガイドライン
共有秘密鍵（Shared Secret）	TACACS+ プロトコルがイネーブルのときにネットワーク デバイスに割り当てられたテキストの文字列。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前にテキストを入力する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。これは必須フィールドではありません。
廃止された共有秘密がアクティブです（Retired Shared Secret is Active）	リタイアメント期間がアクティブな場合に表示されます。
廃止（Retire）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、メッセージ ボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。

フィールド	使用上のガイドライン
残りの廃止期間（Remaining Retired Period）	（上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）次のナビゲーション パスで指定されたデフォルト値が表示されます。**[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）] > [接続設定（Connection Settings）] > [デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]**。デフォルト値は変更することができます。 これにより、新しい共有秘密を入力でき、古い共有秘密は指定された日数にわたってアクティブなままになります。
終了（End）	（上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。
シングル接続モードを有効にする（Enable Single Connect Mode）	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを実行します。 • [レガシーシスコデバイス（Legacy Cisco Devices）] • または、[TACACS+ドラフトコンプライアンスシングル接続のサポート（TACACS+ Draft Compliance Single Connect Support）]。シングル接続モードをディセーブルにすると、ISE はすべての TACACS+ 要求に対して新しい TCP 接続を使用します。

サマリーでは、次の操作を実行できます。

- 廃止期間を日数として指定することで（範囲は 1 ～ 99 です）、古い共有秘密を廃止し、同時に新しい共有秘密を設定することができます。
- 廃止期間中は新旧の共有秘密を使用できます。
- 期限切れになる前に廃止期間を延長できます。
- 廃止期間の終了までは、古い共有秘密のみを使用できます。
- 期限切れになる前に廃止期間を終了できます（[終了（End）] をクリックしてから [送信（Submit）] をクリックします）。

（注） [TACACS+認証設定（TACACS+ Authentication Settings）] オプションへは、**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** > **[追加（Add）]** ページからアクセスすることもできます。

デバイス管理：許可ポリシーの結果

ISE 管理者は、TACACS+ コマンド セットおよび TACACS+ プロファイル（ポリシー結果）を使用して、デバイス管理者に付与される権限およびコマンドを制御することができます。ポリシーはネットワーク デバイスと連動して動作するので、行われる可能性がある偶発的または悪意のある設定変更が回避されます。そのような変更が発生した場合は、デバイス管理の監査レポートを使用して、特定のコマンドを実行したデバイス管理者を追跡することができます。

TACACS+ デバイス管理を許可された FIPS および非 FIPS モードのプロトコル

ポリシーの結果を作成するための Cisco ISE が提供する多数の許可された認証プロトコル サービスがあります。ただし、TACACS+ プロトコルに適用できる PAP/ASCII、CHAP および MS-CHAPv1 などの認証プロトコル サービスは、RADIUS の FIPS 対応 Cisco ISE アプライアンスでディセーブルになっています。その結果、FIPS 対応（**[管理（Administration）]** > **[システム設定（System Settings）]** > **[FIPSモード（FIPS Mode）]**）Cisco ISE アプライアンスを使用している場合は、デバイスの管理のためにこれらのプロトコルを **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可されているプロトコル（Allowed Protocols）]** ページで有効にすることはできません。

したがって、デバイス管理ポリシーの結果で PAP/ASCII、CHAP および MS-CHAPv1 プロトコルを設定するには、FIPS モードと非 FIPS モードのどちらの場合も、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可されているプロトコル（Allowed Protocols）]** ページに移動する必要があります。FIPS モードを有効にすると、デフォルト デバイス管理で許可されたプロトコル設定のみが使用できます。このオプションは、RADIUS では使用できません。

TACACS+ コマンド セット

コマンドセットは、デバイス管理者が実行できるコマンドの指定されたリストを適用します。デバイス管理者がネットワーク デバイスに対して操作コマンドを発行すると、その管理者がこれらのコマンドの発行を認可されているかどうかを判定する問い合わせが ISE に行われます。これは、コマンド認可とも呼ばれます。

コマンド セットのワイルドカードと正規表現

コマンド ラインは、コマンドと 0 個以上の引数から成ります。Cisco ISE は、コマンド ライン（要求）を受信すると、次のさまざまな方法でコマンドおよび引数を処理します。

- ワイルドカード照合パラダイムを使用して、要求内のコマンドをコマンドセットのリストに指定されたコマンドと照合します。

  例：Sh?? または S*

- 正規表現（regex）照合パラダイムを使用して、要求内の引数をコマンド セットのリストに指定された引数と照合します。

  例：Show interface[1-4] port[1-9]:tty*

コマンド ラインおよびコマンド セットのリストの一致

要求されたコマンド ラインをワイルドカードおよび正規表現を含むコマンド セットのリストに一致させるには、次の手順を実行します。

1. コマンド セットのリストを反復し、一致するコマンドを検出します。

   ワイルドカード照合では以下が許可されています。

   - 大文字小文字の区別なし
   - コマンド セット内のコマンドの任意の文字を「?」にでき、要求されたコマンドに存在する必要がある個別の文字に一致させることができます。
   - コマンド セット内のコマンドの任意の文字を「*」にでき、要求されたコマンド内の 0 個以上の文字に一致させることができます。

   次に、例を示します。

要求	コマンド セット	一致	説明
show	show	Y	—
show	SHOW	Y	大文字小文字の区別なし
show	Sh??	Y	任意の文字と一致します
show	Sho??	N	2つ目の「?」は存在しない文字と交差します
show	S*	Y	「*」は任意の文字と一致します
show	S*w	Y	「*」は文字「ho」と一致します

要求	コマンド セット	一致	説明
show	S*p	N	文字「p」は対応しません

2. 一致する各コマンドに対し、Cisco ISE は引数を検証します。

   コマンドセットのリストには、各コマンドのスペースで区切られた一連の引数が含まれています。

   例：Show interface[1-4] port[1-9]:tty.*

   このコマンドには、2 つの引数があります。

   1. 引数 1：interface[1-4]

   2. 引数 2：port[1-9]:tty.*

   要求内のコマンド引数は、パケットに表示される位置が重要な順序で実行されます。コマンド定義内のすべての引数が要求内の引数に一致すると、このコマンド/引数は一致していると見なされます。要求内の無関係な引数はすべて無視されることに注意してください。

（注） 引数には標準の Unix 正規表現を使用します。

複数のコマンド セットを持つルールの処理

1. コマンド セットにコマンドとその引数との一致が含まれる場合、その一致が Deny Always であると、ISE によってそのコマンドセットは Commandset-DenyAlways として指定されます。
2. コマンドセット内のコマンドの一致に Deny Always がない場合は、最初の一致が見つかるまで、コマンド セット内のすべてのコマンドが順番にチェックされます。
   1. 最初の一致が Permit である場合、そのコマンド セットは Commandset-Permit として指定されます。
   2. 最初の一致が Deny である場合、そのコマンド セットは Commandset-Deny として指定されます。
3. ISE は、すべてのコマンド セットを分析したあと、コマンドを次のように認可します。
   1. コマンドセットが Commandset-DenyAlways として指定された場合、ISE によってそのコマンドは拒否されます。
   2. Commandset-DenyAlways がない場合、コマンド セットが Commandset-Permit である場合はそのコマンドが許可されます。そうでない場合、そのコマンドは拒否されます。唯一の例外は、[不一致（Unmatched）] チェックボックスがオンになっている場合です。

TACACS+ コマンド セットの作成

TACACS+コマンドセットのポリシー結果を使用してポリシーセットを作成するには、次の手順を実行します。

ステップ 1 [ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS コマンド セット（TACACS Command Sets）] の順に選択します。

[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシー セット（Device Admin Policy Sets）] ページで TACACS コマンド セットを設定することもできます。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 名前と説明を入力します。

ステップ 4 [追加（Add）] をクリックして、権限の付与、コマンドおよび引数を指定します。

ステップ 5 [付与（Grant）] ドロップダウンで、以下のいずれかを選択できます。

- [許可（Permit）] : 指定したコマンドを許可する場合（たとえば、permit show、permit con* Argument terminal など）。
- [拒否（Deny）] : 指定したコマンドを拒否する場合（たとえば、deny mtrace）。
- [常に拒否（Deny Always）] : 他のコマンドセットで許可されているコマンドをオーバーライドする場合（たとえば、clear auditlogs）。

（注） [付与（Grant）]、[コマンド（Command）] および [引数（Argument）] フィールドの列幅を増やしたり減らしたりするには、アクション アイコンをクリックします。

ステップ 6 [下にリストされていないコマンドを許可（Permit any command that is not listed below）] チェックボックスをオンにして、[付与（Grant）] 列で [許可（Permit）]、[拒否（Deny）] または [常に拒否（Deny Always）] として指定されていないコマンドおよび引数を許可します。

TACACS+ プロファイル

TACACS+プロファイルは、デバイス管理者の最初のログイン セッションを制御します。セッションは、個々の認証、許可、またはアカウンティングの要求を参照します。ネットワークデバイスへのセッション許可要求により、ISE 応答が発生します。この応答には、ネットワークデバイスにより解釈されるトークンが含まれています。ネットワーク デバイスにより、セッション期間中に実行できるコマンドが制限されます。デバイス管理アクセス サービス用の許可ポリシーでは、単一のシェル プロファイルおよび複数のコマンド セットを含めることができます。TACACS+ プロファイル定義は、次の 2 つのコンポーネントに分けられています。

- 共通タスク
- カスタム属性

[TACACS+プロファイル（TACACS+ Profiles）] ページ（[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）]）には、[タスク属性（Task Attribute）] ビューと [未処理（Raw）] ビューの 2 つのビューがあります。共通タスクは [タスク属性（Task Attribute）] ビューを使用して入力でき、カスタム属性は [タスク属性（Task Attribute）] ビューおよび [未処理（Raw）] ビューで作成できます。

[共通タスク（Common Tasks）] セクションを使用すると、頻繁に使用されるプロファイル属性を選択および設定できます。ここに含まれる属性は、TACACS+ プロトコル ドラフト仕様で定義された属性です。ただし、これらの値は、他のサービスからの要求の許可に使用される場合があります。[タスク属性（Task Attribute）] ビューでは、ISE 管理者はデバイス管理者に割り当てられる権限を設定できます。一般的なタスクのタイプは次のとおりです。

- Shell
- WLC
- Nexus
- 汎用（Generic）

[カスタム属性（Custom Attributes）] セクションを使用すると、追加の属性を設定できます。[共通タスク（Common Tasks）] セクションで認識されていない属性のリストも提供されます。各定義は、属性名、属性が必須であるか任意であるかの指定、および属性の値で構成されています。[未処理（Raw）] ビューでは、属性名とその値の間に等号（=）を使用して必須属性を入力することができ、任意の属性は、属性名とその値の間にアスタリスク（*）を使用して入力できます。[未処理（Raw）] ビューで入力された属性は、[タスク属性（Task Attribute）] ビューの [カスタム属性（Custom Attributes）] セクションに反映され、その逆も同様です。[未処理（Raw）] ビューは、クリップボードから属性リスト（たとえば、別の製品の属性リスト）を ISE にコピー ペーストするためにも使用されます。カスタム属性は、非シェル サービスに対して定義できます。

TACACS+ プロファイルの作成

TACACS+ プロファイルを作成するには、次の手順を実行します。

ステップ 1 [ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）] の順に選択します。

[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシー セット（Device Admin Policy Sets）] ページで TACACS コマンド セットを設定することもできます。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [TACACSプロファイル（TACACS Profile）] セクションで、名前と説明を入力します。

ステップ 4 [タスク属性ビュー（Task Attribute View）] タブで、必要な**共通タスク**を確認します。共通タスク設定（360 ページ） ページを参照してください。

ステップ 5 [タスク属性ビュー（Task Attribute View）] タブの [カスタム属性（Custom Attributes）] セクションで、[追加（Add）] をクリックして必須属性を入力します。

共通タスク設定

共通タスクの設定ページを表示するには、**[ワーク センター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[TACACS プロファイル（TACACS Profiles）]** > **[追加（Add）]** に移動します。一般的なタスク タイプは、Shell、WLC、Nexus および Generic です。

Shell

次のオプションは、ISE の管理者がデバイスの管理者権限を設定するために使用できます。

オプション	説明
デフォルトの権限（Default Privilege）	シェル認可のデバイス管理者のデフォルトの（最初の）権限レベルをイネーブルにします。次のオプションのいずれかを選択します。 • 0 ～ 15 の範囲の値を選択します。 • 必要な ID ストア属性を選択します。
最大権限（Maximum Privilege）	イネーブル認証の最大権限レベルを有効にします。0 ～ 15 の範囲の値を選択できます。
アクセス コントロール リスト（Access Control List）	ASCII 文字列（1-251*）または必要な ID ストア属性を選択します。
自動コマンド（Auto Command）	ASCII 文字列（1-248*）または必要な ID ストア属性を選択します。
エスケープなし（No Escape）	エスケープ文字に、次のいずれかのオプションを選択します。 • [True]：エスケープ防止をイネーブルにすることを指定します。 • [False]：エスケープ防止をイネーブルにしないことを指定します。 • 必要な ID ストア属性を選択します。
Timeout	0 ～ 9999 の範囲の値または必要な ID ストア属性を選択します。
アイドル時間（Idle Time）	0 ～ 9999 の範囲の値または必要な ID ストア属性を選択します。

WLC

次のオプションは、ISE の管理者がデバイス管理者による WLC アプリケーションのタブへのアクセスを制御するために使用できます。WLCアプリケーションには次のタブが含まれます：[WLAN]、[コントローラ（Controller）]、[ワイヤレス（Wireless）]、[セキュリティ（Security）]、[管理（Management）] および [コマンド（Commands）]。

オプション	説明
すべて（All）	デバイスの管理者はすべてのWLCアプリケーションのタブにアクセスできます。
モニタ（Monitor）	デバイス管理者はWLCアプリケーションのタブへの読み取り専用アクセス権を持ちます。
ロビー（Lobby）	デバイス管理者は限定された設定の権限のみを持ちます。
オン	デバイス管理者は次のチェックボックスからISE管理者がチェックしたタブにアクセスできます：[WLAN]、[コントローラ（Controller）]、[ワイヤレス（Wireless）]、[セキュリティ（Security）]、[管理（Management）] および [コマンド（Commands）]。

Nexus

次のオプションは、ISE の管理者がデバイス管理者による Cisco Nexus スイッチへのアクセスを制御するために使用できます。

オプション	説明
属性の設定	ISEの管理者は、任意または必須として一般的なタスクによって生成された Nexus 属性を指定できます。

オプション	説明
[ネットワーク ロール（Network Role）]	Nexus が ISE を使用して認証するように設定されると、デバイス管理者は、デフォルトでは、読み取り専用アクセス権を持ちます。デバイス管理者は、これらのロールのいずれかに割り当てることができます。各ロールは許可された操作を定義します。 • なし（None）：権限はありません。 • オペレータ（Operator）（読み取り専用）：全NX-OSデバイスへの完全な読み取りアクセス権を持ちます。 • 管理者（Administrator）（読み取り/書き込み）：全NX-OSデバイスへの完全な読み取り/書き込みアクセス権を持ちます。
仮想デバイス コンテキスト（VDC）	なし（None）：権限はありません。 オペレータ（Operator）（読み取り専用）：VDC への限定された読み取りアクセス 管理者（Administrator）（読み取り/書き込み）：VDCへの限定された読み取り/書き込みアクセス

[汎用（Generic）]

ISE 管理者は、一般的なタスクでは使用できないカスタム属性を指定するオプションを使用します。

イネーブルパスワードを変更するためのコマンドライン インターフェイスへのアクセス

イネーブル パスワードを変更するには、次の手順を実行します。

始める前に

一部のコマンドは特権モードに割り当てられます。したがって、デバイスの管理者がこのモードに認証されているときしか実行できません。

そのデバイスの管理者が特権モードに入ろうとする際に、デバイスは特別なイネーブル認証タイプを送信します。Cisco ISE は、この特別なイネーブル認証タイプを検証するために別のイネーブル パスワードをサポートします。別のイネーブル パスワードはデバイスの管理者が内

部 ID ストアに認証されているときに使用されます。外部 ID ストアとの認証では、同じパスワードが通常のログインに対して使用されます。

ステップ 1 スイッチにログインします。

ステップ 2 Enter を押して次のプロンプトを表示します。

```
Switch>
```

ステップ 3 次のコマンドを実行して、イネーブル パスワードを設定します。

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

（注） パスワードの有効期間がログイン パスワードおよびイネーブル パスワードに設定されている場合、パスワードが指定された時間期間内に変更されないと、ユーザ アカウントは無効になります。Cisco ISE が TACACS+ サーバとして構成され、ネットワーク デバイスで [バイパスを有効にする（Enable Bypass）] オプションが設定されている場合、CLI から（telnet 経由で）イネーブル パスワードを変更できません。内部ユーザのイネーブル パスワードを変更するには、[管理（Administration）] > [IDの管理（Identity Management）] > [アイデンティティ（Identities）] > [ユーザ（Users）] を選択します。

TACACS+ のグローバル設定

TACACS+ のグローバル設定を行うには、次の手順を実行します。

ステップ 1 **[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）]** の順に選択します。

[接続設定（Connection Settings）] タブで、必須フィールドのデフォルト値を変更できます。

- [認証キャッシュタイムアウト（Authorization cache timeout）] フィールドで、内部ユーザの特定の属性を最初の認証要求時にキャッシュ化するために存続可能時間（TTL）の値を設定できます。キャッシュ化された属性には、ユーザ名と、UserGroup などのユーザ固有の属性が含まれます。このような属性は、[システム管理（System Administration）] > [設定（Configuration）] > [ディクショナリ（Dictionaries）] > [ID（Identity）] > [内部ユーザ（Internal Users）] で作成します。デフォルト値は 0 です。つまり、認証キャッシュが無効になっています。
- 単一接続のサポート（Single Connect Support）：シングル接続モードを無効にすると、ISE はすべての TACACS+ 要求に対して新しい TCP 接続を使用します。

ステップ 2 [パスワード変更制御（Password Change Control）] タブで、パスワードの更新を TACACS+ を介して許可するかどうかを制御するのに必要なフィールドを定義します。

[Telnetパスワード変更を有効にする（Enable Telnet Change Password）] セクションのプロンプトは、このオプションが選択されている場合にのみ有効です。選択されていない場合は、[Telnetパスワード変更を無効にする（Disable Telnet Change Password）] のプロンプトが有効になります。パスワード プロンプトはすべてカスタマイズ可能で、必要に応じて変更できます。

[パスワード ポリシー違反メッセージ（Password Policy Violation Message）] フィールドに、新しいパスワードが指定された条件と一致しない場合に、内部ユーザが設定したパスワードに適したエラー メッセージを表示できます。

ステップ 3 [セッションキーの割り当て（Session Key Assignment）] タブで、セッションに TACACS+ 要求をリンクするために必要なフィールドを選択します。

セッション キーは、クライアントからの AAA 要求をリンクするためにモニタリング ノードによって使用されます。デフォルト設定では、[NASアドレス（NAS-Address）]、[ポート（Port）]、[リモートアドレス（Remote-Address）]、および [ユーザ（User）] フィールドが有効になっています。

ステップ 4 [**保存（Save）**] をクリックします。

関連トピック

TACACS+ 認証設定と共有秘密 （353 ページ）
RADIUS トークン サーバのユーザ属性キャッシュ （724 ページ）

Cisco Secure ACS から Cisco ISE へのデータ移行

移行ツールを使用して、ACS 5.5 以降からデータをインポートし、すべてのネットワーク デバイスにデフォルトの TACACS+ 秘密を設定できます。**[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）]** に移動して、[準備（Prepare）] セクションで、[ソフトウェアのダウンロード Web ページ（Download Software Webpage）] をクリックして移行ツールをダウンロードします。ツールを PC に保存し、[migTool] フォルダから migration.bat ファイルを実行し、移行プロセスを開始します。移行に関する詳細については、お使いのバージョンの ISE の『Migration Guide』を参照してください。

デバイス管理アクティビティのモニタ

Cisco ISE では、TACACS+ で設定されたデバイスのアカウンティング、認証、許可、およびコマンドアカウンティングに関する情報を参照できる、さまざまなレポートおよびログが提供されます。オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [レポート（Reports）] > [ISEレポート（ISE Reports）]** の順に選択します。

また、**[操作（Operations）] > [レポート（Reports）] > [ISEレポート（ISE Reports）]** ページでレポートを表示することもできます。

ステップ 2 [レポート セレクタ（Report Selector）] で、[デバイス管理（Device Administration）] を展開し、[認証概要（Authentication Summary）]、[TACACS アカウンティング（TACACS Accounting）]、[TACACS 認証（TACACS Authentication）]、[TACACS 許可（TACACS Authorization）]、[TACACS コマンド アカウンティング（TACACS Command Accounting）]、[失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）]、[ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）]、[ユーザ別上位 N の認証（Top N Authentication by User）] レポートを表示します。

ステップ 3 レポートを選択し、[フィルタ（Filters）] ドロップダウン リストを使用して、検索するデータを選択します。

ステップ 4 データを表示する [時間範囲（Time Range）] を選択します。

ステップ 5 [実行（Run）] をクリックします。

TACACS ライブ ログ

次の表では、TACACS+ AAA の詳細を表示する [TACACS ライブ ログ（TACACS Live Logs）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [TACACS ライブ ログ（TACACS Live Logs）]** です。TACACS ライブ ログはプライマリ PAN だけで表示されます。

表 *36 : TACACS* ライブ ログ

フィールド	使用上のガイドライン
生成日時（Generated Time）	特定のイベントがトリガーされた時点に基づいて、syslog の生成日時を示します。
ログに記録された時刻（Logged Time）	syslog がモニタリング ノードによって処理され、保存された時刻を示します。このカラムは必須です。選択解除することはできません。
ステータス	認証が成功したか失敗したかを示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細（Details）	虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。
セッションキー（Session Key）	ISE によってネットワーク デバイスに返される（EAP の成功メッセージまたはEAP の失敗メッセージにある）セッション キーを示します。

フィールド	使用上のガイドライン
[ユーザ名（Username）]	デバイス管理者のユーザ名を示します。このカラムは必須です。選択解除することはできません。
タイプ（Type）	[認証（Authentication）] および [承認（Authorization）] の 2 つのタイプで構成されます。認証、承認、またはその両方を通過または失敗したユーザ名を示します。このカラムは必須です。選択解除することはできません。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー	特定の許可に選択されているポリシーの名前を表示します。
ISEノード（ISE Node）	アクセス要求が処理される ISE ノードの名前を示します。
ネットワークデバイス名（Network Device Name）	ネットワーク デバイスの名前を示します。
ネットワーク デバイス IP（Network Device IP）	アクセス要求を処理するネットワーク デバイスの IP アドレスを示します。
ネットワーク デバイス グループ（Network Device Groups）	ネットワーク デバイスが属する対応するネットワーク デバイス グループの名前を示します。
デバイスタイプ（Device Type）	異なるネットワーク デバイスからのアクセス要求の処理に使用されるデバイス タイプ ポリシーを示します。
参照先	ネットワーク デバイスからのアクセス要求の処理に使用されるロケーション ベースのポリシーを示します。
デバイス ポート（Device Port）	アクセス要求が行われるデバイスのポート番号を示します。
失敗の理由（Failure Reason）	ネットワーク デバイスによって行われたアクセス要求を拒否した理由を示します。
リモート アドレス（Remote Address）	エンドステーションを一意に識別する IP アドレス、MAC アドレス、またはその他の任意の文字列を示します。

フィールド	使用上のガイドライン
一致したコマンドセット（Matched Command Set）	MatchedCommandSet 属性値が存在する場合はその値を示し、MatchedCommandSet 属性値が空の場合、または属性自体が syslog に存在しない場合は空の値を示します。
シェルプロファイル（Shell Profile）	ネットワーク デバイスでコマンドを実行するためのデバイス管理者に付与された権限を示します。

[TACACS ライブログ（TACACS Live Logs）] ページで、次を実行できます。

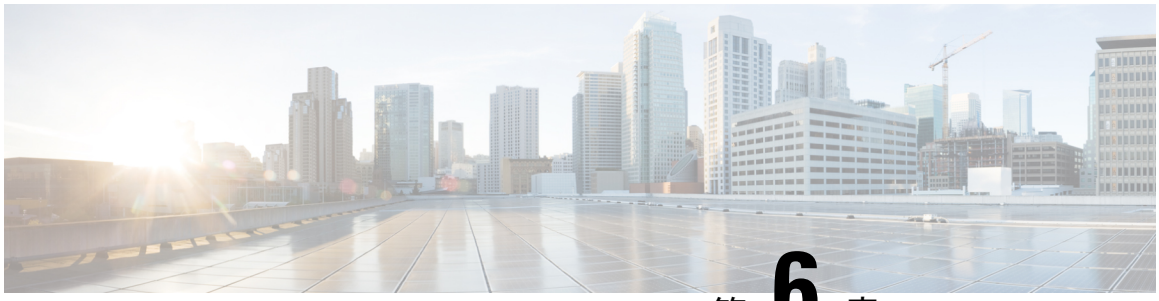
- データを csv または pdf ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタム フィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） すべてのユーザのカスタマイズは、ユーザ設定として保存されます。

関連トピック

TACACS+ デバイス管理

TACACS+ のグローバル設定 （363 ページ）



第 6 章

ゲストおよびセキュア Wi-Fi

Cisco ISE ゲスト サービス

Cisco Identity Services Engine（ISE）ゲスト サービスを使用すると、ビジター、請負業者、コンサルタント、顧客などのゲストにセキュアなネットワーク アクセスを提供することができます。Cisco ISE の Base ライセンスを持つゲストをサポートでき、会社のインフラストラクチャと機能の要件に応じて複数の展開オプションから選択できます。

Cisco ISE は、企業のネットワークおよび内部リソースとサービスへのゲストおよび従業員のオンボーディングを行う Web ベースのモバイル ポータルを提供します。

管理者ポータルで、ゲスト ポータルおよびスポンサー ポータルの作成と編集、ゲスト タイプの定義によるゲストアクセス権限の設定、ゲストアカウントの作成と管理のためのスポンサー権限の割り当てを行うことができます。

- ゲスト ポータル （394 ページ）
- ゲスト タイプおよびユーザ ID グループ （371 ページ）
- スポンサー ポータル （414 ページ）
- スポンサー グループ （416 ページ）

ISE コミュニティ リソース

ISE ゲストおよび Web 認証に関する ISE コミュニティ リソースのリストについては、「ISE Guest Access - ISE Guest and Web Authentication.」を参照してください。

分散環境のエンドユーザのゲスト ポータルとスポンサー ポータル

Cisco ISE のエンドユーザ Web ポータルは、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナに基づき、設定、セッション サポート、およびレポート作成を提供します。

- **管理ノード**：ユーザ、デバイス、およびエンドユーザ ポータルが管理ノードに書き込まれる構成の変更。
- **ポリシー サービス ノード**：エンドユーザ ポータルはポリシー サービス ノードで実行する必要があります。ここでは、ネットワーク アクセス、クライアント プロビジョニング、ゲスト サービス、ポスチャ、およびプロファイリングを含むすべてのセッション トラフィックが処理されます。ポリシー サービス ノードがノード グループに含まれる場合、1 つのノードで障害が発生すると、他のノードが障害を検出し、保留中のセッションをリセットします。
- **モニタリング ノード**：モニタリング ノードは、デバイス ポータル、スポンサー ポータル、およびゲスト ポータルでのエンドユーザおよびデバイスのアクティビティについて、データを収集、集約、およびレポートします。プライマリ モニタリング ノードで障害が発生した場合は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング ノードになります。

ゲスト アカウントとスポンサー アカウント

- **ゲスト アカウント**：ゲストとは、通常、ネットワークへの一時アクセスを必要とする承認ユーザ、担当者、顧客、その他のユーザを表します。いずれかのゲスト展開シナリオを使用して、従業員のネットワーク アクセスを許可する場合は、従業員用のゲスト アカウントを使用することもできます。スポンサーポータルにアクセスして、スポンサーおよびアカウント登録ゲストによって作成されたゲスト アカウントを表示できます。

- **スポンサー アカウント**：スポンサー ポータルを使用して、承認ユーザ用の一時アカウントを作成し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲスト アカウントを作成した後、スポンサー ポータルを使用してそれらのアカウントを管理し、ゲストにアカウントの詳細を提供できます。

次のユーザがゲスト アカウントを作成できます。

- **スポンサー**：管理者ポータルで、ゲスト アカウントを作成し管理するスポンサー ポータルにアクセスできる、スポンサーのアクセス権限と機能のサポートを定義できます。
- **ゲスト**：ゲストは、アカウント登録ゲスト ポータルに自分自身を登録することによって、独自のアカウントを作成することもできます。これらのアカウント登録ゲストは、ポータル設定に基づいて、ログイン クレデンシャルを受け取る前にスポンサーの承認が必要になる場合があります。

  ゲストは、ホットスポット ゲスト ポータルを使用してネットワークにアクセスすることもできます。このポータルでは、ゲスト アカウントやユーザ名およびパスワードなどのログイン クレデンシャルを作成する必要はありません。
- **従業員**：ID ストア（Active Directory、LDAP、内部ユーザなど）に含まれている従業員は、クレデンシャルを持つゲスト ポータル（Sponsored-Guest ポータルおよびアカウント登録ゲスト ポータル）が設定されている場合には、これを使用してアクセスすることもできます。

ゲスト アカウントが作成されると、ゲストは Sponsored-Guest ポータルを使用してネットワークにログインおよびアクセスできます。

ゲスト タイプおよびユーザ ID グループ

各ゲスト アカウントをゲスト タイプに関連付ける必要があります。ゲスト タイプを使用して、スポンサーは、ゲスト アカウントに対して、さまざまなレベルのアクセス権や、さまざまなネットワーク接続時間を割り当てることができます。これらのゲスト タイプは、特定のネットワーク アクセス ポリシーに関連付けられます。Cisco ISE には、次のデフォルト ゲスト タイプが含まれます。

- 担当者：長い期間（最大 1 年）、ネットワークへのアクセスを必要とするユーザ。
- 日次：1 ～ 5 日間の短期間に、ネットワーク リソースへのアクセスを必要とするゲスト。
- 週次：2 ～ 3 週間の間、ネットワークへのアクセスを必要とするユーザ。

ゲスト アカウントを作成する場合、特定のスポンサー グループを特定のゲスト タイプを使用するように制限することができます。このようなグループのメンバーは、そのゲスト タイプに指定された機能のみを持つゲストを作成できます。たとえば、スポンサー グループ ALL_ACCOUNTS は担当者ゲスト タイプのみを使用するように設定でき、スポンサー グループ OWN_ACCOUNTS および GROUP_ACCOUNTS は日次または週次ゲスト タイプを使用するに設定できます。また、通常、アカウント登録ゲスト ポータルを使用するアカウント登録ゲストは、1 日のみのアクセスを必要とするため、これらのゲストには日次ゲスト タイプを割り当てることができます。

ゲスト タイプは、ゲストのユーザ ID グループを定義します。

詳細については、以下を参照してください。

- ユーザ ID グループ （566 ページ）
- ユーザ ID グループの作成 （577 ページ）

ゲスト タイプの作成または編集

デフォルトのゲスト タイプとデフォルトのアクセス権限や設定を編集できます。または、新しいゲスト タイプを作成できます。ユーザが行った変更は、このゲスト タイプを使用して作成された既存のゲスト アカウントに適用されます。ログインしているゲスト ユーザには、ログアウトして再度ログインするまでこれらの変更は表示されません。また、ゲスト タイプを複製して、同じアクセス権限を持つ追加のゲスト タイプを作成できます。

各ゲスト タイプに名前、説明、およびこのゲスト タイプでゲスト アカウントを作成できるスポンサー グループのリストがあります。ゲスト タイプに対して、アカウント登録ゲストにのみ使用すること、（任意のスポンサー グループによる）ゲスト アカウントの作成には使用しないこと、などを指定できます。

下記で説明するフィールドに入力します。

これら設定のナビゲーション パスは、**[ゲスト アクセス（Guest Access）] > [設定（Configure）] > [ゲスト タイプ（Guest Types）]** です。これらの設定を使用して、ネットワークにアクセスできるゲストのタイプおよびそのアクセス権限を作成します。また、このタイプのゲストを作成できるスポンサー グループを指定できます。

フィールド	使用上のガイドライン
ゲスト タイプ名（Guest type name）	デフォルトのゲスト タイプおよび作成した別のタイプと区別できるこのゲスト タイプの名前を入力します（1 ～ 256 文字）。
説明	このゲスト タイプの推奨される使用方法に関する追加情報（最大 2000 文字）を入力します（「アカウント登録ゲストに使用」、「ゲスト アカウントの作成に使用禁止」など）。
言語ファイル（Language File）	このゲスト タイプを使用してポータルに使用する言語ファイルをエクスポートまたはインポートします。
追加データの収集（Collect Additional Data）	ゲストから追加の情報を収集するにはカスタム フィールドを選択します。 カスタム フィールドは、**[ゲストアクセス（Guest Access）] > [設定（Settings）] > [カスタムフィールド（Custom Fields）]** で管理されます。

フィールド	使用上のガイドライン
最大アクセス時間—アカウント有効期間の開始（Maximum Access Time—Account Duration Starts）	[最初のログインから（From first login）]：アカウントの開始時刻は、ゲスト ユーザがゲスト ポータルに最初にログインしたときに開始され、終了時刻は指定された期間に相当します。ゲストユーザはログインしなければ、アカウントがゲストアカウントの消去ポリシーによって削除されるまで、アカウントは初回ログイン待ち状態のままになります。自己登録され、スポンサーが作成したユーザ アカウントは、作成して自分のアカウントにログオンした時点から始まります。 （注） [これらの曜日および時間のみアクセスを許可（Allow access only on these days and times）] を使用すると、ロケーションは、これらの時間のコンテキストで使用されます。FFL アクセスがロケーションに基づかないようにするには、アクセス用の日付と時刻を設定しないでください。 [スポンサーが指定した日付から（From sponsor-specified date）]：このゲスト タイプのゲストがアクセスでき、ネットワークに接続され続けることができる、最大の日数、時間または分を 1 ～ 999 で指定します。 この設定を変更した場合、変更内容はこのゲストタイプを使用して作成された既存のゲストアカウントには適用されません。
これらの曜日および時間のみアクセスを許可（Allow access only on these days and times）	時間範囲を入力し、曜日を選択して、このゲストタイプがいつネットワークにアクセスできるかを指定します。このゲストタイプがこれらの時間パラメータを超えて接続を維持している場合、ログオフされます。時間範囲は、このゲストタイプを使用してゲストに割り当てられた場所で定義されたタイム ゾーンに基づきます。 + および - をクリックして、アクセス時間制限を増減します。
ゲスト アカウントの消去ポリシーの設定（Configure guest account Purge Policy）	エンドポイント消去ジョブをスケジュールできます。エンドポイントの消去スケジュールはデフォルトで有効になっており、Cisco ISE は 30 日以上経過したエンドポイントを削除します。詳細については、「エンドポイントの消去の設定」を参照してください。

フィールド	使用上のガイドライン
ログイン オプション—最大同時ログイン数（Login Options—Maximum simultaneous logins）	このゲスト タイプが同時に実行できる最大ユーザ セッション数を入力します。
ゲストが制限を超えた場合（When guest exceeds limit）	[最大同時ログイン数（Maximum simultaneous logins）] を選択した場合は、その制限に到達した後にユーザが接続したときに実行するアクションも選択する必要があります。 **ゲストが制限を超えた場合** • **最も古い接続を切断（Disconnect the oldest connection）** • **最も新しい接続を切断（Disconnect the newest connection）** • エラーメッセージを示すポータルページにユーザをリダイレクトする（Redirect user to a portal page showing an error message）：特定の時間エラーメッセージが表示され、その後セッションが切断されてユーザがゲスト ポータルにリダイレクトされます。エラー ページの内容は、[メッセージ（Messages）] > [エラーメッセージ（Error Messages）] タブの [ポータルページのカスタマイズ（Portal Page Customization）] ダイアログで設定します。
ゲストが登録可能な最大デバイス数（Maximum devices guests can register）	各ゲストに登録できるデバイスの最大数を入力します。そのゲストタイプのゲストに登録済みの値より小さい値を最大数として設定できます。この値は、新しく作成されたゲストアカウントにのみ適用されます。

フィールド	使用上のガイドライン
ゲストにゲスト ポータルのバイパスを許可する（Allow guest to bypass the Guest portal）	クレデンシャルを持つゲストのキャプティブ ポータル（Web 認証ページ）をバイパスし、有線およびワイヤレス（dot1x）サプリカントまたは VPN クライアントに認証情報を提供することでネットワークにアクセスすることをユーザに許可します。ゲスト アカウントは、[初期ログインを待機（Awaiting Initial Login）] 状態と AUP ページをバイパスして [アクティブ（Active）] 状態になります。 この設定を有効にしない場合、ユーザは初めにクレデンシャルを持つゲストのキャプティブ ポータルを使用してログインしないと、ネットワークの他の部分にアクセスできません。
アカウント期限切れ通知—アカウント期限切れの__日前にアカウント期限切れ通知を送信する（Account Expiration Notification—Send account expiration notification __ days before account expires）	ゲストのアカウントが期限切れになる前にゲストに通知を送信します。期限切れの何日前、何時間前、または何分前に通知するかを指定します。
メッセージの表示言語（View messages in）	電子メールまたは SMS 通知の表示言語を指定します。
E メール	アカウントの失効通知に使用する手段としてメールを選択します。
次のカスタマイズを使用（Use customization from）	別のポータルから電子メールのカスタマイズを選択します。
メッセージ	アカウントの有効期限通知に使用するテキストを入力します。
テキストのコピー元（Copy text from）	アカウントの期限切れ通知のために別のゲスト タイプ用に作成した電子メール テキストを再利用します。
テスト電子メールの送信先（Send test email to me at）	自分の電子メール アドレスに送信することによって、電子メール通知が意図したとおりに表示されることを確認します。
SMS	アカウントの失効通知に使用する手段としてテキスト（SMS）を選択します。
メッセージ	アカウントの有効期限通知に使用するテキストを入力します。
テキストのコピー元（Copy text from）	別のゲスト タイプ用に作成したテキスト メッセージを再使用します。

フィールド	使用上のガイドライン
テスト SMS の送信先（Send test SMS to me at）	自分の携帯電話に送信することによって、テキスト通知が意図したとおりに表示されることを確認します。
これらのスポンサー グループはこのゲスト タイプを作成できる（These sponsor groups can create this guest type）	このゲスト タイプでゲスト アカウントを作成できるスポンサー グループを選択します。 このゲストタイプの使用を無効にする場合は、いずれのスポンサー グループにも割り当てないでください。このゲストタイプの使用を中止するには、リストされたスポンサー グループを削除します。

次のタスク

- このゲスト タイプを使用するスポンサー グループを作成または変更します。
- 該当する場合は、アカウント登録ゲスト ポータルで、このゲスト タイプをアカウント登録ゲストに割り当てます。

ゲスト タイプの無効化

ゲスト アカウントで使用されているゲスト タイプのうち、最後に残ったゲスト タイプは削除できません。使用されているゲスト タイプを削除するには、最初にそのゲスト タイプが使用できなくなることを確認します。ゲスト タイプをディセーブルにしても、そのゲスト タイプで作成したゲスト アカウントには影響しません。

次の手順で、ターゲット ゲスト タイプを準備および無効にする方法を説明します。

ステップ 1 ターゲット ゲスト タイプを使用して、スポンサーがゲストを作成するのを許可しているスポンサー グループを識別します。**[ワークセンター（Work Centers）][ゲストアクセス（Guest Access）][ポータルとコンポーネント（Portals and Components）][スポンサーグループ（Sponsor Groups）]** を選択し、各スポンサー グループを開いて、**[このスポンサーグループはこれらのゲストタイプを使用してアカウントを作成できます（This sponsor group can create accounts using these guest types）]** リストを調べます。

ステップ 2 ターゲット ゲスト タイプを割り当てるアカウント登録ポータルを識別します。**[ワーク センター（Work Center）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** を選択します。各アカウント登録ゲスト ポータルを開きます。ポータルが特定のゲスト タイプを使用している場合、[ポータル設定（Portal Settings）] を展開し、[ゲストとしてこのポータルを使用する従業員のログインオプションの継承元（Employees using this portal as guests inherit login options from）] フィールドに割り当てられたゲスト タイプを変更します。

ステップ 3 削除するゲスト タイプを開き、前の手順で識別したすべてのスポンサー グループを削除します。この操作により、効果的に、すべてのスポンサーがこのゲスト タイプの新しいゲスト アカウントの作成を使用でき

なくします。**[ワークセンター（Work Center）]**>**[ゲストアクセス（Guest Access）]**>**[ポータルとコンポーネント（Portals and Components）]** > **[ゲストタイプ（Guest Type）]** を選択します。

これで完了です。実際にゲストタイプは削除できません。将来的にすべてのポータルで使用しないことを確認します。

エンドポイント ユーザの最大同時ログイン数の設定

ゲストに許可される同時ログインの最大数を設定できます。

ユーザがゲストポータルにログインし、正常に認証されると、ユーザがすでにログインの最大数に達しているかどうかを確認するために、ユーザの既存のログイン数がチェックされます。達していた場合、ゲスト ユーザはエラー ページにリダイレクトされます。エラー ページが表示され、セッションが停止します。そのユーザがインターネットに再度アクセスしようとすると、ユーザの接続はゲスト ポータルのログイン ページにリダイレクトされます。

始める前に

このポータルの許可ポリシーで使用している許可プロファイルで [アクセス タイプ（Access Type）] が *Access_Accept* に設定されていることを確認します。[アクセスタイプ（Access Type）] が *Access_Reject* に設定されている場合は、最大同時ログイン数は機能しません。

ステップ 1 **[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト タイプ（Guest Type）]** の順に選択し、[ログイン オプション（Login Options）] の下で次の操作を実行します。

a) [最大同時ログイン数（Maximum simultaneous logins）] を有効にします。これは、デフォルトのゲストタイプですでに有効になっています。

b) [ゲストが制限を超えた場合（When guest exceeds limit）] の下で、[最も新しい接続を切断（Disconnect the newest connection）] を選択します。

c) [エラーメッセージを示すポータルページにユーザをリダイレクトする（Redirect user to a portal page showing an error message）] を選択して、許可する同時ログインの最大数を選択します。

ステップ 2 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** を選択して認証プロファイルを作成します。

a) [共通タスク（Common Tasks）] で、[Webリダイレクション（Web Redirection）] をチェックし、次の操作を実行します。

- 最初のドロップダウンで、[中央集中Web認証（Centralized Web Auth）] を選択します。
- 前提条件の一部として作成した **ACL** を入力します。
- [値（Value）] の場合、リダイレクト先のゲスト ポータルを選択します。

b) [一般的なタスク（Common Tasks）] でスクロール ダウンして、[再認証（Reauthentication）] をチェックして、次を行います。

- [タイマー（Timer）] に、ユーザがゲスト ポータルにリダイレクトされる前にエラー ページが表示される時間を入力します。
- [再認証中に接続を維持（Maintain Connectivity During Reauthentication）] で、[デフォルト（Default）] を選択します。

ステップ 3 [ポリシー（Policy）]>[ポリシー セット（Policy Sets）] を選択して、属性 NetworkAccess.SessionLimitExceeded が true の場合にユーザがポータルにリダイレクトされるように、許可ポリシーを作成します。

次のタスク

[ポータルページのカスタマイズ（Portal Page Customization）] タブでエラー ページのテキストをカスタマイズするには、**[メッセージ（Messages）][エラーメッセージ（ErrorMessages）]** タブで、エラー メッセージ キー *ui_max_login_sessions_exceeded_error* のテキストを変更します。

期限切れのゲスト アカウントを消去するスケジューリング設定

アクティブなまたは一時停止されたゲストアカウントがアカウント有効期間（スポンサーがアカウントを作成するときに定義）の終了に達すると、そのアカウントは失効します。ゲストアカウントが期限切れになった場合、影響を受けるゲストはネットワークにアクセスできません。スポンサーは、期限切れになったアカウントを、消去される前に延長することができます。ただし、アカウントが消去された場合、スポンサーは、新しいアカウントを作成する必要があります。

期限切れになったゲストアカウントが消去された場合、関連するエンドポイントおよびレポート情報とロギング情報は保持されます。

Cisco ISE は、デフォルトで 15 日ごとに期限切れになったゲスト アカウントを自動的に消去します。[次回消去日（Date of next purge）] は、次の消去の発生時期を示します。次のことも実行できます。

- X 日ごとに消去が行われるようにスケジュール設定します。最初の消去は X 日後の**消去の時刻**に行われ、その後消去は X 日ごとに行われます。
- X 週間ごとに特定の曜日に消去が行われるようにスケジュール設定します。最初の消去は次のその**曜日**の**消去の時刻**に行われ、その後消去は設定された週数おきにその曜日と時刻に行われます。たとえば、月曜日に、5 週間おきに木曜日に消去が行われるように設定したとします。次の消去は、今から 5 週間後の木曜日ではなく、その週の木曜日に行われます。
- [今すぐ消去（Purge Now）] をクリックして、ただちに消去を行います。

消去が実行されるようにスケジュールされているときに Cisco ISE サーバがダウンした場合は、消去は行われません。消去プロセスは、サーバがその時点で動作していれば、次にスケジュールされている消去時刻に再度実行されます。

ステップ 1 **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Settings）] > [ゲスト アカウント消去ポリシー（Guest Account Purge Policy）]** の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 期限切れのゲスト アカウント レコードを即時に消去するには、[今すぐ消去（Purge Now）] をクリックします。
- 消去をスケジュールするには、[期限切れのゲスト アカウントの消去のスケジュール（Schedule purge of expired guest accounts）] をオンにします。

（注） 各消去の完了後に、[次回消去日（Date of next purge）] が次にスケジュールされている消去に合わせてリセットされます。

ステップ 3 [経過後にポータル ユーザ情報を期限切れにする（Expire portal-user information after）] で、ユーザを期限切れにするための非アクティブ日数を指定します。この設定により、使用されていない LDAP および Active Directory アカウントが ISE データベースに無期限に残ることを防ぎます。

最初のログインが行われない場合、指定された期間の終了時にゲスト アカウントが期限切れ状態になり、設定された消去ポリシーに基づいて消去されます。

ステップ 4 [経過後にポータル ユーザ情報を期限切れにする（Expire portal-user information after）] で、ユーザを期限切れにするための非アクティブ日数を指定します。この設定により、使用されていない LDAP および Active Directory アカウントが ISE データベースに無期限に残ることを防ぎます。

ステップ 5 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

ゲスト アカウント作成用のカスタム フィールドの追加

ゲスト アクセスを提供する場合、名前、電子メール アドレス、電話番号以外の情報をゲストから収集する必要がある場合があります。Cisco ISE には、会社のニーズに固有の、ゲストに関する追加情報の収集に使用できるカスタム フィールドが用意されています。ゲスト タイプおよびアカウント登録ゲスト ポータルとスポンサー ポータルにカスタム フィールドを関連付けることができます。Cisco ISE はデフォルトのカスタム フィールドを提供しません。

ステップ 1 すべてのゲスト ポータルとスポンサー ポータルのカスタム フィールドを追加、編集、または削除するには、**[ゲスト アクセス（Guest Access）] > [設定（Settings）] > [カスタム フィールド（Custom Fields）]** を選択します。

ステップ 2 [カスタム フィールド名（Custom Field Name）] に入力し、ドロップダウン リストから**データ タイプ**を選択し、カスタム フィールドに関する追加情報を提供するのに役立つ**ヒント テキスト**を入力します。たとえば、Date of Birth と入力し、[Date-MDY] を選択して、日付形式に関するヒントとして MM/DD/YYYY を入力します。

ステップ 3 [追加（Add）] をクリックします。

カスタム フィールドがリストにアルファベット順またはソート順序のコンテキストで表示されます。

ステップ 4 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

（注） カスタム フィールドを削除すると、ゲスト タイプの [カスタム フィールド（Custom Fields）] リスト、およびアカウント登録ゲスト ポータルとスポンサー ポータルの設定で選択できなくなります。フィールドが使用されている場合、[削除（Delete）] は無効になります。

次のタスク

目的のカスタム フィールドを含めることが可能です。

- そのゲスト タイプで作成されたアカウントにこの情報が含まれるようにゲスト タイプを定義する場合。「ゲスト タイプの作成または編集」を参照してください。
- ゲスト アカウントの作成時にスポンサーが使用するスポンサー ポータルを設定する場合。#unique_407を参照してください。
- アカウント登録ゲスト ポータルを使用してアカウント登録ゲストからの情報を要求する場合。アカウント登録ゲスト ポータルの作成 （406 ページ） を参照してください。

電子メールでの通知用の電子メール アドレスおよび SMTP サーバの指定

Cisco ISE では、スポンサーおよびゲストに、情報と手順を通知する電子メールを送信できます。これらの電子メールでの通知を配信するように SMTP サーバを設定できます。また、ゲストに通知を送信する電子メール アドレスを指定できます。

（注） ゲスト通知には、UTF-8 に互換性がある電子メール クライアントが必要です。

シングル クリック スポンサーの承認機能を使用するには、HTML 対応の電子メール クライアント（機能を有効にする）が必要です。

ステップ 1 電子メール設定を指定し、すべてのゲスト ポータルおよびスポンサー ポータルの SMTP サーバを設定するには、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Settings）] > [ゲスト電子メールの設定（Guest Email Settings）]** の順に選択します。

ステップ 2 [ゲストへの電子メール通知を有効にする（Enable email notifications to guests）] はデフォルトでオンになっています。この設定を無効にした場合、ゲストは、ゲスト ポータルとスポンサー ポータルの設定中に有効にした他の設定に関係なく、電子メールでの通知を受信しません。

ステップ 3 ゲストに電子メールでの通知を送信するために指定されている [デフォルトの送信元メールアドレス（Default “From” email address）] を入力します。たとえば、donotreply*@yourcompany*.com と入力します。

ステップ 4 次のいずれかを実行します。

- ゲストのアカウントを作成したスポンサーからの通知をゲストが受信するようにする場合は、[スポンサーの電子メールアドレスから通知を送信する（スポンサードの場合）（Send notifications from sponsor's email address (if sponsored)）] をオンにします。アカウント登録ゲストは、デフォルトの電子メール アドレスから通知を受信します。
- ゲストがスポンサードかアカウント登録かに関係なく通知を受信するようにする場合は、[常にデフォルトの電子メール アドレスから通知を送信する（Always send notifications from the default email address）] をオンにします。

ステップ 5 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

ゲストのロケーションおよび SSID の割り当て

ゲスト ロケーションはタイム ゾーンの名前を定義し、ゲストにログインした時間関連設定を適用するために ISE によって使用されます。ゲスト ロケーションは、ゲスト アカウントを作成するスポンサー、およびアカウント登録ゲストによってゲストアカウントに割り当てられます。デフォルトのゲスト ロケーションは San Jose です。他のゲスト ロケーションが追加されていない場合、すべてのアカウントにこのゲスト ロケーションが割り当てられます。1 つ以上の新しいロケーションを作成しないと、San Jose のゲスト ロケーションは削除できません。すべてのゲストが San Jose と同じタイムゾーンにいる場合を除き、必要なタイムゾーンで少なくとも 1 つのゲスト ロケーションを作成します。

（注） ゲスト アクセスの時間は、ゲスト ロケーションのタイム ゾーンに基づきます。ゲスト ロケーションのタイム ゾーンがシステムのタイム ゾーンと一致しないと、ゲスト ユーザはログインできなくなることがあります。この場合、ゲスト ユーザには「認証に失敗しました（Authentication Failed）」エラーが表示されることがあります。デバッグ レポートに「ゲストのアクティブ時間はまだ開始していません（Guest active time period not yet started）」というエラー メッセージが表示されることがあります。回避策として、[アカウントの管理（Manage Accounts）] オプションを使用して、ゲスト ユーザのローカル タイム ゾーンに一致するようにゲストのアクセス開始時刻を調整できます。

ここで追加する SSID はスポンサー ポータルで使用できるため、スポンサーは接続する SSID をゲストに伝えることができます。

ゲスト ロケーションまたは SSID がスポンサー ポータルで設定されている場合、またはゲスト アカウントに割り当てられている場合は、削除できません。

ステップ 1 ゲスト ポータルおよびスポンサー ポータルのゲスト ロケーションと SSID を追加、編集、または削除するには、**[ワーク センター（Work Centers）] > [ポータルとコンポーネント（Portals & Components）] > [設定（Settings）] > [ゲスト ロケーションおよび SSID（Guest Locations and SSIDs）]** を選択します。

ステップ 2 [ゲスト ロケーション（Guest Locations）]：

a) サポートが必要な各タイムゾーンに対し、[ロケーション名（Location name）] に入力し、ドロップダウン リストから [タイムゾーン（Time zone）] を選択します。

b) [追加（Add）] をクリックします。

（注） ゲスト ロケーションでは、場所の名前、タイム ゾーンの名前、および GMT オフセットはスタティックであり、これらを変更できません。GMT オフセットは夏時間の変更によって変更されません。GMT オフセットは、リストに表示されているオフセットとは逆です。たとえば、*Etc/GMT+3* は実際には GMT-3 です。

（注） 初回ログインのゲスト タイプの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト タイプ（Guest Types）]** ページでアクセス時間制限を設定する場合にのみ、ゲスト ロケーション（タイム ゾーン）を設定することを確認してください。

ステップ 3 [ゲスト SSID（Guest SSIDs）]：

a) ゲスト ロケーションでゲストが使用できるネットワークの **SSID** 名を入力します。

b) [追加（Add）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。最後に保存した値に戻すには、[リセット（Reset）] をクリックします。

次のタスク

新しいゲスト ロケーションまたは SSID を追加すると、次のことが可能になります。

- スポンサーがゲスト アカウントを作成するときに使用できる SSID を提供します。スポンサー ポータルのポータル設定 （466 ページ）を参照してください。
- スポンサー グループにゲスト ロケーションを追加して、ゲスト アカウントの作成時にそのグループに割り当てられたスポンサーが使用できるようにします。スポンサー グループの設定 （417 ページ）を参照してください。
- アカウント登録ゲスト ポータルを使用してアカウント登録ゲストに使用可能なゲスト ロケーションを割り当てます。アカウント登録ゲスト ポータルの作成 （406 ページ）を参照してください。
- 既存のゲスト アカウントの場合は、アカウントを手動で編集して SSID またはロケーションを追加します。

ゲスト パスワード ポリシーのルール

Cisco ISE には、ゲスト ユーザ パスワードについて次の組み込みルールがあります。

- ゲスト パスワード ポリシーは、スポンサー ポータル、アカウント登録ポータル、CSV ファイルでアップロードされたアカウント、ERS API を使用して作成されたパスワード、およびユーザが作成したパスワードに適用されます。

- ゲスト パスワード ポリシーに対する変更は、ゲスト パスワードの期限が切れて変更が必要になるまで、既存のアカウントに影響しません。
- パスワードは大文字・小文字の区別をします。（Unable to authenticate using the domain name, user name, and password that you specified. Please check the values that you entered and try again. Passwords are case sensitive.）」
- 特殊文字（<、>、/、スペース、カンマ、%）を使用することはできません。
- 最小長および最小必須文字数は、すべてのパスワードに適用されます。
- パスワードとユーザ名を同じにすることはできません。
- 新規パスワードと既存パスワードを同じにすることはできません。
- ゲストアカウントの期限切れとは異なり、ゲストはパスワードが期限切れになる前に通知を受信しません。ゲストパスワードが期限切れになった場合は、スポンサーがパスワードをランダム パスワードにリセットするか、ゲストが現在のログイン クレデンシャルを使用してログインしてからパスワードを変更することができます。

（注） ゲストのデフォルトユーザ名は4文字の英字からなり、パスワードは4文字の数字からなります。短期間のゲストには、短く覚えやすいユーザ名とパスワードが適切です。必要に応じてISE でユーザ名とパスワードの長さを変更できます。

ゲスト パスワード ポリシーと有効期限の設定

すべてのゲスト ポータルのパスワード ポリシーを定義できます。ゲスト パスワード ポリシーは、すべてのゲストアカウントのパスワードの生成方法を決定します。パスワードはアルファベット、数字、特殊文字を組み合わせて作成することができます。また、ゲストパスワードが期限切れになるまでの日数を設定し、ゲストにパスワードのリセットを要求することができます。

ゲスト パスワード ポリシーは、スポンサー ポータル、アカウント登録ポータル、CSV ファイルでアップロードされたアカウント、ERS API を使用して作成されたパスワード、およびユーザが作成したパスワードに適用されます。

ステップ 1 **[ゲスト アクセス（Guest Access）] > [設定（Settings）] > [ゲスト パスワード ポリシー（Guest Password Policy）]** を選択します。

ステップ 2 ゲスト パスワードの [最小パスワード長（Minimum password length）]（文字数）を入力します。

ステップ 3 パスワードの作成にゲストが使用できる各文字セットの文字を指定します。

[許可される文字数と最小値（Allowed Characters and Minimums）] で次のいずれか 1 つのオプションを選択して、ゲスト用のパスワード ポリシーを指定します。

- 各文字セットのすべての文字を使用します。

- 特定の文字の使用を防止するには、ドロップダウン メニューから [カスタム（Custom）] を選択し、その文字を事前定義済みの完全なセットから削除します。

ステップ 4 各セットから、使用する最小文字数を入力します。

4 つの文字セットの必須文字数の合計が、全体の**最小パスワード長**を超えないようにする必要があります。

ステップ 5 [パスワードの有効期限（Password Expiration）] で、次のオプションのいずれかを選択します。

- 最初にログインしてからゲストがパスワードを変更する必要がある頻度（日数）を指定します。期限切れになる前にゲストがパスワードをリセットしないと、次回に元のログイン クレデンシャルを使用してネットワークにログインするときに、パスワードを変更するように促されます。
- パスワードを無期限に設定します。

ステップ 6 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

次のタスク

パスワード要件を提示するためのパスワード ポリシーに関連したエラー メッセージをカスタマイズする必要があります。

1. **[ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [Sponsored-Guest ポータル（Sponsored-Guest Portals）] または [アカウント登録ゲスト ポータル（Self-Registered Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [エラー メッセージ（Error Messages）]** を選択します。
2. キーワード「policy」を検索します。

ゲスト ユーザ名ポリシーのルール

Cisco ISE には、ゲスト ユーザ名ポリシーについて次の組み込みルールがあります。

- ゲスト ユーザ名ポリシーに対する変更は、ゲスト アカウントの期限が切れて変更が必要になるまで、既存のアカウントに影響しません。
- 特殊文字（<、>、/、スペース、カンマ、%）を使用することはできません。
- 最小長および最小必須文字数は、電子メール アドレスに基づいたユーザ名を含め、すべてのシステム生成ユーザ名に適用されます。
- パスワードとユーザ名を同じにすることはできません。

ゲスト ユーザ名ポリシーの設定

ゲストユーザ名の作成方法に関するルールを設定できます。生成されるユーザ名は、電子メールアドレスに基づいて、またはゲストの姓と名に基づいて作成できます。またスポンサーは、ランダムな数のゲストアカウントを作成し、複数のゲストを作成する場合、またはゲストの名

前と電子メールアドレスが利用できない場合に時間を短縮することもできます。ランダムに生成されたゲストユーザ名は、アルファベット、数字、および特殊文字の組み合わせから成ります。これらの設定は、すべてのゲストに影響します。

ステップ 1 すべてのゲスト ポータルとスポンサー ポータルのゲスト ユーザ名ポリシーを定義するには、**[ワーク センター（Work Centers）] > [ポータルとコンポーネント（Portals & Components）] > [設定（Settings）] > [ゲスト ユーザ名ポリシー（Guest Username Policy）]** の順に選択します。

ステップ 2 ゲスト ユーザ名の [ユーザ名の最小長（Minimum username length）]（文字数）を入力します。

ステップ 3 [既知のゲストのユーザ名基準（Username Criteria for Known Guests）] で次のいずれか 1 つのオプションを選択して、既知のゲストのユーザ名を作成するためのポリシーを指定します。

ステップ 4 [ランダムに生成されるユーザ名で使用できる文字（Characters Allowed in Randomly-Generated Usernames）] で次のいずれか 1 つのオプションを選択して、ゲストのランダム ユーザ名を作成するためのポリシーを指定します。

- 各文字セットのすべての文字を使用します。
- 特定の文字の使用を防止するには、ドロップダウン メニューから [カスタム（Custom）] を選択し、その文字を事前定義済みの完全なセットから削除します。

ステップ 5 各セットから、使用する最小文字数を入力します。

3 つの文字セットからの合計文字数は、[ユーザ名の最小長（Minimum username length）] に指定されている数を超えないようにする必要があります。

ステップ 6 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

次のタスク

ユーザ名要件を提示するためのユーザ名ポリシーに関連したエラー メッセージをカスタマイズする必要があります。

1. **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [Sponsored-Guest ポータル（Sponsored-Guest Portal）]、[アカウント登録ゲスト ポータル（Self-Registered Guest Portals）]、[スポンサー ポータル（Sponsor Portals）]、または [デバイス ポータル（My Devices Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [エラー メッセージ（Error Messages）]** の順に選択します。
2. キーワード「policy」を検索します。

SMS プロバイダーおよびサービス

SMS サービスは、クレデンシャルを持つゲスト ポータルを使用しているゲストに SMS 通知を送信します。SMS メッセージを送信する予定がある場合は、このサービスを有効にします。。可能な限り、会社の経費を削減するために、無料の SMS サービス プロバイダーを設定および提供します。

Cisco ISE は、加入者に無料の SMS サービスを提供するさまざまなセルラー サービス プロバイダーをサポートします。Cisco ISE でサービス契約とアカウント クレデンシャルを設定せずに、これらのプロバイダーを使用できます。セルラー サービス プロバイダーには、ATT、Orange、Sprint、T-Mobile、Verizon などがあります。

また、無料の SMS サービスを提供するその他のセルラー サービス プロバイダー、または Click-A-Tell などのグローバル SMS サービス プロバイダーも追加できます。デフォルトのグローバル SMS サービス プロバイダーには、サービス契約が必要です。また、Cisco ISE のアカウント クレデンシャルを設定する必要があります。

- アカウント登録ゲストがアカウント登録フォームで無料 SMS サービス プロバイダーを選択すると、SMS 通知がログイン クレデンシャルとともに無料で送信されます。SMS サービスプロバイダーを選択しない場合は、会社が契約したデフォルトのグローバル SMS サービス プロバイダーが SMS 通知を送信します。
- 自分が作成したゲスト アカウントに対してスポンサーが SMS 通知を送信できるようにする場合は、スポンサー ポータルをカスタマイズして、使用できる適切な SMS サービス プロバイダーをすべて選択します。スポンサー ポータル用の SMS サービス プロバイダーを選択しない場合は、会社が契約したデフォルトのグローバル SMS サービス プロバイダーが SMS サービスを提供します。

SMS プロバイダーは、ISE の SMS ゲートウェイとして設定されます。ISE からの電子メールは SMS ゲートウェイにより SMS に変換されます。SMS ゲートウェイはプロキシ サーバの背後に配置できます。

関連トピック

ゲストに SMS 通知を送信するための SMS ゲートウェイの設定 （386 ページ）
SMS ゲートウェイ設定（SMS Gateway Settings） （1402 ページ）

ゲストに SMS 通知を送信するための SMS ゲートウェイの設定

次のことができるようにするには、Cisco ISE で SMS ゲートウェイを設定する必要があります。

- ログイン クレデンシャルおよびパスワード リセット手順に関する SMS 通知をスポンサーがゲストに手動で送信します。
- ゲストが、自分自身の登録に成功した後、自分のログイン資格情報が含まれた SMS 通知を自動的に受信します。
- ゲスト アカウントの期限が切れる前に実行するアクションに関する SMS 通知をゲストが自動的に受信します。

情報をフィールドに入力するときは、[USERNAME]、[PASSWORD]、[PROVIDER_ID] など、[ ] 内のすべてのテキストを、SMS プロバイダーのアカウントに固有の情報で更新する必要があります。

始める前に

[SMS 電子メール ゲートウェイ（SMS Email Gateway）] オプションに使用するデフォルト SMTP サーバを設定します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMS ゲートウェイ（SMS Gateway）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 次の表を使用して、SMS ゲートウェイを設定します。

表 *37 : SMS* 電子メール ゲートウェイの *SMS* ゲートウェイ設定

フィールド	使用上のガイドライン
SMS ゲートウェイ プロバイダー ドメイン（SMS Gateway Provider Domain）	プロバイダー ドメインと、ゲスト アカウントの携帯電話の番号を入力します。プロバイダーの SMS/MMS ゲートウェイにメッセージを送信するとき、前者が電子メールアドレスのホスト部として使用され、後者はユーザ部分として使用されます。
プロバイダーアカウントアドレス（Provider account address）	（オプション） アカウント アドレスを入力します。これは、電子メールの送信元アドレス（通常、アカウントアドレス）として使用され、**[ゲスト アクセス（Guest Access）] > [設定（Settings）]** の [デフォルトの電子メール アドレス（Default Email Address）] グローバル設定を上書きします。
SMTP API 宛先アドレス（SMTP API destination address）	（オプション） Clickatell SMTP API などの、特定のアカウント受信者アドレスを必要とする SMTP SMS API を使用する場合は、SMTP API 宛先アドレスを入力します。 これは、電子メールの送信先アドレスとして使用され、メッセージ本文のテンプレートはゲストアカウントの携帯電話の番号に置き換えられます。

フィールド	使用上のガイドライン
SMTP API 本文テンプレート（SMTP API body template）	（オプション） Clicketell SMTP API など、SMS の送信に特定の電子メール本文テンプレートを必要とする SMTP SMS API を使用する場合は、SMTP API 本文テンプレートを入力します。 サポートされる動的置換は $mobilenumber$、（形式 $YYYYMMDDHHHMISSmimi$ の）$timestamp$、および $message$ です。 URL に固有識別子が必要な SMS ゲートウェイには $timestamp$$mobilenumber$ を使用できます。

これらの設定へのナビゲーション パスは、**[ゲスト アクセス（Guest Access）]** > **[設定（Settings）]** > **[SMS ゲートウェイ（SMS Gateway）]** です。

HTTP API（GET 方式または POST 方式）でゲストとスポンサーに SMS メッセージを送信するように設定するには、次の設定を使用します。

表 *38 : SMS HTTP API* 用の *SMS* ゲートウェイ設定（*SMS Gateway Settings for SMS HTTP API*）

フィールド	使用上のガイドライン
URL	API の URL を入力します。 このフィールドは、符号化された URL ではありません。ゲストアカウントの携帯電話の番号は、URL に置き換えられます。サポートされる動的置換は $mobilenumber$ および $message$ です。 HTTP API で HTTPS を使用した場合、HTTPS を URL 文字列に含め、Cisco ISE にプロバイダーの信頼できる証明書をアップロードします。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。
データ（URL エンコード部分）（Data (Url encoded portion)）	GET 要求または POST 要求のデータ（URL エンコード部分）を入力します。 このフィールドは、符号化された URL です。デフォルトの GET 方式を使用している場合、データが上で指定した URL に付加されます。
データ部分に HTTP POST 方式を使用（Use HTTP POST method for data portion）	POST 方式を使用する場合は、このオプションをオンにします。 上で指定したデータは、POST 要求の内容として使用されます。

フィールド	使用上のガイドライン
HTTP POST データ コンテンツ タイプ（HTTP POST data content type）	POST 方式を使用する場合は、「plain/text」や「application/xml」などのコンテンツ タイプを指定します。
HTTPS ユーザ名（HTTPS Username） HTTPS パスワード（HTTPS Password） HTTPS ホスト名（HTTPS Host name） HTTPS ポート番号（HTTPS Port number）	この情報を入力します。

ステップ 4 [長いメッセージを複数に分割する（Break up long message into multiple parts）] をオンにして、Cisco ISE で 140 バイトを超えるメッセージを複数のメッセージに分割できるようにします。

ほとんどの SMS プロバイダーは、長い SMS メッセージを自動的に複数に分割します。MMS メッセージは SMS メッセージよりも長くなる可能性があります。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

新しい SMS ゲートウェイを追加すると、次のことが可能になります。

- 期限切れのアカウントに関する SMS 通知をゲストに送信するときに、SMS サービス プロバイダーを選択します。「ゲスト タイプの作成または編集」を参照してください。
- [アカウント登録（Self-Registration）] フォームでアカウント登録ゲストに示される選択肢として、SMS プロバイダーのうちのどれを表示するかを指定します。アカウント登録ゲスト ポータルの作成 （406 ページ） を参照してください。

アカウント登録ゲストのソーシャル ログイン

ゲストは、ゲスト ポータルにユーザ名とパスワードを入力する代わりに、アカウント登録ゲストでクレデンシャルを提供する方法としてソーシャル メディア プロバイダーを選択できます。これを有効にするには、ソーシャル メディア サイトを外部 ID ソースとして設定し、ユーザがその外部 ID（ソーシャル メディア プロバイダー）を使用できるようにするポータルを設定します。ISE のソーシャル メディア ログインに関する追加情報は、こちらをご覧ください。
https://community.cisco.com/t5/security-documents/how-to-configure-amp-use-a-facebook-social-media-login-on-ise/ta-p/3609532

ソーシャル メディアで認証した後、ゲストはソーシャル メディア サイトから取得した情報を編集できます。ソーシャル メディアのクレデンシャルが使用されているにもかかわらず、ソーシャル メディア サイトは、ユーザがそのサイトの情報を使用してログインしたことを認識していません。ISE は引き続き、ソーシャル メディア サイトから取得された情報を今後の追跡のために内部的に使用します。

ユーザがソーシャル メディア サイトから取得した情報を変更しないようにゲスト ポータルを設定したり、登録フォームの表示を抑制することもできます。

ソーシャル ログイン ゲスト フロー

ログイン フローは、ポータル設定を構成する方法によって異なります。ソーシャル メディアのログインは、ユーザ登録なし、ユーザ登録あり、またはユーザ登録とスポンサー承認ありで設定できます。

1. ユーザはアカウント登録ポータルに接続し、ソーシャルメディアを使用してログインすることを選択します。アクセス コードを設定した場合、ユーザはログイン ページにアクセス コードも入力する必要があります。
2. ユーザは認証のためにソーシャル メディア サイトにリダイレクトされます。ユーザは、ソーシャル メディア サイトの基本的なプロファイル情報の使用を承認する必要があります。
3. ソーシャル メディア サイトへのログインが成功すると、ISE はユーザに関する追加情報をソーシャル メディア サイトから取得します。ISE はソーシャル メディア情報を使用してユーザをログオンします。
4. ログイン後、設定に応じて、ユーザは AUP を受け入れなくてはならない場合があります。
5. ログイン フローの次のアクションは設定によって異なります。
   - 登録なし：登録は裏側で行われます。Facebook はログイン用にユーザのデバイスのトークンを ISE に提供します。
   - 登録あり：ユーザには、ソーシャル メディア プロバイダーからの情報が事前に入力された登録フォームを完了するよう指示されます。これにより、ユーザは不足している情報を修正および追加し、ログインのために更新された情報を提出することができます。登録フォームの設定で登録コードを設定した場合は、登録コードも入力する必要があります。
   - 登録およびスポンサー承認あり：ユーザにソーシャルメディア提供の情報を更新させることに加えて、ユーザはスポンサーの承認を待たなければならないという通知を受けます。スポンサーは、アカウントの承認または拒否を要求する電子メールを受け取ります。スポンサーがアカウントを承認すると、ISE はユーザにアクセス権を電子メール送信します。ユーザはゲスト ポータルに接続し、ソーシャル メディア トークンで自動的にログインします。
6. 登録が成功します。ユーザは、アカウント自己登録用のゲスト フォームを送信した後、登録フォームの設定に誘導されます。ユーザのアカウントは、ポータルのゲスト タイプ用に設定されたエンドポイント ID グループに追加されます。
7. ゲスト アカウントが期限切れになるか、またはユーザがネットワークから切断するまで、ユーザはアクセス権を持ちます。

アカウントの有効期限が切れた場合、ユーザのログインを許可する唯一の方法は、アカウントを再アクティブ化することです（そうでない場合は、アカウントを削除します）。ユーザはログイン フローを再度実行する必要があります。

ユーザがネットワークから切断して再接続した場合、ISE の処理は許可ルールによって異なります。ユーザが次のような認証を取得した場合：

```
rule if guestendpoint then permit access
```

ユーザがエンドポイント グループにまだ存在する場合、ユーザはログオン ページにリダイレクトされます。ユーザがまだ有効なトークンを持っている場合は、自動的にログインします。持っていない場合は、登録をやり直す必要があります。

ユーザがもはやエンドポイント グループに属していない場合、ユーザはゲスト ページにリダイレクトされ、登録をやり直します。

ソーシャル ログイン アカウントの期間

アカウント再認証は接続方法によって異なります。

- 802.1x の場合、デフォルトの許可ルールでは、

  ```
  if guestendpoint then permit access
  ```

  デバイスがスリープ状態になった場合、または別の建物にローミングした場合に、ゲストが再接続できるようにします。再接続すると、ゲストページにリダイレクトされ、トークンを使用して自動ログインするか、または再度登録を開始します。

- MAB では、ユーザは再接続するたびにゲスト ポータルにリダイレクトされ、ソーシャル メディアを再度クリックする必要があります。ISE にそのユーザのアカウントのトークン（ゲスト アカウントの有効期限が切れていない）がまだある場合は、ソーシャル メディア プロバイダーに接続する必要はなく、ログインが即座に成功します。

  すべての再接続が別のソーシャル ログインにリダイレクトされないようにするには、デバイスを記憶し、アカウントが期限切れになるまでアクセスを許可する許可ルールを設定できます。アカウントが期限切れになると、そのアカウントはエンドポイント グループから削除され、フローはゲスト リダイレクトのルールにリダイレクトされます。次に例を示します。

  ```
  if wireless_mab and guest endpoint then permit access
  ```

  ```
  if wireless_mab then redirect to self-registration social media portal
  ```

レポートとユーザ トラッキング

ISE ライブ ログと Facebook

- **認証 ID ストア**：ISE のソーシャル メディア アプリで作成したアプリケーションの名前です。
- **Facebook のユーザ名**：Facebook によって報告されたユーザ名です。ユーザが登録時にユーザ名を変更できるようにする場合、ISE によって報告される名前はソーシャル メディアのユーザ名です。

- **SocialMediaIdentifier**：ここでの

  `https://facebook.com/<number>`

  number はソーシャル メディア ユーザを識別します。

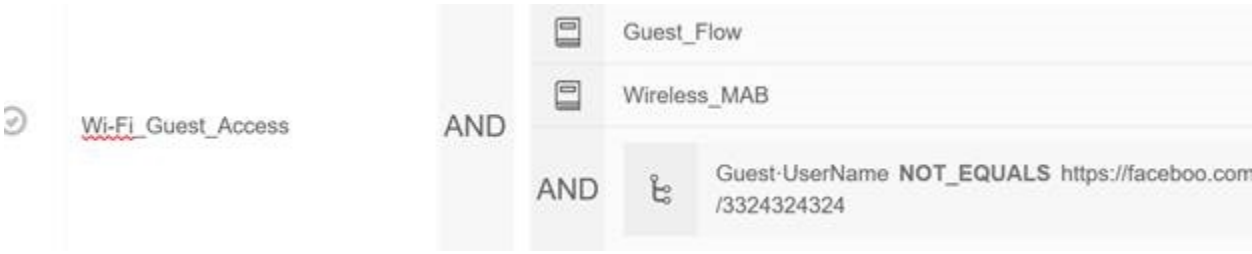
ISE レポート：ゲスト ユーザ名は、ソーシャル メディア サイトのユーザ名です。

Facebook 分析：Facebook の分析を使用して、Facebook のソーシャル ログオンを通じてゲスト ネットワークを使用しているユーザを確認することができます。

ワイヤレスと Facebook：ワイヤレス コントローラの [ユーザ名（User Name）] は、ライブ ログの **SocialMediaIdentifier** と同じ一意の Facebook ID です。ワイヤレス UI の設定を表示するには、**[モニタ（Monitor）]** > **[クライアント（Clients）]** > **[詳細（Detail）]** に移動し、[ユーザ名（User Name）] フィールドを確認します。

ソーシャル メディアで認証されたゲストのブロック

個々のソーシャル メディア ユーザをブロックする許可ルールを作成することができます。これは、トークンが期限切れになっていない場合に Facebook を認証に使用する際に便利です。次の例は、Facebook ユーザ名を使用してブロックされた Wi-Fi 接続のゲスト ユーザを示します。



ISE のソーシャル ログインの設定については、ソーシャル ログインの設定（392 ページ） を参照してください。

ソーシャル ログインの設定

始める前に

ISE が接続できるようにソーシャル メディア サイトを設定します。現在は Facebook のみがサポートされています。

ISE が Facebook にアクセスできるように、次の HTTPS 443 URL が NAD を介して開かれていることを確認します。

```
facebook.co
akamaihd.net
akamai.co
fbcdn.net
```

（注） Facebook のソーシャル ログイン URL は HTTPS です。すべての NAD が HTTPS URL へのリダイレクションをサポートしているわけではありません。https://communities.cisco.com/thread/79494?start=0&tstart=0&mobileredirect=trueを参照してください。

ステップ 1 Facebook で、Facebook アプリケーションを作成します。

a) https://developers.facebook.com にログオンし、開発者としてサインアップします。

b) ヘッダーで [アプリ（Apps）] を選択し、[新しいアプリの追加（Add a New App）] を選択します。

ステップ 2 タイプが [Web] の新しい [製品（Product）]、[Facebook ログイン（Facebook Login）] を追加します。[設定（Settings）] をクリックして、以下を設定します。

- [クライアント OAuth ログイン（Client OAuth Login）] : [いいえ（NO）]
- [Web OAuth ログイン（Web OAuth Login）] : [はい（YES）]
- [Web OAuth の再認証を強制（Force Web OAuth Reauthentication）] : [いいえ（NO）]
- [組み込みブラウザ OAuth ログイン（Embedded Browser OAuth Login）] : [いいえ（NO）]
- [有効な OAuth リダイレクト URI（Valid OAuth redirect URIs）] : ISE から自動リダイレクト URL を追加します
- [デバイスからログイン（Login from Devices）] : [いいえ（NO）]

a) **Save**

ステップ 3 [アプリ レビュー（App Review）]をクリックして、[アプリは現在実行中でパブリックで利用可能です（Your app is currently live and available to the public）] で [はい（Yes）] を選択します。

ステップ 4 ISE で、**[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[ソーシャル ログイン（Social Login）]** に移動して、[追加（Add）] をクリックして、新しいソーシャル ログインの外部 ID ソースを作成します。

- [タイプ（Type）] : ソーシャル ログイン プロバイダーのタイプを選択します。Facebook が現在のところ唯一の選択肢です。
- [アプリ ID（App ID）] : Facebook アプリケーションからアプリ ID を入力します。
- [アプリ秘密（App Secret）] : Facebook アプリケーションからアプリ秘密を入力します。

ステップ 5 ISE で、アカウント登録ポータルでのソーシャル メディアのログインを有効にします。ポータル ページで、**[ポータルおよびページの設定（Portal & Page Settings）]** > **[ログイン ページの設定（Login Page Settings）]** に移動して、[ソーシャル ログインを許可（Allow Social Login）] をオンにします。すると、さらに多くの設定が表示されます。

- [ソーシャル ログイン後に登録フォームを表示（Show registration form after social login）] : これにより、ユーザは Facebook によって提供される情報を変更できます。

- [ゲストの承認が必要（Require guests to be approved）]：スポンサーがアカウントを承認する必要があることをユーザに通知し、ログイン用のクレデンシャルを送信します。

ステップ 6 **[管理（Administration）]** > **[外部 ID ソース（External Identity Sources）]** に移動し、[Facebook ログイン（Facebook Login）] ページを選択し、Facebook の外部 ID ソースを編集します。
これによりリダイレクト URI が作成され、これを Facebook アプリケーションに追加します。

ステップ 7 Facebook で、前のステップの URI を Facebook アプリケーションに追加します。

次のタスク

Facebook では、アプリに関するデータを表示できます。このデータには、Facebook ソーシャル ログインでのゲスト アクティビティが表示されます。

ゲスト ポータル

企業の訪問者が企業のネットワークを使用してインターネットまたはネットワーク上のリソースおよびサービスにアクセスしようとしている場合、ゲスト ポータルを使用してネットワーク アクセスを提供することができます。設定すると、従業員はゲスト ポータルを使用して会社のネットワークにアクセスできます。

3 つのデフォルトのゲスト ポータルがあります。

- ホットスポット ゲスト ポータル：ネットワーク アクセスはクレデンシャルを必要とせずに許可されます。通常、ネットワーク アクセスを許可する前にユーザ ポリシーの認可（AUP）が承認される必要があります。
- Sponsored-Guest ポータル：ゲストのアカウントを作成したスポンサーによりネットワーク アクセスが許可され、ゲストにログイン クレデンシャルが提供されます。
- アカウント登録ゲスト ポータル：ゲストは各自のアカウント クレデンシャルを作成できます。ネットワーク アクセスが付与される前に、スポンサー承認が必要となることがあります。

Cisco ISE は、事前に定義されたデフォルト ポータルなど、複数のゲスト ポータルをホストすることができます。

デフォルトのポータル テーマには、管理者ポータルからカスタマイズできる標準のシスコ ブランドが適用されています。

Wireless Setup には独自のデフォルト テーマ（CSS）があります。ロゴ、バナー、背景画像、色、フォントなどの基本的な設定の一部を変更できます。ISE では、他の設定を変更することでポータルをさらにカスタマイズでき、高度なカスタマイズを行うこともできます。

ゲスト ポータルのクレデンシャル

Cisco ISE では、ゲストにさまざまなタイプのクレデンシャルを使用したログインを要求することによって、保護されたネットワーク アクセスを提供します。ゲストがこれらのクレデンシャルの 1 つまたは組み合わせを使用してログインすることを要求できます。

- ユーザ名：必須。エンドユーザ ポータル（ホットスポット ゲスト ポータルを除く）を使用するすべてのゲストに適用され、ユーザ名ポリシーから取得されます。ユーザ名ポリシーはシステムによって生成されたユーザ名のみに適用され、ゲスト API プログラミング インターフェイスまたはアカウント登録プロセスを使用して指定されたユーザ名には適用されません。**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Settings）] > [ゲスト ユーザ名ポリシー（Guest Username Policy）]** で、ユーザ名に適用するポリシーを設定できます。ゲストは、電子メール、SMS、または印刷形式で、ユーザ名の通知を受け取ることができます。

- パスワード：必須。エンドユーザ ポータル（ホットスポット ゲスト ポータルを除く）を使用するすべてのゲストに適用され、パスワード ポリシーから取得されます。**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Settings）] > [ゲスト パスワード ポリシー（Guest Password Policy）]** で、パスワードに適用するポリシーを設定できます。ゲストは、電子メール、SMS、または印刷形式で、パスワードの通知を受け取ることができます。

- アクセス コード：オプション。ホットスポット ゲスト ポータルおよびクレデンシャルを持つゲスト ポータルを使用するゲストに適用されます。アクセス コードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです（ホワイトボードによって視覚的に、またはロビーアンバサダーにより口頭で）。ネットワークにアクセスするために、屋外にいる誰かに知られたり使用されたりすることはありません。アクセス コードの設定を有効にした場合、次のようになります。

  - スポンサー付きゲストは、[ログイン（Login）] ページで（ユーザ名およびパスワードとともに）これを入力するよう求められます。

  - ホットスポット ゲスト ポータルを使用するゲストは、[利用規定（Acceptable Use Policy (AUP)）] ページでこれを入力するよう求められます。

- 登録コード：オプション。アカウント登録ゲストに適用され、アカウント登録ゲストに提供される方法においてアクセス コードと似ています。登録コード設定が有効な場合、アカウント登録ゲストはアカウント登録フォームでこれを入力するよう求められます。

ユーザ名とパスワードは、社内のスポンサーが（スポンサー付きゲストに対して）提供できます。または、ゲストが自分自身を登録してこれらのクレデンシャルを取得できるように、クレデンシャルを持つゲスト ポータルを設定できます。

関連トピック

ユーザ認証ポリシーの設定

ゲスト タイプおよびユーザ ID グループ （371 ページ）

ホットスポット ゲスト ポータルを使用したゲスト アクセス

Cisco ISE にはネットワーク アクセス機能があり、その機能には「ホットスポット」が含まれています。これは、アクセスポイントで、ゲストはこれを使用してログインにクレデンシャルを必要とすることなくインターネットにアクセスできます。ゲストがコンピュータまたはWebブラウザを搭載した任意のデバイスでホットスポット ネットワークに接続して、Web サイトに接続しようとすると、自動的にホットスポット ゲスト ポータルにリダイレクトされます。この機能では、有線接続と無線接続（Wi-Fi）の両方がサポートされます。

ホットスポット ゲスト ポータルは代替となるゲスト ポータルで、これを使用すると、ゲストにユーザ名とパスワードを要求することなく、ネットワーク アクセスを提供することができ、ゲストアカウントを管理する必要性が軽減されます。代わりに、ゲストデバイスにネットワーク アクセスを直接提供するために、Cisco ISE はネットワーク アクセス デバイス（NAD）およびデバイス登録 Web 認証（デバイス登録 WebAuth）とともに動作します。場合によって、ゲストは、アクセス コードを使用してログインするよう要求されることがあります。通常、これは社内に物理的に存在しているゲストにローカルに提供されるコードです。

ホットスポット ゲスト ポータルをサポートしている場合：

- ホットスポット ゲスト ポータルの設定に基づいて、ゲスト アクセスの条件を満たしている場合、ゲストにネットワーク アクセスが付与されます。
- Cisco ISE によってデフォルトのゲスト ID グループ GuestEndpoints が提供され、これを使用して、ゲスト デバイスを一元的に追跡できます。

クレデンシャルを持つゲスト ポータルを使用したゲスト アクセス

クレデンシャルを持つゲストポータルを使用して、外部ユーザの内部ネットワークおよびサービスと、インターネットへの一時アクセスを識別し許可することができます。スポンサーは、ポータルの [ログイン（Login）] ページでこれらのクレデンシャルを入力することによって、ネットワークにアクセスできる承認ユーザの一時的なユーザ名およびパスワードを作成できます。

次のように取得したユーザ名とパスワードを使用してゲストがログインできるように、クレデンシャルを持つゲスト ポータルを設定できます。

- スポンサーから付与されます。このゲストフローでは、ゲストは、社内に入って個人のゲスト アカウントで設定されたとき、ロビー アンバサダーなどのスポンサーによるグリーティングを受け取ります。
- オプションの登録コードまたはアクセス コードを使用して自分自身を登録した後に付与されます。このゲストフローでは、ゲストは人間の介入なしでインターネットにアクセスでき、これらのゲストにコンプライアンスに使用可能な一意の識別子があることが Cisco ISE によって保証されます。
- オプションの登録コードまたはアクセス コードを使用して自分自身を登録した後に付与されます。ただし、ゲストアカウントの要求がスポンサーによって承認された後のみです。

このゲストフローでは、ゲストにネットワークへのアクセスが提供されますが、追加のスクリーニング レベルが実行された後でのみ提供されます。

また、ログイン時にユーザに新しいパスワードを入力するよう強制できます。

Cisco ISE では、複数のクレデンシャルを持つゲスト ポータルを作成し、これを使用してさまざまな基準に基づいてゲストアクセスを許可することができます。たとえば、日次訪問者に使用されるポータルとは別の、月次担当者向けのポータルを設定できます。

クレデンシャルを持つゲスト ポータルを使用した従業員アクセス

従業員は、そのポータルに設定された ID ソース順序でクレデンシャルにアクセスできれば、従業員クレデンシャルを使用してサインインすることによって、クレデンシャルを持つゲストポータルを使用してネットワークにアクセスすることもできます。

ゲスト デバイスのコンプライアンス

ゲストおよび非ゲストがクレデンシャルを持つゲストポータルを介してネットワークにアクセスした場合、アクセスを許可する前に、そのデバイスのコンプライアンスをチェックすることができます。ゲストおよび非ゲストを [クライアント プロビジョニング（Client Provisioning）] ページにルーティングして、最初にポスチャ エージェントをダウンロードするよう要求することができます。このエージェントは、ポスチャ プロファイルをチェックし、デバイスが準拠しているかどうかを検証します。これは、クレデンシャルを持つゲスト ポータルで、[ゲスト デバイスのコンプライアンス設定（Guest Device Compliance Settings）] のオプションを有効にすることで実行できます。これによって、[クライアント プロビジョニング（Client Provisioning）] ページがゲスト フローの一部として表示されます。

クライアント プロビジョニング サービスでは、ゲストのポスチャ評価および修復が提供されます。クライアント プロビジョニング ポータルは、中央 Web 認証（CWA）のゲスト展開でのみ使用できます。ゲスト ログイン フローによって CWA が実行され、クレデンシャルを持つゲスト ポータルは、利用規定やパスワード変更のチェックを実行した後、クライアント プロビジョニング ポータルにリダイレクトされます。いったんポスチャが評価されると、ポスチャ サブシステムはネットワーク アクセス デバイスに対して許可変更（CoA）を実行し、クライアント再接続を再認証します。

ゲスト ポータルの設定タスク

デフォルト ポータルと、証明書、エンドポイント ID グループ、ID ソース順序、ポータル テーマ、イメージ、および Cisco ISE によって提供されるその他の詳細などのデフォルト設定を使用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

新しいポータルを作成したり、デフォルト ポータルを編集した後は、ポータルの使用を承認する必要があります。いったんポータルの使用を承認すると、後続の設定変更はただちに有効になります。

ポータルを削除する場合は、関連付けられている許可ポリシールールおよび許可プロファイルを先に削除するか、別のポータルを使用するように変更する必要があります。

さまざまなゲストポータルの設定に関連するタスクについては、この表を参照してください。

タスク	ホットスポットゲストポータル	Sponsored-Guest ポータル	アカウント登録ゲストポータル
ポリシーサービスの有効化 （399 ページ）	必須（Required）	必須（Required）	必須（Required）
ゲストポータルの証明書の追加 （399 ページ）	必須（Required）	必須（Required）	必須（Required）
外部 ID ソースの作成（399 ページ）	N/A	必須（Required）	必須（Required）
ID ソース順序の作成（401 ページ）	N/A	必須（Required）	必須（Required）
エンドポイント ID グループの作成 （825 ページ） エンドポイント ID グループの作成（『』の「エンドポイント ID グループの作成」のセクションを参照してください）	必須（Required）	不要（ゲストタイプによって定義される）	不要（ゲストタイプによって定義される）
ホットスポットゲストポータルの作成 （402 ページ）	必須（Required）	N/A	N/A
Sponsored-Guest ポータルの作成 （404 ページ）	N/A	必須（Required）	N/A
アカウント登録ゲストポータルの作成 （406 ページ）	N/A	N/A	必須（Required）
ポータルの許可 （411 ページ）	必須（Required）	必須（Required）	必須（Required）
ゲストポータルのカスタマイズ （412 ページ）	オプション	オプション	オプション

ポリシー サービスの有効化

Cisco ISE エンドユーザ Web ポータルをサポートするには、ホストするノードでポータル ポリシー サービスを有効にする必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。
ステップ 2 ノードをクリックして、[編集（Edit）] をクリックします。
ステップ 3 [全般設定（General Settings）] タブで、[ポリシー サービス（Policy Service）] をオンにします。
ステップ 4 [セッション サービスの有効化（Enable Session Services）] オプションをオンにします。
ステップ 5 [**保存（Save）**] をクリックします。

ゲスト ポータルの証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループ タグに割り当てることができます。すべてのエンドユーザ Web ポータルに使用されるデフォルトの証明書グループ タグは [デフォルト ポータル証明書グループ（Default Portal Certificate Group）] です。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。
ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。
この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。
ステップ 3 **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成または編集（Create or Edit）] > [ポータル設定（Portal Settings）]** の順に選択します。
ステップ 4 新しく追加された証明書に関連付けられた [証明書グループ タグ（Certificate group tag）] ドロップダウン リストから特定の証明書グループ タグを選択します。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバなどの外部 ID ソースに接続して、認証/許可のユーザ情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザ ID を受信して共有できるようにするパッシブ ID サービスを使用するには、を参照してくださいその他の パッシブ ID サービス プロバイダー （647 ページ）。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。
- Active Directory：外部 ID ソースである Active Directory に接続する場合。外部 ID ソースとしての Active Directory （587 ページ）を参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、LDAP （696 ページ）を参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバを追加する場合。詳細については、RADIUS トークン ID ソース （722 ページ）を参照してください。
- RSA SecurID：RSA SecurID サーバを追加する場合。詳細については、RSA ID ソース （730 ページ）を参照してください。
- SAML IDプロバイダー（SAML Id Providers）：Oracle Access Manager などの ID プロバイダー（IdP）を追加する場合。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダ （738 ページ）を参照してください。
- **ソーシャル ログイン**：Facebook などのソーシャル ログインを外部 ID ソースとして追加する場合。アカウント登録ゲストのソーシャル ログイン （389 ページ）を参照してください。

認証用の SAML IDP ポータルにリダイレクトするためのゲスト ポータルの設定

ゲスト ポータルを設定して、ユーザが認証のために SAML IDP ポータルにリダイレクトされるようにすることができます。

ゲスト ポータルで [ログインに次の ID プロバイダ ゲスト ポータルの使用を許可（Allow the following identity-provider guest portal to be used for login）] を設定することで、そのポータルで新しいログインエリアが有効になります。ユーザがそのログインオプションを選択した場合、代替 ID ポータルにリダイレクトされてから（表示されません）、認証のために SAML IDP ログオン ポータルにリダイレクトされます。

たとえば、ゲスト ポータルには従業員ログインのためのリンクがある場合があります。既存のポータルにログインする代わりに、ユーザは従業員ログオン リンクをクリックし、SAML IDP シングル サインオン ポータルにリダイレクトされます。従業員はこの SAML IDP による最後のログオンからのトークンを使用して再接続されるか、その SAML サイトでログインします。これにより、同じポータルでシングル SSID からゲストと従業員の両方を扱うことができます。

次の手順は、SAML IDP を認証用に使用するように設定されている別のポータルを呼び出すゲスト ポータルを設定する方法を示しています。

ステップ 1 外部 ID ソースを設定します。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダ （738 ページ）を参照してください。

ステップ 2 SAML プロバイダーのゲスト ポータルを作成します。ポータル設定で [認証方式（Authentication method）] を SAML プロバイダーに設定します。ユーザにはこのポータルは表示されず、これは単にユーザを SAML

IDP ログオン ページにつなぐためのプレースホルダです。次に説明するように、他のポータルをこのサブポータルにリダイレクトするように設定できます。

ステップ 3 作成したばかりの SAML プロバイダー ポータルのゲスト ポータルにリダイレクトするためのオプションを備えたゲスト ポータルを作成します。これはメイン ポータルで、サブポータルにリダイレクトします。

SAML プロバイダーに見えるように、このポータルの外観をカスタマイズする場合もあります。

a) メイン ポータルの [ログイン ページの設定（Login Page Settings）] で、[ログインに次の ID プロバイダ ゲスト ポータルの使用を許可（Allow the following identity-provider guest portal to be used for login）] にマークを付けます。
b) SAML プロバイダーと使用するために設定したゲスト ポータルを選択します。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲスト ユーザがローカル WebAuth を使用して認証できるようにするには、ゲスト ポータル認証ソースと ID ソース順序に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）]** を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストのデータベースを並べ替えます。

ステップ 6 [高度な検索リスト（Advanced Search List）] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

  Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストに、Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイント ID グループ（Endpoint Identity Groups）] ページで追加のエンドポイント ID グループを作成することもできます。作成したエンドポイント ID グループを編集または削除できます。システム定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集したり、これらのグループを削除したりすることはできません。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するエンドポイント ID グループの名前を入力します（エンドポイント ID グループの名前にスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの説明を入力します。

ステップ 5 [親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

ホットスポット ゲスト ポータルの作成

ホットスポット ゲスト ポータルを提供して、ゲストが、ログインにユーザ名とパスワードを要求されずにネットワークに接続できるようにすることができます。ログイン時にアクセス コードが必要な場合があります。

新しいホットスポット ゲスト ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのホットスポット ゲスト ポータルを削除できます。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、ゲスト フロー図のグラフィカル フローに反映されます。AUP ページなどのページを有効にすると、そのページがフローに表示され、ゲストはポータルで使用できるようになります。無効にすると、フローから削除され、次に有効なページがゲストに表示されます。

[認証成功の設定（Authentication Success Settings）] を除くすべてのページ設定は、任意です。

始める前に

- このポータルで使用するために、必要な証明書とエンドポイント ID グループが設定されていることを確認します。
- ゲストがホットスポット ポータルのために接続する WLC が ISE でサポートされていることを確認します。お使いのバージョンの ISE の『Identity Services Engine Network Component Compatibility』ガイドを参照してください。

ステップ 1 **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）]** の順に選択します。

ステップ 2 新しいポータルを作成する場合は、[ゲスト ポータルの作成（Create Guest Portal）] ダイアログ ボックスで、ポータル タイプとして [ホットスポット ゲスト ポータル（Hotspot Guest Portal）] を選択し、[続行（Continue）] をクリックします。

ステップ 3 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 4 [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 5 [ポータルの設定（Portal Settings）] でポート、イーサネット インターフェイス、証明書グループ タグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 特定のページのそれぞれに適用される次の設定を更新してください。

- [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]：利用規定に同意することをゲストに要求します。
- [ポストログイン バナーページの設定（Post-Login Banner Page Settings）]：必要に応じて、ゲストにアクセス ステータスおよびその他の追加アクションを通知します。
- [VLAN DHCPリリースページの設定（VLAN DHCP Release Page Settings）]：ゲスト デバイスの IP アドレスをゲスト VLAN から解放し、ネットワークの他の VLAN にアクセスするように更新します。
- [認証成功の設定（Authentication Success Settings）]：認証されたゲストに対する表示内容を指定します。
- [サポート情報ページの設定（Support Information Page Settings）]：ネットワーク アクセスの問題のトラブルシューティングのためにヘルプ デスクによって使用される情報をゲストが提供するのを支援します。

ステップ 7 [保存（Save）] をクリックします。システム生成の URL がポータル テスト URL として表示されます。この URL を使用して、ポータルにアクセスし、テストすることができます。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

Sponsored-Guest ポータルの作成

Sponsored-Guestポータルを提供して、指定されたスポンサーがゲストにアクセスを許可できるようにすることができます。

新しい Sponsored-Guest ポータルを作成するか、既存のものを編集または複製できます。Cisco ISEによって提供されているデフォルトのポータルを含む、任意のSponsored-Guestポータルを削除できます。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、ゲストフロー図のグラフィカルフローに反映されます。AUPページなどのページを有効にすると、そのページがフローに表示され、ゲストはポータルで使用できるようになります。無効にすると、フローから削除され、次に有効なページがゲストに表示されます。

次のすべてのページ設定によって、ゲスト用の利用規定（AUP）を表示し、その同意を要求することができます。

- ログイン ページの設定（Login Page Settings）
- 利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）
- BYOD 設定（BYOD Settings）

始める前に

このポータルで使用するために、必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

ステップ 1 **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Configure）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）]** の順に選択します。

ステップ 2 新しいポータルを作成する場合は、[ゲスト ポータルの作成（Create Guest Portal）] ダイアログ ボックスで、ポータル タイプとして [Sponsored-Guest ポータル（Sponsored-Guest Portal）] を選択し、[続行（Continue）] をクリックします。

ステップ 3 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 4 [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 5 [ポータル設定（Portal Settings）] でポート、イーサネット インターフェイス、証明書グループ タグ、ID ソース順序、認証方式などのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 6 特定のページのそれぞれに適用される次の設定を更新してください。

- [ログイン ページの設定（Login Page Settings）]：ゲスト クレデンシャルおよびログイン ガイドラインを指定します。[ゲストが自分のアカウントを作成することを許可する（Allow guests to create their accounts）] オプションを選択した場合、ユーザは独自のゲスト アカウントを作成できます。このオプションが選択されていない場合は、スポンサーがゲスト アカウントを作成する必要があります。

（注） [認証方式（Authentication Method）] フィールドで ID プロバイダー IdP）を選択している場合は、[ログインページ設定（Login Page Settings）] オプションは無効です。

- [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]：別の AUP ページを追加し、クレデンシャルを持つゲスト ポータルを使用する従業員を含むゲスト用の利用規定の動作を定義します。
- [従業員のパスワード変更の設定（Employee Change Password Settings）]：ゲストに、初めてログインした後にパスワードを変更するように指示します。
- [ゲスト デバイス登録の設定（Guest Device Registration Settings）]：Cisco ISE に自動的にゲスト デバイスが登録されるようにするか、またはゲストが手動でこれらのデバイスを登録できるページを表示するかどうかを選択します。
- [BYOD設定（BYOD Settings）]：従業員が自分のパーソナル デバイスを使用してネットワークにアクセスすることを許可します。
- [ポストログイン バナーページの設定（Post-Login Banner Page Settings）]：ネットワーク アクセスを許可する前にゲストに追加情報を通知します。
- [ゲスト デバイスのコンプライアンス設定（Guest Device Compliance Settings）]：ゲストを [クライアント プロビジョニング（Client Provisioning）] ページにルーティングし、最初にポスチャ エージェントをダウンロードするように要求します。
- [VLAN DHCPリリースページの設定（VLAN DHCP Release Page Settings）]：ゲスト デバイスの IP アドレスをゲスト VLAN から解放し、ネットワークの他の VLAN にアクセスするように更新します。
- [認証成功の設定（Authentication Success Settings）]：認証されたゲストに対する表示内容を指定します。
- [サポート情報ページの設定（Support Information Page Settings）]：ネットワーク アクセスの問題のトラブルシューティングのためにヘルプ デスクによって使用される情報をゲストが提供するのを支援します。

ステップ 7 [保存（Save）] をクリックします。システム生成の URL がポータル テスト URL として表示されます。この URL を使用して、ポータルにアクセスし、テストすることができます。

次のタスク

（注） テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータル フローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

アカウント登録ゲスト ポータルの作成

アカウント登録ゲストポータルを提供して、ゲストが自分自身を登録し、自分のアカウントを作成して、ネットワークにアクセスできるようにすることができます。これらのアカウントに対しては、その後も、アクセスを許可する前に、スポンサーによる承認を要求できます。

新しいアカウント登録ゲストポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのアカウント登録ゲスト ポータルを削除できます。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、ゲストフロー図のグラフィカルフローに反映されます。AUPページなどのページを有効にすると、そのページがフローに表示され、ゲストはポータルで使用できるようになります。無効にすると、フローから削除され、次に有効なページがゲストに表示されます。

次のすべてのページ設定によって、ゲスト用の利用規定（AUP）を表示し、その同意を要求することができます。

- ログイン ページの設定（Login Page Settings）
- アカウント登録ページの設定（Self-Registration Page Settings）
- アカウント登録成功ページの設定（Self-Registration Success Page Settings）
- 利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）
- BYOD 設定（BYOD Settings）

始める前に

このポータルに必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

ステップ 1 **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）]** の順に選択します。.

ステップ 2 新しいポータルを作成する場合は、[ゲスト ポータルの作成（Create Guest Portal）] ダイアログ ボックスで、ポータル タイプとして [アカウント登録ゲスト ポータル（Self-Registered Guest Portal）] を選択し、[続行（Continue）] をクリックします。

ステップ 3 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 4 [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 5 [ポータル設定（Portal Settings）] で、ポート、イーサネット インターフェイス、証明書グループ タグ、ID ソース シーケンス、認証方式、およびこのポータルの動作を定義するその他の設定のデフォルト値を更新します。

ポータル設定フィールドの詳細については、クレデンシャルを持つゲスト ポータルのポータル設定 （447 ページ）を参照してください。

ステップ 6 特定のページのそれぞれに適用される次の設定を更新してください。

- [ログイン ページの設定（Login Page Settings）]：ゲスト クレデンシャルおよびログイン ガイドラインを指定します。詳細については、クレデンシャルを持つゲスト ポータルのログイン ページ設定 （449 ページ）を参照してください。
- [アカウント登録ページの設定（Self-Registration Page Settings）]：ゲストが [アカウント登録（Self-Registration）] フォームを送信した後のゲスト エクスペリエンス以外に、アカウント登録ゲストが読み取る情報、および [アカウント登録（Self-Registration）] フォームに入力する必要がある情報を指定します。
- [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]：別の AUP ページを追加し、クレデンシャルを持つゲスト ポータルを使用する従業員を含むゲスト用の利用規定の動作を定義します。詳細については、クレデンシャルを持つゲスト ポータルの利用規定（AUP）ページ設定 （456 ページ）を参照してください。
- [従業員のパスワード変更の設定（Employee Change Password Settings）]：ゲストに、初めてログインした後にパスワードを変更するように指示します。
- [ゲスト デバイス登録の設定（Guest Device Registration Settings）]：Cisco ISE に自動的にゲスト デバイスが登録されるようにするか、またはゲストが手動でこれらのデバイスを登録できるページを表示するかどうかを選択します。
- [BYOD 設定（BYOD Settings）]：従業員が自分のパーソナル デバイスを使用してネットワークにアクセスすることを許可します。詳細については、クレデンシャルを持つゲスト ポータルの BYOD 設定（458ページ）を参照してください。詳細については、クレデンシャルを持つゲスト ポータルの BYOD 設定 （458 ページ）を参照してください。
- [ポストログイン バナー ページ設定（Post-Login Banner Page Settings）]：ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。
- [ゲスト デバイスのコンプライアンス設定（Guest Device Compliance Settings）]：ポスチャ アセスメントのためにゲストを [クライアント プロビジョニング（Client Provisioning）] ページにリダイレクトします。詳細については、クレデンシャルを持つゲスト ポータルのゲスト デバイスのコンプライアンス設定 （461 ページ）を参照してください。
- [VLAN DHCP リリースページの設定（VLAN DHCP Release Page Settings）]：ゲスト デバイスの IP アドレスをゲスト VLAN から解放し、ネットワークの他の VLAN にアクセスするように更新します。詳細については、クレデンシャルを持つゲスト ポータルの BYOD 設定 （458 ページ）を参照してください。
- 認証成功の設定（Authentication Success Settings）：認証後のゲストの宛先を指定します。認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。詳細については、ゲスト ポータルの認証成功の設定 （462 ページ）を参照してください。
- [サポート情報ページの設定（Support Information Page Settings）]：ネットワーク アクセスの問題のトラブルシューティングのためにヘルプ デスクによって使用される情報をゲストが提供するのを支援します。

ステップ 7 [保存（Save）] をクリックします。システム生成の URL がポータル テスト URL として表示されます。この URL を使用して、ポータルにアクセスし、テストすることができます。

次のタスク

（注） テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータル フローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

スポンサーによるアカウント登録のアカウントの承認

登録済みゲストがアカウントの承認を要求するように設定すると、ISE は、アカウントの承認のために電子メールを承認者に送信します。承認者は、訪問先担当者またはスポンサー ユーザのいずれかです。

承認者がスポンサーの場合、アカウントを拒否または承認するリンクを含めるように電子メールを設定できます。承認リンクには、承認をスポンサーの電子メール アドレスに関連付けるトークンが含まれています。スポンサーに認証を要求できます。これにより、トークンは無視されます。トークンはタイムアウトすることもあります。タイムアウトすると、スポンサーは、アカウントを承認する前に認証を受ける必要があります。

アカウント承認オプションは、自己登録ポータルの [登録フォームの設定（Registration Form Settings）] で設定します。この機能は、シングルクリック スポンサー承認とも呼ばれます。

スポンサーが電子メールを開いて承認リンクをクリックすると実行されるアクションは、承認者の設定に応じて異なります。

[承認要求電子メール送信先（Email approval request to）] が次のいずれかに設定されている場合について説明します。

- **[訪問先担当者（person being visited）]**
  - ゲスト アカウントに認証が不要な場合、1 回のクリックでアカウントが承認されます。
  - ゲストアカウントには認証が**必要です**。

  スポンサーポータルの特別なページがスポンサーに表示されます。このページでは、アカウントの承認前にスポンサーがクレデンシャルを入力する必要があります。
- [下に示すスポンサーの電子メールアドレス（Sponsor email addresses listed below）]：Cisco ISE は、指定されるすべての電子メールアドレスに電子メールを送信します。これらのスポンサーのいずれかが承認リンクまたは拒否リンクをクリックすると、スポンサーポータ

ルが表示されます。そのスポンサーがクレデンシャルを入力し、確認されます。スポンサーが所属するスポンサー グループで、スポンサーによるゲスト アカウントの承認が許可されている場合、スポンサーはアカウントを承認できます。クレデンシャルが失敗すると、Cisco ISE では、スポンサー ポータルにログインしてアカウントを手動で承認する指示がスポンサーに対して示されます。

説明

- 前のバージョンの Cisco ISE からデータベースをアップグレードまたは復元する場合は、承認または拒否のリンクを手動で挿入する必要があります。ゲストの承認を要求するように自己登録ポータルを設定した後、次の手順を実行します。

  アカウント登録ゲストポータルを開き、[ポータルページのカスタマイズ（Portal Page Customizations）] タブを選択します。下にスクロールして、[承認要求の電子メール（Approval Request Email）] ページを選択します。そのページの電子メール本文部分で [承認/拒否のリンクを挿入する（Insert Approve/Deny Links）] をクリックします。

- Active Directory および LDAP で認証するスポンサー ポータルのみがサポートされています。つまり、スポンサーは Active Directory または LDAP ユーザである必要があります。
- スポンサーがマッピングするスポンサー グループには、スポンサーが属する Active Directory グループが含まれている必要があります。
- [訪問先担当者（person being visited）] を選択した場合、アカウント登録ゲストがそのフィールドに入力する内容は、スポンサーの電子メールアドレスでなければなりません。アカウント登録ポータルをカスタマイズし、そのフィールド名を「スポンサーの電子メールアドレス」のような名前に変更することを推奨します。ゲストの訪問先担当者を取得するため、必要に応じて新しいフィールドを作成できます。
- スポンサーのリストがある場合、最初のポータルが、スポンサーがログインするポータルではない場合でも、最初のポータルのカスタマイズ内容が使用されます。
- スポンサーは、承認リンクと拒否リンクを使用するために、HTM 対応の電子メール クライアントを使用する必要があります。
- スポンサーの電子メールアドレスが有効なスポンサー用ではない場合、承認電子メールは送信されません。

シングルクリック スポンサーの承認の詳細については、『**ISE Single Click Sponsor ApprovalFAQ**』を参照してください。また、コミュニティドキュメントには、プロセス全体の手順を示すビデオへのリンクもあります。ビデオが実行されない場合は、別のブラウザを試してください。

アカウント承認メール リンクの設定

ネットワークにアクセスする前に、アカウント登録ゲストの承認を要求できます。Cisco ISE は、訪問先担当者の電子メールアドレスを使用して、承認者に通知します。承認者は、訪問先担当者またはスポンサーのいずれかです。承認の詳細については、スポンサーによるアカウント登録のアカウントの承認 （408 ページ）を参照してください。

ステップ 1 **[ワーク センター（Work Centers）] > [ゲスト（Guest）] > [設定（Configure）] > [ゲスト ポータル（Guest Portals）]** に移動し、メール アカウント承認リンクを設定するアカウント登録ポータルを選択します。

ステップ 2 [アカウント登録ページの設定（Self Registration Page Settings）] タブを展開します。

ステップ 3 3. [アカウント登録ゲストの承認が必要である（Require self-registered guests to be approved）] をオンにします。これにより、[承認/拒否のリンクの設定（Approve/Deny Link Settings）] セクションがタブ エリアの下部に表示されます。また、[承認要求メール（Approval Request Email）] の電子メール設定に、承認リンクと拒否リンクが取り込まれます。

[アカウント登録ページの設定（Self-Registration Page Settings）] を選択すると表示されるすべてのフィールドを以下に示します。

- [アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）]：このポータルを使用するアカウント登録ゲストは、ゲストのクレデンシャルを受信する前にスポンサーによる承認が必要であることを指定します。このオプションをクリックすると、スポンサーがアカウント登録ゲストを承認する方法に関する追加のオプションが表示されます。
  - [承認要求電子メール送信先（Email approval request to）]：次のいずれかを選択します。
    - [下に示すスポンサーの電子メールアドレス（sponsor email addresses listed below）]：承認者として指名されたスポンサーの 1 つ以上の電子メール アドレス、またはすべてのゲストの承認要求の送信先となるメール ソフトウェアを入力します。電子メールアドレスが無効な場合、承認は失敗します。
    - [訪問先担当者（person being visited）]：[スポンサーに承認用クレデンシャルの入力を求める（Require sponsor to provide credentials for authentication）] フィールドが表示され、[含めるフィールド（Fields to include）] の [必須（Required）] オプションが有効になります（以前は無効だった場合）。これらのフィールドはアカウント登録フォームに表示され、アカウント登録ゲストからこの情報を要求します。電子メール アドレスが無効な場合、承認は失敗します。
  - [承認/拒否のリンクの設定（Approve/Deny Link Settings）]：このセクションでは次の内容を設定できます。
    - [リンクの有効期間（Links are valid for）]：アカウント承認リンクの有効期間を設定できます。
    - [スポンサーに承認用クレデンシャルの入力を求める（Require sponsor to provide credentials for authentication ）]：このセクションの設定でスポンサーによるアカウント承認用のクレデンシャルの入力が必須ではない場合にも、スポンサーにこの情報を入力させるには、このフィールドをオンにします。このフィールドは、[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] が [訪問先担当者（person being visited）] に設定されている場合にだけ表示されます。
    - [承認権限を検証するためスポンサーがスポンサー ポータルと照合される（Sponsor is matched to a Sponsor Portal to verify approval privileges）]：[詳細 >（Details >）] をクリックして、スポンサーが有効なシステムユーザであり、スポンサー グループのメンバーであり、そのスポンサー グループのメンバーにアカウント承認権限があることを確認するために検索されるポータルを選択します。各スポンサー ポータルには、スポンサーを識別するために使用される ID ソース シーケンスがあります。ポータルはリストされている順序で使用されます。リストの

1 番目のポータルは、スポンサー ポータルで使用されているスタイルとカスタマイズ内容を決定します。

ポータルの許可

ポータルを許可するときは、ネットワーク アクセス用のネットワーク許可プロファイルおよびルールを設定します。

始める前に

ポータルを許可する前にポータルを作成する必要があります。

ステップ 1 ポータルの特別な許可プロファイルを設定します。

ステップ 2 プロファイルの許可ポリシー ルールを作成します。

許可プロファイルの作成

各ポータルには、特別な許可プロファイルを設定する必要があります。

始める前に

デフォルトのポータルを使用しない場合は、許可プロファイルとポータル名を関連付けることができるように、最初にポータルを作成する必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 使用を許可するポータル名を使用して許可プロファイルを作成します。

次のタスク

新しく作成される許可プロファイルを使用するポータル許可ポリシー ルールを作成する必要があります。

ホットスポット ポータルおよび MDM ポータル用の許可ポリシー ルールの作成

ユーザ（ゲスト、スポンサー、従業員）のアクセス要求への応答に使用するポータルのリダイレクション URL を設定するには、そのポータル用の許可ポリシー ルールを定義します。

url-redirect は、ポータル タイプに基づいて次の形式になります。

ip:*port* = IP アドレスとポート番号

PortalID = 一意のポータル名

ホットスポット ゲスト ポータル：
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

モバイル デバイス管理（MDM）ポータル：
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択して、[標準（Standard）] ポリシーで新しい許可ポリシー ルールを作成します。

ステップ 2 [条件（Conditions）] には、ポータルの検証に使用するエンドポイント ID グループを選択します。たとえば、ホットスポット ゲスト ポータルの場合は、デフォルトの [GuestEndpoints] エンドポイント ID グループを選択し、MDM、ポータルの場合は、デフォルトの [RegisteredDevices] エンドポイント ID グループを選択します。

（注） ホットスポット ゲスト ポータルは、Termination CoA だけを発行するため、ゲスト許可ポリシーの検証条件の 1 つとして [Network Access:UseCase EQUALS Guest Flow] を使用しないでください。代わりに、エンドポイントが属する ID グループに照合して検証を行います。次の例を参考にしてください。

- "GuestEndpoint" + Wireless MAB の場合は Permit Access
- Wireless MAB の場合は HotSpot Redirect

ステップ 3 [権限（Permissions）] には、作成したポータル許可プロファイルを選択します。

ゲスト ポータルのカスタマイズ

ポータルの外観およびユーザ（必要に応じてゲスト、スポンサー、または従業員）エクスペリエンスをカスタマイズするには、ポータル テーマをカスタマイズし、ポータル ページの UI 要素を変更して、ユーザに表示されるエラー メッセージと通知を編集します。ポータルのカスタマイズの詳細については、エンドユーザ Web ポータルのカスタマイズ （483 ページ）を参照してください。

定期的な AUP 受け入れの設定

[ポリシー（Policy）] > **[ポリシー セット（Policy Sets）]** を参照し、AUP の期限が切れた場合にゲスト ユーザをクレデンシャルを持つポータルにリダイレクトする新しい許可ルールをリストの上部に作成します。LastAUPAcceptanceHours を目的の最大時間と比較するには条件を使用します（たとえば LastAUPAcceptanceHours > 8）。時間の範囲 1 ～ 999 をチェックできます。

次のタスク

エンドポイントが AUP 設定を受信したことを確認するには、次の手順を実行します。

1. **[管理（Administration）] > [ID（Identities）] > [エンドポイント（EndPoints）]** を選択します。
2. AUP が最後に受け入れられた時刻を確認するエンドポイントをクリックします（*AUPAcceptedTime*）。

定期的な AUP の強制

ポリシーで LastAUPAcceptance を使用して、AUP を承認することをユーザに強制できます。

```
If LastAUPAcceptance >= 24: Hotspot Redirect
If LastAUPacceptance < 24: PermitAccess
If Wireless_MAB: Hotspot Redirect
```

この例では、24 時間ごとにホットスポット ポータルに AUP を強制する方法を示します。

1. ユーザが 24 時間以上前に AUP を承認済みの場合、AUP を受け入れる（初めからやり直す）必要があります。
2. ユーザが 24 時間前以内に AUP を承認済みの場合、セッションを続行します。
3. ネットワーク（MAB）への最初のアクセス時は AUP を承認する必要があります。

クレデンシャルを持つポータルでは、そのポータルの AUP が有効であれば同じ規則を使用できます。

ゲスト ユーザ情報を保存

[アカウントを記憶する（Remember me）] は、ISE でレポートおよびログの MAC アドレスではなくゲストのユーザ名が表示されることを意味します。

ゲストが初回に認証されると、ゲストのデバイスの MAC アドレスがエンドポイント グループに保存され、レポートでユーザ名が使用されます。ユーザが切断され、ネットワークに再接続された場合、MAC アドレスはすでにエンドポイント グループに存在するため、ユーザは再びログイン（認証）する必要はありません。この場合、ユーザ名は利用できないため、レポートとログには MAC アドレスが使用されます。

ISE 2.3 以降、ISE はポータル ユーザ ID を保持し、リリースに応じて一部のレポートに使用します。

- ISE 2.3 にはこの機能が実装されていますが、オフにすることはできません。
- ISE 2.4 には、**[ゲスト（Guest）] > [設定（Settings）] > [ロギング（Logging）]** にこの機能をオフにする機能が追加されました。新規インストールではデフォルトでオンになります。以前のリリースのアップグレードおよび復元では無効になっています。

[アカウントを記憶する（Remember Me）] のロギングの問題に関する詳細については、ISE コミュニティで『ISE 2.3+ Remember Me guest using guest endpoint group logging display』の投稿を参照してください。

[アカウントを記憶する（Remember Me）] の設定に関する詳細については、『ISE Guest Access Deployment guide』を参照してください。 https://communities.cisco.com/docs/DOC-77590

各リリースでサポートされるレポート方法に関する詳細については、該当するリリースのリリース ノートを参照してください。

スポンサー ポータル

スポンサー ポータルは、Cisco ISE ゲスト サービスの主要コンポーネントの 1 つです。スポンサーポータルを使用して、スポンサーは承認ユーザ用の一時アカウントを作成および管理し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲストアカウントを作成した後、スポンサーは、スポンサーポータルを使用して、印刷、電子メール送信、または携帯電話による送信を行ってゲストにアカウントの詳細を提供することもできます。アカウント登録ゲストに企業ネットワークへのアクセス権を提供する前に、スポンサーはゲスト アカウントを承認するように電子メールで要求されることがあります。

スポンサー ポータルでのゲスト アカウントの管理

スポンサー ポータルのログオンのフロー

スポンサー グループにより、スポンサー ユーザに割り当てられる権限のセットが指定されます。スポンサーがスポンサー ポータルにログインすると、次の処理が行われます。

1. ISE がスポンサーのクレデンシャルを検証します。
2. スポンサーの認証が成功すると、ISE は使用可能なすべてのスポンサー グループを検索して、スポンサーが属するスポンサー グループを見つけます。次の両方の条件を満たしている場合は、スポンサーがスポンサー グループに一致しているか、属しています。
   - スポンサーは、設定されているいずれかのメンバー グループのメンバーである。
   - [その他の条件（Other Conditions）] を使用している場合は、そのスポンサーについてすべての条件が true である。
3. スポンサーがスポンサー グループに属している場合、スポンサーはそのグループの権限を取得します。スポンサーは複数のスポンサー グループに属することができます。この場合、属しているすべてのグループの権限が組み合わせられます。スポンサーがどのスポンサー グループにも属していない場合、スポンサー ポータルへのログインは失敗します。

スポンサー グループとその権限は、スポンサー ポータルから独立しています。スポンサーがログインするスポンサー ポータルに関係なく、スポンサー グループの照合には同一アルゴリズムが使用されます。

スポンサー ポータルの使用

スポンサーポータルを使用して、承認された訪問者が企業ネットワークまたはインターネットにセキュアにアクセスできるようにする一時ゲスト アカウントを作成します。ゲスト アカウントを作成したら、スポンサーポータルを使用してこれらのアカウントを管理し、アカウントの詳細情報をゲストに提供することができます。

スポンサー ポータルでは、スポンサーが新しいゲスト アカウントを個別に作成するか、またはファイルからユーザ グループをインポートすることができます。

（注） Active Directory などの外部 ID ストアから承認された ISE 管理者は、スポンサー グループに所属できます。ただし、内部管理者アカウント（デフォルトの「admin」アカウントなど）はスポンサー グループに含めることができません。

スポンサー ポータルを開く方法はいくつかあります。

- 管理者コンソールで、[アカウントの管理（Manage Accounts）] リンクを使用します。管理者コンソールで、[ゲストアクセス（Guest Access）] をクリックしてから、[アカウントの管理（Manage Accounts）] をクリックします。[アカウントの管理（Manage Accounts）] をクリックすると、ALL_ACCOUNTS にアクセスできるデフォルトのスポンサー グループに割り当てられます。新しいゲストアカウントを作成できますが、ゲストに対して通知することはできません。これは、ゲストからのアカウント アクティベーション リクエストを受信するための電子メールアドレスがないためです。同じ権限を持ち、スポンサーポータルにログインしてこれらのアカウントを検索するスポンサーは、通知を送信できます。

  このステップでは、スポンサー ポータルの [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] ページで設定した FQDN が DNS サーバに存在している必要があります。

  NAT ファイアウォールを介してスポンサーポータルにアクセスしている場合、接続はポート 9002 を使用します。

- 管理者コンソールのスポンサー ポータル設定ページから、次の操作を実行します。**[ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）]** をクリックし、スポンサー ポータルを開き、[説明（Description）] フィールドの右側にある [ポータルテストURL（Portal Test URL）] リンクをクリックします。

- ブラウザで、スポンサー ポータルの [ポータル設定（Portal Settings）] ページで設定した URL（FQDN）を開きます。この URL（FQDN）は DNS サーバで定義されている必要があります。

次の作業

スポンサー ポータルの使用法については、お使いのバージョンの ISE の『Sponsor Portal User Guide』（https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html）を参照してください。

スポンサー アカウントの管理

スポンサーは、スポンサー ポータルからゲスト ユーザ アカウントを作成および管理する組織の従業員または請負業者となります。Cisco ISE は、ローカル データベースあるいは外部の Lightweight Directory Access Protocol（LDAP）、Microsoft Active Directory、または SAML ID ストア経由でスポンサーを認証します。外部ソースを使用しない場合、スポンサー用の内部ユーザ アカウントを作成する必要があります。

スポンサー グループ

スポンサー グループは、スポンサー ポータルの使用時にスポンサーに付与される権限を制御します。スポンサーがスポンサー グループのメンバーである場合、スポンサーにはグループに定義されている権限が付与されます。

スポンサーは、次の両方が当てはまる場合にスポンサー グループのメンバーであると見なされます。

1. スポンサーが、スポンサー グループで定義されているメンバー グループの少なくとも 1 つに属している。メンバー グループは、ユーザ ID グループか、Active Directory などの外部 ID ソースから選択されたグループです。
2. スポンサーが、スポンサー グループで指定されているすべてのその他の条件を満たしている。オプションのその他の条件は、ディクショナリ属性で定義される条件です。これらの条件は、許可ポリシーで使用されるものと動作が似ています。

スポンサーは、複数のスポンサー グループのメンバーにすることができます。その場合、スポンサーにはそれらすべてのグループから次のように組み合わされた権限が付与されます。

- いずれかのグループで有効になっている場合、「ゲストのアカウントの削除」などの個々の権限が付与されます。
- スポンサーは、任意のグループでゲスト タイプを使用してゲストを作成できます。
- スポンサーは、任意のグループの場所にゲストを作成できます。
- バッチ サイズ制限などの数値は、グループの最大値が使用されます。

スポンサーがいずれかのスポンサー グループのメンバーでない場合、そのスポンサーはスポンサー ポータルにログインできません。

- ALL_ACCOUNTS：スポンサーは、すべてのゲスト アカウントを管理できます。
- GROUP_ACCOUNTS：スポンサーは、同じスポンサー グループのスポンサーが作成したゲスト アカウントを管理できます。
- OWN_ACCOUNTS：スポンサーは、自分が作成したゲスト アカウントのみを管理できます。

特定のスポンサー グループで使用可能な機能をカスタマイズでき、それによりスポンサー ポータルの機能を制限または拡張できます。次に例を示します。

関連トピック

スポンサー ポータル （414 ページ）

スポンサー アカウントの作成およびスポンサー グループへの割り当て

内部スポンサー ユーザ アカウントを作成し、スポンサー ポータルを使用できるスポンサーを指定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]** を選択します。適切なユーザ ID グループに内部スポンサー ユーザ アカウントを割り当てます。

（注） デフォルトのスポンサー グループには、デフォルトの ID グループ Guest_Portal_Sequence が割り当てられています。

ステップ 2 **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー グループ（Sponsor Groups）] > [作成、編集または複製（Create, Edit or Duplicate）]** の順に選択し、[メンバー（Members）] をクリックします。スポンサー ユーザ ID グループをスポンサー グループにマッピングします。

次のタスク

スポンサーで使用するために、追加で組織に固有のユーザ ID グループを作成することもできます。**[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ユーザ ID グループ（User Identity Groups）]** を選択します。

スポンサー グループの設定

シスコはデフォルトのスポンサー グループを提供します。デフォルト オプションを使用しない場合、新しいスポンサー グループを作成するか、またはデフォルトのスポンサー グループを編集して設定を変更できます。スポンサー グループを複製して、同じ設定と権限を持つスポンサー グループをさらに作成することもできます。

スポンサー グループを無効にすることができます。無効になったグループのメンバーはスポンサー ポータルにログインできなくなります。Cisco ISE によって提供されているデフォルトのスポンサー グループ以外のスポンサー グループを削除できます。

ステップ 1 **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals and Components）] > [スポンサー グループ（Sponsor Groups）] > [作成、編集または複製（Create, Edit or Duplicate）]** の順に選択します。

ステップ 2 [スポンサーグループ名（Sponsor group name）] と [説明（Description）] に入力します。

ステップ 3 [一致基準（Matching Criteria）]：このセクションの設定により、スポンサーがこのグループのメンバーかどうかが判別されます。

- メンバー グループ（Member Groups）：メンバーをクリックして 1 つ以上のユーザ（ID）グループおよび外部 ID ソースのグループを選択し、それらのグループを追加します。ユーザがこのスポン

サー グループのメンバーになるためには、少なくとも 1 つの設定済みグループに属している必要があります。

- その他の条件（Other conditions）：[新しい条件の作成（Create New Condition）] をクリックして、このスポンサー グループに含まれるためにスポンサーが満たす必要がある条件を 1 つ以上構築します。Active Directory、LDAP、SAML、ODBC の ID ストアからの認証属性を使用できますが、RADIUS トークンまたは RSA SecurID ストアは使用できません。内部ユーザ属性も使用できます。条件には、属性、演算子、値があります。
  - ディクショナリ属性 *Name* を使用して条件を作成するには、ID グループ名の前にユーザ ID グループを付けます。次に例を示します。

    InternalUser:Name EQUALS bsmith

    この場合、「bsmith」という名前の内部ユーザだけがこのスポンサー グループに所属できます。
  - Active Directory インスタンスの ExternalGroups 属性を使用して条件を作成するには、一致させるスポンサー ユーザの AD「プライマリ グループ」を選択します。たとえば、ユーザの名前が Smith の場合は *AD1:LastName EQUALS Smith* になります。

1 つ以上の設定されたメンバー グループとの一致に加えて、スポンサーはここで作成するすべての条件に一致する必要があります。認証しているスポンサー ユーザが複数のスポンサー グループの一致基準を満たす場合には、そのユーザには次のようにアクセス許可が付与されます。

- ゲストのアカウントの削除などの個々の権限は、一致するグループのいずれかで有効になっている場合に付与されます。
- スポンサーは、一致するグループのいずれかのゲスト タイプを使用してゲストを作成することができます。
- スポンサーは、一致するグループのいずれかのゲスト タイプを使用してゲストを作成することができます。
- スポンサーは、一致するグループのいずれかの場所でゲストを作成することができます。
- バッチ サイズ制限などの数値については、一致するグループの最も大きな値が使用されます。

[メンバー グループ（Member Groups）] のみが指定されている一致基準、または [その他の条件（Other Conditions）] のみが指定されている一致基準を作成できます。[その他の条件（Other Conditions）] のみを指定する場合、スポンサー グループのスポンサーのメンバーシップは、一致するディクショナリ属性のみに基づいて決定されます。

ステップ 4 このスポンサー グループに基づくスポンサーによって作成できるゲスト タイプを指定するには、[このスポンサーグループはこれらのゲストタイプを使用してアカウントを作成可能（This sponsor group can create accounts using these guest types）] でボックス内をクリックして、1 つ以上のゲスト タイプを選択します。

[次の場所にゲスト タイプを作成（Create Guest Types at）] の下のリンクをクリックして、このスポンサー グループに割り当てるゲスト タイプをさらに作成できます。新しいゲスト タイプを作成した後、その新しいゲスト タイプを選択するには、スポンサー グループを保存して閉じ、再度開いてください。

ステップ 5 [ゲストが訪問するロケーションを選択（Select the locations that guests will be visiting）] を使用して、ゲストアカウントの作成時にスポンサー グループのスポンサーが選択できるロケーション（ゲストの時間帯の設定に使用）を指定します。

[次の場所にゲストロケーションを設定（Configure guest locations at）] の下のリンクをクリックして、ゲストロケーションを追加することで、選択できるロケーションをさらに追加できます。新しいゲストロケーションを作成した後、その新しいゲストロケーションを選択するには、スポンサー グループを保存して閉じ、再度開いてください。

これによって、ゲストが他のロケーションからログインできなくなることはありません。

ステップ 6 スポンサーがユーザの作成後に [通知（Notify）] をクリックする操作を行わずにすむようにするには、[自動ゲスト通知（Automatic guest notification）] の下の [電子メール アドレスが使用可能な場合はアカウント作成時にゲストに電子メールを自動的に送信する（Automatically email guests upon account creation if email address is available）] をオンにします。これにより、電子メールが送信されたことを示すウィンドウが表示されます。また、このオプションをオンにすると、[ゲスト通知は自動送信されました（Guest notifications are sent automatically] というヘッダーがスポンサー ポータルに追加されます。

ステップ 7 [スポンサー作成可能（Sponsor Can Create）] で、このグループ内のスポンサーがゲスト アカウントを作成するために使用できるオプションを設定します。

- 特定のゲストに割り当てられた複数のゲスト アカウント（インポート）（Multiple guest accounts assigned to specific guests (Import)）：スポンサーは、ファイルから姓名などのゲストの詳細をインポートすることによって、複数のゲスト アカウントを作成できます。

  このオプションが有効である場合、[インポート（Import）] ボタンがスポンサー ポータルの [アカウントの作成（Create Accounts）] ページに表示されます。[インポート（Import）] オプションは、Internet Explorer、Firefox、Safari などのデスクトップ ブラウザだけで使用可能です（モバイルは不可）

- バッチ処理の制限（Limit to batch of）：このスポンサー グループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲスト アカウントの数を指定します。

  スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- [ゲストへの複数のゲスト アカウントの割り当て（ランダム）（Multiple guest accounts to be assigned to any guests (Random)）]：スポンサーが、未知のゲストのプレースホルダとして複数のランダム ゲスト アカウントを作成するか、または、または複数のアカウントをすばやく作成することができるようにします。

  このオプションが有効である場合、[ランダム（Random）] ボタンがスポンサー ポータルの [アカウントの作成（Create Accounts）] ページに表示されます。

- デフォルト ユーザ名プレフィックス（Default username prefix）：スポンサーが複数のランダムなゲストアカウントを作成する場合に使用できるユーザ名プレフィックスを指定します。指定した場合、このプレフィックスはランダムなゲスト アカウントを作成するときにスポンサー ポータルに表示されます。また、[スポンサーにユーザ名プレフィックスの指定を許可（Allow sponsor to specify a username prefix）] の設定により、次のようになります。

  - 有効：スポンサーは、スポンサー ポータルでデフォルトのプレフィックスを編集できます。

- 無効：スポンサーは、スポンサー ポータルでデフォルトのプレフィックスを編集できません。

ユーザ名プレフィックスを指定しないか、またはスポンサーにユーザ名プレフィックスの指定を許可しない場合、スポンサーはスポンサー ポータルでユーザ名プレフィックスを割り当てることができません。

- スポンサーにユーザ名プレフィックスの指定を許可（Allow sponsor to specify a username prefix）：このスポンサー グループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲスト アカウントの数を指定します。

  スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

ステップ 8 [スポンサーが管理可能（Sponsor Can Manage）] で、このスポンサー グループのメンバーが表示および管理できるゲスト アカウントを制限できます。

- スポンサーが作成したアカウントのみ（Only accounts sponsor has created）：このグループのスポンサーは、スポンサーの電子メール アカウントに基づいて、スポンサーが作成したゲスト アカウントのみを表示および管理できます。
- このスポンサー グループのメンバーによって作成されたアカウント（Accounts created by members of this sponsor group）：このグループのスポンサーは、このスポンサー グループ内のスポンサーが作成したゲスト アカウントを表示および管理できます。
- すべてのゲスト アカウント（All guest accounts）：スポンサーはすべての保留中のゲスト アカウントを表示および管理できます。

ステップ 9 [スポンサーの権限（Sponsor Can）] で、このスポンサー グループのメンバーに、ゲストのパスワードおよびアカウントに関連する追加の権限を提供できます。

- ゲストの連絡先情報（電子メール、電話番号）の更新（Update guests' contact information (email, Phone Number)）：スポンサーは、自分が管理できるゲスト アカウントについて、ゲストの連絡先情報を変更できます
- ゲストのパスワードの表示/印刷（View/print guests' passwords）：これをオンにすると、スポンサーはゲストのパスワードを印刷することができます。スポンサーは [アカウントの管理（Manage Accounts）] ページおよびゲストの詳細で、ゲストのパスワードを表示できます。これがオフの場合、スポンサーはパスワードを印刷できませんが、ユーザは電子メールまたは SMS（設定済みの場合）を介してパスワードを取得できます。
- ゲストのクレデンシャルを含む SMS 通知の送信（Send SMS notifications with guests' credentials）：スポンサーは、自分が管理できるゲストアカウントについて、アカウントの詳細とログイン クレデンシャルとともにゲストに SMS（テキスト）通知を送信できます。
- ゲスト アカウント パスワードのリセット（Reset guest account passwords）：スポンサーは、自分が管理できるゲストアカウントについて、そのパスワードを Cisco ISE によって生成されたランダムなパスワードにリセットできます。

- ゲストのアカウントの延長（Extend guests' accounts）：スポンサーは、自分が管理できるゲスト アカウントについて、その有効期限を延長できます。スポンサーは、アカウントの有効期限に関してゲストに送信される電子メール通知に自動的にコピーされます。
- ゲストのアカウントの削除（Delete guests' accounts）：スポンサーは、自分が管理できるゲストアカウントについて、アカウントを削除し、ゲストが企業のネットワークにアクセスすることを防ぐことができます。
- ゲストのアカウントの一時停止（Suspend guests' accounts）：スポンサーは、自分が管理できるゲスト アカウントについて、アカウントを一時停止してゲストが一時的にログインすることを防ぐことができます。

  また、このアクションは、許可変更（CoA）終了を発行して、一時停止されていたゲストをネットワークから排除できます。

  - スポンサーに理由の入力を求める（Require sponsor to provide a reason）：ゲスト アカウントの一時停止に対する説明の入力をスポンサーに求めます。

- アカウント登録ゲストからの要求の承認および表示（Approve and view requests from self-registering guests）：このスポンサー グループに含まれているスポンサーは、（承認が必要な）アカウント登録ゲストからのすべての保留中のアカウント要求を表示するか、アクセス先の担当者としてユーザがスポンサーの電子メール アドレスを入力した要求のみを表示できます。この機能では、アカウント登録ゲストによって使用されるポータルで[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] にマークが付けられていて、スポンサーの電子メールが連絡先の担当者としてリストされている必要があります。
  - [保留中のすべてのアカウント（Any pending accounts）]：このグループに所属するスポンサーは、他のスポンサーによって作成されたアカウントを承認およびレビューします。
  - [このスポンサーに割り当てられている保留中のアカウントのみ（Only pending accounts assigned to this sponsor）]：このグループに所属するスポンサーは、スポンサー自身が作成したアカウントだけを表示および承認できます。

- プログラムによるインターフェイス（Guest REST API）を使用した Cisco ISE ゲスト アカウントへのアクセス（Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)）：スポンサーは、自分が管理できるゲスト アカウントについて、Guest REST API プログラミング インターフェイスを使用してゲスト アカウントにアクセスできます。

ステップ 10 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

スポンサー アカウント作成のためのアカウント コンテンツの設定

ゲストとスポンサーが新しいゲスト アカウントの作成時に指定する必要があるユーザ データのタイプを設定できます。ISE アカウントを識別するために必要なフィールドがありますが、その他のフィールドを削除し、独自のカスタム フィールドを追加することができます。

スポンサーによるアカウント作成用のフィールドを設定するには、次の手順に従います。

1. ISE で **[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Sponsor Portals）]** を選択し、スポンサー ポータルを編集します。
2. [ポータル ページのカスタマイズ（Portal Page Customization）] タブを選択します。
3. 下にスクロールして [既知のゲストのアカウント作成（Create Account for Known Guests)] を選択します。
4. 右側の [プレビュー（Preview）] 表示で [設定（Settings）] を選択します。

これらの設定により、スポンサー ポータルでのゲスト アカウントの作成時に表示される、ゲスト アカウントに必要なフィールドが決定します。この設定は、ゲスト タイプ [既知（Known）]、[ランダム（Random）]、および[インポート（Imported）] に適用されます。新しいユーザをインポートするためにスポンサーがダウンロードするテンプレートは動的に作成されるので、[既知のゲスト（Known Guests）] で設定したフィールドだけが含まれます。

アカウントのユーザ名とパスワードのインポート

スポンサーはユーザ名とパスワードをインポートできますが、スポンサーが CSV テンプレートをダウンロードするときにはこれらの行がテンプレートに追加されません。スポンサーはこれらのヘッダーを追加できます。ISE が列を認識できるように、ヘッダーの名前が正しく設定されている必要があります。

- [ユーザ名（Username）]：*User Name* または *UserName* です。
- [パスワード（Password）]：**`password`** である必要があります。

スポンサー ポータルの特別な設定

次の設定は、[インポートされたゲストにアカウントを作成（Create Account for Imported Guests）] ページ、[ポータルページのカスタマイズ（Portal Page Customizations）] タブ、スポンサー ポータルで一意です。

- [スポンサーによるゲストクレデンシャルの電子メールのコピーを許可（Allow sponsor to be copied in Guest Credentials email）]：このオプションを有効にすると、インポートされたゲストに正常に送信されるゲストクレデンシャルの各電子メールがスポンサーにも送信されます。デフォルトでは、電子メールはスポンサーに送信されません。
- [スポンサーによるサマリーの電子メールの受信を許可（Allow sponsor to receive summary email）]：スポンサーがユーザ リストをインポートすると、ISE はインポートされたすべてのユーザを含むサマリーの電子メールを 1 つ送信します。このオプションをオフにすると、スポンサーはインポートされたユーザごとにそれぞれ電子メールを受信します。

スポンサー ポータル フローの設定

デフォルト ポータルと、証明書、エンドポイント ID グループ、ID ソース順序、ポータル テーマ、イメージ、および Cisco ISE によって提供されるその他の詳細などのデフォルト設定を使

用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

会社の営業所やその小売の場所にさまざまなブランディングがある場合、会社にさまざまな製品ブランドがある場合、または市役所が火災、警察、およびその他の部門で異なるテーマのポータルを必要とする場合は、複数のスポンサー ポータルを作成することもできます。

これらは、スポンサー ポータルの設定に関連するタスクです。

始める前に

スポンサー グループの設定 （417ページ）の説明に従い、サイトの既存のスポンサー グループを設定または編集します。

ステップ 1 ポリシー サービスの有効化 （423 ページ）。
ステップ 2 ゲスト サービスの証明書の追加 （423 ページ）。
ステップ 3 外部 ID ソースの作成 （424 ページ）。
ステップ 4 ID ソース順序の作成 （425 ページ）。
ステップ 5 スポンサー ポータルの作成 （425 ページ）。
ステップ 6 （任意） スポンサー ポータルのカスタマイズ （426 ページ）。

ポリシー サービスの有効化

Cisco ISE エンドユーザ Web ポータルをサポートするには、ホストするノードでポータル ポリシー サービスを有効にする必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。
ステップ 2 ノードをクリックして、[編集（Edit）] をクリックします。
ステップ 3 [全般設定（General Settings）] タブで、[ポリシー サービス（Policy Service）] をオンにします。
ステップ 4 [セッション サービスの有効化（Enable Session Services）] オプションをオンにします。
ステップ 5 [**保存（Save）**] をクリックします。

ゲスト サービスの証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループ タグに割り当てることができます。すべてのエンドユーザ Web ポータルに使用されるデフォルトの証明書グループ タグは [デフォルト ポータル証明書グループ（Default Portal Certificate Group）] です。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。

この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。

ステップ 3 **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portals）] > [作成または編集（Create or Edit）] > [ポータル設定（Portal Settings）]** を選択します。

ステップ 4 新しく追加された証明書に関連付けられた [証明書グループ タグ（Certificate Group Tag）] ドロップダウン リストから特定の証明書グループ タグを選択します。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバなどの外部 ID ソースに接続して、認証/許可のユーザ情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザ ID を受信して共有できるようにするパッシブ ID サービスを使用するには、を参照してくださいその他の パッシブ ID サービス プロバイダー （647 ページ）。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。
- Active Directory：外部 ID ソースである Active Directory に接続する場合。 外部 ID ソースとしての Active Directory （587 ページ）を参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、 LDAP （696 ページ）を参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバを追加する場合。詳細については、 RADIUS トークン ID ソース （722 ページ）を参照してください。
- RSA SecurID：RSA SecurID サーバを追加する場合。詳細については、 RSA ID ソース （730 ページ）を参照してください。
- SAML IDプロバイダー（SAML Id Providers）：Oracle Access Manager などの ID プロバイダー（IdP）を追加する場合。詳細については、 外部 ID ソースとしての SAMLv2 ID プロバイダ （738 ページ）を参照してください。
- **ソーシャル ログイン**：Facebook などのソーシャル ログインを外部 ID ソースとして追加する場合。アカウント登録ゲストのソーシャル ログイン （389 ページ）を参照してください。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲスト ユーザがローカル WebAuth を使用して認証できるようにするには、ゲスト ポータル認証ソースと ID ソース順序に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）]** を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストのデータベースを並べ替えます。

ステップ 6 [高度な検索リスト（Advanced Search List）] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

  Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストに、Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

スポンサー ポータルの作成

スポンサー ポータルを提供して、ネットワークに接続してインターネットと内部リソースおよびサービスにアクセスするゲストのアカウントをスポンサーが作成、管理、および承認できるようにすることができます。

Cisco ISE では、別のポータルを作成する必要なく使用できるデフォルトのスポンサー ポータルが用意されています。ただし、新しいスポンサー ポータルを作成するか、既存のものを編集または複製できます。デフォルトのスポンサー ポータル以外のすべてのポータルを削除できます。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブの [ページ設定（Page Settings）] で行った変更は、スポンサー フロー図のグラフィカル フローに反映されます。[AUP]ページなどのページを有効にすると、そのページがフローに表示され、スポンサーはポータルでそれを確認します。無効にした場合は、そのページがフローから削除され、次に有効にされたページがスポンサーに表示されます。

始める前に

このポータルで使用するために、必要な証明書、外部 ID ソース、および ID ソース順序が設定されていることを確認します。

ステップ 1 スポンサー ポータルのポータル設定 （466 ページ） の説明に従って、[ポータル設定（Portal Settings）] ページを設定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 2 スポンサー ポータルのログイン設定 （469 ページ） の説明に従って、[ログイン設定（Login Settings）] ページを設定します。

ステップ 3 スポンサー ポータルの利用規定（AUP）設定 （470 ページ） の説明に従って、[利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）] ページを設定します。

ステップ 4 ゲスト パスワード ポリシーと有効期限の設定 （383 ページ） と ゲスト パスワード ポリシーのルール （382 ページ） の説明に従って、[スポンサーのパスワード変更設定（Sponsor Change Password Settings）] ページを設定します。

ステップ 5 スポンサー ポータルのポストログイン バナー設定 （471 ページ） の説明に従って、[ポストログインバナーページ設定（Post-Login Banner Page Settings）] ページを設定します。

ステップ 6 [スポンサーポータルアプリケーションの設定（Sponsor Portal Application Settings）] では、ポータルをカスタマイズする場合は [ポータルのカスタマイズ（Portal Customization）] タブを参照します。

ステップ 7 [**保存（Save）**] をクリックします。

スポンサー ポータルのカスタマイズ

ポータルの外観およびユーザ エクスペリエンスをカスタマイズするには、ポータル テーマをカスタマイズし、ポータル ページの UI 要素を変更して、ユーザに表示されるエラー メッセージと通知を編集します。ポータルのカスタマイズの詳細については、エンドユーザ Web ポータルのカスタマイズ （483 ページ） を参照してください。

スポンサー アカウント作成のためのアカウント コンテンツの設定

ゲストとスポンサーが新しいゲスト アカウントの作成時に指定する必要があるユーザ データのタイプを設定できます。ISE アカウントを識別するために必要なフィールドがありますが、その他のフィールドを削除し、独自のカスタム フィールドを追加することができます。

スポンサーによるアカウント作成用のフィールドを設定するには、次の手順に従います。

1. ISE で [ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portals）] を選択し、スポンサー ポータルを編集します。
2. [ポータル ページのカスタマイズ（Portal Page Customization）] タブを選択します。
3. 下にスクロールして [既知のゲストのアカウント作成（Create Account for Known Guests)] を選択します。
   - 右側の [プレビュー（Preview）] 表示で [設定（Settings）] を選択します。

   これらの設定により、スポンサーポータルでのゲストアカウントの作成時に表示される、ゲスト アカウントに必要なフィールドが決定します。

この設定は、ゲスト タイプ [既知（Known）]、[ランダム（Random）]、および [インポート（Imported）] に適用されます。新しいユーザをインポートするためにスポンサーがダウンロードするテンプレートは動的に作成されるので、[既知のゲスト（Known Guests）] で設定したフィールドだけが含まれます。

スポンサーによるアカウントのユーザ名とパスワードのインポート

スポンサーはユーザ名とパスワードをインポートできますが、スポンサーがテンプレートをダウンロードするときにはこれらの行はテンプレートに追加されません。スポンサーはこれらのヘッダーを追加できます。ISE が列を認識できるように、ヘッダーの名前が正しく設定されている必要があります。

- **ユーザ名**：**`User Name`** または **`UserName`** のいずれかを指定します。
- **パスワード**：password にする必要があります。

スポンサーに対して使用可能な時間設定項目の設定

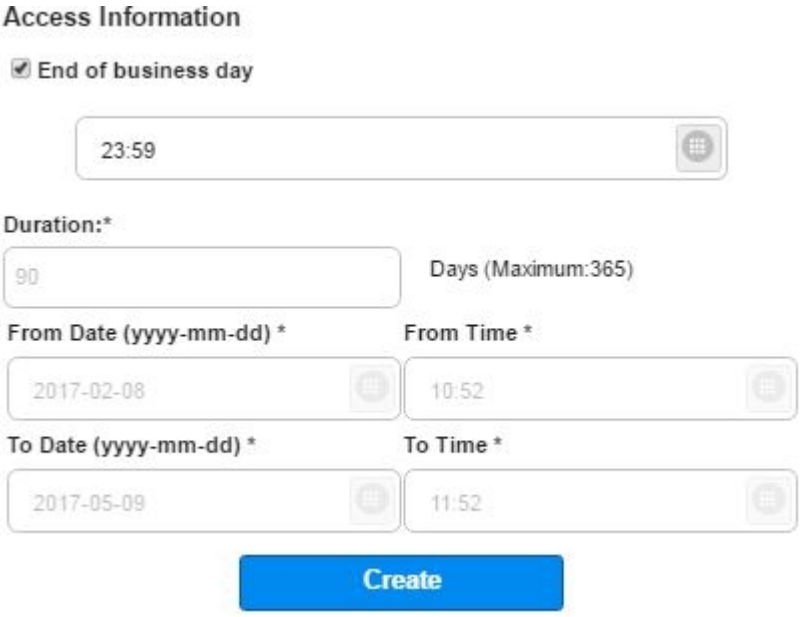
スポンサーは新しいゲストアカウントを作成するときに、アカウントがアクティブである期間を設定します。スポンサーが使用できるオプションを設定して、スポンサーがアカウントの期間と、開始時刻および終了時刻を設定できるようにすることができます。これらのオプションはゲスト タイプ別に設定されます。スポンサーに対し、[アクセス情報（Access Information）] というヘッダーの下に結果が表示されます。

スポンサーのポータル アカウント期間オプションを制御する [ゲスト タイプ（Guest Type）] 設定は、[最大アクセス時間（Maximum Access Time）] ヘッダーの下にあります。この設定について次に説明します。

- [初回ログインから（From-First-Login）]：スポンサー ポータルには [期間（Duration）] フィールドが表示され、その下に [初回ログインから（From-First-Login）] が表示されます。

ゲスト タイプ設定の [最大アカウント期間（Maximum account duration）] により、スポンサーがその期間として入力できる値が決定されます。

- [スポンサーが指定した日付から（From sponsor-specified date）]（該当する場合はアカウント登録の日付）：スポンサーは、期間を [営業日の終わり（End of business day）] として設定するか、または [営業日の終わり（End of business day）] フィールドをオフにして、期間、開始時刻、および終了時刻を設定するかを選択できます。



期間と有効な日付を制御するゲストタイプ設定は、[アクセスを許可する日付と時刻（Allow access only on these days and times）] ヘッダーの下にあります。

- 選択した曜日により、スポンサーのカレンダーで選択できる日付が制限されます。
- 期間と日付を選択すると、スポンサー ポータルで最大アカウント期間が適用されます。

スポンサー ポータルの Kerberos 認証

ISE を設定して、Windows にログオンしているスポンサー ユーザのスポンサー ポータルへのアクセスの認証に Kerberos を使用することができます。このプロセスは、Kerberos チケットで

ログインしているスポンサー ユーザの Active Directory クレデンシャルを使用します。ブラウザが ISE との SSL 接続を確立した後、セキュア トンネル内で Kerberos SSO が実行されます。

次の項目は同じ Active Directory ドメインに存在する必要があります。

- スポンサーの PC
- ISE PSN
- このスポンサー ポータルに設定された FQDN

この要件は、Microsoft では Active Directory フォレスト間の双方向の信頼での Kerberos SSO がサポートされていないため必要です。

スポンサー ユーザは、Windows にログオンする必要があります。

ゲスト ポータルの Kerberos 認証はサポートされていません。

Kerberos の設定

スポンサー ポータルで Kerberos を有効にするには、[スポンサー設定とカスタマイズ（Sponsor Settings and Customization）] ページで [Kerberos SSOを許可する（Allow Kerberos SSO）] チェックボックスをオンにします。

スポンサーのブラウザも正しく設定されていなければなりません。次のセクションでは、各ブラウザを手動で設定する方法を説明します。

Firefox を手動で設定するには

1. アドレス バーに `about:config` と入力します。
2. 表示される警告は無視し、クリックして続行します。
3. 検索バーで `negotiate` を検索します。
4. `network.negotiate-auth.delegation-uris` と `network.negotiate-auth.trusted-uris` に FQDN を追加します。各属性の URL の一覧はコンマで区切られます。
5. タブを閉じます。ブラウザが使用可になり、再起動は必要ありません。

Internet Explorer を手動で設定するには

1. 右上の歯車をクリックし、[インターネットオプション（Internet Options）] を選択します。
2. [セキュリティ（Security）] タブをクリックします。
3. [ローカルイントラネット（Local Intranet）] を選択します。
4. [サイト（Sites）] ボタンをクリックしてから、[詳細（Advanced）] ボタンをクリックします。
5. 文字列に `<mydomain>.com` を追加します（`<mydomain>` はスポンサー ポータル FQDN のワイルド カード）、または FQDN を入力します。
6. [閉じる（Close）] をクリックし、[OK] をクリックします。

7. [詳細（Advanced）] タブをクリックします。
8. [セキュリティ（Security）] チェックボックスまで下方向にスクロールし、[統合Windows認証を有効にする（Enable Integrated Windows Authentication）] チェックボックスが有効になっていることを確認します。
9. コンピュータを再起動します。

Chrome は Internet Explorer から設定を取得します

トラブルシューティング

- コマンド プロンプトで `set user` を実行し、マシンが適切な AD ドメインに連結されていることを確認します。
- コマンド プロンプトで `klist` を実行し、キャッシュされた Kerberos チケットとホスト名の一覧を表示します。
- SPNEGO トークンデータを見ます。NTLM パスワードベースのトークン文字列は、Kerberos トークン文字列よりもはるかに短く、正しいトークン文字列は 1 行に収まりません。
- `kerberos` フィルタを使用して Wireshark を使用し、存在する場合は Kerberos 要求をキャプチャします。

（注） Kerberos SSO オプションを有効にすると、ユーザは、Kerberos SSO が正しく機能するノード FQDN でスポンサー ポータルにアクセスする必要があります。スポンサー ポータルでポータル FQDN が設定されている場合、ユーザがポータル FQDN に接続すると、そのノード FQDN によってこのポータルにリダイレクトされます。

スポンサーがスポンサー ポータルにログインできない

問題

次のエラー メッセージは、スポンサーがスポンサー ポータルにログインしようとしたときに表示されます。

```
“Invalid username or password. Please try again.”
```

原因

- スポンサーが無効なクレデンシャルを入力しました。
- スポンサーは、ユーザ レコードがデータベース（内部ユーザまたは Active Directory）にないため無効です。
- スポンサーが属するスポンサー グループは無効です。

- スポンサーのユーザ アカウントがアクティブな/有効なスポンサー グループのメンバーではありません。これは、スポンサー ユーザの ID グループがいずれのスポンサー グループのメンバーでもないことを意味します。
- スポンサーの内部ユーザ アカウントは無効（一時停止中）です。

ソリューション

- ユーザのクレデンシャルを確認します。
- スポンサー グループを有効にします。
- ユーザ アカウントが無効になっている場合は復元します。
- スポンサー ユーザの ID グループをスポンサー グループのメンバーとして追加します。

ゲストとスポンサーのアクティビティのモニタ

Cisco ISE は、エンドポイントおよびユーザ管理情報、およびゲストとスポンサーのアクティビティを参照できるさまざまなレポートとログを提供します。Cisco ISE 1.2 レポートの一部は廃止されましたが、情報は他のレポートで表示できます。

オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 **[操作（Operations）] > [レポート（Reports）]** を選択します。

ステップ 2 レポート セレクタで、[ゲスト アクセス レポート（Guest Access Reports）] および [エンドポイントとユーザ（Endpoints and Users）] 選択を展開し、さまざまなゲスト、スポンサー、およびエンドポイントに関するレポートを表示します。

ステップ 3 レポートを選択し、[フィルタ（Filters）] ドロップダウン リストを使用して、検索するデータを選択します。

ユーザ名、ポータル名、デバイス名、エンドポイント ID グループ、および他のデータについてフィルタを使用できます。

ステップ 4 データを表示する [時間範囲（Time Range）] を選択します。

ステップ 5 [実行（Run）] をクリックします。

メトリック ダッシュボード

Cisco ISE では、Cisco ISE ホーム ページに表示されるメトリック ダッシュボードで、ネットワークの [認証されたゲスト（Authenticated Guests）] と [アクティブ エンドポイント（Active Endpoints）] を一目で確認できます。

（注） ホットスポット フローの場合、[認証されたゲスト（Authenticated Guests）] ダッシュレットにエンドポイントが表示されません。

AUP 受け入れステータス レポート

AUP 受け入れステータス レポートには、すべてのゲスト ポータルからの、ゲストによる利用規定（AUP）の受け入れのステータスが示されます。このレポートは、**[操作（Operations）]** > **[レポート（Reports）]** > **[ゲスト アクセス レポート（Guest Access Reports）]** > **[AUP 受け入れステータス（AUP Acceptance Status）]** から使用できます。

レポートを使用して、特定の期間のすべての許可および拒否されたAUP接続を追跡できます。

ゲスト アカウンティング レポート

ゲスト アカウンティング レポートは、指定された期間のゲスト ログイン履歴を表示します。このレポートは、**[操作（Operations）]** > **[レポート（Reports）]** > **[ゲスト アクセス レポート（Guest Access Reports）]** > **[ゲスト アカウンティング（Guest Accounting）]** で利用できます。

マスター ゲスト レポート

マスター ゲスト レポートは、さまざまなレポートからのデータを単一のビューへ結合して、複数の異なるレポート ソースからデータをエクスポートできるようにします。データ カラムをさらに追加したり、表示またはエクスポートしないデータ カラムを削除したりできます。このレポートは、**[操作（Operations）]** > **[レポート（Reports）]** > **[ゲスト アクセス レポート（Guest Access Reports）]** > **[マスター ゲスト（Master Guest）]** で利用できます。このレポートには、非推奨のゲスト アクティビティ レポートに含まれていた情報も含まれるようになりました。

このレポートはすべてのゲスト アクティビティを収集し、ゲスト ユーザがアクセスした Web サイトに関する詳細を提供します。このレポートをセキュリティ監査の目的で使用して、ゲスト ユーザがいつネットワークにアクセスして、何を行ったかを確認できます。アクセスした Web サイトの URL などのゲストのインターネット アクティビティを表示するには、初めに次の操作を行う必要があります。

- 成功した認証のロギング カテゴリを有効にします。**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギング カテゴリ（Logging Categories）]** を選択して、[成功した認証（Passed authentications）] を選択します。
- ゲスト トラフィックで使用するファイアウォールで次のオプションを有効にします。
  - HTTP トラフィックを検査し、Cisco ISE モニタリング ノードにデータを送信します。Cisco ISE はゲスト アクティビティ レポートに対して IP アドレスおよびアクセスした URL だけを必要とするため、可能な場合は、この情報だけが含まれるようにデータを制限します。

• Cisco ISE モニタリング ノードに syslog を送信します。

スポンサーのログインおよび監査レポート

スポンサー ログインおよび監査レポートは、次を追跡する統合レポートです。

- スポンサー ポータルでのスポンサーによるログイン アクティビティ。
- スポンサー ポータルでスポンサーが実行したゲスト関連の操作。

このレポートは、**[操作（Operations）] > [レポート（Reports）] > [ゲスト アクセス レポート（Guest Access Reports）] > [スポンサー ログインおよび監査（Sponsor Login and Audit）]** で使用できます。

ゲストおよびスポンサー ポータルの監査ロギング

ゲスト ポータルおよびスポンサー ポータルで特定のアクションが実行されると、基礎となる監査システムに監査ログ メッセージが送信されます。デフォルトでは、これらのメッセージは、/opt/CSCOcpm/logs/localStore/iseLocalStore.log ファイルに記録されます。

これらのメッセージを syslog によってモニタリング/トラブルシューティング システムおよびログ コレクタに送信するように設定することができます。モニタリング サブシステムによって、適切なスポンサー、デバイス監査ログ、およびゲストのアクティビティ ログにこの情報が示されます。

ゲスト ログイン フローは、ゲスト ログインが成功したか失敗したかにかかわらず、監査ログに記録されます。

ゲスト アクセス Web 認証オプション

Cisco ISE ゲスト サービスと Web 認証サービスでは、セキュアなゲスト アクセスを有効にするための複数の展開オプションがサポートされています。ローカルまたは中央 Web 認証とデバイス登録 Web 認証を使用した有線または無線のゲスト接続を提供することができます。

- [中央 Web 認証（Central WebAuth）] : すべてのゲスト ポータルに適用されます。有線および無線の両方の接続要求に対して、中央 Cisco ISE RADIUS サーバを介した Web 認証を使用します。ゲストは、ホットスポット ゲスト ポータルでオプションのアクセス コードを入力するか、クレデンシャルを持つゲスト ポータルでユーザ名とパスワードを入力することにより、後で認証されます。

（注） ユーザ クレデンシャルのブラウザへのリダイレクト（CWA）を使用する場合、複数のタブが開いたブラウザを使用しているユーザはサポートされません。リダイレクト時に、ブラウザが複数のタブを開いていると、ISEはすべてのタブにリダイレクトします。ユーザはポータルにログインできますが、ISE はセッションを承認できず、ユーザはアクセスに失敗します。

この問題を回避するには、ユーザがブラウザ上で 1 つを除くすべてのタブを閉じる必要があります。

- ローカル Web 認証（ローカル WebAuth）：クレデンシャルを持つゲスト ポータルに適用されます。ゲストは、有線接続の場合はスイッチに接続し、ワイヤレス接続の場合はワイヤレスLANコントローラ（WLC）に接続します。ネットワーク アクセスデバイス（NAD）は、認証用のWebページにゲストを転送します。ゲストは、認証のために、クレデンシャルを持つゲスト ポータルでユーザ名とパスワードを入力します。
- デバイス登録 Web 認証（デバイス登録 WebAuth）：ホットスポット ゲスト ポータルにのみ適用されます。Cisco ISE は、Web 認証の前にゲスト デバイスを登録して承認します。ゲストが有線またはワイヤレスNADに接続すると、ゲストはホットスポット ゲスト ポータルに転送されます。ゲストは、クレデンシャル（ユーザ名とパスワード）を入力せずにネットワークにアクセスします。

ISE Community Resource

ゲスト アクセスを提供するように Cisco ISE と Cisco ワイヤレス コントローラを設定する方法については、『ISE Guest AccessPrescriptive Deployment Guide』を参照してください。

ISE のテクニカルノート『ISE Wireless Guest Setup Guide & Wizard』も参照してください。

中央 WebAuth プロセス対応の NAD

このシナリオでは、ネットワーク アクセス デバイス（NAD）で、不明なエンドポイント接続から Cisco ISE RADIUS サーバへの新しい認証要求を作成します。これで、エンドポイントは Cisco ISE への URL-redirect を受け取ります。

（注） webauth-vrf-aware コマンドは、IOS XE 3.7E、IOS 15.2(4)E 以降のバージョンでのみサポートされています。その他のスイッチでは、Virtual Route Forwarding（VRF）環境での WebAuth URL リダイレクトはサポートされていません。このような場合、回避策として、トラフィックを VRF に戻すためのルートをグローバル ルーティング テーブルに追加できます。

ゲストデバイスがNADに接続されている場合、ゲスト サービスのインタラクションは、ゲスト ポータルの中央 WebAuth のログインにつながる MAC 認証バイパス（MAB）要求の形式を

取ります。無線と有線の両方のネットワーク アクセス デバイスに適用される後続の中央 Web 認証（中央 WebAuth）プロセスの概要は、次のとおりです。

1. ゲスト デバイスは、有線接続によって NAD に接続します。ゲスト デバイス上に 802.1X サプリカントはありません。
2. MAB のサービス タイプを扱う認証ポリシーにより、MAB が引き続き失敗し、中央 WebAuth ユーザ インターフェイスの URL-redirect を含む制限付きネットワーク プロファイルが返されます。
3. NAD は、Cisco ISE RADIUS サーバに対して MAB 要求を認証するように設定されています。
4. Cisco ISE RADIUS サーバで MAB 要求が処理されますが、ゲスト デバイスのエンドポイントが見つかりません。

   この MAB の失敗により、制限付きネットワーク プロファイルが適用され、プロファイル内の URL-redirect 値が access-accept で NAD に返されます。この機能をサポートするには、許可ポリシーが存在し、適切な有線または無線 MAB（複合条件下で）と、任意で「Session:Posture Status=Unknown」条件が備わっていることを確認します。NAD では、この値に基づいて、デフォルト ポート 8443 のすべてのゲスト HTTPS トラフィックが URL-redirect 値にリダイレクトされます。

   この場合の標準の URL 値は次のとおりです。

   ```
   https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&portal=<PortalID>&action=cwa
   ```
5. ゲスト デバイスが、Web ブラウザから URL をリダイレクトするための HTTP 要求を開始します。
6. NAD により、最初の access-accept から返された URL-redirect 値に要求がリダイレクトされます。
7. CWA をアクションとしたゲートウェイ URL 値は、ゲスト ポータル ログイン ページにリダイレクトされます。
8. ゲストはログイン クレデンシャルを入力してログイン フォームを送信します。
9. ゲスト サーバはログイン クレデンシャルを認証します。
10. フローのタイプに応じて、次の処理が実行されます。
    - クライアント プロビジョニングを実行するようにゲスト ポータルが設定されていない非ポスチャ フロー（これ以上の検証がない認証）の場合、ゲスト サーバは CoA を NAD に送信します。この CoA により、NAD は Cisco ISE RADIUS サーバを使用してゲスト デバイスを再認証します。設定されたネットワーク アクセスとともに新しい access-accept が NAD に返されます。クライアント プロビジョニングが未設定で、VLAN を変更する必要がある場合、ゲスト ポータルで VLAN IP の更新が行われます。ゲストはログイン クレデンシャルを再入力する必要はありません。初回ログイン時に入力したユーザ名とパスワードが自動的に使用されます。
    - クライアント プロビジョニングを実行するようにゲスト ポータルが設定されているポスチャ フローの場合、ゲスト デバイスの Web ブラウザに、ポスチャ エージェン

トのインストールおよびコンプライアンスのための [クライアント プロビジョニング（Client Provisioning）] ページが表示されます。（必要に応じて、クライアント プロビジョニング リソース ポリシーに「NetworkAccess:UseCase=GuestFlow」条件を含めることもできます）。

Linux 向けのクライアント プロビジョニングやポスチャ エージェントは存在しないため、ゲスト ポータルはクライアント プロビジョニング ポータルにリダイレクトされ、クライアント プロビジョニング ポータルは元のゲスト認証サーブレットにリダイレクトされます。この認証サーブレットで、必要に応じて IP リリース/更新が行われてから、CoA が実行されます。

クライアント プロビジョニング ポータルへのリダイレクションを使用して、クライアント プロビジョニング サービスはゲスト デバイスに非永続的 Web エージェントをダウンロードし、デバイスのポスチャ チェックを実行します（必要に応じて、ポスチャ ポリシーに「NetworkAccess:UseCase=GuestFlow」条件を含めることもできます）。

ゲスト デバイスが非準拠の場合、「NetworkAccess:UseCase=GuestFlow」条件および「Session:Posture Status=NonCompliant」条件を備えた許可ポリシーが設定済みであることを確認してください。

ゲスト デバイスが準拠している場合は、設定した許可ポリシーに「NetworkAccess:UseCase=GuestFlow」条件および「Session:Posture Status=Compliant」条件が含まれていることを確認してください。ここから、クライアント プロビジョニング サービスによって NAD に対して CoA が発行されます。この CoA により、NAD は Cisco ISE RADIUS サーバを使用してゲストを再認証します。設定されたネットワーク アクセスとともに新しい access-accept が NAD に返されます。

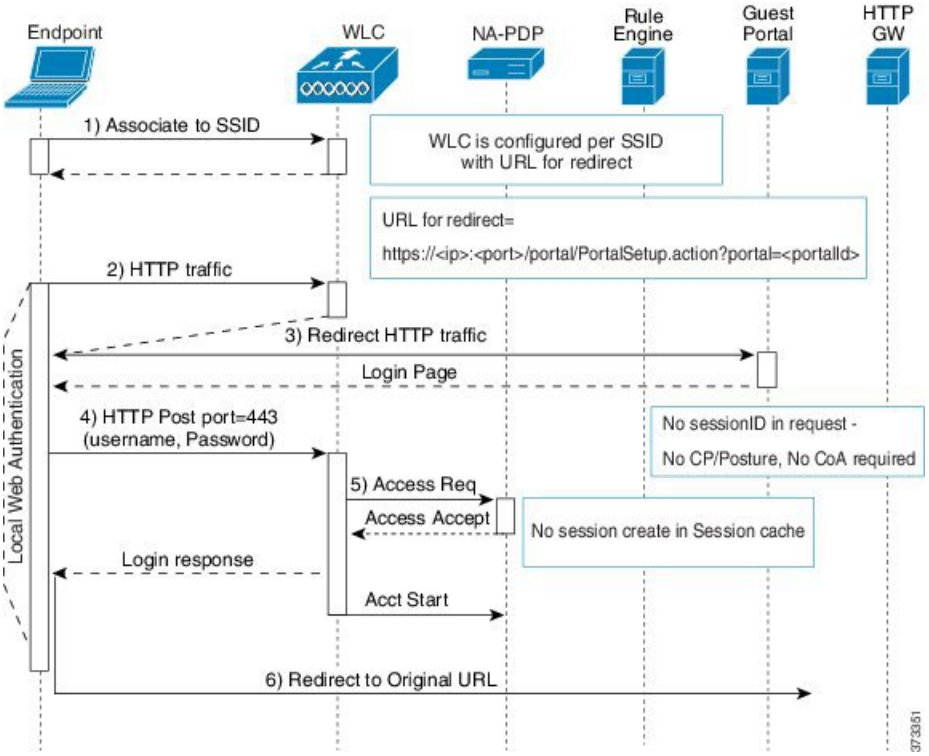
（注） 「NetworkAccess: UseCase=GuestFlow」は、ゲストとしてログインする Active Directory（AD）および LDAP ユーザにも適用できます。

ローカル WebAuth プロセス対応のワイヤレス LAN コントローラ

このシナリオでは、ゲストがログインすると、ワイヤレス LAN コントローラ（WLC）に転送されます。その後、WLC はゲストをゲスト ポータルにリダイレクトします。ゲスト ポータルでは、ログイン クレデンシャルの入力を求められ、必要に応じて利用規定（AUP）の受け入れやパスワードの変更を実行することもできます。完了したら、ゲスト デバイスのブラウザは WLC にリダイレクトされ、POST 経由でログイン クレデンシャルが提供されます。

WLC は、Cisco ISE RADIUS サーバ経由でゲストのログイン処理を行うことができます。その処理が完了したら、WLC はゲスト デバイスのブラウザを元の URL の宛先にリダイレクトします。ゲスト ポータルの元の URL リダイレクトをサポートするためのワイヤレス LAN コントローラ（WLC）とネットワーク アクセス デバイス（NAD）の要件は、リリース IOS-XE 3.6.0.E および 15.2(2)E が動作する WLC 5760 および Cisco Catalyst 3850、3650、2000、3000、および 4000 シリーズ アクセス スイッチです。

図 *10 :* ローカル *WebAuth* 対応 *WLC* の *Non-Posture* フロー



ローカル WebAuth プロセス対応の有線 NAD

このシナリオでは、ゲスト ポータルにより、ゲストのログイン要求がスイッチ（有線 NAD）にリダイレクトされます。ログイン要求は、スイッチにポストされる HTTPS URL の形式になり、ログイン クレデンシャルが含まれます。スイッチにゲスト ログイン要求が届くと、設定済みの Cisco ISE RADIUS サーバを使用してゲストの認証が行われます。

1. Cisco ISE により、HTML リダイレクトを含む login.html ファイルを NAD にアップロードするよう要求されます。HTTPS 要求が発生すると、この login.html ファイルがゲスト デバイスのブラウザに返されます。
2. ゲスト デバイスのブラウザがゲスト ポータルにリダイレクトされます。ここで、ゲストのログイン クレデンシャルが入力されます。
3. 利用規定（AUP）とパスワード変更が処理された後（両方ともオプションです）、ゲスト ポータルにより、ログイン クレデンシャルをポストするゲスト デバイスのブラウザが NAD にリダイレクトされます。
4. NAD により、Cisco ISE RADIUS サーバに対して RADIUS 要求が発行され、ゲストの認証と許可が行われます。

Login.html ページに必要な IP アドレスおよびポートの値

login.html ページの次の HTML コードで、IP アドレスとポートの値を Cisco ISE ポリシー サービス ノードと同じ値に変更する必要があります。デフォルト ポートは 8443 ですが、この値を変更できます。そのため、スイッチに割り当てた値が Cisco ISE の設定と一致していることを確認してください。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/portal/PortalSetup.action?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/portal/PortalSetup.action?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</HTML>
```

カスタム ログイン ページはパブリック Web フォームであるため、次のガイドラインに従ってください。

- ログイン フォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページ タイムアウト、パスワード非表示、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

NAD での HTTPS サーバの有効化

Web ベース認証を使用するには、**ip http secure-server** コマンドを使用してスイッチ内で HTTPS サーバを有効にする必要があります。

NAD 上でのカスタマイズされた認証プロキシ Web ページのサポート

成功、失効、失敗に関するカスタム ページを NAD にアップロードできます。Cisco ISE では特定のカスタマイズは必要ないため、NAD に付属する標準の設定手順を使用して、これらのページを作成できます。

NAD の Web 認証の設定

デフォルトの HTML ページをカスタム ファイルで置き換えて、NAD における Web 認証を完了する必要があります。

始める前に

Web ベースの認証中、スイッチのデフォルト HTML ページの代わりに使用する 4 つの代替 HTML ページを作成します。

ステップ 1 カスタム認証プロキシ Web ページを使用するように指定するには、最初にカスタム HTML ファイルをスイッチのフラッシュ メモリに格納します。スイッチのフラッシュ メモリに HTML ファイルをコピーするには、スイッチで次のコマンドを実行します。

copy tftp/ftp flash

ステップ 2 スイッチに HTML ファイルをコピーした後、グローバル コンフィギュレーション モードで次のコマンドを実行します。

a.	**ip admission proxy http login page file device**:*login-filename*	スイッチのメモリ ファイル システム内で、デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの場所を指定します。device: はフラッシュ メモリです。
b.	**ip admission proxy http success page file device**:*success-filename*	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
c.	**ip admission proxy http failure page file device**:*fail-filename*	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
d.	**ip admission proxy http login expired page file device**:*expired-filename*	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。

ステップ 3 スイッチによって提供されるガイドラインに従って、カスタマイズされた認証プロキシ Web ページを設定します。

ステップ 4 次の例に示すように、カスタム認証プロキシ Web ページの設定を確認します。

```
Switch# show ip admission configuration
Authentication proxy webpage
 Login page           : flash:login.htm
```

```
 Success page          : flash:success.htm
 Fail Page             : flash:fail.htm
 Login expired Page    : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

デバイス登録 WebAuth プロセス

デバイス登録 Web 認証（デバイス登録 WebAuth）およびホットスポット ゲスト ポータルを使用すると、ユーザ名とパスワードを要求しないで、プライベート ネットワークへの接続をゲスト デバイスに許可できます。

このシナリオでは、ゲストは無線接続でネットワークに接続します。デバイス登録 WebAuth プロセス フローの例については、図 11 : ワイヤレス デバイス登録 Web 認証フロー を参照してください。後続のデバイス登録 WebAuth プロセスの概要を次に説明します。無線接続と有線接続の両方で同様のプロセスとなります。

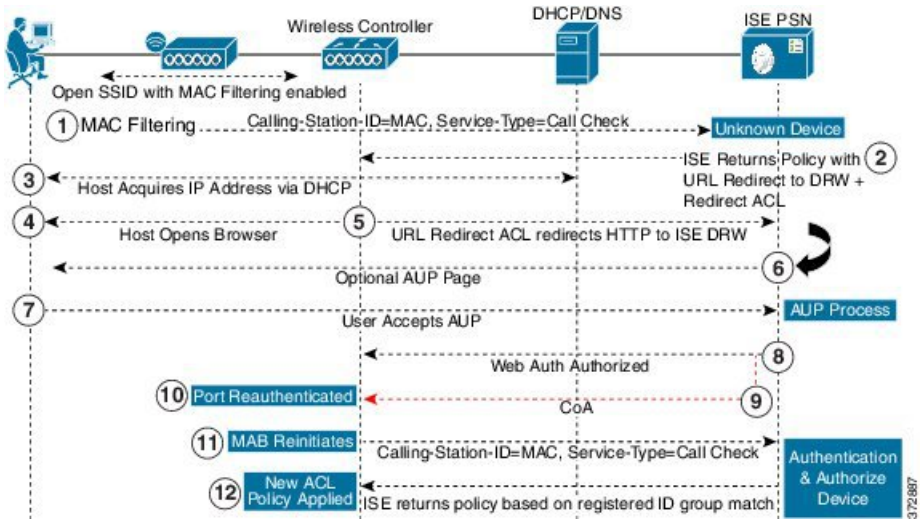
1. ネットワーク アクセス デバイス（NAD）がホットスポット ゲスト ポータルにリダイレクトを送信します。
2. ゲスト デバイスの MAC アドレスがいずれのエンドポイント ID グループにも含まれていないか、利用規定（AUP）accepted 属性が true に設定されていない場合、Cisco ISE は許可プロファイルに指定された URL リダイレクションを使用して応答します。
3. ゲストが何らかの URL にアクセスしようとすると、URL リダイレクションによって AUP ページ（有効な場合）が示されます。
   - ゲストが AUP を受け入れると、デバイスの MAC アドレスに関連付けられたエンドポイントが、設定されたエンドポイント ID グループに割り当てられます。ゲストによる AUP の受け入れを追跡できるよう、この時点で、このエンドポイントの AUP accepted 属性は true に設定されます。
   - ゲストが AUP を受け入れない場合、または、エンドポイントの作成中や更新中などにエラーが発生した場合、エラー メッセージが表示されます。
4. ホットスポット ゲスト ポータルの設定に基づいて、追加情報を含むポスト アクセス バナー ページが表示される場合があります（有効な場合）。
5. エンドポイントが作成または更新された後、許可変更（CoA）終了が NAD に送信されます。
6. CoA の後、NAD は MAC 認証バイパス（MAB）の新しい要求でゲスト接続を再認証します。新規認証では、エンドポイントとそれに関連付けられているエンドポイント ID グループが検索され、設定されているアクセスが NAD に返されます。

7. ホットスポット ゲスト ポータルの設定に基づいて、ゲストは、アクセスを要求した URL、管理者が指定したカスタム URL、または認証の成功ページに誘導されます。

有線とワイヤレスのどちらの場合も、CoA タイプは Termination CoA です。VLAN DHCP リリース（および更新）を実行するようにホットスポット ゲスト ポータルを設定し、それによって、有線と無線の両方の CoA タイプを許可変更に再許可できます。

VLAN DHCP リリースのサポートは、Windows デバイスのみで使用可能です。モバイル デバイスでは利用できません。登録するデバイスがモバイルで、[VLAN DHCP リリース（VLAN DHCP Release）] オプションが有効の場合、ゲストは手動で IP アドレスを更新することを要求されます。モバイル デバイスのユーザの場合は、VLAN を使用するよりも、WLC でアクセス コントロール リスト（ACL）を使用することを推奨します。

図 *11* : ワイヤレス デバイス登録 *Web* 認証フロー



ゲスト ポータル設定

ポータル ID 設定

これらの設定へのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータルまたはスポンサー ポータル（Guest Portals or Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ゲスト ポータルおよびスポンサー ポータルの設定とカスタマイズ（Guest Portals or Sponsor Portals Settings and Customization）]** です。

- ポータル名（Portal Name）：このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル（ブラックリスト、個人所有デバイス持ち込み（BYOD）、クライアントプロビジョニング、モバイルデバイス管理（MDM）、またはデバイスの各ポータル）に使用しないでください。

この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- **説明（Description）**：任意項目です。
- ポータルテスト URL（Portal test URL）：[保存（Save）] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

  リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

  （注） テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。
- 言語ファイル（Language File）：各ポータルタイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

  言語ファイルには、その言語のポータル全体のすべての文字列設定に加え、特定のブラウザのロケール設定（例：フランス語の場合は fr、fr-fr、fr-ca）へのマッピングが含まれています。1 つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

  1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイスポータルにも適用されます。

  [ポータルページのカスタマイズ（Portal Page Customizations）] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に 1 つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

ホットスポット ゲスト ポータルのポータル設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアント プロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- エンドポイント ID グループ（Endpoint identity group）：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。
- __日に達した場合にこの ID グループ内のエンドポイントを消去する（Purge endpoints in this identity group when they reach __ days）：Cisco ISE データベースから消去されるまでの、ユーザのデバイスの登録からの日数を変更します。消去は毎日実行され、消去アクティビティは全体的な消去タイミングと同期されます。変更は、このエンドポイント ID グループ全体に適用されます。

  その他のポリシー条件に基づいてエンドポイント消去ポリシーに変更が加えられた場合、この設定は使用できなくなります。
- **表示言語**
  - [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

ホットスポット ゲスト ポータルの利用規定（AUP）ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]** です。

- [AUP ページを含める（Include an AUP page）]：会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [アクセスコードが必要（Require an access code）]：複数のゲストがネットワークへのアクセスを獲得するために使用する必要があるログイン クレデンシャルとして、アクセス コードを割り当てます。アクセス コードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです（ホワイトボードによって視覚的に、またはロビーアンバサダーにより口頭で）。これは、ネットワークにアクセスするために部外者に認知されることも使用されることもありません。

  個別のゲストにログイン クレデンシャルとして提供されるユーザ名とパスワードに加えて、このオプションを使用できます。
- AUPの最後までのスクロールが必要（Require scrolling to end of AUP）：ユーザが AUP を完全に読んだことを確認します。[同意（Accept）]ボタンは、ユーザがAUPの最後までスクロールするとアクティブになります。AUP がユーザに表示された場合に設定します。

ホットスポット ゲスト ポータルのフローを設定する場合、AUP アクセス コードはエンドポイント ID グループのデバイス登録によって異なります。つまり、[AUPの最後の受け入れとネットワークアクセス：EQUALSゲストフローの使用例（AUP Last Acceptance and Network Access: Use Case EQUALS Guest Flow）] フラグを使用することはできません。ユーザのセッションが接続時に NAD から削除されると、AUP ページが表示されますが、AUP アクセス コードを入力する必要はありません。

AUP アクセス コード ページは、MAC アドレスがホットスポット ポータルの設定に関連付けられたエンドポイントID グループから削除された後にのみ表示されます。エンドポイントは、Cisco ISE の [コンテキストの可視性（Context Visibility）] ページを介してデータベースから手動で削除するか、エンドポイント消去機能を使用し、エンドポイント消去ポリシーを設定して消去します。

ホットスポット ポータルのポストアクセス バナー ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portal s& Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [アクセス後のバナー ページ設定（Post-Access Banner Page Settings）]** です。

この設定を使用して、ゲストにアクセス ステータスおよび必要に応じてその他の追加アクションを通知します。

フィールド	使用上のガイドライン
アクセス後バナー ページを含める（Include a Post-Access Banner page）	ゲストが正常に認証された後、ネットワーク アクセスを付与される前に追加情報を表示します。

クレデンシャルを持つゲスト ポータルのポータル設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアント プロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
- 認証方式（Authentication Method）IDソース順序（Identity source sequence）：ユーザ認証に使用するIDソース順序（ISS）またはIDプロバイダー（IdP）を選択します。ISSは、ユーザ クレデンシャルを確認するために順番に検索されるIDストアのリストです。たとえば、内部ゲストユーザ、内部ユーザ、Active Directory、LDAPディレクトリ などがあります。

  Cisco ISEには、スポンサー ポータル Sponsor_Portal_Sequence用のデフォルトのスポンサーID ソース順序が含まれています。

  IdPを設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

  IDソース順序を設定するには、[管理（Administration）] > [IDの管理（Identity Management）] > [IDソース順序（Identity Source Sequences）] の順に選択します。
- ゲストとしてこのポータルを使用する従業員のログイン オプションの継承元（Employees using this portal as guests inherit login options from）：従業員がこのポータルにログオンしたときに割り当てられるゲスト タイプを選択します。従業員のエンドポイント データは、そのゲスト タイプで属性 [エンドポイント ID グループにデバイス情報を保存する（Store device information in endpoint identity group）] に設定されたエンドポイント ID グループに保存されます。関連付けられたゲスト タイプの他の属性は継承されません。
- **表示言語**
  - [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語がISEでサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語がISEでサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

  [スポンサーに使用可能なSSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前またはSSID（セッション サービス識別子）を入力します。

クレデンシャルを持つゲスト ポータルのログイン ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータ**

ル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ログイン ページの設定（Login Page Settings）] です。

- [アクセスコードが必要（Require an access code）]：複数のゲストがネットワークへのアクセスを獲得するために使用する必要があるログイン クレデンシャルとして、アクセス コードを割り当てます。アクセス コードは、物理的に存在するゲストに対して指定される、主にローカルで認識されるコードです（ホワイトボードによって視覚的に、またはロビー アンバサダーにより口頭で）。これは、ネットワークにアクセスするために部外者に認知されることも使用されることもありません。

  個別のゲストにログイン クレデンシャルとして提供されるユーザ名とパスワードに加えて、このオプションを使用できます。

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザ セッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。

- [頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）]：[頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間（スロットル率）を分単位で設定します。

- [AUPを含める（Include an AUP）]：フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。

  - [同意が必要（require acceptance）]：フローを続行する前に、ユーザが AUP に同意するように強制します。

- [ゲストに自分自身のアカウントの作成を許可（Allow guests to create their own accounts）]：このポータルの [ログイン（Login）] ページで、ゲストが自身を登録するためのオプションが提供されます。このオプションが選択されていない場合は、スポンサーがゲスト アカウントを作成します。これを有効にすることで、このページのタブが有効になり、[アカウント登録ページの設定（Self-Registration Page Settings）]および[アカウント登録成功ページの設定（Self-Registration Success Page Settings）] を設定できます。

  ゲストがこのオプションを選択した場合、自身のゲスト アカウントを作成するために必要な情報を入力できるアカウント登録フォームが示されます。

- [ソーシャルログインを許可（Allow Social Login）]：このポータルのユーザのログイン クレデンシャルを取得するためにソーシャル メディア サイトを使用します。このオプションをチェックすると、次の設定が表示されます。

  - [ソーシャル ログイン後に登録フォームを表示（Show registration form after social login）]：これにより、ユーザは Facebook によって提供される情報を変更できます。

- [ゲストの承認が必要（Require guests to be approved）]：スポンサーがアカウントを承認する必要があることをユーザに通知し、ログイン用のクレデンシャルを送信します。

- [ゲストにログイン後のパスワード変更を許可（Allow guests to change password after login）]：ゲストが正常に認証され、AUPに同意した後に、ゲストに必要に応じてパスワードを変更することを許可します。ゲストが自分のパスワードを変更した場合、スポンサーはゲストにログインクレデンシャル情報を提供できません。スポンサーは、ゲストのパスワードをランダム パスワードにリセットすることだけが可能です。
- [ログインに次の ID プロバイダ ゲスト ポータルの使用を許可（Allow the following identity-provider guest portal to be used for login）]：このオプションをオンにし、SAML Id IDプロバイダを選択すると、その SAML ID のリンクがこのポータルに追加されます。このサブ ポータルは、ユーザが証明書を提供している SAML IDP のように見えるように設定できます。
- [ソーシャル ログインを許可（Allow social login）]：このポータルはすべて、ユーザ ログインにソーシャル メディア タイプを使用します。この項目を選択すると、設定したソーシャル メディア タイプをドロップダウンで選択できます。ソーシャル ログインの設定の詳細については、『』の「アカウント登録ゲストのソーシャル ログイン」のセクションアカウント登録ゲストのソーシャル ログイン （389 ページ）を参照してください。
  - [ソーシャル ログイン後にゲスト フォームを表示（Show guest form after social login）]：このオプションを選択すると、ログオン画面がスキップされます。

アカウント登録ページの設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portal & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [アカウント登録ページの設定（Self-Registration Page Settings）]** です。これらの設定を使用して、ゲストが自身を登録し、提供する必要がある情報をアカウント登録フォームで指定できるようにします。

- [アカウント登録ゲストに割り当てるゲストタイプ（Assign self-registered guests to guest type）]：このポータルを使用するすべてのアカウント登録ゲストに割り当てられるゲストタイプを選択します。
- [アカウントの有効期間（Account valid for）]：アカウントの有効期間を、日、時間、または分で指定します。この期間を超過した場合、管理者またはスポンサーがスポンサー ポータルでアカウント有効期間を延長した場合を除き、アカウントは失効します。
- [アカウント登録に登録コードを必要とする（Require a registration code for self registration）]：アカウント登録ゲストがアカウント登録フォームを正常に送信するために入力する必要があるコードを割り当てます。部外者がシステムにアクセスすることを防ぐために、アクセス コードと同様に、登録コードはオフラインで提供されます。

- [含めるフィールド（Fields to include）]：アカウント登録ページ上で、アカウント登録フォームに表示するフィールドのチェックボックスをオンにします。その後、ゲストがこのフォームを送信してゲストアカウントを受信するために入力が必須であるフィールドのチェックボックスをオンにします。アカウント登録ゲストから重要な情報を収集するために、[SMS サービス プロバイダー（SMS Service Provider）] および [訪問先担当者（Person being Visited）] フィールドを必須にすることができます。
  - [場所（Location）]：アカウント登録のゲストが定義済みリストを使用して登録時に選択できる場所を入力します。これにより、これらのゲストの有効なアクセス時間として自動的に関連するタイムゾーンが割り当てられます。場所の名前は、選択時に混乱を回避するために具体的なものを使用します（たとえば、ボストン オフィス、500 Park Ave New York、シンガポールなど）。

    ゲスト アクセスを時間で制限する予定の場合は、その時間を設定するときにタイムゾーンを使用します。アクセス時間が制御されたゲスト全員がサンノゼのタイムゾーンにいる場合を除き、各自のロケールのタイムゾーンを作成します。場所が1つだけである場合は、その場所がデフォルトの場所として自動的に割り当てられ、ポータルではこのフィールドがゲストに対して表示されません。また、[場所（Location）]は、[含めるフィールド（Fields to include）] のリスト内で無効になります。
  - [SMS サービス プロバイダー（SMS Service Provider）]：アカウント登録フォームに SMS プロバイダーを表示して、アカウント登録ゲストが自分の SMS プロバイダーを選択できるようにします。これで、会社の経費を最小化するために、ゲストの SMS サービスを使用して SMS 通知を送信できるようになります。ゲストが使用できる SMS プロバイダーを 1 つだけ選択した場合は、このフィールドはアカウント登録フォームに表示されません。
  - [訪問先担当者（Person being Visited）]：これはテキスト フィールドであるため、このフィールドを使用する場合には、ゲストに対し、このフィールドに入力する情報について説明してください。
  - [カスタム フィールド（Custom Fields）]：アカウント登録ゲストから追加のデータを収集するために作成したカスタムフィールドを選択します。その後、ゲストがアカウント登録フォームを送信してゲスト アカウントを受信するために入力が必須であるフィールドのチェックボックスをオンにします。これらのフィールドは名前のアルファベット順に表示されます。これらのフィールドは、カスタムフィールドを追加するため、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Settings）] > [カスタム フィールド（Custom Fields）]** で作成します。
  - [AUP を含める（Include an AUP）]：会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
    - [同意が必要（Require acceptance）]：ユーザが AUP を最後まで読んだことを確認します。これにより、アカウント登録ページの [同意する（Accept）] ボタンが設定されます。AUP を [ページ（as on page）] として設定する場合は、ユーザが AUP の終わりまでスクロールするまで [同意する（Accept）] ボタンを無効にすることもできます。

- [次の電子メール アドレスを持つゲストのみを許可（Only allow guests with an email address from）]：アカウント登録ゲストが電子メール アドレスを作成するときに [電子メール アドレス（Email Address）] で使用できるドメイン（例：cisco.com）のホワイトリストを指定します。

  このフィールドを空白のままにすると、[次の電子メール アドレスを持つゲストを許可しない（Do not allow guests with email address from）] にリストされているドメイン以外のすべての電子メール アドレスが有効になります。

- [次の電子メール アドレスを持つゲストを許可しない（Do not allow guests with email address from）]：アカウント登録ゲストが電子メール アドレスを作成するときに [電子メール アドレス（Email Address）] に使用できないドメイン（例：czgtgj.com）のブラックリストを指定します。

- [アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）]：このポータルを使用するアカウント登録ゲストは、ゲストのクレデンシャルを受信する前にスポンサーによる承認が必要であることを指定します。このオプションをクリックすると、スポンサーがアカウント登録ゲストを承認する方法に関する追加のオプションが表示されます。

  - [承認要求電子メール送信先（Email approval request to）]：次のいずれかを選択します。

    - [下に示すスポンサーの電子メールアドレス（sponsor email addresses listed below）]：承認者として指名されたスポンサーの1つ以上の電子メールアドレス、またはすべてのゲストの承認要求の送信先となるメール ソフトウェアを入力します。電子メール アドレスが無効な場合、承認は失敗します。

    - [訪問先担当者（person being visited）]：[スポンサーに承認用クレデンシャルの入力を求める（Require sponsor to provide credentials for authentication）] フィールドが表示され、[含めるフィールド（Fields to include）] の [必須（Required）] オプションが有効になります（以前は無効だった場合）。これらのフィールドはアカウント登録フォームに表示され、アカウント登録ゲストからこの情報を要求します。電子メール アドレスが無効な場合、承認は失敗します。

  - [承認/拒否のリンクの設定（Approve/Deny Link Settings）]：このセクションでは次の内容を設定できます。

    - [リンクの有効期間（Links are valid for）]：アカウント承認リンクの有効期間を設定できます。

    - [スポンサーに承認用クレデンシャルの入力を求める（Require sponsor to provide credentials for authentication）]：このセクションの設定でスポンサーによるアカウント承認用のクレデンシャルの入力が必須ではない場合にも、スポンサーにこの情報を入力させるには、このフィールドをオンにします。このフィールドは、[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] が [訪問先担当者（person being visited）] に設定されている場合にだけ表示されます。

- [承認権限を検証するためスポンサーがスポンサーポータルと照合される（Sponsor is matched to a Sponsor Portal to verify approval privileges）]：[詳細 >（Details >）] をクリックして、スポンサーが有効なシステムユーザであり、スポンサーグループのメンバーであり、そのスポンサーグループのメンバーにアカウント承認権限があることを確認するために検索されるポータルを選択します。各スポンサーポータルには、スポンサーを識別するために使用される ID ソース シーケンスがあります。ポータルはリストされている順序で使用されます。リストの 1 番目のポータルは、スポンサーポータルで使用されているスタイルとカスタマイズ内容を決定します。

- [登録の送信後のゲストの誘導先（After registration submission, direct guest to）]：登録の正常完了後にアカウント登録ゲストを誘導する場所を選択します。
  - [アカウント登録成功（Self-Registration Success）] ページ：アカウント登録に成功したゲストを [アカウント登録成功（Self-Registration Success）] ページに誘導します。このページには、[アカウント登録成功ページ設定（Self Registration Success Page Settings）] で指定したフィールドとメッセージが表示されます。

    すべての情報を表示することが望ましくない場合があります。システムはアカウントの承認待ち（このページで有効になっている場合）であるか、またはこのページで指定されたホワイトリスト、ブラックリスト ドメインに基づいて電子メール アドレスまたは電話番号にログイン クレデンシャルを提供する可能性があるためです。

    [アカウント登録成功ページの設定（Self Registration Success Page Settings）] で [ゲストのアカウント登録成功ページからの直接ログインを許可する（Allow guests to log in directly from the Self-Registration Success page）] を有効にした場合、アカウント登録に成功したゲストはこのページから直接ログインすることができます。これが有効になっていない場合、ゲストは [アカウント登録成功（Self-Registration Success）] ページが表示された後にポータルのログイン ページに誘導されます。

  - [ログインクレデンシャルを取得する方法の手順を含むログインページ（Login page with instructions about how to obtain login credentials）]：アカウント登録に成功したゲストをポータルのログイン ページに再び誘導し、「ゲスト クレデンシャルが電子メール、SMS、または印刷物で提供されるのを待ってからログインに進んでください。」などのメッセージを表示します。

    デフォルト メッセージをカスタマイズするには、[ポータル ページのカスタマイズ（Portal Page Customization）] タブをクリックして、[アカウント登録ページ設定（Self Registration Page Settings）] を選択します。

    システムはアカウントの承認待ち（このページで有効になっている場合）であるか、またはこのページで指定されたホワイトリスト、ブラックリスト ドメインに基づいて電子メール アドレスまたは電話番号にログイン クレデンシャルを提供する可能性があります。

  - [URL]：アカウント登録に成功したゲストを、アカウント クレデンシャルの提供を待機している間に、指定された URL に誘導します。

システムはアカウントの承認待ち（このページで有効になっている場合）であるか、またはこのページで指定されたホワイトリスト、ブラックリストドメインに基づいて電子メール アドレスまたは電話番号にログイン クレデンシャルを提供する可能性があります。

- **[クレデンシャル通知自動送信手段（Send credential notification automatically using）]**：
  - [電子メール（Email）]：アカウント登録に成功したゲストがログイン クレデンシャルを受信する手段のオプションとして電子メールを選択します。このオプションを選択した場合、[電子メール アドレス（Email address）] が [含めるフィールド（Fields to include）] のリストで必須フィールドになり、このオプションを無効にできなくなります。
  - [SMS]：アカウント登録に成功したゲストがログインクレデンシャルを受信する手段のオプションとしてSMSを選択します。このオプションを選択した場合、[SMS サービス プロバイダー（SMS Service Provider）] が [含めるフィールド（Fields to include）] のリストで必須フィールドになり、このオプションを無効にできなくなります。

アカウント登録成功ページの設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portal s& Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [アカウント登録成功ページ設定（Self Registration Success Page Settings）]** です。これらの設定を使用して、正常にアカウント登録したゲストに、ネットワークへのアクセスを獲得するために必要なクレデンシャルを通知します。

フィールド	使用上のガイドライン
アカウント登録の成功ページにこの情報を含める（Include this information on the Self-Registration Success page）	[アカウント登録成功（Self-Registration Success）] ページで正常に登録されたゲストに表示されるフィールドのチェックボックスをオンにします。 スポンサーによるゲストの承認が必要ない場合は、[ユーザ名（Username）] と [パスワード（Password）] のチェックボックスをオンにして、ゲストにこれらのクレデンシャルを表示します。スポンサーの承認が必要な場合、クレデンシャルはゲストが承認された後にのみ提供されるため、これらのフィールドを無効にします。

フィールド	使用上のガイドライン
ゲストは次の手段で情報を自分に送信できる（Allow guest to send information to self using）	正常にアカウント登録したゲストが自分自身にクレデンシャル情報を送信するためのオプションのチェックボックスをオンにします。[印刷（Print）]、[電子メール（Email）]、または [SMS]。
AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）	会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、またはAUPテキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
同意が必要（Require acceptance）	ユーザのアカウントが完全に有効になる前に、ユーザはAUPに同意する必要があります。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。ユーザがAUPに同意しない場合、ネットワークにアクセスできません。
AUPの最後までのスクロールが必要（Require scrolling to end of AUP）	このフィールドは、[ページ上の AUP（AUP on page）] オプションを選択した場合のみ表示されます。 ユーザがAUPを最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。
ゲストをアカウント登録の成功ページから直接ログインできるようにする（Allow guests to log in directly from the Self-Registration Success page）	[アカウント登録の成功（Self-Registration Success）] ページ下部に [ログイン（Login）] ボタンを表示します。これにより、ゲストはログイン ページをバイパスし、自動的にログイン クレデンシャルをポータルに提供して、ポータル フローの次のページ（たとえばAUPページ）を表示できるようになります。

クレデンシャルを持つゲスト ポータルの利用規定（AUP）ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]** です。

- [AUP ページを含める（Include an AUP page）]：会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [従業員に別の AUP を使用する（Use different AUP for employees）]：従業員専用に別の AUP およびネットワーク使用諸条件を表示します。このオプションを選択すると、[従業員用の AUP をスキップ（Skip AUP for employees）] は選択できません。
- [従業員用の AUP をスキップ（Skip AUP for employees）]：従業員は、ネットワークにアクセスする前に AUP に同意する必要はありません。このオプションを選択すると、[従業員に別の AUP を使用する（Use different AUP for employees）] は選択できません。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。

  ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。AUP がユーザに表示された場合に設定します。

  - [初回のログインのみ（On first login only）]：ユーザが初めてネットワークまたはポータルにログインしたときに AUP を表示します。
  - [ログインごと（On every login）]：ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
  - [__ 日ごと（初回のログインから）（Every __ days (starting at first login)）]：ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。

クレデンシャルを持つゲストポータルのゲストによるパスワード変更の設定

ゲストのパスワード変更設定（Guest Change Password Settings）

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ゲストによるパスワード変更設定（Guest Change Password Settings）]** です。

- [ゲストにログイン後のパスワード変更を許可（Allow guests to change password after login）]：ゲストが正常に認証され、AUP に同意した後に、ゲストに必要に応じてパスワードを変更することを許可します。ゲストが自分のパスワードを変更した場合、スポンサーはゲストにログイン クレデンシャル情報を提供できません。スポンサーは、ゲストのパスワードをランダム パスワードにリセットすることだけが可能です。

クレデンシャルを持つゲスト ポータルのゲスト デバイス登録の設定

ゲスト デバイス登録設定（Guest Device Registration Settings）

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ゲスト デバイス登録設定（Guest Device Registration Settings）]** です。

これらの設定を使用して、ゲストがログインしたら Cisco ISE がゲストのデバイスを自動的に登録するようにするか、ゲストがログイン後に手動で自身のデバイスを登録することを許可できます。

各ゲスト タイプの最大デバイス数は、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト タイプ（Guest Types）]** で指定されます。

- [ゲストのデバイスを自動登録（Automatically register guest devices）]：ゲストがこのポータルにアクセスするデバイスのエンドポイントを自動的に作成します。エンドポイントは、このポータルに指定されたエンドポイント ID グループに追加され、。

  許可ルールの作成が可能になり、該当 ID グループ内のエンドポイントへのアクセスが許可されます。そのため、Web 認証は不要になります。

  登録済みデバイスの最大数に到達すると、システムは自動的に最初の登録デバイスを削除し、ゲストがログインしようとしているデバイスを登録し、このことをゲストに通知します。**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト タイプ（Guest Types）]** を選択し、ゲストが登録できるデバイスの最大数を変更します。

- [ゲストにデバイスの登録を許可（Allow guests to register devices）]：ゲストは、名前、説明、および MAC アドレスを入力して、自分のデバイスを手動で登録できます。MAC アドレスはエンドポイント ID グループに関連付けられます。

  登録済みデバイスの最大数に到達した場合に別のデバイスを登録できるようにするには、ゲストは少なくとも 1 個のデバイスを削除する必要があります。

クレデンシャルを持つゲスト ポータルの BYOD 設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [BYOD 設定（BYOD Settings）]** です。

この設定を使用して、従業員などゲスト以外の個人所有デバイスの持ち込み（BYOD）機能を有効にし、クレデンシャルを持つゲストポータルを使用して企業ネットワークにアクセスできるようにします。

フィールド	使用上のガイドライン
従業員がネットワークでパーソナル デバイスを使用することを許可する（Allow employees to use personal devices on the network）	このポータルに [従業員の個人所有デバイス（BYOD）の登録（Employee Bring Your Own Device (BYOD) Registration）] ページを追加して、従業員がデバイス登録プロセスを実行できるようにして、場合によってはネイティブ サプリカントおよび証明書のプロビジョニングを実行できるようにします。これは、従業員のパーソナル デバイス タイプ（iOS、Android、RT またはモバイルを除く Windows、OSX など）のクライアント プロビジョニングの設定に応じて異なります。
エンドポイント ID グループ（Endpoint Identity Group）	ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。
従業員にゲスト アクセスの選択のみを許可する（Allow employees to choose to get guest access only）	従業員をゲスト ネットワークにアクセスさせて、企業ネットワークへのアクセスに必要になることがある追加のプロビジョニングおよび登録を避けます。
登録時にデバイス ID フィールドを表示する（Display Device ID field during registration）	登録プロセス中に、デバイス ID をユーザに表示します。これは、デバイス ID が事前設定されており、BYOD ポータルを使用しているときに変更できない場合も含みます。

フィールド	使用上のガイドライン
元の URL（Originating URL）	ネットワークへの認証に成功すると、可能な場合はユーザのブラウザを、ユーザがアクセスしようとしていた元の Web サイトにリダイレクトします。リダイレクトできない場合は、認証成功ページが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。 Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザード アプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS（dot1X）およびサポート対象外のデバイス（ネットワーク アクセスが許可されている）では、この URL にリダイレクトされます。
成功ページ（Success page）	デバイスの登録が成功したことを示すページを表示します。
URL	ネットワークへの認証に成功すると、ユーザのブラウザを指定された URL（会社の Web サイトなど）にリダイレクトします。

クレデンシャルを持つゲスト ポータルのポストログイン バナー ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portal s& Components）] > [ゲスト ポータルまたはスポンサー ポータル（Guest Portals or Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポストログインバナーページ設定（Post-Login Banner Page Settings）]** です。

これらの設定を使用して、正常なログイン後にユーザ（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

フィールド	使用上のガイドライン
ポストログイン バナー ページを含める（Include a Post-Login Banner page）	ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

クレデンシャルを持つゲスト ポータルのゲスト デバイスのコンプライアンス設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ゲスト デバイスのコンプライアンス設定（Guest Device Compliance Settings）]** です。これらの設定を使用して、ネットワークにアクセスするためにデバイスのクライアントプロビジョニングを実行するようゲストおよびゲスト ポータルを使用する従業員に要求します。

- [ゲスト デバイス コンプライアンスが必要（Require guest device compliance）]：ゲストをポスチャ エージェントのダウンロードを要求する[クライアントプロビジョニング（Client Provisioning）] ページにリダイレクトします。これにより、ウイルス対策ソフトウェアのチェックなど、ゲストのポスチャ ポリシーを設定するゲスト フローにクライアント プロビジョニングが追加されます。

  ゲストが、ネットワークへのアクセスにクレデンシャルを持つゲストポータルを使用している従業員の場合：

  - [BYOD 設定（BYOD Settings）] で [従業員にネットワークでのパーソナル デバイスの使用を許可する（Allow employees to use personal devices on the network）] が有効になっている場合、従業員はBYODフローにリダイレクトされ、クライアントのプロビジョニングは実行されません。
  - [BYOD 設定（BYOD Settings）] で [従業員にネットワークでのパーソナル デバイスの使用を許可する（Allow employees to use personal devices on the network）] および [従業員にゲスト アクセスの選択のみを許可する（Allow employees to choose to get guest access only）] が有効になっていて、従業員がゲスト アクセスを選択する場合、[クライアント プロビジョニング（Client Provisioning）] ページにルーティングされます。

ゲスト ポータルの VLAN DHCP リリース ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portal s& Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [VLAN DHCP リリース ページの設定（VLAN DHCP Release Page Settings）]** です。

- [VLAN DHCPリリースを有効にする（Enable VLAN DHCP release）]：有線環境と無線環境の両方でVLANが変更された後、WindowsデバイスのゲストのIPアドレスを更新します。

  これは、ネットワーク アクセスでゲスト VLAN が新しい VLAN に変更されたときに、最終的な許可処理時の中央 WebAuth（CWA）フローに影響します。ゲストの古い IP アドレスは VLAN の変更の前にリリースされる必要があり、ゲストが新しい VLAN に接続するときに新しいゲスト IP アドレスが DHCP を介して要求される必要があります。IP アドレ

スのリリースと更新操作は、DirectX コントロールを使用する Internet Explorer ブラウザのみでサポートされています。

VLAN DHCP リリース オプションは、モバイル デバイスでは動作しません。代わりに、ゲストが IP アドレスを手動でリセットする必要があります。この方法はデバイスによって異なります。たとえば、Apple iOS デバイスでは、ゲストは Wi-Fi ネットワークを選択して、[リースを更新（Renew Lease）] ボタンをクリックできます。

- [リリースを__秒遅延（Delay to release __ seconds）]：リリース遅延時間を入力します。リリースは、アプレットをダウンロードした直後から、Cisco ISE サーバが CoA 要求を再認証するよう NAD に指示するまでの間に行う必要があるため、この時間は短くすることを推奨します。
- [CoA を__秒遅延（Delay to CoA __ seconds）]：Cisco ISE が CoA の実行を遅延する時間を入力します。十分な時間を指定して（ガイドラインとしてデフォルト値を使用）、アプレットによるクライアント上での IP リリースのダウンロードと実行を可能にします。
- [更新を__秒遅延（Delay to renew __ seconds）]：更新を遅延する値を入力します。この時間は IP リリース値に追加され、コントロールがダウンロードされるまで計時が開始されません。十分な時間を指定して（ガイドラインとしてデフォルト値を使用）、CoA の処理を可能にし、新しい VLAN アクセスが付与されるようにします。

ゲスト ポータルの認証成功の設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [認証成功の設定（Authentication Success Settings）]** です。

これらの設定では、ユーザ（状況に応じてゲスト、スポンサーまたは従業員）に認証の成功が通知されるか、または URL が表示されます。[認証されたらゲストに次を表示：（Once authenticated, take guest to:）] で、次のフィールドを設定します。

- 元の URL（Originating URL）：ネットワークへの認証に成功すると、可能な場合はユーザのブラウザを、ユーザがアクセスしようとしていた元の Web サイトにリダイレクトします。リダイレクトできない場合は、認証成功ページが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。

  Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザード アプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS（dot1X）およびサポート対象外のデバイス（ネットワーク アクセスが許可されている）では、この URL にリダイレクトされます。

- 認証の成功ページ（Authentication Success page）：ユーザの認証に成功した通知。

• URL：ネットワークへの認証に成功すると、ユーザのブラウザを指定されたURL（会社のWeb サイトなど）にリダイレクトします。

（注） 認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。リダイレクトURLがNADのアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。

ゲスト ポータルのサポート情報ページの設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [サポート情報ページの設定（Support Information Page Settings）]** です。

これらの設定を使用して、ヘルプデスクがユーザ（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

フィールド	使用上のガイドライン
サポート情報ページを含める（Include a Support Information Page）	該当ポータルのすべての有効なページ上で、**問い合わせ先**などの情報へのリンクを表示します。
MAC アドレス	[サポート情報（Support Information）] ページにデバイスの MAC アドレスを含めます。
IP アドレス	[サポート情報（Support Information）] ページにデバイスの IP アドレスを含めます。
ブラウザのユーザ エージェント（Browser user agent）	[サポート情報（Support Information）] ページに、要求の発信元のユーザ エージェントの製品名とバージョン、レイアウトエンジン、バージョンなど、ブラウザの詳細を含めます。
ポリシー サーバ（Policy server）	[サポート情報（Support Information）] ページに、このポータルを提供しているISEポリシー サービス ノード（PSN）の IP アドレスを含めます。

フィールド	使用上のガイドライン
障害コード（Failure code）	可能な場合は、ログ メッセージ カタログ内の対応する番号を含めます。メッセージ カタログにアクセスしてこれを表示するには、**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[メッセージ カタログ（Message Catalog）]** に移動します。
フィールドを隠す（Hide field）	含める情報が存在しない場合、[サポート情報（Support Information）] ページ上の該当するフィールドラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード（Failure code）] は、選択されている場合でも表示されません。
値のないラベルを表示（Display label with no value）	含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを[サポート情報（Support Information）]ページに表示します。たとえば、障害コードが不明な場合、[障害コード（Failure code）] は空白であっても表示されます。
デフォルト値でラベルを表示（Display label with default value）	[サポート情報（Support Information）] ページ上の選択されているフィールドに含まれる情報が存在しない場合、このテキストがこれらのすべてのフィールドに表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード（Failure code）] に [使用できません（Not Available）] と表示されます。

スポンサー ポータル アプリケーションの設定

ポータル ID 設定

これらの設定へのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータルまたはスポンサー ポータル（Guest Portals or Sponsor Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ゲスト ポータルおよびスポンサー ポータルの設定とカスタマイズ（Guest Portals or Sponsor Portals Settings and Customization）]** です。

- ポータル名（Portal Name）：このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル（ブラックリスト、個人所有デバイス持ち込み（BYOD）、クライアント プロビジョニング、

モバイルデバイス管理（MDM）、またはデバイスの各ポータル）に使用しないでください。

この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- **説明（Description）**：任意項目です。
- ポータルテスト URL（Portal test URL）：[保存（Save）] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

  リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

  （注） テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。
- 言語ファイル（Language File）：各ポータルタイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

  言語ファイルには、その言語のポータル全体のすべての文字列設定に加え、特定のブラウザのロケール設定（例：フランス語の場合は fr、fr-fr、fr-ca）へのマッピングが含まれています。1 つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

  1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイスポータルにも適用されます。

  [ポータルページのカスタマイズ（Portal Page Customizations）] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に 1 つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

スポンサー ポータルのポータル設定

これらの設定を設定して、ポータルを特定し、すべてのポータルページで使用する言語ファイルを選択します。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアント プロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディングインターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：スポンサーまたはデバイス ポータルに対応する 1 つの固有の FQDN またはホスト名を入力します。たとえば、**sponsorportal.yourcompany.com,sponsor** と入力することで、ユーザはブラウザにこれらのいずれかを入力すると、スポンサー ポータルが表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

  デフォルトの FQDN を変更する場合は、次を実行します。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

- 認証方式（Authentication Method）IDソース順序（Identity source sequence）：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP ディレクトリ などがあります。

  Cisco ISE には、スポンサー ポータル Sponsor_Portal_Sequence 用のデフォルトのスポンサー ID ソース順序が含まれています。

  IdP を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

  ID ソース順序を設定するには、[管理（Administration）] > [IDの管理（Identity Management）] > [IDソース順序（Identity Source Sequences）] の順に選択します。

- [アイドル タイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。
- [Kerberosを許可する（Allow Kerberos）]：スポンサー ポータルへアクセスするためのスポンサーの認証に Kerberos を使用します。ブラウザが ISE との SSL 接続を確立した後、セキュア トンネル内で Kerberos SSO が実行されます。

（注） Kerberos 認証には、同じドメイン内に存在する次の項目が必要です。

- スポンサーの PC
- ISE PSN
- このスポンサー ポータルに設定された FQDN

（注） ゲスト ポータルの Kerberos 認証はサポートされていません。

- **表示言語**
  - [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

- [スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

スポンサー ポータルのログイン設定

スポンサー ポータルのログイン ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Sponsor Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ログイン ページの設定（Login Page Settings）]** です。

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザ セッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）]：[頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間（スロットル率）を分単位で設定します。
- [AUPを含める（Include an AUP）]：フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
  - [同意が必要（require acceptance）]：フローを続行する前に、ユーザが AUP に同意するように強制します。

スポンサー ポータルの利用規定（AUP）設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]** です。

これらの設定を使用して、ユーザ（状況に応じてゲスト、スポンサーまたは従業員）に対して AUP エクスペリエンスを定義します。

フィールド	使用上のガイドライン
AUP ページを含める（Include an AUP page）	会社のネットワーク使用諸条件を、別のページでユーザに表示します。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。
初回のログインのみ（On first login only）	ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUPを表示します。
ログインごと（On every login）	ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
__日ごと（初回のログインから）（Every __ days (starting at first login)）	ユーザがネットワークまたはポータルに初めてログインした後に、定期的にAUPを表示します。

スポンサー ポータルのスポンサーのパスワード変更設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [スポンサーによるパスワード変更設定（Sponsor Change Password Settings）]** です。これらの設定により、スポンサー ポータルを使用するスポンサーのパスワード要件が定義されます。

すべてのユーザのパスワード ポリシーを設定するには、**[管理（Administration）] > [IDの管理（Identity Management）] > [設定（Settings）] > [ユーザパスワードポリシー（User Password Policy）]** を選択します。

フィールド	使用上のガイドライン
スポンサーは自身のパスワードを変更可能（Allow sponsors to change their own passwords）	スポンサーは、スポンサー ポータルにログインした後、自身のパスワードを変更できます。このオプションは、スポンサーが内部ユーザ データベースの一部である場合にだけ、[パスワードの変更（Change Password）] ページを表示します。

スポンサー ポータルのポストログイン バナー設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portal s& Components）] > [ゲスト ポータルまたはスポンサー ポータル（Guest Portals or Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポストログインバナーページ設定（Post-Login Banner Page Settings）]** です。

これらの設定を使用して、正常なログイン後にユーザ（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

フィールド	使用上のガイドライン
ポストログイン バナー ページを含める（Include a Post-Login Banner page）	ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

スポンサー ポータルのサポート情報ページの設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [サポート情報ページの設定（Support Information Page Settings）]** です。

これらの設定を使用して、ヘルプデスクがユーザ（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

フィールド	使用上のガイドライン
サポート情報ページを含める（Include a Support Information Page）	該当ポータルのすべての有効なページ上で、**問い合わせ先**などの情報へのリンクを表示します。
MAC アドレス	[サポート情報（Support Information）] ページにデバイスの MAC アドレスを含めます。
IP アドレス	[サポート情報（Support Information）] ページにデバイスの IP アドレスを含めます。
ブラウザのユーザ エージェント（Browser user agent）	[サポート情報（Support Information）] ページに、要求の発信元のユーザ エージェントの製品名とバージョン、レイアウトエンジン、バージョンなど、ブラウザの詳細を含めます。
ポリシー サーバ（Policy server）	[サポート情報（Support Information）] ページに、このポータルを提供している ISE ポリシー サービス ノード（PSN）の IP アドレスを含めます。
障害コード（Failure code）	可能な場合は、ログ メッセージ カタログ内の対応する番号を含めます。メッセージ カタログにアクセスしてこれを表示するには、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージ カタログ（Message Catalog）]** に移動します。
フィールドを隠す（Hide field）	含める情報が存在しない場合、[サポート情報（Support Information）] ページ上の該当するフィールドラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード（Failure code）] は、選択されている場合でも表示されません。
値のないラベルを表示（Display label with no value）	含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを [サポート情報（Support Information）] ページに表示します。たとえば、障害コードが不明な場合、[障害コード（Failure code）] は空白であっても表示されます。

フィールド	使用上のガイドライン
デフォルト値でラベルを表示（Display label with default value）	[サポート情報（Support Information）] ページ上の選択されているフィールドに含まれる情報が存在しない場合、このテキストがこれらのすべてのフィールドに表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード（Failure code）] に [使用できません（Not Available）] と表示されます。

スポンサー ポータルのゲストへの通知のカスタマイズ

これらの設定へのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ゲストへの通知（Notify Guests）]** です。

[ページのカスタマイズ（Page Customizations）] で、スポンサーがスポンサー ポータルからゲストに送信する通知に表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

[設定（Settings）] では、スポンサーが電子メールまたは SMS を使用してゲストにユーザ名とパスワードを個別に送信できるかどうかを指定できます。また、ヘルプデスクがアクセスの問題をトラブルシューティングするために使用できる情報を提供するために、スポンサーがゲストに [サポート情報（Support Information）] ページを表示できるかどうかを指定できます。

スポンサー ポータルのカスタマイズの管理と承認

これらの設定へのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [管理と承認（Manage and Approve）]** です。

[ページのカスタマイズ（Page Customizations）] で、スポンサー ポータルの [管理と承認（Manage and Approve）] タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

これらには、アカウント（登録済みおよび保留）の概要および詳細ビュー、スポンサーがゲストアカウントに対して実行する編集、拡張、一時停止などの操作に基づいて表示されるポップアップ ダイアログ、さらに汎用ポータルやアカウント アクション メッセージが含まれています。

グローバル設定

ゲストおよびスポンサー ポータルのグローバル設定

[ゲスト アクセス（Guest Access）] > **[設定（Settings）]** を選択します。Cisco ISE 内のゲスト ポータル、スポンサー ポータル、ゲスト タイプ、およびスポンサー グループに適用される、次の一般設定を設定できます。

- ゲスト アカウントの消去、およびユーザ名とパスワードの生成のポリシー。
- 電子メールおよび SMS 通知をゲスト アカウントとスポンサーに送信するときに使用する SMTP サーバおよび SMS ゲートウェイ。
- アカウント登録ゲスト ポータルを使用したゲスト アカウントの作成およびゲストの登録時に選択する場所、タイム ゾーン、SSID およびカスタム フィールド。

これらのグローバル設定を指定すると、特定のゲスト ポータルとスポンサー ポータル、ゲスト タイプおよびスポンサー グループの設定時にそれらを必要に応じて使用できます。

[ポータル設定（Portal settings）] ページには、次のタブがあります。

- [ゲストアカウントの消去ポリシー（Guest Account Purge Policy）]：期限が切れたゲスト アカウントを消去する時期をスケジューリングします。詳細については、期限切れのゲスト アカウントを消去するスケジューリング設定 （378 ページ）を参照してください。
- [カスタムフィールド（Custom Fields）]：ユーザから追加情報を取得するためにゲスト ポータルで使用するカスタム フィールドを追加します。詳細については、ゲスト アカウント作成用のカスタム フィールドの追加 （379 ページ）を参照してください。
- [ゲスト電子メールの設定（Guest Email Settings）]：アカウントの変更をゲストに電子メール通知するかどうかを決定します。詳細については、電子メールでの通知用の電子メール アドレスおよび SMTP サーバの指定 （380 ページ）を参照してください。
- [ゲストのロケーションおよびSSID（Guest Locations and SSIDs）]：ロケーションと、ゲストがそのロケーションで使用できるネットワークのサービス セット識別子（SSID）を設定します。詳細については、ゲストのロケーションおよびSSIDの割り当て （381 ページ）を参照してください。
- [ゲストユーザ名ポリシー（Guest Username Policy）]：ゲスト ユーザ名の作成方法を設定します。詳細については、ゲスト ユーザ名ポリシーの設定 （384 ページ）およびゲスト パスワード ポリシーのルール （382 ページ）を参照してください。
- [ゲストパスワードポリシー（Guest Password Policy）]：すべてのゲスト ポータルとスポンサー ポータルのゲスト パスワード ポリシーを定義します。詳細については、ゲスト パスワード ポリシーと有効期限の設定 （383 ページ）を参照してください。
- [ロギング（Logging）]：ゲスト ユーザは、デバイスの MAC アドレスで追跡されます。ゲスト ユーザがレポートに表示される場合、ユーザ名は MAC アドレスです。このオプショ

ンを選択すると、ユーザ名として MAC アドレスではなく、ポータル ユーザ ID がレポートに表示されます。このオプションの詳細については、ゲスト ユーザ情報を保存 （413 ページ）を参照してください。

ゲスト タイプの設定

これらの設定のナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト タイプ（Guest Types）]** です。これらの設定を使用して、ネットワークにアクセスできるゲストのタイプおよびそのアクセス権限を作成します。また、このタイプのゲストを作成できるスポンサー グループを指定できます。

- [ゲストタイプ名（Guest type name）]：このゲスト タイプを他のゲスト タイプと区別する名前（1 ～ 256 文字）を指定します。
- [説明（Description）]：このゲスト タイプの推奨される使用方法に関する追加情報（最大 2000 文字）を指定します。たとえば、アカウント登録ゲスト用。ゲスト アカウントの作成に使用しない、など。
- [言語ファイル（Language File）]：このフィールドでは、サポート対象のすべての言語で、電子メールの件名、電子メール メッセージ、および SMS メッセージの内容を含む言語ファイルをエクスポートおよびインポートできます。これらの言語とコンテンツは、アカウントが期限切れになった旨の通知に使用され、このゲスト タイプに割り当てられているゲストに送信されます。新しいゲスト タイプを作成すると、ゲスト タイプを保存するまではこの機能は無効です。言語ファイルの編集の詳細については、ポータル言語のカスタマイズ （518 ページ） を参照してください。
- [追加データを収集（Collect Additional Data）]：[カスタムフィールド...（Custom Fields...）] ボタンをクリックして、このゲスト タイプを使用しているゲストから追加データを収集するために使用するカスタム フィールドを選択します。

  カスタム フィールドを管理するには、**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[設定（Settings）]** > **[カスタムフィールド（Custom Fields）]** を選択します。
- **最大アクセス時間（Maximum Access Time）**
  - [アカウント期間の開始（Account duration starts）]：[最初のログインから（From first login）] を選択した場合、アカウントの開始時間は、ゲスト ユーザがゲスト ポータルに最初にログインしたときに開始され、終了時間は指定された期間に相当します。ゲスト ユーザがログインしなければ、アカウントがゲスト アカウント消去ポリシーによって削除されるまで、アカウントは `Awaiting first login` 状態のままになります。

    値は、1 から 999 日、時間、または分です。

    アカウント登録ユーザのアカウントは、ユーザがアカウントを作成し、自分のアカウントにログオンしたときに開始されます。

[スポンサーが指定した日付から（From sponsor-specified date）] を選択した場合は、このゲスト タイプのゲストがネットワークにアクセスして接続を保持できる最大日数、時間数、または分数を入力します。

この設定を変更した場合、変更内容はこのゲストタイプを使用して作成された既存のゲスト アカウントには適用されません。

- [最大アカウント期間（Maximum account duration）]：このゲスト タイプが割り当てられているゲストがログインできる期間（日数、時間数、または分数）を入力します。

（注） アカウント消去ポリシーにより期限切れのゲストアカウントが確認され、期限切れ通知が送信されます。このポリシーは 20 分ごとに実行されるため、アカウント期間を 20 分未満に設定すると、アカウントの消去前に期限切れ通知が送信されることがあります。

[アクセスを許可する日付と時刻（Allow access only on these days and times）] オプションを使用して、このゲストタイプのゲストにアクセスを提供する期間や曜日を指定できます。

- 選択した曜日によって、スポンサーのカレンダーで選択できる日付へのアクセスが制限されます。
- スポンサーが期間と日付を選択すると、スポンサー ポータルで最大アカウント期間が適用されます。

ここで設定するアクセス時刻の設定は、ゲスト アカウントの作成時にスポンサー ポータルで使用できる時刻設定に影響します。詳細については、スポンサーに対して使用可能な時間設定項目の設定 （427 ページ）を参照してください。

- **ログイン オプション**
  - [最大同時ログイン数（Maximum simultaneous logins）]：このゲスト タイプに割り当てられたユーザが同時に実行できる最大ユーザ セッション数を入力します。
  - [ゲストが制限を超えた場合（When guest exceeds limit）]：[最大同時ログイン数（Maximum simultaneous logins）] を選択した場合は、その最大ログイン数に到達した後でユーザが接続したときに実行するアクションも選択する必要があります。
    - **最も古い接続を切断（Disconnect the oldest connection）**
    - [最も新しい接続を切断（Disconnect the newest connection）]：[エラーメッセージを示すポータルページにユーザをリダイレクトする（Redirect user to a portal page showing an error message）] をオプションで選択：特定の時間にわたってエラーメッセージが表示され、その後セッションが切断されてユーザがゲストポータルにリダイレクトされます。エラーメッセージが表示される時間は設定可能です。エラー ページの内容は、**[メッセージ（Messages）] > [エラーメッセージ（Error**

Messages）] ページの [ポータルページのカスタマイズ（Portal Page Customization）] ダイアログで設定します。

- [ゲストが登録できるデバイスの最大数（Maximum devices guests can register）]：各ゲストに登録できるデバイスの最大数を入力します。そのゲストタイプのゲストに登録済みの値より小さい値を最大数として設定できます。この値は、新しく作成されたゲストアカウントにのみ適用されます。新しいデバイスを追加し、最大数に達すると、最も古いデバイスが切断されます。
- [ゲストデバイス登録のためのエンドポイントIDグループ（Endpoint identity group for guest device registration）]：ゲストのデバイスに割り当てるエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。
- [ゲストに対しゲストポータルのバイパスを許可する（Allow guest to bypass the Guest portal）]：クレデンシャルを持つゲスト タイプのキャプティブ ポータル（Web 認証ページ）をバイパスし、有線およびワイヤレス（dot1x）サプリカントまたは VPN クライアントに認証情報を提供することでネットワークにアクセスすることをユーザに許可します。ゲスト アカウントは、AUP が必要な場合でも、[初期ログインを待機（Awaiting Initial Login）] 状態と AUP ページをバイパスして [アクティブ（Active）] 状態になります。

  この設定を有効にしない場合、ユーザは初めにクレデンシャルを持つゲストのキャプティブポータルを使用してログインしないと、ネットワークの他の部分にアクセスできません。

• アカウント有効期限通知

- [アカウント有効期限の __ 日前にアカウント有効期限通知を送信する（Send account expiration notification __ days before account expires）]：アカウントが期限切れになる前にゲストに通知を送信します。有効期限前の日数、時間数、または分数を指定します。
- [メッセージ表示原語（View messages in）]：電子メールまたは SMS 通知の表示言語を指定します。
- [電子メール（Email）]：アカウント有効期限通知を電子メールで送信します。
- [次のポータルのカスタマイズを使用する（Use customization from）]：選択したポータルに対して設定した同一のカスタマイズ内容をこのゲストタイプのアカウント有効期限メールに適用します。
- [テキストのコピー元（Copy text from）]：別のゲスト タイプのアカウント有効期限メールに、作成した電子メール テキストを再利用します。

• テスト電子メールの送信先（Send test email to me at）

- [SMS]：アカウント有効期限通知を SMS で送信します。

SMS の設定は、電子メール通知の設定と同一ですが、[テスト SMS の送信（Send test SMS to me）] の SMS ゲートウェイを選択する点が異なります。

- [スポンサーグループ（Sponsor Groups）]：このゲスト タイプを使用してメンバーがゲスト アカウントを作成できるスポンサー グループを指定します。このゲスト タイプにアクセスできないようにするスポンサー グループは削除します。

スポンサー グループ設定

これらの設定のナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー グループ（Sponsor Groups）]** です。スポンサー グループにメンバーを追加したり、ゲスト タイプおよびロケーション特権を定義したり、ゲストアカウントの作成と管理に関連する権限を設定したりする場合に、これらの設定を使用します。

- [スポンサー グループの無効化（Disable Sponsor Group）]：このスポンサー グループのメンバーがスポンサー ポータルにアクセスできないようにします。

  たとえば、管理者ポータルで設定を変更している間、スポンサーが一時的にスポンサー ポータルにログインできないようにします。あるいは、再びアクティブ化する必要があるまで、年次会議のスポンサーシップ ゲストなど、頻繁には発生しないアクティビティに関するスポンサー グループを無効にします。

- スポンサー グループ名（Sponsor group name）：一意の名前を入力します（1 ～ 256 文字）。

- [説明（Description）]：このスポンサー グループで使用されるゲスト タイプなどの有益な情報を入力します（最大 2000 文字）。

- [ゲスト タイプの設定（Configure Guest Types）]：必要とするゲスト タイプが使用可能でない場合は、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト タイプ（Guest Types）]** の順にクリックし、新しいゲスト タイプを作成するか、または既存のゲスト タイプを編集します。

- **一致基準**

  - メンバー（Members）：[スポンサー グループ メンバーの選択（Select Sponsor Group Members）] ボックスを表示する場合にクリックします。ここでは、使用可能なユーザ ID グループを（内部および外部の ID ストアから）選択し、このスポンサー グループのメンバーとして追加できます。

    - スポンサー グループ メンバー（Sponsor Group Members）：選択したスポンサー グループのリストを検索およびフィルタリングし、含めないグループを削除します。

  - その他の条件（Other conditions）：[新しい条件の作成（Create New Condition）] をクリックして、このスポンサー グループに含まれるためにスポンサーが満たす必要がある条件を 1 つ以上構築します。Active Directory、LDAP、SAML、ODBC の ID ストア

からの認証属性を使用できますが、RADIUS トークンまたは RSA SecurID ストアは使用できません。内部ユーザ属性も使用できます。条件には、属性、演算子、値があります。

- ディクショナリ属性 *Name* を使用して条件を作成するには、ID グループ名の前にユーザ ID グループを付けます。次に例を示します。

  InternalUser:Name EQUALS bsmith

  この場合、「bsmith」という名前の内部ユーザだけがこのスポンサー グループに所属できます。

- このスポンサー グループはこれらのゲスト タイプを使用してアカウントを作成可能（This sponsor group can create accounts using these guest types）：このスポンサー グループのメンバーがゲスト アカウントの作成時に使用できるゲスト タイプを指定します。有効にするスポンサー グループには、使用できる少なくとも 1 つのゲスト タイプが設定されている必要があります。

  このスポンサー グループに 1 つのゲスト タイプのみを割り当てる場合、それが使用可能な唯一の有効なゲストであるため、スポンサー ポータルに表示しないことを選択できます。**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portal）] > [ページ カスタマイズ（Page Customization）] > [アカウントの作成（Create Accounts）] > [ゲスト タイプ（Guest Types）] > [設定（Settings）]** の順に選択します。このオプションを有効にするには、[スポンサーで1つのみ使用できる場合はゲストタイプを非表示（Hide guest type if only one is available to sponsor）] をオンにします。

- ゲストがアクセスするロケーションを選択（Select the locations that guests will be visiting）：このグループのスポンサーがアカウントの作成時にゲストに割り当てることができるさまざまなロケーションを選択します。このことは、これらのゲストアカウントの有効な時間帯を定義し、有効なアクセス時間などゲストに適用するすべての時間パラメータを指定する場合に役立ちます。このことによって、ゲストが他のロケーションからネットワークに接続できなくなることはありません。

  有効にするスポンサー グループには、使用できる少なくとも 1 つのロケーションが設定されている必要があります。

  このスポンサー グループに 1 つのロケーションのみを割り当てると、それが、メンバーが作成するゲスト アカウントの唯一の有効な時間帯になります。デフォルトでは、スポンサー ポータルに表示されません。

スポンサーが作成可能（Sponsor Can Create）

- 特定のゲストに割り当てられた複数のゲスト アカウント（インポート）（Multiple guest accounts assigned to specific guests (Import)）：スポンサーは、ファイルから姓名などのゲストの詳細をインポートすることによって、複数のゲスト アカウントを作成できます。

  このオプションが有効である場合、[インポート（Import）] ボタンがスポンサー ポータルの [アカウントの作成（Create Accounts）] ページに表示されます。[インポート（Import）]

オプションは、Internet Explorer、Firefox、Safari などのデスクトップ ブラウザだけで使用可能です（モバイルは不可）

- バッチ処理の制限（Limit to batch of）：このスポンサー グループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲスト アカウントの数を指定します。

  スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- ゲストへの複数のゲスト アカウントの割り当て（ランダム）（Multiple guest accounts to be assigned to any guests (Random)）：スポンサーが、未知のゲストのプレースホルダとして、または複数のアカウントをすばやく作成する必要がある場合に複数のランダム ゲスト アカウントを作成できるようにします。

  このオプションが有効である場合、[ランダム（Random）] ボタンがスポンサー ポータルの [アカウントの作成（Create Accounts）] ページに表示されます。

- デフォルト ユーザ名プレフィックス（Default username prefix）：スポンサーが複数のランダムなゲスト アカウントを作成する場合に使用できるユーザ名プレフィックスを指定します。指定した場合、このプレフィックスはランダムなゲスト アカウントを作成するときにスポンサー ポータルに表示されます。また、[スポンサーにユーザ名プレフィックスの指定を許可（Allow sponsor to specify a username prefix）] の設定により、次のようになります。

  - 有効：スポンサーは、スポンサー ポータルでデフォルトのプレフィックスを編集できます。
  - 無効：スポンサーは、スポンサー ポータルでデフォルトのプレフィックスを編集できません。

  ユーザ名プレフィックスを指定しないか、またはスポンサーにユーザ名プレフィックスの指定を許可しない場合、スポンサーはスポンサー ポータルでユーザ名プレフィックスを割り当てることができません。

- スポンサーにユーザ名プレフィックスの指定を許可（Allow sponsor to specify a username prefix）：このスポンサー グループが複数のアカウントを同時に作成できる場合、単一のインポート操作で作成可能なゲスト アカウントの数を指定します。

  スポンサーは最大 10,000 個のアカウントを作成できますが、潜在的なパフォーマンスの問題があるため、作成するアカウントの数を制限することを推奨します。

- 開始日を__日後より遅くすることはできない（Start date can be no more than __ days into the future）：有効にして日数を指定すると、作成した複数のゲスト アカウントの開始日をこの日数以内に設定する必要があります。

スポンサーが管理可能（Sponsor Can Manage）

- スポンサーが作成したアカウントのみ（Only accounts sponsor has created）：このグループのスポンサーは、スポンサーの電子メールアカウントに基づいて、スポンサーが作成したゲスト アカウントのみを表示および管理できます。
- このスポンサー グループのメンバーによって作成されたアカウント（Accounts created by members of this sponsor group）：このグループのスポンサーは、このスポンサー グループ内のスポンサーが作成したゲスト アカウントを表示および管理できます。
- すべてのゲスト アカウント（All guest accounts）：スポンサーはすべての保留中のゲスト アカウントを表示および管理できます。

（注） [アカウント登録ゲストからの要求の承認および表示（Approve and view requests from self-registering guests）] にマークを付けて、[スポンサーが可能（Sponsor Can）] の下で [このスポンサーに割り当てられた保留中のアカウントのみ（Only pending accounts assigned to this sponsor）] オプションを使用していない限り、グループ メンバーシップにかかわらず、すべてのスポンサーがすべての保留中のアカウントを表示できます。

スポンサーが可能（Sponsor Can）

- ゲストの連絡先情報（電子メール、電話番号）の更新（Update guests' contact information (email, Phone Number)）：スポンサーは、自分が管理できるゲスト アカウントについて、ゲストの連絡先情報を変更できます
- ゲストのパスワードの表示/印刷（View/print guests' passwords）：これをオンにすると、スポンサーはゲストのパスワードを印刷することができます。スポンサーは [アカウントの管理（Manage Accounts）] ページおよびゲストの詳細で、ゲストのパスワードを表示できます。これがオフの場合、スポンサーはパスワードを印刷できませんが、ユーザは電子メールまたは SMS（設定済みの場合）を介してパスワードを取得できます。
- ゲストのクレデンシャルを含む SMS 通知の送信（Send SMS notifications with guests' credentials）：スポンサーは、自分が管理できるゲスト アカウントについて、アカウントの詳細とログイン クレデンシャルとともにゲストに SMS（テキスト）通知を送信できます。
- ゲスト アカウント パスワードのリセット（Reset guest account passwords）：スポンサーは、自分が管理できるゲスト アカウントについて、そのパスワードを Cisco ISE によって生成されたランダムなパスワードにリセットできます。
- ゲストのアカウントの延長（Extend guests' accounts）：スポンサーは、自分が管理できるゲストアカウントについて、その有効期限を延長できます。スポンサーは、アカウントの有効期限に関してゲストに送信される電子メール通知に自動的にコピーされます。
- ゲストのアカウントの削除（Delete guests' accounts）：スポンサーは、自分が管理できるゲストアカウントについて、アカウントを削除し、ゲストが企業のネットワークにアクセスすることを防ぐことができます。

- ゲストのアカウントの一時停止（Suspend guests' accounts）：スポンサーは、自分が管理できるゲストアカウントについて、アカウントを一時停止してゲストが一時的にログインすることを防ぐことができます。

  また、このアクションは、許可変更（CoA）終了を発行して、一時停止されていたゲストをネットワークから排除できます。

  - スポンサーに理由の入力を求める（Require sponsor to provide a reason）：ゲスト アカウントの一時停止に対する説明の入力をスポンサーに求めます。

- アカウント登録ゲストからの要求の承認および表示（Approve and view requests from self-registering guests）：このスポンサー グループに含まれているスポンサーは、（承認が必要な）アカウント登録ゲストからのすべての保留中のアカウント要求を表示するか、アクセス先の担当者としてユーザがスポンサーの電子メールアドレスを入力した要求のみを表示できます。この機能では、アカウント登録ゲストによって使用されるポータルで [アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] にマークが付けられていて、スポンサーの電子メールが連絡先の担当者としてリストされている必要があります。

  - [保留中のすべてのアカウント（Any pending accounts）]：このグループに所属するスポンサーは、他のスポンサーによって作成されたアカウントを承認およびレビューします。

  - [このスポンサーに割り当てられている保留中のアカウントのみ（Only pending accounts assigned to this sponsor）]：このグループに所属するスポンサーは、スポンサー自身が作成したアカウントだけを表示および承認できます。

- プログラムによるインターフェイス（Guest REST API）を使用した Cisco ISE ゲスト アカウントへのアクセス（Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)）：スポンサーは、自分が管理できるゲスト アカウントについて、Guest REST API プログラミング インターフェイスを使用してゲスト アカウントにアクセスできます。

エンドユーザ ポータル

Cisco ISE では、Web ベースのポータルをエンドユーザの 3 つのプライマリ セットに対して提供しています。

- ゲスト ポータル（ホットスポットとクレデンシャルを持つゲスト ポータル）を使用して企業ネットワークに一時的にアクセスする必要があるゲスト。
- スポンサー ポータルを使用してゲスト アカウントを作成および管理できるスポンサーとして指定されている従業員。
- 個人所有デバイスの持ち込み（BYOD）、モバイル デバイス管理（MDM）、デバイス ポータルなどのさまざまな非ゲスト ポータルを使用して、企業ネットワークでパーソナル デバイスを使用している従業員。

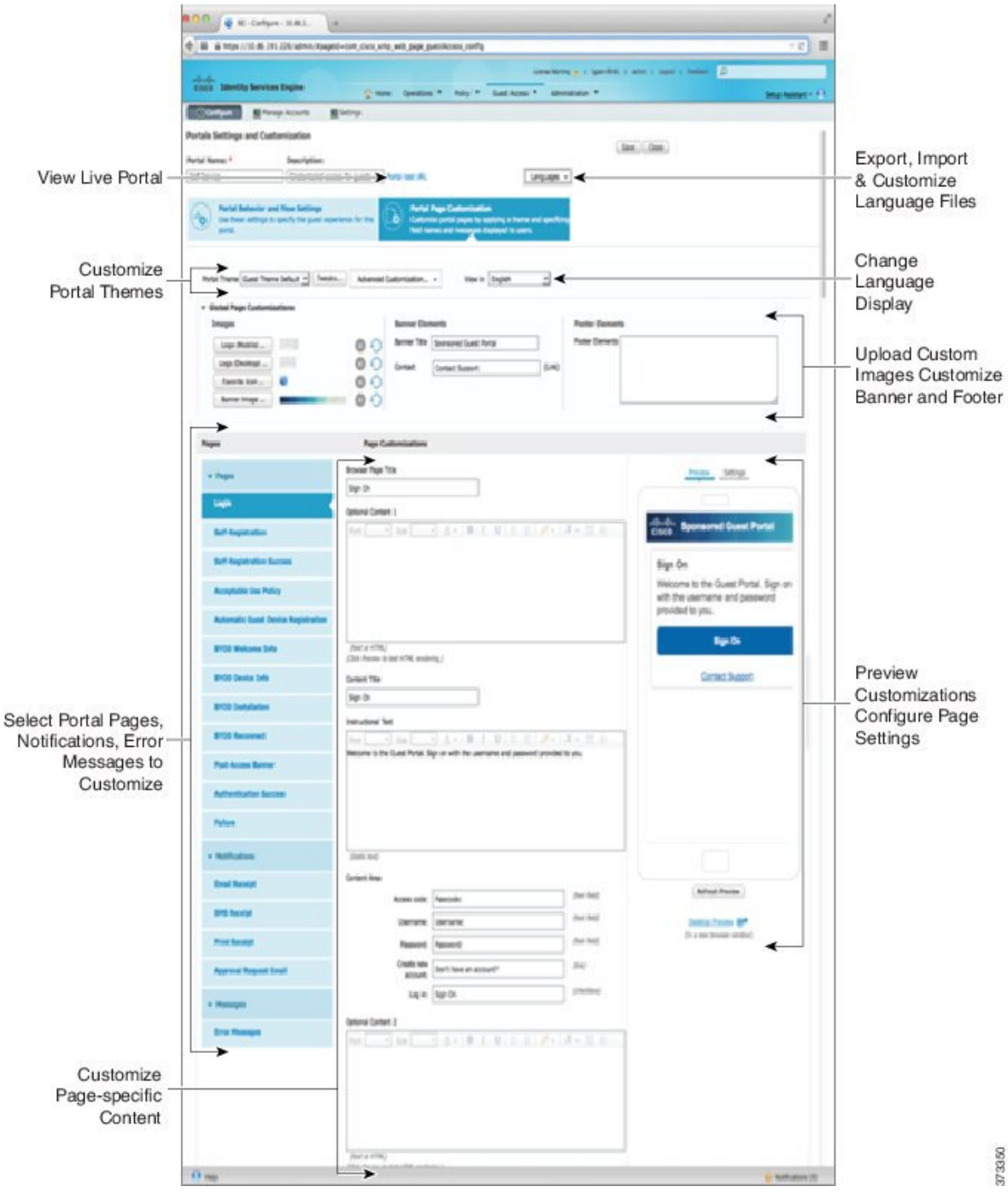
エンドユーザ Web ポータルのカスタマイズ

さまざまなデフォルトポータルが用意されており、これらを編集および複製したり、追加ポータルを作成したりすることができます。ポータルの外観を完全にカスタマイズし、その結果として、ポータルのエクスペリエンスをカスタマイズすることもできます。他のポータルへの影響なく、各ポータルを個別にカスタマイズできます。

ポータル全体またはポータルの特定のページに適用される、次のようなポータルインターフェイスのさまざまな側面をカスタマイズできます。

- テーマ、イメージ、色、バナー、およびフッター
- ポータル テキスト、エラー メッセージ、および通知の表示に使用される言語
- タイトル、コンテンツ、手順、およびフィールドとボタンのラベル
- 電子メール、SMS、およびプリンタでゲストに送信される通知（アカウント登録ゲストポータルとスポンサー ポータルにのみ該当）
- ユーザに表示されるエラー メッセージと情報メッセージ
- 特定の必要によってゲスト情報を収集するカスタム フィールド（アカウント登録ゲストポータルとスポンサー ポータルにのみ該当）

図 *12 :* カスタマイズ用のポータル ページのレイアウト



ISE コミュニティ リソース

Web ポータルのカスタマイズの詳細については、「ISE Portal Builder」および「HowTo: ISE Web Portal Customization Options」を参照してください。

カスタマイズ方法

エンドユーザのポータルページをカスタマイズする方法は複数あり、それぞれ異なるレベルの知識が必要です。

- 基本：すべての変更はポータル カスタマイズ ページで行われます。このページでは次の操作を実行できます。
  - バナーとロゴのアップロード。
  - 一部の色の変更（ボタンを除く）。
  - 画面のテキスト、およびポータル全体で使用される言語の変更。
- 中間（Intermediate）
  - ミニ エディタを使用した HTML および Javascript の追加。
  - jQuery mobile theme roller を使用したすべてのページ要素の色の変更。
- 詳細設定（Advanced）
  - プロパティおよび CSS ファイルの手動による変更。

ポータルをカスタマイズした後、それを複製して（同じタイプの）複数のポータルを作成できます。たとえば、1 つの業務エンティティのホットスポット ゲスト ポータルをカスタマイズした場合、それを複製し、少し変更して他の業務エンティティのカスタム ホットスポット ゲスト ポータルを作成することができます。

ミニ エディタを使用してポータルをカスタマイズするためのヒント

- ミニエディタのボックス内のワードが長いと、ポータルの画面領域のスクロールがオフになる場合があります。これを防ぐには、HTML 段落属性 style="word-wrap: break-word" を使用します。次に例を示します。

```
<p style="word-wrap:break-word">

thisisaverylonglineoftextthatwillexceedthewidthoftheplacethatyouwanttoputitsousethisstructure

</p>
```

- HTML または javascript を使用してポータル ページをカスタマイズする場合は、必ず有効な構文を使用してください。ミニエディタに入力するタグおよびコードは ISE によって検証されません。無効な構文が原因でポータル フロー時に問題が発生する場合があります。

ポータル コンテンツのタイプ

Cisco ISE では、「そのまま」使用するか、または新しいカスタム ファイルを作成するためのモデルとして既存の CSS ファイルを使用することでカスタマイズできる、ポータル テーマの

デフォルト セットが提供されます。ただし、カスタマイズされた CSS ファイルを使用しないでポータルの外観を変更することもできます。

たとえば、独自の企業ロゴやバナーイメージを使用する場合は、単にこれらの新しいイメージファイルをアップロードして使用することができます。ポータルのさまざまな要素および領域の色を変更することによって、デフォルトのカラースキームをカスタマイズできます。カスタム変更時に、カスタム変更を表示する言語を選択することもできます。

ロゴおよびバナーを置き換えるための画像を設計するときは、画像のサイズを次のピクセルサイズに可能な限り近づけてください。

バナー	1724 X 133
デスクトップのロゴ	86 X 45
モバイルのロゴ	80 X 35

ISE はポータルに合わせて画像のサイズを変更しますが、画像が小さすぎるとサイズ変更後に正しく表示されない場合があります。

高度なカスタマイズ（ページ レイアウトの変更、ポータル ページへのビデオ クリップや広告の追加など）を行うには、独自のカスタム CSS ファイルを使用できます。

特定のポータルでのこのようなタイプの変更は、そのポータルのすべてのページにグローバルに適用されます。ページ レイアウトの変更は、ポータル内にグローバルに、または特定の 1 ページのみに適用することができます。

ポータル ページのタイトル、コンテンツ、およびラベル

エンドユーザ Web ポータル ページでゲストに表示されるタイトル、テキスト ボックス、手順、フィールドとボタンのラベル、その他の視覚要素をカスタマイズすることができます。ページをカスタマイズするときには、ページ設定を動的に編集することができます。

これらの変更は、カスタマイズしている特定のページにのみ適用されます。

ポータルの基本的なカスタマイズ

ニーズに最適な事前定義済みテーマを選択し、デフォルト設定のほとんどを使用します。その後、次のような基本的なカスタマイズが可能です。

- ポータルのテーマ カラーの変更 （487 ページ）
- ポータルのアイコン、イメージ、およびロゴの変更 （488 ページ）
- ポータルのバナーおよびフッター要素の更新 （489 ページ）
- ポータルの表示言語の変更 （488 ページ）
- タイトル、手順、ボタン、およびラベル テキストの変更 （490 ページ）
- テキスト ボックスの内容のフォーマットおよびスタイル （490 ページ）

ヒント　更新するときに、カスタマイズの参照 （495 ページ）を行うことができます。

ポータルのテーマ カラーの変更

デフォルト ポータル テーマのデフォルト カラー スキームをカスタマイズして、ポータルのさまざまな要素と領域の色を変更できます。これらの変更は、カスタマイズしているポータル全体に適用されます。

ポータルの色を変更する場合は、次のことに注意してください。

- このオプションを使用して、このポータルで使用するためにインポートしたカスタム ポータル テーマのカラー スキームを変更することはできません。その色の設定を変更するには、カスタム テーマ CSS ファイルを編集する必要があります。
- ポータルのテーマ カラーを変更した後で、[ポータル テーマ（Portal Theme）] ドロップダウン メニューから別のポータルのテーマを選択した場合、元のポータル テーマの変更は失われ、デフォルト カラーに戻ります。
- 変更済みのカラー スキームを使用してポータルのテーマ カラーを調整し、保存する前に色をリセットした場合、カラー スキームはデフォルト カラーに戻り、前の変更はすべて失われます。

ステップ 1　次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [設定（Configure）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > （任意のポータル） > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2　[ポータル テーマ（Portal Theme）] ドロップダウン リストからデフォルト テーマの 1 つを選択します。

ステップ 3　[調整（Tweaks）] をクリックして、選択したデフォルト ポータル テーマの色の設定の一部を上書きします。

a) バナーとページ背景、テキスト、およびラベルの色の設定を変更します。
b) テーマのデフォルト カラー スキームに戻す場合は、[色のリセット（Reset Colors）] をクリックします。
c) [プレビュー（Preview）] で色の変更を確認する場合は、[OK] をクリックします。

ステップ 4 [保存（**Save**）] をクリックします。

ポータルの表示言語の変更

カスタム変更を加えるときに、変更内容を表示する言語を選択できます。この変更は、カスタマイズしているポータル全体に適用されます。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [グローバルなカスタマイズ（Global Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]> [ゲスト アクセス（Guest Access）]> [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [グローバルなカスタマイズ（Global Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）]> [デバイス ポータル管理（Device Portal Management）]> （任意のポータル）> [編集（Edit）]> [ポータル ページのカスタマイズ（Portal Page Customization）]> [グローバルなカスタマイズ（Global Customization）]** を選択します。

ステップ 2 [表示（View In）] ドロップダウン リストから、ページをカスタマイズするときにテキストを表示する言語を選択します。

ドロップダウン リストには、特定のポータルに関連付けられた言語ファイルにあるすべての言語が含まれています。

次のタスク

ポータル ページをカスタマイズするときに選択した言語に加えた変更が、サポート対象のすべての言語プロパティ ファイルで更新されていることを確認します。

ポータルのアイコン、イメージ、およびロゴの変更

独自の企業ロゴ、アイコン、およびバナー イメージを使用する場合は、カスタム イメージをアップロードするだけで既存のイメージを置き換えることができます。サポートされている画像形式は、.gif、.jpg、.jpeg、.png です。これらの変更は、カスタマイズしているポータル全体に適用されます。

始める前に

ポータルのフッター（たとえば、アドバタイズメント）にイメージを含めるには、そのイメージがある外部サーバにアクセスできる必要があります。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [設定（Configure）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > （任意のポータル） > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [イメージ（Images）] で、ロゴ、アイコン、イメージのボタンをクリックし、カスタム イメージをアップロードします。

ステップ 3 [保存（**Save**）] をクリックします。

ポータルのバナーおよびフッター要素の更新

ポータルの各ページのバナーおよびフッターセクションに表示される情報をカスタマイズできます。これらの変更は、カスタマイズしているポータル全体に適用されます。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > （任意のポータル） > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 各ポータル ページに表示される [バナー タイトル（Banner title）] を変更します。

ステップ 3 ポータルを使用するゲスト用に次のリンクを含めます。

- [ヘルプ（Help）]：オンライン ヘルプ（スポンサーおよびデバイス ポータルにのみ提供します）。
- [連絡先（Contact）]：テクニカル サポート（このことができるようにするには、[サポート情報（Support Information）] ページを設定します）。

ステップ 4 各ポータル ページの下部に表示される [フッター要素（Footer Elements）] に利用規約または著作権表示を追加します。

ステップ 5 [保存（**Save**）] をクリックします。

タイトル、手順、ボタン、およびラベル テキストの変更

ポータルに表示されるすべてのテキストを更新できます。カスタマイズするページの各 UI 要素に、入力できる文字数の最小範囲および最大範囲があります。テキストブロックの一部が使用可能な場合、ミニエディタを使用して表示スタイルをテキストに適用できます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。これらのページ要素は、電子メール、SMS、印刷通知ごとに異なります。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）** > **[ポータルとコンポーネント（Portals & Components）]** > **[設定（Configure）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、変更するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、表示された UI 要素を更新します。すべてのページに [ブラウザ ページ タイトル（Browser Page Title）]、[コンテンツ タイトル（Content Title）]、[説明テキスト（Instructional Text）]、[コンテンツ（Content）]、および 2 つの [任意のコンテンツ（Optional Content）] の各テキスト ブロックが含まれています。[コンテンツ（Content）] 領域のフィールドはすべてのページに固有です。

テキスト ボックスの内容のフォーマットおよびスタイル

テキストの基本的な書式設定を行うには、[説明テキスト（Instructional Text）]、[オプションの内容 1（Optional Content 1）]、および [オプションの内容 2（Optional Content 2）] テキスト ボックスにあるミニエディタを使用します。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え（Toggle Full Screen）] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]**>**[ゲスト アクセス（Guest Access）]**> **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）]**>**[デバイス ポータル管理（Device Portal Management）]**> **（任意のポータル）** >**[編集（Edit）]**>**[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、変更するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] の、[説明テキスト（Instructional Text）] および [オプションの内容（Optional Content）] テキスト ボックスで、次の操作を実行できます。

- テキストのフォント、色、サイズを変更します。
- テキストに太字、イタリック体、下線のスタイルを設定します。
- 箇条書きおよび番号付きリストを作成します。

（注） ミニエディタを使用してフォーマットしたテキストに適用されたHTMLタグを見るために[HTMLソースの切り替え（Toggle HTML Source）]ボタンを使用できます。[HTMLソース（HTML Source）]ビューでテキストを編集する場合は、[ポータルページのカスタマイズ（Portal Page Customization）]ウィンドウで変更を保存する前に、[HTMLソースの切り替え（Toggle HTML Source）] ボタンをもう一度クリックします。

ポータル ページのカスタマイズ用の変数

これらのポータル ページ テキスト ボックスへのナビゲーション パス:

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]**>**[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** を選択します。
- デバイス ポータル。**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]**> **（任意のポータル）** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[ページ（Pages）]** を選択します。

ポータルユーザ（ゲスト、スポンサーおよび従業員）に表示される情報の一貫性を維持するために、ポータル コンテンツおよびゲスト通知用のテンプレートを作成するときにこれらの変数を使用します。[説明テキスト（Instructional Text）]、[オプション コンテンツ 1（Optional Content

1）]、および [オプション コンテンツ 2（Optional Content 2）] テキスト ボックスで、各ポータルのテキストを次に示す変数名と置き換えます。

表 *39*：ゲスト ポータルの変数のリスト

表示名	変数名による代替
アクセス コード 電子メール、テキストまたは印刷物の通知を使用して、ゲストにアクセス コードを提供するためのテキスト。	ui_access_code
BYOD IOS SSID デュアルSSIDフローに入った後にデバイスが接続する必要があるネットワークを指定するために使用します。	ui_byod_success_ios_ssid
クライアントプロビジョニングエージェントのタイプ（Client Provisioning Agent Type） AnyConnectエージェントなど、クライアントプロビジョニング ポリシーで現在設定されているエージェントを指定するために使用します。	ui_client_provision_agent_type
クライアントプロビジョニングエージェントの URL（Client Provisioning Agent URL） ポスチャエージェントのダウンロードURLを指定するために使用します。	ui_client_provision_agent_url
クライアントプロビジョニングエージェントインストール分数（Client Provisioning agent install minutes） ゲストに、クライアント プロビジョニング ページでインストール手順を完了する必要がある制限時間（修復タイマーにより設定）を通知するために使用します。タイマーが時間切れになる前にゲストがインストール手順を完了しなかった場合、ゲストはブラウザ ページをリフレッシュして、ログイン プロセスをやり直す必要があります。	ui_client_provision_install_agent_mins
会社	ui_company
電子メール アドレス（Email address）	ui_email_address
終了日時（End date and time）	ui_end_date_time

表示名	変数名による代替
名（First name）	ui_first_name
姓（Last name）	ui_last_name
ロケーション名	ui_location_name
最大登録デバイス数（Maximum registered devices）	ui_max_reg_devices
最大同時ログイン数（Maximum simultaneous logins）	ui_max_siml_login
[パスワード（Password）]	ui_password
訪問先担当者（電子メール）（Person being visited (email)）	ui_person_visited
電話番号（Phone number）	ui_phone_number
訪問の理由（Reason for visit）	ui_reason_visit
SMS プロバイダー（SMS Provider）	ui_sms_provider
SSID ゲストがネットワークに接続するために使用できるワイヤレス ネットワークを指定するために使用します。	ui_ssid
開始日時（Start date and time）	ui_start_date_time
残り時間（Time left）	ui_time_left
[ユーザ名（Username）]	ui_user_name

表 *40* : スポンサー ポータルの変数のリスト

表示名	変数名による代替
ゲスト - 会社（Guest - Company）	ui_guest_company
ゲスト - 電子メール アドレス（Guest - Email address）	ui_guest_email_address
ゲスト- 終了日時（Guest - End date and time）	ui_guest_end_date_time
ゲスト - 名（Guest - First name）	ui_guest_first_name
ゲスト - 姓（Guest - Last name）	ui_guest_last_name

表示名	変数名による代替
ゲスト - ロケーション名（Guest - Location name）	ui_guest_location_name
ゲスト - 最大登録デバイス数（Guest - Maximum registered devices）	ui_guest_max_reg_devices
ゲスト - 最大同時ログイン数（Guest - Maximum simultaneous logins）	ui_guest_max_siml_login
ゲスト - パスワード（Guest - Password）	ui_guest_password
ゲスト - 訪問先担当者（電子メール）（Guest - Person being visited (email)）	ui_guest_person_visited
ゲスト - 電話番号（Guest - Phone number）	ui_guest_phone_number
ゲスト - 訪問の理由（Guest - Reason for visit）	ui_guest_reason_visit
ゲスト - SMS プロバイダー（Guest - SMS Provider）	ui_guest_sms_provider
ゲスト - SSID（Guest - SSID） ゲストがネットワークに接続するために使用できるワイヤレス ネットワークを指定するために使用します。	ui_guest_ssid
ゲスト - 開始日時（Guest - Start date and time）	ui_guest_start_date_time
ゲスト - 残り時間（Guest - Time left）	ui_guest_time_left
ゲスト - ユーザ名（Guest - Username）	ui_guest_user_name
[ユーザ名（Username）] ポータルにログインしたユーザのユーザ名を指定するために使用します。	ui_sponsor_user_name
[ゲスト アクセス情報（Guest Access Information）] ページの [から（From）] を表示するために使用します。	ui_from_label
[ゲスト アクセス情報（Guest Access Information）] ページの [初回ログイン（First Login）] を表示するために使用します。	ui_first_login_text
初回ログイン時にアクセス時間が開始すると、ゲスト アカウントの通知メッセージを表示するために使用します。	ui_notification_first_login_text

表示名	変数名による代替
電子メール通知のアカウントの有効期間を示す動的変数。	ui_access_duration
利用できなくなったアカウントを表示する動的変数。[開始/終了（Start-End）] アカウントでは日付は終了日で、[初回ログインから（From-First-Login）] アカウントでは日付はアカウントの作成日に消去期間日数を足したものです。	ui_account_purge_date
ゲスト ユーザが少なくとも一度以前ログインしたことがある場合、スポンサーが、ゲストのタイプを [初回ログインから（From-First-Login）] から [開始/終了（Start-End）] に変更、または逆に変更することを制限するために使用します。一般的なスポンサー ポータル メッセージに表示されます。	ui_guest_type_change_ffl_startend_not_allowed_error ui_guest_type_change_ startend_ffl_not_allowed_error

表 *41 : MDM* ポータルの変数のリスト

表示名	変数名による代替
MDM - ベンダー名（MDM - Vendor Name）	ui_mdm_vendor_name

表 *42 :* デバイス ポータルの変数のリスト

表示名	変数名による代替
デバイス - ログイン失敗の頻度制限（MyDevices - Login Failure Rate Limit）	$user_login_failure_rate_limit$
デバイス - 最大登録デバイス数（MyDevices - Max Devices to Register）	ui_max_register_devices
デバイス - ユーザ名（MyDevices - User Name） ポータルにログインしたユーザのユーザ名を指定するために使用します。	$session_username$

カスタマイズの参照

カスタマイズがポータルユーザ（ゲスト、スポンサー、従業員）にどのように表示されるかを確認できます。

手順

- [ポータルテストURL（Portal test URL）] をクリックして、変更を表示します。

（注） テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータル フローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。

- 変更がさまざまなデバイスでどのように表示されるかを動的に確認するには、[プレビュー（Preview）] をクリックします。
  - モバイル デバイス：[プレビュー（Preview）] で変更を確認します。
  - デスクトップ デバイス：[プレビュー（Preview）] をクリックし、[デスクトップ プレビュー（Desktop Preview）] をクリックします。新しいタブが開いて、すべての変更がこのタブに表示されます。

変更が表示されない場合は、[プレビューのリフレッシュ（Refresh Preview）] をクリックします。表示されるポータルは、変更を確認するためだけのものです。ボタンをクリックしたり、データを入力したりすることはできません。

カスタム ポータル ファイル

カスタム ポータル ファイル メニューでは、ISE サーバに独自のファイルをアップロードすることができ、（管理者用ポータルを除く）ユーザがアクセスできるすべてのポータルのカスタマイズに使用できます。アップロードしたファイルは PSN に保存され、すべての PSN に同期されます。

サポートされるファイル タイプは次のとおりです。

- .png、.gif、.jpg、.jpeg、ico：背景、お知らせ、広告用
- .htm、.html、.js、.json、.css、.m4a、.m4v、.mp3、.mp4、.mpeg、.ogg、.wav：高度なカスタマイズ用、たとえば、ポータル ビルダー

ファイルのサイズは限定されます：

- ファイルあたり 20 MB
- すべてのファイルの合計が 200 MB

ファイルのリストのパス列には、このサーバ上のファイルの URL が表示されます。この URL は、ミニエディタ外部でそのファイルを参照する場合に使用できます。イメージファイルの場合、リンクをクリックすると、新しいウィンドウが開き、イメージが表示されます。

アップロードされたファイルは、ポータル ページのカスタマイズの下のミニ エディタで、管理者用ポータルを除くすべてのポータル タイプにより参照できます。ミニ エディタにファイ

ルを挿入するには、ツールバーの [ファイルを挿入（insert file）] ボタンをクリックします。[HTML ソース（HTML Source）] ビューに切り替えます。挿入されたファイルが適切な HTML タグで囲まれていることがわかります。

テストのために、表示可能なアップロードファイルを ISE の外部からブラウザで表示することもできます。URL は https://*ise_ip*:8443/portal/customFiles/*filename* です。

ポータルの高度なカスタマイズ

Cisco ISE から提供されるデフォルトのポータル テーマの 1 つを使用しない場合、ニーズに合わせてポータルをカスタマイズできます。そのためには、CSS および Javascript ファイルと jQuery Mobile ThemeRoller アプリケーションの使用経験が必要です。

デフォルトのポータル テーマを変更することはできませんが、次の操作を実行できます。

- ポータルのデフォルト テーマ CSS ファイルのエクスポート（503 ページ）、およびカスタム ポータル テーマを作成する基本として使用できます。
- カスタム ポータル テーマ CSS ファイルの作成（504 ページ）、デフォルトのポータル テーマを編集し、新規ファイルとして保存することによって可能になります。
- カスタム ポータル テーマ CSS ファイルのインポート（516 ページ）、ポータルに適用できます。

専門知識と要件に基づいて、さまざまなタイプの高度なカスタマイズを実行できます。事前定義済み変数を使用して、表示される情報の整合性の実現、ポータル ページへのアドバタイズメントの追加、HTML、CSS、および Javascript コードを使用した内容のカスタマイズ、ポータル ページのレイアウト変更が可能になります。

ポータルを変更するには、各ポータルの [ポータル ページのカスタマイズ（Portal Page Customization）] タブのコンテンツ ボックスに HTML、CSS、および Javascript を追加します。このドキュメントでは、HTML と CSS を使用したカスタマイズの例について説明します。Javascript を使用した例は、ISE コミュニティ（http://cs.co/ise-community）で紹介されています。さらに多くの HTML、CSS、および Javascript の例については、ISE コミュニティ https://community.cisco.com/t5/security-documents/how-to-ise-web-portal-customization-options/ta-p/3619042 を参照してください。

（注） TAC では、Javascript での Cisco ISE ポータルのカスタマイズをサポートしていません。Javascript でのカスタマイズに関する問題が発生した場合は、ISE コミュニティ https://community.cisco.com/t5/identity-services-engine-ise/bd-p/5301j-disc-ise に質問を投稿してください。シスコの従業員およびコミュニティ メンバーがお力になれる場合があります。

高度なポータル カスタマイズの有効化

Cisco ISE では、エンドユーザ ポータルに表示されるコンテンツをカスタマイズすることができます。[ポータルページのカスタマイズ（Portal Page Customization）] にリストされているさまざまなページのテキストボックスにHTML、CSS、およびJavascriptコードを入力できます。

ステップ 1 **[管理（Administration）]>[システム（System）]>[管理者アクセス（Admin Access）]>[設定（Settings）]>[ポータルのカスタマイズ（Portal Customization）] を選択します。**

ステップ 2 [HTML を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML）] がデフォルトでオンになっていることを確認します。この設定によって、[説明テキスト（Instructional Text）]、[オプションの内容 1（Optional Content 1）]、および [オプションの内容 2（Optional Content 2）] テキストボックスに HTML タグを含めることができます。

ステップ 3 [HTMLおよびJavaScriptによるポータルのカスタマイズを有効化（Enable Portal Customization with HTML and JavaScript）] をオンにします。高度な JavaScript カスタマイズには、 <script> tags in the [説明テキスト（Instructional Text）]、[オプションの内容1（Optional Content 1）]、および [オプションの内容2（Optional Content 2）] テキストボックスを含めます。

次のタスク

これで、ポータルに HTML、CSS、および Javascript を入力できるようになります。

ポータル テーマと構造 CSS ファイル

CSS ファイルの使用に関する経験がある場合、デフォルトのポータル テーマ CSS ファイルをカスタマイズして、ポータル プレゼンテーションを変更し、ページ レイアウト、色、フォントなどの要素を操作できます。CSS ファイルをカスタマイズすると、プレゼンテーションの特性の指定における柔軟性と制御が向上し、複数のページでフォーマットを共有することが可能になり、構造化されたコンテンツの複雑さと繰り返しが削減されます。

Cisco ISE エンドユーザ ポータルは、種類が異なる 2 つの CSS ファイル（structure.css および *theme*.css）を使用します。ポータルテーマごとに独自の *theme*.css ファイルがありますが、ポータル タイプにつき structure.css ファイルは 1 つのみです（例：ゲスト ポータルの場合は guest.structure.css、スポンサー ポータルの場合は sponsor.structure.css、デバイス ポータルの場合は mydevices.structure.css）。

structure.css では、ページ レイアウトと構造のスタイルを指定しています。これには各ページの要素の位置が定義され、jQuery Mobile 構造のスタイルも含まれています。structure.css ファイルは表示のみ可能で、編集することはできません。ただし、*theme*.css ファイル内のページ レイアウトを変更し、これらのファイルをポータルにインポートして適用すると、最新の変更が structure.css のスタイルよりも優先されます。

theme.css ファイルは、フォント、ボタンの色、ヘッダーの背景などのスタイルを指定します。*theme*.css ファイルをエクスポートし、テーマ設定を変更してインポートし、ポータルのカスタ

ム テーマとして使用できます。*theme*.css ファイルに対するページ レイアウト スタイルの変更は、structure.css ファイルで定義されるスタイルよりも優先されます。

シスコが提供するデフォルトのポータル *theme*.css ファイルは変更できません。ただし、ファイル内の設定を編集して、新しいカスタム *theme*.css ファイルに保存できます。カスタム *theme*.css ファイルをさらに編集することはできますが、Cisco ISE に再度インポートする場合は、最初に使用されていたのと同じテーマ名にしてください。同じ *theme*.css ファイルに 2 つの異なるテーマ名を使用することはできません。

たとえば、デフォルトの *green theme.css* ファイルを使用して新しいカスタム *blue theme.css* ファイルを作成し、*Blue* と名付けることができます。その後、*blue theme.css* ファイルを編集できますが、これを再度インポートする場合は、同じテーマ名の *Blue* を再利用する必要があります。Cisco ISE はファイル名やその名前とテーマ名の一意性の関係を確認するため、そのファイルを *Red* という名前にすることはできません。ただし、*blue theme.css* ファイルを編集し、*red theme.css* として保存し、新規ファイルをインポートして *Red* と名付けることは可能です。

jQuery Mobile によるテーマ カラーの変更について

シスコのエンドユーザ ポータルのカラー スキームは、jQuery ThemeRoller と互換性があります。ThemeRoller Web サイトを使用して、ポータル全体の色を簡単に編集できます。

ThemeRoller の色の「見本」にはそれぞれ独自のカラー スキームがあります。それらのスキームによって、主要 UI 要素（ツールバー、コンテンツ ブロック、ボタン、リスト項目、フォントのテキスト シャドウなど）の色、テクスチャ、フォントの設定が定義されます。さらに、ボタンのさまざまな操作状態（通常時、マウスオーバー時、押された時）の設定も定義されます。

シスコでは、次の 3 つの見本が使用されます。

- スイッチ A：デフォルトのスイッチ。
- スイッチ B：強調する要素を定義します（例：[承認（Accept）] ボタンなど）。
- スイッチ C：重要な要素を定義します（例：アラート、エラー メッセージ、無効な入力フィールド、削除ボタンなど）。

スイッチを新たに追加して適用する場合は、そのスイッチを使用する要素を含む HTML コードを（オプション コンテンツなどに）追加しない限り、追加したスイッチを適用できません。

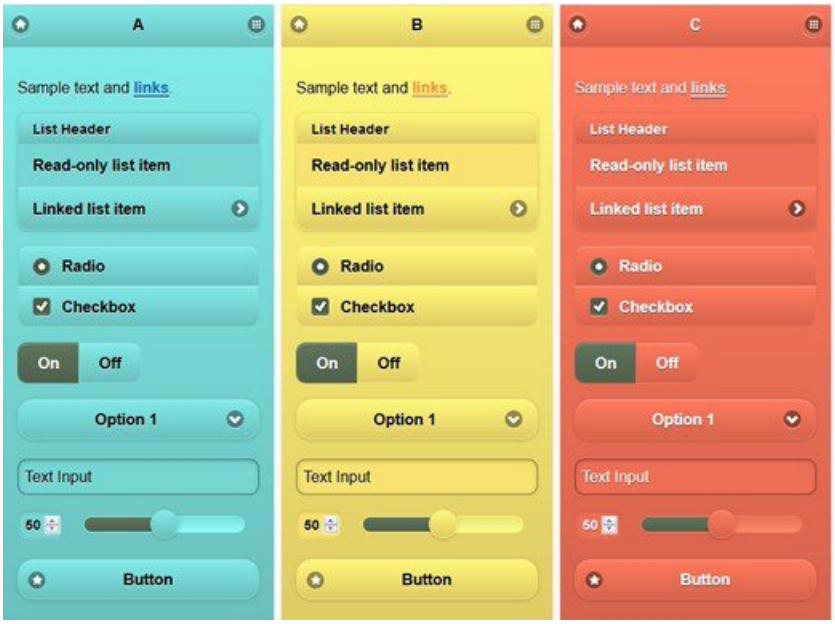
シスコ提供のデフォルトの CSS ファイルを編集するか、またはデフォルトのテーマに定義されている CSS クラスおよび構造に基づいて新しいファイルを作成するには、jQuery Mobile ThemeRoller（リリース 1.3.2）の必要なバージョンを使用してください。

jQuery Mobile ThemeRoller のスウォッチおよびテーマの詳細情報については、『Creating a Custom Theme with ThemeRoller』の「Theming Overview」を参照してください。jQuery Mobile ThemeRoller のオンライン ヘルプを使用して、カスタム テーマをダウンロード、インポート、および共有する方法を学習します。

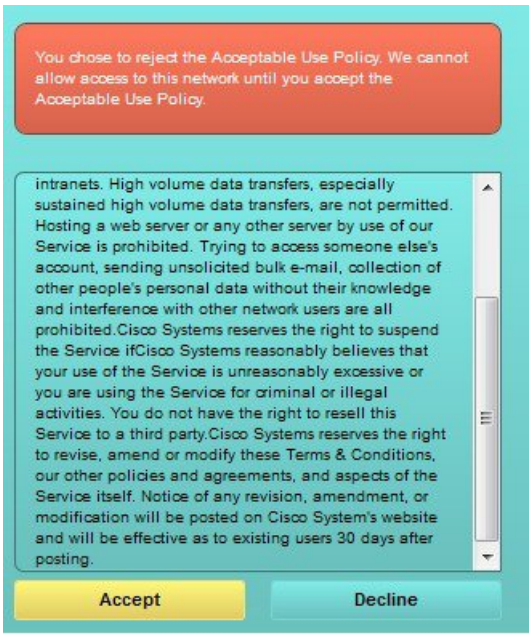
HTML、CSS、およびJavascript コードを使用して、ポータルページに表示されるテキストおよびコンテンツをカスタマイズする方法のチュートリアルについては、Codecademy にアクセスしてください。

シスコの見本を示すテーマの例

見本がどのように使用されるかを示すために、ゲスト ポータルのデフォルト テーマが色の違いを示すように ThemeRoller で編集されました。



次の画面は、ユーザ（見本B）からのアクションを取るボタンとともにゲスト ポータルのログイン エラー（見本 C）を示し、画面の残りは見本 A です。



jQuery Mobile によるテーマ カラーの変更

始める前に

jQuery Mobile ThemeRoller のバージョン 1.3.2 を使用していることを確認します。ご使用のバージョンが次のように画面の左上隅に表示されます。

ステップ 1 ポータルで [設定（Configuration）] タブをクリックして、**[高度なカスタマイズ（Advanced Customization）]** > **[テーマのエクスポート/インポート（Export/Import Themes）]** をクリックし、ポータルから変更する既存のテーマをエクスポートします。

ステップ 2 [カスタムテーマ（Custom Theming）] ダイアログで、更新するテーマをエクスポートします。

ステップ 3 テキスト エディタでそのテーマを開き、すべてを選択してコピーします。

ステップ 4 jQuery Web サイトの [テーマのインポート（Import Theme）] ボックスにテキスト（CSS）を貼り付けます。

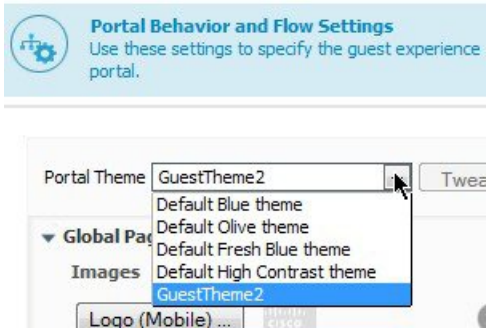
ステップ 5 jQuery Mobil Web ベースのアプリケーションで変更を行います。

ステップ 6 jQuery Web サイトから更新されたテーマをエクスポートします（エクスポート形式は zip）。

ステップ 7 更新されたテーマを解凍し、テーマ フォルダ内の更新されたテーマを PC に展開します。テーマの名前は、jQuery Web サイトで指定した名前です。

ステップ 8 ポータル設定ページの [カスタムテーマ（Custom Theming）] ダイアログで、展開した CSS テーマ ファイルをポータルにインポートします。

ポータル設定ページの [ポータルテーマ（Portal Theme）] ドロップダウンをクリックすることで、古いテーマと新しいテーマを切替えることができます。



ロケーションに基づくカスタマイズ

ゲストアカウントが作成されるときに、それらをロケーションに関連付けて Service Set Identifier（SSID）属性を指定することできます。ロケーションと SSID のどちらも、CSS クラスとして使用することができます。これを使用すると、ゲストのロケーションと SSID に基づいて、それぞれ異なる CSS スタイルをポータル ページに適用できます。

（注） この情報は、クレデンシャルを持つゲストポータルにのみ、ゲストがログインした後に適用されます。

次に例を示します。

- ゲスト ロケーション：ロケーションとして *San Jose* または *Boston* を持つアカウント付きゲストがクレデンシャルを持つゲスト ポータルにログインした場合、**guest-location-san-jose** または **guest-location-boston** のいずれかのクラスをすべてのポータル ページで使用できます。
- ゲスト SSID：*Coffee Shop Wireless* という名前の SSID の場合、すべてのポータル ページで **guest-ssid-coffee-shop-wireless** という CSS クラスを使用できます。この SSID は、ゲストアカウントに指定した SSID であり、ログイン時にゲストが接続した SSID ではありません。

スイッチやワイヤレス LAN コントローラ（WLC）などのデバイスをネットワークに追加するときに、ロケーションも指定できます。このロケーションも CSS クラスとして使用することができ、これを使用すると、ネットワーク デバイスのロケーションに応じて、それぞれ異なる CSS スタイルをポータル ページに適用できます。

たとえば、WLC が *Seattle* に割り当てられ、ゲストが Seattle-WLC から Cisco ISE にリダイレクトされた場合、すべてのポータル ページで **device-location-my-locations-usa-seattle** という CSS クラスを使用できます。

関連トピック

ゲスト ロケーションに基づいたグリーティングのカスタマイズ （511 ページ）

ユーザ デバイス タイプに基づくカスタマイズ

Cisco ISE は、クライアント デバイスのタイプ（ゲスト、スポンサー、または従業員）を検出し、企業のネットワークまたはエンドユーザ Web ポータル（ゲスト、スポンサーおよびデバイス）にアクセスします。タイプは、モバイル デバイス（Android、iOS など）またはデスクトップ デバイス（Windows、MacOS など）のいずれかとして検出されます。デバイス タイプは、CSS クラスとして利用できます。このクラスは、ユーザのデバイス タイプに基づいてポータル ページに異なる CSS スタイルを適用するために使用できます。

ユーザは Cisco ISE のエンドユーザ Web ポータルにログインすると、それらのポータル ページで **cisco-ise-mobile** クラスまたは **cisco-ise-desktop** クラスを使用できます。

関連トピック

ユーザ デバイス タイプに基づいたグリーティングのカスタマイズ （512 ページ）

ポータルのデフォルト テーマ CSS ファイルのエクスポート

シスコが提供するデフォルトのポータルテーマをダウンロードし、ニーズに合わせてカスタマイズできます。それを高度なカスタマイズを実行するための基本として使用できます。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** を選択します。
- デバイス ポータル。**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > （任意のポータル） > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** を選択します。

ステップ 2 [高度なカスタマイズ（Advanced Customization）] ドロップダウン リストから [テーマのエクスポート/インポート（Export/Import Themes）] を選択します。

ステップ 3 [カスタム テーマ（Custom Theming）] ダイアログボックスで、ドロップダウン リストを使用してカスタマイズするテーマを選択します。

ステップ 4 [テーマ CSS のエクスポート（Export Theme CSS）] をクリックして、カスタマイズするデフォルトの *theme.css* ファイルをダウンロードします。

ステップ 5 [保存（Save）] をクリックしてファイルをデスクトップに保存します。

カスタム ポータル テーマ CSS ファイルの作成

カスタム ポータル テーマを作成するには、既存のデフォルト ポータル テーマをカスタマイズして、新規ポータルの *theme*.css ファイルに変更を保存します。デフォルト テーマの設定および見本を変更して、選択したポータルへのグローバルな変更を行うことができます。

始める前に

- カスタマイズするポータルから *theme*.css ファイルをデスクトップにダウンロードします。
- このタスクには、HTML、CSS、および Javascript コードの使用経験が必要です。
- jQuery Mobile ThemeRoller のリリース 1.3.2 を使用します。

ステップ 1 ダウンロードしたポータルの *theme*.css ファイルのコンテンツを jQuery Mobile ThemeRoller ツールにインポートします。

ヒント 変更時に、カスタマイズの参照 （517 ページ） を行うことができます。

ステップ 2 （任意） ポータル コンテンツに組み込まれたリンク （504 ページ）
ステップ 3 （任意） 動的なテキスト更新の変数の挿入 （505 ページ）
ステップ 4 （任意） テキストをフォーマットし、リンクを含めるソース コードの使用 （506 ページ）
ステップ 5 （任意） アドバタイズメントとしてのイメージの追加 （508 ページ）
ステップ 6 （任意） ゲスト ロケーションに基づいたグリーティングのカスタマイズ （511 ページ）
ステップ 7 （任意） ユーザ デバイス タイプに基づいたグリーティングのカスタマイズ （512 ページ）
ステップ 8 （任意） カルーセル アドバタイジングの設定 （509 ページ）
ステップ 9 （任意） ポータル ページのレイアウトの変更 （513 ページ）
ステップ 10 カスタマイズされたファイルを新しい *theme*.css ファイルとして保存します。

（注） デフォルト CSS テーマ ファイルに編集内容を保存することはできません。編集を使用して新しいカスタム ファイルを作成することのみができます。

ステップ 11 新しい *theme*.css ファイルは、準備を整えた後、Cisco ISE にインポートできます。

ポータル コンテンツに組み込まれたリンク

リンクを追加して、ゲストがポータル ページからさまざまな Web サイトにアクセスできるようにすることができます。これらの変更は、カスタマイズしている特定のポータルページにだけ適用されます。

[全画面表示の切り替え（Toggle Full Screen）] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）** > **[ポータルとコンポーネント（Portals and Components]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]**>**[ゲスト アクセス（Guest Access）]**> **[ポータルとコンポーネント（Portals and Components）]** > **[スポンサー ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）]**>**[デバイス ポータル管理（Device Portal Management）]**> **（任意のポータル）** >**[編集（Edit）]**>**[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- 証明書プロビジョニング ポータル。**[管理（Administration）]**>**[デバイス ポータル管理（Device Portal Management）]** > **[証明書プロビジョニング（Certificate Provisioning）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[オプションの内容（Optional Content）] テキスト ブロックで提供されるミニエディタを使用して、ポータル ページへのリンクを追加します。

ステップ 4 [リンクの作成（Create Link）] ボタンをクリックします。
[リンク プロパティ（Link Properties）] ダイアログボックスが表示されます。

ステップ 5 [URL] の [説明（Description）] ウィンドウに、ハイパーリンクする **URL** およびテキストを入力します。

リンクが正しく機能するように、URL にプロトコル識別子を含めます。たとえば、www.cisco.com ではなく http://www.cisco.com を使用します。

ステップ 6 [設定（Set）] をクリックし、[保存（Save）] をクリックします。

ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え（Toggle HTML Source）] ボタンを使用できます。

動的なテキスト更新の変数の挿入

内容を動的に更新する事前定義済みの変数（$variable$）を代わりに使用することによって、ポータルに表示されるテキストのテンプレートを作成することもできます。これにより、ゲストに表示するテキストと情報の一貫性が維持されます。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え（Toggle Full Screen）] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals and Components] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals and Components）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > （任意のポータル）> [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[説明テキスト（Instructional Text）]、[オプションの内容 1（Optional Content 1）]、および [オプションの内容 2（Optional Content 2）] テキスト ボックスで提供されるミニエディタを使用して、ポータル ページのテキスト テンプレートを作成します。

たとえば、複数のゲスト用に単一の初期メッセージ テンプレートを作成し、正常にログインしてネットワークに接続した後にゲストに表示するメッセージをカスタマイズできます。

ステップ 4 通常どおりにテキスト ボックスに情報を入力します。

たとえば、ポータル用の初期メッセージを入力することができます。

```
Welcome to our company’s Guest portal,
```

ステップ 5 テキストの代わりに変数を使用するポイントで、[変数の挿入（Insert Variable）] ボタンをクリックします。変数のリストがポップアップ メニューに表示されます。

ステップ 6 テキストの代わりに使用する変数を選択します。

この例では、初期メッセージに各ゲストの名を表示する [名（First name）] を選択します。変数 **ui_first_name** がカーソル位置に挿入されます。

```
Welcome to our company’s Guest portal,$ui_first_name$.
```

これは John という名のゲストのポータルの初期ページに表示される初期メッセージです。**当社のゲスト ポータルへようこそ、John（Welcome to our company’s Guest portal, John）**。

ステップ 7 テキスト ボックスに情報を入力し終えるまで、必要に応じて続けて変数のリストを使用します。

ステップ 8 [保存（Save）] をクリックします。

ミニエディタを使用してフォーマットしたテキストに適用された HTML タグを見るために [HTML ソースの切り替え（Toggle HTML Source）] ボタンを使用できます。

テキストをフォーマットし、リンクを含めるソース コードの使用

ミニエディタのフォーマットとプレーンテキスト付きリンク アイコンの使用に加えて、HTML、CSS、および Javascript コードを使用して、ポータル ページに表示されるテキストをカスタマイズすることもできます。これらの変更は、カスタマイズしている特定のポータル ページにだけ適用されます。

[全画面表示の切り替え（Toggle Full Screen）] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

始める前に

[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [ポータルのカスタマイズ（Portal Customization）] で [HTML を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML）] がデフォルトで有効になっていることを確認します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > （任意のポータル） > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[説明テキスト（Instructional Text）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスで提供されるミニエディタを使用して、ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] ボタンをクリックします。

ステップ 5 ソース コードを入力します。

たとえば、テキストに下線を引くには、次のように入力します。

```
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

たとえば、HTML コードを使用してリンクを含めるには、次のように入力します。

```
<a href="http://www.cisco.com">Cisco</a>
```

重要 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対（全体的な）URL パスを入力することを確認します。

ステップ 6 **[保存（Save）]** をクリックします。

関連トピック

高度なポータル カスタマイズの有効化 （498 ページ）

アドバタイズメントとしてのイメージの追加

ポータルページの特定の領域に表示されるイメージおよびアドバタイズメントを含めることができます。

[全画面表示の切り替え（Toggle Full Screen）] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

始める前に

[管理（Administration）] > [システム（System）] > [管理アクセス（Admin Access）] > [設定（Settings）] > [ポータルのカスタマイズ（Portal Customization）] で [HTML を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML）] が有効になっていることを確認します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > （任意のポータル） > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[説明テキスト（Instructional Text）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスで提供されるミニエディタを使用して、ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] ボタンをクリックします。

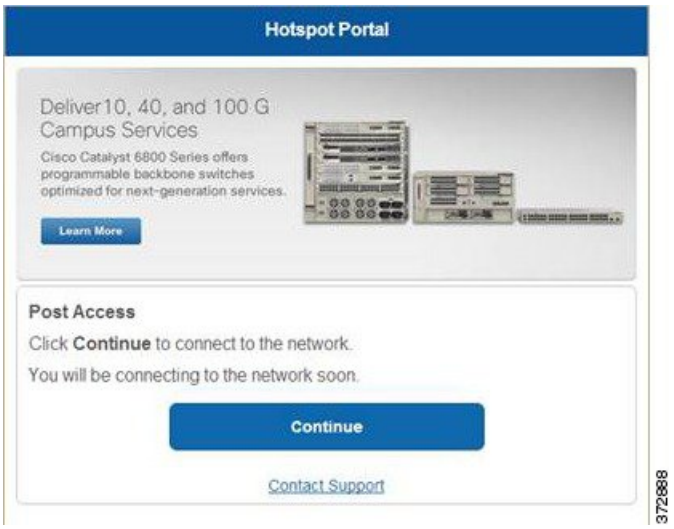
ステップ 5 ソース コードを入力します。

たとえば、ホットスポット ゲスト ポータル ポスト アクセス バナーに HTML コードを使用して製品アドバタイズメントおよびそのイメージを含めるには、このコードを [ポスト アクセス バナー（Post-Access Banner）] ページの [任意のコンテンツ 1（Optional Content 1）] テキスト ボックスに入力します。

```
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p>
<img  src="http://www.static-cisco.com/assets/prod/root/catalyst_6800.jpg" width="100%" />
```

（注） 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対（全体的な）URL パスを入力することを確認します。

図 *13 :* アドバタイズメントのサンプル イメージ



ステップ 6 [保存（**Save**）] をクリックします。

カルーセル アドバタイジングの設定

カルーセルアドバタイジングは、複数の製品イメージまたは説明テキストが表示され、バナー内で循環して繰り返されるアドバタイズメントの形式です。ゲスト ポータルでカルーセル アドバタイジングを使用して、複数の関連製品や、会社が提供するさまざまな製品を宣伝します。

[全画面表示の切り替え（Toggle Full Screen）] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

始める前に

[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [ポータルのカスタマイズ（Portal Customization）] を選択し、[HTML と Javascript を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML and Javascript）] をオンにします。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

- デバイス ポータル。**[管理（Administration）]**>**[デバイス ポータル管理（Device Portal Management）]**>**（任意のポータル）**>**[編集（Edit）]**>**[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[説明テキスト（Instructional Text）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスで提供されるミニエディタを使用して、ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] ボタンをクリックします。

ステップ 5 ソース コードを入力します。

たとえば、ゲスト ポータルで製品イメージを使用してカルーセル アドバタイジングを実装するには、[ポスト アクセス バナー（Post-Access Banner）]（ホットスポット ポータルの場合）または [ポスト ログイン バナー（Post Login Banner）]（クレデンシャルを持つゲスト ポータルの場合）ページの [オプションの内容 1（Optional Content 1）] テキスト ボックスに次の HTML および Javascript コードを入力します。

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 5000);

function changeBanner(){
var bannersArray = ["<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' width='100%'/>",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_0/
n21v1DrawerContainer.img.jpg/1400748629549.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_1/
n21v1DrawerContainer.img.jpg/1376556883237.jpg' width='100%'/>"

];
  var div = document.getElementById("image-ads");
  if(div){
     currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
      div.innerHTML = bannersArray[currentIndex];
   }
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
</style>
<div class="grey" id="image-ads">
<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout- overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg'/>
</div>
```

たとえば、ゲスト ポータルで製品の説明テキストを使用してカルーセル アドバタイジングを実装するには、[ポストアクセスバナー（Post-Access Banner）]（ホットスポット ポータルの場合）または [ポストログインバナー（Post Login Banner）]（クレデンシャルを持つゲスト ポータルの場合）ページの [オプションの内容2（Optional Content 2）] テキスト ボックスに次の HTML および Javascript コードを入力します。

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 2000);

function changeBanner(){
var bannersArray = ["Optimize branch services on a single platform while delivering an optimal
application experience across branch and WAN infrastructure", "Transform your Network Edge to
deliver high-performance, highly secure, and reliable services to unite campus, data center,
and branch networks",  "Differentiate your service portfolio and increase revenues by delivering
end-to-end scalable solutions and subscriber-aware services"];

var colorsArray = ["grey", "blue",  "green"];
  var div = document.getElementById("text-ads");
  if(div){
     currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
      div.innerHTML = bannersArray[currentIndex];
               div.className = colorsArray[currentIndex];
   }
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
.blue{
color: black;
background-color: lightblue;
}
.green{
color: black;
background-color: lightgreen;
}
</style>
<div class="grey" id="text-ads">
Optimize branch services on a single platform while delivering an optimal application
experience across branch and WAN infrastructure
</div>
```

（注） 外部 URL を HTML コードで挿入する場合は、「http」または「https」を含む絶対（全体的な）URL パスを入力する必要があります。

ステップ 6 [保存（**Save**）] をクリックします。

ゲスト ロケーションに基づいたグリーティングのカスタマイズ

次の例に、ゲストがクレデンシャルを持つゲスト ポータル（ホットスポットではない）にログインした後に表示される正常なログイン メッセージを、ゲスト タイプに設定されたロケーションに基づいてカスタマイズする方法を示します。

[全画面表示の切り替え（Toggle Full Screen）] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルのいずれかに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]**>**[ゲスト アクセス（Guest Access）]**> **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、[認証成功（Authentication Success）] ページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[オプションの内容 1（Optional Content 1）] テキスト ボックスで提供されるミニエディタを使用して、HTML ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] ボタンをクリックします。

ステップ 5 ソース コードを入力します。

たとえば、ロケーションベースのグリーティングを含めるには、[オプションコンテンツ1（Optional Content 1）] に次のコードを入力します。

```
<style>
    .custom-greeting {
        display: none;
    }
    .guest-location-san-jose .custom-san-jose-greeting {
        display: block;
    }
    .guest-location-boston .custom-boston-greeting {
        display: block;
    }
</style>
<div class="custom-greeting custom-san-jose-greeting">
    Welcome to The Golden State!
</div>
<div class="custom-greeting custom-boston-greeting">
    Welcome to The Bay State!
</div>
```

正常なログイン後に、特定のロケーションに応じて異なるメッセージがゲストに表示されます。

ユーザ デバイス タイプに基づいたグリーティングのカスタマイズ

ユーザが Cisco ISE エンドユーザ Web ポータル（ゲスト、スポンサーおよびデバイス）のいずれかにログインした後に、ユーザに送信するグリーティングを、クライアント デバイス タイプ（モバイルまたはデスクトップ）に基づいてカスタマイズできます。

[全画面表示の切り替え（Toggle Full Screen）] ボタンを使用して、作業しているテキスト ボックスのサイズを拡大および縮小します。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]**>**[ゲスト アクセス（Guest Access）]**>**[ポータルとコンポーネント（Portals & Components）]**>**[スポンサー ポータル（Guest Portals）]**>**[編集（Edit）]**> **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）]**>**[デバイス ポータル管理（Device Portal Management）]**>**（任意のポータル）**>**[編集（Edit）]**>**[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [ページ（Pages）] で、更新するページを選択します。

ステップ 3 [ページのカスタマイズ（Page Customizations）] で、[オプションの内容 1（Optional Content 1）] テキスト ボックスで提供されるミニエディタを使用して、HTML ソース コードを入力および表示します。

ステップ 4 [HTML ソースの切り替え（Toggle HTML Source）] ボタンをクリックします。

ステップ 5 ソース コードを入力します。

たとえば、AUP ページにデバイス タイプベースのメッセージを含めるには、[AUP] ページの [オプションの内容 1（Optional Content 1）] テキスト ボックスに次のコードを入力します。

```
<style>
    .custom-greeting {
        display: none;
    }
    .cisco-ise-desktop .custom-desktop-greeting {
        display: block;
    }
    .cisco-ise-mobile .custom-mobile-greeting {
        display: block;
    }
</style>
<div class="custom-greeting custom-mobile-greeting">
    Try our New Dark French Roast! Perfect on the Go!
</div>
<div class="custom-greeting custom-desktop-greeting">
    We brough back our Triple Chocolate Muffin!
    Grab a seat and dig in!
</div>
```

ユーザがネットワークまたはポータルへのアクセスを取得するために使用したデバイスに応じて、[AUP] ページに異なるグリーティングが表示されます。

ポータル ページのレイアウトの変更

ページの全体的なレイアウトを操作できます。たとえば、追加情報や情報へのリンクを提供するサイドバーを AUP ページに追加できます。

ステップ 1 作成し、ポータルに適用するカスタム *theme*.css ファイルの末尾に次の CSS コードを追加します。これにより、[オプションの内容 1（Optional Content 1）] テキスト ボックスが次のように表示されるように AUP ページのレイアウトが変更されます。

- デスクトップ デバイス モードのサイド バー
- モバイル デバイス モードのサイド バー

```
#page-aup .cisco-ise-optional-content-1 {
        margin-bottom: 5px;
}
@media all and ( min-width: 60em ) {
        #page-aup .cisco-ise-optional-content-1 {
                float: left;
                margin-right: 5px;
                width: 150px;
        }
        #page-aup .cisco-ise-main-content {
                float: left;
                width: 800px;
        }
        #page-aup .cisco-ise-main-content h1,
        #page-aup .cisco-ise-main-content p {
                margin-right: auto;
                margin-left: -200px;
        }
}
```

次に、ポータルの AUP ページの [オプションの内容1（Optional Content 1）] テキスト ボックスで HTML コードを使用して、リンクを追加できます。

ステップ 2 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portal & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]>[ゲスト アクセス（Guest Access）]> [ポータルとコンポーネント（Portal & Components）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）]>[デバイス ポータル管理（Device Portal Management）]>（任意のポータル）>[編集（Edit）]>[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 3 [ページ（Pages）] で、サイド バーを追加するページを選択します。

ステップ 4 [ページのカスタマイズ（Page Customizations）] で、[オプションの内容 1（Optional Content 1）] テキスト ボックスで提供されるミニエディタを使用して、ソース コードを入力および表示します。

ステップ 5 [HTML ソースの切り替え（Toggle HTML Source）] ボタンをクリックします。

ステップ 6 ソース コードを入力します。

たとえば、AUP ページにサイド バーを含めるには、AUP ページの [オプションの内容 1（Optional Content 1）] テキスト ボックスにこのコードを入力します。

```
<ul data-role="listview">
    <li>Rent a Car</li>
    <li>Top 10 Hotels</li>
    <li>Free Massage</li>
    <li>Zumba Classes</li>
</ul>
```

図 *14* : サンプル *AUP* ページのサイド バーのビュー（デスクトップ デバイス）

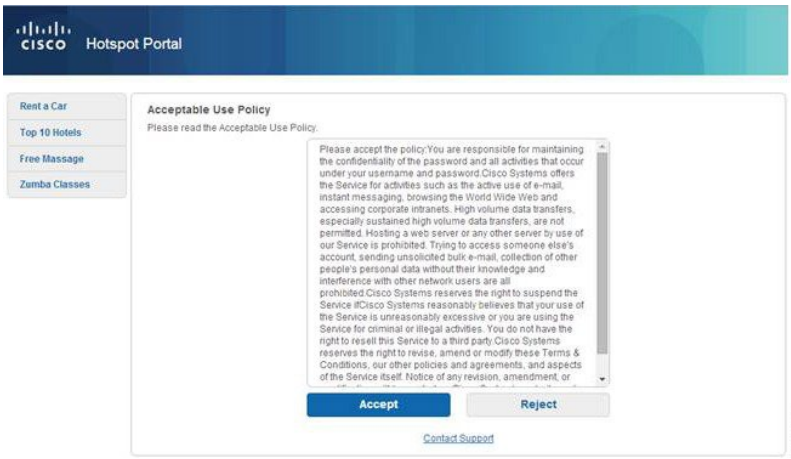
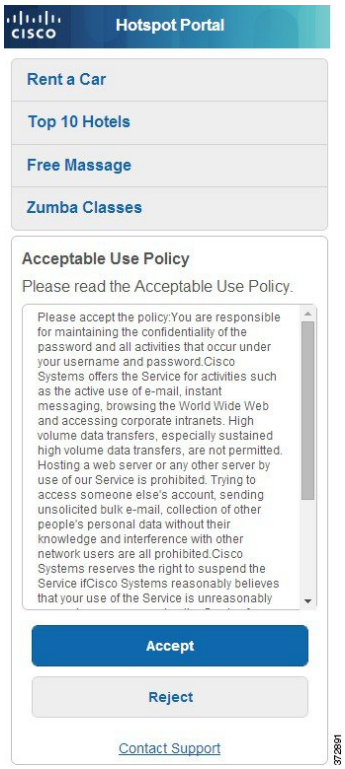


図 *15* : サンプル *AUP* ページのサイド バーのビュー（モバイル デバイス）



ステップ 7 [保存（Save）] をクリックします。

次のタスク

[オプションの内容（Optional Content）] テキスト ボックスに別のテキストまたは HTML コードを入力して、他のページをカスタマイズできます。

カスタム ポータル テーマ CSS ファイルのインポート

作成したカスタム *theme*.css ファイルをアップロードし、エンドユーザ ポータルに適用できます。これらの変更は、カスタマイズしているポータル全体に適用されます。

カスタム *theme*.css ファイルを編集し、Cisco ISE に再度インポートする場合は、最初に使用したテーマ名を使用するように注意してください。同じ *theme*.css ファイルに 2 つの異なるテーマ名を使用することはできません。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[設定（Configure）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [高度なカスタマイズ（Advanced Customization）] ドロップダウン リストから [テーマのエクスポート/インポート（Export/Import Themes）] を選択します。

ステップ 3 [カスタム テーマ（Custom Theming）] ダイアログボックスで、新しい *theme*.css ファイルを検索するには、[参照（Browse）] をクリックします。

ステップ 4 新しいファイルの [テーマ名（Theme Name）] を入力します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

カスタマイズするポータルにこのカスタム ポータル テーマを適用できます。

1. ポータル全体に適用する更新されたテーマを [ポータル テーマ（Portal Themes）] ドロップダウン リストから選択します。
2. [**保存（Save）**] をクリックします。

カスタム ポータル テーマの削除

Cisco ISE にインポートしたカスタム ポータル テーマは、いずれかのポータルで使用されていない場合に削除できます。Cisco ISE によって提供されているデフォルトのテーマを削除することはできません。

始める前に

他のポータルで使用されているポータル テーマを削除することはできません。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]**>**[ゲスト アクセス（Guest Access）]**> **[ポータルとコンポーネント（Portals & Components）]**>**[スポンサー ポータル（Guest Portals）]**>**[編集（Edit）]**> **[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。
- デバイス ポータル。**[管理（Administration）]**>**[デバイス ポータル管理（Device Portal Management）]**> **（任意のポータル）**>**[編集（Edit）]**>**[ポータル ページのカスタマイズ（Portal Page Customization）]** を選択します。

ステップ 2 [高度なカスタマイズ（Advanced Customization）] ドロップダウン リストから [テーマの削除（Delete Themes）] を選択します。

ステップ 3 [テーマ名（Theme Name）] ドロップダウン リストから削除するポータル テーマを選択します。

ステップ 4 [削除（Delete）] をクリックし、[保存（Save）] をクリックします。

カスタマイズの参照

カスタマイズがポータルユーザ（ゲスト、スポンサー、従業員）にどのように表示されるかを確認できます。

手順

- [ポータルテストURL（Portal test URL）] をクリックして、変更を表示します。

（注） テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータル フローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。

- 変更がさまざまなデバイスでどのように表示されるかを動的に確認するには、[プレビュー（Preview）] をクリックします。
  - モバイル デバイス：[プレビュー（Preview）] で変更を確認します。
  - デスクトップ デバイス：[プレビュー（Preview）] をクリックし、[デスクトップ プレビュー（Desktop Preview）] をクリックします。新しいタブが開いて、すべての変更がこのタブに表示されます。

変更が表示されない場合は、[プレビューのリフレッシュ（Refresh Preview）] をクリックします。表示されるポータルは、変更を確認するためだけのものです。ボタンをクリックしたり、データを入力したりすることはできません。

ポータル言語のカスタマイズ

ゲスト、スポンサー、デバイスおよびクライアントプロビジョニングの各ポータルは、サポートされているすべての言語およびロケールにローカライズされています。ローカライズには、テキスト ラベル、メッセージ、フィールド名およびボタン ラベルが含まれます。クライアント ブラウザが Cisco ISE テンプレートにマッピングされていないロケールを要求した場合、ポータルは英語のテンプレートを使用して内容を表示します。

管理者ポータルを使用して、各言語のゲスト、スポンサー、デバイスの各ポータルで使用されるフィールドを個別に変更できます。また、言語を追加することも可能です。現在、クライアントプロビジョニング ポータルについては、これらのフィールドはカスタマイズできません。

デフォルトでは、各タイプのポータルでは 15 言語がサポートされています。[ポータル ページのカスタマイズ（Portal Page Customization）] ページで、ポータルで使用する言語を選択し、オプションで選択した言語でページのコンテンツを更新します。ある言語に合わせてページのフォントとコンテンツを変更しても、他の言語へこの変更は反映されません。[ポータル ページのカスタマイズ（Portal Page Customization）] 画面で行った変更は、次回に言語ファイルをエクスポートするときに組み込まれます。

サポート対象の言語は次のとおりです。

- 中国語（簡体字）
- 中国語（繁体字）
- チェコ語
- Dutch
- 英語
- フランス語
- ドイツ語
- ハンガリー語
- イタリア語
- 日本語
- Korean
- ポーランド語
- ポルトガル語
- ロシア語

- スペイン語

（注） NAC および MAC エージェントのインストーラおよび WebAgent ページはローカライズされていません。

ポータルで使用する言語の編集

1. 編集するポータルを開きます。
2. [ポータル ページのカスタマイズ（Portal Page Customization] タブで、ページの最上部近くにある [表示(view in）] ドロップダウンから、編集する言語を選択します。
3. 必要に応じてコンテンツ、ヘッダー、フォントを変更します。
4. ポータル設定を保存し、更新する次の言語でこのフローを繰り返します。

言語ファイルを編集するには

各 [ポータル ページのカスタマイズ（Portal Page Customization）] ページでは言語ファイルも提供されます。言語ファイルとは、属性ファイルが含まれている ZIP です。これらの属性ファイルは、ポータル フローの一部であるテキストやヘッダーのカスタマイズには使用できますが、[ポータル ページのカスタマイズ（Portal Page Customization）] ページのカスタマイズには使用できません。

言語ファイルには、特定のブラウザ ロケール設定（例：フランス語の場合は fr、fr-fr、fr-ca）へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザ ロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイス ポータルにも適用されます。

zip 形式の言語ファイルをエクスポートし、新規言語の追加や不要な既存言語の削除などを行って更新することができます。

言語ファイルの更新手順については、次を参照してください。

- 言語ファイルのエクスポート （519 ページ）
- 言語ファイルでの言語の追加または削除 （520 ページ）
- 更新された言語ファイルのインポート （521 ページ）

言語ファイルのエクスポート

各ポータル タイプに使用できる言語ファイルをエクスポートして、そのファイルで指定された既存の値を編集およびカスタマイズし、言語を追加または削除できます。

（注） 言語プロパティ ファイル内の一部のディクショナリ キーだけが値（テキスト）で HTML をサポートしています。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[編集（Edit）]** を選択します。
- スポンサー ポータルの場合、**[ワークセンター（Work Centers）]** > **[設定（Configure）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサーポータル（Sponsor Portals]** > **[編集（Edit）]** を選択します
- デバイス ポータルの場合、**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** を選択します

ステップ 2 [言語ファイル（Language File）] をクリックし、ドロップダウン リストから [エクスポート（Export）] を選択します。

ステップ 3 デスクトップに zip 形式の言語ファイルを保存します。例：Hotspot.zip、Self-Registered.zip など。

言語ファイルでの言語の追加または削除

ポータル タイプに使用したい言語が言語ファイルにない場合は、新しい言語プロパティ ファイルを作成し、zip 形式の言語ファイルに追加できます。不要な言語がある場合、その言語プロパティ ファイルを削除できます。

始める前に

言語プロパティ ファイルを追加または削除するには、各ポータル タイプで使用可能な zip 形式の言語ファイルをエクスポートします。

ステップ 1 UTF-8 を表示するエディタ（Notepad ++ など）を使用して、言語を追加または削除するポータル タイプ用の定義済み言語ファイルを開きます。

複数のポータル タイプの言語を追加または削除するには、該当するすべてのポータル プロパティ ファイルを使用します。

ステップ 2 新しい言語を追加するには、既存の言語プロパティ ファイルを他のファイルと同じ命名規則を使用する新しい言語プロパティ ファイルとして zip 形式の言語ファイルに保存します。たとえば、新しい日本語の言語プロパティ ファイルを作成するには、ファイルを Japanese.properties（*LanguageName*.properties）として保存します。

ステップ 3 新しい言語プロパティ ファイルの最初の行にブラウザ ロケール値を指定して、ブラウザ ロケールに新しい言語を関連付けます。たとえば、LocaleKeys= ja,ja-jp（LocaleKeys=*browser locale value*）を Japanese.properties ファイルの最初の行に入力する必要があります。

ステップ 4 新しい言語プロパティ ファイルでディクショナリ キーのすべての値（テキスト）を更新します。

ディクショナリ キーは変更できません。キーの値だけを変更できます。

（注） 一部のディクショナリ キーだけが、値（テキスト）に HTML をサポートしています。

次のタスク

1. すべてのプロパティ ファイル（新規および既存）を zip 形式で圧縮し、新しい zip 形式の言語ファイルを作成します。フォルダやディレクトリは含めないでください。

（注） Mac を使用する場合は、ZIP ファイルを抽出すると、DS ストアが生成されます。編集後に言語ファイルを圧縮する場合は、DS ストアに ZIP を含めないでください。DS ストアの抽出方法については、https://superuser.com/questions/198569/compressing-folders-on-a-mac-without-the-ds-store を参照してください。

2. zip 形式の言語ファイルには新しい名前または元の名前を使用します。
3. エクスポート元の特定のポータルに zip 形式の言語ファイルをインポートします。

更新された言語ファイルのインポート

言語プロパティ ファイルを追加または削除したり、既存のプロパティ ファイルのテキストを更新してカスタマイズした編集済み言語ファイルをインポートできます。

（注） Word ファイルからカスタマイズした内容をコピーして貼り付けることはできません。代わりに [ファイル（File）] > [名前を付けて保存（Save As）] を選択し、Word ファイルを HTML 形式で保存します。その後、この HTML ファイルからカスタマイズした内容をコピーして貼り付けることができます。

ステップ 1 次のポータルに移動します。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Sponsor Portals）]** > **[編集（Edit）]** を選択します。
- デバイス ポータル。**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **（任意のポータル）** > **[編集（Edit）]** を選択します。

ステップ 2 [言語ファイル（Language）] をクリックし、ドロップダウン リストから [インポート（Import）] を選択します。

ステップ 3 デスクトップを参照して新しい zip 形式の言語ファイルを見つけます。

ステップ 4 エクスポートしたポータル タイプに再度インポートします。

次のタスク

変更したテキストまたは追加した新しい言語を表示するには、[表示（View In）] ドロップダウン リストから特定の言語を選択します。

ゲスト通知、承認、およびエラーメッセージのカスタマイズ

各ポータルで内で、ゲストが電子メール、SMS テキスト メッセージ、および印刷物で通知を受け取る方法をカスタマイズできます。これらの通知を使用して、次の場合にログイン クレデンシャルを電子メール送信、テキスト送信、または印刷します。

- ゲストがアカウント登録ゲスト ポータルを使用し、自分自身の登録に成功した場合。
- スポンサーがゲスト アカウントを作成し、ゲストに詳細を提供する場合。スポンサー グループ作成時にスポンサーによる SMS 通知の使用を許可するかどうかを指定できます。これらの機能を利用できる場合は、常に電子メール通知および印刷通知を使用できます。

ネットワークにアクセスしようとするアカウント登録ゲストを承認するよう要求するスポンサー宛電子メール通知をカスタマイズすることもできます。また、ゲストとスポンサーに表示されるデフォルトのエラー メッセージをカスタマイズできます。

電子メールでの通知のカスタマイズ

電子メールでゲストに送信される情報をカスタマイズできます。

始める前に

- 電子メールでの通知を有効にするように SMTP サーバを設定します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMTP サーバ（SMTP Server）]** を選択します。
- ゲストへの電子メールでの通知のサポートを設定します。**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Settings）] > [ゲスト電子メールの設定（Guest Email Settings）]** を選択します。[ゲストへの電子メール通知を有効にする（Enable email notifications to guests）] をオンにします。
- **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [ポータルのカスタマイズ（Portal Customization）]** で [HTML を使用

したポータルのカスタマイズの有効化（Enable portal customization with HTML）] がデフォルトで有効になっていることを確認します。

ステップ 1 自己登録スポンサー ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Sponsor Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ゲストへの通知（Notify Guests）] > [電子メール通知（Email Notification）]** を選択します。

ステップ 2 [グローバル ページのカスタマイズ（Global Page Customizations）] で指定されたデフォルトの [ロゴ（電子メール）（Logo (Email)）] を変更できます。

ステップ 3 [件名（Subject）] および [電子メール本文（Email body）] を指定します。電子メール メッセージに含まれる、ゲスト アカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。

ステップ 4 [設定（Settings）] では、次のことが可能です。

- 異なる電子メールで [ユーザ名とパスワードを個別に送信する（Send username and password separately）]。このオプションを選択すると、**ユーザ名電子メール通知**と**パスワード電子メール通知**をカスタマイズするための 2 つのタブが [ページのカスタマイズ（Page Customizations）] に表示されます。
- 電子メール アドレスへの [テスト電子メールの送信（Send Test Email）]。すべてのデバイスでカスタマイズをプレビューし、適切に表示されることを確認します。

ステップ 5 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

SMS テキスト メッセージ通知のカスタマイズ

SMS テキスト メッセージでゲストに送信される情報をカスタマイズできます。

始める前に

- SMS ゲートウェイに電子メールを送信して、SMS テキスト メッセージを配信するために使用される SMTP サーバを設定します。**[管理（Administration）]>[システム（System）]> [設定（Settings）] > [SMTP サーバ（SMTP Server）]** を選択します。
- SMS テキスト通知をサポートするようにスポンサー グループを設定します。
- サードパーティ SMS ゲートウェイでアカウントを設定します。**[管理（Administration）]> [システム（Systems）] > [設定（Settings）] > [SMS ゲートウェイ（SMS Gateway）]** を選択します。Cisco ISE では、テキスト メッセージが電子メールとしてゲートウェイに送信され、SMS プロバイダー経由で指定したユーザにメッセージが転送されます。
- **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [ポータルのカスタマイズ（Portal Customization）]** で [HTML を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML）] がデフォルトで有効になっていることを確認します。

ステップ 1 アカウント登録ゲスト ポータルおよびスポンサー ポータルの場合は、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータルまたはスポンサー ポータル（Guest or Sponsor Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[SMS 受信または SMS 通知（SMS Receipt or SMS Notification）]** を選択します。

ステップ 2 [メッセージ テキスト（Message Text）] をカスタマイズするには、ミニエディタと HTML タグを使用します。SMS テキスト メッセージに含まれる、ゲスト アカウント情報を指定するには、事前定義済みの変数を使用します。

ステップ 3 [設定（Settings）] では、次のことが可能です。

- 異なるテキスト メッセージで [ユーザ名とパスワードを個別に送信する（Send username and password separately）]。このオプションを選択すると、**ユーザ名メッセージ**と**パスワード メッセージ**をカスタマイズするための 2 つのタブが [ページのカスタマイズ（Page Customizations）] に表示されます。
- 携帯電話への [テスト メッセージの送信（Send Test Message）]。カスタマイズをプレビューし、情報が適切に表示されることを確認します。サポートされる電話番号の形式には、+1 ### ### ####、###-###-####、(###) ### ####、##########、1########## などがあります。

ステップ 4 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

印刷通知のカスタマイズ

ゲスト用に印刷される情報をカスタマイズできます。

（注） 各ポータル内では、印刷通知ロゴは、電子メール通知ロゴの設定から継承されます。

始める前に

[管理（Administration）] > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[ポータルのカスタマイズ（Portal Customization）]** で [HTML を使用したポータルのカスタマイズの有効化（Enable portal customization with HTML）] がデフォルトで有効になっていることを確認します。

ステップ 1 アカウント登録ゲスト ポータルおよびスポンサー ポータルの場合は、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータルまたはスポンサー ポータル（Guest or Sponsor Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[印刷受け取りまたは印刷通知（Print Receipt or Print Notification）]** を選択します。

ステップ 2 [印刷説明テキスト（Print Introduction Text）] を指定します。電子メール メッセージに含まれる、ゲスト アカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。

ステップ 3 サムネールで、または [印刷プレビュー（Print Preview）] をクリックして、カスタマイズをプレビューします。サムネールでは、HTML のカスタマイズを表示できません。
[印刷プレビュー（Print Preview）] オプションを選択した場合、アカウントの詳細を印刷できるウィンドウが表示され、そこで適切に表示されることを確認します。

ステップ 4 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

承認要求の電子メールでの通知のカスタマイズ

アカウント登録ゲストのアカウントが作成され、そのゲストがログインクレデンシャルを取得する前に、アカウント登録ゲストを承認するようスポンサーに要求できます。電子メールでスポンサーに送信される、承認を要求する情報をカスタマイズできます。この通知は、ネットワーク アクセスを許可する前にアカウント登録ゲスト ポータルを使用するアカウント登録ゲストを承認する必要があると指定した場合にのみ表示されます。

始める前に

- 電子メールでの通知を有効にするように SMTP サーバを設定します。**[管理（Administration）] > [システム（Systems）] > [設定（Settings）] > [SMTP サーバ（SMTP Server）]** を選択します。
- ゲストへの電子メールでの通知のサポートを設定します。**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [設定（Settings）] > [ゲスト電子メールの設定（Guest Email Settings）]** を選択します。[ゲストへの電子メール通知を有効にする（Enable email notifications to guests）] をオンにします。
- スポンサーに自己登録アカウントの要求を承認させるには、[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブの [アカウント登録ページの設定（Self-Registration Page Settings）] で、[アカウント登録ゲストが承認される必要がある（Require self-registered guests to be approved）] をオンにします。それによって、[ポータル ページのカスタマイズ（Portal Page Customization）] の [通知（Notifications）] の下の [承認要求の電子メール（Approval Request Email）] タブが有効になり、スポンサーに送られる電子メールをカスタマイズできます。

ステップ 1 **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [設定（Configure）] > [アカウント登録ゲスト ポータル（Self-Registered Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [承認要求電子メール（Approval Request Email）]** を選択します。ここでは次を実行できます。

a) [グローバル ページのカスタマイズ（Global Page Customizations）] で指定されたデフォルトの [ロゴ（Logo）] を変更します。

b) [件名（Subject）] および [電子メール本文（Email body）] を指定します。電子メール メッセージに含まれる、ゲスト アカウント情報を指定するには、事前定義済みの変数を使用します。テキストをカスタマイズするには、ミニエディタと HTML タグを使用します。たとえば、リクエスト承認の電子メー

ルにスポンサー ポータルへのリンクを含めるには、[リンクを作成（Create a Link）] ボタンをクリックして、スポンサー ポータルに FQDN を追加します。

c) [テスト電子メールの送信（Send Test Email）] を使用してすべてのデバイスでカスタマイズをプレビューし、適切に表示されることを確認します。

d) 忘れずに [保存（Save）] をクリックしてから、[閉じる（Close）] をクリックしてください。

ステップ 2 スポンサーが送信する承認電子メールの内容をカスタマイズします。**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Sponsor Portals）]** の順に選択し、[ポータル ページのカスタマイズ（Portal Page Customization）] を選択してから、[メール通知（Email Notification）] タブを選択します。

エラー メッセージの編集

ゲスト、スポンサー、および従業員に表示される [失敗（Failure）] ページに表示されるエラー メッセージを完全にカスタマイズできます。[失敗（Failure）] ページは、ブラックリスト ポータルを除くすべてのエンドユーザ Web ポータルで利用可能です。

ステップ 1 次のいずれかを実行します。

- ゲスト ポータルの場合は、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[メッセージ（Messages）]** > **[エラー メッセージ（Error Messages）]** の順に選択します。
- スポンサー ポータルの場合は、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Sponsor Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[メッセージ（Messages）]** > **[エラー メッセージ（Error Messages）]** の順に選択します。
- デバイス ポータルの場合は、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** >（任意のポータル）> **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[メッセージ（Messages）]** > **[エラー メッセージ（Error Messages）]** を選択します。

ステップ 2 [表示言語（View In）] ドロップダウンから、メッセージのカスタマイズ時にテキストを表示する言語を選択します。

このドロップダウン リストには、特定のポータルに関連付けられた言語ファイルのすべての言語が含まれています。ポータル ページのカスタマイズ時に行った変更でサポート対象の言語プロパティ ファイルを更新します。

ステップ 3 エラー メッセージ テキストを更新します。特定のエラー メッセージを検索するには、エラー メッセージに関連付けられた AUP を検索する **aup** などのキーワードを入力します。

ステップ 4 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

ポータルページのタイトル、コンテンツおよびラベルの文字数制限

[ポータル ページのカスタマイズ（Portal Page Customization）] タブのタイトル、テキスト ボックス、手順、フィールド、ボタン ラベル、およびその他の視覚的な要素に入力できる文字数には上限および下限があります。

ポータル ページのタイトル、コンテンツおよびラベルの文字数制限

ポータル ページの UI 要素へのナビゲーション パスは、次のとおりです。

- ゲスト ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** を選択します。
- スポンサー ポータルの場合、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** を選択します。
- デバイス ポータル。**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] >（任意のポータル）> [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** を選択します。

タイトル、テキストボックス、手順、フィールドとボタンのラベル、およびカスタマイズしているポータルページのその他のビジュアル要素のコンテンツを入力する際に、この情報を使用します。これらの更新は、カスタマイズしている特定のページにのみ適用されます。

（注） シングルバイト文字とマルチバイト文字のどちらを入力するかにかかわらず、識別される最大文字数のみをフィールドに入力できます。マルチバイト文字は文字数制限には影響しません。

フィールドのカテゴリ	フィールド	フィールド ラベル：最小文字数	フィールド ラベル：最大文字数	フィールドの入力値：最小文字数	フィールドの入力値：最大文字数
共通のページ要素	バナー タイトル				256
	フッター要素			[0]	2000
	ブラウザページのタイトル			[0]	256

フィールドのカテゴリ	フィールド	フィールド ラベル：最小文字数	フィールド ラベル：最大文字数	フィールドの入力値：最小文字数	フィールドの入力値：最大文字数
	説明テキスト			[0]	2000
	コンテンツ タイトル			[0]	256
	オプション コンテンツ 1			[0]	2000
	オプション コンテンツ 2			[0]	2000
	ボタン ラベル	[0]	64		
	チェックボックス ラベル	[0]	64		
	タブ ラベル	[0]	64		
	リンク ラベル	[0]	256		
AUP	AUP テキスト			[0]	50,000
メッセージ テキスト	メッセージテキスト（ページに表示）			[0]	2000
	メッセージテキスト（ポップアップ ウィンドウに表示）			[0]	256
フィールド ラベル	すべてのフィールド ラベル	[0]	256		
フィールド入力（一般）	一般的なフィールド入力（次の特別な場合を参照）			[0]	256
フィールド入力（特別な場合）	[アクセス コード（Access Code）] フィールド			1	20
	[登録コード（Registration Code）] フィールド			1	20
	[ユーザ名（Username）] フィールド			1	64

フィールドのカテゴリ	フィールド	フィールド ラベル：最小文字数	フィールド ラベル：最大文字数	フィールドの入力値：最小文字数	フィールドの入力値：最大文字数
	[パスワード（Password）] フィールド			1	256
	[電話番号（Phone Number）] フィールド			[0]	64
	[デバイス ID（Device ID）] フィールド			12	17

ポータルのカスタマイズ

エンドユーザ Web ポータルおよびゲスト エクスペリエンスの外観をカスタマイズできます。カスケーディング スタイル シート（CSS）言語と Javascript の使用経験がある場合、ポータル ページのレイアウトを変更することで、jQuery Mobile ThemeRoller アプリケーションを使用してポータルのテーマをカスタマイズできます。

必要なポータル ページから CSS テーマまたは言語プロパティをエクスポートすることで、すべてのフィールドを表示できます。詳細については、「ポータルのデフォルト テーマ CSS ファイルのエクスポート」を参照してください。

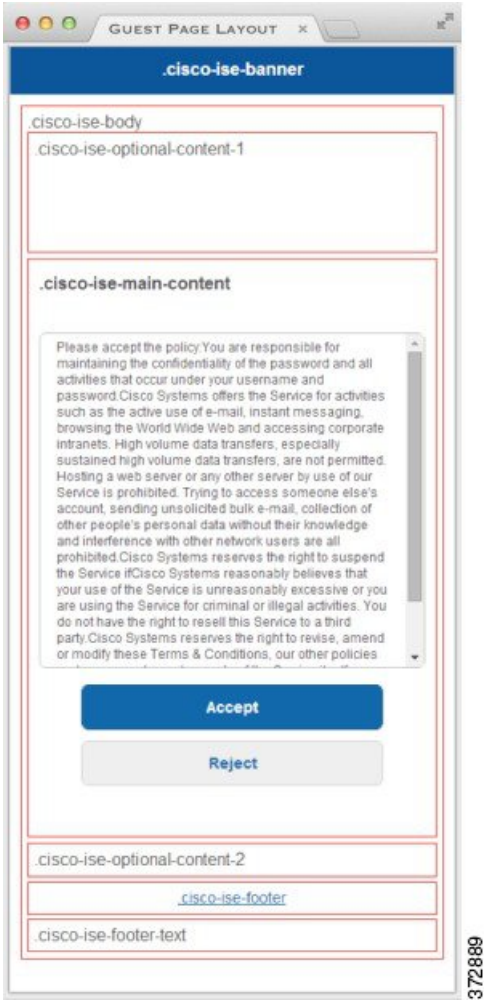
エンドユーザ ポータルのページ レイアウトの CSS クラスと説明

Cisco ISE エンドユーザ Web ポータルのページ レイアウトを定義および変更するには、次の CSS クラスを使用します。

CSS クラス名	説明
cisco-ise-banner	ロゴ、バナー イメージ、およびバナー テキストが含まれます。 スポンサー ポータルおよびデバイス ポータルでは、このクラスにコンテキスト メニューをアクティブ化できるボタンも含まれます。たとえば、このメニューで [ログアウト（Log Out）]、[パスワードの変更（Change Password）] などのオプションが含まれるポップアップ ウィンドウを表示できます。

CSS クラス名	説明
cisco-ise-body	バナーの一部ではないすべてのページの要素が含まれます。
cisco-ise-optional-content-1	デフォルトでは空です。テキスト、リンク、および HTML コードと JavaScript コードを追加できます。
cisco-ise-main-content	説明テキスト、操作ボタン、および cisco-ise-footer コンテナなど、ポータル ページのメイン コンテンツが含まれます。
cisco-ise-optional-content-2	デフォルトでは空です。テキスト、リンク、および HTML コードと JavaScript コードを追加できます。
cisco-ise-footer	フッターの一部です。**サポートへの問い合わせ**やオンライン **ヘルプ**などのリンクのプレースホルダーです。
cisco-ise-footer-text	デフォルトでは空です。著作権表示または免責事項など、ポータル ページの下部に表示するもののプレースホルダーです。

図 *16* : エンドユーザ ポータルのページ レイアウトで使用される *CSS* クラス



ポータル言語ファイルの HTML サポート

各ポータルの圧縮済み言語ファイルには、そのポータルのデフォルト言語プロパティ ファイルが含まれます。各プロパティ ファイルには、ポータルに表示される内容を定義するディクショナリ キーが含まれます。

[説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[オプション コンテンツ 1（Optional Content 1）]、[オプション コンテンツ 2（Optional Content 2）] の各テキスト ボックスの内容など、ポータルに表示されるテキストをカスタマイズすることができます。これらのテキスト ボックスには、デフォルト コンテンツがあるものと空白のものがあります。

これらのテキスト ボックスに関連付けられたディクショナリ キーの一部でのみ、その値（テキスト）で HTML がサポートされます。

ブラックリスト ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [ブラックリスト ポータル（Blacklist Portal）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.blacklist.ui_reject_message

個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [BYOD ポータル（BYOD Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_contact_instruction_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_byod_reg_limit_message
- key.guest.ui_byod_reg_content_message
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_install_winmac_instruction_message

- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_byod_welcome_aup_text
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_error_instruction_message

証明書プロビジョニング ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [証明書プロビジョニング ポータル（Certificate Provisioning Portal）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.manualcertprov.ui_login_instruction_message
- key.manualcertprov.ui_aup_instruction_message
- key.manualcertprov.ui_changepwd_instruction_message
- key.manualcertprov.ui_post_access_instruction_message
- key.manualcertprov.ui_status_csv_invalid_instruction_message
- key.manualcertprov.ui_login_optional_content_1
- key.manualcertprov.ui_login_optional_content_2
- key.manualcertprov.ui_aup_optional_content_1
- key.manualcertprov.ui_aup_optional_content_2
- key.manualcertprov.ui_changepwd_optional_content_1
- key.manualcertprov.ui_changepwd_optional_content_2
- key.manualcertprov.ui_post_access_optional_content_1
- key.manualcertprov.ui_post_access_optional_content_2
- key.manualcertprov.ui_landing_instruction_message
- key.manualcertprov.ui_status_page_single_generated_content
- key.manualcertprov.ui_status_generated_content

クライアント プロビジョニング ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [クライアント プロビジョニング ポータル（Client Provisioning Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

クレデンシャル ゲスト ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Test）]、[コンテンツ（Content）]、[オプション コンテンツ 1（Optional Content 1）]、および [オプション コンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[ゲスト ポータル（Guest Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（ Portal Page Customization）]** > **[ページ（（Pages）]** です。テキスト ボックスのミニ エディタの [HTML

ソースの表示（View HTML Source）]アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_contact_instruction_message
- key.guest.ui_login_optional_content_1
- key.guest.ui_login_optional_content_2
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_device_reg_optional_content_2
- key.guest.ui_device_reg_optional_content_1
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_max_devices_instruction_message
- key.guest.ui_max_devices_optional_content_1
- key.guest.ui_self_reg_results_instruction_message
- key.guest.notification_credentials_email_body
- key.guest.ui_max_devices_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_changepwd_instruction_message
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_aup_instruction_message
- key.guest.ui_changepwd_optional_content_2
- key.guest.ui_changepwd_optional_content_1
- key.guest.ui_self_reg_results_optional_content_2

- key.guest.ui_self_reg_results_optional_content_1
- key.guest.ui_device_reg_instruction_message
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_vlan_execute_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_device_reg_max_reached_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_aup_employee_text
- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_success_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_self_reg_optional_content_2
- key.guest.ui_self_reg_optional_content_1
- key.guest.ui_byod_reg_limit_message
- key.guest.notification_credentials_print_body
- key.guest.ui_byod_reg_content_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_aup_guest_text
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2

- key.guest.ui_self_reg_aup_text
- key.guest.ui_login_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_self_reg_results_aup_text
- key.guest.ui_device_reg_register_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_self_reg_instruction_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_client_provision_posture_agent_scan_message

ホットスポット ゲスト ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Test）]、[コンテンツ（Content）]、[オプション コンテンツ 1（Optional Content 1）]、および [オプション コンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（ Portal Page Customization）] > [ページ（（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message

- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_success_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_vlan_unsupported_error_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_aup_instruction_message
- key.guest.ui_aup_hotspot_text
- key.guest.ui_vlan_execute_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1

モバイル デバイス管理ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[オプション コンテンツ 1（Optional Content 1）]、および [オプション コンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [MDM ポータル（MDM Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.mdm.ui_contact_instruction_message

- key.mdm.ui_mdm_enrollment_after_message
- key.mdm.ui_error_optional_content_2
- key.mdm.ui_error_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_2
- key.mdm.ui_mdm_enroll_instruction_message
- key.mdm.ui_error_instruction_message
- key.mdm.ui_mdm_enrollment_link_message
- key.mdm.ui_mdm_not_reachable_message
- key.mdm.ui_contact_optional_content_2
- key.mdm.ui_mdm_continue_message
- key.mdm.ui_contact_optional_content_1

デバイス ポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.mydevices.ui_add_optional_content_1
- key.mydevices.ui_add_optional_content_2
- key.mydevices.ui_post_access_instruction_message
- key.mydevices.ui_edit_instruction_message
- key.mydevices.ui_contact_optional_content_2
- key.mydevices.ui_contact_optional_content_1
- key.mydevices.ui_changepwd_optional_content_1

- key.mydevices.ui_changepwd_optional_content_2
- key.mydevices.ui_post_access_message
- key.mydevices.ui_home_instruction_message
- key.mydevices.ui_edit_optional_content_1
- key.mydevices.ui_edit_optional_content_2
- key.mydevices.ui_add_instruction_message
- key.mydevices.ui_post_access_optional_content_2
- key.mydevices.ui_post_access_optional_content_1
- key.mydevices.ui_error_instruction_message
- key.mydevices.ui_actions_instruction_message
- key.mydevices.ui_home_optional_content_2
- key.mydevices.ui_aup_optional_content_1
- key.mydevices.ui_aup_optional_content_2
- key.mydevices.ui_home_optional_content_1
- key.mydevices.ui_changepwd_instruction_message
- key.mydevices.ui_contact_instruction_message
- key.mydevices.ui_aup_employee_text
- key.mydevices.ui_login_optional_content_2
- key.mydevices.ui_login_optional_content_1
- key.mydevices.ui_login_instruction_message
- key.mydevices.ui_error_optional_content_1
- key.mydevices.ui_error_optional_content_2
- key.mydevices.ui_aup_instruction_message

スポンサー ポータルの言語ファイルの HTML サポート

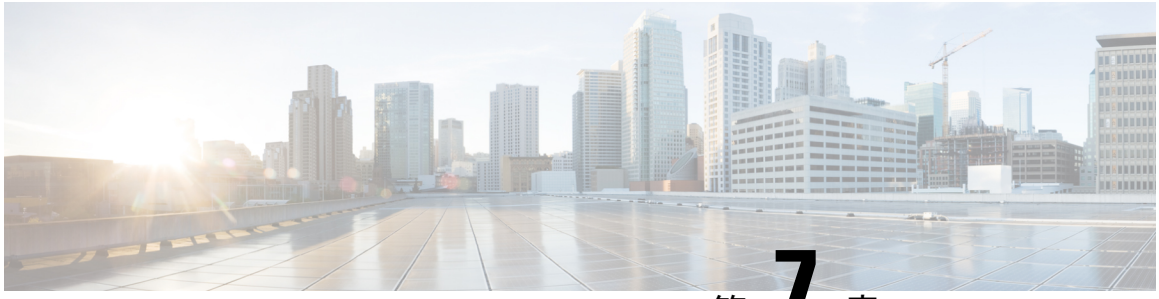
このポータルの [説明テキスト（Instructional Test）]、[コンテンツ（Content）]、[オプション コンテンツ 1（Optional Content 1）]、および [オプション コンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ゲスト アクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals & Components）]** > **[スポンサー ポータル（Sponsor Portals）]** > **[編集（Edit）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[ページ（（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.sponsor.ui_aup_instruction_message
- key.sponsor.ui_create_random_instruction_message
- key.sponsor.ui_home_instruction_message
- key.sponsor.ui_post_access_instruction_message
- key.sponsor.notification_credentials_print_body
- key.sponsor.ui_aup_sponsor_text
- key.sponsor.ui_create_accounts_access_info_instruction_message
- key.sponsor.ui_login_instruction_message
- key.sponsor.notification_credentials_email_body
- key.sponsor.ui_create_known_instruction_message
- key.sponsor.ui_create_import_instruction_message
- key.sponsor.ui_suspend_account_instruction_message
- key.sponsor.ui_post_access_message
- key.sponsor.ui_login_optional_content_2
- key.sponsor.ui_login_optional_content_1
- key.sponsor.notification_credentials_email_password_body
- key.sponsor.ui_contact_optional_content_2
- key.sponsor.ui_contact_optional_content_1
- key.sponsor.ui_login_aup_text
- key.sponsor.ui_changepwd_instruction_message
- key.sponsor.ui_create_accounts_guest_type_instruction_message
- key.sponsor.ui_changepwd_optional_content_1
- key.sponsor.ui_changepwd_optional_content_2
- key.sponsor.notification_credentials_email_username_body
- key.sponsor.ui_aup_optional_content_1
- key.sponsor.ui_aup_optional_content_2
- key.sponsor.ui_post_access_optional_content_1

- key.sponsor.ui_post_access_optional_content_2
- key.sponsor.ui_contact_instruction_message



第 7 章

アセットの可視性

外部 ID ストアを使用した Cisco ISE への管理アクセス

Cisco ISE では、Active Directory、LDAP、RSA SecureID などの外部 ID ストアを介して管理者を認証できます。外部 ID ストアを介した認証の提供に使用できる次の 2 つのモデルがあります。

- 外部認証および許可：管理者に関してローカル Cisco ISE データベースで指定されたクレデンシャルはなく、許可は、外部 ID ストア グループ メンバーシップのみに基づきます。このモデルは、Active Directory および LDAP 認証で使用されます。
- 外部認証および内部許可：管理者の認証クレデンシャルは外部 ID ソースから取得され、許可および管理者ロール割り当てはローカル Cisco ISE データベースを使用して行われます。このモデルは、RSA SecurID 認証で使用されます。この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザ名を設定する必要があります。

認証プロセス時、Cisco ISE は、外部 ID ストアとの通信が確立されなかった場合や失敗した場合はフォールバックし、内部 ID データベースから認証の実行を試行するように設計されています。また、外部認証が設定されている管理者には、ブラウザを起動してログインセッションを開始すると必ず、ログイン ダイアログの [ID ストア（Identity Store）] ドロップダウン セレクタから [内部（Internal）] を選択して Cisco ISE ローカル データベースを介した認証を要求するオプションが依然として表示されます。

上級管理者グループに所属する管理者、および外部 ID ストアを使用して認証および認可するように設定されている管理者は、CLI アクセス用に外部 ID ストアを使用して認証することもできます。

（注） 外部管理者認証を提供するこの方法は、管理者ポータルを介してのみ設定できます。Cisco ISE コマンドライン インターフェイス（CLI）では、これらの機能は設定されません。

ネットワークに既存の外部 ID ストアがまだない場合は、必要な外部 ID ストアをインストールし、これらの ID ストアにアクセスするように Cisco ISE が設定されていることを確認します。

外部認証および許可

デフォルトでは、Cisco ISE によって内部管理者認証が提供されます。外部認証を設定するには、外部 ID ストアで定義している外部管理者アカウントのパスワード ポリシーを作成する必要があります。次に、結果的に外部管理者 RBAC ポリシーの一部となるこのポリシーを外部管理者グループに適用できます。

ネットワークでは、外部 ID ストア経由の認証を提供するほかに、Common Access Card（CAC）認証デバイスを使用する必要もある場合があります。

外部認証を設定するには、次の手順を実行する必要があります。

- 外部 ID ストアを使用してパスワード ベースの認証を設定します。

- 外部管理者グループを作成します。
- 外部管理者グループ用のメニュー アクセスとデータ アクセスの権限を設定します。
- 外部管理者認証の RBAC ポリシーを作成します。

外部 ID ストアを使用したパスワード ベースの認証の設定

最初に、Active Directory や LDAP などの外部 ID ストアを使用して認証を行う管理者のためのパスワード ベースの認証を設定する必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]** を選択します。

ステップ 2 [認証方式（Authentication Method）] タブで、[パスワードベース（Password Based）] を選択し、すでに設定されている外部 ID ソースの 1 つを選択します。たとえば、作成した Active Directory インスタンスを選択します。

ステップ 3 外部 ID ストアを使用して認証を行う管理者のためのその他の特定のパスワード ポリシーを設定します。

ステップ 4 [保存（Save）] をクリックします。

外部管理者グループの作成

外部 Active Directory または LDAP 管理者グループを作成する必要があります。これにより、Cisco ISE は外部 Active Directory または LDAP ID ストアで定義されているユーザ名を使用して、ログイン時に入力した管理者ユーザ名とパスワードを検証します。

Cisco ISE は、外部リソースから Active Directory または LDAP グループ情報をインポートし、それをディクショナリ属性として保存します。次に、この属性を、外部管理者認証方式用の RBAC ポリシーを設定するときのポリシー要素の 1 つとして指定できます。

ステップ 1 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）] を選択します。

[マッピングされた外部グループ（External Groups Mapped）] 列には、内部 RBAC ロールにマップされている外部グループの数が表示されます。管理者ロールに対応する番号をクリックすると、外部グループを表示できます（たとえば、[ネットワーク管理者（Super Admin）] に対して表示されている 2 をクリックすると、2 つの外部グループの名前が表示されます）。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 名前とオプションの説明を入力します。

ステップ 4 [外部（External）] オプション ボタンを選択します。

Active Directory ドメインに接続し、参加している場合は、Active Directory インスタンス名が [名前（Name）] フィールドに表示されます。

ステップ 5 [外部グループ（External Groups）] ドロップダウン リスト ボックスから、この外部管理者グループにマッピングする Active Directory グループを選択します。

追加の Active Directory グループをこの外部管理者グループにマッピングするために「+」記号をクリックします。

ステップ 6 [保存（**Save**）] をクリックします。

内部読み取り専用管理者の作成

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザ（Admin Users）]** を選択します。

ステップ 2 [追加（Add）] をクリックして、[管理ユーザの作成（Create An Admin User）] を選択します。

ステップ 3 [読み取り専用（Read Only）] チェックボックスをオンにして読み取り専用管理者を作成します。

外部グループを読み取り専用管理者グループにマッピング

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] を選択して、外部認証ソースを設定します。詳細については、「**ユーザおよび外部 ID ソースの管理**」の章を参照してください。

ステップ 2 必要な外部 ID ソース（Active Directory や LDAP など）をクリックし、選択した ID ソースからグループを取得します。

ステップ 3 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] を選択して、管理者アクセスの認証方式を ID ソースとマッピングします。

ステップ 4 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）] を選択し、[読み取り専用管理者（Read Only Admin）] グループを選択します。

ステップ 5 タイプの [外部（External）] チェックボックスをオンにして、読み取り専用権限を提供する必要のある外部グループを選択します。

ステップ 6 [保存（Save）] をクリックします。

読み取り専用管理者グループにマップされている外部グループは、他の管理者グループに割り当てることはできません。

外部管理者グループのメニュー アクセス権限とデータ アクセス権限の設定

外部管理者グループに割り当てることができるメニュー アクセス権限とデータ アクセス権限を設定する必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [権限（Permissions）]** を選択します。

ステップ 2 次のいずれかをクリックします。

- [メニュー アクセス（Menu Access）]：外部管理者グループに属するすべての管理者に、メニューまたはサブメニュー レベルでの権限を付与することができます。メニュー アクセス権限によって、アクセスできるサブメニューまたはメニューが決定されます。
- [データ アクセス（Data Access）]：外部管理者グループに属するすべての管理者に、データ レベルでの権限を付与することができます。データ アクセス権限によって、アクセスできるデータが決定されます。

ステップ 3 外部管理者グループのメニュー アクセス権限とデータ アクセス権限を指定します。

ステップ 4 [保存（Save）] をクリックします。

外部管理者認証の RBAC ポリシーの作成

外部 ID ストアを使用して管理者を認証するように Cisco ISE を設定し、同時にカスタム メニュー アクセス権限とデータ アクセス権限を指定するには、新しい RBAC ポリシーを設定する必要があります。このポリシーには、認証用の外部管理者グループ、および外部認証と許可を管理するための Cisco ISE メニュー アクセス権限とデータ アクセス権限が存在している必要があります。

（注） これらの新しい外部属性を指定するように既存（システムプリセット）の RBAC ポリシーを変更することはできません。「テンプレート」として使用する必要がある既存のポリシーがある場合は、そのポリシーを複製し、名前を変更してから、新しい属性を割り当てます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [ポリシー（Policy）]** を選択します。

ステップ 2 ルール名、外部管理者グループ、および権限を指定します。

適切な外部管理者グループが正しい管理者ユーザ ID に割り当てられている必要があることに注意してください。問題の管理者が正しい外部管理者グループに関連付けられていることを確認します。

ステップ 3 [保存（Save）] をクリックします。

管理者としてログインした場合、Cisco ISE RBAC ポリシーが管理者 ID を認証できないと、Cisco ISE では、「認証されていない」ことを示すメッセージが表示され、管理者ポータルにアクセスできません。

内部許可を伴う認証に対する外部IDストアを使用した管理アクセスの設定

この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザ名を設定する必要があります。外部 RSA SecurID ID ストアを使用して管理者認証を提供するように Cisco ISE を設定している場合、管理者のクレデンシャル認証が RSA ID ストアによって実行されます。ただし、許可（ポリシー アプリケーション）は、依然として Cisco ISE 内部データベースに従って行われます。また、外部認証と許可とは異なる、留意する必要がある次の 2 つの重要な要素があります。

- 管理者の特定の外部管理者グループを指定する必要はありません。
- 外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザ名を設定する必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザ（Admin Users）]** を選択します。

ステップ 2 外部 RSA ID ストアの管理者ユーザ名が Cisco ISE にも存在することを確認します。[パスワード（Password）] の下の [外部（External）] オプションをクリックします。

（注） 外部管理者ユーザ ID のパスワードを指定する必要はなく、特別に設定されている外部管理者グループを関連付けられている RBAC ポリシーに適用する必要もありません。

ステップ 3 [保存（**Save**）] をクリックします。

外部認証のプロセス フロー

管理者がログインすると、ログインセッションはそのプロセスにおいて次の手順で処理されます。

1. 管理者が RSA SecurID チャレンジを送信します。
2. RSA SecurID は、チャレンジ応答を返します。
3. 管理者は、ユーザ ID とパスワードを入力する場合と同様に、ユーザ名および RSA SecurID チャレンジ応答を Cisco ISE ログイン ダイアログに入力します。
4. 管理者は、指定した ID ストアが外部 RSA SecurID リソースであることを確認します。
5. 管理者は、[ログイン（Login）] をクリックします。

ログイン時、管理者には、RBAC ポリシーで指定されたメニュー アクセス項目とデータ アクセス項目のみが表示されます。

外部 ID ソース

これらのページでは、Cisco ISE が認証および認可に使用するユーザ データが含まれる外部 ID ソースを設定および管理することができます。

LDAP ID ソースの設定

次の表では、[LDAP ID ソース（LDAP Identity Sources）] ページのフィールドについて説明します。これらのフィールドを使用してLDAPインスタンスを作成し、これに接続します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** です。

LDAP 一般設定

以下の表では、[一般（General）] タブのフィールドについて説明します。

表 *43 : LDAP* 一般設定

フィールド	使用上のガイドライン
名前（Name）	LDAP インスタンスの名前を入力します。この値は、サブジェクト DN および属性を取得するために検索で使用されます。この値は string 型で、最大長は 64 文字です。
説明（Description）	LDAP インスタンスの説明を入力します。この値は string 型で、最大長は 1024 文字です。
スキーマ（Schema）	次の組み込みのスキーマ タイプのいずれかを選択するか、カスタム スキーマを作成できます。 • Active Directory • Sun Directory Server • Novell eDirectory [スキーマ（Schema）]の隣の矢印をクリックすると、スキーマの詳細を表示できます。 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。
（注）　次のフィールドは、カスタム スキーマを選択した場合にのみ編集できます。	

フィールド	使用上のガイドライン
サブジェクト オブジェクト クラス（Subject Objectclass）	サブジェクト DN および属性を取得するために検索で使用する値を入力します。この値は string 型で、最大長は 256 文字です。
サブジェクト名属性（Subject Name Attribute）	要求内のユーザ名を含む属性の名前を入力します。この値は string 型で、最大長は 256 文字です。
グループ名属性（Group Name Attribute）	[グループ名属性（Group Name Attribute）] フィールドに CN または DN またはサポートされる属性を入力します。 • CN：共通名に基づいて LDAP ID ストア グループを取得します。 • DN：識別名に基づいて LDAP ID ストア グループを取得します。
証明書属性（Certificate Attribute）	証明書定義を含む属性を入力します。証明書ベースの認証の場合、クライアントによって提示された証明書を検証するために、これらの定義が使用されます。
グループ オブジェクト クラス（Group Objectclass）	グループとして認識されるオブジェクトを指定するために、検索に使用する値を入力します。この値は string 型で、最大長は 256 文字です。
グループ マップ属性（Group Map Attribute）	マッピング情報を含む属性を指定します。この属性は、選択した参照方向に基づいて、ユーザまたはグループ属性を指定できます。
サブジェクト オブジェクトにグループへの参照が含まれる（Subject Objects Contain Reference To Groups）	所属するグループを指定する属性がサブジェクト オブジェクトに含まれている場合は、このオプション ボタンをクリックします。
グループ オブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）	サブジェクトを指定する属性がグループ オブジェクトに含まれている場合は、このオプション ボタンをクリックします。この値はデフォルト値です。

フィールド	使用上のガイドライン
グループ内のサブジェクトをメンバー属性に保存（Subjects In Groups Are Stored In Member Attribute As）	（[グループ オブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）] オプション ボタンの選択時に限り使用可能）グループ メンバー属性にメンバーが供給される方法を指定します（デフォルトは DN）。
ユーザ情報属性（User Info Attributes）	デフォルトでは、事前設定された属性が次の組み込みのスキーマタイプのユーザ情報（名、姓、電子メール、電話、地域など）を収集するために使用されます。 • Active Directory • Sun Directory Server • Novell eDirectory 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。 [スキーマ（Schema）] ドロップダウン リストから [カスタム（Custom）] オプションを選択し、要件に基づいてユーザ情報の属性を編集することもできます。

LDAP の接続設定

以下の表では、[接続設定（Connection Settings）] タブのフィールドについて説明します。

表 *44 : LDAP* の接続設定

フィールド	使用上のガイドライン
セカンダリ サーバの有効化（Enable Secondary Server）	プライマリ LDAP サーバに障害が発生した場合にバックアップとして使用するセカンダリ LDAP サーバを有効にする場合は、このオプションをオンにします。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバの設定パラメータを入力する必要があります。
プライマリ サーバとセカンダリ サーバ（Primary and Secondary Servers）	

フィールド	使用上のガイドライン
ホスト名/IP（Hostname/IP）	LDAP ソフトウェアを実行しているマシンの IP アドレスまたはDNS名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。
ポート（Port）	LDAP サーバがリッスンしている TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバの管理者からポート番号を取得できます。
各 ISE ノードのサーバの指定（Specify server for each ISE node）	プライマリおよびセカンダリ LDAP サーバの hostnames/IP および各 PSN のポートを設定するには、このチェック ボックスをオンにします。 このオプションを有効にすると、導入のすべてのノードを表示するテーブルが表示されます。ノードを選択し、プライマリおよびセカンダリ LDAP サーバの hostname/IP および選択したノードのポートを設定する必要があります。
アクセス（Access）	[匿名アクセス（Anonymous Access）]：LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバではクライアントが区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへの、クライアント読み取りアクセスが許可されます。認証情報をサーバに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。 [認証されたアクセス（Authenticated Access）]：LDAP ディレクトリの検索が管理クレデンシャルによって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。

フィールド	使用上のガイドライン
管理者 DN（Admin DN）	管理者の DN を入力します。管理者 DN は、[ユーザ ディレクトリ サブツリー（User Directory Subtree）] 下のすべての必要なユーザの検索およびグループの検索を行う権限を持つ LDAP アカウントです。指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、該当 LDAP サーバで認証されたユーザのグループ マッピングは失敗します。
パスワード（Password）	LDAP 管理者アカウントのパスワードを入力します。
セキュアな認証（Secure Authentication）	SSL を使用して Cisco ISE とプライマリ LDAP サーバ間の通信を暗号化する場合にクリックします。[ポート（Port）] フィールドに LDAP サーバでの SSL に使用されるポート番号が入力されていることを確認します。このオプションを有効にした場合は、ルート CA を選択する必要があります。
LDAP サーバのルート CA（LDAP Server Root CA）	ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証を有効にします。
サーバ タイムアウト（Server timeout）	プライマリ LDAP サーバでの接続または認証が失敗したと判断する前に Cisco ISE がプライマリ LDAP サーバからの応答を待つ秒数を入力します。有効な値は 1 ～ 99 です。デフォルトは 10 です。
最大管理接続（Max. Admin Connections）	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、ユーザ ディレクトリ サブツリーおよびグループ ディレクトリ サブツリーの下にあるユーザおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です。デフォルトは 20 です。
N 秒ごとに再接続（Force reconnect every N seconds）	このチェック ボックスをオンにし、2 つ目のテキスト ボックスに、サーバを指定された間隔で LDAP 接続を更新するための適切な値を入力します。有効な範囲は 1 ～ 60 分です。

フィールド	使用上のガイドライン
サーバへのバインドをテスト（Test Bind To Server）	LDAP サーバの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバの詳細を編集して再テストします。
フェールオーバー	
常にプライマリ サーバに最初にアクセスする（Always Access Primary Server First）	Cisco ISE の認証と認可のために常にプライマリ LDAP サーバに最初にアクセスするように設定するには、このオプションをクリックします。
経過後にプライマリ サーバにフェールバック（Failback to Primary Server After）	Cisco ISE で接続しようとしたプライマリ LDAP サーバが到達不可能な場合、Cisco ISE はセカンダリ LDAP サーバへの接続を試行します。Cisco ISE に再びプライマリ LDAP サーバを使用するように設定するには、このオプションをクリックし、テキスト ボックスに値を入力します。

[LDAP] の [ディレクトリ構成（Directory Organization）] タブ

次の表では、[ディレクトリ構成（Directory Organization）] タブのフィールドについて説明します。

表 *45 : [LDAP]* の *[*ディレクトリ構成（*Directory Organization*）*]* タブ

フィールド	使用上のガイドライン
サブジェクト検索ベース（Subject Search Base）	すべてのサブジェクトを含むサブツリーの DN を入力します。次に例を示します。 o=corporation.com サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

フィールド	使用上のガイドライン
グループ検索ベース（Group Search Base）	すべてのグループを含むサブツリーの DN を入力します。次に例を示します。 ou = 組織ユニット、ou = 次の組織ユニット、o = corporation.com グループを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。
形式での MAC アドレスの検索（Search for MAC Address in Format）	LDAPデータベースでの検索に使用する、Cisco ISE の MAC アドレス形式を入力します。内部 ID ソースの MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で供給されます。LDAPデータベースのMACアドレスは、異なる形式で供給できます。ただし、Cisco ISE でホスト ルックアップ要求が受信されると、MACアドレスは内部形式からこのフィールドで指定した形式に変換されます。 ドロップダウン リストを使用して、特定の形式でのMACアドレスの検索を有効にします。<*format*> は次のいずれかです。 • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 選択する形式は、LDAP サーバに供給されているMACアドレスの形式と一致している必要があります。

フィールド	使用上のガイドライン
サブジェクト名の先頭から最後に出現する区切り文字まで削除（Strip start of subject name up to the last occurrence of the separator）	ユーザ名からドメインプレフィックスを削除するための適切なテキストを入力します。 ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、そのユーザ名の初めから区切り文字までのすべての文字が削除されます。ユーザ名に、<start_string> ボックスに指定した文字が複数含まれている場合は、Cisco ISE によって最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザ名が DOMAIN\user1 である場合、Cisco ISE によって user1 が LDAP サーバに送信されます。 （注） <start_string> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。
最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip end of subject name from the first occurrence of the separator）	ユーザ名からドメイン サフィックスを削除するための適切なテキストを入力します。 ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、その区切り文字からユーザ名の末尾までのすべての文字が削除されます。ユーザ名に、このフィールドに指定した文字が複数含まれている場合は、Cisco ISE によって最初の区切り文字から文字が削除されます。たとえば、区切り文字が@で、ユーザ名が *user1@domain* であれば、Cisco ISE は *user1* を LDAP サーバに送信します。 （注） *<end_string>* ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。

LDAP グループ設定

表 *46 : LDAP* グループ設定

フィールド	使用上のガイドライン
追加（Add）	[追加（Add）] > [グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）] を選択して LDAP ディレクトリからグループを選択します。 グループの追加を選択した場合は、新しいグループの名前を入力します。ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。選択したグループが [グループ（Groups）] ページに表示されます。

LDAP 属性設定

表 *47 : LDAP* 属性設定

フィールド	使用上のガイドライン
追加（Add）	[追加（Add）] > [属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）] を選択して LDAP サーバから属性を選択します。 属性を追加する場合は、新しい属性の名前を入力します。ディレクトリから選択する場合は、ユーザ名を入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザの属性を取得します。選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

LDAP 詳細設定

以下の表では、[詳細設定（Advanced Settings）] タブのフィールドについて説明します。

表 *48 : LDAP* 詳細設定

フィールド	使用上のガイドライン
[パスワードの変更を有効にする（Enable password change）]	デバイス管理に PAP プロトコルを使用し、ネットワーク アクセスに RADIUS EAP-GTC プロトコルを使用している場合に、パスワードが期限切れになるか、またはパスワードがリセットされるときに、ユーザがパスワードを変更できるようにするには、このチェックボックスをオンにします。サポートされていないプロトコルでは、ユーザ認証が失敗します。このオプションでは、ユーザが次回のログイン時にパスワードを変更できるようにすることもできます。

関連トピック

LDAP ディレクトリ サービス （696 ページ）
LDAP ユーザ認証 （697 ページ）
LDAP ユーザ ルックアップ （702 ページ）
LDAP ID ソースの追加 （703 ページ）

RADIUS トークン ID ソースの設定

次の表では、RADIUS 外部 ID ソースを設定し、それに接続するために使用できる [RADIUS トークン ID ソース（RADIUS Token Identity Sources）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）]** です。

表 *49 : RADIUS* トークン *ID* ソースの設定

フィールド	使用上のガイドライン
名前（Name）	RADIUS トークン サーバの名前を入力します。許容最大文字数は 64 文字です。
説明	RADIUS トークン サーバの説明を入力します。最大文字数は 1024 です。
SafeWord サーバ（SafeWord Server）	RADIUS ID ソースが SafeWord サーバである場合はこのチェックボックスをオンにします。

フィールド	使用上のガイドライン
セカンダリ サーバの有効化（Enable Secondary Server）	プライマリに障害が発生した場合にバックアップとして使用する Cisco ISE のセカンダリ RADIUS トークン サーバを有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにする場合は、セカンダリ RADIUS トークン サーバを設定する必要があります。
常にプライマリ サーバに最初にアクセスする（Always Access Primary Server First）	Cisco ISE が常にプライマリ サーバに最初にアクセスするには、このオプション ボタンをクリックします。
経過後にプライマリ サーバにフォールバック（Fallback to Primary Server after）	プライマリ サーバに到達できない場合に Cisco ISE がセカンダリ RADIUS トークン サーバを使用して認証できる時間（分単位）を指定するには、このオプション ボタンをクリックします。この時間を過ぎると、Cisco ISE はプライマリ サーバに対する認証を再試行します。
プライマリ サーバ（Primary Server）	
ホスト名/アドレス（Host IP）	プライマリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。
共有秘密鍵（Shared Secret）	この接続のプライマリ RADIUS トークン サーバで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	プライマリ RADIUS トークン サーバが受信しているポート番号を入力します。
サーバ タイムアウト（Server timeout）	プライマリ サーバがダウンしていると判断する前に Cisco ISE がプライマリ RADIUS トークン サーバからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	セカンダリ サーバ（定義されている場合）に移動する前、またはセカンダリ サーバが定義されていない場合は要求をドロップする前に、Cisco ISE がプライマリ サーバへの再接続を試行する回数を指定します。
セカンダリ サーバ（Secondary Server）	

フィールド	使用上のガイドライン
ホスト名/アドレス（Host IP）	セカンダリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。
共有秘密鍵（Shared Secret）	この接続のセカンダリ RADIUS トークン サーバで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	セカンダリ RADIUS トークン サーバが受信しているポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは 1812 です。
サーバ タイムアウト（Server timeout）	セカンダリ サーバがダウンしていると判断する前に Cisco ISE がセカンダリ RADIUS トークン サーバからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	要求をドロップする前に Cisco ISE がセカンダリ サーバへの再接続を試行する回数を指定します。

関連トピック

RADIUS トークン ID ソース （722 ページ）
RADIUS トークン サーバの追加 （728 ページ）

RSA SecurID ID ソースの設定

次の表では、RSA SecurID ID ソースを作成し、それに接続するために使用できる [RSA SecurID ID ソース（RSA SecurID Identity Sources）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[RSA SecurID]** です。

RSA プロンプトの設定

次の表では、[RSA プロンプト（RSA Prompts）] タブ内のフィールドについて説明します。

表 50 : RSA プロンプトの設定

フィールド	使用上のガイドライン
パスコード プロンプトの入力（Enter Passcode Prompt）	パス コードを取得するテキスト文字列を入力します。
次のトークン コードの入力（Enter Next Token Code）	次のトークンを要求するテキスト文字列を入力します。

フィールド	使用上のガイドライン
PIN タイプの選択（Choose PIN Type）	PIN タイプを要求するテキスト文字列を入力します。
システム PIN の受け入れ（Accept System PIN）	システム生成の PIN を受け付けるテキスト文字列を入力します。
英数字 PIN の入力（Enter Alphanumeric PIN）	英数字 PIN を要求するテキスト文字列を入力します。
数値 PIN の入力（Enter Numeric PIN）	数値 PIN を要求するテキスト文字列を入力します。
PIN の再入力（Re-enter PIN）	ユーザに PIN の再入力を要求するテキスト文字列を入力します。

RSA メッセージ設定（RSA Message Settings）

次の表では、[RSA メッセージ（RSA Messages）] タブ内のフィールドについて説明します。

表 *51 : RSA* メッセージ設定（*RSA Messages Settings*）

フィールド	使用上のガイドライン
システム PIN メッセージの表示（Display System PIN Message）	システム PIN メッセージのラベルにするテキスト文字列を入力します。
システム PIN 通知の表示（Display System PIN Reminder）	ユーザに新しい PIN を覚えるように通知するテキスト文字列を入力します。
数字を入力する必要があるエラー（Must Enter Numeric Error）	PIN には数字のみを入力するようにユーザに指示するメッセージを入力します。
英数字を入力する必要があるエラー（Must Enter Alpha Error）	PIN には英数字のみを入力するようにユーザに指示するメッセージを入力します。
PIN 受け入れメッセージ（PIN Accepted Message）	ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
PIN 拒否メッセージ（PIN Rejected Message）	ユーザの PIN がシステムによって拒否されたときに表示されるメッセージを入力します。
ユーザの PIN が異なるエラー（User Pins Differ Error）	ユーザが不正な PIN を入力したときに表示されるメッセージを入力します。

フィールド	使用上のガイドライン
システム PIN 受け入れメッセージ（System PIN Accepted Message）	ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
不正パスワード長エラー（Bad Password Length Error）	ユーザが指定した PIN が、PIN 長ポリシーで指定されている範囲に収まらない場合に表示されるメッセージを入力します。

関連トピック

RSA ID ソース （730 ページ）
Cisco ISE と RSA SecurID サーバの統合 （730 ページ）
RSA ID ソースの追加 （734 ページ）

Cisco ISE ユーザ

この章では、ユーザという用語はネットワークに定期的にアクセスする従業員と請負業者に加え、スポンサーおよびゲスト ユーザを意味します。スポンサーは、スポンサー ポータルからゲスト ユーザ アカウントを作成および管理する組織の従業員または請負業者となります。ゲストユーザは、一定期間組織のネットワーク リソースへのアクセスを必要とする外部ビジターです。

Cisco ISE ネットワーク上のリソースとサービスにアクセスするすべてのユーザのアカウントを作成する必要があります。従業員、請負業者、およびスポンサー ユーザは、管理者ポータルから作成されます。

ユーザ ID

ユーザ ID は、ユーザに関する情報を保持するコンテナに似ており、ユーザのネットワーク アクセス クレデンシャルを形成します。各ユーザの ID はデータにより定義され、ユーザ名、電子メール アドレス、パスワード、アカウントの説明、関連付けられている管理者グループ、ユーザ グループ、ロールなどが含まれます。

ユーザ グループ

ユーザ グループは、特定の一連の Cisco ISE サービスおよび機能へのアクセスを許可する共通の権限セットを共有する個々のユーザの集合です。

ユーザ ID グループ

ユーザのグループ ID は、同じグループに属している特定のユーザ グループを識別および説明する要素で構成されています。グループ名は、このグループのメンバーが持っている機能ロールの説明です。グループは、そのグループに属しているユーザのリストです。

デフォルト ユーザ ID グループ

Cisco ISE には、次の事前定義されたユーザ ID グループが用意されています。

- 従業員：組織の従業員はこのグループに所属します。
- SponsorAllAccount：Cisco ISE ネットワークのすべてのゲスト アカウントを一時停止または復元できるスポンサー ユーザ。
- SponsorGroupAccounts：同じスポンサー ユーザ グループのスポンサー ユーザが作成したゲスト アカウントを一時停止できるスポンサー ユーザ。
- SponsorOwnAccounts：自身が作成したゲストアカウントのみを一時停止できるスポンサー ユーザ。
- ゲスト：ネットワークのリソースへの一時的なアクセスを必要とする訪問者。
- ActivatedGuest：アカウントが有効で、アクティブになっているゲスト ユーザ。

ユーザ ロール

ユーザ ロールは、ユーザが Cisco ISE ネットワークで実行できるタスクやアクセスできるサービスを決定する権限セットです。ユーザ ロールは、ユーザ グループに関連付けられています（ネットワーク アクセス ユーザなど）。

ユーザ アカウントのカスタム属性

Cisco ISE では、ネットワーク アクセス ユーザと管理者の両方に対して、ユーザ属性に基づいてネットワーク アクセスを制限することができます。Cisco ISE では、一連の事前定義されたユーザ属性が用意されており、カスタム属性を作成することもできます。両方のタイプの属性が認証ポリシーを定義する条件で使用できます。パスワードが指定された基準を満たすように、ユーザ アカウントのパスワード ポリシーも定義できます。

カスタム ユーザ属性

[ユーザのカスタム属性（User Custom Attributes）] ページ（[管理（Administration）] > [IDの管理（Identity Management）] > [設定（Settings）] > [ユーザのカスタム属性（User Custom Attributes）]）で、追加のユーザ アカウント属性を設定できます。このページに事前定義済みユーザ属性のリストを表示することもできます。事前定義済みユーザ属性を編集することはできません。

新しいカスタム属性を追加するには、[ユーザのカスタム属性（User Custom Attributes）] ペインに必要な詳細を入力します。[ユーザのカスタム属性（User Custom Attributes）] ページに追加するカスタム属性とデフォルト値が、ネットワーク アクセス ユーザ（[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] > [追加（Add）] / [編集（Edit）]）または管理者ユーザ（[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザ（Admin Users）] > [追加（Add）]/[編集（Edit）]）の追加または編集時に表示されます。これらのデフォルト値は、ネットワーク アクセスまたは管理者ユーザの追加または編集時に変更できます。

ユーザが [ユーザのカスタム属性（User Custom Attributes）] ページで、カスタム属性に対し次のデータ型を選択できます。

- [文字列（String）]：文字列の最大長（文字列属性値の最大許容長）を指定できます。
- [整数（Integer）]：最小値と最大値を設定できます（最小、最大の許容可能な整数値を指定します）。
- [列挙（Enum）]：各パラメータに次の値を指定できます。
  - 内部値
  - 表示値

  デフォルト パラメータを指定することもできます。ネットワーク アクセスまたは管理者ユーザの追加または編集時に、[表示（Display）] フィールドに追加する値が表示されます。
- [浮動小数点数（Float）]
- [パスワード（Password）]：最大文字列の長さを指定できます。
- [Long 型（Long）]：最小値と最大値を設定できます。
- [IP]：デフォルトの IPv4 または IPv6 アドレスを指定できます。
- [ブール型（Boolean）]：True または False をデフォルト値として設定できます。
- [日付（Date）]：カレンダーから日付を選択し、デフォルト値として設定できます。日付は yyyy-mm-dd 形式で表示されます。

ネットワーク アクセスまたは管理者ユーザの追加または編集時、これを必須属性とする場合は、[必須（Mandatory）] チェック ボックスをオンにします。カスタム属性のデフォルト値を設定することもできます。

カスタム属性は、認証ポリシーで使用できます。カスタム属性に設定するデータ型と許容範囲は、ポリシー条件のカスタム属性の値に適用されます。

ユーザ認証の設定

すべての外部 ID ストアで、ネットワーク アクセス ユーザが自分のパスワードを変更できるわけではありません。詳細については、各 ID ソースのセクションを参照してください。

ネットワーク使用パスワード ルールは、**[管理（Administration）] > [IDの管理（Identity Management）] > [設定（Settings）] > [ユーザ認証設定（User Authentication Settings）]** で設定できます。。

[パスワードポリシー（Password Policy）] タブの一部のフィールドに関する追加情報を次に示します。

- **必須の文字**：

  大文字または小文字が必要なユーザ パスワード ポリシーを設定するときに、ユーザの言語でこれらの文字がサポートされていない場合、ユーザはパスワードを設定できません。UTF-8 文字をサポートするには、次のチェックボックス オプションをオフにする必要があります。

  - [小文字の英文字（Lowercase alphabetic characters）]
  - 大文字の英文字（Uppercase alphabetic characters）

- **パスワード変更差分**：

  現在のパスワードを新しいパスワードに変更するときに変更する必要がある最小文字数を指定します。Cisco ISE では、文字の位置を変更することは変更とみなされません。

  たとえば、パスワードの差分が 3 で、現在のパスワードが「?Aa1234?」の場合、「?Aa1567?」（「5」、「6」、「7」は 3 つの新しい文字です）は有効な新しいパスワードです。「?Aa1562?」は、「?」、「2」、および「?」文字が現在のパスワードに含まれているため無効です。文字位置が変更された場合でも、同じ文字が現在のパスワードに含まれているため、「Aa1234??」は無効になります。

  また、パスワード変更差分では、以前の X パスワードが考慮されます。この X は、[パスワードは前のバージョンと異なっている必要があります（Password must be different from the previous versions）] の値です。パスワードの差分が 3 で、パスワードの履歴が 2 である場合は、過去 2 つのパスワードの一部ではない 4 文字を変更する必要があります。

- [辞書の単語（Dictionary words）]：辞書の単語、辞書の単語の逆順での使用、単語内の文字を別の文字で置き換えた単語の使用を制限する場合は、このチェックボックスをオンにします。。

  「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば、「Pa$$w0rd」です。

  - [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。
  - [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択（Choose File）] をクリックし、カスタム辞書ファイルを選択します。このテキスト ファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。

エンドユーザは、定期的にパスワードを変更し、ユーザアカウントが一時的に無効にならないようにする必要があります。[パスワードの有効期間（Password Lifetime）] セクションを使用して、パスワードのリセット間隔と通知を更新できます。パスワードの有効期間を設定するには、[パスワードが変更されていなかった場合は__後にユーザアカウントを無効にする（Disable user account after __ days if password was not changed）] チェックボックスをオンにし、入力ボックスに日数を入力します。パスワードのリセットに関する通知を有効にするには、[パスワードの有効期限が切れる __ 日前に通知を表示する（Display reminder __ days prior to password expiration）] チェックボックスをオンにして、パスワードの有効期限が切れる前にユーザに通知を送信する日数を入力値に入力します。

[アカウント無効化ポリシー（Account Disable Policy）] タブでは、既存のユーザ アカウントを無効にするタイミングに関するルールを設定できます。詳細については、「グローバルにユーザ アカウントを無効にする」を参照してください。

関連トピック

ユーザ アカウントのカスタム属性 （566 ページ）
ユーザの追加 （569 ページ）

ユーザおよび管理者用の自動パスワードの生成

Cisco ISE では、ユーザおよび管理者の作成ページで Cisco ISE パスワード ポリシーに従うインスタント パスワードを生成するための [パスワードの生成（Generate Password）] オプションが導入されています。これにより、ユーザまたは管理者は設定する安全なパスワードを考えるために時間を費やすことなく、Cisco ISE によって生成されたパスワードを使用することができます。

[パスワードの生成（Generate Password）] オプションは、Cisco ISE Web インターフェイスの次の 3 つの場所で使用できます。

- ユーザ：[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]。
- 管理者：[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザ（Admin Users）]。
- ログイン管理者（現在の管理者）：[設定（Settings）]>[アカウント設定（Account Settings）] > [パスワードの変更（Change Password）]。

内部ユーザ操作

-

ユーザの追加

Cisco ISE では、Cisco ISE ユーザの属性を表示、作成、編集、複製、削除、ステータス変更、インポート、エクスポート、または検索できます。

Cisco ISE 内部データベースを使用する場合、Cisco ISE ネットワークのリソースまたはサービスへのアクセスを必要とするすべての新規ユーザのアカウントを作成する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]** を選択します。

[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ID（Identities）] > [ユーザ（Users）] ページにアクセスすることによって、ユーザを作成することもできます。

ステップ 2 新しいユーザを作成するには、[追加（Add）]（+）をクリックします。

ステップ 3 フィールドの値を入力します。

!、%、:、;、[、{、|、}、]、`、?、=、<、>、\、および制御文字をユーザ名に使用しないでください。スペースのみのユーザ名も許可されません。BYOD 用に Cisco ISE 内部認証局（CA）を使用する場合、ここに入力したユーザ名がエンドポイント証明書の共通名として使用されます。Cisco ISE 内部 CA は、「+」または「*」の文字を [共通名（Common Name）] フィールドでサポートしていません。

ステップ 4 [送信（Submit）] をクリックして、Cisco ISE 内部データベースに新しいユーザを作成します。

Cisco ISE ユーザ データのエクスポート

Cisco ISE 内部データベースからユーザ データをエクスポートしなければならない場合があります。Cisco ISE では、パスワード保護された csv ファイル形式でユーザ データをエクスポートすることができます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]** を選択します。

ステップ 2 データをエクスポートするユーザに対応するチェックボックスをオンにします。

ステップ 3 [選択済みをエクスポート（Export Selected）] をクリックします。

ステップ 4 [キー（Key）] フィールドに、パスワードを暗号化するためのキーを入力します。

ステップ 5 [エクスポート開始（Start Export）] をクリックして、users.csv ファイルを作成します。

ステップ 6 [OK] をクリックして、users.csv ファイルをエクスポートします。

Cisco ISE 内部ユーザのインポート

新しい内部アカウントを作成するために、CSV ファイルを使用して新しいユーザデータを ISE にインポートできます。ユーザアカウントをインポートできるページから、テンプレート CSV ファイルをダウンロードできます。**[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]** でユーザをインポートできます。スポンサーはスポンサー ポータルでユーザをインポートできます。ゲスト アカウントのインポート方法については、『Sponsor Portal Guide』で説明しています。スポンサー ゲスト アカウントで使用される情報タイプの設定に関する詳細については、スポンサーアカウント作成のためのアカウント コンテンツの設定 （421 ページ） を参照してください。

（注） CSV ファイルにカスタム属性が含まれている場合、カスタム属性に設定するデータ タイプと許容範囲は、インポート時にカスタム属性の値に適用されます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]** を選択します。

ステップ 2 [インポート（Import）] をクリックして、カンマ区切りテキストファイルからユーザをインポートします。

カンマ区切りテキスト ファイルがない場合は、[テンプレートの生成（Generate a Template）] をクリックし、ヘッダー行に値が取り込まれている CSV ファイルを作成します。

ステップ 3 [ファイル（File）] テキスト ボックスに、インポートするユーザが含まれたファイル名を入力するか、[参照（Browse）] をクリックして、ファイルが配置されている場所に移動します。

ステップ 4 新しいユーザの作成、および既存のユーザの更新の両方を実行する必要がある場合は、[新しいユーザの作成、および新しいデータで既存のユーザを更新（Create new user(s) and update existing user(s) with new data）] チェックボックスをオンにします。

ステップ 5 Cisco ISE 内部データベースに変更を保存するには、[保存（Save）] をクリックします。

（注） すべてのネットワーク アクセス ユーザを一度に削除しないことを推奨します。一度に削除すると、特に非常に大規模なデータベースを使用している場合は、CPU スパイクとサービスのクラッシュにつながる場合があるためです。

エンドポイント設定

次の表に、エンドポイントを作成し、エンドポイントにポリシーを割り当てるために使用できる [エンドポイント（Endpoints）] ページのフィールドを示します。このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** です。

表 *52 :* エンドポイント設定

フィールド	使用上のガイドライン
MAC アドレス（MAC Address）	エンドポイントを静的に作成するには、MAC アドレスを 16 進数形式で入力します。 MAC アドレスは、Cisco ISE 対応のネットワークに接続するインターフェイスのデバイス ID です。

フィールド	使用上のガイドライン
スタティック割り当て（Static Assignment）	[エンドポイント（Endpoints）] ページでエンドポイントを静的に作成する場合このチェックボックスをオンにすると、静的割り当てのステータスが static に設定されます。 エンドポイントのスタティック割り当てのステータスを静的から動的に、または動的から静的に切り替えできます。
ポリシー割り当て	（スタティック割り当てが選択されていない限り、デフォルトで無効）[ポリシー割り当て（Policy Assignment）] ドロップダウン リストから一致するエンドポイント ポリシーを選択します。 次のいずれかを実行できます。 • 一致するエンドポイント ポリシーを選択しないで、デフォルトのエンドポイント ポリシーである不明を使用する場合、スタティック割り当てステータスはエンドポイントに対して動的に設定され、それにより、エンドポイントの動的プロファイリングが可能になります。 • 不明ではなく、一致するエンドポイント ポリシーを選択する場合、スタティック割り当てステータスはそのエンドポイントに対して静的に設定され、[スタティック割り当て（Static Assignment）] チェックボックスが自動的にオンにされます。

フィールド	使用上のガイドライン
スタティック グループ割り当て（Static Group Assignment）	（[スタティック グループ割り当て（Static Group Assignment）] が選択されていない限り、デフォルトで無効）エンドポイントを ID グループに静的に割り当てる場合、このチェックボックスをオンにします。 このチェックボックスをオンにした場合、プロファイリング サービスは、前に他のエンドポイント ID グループに動的に割り当てられたエンドポイントの次のエンドポイント ポリシーの評価時に、そのエンドポイント ID グループを変更しません。 このチェックボックスをオフにした場合、エンドポイント ID グループは、ポリシー設定に基づいて ISE プロファイラにより割り当てられたダイナミック グループです。[スタティック グループ割り当て（Static Group Assignment）] オプションを選択しない場合、エンドポイントは、エンドポイント ポリシーの次回評価時に一致する ID グループに自動的に割り当てられます。

フィールド	使用上のガイドライン
ID グループ割り当て	エンドポイントを割り当てるエンドポイント ID グループを選択します。 エンドポイントを静的に作成する場合、またはエンドポイントのエンドポイント ポリシーの評価時に [一致する ID グループの作成（Create Matching Identity Group）] オプションを使用しない場合は、エンドポイントを ID グループに割り当てることができます。 Cisco ISE には、次のシステムによって作成された次のエンドポイント ID グループがあります。 • ブラックリスト • GuestEndpoints • プロファイル済み • Cisco IP-Phone • ワークステーション • RegisteredDevices • 不明

関連トピック

識別されたエンドポイント （822 ページ）

ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 （816 ページ）

エンドポイントの、LDAP からのインポートの設定

次の表では、LDAP サーバからのエンドポイントのインポートに使用できる [LDAP からのインポート（Import from LDAP）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** です。

表 *53 :* エンドポイントの、*LDAP* からのインポートの設定

フィールド	使用上のガイドライン
接続の設定	
ホスト	LDAP サーバのホスト名または IP アドレスを入力します。

フィールド	使用上のガイドライン
[ポート（Port）]	LDAP サーバのポート番号を入力します。デフォルト ポート 389 を使用して LDAP サーバからインポートするか、デフォルト ポート 636 を使用して SSL を介して LDAP サーバからインポートできます。 （注） Cisco ISE では、任意の設定済みポート番号をサポートします。設定済みの値は、LDAP サーバ接続詳細に一致する必要があります。
セキュア接続を有効にする（Enable Secure Connection）	SSL を介して LDAP サーバからインポートするには、[セキュア接続を有効にする（Enable Secure Connection）] チェックボックスをオンにします。
ルート CA 証明書名	ドロップダウン矢印をクリックして、信頼できる CA 証明書を表示します。 ルート CA 証明書名は、LDAP サーバに接続する場合に必要となる信頼できる CA 証明書を指します。Cisco ISE 内の CA 証明書は、追加（インポート）、編集、削除、およびエクスポートが可能です。
匿名バインド（Anonymous Bind）	匿名バインドを有効にするには、[匿名バインド（Anonymous Bind）] チェックボックスをオンにします。 [匿名バインド（Anonymous Bind）] チェックボックスをオンにするか、または slapd.conf コンフィギュレーション ファイルの LDAP 管理者クレデンシャルを入力する必要があります。
管理者 DN（Admin DN）	slapd.conf コンフィギュレーション ファイルで LDAP 管理者に設定されている識別名（DN）を入力します。 管理者 DN フォーマット例：cn=Admin, dc=cisco.com, dc=com
[パスワード（Password）]	LDAP 管理者に設定されたパスワードを slapd.conf コンフィギュレーション ファイルに入力します。

フィールド	使用上のガイドライン
ベース DN（Base DN）	親エントリの認定者名を入力します。 ベース DN フォーマット例：dc=cisco.com, dc=com
クエリ設定（Query Settings）	
MAC アドレス objectClass（MAC Address objectClass）	MACアドレスのインポートに使用するクエリフィルタを入力します。たとえば、ieee802Device です。
MAC アドレス属性名（MAC Address Attribute Name）	インポートに対して返される属性名を入力します。たとえば、macAddress です。
プロファイル属性名（Profile Attribute Name）	LDAP 属性の名前を入力します。この属性は、LDAP サーバで定義されている各エンドポイント エントリのポリシー名を保持します。 [プロファイル属性名（Profile Attribute Name）] フィールドを設定する場合は、次の点を考慮してください。 • [プロファイル属性名（Profile Attribute Name）] フィールドでこの LDAP 属性を指定しない場合、またはこの属性を誤って設定した場合、インポート操作時にエンドポイントは「不明」としてマークされ、これらのエンドポイントは一致するエンドポイント プロファイリング ポリシーに個別にプロファイリングされます。 • [プロファイル属性名（Profile Attribute Name）] フィールドで LDAP 属性を設定した場合、その属性値は、エンドポイント ポリシーが Cisco ISE 内の既存のポリシーに一致することを確認するために検証され、エンドポイントがインポートされます。エンドポイント ポリシーが既存のポリシーと一致しない場合、それらのエンドポイントはインポートされません。
タイムアウト（秒）（Time Out [seconds]）	時間を秒単位（1 ～ 60 秒）で入力します。

関連トピック

識別されたエンドポイント （822 ページ）
LDAP サーバからのエンドポイントのインポート （821 ページ）

ID グループ操作

ユーザ ID グループの作成

ユーザ ID グループを追加する前に、ユーザ ID グループを作成する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [アイデンティティ グループ（Identity Groups）] > [ユーザ ID グループ（User Identity Groups）] > [追加（Add）]** を選択します。

[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ユーザIDグループ（User Identity Groups）] > [アイデンティティグループ（Identity Groups）] > [ユーザIDグループ（User Identity Groups）] > [追加（Add）] ページにアクセスして、ユーザ ID グループを作成することもできます。

ステップ 2 [名前（Name）] フィールドおよび [説明（Description）] フィールドに値を入力します。[名前（Name）] フィールドでサポートされる文字は次のとおりです：スペース、# $ & ‘ ( ) * + - . / @ _。

ステップ 3 [送信（Submit）] をクリックします。

関連トピック

ユーザ ID グループ （566 ページ）

ユーザ ID グループのエクスポート

Cisco ISE では、ローカルに設定されたユーザ ID グループを csv ファイル形式でエクスポートすることができます。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザ ID グループ（User Identity Groups）] を選択します。

ステップ 2 エクスポートするユーザ ID グループに対応するチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 [OK] をクリックします。

ユーザ ID グループのインポート

Cisco ISE では、ユーザ ID グループを csv ファイル形式でインポートすることができます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザ ID グループ（User Identity Groups）]** を選択します。

ステップ 2 インポートファイルに使用するテンプレートを取得するには、[テンプレートの生成（Generate a Template）] をクリックします。

ステップ 3 [インポート（Import）] をクリックして、カンマ区切りテキスト ファイルからネットワーク アクセス ユーザをインポートします。

ステップ 4 新しいユーザ ID グループの追加、および既存のユーザ ID グループの更新の両方を実行する必要がある場合は、[新しいデータで既存のデータを上書き（Overwrite existing data with new data）] チェックボックスをオンにします。

ステップ 5 [インポート（Import）] をクリックします。

ステップ 6 Cisco ISE データベースに変更を保存するには、[保存（Save）] をクリックします。

エンドポイント ID グループの設定

次の表に、エンドポイント グループを作成するために使用できる [エンドポイント ID グループ（Endpoint Identity Groups）] ページのフィールドを示します。このページへのナビゲーション パスは、[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）] です。

表 *54* : エンドポイント *ID* グループの設定

フィールド	使用上のガイドライン
名前（Name）	作成するエンドポイント ID グループの名前を入力します。
説明	作成するエンドポイント ID グループの説明を入力します。
親グループ（Parent Group）	新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを、[親グループ（Parent Group）] ドロップダウン リストから選択します。

関連トピック

識別されたエンドポイントの、エンドポイント ID グループでのグループ化 （825 ページ）
エンドポイント ID グループの作成 （825 ページ）

最大同時セッション数の設定

最適なパフォーマンスを得るために、同時ユーザ セッション数を制限できます。ユーザ レベルまたはグループ レベルで制限を設定できます。最大ユーザ セッションの設定に応じて、セッション カウントはユーザに適用されます。

ISE ノードごとに各ユーザの同時セッションの最大数を設定できます。この制限を超えるセッションは拒否されます。

ステップ 1 [管理（Administration）]>[システム（System）]>[設定（Settings）]>[最大セッション数（Max Sessions）]>[ユーザ（User）] の順に選択します。

ステップ 2 次のいずれかを実行します。

- 各ユーザに許可される同時セッションの最大数を、[ユーザごとの最大セッション数（Maximum Sessions per User）] フィールドに入力します。

  または

- ユーザのセッション数を無制限にするには、[セッション数無制限（Unlimited Sessions）] チェック ボックスをオンにします。このオプションは、デフォルトで選択されます。

ステップ 3 [保存（Save）] をクリックします。

セッションの最大数がユーザ レベルとグループ レベルの両方で設定されている場合、小さい方の値が優先されます。たとえば、ユーザの最大セッション値が 10 に設定されていて、ユーザが属するグループの最大セッション値が 5 に設定されている場合、ユーザは最大で 5 つのセッションのみを持つことができます。

最大セッション数を 1 に設定しており、ユーザが接続する WLC でサポートされているバージョンの WLC が稼働していない場合、ユーザに対し、切断してから再接続するよう指示するエラーが表示されます。

グループの最大同時セッション数

ID グループの最大同時セッション数を設定できます。

グループ内の少人数のユーザによってすべてのセッションが使用される場合があります。他のユーザからの新しいセッションの作成要求は、セッション数がすでに最大設定値に達しているため、拒否されます。Cisco ISE では、グループ内の各ユーザに最大セッション制限を設定できます。特定の ID グループに所属する各ユーザは、同じグループの他のユーザが開いているセッション数に関係なく、制限以上はセッションを開くことができません。特定のユーザのセッション制限を計算する場合は、ユーザ 1 人あたりのグローバル セッション制限、ユーザが所属する ID グループあたりのセッション制限、グループ内のユーザ 1 人あたりのセッション制限のいずれかの最小設定値が優先されます。

ID グループの同時セッションの最大数を設定するには、次の手順に従います。

ステップ 1 [管理（Administration）]>[システム（System）]>[設定（Settings）]>[最大セッション数（Max Sessions）]>[グループ（Group）] の順に選択します。

設定した ID グループがすべて一覧表示されます。

ステップ 2 編集するグループの横にある [編集（Edit）] アイコンをクリックして、次の値を入力します。

- そのグループに許可される同時セッションの最大数。グループのセッションの最大数を 100 に設定した場合、グループのすべてのメンバーによって確立されたすべてのセッションの総数は 100 を超えることはできません。

  （注）　グループ階層に基づいてグループ レベルのセッションが適用されます。

- そのグループの各ユーザに許可される同時セッションの最大数。このオプションは、グループの最大セッション数を上書きします。

グループの同時セッションの最大数、またはグループ内のユーザの同時セッションの最大数を [無制限（Unlimited）] に設定するには、[グループの最大セッション数/グループ内のユーザの最大セッション数（Max Sessions for User in Group/Max Sessions for User in Group）] フィールドを空白にし、ティック アイコンをクリックし、[保存（Save）] をクリックします。デフォルトでは、両方の値が [無制限（Unlimited）] に設定されています。

ステップ 3 [保存（Save）] をクリックします。

カウンタの時間制限の設定

同時ユーザ セッションのタイムアウトを設定できます。

ステップ 1 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [最大セッション数（Max Sessions）] > [カウンタの時間制限（Counter Time Limit）] の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 無制限（Unlimited）：セッションのタイムアウトまたは時間制限を設定しない場合は、このチェックボックスにマークを付けます。
- [経過後にセッションを削除（Delete sessions after）]：日、時間、分の単位で同時セッションのタイムアウト値を入力できます。セッションが時間制限を超えると、Cisco ISE はカウンタからセッションを削除してセッション数を更新するため、新しいセッションが許可されます。ユーザは、セッションの時間制限を超えた場合、ログアウトされません。

ステップ 3 [保存（Save）] をクリックします。

[RADIUS ライブ ログ（RADIUS Live Logs）] ページでセッション カウントをリセットできます。[ID（Identity）]、[ID グループ（Identity Group）]、[サーバ（Server）] 列に表示される [アクション（Actions）] アイコンをクリックして、セッション カウントをリセットします。セッションをリセットすると、セッションはカウンタから削除されます（これにより、新しいセッションが許可されます）。ユーザのセッションがカウンタから削除されても、ユーザの接続は切断されません。

アカウント無効化ポリシー

Cisco ISE は、Cisco Secure ACS と同等の機能を実現するために、ユーザおよび管理者のアカウント無効化ポリシーを導入しています。ユーザまたは管理者の認証または問い合わせ時に、Cisco ISE は [管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] >[ユーザ認証設定（User Authentication Settings）] ページでグローバル アカウント無効化ポリシー設定を確認し、その設定に基づいて認証または結果を返します。

Cisco ISE は、次の 3 つのポリシーを確認します。

- 指定した日付（yyyy-mm-dd）を超えたらユーザ アカウントを無効にする（Disable user accounts that exceed a specified date (yyyy-mm-dd)）：設定された日付にユーザ アカウントを無効にします。ただし、[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] > [アカウント無効化ポリシー（Account Disable Policy）] で設定された個々のネットワーク アクセス ユーザのアカウント無効化ポリシー設定はグローバル設定よりも優先されます。
- アカウント作成時または最後の有効化から n 日後にユーザアカウントを無効にする（Disable user account after *n* days of account creation or last enable）：アカウントの作成またはアカウントが有効になった最後の日から指定した日数後にユーザ アカウントを無効にします。[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] > [ステータス（Status）] でユーザのステータスを確認できます。
- 非アクティブになってから n 日後にアカウントを無効にする（Disable accounts after *n* days of inactivity）：設定した連続日数、認証されなかった管理者およびユーザアカウントを無効化します。

Cisco Secure ACS から Cisco ISE に移行する際、Cisco Secure ACS ではネットワーク アクセス ユーザ用に指定したアカウント無効化ポリシーの設定は Cisco ISE に移行されます。

個別のユーザ アカウントの無効化

Cisco ISE では、アカウントの無効日が管理者ユーザによって指定された日付を超えた場合は、各個人ユーザのユーザ アカウントを無効にすることができます。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] の順に選択します。

ステップ 2 [追加（Add）] をクリックして新しいユーザを作成するか、既存のユーザの横のチェックボックスをオンにして [編集（Edit）] をクリックして既存のユーザの詳細を編集します。

ステップ 3 [日付を超えたらアカウントを無効化する（Disable account if the date exceeds）] チェックボックスをオンにして、日付を選択します。

このオプションによって、ユーザ レベルで設定した日付を超えたときに、ユーザアカウントをディセーブルにすることができます。必要に応じて、異なるユーザに異なる失効日を設定できます。このオプションは、個々のユーザのグローバル コンフィギュレーションを無効にします。日付には、現在のシステム日付または将来の日付を設定できます。

（注）　現在のシステム日付よりも古い日付は入力できません。

ステップ 4 [送信（Submit）] をクリックして、個々のユーザのアカウント無効化ポリシーを設定します。

グローバルにユーザ アカウントを無効にする

特定の日付、アカウントの作成日または最終アクセス日から数日後、およびアカウントが非アクティブになってから数日後に、ユーザ アカウントを無効にすることができます。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザ認証設定（User Authentication Settings）] > [アカウント無効化ポリシー（Account Disable Policy）] を選択します。

ステップ 2 次のいずれかの操作を実行します。

- [日付を超えるとアカウントを無効にする（Disable account if date exceeds）] チェック ボックスをオンにして、yyyy-mm-dd形式の適切な日付を選択します。このオプションによって、設定した日付の後、ユーザ アカウントを無効にすることができます。ユーザ レベルでの [日付を超えるとアカウントを無効にする（Disable account if date exceeds）] オプションは、このグローバル設定よりも優先されます。
- [アカウントの作成または最後に有効になってから n 日後にアカウントを無効にする（Disable account after n days of account creation or last enable）] チェック ボックスをオンにして、日数を入力します。このオプションは、アカウントの作成日または最終アクセス日が指定した日数を超えたときにユーザ アカウントを無効にします。管理者は、無効化されたユーザ アカウントを手動で有効にでき、有効にすると、日数の数はリセットされます。
- [非アクティブになってからn日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオンにして、日数を入力します。このオプションは、アカウントが指定した日数非アクティブのときにユーザ アカウントを無効にします。

ステップ 3 [送信（Submit）] をクリックし、グローバル アカウント無効化ポリシーを設定します。

内部 ID ソースと外部 ID ソース

アイデンティティ ソースは、ユーザ情報を保存するデータベースです。Cisco ISE は、アイデンティティ ソースのユーザ情報を使用して、認証時にユーザ クレデンシャルを検証します。ユーザ情報には、グループ情報と、そのユーザに関連付けられているその他の属性が含まれます。ID ソースに対してユーザ情報の追加、編集、および削除を行うことができます。

Cisco ISE では内部 ID ソースと外部 ID ソースがサポートされます。スポンサーとゲスト ユーザを認証するために両方のソースを使用できます。

内部 ID ソース

Cisco ISE には、ユーザ情報を保存できる内部ユーザ データベースがあります。内部ユーザ データベースのユーザは、内部ユーザと呼ばれます。Cisco ISE には、Cisco ISE に接続するすべてのデバイスおよびエンドポイントに関する情報を格納する内部エンドポイントデータベースもあります。

外部 ID ソース

Cisco ISE では、ユーザ情報を含む外部 ID ソースを設定することができます。Cisco ISE は外部 ID ソースに接続して、認証用のユーザ情報を取得します。外部 ID ソースには、Cisco ISE サーバおよび証明書認証プロファイルの証明書情報も含まれます。Cisco ISE は外部 ID ソースとの通信に認証プロトコルを使用します。次の表に、認証プロトコルおよびサポートされる外部 ID ソースを示します。

内部ユーザのポリシーを設定する際は、次の点に注意してください。

- 内部 ID ストアに対して内部ユーザを認証するための認証ポリシーを設定します。
- 次のオプションを選択して、内部ユーザ グループの許可ポリシーを設定します。

```
Identitygroup.Name EQUALS User Identity Groups: Group_Name
```

表 *55 :* 認証プロトコルとサポートされている外部 *ID* ソース

プロトコル（認証タイプ）	内部データベース	Active Directory	LDAP	RADIUS トークン サーバまたはRSA
EAP-GTC、PAP（プレーン テキスト パスワード）	○	○	○	○
MS-CHAP パスワード ハッシュ： MSCHAPv1/v2 EAP-MSCHAPv2（PEAP、EAP-FAST、またはEAP-TTLS の内部メソッドとして） LEAP	○	○	否	×
EAP-MD5 CHAP	○	否	×	×

プロトコル（認証タイプ）	内部データベース	Active Directory	LDAP	RADIUS トークンサーバまたはRSA
EAP-TLS PEAP-TLS （証明書取得） （注） TLS 認証（EAP-TLS と PEAP-TLS）に ID ソースは必須ではありませんが、許可ポリシー条件のために任意で追加できます。	×	○	○	否

クレデンシャルを保存する方法は、外部データ ソースの接続タイプと使用される機能に応じて異なります。

- Active Directory ドメイン（パッシブ ID 用ではない）に参加する場合、参加に使用されるクレデンシャルは保存されません。Cisco ISE は、AD コンピュータ アカウントが存在しない場合はそのアカウントを作成し、そのアカウントを使用してユーザを認証します。
- LDAP およびパッシブ ID の場合、外部データ ソースへの接続に使用されるクレデンシャルは、ユーザの認証にも使用されます。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバなどの外部 ID ソースに接続して、認証/許可のユーザ情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザ ID を受信して共有できるようにするパッシブ ID サービスを使用するには、を参照してくださいその他の パッシブ ID サービス プロバイダー （647 ページ）。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。
- Active Directory：外部 ID ソースである Active Directory に接続する場合。外部 ID ソースとしての Active Directory （587 ページ）を参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、LDAP （696 ページ）を参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバを追加する場合。詳細については、RADIUS トークン ID ソース （722 ページ）を参照してください。
- RSA SecurID：RSA SecurID サーバを追加する場合。詳細については、RSA ID ソース （730 ページ）を参照してください。
- SAML IDプロバイダー（SAML Id Providers）：Oracle Access Manager などの ID プロバイダー（IdP）を追加する場合。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダ （738 ページ）を参照してください。
- **ソーシャル ログイン**：Facebook などのソーシャル ログインを外部 ID ソースとして追加する場合。アカウント登録ゲストのソーシャル ログイン （389 ページ）を参照してください。

外部 ID ストア パスワードに対する内部ユーザの認証

Cisco ISE では、外部 ID ストア パスワードに対して内部ユーザを認証できます。Cisco ISE では、[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] ページから、内部ユーザのパスワード ID ストアを選択するオプションが提供されます。管理者は、Cisco ISE の外部 ID ソースのリストから ID ストアを選択することができ、[ユーザ（Users）] ページでユーザを追加するか、または編集します。内部ユーザのデフォルトのパスワード ID ストアは内部 ID ストアです。Cisco Secure ACS ユーザは、Cisco Secure ACS から Cisco ISE への移行中および移行後、同じパスワード ID ストアを維持します。

Cisco ISE はパスワード タイプに対し次の外部 ID ストアをサポートします。

- Active Directory
- LDAP
- ODBC
- RADIUS トークン サーバ
- RSA SecurID サーバ

証明書認証プロファイル

プロファイルごとに、プリンシパルユーザ名として使用する証明書フィールドと、証明書のバイナリ比較を行うかどうかを指定する必要があります。

証明書認証プロファイルの追加

Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）証明書ベースの認証方式を使用する場合は、証明書認証プロファイルを作成する必要があります。従来のユーザ名とパスワードの方法で認証する代わりに、Cisco ISE はクライアントから受信した証明書をサーバ内の証明書と比較してユーザの信頼性を確認します。

始める前に

スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [証明書認証プロファイル（Certificate Authentication Profile）] > [追加（Add）]** を選択します。

ステップ 2 証明書認証プロファイルの名前と説明（任意）を入力します。

ステップ 3 ドロップダウン リストから ID ストアを選択します。

基本証明書のチェックはID ソースを必要としません。証明書にバイナリ比較チェックが必要な場合は、ID ソースを選択する必要があります。ID ソースとして Active Directory を選択した場合は、サブジェクト名、一般名、およびサブジェクト代替名（すべての値）を使用してユーザを検索できます。

ステップ 4 [証明書属性（Certificate Attribute）] または [証明書の任意のサブジェクトまたは代替名属性（Any Subject or Alternative Name Attributes in the Certificate）] から ID の使用を選択します。これは、ログで検索のために使用されます。

[証明書の任意のサブジェクトまたは代替名属性（Any Subject or Alternative Name Attributes in the Certificate）] を選択すると、Active Directory UPN がログ用のユーザ名として使用され、証明書のすべてのサブジェクト名および代替名がユーザの検索に試行されます。このオプションは、ID ソースとして Active Directory を選択した場合にのみ使用できます。

ステップ 5 **クライアント証明書を ID ストアの証明書と照合する**場合に選択します。この場合、ID ソース（LDAP または Active Directory）を選択する必要があります。[Active Directory] を選択した場合は、ID のあいまいさを解決するためにのみ証明書を照合することを選択できます。

- [なし（Never）]：このオプションは、バイナリ比較を実行しません。
- [ID のあいまいさを解決する目的のみ（Only to resolve identity ambiguity）]：このオプションは、あいまいさが見つかった場合にだけ、クライアント証明書と Active Directory のアカウントの証明書とのバイナリ比較を実行します。たとえば、複数の Active Directory アカウントが証明書の識別名に一致することがあります。
- [常にバイナリ比較を実行する（Always perform binary comparison）]：このオプションは、クライアント証明書と ID ストア（Active Directory または LDAP）内のアカウントの証明書とのバイナリ比較を常に実行します。

ステップ 6 [送信（Submit）] をクリックして、証明書認証プロファイルを追加するか、変更を保存します。

外部 ID ソースとしての Active Directory

Cisco ISE は、ユーザ、マシン、グループ、属性などのリソースにアクセスするために、Microsoft Active Directory を外部 ID ソースとして使用します。Active Directory でのユーザとマシンの認証では、Active Directory にリストされているユーザとデバイスに対してのみネットワーク アクセスを許可します。

ISE コミュニティ リソース

ISE Administrative Portal Access with AD Credentials Configuration Example

Active Directory でサポートされる認証プロトコルおよび機能

Active Directory は、一部のプロトコルを使用したユーザとマシンの認証、Active Directory ユーザ パスワードの変更などの機能をサポートしています。次の表に、Active Directory でサポートされる認証プロトコルおよびそれぞれの機能を示します。

表 *56 : Active Directory* でサポートされる認証プロトコル

認証プロトコル	機能
EAP-FAST およびパスワードベースの Protected Extensible Authentication Protocol（PEAP）	MS-CHAPv2 および EAP-GTC の内部方式で EAP-FAST と PEAP を使用するパスワード変更機能を備えたユーザとマシンの認証
Password Authentication Protocol（PAP）	ユーザおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol Version 1（MS-CHAPv1）	ユーザおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）	ユーザおよびマシン認証
Extensible Authentication Protocol-Generic Token Card（EAP-GTC）	ユーザおよびマシン認証
Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）	• ユーザおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling-Transport Layer Security（EAP-FAST-TLS）	• ユーザおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較

認証プロトコル	機能
Protected Extensible Authentication Protocol-Transport Layer Security（PEAP-TLS）	• ユーザおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Lightweight Extensible Authentication Protocol（LEAP）	ユーザ認証

許可ポリシーで使用する Active Directory 属性およびグループの取得

Cisco ISE は、許可ポリシー ルールで使用するために Active Directory からユーザまたはマシンの属性およびグループを取得します。これらの属性は Cisco ISE ポリシーで使用され、ユーザまたはマシンの承認レベルを決定します。Cisco ISE は、認証が成功した後にユーザおよびマシンの Active Directory 属性を取得します。認証とは別に、許可のために属性を取得することもできます。

Cisco ISE は、外部 ID ストア内のグループを使用してユーザまたはコンピュータに権限を割り当てることがあります（たとえば、ユーザをスポンサー グループにマップします）。Active Directory のグループ メンバーシップの次の制限事項に注意してください。

- ポリシー ルールの条件は、次のいずれかを参照します。ユーザまたはコンピュータのプライマリ グループ、ユーザまたはコンピュータが直接メンバーであるグループ、または間接的（ネストされた）グループ。
- ユーザまたはコンピュータのアカウント ドメイン外のドメイン ローカル グループはサポートされません。

（注） Active Directory 属性の値 msRadiusFramedIPAddress を IP アドレスとして使用できます。この IP アドレスは、許可プロファイルのネットワーク アクセス サーバ（NAS）に送信できます。msRADIUSFramedIPAddress 属性は IPv4 アドレスだけをサポートします。ユーザ認証では、ユーザに対し取得された msRadiusFramedIPAddress 属性値が IP アドレス形式に変換されます。

属性およびグループは、参加ポイントごとに取得され、管理されます。これらは許可ポリシーで使用されます（まず参加ポイントを選択し、次に属性を選択します）。許可のスコープごとに属性またはグループを定義することはできませんが、認証ポリシーでスコープを使用できます。認証ポリシーでスコープを使用する場合、ユーザは 1 つの参加ポイントで認証されますが、ユーザのアカウント ドメインへの信頼できるパスがある別の参加ポイント経由で属性またはグループを取得することができます。認証ドメインを使用して、1 つの範囲内にある 2 つの参加ポイントで認証ドメインが重複しないようにすることができます。

（注） マルチ参加ポイント設定の許可プロセス時に、Cisco ISE は、特定のユーザが見つかるまで、認証ポリシーに記載されている順序で参加ポイントを検索します。ユーザが見つかると、参加ポイント内のユーザに割り当てられた属性とグループが、認証ポリシーを評価するために使用されます。

（注） 使用可能な Active Directory グループの最大数については、Microsoft の制限を参照してください。http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

ルールに、/、!、@、\、#、$、%、^、&、*、(、)、_、+、または~のような特殊文字を使用した Active Directory グループ名が含まれる場合、許可ポリシーは失敗します。

明示的な UPN の使用

ユーザ情報と Active Directory のユーザ プリンシパル名（UPN）属性を照合する場合の不確実性を減らすため、明示的な UPN を使用するように Active Directory を設定する必要があります。2 人のユーザが同じ値 *sAMAccountName* を使用した場合、暗示的な UPN を使用すると、あいまいな結果が生成されます。

Active Directory で明示的な UPN を設定するには、[高度な調整（Advanced Tuning）] ページを開いて、属性 *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* を 1 に設定します。

ブール属性のサポート

Cisco ISE は、Active Directory および LDAP ID ストアからのブール属性の取得をサポートしています。

Active Directory または LDAP のディレクトリ属性を設定する際に、ブール属性を設定できます。これらの属性は、Active Directory または LDAP による認証時に取得されます。

ブール属性は、ポリシー ルール条件の設定に使用できます。

ブール属性値は、文字列型として Active Directory または LDAP サーバから取得されます。Cisco ISE は、次のブール属性値をサポートしています。

ブール属性	サポートされる値
[はい（True）]	t、T、true、TRUE、True、1
いいえ（False）	f、F、false、FALSE、False、0

（注） 属性置換はブール属性ではサポートされません。

文字列型としてブール属性（たとえば、msTSAllowLogon）を設定すると、Active Directory または LDAP サーバの属性のブール値は Cisco ISE の文字列属性に設定されます。属性タイプをブール型に変更したり、ブール型として属性を手動で追加できます。

証明書ベース認証の Active Directory 証明書の取得

Cisco ISE では、EAP-TLS プロトコルを使用するユーザまたはマシン認証のための証明書取得がサポートされています。Active Directory 上のユーザまたはマシン レコードには、バイナリ データ型の証明書属性が含まれています。この証明書属性に 1 つ以上の証明書を含めることができます。Cisco ISE ではこの属性は userCertificate として識別され、この属性に対して他の名前を設定することはできません。Cisco ISE はこの証明書を取得し、バイナリ比較の実行に使用します。

証明書認証プロファイルは、証明書の取得に使用する Active Directory のユーザを検索するためにユーザ名を取得するフィールド（たとえば、サブジェクト代替名（SAN）または一般名）を決定します。Cisco ISE は、証明書を取得した後、この証明書とクライアント証明書とのバイナリ比較を実行します。複数の証明書が受信された場合、Cisco ISE は、いずれかが一致するかどうかをチェックするために証明書を比較します。一致が見つかった場合、ユーザまたはマシン認証に合格します。

Active Directory ユーザ認証プロセス フロー

ユーザの認証または問い合わせ時に、Cisco ISE は次のことをチェックします。

- MS-CHAP および PAP 認証では、ユーザが無効かどうか、ロック アウトされているかどうか、期限切れかどうか、またはログイン時間外かどうかを確認します。これらの条件のいくつかが true の場合、認証が失敗します。
- EAP-TLS 認証では、ユーザが無効かどうか、ロック アウトされているかどうかを確認します。これらの条件のいくつかが一致する場合、認証が失敗します。

Active Directory マルチドメイン フォレストのサポート

Cisco ISE では、マルチドメイン フォレストの Active Directory がサポートされます。各フォレスト内で、Cisco ISE は単一のドメインに接続しますが、Cisco ISE が接続されているドメインと他のドメイン間に信頼関係が確立されている場合は、Active Directory フォレストの他のドメインからリソースにアクセスできます。

Active Directory サービスをサポートする Windows サーバ オペレーティング システムのリストについては、『Release Notes for Cisco Identity Services Engine』を参照してください。

（注） Cisco ISE は、ネットワーク アドレス トランスレータの背後にあり、ネットワーク アドレス変換（NAT）アドレスを持つ Microsoft Active Directory サーバをサポートしません。

Active Directory と Cisco ISE の統合の前提条件

ここでは、Cisco ISE と統合する Active Directory を設定するために必要な手動での作業手順を説明します。ただしほとんどの場合、Cisco ISE が Active Directory を自動的に設定するようにできます。次に、Cisco ISE と Active Directory を統合するための前提条件を示します。

- AD ドメイン設定の変更に必要な Active Directory ドメイン管理者クレデンシャルがあることを確認します。
- ISE でのスーパー管理者またはシステム管理者の権限があることを確認します。
- Cisco ISE サーバと Active Directory 間の時間を同期するために Network Time Protocol（NTP）サーバ設定を使用します。Cisco ISE CLI で NTP を設定できます。
- Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。特定の参加ポイントから他のドメインを照会する場合は、参加ポイントと、アクセスする必要があるユーザ情報およびマシン情報があるその他のドメインの間に信頼関係が確立されていることを確認します。信頼関係が確立されていない場合は、信頼できないドメインへの別の参加ポイントを作成する必要があります。信頼関係の確立の詳細については、Microsoft Active Directory のドキュメントを参照してください。
- Cisco ISE の参加先ドメインでは、少なくとも 1 つのグローバル カタログ サーバが動作し、Cisco ISE からアクセス可能である必要があります。

さまざまな操作の実行に必要な Active Directory アカウント権限

参加操作	脱退処理	Cisco ISE マシン アカウント
参加操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシン アカウントがあるかどうかの確認） • ドメインに Cisco ISE マシン アカウントを作成する権限（マシン アカウントが存在しない場合） • 新しいマシン アカウントに属性を設定する権限（Cisco ISE マシン アカウント パスワード、SPN、dnsHostname など） 参加操作を実行するために、ドメイン管理者である必要はありません。	脱退操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシン アカウントがあるかどうかの確認） • ドメインから Cisco ISE マシン アカウントを削除する権限 強制脱退（パスワードなしの脱退）を実行する場合、ドメインからマシン アカウントは削除されません。	Active Directory 接続と通信する Cisco ISE マシン アカウントには、次の権限が必要です。 • パスワードを変更する。 • 認証されるユーザおよびマシンに対応するユーザおよびマシン オブジェクトを読み取る権限 • 情報を取得するために Active Directory をクエリする権限（信頼ドメイン、代替の UPN サフィックスなど） • tokenGroups 属性を読み取る権限 Active Directory でマシン アカウントを事前に作成できます。SAM の名前が Cisco ISE アプライアンスのホスト名と一致する場合は、参加操作中に検索して再利用します。 複数の参加操作が実行される場合、参加ごとに複数のマシン アカウントが Cisco ISE 内で保持されます。

（注） 参加操作または脱退操作に使用するクレデンシャルは Cisco ISE に保存されません。新規に作成された Cisco ISE マシン アカウントのクレデンシャルのみが保存されます。これによって、エンドポイント プローブが実行できるようになります。

通信用に開放するネットワーク ポート

プロトコル	ポート（リモート ローカル）	ターゲット	認証	注記
DNS（TCP/UDP）	49152 以上の乱数	DNS サーバ/AD ドメイン コントローラ	いいえ	—
MSRPC	445	ドメイン コントローラ	あり	—
Kerberos（TCP/UDP）	88	ドメイン コントローラ	あり（Kerberos）	MS AD/KDC
LDAP（TCP/UDP）	389	ドメイン コントローラ	あり	—
LDAP（GC）	3268	グローバル カタログ サーバ	あり	—
NTP	123	NTP サーバ/ドメイン コントローラ	いいえ	—
IPC	80	展開内の他の ISE ノード	あり（RBAC クレデンシャルを使用）	—

DNS サーバ

DNS サーバを設定する場合は、次の処理を実行します。

- Cisco ISE に設定されている DNS サーバで、使用するドメインのすべての正引きおよび逆引き DNS クエリを解決できるようにする必要があります。
- DNS再帰によって遅延が発生してパフォーマンスが重大な悪影響を受ける可能性があるので、権威 DNS サーバで Active Directory レコードを解決することをお勧めします。
- すべての DNS サーバで、追加サイト情報の有無に関係なく、DC、GC、および KDC の SRV クエリに回答できるようにする必要があります。
- パフォーマンスを向上させるために、SRV 応答にサーバ IP アドレスを追加することを推奨します。
- パブリック インターネットでクエリを実行する DNS サーバを使用しないでください。不明な名前を解決する必要がある場合に、ネットワークの情報が漏洩する可能性があります。

外部 ID ソースとしての Active Directory の設定

Easy Connect や PassiveID ワークセンターなどの機能を設定する際に、Active Directory を外部 ID ソースとして設定します。これらの機能の詳細については、Easy Connect （632 ページ）と PassiveID ワークセンター （637 ページ）を参照してください。

外部 ID ソースとして Active Directory を設定する前に、次のことを確認します。

- Microsoft Active Directory サーバがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないこと。
- 参加操作用の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更（Change Password on Next Login）] を使用して設定されていないこと。
- ISE のスーパー管理者またはシステム管理者の権限があること。

（注） Cisco ISE が Active Directory に接続されているときに操作に関する問題がある場合は、**[操作（Operations）] > [レポート（Reports）]** で AD コネクタ操作レポートを参照してください。

外部 ID ソースとして Active Directory を設定するには、次のタスクを実行する必要があります。

1. Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （594 ページ）
2. 認証ドメインの設定 （602 ページ）
3. Active Directory ユーザ グループの設定 （603 ページ）
4. Active Directory ユーザとマシンの属性の設定 （604 ページ）
5. （任意） パスワード変更、マシン認証、およびマシン アクセス制限の設定の変更 （605 ページ）

Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加

始める前に

Cisco ISE ノードが、NTP サーバ、DNS サーバ、ドメイン コントローラ、グローバル カタログ サーバが配置されているネットワークと通信できることを確認します。ドメイン診断ツールを実行して、これらのパラメータをチェックできます。

Active Directory と、パッシブ ID ワーク センターのエージェント、syslog、SPAN、およびエンドポイントの各プローブを使用するには、参加ポイントを作成する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [追加（Add）] をクリックして、Active Directory 参加ポイント名設定のドメイン名と ID ストア名を入力します。

ステップ 3 [送信（Submit）] をクリックします。

新しく作成された参加ポイントをドメインに参加させるかどうかを確認するポップアップ ウィンドウが表示されます。すぐに参加させる場合は [はい（Yes）] をクリックします。

[いいえ（No）] をクリックした場合、設定を保存すると、Active Directory ドメインの設定が（プライマリおよびセカンダリのポリシー サービス ノードに）グローバルに保存されますが、いずれの Cisco ISE ノードもまだドメインに参加しません。

ステップ 4 作成した新しい Active Directory 参加ポイントの横にあるチェックボックスをオンにして [編集（Edit）] をクリックするか、または左側のナビゲーション ペインから新しい Active Directory 参加ポイントをクリックします。展開の参加/脱退テーブルに、すべての Cisco ISE ノード、ノードのロール、およびそのステータスが表示されます。

ステップ 5 参加ポイントがステップ 3 の間にドメインに参加しなかった場合は、関連する Cisco ISE ノードの横にあるチェックボックスをオンにし、[参加（Join）] をクリックして Active Directory ドメインに Cisco ISE ノードを参加させます。

設定を保存した場合も、これを明示的に実行する必要があります。1 回の操作で複数の Cisco ISE ノードをドメインに参加させるには、使用するアカウントのユーザ名とパスワードがすべての参加操作で同じである必要があります。各 Cisco ISE ノードを追加するために異なるユーザ名とパスワードが必要な場合は、Cisco ISE ノードごとに参加操作を個別に実行する必要があります。

ステップ 6 表示される [ドメインへの参加（Join Domain）] ダイアログボックスで Active Directory のユーザ名とパスワードを入力します。

[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザ名とパスワードが保存され、モニタ対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。

参加操作に使用するユーザは、ドメイン自体に存在する必要があります。ユーザが異なるドメインまたはサブドメインに存在する場合、ユーザ名は jdoe@acme.com のように、UPN 表記で表記する必要があります。

ステップ 7 （任意） [組織ユニットの指定（Specify Organizational Unit）] チェックボックスをオンにします。

このチェックボックスは、Cisco ISE ノードのマシン アカウントを CN=Computers,DC=someDomain,DC=someTLD 以外の特定の組織ユニットに配置する場合に、オンにする必要があります。Cisco ISE は、指定された組織ユニットの下にマシン アカウントを作成するか、またはマシン アカウントがすでにある場合は、この場所に移動します。組織ユニットが指定されない場合、Cisco ISE はデフォルトの場所を使用します。値は完全識別名（DN）形式で指定する必要があります。構文は、Microsoft のガイドラインに準拠する必要があります。特別な予約文字（/'+,;=<> など）、改行、スペース、およびキャリッジ リターンは、バックスラッシュ（\）によってエスケープする必要があります。たとえば、OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ や Workstations,DC=someDomain,DC=someTLD のようにします。マシン アカウントがすでに作成されている場合、このチェックボックスをオンにする必要はありません。Active Directory ドメインに参加したマシン アカウントのロケーションを後で変更することもできます。

ステップ 8 [OK] をクリックします。

Active Directory ドメインに参加する複数のノードを選択できます。

参加操作に失敗した場合、失敗メッセージが表示されます。各ノードの失敗メッセージをクリックして、そのノードの詳細なログを表示します。

（注） 参加が完了すると、Cisco ISE によりその AD グループと対応する SIDS が更新されます。Cisco ISE は自動的に SID の更新プロセスを開始します。このプロセスを完了できるようにする必要があります。

（注） DNS SRV レコードが欠落している（参加しようとしているドメインに対し、ドメイン コントローラが SRV レコードをアドバタイズしない）場合は、Active Directory ドメインに Cisco ISE を参加させることができない可能性があります。トラブルシューティング情報については、次の Microsoft Active Directory のマニュアルを参照してください。

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

（注） ISE には最大 200 のドメイン コントローラのみを追加できます。制限を超えると、「エラー発生 <DC FQDN> - DCの数が最大許容数である 200 を超えています（Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200）」というエラーが表示されます。

次のタスク

Active Directory ユーザ グループの設定 （603 ページ）

認証ドメインを設定します。

ドメイン コントローラの追加

ステップ 1 **[ワーク センター（Work Centers）] > [PassiveID] > [プロバイダー（Providers ）]** を選択し、左側のパネルから [Active Directory] を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 （注） パッシブ ID サービスの新しいドメイン コントローラ（DC）を追加するには、その DC のログイン クレデンシャルが必要です。

[PassiveID] タブに移動し、[DC の追加（Add DCs）] をクリックします。

ステップ 4 モニタ対象として参加ポイントに追加するドメイン コントローラの隣にあるチェックボックスをオンにし、[OK] をクリックします。
ドメイン コントローラが [PassiveID] タブの [ドメイン コントローラ（Domain Controllers）] リストに表示されます。

ステップ 5 ドメイン コントローラを設定します。

a) ドメイン コントローラをオンにし、[編集（Edit）] をクリックします。[アイテムの編集（Edit Item）] 画面が表示されます。
b) 必要に応じて、各種ドメイン コントローラ フィールドを編集します。詳細については、Active Directory の設定 （643 ページ）を参照してください。
c) WMI プロトコルを選択した場合は、[設定（Configure）] をクリックして WMI を自動的に設定するか、または [テスト（Test）] をクリックして接続をテストします。WMI の自動設定の詳細については、パッシブ ID 用の WMI の設定 （597 ページ）を参照してください。

DC フェールオーバー メカニズムは DC 優先順位リストに基づいて管理されます。このリストは、フェールオーバーの発生時に DC が選択される順序を決定します。ある DC がオフラインであるか、何らかのエラーのため到達不能な場合には、優先順位リストにおける優先順位が下がります。DC がオンラインに戻ると、優先順位リストにおけるその優先順位が適宜調整されます（上がります）。

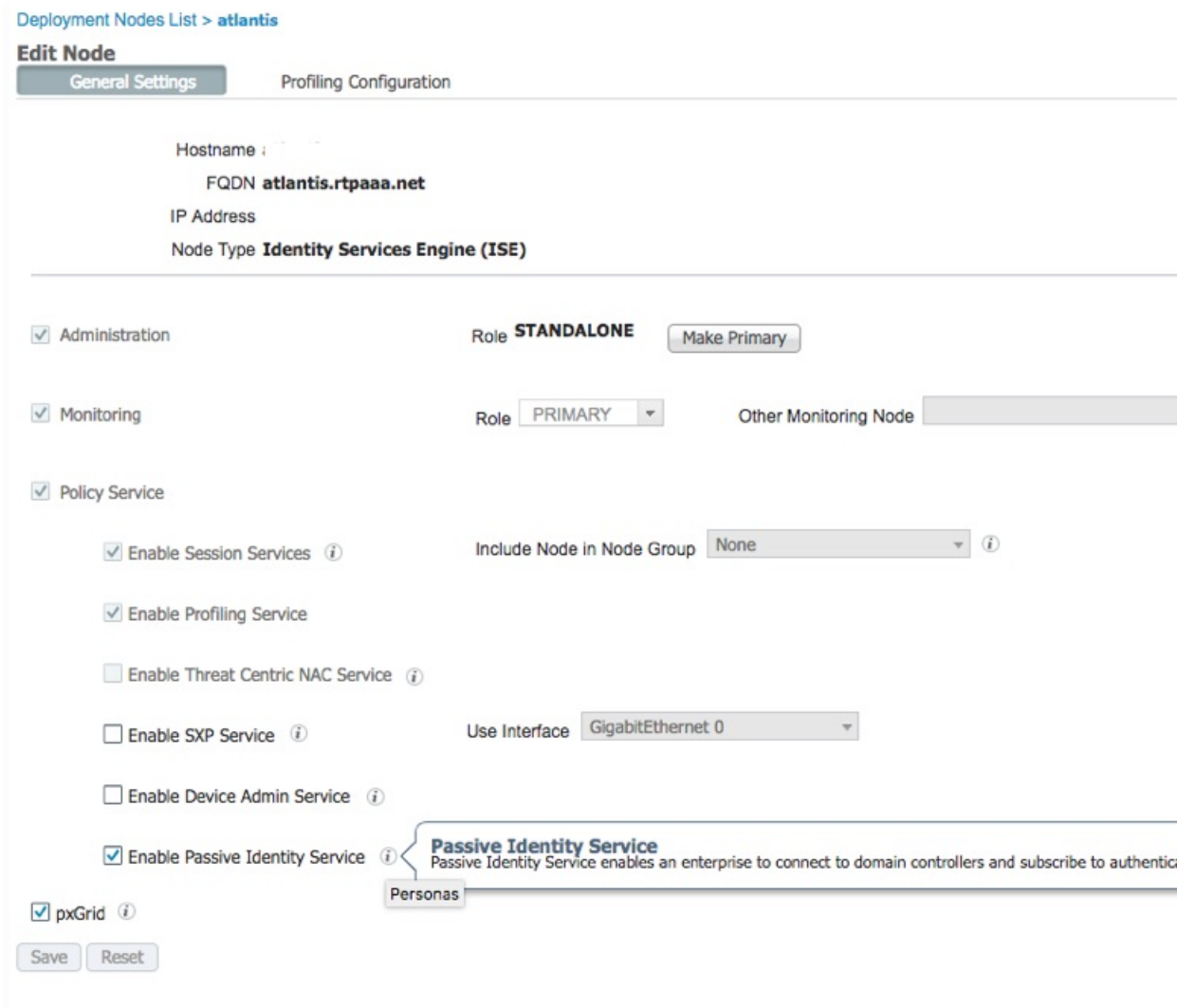
（注） Cisco ISE は、認証フローの読み取り専用ドメイン コントローラをサポートしていません。

パッシブ ID 用の WMI の設定

始める前に

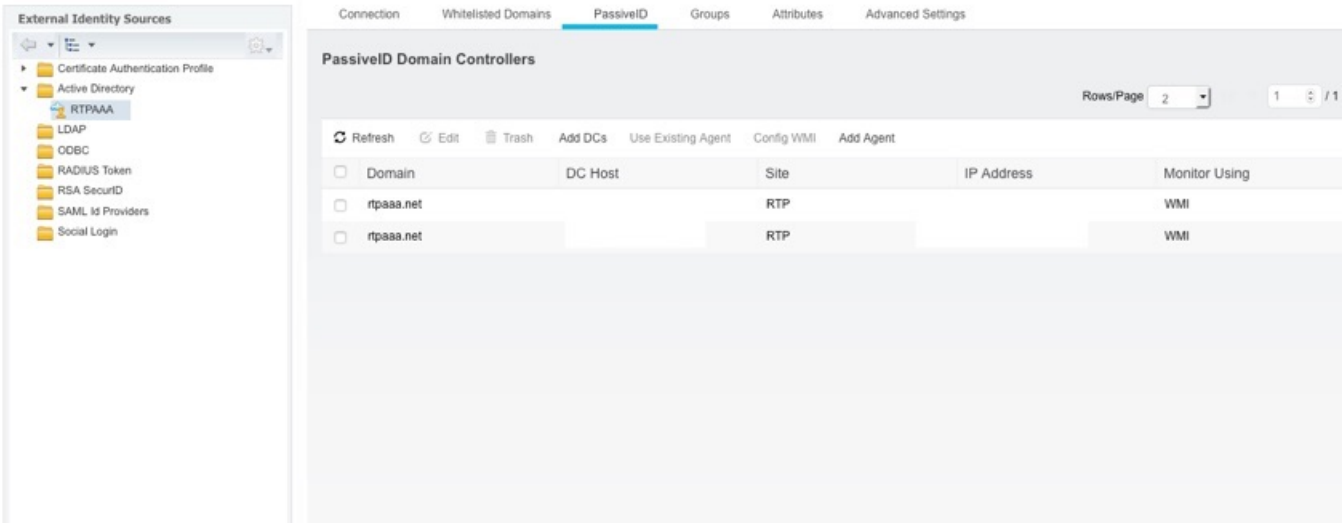
AD ドメイン設定の変更に必要な Active Directory ドメイン管理者クレデンシャルがあることを確認します。[管理（Administration）] > [システム（System）] > [展開（Deployment）] で、このノードのパッシブ ID が有効になっていることを確認します。

図 *17 :*



ステップ 1 **[管理（Administration）] > [IDの管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

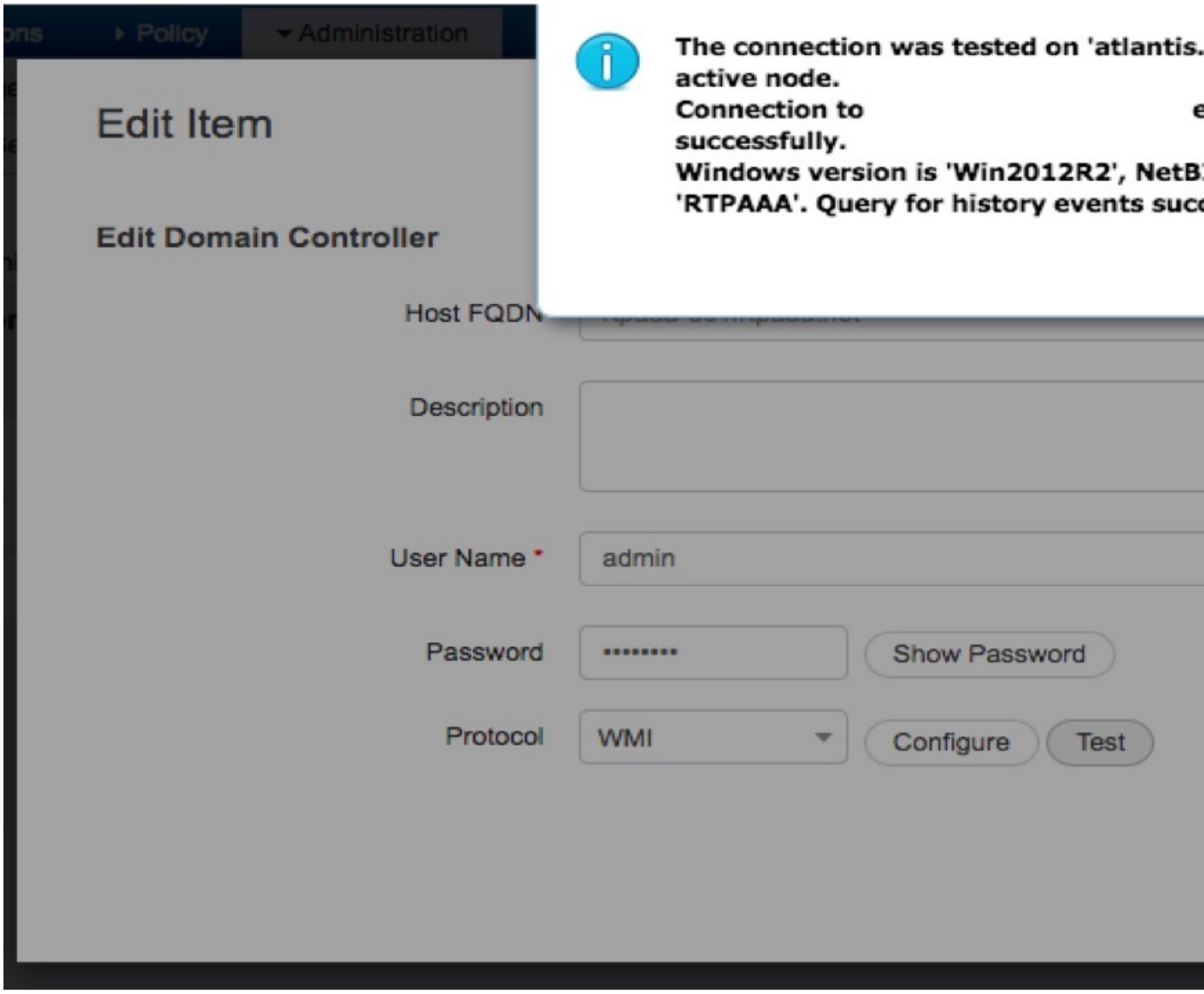
図 *18 :*



ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。詳細については、表 59 : [Active Directory 参加/脱退（Active Directory Join/Leave）] テーブル （644 ページ）を参照してください。

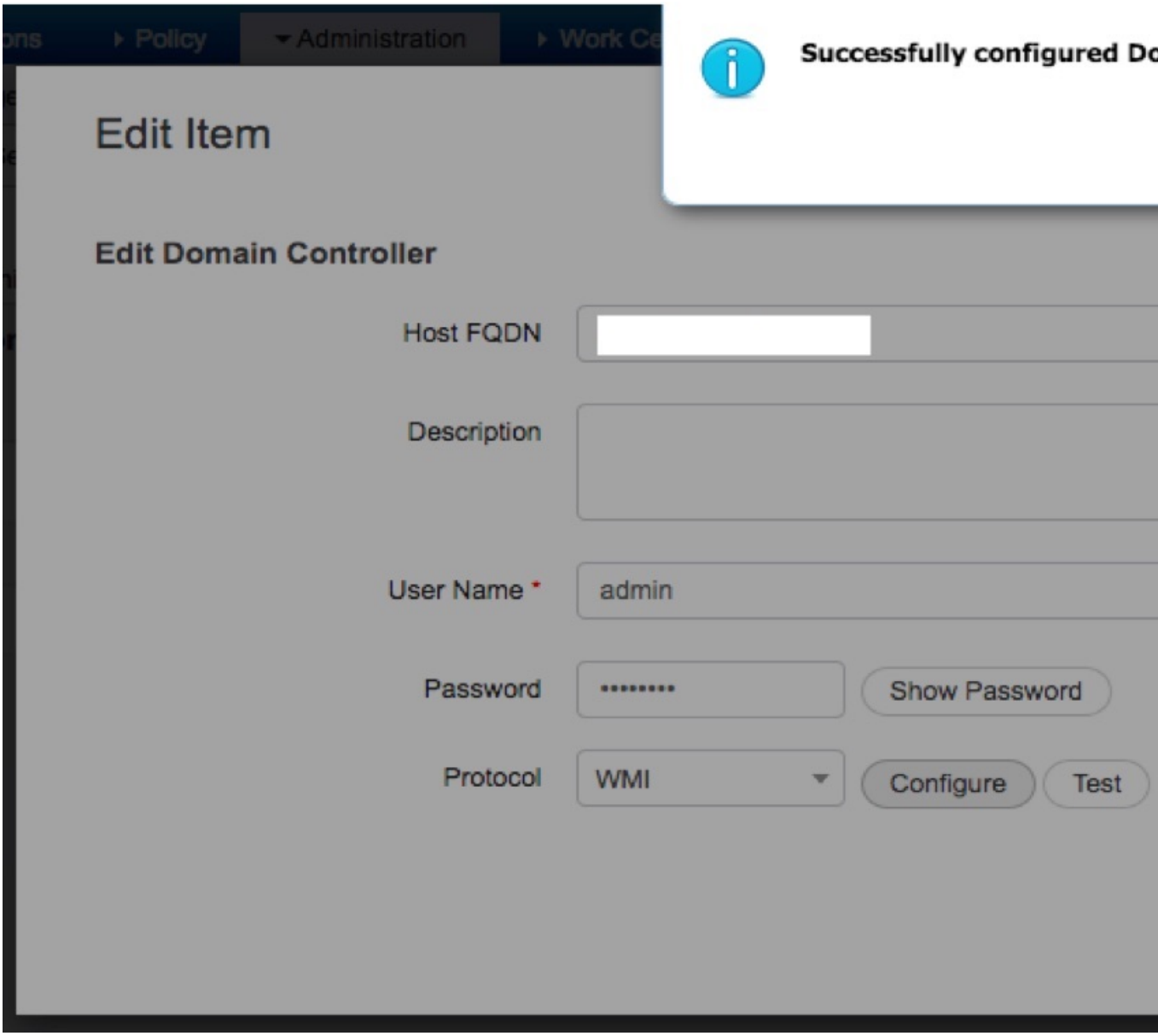
ステップ 3 [パッシブ ID（Passive ID）] タブに移動し、該当するドメイン コントローラの隣にあるチェックボックスをオンにし、[WMI の設定（Config WMI）] をクリックして、選択したドメイン コントローラが ISE により自動的に設定されるようにします。

図 *19 :*



Active Directory とドメイン コントローラを手動で設定する場合、または設定の問題のトラブルシューティングを行う場合は、Active Directory と Cisco ISE の統合の前提条件 （591 ページ）を参照してください。

図 *20 :*



Active Directory ドメインの脱退

この Active Directory ドメインまたはこの参加ポイントからユーザとマシンを認証する必要がない場合は、Active Directory ドメインを脱退できます。

コマンドライン インターフェイスから Cisco ISE アプリケーション設定をリセットする場合、またはバックアップやアップグレードの後に設定を復元する場合、脱退操作が実行され、Cisco ISE ノードがすでに参加している場合は、Active Directory ドメインから切断されます。ただし、

Cisco ISE ノードのアカウントは、Active Directory ドメインから削除されません。脱退操作では Active Directory ドメインからノード アカウントも削除されるため、脱退操作は管理者ポータルから Active Directory クレデンシャルを使用して実行することを推奨します。これは、Cisco ISE ホスト名を変更する場合にも推奨されます。

始める前に

Active Directory ドメインを脱退したが、認証の ID ソースとして（直接または ID ソース順序の一部として）Active Directory を使用している場合、認証が失敗する可能性があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 Cisco ISE ノードの隣にあるチェックボックスをオンにして [脱退（Leave）] をクリックします。

ステップ 4 Active Directory のユーザ名とパスワードを入力し、[OK] をクリックしてドメインを脱退し、Cisco ISE データベースからマシン アカウントを削除します。

Active Directory クレデンシャルを入力すると、Cisco ISE ノードは Active Directory ドメインを脱退し、Active Directory データベースから Cisco ISE マシン アカウントが削除されます。

（注） Active Directory データベースから Cisco ISE マシン アカウントを削除するには、ここに入力する Active Directory クレデンシャルに、ドメインからマシン アカウントを削除する権限がなければなりません。

ステップ 5 Active Directory クレデンシャルがない場合は、[使用可能なクレデンシャルなし（No Credentials Available）] チェックボックスをオンにして、[OK] をクリックします。

[クレデンシャルなしでドメインを脱退（Leave domain without credentials）] チェックボックスをオンにすると、プライマリ Cisco ISE ノードが Active Directory ドメインから脱退します。参加時に Active Directory で作成されたマシン アカウントは、Active Directory 管理者が手動で削除する必要があります。

認証ドメインの設定

Cisco ISE が参加しているドメインは、信頼関係を持つ他のドメインに対して可視性があります。デフォルトでは、Cisco ISE はこれらすべての信頼ドメインに対する認証を許可するように設定されます。認証ドメインのサブセットに対して、Active Directory 展開との相互作用を制限できます。ドメイン認証を設定することにより、接続ポイントごとに特定のドメインを選択して、選択されたドメインに対してのみ認証が実行されるようにできます。認証ドメインでは、接続ポイントから信頼されたすべてのドメインではなく、選択されたドメインのユーザのみを認証するように Cisco ISE に指示するため、セキュリティが向上します。また、認証ドメインでは検索範囲（着信したユーザ名または ID に一致するアカウントの検索）が制限されるため、認証要求処理のパフォーマンスと遅延が改善されます。このことは、着信したユーザ名

または ID にドメイン マークアップ（プレフィクスまたはサフィックス）が含まれていない場合に特に重要です。これらの理由から、認証ドメインを設定することをベストプラクティスとして強く推奨します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 **Active Directory** の参加ポイントをクリックします。

ステップ 3 [認証ドメイン（Authentication Domains）] タブをクリックします。

表に、信頼ドメインのリストが表示されます。デフォルトでは、Cisco ISE はすべての信頼ドメインに対する認証を許可します。

ステップ 4 指定したドメインのみを許可するには、[認証にすべての Active Directory ドメインを使用する（Use all Active Directory domains for authentication）] チェックボックスをオフにします。

ステップ 5 認証を許可するドメインの隣にあるチェックボックスをオンにし、[選択対象の有効化（Enable Selected）] をクリックします。[認証（Authenticate）] カラムで、このドメインのステータスが [はい（Yes）] に変わります。

また、選択したドメインを無効にすることもできます。

ステップ 6 [使用できないドメインを表示（Show Unusable Domains）] をクリックして、使用できないドメインのリストを表示します。使用できないドメインは、単方向の信頼や選択的な認証などの理由により、Cisco ISE が認証に使用できないドメインです。

次のタスク

Active Directory ユーザ グループを設定します。

Active Directory ユーザ グループの設定

Active Directory ユーザ グループを許可ポリシーで使用できるように設定する必要があります。内部的には、Cisco ISE はグループ名のあいまいさの問題を解決し、グループ マッピングを向上させるためにセキュリティ ID（SID）を使用します。SID により、グループ割り当てが正確に一致します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [グループ（Groups）] タブをクリックします。

ステップ 3 次のいずれかを実行します。

a) **[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）]** を選択して、既存のグループを選択します。

b) **[追加（Add）]** > **[グループの追加（Add Group）]** を選択して、グループを手動で追加します。グループ名と SID の両方を指定するか、またはグループ名のみを指定し、[SID を取得（Fetch SID）] を押します。

ユーザ インターフェイス ログインのグループ名に二重引用符（"）を使用しないでください。

ステップ 4 グループを手動で選択する場合は、フィルタを使用してグループを検索できます。たとえば、**admin*** をフィルタ基準として入力し、[グループの取得（Retrieve Groups）] をクリックすると、admin で始まるユーザ グループが表示されます。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。一度に取得できるのは 500 グループのみです。

ステップ 5 許可ポリシーで使用可能にするグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 グループを手動で追加する場合は、新しいグループの名前と SID を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

（注） グループを削除し、そのグループと同じ名前で新しいグループを作成する場合は、[SID 値の更新（Update SID Values）] をクリックして、新しく作成したグループに新しい SID を割り当てる必要があります。アップグレードすると、最初の参加の後に SID が自動的に更新されます。

次のタスク

Active Directory のユーザ属性を設定します。

Active Directory ユーザとマシンの属性の設定

許可ポリシーの条件で使用できるように Active Directory ユーザとマシンの属性を設定する必要があります。

ステップ 1 **[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > [Active Directory] を選択します。

ステップ 2 [属性（Attributes）] タブをクリックします。

ステップ 3 **[追加（Add）]** > **[属性の追加（Add Attribute）]** を選択して属性を手動で追加するか、**[追加（Add）]** > **[ディレクトリから属性を選択（Select Attributes From Directory）]** を選択してディレクトリから属性のリストを選択します。

Cisco ISE では、属性タイプ IP を手動で追加するときに、ユーザ認証に IPv4 または IPv6 アドレスを使用して AD を設定できます。

ステップ 4 ディレクトリからの属性の追加を選択した場合、ユーザの名前を [サンプル ユーザ（Sample User）] フィールドまたは [マシン アカウント（Machine Account）] フィールドに入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザの属性のリストを取得します。たとえば、管理者属性のリストを取得するには **administrator** を入力します。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。

（注） ユーザ名の例を入力する場合、Cisco ISE が接続されているアクティブな Active Directory ドメインからユーザを選択します。マシン属性を取得するマシンの例を選択する場合、マシン名のプレフィックスとして「host/」を追加するか、SAM$ 形式を使用してください。たとえば、host/myhost を使用します。属性の取得時に表示される値の例は説明のみを目的としており、保存されません。

ステップ 5 選択する Active Directory の属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 属性を手動で追加する場合は、新しい属性の名前を入力します。

ステップ 7 [保存（**Save**）] をクリックします。

パスワード変更、マシン認証、およびマシン アクセス制限の設定の変更

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。詳細については、Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （594 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

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

ステップ 3 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 4 必要に応じて、パスワード変更、マシン認証、およびマシンアクセス制限（MAR）の設定を変更します。

これらのオプションはデフォルトで有効になっています。

マシンアクセス制限の有効化 - エージングタイム：MAR キャッシュ内の MAC アドレスがタイムアウトし、削除されるまでの時間（時間）。

ステップ 5 [ダイヤルイン チェックを有効にする（Enable dial-in check）] チェックボックスをオンにして、認証中またはクエリ中にユーザのダイヤルインアクセス権をチェックします。ダイヤルインアクセス権が拒否されている場合は、チェックの結果により認証拒否の原因になります。

ステップ 6 認証中またはクエリ中にサーバからユーザにコールバックするようにするには、[ダイヤルインクライアントのコールバック チェックを有効にする（Enable callback check for dial-in clients）] チェックボックスをオンにします。サーバによって使用される IP アドレスまたは電話番号は、発信者またはネットワーク管理者によって設定されます。チェックの結果は、RADIUS 応答でデバイスに返されます。

ステップ 7 プレーン テキスト認証に Kerberos を使用する場合は、[プレーン テキスト認証に Kerberos を使用（Use Kerberos for Plain Text Authentications）] チェックボックスをオンにします。デフォルトの推奨オプションは MS-RPC です。Kerberos は ISE 1.2 で使用されます。

マシンアクセス制限（MAR）キャッシュ

Cisco ISE のアプリケーションサービスを手動で停止すると、MAR キャッシュ コンテンツ、calling-station-ID リスト、および対応するタイムスタンプを、ローカル ディスクのファイルに保存します。アプリケーション サービスを誤って再起動した場合、Cisco ISE はインスタンスの MAR キャッシュ エントリを保存しません。アプリケーション サービスが再起動すると、Cisco ISE はキャッシュエントリの存続時間に基づいて、ローカルディスクのファイルから MAR キャッシュエントリを読み取ります。再起動後にアプリケーションサービスが起動すると、Cisco ISE はそのインスタンスの現在の時刻と MAR キャッシュエントリの時刻を比較します。現在の時刻と MAR エントリの時刻の差が MAR キャッシュ エントリの存続時間よりも大きい場合は、Cisco ISE はディスクからそのエントリを取得しません。それ以外の場合、Cisco ISE は MAR キャッシュ エントリを取得し、MAR キャッシュ エントリ存続時間を更新します。

MAR キャッシュを設定するには、次の手順を実行します。

外部 ID に ソースで定義されている Active Directory の [詳細設定（Advanced Settings）] タブで、次のオプションがオンになっていることを確認します。

- [マシン認証の有効化（Enable Machine Authentication）]：マシン認証を有効にします。
- [マシンアクセス制限の有効化（Enable Machine Access Restriction）]：承認前にユーザとマシン認証を組み合わせます。

認証で MAR キャッシュを使用するには、次の手順を実行します。

認証ポリシーで `WasMachineAuthenticated is True` を使用します。このルールとクレデンシャルルールを使用すると、デュアル認証を行うことができます。マシン認証は、AD クレデンシャルの前に実行する必要があります。

[システム（System）] > [展開（Deployment）] ページでノードグループを作成した場合は、MAR のキャッシュ配布を有効にします。MAR のキャッシュ配布は、同じノードグループ内のすべての PSN に MAR キャッシュを複製します。

詳細情報

次の Cisco ISE コミュニティのページを参照してください。

- EAP-TLS が使用可能な場合でも MAR が便利な理由 https://community.cisco.com/t5/policy-and-access/mar-why-is-it-useful/td-p/3213527
- MAR エージングタイムと AnyConnect EAP-TLS の比較 https://community.cisco.com/t5/policy-and-access/ise-2-1-mar-aging-time-eap-tls/td-p/3209628

関連トピック

外部 ID ソースとしての Active Directory の設定 （594 ページ）

カスタム スキーマの設定

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 参加ポイントを選択します。

ステップ 3 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 4 [スキーマ（Schema）]セクションの[スキーマ（Schema）] ドロップダウンリストから[カスタム（Custom）] オプションを選択します。必要に応じて、ユーザ情報の属性を更新できます。これらの属性は、ユーザ情報（名、姓、電子メール、電話番号、地域など）の収集に使用されます。

事前設定された属性は、Active Directory スキーマ（組み込みのスキーマ）に使用されます。事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。

Active Directory の複数参加設定のサポート

Cisco ISE では、Active Directory ドメインへの複数参加がサポートされます。Cisco ISE では、50 までの Active Directory 参加がサポートされます。Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。Active Directory の複数ドメイン参加は、各参加の独自のグループ、属性、および許可ポリシーを持つ個別の Active Directory ドメインのセットで構成されます。

同じフォレストに複数回参加できます。つまり、必要に応じて、同じフォレスト内の複数のドメインに参加できます。

Cisco ISE は、単方向の信頼があるドメインに参加できます。このオプションで、単方向の信頼によって生じる権限の問題を回避できます。いずれかの信頼ドメインに参加できるため、両方のドメインを確認できます。

- 参加ポイント：Cisco ISE では、Active Directory ドメインへの個別参加は、参加ポイントと呼ばれます。Active Directory の参加ポイントは、Cisco ISE の ID ストアであり、認証ポリシーで使用できます。属性およびグループの関連ディクショナリがあり、許可条件で使用できます。
- スコープ：グループ化された Active Directory の参加ポイントのサブセットは、スコープと呼ばれます。単一参加ポイントの代わりに、認証結果として認証ポリシーでスコープを使用できます。スコープは、複数の参加ポイントに対してユーザを認証するために使用されます。各参加ポイントに複数のルールを使用する代わりにスコープを使用すると、単一のルールで同じポリシーを作成することができ、Cisco ISE で要求の処理やパフォーマンスの向上にかかる時間を短縮できます。参加ポイントには、複数のスコープが含まれる場合があります。スコープは、ID ソース順序に含まれる場合があります。スコープには関連す

るディクショナリがないため、許可ポリシー条件にスコープを使用することはできません。

新しいCisco ISEのインストールを実行する場合、デフォルトでスコープは存在しません。これは、ノー スコープ モードと呼ばれます。スコープを追加すると、Cisco ISE はマルチスコープモードになります。必要に応じて、ノースコープモードに戻すことができます。すべての参加ポイントは [Active Directory] フォルダに移動されます。

- Initial_Scope は、ノー スコープ モードで追加された Active Directory 参加ポイントの格納に使用される暗黙のスコープです。マルチスコープモードを有効にすると、すべての Active Directory 参加ポイントが自動作成された Initial_Scope に移動します。Initial_Scope の名前を変更できます。
- All_AD_Instances は組み込み型の疑似スコープで、Active Directory 設定には表示されません。これは、認証結果としてポリシーおよび ID 順序にのみ示されます。Cisco ISE で設定されたすべての Active Directory 参加ポイントを選択する場合は、このスコープを選択できます。

Active Directory 参加ポイントを追加する新しいスコープの作成

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [スコープモード（Scope Mode）] をクリックします。
Initial_Scope と呼ばれるデフォルトのスコープが作成され、現在のすべての参加ポイントがこのスコープに配置されます。

ステップ 3 より多くのスコープを作成するには、[追加（Add）] をクリックします。

ステップ 4 新しいスコープの名前と説明を入力します。

ステップ 5 [送信（Submit）] をクリックします。

ID 書き換え

ID 書き換えは、外部 Active Directory システムに渡される前に ID を操作するよう Cisco ISE に指示する拡張機能です。ID を必要な形式（任意のドメイン プレフィクスやサフィックスまたはその他の追加マークアップを含むまたは除く）に変更するためのルールを作成できます。

ID書き換えルールは、サブジェクト検索、認証クエリー、許可クエリーなどの操作のために、クライアントから受信したユーザ名またはホスト名に対してActive Directoryに渡される前に適用されます。Cisco ISE は条件のトークンを照合し、最初の 1 つが一致するとポリシーの処理を停止して、結果に応じて ID 文字列を書き換えます。

書き換え時、角カッコ [ ] で囲まれている（[IDENTITY] など）内容はすべて、評価側では評価されず、代わりに文字列内のその場所に一致する文字列が付加される変数です。角カッコなしはすべて、ルールの評価側と書き換え側の両方で、固定文字列として評価されます。

次に、ユーザによって入力された ID が ACME\jdoe であるとした場合の ID 書き換えの例を示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**[IDENTITY]** に書き換えます。

  結果は jdoe です。このルールは、ACME プレフィクスを持つすべてのユーザ名を削除するよう Cisco ISE に指示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**[IDENTITY]@ACME.com** に書き換えます。

  結果は jdoe@ACME.com です。このルールは、形式をプレフィクス表記からサフィックス表記に、または NetBIOS 形式から UPN 形式に変更するよう Cisco ISE に指示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**ACME2\[IDENTITY]** に書き換えます。

  結果は ACME2\jdoe です。このルールは、特定のプレフィクスを持つすべてのユーザ名を代替プレフィクスに変更するよう Cisco ISE に指示します。

- ID が **[ACME]\jdoe.USA** と一致する場合、**[IDENTITY]@[ACME].com** に書き換えます。

  結果は jdoe\ACME.com です。このルールは、ドットの後の領域を削除するよう Cisco ISE に指示します。この場合は国名で、正しいドメインに置き換えられます。

- ID が **E=[IDENTITY]** と一致する場合、**[IDENTITY]** に書き換えます。

  結果は jdoe です。これは、ID が証明書から取得され、フィールドが電子メール アドレスで、Active Directory がサブジェクトで検索するように設定されている場合に作成可能なルールの例です。このルールは、「E=」を削除するように Cisco ISE に指示します。

- ID が **E=[EMAIL],[DN]** と一致する場合、**[DN]** に書き換えます。

  このルールは、証明書サブジェクトを、E= jdoe@acme.com、CN=jdoe、DC=acme、DC=com から単なる DN、CN=jdoe、DC=acme、DC=com に変換します。これは、ID が証明書サブジェクトから取得され、Active Directory が DN でユーザ検索するように設定されている場合に作成可能なルールの例です。このルールは、電子メール プレフィクスを削除し、DN を生成するよう Cisco ISE に指示します。

次に、ID 書き換えルールを記述する際によくある間違いを示します。

- ID が **[DOMAIN]\[IDENTITY]** と一致する場合、**[IDENTITY]@DOMAIN.com** に書き換えます。

  結果は jdoe@DOMAIN.com です。このルールは、ルールの書き換え側の角カッコ [ ] に [DOMAIN] がありません。

- ID が **DOMAIN\[IDENTITY]** と一致する場合、**[IDENTITY]@[DOMAIN].com** に書き換えます。

  この場合も、結果は jdoe@DOMAIN.com です。このルールは、ルールの評価側の角カッコ [ ] に [DOMAIN] がありません。

ID 書き換えルールは、常に、Active Directory 参加ポイントのコンテキスト内で適用されます。認証ポリシーの結果としてスコープが選択されている場合でも、書き換えルールは、各 Active

Directory 参加ポイントに適用されます。EAP-TLS が使用されている場合、これらの書き換えルールは、証明書から取得される ID にも適用されます。

ID 書き換えの有効化

（注） この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 3 [ID 書き換え（Identity Rewrite）] セクションで、ユーザ名を変更する書き換えルールを適用するかどうかを選択します。

ステップ 4 一致条件および書き換え結果を入力します。表示されるデフォルトルールを削除し、要件に応じてルールを入力できます。Cisco ISE は順番にポリシーを処理し、要求ユーザ名に一致する最初の条件が適用されます。一致トークン（角カッコ内に含まれるテキスト）を使用して、元のユーザ名の要素を結果に転送できます。いずれのルールにも一致しない場合、識別名は変更されません。[テスト開始（Launch Test）] ボタンをクリックして、書き換え処理をプレビューできます。

ID 解決の設定

一部のタイプの ID には、プレフィクスまたはサフィックスのようなドメイン マークアップが含まれます。たとえば、ACME\jdoe などの NetBIOS ID では、「ACME」がドメイン マークアップのプレフィクスで、同様に jdoe@acme.com などの UPN ID では、「acme.com」がドメイン マークアップのサフィックスです。ドメイン プレフィクスは、組織内の Active Directory ドメインの NetBIOS（NTLM）名に一致し、ドメイン サフィックスは、組織内の Active Directory ドメインの DNS 名または代替 UPN サフィックスに一致する必要があります。たとえば、gmail.com は Active Directory ドメインの DNS 名ではないため、jdoe@gmail.com はドメイン マークアップなしとして処理されます。

ID 解決設定では、Active Directory 展開に一致するように、セキュリティおよびパフォーマンスのバランスを調整する重要な設定を指定できます。これらの設定を使用して、ドメイン マークアップのないユーザ名およびホスト名の認証を調整できます。Cisco ISE でユーザのドメインを認識できない場合、すべての認証ドメインでユーザを検索するように設定できます。ユーザが 1 つのドメインで見つかった場合でも、Cisco ISE は ID のあいまいさがないことを確実にするために、すべての応答を待ちます。この処理は、ドメインの数、ネットワークの遅延、負荷などに応じて、時間がかかる場合があります。

ID 解決問題の回避

認証時に、ユーザおよびホストに完全修飾名（つまり、ドメインマークアップが含まれている名前）を使用することを強く推奨します。たとえば、ユーザの UPN と NetBIOS 名、およびホストの FQDN SPN です。これは、複数の Active Directory アカウントが受信ユーザ名と一致する（たとえば、jdoe が jdoe@emea.acme.com および jdoe@amer.acme.com と一致する）など、あいまいエラーが頻繁に生じる場合に特に重要です。場合によっては、完全修飾名を使用することが、問題を解決する唯一の方法になります。また、ユーザに一意のパスワードが設定されていることを保証するだけで十分な場合もあります。したがって、一意の ID を最初から使用すると、効率が向上し、パスワード ロックアウトの問題が減少します。

ID 解決の設定

（注） この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 3 [ID 解決（Identity Resolution）] セクションで、ユーザ名またはマシン名の ID 解決についての次の設定を定義します。この設定によって、ユーザの検索と認証を詳細に制御できます。

最初に、マークアップなしの ID に対する設定を行います。このような場合、次のオプションのいずれかを選択できます。

- [要求を拒否する（Reject the request）]：このオプションを使用すると、SAM 名などのドメイン マークアップがないユーザの認証は失敗します。このことは、複数参加ドメインで、Cisco ISE がすべての参加グローバル カタログの ID を検索する必要があることによって、安全性が低下する可能性がある場合に役立ちます。このオプションによって、ドメイン マークアップを含むユーザ名を使用することがユーザに対して強制されます。
- [結合されたフォレストの「認証ドメイン」のみで検索する（Only search in the “Authentication Domains” from the joined forest）]：このオプションを使用すると、認証ドメインの セクションで指定した、結合ポイントのフォレスト内のドメインのみで ID が検索されます。これはデフォルト オプションであり、SAM アカウント名に対する Cisco ISE 1.2 の動作と同じです。
- [すべての「認証ドメイン」セクションで検索する（Search in all the “Authentication Domains” sections）]：このオプションを使用すると、すべての信頼されたフォレストのすべての認証ドメインで ID が検索されます。これにより、遅延が増加し、パフォーマンスに影響する可能性があります。

Cisco ISE で認証ドメインがどのように設定されているかに基づいて選択します。特定の認証ドメインのみを選択した場合は、それらのドメインのみが検索されます（「結合されたフォレスト」と「すべてのフォレスト」のいずれを選択した場合も）。

2 番目の設定は、Cisco ISE が、[認証ドメイン（Authentication Domains）] セクションで指定された設定に準拠するために必要となるすべてのグローバルカタログ（GC）と通信できない場合に使用します。このような場合、次のオプションのいずれかを選択できます。

- [使用可能なドメインで続行する（Proceed with available domains）]：このオプションを使用すると、使用可能ないずれかのドメインで一致が見つかった場合に認証が続行されます。
- [要求をドロップする（Drop the request）]：このオプションを使用すると、ID 解決で到達不能または使用できないドメインが検出された場合に認証要求がドロップされます。

Active Directory 認証のためのユーザのテスト

Active Directory からユーザ認証を検証するには、[ユーザのテスト（Test User）] ツールを使用できます。グループおよび属性を取得して調査することもできます。単一の参加ポイントまたはスコープのテストを実行できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- すべての参加ポイントのテストを実行するには、**[拡張ツール（Advanced Tools）] > [すべての参加ポイントのユーザをテスト（Test User for All Join Points）]** を選択します。
- 特定の参加ポイントのテストを実行するには、参加ポイントを選択し、[編集（Edit）] をクリックします。Cisco ISE ノードを選択し、[ユーザのテスト（Test User）] をクリックします。

ステップ 3 Active Directory のユーザ（またはホスト）のユーザ名とパスワードを入力します。

ステップ 4 認証タイプを選択します。ステップ 3 のパスワード入力は、ルックアップ オプションを選択する場合には必要ありません。

ステップ 5 すべての参加ポイントに対してこのテストを実行する場合は、このテストを実行する Cisco ISE ノードを選択します。

ステップ 6 Active Directory からグループおよび属性を取得するには、[グループを取得（Retrieve Groups）] および [属性の取得（Retrieve Attributes）] チェック ボックスをオンにします。

ステップ 7 [テスト（Test）] をクリックします。
テスト操作の結果と手順が表示されます。手順で失敗の原因を特定し、トラブルシューティングできます。

また、Active Directory がそれぞれの処理手順（認証、参照、グループおよび属性の取得）を実行するのに要する時間（ミリ秒単位）を表示することもできます。操作にかかる時間がしきい値を超えると、Cisco ISE に警告メッセージが表示されます。

Active Directory の設定の削除

Active Directory を外部 ID ソースとして使用しない場合は、Active Directory の設定を削除する必要があります。別の Active Directory ドメインに参加する場合は、設定を削除しないでください。現在参加しているドメインから脱退し、新しいドメインに参加できます。

始める前に

Active Directory ドメインが残っていることを確認します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 設定された Active Directory の横のチェックボックスをオンにします。

ステップ 3 [ローカル ノード ステータス（Local Node Status）] が [参加していない（Not Joined）] としてリストされていることを確認します。

ステップ 4 [削除（Delete）] をクリックします。

Active Directory データベースから設定を削除しました。後で Active Directory を使用する場合は、有効な Active Directory の設定を再送信できます。

ノードの Active Directory の参加の表示

特定の Cisco ISE ノードのすべての Active Directory 参加ポイントのステータスまたはすべての Cisco ISE ノードのすべての参加ポイントのリストを表示するには、[Active Directory] ページの [ノード ビュー（Node View）] ボタンを使用できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [ノード ビュー（Node View）] をクリックします。

ステップ 3 [ISE Node（ISE ノード）] ドロップダウン リストからノードを選択します。
テーブルに、Active Directory のステータスがノード別に一覧されます。展開に複数の参加ポイントと複数の Cisco ISE ノードがある場合、このテーブルが更新されるまでに数分かかる場合があります。

ステップ 4 その Active Directory 参加ポイントのページに移動し、その他の特定のアクションを実行するには、参加ポイントの [名前（Name）] リンクをクリックします。

ステップ 5 [診断ツール（Diagnostic Tools）] ページに移動して特定の問題のトラブルシューティングを行うには、[診断概要（Diagnostic Summary）] 列のリンクをクリックします。診断ツールでは、ノードごとに各参加ポイントの最新の診断結果が表示されます。

Active Directory の問題の診断

診断ツールは、各 Cisco ISE ノードで実行されるサービスです。診断ツールを使用して、Active Directory 展開を自動的にテストおよび診断したり、Cisco ISE によって Active Directory が使用される場合に機能やパフォーマンスの障害の原因となる可能性がある問題を検出するための一連のテストを実行したりすることができます。

Cisco ISE が Active Directory に参加できない、または Active Directory に対して認証できない理由は、複数あります。このツールは、Cisco ISE を Active Directory に接続するための前提条件が正しく設定されていることを確認するのに役立ちます。また、ネットワーク、ファイアウォール設定、クロック同期、ユーザ認証などの問題の検出に役立ちます。このツールは、手順をステップごとに説明したガイドとして機能し、必要に応じて、中間の各レイヤの問題の修正を支援します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [拡張ツール（Advanced Tools）] ドロップダウン リストをクリックし、[診断ツール（Diagnostic Tools）] を選択します。

ステップ 3 診断を実行する Cisco ISE ノードを選択します。

Cisco ISE ノードを選択しない場合は、すべてのノードでテストが実行されます。

ステップ 4 特定の Active Directory 参加ポイントを選択します。

Active Directory 参加ポイントを選択しない場合は、すべての参加ポイントでテストが実行されます。

ステップ 5 オンデマンドで、またはスケジュールに基づいて診断テストを実行できます。

- テストをすぐに実行するには、[テストを今すぐ実行（Run Tests Now）] を選択します。
- スケジュールした間隔でテストを実行するには、[スケジュールしたテストを実行する（Run Scheduled Tests）] チェックボックスをオンにし、開始時刻とテストの実行間隔（時、日、週単位）を指定します。このオプションを有効にすると、すべての診断テストがすべてのノードとインスタンスに対して実行され、[ホーム（Home）] ダッシュボードの [アラーム（Alarms）] ダッシュレットに障害が報告されます。

ステップ 6 警告ステータスまたは失敗ステータスのテストの詳細を確認するには、[テストの詳細の表示（View Test Details）] をクリックします。
このテーブルを使用して、特定のテストの再実行、実行中のテストの停止、特定のテストのレポートの表示を行うことができます。

Active Directory デバッグ ログの有効化

Active Directory デバッグ ログはデフォルトでは記録されません。展開でポリシー サービス ペルソナを担当する Cisco ISE ノードでこのオプションを有効にする必要があります。Active Directory のデバッグ ログを有効にすると、ISE のパフォーマンスに影響する場合があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログの設定（Debug Log Configuration）]** を選択します。

ステップ 2 Active Directory のデバッグ情報を取得する Cisco ISE ポリシー サービス ノードの隣のオプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 3 [Active Directory] オプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 4 [Active Directory] の隣にあるドロップダウン リストから [DEBUG] を選択します。これにはエラー、警告、および verbose ログが含まれます。完全なログを取得するには、[TRACE] を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

トラブルシューティング用の Active Directory ログ ファイルの入手

可能性がある問題をトラブルシューティングするには、Active Directory のデバッグ ログをダウンロードし、表示します。

始める前に

Active Directory のデバッグ ロギングを有効にする必要があります。

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）]** を選択します。

ステップ 2 Active Directory のデバッグ ログ ファイルを取得するノードをクリックします。

ステップ 3 [デバッグ ログ（Debug Logs）] タブをクリックします。

ステップ 4 このページを下にスクロールして ad_agent.log ファイルを見つけます。このファイルをクリックしてダウンロードします。

Active Directory のアラームおよびレポート

Cisco ISE は、Active Directory に関連するアクティビティをモニタリングし、トラブルシューティングを実行するためのさまざまなアラームおよびレポートを提供します。

アラーム

Active Directory のエラーおよび問題に対して、次のアラームがトリガーされます。

- 構成済みネーム サーバが使用不可（Configured nameserver not available）
- 参加しているドメインが使用不可（Joined domain is unavailable）
- 認証ドメインが使用不可（Authentication domain is unavailable）
- Active Directory フォレストが使用不可（Active Directory forest is unavailable）
- AD コネクタを再起動する必要があります（AD Connector had to be restarted）
- AD：ISE アカウント パスワードの更新に失敗（AD: ISE account password update failed）
- AD：マシン TGT のリフレッシュに失敗（AD: Machine TGT refresh failed）

レポート

次の 2 つのレポートで Active Directory に関連するアクティビティをモニタリングできます。

- RADIUS 認証レポート：このレポートは、Active Directory の認証および許可の詳細な手順を示します。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [認証サービス ステータス（Auth Services Status）] > [RADIUS 認証（RADIUS Authentications）]** にあります。
- AD コネクタ操作レポート：AD コネクタ操作レポートは、AD コネクタが実行するバックグラウンド操作（Cisco ISE サーバ パスワードのリフレッシュ、Kerberos チケットの管理、DNS クエリー、DC 検出、LDAP、および RPC 接続管理など）のログを提供します。Active Directory の障害が発生した場合は、考えられる原因を特定するために、このレポートで詳細を確認できます。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [認証サービス ステータス（Auth Services Status）] > [AD コネクタ操作（AD Connector Operations）]** にあります。

Active Directory の高度な調整

高度な調整機能により、シスコのサポート担当者の管理下で、サポート操作に使用されるノード固有の設定が可能となり、システムのさらに深いレベルでパラメータを調整できるようになります。これらの設定は、通常の管理フローを対象としていません。ガイダンスに従って使用する必要があります。

Active Directory アイデンティティ検索属性

Cisco ISE は、SAM と CN のいずれか、または両方の属性を使用してユーザを識別します。Cisco ISE リリース 2.2 パッチ 5 以降、および 2.3 パッチ 2 以降は、sAMAccountName 属性をデフォルトの属性として使用します。これ以前のリリースでは、SAM と CN の両方の属性がデフォルトで検索されていました。この動作はリリース 2.2 パッチ 5 以降と 2.3 パッチ 2 以降で、CSCvf21978 バグ修正の一部として変更されました。これらのリリースでは、sAMAccountName 属性のみがデフォルトの属性として使用されます。

実際の環境で必要に応じて、SAM と CN のいずれか、または両方を使用するように Cisco ISE を設定できます。SAM および CN が使用される場合、SAMAccountName 属性の値が一意でないと、Cisco ISE は CN 属性値も比較します。

（注） デフォルトでは、Cisco ISE 2.4 の ID 検索の動作は SAM アカウント名のみを検索するように変更されました。このデフォルトの動作を変更するには、「Active Directory アイデンティティ検索の属性の設定」のセクションで説明しているように「IdentityLookupField」フラグの値を変更します。

Active Directory アイデンティティ検索の属性の設定

1. **[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory]**を選択します。[Active Directory] ウィンドウで、[拡張ツール（Advanced Tools）] をクリックし、[高度な調整（Advanced Tuning）] を選択します。次の詳細を入力します。
   - [ISEノード（ISE Node）]：Active Directory に接続される ISE ノードを選択します。
   - [名前（Name）]：変更するレジストリキーを入力します。Active Directory 検索属性を変更するには、`REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField` と入力します。
   - [値（Value）]：ユーザを識別するために ISE で使用する属性を入力します。
     - *SAM*：クエリで SAM のみを使用します（このオプションがデフォルトです）。
     - *CN*：クエリで CN のみを使用します。
     - *SAMCN*：クエリで CN と SAM を使用します。
   - **コメント**：変更内容を記述します（たとえば「デフォルト動作を SAM および CN に変更」）。
2. [値の更新（Update Value）] をクリックしてレジストリを更新します。

   ポップアップウィンドウが表示されます。メッセージを読み取り、変更を受け入れます。ISE の AD コネクタサービスが再起動します。

検索文字列の例

次の例では、ユーザ名が *userd2only* であると想定します。

- SAM 検索文字列：

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(|(cn=userd2only)(sAMAccountName=userd2only)))]
```

- SAM および CN 検索文字列：

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=userd2only))]
```

Active Directory が構成された Cisco ISE をセットアップするための補足情報

Active Directory が構成された Cisco ISE を設定するには、グループ ポリシーを設定し、マシン認証のサプリカントを設定する必要があります。

Active Directory のグループ ポリシーの設定

グループ ポリシー管理エディタにアクセスする方法の詳細については、Microsoft Active Directory のマニュアルを参照してください。

ステップ 1 次の図に示すように、グループ ポリシー管理エディタを開きます。

[グループ ポリシー オブジェクト（Group Policy Objects）] の選択

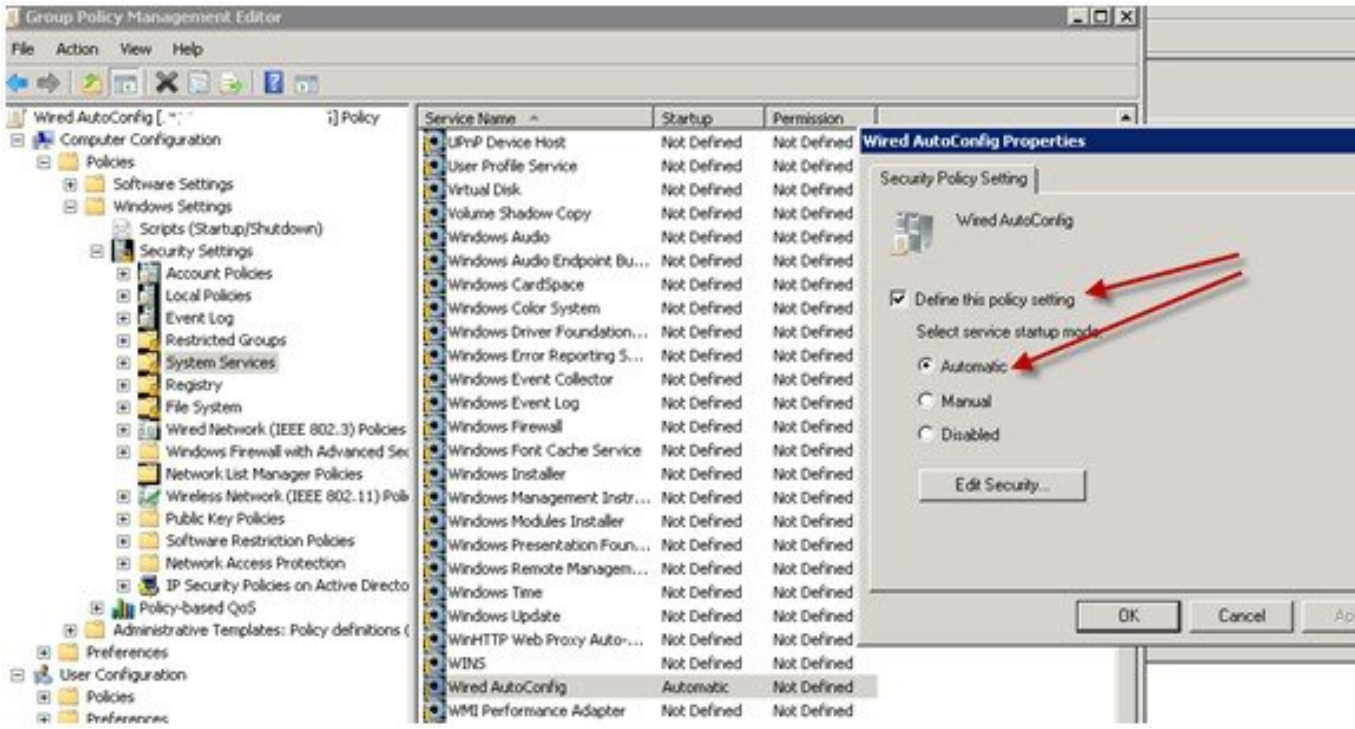
ステップ 2 新しいポリシーを作成し、その説明的な名前を入力するか、既存のドメイン ポリシーに追加します。

例：

次の例では、ポリシー名に Wired Autoconfiguration を使用しています。

ステップ 3 次の図に示すように、[このポリシー設定を定義する（Define this policy setting）] チェックボックスをオンにして、サービス起動モードの [自動（Automatic）] オプション ボタンをクリックします。

ポリシー プロパティ



ステップ 4 目的の組織ユニットまたはドメイン Active Directory レベルでポリシーを適用します。

コンピュータは再起動したときにポリシーを受信し、このサービスが有効になります。

Active Directory に対する EAP-TLS マシン認証のための Odyssey 5.X サプリカントの設定

Active Directory に対する EAP-TLS マシン認証に Odyssey 5.x サプリカントを使用している場合は、サプリカントで次の設定を行う必要があります。

ステップ 1 Odyssey アクセス クライアントを起動します。

ステップ 2 [ツール（Tools）] メニューから [Odyssey アクセス クライアント管理者（Odyssey Access Client Administrator）] を選択します。

ステップ 3 [マシン アカウント（Machine Account）] アイコンをダブルクリックします。

ステップ 4 [マシン アカウント（Machine Account）] ページから、EAP-TLS 認証のプロファイルを設定する必要があります。

a) **[設定（Configuration）] > [プロファイル（Profiles）]** を選択します。

b) EAP-TLS プロファイルの名前を入力します。

c) [認証（Authentication）] タブで、認証方式として [EAP-TLS] を選択します。

d) [証明書（Certificate）] タブで、[証明書を使用したログインを許可（Permit login using my certificate）] チェックボックスをオンにして、サプリカント マシンの証明書を選択します。

e) [ユーザ情報（User Info）] タブで、[マシン クレデンシャルを使用（Use machine credentials）] チェックボックスをオンにします。

このオプションが有効になっている場合、Odyssey サプリカントは host\<*machine_name*> の形式でマシン名を送信します。Active Directory は要求をマシンから送信されていると識別し、認証を実行するコンピュータ オブジェクトを検索します。このオプションが無効になっている場合、Odyssey サプリカントは host\ プレフィクスなしでマシン名を送信します。Active Directory はユーザ オブジェクトを検索し、認証は失敗します。

マシン認証のための AnyConnect エージェント

マシン認証のために AnyConnect エージェントを設定する場合、次のいずれかを実行できます。

- デフォルトのマシン ホスト名（プレフィクス「host/」を含む）を使用する。
- 新しいプロファイルを設定する。その場合、マシン名の前にプレフィクス「host/」を付加する必要があります。

Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件

Easy Connect および パッシブ ID サービスでは、Active Directory ドメイン コントローラによって生成される Active Directory ログイン監査イベントを利用して、ユーザ ログイン情報を収集します。ISE ユーザが接続を行い、ユーザ ログイン情報を取得することができるように、Active Directory サーバを適切に設定する必要があります。ここでは、Easy Connect および パッシブ ID サービスをサポートするように Active Directory ドメインコントローラを設定する方法（Active Directory 側からの設定）について説明します。

Easy Connect およびパッシブ ID サービスをサポートするように Active Directory ドメインコントローラを設定するには（Active Directory 側からの設定）、次の手順に従います：

（注） すべてのドメインのすべてのドメインコントローラを設定する必要があります。

1. ISE から Active Directory の参加ポイントとドメイン コントローラを設定します。Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （594 ページ）およびドメイン コントローラの追加 （596 ページ）を参照してください。
2. ドメイン コントローラごとに WMI を設定します。パッシブ ID 用の WMI の設定 （597 ページ）を参照してください。
3. Active Directory で次の操作を実行します。
   - パッシブ ID サービス の Active Directory の設定 （621 ページ）

- Windows 監査ポリシーの設定 （625 ページ）

4. （オプション）Active Directory で ISE により実行された自動設定のトラブルシューティングを行うには、次の操作を実行します。
   - AD ユーザがドメイン管理グループに属しているときの権限の設定 （625 ページ）
   - AD ユーザがドメイン管理グループの一部ではない場合に必要な権限 （626 ページ）
   - ドメイン コントローラで DCOM を使用するための権限 （627 ページ）
   - WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （629 ページ）
   - AD ドメイン コントローラのセキュリティ イベント ログへのアクセス権の付与 （630 ページ）

パッシブ ID サービス の Active Directory の設定

ISE Easy Connect およびパッシブ ID サービスでは、ユーザ ログイン情報を収集するため、Active Directory ドメイン コントローラにより生成される Active Directory ログイン監査イベントが使用されます。ISE は Active Directory に接続し、ユーザ ログイン情報を取得します。

次の手順は、Active Directory ドメイン コントローラから実行する必要があります。

ステップ 1 該当する Microsoft のパッチが Active Directory ドメイン コントローラにインストールされていることを確認します。

a) Windows Server 2008 には次のパッチが必要です。

- http://support.microsoft.com/kb/958124

  このパッチは、ISE がドメイン コントローラと正常な接続を確立するのを妨げる Microsoft WMI でのメモリ リークを解消します（ISE 管理者は、ISE Active Directory ドメイン コントローラの GUI ページでこの問題を体験する場合があります。この GUI ページでは、接続が正常に確立されたときにステータスが「up」になる必要があります）。

- http://support.microsoft.com/kb/973995

  このパッチは、Microsoft WMI の別のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザ ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。結果として、ISE はこのドメイン コントローラからすべてのユーザ ログイン イベントを取得できない場合があります。

b) Windows Server 2008 R2 では、（SP1 がインストールされていない場合）次のパッチが必要です。

- http://support.microsoft.com/kb/981314

  このパッチは、Microsoft WMI のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザ ログイン イベントをドメイン コントローラのセキュリティ

ログに書き込むのを散発的に妨げます。結果として、ISE はこのドメイン コントローラからすべてのユーザ ログイン イベントを取得できない場合があります。

- http://support.microsoft.com/kb/2617858

このパッチは、Windows Server 2008 R2 での予期しない起動やログイン プロセスの遅れを解消します。

c) Windows プラットフォームの WMI 関連問題には、次のリンクにリストされているパッチが必要です。

- http://support.microsoft.com/kb/2591403

これらのホットフィックスは、WMI サービスおよび関連コンポーネントの動作と機能に関連付けられます。

ステップ 2 Active Directory がユーザ ログイン イベントを Windows セキュリティ ログに記録するのを確認します。

「監査ポリシー」（「グループ ポリシーの管理」設定の一部）が、正常なログインによって、Windows セキュリティ ログに必要なイベントが生成されるように設定されていることを確認します（これはデフォルトの Windows 設定ですが、この設定が適切であることを明示的に確認する必要があります）。「Windows 監査ポリシーの設定」を参照してください。

ステップ 3 ISE が Active Directory に接続するための十分な権限を持つ Active Directory ユーザを設定する必要があります。次の手順では、管理ドメイン グループのユーザ、または管理ドメイン グループではないユーザに対して権限を定義する方法を示します。

- Active Directory ユーザがドメイン管理グループのメンバーである場合に必要な権限（2 ～ 4 ページ）
- Active Directory ユーザがドメイン管理グループのメンバーでない場合に必要な権限（2 ～ 4 ページ）

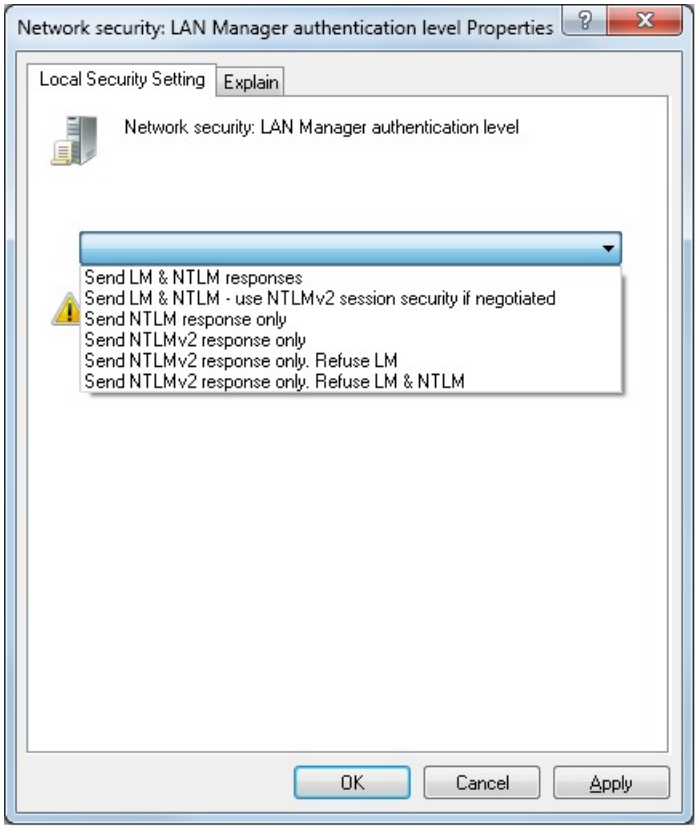
ステップ 4 ISE によって使用される Active Directory ユーザは、NT Lan Manager（NTLM）v1 または v2 のいずれかによって認証を受けることができます。ISE と Active Directory ドメイン コントローラ間の正常な認証済み接続を確実に行うために、Active Directory NTLM の設定が ISE NTLM の設定と合っていることを確認する必要があります。次の表に、すべての Microsoft NTLM オプションと、サポート対象の ISE NTLM アクションを示します。ISE が NTLMv2 に設定される場合、記載されている 6 つのオプションがすべてサポートされます。NTLMv1 をサポートするように ISE が設定されている場合、最初の 5 つのオプションだけがサポートされます。

表 *57 : ISE* と *AD NTLM* のバージョン設定に基づいてサポートされる認証タイプ

ISE NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション NTLMv1 NTLMv2	**NTLMv1**	**NTLMv2**
LM & NTLM応答を送信接続を許可接続を許可（Send LM & NTLM responses connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます

ISE NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション NTLMv1 NTLMv2	NTLMv1	NTLMv2
LM & NTLMを送信：ネゴシエートされた接続が許可された場合にNTLMv2セッションセキュリティを使用接続を許可（Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみNTLM応答を送信接続を許可（Send NTLM response only connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみNTLMv2応答を送信接続を許可（Send NTLMv2 response only connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
NTLMv2応答のみを送信（Send NTLMv2 response only）。LMを拒否接続を許可接続を許可（Refuse LM connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
NTLMv2応答のみを送信（Send NTLMv2 response only）。LM & NTLMを拒否接続を拒否接続を許可（Refuse LM & NTLM connection is refused connection is allowed）	接続は拒否されます	接続が受け入れられます

図 *21 : MS NTLM* 認証タイプのオプション



ステップ 5 Active Directory ドメイン コントローラで `dllhost.exe` へのトラフィックを許可するファイアウォール ルールを作成していることを確認します。

ファイアウォールをオフにするか、または次のポートへの特定の IP（ISE IP アドレス）のアクセスを許可することができます。

- TCP 135：一般的な RPC ポート。非同期 RPC 発信をすると、このポートでリスニングしているサービスが、クライアントに、この要求を処理できるコンポーネントが使用しているポートを通知します。
- UDP 137：NetBIOS 名前解決
- UDP 138：NetBIOS データグラム サービス
- TCP 139：NetBIOS セッション サービス
- TCP 445：SMB

数値の大きいポートは動的に割り当てられ、手動で設定できます。ターゲットとして %SystemRoot%\System32\dllhost.exe を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォール ルールを、特定の IP アドレス（ISE IP）に割り当てることができます。

Windows 監査ポリシーの設定

監査ポリシー（**グループポリシー管理**設定の一部）が正常なログインを許可していることを確認します。これには、AD ドメイン コントローラ マシンの Windows セキュリティ ログに必要なイベントを生成する必要があります。これはデフォルトの Windows 設定ですが、この設定が正しいことを確認する必要があります。

ステップ 1 **[スタート]** > **[Programs]** > **[Administrative Tools]** > **[Group Policy Management]** を選択します。

ステップ 2 [Domains] で関連するドメインに移動し、ナビゲーション ツリーを展開します。

ステップ 3 [Default Domain Controller Policy] を選択し、右クリックして、[編集] を選択します。

グループ ポリシー管理エディターが表示されます。

ステップ 4 **[デフォルトのドメイン コントローラ ポリシー（Default Domain Controllers Policy ）]** > **[コンピュータ設定（Computer Configuration）]** > **[ポリシー（Policies）]** > **[Windows 設定（Windows Settings）]** > **[セキュリティ設定（Security Settings）]** の順に選択します。

- Windows Server 2003 または Windows Server 2008（R2 以外）の場合は **[ローカルポリシー（Local Policies）]** > **[監査ポリシー（Audit Policy）]** の順に選択します。2 つのポリシー項目（[Audit Account Logon Events] と [Audit Logon Events]）で、対応する [Policy Setting] に [Success] 状態が直接的または間接的に含まれていることを確認します。[Success] 状況を間接的に含めるには、[Policy Setting] に [Not Defined] を設定します。この場合、上位ドメインから有効値が継承されるため、[Success] 状態を明示的に含めるようにその上位ドメインの [Policy Setting] を設定する必要があります。
- Windows Server 2008 R2 および Windows 2012 の場合、**[Advanced Audit Policy Configuration]** > **[Audit Policies]** > **[Account Logon]** を選択します。2 つのポリシー項目（[Audit Kerberos Authentication Service] と [Audit Kerberos Service Ticket Operations]）に対応する [Policy Setting] に、前述のように [Success] 状態が直接または間接的に含まれていることを確認します。

ステップ 5 [監査ポリシー] の項目設定が変更されている場合は、`gpupdate /force` を実行して新しい設定を強制的に有効にする必要があります。

AD ユーザがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows 2012 および Windows 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティング システムの特定のレジストリ キーを完全に制御することができません。Active Directory の管理者は、Active Directory ユーザに次のレジストリ キーに対する完全制御権限を提供する必要があります。

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

次の Active Directory のバージョンでは、レジストリ変更は必要ありません。

- Windows 2003

- Windows 2003R2
- Windows 2008

完全な制御を許可するには、次に示すように、まず Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーを右クリックして [オーナー（Owner）] タブに移動します。
ステップ 2 [アクセス許可（Permissions）] をクリックします。
ステップ 3 [詳細設定（Advanced）] をクリックします。

AD ユーザがドメイン管理グループの一部ではない場合に必要な権限

Windows 2012 R2 の場合は、Active Directory ユーザに次のレジストリ キーに対する**完全制御**権限を提供します。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Active Directory ユーザがドメイン管理グループの一部ではなく、ドメイン ユーザ グループの一部である場合は、次の権限も必要です。

- ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加します（下記を参照）
- ドメイン コントローラで DCOM を使用するための権限 （627 ページ）
- WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （629 ページ）

これらの権限は、次の Active Directory のバージョンでのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加する

ISEがドメインユーザとして接続し、ログイン認証イベントを取得できるようにするには、ドメイン コントローラに一部のレジストリ キーを手動で追加する必要があります。エージェントはドメイン コントローラまたはドメイン内のマシンでは必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

キー **DllSurrogate** の値には、2 つのスペースが含まれていることを確認します。

上記のスクリプトに示すように、ファイルの末尾の空の行を含む、空の行を保持してください。

ドメイン コントローラで DCOM を使用するための権限

ISE パッシブ ID サービスに使用される Active Directory ユーザは、ドメイン コントローラで DCOM（リモート COM）を使用する権限がなければなりません。**dcomcnfg** コマンド ライン ツールを使用して権限を設定できます。

ステップ 1 コマンド ラインから **dcomcnfg** ツールを実行します。

ステップ 2 [コンポーネントサービス（Component Services）] を展開します。

ステップ 3 **[コンピュータ（Computers）]** > **[マイコンピュータ（My Computer）]** を展開します。

ステップ 4 メニュー バーで [アクション（Action）] を選択して、[プロパティ（properties）] をクリックし、[COMセキュリティ（COM Security）] をクリックします。

ステップ 5 アクセスおよび起動の両方に対してISEが使用するアカウントに許可権限があることを確認します。Active Directory ユーザは、4 つのオプション（[アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対する [制限の編集（Edit Limits）] と [デフォルトの編集（Edit Default）]）のすべてに追加される必要があります。

ステップ 6 [アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対してローカルおよびリモート アクセスをすべて許可します。

図 ***22 : [***アクセス権限（***Access Permissions***）***]*** のローカルおよびリモート アクセス

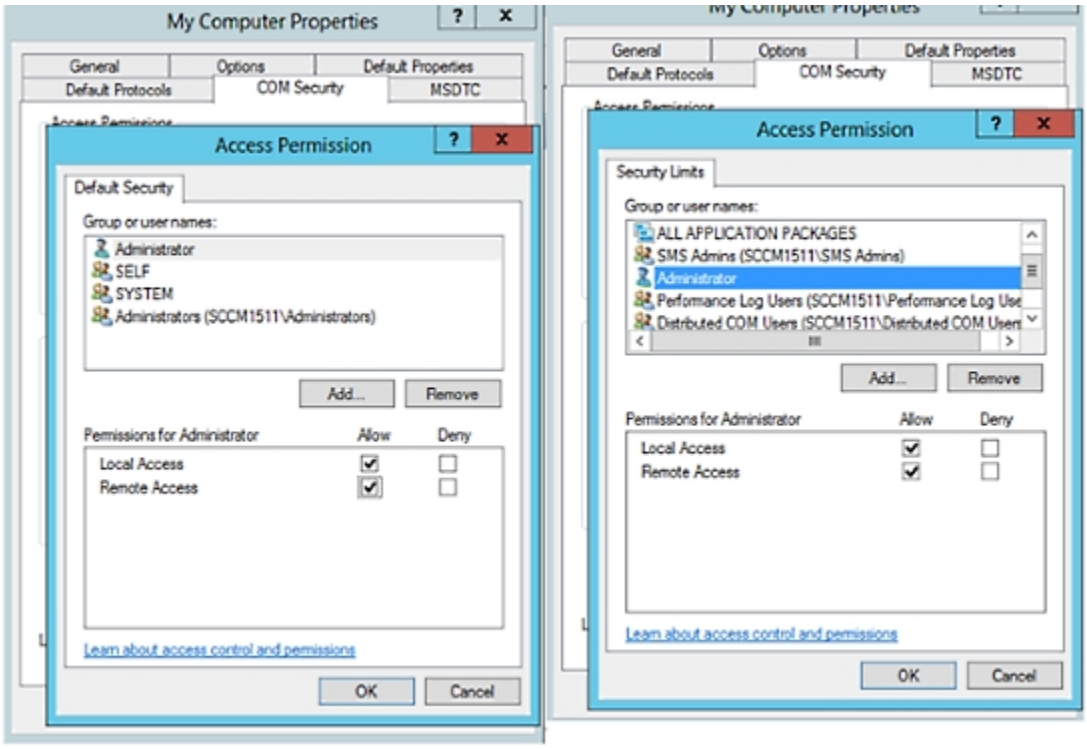
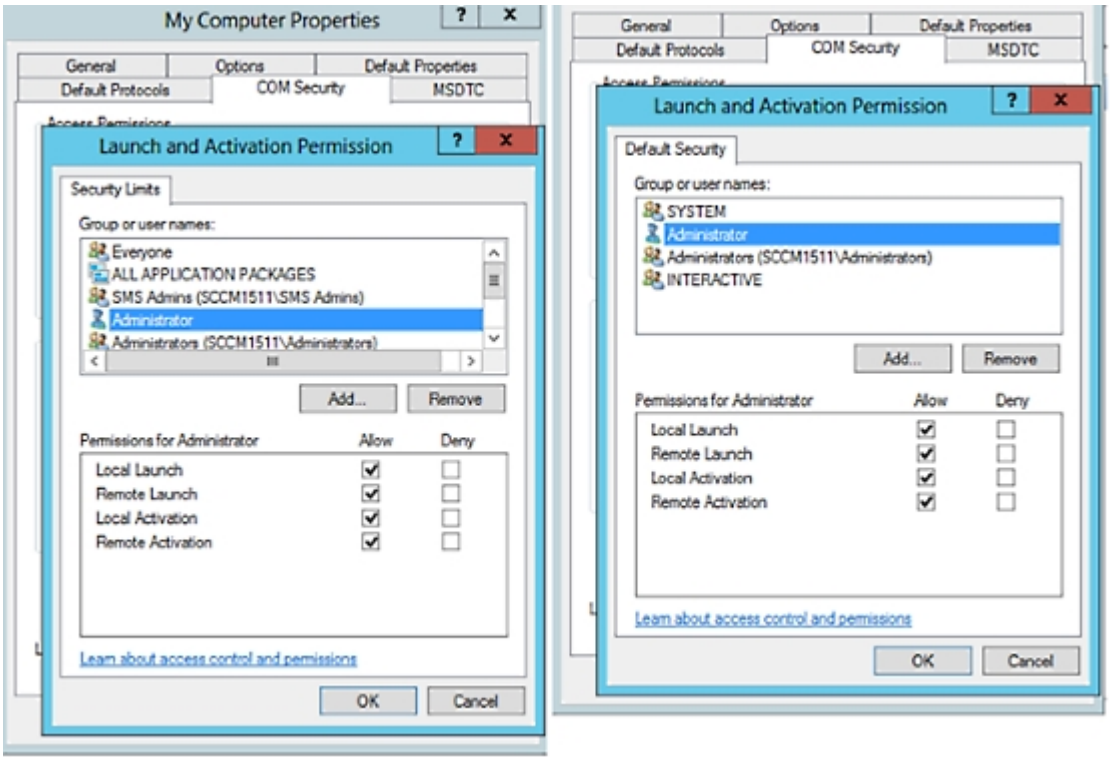


図 *23 : [*起動およびアクティベーションの権限（***Launch and Activation Permissions***）*]* のローカルおよびリモート アクセス



WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Active Directory ユーザには実行メソッドおよびリモートイネーブルのための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

ステップ 1 [スタート] > [Run] をクリックし、`wmimgmt.msc` と入力します。

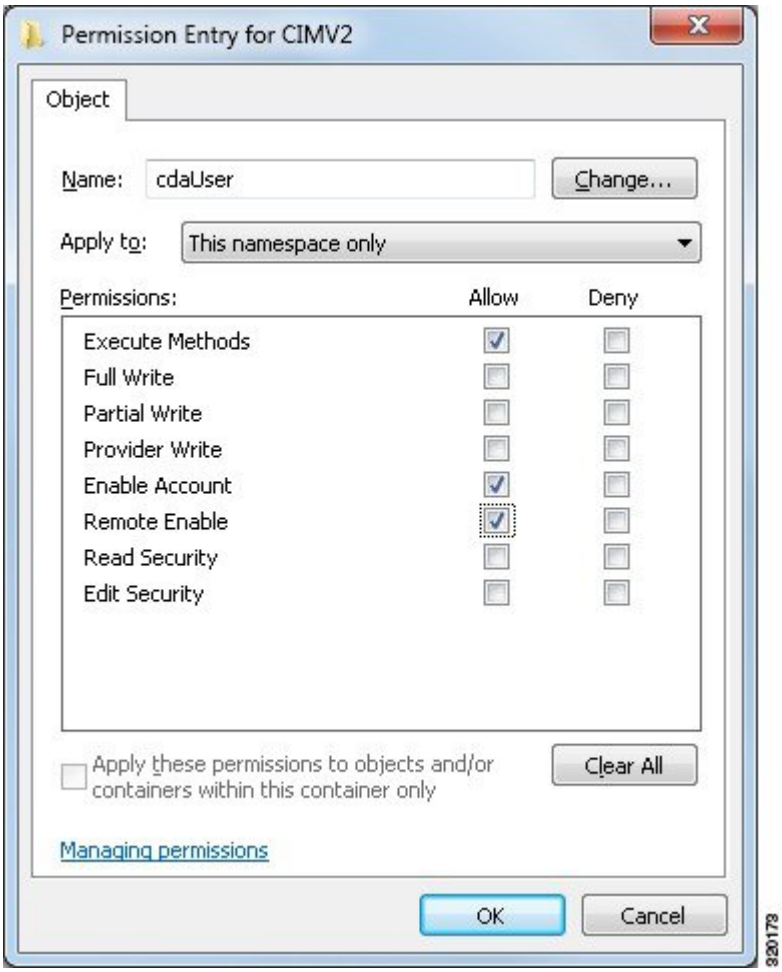
ステップ 2 [WMI Control] を右クリックし、[プロパティ] をクリックします。

ステップ 3 [セキュリティ] タブで [ルート] を展開し、[CIMV2] を選択します。

ステップ 4 [セキュリティ（Security）] をクリックします。

ステップ 5 下に示すように、Active Directory ユーザを追加し、必要な権限を設定します。

図 *24 : WMI Root\CIMv2* 名前空間に必要な権限



AD ドメイン コントローラのセキュリティ イベント ログへのアクセス権の付与

Windows 2008 以降では、ISE ID マッピング ユーザを Event Log Reader と呼ばれるグループに追加することで、AD ドメイン コントローラのログへのアクセス権を付与できます。

Windows のすべての旧バージョンでは、次に示すようにレジストリ キーを編集する必要があります。

ステップ 1 セキュリティ イベント ログへのアクセス権を委任するには、アカウントの SID を検索します。

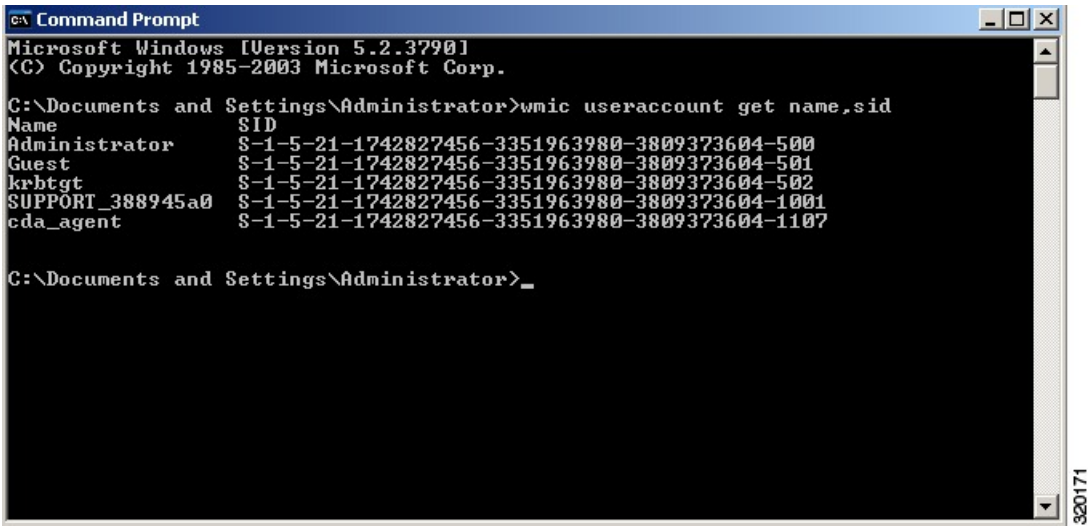
ステップ 2 すべての SID アカウントを表示するには、次の図に示すように、コマンド ラインから次のコマンドを使用します。

```
wmic useraccount get name,sid
```

特定のユーザ名とドメインに対して、次のコマンドを使用することもできます。

```
wmic useraccount where name="iseUser" get domain,name,sid
```

図 *25* : すべての *SID* アカウントの表示



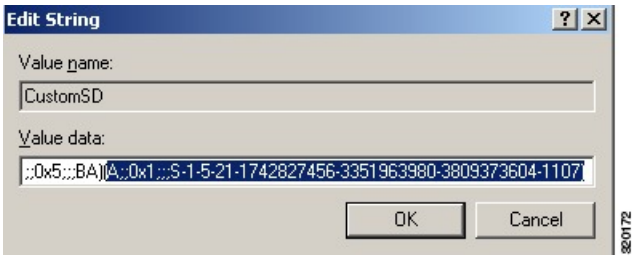
ステップ 3 SID を見つけ、レジストリ エディタを開き、次の場所を参照します。

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog
```

ステップ 4 [セキュ リティ（Security）] をクリックし、[CustomDS] をダブルクリックします。図 2 ～ 7 を参照してください。

たとえば、ise_agent アカウント（`SID : S-1-5-21-1742827456-3351963980-3809373604-1107`）への読み取りアクセスを許可するには、「`(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`」と入力します。

図 *26* : *CustomSD* 文字列の編集



ステップ 5 ドメイン コントローラ上で WMI サービスを再起動します。次の 2 とおりの方法で WMI サービスを再起動できます。

a) CLI から次のコマンドを実行します。

net stop winmgmt

net start winmgmt

b) `Services.msc` を実行します。これにより、Windows サービス管理ツールが開きます。Windows サービス管理ウィンドウで、「**Windows Management Instrumentation**」サービスを検索し、右クリックして [再起動] を選択します。

Easy Connect

Easy Connect により、セキュアな方法で有線接続されたエンドポイントからネットワークにユーザを簡単に接続し、Cisco ISE ではなく Active Directory ドメイン コントローラからユーザを認証することで、それらのユーザをモニタすることができます。Easy Connect により、ISE は Active Directory ドメイン コントローラからユーザ認証情報を収集します。Easy Connect は MS WMI インターフェイスを使用して Windows システム（Active Directory）に接続し、Windows イベント メッセージからのログにクエリを行うため、現在は Windows がインストールされているエンドポイントのみをサポートしています。Easy Connect は MAB を使用した有線接続をサポートし、これは 802.1X よりもずっと設定が容易です。802.1X とは異なり、Easy Connect と MAB では、

- サプリカントを設定する必要がありません
- PKI を設定する必要がありません
- ISE は外部サーバ（AD）がユーザを認証した後に CoA を発行します

Easy Connect は次の動作モードをサポートしています。

- 適用モード：ISE がユーザ クレデンシャルに基づいて、適用のために認証ポリシーをネットワーク デバイスにアクティブにダウンロードします。
- 可視性モード：ISE がセッション マージをパブリッシュし、情報を pxGrid に送信するために NAD デバイス センサーから受信した情報をアカウンティングします。

どちらの場合も、Active Directory（AD）で認証されたユーザは、Cisco ISE のライブ セッション ビューに表示され、サードパーティ製アプリケーションによる Cisco pxGrid インターフェイスを使用してセッションディレクトリからクエリすることができます。既知の情報としては、ユーザ名、IP アドレス、AD DC ホスト名と AD DC NetBIOS 名があります。pxGrid の詳細については、『』の「pxGrid ノード」のセクションpxGrid ノード （77 ページ）を参照してください。

Easy Connect のセットアップが完了したら、ユーザの名前または IP アドレスに基づいて特定ユーザをフィルタリングできます。たとえば IT サービスの管理者が、そのエンドポイントの標準ユーザを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して [ライブ セッション（Live Sessions）] に表示されないようにし、そのエンドポイントの標準ユーザだけが表示されるようにできます。パッシブ ID サービスをフィルタリングするには、パッシブ ID サービスのフィルタリング （688 ページ）を参照してください。

Easy Connect の制限

- MAC 認証バイパス（MAB）は Easy Connect をサポートします。MAB と 802.1X の両方を同じポートで設定できますが、各サービス用に異なる ISE ポリシーが必要です。
- 現在は MAB 接続のみがサポートされています。許可ポリシーで定義されている Easy Connect 条件によって接続が許可され、権限が付与されるため、接続についての独自の認証ポリシーは不要です。
- Easy Connect はハイ アベイラビリティ モードでサポートされます。パッシブ ID を使用して、複数のノードを定義して有効にすることができます。ISE はその後自動的に 1 つの PSN を有効にしますが、その他のノードはスタンバイ状態のままです。
- シスコのネットワーク アクセス デバイス（NAD）のみがサポートされています。
- IPv6 はサポートされていません。
- ワイヤレス接続は現在サポートされていません。
- Kerberos 認証イベントのみが追跡されるため、Easy Connect はユーザ認証のみを有効にし、マシン認証をサポートしません。

Easy Connect は ISE で設定する必要があり、Active Directory ドメイン サーバには Microsoft によって発行された指示とガイドラインに基づいた適切なパッチと設定が必要です。ISE の Active Directory ドメイン コントローラの設定については、次の項を参照してください。 Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件 （620 ページ）

Easy Connect 適用モード

Easy Connect により、ユーザは MAC アドレス バイパス（MAB）プロトコルを使用し、認証のための Active Directory（AD）にアクセスすることで、Windows オペレーティング システムを備えた有線接続されたエンドポイント（通常は PC）からセキュアなネットワークにログオンすることができます。ISE の Easy Connect は、認証されるユーザに関する情報のために Active Directory サーバからの Windows Management Instrumentation（WMI）イベントをリッスンします。AD がユーザを認証すると、ドメイン コントローラがユーザに割り当てられたユーザ名と IP アドレスを含むイベント ログを生成します。ISE が AD からログインの通知を受信し、RADIUS の認可変更（CoA）を発行します。

（注） RADIUS サービス タイプが call-check に設定されている場合、MAC アドレス ルックアップは MAB 要求のために行われません。そのため、この要求への応答は access-accept です。これは ISE のデフォルト設定です。

Easy Connect 適用モードのプロセス フロー

Easy Connect 適用モードのプロセスは次のとおりです。

1. ユーザが有線接続されたエンドポイント（PC など）から NAD に接続します。

2. （MAB 用に設定された）NAD が ISE にアクセス要求を送信します。ISE がアクセスに応答し、ユーザ設定に基づいて、ユーザに AD へのアクセスを許可します。設定では、少なくとも DNS、DHCP、AD へのアクセスを許可する必要があります。
3. ユーザがドメインにログインし、セキュリティ監査イベントが ISE に送信されます。
4. ISE は RADIUS から MAC アドレスを収集し、セキュリティ監査イベントから IP アドレス、ドメイン名、ユーザに関するアカウンティング情報（ログイン情報）を収集します。
5. ISE セッション ディレクトリですべてのデータが収集されてマージされると、（ポリシー サービス ノード（PSN）で管理されている適切なポリシーに基づいて）ISE が NAD に CoA を発行し、そのポリシーに基づいて NAD によりユーザにネットワークへのアクセスが提供されます。

図 *27 : Easy Connect* 適用モードの基本フロー

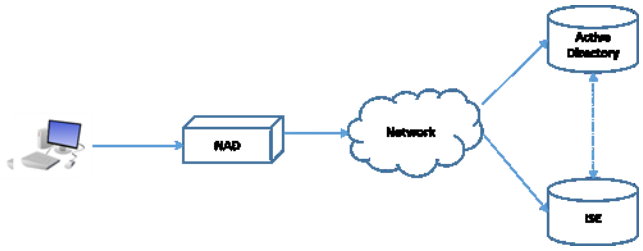
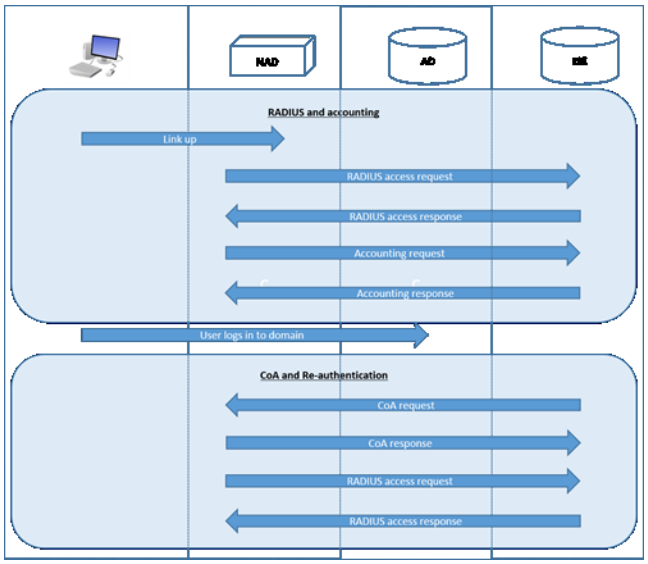


図 *28 : Easy Connect* 適用モードの詳細フロー



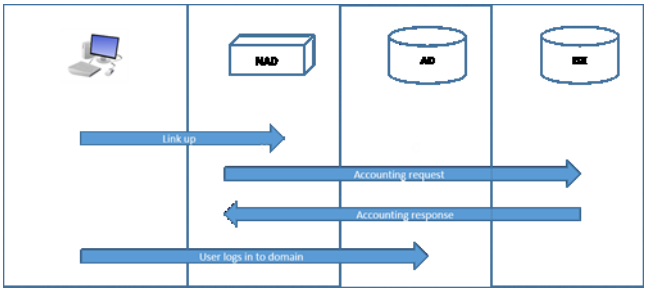
適用モードの設定の詳細については、Easy Connect 適用モードの設定 （635 ページ）を参照してください。

Easy Connect 可視性モード

可視性モードでは、ISE は RADIUS からのアカウンティング情報のみをモニタし（NAD のデバイス センサー機能の一部）、認証は行いません。Easy Connect は RADIUS アカウンティング

と WMI イベントをリッスンし、ログとレポート（およびオプションで pxGrid）にその情報をパブリッシュします。pxGrid が設定されている場合、Active Directory を使用したユーザ ログイン中に RADIUS のアカウンティング開始とセッション終了の両方が pxGrid にパブリッシュされます。

図 *29 : Easy Connect* 可視性モードのフロー



Easy Connect 可視性モードの設定の詳細については、Easy Connect 表示モードの設定 （636 ページ）を参照してください。

Easy Connect 適用モードの設定

始める前に

- 最適なパフォーマンスを得るには、WMI イベントを受け取るための専用の PSN を導入します。
- AD ログイン イベントを受け取る、WMI ノードの Active Directory ドメイン コントローラのリストを作成します。
- Active Directory からユーザ グループを取得するために ISE が参加する必要がある Microsoft ドメインを決定します。
- 認証ポリシーでリファレンスとして使用される Active Directory グループを決定します。
-
- MAB が成功した後、NAD は、（概要で説明されているように）そのポートのユーザが Active Directory サーバにアクセスできるようにする、制限付きアクセス プロファイルを提供する必要があります。

ステップ 1 （注） パッシブ ID サービスは複数のノードで有効にできますが、Easy Connect は一度に 1 つのノードでのみ操作できます。複数のノードのサービスを有効にすると、ISE はアクティブな Easy Connect セッションのために使用するノードを自動的に決定します。

Easy Connect に使用する専用ポリシー サーバ（PSN）でパッシブ ID サービスを有効にして、ISE がグループ情報とイベント情報を Active Directory から取得できるようにします。**[管理（Administration）] > [システム（System）] > [導入（Deployment）]** の順に選択してノードを開き、[全般設定（General Settings）] の下で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] を有効にします。

ステップ 2 Easy Connect が使用する Active Directory 参加ポイントとドメイン コントローラを設定します。この操作の実行方法と詳細については、Active Directory でEasy Connect およびパッシブ ID サービスをサポートするための要件 （620 ページ）を参照してください。

ステップ 3 必要に応じて、さまざまなユーザのグループ用のさまざまなポリシーを作成するために（マーケティング部門従業員と管理部門従業員のための異なるポリシーなど）、AD ドメイン コントローラ グループをマッピングします。**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** の順に選択し、使用する Active Directory を選択して [グループ（Groups）] タブを選択し、認証ポリシーで使用する Active Directory グループを追加します。
ドメイン コントローラ用にマッピングした Active Directory グループは PassiveID ディクショナリで動的に更新され、ポリシー条件ルールを設定するときに使用することができます。

ステップ 4 （注） Easy Connect プロセスが適切に実行され、ISE が有効にされて CoA が発行できるように、Easy Connect 認証に使用されるすべてのプロファイルで [パッシブ ID 追跡（Passive Identity Tracking）] を有効にする必要があります。

パッシブ ID 追跡を有効にします。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）]** の順に選択します。Easy Connect によって使用されるプロファイルについて、プロファイルを開いて [パッシブ ID 追跡（Passive Identify Tracking）] を有効にします。

ステップ 5 ポリシー ルールを作成します。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [認証（Authorization）] > [単純条件（Simple Conditions）]** の順に選択し、Easy Connect 用のルールを作成します。[追加（Add）] をクリックします。次に、条件を定義します。

a) 役立つ名前と説明を入力します。
b) [属性（Attribute）] から PassiveID ディクショナリに移動し、PassiveID_Groups を選択してドメイン コントローラ グループ用の条件を作成するか、PassiveID_user を選択して個々のユーザ用の条件を作成します。
c) 正しい操作を入力します。
d) ポリシーに含めるユーザ名またはグループ名を入力します。

ステップ 6 [送信（Submit）] をクリックします。

Easy Connect 表示モードの設定

始める前に

- 最適なパフォーマンスを得るには、WMI イベントを受け取るための専用の PSN を導入します。
- AD ログイン イベントを受け取る、WMI ノードの Active Directory ドメイン コントローラのリストを作成します。
- Active Directory からユーザ グループを取得するために ISE が参加する必要がある Microsoft ドメインを決定します。
-

ステップ 1 Easy Connect に使用する専用ポリシー サーバ（PSN）でパッシブ ID サービスを有効にして、ISE がグループ情報とイベント情報を Active Directory から取得できるようにします。**[管理（Administration）] > [システム（System）] > [導入（Deployment）]** の順に選択してノードを開き、[全般設定（General Settings）] の下で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] を有効にします。

ステップ 2 Easy Connect が使用する Active Directory 参加ポイントとドメイン コントローラを設定します。この操作の実行方法と詳細については、Active Directory でEasy Connect およびパッシブ ID サービスをサポートするための要件 （620 ページ）を参照してください。

PassiveID ワークセンター

パッシブ ID コネクタ（PassiveID ワークセンター）は一元的なワンストップ インストールおよび実装を提供します。これにより、ユーザ ID 情報を受信してさまざまなセキュリティ製品（Cisco Firepower Management Center（FMC）や Stealthwatch など）のサブスクライバと共有するように、ネットワークを容易に設定できます。パッシブ IDの完全なブローカとして、PassiveID ワークセンター はさまざまなプロバイダー ソース（Active Directory ドメイン コントローラ（AD DC）など）からユーザ ID を収集し、ユーザ ログイン情報を使用中の該当する IP アドレスにマッピングし、そのマッピング情報を、設定されているサブスクライバセキュリティ製品と共有します。

パッシブ ID について

認証、許可、およびアカウンティング（AAA）サーバを提供し、802.1X や Web 認証などのテクノロジーを使用する Cisco Identity Services Engine（ISE）で提供される標準フローは、ユーザまたはエンドポイントと直接通信し、ネットワークへのアクセスを要求し、ログインクレデンシャルを使用して ID を検証およびアクティブに認証します。

パッシブ ID サービスはユーザを直接認証するのではなく、プロバイダーと呼ばれる Active Directory などの外部認証サーバからユーザ ID および IP アドレスを収集し、サブスクライバとこの情報を共有します。まず初めに、PassiveID ワークセンターは、通常、ユーザのログインとパスワードに基づいてプロバイダーからユーザ ID 情報を受信し、ユーザ ID および関連する IP アドレスを照合するために必要な確認とサービスを実行し、認証済み IP アドレスをサブスクライバに提供します。

Passive Identity Connector（PassiveID ワークセンター）のフロー

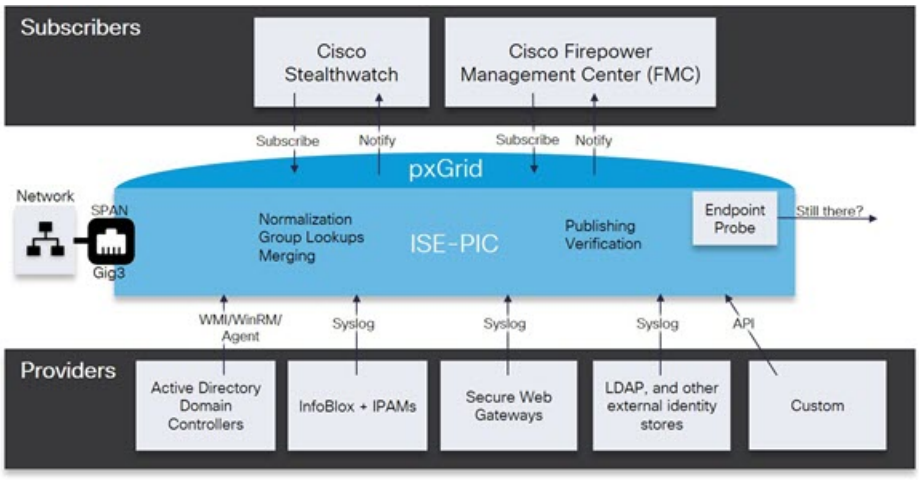
PassiveID ワークセンター のフローは次のとおり。

1. プロバイダーがユーザまたはエンドポイントの認証を実行します。
2. プロバイダーが認証済みのユーザ情報を Cisco ISE に送信します。
3. Cisco ISE によりユーザ情報の正規化、ルックアップ、マージ、解析、および IP アドレスへのマッピングが行われ、マッピングされた詳細情報が pxGrid に対して公開されます。

4. pxGrid サブスクライバはマッピングされたユーザの詳細情報を受信します。

次の図に、Cisco ISE の全体的なフローを示します。

図 *30* : 全体的なフロー



初期セットアップと設定

Cisco PassiveID ワークセンターをすぐに使用できるようにするには、次のフローに従います。

1. DNS サーバを適切に設定していることを確認します。これには、ISE からのクライアントマシンの逆引きの設定も含まれます。詳細については、DNS サーバ （593 ページ）を参照してください。
2. パッシブ ID サービスに使用する専用ポリシー サーバ（PSN）で、パッシブ ID サービスと pxGrid サービスを有効にします。**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択し、該当するノードを開き、[全般設定（General Settings）] の下の [パッシブ ID サービスの有効化（Enable Passive Identity Service）] と [pxGrid] をオンにします。
3. NTP サーバのクロック設定を同期します。
4. ISE パッシブ ID セットアップで、最初のプロバイダーを設定します。詳細については、PassiveID セットアップの使用を開始する （641 ページ）を参照してください。
5. 1 つまたは複数のサブスクライバを設定します。詳細については、サブスクライバ （691 ページ）を参照してください。

最初のプロバイダーとサブスクライバのセットアップ後は、追加のプロバイダーを容易に作成でき（を参照その他の パッシブ ID サービス プロバイダー （647 ページ））、 PassiveID ワークセンター：

- RADIUS ライブ セッション （337 ページ）

- 『』の「Cisco ISE アラーム」のセクションを参照してください。Cisco ISE アラーム （1538 ページ）

PassiveID ワークセンター ダッシュボード

Cisco PassiveID ワークセンター ダッシュボードには、効果的なモニタリングおよびトラブルシューティングに必要不可欠な、統合され、関連付けられた概要と統計データが表示されます。ダッシュボードはリアルタイムに更新されます。特に指定がない限り、ダッシュレットには過去 24 時間のアクティビティが表示されます。ダッシュボードにアクセスするには、**[ワークセンター（Work Centers）] > [PassiveID]** を選択し、左側のパネルで [ダッシュボード（Dashboard）] を選択します。Cisco PassiveID ワークセンター ダッシュボードはプライマリ管理ノード（PAN）でのみ表示できます。

[ホーム（Home）] ページには、 PassiveID ワークセンター データのビューを表示する 2 つのデフォルト ダッシュボードがあります。

- [メイン（Main）] : このビューには、線形の [メトリクス（Metrics）] ダッシュボード、チャート ダッシュレット、およびリスト ダッシュレットが表示されます。PassiveID ワークセンターでは、ダッシュレットは設定できません。使用可能なダッシュレットには次のものがあります。
  - [パッシブ ID メトリック（Passive Identity Metrics）] : [パッシブ ID メトリック（Passive Identity Metrics）] では、現在追跡中の固有のライブ セッションの総数、システムに設定されている ID プロバイダーの総数、ID データをアクティブに配信しているエージェントの総数、および現在設定されているサブスクライバの総数の概要が示されます。
  - [プロバイダー（Providers）] : プロバイダーはユーザ ID 情報を PassiveID ワークセンターに渡します。ISE プローブ(特定のソースからデータを収集するメカニズム）を設定します。プローブを介してプロバイダー ソースからの情報を受信します。たとえば、Active Directory（AD）プローブとエージェント プローブはいずれも ISE-PIC による AD からのデータ収集を支援しますが、syslog プローブは、syslog メッセージを読み取るパーサーからデータを収集します。
  - [サブスクライバ（Subscribers）] : サブスクライバは ISE に接続し、ユーザ ID 情報を取得します。
  - [OS タイプ（OS Types）] : 表示できる唯一の OS タイプは Windows です。Windows のタイプが Windows バージョン別に表示されます。プロバイダーは OS タイプを報告しませんが、ISE はこの情報を取得するため Active Directory を照会できます。ダッシュレットに表示できるエントリの最大数は 1000 です。この数を超えるエンドポイントがある場合、または Windows 以外の OS タイプを表示する場合には、ISE にアップグレードできます。
  - [アラーム（Alarms）] : ユーザ ID 関連アラーム。

プローブおよびプロバイダーとしての Active Directory

Active Directory（AD）は、ユーザ ID 情報（ユーザ名、IP アドレス、ドメイン名など）の取得元である安全性が高く正確なソースです。

AD プローブ（パッシブ ID サービス）は、WMI テクノロジーを使用して AD からユーザ ID 情報を収集しますが、その他のプローブはその他のテクノロジーや手法で AD をユーザ ID プロバイダーとして使用します。ISE が提供するその他のプローブとプロバイダータイプの詳細については、その他の パッシブ ID サービス プロバイダー （647 ページ）を参照してください。

Active Directory プローブを設定すると、次の（ソースとして Active Directory を使用する）その他のプローブも迅速に設定して有効にできます。

- エージェント：Active Directory エージェント （650 ページ）

（注） Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。

- SPAN：SPAN （661 ページ）
- エンドポイント プローブ：エンドポイント プローブ （688 ページ）

また、ユーザ情報の収集時に AD ユーザ グループを使用するために Active Directory プローブを設定します。AD、エージェント、SPAN、および syslog プローブで AD ユーザ グループを使用できます。AD グループの詳細については、Active Directory ユーザ グループの設定 （603 ページ）を参照してください。

Active Directory（WMI）プローブのセットアップ

パッシブ ID サービス向けに Active Directory と WMI を設定するには、[パッシブIDワークセンターウィザード（Passive ID Work Center Wizard）]（PassiveID セットアップの使用を開始する（641 ページ）を参照）を使用するか、または次の手順に従います（追加情報についてはActive Directory でEasy Connect およびパッシブ ID サービスをサポートするための要件 （620 ページ）を参照）。

1. Active Directory プローブを設定します。Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （594 ページ）を参照してください。
2. AD ログイン イベントを受信する 1 つ以上の WMI 設定ノードの Active Directory ドメイン コントローラのリストを作成します。ドメイン コントローラの追加 （596 ページ）を参照してください。
3. Active Directory を ISE と統合するため Active Directory を設定します。パッシブ ID 用の WMI の設定 （597 ページ）を参照してください。
4. （オプション）Active Directory プロバイダーの管理 （643 ページ）。

PassiveID セットアップの使用を開始する

ISE-PIC には、Active Directory からユーザ ID を受信するために、Active Directory を最初のユーザ ID プロバイダーとして容易に設定できるウィザードがあります。ISE-PIC に Active Directory を設定することで、後でその他のプロバイダータイプを設定するプロセスも簡素化されます。Active Directory を設定したら、ユーザ データを受信するクライアントを定義するため、サブスクライバ（Cisco Firepower Management Center（FMC）や Stealthwatch など）を設定する必要があります。サブスクライバの詳細については、サブスクライバ（691 ページ）を参照してください。

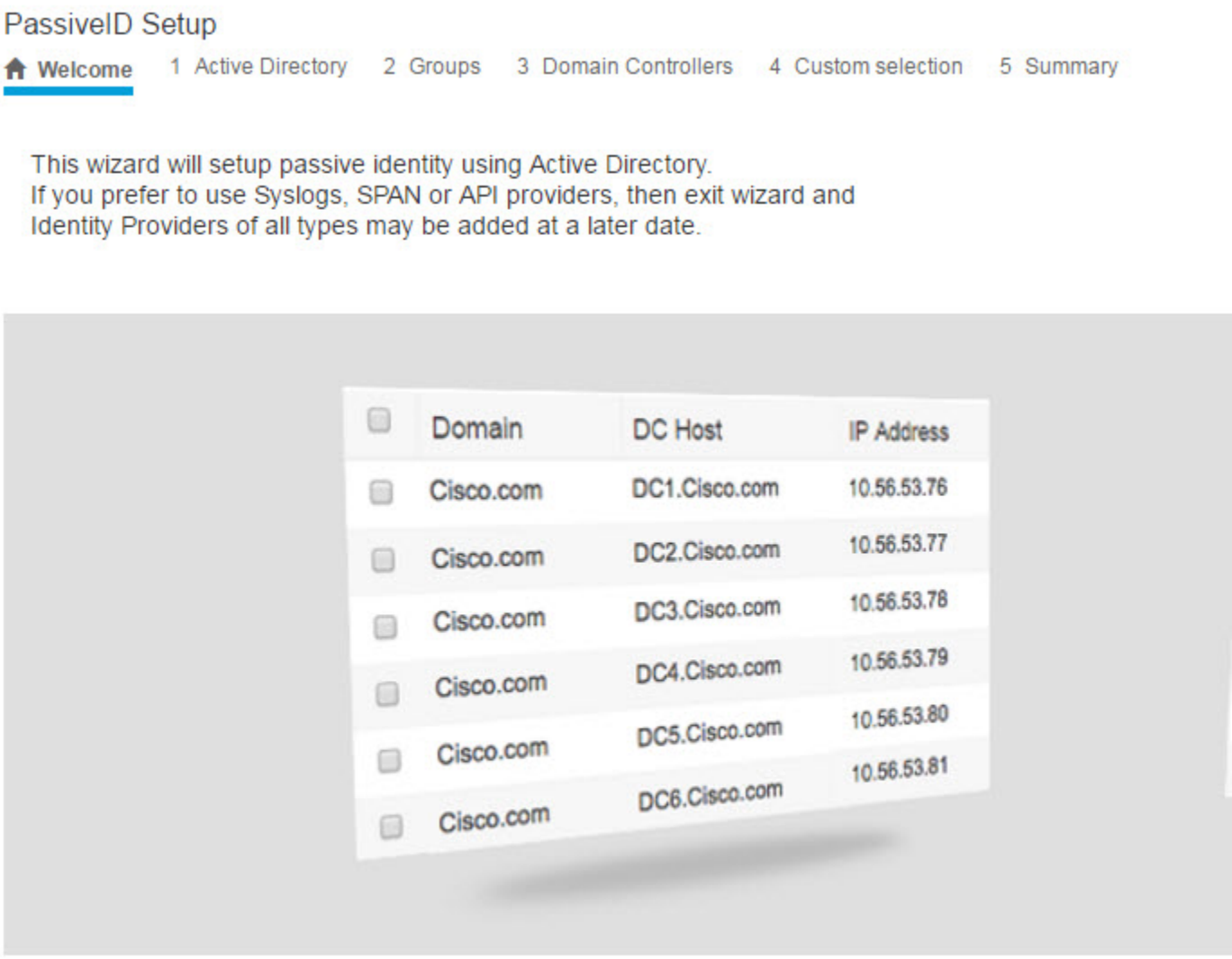
始める前に

- Microsoft Active Directory サーバがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないことを確認します。
- 参加操作用の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更（Change Password on Next Login）] を使用して設定されていないことを確認します。
- ISE でのスーパー管理者またはシステム管理者の権限があることを確認します。
- パッシブ ID サービスに使用する専用ポリシー サーバ（PSN）で、パッシブ ID サービスと pxGrid サービスを有効にします。**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択し、該当するノードを開き、[全般設定（General Settings）] の下の [パッシブ ID サービスの有効化（Enable Passive Identity Service）] と [pxGrid] をオンにします。
- ISE のエントリがドメイン ネーム サーバ（DNS）にあることを確認します。ISE からのクライアント マシンの逆引き参照を適切に設定していることを確認します。詳細については、DNS サーバ （593 ページ）を参照してください。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** を選択します。[パッシブ ID コネクタの概要（Passive Identity Connector Overview）] 画面で [パッシブ ID ウィザード（Passive Identity Wizard）] をクリックします。

[PassiveID セットアップ（PassiveID Setup）] が表示されます。

図 *31 : [PassiveID* セットアップ（*PassiveID Setup*）*]*



ステップ 2 [次へ（Next）] をクリックしてウィザードを開始します。

ステップ 3 [Active Directory] ステップで、設定されているこの Active Directory 参加ポイントを容易に区別できる一意の名前を [参加ポイント名（Join Point Name）] に入力し、Active Directory ドメインから、このノードが接続している Active Directory ドメインのドメイン名を入力し、Active Directory 管理者ユーザの名前とパスワードを入力します。Active Directory のこの設定とその他の設定の詳細については、Active Directory の設定 （643 ページ）を参照してください。

[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザ名とパスワードが保存され、モニタ対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。

ステップ 4 [次へ（Next）] をクリックし、Active Directory グループを定義し、追加してモニタするユーザ グループをすべてオンにします。
前のステップで設定した Active Directory 参加ポイントに基づいて Active Directory ユーザ グループが自動的に表示されます。

ステップ 5 [次へ（Next）] を再度クリックして、[ドメイン コントローラ（Domain Controllers）] ステップに進みます。[ドメイン コントローラ（Domain Controllers）] ステップから、モニタ対象 DC を選択します。[カスタム（Custom）] を選択した場合は、次の画面でモニタする特定の DC を選択します。完了したら、[次へ（Next）] をクリックします。
特定の DC を選択したら、最初の Active Directory プロバイダーの作成は完了です。サマリー画面に、選択した DC とその詳細が表示されます。

ステップ 6 [終了（Exit）] をクリックして、ウィザードを終了します。

次のタスク

最初のプロバイダーとして Active Directory の設定を完了したら、追加のプロバイダー タイプも容易に設定できます。詳細については、を参照してくださいその他の パッシブ ID サービス プロバイダー（647ページ）。さらに、定義したいずれかのプロバイダーが収集したユーザ ID 情報を受信するためのサブスクライバも設定できるようになりました。詳細については、サブスクライバ （691 ページ）を参照してください。

Active Directory プロバイダーの管理

Active Directory 参加ポイントの作成と設定が完了したら、次の作業を行い Active Directory プローブを管理します。

- Active Directory 認証のためのユーザのテスト （612 ページ）
- ノードの Active Directory の参加の表示 （613 ページ）
- Active Directory の問題の診断 （614 ページ）
- Active Directory ドメインの脱退 （601 ページ）
- Active Directory の設定の削除 （613 ページ）
- Active Directory デバッグ ログの有効化 （615 ページ）

Active Directory の設定

Active Directory（AD）は、安全性が高く正確なソースであり、ここからユーザ情報（ユーザ名、IP アドレスなど）が取得されます。

参加ポイントを作成、編集することで Active Directory プローブを作成、管理するには、**[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [Active Directory] を選択します。

詳細については、Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （594 ページ）を参照してください。

表 *58 : Active Directory* 参加ポイント名の設定と *[ドメインへの参加（Join Domain）]* 画面

フィールド	説明
参加ポイント名（Join Point Name）	設定したこの参加ポイントを容易に区別できる一意の名前。
Active Directory ドメイン（Active Directory Domain）	このノードが接続している Active Directory ドメインのドメイン名。
ドメイン管理者（Domain Administrator）	管理者権限を持つ Active Directory ユーザのユーザ プリンシパル名またはユーザ アカウント名。
パスワード（Password）	Active Directory で設定されているドメイン管理者のパスワード。
組織単位の指定（Specifiy Organizational Unit）	管理者の組織単位の情報を入力します。
クレデンシャルの保存（Store Credentials）	[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザ名とパスワードが保存され、モニタ対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。 エンドポイント プローブの場合は、[クレデンシャルの保存（Store Credentials）] を選択する必要があります。

表 *59 : [Active Directory* 参加/脱退（*Active Directory Join/Leave*）*]* テーブル

フィールド	説明
ISE ノード（ISE Node）	インストール環境での特定のノードの URL。
ISE ノードのロール（ISE Node Role）	インストール環境でそのノードがプライマリ ノードまたはセカンダリ ノードのいずれであるかを指定します。
ステータス	ノードが Active Directory ドメインにアクティブに参加しているかどうかを示します。

フィールド	説明
ドメイン コントローラ	Active Directory に参加しているノードの場合、この列には Active Directory ドメインでノードが接続している特定のドメイン コントローラが示されます。
サイト	Active Directory フォレストが ISE に参加する場合、このフィールドには、[Active Directory サイトおよびサービス（Active Directory Sites & Services）] 領域に示されるフォレスト内の特定の Active Directory サイトが示されます。

[プロバイダー（Providers）] > [Active Directory] > [PassiveID] を選択します。

表 *60 : [パッシブ ID ドメイン コントローラ（DC）（Passive ID Domain Controllers (DC)）] リスト*

フィールド	説明
ドメイン	ドメイン コントローラが存在しているサーバの完全修飾ドメイン名。
DC ホスト	ドメインコントローラが存在しているホスト。
サイト	Active Directory フォレストが ISE に参加する場合、このフィールドには、[Active Directory サイトおよびサービス（Active Directory Sites & Services）] 領域に示されるフォレスト内の特定の Active Directory サイトが示されます。
IP アドレス	ドメイン コントローラの IP アドレス。
モニタ方法	次のいずれかの方法で、ユーザ ID 情報を取得するため Active Directory ドメイン コントローラをモニタします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニタします。 • [エージェント名（Agent name）]：ユーザ情報を取得するために Active Directory をモニタするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウン リストから使用するエージェントを選択します。エージェントの詳細については、Active Directory エージェント（650 ページ） を参照してください。

[プロバイダー（Providers）] > **[Active Directory]** > **[PassiveID]** を選択します。編集する AD 参加ポイントのリンクをクリックし、[PassiveID] タブに移動して [編集（Edit）] をクリックし、リストから既存のドメイン コントローラを編集します。

表 *61 : [パッシブ ID ドメイン コントローラ（DC）（Passive ID Domain Controllers (DC)）] 編集画面*

フィールド	説明
ホスト FQDN	ドメイン コントローラが存在しているサーバの完全修飾ドメイン名を入力します。
説明	このドメイン コントローラを容易に特定できるように、一意の説明を入力します。
ユーザ名	Active Directory にアクセスするための管理者のユーザ名。
パスワード	Active Directory にアクセスするための管理者のパスワード。
プロトコル	次のいずれかの方法で、ユーザ ID 情報を取得するため Active Directory ドメイン コントローラをモニタします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニタします。 • [エージェント名（Agent name）]：ユーザ情報を取得するために Active Directory をモニタするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウン リストから使用するエージェントを選択します。エージェントの詳細については、Active Directory エージェント （650 ページ） を参照してください。

表 *62 : Active Directory グループ*

説明
Active Directory グループは Active Directory から定義および管理されます。このノードに参加している Active Directory のグループは、このタブで確認できます。Active Directory の詳細については、https://msdn.microsoft.com/en-us/library/bb742437.aspx を参照してください。

表 *63 : Active Directory* の詳細設定

フィールド	説明
履歴期間（History interval）	すでに発生したユーザ ログインの情報をパッシブ ID サービスが読み取る期間。これは、パッシブ ID サービスの起動時または再起動時に、このサービスが使用不可であった間に生成されたイベントを確認するために必要となります。エンドポイント プローブがアクティブな場合、この期間の頻度が維持されます。
ユーザ セッションのエージング タイム（User session aging time）	ユーザがログインできる時間です。パッシブ ID サービスでは、DC からの新しいユーザ ログイン イベントが識別されますが、DC はユーザがログオフする時点を報告しません。エージング タイムを使用すると、Cisco ISE で、ユーザがログインする時間間隔を決定できます。
NTLM プロトコル設定（NTLM Protocol settings）	Cisco ISE と DC の間の通信プロトコルとして [NTLMv1] または [NTLMv2] を選択できます。推奨されるデフォルトは [NTLMv2] です。

その他の パッシブ ID サービス プロバイダー

ISE が ID 情報（パッシブ ID サービス）を、サービスをサブスクライブするコンシューマ（サブスクライバ）に提供できるようにするため、最初に ISE プローブを設定する必要があります。このプローブは ID プロバイダーに接続します。

次の表に、ISE から使用可能なプロバイダーとプローブのすべてのタイプについて詳しく説明します。この章の残りの部分では、Active Directory 以外で使用できるすべてのタイプについて説明していますが、Active Directory で使用できるタイプについては、専用の章で詳しく説明します。詳細については、プローブおよびプロバイダーとしての Active Directory （640 ページ）を参照してください。

定義できるプロバイダー タイプを次に示します。

表 *64 :* プロバイダー タイプ

プロバイダータイプ（プローブ）	説明	送信元システム（プロバイダー）	テクノロジー	収集されるユーザ ID 情報	ドキュメント リンク
Active Directory（AD）	ユーザ情報の取得元である安全性が高く正確で最も一般的なソース。 プローブとして機能する場合、AD は WMI テクノロジーを使用して認証済みユーザ ID を送信します。 また AD 自体が、プローブではなく、その他のプローブがユーザデータを取得するソース システム（プロバイダー）として機能します。	Active Directory ドメイン コントローラ	WMI	• ユーザ名（User name） • IP アドレス • ドメイン	プローブおよびプロバイダーとしての Active Directory （640 ページ）
エージェント（Agents）	Active Directory ドメイン コントローラまたはメンバー サーバにインストールされているネイティブ 32 ビット アプリケーション。エージェント プローブは、ユーザ ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。		ドメインコントローラまたはメンバーサーバにインストールされているエージェント。	• ユーザ名（User name） • IP アドレス • ドメイン	Active Directory エージェント （650 ページ） （注） Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。

プロバイダータイプ（プローブ）	説明	送信元システム（プロバイダー）	テクノロジー	収集されるユーザ ID 情報	ドキュメント リンク
エンドポイント（Endpoint）	設定されているその他のプローブに加えて、ユーザが接続しているかどうかを確認するため、常にバックグラウンドで実行されます。		WMI	ユーザが接続しているかどうか	エンドポイント プローブ （688 ページ）
SPAN	ネットワーク トラフィックをリッスンし、Active Directory データに基づいてユーザ ID 情報を抽出するため、ネットワーク スイッチに導入されています。		SPAN（スイッチにインストール）と Kerberos メッセージ	• ユーザ名（User name） • IP アドレス • ドメイン	SPAN （661 ページ）
API プロバイダー	ISE が提供する RESTful API サービスを使用して、RESTful API クライアントと通信するようにプログラミングされている任意のシステムから、ユーザ ID 情報を収集します。	REST API クライアントと通信するようにプログラミングされている任意のシステム。	RESTful API。JSON 形式でサブスクライバに送信されるユーザ ID。	• ユーザ名（User name） • IP アドレス • ポート範囲（Port range） • ドメイン（Domain）	API プロバイダー （655 ページ）

プロバイダータイプ（プローブ）	説明	送信元システム（プロバイダー）	テクノロジー	収集されるユーザ ID 情報	ドキュメント リンク
Syslog	syslog メッセージを解析し、ユーザ ID（MAC アドレスを含む）を取得します。	• 標準 syslog メッセージ プロバイダー • DHCP サーバ	syslog メッセージ	• ユーザ名（User name） • IP アドレス • MAC アドレス • ドメイン	syslog プロバイダー（663 ページ）

Active Directory エージェント

パッシブ ID サービス ワーク センターから、ネイティブ 32 ビット アプリケーション、ドメイン コントローラ（DC）エージェントを、（設定に応じて）Active Directory（AD）ドメイン コントローラ（DC）またはメンバー サーバ上の任意の場所にインストールし、AD からユーザ ID 情報を取得して、設定したサブスクライバにこれらの ID を送信します。エージェント プローブは、ユーザ ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。エージェントは個別のドメインまたは AD ドメインにインストールできます。インストールされたエージェントは、1 分ごとに ISE にステータス更新情報を提供します。

エージェントは ISE が自動的にインストールおよび設定するか、またはユーザが手動でインストールすることができます。インストールが完了すると、次のようになります。

- エージェントとその関連ファイルはパス **Program Files/Cisco/Cisco ISE PassiveID Agent** にインストールされています。
- エージェントのロギング レベルを指定する **PICAgent.exe.config** という設定ファイルがインストールされます。この設定ファイル内でロギング レベルを手動で変更できます。
- CiscoISEPICAgent.log ファイルにはすべてのロギング メッセージが保存されます。
- nodes.txt ファイルには、展開内でエージェントが通信できるすべてのノードのリストが含まれています。エージェントはリストの最初のノードと通信します。このノードと通信できない場合、エージェントはリストのノード順序に従ってノードとの通信を試行します。手動でのインストールの場合、このファイルを開き、ノード IP アドレスを入力する必要があります。（手動または自動での）インストールの完了後にこのファイルを変更するには、このファイルを手動で更新する必要があります。ファイルを開き、ノード IP アドレスを必要に応じて追加、変更、または削除します。
- Cisco ISE PassiveID Agent サービスはマシン上で稼働します。このサービスは [Windows サービス（Windows Services）] ダイアログボックスから管理できます。

- ISE は最大 100 個のドメイン コントローラをサポートでき、それぞれのエージェントは最大 10 個のドメイン コントローラをモニタできます。

（注） 100 個のドメイン コントローラをモニタするには、10 個のエージェントを設定する必要があります。

（注） Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。

エージェントをインストールできない場合、パッシブ ID サービスには Active Directory プローブを使用します。詳細については、プローブおよびプロバイダーとしての Active Directory （640 ページ）を参照してください。

Active Directory エージェントの自動インストールおよび展開

ユーザ ID についてドメイン コントローラをモニタするようにエージェント プロバイダーを設定するときには、エージェントがメンバー サーバまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE が自動的にインストールするか、またはユーザが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニタするように設定する必要があります。このプロセスでは、自動インストールを有効にし、ドメイン コントローラをモニタするようにエージェントを設定する方法について説明します。

始める前に

始める前に：

- サーバ側からの関連 DNS サーバの逆引き参照を設定します。ISE の DNS サーバ設定要件の詳細については、DNS サーバ （593 ページ）を参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/framework を参照してください。
- アクティブなパッシブ ID および pxGrid サービス。詳細については、初期セットアップと設定 （638 ページ）を参照してください。
- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダーとしての Active Directory （640 ページ）を参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザ グループを使用します。AD グループの詳細については、Active Directory ユーザ グループの設定 （603 ページ）を参照してください。

ステップ 1 現在設定されているすべてのドメイン コントローラ（DC）エージェントを表示し、既存のエージェントを編集、削除し、新しいエージェントを設定するには、**[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [エージェント（Agents）] を選択します。

ステップ 2 新しいエージェントを追加するには、テーブルの上部で [追加（Add）] をクリックします。既存のクライアントを編集または変更するには、テーブルでエージェントをオンにし、テーブル上部で [編集（Edit）] をクリックします。

ステップ 3 新しいエージェントを作成し、この設定で指定するホストに自動的にインストールするには、[新規エージェントの展開（Deploy New Agent）] を選択します。

ステップ 4 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、Active Directory エージェントの設定 （654 ページ）を参照してください。

ステップ 5 [展開（Deploy）] をクリックします。
設定で指定したドメインに基づいてエージェントが自動的にホストにインストールされ、設定が保存されます。エージェントは [エージェント（Agents）] テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 6 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [Active Directory] を選択して、現在設定されているすべての参加ポイントを表示します。

ステップ 7 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 8 前提条件の一部として追加したドメイン コントローラを使用するため、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 9 作成したエージェントを使用してモニタするドメイン コントローラをオンにし、[編集（Edit）] をクリックします。

ステップ 10 表示されるダイアログボックスで、必須フィールドに値が入力されていることを確認し、[プロトコル（Protocol）] ドロップダウンから [エージェント（Agent）] を選択します。表示される [エージェント（Agent）] フィールドのドロップダウンリストから、作成したエージェントを選択します。エージェントのユーザ名およびパスワードのクレデンシャルを作成している場合は、このクレデンシャルを入力して [保存（Save）] をクリックします。
ドメイン コントローラに対してエージェントが有効になり、ダイアログボックスが閉じます。

Active Directory エージェントの手動インストールおよび展開

ユーザ ID についてドメイン コントローラをモニタするようにエージェント プロバイダーを設定するときには、エージェントがメンバー サーバまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE が自動的にインストールするか、またはユーザが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニタするように設定する必要があります。このプロセスでは、エージェントを手動でインストールし、ドメイン コントローラをモニタするように設定する方法について説明します。

始める前に

始める前に：

- サーバ側からの関連 DNS サーバの逆引き参照を設定します。ISE の DNS サーバ設定要件の詳細については、DNS サーバ （593 ページ）を参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/framework を参照してください。
- アクティブなパッシブ ID および pxGrid サービス。詳細については、初期セットアップと設定 （638 ページ）を参照してください。
- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダーとしての Active Directory （640 ページ）を参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザ グループを使用します。AD グループの詳細については、Active Directory ユーザ グループの設定 （603 ページ）を参照してください。

ステップ 1 現在設定されているすべてのドメイン コントローラ（DC）エージェントを表示し、既存のエージェントを編集、削除し、新しいエージェントを設定するには、**[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [エージェント（Agents）] を選択します。

ステップ 2 [エージェントのダウンロード（Download Agent）] をクリックし、手動でインストールするための **picagent-installer.zip** ファイルをダウンロードします。
このファイルは Windows の標準ダウンロード フォルダにダウンロードされます。

ステップ 3 ZIP ファイルを指定のホスト マシンに保存してインストールを実行します。

ステップ 4 ISE GUI から **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** をもう一度選択し、左側のパネルから [エージェント（Agents）] を選択します。

ステップ 5 新しいエージェントを設定するには、テーブルの上部で [追加（Add）] をクリックします。既存のクライアントを編集または変更するには、テーブルでエージェントをオンにし、テーブル上部で [編集（Edit）] をクリックします。

ステップ 6 すでにホストマシンにインストールしているエージェントを設定するには、[既存のエージェントの登録（Register Existing Agent）] を選択します。

ステップ 7 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、Active Directory エージェントの設定 （654 ページ）を参照してください。

ステップ 8 [Save] をクリックします。
エージェント設定が保存されます。エージェントは [エージェント（Agents）] テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 9 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [Active Directory] を選択して、現在設定されているすべての参加ポイントを表示します。

ステップ 10 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 11 前提条件の一部として追加したドメイン コントローラを使用するため、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 12 作成したエージェントを使用してモニタするドメイン コントローラをオンにし、[編集（Edit）] をクリックします。

ステップ 13 表示されるダイアログボックスで、必須フィールドに値が入力されていることを確認し、[プロトコル（Protocol）] ドロップダウンから [エージェント（Agent）] を選択します。表示される [エージェント（Agent）] フィールドのドロップダウンリストから、作成したエージェントを選択します。エージェントのユーザ名およびパスワードのクレデンシャルを作成している場合は、このクレデンシャルを入力して [保存（Save）] をクリックします。
ドメイン コントローラに対してエージェントが有効になり、ダイアログボックスが閉じます。

エージェントのアンインストール

自動または手動でインストールされたエージェントは、Windows から直接（手動で）簡単にアンインストールできます。

ステップ 1 [Windows] ダイアログで [プログラムと機能（Programs and Features）] に移動します。

ステップ 2 インストールされているプログラムのリストで [Cisco ISE PassiveID エージェント（Cisco ISE PassiveID Agent）] を見つけて選択します。

ステップ 3 [アンインストール（Uninstall）] をクリックします。

Active Directory エージェントの設定

ISE が、さまざまなドメイン コントローラ（DC）からユーザ ID 情報を取得し、その情報をパッシブ ID サービス サブスクライバに配信するために、ネットワーク内の指定されたホストにエージェントを自動的にインストールすることを許可します。

エージェントを作成および管理するには、**[プロバイダー（Providers）]** > **[エージェント（Agents）]** を選択します。Active Directory エージェントの自動インストールおよび展開 （651 ページ）を参照してください。

[エージェント（Agents）] テーブルで現在のエージェントのステータスを確認します。**[プロバイダー（Providers）]** > **[エージェント（Agents）]** を選択します。

表 65 : [エージェント（Agents）] テーブル

フィールド	説明
名前（Name）	設定したエージェント名。
ホスト（Host）	エージェントがインストールされているホストの完全修飾ドメイン名。
モニタリング（Monitoring）	指定されたエージェントがモニタするドメイン コントローラのカンマ区切りリストです。

表 *66 :* 新規エージェント（*Agents New*）

フィールド	説明
新規エージェントの展開（Deploy New Agent）または既存のエージェントの登録（Register Existing Agent）	• 新規エージェントの展開（Deploy New Agent）：指定されたホストに新規エージェントをインストールします。 • 既存のエージェントの登録（Register Existing Agent）：ホストにエージェントを手動でインストールし、 パッシブ ID サービス がサービスを有効にできるようにするため、この画面でそのエージェントを設定します。
名前（Name）	エージェントを容易に把握できる名前を入力します。
説明（Description）	エージェントを容易に把握できる説明を入力します。
ホスト FQDN（Host FQDN）	エージェントがインストールされているホスト(既存のエージェントの登録の場合）またはインストールされるホスト（自動展開の場合）の完全修飾ドメイン名です。
ユーザ名 （User Name）	エージェントをインストールするホストにアクセスするためのユーザ名を入力します。パッシブ ID サービスは、これらのクレデンシャルを使用してエージェントをインストールします。
パスワード（Password）	エージェントをインストールするホストにアクセスするためのユーザ パスワードを入力します。 パッシブ ID サービスは、これらのクレデンシャルを使用してエージェントをインストールします。

API プロバイダー

Cisco ISE の API プロバイダー機能では、カスタマイズしたプログラムまたはターミナル サーバ（TS）エージェントから組み込み ISE パッシブ ID サービス REST API サービスにユーザ ID 情報をプッシュできます。これにより、ネットワークからプログラミング可能なクライアントをカスタマイズして、任意のネットワーク アクセス制御（NAC）システムから収集されたユーザ ID をこのサービスに送信するようにできます。さらに Cisco ISE API プロバイダーにより、すべてのユーザの IP アドレスが同一であるが、各ユーザに固有のポートが割り当てられるネットワーク アプリケーション（Citrix サーバの TS-Agent など）と対話できます。

たとえば、Active Directory（AD）サーバに対して認証されたユーザの ID マッピングを提供する Citrix サーバで稼働するエージェントは、新しいユーザがログインまたはログオフするたびに、ユーザ セッションを追加または削除する REST 要求を ISE に送信できます。ISE は、クライアントから送信されたユーザ ID 情報（IP アドレス、割り当てられたポートなど）を取得し、事前に設定されているサブスクライバ（Cisco Firepower Management Center（FMC）など）に送信します。

ISE REST API フレームワークは、HTTPS プロトコルを介した REST サービスを実装し（クライアント証明書の検証は不要）、ユーザ ID 情報が JSON（JavaScript Object Notation）形式で送信されます。JSON の詳細については、http://www.json.org/ を参照してください。

ISE REST API サービスは、1 つのシステムに同時にログインしている複数のユーザを区別するため、ユーザ ID を解析し、その情報をポート範囲にマッピングします。ポートがユーザに割り当てられるたびに、API がメッセージを ISE に送信します。

REST API プロバイダーのフロー

カスタマイズしたクライアントを ISE のプロバイダーとして宣言し、そのカスタマイズしたプログラム（クライアント）が RESTful 要求を送信できるようにして、ISE からカスタマイズした クライアントへのブリッジを設定している場合、ISE REST サービスは次のように機能します。

1. ISE はクライアント認証のために認証トークンを必要とします。通信開始時と、ISE から以前のトークンの期限が切れたことが通知されるたびに、クライアント マシンのカスタマイズしたプログラムから認証トークンを求める要求が送信されます。この要求への応答としてトークンが返されます。これによりクライアントと ISE サービス間の継続的な通信が可能になります。
2. ユーザがネットワークにログインすると、クライアントはユーザ ID 情報を取得し、API Add コマンドを使用してこの情報を ISE REST サービスに送信します。
3. ISE はユーザ ID 情報を受信してマッピングします。
4. ISE はマッピングされたユーザ ID 情報をサブスクライバに送信します。
5. 必要な場合は常に、カスタマイズされたマシンはユーザ情報削除要求を送信できます。このためには、Remove API コールを送信し、Add コールの送信時に応答として受信したユーザ ID を含めます。

ISE での REST API プロバイダーの操作

ISE で REST サービスをアクティブにするには、次の手順に従います。

1. クライアント側を設定します。詳細については、クライアント ユーザ マニュアルを参照してください。
2. パッシブ ID サービスと pxGrid サービスをアクティブにします。詳細については、初期セットアップと設定 （638 ページ）を参照してください。

3. DNS サーバを適切に設定していることを確認します。これには、ISE からのクライアントマシンの逆引きの設定も含まれます。 の DNS サーバ設定要件の詳細については、DNS サーバ （593 ページ）を参照してください。
4. パッシブ ID サービス の ISE REST サービスへのブリッジの設定 （657 ページ）を参照してください。

（注） TS-Agent と連携するように API プロバイダーを設定するには、ISE からそのエージェントへのブリッジの作成時に TS-Agent 情報を追加します。その後、TS-Agent のマニュアルで API コールの送信について確認してください。

5. 認証トークンを生成し、追加要求と削除要求を API サービスに送信します。#unique_699。

パッシブ ID サービス の ISE REST サービスへのブリッジの設定

ISE REST API サービスが特定のクライアントから情報を受信できるようにするには、まず ISE でその特定のクライアントを定義する必要があります。異なる IP アドレスを使用して複数の REST API クライアントを定義できます。

始める前に

始める前に：

- パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。詳細については、初期セットアップと設定 （638 ページ）を参照してください。
- DNS サーバを適切に設定していることを確認します。これには、ISE からのクライアントマシンの逆引きの設定も含まれます。ISE の DNS サーバ設定要件の詳細については、DNS サーバ （593 ページ）を参照してください。

ステップ 1 現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定するには、**[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [API プロバイダー（API Providers）] を選択します。
[API プロバイダー（API Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しいクライアントを追加するには、テーブルの上部で [追加（Add）] をクリックします。既存のクライアントを編集または変更するには、テーブルでクライアントをオンにし、テーブル上部で [編集（Edit）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、API プロバイダーの設定 （658 ページ）を参照してください。

ステップ 4 [送信（Submit）] をクリックします。

クライアント設定が保存され、更新された [API プロバイダー（API Providers）] テーブルが画面に表示されます。これで、クライアントは ISE REST サービスにポストを送信できるようになりました。

次のタスク

認証トークンとユーザ ID を ISE REST サービスに送信するように、カスタマイズしたクライアントをセットアップします。パッシブ ID REST サービスへの API コールの送信 （658 ページ）を参照してください。

パッシブ ID REST サービスへの API コールの送信

始める前に

パッシブ ID サービス の ISE REST サービスへのブリッジの設定 （657 ページ）

ステップ 1 Cisco ISE URL をブラウザのアドレス バーに入力します（たとえば *https://<ise hostname or ip address>/admin/*）。

ステップ 2 .ISE GUI の [APIプロバイダー（API Providers）] 画面で指定および設定したユーザ名とパスワードを入力します。詳細については、パッシブ ID サービス の ISE REST サービスへのブリッジの設定 （657 ページ）を参照してください。

ステップ 3 Enter キーを押します。

ステップ 4 ターゲット ノードの [URL アドレス（URL Address）] フィールドに API コールを入力します。

ステップ 5 [送信（Send）] をクリックして API コールを発行します。

次のタスク

さまざまな API コールとそのスキーマおよび結果の詳細については、API コール （659 ページ）を参照してください。

API プロバイダーの設定

[プロバイダー（Providers）] > [API プロバイダー（Providers）] を選択して、の新しい REST API クライアントを設定します。

（注） 次のようにリクエスト コールを使用して完全な API 定義とオブジェクト スキーマを取得できます。

- 完全な API の指定（wadl）：https://YOUR_ISE:9094/application.wadl
- API モデルとオブジェクト スキーマ：https://YOUR_ISE:9094/application.wadl/xsd0.xsd

表 *67 : API* プロバイダーの設定

フィールド	説明
名前（Name）	このクライアントを他のクライアントから容易に区別できる一意の名前を入力します。
説明（Description）	このクライアントのわかりやすい説明を入力します。
ステータス	設定完了後すぐにクライアントが REST サービスとやりとりできるようにするには、[有効（Enabled）] を選択します。
ホスト/IP（Host/ IP）	クライアント ホスト マシンの IP アドレスを入力します。DNS サーバを適切に設定していることを確認します。これには、ISE からのクライアント マシンの逆引きの設定も含まれます。
ユーザ名（User name）	REST サービスへの送信時に使用する一意のユーザ名を作成します。
パスワード（Password）	REST サービスへの送信時に使用する一意のパスワードを作成します。

API コール

Cisco ISE で パッシブ ID サービスのユーザ ID イベントを管理するには、次の API コールを使用します。

目的：認証トークンの生成

- **要求**

  POST

  https://<PIC IP アドレス>:9094/api/fmi_platform/v1/identityauth/generatetoken

  この要求には BasicAuth 許可ヘッダーが含まれている必要があります。ISE-PIC GUI で以前に作成した API プロバイダーのクレデンシャルを提供します。詳細については、API プロバイダーの設定 （658 ページ）を参照してください。

- **応答ヘッダー**

  このヘッダーには X-auth-access-token が含まれています。これは、追加の REST 要求を送信するときに使用するトークンです。

- **応答本文**

  HTTP 204 No Content

目的：ユーザの追加

- 要求

  POST

  https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity

  POST 要求のヘッダーに X-auth-access-token を追加します。（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）

- 応答ヘッダー

  201 Created

- 応答本文

  {

  "user": "<ユーザ名>",

  "srcPatRange": {

  "userPatStart": <ユーザ PAT 開始値>,

  "userPatEnd": <ユーザ PAT 終了値>,

  "patRangeStart": <PAT 範囲開始値>

  },

  "srcIpAddress": "<src IP アドレス>",

  "agentInfo": "<エージェント名>",

  "timestamp": "<ISO_8601 形式、例：“YYYY-MM-DDTHH:MM:SSZ" >",

  "domain": "<ドメイン>"

  }

- 注記

  - 上記の JSON で 1 つの IP ユーザ バインディングを作成するには srcPatRange を削除します。
  - 応答本文には「ID」（作成されたユーザ セッション バインディングの固有識別子）が含まれています。削除するユーザを指定する DELETE 要求を送信するときに、この ID を使用してください。
  - この応答には、新たに作成されたユーザ セッション バインディングの URL であるセルフ リンクも含まれています。

目的：ユーザの削除

- 要求

  DELETE

https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity/<id>

<id> に、Add 応答で受信した ID を入力します。

DELETE 要求のヘッダーに X-auth-access-token を追加します。（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）

- **応答ヘッダー**

  200 OK

- **応答本文**

  応答本文には、削除されたユーザ セッション バインディングの詳細が含まれています。

SPAN

SPAN は、ISE がネットワークをリッスンし、ユーザ情報を取得できるようにユーザが容易に設定できるようにする、パッシブ ID サービスです。このとき、Active Directory が ISE と直接連携するように設定する必要はありません。SPAN はネットワーク トラフィックをスニフィングし、特に Kerberos メッセージを調べ、Active Directory により保存されているユーザ ID 情報を抽出し、その情報を ISE に送信します。ISE は次にその情報を解析し、最終的にはユーザ名、IP アドレス、およびドメイン名を、ISE からすでに設定しているサブスクライバに送信します。

SPAN がネットワークをリッスンし、Active Directory ユーザ情報を抽出できるようにするには、ISE と Active Directory の両方がネットワーク上の同一スイッチに接続している必要があります。これにより、SPAN は Active Directory からすべてのユーザ ID データをコピーおよびミラーリングできます。

SPAN により、ユーザ情報は次のように取得されます。

1. ネットワーク上のユーザ エンドポイントがログインします。
2. ログイン データとユーザ データは Kerberos メッセージに保存されます。
3. ユーザがログインし、ユーザ データがスイッチを通過すると、SPAN がネットワーク データをミラーリングします。
4. ISE は、ユーザ情報を取得するためネットワークをリッスンし、ミラーリングされたデータをスイッチから取得します。
5. ISE はユーザ情報を解析し、パッシブ ID マッピングを更新します。
6. ISE は解析後のユーザ情報をサブスクライバに送信します。

SPAN の使用

始める前に

ISE がネットワーク スイッチから SPAN トラフィックを受信できるようにするには、最初にそのスイッチをリッスンするノードとノードインターフェイスを定義する必要があります。インストールされている複数の ISE ノードをリッスンするには、SPAN を設定します。ネットワークをリッスンするように設定できるインターフェイスは、ノードごとに 1 つのみです。また、リッスンするために使用するインターフェイスは SPAN 専用である必要があります。

開始する前に、パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。SPAN の設定に使用可能なインターフェイスのリストには、パッシブ ID が有効なノードだけが表示されます。詳細については、初期セットアップと設定（638 ページ）を参照してください。

また、次の操作を行う必要があります。

- ネットワークで Active Directory が設定されていることを確認します。
- スイッチが ISE と通信できることを確認するために、Active Directory に接続しているネットワーク上のスイッチで CLI を実行します。
- AD からネットワークをミラーリングするようにスイッチを設定します。
- SPAN 専用の ISE ネットワーク インターフェイス カード（NIC）を設定します。この NIC は SPAN トラフィック専用で使用されます。
- SPAN 専用の NIC が、コマンドライン インターフェイスからアクティブにされていることを確認します。
- Kerberos トラフィックのみを SPAN ポートに送信する VACL を作成します。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、次に左側のパネルから [SPAN] を選択して SPAN を設定します。

ステップ 2 （注） GigabitEthernet0 ネットワーク インターフェイス カード（NIC）は使用可能なままにし、SPAN の設定には使用可能な別の NIC を選択することが推奨されます。GigabitEthernet0 は、システム管理の目的で使用されます。

わかりやすい説明を入力し（オプション）、[有効（Enabled）] ステータスを選択し、ネットワーク スイッチのリッスンに使用する関連 NIC とノードを選択します。詳細については、SPAN 設定 （663 ページ）を参照してください。

ステップ 3 [Save] をクリックします。
SPAN 設定が保存され、ISE-PIC ISE がネットワーク トラフィックをアクティブにリッスンします。

SPAN 設定

SPAN をクライアント ネットワークにインストールすることで、展開した各ノードから、 ISE がユーザ ID を受信することを簡単に設定できます。

表 *68 : SPAN* 設定

フィールド	説明
説明（Description）	現在有効なノードとインターフェイスがわかる固有の説明を入力します。
ステータス	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。
インターフェイス NIC（Interface NIC）	ISE にインストールされている 1 つ以上のノードを選択してから、選択したノードごとに、ネットワークをリッスンして情報を得るノード インターフェイスを選択します。 （注） GigabitEthernet0 NIC を引き続き使用可能にし、SPAN の設定には他に使用可能な NIC を選択することが推奨されます。GigabitEthernet0 は、システム管理の目的で使用されます。

syslog プロバイダー

syslog 機能により、 パッシブ ID サービスは syslog メッセージを配信する任意のクライアント（ID データ プロバイダー）からの syslog メッセージを解析し、MAC アドレスなどのユーザ ID 情報を送信します。syslog メッセージには、通常の syslog メッセージ（InfoBlox、Blue Coat、BlueCat、Lucent などのプロバイダーからのメッセージ）と DHCP syslog メッセージがあります。このマッピングされたユーザ ID データがサブスクライバに配信されます。

管理者がパッシブ ID および pxGrid サービスをアクティブにし、GUI から syslog クライアントを設定すると、パッシブ ID サービスはさまざまなプロバイダーから受信した syslog メッセージを使用します。管理者はプロバイダーの設定時に、接続方法（TCP または UDP）と解析に使用する syslog テンプレートを指定します。

（注） 設定されている接続タイプが TCP であり、メッセージ ヘッダーに問題があるためにホスト名を解析できない場合、ISE はパケットで受信した IP アドレスを、ISE で設定されている syslog メッセージのプロバイダー リストのすべてのプロバイダーの IP アドレスと照合しようとします。このリストを表示するには、**[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** > **[syslog プロバイダー（Syslog Providers）]** を選択します。メッセージ ヘッダーを調べ、解析が正常に実行されるように、必要に応じてカスタマイズすることが推奨されます。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （672 ページ） を参照してください。

設定が完了したら、syslog プローブは受信した syslog メッセージを ISE パーサーに送信します。パーサーはユーザ ID 情報をマッピングし、その情報を ISE に公開します。次に ISE が、解析およびマッピングされたユーザ ID 情報を パッシブ ID サービス サブスクライバに配信します。

（注） DHCP syslog メッセージにはユーザ名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE は、ユーザ ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザ（[ライブ セッション（Live Sessions）] で表示）を調べ、その後各ユーザの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスを照合してユーザ照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザに一致しない場合、メッセージは解析されず、ユーザ ID は配信されません。

ISE からの syslog メッセージを解析してユーザ ID を取得するには、次の操作を行います。

- ユーザ ID データの送信元 syslog クライアントを設定します：syslog クライアントの設定（664 ページ）
- 1 つのメッセージ ヘッダーをカスタマイズします：syslog ヘッダーのカスタマイズ （672 ページ）
- テンプレートを作成してメッセージ本文をカスタマイズします：syslog メッセージ本文のカスタマイズ （670 ページ）
- 解析に使用するメッセージテンプレートとして syslog クライアントを設定する場合には、ISE で事前に定義されているメッセージテンプレートを使用します。あるいは、これらの事前定義テンプレートに基づいてヘッダーまたは本文のテンプレートをカスタマイズします。syslog 事前定義メッセージ テンプレートの使用 （676 ページ）

syslog クライアントの設定

ISE が特定のクライアントからの syslog メッセージをリッスンできるようにするには、最初に ISE でその特定のクライアントを定義する必要があります。異なる IP アドレスを使用して複数のプロバイダーを定義できます。

始める前に

開始する前に、パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。詳細については、初期セットアップと設定 （638 ページ）を参照してください。

ステップ 1 現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定するには、**[ワーク センター（Work Centers）]** > **[PassiveID]** > **[syslog プロバイダー（Syslog Providers）]** を選択し、左側のパネルから [エージェント（Agents）] を選択します。
[syslog プロバイダー（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを設定するには、テーブルの上部で [追加（Add）] をクリックします。以前に設定したクライアントを編集または変更するには、テーブルでクライアントをオンにし、テーブル上部で [編集（Edit）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドを入力し（詳細についてはSyslog の設定（Syslog Settings） （665 ページ）を参照）、必要に応じてメッセージテンプレートを作成します（詳細についてはsyslog メッセージ本文のカスタマイズ （670 ページ）を参照）。

ステップ 4 [送信（Submit）] をクリックします。
クライアント設定が保存され、更新された [syslog プロバイダー（Syslog Providers）] テーブルが画面に表示されます。

Syslog の設定（Syslog Settings）

特定のクライアントから syslog メッセージによってユーザ ID（MAC アドレスを含む）を受信するように ISE を設定します。異なる IP アドレスを使用して複数のプロバイダーを定義できます。

[ワーク センター（Work Centers）] > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [syslog プロバイダー（Syslog Providers）] を選択し、テーブルで [追加（Add）] をクリックして、新しい syslog クライアントを作成します。

表 69 : syslog プロバイダー

フィールド	説明
名前（Name）	設定したこのクライアントを容易に区別できる一意の名前を入力します。
説明	この syslog プロバイダーのわかりやすい説明。
ステータス	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。
ホスト	ホスト マシンの FQDN を入力します。

フィールド	説明
接続タイプ（Connection Type）	ISE が syslog メッセージをリッスンするチャネルを指定するため、UDP または TCP を入力します。 （注） 設定されている接続タイプが TCP であり、メッセージヘッダーに問題があるためにホスト名を解析できない場合、ISE-PICISE はパケットで受信した IP アドレスを、ISE-PICISE で設定されている syslog メッセージのプロバイダーリストのすべてのプロバイダーの IP アドレスと照合しようとします。 このリストを表示するには、**[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** > **[syslog プロバイダー（Syslog Providers）]** を選択します。メッセージヘッダーを調べ、解析が正常に実行されるように、必要に応じてカスタマイズすることが推奨されます。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ（672 ページ） を参照してください。

フィールド	説明
テンプレート（Template）	

フィールド	説明
	テンプレートにより正確な本文メッセージ構造が指定されます。これにより、パーサーは syslog メッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。 たとえば、テンプレートでは正確なユーザ名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザ名を検出できます。 このフィールドでは、syslog メッセージを認識して正しく解析するために使用される（syslog メッセージの本文の）テンプレートを指定します。 事前定義のドロップダウンリストから選択するか、または [新規（New）] をクリックして独自のカスタム テンプレートを作成します。新しいテンプレートの作成の詳細については、syslog メッセージ本文のカスタマイズ （670 ページ）を参照してください。ほとんどの事前定義テンプレートでは正規表現が使用されています。カスタム テンプレートでも正規表現を使用する必要があります。 （注） 編集または削除できるのはカスタム テンプレートだけであり、ドロップダウンの事前定義システム テンプレートは変更できません。 現在 ISE に含まれている事前定義 DHCP プロバイダー テンプレートを次に示します。 • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP （注） DHCP syslog メッセージにはユーザ名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE-PICISE は、ユーザ ID 情報を正しく解析して配信するために、最

フィールド	説明
	初にローカル セッション ディレクトリに登録されているユーザ（[ライブ セッション（Live Sessions）] で表示）を調べ、その後各ユーザの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスを照合してユーザ照合を試行します。 DHCP syslog メッセージから受信したデータが、現在ログインしているユーザに一致しない場合、メッセージは解析されず、ユーザ ID は配信されません。 ISE には次の事前定義の標準 syslog プロバイダー テンプレートがあります。 • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN テンプレートについては、syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照してください。
デフォルト ドメイン（Default Domain）	syslog メッセージで特定のユーザに対してドメインが指定されていない場合、このデフォルト ドメインが自動的にそのユーザに割り当てられます。これにより、すべてのユーザにドメインが割り当てられます。 デフォルト ドメインまたはメッセージから解析されたドメインにユーザ名が付加され、username@domain となります。したがって、ユーザとユーザグループに関する詳細情報を取得するためには、ドメインを含めます。

syslog メッセージ構造のカスタマイズ（テンプレート）

テンプレートは正確なメッセージ構造を指定します。これにより、パーサーはsyslogメッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。たとえば、テンプレートでは正確なユーザ名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザ名を検出できます。テンプレートにより、新規マッピング メッセージとマッピング削除メッセージの両方に対応する構造が決定します。

Cisco ISE では、パッシブ ID パーサーが使用する 1 つのメッセージ ヘッダーと複数の本文構造をカスタマイズできます。

パッシブ ID パーサーが、メッセージがユーザ ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザ名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

メッセージテンプレートをカスタマイズするときに、事前定義オプションで使用されている正規表現とメッセージ構造を調べ、ISE-PICISE の事前定義メッセージ テンプレートに基づいてカスタマイズを行うかどうかを決定できます。事前定義テンプレートの正規表現、メッセージ構造、例などの詳細については、syslog事前定義メッセージテンプレートの使用 （676ページ）を参照してください。

次の内容をカスタマイズできます。

- 1 つのメッセージ ヘッダー：syslog ヘッダーのカスタマイズ （672 ページ）
- 複数のメッセージ本文：syslog メッセージ本文のカスタマイズ （670 ページ）。

（注） DHCP syslog メッセージにはユーザ名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE-PICISE は、ユーザ ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザ（[ライブ セッション（Live Sessions）] で表示）を調べ、その後各ユーザの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスを照合してユーザ照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザに一致しない場合、メッセージは解析されず、ユーザ ID は配信されません。

DHCPメッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCPメッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義のDHCPテンプレートを使用してください。

syslog メッセージ本文のカスタマイズ

Cisco ISE では、パッシブ ID パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます（メッセージ本文のカスタマイズ）。テンプレートには、ユーザ名、IPアドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） DHCP syslog メッセージにはユーザ名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE-PICISE は、ユーザ ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザ（[ライブ セッション（Live Sessions）] で表示）を調べ、その後各ユーザの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスを照合してユーザ照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザに一致しない場合、メッセージは解析されず、ユーザ ID は配信されません。

DHCP メッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCP メッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義の DHCP テンプレートを使用してください。

syslog クライアント設定画面から、syslog メッセージ本文テンプレートを作成および編集します。

（注） 各自でカスタマイズしたテンプレートだけを編集できます。システムに用意されている事前定義テンプレートは変更できません。

ステップ 1 現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定するには、**[ワーク センター（Work Centers）]** > **[PassiveID]** > **[syslog プロバイダー（Syslog Providers）]** を選択し、左側のパネルから [エージェント（Agents）] を選択します。
[syslog プロバイダー（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを追加するには [追加（Add）] をクリックし、すでに設定されているクライアントを更新するには [編集（Edit）] をクリックします。テンプレートを追加または編集するだけの場合、どのオプションを選択するかは関係ありません。syslog クライアントの設定と更新については、syslog クライアントの設定 （664 ページ）を参照してください。

ステップ 3 [syslog プロバイダー（Syslog Providers）] 画面の [テンプレート（Template）] フィールドの隣にある [新規（New）] をクリックし、新しいメッセージ テンプレートを作成します。既存のテンプレートを編集するには、ドロップダウンリストからテンプレートを選択して [編集（Edit）] をクリックします。
[syslog テンプレート（Syslog Template）] 画面が表示されます。

ステップ 4 必須フィールドをすべて指定します。

値を正しく入力する方法の詳細については、syslog カスタマイズ テンプレートの設定と例 （673 ページ）を参照してください。

ステップ 5 [テスト（Test）]をクリックして、入力した文字列に基づいてメッセージが正しく解析されていることを確認します。

ステップ 6 [保存（Save）] をクリックします。

カスタマイズしたテンプレートが保存され、新しい syslog クライアントの設定時と既存の syslog クライアントの更新時に [テンプレート（Template）] フィールドのドロップダウンリストにこのテンプレートが表示されます。

syslog ヘッダーのカスタマイズ

syslog ヘッダーには、メッセージの送信元のホスト名が他の詳細情報と共に含まれています。syslog メッセージが ISE メッセージ パーサーで認識されない場合は、ホスト名の後に続く区切り文字を設定し、ISE がホスト名を認識してメッセージを正しく解析できるようにすることで、メッセージヘッダーをカスタマイズする必要がある場合があります。この画面のフィールドの詳細については、syslog カスタマイズテンプレートの設定と例（673 ページ）を参照してください。カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダー タイプにこの設定が追加されます。

（注） 1 つのヘッダーだけをカスタマイズできます。ヘッダーのカスタマイズ後に、[カスタム ヘッダー（Custom Header）] をクリックして保存するテンプレートを作成し、[送信（Submit）] をクリックすると、最新の設定が保存され、以前のカスタマイズ内容が上書きされます。

ステップ 1 現在設定されているすべてのクライアントを表示し、既存のクライアントを編集、削除し、新しいクライアントを設定するには、**[ワーク センター（Work Centers）]** > **[PassiveID]** > **[syslog プロバイダー（Syslog Providers）]** を選択し、左側のパネルから [エージェント（Agents）] を選択します。
[syslog プロバイダー（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 [カスタム ヘッダー（Custom Header）] をクリックして [syslog カスタム ヘッダー（Syslog Custom Header）] 画面を開きます。

ステップ 3 [サンプル syslog を貼り付ける（Paste sample syslog）] に、syslog メッセージのヘッダー形式の例を入力します。たとえば、メッセージの 1 つからヘッダー **`<181>Oct 10 15:14:08 Cisco.com`** をコピーして貼り付けます。

ステップ 4 [区切り文字（Separator）] フィールドで、単語をスペースとタブのいずれで区切るかを指定します。

ステップ 5 [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドで、ヘッダーのどの位置がホスト名であるかを指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。

[ホスト名（Hostname）] フィールドに、最初の 3 つのフィールドに示される詳細情報に基づいてホスト名が表示されます。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。

<181>Oct 10 15:14:08 Cisco.com

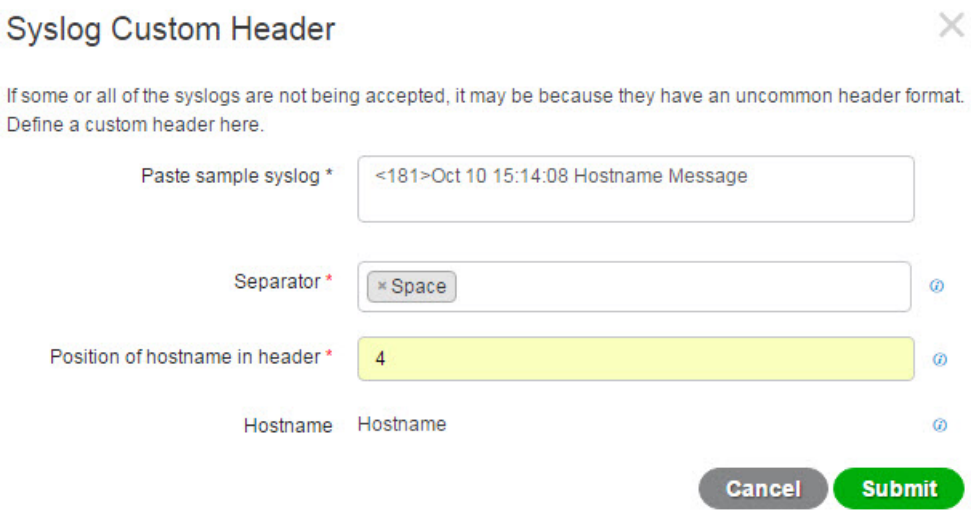
区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。

[ホスト名（Hostname）] には自動的に Cisco.com と表示されます。これは、[syslog の例を貼り付ける（Paste sample syslog）] フィールドに貼り付けたヘッダー フレーズの 4 番目の単語です。

ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

この例を次のスクリーン キャプチャに示します。

図 *32 : syslog* ヘッダーのカスタマイズ



ステップ 6 （注） 1 つのヘッダーだけをカスタマイズできます。ヘッダーのカスタマイズ後に、[カスタム ヘッダー（Custom Header）] をクリックして保存するテンプレートを作成し、[送信（Submit）] をクリックすると、最新の設定が保存され、以前のカスタマイズ内容が上書きされます。

[送信（Submit）] をクリックします。
カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダータイプにこの設定が追加されます。

syslog カスタマイズ テンプレートの設定と例

Cisco ISE では、パッシブ ID パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます。カスタマイズされたテンプレートは、新規マッピング メッセージとマッピング削除メッセージの両方に対応する構造を決定します。パッシブ ID パーサーが、メッセージがユーザ ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザ名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されます。カスタマイズテンプレートでも正規表現を使用してください。

syslog ヘッダーの各部分

ホスト名の後に続く区切り文字を設定することで、syslog プローブが認識する単一ヘッダーをカスタマイズできます。

[ワーク センター（Work Centers）] > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [syslog プロバイダー（Syslog Providers）] を選択し、テーブルで [カスタム ヘッダー（Custom Header）] をクリックして、カスタム syslog メッセージ ヘッダーを作成します。

次の表に、カスタム syslog ヘッダーに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 72 : カスタマイズ テンプレートの正規表現（676 ページ）を参照してください。

表 *70 : syslog* カスタム ヘッダー

フィールド	説明
syslog の例を貼り付ける（Paste sample syslog）	syslog メッセージにヘッダー形式の例を入力します。たとえば、次のヘッダーをコピーして貼り付けます。 **`<181>Oct 10 15:14:08 Hostname Message`**
区切り文字（Separator）	単語をスペースまたはタブのいずれで区切るかを指定します。
ヘッダーのホスト名の位置（Position of hostname in header）	ヘッダーでのホスト名の位置を指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。

フィールド	説明
ホストネーム	最初の 3 つのフィールドに示される詳細情報に基づいて、ホスト名を表示します。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。 <181>Oct 10 15:14:08 Hostname Message 区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。 [ホスト名（Hostname）] には Hostname が自動的に表示されます。 ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

メッセージ本文の syslog テンプレートの各部分と説明

次の表に、カスタマイズ syslog メッセージ テンプレートに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 72 : カスタマイズ テンプレートの正規表現 （676 ページ）を参照してください。

表 *71 : syslog* テンプレート

パート	フィールド	説明
	名前（Name）	このテンプレートの目的がわかる一意の名前。
マッピング操作	新規マッピング	新しいユーザを追加するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、F5 VPN にログインした新しいユーザを示すには、このフィールドに「logged on from」と入力します。
	削除されたマッピング	ユーザを削除するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、削除する必要がある ASA VPN のユーザを示すには、このフィールドに「session disconnect」と入力します。

パート	フィールド	説明
ユーザデータ	IPアドレス	キャプチャする IP アドレスを示す正規表現。 たとえば Bluecat メッセージの場合、この IP アドレス範囲内のユーザの ID をキャプチャするには、次のように入力します。 (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))
	ユーザ名	キャプチャするユーザ名形式を示す正規表現。
	ドメイン	キャプチャするドメインを示す正規表現。
	MAC アドレス	キャプチャする MAC アドレスの形式を示す正規表現。

正規表現の例

メッセージを解析するため、正規表現を使用します。ここでは、IPアドレス、ユーザ名、およびマッピング追加メッセージを解析する正規表現の例を示します。

たとえば、正規表現を使用して次のメッセージを解析します。

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

次の表に、正規表現の定義を示します。

表 *72 :* カスタマイズ テンプレートの正規表現

パート	[正規表現（Regular Expression）]
IP アドレス	Address <([^\s]+)>|address ([^\s]+)
ユーザ名（User name）	User <([^\s]+)>| Username = ([^\s]+)
マッピング追加メッセージ（Add mapping message）	(%ASA-4-722051|%ASA-6-713228)

syslog 事前定義メッセージ テンプレートの使用

syslog メッセージには、ヘッダーとメッセージ本文を含む標準構造があります。

ここでは、メッセージの送信元に基づいてサポートされているヘッダーの内容の詳細や、サポートされている本文の構造など、Cisco ISE が提供する事前定義テンプレートについて説明します。

また、システムで事前に定義されていないソース用に、カスタマイズした本文コンテンツを使用した独自のテンプレートを作成することもできます。ここでは、カスタムテンプレートでサポートされる構造について説明します。メッセージの解析時には、システムで事前定義されているヘッダーに加え、1つのカスタマイズヘッダーを設定できます。また、メッセージ本文には、服すのカスタマイズテンプレートを設定できます。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （672 ページ） を参照してください。本文のカスタマイズの詳細については、syslog メッセージ本文のカスタマイズ （670 ページ） を参照してください。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されています。カスタムテンプレートでも正規表現を使用する必要があります。

メッセージ ヘッダー

パーサーで認識されるヘッダータイプには、すべてのクライアントマシンのすべてのメッセージタイプ（新規および削除）について認識される2つのタイプがあります。これらのヘッダーは次のとおりです。

- <171>Host message
- <171>Oct 10 15:14:08 Host message

受信されたヘッダーはホスト名を検出するため解析されます。ホスト名は、IPアドレス、ホスト名、または完全 FQDN のいずれかです。

ヘッダーもカスタマイズできます。ヘッダーをカスタマイズするには、syslog ヘッダーのカスタマイズ （672 ページ）を参照してください。

syslog ASA VPN 事前定義テンプレート

ASA VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

本文メッセージ	解析例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] （注） このメッセージタイプから解析されるIPアドレスは、メッセージに示されているようにプライベートIPアドレスです。
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] （注） このメッセージタイプから解析されたIPアドレスはIPv4アドレスです。

マッピング削除本文メッセージ

ここではパーサーでASA VPNのためにサポートされているマッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[UserA,10.1.1.1]

本文メッセージ
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

syslog Bluecat 事前定義テンプレート

Bluecat でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング本文メッセージ

ここでは、Bluecat syslog で新規マッピングとしてサポートされるメッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

本文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

マッピング削除メッセージ

Bluecat のマッピング削除メッセージはありません。

syslog F5 VPN 事前定義テンプレート

F5 VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな F5 VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[user=UserA,ip=172.16.0.12]

本文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

マッピング削除メッセージ

現在、F5 VPN でサポートされている削除メッセージはありません。

syslog Infoblox 事前定義テンプレート

Infoblox でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

本文メッセージ
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)

本文メッセージ
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

マッピング削除メッセージ

マッピング削除では次のメッセージがサポートされています。

パーサーはさまざまな本文メッセージをマッピング削除メッセージとして認識します。これについて次の表で説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

- MAC アドレスが含まれている場合：

  [00:0c:29:a2:18:34,10.0.10.100]

- MAC アドレスが含まれていない場合：

  [10.0.10.100]

本文メッセージ
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

syslog Linux DHCPd3 事前定義テンプレート

Linux DHCPd3 でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング メッセージ

次の表では、パーサーが認識するさまざまな Linux DHCPd3 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

マッピング削除本文メッセージ

ここではパーサーで Linux DHCPd3 のためにサポートされているマッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[00:0c:29:a2:18:34 ,10.0.10.100]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

syslog MS DHCP 事前定義テンプレート

MS DHCP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな MS DHCP 本文メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0

マッピング削除本文メッセージ

ここではパーサーで MS DHCP のためにサポートされているマッピング削除メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

syslog SafeConnect NAC 事前定義テンプレート

SafeConnect NAC でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな SafeConnect NAC 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

本文メッセージ
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

マッピング削除メッセージ

現在、Safe Connect でサポートされている削除メッセージはありません。

syslog Aerohive 事前定義テンプレート

Aerohive でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Aerohive 本文メッセージについて説明します。

本文で解析される詳細には、ユーザ名と IP アドレスがあります。解析に使用される正規表現の例を次に示します。

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

受信された本文が解析され、次のようにユーザの詳細が判明します。

[UserA,10.5.50.52]

本文メッセージ
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

マッピング削除メッセージ

現在、Aerohive からのマッピング削除メッセージはサポートされていません。

syslog Blue Coat 事前定義テンプレート：Main Proxy、Proxy SG、Squid Web Proxy

Blue Coat の次のメッセージ タイプがサポートされています。

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

BlueCoat メッセージでサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Blue Coat 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザの詳細が判明します。

[UserA,192.168.10.24]

本文メッセージ（この例は、**BlueCoat プロキシ SG** メッセージからの引用です）
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

次の表では、新規マッピング メッセージに使用されるクライアント別の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\s(?:[0-9]{1,3}\.){3}[0-9]{1,3}\s(?:[a-zA-Z0-9]{1,4}:){1,7}[a-zA-Z0-9]{1,4})\s** ユーザ名（User name） **\s\-\s([a-zA-Z0-9_]+)\s\-\s**

クライアント	正規表現
BlueCoat Proxy SG	新規マッピング **(\-\sPROXIED){1}** IP **\(?:[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\)\s[a-zA-Z0-9]{4,12}\([a-zA-Z0-9]{4,8}\)\s[a-zA-Z0-9_]+\s-** ユーザ名（User name） **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid Web Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\(?:[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\)\s[a-zA-Z0-9]{4,12}\([a-zA-Z0-9]{4,8}\)\sTCP** ユーザ名（User name） **\s([a-zA-Z0-9\._]+)\s\-\/**

マッピング削除メッセージ

Blue Coat クライアントではマッピング削除メッセージがサポートされていますが、現在利用できる例はありません。

次の表では、マッピング削除メッセージに使用されるクライアント別の既知の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	現在利用できる例はありません。
BlueCoat Squid Web Proxy	**(TCP_MISS|TCP_NC_MISS){1}**

syslog ISE および ACS 事前定義テンプレート

パーサーは ISE または ACS クライアントをリッスンするときに、次のメッセージ タイプを受信します。

- 認証成功：ユーザが ISE または ACS により認証されると、認証が成功したことを通知し、ユーザの詳細情報を記述した認証成功メッセージが発行されます。このメッセージが解析され、このメッセージのユーザの詳細とセッション ID が保存されます。
- アカウンティング開始およびアカウンティング更新メッセージ（新規マッピング）：ISE または ACS から受信したアカウンティング開始メッセージまたはアカウンティング更新メッセージは、認証成功メッセージから保存されたユーザの詳細とセッション ID を使用して解析され、ユーザがマッピングされます。

- アカウンティング終了（マッピング削除）：ISEまたはACSから受信されると、システムからユーザ マッピングが削除されます。

ISE および ACS でサポートされる syslog メッセージの形式とタイプについて説明します。

認証成功メッセージ

認証成功メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- **解析例**

  ユーザ名とセッション ID だけが解析されます。

  [UserA,5]

アカウンティング開始/更新（新規マッピング）メッセージ

新規マッピング メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザ名、フレームIPアドレス、およびMACアドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

マッピング削除メッセージ

マッピング削除では次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザ名、フレームIPアドレス、およびMACアドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

syslog Lucent QIP 事前定義テンプレート

Lucent QIP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（syslog 事前定義メッセージ テンプレートの使用 （676 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまなLucent QIP本文メッセージについて説明します。

これらのメッセージの正規表現構造を次に示します。

DHCP_GrantLease|:DHCP_RenewLease

受信された本文が解析され、次のようにユーザの詳細が判明します。

[00:0C:29:91:2E:5D,10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

マッピング削除本文メッセージ

次の表では、パーサーが認識するさまざまなLucent QIP本文メッセージについて説明します。

これらのメッセージの正規表現構造を次に示します。

Delete Lease:|DHCP Auto Release:

受信された本文が解析され、次のようにユーザの詳細が判明します。

[10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

パッシブ ID サービスのフィルタリング

特定のユーザを名前やIPアドレスに基づいてフィルタリングできます。たとえばITサービスの管理者が、そのエンドポイントの標準ユーザを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して [ライブ セッション（Live Sessions）] に表示されないようにし、そのエンドポイントの標準ユーザだけが表示されるようにできます。[ライブ セッション（Live Session）] には、マッピング フィルタでフィルタリングされていないパッシブ ID サービス コンポーネントが表示されます。フィルタは必要なだけ追加できます。「OR」論理演算子をフィルタの間に適用します。両方のフィールドを 1 つのフィルタで指定する場合は、「AND」論理演算子をこれらのフィールドの間に適用します。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから [マッピング フィルタ（Mapping Filters）] を選択します。

ステップ 2 **[プロバイダー（Providers）]** > **[マッピング フィルタ（Mapping Filters）]** を選択します。

ステップ 3 [追加（Add）] をクリックし、フィルタするユーザのユーザ名やIPアドレスを入力して、[送信（Submit）] をクリックします。

ステップ 4 現在モニタリング セッション ディレクトリにログインしてしているフィルタリングされていないユーザを表示するには、**[操作（Operations）]** > **[RADIUSライブログ（RADIUS Livelog）]** を選択します。

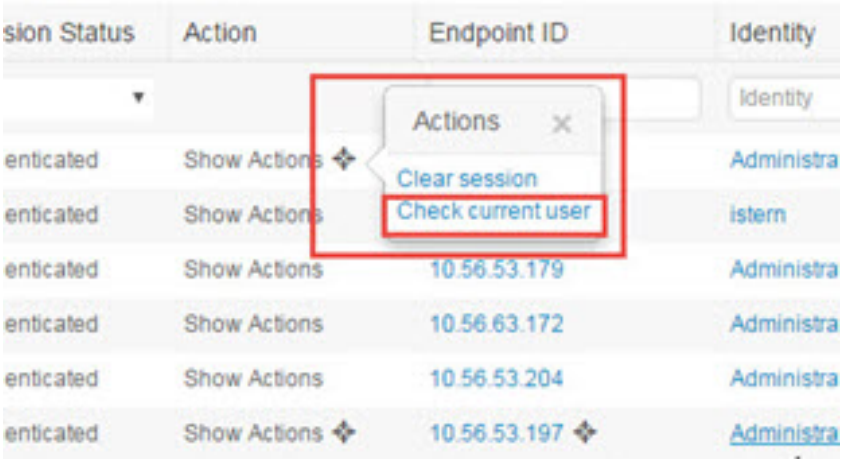
エンドポイント プローブ

設定可能なカスタム プロバイダーの他に、パッシブ ID サービス がアクティブになると ISE でエンドポイント プローブが有効になります。エンドポイント プローブは、特定の各ユーザがまだシステムにログインしているかどうかを定期的にチェックします。

（注） エンドポイントがバックグラウンドで実行されることを確認するには、まず最初の Active Directory 参加ポイントを設定し、[クレデンシャルの保存（Store Credentials）] を選択していることを確認します。エンドポイントプローブの設定の詳細については、エンドポイントプローブの使用 （690 ページ）を参照してください。

エンドポイントのステータスを手動で確認するには、[アクション（Actions）] 列から [ライブセッション（Live Sessions）] に移動し、[アクションを表示（Show Actions）] をクリックし、次の図に示すように [現在のユーザを確認（Check current user）] を選択します。

図 *33* : 現在のユーザの確認



エンドポイントユーザのステータスと手動でのチェックの実行の詳細については、RADIUS ライブ セッション （337 ページ）を参照してください。

エンドポイントプローブはユーザが接続していることを認識します。特定のエンドポイントのセッションが最後に更新された時点から 4 時間経過している場合には、ユーザがまだログインしているかどうかを確認し、次のデータを収集します。

- MAC アドレス
- オペレーティング システムのバージョン

このチェックに基づいてプローブは次の操作を実行します。

- ユーザがまだログインしている場合、プローブは ISE を [アクティブユーザ（Active User）] ステータスで更新します。
- ユーザがログアウトしている場合、セッション状態は [終了（Terminated）] に更新され、15 分経過後にユーザはセッション ディレクトリから削除されます。
- ユーザと通信できない場合、たとえばファイアウォールによって通信が防止されているか、エンドポイントがシャットダウンしている場合などには、ステータスが [到達不可能

（Unreachable）] として更新され、サブスクライバポリシーによってユーザセッションの処理方法が決定します。エンドポイントは引き続きセッションディレクトリに残ります。

エンドポイント プローブの使用

始める前に

サブネット範囲に基づいてエンドポイント プローブを作成および有効にできます。PSN ごとに1つのエンドポイントプローブを作成できます。エンドポイントプローブを使用するには、次のように設定していることを確認してください。

- エンドポイントはポート 445 とのネットワーク接続が必要です。
- ISE から 1 番目の Active Directory 参加ポイントを設定し、プロンプトが表示されたら [クレデンシャルの選択（Select Credentials）] を選択してください。参加ポイントの詳細については、プローブおよびプロバイダーとしての Active Directory （640 ページ）を参照してください。

（注） エンドポイントがバックグラウンドで実行するようにするため、最初に 1 番目の Active Directory 参加ポイントを設定する必要があります。これにより、Active Directory プローブが完全に設定されていない場合でもエンドポイントプローブを実行できるようになります。

ステップ 1 **[ワーク センター（Work Centers）] > [パッシブ ID（Passive ID）] > [プロバイダー（Providers）]** を選択し、[エンドポイント プローブ（Endpoint Probes）] を選択します。

ステップ 2 新しいエンドポイント プローブを作成するには、[追加（Add）] をクリックします。

ステップ 3 必須フィールドに入力し、[ステータス（Status）] フィールドで [有効化（Enable）] を選択していることを確認してから、[送信（Submit）] をクリックします。詳細については、エンドポイント プローブ設定 （690 ページ）を参照してください。

エンドポイント プローブ設定

サブネット範囲に基づいて PSN ごとに 1 つのエンドポイント プローブを作成します。展開で複数の PSN を使用している場合、個別のサブネット セットに各 PSN を割り当てることができます。この場合、各プローブを異なるユーザ グループに使用します。

[ワーク センター（Work Centers）] > [パッシブ ID（Passive ID）] > [プロバイダー（Providers）] を選択し、次に [エンドポイント プローブ（Endpoint Probes）] を選択して、PSN に新しいエンドポイント プローブを設定します。

表 *73 :* エンドポイント プローブ設定

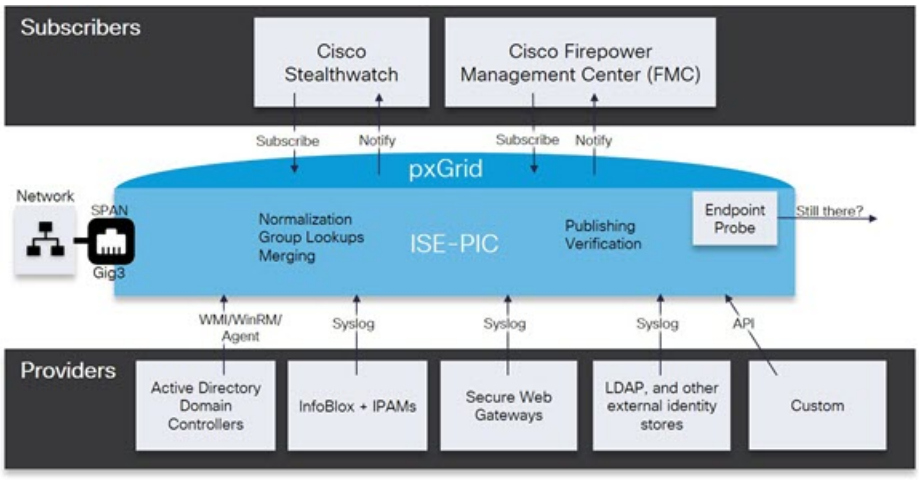
フィールド	説明
名前（Name）	このプローブの用途を示す一意の名前を入力します。
説明（Description）	このプローブの用途を示す一意の説明を入力します。
ステータス（Status）	このプローブをアクティブにするには[有効化（Enable）] を選択します。
ホスト名	展開で使用可能な PSN のリストから、このプローブの PSN を選択します。
サブネット	このプローブがチェックする必要があるエンドポイントのグループのサブネット範囲を入力します。標準のサブネット マスク範囲と、カンマで区切ったサブネット アドレスを使用します。 例： 10.56.14.111/32,1.1.1.1/24,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 各範囲は一意である必要があり、相互に重複していてはなりません。たとえば、範囲 2.2.2.0/16,2.2.3.0/16 は相互に重複しているため、同一プローブに対して入力できません。

サブスクライバ

パッシブ ID サービス は、さまざまなプロバイダーから収集し、Cisco ISE セッション ディレクトリにより保存された認証済みユーザ ID を、Cisco Stealthwatch や Cisco Firepower Management Center（FMC）などのその他のネットワーク システムに送信するため、Cisco pxGrid サービスを使用します。

次の図では、pxGrid ノードが外部プロバイダーからユーザ ID を収集しています。これらの ID は解析、マッピング、およびフォーマットされます。pxGrid はこれらのフォーマット済みのユーザ ID を取得し、パッシブ ID サービス サブスクライバに送信します。

図 *34* : パッシブ *ID* サービス フロー



Cisco ISE に接続するサブスクライバは、pxGrid サービスの使用を登録する必要があります。サブスクライバは、クライアントになるために pxGrid SDK を介してシスコから使用可能な pxGrid クライアント ライブラリを採用する必要があります。サブスクライバは、一意の名前と証明書ベースの相互認証を使用して pxGrid にログインできます。Cisco pxGrid サブスクライバは、有効な証明書を送信すると、ISE により自動的に承認されます。

サブスクライバは設定されている pxGrid サーバのホスト名または IP アドレスのいずれかに接続できます。不必要なエラーが発生することを防ぎ、DNS クエリが適切に機能するようにするため、ホスト名を使用することが推奨されます。公開および登録するためにサブスクライバの pxGrid で作成される、情報トピックまたはチャネル機能があります。Cisco ISE では SessionDirectory と IdentityGroup だけがサポートされています。機能情報は、公開、ダイレクト クエリ、または一括ダウンロード クエリによりパブリッシャから取得でき、[機能（Capabilities）] タブの [サブスクライバ（Subscribers）] で確認できます。

サブスクライバが ISE から情報を受信できるようにするには、次の操作を行います。

1. 必要に応じて、サブスクライバ側から証明書を生成します。
2. PassiveID ワーク センターからサブスクライバの pxGrid 証明書の生成 （693 ページ）を参照してください。
3. サブスクライバの有効化 （694 ページ）。サブスクライバが ISE からユーザ ID を受信できるようにするため、このステップを実行するか、承認を自動的に有効にします。サブスクライバの設定 （695 ページ） を参照してください。

サブスクライバの pxGrid 証明書の生成

始める前に

pxGrid とサブスクライバの間の相互信頼を保証するため、pxGrid サブスクライバの証明書を生成できます。これにより、ISE からサブスクライバにユーザ ID を渡すことが可能になります。次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[サブスクライバ（Subscribers）]** を選択し、[証明書（Certificates）] タブに移動します。

ステップ 2 [処理の選択（I want to）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- 単一の証明書の生成（証明書署名要求なし）（Generate a single certificate without a certificate signing request）：このオプションを選択すると、コモン ネーム（CN）を入力する必要があります。[コモン ネーム（Common Name）] フィールドに、pxGrid をプレフィックスとして含む pxGrid FQDN を入力します。たとえば www.pxgrid-ise.ise.net です。あるいはワイルドカードを使用します。たとえば *.ise.net です。
- 単一の証明書の生成（証明書署名要求あり）（Generate a single certificate with a certificate signing request）：このオプションを選択すると、証明書署名要求の詳細を入力する必要があります。
- 一括証明書の生成（Generate bulk certificates）：必要な詳細を含む CSV ファイルをアップロードすることができます。
- [ルート証明書チェーンのダウンロード（Download root certificate chain）]：pxGrid クライアントの信頼できる証明書ストアに追加するために、ISE パブリック ルート証明書をダウンロードします。ISE pxGrid ノードは、新規に署名された pxGrid クライアント証明書だけを信頼します（あるいはこの逆）。これにより、外部の認証局を使用する必要がなくなります。

ステップ 3 （オプション）この証明書の説明を入力できます。

ステップ 4 この証明書のベースとなる pxGrid 証明書テンプレートを表示または編集します。証明書テンプレートには、そのテンプレートに基づいて認証局（CA）によって発行されたすべての証明書に共通のプロパティが含まれています。証明書テンプレートは、件名、サブジェクト代替名（SAN）、キー タイプ、キー サイズ、使用する必要がある SCEP RA プロファイル、証明書の有効期間、証明書がクライアントまたはサーバの認証またはその両方に使用される必要があるかどうかを指定した拡張キーの使用状況（EKU）を定義します。内部 Cisco ISE CA（ISE CA）は、証明書テンプレートを使用し、そのテンプレートに基づいて証明書を発行します。このテンプレートを編集するには、**[管理（Administration）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[証明書テンプレート（Certificate Templates）]** を選択します。

ステップ 5 サブジェクト代替名（SAN）を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- FQDN：ISE ノードの完全修飾ドメイン名を入力します。たとえば www.isepic.ise.net です。あるいは FQDN にワイルドカードを使用します。たとえば *.ise.net です。

  pxGrid FQDN も入力できる追加の行を FQDN に追加できます。これは [コモンネーム（Common Name）] フィールドで使用する FQDN と同一である必要があります。

- [IP アドレス（IP address）]：この証明書に関連付ける ISE ノードの IP アドレスを入力します。サブスクライバが FQDN ではなく IP アドレスを使用する場合には、この情報を入力する必要があります。

（注） このフィールドは、[一括証明書の生成（Generate bulk certificates）] オプションを選択している場合には表示されません。

ステップ 6 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- Private Enhanced Electronic Mail（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY----」タグで終わります。
- PKCS12 形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル）：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンド エンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成（Create）] をクリックします。

サブスクライバの有効化

サブスクライバが からユーザ ID を受信できるようにするため、このタスクを実行するか、または承認を自動的に有効にする必要があります。サブスクライバの設定（695 ページ）を参照してください。

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- パッシブ ID サービスを有効にします。詳細については、Easy Connect（632 ページ）を参照してください。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[サブスクライバ（Subscribers）]** を選択し、[クライアント（Clients）] タブが表示されることを確認します。

ステップ 2 サブスクライバの隣にあるチェックボックスをオンにして [承認（Approve）] をクリックします。

ステップ 3 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

ライブ ログからのサブスクライバ イベントの表示

[ライブ ログ（Live Logs）] ページにはすべてのサブスクライバ イベントが表示されます。イベント情報には、イベント タイプ、タイムスタンプ、サブスクライバ名、機能名が含まれています。

[サブスクライバ（Subscribers）] に移動し、[ライブ ログ（Live Log）] タブを選択し、イベント リストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

サブスクライバの設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** > **[設定（Settings）]** を選択します。

ステップ 2 必要に応じて、次のオプションを選択します。

- 新しいアカウントの自動承認（Automatically Approve New Accounts）：このチェック ボックスにマークを付けると、新しい pxGrid クライアントからの接続要求が自動的に承認されます。
- パスワード ベースのアカウント作成の許可（Allow Password Based Account Creation）：このチェック ボックスにマークを付けると、pxGrid クライアントのユーザ名/パスワード ベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

  pxGrid クライアントは、REST API を介してユーザ名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

ステップ 3 [保存（Save）] をクリックします。

PassiveID ワークセンター でのサービスのモニタリングとトラブルシューティング

モニタリング、トラブルシューティング、およびレポーティングの各ツールを使用して PassiveID ワークセンター を管理する方法について説明します。

- RADIUS ライブ セッション （337 ページ）
- 『』の「レポート」のセクションを参照してください。Cisco ISE レポート （299 ページ）
- 着信トラフィックを検証する TCP ダンプ ユーティリティ （1582 ページ）

LDAP

Lightweight Directory Access Protocol（LDAP）は、RFC 2251 で定義されている、TCP/IP 上で動作するディレクトリ サービスの問い合わせおよび変更のためのネットワーキング プロトコルです。LDAP は、X.500 ベースのディレクトリ サーバにアクセスするためのライトウェイト メカニズムです。

Cisco ISE は、LDAP プロトコルを使用して LDAP 外部データベース（ID ソースとも呼ばれる）と統合します。

LDAP ディレクトリ サービス

LDAP ディレクトリ サービスは、クライアント/サーバ モデルに基づきます。クライアントは、LDAP サーバに接続し、操作要求をサーバに送信することで、LDAP セッションを開始します。サーバは、応答を送信します。1 台以上の LDAP サーバに、LDAP ディレクトリ ツリーまたは LDAP バックエンド データベースからのデータが含まれています。

ディレクトリ サービスは、情報を保持するデータベースであるディレクトリを管理します。ディレクトリ サービスは、情報を保存するために分散モデルを使用します。その情報は、通常はディレクトリ サーバ間で複製されます。

LDAP ディレクトリは、単純なツリー階層で編成されており、数多くのサーバ間で分散できます。各サーバには、定期的に同期化されるディレクトリ全体の複製バージョンを配置できます。

ツリーのエントリには属性のセットが含まれており、各属性には名前（属性タイプまたは属性の説明）と 1 つ以上の値があります。属性はスキーマに定義されます。

各エントリには、固有識別情報、つまり識別名（DN）があります。この名前には、エントリ内の属性で構成されている相対識別名（RDN）と、それに続く親エントリの DN が含まれています。DN は完全なファイル名、RDN はフォルダ内の相対ファイル名と考えることができます。

複数の LDAP インスタンス

IP アドレスまたはポートの設定が異なる複数の LDAP インスタンスを作成することにより、異なる LDAP サーバを使用するか、または同じ LDAP サーバ上の異なるデータベースを使用して認証を行うように、Cisco ISE を設定できます。プライマリ サーバの各 IP アドレスおよびポートの設定は、セカンダリ サーバの IP アドレスおよびポートの設定とともに、Cisco ISE LDAP ID ソース インスタンスに対応する LDAP インスタンスを形成します。

Cisco ISE では、個々の LDAP インスタンスが一意の LDAP データベースに対応している必要はありません。複数の LDAP インスタンスを、同一のデータベースにアクセスするように設定できます。この方法は、LDAP データベースにユーザまたはグループのサブツリーが複数含まれている場合に役立ちます。各 LDAP インスタンスでは、ユーザとグループに対してそれぞれ単一のサブツリー ディレクトリだけをサポートするため、Cisco ISE が認証要求を送信するユー

ザ ディレクトリとグループ ディレクトリのサブツリーの組み合わせごとに、別々の LDAP インスタンスを設定する必要があるからです。

LDAP フェールオーバー

Cisco ISE は、プライマリ LDAP サーバとセカンダリ LDAP サーバ間でのフェールオーバーをサポートします。フェールオーバーは、LDAP サーバがダウンしているかまたは到達不可能なために Cisco ISE で LDAP サーバに接続できないことが原因で認証要求が失敗した場合に発生します。

フェールオーバー設定が指定され、Cisco ISE で接続しようとした最初の LDAP サーバが到達不可能な場合、Cisco ISE は常に 2 番目の LDAP サーバへの接続を試行します。再度、Cisco ISE で最初の LDAP サーバを使用する場合は、[フェールバック再試行の遅延（Failback Retry Delay）] テキスト ボックスに値を入力する必要があります。

（注） Cisco ISE では、常にプライマリ LDAP サーバを使用して、認証ポリシーで使用するグループと属性を管理者ポータルから取得します。このため、プライマリ LDAP サーバはこれらの項目を設定するときにアクセス可能である必要があります。Cisco ISE では、フェールオーバーの設定に従って、実行時に認証と許可にのみセカンダリ LDAP サーバを使用します。

LDAP 接続管理

Cisco ISE では、複数の同時 LDAP 接続がサポートされます。接続は、最初の LDAP 認証時にオンデマンドで開かれます。最大接続数は、LDAP サーバごとに設定されます。事前に接続を開いておくと、認証時間が短縮されます。同時バインディング接続に使用する最大接続数を設定できます。開かれる接続の数は、LDAP サーバ（プライマリまたはセカンダリ）ごとに異なる場合があり、サーバごとに設定される最大管理接続数に基づいて決まります。

Cisco ISE は、Cisco ISE で設定されている LDAP サーバごとに、開いている LDAP 接続（バインディング情報を含む）のリストを保持します。認証プロセス中に、Connection Manager は開いている接続をプールから検索しようとします。開いている接続が存在しない場合、新しい接続が開かれます。

LDAP サーバが接続を閉じた場合、Connection Manager はディレクトリを検索する最初のコールでエラーをレポートし、接続を更新しようとします。認証プロセスが完了した後、Connection Manager は接続を解放します。

LDAP ユーザ認証

LDAP を外部 ID ストアとして設定できます。Cisco ISE はプレーン パスワード認証を使用します。ユーザ認証には次の処理が含まれます。

- LDAP サーバでの、要求のユーザ名に一致するエントリの検索
- ユーザ パスワードと、LDAP サーバで見つかったパスワードとの照合

- ポリシーで使用するグループ メンバーシップ情報の取得
- ポリシーおよび許可プロファイルで使用するように指定された属性の値の取得

ユーザを認証するために、Cisco ISE は LDAP サーバにバインド要求を送信します。バインド要求には、ユーザの DN およびユーザ パスワードがクリア テキストで含まれています。ユーザの DN およびパスワードが LDAP ディレクトリ内のユーザ名およびパスワードと一致した場合に、ユーザは認証されます。

Active Directory が LDAP として使用されている場合は、UPN 名がユーザ認証に使用されます。Sun ONE Directory Server が LDAP として使用されている場合は、SAM 名がユーザ認証に使用されます。

（注） Cisco ISE は、ユーザ認証ごとに 2 つの searchRequest メッセージを送信します。これは、Cisco ISE の許可またはネットワークのパフォーマンスに影響しません。2 番目の LDAP 要求では、Cisco ISE が正しい ID と通信していることを確認します。

（注） DNS クライアントとしての Cisco ISE は、DNS 応答で返された最初の IP のみを使用して、LDAP バインドを実行します。

Secure Sockets Layer（SSL）を使用して LDAP サーバへの接続を保護することを推奨します。

（注） パスワードの変更は、パスワードの有効期限が切れた後にアカウントの残りの猶予ログインがあるときにのみ、LDAP でサポートされます。パスワードが正常に変更された場合、LDAP サーバの bindResponse は LDAP_SUCCESS であり、bindResponse メッセージに残りの猶予ログインの制御フィールドが含まれます。bindResponse メッセージにさらなる制御フィールド（残りの猶予ログイン以外）が含まれる場合は、Cisco ISE がメッセージを復号できない可能性があります。

許可ポリシーで使用する LDAP グループおよび属性の取得

Cisco ISE は、ディレクトリ サーバでバインド操作を実行し、サブジェクトを検索および認証することによって、LDAP ID ソースに対してサブジェクト（ユーザまたはホスト）を認証できます。認証が成功した後、Cisco ISE は、要求された場合、常にサブジェクトに所属するグループおよび属性を取得できます。Cisco ISE 管理者ポータルで取得されるように属性を設定するには、**[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [LDAP]** を選択します。Cisco ISE は、これらのグループおよび属性を使用してサブジェクトを許可できます。

ユーザの認証または LDAP ID ソースの問い合わせを行うために、Cisco ISE は LDAP サーバに接続し、接続プールを保持します。

Active Directory が LDAP ストアとして設定されている場合は、グループ メンバーシップに関する次の制限事項に注意する必要があります。

- ユーザまたはコンピュータは、ポリシー条件でポリシー ルールに一致するように定義されたグループの直接的なメンバーである必要があります。
- 定義されたグループは、ユーザまたはコンピュータのプライマリ グループではない可能性があります。この制限は、Active Directory が LDAP ストアとして設定されている場合にのみ適用されます。

LDAP グループ メンバーシップ情報の取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからグループ メンバーシップ情報を取得する必要があります。LDAP サーバは、サブジェクト（ユーザまたはホスト）とグループ間の関連付けを次の方法のいずれかで表します。

- グループがサブジェクトを参照：グループ オブジェクトには、サブジェクトを指定する属性が含まれています。サブジェクトの識別子は、次のものとしてグループに供給できます。
  - 識別名
  - プレーン ユーザ名
- サブジェクトがグループを参照：サブジェクト オブジェクトには、所属するグループを指定する属性が含まれています。

LDAP ID ソースには、グループ メンバーシップ情報の取得のために次のパラメータが含まれています。

- [参照方向（Reference direction）]：このパラメータは、グループ メンバーシップを決定するときに使用する方法を指定します（グループからサブジェクトへまたはサブジェクトからグループへ）。
- [グループ マップ属性（Group Map Attribute）]：このパラメータは、グループ メンバーシップ情報を含む属性を示します。
- [グループ オブジェクト クラス（Group Object Class）]：このパラメータは、特定のオブジェクトがグループとして認識されることを決定します。
- [グループ検索サブツリー（Group Search Subtree）]：このパラメータは、グループ検索の検索ベースを示します。
- [メンバー タイプ オプション（Member Type Option）]：このパラメータは、グループ メンバー属性にメンバーが保存される方法を指定します（DN として、またはプレーン ユーザ名として）。

LDAP 属性の取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからサブジェクト属性を取得する必要があります。LDAP ID ソースのインスタンスごとに、ID ソースディクショナリが作成されます。これらのディレクトリでは、次のデータ型の属性がサポートされています。

- 文字列
- 符号なし 32 ビット整数
- IPv4 アドレス

符号なし整数および IPv4 属性の場合、Cisco ISE は取得した文字列を対応するデータ型に変換します。変換が失敗した場合、または属性の値が取得されなかった場合、Cisco ISE ではデバッグ メッセージをロギングしますが、認証またはルックアップ プロセスは失敗しません。

変換が失敗した場合、または Cisco ISE で属性の値が取得されない場合に、Cisco ISE で使用できるデフォルトの属性値を任意で設定できます。

LDAP 証明書の取得

ユーザ ルックアップの一部として証明書取得を設定した場合、Cisco ISE は証明書属性の値を LDAP から取得する必要があります。証明書属性の値を LDAP から取得するには、LDAP ID ソースの設定時に、アクセスする属性のリストで証明書属性をあらかじめ設定しておく必要があります。

LDAP グループ メンバーシップ情報の取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからグループ メンバーシップ情報を取得する必要があります。LDAP サーバは、サブジェクト（ユーザまたはホスト）とグループ間の関連付けを次の方法のいずれかで表します。

- グループがサブジェクトを参照：グループ オブジェクトには、サブジェクトを指定する属性が含まれています。サブジェクトの識別子は、次のものとしてグループに供給できます。
  - 識別名
  - プレーン ユーザ名
- サブジェクトがグループを参照：サブジェクト オブジェクトには、所属するグループを指定する属性が含まれています。

LDAP ID ソースには、グループ メンバーシップ情報の取得のために次のパラメータが含まれています。

- [参照方向（Reference direction）]：このパラメータは、グループ メンバーシップを決定するときに使用する方法を指定します（グループからサブジェクトへまたはサブジェクトからグループへ）。

- [グループ マップ属性（Group Map Attribute）]：このパラメータは、グループ メンバーシップ情報を含む属性を示します。
- [グループ オブジェクト クラス（Group Object Class）]：このパラメータは、特定のオブジェクトがグループとして認識されることを決定します。
- [グループ検索サブツリー（Group Search Subtree）]：このパラメータは、グループ検索の検索ベースを示します。
- [メンバー タイプ オプション（Member Type Option）]：このパラメータは、グループ メンバー属性にメンバーが保存される方法を指定します（DN として、またはプレーン ユーザ名として）。

LDAP 属性の取得

ユーザ認証、ユーザ ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからサブジェクト属性を取得する必要があります。LDAP ID ソースのインスタンスごとに、ID ソースディクショナリが作成されます。これらのディレクトリでは、次のデータ型の属性がサポートされています。

- 文字列
- 符号なし 32 ビット整数
- IPv4 アドレス

符号なし整数および IPv4 属性の場合、Cisco ISE は取得した文字列を対応するデータ型に変換します。変換が失敗した場合、または属性の値が取得されなかった場合、Cisco ISE ではデバッグ メッセージをロギングしますが、認証またはルックアップ プロセスは失敗しません。

変換が失敗した場合、または Cisco ISE で属性の値が取得されない場合に、Cisco ISE で使用できるデフォルトの属性値を任意で設定できます。

LDAP 証明書の取得

ユーザ ルックアップの一部として証明書取得を設定した場合、Cisco ISE は証明書属性の値を LDAP から取得する必要があります。証明書属性の値を LDAP から取得するには、LDAP ID ソースの設定時に、アクセスする属性のリストで証明書属性をあらかじめ設定しておく必要があります。

LDAP サーバによって返されるエラー

次のエラーが認証プロセス中に発生する可能性があります。

- 認証エラー：Cisco ISE は、認証エラーを Cisco ISE ログ ファイルに記録します。

  LDAP サーバがバインディング（認証）エラーを返す理由で考えられるのは、次のとおりです。

  - パラメータ エラー：無効なパラメータが入力された

- ユーザアカウントが制限されている（無効、ロックアウト、期限切れ、パスワード期限切れなど）
- 初期化エラー：LDAP サーバのタイムアウト設定を使用して、LDAP サーバでの接続または認証が失敗したと判断する前に Cisco ISE が LDAP サーバからの応答を待つ秒数を設定します。

  LDAP サーバが初期化エラーを返す理由で考えられるのは、次のとおりです。

  - LDAP がサポートされていない。
  - サーバがダウンしている。
  - サーバがメモリ不足である。
  - ユーザに特権がない。
  - 間違った管理者クレデンシャルが設定されている。

外部リソースエラーとして次のエラーがロギングされ、LDAPサーバで考えられる問題が示されます。

- 接続エラーが発生した
- タイムアウトが期限切れになった
- サーバがダウンしている
- サーバがメモリ不足である

未知ユーザ エラーとして次のエラーがロギングされます。

- データベースにユーザが存在しない

ユーザは存在するが送信されたパスワードが無効である場合、無効パスワードエラーとして次のエラーがロギングされます。

- 無効なパスワードが入力された

LDAP ユーザ ルックアップ

Cisco ISE は LDAP サーバを使用したユーザ ルックアップ機能をサポートしています。この機能を使用すると、認証なしでLDAPデータベース内のユーザを検索し、情報を取得できます。ユーザ ルックアップ プロセスには次のアクションが含まれます。

- LDAP サーバでの、要求のユーザ名に一致するエントリの検索
- ポリシーで使用するユーザ グループ メンバーシップ情報の取得
- ポリシーおよび許可プロファイルで使用するように指定された属性の値の取得

LDAP MAC アドレス ルックアップ

Cisco ISE は MAC アドレス ルックアップ機能をサポートしています。この機能を使用すると、認証なしで LDAP データベース内の MAC アドレスを検索し、情報を取得できます。MAC アドレス ルックアップ プロセスには次のアクションが含まれます。

- デバイスの MAC アドレスと一致するエントリの LDAP サーバを検索する
- ポリシーで使用するデバイスの MAC アドレス グループ情報の取得
- ポリシーで使用する指定された属性の値の取得

LDAP ID ソースの追加

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- Cisco ISE は、許可ポリシーで使用するグループおよび属性を取得するためにプライマリ LDAP サーバを常に使用します。このため、プライマリ LDAP サーバはこれらの項目を設定するときに到達可能である必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] >** [LDAP] > [追加（Add）] を選択します。

ステップ 2 値を入力します。

ステップ 3 [送信（Submit）] をクリックして、LDAP インスタンスを作成します。

LDAP ID ソースの設定

次の表では、[LDAP ID ソース（LDAP Identity Sources）] ページのフィールドについて説明します。これらのフィールドを使用して LDAP インスタンスを作成し、これに接続します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** です。

LDAP 一般設定

以下の表では、[一般（General）] タブのフィールドについて説明します。

表 *74 : LDAP* 一般設定

フィールド	使用上のガイドライン
名前（Name）	LDAP インスタンスの名前を入力します。この値は、サブジェクト DN および属性を取得するために検索で使用されます。この値は string 型で、最大長は 64 文字です。
説明（Description）	LDAP インスタンスの説明を入力します。この値は string 型で、最大長は 1024 文字です。
スキーマ（Schema）	次の組み込みのスキーマ タイプのいずれかを選択するか、カスタム スキーマを作成できます。 • Active Directory • Sun Directory Server • Novell eDirectory [スキーマ（Schema）] の隣の矢印をクリックすると、スキーマの詳細を表示できます。 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。
（注）　次のフィールドは、カスタム スキーマを選択した場合にのみ編集できます。	
サブジェクト オブジェクト クラス（Subject Objectclass）	サブジェクト DN および属性を取得するために検索で使用する値を入力します。この値は string 型で、最大長は 256 文字です。
サブジェクト名属性（Subject Name Attribute）	要求内のユーザ名を含む属性の名前を入力します。この値は string 型で、最大長は 256 文字です。
グループ名属性（Group Name Attribute）	[グループ名属性（Group Name Attribute）] フィールドに CN または DN またはサポートされる属性を入力します。 • CN：共通名に基づいて LDAP ID ストア グループを取得します。 • DN：識別名に基づいて LDAP ID ストア グループを取得します。

フィールド	使用上のガイドライン
証明書属性（Certificate Attribute）	証明書定義を含む属性を入力します。証明書ベースの認証の場合、クライアントによって提示された証明書を検証するために、これらの定義が使用されます。
グループ オブジェクト クラス（Group Objectclass）	グループとして認識されるオブジェクトを指定するために、検索に使用する値を入力します。この値は string 型で、最大長は 256 文字です。
グループ マップ属性（Group Map Attribute）	マッピング情報を含む属性を指定します。この属性は、選択した参照方向に基づいて、ユーザまたはグループ属性を指定できます。
サブジェクト オブジェクトにグループへの参照が含まれる（Subject Objects Contain Reference To Groups）	所属するグループを指定する属性がサブジェクト オブジェクトに含まれている場合は、このオプション ボタンをクリックします。
グループ オブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）	サブジェクトを指定する属性がグループ オブジェクトに含まれている場合は、このオプション ボタンをクリックします。この値はデフォルト値です。
グループ内のサブジェクトをメンバー属性に保存（Subjects In Groups Are Stored In Member Attribute As）	（[グループ オブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）] オプション ボタンの選択時に限り使用可能）グループ メンバー属性にメンバーが供給される方法を指定します（デフォルトは DN）。

フィールド	使用上のガイドライン
ユーザ情報属性（User Info Attributes）	デフォルトでは、事前設定された属性が次の組み込みのスキーマタイプのユーザ情報（名、姓、電子メール、電話、地域など）を収集するために使用されます。 • Active Directory • Sun Directory Server • Novell eDirectory 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。 [スキーマ（Schema）] ドロップダウン リストから [カスタム（Custom）] オプションを選択し、要件に基づいてユーザ情報の属性を編集することもできます。

LDAP の接続設定

以下の表では、[接続設定（Connection Settings）] タブのフィールドについて説明します。

表 *75 : LDAP* の接続設定

フィールド	使用上のガイドライン
セカンダリ サーバの有効化（Enable Secondary Server）	プライマリ LDAP サーバに障害が発生した場合にバックアップとして使用するセカンダリ LDAP サーバを有効にする場合は、このオプションをオンにします。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバの設定パラメータを入力する必要があります。
プライマリ サーバとセカンダリ サーバ（Primary and Secondary Servers）	
ホスト名/IP（Hostname/IP）	LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。

フィールド	使用上のガイドライン
ポート（Port）	LDAP サーバがリッスンしている TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバの管理者からポート番号を取得できます。
各 ISE ノードのサーバの指定（Specify server for each ISE node）	プライマリおよびセカンダリ LDAP サーバの hostnames/IP および各 PSN のポートを設定するには、このチェック ボックスをオンにします。 このオプションを有効にすると、導入のすべてのノードを表示するテーブルが表示されます。ノードを選択し、プライマリおよびセカンダリ LDAP サーバの hostname/IP および選択したノードのポートを設定する必要があります。
アクセス（Access）	[匿名アクセス（Anonymous Access）]：LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバではクライアントが区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへの、クライアント読み取りアクセスが許可されます。認証情報をサーバに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。 [認証されたアクセス（Authenticated Access）]：LDAP ディレクトリの検索が管理クレデンシャルによって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。

フィールド	使用上のガイドライン
管理者 DN（Admin DN）	管理者の DN を入力します。管理者 DN は、[ユーザ ディレクトリ サブツリー（User Directory Subtree）] 下のすべての必要なユーザの検索およびグループの検索を行う権限を持つ LDAP アカウントです。指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、該当 LDAP サーバで認証されたユーザのグループ マッピングは失敗します。
パスワード（Password）	LDAP 管理者アカウントのパスワードを入力します。
セキュアな認証（Secure Authentication）	SSL を使用して Cisco ISE とプライマリ LDAP サーバ間の通信を暗号化する場合にクリックします。[ポート（Port）] フィールドに LDAP サーバでの SSL に使用されるポート番号が入力されていることを確認します。このオプションを有効にした場合は、ルート CA を選択する必要があります。
LDAP サーバのルート CA（LDAP Server Root CA）	ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証を有効にします。
サーバ タイムアウト（Server timeout）	プライマリ LDAP サーバでの接続または認証が失敗したと判断する前に Cisco ISE がプライマリ LDAP サーバからの応答を待つ秒数を入力します。有効な値は 1 ～ 99 です。デフォルトは 10 です。
最大管理接続（Max. Admin Connections）	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、ユーザ ディレクトリ サブツリーおよびグループ ディレクトリ サブツリーの下にあるユーザおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です。デフォルトは 20 です。
N 秒ごとに再接続（Force reconnect every N seconds）	このチェック ボックスをオンにし、2 つ目のテキスト ボックスに、サーバを指定された間隔で LDAP 接続を更新するための適切な値を入力します。有効な範囲は 1 ～ 60 分です。

フィールド	使用上のガイドライン
サーバへのバインドをテスト（Test Bind To Server）	LDAP サーバの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバの詳細を編集して再テストします。
フェールオーバー	
常にプライマリ サーバに最初にアクセスする（Always Access Primary Server First）	Cisco ISE の認証と認可のために常にプライマリ LDAP サーバに最初にアクセスするように設定するには、このオプションをクリックします。
経過後にプライマリ サーバにフェールバック（Failback to Primary Server After）	Cisco ISE で接続しようとしたプライマリ LDAP サーバが到達不可能な場合、Cisco ISE はセカンダリ LDAP サーバへの接続を試行します。Cisco ISE に再びプライマリ LDAP サーバを使用するように設定するには、このオプションをクリックし、テキスト ボックスに値を入力します。

[LDAP] の [ディレクトリ構成（Directory Organization）] タブ

次の表では、[ディレクトリ構成（Directory Organization）] タブのフィールドについて説明します。

表 *76 : [LDAP]* の *[*ディレクトリ構成（*Directory Organization*）*]* タブ

フィールド	使用上のガイドライン
サブジェクト検索ベース（Subject Search Base）	すべてのサブジェクトを含むサブツリーの DN を入力します。次に例を示します。 o=corporation.com サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

フィールド	使用上のガイドライン
グループ検索ベース（Group Search Base）	すべてのグループを含むサブツリーの DN を入力します。次に例を示します。 ou = 組織ユニット、ou = 次の組織ユニット、o = corporation.com グループを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。
形式での MAC アドレスの検索（Search for MAC Address in Format）	LDAPデータベースでの検索に使用する、Cisco ISE の MAC アドレス形式を入力します。内部 ID ソースの MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で供給されます。LDAPデータベースのMACアドレスは、異なる形式で供給できます。ただし、Cisco ISE でホスト ルックアップ要求が受信されると、MACアドレスは内部形式からこのフィールドで指定した形式に変換されます。 ドロップダウン リストを使用して、特定の形式でのMACアドレスの検索を有効にします。<*format*> は次のいずれかです。 • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 選択する形式は、LDAP サーバに供給されているMACアドレスの形式と一致している必要があります。

フィールド	使用上のガイドライン
サブジェクト名の先頭から最後に出現する区切り文字まで削除（Strip start of subject name up to the last occurrence of the separator）	ユーザ名からドメインプレフィックスを削除するための適切なテキストを入力します。 ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、そのユーザ名の初めから区切り文字までのすべての文字が削除されます。ユーザ名に、<start_string> ボックスに指定した文字が複数含まれている場合は、Cisco ISE によって最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザ名が DOMAIN\user1 である場合、Cisco ISE によって user1 が LDAP サーバに送信されます。 （注） <start_string> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。
最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip end of subject name from the first occurrence of the separator）	ユーザ名からドメイン サフィックスを削除するための適切なテキストを入力します。 ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、その区切り文字からユーザ名の末尾までのすべての文字が削除されます。ユーザ名に、このフィールドに指定した文字が複数含まれている場合は、Cisco ISE によって最初の区切り文字から文字が削除されます。たとえば、区切り文字が@で、ユーザ名が *user1@domain* であれば、Cisco ISE は *user1* を LDAP サーバに送信します。 （注） *<end_string>* ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。

LDAP グループ設定

表 *77 : LDAP* グループ設定

フィールド	使用上のガイドライン
追加（Add）	[追加（Add）] > [グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）] を選択して LDAP ディレクトリからグループを選択します。 グループの追加を選択した場合は、新しいグループの名前を入力します。ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。選択したグループが [グループ（Groups）] ページに表示されます。

LDAP 属性設定

表 *78 : LDAP* 属性設定

フィールド	使用上のガイドライン
追加（Add）	[追加（Add）] > [属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）] を選択して LDAP サーバから属性を選択します。 属性を追加する場合は、新しい属性の名前を入力します。ディレクトリから選択する場合は、ユーザ名を入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザの属性を取得します。選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

LDAP 詳細設定

以下の表では、[詳細設定（Advanced Settings）] タブのフィールドについて説明します。

表 *79 : LDAP* 詳細設定

フィールド	使用上のガイドライン
[パスワードの変更を有効にする（Enable password change）]	デバイス管理に PAP プロトコルを使用し、ネットワーク アクセスに RADIUS EAP-GTC プロトコルを使用している場合に、パスワードが期限切れになるか、またはパスワードがリセットされるときに、ユーザがパスワードを変更できるようにするには、このチェックボックスをオンにします。サポートされていないプロトコルでは、ユーザ認証が失敗します。このオプションでは、ユーザが次回のログイン時にパスワードを変更できるようにすることもできます。

関連トピック

LDAP ディレクトリ サービス （696 ページ）
LDAP ユーザ認証 （697 ページ）
LDAP ユーザ ルックアップ （702 ページ）
LDAP ID ソースの追加 （703 ページ）

LDAP スキーマの設定

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] を選択します。

ステップ 2 LDAP インスタンスを選択します。

ステップ 3 [全般（General）] タブをクリックします。

ステップ 4 [スキーマ（Schema）] オプションの近くにあるドロップダウン矢印をクリックします。

ステップ 5 [スキーマ（Schema）] ドロップダウン リストから必要なスキーマを選択します。[カスタム（Custom）] オプションを選択して、要件に基づいて属性を更新できます。

事前定義属性は、組み込みスキーマ（Active Directory、Sun directory Server、Novell eDirectory など）に使用されます。事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。

プライマリおよびセカンダリ LDAP サーバの設定

LDAP インスタンスを作成したら、プライマリ LDAP サーバに対する接続を設定する必要があります。セカンダリ LDAP サーバの設定は、オプションです。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集するLDAPインスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）]をクリックします。

ステップ 3 [接続（Connection）] タブをクリックして、プライマリおよびセカンダリ サーバを設定します。

ステップ 4 「LDAP ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 [送信（Submit）] をクリックして接続パラメータを保存します。

LDAP サーバからの属性を取得するための Cisco ISE の有効化

Cisco ISE で LDAP サーバからユーザとグループのデータを取得するには、Cisco ISE で LDAP ディレクトリの詳細を設定する必要があります。LDAP ID ソースでは、次の 3 つの検索が適用されます。

- 管理のためのグループ サブツリーのすべてのグループの検索
- ユーザを特定するためのサブジェクト サブツリーのユーザの検索
- ユーザが所属するグループの検索

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] >** [LDAP] を選択します。

ステップ 2 編集するLDAPインスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）]をクリックします。

ステップ 3 [ディレクトリ構成（Directory Organization）] タブをクリックします。

ステップ 4 「LDAP ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 [送信（Submit）] をクリックして設定を保存します。

LDAP サーバからのグループ メンバーシップ詳細の取得

新しいグループを追加するか、LDAP ディレクトリからグループを選択できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集するLDAPインスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）]をクリックします。

ステップ 3 [グループ（Groups）] タブをクリックします。

ステップ 4 **[追加（Add）]>[グループの追加（Add Group）]** を選択して新しいグループを追加するか、**[追加（Add）]> [ディレクトリからグループを選択（Select Groups From Directory）]** を選択して LDAP ディレクトリからグループを選択します。

a) グループの追加を選択した場合は、新しいグループの名前を入力します。

b) ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。検索条件には、アスタリスク（*）ワイルドカード文字を含めることができます。

ステップ 5 選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

選択したグループが [グループ（Groups）] ページに表示されます。

ステップ 6 グループ選択を保存するには、[送信（Submit）] をクリックします。

（注） Active Directory の組み込みグループは、Active Directory が Cisco ISE の LDAP ID ストアとして設定されているときにはサポートされません。

LDAP サーバからのユーザ属性の取得

許可ポリシーで使用する LDAP サーバからユーザ属性を取得できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集する LDAP インスタンスの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 [属性（Attributes）] タブをクリックします。

ステップ 4 **[追加（Add）] > [属性の追加（Add Attribute）]** を選択して新しい属性を追加するか、**[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）]** を選択して LDAP サーバから属性を選択します。

a) 属性を追加する場合は、新しい属性の名前を入力します。

b) ディレクトリから選択する場合は、例のユーザを入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザの属性を取得します。アスタリスク（*）ワイルドカード文字を使用できます。

Cisco ISE では、属性タイプ IP を手動で追加するときに、ユーザ認証に IPv4 または IPv6 アドレスを使用して LDAP サーバを設定できます。

ステップ 5 選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 属性選択を保存するには、[送信（Submit）] をクリックします。

LDAP ID ソースによるセキュア認証の有効化

LDAP 設定ページで [セキュア認証（Secure Authentication）] オプションを選択すると、Cisco ISE は LDAP ID ソースとのセキュアな通信に SSL を使用します。LDAP ID ソースへのセキュアな接続は以下を使用して確立されます。

- SSL トンネル：SSL v3 または TLS v1（LDAP サーバでサポートされる最も強力なバージョン）を使用

- サーバ認証（LDAP サーバの認証）：証明書ベース
- クライアント認証（Cisco ISE の認証）：なし（管理者のバインドは SSL トンネル内で使用されます）
- 暗号スイート：Cisco ISE でサポートされるすべての暗号スイート

最も強力な暗号化と Cisco ISE がサポートする暗号方式を備えている TLS v1 を使用することを推奨します。

Cisco ISE が LDAP ID ソースと安全に通信できるようにするには、次の手順を実行します。

始める前に

- Cisco ISE は、LDAP サーバに接続する必要があります
- TCP ポート 636 を開く必要があります

ステップ 1 LDAP サーバにサーバ証明書を発行した CA の認証局（CA）チェーン全体を Cisco ISE にインポートします（**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**）。

完全な CA チェーンは、ルート CA 証明書および中間 CA 証明書を参照し、LDAP サーバ証明書は参照しません。

ステップ 2 LDAP ID ソースとの通信時にセキュア認証を使用するように Cisco ISE を設定します（**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]**。[接続設定（Connection Settings）] タブで [セキュア認証（Secure Authentication）] チェックボックスを必ずオンにしてください）。

ステップ 3 LDAP ID ストアでルート CA 証明書を選択します。

ODBC ID ソース

オープン データベース コネクティビティ（ODBC）準拠データベースは、ユーザとエンドポイントを認証する外部 ID ソースとして使用できます。ODBC ID ストアは、ID ストアの順序で、ゲストおよびスポンサーの認証に使用できます。また、BYOD フローにも使用できます。

サポートされているデータベース エンジンは次のとおりです。

- MySQL
- Oracle
- PostgreSQL
- Microsoft SQL Server
- Sybase

ODBC 準拠データベースに対して認証するように Cisco ISE を設定しても、データベースの設定には影響を与えません。データベースを管理するには、データベースのマニュアルを参照してください。

ODBC データベースのクレデンシャルチェック

Cisco ISE は、ODBC データベースに対する 3 つの異なるタイプのクレデンシャルチェックをサポートしています。それぞれのクレデンシャル チェック タイプに適切な SQL ストアドプロシージャを設定する必要があります。ストアドプロシージャは、ODBCデータベースで適切なテーブルをクエリし、ODBCデータベースから出力パラメータやレコードセットを受信するために使用されます。データベースは、ODBCクエリに応答してレコードセットまたは名前付きパラメータのセットを返すことができます。

パスワードは、クリアテキストまたは暗号化形式でODBCデータベースに保存できます。Cisco ISEによって呼び出された場合は、ストアドプロシージャでパスワードをクリアテキストに復号化できます。

クレデンシャル チェック タイプ	ODBC 入力パラメータ	ODBC 出力パラメータ	クレデンシャル チェック	認証プロトコル
ODBC データベースのプレーンテキストパスワード認証	[ユーザ名（Username）] [パスワード（Password）]	結果 グループ アカウント情報 エラー文字列	ユーザ名とパスワードが一致すると、関連するユーザ情報が返されます。	PAP EAP-GTC（PEAP または EAP-FAST の内部メソッドとして） TACACS
ODBC データベースから取得したプレーンテキストパスワード	[ユーザ名（Username）]	結果 グループ アカウント情報 エラー文字列 パスワード	ユーザ名が見つかった場合、そのパスワードと関連するユーザ情報がストアドプロシージャによって返されます。Cisco ISE は、認証方式に基づいてパスワードハッシュを計算し、クライアントから受信したものと比較します。	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2（PEAP または EAP-FAST の内部メソッドとして） TACACS
ルックアップ	[ユーザ名（Username）]	結果 グループ アカウント情報 エラー文字列	ユーザ名が見つかった場合、該当するユーザ情報が返されます。	MAB PEAP、EAP-FAST、EAP-TTLS の高速再接続

（注） 出力パラメータで返されるグループは、Cisco ISE では使用されません。グループの取得ストアドプロシージャによって取得されたグループのみが Cisco ISE で使用されます。アカウント情報は、認証の監査ログにのみ含まれています。

次の表に、ODBC データベース ストアドプロシージャと Cisco ISE 認証結果コードによって返される、結果コード間のマッピングを示します。

（ストアドプロシージャによって返される）結果コード	説明	Cisco ISE 認証結果コード
[0]	CODE_SUCCESS	該当なし（認証成功）
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	失敗しました（Failed）
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	エラー（Error）
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired

（注） Cisco ISE は、このマッピングされた認証結果コードに基づいて実際の認証またはルックアップ操作を実行します。

ODBC データベースからグループと属性を取得するためにストアドプロシージャを使用できます。

プレーンテキストパスワード認証用のレコードセットを返すサンプルのプロシージャ（Microsoft SQL Server 用）

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset]
       @username varchar(64), @password varchar(255)
AS
BEGIN
       IF EXISTS( SELECT  username
       FROM  NetworkUsers
       WHERE  username  = @username
       AND  password  = @password )
       SELECT 0,11,'give full access','No Error'
       FROM  NetworkUsers
       WHERE  username  = @username
       ELSE
```

```
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

プレーンテキストパスワード取得用のレコードセットを返すサンプルのプロシージャ（Microsoft SQL Server 用）

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error',password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

ルックアップ用のレコードセットを返すサンプルのプロシージャ（Microsoft SQL Server 用）

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

プレーン テキスト パスワード認証用のパラメータを返すサンプルのプロシージャ（Microsoft SQL Server 用）

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters]
        @username varchar(64), @password varchar(255), @result INT OUTPUT, @group
varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc',  @errorString='ODBC Authen Error'
END
```

プレーン テキスト パスワード取得用のパラメータを返すサンプルのプロシージャ（Microsoft SQL Server 用）

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters]
       @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
```

```
 varchar(255) OUTPUT, @errorString varchar(255) OUTPUT, @password varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error', @password=password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

ルックアップ用のパラメータを返すサンプルのプロシージャ（Microsoft SQL Server 用）

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters]
       @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
 varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

Microsoft SQL Server からグループを取得するサンプルのプロシージャ

```
CREATE PROCEDURE [dbo].[ISEGroupsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                select 'accountants', 'engineers', 'sales','test_group2'
        end
        else
                set @result = 1
END
```

ユーザ名が「*」の場合にすべてのユーザのすべてのグループを取得するサンプルのプロシージャ（Microsoft SQL Server 用）

```
ALTER PROCEDURE [dbo].[ISEGroupsH]
                @username varchar(64), @result int output
AS
BEGIN
                if @username = '*'
                begin
                                -- if username is equal to '*' then return all existing
 groups
                                set @result = 0
                                select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4'
                end
```

```
                else
                if exists (select * from NetworkUsers where username = @username)
                begin
                                set @result = 0
                                select 'accountants'
                end
                else
                                set @result = 1
END
```

Microsoft SQL Server から属性を取得するサンプルのプロシージャ

```
CREATE PROCEDURE [dbo].[ISEAttrsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                                select phone as phone, username as username, department
 as department, floor as floor, memberOf as memberOf, isManager as isManager from
NetworkUsers where username = @username
        end
        else
                set @result = 1
END
```

ODBC 設定のその他の例

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/211581-Configure-ODBC-on-ISE-2-3-with-Oracle-Da.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200644-Configure-ODBC-on-ISE-2-1-with-PostgreSQ.html

ODBC ID ソースの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] を選択します。

ステップ 2 [ODBC] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [一般（General）] タブで、ODBC ID ソースの名前と説明を入力します。

ステップ 5 [接続（Connection）] タブで、次の詳細情報を入力します。

- ODBC データベースのホスト名または IP アドレス（データベースに非標準 TCP ポートが使用されている場合は、次の形式でポート番号を指定できます。ホスト名または IP アドレス:ポート）
- ODBC データベースの名前

- 管理者のユーザ名およびパスワード（Cisco ISE がこれらのクレデンシャルを使用してデータベースに接続します）
- 秒単位のサーバのタイムアウト（デフォルトは 5 秒）
- 接続の試行（デフォルトは 1）
- データベースタイプを選択します。次のいずれかを実行します。
  - MySQL
  - Oracle
  - PostgreSQL
  - Microsoft SQL Server
  - Sybase

ステップ 6 [テスト接続（Test Connection）] をクリックして ODBC データベースとの接続を確認し、設定された使用例用のストアドプロシージャの存在を確認します。

ステップ 7 [ストアドプロシージャ（Stored Procedures）] タブで、次の詳細情報を入力します。

ステップ 8 [属性（Attributes）] タブに必要な属性を追加します。属性の追加時に、属性名が認証ポリシールールでどのように表示されるかを指定できます。

ステップ 9 [グループ（Groups）] タブにユーザグループを追加します。また、ユーザ名または MAC アドレスを指定して ODBC データベースからグループを取得することもできます。これらのグループは、認証ポリシーで使用できます。

グループおよび属性の名前を変更できます。デフォルトでは、[ISE の名前（Name in ISE）] フィールドに表示される名前は ODBC データベースのものと同じですが、この名前は変更できます。この名前が認証ポリシーで使用されます。

ステップ 10 [送信（Submit）] をクリックします。

RADIUS トークン ID ソース

RADIUS プロトコルをサポートし、ユーザおよびデバイスに認証、許可、アカウンティング（AAA）サービスを提供するサーバは、RADIUS サーバと呼ばれます。RADIUS ID ソースは、サブジェクトとそのクレデンシャルの集合を含み、通信に RADIUS プロトコルを使用する外部 ID ソースです。たとえば、Safeword トークンサーバは、複数のユーザおよびそのクレデンシャルをワンタイム パスワードとして含めることができる ID ソースであり、Safeword トークンサーバによって提供されるインターフェイスでは、RADIUS プロトコルを使用して問い合わせることができます。

Cisco ISE では、RADIUS RFC 2865 準拠のいずれかのサーバが外部 ID ソースとしてサポートされています。Cisco ISE では、複数の RADIUS トークン サーバ ID がサポートされています。

たとえば、RSA SecurID サーバや SafeWord サーバなどです。RADIUS ID ソースは、ユーザを認証するために使用される任意の RADIUS トークン サーバと連携できます。

（注） MAB認証では、プロセスホストルックアップオプションを有効にする必要があります。MAB認証を使用するデバイスはOTPまたはRADIUSトークン（RADIUSトークン サーバ認証に必要）を生成できないため、MAB 認証用に外部 ID ソースとして使用される RADIUS トークン サーバを設定しないことをお勧めします。そのため、認証は失敗します。MAB 要求の処理には、外部 RADIUS サーバ オプションを使用できます。

RADIUS トークン サーバでサポートされる認証プロトコル

Cisco ISE では、RADIUS ID ソースに対して次の認証プロトコルがサポートされています。

- RADIUS PAP
- 内部拡張認証プロトコル汎用トークン カード（EAP-GTC）を含む保護拡張認証プロトコル（PEAP）
- 内部 EAP-GTC を含む EAP-FAST

通信に RADIUS トークン サーバで使用されるポート

RADIUS ID トークン サーバでは、認証セッションに UDP ポートが使用されます。このポートはすべての RADIUS 通信に使用されます。Cisco ISE で RADIUS ワンタイム パスワード（OTP）メッセージを RADIUS 対応トークン サーバに送信するには、Cisco ISE と RADIUS 対応トークン サーバの間のゲートウェイ デバイスが、UDP ポートを介した通信を許可するように設定されている必要があります。UDP ポートは、管理者ポータルを介して設定できます。

RADIUS 共有秘密

Cisco ISE で RADIUS ID ソースを設定するときに、共有秘密を指定する必要があります。この共有秘密情報は、RADIUS トークン サーバ上で設定されている共有秘密情報と同一である必要があります。

RADIUS トークン サーバでのフェールオーバー

Cisco ISE では、複数の RADIUS ID ソースを設定できます。各 RADIUS ID ソースには、プライマリとセカンダリの RADIUS サーバを指定できます。Cisco ISE からプライマリ サーバに接続できない場合は、セカンダリ サーバが使用されます。

RADIUS トークン サーバの設定可能なパスワード プロンプト

RADIUS ID ソースでは、パスワード プロンプトを設定できます。パスワード プロンプトは、管理者ポータルを介して設定できます。

RADIUS トークン サーバのユーザ認証

Cisco ISE は、ユーザ クレデンシャル（ユーザ名とパスコード）を取得し、RADIUS トークン サーバに渡します。また、Cisco ISE は RADIUS トークン サーバ認証処理の結果をユーザに中継します。

RADIUS トークン サーバのユーザ属性キャッシュ

RADIUS トークン サーバでは、デフォルトではユーザ ルックアップはサポートされていません。ただし、ユーザ ルックアップは次の Cisco ISE 機能に不可欠です。

- PEAP セッション再開：この機能によって、認証の成功後、EAP セッションの確立中に PEAP セッションを再開できます。
- EAP/FAST 高速再接続：この機能によって、認証の成功後、EAP セッションの確立中に高速再接続が可能になります。
- TACACS+ 許可：TACACS+ 認証に成功すると発生します。

Cisco ISE では、これらの機能のユーザ ルックアップ要求を処理するために、成功した認証の結果がキャッシュされます。成功した認証すべてについて、認証されたユーザの名前と取得された属性がキャッシュされます。失敗した認証はキャッシュに書き込まれません。

キャッシュは、実行時にメモリで使用可能であり、分散展開の Cisco ISE ノード間で複製されません。管理者ポータルを介してキャッシュの存続可能時間（TTL）制限を設定できます。ID キャッシング オプションを有効にし、エージング タイムを分単位で設定する必要があります。指定した時間、キャッシュはメモリで使用可能です。

ID 順序での RADIUS ID ソース

ID ソース順序で認証順序用の RADIUS ID ソースを追加できます。ただし、属性取得順序用の RADIUS ID ソースを追加することはできません。これは、認証しないで RADIUS ID ソースを問い合わせることはできないためです。RADIUS サーバによる認証中、Cisco ISE では異なるエラーを区別できません。すべてのエラーに対して RADIUS サーバから Access-Reject メッセージが返されます。たとえば、RADIUS サーバでユーザが見つからない場合、RADIUS サーバからは User Unknown ステータスの代わりに Access-Reject メッセージが返されます。

RADIUS サーバがすべてのエラーに対して同じメッセージを返す

RADIUS サーバでユーザが見つからない場合、RADIUS サーバからは Access-Reject メッセージが返されます。Cisco ISE では、管理者ポータルを使用してこのメッセージを [認証失敗

（Authentication Failed）] メッセージまたは [ユーザが見つからない（User Not Found）] メッセージとして設定するためのオプションを使用できます。ただし、このオプションを使用すると、ユーザが未知の状況だけでなく、すべての失敗状況に対して「ユーザが見つからない（User Not Found）」メッセージが返されます。

次の表は、RADIUS ID サーバで発生するさまざまな失敗状況を示しています。

表 *80 :* エラー処理

失敗状況	失敗の理由
認証に失敗	• ユーザが未知である。 • ユーザが不正なパスコードでログインしようとしている。 • ユーザ ログイン時間が期限切れになった。
プロセスの失敗	• RADIUS サーバが Cisco ISE で正しく設定されていない。 • RADIUS サーバが使用できない。 • RADIUS パケットが偽装として検出されている。 • RADIUS サーバとのパケットの送受信の問題。 • タイムアウト。
不明なユーザ	認証が失敗し、[拒否で失敗（Fail on Reject）] オプションが false に設定されている。

Safeword サーバでサポートされる特別なユーザ名の形式

Safeword トークン サーバでは、次のユーザ名フォーマットでの認証がサポートされています。

ユーザ名：Username, OTP

Cisco ISE では、認証要求を受信するとすぐにユーザ名が解析され、次のユーザ名に変換されます。

ユーザ名：Username

Safeword トークン サーバでは、これらの両方のフォーマットがサポートされています。Cisco ISE はさまざまなトークン サーバと連携します。SafeWord サーバを設定する場合、Cisco ISE でユーザ名を解析して指定のフォーマットに変換するには、管理者ポータルで [SafeWord サーバ（SafeWord Server）] チェックボックスをオンにする必要があります。この変換は、要求が

RADIUS トークン サーバに送信される前に、RADIUS トークン サーバ ID ソースで実行されます。

RADIUS トークン サーバでの認証要求と応答

Cisco ISE が RADIUS 対応トークン サーバに認証要求を転送する場合、RADIUS 認証要求には次の属性が含まれます。

- User-Name（RADIUS 属性 1）
- User-Password（RADIUS 属性 2）
- NAS-IP-Address（RADIUS 属性 4）

Cisco ISE は次の応答のいずれかを受信すると想定されます。

- Access-Accept：属性は必要ありませんが、応答には RADIUS トークン サーバの設定に基づいてさまざまな属性が含まれる場合があります。
- Access-Reject：属性は必要ありません。
- Access-Challenge：RADIUS RFC ごとに必要な属性は次のとおりです。
  - State（RADIUS 属性 24）
  - Reply-Message（RADIUS 属性 18）
  - 次の 1 つ以上の属性：Vendor-Specific、Idle-Timeout（RADIUS 属性 28）、Session-Timeout（RADIUS 属性 27）、Proxy-State（RADIUS 属性 33）

    Access-Challenge ではそれ以外の属性は使用できません。

RADIUS トークン ID ソースの設定

次の表では、RADIUS 外部 ID ソースを設定し、それに接続するために使用できる [RADIUS トークン ID ソース（RADIUS Token Identity Sources）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）]** です。

表 *81 : RADIUS* トークン *ID* ソースの設定

フィールド	使用上のガイドライン
名前（Name）	RADIUS トークン サーバの名前を入力します。許容最大文字数は 64 文字です。
説明	RADIUS トークン サーバの説明を入力します。最大文字数は 1024 です。

フィールド	使用上のガイドライン
SafeWord サーバ（SafeWord Server）	RADIUS ID ソースが SafeWord サーバである場合はこのチェックボックスをオンにします。
セカンダリ サーバの有効化（Enable Secondary Server）	プライマリに障害が発生した場合にバックアップとして使用する Cisco ISE のセカンダリ RADIUS トークン サーバを有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにする場合は、セカンダリ RADIUS トークン サーバを設定する必要があります。
常にプライマリ サーバに最初にアクセスする（Always Access Primary Server First）	Cisco ISE が常にプライマリ サーバに最初にアクセスするには、このオプション ボタンをクリックします。
経過後にプライマリ サーバにフォールバック（Fallback to Primary Server after）	プライマリ サーバに到達できない場合に Cisco ISE がセカンダリ RADIUS トークン サーバを使用して認証できる時間（分単位）を指定するには、このオプション ボタンをクリックします。この時間を過ぎると、Cisco ISE はプライマリ サーバに対する認証を再試行します。
プライマリ サーバ（Primary Server）	
ホスト名/アドレス（Host IP）	プライマリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。
共有秘密鍵（Shared Secret）	この接続のプライマリ RADIUS トークン サーバで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	プライマリ RADIUS トークン サーバが受信しているポート番号を入力します。
サーバ タイムアウト（Server timeout）	プライマリ サーバがダウンしていると判断する前に Cisco ISE がプライマリ RADIUS トークン サーバからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	セカンダリ サーバ（定義されている場合）に移動する前、またはセカンダリ サーバが定義されていない場合は要求をドロップする前に、Cisco ISE がプライマリ サーバへの再接続を試行する回数を指定します。

フィールド	使用上のガイドライン
セカンダリ サーバ（Secondary Server）	
ホスト名/アドレス（Host IP）	セカンダリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。
共有秘密鍵（Shared Secret）	この接続のセカンダリ RADIUS トークン サーバで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	セカンダリ RADIUS トークン サーバが受信しているポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは 1812 です。
サーバ タイムアウト（Server timeout）	セカンダリ サーバがダウンしていると判断する前に Cisco ISE がセカンダリ RADIUS トークン サーバからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	要求をドロップする前に Cisco ISE がセカンダリ サーバへの再接続を試行する回数を指定します。

関連トピック

RADIUS トークン ID ソース （722 ページ）
RADIUS トークン サーバの追加 （728 ページ）

RADIUS トークン サーバの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）] > [追加（Add）]** を選択します。

ステップ 2 [一般（General）] タブおよび [接続（Connection）] タブに値を入力します。

ステップ 3 [認証（Authentication）] タブをクリックします。

このタブでは、RADIUS トークン サーバからの Access-Reject メッセージへの応答を制御できます。この応答は、クレデンシャルが無効であること、またはユーザが不明であることのいずれかを意味する場合があります。Cisco ISE は、認証失敗か、またはユーザが見つからないかのいずれかの応答を受け入れます。このタブでは、ID キャッシングを有効にし、キャッシュのエージング タイムを設定することもできます。パスワードを要求するプロンプトを設定することもできます。

a) RADIUS トークン サーバからの Access-Reject 応答を認証失敗として処理する場合は、[拒否を「認証失敗」として処理（Treat Rejects as 'authentication failed'）] オプション ボタンをクリックします。
b) RADIUS トークン サーバからの Access-Reject 応答を未知ユーザ エラーとして処理する場合は、[拒否を「ユーザが見つからない」として処理（Treat Rejects as 'user not found'）] オプション ボタンをクリックします。

ステップ 4 RADIUS トークン サーバとの最初の認証の成功の後、Cisco ISE でキャッシュにパスコードを保存し、設定された期間内に発生した後続の認証に対しキャッシュされたユーザのクレデンシャルを使用する場合、[パスコード キャッシングの有効化（Enable Passcode Caching）] チェック ボックスをオンにします。

パスコードをキャッシュ内に保存する必要がある秒数を [エージング タイム（Aging Time）] フィールドに入力します。この期間内にユーザは同じパスコードで複数回の認証を行うことができます。デフォルト値は 30 秒です。有効な範囲は 1 ～ 300 秒です。

（注） Cisco ISE は、認証が初めて失敗した後でキャッシュをクリアします。ユーザは新しい有効なパスコードを入力する必要があります。

（注） EAP-FAST-GTC などの、パスコードの暗号化をサポートするプロトコルを使用する場合にのみこのオプションを有効にすることを強く推奨します。RADIUS トークン サーバでサポートされている認証プロトコルについては、次を参照してください。RADIUS トークン サーバでサポートされる認証プロトコル （723 ページ）

ステップ 5 [許可（Authorization）] タブをクリックします。

このタブでは、Cisco ISE への Access-Accept 応答を送信中に RADIUS トークン サーバによって返されるこの属性に対して表示される名前を設定できます。この属性は、許可ポリシー条件で使用できます。デフォルト値は CiscoSecure-Group-Id です。

（注） 外部 ID ソースから Access-Accept で属性を送信する場合、外部 ID ソースは属性名および値として <ciscoavpair> を ACS 形式（<attrname>=<attrvalue>）で送信する必要があります。<attrname> は [許可（Authorization）] タブで設定します。

ステップ 6 [送信（Submit）] をクリックします。

RADIUS トークン サーバの削除

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ID ソース順序に含まれる RADIUS トークン サーバを選択していないことを確認します。ID ソース順序に含まれる RADIUS トークン サーバを削除用に選択した場合、削除操作は失敗します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）]** を選択します。

ステップ 2 削除する RADIUS トークン サーバの隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして、選択した RADIUS トークン サーバを削除します。

削除する RADIUS トークン サーバを複数選択し、その 1 つが ID ソース順序で使用されている場合、削除操作は失敗し、いずれの RADIUS トークン サーバも削除されません。

RSA ID ソース

Cisco ISE では、外部データベースとして RSA SecurID サーバがサポートされています。RSA SecurID の 2 要素認証は、ユーザの PIN と、タイム コード アルゴリズムに基づいて使い捨てのトークン コードを生成する個別に登録された RSA SecurID トークンで構成されます。異なるトークン コードが固定間隔（通常は 30 または 60 秒ごと）で生成されます。RSA SecurID サーバでは、この動的な認証コードが検証されます。各 RSA SecurID トークンは固有であり、過去のトークンに基づいて将来のトークンの値を予測することはできません。そのため、正しいトークン コードが PIN とともに提示された場合、その人が有効なユーザである確実性が高くなります。したがって、RSA SecurID サーバでは、従来の再利用可能なパスワードよりも信頼性の高い認証メカニズムが提供されます。

Cisco ISE では、次の RSA ID ソースがサポートされています。

- RSA ACE/Server 6.x シリーズ
- RSA Authentication Manager 7.x および 8.0 シリーズ

次のいずれかの方法で、RSA SecurID 認証テクノロジーと統合できます。

- RSA SecurID エージェントの使用：ユーザは、RSA のネイティブ プロトコルによってユーザ名およびパスコードで認証されます。
- RADIUS プロトコルの使用：ユーザは、RADIUS プロトコルによってユーザ名およびパスコードで認証されます。

Cisco ISE の RSA SecurID トークン サーバは、RSA SecurID 認証テクノロジーと RSA SecurID エージェントを使用して接続します。

Cisco ISE では、1 つの RSA 領域だけがサポートされています。

Cisco ISE と RSA SecurID サーバの統合

Cisco ISE と RSA SecurID サーバを接続するには、次の 2 つの管理ロールが必要です。

- RSA サーバ管理者：RSA システムおよび統合を設定および維持します

- Cisco ISE 管理者：Cisco ISE を RSA SecurID サーバに接続するように設定し、設定を維持します

ここでは、Cisco ISE に RSA SecurID サーバを外部 ID ソースとして接続するために必要なプロセスについて説明します。RSA サーバについての詳細は、RSA に関するドキュメントを参照してください。

Cisco ISE の RSA 設定

RSA 管理システムでは sdconf.rec ファイルが生成されます。このファイルは RSA システム管理者によって提供されます。このファイルを使用すると、Cisco ISE サーバを領域内の RSA SecurID エージェントとして追加できます。このファイルを参照して Cisco ISE に追加する必要があります。プライマリ Cisco ISE サーバは、複製のプロセスによってこのファイルをすべてのセカンダリ サーバに配布します。

RSA SecurID サーバに対する RSA エージェント認証

sdconf.rec ファイルがすべての Cisco ISE サーバにインストールされると、RSA エージェント モジュールが初期化され、RSA 生成のクレデンシャルによる認証が各 Cisco ISE サーバで実行されます。展開内の各 Cisco ISE サーバ上のエージェントが正常に認証されると、RSA サーバとエージェント モジュールは securid ファイルをダウンロードします。このファイルは Cisco ISE ファイル システムに存在し、RSA エージェントによって定義された既知の場所にあります。

分散 Cisco ISE 環境の RSA ID ソース

分散 Cisco ISE 環境で RSA ID ソースを管理するには、次の操作が必要です。

- sdconf.rec および sdopts.rec ファイルのプライマリ サーバからセカンダリ サーバへの配布。
- securid および sdstatus.12 ファイルの削除。

Cisco ISE 展開の RSA サーバの更新

Cisco ISE で sdconf.rec ファイルを追加した後、RSA サーバを廃止する場合、または新しい RSA セカンダリ サーバを追加する場合、RSA SecurID 管理者は sdconf.rec ファイルを更新することがあります。更新されたファイルは RSA SecurID 管理者によって提供されます。更新されたファイルによって Cisco ISE を再設定できます。Cisco ISE では、更新されたファイルが複製プロセスによって展開内のセカンダリ Cisco ISE サーバに配布されます。Cisco ISE では、まずファイル システムのファイルを更新し、RSA エージェント モジュールに合わせて調整して再起動プロセスを適切に段階的に行います。sdconf.rec ファイルが更新されると、sdstatus.12 および securid ファイルがリセット（削除）されます。

自動 RSA ルーティングの上書き

領域内に複数の RSA サーバを持つことができます。sdopts.rec ファイルはロード バランサの役割を果たします。Cisco ISE サーバと RSA SecurID サーバはエージェント モジュールを介して動作します。Cisco ISE に存在するエージェント モジュールは、領域内の RSA サーバを最大限

に利用するためにコストベースのルーティングテーブルを保持します。ただし、領域の各Cisco ISE サーバの手動設定を使用してこのルーティングを上書きするには、管理者ポータルで sdopts.rec と呼ばれるテキスト ファイルを使用します。このファイルの作成方法については、RSA に関するドキュメントを参照してください。

RSA ノード秘密リセット

securid ファイルは秘密ノード キー ファイルです。RSA が最初に設定されると、RSA では秘密を使用してエージェントが検証されます。Cisco ISE に存在する RSA エージェントが RSA サーバに対して初めて正常に認証されると、securid と呼ばれるファイルがクライアント マシン上に作成され、このファイルを使用して、マシン間で交換されるデータが有効であることが確認されます。展開内の特定の Cisco ISE サーバまたはサーバのグループから securid ファイルを削除する必要がある場合があります（たとえば、RSA サーバでのキーのリセット後など）。領域に対する Cisco ISE サーバからこのファイルを削除するには、Cisco ISE 管理者ポータルを使用できます。Cisco ISE の RSA エージェントが次回正常に認証されたとき、新しい securid ファイルが作成されます。

（注） Cisco ISE の最新リリースへのアップグレード後に認証が失敗した場合は、RSA 秘密をリセットします。

RSA の自動可用性のリセット

sdstatus.12 ファイルは、領域内の RSA サーバのアベイラビリティに関する情報を提供します。たとえば、いずれのサーバがアクティブで、いずれのサーバがダウンしているかに関する情報を提供します。エージェント モジュールは領域内の RSA サーバと連携して、このアベイラビリティ ステータスを維持します。この情報は、sdstatus.12 ファイルに連続的に表示されます。このファイルは、Cisco ISE ファイル システムの既知の場所に供給されます。このファイルは古くなり、現在のステータスが反映されていないことがあります。その場合、現在のステータスが反映されるように、このファイルを削除する必要があります。特定の領域に対する固有の Cisco ISE サーバからファイルを削除するには、管理者ポータルを使用できます。Cisco ISE は RSA エージェントに合わせて調整して、再起動が正しく段階的に行われるようにします。

アベイラビリティ ファイル sdstatus.12 は、securid ファイルがリセットされるか、sdconf.rec または sdopts.rec ファイルが更新されるたびに削除されます。

RSA SecurID ID ソースの設定

次の表では、RSA SecurID ID ソースを作成し、それに接続するために使用できる [RSA SecurID ID ソース（RSA SecurID Identity Sources）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID]** です。

RSA プロンプトの設定

次の表では、[RSA プロンプト（RSA Prompts）] タブ内のフィールドについて説明します。

表 *82 : RSA* プロンプトの設定

フィールド	使用上のガイドライン
パスコード プロンプトの入力（Enter Passcode Prompt）	パス コードを取得するテキスト文字列を入力します。
次のトークン コードの入力（Enter Next Token Code）	次のトークンを要求するテキスト文字列を入力します。
PIN タイプの選択（Choose PIN Type）	PIN タイプを要求するテキスト文字列を入力します。
システム PIN の受け入れ（Accept System PIN）	システム生成の PIN を受け付けるテキスト文字列を入力します。
英数字 PIN の入力（Enter Alphanumeric PIN）	英数字 PIN を要求するテキスト文字列を入力します。
数値 PIN の入力（Enter Numeric PIN）	数値 PIN を要求するテキスト文字列を入力します。
PIN の再入力（Re-enter PIN）	ユーザに PIN の再入力を要求するテキスト文字列を入力します。

RSA メッセージ設定（RSA Message Settings）

次の表では、[RSA メッセージ（RSA Messages）] タブ内のフィールドについて説明します。

表 *83 : RSA* メッセージ設定（*RSA Messages Settings*）

フィールド	使用上のガイドライン
システム PIN メッセージの表示（Display System PIN Message）	システム PIN メッセージのラベルにするテキスト文字列を入力します。
システム PIN 通知の表示（Display System PIN Reminder）	ユーザに新しい PIN を覚えるように通知するテキスト文字列を入力します。
数字を入力する必要があるエラー（Must Enter Numeric Error）	PIN には数字のみを入力するようにユーザに指示するメッセージを入力します。
英数字を入力する必要があるエラー（Must Enter Alpha Error）	PIN には英数字のみを入力するようにユーザに指示するメッセージを入力します。

フィールド	使用上のガイドライン
PIN 受け入れメッセージ（PIN Accepted Message）	ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
PIN 拒否メッセージ（PIN Rejected Message）	ユーザの PIN がシステムによって拒否されたときに表示されるメッセージを入力します。
ユーザの PIN が異なるエラー（User Pins Differ Error）	ユーザが不正な PIN を入力したときに表示されるメッセージを入力します。
システム PIN 受け入れメッセージ（System PIN Accepted Message）	ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
不正パスワード長エラー（Bad Password Length Error）	ユーザが指定した PIN が、PIN 長ポリシーで指定されている範囲に収まらない場合に表示されるメッセージを入力します。

関連トピック

RSA ID ソース （730 ページ）
Cisco ISE と RSA SecurID サーバの統合 （730 ページ）
RSA ID ソースの追加 （734 ページ）

RSA ID ソースの追加

RSA ID ソースを作成するには、RSA コンフィギュレーション ファイル（sdconf.rec）をインポートする必要があります。RSA 管理者から sdconf.rec ファイルを取得する必要があります。このタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

RSA ID ソースを追加するには、次のタスクを実行します。

RSA コンフィギュレーション ファイルのインポート

Cisco ISE に RSA ID ソースを追加するには、RSA コンフィギュレーション ファイルをインポートする必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）]** を選択します。

ステップ 2 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから新しい sdconf.rec ファイルまたは更新された sdconf.rec ファイルを選択します。

初めて RSA ID ソースを作成する場合、[新しい sdconf.rec ファイルのインポート（Import new sdconf.rec file）] フィールドは必須フィールドです。これ以降は、既存の sdconf.rec ファイルを更新されたファイルで置き換えることができますが、既存のファイルの置き換えは任意です。

ステップ 3 サーバのタイムアウト値を秒単位で入力します。Cisco ISE はタイムアウトになる前に、指定された秒数 RSA サーバからの応答を待ちます。この値には、1 ～ 199 の任意の整数を指定できます。デフォルト値は 30 秒です。

ステップ 4 PIN が変更された場合に強制的に再認証するには、[変更 PIN で再認証（Reauthenticate on Change PIN）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

Cisco ISE は、次のシナリオもサポートします。

- Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット。
- RSA ID ソースの認証制御オプションの設定。

Cisco ISE サーバのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット

ステップ 1 Cisco ISE サーバにログインします。

ステップ 2 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）]** を選択します。

ステップ 3 [RSA インスタンス ファイル（RSA Instance Files）] タブをクリックします。

このページには、展開内のすべての Cisco ISE サーバの sdopts.rec servers ファイルが一覧表示されます。

ユーザが RSA SecurID トークン サーバに対して認証されると、ノードのシークレット ステータスは [作成済み（Created）] と表示されます。ノードのシークレット ステータスは、[作成済み（Created）] または [未作成（Not Created）] のどちらかになります。消去されると、ノードのシークレット ステータスは [未作成（Not Created）] と表示されます。

ステップ 4 特定の Cisco ISE サーバの sdopts.rec ファイルの横にあるオプション ボタンをクリックし、[オプション ファイルの更新（Update Options File）] をクリックします。

[現在のファイル（Current File）] 領域に既存のファイルが表示されます。

ステップ 5 次のいずれかを実行します。

- [RSA エージェントが保持する自動ロード バランシング ステータスを使用（Use the Automatic Load Balancing status maintained by the RSA agent）]：RSA エージェントでロード バランシングを自動的に管理する場合は、このオプションを選択します。
- [次で選択された sdopts.rec ファイルで自動ロード バランシング ステータスを上書き（Override the Automatic Load Balancing status with the sdopts.rec file selected below）]：特定のニーズに基づいて手動でロード バランシングを設定する場合は、このオプションを選択します。このオプションを選択する場合は、[参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから新しい sdopts.rec ファイルを選択する必要があります。

ステップ 6 [OK] をクリックします。

ステップ 7 Cisco ISE サーバに対応する行をクリックして、そのサーバの securid および sdstatus.12 ファイルをリセットします。

a) ドロップダウン矢印をクリックし、[securid ファイルのリセット（Reset securid File）] 列と [sdstatus.12 ファイルのリセット（Reset sdstatus.12 File）] 列の [送信で削除（Remove on Submit）] を選択します。

（注） [sdstatus.12 ファイルのリセット（Reset sdstatus.12 File）] フィールドはユーザのビューから非表示になっています。このフィールドを表示するには、最も内側のフレームで垂直および水平スクロール バーを使用して、下にスクロールし、次に右にスクロールします。

b) この行で [保存（Save）] をクリックして変更を保存します。

ステップ 8 [**保存（Save**）] をクリックします。

RSA ID ソースの認証制御オプションの設定

Cisco ISE がどのように認証失敗を定義し、ID キャッシングを有効にするかを指定できます。RSA ID ソースでは、「認証失敗」エラーと「ユーザが見つからない」エラーは区別されず、Access-Reject 応答が送信されます。

Cisco ISE で、要求の処理および失敗のレポート中に、これらの失敗をどのように処理するかを定義できます。ID キャッシングによって、Cisco ISE では、Cisco ISE サーバに対して認証に失敗した要求を 2 回目に処理できます。前の認証から取得された結果および属性を、キャッシュで利用できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）]** を選択します。

ステップ 2 [認証制御（Authentication Control）] タブをクリックします。

ステップ 3 次のいずれかを実行します。

- [拒否を「認証失敗」として処理（Treat Rejects as "authentication failed"）]：拒否された要求を認証失敗として処理する場合は、このオプションを選択します。
- [拒否を「ユーザが見つからない」として処理（Treat Rejects as "user not found"）]：拒否された要求をユーザが見つからないエラーとして処理する場合は、このオプションを選択します。

ステップ 4 最初に認証が成功した後に Cisco ISE がキャッシュにパスコードを保存し、設定された期間内に認証が行われた場合にキャッシュされたユーザ クレデンシャルを後続の認証のために使用するようにする場合は、[パスコード キャッシュの有効化（Enable Passcode Caching）] チェック ボックスにマークを付けます。

パスコードをキャッシュ内に保存する必要がある秒数を [エージング タイム（Aging Time）] フィールドに入力します。この期間内にユーザは同じパスコードで複数回の認証を行うことができます。デフォルト値は 30 秒です。有効な範囲は 1 ～ 300 秒です。

（注） Cisco ISE は、認証が初めて失敗した後でキャッシュをクリアします。ユーザは新しい有効なパスコードを入力する必要があります。

（注） EAP-FAST-GTC などの、パスコードの暗号化をサポートするプロトコルを使用する場合にのみこのオプションを有効にすることを強く推奨します。

ステップ 5 ISE で、Cisco ISE サーバに対して認証に失敗した要求を 2 回目に処理する場合は、[IDキャッシングの有効化（Enable Identity Caching）] チェックボックスをオンにします。

ステップ 6 [保存（**Save**）] をクリックして、設定を保存します。

RSA プロンプトの設定

Cisco ISE では、RSA SecurID サーバに送信される要求の処理中にユーザに表示される RSA プロンプトを設定できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID]** を選択します。

ステップ 2 [プロンプト（Prompts）] をクリックします。

ステップ 3 「RSA SecurID ID ソースの設定」の説明に従って、値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

RSA メッセージの設定

Cisco ISE では、RSA SecurID サーバに送信される要求の処理中にユーザに表示されるメッセージを設定できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID]** を選択します。

ステップ 2 [プロンプト（Prompts）] をクリックします。

ステップ 3 [メッセージ（Messages）] タブをクリックします。

ステップ 4 「RSA SecurID ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 [送信（Submit）] をクリックします。

外部 ID ソースとしての SAMLv2 ID プロバイダ

Security Assertion Markup Language（SAML）は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のアプリケーションにシームレスにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。SAML により、ID プロバイダ（IdP）とサービスプロバイダー（この場合はISE）の間で、セキュリティ認証情報を交換できます。

SAML シングル サインオン（SSO）は、IdP とサービス プロバイダーの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。サービス プロバイダは IdP のユーザ情報を信頼して、さまざまなサービスやアプリケーションにアクセスできるようにします。

SAML SSO を有効にすると、次のようないくつかの利点が得られます。

- 異なるユーザ名とパスワードの組み合わせを入力する必要がなくなるため、パスワードの劣化が軽減します。
- 同じ ID に資格情報を再入力する時間が省けるため、生産性が向上します。
- アプリケーションをホストしているお使いのシステムからサードパーティのシステムに、認証を転送します。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

IdPは、ユーザ、システム、またはサービスのID情報を作成、維持、管理する認証モジュールです。IdPは、ユーザクレデンシャルを保管、検証し、ユーザがサービス プロバイダーの保護リソースにアクセスできる SAML 応答を生成します。

（注） IdP サービスをよく理解している必要があります。現在インストールされていて、操作可能であることを確認してください。

SAML SSO は次のポータルでサポートされます。

- ゲスト ポータル（スポンサー付きおよびアカウント登録）
- スポンサー ポータル
- デバイス ポータル
- 証明書プロビジョニング ポータル

BYOD ポータルでは外部 ID ソースとして IdP を選択できませんが、ゲスト ポータルでは IdP を選択し、BYOD フローをイネーブルにできます。

Cisco ISE は SAMLv2 に準拠しており、Base64 でエンコードされた証明書を使用するすべての SAMLv2 準拠 IdP をサポートしています。次に示す IdP が Cisco ISE でテストされました。

- Oracle Access Manager（OAM）
- Oracle Identity Federation（OIF）
- SecureAuth
- PingOne
- PingFederate
- Azure Active Directory

IdP は、ID ソース順序に追加できません。

指定された時間（デフォルトでは5分）にアクティビティがない場合は、SSOセッションが終了し、セッション タイムアウトのエラー メッセージが表示されます。

ポータルの [エラー（Error）] ページに [再度サインオン（Sign On Again）] ボタンを追加する場合は、[ポータルエラー（Portal Error）] ページの [オプションコンテンツ（Optional Content）] フィールドに次の JavaScript を追加します。

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'"
type="button">再サインオン</button>
```

SAML ID プロバイダーの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 証明書が IdP で自己署名されていない場合は、信頼できる証明書ストアに認証局（CA）証明書をインポートします。[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）] の順に選択し、CA 証明書をインポートします。

ステップ 2 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）][ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [外部 ID ソース（External Identity Sources）] を選択します。

ステップ 3 [SAML ID プロバイダー（SAML Id Providers）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [SAML ID プロバイダー（SAML Identity Provider）] ページで、次の詳細情報を入力します。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 [ポータル設定（Portal Settings）] ページ（ゲスト ポータル、証明書プロビジョニングまたはデバイス ポータル）に移動して、[認証方式（Authentication Method）] フィールドでそのポータルにリンクする IdP を選択します。

[ポータル設定（Portal Settings）] ページにアクセスするには、次の手順を実行します。

- ゲスト ポータル：**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals and Components）]** > **[ゲストポータル（Guest Portals）]** > **[作成、編集または複製（Create, Edit, or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ポータル設定（Portal Settings）]** の順に選択します（『』の「クレデンシャルを持つゲスト ポータルのポータル設定」のセクションクレデンシャルを持つゲスト ポータルのポータル設定 （447 ページ）を参照してください）。
- スポンサー ポータル：**[ワークセンター（Work Centers）]** > **[ゲストアクセス（Guest Access）]** > **[ポータルとコンポーネント（Portals and Components）]** > **[スポンサーポータル（Sponsor Portals）]** > **[作成、編集または複製（Create, Edit, or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ポータル設定（Portal Settings）]** の順に選択します（スポンサー ポータルのポータル設定 （466 ページ）を参照してください）。
- デバイス ポータル：[ワークセンター（Work Centers）] > [BYOD] > [設定（Configure）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit, or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）] [管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイス（My Devices）] > [作成、編集または複製（Create, Edit, or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]を選択します（デバイス ポータルのポータル設定 （1484 ページ）を参照してください）。
- 証明書プロビジョニング ポータル：[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）] > [作成、編集または複製（Create, Edit, or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）] の順に選択します（「証明書プロビジョニング ポータルのポータル設定」を参照してください）。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [SAML ID プロバイダー（SAML Id Providers）][ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [外部 ID ソース（External Identity Sources）] > [SAML ID プロバイダー（SAML Id Providers）] を選択します。そのポータルにリンクする IdP を選択し、[編集（Edit）] をクリックします。

ステップ 10 （オプション）[サービス プロバイダー情報（Service Provider Info）] タブで、ロード バランサの詳細を追加します。ISE ノードの前にロード バランサを追加することで、ID プロバイダーの設定を簡素化し、ISE ノードの負荷を最適化できます。

ロード バランサはソフトウェアベースまたはハードウェアベースのアプライアンスである可能性があります。導入の ISE ノードに要求を転送できる必要があります（[ポータル設定（Portal Settings）] ページで指定されたポートを使用して）。

ロード バランサを使用する場合は、ロード バランサの URL のみがサービス プロバイダーのメタデータ ファイルで提供されます。ロード バランサが追加されていない場合は、複数の AssertionConsumerService URL がサービス プロバイダーのメタデータ ファイルに含まれます。

（注） ポータル FQND 設定でロード バランサに同じ IP アドレスを使用しないようにすることが推奨されます。

ステップ 11 [サービスプロバイダー情報（Service Provider Info）] タブで、[エクスポート（Export）] をクリックして、サービス プロバイダーのメタデータ ファイルをエクスポートします。

エクスポートされたメタデータには、Cisco ISE の署名証明書が含まれています。署名証明書は、選択したポータルの証明書と同一です。

エクスポートされたメタデータの ZIP ファイルには、各 IdP の設定に関する基本的な説明を含む Readme ファイルが含まれています（Azure Active Directory、PingOne、PingFederate、SecureAuth、OAM など）。

（注） ロードバランサが設定されていない、または次のようなポータル設定に変更がある場合は、サービス プロバイダーのメタデータを再度エクスポートする必要があります。

- 新しい ISE ノードが登録された場合
- ノードのホスト名または IP アドレスが変更された場合
- デバイス、スポンサー、または証明書プロビジョニング ポータルの完全修飾ドメイン名（FQDN）が変わりました
- ポートまたはインターフェイス設定が変更された

更新されたメタデータが再エクスポートされない場合、ユーザ認証が IdP 側で失敗する可能性があります。

ステップ 12 ダイアログボックスで [参照（Browse）] をクリックして、圧縮ファイルをローカルに保存します。メタデータ ファイルのフォルダを解凍します。フォルダを解凍すると、ポータルの名前が付いたメタデータ ファイルを取得します。メタデータ ファイルには、プロバイダー ID とバインディング URI が含まれています。

ステップ 13 管理ユーザとして IdP にログインし、サービス プロバイダーのメタデータ ファイルをインポートします。サービス プロバイダーのメタデータ ファイルをインポートする方法の詳細については、ID プロバイダーのメタデータファイルをインポートする方法の詳細については、IDプロバイダーのユーザユーザマニュアルを参照してください。

ステップ 14 [グループ（Groups）] タブで、必要なユーザ グループを追加します。

[グループ メンバーシップ属性（Group Membership Attribute）] フィールドにユーザのグループ メンバーシップを指定するアサーション属性を入力します。

ステップ 15 [属性（Attributes）] タブにユーザ属性を追加します。属性を追加するときに、属性が IdP から返されたアサーションでどのように表示されるかを指定できます。[ISE の名前（Name in ISE）] フィールドに指定した名前はポリシー ルールに表示されます。属性でサポートされているのは、次のデータ型です。

- 文字列
- 整数（Integer）
- IPv4
- ブール値

（注） グループと属性の追加は必須ではありません。これらのグループと属性は、ポリシーとルールの設定に使用できます。スポンサー ポータルを使用している場合は、グループを追加してこれらのグループを選択し、スポンサー グループの設定を構成することができます。

ステップ 16 [詳細設定（Advanced Settings）] タブで、次のオプションを設定します。

- [ID属性（Identity Attribute）]：認証中のユーザの ID を指定する属性を選択します。[属性（Attribute）] ドロップダウン リストからサブジェクト名属性または属性を選択できます。

  （注） Cisco ISE は、件名（NameID）が一時的なまたは永続的な形式で含まれる SAML IdP 応答をサポートしていません。このような方法が使用され、認証が失敗する場合、Cisco ISE は SAML IdP 応答からユーザ名属性アサーションを取得できません。

- [メール属性（Email attribute）]：スポンサーの電子メール アドレスを含む属性を選択します。これには、セルフサービスのゲストの要求とスポンサーが一致する必要があります。
- [メール属性（Email attribute）]：ユーザの電子メール アドレスを返すアサーション属性を選択します。スポンサー付きゲストのリストが 1 人のスポンサーに承認されるようにフィルタリング（制限）する場合は、メール属性を設定する必要があります。
- 複数値属性の場合は、次のいずれかのオプションを選択します。
  - [個別のXML要素で各値（Each value in a separate XML element）]：個別の XML 要素で同じ属性の複数の値を IdP が返すには、このオプションをクリックします。
  - [単一の XML 要素で複数の値（Multiple values in a single XML element）]：単一の XML 要素で複数値を IdP が返すには、このオプションをクリックします。テキスト ボックスにデリミタを指定できます。
- ログアウト設定（Logout Settings）
  - [ログアウト要求の署名（Sign Logout Requests）]：ログアウト要求に署名されるようにする場合は、このチェックボックスをオンにします。このオプションは、OAM および OIF では表示されません。

    （注） SecureAuth は SAML ログアウトをサポートしていません。

  - [ログアウト URL（Logout URL）]：ロード バランサが設定されていなければ、このオプションは OAM および OIF だけに表示されます。ユーザがスポンサー ポータルまたはデバイス ポータルからログアウトすると、ユーザは SSO セッションを終了するために IdP でログアウト URL にリダイレクトされ、その後、ログイン ページにリダイレクトされます。
  - [リダイレクト パラメータ名（Redirect Parameter Name）]：ロード バランサが設定されていなければ、このオプションは OAM および OIF だけに表示されます。リダイレクト パラメータは、ユーザがログアウト後にリダイレクトされる必要があるログイン ページの URL を渡すために使用されます。リダイレクト パラメータ名は、IdP に基づいて異なる場合があります（たとえば end_url や returnURL）。このフィールドは大文字と小文字が区別されます。

    ログアウトが正常に動作しない場合は、ログアウト URL およびリダイレクト パラメータ名について、ID プロバイダーのマニュアルを確認してください。マニュアルを確認してください。

ステップ 17 [送信（Submit）] をクリックします。

例

Ping Federate の設定の例については、『**Configure ISE 2.1 Guest Portal with PingFederate SAML SSO**』を参照してください。

ID プロバイダの削除

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

削除する IdP がいずれのポータルにもリンクされていないことを確認します。IdP がポータルにリンクされている場合、削除操作は失敗します。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [SAML ID プロバイダー（SAML Id Providers）][ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [外部 ID ソース（External Identity Sources）] > [SAML ID プロバイダー（SAML Id Providers）] を選択します。

ステップ 2 削除する IdP の隣のチェックボックスをオンにして、[削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして、選択した IdP を削除します。

認証失敗ログ

SAML ID ストアに対する認証が失敗し、IdP がユーザを ISE ポータルに（SAML 応答を通じて）リダイレクトすると、ISE は認証ログに障害の理由を報告します。ゲスト ポータルで（BYOD フローの有効無効に関係なく）、認証の失敗の原因を知るために、RADIUS Livelog（[操作（Operations）] > [RADIUS] > [ライブ ログ（Live Logs）]）を確認できます。ポータルおよびスポンサー ポータル認証失敗の原因を把握するためには、デバイス ポータルおよびスポンサー ポータルで、デバイス ログイン/監査レポートとスポンサー ログイン/監査レポート（[操作（Operations）] > [レポート（Reports）] > [ゲスト（Guest）]）を確認できます。

ログアウトで障害が発生した場合、My Devices、スポンサーおよびゲスト ポータルの障害の原因を知るためにレポートおよびログを確認することができます。

認証が失敗する原因には次のものが考えられます。

- SAML 応答の解析エラー
- SAML 応答の検証エラー（不正な発行者など）
- SAML アサーションの検証エラー（誤った対象者など）
- SAML 応答署名の検証エラー（不正な署名など）
- IdP 署名証明書のエラー（失効した証明書など）

（注） Cisco ISE は、暗号化されたアサーションを含む SAML 応答をサポートしていません。IdP で設定すると、ISE に次のエラー メッセージが表示されます：`FailureReason=24803 Unable to find 'username' attribute assertion`。

認証に失敗した場合は、認証ログの「DetailedInfo」属性を確認することを推奨します。この属性では、障害理由に関する追加情報が提供されます。

ID ソース順序

ID ソース順序は、Cisco ISE がそれぞれ異なるデータベース内でユーザ クレデンシャルを検索する順序を定義します。

Cisco ISE に接続されている 2 つ以上のデータベースにユーザ情報がある場合、Cisco ISE でこれらの ID ソース内の情報を検索する順序を定義できます。一致が見つかると、Cisco ISE はそれ以上の検索を行いませんが、クレデンシャルを評価し、ユーザに結果を返します。このポリシーは最初の一致ポリシーです。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲスト ユーザがローカル WebAuth を使用して認証できるようにするには、ゲスト ポータル認証ソースと ID ソース順序に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）]** を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストのデータベースを並べ替えます。

ステップ 6 [高度な検索リスト（Advanced Search List）] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。

- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

  Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストに、Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

ID ソース順序の削除

ポリシーで今後使用しない ID ソース順序を削除できます。

始める前に

- 削除する ID ソース順序がいずれの認証ポリシーでも使用されていないことを確認してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]** を選択します。

ステップ 2 削除する ID ソース順序の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして ID ソース順序を削除します。

レポートでの ID ソースの詳細

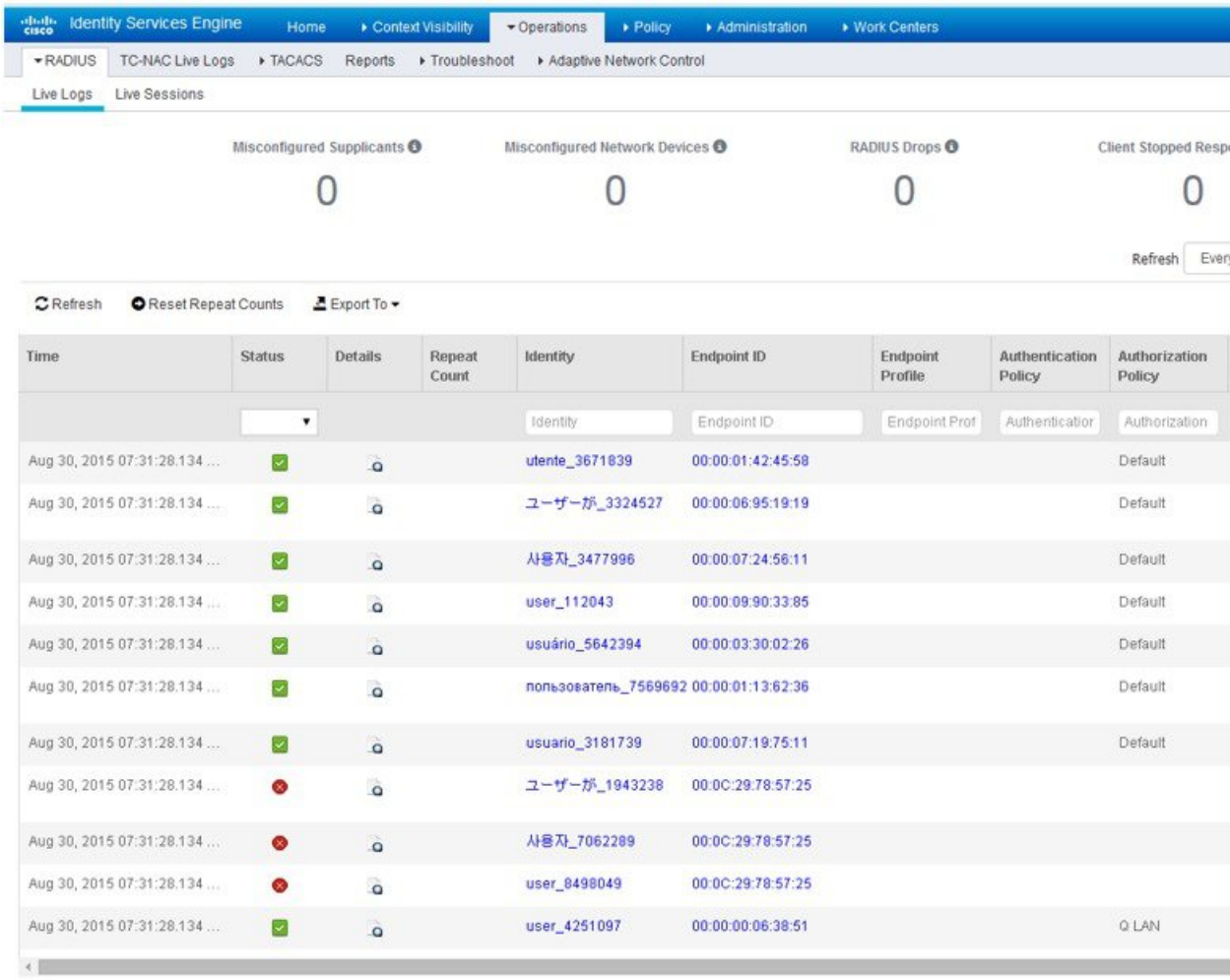
Cisco ISE は認証ダッシュレットおよび ID ソース レポートで ID ソースに関する情報を提供します。

[認証（Authentications）] ダッシュレット

[認証（Authentications）] ダッシュレットから、障害の理由などの詳細情報にドリルダウンできます。

[操作（Operations）] > [RADIUS ライブログ（RADIUS Livelog）] の順に選択して、リアルタイムで認証の概要を表示します。RADIUS ライブ ログの詳細については、『』の「RADIUS ライブ ログ」のセクションRADIUS ライブ ログ （333 ページ）を参照してください。

図 *35 : RADIUS* ライブ ログ



ID ソース レポート

Cisco ISE は ID ソースに関する情報を含むさまざまなレポートを提供します。これらのレポートの詳細については、「使用可能なレポート」の項を参照してください。

ネットワークのプロファイリングされたエンドポイント

プロファイラ サービスは、ネットワーク上にあるすべてのエンドポイントの機能（Cisco ISE では ID とも呼ばれる）を、デバイス タイプにかかわらず識別、検索、および特定して、企業ネットワークへの適切なアクセスを保証および維持するのに役立ちます。Cisco ISE プロファ

イラ機能では、さまざまなプローブを使用して、ネットワーク上にあるすべてのエンドポイントの属性を収集し、それらを既知のエンドポイントが関連ポリシーおよびIDグループに従って分類されるプロファイラ アナライザに渡します。

プロファイラ フィード サービスによって、管理者は、新規および更新されたエンドポイントプロファイリングポリシーや更新されたOUIデータベースを、指定されたCiscoフィードサーバからの、サブスクリプションを介したCisco ISEへのフィードとして取得できます。

プロファイラ条件の設定

次の表では、[プロファイラ条件（Profiler Condition）]ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[プロファイリング（Profiling）]** です。

表 ***84 :*** プロファイラ条件の設定

フィールド名	使用上のガイドライン
[名前（Name）]	プロファイラ条件の名前。
説明	プロファイラ条件の説明。
[タイプ（Type）]	事前定義済みタイプのいずれかを選択します。
属性名（Attribute Name）	プロファイラ条件が基づく属性を選択します。
演算子	演算子を選択します。
属性値（Attribute Value）	選択した属性の値を入力します。事前定義された属性値を含む属性名の場合、事前定義された値のドロップダウン リストが表示され、値を選択できます。
システム タイプ（System Type）	プロファイリング条件は、次のいずれかのタイプになります。 • [シスコ提供（Cisco Provided）]：シスコ提供として識別され、展開時にCisco ISEによって提供されるプロファイリング条件。システムから編集したり削除したりすることはできません。 • [管理者作成（Administrator Created）]：管理者作成として識別され、Cisco ISEの管理者として作成したプロファイリング条件。

関連トピック

Cisco ISE プロファイリング サービス （748 ページ）
プロファイラ条件 （777 ページ）
プロファイラ フィード サービス （828 ページ）
プロファイラ条件の作成 （797 ページ）

Cisco ISE プロファイリング サービス

Cisco Identity Services Engine（ISE）のプロファイリング サービスは、ネットワークに接続されているデバイスおよびその場所を識別します。エンドポイントは Cisco ISE に設定されたエンドポイント プロファイリング ポリシーに基づいてプロファイリングされます。次に、Cisco ISE では、ポリシー評価の結果に基づいてネットワークのリソースにアクセスする権限がエンドポイントに付与されます。

プロファイリング サービス：

- IEEE 規格 802.1X ポートベースの認証アクセス コントロール、MAC 認証バイパス（MAB）認証、およびネットワーク アドミッション コントロール（NAC）をさまざまな規模および複雑度の企業ネットワークに使用して、認証の効率的かつ効果的な展開および継続的な管理を容易にします。
- デバイス タイプにかかわらず、接続されたすべてのネットワーク エンドポイントの機能を特定、検索、および決定します。
- 一部のエンドポイントへのアクセスを誤って拒否しないようにします。

ISE Community Resource

ISE Endpoint Profiles

How To: ISE Profiling Design Guide

プロファイラ ワーク センター

[プロファイラ ワーク センター（Profiler Work Center）] メニュー（[ワーク センター（Work Centers）]>[プロファイラ（Profiler）]）には、すべてのプロファイラ ページが含まれ、ISE の管理者向けの単一の窓口として機能します。[プロファイラ ワーク センター（Profiler Work Center）] メニューには次のオプションがあります：[概要（Overview）]、[外部 ID ストア（Ext ID Stores）]、[ネットワーク デバイス（Network Devices）]、[エンドポイント分類（Endpoint Classification）]、[ノード設定（Node Config）]、[フィード（Feeds）]、[手動スキャン（Manual Scans）]、[ポリシー要素（ポリシーの要素）]、[プロファイリング ポリシー（Profiling Policies）]、[許可ポリシー（Authorization Policy）]、[トラブルシューティング（Troubleshoot）]、[レポート（Reports）]、[設定（Settings）] および [ディクショナリ（Dictionaries）]。

[プロファイラ（Profiler）] ダッシュボード

[プロファイラ（Profiler）] ダッシュボード（[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [エンドポイント分類（Endpoint Classification）]）は、ネットワーク内のプロファイル、エンドポイント、アセットの集中型モニタリング ツールです。このダッシュボードには、グラフと表の形式でデータが表示されます。[プロファイル（Profiles）] ダッシュレットには、ネットワークで現在アクティブな論理プロファイルとエンドポイント プロファイルが表示されます。[エンドポイント（Endpoints）] ダッシュレットには、ネットワークに接続するエンドポイントの ID グループ、PSN、OS タイプが表示されます。[アセット（Assets）] ダッシュレットには、ゲスト、BYOD、企業などのフローが表示されます。表には接続されたさまざまなエンドポイントが表示され、新しいエンドポイントを追加することもできます。

プロファイリング サービスを使用したエンドポイント インベントリ

プロファイリング サービスを使用して、ネットワークに接続されたすべてのエンドポイントの機能を検出、特定、および決定することができます。デバイスのタイプに関係なく、エンドポイントの企業ネットワークへの適切なアクセスを、保障し、保持できます。

プロファイリング サービスでは、エンドポイントの属性をネットワーク デバイスとネットワークから収集し、エンドポイントをそのプロファイルに従って特定のグループに分類します。一致したプロファイルを持つエンドポイントが Cisco ISE データベースに保存されます。プロファイリング サービスで処理されるすべての属性は、プロファイラ ディクショナリに定義されている必要があります。

プロファイリング サービスは、ネットワークの各エンドポイントを識別し、そのプロファイルに従ってシステム内の既存のエンドポイントの ID グループ、またはシステム内で作成できる新しいグループにそれらのエンドポイントをグループ化します。エンドポイントをグループ化して既存の ID グループにエンドポイント プロファイリング ポリシーを適用することで、エンドポイントと対応するエンドポイント プロファイリング ポリシーのマッピングを決定できます。

Cisco ISE プロファイラ キュー制限の設定

Cisco ISE プロファイラは、ネットワークから大量のエンドポイント データを短時間で収集します。それにより、一部の遅い Cisco ISE コンポーネントがプロファイラによって生成されるデータを処理するときにバックログが蓄積されるため、Java 仮想マシン（JVM）のメモリ使用率が増大し、パフォーマンスの低下および安定性の問題が生じます。

プロファイラが JVM メモリ使用率を増やさず、また、JVM がメモリ不足になり、再起動しないように、プロファイラの次の内部コンポーネントに制限が適用されます。

- エンドポイント キャッシュ：内部キャッシュのサイズは制限され、サイズが制限を超えると定期的に消去する必要があります（最長時間未使用方式に基づく）。
- フォワーダ：プロファイラによって収集されたエンドポイント情報のメイン入力キュー。

- イベント ハンドラ：高速コンポーネントを接続解除する内部キューで、（通常、データベース クエリーに関連する）低速処理コンポーネントにデータを提供します。

エンドポイント キャッシュ

- maxEndPointsInLocalDb = 100000（キャッシュ内のエンドポイント オブジェクト）
- endPointsPurgeIntervalSec = 300（秒単位のエンドポイント キャッシュ消去スレッド間隔）
- numberOfProfilingThreads = 8（スレッド数）

制限は、すべてのプロファイラ内部イベント ハンドラに適用されます。キュー サイズ制限に達すると、モニタリング アラームがトリガーされます。

Cisco ISE プロファイラのキュー サイズの制限

- forwarderQueueSize = 5000（エンドポイント収集イベント）
- eventHandlerQueueSize = 10000（イベント）

イベント ハンドラ

- NetworkDeviceEventHandler：すでにキャッシュされているネットワーク アクセス デバイス（NAD）の重複 IP アドレスのフィルタリングのほか、ネットワーク デバイスのイベント用。
- ARPCacheEventHandler：ARP キャッシュのイベント用。

Cisco ISE ノードでのプロファイリング サービスの設定

Cisco ISE 対応のネットワークでネットワーク リソースを使用しているすべてのエンドポイントのコンテキスト インベントリを提供するプロファイリング サービスを設定できます。

デフォルトですべての管理、モニタリング、およびポリシー サービスのペルソナを担当する単一の Cisco ISE ノードで実行されるようにプロファイリング サービスを設定できます。

分散展開では、プロファイリング サービスは、ポリシー サービス ペルソナを担当する Cisco ISE ノードでのみ実行され、管理ペルソナとモニタリング ペルソナを担当する他の Cisco ISE ノードでは実行されません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。

ステップ 3 [展開ノード（Deployment Nodes）] ページで [編集（Edit）] をクリックします。

ステップ 4 [全般設定（General Settings）] タブで [ポリシー サービス（Policy Service）] チェックボックスをオンにします。[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 次の作業を実行します。

a) [セッション サービスの有効化（Enable Session Services）] チェックボックスをオンにして、ネットワーク アクセス セッション サービス、ポスチャ セッション サービス、ゲスト セッション サービス、およびクライアント プロビジョニング セッション サービスを実行します。

b) [プロファイリング サービスの有効化（Enable Profiling Service）] チェックボックスをオンにして、プロファイリング サービスを実行します。

c) デバイス管理サービスを実行し、企業のネットワーク デバイスを制御および監査するには、[デバイス管理サービスの有効化（Enable Device Admin Service）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックしてノード設定を保存します。

プロファイリング サービスによって使用されるネットワーク プローブ

ネットワーク プローブは、ネットワーク上のエンドポイントから属性を収集するために使用される方法です。プローブを使用して、エンドポイントを Cisco ISE データベース内の一致するプロファイルで作成または更新できます。

Cisco ISE では、ネットワーク デバイスの動作を分析してデバイス タイプを決定する多数のネットワーク プローブを使用して、デバイスをプロファイリングすることができます。ネットワーク プローブは、ネットワーク可視性の向上に役立ちます。

IP アドレスと MAC アドレスのバインディング

エンドポイントを作成または更新するには、企業ネットワークの MAC アドレスのみを使用できます。ARP キャッシュにエントリが見つからない場合は、Cisco ISE で HTTP パケットの L2 MAC アドレスと NetFlow パケットの IN_SRC_MAC を使用してエンドポイントを作成または更新できます。エンドポイントが 1 ホップだけ離れている場合、プロファイリング サービスは L2 隣接関係に依存します。エンドポイントに L2 隣接関係がある場合、エンドポイントの IP アドレスと MAC アドレスはすでにマッピングされているため、IP-MAC キャッシュ マッピングは必要ありません。エンドポイントに L2 隣接関係が存在せず、エンドポイントが複数ホップ離れている場合、マッピングは信頼できない場合があります。収集する NetFlow パケットの既知の属性には、PROTOCOL、L4_SRC_PORT、IPV4_SRC_ADDR、L4_DST_PORT、IPV4_DST_ADDR、IN_SRC_MAC、OUT_DST_MAC、IN_SRC_MAC、OUT_SRC_MAC などがあります。エンドポイントに L2 隣接関係が存在せず、L3 ホップに関して複数ホップ離れている場合は、IN_SRC_MAC 属性で L3 ネットワーク デバイスの MAC アドレスのみが伝送されます。Cisco ISE で HTTP プローブが有効になっている場合は、HTTP 要求メッセージによってペイロード データでエンドポイントの IP アドレスと MAC アドレスが伝送されないため、HTTP パケットの MAC アドレスを使用してのみエンドポイントを作成できます。Cisco ISE では、プロファイリング サービスで ARP キャッシュが実装されるため、エンドポイントの IP アドレスと MAC アドレスを確実にマッピングできます。ARP キャッシュを機能させるには、DHCP プローブまたは RADIUS プローブを有効にする必要があります。DHCP プローブと RADIUS プ

ローブは、ペイロードデータでエンドポイントのIPアドレスとMACアドレスを伝送します。DHCP プローブの dhcp-requested address 属性と RADIUS プローブの Framed-IP-address 属性によって、エンドポイントのIPアドレスがそのMACアドレスとともに伝送されます。これらのアドレスは、マッピングして ARP キャッシュに格納できます。

NetFlow プローブ

Cisco ISE プロファイラは Cisco IOS NetFlow Version 9 を実装しています。NetFlow Version 9 には、Cisco ISE プロファイリング サービスをサポートするためのプロファイラの拡張に必要な追加機能があるため、これを使用することを推奨します。

NetFlow Version 9 の属性を NetFlow 対応のネットワーク アクセス デバイスから収集して、エンドポイントを作成したり、Cisco ISE データベース内の既存のエンドポイントを更新できます。NetFlow Version 9 は、エンドポイントの送信元 MAC アドレスと宛先 MAC アドレスを割り当てて、更新するように設定できます。NetFlow 属性のディクショナリを作成して NetFlow ベースのプロファイリングに対応することもできます。

NetFlow Version 9 レコード フォーマットの詳細については、『NetFlow Version 9 Flow-Record Format』マニュアルの表 6「NetFlow Version 9 Field Type Definitions」を参照してください。

さらに、Cisco ISE は Version 5 以前の NetFlow バージョンをサポートします。ネットワークで NetFlow Version 5 を使用する場合は、Version 5 をアクセス レイヤのプライマリ ネットワーク アクセス デバイス（NAD）でのみ使用できます。他のデバイスでは動作しません。

Cisco IOS NetFlow Version 5 パケットには、エンドポイントの MAC アドレスが含まれません。NetFlow Version 5 から収集された属性は、Cisco ISE データベースに直接追加できません。IP アドレスを使用してエンドポイントを検出し、エンドポイントに NetFlow Version 5 の属性を付加できます。このことは、ネットワーク アクセス デバイスの IP アドレスと NetFlow Version 5 属性から抽出される IP アドレスを組み合わせることによって実行できます。ただし、これらのエンドポイントを RADIUS または SNMP プローブで事前に検出しておく必要があります。

NetFlow Version 5 以前のバージョンでは、MAC アドレスは IP フローの一部ではありません。このため、エンドポイントのキャッシュにあるネットワーク アクセス デバイスから収集された属性情報を関連付けることにより、エンドポイントの IP アドレスをプロファイリングすることが必要となります。

NetFlow Version 5 レコード フォーマットの詳細については、『NetFlow Services Solutions Guide』の表 2「Cisco IOS NetFlow Flow Record and Export Format Content Information」を参照してください。

DHCP プローブ

Cisco ISE 展開のダイナミック ホスト コンフィギュレーション プロトコル プローブを有効にすると、Cisco ISE プロファイリング サービスで INIT-REBOOT および SELECTING メッセージ タイプの新しい要求だけに基づいてエンドポイントを再プロファイリングできます。RENEWING や REBINDING などの他の DHCP メッセージ タイプは処理されますが、エンドポイントのプロファイリングには使用されません。DHCPパケットから解析された属性は、エンドポイント属性にマッピングされます。

INIT-REBOOT 状態中に生成された DHCPREQUEST メッセージ

DHCPクライアントが前に割り当てられてキャッシュされた設定を確認する場合、クライアントはサーバ識別子（server-ip）オプションを入力できません。代わりに、前に割り当てられたIP アドレスを要求された IP アドレス（requested-ip）オプションに入力する必要があります。また、DHCPREQUEST メッセージの Client IP Address（ciaddr）フィールドをゼロで埋める必要があります。要求された IP アドレスが正しくない場合、またはクライアントが誤ったネットワークに配置されている場合、DHCP サーバはDHCPNAK メッセージをクライアントに送信します。

SELECTING 状態中に生成された DHCPREQUEST メッセージ

DHCP クライアントは、サーバ識別子（server-ip）オプションで選択された DHCP サーバの IP アドレスを挿入し、要求された IP アドレス（requested-ip）オプションにクライアントによって選択された DHCPOFFER の Your IP Address（yiaddr）フィールドの値を入力します。また、「ciaddr」フィールドをゼロで埋めます。

表 *85*：さまざまな状態からの *DHCP* クライアント メッセージ

—	INIT-REBOOT	SELECTING	RENEWING	REBINDING
ブロードキャスト/ユニキャスト	broadcast	broadcast	ユニキャスト	broadcast
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP アドレス	IP アドレス

DHCP ブリッジ モードのワイヤレス LAN コントローラ設定

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）ブリッジ モードでワイヤレス LAN コントローラ（WLC）を設定することを推奨します。このモードでは、ワイヤレスクライアントから Cisco ISE にすべての DHCP パケットを転送できます。WLC Web インターフェイスの **[コントローラ（Controller）]** > **[詳細設定（Advanced）]** > **[DHCP マスター コントローラ モード（DHCP Master Controller Mode）]** > **[DHCP パラメータ（DHCP Parameters）]** で使用可能な [DHCP プロキシの有効化（Enable DHCP Proxy）] チェックボックスをオフにする必要があります。DHCP IP ヘルパー コマンドが Cisco ISE ポリシー サービス ノードを指していることも確認する必要があります。

DHCP SPAN プローブ

DHCP スイッチド ポート アナライザ（SPAN）プローブは、Cisco ISE ノードで初期化されると、特定インターフェイス上のネットワーク アクセスデバイスからのネットワーク トラフィックをリッスンします。DHCP SPAN パケットを DHCP サーバから Cisco ISE プロファイラに転送するようにネットワーク アクセス デバイスを設定する必要があります。プロファイラはこ

れらの DHCP SPAN パケットを受信して解析し、エンドポイントのプロファイリングに使用できるエンドポイント属性を取得します。

次に例を示します。

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

HTTP プローブ

HTTP プローブでは、識別文字列が HTTP 要求ヘッダー フィールド User-Agent を使って転送されます。このフィールドは、IP タイプのプロファイリング条件の作成、および Web ブラウザ情報の確認に使用される属性です。プロファイラは Web ブラウザ情報を User-Agent 属性および要求メッセージの他の HTTP 属性から取得し、エンドポイント属性のリストに追加します。

Cisco ISE はポート 80 およびポート 8080 で Web ブラウザからの通信をリッスンします。Cisco ISE には、多くのデフォルト プロファイルが用意されています。これらのプロファイルはシステムに組み込まれ、User-Agent 属性に基づいてエンドポイントを識別します。

HTTP はデフォルトで有効になっています。CWA、Hotspot、BYOD、MDM、およびポスチャなどの複数の ISE サービスは、クライアントの Web ブラウザの URL リダイレクトに依存しています。リダイレクトされるトラフィックには、接続されたエンドポイントの RADIUS セッション ID が含まれています。PSN でこれらの URL リダイレクトフローを終端すると、復号化された HTTPS データが可視化されます。HTTP プローブが PSN で無効になっている場合でも、ノードは Web トラフィックからブラウザのユーザエージェント文字列を解析し、関連付けられたセッション ID に基づいてエンドポイントにデータを関連付けます。この方法でブラウザ文字列が収集されると、データのソースが HTTP プローブではなく、ゲストポータルまたは CP（クライアント プロビジョニング）としてリストされます。

HTTP SPAN プローブ

Cisco ISE 展開の HTTP プローブをスイッチド ポート アナライザ（SPAN）プローブとともに有効にすると、プロファイラは指定されたインターフェイスからの HTTP パケットをキャプチャできます。SPAN 機能は、Cisco ISE サーバが Web ブラウザからの通信をリッスンするポート 80 で使用できます。

HTTP SPAN は、HTTP 要求ヘッダー メッセージの HTTP 属性を IP ヘッダー（L3 ヘッダー）の IP アドレスとともに収集し、L2 ヘッダーのエンドポイントの MAC アドレスに基づいてエンドポイントに関連付けることができます。この情報は、Apple デバイスやさまざまなオペレーティング システムのコンピュータなどの各種モバイルおよびポータブル IP 対応デバイスを識別するのに役立ちます。ゲスト ログインまたはクライアント プロビジョニング ダウンロード時に Cisco ISE サーバでキャプチャをリダイレクトするため、各種モバイルおよびポータブル IP 対応デバイスの識別の信頼性が向上しました。これにより、プロファイラは User-Agent 属性とその他の HTTP 属性を要求メッセージから取得し、Apple デバイスなどのデバイスを識別できます。

VMware で実行中の Cisco ISE の HTTP 属性の収集の無効化

Cisco ISE を ESX サーバ（VMware）に展開している場合、Cisco ISE プロファイラはダイナミック ホスト コンフィギュレーション プロトコル トラフィックを収集しますが、vSphere クライアント上の設定の問題により HTTP トラフィックを収集しません。VMware セットアップで HTTP トラフィックを収集するには、Cisco ISE プロファイラのために作成する仮想スイッチの無差別モードを Accept から Reject（デフォルト）に変更して、セキュリティを設定します。DHCP および HTTP のスイッチド ポート アナライザ（SPAN）プローブが有効になっている場合は、Cisco ISE プロファイラによって DHCP トラフィックと HTTP トラフィックの両方が収集されます。

pxGrid プローブ

pxGrid プローブは、外部ソースからエンドポイントコンテキストを受信するために Cisco pxGrid を利用します。Cisco ISE 2.4 より前は、Cisco ISE はパブリッシャおよび共有されたさまざまなコンテキスト情報（セッション id、グループ情報、外部サブスクライバへの設定要素など）のみを提供していました。Cisco ISE 2.4 での pxGrid プローブの導入により、パブリッシャおよび Cisco ISE ポリシーサービスノードがサブスクライバになるという他のソリューションが提供されます。

pxGrid プローブは、エンドポイントアセットのトピック /topic/com.cisco.endpoint.asset、サービス名 com.cisco.endpoint.asset を使用する pxGrid v2 仕様に基づいています。次の表に、プレフィックス asset が先行するすべてのトピック属性を示します。

表 *86 :* エンドポイントアセットのトピック

属性名	タイプ	説明
assetId	長整数型	アセット ID
assetName	文字列	アセット名
assetIpAddress	文字列	IP アドレス
assetMacAddress	文字列	MAC アドレス
assetVendor	文字列	製造元
assetProductId	文字列	製品コード
assetSerialNumber	文字列	シリアル番号
assetDeviceType	文字列	デバイスタイプ
assetSwRevision	文字列	S/W リビジョン番号
assetHwRevision	文字列	H/W リビジョン番号
assetProtocol	文字列	プロトコル

assetConnectedLinks	配列	ネットワーク リンク オブジェクトの配列
assetCustomAttributes	配列	カスタム名と値のペアの配列

シスコおよびサードパーティ製品は、これらの事前定義された属性を使用して、エンドポイントに関する情報を公開できます。デバイスのMACアドレス（assetMacAddress）やIPアドレス（assetIpAddress）などのネットワーク資産を追跡するために一般的に使用される属性に加えて、このトピックでは、ベンダーが固有のエンドポイント情報をカスタム属性（assetCustomAttributes）として公開することができます。Cisco ISE でエンドポイントカスタム属性を使用すると、pxGrid で共有される一意のベンダー属性セットごとにスキーマの更新を必要とせずに、さまざまな使用例に関するトピックを拡張できます。

RADIUS プローブ

Cisco ISE で認証に RADIUS を使用するように設定し、クライアント サーバ トランザクションで使用できる共有秘密を定義できます。RADIUS サーバから RADIUS 要求および応答メッセージを受信すると、プロファイラはエンドポイントのプロファイリングに使用できる RADIUS 属性を収集できます。

Cisco ISE は RADIUS サーバおよび他の RADIUS サーバに対する RADIUS プロキシ クライアントとして動作できます。プロキシ クライアントとして動作する場合は、外部の RADIUS サーバを使用して RADIUS 要求および応答メッセージを処理します。

また、RADIUSプローブは、デバイスセンサーによってRADIUSアカウンティングパケットで送信された属性も収集します。詳細については、IOSセンサー組み込みスイッチからの属性の収集（772ページ）およびIOSセンサー組み込みネットワークアクセスデバイスの設定チェックリスト（773ページ）を参照してください。

RADIUS プローブは、プロファイルサービス用に設定されていないシステムであっても、デフォルトで実行し、ISE がコンテキスト可視性サービスで使用するエンドポイント認証および認可の詳細を追跡できるようにします。また、RADIUSプローブサービスおよびプロファイリングサービスは、消去操作のために登録されたエンドポイントの作成および更新の時間を追跡するためにも使用されます。プロファイリングサービスが有効になっており、プローブが有効になっている場合は、RADIUS から学習した新しい属性もプロファイリングをトリガーします。それ以外の場合、属性は収集されますが、プロファイリングはデバイスセンサーを含むRADIUS 学習データに基づいてトリガーされません。

表 *87 : RADIUS*の プローブを使用して収集した共通属性

User-Name	**Calling-Station-Id**	**Called-Station-Id**	**Framed-IP-Address**
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
デバイスタイプ（NAD）	ロケーション（NAD）	認証ポリシー（Authentication policy）	許可ポリシー

（注） Cisco ISE がアカウンティング終了を受信すると、エンドポイントが最初に IP アドレスでプロファイルされた場合、対応するエンドポイントを再プロファイルするように Cisco ISE がトリガーされます。したがって、IPアドレスを使用してプロファイルされたエンドポイントのカスタムプロファイルがある場合、これらのプロファイルの確実度係数の合計を満たす唯一の方法は、プロファイルが対応する IP アドレスで一致することです。

ネットワーク スキャン（NMAP）プローブ

NMAP プローブについて

Cisco ISE では、NMAP セキュリティ スキャナを使用して、サブネット内のデバイスを検出できます。プロファイリング サービスの実行が有効になっているポリシー サービス ノードで NMAP プローブをイネーブルにします。エンドポイント プロファイリング ポリシーでそのプローブからの結果を使用します。

NMAP の各手動サブネット スキャンには、エンドポイント ソース情報をそのスキャン ID で更新するために使用される一意の数値 ID があります。エンドポイント検出時に、エンドポイント ソース情報を更新して、ネットワーク スキャン プローブで検出されたことを示すこともできます。

NMAP の手動サブネット スキャンは、静的な IP アドレスが割り当てられたプリンタなど、常に Cisco ISE ネットワークに接続されているために、他のプローブで検出できないデバイスを検出する場合に便利です。

NMAP スキャンの制限

サブネットのスキャンには非常に多くのリソースを消費します。サブネットのスキャンは時間のかかるプロセスです。これは、サブネットのサイズや密度によって異なります。アクティブなスキャンの数は常に 1 つに制限されるため、同時にスキャンできるサブネットは 1 つだけです。また、サブネット スキャンの進行中にいつでもサブネット スキャンをキャンセルできます。[クリック（Click）] を使用して、最新のスキャン結果のリンクを表示できます。これにより、**[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャンの結果（Manual NMAP Scan Results）]** に保存されている最新のネットワーク スキャン結果を表示できます。

手動 NMAP スキャン

次の NMAP コマンドを使用すると、サブネットがスキャンされ、nmapSubnet.log に出力が送信されます。

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

表 *88 :* 手動サブネット スキャンの *NMAP* コマンド

-O	OS 検出の有効化

-sU	UDP スキャン
-p <port ranges>	特定のポートのみスキャンします。たとえば、U:161, 162 と指定します。
oN	通常の出力
oX	XML 出力

NMAP の手動サブネット スキャンの SNMP 読み取り専用コミュニティ ストリング

NMAP の手動サブネット スキャンは、エンドポイントで UDP ポート 161 が開かれ、その結果、より多くの属性が収集されることを検出したときには、SNMP クエリーで拡張されます。NMAP 手動サブネット スキャン中は、ネットワーク スキャン プローブによって、デバイスで SNMP ポート 161 が開いているかどうかが検出されます。ポートが開いている場合は、SNMP バージョン 2c のデフォルトのコミュニティ ストリング（public）を使用して SNMP クエリがトリガーされます。

デバイスで SNMP がサポートされ、デフォルトの読み取り専用コミュニティ ストリングが public に設定されている場合は、デバイスの MAC アドレスを MIB 値「ifPhysAddress」から取得できます。

さらに、[プロファイラ設定（Profiler Configuration）] ページでは、NMAP の手動でのネットワーク スキャンのために、カンマで区切られた追加の SNMP 読み取り専用コミュニティ ストリングを設定できます。また、SNMP バージョン 1 および 2c の SNMP MIB ウォーク用に新しい読み取り専用コミュニティ文字列を指定できます。SNMP 読み取り専用コミュニティ文字列の設定については、CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定（765 ページ）を参照してください。

手動 NMAP スキャンの結果

最新のネットワーク スキャン結果は、[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャンの結果（Manual NMAP Scan Results）] に保存されます。[手動 NMAP スキャンの結果（Manual NMAP Scan Results）] ページには、任意のサブネットに対して手動でのネットワーク スキャンを実行し、その結果として検出された最新のエンドポイントのみが、関連付けられたエンドポイント プロファイル、MAC アドレス、およびスタティック割り当てステータスとともに表示されます。このページでは、必要に応じて、エンドポイント サブネットで検出されたポイントをより適切に分類するために編集できます。

Cisco ISE を使用すると、プロファイリング サービスの実行が有効になっている [ポリシー サービス（Policy Service）] ノードで手動でのネットワーク スキャンを実行できます。展開内のプライマリ管理 ISE ノード ユーザ インターフェイスでポリシー サービス ノードを選択し、そのポリシー サービス ノードで手動でのネットワーク スキャンを実行する必要があります。任意のサブネットに対する手動でのネットワーク スキャン時に、ネットワーク スキャン プローブにより、指定されたサブネット上のエンドポイントとそのオペレーティング システムが検出され、SNMP サービス用の UDP ポート 161 および 162 がチェックされます。

その他の情報

手動での NMAP スキャンの結果に関する追加情報を以下に示します。

- 不明なエンドポイントを検出するには、NMAP が NMAP スキャンまたはサポートする SNMP スキャンを介して IP/MAC バインディングを学習できる必要があります。
- ISE は、RADIUS 認証または DHCP プロファイリングを使用して、既知のエンドポイントの IP/MAC バインディングを学習します。
- IP/MAC バインディングは、展開内の PSN ノード間で複製されません。したがって、ローカル データベースに IP/MAC バインディングがある PSN（たとえば、MAC アドレスが最後に認証された PSN）から手動スキャンを開始する必要があります。
- NMAP スキャンの結果には、手動または自動にかかわらず、NMAP が以前にスキャンしたエンドポイントに関する情報は表示されません。

DNS プローブ

Cisco ISE 展開のドメイン ネーム サーバ（DNS）プローブを使用すると、プロファイラはエンドポイントを検索し、完全修飾名（FQDN）を取得できます。Cisco ISE 対応のネットワークでエンドポイントが検出されたら、エンドポイント属性のリストが NetFlow、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP プローブから収集されます。

Cisco ISE をスタンドアロンで展開する場合、または初めて分散環境に展開する場合は、セットアップ ユーティリティを実行して Cisco ISE アプライアンスを設定するように求められます。セットアップ ユーティリティを実行するときに、ドメイン ネーム システム（DNS）ドメインとプライマリ ネームサーバ（プライマリ DNS サーバ）を設定します。設定時には、1 つ以上のネームサーバを設定できます。Cisco ISE の展開後に、CLI コマンドを使用して DNS ネームサーバを変更または追加することもできます。

DNS FQDN ルックアップ

DNS ルックアップを実行する前に、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP のいずれかのプローブを DNS プローブとともに起動する必要があります。これにより、プロファイラの DNS プローブは、Cisco ISE 展開に定義されている、指定されたネームサーバに対して逆引き DNS ルックアップ（FQDN ルックアップ）を実行できます。新しい属性がエンドポイントの属性リストに追加され、エンドポイント プロファイリング ポリシーの評価に使用できます。FQDN は、システム IP ディクショナリに存在する新しい属性です。エンドポイント プロファイリング条件を作成して、FQDN 属性およびそのプロファイリング用の値を検証できます。次は、DNS ルックアップ、およびこれらの属性を収集するプローブに必要な特定のエンドポイント属性です。

- dhcp-requested-address 属性：DHCP プローブと DHCP SPAN プローブによって収集される属性
- SourceIP 属性：HTTP プローブによって収集される属性
- Framed-IP-Address 属性：RADIUS プローブによって収集される属性

• cdpCacheAddress 属性：SNMP プローブによって収集される属性

WLC Web インターフェイスでの呼出端末 ID タイプの設定

WLC Web インターフェイスを使用して、呼出端末 ID タイプ情報を設定できます。WLC Web インターフェイスの [セキュリティ（Security）] タブに移動すると、[RADIUS RADIUS 認証サーバ（Authentication Servers）] ページで発信側ステーション ID を設定できます。[MAC デリミタ（MAC Delimiter）] フィールドは、WLC ユーザ インターフェイスのデフォルトでは、[コロン（Colon）] に設定されます。

WLC Web インターフェイスで設定する方法の詳細については、『Cisco Wireless LAN Controller Configuration Guide, Release 7.2』の第 6 章「Configuring Security Solutions」を参照してください。

config radius callStationIdType コマンドを使用して WLC CLI で設定する方法の詳細については、『Cisco Wireless LAN Controller Command Reference Guide, Release 7.2』の第 2 章「Controller Commands」を参照してください。

ステップ 1 ワイヤレス LAN コントローラのユーザ インターフェイスにログインします。

ステップ 2 [セキュリティ（Security）] をクリックします。

ステップ 3 [AAA] を展開して、**[RADIUS]** > **[認証（Authentication）]** を選択します。

ステップ 4 [呼出端末 ID タイプ（Call Station ID Type）] ドロップダウン リストから [システム MAC アドレス（System MAC Address）] を選択します。

ステップ 5 FIPS モードで Cisco ISE を実行する場合は、[AES キー ラップ（AES Key Wrap）] チェックボックスをオンにします。

ステップ 6 [MAC 区切り文字（MAC Delimiter）] ドロップダウン リストから [コロン（Colon）] を選択します。

SNMP クエリ プローブ

[ノードの編集（Edit Node）] ページでの SNMP クエリー プローブの設定に加えて、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス（Network Devices）]** でその他の Simple Management Protocol 設定を行う必要があります。

[ネットワーク デバイス（Network Devices）] リスト ページで新しいネットワーク アクセス デバイス（NAD）の SNMP 設定を行うことができます。ネットワーク アクセスデバイスの SNMP クエリー プローブまたは SNMP 設定に指定したポーリング間隔で、NAD に定期的にクエリーを実行します。

次の設定に基づいて、特定の NAD の SNMP クエリーをオンおよびオフにすることができます。

• [リンクアップ時に SNMP クエリー（SNMP Query on Link up）] および [新しい MAC の通知（New MAC notification）] のオンまたはオフ

- Cisco Discovery Protocol 情報の [リンクアップ時に SNMP クエリー（SNMP Query on Link up）] および [新しい MAC の通知（New MAC notification）] のオンまたはオフ
- SNMP クエリー タイマーをデフォルトでスイッチごとに 1 時間に 1 回

iDevice および SNMP をサポートしないその他のモバイル デバイスでは、ARP テーブルによって MAC アドレスを検出でき、SNMP クエリー プローブによってネットワーク アクセス デバイスからクエリーを実行できます。

SNMP クエリに関する Cisco Discovery Protocol のサポート

ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスのすべてのポートで Cisco Discovery Protocol を有効（デフォルト）にする必要があります。ネットワーク デバイスのいずれかのポートで Cisco Discovery Protocol を無効にすると、接続されているすべてのエンドポイントの Cisco Discovery Protocol 情報が失われるため、正しくプロファイリングを実行できなくなる可能性があります。ネットワーク デバイスで cdp run コマンドを使用して Cisco Discovery Protocol をグローバルに有効にし、ネットワーク アクセス デバイスのインターフェイスで cdp enable コマンドを使用して Cisco Discovery Protocol を有効にします。ネットワーク デバイスとインターフェイスで Cisco Discovery Protocol を無効にするには、コマンドの先頭に no キーワードを使用します。

SNMP クエリに関する Link Layer Discovery Protocol のサポート

Cisco ISE プロファイラは LLDP の属性を収集するために SNMP クエリーを使用します。RADIUS プローブを使用して、ネットワーク デバイスに組み込まれている Cisco IOS センサーから LLDP 属性を収集することもできます。ネットワーク アクセス デバイスで LLDP グローバル コンフィギュレーション コマンドおよび LLDP インターフェイス コンフィギュレーション コマンドの設定に使用できるデフォルトの LLDP 構成設定を確認してください。

表 *89* : デフォルトの *LLDP* 設定

機能	機能
LLDP グローバル ステート	無効
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	有効（すべての TLV の送受信が可能）
LLDP インターフェイス ステート	[有効（Enabled）]
LLDP 受信	[有効（Enabled）]
LLDP 転送	[有効（Enabled）]
LLDP med-tlv-select	有効（すべての LLDP-MED TLV の送信が可能）

単一文字で表示される CDP および LLDP の機能コード

エンドポイントの属性リストには、lldpCacheCapabilities 属性と lldpCapabilitiesMapSupported 属性の 1 文字の値が表示されます。値は、CDP と LLDP を実行するネットワーク アクセス デバイスに対して表示される機能コードです。

例 1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

例 2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

例 3

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

SNMP トラップ プローブ

SNMP トラップは、MAC 通知、linkup、linkdown、および informs をサポートする特定のネットワーク アクセスデバイスから情報を受信します。SNMP トラッププローブは、ポートがアップまたはダウンし、エンドポイントがネットワークから切断するか、またはネットワークに接続したときに、特定のネットワーク アクセス デバイスから情報を受信します。そのため、受信した情報は Cisco ISE にエンドポイントを作成するのに十分ではありません。

SNMP トラップを完全に機能させ、エンドポイントを作成するには、トラップを受信したときに SNMP クエリー プローブがネットワーク アクセス デバイスの特定のポートでポーリング イベントをトリガーするように SNMP クエリーを有効にする必要があります。この機能を完全に動作させるには、ネットワーク アクセス デバイスと SNMP トラップを設定する必要があります。

（注） Cisco ISE では、ワイヤレス LAN コントローラ（WLC）とアクセス ポイント（AP）から受信した SNMP トラップはサポートされません。

Active Directory プローブ

AD のプローブ：

- Windows エンドポイントの OS 情報の明瞭度を向上させます。Microsoft AD はバージョンとサービス パックのレベルを含む、AD に参加しているコンピュータの OS の詳細情報を追跡します。AD のプローブは、AD のランタイム コネクタを使用してこの情報を直接取得し、クライアント OS 情報の信頼性の高いソースを提供します。
- 社内および社外の資産を区別するのに役立ちます。AD のプローブで使用される基本的ですが重要な属性は、エンドポイントが AD にあるかどうかです。この情報は AD に含まれるエンドポイントを管理対象デバイスまたは企業資産として分類するために使用できます。

[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [プロファイリング設定（Profiling Configuration）] ページで AD プローブを有効化できます。このプローブを有効にすると、ISE はホスト名を受信するとすぐに、新しいエンドポイントの AD 属性を取得します。ホスト名は通常 DHCP または DNS プローブから正常に学習されます。正常に取得すると、ISE は再スキャンがタイムアウトになるまで、同じエンドポイントに対し AD を再度問い合わせようとはしません。これにより属性の問い合わせに対する AD の負荷が制限されます。再スキャン タイマーは、**[再スキャンまでの日数（Days Before Rescan）]** フィールド（[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [プロファイリング設定（Profiling Configuration）] > [Active Directory] ）で設定できます。エンドポイントでの追加のプロファイリング アクティビティがあれば、AD はもう一度クエリーされます。

次の AD プローブの属性は ACTIVEDIRECTORY 条件を使用して、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [プロファイリング（Profiling）]** でマッチングさせることができます。AD のプローブを使用して集められた AD 属性は、[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] ページのエンドポイントの詳細にプレフィックス「AD」が付いて表示されます。

- AD-Host-Exists
- AD-Join-Point
- AD-Operating-System
- AD-OS-Version
- AD-Service-Pack

Cisco ISE ノードごとのプローブの設定

ポリシー サービス ペルソナを担当する展開の Cisco ISE ノードごとに、[プロファイリング設定（Profiling Configuration）] タブで次のプローブを 1 つ以上設定できます。

- [スタンドアロン ノード（A standalone node）] : デフォルトですべての管理、モニタリング、およびポリシー サービスのペルソナを担当する単一のノードに Cisco ISE を展開した場合。
- [複数ノード（Multiple nodes）] : 展開でポリシー サービス ペルソナを担当するノードを複数登録した場合。

（注） デフォルトでは、すべてのプローブが有効になっているわけではありません。一部のプローブは、チェックマークで明示的に有効にされていない場合でも部分的に有効になります。プロファイリングの設定は、現在、各 PSN に固有です。展開内の各 PSN は、同一のプロファイラ構成設定を使用して設定することを推奨します。

始める前に

Cisco ISE ノードごとのプローブは、管理ノードからのみ設定できます。管理ノードは、分散展開のセカンダリ管理ノードで使用できません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。

ステップ 3 [展開ノード（Deployment Nodes）] ページで [編集（Edit）] をクリックします。

ステップ 4 [全般設定（General Settings）] タブで [ポリシー サービス（Policy Service）] チェックボックスをオンにします。[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 [プロファイリング サービスの有効化（Enable Profiling Service）] チェックボックスをオンにします。

ステップ 6 [プロファイリング設定（Profiling Configuration）] タブをクリックします。

ステップ 7 各プローブの値を設定します。

ステップ 8 [保存（Save）] をクリックしてプローブ設定を保存します。

CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定

Cisco ISE では、グローバル コンフィギュレーションで、[プロファイラ設定（Profiler Configuration）] ページで許可変更（CoA）を発行し、プロファイリング サービスを有効にしてすでに認証されているエンドポイントに対する制御を拡張することができます。

さらに、[プロファイラ設定（Profiler Configuration）] ページでは、NMAP の手動でのネットワーク スキャンのために、カンマで区切られた追加の SNMP 読み取り専用コミュニティ ストリングを設定できます。SNMP RO コミュニティ ストリングは、[現在のカスタム SNMP コミュニティ ストリング（Current custom SNMP community strings）] フィールドに表示されるのと同じ順序で使用されます。

[プロファイラ設定（Profiler Configuration）] ページでは、エンドポイント属性のフィルタリングを設定することもできます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）]** を選択します。

ステップ 2 次のいずれかの設定を選択して、CoA タイプを設定します。

- [CoA なし（No CoA）]（デフォルト）：このオプションを使用して、CoA のグローバル コンフィギュレーションを無効にできます。この設定は、エンドポイント プロファイリング ポリシーごとに設定された CoA を上書きします。目的が可視性のみの場合は、デフォルト値 の [CoA なし（No CoA）] のままにします。
- [ポート バウンス（Port Bounce）]：スイッチ ポートのセッションが 1 つだけである場合は、このオプションを使用できます。ポートに複数のセッションがある場合は、[再認証（Reauth）] オプションを使用します。プロファイルの変更に基づいてアクセスポリシーをすぐに更新することが目的の場合は、[ポートバウンス（Port Bounce）] オプションを選択します。これにより、クライアントレス エンドポイントが再認可され、必要に応じて、IP アドレスが更新されます。
- [再認証（Reauth）]：このオプションを使用して、すでに認証されているエンドポイントをプロファイリング時に再認証できます。 現在のセッションの再認可に従った VLAN またはアドレスの変更が予期されていない場合は、[再認証（Reauth）] オプションを選択します。

  （注） 1 つのポートに複数のアクティブなセッションがある場合は、CoA に [ポートバウンス（Port Bounce）] オプションを設定しても、プロファイリングサービスによって [再認証（Reauth）] オプションが指定された CoA が発行されます。この機能を使用すると、[ポート バウンス（Port Bounce）] オプションの場合のように他のセッションが切断されるのを回避できます。

ステップ 3 NMAP の手動でのネットワークスキャンのために、カンマで区切られた新しい SNMP コミュニティ文字列を [カスタム SNMP コミュニティ文字列の変更（Change Custom SNMP Community Strings）] フィールドに入力し、[カスタム SNMP コミュニティ文字列の確認（Confirm Custom SNMP Community Strings）] フィールドに文字列を再入力します。

デフォルトの SNMP コミュニティ文字列は「public」です。これを確認するには、[現在のカスタム SNMP コミュニティ文字列（Current Custom SNMP Community Strings）] セクションの [表示（Show）] をクリックします。

ステップ 4 [エンドポイント属性フィルタ（Endpoint Attribute Filter）] チェックボックスをオンにして、エンドポイント属性のフィルタリングを有効にします。

[エンドポイント属性フィルタ（EndPoint Attribute Filter）] を有効にすると、Cisco ISE プロファイラは、重要な属性のみを保持し、その他の属性をすべて廃棄します。詳細については、ホワイトリストを使用してエンドポイント属性をフィルタリングするグローバル設定（770ページ）およびISEデータベースの持続性とパフォーマンスの属性フィルタ（769 ページ）の項を参照してください。ベストプラクティスとして、実稼働展開では [エンドポイント属性フィルタ（Endpoint Attribute Filter）] を有効にすることを推奨します。

ステップ 5 [プローブデータパブリッシャの有効化（Enable Probe Data Publisher）] チェックボックスをオンにして、Cisco ISE でエンドポイント プローブ データを、ISE でのエンドポイント オンボーディングの分類にこのデータが必要な pxGrid サブスクライバにパブリッシュします。PxGrid サブスクライバは、初期導入フェーズ中に一括ダウンロードを使用して、Cisco ISE からエンドポイントレコードをプルできます。Cisco ISE は、PAN で更新されるたびに、エンドポイントレコードを pxGrid サブスクライバに送信します。このオプションはデフォルトでは無効になっています。

このオプションを有効にする場合は、導入環境で pxGrid ペルソナが有効になっていることを確認します。

（注） このオプションは、Cisco ISE 2.4 パッチ 10 以降で使用できます。

ステップ 6 [保存（Save）] をクリックします。

認証されたエンドポイントに対する許可変更のグローバル設定

デフォルトの [CoA なし（No CoA）] オプションを使用して認可変更（CoA）を無効にするか、またはポートバウンスと再認証オプションを使用して CoA を有効にするグローバル コンフィギュレーション機能を使用できます。Cisco ISE の CoA でポート バウンスを設定している場合は、「CoA 免除」の項で説明されているように、プロファイリング サービスにより他の CoA が発行されることがあります。

選択したグローバル コンフィギュレーションでは、より具体的な設定がない場合のみ、デフォルトの CoA 動作が規定されます。「エンドポイント プロファイリング ポリシーごとの許可変更の設定 （808 ページ）」を参照してください。

RADIUS プローブまたはモニタリング ペルソナの REST API を使用して、エンドポイントの認証できます。RADIUS プローブを有効にして、パフォーマンスを向上させることができます。CoA を有効にした場合は、Cisco ISE アプリケーションで CoA 設定と合わせて RADIUS プローブを有効にしてパフォーマンスを向上させることを推奨します。これにより、プロファイリング サービスは収集された RADIUS 属性を使用して、エンドポイントに適切な CoA を発行できます。

Cisco ISE アプリケーションで RADIUS プローブを無効にした場合は、モニタリング ペルソナの REST API を使用して CoA を発行できます。これにより、プロファイリング サービスは幅

広いエンドポイントをサポートできます。分散展開では、モニタリング ペルソナの REST API を使用して CoA を発行するために、モニタリング ペルソナを担当する Cisco ISE ノードがネットワークに少なくとも 1 つ存在している必要があります。

プライマリおよびセカンダリ モニタリング ノードは同一のセッション ディレクトリ情報を持つため、Cisco ISE は、分散展開内の REST クエリーのデフォルトの宛先としてプライマリおよびセカンダリ モニタリング ノードを適宜指定します。

許可変更の発行の使用例

次の場合に、プロファイリング サービスによって許可変更が発行されます。

- エンドポイントが削除される：エンドポイントが [エンドポイント（Endpoints）] ページから削除され、そのエンドポイントがネットワークから接続解除または排除された場合。
- 例外アクションが設定される：エンドポイントに異常または許容できないイベントをもたらす例外アクションがプロファイルごとに設定されている場合。プロファイリング サービスは、CoA を発行して対応するスタティック プロファイルにエンドポイントを移動します。
- エンドポイントが初めてプロファイリングされる：エンドポイントがスタティックに割り当てられておらず、初めてプロファイリングされる場合（たとえば、プロファイルが不明プロファイルから既知のプロファイルに変更された場合）。
    - エンドポイント ID グループが変更される：エンドポイントが許可ポリシーで使用されるエンドポイント ID グループに対して追加または削除された場合。

      エンドポイント ID グループが変更され、エンドポイント ID グループが次のために許可ポリシーで使用されている場合、プロファイリング サービスは CoA を発行します。
        - 動的にプロファイリングされる場合のエンドポイントに対するエンドポイント ID グループの変更
        - ダイナミック エンドポイントに対してスタティック割り当てフラグが true に設定されている場合のエンドポイント ID グループの変更
- エンドポイント プロファイリングのポリシーが変更され、ポリシーが許可ポリシーで使用される：エンドポイント プロファイリング ポリシーが変更され、許可ポリシーで使用される論理的なプロファイルにそのポリシーが含まれる場合。エンドポイント プロファイリング ポリシーは、プロファイリング ポリシーの一致のため、または、エンドポイントが論理的なプロファイルに関連付けられたエンドポイント プロファイリング ポリシーにスタティックに割り当てられるときに、変更される場合があります。両方の場合で、エンドポイント プロファイリング ポリシーが許可ポリシーで使用される場合のみ、プロファイリング サービスは CoA を発行します。

許可変更の発行の免除

エンドポイントIDグループが変更され、スタティック割り当てがすでにtrueの場合、プロファイリング サービスはCoA を発行しません。

Cisco ISE は次の理由で CoA を発行しません。

- エンドポイントがネットワークから切断されている：ネットワークから切断されているエンドポイントが検出された場合。
- 有線（Extensible Authentication Protocol）EAP 対応エンドポイントが認証された：認証された有線 EAP 対応エンドポイントが検出された場合。
- ポートごとに複数のアクティブセッション：1 つのポートに複数のアクティブなセッションがある場合は、CoA に [ポート バウンス（Port Bounce）] オプションを設定しても、プロファイリング サービスによって [再認証（Reauth）] オプションが指定された CoA が発行されます。
- ワイヤレス エンドポイント検出時のパケット オブ ディスコネクト CoA（セッションの終了）：エンドポイントがワイヤレスとして検出されて、パケットオブディスコネクトCoA（セッション終了）がポート バウンス CoA の代わりに送信された場合。この変更の利点は、ワイヤレス LAN コントローラ（WLC）CoA がサポートされていることです。
- プロファイラ CoA は、許可プロファイルで設定された論理プロファイルに対して、[論理プロファイルでエンドポイントのプロファイラCoAを抑制する（Suppress Profiler CoA for endpoints in Logical Profile）] オプションを使用すると抑制されます。デフォルトでは、プロファイラ CoA は他のすべてのエンドポイントに対してトリガーされます。
- グローバルな [CoA なし（No CoA）] 設定がポリシー CoA を上書きする：グローバルな [CoA なし（No CoA）] は、エンドポイント プロファイリング ポリシーのすべての構成設定を上書きします。エンドポイント プロファイリングポリシーごとに設定された CoA に関係なく、Cisco ISE で CoA が発行されないためです。

（注） [CoA なし（No CoA）] および [再認証（Reauth）] CoA 設定は影響を受けません。また、プロファイラ サービスは有線およびワイヤレス エンドポイントに同じ CoA の設定を適用します。

CoA 設定の各タイプに発行される許可変更

表 *90 : CoA* 設定の各タイプに発行される許可変更

シナリオ	CoA なし設定	ポート バウンス設定	再認証設定	その他の情報
Cisco ISE における CoA グローバル コンフィギュレーション（一般的な設定）	CoA なし（No CoA）	ポート バウンス	再認証（Reauthentication）	—
エンドポイントがネットワークで検出された場合	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	許可変更は、RADIUS 属性の Acct -Status -Type 値 Stop で判別されます。
同じスイッチ ポートで複数のアクティブ セッションと有線接続	CoA なし（No CoA）	再認証（Reauthentication）	再認証（Reauthentication）	再認証は、他のセッションの切断を回避します。
ワイヤレス エンドポイント	CoA なし（No CoA）	切断パケット CoA（セッション終了）	再認証（Reauthentication）	ワイヤレス LAN コントローラに対するサポート。
不完全な CoA データ	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	原因は RADIUS 属性の欠落。

ISE データベースの持続性とパフォーマンスの属性フィルタ

Cisco ISE は、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP ヘルパーと DHCP SPAN の両方）、HTTP、RADIUS、およびシンプル ネットワーク管理プロトコルの各プローブのフィルタを実装しています。ただし、パフォーマンスの低下に対処するために NetFlow は除外されています。各プローブ フィルタには、一時的でエンドポイント プロファイルとは関係のない属性のリストが含まれ、これらの属性はプローブによって収集された属性から削除されます。

isebootstrap ログ（isebootstrap-yyyymmdd-xxxxxx.log）には、辞書からの属性がフィルタリングされた状態で、辞書の作成を処理するメッセージが含まれます。エンドポイントがフィルタリ

ング フェーズを通過するときに、フィルタリングが行われたことを示すデバッグ メッセージをログに記録するように設定することもできます。

Cisco ISE プロファイラは、次のエンドポイント属性フィルタを呼び出します。

- DHCP ヘルパーと DHCP SPAN の両方の DHCP フィルタには、不要なすべての属性が含まれ、これらの属性は DHCP パケットの解析後に削除されます。フィルタリング後の属性は、エンドポイントのエンドポイント キャッシュ内にある既存の属性とマージされます。
- HTTP フィルタは、HTTP パケットからの属性のフィルタリングに使用され、フィルタリング後の属性セットに大幅な変更はありません。
- RADIUS フィルタは、syslog 解析が完了すると使用され、エンドポイント属性がプロファイリングのためにエンドポイント キャッシュにマージされます。
- SNMP クエリー用の SNMP フィルタには、CDP および LLDP フィルタが含まれています。これらのフィルタはすべて SNMP クエリー プローブに使用されます。

ホワイトリストを使用してエンドポイント属性をフィルタリングするグローバル設定

収集ポイントで頻繁には変わらないエンドポイント属性の数を減らして、永続性イベントおよび複製イベントの数を減らすことができます。[エンドポイント属性フィルタ（EndPoint Attribute Filter）] を有効にすると、Cisco ISE プロファイラは、重要な属性のみを保持し、その他の属性をすべて廃棄します。重要な属性とは、Cisco ISE システムによって使用される属性またはエンドポイント プロファイリング ポリシーやルールで明確に使用される属性です。

[エンドポイント属性フィルタ（EndPoint Attribute Filter）] を有効にするには、CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定（765 ページ）の項を参照してください。

ホワイトリストは、カスタム エンドポイント プロファイリング ポリシー内でエンドポイントのプロファイリングに使用される属性のセットであり、許可変更（CoA）、個人所有デバイスの持ち込み（BYOD）、デバイス登録 WebAuth（DRW）などが Cisco ISE で期待どおりに機能するために不可欠な属性のセットです。ホワイトリストは、無効になっている場合でも、エンドポイントの所有権が変わった場合に（属性が複数のポリシーのサービス ノードによって収集されている場合）、常に基準として使用されます。

デフォルトではホワイトリストは無効で、属性は、属性フィルタが有効になっている場合にのみドロップされます。ホワイトリストは、フィードからの変更など、エンドポイントプロファイリングポリシーが変更されると、プロファイリングポリシーに新しい属性を含めるように、動的に更新されます。ホワイトリストにない属性は収集時に即座にドロップされ、属性をプロファイリングエンドポイントに加えることはできません。バッファリングと組み合わせると、永続性イベントの数を減らすことができます。

ホワイトリストに次の2つのソースから決定された属性のセットが含まれていることを確認する必要があります。

- エンドポイントをプロファイルに適合させるためにデフォルトプロファイルで使用される属性のセット。
- 許可変更（CoA）、個人所有デバイスの持ち込み（BYOD）、デバイス登録 WebAuth（DRW）などが Cisco ISE で期待どおりに機能するために不可欠な属性のセット。

（注） ホワイトリストに新しい属性を追加するには、管理者がその属性を使用する新しいプロファイラ条件とポリシーを作成する必要があります。この新しい属性は、保存された属性と複製された属性のホワイトリストに自動的に追加されます。

表 *91* : ホワイトリストの属性

AAA-Server	BYODRegistration
Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	説明
DestinationIPAddress	Device Identifier
デバイス名（Device Name）	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
[FQDN]	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	製品

RegistrationTimeStamp	—
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

IOS センサー組み込みスイッチからの属性の収集

IOS センサーの統合によって、Cisco ISE ランタイムと Cisco ISE プロファイラでスイッチから送信された任意またはすべての属性を収集できるようになりました。RADIUS プロトコルを使用して、DHCP、CDP、および LLDP 属性をスイッチから直接収集できます。DHCP、CDP、および LLDP について収集された属性は、解析され、次の場所のプロファイラ ディクショナリの属性にマッピングされます（**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）]**）。

デバイス センサー用にサポートされている Catalyst プラットフォームについては、https://communities.cisco.com/docs/DOC-72932 を参照してください。

IOS センサー組み込みネットワーク アクセス デバイス

IOS センサー組み込みネットワーク アクセス デバイスと Cisco ISE の統合では、次のコンポーネントが含まれます。

- IOS センサー
- DHCP、CDP および LLDP のデータを収集するためにネットワーク アクセス デバイス（スイッチ）に組み込まれているデータ コレクタ
- データを処理し、エンドポイントのデバイス タイプを決定するアナライザ

アナライザを展開するには次の 2 つの方法がありますが、2 つを組み合わせて使用することは想定されていません。

- アナライザを Cisco ISE に展開する
- アナライザをセンサーとしてスイッチに組み込む

IOS センサー組み込みネットワーク アクセス デバイスの設定チェックリスト

ここでは、スイッチから直接 DHCP、CDP、および LLDP の属性を収集するために、IOS センサー対応スイッチと Cisco ISE で設定する必要のある作業のリストの概要を説明します。

- RADIUS プローブが Cisco ISE で有効になっていることを確認します。
- ネットワーク アクセス デバイスで DHCP、CDP、および LLDP 情報を収集するための IOS センサーがサポートされていることを確認します。
- ネットワーク アクセス デバイスで、エンドポイントから CDP 情報と LLDP 情報を取得するために次の CDP コマンドと LLDP コマンドが実行されていることを確認します。

```
cdp enable
lldp run
```

- 標準の AAA コマンドと RADIUS コマンドを使用して、セッション アカウンティングが個別に有効になっていることを確認します。

  コマンドの使用例を示します。

```
aaa new-model
aaa accounting dot1x default start-stop group radius

radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
radius-server vsa send accounting
```

- IOS センサー固有のコマンドを実行していることを確認します。
  - アカウンティング拡張の有効化

    ネットワーク アクセス デバイスで IOS センサー プロトコル データを RADIUS アカウンティング メッセージに追加したり、新しいセンサー プロトコル データの検出時に追加のアカウンティング イベントを生成したりできるようにする必要があります。つまり、RADIUS アカウンティング メッセージには、すべての CDP、LLDP、および DHCP 属性が含まれている必要があります。

    次のグローバル コマンドを入力します。

    device-sensor accounting

  - アカウンティング拡張の無効化

（アカウンティング機能がグローバルに有効になっている場合、）（アカウンティング）ネットワーク アクセス デバイスで、特定のポートでホストされているセッションについて IOS センサー プロトコル データを RADIUS アカウンティング メッセージに追加できないようにするには、適切なポートで次のコマンドを入力します。

no device-sensor accounting

- TLV 変更のトラッキング

  デフォルトでは、サポートされている各ピアプロトコルでクライアント通知とアカウンティングイベントが生成されるのは、特定のセッションのコンテキストで前に受信したことのないタイプ、長さ、値（TLV）が着信パケットに含まれている場合だけです。

  新しい TLV が存在するか、または前に受信した TLV の値が異なる場合は、すべての TLV 変更に対するクライアント通知とアカウンティング イベントを有効にする必要があります。次のコマンドを入力します。

  device-sensor notify all-changes

- ネットワーク アクセス デバイスで IOS Device Classifier（ローカル アナライザ）が無効になっていることを確認します。

  次のコマンドを入力します。

```
no macro auto monitor
```

（注） このコマンドにより、ネットワーク アクセス デバイスは変更ごとに 2 つの同じ RADIUS アカウンティング メッセージを送信できなくなります。

ISE プロファイラによる Cisco IND コントローラのサポート

ISE は、Cisco Industrial Network Director（IND）に接続されたデバイスの状態をプロファイル化して表示できます。PxGrid は、ISE と Cisco Industrial Network Director を接続してエンドポイント（IoT）データの通信を行います。ISE の pxGrid は CIND イベントを消費し、CIND にクエリを行ってエンドポイント タイプを更新します。

ISE プロファイラには、IoT デバイス用のディクショナリ属性があります。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** に移動し、システム ディクショナリのリストから *IOTASSET* を選択して、ディクショナリ属性を確認します。

ガイドラインと推奨事項

プロファイル用に複数の ISE ノードが設定されている場合、1 つのノードで IND の pxGrid を有効にすることを推奨します。

ISE がダウンした場合、再起動したときに CIND で IND に再接続します。再接続するには、CIND の [pxGrid] ページに移動し、**[再接続（Reconnect）]** をクリックします。

複数の IND デバイスを単一の ISE に接続できます。

複数のパブリッシャ（IND）から同じエンドポイントを受信した場合、ISE は最後のパブリッシャのデータのみをそのエンドポイント用に保持します。

pxGrid で、ISE はサービス名 *com.cisco.endpoint.asset* および */topic/com.cisco.endpoint.asset.* から IND データを受け取ります。

IND プロファイリング プロセス フロー

CIND アセット ディスカバリでは IoT デバイスを検出し、そのデバイスのエンドポイント データを pxGrid にパブリッシュします。ISE は、pxGrid 上のイベントを認識し、エンドポイント データを取得します。ISE のプロファイラ ポリシーは、ISE プロファイラ ディクショナリ内の属性にデバイス データを割り当て、これらの属性を ISE のエンドポイントに適用します。

ISE の既存の属性を満たさない IoT エンドポイント データは保存されません。ただし、ISE でさらに属性を作成して CIND に登録することができます。

ISE は、pxGrid を介した CIND への接続が最初に確立されるときにエンドポイントの一括ダウンロードを行います。ネットワークに障害があると、ISE は蓄積されたエンドポイント変更を再び一括ダウンロードします。

IND プロファイル用の ISE および CIND の設定

（注） CIND で pxGrid を有効化する前に、ISE 証明書を CIND にインストールし、CIND 証明書を ISE にインストールする必要があります。

1. ISE で pxGrid を有効にする：**[管理（Administration）]** > **[展開（Deployment）]** に移動します。pxGrid コンシューマとして使用する予定の PSN を編集し、pxGrid を有効にします。この PSN は、Cisco IND およびプロファイリングによってパブリッシュされた pxGrid データからエンドポイントを作成します。
2. ISE で pxGrid 証明書を作成する：**[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** に移動し、pxGrid が実行中であることを確認します。次に **[証明書（Certificates）]** タブをクリックし、証明書フィールドに入力します。**[作成（Create）]** をクリックすると証明書が発行され、ダウンロードディレクトリを選択するためのウィンドウが開かれます。証明書は選択したディレクトリに zip 形式でダウンロードされます。
   - [処理の選択（I want to）] では「**単一の証明書の生成（証明書署名要求なし）（Generate a single certificate without a certificate signing request）**」を選択し、接続する CIND の名前を入力します。

- [証明書のダウンロード形式（Certificate Download Format）] では、**PKS12 形式**を選択します。
- [証明書のパスワード（Certificate Password）] では、パスワードを作成します。

（注） ISEの内部CAが有効になっている必要があります。ご使用のブラウザでポップアップをブロックしている場合は、証明書をダウンロードできません。証明書を解凍して、この次の手順でPEM ファイルを使用できるようにします。

3. CIND で CIND 証明書をエクスポートする：CIND で **[設定（Settings）]** > **[pxGrid]** に移動し、**[.pem IND 証明書をインストールする（Download .pem IND certificate）]** をクリックします。このウィンドウを開いたままにします。
4. ISE で **[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** > **[すべてのクライアント（All Clients）]** に移動します。IND pxGrid クライアントが表示されたら、それを承認します。
5. CIND でスライダを移動して、pxGrid を有効にします。別の画面が開き、そこで ISE ノードの場所、ISE で pxGrid サーバ用に入力した証明書の名前、指定したパスワードを定義します。**[証明書のアップロード（Upload Certificate）]** をクリックして、ISE pxGrid PEM ファイルを検索します。
6. ISE で CIND システム証明書をインポートする：**[管理（Administration）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** に移動し、**[インポート（Import）]** ボタンをクリックして、CIND から取得した証明書のパスを入力します。
7. CIND で **[アクティベート（Activate）]** をクリックします。
8. ISE で、[管理（Adminstration）] > [展開（Deployment）] に移動し、IND 接続に使用している PSN を選択し、[プロファイリング（Profiling）] ページを選択して、pxGrid プローブを有効にします。
9. ISE と CIND の間の pxGrid 接続がアクティブになりました。それを確認するには、CIND が検出した IoT エンドポイントを表示します。

IND プロファイリング用の属性の追加

CINDは、ISEディクショナリに含まれない属性を返す場合があります。ISEに属性をさらに追加することによって、IoT デバイスをより正確にプロファイルすることができます。新しい属性を追加するには、ISE でカスタム属性を作成し、pxGrid を介してその属性を CIND に送信します。

1. ISE で属性を作成する：**[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[設定（Settings）]** に移動して、**エンドポイント カスタム属性**を選択します。属性のエンドポイント属性を作成します。

2. これで、プロファイラ ポリシーでこの属性を使用して、新しい属性でアセットを識別できるようになります。**[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** に移動して、新しいプロファイラ ポリシーを作成します。[ルール（Rule）] セクションで、新しいルールを作成します。属性または値を追加する場合は、[CUSTOMATTRIBUTE] フォルダと、作成したカスタム属性を選択します。

プロファイラ条件

プロファイラ条件はポリシー要素であり、他の条件とほとんど同じです。ただし、認証、許可、およびゲスト条件とは異なり、プロファイリング条件は限られた数の属性に基づいています。[プロファイラ条件（Profiler Conditions）] ページに Cisco ISE で使用できる属性とその説明が表示されます。

プロファイラ条件は次のとおりです。

- シスコ提供：Cisco ISE には展開時に事前定義されたプロファイリング条件が含まれており、[プロファイラ条件（Profiler Conditions）] ページでシスコ提供の条件として識別されます。シスコ提供のプロファイリング条件を削除することはできません。

  [ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[ディクショナリ（Dictionaries）]>[システム（System）] からアクセスできる場所にあるシステム プロファイラ ディクショナリにもシスコ提供条件があります。

  たとえば、MAC ディクショナリです。一部の製品では、OUI（固有識別子情報）がデバイスの製造組織を識別するために最初に使用できる固有属性です。これはデバイスの MAC アドレスのコンポーネントです。MAC ディクショナリには、MACAddress および OUI 属性が含まれています。

- 管理者作成：ユーザが Cisco ISE の管理者として作成するプロファイラ条件、複製された事前定義済みのプロファイリング条件は管理者作成として識別されます。[プロファイラ条件（Profiler Conditions）] ページでプロファイラ ディクショナリを使用して、DHCP、MAC、SNMP、IP、RADIUS、NetFlow、CDP、LLDP、および NMAP タイプのプロファイラ条件を作成できます。

プロファイリング ポリシーの数の推奨上限は 1000 ですが、最高 2000 までプロファイリング ポリシーを拡張できます。

プロファイリング ネットワーク スキャン アクション

エンドポイント スキャン アクションは、エンドポイント プロファイリング ポリシーで参照できる設定可能なアクションであり、ネットワーク スキャン アクションに関連付けられている条件が満たされるとトリガーされます。

Cisco ISE システムにおけるリソース使用量を制限するために、エンドポイントをスキャンする場合はエンドポイント スキャンが使用されます。ネットワーク スキャン アクションでは、リソースを大量に消費するネットワーク スキャンとは異なり、1 つのエンドポイントをスキャ

ンします。これにより、エンドポイントの全体的な分類が向上し、エンドポイントのエンドポイントプロファイルが再定義されます。エンドポイントスキャンは、1度に1つずつしか処理できません。

1 つのネットワーク スキャン アクションをエンドポイント プロファイリング ポリシーに関連付けることができます。Cisco ISE には、ネットワーク スキャン アクションに 3 つの走査方式が事前定義されています。たとえば、OS-scan、SNMPPortsAndOS-scan、および CommonPortsAndOS-scan といった3つの走査方式のいずれか、またはすべてを含めることができます。OS-scan、SNMPPortsAndOS-scan、および CommonPortsAndOS-scans を編集または削除できません。これらは、Cisco ISE の事前定義済みネットワーク スキャン アクションです。独自の新しいネットワーク スキャン アクションを作成することもできます。

エンドポイントを適切にプロファイリングしたら、設定済みのネットワーク スキャンアクションをエンドポイントに対して使用できません。たとえば、Apple-Device をスキャンすると、スキャンされたエンドポイントを Apple デバイスに分類できます。OS-scan によってエンドポイントで実行されているオペレーティング システムが特定されたら、Apple-Device プロファイルに一致しなくなりますが、Apple デバイスの適切なプロファイルに一致します。

新しいネットワーク スキャン アクションの作成

エンドポイント プロファイリング ポリシーに関連付けられたネットワーク スキャン アクションでは、エンドポイントのオペレーティング システム、簡易ネットワーク管理プロトコル（SNMP）ポート、および一般ポートがスキャンされます。シスコでは、最も一般的な NMAP スキャンのためのネットワーク スキャン アクションを提供していますが、独自のものを作成することもできます。

新しいネットワーク スキャンを作成する場合は、NMAP プローブがスキャンする情報のタイプを定義します。

始める前に

ネットワーク スキャン（NMAP）プローブは、ネットワーク スキャン アクションをトリガーするルールを定義する前にイネーブルにする必要があります。その手順は、「Cisco ISE ノードごとのプローブの設定」で説明します。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[プロファイリング（Profiling）]** > **[ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）]** を選択します。または、**[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[ポリシー要素（Policy Elements）]** > **[NMAPスキャンアクション（NMAP Scan Actions）]** を選択することもできます。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するネットワーク スキャン アクションの名前と説明を入力します。

ステップ 4 次のエンドポイントをスキャンする場合、1 つ以上のチェックボックスをオンにします。

- [OSのスキャン（Scan OS）]：オペレーティング システムをスキャンする場合
- [SNMP ポートのスキャン（Scan SNMP Port）]：SNMP ポート（161、162）をスキャンする場合

- [一般ポートのスキャン（Scan Common Port）]：一般ポートをスキャンする場合
- [カスタム ポートのスキャン（Scan Custom Ports）]：カスタム ポートをスキャンする場合。
- [サービス バージョン情報を含むスキャン（Scan Include Service Version Information）]：デバイスの詳細な説明を含むことがあるバージョン情報をスキャンする場合。
- [SMB 検出スクリプトの実行（Run SMB Discovery Script）]：SMB ポート（445 および 139）をスキャンして、OS やコンピュータ名などの情報を取得する場合。
- [NMAP ホスト検出のスキップ（Skip NMAP Host Discovery）]：NMAP スキャンの最初のホスト検出ステージをスキップする場合。

（注） [NMAP ホスト検出のスキップ（Skip NMAP Host Discovery）] オプションは自動 NMAP スキャンではデフォルトでオンになっていますが、手動 NMAP スキャンを実行する場合は選択する必要があります。

ステップ 5 [送信（Submit）] をクリックします。

NMAP オペレーティング システム スキャン

オペレーティング システム スキャン（OS-scan）タイプでは、エンドポイントで実行されているオペレーティング システム（および OS バージョン）がスキャンされます。これはリソースを大量に消費するスキャンです。

NMAP ツールには、信頼できない結果をまねく可能性がある OS-scan 上の制限があります。たとえば、スイッチやルータなどのネットワーク デバイスのオペレーティング システムをスキャンすると、NMAP OS-scan から、それらのデバイスについて正しくない operating-system 属性が返されることがあります。Cisco ISE は精度が 100% ではない場合でも、operating-system 属性を表示します。

ルールで NMAP operating-system 属性を使用するエンドポイント プロファイリング ポリシーに低い確実度値の条件（確実度係数の値）を設定する必要があります。NMAP:operating-system 属性に基づいてエンドポイント プロファイリング ポリシーを作成するときは、NMAP からの不正な結果をフィルタリングする AND 条件を含めることを推奨します。

[OS のスキャン（Scan OS）] をエンドポイント プロファイリング ポリシーに関連付けた場合、次の NMAP コマンドはオペレーティング システムをスキャンします。

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

次の NMAP コマンドを使用すると、サブネットがスキャンされ、nmapSubnet.log に出力が送信されます。

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

表 *92 :* 手動サブネット スキャンの *NMAP* コマンド

-O	OS 検出の有効化

-sU	UDP スキャン
-p <port ranges>	特定のポートのみスキャンします。たとえば、U:161, 162 と指定します。
oN	通常の出力
oX	XML 出力

オペレーティング システム ポート

次の表に、NMAP が OS のスキャンに使用する TCP ポートを示します。また、NMAP は ICMP および UDP ポート 51824 を使用します。

1	3	4	[6]	7	9	13	17	19
20	21	22	23	24	25	26	30	32
33	37	54	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
[1000]	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040 ～ 1100
1102	1104	1105	1106	1107	1108	1110	1111	1112

1113	1114	1117	1119	1121	1122	1123	1124	1126
1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720
1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972	1974	1984	1998 ～ 2010	2013	2020	2021
2022	2030	2033	2034	2035	2038	2040 ～ 2043	2045 ～ 2049	2065
2068	2099	2100	2103	2105 ～ 2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381 ～ 2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659

3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000 ～ 4006	4045	4111	4125	4126	4129	4224	4242
4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000 ～ 5004	5009	5030
5033	5050	5051	5054	[5060]	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900 ～ 5907	5910	5911	5915	5922	5925	5950	5952	5959
5960 ～ 5963	5987 ～ 5989	5998 ～ 6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565 ～ 6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080 ～ 8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654

8701	8800	8873	8888	8899	8994	9,000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616
10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774
32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389
50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

NMAP SNMP ポート スキャン

SNMP ポート（161 および 162）が開いている場合、SNMPPortsAndOS-scan タイプは、エンドポイントが実行中のオペレーティング システム（およびOSバージョン）をスキャンし、SNMP クエリーをトリガーします。さらに分類するために、識別されて不明プロファイルと最初に一致したエンドポイントに使用できます。

[SNMP ポートのスキャン（Scan SNMP Port）] をエンドポイント プロファイリング ポリシーに関連付けた場合、次の NMAP コマンドは SNMP ポート（UDP 161 と 162）をスキャンします。

nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>

表 *93 :* エンドポイントの *SNMP* ポート スキャンの *NMAP* コマンド

-sU	UDP スキャン。
-p <port-ranges>	特定のポートのみスキャンします。たとえば、UDP ポート 161 と 16.2 をスキャンします
oN	通常の出力。
oX	XML 出力。
IP-address	スキャン対象のエンドポイントの IP アドレス。

NMAP 一般ポート スキャン

CommanPortsAndOS-scan タイプでは、エンドポイントで実行されているオペレーティング システム（および OS バージョン）がスキャンされ、SNMP ポートではなく一般ポート（TCP と UDP）もスキャンされます。[一般ポートのスキャン（Scan Common Port）] をエンドポイント プロファイリング ポリシーに関連付けると、次の NMAP コマンドが一般ポートをスキャンします。nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>

表 *94 :* エンドポイントの一般ポート スキャンの *NMAP* コマンド

-sTU	TCP 接続スキャンと UDP スキャンの両方。
-p <port ranges>	TCP ポート 21、22、23、25、53、80、110、135、139、143、443、445、3306、3389、8080、および UDP ポート 53、67、68、123、135、137、138、139、161、445、500、520、631、1434、1900 をスキャンします。
oN	通常の出力。
oX	XML 出力。
IP アドレス	スキャン対象のエンドポイントの IP アドレス。

一般ポート

次の表に、NMAP がスキャンのために使用する一般的なポートを示します。

表 *95*：一般ポート

TCP ポート（TCP Ports）		**UDP ポート**	
ポート	**サービス**	**ポート**	**サービス**
21/tcp	FTP	53/udp	ドメイン
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	ドメイン	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	ルート
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

NMAP カスタム ポート スキャン

一般的なポートに加えて、カスタム ポートを使用して（**[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシー要素（Policy Elements）] > [NMAP スキャン アクション（NMAP Scan Actions）]** または **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）]**）、自動および手動 NMAP スキャン動作を指定できます。NMAP プローブが、指定した開いているカスタム ポートを通じてエンドポイントから属性を収集します。これらの属性は、[ISE ID（ISE Identity）] ページのエンドポイントの属性で更新されます（**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]**）。各スキャン動作に、最大で 10 個の UDP および 10 個の TCP ポートを指定することができます。一般ポートとして指定されているものと同じポート番号を使用できません。詳細については、「McAfee ePolicy Orchestrator を使用してプロファイリング ポリシーを設定します」のセクションを参照してください。

サービス バージョン情報を含む NMAP スキャン

サービス バージョン情報を含む NMAP プローブは、デバイスで実行されているサービスに関する情報を収集することによる、より優れた分類のためにエンドポイントを自動的にスキャンします。このサービス バージョン オプションは、一般ポートまたはカスタム ポートと組み合わせることができます。

例：

CLI コマンド：nmap -sV -p T:8083 172.21.75.217

出力：

[ポート（Port）]	状態	サービス	バージョン
8083/tcp	open	http	McAfee ePolicy Orchestrator Agent 4.8.0.1500 (ePOServerName: WIN2008EPO, AgentGuid: {15D70A24-33BA-40A7-762E})

NMAP SMB 検出スキャン

NMAP SMB 検出スキャンにより、Windows バージョンを区別し、よりよいエンドポイントのプロファイリングが得られます。NMAP が提供する SMB 検出スクリプトを実行するように NMAP スキャン アクションを設定できます。

NMAP スキャン アクションは Windows のデフォルト ポリシーに組み込まれ、エンドポイントがポリシーおよびスキャン ルールに一致すると、そのエンドポイントでスキャンされ、結果は、正確な Windows バージョンの決定に役立ちます。さらに、ポリシーは、フィード サービスで設定され、新しい事前定義済 NMAP スキャンが SMB の検出オプションで作成されます。

NMAP スキャン アクションは Microsoft ワークステーション ポリシーにより呼び出され、スキャンの結果は、オペレーティング システムの属性の下のエンドポイントに保存され、Windows ポリシーに活用されます。また、サブネットの手動スキャンの SMB 検出スクリプト オプションも用意されています。

（注） SMB 検出では、エンドポイントで Windows ファイル共有オプションを有効にしてください。

SMB 検出属性

SMB 検出スクリプトがエンドポイントで実行されるときに、新しい SMB 検出属性（SMB.Operating-system など）がエンドポイントに追加されます。これらの属性は、フィード サービスの Windows エンドポイント プロファイリング ポリシーの更新に対して考慮されます。SMB 検出スクリプトが実行されるときに、SMB 検出属性には SMB.operating-system、

SMB.lanmanager、SMB.server、SMB.fqdn、SMB.domain、SMB.workgroup、SMB.cpe などのように、SMB が前に追加されます。

NMAP ホスト検出のスキップ

それぞれの IP アドレスのすべてのポートをスキャンすることは時間のかかるプロセスです。スキャンの目的によって、アクティブなエンドポイントの NMAP ホストの検出を省略できます。

NMAP スキャンがエンドポイントの分類の後にトリガーされると、プロファイラはエンドポイントのホストの検出を常にスキップします。ただし、手動スキャン アクションが NMAP ホスト検出のスキップ スキャンを有効にした後でトリガーされると、ホストの検出がスキップされます。

NMAP スキャン ワークフロー

NMAP スキャンを実行するための手順：

始める前に

NMAP SMB 検出スクリプトを実行するには、そのシステムでファイル共有を有効にする必要があります。例については、「NMAP SMB 検出スクリプトを実行するためのファイル共有の有効化」トピックを参照してください。

ステップ 1 SMB スキャン アクションの作成。

ステップ 2 SMB スキャン アクションを使用したプロファイラ ポリシーの設定。

ステップ 3 SMB 属性を使用した新しい条件の追加。

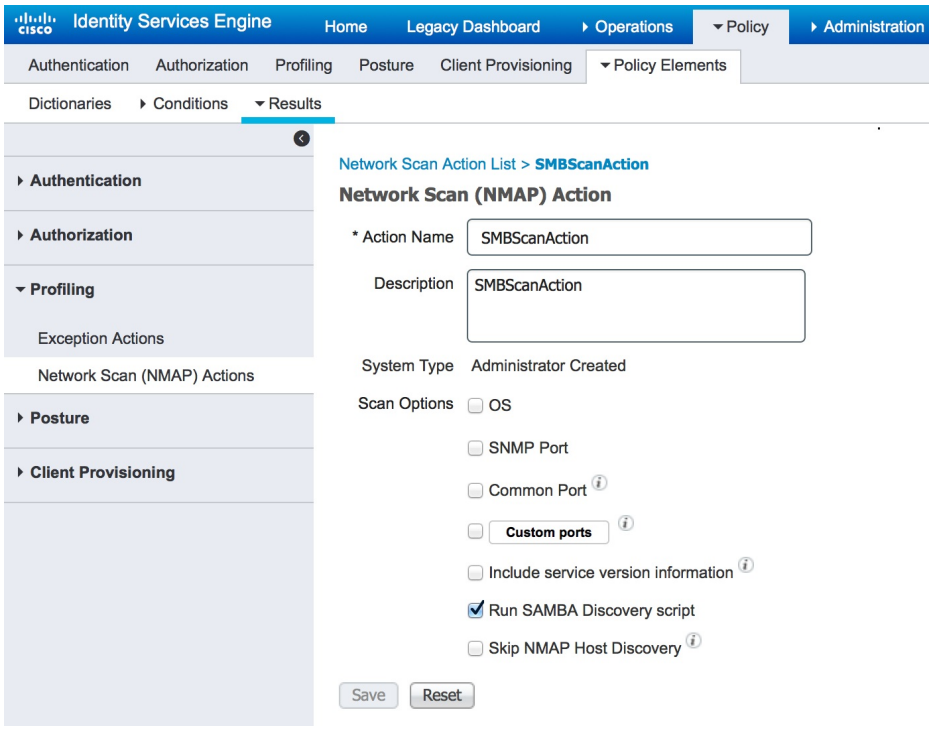
SMB スキャン アクションの作成

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[プロファイリング（Profiling）]** > **[ネットワーク スキャン（NMAP）アクション（Network Scan（NMAP）Actions）]** ページを選択します。

ステップ 2 [アクション名（Action Name）] と [説明（Description）] に入力します。

ステップ 3 [SMB 検出スクリプトの実行（Run SMB Discovery Script）] チェックボックスをオンにします。

ステップ 4 [追加（Add）] をクリックして、ネットワーク アクセス ユーザを作成します。



次のタスク

SMB スキャン アクションを使用してプロファイラ ポリシーを設定する必要があります。

SMB スキャン アクションを使用したプロファイラ ポリシーの設定

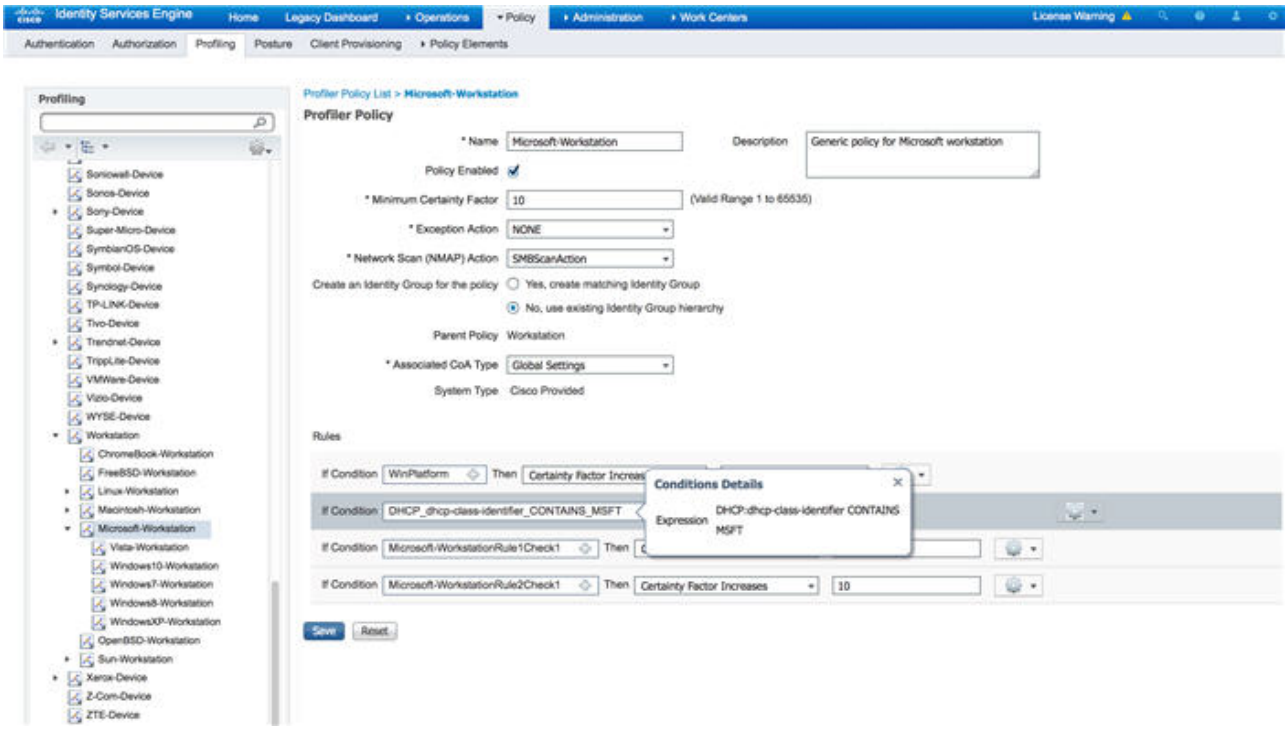
始める前に

SMB スキャン アクションを使用してエンドポイントをスキャンするための新しいプロファイラ ポリシーを作成する必要があります。たとえば、DHCP クラス ID に MSFT 属性が含まれている場合にネットワーク アクションを実行する必要があるルールを指定して、Microsoft Workstation をスキャンすることができます。

ステップ 1 **[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[追加（Add）]** ページの順に選択します。

ステップ 2 [名前（Name）] と [説明（Description）] に入力します。

ステップ 3 ドロップダウンで、作成したスキャン アクション（SMBScanAction など）を選択します。
ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Action）



次のタスク

SMB 属性を使用して新しい条件を追加する必要があります。

SMB 属性を使用した新しい条件の追加

始める前に

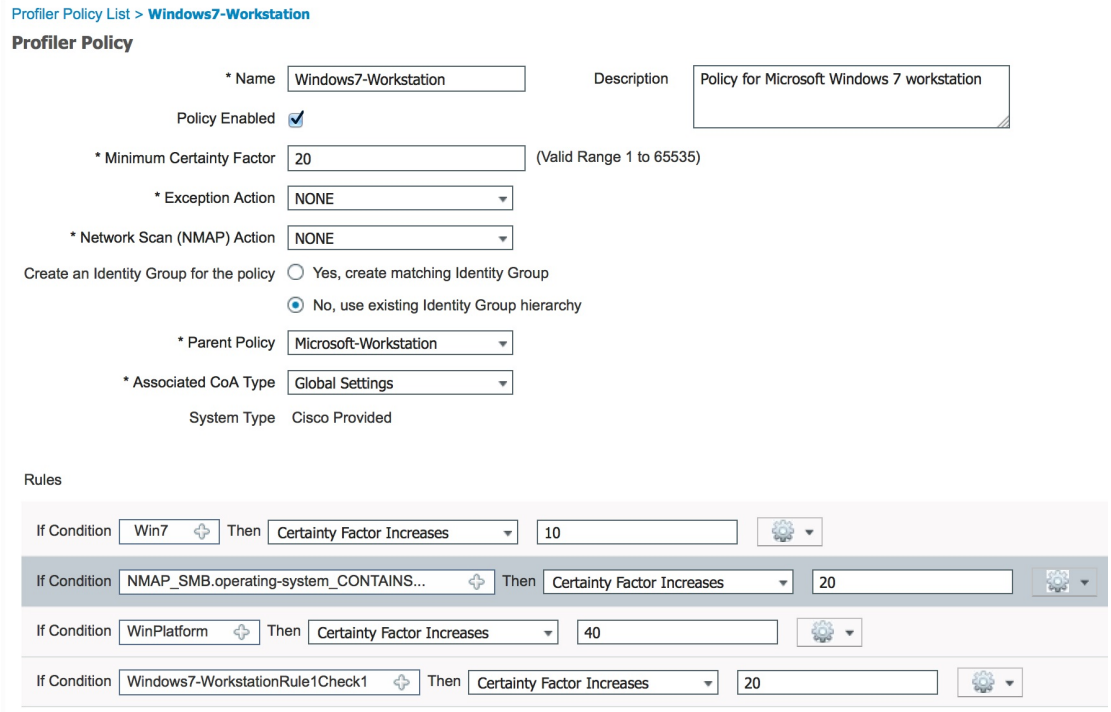
エンドポイントのバージョンをスキャンするには新しいプロファイラ ポリシーを作成する必要があります。たとえば、Microsoft ワークステーション親ポリシーの下で Windows 7 をスキャンできます。

ステップ 1 **[ポリシー（Policy）] > [プロファイリング（Profiling）] > [追加（Add）]** ページの順に選択します。

ステップ 2 [名前（Name）]（たとえば Windows-7Workstation）と [説明（Description）] を入力します。

ステップ 3 [ネットワーク スキャン（NMAP）アクション（Network Scan（NMAP）Action）] ドロップダウンでは [なし（None）] を選択します。

ステップ 4 [親ポリシー（Parent Policy）] ドロップダウンでは Microsoft ワークステーション ポリシーを選択します。



NMAP SMB 検出スクリプトを実行するためのファイル共有の有効化

NMAP SMB 検出スクリプトを実行するために、Windows OS バージョン 7 のファイル共有を有効にする例を次に示します。

ステップ 1 [コントロール パネル] > [ネットワークとインターネット] の順に選択します。

ステップ 2 [ネットワークと共有センター（Network and Sharing Center）] を選択します。

ステップ 3 [共有の詳細設定の変更] を選択します。

ステップ 4 [ファイルとプリンターの共有を有効にする] オプション ボタンが選択されていることを確認します。

ステップ 5 [40 ビット暗号化または 56 ビット暗号化を使用するデバイスのためのファイル共有を有効にする] オプション ボタンと [パスワード保護の共有を有効にする] オプション ボタンが選択されていることを確認します。

ステップ 6 （オプション）[変更を保存] をクリックします。

ステップ 7 ファイアウォール設定を設定します。

a) コントロール パネルで、**[システムとセキュリティ]** > **[Windows ファイアウォール]** > **[Windows ファイアウォールによるプログラムの許可]** の順に選択します。

b) [ファイルとプリンターの共有] チェックボックスを必ずオンにしてください。

c) [OK] をクリックします。

ステップ 8 共有フォルダを設定します。

a) 接続先フォルダを右クリックし、[プロパティ] を選択します。

b) [共有] タブをクリックし、[共有] をクリックします。

c) [ファイルの共有] ダイアログボックスで、必要な名前を追加して、[共有] をクリックします。
d) 選択したフォルダを共有した後で、[完了] をクリックします。
e) [詳細な共有] をクリックし、[このフォルダーの共有] チェックボックスをオンにします。
f) [アクセス許可（Permissions）] をクリックします。
g) [スキャンのアクセス許可（Permissions for Scans）] ダイアログボックスで、[全員（Everyone）] を選択し、[フル コントロール（Full Control）] チェックボックスをオンにします。
h) [OK] をクリックします。

NMAP スキャンからのサブネットの除外

エンドポイントの OS または SNMP ポートを特定するために NMAP スキャンを実行できます。

NMAP スキャンを実行するときに、NMAP でスキャンしないサブネット全体または IP 範囲を除外できます。[NMAP スキャン サブネット除外（NMAP Scan Subnet Exclusions）] ページ（[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）] > [NMAP スキャン サブネット除外（NMAP Scan Subnet Exclusions）]）でサブネットまたは IP 範囲を設定できます。これにより、ネットワークの負荷が制限され、相当の時間を節約できます。

手動 NMAP スキャンの場合は、[手動 NMAP スキャンの実行（Run Manual NMAP Scan）] ページ（[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャン（Manual NMAP Scan）] > [NMAP スキャン サブネット除外の設定（Configure NMAP Scan Subnet Exclusions At）]）を使用してサブネットまたは IP 範囲を指定できます。

手動 NMAP スキャンの設定

自動 NMAP スキャンに使用可能なオプションを使用して手動 NMAP スキャン（**[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャン（Manual NMAP Scan）]**）を実行できます。スキャン オプションまたは事前定義されているオプションを選択できます。

表 *96 :* 手動 *NMAP* スキャンの設定

フィールド	使用上のガイドライン
ノード	NMAP スキャンが実行する ISE ノードを選択します。
サブネットの手動スキャン（Manual Scan Subnet）	NMAP スキャンを実行するエンドポイントのサブネットの IP アドレスの範囲を入力します。

フィールド	使用上のガイドライン
NMAP スキャン サブネット除外の設定（Configure NMAP Scan Subnet Exclusions At）	**[ワーク センター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[設定（Settings）]** > **[NMAP スキャン サブネット除外（NMAP Scan Subnet Exclusions）]** ページに誘導されます。除外する IP アドレスとサブネット マスクを指定します。一致が見つかると、NMAP スキャンは実行されません。
NMAP スキャン サブネット	• スキャン オプションの指定 • または、既存の NMAP スキャンを選択します
スキャン オプションの指定	必要なスキャン オプションを選択します（OS、SNMP ポート、共通ポート、カスタム ポート、サービス バージョン情報を含む、SMB 検出スクリプトの実行、NMAP ホスト検出のスキップ）。詳細については、「新しいネットワーク スキャン アクションの作成」のトピックを参照してください。
既存の NMAP スキャンを選択します	[既存の NMAP スキャン アクション（Existing NMAP Scan Actions）] ドロップダウンが表示され、デフォルトのプロファイラ NMAP スキャン アクションが表示されます。
デフォルトのスキャン オプションにリセット（Reset to Default Scan Options）	デフォルト設定を復元するには、このボタンをクリックします（すべてのスキャン オプションをチェックします）。
名前を付けて NMAP スキャン アクションを保存（Save as NMAP Scan Action）	アクション名と説明を入力します。

手動 NMAP スキャンの実行

ステップ 1 **[ワーク センター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[手動スキャン（Manual Scans）]** > **[手動 NMAP スキャン（Manual NMAP Scan）]** の順に選択します。

ステップ 2 [ノード（Node）] ドロップダウンで、NMAP スキャンを実行する予定の ISE ノードを選択します。

ステップ 3 [サブネットの手動スキャン（Manual Scan Subnet）] テキスト ボックスに、オープン ポートをチェックする予定のエンドポイントのサブネット アドレスを入力します。

ステップ 4 必要な [スキャン オプション（Scan Options）] を選択します。

a) [スキャン オプションの指定（Specify Scan Options）] を選択し、ページの右側で、必要なスキャン オプションを選択します。詳細については、「新しいネットワーク スキャン アクションの作成」ページを参照してください。

b) または、[既存の NMAP スキャン アクションの選択（Select An Existing NMAP Scan Action）] を選択して、MCAFeeEPOOrchestratorClientScan などのデフォルトの NMAP アクションを選択します。

ステップ 5 [スキャンの実行（Run Scan）] をクリックします。

McAfee ePolicy Orchestratorを使用してプロファイリング ポリシーを設定します

サービスのプロファイリングを行うCisco ISEは、McAfee ePolicy Orchestrator （McAfee ePO）クライアントをエンドポイントに登録するかどうかが検出されます。これにより、特定のエンドポイントが組織に属しているかどうかを確認する上で役立ちます。

プロセスに関与するエンティティは、:

- ISEサーバ
- McAfee ePOサーバ
- McAfee ePO Agent

Cisco ISEは、オンボードNMAPスキャン動作（）をMCAFeeEPOOrchestratorClientscan McAfeeのエージェントが設定されているポート上でNMAP McAfeeのスクリプトを使用して、エンドポイントで実行されているかどうかを確認できます。また、カスタム ポートマップを使用して新しいNMAPスキャン オプション作成できます（たとえば、8082）。McAfee ePOソフトウェアを使用して、次の手順に従って、新しいNMAPスキャン動作を設定可能:

ステップ 1 McAfee ePo NMAP スキャン アクションの設定。

ステップ 2 McAfee ePO Agent の設定。

ステップ 3 McAfee ePO NMAP スキャン アクションを使用したプロファイラ ポリシーの設定。

McAfee ePo NMAP スキャン アクションの設定

ステップ 1 **[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [ポリシー要素（Policy Elements）] > [ネットワーク スキャン（NMAP）アクション（Network Scan（NMAP）Actions）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [アクション名（Action Name）] と [説明（Description）] に入力します。

ステップ 4 [スキャン オプション（Scan Options）] では、[カスタム ポート（Custom Ports）] をオンにします。

ステップ 5 [カスタム ポート（Custom Ports）] ダイアログボックスで、必要な TCP ポートを追加します。TCP ポート 8080 は、McAfee ePO に対してデフォルトで有効になっています。

ステップ 6 [サービス バージョン情報を含む（Include Service Version Information）] チェック ボックスをオンにします。

ステップ 7 [送信（Submit）] をクリックします。

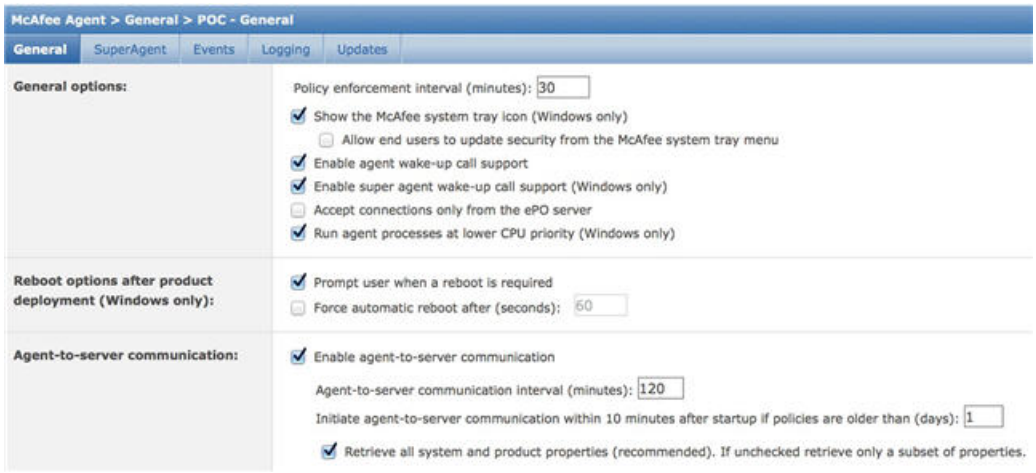
次のタスク

McAfee ePO Agent を設定します。

McAfee ePO Agent の設定

ステップ 1 McAfee ePO サーバで、McAfee ePO Agent と ISE サーバ間の通信を容易にするために推奨される設定を確認します。

図 *36 : McAfee ePO Agent* の推奨されるオプション



ステップ 2 [ePO サーバからのみ接続を受け入れる（Accept Connections Only From The ePO Server）] のマークが外されていることを確認します。

次のタスク

McAfee ePO NMAP スキャン アクションを使用して、プロファイラ ポリシーを設定します。

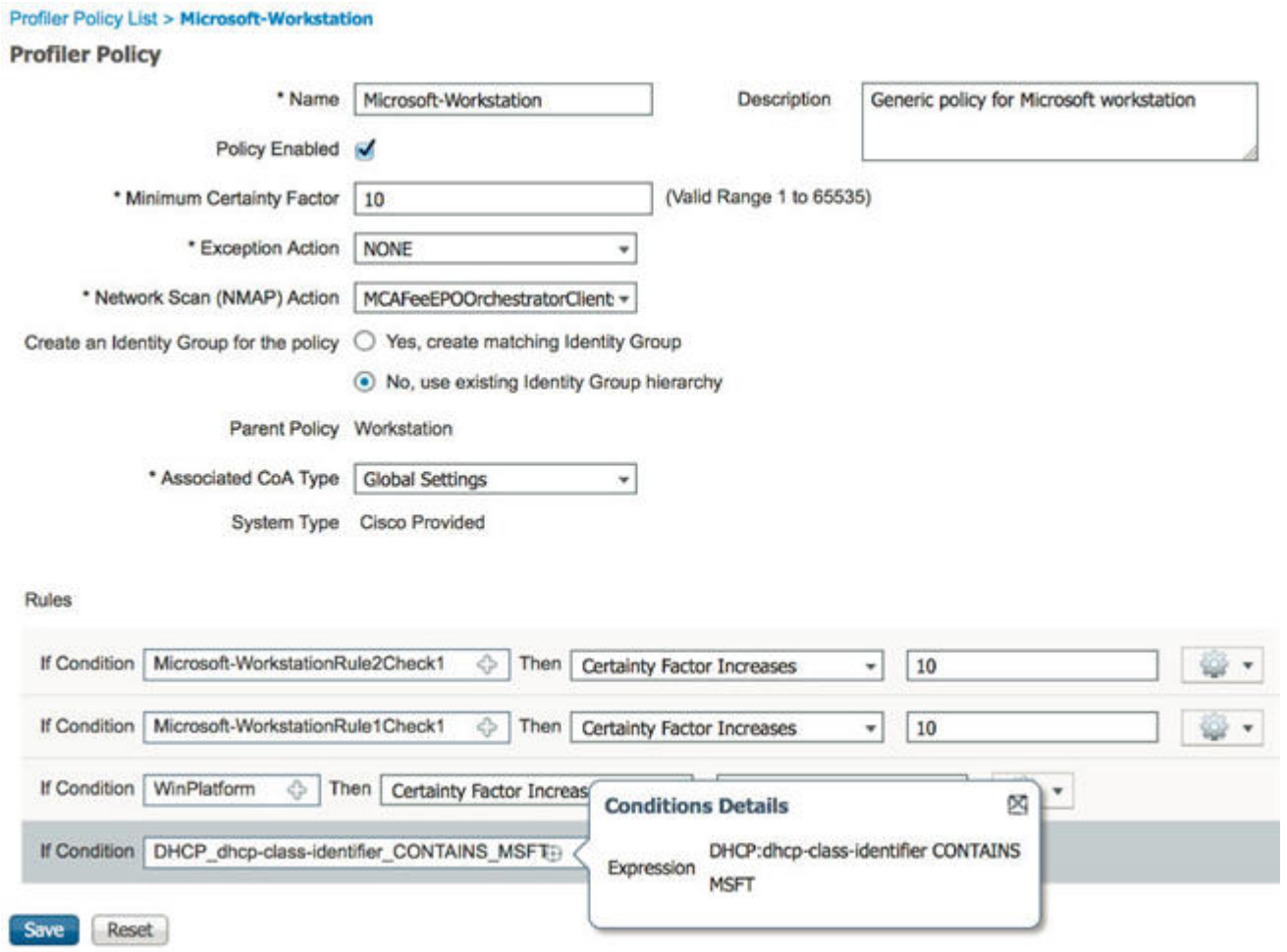
McAfee ePO NMAP スキャン アクションを使用したプロファイラ ポリシーの設定

ステップ 1 **[ポリシー（Policy）] > [プロファイリング（Profiling）] > [追加（Add）]** の順に選択します。

ステップ 2 [名前（Name）] と [説明（Description）] に入力します。

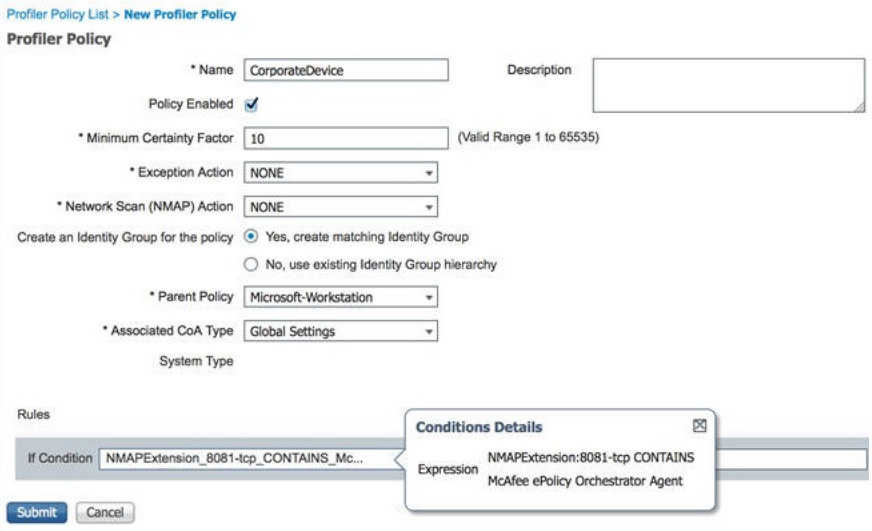
ステップ 3 [ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Action）] ドロップダウンで、必要なアクション（MCAFeeEPOOrchestratorClientscan など）を選択します。

ステップ 4 親プロファイラ ポリシー（DHCP クラス ID に MSFT 属性が含まれているかどうかを確認するルールを含む Microsoft-Workstation など）を作成します。



ステップ 5 McAfee ePO Agent がエンドポイントにインストールされているかどうかを確認するために、親 NMAP McAfee ePO ポリシー（Microsoft-Workstation など）内に新しいポリシー（CorporateDevice など）を作成します。

条件を満たすエンドポイントが会社のデバイスとしてプロファイルされます。このポリシーを使用して、McAfee ePO Agent によってプロファイルされたエンドポイントを新しい VLAN に移動することができます。



プロファイラ エンドポイント カスタム属性

エンドポイントの **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント カスタム属性（Endpoint Custom Attributes）]** ページを使用して、エンドポイントがプローブから収集する属性の他に、属性をエンドポイントに割り当てることができます。エンドポイントのカスタム属性は、認可ポリシーでエンドポイントのプロファイルを作成するために使用できます。

最大100個のエンドポイントのカスタム属性を作成できます。サポートされるエンドポイントのカスタム属性の型は次のとおりです：Int、String、Long、Boolean および Float。

[コンテキストディレクトリ（Context Directory）] > [エンドポイント（Endpoints）] > [エンドポイント分類（Endpoint Classification）] ページで、エンドポイントのカスタム属性の値を追加できます。

エンドポイントのカスタム属性に対するユースケースには、特定の属性に基づくホワイトリストまたはブラックリストデバイスへ、または認証に基づく特定の権限の割り当てが含まれています。

認証ポリシーでのエンドポイント カスタム属性の使用

[エンドポイントカスタム属性（Endpoint Custom Attributes）]セクションを使用すると、追加の属性を設定できます。各定義は属性とタイプ（String、Int、Boolean、Float、Long）で構成されます。エンドポイントカスタム属性を使用して、デバイスのプロファイリングを行うことができます。

（注） エンドポイントにカスタム属性を追加するには、plus 以降のライセンスが必要です。

エンドポイント カスタム属性を使用して許可ポリシーを作成する手順を以下に示します。

ステップ 1 エンドポイント カスタム属性を作成し、値を割り当てます。

a) **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント カスタム属性（Endpoint Custom Attributes）]** の順に選択します。

b) [エンドポイント カスタム属性（Endpoint Custom Attributes）] 領域で、[属性名（Attribute Name）]（たとえば、deviceType）と [データ型（Data Type）]（たとえば、String）とパラメータを入力します。

c) [保存（Save）] をクリックします。

d) **[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [概要（Summary）]** の順に選択します。

e) カスタム属性値を割り当てます。

- 必要な MAC アドレスのチェックボックスをオンにし、[編集（Edit）] をクリックします。
- または、必要な MAC アドレスをクリックして、[エンドポイント（Endpoints）] ページで、[編集（Edit）] をクリックします。

f) [エンドポイントの編集（Edit Endpoint）] ダイアログボックスの [カスタム属性（Custom Attribute）] 領域に、必須の属性値（たとえば、deviceType = Apple-iPhone）を入力します。

g) [保存（Save）] をクリックします。

ステップ 2 カスタム属性と値を使用して許可ポリシーを作成します。

a) **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]** を選択します。

b) エンドポイントの辞書からカスタム属性を選択することで、許可ポリシーを作成します（たとえば、Rule Name: Corporate Devices, Conditions:EndPoints:deviceType Contains Apple-iPhone, Permissions: then PermitAccess）。

c) **[保存（Save）]** をクリックします。

関連トピック

プロファイラ エンドポイント カスタム属性 （796 ページ）

プロファイラ条件の作成

Cisco ISE のエンドポイント プロファイリング ポリシーを使用すると、ネットワーク上で検出されたエンドポイントを分類し、特定のエンドポイント ID グループに割り当てることができます。これらのエンドポイント プロファイリング ポリシーは、エンドポイントを分類し、グループ化するために Cisco ISE が評価するプロファイリング条件から構成されます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [プロファイリング（Profiling）] > [追加（Add）]** を選択します。

ステップ 2 エンドポイント プロファイリング ポリシーの設定 （799 ページ）の説明に従って、フィールドに値を入力します。

ステップ 3 [送信（Submit）] をクリックして、プロファイラ条件を保存します。

ステップ 4 さらに多くの条件を作成するには、この手順を繰り返します。

エンドポイント プロファイリング ポリシー ルール

ルールを定義すると、すでにポリシー要素ライブラリに作成および保存されているライブラリから 1 つ以上のプロファイリング条件を選択し、確実度係数の整数値を各条件に関連付けるか、例外アクションまたはネットワーク スキャン アクションをその条件に関連付けることができます。例外アクションまたはネットワーク スキャン アクションは、Cisco ISE がエンドポイントの分類全体に関するプロファイリング ポリシーを評価しているときに、設定可能なアクションをトリガーするために使用します。

特定のポリシー内のルールが OR 演算子で個別に評価されると、各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。エンドポイント プロファイリング ポリシーのルールが一致した場合、そのプロファイリング ポリシーおよび一致するポリシーは、それらがネットワーク上で動的に検出された場合のエンドポイントと同じです。

ルール内で論理的にグループ化される条件

エンドポイント プロファイリング ポリシー（プロファイル）には、単一の条件または AND 演算子や OR 演算子を使用して論理的に結合された複数の単一条件の組み合わせが含まれ、これらの条件と照合して、ポリシー内の特定のルールについてエンドポイントをチェック、分類、およびグループ化することができます。

条件は、収集されたエンドポイント属性値をエンドポイントの条件に指定されている値と照合するために使用されます。複数の属性をマッピングする場合は、条件を論理的にグループ化して、ネットワーク上のエンドポイントの分類に使用できます。ルールで対応する確実度メトリック（定義済みの整数値）が関連付けられている 1 つ以上の条件とエンドポイントを照合するか、または、条件に関連付けられた例外アクション、または条件に関連付けられたネットワーク スキャン アクションをトリガーすることができます。

確実度係数

プロファイリング ポリシーの最小確実度メトリックは、エンドポイントの一致するプロファイルを評価します。エンドポイント プロファイリング ポリシーの各ルールには、プロファイリング条件に関連付けられた最小確実度メトリック（整数値）があります。確実度メトリックは、エンドポイント プロファイリング ポリシー内のすべての有効ルールに対して追加される

尺度で、エンドポイント プロファイリング ポリシー内の各条件がエンドポイントの全体的な分類の改善にどの程度役立つかを測定します。

各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。すべての有効なルールの確実度メトリックが合計され、照合の確実度が求められます。この値は、エンドポイントプロファイリング ポリシーに定義されている最小の確実度係数を超えている必要があります。デフォルトでは、すべての新しいプロファイリング ポリシー ルールおよび事前に定義されたプロファイリング ポリシーで、最小の確実度係数は 10 です。

エンドポイント プロファイリング ポリシーの設定

次の表では、[エンドポイントポリシー（Endpoint Policies）] ウィンドウのフィールドについて説明します。このページのナビゲーション パスは、**[ポリシー（Policy）] > [プロファイリング（Profiling）] > [プロファイリング ポリシー（Profiling Policies）]** です。

表 *97* : エンドポイント プロファイリング ポリシーの設定

フィールド名	使用上のガイドライン
名前（Name）	作成するエンドポイントプロファイリング ポリシーの名前を入力します。
説明	作成するエンドポイントプロファイリング ポリシーの説明を入力します。
ポリシー有効（Policy Enabled）	デフォルトでは [ポリシー有効（Policy Enabled）] チェックボックスはオンになっており、エンドポイントのプロファイリング時に、一致するプロファイリング ポリシーが関連付けられます。 オフになっている場合、エンドポイントのプロファイリング時に、エンドポイントプロファイリング ポリシーは除外されます。
最小確実度計数（Minimum Certainty Factor）	プロファイリング ポリシーに関連付ける最小値を入力します。デフォルト値は 10 です。
例外アクション（Exception Action）	プロファイリング ポリシー内のルールを定義するときに条件に関連付ける例外アクションを選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [例外アクション（Exception Actions）] で定義されます。

フィールド名	使用上のガイドライン
ネットワーク スキャン（NMAP）アクション（**Network Scan (NMAP) Action**）	必要に応じて、プロファイリング ポリシー内のルールを定義するときに条件に関連付けるネットワーク スキャン アクションをリストから選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）] > [結果（Results）]>[プロファイリング（Profiling）]>[ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Actions）] で定義されます。
ポリシーの ID グループの作成（**Create an Identity Group for the policy**）	エンドポイント ID グループを作成するには、次のオプションのいずれかをオンにします。 • はい、一致する ID グループを作成します（**Yes, create matching Identity Group**） • いいえ、既存の ID グループ階層を使用します（**No, use existing Identity Group hierarchy**）
はい、一致する ID グループを作成します（**Yes, create matching Identity Group**）	既存のプロファイリング ポリシーを使用する場合、このオプションを選択します。 このオプションは、これらのエンドポイントの一致する ID グループを作成します。エンドポイント プロファイルが既存のプロファイリング ポリシーと一致した場合に、ID グループは Profiled エンドポイント ID グループの子になります。 たとえば、ネットワーク上で検出されたエンドポイントが Xerox-Device プロファイルに一致する場合は、[エンドポイント ID グループ（Endpoint Identity Groups）] ページで Xerox-Device エンドポイント ID グループが作成されます。

フィールド名	使用上のガイドライン
いいえ、既存の ID グループ階層を使用します（**No, use existing Identity Group hierarchy**）	プロファイリング ポリシーおよび ID グループの階層構造を使用して、一致する親エンドポイント ID グループにエンドポイントを割り当てるには、このチェックボックスをオンにします。 このオプションを使用すると、エンドポイントプロファイリング ポリシー階層を利用することができ、エンドポイントはいずれかの一致する親エンドポイント ID グループ、さらに、親 ID グループに関連付けられたエンドポイント ID グループに割り当てられます。 たとえば、既存のプロファイルに一致するエンドポイントは、適切な親エンドポイント ID グループの下にグループ化されます。ここで、不明プロファイルに一致するエンドポイントは、[不明（Unknown）] の下にグループ化され、既存のプロファイルに一致するエンドポイントは、プロファイリングされたエンドポイント ID グループの下にグループ化されます。次の例を参考にしてください。 • エンドポイントが Cisco-IP-Phone プロファイルに一致する場合、これらのエンドポイントは Cisco-IP-Phone エンドポイント ID グループの下でグループ化されます。 • エンドポイントが Workstation プロファイルに一致する場合、これらのエンドポイントは、Workstation エンドポイント ID グループの下でグループ化されます。 Cisco-IP-Phone および Workstation エンドポイント ID グループは、システム内の Profiled エンドポイント ID グループに関連付けられます。
親ポリシー（**Parent Policy**）	新しいエンドポイントプロファイリング ポリシーを関連付ける、システムで定義されている親プロファイリングポリシーを選択します。 子にルールと条件を継承できる親プロファイリング ポリシーを選択できます。

フィールド名	使用上のガイドライン
関連 CoA タイプ（Associated CoA Type）	エンドポイントプロファイリングポリシーと関連付ける次のいずれかの CoA タイプを選択します。 • CoA なし（No CoA） • ポート バウンス • 再認証（Reauth） • [グローバル設定（Global Settings）] : [管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）] で設定されたプロファイラ設定から適用されます。
ルール（Rule）	エンドポイントプロファイリングポリシーで定義された 1 つ以上のルールにより、エンドポイントの一致するプロファイリングポリシーが決定されます。これにより、プロファイルに応じたエンドポイントのグループ化が可能になります。 ポリシー要素ライブラリからの 1 つ以上のプロファイリング条件がルールに使用され、エンドポイント属性およびその値が、全体的な分類用に検証されます。

フィールド名	使用上のガイドライン
条件（**Conditions**）	

フィールド名	使用上のガイドライン
	プラス（+）記号をクリックして、条件の固定オーバーレイを展開します。マイナス（-）記号をクリックするか、固定オーバーレイの外側をクリックして条件を閉じます。 [既存の条件をライブラリから選択（Select Existing Condition from Library）] または [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] をクリックします。 [既存の条件をライブラリから選択（Select Existing Condition from Library）]：ポリシー要素ライブラリからシスコによって事前定義された条件を選択して、式を定義できます。 [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）]：さまざまなシステム辞書またはユーザ定義辞書から属性を選択して、式を定義できます。 プロファイリング条件と次のいずれかとを関連付けることができます。 • 各条件の確実度係数の整数値 • その条件の例外アクションまたはネットワーク スキャン アクション プロファイリング条件と関連付ける、次のいずれかの定義済み設定を選択します。 • [確実度計数が増加する（Certainty Factor Increases）]：各ルールの確実度値を入力します。この値は、全体的な分類に関するすべての一致ルールに対して追加されます。 • [例外の操作を行う（Take Exception Action）]：このエンドポイント プロファイリング ポリシーの [例外アクション（Exception Action）] フィールドで設定された例外アクションがトリガーされます。 • [ネットワークスキャンを行う（Take Network Scan Action）]：このエンドポイント プロファイリング ポリシーの [ネットワークスキャン（NMAP）アクション

フィールド名	使用上のガイドライン
	（Network Scan (NMAP) Action）] フィールドで設定されたネットワーク スキャン アクションがトリガーされます。
既存の条件をライブラリから選択（Select Existing Condition from Library）	次を実行できます。 • ポリシー要素ライブラリに存在するシスコによって事前定義された条件を選択できます。AND または OR 演算子を使用して複数の条件を追加できます。 • [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。 • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます • [複製（Duplicate）]：選択した条件のコピーを作成します • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます • [削除（delete）]：選択した条件を削除します。

フィールド名	使用上のガイドライン

新しい条件の作成（高度なオプション）（**Create New Condition (Advance Option)**）	次を実行できます。
	• 式にアドホック属性/値の組み合わせを追加し、AND または OR 演算子を使用すると、複数の条件を追加できます。
	• [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。
	  • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます
	  • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます
	  • [複製（Duplicate）]：選択した条件のコピーを作成します
	  • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます
	  • [削除（delete）]：選択した条件を削除します。 AND または OR 演算子を使用できます

関連トピック

Cisco ISE プロファイリング サービス （748 ページ）
エンドポイント プロファイリング ポリシーの作成 （806 ページ）
UDID 属性を使用するエンドポイント コンテキストの可視性 （860 ページ）

エンドポイント プロファイリング ポリシーの作成

[プロファイリング ポリシー（Profiling Policies）] ページを使用して、Cisco ISE の管理者として作成したエンドポイント プロファイリング ポリシーおよび展開時に Cisco ISE によって提供されるエンドポイント プロファイリング ポリシーを管理できます。

新しいプロファイリングポリシーを作成して、エンドポイントをプロファイリングするには、[新しいプロファイラ ポリシー（New Profiler Policy）] ページで次のオプションを使用します。

- ポリシー有効（Policy Enabled）

- [ID グループの作成（Create an Identity Group）]：一致するエンドポイント ID グループを作成するか、またはエンドポイント ID グループ階層を使用するポリシーの場合
- 親ポリシー（Parent Policy）
- 関連 CoA タイプ（Associated CoA Type）

（注） [プロファイリング ポリシー（Profiling Policies）] ページでエンドポイント ポリシーを作成する場合は、Web ブラウザの停止ボタンを使用しないでください。このアクションによって、[新しいプロファイラ ポリシー（New Profiler Policy）] ページでのロードが停止され、アクセス時にリスト ページ内のその他のリスト ページおよびメニューがロードされ、リスト ページ内のフィルタ メニュー以外のすべてのメニューでの操作を実行できなくなります。リスト ページ内ですべてのメニューの操作を実行するには、Cisco ISE からログアウトし、再度ログインする必要がある場合があります。

類似した特性のプロファイリング ポリシーを作成するには、すべての条件を再定義して新しいプロファイリング ポリシーを作成するのではなく、エンドポイント プロファイリング ポリシーを複製して変更することができます。

ステップ 1 **[ポリシー（Policy）]>[プロファイリング（Profiling）]>[プロファイリング ポリシー（Profiling Policies）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成する新しいエンドポイント ポリシーの名前と説明を入力します。[ポリシー有効（Policy Enabled）] チェックボックスはデフォルトでオンになっており、エンドポイントのプロファイリング時に検証するエンドポイント プロファイリング ポリシーが含まれます。

ステップ 4 有効範囲 1 ～ 65535 の最小の確実度係数の値を入力します。

ステップ 5 [例外アクション（Exception Action）] ドロップダウン リストの隣にある矢印をクリックして、例外アクションを関連付けるか、[ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）] ドロップダウン リストの隣にある矢印をクリックして、ネットワーク スキャン アクションを関連付けます。

ステップ 6 [ポリシーの ID グループの作成（Create an Identity Group for the policy）] で次のオプションのいずれか 1 つを選択します。

- **はい、一致する ID グループを作成します（Yes, create matching Identity Group）**
- **いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）**

ステップ 7 [親ポリシー（Parent Policy）] ドロップダウン リストの隣の矢印をクリックして、新しいエンドポイント ポリシーに親ポリシーを関連付けます。

ステップ 8 [関連付ける CoA タイプ（Associated CoA Type）] ドロップダウン リストで、関連付ける CoA タイプを選択します。

ステップ 9 ルールをクリックし、条件を追加して、各条件の確実度係数の整数値を関連付けるか、エンドポイントの全体的な分類のその条件の例外アクションまたはネットワーク スキャン アクションを関連付けます。

ステップ 10 [送信（Submit）] をクリックしてエンドポイント ポリシーを追加するか、または [新しいプロファイラ ポリシー（New Profiler Policy）] ページの [プロファイラ ポリシー リスト（Profiler Policy List）] リンクをクリックして [プロファイリング ポリシー（Profiling Policies）] ページに戻ります。

エンドポイント プロファイリング ポリシーごとの許可変更の設定

Cisco ISE の許可変更（CoA）タイプのグローバル コンフィギュレーションに加えて、各エンドポイント プロファイリング ポリシーに関連付けられた特定のタイプの CoA も発行するように設定できます。

グローバル CoA なしタイプの設定は、エンドポイント プロファイリング ポリシーで設定された各 CoA タイプを上書きします。グローバル CoA タイプが CoA なしタイプ以外に設定されている場合、各エンドポイント プロファイリング ポリシーはグローバル CoA の設定を上書きできます。

CoA がトリガーされると、各エンドポイント プロファイリング ポリシーは、次のように実際の CoA タイプを決定できます。

- [全般設定（General Settings）]：これは、グローバル コンフィギュレーションごとに CoA を発行するすべてのエンドポイント プロファイリング ポリシーのデフォルトの設定です。
- [CoA なし（No CoA）]：この設定はグローバル コンフィギュレーションを上書きし、そのプロファイルの CoA を無効にします。
- [ポート バウンス（Port Bounce）]：この設定は、グローバル ポート バウンスおよび再認証設定タイプを上書きし、ポート バウンス CoA を発行します。
- [再認証（Reauth）]：この設定は、グローバル ポート バウンスおよび再認証設定タイプを上書きし、再認証 CoA を排出します。

（注） プロファイラ グローバル CoA 設定がポート バウンス（または再認証）に設定されている場合は、モバイル デバイスの BYOD フローが切断されないように、対応するエンドポイント プロファイリング ポリシーを [CoA なし（No CoA）]、[ポリシーごとの CoA（per-policy CoA）] オプションを指定して設定していることを確認します。

グローバルおよびエンドポイント プロファイリング ポリシー設定に基づいて各場合に発行されたすべての CoA タイプと実際の CoA タイプが組み合わされた設定については、次の概要を参照してください。

表 *98 :* 設定のさまざまな組み合わせに発行された *CoA* タイプ

グローバル **CoA** タイプ	ポリシーごとに設定されたデフォルトの **CoA** タイプ	ポリシーごとの **CoA** なしタイプ	ポリシーごとのポート バウンス タイプ	ポリシーごとの再認証タイプ
CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）
ポート バウンス	ポート バウンス	CoA なし（No CoA）	ポート バウンス	再認証（Re-Auth）
再認証（Reauth）	再認証（Reauth）	CoA なし（No CoA）	ポート バウンス	再認証（Re-Auth）

エンドポイント プロファイリング ポリシーのインポート

エクスポート機能で作成できる同じ形式を使用して、XML ファイルからエンドポイント プロファイリング ポリシーをインポートできます。親ポリシーが関連付けられている、新しく作成されたプロファイリング ポリシーをインポートする場合は、子ポリシーを定義する前に親ポリシーを定義しておく必要があります。

インポート ファイルでは、エンドポイント プロファイリング ポリシーが階層構造になっており、最初に親ポリシー、次にポリシーに定義されているルールとチェックとともにインポートしたプロファイルが含まれます。

ステップ 1 **[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[プロファイリング（Profiling）]** > [プロファイリング ポリシー（Profiling Policies）] を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、前にエクスポートしてこれからインポートするファイルを特定します。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 [プロファイリング ポリシー（Profiling Policies）] ページに戻るには、[プロファイラ ポリシー リスト（Profiler Policy List）] リンクをクリックします。

エンドポイント プロファイリング ポリシーのエクスポート

他の Cisco ISE 展開にエンドポイント プロファイリング ポリシーをエクスポートできます。または、XML ファイルを独自のポリシーを作成するためのテンプレートとして使用してインポートできます。ファイルをシステムのデフォルトの場所にダウンロードして、後でインポートに使用することもできます。

エンドポイント プロファイリング ポリシーをエクスポートする際にダイアログが表示され、適切なアプリケーションで profiler_policies.xml を開くか、保存するように要求されます。これ

は XML 形式のファイルで、Web ブラウザまたは他の適切なアプリケーションで開くことができます。

ステップ 1 **[ポリシー（Policy）] > [プロファイリング（Profiling）] > [プロファイリング（Profiling）] > [プロファイリング（Profiling Policies）]** を選択します。

ステップ 2 [エクスポート（Export）] を選択し、次のいずれかを選択します。

- [選択済みをエクスポート（Export Selected）] : [プロファイリング ポリシー（Profiling Policies）] ページで選択済みのエンドポイント プロファイリングのポリシーだけをエクスポートできます。
- [選択済みとエンドポイントをエクスポート（Export Selected with Endpoints）] : 選択済みのエンドポイント プロファイリング ポリシーと、選択済みのエンドポイント プロファイリング ポリシーでプロファイリングされたエンドポイントをエクスポートできます。
- [すべてエクスポート（Export All）] : デフォルトでは、[プロファイリング ポリシー（Profiling Policies）] ページのすべてのプロファイリング ポリシーをエクスポートできます。

ステップ 3 [OK] をクリックして、profiler_policies.xml ファイルのエンドポイント プロファイリング ポリシーをエクスポートします。

事前定義されたエンドポイント プロファイリング ポリシー

Cisco ISE を展開するとき、Cisco ISE には事前定義されたデフォルトのプロファイリング ポリシーが含められます。その階層構造を使用して、ネットワーク上の識別されたエンドポイントを分類し、それらを一致するエンドポイント ID グループに割り当てることができます。エンドポイント プロファイリング ポリシーは階層的であるため、[プロファイリング ポリシー（Profiling Policies）] ページにはデバイスの一般的な（親）ポリシーと、親ポリシーが [プロファイリング ポリシー（Profiling Policies）] リスト ページに関連付けられている子ポリシーが表示されます。

[プロファイリング ポリシー（Profiling Policies）] ページには、エンドポイント プロファイリング ポリシーとともに、その名前、タイプ、説明、およびステータス（検証が有効になっているかどうか）が表示されます。

エンドポイント プロファイリング ポリシー タイプは、次のように分類されます。

- シスコ提供：Cisco ISE で事前定義されたエンドポイント プロファイリング ポリシーはシスコ提供タイプとして識別されます。
  - 管理者による変更：事前定義されたエンドポイント プロファイリング ポリシーを変更したときに、エンドポイント プロファイリング ポリシーは管理者による変更タイプとして識別されます。Cisco ISE では、事前定義されたエンドポイント プロファイリング ポリシーに行った変更がアップグレード時に上書きされます。

- 管理者作成：作成したエンドポイント プロファイリング ポリシー、またはシスコ提供のエンドポイント プロファイリング ポリシーを複製したときのエンドポイント プロファイリング ポリシーは、管理者作成タイプとして識別されます。

一連のエンドポイントの一般的なポリシー（親）を作成して、その子がルールと条件を継承できるようにすることを推奨します。エンドポイントを分類する必要がある場合は、エンドポイントをプロファイリングするときに、まずエンドポイントプロファイルを親ポリシーと、次にその子孫（子）ポリシーと照合する必要があります。

たとえば、Cisco-Deviceは、すべてのシスコデバイスの一般的なエンドポイントプロファイリングのポリシーであり、シスコデバイスの他のポリシーは、Cisco-Deviceの子です。エンドポイントをCisco-IP-Phone 7960として分類する必要がある場合は、まずこのエンドポイントのエンドポイント プロファイルを親のCisco-Deviceポリシー、その子のCisco-IP-Phoneポリシーと照合する必要があり、その後さらに分類するためにCisco-IP-Phone 7960 プロファイリング ポリシーと照合します。

（注） Cisco ISE では、管理者によって変更されたポリシーや子ポリシーは、シスコ提供のラベルが付いていても上書きされません。管理者が変更したポリシーが削除されると、以前のシスコ提供のポリシーに戻ります。次にフィードの更新が発生すると、すべての子ポリシーが更新されます。

アップグレード中に上書きされる事前定義されたエンドポイントプロファイリング ポリシー

[プロファイリング ポリシー（Profiling Policies）] ページで既存のエンドポイント プロファイリング ポリシーを編集できます。また、事前定義されたエンドポイント プロファイリング ポリシーを変更するときは、事前定義されたエンドポイントプロファイルのコピーにすべての設定を保存する必要があります。

アップグレード時に、事前定義されたエンドポイントプロファイルに保存した設定が上書きされます。

エンドポイント プロファイリング ポリシーを削除できない

[プロファイリング ポリシー（Profiling Policies）] ページで選択したエンドポイント プロファイリングポリシーまたはすべてのエンドポイントプロファイリングポリシーを削除できます。デフォルトでは、[プロファイリングポリシー（Profiling Policies）]ページからすべてのエンドポイント プロファイリング ポリシーを削除できます。[プロファイリング ポリシー（Profiling Policies）]ページですべてのエンドポイントプロファイリングポリシーを選択して削除しようとしても、エンドポイント プロファイリング ポリシーが他のエンドポイント プロファイリングポリシーにマッピングされた親ポリシーであるか、または許可ポリシーにマッピングされ、かつ他のエンドポイント プロファイリング ポリシーの親ポリシーである場合、そのエンドポイント プロファイリング ポリシーは削除できません。

次の例を参考にしてください。

- シスコ提供のエンドポイント プロファイリング ポリシーは削除できません。
- エンドポイント プロファイルが他のエンドポイント プロファイルの親として定義されている場合は、[プロファイリング ポリシー（Profiling Policies）]ページで親プロファイルを削除できません。たとえば、Cisco-Deviceは、シスコ デバイスの他のエンドポイント プロファイリング ポリシーの親です。
- 許可ポリシーにマッピングされているエンドポイントプロファイルは削除できません。たとえば、Cisco-IP-Phone は Profiled Cisco IP Phones 許可ポリシーにマッピングされ、Cisco IP Phone の他のエンドポイント プロファイリング ポリシーの親です。

Draeger 医療機器用の事前定義済みプロファイリング ポリシー

Cisco ISE のデフォルトのエンドポイント プロファイルには、Draeger 医療機器用の一般的なポリシー、Draeger-Delta 医療機器用のポリシー、および Draeger-M300 医療機器用のポリシーが含まれます。両方の医療機器にポート 2050 と 2150 があるため、デフォルトの Draeger エンドポイント プロファイリング ポリシーを使用しても、Draeger-Delta 医療機器と Draeger-M300 医療機器を分類できません。

使用中の環境では、これらの Draeger デバイスにポート 2050 と 2150 があるため、デフォルトの Draeger-Delta and Draeger-M300 エンドポイント プロファイリング ポリシーでデバイスの宛先 IP アドレスのチェックに加えて、これらの医療機器を区別できるようにルールを追加する必要があります。

Cisco ISE には、Draeger 医療機器のエンドポイント プロファイリング ポリシーで使用される次のプロファイリング条件があります。

- ポート 2000 が含まれる Draeger-Delta-PortCheck1
- ポート 2050 が含まれる Draeger-Delta-PortCheck2
- ポート 2100 が含まれる Draeger-Delta-PortCheck3
- ポート 2150 が含まれる Draeger-Delta-PortCheck4
- ポート 1950 が含まれる Draeger-M300PortCheck1
- ポート 2050 が含まれる Draeger-M300PortCheck2
- ポート 2150 が含まれる Draeger-M300PortCheck3

不明なエンドポイントのエンドポイント プロファイリング ポリシー

既存のプロファイルに一致せず、Cisco ISE でプロファイリングできないエンドポイントは、不明なエンドポイントです。不明プロファイルは、エンドポイントについて収集された属性が Cisco ISE の既存のプロファイルと一致しない場合にそのエンドポイントに割り当てられるデフォルトのシステム プロファイリング ポリシーです。

不明プロファイルは次のシナリオで割り当てられます。

- エンドポイントが Cisco ISE で動的に検出され、そのエンドポイントに一致するエンドポイント プロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。
- エンドポイントが Cisco ISE で静的に追加され、静的に追加されたエンドポイントに一致するエンドポイント プロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。

  ネットワークにエンドポイントを静的に追加した場合、そのエンドポイントは Cisco ISE のプロファイリング サービスによってプロファイリングされません。不明プロファイルを適切なプロファイルに後で変更できます。割り当てたプロファイリング ポリシーは、Cisco ISE によって再プロファイリングされることはありません。

静的に追加されたエンドポイントのエンドポイントプロファイリングポリシー

静的に追加されたエンドポイントをプロファイリングするために、プロファイリング サービスは、新しい MATCHEDPROFILE 属性をエンドポイントに追加することによって、エンドポイントのプロファイルを計算します。計算されたプロファイルは、そのエンドポイントが動的にプロファイリングされるときのエンドポイントの実際のプロファイルです。これにより、静的に追加されたエンドポイントの計算されたプロファイルと動的にプロファイリングされたエンドポイントに一致するプロファイルの間の不一致を見つけることができます。

スタティックIPデバイスのエンドポイントプロファイリングポリシー

静的に割り当てられた IP アドレスを持つエンドポイントがある場合、そのスタティック IP デバイスのプロファイルを作成できます。

スタティック IP アドレスが割り当てられているエンドポイントをプロファイリングするには、RADIUS プローブまたは SNMP クエリー プローブと SNMP トラップ プローブを有効にする必要があります。

エンドポイント プロファイリング ポリシーの一致

1 つ以上のルールで定義されているプロファイリング条件がプロファイリング ポリシーに一致する場合、Cisco ISE は、エンドポイント用に選択されたポリシーを、評価されたポリシーではなく、一致したポリシーであると常に見なします。ここで、そのエンドポイントのスタティック割り当てのステータスがシステムで false に設定されます。ただし、エンドポイントの編集時にスタティック割り当て機能を使用して、システム内の既存のプロファイリング ポリシーに静的に再割り当てした後は、true に設定されることがあります。

次は、エンドポイントの一致したポリシーに適用されます。

- スタティックに割り当てられたエンドポイントでは、プロファイリング サービスは MATCHEDPROFILE を計算します。
- 動的に割り当てられたエンドポイントでは、MATCHEDPROFILE は一致するエンドポイント プロファイルと同じです。

ダイナミック エンドポイントに一致するプロファイリング ポリシーは、プロファイリング ポリシーで定義された 1 つ以上のルールを使用して特定できます。また、分類のために、必要に応じてエンドポイント ID グループを割り当てることができます。

エンドポイントが既存のポリシーにマッピングされる場合、プロファイリング サービスは、一連のポリシーが一致する最も近い親プロファイルをプロファイリング ポリシーの階層で検索し、エンドポイントを適切なエンドポイント ポリシーに割り当てます。

許可に使用するエンドポイント プロファイリング ポリシー

許可ルールにエンドポイント プロファイリング ポリシーを使用できます。このとき、エンドポイント プロファイリング ポリシーのチェックを含めるように属性として新しい条件を作成できます。属性値は、エンドポイント プロファイリング ポリシーの名前になります。エンドポイント プロファイリング ポリシーを、エンドポイント辞書から選択できます。エンドポイント プロファイリング ポリシーには、属性 PostureApplicable、EndPointPolicy、LogicalProfile および BYODRegistration が含まれています。

PostureApplicable の属性値は、オペレーティング システムに基づいて自動設定されます。この値は、IOS および Android デバイスでは [なし（No）] に設定されます。これらのプラットフォームでは、ポスチャを実行するための AnyConnect がないためです。この値は、Mac OSX および Windows デバイスでは [はい（Yes）] に設定されます。

EndPointPolicy、BYODRegistration および ID グループの組み合わせを含む許可ルールを定義できます。

エンドポイント プロファイリング ポリシーの論理プロファイルによるグループ化

論理プロファイルは、エンドポイント プロファイリング ポリシーがシスコ提供か、管理者作成かに関係なく、プロファイルまたは関連付けられているプロファイルのカテゴリのコンテナです。エンドポイント プロファイリング ポリシーは、複数の論理プロファイルに関連付けることができます。

許可ポリシー条件で論理プロファイルを使用して、プロファイルのカテゴリでネットワーク全体のアクセス ポリシーの作成に役立てることができます。許可の単純条件を作成して、許可ルールに含めることができます。許可条件で使用できる属性と値のペアは、論理プロファイル（属性）および論理プロファイルの名前（値）であり、エンドポイント システム ディクショナリ内にあります。

たとえば、カテゴリに一致するエンドポイント プロファイリング ポリシーを論理プロファイルに割り当てることによって、Android、Apple iPhone、Blackberry などのすべてのモバイル デバイスの論理プロファイルを作成できます。Cisco ISE には、すべての IP フォンのデフォルトの論理プロファイルである IP-Phone が含まれ、IP-Phone には、IP-Phone、Cisco IP-Phone、Nortel-IP-Phone-2000-Series、および Avaya-IP-Phone プロファイルが含まれます。

論理プロファイルの作成

エンドポイント プロファイリング ポリシーのカテゴリをグループ化するために使用できる論理プロファイルを作成でき、それにより、プロファイルまたは関連付けられているプロファイルのカテゴリ全体を作成できます。エンドポイント プロファイリング ポリシーを割り当てられたセットから削除して、使用可能なセットに戻すこともできます。ロジカルプロファイルの詳細については、エンドポイントプロファイリングポリシーの論理プロファイルによるグループ化 （814 ページ）を参照してください。

ステップ 1 **[ポリシー（Policy）]>[プロファイリング（Profiling）]>[プロファイリング（Profiling）]>[論理プロファイル（Logical Profiles）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] のテキスト ボックスに新しい論理プロファイルの名前と説明を入力します。

ステップ 4 [使用可能なポリシー（Available Policies）] からエンドポイント プロファイリング ポリシーを選択して、論理プロファイルに割り当てます。

ステップ 5 右矢印をクリックして、選択したエンドポイント プロファイリング ポリシーを [割り当てられたポリシー（Assigned Policies）] に移動します。

ステップ 6 [送信（Submit）] をクリックします。

プロファイリング例外アクション

例外アクションは、エンドポイント プロファイリング ポリシーで参照できる単一の設定可能なアクションであり、アクションに関連付けられている例外条件が満たされるとトリガーされます。

例外アクションのタイプは次のいずれかになります。

- シスコ提供：シスコ提供の例外アクションは削除できません。Cisco ISE では、Cisco ISE のエンドポイントをプロファイリングするときに、次の編集不能なプロファイリング例外アクションがトリガーされます。
  - 許可変更：エンドポイントが許可ポリシーで使用されるエンドポイント ID グループに対して追加または削除される場合、プロファイリング サービスは許可変更を発行します。

- エンドポイント削除：エンドポイントが [エンドポイント（Endpoints）] ページでシステムから削除されるか、Cisco ISE ネットワーク上で編集ページから不明プロファイルに再割り当てされると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。
- FirstTimeProfiled：エンドポイントが Cisco ISE で初めてプロファイリングされ、そのエンドポイントのプロファイルが不明プロファイルから既存のプロファイルに変更されて、そのエンドポイントが Cisco ISE ネットワーク上で認証に失敗すると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。

- 管理者作成：Cisco ISE では、作成したプロファイリング例外アクションがトリガーされます。

例外アクションの作成

1 つ以上の例外ルールを定義し、1 つのプロファイリング ポリシーに関連付けることができます。この関連付けにより、Cisco ISE でエンドポイントをプロファイリングする際にプロファイリング ポリシーが一致し、少なくとも 1 つの例外ルールが一致する場合、例外アクション（単一の設定可能なアクション）がトリガーされます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [例外アクション（Exception Actions）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] のテキスト ボックスに例外アクションの名前と説明を入力します。

ステップ 4 [CoA アクション（CoA Action）] チェックボックスをオンにします。

ステップ 5 [ポリシー割り当て（Policy Assignment）] ドロップダウン リストをクリックしてエンドポイント ポリシーを選択します。

ステップ 6 [送信（Submit）] をクリックします。

ポリシーおよびIDグループのスタティック割り当てによるエンドポイントの作成

[エンドポイント（Endpoints）] ページでエンドポイントの MAC アドレスを使用して、新しいエンドポイントを静的に作成できます。また、スタティック割り当ての [エンドポイント（Endpoints）] ページで、エンドポイント プロファイリング ポリシーおよび ID グループを選択できます。

通常のモバイルデバイス（MDM）エンドポイントは、[エンドポイント ID（Endpoints Identities）] リストに表示されます。リストページには、[ホスト名（Hostname）]、[デバイス タイプ（Device

Type）]、[デバイス ID（Device ID）] など、MDM エンドポイントの属性のカラムが表示されます。[スタティック割り当て（Static Assignment）]、[スタティック グループ割り当て（Static Group Assignment）] などのその他のカラムは、デフォルトでは表示されません。

（注） このページを使用して、MDM エンドポイントを追加、編集、削除、インポートまたはエクスポートすることはできません。

ステップ 1 **[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 エンドポイントの MAC アドレスをコロンで区切られた 16 進表記で入力します。

ステップ 4 [ポリシー割り当て（Policy Assignment）] ドロップダウン リストから一致するエンドポイント ポリシーを選択して、スタティック割り当てステータスをダイナミックからスタティックに変更します。

ステップ 5 [スタティック割り当て（Static Assignment）] チェックボックスをオンにして、エンドポイントに割り当てられたスタティック割り当てのステータスをダイナミックからスタティックに変更します。

ステップ 6 [ID グループ割り当て（Identity Group Assignment）] ドロップダウン リストから、新しく作成されたエンドポイントを割り当てるエンドポイント ID グループを選択します。

ステップ 7 エンドポイント ID グループのダイナミック割り当てをスタティックに変更するには、[スタティック グループ割り当て（Static Group Assignment）] チェックボックスをオンにします。

ステップ 8 [送信（Submit）] をクリックします。

CSV ファイルからのエンドポイントのインポート

Cisco ISE テンプレートから作成した CSV ファイルからエンドポイントをインポートし、エンドポイントの詳細を使用して更新することができます。ISE からエクスポートされたエンドポイントには約 75 個の属性が含まれているため、別の ISE 展開に直接インポートすることはできません。インポートが許可されていない列が CSV ファイルにある場合は、列のリストを含むメッセージが表示されます。ファイルを再度インポートする前に、指定された列を削除する必要があります。

（注） エンドポイントのカスタム属性をインポートするには、正しいデータ タイプを使用して **[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[設定（Settings）]** > **[エンドポイント カスタム属性（Endpoint Custom Attributes）]** ページで CSV ファイルと同じカスタム属性を作成する必要があります。これらのコマンドには、「CUSTOM.」というプレフィックスを付けてエンドポイント属性と区別する必要があります。

インポートできる属性は約 30 あります。このリストには、MACAddress、EndPointPolicy、IdentityGroup が含まれています。オプション属性は次のとおりです。

説明	PortalUser	LastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	デバイスタイプ（Device Type）	host-name
PortalUser.GuestStatus	StaticAssignment	参照先
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<custom attribute name>	—	—

ファイル ヘッダーは、デフォルトのインポート テンプレートで指定されている形式にして、エンドポイントのリストが次の順序で表示されるようにする必要があります。MACAddress、EndpointPolicy、IdentityGroup、<オプション属性として上に記載されている属性のリスト>。次のファイル テンプレートを作成できます。

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <オプション属性として上に記載されている属性のリスト>

MAC アドレスを除くすべての属性値は、CSV ファイルからエンドポイントをインポートする際に省略可能です。特定の値のないエンドポイントをインポートする場合も、値はカンマで区切られます。

次の例を参考にしてください。

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser, など

ステップ 1 **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** の順に選択します。

ステップ 2 [ファイルからインポート（Import from File）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、作成済みの CSV ファイルを見つけます。

ステップ 4 [送信（Submit）] をクリックします。

エンドポイントで使用可能なデフォルトのインポート テンプレート

エンドポイントのインポートに使用できるエンドポイントを更新できるテンプレートを生成できます。デフォルトで、[テンプレートの生成（Generate a Template）] リンクを使用して、Microsoft Office Excel アプリケーションで CSV ファイルを作成し、このファイルをシステム上にローカルに保存できます。ファイルは **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** > **[ファイルからインポート（Import from File）]** にあります。[テンプレートの生成（Generate a Template）] リンクを使用してテンプレートを作成でき、Cisco ISE サーバは、[template.csv を開く（Opening template.csv）] ダイアログを表示します。このダイアログを使用すると、デフォルトの template.csv ファイルを開いたり、template.csv ファイルをシステム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルは Microsoft Office Excel アプリケーションで開かれます。デフォルトの template.csv ファイルには、MAC アドレス、エンドポイント ポリシー、エンドポイント ID グループ、およびその他のオプション属性が表示されるヘッダー行が含まれています。

エンドポイントの MAC アドレス、エンドポイント プロファイリング ポリシー、エンドポイント ID グループを、インポートするオプションの属性値とともに更新し、新しいファイル名を使用してファイルを保存します。このファイルをエンドポイントのインポートのために使用できます。[テンプレートの生成（Generate a Template）] リンクを使用したときに作成される template.csv ファイルのヘッダー行を参照してください。

表 *99 : CSV* テンプレート ファイル

MAC	EndPointPolicy	IdentityGroup	その他のオプションの属性
11:11:11:11:11:11	Android	プロファイル済み	<Empty>/<Value>

インポート中の不明なエンドポイントの再プロファイリング

インポートに使用するファイルに、MAC アドレスを持つエンドポイントがあり、それらに割り当てられているエンドポイントプロファイリング ポリシーが不明プロファイルである場合、これらのエンドポイントはインポート中に Cisco ISE でただちに一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。ただし、不明プロファイルに静的に割り当てられることはありません。エンドポイントに割り当てられているエンドポイント プロファイリング ポリシーが CSV ファイルにない場合、これらのエンドポイントは不明プロファイルに割り当てられ、一致するエンドポイント プロファイリング ポリシーに再プロファイリ

ングされます。次に、Cisco ISE が、インポート中に Xerox_Device プロファイルに一致する不明プロファイルをどのように再プロファイリングするか、および割り当てられていないエンドポイントをどのように再プロファイリングするかを示します。

表 *100* : 不明プロファイル：ファイルからのインポート

MAC アドレス（MAC Address）	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:02	不明。	Xerox-Device
00:00:00:00:01:03	不明。	Xerox-Device
00:00:00:00:01:04	不明。	Xerox-Device
00:00:00:00:01:05	プロファイルがエンドポイントに割り当てられていない場合、そのエンドポイントは不明プロファイルに割り当てられ、一致するプロファイルに再プロファイリングされます。	Xerox-Device

インポートされない無効な属性を持つエンドポイント

CSV ファイルに存在するエンドポイントのいずれかに無効な属性がある場合、エンドポイントはインポートされず、エラー メッセージが表示されます。

たとえば、エンドポイントがインポートに使用されるファイル内で無効なプロファイルに割り当てられている場合、それらのエンドポイントは、Cisco ISE には一致するプロファイルがないためインポートされません。エンドポイントが CSV ファイル内の無効なプロファイルに割り当てられている場合、それらのエンドポイントがインポートされない仕組みを下に示します。

表 *101* : 無効なプロファイル：ファイルからのインポート

MAC アドレス（MAC Address）	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:02	不明。	Xerox-Device

MAC アドレス（MAC Address）	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:05	00:00:00:00:01:05 などのエンドポイントが Cisco ISE 使用可能なプロファイル以外の無効なプロファイルに割り当てられている場合、Cisco ISE では、ポリシー名が無効で、エンドポイントがインポートされないことを示す警告メッセージが表示されます。	エンドポイントは、Cisco ISE 内に一致するプロファイルがないためインポートされません。

LDAP サーバからのエンドポイントのインポート

エンドポイントの MAC アドレス、関連するプロファイル、およびエンドポイント ID グループを LDAP サーバからセキュアにインポートできます。

始める前に

エンドポイントをインポートする前に、LDAP サーバがインストールされていることを確認します。

LDAP サーバからインポートするには、接続設定値およびクエリー設定値を設定する必要があります。接続設定値またはクエリー設定値が Cisco ISE で間違って設定されていると、「LDAP インポートが失敗：（LDAP import failed:）」エラー メッセージが表示されます。

ステップ 1 **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** > **[LDAP からのインポート（Import From LDAP）]** の順に選択します。

ステップ 2 接続設定の値を入力します。

ステップ 3 クエリー設定の値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

カンマ区切り形式ファイルを使用したエンドポイントのエクスポート

選択したエンドポイントまたはすべてのエンドポイントを Cisco ISE サーバから CSV ファイルでエクスポートできます。このファイルで、エンドポイントは MAC アドレス、エンドポイント プロファイリング ポリシー、およびエンドポイント ID グループと、約 75 属性とともに一覧表示されます。Cisco ISE で作成されたカスタム属性は、CSV ファイルにエクスポートすることもでき、「CUSTOM.」というプレフィクスが付けられて、他のエンドポイント属性と区別できます。

（注） 1 つの導入からエクスポートされたエンドポイントのカスタム属性を別の導入にインポートするには、**[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[設定（Settings）]** > **[エンドポイント カスタム属性（Endpoint Custom Attributes）]** ページで同じカスタム属性を作成し、最初の導入で指定したのと同じデータ タイプを使用する必要があります。

[すべてエクスポート（Export All）] では Cisco ISE のすべてのエンドポイントがエクスポートされ、[選択済みをエクスポート（Export Selected）] ではユーザが選択したエンドポイントのみがエクスポートされます。デフォルトでは、profiler_endpoints.csv が CSV ファイルであり、Microsoft Office Excel が CSV ファイルを開くデフォルトのアプリケーションです。

ステップ 1 **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** を選択します。

ステップ 2 [エクスポート（Export）] をクリックし、次のいずれかを選択します。

- [選択済みをエクスポート（Export Selected）] : [エンドポイント（Endpoints）] ページで選択したエンドポイントだけをエクスポートできます。
- [すべてエクスポート（Export All）] : デフォルトで、[エンドポイント（Endpoints）] ページのすべてのエンドポイントをエクスポートできます。

ステップ 3 [OK] をクリックして、profiler_endpoints.csv ファイルを保存します。

エクスポートされたスプレッドシート内の属性のほとんどはシンプルなものです。属性の説明は次のとおりです。

- *UpdateTime*：エンドポイント属性の変更により、プロファイラがエンドポイントを最後に更新した時間。エンドポイントセッションの開始以降、更新がない場合、値は 0 です。更新中、一時的に空白になります。
- *InactivityTime*：エンドポイントがアクティブになってからの時間。

識別されたエンドポイント

Cisco ISE では、ネットワークに接続してネットワーク リソースを使用する識別されたエンドポイントが、[エンドポイント（Endpoints）] ページに表示されます。エンドポイントは、通常、有線および無線のネットワーク アクセス デバイスと VPN を介してネットワークに接続するネットワーク対応デバイスです。エンドポイントとして、パーソナル コンピュータ、ラップトップ、IP Phone、スマートフォン、ゲーム コンソール、プリンタ、ファクス機などがあります。

16 進数形式で表したエンドポイントの MAC アドレスは、常にエンドポイントの一意の表現ですが、それらに関連付けられた属性と値のさまざまなセット（属性と値のペアと呼ばれる）でエンドポイントを識別することもできます。エンドポイントの属性のさまざまなセットは、エ

ンドポイント機能、ネットワーク アクセス デバイスの機能と設定、およびこれらの属性の収集に使用する方法（プローブ）に基づいて収集できます。

動的にプロファイリングされるエンドポイント

エンドポイントは、ネットワークで検出されると、設定されているプロファイリングエンドポイントのプロファイリングポリシーに基づいて動的にプロファイリングされ、プロファイルに応じて一致するエンドポイント ID グループに割り当てられます。

静的にプロファイリングされるエンドポイント

MAC アドレスを使用してエンドポイントを作成し、Cisco ISE のエンドポイント ID グループとともにプロファイルをそのエンドポイントに割り当てると、エンドポイントを静的にプロファイリングすることができます。Cisco ISE では、静的に割り当てられたエンドポイントに対して、プロファイリング ポリシーおよび ID グループを再割り当てしません。

不明なエンドポイント

エンドポイントに対して一致するプロファイリングポリシーがない場合、不明なプロファイリングポリシー（「不明」）を割り当てることで、エンドポイントを不明としてプロファイリングできます。不明なエンドポイント ポリシーにプロファイリングされたエンドポイントの場合、そのエンドポイントに対して収集された属性または属性セットを使用してプロファイルを作成する必要があります。いずれのプロファイルにも一致しないエンドポイントは、不明なエンドポイント ID グループにグループ化されます。

識別されたエンドポイントの、ポリシー サービス ノード データベースへのローカル保存

Cisco ISE は識別されたエンドポイントをポリシー サービス ノードのデータベースにローカルに書き込みます。エンドポイントをデータベースにローカル保存した後は、それらのエンドポイントは、重要な属性がエンドポイントで変更され、他のポリシーサービス ノードデータベースに複製されているときにのみ、管理ノードデータベースで使用できる（リモート書き込み）ようになります。

重要な属性は次のとおりです。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser

- DeviceRegistrationStatus
- BYODRegistration

Cisco ISE でエンドポイント プロファイル定義を変更した場合、すべてのエンドポイントを再プロファイリングする必要があります。エンドポイント属性を収集するポリシー サービス ノードが、これらのエンドポイントの再プロファイリングを担当します。

あるポリシー サービス ノードが、最初は別のポリシー サービス ノードによって属性が収集されていたエンドポイントに関する属性を収集し始めると、エンドポイントの所有権が現在のポリシー サービス ノードに移ります。新しいポリシー サービス ノードは、前のポリシー サービス ノードから最新の属性を取得して、すでに収集されている属性と調整します。

重要な属性がエンドポイントで変更されると、エンドポイントの属性は管理ノード データベースに自動的に保存され、エンドポイントの最新の重要な変更を使用できます。エンドポイントを所有するポリシー サービス ノードが何らかの理由で使用できない場合、管理 ISE ノードが所有者を失ったエンドポイントを再プロファイリングします。また、このようなエンドポイントに対して新しいポリシー サービス ノードを設定する必要があります。

クラスタのポリシー サービス ノード

Cisco ISE では、ポリシー サービス ノード グループをクラスタとして使用するため、クラスタ内の複数のノードが同じエンドポイントの属性を収集するときに、エンドポイント属性を交換できます。1 つのロード バランサの背後に存在する、すべてのポリシー サービス ノードに対するクラスタを作成することを推奨します。

現在のオーナー以外の別のノードが同じエンドポイントの属性を受信した場合、属性をマージし、所有権の変更が必要かどうかを決定するために、現在のオーナーから最新の属性を要求するメッセージをクラスタ全体に送信します。Cisco ISE でノード グループを定義していない場合は、すべてのノードが 1 つのクラスタ内にあると想定されます。

Cisco ISE でエンドポイントの作成と複製への変更は行われません。エンドポイントの所有権の変更のみが、プロファイリングに使用される、静的属性と動的属性から作成される属性のリスト（ホワイト リスト）に基づいて決定されます。

次のいずれかの属性が変更された場合、後続の属性の収集時に、エンドポイントは管理ノードで更新されます。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser

- DeviceRegistrationStatus
- BYODRegistration

エンドポイントが管理ノードで編集および保存されている場合、この属性はエンドポイントの現在のオーナーから取得されます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイント ID グループ（Endpoint Identity Groups）] ページで追加のエンドポイント ID グループを作成することもできます。作成したエンドポイント ID グループを編集または削除できます。システム定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集したり、これらのグループを削除したりすることはできません。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するエンドポイント ID グループの名前を入力します（エンドポイント ID グループの名前にスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの説明を入力します。

ステップ 5 [親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

識別されたエンドポイントの、エンドポイントIDグループでのグループ化

Cisco ISE では、エンドポイント プロファイリング ポリシーに基づいて、検出されたエンドポイントを対応するエンドポイント ID グループにグループ化します。プロファイリング ポリシーは階層構造になっており、Cisco ISE のエンドポイント ID グループ レベルで適用されます。エンドポイントをエンドポイント ID グループにグループ化し、プロファイリング ポリシーをエンドポイント ID グループに適用すると、Cisco ISE により、対応するエンドポイント プロファイリング ポリシーを確認してエンドポイント プロファイルへのエンドポイントのマッピングを決定できます。

Cisco ISE によってエンドポイント ID グループのセットがデフォルトで作成され、これを使用して、エンドポイントを動的または静的に割り当てできる独自の ID グループを作成できます。エンドポイント ID グループを作成し、システムが作成した ID グループの 1 つにその ID グルー

プを関連付けることができます。また、自分が作成したエンドポイントをシステム内のいずれかの ID グループに静的に割り当てることができ、ID グループがプロファイリング サービスで再割り当てされることはありません。

エンドポイントに対して作成されるデフォルトのエンドポイントIDグループ

Cisco ISE は次の 5 つのエンドポイント ID グループをデフォルトで作成します。ブラックリスト、GuestEndpoints、プロファイル済み、RegisteredDevices、不明。さらに、プロファイル済み（親）ID グループに関連付けられている Cisco-IP-Phone やワークステーションなどの追加の 2 つの ID グループを作成します。親グループは、システムに存在するデフォルトの ID グループです。

Cisco ISE は次のエンドポイント ID グループを作成します。

- ブラックリスト：このエンドポイント ID グループには、Cisco ISE でこのグループに静的に割り当てられたエンドポイントおよびデバイス登録ポータルでブラックリストに記載されたエンドポイントが含まれます。許可プロファイルを Cisco ISE で定義して、このグループのエンドポイントへのネットワーク アクセスを許可または拒否できます。
- GuestEndpoints：このエンドポイント ID グループには、ゲスト ユーザが使用するエンドポイントが含まれます。
- プロファイル済み：このエンドポイント ID グループには、Cisco ISE の Cisco IP Phone およびワークステーションを除くエンドポイント プロファイリング ポリシーに一致するエンドポイントが含まれます。
- 登録済みデバイス：このエンドポイント ID グループには、デバイス登録ポータルを介して従業員が追加した登録済みデバイスであるエンドポイントが含まれます。プロファイリング サービスは通常、これらのデバイスがこのグループに割り当てられている場合、これらのデバイスを引き続きプロファイリングします。エンドポイントは Cisco ISE のこのグループに静的に割り当てられ、プロファイリング サービスがこれらのエンドポイントを他の ID グループに割り当てることはできません。これらのデバイスは、エンドポイント リストの他のエンドポイントと同様に表示されます。デバイス登録ポータルを介して追加されたこれらのデバイスに対して、Cisco ISE の [エンドポイント（Endpoints）] ページのエンドポイント リストで編集、削除およびブラックリストへの記載を実行できます。デバイス登録ポータルでブラックリストに記載されたデバイスは、ブラックリスト エンドポイント ID グループに割り当てられ、Cisco ISE に存在する許可プロファイルは、ブラックリストに記載されたデバイスを URL（「無許可ネットワーク アクセス」と表示される、ブラックリストに記載されたデバイスのデフォルト ポータル ページ）にリダイレクトします。
- 不明：このエンドポイント ID グループには、Cisco ISE のプロファイルに一致しないエンドポイントが含まれます。

上記のシステムで作成されたエンドポイント ID グループに加えて、Cisco ISE ではプロファイル済み ID グループに関連付けられる次のエンドポイント ID グループが作成されます。

- Cisco-IP-Phone：ネットワーク上のすべてのプロファイル済みCisco IP Phoneが含まれるIDグループです。
- ワークステーション：ネットワーク上のすべてのプロファイル済みワークステーションが含まれる ID グループです。

一致するエンドポイント プロファイリング ポリシーに対して作成されるエンドポイント ID グループ

既存のポリシーと一致するエンドポイント ポリシーがある場合、プロファイリング サービスは一致するエンドポイントID グループを作成できます。このID グループは、プロファイル済みエンドポイントID グループの子になります。エンドポイントポリシーを作成する場合、[プロファリング ポリシー（Profiling Policies）] ページの [一致する ID グループの作成（Create Matching Identity Group）] チェックボックスをオンにして、一致するエンドポイントID グループを作成できます。プロファイルのマッピングが削除されない限り、一致する ID グループは削除できません。

エンドポイント ID グループでの静的なエンドポイントの追加

エンドポイント ID グループの静的に追加されたエンドポイントを追加または削除できます。

[エンドポイント（Endpoints）] ウィジェットのエンドポイントのみを特定の ID グループに追加できます。エンドポイントを特定のエンドポイント ID グループに追加した場合、そのエンドポイントは、前に動的にグループ化されたエンドポイント ID グループから移動されます。

エンドポイントを最近追加したエンドポイント ID グループから削除すると、そのエンドポイントは、適切な ID グループに再プロファイリングされます。エンドポイントは、システムから削除されませんが、エンドポイントの ID グループからのみ削除されます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 エンドポイント ID グループを選択して [編集（Edit）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [エンドポイント（Endpoints）] ウィジェットでエンドポイントを選択して、選択したエンドポイントをエンドポイント ID グループに追加します。

ステップ 5 [エンドポイント グループ リスト（Endpoint Group List）] リンクをクリックして、[エンドポイント ID グループ（Endpoint Identity Groups）] ページに戻ります。

ダイナミックエンドポイントの、IDグループへの追加または削除後の再プロファイリング

エンドポイント ID グループが静的に割り当てられていない場合、エンドポイント ID グループに追加した、またはエンドポイント ID グループから削除したエンドポイントは、再プロファイリングされます。ISE プロファイラにより動的に識別されたエンドポイントは、適切なエンドポイント ID グループに表示されます。動的に追加されたエンドポイントをエンドポイント ID グループから削除した場合、Cisco ISE では、エンドポイント ID グループからエンドポイントを正常に削除したが、それらのエンドポイントをエンドポイント ID グループに再プロファイリングして戻すことを示すメッセージが表示されます。

許可ルールで使用されるエンドポイント ID グループ

エンドポイント ID グループを許可ポリシーで効率的に使用して、検出されたエンドポイントに適切なネットワーク アクセス権限を付与することができます。たとえば、すべてのタイプの Cisco IP Phone 用の許可ルールが、デフォルトで、Cisco ISE の **[ポリシー セット（Policy Sets）]** > **[デフォルト（Default）]** > **[許可ポリシー（Authorization Policy）]** で使用できます。

エンドポイント プロファイリング ポリシーがスタンドアロン ポリシー（他のエンドポイント プロファイリング ポリシーの親でない）であるか、またはエンドポイント プロファイリング ポリシーの親ポリシーが無効でないことを確認する必要があります。

プロファイラ フィード サービス

プロファイラ条件、例外アクション、および NMAP スキャン アクションは、シスコ提供または管理者作成として分類され、システム タイプ属性に表示されます。エンドポイント プロファイリング ポリシーは、シスコ提供、管理者作成、または管理者による変更として分類されます。これらの分類は、システム タイプ属性に表示されます。

システム タイプ属性によって、プロファイラ条件、例外アクション、NMAP スキャン アクション、およびエンドポイント プロファイリング ポリシーに対して異なる操作を実行できます。シスコ提供の条件、例外アクション、NMAP スキャン アクションは編集または削除できません。シスコが提供するエンドポイント ポリシーは削除できません。ポリシーを編集すると、管理者による変更と見なされます。フィード サービスによってポリシーが更新されると、管理者によって変更されたポリシーは、それが基づいていたシスコ提供ポリシーの最新のバージョンに置き換えられます。

新規および更新されたエンドポイント プロファイリング ポリシーと更新された OUI データベースは、Cisco フィード サーバから取得できます。Cisco ISE へのサブスクリプションが必要です。また、適用、成功、および失敗のメッセージに関する電子メール通知を受信することもできます。シスコによるフィード サービスの改善のため、フィード サービス アクションに関する匿名の情報をシスコに返信することができます。

OUI データベースには、ベンダーに割り当てられた MAC OUI が含まれています。OUI リストは、次の URL から入手できます。 http://standards.ieee.org/develop/regauth/oui/oui.txt

Cisco ISE は毎日ローカル Cisco ISE サーバのタイム ゾーンの午前 1:00 にポリシーと OUI データベースの更新をダウンロードします。Cisco ISE は、これらのダウンロードされたフィード サーバ ポリシーを自動的に適用し、また、以前の状態に復元できるように変更内容を保存します。以前の状態に復元すると、新しいエンドポイント プロファイリング ポリシーは削除され、更新されたエンドポイント プロファイリング ポリシーは以前の状態に復元されます。さらに、プロファイラ フィード サービスは自動的に無効になります。

また、オフライン モードで手動でフィード サービスを更新することもできます。ISE 展開をシスコ フィード サービスに接続できない場合には、このオプションを使用して更新プログラムを手動でダウンロードすることができます。

（注） 60 日間のうち、ライセンスがコンプライアンス外（OOC）となっている日数が 45 日間に達すると、フィード サービスからの更新が許可されなくなります。ライセンスがコンプライアンス外になるのは、ライセンスの有効期限が切れるか、または使用が許可されているセッション数を超えた時点です。

プロファイラ フィード サービスの設定

プロファイラ フィード サービスは、Cisco フィード サーバから新規および更新されたエンドポイント プロファイリング ポリシーと MAC OUI データベース更新を取得します。フィード サービスが使用できない場合、またはその他のエラーが発生した場合は、操作監査レポートで報告されます。

匿名のフィード サービス使用レポートをシスコに返信するように Cisco ISE を設定できます。そのレポートでは、次の情報がシスコに送信されます。

- Hostname：Cisco ISE ホスト名
- MaxCount：エンドポイントの合計数
- ProfiledCount：プロファイリングされたエンドポイント カウント
- UnknownCount：不明なエンドポイント カウント
- MatchSystemProfilesCount：シスコ提供のプロファイル カウント
- UserCreatedProfiles：ユーザ作成のプロファイル カウント

シスコから提供されるプロファイリング ポリシーの CoA タイプを変更できます。フィード サービスがそのポリシーを更新すると、CoA タイプは変更されませんが、そのポリシーの残りの属性は引き続き更新されます。

始める前に

分散展開またはスタンドアロン ISE ノードでは、Cisco ISE 管理者ポータルからのみプロファイラ フィード サービスを設定できます。

フィード更新について管理者ポータルから電子メール通知を送信する場合は、Simple Mail Transfer Protocol（SMTP）サーバを設定します（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]**）。

フィード サービスをオンラインで更新するには、次の手順に従います。

ステップ 1 **[管理（Administration）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** の順に選択し、Verisign Class 3 Public Primary Certification Authority および Verisign Class 3 Server CA - G3 が有効であることを確認します。

ステップ 2 **[ワーク センター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[フィード（Feeds）]** の順に選択します。
[管理（Administration）] > **[フィードサービス（FeedService）]** > **[プロファイラ（Profiler）]** ページでこのオプションにアクセスすることもできます。

ステップ 3 [オンライン サブスクリプションの更新（Online Subscription Update）] タブをクリックします。

ステップ 4 [フィードサービス接続のテスト（Test Feed Service Connection）] ボタンをクリックして、Cisco フィード サービスへの接続があり、証明書が有効であることを確認します。

ステップ 5 [オンライン サブスクリプション更新の有効化（Enable Online Subscription Update）] チェック ボックスをオンにします。

ステップ 6 HH:MM 形式で時刻（Cisco ISE サーバのローカル タイム ゾーン）を入力します。デフォルトでは、Cisco ISE フィード サービスは毎日午前 1 時にスケジュールされます。

ステップ 7 [ダウンロードが行われたら管理者に通知（Notify administrator when download occurs）] チェック ボックスをオンにして、[管理者の電子メール アドレス（Administrator email address）] テキスト ボックスに電子メール アドレスを入力します。Cisco ISE が非機密情報（今後のリリースでよりよいサービスと追加機能を提供するために使用される）を収集することを許可する場合、[プロファイリング精度を上げるために Cisco 匿名情報を提供する（Provide Cisco anonymous information to help improve profiling accuracy）] チェック ボックスをオンにします。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 [今すぐ更新（Update Now）] をクリックします。

最後のフィード サービス更新以降に作成された新規および更新されたプロファイルをチェックするために Cisco フィード サーバに連絡するように Cisco ISE に指示します。これによりシステム内のすべてのエンドポイントが再プロファイリングされ、システム負荷が増加する可能性があります。エンドポイント プロファイリング ポリシーの更新のため、現在 Cisco ISE に接続している一部のエンドポイントの許可ポリシーが変更される場合があります。

最後のフィード サービス以降に作成された新規および更新されたプロファイルを更新すると [今すぐ更新（Update Now）] ボタンは無効になり、ダウンロードの完了後にのみ有効になります。[プロファイラ フィード サービス設定（Profiler Feed Service Configuration）] ページから別の場所に移動し、このページに戻ります。

関連トピック

オフラインでのプロファイラ フィード サービスの設定 （831 ページ）

オフラインでのプロファイラ フィード サービスの設定

Cisco ISE と Cisco フィード サーバが直接接続されていないときに、フィード サービスをオフラインで更新できます。Cisco フィードサーバからオフライン更新プログラム パッケージをダウンロードし、Cisco ISE にオフライン フィード更新プログラムを使用してアップロードできます。またフィードサーバに追加される新しいポリシーに関する電子メール通知を設定することもできます。

オフラインでのプロファイラ フィード サービス設定には、次のタスクが含まれます。

1. オフライン更新プログラム パッケージのダウンロード
2. オフライン フィード更新の適用

オフライン更新プログラム パッケージのダウンロード

オフライン更新プログラム パッケージをダウンロードするには、以下のステップに従います。

ステップ 1 **[ワーク センター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[フィード（Feeds）]** の順に選択します。
[管理（Administration）] > **[フィードサービス（FeedService）]** > **[プロファイラ（Profiler）]** ページでこのオプションにアクセスすることもできます。

ステップ 2 [オフライン手動更新（Offline Manual Update）] タブをクリックします。

ステップ 3 [更新されているプロファイル ポリシーのダウンロード（Download Updated Profile Policies）] リンクをクリックします。フィード サービス パートナー ポータルにリダイレクトされます。
また、ブラウザから https://ise.cisco.com/partner/ にアクセスして、フィード サービス パートナー ポータルに直接アクセスすることもできます。

ステップ 4 初めてのユーザは、各種条件および契約に同意します。
要求を承認するフィードサービス管理者に電子メールが送信されます。承認されると、確認用の電子メールが届きます

ステップ 5 Cisco.com のクレデンシャルを使用してパートナー ポータルにログインします。

ステップ 6 [オフライン フィード（Offline Feed）] > [パッケージのダウンロード（Download Package）] の順に選択します。

ステップ 7 [パッケージの生成（Generate Package）] をクリックします。

ステップ 8 [オフライン 更新プログラム パッケージの内容を表示するにはクリックしてください（Click to View the Offline Update Package contents）] リンクをクリックして、生成したパッケージに含まれるすべてのプロファイルと OUI を表示します。

- [フィード プロファイラ 1（Feed Profiler 1）] と [フィード OUI（Feed OUI）] の下のポリシーは Cisco ISE の全バージョンにダウンロードされます。
- [フィード プロファイラ 2（Feed Profiler 2）] の下のポリシーは Cisco ISE リリース 1.3 以降のみにダウンロードされます。
- [フィード プロファイラ 3（Feed Profiler 2）] の下のポリシーは Cisco ISE リリース 2.1 以降のみにダウンロードされます。

ステップ 9 [パッケージのダウンロード（Download Package）] をクリックして、ローカル システムにファイルを保存します。
保存したファイルを Cisco ISE サーバにアップロードして、ダウンロードしたパッケージのフィード更新プログラムを適用できます。

オフライン フィード更新の適用

ダウンロードしたオフライン フィード更新を適用するには：

始める前に

フィード更新を適用する前に、オフライン更新プログラム パッケージをダウンロードしている必要があります。

ステップ 1 **[ワーク センター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[フィード（Feeds）]** の順に選択します。
[管理（Administration）] > **[フィードサービス（FeedService）]** > **[プロファイラ（Profiler）]** ページでこのオプションにアクセスすることもできます。
ステップ 2 [オフライン手動更新（Offline Manual Update）] タブをクリックします。
ステップ 3 [参照（Browse）] をクリックして、ダウンロードしたプロファイラ フィード パッケージを選択します。
ステップ 4 [更新の適用（Apply Update）] をクリックします。

プロファイルと OUI の更新に関する電子メール通知の設定

プロファイルと OUI の更新通知を受信する電子メール アドレスを設定できます。

電子メール通知を設定するには、次の手順に従います。

ステップ 1 オフライン更新プログラム パッケージのダウンロードセクションの手順 1 ～ 5 を実行し、フィード サービス パートナー ポータルに移動します。
ステップ 2 [オフライン フィード（Offline Feed）] > [電子メール設定（Email Preferences）] を選択します。
ステップ 3 通知を受信するには、[通知の有効化（Enable Notifications）] チェック ボックスをオンにします。
ステップ 4 新しい更新通知を受信する頻度を設定するには、[日数（days）] ドロップダウン リストから日数を選択します。
ステップ 5 電子メール アドレスまたはアドレスを入力し、[保存（Save）] をクリックします。

フィード更新の取り消し

前回の更新で更新されたエンドポイント プロファイリング ポリシーに戻り、プロファイラ フィード サービスの前回の更新により新しく追加されたが、エンドポイント プロファイリング ポリシーおよび OUI を削除できます。

エンドポイント プロファイリング ポリシーは、フィード サーバからの更新後に変更された場合、システムで変更されません。

ステップ 1 **[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[フィード（Feeds）]** の順に選択します。

ステップ 2 変更設定監査レポートで設定変更を表示する場合は、[更新レポート ページに移動（Go to Update Report Page）] をクリックします。

ステップ 3 [最新を元に戻す（Undo Latest）] をクリックします。

プロファイラ レポート

Cisco ISE には、エンドポイントプロファイリングに関するさまざまなレポートと、ネットワークの管理に使用できるトラブルシューティング ツールが用意されています。現在のデータに加えて履歴のレポートを生成できます。レポートの一部をドリルダウンして詳細を表示できます。大規模なレポートの場合、レポートをスケジュールし、さまざまな形式でダウンロードすることもできます。

[操作（Operations）]>[レポート（Reports）]>[エンドポイントとユーザ（Endpoints and Users）] からエンドポイントに関する次のレポートを実行できます。

- エンドポイント セッション履歴
- プロファイリングされたエンドポイントの概要
- エンドポイント プロファイルの変更
- エンドポイントによる上位承認
- 登録済みエンドポイント

エンドポイントの異常な動作の検出

Cisco ISE により、不正な MAC アドレスの使用からネットワークが保護されます。ISE は MAC アドレス スプーフィングに関与しているエンドポイントを検出し、疑わしいエンドポイントの権限を制限できます。

プロファイラ設定ページには、異常な動作に関する次の 2 つのオプションがあります。

- 異常な動作の検出を有効にする（Enable Anomalous Behavior Detection）
- 異常な動作の適用を有効にする（Enable Anomalous Behavior Enforcement）

異常な動作の検出を有効にすると、Cisco ISE はデータを調査し、NAS ポート タイプ、DHCP クラス ID、およびエンドポイント ポリシーに関連する属性の変更について、既存のデータとの矛盾がないかどうかを確認します。該当する場合、**AnomalousBehavior** 属性が True に設定され、エンドポイントに追加されます。これは、[可視性のコンテキスト（Visibility Context）] ページでエンドポイントをフィルタリングおよび表示する際に役立ちます。該当する MAC アドレスの監査ログも生成されます。

異常な動作の検出を有効にすると、Cisco ISE は、既存のエンドポイントの次の属性が変更されたかどうかを検査します。

1. ポートタイプ—エンドポイントのアクセス方式が変更されたかどうかを判断します。これは、有線 Dot1x 経由で接続したものと同じ MAC アドレスがワイヤレス Dot1x にも使用されていた場合（およびその逆の場合）に適用されます。
2. DHCP クラス ID—エンドポイントのクライアントまたはベンダーのタイプが変更されたかどうかを判断します。これは、DHCP クラス ID 属性に特定の値が入力された後で別の値に変更された場合にのみ当てはまります。エンドポイントが静的 IP アドレスで構成されている場合、Cisco ISE での DHCP クラス ID 属性は空です。後で別のデバイスがこのエンドポイントの MAC アドレスをスプーフィングして DHCP を使用すると、クラス ID が空の値から特定の文字列に変更されます。これによって異常な動作の検出がトリガーされることはありません。
3. エンドポイント ポリシー—重要なプロファイル変更があったかどうかを判断します。これは、エンドポイントのプロファイルが [電話（Phone）] または [プリンタ（Printer）] から [ワークステーション（Workstation）] に変更されたときに適用されます。

異常な動作の適用を有効にすると、異常な動作が検出された時点で CoA が発行されます。これは、[プロファイラ設定（Profiler Configuration）] ページで設定した許可ルールに基づいて、疑わしいエンドポイントを再許可するときに使用できます。

異常な動作に関する許可ポリシー ルールをエンドポイントに設定するには、「」を参照してください。

異常な動作が発生しているエンドポイントに関する許可ポリシー ルールの設定

異常な動作が発生しているエンドポイントに対して実行するアクションを選択するには、[許可ポリシー（Authorization Policy）] ページで対応するルールを設定します。

ステップ 1 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択します。

ステップ 2 デフォルト ポリシーに対応する [表示（View）] 列から矢印アイコン をクリックすると、[設定（Set）] ビュー画面が開き、デフォルト許可ポリシーを表示および管理できます。

ステップ 3 いずれかの行の [アクション（Actions）] 列から、歯車アイコンをクリックし、ドロップダウン リストから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して新しい認証ルールを挿入します。
[ポリシー セット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 4 [ルール名（Rule Name）] に入力します。

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性を選択します（たとえば、Endpoints.AnomalousBehaviorEqualsTrue）。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップすることもできます。

ステップ 7 [使用（Use）] をクリックして、異常な動作を伴うエンドポイントの許可ポリシー ルールを設定します。

ステップ 8 [完了（Done）] をクリックします。

異常な動作が発生しているエンドポイントの表示

次のいずれかのオプションを使用して、異常な動作が発生しているエンドポイントを表示できます。

- [ホーム（Home）] > [概要（Summary）] > [メトリック（Metrics）] から [異常な動作（Anomalous Behavior）] をクリックします。この操作により、ページ下部のペインに [異常な動作（Anomalous Behavior）] 列がある新しいタブが表示されます。
- [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [エンドポイントの分類（Endpoint Classification）] を選択します。ページ下部のペインで [異常な動作（Anomalous Behavior）] 列を確認できます。
- 次の手順で説明するように、[コンテキストの可視性（Context Visibility）] ページの [認証（Authentication）] ビューまたは [侵害されたエンドポイント（Compromised Endpoints）] ビューで新しい [異常な動作（Anomalous Behavior）] 列を作成できます。

ステップ 1 [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [認証（Authentication）] または [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [侵害されたエンドポイント（Compromised Endpoints）] を選択します。

ステップ 2 ページ下部のペインにある [設定（Settings）] アイコンをクリックし、[異常な動作（Anomalous Behavior）] チェックボックスをオンにします。

ステップ 3 [移動（Go）] をクリックします。
[認証（Authentication）] ビューまたは [侵害されたエンドポイント（Compromised Endpoints）] ビューで [異常な動作（Anomalous Behavior）] 列を表示できます。

ポリシーおよびIDグループのスタティック割り当てによるエンドポイントの作成

[エンドポイント（Endpoints）] ページでエンドポイントの MAC アドレスを使用して、新しいエンドポイントを静的に作成できます。また、スタティック割り当ての [エンドポイント（Endpoints）] ページで、エンドポイント プロファイリング ポリシーおよび ID グループを選択できます。

通常のモバイルデバイス（MDM）エンドポイントは、[エンドポイント ID（Endpoints Identities）] リストに表示されます。リストページには、[ホスト名（Hostname）]、[デバイスタイプ（Device Type）]、[デバイス ID（Device ID）] など、MDM エンドポイントの属性のカラムが表示されます。[スタティック割り当て（Static Assignment）]、[スタティック グループ割り当て（Static Group Assignment）] などのその他のカラムは、デフォルトでは表示されません。

（注） このページを使用して、MDM エンドポイントを追加、編集、削除、インポートまたはエクスポートすることはできません。

ステップ 1 **[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 エンドポイントの MAC アドレスをコロンで区切られた 16 進表記で入力します。

ステップ 4 [ポリシー割り当て（Policy Assignment）] ドロップダウン リストから一致するエンドポイント ポリシーを選択して、スタティック割り当てステータスをダイナミックからスタティックに変更します。

ステップ 5 [スタティック割り当て（Static Assignment）] チェックボックスをオンにして、エンドポイントに割り当てられたスタティック割り当てのステータスをダイナミックからスタティックに変更します。

ステップ 6 [ID グループ割り当て（Identity Group Assignment）] ドロップダウン リストから、新しく作成されたエンドポイントを割り当てるエンドポイント ID グループを選択します。

ステップ 7 エンドポイント ID グループのダイナミック割り当てをスタティックに変更するには、[スタティック グループ割り当て（Static Group Assignment）] チェックボックスをオンにします。

ステップ 8 [送信（Submit）] をクリックします。

CSV ファイルからのエンドポイントのインポート

Cisco ISE テンプレートから作成した CSV ファイルからエンドポイントをインポートし、エンドポイントの詳細を使用して更新することができます。ISE からエクスポートされたエンドポイントには約 75 個の属性が含まれているため、別の ISE 展開に直接インポートすることはできません。インポートが許可されていない列が CSV ファイルにある場合は、列のリストを含

むメッセージが表示されます。ファイルを再度インポートする前に、指定された列を削除する必要があります。

（注） エンドポイントのカスタム属性をインポートするには、正しいデータ タイプを使用して **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント カスタム属性（Endpoint Custom Attributes）]** ページで CSV ファイルと同じカスタム属性を作成する必要があります。これらのコマンドには、「CUSTOM.」というプレフィックスを付けてエンドポイント属性と区別する必要があります。

インポートできる属性は約 30 あります。このリストには、MACAddress、EndPointPolicy、IdentityGroup が含まれています。オプション属性は次のとおりです。

説明	PortalUser	LastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	デバイスタイプ（Device Type）	host-name
PortalUser.GuestStatus	StaticAssignment	参照先
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<custom attribute name>	—	—

ファイル ヘッダーは、デフォルトのインポート テンプレートで指定されている形式にして、エンドポイントのリストが次の順序で表示されるようにする必要があります。MACAddress、EndpointPolicy、IdentityGroup、<オプション属性として上に記載されている属性のリスト>。次のファイル テンプレートを作成できます。

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <オプション属性として上に記載されている属性のリスト>

MAC アドレスを除くすべての属性値は、CSV ファイルからエンドポイントをインポートする際に省略可能です。特定の値のないエンドポイントをインポートする場合も、値はカンマで区切られます。

次の例を参考にしてください。

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser, など

ステップ 1 **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** の順に選択します。

ステップ 2 [ファイルからインポート（Import from File）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、作成済みの CSV ファイルを見つけます。

ステップ 4 [送信（Submit）] をクリックします。

エンドポイントで使用可能なデフォルトのインポート テンプレート

エンドポイントのインポートに使用できるエンドポイントを更新できるテンプレートを生成できます。デフォルトで、[テンプレートの生成（Generate a Template）] リンクを使用して、Microsoft Office Excel アプリケーションで CSV ファイルを作成し、このファイルをシステム上にローカルに保存できます。ファイルは **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** > **[ファイルからインポート（Import from File）]** にあります。[テンプレートの生成（Generate a Template）] リンクを使用してテンプレートを作成でき、Cisco ISE サーバは、[template.csv を開く（Opening template.csv）] ダイアログを表示します。このダイアログを使用すると、デフォルトの template.csv ファイルを開いたり、template.csv ファイルをシステム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルは Microsoft Office Excel アプリケーションで開かれます。デフォルトの template.csv ファイルには、MAC アドレス、エンドポイント ポリシー、エンドポイント ID グループ、およびその他のオプション属性が表示されるヘッダー行が含まれています。

エンドポイントの MAC アドレス、エンドポイント プロファイリング ポリシー、エンドポイント ID グループを、インポートするオプションの属性値とともに更新し、新しいファイル名を使用してファイルを保存します。このファイルをエンドポイントのインポートのために使用できます。[テンプレートの生成（Generate a Template）] リンクを使用したときに作成される template.csv ファイルのヘッダー行を参照してください。

表 *102 : CSV* テンプレート ファイル

MAC	EndPointPolicy	IdentityGroup	その他のオプションの属性
11:11:11:11:11:11	Android	プロファイル済み	<Empty>/<Value>

インポート中の不明なエンドポイントの再プロファイリング

インポートに使用するファイルに、MAC アドレスを持つエンドポイントがあり、それらに割り当てられているエンドポイントプロファイリング ポリシーが不明プロファイルである場合、これらのエンドポイントはインポート中に Cisco ISE でただちに一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。ただし、不明プロファイルに静的に割り当てられることはありません。エンドポイントに割り当てられているエンドポイント プロファイリング ポリシーが CSV ファイルにない場合、これらのエンドポイントは不明プロファイルに割り当てられ、一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。次に、Cisco ISE が、インポート中に Xerox_Device プロファイルに一致する不明プロファイルをどのように再プロファイリングするか、および割り当てられていないエンドポイントをどのように再プロファイリングするかを示します。

表 *103 :* 不明プロファイル：ファイルからのインポート

MAC アドレス（MAC Address）	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:02	不明。	Xerox-Device
00:00:00:00:01:03	不明。	Xerox-Device
00:00:00:00:01:04	不明。	Xerox-Device
00:00:00:00:01:05	プロファイルがエンドポイントに割り当てられていない場合、そのエンドポイントは不明プロファイルに割り当てられ、一致するプロファイルに再プロファイリングされます。	Xerox-Device

インポートされない無効な属性を持つエンドポイント

CSV ファイルに存在するエンドポイントのいずれかに無効な属性がある場合、エンドポイントはインポートされず、エラー メッセージが表示されます。

たとえば、エンドポイントがインポートに使用されるファイル内で無効なプロファイルに割り当てられている場合、それらのエンドポイントは、Cisco ISE には一致するプロファイルがないためインポートされません。エンドポイントが CSV ファイル内の無効なプロファイルに割

り当てられている場合、それらのエンドポイントがインポートされない仕組みを下に示します。

表 *104 :* 無効なプロファイル：ファイルからのインポート

MAC アドレス（MAC Address）	Cisco ISE でのインポート前に割り当てられたエンドポイント プロファイリング ポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイント プロファイリング ポリシー
00:00:00:00:01:02	不明。	Xerox-Device
00:00:00:00:01:05	00:00:00:00:01:05 などのエンドポイントが Cisco ISE 使用可能なプロファイル以外の無効なプロファイルに割り当てられている場合、Cisco ISE では、ポリシー名が無効で、エンドポイントがインポートされないことを示す警告メッセージが表示されます。	エンドポイントは、Cisco ISE 内に一致するプロファイルがないためインポートされません。

LDAP サーバからのエンドポイントのインポート

エンドポイントの MAC アドレス、関連するプロファイル、およびエンドポイント ID グループを LDAP サーバからセキュアにインポートできます。

始める前に

エンドポイントをインポートする前に、LDAP サーバがインストールされていることを確認します。

LDAP サーバからインポートするには、接続設定値およびクエリー設定値を設定する必要があります。接続設定値またはクエリー設定値が Cisco ISE で間違って設定されていると、「LDAP インポートが失敗：（LDAP import failed:）」エラー メッセージが表示されます。

ステップ 1 **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** > **[LDAP からのインポート（Import From LDAP）]** の順に選択します。

ステップ 2 接続設定の値を入力します。

ステップ 3 クエリー設定の値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

カンマ区切り形式ファイルを使用したエンドポイントのエクスポート

選択したエンドポイントまたはすべてのエンドポイントを Cisco ISE サーバから CSV ファイルでエクスポートできます。このファイルで、エンドポイントは MAC アドレス、エンドポイント プロファイリング ポリシー、およびエンドポイント ID グループと、約 75 属性とともに一覧表示されます。Cisco ISE で作成されたカスタム属性は、CSV ファイルにエクスポートすることもでき、「CUSTOM.」というプレフィクスが付けられて、他のエンドポイント属性と区別できます。

（注） 1 つの導入からエクスポートされたエンドポイントのカスタム属性を別の導入にインポートするには、**[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[設定（Settings）]** > **[エンドポイント カスタム属性（Endpoint Custom Attributes）]** ページで同じカスタム属性を作成し、最初の導入で指定したのと同じデータ タイプを使用する必要があります。

[すべてエクスポート（Export All）] では Cisco ISE のすべてのエンドポイントがエクスポートされ、[選択済みをエクスポート（Export Selected）] ではユーザが選択したエンドポイントのみがエクスポートされます。デフォルトでは、profiler_endpoints.csv が CSV ファイルであり、Microsoft Office Excel が CSV ファイルを開くデフォルトのアプリケーションです。

ステップ 1 **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** を選択します。

ステップ 2 [エクスポート（Export）] をクリックし、次のいずれかを選択します。

- [選択済みをエクスポート（Export Selected）] : [エンドポイント（Endpoints）] ページで選択したエンドポイントだけをエクスポートできます。
- [すべてエクスポート（Export All）] : デフォルトで、[エンドポイント（Endpoints）] ページのすべてのエンドポイントをエクスポートできます。

ステップ 3 [OK] をクリックして、profiler_endpoints.csv ファイルを保存します。

エクスポートされたスプレッドシート内の属性のほとんどはシンプルなものです。属性の説明は次のとおりです。

- *UpdateTime*：エンドポイント属性の変更により、プロファイラがエンドポイントを最後に更新した時間。エンドポイントセッションの開始以降、更新がない場合、値は 0 です。更新中、一時的に空白になります。
- *InactivityTime*：エンドポイントがアクティブになってからの時間。

識別されたエンドポイント

Cisco ISE では、ネットワークに接続してネットワーク リソースを使用する識別されたエンドポイントが、[エンドポイント（Endpoints）] ページに表示されます。エンドポイントは、通常、有線および無線のネットワーク アクセス デバイスと VPN を介してネットワークに接続するネットワーク対応デバイスです。エンドポイントとして、パーソナル コンピュータ、ラップトップ、IP Phone、スマートフォン、ゲーム コンソール、プリンタ、ファクス機などがあります。

16 進数形式で表したエンドポイントの MAC アドレスは、常にエンドポイントの一意の表現ですが、それらに関連付けられた属性と値のさまざまなセット（属性と値のペアと呼ばれる）でエンドポイントを識別することもできます。エンドポイントの属性のさまざまなセットは、エンドポイント機能、ネットワーク アクセス デバイスの機能と設定、およびこれらの属性の収集に使用する方法（プローブ）に基づいて収集できます。

動的にプロファイリングされるエンドポイント

エンドポイントは、ネットワークで検出されると、設定されているプロファイリング エンドポイントのプロファイリング ポリシーに基づいて動的にプロファイリングされ、プロファイルに応じて一致するエンドポイント ID グループに割り当てられます。

静的にプロファイリングされるエンドポイント

MAC アドレスを使用してエンドポイントを作成し、Cisco ISE のエンドポイント ID グループとともにプロファイルをそのエンドポイントに割り当てると、エンドポイントを静的にプロファイリングすることができます。Cisco ISE では、静的に割り当てられたエンドポイントに対して、プロファイリング ポリシーおよび ID グループを再割り当てしません。

不明なエンドポイント

エンドポイントに対して一致するプロファイリング ポリシーがない場合、不明なプロファイリング ポリシー（「不明」）を割り当てることで、エンドポイントを不明としてプロファイリングできます。不明なエンドポイント ポリシーにプロファイリングされたエンドポイントの場合、そのエンドポイントに対して収集された属性または属性セットを使用してプロファイルを作成する必要があります。いずれのプロファイルにも一致しないエンドポイントは、不明なエンドポイント ID グループにグループ化されます。

識別されたエンドポイントの、ポリシー サービス ノード データベースへのローカル保存

Cisco ISE は識別されたエンドポイントをポリシー サービス ノードのデータベースにローカルに書き込みます。エンドポイントをデータベースにローカル保存した後は、それらのエンドポイントは、重要な属性がエンドポイントで変更され、他のポリシーサービス ノードデータベースに複製されているときにのみ、管理ノードデータベースで使用できる（リモート書き込み）ようになります。

重要な属性は次のとおりです。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

Cisco ISE でエンドポイント プロファイル定義を変更した場合、すべてのエンドポイントを再プロファイリングする必要があります。エンドポイント属性を収集するポリシーサービス ノードが、これらのエンドポイントの再プロファイリングを担当します。

あるポリシー サービス ノードが、最初は別のポリシー サービス ノードによって属性が収集されていたエンドポイントに関する属性を収集し始めると、エンドポイントの所有権が現在のポリシー サービス ノードに移ります。新しいポリシー サービス ノードは、前のポリシー サービス ノードから最新の属性を取得して、すでに収集されている属性と調整します。

重要な属性がエンドポイントで変更されると、エンドポイントの属性は管理ノードデータベースに自動的に保存され、エンドポイントの最新の重要な変更を使用できます。エンドポイントを所有するポリシー サービス ノードが何らかの理由で使用できない場合、管理 ISE ノードが所有者を失ったエンドポイントを再プロファイリングします。また、このようなエンドポイントに対して新しいポリシー サービス ノードを設定する必要があります。

クラスタのポリシー サービス ノード

Cisco ISE では、ポリシー サービス ノード グループをクラスタとして使用するため、クラスタ内の複数のノードが同じエンドポイントの属性を収集するときに、エンドポイント属性を交換できます。1 つのロード バランサの背後に存在する、すべてのポリシー サービス ノードに対するクラスタを作成することを推奨します。

現在のオーナー以外の別のノードが同じエンドポイントの属性を受信した場合、属性をマージし、所有権の変更が必要かどうかを決定するために、現在のオーナーから最新の属性を要求するメッセージをクラスタ全体に送信します。Cisco ISE でノード グループを定義していない場合は、すべてのノードが 1 つのクラスタ内にあると想定されます。

Cisco ISE でエンドポイントの作成と複製への変更は行われません。エンドポイントの所有権の変更のみが、プロファイリングに使用される、静的属性と動的属性から作成される属性のリスト（ホワイト リスト）に基づいて決定されます。

次のいずれかの属性が変更された場合、後続の属性の収集時に、エンドポイントは管理ノードで更新されます。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

エンドポイントが管理ノードで編集および保存されている場合、この属性はエンドポイントの現在のオーナーから取得されます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイント ID グループ（Endpoint Identity Groups）] ページで追加のエンドポイント ID グループを作成することもできます。作成したエンドポイント ID グループを編集または削除できます。システム定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集したり、これらのグループを削除したりすることはできません。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するエンドポイント ID グループの名前を入力します（エンドポイント ID グループの名前にスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの説明を入力します。

ステップ 5 [親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

識別されたエンドポイントの、エンドポイント ID グループでのグループ化

Cisco ISE では、エンドポイント プロファイリング ポリシーに基づいて、検出されたエンドポイントを対応するエンドポイント ID グループにグループ化します。プロファイリング ポリシーは階層構造になっており、Cisco ISE のエンドポイント ID グループ レベルで適用されます。エンドポイントをエンドポイント ID グループにグループ化し、プロファイリング ポリシーをエンドポイント ID グループに適用すると、Cisco ISE により、対応するエンドポイント プロファイリング ポリシーを確認してエンドポイント プロファイルへのエンドポイントのマッピングを決定できます。

Cisco ISE によってエンドポイント ID グループのセットがデフォルトで作成され、これを使用して、エンドポイントを動的または静的に割り当てできる独自の ID グループを作成できます。エンドポイント ID グループを作成し、システムが作成した ID グループの 1 つにその ID グループを関連付けることができます。また、自分が作成したエンドポイントをシステム内のいずれかの ID グループに静的に割り当てることができ、ID グループがプロファイリング サービスで再割り当てされることはありません。

エンドポイントに対して作成されるデフォルトのエンドポイント ID グループ

Cisco ISE は次の 5 つのエンドポイント ID グループをデフォルトで作成します。ブラックリスト、GuestEndpoints、プロファイル済み、RegisteredDevices、不明。さらに、プロファイル済み（親）ID グループに関連付けられている Cisco-IP-Phone やワークステーションなどの追加の 2 つの ID グループを作成します。親グループは、システムに存在するデフォルトの ID グループです。

Cisco ISE は次のエンドポイント ID グループを作成します。

- ブラックリスト：このエンドポイント ID グループには、Cisco ISE でこのグループに静的に割り当てられたエンドポイントおよびデバイス登録ポータルでブラックリストに記載されたエンドポイントが含まれます。許可プロファイルを Cisco ISE で定義して、このグループのエンドポイントへのネットワーク アクセスを許可または拒否できます。
- GuestEndpoints：このエンドポイント ID グループには、ゲスト ユーザが使用するエンドポイントが含まれます。
- プロファイル済み：このエンドポイント ID グループには、Cisco ISE の Cisco IP Phone およびワークステーションを除くエンドポイント プロファイリング ポリシーに一致するエンドポイントが含まれます。
- 登録済みデバイス：このエンドポイント ID グループには、デバイス登録ポータルを介して従業員が追加した登録済みデバイスであるエンドポイントが含まれます。プロファイリング サービスは通常、これらのデバイスがこのグループに割り当てられている場合、これらのデバイスを引き続きプロファイリングします。エンドポイントは Cisco ISE のこのグループに静的に割り当てられ、プロファイリング サービスがこれらのエンドポイントを他の ID グループに割り当てることはできません。これらのデバイスは、エンドポイント リストの他のエンドポイントと同様に表示されます。デバイス登録ポータルを介して追加されたこれらのデバイスに対して、Cisco ISE の [エンドポイント（Endpoints）] ページのエンドポイント リストで編集、削除およびブラックリストへの記載を実行できます。デバイス登録ポータルでブラックリストに記載されたデバイスは、ブラックリスト エンドポイン

トID グループに割り当てられ、Cisco ISE に存在する許可プロファイルは、ブラックリストに記載されたデバイスをURL（「無許可ネットワーク アクセス」と表示される、ブラックリストに記載されたデバイスのデフォルト ポータル ページ）にリダイレクトします。

- 不明：このエンドポイント ID グループには、Cisco ISE のプロファイルに一致しないエンドポイントが含まれます。

上記のシステムで作成されたエンドポイント ID グループに加えて、Cisco ISE ではプロファイル済み ID グループに関連付けられる次のエンドポイント ID グループが作成されます。

- Cisco-IP-Phone：ネットワーク上のすべてのプロファイル済みCisco IP Phoneが含まれるID グループです。
- ワークステーション：ネットワーク上のすべてのプロファイル済みワークステーションが含まれる ID グループです。

一致するエンドポイント プロファイリング ポリシーに対して作成されるエンドポイント ID グループ

既存のポリシーと一致するエンドポイント ポリシーがある場合、プロファイリング サービスは一致するエンドポイントID グループを作成できます。この ID グループは、プロファイル済みエンドポイントID グループの子になります。エンドポイントポリシーを作成する場合、[プロファリング ポリシー（Profiling Policies）] ページの [一致する ID グループの作成（Create Matching Identity Group）] チェックボックスをオンにして、一致するエンドポイントID グループを作成できます。プロファイルのマッピングが削除されない限り、一致する ID グループは削除できません。

エンドポイント ID グループでの静的なエンドポイントの追加

エンドポイント ID グループの静的に追加されたエンドポイントを追加または削除できます。

[エンドポイント（Endpoints）] ウィジェットのエンドポイントのみを特定の ID グループに追加できます。エンドポイントを特定のエンドポイント ID グループに追加した場合、そのエンドポイントは、前に動的にグループ化されたエンドポイント ID グループから移動されます。

エンドポイントを最近追加したエンドポイント ID グループから削除すると、そのエンドポイントは、適切な ID グループに再プロファイリングされます。エンドポイントは、システムから削除されませんが、エンドポイントの ID グループからのみ削除されます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 エンドポイント ID グループを選択して [編集（Edit）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [エンドポイント（Endpoints）] ウィジェットでエンドポイントを選択して、選択したエンドポイントをエンドポイント ID グループに追加します。

ステップ 5 [エンドポイント グループ リスト（Endpoint Group List）] リンクをクリックして、[エンドポイント ID グループ（Endpoint Identity Groups）] ページに戻ります。

ダイナミック エンドポイントの、ID グループへの追加または削除後の再プロファイリング

エンドポイント ID グループが静的に割り当てられていない場合、エンドポイント ID グループに追加した、またはエンドポイント ID グループから削除したエンドポイントは、再プロファイリングされます。ISE プロファイラにより動的に識別されたエンドポイントは、適切なエンドポイント ID グループに表示されます。動的に追加されたエンドポイントをエンドポイント ID グループから削除した場合、Cisco ISE では、エンドポイント ID グループからエンドポイントを正常に削除したが、それらのエンドポイントをエンドポイント ID グループに再プロファイリングして戻すことを示すメッセージが表示されます。

許可ルールで使用されるエンドポイント ID グループ

エンドポイント ID グループを許可ポリシーで効率的に使用して、検出されたエンドポイントに適切なネットワーク アクセス権限を付与することができます。たとえば、すべてのタイプの Cisco IP Phone 用の許可ルールが、デフォルトで、Cisco ISE の **[ポリシー セット（Policy Sets）]** > **[デフォルト（Default）]** > **[許可ポリシー（Authorization Policy）]** で使用できます。

エンドポイント プロファイリング ポリシーがスタンドアロン ポリシー（他のエンドポイント プロファイリング ポリシーの親でない）であるか、またはエンドポイント プロファイリング ポリシーの親ポリシーが無効でないことを確認する必要があります。

クライアントマシン上のエージェントのダウンロードの問題

問題

ユーザの認証と許可の後、クライアント マシン ブラウザに「ポリシーが一致しません（no policy matched）」のエラー メッセージが表示されます。この問題は、認証のクライアント プロビジョニング フェーズ中のユーザ セッションに該当します。

考えられる原因

クライアント プロビジョニング ポリシーに必要な設定が欠落している可能性があります。

ポスチャ エージェントのダウンロードの問題

ポスチャ エージェントのインストーラをダウンロードするには、次のものが必要があることに注意してください。

- エージェントを初めてクライアント マシンにインストールする場合、ユーザはブラウザ セッションでActiveXインストーラを許可する必要があります（クライアント プロビジョニング ダウンロード ページでは、この情報の指定を求められます）。
- クライアント マシンには、インターネット アクセスが必要です。

解像度

- クライアント プロビジョニング ポリシーが Cisco ISE に存在することを確認します。存在する場合は、ポリシー内に定義されているポリシー ID グループ、条件およびエージェントのタイプを確認します（また、すべてのデフォルト値のプロファイルも含め、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）] > [NACまたは AnyConnect ポスチャプロファイル（NAC or AnyConnect Posture Profile）] >[AnyConnect ポスチャプロファイル（AnyConnect Posture Profile）]で設定されたエージェント プロファイルが存在するかどうかについても確認します）。
- アクセス スイッチのポートをバウンスすることにより、クライアント マシンの再認証を試行します。

エンドポイント

これらのページでは、ネットワークに接続するエンドポイントを設定および管理することができます。

エンドポイント設定

次の表に、エンドポイントを作成し、エンドポイントにポリシーを割り当てるために使用できる [エンドポイント（Endpoints）] ページのフィールドを示します。このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** です。

表 *105 :* エンドポイント設定

フィールド	使用上のガイドライン
MAC アドレス（MAC Address）	エンドポイントを静的に作成するには、MAC アドレスを 16 進数形式で入力します。 MAC アドレスは、Cisco ISE 対応のネットワークに接続するインターフェイスのデバイス ID です。
スタティック割り当て（Static Assignment）	[エンドポイント（Endpoints）] ページでエンドポイントを静的に作成する場合このチェックボックスをオンにすると、静的割り当てのステータスが static に設定されます。 エンドポイントのスタティック割り当てのステータスを静的から動的に、または動的から静的に切り替えできます。

フィールド	使用上のガイドライン
ポリシー割り当て	（スタティック割り当てが選択されていない限り、デフォルトで無効）[ポリシー割り当て（Policy Assignment）] ドロップダウン リストから一致するエンドポイント ポリシーを選択します。 次のいずれかを実行できます。 • 一致するエンドポイント ポリシーを選択しないで、デフォルトのエンドポイント ポリシーである不明を使用する場合、スタティック割り当てステータスはエンドポイントに対して動的に設定され、それにより、エンドポイントの動的プロファイリングが可能になります。 • 不明ではなく、一致するエンドポイント ポリシーを選択する場合、スタティック割り当てステータスはそのエンドポイントに対して静的に設定され、[スタティック割り当て（Static Assignment）] チェックボックスが自動的にオンにされます。
スタティック グループ割り当て（Static Group Assignment）	（[スタティック グループ割り当て（Static Group Assignment）] が選択されていない限り、デフォルトで無効）エンドポイントを ID グループに静的に割り当てる場合、このチェックボックスをオンにします。 このチェックボックスをオンにした場合、プロファイリング サービスは、前に他のエンドポイントID グループに動的に割り当てられたエンドポイントの次のエンドポイントポリシーの評価時に、そのエンドポイントID グループを変更しません。 このチェックボックスをオフにした場合、エンドポイントID グループは、ポリシー設定に基づいて ISE プロファイラにより割り当てられたダイナミック グループです。[スタティック グループ割り当て（Static Group Assignment）] オプションを選択しない場合、エンドポイントは、エンドポイント ポリシーの次回評価時に一致するID グループに自動的に割り当てられます。

フィールド	使用上のガイドライン

ID グループ割り当て	エンドポイントを割り当てるエンドポイント ID グループを選択します。
	
	エンドポイントを静的に作成する場合、またはエンドポイントのエンドポイント ポリシーの評価時に [一致する ID グループの作成（Create Matching Identity Group）] オプションを使用しない場合は、エンドポイントを ID グループに割り当てることができます。
	
	Cisco ISE には、次のシステムによって作成された次のエンドポイント ID グループがあります。
	
	• ブラックリスト
	• GuestEndpoints
	• プロファイル済み
	  • Cisco IP-Phone
	  • ワークステーション
	• RegisteredDevices
	• 不明

関連トピック

識別されたエンドポイント （822 ページ）

ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 （816 ページ）

エンドポイントの、LDAP からのインポートの設定

次の表では、LDAP サーバからのエンドポイントのインポートに使用できる [LDAP からのインポート（Import from LDAP）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]** です。

表 *106* : エンドポイントの、*LDAP* からのインポートの設定

フィールド	使用上のガイドライン
接続の設定	
ホスト	LDAP サーバのホスト名または IP アドレスを入力します。

フィールド	使用上のガイドライン
[ポート（Port）]	LDAP サーバのポート番号を入力します。デフォルト ポート 389 を使用して LDAP サーバからインポートするか、デフォルトポート 636 を使用して SSL を介して LDAP サーバからインポートできます。 （注） Cisco ISE では、任意の設定済みポート番号をサポートします。設定済みの値は、LDAP サーバ接続詳細に一致する必要があります。
セキュア接続を有効にする（Enable Secure Connection）	SSL を介して LDAP サーバからインポートするには、[セキュア接続を有効にする（Enable Secure Connection）] チェックボックスをオンにします。
ルート CA 証明書名	ドロップダウン矢印をクリックして、信頼できる CA 証明書を表示します。 ルート CA 証明書名は、LDAP サーバに接続する場合に必要となる信頼できる CA 証明書を指します。Cisco ISE 内の CA 証明書は、追加（インポート）、編集、削除、およびエクスポートが可能です。
匿名バインド（Anonymous Bind）	匿名バインドを有効にするには、[匿名バインド（Anonymous Bind）] チェックボックスをオンにします。 [匿名バインド（Anonymous Bind）] チェックボックスをオンにするか、または slapd.conf コンフィギュレーション ファイルの LDAP 管理者クレデンシャルを入力する必要があります。
管理者 DN（Admin DN）	slapd.conf コンフィギュレーション ファイルで LDAP 管理者に設定されている識別名（DN）を入力します。 管理者 DN フォーマット例：cn=Admin, dc=cisco.com, dc=com
[パスワード（Password）]	LDAP 管理者に設定されたパスワードを slapd.conf コンフィギュレーション ファイルに入力します。

フィールド	使用上のガイドライン
ベース DN（Base DN）	親エントリの認定者名を入力します。 ベース DN フォーマット例：dc=cisco.com, dc=com
クエリ設定（Query Settings）	
MAC アドレス objectClass（MAC Address objectClass）	MACアドレスのインポートに使用するクエリフィルタを入力します。たとえば、ieee802Device です。
MAC アドレス属性名（MAC Address Attribute Name）	インポートに対して返される属性名を入力します。たとえば、macAddress です。
プロファイル属性名（Profile Attribute Name）	LDAP 属性の名前を入力します。この属性は、LDAP サーバで定義されている各エンドポイント エントリのポリシー名を保持します。 [プロファイル属性名（Profile Attribute Name）] フィールドを設定する場合は、次の点を考慮してください。 • [プロファイル属性名（Profile Attribute Name）] フィールドでこの LDAP 属性を指定しない場合、またはこの属性を誤って設定した場合、インポート操作時にエンドポイントは「不明」としてマークされ、これらのエンドポイントは一致するエンドポイント プロファイリング ポリシーに個別にプロファイリングされます。 • [プロファイル属性名（Profile Attribute Name）] フィールドで LDAP 属性を設定した場合、その属性値は、エンドポイント ポリシーが Cisco ISE 内の既存のポリシーに一致することを確認するために検証され、エンドポイントがインポートされます。エンドポイント ポリシーが既存のポリシーと一致しない場合、それらのエンドポイントはインポートされません。
タイムアウト（秒）（Time Out [seconds]）	時間を秒単位（1 ～ 60 秒）で入力します。

関連トピック

識別されたエンドポイント （822 ページ）
LDAP サーバからのエンドポイントのインポート （821 ページ）

エンドポイント プロファイリング ポリシーの設定

次の表では、[エンドポイントポリシー（Endpoint Policies）] ウィンドウのフィールドについて説明します。このページのナビゲーション パスは、**[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[プロファイリング ポリシー（Profiling Policies）]** です。

表 *107 :* エンドポイント プロファイリング ポリシーの設定

フィールド名	使用上のガイドライン
名前（Name）	作成するエンドポイントプロファイリング ポリシーの名前を入力します。
説明	作成するエンドポイントプロファイリング ポリシーの説明を入力します。
ポリシー有効（Policy Enabled）	デフォルトでは [ポリシー有効（Policy Enabled）] チェックボックスはオンになっており、エンドポイントのプロファイリング時に、一致するプロファイリング ポリシーが関連付けられます。 オフになっている場合、エンドポイントのプロファイリング時に、エンドポイントプロファイリング ポリシーは除外されます。
最小確実度計数（Minimum Certainty Factor）	プロファイリング ポリシーに関連付ける最小値を入力します。デフォルト値は 10 です。
例外アクション（Exception Action）	プロファイリング ポリシー内のルールを定義するときに条件に関連付ける例外アクションを選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [例外アクション（Exception Actions）] で定義されます。

フィールド名	使用上のガイドライン
ネットワーク スキャン（NMAP）アクション（**Network Scan (NMAP) Action**）	必要に応じて、プロファイリング ポリシー内のルールを定義するときに条件に関連付けるネットワーク スキャン アクションをリストから選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）] > [結果（Results）]>[プロファイリング（Profiling）]>[ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Actions）] で定義されます。
ポリシーの ID グループの作成（**Create an Identity Group for the policy**）	エンドポイントIDグループを作成するには、次のオプションのいずれかをオンにします。 • はい、一致する ID グループを作成します（**Yes, create matching Identity Group**） • いいえ、既存の ID グループ階層を使用します（**No, use existing Identity Group hierarchy**）
はい、一致する ID グループを作成します（**Yes, create matching Identity Group**）	既存のプロファイリング ポリシーを使用する場合、このオプションを選択します。 このオプションは、これらのエンドポイントの一致するIDグループを作成します。エンドポイント プロファイルが既存のプロファイリング ポリシーと一致した場合に、IDグループは Profiled エンドポイント ID グループの子になります。 たとえば、ネットワーク上で検出されたエンドポイントが Xerox-Device プロファイルに一致する場合は、[エンドポイント ID グループ（Endpoint Identity Groups）] ページで Xerox-Device エンドポイント ID グループが作成されます。

フィールド名	使用上のガイドライン
いいえ、既存の ID グループ階層を使用します（**No, use existing Identity Group hierarchy**）	プロファイリング ポリシーおよび ID グループの階層構造を使用して、一致する親エンドポイント ID グループにエンドポイントを割り当てるには、このチェックボックスをオンにします。 このオプションを使用すると、エンドポイントプロファイリング ポリシー階層を利用することができ、エンドポイントはいずれかの一致する親エンドポイント ID グループ、さらに、親 ID グループに関連付けられたエンドポイント ID グループに割り当てられます。 たとえば、既存のプロファイルに一致するエンドポイントは、適切な親エンドポイント ID グループの下にグループ化されます。ここで、不明プロファイルに一致するエンドポイントは、[不明（Unknown）] の下にグループ化され、既存のプロファイルに一致するエンドポイントは、プロファイリングされたエンドポイント ID グループの下にグループ化されます。次の例を参考にしてください。 • エンドポイントが Cisco-IP-Phone プロファイルに一致する場合、これらのエンドポイントは Cisco-IP-Phone エンドポイント ID グループの下でグループ化されます。 • エンドポイントが Workstation プロファイルに一致する場合、これらのエンドポイントは、Workstation エンドポイント ID グループの下でグループ化されます。 Cisco-IP-Phone および Workstation エンドポイント ID グループは、システム内の Profiled エンドポイント ID グループに関連付けられます。
親ポリシー（**Parent Policy**）	新しいエンドポイントプロファイリング ポリシーを関連付ける、システムで定義されている親プロファイリングポリシーを選択します。 子にルールと条件を継承できる親プロファイリング ポリシーを選択できます。

フィールド名	使用上のガイドライン
関連 CoA タイプ（Associated CoA Type）	エンドポイントプロファイリングポリシーと関連付ける次のいずれかの CoA タイプを選択します。 • CoA なし（No CoA） • ポート バウンス • 再認証（Reauth） • [グローバル設定（Global Settings）] : [管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）] で設定されたプロファイラ設定から適用されます。
ルール（Rule）	エンドポイントプロファイリングポリシーで定義された 1 つ以上のルールにより、エンドポイントの一致するプロファイリングポリシーが決定されます。これにより、プロファイルに応じたエンドポイントのグループ化が可能になります。 ポリシー要素ライブラリからの 1 つ以上のプロファイリング条件がルールに使用され、エンドポイント属性およびその値が、全体的な分類用に検証されます。

フィールド名	使用上のガイドライン
条件（**Conditions**）	

フィールド名	使用上のガイドライン
	プラス（+）記号をクリックして、条件の固定オーバーレイを展開します。マイナス（-）記号をクリックするか、固定オーバーレイの外側をクリックして条件を閉じます。 [既存の条件をライブラリから選択（Select Existing Condition from Library）] または [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] をクリックします。 [既存の条件をライブラリから選択（Select Existing Condition from Library）]：ポリシー要素ライブラリからシスコによって事前定義された条件を選択して、式を定義できます。 [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）]：さまざまなシステム辞書またはユーザ定義辞書から属性を選択して、式を定義できます。 プロファイリング条件と次のいずれかとを関連付けることができます。 • 各条件の確実度係数の整数値 • その条件の例外アクションまたはネットワーク スキャン アクション プロファイリング条件と関連付ける、次のいずれかの定義済み設定を選択します。 • [確実度計数が増加する（Certainty Factor Increases）]：各ルールの確実度値を入力します。この値は、全体的な分類に関するすべての一致ルールに対して追加されます。 • [例外の操作を行う（Take Exception Action）]：このエンドポイント プロファイリング ポリシーの [例外アクション（Exception Action）] フィールドで設定された例外アクションがトリガーされます。 • [ネットワークスキャンを行う（Take Network Scan Action）]：このエンドポイント プロファイリング ポリシーの [ネットワークスキャン（NMAP）アクション

フィールド名	使用上のガイドライン
	（Network Scan (NMAP) Action）] フィールドで設定されたネットワーク スキャン アクションがトリガーされます。
既存の条件をライブラリから選択（Select Existing Condition from Library）	次を実行できます。 • ポリシー要素ライブラリに存在するシスコによって事前定義された条件を選択できます。AND または OR 演算子を使用して複数の条件を追加できます。 • [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。 • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます • [複製（Duplicate）]：選択した条件のコピーを作成します • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます • [削除（delete）]：選択した条件を削除します。

フィールド名	使用上のガイドライン

新しい条件の作成（高度なオプション）（**Create New Condition (Advance Option)**）	次を実行できます。
	• 式にアドホック属性/値の組み合わせを追加し、AND または OR 演算子を使用すると、複数の条件を追加できます。
	• [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。
	  • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます
	  • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます
	  • [複製（Duplicate）]：選択した条件のコピーを作成します
	  • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます
	  • [削除（delete）]：選択した条件を削除します。 AND または OR 演算子を使用できます

関連トピック

Cisco ISE プロファイリング サービス （748 ページ）
エンドポイント プロファイリング ポリシーの作成 （806 ページ）
UDID 属性を使用するエンドポイント コンテキストの可視性 （860 ページ）

UDID 属性を使用するエンドポイント コンテキストの可視性

固有識別子（UDID）は、特定のエンドポイントの MAC アドレスを識別するエンドポイント属性です。エンドポイントは複数の MAC アドレスを持つことがあります。たとえば、有線インターフェイスに 1 つ、ワイヤレスインターフェイス用にもう 1 つの MAC アドレスがある場合があります。AnyConnect エージェントはそのエンドポイントの UDID を生成し、それをエンドポイント属性として保存します。エンドポイントの UDID は一定であり、AnyConnect のインストールまたはアンインストールに伴って変更されることはありません。UDID を使用すると、[コンテキストの可視性（Context Visibility）] ウィンドウ（[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [コンプライアンス（Compliance）]）では、複

数のNICが装着されているエンドポイントの場合は複数のエントリではなく1つのエントリが表示されます。MACアドレスではなく特定のエンドポイントに対してポスチャ制御を行うことができます。

（注） UDIDを作成するには、エンドポイントのAnyConnectが4.7以上である必要があります。

IF-MIB

表 *108 :*

オブジェクト	OID
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

SNMPv2-MIB

表 *109 :*

オブジェクト	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0

オブジェクト	OID
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

IP-MIB

表 *110*:

オブジェクト	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToPhysicalPhysAddress	1.3.6.1.2.1.4.35.1.4

CISCO-CDP-MIB

表 *111*:

オブジェクト	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11

オブジェクト	OID
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

CISCO-VTP-MIB

表 *112* :

オブジェクト	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

CISCO-STACK-MIB

表 *113* :

オブジェクト	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

BRIDGE-MIB

表 *114*：

オブジェクト	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

OLD-CISCO-INTERFACE-MIB

表 *115*：

オブジェクト	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

CISCO-LWAPP-AP-MIB

表 *116*：

オブジェクト	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.2
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.1.9
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11

オブジェクト	OID
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

CISCO-LWAPP-DOT11-CLIENT-MIB

表 *117*:

オブジェクト	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1

オブジェクト	OID
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

CISCO-AUTH-FRAMEWORK-MIB

表 ***118*** *:*

オブジェクト	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10

オブジェクト	OID
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

EEE8021-PAE-MIB: RFC IEEE 802.1X

表 *119 :*

オブジェクト	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

HOST-RESOURCES-MIB

表 *120 :*

オブジェクト	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

LLDP-MIB

表 *121 :*

オブジェクト	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5

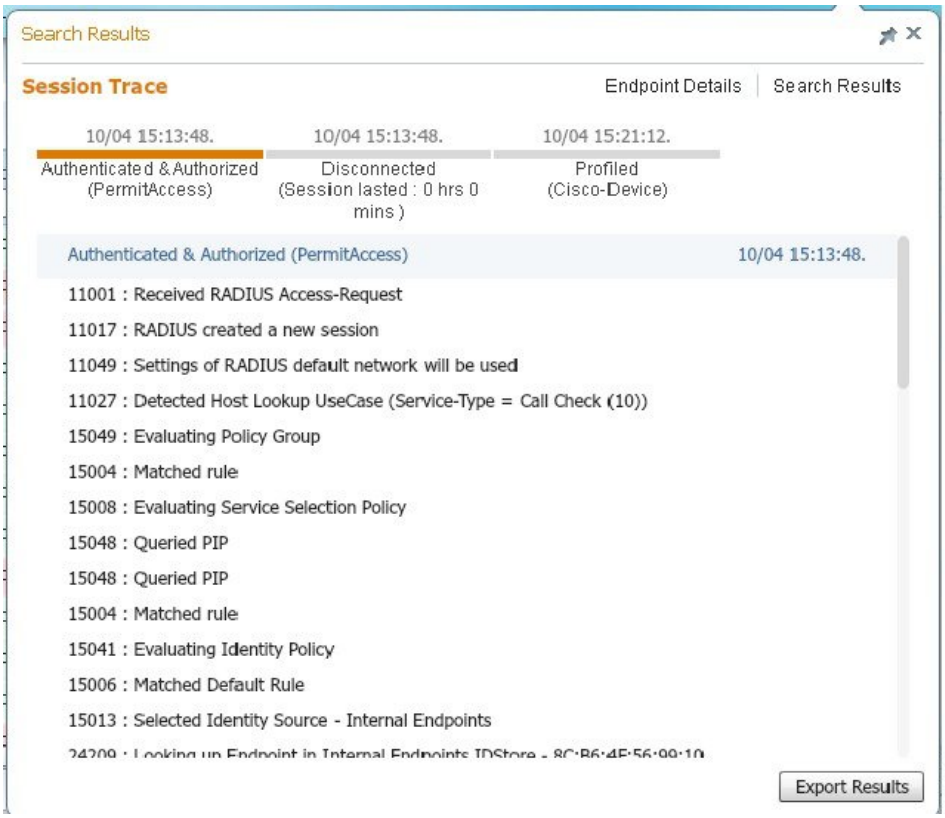
オブジェクト	OID
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
ldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

エンドポイントのセッションのトレース

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用して、特定のエンドポイントのセッション情報を取得できます。基準に基づいて検索する場合は、エンドポイントのリストを取得します。エンドポイントのセッショントレース情報を表示するには、そのエンドポイントをクリックします。次の図に、エンドポイントに表示されるセッショントレース情報の例を示します。

（注） 検索に使用されるデータ セットは、インデックスとしてのエンドポイント ID に基づいています。したがって、認証が行われる場合、検索結果セットにそれらを含めるには、認証にエンドポイントのエンドポイント ID が必要です。

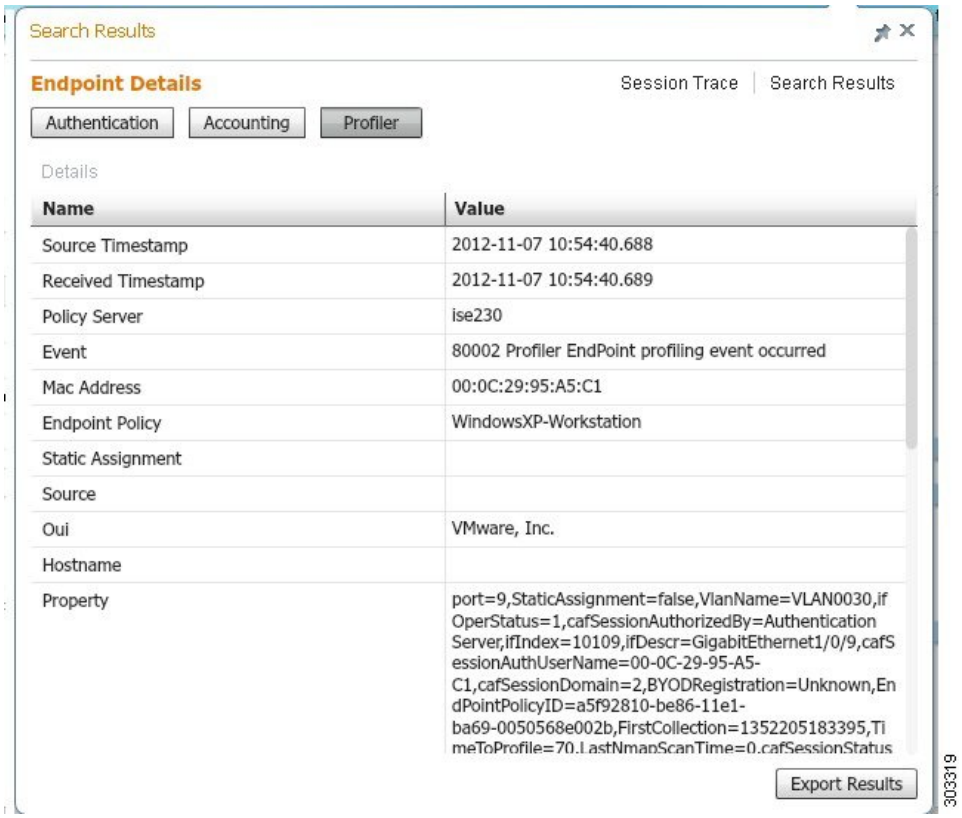
図 *37* : エンドポイントのセッションのトレース



上部にあるクリック可能なタイムラインを使用すると、主な許可の遷移を確認できます。[結果のエクスポート（Export Results）] ボタンをクリックして、.csv 形式で結果をエクスポートすることもできます。レポートはブラウザにダウンロードされます。

特定のエンドポイントの認証、アカウンティング、およびプロファイラの詳細情報を表示するには、[エンドポイントの詳細（Endpoint Details）] リンクをクリックします。次の図に、エンドポイントに対して表示されたエンドポイントの詳細情報の例を示します。

図 *38 :* エンドポイントの詳細



ディレクトリからのセッションの削除

次のように、セッションが、モニタリングおよびトラブルシューティング ノード上のセッション ディレクトリから削除されます。

- 終了したセッションは、終了後 15 分で削除されます。
- 認証はあるがアカウンティングがない場合、このようなセッションは 1 時間後に削除されます。
- すべての非アクティブ セッションは 5 日後に消去されます。

エンドポイントのグローバル検索

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用して、エンドポイントを検索できます。次の条件を使用してエンドポイントを検索できます。

- ユーザ名（User name）
- MAC アドレス（MAC Address）

- IPアドレス（IP Address）
- 許可プロファイル
- エンドポイント プロファイル
- 失敗の理由
- ID グループ
- ID ストア
- ネットワーク デバイス名
- ネットワーク デバイス タイプ
- オペレーティング システム（Operating System）
- ポスチャ ステータス
- 参照先
- セキュリティ グループ（Security Group）
- ユーザ タイプ（User Type）

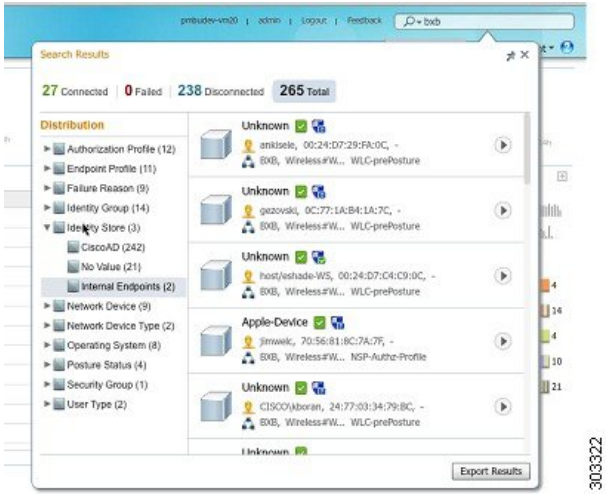
データを表示するには、[検索（Search）] フィールドに任意の検索条件の少なくとも 3 文字以上を入力する必要があります。

（注） エンドポイントが Cisco ISE によって認証された場合、またはそのアカウンティングの更新が受信された場合は、グローバル検索で確認できます。手動で追加され、Cisco ISE による認証または考慮がされていないエンドポイントは、検索結果に表示されません。

検索結果には、エンドポイントの現在のステータスに関する詳細および概要の情報が表示され、これをトラブルシューティングに使用することができます。検索結果には、上位 25 のエントリのみが表示されます。結果を絞り込むためにフィルタを使用することを推奨します。

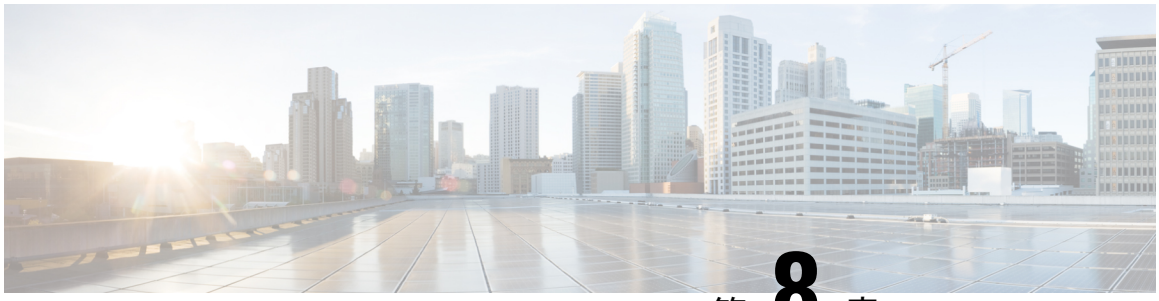
次の図は、検索結果の例を示しています。

図 *39 :* エンドポイントの検索結果



左パネルの任意のプロパティを使用して、結果をフィルタリングします。エンドポイントをクリックして、エンドポイントに関する次のような詳細情報を表示することもできます。

- セッションのトレース
- 認証の詳細
- アカウンティングの詳細
- ポスチャの詳細
- プロファイラの詳細
- クライアント プロビジョニングの詳細
- ゲスト アカウンティングおよびアクティビティ



第 8 章

個人所有デバイスの持ち込み（BYOD）

企業ネットワークのパーソナル デバイス（BYOD）

企業ネットワーク上のパーソナル デバイスをサポートする場合は、ユーザ（従業員、請負業者、およびゲスト）とそのデバイスを認証および許可することで、ネットワーク サービスおよび企業データを保護する必要があります。Cisco ISE は、従業員が企業ネットワーク上でパーソナル デバイスを安全に使用できるようにするために必要なツールを提供します。

ゲストは、ゲスト ポータルへのログイン時に、自動的に自分のデバイスを登録することができます。ゲストは、ゲスト タイプに定義されている最大数まで追加デバイスを登録できます。これらのデバイスは、ポータル構成に基づいてエンドポイント ID グループに登録されます。

ゲストは、ネイティブ サプリカント プロビジョニング（Network Setup Assistant）を実行するか、またはデバイスを [デバイス（My Devices）] ポータルに追加して、パーソナル デバイスをネットワークに追加できます。オペレーティング システムに基づいて、使用する適切なネイティブ サプリカント プロビジョニング ウィザードを決定するネイティブ サプリカント プロファイルを作成できます。

ネイティブ サプリカント プロファイルはすべてのデバイスで使用できるわけではないため、ユーザはデバイス ポータルを使用してこれらのデバイスを手動で追加することができます。または、これらのデバイスを登録するように BYOD ルールを設定できます。

ISE コミュニティ リソース

How To: ISE and BYOD - Onboarding, Registering, and Provisioning

How To: ISE and BYOD - Using Certificates for Differentiated Access

分散環境のエンドユーザのデバイス ポータル

Cisco ISE のエンドユーザ Web ポータルは、管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナに基づき、設定、セッション サポート、およびレポート作成を提供します。

- **管理ノード**：ユーザ、デバイス、およびエンドユーザ ポータルが管理ノードに書き込まれる構成の変更。
- **ポリシー サービス ノード**：エンドユーザ ポータルはポリシー サービス ノードで実行する必要があります。ここでは、ネットワーク アクセス、クライアント プロビジョニング、ゲスト サービス、ポスチャ、およびプロファイリングを含むすべてのセッション トラフィックが処理されます。ポリシー サービス ノードがノード グループに含まれる場合、1 つのノードで障害が発生すると、他のノードが障害を検出し、保留中のセッションをリセットします。
- **モニタリング ノード**：モニタリング ノードは、デバイス ポータル、スポンサー ポータル、およびゲスト ポータルでのエンドユーザおよびデバイスのアクティビティについて、データを収集、集約、およびレポートします。プライマリ モニタリング ノードで障害が発生した場合は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング ノードになります。

デバイス ポータルのグローバル設定

[ワーク センター（Work Centers）] > [BYOD] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）] または **[管理（Administration）] > [デバイス ポータルの管理（Device Portal Management）] > [設定（Settings）]** を選択します。

BYOD ポータルおよびデバイス ポータルの次の一般設定を設定できます。

- [従業員が登録するデバイス（Employee Registered Devices）]：[従業員を制限（Restrict employees to）] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は 5 デバイスに設定されています。
- [再試行 URL（Retry URL）]：デバイスを Cisco ISE にリダイレクトするために使用できる URL を [オンボードのための再試行 URL（Retry URL for onboarding）] に入力します。

これらの一般的な設定値を設定したら、これらの設定は会社に設定したすべて BYOD ポータルおよびデバイス ポータルに適用されます。

関連トピック

従業員が登録するパーソナル デバイス数の制限 （882 ページ）
BYOD 登録に再接続する URL の提供 （883 ページ）
分散環境のエンドユーザのデバイス ポータル （874 ページ）

パーソナル デバイス ポータル

Cisco ISE では、従業員が所有するパーソナル デバイスをサポートするために複数の Web ベース ポータルが提供されています。これらのデバイス ポータルは、ゲスト ポータル フローまたはスポンサー ポータル フローには関与しません。

次のポータルを使用します。

- **ブラックリスト ポータル**：「ブラックリスト」に掲載されているためネットワーク アクセスには使用できないパーソナル デバイスに関する情報を提供します。
- **BYOD ポータル**：従業員がネイティブ サプリカント プロビジョニング機能を使用して自分のパーソナル デバイスを登録できるようにします。
- **証明書プロビジョニング ポータル**：管理者および従業員が BYOD フローを通過できないデバイスについてユーザ/デバイス証明書を要求できるようにします。
- **クライアント プロビジョニング ポータル**：コンプライアンスをチェックするポスチャ エージェントを自分のデバイスにダウンロードするよう従業員に強制します。
- **MDM ポータル**：従業員が外部のモバイル デバイス管理（MDM）システムに自分のモバイル デバイスを登録できるようにします。
- **デバイス ポータル**：従業員がパーソナル デバイス（ネイティブ サプリカント プロビジョニングをサポートしないデバイスを含む）を追加および登録し、管理できるようにします。

Cisco ISE には、事前定義済みのデフォルト ポータルのセットを含む複数のデバイス ポータルを Cisco ISE サーバでホストする機能が用意されています。デフォルトのポータル テーマには、管理者ポータルからカスタマイズできる標準のシスコ ブランドが適用されています。組織に固有のイメージ、ロゴ、およびカスケーディング スタイル シート（CSS）ファイルをアップロードして、ポータルをさらにカスタマイズすることもできます。

デバイス ポータルへのアクセス

ステップ 1 デバイス ポータルへのアクセスには、次のいずれかを実行します。

- **[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** をクリックします。[デバイス ポータルの設定およびカスタマイズ（Configure and Customize Device Portals）] ページには、サポートされるデバイス ポータルのリストが表示されます。
- **[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** を選択します。ドロップダウン メニューにサポートされるデバイス ポータルが表示されます。

ステップ 2 設定する特定のデバイス ポータルを選択します。

ブラックリスト ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

従業員が自分のパーソナル デバイスを紛失したり盗まれたりした場合、デバイス ポータルでデバイスのステータスを更新して、ブラックリスト エンドポイント ID グループにデバイスを追加できます。これにより、不正なネットワーク アクセスにデバイスが使用されることを防ぎます。誰かがこれらのデバイスの1つを使用してネットワークに接続しようとすると、ブラックリスト ポータルにリダイレクトされ、デバイスがネットワークへのアクセスを拒否することが通知されます。デバイスが見つかった場合、従業員はデバイス ポータルでデバイスを復元し、デバイスを再登録せずにネットワーク アクセスを回復できます。デバイスの盗難か紛失かによっては、デバイスをネットワークに接続する前に、追加のプロビジョニングが必要になる場合があります。

ブラックリスト ポータルのポート設定（デフォルトはポート 8444）を設定できます。ポート番号を変更する場合は、別のエンドユーザ ポータルで使用されていないことを確認してください。

ブラックリスト ポータルの設定については、ブラックリスト ポータルの編集 （888ページ）を参照してください。

証明書プロビジョニング ポータル

従業員は、証明書プロビジョニング ポータルに直接アクセスできます。

証明書プロビジョニング ポータルでは、従業員はオンボーディング フローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスは、BYOD フローを通過できず、証明書を手動で発行する必要があります。証明書プロビジョニング ポータルで、権限のある一連のユーザは、そのようなデバイスに対する証明書要求をアップロードし、キー ペアを生成し（必要に応じて）、証明書をダウンロードできます。

従業員は、このポータルにアクセスして、1 つの証明書について要求を行うか、または CSV ファイルを使用して一括証明書要求を行うことができます。

ISE コミュニティ リソース

Identity Services Engine 証明書プロビジョニング ポータルの機能と設定については、「ISE 2.0: Certificate Provisioning Portal」を参照してください。

個人所有デバイスの持ち込みポータル

従業員は、このポータルに直接アクセスしません。

従業員は、ネイティブ サプリカントを使用してパーソナル デバイスを登録すると、個人所有デバイスの持ち込み（BYOD）ポータルにリダイレクトされます。従業員がパーソナルデバイスを使用して初めてネットワークにアクセスを試みると、手動で Network Setup Assistant（NSA）ウィザードをダウンロードして起動するように求められ、ネイティブ サプリカントの登録およ

びインストールに進む場合があります。デバイスを登録すると、デバイス ポータルを使用して、それを管理できます。

（注） BYOD フローは、デバイスが AnyConnect Network Access Manager（NAM）を使用してネットワークに接続すると、サポートされません。

関連トピック

BYOD ポータルの作成 （891 ページ）
企業ネットワークのパーソナル デバイス（BYOD） （873 ページ）

クライアント プロビジョニング ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

クライアント プロビジョニング システムでは、企業ネットワークにアクセスしようとしているデバイスのポスチャ評価および修復を行います。従業員がデバイスを使用してネットワークアクセスを要求したときに、クライアント プロビジョニング ポータルにルーティングして、最初にポスチャ エージェントをダウンロードするように要求できます。ポスチャ エージェントは、デバイスにアンチウイルス ソフトウェアがインストールされていることや、オペレーティング システムがサポートされていることの確認など、コンプライアンスに関するデバイスのスキャンを行います。

関連トピック

クライアント プロビジョニング ポータルの作成 （894 ページ）

モバイル デバイス管理ポータル

従業員は、このポータルに直接アクセスするのではなく、このポータルにリダイレクトされます。

数多くの会社で、従業員のモバイル デバイスを管理するために、モバイル デバイス管理（MDM）システムを使用しています。

Cisco ISE では外部 MDM システムとの統合が許可されており、従業員はこれを使用して、モバイルデバイスを登録し、企業ネットワークにアクセスすることができます。シスコでは、従業員がデバイスを登録し、ネットワークに接続するために使用できる外部MDMインターフェイスを提供しています。

MDM ポータルを使用することで、従業員は外部 MDM システムに登録できます。

従業員は、デバイス ポータルを使用して、PIN コードでのデバイスのロック、工場出荷時のデフォルト設定へのデバイスのリセット、デバイス登録時にインストールされていたアプリケーションおよび設定の削除など、モバイル デバイスの管理を行うことができます。

Cisco ISE では、すべての外部 MDM システム用に単一の MDM ポータルを、または個々の MDM システムごとに 1 つのポータルを使用できます。

MDM サーバを ISE とともに動作するように設定する方法については、MDM ポータルの作成（896 ページ）を参照してください。

デバイス ポータル

従業員は、デバイス ポータルに直接アクセスできます。

ネットワーク アクセスが必要な一部のネットワーク デバイスは、ネイティブ サプリカント プロビジョニングでサポートされていないため、BYOD ポータルを使用して登録することができません。ただし、従業員は、オペレーティング システムがサポートされていないか、Web ブラウザが搭載されていないパーソナル デバイス（プリンタ、インターネット ラジオ、その他のデバイスなど）を、デバイス ポータルを使用して追加および登録することができます。

従業員は、デバイスの MAC アドレスを入力して、新しいデバイスを追加および管理できます。従業員が、デバイス ポータルを使用してデバイスを追加すると、Cisco ISE はそのデバイスを **RegisteredDevices** エンドポイント ID グループのメンバーとして、[エンドポイント（Endpoints）] ページに追加します（別のエンドポイント ID グループに、すでに静的に割り当てられている場合を除く）。デバイスは、Cisco ISE の他のエンドポイントと同様にプロファイリングされ、ネットワーク アクセスのための登録プロセスが行われます。

1 つのデバイスからの 2 つの MAC アドレスがユーザによりデバイス ポータルに入力されると、それらが同じホスト名を持ち、ISE で 1 つのエントリとして統合されていることがプロファイリングによって設定されます。たとえば、ユーザは有線および無線のアドレスでラップトップを登録します。そのデバイス上での削除などの操作は、両方のアドレスで機能します。

登録済みデバイスがポータルから削除されると、デバイス登録状態属性と BYOD 登録状態属性は、それぞれ [未登録（NotRegistered）] および [いいえ（No）] に変更されます。ただし、これらの属性は、従業員のデバイス登録時にのみ使用される BYOD 属性であるため、ゲスト（従業員以外）がクレデンシャルを持つゲスト ポータルの [ゲスト デバイス登録（Guest Device Registration）] ページを使用してデバイスを登録した場合は、変更されずそのままになります。

従業員は、BYOD またはデバイス ポータルを使用して自分のデバイスを登録しているかどうかに関係なく、デバイス ポータルを使用してそれらを管理できます。

（注） 管理者ポータルがダウンしている場合、デバイス ポータルは使用できません。

関連トピック

デバイス ポータルの作成 （898 ページ）

BYOD の展開オプションとステータス ワークフロー

パーソナルデバイスをサポートする BYOD 展開フローは、次の要因によって若干異なります。

- シングルまたはデュアル SSID：シングル SSID の場合は、証明書の登録、プロビジョニング、およびネットワーク アクセスに同じ WLAN が使用されます。デュアル SSID 展開では、2 つの SSID があります。1 つは登録およびプロビジョニングを提供し、もう 1 つはセキュアなネットワーク アクセスを提供します。
- Windows、MacOS、iOS、または Android デバイス：ネイティブ サプリカントのフローは、サポートされているパーソナル デバイスを利用する従業員を BYOD ポータルにリダイレクトしてこれらのデバイス情報を確認することによって、デバイスのタイプに関係なく、同様に開始します。プロセスはデバイス タイプに応じて分岐します。

従業員がネットワークに接続する

1. **従業員のクレデンシャルが認証される**：Cisco ISE は、社内 Active Directory または社内の他の ID ストアと照合して従業員を認証し、許可ポリシーを提供します。
2. **デバイスが BYOD ポータルにリダイレクトされる**：デバイスが BYOD ポータルにリダイレクトされます。デバイスの [MAC アドレス（MAC address）] フィールドは自動的に事前設定されます。ユーザはデバイス名と説明を追加できます。
3. **ネイティブ サプリカントが設定される（MacOS、Windows、iOS、Android）**：ネイティブ サプリカントが設定されます。ただしこのプロセスはデバイスに応じて異なります。
   - MacOS および Windows デバイス：従業員が BYOD ポータルで [登録（Register）] をクリックして、サプリカント プロビジョニング ウィザード（Network Setup Assistant）をダウンロードしてインストールします。このウィザードではサプリカントが設定され、EAP-TLS 証明書ベース認証に使用する証明書が（必要に応じて）提供されます。デバイスの MAC アドレスと従業員のユーザ名が発行済み証明書に組み込まれます。

     （注） Network Setup Assistant は、そのデバイスのユーザが管理者権限を持っていない限り、Windows デバイスにダウンロードすることはできません。エンドユーザに管理者権限を与えることができない場合は、BYOD フローを使用するのではなく、GPO を使用して証明書をユーザのデバイスにプッシュします。

     （注） バージョン OSx 10.15 以降では、ユーザはサプリカント プロビジョニング ウィザード（SPW）のダウンロードを許可する必要があります。ユーザのデバイスに、Cisco ISE サーバからのダウンロードを許可または拒否するように求めるウィンドウが表示されます。

   - iOS デバイス：Cisco ISE ポリシー サーバは Apple の iOS ワイヤレス機能を使用して新しいプロファイルを IOS デバイスに送信します。このプロファイルには次の情報が含まれます。

- 発行済み証明書（設定されている場合）には iOS デバイスの MAC アドレスと従業員のユーザ名が組み込まれます。
- 802.1X 認証の EAP-TLS の使用を強制できる Wi-Fi サプリカント プロファイル。

- Android デバイス：Cisco ISE は、従業員に Google Play ストアから Cisco Network Setup Assistant（NSA）をダウンロードするように要求し、ルーティングします。アプリのインストール後に、従業員はNSA を開いてセットアップ ウィザードを開始できます。このウィザードでは、サプリカントの設定と、デバイスの設定に使用される発行済み証明書が生成されます。

4. **認可変更が発行される**：ユーザがオンボーディング フローを通過すると、Cisco ISE は認可変更（CoA）を開始します。これにより、MacOS X、Windows、および Android デバイスはセキュアな 802.1X ネットワークに再接続します。シングル SSID の場合、iOS デバイスも自動的に接続されますが、デュアル SSID の場合、ウィザードは iOS ユーザに手動で新しいネットワークに接続するように要求します。

（注） サプリカントを使用しない BYOD フローを設定できます。Cisco ISE コミュニティの資料（https://supportforums.cisco.com/blog/12705471/ise-byod-registration-only-without-native-supplicant-or-certificate-provisioning）を参照してください。

（注） [ターゲットネットワークが非表示になっている場合に有効にする（Enable if Target Network is Hidden）] チェック ボックスをオンにするのは、実際の WI-Fi ネットワークが非表示の場合に限ります。そうしないと、特にシングル SSID フロー（同じ Wi-Fi ネットワーク/SSID がオンボーディングと接続の両方に使用されている）の特定の iOS デバイスに対して Wi-Fi ネットワーク設定が適切にプロビジョニングされない場合があります。

BYOD セッション エンドポイント属性

エンドポイント属性 *BYODRegistration* の状態は、BYOD フローにおいて次の状態に変化します。

- *Unknown*：デバイスが BYOD フローを通過していません。
- *Yes*：デバイスは BYOD フローを通過し、登録されました。
- *No*：デバイスが BYOD フローを通過しましたが、登録されていません。つまり、デバイスは削除されています。

デバイス登録ステータスのエンドポイント属性

エンドポイント属性 *DeviceRegistrationStatus* の状態は、デバイス登録中に次の状態に変化します。

- *Registered*：デバイスは BYOD フローを通過し、登録されました。この属性が Pending から Registered になるまでに 20 分の遅れがあります。
- *Pending*：デバイスはBYODフローを通過し、登録されました。ただし、ISEはネットワーク上でこのデバイスを認識していません。
- *Not Registered*：デバイスがBYODフローを通過していません。これは、この属性のデフォルト状態です。
- *Stolen*：ユーザがデバイス ポータルにログインし、現在オンボーディングされているデバイスをStolenとしてマークしました。この状況が発生した場合は次のような処理が行われます。
  - 証明書とプロファイルをプロビジョニングしてデバイスのオンボーディングが行われた場合、ISE はそのデバイスに対してプロビジョニングされた証明書を失効させ、デバイスの MAC アドレスを **ブラックリスト**ID グループに割り当てます。そのデバイスはネットワークにアクセスできなくなります。
  - （証明書は含めず）プロファイルのみをプロビジョニングしてデバイスのオンボーディングが行われた場合、ISE はそのデバイスを **ブラックリスト** エンドポイント ID グループに割り当てます。この状況に対応する許可ポリシーを作成していない場合は、デバイスは引き続きネットワークにアクセスできます。たとえば、**IF Endpoint Identity Group is Blacklist AND BYOD_is_Registered THEN DenyAccess** となります。

  管理者は、さまざまなデバイスに対してネットワーク アクセスを無効にするアクション（証明書の削除や失効など）を行います。

  ユーザが盗まれたデバイスを復元すると、ステータスは *not registered* に戻ります。ユーザはそのデバイスを削除してからもう一度追加する必要があります。これにより、オンボーディング プロセスが開始されます。
- *Lost*：ユーザがデバイス ポータルにログオンし、現在オンボーディングされているデバイスを Lost としてマークしました。これにより、次のアクションが実行されます。
  - そのデバイスは **ブラックリスト** ID グループに割り当てられます。
  - デバイスに対してプロビジョニングされた証明書は失効します。
  - デバイスのステータスが *Lost.* に更新されます。
  - 「BYODRegistration」が *No* に更新されます。

  紛失デバイスをブロックする許可ポリシーを作成していない場合、紛失デバイスは引き続きネットワークにアクセスできます。ルールで **ブラックリスト** ID グループまたは *endpoint:BYODRegistration* 属性を使用できます。たとえば、**IF Endpoint Identity Group is Blacklist AND EndPoints:BYODRegistrations Equals No THEN BYOD** と指定できます。きめ細かなアクセスを設定するには、*NetworkAccess:EAPAuthenticationMethod Equals PEAP or*

EAP-TLS or EAP-FAST" , InternalUser:IdentityGroup Equals <<group>> をルールの IF 部分に追加することもできます。

従業員が登録するパーソナル デバイス数の制限

従業員が 1 ～ 999 のパーソナル デバイスを登録できるようにすることができます。従業員がパーソナルデバイスの登録に使用したポータルに関係なく、この設定では、すべてのポータルにわたって登録されるデバイスの最大数を定義します。

ステップ 1 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）]** を選択します。

ステップ 2 [従業員を制限（Restrict employees to）] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は 5 デバイスに設定されています。

ステップ 3 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

ネイティブ サプリカントを使用したデバイス登録のサポート

ネイティブ サプリカント プロファイルを作成して、Cisco ISE ネットワークでパーソナル デバイスをサポートできます。ユーザの許可要件に関連付けるプロファイルに基づいて、Cisco ISE はネットワークにアクセスするユーザのパーソナルデバイスをセットアップするために必要なサプリカント プロビジョニング ウィザードを提供します。

従業員がパーソナルデバイスを使用して初めてネットワークへのアクセスを試みると、登録およびサプリカントの設定の手順が自動的に示されます。デバイスを登録した後、デバイス ポータルを使用してデバイスを管理できます。

ネイティブ サプリカントがサポートするオペレーティング システム

ネイティブ サプリカントは、次のオペレーティング システムでサポートされます。

- Android（Amazon Kindle、B&N Nook を除く）
- Mac OS X（Apple Mac コンピュータの場合）
- Apple iOS デバイス（Apple iPod、iPhone、および iPad）
- Microsoft Windows 7、8（RT を除く）、Vista、および 10

クレデンシャルを持つゲスト ポータルを使用したパーソナル デバイスの登録を従業員に許可

クレデンシャルを持つゲスト ポータルを利用している従業員は、自分のパーソナル デバイスを登録できます。BYOD ポータルによって提供されるセルフ プロビジョニング フローにより、従業員は Windows、MacOS、iOS および Android デバイスで使用可能なネイティブ サプリカントを使用してネットワークにデバイスを直接接続できます。

始める前に

ネイティブ サプリカント プロファイルを作成する必要があります。

ステップ 1 **[ワーク センター（Work Center）] > [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲスト ポータル（Guest Portals）]** を選択します。

ステップ 2 従業員がネイティブ サプリカントを使用して自分のデバイスを登録するために使用できるクレデンシャルを持つゲスト ポータルを選択し、[編集（Edit）] をクリックします。

ステップ 3 [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブおよび [BYOD 設定（BYOD Settings）] で、[従業員にネットワークでのパーソナル デバイスの使用を許可する（Allow employees to use personal devices on the network）] をオンにします。

ステップ 4 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

BYOD 登録に再接続する URL の提供

BYOD ポータルを使用してパーソナル デバイスを登録中に問題が発生した従業員に、登録プロセスへの再接続を可能にする情報を提供できます。

ステップ 1 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [設定（Settings）] > [再試行 URL（Retry URL）]** を選択します。

ステップ 2 IP アドレスを変更するか、またはデバイスを Cisco ISE にリダイレクトするために使用できる URL を [オンボードのための再試行 URL（Retry URL for onboarding）] に入力します。

登録プロセス中に従業員のデバイスに問題が発生した場合、デバイスはインターネットに自動的に再接続しようとします。この時点で、ここに入力する IP アドレスまたはドメイン名がデバイスを Cisco ISE にリダイレクトし、オンボーディング プロセスが再開されます。デフォルト値は 1.1.1.1 です。

ステップ 3 [保存（Save）]をクリックします。設定の更新を保存しない場合は、[リセット（Reset）]をクリックして、最後に保存した値に戻します。

デバイス ポータルの設定タスク

デフォルトポータルと、証明書、エンドポイントIDグループ、IDソース順序、ポータルテーマ、イメージ、およびCisco ISEによって提供されるその他の詳細などのデフォルト設定を使用できます。デフォルト設定を使用しない場合は、新しいポータルを作成するか、必要性に合うように既存の設定を編集する必要があります。同じ設定で複数のポータルを作成する場合は、ポータルを複製できます。

新しいポータルを作成したり、デフォルトポータルを編集した後は、ポータルの使用を承認する必要があります。いったんポータルの使用を承認すると、後続の設定変更はただちに有効になります。

デバイス ポータルを使用するための許可は必要ありません。

ポータルを削除する場合は、関連付けられている許可ポリシールールおよび許可プロファイルを先に削除するか、別のポータルを使用するように変更する必要があります。

この表を使用して、異なるデバイス ポータルの設定に関連するタスクを確認できます。

タスク	ブラックリスト ポータル	BYOD ポータル	クライアント プロビジョニング ポータル	MDM ポータル	デバイス ポータル
ポリシー サービスの有効化 （885 ページ）	必須（Required）	必須（Required）	必須（Required）	必須（Required）	必須（Required）
デバイス ポータルへの証明書の追加 （886 ページ）	必須（Required）	必須（Required）	必須（Required）	必須（Required）	必須（Required）
外部 ID ソースの作成 （886 ページ）	不要	不要	不要	不要	必須（Required）
ID ソース順序の作成 （887 ページ）	不要	不要	不要	不要	必須（Required）
エンドポイント ID グループの作成 （888 ページ）	不要	必須（Required）	不要	必須（Required）	必須（Required）

タスク	ブラックリスト ポータル	BYOD ポータル	クライアント プロビジョニング ポータル	MDM ポータル	デバイス ポータル
ブラックリスト ポータルの編集（888 ページ）	必須（Required）	N/A	N/A	N/A	N/A
BYOD ポータルの作成（891 ページ）	N/A	必須（Required）	N/A	N/A	N/A
クライアント プロビジョニング ポータルの作成（894 ページ）	N/A	N/A	必須（Required）	N/A	N/A
MDM ポータルの作成（896 ページ）	N/A	N/A	N/A	必須（Required）	N/A
デバイス ポータルの作成（898 ページ）	N/A	N/A	N/A	N/A	必須（Required）
許可プロファイルの作成（899 ページ）	N/A	必須（Required）	必須（Required）	必須（Required）	不要
デバイス ポータルのカスタマイズ（901 ページ）	オプション	オプション	オプション	オプション	オプション

ポリシー サービスの有効化

Cisco ISE エンドユーザ Web ポータルをサポートするには、ホストするノードでポータル ポリシー サービスを有効にする必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択します。
ステップ 2 ノードをクリックして、[編集（Edit）] をクリックします。
ステップ 3 [全般設定（General Settings）] タブで、[ポリシー サービス（Policy Service）] をオンにします。
ステップ 4 [セッション サービスの有効化（Enable Session Services）] オプションをオンにします。

ステップ 5 [保存（Save）] をクリックします。

デバイス ポータルへの証明書の追加

デフォルトの証明書を使用しない場合は、有効な証明書を追加して、証明書グループ タグに割り当てることができます。すべてのエンドユーザ Web ポータルに使用されるデフォルトの証明書グループ タグは [デフォルト ポータル証明書グループ（Default Portal Certificate Group）] です。

（注） BYOD は、3 つ以上の証明書チェーンをサポートしていません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 システム証明書を追加し、ポータルに使用する証明書グループ タグに割り当てます。

この証明書グループ タグは、ポータルを作成または編集するときに選択できるようになります。

ステップ 3 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > （任意のポータル） > [作成または編集（Create or Edit）] > [ポータル設定（Portal Settings）]** を選択します。

ステップ 4 新しく追加された証明書に関連付けられた [証明書グループ タグ（Certificate Group Tag）] ドロップダウン リストから特定の証明書グループ タグを選択します。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバなどの外部 ID ソースに接続して、認証/許可のユーザ情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザ ID を受信して共有できるようにするパッシブ ID サービスを使用するには、を参照してくださいその他の パッシブ ID サービス プロバイダー （647 ページ）。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。

- Active Directory：外部 ID ソースである Active Directory に接続する場合。外部 ID ソースとしての Active Directory （587 ページ）を参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、LDAP （696 ページ）を参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバを追加する場合。詳細については、RADIUS トークン ID ソース （722 ページ）を参照してください。
- RSA SecurID：RSA SecurID サーバを追加する場合。詳細については、RSA ID ソース （730 ページ）を参照してください。
- SAML IDプロバイダー（SAML Id Providers）：Oracle Access Manager などの ID プロバイダー（IdP）を追加する場合。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダ （738 ページ）を参照してください。
- **ソーシャル ログイン**：Facebook などのソーシャル ログインを外部 ID ソースとして追加する場合。アカウント登録ゲストのソーシャル ログイン （389 ページ）を参照してください。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ゲスト ユーザがローカル WebAuth を使用して認証できるようにするには、ゲスト ポータル認証ソースと ID ソース順序に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] > [追加（Add）]** を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リスト ボックスの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストのデータベースを並べ替えます。

ステップ 6 [高度な検索リスト（Advanced Search List）] 領域で、次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus 属性を ProcessError に設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が検索を中止する場合。
- [ユーザが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]：最初に選択された ID ソースでユーザが見つからないとき、Cisco ISE が順序内の他の選択された ID ソースの検索を続行する場合。

Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストに、Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイント ID グループ（Endpoint Identity Groups）] ページで追加のエンドポイント ID グループを作成することもできます。作成したエンドポイント ID グループを編集または削除できます。システム定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集したり、これらのグループを削除したりすることはできません。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するエンドポイント ID グループの名前を入力します（エンドポイント ID グループの名前にスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの説明を入力します。

ステップ 5 [親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 [送信（Submit）] をクリックします。

ブラックリスト ポータルの編集

Cisco ISE では、Cisco ISE でブラックリストに登録されている紛失したり、盗難にあったりしたデバイスが企業ネットワークへのアクセスを試行した場合に、情報が表示される単一のブラックリスト ポータルが提供されます。

デフォルトのポータル設定を編集し、ポータルについて表示されるデフォルトのメッセージをカスタマイズすることのみができます。新しいブラックリストポータルを作成することはできず、デフォルト ポータルを複製または削除することもできません。

始める前に

このポータルで使用するために、必要な証明書が設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [ブラックリスト ポータル（Blacklist Portal）] > [編集（Edit）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 3 ポータルで使用する言語ファイルをエクスポートおよびインポートするには、[言語（Languages）] メニューを使用します。

ステップ 4 [ポータルの設定（Portal Settings）] で証明書グループ タグ、言語などのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアント プロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PANがポータルの実行に使用できるPSNインターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上のIPアドレスを使用してイーサネットインターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべてのPSNがゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイスIPに解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、そのPSNにボンドセットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- **表示言語**
  - [ブラウザのロケールを使用する（Use browser locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。

- [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前またはSSID（セッションサービス識別子）を入力します。

ステップ 5 [ポータル ページのカスタマイズ（Portal Page Customization）] タブで、許可されていないデバイスがネットワークへのアクセスの取得を試行した場合にポータルに表示されるパージタイトルおよびメッセージテキストをカスタマイズします。

ステップ 6 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

BYOD ポータルの作成

個人所有デバイスの持ち込み（BYOD）ポータルを提供して、ネットワークへのアクセスの許可の前に登録とサプリカント設定を行うことができるように、従業員がパーソナルデバイスを登録できるようにすることができます。

新しいBYODポータルを作成するか、既存のものを編集または複製できます。Cisco ISEによって提供されているデフォルトのポータルを含むすべての BYOD ポータルを削除できます。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、デバイス ポータル フロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ページなどのページを有効にすると、そのページがフローに表示され、従業員はポータルで使用できるようになります。無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書とエンドポイント ID グループが設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [BYOD ポータル（BYOD Portals）] > [作成、編集または複製（Create, Edit or Duplicate）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] でポート、証明書グループ タグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 5 ネットワーク アクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、[サポート情報ページの設定（Support Information Page Settings）] を更新します。

ステップ 6 [ポータル ページのカスタマイズ（Portal Page Customization）] タブで、プロビジョニング プロセス時に次のページに表示される [コンテンツ領域（Content Area）] メッセージ テキストをカスタマイズします。

- [BYOD ウェルカム（BYOD Welcome）] ページ：
  - [デバイス設定が必要（Device Configuration Required）]：デバイスが BYOD ポータルに初めてリダイレクトされ、証明書のプロビジョニングが必要な場合。
  - [証明書の更新が必要（Certificate Needs Renewal）]：前の証明書が更新される必要がある場合。
- [BYOD デバイス情報（BYOD Device Information）] ページ：
  - [最大デバイス数に到達（Maximum Devices Reached）]：従業員が登録できるデバイスの最大数に到達した場合。
  - [必要なデバイス情報（Required Device Information）]：従業員がデバイスを登録できるようにするために必要なデバイス情報を要求している場合。
- [BYOD インストール（BYOD Installation）] ページ：
  - [デスクトップ インストール（Desktop Installation）]：デスクトップ デバイス用のインストール情報を提供する場合。
  - [iOS インストール（iOS Installation）]：iOS モバイル デバイス用のインストールの指示を提供する場合。
  - [Android インストール（Android Installation）]：Android モバイル デバイス用のインストールの指示を提供する場合。
- [BYOD 成功（BYOD Success）] ページ：
  - [成功（Success）]：デバイスが設定され、自動的にネットワークに接続される場合。
  - [成功：手動手順（Success: Manual Instructions）]：デバイスが正常に設定され、従業員がネットワークに手動で接続する必要がある場合。
  - [成功：サポート対象外のデバイス（Success: Unsupported Device）]：サポート対象外のデバイスがネットワークに接続できる場合。

ステップ 7 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

クライアント プロビジョニング ポータルの作成

Cisco ISE では証明書プロビジョニング ポータルが提供され、そこではオンボーディング フローを通過できないデバイスについて証明書を要求することができます。たとえば、販売時点管理端末などのデバイスがあります。1つの証明書について要求を行うか、またはCSVファイルを使用して一括証明書要求を行うことができます。

デフォルトのポータル設定を編集し、ポータルに表示されるメッセージをカスタマイズすることができます。また、証明書プロビジョニング ポータルを作成、複製、および削除することもできます。

証明書プロビジョニング ポータルにアクセスできるユーザには 2 つのタイプがあります。

- 管理者権限を持つ内部または外部のユーザ：自分自身と他人に対し証明書を生成できます。
- 他のすべてのユーザ：自分自身にのみ証明書を生成できます。

スーパー管理ロールまたは ERS 管理ロールを割り当てられたユーザ（ネットワーク アクセス ユーザ）はこのポータルにアクセスでき、他人のために証明書を要求できます。ただし、新しい内部管理ユーザを作成し、スーパー管理ロールまたは ERS 管理ロールを割り当てると、内部管理ユーザはこのポータルにアクセスできません。最初にネットワーク アクセス ユーザを作成し、それからユーザをスーパー管理グループまたは ERS 管理グループに追加する必要があります。スーパー管理グループまたはERS管理グループに追加されている既存のネットワーク アクセス ユーザは、このポータルにアクセスできます。

証明書プロビジョニング ポータルにアクセスするための管理者アカウントを作成するには、次の手順を実行します。

1. 内部ユーザを追加します（[管理（Administration）] > [IDの管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] > [追加（Add）]）。
2. ユーザをスーパー管理グループまたは ERS 管理グループに追加します（[管理（Administration）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理ユーザ（Admin Users）] > [追加（Add）] > [既存のネットワークアクセスユーザから選択（Select from existing network access user）]）。これでユーザが内部ネットワーク アクセス ユーザとスーパー管理ユーザまたは ERS 管理ユーザの両方になりました。

他のユーザがポータルにアクセスし、自分自身の証明書を生成できるようにするには、証明書プロビジョニング ポータルの設定を行います（[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニングポータル（Certificate Provisioning Portal）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]）。[認証方式（Authentication Method）] で適切な ID ソースまたは ID ソース順序を選択し、[承認済みグループの設定（Configure Authorized Groups）] でユーザ グループを選択します。選択したグループに属するすべてのユーザが、ポータルにアクセスし、自分自身の証明書を生成できるようになります。

始める前に

このポータルで使用するために、必要な証明書が設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニングポータル（Certificate Provisioning Portal）] > [作成（Create）]** の順に選択します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ステップ 3 [言語ファイル（Language File）] メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] で証明書グループ タグ、言語などのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 5 [ポータルページのカスタマイズ（Portal Page Customization）] タブで、ポータルに表示されるページ タイトルおよびメッセージ テキストをカスタマイズします。

ステップ 6 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

クライアント プロビジョニング ポータルの作成

クライアント プロビジョニング ポータルを提供して、ネットワークへのアクセスを許可する前に、デバイスのポスチャ コンプライアンスを確認する Cisco AnyConnect ポスチャ コンポーネントまたは を従業員がダウンロードできるようにすることができます。

新しいクライアント プロビジョニング ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのクライアント プロビジョニング ポータルを削除できます。

スーパー管理ロールまたは ERS 管理ロールを割り当てられたユーザ（ネットワーク アクセス ユーザ）はこのポータルにアクセスできます。ただし、新しい内部管理ユーザを作成し、スーパー管理ロールまたは ERS 管理ロールを割り当てると、内部管理ユーザはこのポータルにアクセスできません。最初にネットワーク アクセス ユーザを作成し、それからユーザをスーパー管理グループまたは ERS 管理グループに追加する必要があります。スーパー管理グループまたは ERS 管理グループに追加されている既存のネットワーク アクセス ユーザは、このポータルにアクセスできます。

クライアント プロビジョニング ポータルにアクセスするための管理者アカウントを作成するには、次の手順を実行します。

1. 内部ユーザを追加します（[管理（Administration）] > [IDの管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）] > [追加（Add）]）。
2. ユーザをスーパー管理グループまたは ERS 管理グループに追加します（[管理（Administration）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理ユーザ（Admin Users）] > [追加（Add）] > [既存のネットワークアクセスユーザから選

択（Select from existing network access user）]）。これでユーザが内部ネットワーク アクセス ユーザとスーパー管理ユーザまたは ERS 管理ユーザの両方になりました。

他のユーザがポータルにアクセスし、自分自身の証明書を生成できるようにするには、クライアント プロビジョニング ポータルの設定を行います（[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [クライアント プロビジョニング（Client Provisioning）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]）。[認証方式（Authentication Method）] で適切な ID ソースまたは ID ソース順序を選択し、[承認済みグループの設定（Configure Authorized Groups）] でユーザ グループを選択します。選択したグループに属するすべてのユーザが、ポータルにアクセスできるようになります。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、デバイス ポータル フロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ページなどのページを有効にすると、そのページがフローに表示され、従業員はポータルで使用できるようになります。無効にすると、フローから削除されます。

始める前に

このポータルで使用するために設定されている必要な証明書とクライアント プロビジョニング ポリシーがあることを確認します。

ステップ 1 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [クライアント プロビジョニング ポータル（Client Provisioning Portals）] > [作成、編集または複製（Create, Edit or Duplicate）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] でポート、証明書グループ タグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 5 ネットワーク アクセスの問題のトラブルシューティングのためにヘルプデスクが使用する情報を従業員が提供するのに役立つように、[サポート情報ページの設定（Support Information Page Settings）] を更新します。

ステップ 6 [ポータル ページのカスタマイズ（Portal Page Customization）] タブで、プロビジョニング プロセス時にクライアント プロビジョニング ポータルに表示される [コンテンツ領域（Content Area）] メッセージ テキストをカスタマイズします。

a) [クライアント プロビジョニング（Client Provisioning）] ページ：

- [確認、スキャン、および準拠（Checking, Scanning and Compliant）]：ポスチャ エージェントが正常にインストールされ、デバイスがポスチャ要件に準拠していることを確認、スキャン、および検証する場合。

- [非準拠（Non-compliant）]：ポスチャ エージェントが、デバイスがポスチャ要件に準拠していないと判断した場合。

b) [クライアント プロビジョニング（エージェントが見つかりませんでいた）（Client Provisioning (Agent Not Found)）] ページ：

- [エージェントが見つかりませんでした（Agent Not Found）]：ポスチャ エージェントがデバイスで検出されない場合。
- [手動インストールの手順（Manual Installation Instructions）]：デバイスに Java または Active X ソフトウェアがインストールされていない場合の、ポスチャ エージェントを手動でダウンロードし、インストールする方法の手順。
- [インストール、Java/ActiveX なし（Install, No Java/ActiveX）]：デバイスに Java または Active X ソフトウェアがインストールされていない場合の、手動で Java プラグインをダウンロードし、インストールする方法の手順。
- [エージェント インストール済み（Agent Installed）]：ポスチャ エージェントがデバイスで検出された場合の、ポスチャ エージェントを開始する方法の手順。これにより、デバイスがポスチャ要件に準拠するかどうかが確認される。

ステップ 7 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。

関連トピック

ポータルの許可 （411 ページ）
デバイス ポータルのカスタマイズ （901 ページ）

MDM ポータルの作成

モバイル デバイス管理（MDM）ポータルを提供して、従業員が、企業ネットワークでの使用のために登録されたモバイル デバイスを管理できるようにすることができます。

新しい MDM ポータルを作成するか、既存のものを編集または複製できます。すべての MDM システムに対して 1 つの MDM ポータルを設定できます。または、各システムに対し 1 つのポータルを作成できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべての MDM ポータルを削除できます。デフォルトのポータルは、サードパーティの MDM プロバイダー用です。

新しいMDMポータルを作成するか、既存のものを編集または複製できます。Cisco ISEによって提供されているデフォルトのポータルを含むすべての MDM ポータルを削除できます。デフォルトのポータルは、サードパーティの MDM プロバイダー用です。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、デバイス ポータル フロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ページなどのページを有効にすると、そのページがフローに表示され、従業員はポータルで使用できるようになります。無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書とエンドポイント ID グループが設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [MDM ポータル（MDM Portals）] > [作成、編集または複製（Create, Edit or Duplicate）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] でポート、証明書グループ タグ、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 5 特定のページのそれぞれに適用される次の設定を更新してください。

- [従業員のモバイル デバイス管理の設定（Employee Mobile Device Management Settings）] では、サードパーティの MDM プロバイダーを設定するために提供されているリンクにアクセスし、MDM ポータルを使用して従業員の受信ポリシーによる動作を定義します。
- ネットワーク アクセスの問題のトラブルシューティングのためにヘルプ デスクによって使用される情報をゲストが提供するのに役立つように、[サポート情報ページの設定（Support Information Page Settings）] を更新します。

ステップ 6 [ポータル ページのカスタマイズ（Portal Page Customization）] タブで、デバイス登録プロセス時に MDM ポータルに表示される [コンテンツ領域（Content Area）] メッセージをカスタマイズします。

- [到達不能（Unreachable）]：選択された MDM システムにアクセスできない場合。
- [非準拠（Non-compliant）]：登録されるデバイスが MDM システムの要件に準拠していない場合。
- [続行（Continue）]：接続に問題がある場合にデバイスがネットワークへの接続を試行する必要がある場合。
- [登録（Enroll）]：デバイスが MDM エージェントを必要とし、かつそのデバイスを MDM システムに登録する必要がある場合。

ステップ 7 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

次のタスク

ポータルを使用するには、そのポータルを許可する必要があります。ポータルを使用できるように許可する前または後に、ポータルをカスタマイズすることもできます。また、次のトピックを参照してください。

- デバイス ポータルへの証明書の追加 （886 ページ）
- エンドポイント ID グループの作成 （888 ページ）
- 許可プロファイルの作成 （899 ページ）
- デバイス ポータルのカスタマイズ （901 ページ）

デバイス ポータルの作成

デバイス ポータルを提供して、従業員が、ネイティブ サプリカントをサポートせず、個人所有デバイスの持ち込み（BYOD）を使用して追加できないパーソナルデバイスを追加および登録できるようにすることができます。デバイス ポータルを使用して、いずれかのポータルを使用して追加されたすべてのデバイスを管理できます。

新しいデバイス ポータルを作成するか、既存のものを編集または複製できます。Cisco ISE によって提供されているデフォルトのポータルを含むすべてのデバイス ポータルを削除できます。

[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] タブのページ設定に加えた変更は、デバイス ポータル フロー図のグラフィカル フローに反映されます。[サポート情報（Support Information）] ページなどのページを有効にすると、そのページがフローに表示され、従業員はポータルで使用できるようになります。無効にすると、フローから削除されます。

始める前に

このポータルで使用するために、必要な証明書、外部 ID ストア、ID ソース順序、およびエンドポイント ID グループが設定されていることを確認します。

ステップ 1 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）]** を選択します。

ステップ 2 ポータルの一意の [ポータル名（Portal Name）] および [説明（Description）] を指定します。

ここで使用するポータル名が他のエンドユーザ ポータルに使用されていないことを確認します。

ステップ 3 [言語ファイル（Language File）] ドロップダウン メニューを使用して、ポータルで使用する言語ファイルをエクスポートおよびインポートします。

ステップ 4 [ポータルの設定（Portal Settings）] でポート、証明書グループ タグ、ID ソース順序、エンドポイント ID グループなどのデフォルト値を更新し、ポータル全体に適用する動作を定義します。

ステップ 5 特定のページのそれぞれに適用される次の設定を更新してください。

- [ログイン ページの設定（Login Page Settings）]：従業員クレデンシャルおよびログイン ガイドラインを指定します。
- [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]：別の AUP ページを追加し、従業員の利用規定の動作を定義します。
- [ポストログイン バナーページの設定（Post-Login Banner Page Settings）]：ポータルへのログイン後に、従業員に追加情報を通知します。
- [従業員のパスワード変更の設定（Employee Change Password Settings）]：従業員の自身のパスワードの変更を許可します。このオプションは、従業員が内部ユーザ データベースの一部である場合にのみ有効になります。

ステップ 6 [ポータル ページのカスタマイズ（Portal Page Customization）] タブで、登録および管理時にデバイス ポータルに表示される次の情報をカスタマイズします。

- タイトル、コンテンツ、フィールド、およびボタン ラベル
- エラー メッセージおよび通知メッセージ

ステップ 7 [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

次のタスク

ポータルの外観を変更する場合は、ポータルをカスタマイズできます。参照先

関連トピック

デバイス ポータルのカスタマイズ （901 ページ）
デバイス ポータル （878 ページ）
従業員が追加したデバイスの表示 （901 ページ）

許可プロファイルの作成

ポータルを許可するときは、ネットワーク アクセス用のネットワーク許可プロファイルおよびルールを設定します。

始める前に

ポータルを許可する前にポータルを作成する必要があります。

ステップ 1 ポータルの特別な許可プロファイルを設定します。
ステップ 2 プロファイルの許可ポリシー ルールを作成します。

許可プロファイルの作成

各ポータルには、特別な許可プロファイルを設定する必要があります。

始める前に

デフォルトのポータルを使用しない場合は、許可プロファイルとポータル名を関連付けることができるように、最初にポータルを作成する必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 使用を許可するポータル名を使用して許可プロファイルを作成します。

次のタスク

新しく作成される許可プロファイルを使用するポータル許可ポリシー ルールを作成する必要があります。

許可ポリシー ルールの作成

ユーザ（ゲスト、スポンサー、従業員）のアクセス要求への応答に使用するポータルのリダイレクション URL を設定するには、そのポータル用の許可ポリシー ルールを定義します。

url-redirect は、ポータル タイプに基づいて次の形式になります。

ip:port = IP アドレスとポート番号

PortalID = 一意のポータル名

ホットスポット ゲスト ポータル：
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

モバイル デバイス管理（MDM）ポータル：
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択して、[標準（Standard）] ポリシーで新しい許可ポリシー ルールを作成します。

ステップ 2 [条件（Conditions）] には、ポータルの検証に使用するエンドポイント ID グループを選択します。たとえば、ホットスポット ゲスト ポータルの場合は、デフォルトの [GuestEndpoints] エンドポイント ID グループを選択し、MDM、ポータルの場合は、デフォルトの [RegisteredDevices] エンドポイント ID グループを選択します。

（注） ホットスポット ゲスト ポータルは、Termination CoA だけを発行するため、ゲスト許可ポリシーの検証条件の 1 つとして [Network Access:UseCase EQUALS Guest Flow] を使用しないでください。代わりに、エンドポイントが属する ID グループに照合して検証を行います。次の例を参考にしてください。

- "GuestEndpoint" + Wireless MAB の場合は Permit Access
- Wireless MAB の場合は HotSpot Redirect

ステップ 3 [権限（Permissions）] には、作成したポータル許可プロファイルを選択します。

デバイス ポータルのカスタマイズ

ポータルの外観およびユーザ（必要に応じてゲスト、スポンサー、または従業員）エクスペリエンスをカスタマイズするには、ポータル テーマをカスタマイズし、ポータル ページの UI 要素を変更して、ユーザに表示されるエラー メッセージと通知を編集します。ポータルのカスタマイズの詳細については、エンドユーザ Web ポータルのカスタマイズ （483 ページ）を参照してください。

従業員が追加するパーソナル デバイスの管理

従業員が個人所有デバイスの持ち込み（BYOD）またはデバイス ポータルを使用してデバイスを登録すると、デバイスはエンドポイント リストに表示されます。従業員はデバイスを削除して自分のアカウントからデバイスを切り離すことができますが、デバイスは Cisco ISE データベースに残ります。この結果、従業員は、デバイスの使用時に発生するエラーの解決に管理者の支援を必要とする場合があります。

従業員が追加したデバイスの表示

[エンドポイント（Endpoints）] リスト ページに表示される [ポータル ユーザ（Portal User）] フィールドを使用して、特定の従業員が追加したデバイスを特定できます。これは、特定のユーザが登録したデバイスを削除する必要がある場合に役立つことがあります。デフォルトでは、このフィールドは表示されないため、検索する前に最初に有効にする必要があります。

ステップ 1 **[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

ステップ 2 [設定（Settings）] アイコンをクリックし、[カラム（Columns）] を選択します。

ステップ 3 [ポータル ユーザ（Portal User）] を選択して、[エンドポイント（Endpoints）] リストに情報を表示します。

ステップ 4 [表示（Show）] ドロップダウン リストをクリックし、[クイック フィルタ（Quick Filter）] を選択します。

ステップ 5 [ポータル ユーザ（Portal User）] フィールドにユーザの名前を入力して、その特定のユーザに割り当てられたエンドポイントのみを表示します。

デバイスをデバイス ポータルに追加するときのエラー

従業員は、別の従業員がすでに追加したサービスを追加することはできません。デバイスは引き続きエンドポイント データベースに含まれます。

Cisco ISE データベースにすでに存在しているデバイスを従業員が追加しようとした場合：

- さらに、デバイスがネイティブサプリカントプロビジョニングをサポートしている場合、BYODポータルからデバイスを追加することを推奨します。この場合、デバイスがネットワークに最初に追加されたときに作成された登録詳細がすべて上書きされます。
- デバイスがプリンタなどのMAC認証バイパス（MAB）デバイスである場合、デバイスの所有権を最初に解決する必要があります。必要に応じて、管理者ポータルを使用してエンドポイントデータベースからデバイスを削除できます。これにより、新しい所有者は、デバイス ポータルを使用して正常にデバイスを追加できます。

（注） 管理者ポータルがダウンしている場合、デバイス ポータルは使用できません。

デバイス ポータルから削除されたデバイスはエンドポイント データベースに残っている

従業員がデバイス ポータルからデバイスを削除すると、そのデバイスは従業員の登録済みデバイスのリストから削除されますが、Cisco ISE エンドポイント データベースに残っており、エンドポイント リストに表示されます。

[エンドポイント（Endpoints）] ページからデバイスを完全に削除するには、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

従業員が登録するパーソナル デバイス数の制限

従業員が 1 ～ 999 のパーソナル デバイスを登録できるようにすることができます。従業員がパーソナルデバイスの登録に使用したポータルに関係なく、この設定では、すべてのポータルにわたって登録されるデバイスの最大数を定義します。

ステップ 1 **[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）]** を選択します。

ステップ 2 [従業員を制限（Restrict employees to）] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は 5 デバイスに設定されています。

ステップ 3 [保存（Save）] をクリックします。設定の更新を保存しない場合は、[リセット（Reset）] をクリックして、最後に保存した値に戻します。

デバイスポータルおよびエンドポイントアクティビティのモニタ

Cisco ISE は、エンドポイントおよびユーザ管理情報、およびゲストとスポンサーのアクティビティを参照できるさまざまなレポートとログを提供します。Cisco ISE 1.2 レポートの一部は廃止されましたが、情報は他のレポートで表示できます。

オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 **[操作（Operations）] > [レポート（Reports）]** を選択します。

ステップ 2 レポート セレクタで、[ゲスト アクセス レポート（Guest Access Reports）] および [エンドポイントとユーザ（Endpoints and Users）] 選択を展開し、さまざまなゲスト、スポンサー、およびエンドポイントに関するレポートを表示します。

ステップ 3 レポートを選択し、[フィルタ（Filters）] ドロップダウン リストを使用して、検索するデータを選択します。

ユーザ名、ポータル名、デバイス名、エンドポイント ID グループ、および他のデータについてフィルタを使用できます。

ステップ 4 データを表示する [時間範囲（Time Range）] を選択します。

ステップ 5 [実行（Run）] をクリックします。

デバイス ログインおよび監査レポート

デバイス ログインおよび監査レポートは、次のものを追跡する統合レポートです。

- デバイス ポータルでの従業員によるログイン アクティビティ。
- デバイス ポータルで従業員が実行したデバイス関連の操作。

このレポートは、**[操作（Operations）] > [レポート（Reports）] > [ゲスト アクセス レポート（Guest Access Reports）] > [デバイス ログインおよび監査レポート（My Devices Login and Audit）]** で使用できます。

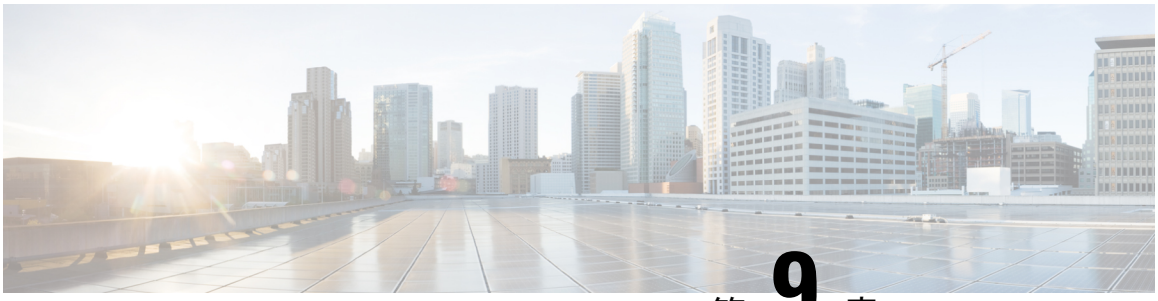
登録済みエンドポイント レポート

[登録済みエンドポイント レポート（Registered Endpoints report）] には、従業員によって登録されたすべてのエンドポイントに関する情報が表示されます。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザ（Endpoints and Users）] > [登録済みエンドポイント（Registered Endpoints）]** で使用できます。ID、エンドポイント ID、アイデンティティ プロファイルなどに対してクエリーを実行し、レポートを生成できます。サ

プリカント プロビジョニング統計情報および関連データの詳細については、クライアント プロビジョニング レポートの表示に関する説明を参照してください。

エンドポイントデータベースに対するクエリーを実行して、RegisteredDevices エンドポイント ID グループに割り当て済みのエンドポイントの情報を取得することができます。また、[ポータルユーザ（Portal User）] 属性がヌル以外の値に設定されている特定のユーザについてレポートを生成することもできます。

[登録済みエンドポイント レポート（Registered Endpoints Report）] には、特定のユーザによって指定の期間内にデバイス登録ポータルから登録されたエンドポイントのリストに関する情報が表示されます。



第 9 章

安全な有線アクセス

Cisco ISE でのネットワークデバイスの定義

スイッチやルータなどのネットワーク デバイスは、認証、許可、アカウンティング（AAA）クライアントであり、これを使用して、AAA サービス要求が Cisco ISE に送信されます。Cisco ISE がネットワーク デバイスとやり取りするように、ネットワーク デバイスを定義する必要があります。ネットワーク デバイスを RADIUS または TACACS AAA に設定したり、プロファイリング サービスでプロファイリング エンドポイントの Cisco Discovery Protocol 属性および Link Layer Discovery Protocol 属性を収集するための Simple Network Management Protocol（SNMP）を設定したり、TrustSec デバイスの TrustSec 属性を設定することができます。Cisco ISE に定義されていないネットワーク デバイスは、Cisco ISE から AAA サービスを受信できません。

ネットワーク デバイスの定義：

- ネットワーク デバイスに応じたベンダー プロファイルを選択できます。プロファイルには、URL ダイレクトや許可変更の設定などの、デバイスに事前定義された設定が含まれています。
- RADIUS 認証用の RADIUS プロトコルを設定できます。Cisco ISE はネットワーク デバイスから RADIUS 要求を受信すると、対応するデバイス定義を探して設定されている共有秘密を取得します。デバイス定義が見つかった場合、デバイスに設定されている共有秘密を取得し、それを要求内の共有秘密と照合してアクセスを認証します。共有秘密が一致すると、RADIUS サーバは、さらにポリシーと設定に基づいて要求を処理します。一致しない場合は、拒否応答がネットワーク デバイスに送信されます。失敗した認証レポートが生成され、失敗の理由が示されます。

- TACACS+ 認証用の TACACS+ プロトコルを設定できます。Cisco ISE はネットワーク デバイスから TACACS+ 要求を受信すると、対応するデバイス定義を探して設定されている共有秘密を取得します。デバイス定義が見つかった場合、デバイスに設定されている共有秘密を取得し、それを要求内の共有秘密と照合してアクセスを認証します。共有秘密が一致すると、TACACS+ サーバは、さらにポリシーと設定に基づいて要求を処理します。一致しない場合は、拒否応答がネットワーク デバイスに送信されます。失敗した認証レポートが生成され、失敗の理由が示されます。
- プロファイリング サービスがネットワーク デバイスと通信し、ネットワーク デバイスに接続されているエンドポイントをプロファイリングするように、ネットワーク デバイス定義で簡易ネットワーク管理プロトコル（SNMP）を設定できます。
- Cisco TrustSec ソリューションの一部となる可能性がある TrustSec 対応デバイスからの要求を処理するには、Cisco ISE に TrustSec 対応デバイスを定義する必要があります。TrustSec ソリューションをサポートするスイッチはすべて TrustSec 対応デバイスです。

  TrustSec デバイスでは IP アドレスは使用されません。代わりに、TrustSec デバイスが Cisco ISE と通信できるように、その他の設定を定義する必要があります。

  TrustSec 対応デバイスは Cisco ISE との通信に TrustSec 属性を使用します。Nexus 7000 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、Catalyst 4000 シリーズ スイッチ、Catalyst 3000 シリーズ スイッチなどの TrustSec 対応デバイスは、TrustSec デバイスの追加時に定義した TrustSec 属性を使用して認証されます。

（注） Cisco ISE でネットワーク デバイスを設定する際には、共有秘密にバックスラッシュ（\）を含めないことをお勧めします。これは、Cisco ISE をアップグレードすると、共有秘密にバックスラッシュが表示されなくなるためです。ただし、Cisco ISE をアップグレードせずに再イメージ化すると、共有秘密にバックスラッシュが表示されます。

Cisco ISE でのデフォルト ネットワーク デバイスの定義

Cisco ISE では、RADIUS および TACACS 認証のデフォルトのデバイス定義がサポートされています。特定の IP アドレスのデバイス定義が見つからない場合、Cisco ISE で使用できるデフォルトのネットワーク デバイスを定義することができます。この機能を使用すると、新しくプロビジョニングされたデバイスのデフォルトの RADIUS または TACACS 共有秘密とアクセス レベルを定義できます。

（注） 基本的な RADIUS および TACACS 認証のみにデフォルトのデバイス定義を追加することを推奨します。高度なフローについては、ネットワーク デバイスごとに個別のデバイス定義を追加する必要があります。

Cisco ISE は、ネットワーク デバイスから RADIUS または TACACS 要求を受信すると、対応するデバイス定義を検索して、ネットワーク デバイス定義に設定されている共有秘密を取得します。

RADIUS または TACACS 要求が受信されると、Cisco ISE は次の手順を実行します。

1. 要求内の IP アドレスに一致する特定の IP アドレスを探します。
2. 範囲を調べて、要求内の IP アドレスが指定された範囲内にあるかどうかを確認します。
3. ステップ 1 と 2 の両方が失敗すると、要求の処理にデフォルトのデバイス定義（定義されている場合）が使用されます。

Cisco ISE は、そのデバイスのデバイス定義に設定されている共有秘密を取得し、それを RADIUS または TACACS 要求内の共有秘密と照合してアクセスを認証します。デバイス定義が見つからない場合、Cisco ISE はデフォルトのネットワーク デバイス定義から共有秘密を取得し、RADIUS または TACACS 要求を処理します。

Cisco ISE でのネットワークデバイスの追加

Cisco ISE でネットワークデバイスを追加したり、デフォルトのネットワークデバイスを使用したりできます。

また、**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** ページで、ネットワーク デバイスを作成することもできます。

始める前に

ネットワークデバイスで AAA 機能が有効になっていることを確認します。詳細については、を参照してくださいAAA 機能を有効にするコマンド （1518 ページ）

ステップ 1 **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ネットワークデバイスの [名前（Name）] を入力します。

ステップ 4 （注） IPv4 および IPv6 は、ネットワーク デバイス（TACACS および RADIUS）設定および外部 RADIUS サーバ設定でサポートされるようになりました。IPv4 アドレスを入力する場合は、範囲とサブネット マスクを使用できます。IPv6 では、範囲がサポートされていません。

IP アドレスを入力します。

ステップ 5 （任意）[RADIUS 認証設定（RADIUS Authentication Settings）] チェックボックスをオンにして、RADIUS プロトコル認証を設定します。

ステップ 6 （任意）[TACACS 認証設定（TACACS Authentication Settings）] チェックボックスをオンにして、TACACS プロトコル認証を設定します。

ステップ 7 （任意）[SNMP の設定（SNMP Settings）] チェックボックスをオンにして、デバイス情報を収集するプロファイリング サービスの簡易ネットワーク管理プロトコルを設定します。

ステップ 8 （任意）TrustSec 対応デバイスを設定するには [高度なTrustSec設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 9 [送信（Submit）] をクリックします。

Cisco ISE へのネットワーク デバイスのインポート

カンマ区切り形式（CSV）ファイルを使用して、Cisco ISE ノードにデバイス定義のリストをインポートできます。Cisco ISE にネットワーク デバイスをインポートする前に、インポートしたテンプレートを更新する必要があります。同じリソース タイプのインポートを同時に実行できません。たとえば、2 つの異なるインポート ファイルから同時にネットワーク デバイスをインポートできません。

管理者ポータルから CSV テンプレートをダウンロードし、テンプレートにデバイス定義の詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

デバイスのインポート中に、新しいレコードを作成するか、または既存のレコードを更新できます。インポートされたデバイスの数の概要が表示され、インポート プロセス中に見つかったエラーが報告されます。デバイスをインポートする場合、Cisco ISE で最初のエラーが発生した場合、既存のデバイス定義を新しい定義で上書きするか、またはインポート プロセスを停止するかを定義できます。

リリース間でインポート テンプレートが異なるため、Cisco ISE の以前のリリースでエクスポートされたネットワーク デバイスをインポートすることはできません。

（注） すべてのオクテットで IP 範囲を持つネットワーク デバイスをインポートできます。

（注） IPv4 および IPv6 は、ネットワーク デバイス（TACACS および RADIUS）設定および外部 RADIUS サーバ設定でサポートされるようになりました。IPv4 アドレスを入力する場合は、範囲とサブネット マスクを使用できます。IPv6 では、範囲がサポートされていません。

ステップ 1 **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [新しいデータで既存のデータを上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。

ステップ 5 [最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 6 [インポート（Import）] をクリックします。

Cisco ISE からのネットワーク デバイスのエクスポート

Cisco ISE で設定されたネットワーク デバイスを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのネットワーク デバイスをインポートできます。

（注） すべてのオクテットで IP 範囲を持つネットワーク デバイスをエクスポートできます。

ステップ 1 **[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [エクスポート（Export）] をクリックします。

ステップ 3 ネットワーク デバイスをエクスポートするには、次のいずれかを行うことができます。

- エクスポートするデバイスの隣にあるチェックボックスをオンにし、**[エクスポート（Export）]** > **[選択済みをエクスポート（Export Selected）]** を選択します。
- 定義されているすべてのネットワーク デバイスをエクスポートするには、**[エクスポート（Export）]**> **[すべてエクスポート（Export All）]** を選択します。

ステップ 4 ローカル ハード ディスクに export.csv ファイルを保存します。

ネットワーク デバイス設定の問題のトラブルシューティング

ステップ 1 **[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般ツール（General Tools）]** > **[設定バリデータの評価（Evaluate Configuration Validator）]** を選択します。

ステップ 2 設定を評価するデバイスのネットワーク デバイス IP アドレスを入力し、必要に応じて他のフィールドを指定します。

ステップ 3 推奨テンプレートと比較する設定オプションを選択します。

ステップ 4 [実行（Run）] をクリックします。

ステップ 5 [ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更します。

ステップ 6 分析するインターフェイスの隣のチェックボックスをオンにして、[送信（Submit）] をクリックします。

ステップ 7 [結果概要の表示（Show Results Summary）] をクリックします。

Execute Network Device Command 診断ツール

Execute Network Device Command 診断ツールを使用すると、ネットワーク デバイスに対して **show** コマンドを実行することができます。結果は、コンソールに表示される場合とまったく同じ形式であり、デバイスの設定における問題を特定するために使用できます。設定が間違っていると思われる場合や、設定を検証したい場合、または単にどのように設定されているか関心がある場合に、使用することができます。

Cisco ISE でのサードパーティ ネットワーク デバイスのサポート

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、サードパーティ製ネットワーク アクセス デバイス（NAD）をサポートします。NAD プロファイルは、ベンダー側の導入に関係なく、シンプルなポリシー設定でサードパーティ デバイスの機能を定義します。ネットワーク デバイス プロファイルには、次のものが含まれています。

- RADIUS、TACACS+、TrustSec などの、ネットワーク デバイスがサポートするプロトコル。デバイスに存在するベンダー固有の RADIUS ディクショナリを Cisco ISE にインポートできます。
- デバイスが有線 MAB、802.1x などのさまざまなフローに使用する属性および値。これを使用して、Cisco ISE は使用される属性に従ってデバイスに適切なフロー タイプを検出できます。
- デバイスが持つ認可変更（CoA）機能。RFC 5176 では CoA 要求のタイプが定義されますが、要求に必要な属性はデバイスによって異なります。RFC 5176 サポート付きのほとんどのシスコ以外のデバイスは、「プッシュ」および「切断」機能もサポートします。RADIUS CoA タイプをサポートしていないデバイスについては、ISE も SNMP CoA をサポートします。CoA タイプの詳細については、以降に説明します。
- デバイスが MAB に使用する属性およびプロトコル。さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。
- デバイスで使用される VLAN および ACL の権限。プロファイルを保存すると、Cisco ISE は設定された各権限に対し許可プロファイルを自動的に生成します。
- URL リダイレクションは、BYOD、ゲスト、ポスチャなどの高度なフローに必要です。デバイス内で見つかる URL リダイレクションには、スタティックとダイナミックの 2 つのタイプがあります。スタティック URL リダイレクションの場合は、ISE ポータル URL をコピーして設定に貼り付けることができます。ダイナミック URL リダイレクションの場合、ISE は RADIUS 属性を使用して、リダイレクト先をネットワーク デバイスに伝えます。また、デバイスがダイナミック URL もスタティック URL もサポートしていない場合には、ISE が URL リダイレクトをシミュレートする認証 VLAN を提供します。認証 VLAN は、ISE ボックスで実行されている DHCP/DNS サービスに基づいています。認証 VLAN を作成するには、DHCP/DNS サービス設定を定義します。詳細については、『』の「DHCP

および DNS サービス」のセクション「DHCP および DNS サービス」を参照してください。URL リダイレクト フローの詳細については、以降に説明します。

ISE でデバイスを定義したら、これらのデバイス プロファイルを設定するか、ISE によって提供された事前設定済みデバイス プロファイルを使用して、Cisco ISE が基本フローや、プロファイラ、ゲスト、BYOD、MAB、ポスチャなどの高度なフローを有効にするために使用する機能を定義します。

URL リダイレクト メカニズムと認証 VLAN

ネットワークでサードパーティ デバイスが使用されていて、デバイスがダイナミックまたはスタティック URL リダイレクトをサポートしていない場合、ISE が URL リダイレクト フローをシミュレートします。このようなデバイスの URL リダイレクト シミュレーション フローは、ISE ボックスで DHCP/DNS サービスを実行することで動作します（詳細については、『』の「DHCP および DNS サービス」のセクション「DHCP および DNS サービス」を参照してください）。認証 VLAN フローは次のとおりです。

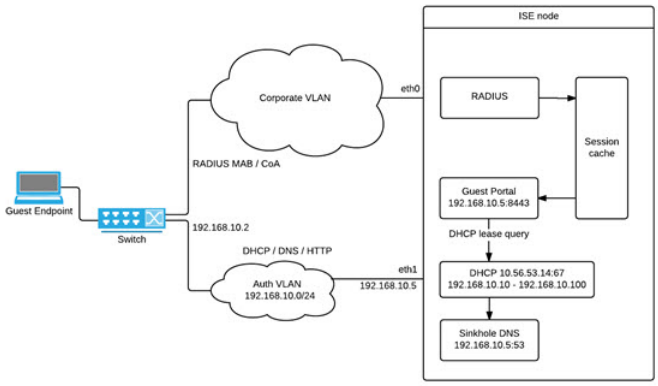
1. ゲスト エンドポイントが NAD に接続します。
2. デバイスが ISE に RADIUS/MAB 要求を送信します。
3. ISE が認証/承認ポリシーを実行し、ユーザ アカウンティング情報を保存します。
4. ISE が認証 VLAN ID を含む RADIUS アクセス/承認メッセージを送信します。
5. ゲスト エンドポイントがネットワーク アクセスを受け取ります。
6. エンドポイントが DHCP 要求を送信し、ISE DHCP サービスからクライアント IP アドレスと ISE シンクホール DNS IP アドレスを取得します。
7. ゲスト エンドポイントがブラウザを開きます。ブラウザが DNS クエリを送信し、ISE IP アドレスを受け取ります。
8. エンドポイント HTTP または HTTPS 要求が ISE ボックスに送られます。
9. ISE は HTTP 301/Moved で応答し、ゲスト ポータル URL を提供します。エンドポイント ブラウザがゲスト ポータル ページにリダイレクトされます。
10. ゲスト エンドポイント ユーザが認証のためにログインします。
11. コンプライアンスの検証が完了すると、ISE は NAD に応答し、CoA の送信、エンドポイントの認証、シンクホールのバイパスを行います。
12. CoA に基づいて適切なアクセスがユーザに提供され、エンドポイントが企業 DHCP から IP アドレスを受信し、ユーザがネットワークを使用できるようになります。

エンドポイントが認証を通過する前にゲスト エンドポイントによって不正なネットワーク アクセスが行われないように、認証 VLAN は社内ネットワークから分離する必要があります。認証 VLAN IP ヘルパーを設定して ISE マシンを示すか、いずれかの ISE ネットワーク インターフェイスを認証 VLAN に接続します。VLAN（DHCP/DNS サーバ）設定の詳細については、『』の「DHCP および DNS サービス」のセクション「DHCP および DNS サービス」を参照し

てください。NAD 設定から VLAN IP ヘルパーを設定することで、複数の VLAN を 1 つのネットワーク インターフェイス カードに接続することができます。IP ヘルパーの設定の詳細については、デバイス用のアドミニストレーションガイドの指示を参照してください。さらに、ゲスト フローについて、通常のゲスト フローと同様にゲスト ポータルを定義して、MAB 認証にバインドされる認証プロファイルでそのポータルを選択します。ゲスト ポータルの詳細については、『』の「Cisco ISE ゲスト サービス」のセクションCisco ISE ゲスト サービス （369 ページ）を参照してください。

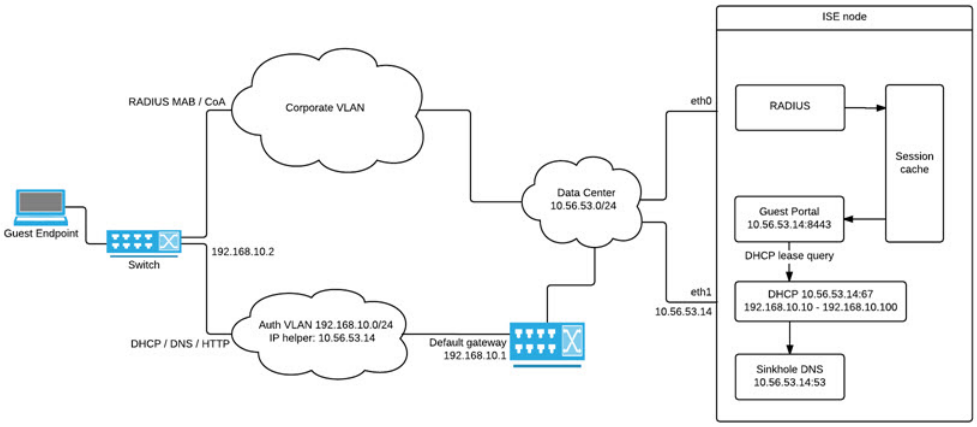
次の図に、認証 VLAN が定義されているときの基本的なネットワーク設定を示します（認証 VLAN が Cisco ISE ノードに直接接続されています）。

図 *40 : Cisco ISE* ノードに接続する認証 *VLAN*



次の図に、認証 VLAN と IP ヘルパーを備えたネットワークを示します。

図 *41 : IP* ヘルパーを備えた認証 *VLAN*



CoA タイプ

ISE は、RADIUS と SNMP の両方の CoA タイプをサポートします。RADIUS または SNMP CoA タイプのサポートは、基本的なフローでは必須ではありませんが、NAD が複雑なフローで機

能するために必要です。ISE から NAD を設定するときにデバイスによってサポートされる RADIUS および SNMP の設定を定義し、NAD プロファイルを設定するときに特定のフローのために使用される CoA タイプを示します。NAD のプロトコルの定義の詳細については、『』の「ネットワーク デバイス」のセクション「ネットワーク デバイス」を参照してください。ISE でデバイスと NAD のプロファイルを作成する前に、NAD でどのタイプがサポートされているかをサードパーティ サプライヤに確認してください。

ネットワーク デバイス プロファイル

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、一部のサードパーティ製ネットワーク アクセス デバイス（NAD）をサポートします。これらのプロファイルによって、基本フローと、ゲスト、BYOD、MAB、ポスチャなどの高度なフローを有効にするために Cisco ISE が使用する機能が定義されます。

Cisco ISE には、いくつかのベンダーからのネットワーク デバイスの定義済みプロファイルが含まれています。Cisco ISE 2.1 は、次の表に記載されているベンダー デバイスでテストされています。

表 *122 : Cisco ISE 2.1* でテスト済みのベンダー デバイス

Device Type	Vendor	CoA タイプ	URL リダイレクト タイプ	サポートされる/検証済みの使用例				
				802.1X/ MAB	CoA のないプロファイラ	CoA があるプロファイラ	ポスチャ（Posture）	ゲスト/BYOD
ワイヤレス	Aruba 7000、InstantAP	RADIUS	スタティック URL	√	√	√	√	√
	Motorola RFS 4000	RADIUS	ダイナミック URL	√	√	√	√	√
	HP 830	RADIUS	スタティック URL	√	√	√	√	√
	Ruckus ZD 1200	RADIUS	—	√	√	√	√	√

有線	HP A5500	RADIUS	ISE が提供する認証 VLAN	√	√	√	√	√
	HP 3800 および 2920 (ProCurve)	RADIUS	ISE が提供する認証 VLAN	√	√	√	√	√
	Alcatel 6850	SNMP	ダイナミック URL	√	√	√	√	√
	Brocade ICX 6610	RADIUS	ISE が提供する認証 VLAN	√	√	√	√	√
	Juniper EX3300-24p	RADIUS	ISE が提供する認証 VLAN	√	√	√	√	√
その他のサードパーティ製 NAD の場合は、デバイスのプロパティおよび機能を識別し、Cisco ISE でカスタム NAD プロファイルを作成する必要があります。				√	√	CoA サポートが必要	CoA サポートが必要です。URL リダイレクトについて、有線デバイスに URL リダイレクトがない場合は、ISE 認証 VLAN を利用します。ワイヤレスデバイスは認証 VLAN でテストされていません。	

定義済みプロファイルがないその他のサードパーティ製ネットワーク デバイス用のカスタム NAD プロファイルを作成できます。ゲスト、BYOD、ポスチャなどの高度なフローについては、デバイスは、RFC 5176、「許可変更（CoA）」をサポートしている必要があります。これらのフローに対するサポートは、NAD の機能によって異なります。ネットワーク デバイス プロファイルに必要な多くの属性については、デバイスの管理ガイドを参照する必要があります。

リリース 2.0 以前のシスコ以外の NAD を展開し、それらを使用するようにポリシー ルール/RADIUS ディクショナリを作成した場合、これらはアップグレード後に通常どおりに機能し続けます。

ISE Community Resource

サードパーティ製 NAD プロファイルについては、「ISE Third-Party NAD Profiles and Configs」を参照してください。

Cisco ISE でのサードパーティ製ネットワーク デバイスの設定

Cisco ISE は、ネットワーク デバイス プロファイルを使用して、サードパーティ製ネットワーク アクセス デバイス（NAD）をサポートします。これらのプロファイルによって、ゲスト、BYOD、MAB、ポスチャなどのフローを有効にするために Cisco ISE が使用する機能が定義されます。

始める前に

『Cisco Identity Services Engine 管理者ガイド』のネットワーク デバイス プロファイル （913 ページ）の定義を確認してください。

ステップ 1 デバイスが ISE で設定されていることを確認します。ゲスト、BYOD またはポスチャのワークフローを設定している場合、認可変更（CoA）が定義され、NAD の URL リダイレクト機能が、関連する ISE ポータルをポイントするように設定されていることを確認します。URL リダイレクトの場合は、ポータルのランディング ページから ISE ポータルの URL をコピーできます。ISE の NAD の CoA タイプおよび URL リダイレクトの設定に関する詳細については、『』の「ネットワークデバイス」のセクションネットワークデバイス（1429ページ）を参照してください。さらに、手順については、サードパーティデバイスの管理ガイドを参照してください。

ステップ 2 デバイスに適切な NAD プロファイルが ISE で利用できることを確認します。既存のプロファイルを表示するには、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス プロファイル（Network Device Profiles）]** を選択します。適切なプロファイルが ISE に存在しない場合は、カスタムプロファイルを作成します。カスタムプロファイルの作成方法の詳細については、ネットワーク デバイス プロファイルの作成 （916 ページ）を参照してください。

ステップ 3 設定する NAD に NAD プロファイルを割り当てます。**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]** を選択します。プロファイルを割り当てるデバイスを開き、[デバイス プロファイル（Device Profile）] ドロップダウン リストから適切なプロファイルを選択します。

ステップ 4 ポリシー ルールを設定する場合は、許可プロファイルをステップ 1 で NAD プロファイルに明示的に設定する必要があります。または、VLAN または ACL を使用するだけの場合、あるいはネットワークに異なるベンダーからのさまざまなデバイスがある場合は、[いずれか（Any）]に設定します。許可プロファイルの NAD プロファイルを設定するには、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [許可プロファイル（Authorization Profiles）]** を選択します。関連する認可プロファイルを開き、[ネットワーク デバイス プロファイル（Network Device Profiles）] ドロップダウン リストから関連する NAD プロファイルを選択します。ゲスト フロー用に認証 VLAN を使用する場合、通常のゲスト フローと同様に、ゲスト ポータルを定義し、MAB 認証にバインドされた認証プロファイルでそのポータルを選択する必要があります。ゲスト ポータルの詳細については、『』の「Cisco ISE ゲスト サービス」のセクションCisco ISE ゲスト サービス （369 ページ）を参照してください。を参照してください。

ネットワーク デバイス プロファイルの作成

始める前に

- カスタム プロファイルの作成方法の詳細については、『Network Access Device Profiles with Cisco Identity Services Engine』ドキュメントを確認してください。
- ほとんどの NAD には、標準の IETF RADIUS 属性に加えて多数のベンダー固有の属性を提供する、ベンダー固有の RADIUS ディクショナリがあります。ネットワーク デバイスにベンダー固有の RADIUS ディクショナリがある場合は、それを Cisco ISE にインポートします。RADIUS ディクショナリが必要な手順については、サードパーティ製デバイスの管理ガイドを参照してください。ISE から、**[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[システム（System）]** > **[RADIUS]** > **[RADIUS ベンダー（RADIUS Vendors）]** を選択します。RADIUS ディクショナリのインポートの詳細については、『』の「RADIUS ベンダー ディクショナリの作成」のセクションRADIUS ベンダー ディクショナリの作成 （1027 ページ）を参照してください。
- ゲストやポスチャなどの複雑なフローの場合、デバイスは RFC 5176、許可変更（CoA）をサポートしている必要があります。
- ネットワーク デバイスのプロファイルを作成するためのフィールドと値の詳細については、『』の「ネットワーク デバイス プロファイルの設定」のセクション「ネットワーク デバイス プロファイル設定」を参照してください。

ステップ 1 **[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイスプロファイル（Network Device Profiles）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ネットワーク デバイスの名前と説明を入力します。

ステップ 4 ネットワーク デバイスのベンダーを選択します。

ステップ 5 デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスが RADIUS、TACACS+、TrustSec をサポートする場合には、各ボックスにマークを付けます。実際に使用するプロトコルにのみマークを付ける必要があります。デバイスが RADIUS をサポートしている場合は、[RADIUS ディクショナリ（RADIUS Dictionaries）] フィールドのダイナミック ドロップダウン リストからネットワーク デバイスで使用する RADIUS ディクショナリを選択します。

ステップ 6 [テンプレート（Templates）] セクションから次のように関連情報を入力します。

a) [認証/許可（Authentication/Authorization）] から、フローのタイプ、属性エイリアシングおよびホスト ルックアップに対するデバイスのデフォルト設定を設定します。[フロータイプの条件（Flow Type Conditions）] には、デバイスが有線 MAB または 802.1x などのさまざまなフローに使用する、属性と値を入力してください。これにより、Cisco ISE は使用される属性に従ってデバイスに適切なフロー タイプを検出できます。MAB 用の IETF 標準がないため、ベンダーごとに異なる値が Service-Type に使用されています。正しい設定を判断するには、デバイスのユーザ ガイドを参照するか、または MAB 認証のスニファ トレースを使用してください。[属性エイリアシング（Attribute Aliasing）] から、デバイス固有の属性名を共通名にマップして、ポリシー ルールを簡素化することができます。現在は、SSID のみが定義されています。デバイスにワイヤレス SSID の概念がある場合には、使用される属性に対し

てこれを設定します。ISE は、これを正規化された RADIUS ディクショナリの SSID という属性にマッピングします。これは、1 つのルールの SSID を参照でき、基盤となる属性が異なっていても複数のデバイスで動作するので、ポリシールールの設定を簡素化します。[ホストルックアップ（Host Lookup）] から、[ホストルックアップの処理（Process Host Lookup）] オプションを有効にして、サードパーティの指示に基づいて、デバイスに関連する MAB プロトコルと属性を選択します。

b) [権限（Permissions）] から、VLAN および ACL に関するネットワーク デバイスのデフォルト設定を行います。これらは自動的に、ISE で作成した認可プロファイルに基づいてマッピングされます。

c) [許可変更（CoA）（Change of Authorization（CoA））] から、デバイスの CoA 機能を設定します。

d) [リダイレクト（Redirect）] セクションを展開し、デバイスの URL リダイレクト機能を設定します。URL リダイレクションは、ゲスト、BYOD およびポスチャに必要です。

ステップ 7 [送信（Submit）] をクリックします。

Cisco ISE からのネットワーク デバイス プロファイルのエクスポート

XML ファイルを編集してから、そのファイルを新しいネットワーク プロファイルとしてインポートするために、Cisco ISE で設定された単一または複数のネットワーク デバイス プロファイルを XML 形式でエクスポートします。

始める前に

『Network Access Device Profiles with Cisco Identity Services Engine』のドキュメントを参照してください。

ステップ 1 **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス プロファイル（Network Device Profiles）]** を選択します。

ステップ 2 [エクスポート（Export）] をクリックします。

ステップ 3 エクスポートするデバイスの隣にあるチェックボックスをオンにし、**[エクスポート（Export）] > [選択済みをエクスポート（Export Selected）]** を選択します。

ステップ 4 DeviceProfiles.xml ファイルがローカル ハード ディスクにダウンロードされます。

Cisco ISE へのネットワーク デバイス プロファイルのインポート

Cisco ISE XML 構造を備えた単一の XML ファイルを使用して、ISE に単一または複数のネットワーク デバイス プロファイルをインポートできます。複数のインポート ファイルから同時にネットワーク デバイス プロファイルをインポートすることはできません。

通常は、まずテンプレートとして使用するために管理者ポータルから既存のプロファイルをエクスポートします。必要に応じてデバイスプロファイルの詳細をファイルに入力し、XML ファイルとして保存してから、編集したファイルを Cisco ISE に再度インポートします。複数のプロファイルを扱うには、単一の XML ファイルとして一緒に構造化された複数のプロファイル

をエクスポートし、ファイルを編集してから一緒にインポートして、ISE で複数のファイルを作成します。

デバイスプロファイルのインポート中は、新しいレコードの作成のみができます。既存のプロファイルは上書きできません。既存のプロファイルを編集してから上書きするには、既存のプロファイルをエクスポートし、ISE からそのプロファイルを削除してから、適切に編集した後にそのプロファイルをインポートします。

始める前に

『Network Access Device Profiles with Cisco Identity Services Engine』のドキュメントを参照してください。

ステップ 1 **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス プロファイル（Network Device Profiles）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから XML ファイルを選択します。

ステップ 4 [インポート（Import）] をクリックします。

ネットワークデバイスグループ（NetworkDeviceGroups）

Cisco ISE では、階層型ネットワーク デバイス グループ（NDG）を作成できます。NDG は、地理的な場所、デバイス タイプ、ネットワーク内での相対的な位置（アクセス レイヤ、データ センターなど）のようなさまざまな基準に基づいて、ネットワーク デバイスを論理的にグループ化するために使用できます。たとえば、地理的な場所に基づいてネットワーク デバイスを編成するには、大陸、地域、または国でグループ化できます。

- アフリカ -> 南部 -> ナミビア
- アフリカ -> 南部 -> 南アフリカ
- アフリカ -> 南部 -> ボツワナ

デバイス タイプに基づいてネットワーク デバイスをグループ化することもできます。

- アフリカ -> 南部 -> ボツワナ -> ファイアウォール
- アフリカ -> 南部 -> ボツワナ -> ルータ
- アフリカ -> 南部 -> ボツワナ -> スイッチ

ネットワーク デバイスは、1 つ以上の階層型 NDG に割り当てることができます。したがって、Cisco ISE が、設定された NDG の順序リスト全体を参照して特定のデバイスに割り当てる適切

なグループを決定するとき、同じデバイス プロファイルが複数のデバイス グループに適用されている場合、Cisco ISE は最初に一致したデバイス グループを適用します。

作成できる NDG の最大数に制限はありません。NDG の階層レベル（親グループを含む）は最大 6 レベルまで作成できます。

ツリー ビューやフラット テーブル ビューでデバイス グループ階層を表示できます。ツリー ビューで、ルート ノードはツリーの最上位に表示され、子グループが階層順序で次に続きます。各ルート グループに属するすべてのデバイスを表示するには、[すべて展開（Expand All）] をクリックします。ルート グループだけを表示するには、[すべて折りたたむ（Collapse All）] をクリックします。

フラット テーブル ビューでは、各デバイス グループの階層が [グループ階層（Group Hierarchy）] 列に表示されます。

また、各子グループに割り当てられたネットワーク デバイスの数を確認できます。そのデバイス グループに割り当てられているすべてのネットワーク デバイスを一覧表示する、[ネットワーク デバイス（Network Devices）] ウィンドウを起動するには、この番号付きリンクをクリックしてください。デバイス グループに追加デバイスを追加したり、別のデバイス グループに既存のデバイスを移動できます。

デバイス グループを追加するときに、新しいグループをルート グループとして追加するか、親グループとして既存のグループを選択する必要があるかどうかを指定できます。

（注） デバイスが割り当てられているデバイス グループは削除できません。デバイス グループを削除する前に、すべての既存のデバイスを別のデバイス グループに移動する必要があります。

ルート ネットワーク デバイス グループ

Cisco ISE には、すべてのデバイス タイプとすべてのロケーションという 2 つの定義済みルート NDG が含まれます。これらの事前定義された NDG を編集、複製、または削除することはできませんが、それらの下に新しいデバイス グループを追加できます。

ルート ネットワーク デバイス グループ（NDG）を作成し、[ネットワーク デバイス グループ（Network Device Groups）] ページでそのルート グループの下に子 NDG を作成できます。

ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性

新しいネットワーク デバイス グループを作成すると、新しいネットワーク デバイス属性がシステムに定義されているデバイス ディクショナリに追加され、ポリシー定義に使用できるようになります。Cisco ISE では、デバイス タイプ、ロケーション、モデル名、およびネットワーク デバイス上で実行しているソフトウェア バージョンなどのデバイス ディクショナリ属性に基づいて認証ポリシーと許可ポリシーを設定できます。

Cisco ISE へのネットワーク デバイス グループのインポート

カンマ区切り形式（CSV）ファイルを使用して Cisco ISE ノードにネットワーク デバイス グループをインポートできます。同じリソース タイプのインポートを同時に実行できません。たとえば、2 つの異なるインポート ファイルから同時にネットワーク デバイス グループをインポートできません。

管理者ポータルから CSV テンプレートをダウンロードし、テンプレートにデバイス グループの詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

デバイス グループのインポート中に、新しいレコードを作成するか、または既存のレコードを更新できます。デバイス グループをインポートする場合、Cisco ISE で最初のエラーが発生した場合、既存のデバイス グループを新しいグループで上書きするか、またはインポート プロセスを停止するかを定義できます。

ステップ 1 **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] > [グループ（Groups）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [新しいデータで既存のデータを上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。

ステップ 5 [最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 6 [ネットワーク デバイス グループ（Network Device Groups）] リスト ページに戻るには、[インポート（Import）] または [ネットワーク デバイス グループ リスト（Network Device Groups List）] リンクをクリックします。

Cisco ISE からのネットワーク デバイス グループのエクスポート

Cisco ISE に設定されたネットワーク デバイス グループを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのネットワーク デバイス グループをインポートできます。

ステップ 1 **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] > [グループ（Groups）]** を選択します。

ステップ 2 ネットワーク デバイス グループをエクスポートするには、次のいずれかを行うことができます。

- エクスポートするデバイス グループの横にあるチェックボックスをオンにし、**[エクスポート（Export）] > [選択済みをエクスポート（Export Selected）]** を選択します。
- **[エクスポート（Export）] > [すべてエクスポート（Export All）]** を選択して、定義されたネットワーク デバイス グループをすべてエクスポートします。

ステップ 3 ローカル ハード ディスクに export.csv ファイルを保存します。

ネットワーク デバイス グループ（Network Device Groups）

これらのページを使用すると、ネットワーク デバイス グループを設定し、管理することができます。

ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用できる [ネットワーク デバイス グループ（Network Device Groups）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[グループ（Groups）]** です。

[ワークセンター（Work Centers）] > **[デバイス管理（Device Administration）]** > **[ネットワークデバイスグループ（Network Device Groups）]** > **[グループ（Groups）]** ページでネットワーク デバイス グループを作成することもできます。

表 *123* : ネットワーク デバイス グループの設定

フィールド	使用上のガイドライン
名前（Name）	ルート ネットワーク デバイス グループ（NDG）の名前を入力します。ルート NDG の下の後続のすべての子ネットワーク デバイス グループに対して、新しいネットワーク デバイス グループの名前を入力します。 ルート ノードを含み、最大で 6 つのノードを NDG 階層に含めることができます。各 NDG 名は最大 32 文字です。
説明	ルートまたは子のネットワーク デバイス グループの説明を入力します。
親グループ（Parent Group）	親グループとして既存のグループを選択するか、ルートグループとして、この新しいグループを追加できます。

関連トピック

ネットワーク デバイス グループ（Network Device Groups） （918 ページ）
ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性 （919 ページ）
Cisco ISE でのネットワークデバイスの追加 （231 ページ）

ネットワーク デバイス グループのインポート設定

次の表では、Cisco ISE にネットワーク デバイス グループをインポートするために使用できる [ネットワーク デバイス グループ インポート（Network Device Group Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[グループ（Groups）]** です。

表 *124 :* ネットワーク デバイス グループのインポート設定

フィールド	使用上のガイドライン
テンプレートの生成（Generate a Template）	カンマ区切り形式（.csv）テンプレート ファイルを作成するには、このリンクをクリックします。 同じ形式のネットワーク デバイス グループ情報でテンプレートを更新し、それらのネットワーク デバイス グループを Cisco ISE 展開にインポートするためにローカルで保存します。
ファイル（File）	作成したか、または Cisco ISE 展開から以前にエクスポートしたカンマ区切り形式ファイルの場所を参照するには、[参照（Browse）] をクリックします。 インポートを使用して、新しい、更新されたネットワーク デバイス グループ情報を含むネットワーク デバイス グループを別の Cisco ISE 展開にインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	Cisco ISE で既存のネットワーク デバイス グループをインポート ファイル内のデバイス グループに置き換える場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポート ファイル内の新しいネットワーク デバイス グループがネットワーク デバイス グループ リポジトリに追加されます。重複エントリは無視されます。

フィールド	使用上のガイドライン
最初のエラーでインポートを停止（Stop Import on First Error）	インポート中にエラーが発生すると、Cisco ISE にインポートを中止させる場合、このチェックボックスをオンにしますが、Cisco ISE はエラーのその時点までネットワーク デバイス グループをインポートします。 このチェックボックスがオフで、エラーが発生した場合は、エラーが報告され、Cisco ISE はデバイス グループを引き続きインポートします。

関連トピック

ネットワーク デバイス グループ（Network Device Groups） （918 ページ）
ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性 （919 ページ）
Cisco ISE へのネットワーク デバイス グループのインポート （920 ページ）

Cisco ISE でのテンプレートのインポート

Cisco ISE では、カンマ区切り形式（CSV）ファイルを使用して大量のネットワーク デバイスやネットワーク デバイス グループをインポートできます。テンプレートには、フィールドのフォーマットを定義するヘッダー行が含まれます。ヘッダー行は編集しないでそのまま使用してください。

デフォルトで、[テンプレートの生成（Generate a Template）] リンクを使用して、Microsoft Office Excel アプリケーションに CSV ファイルをダウンロードし、このファイル形式をシステム上にローカルに保存できます。[テンプレートの生成（Generate a Template）] リンクをクリックすると、Cisco ISE サーバは、[template.csv を開く（Opening template.csv）] ダイアログを表示します。このダイアログを使用すると、template.csv ファイルを開いて、その template.csv ファイルにネットワーク デバイスおよびネットワーク デバイス グループに適切な名前を付けて、システム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルはデフォルトで Microsoft Office Excel アプリケーションで開かれます。

ネットワーク デバイスのインポート テンプレート形式

次の表では、テンプレート ヘッダーのフィールドとネットワーク デバイスの CSV ファイルにおけるこれらのフィールドの説明を示します。

表 *125 :* ネットワーク デバイスの *CSV* テンプレートのフィールドと説明

フィールド	説明
Name：文字列（32）	（必須）このフィールドはネットワーク デバイスの名前です。これは、最大32文字の英数字文字列です。
Description:String(256)	このフィールドは、ネットワーク デバイスの任意の説明です。最大 256 文字の文字列。
IP Address:Subnets（a.b.c.d/m|...）	（必須）このフィールドは、ネットワーク デバイスのIPアドレスおよびサブネットマスクです。（パイプ記号「|」で区切って複数の値を指定できます）。 IPv4 および IPv6、ネットワーク デバイス（TACACS および RADIUS）設定および外部 RADIUS サーバ設定でサポートされるようになりました。 （注） IPv4 および IPv6 は、ネットワーク デバイス（TACACS および RADIUS）設定および外部 RADIUS サーバ設定でサポートされるようになりました。IPv4アドレスを入力する場合は、範囲とサブネットマスクを使用できます。IPv6では、範囲がサポートされていません。
Model Name：文字列（32）	（必須）このフィールドはネットワーク デバイスのモデル名です。これは、最大32文字の文字列です。
Software Version：文字列（32）	（必須）このフィールドはネットワーク デバイスのソフトウェアバージョンです。これは、最大 32 文字の文字列です。
Network Device Groups：文字列（100）	（必須）このフィールドは、既存のネットワーク デバイス グループにする必要があります。サブグループを指定できますが、親グループとサブグループの両方をスペースで区切って含める必要があります。最大 100 文字の文字列（たとえば、Location#All Location#US）です。

フィールド	説明
Authentication:Protocol:String(6)	これはオプションのフィールドです。認証に使用するプロトコルです。唯一の有効な値は RADIUS です（大文字と小文字は区別されません）。
Authentication:Shared Secret:String(128)	（認証プロトコルのフィールドの値を入力した場合は必須）このフィールドは、最大 128 文字の文字列です。
EnableKeyWrap：ブール（true|false）	これはオプションのフィールドです。これはネットワーク デバイスでサポートされている場合に限り有効です。有効な値は true または false です。
EncryptionKey：文字列（ascii:16|hexa:32）	（KeyWrapを有効にした場合は必須）セッションの暗号化に使用される暗号キーを示します。 ASCII：16 文字（バイト）の長さ 16 進数：32 文字（バイト）の長さ。
AuthenticationKey：文字列（ascii:20|hexa:40）	（KeyWrap を有効にした場合は必須）。RADIUS メッセージに対するキー付き Hashed Message Authentication Code（HMAC）の計算を示します。 ASCII：20 文字（バイト）の長さ 16 進数：40 文字（バイト）の長さ。
InputFormat：文字列（32）	暗号化と認証キーの入力形式を示します。有効な値は、ASCII または Hexadecimal です。
SNMP:Version：列挙（|2c|3）	これはオプションのフィールドで、プロファイラ サービスによって使用されます。SNMP プロトコルのバージョンです。有効な値は1、2c、または 3 です。
SNMP:RO Community:String(32)	（SNMP バージョンのフィールドの値を入力した場合は必須）SNMP読み取り専用のコミュニティ。これは、最大32 文字の文字列です。
SNMP:RW Community:String(32)	（SNMP バージョンのフィールドの値を入力した場合は必須）SNMP 読み取り書き込みコミュニティ。これは、最大32 文字の文字列です。

フィールド	説明
SNMP:Username:String(32)	これはオプションのフィールドです。これは、最大 32 文字の文字列です。
SNMP:Security Level:Enumeration(Auth|No Auth|Priv)	（SNMP バージョン 3 を選択した場合は必須）有効な値は、Auth、No Auth、または Priv です。
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	（SNMP セキュリティ レベルで Auth または Priv を入力した場合は必須）有効な値は、MD5 または SHA です。
SNMP:Authentication Password:String(32)	（SNMP セキュリティ レベルで Auth を入力した場合は必須）これは、最大 32 文字の文字列です。
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	（SNMP セキュリティ レベルで Priv を入力した場合は必須）有効な値は、DES、AES128、AES192、AES256、または 3DES です。
SNMP:Privacy Password:String(32)	（SNMP セキュリティ レベルで Priv を入力した場合は必須）これは、最大 32 文字の文字列です。
SNMP:Polling Interval:Integer:600-86400 seconds	これはオプションのフィールドで、SNMP ポーリング間隔を設定します。有効な値は 600 ～ 86400 の整数です。
SNMP:Is Link Trap Query:Boolean(true|false)	これはオプションのフィールドで、SNMP リンク トラップを有効または無効にします。有効な値は true または false です。
SNMP:Is MAC Trap Query：ブール（true|false）	これはオプションのフィールドで、SNMP MAC トラップを有効または無効にします。有効な値は true または false です。
SNMP:Originating Policy Services Node：文字列（32）	これはオプションのフィールドです。SNMP データのポーリングに使用される ISE サーバを示します。デフォルトでは自動ですが、別の値を割り当てて設定を上書きできます。
Trustsec:Device Id：文字列（32）	これはオプションのフィールドです。これは、TrustSec デバイス ID で、最大 32 文字の文字列です。

フィールド	説明
Trustsec:Device Password：文字列（256）	（TrustSec デバイス ID を入力した場合は必須）これはTrustSecデバイスのパスワードで、最大 256 文字の文字列です。
Trustsec:Environment Data Download Interval：整数：1-2147040000 秒	これはオプションのフィールドです。これはTrustSec環境データのダウンロード間隔です。有効な値は 1 ～ 24850 の整数です。
Trustsec:Peer Authorization Policy Download Interval：整数：1-2147040000 秒	これはオプションのフィールドです。これはTrustSec のピア許可ポリシーのダウンロード間隔です。有効な値は1～24850の整数です。
Trustsec:Reauthentication Interval：整数：1-2147040000 秒	これはオプションのフィールドです。これはTrustSec の再認証間隔です。有効な値は 1 ～ 24850 の整数です。
Trustsec:SGACL List Download Interval：整数：1-2147040000 秒	これはオプションのフィールドです。また、TrustSec SGACL リストのダウンロード間隔です。有効な値は 1 ～ 24850 の整数です。
Trustsec:Is Other Trustsec Devices Trusted：ブール（true|false）	これはオプションのフィールドです。TrustSecが信頼できるかどうかを示します。有効な値は true または false です。
Trustsec:Notify this device about Trustsec configuration changes：文字列（ENABLE_ALL|DISABLE_ALL）	これはオプションのフィールドです。TrustSecデバイスに対する TrustSec 設定変更を通知します。有効な値は ENABLE_ALL または DISABLE_ALL です
Trustsec:Include this device when deploying Security Group Tag Mapping Updates：ブール（true|false）	これはオプションのフィールドです。これは、SGT に含まれる TrustSec デバイスです。有効な値は true または false です。
Deployment:Execution Mode Username:String(32)	これはオプションのフィールドです。デバイス設定を編集する権限を持っているユーザ名です。これは、最大 32 文字の文字列です。
Deployment:Execution Mode Password:String(32)	これはオプションのフィールドです。デバイスパスワードで、最大32文字の文字列です。
Deployment:Enable Mode Password:String(32)	これはオプションのフィールドです。設定を編集するためのデバイスのイネーブルパスワードで、最大 32 文字の文字列です。

フィールド	説明
Trustsec:PAC issue date：日付	これは、TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行日を表示するフィールドです。
Trustsec:PAC expiration date：日付	これは、TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の有効期限を表示するフィールドです。
Trustsec:PAC issued by：文字列	これは、TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行者（TrustSec管理者）の名前を表示するフィールドです。文字列です。

ネットワーク デバイス グループのインポート テンプレート形式

次の表に、テンプレート ヘッダーのフィールドとネットワーク デバイス グループの CSV ファイルにおけるこれらのフィールドの説明を示します。

表 *126*：ネットワーク デバイス グループの *CSV* テンプレートのフィールドと説明

フィールド	説明
Name：文字列（100）	（必須）このフィールドはネットワーク デバイス グループの名前です。最大 100 文字の文字列です。NDGの完全な名前の長さは、最大100 文字です。たとえば、親グループ Global > Asia の下にサブグループ India を作成している場合、作成する NDG の完全な名前は Global#Asia#India になり、この完全な名前の長さは 100 文字を超えることはできません。NDG の完全な名前の長さが 100 文字を超えた場合、NDG の作成は失敗します。
Description:String(1024)	これは、オプションのネットワーク デバイス グループの説明です。これは、最大1024 文字の文字列です。
Type：文字列（64）	（必須）このフィールドはネットワーク デバイス グループのタイプです。これは、最大64 文字の文字列です。
Is Root：ブール（true|false）	（必須）これは、特定のネットワーク デバイス グループがルート グループかどうかを示すフィールドです。有効な値は true または false です。

Cisco ISE-NAD 通信を保護する IPsec セキュリティ

インターネット プロトコル セキュリテ（IPsec）は、インターネット プロトコルにセキュリティを提供するプロトコルのセットです。AAA プロトコル、RADIUS および TACACS+ は MD5 ハッシュ アルゴリズムを使用します。セキュリティを強化するため、Cisco ISE には IPsec 機能があります。IPsec は、送信者を認証し、送信中のデータ変更を検出し、送信されたデータを暗号化することで通信を保護します。

Cisco ISE は、トンネル モードとトランスポート モードで IPsec をサポートしています。Cisco ISE インターフェイスで IPsec を有効にし、ピアを設定すると、通信を保護するため Cisco ISE と NAD の間に IPsec トンネルが作成されます。

事前共有キーを定義するか、または IPsec 認証に X.509 証明書を使用できます。IPsec は、ギガビット イーサネット 1 ～ 5 のインターフェイスで有効にできます。IPsec は PSN あたり 1 つの Cisco ISE インターフェイスでのみ設定できます。

IPSec は、スマート ライセンスがデフォルトで有効になっているため（e0/2—> eth2）、ギガビット イーサネット 2 で有効にすることはできません。ただし、IPSec を有効にする必要がある場合は、スマート ライセンスに別のインターフェイスを選択する必要があります。

（注） ギガビット イーサネット 0 とボンド 0（ギガビット イーサネット 0 およびギガビット イーサネット 1 インターフェイスがボンディングされている場合）は、Cisco ISE CLI の管理インターフェイスです。ギガビット イーサネット 0 およびボンド 0 では IPsec はサポートされていません。

必要なコンポーネントには次のものがあります。

- Cisco ISE、リリース 2.2 以降
- Cisco IOS ソフトウェア、C5921 ESR（埋め込み型サービス ルータ）ソフトウェア（C5921_I86-UNIVERSALK9-M）：ESR 5921 設定では、デフォルトでトンネル モードとトランスポート モードで IPsec がサポートされています。Diffie-Hellman Group 14 および Group 16 がサポートされています。

（注） C5921 ESR ソフトウェアは Cisco ISE リリース 2.2 以降に付属しています。このソフトウェアを使用可能にするには ESR ライセンスが必要です。ESR ライセンスの情報については、『Cisco 5921 Embedded Services Router Integration Guide』を参照してください。

Cisco ISE での RADIUS IPsec の設定

Cisco ISE で RADIUS IPsec を設定するには、次の操作を行う必要があります。

ステップ 1 Cisco ISE CLI からインターフェイスで IP アドレスを設定します。

ギガビット イーサネット 1 からギガビット イーサネット 5 インターフェイス（ボンド 1 およびボンド 2）では、IPsec がサポートされています。ただし、IPsec は Cisco ISE ノードの 1 つのインターフェイスでのみ設定できます。

ステップ 2 直接接続ネットワーク デバイスを IPsec ネットワーク デバイス グループに追加します。

（注） RADIUS IPsec では、スタティック ルート ゲートウェイがデバイスのインターフェイスに直接接続している必要があります。

a) [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] の順に選択します。
b) [ネットワーク デバイス（Network Devices）] ページで [追加（Add）] をクリックします。
c) 追加するネットワーク デバイスの名前、IP アドレス、サブネットを入力します。
d) [IPSEC] ドロップダウンリストから、[はい（Yes）] を選択します。
e) [RADIUS 認証設定（RADIUS Authentication Settings）] チェックボックスをオンにします。
f) [共有秘密（Shared Secret）] フィールドに、ネットワーク デバイスに設定した共有秘密キーを入力します。
g) [送信（Submit）] をクリックします。

ステップ 3 （オプション。スマート ライセンスでのみ必要）。Cisco Smart Software Manager（CSSM）とのやりとりのために個別の管理インターフェイスを追加します。また、ESR にはスマート ソフトウェア マネージャ サテライトも使用できます。このためには、Cisco ISE CLI から次のコマンドを実行し、対応する管理インターフェイス（ギガビット イーサネット 1 ～ 5（またはボンド 1 または 2）を選択します。

ise/admin# **license esr smart** {*interface*}

このインターフェイスは、Cisco.com に到達してシスコのオンライン ライセンス サーバにアクセスできる必要があります。

ステップ 4 Cisco ISE CLI から直接接続ゲートウェイにネットワーク デバイスを追加します。

ip route ［*destination network*］［*network mask*］**gateway** ［*next-hop address*］

ステップ 5 IPsec に対し Cisco ISE ノードを有効にします。

a) [管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [IPSec] を選択します。

展開内のすべての Cisco ISE ノードがこのページにリストされます。

b) IPsec を有効にする Cisco ISE ノードの横のチェックボックスをオンにして、[有効化（Enable）] オプション ボタンをクリックします。
c) IPsec 通信に使用するインターフェイスを選択します。
d) 次のオプションから、選択されている ISE ノードの認証タイプを選択します。

- [事前共有キー（Pre-shared Key）]：このオプションを選択した場合は、事前共有キーを入力し、ネットワーク デバイスで同じキーを設定する必要があります。事前共有キーには英数字を使用してください。特殊文字はサポートされていません。ネットワーク デバイスで事前共有キーを設定

する方法については、ネットワーク デバイスのマニュアルを参照してください。事前共有キー設定の出力例については、例：Cisco Catalyst 3850 での事前共有キー設定の出力 （939 ページ）を参照してください。

- [X.509 証明書（X.509 Certificates）]：このオプションを選択した場合は、Cisco ISE CLI から ESR シェルに進み、ESR 5921 の X.509 証明書を設定してインストールします。次に、ネットワーク デバイスで IPsec を設定します。この説明については、ESR-5921 での X.509 証明書の設定とインストール （933 ページ）を参照してください。

e) [保存（Save）] をクリックします。

（注） IPsec 設定を直接変更することはできません。IPsec が有効な場合にトンネルまたは認証を変更するには、現在の IPsec トンネルを無効にし、IPsec 設定を変更し、異なる設定で IPsec トンネルを再度有効にします。

（注） IPsec が有効になると、Cisco ISE インターフェイスから IP アドレスが削除され、インターフェイスがシャットダウンします。ユーザが Cisco ISE CLI からログインすると、インターフェイスが表示されますが IP アドレスは表示されず、シャットダウン状態になります。この IP アドレスは ESR-5921 インターフェイスで設定されます。

ステップ 6 **esr** と入力して ESR シェルを開始します。

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE
 (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

（注） FIPS に準拠するため、8 文字以上のシークレット パスワードを設定する必要があります。**Enable secret level 1** コマンドを入力してパスワードを指定します。

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

（注） カスタム RADIUS ポートを GUI から設定する場合（1645、1646、1812、および 1813 以外）、ESR シェルで次の CLI コマンドを入力し、設定した RADIUS ポートを受け入れます。

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

ステップ 7 （オプション：ステップ 3 でスマート ライセンスを有効にしていない場合にのみ必要）。Classic ライセンスまたは Evaluation ライセンス（有効期間 90 日）を Cisco ISE アプライアンスに追加します。

- Cisco ISE CLI から次のコマンドを実行してライセンス ファイルをダウンロードします。

```
ise/admin# license esr classic import esr.lic repository esrrepo
```

Classic ライセンスの詳細については、『Cisco 5921 Embedded Services Router Integration Guide』の「Licensing the Software with Classic Licensing」を参照してください。

ステップ 8 IPsec トンネルと、IPsec トンネル経由での RADIUS 認証を検証します。

a) Cisco ISE にユーザを追加し、ユーザ グループに割り当てます（[管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]）。

b) Cisco ISE と NAD の間で IPsec トンネルが確立されていることを確認します。手順は次のとおりです。

1. **ping** コマンドを使用して、Cisco ISE と NAD の間の接続が確立されているかどうかをテストします。

2. ESR シェルまたは NAD CLI から次のコマンドを実行して、接続がアクティブ状態であるかどうかを確認します。 **show crypto isakmp sa**

```
ise-esr5921#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.30.1    192.168.30.3    QM_IDLE           1001 ACTIVE
```

3. ESR シェルまたは NAD CLI から次のコマンドを実行して、トンネルが確立されているかどうかを確認します。 **show crypto ipsec sa**

```
ise-esr5921#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: radius, local addr 192.168.30.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.30.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.168.30.2/255.255.255.255/0/0)
   current_peer 192.168.30.2 port 500
     PERMIT, flags={}
    #pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
    #pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x393783B6(959939510)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8EA0F6EE(2392913646)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237963/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
```

```
 spi: 0x393783B6(959939510)
   transform: esp-aes esp-sha256-hmac ,
   in use settings ={Tunnel, }
   conn id: 100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius
   sa timing: remaining key lifetime (k/sec): (4237970/2229)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

c) 次のいずれかの方法で RADIUS 認証を検証します。

- ステップ 8（a）で作成したユーザのクレデンシャルを使用してネットワーク デバイスにログインします。RADIUS 認証要求が Cisco ISE ノードに送信されます。[ライブ認証（Live Authentications）] ページで詳細を確認します。
- エンド ホストをネットワーク デバイスに接続し、802.1X 認証を設定します。ステップ 8（a）で作成したユーザのクレデンシャルを使用してエンド ホストにログインします。RADIUS 認証要求が Cisco ISE ノードに送信されます。[ライブ認証（Live Authentications）] ページで詳細を確認します。

ESR-5921 での X.509 証明書の設定とインストール

ESR-5921 で X.509 証明書を設定およびインストールするには、次の手順を実行します。

ステップ 1 **esr** と入力して ESR シェルを開始します。

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE
 (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

（注） FIPS に準拠するため、8 文字以上のシークレット パスワードを設定する必要があります。**Enable secret level 1** コマンドを入力してパスワードを指定します。

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

（注） カスタムRADIUSポートをGUIから設定する場合（1645、1646、1812、および1813以外）、ESRシェルで次の CLI コマンドを入力し、設定した RADIUS ポートを受け入れます。

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

ステップ 2 次のコマンドを使用して RSA キー ペアを生成します。

例：

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

ステップ 3 次のコマンドを使用してトラスト ポイントを作成します。

例：

```
crypto pki trustpoint trustpoint-name

enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=networkdevicename.cisco.com
revocation-check none
rsakeypair rsa2048
```

ステップ 4 次のコマンドを使用して CSR を生成します。

例：

```
crypto pki enroll rsaca-mytrustpoint

Display Certificate Request to terminal? [yes/no]: yes
```

ステップ 5 CSR の出力をテキスト ファイルにコピーし、署名のために外部 CA に送信し、署名された証明書と CA 証明書を取得します。

ステップ 6 次のコマンドを使用して CA をインポートします。

例：

```
crypto pki authenticate rsaca-mytrustpoint
```

CA 証明書の内容（「—BEGIN—」行と「—-End—」行を含む）をコピーして貼り付けます。

ステップ 7 次のコマンドを使用して、署名付き証明書をインポートします。

例：

```
crypto pki import rsaca-mytrustpoint
```

署名付き証明書の内容（「—BEGIN—」行と「—-End—」行を含む）をコピーして貼り付けます。

以下に、Cisco 5921 ESR で X.509 証明書を設定してインストールするときの出力の例を示します。

```
ise-esr5921#show running-config
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
no aaa new-model
```

```
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address
 to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint rsaca-mytrustpoint
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=ise-5921.cisco.com
revocation-check none
rsakeypair rsa2048
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain rsaca-mytrustpoint
certificate 39
```

```
  30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
  61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06
  03550407 0C035254 50310E30 0C060355 040A0C05 43495343 4F310C30 0A060355
  040B0C03 53544F31 19301706 03550403 0C107273 6163612E 65726368 616F2E63
  6F6D301E 170D3136 30393031 32313037 34335A17 0D313730 39303132 31303734
  335A301D 311B3019 06035504 03131269 73652D35 3932312E 63697363 6F2E636F
  6D308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
  0100EE87 CABFBA18 7E0405A8 ACAAAB23 E7CB6109 2CF98BAE 8EE93536 BF1EBBD3
  73E60BE7 F430B5AF EBF8B0C5 969B2828 A6783BB4 64E333E4 29C8744E 6E783617
  194AF1B0 7F04B4EA B89FD6EB F9C4F2DD 196DC6E0 CAA49B8B 665B6E0D 2FBC1D2F
  8E8181B9 60FAE126 D1B2E4E4 1F321A97 10C1B76A C2BB3174 361B13FA 2CB7BDFE
  22C0C33F 2792D714 C41E2237 00B1AE49 6593DCC3 A799D526 D81F9706 A71DA14E
  5ED76038 7A2C84B4 C668E35C 337BA1DC 9CA56AC2 C8E0059F 660CE39C 925310A0
  F9A21FFB 3C3C507A 20B924F7 E0125D60 6552321C 35736079 42449401 15E68DA6
  B4776DAA FB5AFDF8 59E31373 263175E3 1F14416A 24C21D69 A46173B6 96CC84FB
  5B9D0203 010001A3 818C3081 89300906 03551D13 04023000 302C0609 60864801
  86F84201 0D041F16 1D4F7065 6E53534C 2047656E 65726174 65642043 65727469
  66696361 7465301D 0603551D 0E041604 146DD31C 03690B98 330B67FA 6EDC7B20
  F99FB924 60301F06 03551D23 04183016 8014966A 0C21AF96 3E827690 423599CC
  EE8087A1 2909300E 0603551D 0F0101FF 04040302 05A0300D 06092A86 4886F70D
  01010B05 00038201 0100C0B9 D2845D97 6FFC16DB 01559659 BC1DECA6 E1A01965
  1F6CD459 E03D7ABE 91179FEB 08BF5B9B 84B62C36 236F528E E30C921C 81DA29E1
  EA3DFDC1 B0B0EEBA 14EADAEC 078576E4 D643A0EF 7D8E0880 C5FC3965 811B08C0
  5696DBF5 FADA4092 ACF549B8 2257F508 636D52AA 6CDC9596 AB43313F 6C33C9C1
  2CFDDBE3 EA9D407C 8D1B0F49 BBACD0CD 2832AC12 CD3FEFC8 501E1639 A4EFDC27
  69CA0147 971A1B2D DB2758E6 A84AFC86 4F9A4942 3D7EDBCC 7BDCC1BB 61F69B31
  BF13E39B 10AAC31C 55E73C8B C30BE516 7C506FF4 AC367D94 814A6880 EF201A6D
  CD2E1A95 7BBEC982 01CE867D 931F56E1 1EF1C457 9DC9A0BE 9DB2DC9B 19873585
  89AE82F6 A37E51D6 EECD
        quit
certificate ca 008DD3A81106B14664
  308203A2 3082028A A0030201 02020900 8DD3A811 06B14664 300D0609 2A864886
  F70D0101 05050030 61310B30 09060355 04061302 5553310B 30090603 5504080C
  024E4331 0C300A06 03550407 0C035254 50310E30 0C060355 040A0C05 43495343
  4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273 6163612E
  65726368 616F2E63 6F6D301E 170D3135 31303231 32313135 34335A17 0D323531
  30313832 31313534 335A3061 310B3009 06035504 06130255 53310B30 09060355
  04080C02 4E43310C 300A0603 5504070C 03525450 310E300C 06035504 0A0C0543
  4953434F 310C300A 06035504 0B0C0353 544F3119 30170603 5504030C 10727361
  63612E65 72636861 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500
  0382010F 00308201 0A028201 0100CB82 2AECEE38 1BCB27B9 FA5F2FBD 8609B190
  16A6F741 5BEC18B8 8B260CAF 190EA1CE 063BC558 556DC085 6FAC5425 14AFE225
  0E9E3A12 05F3DA7E D17E03F2 7FFE92FB 38D67027 DBC5C175 EB53E96B 66C20D11
  B4C32D38 AE04385C 8FD4CB74 31A97824 CA1CAFD5 091806C3 6F9CBF8D DC42DD5B
  D985703D F3BB9ED1 7DE99614 422D765C 86AB25CD E80008C5 22049BE8 66D1CA27
  E1EB6D4F 4FD3CC18 E091BBF0 6FE0EB52 B33F231A 6D6B7190 4196C929 D22E2C42
  B9CD2BBD 24550E82 8CD8838F C41B4DAD 2FA1636A 5787BBB2 F21E4718 335B005B
  DFBE6EA7 56EBE30B D52DE85F FFAF0189 E372CBFC 44BFF235 4DA7C9EF DAAC6D0A
  A196DA5A 1B525175 C26B3581 EA4B0203 010001A3 5D305B30 1D060355 1D0E0416
  0414966A 0C21AF96 3E827690 423599CC EE8087A1 2909301F 0603551D 23041830
  16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405
  30030101 FF300B06 03551D0F 04040302 02A4300D 06092A86 4886F70D 01010505
  00038201 01002334 A3F0E5D3 4D229985 67A07754 73EC52E3 05B7D05F 926CC863
  220F849B 861C36B2 EF7C3485 474D4EF0 73895879 CAE08BBB 183B7CFA A20C4354
  86C6D9DF D445DACE C252C608 236F6673 F3F3C329 474B22E8 660BF91E 41054B8D
  43B80E44 AE69C164 2C9F41A2 8284F577 21FFAB8E A6771A5E DD34EBE4 A0DC2EAD
  95702010 02964566 478DA90F 5E134643 81A5F5EA 362D0394 1F9F23D1 DEE50B07
  12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723EBC B50E740B 0A9270E3
  60E2ED42 7F10D1A6 F6735144 AE93BF86 3D5A0502 6811D2BD 6E694693 28DE84C5
  3747CF0A D2B8D6C9 6CBEBA0A D1137CF8 E31CBF6B 437D82DD D74A4A9F 3557B3D9
  D0BD055F 65A8
        quit
license udi pid CISCO5921-K9 sn 9XG4481W768
username lab password 0 lab
```

```
!
redundancy
!
crypto keyring MVPN-spokes
rsa-pubkey address 0.0.0.0
  address 0.0.0.0
  key-string
  quit
!
crypto isakmp policy 10
encr aes
hash sha256
group 16
!
crypto isakmp policy 20
encr aes
hash sha256
group 14
crypto isakmp profile MVPN-profile
   description LAN-to-LAN for spoke router(s) connection
   keyring MVPN-spokes
   match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
mode transport
!
crypto dynamic-map MVPN-dynmap 10
set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 192.168.20.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
!
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
```

```
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none
!
end
```

以下に、Cisco Catalyst 3850 で X.509 証明書を設定してインストールするときの出力の例を示します。

```
cat3850#show running-config

enable password lab
!
username lab password 0 lab
aaa new-model

!

aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable

!

crypto isakmp policy 10

encr aes

hash sha256
authentication rsa-sig
group 16
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel

!

crypto ipsec profile radius-profile

!

crypto map radius 10 ipsec-isakmp
set peer 192.168.20.1
set transform-set radius

match address 100

!

interface GigabitEthernet1/0/1
no switchport
```

```
ip address 192.168.20.2 255.255.255.0

crypto map radius

!
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
!
snmp-server community public RO
snmp-server community private RW
!
radius server rad-ise
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

key secret
```

例：Cisco Catalyst 3850 での事前共有キー設定の出力

Cisco Catalyst 3850 で事前共有キーを設定する場合の出力の例を次に示します。

```
cat3850#show running-config

enable password lab
 !
 username lab password 0 lab
 aaa new-model
 !
 aaa group server radius ise
 server name ise-vm
 deadtime 60
 !
 aaa authentication login default group radius local

 aaa authentication enable default group radius enable

!

crypto isakmp policy 10

 encr aes

 hash sha256
 authentication pre-share
 group 16
 crypto isakmp key 123456789 address 0.0.0.0
 !
 crypto ipsec security-association lifetime seconds 86400
 !
 crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
 !
 crypto ipsec profile radius-profile
 !
 crypto map radius 10 ipsec-isakmp
 set peer 192.168.20.1
 set transform-set radius
 match address 100
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.20.2 255.255.255.0
```

```
 crypto map radius
!
 access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
 !
 snmp-server community public RO
 snmp-server community private RW
 !
 radius server rad-ise
 address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

 key secret
```

Mobile Device Manager と Cisco ISE との相互運用性

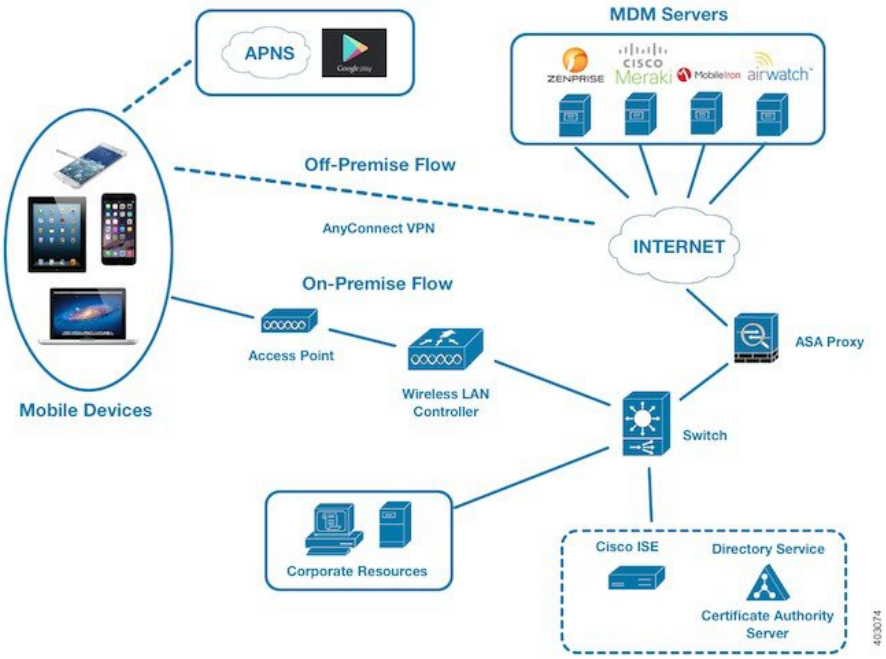
モバイルデバイス管理（MDM）サーバはモバイル事業者、サービスプロバイダー、企業にわたって展開されたモバイルデバイスの保護、モニタ、管理、およびサポートを行います。MDM サーバはポリシー サーバとして機能し、ポリシー サーバは展開環境のモバイル デバイスにある一部のアプリケーション（電子メール アプリケーションなど）の使用を制御します。ただし、ネットワークは、ACLに基づいてエンドポイントへのきめ細かいアクセス権を提供できる唯一のエンティティです。Cisco ISE は必要なデバイス属性について MDM サーバにクエリを行い、それらのデバイスに対してネットワーク アクセス コントロールを提供する ACL を作成します。

さまざまなベンダーからのサーバなど、複数のアクティブなMDMサーバをネットワークで実行できます。これにより、ロケーションやデバイスタイプなどのデバイスの要因に基づいて、異なる MDM サーバに異なるエンドポイントをルーティングすることができます。

また、Cisco ISE は、シスコの MDM API バージョン 2 を使用して MDM サーバと統合し、デバイスが AnyConnect 4.1 および Cisco ASA 9.3.2 以降を介して VPN 経由でネットワークにアクセスできるようにします。

この図では、Cisco ISE が適用ポイントで、MDM ポリシー サーバがポリシー情報ポイントです。Cisco ISE は、MDM サーバからデータを取得して、完全なソリューションを提供します。

図 *42 : MDM* の *Cisco ISE* との相互運用性



1 つ以上の外部 Mobile Device Manager（MDM）サーバと相互運用するように Cisco ISE を設定できます。サードパーティのこのタイプの接続を設定することによって、MDM データベースにある詳細情報を活用できます。Cisco ISE は REST API コールを使用して、外部 MDM サーバから情報を取得します。Cisco ISE はスイッチ、アクセス ルータ、ワイヤレス アクセス ポイント、その他のネットワーク アクセス ポイントに適切なアクセス コントロール ポリシーを適用して、Cisco ISE ネットワークへのリモート デバイス アクセスをより適切に制御します。

サポートされる MDM ベンダーは次のとおりです。サポートされる MDM サーバ （943 ページ）

サポートされる MDM の使用例

Cisco ISE が外部 MDM サーバを使用して実行する機能は、次のとおりです。

- デバイス登録の管理：ネットワークにアクセスする未登録のエンドポイントは、MDM サーバ上でホストされている登録ページにリダイレクトされます。デバイス登録には、ユーザ ロール、デバイス タイプなどが含まれます。
- デバイスの修復の処理：修復中のエンドポイントには制限付きアクセス権だけが付与されます。
- エンドポイント データの増加：Cisco ISE プロファイラを使用して収集できない、MDM サーバの情報でエンドポイント データベースを更新します。エンドポイントが MDM のモニタ対象デバイスの場合、Cisco ISE は **[ワークセンター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]** ページを使用して表示できる 6 つのデバイス属性を使用します。次に例を示します。
  - MDMImei: 99 000100 160803 3

- MDMManufacturer: Apple
- MDMModel: iPhone
- MDMOSVersion: iOS 6.0.0
- MDMPhoneNumber: 9783148806
- MDMSerialNumber: DNPGQZGUDTF9

- Cisco ISE は、4 時間ごとに MDM サーバをポーリングし、デバイス コンプライアンス データを確認します。これは管理者が設定できます。
- MDM サーバを介したデバイス手順の発行：MDM サーバを介してユーザのデバイスに対するリモート アクションを発行します。管理者は、ISE コンソールからリモート操作を開始します。

ベンダー MDM 属性

ISE で MDM サーバを設定すると、このベンダーの属性は ISE システム ディクショナリに **mdm** という名前で新しいエントリに追加されます。次の属性は登録ステータスで使用され、MDM ベンダーで一般的にサポートされています。

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- PhoneNumber
- MDMServerName
- MDMServerReachable
- MEID
- モデル
- UDID

ベンダー固有の属性はサポートされませんが、ベンダーがその属性をサポートする場合は、ERS API を使用してベンダー固有の属性を変換できる場合があります。

新しい MDM ディクショナリ属性は許可ポリシーで使用可能です。

サポートされる MDM サーバ

サポートされる MDM サーバは、次のベンダーの製品です。

- 絶対値（Absolute）
- AirWatch
- Citrix XenMobile
- Globo
- Good Technology
- IBM MaaS360
- JAMF ソフトウェア
- Meraki SM/EMM
- MobileIron

（注） 一部のバージョンの MobileIron は ISE では動作しません。MobileIron はこの問題を認識しており、修正があります。詳細については、MobileIron までご連絡ください。

- SAP Afaria
- SOTI
- Symantec
- Tangoe
- Microsoft Intune - モバイル デバイス用
- Microsoft SCCM -デスクトップ デバイス用

ISE コミュニティ リソース

How To: Meraki EMM / MDM Integration with ISE

MDM サーバにより使用されるポート

次の表に、相互に通信ができるように Cisco ISE と MDM サーバ間で開く必要のあるポートを示します。MDM エージェントおよびサーバで開く必要があるポートのリストについては、MDM サーバのドキュメントを参照してください。

表 *127 : MDM* サーバにより使用されるポート

MDM サーバ	ポート
MobileIron	443
Zenprise	443
Good	19005
Airwatch	443
Afaria	443
Fiberlink MaaS	443
Meraki	443
Microsoft Intune	80 および 443
Microsoft SCCM	80 および 443

MDM 統合プロセス フロー

ここでは、MDM 統合プロセスについて説明します。

1. ユーザはデバイスを SSID に関連付けます。
2. Cisco ISE は、MDM サーバに対して API コールを実行します。
3. この API コールは、このユーザのデバイスとデバイスのポスチャ ステータスのリストを戻します。

（注） 入力パラメータは、エンドポイントデバイスの MAC アドレスです。オフプレミスの Apple iOS デバイス（VPN 経由で Cisco ISE に接続するデバイス）の場合、これは UDID です。

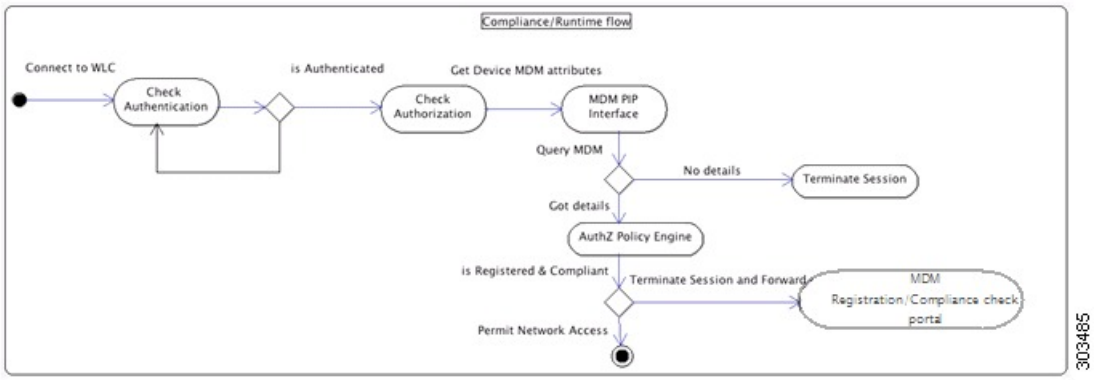
4. ユーザのデバイスがこのリストにない場合、デバイスが登録されていないことを意味します。Cisco ISE は、Cisco ISE にリダイレクトされる許可要求を NAD に送信します。ユーザが MDM サーバ ページに表示されます。

（注） MDM ポータルを介して Cisco ISE ネットワークの外の MDM サーバに登録済みのデバイスを登録する必要があります。これは Cisco ISE、リリース 1.4 以降に適用されます。ISE の以前のバージョンでは、Cisco ISE ネットワークの外に登録済みのデバイスはポスチャ ポリシーに準拠している場合に自動的に登録されます。

5. Cisco ISE は、MDM を使用してデバイスをプロビジョニングし、デバイスを登録するための適切なページをユーザに表示します。

6. ユーザは MDM サーバにデバイスを登録し、MDM サーバは Cisco ISE に要求をリダイレクトします（自動リダイレクションまたは手動のブラウザ リフレッシュによって）。
7. Cisco ISE は MDM サーバに対して再度ポスチャ ステータスのクエリーを実行します。
8. ユーザのデバイスが MDM サーバで設定されているポスチャ（コンプライアンス）ポリシーに準拠していない場合、デバイスがポリシーに準拠しておらず、準拠する必要があることがユーザに通知されます。
9. ユーザのデバイスがポリシーに準拠するようになった後、MDM のサーバは内部テーブルのデバイスのステータスを更新します。
10. ここでユーザがブラウザをリフレッシュすると、制御が Cisco ISE に返されます。
11. Cisco ISE はコンプライアンス情報を取得するために MDM サーバを 4 時間ごとにポーリングし、必要に応じて許可変更（CoA）を発行します。これは管理者が設定できます。また、Cisco ISE は 5 分ごとに MDM サーバをチェックして使用できるかどうかを確認します。

次の図は、MDM プロセス フローを示しています。



（注） 一度に 1 つの MDM サーバに登録できるデバイスは 1 台のみです。別のベンダーから MDM サービスに同じデバイスを登録する場合、デバイスから前のベンダーのプロファイルを削除する必要があります。MDM サービスは通常、「企業ワイプ」を提供し、これはデバイスからベンダーの設定のみを削除します（デバイス全体ではありません）。ユーザはこのファイルを削除することもできます。たとえば、IOS デバイスで、[設定（Settings）] > [全般（General）] > [デバイス管理（Device management）] の順に移動し、削除の管理をクリックすることができます。または、ISE の MyDevices ポータルに移動し、企業ワイプをクリックすることができます。

Cisco ISE による MDM サーバの設定

Cisco ISE で MDM サーバを設定するには、次の高レベル タスクを実行します。

ステップ 1 Azure に PAN の証明書をインポートする Intune を除き、Cisco ISE に MDM のサーバ証明書をインポートします。

ステップ 2 Mobile Device Manager の定義を作成します。

ステップ 3 ワイヤレス LAN コントローラの ACL を設定します。

ステップ 4 MDM サーバに未登録のデバイスをリダイレクトするための許可プロファイルを設定します。

ステップ 5 ネットワークに複数の MDM サーバがある場合は、各ベンダーに個別の許可プロファイルを設定します。

ステップ 6 MDM 使用例の許可ポリシー ルールを設定します。

Cisco ISE への MDM サーバ証明書のインポート

Cisco ISE を MDM サーバに接続するには、Cisco ISE 証明書ストアに MDM サーバ証明書をインポートする必要があります。MDM サーバに CA 署名付き証明書がある場合は、Cisco ISE 証明書ストアにルート CA をインポートする必要があります。

（注） Microsoft Azure の場合は、ISE 証明書を Azure にインポートします。詳細については、MDM サーバとしての Microsoft Intune の設定 （950 ページ）を参照してください。

ステップ 1 MDM サーバ証明書を MDM サーバからエクスポートして、ローカル マシンに保存します。

ステップ 2 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificate）] > [インポート（Import）]** を選択します。

ステップ 3 [参照（Browse）] をクリックして、MDM サーバから取得した MDM サーバ証明書を選択します。

ステップ 4 わかりやすい名前を追加します。

ステップ 5 [ISE内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにします。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 [証明書ストア（Certificate Store）] リスト ページに MDM サーバ証明書が一覧表示されることを確認します。

次のタスク

ISE でのモバイル デバイス管理サーバの定義 （946 ページ）

。

ISE でのモバイル デバイス管理サーバの定義

外部 MDM サーバ用のモバイル デバイス管理（MDM）定義とデスクトップ デバイス マネージャ（SCCM）定義を 1 つ以上作成できます。

1. **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [外部 MDM（External MDM）]** の順に選択します。
2. [追加（Add）] をクリックします。
3. 追加する MDM サーバの名前と説明を入力します。
4. [サーバ タイプ（Server Type）] で、[モバイル デバイス マネージャ（Mobile Device Manager）] または [デスクトップ デバイス マネージャ（Desktop Device Manager）] を選択します。どちらを選択するかで、どのフィールドが次に表示されるかが決定します。[デスクトップ デバイス マネージャ（Desktop Device Manager）] を選択した場合は、「デスクトップデバイス管理 （949ページ）」に進みます。[モバイルデバイスマネージャ（Mobile Device Manager）] を選択した場合は、次の手順を続行します。
5. [認証タイプ（Authentication Type）] で、[ベーシック（Basic）] または [OAuth - クライアント クレデンシャル（OAuth - Client Credentials）] を選択します。Microsoft Intune サーバを設定する [OAuth -クライアント クレデンシャル（OAuth - Client Credentials）] を選択した場合は、「モバイル デバイス管理 - OAuth - クライアント クレデンシャル（Mobile Device Management - OAuth - Client Credentials） （948 ページ）」に進みます。[ベーシック（Basic）] を選択した場合は、次の手順を続行します。
6. すべての画面で、MDM サーバ定義の名前と説明が求められます。ここでは、サーバと認証タイプに基づいて、その他のフィールドと手順について説明しています。

モバイル デバイス管理：ベーシック

- ホスト名/IPアドレス（Host Name / IP Address）：MDM サーバのホスト名または IP アドレスを入力します。
- ポート（Port）：MDM サーバとの接続に使用するポートを入力します。通常は 443。
- インスタンス名（Instance Name）：この MDM サーバに複数のインスタンスがある場合に、接続するインスタンスを入力します。
- ポーリング間隔（Polling Interval）：Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報を確認するためのポーリング間隔（分単位）を入力します。MDM サーバ上のポーリング間隔に一致するようにこの値を設定します。有効な範囲は 15 ～ 1440 分です。デフォルト値は 240 分です。ネットワーク上の少数のアクティブ クライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブ クライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。

  ポーリング間隔を 0 に設定すると、ISE は MDM サーバとの通信をディセーブルにします。
- 準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）：エンドポイントが認証または再認証されるときに、ISE はそのエンドポイントの MDM 変数を取得するのにキャッシュを使用します。キャッシュされた値が [準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）] の値よりも古い場合、ISE は新しい値を取得するために、MDM サーバへのデバイス クエリを作成します。準拠ステータスが変更されると、ISE は CoA をトリガーします。

有効な範囲は 1 ～ 1440 分です。デフォルト値は 1 分です。

モバイル デバイス管理 - OAuth - クライアント クレデンシャル（Mobile Device Management - OAuth - Client Credentials）

OAuth を使用するには、OAuth サーバの設定が必要です。これについては、次で説明します。MDM サーバとしての Microsoft Intune の設定 （950 ページ）

- 自動検出URL（Auto Discovery URL）：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph APIエンドポイント（Microsoft Azure AD Graph API Endpoint）] の値を入力します。この URL は、アプリケーションが Graph API を使用して Microsoft Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>` です。

- クライアントID（Client ID）：アプリケーションの固有識別子。アプリケーションが、Microsoft Azure AD Graph API、Microsoft Intune API などの他のアプリケーションのデータにアクセスする場合に、この属性を使用します。

- トークン発行URL（Token Issuing URL）：前のステップの [OAuth2.0認証エンドポイント（Oauth2.0 Authorization Endpoint）] の値を入力します。これは、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション（ISE）にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。

- トークン対象者（Token Audience）：トークンが対象とする受信者リソース。パブリックの既知の Microsoft Intune API の APP ID URL。

- ポーリング間隔（Polling Interval）：Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報を確認するためのポーリング間隔（分単位）を入力します。MDM サーバ上のポーリング間隔に一致するようにこの値を設定します。有効な範囲は15～1440分です。デフォルト値は240分です。ネットワーク上の少数のアクティブクライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブ クライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。

  ポーリング間隔を0に設定すると、ISEはMDMサーバとの通信をディセーブルにします。

- 準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）：エンドポイントが認証または再認証されるときに、ISE はそのエンドポイントの MDM 変数を取得するのにキャッシュを使用します。キャッシュされた値が [準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）] の値よりも古い場合、ISE は新しい値を取得するために、MDM サーバへのデバイス クエリを作成します。準拠ステータスが変更されると、ISE は CoA をトリガーします。

有効な範囲は 1 ～ 1440 分です。デフォルト値は 1 分です。

デスクトップ デバイス管理

次の設定では、ISE と通信できるように SCCM サーバの WMI を設定する必要があります。詳細については、ISE 用の Microsoft SCCM サーバの設定 （954 ページ）を参照してください。

- ホスト名/IPアドレス（Host Name / IP Address）：MDM サーバのホスト名または IP アドレスを入力します。
- サイトまたはインスタンス名（Site or Instance Name）：サイト名または、MDM サーバに複数のインスタンスがある場合はインスタンス名を入力します。

Microsoft Intune および SCCM のための ISE MDM サポート

- **Microsoft Intune**：MDM-ISE はパートナー MDM サーバ管理モバイル デバイスとして、Microsoft の Intune デバイス管理をサポートします。

  Intune サーバ管理モバイル デバイスの OAuth 2.0 クライアント アプリケーションとして ISE を設定します。ISE は、Azure からトークンを取得し、ISE Intune アプリケーションとのセッションを確立します。

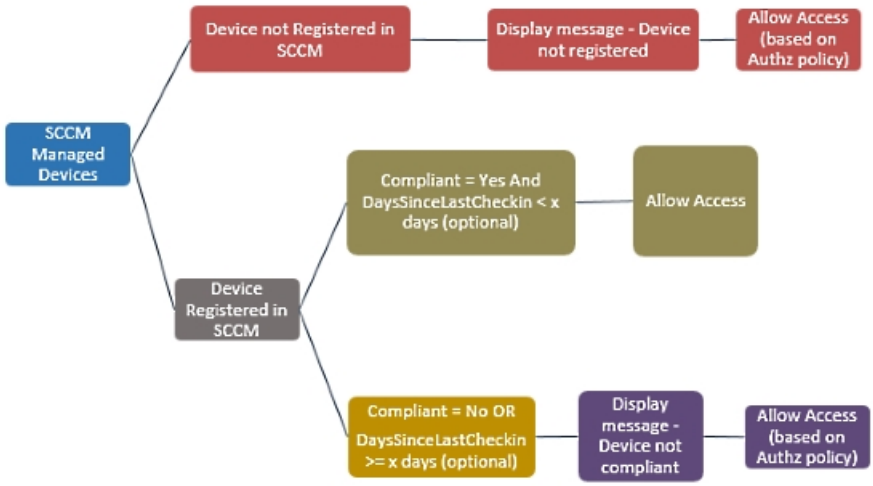
  Intune がクライアント アプリケーションとどのように通信するかについての詳細は、https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx を参照してください。

- **デスクトップ デバイス マネージャ（Microsoft SCCM）**：ISE は Microsoft System Center Configuration Manager（SCCM）を Windows コンピュータの管理用パートナー MDM サーバとしてサポートします。ISE は、WMI を使用してコンプライアンス情報を SCCM サーバから取得し、その情報を使用してユーザの Windows デバイスへのネットワーク アクセスを許可または拒否します。

SCCM のワークフロー

ISE はデバイスが登録されているかについて、また登録済みの場合は準拠しているかどうかについて SCCM サーバから情報を取得できます。次の図に、SCCM により管理されるデバイス用のワークフローを示します。

図 *43 : SCCM* のワークフロー



デバイスを接続し、SCCM ポリシーが一致すると、ISE はコンプライアンスと最終ログイン（チェックイン）時間を取得するために、許可ポリシーで指定されている SCCM サーバを照会します。この情報を使用して、ISE はエンドポイントのリストのデバイスのコンプライアンス ステータスと lastCheckinTimeStamp を更新します。

デバイスが準拠していないか SCCM に登録されていない、およびリダイレクト プロファイルが許可ポリシーで使用されている場合、デバイスが準拠していないか SCCM に登録されていないというメッセージがユーザに表示されます。ユーザがメッセージを受け取った後、ISE は SCCM 登録サイトへ CoA を発行できます。承認ポリシーおよびプロファイルに基づいてユーザにアクセスを許可できます。

Microsoft SCCM サーバ接続の監視

ポーリングは SCCM 用に設定できません。

ISE は、SCCM サーバへの接続を検証し、ISE が SCCM サーバへの接続を失うとアラームを発生させる、MDM ハートビート ジョブを実行します。ハートビート ジョブの間隔は設定できません。

MDM サーバとしての Microsoft Intune の設定

ISE の MDM サーバとして Microsoft Intune を設定することは、他の MDM サーバの設定とは少し異なります。Azure への ISE の接続および ISE への Azure の接続を設定するには、次の手順を使用します。

1. パブリック証明書を Intune/Azure Active Directory テナントから取得し、ISE にインポートして SSL ハンドシェイクをサポートします。
    1. 1. サイトがテナントを持つ Intune 管理コンソールまたは Azure 管理コンソールにログオンします。

2. ブラウザを使用して証明書の詳細を取得します。たとえば、Internet Explorer の場合は次のように操作します。
    1. ブラウザのツールバーのロックシンボルをクリックしてから、[証明書の表示（View Certficates）] をクリックします。
    2. [証明書（Certificate）] ウィンドウで、[認証パス（Certification Path）] タブを選択します。
    3. Baltimore Cyber Trust ルートを見つけて、そのルート証明書をエクスポートします。
3. ISE で、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** の順に選択し、保存したルート証明書をインポートします。証明書に Azure MDM などのわかりやすい名前を付けます。

2. ISE 自己署名証明書をエクスポートし、InTune/Azure 用に準備をします。
    1. PAN で、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** の順に移動し、デフォルトの自己署名サーバ証明書を選択して、[エクスポート（Export）] をクリックします。
    2. [証明書のみエクスポート（Export Certificate Only）]（デフォルト）を選択し、保存する場所を選択します。

    エクスポートされた証明書ファイルに次の PowerShell スクリプトを実行します。

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("mycer.cer")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)

$keyid = [System.Guid]::NewGuid().ToString()
```

    次の手順で使用するため、**$base64Thumbprint、$base64Value、$keyid** の値をメモしておきます。

3. Intune で ISE アプリケーションを作成します。
    1. Microsoft Azure 管理ポータルで顧客ドメインにサインインし、**[ディレクトリ（Directory）] > [アプリケーション（Applications）] > [アプリケーションの追加（Add an Application）]** に移動して、[自分の組織が開発中のアプリケーションの追加（Add an application my organization is developing）] を選択します。
    2. 次のパラメータを使用して、Azure で ISE アプリケーションを設定します。
        - アプリケーション名（Application Name）：**ISE** と入力します。
        - [Web アプリケーションまたは Web アプリ（WEB APPLICATION AND/OR WEB APP）] を選択します。

- サインオン URL およびアプリ ID URL（SIGN-ON URL and APP ID URL）：任意の有効な URL を追加します。この値は ISE では使用されません。

4. Azure からマニフェスト ファイルを取得し、ISE 証明書情報を追加して、更新されたマニフェストを Azure にアップロードします。

   1. Microsoft Azure 管理ポータル（https://manage.windowsazure.com）で、AAD スナップインを開き、ISE アプリケーションに移動します。

   [マニフェストの管理（Manage Manifest）] メニューからアプリケーション マニフェスト ファイルをダウンロードします。

5. *Base64 Encoded String of ISE PAN cert* を、PowerShell スクリプトの $base64Value である、エクスポートされ編集された ISE からの証明書ファイルと置き換えて、次の例のようにマニフェスト json ファイルの [keyCredentials] フィールドを更新します。

```
"keyCredentials": [
                                {
                               "customKeyIdentifier": "$base64Thumbprint_from_above",

                                  "keyId": "$keyid_from_above",
                                  "type": "AsymmetricX509Cert",
                                  "usage": "Verify",
                                  "value": "Base64 Encoded String of ISE PAN cert"
                                }
                            ]
```

（注） マニフェスト ファイルの名前は変更しないようにします。

KeyCredentials の複雑なタイプは、http://msdn.microsoft.com/en-us/library/azure/dn151681.aspx でドキュメント化されています。

6. Azure に更新されたマニフェスト ファイルをアップロードします。

7. Microsoft Azure 管理ポータルで、アプリ エンドポイントのリストに移動します。次のエンドポイント属性の値を使用して ISE を設定します。

   - MICROSOFT AZURE AD GRAPH API ENDPOINT
   - OAUTH 2.0 TOKEN ENDPOINT

8. ISE で、ISE の Intune サーバを設定します。設定と外部 MDM サーバの詳細については、ISE でのモバイル デバイス管理サーバの定義 （946 ページ）を参照してください。Intune にとって重要なフィールドは次のとおりです。

   - 自動検出URL（Auto Discovery URL）：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph APIエンドポイント（Microsoft Azure AD Graph API Endpoint）] の値を入力します。この URL は、アプリケーションが Graph API を使用して Microsoft Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この

URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>` です。

- クライアントID（Client ID）：アプリケーションの固有識別子。アプリケーションが、Microsoft Azure AD Graph API、Microsoft Intune API などの他のアプリケーションのデータにアクセスする場合に、この属性を使用します。
- トークン発行URL（Token Issuing URL）：前のステップの [OAuth2.0認証エンドポイント（Oauth2.0 Authorization Endpoint）] の値を入力します。これは、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション（ISE）にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。
- トークン対象者（Token Audience）：トークンが対象とする受信者リソース。パブリックの既知の Microsoft Intune API の APP ID URL。

Intune アプリケーションの詳細については、次のリンクを参照してください。

- https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx
- http://blogs.msdn.com/b/exchangedev/archive/2015/01/22/building-daemon-or-service-apps-with-office-365-mail-calendar-and-contacts-apis-oauth2-client-credentials-flow.aspx
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-manifest

Microsoft SCCM のポリシー設定の例

ポリシーでは次の新しいディクショナリ エントリが使用され、SCCM をサポートすることができます。

- MDM.DaysSinceLastCheckin：ユーザが最後に確認してからの日数、または SCCM のデバイスと同期してからの日数で、1 ～ 365 日です。
- MDM.UserNotified：値は Y または N です。ユーザが登録されていないことをユーザに通知したかどうかを示します。さらに、登録ポータルへの制限付きアクセスやリダイレクトを許可し、またはアクセスを拒否できます。
- MDM.ServerType：値はモバイル デバイス マネージャの場合 MDM またはデスクトップ デバイス マネージャの場合 DM です。

次のサンプル ポリシー セットで SCCM をサポートする一連のポリシーを示します。

ポリシー名	条件（IF）	実行されるアクション（Then）
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCMRedirect
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCMRedirect
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

ISE 用の Microsoft SCCM サーバの設定

ISE は、WMI を使用して SCCM サーバと通信します。WMI は、SCCM を実行している Windows サーバで設定する必要があります。

（注） ISE 統合に使用するユーザ アカウントは、次のいずれかの条件を満たしている必要があります。

- SMS 管理ユーザ グループのメンバーである。
- WMI 名前空間で SMS オブジェクトと同じアクセス許可がある。

  `root\sms\site_<sitecode>`

  サイトコードは SCCM サイトです。

AD ユーザがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows 2012 および Windows 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティング システムの特定のレジストリ キーを完全に制御することができません。Active Directory の管理者は、Active Directory ユーザに次のレジストリ キーに対する完全制御権限を提供する必要があります。

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

次の Active Directory のバージョンでは、レジストリ変更は必要ありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、次に示すように、まず Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーを右クリックして [オーナー（Owner）] タブに移動します。

ステップ 2 [アクセス許可（Permissions）] をクリックします。

ステップ 3 [詳細設定（Advanced）] をクリックします。

AD ユーザがドメイン管理グループの一部ではない場合に必要な権限

Windows 2012 R2 の場合は、Active Directory ユーザに次のレジストリ キーに対する**完全制御**権限を提供します。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Active Directory ユーザがドメイン管理グループの一部ではなく、ドメイン ユーザ グループの一部である場合は、次の権限も必要です。

- ISEがドメイン コントローラに接続できるようにするレジストリ キーを追加します（下記を参照）
- ドメイン コントローラで DCOM を使用するための権限 （627 ページ）
- WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （629 ページ）

これらの権限は、次の Active Directory のバージョンでのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加する

ISEがドメインユーザとして接続し、ログイン認証イベントを取得できるようにするには、ドメイン コントローラに一部のレジストリ キーを手動で追加する必要があります。エージェントはドメイン コントローラまたはドメイン内のマシンでは必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

キー **DllSurrogate** の値には、2 つのスペースが含まれていることを確認します。

上記のスクリプトに示すように、ファイルの末尾の空の行を含む、空の行を保持してください。

ドメイン コントローラで DCOM を使用するための権限

ISE パッシブ ID サービスに使用される Active Directory ユーザは、ドメイン コントローラで DCOM（リモート COM）を使用する権限がなければなりません。**dcomcnfg** コマンド ライン ツールを使用して権限を設定できます。

ステップ 1 コマンド ラインから **dcomcnfg** ツールを実行します。

ステップ 2 [コンポーネントサービス（Component Services）] を展開します。

ステップ 3 **[コンピュータ（Computers）] > [マイコンピュータ（My Computer）]** を展開します。

ステップ 4 メニュー バーで [アクション（Action）] を選択して、[プロパティ（properties）] をクリックし、[COMセキュリティ（COM Security）] をクリックします。

ステップ 5 アクセスおよび起動の両方に対して ISE が使用するアカウントに許可権限があることを確認します。Active Directory ユーザは、4 つのオプション（[アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対する [制限の編集（Edit Limits）] と [デフォルトの編集（Edit Default）]）のすべてに追加される必要があります。

ステップ 6 [アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対してローカルおよびリモート アクセスをすべて許可します。

図 *44 : [アクセス権限（**Access Permissions**）] のローカルおよびリモート アクセス*

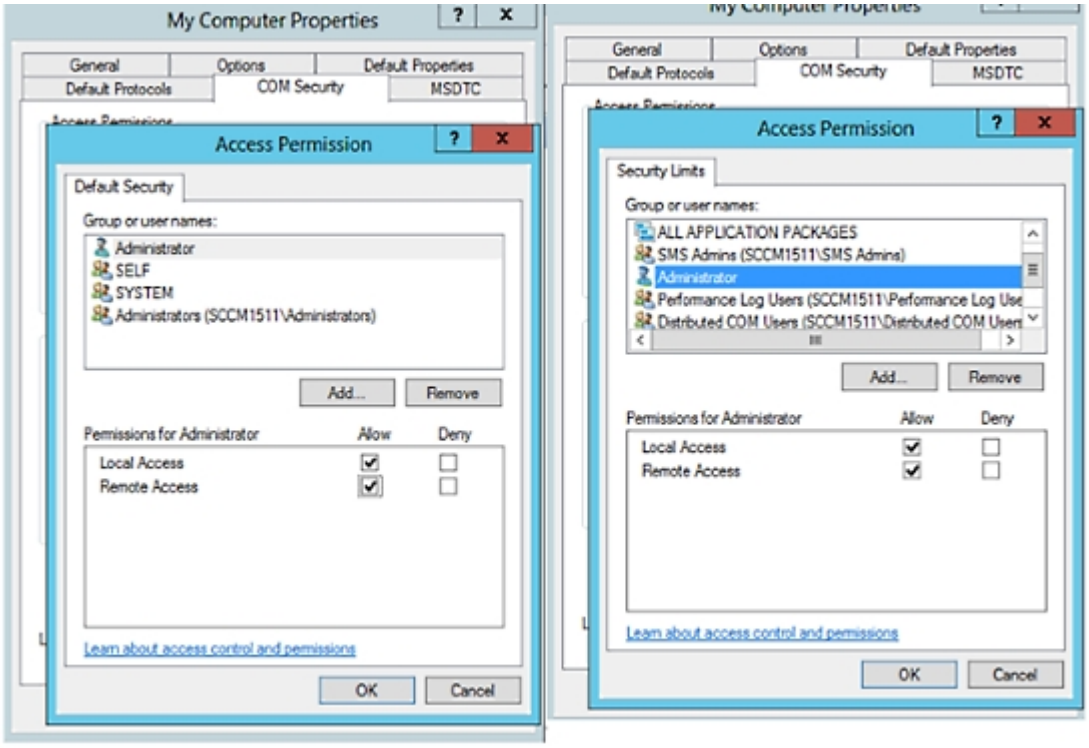
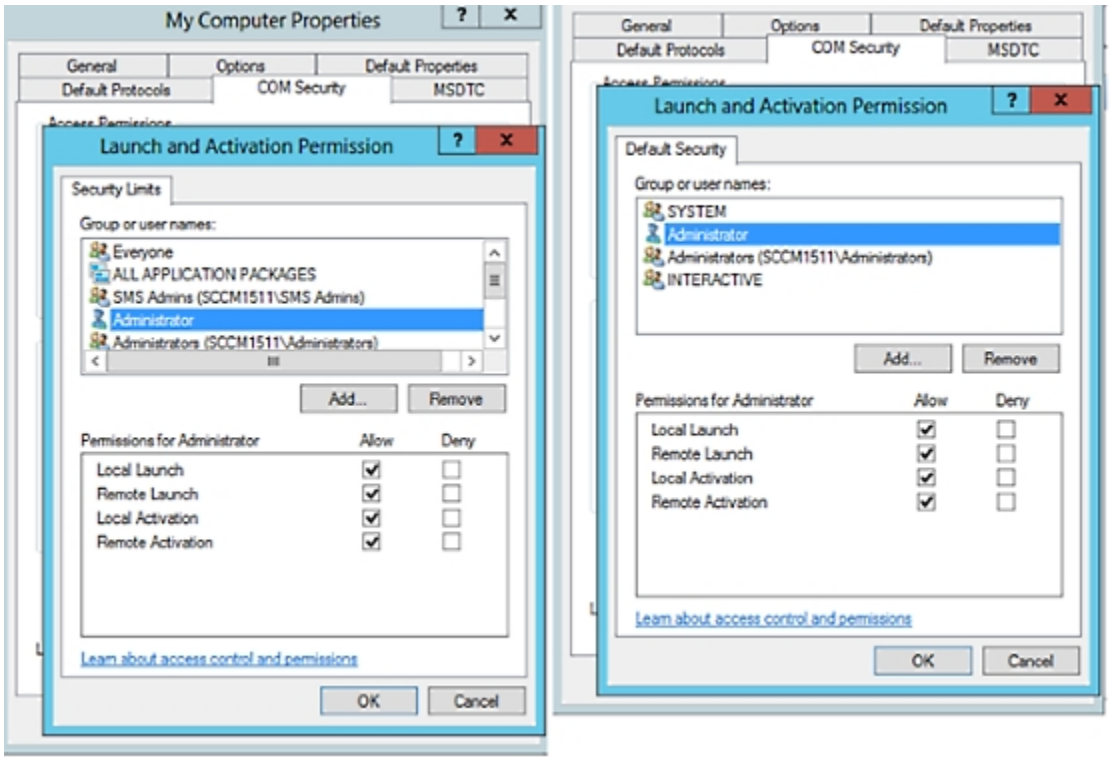


図 *45 : [*起動およびアクティベーションの権限（***Launch and Activation Permissions***）*]* のローカルおよびリモート アクセス



WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Active Directory ユーザには実行メソッドおよびリモートイネーブルのための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

ステップ 1 [スタート] > [Run] をクリックし、`wmimgmt.msc` と入力します。

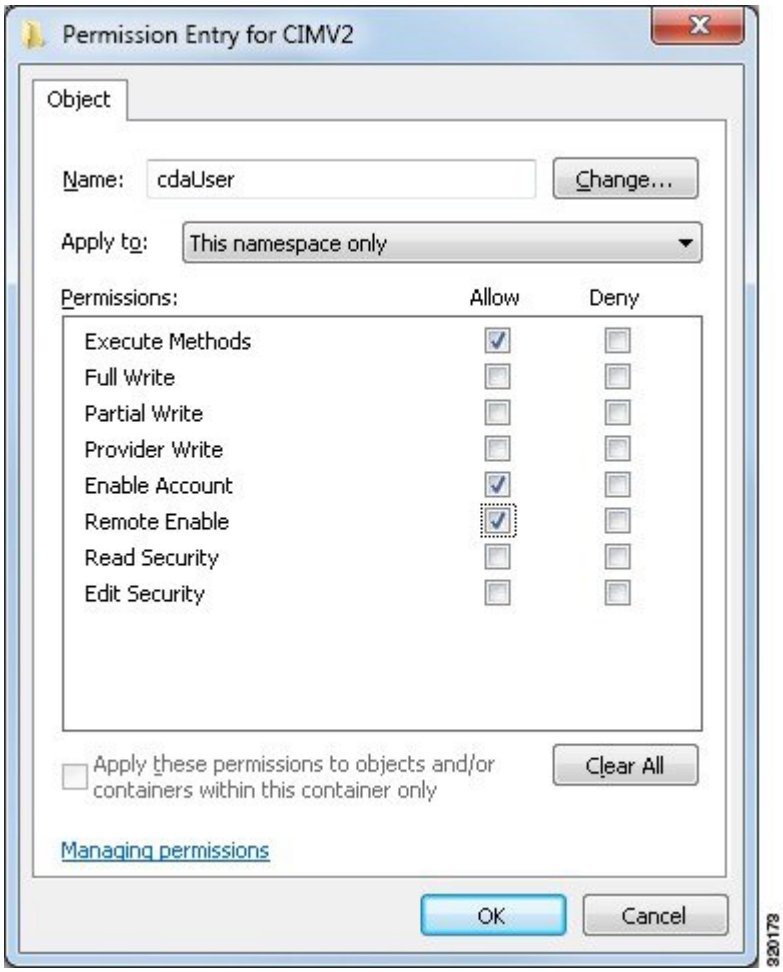
ステップ 2 [WMI Control] を右クリックし、[プロパティ] をクリックします。

ステップ 3 [セキュリティ] タブで [ルート] を展開し、[CIMV2] を選択します。

ステップ 4 [セキュリティ（Security）] をクリックします。

ステップ 5 下に示すように、Active Directory ユーザを追加し、必要な権限を設定します。

図 *46 : WMI Root\CIMv2* 名前空間に必要な権限



WMI アクセス用にファイアウォール ポートを開く

Active Directory ドメイン コントローラのファイアウォール ソフトウェアは、WMI へのアクセスをブロックすることがあります。ファイアウォールをオフにするか、または次のポートへの特定の IP（ISE IP アドレス）のアクセスを許可することができます。

- TCP 135：一般的な RPC ポート。非同期 RPC 発信をすると、このポートでリスニングしているサービスが、クライアントに、この要求を処理できるコンポーネントが使用しているポートを通知します。
- UDP 138：NetBIOS データグラム サービス
- TCP 139：NetBIOS セッション サービス
- TCP 445：SMB

（注） Cisco ISE 1.3 以降は SMB 2.0 をサポートします。

数値の大きいポートは動的に割り当てられ、手動で設定できます。ターゲットとして %SystemRoot%\System32\dllhost.exe を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォール ルールを、特定の IP アドレス（ISE IP）に割り当てることができます。

未登録のデバイスのリダイレクトのための許可プロファイルの設定

各外部 MDM サーバの未登録のデバイスをリダイレクトするには、Cisco ISE で許可プロファイルを設定する必要があります。

始める前に

- Cisco ISE で MDM サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、MDM ディクショナリ属性を使用して許可ポリシーを作成できます。
- 未登録のデバイスをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。
- インターネット接続にプロキシを使用していて、MDM サーバが内部ネットワークの一部である場合は、プロキシ バイパス リストに MDM サーバ名または IP アドレスを追加する必要があります。**[管理（Administration）]** > **[設定（Settings）]** > **[プロキシ設定（Proxy Settings）]**の順に選択して、このアクションを実行します。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** > **[追加（Add）]** を選択します。

ステップ 2 準拠していないまたは登録されていない未登録デバイスをリダイレクトするための許可プロファイル作成します。

ステップ 3 MDM サーバ名と一致する許可プロファイルの名前を入力します。

ステップ 4 アクセス タイプとして ACCESS_ACCEPT を選択します。

ステップ 5 [Web リダイレクション（Web Redirection）] チェックボックスをオンにし、ドロップダウン リストから [MDM リダイレクト（MDM Redirect）] を選択します。

ステップ 6 ワイヤレス LAN コントローラ上で設定した ACL の名前を [ACL] フィールドに入力します。

ステップ 7 [値（Value）] ドロップダウン リストから MDM ポータルを選択します。

ステップ 8 ドロップダウン リストから、使用する MDM サーバを選択します。

ステップ 9 [送信（Submit）] をクリックします。

次のタスク

MDM 使用例の許可ポリシー ルールの設定。

MDM 使用例の許可ポリシー ルールの設定

MDM 設定を完了するには、Cisco ISE で許可ポリシー ルールを設定する必要があります。

始める前に

- Cisco ISE 証明書ストアに MDM サーバ証明書を追加します。
- Cisco ISE で MDM サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、MDM ディクショナリ属性を使用して許可ポリシーを作成できます。
- 未登録のデバイスまたは非準拠のデバイスをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー セット（Policy Sets）]** を選択し、許可ポリシー ルールを表示するポリシー セットを展開します。

ステップ 2 次のルールを追加します。

- [MDM_Un_Registered_Non_Compliant]：MDM サーバに登録されていないか、MDM ポリシーに準拠していないデバイスの場合。要求がこのルールに一致すると、ISE MDM ページが表示され、MDM でのデバイスの登録に関する情報が示されます。
- [PERMIT]：デバイスが Cisco ISE および MDM に登録されており、Cisco ISE および MDM ポリシーに準拠している場合、Cisco ISE で設定されたアクセス コントロール ポリシーに基づいてネットワークへのアクセス権が付与されます。

次の図は、この設定の例を示します。

図 *47 : MDM* の使用例の許可ポリシー ルール

ステップ 3 **[保存（Save）]** をクリックします。

デバイスのワイプまたはロック

Cisco ISE では、失われたデバイスをワイプしたり、PIN ロックをオンにしたりできます。これは [エンドポイント（Endpoints）] ページから行うことができます。

ステップ 1 **[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

ステップ 2 ワイプまたはロックするデバイスの横にあるチェックボックスをオンにします。

ステップ 3 [MDM アクセス（MDM Access）] ドロップダウン リストから、次のオプションのいずれかを選択します。

- [完全ワイプ（Full Wipe）]：このオプションを使用すると、MDM ベンダーに応じて、企業アプリケーションが削除されるか、またはデバイスが工場出荷時の設定にリセットされます。
- [企業ワイプ（Corporate Wipe）]：MDM サーバ ポリシーで設定したアプリケーションを削除します
- [PIN ロック（PIN Lock）]：デバイスをロックします

ステップ 4 [はい（Yes）] をクリックして、デバイスをワイプまたはロックします。

Mobile Device Manager のレポートの表示

Cisco ISE では、MDM サーバ定義のすべての追加、更新、および削除を記録します。これらのイベントは、選択された期間での任意のシステム管理者によるすべての設定変更を報告する「変更設定監査」レポートで表示できます。

[操作（Operations）] > [レポート（Reports）] > [変更設定監査（Change Configuration Audit）] > [MDM] を選択し、結果のレポートで表示する期間を指定します。

Mobile Device Manager のログの表示

[メッセージ カタログ（Message Catalog）] ページを使用して、Mobile Device Manager のログ メッセージを表示できます。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージカタログ（Message Catalog）]** を選択します。MDM ログ エントリのデフォルトのレポーティング レベルは「INFO」です。レポーティング レベルを「DEBUG」または「TRACE」に変更できます。

Mobile Device Manager と Cisco ISE との相互運用性

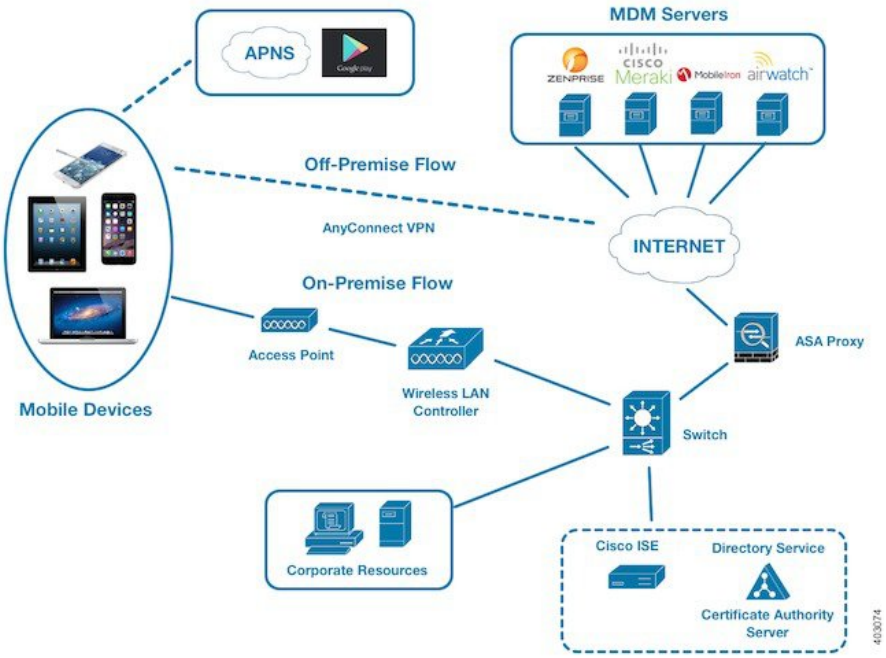
モバイルデバイス管理（MDM）サーバはモバイル事業者、サービス プロバイダー、企業にわたって展開されたモバイルデバイスの保護、モニタ、管理、およびサポートを行います。MDM サーバはポリシー サーバとして機能し、ポリシー サーバは展開環境のモバイル デバイスにある一部のアプリケーション（電子メール アプリケーションなど）の使用を制御します。ただし、ネットワークは、ACL に基づいてエンドポイントへのきめ細かいアクセス権を提供できる唯一のエンティティです。Cisco ISE は必要なデバイス属性について MDM サーバにクエリを行い、それらのデバイスに対してネットワーク アクセス コントロールを提供する ACL を作成します。

さまざまなベンダーからのサーバなど、複数のアクティブなMDMサーバをネットワークで実行できます。これにより、ロケーションやデバイスタイプなどのデバイスの要因に基づいて、異なる MDM サーバに異なるエンドポイントをルーティングすることができます。

また、Cisco ISE は、シスコの MDM API バージョン 2 を使用して MDM サーバと統合し、デバイスが AnyConnect 4.1 および Cisco ASA 9.3.2 以降を介して VPN 経由でネットワークにアクセスできるようにします。

この図では、Cisco ISE が適用ポイントで、MDM ポリシー サーバがポリシー情報ポイントです。Cisco ISE は、MDM サーバからデータを取得して、完全なソリューションを提供します。

図 *48 : MDM* の *Cisco ISE* との相互運用性



1 つ以上の外部 Mobile Device Manager（MDM）サーバと相互運用するように Cisco ISE を設定できます。サードパーティのこのタイプの接続を設定することによって、MDM データベースにある詳細情報を活用できます。Cisco ISE は REST API コールを使用して、外部 MDM サーバから情報を取得します。Cisco ISE はスイッチ、アクセス ルータ、ワイヤレス アクセス ポイント、その他のネットワーク アクセス ポイントに適切なアクセス コントロール ポリシーを適用して、Cisco ISE ネットワークへのリモート デバイス アクセスをより適切に制御します。

サポートされるMDMベンダーは次のとおりです。サポートされるMDMサーバ（943ページ）

サポートされる MDM の使用例

Cisco ISE が外部 MDM サーバを使用して実行する機能は、次のとおりです。

- デバイス登録の管理：ネットワークにアクセスする未登録のエンドポイントは、MDMサーバ上でホストされている登録ページにリダイレクトされます。デバイス登録には、ユーザロール、デバイス タイプなどが含まれます。

- デバイスの修復の処理：修復中のエンドポイントには制限付きアクセス権だけが付与されます。
- エンドポイント データの増加：Cisco ISE プロファイラを使用して収集できない、MDM サーバの情報でエンドポイントデータベースを更新します。エンドポイントがMDMのモニタ対象デバイスの場合、Cisco ISE は **[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]** ページを使用して表示できる 6 つのデバイス属性を使用します。次に例を示します。
  - MDMImei: 99 000100 160803 3
  - MDMManufacturer: Apple
  - MDMModel: iPhone
  - MDMOSVersion: iOS 6.0.0
  - MDMPhoneNumber: 9783148806
  - MDMSerialNumber: DNPGQZGUDTF9
- Cisco ISE は、4 時間ごとに MDM サーバをポーリングし、デバイス コンプライアンス データを確認します。これは管理者が設定できます。
- MDM サーバを介したデバイス手順の発行：MDM サーバを介してユーザのデバイスに対するリモートアクションを発行します。管理者は、ISE コンソールからリモート操作を開始します。

ベンダー MDM 属性

ISE で MDM サーバを設定すると、このベンダーの属性は ISE システム ディクショナリに **mdm** という名前で新しいエントリに追加されます。次の属性は登録ステータスで使用され、MDM ベンダーで一般的にサポートされています。

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- PhoneNumber
- MDMServerName
- MDMServerReachable

- MEID
- モデル
- UDID

ベンダー固有の属性はサポートされませんが、ベンダーがその属性をサポートする場合は、ERS API を使用してベンダー固有の属性を変換できる場合があります。

新しい MDM ディクショナリ属性は許可ポリシーで使用可能です。

サポートされる MDM サーバ

サポートされる MDM サーバは、次のベンダーの製品です。

- 絶対値（Absolute）
- AirWatch
- Citrix XenMobile
- Globo
- Good Technology
- IBM MaaS360
- JAMF ソフトウェア
- Meraki SM/EMM
- MobileIron

（注） 一部のバージョンの MobileIron は ISE では動作しません。MobileIron はこの問題を認識しており、修正があります。詳細については、MobileIron までご連絡ください。

- SAP Afaria
- SOTI
- Symantec
- Tangoe
- Microsoft Intune - モバイル デバイス用
- Microsoft SCCM -デスクトップ デバイス用

ISE コミュニティ リソース

How To: Meraki EMM / MDM Integration with ISE

MDM サーバにより使用されるポート

次の表に、相互に通信ができるように Cisco ISE と MDM サーバ間で開く必要のあるポートを示します。MDM エージェントおよびサーバで開く必要があるポートのリストについては、MDM サーバのドキュメントを参照してください。

表 *128 : MDM* サーバにより使用されるポート

MDM サーバ	ポート
MobileIron	443
Zenprise	443
Good	19005
Airwatch	443
Afaria	443
Fiberlink MaaS	443
Meraki	443
Microsoft Intune	80 および 443
Microsoft SCCM	80 および 443

MDM 統合プロセス フロー

ここでは、MDM 統合プロセスについて説明します。

1. ユーザはデバイスを SSID に関連付けます。
2. Cisco ISE は、MDM サーバに対して API コールを実行します。
3. この API コールは、このユーザのデバイスとデバイスのポスチャ ステータスのリストを戻します。

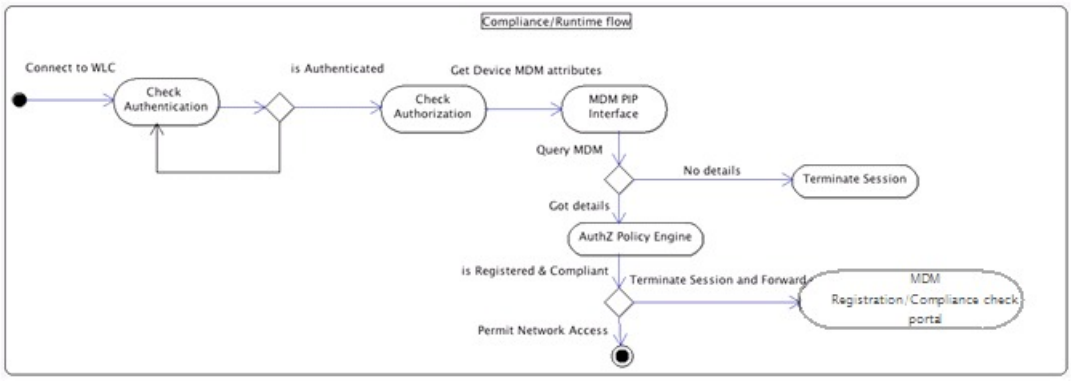
（注） 入力パラメータは、エンドポイントデバイスの MAC アドレスです。オフプレミスの Apple iOS デバイス（VPN 経由で Cisco ISE に接続するデバイス）の場合、これは UDID です。

4. ユーザのデバイスがこのリストにない場合、デバイスが登録されていないことを意味します。Cisco ISE は、Cisco ISE にリダイレクトされる許可要求を NAD に送信します。ユーザが MDM サーバ ページに表示されます。

（注） MDM ポータルを介して Cisco ISE ネットワークの外の MDM サーバに登録済みのデバイスを登録する必要があります。これは Cisco ISE、リリース 1.4 以降に適用されます。ISE の以前のバージョンでは、Cisco ISE ネットワークの外に登録済みのデバイスはポスチャ ポリシーに準拠している場合に自動的に登録されます。

5. Cisco ISE は、MDM を使用してデバイスをプロビジョニングし、デバイスを登録するための適切なページをユーザに表示します。
6. ユーザは MDM サーバにデバイスを登録し、MDM サーバは Cisco ISE に要求をリダイレクトします（自動リダイレクションまたは手動のブラウザ リフレッシュによって）。
7. Cisco ISE は MDM サーバに対して再度ポスチャ ステータスのクエリーを実行します。
8. ユーザのデバイスが MDM サーバで設定されているポスチャ（コンプライアンス）ポリシーに準拠していない場合、デバイスがポリシーに準拠しておらず、準拠する必要があることがユーザに通知されます。
9. ユーザのデバイスがポリシーに準拠するようになった後、MDM のサーバは内部テーブルのデバイスのステータスを更新します。
10. ここでユーザがブラウザをリフレッシュすると、制御が Cisco ISE に返されます。
11. Cisco ISE はコンプライアンス情報を取得するために MDM サーバを 4 時間ごとにポーリングし、必要に応じて許可変更（CoA）を発行します。これは管理者が設定できます。また、Cisco ISE は 5 分ごとに MDM サーバをチェックして使用できるかどうかを確認します。

次の図は、MDM プロセス フローを示しています。



（注） 一度に 1 つの MDM サーバに登録できるデバイスは 1 台のみです。別のベンダーから MDM サービスに同じデバイスを登録する場合、デバイスから前のベンダーのプロファイルを削除する必要があります。MDM サービスは通常、「企業ワイプ」を提供し、これはデバイスからベンダーの設定のみを削除します（デバイス全体ではありません）。ユーザはこのファイルを削除することもできます。たとえば、IOS デバイスで、[設定（Settings）] > [全般（General）] > [デバイス管理（Device management）] の順に移動し、削除の管理をクリックすることができます。または、ISE の MyDevices ポータルに移動し、企業ワイプをクリックすることができます。

Cisco ISE による MDM サーバの設定

Cisco ISE で MDM サーバを設定するには、次の高レベル タスクを実行します。

ステップ 1 Azure に PAN の証明書をインポートする Intune を除き、Cisco ISE に MDM のサーバ証明書をインポートします。

ステップ 2 Mobile Device Manager の定義を作成します。

ステップ 3 ワイヤレス LAN コントローラの ACL を設定します。

ステップ 4 MDM サーバに未登録のデバイスをリダイレクトするための許可プロファイルを設定します。

ステップ 5 ネットワークに複数の MDM サーバがある場合は、各ベンダーに個別の許可プロファイルを設定します。

ステップ 6 MDM 使用例の許可ポリシー ルールを設定します。

Cisco ISE への MDM サーバ証明書のインポート

Cisco ISE を MDM サーバに接続するには、Cisco ISE 証明書ストアに MDM サーバ証明書をインポートする必要があります。MDM サーバに CA 署名付き証明書がある場合は、Cisco ISE 証明書ストアにルート CA をインポートする必要があります。

（注） Microsoft Azure の場合は、ISE 証明書を Azure にインポートします。詳細については、MDM サーバとしての Microsoft Intune の設定 （950 ページ）を参照してください。

ステップ 1 MDM サーバ証明書を MDM サーバからエクスポートして、ローカル マシンに保存します。

ステップ 2 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificate）] > [インポート（Import）]** を選択します。

ステップ 3 [参照（Browse）] をクリックして、MDM サーバから取得した MDM サーバ証明書を選択します。

ステップ 4 わかりやすい名前を追加します。

ステップ 5 [ISE内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにします。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 [証明書ストア（Certificate Store）] リスト ページに MDM サーバ証明書が一覧表示されることを確認します。

次のタスク

ISE でのモバイル デバイス管理サーバの定義 （946 ページ）

。

ISE でのモバイル デバイス管理サーバの定義

外部 MDM サーバ用のモバイル デバイス管理（MDM）定義とデスクトップ デバイス マネージャ（SCCM）定義を 1 つ以上作成できます。

1. **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [外部 MDM（External MDM）]** の順に選択します。
2. [追加（Add）] をクリックします。
3. 追加する MDM サーバの名前と説明を入力します。
4. [サーバ タイプ（Server Type）] で、[モバイル デバイス マネージャ（Mobile Device Manager）] または [デスクトップ デバイス マネージャ（Desktop Device Manager）] を選択します。どちらを選択するかで、どのフィールドが次に表示されるかが決定します。[デスクトップ デバイス マネージャ（Desktop Device Manager）] を選択した場合は、「デスクトップ デバイス管理 （971 ページ）」に進みます。[モバイルデバイス マネージャ（Mobile Device Manager）] を選択した場合は、次の手順を続行します。
5. [認証タイプ（Authentication Type）] で、[ベーシック（Basic）] または [OAuth - クライアント クレデンシャル（OAuth - Client Credentials）] を選択します。Microsoft Intune サーバを設定する [OAuth -クライアント クレデンシャル（OAuth - Client Credentials）] を選択した場合は、「モバイル デバイス管理 - OAuth - クライアント クレデンシャル（Mobile Device Management - OAuth - Client Credentials） （970 ページ）」に進みます。[ベーシック（Basic）] を選択した場合は、次の手順を続行します。
6. すべての画面で、MDM サーバ定義の名前と説明が求められます。ここでは、サーバと認証タイプに基づいて、その他のフィールドと手順について説明しています。

モバイル デバイス管理：ベーシック

- ホスト名/IPアドレス（Host Name / IP Address）：MDM サーバのホスト名または IP アドレスを入力します。
- ポート（Port）：MDM サーバとの接続に使用するポートを入力します。通常は 443。

- インスタンス名（Instance Name）：この MDM サーバに複数のインスタンスがある場合に、接続するインスタンスを入力します。
- ポーリング間隔（Polling Interval）：Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報を確認するためのポーリング間隔（分単位）を入力します。MDM サーバ上のポーリング間隔に一致するようにこの値を設定します。有効な範囲は15～1440分です。デフォルト値は240分です。ネットワーク上の少数のアクティブ クライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブ クライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。

  ポーリング間隔を0に設定すると、ISEはMDMサーバとの通信をディセーブルにします。
- 準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）：エンドポイントが認証または再認証されるときに、ISE はそのエンドポイントの MDM 変数を取得するのにキャッシュを使用します。キャッシュされた値が [準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）] の値よりも古い場合、ISE は新しい値を取得するために、MDM サーバへのデバイス クエリを作成します。準拠ステータスが変更されると、ISE は CoA をトリガーします。

  有効な範囲は 1 ～ 1440 分です。デフォルト値は 1 分です。

モバイル デバイス管理 - OAuth - クライアント クレデンシャル（Mobile Device Management - OAuth - Client Credentials）

OAuth を使用するには、OAuth サーバの設定が必要です。これについては、次で説明します。MDM サーバとしての Microsoft Intune の設定 （950 ページ）

- 自動検出URL（Auto Discovery URL）：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph APIエンドポイント（Microsoft Azure AD Graph API Endpoint）] の値を入力します。この URL は、アプリケーションが Graph API を使用して Microsoft Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>` です。
- クライアントID（Client ID）：アプリケーションの固有識別子。アプリケーションが、Microsoft Azure AD Graph API、Microsoft Intune API などの他のアプリケーションのデータにアクセスする場合に、この属性を使用します。
- トークン発行URL（Token Issuing URL）：前のステップの [OAuth2.0認証エンドポイント（Oauth2.0 Authorization Endpoint）] の値を入力します。これは、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション（ISE）にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。

- トークン対象者（Token Audience）：トークンが対象とする受信者リソース。パブリックの既知の Microsoft Intune API の APP ID URL。
- ポーリング間隔（Polling Interval）：Cisco ISE が MDM サーバをポーリングしてコンプライアンス チェック情報を確認するためのポーリング間隔（分単位）を入力します。MDM サーバ上のポーリング間隔に一致するようにこの値を設定します。有効な範囲は15～1440分です。デフォルト値は240分です。ネットワーク上の少数のアクティブ クライアントをテストする場合のみポーリング間隔を 60 分未満に設定することを推奨します。多くのアクティブ クライアントを持つ実稼働環境でこの値を 60 分未満に設定すると、システムの負荷が大幅に増加し、パフォーマンスに悪影響を与える場合があります。

  ポーリング間隔を0に設定すると、ISEはMDMサーバとの通信をディセーブルにします。
- 準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）：エンドポイントが認証または再認証されるときに、ISE はそのエンドポイントの MDM 変数を取得するのにキャッシュを使用します。キャッシュされた値が [準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）] の値よりも古い場合、ISE は新しい値を取得するために、MDM サーバへのデバイス クエリを作成します。準拠ステータスが変更されると、ISE は CoA をトリガーします。

  有効な範囲は 1 ～ 1440 分です。デフォルト値は 1 分です。

デスクトップ デバイス管理

次の設定では、ISE と通信できるように SCCM サーバの WMI を設定する必要があります。詳細については、ISE 用の Microsoft SCCM サーバの設定 （954 ページ）を参照してください。

- ホスト名/IPアドレス（Host Name / IP Address）：MDM サーバのホスト名または IP アドレスを入力します。
- サイトまたはインスタンス名（Site or Instance Name）：サイト名または、MDM サーバに複数のインスタンスがある場合はインスタンス名を入力します。

Microsoft Intune および SCCM のための ISE MDM サポート

- **Microsoft Intune**：MDM-ISE はパートナー MDM サーバ管理モバイル デバイスとして、Microsoft の Intune デバイス管理をサポートします。

  Intune サーバ管理モバイル デバイスの OAuth 2.0 クライアント アプリケーションとして ISE を設定します。ISE は、Azure からトークンを取得し、ISE Intune アプリケーションとのセッションを確立します。

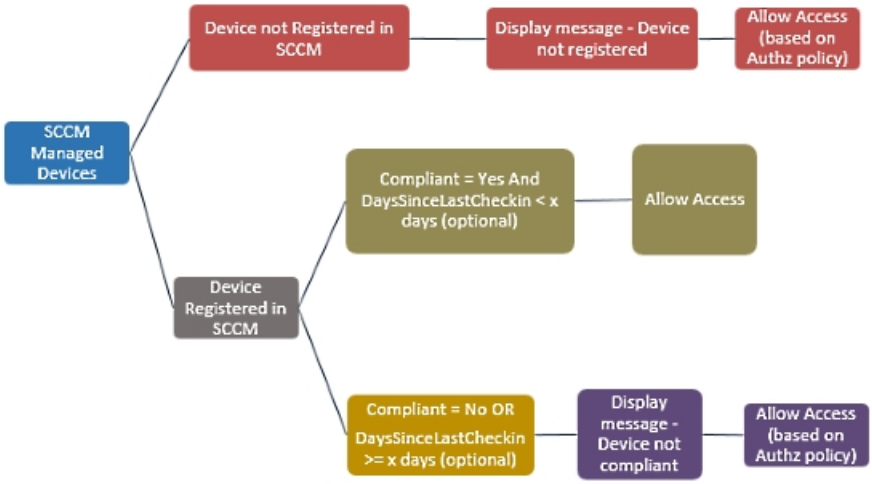
  Intune がクライアント アプリケーションとどのように通信するかについての詳細は、https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx を参照してください。
- **デスクトップ デバイス マネージャ（Microsoft SCCM）**：ISE は Microsoft System Center Configuration Manager（SCCM）を Windows コンピュータの管理用パートナー MDM サーバとしてサポートします。ISE は、WMI を使用してコンプライアンス情報を SCCM サー

バから取得し、その情報を使用してユーザの Windows デバイスへのネットワーク アクセスを許可または拒否します。

SCCM のワークフロー

ISE はデバイスが登録されているかについて、また登録済みの場合は準拠しているかどうかについて SCCM サーバから情報を取得できます。次の図に、SCCM により管理されるデバイス用のワークフローを示します。

図 *49 : SCCM* のワークフロー



デバイスを接続し、SCCM ポリシーが一致すると、ISE はコンプライアンスと最終ログイン（チェックイン）時間を取得するために、許可ポリシーで指定されている SCCM サーバを照会します。この情報を使用して、ISE はエンドポイントのリストのデバイスのコンプライアンス ステータスと lastCheckinTimeStamp を更新します。

デバイスが準拠していないか SCCM に登録されていない、およびリダイレクト プロファイルが許可ポリシーで使用されている場合、デバイスが準拠していないか SCCM に登録されていないというメッセージがユーザに表示されます。ユーザがメッセージを受け取った後、ISE は SCCM 登録サイトへ CoA を発行できます。承認ポリシーおよびプロファイルに基づいてユーザにアクセスを許可できます。

Microsoft SCCM サーバ接続の監視

ポーリングは SCCM 用に設定できません。

ISE は、SCCM サーバへの接続を検証し、ISE が SCCM サーバへの接続を失うとアラームを発生させる、MDM ハートビート ジョブを実行します。ハートビート ジョブの間隔は設定できません。

MDM サーバとしての Microsoft Intune の設定

ISE の MDM サーバとして Microsoft Intune を設定することは、他の MDM サーバの設定とは少し異なります。Azure への ISE の接続および ISE への Azure の接続を設定するには、次の手順を使用します。

1. パブリック証明書を Intune/Azure Active Directory テナントから取得し、ISE にインポートして SSL ハンドシェイクをサポートします。
    1. 1. サイトがテナントを持つ Intune 管理コンソールまたは Azure 管理コンソールにログオンします。
    2. ブラウザを使用して証明書の詳細を取得します。たとえば、Internet Explorer の場合は次のように操作します。
        1. ブラウザのツールバーのロック シンボルをクリックしてから、[証明書の表示（View Certficates）] をクリックします。
        2. [証明書（Certificate）] ウィンドウで、[認証パス（Certification Path）] タブを選択します。
        3. Baltimore Cyber Trust ルートを見つけて、そのルート証明書をエクスポートします。
    3. ISE で、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** の順に選択し、保存したルート証明書をインポートします。証明書に Azure MDM などのわかりやすい名前を付けます。
2. ISE 自己署名証明書をエクスポートし、InTune/Azure 用に準備をします。
    1. PAN で、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** の順に移動し、デフォルトの自己署名サーバ証明書を選択して、[エクスポート（Export）] をクリックします。
    2. [証明書のみエクスポート（Export Certificate Only）]（デフォルト）を選択し、保存する場所を選択します。

    エクスポートされた証明書ファイルに次の PowerShell スクリプトを実行します。

    ```
    $cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
    $cer.Import("mycer.cer")
    $bin = $cer.GetRawCertData()
    $base64Value = [System.Convert]::ToBase64String($bin)

    $bin = $cer.GetCertHash()
    $base64Thumbprint = [System.Convert]::ToBase64String($bin)

    $keyid = [System.Guid]::NewGuid().ToString()
    ```

    次の手順で使用するため、**$base64Thumbprint、$base64Value、$keyid** の値をメモしておきます。
3. Intune で ISE アプリケーションを作成します。

1. Microsoft Azure 管理ポータルで顧客ドメインにサインインし、**[ディレクトリ（Directory）]**>**[アプリケーション（Applications）]**>**[アプリケーションの追加（Add an Application）]** に移動して、[自分の組織が開発中のアプリケーションの追加（Add an application my organization is developing）] を選択します。
2. 次のパラメータを使用して、Azure で ISE アプリケーションを設定します。
   - アプリケーション名（Application Name）：**ISE** と入力します。
   - [Web アプリケーションまたは Web アプリ（WEB APPLICATION AND/OR WEB APP）] を選択します。
   - サインオン URL およびアプリ ID URL（SIGN-ON URL and APP ID URL）：任意の有効な URL を追加します。この値は ISE では使用されません。

4. Azure からマニフェスト ファイルを取得し、ISE 証明書情報を追加して、更新されたマニフェストを Azure にアップロードします。
   1. Microsoft Azure 管理ポータル（https://manage.windowsazure.com）で、AAD スナップインを開き、ISE アプリケーションに移動します。

   [マニフェストの管理（Manage Manifest）] メニューからアプリケーション マニフェスト ファイルをダウンロードします。
5. *Base64 Encoded String of ISE PAN cert* を、PowerShell スクリプトの $base64Value である、エクスポートされ編集された ISE からの証明書ファイルと置き換えて、次の例のようにマニフェスト json ファイルの [keyCredentials] フィールドを更新します。

```
"keyCredentials": [
                                {
                               "customKeyIdentifier": "$base64Thumbprint_from_above",

                                  "keyId": "$keyid_from_above",
                                  "type": "AsymmetricX509Cert",
                                  "usage": "Verify",
                                  "value": "Base64 Encoded String of ISE PAN cert"
                                }
                            ]
```

（注） マニフェスト ファイルの名前は変更しないようにします。

KeyCredentials の複雑なタイプは、http://msdn.microsoft.com/en-us/library/azure/dn151681.aspx でドキュメント化されています。

6. Azure に更新されたマニフェスト ファイルをアップロードします。
7. Microsoft Azure 管理ポータルで、アプリ エンドポイントのリストに移動します。次のエンドポイント属性の値を使用して ISE を設定します。
   - MICROSOFT AZURE AD GRAPH API ENDPOINT
   - OAUTH 2.0 TOKEN ENDPOINT

8. ISE で、ISE の Intune サーバを設定します。設定と外部 MDM サーバの詳細については、ISE でのモバイル デバイス管理サーバの定義 （946 ページ）を参照してください。Intune にとって重要なフィールドは次のとおりです。

   - 自動検出URL（Auto Discovery URL）：Microsoft Azure 管理ポータルの [Microsoft Azure AD Graph APIエンドポイント（Microsoft Azure AD Graph API Endpoint）] の値を入力します。この URL は、アプリケーションが Graph API を使用して Microsoft Azure AD ディレクトリのデータに直接アクセスできるエンドポイントです。URL の形式は `https://<hostname>/<tenant id>`、たとえば、`https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329` です。この URL の拡大バージョンもプロパティ ファイルに含まれます。形式は、`https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>` です。
   - クライアントID（Client ID）：アプリケーションの固有識別子。アプリケーションが、Microsoft Azure AD Graph API、Microsoft Intune API などの他のアプリケーションのデータにアクセスする場合に、この属性を使用します。
   - トークン発行URL（Token Issuing URL）：前のステップの [OAuth2.0認証エンドポイント（Oauth2.0 Authorization Endpoint）] の値を入力します。これは、アプリケーションが OAuth2.0 を使用してアクセス トークンを取得できるエンドポイントです。アプリケーションが認証されると、Microsoft Azure AD はアプリケーション（ISE）にアクセス トークンを発行します。このトークンを使用するとアプリケーションから Graph API/Intune API を呼び出すことができます。
   - トークン対象者（Token Audience）：トークンが対象とする受信者リソース。パブリックの既知の Microsoft Intune API の APP ID URL。

Intune アプリケーションの詳細については、次のリンクを参照してください。

- https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx
- http://blogs.msdn.com/b/exchangedev/archive/2015/01/22/building-daemon-or-service-apps-with-office-365-mail-calendar-and-contacts-apis-oauth2-for-the-enterprise.aspx
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications
- https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-manifest

Microsoft SCCM のポリシー設定の例

ポリシーでは次の新しいディクショナリ エントリが使用され、SCCM をサポートすることができます。

- MDM.DaysSinceLastCheckin：ユーザが最後に確認してからの日数、または SCCM のデバイスと同期してからの日数で、1 ～ 365 日です。

- MDM.UserNotified：値は Y または N です。ユーザが登録されていないことをユーザに通知したかどうかを示します。さらに、登録ポータルへの制限付きアクセスやリダイレクトを許可し、またはアクセスを拒否できます。
- MDM.ServerType：値はモバイル デバイス マネージャの場合 MDM またはデスクトップ デバイス マネージャの場合 DM です。

次のサンプル ポリシー セットで SCCM をサポートする一連のポリシーを示します。

ポリシー名	条件（IF）	実行されるアクション（Then）
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCMRedirect
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCMRedirect

ポリシー名	条件（IF）	実行されるアクション（Then）
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

ISE 用の Microsoft SCCM サーバの設定

ISE は、WMI を使用して SCCM サーバと通信します。WMI は、SCCM を実行している Windows サーバで設定する必要があります。

（注） ISE 統合に使用するユーザ アカウントは、次のいずれかの条件を満たしている必要があります。

- SMS 管理ユーザ グループのメンバーである。
- WMI 名前空間で SMS オブジェクトと同じアクセス許可がある。

  `root\sms\site_<sitecode>`

  サイトコードは SCCM サイトです。

AD ユーザがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows 2012 および Windows 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティング システムの特定のレジストリ キーを完全に制御することができません。Active Directory の管理者は、Active Directory ユーザに次のレジストリ キーに対する完全制御権限を提供する必要があります。

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

次の Active Directory のバージョンでは、レジストリ変更は必要ありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、次に示すように、まず Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーを右クリックして [オーナー（Owner）] タブに移動します。
ステップ 2 [アクセス許可（Permissions）] をクリックします。
ステップ 3 [詳細設定（Advanced）] をクリックします。

AD ユーザがドメイン管理グループの一部ではない場合に必要な権限

Windows 2012 R2 の場合は、Active Directory ユーザに次のレジストリ キーに対する**完全制御**権限を提供します。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Active Directory ユーザがドメイン管理グループの一部ではなく、ドメイン ユーザ グループの一部である場合は、次の権限も必要です。

- ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加します（下記を参照）
- ドメイン コントローラで DCOM を使用するための権限 （627 ページ）
- WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （629 ページ）

これらの権限は、次の Active Directory のバージョンでのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ISE がドメイン コントローラに接続できるようにするレジストリ キーを追加する

ISE がドメインユーザとして接続し、ログイン認証イベントを取得できるようにするには、ドメイン コントローラに一部のレジストリ キーを手動で追加する必要があります。エージェントはドメイン コントローラまたはドメイン内のマシンでは必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキスト ファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

キー **DllSurrogate** の値には、2 つのスペースが含まれていることを確認します。

上記のスクリプトに示すように、ファイルの末尾の空の行を含む、空の行を保持してください。

ドメイン コントローラで DCOM を使用するための権限

ISE パッシブ ID サービスに使用される Active Directory ユーザは、ドメイン コントローラで DCOM（リモート COM）を使用する権限がなければなりません。**dcomcnfg** コマンド ライン ツールを使用して権限を設定できます。

ステップ 1 コマンド ラインから **dcomcnfg** ツールを実行します。

ステップ 2 [コンポーネントサービス（Component Services）] を展開します。

ステップ 3 **[コンピュータ（Computers）]** > **[マイコンピュータ（My Computer）]** を展開します。

ステップ 4 メニュー バーで [アクション（Action）] を選択して、[プロパティ（properties）] をクリックし、[COMセキュリティ（COM Security）] をクリックします。

ステップ 5 アクセスおよび起動の両方に対して ISE が使用するアカウントに許可権限があることを確認します。Active Directory ユーザは、4 つのオプション（[アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対する [制限の編集（Edit Limits）] と [デフォルトの編集（Edit Default）]）のすべてに追加される必要があります。

ステップ 6 [アクセス権限（Access Permissions）] および [起動およびアクティベーションの権限（Launch and Activation Permissions）] の両方に対してローカルおよびリモート アクセスをすべて許可します。

図 *50 : [*アクセス権限（***Access Permissions***）*]* のローカルおよびリモート アクセス

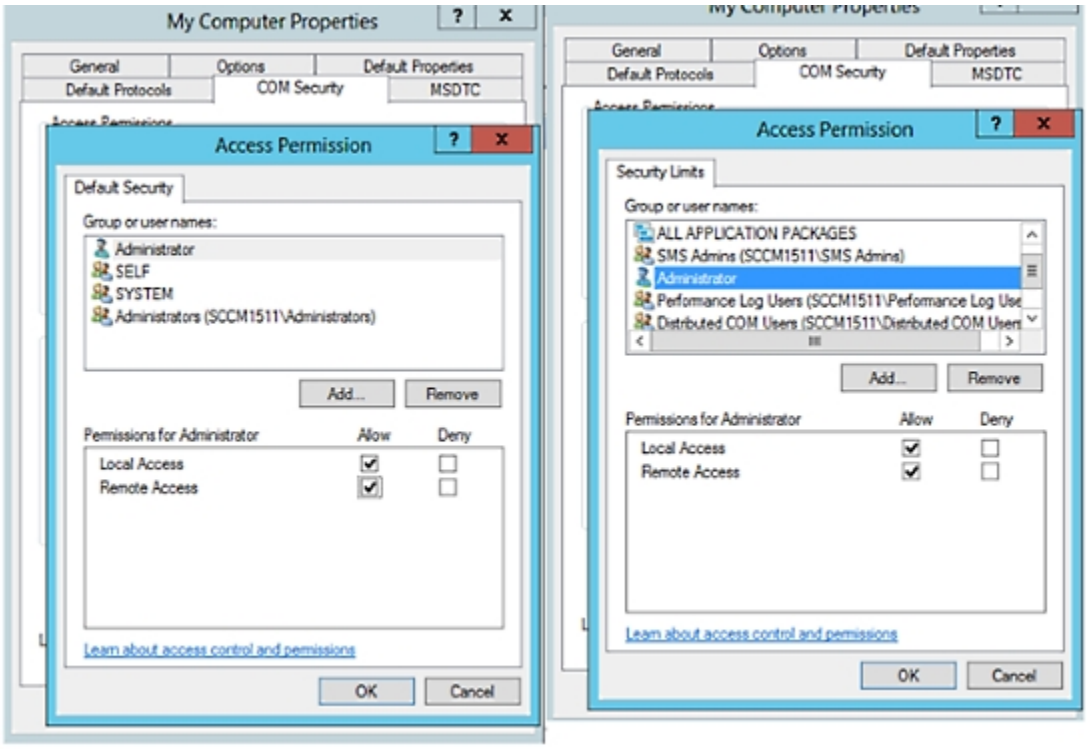
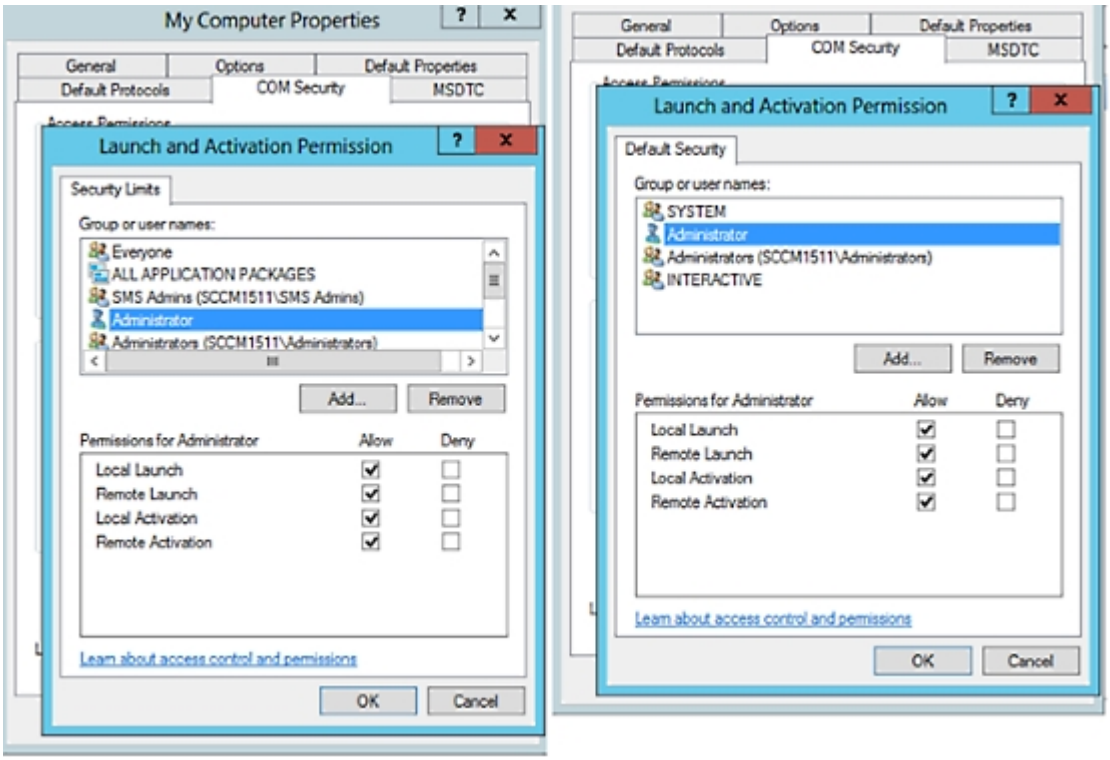


図 *51 : [*起動およびアクティベーションの権限（***Launch and Activation Permissions***）*]* のローカルおよびリモート アクセス



WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Active Directory ユーザには実行メソッドおよびリモートイネーブルのための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

ステップ 1 [スタート] > [Run] をクリックし、`wmimgmt.msc` と入力します。

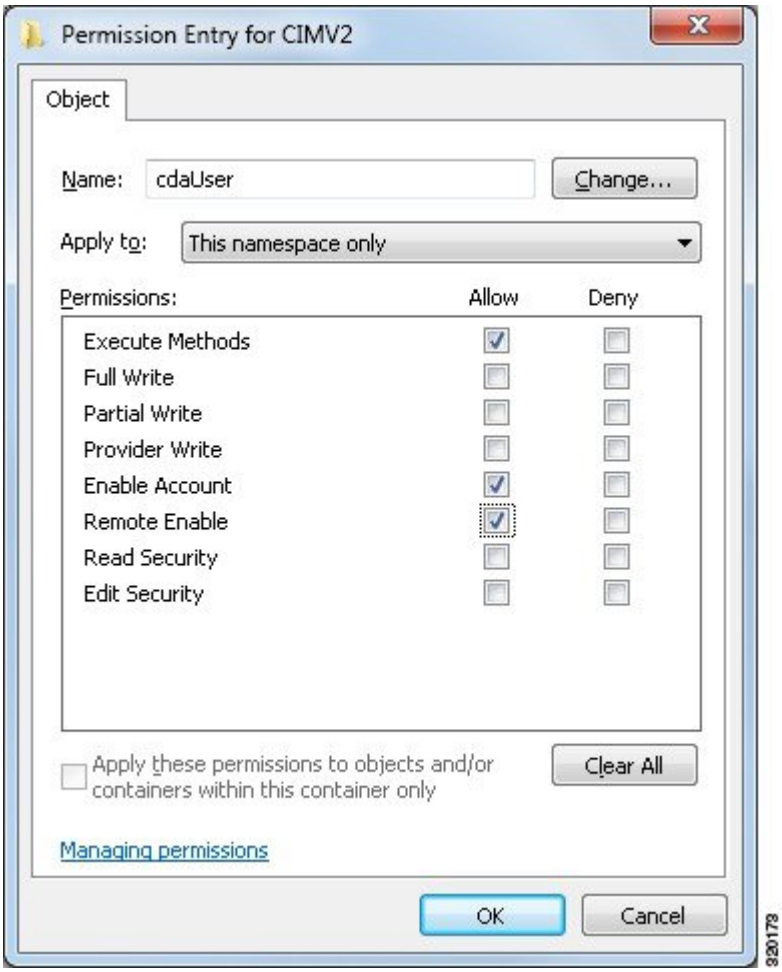
ステップ 2 [WMI Control] を右クリックし、[プロパティ] をクリックします。

ステップ 3 [セキュリティ] タブで [ルート] を展開し、[CIMV2] を選択します。

ステップ 4 [セキュリティ（Security）] をクリックします。

ステップ 5 下に示すように、Active Directory ユーザを追加し、必要な権限を設定します。

図 *52 : WMI Root\CIMv2* 名前空間に必要な権限



WMI アクセス用にファイアウォール ポートを開く

Active Directory ドメイン コントローラのファイアウォール ソフトウェアは、WMI へのアクセスをブロックすることがあります。ファイアウォールをオフにするか、または次のポートへの特定の IP（ISE IP アドレス）のアクセスを許可することができます。

- TCP 135：一般的な RPC ポート。非同期 RPC 発信をすると、このポートでリスニングしているサービスが、クライアントに、この要求を処理できるコンポーネントが使用しているポートを通知します。
- UDP 138：NetBIOS データグラム サービス
- TCP 139：NetBIOS セッション サービス
- TCP 445：SMB

（注） Cisco ISE 1.3 以降は SMB 2.0 をサポートします。

数値の大きいポートは動的に割り当てられ、手動で設定できます。ターゲットとして %SystemRoot%\System32\dllhost.exe を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォール ルールを、特定の IP アドレス（ISE IP）に割り当てることができます。

未登録のデバイスのリダイレクトのための許可プロファイルの設定

各外部 MDM サーバの未登録のデバイスをリダイレクトするには、Cisco ISE で許可プロファイルを設定する必要があります。

始める前に

- Cisco ISE で MDM サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、MDM ディクショナリ属性を使用して許可ポリシーを作成できます。
- 未登録のデバイスをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。
- インターネット接続にプロキシを使用していて、MDM サーバが内部ネットワークの一部である場合は、プロキシ バイパス リストに MDM サーバ名または IP アドレスを追加する必要があります。**[管理（Administration）] > [設定（Settings）] > [プロキシ設定（Proxy Settings）]**の順に選択して、このアクションを実行します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）] > [追加（Add）]** を選択します。

ステップ 2 準拠していないまたは登録されていない未登録デバイスをリダイレクトするための許可プロファイル作成します。

ステップ 3 MDM サーバ名と一致する許可プロファイルの名前を入力します。

ステップ 4 アクセス タイプとして ACCESS_ACCEPT を選択します。

ステップ 5 [Web リダイレクション（Web Redirection）] チェックボックスをオンにし、ドロップダウン リストから [MDM リダイレクト（MDM Redirect）] を選択します。

ステップ 6 ワイヤレス LAN コントローラ上で設定した ACL の名前を [ACL] フィールドに入力します。

ステップ 7 [値（Value）] ドロップダウン リストから MDM ポータルを選択します。

ステップ 8 ドロップダウン リストから、使用する MDM サーバを選択します。

ステップ 9 [送信（Submit）] をクリックします。

次のタスク

MDM 使用例の許可ポリシー ルールの設定。

MDM 使用例の許可ポリシー ルールの設定

MDM 設定を完了するには、Cisco ISE で許可ポリシー ルールを設定する必要があります。

始める前に

- Cisco ISE 証明書ストアに MDM サーバ証明書を追加します。
- Cisco ISE で MDM サーバ定義を作成したことを確認します。正常に MDM サーバと ISE を統合した後に限り、MDM ディクショナリにデータが入力され、MDM ディクショナリ属性を使用して許可ポリシーを作成できます。
- 未登録のデバイスまたは非準拠のデバイスをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択し、許可ポリシー ルールを表示するポリシー セットを展開します。

ステップ 2 次のルールを追加します。

- [MDM_Un_Registered_Non_Compliant]：MDM サーバに登録されていないか、MDM ポリシーに準拠していないデバイスの場合。要求がこのルールに一致すると、ISE MDM ページが表示され、MDM でのデバイスの登録に関する情報が示されます。
- [PERMIT]：デバイスが Cisco ISE および MDM に登録されており、Cisco ISE および MDM ポリシーに準拠している場合、Cisco ISE で設定されたアクセス コントロール ポリシーに基づいてネットワークへのアクセス権が付与されます。

  次の図は、この設定の例を示します。

  図 *53 : MDM* の使用例の許可ポリシー ルール

ステップ 3 **[保存（Save）]** をクリックします。

MDM Interoperability のためのワイヤレス LAN コントローラでの ACL の設定

未登録のデバイスおよび証明書プロビジョニングをリダイレクトするために許可ポリシーで使用する ACL をワイヤレス LAN コントローラで設定します。ACL は次の順序にする必要があります。

ステップ 1 サーバからクライアントへのすべての発信トラフィックを許可します。

ステップ 2 （任意）トラブルシューティングのためにクライアントからサーバへの ICMP 着信トラフィックを許可します。

ステップ 3 未登録および非準拠のデバイスが MDM エージェントをダウンロードし、コンプライアンス チェックに進むように MDM サーバへのアクセスを許可します。

ステップ 4 Web ポータルおよびサプリカント用 ISE、および証明書プロビジョニング フローに対するクライアントからサーバへのすべての着信トラフィックを許可します。

ステップ 5 名前解決のためにクライアントからサーバへの着信 DNS トラフィックを許可します。

ステップ 6 IP アドレスのためにクライアントからサーバへの着信 DHCP トラフィックを許可します。

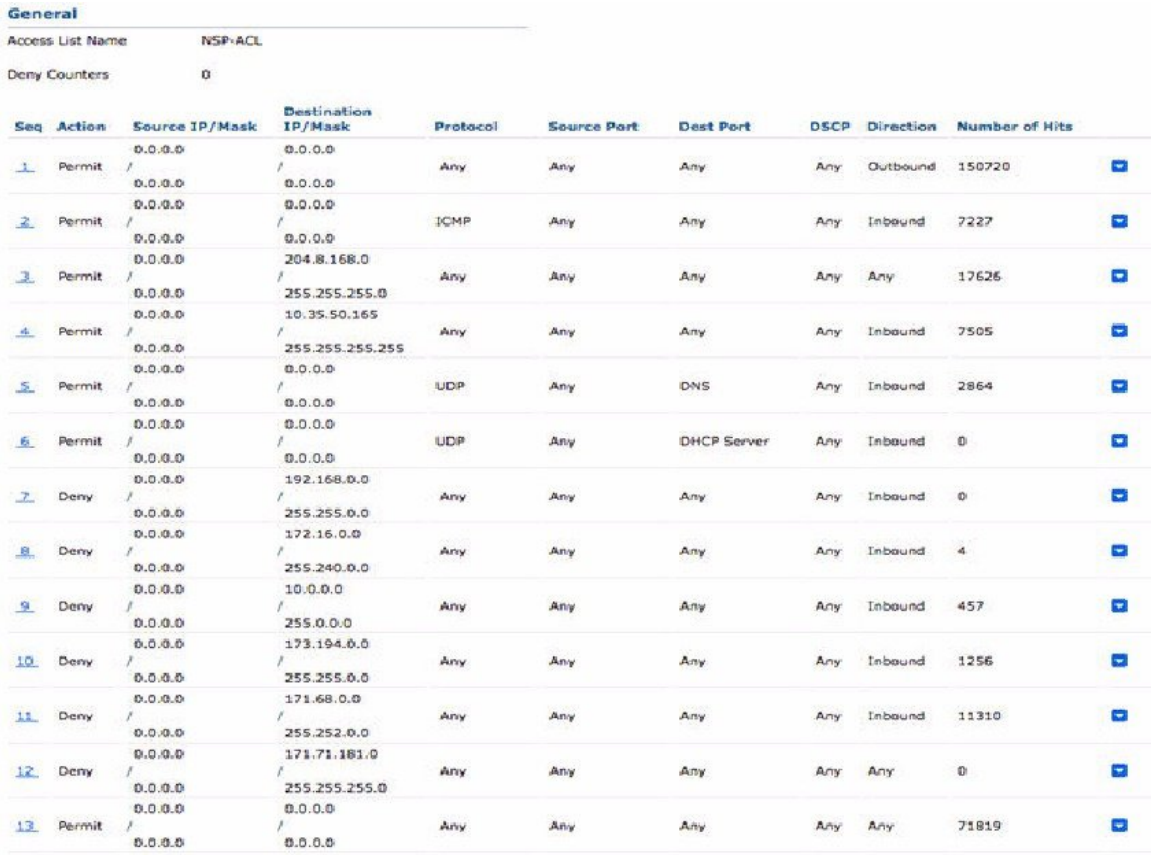
ステップ 7 ISE へのリダイレクションのための、クライアントからサーバへの企業リソースに対するすべての着信トラフィックを（会社のポリシーに応じて）拒否します。

ステップ 8 （任意）残りのトラフィックを許可します。

例

次の例では、未登録のデバイスを BYOD フローにリダイレクトするための ACL を示しています。この例では、Cisco ISE IP アドレスは 10.35.50.165 で、社内ネットワークの IP アドレスは 192.168.0.0 および 172.16.0.0（リダイレクト用）で、MDM サーバ サブネットは 204.8.168.0 です。

図 *54 :* 登録されていないデバイスをリダイレクトするための *ACL*



General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

デバイスのワイプまたはロック

Cisco ISE では、失われたデバイスをワイプしたり、PIN ロックをオンにしたりできます。これは [エンドポイント（Endpoints）] ページから行うことができます。

ステップ 1 **[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

ステップ 2 ワイプまたはロックするデバイスの横にあるチェックボックスをオンにします。

ステップ 3 [MDM アクセス（MDM Access）] ドロップダウン リストから、次のオプションのいずれかを選択します。

- [完全ワイプ（Full Wipe）] : このオプションを使用すると、MDM ベンダーに応じて、企業アプリケーションが削除されるか、またはデバイスが工場出荷時の設定にリセットされます。
- [企業ワイプ（Corporate Wipe）] : MDM サーバ ポリシーで設定したアプリケーションを削除します
- [PIN ロック（PIN Lock）] : デバイスをロックします

ステップ 4 [はい（Yes）] をクリックして、デバイスをワイプまたはロックします。

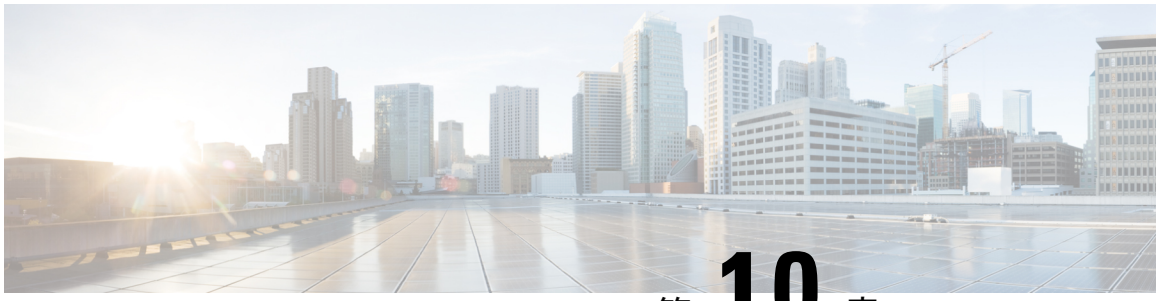
Mobile Device Manager のレポートの表示

Cisco ISE では、MDM サーバ定義のすべての追加、更新、および削除を記録します。これらのイベントは、選択された期間での任意のシステム管理者によるすべての設定変更を報告する「変更設定監査」レポートで表示できます。

[操作（Operations）] > [レポート（Reports）] > [変更設定監査（Change Configuration Audit）] > [MDM] を選択し、結果のレポートで表示する期間を指定します。

Mobile Device Manager のログの表示

[メッセージ カタログ（Message Catalog）] ページを使用して、Mobile Device Manager のログ メッセージを表示できます。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージカタログ（Message Catalog）]** を選択します。MDM ログ エントリのデフォルトのレポーティング レベルは「INFO」です。レポーティング レベルを「DEBUG」または「TRACE」に変更できます。



第 10 章

セグメンテーション

ポリシー セット

Cisco ISE はポリシーベースのネットワークアクセス制御ソリューションで、ネットワーク アクセスポリシーセットを提供し、ワイヤレス、有線、ゲスト、およびクライアントプロビジョニングなど、さまざまなネットワーク アクセスの使用例を管理できます。ポリシー セット（ネットワーク アクセスとデバイス管理の両方のセット）を使用すると、認証および許可ポリシーを論理的に同じセットにグループ化することができます。ロケーション、アクセス タイプ、類似パラメータに基づくポリシー セットなどの領域に基づいて、複数のポリシー セットを作成できます。ISE をインストールすると、デフォルトのポリシー セットであるポリシーセットが常に 1 つ定義され、デフォルトのポリシーセットには、事前定義されたデフォルトの認証、許可、および例外のポリシー ルールが含まれています。

ポリシーセットを作成するときは、ネットワーク アクセス サービスはポリシーセット レベルで、ID ソースは認証ポリシー レベルで、ネットワーク許可は許可ポリシー レベルで選択するように、（条件および結果で設定された）これらのルールを設定できます。さまざまなベンダーに対し、Cisco ISE 対応ディクショナリからの属性のいずれかを使用して、1 つまたは複数の条件を定義できます。Cisco ISE では、再利用可能な個別のポリシー要素として条件を作成できます。

ネットワーク デバイスと通信するためにポリシー セットごとに使用されるネットワーク アクセス サービスは、そのポリシー セットの最上位レベルで定義されます。ネットワーク アクセス サービスには次のものがあります。

- 許可されたプロトコル：初期要求とプロトコル ネゴシエーションを処理するように設定されたプロトコル
- プロキシ サービス：処理のために外部 RADIUS サーバに要求を送信します

（注） [デバイス管理（Device Administration）] ワーク センターから、ポリシー セットに関連する TACACS サーバ順序を選択することもできます。TACACS サーバ順序を使用して、一連の TACACS プロキシ サーバを処理用に設定します。

[ポリシーセット（Policy Set）]テーブルから確認できるポリシーセットの最上位レベルのルールが、セット全体に適用され、残りのポリシーと例外のルールの前に一致している場合、ポリシー セットは階層的に構成されています。その後、セットのルールが次の順序で適用されます。

1. 認証ポリシー ルール
2. ローカル ポリシー例外
3. グローバル ポリシー例外
4. 許可ポリシー ルール

（注） ポリシーセットの機能は、ネットワーク アクセスとデバイス管理ポリシーの場合と同じです。この章で説明するすべてのプロセスは、[ネットワーク アクセス（Network Access）]および[デバイス管理（Device Administration）] ワーク センターの両方で作業する場合に適用できます。この章では、[ネットワーク アクセス（Network Access）] ワーク センターのポリシー セットについて具体的に説明します。このワーク センターをアクセスするには、**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ポリシー セット（Policy Sets）]** を選択します。

ISE コミュニティ リソース

WLC からの RADIUS 結果の使用については、「WLC Called-Station-ID（RADIUS 認証とアカウンティングの設定）（WLC Called-Station-ID (Radius Authentication and Accounting Config)）」を参照してください。

ポリシー セットの構成時の設定

次の表では、[ポリシーセット（Policy Sets）] ウィンドウのフィールドについて説明します。このフィールドから、認証、例外、および許可ポリシーを含むポリシーセットを設定できます。ネットワーク アクセス ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ポリシー セット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシー セット（Device Admin Policy Sets）]** を選択します。

表 *129 :* ポリシー セットの構成時の設定

フィールド名	使用上のガイドライン
[ステータス（Status）]	このポリシーのステータスを選択します。次のいずれかを設定できます。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニタのみ（Monitor Only）]：このポリシー条件は評価されません。
ポリシー セット名	このポリシー セットの一意の名前を入力します。

フィールド名	使用上のガイドライン
条件（**Conditions**）	新しいポリシー行から、プラス（+）アイコンをクリックするか、既存のポリシー行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
説明	ポリシーの一意の説明を入力します。
許可されているプロトコルまたはサーバ順序（**Allowed Protocols or Server Sequence**）	すでに作成した許可されているプロトコルを選択するか、または（+）記号をクリックして [新しい許可されているプロトコルを作成（Create a New Allowed Protocol）] するか、[新しいRADIUS順序を作成（Create a New Radius Sequence）] するか、または [TACACS 順序を作成（Create a TACACS Sequence）] します。
条件（**Conditions**）	新しい例外行から、プラス（+）アイコンをクリックするか、既存の例外行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
ヒット数（**Hits**）	ヒット数は、条件が一致した回数を示す診断ツールです。このアイコンが最後に更新された時刻を表示し、ゼロにリセットし、更新の頻度を表示するには、アイコンにカーソルを合わせます。

フィールド名	使用上のガイドライン
アクション	さまざまなアクションを表示して選択するには、[アクション（Actions）] 列の歯車アイコン をクリックします。 • [上に新しい行を挿入（Insert new row above）] : [アクション（Actions）] メニューを開いたポリシーの上に新しいポリシーを挿入します。 • [下に新しい行を挿入（Insert new row below）] : [アクション（Actions）] メニューを開いたポリシーの下に新しいポリシーを挿入します。 • [上に複製（Duplicate above）] : 元のセットの上に、[アクション（Actions）] メニューを開いたポリシーの上に複製ポリシーを挿入します。 • [下に複製（Duplicate below）] : 元のセットの下に、[アクション（Actions）] メニューを開いたポリシーの下に複製ポリシーを挿入します。 • [削除（Delete）] : ポリシーセットを削除します。
表示（View）	矢印アイコンをクリックすると、特定のポリシーセットの [設定（Set）] ビューが開き、認証、例外、および許可のサブポリシーが表示されます。

認証ポリシー

各ポリシーセットには、そのセットの認証ポリシーを表す複数の認証ルールを含めることができます。認証ポリシーの優先順位は、（[認証ポリシー（Authentication Policy）] 領域の [設定（Set）] ビュー ページから）ポリシー セット自体に表示されるポリシーに対する順序に基づいて決定されます。

Cisco ISE は、ポリシー セット レベルで設定された設定に基づいて、ネットワーク アクセス サービス（許可されたプロトコルまたはサーバ順序のいずれか）を動的に選択し、その後、認証ポリシー レベルおよび許可ポリシー レベルから ID ソースおよび結果をチェックします。複数の条件を、Cisco ISE ディクショナリ内の任意の属性を使用して定義できます。Cisco ISE で

は、個々のポリシー要素として条件を作成し、ライブラリに保存してから、他のルールベースのポリシーに再利用することができます。

認証ポリシーの結果である ID 特定方法は、次のいずれかになります。

- アクセスを拒否：ユーザへのアクセスは拒否され、認証は実行されません。
- ID データベース：次のいずれかの単一の ID データベース。
  - 内部ユーザ
  - ゲスト ユーザ
  - 内部エンドポイント
  - Active Directory
  - Lightweight Directory Access Protocol（LDAP）データベース
  - RADIUS トークン サーバ（RSA または SafeWord サーバ）
  - 証明書認証プロファイル
- ID ソース順序：認証に使用する ID データベースの順序。

最初の Cisco ISE インストール時に実装されるデフォルト ポリシー セットには、デフォルトの ISE 認証ルールおよび許可ルールが含まれています。デフォルト ポリシー セットには、認証と許可のための追加の柔軟な組み込みルール（デフォルトではない）も含まれています。これらのポリシーにルールを追加して、組み込みルールを削除および変更できますが、デフォルト ルールを削除することはできず、デフォルト ポリシー セットを削除することはできません。

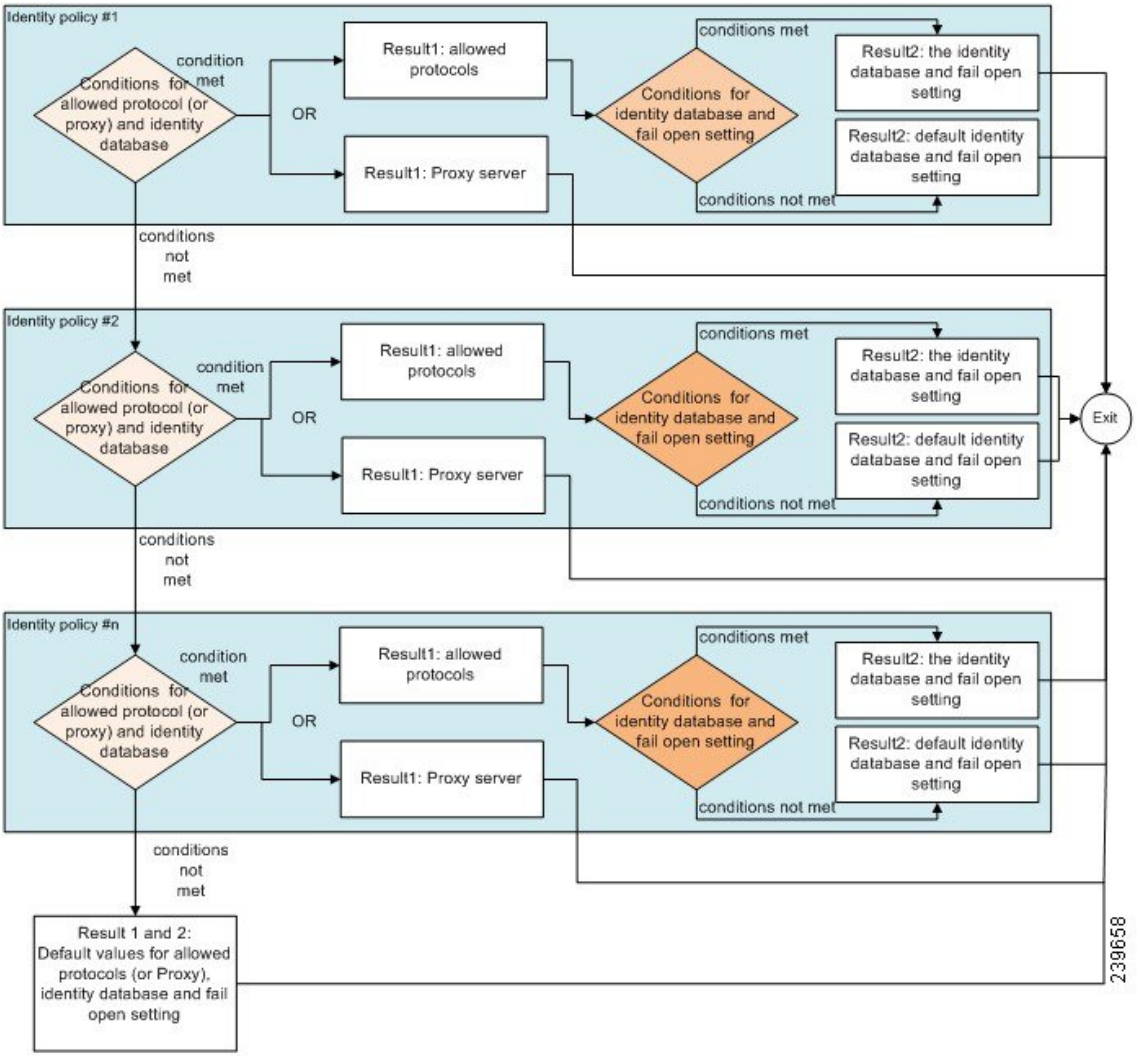
認証ポリシーのフロー

認証ポリシーでは、条件と結果で構成される複数のルールを定義できます。ISE は、指定した条件を評価し、評価の結果に基づいて、対応する結果を割り当てます。ID データベースは、基準に一致する最初のルールに基づいて選択されます。

異なるデータベースで構成される ID ソース順序を定義することもできます。Cisco ISE がデータベースを検索する順序を定義できます。Cisco ISE は、認証が成功するまで指定された順序でこれらのデータベースにアクセスします。1 つの外部データベースに同一ユーザの複数のインスタンスが存在する場合、認証は失敗します。1 つの ID ソース内で、ユーザ レコードは重複できません。

ID ソース順序には、3 つのデータベース、または多くとも 4 つのデータベースを使用することを推奨します。

図 *55 :* 認証ポリシーのフロー



認証失敗：ポリシー結果オプション

識別方法としてアクセス拒否を選択した場合、要求への応答として拒否メッセージが送信されます。ID データベースまたは ID ソース順序を選択して、認証が成功した場合、処理は同じポリシーセットに対して設定された許可ポリシーに対して続行されます。一部の認証は失敗し、その場合次のように分類されます。

- 認証の失敗：クレデンシャルが正しくない、無効なユーザであることなどが原因で認証が失敗したことを示す明確な応答を受信します。アクションのデフォルト コースは拒否です。
- ユーザが見つからない：どの ID データベースでもこのユーザが見つかりませんでした。アクションのデフォルト コースは拒否です。

- 処理の失敗：ID データベース（複数の場合もある）にアクセスできません。アクションのデフォルト コースはドロップです。

Cisco ISE では、認証失敗に対して次のアクションのコースのいずれかを設定することができます。

- [拒否（Reject）]：拒否応答が送信されます。
- [ドロップ（Drop）]：応答は送信されません。
- [続行（Continue）]：許可ポリシーに従って Cisco ISE を継続します。

[続行（Continue）] オプションを選択した場合でも、使用されているプロトコルの制限により Cisco ISE が要求の処理を実行できない場合があります。PEAP、LEAP、EAP-FAST、EAP-TLS、または RADIUS MSCHAP を使用した認証では、認証に失敗したり、ユーザが見つからなかったときには、要求の処理を続行することはできません。

認証に失敗した場合、PAP/ASCII または MAC 認証バイパス（MAB またはホスト ルックアップ）の許可ポリシーの処理を続行できます。その他のすべての認証プロトコルの場合、認証に失敗すると、次のいずれかの状態となります。

- 認証の失敗：拒否応答が送信されます。
- ユーザまたはホストが見つからない：拒否応答が送信されます。
- 処理に問題が発生：応答は送信されず、要求はドロップされます。

認証ポリシーの設定

必要に応じて、複数の認証ルールを設定および管理することによって、ポリシーセットごとに認証ポリシーを定義します。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 ネットワーク アクセス ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ポリシー セット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシー セット（Device Admin Policy Sets）]** を選択します。

ステップ 2 認証ポリシーを追加または更新するポリシーセットの行から、ポリシーセットの詳細のすべてにアクセスし、認証および許可ポリシーとポリシー例外を作成するために、[ポリシーセット（Policy Sets）]テーブルの [表示（View）] 列から > をクリックします。

ステップ 3 ページの認証ポリシー部分の横にある矢印アイコンをクリックして、テーブル内のすべての認証ポリシールールを展開して表示します。

ステップ 4 いずれかの行の[アクション（Actions）]列から、歯車アイコンをクリックします。ドロップダウンメニューから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して、新しい認証ポリシールールを挿入します。
[認証ポリシー（Authentication Policy）] テーブルに新しい行が表示されます。

ステップ 5 [ステータス（Status）] 列から、現在の [ステータス（Status）] アイコンをクリックし、ドロップダウンリストから必要に応じてポリシーセットのステータスを更新します。[ステータス（Status）]の詳細については、認証ポリシーの構成設定 （997 ページ） を参照してください。

ステップ 6 テーブル内のルールの場合は、[ルール名（Rule Name）] または [説明（Description）] のセルをクリックして、フリーテキストを変更します。

ステップ 7 条件を追加または変更するには、[条件（Conditions）] 列のセルにカーソルを合わせ、  をクリックします。[条件スタジオ（Conditions Studio）] が開きます。詳細については、ポリシー条件 （1018 ページ）を参照してください。

選択するすべての属性に「Equals」、「Not Equals」、「In」、「Not In」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現（REGEX）をサポートし、使用します。

（注） 単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数値属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。リストの場合、「in」演算子は、特定の値がリスト内に存在するかどうかをチェックします。単一文字列の場合、「in」演算子は、文字列が「equals」演算子などと同じかどうかをチェックします。

ステップ 8 チェックして一致させる順序に従って、テーブル内のポリシーを編成します。ルールの順序を変更するには、行をドラッグして正しい位置にドロップします。

ステップ 9 [保存（Save）] をクリックすると、変更内容が保存されて実装されます。

次のタスク

1. 許可ポリシーの設定

認証ポリシーの構成設定

次の表では、[ポリシーセット（Policy Sets）] ウィンドウの [認証ポリシー（Authentication Policy）] セクションのフィールドについて説明します。このフィールドから、認証サブポリシーをポリシーセットの一部として構成できます。ネットワークアクセスポリシーの場合は、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ポリシー セット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシー セット（Device Admin Policy Sets）]** を選択します。[ポリシー セット（Policy Sets）] ページから、**[表示（View）] > [認証ポリシー（Authentication Policy）]** を選択します。

表 *130 :* 認証ポリシーの構成設定

フィールド名	使用上のガイドライン
[ステータス（Status）]	このポリシーのステータスを選択します。次のいずれかを設定できます。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニタのみ（Monitor Only）]：このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証（Live Log authentication）] ページでこのポリシー条件の結果を照会できます。ここでは、モニタされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加する場合に、条件がもたらす結果が正しいかどうかを判断できないことがあります。この場合、モニタ モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。
ルール名	この認証ポリシーの名前を入力します。
条件（Conditions）	新しいポリシー行から、プラス（+）アイコンをクリックするか、既存のポリシー行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
使用（Use）	認証に使用する ID ソースを選択します。ID ソース順序が設定済みである場合、これを選択することも可能です。 デフォルトの ID ソースを編集して、このルールで定義されたいずれの ID ソースも要求に一致しない場合に Cisco ISE が使用する ID ソースを指定できます。

フィールド名	使用上のガイドライン
オプション（**Options**）	認証失敗、ユーザが見つからない、プロセス障害、の各イベントに対する今後のアクションのコースを定義します。次のいずれかのオプションを選択できます。 • [拒否（Reject）]：拒否応答が送信されます。 • [ドロップ（Drop）]：応答は送信されません。 • [続行（Continue）]：Cisco ISE は認証ポリシーの処理を続行します。
ヒット数（**Hits**）	ヒット数は、条件が一致した回数を示す診断ツールです。
アクション	さまざまなアクションを表示して選択するには、[アクション（Actions）] 列の歯車アイコン をクリックします。 • [上に新しい行を挿入（Insert new row above）]：[アクション（Actions）] メニューを開いたポリシーの上に新しい認証ポリシーを挿入します。 • [下に新しい行を挿入（Insert new row below）]：[アクション（Actions）] メニューを開いたポリシーの下に新しい認証ポリシーを挿入します。 • [上に複製（Duplicate above）]：元のセットの上に、[アクション（Actions）] メニューを開いたポリシーの上に複製認証ポリシーを挿入します。 • [下に複製（Duplicate below）]：元のセットの下に、[アクション（Actions）] メニューを開いたポリシーの下に複製認証ポリシーを挿入します。 • [削除（Delete）]：ポリシーセットを削除します。

パスワード ベースの認証

認証とは、ユーザ情報を検証してユーザ ID を確認することです。従来の認証方式では、名前とある決まったパスワードが使用されていました。これは、最も一般的かつ単純で、低コストの認証方式です。この方式の欠点は、ユーザ名やパスワードの情報が簡単に第三者に伝えられたり、推測または不正に取得されたりする可能性がある点です。単純な暗号化されていないユーザ名とパスワードを使用する方法は、強力な認証方式とは考えられていませんが、インターネットアクセスなど、許可または特権レベルが低い場合は十分に要件を満たす可能性があります。

暗号化されたパスワードと暗号化技術を使用したセキュアな認証

ネットワーク上でパスワードが不正に取得される危険性を低減するには、暗号化を使用する必要があります。RADIUS などのクライアント/サーバ アクセス コントロール プロトコルでは、パスワードを暗号化することにより、ネットワーク内でパスワードが不正に取得される事態を防止します。ただし、RADIUS は認証、許可、およびアカウンティング（AAA）クライアントと Cisco ISE との間でだけ動作します。認証プロセスでは、このポイントの前で、許可されていないユーザが次のような例で暗号化されていないパスワードを入手する可能性があります。

- 電話回線を介してダイヤルアップ接続を行うエンドユーザ クライアントとの間の通信
- ネットワーク アクセス サーバで終了する ISDN 回線
- エンドユーザ クライアントとホスティング デバイスの間の Telnet セッションを介して行われる通信

さらに安全な方式では、チャレンジハンドシェイク認証プロトコル（CHAP）、ワンタイムパスワード（OTP）、および高度な EAP ベースのプロトコルの内部で使用されるような暗号化技術を使用します。Cisco ISE は、これらのさまざまな認証方式をサポートしています。

認証方式と許可特権

認証と許可には基本的な暗黙の関係があります。ユーザに与えられる許可特権が多くなればなるほど、それに応じて認証を強化する必要があります。Cisco ISE では、さまざまな認証方式を提供することにより、この関係がサポートされています。

認証ダッシュレット

Cisco ISE のダッシュボードには、ネットワークとデバイスに対し行われたすべての認証の概要が表示されます。これには、認証ダッシュレットにある認証および許可の失敗についての概要情報が表示されます。

RADIUS 認証ダッシュレットには、Cisco ISE が処理した認証に関する次の統計情報が表示されます。

- 認証成功、認証失敗、同一ユーザによる同時ログインなど、Cisco ISE が処理した RADIUS 認証要求の総数。

- Cisco ISE が処理した、失敗した RADIUS 認証要求の総数。

また、TACACS+認証の概要を表示することもできます。TACACS+認証ダッシュレットには、デバイス認証の統計情報が表示されます。

デバイス管理認証の詳細については、TACACS ライブ ログ （342 ページ）を参照してください。RADIUS ライブ ログ設定の詳細については、RADIUS ライブ ログ （333 ページ）を参照してください。

ISE コミュニティ リソース

認証と許可の失敗のトラブルシューティング方法については、「How To: Troubleshoot ISE Failed Authentications & Authorizations」を参照してください。

認証結果の表示

Cisco ISE にはリアルタイムで認証の概要を表示するさまざまな方法があります。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 ネットワーク認証（RADIUS）の場合は、**[操作（Operations）] > [RADIUS] > [ライブ ログ（Live Logs）]** を選択し、デバイス認証（TACACS）の場合は、**[操作（Operations）] > [TACACS] > [ライブ ログ（Live Logs）]** を選択して、リアルタイムの認証の概要を表示します。

ステップ 2 認証の概要を表示するには、次のような方法があります。

- [ステータス（Status）]アイコンの上にマウス カーソルを移動すると、認証の結果と概要を表示できます。ステータスの詳細とともにポップアップが表示されます。
- 結果をフィルタリングするには、リストの最上部に表示される 1 つ以上の任意のテキスト ボックスに検索条件を入力して **Enter** を押します。
- 詳細レポートを表示するには、[詳細（Details）] カラムにある虫眼鏡アイコンをクリックします。

（注） 認証概要レポートまたはダッシュボードが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。

認証レポートおよびトラブルシューティング ツール

認証の詳細の他に、Cisco ISE では、ネットワークの効率的な管理に使用できるさまざまなレポートおよびトラブルシューティング ツールが提供されます。

ネットワーク内の認証の傾向およびトラフィックを把握するために実行できるさまざまなレポートがあります。現在のデータに加えて履歴のレポートを生成できます。認証レポートのリストは次のとおりです。

- AAA の診断
- RADIUS アカウンティング（RADIUS Accounting）
- RADIUS 認証
- 認証概要（Authentication Summary）

（注） Cisco Catalyst 4000 シリーズ スイッチで IPv6 スヌーピングを有効にする必要があります、有効にしないと、IPv6 アドレスが認証セッションにマッピングされず、show の出力に表示されません。IPv6 スヌーピングを有効にするには、次のコマンドを使用します。

```
vlan config <vlan-number>
 ipv6 snooping
 end
ipv6 nd raguard policy router
 device-role router
interface <access-interface>
  ipv6 nd raguard
interface <uplink-interface>
  ipv6 nd raguard attach-policy router
  end
```

認可ポリシー

許可ポリシーは、Cisco ISE ネットワーク許可サービスのコンポーネントです。このサービスを使用して、ネットワーク リソースにアクセスする特定のユーザおよびグループの許可ポリシーを定義し、許可プロファイルを設定することができます。

許可ポリシーには条件付きの要件を含めることができ、この要件では、1つ以上の許可プロファイルを返すことができる許可チェックを含む複合条件を使用して、1 つ以上の ID グループを組み合わせます。さらに、条件付きの要件は、特定の ID グループの使用とは別に存在することがあります。

許可プロファイルは、Cisco ISE で許可ポリシーを作成するときに使用されます。許可ポリシーは許可ルールで構成されます。許可ルールには、名前、属性、および権限の 3 つの要素があります。権限要素は、許可プロファイルにマッピングされます。

Cisco ISE の許可プロファイル

許可ポリシーは、特定のユーザおよびグループの ID にルールを関連付け、対応するプロファイルを作成します。これらのルールが設定された属性と一致する場合は、常に、権限を付与する、対応する許可プロファイルがポリシーによって返され、ネットワーク アクセスがこれに応じて許可されます。

たとえば、許可プロファイルには、次のタイプに含まれるさまざまな権限を含めることができます。

- 標準プロファイル
- 例外プロファイル
- デバイスベースのプロファイル

プロファイルは、利用可能なベンダー ディクショナリのいずれかに保存されているリソースセットから選択された属性で構成され、特定の許可ポリシーの条件が一致したときに返されます。許可ポリシーには単一のネットワーク サービス ルールにマッピングする条件を含めることができるため、許可チェックのリストを含めることもできます。

許可確認は、返される許可プロファイルに準拠する必要があります。許可確認は、通常、ライブラリに追加できるユーザ定義名を含む1つ以上の条件から構成され、他の許可ポリシーで再利用できます。

許可プロファイルの権限

許可プロファイルの権限設定を開始する前に、以下を確認します。

- 許可ポリシーおよび許可プロファイル間の関係を理解している
- 許可プロファイル ページをよく理解している
- ポリシーおよびプロファイルを設定する場合に必要な基本ガイドラインを知っている
- 許可プロファイルの権限の構成を理解している

許可プロファイルを使用するには、**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]**>**[結果（Results）]** を選択します。左側のメニューから、**[認証（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。

ネットワークでさまざまなタイプの許可プロファイルのポリシー要素権限を表示、作成、変更、削除、複製、または検索するプロセスの開始点として [結果（Results）] ナビゲーションペインを使用します。[結果（Results）] ペインには、最初 [認証（Authentication）]、[許可（Authorization）]、[プロファイリング（Profiling）]、[ポスチャ（Posture）]、[クライアントプロビジョニング（Client Provisioning）]、および [TrustSec] のオプションが表示されています。

許可プロファイルでは、RADIUS 要求が受け入れられたときに返される属性を選択できます。Cisco ISE では、[共通タスク（Common Tasks）] 設定を設定して共通に使用される属性をサポートできるメカニズムが提供されます。Cisco ISE が基盤となる RADIUS 値に変換する [共通タスク（Common Tasks）] 属性の値を入力する必要があります。

ISE コミュニティ リソース

802.1x サプリカント（Cisco AnyConnect Mobile Security）とオーセンティケータ（スイッチ）間の Media Access Control Security（MACsec）暗号化を設定する方法の例については、「MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example」を参照してください。

ロケーションに基づく認証

Cisco ISE は、Cisco モビリティ サービス エンジン（MSE）と統合し、物理ロケーション ベースの認証を導入します。Cisco ISE は、MSE からの情報を使用して、MSE によって報告されるユーザの実際の位置に基づいて差別化されたネットワーク アクセスを提供します。

この機能を使用すると、エンドポイントのロケーション情報を使用して、ユーザが適切なゾーンにいる場合にネットワーク アクセスを提供できます。また、エンドポイントのロケーションをポリシーの追加属性として追加して、デバイスのロケーションに基づいてより詳細なポリシー許可のセットを定義することもできます。次のように、ロケーションベースの属性を使用する許可ルール内で条件を設定できます。

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

ロケーション階層（キャンパス/ビルディング/フロア構造）を定義して、Cisco Prime Infrastructure のアプリケーションを使用してセキュアおよび非セキュアのゾーンを設定できます。ロケーション階層を定義した後、ロケーション階層データを MSE サーバと同期する必要があります。Cisco Prime Infrastructure の詳細については、http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html を参照してください。

1 つまたは複数の MSE インスタンスを追加して、MSE ベースのロケーション データを許可プロセスに統合できます。これらの MSE からロケーション階層データを取得し、このデータを使用してロケーション ベースの許可ルールを設定できます。

エンドポイントの移動を追跡するには、許可プロファイルの作成時に [移動の追跡（Track Movement）] チェックボックスをオンにします。Cisco ISE は、5 分ごとにエンドポイント ロケーションの関連 MSE にクエリを行い、ロケーションが変更されたかどうかを確認します。

（注） 複数のユーザを追跡すると、頻繁な更新によってパフォーマンスに影響します。[移動の追跡（Track Movement）] オプションは、上位のセキュリティ ロケーションに使用できます。

ロケーション ツリーは、MSE インスタンスから取得されたロケーション データを使用して作成されます。ロケーション ツリーを使用して、許可ポリシーに公開するロケーション エントリを選択できます。

（注） ロケーション サービスを使用するには、ISE Plus ライセンスが必要です。

MSE サーバの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理（Administration）]>[ネットワークリソース（Network Resources）]>[ロケーションサービス（Location Services）]>[ロケーションサーバ（Location Servers）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 サーバ名、ホスト名/IP アドレス、パスワードなど、MSE サーバの詳細を入力します。

ステップ 4 指定したサーバの詳細を使用して MSE の接続性をテストするには、[テスト（Test）] をクリックします。

ステップ 5 （任意）エンドポイントがこの MSE に現在接続されているかどうかを確認するには、[ロケーション検索（Find Location）] フィールドにエンドポイントの MAC アドレスを入力し、[検索（Find）] をクリックします。

エンドポイントのロケーションが見つかった場合は、*Campus:Building:Floor:Zone* の形式で表示されます。ロケーションの階層およびゾーンの設定によっては、複数のエントリが表示される場合があります。たとえば、*Campus1* という名前のキャンパス内のビルディング（*building1*）のすべてのフロアが非セキュア ゾーンとして定義され、最初のフロアのラボエリアがセキュア ゾーンとして定義されている場合、エンドポイントがそのラボ エリアにある場合は、次のエントリが表示されます。

見つかった場所：

Campus1#building1#floor1#LabArea

Campus1#building1#floor1#NonSecureZone

ステップ 6 [送信（Submit）] をクリックします。
新しい MSE を追加したら、[ロケーションツリー（Location Tree）] ページに移動し、[更新の取得（Get Update）] をクリックして、ロケーション階層を取得し、それをロケーション ツリーに追加します。このツリーで定義されたフィルタがある場合、これらのフィルタは新しい MSE エントリにも適用されます。

ロケーション ツリー

ロケーション ツリーは、MSE インスタンスから取得されたロケーション データを使用して作成されます。ロケーション ツリーを表示するには、[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ロケーションサービス（Location Services）] > [ロケーションツリー（Location Tree）] を選択します。

1 つのビルディングに複数の MSE がある場合、Cisco ISE はすべての MSE からロケーションの詳細を照合し、単一のツリーとして表示します。

ロケーション ツリーを使用して、許可ポリシーに公開するロケーション エントリを選択できます。また、要件に基づいて特定のロケーションを非表示にすることもできます。ロケーションを非表示にする前にロケーション ツリーを更新することを推奨します。非表示にされたロケーションは、ツリーが更新されても非表示のままになります。

許可ルールに関連するロケーション エントリが変更または削除された場合は、影響を受けるルールをディセーブルにし、これらのロケーションを [不明（Unknown）] として設定するか、または影響を受ける各ルールに代替ロケーションを選択する必要があります。変更を適用したり更新をキャンセルする前に新しいツリー構造を確認する必要があります。

すべての MSE から最新のロケーション階層構造を取得するには、[更新の取得（Get Update）] をクリックします。新しいツリー構造を確認したら、[保存（Save）] をクリックして変更を適用します。

ダウンロード可能 ACL

アクセス コントロール リスト（ACL）はアクセス コントロール エントリ（ACE）のリストで、ポリシー適用ポイント（スイッチなど）によってリソースに適用できます。各 ACE は、読み取り、書き込み、実行など、このオブジェクトに対してユーザごとに許可された権限を識別します。たとえば、ある ACE で販売グループに書き込み権限を許可し、別の ACE で組織内の他のすべての従業員に読み取り権限を許可して、ネットワーク内の販売エリアを使用するように ACL を設定できます。RADIUS プロトコルの場合、送信元と宛先の IP アドレス、トランスポート プロトコル、および他のパラメータをフィルタリングして、ACL は許可を付与します。スタティック ACL はスイッチ上に配置されており、スイッチから直接設定でき、ISE GUI から許可ポリシーに適用できます。ダウンロード可能な ACL（DACL）は、ISE GUI から許可ポリシーで設定、管理、および適用できます。

ISE でネットワーク許可ポリシーに DACL を実装する場合：

1. **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ダウンロード可能なACL（Downloadable ACLs）]** から新規または既存の DACL を設定します。詳細については、ダウンロード可能ACLに対する権限の設定 （1006ページ）を参照してください。
2. 設定済みの DACL を使用して、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）]** から新規または既存の許可プロファイルを設定します。
3. **[ポリシー（Policy）] > [ポリシーセット（Policy Sets]** から新規および既存のポリシー セットを作成および設定する場合は、設定済みの許可プロファイルを実装します。

ダウンロード可能 ACL に対する権限の設定

ISE の場合、ダウンロード可能な ACL（DACL）は、さまざまなユーザおよびユーザ グループがネットワークにアクセスする方法を制御するために許可ポリシーで設定および実装できます。デフォルト許可 DACL は、次のデフォルト プロファイルを含む ISE のインストール時に使用できます。

- DENY_ALL_TRAFFIC
- PERMIT_ALL_TRAFFIC

DACL を使用する場合、これらのデフォルトは設定できませんが、他の同じような DACL を作成するために複製することはできます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能 ACL（Downloadable ACLs）]** を選択します。

ステップ 2 [ダウンロード可能なACL（Downloadable ACLs）] テーブル上部の [追加（Add）] をクリックするか、既存の DACL を選択し、テーブル上部の [複製（Duplicate）] をクリックします。

ステップ 3 次のルールに留意しながら、DACL に適切な値を入力または編集します。

- [名前（Name）] フィールドのサポート対象の文字：英数字、ハイフン（-）、ドット（.）、アンダースコア（_）
- キーワード **Any** が DACL のすべての ACE のソースである必要があります。DACL がプッシュされると、ソースの **Any** がスイッチに接続されているクライアントの IP アドレスで置き換えられます。

（注） [IP バージョン（IP Version）] フィールドは、DACL がいずれかの認証プロファイルにマッピングされている場合は編集できません。この場合、[認証プロファイル（Authorization Profiles）] から DACL 参照を削除し、IP バージョンを編集して、[認証プロファイル（Authorization Profiles）] の DACL を再マッピングします。

ステップ 4 必要に応じて、ACE のすべてのリストの作成が完了したら、[DACL構文のチェック（Check DACL Syntax）] をクリックしてリストを検証します。検証エラーが発生した場合、自動的に表示されるウィンドウで無効な構文を識別する特定の指示が返されます。

ステップ 5 [送信（Submit）] をクリックします。

Active Directory ユーザ許可のためのマシン アクセス制限

Cisco ISE には、Microsoft Active Directory 認証ユーザの許可を制御する追加の方法を提供する、マシン アクセス制限（MAR）コンポーネントが含まれています。この形式の許可は、Cisco ISE ネットワークにアクセスするために使用されるコンピュータのマシン認証に基づきます。成功したマシン認証ごとに、Cisco ISE は、RADIUS Calling-Station-ID 属性（属性 31）で受信した値を、成功したマシン認証の証拠としてキャッシュします。

Cisco ISE は、[Active Directory の設定（Active Directory Settings）] ページの [存続可能時間（Time to Live）] パラメータで設定された時間が失効になるまで各 Calling-Station-ID 属性値をキャッシュに保持します。失効したパラメータは、Cisco ISE によってキャッシュから削除されます。

ユーザをエンドユーザ クライアントから認証する場合、Cisco ISE は、成功したマシン認証の Calling-Station-ID 値のキャッシュを検索して、ユーザ認証要求で受信した Calling-Station-ID 値を見つけようとします。Cisco ISE が一致するユーザ認証 Calling-Station-ID 値をキャッシュで見つけた場合、これは、次の方法で認証を要求するユーザに Cisco ISE が権限を割り当てる方法に影響します。

- Calling-Station-ID 値が Cisco ISE キャッシュで見つかった値と一致する場合、成功した許可の許可プロファイルを割り当てます。
- Calling-Station-ID 値が Cisco ISE キャッシュの値と一致しないことがわかった場合、マシン認証のない成功したユーザ認証の許可プロファイルを割り当てます。

許可ポリシーおよびプロファイルの設定のガイドライン

許可ポリシーおよびプロファイルを管理または運用する場合、次のガイドラインに従ってください。

- 作成するルール名は、サポートされている次の文字のみを使用する必要があります。

- 記号：プラス（+）、ハイフン（-）、アンダースコア（_）、ピリオド（.）、およびスペース（ ）。
- アルファベット文字：A ～ Z、a ～ z。
- 数字：0 ～ 9。

- ID グループのデフォルトは「Any」です（このグローバル デフォルトを使用してすべてのユーザに適用できます）。
- 条件では、1 つ以上のポリシー値を設定することが許可されています。ただし、条件はオプションであり、許可ポリシーを作成する場合に必須ではありません。次に、条件を作成する 2 つの方法を示します。
  - 選択肢の対応するディクショナリから既存の条件または属性を選択します。
  - 推奨値を選択またはテキストボックスを使用してカスタム値を入力できるカスタム条件を作成します。
- 作成する条件名は、サポートされている次の文字のみを使用する必要があります。
  - 記号：ハイフン（-）、アンダースコア（_）、およびピリオド（.）。
  - アルファベット文字：A ～ Z、a ～ z。
  - 数字：0 ～ 9。
- 権限は、ポリシーに使用する許可プロファイルを選択するときに重要です。権限は、特定のリソースへのアクセス権を付与したり、特定のタスクの実行を可能にしたりできます。たとえば、あるユーザが特定の ID グループ（デバイス管理者など）に属しており、そのユーザが定義済みの条件（サイトがボストンにあるなど）を満たしている場合、このユーザは、そのグループに関連付けられた権限（特定のネットワーク リソースのセットへのアクセス権、デバイスへの特定の操作を実行する権限など）を付与されます。

許可ポリシーの設定

[ポリシー（Policy）] メニューから許可ポリシーの属性および構成要素を作成したら、[ポリシーセット（Policy Sets）] メニューからポリシー セット内で許可ポリシーを作成します。

始める前に

この手順を開始する前に、ID グループと条件など、許可ポリシーの作成に使用されるさまざまなビルディング ブロックについて基本を理解しておく必要があります。

ステップ 1 ネットワーク アクセス ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ポリシー セット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシー セット（Device Admin Policy Sets）]** を選択します。

ステップ 2 [表示（View）]列から、 をクリックしてすべてのポリシーセットの詳細にアクセスし、認証および許可ポリシーとポリシー例外を作成します。

ステップ 3 ページの許可ポリシー部分の横にある矢印アイコンをクリックして、[許可ポリシー（Authorization Policy）]テーブルを展開して表示します。

ステップ 4 いずれかの行の [アクション（Actions）] 列から、歯車アイコンをクリックします。ドロップダウン メニューから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して、新しい許可ポリシー ルールを挿入します。
[許可ポリシー（Authorization Policy）] テーブルに新しい行が表示されます。

ステップ 5 ポリシーのステータスを設定するには、現在の[ステータス（Status）]アイコンをクリックし、ドロップダウンリストの[ステータス（Status）]列から必要なステータスを選択します。ステータスの詳細については、許可ポリシーの設定 （1010 ページ） を参照してください。

ステップ 6 テーブル内のポリシーの場合は、[ルール名（Rule Name）] のセルをクリックしてフリーテキストを変更し、一意のルール名を作成します。

ステップ 7 条件を追加または変更するには、[条件（Conditions）] 列のセルにカーソルを合わせ、 をクリックします。[条件スタジオ（Conditions Studio）] が開きます。詳細については、ポリシー条件 （1018 ページ） を参照してください。

選択するすべての属性に「Equals」、「Not Equals」、「In」、「Not In」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現（REGEX）をサポートし、使用します。

（注） 単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数値属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。リストの場合、「in」演算子は、特定の値がリスト内に存在するかどうかをチェックします。単一文字列の場合、「in」演算子は、文字列が「equals」演算子などと同じかどうかをチェックします。

ステップ 8 ネットワーク アクセス結果プロファイルの場合は、[結果プロファイル（Results Profiles）] ドロップダウンリストから関連する許可プロファイルを選択するか、または を選択またはクリックして、[新しい許可プロファイルの作成（Create a New Authorization Profile）] を選択し、[新しい標準プロファイルの追加（Add New Standard Profile）] 画面が開いたら、次の手順を実行します。

a) 必要に応じて値を入力して、新しい許可プロファイルを設定します。次の点を考慮してください。

- [名前（name）] フィールドでサポートされる文字は次のとおりです：スペース、! # $ % & ‘ ( ) * + , - . / ; = ? @ _ {。
- 画面下部に動的に表示される [属性詳細（Attributes Details）] から許可プロファイル RADIUS 構文をダブルチェックできます。

b) [保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、許可プロファイルを作成します。

c) [ポリシー セット（Policy Sets）] 領域外のプロファイルを作成、管理、編集、および削除するには、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 9 ネットワーク アクセス結果のセキュリティ グループの場合は、[結果のセキュリティ グループ（Results Security Groups）] ドロップダウンリストから関連するセキュリティ グループを選択するか、または ➕ をクリックして、[新しいセキュリティ グループの作成（Create a New Security Group）] を選択し、[新しいセキュリティ グループの作成（Create New Security Group）] 画面が開いたら、次の手順を実行します。

a) 新規セキュリティ グループの名前と説明（オプション）を入力します。

b) この SGT を ACI に反映するには、[ACI に伝播（Propagate to ACI）] チェック ボックスをオンにします。この SGT に関連する SXP マッピングは、ACI が [ACI の設定（ACI Settings）] ページで選択した VPN に属するときのみ ACI に反映されます。

このオプションはデフォルトでは無効になっています。

c) タグ値を入力します。タグ値は、手動で入力したり、自動生成されるようにしたり設定できます。また SGT の範囲を予約できます。これは、から設定できます。[一般TrustSecの設定（General TrustSec Settings）] ページ（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）]）。

d) [送信（Submit）] をクリックします。

詳細については、セキュリティ グループの設定 （1118 ページ）を参照してください。

ステップ 10 TACACS+ の結果については、[結果（Results）] ドロップダウンリストから関連するコマンド セットとシェル プロファイルを選択するか、または [コマンド セット（Command Sets）] または [シェル プロファイル（Shell Profiles）] 列で ➕ をクリックして、[コマンドの追加（Add Commands）] 画面または [シェル プロファイルの追加（Add Shell Profile）] をそれぞれ開きます。[新しいコマンドセットの作成（Create a New Command Set）] または [新しいシェル プロファイルの作成（Create a New Shell Profile）] を選択し、フィールドに入力します。

ステップ 11 テーブル内でポリシーをチェックして一致させる順序を編成します。

ステップ 12 [保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、この新しい許可ポリシーを作成します。

許可ポリシーの設定

次の表では、[ポリシーセット（Policy Sets）] ウィンドウの [許可ポリシー（Authorization Policy）] セクションのフィールドについて説明します。このフィールドから、許可ポリシーをポリシー セットの一部として構成できます。ネットワーク アクセス ポリシーの場合は、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ポリシー セット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシー セット（Device Admin Policy Sets）]** を選択します。[ポリシー セット（Policy Sets）] ページから、**[表示（View）] > [許可ポリシー（Authorization Policy）]** を選択します。

表 *131 :* 許可ポリシーの構成時の設定

フィールド名	使用上のガイドライン
[ステータス（Status）]	このポリシーのステータスを選択します。次のいずれかを設定できます。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニタのみ（Monitor Only）]：このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証（Live Log authentication）] ページでこのポリシー条件の結果を照会できます。ここでは、モニタされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加する場合に、条件がもたらす結果が正しいかどうかを判断できないことがあります。この場合、モニタ モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。
ルール名	このポリシーの一意の名前を入力します。
条件（**Conditions**）	新しいポリシー行から、プラス（+）アイコンをクリックするか、既存のポリシー行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
結果またはプロファイル（**Results or Profiles**）	関連する許可プロファイルを選択します。これにより、構成されたセキュリティ グループに提供される権限のそれぞれのレベルが決まります。関連する許可プロファイルをまだ設定していない場合は、インラインで行うことができます。
結果またはセキュリティグループ（**Results or Security Groups**）	関連するセキュリティグループを選択します。これにより、特定のルールに関連するユーザのグループが決まります。関連するセキュリティ グループをまだ設定していない場合は、インラインで行うことができます。

フィールド名	使用上のガイドライン
結果またはコマンドセット（**Results or Command Sets**）	コマンド セットは、デバイス管理者が実行できるコマンドの指定されたリストを適用します。デバイス管理者がネットワーク デバイスに対して操作コマンドを発行すると、その管理者がこれらのコマンドの発行を認可されているかどうかを判定する問い合わせが ISE に行われます。これは、コマンド認可とも呼ばれます。
結果またはシェルプロファイル（**Results or Shell Profiles**）	TACACS+ シェル プロファイルは、デバイス管理者の最初のログイン セッションを制御します。
ヒット数（**Hits**）	ヒット数は、条件が一致した回数を示す診断ツールです。
アクション	さまざまなアクションを表示して選択するには、[アクション（Actions）] 列の歯車アイコン をクリックします。 • [上に新しい行を挿入（Insert new row above）] : [アクション（Actions）] メニューを開いたルールの上に新しい許可ルールを挿入します。 • [下に新しい行を挿入（Insert new row below）] : [アクション（Actions）] メニューを開いたルールの下に新しい許可ルールを挿入します。 • [上に複製（Duplicate above）] : 元のセットの上に、[アクション（Actions）] メニューを開いたルールの上に複製許可ルールを挿入します。 • [下に複製（Duplicate below）] : 元のセットの下に、[アクション（Actions）] メニューを開いたルールの下に複製許可ルールを挿入します。 • [削除（Delete）] : ルールを削除します。

許可プロファイルの設定

[許可プロファイル（Authorization Profiles）] ウィンドウの次のフィールドで、ネットワークアクセスの属性を定義します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]**> **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** です。

許可プロファイルの設定

- [名前（Name）]：この新しい認証プロファイルの名前を入力します。
- [説明（Description）]：許可プロファイルの説明を入力します。
- [アクセスタイプ（Access Type）]：アクセスタイプ（[ACCESS_ACCEPT] または [ACCESS_REJECT]）を選択します。
- [サービステンプレート（Service Template）]：SAnet対応デバイスとのセッションをサポートするには、このオプションを有効にします。Cisco ISEは、許可プロファイルを「サービステンプレート」互換としてマークする特別なフラグを使用して、許可プロファイルにサービステンプレートを実装します。サービステンプレートは許可プロファイルでもあるため、SAnetデバイスと非SAnetデバイスの両方をサポートする単一のポリシーとして機能します。
- [移動の追跡（Track Movement）]：Cisco Mobility Services Engine（MSE）を使用してユーザの場所を追跡するには、このオプションを有効にします。

（注） このオプションは、Cisco ISEのパフォーマンスに影響を与える可能性があります。これは、セキュリティレベルの高い場所を対象としています。

- [Passive Identityトラッキング（Passive Identity Tracking）]：ポリシーの適用とユーザトラッキングのためにPassive IdentityのEasy Connect機能を使用するには、このオプションを有効にします。

一般的なタスク

一般的なタスクは、ネットワークアクセスに適用される特定の権限とアクションです。

- [DACL名（DACL Name）]：ダウンロード可能なACLを使用するには、このオプションを有効にします。デフォルト値（**PERMIT_ALL_TRAFFIC** または **DENY_ALL_TRAFFIC**）を使用するか、次のディクショナリから属性を選択することができます。
  - 外部IDストア（属性）（External identity store (attributes)）
  - エンドポイント
  - 内部ユーザ

- 内部エンドポイント

DACLの追加、または既存のDACLの編集および管理の詳細については、ダウンロード可能 ACL （1006 ページ）を参照してください。

- [ACL（フィルタID）（ACL（Filter-ID））]：RADIUS フィルタ ID 属性を設定するには、このオプションを有効にします。フィルタ ID は、NAD の ACL を指定します。フィルタ ID を定義すると、Cisco ISE はファイル名に「.in」を追加します。フィルタ ID は [属性の詳細（Attributes Details）] ペインに表示されます。[ACL IPv6（フィルタID）（ACL IPv6（Filter-ID））] は、NAD への IPv6 接続と同じ方法で動作します。
- [セキュリティグループ（Security group）]：認証の一部としてセキュリティグループ（SGT）を割り当てるには、このオプションを有効にします。
  - Cisco ISE が Cisco DNA Center と統合されていない場合、Cisco ISE は VLAN ID 1 を割り当てます。
  - Cisco ISE が Cisco DNA Center と統合されている場合は、Cisco DNA Center が Cisco ISE と共有する仮想ネットワーク（VN）を選択し、[データタイプ（Data Type）] とサブネット/アドレスプールを選択します。

（注） セキュリティグループタスクには、セキュリティグループと VN が含まれています。セキュリティグループを設定する場合、VLAN を設定することはできません。エンドポイントデバイスは、1 つの仮想ネットワークにのみ割り当てることができます。

- [VLAN]：仮想LAN（VLAN）IDを指定するには、このオプションを有効にします。VLAN ID には、整数または文字列値を入力できます。このエントリの形式は、Tunnel-Private-Group-ID:VLANnumber です。
- [音声ドメイン権限（Voice Domain Permission）]：ダウンロード可能な ACL を使用するには、このオプションを有効にします。`cisco-av-pair` のベンダー固有属性（VSA）を `device-traffic-class=voice` の値と関連付けます。複数ドメインの許可モードでは、ネットワークスイッチがこの VSA を受信した場合、エンドポイントは、許可後に音声ドメインに接続されます。
- [Webリダイレクション（CWA、DRW、MDM、NSP、CPP）（Web Redirection（CWA, DRW, MDM, NSP, CPP））]：認証後に Web リダイレクションを有効にするには、このオプションを有効にします。
  - リダイレクションのタイプを選択します。選択した Web リダイレクションのタイプには、次で説明する追加のオプションが表示されます。
  - Cisco ISE が NAD に送信するリダイレクションをサポートするための ACL を入力します。

    NAD に送信するために入力する ACL は、cisco-av ペアとして [属性の詳細（Attributes Details）] ペインに表示されます。たとえば、**acl119** と入力した場合、これは [属性の

詳細（Attributes Details）] ペインには `cisco-av-pair = url-redirect-acl = acl119` と表示されます。

- 選択した Web リダイレクションタイプのその他の設定を選択します。

次のタイプの Web リダイレクションのいずれかを選択します。

- [中央集中Web認証（Centralized Web Auth）] : [値（Value）] ドロップダウンから選択したポータルにリダイレクトします。
- [クライアント プロビジョニング（ポスチャ）（Client Provisioning (Posture)）] : クライアントでポスチャを有効にするため、[値（Value）] ドロップダウンから選択したクライアント プロビジョニング ポータルにリダイレクトします。
- [ホットスポット: リダイレクト（Hot Spot: Redirect）] : [値（Value）] ドロップダウンから選択したホットスポットポータルにリダイレクトします。
- [MDM リダイレクト（MDM Redirect）] : 指定した MDM サーバの MDM ポータルにリダイレクトします。
- [ネイティブサプリカントのプロビジョニング（Native Supplicant Provisioning）] : [値（Value）] ドロップダウンから選択した BYOD にリダイレクトします。

Web リダイレクションタイプを選択し、必要なパラメータを入力したら、次のオプションを設定します。

- [証明書更新メッセージの表示（Display Certificates Renewal Message）] : 証明書更新メッセージを表示するには、このオプションを有効にしますurl-redirect 属性値が変更され、この値に証明書が有効である日数が含まれます。このオプションは、中央集中型 Web 認証のみに使用できます。
- [スタティックIP/ホスト名/FQDN（Static IP/Host Name/FQDN）] : ユーザを別の PSN にリダイレクトするには、このオプションを有効にします。ターゲットIPアドレス、ホスト名、またはFQDNを入力します。このオプションを設定しない場合、ユーザはこの要求を受信したポリシーサービスノードの FQDN にリダイレクトされます。
- [論理プロファイルでエンドポイントのプロファイラCoAを抑制する（Suppress Profiler CoA for endpoints in Logical Profile）] : 特定のタイプのエンドポイントデバイスのリダイレクトをキャンセルするには、このオプションを有効にします。

- [自動スマートポート（Auto smartport）] : 自動スマートポート機能を使用するには、このオプションを有効にします。イベント名を入力します。これにより、この値を持つ VSA の cisco-av-pair が `auto-smart-port=event_name` として作成されます。この値は、[属性詳細（Attributes Details）] ペインに表示されます。
- [アクセスの脆弱性（Access Vulnerabilities）] : このオプションを有効にすると、このエンドポイントでの脅威中心型 NAC 脆弱性評価を許可の一環として実行できます。アダプタを選択し、スキャンを実行するタイミングを選択します。

- [再認証（Reauthentication）]：再認証中にエンドポイントを接続したままにするには、このオプションを有効にします。 [RADIUS要求（RADIUS-Request）]（1）を使用することを選択して、再認証中に接続を維持することを選択します。 デフォルトの [RADIUS要求（RADIUS-Request）]（0）では、既存のセッションを切断します。非アクティビティタイマーを設定することもできます。
- [MACSec ポリシー（MACSec Policy）]：MACSec 対応クライアントが Cisco ISE に接続するたびにMACSec暗号化ポリシーを使用するには、このオプションを有効にします。次のオプションのいずれかを選択します。[must-secure]、[should-secure]、または [must-not-secure]。 設定は [属性詳細（Attributes Details）] ペインに `cisco-av-pair = linksec-policy=must-secure` と表示されます。
- [NEAT]：ネットワーク間の ID 認識を拡張するネットワーク エッジ アクセス トポロジ（NEAT）を使用するには、このオプションを有効にします。このチェックボックスをオンにすると、[属性の詳細（Attributes Details）] ペインに、`cisco-av-pair = device-traffic-class=switch` と表示されます。
- [Web認証（ローカルWeb認証）（Web Authentication（Local Web Auth））]：この許可プロファイルのローカル Web 認証を使用するには、このオプションを有効にします。この値では、Cisco ISE が DACL とともに VSA を送信することによって Web 認証の許可をスイッチが認識できます。VSA は `cisco-av-pair = priv-lvl=15` で、これは [属性の詳細（Attributes Details）] ペインに表示されます。
- [Airespace ACL名（Airespace ACL Name）]：Cisco Airespace ワイヤレスコントローラに ACL 名を送信するには、このオプションを有効にします。Airespace VSA はこの ACL を使用して、ローカルで定義された WLC 上の接続への ACL を許可します。たとえば、**rsa-1188** と入力した場合、これは [属性の詳細（Attributes Details）] ペインに `Airespace-ACL-Name = rsa-1188` と表示されます。
- [ASA VPN]：適応型セキュリティアプライアンス（ASA）VPN グループポリシーを割り当てるには、このオプションを有効にします。ドロップダウンリストから、VPN グループポリシーを選択します。
- [AVCプロファイル名（AVC Profile Name）]：このエンドポイントでアプリケーションの可視性を実行するには、このオプションを有効にします。使用する AVC プロファイルを入力します。

高度な属性設定（Advanced Attributes Settings）

- [ディクショナリ（Dictionaries）]：下矢印アイコンをクリックし、[ディクショナリ（Dictionaries）] ウィンドウに選択可能なオプションを表示します。 最初のフィールドで設定する必要があるディクショナリと属性を選択します。
- [属性値（Attribute Values）]：下矢印アイコンをクリックし、[属性値（Attribute Values）] ウィンドウに選択可能なオプションを表示します。2番目のフィールドに目的の属性グループおよび属性値を選択します。この値は、最初のフィールドで選択した値と一致します。設定する [高度な属性（Advanced Attributes）] が [属性の詳細（Attribute Details）] パネルに表示されます。

（注） [属性の詳細（Attributes Details）] ペインに表示される読み取り専用の値を変更または削除するには、対応する [共通タスク（Common Tasks）] フィールド、または [高度な属性設定（Advanced Attributes Settings）] ペインの [属性値（Attribute Values）] で選択した属性でこれらの値を変更または削除します。

- [属性の詳細（Attributes Details）]：このペインには、[共通タスク（Common Tasks）] および [高度な属性（Advanced Attributes）] に設定した設定済みの属性値が表示されます。

（注） [属性の詳細（Attributes Details）] ペインに表示される値は読み取り専用です。

関連トピック

Cisco ISE の許可プロファイル （1002 ページ）
許可プロファイルの権限 （1003 ページ）
未登録のデバイスのリダイレクトのための許可プロファイルの設定 （960 ページ）
許可プロファイルの作成 （411 ページ）

許可ポリシーの例外

各ポリシー セット内では、通常の許可ポリシーの他に、ローカルの例外ルール（各ポリシー セットの [設定（Set）] ビューの [許可ポリシーのローカル例外（Authorization Policy Local Exceptions）] パートから定義される）およびグローバル例外ルール（各ポリシー セットの [設定（Set）] ビューの [許可ポリシーのグローバル例外（Authorization Policy Global Exceptions）] パートから定義される）も定義できます。

グローバル許可例外ポリシーを使用すると、すべてのポリシーセット内のすべての許可ルールを上書きするルールを定義できます。グローバル許可例外ポリシーを設定すると、すべてのポリシーセットに追加されます。グローバル許可例外ポリシーは、現在設定されているポリシーセットのいずれかから更新できます。グローバル許可例外ポリシーを更新するたびに、それらの更新がすべてのポリシー セットに適用されます。

ローカル許可例外ルールは、グローバル例外ルールを上書きします。許可ルールは、許可ポリシーのローカル例外規則、グローバル例外規則、通常ルールの順番で処理されます。

許可例外ポリシー ルールは、許可ポリシー ルールと同じように設定されます。例外ポリシーを設定するには、上記の通常の許可ポリシーの設定手順を参照してください。許可ポリシーの設定 （1008 ページ）

ローカル例外およびグローバル例外の構成時の設定

ネットワーク アクセス ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ポリシー セット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシー セット（Device Admin Policy Sets）]** を選択します。[ポリシーセット（Policy Sets）] ウィンドウから、**[表示（View）]** > **[ローカル例外ポリシー（Local Exceptions Policy）]** または [グローバル例外ポリシー（Global Exceptions Policy）] を選択します。

許可例外設定は、許可ポリシー設定と同じで、許可ポリシーの設定（1010ページ） で説明されています。

ポリシー条件

Cisco ISE はルールベースのポリシーを使用してネットワーク アクセスを提供します。ポリシーは、ルールが条件で構成されているルールと結果のセットです。Cisco ISE では、個々のポリシー要素として条件を作成し、システム ライブラリに保存してから、[条件スタジオ（Conditions Studio）] の他のルールベースのポリシーに再利用することができます。

条件では演算子（等しい、等しくない、より大きい、など）と値を使用し、必要に応じて単純にすることも、複雑にすることもできます。また、複数の属性、演算子、複雑な階層を含めることもできます。実行時に、Cisco ISE はポリシー条件を評価し、ポリシー評価が true または false 値のどちらを返すかに応じて、定義された結果を適用します。

条件を作成して一意の名前を割り当てた後、この条件を [条件スタジオ ライブラリ（Conditions Studio Library）] から選択することで、さまざまなルールとポリシーにわたって複数回再利用することができます。例を次に示します。

```
Network Conditions.MyNetworkCondition EQUALS true
```

ポリシーで使用されているか、または別の条件の一部である条件は [条件スタジオ（Conditions Studio）] から削除できません。

各条件は、オブジェクトのリストを定義します。このリストはポリシー条件に含めることができ、これにより、要求で示される定義と照合される定義セットになります。

演算子 `EQUALS true` を使用して、ネットワーク条件が true であるかどうか（要求に指定されている値がネットワーク条件の 1 つ以上のエントリと一致しているかどうか）を確認するか、または`EQUALS false` を使用して、ネットワーク条件が false であるかどうか（ネットワーク条件のどのエントリとも一致しないかどうか）を確認することができます。

Cisco ISE には、事前定義されたスマート条件も用意されています。この条件は、ポリシーで個別に使用したり、独自のカスタマイズされた条件で構成要素として使用でき、必要に応じて更新および変更できます。

次の固有のネットワーク条件を作成してネットワークへのアクセスを制限することができます。

- エンドステーション ネットワーク条件（Endstation Network Conditions）：接続が開始および終了されるエンドステーションに基づきます。

  Cisco ISE はリモート アドレスの [TO] フィールド（TACACS+ 要求または RADIUS 要求であるかに基づいて取得）を評価し、これがエンドポイントの IP アドレス、MAC アドレス、発信側回線 ID（CLI）、または着信番号識別サービス（DNIS）のいずれであるかを確認します。

  RADIUS 要求では、この ID は属性 31（Calling-Station-Id）で使用できます。

  TACACS+ 要求では、リモート アドレスにスラッシュ（/）が含まれている場合、スラッシュより前の部分は [FROM] の値として見なされ、スラッシュより後の部分は [TO] 値として見なされます。たとえば、要求に CLI/DNIS と指定されている場合、CLI は [FROM] の値と見なされ、DNIS は [TO] の値と見なされます。スラッシュが含まれていない場合は、リモート アドレス全体が [FROM] の値として見なされます（IP アドレス、MAC アドレス、CLI いずれの場合でも）。

- デバイス ネットワーク条件（Device Network Conditions）：要求を処理する AAA クライアントに基づきます。

  ネットワーク デバイスは、IP アドレス、ネットワーク デバイス リポジトリで定義されているデバイス名、またはネットワーク デバイス グループによって識別されます。

  RADIUS 要求では、属性 4（NAS-IP-Address）が指定されている場合、Cisco ISE はこの属性から IP アドレスを取得します。属性 32（NAS-Identifier）が存在する場合、Cisco ISE は属性 32 から IP アドレスを取得します。これらの属性が存在しない場合は、受信したパケットから IP アドレスを取得します。

  デバイス ディクショナリ（NDG ディクショナリ）にはネットワーク デバイス グループ属性（Location、Device Type、または NDG を表すその他の動的に作成された属性など）が含まれています。これらの属性には、現在のデバイスに関連するグループが含まれています。

- [デバイス ポート ネットワーク条件（Device Port Network Conditions）]：デバイスの IP アドレス、名前、NDG、およびポート（エンドポイントが接続しているデバイスの物理ポート）に基づきます。

  RADIUS 要求では、属性 5（NAS-Port）が要求内に存在する場合、Cisco ISE はこの属性から値を取得します。属性 87（NAS-Port-Id）が要求内に存在する場合、Cisco ISE は属性 87 から要求を取得します。

  TACACS+ 要求では、Cisco ISE はその ID を（すべてのフェーズの）開始要求のポート フィールドから取得します。

これらの固有条件の詳細については、特別なネットワーク アクセス条件 （1041 ページ） を参照してください。

ディクショナリおよびディクショナリ属性

ディクショナリは、ドメインのアクセスポリシーの定義に使用できる属性と許容値のドメイン固有カタログです。個々のディクショナリは、属性タイプの同種の集合です。ディクショナリで定義された属性は同じ属性タイプを持ち、タイプは特定の属性のソースまたはコンテキストを示します。

属性タイプは次のいずれかになります。

- MSG_ATTR
- ENTITY_ATTR
- PIP_ATTR

属性と許容値に加えて、ディクショナリには名前と説明、データ型、デフォルト値などの属性に関する情報が含まれます。属性は、次のいずれかのデータ型となります。BOOLEAN、FLOAT、INTEGER、IPv4、IPv6、OCTET_STRING、STRING、UNIT32、および UNIT64。

Cisco ISE ではインストール中にシステム ディクショナリが作成され、ユーザ ディクショナリを作成できます。

属性は、異なるシステム ディクショナリに格納されます。属性を使用して、条件を構成します。属性は、複数の条件で再利用できます。

ポリシー条件を作成するときに、有効な属性を再利用するには、サポートされている属性を含むディクショナリから選択します。たとえば、Cisco ISE は、AuthenticationIdentityStore という属性を提供しています。これは NetworkAccess ディクショナリにあります。この属性は、ユーザの認証中にアクセスされた最後の ID ソースを識別します。

- 認証中に単一の ID ソースが使用されると、この属性には認証が成功した ID ストアの名前が含まれます。
- 認証中に ID ソース順序を使用する場合、この属性にはアクセスされた最後の ID ソースの名前が含まれます。

AuthenticationStatus 属性を AuthenticationIdentityStore 属性と組み合わせて使用し、ユーザが正常に認証された ID ソースを識別する条件を定義できます。たとえば、許可ポリシーで LDAP ディレクトリ（LDAP13）を使用してユーザが認証された条件をチェックするために、次の再利用可能な条件を定義できます。

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

（注） AuthenticationIdentityStore は、条件にデータを入力できるテキストフィールドを表します。このフィールドには、名前を必ず正しく入力またはコピーします。ID ソースの名前が変更された場合は、ID ソースの変更と一致するように、この条件を変更する必要があります。

以前認証されたエンドポイント ID グループに基づく条件を定義するために、Cisco ISE では、エンドポイント ID グループ 802.1X 認証ステータスの間に定義された許可をサポートしています。Cisco ISE では、802.1X 認証を実行するとき、RADIUS 要求の「Calling-Station-ID」フィールドから MAC アドレスを抽出し、この値を使用して、デバイスのエンドポイント ID グループ（endpointIDgroup 属性として定義）のセッション キャッシュを検索して読み込みます。このプロセスによって、許可ポリシー条件の作成に endpointIDgroup 属性を使用できるようになり、ユーザ情報に加えてこの属性を使用して、エンドポイント ID グループ情報に基づく許可ポリシーを定義できます。

（注） Calling-Station-ID は Cisco ISE2.3 以降の AA:BB:CC:DD:EE:FF 形式でのみ受け入れられます。したがって、承認条件は、Calling-Station-ID が AA-BB-CC-DD-EE-FF 形式で提供されていると失敗する可能性があります。

エンドポイント ID グループの条件は、[許可ポリシー設定（authorization policy configuration）] ページの [ID グループ（ID Groups）] カラムで定義できます。ユーザ関連情報に基づく条件は、許可ポリシーの [その他の条件（Other Conditions）] のセクションで定義する必要があります。ユーザ情報が内部ユーザ属性に基づいている場合は、内部ユーザ ディクショナリの ID グループ属性を使用します。たとえば、「User Identity Group:Employee:US」のような値を使用して、ID グループに完全な値のパスを入力できます。

ネットワーク アクセス ポリシーでサポートされるディクショナリ

Cisco ISE は、認証ポリシーと許可ポリシーの条件とルールを構築する際に必要なさまざまな属性を含む次のシステム格納ディクショナリをサポートしています。

- システム定義されたディクショナリ
  - CERTIFICATE
  - DEVICE
  - RADIUS
- RADIUS ベンダー ディクショナリ
  - Airespace
  - Cisco
  - Cisco-BBSM
  - Cisco-VPN3000
  - Microsoft
  - Network Access

許可ポリシー タイプの場合、条件で設定された検証は、戻される許可プロファイルに従う必要があります。

確認には、通常、ライブラリに追加して他のポリシーで再利用できるユーザ定義名を含む1つ以上の条件が含まれます。

以下の項では、条件の設定に使用できるサポートされている属性とディクショナリについて説明します。

ディクショナリによってサポートされる属性

表に、ディクショナリでサポートされる固定属性を示します。これらの属性をポリシー条件内で使用できます。作成する条件のタイプによっては、使用できない属性もあります。

たとえば、認証ポリシー内でアクセス サービスを選択する条件を作成する場合、使用できるネットワーク アクセス属性は、Device IP Address、ISE Host Name、Network Device Name、Protocol、および Use Case のみです。

次の表に示す属性をポリシー条件に使用できます。

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
Device	Device Type（定義済みのネットワーク デバイス グループ）	○	○
	Device Location（定義済みのネットワーク デバイス グループ）		
	Other Custom Network Device Group		
	ソフトウェア バージョン（Software Version）		
	モデル名（Model Name）		
RADIUS	すべての属性	○	○

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
Network Access	ISE Host Name	○	○
	AuthenticationMethod	×	○
	AuthenticationStatus	×	×
	CTSDeviceID	×	×
	Device IP Address（デバイス IP アドレス）	○	○
	EapAuthentication（マシンのユーザの認証時に使用される EAP 方式）	×	○
	EapTunnel（トンネルの確立に使用される EAP 方式）	×	○
	プロトコル	○	○
	UseCase	○	○
	UserName	×	○
	WasMachineAuthenticated	×	×

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
証明書	Common Name	×	○
	国（Country）		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	シリアル番号（Serial Number）		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	発行元（Issuer）		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
	Issuer - Street Address		
	Issuer - Domain Component		
	Issuer - User ID		

システム定義のディクショナリとディクショナリ属性

Cisco ISE は、インストール中にシステム ディクショナリを作成します。これは、[システム ディクショナリ（System Dictionaries）] ページで確認できます。システム定義のディクショナリ属性は、読み取り専用の属性です。その特性のため、既存のシステム定義のディクショナリは表示することのみができます。システム定義の値またはシステムディクショナリ内の属性を作成、編集、削除することはできません。

システム定義のディクショナリ属性は、属性の記述名、ドメインによって認識される内部名、および許容値とともに表示されます。

また、Cisco ISE は Internet Engineering Task Force（IETF）で定義され、システム定義のディクショナリにも含まれる IETF RADIUS 属性セット用にディクショナリ デフォルトを作成します。ID を除くすべてのフリー IETF RADIUS 属性フィールドを編集できます。

システム ディクショナリおよびディクショナリ属性の表示

システムディクショナリ内のシステム定義の属性を作成、変更、削除することはできません。システム定義された属性は表示することのみができます。ディクショナリの名前と説明に基づくクイック検索またはユーザ定義の検索ルールに基づく高度な検索を実行できます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）]** を選択します。

ステップ 2 [システム ディクショナリ（System Dictionaries）] ページからシステム ディクショナリを選択して [表示（View）] をクリックします。

ステップ 3 [ディクショナリ属性（Dictionary Attributes）] をクリックします。

ステップ 4 リストからシステム ディクショナリを選択して [表示（View）] をクリックします。

ステップ 5 [システム ディクショナリ（System Dictionaries）] ページに戻るには、[ディクショナリ（Dictionaries）] リンクをクリックします。

ユーザ定義のディクショナリとディクショナリ属性

Cisco ISE では、[ユーザ ディクショナリ（User Dictionary）] ページで作成したユーザ定義ディクショナリが表示されます。システムで作成され、保存された既存のユーザ ディクショナリの [ディクショナリ名（Dictionary Name）] または [ディクショナリ タイプ（Dictionary Type）] の値は変更できません。

[ユーザ ディクショナリ（User Dictionaries）] ページでは、次の操作を実行できます。

- ユーザ ディクショナリを編集および削除します。
- 名前および説明に基づいてユーザ ディクショナリを検索します。

- ユーザディクショナリのユーザ定義のディクショナリ属性を追加、編集、および削除します。
- NMAP スキャン機能を使って、NMAP 拡張ディクショナリの属性を削除します。カスタム ポートが [NMAP スキャン アクション（NMAP Scan Actions）] ページで追加または削除されると、対応するカスタム ポート属性がディクショナリで追加、削除または更新されます。
- ディクショナリ属性の許容値を追加または削除します。

ユーザ定義のディクショナリの作成

ユーザ定義のディクショナリを作成、編集、または削除できます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[ユーザ（User）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ユーザ ディクショナリの名前、オプションの説明、およびバージョンを入力します。

ステップ 4 [ディクショナリ属性タイプ（Dictionary Attribute Type）] ドロップダウン リストから属性タイプを選択します。

ステップ 5 [送信（Submit）] をクリックします。

ユーザ定義のディクショナリ属性の作成

ユーザディクショナリの、ユーザ定義のディクショナリ属性を追加、編集および削除したり、ディクショナリ属性に使用できる値を追加または削除したりすることができます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** > **[ユーザ（User）]** を選択します。

ステップ 2 [ユーザ ディクショナリ（User Dictionaries）] ページからユーザ ディクショナリを選択して [編集（Edit）] をクリックします。

ステップ 3 [ディクショナリ属性（Dictionary Attributes）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 ディクショナリ属性の属性名、オプションの説明、および内部名を入力します。

ステップ 6 [データ型（Data Type）] ドロップダウン リストからデータ型を選択します。

ステップ 7 [追加（Add）] をクリックして、[使用できる値（Allowed Values）] テーブルで名前、使用できる値、およびデフォルト ステータスを設定します。

ステップ 8 [送信（Submit）] をクリックします。

RADIUS ベンダー ディクショナリ

Cisco ISE では、一連の RADIUS ベンダー ディクショナリを定義したり、それぞれの一連の属性を定義したりできます。リスト内の各ベンダー定義には、ベンダー名、ベンダー ID、および簡単な説明が含まれています。

Cisco ISE では、次の RADIUS ベンダー ディクショナリがデフォルトで提供されます。

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

RADIUSプロトコルは、これらのベンダーディクショナリと、許可プロファイルとポリシー条件で使用できるベンダー固有属性をサポートします。

RADIUS ベンダー ディクショナリの作成

RADIUSベンダーディクショナリを作成、編集、削除、エクスポート、およびインポートすることもできます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [RADIUS（Radius）] > [RADIUS ベンダー（Radius Vendors）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 RADIUS ベンダーの Internet Assigned Numbers Authority（IANA）で承認されている RADIUS ベンダー ディクショナリの名前、オプションの説明、およびベンダー ID を入力します。

ステップ 4 属性値から取得したバイト数を選択して、[ベンダー属性タイプ フィールド長（Vendor Attribute Type Field Length）] ドロップダウン リストから属性タイプを指定します。有効な値は、1、2、および4です。デフォルト値は 1 です。

ステップ 5 属性値から取得したバイト数を選択して、[ベンダー属性サイズ フィールド長（Vendor Attribute Size Field Length）] ドロップダウン リストから属性長を指定します。有効な値は 0 と 1 です。デフォルト値は 1 です。

ステップ 6 [送信（Submit）] をクリックします。

RADIUS ベンダー ディクショナリ属性の作成

CiscoISEがサポートするRADIUSベンダー属性を作成、編集、および削除できます。各RADIUSベンダー属性には、名前、データ型、説明、および方向（要求のみに関連する、応答のみに関連する、または両方に関連するかどうかを指定）が含まれています。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [RADIUS（Radius）] > [RADIUS ベンダー（Radius Vendors）]** を選択します。

ステップ 2 RADIUS ベンダーディクショナリ リストから RADIUS ベンダーディクショナリを選択して [編集（Edit）] をクリックします。

ステップ 3 [ディクショナリ属性（Dictionary Attributes）] をクリックし、[追加（Add）] をクリックします。

ステップ 4 RADIUS ベンダー属性の属性名とオプションの説明を入力します。

ステップ 5 [データ型（Data Type）] ドロップダウン リストからデータ型を選択します。

ステップ 6 [MAC オプションの有効化（Enable MAC option）] チェックボックスを選択します。

ステップ 7 RADIUS 要求のみ、RADIUS 応答のみ、またはその両方に適用される方向を [方向（Direction）] ドロップダウン リストから選択します。

ステップ 8 [ID] フィールドにベンダー属性 ID を入力します。

ステップ 9 [タグ付けの許可（Allow Tagging）] チェックボックスをオンにします。

ステップ 10 [プロファイルのこの属性の複数インスタンスを許可する（Allow multiple instances of this attribute in a profile）] チェックボックスをオンにします。

ステップ 11 [追加（Add）] をクリックして、[使用できる値（Allowed Values）] テーブルにベンダー属性の使用できる値を追加します。

ステップ 12 [送信（Submit）] をクリックします。

HP RADIUS IETF サービス タイプ属性

Cisco ISE では、RADIUS IETF サービス タイプ属性に 2 つの新しい値が導入されました。RADIUS IETF サービス タイプ属性は、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [RADIUS] > [IETF] で使用できます。ポリシーの条件で次の 2 つの値を使用できます。これら 2 つの値は、特に HP のデバイスがユーザの権限を理解できるように設計されています。

列挙名	列挙値
HP-Oper	252
HP-User	255

RADIUS ベンダー ディクショナリ属性の設定

ここでは、Cisco ISE で使用される RADIUS ベンダーのディクショナリについて説明します。

次の表に、RADIUS ベンダーのディクショナリ属性を設定できるようにする RADIUS ベンダーの [ディクショナリ（Dictionary）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [RADIUS] > [RADIUSベンダー（RADIUS Vendors）]** です。

表 *132 : RADIUS* ベンダー ディクショナリ属性の設定

フィールド名	使用上のガイドライン
属性名（**Attribute Name**）	選択した RADIUS ベンダーのベンダー固有属性名を入力します。
説明	ベンダー固有属性のオプションの説明を入力します。
内部名	内部のデータベースで表されるベンダー固有属性の名前を入力します。
データ タイプ	ベンダー固有属性に対して、次のデータ型のいずれかを選択します。 • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4 • IPV6
MAC を有効にするオプション（Enable MAC option）	MACアドレスとしてのRADIUS属性の比較を有効にするには、このチェックボックスをオンにします。デフォルトで、RADIUS 属性 Calling-Station-ID に対して、このオプションは有効とマークされ、無効にできません。RADIUSベンダーディクショナリ内の別のディクショナリ属性（文字列型）の場合は、このオプションを有効または無効にできます。 このオプションを有効にした場合、認証および許可条件の設定中に、テキスト オプションを選択して比較をクリアな文字列にするか、またはMACアドレスオプションを選択して比較をMACアドレスにするかを定義できます。
方向（**Direction**）	RADIUS メッセージに適用するいずれかのオプションを選択します。
ID	ベンダー属性IDを入力します。有効な範囲は 0 ～ 255 です。

フィールド名	使用上のガイドライン
タギングの許可（Allow Tagging）	RFC2868 で定義するように、タグを持つことが許可されるものとして属性をマークするには、このチェック ボックスをオンにします。タグの目的は、トンネル化されたユーザの属性のグループ化を許可することです。詳細については、RFC2868 を参照してください。 タグ付けされた属性のサポートでは、特定のトンネルに関するすべての属性のそれぞれのタグ フィールドに同じ値が含まれ、各セットに Tunnel-Preference 属性の適切に評価されたインスタンスが含まれていることが保証されます。これは、マルチベンダー ネットワーク環境に使用すべきトンネル属性に適合しているため、複数のベンダーで製造されたネットワーク アクセス サーバ（NAS）間の相互運用性の問題を解決します。
プロファイルでこの属性の複数のインスタンスを許可する（Allow Multiple Instances of this Attribute in a Profile）	プロファイルでこの RADIUS ベンダー固有属性の複数のインスタンスが必要な場合は、このチェックボックスをオンにします。

関連トピック

システム定義のディクショナリとディクショナリ属性 （1025 ページ）
ユーザ定義のディクショナリとディクショナリ属性 （1025 ページ）
RADIUS ベンダー ディクショナリ （1027 ページ）
RADIUS ベンダー ディクショナリの作成 （1027 ページ）

[条件スタジオ（Conditions Studio）] の操作

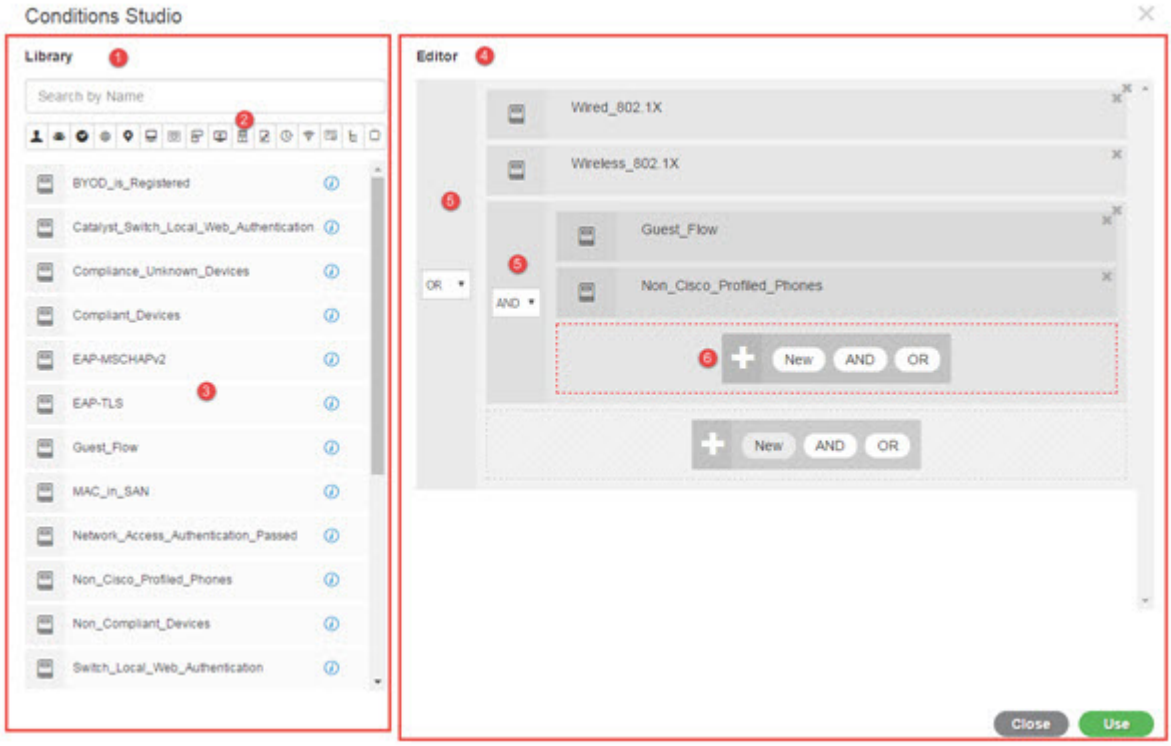
[条件スタジオ（Conditions Studio）] は、条件の作成、管理、および再利用に使用します。条件には複数のルールを含めることができ、1 つのみのレベルまたは複数の階層レベルを含む任意の複雑度で構築できます。[条件スタジオ（Conditions Studio）] を使用して新しい条件を作成する場合は、[ライブラリ（Library）] にすでに保存している条件ブロックを使用することができ、それらの保存された条件ブロックを更新および変更することもできます。後で条件を作成および管理する際に、クイック カテゴリ フィルタなどを使用して、必要なブロックと属性を簡単に見つけることができます。

ネットワーク アクセス ポリシーの場合は、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ポリシー セット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシー セット（Device Admin Policy Sets）]** を選択します。

いずれかのポリシーセットの特定のルールにすでに適用されている条件を編集または変更するには、[条件（Conditions）] 列のセルにカーソルを合わせ をクリックするか、または新しい条件を作成するには [ポリシーセット（Policy Set）] テーブルの [条件（Conditions）] 列のプラス記号 をクリックします。その条件は、すぐに同じポリシーセットに適用することができます。または、後で使用するために [ライブラリ（Library）] に保存することもできます。

次の図に、[条件スタジオ（Conditions Studio）] の主な要素を示します。

図 *56 : [条件スタジオ（Conditions Studio）]*



[条件スタジオ（Conditions Studio）] は、[ライブラリ（Library）] と [エディタ（Editor）] の 2 つの主要部分に分かれています。[ライブラリ（Library）] には再使用のために条件ブロックが保存され、[エディタ（Editor）] では保存されたブロックを編集したり新しいブロックを作成できます。

次の表では、[条件スタジオ（Conditions Studio）] のさまざまな部分について説明します。

フィールド	使用上のガイドライン
ライブラリ（Library）	再利用のために ISE データベースで作成され保存されたすべての条件ブロックのリストを表示します。これらの条件ブロックを現在編集している条件の一部として使用するには、それらを [ライブラリ（Library）] から [エディタ（Editor）] の関連レベルにドラッグ アンド ドロップし、必要に応じて演算子を更新します。 条件は複数のカテゴリに関連付けることができるため、[ライブラリ（Library）] に保存されている条件はすべて [ライブラリ（Library）] アイコン  で表されます。 また、[ライブラリ（Library）] の各条件の横には、iアイコンがあります。このアイコンの上にカーソルを置くと、条件の完全な説明や、関連付けられているカテゴリが表示され、また、ライブラリから条件を完全に削除できます。ポリシーで使用されている条件は削除できません。 ライブラリ条件のいずれかを [エディタ（Editor）] にドラッグ アンド ドロップして、現在編集されているポリシーに単独で使用するか、または現在のポリシーで使用されるさらに複雑な条件の構成要素として使用するか、あるいは [ライブラリ（Library）] に新しい条件として保存します。[エディタ（Editor）] に条件をドラッグ アンド ドロップしてその条件を変更し、[ライブラリ（Library）] に同じ名前または新しい名前で保存することもできます。 インストール時には事前定義された条件もあります。これらの条件は、変更および削除することもできます。

フィールド	使用上のガイドライン
検索およびフィルタ（Search and filter）	名前で条件を検索したり、カテゴリ別にフィルタリングしたりできます。同様に、[エディタ（Editor）] の [クリックして属性を追加する（Click to add an attribute）] フィールドから属性を検索およびフィルタリングすることもできます。ツールバー上のアイコンは、件名や住所などの異なる属性カテゴリを表します。アイコンをクリックすると、特定のカテゴリに関連する属性が表示されます。カテゴリ ツールバーの強調表示されたアイコンをクリックすると、そのカテゴリが選択解除され、フィルタが削除されます。
条件リスト（Conditions List）	[ライブラリ（Library）] 内のすべての条件の完全なリスト、または検索またはフィルタの結果に基づく [ライブラリ（Library）] 内の条件のリスト。
エディタ（Editor）	すぐに使用する新しい条件を作成するだけでなく、今後使用するためにシステム ライブラリに条件を保存したり、既存の条件を編集して、即座に使用したり今後使用するためにその変更を [ライブラリ（Library）] に保存します。 新しい条件を作成するために [条件スタジオ（Conditions Studio）] を開くと（ポリシー セット テーブルのいずれかのプラス記号をクリック）、最初のルールを追加できる空白の行が 1 つだけ表示されます。 [エディタ（Editor）] が空のフィールドとともに表示される場合は、演算子アイコンは表示されません。

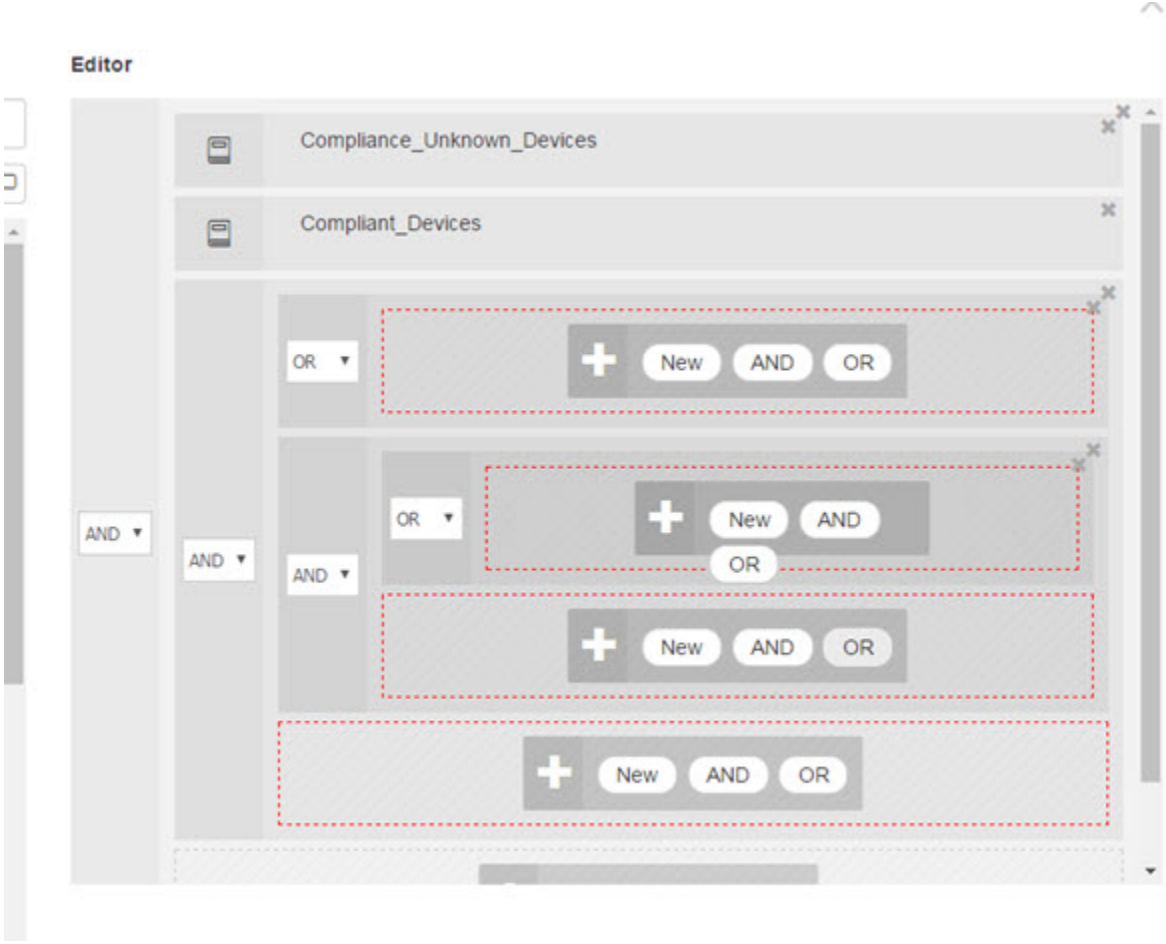
フィールド	使用上のガイドライン
	[エディタ（Editor）] は、さまざまな仮想列と行に分かれています。 列は異なる階層レベルを表し、各列は階層内の位置に基づいてインデントされます。行は個々のルールを表します。レベルごとに 1 つまたは複数のルールを作成し、複数のレベルを含めることができます。 上記のイメージの例は、構築または編集中の条件を示しており、ルールの階層を含んでいます。図の第 1 レベルと第 2 レベルの両方に番号 5 が付けられています。上位親レベルのルールは、演算子 OR を使用します。 演算子を選択して階層レベルを作成した後で演算子を変更するには、この列に表示されているドロップダウンリストから該当するオプションを選択するだけです。 演算子のドロップダウンリストに加えて、各ルールにはこの列に関連するアイコンがあり、そのルールが属するカテゴリが示されています。アイコンの上にカーソルを置くと、ツールチップにカテゴリの名前が示されます。 ライブラリに保存されると、すべての条件ブロックに [ライブラリ（Library）] アイコンが割り当てられ、[エディタ（Editor）] に表示されたカテゴリ アイコンが置き換えられます。 最後に、関連するすべての一致項目を**除外する**ルールが設定されている場合、Is-Not インジケータもこの列に表示されます。たとえば、London という値を持つロケーション属性が Is-Not に設定されている場合、ロンドンからのすべてのデバイスはアクセスが拒否されます。

フィールド	使用上のガイドライン
	この領域には、階層レベルで作業するときに使用できるオプションと、条件内の複数のルールが表示されます。 任意の列または行にカーソルを置くと、関連するアクションが表示されます。アクションを選択すると、そのアクションがそのセクションとすべての子セクションに適用されます。たとえば、階層 A の 5 つのレベルで、第 3 レベルの任意のルールから AND を選択すると、元のルールの下に新しい階層 B が作成され、元のルールが階層 B の親ルールになるように階層 A に埋め込まれます。 新しい条件を最初から作成するために [条件スタジオ（Condition Studio）] を最初に開くと、[エディタ（Editor）] 領域には、設定可能な単一ルールの 1 行のみと、関連する演算子を選択するオプション、または関連条件を [ライブラリ（Library）] からドラッグ アンド ドロップするオプションが含まれています。 **AND** および **OR** 演算子オプションを使用して、条件にレベルを追加できます。オプションをクリックしたときと同じレベルで新しいルールを作成するには、[新規（New）] を選択します。[新規（New）] オプションは、階層の最上位レベルに少なくとも 1 つのルールを設定した場合にのみ表示されます。

ポリシー条件の設定、編集および管理

[条件スタジオ（Conditions Studio）] は、条件の作成、管理、および再利用に使用します。条件には複数のルールを含めることができ、1 つのみのレベルまたは複数の階層レベルを含む任意の複雑度で構築できます。次の図のように、[条件スタジオ（Conditions Studio）] の [エディタ（Editor）] 側から条件階層を管理します。

図 *57 : [*エディタ（***Editor***）*]* : 条件階層



新しい条件を作成する場合は、[ライブラリ（Library）]にすでに保存している条件ブロックを使用することができ、それらの保存された条件ブロックを更新および変更することもできます。条件を作成および管理する際に、クイック カテゴリ フィルタなどを使用して、必要なブロックと属性を簡単に見つけることができます。

条件ルールを作成および管理する場合は、属性、演算子、および値を使用します。

Cisco ISE には、最も一般的な使用例の一部に関する事前定義された条件ブロックも含まれています。これらの事前定義された条件を要件に合わせて編集できます。設定済みブロックを含む、再使用のために保存された条件は、このタスクで説明するように、[条件スタジオ（Conditions Studio）] の [ライブラリ（Library）] に保存されます。

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 [ポリシーセット（Policy Sets）]領域にアクセスします。**[ポリシー（Policy）]**>**[ポリシー セット（Policy Sets）]** を選択します。

ステップ 2 [条件スタジオ（Conditions Studio）] にアクセスして新しい条件を作成したり、既存の条件ブロックを編集して、特定のポリシー セット（および関連するポリシーとルール）のために設定したルールの一部としてそれらの条件を使用したり、今後使用するために [ライブラリ（Library）] に保存します。

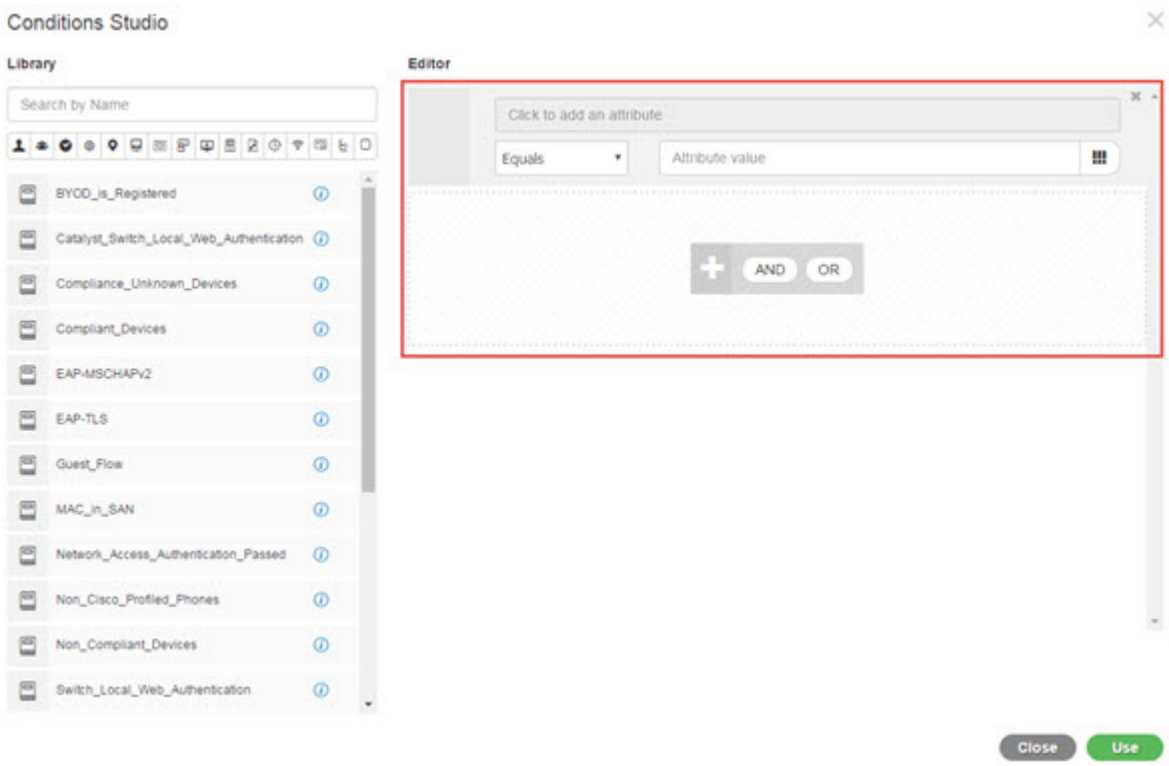
a) ポリシー セット全体（認証ポリシー ルールに照合する前にチェックされる条件）に関連する条件を作成するには、メインの [ポリシー セット（Policy Set）] ページで [ポリシー セット（Policy Set）] テーブルの [条件（Conditions）] 列から ✚ をクリックします。

b) または、認証および許可のすべてのルールを含む [設定（Set）] ビューを表示するには、特定のポリシー セットの行から › をクリックします。[設定（Set）] ビューから、ルールの表のいずれかの [条件（Conditions）] 列のセルにカーソルを合わせ、✚ をクリックして [条件スタジオ（Conditions Studio）] を開きます。

c) すでにポリシー セットに適用されている条件を編集する場合は、✎ をクリックして [条件スタジオ（Conditions Studio）] にアクセスします。

[条件スタジオ（Conditions Studio）] が開きます。新しい条件を作成するために開いた場合は、次の画像のように表示されます。フィールドの説明と、ポリシー セットに既に適用されている条件を編集するために開いた場合の [条件スタジオ（Conditions Studio）] の例を参照するには、[条件スタジオ（Conditions Studio）] の操作 （1030 ページ） を参照してください。

図 *58 : [条件スタジオ（Conditions Studio）]*：新しい条件の作成



ステップ 3 [ライブラリ（Library）] からの既存の条件ブロックを、作成または編集している条件のルールとして使用します。

a) [ライブラリ（Library）] のカテゴリ ツールバーから関連するカテゴリを選択してフィルタリングすると、選択したカテゴリの属性を含むすべてのブロックが表示されます。複数のルールを含むが、それらのルールの少なくとも 1 つに対して選択したカテゴリの属性を使用している条件ブロックも表示されます。追加のフィルタが追加されている場合、表示される結果には、特定のフィルタからの条件ブロックのみが含まれ、含まれている他のフィルタも照合されます。たとえば、ツールバーから [ポート（Ports）] カテゴリを選択し、[名前で検索（Search by Name）] フィールドにフリー テキストとして「auth」と入力すると、名前に「auth」が含まれているポートに関連するすべてのブロックが表示されます。カテゴリ ツールバーの強調表示されたアイコンを再度クリックすると選択解除され、そのフィルタが削除されます。

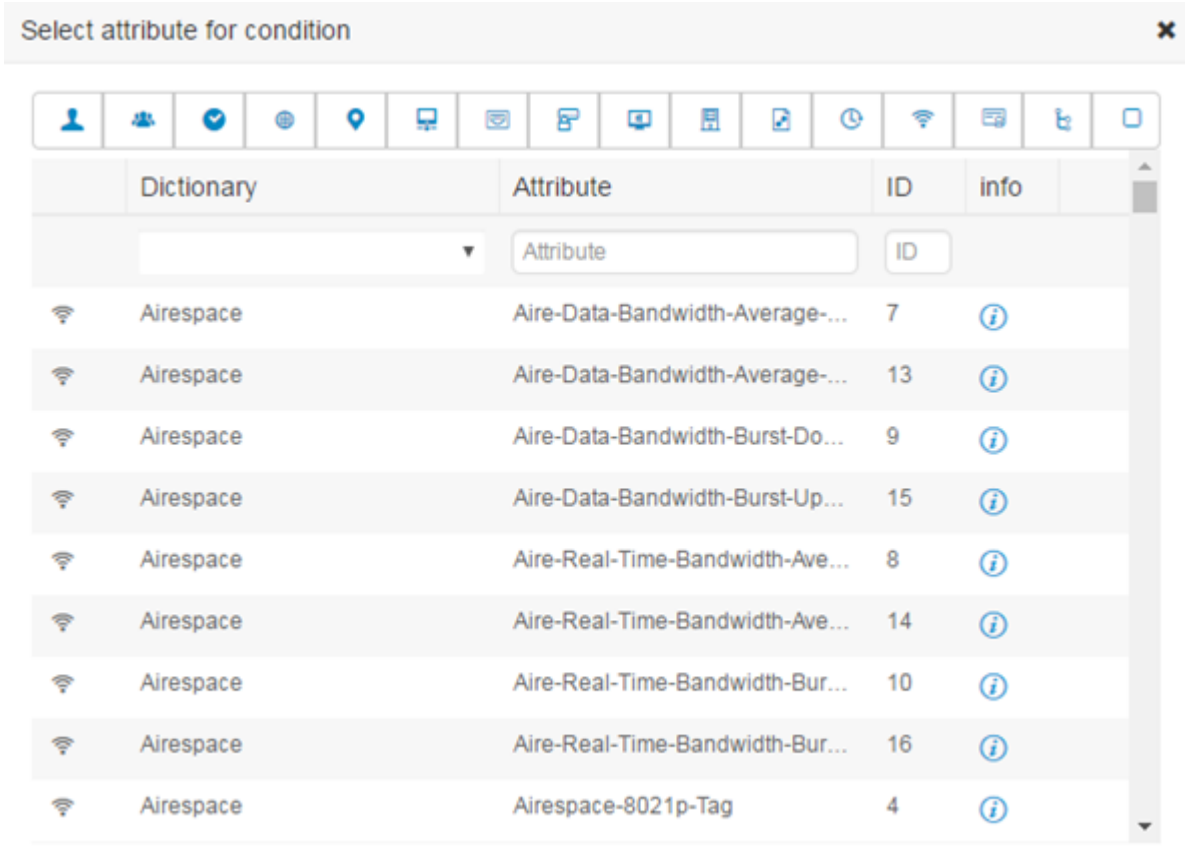
b) フリーテキストで条件ブロックを検索するには、検索しているブロックの名前に表示される [名前で検索（Search by Name）] フリー テキスト フィールドに、任意の用語または用語の一部を入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。カテゴリが選択されていない場合（いずれのアイコンも強調表示されていない場合）、結果にはすべてのカテゴリの条件ブロックが含まれます。カテゴリ アイコンがすでに選択されている場合（表示されているリストがすでにフィルタされている場合）、表示される結果には、特定のテキストを使用する特定のカテゴリのブロックのみが含まれます。

c) 条件ブロックを見つけたら、それを [エディタ（Editor）] にドラッグし、作成しているブロックの正しいレベルにドロップします。間違った場所にドロップした場合は、正しく配置されるまで [エディタ（Editor）] 内から再度ドラッグ アンド ドロップできます。

d) 作業中の条件に関連する変更を加えるには、[エディタ（Editor）] からブロックにカーソルを合わせ、[編集（Edit）] をクリックしてルールを変更し、[ライブラリ（Library）] のルールをその変更で上書きしたり、ルールを新しいブロックとして [ライブラリ（Library）] に保存します。
[エディタ（Editor）] にドロップされたときに読み込み専用であったブロックを編集できるようになりました。そのブロックには、[エディタ（Editor）] 内の他のすべてのカスタマイズされたルールと同じフィールド、構造、リスト、アクションがあります。このルールの編集の詳細については、次の手順に進みます。

ステップ 4 同じレベルでルールを追加するには、現在のレベルに演算子を追加します。[AND]、[OR]、または ['Is not' に設定（Set to 'Is not'）] を選択します。['Is not' に設定（Set to 'Is not'）] は、個々のルールにも適用できます。

ステップ 5 属性ディクショナリを使用してルールを作成および編集するには、[クリックして属性を追加する（Click to add an attribute）] フィールドをクリックします。次の画像のように、属性セレクタが開きます。



属性セレクタの要素を次の表で説明します。

フィールド	使用上のガイドライン
[属性カテゴリ（Attribute Category）] ツールバー	異なる属性カテゴリごとに固有のアイコンが含まれています。カテゴリ別に表示をフィルタ処理するには任意の属性カテゴリ アイコンを選択します。 強調表示されたアイコンをクリックすると選択解除され、フィルタが削除されます。
ディクショナリ	属性が格納されているディクショナリの名前を示します。ベンダー ディクショナリ別に属性をフィルタリングするには、ドロップダウンから特定のディクショナリを選択します。
属性（Attribute）	属性の名前を示します。属性をフィルタリングするには、使用可能なフィールドに属性名のフリー テキストを入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。

フィールド	使用上のガイドライン
ID	一意の属性 ID 番号を示します。属性をフィルタリングするには、使用可能なフィールドに ID 番号を入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。
情報（Info）	属性に関する詳細を表示するには、関連する属性の行にある情報アイコンの上にカーソルを置きます。

a) 属性セレクタ検索で、必要な属性をフィルタリングして検索します。属性セレクタの任意の部分でフリー テキストをフィルタリングまたは入力すると、他のフィルタがアクティブ化されていない場合、結果には選択されたフィルタのみに関連するすべての属性が含まれます。複数のフィルタを使用すると、表示される検索結果はすべてのフィルタに一致します。たとえば、ツールバーの [ポート（Port）] アイコンをクリックし、[属性（Attribute）] 列に「auth」と入力すると、名前に「auth」が含まれる [ポート（Ports）] カテゴリの属性のみが表示されます。カテゴリを選択すると、ツールバーのアイコンが青色で強調表示され、フィルタリングされたリストが表示されます。カテゴリ ツールバーの強調表示されたアイコンを再度クリックすると選択解除され、そのフィルタが削除されます。

b) 関連する属性をルールに追加するには、その属性を選択します。
属性セレクタが閉じ、選択した属性が [クリックして属性を追加する（Click to add an attribute）] フィールドに追加されます。

c) [等しい（Equals）] ドロップダウンリストから、関連する演算子を選択します。

選択するすべての属性に「Equals」、「Not Equals」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現（REGEX）をサポートし、使用します。

単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数値属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。

d) [属性値（Attribute value）] フィールドから、次のいずれかを実行します。

- フィールドにフリー テキスト値を入力します。
- リストから動的にロードする値を選択します（関連する場合は、前の手順で選択した属性によって異なります）。
- 条件ルールの値として別の属性を使用します。フィールドの横にあるテーブル アイコンを選択して、属性セレクタを開き、関連する属性を検索、フィルタリング、および選択します。属性セレクタが閉じ、選択した属性が [属性値（Attribute value）] フィールドに追加されます。

ステップ 6 条件ブロックとして [ライブラリ（Library）] にルールを保存します。

a) [ライブラリ（Library）] にブロックとして保存するルールまたはルールの階層の上にマウス カーソルを置きます。[重複（Duplicate）] ボタンと [保存（Save）] ボタンは、単一の条件ブロックとして保存できるルールまたはルールのグループに対して表示されます。ルールのグループをブロックとし

て保存する場合は、階層全体のブロックされた領域内の階層全体の下部からアクション ボタンを選択します。

b) [保存（Save）] をクリックします。[保存（Save）] 条件画面が表示されます。

c) 次のどちらかを選択します。

- [既存のライブラリ条件に保存（Save to Existing Library Condition）] : [ライブラリ（Library）] 内の既存の条件ブロックを作成した新しいルールで上書きし、[リストから選択（Select from list）] ドロップダウンリストから上書きする条件ブロックを選択するには、このオプションを選択します。
- [新しいライブラリ条件として保存（Save as a new Library Condition）] : [条件名（Condition Name）] フィールドにブロックの一意の名前を入力します。

d) 必要に応じて、[説明（Description）] フィールドに説明を入力します。この説明は、[ライブラリ（Library）]内の任意の条件ブロックの情報アイコン上にマウスを置いた場合に表示され、さまざまな条件ブロックとその用途をすばやく識別できます。

e) [保存（Save）] をクリックして、条件ブロックを [ライブラリ（Library）] に保存します。

ステップ 7 新しい子レベルに新しいルールを作成するには、[AND] または [OR] をクリックして、既存の親階層と作成している子階層の間に正しい演算子を適用します。選択した演算子を使用して、演算子を選択したルールまたは階層の子として、エディタ階層に新しいセクションが追加されます。

ステップ 8 現在の既存のレベルで新しいルールを作成するには、該当するレベルから [新規（New）] をクリックします。新しいルールの新しい空の行が、開始したレベルと同じレベルで表示されます。

ステップ 9 [X] をクリックして、[エディタ（Editor）] とそのすべての子から条件を削除します。

ステップ 10 [重複（Duplicate）] をクリックすると、階層内の特定の条件が自動的にコピー アンド ペーストされ、同じレベルで追加の同一の子が作成されます。[重複（Duplicate）]ボタンをクリックしたレベルに応じて、子の有無にかかわらず個々のルールを複製できます。

ステップ 11 ページ下部の [使用（Use）] をクリックして、[エディタ（Editor）] で作成した条件を保存し、その条件をポリシー セットに実装します。

特別なネットワーク アクセス条件

この項では、ポリシーセットを作成するときに役立つ固有条件について説明します。これらの条件は、[条件スタジオ（Conditions Studio）]から作成することはできず、独自のプロセスがあります。

デバイス ネットワーク条件の設定

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [デバイス ネットワーク条件（Device Network Conditions）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IP アドレス：IP アドレスまたはサブネットの一覧を、1 行に 1 つ追加できます。IP アドレス/サブネットは IPv4 または Ipv6 形式で指定できます。
- デバイス名（Device Name）：デバイス名の一覧を、1 行に 1 つ追加することができます。ネットワーク デバイス オブジェクトで設定されているものと同じデバイス名を入力する必要があります。
- [デバイス グループ（Device Groups）]：ルート NDG、カンマ、（ルート NDG 配下の）NDG の順でタプル一覧を追加できます。タプルは、1 行に 1 つにする必要があります。

ステップ 5 [送信（Submit）] をクリックします。

デバイス ポート ネットワーク条件の設定

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [デバイス ポート ネットワーク条件（Device Port Network Conditions）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IP アドレス（IP Addresses）：次の順序で詳細を入力します。IP アドレスまたはサブネット、カンマ、（デバイスによって使用される）ポート。タプルは、1 行に 1 つにする必要があります。
- デバイス（Devices）：次の順序で詳細を入力します。デバイス名、カンマ、ポート。タプルは、1 行に 1 つにする必要があります。ネットワーク デバイス オブジェクトで設定されているものと同じデバイス名を入力する必要があります。
- デバイス グループ（Device Groups）：次の順序で詳細を入力します。ルート NDG、カンマ、（ルート下の）NDG、ポート。タプルは、1 行に 1 つにする必要があります。

ステップ 5 [送信（Submit）] をクリックします。

エンドステーション ネットワーク条件の設定

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [エンドステーション ネットワーク条件（Endstation Network Conditions）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IP アドレス：IP アドレスまたはサブネットの一覧を、1 行に 1 つ追加できます。IP アドレス/サブネットは IPv4 または Ipv6 形式で指定できます。
- MAC アドレス：カンマ区切りのエンドステーション MAC アドレスと宛先 MAC アドレスの一覧を入力できます。各 MAC アドレスには 12 桁の 16 進数を含め、次の形式のいずれかで指定してください。nn:nn:nn:nn:nn:nn、nn-nn-nn-nn-nn-nn、nnnn.nnnn.nnnn、nnnnnnnnnnnn。

  エンドステーション MAC または宛先 MAC が必要でない場合は、代わりにトークン「-ANY-」を使用します。
- CLI/DNIS：カンマ区切りの発信者 ID（CLI）および受信者 ID（DNIS）の一覧を追加できます。発信者 ID（CLI）または受信者 ID（DNIS）が必要でない場合は、代わりにトークン「-ANY-」を使用します。

ステップ 5 [送信（Submit）] をクリックします。

時刻と日付の条件の作成

[ポリシー要素条件（Policy Elements Conditions）] ページを使用して、時刻と日付のポリシー要素条件を表示、作成、変更、削除、複製、および検索します。ポリシー要素は、設定した特定の時刻と日付の属性設定に基づく条件を定義する共有オブジェクトです。

時刻と日付の条件を使用すると、Cisco ISE システム リソースにアクセスする権限を、作成した属性設定で指定された特定の時刻と日付に設定または制限できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [共通（Common）] > [時刻と日付（Time and Date）] > [追加（Add）]** を選択します。

ステップ 2 フィールドに適切な値を入力します。

- [標準設定（Standard Settings）] 領域で、アクセスを提供する日時を指定します。
- [例外（Exceptions）] 領域で、アクセスを制限する日時の範囲を指定します。

ステップ 3 [送信（Submit）] をクリックします。

許可ポリシーで IPv6 条件属性を使用する

Cisco ISE では、エンドポイントからの IPv6 トラフィックを検出、管理、保護できます。

IPv6 対応エンドポイントが Cisco ISE ネットワークに接続すると、IPv6 ネットワーク経由でネットワークアクセスデバイス（NAD）と通信します。NADは、アカウンティングおよびプロファイリングの情報をエンドポイント（IPv6 値を含む）から Cisco ISE に IPv4 ネットワークを介して伝達します。ルール条件で IPv6 属性を使用して、IPv6 対応エンドポイントからのそのような要求を処理し、エンドポイントが準拠していることを保証するための、認証プロファイルおよびポリシーを Cisco ISE で設定できます。

ワイルドカード文字は、IPv6 プレフィックスと IPv6 インターフェイスの値で使用できます。たとえば、2001:db8:1234::/48 です。

サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記：コロンで区切られた 4 つの 16 進数桁の 8 つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。
- 短縮表記：1 つのグループ内にある先行ゼロは除きます。ゼロのグループを 2 つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切りの 4 つの表記（IPv4 対応付けおよび IPv4 互換性 IPv6 アドレス）：たとえば、::ffff:192.0.2.128 です。

サポートされている IPv6 属性は次のとおりです。

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address
- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

サポートされるシスコの属性と値のペアおよび対応する IETF 属性を次の表に示します：

シスコの属性と値のペア	IETF 属性
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address

シスコの属性と値のペア	IETF 属性
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

[RADIUSライブログ（RADIUS Live Logs）] ページ、RADIUS 認証レポート、RADIUS アカウンティング レポート、現在アクティブなセッション レポート、RADIUS エラー レポート、設定が誤っている NAS レポート、EPS 監査レポート、および設定が誤っているサプリカント レポートは、IPv6 アドレスをサポートしています。[RADIUSライブログ（RADIUS Live Logs）] ページ、またはこれらのレポートのいずれかから、これらのセッションの詳細を表示できます。IPv4、IPv6、または MAC アドレスでレコードをフィルタリングできます。

（注） IPv6 対応の DHCPv6 ネットワークに Android デバイスを接続すると、そのデバイスは DHCP サーバからリンクローカルの IPv6 アドレスのみを受信します。したがって [ライブ ログ（Live Log）] と [エンドポイント（Endpoints）] ページ（**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]**）にはグローバル IPv6 アドレスは表示されません。

次の手順は、許可ポリシーに IPv6 属性を設定する方法を説明します。

始める前に

展開内の NAD が IPv6 による AAA をサポートしていることを確認します。NAD で IPv6 の AAA サポートをイネーブルにする方法については、『**AAA Support for IPv6**』を参照してください。

ステップ 1 ネットワーク アクセス ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ポリシー セット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワーク センター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシー セット（Device Admin Policy Sets）]** を選択します。

ステップ 2 許可ルールを作成します。

ステップ 3 許可ルールを作成するときは、[条件スタジオ（Conditions Studio）]から条件を作成します。[条件スタジオ（Conditions Studio）] で、RADIUS ディクショナリから、RADIUS IPv6 属性、演算子、および値を選択します。

ステップ 4 [完了（Done）][保存（Save）]をクリックして、許可ルールをポリシー セットに保存します。

ポリシー セット プロトコルの設定

これらのプロトコルを使用してポリシー セットを作成、保存、実装する前に、Cisco ISE でグローバル プロトコル設定を定義する必要があります。[プロトコル設定（Protocol Settings）] ページを使用して、ネットワーク内の他のデバイスと通信する Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）、Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）、および Protected Extensible Authentication Protocol（PEAP）の各プロトコルのグローバル オプションを定義できます。

サポートされているネットワーク アクセス ポリシー セット プロトコル

ネットワーク アクセス ポリシー セット ポリシーの定義時に選択可能なプロトコルを次に示します。

- Password Authentication Protocol（PAP）
- Protected Extensible Authentication Protocol（PEAP）
- Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）
- Extensible Authentication Protocol-Message Digest 5（EAP-MD5）
- Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）
- Extensible Authentication Protocol-Tunneled Transport Layer Security（EAP-TTLS; 拡張認証プロトコル - トンネル方式トランスポート層セキュリティ）
- Protected Extensible Authentication Protocol-Transport Layer Security（PEAP-TLS）

プロトコルとして EAP-FAST を使用するためのガイドライン

EAP-FAST を認証プロトコルとして使用する場合は、次のガイドラインに従ってください。

- EAP-FAST 受信クライアント証明書が認証されたプロビジョニングで有効な場合は、EAP-TLS 内部方式を有効にすることを強く推奨します。認証されたプロビジョニングの EAP-FAST 受信クライアント証明書は別の認証方式ではなく、ユーザを認証するのと同じ証明書のクレデンシャルのタイプを使用した略式のクライアント証明書認証ですが、内部方式を実行する必要がありません。
- PAC なしの完全なハンドシェイクおよび認定 PAC プロビジョニングとの認証プロビジョニング作業に対するクライアント証明書を受け入れます。PAC なしのセッション再開、匿名 PAC プロビジョニング、PAC ベース認証には動作しません。

- EAP 属性は、認証の順序とは関係なく、ID ごとにモニタリング ツールの認証詳細に、まずユーザ順、次にマシン順に表示されます（したがって EAP チェーニングは 2 回表示されます）。
- EAP-FAST 認可 PAC が使用される場合、ライブ ログに表示される EAP 認証方式は完全認証に使用される認証方式と同じ（PEAP でのように）であり、参照としてではありません。
- EAP チェーン モードでは、トンネル PAC が期限切れになると、ISE がプロビジョニングにフォールバックし、AC 要求ユーザおよびマシン認可 PAC（マシン許可 PAC）はプロビジョニングできません。後続の PAC ベースの認証通信で AC が要求したときにプロビジョニングされます。
- Cisco ISE がチェーンに、AC がシングル モードに設定されている場合は、AC は IdentityType TLV で ISE に応答しますただし、2 番目の ID 認証は失敗します。この通信から、クライアントのチェーニング実行は適切であるが、現在はシングル モードで構成されていることがわかります。
- Cisco ISE は AD にのみチェーンしている EAP-FAST のマシンとユーザの両方の属性およびグループをサポートします。LDAP および内部 DB ISE に対しては、最新の ID 属性のみを使用します。

（注） High Sierra、Mojave、または Catalina MAC OSX デバイスに EAP-FAST 認証プロトコルを使用すると、「EAP-FAST 暗号化バインドの検証に失敗しました（EAP-FAST cryptobinding verification failed）」というメッセージが表示される場合があります。これらの MAC OSX デバイスに EAP-FAST を使用する代わりに PEAP または EAP-TLS を使用するよう、[許可プロトコル（Allowed Protocols）] ページの [優先EAPプロトコル（Preferred EAP Protocol）] フィールドを設定することをお勧めします。

EAP-FAST の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [EAP-FAST の設定（EAP-FAST Settings）]** を選択します。

ステップ 2 EAP-FAST プロトコルの定義に必要な詳細を入力します。

ステップ 3 以前に生成されたマスター キーおよび PAC をすべて失効させるには、[失効（Revoke）] をクリックします。

ステップ 4 EAP-FAST 設定を保存するには、[保存（Save）] をクリックします。

EAP-FAST の PAC の生成

Cisco ISE の [PAC の生成（Generate PAC）] オプションを使用して、EAP-FAST プロトコルのトンネル PAC またはマシン PAC を生成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）]** を選択します。
ステップ 2 左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。
ステップ 3 **[EAP-FAST] > [PAC の生成（Generate PAC）]** を選択します。
ステップ 4 EAP-FAST プロトコルのマシン PAC を生成する場合に必要な詳細を入力します。
ステップ 5 [PAC の生成（Generate PAC）] をクリックします。

EAP-FAST 設定

次の表に、EAP-FAST、EAP-TLS、および PEAP プロトコルを設定するために使用できる [プロトコル設定（Protocol Settings）] ページのフィールドを示します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-FAST] > [EAP-FAST 設定（EAP-FAST Settings）]** です。

表 *133 : EAP-FAST* の設定

フィールド	使用上のガイドライン
機関識別情報の説明（Authority Identity Info Description）	クレデンシャルをクライアントに送信する Cisco ISE ノードを説明したわかりやすい文字列を入力します。クライアントは、この文字列をタイプ、長さ、および値（TLV）の Protected Access Credentials（PAC）情報で認識できます。デフォルト値は、Identity Services Engine です。
マスター キー生成期間（Master Key Generation Period）	マスターキー生成期間を、秒、分、時間、日、または週単位で指定します。値は、1 ～ 2147040000 秒の正の整数である必要があります。デフォルトは 604800 秒で、これは 1 週間と同等です。
すべてのマスター キーおよび PAC の失効（Revoke all master keys and PACs）	すべてのマスターキーと PAC を失効させるには、[失効（Revoke）] をクリックします。

フィールド	使用上のガイドライン
PAC なしセッション再開の有効化（Enable PAC-less Session Resume）	PAC ファイルなしで EAP-FAST を使用する場合は、このチェックボックスをオンにします。
PAC なしセッションのタイムアウト（PAC-less Session Timeout）	PAC なしセッションの再開がタイムアウトするまでの時間を秒単位で指定します。デフォルトは 7200 秒です。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
プロトコルとして EAP-FAST を使用するためのガイドライン （1046 ページ）
EAP-FAST の利点 （1095 ページ）
EAP-FAST の設定 （1047 ページ）

PAC の設定

次の表では、[PAC の生成（Generate PAC）] ページ上のフィールドについて説明します。これらのフィールドを使用して、EAP-FAST 認証用の Protected Access Credentials を設定します。このページのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-FAST]** > **[PAC の生成（Generate PAC）]** です。

表 *134 : EAP-FAST* の *PAC* の生成の設定

フィールド	使用上のガイドライン
トンネル PAC（Tunnel PAC）	トンネル PAC を生成するには、このオプション ボタンをクリックします。
マシン PAC（Machine PAC）	マシン PAC を生成するには、このオプション ボタンをクリックします。
TrustSec PAC	TrustSec PAC を生成するには、このオプション ボタンをクリックします。

フィールド	使用上のガイドライン
ID（Identity）	（トンネル PAC およびマシン PAC の ID フィールド用）EAP-FAST プロトコルによって「内部ユーザ名」として示されるユーザ名またはマシン名を指定します。ID 文字列がそのユーザ名と一致しない場合、認証は失敗します。これは、適応型セキュリティ アプライアンス（ASA）で定義されているホスト名です。ID 文字列は、ASA ホスト名に一致する必要があります。一致しない場合、ASA は生成された PAC ファイルをインポートできません。TrustSec PAC を生成する場合、[ID（Identity）] フィールドにより TrustSec ネットワーク デバイスのデバイス ID が指定され、EAP-FAST プロトコルによりイニシエータ ID とともに提供されます。ここに入力した ID 文字列がそのデバイス ID に一致しない場合、認証は失敗します。
PAC 存続可能時間（PAC Time To Live）	（トンネル PAC およびマシン PAC 用）PAC の有効期限を指定する値を秒単位で入力します。デフォルトは 604800 秒で、これは 1 週間と同等です。この値は、1 ～ 157680000 秒の正の整数である必要があります。TrustSec PAC に対しては、日、週、月、または年単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。
暗号化キー（Encryption Key）	暗号キーを入力します。キーの長さは 8 ～ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。
期限日（Expiration Date）	（TrustSec PAC のみ）有効期限は、PAC 存続可能時間に基づいて計算されます。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
プロトコルとして EAP-FAST を使用するためのガイドライン （1046 ページ）
EAP-FAST の PAC の生成 （1048 ページ）

認証プロトコルとしての EAP-TTLS の使用

EAP-TTLS は、EAP-TLS プロトコルの機能を拡張する 2 フェーズ プロトコルです。フェーズ 1 では、セキュアなトンネルを構築し、フェーズ 2 で使用するセッション キーを導出し、サー

バとクライアント間で属性および内部方式データを安全にトンネリングします。フェーズ2中では、トンネリングされた属性を使用して、多数のさまざまなメカニズムを使用する追加認証を実行できます。

Cisco ISE は、次のようなさまざまな TTLS サプリカントから認証を処理できます。

- Windows 上の AnyConnect Network Access Manager（NAM）
- Windows 8.1 ネイティブ サプリカント
- セキュア W2（MultiOS で JoinNow とも呼ばれます）
- MAC OS X ネイティブ サプリカント
- IOS ネイティブ サプリカント
- Android ベースのネイティブ サプリカント
- Linux WPA サプリカント

（注） 暗号化バインドが必要な場合は、内部方式として EAP-FAST を使用する必要があります。

EAP-TLS の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロトコル（Protocols）]>[EAP-TTLS] を選択します。

ステップ 2 [EAP-TTLS設定（EAP-TTLS Settings）] ページに必要な詳細を入力します。

ステップ 3 [保存（**Save**）] をクリックします。

EAP-TTLS 設定

次の表では、[EAP-TTLS設定（EAP-TTLS Settings）]ページのフィールドについて説明します。このページへのナビゲーション パスは、[管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロトコル（Protocols）]>[EAP-TTLS] です。

表 *135 : EAP-TTLS* 設定

フィールド	使用上のガイドライン
EAP-TTLSセッションの再開を有効にする（Enable EAP-TTLS Session Resume）	このチェックボックスをオンにすると、Cisco ISE はユーザが EAP-TTLS 認証のフェーズ 2 で正常に認証された場合に限り、EAP-TTLS 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の EAP-TTLS セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、EAP-TTLS のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。 （注） EAP-TTLS セッションが再開されると、内部方式はスキップされます。
EAP-TTLSセッションタイムアウト（EAP-TTLS Session Timeout）	EAP-TTLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
認証プロトコルとしての EAP-TTLS の使用 （1050 ページ）
EAP-TLS の設定 （1051 ページ）

EAP-TLS の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-TLS]** を選択します。

ステップ 2 EAP-TLS プロトコルの定義に必要な詳細を入力します。

ステップ 3 EAP-TLS 設定を保存するには、[保存（Save）] をクリックします。

EAP-TLS 設定

次の表に、EAP-TLS プロトコル設定を行うために使用できる [EAP-TLS 設定（EAP-TLS Settings）] ページのフィールドを示します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-TLS]** です。

表 *136 : EAP-TLS* 設定

フィールド	使用上のガイドライン
EAP-TLS セッションの再開を有効にする（Enable EAP-TLS Session Resume）	完全な EAP-TLS 認証に成功したユーザの簡略化された再認証をサポートする場合にオンにします。この機能により、Secure Sockets Layer（SSL）ハンドシェイクのみでユーザの再認証が可能となり、証明書の適用が不要になります。EAP-TLS セッションは、タイムアウトしていない限り動作を再開します。
EAP-TLS セッション タイムアウト（EAP-TLS Session Timeout）	EAP-TLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。
[ステートレス セッション再開（Stateless Session Resume）]	
マスター キー生成期間（Master Key Generation Period）	マスターキー再生成までの時間を入力します。この値により、マスター キーがアクティブである期間が決定します。この値は秒、分、時、日数、または週数で入力できます。
[取り消し（Revoke）]	これまでに生成されたすべてのマスター キーとチケットをキャンセルするには、[取り消し（Revoke）] をクリックします。このオプションは、セカンダリ ノードでは無効です。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
EAP-TLS の設定 （1052 ページ）

PEAP の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** を選択します。

ステップ 2 左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。
ステップ 3 [PEAP] を選択します。
ステップ 4 PEAP プロトコルの定義に必要な詳細を入力します。
ステップ 5 PEAP 設定を保存するには、[保存（Save）] をクリックします。

PEAP 設定

次の表では、PEAP プロトコル設定を行うために使用できる [PEAP 設定（PEAP Settings）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[PEAP]** です。

表 *137 : PEAP* 設定

フィールド	使用上のガイドライン
PEAP セッションの再開を有効にする（Enable PEAP Session Resume）	このチェックボックスをオンにすると、Cisco ISE はユーザが PEAP 認証のフェーズ 2 で正常に認証された場合に限り、PEAP 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の PEAP セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、PEAP のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。PEAP セッション再開機能を動作させるには、PEAP セッション タイムアウト値を指定する必要があります。
PEAP セッション タイムアウト（PEAP Session Timeout）	PEAP セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。
高速再接続を有効にする（Enable Fast Reconnect）	このチェックボックスをオンにすると、セッション再開機能が有効な場合に、ユーザ クレデンシャルを確認しないで PEAP セッションが Cisco ISE で再開することが許可されます。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
PEAP の設定 （1053 ページ）
PEAP の使用の利点 （1094 ページ）
PEAP プロトコルでサポートされているサプリカント （1094 ページ）
PEAP プロトコルのフロー （1094 ページ）

RADIUS の設定

認証に失敗、または認証成功のレポートの繰り返しの抑制に失敗したクライアントを検出するように RADIUS 設定を設定することができます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）]** を選択します。
ステップ 2 [設定（Settings）] ナビゲーション ペインで [プロトコル（Protocols）] をクリックします。
ステップ 3 [RADIUS] を選択します。
ステップ 4 RADIUS 設定の定義に必要な詳細を入力します。
ステップ 5 [保存（Save）] をクリックして、設定を保存します。

RADIUS 設定

次の表に、[RADIUS 設定（RADIUS Settings）] ページにある各フィールドの説明を示します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS]** です。

[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）] オプションを有効にすると、認証が繰り返し失敗するクライアントは監査ログに出力されず、指定された期間にわたってこれらのクライアントからの要求が自動的に拒否されます。また、認証失敗回数を指定できます。失敗回数がこの回数を超えると、これらのクライアントからの要求は拒否されます。たとえばこの値を 5 に設定すると、クライアント認証が 5 回失敗した場合、指定された期間にわたってそのクライアントから受信する要求はすべて拒否されます。

（注） 認証失敗の原因が誤ったパスワードの入力である場合、クライアントは抑制されません。

表 *138 : RADIUS* 設定

フィールド	使用上のガイドライン
[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）]	
[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）]	同じ理由で繰り返し認証に失敗するクライアントを抑止するには、このチェックボックスをオンにします。これらのクライアントは監査ログに出力されず、また [繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] オプションが有効な場合には、指定された期間にわたってこれらのクライアントからの要求が拒否されます。

フィールド	使用上のガイドライン
[2 回の失敗を検出する期間（Detect Two Failures Within）]	分単位で時間間隔を入力します。クライアントがこの期間内に同じ理由で 2 回認証に失敗すると、監査ログに出力されず、また[繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] オプションが有効な場合には、指定された期間にわたってこのクライアントからの要求が拒否されます。
[失敗を報告する間隔（Report Failures Once Every）]	報告対象の認証失敗の時間間隔を分単位で入力します。たとえば、この値を 15 分に設定すると、繰り返し認証に失敗するクライアントが 15 分に 1 回だけ監査ログに報告されるため、報告の重複が防止されます。
[繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）]	認証が繰り返し失敗するクライアントからの RADIUS 要求を自動的に拒否するには、このチェック ボックスをオンにします。Cisco ISE による不要な処理を防ぎ、Denial of Service（DoS）攻撃から防御するには、このオプションを有効にします。
[自動拒否前の失敗回数（Failures Prior to Automatic Rejection）]	認証失敗回数を入力します。認証失敗回数がこの値を超えると、繰り返し失敗するクライアントからの要求は自動的に拒否されます。設定されている期間（[要求を拒否する期間（Continue Rejecting Requests for）] で指定）にわたり、これらのクライアントから受信する要求はすべて自動的に拒否されます。この期間が経過した後では、これらのクライアントからの認証要求が処理されます。
[要求を拒否する期間（Continue Rejecting Requests for）]	繰り返し失敗するクライアントからの要求を拒否する時間間隔を分単位で入力します。
[繰り返し発生するアカウンティング更新を無視する期間（Ignore Repeated Accounting Updates Within）]	この期間内に繰り返し発生するアカウンティング更新は無視されます。
[成功レポートの抑制（Suppress Successful Reports）]	
繰り返される認証成功の抑制（Suppress Repeated Successful Authentications）	直近の 24 時間で、ID、ネットワーク デバイス、および許可のコンテキストに変更がない認証要求成功が繰り返し報告されないようにするには、このチェックボックスをオンにします。

フィールド	使用上のガイドライン
[認証の詳細（Authentications Details）]	
[次よりも長いステップを強調表示（Highlight Steps Longer Than）]	ミリ秒単位で時間間隔を入力します。1つのステップの実行が指定のしきい値を超えると、認証詳細ページでそのステップがクロック アイコンでマークされます。
無効なユーザ名を開示する（Disclose Invalid Usernames）	このチェック ボックスをオンにすると、RADIUS ライブ ログに「USERNAME」または「INVALID」とラベル付けされたユーザ名が開示されます。認証概要レポートのように、RADIUS ライブ ログにもログイン済みのユーザ名を表示できます。このオプションは、30分後に自動的に無効になります。
RADIUS UDP ポート	
認証ポート（Authentication Port）	RADIUS UDP の認証フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1812 とポート 1645 が使用されます。値の範囲は 1024 ～ 65535 です。
アカウンティング ポート（Accounting Port）	RADIUS UDP のアカウンティング フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1813 とポート 1646 が使用されます。値の範囲は 1024 ～ 65535 です。 （注） これらのポートが他のサービスにより使用されていないことを確認します。
RADIUS DTLS	
認証およびアカウンティング ポート（Authentication and Accounting Port）	RADIUS DTLS の認証およびアカウンティング フローに使用するポートを指定します。デフォルトでは、ポート 2083 が使用されます。値の範囲は 1024 ～ 65535 です。 （注） このポートが他のサービスにより使用されていないことを確認します。

フィールド	使用上のガイドライン
アイドル タイムアウト	パケットがネットワーク デバイスから届かなかったら、TLS セッションを終了する前に、Cisco ISE を待機する時間を秒単位で入力します。デフォルト値は 120 秒です。有効な範囲は 60 ～ 600 秒です。
RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification）	Cisco ISE が DTLS ハンドシェイク中に RADIUS/DTLS クライアントの ID を確認するようにする場合は、このチェックボックスをオンにします。クライアント ID が有効でない場合、Cisco ISE はハンドシェイクに失敗します。デフォルトのネットワーク デバイスが設定されている場合、ID チェックはスキップされます。ID チェックは次の順序で実行されます。 1. クライアント証明書にサブジェクト代替名（SAN）属性が含まれている場合： • SAN に DNS 名が含まれている場合、証明書に指定されている DNS 名が Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。 • SAN に IP アドレスが含まれていて（DNS 名が含まれていない場合）、証明書で指定された IP アドレスが Cisco ISE で設定されているすべてのデバイス IP アドレスと比較されます。 2. 証明書に SAN が含まれていない場合、サブジェクト CN は Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。不一致の場合、Cisco ISE はハンドシェイクに失敗します。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
Cisco ISE の RADIUS プロトコルのサポート （1061 ページ）
RADIUS の設定 （1055 ページ）

セキュリティ設定の構成

セキュリティ設定を構成するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [セキュリティ設定（Security Settings）]** を選択します。

ステップ 2 [セキュリティ設定（Security Settings）] ページで、次の必須オプションを選択します。

- TLS 1.0を許可（Allow TLS 1.0）：次のワークフローについて、従来のピアとの通信に TLS 1.0 を許可します。
  - Cisco ISE は、EAP サーバとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- TLS 1.1を許可（Allow TLS 1.1）：次のワークフローについて、従来のピアとの通信に TLS 1.1 を許可します。
  - Cisco ISE は、EAP サーバとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- SHA1暗号化を許可（Allow SHA1 Ciphers）：次のワークフローについて、ピアとの通信に SHA-1 暗号化を許可します。
  - Cisco ISE は、EAP サーバとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバとして設定されます
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます

  （注） セキュリティを強化するために、SHA-256 または SHA-384 暗号化を使用することを推奨します。

- ECDHE-RSA暗号化を許可（Allow ECDHE-RSA Ciphers）：次のワークフローについて、ピアとの通信に ECDHE-RSA 暗号化を許可します。
  - Cisco ISE は、EAP サーバとして設定されます

- Cisco ISE は、RADIUS DTLS サーバとして設定されます
- Cisco ISE は、RADIUS DTLS クライアントとして設定されます
- Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします
- Cisco ISE は、セキュアな syslog クライアントとして設定されます
- Cisco ISE は、セキュアな LDAP クライアントとして設定されます

- 3DES暗号化を許可（Allow 3DES ciphers）：次のワークフローについて、ピアとの通信に 3DES 暗号化を許可します。
  - Cisco ISE は、EAP サーバとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバとして設定されます
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます

- 目的の検証なしで証明書を受け入れる（Accept Certificates without Validating Purpose）：ISE が EAP または RADIUS DTLS サーバとして機能する場合、キー使用拡張に ECDHE-ECDSA 暗号化の keyAgreement ビットまたは他の暗号化の keyEncipherment ビットが含まれているかどうかを確認することなく、クライアント証明書が受け入れられます。

- ISE の DSS 暗号化をクライアントとして許可（Allow DSS ciphers for ISE as a client）：次のワークフローについて、Cisco ISE がクライアントとして機能する場合、サーバとの通信に DSS 暗号化を許可します。
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます

- ISEの従来の安全でないTLS再ネゴシエーションをクライアントとして許可（Allow Legacy Unsafe TLS Renegotiation for ISE as a Client）：次のワークフローについて、安全な TLS 再ネゴシエーションをサポートしていない従来の TLS サーバとの通信を許可します。
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます

ステップ 3 [保存（**Save**）] をクリックします。

Cisco ISE の RADIUS プロトコルのサポート

RADIUS は、クライアント/サーバ プロトコルです。リモート アクセス サーバは、このプロトコルを使用して中央サーバと通信してダイヤルイン ユーザを認証し、要求されたシステムまたはサービスへのアクセスを許可します。RADIUS を使用すると、すべてのリモート サーバが共有できる中央データベースでユーザ プロファイルを管理できます。このプロトコルはセキュリティを向上させます。また、このプロトコルを使用して、単一の管理ネットワーク ポイントで適用されるポリシーを設定できます。

RADIUS は、Cisco ISE の RADIUS クライアントとしても機能し、リモート RADIUS サーバへの要求をプロキシ処理します。また、アクティブ セッション中に許可変更（CoA）アクティビティを提供します。

Cisco ISE では、RFC 2865 と、その仕様および拡張仕様に記載されているすべての一般的な RADIUS 属性の包括的なサポートに従って、RADIUS プロトコルのフローがサポートされます。Cisco ISE では、Cisco ISE ディクショナリで定義されているベンダーだけを対象に、ベンダー固有属性の解析がサポートされます。

RADIUS インターフェイスでは、RFC 2865 で定義されている次の属性データ型がサポートされます。

- テキスト（Unicode Transformation Format（UTF））
- 文字列（バイナリ）
- アドレス（IP）
- 整数（Integer）
- 時刻（Time）

ISE コミュニティ リソース

Cisco ISE でサポートされるネットワーク アクセス属性については、「ISE Network Access Attributes」を参照してください。

許可されるプロトコル

次の表に、認証中に使用するプロトコルを設定できるようにする [許可されるプロトコル（Allowed Protocols）] ウィンドウのフィールドを示します。ナビゲーション パスは、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authentication）]** > **[許可されるプロトコル（Allowed Protocols）]** です。

表 *139 :* 許可されるプロトコル

フィールド名	使用上のガイドライン
[許可されているプロトコル（Allowed Protocols）] > [認証バイパス（Authentication Bypass）]	
ホスト ルックアップの処理（Process Host Lookup）	Cisco ISE がホスト ルックアップ要求を処理できるようにするには、このチェックボックスをオンにします。ホストルックアップ要求は、RADIUS Service-Type が 10（Call-Check）に等しく、ユーザ名が Calling-Station-ID に等しい場合は PAP/CHAP プロトコルに対して処理されます。ホスト ルックアップ要求は、Service-Type が 1（Framed）に等しく、ユーザ名が Calling-Station-ID に等しい場合は EAP-MD5 プロトコルに対して処理されます。Cisco ISE でホスト ルックアップ要求を無視し、認証にシステム ユーザ名属性の元の値を使用するには、このチェックボックスをオフにします。オフにすると、メッセージ処理はプロトコル（たとえば PAP）に従って行われます。 （注） このオプションを無効にすると、既存の MAB 認証で障害が発生する可能性があります。
[許可されているプロトコル（Allowed Protocols）] > [認証プロトコル（Authentication Protocols）]	
PAP/ASCII を許可（Allow PAP/ASCII）	このオプションによって、PAP/ASCII が有効になります。PAP は、平文パスワード（つまり暗号化されていないパスワード）を使用する最も安全性の低い認証プロトコルです。
CHAP を許可（Allow CHAP）	このオプションによって、CHAP 認証が有効になります。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。
MS-CHAPv1 を許可（Allow MS-CHAPv1）	MS-CHAPv1 を有効にするには、このチェックボックスをオンにします。
MS-CHAPv2 を許可（Allow MS-CHAPv2）	MS-CHAPv2 を有効にするには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
EAP-MD5 を許可（Allow EAP-MD5）	EAP ベースの MD5 パスワード ハッシュ認証を有効にするには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
EAP-TLS を許可（Allow EAP-TLS）	

フィールド名	使用上のガイドライン
	EAP-TLS 認証プロトコルを有効にする場合、およびEAP-TLS設定値を設定する場合は、このチェックボックスをオンにします。エンドユーザ クライアントからの EAP Identity 応答で提示されたユーザ ID を Cisco ISE が確認する方法を指定できます。ユーザIDは、エンドユーザ クライアントによって提示された証明書の情報に照らして確認されます。この比較は、Cisco ISE とエンドユーザ クライアントとの間にEAP-TLS トンネルが確立された後に行われます。 （注） EAP-TLS は、証明書ベースの認証プロトコルです。EAP-TLS認証が行われるのは、証明書の設定に必要な手順を完了した場合に限られます。 • [期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）]：ユーザが証明書を更新できるようにする場合は、このチェックボックスをオンにします。このチェックボックスをオンにすると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシールールを設定します。 • [ステートレスセッション再開を有効にする（Enable Stateless Session Resume）]：セッション状態をサーバに保存する必要なしでEAP-TLSセッションを再開できるようにするには、このチェックボックスをオンにします。Cisco ISE では RFC 5077 で記述されているセッション チケット拡張もサポートされます。Cisco ISE はチケットを作成してEAP-TLS クライアントにそのチケットを送信します。クライアントはセッションを再開するためにそのチケットを ISE に提示します。 • [プロアクティブセッションチケット更新（Proactive Session Ticket update）]：セッションチケットが更新される前に経過す

フィールド名	使用上のガイドライン
	る必要がある存続可能時間（TTL）の量を示すパーセント値を入力します。たとえば、値に60を入力すると、セッションチケットはTTLの60パーセントが経過した後で更新されます。 • [セッションチケットの存続時間（Session ticket Time to Live）]：セッションチケットが期限切れになるまでの時間を入力します。この値は、セッション チケットがアクティブである期間を決定します。この値は秒、分、時、日数、または週数で入力できます。
LEAP を許可（Allow LEAP）	Lightweight Extensible Authentication Protocol（LEAP）認証を有効にするには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
PEAP を許可（**Allow PEAP**）	

フィールド名	使用上のガイドライン
	PEAP認証プロトコルおよびPEAP設定値を有効にする場合は、このチェックボックスをオンにします。デフォルトの内部方式は、MS-CHAPv2 です。 [PEAP を許可（Allow PEAP）] チェックボックスをオンにすると、次の PEAP 内部方式を設定できます。 • [EAP-MS-CHAPv2を許可（Allow EAP-MS-CHAPv2）]：内部方式として EAP-MS-CHAPv2 を使用する場合は、このチェックボックスをオンにします。 • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザクレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。 • [EAP-GTCを許可（Allow EAP-GTC）]：内部方式としてEAP-GTC を使用する場合は、このチェックボックスをオンにします。 • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザクレデンシャルを要求する回数を指定します。有効範囲は 0 ～ 3 です。 • [EAP-TLSを許可（Allow EAP-TLS）]：内部方式として EAP-TLS を使用する場合は、このチェックボックスをオンにします。 ユーザによる証明書の更新を許可する場

フィールド名	使用上のガイドライン
	合は、[期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）] チェックボックスをオンにします。このチェックボックスをオンにすると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。 • [暗号化バインドTLVを要求（Require cryptobinding TLV）]：EAP ピアと EAP サーバの両方が PEAP 認証の内部および外部 EAP 認証に参加する場合、このチェックボックスをオンにします。 • [レガシークライアントにのみPEAPv0を許可（Allow PEAPv0 only for legacy clients）]：PEAP サプリカントが PEAPv0 を使用してネゴシエーションできるようにするには、このチェックボックスをオンにします。一部のレガシー クライアントは PEAPv1 プロトコル規格に準拠しません。そのような PEAP カンバセーションがドロップされないようにするには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
EAP-FAST を許可（Allow EAP-FAST）	

フィールド名	使用上のガイドライン
	EAP-FAST 認証プロトコルおよび EAP-FAST 設定を有効にする場合は、このチェックボックスをオンにします。EAP-FAST プロトコルは、同じサーバ上の複数の内部プロトコルをサポートできます。デフォルトの内部方式は、MS-CHAPv2 です。 [EAP-FAST を許可（Allow EAP-FAST）] チェックボックスをオンにすると、EAP-FAST を内部方式として設定できます。 • **EAP-MS-CHAPv2 を許可（Allow EAP-MS-CHAPv2）** • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザクレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。 • **EAP-GTC を許可（Allow EAP-GTC）** [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザクレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。 • [PACの使用（Use PACs）]：EAP-FAST クライアントに認可 Protected Access Credentials（PAC）をプロビジョニングするように Cisco ISE を設定する場合にこのオプションを選択します。追加の PAC オプションが表示されます。 • [PACを使用しない（Don’t use PACs）]：トンネルまたはマシン PAC を発行したり受け入れたりしないで EAP-FAST を使用するように Cisco ISE を設定する場合にこ

フィールド名	使用上のガイドライン
	のオプションを選択します。PAC のすべての要求は無視され、Cisco ISE は PAC を含まない Success-TLV で応答します。 このオプションを選択すると、マシン認証を実行するように Cisco ISE を設定できます。 • [EAP-TLSを許可（Allow EAP-TLS）]：内部方式として EAP-TLS を使用する場合は、このチェックボックスをオンにします。 ユーザによる証明書の更新を許可する場合は、[期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）] チェックボックスをオンにします。このチェックボックスをオンにすると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。

フィールド名	使用上のガイドライン
	• [EAPチェーンを有効化（Enable EAP Chaining）]：EAP チェーンを有効にするには、このチェックボックスをオンにします。 EAP チェーンによって、Cisco ISE はユーザ認証とマシン認証の結果を関連付け、EAPChainingResult 属性を使用して適切な許可ポリシーを適用することができます。 EAP チェーンには、クライアント デバイスで EAP チェーンをサポートするサプリカントが必要です。サプリカントで[ユーザ認証およびマシン認証（User and Machine Authentication）] オプションを選択します。 EAP チェーンは、EAP-FAST プロトコル（PAC ベース モードおよび PAC レス モードの両方）を選択するときに使用できます。 PAC ベースの認証では、ユーザ認可 PAC またはマシン認可 PAC のいずれかを使用するか、両方を使用して内部方式をスキップすることができます。 証明書ベースの認証では、（許可されるプロトコル サービスの）EAP-FAST プロトコルに対して[プロビジョニングの受信クライアント証明書（Accept Client Certificate for Provisioning）] オプションが有効な場合、およびエンドポイント（AnyConnect）がトンネル内のユーザ証明書を送信するように設定されている場合、トンネルの確立中に、ISE が証明書を使用してユーザを認証し（内部方式はスキップされます）、マシン認証は内部方式によって実行されます。これらのオプションが設定されていない場合、EAP-TLS が内部方式としてユーザ認証に使用されます。 EAP チェーンを有効にした後、許可ポリシーを更新し、NetworkAccess:EapChainingResult 属性を使用して条件を追加し、適切な権限を割り

フィールド名	使用上のガイドライン
	当てます。

フィールド名	使用上のガイドライン
EAP-TTLSを許可（Allow EAP-TTLS）	

フィールド名	使用上のガイドライン

	EAP-TTLS プロトコルを有効にする場合に、このチェックボックスをオンにします。
	
	次の内部方式を設定できます。
	
	• [PAP/ASCIIを許可（Allow PAP/ASCII）]：内部方式として PAP/ASCII を使用する場合は、このチェックボックスをオンにします。EAP-TTLS PAP は、トークンおよび OTP ベースの認証で使用できます。
	
	• [CHAPを許可（Allow CHAP）]：内部方式として CHAP を使用する場合は、このチェックボックスをオンにします。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。
	
	• [MS-CHAPv1を許可（Allow MS-CHAPv1）]：内部方式として MS-CHAPv1 を使用する場合は、このチェックボックスをオンにします。
	
	• [MS-CHAPv2を許可（Allow MS-CHAPv2）]：内部方式として MS-CHAPv2 を使用する場合は、このチェックボックスをオンにします。
	
	• [EAP-MD5を許可（Allow EAP-MD5）]：内部方式として EAP-MD5 を使用する場合は、このチェックボックスをオンにします。
	
	• [EAP-MS-CHAPv2を許可（Allow EAP-MS-CHAPv2）]：内部方式として EAP-MS-CHAPv2 を使用する場合は、このチェックボックスをオンにします。
	
	  • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。
	
	  • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザクレデンシャルを要求する回数を指定

フィールド名	使用上のガイドライン
	します。有効な値は 0 ～ 3 です。
優先 EAP プロトコル（Preferred EAP protocol）	EAP-FAST、PEAP、LEAP、EAP-TLS、EAP-TTLS、およびEAP-MD5 から任意の優先 EAP プロトコルを選択するには、このチェックボックスをオンにします。優先プロトコルを指定しない場合、EAP-TLS がデフォルトで使用されます。
EAP-TLS L ビット（EAP-TLS L-bit）	デフォルトで、ISE からの TLS Change Cipher Spec メッセージと暗号化ハンドシェイクメッセージの長さの含まれるフラグ（L ビットフラグ）を予測するレガシー EAP サプリカントをサポートするには、このチェックボックスをオンにします。
EAP の脆弱な暗号の許可（Allow Weak Ciphers for EAP）	このオプションを有効にすると、レガシー クライアントが脆弱な暗号（RSA_RC4_128_SHA、RSA_RC4_128_MD5 など）を使用してネゴシエートすることができます。レガシー クライアントが脆弱な暗号化だけをサポートしている場合に限り、このオプションを有効にすることを推奨します。 このオプションはデフォルトでは無効になっています。 （注） Cisco ISE は、EDH_RSA_DES_64_CBC_SHA および EDH_DSS_DES_64_CBC_SHA をサポートしていません。

フィールド名	使用上のガイドライン
すべての RADIUS 要求にメッセージオーセンティケータが必要（Require Message Authenticator for all RADIUS Requests）	このオプションを有効にすると、Cisco ISE は、RADIUS メッセージ オーセンティケータ属性が RADIUS メッセージがあるかどうかを検証します。メッセージ オーセンティケータ属性がない場合、RADIUS メッセージは破棄されます。 このオプションを有効にすると、スプーフィングされたアクセス要求メッセージおよび RADIUS メッセージの改ざんに対する保護が提供されます。 RADIUS メッセージ オーセンティケータ属性は、RADIUS メッセージ全体の Message Digest 5（MD5）ハッシュです。 （注） EAP はメッセージ オーセンティケータ属性をデフォルトで使用するので、これを有効にする必要はありません。

関連トピック

TACACS+ デバイス管理を許可された FIPS および非 FIPS モードのプロトコル （355 ページ）
ネットワーク アクセスの許可されるプロトコルの定義 （1088 ページ）

PAC オプション

次の表では、[許可されるプロトコルサービスリスト（Allowed Protocols Services List）] ウィンドウで [PACを使用（Use PAC）] を選択した後のフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authentication）]** > **[許可されるプロトコル（Allowed Protocols）]** です。

表 *140 : PAC* オプション

フィールド名	使用上のガイドライン
PAC を使用（Use PAC）	

フィールド名	使用上のガイドライン
	• [トンネルPACの存続可能時間（Tunnel PAC Time To Live）]：存続可能時間（TTL）の値によって PAC のライフタイムが制限されます。ライフタイム値と単位を指定します。デフォルトは 90 日です。範囲は 1 ～ 1825 日です。 • [プロアクティブPAC更新の条件：<n%>のPAC TTLが残っている場合（Proactive PAC Update When: <n%> of PAC TTL is Left）]：Update 値により、クライアントに有効な PAC が保持されます。Cisco ISE は、最初に認証が成功してから TTL によって設定された有効期限までに更新を開始します。update 値は、TTL の残り時間のパーセンテージです。デフォルトは 90% です。 • [匿名インバンドPACプロビジョニングを許可（Allow Anonymous In-band PAC Provisioning）]：Cisco ISE でクライアントとのセキュアな匿名 TLS ハンドシェイクを確立し、クライアントに PAC をプロビジョニングする場合にこのチェックボックスをオンにします。その際、EAP-FAST のフェーズ 0 と EAP-MSCHAPv2 が使用されます。匿名 PAC プロビジョニングを有効にするには、内部方式として EAP-MSCHAPv2 と EAP-GTC の両方を選択する必要があります。 • [認証付きインバンドPACプロビジョニングを許可（Allow Authenticated In-band PAC Provisioning）]：Cisco ISE は SSL サーバ側の認証を使用して、EAP-FAST のフェーズ 0 中にクライアントに PAC をプロビジョニングします。このオプションは匿名プロビジョニングよりもセキュアですが、サーバ証明書および信頼できるルート CA が Cisco ISE にインストールされている必要があります。 このオプションをオンにすると、認証された PAC プロビジョニングの成功後に Access-Accept メッセージをクライアントに返すように Cisco ISE を設定できます。

フィールド名	使用上のガイドライン
	• [認証されたプロビジョニングの後にサーバからAccess-Acceptを返す（Server Returns Access Accept After Authenticated Provisioning）]：認証された PAC プロビジョニングの後に Cisco ISE から access-accept パッケージを返す場合にこのチェックボックスをオンにします。 • [マシン認証を許可（Allow Machine Authentication）]：Cisco ISE でエンドユーザクライアントにマシン PAC をプロビジョニングし、（マシンクレデンシャルを持たないエンドユーザクライアントに対して）マシン認証を実行する場合にこのチェックボックスをオンにします。マシン PAC は、要求（インバンド）によって、または管理者（アウトオブバンド）によって、クライアントにプロビジョニングできます。Cisco ISE がエンドユーザクライアントから有効なマシン PAC を受信すると、その PAC からマシン ID の詳細が抽出され、Cisco ISE 外部 ID ソースで確認されます。マシン認証の外部 ID ソースとして Cisco ISE によってサポートされるのは、Active Directory だけです。その詳細が正しいことが確認されると、その後の認証は実行されません。 このオプションをオンにすると、マシン PAC を使用するために受け入れることができる期間の値を入力できます。Cisco ISE は、期限切れのマシン PAC を受け取ると、（エンドユーザ クライアントからの新規マシン PAC 要求を待たずに）エンドユーザ クライアントに新規マシン PAC を自動的に再プロビジョニングします。

フィールド名	使用上のガイドライン
	• [ステートレスセッション再開の有効化（Enable Stateless Session Resume）]：Cisco ISE で EAP-FAST クライアントに認可 PAC をプロビジョニングし、EAP-FAST のフェーズ 2 をスキップする場合にこのチェックボックスをオンにします（デフォルトはオン）。 このチェックボックスは次の場合にオフにします。 • Cisco ISE が EAP-FAST クライアントに認可 PAC をプロビジョニングしないようにする場合 • EAP-FAST のフェーズ 2 を常に実行する場合 このオプションをオンにすると、ユーザ認可 PAC の認可期間を入力できます。この期間の終了後、PAC は期限切れになります。Cisco ISE は期限切れの認可 PAC を受信すると、EAP-FAST 認証のフェーズ 2 を実行します。

関連トピック

OOB TrustSec PAC （1115 ページ）
EAP-FAST の PAC の生成 （1048 ページ）

RADIUS プロキシ サーバとして機能する Cisco ISE

Cisco ISE は、RADIUS サーバおよび RADIUS プロキシ サーバとして機能できます。プロキシ サーバとして機能する場合、Cisco ISE はネットワーク アクセス サーバ（NAS）から認証要求およびアカウンティング要求を受信し、これらの要求を外部 RADIUS サーバに転送します。Cisco ISE は要求の結果を受け取り、NAS に返します。

Cisco ISE は、同時に複数の外部 RADIUS サーバへのプロキシ サーバとして動作できます。RADIUS サーバ順序で設定した外部 RADIUS サーバを使用できます。次に説明する [外部 RADIUS サーバ（External RADIUS Server）] ページには、Cisco ISE で定義した外部 RADIUS サーバがすべて表示されます。フィルタ オプションを使用して、名前または説明、またはその両方に基づいて特定の RADIUS サーバを検索することができます。単純な認証ポリシーとルールベースの認証ポリシーの両方で、RADIUS サーバ順序を使用して要求を RADIUS サーバにプロキシできます。

RADIUS サーバ順序は、RADIUS-Username 属性からドメイン名を抜き取り（ストリッピング）、RADIUS 認証に使用します。このドメイン ストリッピングは EAP 認証には使用できません。EAP 認証では EAP-Identity 属性が使用されます。RADIUS プロキシ サーバは RADIUS-Username 属性からユーザ名を取得し、RADIUS サーバ順序の設定時に指定した文字列からユーザ名を抜き取ります。EAP 認証の場合は、RADIUS プロキシ サーバはユーザ名を EAP-Identity 属性から取得します。RADIUS サーバ順序を使用する EAP 認証は、EAP-Identity 値と RADIUS-Username 値が同一である場合のみ成功します。

外部 RADIUS サーバの設定

Cisco ISE で外部 RADIUS サーバを設定して、要求を外部 RADIUS サーバに送信できるようにする必要があります。タイムアウト時間および接続試行回数を定義できます。

始める前に

- この項で作成した外部RADIUSサーバは、それだけでは使用できません。RADIUSサーバ順序を作成して、この項で作成したRADIUSサーバを使用するように設定する必要があります。これにより、RADIUS サーバ順序を認証ポリシーで使用できるようになります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]**>**[ネットワーク リソース（Network Resources）]**>**[外部 RADIUS サーバ（External RADIUS Servers）]** を選択します。

[RADIUS サーバ（RADIUS Servers）] ページが表示され、Cisco ISE で定義された外部 RADIUS サーバのリストが示されます。

ステップ 2 外部 RADIUS サーバを追加するには、[追加（Add）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信（Submit）] をクリックして、外部 RADIUS サーバの設定を保存します。

RADIUS サーバ順序の定義

Cisco ISE の RADIUS サーバ順序を使用すると、NAD からの要求を外部 RADIUS サーバにプロキシできます。外部 RADIUS サーバは要求を処理して結果を Cisco ISE に返し、Cisco ISE はその応答を NAD に転送します。

[RADIUS サーバ順序（RADIUS Server Sequences）] ページに、Cisco ISE で定義したすべての RADIUS サーバの順序が表示されます。このページを使用して、RADIUS サーバの作成、編集、または複製が可能です。

始める前に

- この手順を開始する前に、プロキシサービスの基本を理解し、関連リンクの最初のエントリのタスクを正常に完了している必要があります。

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[RADIUS サーバ順序（RADIUS Server Sequences）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信（Submit）] をクリックして、ポリシーに使用する RADIUS サーバ順序を保存します。

TACACS+ プロキシ クライアントとして機能する Cisco ISE

Cisco ISE は、外部 TACACS+ サーバへのプロキシ クライアントとして機能できます。プロキシ クライアントとして機能する場合、Cisco ISE はネットワーク アクセス サーバ（NAS）から認証要求、許可要求およびアカウンティング要求を受信し、これらの要求を外部 TACACS+ サーバに転送します。Cisco ISE は要求の結果を受け取り、NAS に返します。

[TACACS+外部サーバ（TACACS+ External Servers）] ページには、Cisco ISE で定義した外部 TACACS+ サーバがすべて表示されます。フィルタ オプションを使用して、名前または説明、またはその両方に基づいて特定の TACACS+ サーバを検索することができます。

Cisco ISE は、同時に複数の外部 TACACS+ サーバへのプロキシ クライアントとして動作できます。複数の外部サーバを設定するには、[TACACS+サーバの順序（TACACS+ server sequence）] ページを使用できます。詳細については、「TACACS+ サーバ順序の設定」ページを参照してください。

外部 TACACS+ サーバの設定

Cisco ISE で外部 TACACS サーバを設定して、要求を外部 TACACS サーバに送信できるようにする必要があります。タイムアウト時間および接続試行回数を定義できます。

始める前に

- この項で作成した外部 TACACS サーバは、ポリシーに直接使用できません。TACACS サーバ順序を作成して、この項で作成した TACACS サーバを使用するように設定する必要があります。これにより、TACACS サーバ順序をポリシー セットで使用できるようになります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[TACACS外部サーバ（TACACS External Servers）]** の順に選択します。

[TACACS外部サーバ（TACACS External Servers）] ページが表示され、Cisco ISE で定義された外部 TACACS サーバのリストが示されます。

ステップ 2 外部 TACACS サーバを追加するには、[追加（Add）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信（Submit）] をクリックして、外部 TACACS サーバの設定を保存します。

TACACS+ 外部サーバの設定

次の表では、[TACACS外部サーバ（TACACS External Servers）] ページのフィールドについて説明します。ナビゲーション パスは、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[TACACS外部サーバ（TACACS External Servers）]** ページです。

表 *141 : TACACS+* 外部サーバの設定

フィールド	使用上のガイドライン
名前（Name）	TACACS+ 外部サーバの名前を入力します。
説明	TACACS+ 外部サーバ設定の説明を入力します。
ホスト名/アドレス（Host IP）	リモート TACACS+ 外部サーバの IP アドレス（IPv4 または IPv6 アドレス）を入力します。
接続ポート（Connection Port）	リモート TACACS+ 外部サーバのポート番号を入力します。ポート番号は 49 です。
Timeout	ISE が外部 TACACS+ サーバからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は 1 ～ 120 です。
共有秘密鍵（Shared Secret）	TACACS+ 外部サーバとの接続を保護するのに使用するテキスト文字列。正しく設定されていない場合、接続は TACACS+ 外部サーバによって拒否されます。

フィールド	使用上のガイドライン
シングル接続を使用（Use Single Connect）	TACACS プロトコルは、接続にセッションを関連付けるための 2 つのモード、シングル接続と非シングル接続をサポートしています。シングル接続モードは、クライアントが開始する可能性がある多数の TACACS+ セッションに対し、単一の TCP 接続を再使用します。非シングル接続では、クライアントが開始するすべての TACACS+ セッションに対し、新しい TCP 接続が開かれます。TCP 接続は、各セッションの後に閉じられます。 トラフィックが多い環境では、[シングル接続を使用（Use Single Connect）] チェックボックスをオンにし、トラフィックが少ない環境ではオフにできます。

TACACS+ サーバ順序の定義

Cisco ISE の TACACS+ サーバ順序を使用すると、NAD からの要求を外部 TACACS+ サーバにプロキシできます。外部 TACACS+ サーバは要求を処理して結果を Cisco ISE に返し、Cisco ISE はその応答を NAD に転送します。[TACACS+サーバ順序（TACACS+ Server Sequences）] ページに、Cisco ISE で定義したすべての TACACS+ サーバの順序が表示されます。このページを使用して、TACACS+ サーバ順序の作成、編集、または複製が可能です。

始める前に

- プロキシ サービス、Cisco ISE 管理者グループ、アクセス レベル、権限、および制限の基本を理解している必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- TACACS+ サーバ順序で使用する外部 TACACS+ サーバがすでに定義されていることを確認します。

ステップ 1 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [TACACS外部サーバ順序（TACACS External Server Sequence）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 必要な値を入力します。

ステップ 4 [送信（Submit）] をクリックして、ポリシーに使用する TACACS+ サーバ順序を保存します。

TACACS+ サーバ順序の設定

次の表では、[TACACSサーバ順序（TACACS Server Sequence）] ページのフィールドについて説明します。ナビゲーション パスは、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワークリソース（Network Resources）]** > **[TACACSサーバ順序（TACACS Server Sequence）]** ページです。

表 *142 : TACACS+* サーバ順序の設定

フィールド	使用上のガイドライン
名前（Name）	TACACS プロキシ サーバ順序の名前を入力します。
説明	TACACS プロキシ サーバ順序の説明を入力します。
サーバ リスト（Server List）	[使用可能（Available）] リストから必要な TACACS プロキシ サーバを選択します。[使用可能（Available）] リストには、[TACACS外部サービス（TACACS External Services）] ページで設定されている TACACS プロキシ サーバのリストが含まれています。
ロギング制御（Logging Control）	ロギング制御を有効にするにはオンにします。 • ローカル アカウンティング：アカウンティング メッセージは、デバイスからの要求を処理するサーバによってログに記録されます。 • リモート アカウンティング：アカウンティング メッセージは、デバイスからの要求を処理するプロキシ サーバによってログに記録されます。

フィールド	使用上のガイドライン
ユーザ名の除去（Username Stripping）	ユーザ名のプレフィックス/サフィックスの除去 • [プレフィックスの除去（Prefix Strip）]：プレフィックスからユーザ名を取り除く場合にオンにします。たとえば、サブジェクト名がacme\smith、区切り文字が\の場合、ユーザ名はsmithになります。デフォルトの区切り文字は\です。 • [サフィックスの除去（Suffix Strip）]：サフィックスからユーザ名を取り除く場合にオンにします。たとえば、サブジェクト名がsmith@acme.com、区切り文字が@の場合、ユーザ名はsmithになります。デフォルトの区切り文字は@です。

ネットワーク アクセス サービス

ネットワーク アクセス サービスには、要求に対する認証ポリシー条件が含まれています。たとえば有線802.1Xや有線MABなど、さまざまな用途向けに個別のネットワーク アクセス サービスを作成することができます。ネットワーク アクセス サービスを作成するには、許可されているプロトコルまたはサーバ順序を設定します。その後、ネットワーク アクセス ポリシーのネットワーク アクセス サービスが [ポリシー セット（Policy Sets）] ページから構成されます。

ネットワーク アクセスの許可されるプロトコルの定義

許可されるプロトコルは、ネットワーク リソースへのアクセスを要求するデバイスとの通信にCisco ISE が使用できるプロトコルのセットを定義します。許可されるプロトコル アクセス サービスは、認証ポリシーを設定する前に作成する必要がある独立したエントリです。許可されるプロトコル アクセス サービスは、特定の使用例に対して選択されたプロトコルが含まれているオブジェクトです。

[許可されるプロトコル サービス（Allowed Protocols Services）] ページには、作成した許可されるプロトコル サービスがすべて表示されます。Cisco ISE で事前に定義されたデフォルトのネットワーク アクセス サービスが存在します。

始める前に

この手順を開始する前に、認証に使用するプロトコル サービスの基本を理解している必要があります。

- この章の「Cisco ISE認証ポリシー」の項を参照して、さまざまなデータベースでサポートされる認証タイプおよびプロトコルについて理解します。

- 「PAC オプション」を確認して、各プロトコル サービスの機能とオプションを理解し、使用しているネットワークに最適な選択ができるようにしてください。
- 手順を進める前に、グローバル プロトコル設定を必ず定義してください。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）]** を選択します。

Cisco ISE が FIPS モードで動作するように設定されている場合は、一部のプロトコルがデフォルトで無効になり、それらのプロトコルを設定できません。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 必要な情報を入力します。

ステップ 4 ネットワークに適切な認証プロトコルとオプションを選択します。

ステップ 5 PAC の使用を選択した場合、適切な選択を行います。

匿名 PAC プロビジョニングを有効にするには、内部方式として EAP-MSCHAPv2 と Extensible Authentication Protocol-Generic Token Card（EAP-GTC）の両方を選択する必要があります。また Cisco ISE では、マシン認証の外部 ID ソースとしては Active Directory だけがサポートされる点に注意してください。

ステップ 6 [送信（Submit）] をクリックして、許可されるプロトコル サービスを保存します。

許可されるプロトコル サービスは、単純な認証ポリシーおよびルールベースの認証ポリシーのページで独立したオブジェクトとして表示されます。このオブジェクトは異なるルールに使用できます。

これで、単純な認証ポリシーおよびルールベースの認証ポリシーを作成できるようになります。

内部方式として EAP-MSCHAP を無効にし、PEAP または EAP-FAST の EAP-GTC と EAP-TLS 内部方式を有効にすると、ISE は内部方式のネゴシエーション中に EAP-GTC 内部方式を開始します。最初の EAP-GTC メッセージがクライアントに送信される前に、ISE は ID 選択のポリシーを実行して、ID ストアから GTC パスワードを取得します。このポリシーの実行中、EAP 認証は EAP-GTC と同じです。EAP-GTC 内部方式がクライアントによって拒否され、EAP-TLS がネゴシエートされても、ID ストア ポリシーが再び実行されることはありません。ID ストア ポリシーが EAP 認証属性に基づいている場合、本当の EAP 認証は EAP-TLS でありながら ID ポリシー評価後に設定されたため、予期しない結果になることがあります。

ユーザのネットワーク アクセス

ネットワーク アクセスでは、ホストはネットワーク デバイスに接続し、ネットワーク リソースの使用を要求します。ネットワーク デバイスは、新しく接続されたホストを識別し、転送方式として RADIUS プロトコルを使用して、ユーザの認証および許可を Cisco ISE に要求します。

Cisco ISE では、RADIUS プロトコルを使用して転送されるプロトコルに応じて、ネットワーク アクセス フローがサポートされます。

EAP を使用しない RADIUS ベースのプロトコル

EAP を含まない RADIUS ベースのプロトコルは、次のとおりです。

- Password Authentication Protocol（PAP）
- CHAP
- Microsoft Challenge Handshake Authentication Protocol version 1（MS-CHAPv1）
- MS-CHAP バージョン 2（MS-CHAPv2）

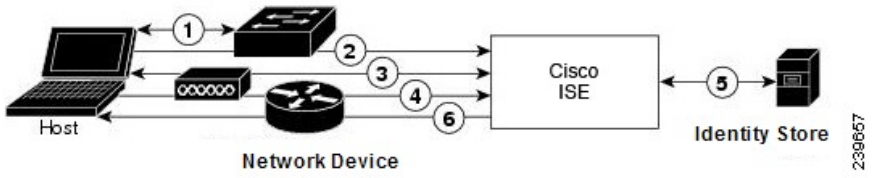
RADIUS-Based Non-EAP 認証フロー

ここでは、EAP 認証を使用しない RADIUS ベースのフローについて説明します。PAP 認証を使用する RADIUS ベースのフローは、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが RADIUS 要求（Access-Request）を Cisco ISE に送信します。この要求には、使用する特定のプロトコル（PAP、CHAP、MS-CHAPv1、または MS-CHAPv2）に適した RADIUS 属性が含まれます。
3. Cisco ISE では、ID ストアを使用してユーザ クレデンシャルを検証します。
4. RADIUS 応答（Access-Accept または Access-Reject）が、決定を適用するネットワーク デバイスに送信されます。

次の図は、EAP を使用しない RADIUS ベースの認証を示しています。

図 *59 : EAP* を使用しない *RADIUS* ベースの認証



Cisco ISE でサポートされる非 EAP プロトコルは次のとおりです。

パスワード認証プロトコル

PAP では、ユーザが双方向ハンドシェイクを使用して ID を確立できる単純な方法が提供されます。PAP パスワードは共有秘密を使用して暗号化されるため、最もセキュリティ レベルの低い認証プロトコルです。PAP は、反復的な試行錯誤攻撃に対する保護がほとんどないため、確実な認証方式ではありません。

Cisco ISE の *RADIUS-Based PAP* 認証

Cisco ISE では、ID ストアに対してユーザ名とパスワードのペアをチェックし、最終的にその認証を確認するか、接続を終了します。

Cisco ISE では、異なるセキュリティ レベルを同時に使用して、さまざまな要件に対応できます。PAP は双方向ハンドシェイク手順を適用します。認証に成功した場合、Cisco ISE は確認応答を返します。認証に失敗した場合、Cisco ISE は接続を終了するか、認証の要求元にもう一度チャンスを与えます。

認証の要求元が、試行の頻度とタイミングを総合的に制御します。したがって、より強力な認証方式を使用できるサーバは、PAP よりも前にその方式のネゴシエーションを提案します。PAP は RFC 1334 で定義されています。

Cisco ISE では、RADIUS UserPassword 属性に基づく標準の RADIUS PAP 認証がサポートされます。RADIUS PAP 認証は、すべての ID ストアと互換性があります。

PAP 認証フローを使用する RADIUS には、試行の成功と失敗のロギングが含まれます。

チャレンジ ハンドシェイク認証プロトコル

CHAP は、応答時に一方向の暗号化を使用するチャレンジ/レスポンス方式です。CHAP を使用することで、Cisco ISE は、セキュリティ レベルの高い順からセキュリティ暗号化方式をネゴシエートし、プロセス中に伝送されるパスワードを保護します。CHAP パスワードは再利用が可能です。Cisco ISE 内部データベースを認証に使用する場合は、PAP または CHAP のどちらかを使用できます。CHAP は、Microsoft ユーザ データベースでは使用できません。RADIUS PAP と比較した場合、エンドユーザ クライアントから AAA クライアントに通信するときに CHAP を使用すると、パスワードが暗号化されるため、高いセキュリティ レベルを確保できます。

Cisco ISE では、RADIUS ChapPassword 属性に基づく標準の RADIUS CHAP 認証がサポートされます。Cisco ISE では、外部 ID ストアを使用した RADIUS CHAP 認証だけがサポートされます。

Microsoft Challenge Handshake Authentication Protocol Version 1

Cisco ISE では、RADIUS MS-CHAPv1 認証およびパスワード変更機能がサポートされます。RADIUS MS-CHAPv1 には、Change-Password-V1 と Change-Password-V2 の 2 つのバージョンのパスワード変更機能が含まれます。Cisco ISE は RADIUS MS-CHAP-CPW-1 属性に基づいた Change-Password-V1 パスワード変更をサポートせず、MS-CHAP-CPW-2 属性に基づいた Change-Password-V2 のみをサポートします。RADIUS MS-CHAPv1 認証およびパスワード変更機能は、次の ID ソースを使用してサポートされます。

- 内部 ID ストア
- Microsoft Active Directory ID ストア

Microsoft Challenge Handshake Authentication Protocol Version 2

RADIUS MS-CHAPv2 認証およびパスワード変更機能は、次の ID ソースでサポートされます。

- 内部 ID ストア
- Microsoft Active Directory ID ストア

RADIUS ベースの EAP プロトコル

EAP では、さまざまな認証タイプをサポートする拡張可能なフレームワークが提供されます。ここでは、Cisco ISE でサポートされる EAP 方式について説明します。次のトピックを扱います。

単純な EAP 方式

- EAP-Message Digest 5
- Lightweight EAP

認証に Cisco ISE サーバ証明書を使用する EAP 方式

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

上記にリストした方式とは別に、サーバ認証とクライアント認証の両方に証明書を使用する EAP 方式があります。

RADIUS-Based EAP 認証フロー

認証プロセスで EAP が使用される場合は常に、そのプロセスよりも、具体的にどの EAP 方式（および該当する場合は内部方式）を使用する必要があるかを決定するネゴシエーションフェーズが先行します。EAP ベースの認証は、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが EAP 要求をホストに送信します。
3. ホストは、EAP 応答によって、ネットワーク デバイスに応答します。
4. ネットワーク デバイスは、ホストから受信した EAP 応答を RADIUS Access-Request 内に（EAP-Message RADIUS 属性を使用して）カプセル化し、RADIUS Access-Request を Cisco ISE に送信します。
5. Cisco ISE は、RADIUS パケットから EAP 応答を抽出して新しい EAP 要求を作成し、この EAP 要求を RADIUS Access-Challenge 内に（この場合も EAP-Message RADIUS 属性を使用して）カプセル化し、ネットワーク デバイスに送信します。
6. ネットワーク デバイスは、EAP 要求を抽出し、ホストへ送信します。

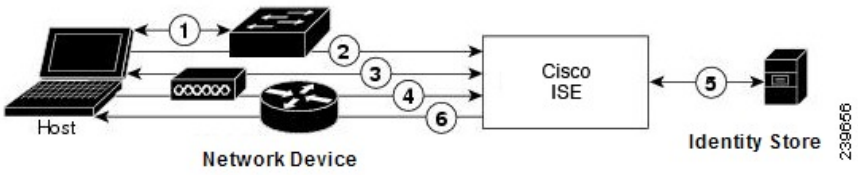
この方法で、ホストと Cisco ISE は間接的に EAP メッセージを交換します（EAP メッセージは、RADIUS を使用して転送され、ネットワーク デバイスを介して渡されます）。この方法で交換される EAP メッセージの最初のセットによって、特定の EAP 方式がネゴシエートされます。その後、認証を実行する場合に、この EAP 方式が使用されます。

その後交換される EAP メッセージは、実際の認証の実行に必要なデータを伝送するために使用されます。ネゴシエートされた特定の EAP 認証方式で必要な場合、Cisco ISE では ID ストアを使用してユーザ クレデンシャルを検証します。

Cisco ISE では、認証が成功か失敗かを決定した後、EAP-Success または EAP-Failure メッセージを、RADIUS Access-Accept または Access-Reject メッセージ内にカプセル化された状態で、ネットワーク デバイスに（最終的にはホストにも）送信します。

次の図は、EAP を使用する RADIUS ベースの認証を示しています。

図 *60 : EAP* を使用する *RADIUS* ベースの認証



Extensible Authentication Protocol-Message Digest 5

Extensible Authentication Protocol-Message Digest 5（EAP-MD5）では、一方向のクライアント認証が提供されます。サーバは、クライアントにランダムチャレンジを送信します。クライアントは、チャレンジとそのパスワードを MD5 で暗号化することによって、応答でその ID を証明します。中間者がチャレンジと応答を見ることができるため、EAP-MD5 は、公開メディアで使用される場合にはディクショナリ攻撃に対して脆弱です。サーバ認証が行われないため、スプーフィングに対しても脆弱です。Cisco ISE では、Cisco ISE 内部 ID ストアに対する EAP-MD5 認証がサポートされます。EAP-MD5 プロトコルを使用している場合は、ホスト ルックアップもサポートされます。

Lightweight Extensible Authentication Protocol

Cisco ISE では現在、Lightweight Extensible Authentication Protocol（LEAP）を Cisco Aironet ワイヤレス ネットワーキングに対してだけ使用します。このオプションを有効にしないと、LEAP 認証を実行するように設定された Cisco Aironet エンドユーザ クライアントは、ネットワークにアクセスできなくなります。Cisco Aironet エンドユーザ クライアントすべてが Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）などの異なる認証プロトコルを使用する場合は、このオプションを無効にすることを推奨します。

（注） [ネットワーク デバイス（Network Devices）] セクションで RADIUS（Cisco Aironet）デバイスとして定義された AAA クライアントを使用してユーザがネットワークにアクセスする場合は、LEAP、EAP-TLS、またはその両方を有効にする必要があります。これ以外の場合、Cisco Aironet ユーザは認証を受けることができません。

保護拡張認証プロトコル

保護拡張認証プロトコル（PEAP）では、相互認証が提供され、脆弱なユーザ クレデンシャルの機密性と整合性が保証されます。またこのプロトコルでは、自身をパッシブ（盗聴）および

アクティブ（中間者）攻撃から保護し、セキュアに暗号キー関連情報を生成します。PEAPは、IEEE 802.1X 標準および RADIUS プロトコルと互換性があります。Cisco ISE では、Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol（EAP-MS-CHAP）、Extensible Authentication Protocol-Generic Token Card（EAP-GTC）、および EAP-TLS 内部方式で PEAP バージョン 0（PEAPv0）と PEAP バージョン 1（PEAPv1）がサポートされます。Cisco Secure Services Client（SSC）サプリカントでは、Cisco ISE でサポートされるすべての PEAPv1 内部方式がサポートされます。

PEAP の使用の利点

PEAP を使用すると、次のような利点があります。PEAP は、広く実装されセキュリティが細部にわたって確認された TLS に基づいています。キーを生成しない方式に対しては、キーを確立します。トンネル内でIDを送信します。内部方式の交換と結果メッセージを保護します。フラグメンテーションがサポートされます。

PEAP プロトコルでサポートされているサプリカント

PEAP では、次のサプリカントがサポートされます。

- Microsoft Built-In Clients 802.1X XP
- Microsoft Built-In Clients 802.1X Vista
- Cisco Secure Services Client（SSC）Release 4.0
- Cisco SSC リリース 5.1
- Funk Odyssey Access Client リリース 4.72
- Intel リリース 12.4.0.0

PEAP プロトコルのフロー

PEAP カンバセーションは、次の 3 つの部分に分かれます。

1. Cisco ISE とピアが TLS トンネルを構築します。Cisco ISE は自身の証明書を提示しますが、ピアは提示しません。ピアと Cisco ISE はキーを作成して、トンネル内のデータを暗号化します。
2. 内部方式によって、次のようにトンネル内のフローが決定されます。
   - EAP-MS-CHAPv2 内部方式：EAP-MS-CHAPv2 パケットは、ヘッダーなしでトンネル内を移動します。ヘッダーの先頭のバイトにタイプ フィールドが含まれます。EAP-MS-CHAPv2 内部方式では、パスワード変更機能がサポートされます。ユーザが管理者ポータルでパスワードの変更を試行できる回数を設定できます。ユーザ認証の試行回数はこの数値によって制限されます。
   - EAP-GTC 内部方式：PEAPv0 と PEAPv1 の両方で、EAP-GTC 内部方式がサポートされます。サポートされるサプリカントでは、EAP-GTC内部方式を使用するPEAPv0はサポートされません。EAP-GTCでは、パスワード変更機能がサポートされます。ユーザが管理者ポータルでパスワードの変更を試行できる回数を設定できます。ユーザ認証の試行回数はこの数値によって制限されます。

- EAP-TLS内部方式：Windows組み込みサプリカントでは、トンネルが確立された後のメッセージのフラグメンテーションはサポートされず、このことはEAP-TLS内部方式に影響を与えます。Cisco ISEでは、トンネルが確立された後の外部PEAPメッセージのフラグメンテーションはサポートされません。トンネルの確立中、フラグメンテーションはPEAPのマニュアルで指定されているとおりに動作します。PEAPv0ではEAP-TLSパケットのヘッダーが削除され、PEAPv1ではEAP-TLSパケットがそのまま送信されます。
- Extensible Authentication Protocol-type, length, value（EAP-TLV）拡張：EAP-TLVパケットはそのまま送信されます。EAP-TLVパケットは、トンネル内をヘッダー付きで移動します。

3. カンバセーションが内部方式に到達した場合、保護された成功と失敗の確認応答があります。

   クライアントEAPメッセージは常にRADIUS Access-Requestメッセージで送信され、サーバEAPメッセージは常にRADIUS Access-Challengeメッセージで送信されます。EAP-Successメッセージは、常にRADIUS Access-Acceptメッセージで送信されます。EAP-Failureメッセージは、常にRADIUS Access-Rejectメッセージで送信されます。クライアントPEAPメッセージをドロップすると、RADIUSクライアントメッセージがドロップされます。

（注） Cisco ISEは、PEAPv1通信中にEAP-SuccessまたはEAP-Failureメッセージの確認を要求します。ピアは、成功または失敗メッセージの受信を確認するために空のTLSデータ フィールドを含むPEAPパケットを返送する必要があります。

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）は、相互認証を提供する認証プロトコルであり、共有秘密を使用してトンネルを確立します。このトンネルは、パスワードに基づく弱い認証方式を保護するために使用されます。Protected Access Credentials（PAC）キーと呼ばれる共有秘密は、トンネルのセキュリティを確保するときにクライアントとサーバを相互認証するために使用されます。

*EAP-FAST*の利点

EAP-FASTは、他の認証プロトコルに比べて次の利点があります。

- 相互認証：EAPサーバはピアのIDと信頼性を確認できる必要があり、ピアはEAPサーバの信頼性を確認できる必要があります。
- パッシブ ディクショナリ攻撃に対する耐性：多くの認証プロトコルでは、ピアからEAPサーバにパスワードがクリアテキストまたはハッシュとして明示的に提供される必要があります。
- 中間者攻撃に対する耐性：相互認証された保護トンネルの確立時に、プロトコルは、ピアとEAPサーバとの間のカンバセーションに攻撃者が情報を挿入することを防ぐ必要があります。

- MS-CHAPv2や汎用トークンカード（GTC）などの多くの異なるパスワード認証インターフェイスをサポートできる柔軟性：EAP-FASTは、同じサーバで複数の内部プロトコルをサポートできる拡張可能なフレームワークです。
- 効率性：無線メディアを使用する場合、ピアは計算資源と電源リソースを制限されます。EAP-FAST では、ネットワーク アクセス通信の計算を軽量化できます。
- 認証サーバのユーザごとの認証状態要件の最小化：大規模な展開では、通常、多くのサーバが多くのピアに対する認証サーバとして機能する必要があります。ユーザ名とパスワードを使用してネットワークにアクセスするのと同じように、ピアが同じ共有秘密を使用してトンネルのセキュリティを確保することも強く推奨されます。EAP-FASTにより、サーバでキャッシュおよび管理する必要があるユーザごとおよびデバイスごとの状態を最小にすることができ、ピアによる強力な単一共有秘密の使用が容易になります。

EAP-FAST フロー

EAP-FAST プロトコルのフローは常に、次のフェーズを組み合わせたものになります。

1. プロビジョニング フェーズ：これはEAP-FAST のフェーズ 0 です。このフェーズでは、Cisco ISE とピアとの間で共有される、PAC と呼ばれる一意の強力な秘密を使用して、ピアがプロビジョニングされます。
2. トンネル確立フェーズ：PACを使用して新しいトンネルキーを確立することによって、クライアントとサーバを相互認証します。トンネルキーはその後、残りのカンバセーションを保護するために使用され、メッセージの機密性と信頼性を提供します。
3. 認証フェーズ：認証がトンネル内で処理され、セッションキーの生成と保護された終了が行われます。Cisco ISE では、EAP-FAST バージョン 1 および 1a がサポートされます。

シスコ以外のデバイスからの MAB の有効化

次の設定を順番に設定して、シスコ以外のデバイスから MAB を設定します。

ステップ 1 認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。プロファイラ サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。

ステップ 2 シスコ以外のデバイス（PAP、CHAP、EAP-MD5）で使用される MAC 認証のタイプに基づいて、ネットワーク デバイス プロファイルを作成します。

a) [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス プロファイル（Network Device Profiles）] の順に選択します。
b) [追加（Add）] をクリックします。
c) ネットワーク デバイス プロファイルの名前と説明を入力します。
d) [ベンダー（Vendor）] ドロップダウン リストからベンダー名を選択します。
e) デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスがRADIUSをサポートする場合は、ネットワーク デバイスで使用する RADIUS ディクショナリを選択します。
f) [認証/許可（Authentication/Authorization）]セクションを展開し、フロータイプ、属性エイリアシング、およびホスト ルックアップに関するデバイスのデフォルト設定を行います。

g) [ホスト ルックアップ（MAB）（Host Lookup (MAB)）] セクションで、次を実行します。

- [ホスト ルックアップの処理（Process Host Lookup）]：ネットワーク デバイス プロファイルで使用されるホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。

  さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。デバイス タイプに応じて、使用しているプロトコルの [パスワードを確認（Check Password）] チェック ボックスまたは [Calling-Station-Id が MAC アドレスと等しいかを確認（Checking Calling-Station-Id equals MAC Address）] チェック ボックス、またはその両方をオンにします。

- [PAP/ASCII 経由（Via PAP/ASCII）]：ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。

- [CHAP 経由（Via CHAP）]：ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。

- [EAP-MD5 経由（Via EAP-MD5）]：ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。

h) [アクセス許可（Permissions）]、[認可変更（CoA）（Change of Authorization (CoA)）]、[リダイレクト（Redirect）] のセクションで必要な詳細を入力して、[送信（Submit）] をクリックします。

カスタム NAD プロファイルを作成する方法については、『Network Access Device Profiles with Cisco Identity Services Engine』を参照してください。

ステップ 3 [管理（Administration）]>[ネットワーク リソース（Network Resources）]>[ネットワーク デバイス（Network Devices）] の順に選択します。

ステップ 4 MAB を有効にするデバイスを選択して、[編集（Edit）] をクリックします。

ステップ 5 [ネットワーク デバイス（Network Device）] ページの [デバイス プロファイル（Device Profile）] ドロップダウン リストから、手順 2 で作成したネットワーク デバイス プロファイルを選択します。

ステップ 6 [保存（Save）] をクリックします。

（注） Cisco NAD では、MAB および Web/ユーザ認証に使用する Service-Type 値は異なります。これにより、Cisco NAD を使用する場合に、ISE は MAB と Web 認証を区別できます。シスコ以外の一部の NAD では、MAB と Web/ユーザ認証に同じ値の Service-Type 属性を使用しています。この場合、アクセス ポリシーでセキュリティ上の問題につながる場合があります。シスコ以外のデバイスで MAB を使用する場合は、ネットワーク セキュリティが侵害されないように、追加の許可ポリシー ルールを設定することを推奨します。たとえば、プリンタで MAB を使用する場合は、ACL のプリンタ プロトコル ポートに制限する許可ポリシー ルールを設定できます。

シスコ デバイスからの MAB の有効化

次の設定を順番に設定して、シスコ デバイスから MAB を設定します。

ステップ 1 認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。プロファイラ サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。

ステップ 2 シスコ デバイス（PAP、CHAP、EAP-MD5）で使用される MAC 認証のタイプに基づいて、ネットワーク デバイス プロファイルを作成します。

a) [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス プロファイル（Network Device Profiles）] の順に選択します。

b) [追加（Add）] をクリックします。

c) ネットワーク デバイス プロファイルの名前と説明を入力します。

d) デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスが RADIUS をサポートする場合は、ネットワーク デバイスで使用する RADIUS ディクショナリを選択します。

e) [認証/許可（Authentication/Authorization）] セクションを展開し、フロー タイプ、属性エイリアシング、およびホスト ルックアップに関するデバイスのデフォルト設定を行います。

f) [ホスト ルックアップ（MAB）（Host Lookup (MAB)）] セクションで、次を実行します。

- [ホスト ルックアップの処理（Process Host Lookup）]：ネットワーク デバイス プロファイルで使用されるホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。

  デバイス タイプに応じて、使用しているプロトコルの [パスワードを確認（Check Password）] チェックボックスまたは [Calling-Station-Id が MAC アドレスと等しいかを確認（Checking Calling-Station-Id equals MAC Address）] チェックボックス、またはその両方をオンにします。

- [PAP/ASCII 経由（Via PAP/ASCII）]：ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。

- [CHAP 経由（Via CHAP）]：ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。

- [EAP-MD5 経由（Via EAP-MD5）]：ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。

g) [アクセス許可（Permissions）]、[認可変更（CoA）（Change of Authorization (CoA)）]、[リダイレクト（Redirect）] のセクションで必要な詳細を入力して、[送信（Submit）] をクリックします。

カスタム NAD プロファイルを作成する方法については、『Network Access Device Profiles with Cisco Identity Services Engine』を参照してください。

ステップ 3 [管理（Administration）]>[ネットワーク リソース（Network Resources）]>[ネットワーク デバイス（Network Devices）] の順に選択します。

ステップ 4 MAB を有効にするデバイスを選択して、[編集（Edit）] をクリックします。

ステップ 5 [ネットワーク デバイス（Network Device）] ページの [デバイス プロファイル（Device Profile）] ドロップダウン リストから、手順 2 で作成したネットワーク デバイス プロファイルを選択します。

ステップ 6 [保存（Save）] をクリックします。

ISE コミュニティ リソース

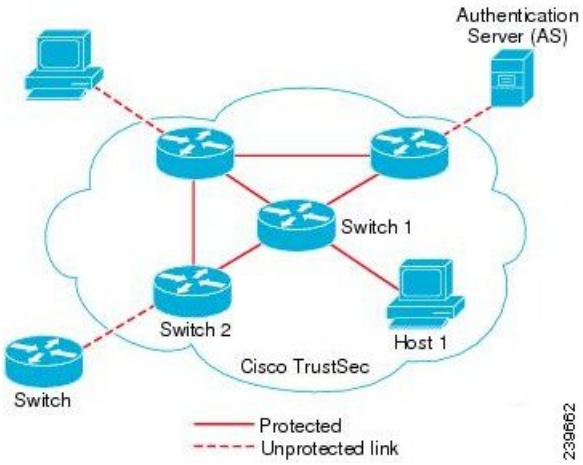
IP フォンの認証機能については、「Phone Authentication Capabilities」を参照してください。

TrustSec アーキテクチャ

Cisco TrustSec ソリューションでは、信頼ネットワーク デバイスのクラウドを確立して、セキュアなネットワークを構築します。Cisco TrustSec クラウド内の個々のデバイスは、そのネイバー（ピア）によって認証されます。TrustSec クラウド内のデバイス間の通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。TrustSec ソリューションでは、認証中に取得したデバイスおよびユーザ ID 情報を使用して、ネットワークに入ってきたパケットを分類（色付け）します。このパケット分類は、パケットが TrustSec ネットワークに入ってきたときに、そのパケットにタグ付けすることによって維持されます。これにより、パケットはデータ パス全体で正しく識別され、セキュリティおよびその他のポリシー基準が適用されるようになります。このタグは、セキュリティ グループ タグ（SGT）と呼ばれることもあります。エンドポイント デバイスで SGT に応じてトラフィックをフィルタリングできるようにすることにより、Cisco ISE でアクセス コントロール ポリシーを適用できるようになります。

次の図に、TrustSec ネットワーク クラウドの例を示します。

図 *61 : TrustSec* アーキテクチャ



ISE コミュニティ リソース

Cisco TrustSec を使用してネットワーク セグメンテーションを簡素化、セキュリティを強化する方法については、「Simplify Network Segmentation with Cisco TrustSec」と「Policy-Based Software Defined Segmentation and Cisco TrustSec Improve Security White Paper」を参照してください。

Cisco TrustSec プラットフォーム サポート マトリックスのリストについては、「Cisco TrustSec Platform Support Matrix」を参照してください。

利用可能な TrustSec のサポート ドキュメントのリストについては、「Cisco TrustSec」を参照してください。

TrustSec コミュニティ リソースのリストについては、TrustSec Communityを参照してください。

TrustSec のコンポーネント

主な TrustSec のコンポーネント：

- ネットワーク デバイス アドミッション コントロール（NDAC）：信頼ネットワークでは、認証中に、TrustSec クラウド内にある各ネットワーク デバイス（イーサネット スイッチなど）のクレデンシャルおよび信頼性が、そのピア デバイスによって検証されます。NDAC は IEEE 802.1X ポートベース認証を使用し、その拡張認証プロトコル（EAP）方式として Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）を使用します。NDAC プロセスの認証および許可が成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションが実行されます。
- エンドポイント アドミッション コントロール（EAC）：TrustSec クラウドに接続しているエンドポイント ユーザまたはデバイスの認証プロセス。EAC は一般的にアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可が成功すると、ユーザまたはデバイスに対する SGT 割り当てが実行されます。認証および許可の EAC アクセス方法には次のものがあります。
  - 802.1X ポートベースの認証
  - MAC 認証バイパス（MAB）
  - Web 認証（WebAuth）
- セキュリティ グループ（SG）：アクセス コントロール ポリシーを共有するユーザ、エンドポイント デバイス、およびリソースのグループ。SG は、管理者が Cisco ISE で定義します。新規ユーザおよびデバイスが TrustSec ドメインに追加されると、Cisco ISE では、これらの新規エントリを適切なセキュリティ グループに割り当てます。
- セキュリティ グループ タグ（SGT）：TrustSec サービスは各セキュリティ グループに、その範囲が TrustSec ドメイン内でグローバルな一意のセキュリティ グループ番号（16 ビット）を割り当てます。スイッチ内のセキュリティ グループの数は、認証されたネットワーク エンティティの数に制限されます。セキュリティ グループ番号を手動で設定する必要

はありません。これらは自動的に生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。

- セキュリティ グループ アクセス コントロール リスト（SGACL）：SGACL では、割り当てられている SGT に基づいてアクセスおよび権限を制御できます。権限をロールにまとめることにより、セキュリティポリシーの管理が容易になります。デバイスを追加するときに、1 つ以上のセキュリティ グループを割り当てるだけで、即座に適切な権限が付与されます。セキュリティ グループを変更することにより、新しい権限を追加したり、現在の権限を制限することもできます。
- セキュリティ交換プロトコル（SXP）：SGT 交換プロトコル（SXP）は、TrustSec サービス用に開発されたプロトコルで、SGT 対応ハードウェアをサポートしていないネットワーク デバイス間で、SGT/SGACL をサポートしているハードウェアに IP-SGT バインディングを伝播します。
- 環境データのダウンロード：TrustSec デバイスは、初めて信頼ネットワークに参加するときに、その環境データを Cisco ISE から取得します。デバイス上の一部のデータは、手動で設定することもできます。デバイスでは、期限切れになる前に環境データを更新する必要があります。TrustSec デバイスは、次の環境データを Cisco ISE から取得します。
  - サーバ リスト：クライアントがその後の RADIUS 要求に使用できるサーバのリスト（認証および許可の両方）
  - デバイス SG：そのデバイス自体が属しているセキュリティ グループ
  - 有効期間：TrustSec デバイスが環境データをダウンロードまたはリフレッシュする頻度を制御する期間
- ID とポートとのマッピング：エンドポイントの接続先のポートでスイッチが ID を定義するための方法で、この ID を使用して Cisco ISE サーバ内の特定の SGT 値が検索されます。

TrustSec の用語

次の表は、TrustSec ソリューションで使用される一般的な用語の一部と、TrustSec 環境でのその意味を示しています。

表 *143 : TrustSec* の用語

用語	意味
サプリカント	信頼ネットワークへの参加を試行するデバイス。
認証	信頼ネットワークへの参加を許可する前に、各デバイスの ID を検証するプロセス。

用語	意味
許可	信頼ネットワーク上のリソースへのアクセスを要求しているデバイスに対し、デバイスの認証IDに基づいてアクセスのレベルを決定するプロセス。
アクセス コントロール	各パケットに割り当てられている SGT に基づいて、パケットごとにアクセス コントロールを適用するプロセス。
セキュアな通信	信頼ネットワーク内の各リンクを経由して流れるパケットをセキュリティで保護するための、暗号化、整合性、データパス リプレイ保護のプロセス。
TrustSec デバイス	TrustSec ソリューションをサポートする Cisco Catalyst 6000 シリーズまたは Cisco Nexus 7000 シリーズのスイッチ。
TrustSec 対応デバイス	TrustSec 対応デバイスは、TrustSec 対応のハードウェアとソフトウェアを備えています。たとえば、Nexus オペレーティング システムを搭載した Nexus 7000 シリーズ スイッチなどです。
TrustSec シード デバイス	Cisco ISE サーバに対して直接認証を行う TrustSec デバイス。オーセンティケータとサプリカントの両方として機能します。
受信側	Cisco TrustSec ソリューションが有効になっているネットワーク内の TrustSec 対応デバイスにパケットが初めて到達すると、SGT を使用してパケットにタグが付けられます。この信頼ネットワークへの入り口点を入力と呼びます。
送信側	Cisco TrustSec ソリューションが有効になっているネットワーク内の最後の TrustSec 対応デバイスをパケットが通過すると、タグが解除されます。この信頼ネットワークからの出口点を出力と呼びます。

TrustSec のサポートされるスイッチと必要なコンポーネント

Cisco TrustSec ソリューションが有効になった Cisco ISE ネットワークを設定するには、TrustSec ソリューションおよび他のコンポーネントをサポートするスイッチが必要です。スイッチ以外に、IEEE 802.1X プロトコルを使用した ID ベースのユーザ アクセス コントロールには、その他のコンポーネントも必要です。TrustSec をサポートするシスコ スイッチのプラットフォームおよび必要なコンポーネントの完全な最新のリストについては、「Cisco TrustSec-Enabled Infrastructure」を参照してください。

Cisco DNA Center との統合

Cisco ISE は、Cisco のデジタル ネットワーク アーキテクチャ（DNA）の主要なコンポーネントです。Cisco DNA Center では、ビジネスの俊敏性を提供しているネットワークを自動化することができます。Cisco ISE が提供します。Cisco ISE と Cisco DNA Center を統合すると、Cisco ISE は Cisco DNA Center にエンドポイント認証を行います。

Cisco ISE への Cisco DNA Center の接続

DNAC ユーザ ガイドの Cisco DNA Center と ISE の設定に関する要件および手順を参照してください（https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html）。

このセクションでは、Cisco DNA Center 向けの Cisco ISE 設定に関する追加情報について説明します。

- パスワード：Cisco DNA Center は CLI コマンドの実行のために Cisco ISE に接続する場合、Cisco ISE CLI のパスワードを使用します。CLI と管理者のユーザ名とパスワードは同じである必要があります。システム パスワードの詳細については、Cisco ISE への管理アクセス （18 ページ）を参照してください。
- API：Cisco DNA Center は ISE API を呼び出すことによって一部の ISE を設定します。API アクセスは Cisco ISE で有効にし、CSRF では有効にしないでください。詳細については、外部 RESTful サービス API の有効化 （131 ページ）を参照してください。
- pxGrid：Cisco ISE は pxGrid コントローラで、Cisco DNA Center はサブスクライバです。Cisco ISE と Cisco DNA Center の両方で、SGT と SGACL 情報が含まれる Trustsec（SD-Access）コンテンツをモニタします。Cisco ISE と Cisco DNA Center 間でシステム クロックを同期する必要があります。Cisco ISE は証明書を使用して pxGrid に接続します。これは、接続のために Cisco DNA Center によって設定されます。Cisco ISE の pxGrid の詳細については、『』の「pxGrid ノード」のセクションpxGrid ノード （77 ページ）を参照してください。
- Cisco ISE IP アドレス：ISE PAN と Cisco DNA Center 間は直接接続する必要があります。プロキシ、ロード バランサ、または仮想 IP アドレスを使用することはできません。Cisco ISE と Cisco DNA Center の両方で、それぞれのスタティック アドレスを設定します。

Cisco ISE がプロキシを使用していないことを確認します。使用している場合は、プロキシから Cisco DNA Center IP を除外します。

- SXP：Cisco DNA Center との通信に SXP は必要ありません。Cisco ISE と Cisco DNA 管理対象ネットワークを接続する場合に SXP を有効にすると、Cisco ISE は Trustsec（SD-Access）のハードウェアをサポートしないネットワーク デバイスと通信できます。
- Cisco ISE との接続用の証明書：
  - Cisco ISE 管理証明書では、件名または SAN に Cisco ISE IP または FQDN を含める必要があります。
  - ECDSA キーは、SSH キー、ISE SSH アクセス、または Cisco DNA Center と Cisco ISE の接続用の証明書ではサポートされません。
  - Cisco DNA Center の自己署名証明書では、cA:TRUE (RFC5280 section-4.2.19) の基本制約の拡張を使用する必要があります。

TrustSec ダッシュボード

TrustSec ダッシュボードは、TrustSec ネットワークの一元化されたモニタリング ツールです。

TrustSec ダッシュボードには次のダッシュレットが含まれています。

- メトリック：[メトリック（Metrics）] ダッシュレットには、TrustSec ネットワークの動作に関する統計情報が表示されます。
- アクティブな SGT セッション：[アクティブなSGTセッション（Active SGT Sessions）] ダッシュレットには、ネットワークで現在アクティブな SGT セッションが表示されます。[アラーム（Alarms）] ダッシュレットには、TrustSec セッション関連のアラームが表示されます。
- アラーム
- NAD/SGT クイック ビュー：[クイックビュー（Quick View）] ダッシュレットには、NAD および SGT の TrustSec 関連情報が表示されます。
- TrustSec セッション/NAD アクティビティ ライブ ログ：アクティブな TrustSec セッションを表示するには、[ライブログ（Live Log）] ダッシュレットの [TrustSecセッション（TrustSec Sessions）] リンクをクリックします。また、NAD から Cisco ISE への TrustSec プロトコル データ要求と応答に関する情報を表示することもできます。

メトリック

このセクションには、TrustSec ネットワークの動作に関する統計情報が表示されます。タイムフレーム（たとえば、過去 2 時間、過去 2 日 など）とチャート タイプ（たとえば、棒、折れ線、スプラインなど）を選択できます。

最新のバー値がグラフに表示されます。また、前のバーからのパーセンテージの変化も表示されます。バー値に増加がある場合、プラス記号付きの緑色で表示されます。値に減少がある場合、マイナス記号付きの赤色で表示されます。

値が計算された時刻とその正確な値を <Value:xxxx Date/Time: xxx> 形式で表示するには、グラフのバーにカーソルを置きます。

次のメトリックを表示できます。

SGTセッション（SGT sessions）	選択された時間内に作成された SGT セッションの総数が表示されます。 （注） SGT セッションは、認証フローの一部として SGT を受信したユーザ セッションです。
使用中のSGT（SGTs in use）	選択された時間内に使用された固有の SGT の総数が表示されます。たとえば、1 時間で 200 の TrustSec セッションがあったが、ISE が認証応答で 6 つのタイプの SGT でしか応答しなかった場合、グラフにはこの時間に値 6 が表示されます。
アラーム	選択された時間内に発生したアラームおよびエラーの総数が表示されます。エラーは赤色で表示され、アラームは黄色で表示されます。
使用中のNAD（NADs in use）	選択された時間内に TrustSec 認証に参加した固有の NAD の数が表示されます。

現在のネットワーク ステータス

このダッシュボードの中間部分には、TrustSec ネットワークの現在のステータスに関する情報が表示されます。グラフに表示される値は、ページがロードされると更新され、[ダッシュボードの更新（Refresh Dashboard）] オプションを使用して更新できます。

アクティブな SGT セッション

このダッシュレットには、ネットワークで現在アクティブな SGT セッションが表示されます。上位 10 個の最もよく使用されている SGT または最も使用頻度の低い SGT を表示できます。X 軸には SGT 使用率が表示され、Y 軸には SGT の名前が表示されます。

SGT の TrustSec セッションの詳細を表示するには、その SGT に対応するバーをクリックします。その SGT に関連する TrustSec セッションの詳細が [ライブログ（Live Log）] ダッシュレットに表示されます。

アラーム

このダッシュレットには、TrustSec セッション関連のアラームが表示されます。次の詳細情報を表示できます。

- [アラームの重大度（Alarm Severity）]：アラームの重大度レベルを示すアイコンが表示されます。
  - [高（High）]：TrustSec ネットワーク内の障害を示すアラームが含まれます（たとえば、PAC の更新が失敗したデバイスなど）。赤色のアイコンが付いています。
  - [中（Medium）]：ネットワーク デバイスの誤った設定を示す警告が含まれます（たとえば、CoA メッセージの受け入れを失敗したデバイスなど）。黄色でマークされます。
  - [低（Low）]：ネットワーク動作の一般情報および更新が含まれます（たとえば、TrustSec の設定変更など）。青色でマークされます。
- アラームの説明
- このアラーム カウンタが最後にリセットされてからアラームが発生した回数。
- アラームが最後に発生した時刻

クイック ビュー

[クイックビュー（Quick View）] ダッシュレットには、NAD の TrustSec 関連情報が表示されます。SGT の TrustSec 関連情報を表示することもできます。

NAD クイック ビュー

[検索（Search）] ボックスに詳細を表示する TrustSec ネットワーク デバイスの名前を入力し、**Enter** を押します。検索ボックスには自動入力機能があり、ユーザがテキスト ボックスに入力すると、ドロップ ダウンに一致するデバイス名がフィルタされ表示されます。

次の詳細情報が表示されます。

- [NDG（NDGs）]：このネットワーク デバイスが属するネットワーク デバイス グループ（NDG）がリストされます。
- [IPアドレス（IP Address）]：ネットワーク デバイスの IP アドレス。[ライブログ（Live Logs）] ダッシュレットに NAD アクティビティの詳細を表示するには、このリンクをクリックします。
- [アクティブセッション（Active sessions）]：このデバイスに接続されているアクティブな TrustSec セッションの数。
- [PACの有効期限（PAC expiry）]：PAC の失効日。
- [最後のポリシー更新（Last Policy Refresh）]：ポリシーを最後にダウンロードした日付。
- [最後の認証（Last Authentication）]：このデバイスの最後の認証レポートのタイムスタンプ。
- [アクティブSGT（Active SGTs）]：このネットワークデバイスに関連するアクティブセッションで使用されている SGT がリストされます。カッコ内に表示される数字は、現在こ

の SGT を使用しているセッションの数を示します。[ライブ ログ（Live Log）] ダッシュレットに TrustSec セッションの詳細を表示するには、SGT のリンクをクリックします。

[最新ログの表示（Show Latest Logs）] オプションを使用して、デバイスの NAD アクティビティのライブ ログを表示できます。

SGT クイック ビュー

[検索（Search）] ボックスに詳細を表示する SGT の名前を入力し、**Enter** を押します。

次の情報がこのダッシュレットに表示されます。

- [値（Value）]：SGT 値（10 進数と 16 進数の両方）。
- [アイコン（Icon）]：この SGT に割り当てられているアイコンが表示されます。
- [アクティブセッション（Active sessions）]：現在この SGT を使用しているアクティブなセッションの数。
- [固有ユーザ（Unique users）]：この SGT をアクティブ セッションに保持する固有ユーザ名の数。
- [更新されたNAD（Updated NADs）]：この SGT のポリシーをダウンロードした NAD の数。

ライブ ログ

アクティブな TrustSec セッション（応答の一部として SGT があるセッション）を表示するには [TrustSecセッション（TrustSec Sessions）] リンクをクリックします。

NAD から Cisco ISE への TrustSec プロトコル データ要求と応答に関する情報を表示するには、[NADアクティビティ（NAD Activity）] リンクをクリックします。

TrustSec のグローバル設定

Cisco ISE が TrustSec サーバとして機能して TrustSec サービスを提供するには、いくつかのグローバル TrustSec 設定を定義する必要があります。

始める前に

- TrustSec グローバル設定を設定する前に、グローバル EAP-FAST 設定が定義されていることを確認します（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-FAST]** > **[EAP-FAST 設定（EAP-FAST Settings）]** を選択）。

  [機関識別情報の説明（Authority Identity Info Description）] を Cisco ISE サーバ名に変更することができます。この説明は、クレデンシャルをエンドポイント クライアントに送信する Cisco ISE サーバを説明したわかりやすい文字列にします。Cisco TrustSec アーキテク

チャのクライアントには、IEEE 802.1X 認証の EAP 方式として EAP-FAST を実行するエンドポイント、または Network Device Access Control（NDAC）を実行するサプリカント ネットワーク デバイスのいずれも使用できます。クライアントは、この文字列を Protected Access Credentials（PAC）Type-Length-Value（TLV）情報で認識できます。デフォルト値は、Identity Services Engine です。NDAC 認証時に、ネットワーク デバイスで Cisco ISE PAC 情報が一意に識別されるように、この値を変更する必要があります。

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）] の順に選択します。

ステップ 2 フィールドに値を入力します。フィールドの詳細については、次を参照してください。 一般 TrustSec の設定 （1108 ページ）

ステップ 3 [保存（**Save**）] をクリックします。

次のタスク

- TrustSec デバイスの設定 （1114 ページ）

一般 TrustSec の設定

Cisco ISE が TrustSec サーバとして機能したり、TrustSec サービスを提供したりするには、グローバル TrustSec 設定を定義します。次の表に、[TrustSec 設定（TrustSec Settings）] ウィンドウのフィールドの説明を示します（（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）]）。

TrustSec 展開の確認

このオプションを選択すると、すべてのネットワークデバイスに最新の TrustSec ポリシーが展開されているかどうかを確認できます。Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合は [アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] および [ホーム（Home）] > [サマリ（Summary）]）にアラームが表示されます。TrustSec ダッシュ ボードに、以下のアラームが表示されます。

- 検証プロセスが開始または完了するたびに、[情報（Info）] アイコンとともにアラームが表示されます。
- 新しい展開要求により検証プロセスがキャンセルされた場合は、[情報（Info）] アイコンとともにアラームが表示されます。
- 検証プロセスがエラーで失敗した場合は、[警告（Warning）] アイコンとともにアラームが表示されます。たとえば、ネットワーク デバイスとの SSH 接続を開けない場合やネッ

トワーク デバイスが使用できない場合、あるいは Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合などです。

[展開の検証（Verify Deployment）] オプションは、次のウィンドウでも使用できます。

- **[ワーク センター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティ グループ（Security Groups）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ ACL（Security Group ACLs）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [送信元ツリー（Source Tree）]**
- **[ワーク センター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [宛先ツリー（Destination Tree）]**

[すべての展開後に自動検証（Automatic Verification After Every Deploy）]：それぞれの展開後に、Cisco ISE ですべてのネットワーク デバイス上の更新を検証するには、このチェックボックスをオンにします。展開プロセスが完了したら、[展開プロセス後の時間（Time after Deploy Process）] フィールドに指定した時間が経過した後に、検証プロセスが開始されます。

[展開プロセス後の時間（Time after Deploy Process）]：展開プロセスが完了した後、検証プロセスを開始する前に Cisco ISE に待機させる時間を指定します。有効な範囲は、10 ～ 60 分です。

待機期間中に新しい展開が要求された場合や別の検証が進行中の場合は、現在の検証プロセスはキャンセルされます。

[今すぐ検証（Verify Now）]：検証プロセスをすぐに開始するには、このオプションをクリックします。

Protected Access Credential（PAC）

- [トンネル PAC の存続可能時間（Tunnel PAC Time to Live）]：

  PAC の有効期限を指定します。トンネル PAC は EAP-FAST プロトコル用のトンネルを生成します。時間を秒、分、時、日数、または週数で指定できます。デフォルト値は 90 日です。有効な範囲は次のとおりです。

  - 1 ～ 157680000 秒
  - 1 ～ 2628000 分
  - 1 ～ 43800 時間
  - 1 ～ 1825 日
  - 1 ～ 260 週間

- [プロアクティブ PAC 更新を次の後に実行する（Proactive PAC Update Will Occur After）]：Cisco ISE は、認証に成功した後、設定したパーセンテージのトンネル PAC TTL が残っているときに、新しい PAC をクライアントに予防的に提供します。PAC の期限が切れる前に最初の認証が正常に行われると、サーバはトンネル PAC の更新を開始します。このメカニズムにより、有効な PAC でクライアントが更新されます。デフォルト値は 10% です。

セキュリティグループタグ番号の割り当て

- [システムで SGT 番号を割り当てる（System will Assign SGT Numbers）]：Cisco ISE に SGT 番号を自動生成させる場合は、このオプションを選択します。
- [範囲内の番号を除外する（Except Numbers In range）]：手動設定用に SGT 番号の範囲を予約する場合は、このオプションを選択します。Cisco ISE は、SGT の生成時にこの範囲の数値を使用しません。
- [ユーザが手動で SGT 番号を入力する（User Must Enter SGT Numbers Manually）]：SGT 番号を手動で定義する場合は、このオプションを選択します。

APIC EPGのセキュリティグループタグのナンバリング（Security Group Tag Numbering for APIC EPGs）

[APIC EPG 用のセキュリティグループタグの番号付け（Security Group Tag Numbering for APIC EPGs）]：APIC から学習した EPG に基づいて SGT を作成する場合は、このチェックボックスをオンにし、使用する番号の範囲を指定します。

セキュリティグループの自動作成

[認証ルールを作成するときにセキュリティグループを自動作成する（Auto Create Security Groups When Creating Authorization Rules）]：認可ポリシーのルールを作成する際に SGT を自動的に作成する場合は、このチェックボックスをオンにします。

このオプションを選択した場合は、[認可ポリシー（Authorization Policy）] ウィンドウの上部に、「 自動セキュリティグループの作成がオンです（Auto Security Group Creation is On）」というメッセージが表示されます。

自動作成された SGT は、ルール属性に基づいて命名されます。

（注） 自動作成された SGT は、それに対応する認可ポリシールールを削除しても削除されません。

デフォルトでは、新規インストールまたはアップグレードの後でこのオプションが無効になります。

- [自動命名オプション（Automatic Naming Options）]：自動作成される SGT の命名規則を定義するには、このオプションを使用します。

（必須）[名前に次が含まれます（Name Will Include）]：次のオプションのいずれかを選択します。

- **ルール名**
- **SGT番号（SGT number）**
- **ルール名およびSGT番号（Rule name and SGT number）**

デフォルトでは、[ルール名（Rule name）] オプションが選択されます。

オプションで、SGT 名に以下の情報を追加できます。

- ポリシーセット名（Policy Set Name）（このオプションは [ポリシーセット（Policy Sets）] が有効な場合にのみ使用可能です）
- プレフィックス（Prefix）（8 文字まで）
- サフィックス（Suffix）（8 文字まで）

Cisco ISE は、選択内容に応じて [サンプル名（Example Name）] フィールドにサンプル SGT 名を表示します。

同じ名前の SGT が存在している場合、ISE は SGT 名に「*_x*」を付け加えます。*x* は（現在の名前に 1 が使用されていない場合は）1 から始まる最初の値です。新しい名前が 32 文字より長い場合、Cisco ISE によって最初の 32 文字に切り捨てられます。

ホスト名の IP SGT 静的マッピング

[ホスト名の IP SGT 静的マッピング（IP SGT Static Mapping of Hostnames）]：FQDN とホスト名が使用される場合、Cisco ISE はマッピングを展開して展開状態を検査する際に、PAN および PSN ノード内の対応する IP アドレスを検索します。DNS クエリによって返される IP アドレス用に作成されるマッピングの数を指定する場合は、このオプションを使用します。次のいずれかのオプションを選択できます。

- **DNS クエリによって返されるすべての IP アドレスに対してマッピングを作成する（Create mappings for all IP addresses returned by a DNS query）**
- **DNSクエリによって返される最初のIPv4アドレスおよび最初のIPv6アドレスに対してのみマッピングを作成する（Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query）**

関連トピック

TrustSec アーキテクチャ （1099 ページ）
TrustSec のコンポーネント （1100 ページ）
TrustSec のグローバル設定 （1107 ページ）

TrustSec マトリックスの設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSecマトリックスの設定（TrustSec Matrix Settings）] の順に選択します。

ステップ 2 [TrustSecマトリックスの設定（TrustSec Matrix Settings）] ページに必要な詳細を入力します。

ステップ 3 [保存（**Save**）] をクリックします。

TrustSec マトリックスの設定

次の表に、[TrustSecマトリックスの設定（TrustSec Matrix Settings）] ページにある各フィールドの説明を示します。このページへのナビゲーションパスは、[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSecマトリックスの設定（TrustSec Matrix Settings）] です。

表 *144 : TrustSec* マトリックスの設定

フィールド	使用上のガイドライン
複数のSGACLを許可（Allow Multiple SGACLs）	セル内で複数のSGACLを許可するには、このチェックボックスをオンにします。このオプションが選択されていない場合、Cisco ISE はセル 1 つあたり 1 つの SGACL のみを許可します。 デフォルトでは、新たにインストールすると、このオプションはディセーブルになります。 アップグレード後、Cisco ISE は出力セルをスキャンし、複数の SGACL が割り当てられたセルを少なくとも 1 つ特定した場合、管理者に複数の SGACL をセルに追加することを許可します。それ以外の場合は、セル 1 つあたり 1 つの SGACL のみを許可します。 （注） 複数の SGACL を無効にする前に、複数の SGACL を含むセルを 1 つの SGACL のみを含めるように編集する必要があります。

フィールド	使用上のガイドライン
モニタリングの許可（Allow Monitoring）	マトリクス内のすべてのセルのモニタリングをイネーブルにする場合は、このチェックボックスをオンにします。モニタリングがディセーブルの場合、[セルの編集（Edit Cell）] ダイアログで、[すべてをモニタ（Monitor All）] アイコンはグレー表示され、[モニタ（Monitor）] オプションはディセーブルになります。 デフォルトでは、新たにインストールすると、モニタリングはディセーブルになります。 （注） マトリクス レベルでモニタリングをディセーブルにする前に、現在モニタされているセルのモニタリングをディセーブルにする必要があります。
SGT番号の表示（Show SGT Numbers）	マトリクス セルの SGT 値（10 進数および 16 進数の両方）を表示または非表示にするには、このオプションを使用します。 デフォルトでは、SGT 値はセルに表示されます。
アピアランス設定（Appearance Settings）	次のオプションを使用できます。 • [カスタム設定（Custom settings）] : デフォルトのテーマ（パターンなしの色）が最初に表示されます。独自の色とパターンを設定できます。 • [デフォルト設定（Default settings）] : パターンなしの色の定義済みリスト（編集不可）。 • [アクセシビリティ設定（Accessibility settings）] : パターンありの色の定義済みリスト（編集不可）。

フィールド	使用上のガイドライン
色/パターン（Color/Pattern）	マトリックスを読み取りやすくするために、セルの内容に基づいて、マトリックスセルに色とパターンを適用できます。 使用可能な表示タイプは、次のとおりです。 • [IPを許可/IPログを許可（Permit IP/Permit IP Log）]：セル内に設定されます • [IPを拒否/IPログを拒否（Deny IP/Deny IP Log）]：セル内に設定されます • [SGACL（SGACLs）]：セル内に設定されている SGACL 用 • [IPを許可/IPログを許可（継承）（Permit IP/Permit IP Log (Inherited)）]：デフォルト ポリシーから取得されます（設定されていないセル用） • [IPを拒否/IPログを拒否（継承）（Deny IP/Deny IP Log (Inherited)）]：デフォルト ポリシーから取得されます（設定されていないセル用） • [SGACL（継承）（SGACLs (Inherited)）]：デフォルトポリシーから取得されます（設定されていないセル用）

関連トピック

出力ポリシー （1125 ページ）
マトリクス ビュー （1126 ページ）
TrustSec マトリックスの設定 （1112 ページ）

TrustSec デバイスの設定

Cisco ISE で TrustSec 対応デバイスからの要求を処理するには、これらの TrustSec 対応デバイスを Cisco ISE で定義しておく必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ネットワーク デバイス（Network Devices）] セクションで、必要な情報を入力します。

ステップ 4 TrustSec 対応デバイスを設定するために [高度な TrustSec 設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 5 [送信（Submit）] をクリックします。

OOB TrustSec PAC

すべての TrustSec ネットワーク デバイスで、EAP-FAST プロトコルの一部として TrustSec PAC が保持されています。これはセキュアな RADIUS プロトコルでも使用され、ここでは RADIUS 共有秘密が PAC で伝送されるパラメータから作成されます。これらのパラメータの 1 つである発信側 ID には、TrustSec ネットワーク デバイス ID、つまりデバイス ID が保持されます。

デバイスが TrustSec PAC を使用して識別される場合、Cisco ISE でそのデバイス用に設定されているデバイス ID と、PAC の発信側 ID が一致していない場合、認証に失敗します。

一部の TrustSec デバイス（Cisco ASA ファイアウォールなど）では EAP-FAST プロトコルをサポートしていません。したがって、Cisco ISE ではこれらのデバイスを EAP-FAST を介した TrustSec PAC でプロビジョニングできません。代わりに、TrustSec PAC は Cisco ISE 上で生成され、手動でデバイスにコピーされます。そのため、これをアウトオブバンド（OOB）TrustSec PAC 生成と呼びます。

Cisco ISE で PAC を生成すると、暗号キーで暗号化された PAC ファイルが生成されます。

ここでは、次の内容について説明します。

[設定（Settings）] 画面からの TrustSec PAC の生成

[設定（Settings）] 画面から TrustSec PAC を生成できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）]** を選択します。

ステップ 2 左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。

ステップ 3 **[EAP-FAST]** > **[PAC の生成（Generate PAC）]** を選択します。

ステップ 4 TrustSec PAC を生成します。

[ネットワーク デバイス（Network Devices）] 画面からの TrustSec PAC の生成

[ネットワーク デバイス（Network Devices）] 画面から TrustSec PAC を生成できます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。[ネットワーク デバイス（Network Devices）] ナビゲーション ペインのアクション アイコンから [新規デバイスの追加（Add new device）] をクリックすることもできます。

ステップ 3 新規デバイスを追加する場合は、デバイス名を入力します。

ステップ 4 TrustSec デバイスを設定するために [高度な TrustSec 設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 5 [アウトオブバンド（OOB）TrustSec PAC（Out of Band (OOB) TrustSec PAC）] サブ セクションで、[PAC の生成（Generate PAC）] をクリックします。

ステップ 6 次の詳細事項を入力します。

- [PAC 存続可能時間（PAC Time to Live）]：日、週、月、および年の単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。
- [暗号化キー（Encryption Key）]：暗号キーを入力します。キーの長さは 8 ～ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。

  暗号キーを使用して、生成されるファイルの PAC が暗号化されます。このキーは、デバイスで PAC ファイルを復号化する場合にも使用されます。したがって、後で使用できるように管理者が暗号キーを保存しておくことを推奨します。

  [ID（Identity）] フィールドは TrustSec ネットワーク デバイスのデバイス ID を示し、このフィールドには EAP-FAST プロトコルによって発信側 ID が提供されます。ここに入力した ID 文字列がネットワーク デバイスの作成ページの [TrustSec] セクションで定義されたデバイス ID と一致しない場合、認証は失敗します。

  有効期限は、PAC 存続可能時間に基づいて計算されます。

ステップ 7 [PAC の生成（Generate PAC）] をクリックします。

[ネットワーク デバイス リスト（Network Devices List）] 画面からの TrustSec PAC の生成

[ネットワーク デバイス リスト（Network Devices list）] 画面から TrustSec PAC を生成できます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] をクリックします。

ステップ 3 TrustSec PAC を生成するデバイスの隣にあるチェックボックスをオンにし、[PAC の生成（Generate PAC）] をクリックします。

ステップ 4 フィールドで詳細を提供します。

ステップ 5 [PAC の生成（Generate PAC）] をクリックします。

[プッシュ（Push）] ボタン

出力ポリシーの [プッシュ（Push）] オプションは CoA 通知を開始します。この通知は、Cisco ISE からの出力ポリシー設定変更に関する更新を、ただちに要求するよう TrustSec デバイスに伝えます。

TrustSec AAA サーバの設定

AAA サーバ リスト内に、Trustsec が有効になっている Cisco ISE サーバのリストを設定することができます。TrustSec デバイスは、これらのサーバのいずれかに対し認証を行います。[プッシュ（Push）] をクリックすると、このリスト内の新しいサーバが TrustSec デバイスにダウンロードされます。TrustSec デバイスは、認証を試行するときに、このリストから Cisco ISE サーバを選択します。最初のサーバがダウン状態またはビジー状態の場合、TrustSec デバイスはこのリストにある別の任意のサーバに対して自分自身の認証を行うことができます。デフォルトでは、プライマリ Cisco ISE サーバは、TrustSec AAA サーバです。より信頼性の高い Trustsec 環境には、より多くの Cisco ISE サーバを設定することをお勧めします。

このページには、TrustSec AAA サーバとして設定した展開内の Cisco ISE サーバがリストされます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [TrustSec AAAサーバ（TrustSec AAA Servers）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 説明に従って値を入力します。

- [名前（Name）]：この AAA サーバ リスト内で Cisco ISE サーバに割り当てる名前。この名前は、Cisco ISE サーバのホスト名と異なっていてもかまいません。
- [説明（Description）]：説明（任意）。
- [IP]：AAA サーバ リストに追加する Cisco ISE サーバの IP アドレス。
- [ポート（Port）]：TrustSec デバイスとサーバ間の通信が行われるポート。デフォルトは 1812 です。

ステップ 4 [プッシュ（Push）] をクリックします。

次のタスク

セキュリティ グループを設定します。

セキュリティ グループの設定

セキュリティ グループ（SG）またはセキュリティ グループ タグ（SGT）は、TrustSec ポリシー設定で使用される要素です。SGT は、パケットが信頼ネットワーク内を移動する場合に付加されます。これらのパケットは、信頼ネットワークに入ったとき（入力）にタグ付けされ、信頼ネットワークから離れるとき（出力）にタグ解除されます。

SGT は順次的な方法で生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。Cisco ISE は、SGT の生成時に予約済みの番号をスキップします。

TrustSec サービスはこれらの SGT を使用して、出力時に TrustSec ポリシーを適用します。

管理者ポータルで次のページからセキュリティ グループを設定できます。

- [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）]。
- **[設定（Configure）] > [新規セキュリティ グループの作成（Create New Security Group）]** の出力ポリシーページから直接。

[プッシュ（Push）] ボタンをクリックすると、複数の SGT を更新した後に、環境 CoA 通知を開始できます。この環境 CoA 通知はすべての TrustSec ネットワーク デバイスに送信され、ポリシー/データ リフレッシュ要求を開始することを強制します。

セキュリティ グループの追加

TrustSec ソリューション内の個々のセキュリティ グループに一意の SGT を割り当てる必要があります。Cisco ISE では 65,535 SGT までサポートされていますが、SGT の数を少なくすると、TrustSec ソリューションをより簡単に展開および管理できるようになります。最大で 4,000 SGT までにすることを推奨します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）] を選択します。

ステップ 2 [追加（Add）] をクリックして新規セキュリティ グループを追加します。

ステップ 3 新規セキュリティ グループの名前と説明（オプション）を入力します。

ステップ 4 この SGT を ACI に反映するには、[ACI に伝播（Propagate to ACI）] チェック ボックスをオンにします。この SGT に関連する SXP マッピングは、ACI が [ACI の設定（ACI Settings）] ページで選択した VPN に属するときのみ ACI に反映されます。

このオプションはデフォルトでは無効になっています。

ステップ 5 タグ値を入力します。タグ値は、手動で入力したり、自動生成されるようにしたり設定できます。また SGT の範囲を予約できます。これは、から設定できます。[一般TrustSecの設定（General TrustSec Settings）] ページ（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）]）。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

セキュリティ グループ アクセス コントロール リストの設定

Cisco ISE へのセキュリティ グループのインポート

カンマ区切り形式（CSV）ファイルを使用して Cisco ISE ノードにセキュリティ グループをインポートできます。Cisco ISE にセキュリティ グループをインポートする前に、テンプレートを更新する必要があります。同じリソース タイプのインポートを同時に実行できません。たとえば、2 つの異なるインポート ファイルから同時にセキュリティ グループをインポートできません。

管理者ポータルからCSVテンプレートをダウンロードし、テンプレートにセキュリティ グループの詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

セキュリティ グループのインポート中、Cisco ISE で最初のエラーが発生した場合、インポート プロセスを停止できます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）] を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 5 [インポート（Import）] をクリックします。

Cisco ISE からのセキュリティ グループのエクスポート

Cisco ISE で設定されたセキュリティ グループを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのセキュリティ グループをインポートできます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）] を選択します。

ステップ 2 [エクスポート（Export）] をクリックします。

ステップ 3 セキュリティ グループをエクスポートするには、次のいずれかを実行できます。

- エクスポートするグループの隣にあるチェックボックスをオンにし、**[エクスポート（Export）]** > **[選択済みをエクスポート（Export Selected）]** を選択します。
- **[エクスポート（Export）]** > **[すべてエクスポート（Export All）]** を選択して、定義されたすべてのセキュリティ グループをエクスポートします。

ステップ 4 ローカル ハード ディスクに export.csv ファイルを保存します。

IP SGT スタティック マッピングの追加

IP-SGT スタティック マッピングを使用して、TrustSec デバイスと SXP ドメインに統一された方法でマッピングを展開することができます。新しい IP-SGT スタティック マッピングを作成するときに、このマッピングを展開する SXP ドメインとデバイスを指定できます。また、IP-SGT マッピングをマッピング グループに関連付けることもできます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティック マッピング（IP SGT Static Mapping）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ホスト名または IP アドレスを入力します。

ステップ 4 既存のマッピング グループを使用する場合は、[マッピング グループに追加（Add to a Mapping Group）] をクリックして、[マッピング グループ（Mapping Group）] ドロップダウン リストから必要なグループを選択します。

この IP アドレス/ホスト名を SGT に個別にマッピングする場合は、[SGT に個別にマッピング（Map to SGT Individually）] をクリックして以下を実行します。

- [SGT] ドロップダウン リストから SGT を選択します。
- マッピングを展開する必要がある SXP VPN グループを選択します。
- このマッピングを展開するデバイスを指定します。すべての TrustSec デバイス、選択されたネットワーク デバイス グループ、または選択されたネットワーク デバイスにマッピングを展開できます。

ステップ 5 **[保存（Save）]** をクリックします。

IP SGT スタティック マッピングの展開

マッピングを追加した後、[展開（Deploy）] オプションを使用して、対象のネットワーク デバイスでこのマッピングを展開します。マッピングをすでに保存している場合でも、これを明示

的に行う必要があります。デバイスの展開ステータスを確認するには、[ステータスを確認（Check Status）] をクリックします。

ステップ 1 [ワークセンター（Work Centers）] タブから、[TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）] を選択します。

ステップ 2 展開するマッピングの近くにあるチェックボックスをオンにします。すべてのマッピングを展開する場合は、一番上のチェックボックスをオンにします。

ステップ 3 [展開（Deploy）] をクリックします。

すべての TrustSec デバイスが [IP SGTスタティックマッピングの展開（Deploy IP SGT Static Mapping）] ウィンドウにリストされます。

ステップ 4 選択したマッピングの展開先となる適切なデバイスまたはデバイス グループの横にあるチェックボックスをオンにします。

- すべてのデバイスを選択する場合は、一番上のチェックボックスをオンにします。
- フィルタリング オプションを使用して、特定のデバイスを検索します。
- デバイスを何も選択しない場合は、選択したマッピングがすべての TrustSec デバイスに展開されます。
- 新しいマッピングを展開するデバイスを選択すると、新しいマッピングの影響を受ける**すべて**のデバイスが ISE によって選択されます。

ステップ 5 [展開（Deploy）] をクリックします。[展開（Deploy）] ボタンをクリックすると、新しいマップによって影響を受けるすべてのデバイスのマッピングが更新されます。

[展開ステータス（Deployment Status）] ウィンドウに、デバイスが更新される順序と、エラーのために（またはデバイスが到達不能なために）更新されないデバイスが示されます。展開が完了すると、このウィンドウに、正常に更新されたデバイスの合計数と更新されないデバイスの数が表示されます。

[IP SGTスタティックマッピング（IP SGT Static Mapping）] ページの [ステータスを確認（Check Status）] オプションを使用して、特定のデバイスの同じ IP アドレスに複数の異なる SGT が割り当てられているかどうかを確認します。このオプションを使用すると、競合するマッピングがあるデバイス、複数の SGT にマッピングされている IP アドレス、および同じ IP アドレスに割り当てられている複数の SGT を見つけることができます。展開でデバイス グループ、FQDN、ホスト名、または IPv6 アドレスが使用される場合でも、[ステータスを確認（Check Status）] オプションを使用できます。競合するマッピングを展開する前に、それらのマッピングを削除するか、展開の範囲を変更する必要があります。

IP SGT 静的マッピングでは IPv6 アドレスを使用できます。SSH または SXP を使用して、特定のネットワーク デバイスまたはネットワーク デバイス グループにこれらのマッピングを伝達できます。

FQDN とホスト名が使用される場合、Cisco ISE はマッピングを展開して展開ステータスを検査する際に、PAN および PSN ノード内の対応する IP アドレスを検索します。

[一般TrustSecの設定（General TrustSec Settings）] ウィンドウの [ホスト名のIP SGTスタティックマッピング（IP SGT Static Mapping of Hostnames）] オプションを使用して、DNS クエリによって返される IP アドレス用に作成されるマッピング数を指定します。次のオプションのいずれかを選択します。

- DNSクエリによって返されるすべてのIPアドレスに対してマッピングを作成する（Create mappings for all IP addresses returned by a DNS query）。
- DNSクエリによって返される最初のIPv4アドレスおよび最初のIPv6アドレスに対してのみマッピングを作成する（Create mappings only for the first IPv4 address and the first IPv6 address returned by a DNS query）。

Cisco ISE への IP SGT スタティック マッピングのインポート

CSV ファイルを使用して IP SGT マッピングをインポートできます。

また、管理者ポータルからCSVテンプレートをダウンロードし、マッピングの詳細を入力し、CSV ファイルとしてテンプレートを保存して、Cisco ISE にインポートすることができます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）] の順に選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [アップロード（Upload）] をクリックします。

Cisco ISE からの IP SGT スタティック マッピングのエクスポート

IP SGT マッピングを CSV ファイルの形式でエクスポートできます。このファイルを使用して、これらのマッピングを別の Cisco ISE ノードにインポートできます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）] の順に選択します。

ステップ 2 次のいずれかを実行します。

- エクスポートするマッピングの隣にあるチェックボックスをオンにし、[エクスポート（Export）]>[選択済み（Selected）] を選択します。
- [エクスポート（Export）]>[すべて（All）] を選択して、すべてのマッピングをエクスポートします。

ステップ 3 ローカル ハード ディスクに mappings.csv ファイルを保存します。

SGT マッピング グループの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティック マッピング（IP SGT Static Mapping）] > [グループの管理（Manage Groups）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 マッピング グループの名前と説明を入力します。

ステップ 4 次の手順を実行します。

- [SGT] ドロップダウン リストから SGT を選択します。
- マッピングを展開する必要がある SXP VPN グループを選択します。
- マッピングを展開するデバイスを指定します。すべての TrustSec デバイス、選択されたネットワーク デバイス グループ、または選択されたネットワーク デバイスにマッピングを展開できます。

ステップ 5 [保存（Save）] をクリックします。

あるマッピング グループから別のマッピング グループに IP SGT マッピングを移動できます。

また、マッピングおよびマッピング グループを更新または削除できます。マッピングまたはマッピング グループを更新するには、更新するマッピングまたはマッピング グループの横にあるチェック ボックスにマークを付けてから、[編集（Edit）] をクリックします。マッピングまたはマッピング グループを削除するには、削除するマッピングまたはマッピング グループの横にあるチェック ボックスにマークを付けてから、[ごみ箱（Trash）]>[選択済み（Selected）] の順にクリックします。マッピング グループが削除されると、そのグループ内の IP SGT マッピングも削除されます。

セキュリティ グループ アクセス コントロール リストの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループACL（Security Group ACLs）] を選択します。

ステップ 2 [追加（Add）] をクリックして新規セキュリティ グループ ACL を作成します。

ステップ 3 次の情報を入力します。

- [名前（Name）]：SGACL の名前

- [説明（Description）]：SGACL の説明（任意）
- [IP バージョン（IP Version）]：この SGACL でサポートされる IP バージョン：
  - [IPv4]：IP バージョン 4（IPv4）がサポートされます
  - [IPv6]：IP バージョン 6（IPv6）がサポートされます
  - [非認識（Agnostic）]：IPv4 と IPv6 の両方がサポートされます
- セキュリティ グループ ACL の内容：アクセス コントロール リスト（ACL）コマンド。次に例を示します。

  permit icmp

  deny ip

  ISE 内では SGACL 入力の構文が検査されません。スイッチ、ルータ、アクセス ポイントをエラーなく適用できるように、正しい構文を確実に使用してください。デフォルト ポリシーを **permit IP**、**permit ip log**、**deny ip**、または **deny ip log** として設定できます。TrustSec ネットワーク デバイスでは、デフォルト ポリシーを特定セルのポリシーの最後に付加します。

  参考用に SGACL の 2 つの例を示します。どちらにも最終的な catch-all ルールが含まれています。最初の例では、最終的な catch-all ルールとして拒否し、2 番目の例では許可します。

  Permit_Web_SGACL

```
permit tcp dst eq 80
permit tcp dst eq 443
deny ip
```

  Deny_JumpHost_Protocols

```
deny tcp dst eq 23
deny tcp dst eq 23
deny tcp dst eq 3389
permit ip
```

  次の表に、IOS、IOS XE、NS OS オペレーティング システム用の SGACL の構文を示します。

SGACL CLI と ACE	**IOS、IOS XE、NX OS で共通の構文**
config acl	deny、exit、no、permit
拒否 許可	ahp、eigrp、gre、icmp、igmp、ip、nos、ospf、pcp、pim、tcp、udp
deny tcp deny tcp src deny tcp dst	dst、log、src
deny tcp dst eq deny tcp src eq	範囲は 0 ～ 65535

SGACL CLI と ACE	IOS、IOS XE、NX OS で共通の構文
deny udp deny udp src deny udp dest	Dst、log、src
deny tcp dst eq www deny tcp src eq www	範囲は 0 ～ 65535

（注） Hypens は一部のシスコのスイッチでは許可されていません。したがって、`permit dst eq 32767-65535` は有効ではありません。`permit dst eq range 32767 65535` を使用します。

ステップ 4 [プッシュ（Push）] をクリックします。
[プッシュ（Push）] オプションは CoA 通知を開始します。この通知は、Cisco ISE からの設定変更に関する更新をただちに要求するよう TrustSec デバイスに伝えます。

（注） Cisco ISE では次の事前定義済み SGACL を使用します：許可 IP、許可 IP ログ、拒否 IP、または拒否 IP ログ。これらの SGACL で GUI または ERS API を使用すると、TrustSec マトリックスを設定できます。これらの SGACL は GUI のセキュリティ グループ ACL リストのページに表示されませんが、ERS API を使用して利用可能な SGACL（ERS getAll 呼び出し）を表示すると表示されます。

出力ポリシー

出力テーブルには、送信元 SGT および宛先 SGT が、予約済みのものもそうでないものもあわせてリストされます。また、このページでは、出力テーブルをフィルタリングして特定のポリシーを表示することや、これらのプリセットフィルタを保存することもできます。送信元SGTから宛先SGTに到達しようとすると、TrustSec対応デバイスは、出力ポリシーで定義されているTrustSecポリシーに基づいてSGACLを適用します。Cisco ISEはポリシーを作成してプロビジョニングします。

TrustSec ポリシーの作成に必要な基本的構築ブロックである SGT および SGACL を作成した後に、SGACL を送信元 SGT および宛先 SGT に割り当てることによって、それらの関係を確立できます。

送信元 SGT と宛先 SGT のそれぞれの組み合わせが、出力ポリシーのセルになります。

出力ポリシーは、[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] ページで表示できます。

それぞれ異なる 3 つの方法で出力ポリシーを表示できます。

- 送信元ツリー ビュー

- 宛先ツリー ビュー
- マトリクス ビュー

送信元ツリー ビュー

送信元ツリー ビューには、簡潔で組織化された送信元 SGT のビューが折りたたまれた状態で表示されます。送信元 SGT を展開すると、選択した送信元 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、宛先 SGT にマッピングされている送信元 SGT のみが表示されます。特定の送信元 SGT を展開すると、この送信元 SGT にマッピングされているすべての宛先 SGT とその対応するポリシー（SGACL）がテーブルに表示されます。

一部のフィールドの隣に 3 個のドット（...）が表示されます。これは、セルにより多くの情報が含まれていることを示しています。カーソルを 3 個のドットの上に置くと、クイック ビュー ポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

宛先ツリー ビュー

宛先ツリー ビューには、簡潔で組織化された宛先 SGT のビューが折りたたまれた状態で表示されます。宛先 SGT を展開すると、選択した宛先 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、送信元 SGT にマッピングされている宛先 SGT のみが表示されます。特定の宛先 SGT を展開すると、この宛先 SGT にマッピングされているすべての送信元 SGT と対応するポリシー（SGACL）が表に示されます。

一部のフィールドの隣に 3 個のドット（...）が表示されます。これは、セルにより多くの情報が含まれていることを示しています。カーソルを 3 個のドットの上に置くと、クイック ビュー ポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

マトリクス ビュー

出力ポリシーのマトリクス ビューは、スプレッドシートに似ています。ここには 2 つの軸があります。

- 送信元軸：垂直軸にはすべての送信元 SGT がリストされます。
- 宛先軸：水平軸にはすべての宛先 SGT がリストされます。

送信元 SGT と宛先 SGT のマッピングが、セルとして示されます。セルにデータが含まれている場合、対応する送信元 SGT と宛先 SGT 間にマッピングがあるということになります。マトリクス ビューには 2 つのタイプのセルがあります。

- マッピングされたセル：送信元SGTと宛先SGTのペアが、順序付けされたSGACLのセットに関連付けられ、特定のステータスになっている場合。
- マッピングされていないセル：送信元 SGT と宛先 SGT のペアが、SGACL に関連付けられてなく、特定のステータスになっていない場合。

出力ポリシー セルには、送信元 SGT、宛先 SGT、最終的な catch-all ルールが 1 つのリストとして SGACL の下にカンマで区切られて表示されます。最終的な catch-all ルールは、[なし（None）] に設定されている場合には表示されません。マトリクス内の空のセルは、マッピングされていないセルを示します。

出力ポリシーのマトリクス ビューでは、マトリクスをスクロールして目的のセルのセットを表示できます。ブラウザがマトリクスデータ全体を一度にロードすることはありません。ブラウザは、ユーザがスクロールした領域に移入されるデータをサーバに要求します。これにより、メモリのオーバーフローとパフォーマンスの問題が回避されます。

[表示（View）] ドロップダウン リストで次のオプションを使用して、マトリックス ビューを変更できます。

- [SGACL名ありで簡易設定（Condensed with SGACL names）]：このオプションを選択すると、空のセルは非表示になり、SGACL 名がセルに表示されます。
- [SGACL名なしで簡易設定（Condensed without SGACL names）]：空のセルは非表示になり、SGACL 名はセルに表示されません。このビューは、より多くのマトリックス セルを表示し、色、パターンおよびアイコン（セルのステータス）を使用して、セルの内容を区別する場合に便利です。
- [SGACL名ありでフル（Full with SGACL names）]：このオプションを選択すると、左側と上側のメニューは非表示になり、SGACL 名がセルに表示されます。
- [SGACL名なしでフル（Full without SGACL names）]：このオプションを選択すると、マトリックスは全画面モードで表示され、SGACL 名はセルに表示されません。

ISE では、カスタム ビューを作成し、名前を付け、保存できます。カスタム ビューを作成するには、[表示（Show）] > [カスタムビューの作成（Create Custom View）] の順に選択します。また、ビューの条件を更新したり、未使用のビューを削除することもできます。

[マトリックス（Matrix）] ビューは、[ソース（Source）] ビューおよび [送信先（Destination）] ビューと同じ GUI 要素を持っています。ただし、次の追加要素を含みます。

マトリクスの次元

次元ビューの [次元（Dimension）] ドロップダウン リストでは、マトリクスの次元を設定することができます。

マトリクスのインポート/エクスポート

[インポート（Import）] および [エクスポート（Export）] ボタンを使用すると、マトリクスをインポートまたはエクスポートできます。

カスタム ビューの作成

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [マトリックスビュー（Matrix View）] ページで、[表示（Show）] ドロップダウン リストから [カスタム ビューの作成（Create Custom View）] オプションを選択します。

ステップ 2 [ビューの編集（Edit View）] ダイアログボックスで、次の詳細情報を入力します。

- [ビュー名（View Name）]：カスタム ビューの名前を入力します。
- [送信元セキュリティグループ（Source Security Groups）]：カスタム ビューに含める SGT を [表示（Show）] 転送ボックスに移動します。
- [着信先関連の表示（Show Relevant for Destination）]：[送信元セキュリティグループの表示（Source Security Group Show）]転送ボックスの選択内容を上書きして、[着信先セキュリティグループの非表示（Destination Security Group Hide）] 転送ボックスのすべてのエントリをコピーするには、このチェックボックスをオンにします。200 を超えるエントリがある場合、データはコピーされず、警告メッセージが表示されます。
- [着信先セキュリティグループ（Destination Security Groups）]：カスタム ビューに含める SGT を [表示（Show）] 転送ボックスに移動します。
- [送信元関連の表示（Show Relevant for Source）]：[着信先セキュリティグループの表示（Destination Security Group Show）]転送ボックスの選択内容を上書きして、[送信元セキュリティグループの非表示（Source Security Group Hide）]転送ボックスのすべてのエントリをコピーするには、このチェックボックスをオンにします。
- [次によってマトリックスをソートする（Sort Matrix By）]：次のいずれかのオプションを選択します。
  - 手動順序（Manual Order）
  - タグ番号（Tag Number）
  - SGT名（SGT Name）

ステップ 3 [保存（**Save**）] をクリックします。

マトリクス操作

マトリクスでの移動

カーソルでマトリクス コンテンツ領域をドラッグするか、または水平および垂直スクロール バーを使用して、マトリクス内を移動できます。セルをクリックしたままにし、マトリクス コンテンツ全体を任意の方向にドラッグできます。送信元および宛先のバーがセルと一緒に移動します。セルを選択すると、マトリクス ビューによってそのセルと対応する行（送信元 SGT）

およびカラム（宛先 SGT）が強調表示されます。選択したセルの座標（送信元 SGT および宛先 SGT）がマトリクス コンテンツ領域の下に表示されます。

マトリクスでのセルの選択

マトリクス ビューでセルを選択するには、該当のセルをクリックします。選択したセルが別の色で表示され、送信元 SGT および宛先 SGT が強調表示されます。セルをもう一度クリックするか、または別のセルを選択することで、セルの選択を解除できます。複数セルの選択は、マトリクス ビューでは許可されていません。セルをダブルクリックして、セルの設定を編集します。

出力ポリシーの SGACL の設定

[出力ポリシー（Egress Policy）] ページでセキュリティ グループ ACL を直接作成できます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] の順に選択します。

ステップ 2 [送信元ツリービュー（Source Tree View）] または [宛先ツリービュー（Destination Tree View）] ページから、[設定（Configure）] > [新しいセキュリティグループACLの作成（Create New Security Group ACL）] を選択します。

ステップ 3 必要な詳細を入力し、[送信（Submit）] をクリックします。

ワーク プロセスの設定

始める前に

次のタスクを実行するには、スーパー管理者である必要があります。

ステップ 1 [ワーク センター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ワーク プロセスの設定（Work Process Settings）] の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 単一マトリックス（Single Matrix）：TrustSec ネットワーク上のすべてのデバイスに対してポリシー マトリックスを 1 つのみ作成するには、このオプションを選択します。
- 複数マトリックス（Multiple Matrices）：さまざまなシナリオで複数のポリシー マトリックスを作成できるようにします。これらのマトリックスを使用して、さまざまなネットワーク デバイスに異なるポリシーを展開できます。

  （注） マトリックスは独立していて、各ネットワーク デバイスを 1 つのマトリックスのみに割り当てることができます。

- 承認プロセス付き実稼働およびステージング マトリックス（Production and Staging Matrices with Approval Process）：ワークフロー モードを有効にするには、このオプションを選択します。エディタ ロールお

よび承認者ロールに割り当てられるユーザを選択します。ユーザは、ポリシー管理者グループおよびスーパー管理者グループからのみ選択できます。ユーザはエディタ ロールおよび承認者ロールの両方に割り当てることはできません。

エディタまたは承認者ロールが割り当てられたユーザの電子メール アドレスが設定されていることを確認します。設定されていないと、ワークフロー プロセスに関する電子メール通知がこれらのユーザに送信されません。

ワークフローモードを有効にすると、エディタのロールが割り当てられたユーザは、ステージング マトリックスを作成し、ステージング ポリシーを展開するデバイスを選択して、承認者に承認を求めるステージング ポリシーを送信できます。承認者ロールが割り当てられたユーザは、ステージング ポリシーを確認し、要求を承認または拒否することができます。ステージング ポリシーが承認者によって確認され、承認された後でのみ、ステージング ポリシーを選択したネットワーク デバイスに展開できます。

ステップ 3 DEFCON マトリックスを作成する場合は、[DEFCON を使用する（Use DEFCONS）] チェックボックスをオンにします。

DEFCONS マトリックスは、ネットワーク セキュリティ侵害の発生時に簡単に展開できるスタンバイ ポリシー マトリックスです。

重大度レベル [重大（Critical）]、[深刻（Severe）]、[実質的（Substantial）]、および [適度（Moderate）] の DEFCON マトリックスを作成できます。

DEFCON マトリックスがアクティブになると、対応する DEFCON ポリシーがすべての TrustSec ネットワーク デバイスにすぐに展開されます。ネットワーク デバイスから DEFCON ポリシーを削除するには、非アクティブ化オプションを使用できます。

ステップ 4 [**保存（Save）**] をクリックします。

[マトリックス登録（Matrices Listing）] ページ

TrustSec ポリシー マトリックスと DEFCON マトリックスは、[マトリックス登録（Matrices Listing）] ページに表示されます（[ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス登録（Matrices List）]）。各マトリックスに割り当てられているデバイスの数を確認することもできます。

（注） [マトリックス登録（Matrices Listing）] ページは、単一マトリックス モードが有効であり、DEFCON マトリックス オプションが無効な場合は表示されません。

[マトリックス登録（Matrices Listing）] ページからは、次のことが行えます。

- 新しいマトリックスの追加
- 既存のマトリックスの編集

- マトリックスの削除
- 既存のマトリックスの複製
- マトリックスへの NAD の割り当て

[NAD の割り当て（Assign NADs）] オプションを使用して、マトリックスに NAD を割り当てることができます。手順は次のとおりです。

1. [ネットワーク デバイスの割り当て（Assign Network Devices）] ウィンドウで、マトリックスに割り当てるネットワーク デバイスを選択します。フィルタ オプションを使用してネットワーク デバイスを選択することもできます。
2. [マトリックス（Matrix）] ドロップダウン リストから、マトリックスを選択します。既存のすべてのマトリックスとデフォルトのマトリックスがこのドロップダウン リストに表示されます。

デバイスをマトリックスに割り当てたら、[プッシュ（Push）] をクリックし、TrustSec の設定変更を該当するネットワーク デバイスに通知します。

[マトリックス登録（Matrices Listing）] ページで作業を行うときは、次の点に注意してください。

- デフォルトのマトリックスを編集、削除、名前変更することはできません。
- 新しいマトリックスを作成する際は、空のマトリックスから開始することや、既存のマトリックスからポリシーをコピーすることができます。
- マトリックスを削除すると、そのマトリックスに割り当てられている NAD が自動的にデフォルトのマトリックスに移動します。
- 既存のマトリックスをコピーするとマトリックスのコピーが作成されますが、デバイスはコピーされたマトリックスに自動的に割り当てられません。
- 複数マトリックス モードでは、すべてのデバイスが初期段階でデフォルトのマトリックスに割り当てられます。
- 複数マトリックス モードでは、一部の SGACL がマトリックス間で共有されることがあります。この場合、SGACL コンテンツを変更すると、セルにその SGACL が含まれているすべてのマトリックスに影響します。
- 複数マトリックスは、ステージングが進行中のときに有効にすることはできません。
- 複数マトリックス モードから単一マトリックス モードに変更すると、すべての NAD が自動的にデフォルトのマトリックスに割り当てられます。
- 現在有効になっている場合は、DEFCON マトリックスを削除することはできません。

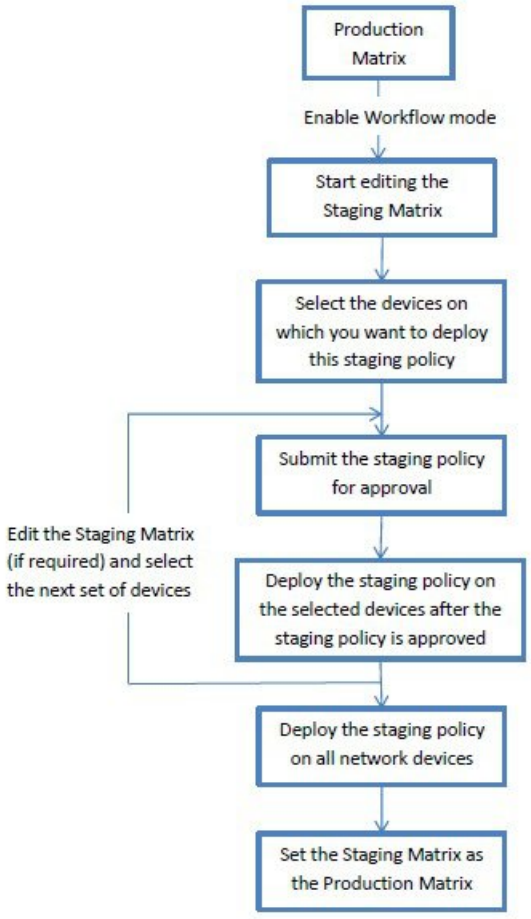
TrustSec マトリックス ワークフロー プロセス

マトリクスのワークフロー機能は、すべてのネットワーク デバイスにポリシーを導入する前に、このマトリックスのドラフト版（ステージング マトリックスとも呼ばれます）を使用して、デバイスの制限されたセットで新しいポリシーをテストできます。承認のためのステージング ポリシーを送信し、承認されると、選択したネットワーク デバイスにステージング ポリシーを導入できます。この機能により、必要に応じて、デバイスの制限されたセットへの新しいポリシーの導入、適切に機能しているかの確認、変更を行うことができます。次の一連のデバイスまたはすべてのデバイスにポリシーを適用し続けることもできます。ステージング ポリシーがすべてのネットワーク デバイスに導入されると、ステージング マトリックスは新たな実稼働マトリックスとして設定できます。

ワークフロー モードを有効にすると、エディタ ロールに割り当てられたユーザは、ステージング マトリクスを作成し、マトリクス セルを編集できます。ステージング マトリックスは、TrustSec ネットワークに現在展開されている実稼働マトリックスのコピーです。エディタは、ステージング ポリシーを展開し、承認のために承認者にステージング ポリシーを送信するデバイスを選択できます。承認者ロールが割り当てられたユーザは、ステージング ポリシーを確認し、要求を承認または拒否することができます。ステージング ポリシーが承認者によって確認され、承認された後でのみ、ステージング ポリシーを選択したネットワーク デバイスに展開できます。

次の図で、ワークフロー プロセスについて説明します。

図 *62 :* マトリックス ワークフロー プロセス



上級管理ユーザは、ワークフロー プロセスの設定ページ（[ワーク センター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ワークフロー プロセス（Workflow Process）]）で、エディタおよび承認者ロールに割り当てられたユーザを選択できます。

ステージング ポリシーが選択されたデバイスに導入された後では、SGT および SGACL を編集できませんが、マトリクスセルは編集できます。設定の差分レポートを使用して、実稼働マトリックスとステージングマトリックスの違いを追跡できます。また、ステージング処理中にそのセルへの変更を表示するには、セルで [デルタ（Delta）] アイコンをクリックします。

次の表では、ワークフローのさまざまな段階を説明します。

ステージ	説明
ステージングを編集中（Staging in Edit）	エディタがステージングマトリックスの編集を開始すると、マトリックスは [ステージングを編集中（Staging in Edit）] 状態に移行します。ステージング マトリックスを編集したら、エディタは、新しいステージング ポリシーを導入するデバイスを選択できます。
ステージングの承認待ち（Staging Awaiting Approval）	マトリックスの編集後、エディタは確認および承認を受けるために承認者にステージング マトリックスを送信します。 承認のためにステージング マトリックスを送信する時に、エディタは承認者に送信される電子メールにコメントを追加できます。 承認者は、ステージング ポリシーを確認し、要求を承認または拒否することができます。承認者は、選択したネットワーク デバイスと設定の差分レポートを表示できます。要求の承認または拒否時に、承認者はエディタに送信される電子メールにコメントを追加できます。 エディタはステージング ポリシーがどのネットワーク デバイスにも導入されていなければ承認リクエストをキャンセルできます。
展開の承認取得済み（Deploy Approved）	承認者が要求を承認すると、ステージング マトリックスは [展開の承認取得済み（Deploy Approved）] 状態に移行します。要求が拒否された場合、マトリックスは [ステージングを編集中（Staging in Edit）] 状態に戻されます。 エディタはステージング ポリシーが承認者によって承認された後でのみ、ステージングポリシーを選択したネットワーク デバイスに導入できます。

ステージ	説明
一部展開済み（Partially deployed）	ステージング マトリックスが選択したデバイスに展開された後、マトリックスは [一部展開済み（Partially deployed）] 状態に移行します。マトリックスは、ステージング ポリシーがすべてのネットワーク デバイスに導入されるまで、[一部展開済み（Partially deployed）] ステージのままです。 このステージでは、SGT および SGACL を編集できませんが、マトリクス セルは編集できます。 最新のポリシーが導入されていないデバイス（同期していないデバイス）は、[ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウにオレンジ色（イタリック体）で表示されます。このステータスは、導入の進捗状況のステータス バーにも表示されます。エディタはこれらのデバイスを選択し、さまざまな導入サイクルで更新されたデバイスを同期するように承認を要求できます。
完全に展開済み（Fully deployed）	上記の手順は、ステージング ポリシーがすべてのネットワーク デバイスに展開されるまで繰り返されます。ステージング マトリックスをすべてのネットワーク デバイスに展開する場合、承認者はステージング マトリックスを実稼働マトリックスとして設定できます。 実稼働マトリックスをステージング マトリックスに置き換えた後では、実稼働マトリックスの以前のバージョンへのロールバックはできないため、新たな実稼働マトリクスとしてステージング マトリクスを設定する前に実稼働マトリクスのコピーを取得しておくことをお勧めします。

[ワークフロー（Workflow）] ドロップダウン リストに表示されるオプションは、ワークフローの状態とユーザ ロール（エディタまたは承認者）によって異なります。次の表に、エディタおよび承認者に表示されるメニュー オプションを示します。

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
ステージングを編集中（Staging in Edit）	• ネットワークデバイスの選択（Select network devices） 次のオプションが[ネットワーク デバイスの導入（Network Device Deployment）]ウィンドウで使用できます。 • 選択したデバイスの承認要求（Request approval for selected devices） • すべての/フィルタリングされたステージング リストの承認要求（Request approval for all/filtered Staging list） • すべての/フィルタリングされた実稼働リストの承認要求（Request approval for all/filtered Production list） • すべての/フィルタリングされたデバイスの承認要求（Request approval for all/filtered devices） • 選択したデバイスの承認要求（Request approval for selected devices） • ステージングの破棄（Discard staging） • デルタの表示（View deltas）	• ネットワークデバイスの表示（View network devices） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
ステージングの承認待ち（Staging Awaiting Approval）	• 承認要求のキャンセル（Cancel approval request） • ネットワークデバイスの表示（View network devices） 次のオプションが[ネットワーク デバイスの導入（Network Device Deployment）]ウィンドウで使用できます。 • 承認要求のキャンセル（Cancel approval request） • デルタの表示（View deltas）	• 展開の承認（Approve deploy） • 展開の拒否（Reject deploy） • ネットワークデバイスの表示（View network devices） 次のオプションが[ネットワーク デバイスの導入（Network Device Deployment）]ウィンドウで使用できます。 • 展開の承認（Approve deploy） • 展開の拒否（Reject deploy） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
承認済み：展開の準備完了（Approved - ready to deploy）	• [展開（Deploy）] • 承認要求のキャンセル（Cancel approval request） • ネットワークデバイスの表示（View network devices） 次のオプションが[ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • [展開（Deploy）] • 承認要求のキャンセル（Cancel approval request） • デルタの表示（View deltas）	• 展開の拒否（Reject deploy） • ネットワークデバイスの表示（View network devices） 次のオプションが[ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • 展開の拒否（Reject deploy） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
一部展開済み（Partially deployed）	• ネットワークデバイスの選択（Select network devices） 次のオプションが[ネットワーク デバイスの導入（Network Device Deployment）]ウィンドウで使用できます。 • 選択したデバイスの承認要求（Request approval for selected devices） • すべての/フィルタリングされたステージング リストの承認要求（Request approval for all/filtered Staging list） • すべての/フィルタリングされた実稼働リストの承認要求（Request approval for all/filtered Production list） • すべての/フィルタリングされたデバイスの承認要求（Request approval for all/filtered devices） • 選択したデバイスの承認要求（Request approval for selected devices） • デルタの表示（View deltas）	• ネットワークデバイスの表示（View network devices） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
完全に展開済み（Fully deployed）	• ネットワークデバイスの選択（Select network devices） 次のオプションが[ネットワーク デバイスの導入（Network Device Deployment）]ウィンドウで使用できます。 • 選択したデバイスの承認要求（Request approval for selected devices） • すべての/フィルタリングされたステージング リストの承認要求（Request approval for all/filtered Staging list） • すべての/フィルタリングされた実稼働リストの承認要求（Request approval for all/filtered Production list） • すべての/フィルタリングされたデバイスの承認要求（Request approval for all/filtered devices） • 選択したデバイスの承認要求（Request approval for selected devices） • デルタの表示（View deltas）	• 実稼働として設定（Set as production） • ネットワークデバイスの表示（View network devices） • デルタの表示（View deltas）

ワークフロー オプションは、[送信元ツリービュー（Source Tree View）]と[宛先ツリービュー（Destination Tree View）]でも使用できます。

TrustSec ポリシーのダウンロード レポート（[ワーク センター（Work Centers）] > [TrustSec] > [レポート（Reports）]）を使用して、ステージング/実稼働ポリシーをダウンロードしたデバイスのリストを表示できます。TrustSec ポリシーのダウンロードは、ポリシー（SGT/SGACL）のダウンロードのために、ネットワーク デバイスによって送信された要求と ISE によって送信された詳細を示します。ワークフローモードを有効にしている場合、要求を実稼働マトリックスまたはステージング マトリックスに対してフィルタ処理することができます。

出力ポリシー テーブル セルの設定

Cisco ISE では、ツールバーで使用可能なさまざまなオプションを使用して、セルを設定できます。Cisco ISE では、選択した送信元 SGT および宛先 SGT がマッピングされたセルと同一である場合には、セルを設定できません。

出力ポリシー セルのマッピングの追加

[ポリシー（Policy）] ページから出力ポリシーのマッピング セルを追加できます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] の順に選択します。

ステップ 2 マトリクス セルを選択するには、次の手順を実行します。

- マトリクス ビューで、セルをクリックして選択します。
- 送信元ツリー ビューおよび宛先ツリー ビューで、内部テーブル内の行のチェックボックスをオンにして選択します。

ステップ 3 新しいマッピング セルを追加するには [追加（Add）] をクリックします。

ステップ 4 次の項目について適切な値を選択します。

- 送信元セキュリティ グループ（Source Security Group）
- 宛先セキュリティ グループ（Destination Security Group）
- ステータス（Status）、セキュリティ グループ ACL（Security Group ACLs）
- 最終的な catch-all ルール（Final Catch All Rule）

ステップ 5 [**保存（Save**）] をクリックします。

出力ポリシーのエクスポート

ステップ 1 [ワーク センター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [エクスポート（Export）] の順に選択します。

ステップ 2 エクスポートしたファイルに空のセル（SGACL が設定されていないセル）を含める場合は、[空のセルを含める（Include Empty Cells）] チェック ボックスにマークを付けます。

このオプションが有効になっている場合、マトリックス全体がエクスポートされ、空のセルは[SGACL]列に「空（Empty）」キーワードでマークされます。

（注） エクスポートされたファイルに 500000 を超える行が含まれていないことを確認してください。そうでない場合、エクスポートが失敗する場合があります。

ステップ 3 次のオプションのいずれかを選択します。

- [ローカルディスク（Local Disk）]：ローカル ドライブにファイルをエクスポートする場合は、このオプションを選択します。
- [リポジトリ（Repository）]：リモート リポジトリにファイルをエクスポートする場合は、このオプションを選択します。

ファイルをエクスポートする前にリポジトリを設定する必要があります。リポジトリを設定するには、[管理（Administration）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）] の順に選択します。読み取りおよび書き込みアクセス権が選択したリポジトリに提供されていることを確認します。

暗号キーを使用してエクスポートされたファイルを暗号化できます。

ファイル名は変更することができます。ファイル名は、50 文字以内でなければなりません。デフォルトでは、ファイル名には現在の時刻が含まれていますが、同じファイル名がリモート リポジトリに存在する場合は、ファイルが上書きされます。

ステップ 4 [エクスポート（Export）] をクリックします。

出力ポリシーのインポート

出力ポリシーをオフラインで作成し、Cisco ISE にインポートすることができます。セキュリティ グループ タグの数が多い場合、セキュリティ グループ ACL マッピングを 1 つずつ作成すると、時間がかかることがあります。代わりに、出力ポリシーをオフラインで作成し、Cisco ISE にインポートすることにより、時間を節約できます。インポート中、Cisco ISE は CSV ファイルのエントリを出力ポリシー マトリクスに追加し、データは上書きしません。

次の場合、出力ポリシーのインポートは失敗します。

- 送信元または宛先 SGT が存在しない
- SGACL が存在しない
- モニタ ステータスが、そのセルについて Cisco ISE で現在設定されているものと異なる

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [インポート（Import）] の順に選択します。

ステップ 2 [テンプレートの生成（Generate a Template）] をクリックします。

ステップ 3 [出力ポリシー（Egress Policy）] ページからテンプレート（CSV ファイル）をダウンロードし、CSV ファイルに次の情報を入力します。

- 送信元 SGT（Source SGT）
- 宛先 SGT（Destination SGT）
- SGACL
- モニタ ステータス（有効、無効、またはモニタ対象）

ステップ 4 インポートするポリシーで既存のポリシーが上書きされるようにする場合は、[新しいデータで既存のデータを上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。空セル（「Empty」キーワードでマークされた、[SGACL] 列のセル）がインポートされたファイルに含まれていると、対応するマトリックスのセルの既存のポリシーが削除されます。

イーグレス ポリシーをエクスポートする際に空セルを含めるには、[空のセルを含める（Include Empty Cells）] チェックボックスをオンにします。詳細については、出力ポリシーのエクスポート（1141 ページ）を参照してください。

ステップ 5 [ファイルの検証（Validate File）] をクリックして、インポートされたファイルを検証します。Cisco ISE は、ファイルをインポートする前に CSV 構造、SGT 名、SGACL、およびファイル サイズを検証します。

ステップ 6 エラーが発生した場合にインポートを中止するには、[最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 7 [インポート（Import）] をクリックします。

出力ポリシーの SGT の設定

[出力ポリシー（Egress Policy）] ページでセキュリティ グループを直接作成できます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] の順に選択します。

ステップ 2 [送信元ツリービュー（Source Tree View）] または [宛先ツリービュー（Destination Tree View）] ページから、[設定（Configure）] > [新しいセキュリティグループの作成（Create New Security Group）] を選択します。

ステップ 3 必要な詳細を入力し、[送信（Submit）] をクリックします。

モニタ モード

出力ポリシーの [すべてをモニタ（Monitor All）] オプションを使用すると、出力ポリシー設定ステータス全体を 1 回のクリックでモニタ モードに変更できます。[出力ポリシー（egress policy）] ページの [すべてをモニタ（Monitor All）] チェックボックスをオンにして、すべてのセルの出力ポリシー設定ステータスをモニタ モードに変更します。[すべてをモニタ（Monitor All）] チェックボックスをオンにすると、設定ステータスが次のように変更されます。

- ステータスが [有効（Enabled）] であるセルはモニタ対象として動作しますが、有効であるかのように表示されます。
- ステータスが [無効（Disabled）] であるセルは何も影響を受けません。
- ステータスが [モニタ（Monitor）] であるセルは、[モニタ対象（Monitored）] のままになります。

[すべてをモニタ（Monitor All）] チェックボックスをオフにすると、元の設定ステータスに戻ります。データベース内の実際のセルのステータスは変更されません。[すべてをモニタ（Monitor All）] をオフにすると、出力ポリシーのそれぞれのセルが元の設定ステータスに戻ります。

モニタ モードの機能

モニタ モードのモニタリング機能は次の操作に役立ちます。

- フィルタリングされているけれども、モニタ モードではモニタされているトラフィックの量の確認
- SGT-DGT ペアがモニタ モードであるか強制モードであるかの確認と、ネットワーク内で異常なパケット ドロップが発生していないかどうかの観察
- SGACL ドロップが実際に強制モードによって強制されているのか、またはモニタ モードによって許可されているのかの確認
- モードのタイプ（モニタ、強制、または両方）に基づいたカスタム レポートの作成
- NAD に適用されている SGACL、および表示の不一致（ある場合）の識別

不明セキュリティ グループ

不明セキュリティ グループは事前に設定されているセキュリティ グループで、変更不可能であり、タグ値 0 の TrustSec を表します。

Ciscoセキュリティ グループのネットワーク デバイスは、送信元または宛先のいずれかの SGT がない場合に不明 SGT を参照するセルを要求します。送信元のみが不明の場合、要求は <unknown, Destination SGT> セルに適用されます。宛先のみが不明の場合、要求は <source SGT, unknown> セルに適用されます。送信元および宛先の両方が不明の場合、要求は <Unknown, Unknown> セルに適用されます。

デフォルト ポリシー

デフォルト ポリシーは、<ANY,ANY> セルを参照します。任意の送信元 SGT が任意の宛先 SGT にマッピングされています。ここでは、ANY SGT は変更不可能であり、送信元 SGT にも宛先 SGT にも表示されません。ANY SGT は ANY SGT とのみペアにできます。他の SGT とはペアにできません。TrustSec ネットワーク デバイスでは、デフォルト ポリシーを特定セルのポリシーの最後に付加します。

- つまり、セルが空白の場合は、デフォルト ポリシーのみが含まれることになります。

- セルにポリシーが含まれる場合、結果のポリシーは、セル固有のポリシーとその後に続くデフォルト ポリシーの組み合わせになります。

Cisco ISE では、セル ポリシーおよびデフォルト ポリシーは 2 つの別々の SGACL セットになり、デバイスは 2 つの別々のポリシー クエリーの応答としてこれらのセットを取得します。

デフォルト ポリシーの設定は、他のセルと次の点で異なります。

- ステータスは [有効（Enabled）] または [モニタ対象（Monitored）] の 2 つの値しかとることができません。
- セキュリティ グループ ACL は、デフォルト ポリシーでは任意のフィールドであるため、空白のままにできます。
- 最終的な catch-all ルールは次のいずれかになります。許可 IP、拒否 IP、許可 IP ログ、または拒否 IP ログ。デフォルト ポリシーを上回る安全策はないため、ここで [なし（None）] オプションを使用できないことは明らかです。

SGT の割り当て

Cisco ISE では、デバイスのホスト名または IP アドレスがわかっている場合に、TrustSec デバイスに SGT を割り当てることができます。特定のホスト名または IP アドレスを持つデバイスがネットワークに参加すると、Cisco ISE によって認証前に SGT が割り当てられます。

次の SGT がデフォルトで作成されています。

- SGT_TrustSecDevices
- SGT_NetworkServices
- SGT_Employee
- SGT_Contractor
- SGT_Guest
- SGT_ProductionUser
- SGT_Developer
- SGT_Auditor
- SGT_PointofSale
- SGT_ProductionServers
- SGT_DevelopmentServers
- SGT_TestServers
- SGT_PCIServers
- SGT_BYOD
- SGT_Quarantine

セキュリティ グループ タグをエンドポイントにマップするようにデバイスを手動で設定する必要がある場合もあります。このマッピングは [セキュリティ グループ マッピング（Security Group Mappings）] ページから作成できます。この操作を実行する前に、SGT の範囲が予約済みであることを確認します。

ISE では、最大 10,000 の IP-to-SGT マッピングを作成できます。IP-to-SGT マッピング グループを作成して、このような大規模なマッピングを論理的にグループ化することができます。各 IP-to-SGT マッピング グループには、IP アドレスのリスト、マップ先の単一のセキュリティ グループ、およびこれらのマッピングの展開対象であるネットワーク デバイスまたはネットワーク デバイス グループが含まれています。

NDAC 許可

デバイスに SGT を割り当てることで TrustSec ポリシーを設定できます。TrustSec デバイスの ID 属性に基づいて、デバイスにセキュリティ グループを割り当てることができます。

NDAC 許可の設定

始める前に

- ポリシーで使用するためのセキュリティ グループを作成します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [ネットワークデバイス許可（Network Device Authorization）] の順に選択します。

ステップ 2 [デフォルト ルール（Default Rule）] 行の右側にある [操作（Action）] アイコンをクリックし、[新規行を上に挿入（Insert New Row Above）] をクリックします。

ステップ 3 このルールの名前を入力します。

ステップ 4 [条件（Conditions）] の隣にあるプラス記号（+）をクリックして、ポリシー条件を追加します。

ステップ 5 [新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）] をクリックすると、新しい条件を作成できます。

ステップ 6 [セキュリティ グループ（Security Group）] ドロップダウン リストから、この条件の評価が true になった場合に割り当てる SGT を選択します。

ステップ 7 この行の [操作（Action）] アイコンをクリックして、現在のルールの上または下に、デバイス属性に基づいた別のルールを追加します。このプロセスを繰り返して、TrustSec ポリシーに必要なすべてのルールを作成できます。ルールをドラッグ アンド ドロップし、  アイコンをクリックすることでこれらの順序を変更できます。既存の条件を複製することもできますが、ポリシー名は必ず変更してください。

評価が true になる最初のルールによって、評価の結果が決まります。いずれのルールも一致しなかった場合、デフォルト ルールが適用されます。デフォルト ルールを編集して、いずれのルールも一致しなかった場合にデバイスに適用される SGT を指定できます。

ステップ 8 [保存（Save）] をクリックして TrustSec ポリシーを保存します。

ネットワーク デバイス ポリシーを設定した後に、TrustSec デバイスで認証を行おうとすると、デバイスはその SGT およびそのピアの SGT を取得し、関連するすべての詳細をダウンロードできるようになります。

エンドユーザの許可の設定

Cisco ISE では、許可ポリシー評価の結果としてセキュリティ グループを割り当てることができます。このオプションを使用すると、ユーザおよびエンドポイントにセキュリティ グループを割り当てることができます。

始める前に

- 許可ポリシーについての情報を参照してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [承認ポリシー（Authorization Policy）] の順に選択します。

ステップ 2 新しい許可ポリシーを作成します。

ステップ 3 権限のセキュリティ グループを選択します。

あるユーザまたはエンドポイントについて、この許可ポリシーで指定した条件が true の場合、このセキュリティ グループがそのユーザまたはエンドポイントに割り当てられ、このユーザまたはエンドポイントによって送信されたすべてのデータ パケットにこの特定の SGT でタグが付けられます。

TrustSec の設定およびポリシー プッシュ

Cisco ISE では、許可変更（CoA）がサポートされています。これを使用すると、Cisco ISE で TrustSec の設定およびポリシーの変更を TrustSec デバイスに通知でき、デバイスでは関連データの取得要求でこれに応答できるようになります。

CoA 通知では、TrustSec ネットワーク デバイスをトリガーし、環境 CoA またはポリシー CoA のいずれかを送信できます。

また、基本的に TrustSec CoA 機能をサポートしないデバイスに設定変更をプッシュできます。

CoA でサポートされるネットワーク デバイス

Cisco ISE は次のネットワーク デバイスに CoA 通知を送信します。

- 単一の IP アドレスを持つネットワーク デバイス（サブネットはサポートされません）

- TrustSec デバイスとして設定されているネットワーク デバイス
- CoA サポート対象として設定されているネットワーク デバイス

複数のセカンダリが存在する分散環境に Cisco ISE が展開されており、これらのセカンダリがそれぞれ異なるデバイス セットと相互運用している場合、CoA 要求は Cisco ISE プライマリ ノードからすべてのネットワーク デバイスに送信されます。そのため、TrustSec ネットワーク デバイスは、Cisco ISE プライマリ ノードで CoA クライアントとして設定されている必要があります。

デバイスは、Cisco ISE プライマリ ノードに CoA NAK または ACK を返します。ただし、ネットワーク デバイスからの次の TrustSec セッションは、ネットワーク デバイスが他の AAA 要求をすべて送信する Cisco ISE ノードに送信され、必ずしもプライマリ ノードに送信されるわけではありません。

非 CoA サポート デバイスへの設定変更のプッシュ

一部のプラットフォームでは、許可変更（CoA）について Cisco ISE の「プッシュ」機能はサポートされていません。例：Nexus ネットワーク デバイスの一部のバージョン。この場合、ISE はネットワーク デバイスに接続し、ISE に対して更新された設定要求をデバイスがトリガーするようにします。これを行うために、ISE はネットワーク デバイスへの SSHv2 トンネルを開き、TrustSec ポリシーマトリクスのリフレッシュをトリガーするコマンドを送信します。この方法は、CoA プッシュをサポートするネットワーク プラットフォームでも実行できます。

ステップ 1 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** の順に選択します。

ステップ 2 必要なネットワーク デバイスの横にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ネットワーク デバイスの名前、IP アドレス、RADIUS および TrustSec 設定が正しく設定されていることを確認します。

ステップ 3 [高度な TrustSec 設定（Advanced TrustSec Settings）] まで下にスクロールし、[TrustSec 通知および更新（TrustSec Notifications and Updates）] セクションで、[デバイスに設定変更を送信（Send configuration changes to device）] チェックボックスをオンにして [CLI（SSH）（CLI (SSH)）] オプション ボタンをクリックします。

ステップ 4 （任意） SSH キーを指定します。

ステップ 5 デバイス インターフェイスのクレデンシャルを使用して IP-SGT マッピングを取得するには、この SGA デバイスに対して [セキュリティ グループ タグ マッピングの展開時にこのデバイスを含める（Include This Device When Deploying Security Group Tag Mapping Updates）] チェックボックスをオンにします。

ステップ 6 EXEC モードでデバイス設定を編集する権限を持つユーザのユーザ名とパスワードを入力します。

ステップ 7 （任意） 設定を編集できるデバイスの EXEC モード パスワードを有効にするためのパスワードを入力します。[表示（Show）] をクリックして、このデバイスにすでに設定されている EXEC モード パスワードを表示できます。

ステップ 8 ページの下部にある [送信（Submit）] をクリックします。

ネットワーク デバイスは、TrustSec の変更をプッシュするように設定されました。Cisco ISE ポリシーを変更した後で、ネットワーク デバイスに新規設定を反映させるには、[プッシュ（Push）] をクリックします。

SSH キーの検証

SSH キーを使用してセキュリティを強化することもできます。Cisco ISE では、SSH キー検証機能によってこれをサポートします。

この機能を使用するには、Cisco ISE からネットワーク デバイスに SSHv2 トンネルを開いて、ネットワーク デバイスの独自の CLI を使用して SSH キーを取得します。このキーをコピーし、検証のために Cisco ISE に貼り付けます。SSH キーが誤っている場合、Cisco ISE は接続を終了します。

制限：現在、Cisco ISE が検証できるのは 1 つの IP のみです（IP の範囲、または IP 内のサブネットは検証できません）

始める前に

次のものが必要です。

- ログイン クレデンシャル
- SSH キーを取得する CLI コマンド

（Cisco ISE とセキュアに通信できるようにするネットワーク デバイスのもの）

ステップ 1 ネットワーク デバイス上：

a) Cisco ISE が SSH キー検証を使用して通信するネットワーク デバイスにログインします。
b) デバイスの CLI を使用して SSH キーを表示します。

例：

Catalyst デバイスの場合、コマンドは次のとおりです。`sho ip ssh`。

c) 表示された SSH キーをコピーします。

ステップ 2 Cisco ISE ユーザ インターフェイスから、次の手順を実行します。

a) **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]** を選択し、必要なネットワーク デバイス名、IP アドレス、RADIUS および TrustSec 設定が正しく設定されていることを確認します。
b) [高度な TrustSec 設定（Advanced TrustSec Settings）] まで下にスクロールし、[TrustSec 通知および更新（TrustSec Notifications and Updates）] セクションで、[デバイスに設定変更を送信（Send configuration changes to device）] チェックボックスをオンにして [CLI（SSH）（CLI (SSH)）] オプション ボタンをクリックします。
c) [SSH キー（SSH Key）] フィールドに、ネットワーク デバイスから取得した SSH キーを貼り付けます。

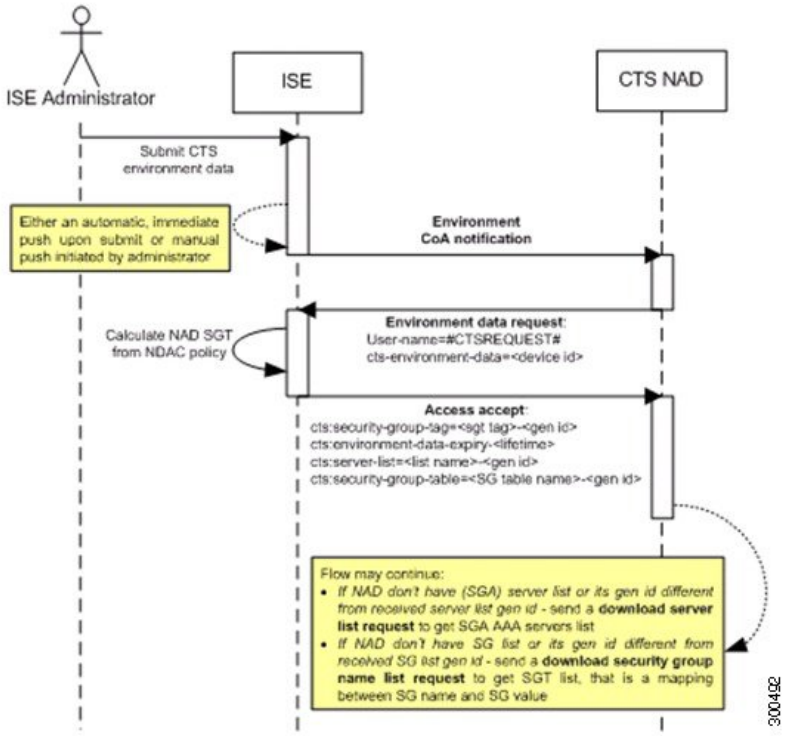
d) ページの下部にある [送信（Submit）] をクリックします。

ネットワーク デバイスは、SSH キー検証を使用して Cisco ISE と通信するようになりました。

環境 CoA 通知のフロー

次の図は、環境 CoA 通知のフローを示しています。

図 *63* : 環境 *CoA* 通知のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに環境 CoA 通知を送信します。
2. デバイスは、環境データ要求を返します。
3. 環境データ要求への応答で、Cisco ISE は次の情報を返します。

   要求を送信したデバイスの環境データ：これには、（NDAC ポリシーから推測される）TrustSec デバイスの SGT およびダウンロード環境 TTL が含まれます。

   TrustSec AAA サーバ リストの名前および生成 ID。

   （複数の可能性がある）SGT テーブルの名前および生成 ID：これらのテーブルには SGT 名と SGT 値がリストされ、一緒に SGT の完全リストも保持されます。

4. デバイスが TrustSec AAA サーバ リストを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、AAA サーバ リストの内容を取得します。
5. デバイスが応答にリストされている SGT テーブルを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、その SGT テーブルの内容を取得します。

環境 CoA トリガー

環境 CoA は次のものに関して開始できます。

- ネットワーク デバイス
- セキュリティ グループ
- AAA サーバ

ネットワーク デバイスの環境 CoA のトリガー

ネットワーク デバイスに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [管理（Administration）]>[ネットワーク リソース（Network Resources）]>[ネットワーク デバイス（Network Devices）]**[ワーク センター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 ネットワーク デバイスを追加または編集します。

ステップ 3 [高度な TrustSec 設定（Advanced TrustSec Settings）] セクションで、[TrustSec 通知および更新（TrustSec Notifications and Updates）] パラメータを更新します。

環境属性の変更は、変更が発生した特定の TrustSec ネットワーク デバイスにのみ通知されます。

単一のデバイスのみが影響を受けるため、環境 CoA 通知は送信直後に送信されます。結果として、そのデバイスの環境属性が更新されます。

セキュリティ グループの環境 CoA のトリガー

セキュリティ グループに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）] を選択します。

ステップ 2 [セキュリティ グループ（Security Group）] ページで、SGT の名前を変更します。これにより、その SGT のマッピング値の名前が変更されます。これで環境変更がトリガーされます。

ステップ 3 複数の SGT の名前を変更した後、[プッシュ（Push）] ボタンをクリックして、環境 CoA 通知を開始します。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、変更されたすべての SGT の更新が提供されます。

TrustSec AAA サーバの環境 CoA のトリガー

TrustSec AAA サーバに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [TrustSec AAAサーバ（TrustSec AAA Servers）] を選択します。

ステップ 2 [TrustSec AAA サーバ（TrustSec AAA Servers）] ページで、TrustSec AAA サーバの設定を作成、削除、または更新します。これで環境変更がトリガーされます。

ステップ 3 複数の TrustSec AAA サーバを設定した後、[プッシュ（Push）] ボタンをクリックして、環境 CoA 通知を開始します。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、変更されたすべての TrustSec AAA サーバの更新を提供します。

NDAC ポリシーの環境 CoA のトリガー

NDAC ポリシーに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [ポリシー（Policy）] > [ネットワークデバイス許可（Network Device Authorization）] の順に選択します。

[NDAC ポリシー（NDAC policy）] ページで、NDAC ポリシーのルールを作成、削除、または更新できます。これらの環境変更は、すべてのネットワーク デバイスに通知されます。

ステップ 2 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [ネットワークデバイス許可（Network Device Authorization）] の順に選択します。

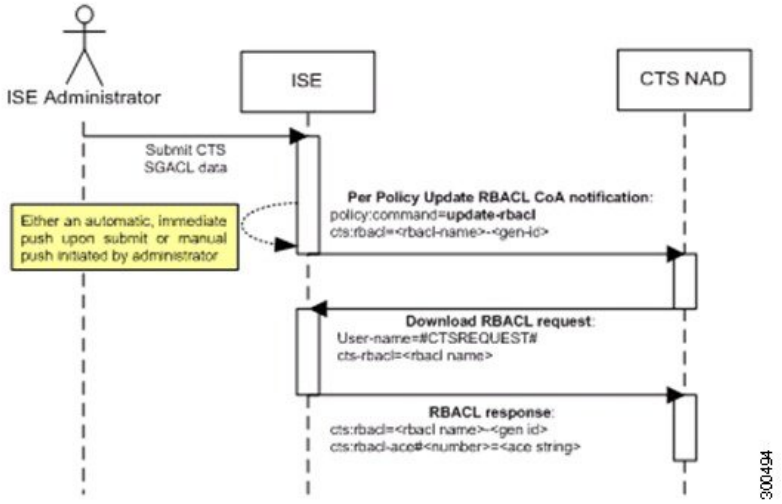
[NDAC ポリシー（NDAC policy）] ページで、NDAC ポリシーのルールを作成、削除、または更新できます。これらの環境変更は、すべてのネットワーク デバイスに通知されます。

ステップ 3 [NDAC ポリシー（NDAC policy）] ページで [プッシュ（Push）] ボタンをクリックすることで、環境 CoA 通知を開始できます。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、ネットワーク デバイス自体の SGT の更新を提供します。

SGACL コンテンツ更新のフロー

次の図に、SGACL コンテンツ更新のフローを示します。

図 *64 : SGACL* コンテンツ更新のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに SGACL 名前付きリストの更新 CoA 通知を送信します。通知には、SGACL 名と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGACL データ要求で応答できます。

   SGACL が、デバイスが保持する出力セルに含まれている場合。デバイスには出力ポリシー データのサブセットが保持されます。これらは、そのネイバーデバイスおよびエンドポイントの SGT に関連するセルです（選択した宛先 SGT の出力ポリシー カラム）。

   CoA 通知内の生成 ID が、この SGACL 用にデバイスが保持している生成 ID と異なっている。
3. SGACL データ要求への応答で、Cisco ISE は SGACL のコンテンツ（ACE）を返します。

SGACL 名前付きリストの更新 CoA の開始

SGACL 名前付きリストの更新 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループACL（Security Group ACLs）] を選択します。

ステップ 2 SGACL のコンテンツを変更します。SGACL を送信すると、SGACL の生成 ID が変更されます。

ステップ 3 複数の SGACL のコンテンツを変更した後、[プッシュ（Push）] ボタンをクリックして、SGACL 名前付きリストの更新 CoA 通知を開始します。この通知は、すべての TrustSec ネットワーク デバイスに送信され、関連するデバイスのその SGACL コンテンツの更新が提供されます。

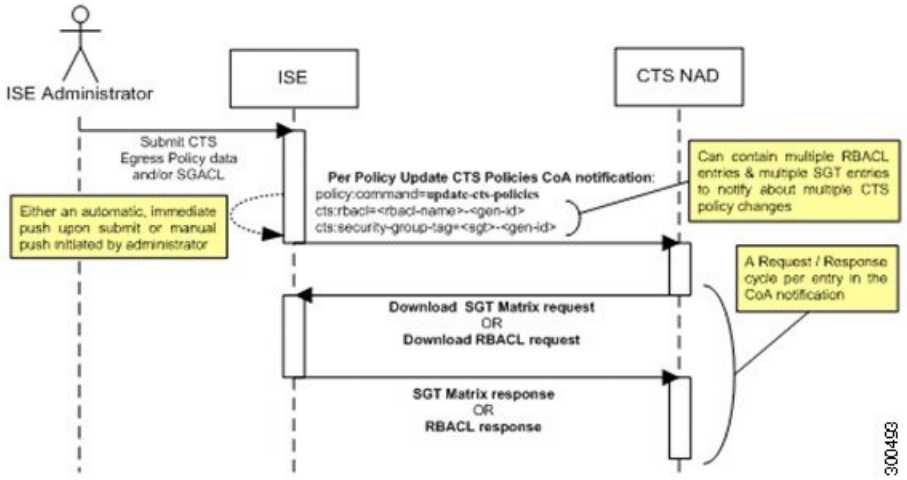
SGACL の名前または IP バージョンを変更しても、その生成 ID は変更されません。そのため、SGACL 名前付きリストの更新 CoA 通知を送信する必要はありません。

ただし、出力ポリシーで使用中の SGACL の名前または IP バージョンを変更することは、その SGACL を含むセルが変更されることを意味するため、この変更でそのセルの宛先 SGT の生成 ID が変更されます。

ポリシーの更新 CoA 通知のフロー

次の図に、ポリシーの CoA 通知のフローを示します。

図 *65 :* ポリシーの *CoA* 通知のフロー

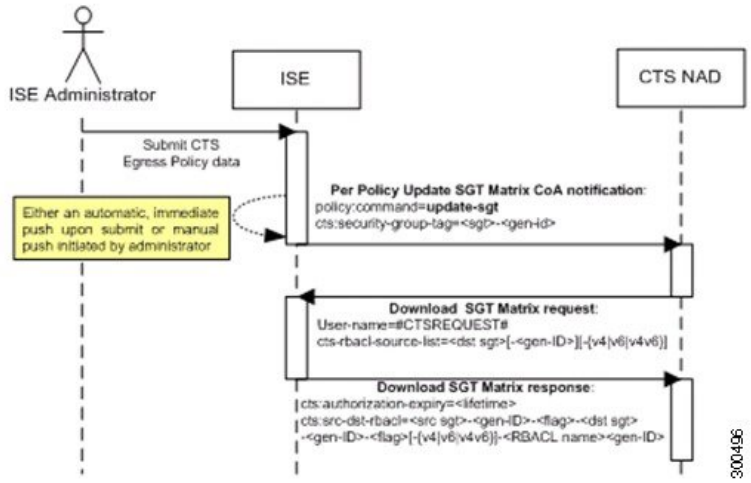


1. Cisco ISE は、TrustSec ネットワーク デバイスにポリシーの更新 CoA 通知を送信します。通知には、複数の SGACL 名とその生成 ID、および複数の SGT 値とその生成 ID が含まれることがあります。
2. デバイスは、複数の SGACL データ要求か複数の SGT データ、またはその両方で応答できます。
3. 各 SGACL データ要求または SGT データ要求に対する応答で、Cisco ISE は関連するデータを返します。

SGT マトリクスの更新 CoA のフロー

次の図に、SGT マトリクスの更新 CoA のフローを示します。

図 *66 : SGT* マトリクスの更新 *CoA* のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに SGT マトリクスの更新 CoA 通知を送信します。通知には、SGT 値と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGT データ要求で応答できます。

   SGT がネイバーデバイスまたはエンドポイントの SGT である場合。デバイスは、ネイバーデバイスおよびエンドポイントの SGT に関連するセルをダウンロードして保持します（宛先 SGT）。

   CoA 通知内の生成 ID が、この SGT 用にデバイスが保持している生成 ID と異なっている。
3. SGT データ要求に対する応答で、Cisco ISE は、送信元および宛先 SGT、セルのステータス、そのセルに設定されている SGACL 名の順序リストなど、すべての出力セルのデータを返します。

出力ポリシーからの、SGT マトリクスの更新 CoA の開始

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] の順に選択します。

ステップ 2 [出力ポリシー（Egress Policy）] ページで、セルの内容（ステータス、SGACL）を変更します。

ステップ 3 変更を送信すると、そのセルの宛先 SGT の生成 ID が変更されます。

ステップ 4 複数の出力セルの内容を変更した後、[プッシュ（Push）] ボタンをクリックして、SGT マトリクスの更新 CoA 通知を開始します。この通知は、すべての TrustSec ネットワーク デバイスに送信され、関連するデバイスのセルの内容の更新が提供されます。

TrustSec CoA の概要

次の表に、TrustSec CoA の開始を要求するさまざまなシナリオ、各シナリオで使用される CoA のタイプ、および関連する UI ページの概要を示します。

表 *145 : TrustSec CoA* の概要

UI ページ	CoA をトリガーする操作	トリガー方法	CoA タイプ	送信先
ネットワーク デバイス（Network Device）	ページの [TrustSec] セクションでの環境 TTL の変更	TrustSec ネットワーク デバイスで正常に送信が行われたとき	環境	特定のネットワーク デバイス
TrustSec AAA サーバ（TrustSec AAA Server）	TrustSec AAA サーバの変更（作成、更新、削除、順序変更）	[TrustSec AAA サーバ（TrustSec AAA servers）] リスト ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス
セキュリティ グループ（Security Group）	SGT の変更（作成、名前変更、削除）	[SGT] リスト ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス
NDAC ポリシー（NDAC Policy）	NDAC ポリシーの変更（作成、更新、削除）	[NDAC ポリシー（NDAC policy）] ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス

UI ページ	CoA をトリガーする操作	トリガー方法	CoA タイプ	送信先
SGACL	SGACL ACE の変更	[SGACL] リストページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	RBACL 名前付きリストの更新	すべての TrustSec ネットワーク デバイス
	SGACL 名または IP バージョンの変更	[SGACL] リストページの [プッシュ（Push）] ボタンまたは出力テーブルのポリシー プッシュ ボタンをクリックすると、累積された変更をプッシュできます。	更新 SGT マトリクス	すべての TrustSec ネットワーク デバイス
出力ポリシー（Egress Policy）	SGT の生成 ID を変更するすべての操作	[出力ポリシー（egress policy）] ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	更新 SGT マトリクス	すべての TrustSec ネットワーク デバイス

セキュリティ グループ タグの交換プロトコル

セキュリティ グループ タグ（SGT）の交換プロトコル（SXP）は、TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播するために使用されます。SXP は、ある SGT 対応ネットワーク デバイスから別のデバイスに IP アドレスとともにエンドポイントの SGT を転送するために使用されます。SXP が転送するデータは、IP-SGT マッピングと呼ばれます。エンドポイントが属する SGT は静的または動的に割り当てることができ、SGT はネットワーク ポリシーで分類子として使用できます。

ノードで SXP サービスをイネーブルにするには、[ノードの一般設定（General Node Settings）] ページで [SXPサービスの有効化（Enable SXP Service）] チェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。

SXP はトランスポート プロトコルとして TCP を使用して、2 つの個別のネットワーク デバイス間に SXP 接続をセットアップします。各 SXP 接続には、SXP スピーカーとして指定されたピアと、SXP リスナーとして指定されたピアがあります。ピアは双方向モードで設定することもでき、そのモードでは、それぞれがスピーカーとリスナーの両方として機能します。接続はいずれかのピアによって開始できますが、マッピング情報は常にスピーカーからリスナーに伝播されます。

（注） セッションのバインディングは常にデフォルトの SXP ドメインに伝播されます。

次の表には、SXP 環境で使用される一般的な用語のいくつかを示しています。

IP-SGT マッピング	SXP 接続を介して交換される SGT マッピングへの IP アドレス。 SXP デバイスで学習されたすべてのマッピング（スタティック マッピングおよびセッション マッピングを含む）を表示するには、[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [すべてのSXPマッピング（All SXP Mappings）] の順に選択します。
SXP スピーカー	SXP 接続を介して IP-SGT マッピングを送信するピア。
SXP リスナー	SXP 接続を介して IP-SGT マッピングを受信するピア。

Cisco ISE に追加された SXP ピア デバイスを表示するには、[ワークセンター（Work centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）] の順に選択します。

（注） SXP サービスはスタンドアロン ノードで実行することを推奨します。

SXP サービスを使用する際は、次の点に注意してください。

- Cisco ISE は、同じ IP アドレスを持つ複数の SXP セッション バインディングをサポートしていません。
- RADIUS アカウンティング更新の頻度が高すぎる（数秒に約 6 から 8 のアカウンティング更新）場合、アカウンティング更新パケットがドロップされる可能性があり、SXP が IP-SGT バインディングを受信できないことがあります。
- 以前のバージョンの ISE からアップグレードした後は、SXP は自動的に起動しません。アップグレード後に、SXP パスワードを変更し、SXP プロセスを再起動する必要があります。

SXP デバイスの追加

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 デバイスの詳細を入力します。

- CSV ファイルを使用して SXP デバイスを追加するには、[CSVファイルからアップロード（Upload from a CSV file）] をクリックします。CSV ファイルを参照して選択し、[アップロード（Upload）] をクリックします。

  また、CSV テンプレート ファイルをダウンロードして、追加するデバイスの詳細を入力し、CSV ファイルをアップロードすることもできます。

- 各 SXP デバイスのデバイスの詳細を手動で追加するには、[単一デバイスの追加（Add Single Device）] をクリックします。

  ピア デバイスの名前、IP アドレス、SXP ロール（リスナー、スピーカー、または両方）、パスワード タイプ、SXP バージョン、および接続されている PSN を入力します。また、ピア デバイスが接続されている SXP ドメインも指定する必要があります。

ステップ 4 （任意）[詳細設定（Advanced Settings）] をクリックし、次の詳細を入力します。

- [最小許容ホールドタイマー（Minimum Acceptable Hold Timer）]：スピーカーが接続状態を保持するためにキープアライブ メッセージを送信する時間を秒単位で指定します。値の範囲は 1 ～ 65534 です。
- [キープアライブタイマー（Keep Alive Timer）]：アップデート メッセージによって他の情報がエクスポートされないインターバル期間にキープアライブ メッセージのディスパッチをトリガーするためにスピーカーによって使用されます。値の範囲は 0 ～ 64000 です。

ステップ 5 [保存（**Save**）] をクリックします。

SXP ドメイン フィルタの追加

SXP デバイスで学習されたすべてのマッピング（スタティック マッピングおよびセッション マッピングを含む）は、[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [すべての SXP マッピング（All SXP Mappings）] ページで表示できます。

デフォルトでは、ネットワーク デバイスから学習されたセッション マッピングは、デフォルトの VPN グループにのみ送信されます。SXP ドメイン フィルタを作成して、異なる SXP ドメイン（VPN）にマッピングを送信できます。

SXP ドメイン フィルタを追加するには、次の手順を実行します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワーク センター（Work Centers）] > [TrustSec] > [SXP] > [すべての SXP マッピング（All SXP Mappings）] の順に選択します。

ステップ 2 [SXP ドメイン フィルタの追加（Add SXP Domain Filter）] をクリックします。

ステップ 3 次の手順を実行します。

- サブネットの詳細を入力します。このサブネットからの IP アドレスを持つネットワーク デバイスのセッション マッピングは、[SXP ドメイン（SXP Domain）] フィールドで選択された SXP ドメイン（VPN）に送信されます。
- [SGT] ドロップダウン リストから SGT を選択します。この SGT に関連するセッション マッピングは、[SXP ドメイン（SXP Domain）] フィールドで選択された SXP ドメインに送信されます。

  サブネットと SGT の両方を指定した場合、このフィルタに一致するセッション マッピングは、[SXP ドメイン（SXP Domain）] フィールドで選択した SXP ドメインに送信されます。
- マッピングを送信する必要がある SXP ドメインを選択します。

ステップ 4 [保存（Save）] をクリックします。

SXP ドメイン フィルタを更新または削除することもできます。フィルタを更新するには、[SXP ドメイン フィルタの管理（Manage SXP Domain Filter）] をクリックし、更新するフィルタの横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。フィルタを削除するには、削除するフィルタの横にあるチェックボックスをオンにして、[ごみ箱（Trash）]>[選択済み（Selected）] をクリックします。

SXP の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [SXP設定（SXP Settings）] の順に選択します。

ステップ 2 [SXP設定（SXP Settings）] ページに必要な詳細を入力します。

[SXP バインディングを PxGrid で公開（Publish SXP Bindings on PxGrid）] チェックボックスをオフにすると、IP-SGT マッピングはネットワーク デバイス全体に伝達されません。

ステップ 3 [保存（Save）] をクリックします。

（注） SXP 設定が変更されると、SXP サービスが再起動されます。

TrustSec-ACI 統合

Cisco ISE では、SGT および SXP マッピングを内部エンドポイント グループ（IEPG）、外部エンドポイント グループ（EEPG）、シスコ アプリケーション セントリック インフラストラクチャ（ACI）のエンドポイント（EP）設定と同期することができます。

Cisco ISE は、ISE で IEPG を同期して関連する読み取り専用 SGT を作成することで、ACI ドメインから TrustSec ドメインに着信するパケットをサポートします。これらの SGT は、ACI に設定されたエンドポイントをマッピングし、ISE で関連 SXP マッピングを作成します。SGT は [セキュリティグループ（Security Groups）] ページに表示されます（[学習元（Learned From）] フィールドに値 [ACI] が入った状態で）。[すべての SXP マッピング（All SXP Mappings）] ページで SXP マッピングを表示できます。これらのマッピングは、（[ACIの設定（ACI Settings）] ページで）[ポリシープレーン（Policy Plane）] オプションが選択され、SXP デバイスが [ACI の設定（ACI Settings）] ページで設定した SXP ドメインに属している場合にのみ、ACI に送信されます。

（注） 読み取り専用 SGT は、IP-SGT マッピング、マッピング グループ、および SXP ローカル マッピングでは使用できません。

セキュリティ グループを追加する際には、[ACIに伝播（Propagate to ACI）] オプションを使用して、SGT を ACI に送信する必要があるかどうかを指定できます。このオプションを有効にすると、この SGT に関連する SXP マッピングが ACI に送信されます。ただし、（[ACIの設定（ACI Settings）] ページで）[ポリシープレーン（Policy Plane）] オプションが選択され、SXP デバイスが [ACIの設定（ACI Settings）] ページで設定した SXP ドメインに属している場合にのみ、ACI に送信されます。

ACI は SGT を同期して関連する EEPG を作成することで、TrustSec ドメインから ACI ドメインに送信されるパケットをサポートします。ACI は、Cisco ISE からの SXP マッピングに基づいて EEPG でサブネットを作成します。これらのサブネットは、対応する SXP マッピングが Cisco ISE で削除されるときに、ACI から削除されません。

IEPG が ACI で更新されると、対応する SGT 設定が Cisco ISE で更新されます。SGT が Cisco ISE に追加されると、新しい EEPG が ACI に作成されます。SGT が削除されると、対応する EEPG が ACI で削除されます。エンドポイントが ACI で更新されると、対応する SXP マッピングは Cisco ISE で更新されます。

ACI サーバとの接続が失われると、接続が再確立されるときに、Cisco ISE は再びデータを再同期します。

（注） ACI の統合機能を使用するには、SXP サービスを有効にする必要があります。

ACI の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 信頼できる証明書ストアに ACI 証明書をインポートします。[管理（Administration）]>[システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）] の順に選択し、証明書をインポートします。

ステップ 2 [ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ACI の設定（ACI Settings）] の順に選択します。

ステップ 3 [TrustSec-ACI ポリシー要素の交換（TrustSec-ACI Policy Element Exchange）] チェックボックスをオンにして、SGT および SXP マッピングと ACI の IEPG、EEPG、エンドポイントの設定とを同期します。

ステップ 4 次のオプションのいずれかを選択します。

- [ポリシープレーン（Policy Plane）]：Cisco ISE が SGT、EPG、および SXP 情報を交換するために APIC データ センターだけとやりとりするようにするには、このオプションを選択します。
- [データプレーン（Data Plane）]：このオプションを選択すると、TrustSec ネットワークと APIC 制御ネットワーク間で接続する ASR デバイスに対し、SGT と EPG 以外に追加情報が提供されます。これらの ASR デバイスには、SGT から EPG および EPG から SGT への変換のための変換テーブルが含まれている必要があります。

  （注） [データプレーン（Data Plane）] オプションを選択した場合、SXP マッピングは ACI に伝播されません。

ステップ 5 [ポリシー プレーン（Policy Plane）] オプションを選択した場合は、次の詳細を入力してください。

- IP アドレス/ホスト名（IP address/Hostname）：ACI サーバの IP アドレスまたはホスト名を入力します。カンマで区切った 3 つの IP アドレスまたはホスト名を入力できます。
- 管理者名/パスワード（Admin Name/Password）：ACI 管理ユーザのユーザ名とパスワードを入力します。
- テナント（Tenant）：ACI で設定されているテナントの名前を入力します。
- L3 ルートネットワーク名（L3 Route Network Name）：ポリシー要素を同期させるために ACI で設定されているレイヤ 3 ルート ネットワークの名前を入力します。

[テスト設定（Test Settings）] をクリックして、ACI サーバとの接続性を確認します。

- 新規 SGT サフィックス（New SGT Suffix）：このサフィックスは、ACI から学習された EPG に基づいて新規に作成された SGT に追加されます。

  （注） EPG 名が 32 文字を超える場合は切り捨てられます。ただし、[セキュリティ グループ（Security Groups）] リスト ページの [説明（Description）] フィールドで EPG のフルネーム、アプリケーション プロファイル名、SGT サフィックスの詳細を確認できます。

- 新規 EPG サフィックス（New EPG Suffix）：このサフィックスは、Cisco ISE から学習された SGT に基づいて ACI で新規に作成された EPG に追加されます。
- [SXP 伝達（SXP Propagation）] 領域で、すべての SXP ドメインを選択するか、または ACI とマッピングを共有する SXP ドメインを指定することができます。

ステップ 6 [データ プレーン（Data Plane）] オプションを選択した場合は、次の詳細を入力してください。

- [SXP を使用して伝播（Propagate using SXP）]：Cisco ISE に ACI からエンドポイント（EP）データを学習させ、SXP を使用して EP データを伝播させる場合は、このチェックボックスをオンにします。

  （注） このオプションを選択する場合は、展開ノード（[管理（Administration）]>[システム（System）] > [展開（Deployment）]）で SXP サービスが有効になっていることを確認します。

- IP アドレス/ホスト名（IP address/Hostname）：ACI サーバの IP アドレスまたはホスト名を入力します。カンマで区切った 3 つの IP アドレスまたはホスト名を入力できます。
- 管理者名/パスワード（Admin Name/Password）：ACI 管理ユーザのユーザ名とパスワードを入力します。
- テナント（Tenant）：ACI で設定されているテナントの名前を入力します。

  [テスト設定（Test Settings）] をクリックして、ACI サーバとの接続性を確認します。

- IEPG の最大数（Max number of IEPGs）：SGT に変換される IEPG の最大数を指定します。IEPG はアルファベット順に変換されます。デフォルト値は 1000 です。
- SGT の最大数（Max number of SGTs）：IEPG に変換される SGT の最大数を指定します。SGT はアルファベット順に変換されます。デフォルト値は 500 です。
- 新規 SGT サフィックス（New SGT Suffix）：このサフィックスは、ACI から学習された EPG に基づいて新規に作成された SGT に追加されます。
- 新規 EPG サフィックス（New EPG Suffix）：このサフィックスは、Cisco ISE から学習された SGT に基づいて ACI で新規に作成された EPG に追加されます。
- [タグなしパケットの EEPG 名（EEPG name for untagged packets）]：EEPG に変換されない TrustSec パケットは、ACI でこの名前を使用してタグ付けされます。

ステップ 7 [保存（**Save**）] をクリックします。

ユーザ レポート別上位 N 個の RBACL ドロップの実行

ユーザ レポート別上位 N 個の RBACL ドロップを実行して、特定のユーザによるポリシー違反（パケット ドロップに基づく）を表示できます。

ステップ 1 [操作（Operations）] > [レポート（Reports）] > [TrustSec] を選択します。

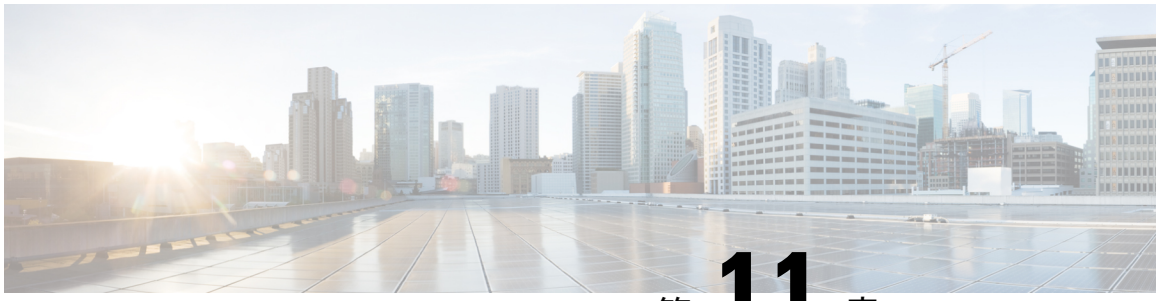
ステップ 2 [ユーザ別上位 N 個の RBACL ドロップ（Top N RBACL Drops by User）] をクリックします。

ステップ 3 [フィルタ（Filters）] ドロップダウン メニューから、必要なモニタ モードを追加します。

ステップ 4 選択したパラメータの値をこれに応じて入力します。[強制モード（Enforcement mode）] ドロップダウン リストから、[強制（Enforce）]、[モニタ（Monitor）]、または [両方（Both）] としてモードを指定できます。

ステップ 5 [時間範囲（Time Range）] ドロップダウン メニューから、レポート データを収集する期間を選択します。

ステップ 6 [実行（Run）] をクリックして、選択したパラメータとともに特定の期間のレポートを実行します。



第 11 章

コンプライアンス

ポスチャ サービス

ポスチャは、Cisco Identity Services Engine（Cisco ISE）のサービスです。ポスチャを使用すると、ネットワークに接続する前に、エンドポイントのコンプライアンス（ポスチャとも呼ばれる）をチェックできます。AnyConnect ISE ポスチャ エージェントなどのポスチャ エージェントは、エンドポイントで実行されます。クライアントプロビジョニングは、エンドポイントが適切なポスチャ エージェントを受信できるようにします。

Cisco ISE の ISE ポスチャ エージェントでは、以前のユーザと完全に切断されていないため、ネイティブ サプリカントを使用する場合は Windows のユーザの簡易切り替え機能がサポートされません。新しいユーザが送信されると、古いユーザのプロセスとセッション ID がエージェントによってハングされるため、新しいポスチャ セッションが開始できません。Microsoft のセキュリティ ポリシーに従い、ユーザの簡易切り替え機能を無効にすることを推奨します。

（注） ISE では、セッション制御は複数のノードで行われます。

MnT ノードでは、セッションは次の場合に削除されます。

- アカウンティングの開始があるのにアカウンティングの停止（古いセッション）がない場合、セッションは 5 日以内に削除されます。
- アカウンティングの停止後にアカウンティングの開始がある場合、セッションは数時間以内に削除されます。
- アカウンティングの開始または停止がない場合、セッションは数時間以内に削除されます。

PSN ノードでは、セッションは次の場合に削除されます。

- アカウンティングの停止を受信した場合。
- セッションキャッシュが消去された場合、特に多くのセッションがある場合、またはPSNをリロードした場合。

リダイレクトのないポスチャをマルチノード展開で使用し、セッションを適切に管理しないと、ポスチャ機能に影響する可能性があります。

ISE コミュニティ リソース

Configure ISE 2.1 and AnyConnect 4.3 Posture USB Check

How To Configure Posture with AnyConnect Compliance Module and ISE 2.0

ポスチャ サービスのコンポーネント

Cisco ISE ポスチャ サービスには、主にポスチャ管理サービスとポスチャ ランタイム サービスが含まれます。

ポスチャ管理サービス

Cisco ISE に APeX ライセンスをインストールしていない場合、ポスチャ管理サービス オプションは管理者ポータルから使用できません。

管理サービスは、ポスチャ サービス用に設定された要件および許可ポリシーに関連付けられた、ポスチャ固有のカスタム条件および修復アクションに対するバックエンドサポートを提供します。

ポスチャ ランタイム サービス

ポスチャ ランタイム サービスでは、ポスチャ評価およびクライアントの修復のためにクライアント エージェントと Cisco ISE サーバの間で実行されるすべての相互作用をカプセル化します。

ポスチャ ランタイム サービスは検出フェーズから開始します。エンドポイント セッションは、エンドポイントが 802.1x 認証に成功した後に作成されます。クライアント エージェントは、次の順序で各種の方式によって検出パケットを送信して Cisco ISE ノードへの接続を試行します。

1. HTTP 経由で Cisco ISE サーバのポート 80 へ（設定されている場合）
2. HTTPS 経由で Cisco ISE サーバのポート 8905 へ（設定されている場合）
3. HTTP 経由でデフォルト ゲートウェイのポート 80 へ
4. HTTPS 経由でポート 8905 からそれぞれ前にアクセスしたサーバへ
5. HTTP 経由で enroll.cisco.com のポート 80 へ

ポスチャ フェーズは、利用規定（存在する場合）が受け入れられると開始されます。Cisco ISE ノードはクライアント エージェントにポスチャ ドメインのポスチャ トークンを発行します。ポスチャ トークンにより、エンドポイントではポスチャ プロセスを再度実行せずにネットワークに再接続できます。これには、エージェント GUID、利用規定のステータス、エンドポイントのオペレーティング システム情報などの情報が含まれています。

ポスチャ フェーズで使用されるメッセージは、NEA PB/PA 形式（RFC5792）です。

ポスチャ タイプ

Cisco ISE ポスチャ ポリシーを監視および適用するために使用できる 3 つのポスチャ タイプがあります。

- AnyConnect：AnyConnect エージェントを展開し、クライアントとのやりとりが必要な Cisco ISE ポスチャ ポリシーを監視し、適用します。
- AnyConnect Stealth：ユーザの操作なしで、サービスとしてポスチャを実行します。
- Temporal Agent：クライアント上で実行するように Cisco ISE GUI で設定できる一時実行可能ファイル。クライアントが信頼ネットワークにアクセスしようとすると、Cisco ISE は、ユーザがクライアント上で実行する必要のある実行可能ファイルをプッシュします。Termporal Agent は、コンプライアンス ステータスを再び検査し、そのステータスを Cisco ISE に送信します。Cisco ISE は結果に基づいて必要なアクションを実行します。コンプライアンス処理が完了すると、クライアントから一時エージェントが削除されます。一時エージェントは、カスタム修復をサポートしていません。デフォルトの修復では、メッセージ テキストのみがサポートされます。

（注）

- [ポスチャ タイプ（Posture Types）] を [Temporal Agent]、[コンプライアンス モジュール（Compliance Module）] を [4.x 以降（4.x or later）] として、ポスチャ ポリシーを設定できます。このようなポリシーの修復と要件を作成する際は、コンプライアンス モジュールを「3.x 以前」または「任意のバージョン」に変更しないように注意してください。
- Termporal Agent の場合は、[要件（Requirements）] ページで [インストール（Installation）] チェック タイプを含むパッチ管理条件のみを表示できます。
- Cisco ISE は、Mac OSX 向け Temporal Agent を使用した VLAN 制御ポスチャ環境をサポートしていません。これは、ネットワーク アクセスを既存の VLAN から新しい VLAN に変更するときに、VLAN の変更前にユーザの IP アドレスを解放し、ユーザが新しい VLAN に接続するときに新しい IP アドレスを DHCP 経由で要求する必要があるためです。これにはルート権限が必要ですが、Temporal Agent はユーザ プロセスとして実行します。

  Cisco ISE は、エンドポイント IP アドレスの更新を必要としない ACL 制御のポスチャ環境をサポートしています。

Temporal Agent によってサポートされない条件：

- サービス条件 MAC：システム デーモン チェック
- サービス条件 MAC：デーモンまたはユーザ エージェント チェック
- PM：最新チェック
- PM：有効化チェック
- DE：暗号化チェック

[クライアント プロビジョニング（Client Provisioning）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]）と [ポスチャ要件（Posture Requirements）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]）に、ポスチャ タイプが含まれており、推奨されるベストプラクティスは、[クライアントプロビジョニング（Client Provisioning）]ページでポスチャ プロファイルをプロビジョニングすることです。

ポスチャ要件で AnyConnect ステルス ポスチャ タイプを選択すると、一部の条件、修復、または条件内の属性が無効になります（灰色表示）。たとえば、手動修復ではクライアント側のやりとりが必要となるため、AnyConnect ステルス要件を有効にすると、[手動修復タイプ（Manual Remediation Type）] が無効になります（灰色表示）。

AnyConnect ステルス モードの展開で、ポスチャ プロファイルを AnyConnect 設定にマッピングし、Anyconnect設定を[クライアントプロビジョニング（Client Provisioning）]ページにマッピングする場合、次の処理がサポートされます。

- AnyConnect によるポスチャ プロファイルの読み取りと必要なモードの設定
- 初回ポスチャ要求における AnyConnect による選択したモードに関する情報の Cisco ISE への送信
- Cisco ISEによるモードおよびその他の要因（ID グループ、OS、コンプライアンス モジュールなど）に基づく正しいポリシーの照合。

（注） AnyConnect バージョン 4.4 以降では、ステルス モードでの Cisco ISE ポスチャがサポートされています。

関連トピック

AnyConnect ステルス モードのワークフローの設定 （1253 ページ）
Cisco Temporal Agent のワークフローの設定 （1258 ページ）

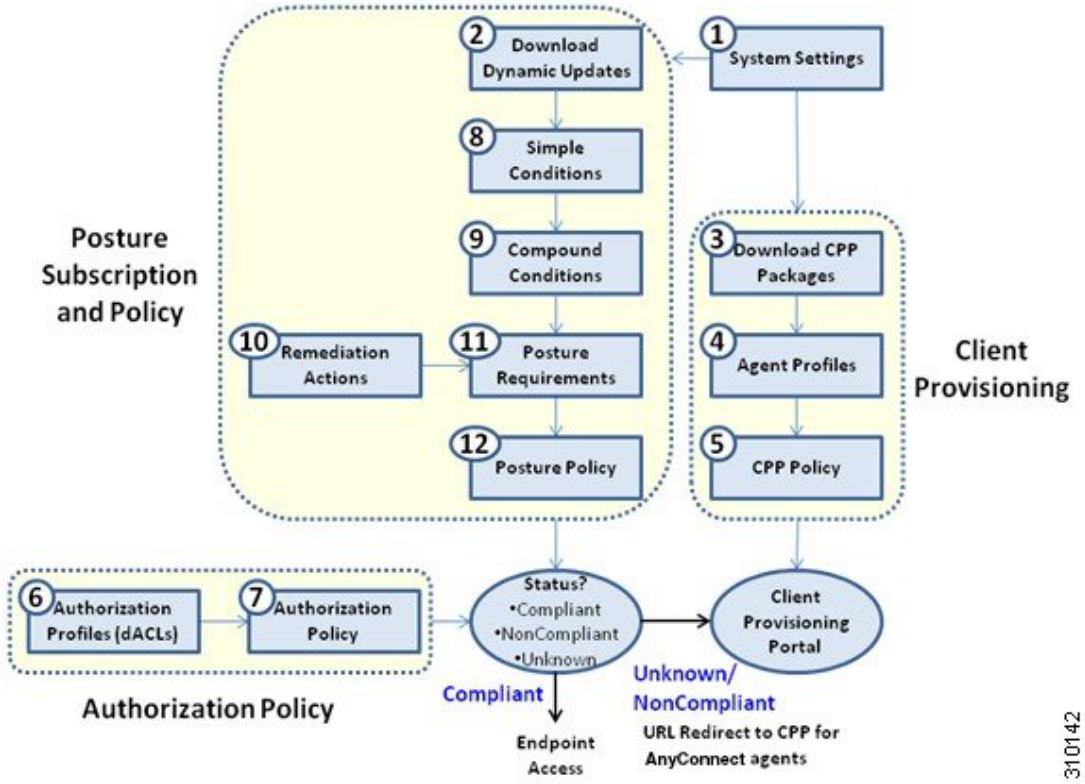
Cisco ISE ポスチャ エージェント

ポスチャ エージェントとは、Cisco ISE ネットワークにログインしているクライアント マシンに存在するアプリケーションです。クライアントがネットワークにログインしていない場合でも、エージェントは永続的にすることができ（AnyConnect と同様）、インストール後もクライアント マシンに残ります。エージェントは一時的にすることもでき（ や Windows および Mac OS 向けの Cisco Temporal Agent と同様）、ログイン セッション終了後にクライアント マシンから削除されます。いずれの場合も、エージェントはネットワークにログインし、適切なアクセスプロファイルを受け取り、クライアントマシンでポスチャ評価を実行してネットワークのコアにアクセスする前にネットワーク セキュリティ ガイドラインに従うようにします。

（注） Windows 向けの Cisco Temporal Agent は、クライアント プロビジョニング ポータルをサポートし、URL リダイレクションを使用します。

ポスチャおよびクライアントプロビジョニングポリシーワークフロー

図 *67 : Cisco ISE* のポスチャおよびクライアント プロビジョニング ポリシー ワークフロー



ポスチャ検出のステージ1では、すべてのディスカバリプローブが、ポスチャエージェントによって同時に実行されます。タイムアウト値は5秒です。ステージ2には2つのディスカバリプローブが含まれています。これにより、ポスチャモジュールはPSNへの接続を確立できます。このPSNへの接続は、リダイレクションがサポートされていない環境での認証をサポートしています。ステージ2では、すべてのプローブが連続しています。ステージ2に障害が発生した場合、ポスチャエージェントは再度ステージ1を試行します。このサイクルは30秒間継続します。その後、「ポリシーサーバが検出されません」と表示されます。この状態は、ディスカバリプローブがトリガーされるまで続きます。

ポスチャ サービス ライセンス

Cisco ISEは、Baseライセンス、Plusライセンス、APeXライセンスの3種類のライセンスを提供します。プライマリ PANで APeXライセンスをインストールしないと、ポスチャ要求はCisco ISEで実行されません。Cisco ISEのポスチャ サービスは、1つのノードまたは複数のノードで実行できます。

ポスチャ サービス展開

Cisco ISE は、スタンドアロン環境（単一ノード）または分散環境（複数ノード）に展開できます。

スタンドアロン Cisco ISE 展開では、単一のノードをすべての管理サービス、モニタリングとトラブルシューティング サービス、およびポリシー実行時サービスに設定できます。

分散 Cisco ISE 展開では、各ノードを、管理サービス、モニタリングとトラブルシューティング サービス、およびポリシー実行時サービスの Cisco ISE ノードとして設定できます。管理サービスを実行しているノードは、Cisco ISE 展開内のプライマリ ノードです。他のサービスを実行している他のノードは、互いのバックアップ サービス用に設定できるセカンダリ ノードです。

Cisco ISE でのポスチャ セッション サービスの有効化

始める前に

- クライアントから受信したすべてのポスチャ要求に対応するには、Cisco ISE でセッション サービスを有効にし、拡張ライセンス パッケージをインストールする必要があります。
- 分散展開に複数のノードを登録している場合は、登録したすべてのノードがプライマリ ノードとは別に [展開ノード（Deployment Nodes）] ページに表示されます。各ノードを Cisco ISE ノード（管理ペルソナ、ポリシー サービス ペルソナ、およびモニタリング ペルソナ）として設定できます。
- ポスチャ サービスは、ポリシー サービス ペルソナを担当する Cisco ISE ノードでのみ実行され、分散展開で管理ペルソナとモニタリング ペルソナを担当する Cisco ISE ノードでは実行されません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [展開（Deployment）]** を選択します。

ステップ 2 [展開ノード（Deployment Nodes）] ウィンドウから Cisco ISE ノードを選択します。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 [全般設定（General Settings）] タブで [ポリシーサービス（Policy Service）] チェックボックスをオンにします。

[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 ポリシーサービス ペルソナでネットワーク アクセス、ポスチャ、ゲスト、およびクライアント プロビジョニングのセッション サービスを実行するには、[セッション サービスの有効化（Enable Session Services）] チェックボックスをオンにします。セッション サービスを停止するには、このチェックボックスをオフにします。

ステップ 6 **[保存（Save）]** をクリックします。

ポスチャ評価レポートの実行

ポスチャの詳細な評価を実行して、ポスチャ評価中に使用されるポスチャ ポリシーに対するクライアントのコンプライアンスの詳細なステータスを生成できます。

ステップ 1 **[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [エンドポイントとユーザ（Endpoints and Users）] > [ポスチャの詳細な評価（Posture Detail Assessment）]** を選択します。

ステップ 2 [時間範囲（Time Range）] ドロップダウン リストから特定の期間を選択します。

ステップ 3 [実行（Run）] をクリックして、選択した期間中にアクティブだったすべてのエンド ポイントの概要を表示します。

ポスチャ管理の設定

ポスチャ サービス用の管理者ポータルをグローバルに設定できます。シスコから Web 経由で自動的に Cisco ISE サーバに更新をダウンロードできます。また、オフラインで、後で、Cisco ISE を手動で更新することもできます。さらに、クライアントに AnyConnect、NAC Agent、Web Agent などのエージェントがインストールされていると、クライアントにポスチャ評価および修復サービスが提供されます。クライアント エージェントは、Cisco ISE に対してクライアントのコンプライアンス ステータスを定期的に更新します。ログインおよびポスチャの要件評価が正常に完了した後、ネットワーク使用の利用規約への準拠をエンドユーザに求めるリンクが示されたダイアログがクライアント エージェントに表示されます。このリンクを使用して、エンドユーザがネットワークへのアクセス権を取得する前に同意する、企業ネットワークのネットワーク使用情報を定義できます。

クライアントのポスチャ要件

ポスチャの要件を作成するには、次の手順を実行します。

1. [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）] を選択します。
2. 要件行の末尾にある [編集（Edit）] ドロップダウンリストから、[新しい要件の挿入（Insert New Requirement）] を選択します。
3. 必要な詳細を入力し、[完了（Done）] をクリックします。

次の表に、[クライアントのポスチャ要件（Client Posture Requirements）] ページのフィールドを示します。

表 *146* : ポスチャ要件

フィールド名	使用上のガイドライン
[名前（Name）]	要件の名前を入力します。
オペレーティング システム	オペレーティング システムを選択します。 プラス記号 [+] をクリックして、複数のオペレーティング システムをポリシーに関連付けます。 マイナス記号 [-] をクリックして、ポリシーからオペレーティング システムを削除します。
コンプライアンス モジュール	[準拠モジュール（Compliance Module）] ドロップダウンリストから必要な準拠モジュールを選択します。 • 4.x 以降（4.x or Later）：マルウェア対策、ディスク暗号化、Patch Management、および USB の各種条件をサポートします。 • 3.x 以前（3.x or Earlier）：ウイルス対策、スパイウェア対策、ディスク暗号化、およびパッチ管理の各種条件をサポートします • すべてのバージョン（Any Version）：ファイル、サービス、レジストリ、アプリケーション、および複合の各種条件をサポートします。 コンプライアンスモジュールの詳細については、コンプライアンス モジュール（1194 ページ）を参照してください。

フィールド名	使用上のガイドライン
ポスチャタイプ	[ポスチャタイプ（Posture Type）] ドロップダウンリストから、必要なポスチャタイプを選択します。 • [AnyConnect]：AnyConnect エージェントを展開し、クライアントとのやり取りが必要な Cisco ISE ポリシーを監視し、適用します。 • [AnyConnect ステルス（AnyConnect Stealth）]：AnyConnect エージェントを展開し、クライアントとやり取りしない Cisco ISE ポスチャポリシーを監視し、適用します。 • [Temporal Agent]：コンプライアンス ステータスを確認するためにクライアント上で実行される一時実行可能ファイル。
条件（**Conditions**）	リストから条件を選択します。 [操作（Action）] アイコンをクリックして、ユーザ定義の条件を作成して、要件に関連付けることもできます。ユーザ定義の条件を作成中に関連する親オペレーティング システムは編集できません。 pr_WSUSRule は、Windows Server Update Services（WSUS）修復が関連付けられているポスチャ要件で使用される、ダミーの複合条件です。関連 WSUS 修復アクションは、重大度レベル オプションを使用して Windows Updates を検証するように設定する必要があります。この要件が失敗すると、Windows クライアントにインストールされている NAC Agent は、WSUS 修復で定義した重大度レベルに基づいて WSUS 修復アクションを適用します。 pr_WSUSRule は複合条件のリストページには表示できません。条件ウィジェットからのみ pr_WSUSRule を選択できます。

フィールド名	使用上のガイドライン
修復アクション（Remediation Actions）	リストから修復を選択します。 修復アクションを作成して、要件に関連付けることもできます。 Agentユーザとの通信に使用できるすべての修復タイプのテキスト ボックスがあります。修復アクションに加えて、クライアントの非準拠に関してメッセージで Agent ユーザと通信することができます。 [メッセージ テキストのみ（Message Text Only）] オプションで Agent ユーザに非準拠について通知します。また、詳細情報を得るためにヘルプ デスクに連絡したり、クライアントを手動で修復したりするオプションの手順がユーザに提供されています。このシナリオでは、NAC Agentは修復アクションをトリガーしません。

関連トピック

ポスチャ評価の利用規定の設定 （1188 ページ）
クライアントのポスチャ要件の作成 （1249 ページ）

クライアントのタイマー設定

ユーザが修復するためのタイマー、あるステータスから別のステータスに移行するためのタイマー、およびログイン成功画面を制御するためのタイマーをセットアップできます。

エージェントプロファイルを設定して、修復タイマー、ネットワーク遷移遅延タイマー、およびクライアントマシン上でログイン成功画面を制御するために使用するタイマー制御し、これらの設定がポリシーベースになるようにすることを推奨します。**[NAC または AnyConnect ポスチャプロファイル（NAC or AnyConnect Posture Profile）]** ウィンドウ（**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアントのプロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** > **[追加（Add）]** > **[NAC または AnyConnect ポスチャプロファイル（NAC or AnyConnect Posture Profile）]** のクライアントのプロビジョニングリソースのエージェントのすべてのタイマーを設定できます。

しかし、クライアント プロビジョニング ポリシーに一致するように設定されたエージェントプロファイルがない場合、[全般設定（General Settings）] の設定ウィンドウ（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]**）の設定を使用できます。

指定した時間内で修復するためのクライアントの修復タイマーの設定

指定した時間内にクライアントを修復するためのタイマーを設定できます。最初の評価時にクライアントが設定されたポスチャ ポリシーを満たすことに失敗した場合、エージェントは修復タイマーに設定された時間内にクライアントが修復するのを待ちます。クライアントがこの指定時間内の修復に失敗すると、クライアント エージェントはポスチャ ランタイム サービスにレポートを送信します。その後、クライアントは非準拠ステートに移行されます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [修復タイマー（Remediation Timer）] フィールドに、分単位で時間の値を入力します。

デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。

ステップ 3 [**保存（Save**）] をクリックします。

クライアントの遷移のためのネットワーク遷移遅延タイマーの設定

ネットワーク遷移遅延タイマーを使用して、指定した時間内に、クライアントがある状態から別の状態に遷移するためのタイマーを設定できます。これは、許可変更（CoA）が完了するために必要となります。ポスチャの成功時と失敗時にクライアントが新しい VLAN の IP アドレスを取得するための時間がかかる場合は、より長い遅延時間が必要になることがあります。クライアントが正常にポスチャされると、Cisco ISE は、ネットワーク遷移遅延タイマーで指定された時間内に未知から準拠モードへ移行することを許可します。ポスチャに失敗すると、Cisco ISE は、タイマーで指定された時間内にクライアントが未知から非準拠モードへ移行することを許可します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [ネットワーク遷移遅延（Network Transition Delay）] フィールドに時間値を秒単位で入力します。

デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。

ステップ 3 [**保存（Save**）] をクリックします。

ログイン成功ウィンドウを自動的に閉じる設定

ポスチャ評価が正常に完了した後、クライアント エージェントは一時的なネットワーク アクセス画面を表示します。ユーザはログイン ウィンドウで [OK] ボタンをクリックして、この画面を閉じる必要があります。指定した時間の経過後にこのログイン画面を自動的に閉じるタイマーを設定できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）] チェックボックスをオンにします。

ステップ 3 [経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）] チェックボックスの横のフィールドに時間値を秒単位で入力します。

有効な値の範囲は 0 ～ 300 秒です。時間をゼロに設定すると、AnyConnect はログイン成功画面を表示しません。

ステップ 4 [保存（Save）] をクリックします。

非エージェント デバイスへのポスチャ ステータスの設定

Linux または iDevice などの非エージェント デバイスで実行されるエンドポイントのポスチャ ステータスを設定できます。Android デバイスおよび iPod、iPhone、iPad などの Apple の iDevice が Cisco ISE 対応ネットワークに接続する場合、これらのデバイスはデフォルト ポスチャ ステータスの設定を引き継ぎます。

これらの設定は、ポスチャのランタイム中に一致するポリシーが見つからない場合、Windows および Macintosh オペレーティング システムで実行されるエンドポイントにも適用されます。

始める前に

エンドポイントにポリシーを適用するには、対応するクライアント プロビジョニング ポリシー（エージェントのインストール パッケージ）を設定する必要があります。そうしないと、エンドポイントのポスチャ ステータスは自動的にデフォルト設定が反映されます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** を選択します。

ステップ 2 [デフォルトポスチャステータス（Default Posture Status）] ドロップダウン リストから、オプションに [準拠（Compliant）] または [非準拠（Noncompliant）] を選択します。

ステップ 3 [保存（Save）] をクリックします。

ポスチャのリース

ユーザがネットワークにログインするたびにポスチャ評価を実行したり、指定した間隔でポスチャ評価を実行したりするよう Cisco ISE を設定できます。有効な範囲は 1 ～ 365 日です。

この設定は、ポスチャ評価に AnyConnect エージェントを使用するユーザだけに適用されます。

ポスチャ リースがアクティブな場合、Cisco ISE は最新の既知のポスチャを使用しますが、コンプライアンスの確認のためにエンドポイントに接続しません。ただし、ポスチャ リースが期限切れになると、Cisco ISE はエンドポイントの再認証またはポスチャ再評価を自動的にトリガーしません。同じセッションが使用されているため、エンドポイントは同じコンプライアンス状態のままになります。エンドポイントが再認証されると、ポスチャが実行され、ポスチャ リース時間がリセットされます。

使用例のシナリオ

- ユーザはエンドポイントにログオンし、1 日に設定されているポスチャ リースにポスチャ準拠させます。
- ユーザは4時間後にエンドポイントからログオフします（この時点で、ポスチャ リースは 20 時間残っています）。
- ユーザは 1 時間後に再度ログオンします。この時点で、ポスチャ リースは 19 時間残っています。最新の既知のポスチャ状態は準拠状態でした。したがって、エンドポイントでポスチャが実行されることなく、ユーザにアクセス権が付与されます。
- ユーザは 4 時間後にログオフします（この時点で、ポスチャ リースは 15 時間残っています）。
- ユーザは 14 時間後にログオンします。ポスチャ リースは 1 時間残っています。最新の既知のポスチャ状態は準拠状態でした。エンドポイントでポスチャが実行されることなく、ユーザにアクセス権が付与されます。
- 1 時間後、ポスチャ リースは期限切れになります。同じユーザ セッションが使用されているため、ユーザは引き続きネットワークに接続されています。
- 1 時間後、ユーザはログオフします（セッションはユーザに関連付けられていますが、マシンには関連付けられていないため、マシンはネットワーク上に留まることができます）。
- 1 時間後、ユーザはログオンします。ポスチャ リースが期限切れになり、新しいユーザ セッションが開始されるため、マシンはポスチャアセスメントを実行し、その結果がCisco ISE に送信され、ポスチャ リース時間が 1 日にリセットされます（この使用例の場合）。

定期的再評価

定期的再評価（PRA）は、コンプライアンスについてすでに適切にポスチャされているクライアントにのみ実行できます。PRA は、クライアントがネットワーク上で準拠していない場合には実行されません。

PRA は、エンドポイントが準拠ステートになっている場合にのみ有効であり、適用可能です。ポリシー サービス ノードは関連するポリシーを調べ、設定で定義されているクライアント ロールに応じて要件をコンパイルし、PRA を適用します。PRA 設定の一致が見つかった場合、ポリシー サービス ノードは、クライアントの PRA 設定で定義されている PRA 属性を使用して、クライアント エージェントに応答してから、CoA 要求を発行します。クライアント エージェントは、設定に指定された間隔に基づいて定期的に PRA 要求を送信します。PRA が成功した場合、または、PRA 設定に指定されているアクションが続行になっている場合、クライアント

は準拠ステートのままになります。クライアントが PRA を満たしていない場合、準拠ステートから非準拠ステートに移行します。

PostureStatus 属性は、ポスチャ再評価要求の場合でも、PRA 要求で現在のポスチャ ステータスを不明ではなく準拠と示します。PostureStatus はモニタリング レポートでも更新されます。

ポスチャのリースが有効期限内の場合、アクセス コントロール リスト（ACL）に基づいてエンドポイントが準拠し、PRA が開始されます。PRA が失敗すると、エンドポイントが非準拠になり、ポスチャのリースがリセットされます。

定期的再評価の設定

コンプライアンスに対してすでに正常にポスチャされているクライアントだけの定期的な再評価を設定できます。システムで定義されているユーザ ID グループに各 PRA を設定できます。

始める前に

- 各 PRA 設定に、一意のグループ、または設定に割り当てられているユーザ ID グループの一意の組み合わせがあることを確認します。
- 2 つの一意のロールである role_test_1 および role_test_2 を PRA 設定に割り当てることができます。論理演算子とこれら 2 つのロールを組み合わせ、2 つのロールの一意の組み合わせとして PRA 設定に割り当てることができます。たとえば、role_test_1 OR role_test_2 とします。
- 2 つの PRA 設定に共通のユーザ ID グループがないことを確認します。
- PRA 設定がユーザ ID グループ「Any」にすでに存在する場合、次のことを実行しないと、他の PRA 設定を作成できません。
  - *Any* 以外のユーザ ID グループを反映するように、任意のユーザ ID グループで既存の PRA 設定を更新します。
  - ユーザ ID グループ「*Any*」の既存の PRA 設定を削除します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 新しい PRA を作成するには、[新規再評価の設定（New Reassessment Configuration）] ページで値を変更します。

ステップ 4 [送信（Submit）] をクリックして、PRA 設定を作成します。

ポスチャのトラブルシューティングの設定

次の表では、ネットワーク内のポスチャ問題の検出と解決に使用する [ポスチャのトラブルシューティング（Posture troubleshooting）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ポスチャのトラブルシューティング（Posture Troubleshooting）]** です。

表 *147 :* ポスチャのトラブルシューティングの設定

オプション	使用上のガイドライン
トラブルシューティングが必要なポスチャ イベントの検索と選択	
[ユーザ名（Username）]	フィルタリング基準として使用するユーザ名を入力します。
MAC アドレス（MAC Address）	フィルタリング基準として使用する MAC アドレスを、xx-xx-xx-xx-xx-xx 形式で入力します。
ポスチャ ステータス（Posture Status）	フィルタリング基準として使用する認証ステータスを選択します。
失敗の理由（Failure Reason）	失敗理由を入力するか、または [選択（Select）] をクリックしてリストから失敗理由を選択します。失敗理由をクリアするには、[クリア（Clear）] をクリックします。
時間範囲（Time Range）	時間範囲を選択します。この時間範囲に作成された RADIUS 認証レコードが使用されます。
開始日時：（Start Date-Time:）	（[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合にのみ使用可能）開始日時を入力するか、またはカレンダ アイコンをクリックして開始日時を選択します。日付は *mm/dd/yyyy* 形式、時刻は *hh:mm* 形式である必要があります。
終了日時：（End Date-Time:）	（[時間範囲（Time Range）] として [カスタム（Custom）] を選択した場合にのみ使用可能）終了日時を入力するか、またはカレンダ アイコンをクリックして終了日時を選択します。日付は *mm/dd/yyyy* 形式、時刻は *hh:mm* 形式である必要があります。
レコード数の取得（Fetch Number of Records）	表示するレコードの数を選択します。10、20、50、100、200、または 500 を選択できます。
検索結果	

オプション	使用上のガイドライン
時刻（Time）	イベントの時刻
ステータス	ポスチャ ステータス
[ユーザ名（Username）]	イベントに関連付けられたユーザ名
MAC アドレス（MAC Address）	システムの MAC アドレス
失敗の理由（Failure Reason）	イベントの障害理由

関連トピック

エンドポイント ポスチャの障害のトラブルシューティング （1579 ページ）
ポスチャのトラブルシューティング ツール （1261 ページ）

ポスチャの全般設定

次の表では、修復時間およびポスチャ ステータスなどの一般的なポスチャ設定を行うために使用できる [ポスチャの全般設定（Posture General Settings）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]** です。

表 *148* : ポスチャの全般設定

フィールド	使用上のガイドライン
修復タイマー（Remediation Timer）	分単位で時間値を入力します。デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。
ネットワーク遷移遅延（Network Transition Delay）	秒単位で時間値を入力します。デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。
デフォルトのポスチャ ステータス（Default Posture Status）	準拠または非準拠を選択します。Linux のような非エージェント デバイスは、ネットワークに接続している間、このステータスを想定します。

フィールド	使用上のガイドライン
一定時間（秒）経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）	このチェックボックスをオンにすると、指定された時間後に、ログイン成功画面が自動的に閉じます。 チェックボックスの隣のフィールドに、時間値を秒単位で入力します。 0 ～ 300 秒にログイン画面が自動的に閉じるようにタイマーを設定できます。時間をゼロに設定した場合は、クライアント上のエージェントはログイン成功画面を表示しません。
連続モニタリング間隔（Continuous Monitoring Interval）	AnyConnect がモニタリング データの送信を開始するまでの時間間隔を指定します。アプリケーション条件の場合アプリケーションおよびハードウェア条件の場合、デフォルト値は 5 分です。
ステルス モードでの利用規約（Acceptable Use Policy in Stealth Mode）	会社のネットワーク使用条件が満たされていない場合、ステルス モードで [ブロック（Block）] を選択して、クライアントを非準拠ポスチャ ステータスに移行します。
ポスチャのリース	
ユーザがネットワークに接続するたびにポスチャ評価を行う（Perform posture assessment every time a user connects to the network）	ユーザがネットワークに接続するたびにポスチャ評価を開始するには、このオプションを選択します。
n 日おきにポスチャ評価を行う（Perform posture assessment every n days）	クライアントがすでにポスチャ準拠であるものの、指定された日数が経過したら、ポスチャ評価を開始する場合は、このオプションを選択します。
最後の既知の良い状態をキャッシュする（Cache Last Known Good State）	ポスチャ評価の結果をキャッシュするには、Cisco ISE のこのチェックボックスをオンにします。デフォルトでは、このフィールドは無効です。
最後の既知の良い状態（Last Known Good State）	[最後の既知の良い状態をキャッシュする（Cache Last Known Good State）] チェックボックスをオンにしている場合のみ該当します。Cisco ISE は、このフィールドに指定した期間にわたり、ポスチャ評価の結果をキャッシュします。有効な値は、1 ～ 30 日、1 ～ 720 時間、または 1 ～ 43200 分です。

関連トピック

ポスチャ サービス （1166 ページ）
ポスチャ管理の設定 （1173 ページ）
ポスチャのリース （1178 ページ）
Cisco ISE でのポスチャ セッション サービスの有効化 （1172 ページ）
指定した時間内で修復するためのクライアントの修復タイマーの設定 （1177 ページ）
クライアントの遷移のためのネットワーク遷移遅延タイマーの設定 （1177 ページ）
ログイン成功ウィンドウを自動的に閉じる設定 （1177 ページ）
非エージェント デバイスへのポスチャ ステータスの設定 （1178 ページ）

Cisco ISE へのポスチャ更新のダウンロード

ポスチャ更新には、Windows および Macintosh オペレーティング システムの両方のアンチウイルスとアンチスパイウェアの一連の事前定義済みのチェック、ルール、サポート表、およびシスコでサポートされるオペレーティング システム情報が含まれます。また、ローカル ファイル システムの更新の最新のアーカイブを含むファイルから Cisco ISE をオフラインで更新することもできます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。通常、このプロセスには約 20 分かかります。初回ダウンロード後に、差分更新が自動的にダウンロードされるように Cisco ISE を設定できます。

Cisco ISE では、初回ポスチャ更新時に 1 回のみ、デフォルトのポスチャ ポリシー、要件、および修復を作成します。それらを削除した場合、Cisco ISE は後続の手動またはスケジュールされた更新中にこれらを再作成しません。

始める前に

ポスチャ リソースを Cisco ISE にダウンロードできる適切なリモート ロケーションにアクセスできるようにするには、5-2 ページの「Cisco ISE でのプロキシ設定の指定」の説明に従ってネットワークにプロキシが正しく設定されていることを確認する必要がある場合があります。

[ポスチャ更新（Posture Update）] ページを使用して、Web から更新を動的にダウンロードできます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]** を選択します。

ステップ 2 [Web] オプションを選択して、更新を動的にダウンロードします。

ステップ 3 [デフォルトに設定（Set to Default）] をクリックして、[フィードURLの更新（Update Feed URL）] フィールドにシスコのデフォルト値を設定します。

ネットワークで URL リダイレクション機能（プロキシ サーバ経由など）を制限しているために、上記の URL へのアクセスに問題がある場合は、Cisco ISE で関連トピックの代替 URL を指定してください。

ステップ 4 [ポスチャ更新（Posture Updates）] ページの値を変更します。

ステップ 5 シスコからの更新をダウンロードするには、[今すぐ更新（Update Now）] をクリックします。

更新された後、[ポスチャ更新（Posture Updates）] ページに、[ポスチャ更新（Posture Updates）] ページの [更新情報（Update Information）] セクションの更新の確認として現在のシスコ更新のバージョン情報が表示されます。

ステップ 6 [はい（Yes）] をクリックして続行します。

ポスチャ更新の自動ダウンロード

最初の更新後に、更新を確認し、自動的にダウンロードするようにCisco ISEを設定できます。

始める前に

- 最初にポスチャ更新をダウンロードして、更新を確認し、自動的にダウンロードするように Cisco ISE を設定しておく必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）]** を選択します。

ステップ 2 [ポスチャ更新（Posture Updates）] ページで [初期遅延から開始される更新の自動確認（Automatically check for updates starting from initial delay）] チェックボックスをオンにします。

ステップ 3 初期遅延時間を hh:mm:ss の形式で入力します。

Cisco ISE は、初期遅延時間の終了後に確認を開始します。

ステップ 4 時間間隔を時間単位で入力します。

Cisco ISE は初期遅延時間から指定した間隔で、展開に更新をダウンロードします。

ステップ 5 [保存（**Save**）] をクリックします。

ポスチャの利用規定の構成設定

次の表では、ポスチャのアクセプタブルユースポリシーを設定するために使用できるポスチャの [利用規定設定（Acceptable Use Policy Configurations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [利用規定（Acceptable Use Policy）]** です。

表 *149* : ポスチャ *AUP* の設定

フィールド	使用上のガイドライン
構成名	ユーザが作成する AUP 設定の名前を入力します。
設定の説明（Configuration Description）	ユーザが作成する AUP 設定の説明を入力します。
エージェントユーザへの AUP の表示（Windows の場合のみ）	オンにした場合、[エージェントユーザへの AUP の表示（Show AUP to Agent users）] チェックボックスはユーザ（Windows のみ）にネットワークの利用規約へのリンクを表示し、それをクリックすると、認証およびポスチャ評価が成功したときに AUP が表示されます。
AUP メッセージの URL を使用（Use URL for AUP message）オプション ボタン	選択した場合、認証およびポスチャ評価が成功したときにクライアントがアクセスする必要がある AUP メッセージへの URL を AUP URL に入力する必要があります。
AUP メッセージのファイルを使用（Use file for AUP message）オプション ボタン	選択した場合、場所を参照し、トップ レベルに index.html を含む AUP ファイルにジップ形式のファイルをアップロードします。 .zip ファイルには、index.html ファイルに加えて、他のファイルおよびサブディレクトリを含めることができます。これらのファイルは、HTML タグを使用して相互に参照できます。
AUP URL	クライアントは認証およびポスチャ評価が成功したときにアクセスする必要がある AUP への URL を入力します。
AUP ファイル（AUP File）	[AUP ファイル（AUP File）] で、ファイルを参照し、Cisco ISE サーバにアップロードします。これは zip 形式のファイルで、zip 形式のファイルではトップ レベルに index.html ファイルを含める必要があります。

フィールド	使用上のガイドライン
ユーザ ID グループの選択（Select User Identity Groups）	[ユーザ ID グループの選択（Select User Identity Groups）] ドロップダウン リストで、AUP 設定の一意のユーザ ID グループまたはユーザ ID グループの一意の組み合わせを選択します。 AUP 設定を作成する場合は、次の点に注意してください。 • ポスチャ AUP は、ゲスト フローには適用できません。 • 各設定には、一意のユーザ ID グループ、またはユーザ ID グループの一意の組み合わせが必要です。 • 2 つの設定が共通のユーザ ID グループを持つことはできません。 • ユーザ ID グループ「Any」で AUP 設定を作成する場合は、まず他のすべての AUP 設定を削除します。 • ユーザ ID グループ「Any」を使用して AUP 設定を作成した場合、一意のユーザ ID グループ、または複数のユーザ ID グループを使用して他の AUP 設定を作成することはできません。Any 以外のユーザ ID グループを使用して AUP 設定を作成するには、最初にユーザ ID グループ「Any」を使用した既存の AUP 設定を削除するか、ユーザ ID グループ「Any」を使用した既存の AUP 設定を一意のユーザ ID グループまたは複数のユーザの ID グループを使用して更新します。
利用規定設定 - 設定リスト（Acceptable use policy configurations—Configurations list）	既存の AUP 設定と AUP 設定に関連付けられたエンドユーザ ID グループを一覧表示します。

関連トピック

ポスチャ サービス （1166 ページ）
ポスチャ評価の利用規定の設定 （1188 ページ）

ポスチャ評価の利用規定の設定

ログインし、クライアントのポスチャ評価が成功すると、クライアントエージェントにより一時的なネットワークアクセス画面が表示されます。この画面には、利用規定（AUP）へのリンクが含まれています。ユーザがリンクをクリックすると、ネットワーク利用条件を表示するページにリダイレクトされます。その条件を読み、同意する必要があります。

各利用規定設定には、一意のユーザ ID グループ、またはユーザ ID グループの一意の組み合わせが必要です。Cisco ISE は最初に一致したユーザ ID グループの AUP を見つけ、AUP を表示するクライアント エージェントと通信します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [利用規定（Acceptable Use Policy）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [新規利用規定設定（New Acceptable Use Policy Configuration）] ページで値を変更します。

ステップ 4 [送信（Submit）] をクリックします。

ポスチャ条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの 1 つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

ネットワークに Cisco ISE を初めて展開する場合は、Web からポスチャ更新をダウンロードできます。このプロセスは、初期ポスチャ更新と呼ばれます。

初期ポスチャ更新の後、Cisco ISE はシスコ定義の単純および複合条件も作成します。シスコ定義の単純条件はプレフィクスとして pc_ が付けられ、複合条件はプレフィクスとして pr_ が付けられています。

ダイナミック ポスチャ更新の結果としてシスコ定義の条件を Web を介してダウンロードするように Cisco ISE を設定することもできます。シスコ定義のポスチャ条件を削除または編集することはできません。

ユーザ定義の条件やシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

単純ポスチャ条件

[ポスチャナビゲーション（Posture Navigation）] ペインを使用して、次の単純条件を管理できます。

- ファイル条件：ファイルの存在、ファイルの日付、およびクライアントのファイル バージョンを確認する条件。
- レジストリ条件：レジストリ キーの存在またはクライアントのレジストリ キーの値を確認する条件。
- アプリケーション条件：アプリケーションまたはプロセスがクライアント上で実行されているかまたは実行されていないかを確認する条件。

（注） プロセスがインストールされ実行されている場合、ユーザは準拠します。ただし、アプリケーション条件が逆ロジックで動作している場合は、アプリケーションがインストールされておらず実行されていなくも、エンドユーザは準拠します。アプリケーションがインストールされ実行されている場合、エンドユーザは準拠しません。

- サービス条件：サービスがクライアント上で実行されているかまたは実行されていないかを確認する条件。
- ディクショナリ条件：ディクショナリ属性と値を確認する条件。
- USB 条件：USB マス ストレージ デバイスの有無をチェックする条件。

単純ポスチャ条件の作成

ポスチャ ポリシーまたは他の複合条件で使用できる、ファイル、レジストリ、アプリケーション、サービス、およびディクショナリ単純条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]** を選択します。

ステップ 2 [ファイル（File）]、[レジストリ（Registry）]、[アプリケーション（Application）]、[サービス（Service）]、または [ディクショナリ単純条件（Dictionary Simple Condition）] のいずれかを選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 フィールドに適切な値を入力します。

ステップ 5 [送信（Submit）] をクリックします。

複合ポスチャ条件

複合条件は、1つ以上の単純条件、または複合条件で構成されます。ポスチャ ポリシーを定義する場合、次の複合条件を使用できます。

- 複合条件：1 つ以上の単純条件、またはタイプがファイル、レジストリ、アプリケーション、またはサービス条件の複合条件が含まれます
- アンチウイルス複合条件：1 つ以上の AV 条件、または AV 複合条件が含まれます
- アンチスパイウェア複合条件：1 つ以上の AS 条件、または AS 複合条件が含まれます
- ディクショナリ複合条件：1 つ以上のディクショナリ単純条件またはディクショナリ複合条件が含まれます
- マルウェア対策条件：1 つ以上の AM 条件が含まれます

ディクショナリ複合条件の設定

次の表に、[ディクショナリ複合条件（Dictionary Compound Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[ディクショナリ複合条件（Dictionary Compound Conditions）]** です。

表 *150 :* ディクショナリ複合条件の設定

フィールド名	使用上のガイドライン
[名前（Name）]	作成するディクショナリ複合条件の名前を入力します。
説明	作成するディクショナリ複合条件の説明を入力します。
既存の条件をライブラリから選択（Select Existing Condition from Library）	ポリシー要素ライブラリから事前定義済みの条件を選択して式を定義するか、または後のステップでアドホック属性/値のペアを式に追加します。
条件名（Condition Name）	ポリシー要素ライブラリからすでに作成しているディクショナリ単純条件を選択します。
式（Expression）	[条件名（Condition Name）] ドロップダウンリストでの選択に基づいて式が更新されます。

フィールド名	使用上のガイドライン
AND または OR 演算子（AND or OR operator）	ライブラリから追加できるディクショナリ単純条件を論理的に組み合わせるには、AND または OR 演算子を選択します。 次の操作を行うには、[操作（Action）]アイコンをクリックします。 • 属性/値の追加（Add Attribute/Value） • ライブラリから条件を追加（Add Condition from Library） • 削除（Delete）
新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）	さまざまなシステムディクショナリまたはユーザ定義ディクショナリから属性を選択します。 後のステップで事前定義された条件をポリシー要素ライブラリから追加することもできます。
条件名（Condition Name）	すでに作成したディクショナリ単純条件を選択します。
式（Expression）	[式（Expression）] ドロップダウン リストから、ディクショナリ単純条件を作成できます。
演算子	属性に値を関連付ける演算子を選択します。
値	ディクショナリ属性に関連付ける値を入力するか、またはドロップダウン リストから値を選択します。

関連トピック

ディクショナリおよびディクショナリ属性
単純条件と複合条件
複合ポスチャ条件 （1190 ページ）
複合ポスチャ条件の作成 （1196 ページ）

Windows クライアントでの自動アップデートを有効にするための事前定義の条件

pr_AutoUpdateCheck_Rule はシスコによって事前定義された条件であり、[複合条件（Compound Conditions）]ページにダウンロードされます。この条件を使用すると、Windows クライアント上で自動アップデート機能が有効になっているかどうかを確認することができます。Windows

クライアントがこの要件を満たさない場合、ネットワークアクセスコントロール（NAC）エージェントによって、Windowsクライアントの自動アップデート機能が強制的に有効になります（修復）。この修復後、Windowsクライアントはポスチャ準拠になります。自動アップデート機能がWindowsクライアント上で有効になっていない場合は、ポスチャポリシーで関連付けたWindows Update修復でWindows管理者設定を上書きします。

事前設定済みアンチウイルスおよびアンチスパイウェア条件

Cisco ISEの[AV複合条件（AV Compound Condition）]および[AS複合条件（AS Compound Condition）]ページには、アンチウイルスとアンチスパイウェアの事前設定済みの複合条件がロードされます。これらの条件は、WindowsおよびMacintoshオペレーティングシステムのアンチウイルスおよびアンチスパイウェアサポート表で定義されます。これらの複合条件では、指定されたアンチウイルスとアンチスパイウェア製品がすべてのクライアント上に存在するかどうかを確認できます。Cisco ISEで新しいアンチウイルスとアンチスパイウェアの複合条件を作成することもできます。

アンチウイルスとアンチスパイウェア サポート表

Cisco ISEは、各ベンダー製品の最新バージョンおよび定義ファイルの日付を提供するアンチウイルスとアンチスパイウェアサポート表を使用します。ユーザは頻繁にアンチウイルスとアンチスパイウェアサポート表をポーリングする必要があります。アンチウイルスとアンチスパイウェアのベンダーはアンチウイルスとアンチスパイウェア定義ファイルを頻繁に更新するため、各ベンダー製品の最新バージョンおよび定義ファイルの日付を検索します。

新しいアンチウイルスとアンチスパイウェアのベンダー、製品、リリースのサポートを反映するようにアンチウイルスとアンチスパイウェア サポート表が更新されるたびに、NAC Agentは新しいアンチウイルスとアンチスパイウェア ライブラリを受け取ります。これは、NAC Agentがより新しい追加機能をサポートするのに役立ちます。NAC Agentがこのサポート情報を取得すると、定期的に更新されるse-checks.xmlファイル（se-templates.tar.gzアーカイブでse-rules.xmlファイルとともに公開される）で最新の定義情報をチェックし、クライアントがポスチャポリシーに準拠しているかどうかを決定します。特定のアンチウイルスまたはアンチスパイウェア製品のアンチウイルスとアンチスパイウェアライブラリによってサポートされている機能に応じて、適切な要件がNAC Agentに送信され、ポスチャ検証中にクライアント上でそれらの存在、および特定のアンチウイルスおよびアンチスパイウェア製品のステータスが検証されます。

ISEポスチャエージェントでサポートされているウイルス対策およびマルウェア対策製品の詳細については、Cisco.comにあるCisco AnyConnect ISEポスチャのサポート表を参照してください。

マルウェア対策のポスチャ条件を作成する際に、コンプライアンスモジュールの最小バージョンを確認できます。ポスチャフィードが更新されたら、[ワークセンター（Work Centers）]>

[ポスチャ（Posture）]>[ポリシー要素（Policy Elements）]>[マルウェア対策条件（Anti-Malware Condition）]を選択し、[オペレーティングシステム（Operating System）]と[ベンダー（Vendor）]を選択してサポート表を表示します。

（注） マルウェア対策のエンドポイントセキュリティ ソリューション（FireEye、Cisco AMP、Sophos など）の一部には、それぞれの集中型サービスへネットワークを通じてアクセスしないと機能しないものがあります。このような製品の場合、AnyConnect ISE の章 (または OESIS ライブラリ) は、エンドポイントがインターネットに接続されていることを想定しています。このようなエンドポイントについては、これらのオンラインエージェントのための事前ポスチャ（オフライン検出が有効になっていない場合）時にインターネットアクセスを許可することを推奨します。このような場合には、署名定義の条件が適用されないことがあります。

インライン ポスチャ ノード

インライン ポスチャ ノードは、ネットワーク上のワイヤレス LAN コントローラ（WLC）および VPN コンセントレータなどのネットワーク アクセス デバイスの背後にある、ゲートキーピング ノードです。インライン ポスチャ ノードにより、ユーザが認証され、アクセス権が与えられた後にアクセス ポリシーが適用され、WLC または VPN で処理できない許可変更（CoA）要求が処理されます。Cisco ISE では、プライマリ ロールまたはセカンダリ ロールを担当できるインライン ポスチャ ノードを 2 つ使用してハイ アベイラビリティを実現できます。

インライン ポスチャ ノードは、専用ノードである必要があります。このノードはインライン ポスチャ サービス専用である必要があり、他の Cisco ISE サービスと同時に実行することはできません。同様に、そのサービスの特性のため、インライン ポスチャ ノードはどのペルソナも担当することができません。たとえば、Cisco ISE ネットワークの管理サービスを提供する管理ノード、ネットワーク アクセス サービス、ポスチャ サービス、プロファイル サービス、およびゲスト サービスを提供するポリシー サービス ノード、またはモニタリング サービスおよびトラブルシューティング サービスを提供するモニタリング ノードとして稼働することはできません。

インライン ポスチャのペルソナは Cisco ISE 3495 プラットフォームではサポートされません。インライン ポスチャのペルソナは、サポートされるプラットフォームである Cisco ISE 3315、Cisco ISE 3355、Cisco ISE 3395、または Cisco ISE 3415 のいずれかにインストールしてください。

インライン ポスチャ ノードの Web ベースのユーザ インターフェイスにアクセスすることはできません。これは、PAN からのみ設定できます。

インライン ポスチャ ノードのインストール

Cisco.com からインライン ポスチャ ISO（IPN ISO）イメージをダウンロードし、サポートされているプラットフォームのいずれかにインストールします。次に、コマンドライン インター

フェイス（CLI）を使用して証明書を設定する必要があります。これで、管理者ポータルからこのノードを登録できます。

（注） リリース 1.31.4 用の別個のインライン ポスチャ ISO イメージはありません。1.2 IPN ISO イメージを使用して、インライン ポスチャ ノードをインストールおよび設定します。

インライン ポスチャ アプリケーションをインストールして設定した後、インライン ポスチャ ノードを登録するには、証明書を設定する必要があります。詳細については、『Cisco Identity Services Engine Hardware Installation Guide』を参照してください。

インライン ポスチャ ノードの登録

登録時にノードのタイプ（Cisco ISE またはインライン ポスチャ）を決定することを推奨します。後でノードタイプを変更する場合は、ノードを展開から登録解除し、スタンドアロン ノードで Cisco ISE を再起動してから、そのノードを登録する必要があります。

始める前に

- プライマリ ノードの証明書信頼リスト（CTL）に、登録するセカンダリ ノードの HTTPS 証明書を検証するための適切な認証局（CA）証明書があることを確認します。
- セカンダリ ノードをプライマリ ノードに登録した後、セカンダリ ノードで HTTPS 証明書を変更する場合は、プライマリ ノードの CTL に適切な CA 証明書をインポートする必要があります。

ステップ 1 PAN にログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 3 左側のナビゲーション ペインで、[展開（Deployment）] をクリックします。

ステップ 4 **[登録（Register）] > [インライン ポスチャ ノードの登録（Register an Inline Posture Node）]** を選択して、セカンダリ インライン ポスチャ ノードを登録します。

コンプライアンス モジュール

コンプライアンス モジュールには、ベンダー名、製品バージョン、製品名、および Cisco ISE のポスチャ条件をサポートする OPSWAT が提供する属性などのフィールドのリストが含まれています。

ベンダーは頻繁に製品バージョンや定義ファイルの日付を更新するので、頻繁にアップデートのコンプライアンス モジュールをポーリングすることで、各ベンダーの製品の最新バージョンおよび定義ファイルの日付を調べる必要があります。新しいベンダー、製品、およびリリース

のサポートを反映してコンプライアンス モジュールが更新されるたびに、AnyConnect のエージェントは新しいライブラリを受信します。これは、AnyConnect のエージェントがより新しい追加機能をサポートするのに役立ちます。AnyConnect のエージェントがこのサポート情報を取得すると、定期的に更新される se-checks.xml ファイル（se-templates.tar.gz アーカイブで se-rules.xml ファイルとともに公開される）で最新の定義情報をチェックし、クライアントがポスチャ ポリシーに準拠しているかどうかを決定します。特定のアンチウイルス、アンチスパイウェア、マルウェア対策、ディスク暗号化またはパッチ管理製品のライブラリによってサポートされている機能に応じて、適切な要件が AnyConnect エージェントに送信され、ポスチャ検証中にクライアント上でそれらの存在、およびクライアントでの特定の製品のステータスが検証されます。

コンプライアンス モジュールは、Cisco.com で入手可能です。

次の表に、ISE ポスチャ ポリシーをサポートするまたはしない OPSWAT API バージョンを示します。バージョン 3 および 4 をサポートするエージェントごとに異なるポリシー ルールがあります。

表 *151 : OPSWAT API* バージョン

ポスチャ条件	コンプライアンス モジュールのバージョン
OPSWAT	
アンチウイルス	3.x 以前
スパイウェア対策	3.x 以前
マルウェア対策	4.x 以降
ディスク暗号化	3.x 以前および 4.x 以降
パッチ管理	3.x 以前および 4.x 以降
USB	4.x 以降
非 OPSWAT	
ファイル（File）	すべてのバージョン
Application	すべてのバージョン
複合	すべてのバージョン
レジストリ	すべてのバージョン
サービス	すべてのバージョン

（注）
- 上記のバージョンのいずれかがインストールされた可能性のあるクライアントを予測して、バージョン 3.x 以前およびバージョン 4.x 以降用に別個のポスチャ ポリシーを作成する必要があります。
- OESIS バージョン 4 のサポートはコンプライアンス モジュール 4.x および Cisco AnyConnect 4.3 以降に提供されます。しかし、AnyConnect 4.3 は OESIS バージョン 3 とバージョン 4 のポリシーの両方をサポートします。
- バージョン 4 コンプライアンス モジュールは、ISE 2.1 以降でサポートされています。

ポスチャ コンプライアンスのチェック

ステップ 1 Cisco ISE にログインし、ダッシュボードにアクセスします。

ステップ 2 [ポスチャ コンプライアンス（Posture Compliance）] ダッシュレットで、カーソルを積み上げ棒またはスパークラインに合わせます。

ツール チップに詳細情報が示されます。

ステップ 3 データ カテゴリを展開すると、詳細を参照できます。

ステップ 4 [ポスチャ コンプライアンス（Posture Compliance）] ダッシュレットを大きくします。

詳細なリアルタイム レポートが表示されます。

（注） [コンテキストの可視性（Context Visibility ）] ウィンドウにポスチャ コンプライアンス レポートを表示できます。[コンテキストの可視性（Context Visibility ）] > [エンドポイント（Endpoints）] > [コンプライアンス（Compliance）] に移動します。このウィンドウには、コンプライアンス ステータス、場所、エンドポイント、およびカテゴリ別のアプリケーションに基づいてさまざまなチャートが表示されます。

アクティブなセッションがないエンドポイントのポスチャ ステータスが表示される場合があります。たとえば、エンドポイントの最新の既知のポスチャ ステータスが準拠の場合、エンドポイントセッションが終了していても、エンドポイントで次の更新を受信するまで、[コンテキストの可視性（Context Visibility）] ウィンドウのステータスは準拠のままになります。ポスチャ ステータスは、このエンドポイントが削除または消去されるまで、[コンテキストの可視性（Context Visibility）] ウィンドウで保持されます。

複合ポスチャ条件の作成

ポスチャ評価と検証のポスチャ ポリシーで使用できる複合条件を作成できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[複合条件（Compound Conditions）]** > **[追加（Add）]** を選択します。

ステップ 2 フィールドに適切な値を入力します。

ステップ 3 条件を検証するために [式の確認（Validate Expression）] をクリックします。

ステップ 4 [送信（Submit）] をクリックします。

パッチ管理条件の作成

選択したベンダーのパッチ管理製品のステータスを確認するポリシーを作成できます。

たとえば、Microsoft System Center Configuration Manager（SCCM）、クライアント バージョン 4.x ソフトウェア製品がエンドポイントにインストールされているかどうかを確認する条件を作成できます。

（注） Cisco ISE および AnyConnect のサポート対象バージョンは次のとおりです。

- Cisco ISE バージョン 1.4 以降
- AnyConnect バージョン 4.1 以降

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[パッチ管理条件（Patch Management Condition）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）] フィールドに条件名を入力し、[説明（Description）] フィールドにその説明を入力します。

ステップ 4 [オペレーティングシステム（Operating System）] ドロップダウン フィールドから、適切なオペレーティング システムを選択します。

ステップ 5 ドロップダウン リストから [コンプライアンスモジュール（Compliance Module）] を選択します。

ステップ 6 ドロップダウン リストから [ベンダー名（Vendor Name）] を選択します。

ステップ 7 [チェックタイプ（Check Type）] を選択します。

ステップ 8 [インストール済みパッチの確認（Check Patches Installed）] ドロップダウン リストから適切なパッチを選択します。

ステップ 9 [送信（Submit）] をクリックします。

関連トピック

パッチ管理条件の設定 （1225 ページ）
パッチ管理修復の追加 （1244 ページ）

ディスク暗号化条件の作成

エンドポイントが指定されたデータ暗号化ソフトウェアに準拠しているかどうかを確認するポリシーを作成できます。

たとえば、C: ドライブがエンド ポイントで暗号化されているかどうかを確認する条件を作成できます。C: ドライブが暗号化されていない場合、エンド ポイントはコンプライアンス違反通知を受信し、ISE はメッセージをログに記録します。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。AnyConnect ISE ポスチャ エージェントを使用している場合にのみ、ポスチャ要件とディスク暗号化条件を関連付けることができます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Condition）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ディスク暗号化条件（Disk Encryption Condition）] ページで、フィールドに適切な値を入力します。

ステップ 4 [送信（Submit）] をクリックします。

ポスチャ条件の設定

ここでは、ポスチャに使用される単純条件および複合条件について説明します。

ファイル条件の設定

次の表では、[ファイル条件（File Conditions）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ファイル条件（File Conditions）]** です。

表 *152 :* ファイル条件の設定

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
名前（**Name**）	ファイル条件の名前を入力します。	ファイル条件の名前を入力します。
説明	ファイル条件の説明を入力します。	ファイル条件の説明を入力します。
オペレーティング システム（**Operating System**）	ファイル条件が適用される Windows オペレーティング システムを選択します。	ファイル条件が適用される Mac OS X を選択します。
ファイル タイプ（**File Type**）	次のいずれか 1 つの事前定義済み設定を選択します。 • FileDate：特定のファイル作成日またはファイル更新日のファイルがシステムに存在するかどうかをチェックします。 • FileExistence：システムにファイルが存在するかどうかをチェックします。 • FileVersion：特定のバージョンのファイルがシステムに存在するかどうかをチェックします。 • CRC32：チェックサム関数を使用してファイルのデータ整合性をチェックします。 • SHA-256：ハッシュ関数を使用してファイルのデータ整合性をチェックします。	次のいずれか 1 つの事前定義済み設定を選択します。 • FileDate：特定のファイル作成日またはファイル更新日のファイルがシステムに存在するかどうかをチェックします。 • FileExistence：システムにファイルが存在するかどうかをチェックします。 • CRC32：チェックサム関数を使用してファイルのデータ整合性をチェックします。 • SHA-256：ハッシュ関数を使用してファイルのデータ整合性をチェックします。 • PropertyList：loginwindow.plist などの plist ファイルのプロパティ値をチェックします。

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
データ型と演算子（Data Type and Operator）	NA	（ファイル タイプとして [PropertyList] を選択した場合に限り使用可能）plist ファイル内で検索するデータ型またはキーの値を選択します。各データ型には、一連の演算子が含まれています。 • 未指定（Unspecified）：指定したキーの存在をチェックします。 演算子（Exists、DoesNotExist）を入力します。 • 番号（Number）：指定した番号データ型のキーをチェックします。 演算子（equals、does not equal、greater than、less than、greater than または equal to、less than または equal to）と値を入力します。 • 文字列（String）：指定した文字列データ型のキーをチェックします。 演算子（equals、does not equal、equals (ignore case)、starts with、does not start with、contains、does not contain、ends with、does not end with）と値を入力します。 • バージョン（Version）：バージョン文字列で指定したキーの値をチェックします。 演算子（earlier than、later than、same as）と値を入力します。

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
プロパティ名	NA	（ファイル タイプとして [PropertyList] を選択した場合に限り使用可能）キーの名前（たとえば BuildVersionStampAsNumber）を入力します。

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
ファイル パス（**File Path**）		次のいずれか 1 つの事前定義済み設定を選択します。 • ルート（Root）：ルート（/）ディレクトリ内のファイルをチェックします。 ファイルのパスを入力します。 • ホーム（Home）：ホーム（~）ディレクトリ内のファイルをチェックします。 ファイルのパスを入力します。

フィールド名	Windows OS での使用ガイドライン	Mac OS X での使用ガイドライン
	次のいずれか 1 つの事前定義済み設定を選択します。 • ABSOLUTE_PATH：ファイルの完全修飾パスのファイルをチェックします。 例：C:\<directory>\file name。その他の設定では、ファイル名のみを入力します。 • SYSTEM_32：C:\WINDOWS\system32 ディレクトリ内のファイルをチェックします。ファイル名を入力します。 • SYSTEM_DRIVE：C:\ ドライブ内のファイルをチェックします。ファイル名を入力します。 • SYSTEM_PROGRAMS：C:\Program Files 内のファイルをチェックします。ファイル名を入力します。 • SYSTEM_ROOT：Windows システムのルートパス内のファイルをチェックします。ファイル名を入力します。 • USER_DESKTOP：指定したファイルが Windows ユーザのデスクトップにあるかどうかをチェックします。ファイル名を入力します。 • USER_PROFILE：ファイルが Windows ユーザのローカル プロファイル ディレクトリにあるかど	

フィールド名	**Windows OS** での使用ガイドライン	**Mac OS X** での使用ガイドライン
	うかをチェックします。ファイルのパスを入力します。	
ファイル日付タイプ（File Date Type）	（ファイル タイプとして [FileDate] を選択した場合に限り使用可能）[作成日（Creation Date）] または [変更日（Modification Date）] を選択します。	（ファイル タイプとして [FileDate] を選択した場合に限り使用可能）[作成日（Creation Date）] または [変更日（Modification Date）] を選択します。
ファイル演算子	[ファイル演算子（File Operator）] オプションは、[ファイル タイプ（File Type）] で選択した設定に応じて変化します。次の設定を適切に選択します。 FileDate • EarlierThan • LaterThan • EqualTo • 内部（Within）：最後の *n* 日数。有効な値は、1 ～ 300 日です） FileExistence • Exists • DoesNotExist FileVersion • EarlierThan • LaterThan • EqualTo	[ファイル演算子（File Operator）] オプションは、[ファイル タイプ（File Type）] で選択した設定に応じて変化します。次の設定を適切に選択します。 FileDate • EarlierThan • LaterThan • EqualTo • 内部（Within）：最後の *n* 日数。有効な値は、1 ～ 300 日です） FileExistence • Exists • DoesNotExist

フィールド名	Windows OS での使用ガイドライン	Mac OS X での使用ガイドライン
ファイルの CRC データ（File CRC Data）	（ファイル タイプとして [CRC32] を選択した場合に限り使用可能）チェックサムの値（たとえば 0x3c37fec3）を入力してファイルの整合性をチェックできます。チェックサム値は 16 進数の整数 0x で始まる必要があります。	（ファイル タイプとして [CRC32] を選択した場合に限り使用可能）チェックサムの値（たとえば 0x3c37fec3）を入力してファイルの整合性をチェックできます。チェックサム値は 16 進数の整数 0x で始まる必要があります。
ファイルのSHA-256データ（File SHA-256 Data）	（ファイル タイプとして [SHA-256] を選択した場合に限り使用可能）64 バイトの 16 進数のハッシュ値を入力してファイルの整合性をチェックできます。	（ファイル タイプとして [SHA-256] を選択した場合に限り使用可能）64 バイトの 16 進数のハッシュ値を入力してファイルの整合性をチェックできます。
日付および時刻（Date and Time）	（ファイル タイプとして **FileDate** を選択した場合に限り使用可能）クライアント システムの日付と時刻を、mm/dd/yyyy および hh:mm:ss 形式で入力します。	（ファイル タイプとして **FileDate** を選択した場合に限り使用可能）クライアント システムの日付と時刻を、mm/dd/yyyy および hh:mm:ss 形式で入力します。

関連トピック

単純ポスチャ条件 （1188 ページ）
複合ポスチャ条件 （1190 ページ）
ポスチャ条件の作成 （1256 ページ）

ファイアウォール条件の設定

ファイアウォール条件により、特定のファイアウォール製品がエンドポイントで稼働しているかどうかがチェックされます。サポートされているファイアウォール製品のリストは、OPSWAT サポート チャートに基づいています。初回ポスチャと定期的再評価（PRA）の実行中にポリシーを適用できます。

Cisco ISE は、Windows および Mac OS のデフォルトのファイアウォール条件を提供します。これらの条件は、デフォルトで無効になっています。

フィールド名	使用上のガイドライン
名前（Name）	ファイアウォール条件の名前を入力します。
説明	ファイアウォール条件の説明を入力します。

フィールド名	使用上のガイドライン
コンプライアンス モジュール	必要なコンプライアンス モジュールを選択します。 • 4.x 以降 • 3.x 以降 • 任意のバージョン（Any Version）
オペレーティング システム	必要なファイアウォール製品がエンドポイントにインストールされているかどうかを確認します。Windows OS または Mac OSX を選択できます。
ベンダー	ドロップダウン リストからベンダー名を選択します。ベンダーのファイアウォール製品とそれらのチェック タイプが取得され、[選択したベンダーの製品（Products for Selected Vendor）]テーブルに表示されます。テーブル内のリストは、選択したオペレーティング システムによって変わります。
チェック タイプ（**Check Type**）	[有効（Enabled）]：特定のファイアウォールがエンドポイントで稼働しているかどうかをチェックします。ベンダーの製品が選択したチェック タイプをサポートしているかどうかを [選択したベンダーの製品（Products for Selected Vendor）] リストを参照することで確認します。

レジストリ条件の設定

次の表では、[レジストリ条件（Registry Conditions）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]>[ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [レジストリ条件（Registry Conditions）]** です。

表 ***153 :*** レジストリ条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	レジストリ条件の名前を入力します。
説明	レジストリ条件の説明を入力します。

フィールド名	使用上のガイドライン
レジストリ タイプ（**Registry Type**）	レジストリ タイプとして事前定義済み設定の 1 つを選択します。
レジストリ ルート キー（**Registry Root Key**）	レジストリ ルート キーとして事前定義済み設定の 1 つを選択します。
サブ キー（**Sub Key**）	レジストリ ルート キーに指定されたパスのレジストリ キーをチェックするには、バックスラッシュ（「\」）なしでサブ キーを入力します。 たとえば、SOFTWARE\Symantec\Norton AntiVirus\version によって、次のパスのキーがチェックされます。 HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
値の名前（**Value Name**）	（[レジストリ タイプ（Registry Type）] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能） [RegistryValue] をチェックするレジストリ キー値の名前を入力します。 これは [RegistryValueDefault] のデフォルト フィールドです。
値データ型（**Value Data Type**）	（[レジストリ タイプ（Registry Type）] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能）次の設定の 1 つを選択します。 • [未指定（Unspecified）]：レジストリ キー値があるかどうかをチェックします。このオプションは、[RegistryValue] の場合にのみ使用できます。 • [数字（Number）]：レジストリ キー値の指定された数字をチェックします • [文字列（String）]：レジストリ キー値の文字列をチェックします • [バージョン（Version）]：レジストリ キー値のバージョンをチェックします
値演算子（**Value Operator**）	設定を適切に選択します。

フィールド名	使用上のガイドライン
値データ	（[レジストリ タイプ（Registry Type）] として [RegistryValue] または [RegistryValueDefault] を選択した場合にのみ使用可能）[値データ型（Value Data Type）] で選択したデータ型に応じてレジストリ キーの値を入力します。
オペレーティング システム	レジストリ条件を適用する必要のあるオペレーティング システムを選択します。

関連トピック

単純ポスチャ条件 （1188 ページ）
複合ポスチャ条件 （1190 ページ）

アプリケーション条件の設定

次の表に、[アプリケーション条件（Application Conditions）] ページのフィールドを示します。このページへのナビゲーション パスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [アプリケーション条件（Application Conditions）]** です。

表 *154* : アプリケーション条件の設定

フィールド	使用上のガイドライン
名前（Name）	アプリケーションの条件の名前を入力します。
説明	アプリケーションの状態の説明を入力します。
オペレーティング システム（Operating System）	アプリケーション条件が適用される Windows OS または MAC OSX を選択します。
プロセス名	調べるアプリケーションの名前を入力します。
アプリケーション演算子（Application Operator）	調べるステータスを選択します。

関連トピック

単純ポスチャ条件 （1188 ページ）
複合ポスチャ条件 （1190 ページ）

継続的なエンドポイント属性モニタリング

ポスチャ アセスメントの実行中に動的な変更が確認されるようにするため、AnyConnect エージェントを使用してさまざまなエンドポイント属性を継続的にモニタします。これによりエン

ドポイントの全体的な可視性が向上し、動作に基づいてポスチャ ポリシーを作成できるようになります。AnyConnect エージェントは、エンドポイントにインストールされ実行されているアプリケーションをモニタします。この機能をオンまたはオフにできます。また、データのモニタ頻度を設定できます。デフォルトでは、データは5分間隔で収集され、データベースに保存されます。初回ポスチャでは、AnyConnectがすべての実行中アプリケーションとインストールされているアプリケーションのリストを報告します。初回ポスチャの後に、AnyConnectエージェントはX分間隔でアプリケーションをスキャンし、最終スキャンでの差異をサーバに送信します。サーバはすべての実行中アプリケーションとインストールされているアプリケーションのリストを表示します。

アプリケーション条件の設定

エンドポイントにインストールされているアプリケーションに対するアプリケーション条件クエリ。これにより、エンドポイントで配信されているソフトウェアの集約された可視性を確認できます。たとえば、この情報に基づいてポリシーを作成し、デスクトップ チームと協力してソフトウェア ライセンスの数を減らすことができます。

次の表に、[アプリケーション条件（Application Conditions）]ページのフィールドを示します。このページへのナビゲーション パスは **[ワーク センター（Work Centers）]** > **[ポスチャ（Posture）]** > **[ポリシー要素（Policy Elements）]** > **[アプリケーション条件（Application Condition）]** > **[追加（Add）]** です。

フィールド名	使用上のガイドライン
名前（Name）	アプリケーション条件の名前を入力します。
説明	アプリケーション条件の説明を入力します。
オペレーティング システム	アプリケーション条件が適用される Windows OS または MAC OSX を選択します。
コンプライアンス モジュール	OESIS バージョン 4.x 以降、3.x 以前、またはすべてのバージョンのサポート。
次を確認（Check By）	次のいずれかを実行します。 • [プロセス（Process）]：エンドポイントでプロセスが実行されているかどうかを確認するには、このオプションをオンにします。 • [アプリケーション（Application）]：エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションをオンにします。

フィールド名	使用上のガイドライン
プロセス名	（[次を確認（Check By）] オプションで [プロセス（Process）] を選択した場合に使用可能）必要なプロセス名を入力します。
アプリケーション演算子（**Application Operator**）	（[次を確認（Check By）] オプションで [プロセス（Process）] を選択した場合に使用可能）次のいずれかを選択します。 • [実行中（Running）]：エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションを選択します。 • [実行されていない（Not Running）]：エンドポイントでアプリケーションが実行されていないかどうかを確認するには、このオプションをオンにします。
アプリケーションの状態（**Application State**）	（[次を確認（Check By）] オプションで [アプリケーション（Application）] を選択した場合に使用可能）次のいずれかを選択します。 • [インストール済み（Installed）]：クライアントのシステムに悪質なアプリケーションがインストールされているかどうかを調べるには、このオプションをオンにします。 悪意のあるアプリケーションがある場合は、修復アクションがトリガーされます。 • [実行中（Running）]：エンドポイントでアプリケーションが実行されているかどうかを確認するには、このオプションをオンにします。

フィールド名	使用上のガイドライン
次をプロビジョニング（**Provision By**）	（[次を確認（Check By）] オプションで [アプリケーション（Application）] を選択した場合に使用可能）次のいずれかを選択します。 • [すべて（Everything）] : [ブラウザ（Browser）]、[パッチ管理（Patch Management）] など、リストされているすべてのカテゴリを選択できます。 • [名前（Name）] : 1 つ以上のカテゴリを選択します。 たとえば [ブラウザ（Browser）] カテゴリを選択すると、[ベンダー（Vendor）] ドロップダウン リストに対応するベンダーが表示されます。 • [カテゴリ（Category）] : 1 つ以上のカテゴリ（[マルウェア対策（Anti-Malware）]、[バックアップ（Backup）]、[ブラウザ（Browser）]、[データストレージ（Data Storage）] など）をオンにできます。 （注） カテゴリは OPSWAT ライブラリから動的に更新されます。

[コンテキストの可視性（Context Visibility）] > **[エンドポイント（Endpoints）]** > **[コンプライアンス（Compliance）]** ウィンドウで、各エンドポイントでインストールされているアプリケーションと実行中のアプリケーションの数を確認できます。

[ホーム（Home）] > **[概要（Summary）]** > **[コンプライアンス（Compliance）]** ウィンドウに、ポスチャアセスメント対象であり準拠しているエンドポイントのパーセンテージが表示されます。

サービス条件の設定

次の表では、[サービス条件（Service Conditions）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[サービス条件（Service Condition）]** です。

表 *155* : サービス条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	サービス条件の名前を入力します。

フィールド名	使用上のガイドライン
説明	サービス条件の説明を入力します。
オペレーティング システム（**Operating Systems**）	サービス条件を適用する必要のあるオペレーティングシステムを選択します。Windows OSまたはMac OSXのさまざまなバージョンを選択できます。
サービス名（**Service Name**）	ルートとして動作するデーモンまたはユーザエージェントサービスの名前を入力します（たとえばcom.apple.geod）。AnyConnectエージェントは、コマンド **sudo launchctl list** を使用してサービス条件を確認します。
サービス タイプ	クライアントのコンプライアンスを確実にするためにAnyConnectが調べる必要があるタイプ オブ サービスを選択します。 • [デーモン（Daemon）]：マルウェアに対するクライアントデバイスのスキャンなど、指定したサービスがクライアントのデーモンサービスの指定されたリストにあるかどうかをチェックします。 • [ユーザエージェント（User Agent）]：マルウェアが検出された場合に実行するサービスなど、指定したサービスがクライアントのユーザサービスの指定されたリストにあるかどうかをチェックします。 • [デーモンまたはユーザエージェント（Daemon or User Agent）]：指定したサービスがデーモンまたはユーザエージェントのサービスリストにあるかどうかをチェックします。

フィールド名	使用上のガイドライン
サービス オペレータ（Service Operator）	クライアントでチェックするサービス ステータスを選択します。 • [Windows OS]：サービスが [実行している（Running）] か、または [実行していない（Not Running）] かをチェックします。 • [Mac OSX]：サービスが [ロード済み（Loaded）] か、[ロードされていない（Not Loaded）] か、[ロード済みで実行している（Loaded and Running）] か、[終了コード付きでロード済み（Loaded with Exit Code）] か、[ロード済みで実行しているまたは終了コードが付いている（Loaded & running or with Exit code）] かどうかをチェックします。

関連トピック

単純ポスチャ条件 （1188 ページ）
複合ポスチャ条件 （1190 ページ）

ポスチャ複合条件の設定

次の表に、[複合条件（Compound Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[複合条件（Compound Conditions）]** です。

表 *156 :* ポスチャ複合条件の設定

フィールド名	使用上のガイドライン
名前（Name）	作成する複合条件の名前を入力します。
説明	作成する複合条件の説明を入力します。
オペレーティング システム	1 つ以上の Windows オペレーティング システムを選択します。これにより、条件が適用される Windows オペレーティング システムを関連付けることができます。
カッコ ( )（Parentheses ( )）	ファイル、レジストリ、アプリケーション、サービス条件という単純な条件タイプから 2 つの単純条件を組み合わせるには、カッコをクリックします。

フィールド名	使用上のガイドライン
（&）：AND 演算子（AND 演算子には「&」を使用します）	複合条件内には AND 演算子（アンパサンド（&））を使用できます。たとえば、**Condition1 & Condition2** と入力します。
（|）：OR 演算子（OR 演算子には「|」を使用します）	複合条件内には OR 演算子（縦線「|」）を使用できます。たとえば、**Condition1 & Condition2** と入力します。
（!）：NOT 演算子（NOT 演算子には「!」を使用します）	複合条件内には NOT 演算子（感嘆符（!））を使用できます。たとえば、**Condition1 & Condition2** と入力します。
単純条件	ファイル、レジストリ、アプリケーション、サービス条件という単純条件のリストから選択します。 また、オブジェクト セレクタからファイル、レジストリ、アプリケーション、サービス条件という単純条件を作成できます。 ファイル、レジストリ、アプリケーション、サービス条件という単純条件を作成するには、[操作（Action）] ボタンのクイック ピッカー（下向き矢印）をクリックします。

関連トピック

ポスチャ条件 （1188 ページ）
複合ポスチャ条件の作成 （1196 ページ）

ウイルス対策条件の設定

次の表では、[ウイルス対策条件（Anti-Virus Condition）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ウイルス対策条件（Anti-Virus Condition）]** です。

表 *157* : ウイルス対策条件の設定

フィールド名	使用上のガイドライン
名前（Name）	作成するウイルス対策条件の名前を入力します。
説明	作成するウイルス対策条件の説明を入力します。

フィールド名	使用上のガイドライン
オペレーティング システム	オペレーティング システムを選択して、クライアント上のアンチウイルス プログラムのインストールをチェックするか、または条件が適用される最新のアンチウイルス定義ファイルの更新をチェックします。
ベンダー	ドロップダウン リストからベンダーを選択します。ベンダーを選択すると、アンチウイルス製品およびバージョンが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。
チェック タイプ（**Check Type**）	クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするかを選択します。
インストール	クライアント上のアンチウイルス プログラムのインストールのみをチェックする場合に選択します。
定義（**Definition**）	クライアント上のアンチウイルス製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。
最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）（**Check against latest AV definition file version, if available**）	（[定義（Definition）] チェック タイプを選択した場合にのみ使用可能）クライアントのアンチウイルス定義ファイルのバージョンをチェックする場合に選択します。Cisco ISE でのポスチャ更新の結果として、最新のアンチウイルス定義ファイルのバージョンを使用できるときには、そのバージョンに対するチェックが行われます。それ以外の場合、このオプションを使用すると、クライアント上の定義ファイルの日付を、Cisco ISE の最新の定義ファイルの日付に対してチェックできます。

フィールド名	使用上のガイドライン
ウイルス定義ファイルを（有効）にすることを許可する（**Allow virus definition file to be (Enabled)**）	（定義チェック タイプを選択した場合のみ使用可能）アンチウイルス定義ファイルのバージョンと、クライアント上の最新のアンチウイルス定義ファイルの日付をチェックする場合に選択します。最新の定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付から、次のフィールド（[より古い日数（days older than）] フィールド）で定義した日数よりも古いことは許容されません。 オフにした場合、[最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。（Check against latest AV definition file version, if available.）] オプションを使用してアンチウイルス定義ファイルのバージョンのみをチェックすることができます。
より古い日数（**Days Older Than**）	クライアント上の最新のアンチウイルス定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付または現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。
最新のファイルの日付（**Latest File Date**）	[より古い日数（days older than）] クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のアンチウイルス定義ファイルの日付が、製品の最新のアンチウイルス定義ファイルの日付よりも古いことは許容されません。
現在のシステム日付（**Current System Date**）	[より古い日数（days older than）] クライアント上のアンチウイルス定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のアンチウイルス定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。

フィールド名	使用上のガイドライン
選択したベンダーの製品（Products for Selected Vendor）	テーブルからアンチウイルス製品を選択します。[新しいアンチウイルス条件（New Anti-virus Compound Condition）] ページで選択したベンダーに基づいて、テーブルは、アンチウイルス製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。 テーブルから製品を選択すると、アンチウイルス プログラムのインストールをチェックしたり、最新のアンチウイルス定義ファイルの日付および最新バージョンをチェックしたりできます。

関連トピック

複合ポスチャ条件 （1190 ページ）
事前設定済みアンチウイルスおよびアンチスパイウェア条件 （1192 ページ）
アンチウイルスとアンチスパイウェア サポート表 （1192 ページ）

アンチスパイウェア複合条件の設定

次の表に、[AS複合条件（AS Compound Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [AS複合条件（AS Compound Condition）]** です。

表 *158* : アンチスパイウェア複合条件の設定

フィールド名	使用上のガイドライン
名前（Name）	作成するアンチスパイウェア複合条件の名前を入力します。
説明	作成するアンチスパイウェア複合条件の説明を入力します。
オペレーティング システム（Operating System）	オペレーティング システムを選択すると、クライアント上のアンチスパイウェア プログラムのインストールをチェックするか、または条件が適用される最新のアンチスパイウェア定義ファイルの更新をチェックすることができます。

フィールド名	使用上のガイドライン
ベンダー（**Vendor**）	ドロップダウン リストからベンダーを選択します。ベンダーを選択すると、アンチスパイウェア製品およびバージョンが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。
チェック タイプ（**Check Type**）	クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするか、いずれかのタイプを選択します。
インストール	クライアント上のアンチスパイウェア プログラムのインストールのみをチェックする場合に選択します。
定義（**Definition**）	クライアント上のアンチスパイウェア製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。
ウイルス定義ファイルを（有効）にすることを許可する（**Allow Virus Definition File to be (Enabled)**）	このチェックボックスは、アンチスパイウェア定義チェック タイプを作成するときはオンにし、アンチスパイウェア インストール チェック タイプを作成するときはオフにします。 オンにすると、その選択により、クライアント上のアンチスパイウェア定義ファイルのバージョンおよび最新のアンチスパイウェア定義ファイルの日付をチェックできます。最新の定義ファイルの日付が、現在のシステム日付から、[より古い日数（days older than）] フィールドで定義した日数より古いことは許容されません。 オフの場合、その選択により、[ウイルス定義ファイルを（有効）にすることを許可する（Allow virus definition file to be (Enabled)）] チェックボックスがオフのときに、アンチスパイウェア定義ファイルのバージョンのみをチェックすることができます。
より古い日数（**Days Older Than**）	クライアント上の最新のアンチスパイウェア定義ファイルの日付が、現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。

フィールド名	使用上のガイドライン
現在のシステム日付（**Current System Date**）	[より古い日数（days older than）] クライアント上のアンチスパイウェア定義ファイルの日付をチェックすることを選択します。この日付は、フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のアンチスパイウェア定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。
選択したベンダーの製品（**Products for Selected Vendor**）	テーブルからアンチスパイウェア製品を選択します。[新しいアンチスパイウェア複合条件（New Anti-spyware Compound Condition）] ページで選択したベンダーに基づいて、テーブルは、アンチスパイウェア製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。 テーブルから製品を選択すると、アンチスパイウェア プログラムのインストールをチェックしたり、最新のアンチスパイウェア定義ファイルの日付および最新バージョンをチェックしたりできます。

関連トピック

複合ポスチャ条件 （1190 ページ）
事前設定済みアンチウイルスおよびアンチスパイウェア条件 （1192 ページ）
アンチウイルスとアンチスパイウェア サポート表 （1192 ページ）

マルウェア対策条件の設定

マルウェア対策条件はスパイウェア対策条件とウイルス対策条件の組み合わせで、OESIS バージョン 4.x 以降のコンプライアンス モジュールでサポートされています。次の表では、[マルウェア対策条件（Antimalware Conditions）] ウィンドウのフィールドについて説明します。ナビゲーションパスは、**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャ要素（Posture Elements）] > [条件（Conditions）] > [マルウェア対策（Antimalware）]** です。また、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [マルウェア対策条件（Antimalware Condition）]** ウィンドウでもこのオプションにアクセスできます。

（注） 最新の定義が適用されるようにインストールしたマルウェア対策製品を手動で1回以上更新することをお勧めします。更新しないと、マルウェア対策定義のAnyConnectを使用したポスチャチェックが失敗します。

表 *159 :* マルウェア対策条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	マルウェア対策条件の名前を入力します。
説明	マルウェア対策条件の説明を入力します。
コンプライアンス モジュール	OESIS バージョン 4.x 以降のサポート。
オペレーティング システム（**Operating System**）	オペレーティング システムを選択して、クライアント上のマルウェア対策プログラムのインストールをチェックするか、または条件が適用される最新のマルウェア対策定義ファイルの更新をチェックします。MAC と Windows OS の両方をサポートしています。
ベンダー（**Vendor**）	ドロップダウン リストからベンダーを選択します。選択したベンダーのマルウェア対策製品、バージョン、最新の定義日、最新の定義バージョン、最小コンプライアンス モジュール バージョンが [選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。
チェック タイプ（**Check Type**）	クライアント上でインストールをチェックするか、または最新の定義ファイルの更新をチェックするかを選択します。
インストール	クライアント上のマルウェア対策プログラムのインストールのみをチェックする場合に選択します。
定義（**Definition**）	クライアント上のマルウェア対策製品の、最新の定義ファイルの更新のみをチェックする場合に選択します。

フィールド名	使用上のガイドライン
最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）（**Check Against Latest AV Definition File Version, if Available**）	（[定義（Definition）] チェック タイプを選択した場合にのみ使用可能）クライアントのマルウェア対策定義ファイルのバージョンをチェックする場合に選択します。Cisco ISE でのポスチャ更新の結果として、最新のマルウェア対策定義ファイルのバージョンを使用できるときには、そのバージョンに対するチェックが行われます。それ以外の場合、このオプションを使用すると、クライアント上の定義ファイルの日付を、Cisco ISE の最新の定義ファイルの日付に対してチェックできます。 このチェックは、選択した製品の [最新の定義日（Latest Definition Date）] または [最新の定義バージョン（Latest Definition Version）] フィールドの Cisco ISE に値が記載されている場合にのみ機能します。そうでない場合は、[現在のシステム日付（Current System Date）] フィールドを使用する必要があります。
ウイルス定義ファイルを（有効）にすることを許可する（**Allow Virus Definition File to be (Enabled)**）	（定義チェック タイプを選択した場合のみ使用可能）マルウェア対策定義ファイルのバージョンと、クライアント上の最新のマルウェア対策定義ファイルの日付をチェックする場合に選択します。最新の定義ファイルの日付が、製品の最新のマルウェア対策定義ファイルの日付または現在のシステム日付から、次のフィールド（[より古い日数（days older than）] フィールド）で定義した日数よりも古いことは許容されません。 オフにした場合、[最新の AV 定義ファイルのバージョンに対してチェックします（使用可能な場合）。（Check against latest AV definition file version, if available.）] オプションを使用してマルウェア対策定義ファイルのバージョンのみをチェックすることができます。
より古い日数（**Days Older Than**）	クライアント上の最新のマルウェア対策定義ファイルの日付が、製品の最新のマルウェア対策定義ファイルの日付または現在のシステム日付よりも何日古いことが許容されるかを定義します。デフォルト値は 0 です。

フィールド名	使用上のガイドライン
最新のファイルの日付（**Latest File Date**）	クライアント上のマルウェア対策定義ファイルの日付をチェックすることを選択します。この日付は、[より古い日数（days older than）] フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のマルウェア対策定義ファイルの日付が、製品の最新のマルウェア対策定義ファイルの日付よりも古いことは許容されません。 このチェックは、選択した製品の [最新の定義日（Latest Definition Date）] フィールドの Cisco ISE に値が記載されている場合にのみ機能します。そうでない場合は、[現在のシステム日付（Current System Date）] フィールドを使用する必要があります。
現在のシステム日付（**Current System Date**）	クライアント上のマルウェア対策定義ファイルの日付をチェックすることを選択します。この日付は、[より古い日数（days older than）] フィールドで定義した日数だけ古いことが許容されます。 日数をデフォルト値（0）に設定する場合、クライアント上のマルウェア対策定義ファイルの日付が、現在のシステム日付よりも古いことは許容されません。
選択したベンダーの製品（**Products for Selected Vendor**）	テーブルからマルウェア対策製品を選択します。[新しいマルウェア対策条件（New Antimalware Condition）] ページで選択したベンダーに基づいて、テーブルは、マルウェア対策製品およびバージョン、提供する修復のサポート、最新の定義ファイルの日付とバージョンに関する情報を取得します。 テーブルから製品を選択すると、マルウェア対策プログラムのインストールをチェックしたり、最新のマルウェア対策定義ファイルの日付および最新バージョンをチェックしたりできます。

関連トピック

複合ポスチャ条件 （1190 ページ）

ディクショナリ単純条件の設定

次の表に、[ディクショナリ単純条件（Dictionary Simple Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[ディクショナリ単純条件（Dictionary Simple Conditions）]** です。

表 *160* : ディクショナリ単純条件の設定

フィールド名	使用上のガイドライン
[名前（Name）]	作成するディクショナリ単純条件の名前を入力します。
説明	作成するディクショナリ単純条件の説明を入力します。
属性（Attribute）	ディクショナリから属性を選択します。
演算子	選択した属性に値を関連付ける演算子を選択します。
値	ディクショナリ属性に関連付ける値を入力するか、またはドロップダウン リストから事前定義済みの値を選択します。

関連トピック

ディクショナリおよびディクショナリ属性
単純条件と複合条件
単純ポスチャ条件 （1188 ページ）
単純ポスチャ条件の作成 （1189 ページ）

ディクショナリ複合条件の設定

次の表に、[ディクショナリ複合条件（Dictionary Compound Conditions）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[ディクショナリ複合条件（Dictionary Compound Conditions）]** です。

表 *161* : ディクショナリ複合条件の設定

フィールド名	使用上のガイドライン
[名前（Name）]	作成するディクショナリ複合条件の名前を入力します。

フィールド名	使用上のガイドライン
説明	作成するディクショナリ複合条件の説明を入力します。
既存の条件をライブラリから選択（**Select Existing Condition from Library**）	ポリシー要素ライブラリから事前定義済みの条件を選択して式を定義するか、または後のステップでアドホック属性/値のペアを式に追加します。
条件名（**Condition Name**）	ポリシー要素ライブラリからすでに作成しているディクショナリ単純条件を選択します。
式（**Expression**）	[条件名（Condition Name）] ドロップダウンリストでの選択に基づいて式が更新されます。
AND または **OR** 演算子（**AND or OR operator**）	ライブラリから追加できるディクショナリ単純条件を論理的に組み合わせるには、AND または OR 演算子を選択します。 次の操作を行うには、[操作（Action）] アイコンをクリックします。 • 属性/値の追加（Add Attribute/Value） • ライブラリから条件を追加（Add Condition from Library） • 削除（Delete）
新しい条件の作成（高度なオプション）（**Create New Condition (Advance Option)**）	さまざまなシステムディクショナリまたはユーザ定義ディクショナリから属性を選択します。 後のステップで事前定義された条件をポリシー要素ライブラリから追加することもできます。
条件名（**Condition Name**）	すでに作成したディクショナリ単純条件を選択します。
式（**Expression**）	[式（Expression）] ドロップダウン リストから、ディクショナリ単純条件を作成できます。
演算子	属性に値を関連付ける演算子を選択します。
値	ディクショナリ属性に関連付ける値を入力するか、またはドロップダウン リストから値を選択します。

関連トピック

ディクショナリおよびディクショナリ属性

単純条件と複合条件
複合ポスチャ条件 （1190 ページ）
複合ポスチャ条件の作成 （1196 ページ）

パッチ管理条件の設定

次の表に、[パッチ管理条件（Patch Management Conditions）] ウィンドウのフィールドを示します。ナビゲーションパスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [パッチ管理条件（Patch Management Conditions）]** です。

表 *162 :* パッチ管理条件

フィールド名	使用上のガイドライン
名前（Name）	パッチ管理条件の名前を入力します。
説明	パッチ管理条件の説明を入力します。
オペレーティング システム	オペレーティング システムを選択して、エンドポイント上のパッチ管理ソフトウェアのインストールをチェックするか、または条件が適用される最新のパッチ管理定義ファイルの更新をチェックします。Windows OS または Mac OSX を選択できます。また、パッチ管理条件を作成する複数のオペレーティング システムのバージョンを選択することもできます。
ベンダー名（Vendor Name）	ドロップダウン リストからベンダー名を選択します。ベンダーのパッチ管理製品とそれらのサポート対象バージョン、チェック タイプ、および最小対応モジュールのサポートが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されます。テーブル内のリストは、選択したオペレーティング システムによって変わります。

フィールド名	使用上のガイドライン
チェック タイプ（**Check Type**）	

フィールド名	使用上のガイドライン
	次のオプションのいずれかを選択します。 • [インストール（Installation）]：選択した製品がエンドポイントにインストールされているかどうかを確認します。 このチェック タイプは、すべてのベンダーでサポートされています。 （注） Cisco Temporal Agent の場合は、[要件（Requirements）]ページで[インストール（Installation）] チェック タイプを含むパッチ管理条件のみを表示できます。 • [有効（Enabled）]：選択した製品がエンドポイントで有効かどうかを確認します。ベンダーの製品が選択したチェック タイプをサポートしているかどうかを[選択したベンダーの製品（Products for Selected Vendor）]リストを参照することで確認します。 • [最新（Up to Date）]：選択した製品に欠けているパッチがないかどうかを確認します。ベンダーの製品が選択したチェック タイプをサポートしているかどうかを[選択したベンダーの製品（Products for Selected Vendor）] リストを参照することで確認します。 [ベンダー名（Vendor Name）] で指定したベンダーがサポートする製品のリストを表示するには、[選択したベンダーの製品（Products for Selected Vendor）] ドロップダウン矢印をクリックします。たとえば、製品 1 と 製品 2 の 2 つの製品を持つベンダーA を選択したとします。製品 1 は [有効（Enabled）] オプションをサポートしているが、製品 2 はサポートしていない場合があります。または、製品1がチェック タイプのいずれもサポートしていない場合は、グレー表示されます。 （注） （Cisco ISE 2.3 以降および AnyConnect 4.5 以上に適用されます）SCCM のパッチ管理条件で [最新（Up to Date）] チェック タイプを

フィールド名	使用上のガイドライン
	選択すると、Cisco ISE は次の動作を行います 1. Microsoft API を使用して、指定された重大度レベルの現在のセキュリティ パッチを確認します。 2. その欠落しているセキュリティ パッチに対するパッチ管理修復をトリガーします。
インストール済みパッチの確認（Check Patches Installed）	（[最新（Up To Date）] チェック タイプを選択している場合にのみ使用可能。）欠落しているパッチの重大度レベルを設定し、重大度に基づいて展開することができます。次の重大度レベルのいずれかを選択します。 • [クリティカルのみ（Critical Only）]：クリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [重要およびクリティカル（Important and Critical）]：重要かつクリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [中程度、重要およびクリティカル（Moderate, Important, & Critical）]：中程度、重要およびクリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [低程度からクリティカルまで（Low To Critical）]：低程度、中程度、重要、およびクリティカルなソフトウェアパッチが展開内のエンドポイントにインストールされているかどうかを確認します。 • [すべて（All）]：すべての重大度レベルの欠落しているパッチをインストールします。

関連トピック

ソフトウェアパッチのインストール （262 ページ）
ソフトウェアパッチのロールバック （263 ページ）
パッチのインストールおよびロールバックの変更の表示
パッチ管理条件の作成 （1197 ページ）

ディスク暗号化条件の設定

次の表では、[ディスク暗号化条件（Disk Encryption Condition）] ウィンドウのフィールドについて説明します。ナビゲーションパスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Condition）] です。

表 *163 :* ディスク暗号化条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するディスク暗号化条件の名前を入力します。
説明	ディスク暗号化条件の説明を入力します。
オペレーティング システム	ディスクを暗号化のためにチェックするエンドポイントのオペレーティング システムを選択します。Windows OS または Mac OSX を選択できます。また、ディスク暗号化条件を作成するための複数のバージョンのオペレーティング システムを選択することもできます。
ベンダー名（**Vendor Name**）	ドロップダウン リストからベンダー名を選択します。ベンダーのデータ暗号化製品およびそれらのサポート対象バージョン、暗号化状態チェック、および最小対応モジュールサポートが取得され、[選択したベンダーの製品（Products for Selected Vendor）] テーブルに表示されますテーブル内のリストは、選択したオペレーティング システムによって変わります。

フィールド名	使用上のガイドライン
[所在地（Location）]	オプションが [選択したベンダーの製品（Products for Selected Vendor）] セクションでオンになっている場合にのみ有効です。次のオプションのいずれかを選択します。 • [特定のロケーション（Specific Location）]：指定したディスクドライブがエンドポイントで暗号化されているか（たとえば Windows OS の場合は C:）、または指定したボリュームラベルが暗号化されているか（たとえば、Mac OSX の場合は Mackintosh HD）を確認します。 • [システムロケーション（System Location）]：デフォルトの Windows OS のシステムドライブまたは Mac OSX のハードドライブがエンドポイントで暗号化されているかを確認します。 • [すべての内部ドライブ（All Internal Drives）]：内部のドライブを確認します。マウントおよび暗号化されたすべてのハードディスクと、すべての内部パーティションが含まれます。読み取りのみのドライブ、システム リカバリ ディスク/パーティション、ブート パーティション、ネットワーク パーティション、およびエンドポイント外のさまざまな物理ディスク ドライブ（USB およびサンダーボルトを介して接続されたディスク ドライブを含むがこれに限定されない）は除外されます。検証済みの暗号化ソフトウェア製品には次のものがあります。 • Bit-locker-6.x/10.x • Windows 7 上の Checkpoint 80.x

フィールド名	使用上のガイドライン
暗号化状態（**Encryption State**）	[暗号化状態（Encryption State）] チェックボックスは、選択した製品が暗号化状態チェックをサポートしていない場合はディセーブルになっています。リピータは、チェックボックスがオンになっている場合のみ表示されます。[完全に暗号化済み（Fully Encrypted）] オプションを選択して、クライアントのディスクドライブが完全に暗号化されているかどうかを確認できます。 たとえば TrendMicro に対し条件を作成し、2 つのベンダー（一方のベンダーの [暗号化状態（Encryption State）] は「はい（Yes）」でもう一方の [暗号化状態（Encryption State）] は「いいえ（No）」）を選択した場合、ベンダーの暗号化状態の一方が「いいえ（No）」になっているので [暗号化状態（Encryption State）] はディセーブルになります。 （注） リピータをクリックすることで追加のロケーションを追加でき、各ロケーション間の関係は論理 AND 演算子です。

関連トピック

ディスク暗号化条件の作成 （1198 ページ）

USB 条件の設定

次の表では、[USB条件（USB Condition）] ウィンドウのフィールドについて説明します。ナビゲーションパスは、**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [USB]** です。また、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [USB条件（USB Condition）]** ウィンドウに移動することもできます。

USB チェックは事前定義された条件で、Windows OS のみをサポートしています。

表 *164 : USB* 条件の設定

フィールド名	使用上のガイドライン
名前（**Name**）	USB_Check
説明	シスコの事前定義チェック
オペレーティング システム	Windows

フィールド名	使用上のガイドライン
コンプライアンス モジュール	バージョン 4.x 以降向けの、ISE のポスチャ準拠モジュールの表示専用フィールドのサポート。

関連トピック

単純ポスチャ条件 （1188 ページ）

ハードウェア属性条件の設定

[ポリシー（Policy）]>[ポリシー要素（Policy Elements）]>[ハードウェア属性条件（Hardware Attributes Condition）] を選択して、[ハードウェア属性条件（Hardware Attributes Condition）] ウィンドウにアクセスします。次の表では、[ハードウェア属性条件（Hardware Attributes Condition）] ウィンドウのフィールドについて説明します。

フィールド名	使用上のガイドライン
名前（Name）	Hardware_Attributes_Check：条件に割り当てられたデフォルトの名前。
説明	クライアントからハードウェア属性を収集するシスコの事前定義済みチェック。
オペレーティング システム	Windows すべてまたは Mac OS
コンプライアンス モジュール	4.x 以降

関連トピック

ハードウェア ダッシュボード （108 ページ）

ポスチャ ポリシーの設定

ポスチャ ポリシーは 1 つ以上の ID グループおよびオペレーティング システムに関連付けられたポスチャ要件の集合です。ディクショナリ属性は、デバイスの異なるポリシーを定義する、ID グループおよびオペレーティング システムと組み合わされたオプションの条件です。

Cisco ISE には、適合しないデバイスの猶予時間を設定するオプションが用意されています。デバイスが適合していないことが判明した場合、Cisco ISE はポスチャ評価結果キャッシュ内で以前の正常な状態を検索し、デバイスに猶予時間を与えます。デバイスには、猶予期間中にネットワークへのアクセス権が付与されます。分、時、または日単位（最大 30 日）で猶予期間を設定できます。

詳細については、『ISE Posture Prescriptive Deployment Guide』の「Posture Policy」の項を参照してください。

（注）
- デバイスの猶予期間中に、ポスチャ ポリシーで指定された猶予期間を更新した場合、次のようになります。
  - （猶予期間が延長された場合）以前の猶予期間が経過するかデバイスが Cisco ISE から削除されたときに、新しい猶予期間が適用されます。
  - （猶予期間が短縮された場合）デバイスがポスチャ フロー プロセスを再び流れた場合にのみ、新しい猶予期間がデバイスに適用されます。

（注） コンテキスト有用性エンドポイントは、クライアントが猶
であることを[コンプライアンスステータス（Compliance S
列に表示しません。準拠していると表示されます。

- 猶予期間は Temporal Agent には適用されません。
- （それぞれ異なる猶予期間を設定した）複数のポスチャ ポリシーにデバイスが一致する場合、それらの異なるポリシーで設定された最大の猶予期間がデバイスに与えられます。
- デバイスが猶予期間になると、アクセプタブル ユース ポリシー（AUP）は表示されません。

始める前に

- AUP について理解している必要があります。
- 定期的再評価（PRA）について理解している必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[ポスチャ（Posture）]** または **[ワーク センター（Work Centers）]** > **[ポスチャ（Posture）]** > **[ポスチャ ポリシー（Posture Policy）]** を選択します。

ステップ 2 ドロップダウンの矢印を使用して新しいポリシーを追加します。

ステップ 3 プロファイルを編集するには、ポリシーをダブルクリックするか、または行の末尾にある [編集（Edit）] をクリックします。

ステップ 4 [ルールステータス（Rule Status）] ドロップダウン リストで [有効（Enabled）] または [無効（Disabled）] を選択します。

ステップ 5 [ポリシーオプション（Policy Options）] でドロップダウンを選択し、[猶予期間の設定（Grace Period Settings）] を分単位、時間単位、日単位で指定します。

有効な値は次のとおりです。

- 1 ～ 30 日
- 1 ～ 720 時間

- 1 ～ 43200 分

デフォルトでは、この設定は無効です。

ステップ 6 （オプション）[遅延通知（Delayed Notification）] という名前のスライダをドラッグし、猶予期間の特定の割合が過ぎるまで、猶予期間プロンプトがユーザに遅れて表示されるようにします。たとえば、通知遅延期間が 50 % に設定され、設定されている猶予期間が 10 分の場合、Cisco ISE は 5 分後にポスチャ ステータスをチェックし、エンドポイントが準拠していないと判断した場合は猶予期間通知を表示します。エンドポイントのステータスが準拠している場合、猶予期間通知は表示されません。通知遅延期間が 0 % に設定されている場合は、猶予期間の開始時に直ちに問題の解決を促すメッセージが表示されます。ただし、エンドポイントは、猶予期間の有効期限が切れるまで、アクセス権が付与されます。このフィールドのデフォルト値は 0% です。有効な範囲は 0 ～ 95% です。

ステップ 7 [ルール名（Rule Name）] フィールドに、ポリシーの名前を入力します。

（注） 予期しない結果を回避するためのベストプラクティスは、各要件でポスチャ ポリシーを個別のルールとして設定することです。

ステップ 8 [IDグループ（Identity Groups）] 列から任意の ID グループを選択します。

ユーザまたはエンドポイントの ID グループに基づいて、ポスチャ ポリシーを作成することができます。

ステップ 9 [オペレーティングシステム（Operating Systems）] 列からオペレーティング システムを選択します。

ステップ 10 [準拠モジュール（Compliance Module）] 列から必要な準拠モジュールを選択します。

- 4.x 以降（4.x or Later）：マルウェア対策、ディスク暗号化、Patch Management、および USB の各種条件をサポートします。
- 3.x 以前（3.x or Earlier）：ウイルス対策、スパイウェア対策、ディスク暗号化、および Patch Management の各種条件をサポートします
- すべてのバージョン（Any Version）：ファイル、サービス、レジストリ、アプリケーション、および複合の各種条件をサポートします。

ステップ 11 [ポスチャタイプ（Posture Type）] 列から、[ポスチャタイプ（Posture Type）] を選択します。

- [AnyConnect]：AnyConnect エージェントを展開し、クライアントとのやりとりが必要な Cisco ISE ポリシーを監視し、適用します。
- [AnyConnect ステルス（AnyConnect Stealth）]：AnyConnect エージェントを展開し、クライアントとやりとりしない Cisco ISE ポスチャ ポリシーを監視し、適用します。
- [Temporal Agent]：準拠のステータスを確認するためにクライアント上で実行される一時実行可能ファイル。

ステップ 12 [その他の条件（Other Conditions）] では、1 つ以上のディクショナリ属性を追加し、単純条件または複合条件としてディクショナリに保存できます。

（注） [ポスチャポリシー（Posture Policy）] ウィンドウで作成したディクショナリ単純条件とディクショナリ複合条件は、許可ポリシーを設定するときには表示されません。

ステップ 13 [要件（Requirements）] フィールドに要件を指定します。
ステップ 14 [**保存（Save**）] をクリックします。

AnyConnect のワークフローの設定

AnyConnect エージェントを設定するには、Cisco ISE で次の手順を実行します。

ステップ 1 AnyConnect エージェントプロファイルを作成します。
ステップ 2 AnyConnect パッケージの AnyConnect 設定を作成します。
ステップ 3 クライアント プロビジョニング ポリシーを作成します。
ステップ 4 （任意）カスタムポスチャを作成します。
ステップ 5 （任意）カスタム修復アクションを作成します。
ステップ 6 （任意）カスタムポスチャの要件を作成します。
ステップ 7 ポスチャポリシーを作成します。
ステップ 8 クライアント プロビジョニング ポリシーを設定します。
ステップ 9 認証プロファイルを作成します。
ステップ 10 認証ポリシーを設定します。

証明書ベースの条件のための前提条件

クライアント プロビジョニングおよびポスチャ ポリシーのルールに、証明書の属性に基づく条件を含めることができます。クライアント プロビジョニングまたはポスチャ ポリシーにおける証明書ベースの条件では、同じ証明書属性に基づいて一致する許可ポリシー ルールが存在することが前提条件になります。

たとえば、図に示されているように同じ属性を使用する必要があります。[発行者 - 共通名（Issuer – Common Name）] 属性が、クライアント プロビジョニングまたはポスチャと許可ポリシーの両方で使用されています。

図 *68 : Cisco* のプロビジョニング ポリシー

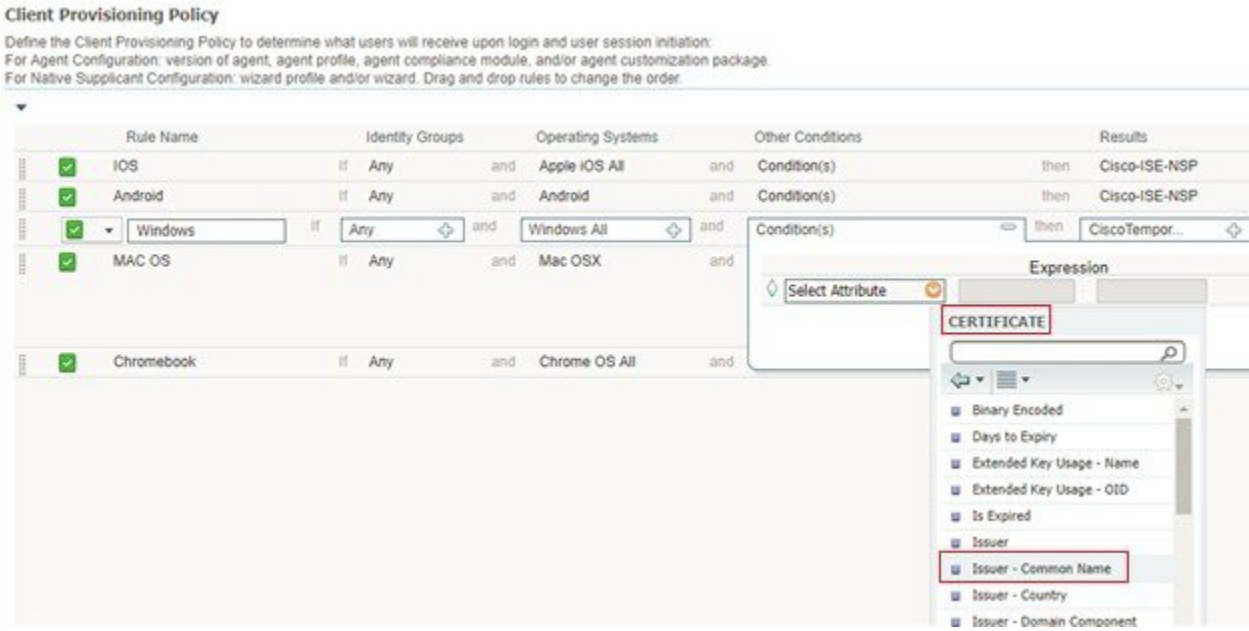
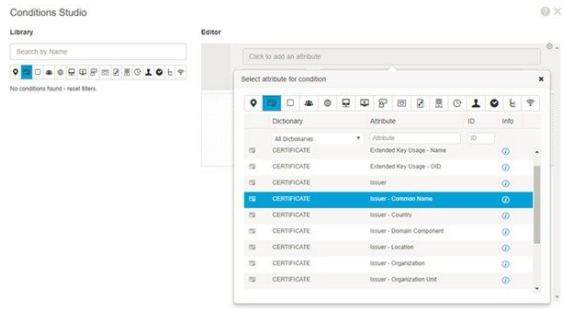


図 *69 : [*条件スタジオ（***Conditions Studio***）*]*



（注） ISE サーバ証明書は、AnyConnect 4.6 MR2 以降のシステム証明書ストアで信頼できる必要があります。昇格権限を必要とするポスチャ チェックおよび修復は、サーバが信頼されていない場合は機能しません。

- Windows OS：サーバ証明書をシステム証明書ストアに追加する必要があります。
- MAC OS：サーバ証明書をシステム キーチェーンに追加する必要があります。コマンドライン ユーティリティを使用して証明書を信頼することをお勧めします。キーチェーン アクセス アプリケーションを使用してシステム キーチェーンに証明書を追加しても、ログイン キーチェーンにすでに存在する場合は機能しないことがあります。

デフォルトのポスチャ ポリシー

Cisco ISE ソフトウェアには、ポスチャ ポリシーおよびプロファイルの作成を容易にする、事前設定されたポスチャ ポリシー（[ポリシー（Policy）]>[ポスチャ（Posture）]）が多数用意されています。これらのポリシーは、デフォルトで無効になっています。要件に基づいて、これらのポリシーを有効にできます。以下は、デフォルトのポスチャ ポリシーの一部です。

ルール名	説明	要件
Default_Antimalware_Policy_Mac	エンドポイントに、サポートされているベンダーのマルウェア対策ソフトウェア（AnyConnect で認識されているもの）がインストールされ、デバイスで実行されているかどうかを確認します。	Any_AM_Installation
Default_Antimalware_Policy_Win	エンドポイントに、サポートされているベンダーのマルウェア対策ソフトウェア（AnyConnect で認識されているもの）がインストールされ、デバイスで実行されているかどうかを確認します。	Any_AM_Installation_Win
Default_AppVis_Policy_Mac	情報を収集し、特定のエンドポイントにインストールされているすべてのアプリケーションを報告します。	Default_AppVis_Requirement_Mac
Default_AppVis_Policy_Win	情報を収集し、特定のエンドポイントにインストールされているすべてのアプリケーションを報告します。	Default_AppVis_Requirement_Win
Default_Firewall_Policy_Mac	エンドポイントに、サポートされているベンダーのファイアウォール プログラム（AnyConnect で認識されているもの）がインストールされているかどうかを確認します。	Default_Firewall_Requirement_Mac

ルール名	説明	要件
Default_Firewall_Policy_Win	エンドポイントに、サポートされているベンダーのファイアウォール プログラム（AnyConnect で認識されているもの）がインストールされているかどうかを確認します。	Default_Firewall_Requirement_Win
Default_USB_Block_Win	エンドポイント デバイスに USB ストレージ デバイスが接続されていないことを確認します。	USB_Block

クライアント ポスチャ評価

Cisco ISE を使用すると、適用されたネットワーク セキュリティ対策の適切さと効果を維持するために、保護されたネットワークにアクセスする任意のクライアントマシンに対してセキュリティ機能を検証し、そのメンテナンスを行うことができます。Cisco ISE 管理者は、クライアントマシンで最新のセキュリティ設定またはアプリケーションを使用できるよう設計されたポスチャ ポリシーを使用することによって、どのクライアント マシンでも、企業ネットワークへのアクセスについて定義されたセキュリティ標準を満たし、その状態を継続することを保証できます。ポスチャ コンプライアンス レポートによって、ユーザがログインしたとき、および定期的再評価が行われるたびに、クライアントマシンのコンプライアンス レベルのスナップショットが Cisco ISE に提供されます。

ポスチャ評価およびコンプライアンスは、Cisco ISE で提供される次のいずれかのエージェント タイプを使用して行われます。

- AnyConnect ISE Agent：Windows または Mac OS X クライアントにインストールできる永続的なエージェントであり、ポスチャ コンプライアンス機能を実行します。
- Cisco Temporal Agent：コンプライアンス ステータスを確認するためにクライアント上で実行される一時実行可能ファイル。エージェントは、ログインセッションが終了した後にクライアント マシンから削除されます。デフォルトでは、エージェントは Cisco ISE ISO イメージに存在し、インストール中に Cisco ISE にアップロードされます。

ポスチャ評価オプション

次の表に、Windows および Macintosh の ISE Posture Agent、および Windows の Web Agent でサポートされるポスチャ評価（ポスチャ条件）オプションのリストを示します。

表 *165 :* ポスチャ評価オプション

Windows 用 ISE ポスチャ エージェント	Windows 用 Cisco Temporal エージェント	Macintosh OS X 用 ISE ポスチャ エージェント	Macintosh OS X 用 Cisco Temporal エージェント
オペレーティング システム/サービス パック/ホットフィックス	—	—	—
サービス チェック	サービス チェック（Temporal エージェント 4.5 および ISE 2.3）	サービス チェック（AC 4.1 および ISE 1.4）	デーモン チェックはサポートされていません
レジストリ チェック	レジストリ チェック（Temporal エージェント 4.5 および ISE 2.3）	—	—
ファイル チェック	ファイル チェック（Temporal エージェント 4.5 および ISE 2.3）	ファイル チェック（AC 4.1 および ISE 1.4）	ファイル チェック（Temporal エージェント 4.5 および ISE 2.3）
アプリケーション チェック	アプリケーション チェック（Temporal エージェント 4.5 および ISE 2.3）	アプリケーション チェック（AC 4.1 および ISE 1.4）	アプリケーション チェック（Temporal エージェント 4.5 および ISE 2.3）
アンチウイルスのインストール	マルウェア対策のインストール	アンチウイルスのインストール	マルウェア対策のインストール
アンチウイルス バージョン/アンチウイルス定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチウイルス バージョン/アンチウイルス定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
アンチスパイウェアのインストール	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチスパイウェアのインストール	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます

Windows 用 ISE ポスチャ エージェント	Windows 用 Cisco Temporal エージェント	Macintosh OS X 用 ISE ポスチャ エージェント	Macintosh OS X 用 Cisco Temporal エージェント
アンチスパイウェア バージョン/アンチスパイウェア定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます	アンチスパイウェア バージョン/アンチスパイウェア定義日	OPSWAT バージョン 4 が使用されますが、そのためウイルス対策/スパイウェア対策はサポートされません。マルウェア対策のみがサポートされます
パッチ管理チェック（AC 4.1 および ISE 1.4）	パッチ管理のインストールのみチェック	パッチ管理チェック（AC 4.1 および ISE 1.4）	—
実行中の Windows Update	—	—	—
Windows Update の設定	—	—	—
WSUS のコンプライアンス設定	—	—	—

ポスチャ修復オプション

次の表に、Windows および Macintosh の ISE Posture Agent、および Windows の Web Agent でサポートされる修復オプション（ポスチャ条件）のリストを示します。

表 *166* : ポスチャ修復オプション

ISE ポスチャ エージェント Windows	ISE ポスチャ エージェント Macintosh OS X
メッセージ テキスト（ローカル チェック）	メッセージ テキスト（ローカル チェック）
URL リンク（リンク分散）	URL リンク（リンク分散）
ファイル配布	—
プログラム起動	—
アンチウイルス定義更新	アンチウイルス ライブ更新
アンチスパイウェア定義更新	アンチスパイウェア ライブ更新
パッチ管理修復（AC 4.1 および ISE 1.4）	—
Windows Update	—

ISE ポスチャ エージェント Windows	ISE ポスチャ エージェント Macintosh OS X
WSUS	—

ISE Community Resource
Cisco ISE and SCCM integration Reference Guide

ポスチャのカスタム条件

ポスチャ条件は次の単純条件のいずれかになります。ファイル、レジストリ、アプリケーション、サービス、またはディクショナリ条件。これらの単純条件のうちの1つ以上の条件によって複合条件が形成され、複合条件はポスチャ要件と関連付けることができます。

最初のポスチャ更新の後に、Cisco ISE もシスコ定義の単純条件と複合条件を作成します。シスコ定義の単純条件では pc_ as が使用され、複合条件では pr_ as が使用されます。

ユーザ定義の条件またはシスコ定義の条件には、単純条件と複合条件の両方が含まれます。

ポスチャ サービスは、アンチウイルスおよびアンチスパイウェア（AV/AS）複合条件に基づいた内部チェックを使用します。このため、ポスチャ レポートは、作成した正確な AV/AS 複合条件名を反映しません。レポートには、AV/AS 複合条件の内部チェックの名前だけが表示されます。

たとえば、任意のベンダーおよび製品をチェックする「MyCondition_AV_Check」という名前の AV 複合条件を作成した場合、ポスチャ レポートには、条件名として、「MyCondition_AV_Check」ではなく、内部チェック「av_def_ANY」が表示されます。

ポスチャ エンドポイントのカスタム属性

ポスチャ エンドポイントのカスタム属性を使用して、クライアント プロビジョニングおよびポスチャ ポリシーを作成できます。最大100個のエンドポイントのカスタム属性を作成できます。以下のタイプのエンドポイント カスタム属性がサポートされています：Int、String、Long、Boolean、Float、IP、および Date。

エンドポイント カスタム属性は、特定の属性に基づいてデバイスをホワイトリスト登録またはブラックリスト登録するために使用することも、ポスチャまたはクライアント プロビジョニング ポリシーに基づいて特定の権限を割り当てるために使用することもできます。

エンドポイント カスタム属性を使用したポスチャ ポリシーの作成

エンドポイント カスタム属性を使用してポスチャ ポリシーを作成するには、次の手順を実行します。

ステップ 1 エンドポイント カスタム属性を作成します。

a) **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント カスタム属性（Endpoint Custom Attributes）]** の順に選択します。

b) [エンドポイント カスタム属性（Endpoint Custom Attributes）] 領域に、[属性名（Attribute Name）]（たとえば、deviceType）と [データ型（Data Type）]（たとえば、String）を入力します。

c) [保存（Save）] をクリックします。

ステップ 2 カスタム属性に値を割り当てます。

a) [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] の順に選択します。

b) カスタム属性値を割り当てます。

- 必要な MAC アドレスのチェックボックスをオンにし、[編集（Edit）] をクリックします。
- または、必要なMACアドレスをクリックし、[エンドポイント（Endpoints）]ページで[編集（Edit）] をクリックします。

c) 作成したカスタム属性が、[エンドポイントの編集（Edit Endpoint）] ダイアログボックスの [カスタム属性（Custom Attributes）] 領域に表示されていることを確認します。

d) [編集（Edit）] をクリックし、必要な属性値を入力します（たとえば、deviceType = Apple-iPhone）。

e) [保存（Save）] をクリックします。

ステップ 3 カスタム属性と値を使用してポスチャ ポリシーを作成します。

a) [ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャ ポリシー（Posture Policy）] を選択します。

b) 必要なポリシーを作成します。[その他の条件（Other Conditions）] をクリックしてカスタム属性を選択し、必要なディクショナリを選択します（たとえば、ステップ 1 で作成したカスタム属性である [エンドポイント（Endpoints）] > [deviceType] を選択します）。詳細については、Cisco Temporal Agent のワークフローの設定 （1258 ページ） を参照してください。

c) [保存（Save）] をクリックします。

エンドポイント カスタム属性を使用してクライアント プロビジョニング ポリシーを作成するには、次の手順を実行します。

1. [ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [クライアント プロビジョニング（Client Provisioning）] > [クライアント プロビジョニング ポリシー（Client Provisioning Policy）] を選択します。

2. 必要なポリシーを作成します。
   - 必要なルールを作成します（たとえば、Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。
   - [その他の条件（Other Conditions）] をクリックして必要なディクショナリを選択して、カスタム属性を選択します。

カスタム ポスチャ修復アクション

カスタムポスチャ修復アクションは、ファイル、リンク、アンチウイルスまたはアンチスパイウェア定義の更新、プログラムの起動、Windows Update、Windows Server Update Services（WSUS）の修復タイプです。

ファイル修復の追加

ファイル修復により、クライアントはコンプライアンスに必要なファイルのバージョンをダウンロードできます。クライアントエージェントは、コンプライアンスのためにクライアントが必要とするファイルを使用してエンドポイントを修復します。

[ファイル修復（File Remediations）] ページでファイル修復をフィルタリング、表示、追加、または削除することはできますが、ファイル修復を編集することはできません。[ファイル修復（File Remediations）] ページには、すべてのファイル修復がそれらの名前と説明、および修復に必要なファイルとともに表示されます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] >** [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [ファイル修復（File Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [名前（Name）] フィールドに名前を入力し、[説明（Description）] フィールドにファイル修復の説明を入力します。

ステップ 6 [新規ファイル修復（New File Remediation）] ページで値を変更します。

ステップ 7 [送信（Submit）] をクリックします。

リンク修復の追加

リンク修復により、クライアントは修復ページまたはリソースにアクセスするための URL をクリックできます。クライアントエージェントはリンクを使用してブラウザを開き、クライアントはコンプライアンスのために自身を修復できます。

[リンク修復（Link Remediation）]ページには、すべてのリンク修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [リンク修復（Link Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規リンク修復（New Link Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

パッチ管理修復の追加

パッチ管理修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[パッチ管理修復（Patch Management Remediation）]ページには、修復タイプ、パッチ管理ベンダーの名前、およびさまざまな修復オプションが表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [パッチ管理修復（Patch Management Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [パッチ管理修復（Patch Management Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックして、[パッチ管理修復（Patch Management Remediation）] ページに修復アクションを追加します。

関連トピック

パッチ管理修復

アンチウイルス修復の追加

アンチウイルス修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AV 修復（AV Remediations）] ページには、すべてのアンチウイルス修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [AV 修復（AV Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 AV 修復（New AV Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

アンチスパイウェア修復の追加

アンチスパイウェア修復を作成して、修復後にコンプライアンスのために最新のファイル定義でクライアントを更新できます。

[AS 修復（AS Remediations）] ページには、すべてのアンチウイルス修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [AS 修復（AS Remediations）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 AS 修復（New AS Remediations）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

関連トピック

アンチスパイウェア修復

プログラム修復起動の追加

コンプライアンスのために、クライアントエージェントが 1 つ以上のアプリケーションを起動してクライアントを修復するプログラム修復起動を作成できます。

[プログラム修復起動（Launch Program Remediations）] ページには、すべてのプログラム修復起動がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [プログラム起動修復（Launch Program Remediation）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [新規プログラム修復起動（New Launch Program Remediation）] ページで値を変更します。
ステップ 6 [送信（Submit）] をクリックします。

プログラム修復起動のトラブルシューティング

問題

プログラム修復起動を使用して、アプリケーションを修復として起動すると、アプリケーションは正常に開始されます（Windows Task Manager で観察されます）が、アプリケーション UI は表示されません。

ソリューション

プログラム起動 UI アプリケーションはシステム権限で実行され、[インタラクティブサービス検出（ISD）（Interactive Service Detection (ISD)）] ウィンドウに表示されます。プログラム起動 UI アプリケーションを表示するには、次の OS で ISD をイネーブルにする必要があります。

- Windows Vista：ISD はデフォルトで停止状態になっています。services.msc で ISD サービスを起動して、ISD をイネーブルにします。
- Windows 7：ISD サービスはデフォルトでイネーブルになっています。
- Windows 8/8.1：レジストリ \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows で「NoInteractiveServices」を 1 から 0 に変更することで ISD をイネーブルにします。

Windows Update 修復の追加

[Windows Update 修復（Windows update remediations）] ページには、すべての Windows Update 修復がそれらの名前と説明、および修復のモードとともに表示されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > > **[ポスチャ（Posture）]** を選択します。
ステップ 2 [修復アクション（Remediation Actions）] をクリックします。
ステップ 3 [Windows Update 修復（Windows Update Remediation）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [新規 Windows Update 修復（New Windows Update Remediation）] ページで値を変更します。
ステップ 6 [送信（Submit）] をクリックします。

Windows Server Update Services 修復の追加

コンプライアンスのためにローカルに管理されているか、または Microsoft で管理されている WSUS サーバから最新の WSUS 更新を受信するように Windows クライアントを設定できます。Windows Server Update Services（WSUS）修復は、ローカルに管理されている WSUS サーバまたは Microsoft で管理されている WSUS サーバから最新の Windows サービス パック、ホットフィックス、およびパッチをインストールします。

クライアント エージェントをローカルの WSUS Agent と統合して、エンドポイントの WSUS 更新が最新かどうかをチェックする WSUS 修復を作成できます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > [ポスチャ（Posture）] を選択します。

ステップ 2 [修復アクション（Remediation Actions）] をクリックします。

ステップ 3 [Windows Server Update Service 修復（Windows Server Update Services Remediation）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [新規 Windows Server Update Service 修復（New Windows Server Update Services Remediation）] ページで値を変更します。

ステップ 6 [送信（Submit）] をクリックします。

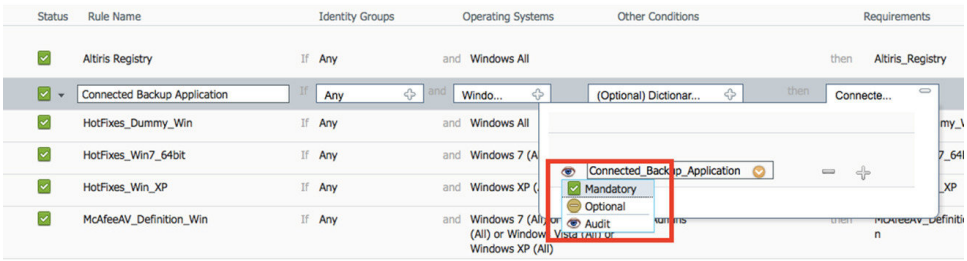
ポスチャ評価要件

ポスチャ要件は、ロールおよびオペレーティング システムとリンクできる修復アクションを伴う一連の複合条件です。ネットワークに接続しているすべてのクライアントは、ネットワークで適合ホストになるためにはポスチャ評価中に必須要件を満たす必要があります。

ポスチャ ポリシー要件は、ポスチャ ポリシーの必須、オプション、または監査タイプに設定できます。要件がオプションで、クライアントがこれらの要件を満たさない場合、クライアントにはエンドポイントのポスチャ評価中に続行するオプションがあります。

ポスチャ チェックは、必須、オプション、および監査の順に評価されます。必須のチェックが失敗すると、関連する監査チェックは実行されません。

図 *70*：ポスチャ ポリシーの要件タイプ



必須要件

ポリシーの評価時に、エージェントはポスチャ ポリシーに定義されている必須要件を満たすことができないクライアントに修復オプションを提供します。エンドユーザは、修復タイマー設定で指定された時間内に要件を満たすように修復する必要があります。

たとえば、絶対パス内にC:\temp\text.fileがあるかをチェックするために、ユーザ定義の条件を含む必須要件を指定したとします。ファイルがない場合、必須要件は失敗し、ユーザは [非準拠（Non-Compliant）] 状態になります。

オプション要件

ポリシーの評価時に、クライアントがポスチャ ポリシーに指定されたオプション要件を満たすことができない場合に、エージェントは続行するためのオプションをクライアントに提供します。エンドユーザは、指定されたオプション要件をスキップすることができます。

たとえば、Calc.exeなどのクライアントマシンで実行するアプリケーションをチェックするために、ユーザ定義の条件を含むオプション要件を指定したとします。クライアントが条件を満たすことができない場合、オプション要件がスキップされ、エンドユーザが[準拠（Compliant）] 状態になるように、さらに続行するためのオプションがエージェントによって促されます。

監査要件

監査要件は内部用に指定され、エージェントはポリシー評価時の合格または失敗のステータスに関係なく、メッセージやエンドユーザからの入力を促しません。

たとえば、エンドユーザにアンチウイルス プログラムの最新バージョンがあるかどうかを確認するために、必須のポリシー条件を作成中だとします。ポリシー条件として実際に適用する前に非準拠のエンドユーザを見つける場合は、その条件を監査要件として指定できます。

可視性要件

ポリシー評価の間に、エージェントが可視性要件のコンプライアンス データを 5 ～ 10 分ごとにレポートします。

非準拠ステートでスタックしたクライアント システム

クライアント マシンが必須要件を修復できない場合、ポスチャ ステータスは「非準拠」に変更され、エージェント セッションは隔離されます。クライアント マシンを「非準拠」状態から移行するには、エージェントがクライアントマシン上でポスチャ評価を再び開始するようにポスチャ セッションを再起動する必要があります。次のようにポスチャ セッションを再起動できます。

- 802.1X 環境での有線およびワイヤレス許可変更（CoA）：
  - [新しい許可プロファイル（New Authorization Profiles）] ページで新しい許可プロファイルを作成するときに、特定の許可ポリシーの再認証タイマーを設定できます。詳細については、20-11 ページの「ダウンロード可能 ACL の権限の設定」の項を参照してください。

- 有線ユーザは、ネットワークの接続を切断して再接続すると、隔離状態から移行できます。ワイヤレス環境では、ユーザは、ワイヤレス LAN コントローラ（WLC）から切断し、ユーザのアイドルタイムアウト時間が過ぎるまで待機してから、ネットワークへの再接続を試行する必要があります。

- VPN 環境：VPN トンネルを切断し、再接続します。

クライアントのポスチャ要件の作成

[要件（Requirements）] ページでは、ユーザ定義の条件とシスコ定義の条件、および修復アクションを関連付けて要件を作成できます。[要件（Requirements）] ページで作成および保存されたユーザ定義の条件および修復アクションは、それぞれのリスト ページに表示されます。

始める前に

- ポスチャの利用規定（AUP）について理解している必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]** を選択します。

ステップ 2 [要件（Requirements）] ページに値を入力します。

ステップ 3 読み取り専用モードでポスチャ要件を保存するには、[完了（Done）] をクリックします。

ステップ 4 [保存（**Save**）] をクリックします。

ポスチャ再評価の構成設定

次の表では、ポスチャ再評価の設定に使用できる [ポスチャ再評価設定（Posture Reassessment Configurations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]** です。

表 *167 :* ポスチャ再評価の構成設定

フィールド	使用上のガイドライン
構成名	PRA 設定の名前を入力します。
設定の説明（Configuration Description）	PRA 設定の説明を入力します。
再評価適用を使用?（Use Reassessment Enforcement?）	ユーザ ID グループの PRA 設定を適用するには、チェックボックスをオンにします。

フィールド	使用上のガイドライン
適用タイプ（Enforcement Type）	適用する次のアクションを選択します。 • [続行（Continue）]：ユーザはポスチャ要件に関係なくクライアントを修復できるようにユーザ介入なしの特権アクセスが引き続き提供されます。 • [ログオフ（Logoff）]：クライアントが非準拠の場合、ユーザを強制的にネットワークからログオフします。 クライアントが再度ログインしたときのコンプライアンス ステータスは不明です。 • [修復（Remediate）]：クライアントが非準拠の場合、エージェントは修復のために指定の期間待機します。 クライアントが修復された後、エージェントはポリシーサービス ノードにPRA レポートを送信します。修復がクライアントで無視された場合、エージェントはクライアントにネットワークからログオフすることを強制するために、ポリシーサービス ノードにログオフ要求を送信します。 ポスチャ要件が [必須（mandatory）] に設定されている場合、RADIUS セッションはPRA 障害アクションの結果としてクリアされ、クライアントを再びポスチャするには新しい RADIUS セッションを開始する必要があります。 ポスチャ要件が [任意（Optional）] に設定されている場合、クライアント上のエージェントではユーザがエージェントから [続行（Continue）] オプションをクリックできます。ユーザは、制限なしで現在のネットワークにとどまることができます。
インターバル（Interval	最初のログイン成功後にクライアントで PRA を開始する間隔を分単位で入力します。 デフォルト値は 240 分です。最小値は 60 分、最大値は 1440 分です。

フィールド	使用上のガイドライン
猶予時間（Grace time）	クライアントが修復を完了することのできる時間間隔を分単位で入力します。猶予時間をゼロにすることはできません。また、PRA 間隔より大きくする必要があります。デフォルトの最小間隔（5 分）から最小 PRA 間隔までの範囲にすることができます。 最小値は 5 分、最大値は 60 分です。 （注） 猶予時間は、クライアントがポスチャの再評価に失敗した後、適用タイプが修復アクションに設定されている場合にだけ有効です。
ユーザ ID グループの選択（Select User Identity Groups）	PRA設定に対して一意のグループまたはグループの一意の組み合わせを選択します。
PRA の設定（PRA configurations）	既存の PRA 設定と PRA 設定に関連付けられたユーザ ID グループを表示します。

関連トピック

ポスチャのリース （1178 ページ）
定期的再評価 （1179 ページ）
ポスチャ評価オプション
ポスチャ修復オプション （1240 ページ）
ポスチャのカスタム条件 （1241 ページ）
カスタム ポスチャ修復アクション （1243 ページ）
定期的再評価の設定 （1180 ページ）

ポスチャのカスタム権限

カスタム権限は、Cisco ISE で定義する標準許可プロファイルです。標準許可プロファイルは、エンドポイントの一致するコンプライアンス ステータスに基づいてアクセス権を設定します。ポスチャ サービスでは、ポスチャは大きく不明プロファイル、準拠プロファイル、および非準拠プロファイルに分類されます。ポスチャ ポリシーおよびポスチャ要件によって、エンドポイントのコンプライアンス ステータスが決まります。

VLAN、DACL および他の属性値ペアの異なるセットを持つことができるエンドポイントの不明、準拠、および非準拠のポスチャ ステータスに対して 3 つの異なる許可プロファイルを作成する必要があります。これらのプロファイルは、3 つの異なる許可ポリシーに関連付けることができます。これらの許可ポリシーを区別するために、Session:PostureStatus 属性を他の条件とともに使用できます。

不明プロファイル

エンドポイントに一致するポスチャ ポリシーが定義されていない場合、そのエンドポイントのポスチャ コンプライアンス ステータスは不明に設定されることがあります。不明のポスチャ コンプライアンス ステータスは、一致するポスチャ ポリシーが有効であるが、エンドポイントに対してポスチャ評価がまだ行われておらず、従ってクライアント エージェントによってコンプライアンス レポートが提供されていないエンドポイントにも適用できます。

準拠プロファイル

エンドポイントに一致するポスチャ ポリシーが定義されている場合、そのエンドポイントのポスチャ コンプライアンス ステータスは準拠に設定されます。ポスチャ評価が行われると、エンドポイントは、一致するポスチャ ポリシー内に定義されているすべての必須要件を満たします。準拠とポスチャされているエンドポイントには、ネットワークに対する特権ネットワーク アクセスを付与できます。

非準拠プロファイル

エンドポイントのポスチャ コンプライアンス ステータスが非準拠に設定されるのは、そのエンドポイントに対して一致するポスチャ ポリシーが定義されているが、ポスチャ評価の実行中にすべての必須要件を満たすことができない場合です。非準拠としてポスチャされたエンドポイントは、修復アクションを含むポスチャ要件に一致し、自らを修復するために修復リソースへ制限付きのネットワーク アクセスが付与される必要があります。

標準許可ポリシーの設定

[許可ポリシー（Authorization Policy）] ページでは、標準許可ポリシーと例外許可ポリシーの 2 種類の許可ポリシーを定義できます。ポスチャに固有の標準許可ポリシーは、エンドポイントのコンプライアンス ステータスに基づいて、ポリシー決定を行うために使用されます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択します。

ステップ 2 [ビュー（View）] 列で、対応するデフォルトポリシーに隣接する矢印アイコンをクリックします。

ステップ 3 [アクション（Actions）] 列で、歯車アイコンをクリックし、ドロップダウン リストから新しい認証ポリシーを選択します
[ポリシーセット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 4 着信サービス名を入力します。

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性を選択します。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 7 [使用（Use）] をクリックして、読み取り専用モードで新しい標準許可ポリシーを作成します。
ステップ 8 [保存（**Save**）] をクリックします。

ポスチャとネットワーク ドライブ マッピングのベスト プラクティス

Windows エンドポイントのポスチャ アセスメント実行中に、エンドポイント ユーザがデスクトップへのアクセスするときに遅延が生じることがあります。これは、Windows でユーザがデスクトップにアクセスできるようにする前に、ファイル サーバのドライブ文字のマッピングを復元しようとすることが原因で発生する場合があります。ポスチャ実行中の遅延を防ぐためのベスト プラクティスを次に示します。

- ファイル サーバ ドライブ文字をマッピングするときには AD にアクセスする必要があるため、エンドポイントは Active Directory サーバにアクセスできる必要があります。（AnyConnect ISE ポスチャ エージェントを使用した）ポスチャがトリガーされると、AD へのアクセスがブロックされ、これが原因でログインが遅延します。ポスチャが完了する前に、ポスチャ修復 ACL を使用して AD サーバへのアクセスを提供します。
- ポスチャ完了までのログイン スクリプトの遅延を設定し、その後 Persistence 属性を NO に設定する必要があります。Windows はログイン中にすべてのネットワーク ドライブへの再接続を試行しますが、AnyConnect ISE ポスチャ エージェントが完全なネットワーク アクセスを得るまでは、この操作を完了できません。

AnyConnect ステルス モードのワークフローの設定

ステルス モードでの AnyConnect の設定プロセスには、一連の手順があります。Cisco ISE で次の手順を実行する必要があります。

ステップ 1 AnyConnect エージェント プロファイルを作成します。「AnyConnect エージェント プロファイルの作成」を参照してください。
ステップ 2 AnyConnect パッケージの AnyConnect 設定を作成します。「AnyConnect パッケージの AnyConnect 設定の作成」を参照してください。
ステップ 3 Cisco ISE でオープン DNS プロファイルをアップロードします。「Cisco ISE へのオープン DNS プロファイルのアップロード」を参照してください。
ステップ 4 クライアント プロビジョニング ポリシーを作成します。「クライアント プロビジョニング ポリシーの作成」を参照してください。
ステップ 5 ポスチャ条件を作成します。「ポスチャ条件の作成」を参照してください。
ステップ 6 ポスチャ修復を作成します。「ポスチャ修復の作成」を参照してください。

ステップ 7 クライアントレスモードでポスチャ要件を作成します。「ステルス モードでのポスチャ要件の作成」を参照してください。

ステップ 8 ポスチャ ポリシーを作成します。「ポスチャ ポリシーの作成」を参照してください。

ステップ 9 認証プロファイルを設定します。

a) **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。

b) [追加（Add）] をクリックして、プロファイルの [名前（Name）] に入力します。

c) [共通タスク（Common Tasks）] で、[Web リダイレクション（CWA、MDM、NSP、CPP）（Web Redirection (CWA, MDM, NSP, CPP)）] を有効にし、ドロップダウンリストから [クライアント プロビジョニング（ポスチャ）（Client provisioning (Posture)）] を選択し、リダイレクト [ACL] の名前を入力して、[クライアント プロビジョニング ポータル（Client Provisioning Portal）] 値を選択します。新しいクライアント プロビジョニング ポータルは、**[ワークセンター（Work Centers）]** > **[ポスチャ（Posture）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[クライアント プロビジョニング ポータル（Client Provisioning Portal）]** で編集または作成できます。

ステップ 10 許可ポリシーを設定します。

a) **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択します。

b) [>] をクリックして [認可ポリシー（Authorization Policy）] を選択し、[+] アイコンをクリックして **Session:Posture Status EQUALS Unknown** と以前に設定した認証プロファイルが備わっている新しいルールを作成します。

c) 以前のルールの上に、**Session:Posture Status EQUALS NonCompliant** 条件を備えた新しい認証ルールと、**Session:Posture Status EQUALS Compliant** 条件を備えた別の新しい認証ルールを作成します

AnyConnect エージェント プロファイルの作成

始める前に

Mac および Windows OS 用の AnyConnect Cisco パッケージおよび AnyConnect 準拠モジュールをアップロードする必要があります。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアントプロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** ページを選択します。

ステップ 2 [追加（Add）] ドロップダウンリストから、**[NAC エージェントまたは AnyConnect ポスチャプロファイル（NAC Agent or AnyConnect Posture Profile）]**を選択します。

ステップ 3 [ポスチャ エージェント プロファイルの設定（Posture Agent Profile Settings）] ドロップダウンリストから [AnyConnect] を選択します。

ステップ 4 [名前（Name）] フィールドに、目的の名前（たとえば、AC_Agent_Profile）を入力します。

ステップ 5 [エージェントの動作（Agent Behavior）] セクションでは、[ステルス モード（Stealth Mode）] パラメータで[クライアントレス（Clientless）][有効（Enabled）] を選択します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

AnyConnect パッケージの AnyConnect 設定を作成する必要があります。

AnyConnect パッケージの AnyConnect 設定の作成

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** ページに移動します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[AnyConnect 設定（AnyConnect Configuration）] を選択します。

ステップ 3 [AnyConnect パッケージの選択（Select AnyConnect Package）] ドロップダウン リストから、必要な AnyConnect パッケージを選択します（AnyConnectDesktopWindows 4.4.117.0 など）。

ステップ 4 [設定名（Configuration Name）] テキスト ボックスに、必要な名前を入力します（AC_Win_44117 など）。

ステップ 5 [コンプライアンス モジュール（Compliance Module）] ドロップダウン リストで、必要なコンプライアンス モジュールを選択します（AnyConnectComplianceModuleWindows 4.2.437.0 など）。

ステップ 6 [AnyConnect モジュール選択（AnyConnect Module Selection）] セクションで、[ISE ポスチャ（ISE Posture）] と [ネットワーク アクセス マネージャ（Network Access Manager）] のチェック ボックスにマークを付けます。

ステップ 7 [プロファイル選択（Profile Selection）] セクションの [ISE ポスチャ（ISE Posture）] ドロップダウン リストで、AnyConnect エージェント プロファイルを選択します（AC_Agent_Profile など）。

ステップ 8 [ネットワーク アクセス マネージャ（Network Access Manager）] ドロップダウン リストから、必要な AnyConnect エージェント プロファイルを選択します（AC_Agent_Profile など）。

次のタスク

クライアントにプッシュされるオープン DNS プロファイルをアップロードする必要があります。

Cisco ISE へのオープン DNS プロファイルのアップロード

オープン DNS プロファイルがクライアントにプッシュされます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** ページに移動します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[ローカル ディスクのエージェント リソース（Agent Resources From Local Disk）] を選択します。

ステップ 3 [カテゴリ（Category）] ドロップダウン リストから [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 4 [タイプ（Type）] ドロップダウン リストから、[AnyConnect プロファイル（AnyConnect Profile）] を選択します。

ステップ 5 [名前（Name）] テキスト ボックスに、目的の名前（たとえば、OpenDNS）を入力します。

ステップ 6 [参照（Browse）] をクリックして、ローカル ディスクから JSON ファイルを見つけます。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

クライアント プロビジョニング ポリシーを作成する必要があります。

クライアント プロビジョニング ポリシーの作成

ステップ 1 **[ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）]** ページに移動します。

ステップ 2 必要なルールを作成します（たとえば、Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117）。

次のタスク

ポスチャ条件を作成する必要があります。

ポスチャ条件の作成

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ファイル条件（File Condition）]** の順に移動します。

ステップ 2 必要な名前を入力します（filechk など）。

ステップ 3 [オペレーティング システム（Operating Systems）] ドロップダウン リストから、[Windows 7（すべて）（Windows 7 (All)）] を選択します。

ステップ 4 [ファイル タイプ（File Type）] ドロップダウン リストから、[FileExistence] を選択します。

ステップ 5 [ファイル パス（File Path）] ドロップダウン リストから、[ABSOLUTE_PATH C:\test.txt] を選択します。

ステップ 6 [ファイル演算子（File Operator）] ドロップダウン リストから、[DoesNotExist] を選択します。

次のタスク

ポスチャ修復を作成する必要があります。

ポスチャ修復の作成

ファイル条件により、test.txtファイルがエンドポイントに存在するかどうかが確認されます。存在しない場合の修復は、USB ポートをブロックし、USB デバイスを使用したファイルのインストールを防止することです。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[修復アクション（Remediation Actions）]** > **[USB 修復（USB Remediations）]** ページに移動します。

ステップ 2 必要な名前を入力します（clientless_mode_block など）。

ステップ 3 [送信（Submit）] をクリックします。

次のタスク

ポスチャ要件を作成する必要があります。

ステルス モードでのポスチャ要件の作成

[要件（Requirements）] ページから修復アクションを作成する際は、ステルス モードに適した次の修復だけが表示されます：[マルウェア対策（Anti-Malware）]、[プログラム起動（Launch Program）]、[パッチ管理（Patch Management）]、[USB]、[Windows Server Update Services]、および [Windows Update]。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** ページに移動します。

ステップ 2 ポスチャの必須要件を作成します（たとえば、Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=AnyConnect Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block）。

次のタスク

ポスチャ ポリシーを作成する必要があります。

ポスチャ ポリシーの作成

始める前に

ポスチャ ポリシーの要件およびポリシーがクライアントレス モードで作成されていることを確認してください。

ステップ 1 **[ポリシー（Policy）]** > **[ポスチャ（Posture）]** を選択します。

ステップ 2 必要なルールを作成します。たとえば、Identity Groups=Any and Operating Systems=Windows 7(All) および Compliance Module=4.x or late および Posture Type=AnyConnect Stealth の場合、Requirements=win7Req となります。

（注） URL リダイレクションのないクライアント プロビジョニングの場合、ネットワーク アクセスまたはRADIUS に固有の属性を使用して条件を設定しても条件は機能せず、Cisco ISE サーバで特定ユーザのセッション情報が使用可能ではないことが原因で、クライアント プロビジョニング ポリシーの照合が失敗することがあります。ただし、Cisco ISE では外部で追加された ID グループに対して条件を設定できます。

AnyConnect ステルス モード通知の有効化

Cisco ISE では AnyConnect ステルス モード展開に対し、いくつかの新しい障害の発生通知を提供します。ステルス モードでの障害の発生通知を有効にすると、有線、ワイヤレスまたはVPN 接続で問題を特定できます。ステルス モードでの通知を有効にするには、次のようにします。

（注） AnyConnect バージョン 4.5.0.3040 以降は、ステルスモードでの通知をサポートします。

始める前に

ステルス モードで AnyConnect を設定します。

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] を選択します。

ステップ 2 [追加（Add）] > **[NAC Agent またはAnyConnect ISE ポスチャプロファイル（NAC Agent or AnyConnect ISE Posture Profile）]** を選択します。

ステップ 3 [カテゴリの選択（Select a Category）] ドロップダウン リストから [AnyConnect] を選択します。

ステップ 4 [エージェントの動作（Agent Behavior）] セクションで、[ステルスモードで通知を有効にする（Enable notifications in stealth mode）] オプションに [有効（Enabled）] を選択します。

Cisco Temporal Agent のワークフローの設定

Cisco temporal agent を設定するプロセスには、一連の手順があります。Cisco ISE で次の手順を実行する必要があります。

ステップ 1 ポスチャ条件の作成

ステップ 2 ポスチャ要件の作成

ステップ 3 ポスチャ ポリシーの作成

ステップ 4 クライアント プロビジョニング ポリシーの設定

ステップ 5 認証プロファイルを設定します。

a) **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。

b) [追加（Add）] をクリックして、プロファイルの [名前（Name）] に入力します。

c) [共通タスク（Common Tasks）] で、[Web リダイレクション（CWA、MDM、NSP、CPP）（Web Redirection (CWA, MDM, NSP, CPP)）] を有効にし、ドロップダウンリストから [クライアント プロビジョニング（ポスチャ）（Client provisioning (Posture)）] を選択し、リダイレクト [ACL] の名前を入力して、[クライアントプロビジョニング ポータル（Client Provisioning Portal）] 値を選択します。新しいクライアント プロビジョニング ポータルは、**[ワークセンター（Work Centers）]** > **[ポスチャ（Posture）]** > **[クライアント プロビジョニング（Client Provisioning）]** > **[クライアント プロビジョニング ポータル（Client Provisioning Portal）]** で編集または作成できます。

ステップ 6 許可ポリシーを設定します。

a) **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択します。

b) [>] をクリックして [認可ポリシー（Authorization Policy）] を選択し、[+] アイコンをクリックして **Session:Posture Status EQUALS Unknown** と以前に設定した認証プロファイルが備わっている新しいルールを作成します。

c) 以前のルールの上に、**Session:Posture Status EQUALS NonCompliant** 条件を備えた新しい認証ルールと、**Session:Posture Status EQUALS Compliant** 条件を備えた別の新しい認証ルールを作成します

ステップ 7 Cisco Temporal Agent のダウンロードと起動

ポスチャ条件の作成

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[ポスチャ（Posture）]** > **[ファイル条件（File Condition）]** の順に移動します。

ステップ 2 必要な名前を入力します（filecondwin など）。

ステップ 3 [オペレーティング システム（Operating Systems）] ドロップダウン リストから、[Windows 7（すべて）（Windows 7 (All)）] を選択します。

ステップ 4 [ファイル タイプ（File Type）] ドロップダウン リストから、[FileExistence] を選択します。

ステップ 5 [ファイル パス（File Path）] ドロップダウン リストから、[ABSOLUTE_PATH C:\test.txt] を選択します。

ステップ 6 [ファイル演算子（File Operator）] ドロップダウン リストから、[DoesNotExist] を選択します。

ポスチャ要件の作成

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[ポスチャ（Posture）]** > **[要件（Requirements）]** を選択します。

ステップ 2 [編集（Edit）] ドロップダウンリストから、[新しい要件の挿入（Insert New Requirement）] を選択します。

ステップ 3 [名前（Name）]、[オペレーティング システム（Operating Systems）]、および [コンプライアンス モジュール（Compliance Module）] を入力します（たとえば、Name filereqwin、Operating Systems Windows All、Compliance Module 4.x or later）。

ステップ 4 [ポスチャ タイプ（Posture Type）] ドロップダウンで、[Temporal Agent] を選択します。

ステップ 5 必要な条件（たとえば、filecondwin）を選択します。

（注） Cisco Temporal Agent の場合は、[要件（Requirements）] ページで [インストール（Installation）] チェック タイプを含むパッチ管理条件のみを表示できます。

ステップ 6 [メッセージ テキストのみ（Message Text Only）] 修復アクションを選択します。

（注） 一時エージェントは、AnyConnect 4.x 以降でサポートされています。

ポスチャ ポリシーの作成

ステップ 1 **[ポリシー（Policy）]** > **[ポスチャ（Posture）]** を選択します。

ステップ 2 必要なルールを作成します（たとえば、Name=filepolicywin、Identity Groups=Any、Operating Systems=Windows All、Compliance Module=4.x or later、Posture Type=Temporal Agent、および Requirements=filereqwin）。

クライアント プロビジョニング ポリシーの設定

ステップ 1 **[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 必要なルールを作成します（たとえば、Rule Name=Win、Identity Groups=Any、Operating Systems=Windows All、Other Conditions=Conditions、Results=CiscoTemporalAgentWindows4.5）。

Cisco Temporal Agent のダウンロードと起動

ステップ 1 SSID に接続します。

ステップ 2 ブラウザを起動すると、クライアント プロビジョニング ポータルにリダイレクトされます。

ステップ 3 [開始（Start）] をクリックします。これにより、Cisco Temporal Agent がインストールされ、動作しているかどうかがチェックされます。

ステップ 4 [ここに初めて来ました（This Is My First Time Here）] をクリックします。

ステップ 5 [Cisco Temporal Agent をダウンロードして起動するにはここをクリック（Click Here to Download and Launch Cisco Temporal Agent）] を選択します。

ステップ 6 Windows または Mac OSX 用の Cisco Temporal Agent .exe または .dmg ファイルをそれぞれ保存します。Windows の場合は .exe ファイルを実行し、Mac OSX の場合は .dmg ファイルをダブルクリックして、acisetempagent アプリケーションを実行します。
Cisco Temporal Agent はクライアントをスキャンし、結果（非準拠を示す赤い十字マークなど）を表示します。

ポスチャのトラブルシューティング ツール

[ポスチャのトラブルシューティング（Posture Troubleshooting）] ツールは、ポスチャ チェック エラーの原因を見つけ、次のことを識別するのに役立ちます。

- どのエンドポイントがポスチャに成功し、どのエンドポイントが成功しなかったか。
- エンドポイントがポスチャに失敗した場合、ポスチャ プロセスのどの手順が失敗したか。
- どの必須および任意のチェックが成功および失敗したか。

ユーザ名、MAC アドレス、ポスチャ ステータスなどのパラメータに基づいて要求をフィルタリングすることによって、この情報を特定します。

Cisco ISE でのクライアント プロビジョニングの設定

クライアントプロビジョニングを有効にして、ユーザがクライアントプロビジョニング リソースをダウンロードし、エージェント プロファイルを設定できるようにします。Windows クライアント、Mac OS X クライアント、およびパーソナル デバイスのネイティブ サプリカント プロファイルのエージェント プロファイルを設定できます。クライアント プロビジョニングを無効にすると、ネットワークにアクセスしようとするユーザには、クライアントプロビジョニング リソースをダウンロードできないことを示す警告メッセージが表示されます。

始める前に

プロキシを使用していて、クライアント プロビジョニング リソースをリモート システムでホスティングしている場合は、プロキシがクライアントにそのリモート ロケーションへのアクセスを許可していることを確認します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [クライアント プロビジョニング（Client Provisioning）]** または **[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [設定**

（**Settings**）]>[ソフトウェア アップデート（**oftware Updates**）]>[クライアント プロビジョニング（**Client Provisioning**）] の順に選択します。

ステップ 2 [プロビジョニングの有効化（Provision Enable）] ドロップダウン リストから、**Enable** または **Disable** を選択します。

ステップ 3 **Enable Automatic Download** ドロップダウン リストから、**Enable** を選択します。

フィードのダウンロードには、すべての使用可能なクライアント プロビジョニング リソースが含まれています。これらのリソースの一部は、展開に関連していない場合があります。シスコでは、このオプションを設定する代わりに可能な限りリソースを手動でダウンロードすることを推奨します。

ステップ 4 [フィード URL の更新（Update Feed URL）] : [フィード URL の更新（Update Feed URL）] テキスト ボックスに、Cisco ISE で検索するシステム アップデートの URL を指定します。たとえば、クライアント プロビジョニング リソースをダウンロードするためのデフォルト URL は https://www.cisco.com/web/secure/spa/provisioning-update.xml. です。

ステップ 5 [ネイティブ サプリカント プロビジョニング ポリシーを使用できない（Native Supplicant Provisioning Policy Unavailable）] : デバイスに対するクライアント プロビジョニング リソースがない場合は、ここでフローの進め方を決定します。

- **Allow Network Access**：ユーザは、ネイティブ サプリカント ウィザードをインストールおよび起動せずに、デバイスをネットワークに登録することを許可されます。
- **Apply Defined Authorization Policy**：ユーザは、標準認証および（ネイティブ サプリカント プロビジョニング プロセスではない）許可ポリシーを適用して Cisco ISE ネットワークへのアクセスを試みる必要があります。このオプションを有効にすると、ユーザ デバイスに対して、ユーザの ID に適用されたすべてのクライアント プロビジョニング ポリシーに従った標準登録が行われます。Cisco ISE ネットワークにアクセスするためにユーザのデバイスが証明書を必要とする場合は、第 15 章の「End_User Web ポータルのセットアップとカスタマイズ」の「カスタム言語テンプレートの追加」の項の説明に従って、カスタマイズ可能なユーザ提示テキスト フィールドを使用して有効な証明書を取得して適用する方法もユーザに詳細に指示する必要があります。

ステップ 6 **Save** をクリックします。

次のタスク

クライアント プロビジョニング リソース ポリシーを設定します。

クライアント プロビジョニン リソース

クライアント プロビジョニング リソースは、エンドポイントがネットワークに接続した後にエンドポイントにダウンロードされます。クライアント プロビジョニング リソースは、デスクトップの場合はコンプライアンスとポスチャ エージェントで構成され、電話およびタブレットの場合はネイティブ サプリカント プロファイルで構成されます。クライアント プロビジョニング ポリシーによって、これらのプロビジョニング リソースがエンドポイントに割り当てられ、ネットワーク セッションが開始します。

クライアント プロビジョニング リソースは、**[ポリシー要素（Policy Elements）]** > **[結果（Results）]**>**[クライアントプロビジョニング（Client Provisioning）]**>**[リソース（Resources）]** にリストされます。次のリソース タイプは、[追加（Add）] ボタンをクリックすることでリストに追加できます。

- [Ciscoサイトのエージェントリソース（Agent resources from Cisco Site）]：クライアント プロビジョニング ポリシーで使用できるようにする [NAC]、[AnyConnect] および [サプリカントプロビジョニング（Supplicant Provisioning）] ウィザードを選択します。シスコは、新しいリソースを追加したり既存のリソースを更新することで、定期的にこのリソースのリストを更新します。すべてのシスコのリソースおよびリソースの更新を自動的にダウンロードするようにISEを設定することもできます。詳細については、Cisco ISE でのクライアント プロビジョニングの設定 （1261 ページ） を参照してください。
- [ローカルディスクのエージェントリソース（Agent resources from local disk）]：ISE にアップロードする PC 上のリソースを選択します。ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加 （1264 ページ） を参照してください。
- [AnyConnect設定（AnyConnect Configuration）]：クライアント プロビジョニングで使用できるようにする AnyConnect PC クライアントを選択します。詳細については、「AnyConnect 設定の作成」を参照してください。
- [ネイティブサプリカントプロファイル（Native Supplicant Profile）]：ネットワークの設定が含まれている電話とタブレット用のサプリカントプロファイルを設定します。詳細については、「ネイティブ サプリカント プロファイルの作成」を参照してください。
- [NACエージェントまたはAnyConnect ISEポスチャプロファイル（NAC Agent or AnyConnect ISE Posture Profile）]：エージェント XML プロファイルを作成/配布しない場合は、ここで NAC エージェントと AnyConnect ISE ポスチャを設定します。AnyConnect ISE ポスチャ エージェントおよびISEポスチャ プロファイル エディタの詳細については、お使いのバージョンの AnyConnect（https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html）の『AnyConnect Administrators Guide』を参照してください。

クライアント プロビジョニング リソースを作成した後、エンドポイントにクライアント プロビジョニング リソースを適用するクライアント プロビジョニング ポリシーを作成します。クライアントプロビジョニング リソース ポリシーの設定（1296ページ） を参照してください。

関連トピック

Cisco ISE でのクライアント プロビジョニングの設定 （1261 ページ）
シスコからのクライアント プロビジョニング リソースの追加 （1264 ページ）
クライアント プロビジョニング リソースの自動ダウンロード
ローカルマシンからのシスコ提供のクライアントプロビジョニング リソースの追加 （1264 ページ）
ローカル マシンからの AnyConnect 用の顧客作成リソースの追加 （1265 ページ）

シスコからのクライアント プロビジョニング リソースの追加

Windows クライアントおよび MAC OS x クライアント用の AnyConnect および Cisco NAC Agent と Cisco Web エージェントのために Cisco.com からクライアント プロビジョニング リソースを追加できます。選択したリソースおよび利用できるネットワーク帯域幅によっては、Cisco ISE にクライアント プロビジョニング リソースをダウンロードするのに数分かかることがあります。

始める前に

- Cisco ISE で正しいプロキシ設定が設定されていることを確認します。
- Cisco ISE でクライアント プロビジョニングを有効にします。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [Cisco サイトのエージェント リソース（Agent resources from Cisco site）]** を選択します。

ステップ 3 [ダウンロード リモート リソース（Download Remote Resources）] ダイアログボックスで選択可能なリストから必要なクライアント プロビジョニング リソースを 1 つ以上選択します。

ステップ 4 **Save** をクリックします。

次のタスク

Cisco ISE に正常にクライアント プロビジョニング リソースを追加したら、クライアント プロビジョニング リソース ポリシーの設定を開始します。

ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加

シスコから以前にダウンロードしたクライアント プロビジョニング リソースをローカルディスクから追加できます。

始める前に

Cisco ISE には、必ず現行のサポートされているリソースのみをアップロードしてください。サポートされていない古いリソースでは、クライアントアクセスに重大な問題が発生する可能性があります。

Cisco.com からリソース ファイルを手動でダウンロードする場合は、リリース ノートの「Cisco ISE Offline Updates」の項を参照してください。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [ローカル ディスクのエージェント リソース（Agent resources from local disk）]** を選択します。

ステップ 3 [カテゴリ（Category）] ドロップダウンから [シスコ提供パッケージ（Cisco Provided Packages）] を選択します。

ステップ 4 **Browse** をクリックし、Cisco ISE にダウンロードするリソース ファイルがあるローカル マシン上のディレクトリに移動します。

以前に Cisco からローカル マシンにダウンロードした AnyConnect、Cisco NAC Agent、または Cisco Web エージェントのリソースを追加できます。

ステップ 5 **Submit** をクリックします。

次のタスク

Cisco ISE に正常にクライアント プロビジョニング リソースを追加したら、クライアント プロビジョニング リソース ポリシーの設定できます。

ローカル マシンからの AnyConnect 用の顧客作成リソースの追加

AnyConnect カスタマイズ パッケージ、AnyConnect ローカリゼーション パッケージ、AnyConnect プロファイルなどの顧客作成リソースをローカル マシンから Cisco ISE に追加します。

始める前に

AnyConnect の顧客作成リソースがローカル ディスクに zip 形式のファイルで使用可能であることを確認します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ローカル ディスクのエージェント リソース（Agent Resources from local disk）] を選択します。

ステップ 4 [カテゴリ（Category）] ドロップダウンから [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 5 AnyConnect リソースの名前と説明を入力します。

ステップ 6 [参照（Browse）] をクリックし、Cisco ISE にダウンロードするリソース ファイルがあるローカル マシン上のディレクトリに移動します。

ステップ 7 Cisco ISE にアップロードする次の AnyConnect リソースを選択します。

- AnyConnect カスタマイゼーション バンドル
- AnyConnect ローカリゼーション バンドル
- AnyConnect プロファイル
- 高度なマルウェア防御（AMP）イネーブラ プロファイル

ステップ 8 [送信（Submit）] をクリックします。

[アップロードされた AnyConnect リソース（Uploaded AnyConnect Resources）] 表に、Cisco ISE に追加する AnyConnect リソースが表示されます。

次のタスク

AnyConnect エージェント プロファイルの作成

ネイティブ サプリカント プロファイルの作成

ネイティブ サプリカント プロファイルを作成して、ユーザが独自のデバイスを Cisco ISE ネットワークに含めることができます。ユーザがサインインすると、Cisco ISE は、ユーザの承認要件に関連付けられたプロファイルを使用して、必要なサプリカント プロビジョニング ウィザードを選択します。ウィザードは、ユーザのパーソナルデバイスを起動して設定し、ネットワークにアクセスします。

（注） プロビジョニング ウィザードは、アクティブなインターフェイスのみを設定します。このため、有線接続ユーザと無線接続ユーザは、どちらもアクティブになっている場合を除き、両方のインターフェイスにはプロビジョニングされません。

始める前に

- TCP ポート 8905 を開き、Cisco AnyConnect Agent、Cisco Web Agent、およびサプリカント プロビジョニング ウィザードのインストールを有効にします。ポートの使用法の詳細については、『*Cisco Identity Services Engine Hardware Installation Guide*』の付録「Cisco ISE Appliance Ports Reference」を参照してください。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 **[追加（Add）] > [ネイティブ サプリカント プロファイル（Native Supplicant Profile）]** を選択します。

ステップ 3 に示す説明を使用して、プロファイルを作成します。 ネイティブ サプリカント プロファイルの設定 （1267 ページ）

次のタスク

「複数ゲスト ポータルのサポート」の項の説明に従って、従業員が自分のパーソナル デバイスをネットワークに直接接続できるようにセルフ プロビジョニング機能を有効にします。

ネイティブ サプリカント プロファイルの設定

[ポリシー（Policy）] > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[クライアント プロビジョニング リソース（Client Provisioning Resources）]** の順に選択し、ネイティブ サプリカント プロファイルを追加すると、次の設定が表示されます。

- [名前（Name）]：作成するネイティブ サプリカント プロファイルの名前。このプロファイルを適用するオペレーティング システムを選択します。各プロファイルは、ISE がクライアントのネイティブ サプリカントに適用するネットワーク接続の設定を定義します。

ワイヤレス プロファイル

1 つ以上のワイヤレス プロファイルを設定します。クライアントで使用可能にする SSID ごとに 1 つを設定します。

- [SSID名（SSID Name）]：クライアントが接続する SSID の名前。
- [プロキシ自動コンフィギュレーションファイルのURL（Proxy Auto-Config File URL）]：サプリカントのネットワーク設定を取得するためにクライアントがプロキシに接続する場合は、そのプロキシ サーバへの URL を入力します。
- **プロキシホスト/IP（Proxy Host/IP）**
- **プロキシ ポート（Proxy Port）**
- [セキュリティ（Security）]：WPA または WPA2 を使用するようにクライアントを設定します。
- [許可されているプロトコル（Allowed Procotol）]：クライアントが認証サーバに接続するのに使用するプロトコルを設定します（PEAP または EAP-TLS）。
- [証明書テンプレート（Certificate Template）]：TLS の場合は、**[管理（Administration）]** > **[システム証明書（System Certificates）]** > **[認証局（Certificate Authority）]** > **[証明書テンプレート（Certificate Templates）]** で定義された証明書テンプレートのいずれかを選択します。

オプション設定は、「オプション設定：*Windows* の場合」の項で説明します。

iOS 設定

- **ターゲットネットワークが非表示になっている場合に有効にする（Enable if target network is hidden）**

有線プロファイル

- [許可されているプロトコル（Allowed Protocol）]：クライアントが認証サーバに接続するのに使用するプロトコルを設定します（PEAP または EAP-TLS）。
- [証明書テンプレート（Certificate Template）]：TLS の場合は、[管理（Administration）][システム証明書（System Certificates）][認証局（Certificate Authority）][証明書テンプレート（Certificate Templates）] で定義された証明書テンプレートのいずれかを選択します。

オプション設定：Windows の場合

[オプション（Optional）] を展開すると、Windows クライアントの場合は次のフィールドも使用できます。

- [認証モード（Authentication Mode）]：許可のクレデンシャルとして、[ユーザ（User）]、[マシン（Machine）] またはその両方を使用するかを決定します。
- [自動的にログイン名とパスワード（およびもしあればドメイン）を使用する（Automatically use logon name and password (and domain if any)）]：認証モードで [ユーザ（User）] を選択すると、ユーザにプロンプトを表示することなくログインおよびパスワードを使用します（その情報が使用できる場合）。
- [高速再接続を有効にする（Enable Fast Reconnect）]：セッションの再開機能が PEAP プロトコル オプションで有効な場合（これは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[PEAP]** で設定されます）、PEAP セッションはユーザ クレデンシャルをチェックすることなく再開できます。
- [隔離チェックを有効にする（Enable Quarantine Checks）]：クライアントが隔離されたかどうかを確認します。
- [サーバが暗号化バインドTLVを示さない場合に切断する（Disconnect if server does not present cryptobinding TLV）]：暗号化バインド TLV がネットワーク接続でサポートされていない場合に切断します。
- [新規サーバまたは信頼できる証明機関の承認をユーザに求めない（Do not prompt user to authorize new servers or trusted certification authorities）]：自動的にユーザ証明書を受け入れ、ユーザにプロンプトを表示しません。
- [ネットワークが名前（SSID）をブロードキャストしていなくても接続する（Connect even if the network is not broadcasting its name (SSID)）]：ワイヤレス プロファイルの場合のみ。

各種ネットワークでの URL リダイレクトなしでのクライアント プロビジョニング

URL リダイレクトなしのクライアント プロビジョニングは、サードパーティの NAC で CoA がサポートされていない場合に必要です。クライアント プロビジョニングは、URL リダイレクトの有無にかかわらず実行できます。

（注） URL リダイレクションを使用するクライアント プロビジョニングの場合、クライアント マシンにプロキシ設定が構成されている場合は、ブラウザ設定の例外リストに Cisco ISE を追加してください。この設定は、URL リダイレクションを使用するすべてのフロー、BYOD、MDM、ゲスト、およびポスチャに適用されます。たとえば、Windows マシンでは、次の手順を実行します。

1. コントロール パネルから、[Internet Properties] をクリックします。
2. [Connections] タブを選択します。
3. [LAN settings] をクリックします。
4. [プロキシ サーバー] 領域から、[Advanced] をクリックします。
5. [Exceptions] ボックスに Cisco ISE ノードの IP アドレスを入力します。
6. [OK] をクリックします。

各種ネットワークでリダイレクトなしでエンドポイントをプロビジョニングする手順を次に示します。

Dot1X EAP-TLS

1. プロビジョニングされた認証を使用して Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする。

   AnyConnect がポスチャを実行する。エンドポイントがポスチャ コンプライアンスに基づいて正しいネットワークに移動する。

Dot1X PEAP

1. NSP 経由でユーザ名とパスワードを使用して Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする

   AnyConnect がポスチャを実行する。エンドポイントがポスチャ コンプライアンスに基づいて正しいネットワークに移動する。

MAB（有線ネットワーク）

1. Cisco ISE ネットワークに接続する。
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする。

   AnyConnect がポスチャを実行する。エンドポイントがポスチャ コンプライアンスに基づいて正しいネットワークに移動する。

MAB（ワイヤレス ネットワーク）

1. Cisco ISE ネットワークに接続する
2. ブラウザ ウィンドウを開き、プロビジョニング URL（provisioning.cisco.com）を入力する。
3. 内部ユーザ、AD、LDAP、または SAML を介して CP ポータルにログインする。

   AnyConnect がポスチャを実行する。ポスチャはワイヤレス 802.1X の場合にのみ開始する。

AMP イネーブラ プロファイルの設定

次の表に、[高度なマルウェア防御（AMP）イネーブラプロファイル（Advanced Malware Protection (AMP) Enabler Profile）] ページのフィールドを示します。ナビゲーション パスは、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** です。

[追加（Add）] ドロップダウン矢印をクリックし、[AMPイネーブラプロファイル（AMP Enabler Profile）] を選択します。

表 ***168 : [AMP*イネーブラプロファイル（*AMP Enabler Profile*）*] ページ***

フィールド	使用上のガイドライン
名前（Name）	ユーザが作成する AMP イネーブラ プロファイルの名前を入力します。
説明	AMP イネーブラ プロファイルの説明を入力します。

フィールド	使用上のガイドライン
AMPイネーブラのインストール（Install AMP Enabler）	• **Windows インストーラ**：Windows OS ソフトウェアの AMP をホストするローカル サーバの URL を指定します。AnyConnect モジュールはこの URL を使用して、エンドポイントに .exe ファイルをダウンロードします。ファイル サイズは約 25 MB です。 • **Mac インストーラ**：Mac OSX ソフトウェアの AMP をホストするローカル サーバの URL を指定します。AnyConnect モジュールはこの URL を使用して、エンドポイントに .pkg ファイルをダウンロードします。ファイルサイズは約 6 MB です。 [オン（Check）] ボタンは、サーバと通信を行って URL が有効かどうかを確認します。URL が有効の場合は、「ファイルが見つかりました（File found）」メッセージが表示され、有効でない場合はエラー メッセージが表示されます。
AMPイネーブラのアンインストール（Uninstall AMP Enabler）	エンドポイントからエンドポイント ソフトウェアの AMP をアンインストールします。
開始メニューへの追加（Add to Start Menu）	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントの [開始（Start）] メニューにエンドポイント ソフトウェアの AMP のショートカットを追加します。
デスクトップへの追加（Add to Desktop）	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントのデスクトップにエンドポイント ソフトウェアの AMP のショートカットを追加します。
コンテキストメニューへの追加（Add to Context Menu）	エンドポイント ソフトウェアの AMP がエンドポイントにインストールされた後、エンドポイントの右クリック コンテキスト メニューに [今すぐスキャン（Scan Now）] オプションを追加します。

組み込みプロファイル エディタを使用した AMP イネーブラ プロファイルの作成

ISE 埋め込みプロファイル エディタまたはスタンドアロン エディタを使用して、AMP イネーブラ プロファイルを作成できます。

ISE 埋め込みプロファイル エディタを使用して AMP イネーブル プロファイルを作成するには、次の手順を実行します。

始める前に

- SOURCEfire ポータルからエンドポイント ソフトウェアの AMP をダウンロードし、ローカル サーバでホスティングします。
- [管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] に移動して、エンドポイント ソフトウェアの AMP をホストするサーバの証明書を ISE 証明書ストアにインポートします。
- [AMPイネーブラ（AMP Enabler）] オプションが [AnyConnect設定（AnyConnect Configuration）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client provisioning）] > [リソース（Resources）] > [追加（Add）] > [AnyConnect設定（AnyConnect Configuration）] > [AnyConnectパッケージの選択（Select AnyConnect Package）]）の [AnyConnectモジュール選択（AnyConnect Module Selection）] および [プロファイル選択（Profile Selection）] セクションで選択されていることを確認します。
- SOURCEfire ポータルにログインして、エンドポイント グループのポリシーを作成し、エンドポイント ソフトウェアの AMP をダウンロードする必要があります。ソフトウェアには、選択したポリシーが事前設定されています。2 つのイメージ、すなわち Windows OS の場合はエンドポイント ソフトウェアの AMP、Mac OSX の場合はエンドポイント ソフトウェアの AMP の再頒布可能なバージョンをダウンロードする必要があります。ダウンロードされたソフトウェアは、エンタープライズネットワークからアクセスできるサーバでホストされます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョン（Client Provision）] > [リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] ドロップダウンをクリックします。

ステップ 3 [AMPイネーブラプロファイル（AMP Enabler Profile）] を選択して、新しい AMP イネーブラ プロファイルを作成します。

ステップ 4 フィールドに適切な値を入力します。

ステップ 5 [送信（Submit）] をクリックして、プロファイルを [リソース（Resources）] ページに保存します。

スタンドアロン エディタを使用した AMP イネーブラ プロファイルの作成

AnyConnect スタンドアロンエディタを使用して、AMP イネーブラ プロファイルを作成するには、次の手順を実行します。

始める前に

AnyConnect 4.1 スタンドアロン エディタを使用して、XML 形式のプロファイルをアップロードして AMP イネーブラ プロファイルを作成できます。

- Cisco.com から Windows および Mac OS の AnyConnect スタンドアロン プロファイル エディタをダウンロードします。
- スタンドアロン プロファイル エディタを起動し、[AMPイネーブラプロファイルの設定（AMP Enabler Profile Settings）]AMP イネーブラ プロファイルの設定（1270 ページ）で指定されているようにフィールドに入力します。
- プロファイルを XML ファイルとしてローカル ディスクに保存します。
- [AMPイネーブラ（AMP Enabler）] オプションが [AnyConnect設定（AnyConnect Configuration）] ページ（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client provisioning）] > [リソース（Resources）] > [追加（Add）] > [AnyConnect設定（AnyConnect Configuration）] > [AnyConnectパッケージの選択（Select AnyConnect Package）]）の [AnyConnectモジュール選択（AnyConnect Module Selection）] および [プロファイル選択（Profile Selection）] セクションで選択されていることを確認します。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ローカルディスクのエージェントリソース（Agent resources from local disk）] を選択します。

ステップ 4 [カテゴリ（Category）] ドロップダウンから [顧客作成のパッケージ（Customer Created Packages）] を選択します。

ステップ 5 [タイプ（Type）] ドロップダウンから [AMPイネーブラプロファイル（AMP Enabler Profile）] を選択します。

ステップ 6 [名前（Name）] と [説明（Description）] に入力します。

ステップ 7 [参照（Browse）] をクリックして、ローカル ディスクから保存済みプロファイル（XML ファイル）を選択します。次に、カスタマイズされたインストール ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Install>
 <WindowsConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
```

```
</WindowsConnectorLocation>
 <MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
 <StartMenu>true</StartMenu>
 <DesktopIcon>false</DesktopIcon>
 <ContextIcon>true</ContextIcon>
 </Install>
 </FAConfiguration>
</FAProfile>
```

次に、カスタマイズされたアンインストール ファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Uninstall>
 </Uninstall>
 </FAConfiguration>
</FAProfile>
```

ステップ 8 [送信（Submit）] をクリックします。
新しく作成された AMP イネーブラ プロファイルが [リソース（Resources）] ページに表示されます。

一般的な AMP イネーブラ インストール エラーのトラブルシューティング

[Windowsインストーラ（Windows Installer）] または [MACインストーラ（MAC Installer）] テキスト ボックスに SOURCEfire URL を入力して [オン（Check）] をクリックすると、次のエラーのいずれかが発生する場合があります。

- エラー メッセージ：「MacまたはWindowsのインストーラファイルを含むサーバの証明書がISEによって信頼されていません。（The certificate for the server containing the Mac/Windows installer file is not trusted by ISE.）信頼証明書を [管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] に追加します。（Add a trust certificate to **Administration** > **Certificates** > **Trusted Certificates**.）」

  このエラー メッセージは、Cisco ISE 証明書ストアに SOURCEfire の信頼できる証明書をインポートしていない場合に表示されます。SOURCEfire の信頼できる証明書を入手し、Cisco ISE の信頼できる証明書ストア（[管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]）にインポートします。

- エラー メッセージ：「インストーラファイルがこの場所で見つかりません。接続の問題である可能性があります。（The installer file is not found at this location, this may be due to a connection issue.）有効なパスを [インストーラ（Installer）] テキスト ボックスに入力するか、または接続を確認します。（Enter a valid path in the Installer text box or check your connection.）」

  このエラー メッセージは、エンドポイント ソフトウェアの AMP をホストしているサーバがダウンした場合、または [Windowsインストーラ（Windows Installer）] または [MACインストーラ（MAC Installer）] テキスト ボックスに入力ミスがある場合に表示されます。

- エラー メッセージ：「[Windowsインストーラ（Windows Installer）]または[MACインストーラ（MAC Installer）]テキスト ボックスに有効なURLが含まれていません。（The Windows/Mac installer text box does not contain a valid URL.）」

  このエラー メッセージは、構文的に正しくないURL形式を入力した場合に表示されます。

Cisco ISE の Chromebook デバイスのオンボーディングのサポート

Chromebookデバイスは他のデバイス（Apple、Windows、Android）とは異なり管理型デバイス（Google ドメインによって管理）で、オンボーディング サポートが制限されています。Cisco ISE はネットワークでの Chromebook デバイスのオンボーディングをサポートしています。オンボーディングとは、Cisco ISE による認証の後にネットワークに安全に接続できるように、エンドポイントに必要な設定とファイルを配送するプロセスのことです。このプロセスには、証明書のプロビジョニングやネイティブ サプリカントのプロビジョニングが含まれています。ただし、Chromebookデバイスでは、証明書のプロビジョニングのみが実行できます。ネイティブ サプリカントのプロビジョニングは、Google 管理コンソールで実行されます。

管理されていない Chromebook デバイスは、安全なネットワークへのオンボーディングができません。

Chromebook オンボーディング プロセスに関与するエンティティは次のとおりです。

- Google 管理者
- ISE 管理者
- Chromebook ユーザ/デバイス
- Google 管理コンソール（Google 管理者が管理）

Google 管理者：

- 次のライセンスの安全性を確保します。
  1. Google 管理コンソール設定のための Google Apps 管理者ライセンス。URL：https://admin.google.com。Google管理コンソールを使用して、管理者は組織内の人間のための Google サービスを管理できます。
  2. Chromebook のデバイス管理ライセンス。URL：https://support.google.com/chrome/a/answer/2717664?hl=en。Chromebook のデバイス管理ライセンスは、特定の Chromebook デバイスに対して設定を行い、ポリシーを適用するために使用されます。ユーザアクセスの制御、機能のカスタマイズ、ネットワークアクセスの設定などのためのデバイス設定への Google 管理者アクセス権を提供します。
- Googleデバイス ライセンスによるChromebookデバイスのプロビジョニングと登録を促進します。

- Google 管理コンソールを通じて Chromebook デバイスを管理します。
- 各 Chromebook ユーザの Wi-Fi ネットワーク設定のセットアップと管理を行います。
- Chromebook デバイスでアプリケーションの設定と強制されている拡張機能のインストールを行い、Chromebook デバイスを管理します。Chromebook デバイスのオンボーディングには、Chromebook デバイスに Cisco Network Setup Assistant 拡張機能がインストールされている必要があります。これにより、Chromebook デバイスが Cisco ISE に接続し、ISE 証明書をインストールできるようになります。証明書のインストールの操作は管理対象デバイスにのみ許可されるため、この拡張機能は強制的にインストールされます。
- サーバの検証と安全な接続を実現するために、Cisco ISE 証明書が Google 管理コンソールにインストールされていることを確認します。Google 管理者が、証明書がデバイスに対して生成されるか、ユーザに対して生成されるかを決定します。Cisco ISE には次のオプションがあります。
  - Chromebook デバイスを共有しない単一のユーザ用に証明書を生成します。
  - 複数のユーザで共有される Chromebook デバイス用に証明書を生成します。必要な追加設定については、「Google 管理コンソールでのネットワークの設定と拡張機能の強制」セクションの手順 5 を参照してください。

  ISE が Chromebook デバイスで証明書のプロビジョニングを実行するために信頼され、EAP-TLS 証明書ベースの認証が許可されるように、Google 管理者が ISE サーバ証明書をインストールします。Google Chrome バージョン 37 以降は、Chromebook デバイスの証明書ベースの認証をサポートしています。Google 管理者は Google 管理コンソールで ISE プロビジョニング アプリケーションをロードし、ISE から証明書を取得するために Chromebook デバイスで使用できるようにする必要があります。
- 推奨される Google ホスト名が、SSL の安全な接続のために WLC で設定された ACL 定義リストのホワイト リストにあることを確認します。Google サポート ページの推奨されるホスト名のホワイト リストを参照してください。

ISE 管理者：

- 証明書テンプレートの構造を含む、Chromebook OS のネイティブ サプリカント プロファイルを定義します。
- Chromebook ユーザの Cisco ISE で必要な認証ルールとクライアント プロビジョニング ポリシーを作成します。

Chromebook ユーザ：

- Chromebook デバイスを消去し、Google ドメインに登録して、Google 管理者によって定義された適用ポリシーを保護します。
- Chromebook デバイス ポリシーと、Google 管理コンソールによってインストールされた、強制されている Cisco Network Setup Assistant 拡張機能を受信します。
- Google 管理者によって定義されているとおりにプロビジョニングされた SSID に接続して、ブラウザを開いて BYOD ページを表示し、オンボーディング プロセスを開始します。
- Cisco Network Setup Assistant が Chromebook デバイスにクライアント証明書をインストールし、これによりデバイスが EAP-TLS 証明書ベースの認証を行えるようになります。

Google 管理コンソール：

Google 管理コンソールは Chromebook デバイス管理をサポートし、安全なネットワークの設定と、Chromebook への Cisco Network Setup Assistant 証明書管理拡張機能のプッシュができます。この拡張機能は SCEP 要求を Cisco ISE に送信し、クライアント証明書をインストールして、安全な接続とネットワークへのアクセスを可能にします。

共有環境での Chromebook デバイスの使用のベスト プラクティス

Chromebook デバイスが学校や図書館などの共有環境で使用される場合、Chromebook デバイスはさまざまなユーザによって共有されます。シスコが推奨するベストプラクティスの一部は、次のとおりです。

- 特定のユーザ（学生または教授）の名前で Chromebook デバイスをオンボーディングする場合、ユーザの名前が証明書の [件名（Subject）] フィールドの [共通名（CN）（Common Name (CN)）] に入力されます。また、共有 Chromebook がその特定のユーザの My Devices ポータルに表示されます。そのため、共有デバイスではオンボーディング時に共有クレデンシャルを使用し、特定のユーザの My Devices ポータルのリストにのみデバイスが表示されるようにすることを推奨します。共有アカウントは、個別のアカウントとして管理者または教授が管理し、共有デバイスを制御することができます。
- ISE 管理者は、共有 Chromebook デバイス用のカスタム証明書テンプレートを作成し、ポリシーで使用することができます。たとえば、[件名-共通名（CN）（Subject-Common Name (CN)）] 値に一致する標準の証明書テンプレートを使用する代わりに、証明書の名前（chrome-shared-grp1 など）を指定して同じ名前を Chromebook デバイスに割り当てることができます。ポリシーは、Chromebook デバイスへのアクセスを許可または拒否するために、名前で一致させるように設計できます。
- ISE 管理者は、（アクセスが制限される必要があるデバイスの）Chromebook オンボーディングを経る必要があるすべての Chromebook デバイスの MAC アドレスを備えたエンドポイント グループを作成することができます。認証ルールは、デバイス タイプ Chromebook とともにこれを呼び出す必要があります。これにより、アクセスが NSP にリダイレクトされます。

Chromebook オンボーディング プロセス

Chromebook オンボーディング プロセスは、次の一連のステップを実行します。

ステップ 1 Google 管理コンソールでのネットワークの設定と拡張機能の強制 。
ステップ 2 Chromebook オンボーディングのための ISE の設定。
ステップ 3 Chromebook デバイスのワイプ。
ステップ 4 Google 管理コンソールへの Chromebook の登録。
ステップ 5 BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続。

Google 管理コンソールでのネットワークの設定と拡張機能の強制

Google 管理者は、次の手順を実行します。

ステップ 1 Google 管理コンソールにログインします。

a) ブラウザで URL https://admin.google.com を入力します。

b) 必要なユーザ名とパスワードを入力します。

c) [Welcome to Admin Console] ページで、[Device Management] をクリックします。

d) [デバイス管理（Device Management）] ページで、[ネットワーク（Network）] をクリックします。

ステップ 2 管理対象デバイスの Wi-Fi ネットワークをセットアップします。

a) [ネットワーク（Networks）] ページで、[Wi-Fi] をクリックします。

b) [Add Wi-Fi] をクリックして、必要な SSID を追加します。詳細については、「Google 管理コンソール：Wi-Fi ネットワーク設定」を参照してください。

MAB フローについては、2 つの SSID を作成し、1 つをオープン ネットワーク用、もう 1 つを証明書認証用にします。ユーザがオープン ネットワークに接続すると、Cisco ISE ACL は、認証のために、ユーザをクレデンシャルを持つゲスト ポータルにリダイレクトします。認証が成功すると、ACL はユーザを BYOD ポータルにリダイレクトします。

ISE 証明書が中間 CA によって発行された場合は、ルート CA ではなく、中間証明書を「サーバ認証局」にマッピングする必要があります。

c) [追加（Add）] をクリックします。

ステップ 3 強制拡張機能を作成します。

a) [デバイス管理（Device Management）] ページの [デバイス設定（Device Settings）] 領域で、[Chrome管理（Chrome Management）] をクリックします

b) [User Settings] をクリックします。

c) 下にスクロールして、[アプリケーションと拡張機能（Apps and Extensions）] セクションの [強制的にインストールされたアプリケーションと拡張機能（Force-Installed Apps and Extensions）] オプションで、[強制的にインストールされたアプリケーションの管理（Manage Force-Installed Apps）] をクリックします。

ステップ 4 強制拡張機能をインストールします。

a) [強制的にインストールされたアプリケーションと拡張機能（Force-Installed Apps and Extensions）] ページで、[Chromeウェブストア（Chrome Web Store）] をクリックします。

b) [検索（Search）] テキスト ボックスに「Cisco Network Setup Assistant」と入力して、拡張機能を見つけます。

Chromebook デバイスの Cisco Network Setup Assistant 拡張機能は、Cisco ISE の証明書を要求し、Chromebook デバイスに ISE の証明書をインストールします。証明書のインストールは管理対象デバイスに対してのみ許可されるため、この拡張機能は、強制的にインストールされるように設定する必要があります。登録プロセス中にこの拡張機能がインストールされていない場合は、Cisco ISE の証明書をインストールすることはできません。

拡張機能でサポートされている言語の詳細については、「Cisco ISE 国際化およびローカリゼーション」を参照してください。

c) [Add] をクリックして、強制的にアプリをインストールします。
d) [保存（Save）] をクリックします。

ステップ 5 （オプション）複数のユーザに共有されている Chromebook デバイスに証明書をインストールするには、コンフィギュレーション ファイルを定義します。

a) メモ帳ファイルに次のコードをコピー アンド ペーストして、ローカル ディスクに保存します。

```
{
  "certType": {
    "Value": "system"
  }
}
```

b) **[Device Management]** > **[Chromebook Management]** > **[App Management]** の順に選択します。
c) [Cisco Network Setup Assistant] 拡張機能をクリックします。
d) [User Settings] をクリックし、ドメインを選択します。
e) [設定ファイルのアップロード（Upload Configuration File）] をクリックし、ローカルディスクに保存した .txt ファイルを選択します。

（注） Cisco Network Setup Assistant で複数のユーザが共有するデバイスの証明書を作成するには、このメモ帳ファイルを Google 管理コンソールに追加する必要があります。追加しないと、Cisco NSA はシングル ユーザ用の証明書を作成します。

f) [保存（Save）] をクリックします。

ステップ 6 （オプション）Chromebook を共有しないシングル ユーザの証明書をインストールします。

a) **[Device Management]** > **[Network]** > **[Certificates]** の順に選択します。
b) [Certificates] セクションで、[Add Certificate] をクリックして、Cisco ISE の証明書ファイルをアップロードします。

次のタスク

Chromebook オンボーディングのための ISE の設定

Chromebook オンボーディングのための ISE の設定

始める前に

ISE 管理者は、[ポリシー（Policy）]>[ポリシー セット（Policy Sets）] ページで必要なポリシーを作成する必要があります。

認証ポリシーの例を次に示します。

Rule Name: Full_Access_After_Onboarding, Conditions: If RegisteredDevices AND Wireless_802.1x AND Endpoints:BYODRegistration EQUALS Yes AND Certificate: Subject Alternative Name Equals

RadiusCalling-Station-ID AND Network Access: EAP-Authentication EQUALS EAP-TLS Then CompliantNetworkAccess.

CompliantNetworkAccess は、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[Authorization（認証）]** > **[認証プロファイル（Authorization Profiles）]** ページで設定されている認証結果です。

ステップ 1 Cisco ISE でネイティブ サプリカント プロファイル（NSP）を設定します。

a) **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** の順に選択します。

b) **[クライアント プロビジョニング（Client Provisioning）]** > **[リソース（Resources）]** の順にクリックします。

Chromebook デバイスが新規 Cisco ISE インストールの [クライアント プロビジョニング（Client Provisioning）] ページに表示されます。ただし、アップグレードの場合は、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）] ページからポスチャの更新プログラムをダウンロードする必要があります。

c) **[追加（Add）]** > **[ネイティブ サプリカント プロファイル（Native Supplicant Profile）]** の順にクリックします。

d) [名前（Name）] と [説明（Description）] に入力します。

e) **[オペレーティング システム（Operating System）]** フィールドで、**[Chrome OS すべて（Chrome OS All）]** を選択します。

f) **[証明書テンプレート（Certificate Template）]** フィールドで、必要な証明書テンプレートを選択します。

g) [送信（Submit）] をクリックします。SSID が Google 管理コンソールからプロビジョニングされていて、ネイティブ サプリカント プロビジョニング フローからではないことを確認します。

ステップ 2 [クライアント プロビジョニング（Client Provisioning）] ページで NSP をマッピングします。

a) [ポリシー（Policy）] > [クライアント プロビジョニング（Client Provisioning）] の順に選択します。

b) 結果を定義します。

- クライアント プロビジョニング ポリシーの [結果（Results）] で組み込みのネイティブ サプリカント設定（Cisco-ISE-Chrome-NSP）を選択します。
- または、新しいルールを作成し、Chromebook デバイス用に作成された [結果（Result）] が選択されていることを確認します。

Chromebook デバイスのワイプ

Chromebook デバイスは、Google 管理コンソールが Google 管理者により設定された後でワイプされる必要があります。Chromebook ユーザはデバイスをワイプする必要があり、これは拡張を強制し、ネットワークを設定する一度だけの処理です。詳細については、次の URL https://support.google.com/chrome/a/answer/1360642を参照してください。

Chromebook ユーザは次の手順を実行します。

ステップ 1 **Esc + Refresh + Power** キーの組み合わせを押します。画面に黄色い感嘆符（!）が表示されます。

ステップ 2 開発モードを開始するには、**Ctrl + D** キーの組み合わせを押してから、**Enter** キーを押します。画面に赤い感嘆符が表示されます。

ステップ 3 **Ctrl + D** キーの組み合わせを押します。Chromebook はローカルデータを削除して、初期状態に戻ります。この削除には約 15 分かかります。

ステップ 4 移行が完了したら、**Space** キーを押してから **Enter** キーを押して、確認モードに戻ります。

ステップ 5 サインインする前に Chromebook を登録します。

次のタスク

Google 管理コンソールに Chromebook を登録します。

Google 管理コンソールへの Chromebook の登録

Chromebook のデバイスをプロビジョニングするには、Chromebook ユーザは最初に Google 管理コンソールページに登録し、デバイスポリシーおよび強制拡張を受信する必要があります。

ステップ 1 Chromebook のデバイスの電源を入れ、サインオン画面が表示されるまで、画面上の指示に従います。まだサインインしないでください。

ステップ 2 Chromebook のデバイスにサインインする前に、**Ctrl + Alt + E** のキーの組み合わせを押します。[エンタープライズ登録（Enterprise Enrolment）] 画面が表示されます。

ステップ 3 E メールアドレスを入力し、[次へ（Next）] をクリックします。
次のメッセージが表示されます：「デバイスは企業管理用に正しく登録されています（Your device has successfully been enrolled for enterprise management.）」。

ステップ 4 [完了（Done）] をクリックします。

ステップ 5 Google 管理のようこそレターからのユーザ名とパスワード、または登録資格があるアカウントの既存の Google アプリケーション ユーザのユーザ名とパスワードを入力します。

ステップ 6 [デバイスの登録（Enroll Device）] をクリックします。デバイスが正常に登録されると、確認メッセージが表示されます。

Chromebook の登録の処理は一度だけであることに注意してください。

BYOD オンボーディング用の Cisco ISE ネットワークへの Chromebook の接続

デュアル SSID 用の手順：EAP-TLS プロトコルを使用して 802.x ネットワークに接続する場合、Chromebook ユーザは次の手順を実行します。

（注） デュアル SSID を使用している場合：802.x PEAP から EAP-TLS ネットワークに接続するときは、ネットワーク サプリカント（Web ブラウザではなく）にクレデンシャルを入力して、ネットワークに接続してください。

ステップ 1 Chromebook で [設定（Settings）] をクリックします。

ステップ 2 [インターネット接続（Internet Connection）] セクションで、[Wi-Fi ネットワークをプロビジョニングする（Provisioning Wi-Fi Network）] をクリックしてから、該当するネットワークをクリックします。

ステップ 3 クレデンシャルを持つゲスト ポータルが開きます。

1. [サインオン（Sign On）] ページで、[ユーザ名（Username）] と [パスワード（Password）] を入力します。
2. [サインオン（Sign-on）] をクリックします。

ステップ 4 BYOD のウェルカム ページで、[開始（Start）] をクリックします。

ステップ 5 [デバイス情報（Device Information）] フィールドにデバイスの名前と説明を入力します。たとえば、「パーソナル デバイス：学校で使用するジェーンの Chromebook、または共有デバイス：ライブラリ Chromebook #1 または教室 1 Chromebook #1」と入力します。

ステップ 6 [続行（Continue）] をクリックします。

ステップ 7 [Cisco Network Setup Assistant] ダイアログ ボックスで [はい（Yes）] をクリックして、セキュアなネットワークにアクセスするための証明書をインストールします。

Google 管理者がセキュアな Wi-Fi を設定した場合、ネットワーク接続は自動的に行われます。そうでない場合は、使用可能なネットワークのリストからセキュアな SSID を選択します。

すでにドメインに登録され、Cisco Network Setup Assistant の拡張を取得済みの Chromebook ユーザは、自動更新を待たずに、拡張を更新できます。次の手順を実行して、拡張を手動で更新します。

1. Chromebook で、ブラウザを開き、次の URL を入力してください。**chrome://Extensions**
2. [開発者モード（Developer Mode）] チェック ボックスをオンにします。
3. [今すぐ拡張を更新（Update Extensions Now）] をクリックします。
4. Cisco Network Setup Assistant の拡張バージョンが 2.1.0.35 以上であることを確認します。

Google 管理コンソール：Wi-Fi ネットワーク設定

Wi-Fi ネットワークの設定を使用して、顧客ネットワークの SSID を設定するか、または証明書属性（EAP-TLS 用）を使用して証明書を照合します。証明書が Chromebook にインストールされるときに、Google管理設定と同期されます。接続は、定義された証明書属性のいずれかが SSID 設定と一致したときのみ確立されます。

以下に、EAP-TLS、PEAPおよびオープン ネットワーク フローに特有な必須フィールドを示します。これらは、Google 管理コンソール ページで各 Chromebook ユーザに対し、Wi-Fi ネットワークを設定するようにGoogle管理者が設定します。（[デバイス管理（Device Administration）] > [ネットワーク（Network ）] > [Wi-Fi] > [Wi-Fi の追加（Add Wi-Fi）]）。

フィールド	EAP-TLS	PEAP	オープン（Open）
[名前（Name）]	ネットワーク接続の名前を入力します。	ネットワーク接続の名前を入力します。	ネットワーク接続の名前を入力します。
サービスセット識別子（SSID）	SSID（たとえば、tls_ssid）を入力します。	SSID（たとえば、tls_ssid）を入力します。	SSID（たとえば、tls_ssid）を入力します。
この SSID はブロードキャストされません	オプションを選択します。	オプションを選択します。	オプションを選択します。
自動的に接続	オプションを選択します。	オプションを選択します。	オプションを選択します。
セキュリティ タイプ	WPA/WPA2 Enterprise（802.1x）	WPA/WPA2 Enterprise（802.1x）	オープン（Open）
Extensible Authentication Protocol	EAP-TLS	PEAP	—
内部プロトコル	—	• 自動（Automatic） • MSCHAP v2（オプションを選択） • MD5 • PAP • MSCHAP • GTC	—
外部 ID	—	—	—

フィールド	EAP-TLS	PEAP	オープン（Open）
[ユーザ名（Username）]	必要に応じて、固定値を設定するか、またはユーザログインから変数を使用します：${LOGIN_ ID} または ${LOGIN_EMAIL}。	ISE（内部 ISE ユーザ / AD / その他の ISE ID）とパスワードフィールドに対し認証する PEAP クレデンシャルを入力します。	—
サーバ認証局（Server Certificate Authority）	ISE 証明書を選択します（[デバイス管理（Device Administration）] > [ネットワーク（Network ）] > [証明書（Certificates）] からインポートされます）。	ISE 証明書を選択します（[デバイス管理（Device Administration）] > [ネットワーク（Network ）] > [証明書（Certificates）] からインポートされます）。	—
プラットフォームによるこの Wi-Fi ネットワークへのアクセス制限	• モバイル デバイスを選択します。 • Chromebooks を選択します。	• モバイル デバイスを選択します。 • Chromebooks を選択します。	—
クライアントの登録 URL	登録されていないユーザに対して Chromebook デバイスのブラウザがリダイレクトされる先の URL を入力します。未登録のユーザをリダイレクトするために、ワイヤレス LAN コントローラの ACL を設定します。	—	—

フィールド	EAP-TLS	PEAP	オープン（Open）
発行者パターン	証明書属性。少なくとも1つの属性を、インストールされた証明書属性に一致する、発行者パターンまたはサブジェクトパターンから選択してください。証明書を受け入れるように Chromebook デバイスに一致する証明書属性を指定します。 • 共通名：証明書のサブジェクトフィールド、またはノードのFQDNと一致している必要がある証明書のサブジェクトフィールドのワイルドカード ドメインを参照します。 • 地域：証明書のサブジェクトに関連するテスト地域（市）を参照してください。 • 組織：証明書のサブジェクトに関連する組織名を参照します。 • 組織単位：証明書のサブジェクトに関連する組織単位の名前を参照します。	—	—

フィールド	EAP-TLS	PEAP	オープン（Open）
サブジェクトパターン	証明書属性。少なくとも1つの属性を、インストールされた証明書属性に一致する、発行者パターンまたはサブジェクトパターンから選択してください。証明書を受け入れるように Chromebook デバイスに一致する証明書属性を指定します。 • 共通名：証明書のサブジェクトフィールド、またはノードのFQDNと一致している必要がある証明書のサブジェクトフィールドのワイルドカード ドメインを参照します。 • 地域：証明書のサブジェクトに関連するテスト地域（市）を参照してください。 • 組織：証明書のサブジェクトに関連する組織名を参照します。 • 組織単位：証明書のサブジェクトに関連する組織単位の名前を参照します。	—	—

フィールド	EAP-TLS	PEAP	オープン（Open）
プロキシの設定	• インターネットへの直接接続（選択済み） • 手動でのプロキシ設定 • 自動でのプロキシ設定	• インターネットへの直接接続（選択済み） • 手動でのプロキシ設定 • 自動でのプロキシ設定	—
ネットワークの適用	By User	By User	—

Cisco ISE での Chromebook デバイス アクティビティのモニタ

Cisco ISE は Chromebook のデバイスの認証と認可に関する情報を表示するさまざまなレポートとログを提供します。オン デマンドまたは定期的にこれらのレポートを実行できます。[操作（Operations）] > [RADIUS] > [ライブ ログ（Live Logs）] ページで、認証方法（たとえば、802.1x）と認証プロトコル（たとえば、EAP-TLS）を表示することができます。また、[ワークセンター（Work Center）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）] ページに移動して、Chromebook デバイスとして分類されたエンドポイントの数も識別できます。

オンボーディング中の Chromebook デバイスのトラブルシューティング

このセクションでは、Chromebook デバイスのオンボーディング中に発生する可能性のある問題について説明します。

- エラー：webstore から拡張をインストールできない：webstore から拡張をインストールできません。これは、ネットワーク管理者によって Chromebook デバイスに自動的にインストールされます。
- エラー：証明書のインストールを完了したが、セキュアなネットワークに接続できない：管理コンソールで、インストールした証明書が定義された発行者とサブジェクトの属性パターンと一致していることを確認します。以下からインストールされた証明書に関する情報を得ることができます。chrome://settings/certificates
- エラー：Chromebook でセキュアなネットワークに手動で接続しようとして、「ネットワーク証明書の取得（Obtain Network Certificate）」のエラー メッセージが表示される：[新しい証明書の取得（Get New Certificate）] をクリックしてブラウザを開き、証明書をインストールする ISE BYOD にリダイレクトされます。ただし、セキュアなネットワークに接続できない場合は、管理コンソールで、インストールされた証明書が定義された発行者とサブジェクトの属性パターンと一致していることを確認します。

- エラー：[新しい証明書の取得（Get New Certificate）] をクリックしたが、www.cisco.com に転送される：ユーザはISEにリダイレクトされ、証明書のインストールプロセスを開始するために、プロビジョニングするSSIDに接続する必要があります。適切なアクセス リストがこのネットワーク用に定義されていることを確認します。
- エラー：エラーメッセージ「管理対象デバイスのみがこの拡張を使用できます。ヘルプデスクまたはネットワーク管理者にお問い合わせください（Only managed devices can use this extension. Contact helpdesk or network administrator）」が表示される：Chromebookは管理対象デバイスであり、デバイスで証明書をインストールするには、拡張は、Chrome OS APIにアクセスするために強制インストールとして設定する必要があります。拡張は、Google Webストアからダウンロードして手動でインストールすることもできますが、登録されていないChromebookユーザは証明書をインストールすることはできません。

  登録されていないChromebookデバイスは、ユーザがドメインユーザ グループに属する場合に証明書を保護できます。拡張はデバイスのドメインユーザを追跡します。ただし、ドメイン ユーザは登録されていないデバイスのユーザ単位の認証キーを生成できます。
- エラー：Google の管理コンソールで SSID が接続された順番が不明：
  - いくつかの SSID（PEAP、および EAP-TLS）が Google の管理コンソールで設定された場合、証明書がインストールされ、属性が一致すると、Chrome OS は SSID が設定された順序にかかわらず、証明書ベースの認証を使用して SSID に自動的に接続します。
  - 2つのEAP-TLS SSIDが同じ属性で一致した場合、接続は、信号強度や他のネットワーク レベルの信号などの、ユーザまたは管理者で制御できないその他の要因に依存します。
  - 複数のEAP-TLSの証明書がChromebookデバイスにインストールされ、そのすべてが管理コンソールで設定された証明書パターンと一致した場合、一番新しい証明書が接続に使用されます。

Cisco AnyConnect セキュア モビリティ

Cisco ISEは、Cisco ISEポスチャ要件のAnyConnectで統合モジュールを使用します。AnyConnectは、同じエンドポイントのCisco ISE NAC Agentと共存するポスチャ エージェントです。一度にアクティブになるエージェントは1つのみです。

（注） Cisco AnyConnect は CWA フローをサポートしていません。[ワーク センター（Work Centers）] の [ゲスト アクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）][設定（Configure）]>[ゲスト ポータル（Guest Portals）] >[作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ゲスト デバイスのコンプライアンス設定（Guest Device Compliance Settings）] ページの [ゲスト デバイス コンプライアンスが必要（Require guest device compliance）] フィールドを使用してゲストポータルから AnyConnect をプロビジョニングすることはできません。代わりに、クライアント プロビジョニング ポータルで AnyConnect をプロビジョニングします。この方法を使用すると、許可権限で設定されているようにリダイレクションが実行されます。

（注） ネットワークのメディアを切り替えるときに、AnyConnect ISE ポスチャモジュールが変更後のネットワークを検出し、クライアントを再評価するように、デフォルトのゲートウェイを変更する必要があります。

Cisco ISE を AnyConnect エージェントと統合すると、Cisco ISE は次のように機能します。

- AnyConnect のバージョン 4.0 および以降のリリースを展開するためのステージング サーバとして機能する
- Cisco ISE ポスチャ要件の AnyConnect ポスチャ コンポーネントとやり取りする
- AnyConnect プロファイル、カスタマイズおよび言語パッケージ、および Windows と Mac OS X の各オペレーティング システムの OPSWAT のライブラリ更新の展開をサポートする
- AnyConnect およびレガシー エージェントを同時にサポートします

AnyConnect 設定の作成

AnyConnect 設定には、AnyConnect ソフトウェアおよび関連するコンフィギュレーション ファイルが含まれます。この設定は、ユーザがクライアントで AnyConnect リソースをダウンロードしてインストールできるクライアントプロビジョニングポリシーで使用できます。AnyConnect を展開するために ISE および ASA を使用した場合、設定は両方のヘッドエンドで一致する必要があります。

（注） VPN に接続するときに ISE ポスチャ モジュールをプッシュするには、シスコの Adaptive Security Device Manager（ASDM）GUI ツールを使用する Cisco 適応型セキュリティ アプライアンス（ASA）を使用して AnyConnect エージェントをインストールすることをお勧めします。ASA は、VPN ダウンローダを使用してインストールを行います。ダウンロードでは、ISE ポスチャ プロファイルは ASA によってプッシュされ、後続のプロファイルのプロビジョニングに必要なホスト検出が利用可能になってから、ISE ポスチャ モジュールが ISE に接続します。その一方、ISE では、ISE ポスチャ モジュールは ISE が検出された後にのみプロファイルを取得し、これがエラーの原因になることがあります。したがって、VPN に接続するとき ASA を ISE ポスチャ モジュールにプッシュすることを推奨します。

始める前に

AnyConnect 設定オブジェクトを設定する前に、次の手順を実行する必要があります。

1. Cisco ソフトウェアのダウンロードページから AnyConnect ヘッドエンド展開パッケージとコンプライアンスモジュールをダウンロードします。
2. これらのリソースを Cisco ISE にアップロードします（ローカル マシンからのシスコ提供のクライアント プロビジョニング リソースの追加 （1264 ページ）を参照）。
3. （任意）カスタマイズおよびローカライズのバンドルを追加します（ローカルマシンからの AnyConnect 用の顧客作成リソースの追加 （1265 ページ）を参照）。
4. AnyConnect のポスチャ エージェント プロファイルを設定します（ポスチャ エージェント プロファイルの作成 （1291 ページ）を参照）。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョン（Client Provision）] > [リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] をクリックして、AnyConnect 設定を作成します。

ステップ 3 [AnyConnect 設定（AnyConnect Configuration）] を選択します。

ステップ 4 以前にアップロードした AnyConnect パッケージを選択します。たとえば、AnyConnectDesktopWindows xxx.x.xxxxx.x を選択します。

ステップ 5 現在の AnyConnect 設定の名前を入力します。たとえば、AC Config xxx.x.xxxxx.x とします。

ステップ 6 以前にアップロードしたコンプライアンス モジュールを選択します。たとえば、AnyConnectComplianceModulewindows x.x.xxxx.x を選択します。

ステップ 7 1 つ以上の AnyConnect モジュールのチェックボックスをオンにします。たとえば、ISE ポスチャ、VPN、ネットワーク アクセス マネージャ、Web セキュリティ、AMP イネーブラ、ASA ポスチャ、Start Before Log on（Windows OS のみ）、Diagnostic and Reporting Tool の中から、1 つ以上のモジュールを選択します。

（注） [AnyConnect モジュール選択（AnyConnect Module Selection）] で VPN モジュールをオフにしても、プロビジョニングされたクライアントの VPN タイルは無効になりません。AnyConnect GUI の VPN タイルを無効にするには、VPNDisable_ServiceProfile.xml を設定する必要があります。AnyConnect がデフォルトの場所にインストールされているシステムでは、このファイルは C:\Program Files\Cisco にあります。AnyConnect が別の場所にインストールされている場合、このファイルは <AnyConnect がインストールされているパス>\Cisco にあります。

ステップ 8 選択した AnyConnect モジュール用の AnyConnect プロファイルを選択します。たとえば、ISE ポスチャ、VPN、NAM および Web セキュリティを選択します。

ステップ 9 AnyConnect カスタマイズ バンドルおよびローカリゼーション バンドルを選択します。

ステップ 10 [送信（Submit）] をクリックします。

ポスチャ エージェント プロファイルの作成

AnyConnect ポスチャのエージェント プロファイルを作成するには、次の手順を実行します。このプロファイルでは、ポスチャ プロトコルのエージェントの動作を定義するパラメータを指定できます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [NAC AnyConnect エージェント ポスチャ プロファイル（NAC AnyConnect Agent Posture Profile）] を選択します。

ステップ 4 [ポスチャ エージェント プロファイルの設定（Posture Agent Profile Settings）] で、[AnyConnect]

ステップ 5 次のパラメータを設定します。

- Cisco ISE ポスチャ エージェントの動作
- クライアント IP アドレスの変更
- Cisco ISE ポスチャ プロトコル

ステップ 6 [送信（Submit）] をクリックします。

クライアント IP アドレスのリフレッシュ設定

次の表に、VLAN の変更後に IP アドレスをリフレッシュするようにクライアントのパラメータを設定できる [NAC AnyConnect ポスチャ プロファイル（NAC AnyConnect Posture Profile）] ページのフィールドを示します。このページへのナビゲーションパスは、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）] > [NAC または AnyConnect

ポスチャプロファイル（NAC or AnyConnect Posture Profile）][NAC または AnyConnect ポスチャプロファイル（NAC or AnyConnect Posture Profile）]です。

フィールド	デフォルト値（**Default Value**）	モード（**Cisco NAC Agent** にのみ該当）	使用上のガイドライン
VLAN 検出間隔（VLAN detection interval）	0、5	マージ	この設定は、エージェントが VLAN 変更をチェックする間隔です。 Windows NAC エージェントの場合、デフォルト値は 0 です。デフォルトでは、認証 VLAN 変更機能へのアクセスは Windows に対して無効にされます。有効な値の範囲は 0 ～ 5 秒です。 Mac OS X エージェントの場合、デフォルト値は 5 です。Mac OS X のデフォルトでは、認証 VLAN 変更機能へのアクセスは、VlanDetectInteval を 5 秒として有効になっています。有効な範囲は 5 ～ 900 秒です。 0：認証 VLAN 変更機能へのアクセスは無効化されます。 1 ～ 5：エージェントはインターネット制御メッセージプロトコル（ICMP）またはアドレス解決プロトコル（ARP）クエリーを 5 秒ごとに送信します。 6 ～ 900：ICMP/ARP クエリーが x 秒ごとに送信されます。

フィールド	デフォルト値（Default Value）	モード（Cisco NAC Agent にのみ該当）	使用上のガイドライン
UI なしの VLAN 検出の有効化（Enable VLAN detection without UI）（Mac OS X クライアントには適用できません）	なし	マージ	この設定は、ユーザがログインしていないときでも VLAN 検出を有効または無効にします。 No：VLAN 検出機能は無効です。 Yes：VLAN 検出機能が有効です。
再試行検出数（Retry detection count）	3	マージ	インターネット制御メッセージプロトコル（ICMP）またはアドレス解決プロトコル（ARP）ポーリングが失敗する場合、この設定で、クライアント IP アドレスをリフレッシュする前に x 回再試行するようにエージェントを設定します。
Ping または ARP（Ping or ARP）	[0] 有効な範囲は 0 ～ 2 です。	マージ	この設定は、クライアント IP アドレスの変更を検出するために使用する方式を指定します。 0：ICMP を使用してポーリング 1：ARP を使用してポーリング 2：最初に ICMP を使用し、（ICMP が失敗した場合は）ARP を使用してポーリング
ping の最大タイムアウト（Maximum timeout for ping）	1 有効な値の範囲は 1 ～ 10 秒です。	マージ	ICMP を使用してポーリングし、指定した時間内に応答がない場合は、ICMP ポーリングの失敗を宣言します。

フィールド	デフォルト値（Default Value）	モード（Cisco NAC Agent にのみ該当）	使用上のガイドライン
エージェント IP のリフレッシュの有効化（Enable agent IP refresh）	Yes（デフォルト）	上書き	この設定は、スイッチ（または WLC）が各スイッチポートでクライアントのログインセッション用 VLAN を変更した後にクライアント マシンが IP アドレスをリフレッシュするかどうかを指定します。
DHCP 更新遅延（DHCP renew delay）	[0] 有効な値の範囲は 0 ～ 60 秒です。	上書き	この設定は、ネットワーク DHCP サーバからの新しい IP アドレスの要求を試行する前に、クライアントマシンが待機するように指定します。
DHCP リリース遅延（DHCP release delay）	[0] 有効な値の範囲は 0 ～ 60 秒です。	上書き	この設定は、現在の IP アドレスをリリースする前にクライアントマシンが待機するように指定します。

（注） パラメータ値は、既存のエージェントプロファイル設定とマージするか、または上書きして、Windows および Mac OS X クライアントで適切に IP アドレスがリフレッシュされるように設定します。

ポスチャ プロトコル設定

次の表に、Cisco ISE で AnyConnect のポスチャ プロトコル設定を設定できる [NACまたは AnyConnectのポスチャプロファイル（NAC or AnyConnect Posture Profile）] ページのフィールドを示します。Anyconnect のポスチャ プロトコル設定のその他のフィールドについては、お使いのバージョンの AnyConnect の『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

フィールド	デフォルト値（Default Value）	使用上のガイドライン
[Call Home リスト（Call Home List）]	—	IP アドレスとポートをコロンで結んだカンマ区切りリストを入力します。
[バックオフ タイマー（Back-off Timer）]	30 秒	この設定により、Anyconnect エージェントは最大時間制限に達するまでディスカバリ パケットを送信することで、ディスカバリ ターゲット（リダイレクション ターゲットおよび以前に接続していた PSN）に継続的に到達できます。有効な値の範囲は 10 ～ 600 秒です。

継続的なエンドポイント属性モニタリング

ポスチャ アセスメントの実行中に動的な変更が確認されるようにするため、AnyConnect エージェントを使用してさまざまなエンドポイント属性を継続的にモニタします。これによりエンドポイントの全体的な可視性が向上し、動作に基づいてポスチャ ポリシーを作成できるようになります。AnyConnect エージェントは、エンドポイントにインストールされ実行されているアプリケーションをモニタします。この機能をオンまたはオフにできます。また、データのモニタ頻度を設定できます。デフォルトでは、データは5分間隔で収集され、データベースに保存されます。初回ポスチャでは、AnyConnectがすべての実行中アプリケーションとインストールされているアプリケーションのリストを報告します。初回ポスチャの後に、AnyConnectエージェントはX分間隔でアプリケーションをスキャンし、最終スキャンでの差異をサーバに送信します。サーバはすべての実行中アプリケーションとインストールされているアプリケーションのリストを表示します。

Cisco Web Agent

Cisco Web Agent では、クライアント マシンのための一時的なポスチャ評価を提供します。

ユーザは Cisco Web Agent 実行ファイルを起動することができ、ActiveX コントロールまたは Java アプレットによって、クライアント マシンの一時ディレクトリに Web Agent ファイルがインストールされます。

Cisco Web Agent は、ユーザがログインすると、ユーザ ロールまたはオペレーティング システムに設定された要件を Cisco ISE サーバから取得し、必要なパッケージのホスト レジストリ、プロセス、アプリケーション、およびサービスをチェックし、レポートを Cisco ISE サーバに送信します。クライアントマシンに関する要件が満たされている場合、ユーザはネットワークにアクセスできます。要件が満たされていない場合、Web Agent は満たされていない要件ごとに、ユーザにダイアログを表示します。ダイアログにより、クライアントマシンの要件を満た

すための手順および対処法が提供されます。あるいは、指定された要件が満たされない場合は、ユーザ ログイン ロールの要件を満たすようにクライアント システムの修復試行中は制限付きのネットワーク アクセスを受け入れるという選択もできます。

（注） ActiveX は 32 ビット版の Internet Explorer でのみサポートされます。Firefox Web ブラウザまたは 64 ビット版の Internet Explorer のバージョンでは、ActiveX をインストールできません。

クライアント プロビジョニング リソース ポリシーの設定

クライアントの場合、どのユーザがリソース（エージェント、エージェント コンプライアンス モジュール、エージェント カスタマイズ パッケージ/プロファイル）のどのバージョン（または複数のバージョン）をログイン時およびユーザ セッション開始時に Cisco ISE から受信するかは、クライアント プロビジョニング リソース ポリシーによって決定されます。

AnyConnect の場合、クライアント プロビジョニング リソース ページからリソースを選択し、クライアント プロビジョニング ポリシー ページで使用できる AnyConnect 設定を作成することができます。AnyConnect 設定は、AnyConnect ソフトウェアとそのさまざまなコンフィギュレーション ファイルとの関連付けであり、これらのファイルには、Windows および Mac OS X クライアントの AnyConnect バイナリ パッケージ、コンプライアンス モジュール、モジュール プロファイル、AnyConnect のカスタマイズおよび言語パッケージなどがあります。

始める前に

- 有効なクライアント プロビジョニング リソース ポリシーを作成する前に、Cisco ISE にリソースを追加したことを確認します。エージェント コンプライアンス モジュールをダウンロードすると、システムで使用している既存のモジュールがあれば常にそれが上書きされます。
- クライアント プロビジョニング ポリシーで使用されているネイティブのサプリカント プロファイルをチェックして、ワイヤレス SSID が正しいことを確認します。iOS デバイスの場合、接続対象ネットワークが非表示の場合は、[iOSの設定（iOS Settings）] エリアで [ターゲットネットワークが非表示になっている場合に有効にする（Enable if target network is hidden）] チェック ボックスをオンにします。
- 証明書属性に基づく条件を含むクライアント プロビジョニング ルールについては、「証明書ベースの条件のための前提条件」のセクションを参照してください。

ステップ 1 **[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 動作のドロップダウン リストから **Enable**、**Disable**、または **Monitor** を選択します。

- **Enable**：ユーザがネットワークにログインし、クライアントプロビジョニングポリシーのガイドラインに従っている場合に、Cisco ISEがこのポリシーを使用して、クライアントプロビジョニング機能を果たすようにします。
- **Disable**：Cisco ISE は、指定されたリソース ポリシーを使用せずにクライアント プロビジョニング機能を果たします。
- **Monitor**：ポリシーを無効にし、クライアント プロビジョニング セッション要求を監視し、Cisco ISE が [モニタ対象（Monitored）] のポリシーに基づいて起動しようとした回数を確認します。

ステップ 3 [ルール名（Rule Name）] テキスト ボックスに、新しいリソース ポリシーの名前を入力します。

ステップ 4 Cisco ISE にログインするユーザが属する ID グループを 1 つ以上指定します。

設定した既存の ID グループのリストから、あらゆる ID タイプを指定することも、1 つ以上のグループを選択することもできます。

ステップ 5 [オペレーティング システム（Operating Systems）] フィールドを使用して、ユーザが Cisco ISE にログインする際に使用するクライアント マシンまたはデバイスで動作している 1 つ以上のオペレーティング システムを指定します。

[Android]、[Mac iOS]、[Mac OS X] などの単一のオペレーティング システムや、[Windows XP（すべて）（Windows XP (All)）] や [Windows 7（すべて）（Windows 7 (All)）] など、複数のクライアント マシン オペレーティング システムに対応する包括的なオペレーティング システムの指定を選択できます。

（注） Cisco ISE GUI のクライアント プロビジョニング ポリシー ページに、MAC OS 10.6/10.7/10.8 を選択できるオプションがありますが、これらのバージョンはAnyConnectではサポートされていません。

ステップ 6 [その他の条件（Other Conditions）] フィールドで、この特定のリソース ポリシー用に作成する新しい式を指定します。

ステップ 7 クライアント マシンの場合は、[エージェント設定（Agent Configuration）] を使用して、クライアント マシンで利用可能にし、プロビジョニングするエージェント タイプ、コンプライアンス モジュール、エージェント カスタマイズ パッケージ/プロファイルを指定します。

クライアントマシンでエージェントがポップアップできるようにするには、クライアントプロビジョニングのURLを許可ポリシーに含める必要があります。これにより、ランダムなクライアントからの要求が回避され、適切なリダイレクトURLを持つクライアントのみがポスチャ評価を要求できるようになります。

ステップ 8 **Save** をクリックします。

次のタスク

1 つ以上のクライアント プロビジョニング リソース ポリシーを正常に設定したら、ログイン中にクライアント マシンのポスチャ評価を実行するように Cisco ISE の設定を開始できます。

クライアント プロビジョニング ポリシーの Cisco ISE ポスチャ エージェントの設定

クライアントマシンについては、エージェントタイプ、コンプライアンスモジュール、エージェント カスタマイズ パッケージ/プロファイルを、ユーザがクライアントマシンにダウンロードおよびインストールできるように設定します。

始める前に

Cisco ISE の AnyConnect のクライアント プロビジョニング リソースを追加している必要があります。

ステップ 1 **Agent** ドロップダウン リストから使用可能なエージェントを選択し、ここで定義したエージェントのアップグレード（ダウンロード）がクライアント マシンに対して必須かどうかを、**Is Upgrade Mandatory** オプションを必要に応じて有効または無効にすることによって指定します。

Is Upgrade Mandatory 設定は、エージェントのダウンロードにのみ適用されます。エージェント プロファイル、コンプライアンス モジュール、およびエージェント カスタマイズ パッケージの更新は常に必須です。

ステップ 2 **Profile** ドロップダウン リストから既存のエージェント プロファイルを選択します。

ステップ 3 **Compliance Module** ドロップダウン リストを使用して使用可能なコンプライアンス モジュールを選択し、クライアント マシンにダウンロードします。

ステップ 4 **Agent Customization Package** ドロップダウン リストから、クライアント マシンに使用可能なエージェント カスタマイズ パッケージを選択します。

パーソナル デバイスのネイティブ サプリカントの設定

従業員は、Windows、Mac OS、iOS、および Android デバイスで使用可能なネイティブ サプリカントを使用して、ネットワークに自分のパーソナルデバイスを直接接続できます。パーソナル デバイスに関して、登録されているパーソナル デバイスで使用可能にし、プロビジョニングするネイティブ サプリカントの設定を指定します。

始める前に

ユーザがログインするとき、そのユーザの許可要件と関連付けるプロファイルに基づいて、Cisco ISE が、ユーザのパーソナル デバイスを設定するために必要なサプリカント プロビジョニング ウィザードを提供して、ネットワークにアクセスするように、ネイティブ サプリカント プロファイルを作成します。

ステップ 1 **[ポリシー（Policy）]** > **[クライアント プロビジョニング（Client Provisioning）]** を選択します。

ステップ 2 動作のドロップダウン リストから **Enable**、**Disable**、または **Monitor** を選択します。

ステップ 3 [ルール名（Rule Name）] テキスト ボックスに、新しいリソース ポリシーの名前を入力します。

ステップ 4 次を指定します。

- [ID グループ（Identity Groups）] フィールドを使用して、Cisco ISE にログインするユーザが属する ID グループを 1 つ以上指定します。
- [オペレーティング システム（Operating System）] フィールドを使用して、ユーザが Cisco ISE にログインする際に使用するパーソナル デバイスで動作している 1 つ以上のオペレーティング システムを指定します。
- [その他の条件（Other Conditions）] フィールドを使用して、この特定のリソース ポリシー用に作成する新しい式を指定します。

ステップ 5 パーソナル デバイスの場合、[ネイティブサプリカントの設定（Native Supplicant Configuration）] を使用し、特定の**Configuration Wizard**を選択して、パーソナル デバイスに配信します。

ステップ 6 指定されたパーソナル デバイス タイプに適用可能な **Wizard Profile** を指定します。

ステップ 7 [**保存（Save**）] をクリックします。

クライアント プロビジョニング レポート

Cisco ISE のモニタリングおよびトラブルシューティング機能にアクセスし、ユーザ ログイン セッションの成功または失敗の全体のトレンドをチェックし、特定の期間にネットワークにログインしたクライアントマシンの数およびタイプに関する統計情報を収集し、また、クライアント プロビジョニング リソースでの最近の設定変更をチェックすることができます。

クライアント プロビジョニングの要求

[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [エンドポイントおよびユーザ（Endpoints and Users）] > [クライアント プロビジョニング（Client Provisioning）] レポートには、クライアントプロビジョニング要求の成功および失敗に関する統計情報が表示されます。**Run** を選択していずれかのプリセット期間を指定すると、Cisco ISE によってデータベースが調べられ、生成されたクライアント プロビジョニング データが表示されます。

サプリカント プロビジョニングの要求

[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] > [エンドポイントおよびユーザ（Endpoints and Users）] > [サプリカント プロビジョニング（Supplicant Provisioning）] ウィンドウには、最近の成功および失敗したユーザ デバイス登録およびサプリカント プロビジョニング要求に関する情報が表示されます。**Run** を選択していずれかのプリセット期間を指定すると、Cisco ISE によってデータベースが調べられ、生成されたサプリカント プロビジョニング データが表示されます。

サプリカント プロビジョニング レポートは、特定の期間にデバイス登録ポータルから登録されたエンドポイントのリストに関する情報が提供されます。これには、ログイン日時、ID（ユーザ ID）、IP アドレス、MAC アドレス（エンドポイント ID）、サーバ プロファイル、エンド

ポイント オペレーティング システム、SPW バージョン、障害理由（ある場合）、登録のステータスなどのデータが含まれます。

クライアント プロビジョニング イベント ログ

クライアントの動作の問題の診断に役立つイベント ログ エントリを検索できます。たとえば、ネットワーク上のクライアント マシンがログイン時にクライアント プロビジョニング リソースの更新を取得できないという問題の原因を特定する必要がある場合があります。ポスチャおよびクライアントプロビジョニングの監査、ポスチャおよびクライアントプロビジョニングの診断のロギング エントリを使用できます。

クライアントプロビジョニングポータルのポータル設定

これらの設定へのナビゲーション パスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[クライアント プロビジョニング ポータル（Client Provisioning Portals）]** > **[作成、編集、複製または削除（Create, Edit, Duplicate, or Delete）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** です。

ポータル設定

- HTTPS ポート（HTTPS Port）：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合、この制限に従うようにポート設定を変更する必要があります。
- 使用可能インターフェイス（Allowed interfaces）：ポータルを実行できる PSN インターフェイスを選択します。PSN で使用可能なインターフェイスを備えた PSN のみがポータルを作成できます。物理およびボンディングされたインターフェイスの任意の組み合わせを設定できます。これは PSN 全体の設定です。すべてのポータルはこれらのインターフェイスでのみ動作し、このインターフェイス設定はすべての PSN に適用されます。
  - 異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名は、インターフェイス IP に解決される必要があります。
  - ISE CLI の ip host x.x.x.x yyy.domain.com をセカンダリ インターフェイス IP と FQDN をマッピングするように設定します。これは証明書のサブジェクト名/サブジェクトの代替名を一致させるために使用されます。

- ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディングインターフェイスを設定しようとします。これが成功しない場合、その PSN にボンド セットがなかったことが原因である可能性があるので、PSNはエラーを記録して終了します。物理インターフェイスでポータルを開始しようとはしません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために2つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理NIC と対応するボンディングされたNICの両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSNは物理インターフェイスでポータルを開始しようとします。

- 証明書グループ タグ（Certificate group tag）：ポータルの HTTPS トラフィックに使用する証明書グループのグループ タグを選択します。
- [認証方式（Authentication Method）]：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP などがあります。

  Cisco ISE には、クライアント プロビジョニング ポータル用のデフォルトのクライアント プロビジョニング ID ソース順序 Certificate_Portal_Sequence が含まれています。

- 完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）：クライアント プロビジョニング ポータル用に少なくとも 1 つの一意の FQDN、ホスト名、またはその両方を入力します。たとえば、「provisionportal.yourcompany.com」と入力した場合、ユーザはこれらのいずれかをブラウザに入力して証明書プロビジョニング ポータルに到達できます。
  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに確実に解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

（注） URL リダイレクトなしのクライアントプロビジョニングの場合、[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）] フィールドに入力するポータル名は、DNS 設定で設定されている必要があります。URL リダイレクトなしのクライアント プロビジョニングを有効にするため、この URL をユーザに通知する必要があります。

- アイドル タイムアウト（Idle timeout）：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

（注） クライアント プロビジョニング ポータルではポート番号と証明書を定義できます。これにより、ホストはクライアントプロビジョニングとポスチャに同じ証明書をダウンロードすることを許可します。ポータル証明書が正式な認証局により署名されている場合、セキュリティ警告は表示されません。自己署名証明書の場合、ポータルと Cisco AnyConnect Posture コンポーネントの両方でセキュリティ警告を受け取ります。

ログイン ページの設定（Login Page Settings）

- [ログインの有効化（Enable Login）]：クライアント プロビジョニング ポータルのログイン手順を有効にするには、このチェック ボックスを選択します
- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：単一のブラウザ セッションからのログイン試行失敗回数を指定します。この回数を超過すると、Cisco ISE はログイン試行を実行できる頻度を意図的に低下させて、追加のログイン試行を防ぎます。ログイン失敗がこの回数に達した後のログイン試行の間隔は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で指定されます。
- [頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）]：[頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間を分単位で設定します。
- [AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）]：会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
- [同意が必要（Require acceptance）]：ポータルにアクセスする前にユーザが AUP を受け入れることを要求します。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。AUP を受け入れないユーザは、ポータルにアクセスできません。

- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。

利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP を含める（Include an AUP）]：会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：ユーザが AUP を完全に読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。
- [初回のログインのみ（On first login only）]：ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
- [ログインごと（On every login）]：ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [_ 日ごと（初回のログインから）（Every _____ days (starting at first login)）]：ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。

ポストログイン バナー ページ設定（Post-Login Banner Page Settings）

[ポストログイン バナー ページを含める（Include a Post-Login Banner page）]：ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

パスワード変更設定（Change Password Settings）

[内部ユーザに自身のパスワードの変更を許可する（Allow internal users to change their own passwords）]：従業員がクライアント プロビジョニング ポータルにログインして、自分のパスワードを変更できるようにします。これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

関連トピック

クライアント プロビジョニング ポータル （877 ページ）
クライアント プロビジョニング ポータルの作成 （894 ページ）
クライアント プロビジョニング ポータルの言語ファイルの HTML サポート （534 ページ）

クライアントプロビジョニングポータルの言語ファイルの HTML サポート

このポータルの [説明テキスト（Instructional Text）]、[コンテンツ（Content）]、[任意のコンテンツ 1（Optional Content 1）]、および [任意のコンテンツ 2（Optional Content 2）] テキスト ボックスへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [クライアント プロビジョニング ポータル（Client Provisioning Portals）] > [編集（Edit）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [ページ（Pages）]** です。テキスト ボックスのミニ エディタの [HTML ソースの表示（View HTML Source）] アイコンを使用して、コンテンツに HTML コードを追加できます。

ポータルの言語プロパティ ファイルの次のディクショナリ キーで、テキスト内の HTML がサポートされています。

（注） これは、ファイル内のディクショナリ キーの完全なリストではありません。

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1

- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

第 12 章

脅威の封じ込め

脅威中心型 NAC サービス

脅威中心型ネットワーク アクセス コントロール（TC-NAC）機能により、脅威および脆弱性のアダプタから受信する脅威と脆弱性の属性に基づいて、許可ポリシーを作成できます。脅威の重大度レベルと脆弱性評価の結果は、エンドポイントまたはユーザのアクセス レベルを動的に制御するために使用できます。

忠実度の高い侵害の兆候（IoC）、脅威検出イベント、およびCVSS スコアを Cisco ISE に送信するように脆弱性および脅威のアダプタを設定できます。これにより、エンドポイントの権限とコンテキストを適宜変更するための脅威中心型アクセス ポリシーを作成できます。

Cisco ISE では次のアダプタがサポートされています。

- SourceFire FireAMP
- Cognitive Threat Analytics（CTA）アダプタ
- Qualys

（注） TC-NAC フローで現在サポートされているのは Qualys Enterprise Edition のみです。

- Rapid7 Nexpose
- Tenable Security Center

エンドポイントの脅威イベントが検出されたら、[侵害されたエンドポイント（Compromised Endpoints）] ページでエンドポイントの MAC アドレスを選択して ANC ポリシー（Quarantine など）を適用できます。Cisco ISE は、そのエンドポイントに対して CoA をトリガーし、対応する ANC ポリシーを適用します。ANC ポリシーが使用可能ではない場合、Cisco ISE はそのエンドポイントに対して CoA をトリガーし、元の許可ポリシーを適用します。[侵害されたエンドポイント（Compromised Endpoints）] ページの [脅威と脆弱性のクリア（Clear Threat and Vulnerabilities）] オプションを使用して、（Cisco ISE システム データベースから）エンドポイントに関連付けられている脅威と脆弱性をクリアできます。

脅威ディクショナリには次の属性がリストされます。

- CTA-Course_Of_Action（値は Internal Blocking、Eradication、または Monitoring です。）
- Qualys-CVSS_Base_Score
- Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

Base Score 属性と Temporal Score 属性の有効な範囲は 0 ~ 10 です。

脆弱性イベントがエンドポイントに受信されると、Cisco ISE はそのエンドポイントの CoA をトリガーします。ただし、脅威イベントの受信時には CoA はトリガーされません。

脆弱性属性を使用して、属性の値に基づいて脆弱なエンドポイントを自動的に隔離する許可ポリシーを作成できます。次に例を示します。

```
Any Identity Group & Threat:Qualys-CVSS_Base_Score > 7.0 -> Quarantine
```

脅威中心型 NAC サービスを有効にする際には、次の点に注意してください。

- 脅威中心型 NAC サービスを使用するには、Apex ライセンスが必要です。
- 脅威中心型 NAC サービスは、展開内の 1 つのノードでのみ有効にできます。
- 脆弱性アセスメント サービスでは、ベンダーあたり 1 つのアダプタ インスタンスだけを追加できます。ただし、FireAMP アダプタ インスタンスは複数追加できます。
- 設定を失わずにアダプタを停止、再開できます。アダプタの設定後は、任意の時点でアダプタを停止できます。ISE サービスの再起動時でもアダプタはこの状態のままになります。アダプタを再起動するには、アダプタを選択して [再起動（Restart）] をクリックします。

（注） アダプタが [停止（Stopped）] 状態の場合、アダプタ インスタンスの名前だけを編集できます。アダプタ設定や詳細設定は編集できません。

[脅威中心型 NAC ライブ ログ（Threat Centric NAC Live Logs）] ページ（[操作（Operations）] > [TC NAC ライブ ログ（TC NAC Live Log）]）には、脅威イベントと脆弱性イベントがすべて表示されます。エンドポイントのインシデント タイプ、アダプタ名、一致する許可ルール、許可プロファイル（新しいプロファイルと古いプロファイル）が表示されます。また、イベントの詳細情報も確認できます。

エンドポイントの脅威情報は次に示すページで確認できます。

- [ホーム（Home）] ページ > [脅威（Threat）] ダッシュボード
- [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [侵害されたエンドポイント（Compromised Endpoints）]

脅威中心型 NAC サービスによりトリガーされるアラームを次に示します。

- Adapter not reachable（syslog ID：91002）：アダプタに到達できないことを示します。
- Adapter Connection Failed（syslog ID：91018）：アダプタに到達できるが、アダプタとソース サーバの間の接続がダウンしていることを示します。
- Adapter Stopped Due to Error（syslog ID：91006）：このアラームは、アダプタが必要な状態になっていない場合にトリガーされます。このアラームが表示されたら、アダプタ設定とサーバ接続を調べてください。詳細については、アダプタ ログを参照してください。
- Adapter Error（syslog ID：91009）：Qualys アダプタが Qualys サイトとの接続を確立できないか、またはこのサイトから情報をダウンロードできないことを示します。

脅威中心型 NAC サービスで使用できるレポートを次に示します。

- アダプタのステータス：アダプタのステータス レポートには、脅威と脆弱性のアダプタのステータスが表示されます。
- COA イベント：エンドポイントの脆弱性イベントを受信すると、Cisco ISE はそのエンドポイントについて CoA をトリガーします。CoA イベント レポートには、これらの CoA イベントのステータスが表示されます。また、これらのエンドポイントの新旧の認証ルールとプロファイルの詳細が表示されます。
- 脅威イベント：脅威イベント レポートには、設定したさまざまなアダプタから Cisco ISE が受信した脅威イベントがすべて表示されます。脆弱性アセスメントのイベントは、このレポートには含まれません。
- 脆弱性アセスメント：脆弱性アセスメント レポートには、エンドポイントで実行中のアセスメントに関する情報が示されます。このレポートを表示して、設定されたポリシーに基づいてアセスメントが行われているかどうかを確認することができます。

[操作（Operations）] > [レポート（Reports）] > [診断（Diagnostics）] > [ISE カウンタ（ISE Counters）] > [しきい値カウンタのトレンド（Threshold Counter Trends）] で、次の情報を確認できます。

- 受信したイベントの総数
- 脅威イベントの総数

- 脆弱性イベントの総数
- （PSN に対して）発行された CoA の総数

これらの属性の値は 5 分おきに収集されるため、この値は直近 5 分間の数を表します。

[脅威（Threat）] ダッシュボードには次のダッシュレットが表示されます。

- [侵害されたエンドポイントの総数（Total Compromised Endpoints）] ダッシュレットには、ネットワーク上で現在影響を受けているエンドポイント（接続エンドポイントと切断エンドポイントの両方）の総数が表示されます。
- [特定期間における侵害されたエンドポイント（Compromised Endpoints Over Time）] ダッシュレットには、指定された期間におけるエンドポイントへの影響の履歴ビューが表示されます。
- [上位の脅威（Top Threats）] ダッシュレットには、影響を受けるエンドポイントの数と脅威の重大度に基づく上位の脅威が表示されます。
- [脅威ウォッチリスト（Threats Watchlist）] ダッシュレットを使用して、選択したイベントのトレンドを分析できます。

[上位の脅威（Top Threats）] ダッシュレットでは、バブルのサイズが影響を受けるエンドポイントの数を示し、薄い影が付いているエリアが切断されているエンドポイントの数を示します。色と縦方向の目盛りで脅威の重大度を示します。脅威には、インディケータとインシデントという 2 つのカテゴリがあります。インディケータの重大度属性は「Likely_Impact」、インシデントの重大度属性は「Impact_Qualification」です。

[侵害されたエンドポイント（Compromised Endpoint）] ページには、影響を受けるエンドポイントのマトリックス ビューと、各脅威カテゴリの影響の重大度が示されます。エンドポイントの詳細な脅威情報を表示するには、デバイス リンクをクリックします。

[実行されたアクション（Course Of Action）] チャートには、CTA アダプタから受信した CTA-Course_Of_Action 属性に基づき、脅威インシデントに対して実行されたアクション（[内部ブロック（Internal Blocking）]、[撲滅（Eradication）]、または [モニタリング（Monitoring）]）が表示されます。

[ホーム（Home）] ページの [脆弱性（Vulnerability）] ダッシュボードには、次のダッシュレットが表示されます。

- [脆弱なエンドポイントの総数（Total Vulnerable Endpoints）] ダッシュレットには、指定された値よりも大きい CVSS スコアを持つエンドポイントの総数が表示されます。また、CVSS スコアが指定された値よりも大きい接続エンドポイントと切断エンドポイントの総数も表示されます。
- [上位の脆弱性（Top Vulnerability）] ダッシュレットには、影響を受けるエンドポイントの数または脆弱性の重大度に基づく上位の脅威が表示されます。[上位の脆弱性（Top Vulnerability）] ダッシュレットでは、バブルのサイズが影響を受けるエンドポイントの数を示し、薄い影が付いているエリアが切断されているエンドポイントの数を示します。色と縦方向の目盛りで脆弱性の重大度を示します。

- [脆弱性ウォッチリスト（Vulnerability Watchlist）] ダッシュレットを使用して、一定期間にわたる選択した脆弱性のトレンドを分析できます。ダッシュレットで検索アイコンをクリックし、ベンダー固有の ID（Qualys の ID 番号の場合は「qid」）を入力して、その ID 番号の傾向を選択して表示します。
- [特定期間における脆弱なエンドポイント（Vulnerable Endpoints Over Time）] ダッシュレットには、一定期間におけるエンドポイントへの影響の履歴ビューが表示されます。

[脆弱なエンドポイント（Vulnerable Endpoints）] ページの [CVSS 別エンドポイント数（Endpoint Count By CVSS）] グラフには、影響を受けるエンドポイントの数とその CVSS スコアが表示されます。[脆弱なエンドポイント（Vulnerable Endpoints）] ページでは、影響を受けるエンドポイントのリストも表示されます。各エンドポイントの詳細な脆弱性情報を表示するには、デバイス リンクをクリックします。

脅威中心型 NAC サービス ログはサポート バンドルに含まれています（『』の「Cisco ISE ログ ファイルのダウンロード」のセクションCisco ISE ログ ファイルのダウンロード（1588 ページ）を参照してください）。脅威中心型 NAC サービス ログは support/logs/TC-NAC/ にあります。

脅威中心型 NAC サービスの有効化

脆弱性と脅威のアダプタを設定するには、まず脅威中心型 NAC サービスを有効にする必要があります。このサービスは、導入内の 1 つのポリシー サービス ノードでのみ有効にできます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 脅威中心型 NAC サービスを有効にする PSN の隣にあるチェック ボックスにマークを付けて、[編集（Edit）] をクリックします。

ステップ 3 [脅威中心型 NAC サービスの有効化（Enable Threat Centric NAC Service）] チェック ボックスにマークを付けます。

ステップ 4 [保存（**Save**）] をクリックします。

関連トピック

SourceFire FireAMP アダプタの追加 （1311 ページ）
Cognitive Threat Analytics アダプタの追加 （1313 ページ）
CTA アダプタの許可プロファイルの設定 （1315 ページ）
Course of Action 属性を使用した許可ポリシーの設定 （1315 ページ）
脅威中心型 NAC サービス （1307 ページ）

SourceFire FireAMP アダプタの追加

始める前に

- SourceFire FireAMP のアカウントが必要です。

- すべてのエンドポイントの FireAMP クライアントを導入する必要があります。
- 脅威中心型 NAC サービスを展開ノードで有効にする必要があります（脅威中心型 NAC サービスの有効化 （1311 ページ）を参照）。
- FireAMP アダプタは REST API コール（AMP クラウドへ）、およびイベントを受信する AMQP に SSL を使用します。また、プロキシの使用をサポートしています。FireAMP アダプタは通信にポート 443 を使用します。

ステップ 1 [管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サード パーティ ベンダー（Third Party Vendors）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから [AMP：脅威（AMP：Threat）] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ベンダー インスタンスのリスト ページを更新します。ベンダー インスタンスのリスト ページでアダプタのステータスが [設定準備完了（Ready to Configure）] に変更された後でのみ、アダプタを設定できます。

ステップ 7 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 8 （オプション）すべてのトラフィックをルーティングするように SOCKS プロキシ サーバを設定した場合、プロキシ サーバのホスト名とポート番号を入力します。

ステップ 9 接続するクラウドを選択します。US クラウドまたは EU クラウドを選択できます。

ステップ 10 サブスクライブするイベント ソースを選択します。次のオプションを使用できます。

- [AMP イベントのみ（AMP events only）]
- [CTA イベントのみ（CTA events only）]
- [CTA と AMP のイベント（CTA and AMP events）]

ステップ 11 FireAMP リンクをクリックし、admin として FireAMP にログインします。[アプリケーション（Applications）] ペインの [許可（Allow）] をクリックして、ストリーミング イベント エクスポート要求を許可します。
Cisco ISE にリダイレクトします。

ステップ 12 監視するイベントを選択します（たとえば、不審なダウンロード、疑わしいドメインへの接続、実行されたマルウェア、Java 侵害）。

詳細設定の変更またはアダプタの再設定時に、AMPクラウドに新しいイベントが追加されている場合、これらのイベントも [イベントリスト（Events Listing）] ページに表示されます。

アダプタ用のログ レベルを選択できます。選択可能なオプションは、[エラー（Error）]、[情報（Info）]、[デバッグ（Debug）] です。

アダプタ インスタンスの設定の要約が [設定サマリー（Configuration Summary）] ページに表示されます。

Cognitive Threat Analytics アダプタの追加

始める前に

- 脅威中心型 NAC サービスを展開ノードで有効にする必要があります（脅威中心型 NAC サービスの有効化 （1311 ページ）を参照）。
- http://cognitive.cisco.com/login から Cisco Cognitive Threat Analytics（CTA）ポータルにログインし、CTA STIX/TAXII サービスを要求します。詳細については、『Cisco ScanCenter Administrator Guide』を参照してください。
- Cognitive Threat Analytics（CTA）アダプタは、SSL とともに TAXII プロトコルを使用して、CTA クラウドをポーリングし、検出された脅威を確認します。また、プロキシの使用をサポートしています。
- 信頼できる証明書ストアにアダプタ証明書をインポートします。[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）] の順に選択し、証明書をインポートします。

ステップ 1 [管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サード パーティ ベンダー（Third Party Vendors）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから [CTA：脅威（CTA：Threat）] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ベンダー インスタンスのリスト ページを更新します。ベンダー インスタンスのリスト ページでアダプタのステータスが [設定準備完了（Ready to Configure）] に変更された後でのみ、アダプタを設定できます。

ステップ 7 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 8 次の詳細を入力します。

- [CTA STIX/TAXII サービスの URL（CTA STIX/TAXII service URL）]：CTA クラウド サービスの URL。デフォルトでは URL https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService/ が使用されます。
- [CTA フィード名（CTA feed name）]：CTA クラウド サービスのフィード名を入力します。
- [CTA ユーザ名とパスワード（CTA username and password）]：CTA クラウド サービスのユーザ名とパスワードを入力します。
- [プロキシホストとポート（Proxy host and port）]（オプション）すべてのトラフィックをルーティングするようにプロキシサーバを設定した場合、プロキシサーバのホスト名とポート番号を入力します。
- [ポーリング間隔（Polling interval）]：各ポーリング間の間隔です。デフォルト値は 30 分です。

- [最初のポーリング期間（時間数）（First Poll Duration in hours）]：最初のポーリングで取得されるデータの経過時間。デフォルト値は 2 時間です。最大値は 12 時間です。
- [インシデント タイプ（Incident Type）]：次のオプションを使用できます。
  - [CTA イベントのみ（CTA events only）]
  - [AMP イベントのみ（AMP events only）]
  - [CTA と AMP のイベント（CTA and AMP events）]

ステップ 9 [Next] をクリックします。

ステップ 10 次のオプションを設定するには、[詳細設定（Advanced Settings）] をクリックします。

- [影響の指定（Impact Qualification）]：ポーリングするインシデントの重大度レベルを選択します。次のオプションを使用できます。
  - [1 - 影響なし（1 - Insignificant）]
  - [2 - 妨害（2 - Distracting）]
  - [3 - 困難（3 - Painful）]
  - [4 - 損害発生（4 - Damaging）]
  - [5 - 壊滅的（5 - Catastrophic）]

  [3 - 困難（3 - Painful）] を選択した場合、重大度レベルが [3 - 困難（3 - Painful）] またはそれ以上（この場合 [4 - 損害発生（4 - Damaging）] と [5 - 壊滅的（5 - Catastrophic）]）のインシデントがポーリングされます。
- [ロギング レベル（Logging Level）]：アダプタのログ レベルを選択します。選択可能なオプションは、[エラー（Error）]、[情報（Info）]、[デバッグ（Debug）] です。

ステップ 11 [終了（Finish）] をクリックします。

（注） CTA は Web プロキシ ログに IP アドレスまたはユーザ名としてリストされているユーザ ID を処理します。具体的には、IP アドレスの場合、プロキシ ログで使用可能なデバイスの IP アドレスが、内部ネットワークの別のデバイスの IP アドレスと競合する可能性があります。たとえば AnyConnect 経由で接続するローミング ユーザと、インターネットに直接接続するスプリット トンネルが獲得するローカル IP 範囲アドレス（例：10.0.0.X）が、内部ネットワークで使用されている重複するプライベート IP 範囲のアドレスと競合することがあります。不一致のデバイスに隔離アクションが適用されることを防ぐポリシーを定義するときには、論理ネットワーク アーキテクチャを考慮することが推奨されます。

CTA アダプタの許可プロファイルの設定

脅威イベントごとに、CTA アダプタは Course of Action 属性の値「Internal Blocking」、「Monitoring」、または「Eradication」のいずれかを返します。これらの値に基づいて許可プロファイルを作成できます。

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 許可プロファイルの名前および説明を入力します。

ステップ 4 アクセス タイプを選択します。

ステップ 5 必要な詳細を入力し、[送信（Submit）] をクリックします。

Course of Action 属性を使用した許可ポリシーの設定

脅威イベントが報告されたエンドポイントに対して許可ポリシーを設定するには、CTA-Course_Of_Action 属性を使用できます。この属性は [脅威（Threat）] ディレクトリで使用できます。

また、CTA-Course_Of_Action 属性に基づいて例外ルールを作成することもできます。

ステップ 1 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択します。
脅威イベントが発生したエンドポイントについて、既存のポリシー ルールを編集するか、または新しい例外ルールを作成することができます。

ステップ 2 CTA-Course_Of_Action 属性値を検査するための条件を作成し、適切な許可プロファイルを割り当てます。次に例を示します。

Network_Access_Authentication_Passed AND ThreatCTA-Course_Of_Action CONTAINS Internal Blocking then blocking (authorization profile)

（注） 「Internal Blocking」はエンドポイントの隔離に使用することが推奨される Course of Action 属性です。

ステップ 3 [保存（Save）] をクリックします。

エンドポイントの脅威イベントを受信すると、Cisco ISE は、そのエンドポイントに一致する許可ポリシーがあるかどうかを調べ、エンドポイントがアクティブな場合にのみ CoA をトリガーします。エンドポイントがオフラインの場合、脅威イベントの詳細が脅威イベント レポートに追加されます（[操作（Operations）] > [レポート（Reports）] > [脅威中心型 NAC（Threat Centric NAC] > [脅威イベント（Threat Events）]）。

（注） CTA が 1 つのインシデントで複数のリスクとそれらに関連付けられている Course of Action 属性を送信することがあります。たとえば 1 つのインシデントで「Internal Blocking」と「Monitoring」（Course of Action 属性）を送信することがあります。この場合、「equals」演算子を使用してエンドポイントを隔離する許可ポリシーが設定されていると、エンドポイントは隔離されません。次に例を示します。

```
CTA-Course_Of_Action EQUALS Internal Blocking then Quarantine_Systems (authorization
profile)
```

この場合、エンドポイントを隔離するには許可ポリシーで「contains」演算子を使用する必要があります。次に例を示します。

```
CTA-Course_Of_Action CONTAINS Internal Blocking then Quarantine_Systems
```

Cisco ISE での脆弱性アセスメントのサポート

Cisco Identity Services Engine は次の脆弱性アセスメント（VA）エコシステム パートナーと連携し、Cisco ISE ネットワークに接続するエンドポイントの脆弱性アセスメント結果を取得します。

- Qualys：Qualysは、ネットワークに導入されているスキャナアプライアンスを使用するクラウド ベースの評価システムです。Cisco ISE では、Qualys と通信して VA 結果を取得するアダプタを設定できます。管理者ポータルからアダプタを設定できます。アダプタを設定するには、スーパー管理者権限を持つ Cisco ISE 管理者アカウントが必要です。Qualys アダプタは、Qualys クラウド サービスとの通信に REST API を使用します。REST API にアクセスするには、Qualys でマネージャ権限が付与されたユーザアカウントが必要です。Cisco ISE は次の Qualys REST API を使用します。
  - Host Detection List API：エンドポイントの最新スキャン結果を確認します。
  - Scan API：エンドポイントのオンデマンド スキャンをトリガーします。

  Qualys により、サブスクライブ ユーザが実行できる API コールの数に制限が適用されます。デフォルトのレート制限カウントは、24 時間あたり 300 です。Cisco ISE は Qualys API バージョン 2.0 を使用して Qualys に接続します。これらの API 機能の詳細については、『Qualys API V2 User Guide』を参照してください。
- Rapid7 Nexpose：Cisco ISE は脆弱性管理ソリューションである Rapid 7 Nexpose と連携して、脆弱性の検出を促進します。これにより、このような脅威に迅速に対応できるようになります。Cisco ISE は Nexpose から脆弱性データを受信し、ISE で設定したポリシーに基づいて、影響を受けるエンドポイントを隔離します。Cisco ISE ダッシュボードから、影響を受けるエンドポイントを確認し、適切なアクションを実行できます。

  Cisco ISE は Nexpose リリース 6.4.1 でテスト済みです。
- Tenable Security Center（Nessus スキャナ）：Cisco ISE は Tenable SecurityCenter と連携し、（Tenable SecurityCenter により管理される）Tenable Nessus スキャナから脆弱性データを受信します。また、ISE で設定したポリシーに基づいて、影響を受けるエンドポイントを隔

離します。Cisco ISE ダッシュボードから、影響を受けるエンドポイントを確認し、適切なアクションを実行できます。

Cisco ISE はTenable SecurityCenter 5.3.2 でテスト済みです。

エコシステム パートナーからの結果は Structured Threat Information Expression（STIX）表現に変換され、この値に基づき、必要に応じて認可変更（CoA）がトリガーされ、適切なアクセス レベルがエンドポイントに付与されます。

エンドポイントの脆弱性に関する評価にかかる時間は、さまざまな要因に基づいて異なるため、VA をリアルタイムで実行することはできません。エンドポイントの脆弱性に関する評価にかかる時間に影響する要因を次に示します。

- 脆弱性アセスメント エコシステム
- スキャン対象の脆弱性のタイプ
- 有効なスキャンのタイプ
- エコシステムによりスキャナ アプライアンスに割り当てられるネットワーク リソースとシステム リソース

このリリースの Cisco ISE では、IPv4 アドレスを持つエンドポイントのみが脆弱性を評価できます。

脆弱性アセスメント サービスの有効化と設定

Cisco ISE で脆弱性アセスメント サービスを有効にして設定するには、次の作業を行います。

ステップ 1 脅威中心型 NAC サービスの有効化 （1311 ページ）。

ステップ 2 次の設定を行います。

- Qualys アダプタ（Qualys アダプタの設定 （1318 ページ）を参照）。
- Nexpose アダプタ（Nexpose アダプタの設定 （1321 ページ）を参照）。
- Tenable アダプタ（Tenable アダプタの設定 （1325 ページ）を参照）。

ステップ 3 認可プロファイルの設定 （1328 ページ）。

ステップ 4 脆弱なエンドポイントを隔離する例外ルールの設定 （1329 ページ）。

脅威中心型 NAC サービスの有効化

脆弱性と脅威のアダプタを設定するには、まず脅威中心型 NAC サービスを有効にする必要があります。このサービスは、導入内の 1 つのポリシー サービス ノードでのみ有効にできます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 脅威中心型NACサービスを有効にするPSNの隣にあるチェック ボックスにマークを付けて、[編集（Edit）] をクリックします。

ステップ 3 [脅威中心型 NAC サービスの有効化（Enable Threat Centric NAC Service）] チェック ボックスにマークを付けます。

ステップ 4 [保存（**Save**）] をクリックします。

関連トピック

SourceFire FireAMP アダプタの追加 （1311 ページ）
Cognitive Threat Analytics アダプタの追加 （1313 ページ）
CTA アダプタの許可プロファイルの設定 （1315 ページ）
Course of Action 属性を使用した許可ポリシーの設定 （1315 ページ）
脅威中心型 NAC サービス （1307 ページ）

Qualys アダプタの設定

Cisco ISE は、Qualys 脆弱性アセスメント エコシステムをサポートしています。Cisco ISE 用の Qualys アダプタを作成して、Qualys と通信し、VA 結果を取得する必要があります。

始める前に

- 次のユーザ アカウントを準備する必要があります。
  - ベンダー アダプタを設定できる、スーパー管理者権限を持つ Cisco ISE の管理者ユーザ アカウント。
  - 管理者権限を持つ Qualys のユーザ アカウント
- 適切な Qualys ライセンス サブスクリプションがあることを確認します。Qualys レポート センター、ナレッジベース（KBX）、APIにアクセスする必要があります。詳細については、Qualys アカウント マネージャにお問い合わせください。
- Cisco ISE の信頼できる証明書ストアに Qualys サーバ証明書をインポートします（[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]）。適切なルートと中間証明書が、Cisco ISEの信頼できる証明書ストアにインポートされている（または存在する）ことを確認します。
- Qualys API ガイドの次の設定を参照してください。
  - Qualys で CVSS スコアが有効になっていることを確認します（[レポート（Reports）] > [設定（Setup）] > [CVSS スコア（CVSS Scoring）] > [CVSS スコアの有効化（Enable CVSS Scoring）]）。
  - Qualys にエンドポイントの IP アドレスとサブネット マスクが追加されていることを確認します（[アセット（Assets）] > [ホスト アセット（Host Assets）]）。
  - Qualysオプションプロファイルの名前があることを確認します。オプションプロファイルは、Qualys がスキャンのために使用するスキャナ テンプレートです。認証され

たスキャンを含むオプション プロファイルを使用することを推奨します（このオプションは、エンドポイントの MAC アドレスも確認します）。

• HTTPS/SSL（ポート 443）を介して Qualys と通信する Cisco ISE。

ステップ 1 **[管理（Administration）]>[脅威中心型 NAC（Threat Centric NAC）]>[サードパーティ ベンダー（Third Party Vendors）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから、[Qualys:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば、Qualys_Instance などです。

設定されているアダプタ インスタンスのリストを含むリスト ページが表示されます。

ステップ 5 ベンダー インスタンスのリスト ページを更新します。新しく追加された Qualys_Instance アダプタのステータスが、[設定準備完了（Ready to Configure）] に変化します。

ステップ 6 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 7 Qualys の設定画面で次の値を入力し、[次へ（Next）] をクリックします。

フィールド	説明
REST API ホスト（REST API Host）	Qualys クラウドをホストするサーバのホスト名です。この情報については、Qualys の担当者にお問い合わせください。
REST API ポート（REST API Port）	443
[ユーザ名（Username）]	管理者権限を持つ Qualys のユーザ アカウントです。
[パスワード（Password）]	Qualys ユーザ アカウントのパスワードです。
HTTP プロキシ ホスト（HTTP Proxy Host）	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバがある場合は、プロキシ サーバのホスト名を入力します。
HTTP プロキシ ポート（HTTP Proxy Port）	プロキシ サーバが使用するポート番号を入力します。

Qualys サーバへの接続が確立されると、Qualys スキャナのリストを含む [スキャナ マッピング（Scanner Mappings）] ページが表示されます。ネットワークからの Qualys スキャナがこのページに表示されます。

ステップ 8 Cisco ISE がオンデマンド スキャンに使用するデフォルトのスキャナを選択します。

ステップ 9 [スキャナ マッピングに対する PSN（PSN to Scanner Mapping）] エリアで、PSN ノードに対して 1 つ以上の Qualys スキャナ アプライアンスを選択し、[次へ（Next）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

ステップ 10 [詳細設定（Advanced Settings）] ページに次の値を入力します。このページの設定は、オンデマンド スキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド	説明
オプション プロファイル（Option Profile）	Qualys がエンドポイントのスキャンのために使用するオプション プロファイルを選択します。デフォルト オプション プロファイルである、[初期オプション（Initial Options）] を選択できます。
最後のスキャン結果 - チェック設定	
分単位の最後のスキャン結果のチェック間隔（Last scan results check interval in minutes）	（ホスト検出リスト API のアクセス レートに影響します）経過後に最後のスキャン結果を再度チェックする必要がある、分単位の時間間隔です。有効な範囲は 1 ～ 2880 です。
最後のスキャン結果がチェックされる前の最大結果数（Maximum results before last scan results are checked）	（ホスト検出リスト API のアクセス レートに影響します）キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[分単位の最後のスキャン結果のチェック間隔（Last scan results check interval in minutes）] フィールドで指定された時間間隔の前に最後のスキャン結果がチェックされます。有効な範囲は 1 ～ 1000 です。
MAC アドレスの確認（Verify MAC address）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Qualys からの最後のスキャン結果はエンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
分単位のスキャン トリガー間隔（Scan trigger interval in minutes）	（スキャン API のアクセス レートに影響します）経過後にオンデマンド スキャンがトリガーされる、分単位の時間間隔です。有効な範囲は 1 ～ 2880 です。
スキャンがトリガーされる前の最大要求数（Maximum requests before scan is triggered）	（スキャン API のアクセス レートに影響します）キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[分単位のスキャン トリガー間隔（Scan trigger interval in minutes）] フィールドで指定された時間間隔の前にオンデマンド スキャンがトリガーされます。有効な範囲は 1 ～ 1000 です。

フィールド	説明
分単位のスキャンステータスのチェック間隔（Scan status check interval in minutes）	経過後に Cisco ISE が Qualys と通信してスキャンのステータスをチェックする、分単位の時間間隔です。有効な範囲は 1 ～ 60 です。
同時にトリガーできるスキャン数（Number of scans that can be triggered concurrently）	（このオプションは、[スキャナ マッピング（Scanner Mappings）] 画面で各 PSN にマッピングされているスキャナの数に依存しています）各スキャナは同時に 1 つの要求のみを処理できます。PSN に複数のスキャナをマッピングしている場合は、選択したスキャナの数に基づいてこの値を増やすことができます。有効な範囲は 1 ～ 200 です。
分単位のスキャンタイムアウト（Scan timeout in minutes）	経過後にスキャン要求がタイムアウトする、分単位の時間です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は 20 ～ 1440 です。
スキャナごとの送信される IP アドレスの最大数（Maximum number of IP addresses to be submitted per scanner）	処理のために Qualys に送信される単一の要求にキュー登録できる要求の数を示します。有効な範囲は 1 ～ 1000 です。
アダプタ ログ ファイル用のログ レベルの選択（Choose the log level for adapter log files）	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー（ERROR）]、[情報（INFO）]、[デバッグ（DEBUG）]、[トレース（TRACE）] です。

ステップ 11 [次へ（Next）] をクリックして、構成設定を確認します。

ステップ 12 [終了（Finish）] をクリックします。

Nexpose アダプタの設定

Cisco ISE 用の Nexpose アダプタを作成して、Nexpose と通信し、VA 結果を取得する必要があります。

始める前に

- Cisco ISE で脅威中心型 NAC サービスを有効にしていることを確認します。
- Nexpose Security Console にログインし、ユーザ アカウントを作成して次の権限をこのアカウントに付与します。
  - サイトの管理
  - レポートの作成
- Cisco ISE の信頼できる証明書ストアに Nexpose サーバ証明書をインポートします（[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]）。適切なルートと中間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている（または存在する）ことを確認します。
- HTTPS/SSL（ポート 3780）を介して Nexpose と通信する Cisco ISE。

ステップ 1 **[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サード パーティ ベンダー（Third Party Vendors）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウンリストから [Rapid7 Nexpose:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば Nexpose と入力します。

設定されているアダプタ インスタンスのリストを含むリスト ページが表示されます。

ステップ 5 ベンダー インスタンスのリスト ページを更新します。新しく追加された Nexpose アダプタのステータスが、[設定準備完了（Ready to Configure）] に変化します。

ステップ 6 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 7 Nexpose の設定画面で次の値を入力し、[次へ（Next）] をクリックします。

フィールド	説明
[Nexpose ホスト（Nexpose Host）]	Nexpose サーバのホスト名。
[Nexpose ポート（Nexpose Port）]	3780。
[ユーザ名（Username）]	Nexpose 管理者ユーザ アカウント。
[パスワード（Password）]	Nexpose 管理者ユーザ アカウントのパスワード。

フィールド	説明
HTTP プロキシ ホスト（HTTP Proxy Host）	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバがある場合は、プロキシ サーバのホスト名を入力します。
HTTP プロキシ ポート（HTTP Proxy Port）	プロキシ サーバが使用するポート番号を入力します。

ステップ 8 [次へ（Next）] をクリックして拡張設定を設定します。

ステップ 9 [詳細設定（Advanced Settings）] ページに次の値を入力します。このページの設定は、オンデマンド スキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド	説明
最新スキャン結果のチェックの設定	
[最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）]	最新スキャン結果を再度確認するまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。
[最新スキャン結果を確認するトリガーとなる保留要求数（Number of pending requests that can trigger checking the latest scan results）]	[最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）] フィールドに指定した期間が経過していない場合でも、キューに登録されたスキャン要求の数がここで指定する最大数を超えると、最新スキャン結果が確認されます。有効な範囲は 1 ～ 1000 です。
MAC アドレスの確認（Verify MAC address）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Nexpose からの最後のスキャン結果はエンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
[各サイトのスキャン トリガー間隔（分単位）（Scan trigger interval for each site in minutes）]	スキャンがトリガーされるまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。

フィールド	説明
最新スキャン結果のチェックの設定	
[各サイトのスキャンのトリガーとなる保留要求の数（Number of pending requests before a scan is triggered for each site）]	キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[スキャン トリガー間隔（分単位）（Scan trigger interval in minutes）] フィールドで指定された時間間隔が経過する前にスキャンがトリガーされます。有効な範囲は1～1000です。
分単位のスキャンタイムアウト（Scan timeout in minutes）	経過後にスキャン要求がタイムアウトする、分単位の時間です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は 20 ～ 1440 です。
[スキャンを同時にトリガーできるサイトの数（Number of sites for which scans could be triggered concurrently）]	スキャンを同時に実行できるサイトの数。有効な範囲は 1 ～ 200 です。
タイムゾーン（Timezone）	Nexpose サーバで設定されているタイム ゾーンに基づいてタイム ゾーンを選択します。
[HTTP タイムアウト（秒単位）（Http timeout in seconds）]	Cisco ISE が Nexpose からの応答を待機する時間間隔。有効な範囲は 5 ～ 1200 です。
アダプタ ログ ファイル用のログ レベルの選択（Choose the log level for adapter log files）	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー（ERROR）]、[情報（INFO）]、[デバッグ（DEBUG）]、[トレース（TRACE）] です。

ステップ 10 [次へ（Next）] をクリックして、構成設定を確認します。

ステップ 11 [終了（Finish）] をクリックします。

Tenable アダプタの設定

Cisco ISE が Tenable SecurityCenter（Nessus スキャナ）と通信し、VA 結果を取得するためには、Tenable アダプタを作成する必要があります。

始める前に

（注） Cisco ISE で Tenable Adapter を設定する前に、Tenable SecurityCenter で次の項目を設定する必要があります。これらの設定については、Tenable SecurityCenter のマニュアルを参照してください。

- Tenable Security Center と Tenable Nessus Vulnerability Scanner がインストールされている必要があります。Tenable Nessus スキャナの登録時に、[登録（Registration）] フィールドで [SecurityCenter で管理（Managed by SecurityCenter）] を必ず選択します。
- Tenable SecurityCenter で Security Manager 権限を持つユーザ アカウントを作成します。
- SecurityCenter でリポジトリを作成します（管理者クレデンシャルを使用して Tenable SecurityCenterにログインし、[リポジトリ（Repository）]>[追加（Add）] を選択します）。
- リポジトリにスキャン対象のエンドポイント IP 範囲を追加します。
- Nessus スキャナを追加します。
- スキャン ゾーンを作成し、作成したスキャン ゾーンと、これらのスキャン ゾーンにマッピングされているスキャナに、IP アドレスを割り当てます。
- ISE のスキャン ポリシーを作成します。
- アクティブなスキャンを追加し、ISE スキャン ポリシーに関連付けます。設定項目、ターゲット（IP/DNS 名）を設定します。
- システム証明書とルート証明書を Tenable SecurityCenter からエクスポートし、Cisco ISE の信頼できる証明書ストアにインポートします（[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]）。適切なルートと中間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている（または存在する）ことを確認します。
- HTTPS/SSL（ポート 443）を介して Tenable SecurityCenter と通信する Cisco ISE。

ステップ 1 **[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティ ベンダー（Third Party Vendors）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから、[Tenable Security Center:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば、Tenable。

設定されているアダプタ インスタンスのリストを含むリスト ページが表示されます。

ステップ 5 ベンダー インスタンスのリスト ページを更新します。新しく追加された Tenable アダプタのステータスが、[設定準備完了（Ready to Configure）] に変化します。

ステップ 6 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 7 Tenable SecurityCenter の設定画面で次の値を入力し、[次へ（Next）] をクリックします。

フィールド	説明
[Tenable SecurityCenter ホスト（Tenable SecurityCenter Host）]	Tenable SecurityCenter のホスト名。
[Tenable SecurityCenter ポート（Tenable SecurityCenter Port）]	443
[ユーザ名（Username）]	Tenable SecurityCenter でセキュリティ マネージャ権限を持つユーザ アカウントのユーザ名。
[パスワード（Password）]	Tenable SecurityCenter でセキュリティ マネージャ権限を持つユーザ アカウントのパスワード。
HTTP プロキシ ホスト（HTTP Proxy Host）	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバがある場合は、プロキシ サーバのホスト名を入力します。
HTTP プロキシ ポート（HTTP Proxy Port）	プロキシ サーバが使用するポート番号を入力します。

ステップ 8 [Next] をクリックします。

ステップ 9 [詳細設定（Advanced Settings）] ページに次の値を入力します。このページの設定は、オンデマンド スキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド	説明
リポジトリ（Repository）	Tenable SecurityCenter で作成したリポジトリを選択します。
[スキャン ポリシー（Scan Policy）]	Tenable SecurityCenter で、ISE 用に作成したスキャン ポリシーを選択します。
最新スキャン結果のチェックの設定	

フィールド	説明
[最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）]	最新スキャン結果を再度確認するまでの時間間隔（分単位）。有効な範囲は1～2880です。
[最新スキャン結果を確認するトリガーとなる保留要求数（Number of pending requests that can trigger checking the latest scan results）]	[最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）] フィールドに指定した期間が経過していない場合でも、キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、最新スキャン結果が確認されます。有効な範囲は 1 ～ 1000 です。デフォルトは 10 です。
MAC アドレスの確認（Verify MAC address）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Tenable SecurityCenter からの最新スキャン結果は、エンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
[各サイトのスキャン トリガー間隔（分単位）（Scan trigger interval for each site in minutes）]	オンデマンド スキャンがトリガーされるまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。
[スキャンのトリガーとなる保留要求の数（Number of pending requests before a scan is triggered）]	キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[スキャン トリガー間隔（分単位）（Scan trigger interval in minutes）] フィールドで指定された時間間隔が経過する前にオンデマンド スキャンがトリガーされます。有効な範囲は 1 ～ 1000 です。
分単位のスキャン タイムアウト（Scan timeout in minutes）	経過後にスキャン要求がタイムアウトする期間（分単位）です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は 20 ～ 1440 です。

フィールド	説明
[並列実行可能なスキャンの数（Number of scans that could run in parallel）]	同時に実行できるスキャンの数。有効な範囲は 1 ～ 200 です。
[HTTP タイムアウト（秒単位）（Http timeout in seconds）]	Cisco ISE が Tenable SecurityCenter からの応答を待機する時間間隔。有効な範囲は 5 ～ 1200 です。
アダプタ ログ ファイル用のログ レベルの選択（Choose the log level for adapter log files）	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー（ERROR）]、[情報（INFO）]、[デバッグ（DEBUG）]、[トレース（TRACE）] です。

ステップ 10 [次へ（Next）] をクリックして、構成設定を確認します。

ステップ 11 [終了（Finish）] をクリックします。

認可プロファイルの設定

Cisco ISE の許可プロファイルに、脆弱性がないかエンドポイントをスキャンするオプションが含まれるようになりました。スキャンの定期的な実行を選択できます。また、これらのスキャンの時間間隔を指定することもできます。許可プロファイルを定義した後、既存の認可ポリシー ルールに適用するか、または新しい認可ポリシー ルールを作成できます。

始める前に

脅威中心型 NAC サービスを有効にし、ベンダー アダプタを設定する必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [認証（Authorization）] > [許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 新規の許可プロファイルを作成するか、既存のプロファイルを編集します。

ステップ 3 [共通タスク（Common Tasks）] 領域で、[脆弱性を評価する（Assess Vulnerabilities）] チェックボックスをオンにします。

ステップ 4 [アダプタ インスタンス（Adapter Instance）] ドロップダウン リストから、設定したベンダー アダプタを選択します。たとえば、Qualys_Instance などです。

ステップ 5 最後のスキャンからの時間がテキスト ボックスよりも大きい場合は、トリガー スキャンのスキャン間隔を時間単位で入力します。有効な範囲は 1 ～ 9999 です。

ステップ 6 [上の間隔を使用して定期的に評価する（Assess periodically using above interval）] チェックボックスをオンにします。

ステップ 7 [送信（Submit）] をクリックします。

脆弱なエンドポイントを隔離する例外ルールの設定

例外ルールを設定し、脆弱なエンドポイントへのアクセスを制限するには、次の脆弱性アセスメント属性を使用できます。

- Threat:Qualys-CVSS_Base_Score
- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

これらの属性は [脅威（Threat）] ディレクトリで使用できます。有効な値の範囲は 0 ～ 10 です。

エンドポイントの隔離、アクセスの制限（別のポータルへのリダイレクト）、または要求の拒否のいずれかを選択できます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー セット（Policy Sets）]** を選択します。
既存のポリシー ルールを編集するか、または VA 属性のチェックについて新しい例外ルールを作成します。

ステップ 2 Qualys スコアを確認して適切な許可プロファイルを割り当てるための条件を作成します。次に例を示します。

Any Identity Group & Threat:Qualys-CVSS_Base_Score > 5 -> Quarantine (authorization profile)

ステップ 3 [保存（**Save**）] をクリックします。

脆弱性アセスメント ログ

Cisco ISE には、VA サービスのトラブルシューティングのための次のログがあります。

- vaservice.log：VA コア情報が含まれており、TC-NAC サービスを実行しているノードで使用可能です。
- varuntime.log：エンドポイントと VA フローに関する情報が含まれており、モニタリング ノードと、TC-NAC サービスを実行しているノードで使用可能です。
- vaaggregation.log：1 時間ごとに収集されるエンドポイントの脆弱性に関する情報が含まれており、プライマリ管理ノードで使用可能です。

展開とノードの設定

[展開ノード（Deployment Nodes）] ページを使用すると、Cisco ISE（管理、ポリシー サービス、およびモニタリング）ノードを設定し、展開を設定することができます。

展開ノードリストウィンドウ

次の表に、展開内の Cisco ISE ノードを設定するために使用できる [展開のノードリスト（Deployment Nodes List）] ページのフィールドを示します。このページへのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** です。

フィールド名	使用上のガイドライン
ホスト名（**Hostname**）	ノードのホスト名を表示します。
ノード タイプ（**Node Type**）	ノード タイプを表示します。次のいずれかを設定できます。 • Cisco ISE（管理、ポリシー サービス、およびモニタリング）ノード
ペルソナ（**Personas**）	（ノード タイプが Cisco ISE の場合にのみ表示）Cisco ISE ノードが担当してきたペルソナがリストされます。[管理（Administration）]、[ポリシー サービス（Policy Service）] などがあります。
ロール（**Role**）	このノードで管理ペルソナまたはモニタリング ペルソナが有効になっている場合、これらのペルソナが担当しているロール（プライマリ、セカンダリ、またはスタンドアロン）が示されます。ロールは、次のうちの 1 つまたは複数にできます。 • [PRI（A）] : プライマリ PAN を意味します • [SEC（A）] : セカンダリ PAN を意味します • [PRI（M）] : プライマリ モニタリング ノードを意味します • [SEC（M）] : セカンダリ モニタリング ノードを意味します

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

関連トピック

Cisco ISE 分散展開 （32 ページ）
Cisco ISE 展開の用語 （27 ページ）
Cisco ISE ノードの設定 （28 ページ）
セカンダリ Cisco ISE ノードの登録

ノードの一般設定

次の表で、Cisco ISE ノードの [全般設定 (General Settings)] ウィンドウのフィールドについて説明します。このウィンドウでは、ペルソナをノードに割り当て、そのサービスを実行するように設定できます。このタブのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** > **[展開ノード（Deployment Node）]** > **[編集（Edit）]** > **[全般設定（General Settings）]** です。

表 *169* : ノードの一般設定

フィールド名	使用上のガイドライン
ホスト名（**Hostname**）	Cisco ISE ノードのホスト名を表示します。
FQDN	Cisco ISE ノードの完全修飾ドメイン名を表示します。たとえば、ise1.cisco.com などです。
IP アドレス	Cisco ISE ノードの IP アドレスを表示します。
ノード タイプ（**Node Type**）	ノード タイプを表示します。
ペルソナ（**Personas**）	

フィールド名	使用上のガイドライン
管理（**Administration**）	Cisco ISE ノードに管理ペルソナを担当させる場合は、このチェックボックスをオンにします。管理ペルソナは、管理サービスを提供するようライセンスされているノードでのみ有効にできます。 ロール（Role）：管理ペルソナが展開で担当しているロールを表示します。[スタンドアロン（Standalone）]、[プライマリ（Primary）]、[セカンダリ（Secondary）] のいずれかの値になります。 プライマリにする（Make Primary）：ノードをプライマリ Cisco ISE ノードにする場合にこのボタンをクリックします。展開では 1 つのプライマリ Cisco ISE ノードのみを使用できます。このページのその他のオプションは、ノードをプライマリにした後にのみアクティブになります。展開では 2 つの管理ノードのみを使用できます。ノードにスタンドアロン ロールが割り当てられている場合、[プライマリにする（Make Primary）] ボタンがノードの横に表示されます。ノードにセカンダリ ロールが割り当てられている場合、[プライマリに昇格（Promote to Primary）] ボタンがノードの横に表示されます。ノードにプライマリ ロールがあり、そのノードを使用して登録されている他のノードがない場合は、ノードの横に[スタンドアロンにする（Make Standalone）] ボタンが表示されます。このボタンをクリックすると、プライマリ ノードをスタンドアロン ノードにすることができます。

フィールド名	使用上のガイドライン
モニタリング	

フィールド名	使用上のガイドライン
	Cisco ISE ノードにモニタリング ペルソナを担当させ、ログ コレクタとして機能させる場合は、このチェックボックスをオンにします。分散展開内にモニタリング ノードが少なくとも 1 つ存在する必要があります。プライマリ PAN の設定時に、モニタリング ペルソナを有効にする必要があります。展開内のセカンダリ モニタリング ノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリング ペルソナを無効にしたりできます。 VMware プラットフォームで Cisco ISE ノードをログ コレクタとして設定するには、次のガイドラインに従って最低限必要なディスク領域を決定します。1 日あたりネットワーク内のエンドポイント 1 つにつき 180 KB、1 日あたりネットワーク内の Cisco ISE ノード 1 つにつき 2.5 MB となります。 モニタリング ノードに何ヵ月分のデータを格納するかに応じて、必要な最大ディスク領域を計算します。展開にモニタリング ノードが 1 つしかない場合は、スタンドアロン ロールを担当します。展開に2つのモニタリング ノードがある場合は、Cisco ISE に、プライマリ-セカンダリ ロールを設定する他のモニタリング ノードの名前が表示されます。これらのロールを設定するには、次のいずれかを選択します。 • プライマリ（Primary）：現在のノードをプライマリ モニタリング ノードにする場合。 • セカンダリ（Secondary）：現在のノードをセカンダリ モニタリング ノードにする場合。 • なし（None）：モニタリングノードにプライマリ/セカンダリ ロールを担当させない場合。 モニタリング ノードの 1 つをプライマリまたはセカンダリとして設定すると、もう一方のモニタリング ノードが自動的にそれぞれセカンダリ ノードまたはプライマリ ノードになります。プライマリ モニタリング ノードおよび

フィールド名	使用上のガイドライン
	セカンダリ モニタリング ノードは、管理ログおよびポリシー サービス ログを受信します。1 つのモニタリングノードのロールを [なし（None）]に変更した場合、他方のモニタリングノードのロールも同様に [なし（None）] になり、それによって高可用性ペアがキャンセルされます。モニタリングノードとしてノードを指定すると、そのノードが **[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[リモートロギングターゲット（Remote Logging Targets）]** ウィンドウで syslog ターゲットとして表示されます。

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

フィールド名	使用上のガイドライン
	次のサービスの 1 つまたはすべてを有効にするには、このチェックボックスをオンにします。 • [セッションサービスの有効化（Enable Session Services）] : ネットワーク アクセス サービス、ポスチャサービス、ゲスト サービス、およびクライアント プロビジョニング サービスを有効にするには、このチェックボックスをオンにします。このポリシー サービス ノードが属するグループを、[ノードをノード グループに含める（Include Node in Node Group）] ドロップダウン リストから選択します。CA サービスと EST サービスは、セッション サービスが有効になっているポリシーサービスノードでのみ実行できることに注意してください。 [ノードをノードグループに含める（Include Node in Node Group）] については、このポリシーサービスモードをどのグループにも含めない場合は [なし（None）] を選択します。 同じノード グループ内のすべてのノードが、ネットワーク アクセス デバイス（NAD）で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノード グループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロード バランサを使用していない場合、ノード グループ内のノードは、NAD で設定されている RADIUS サーバおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバとしても設定できます。 多数の ISE ノード（RADIUS サーバおよび動的許可クライアントとして）を持つ単一の NAD を設定できますが、すべてのノードが同じノード グループに属している必要はありません。

フィールド名	使用上のガイドライン
	ノード グループのメンバーは、ギガビット イーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノード グループのメンバーは L2 隣接関係である必要はありませんが、十分な帯域幅と到達可能性を確保するには L2 隣接関係が強く推奨されます。詳細については、『』の「ポリシー サービス ノード グループの作成」のセクションポリシー サービス ノード グループの作成（87 ページ）を参照してください。 • プロファイリング サービスの有効化（Enable Profiling Service）：プロファイラ サービスを有効にするには、このチェックボックスをオンにします。プロファイリング サービスを有効にする場合は、[Profiling Configuration（プロファイリング設定）] タブをクリックし、必要に応じて詳細を入力する必要があります。ポリシー サービス ノードで実行されるサービスを有効または無効にしたり、このノードを変更したりする場合は、そのサービスが実行されるアプリケーション サーバ プロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。ノードでアプリケーション サーバがいつ再起動したかを確認するには、CLI で show application status ise コマンドを使用します。 • 脅威中心型NACサービスの有効化（Enable Threat Centric NAC Service）：脅威中心型ネットワーク アクセス コントロール（TC-NAC）機能を有効にするには、このチェックボックスをオンにします。この機能では、脅威と脆弱性のアダプタから受信した脅威と脆弱性の属性に基づいて認証ポリシーを作成することができます。脅威の重大度レベルと脆弱性評価の結果は、エンドポイントまたはユーザのアクセス レベルを動的に制御するために使用できます。

フィールド名	使用上のガイドライン
	• SXPサービスの有効化（Enable SXP Service）：ノードで SXP サービスを有効にするには、このチェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。 NIC ボンディングまたはチーミングを設定している場合は、ボンディングされたインターフェイスも物理インターフェイスとともに [使用インターフェイス（Use Interface）] ドロップダウン リストに表示されます。 • デバイス管理サービスの有効化（Enable Device Admin Service）：TACACS ポリシーセット、ポリシー結果などを作成し、ネットワークデバイスの設定を制御および監査するには、このチェックボックスをオンにします。 • パッシブIDサービスの有効化（Enable Passive Identity Service）：ID マッピング機能を有効にするには、このチェックボックスをオンにします。この機能を使用すると、Cisco ISE ではなくドメイン コントローラ（DC）で認証されるユーザをモニタすることができます。Cisco ISE がユーザのネットワーク アクセスをアクティブには認証しないネットワークでは、ID マッピング機能を使用して、Active Directory（AD）ドメイン コントローラからユーザ認証情報を収集することができます。

フィールド名	使用上のガイドライン
pxGrid	pxGridペルソナを有効にするには、このチェック ボックスをオンにします。Cisco pxGridは、Cisco ISE セッション ディレクトリからCisco Adaptive Security Appliance（ASA）などの他のポリシー ネットワーク システムへコンテキスト依存情報を共有するために使用されます。pxGrid フレームワークは、ポリシー データや設定データをノード間で交換するためにも使用できます（たとえば、ISEとサードパーティ ベンダー間でのタグやポリシー オブジェクトの共有）。また、脅威情報など、非 ISE 関連情報の交換用にも使用できます。

関連トピック

分散 Cisco ISE 展開のペルソナ （28 ページ）
管理ノード （59 ページ）
ポリシー サービス ノード （69 ページ）
モニタリング ノード （70 ページ）
pxGrid ノード （77 ページ）
プライマリおよびセカンダリの Cisco ISE ノードの同期 （86 ページ）
ポリシー サービス ノード グループの作成 （87 ページ）
ISE pxGrid ノードの展開 （80 ページ）
ノード ペルソナとサービスの変更 （86 ページ）
自動フェールオーバー用のモニタリング ノードの設定 （76 ページ）

プロファイリング ノードの設定

次の表では、プロファイラ サービスのプローブの設定に使用できる [プロファイリング設定（Profiling Configuration）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [ISE ノード（ISE Node）] > [編集（Edit）] > [プロファイリング設定（Profiling Configuration）]** です。

表 *170 :* プロファイリング ノードの設定

フィールド名	使用上のガイドライン
NetFlow	ルータから送信された NetFlow パケットを受信および解析するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに NetFlow を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。 • [インターフェイス（Interface）] : ISE ノード上のインターフェイスを選択します。 • [ポート（Port）] : NetFlow エクスポートがルータから受信した NetFlow リスナー ポート番号を入力します。デフォルト ポートは 9996 です。
DHCP	IP ヘルパーから DHCP パケットをリッスンするために、ポリシーサービスペルソナを担当した Cisco ISE ノードごとに DHCP を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。 • [ポート（Port）] : DHCP サーバの UDP ポート番号を入力します。デフォルト ポートは 67 です。 • [インターフェイス（Interface）] : ISE ノード上のインターフェイスを選択します。 • [ポート（Port）] : DHCP サーバの UDP ポート番号を入力します。デフォルト ポートは 67 です。
DHCP SPAN	DHCP パケットを収集するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに DHCP SPAN を有効にする場合は、このチェックボックスをオンにします。 • [インターフェイス（Interface）] : ISE ノード上のインターフェイスを選択します。

フィールド名	使用上のガイドライン
HTTP	HTTPパケットを受信および解析するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとにHTTP を有効にする場合は、このチェックボックスをオンにします。 • [インターフェイス（Interface）] : ISE ノード上のインターフェイスを選択します。
『**RADIUS**』	IOS センサー対応デバイスから RADIUS セッション属性、さらに CDP 属性と LLDP 属性を収集するために、ポリシー サービス ペルソナを担当した ISE ノードごとに RADIUS を有効にする場合は、このチェックボックスをオンにします。
ネットワーク スキャン（**NMAP**）（**Network Scan (NMAP)**）	NMAP プローブをイネーブルにするには、このボックスをオンにします。
DNS	FQDN の DNS ルックアップを実行するために、ポリシー サービス ペルソナを担当した ISE ノードごとに DNS を有効にする場合は、このチェックボックスをオンにします。秒単位でタイムアウト時間を入力します。 （注） DNSプローブを分散展開内の特定のCisco ISE ノードで動作させるには、DHCP、DHCP SPAN、HTTP、RADIUS、SNMPのいずれかのプローブを有効にする必要があります。DNSルックアップの場合、上記のいずれかのプローブを DNS プローブとともに起動する必要があります。

フィールド名	使用上のガイドライン
SNMP クエリ（SNMP Query）	指定した間隔でネットワーク デバイスをポーリングするために、ポリシー サービス ペルソナを担当したISEノードごとにSNMPクエリーを有効にする場合は、このチェックボックスをオンにします。[再試行（Retries）]、[タイムアウト（Timeout）]、[イベント タイムアウト（Event Timeout）]、任意の [説明（Description）] の各フィールドに値を入力します。 （注） SNMPクエリープローブの設定に加えて、[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] の場所にある他のSNMP設定も行う必要があります。ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスでシスコ デバイス プロトコル（CDP）およびLink Layer Discovery Protocol（LLDP）をグローバルに有効にしていることを確認します。

フィールド名	使用上のガイドライン
SNMP トラップ（SNMP Trap）	ネットワーク デバイスから linkUp、linkDown、MAC 通知トラップを受信するために、ポリシー サービス ペルソナを担当した ISE ノードごとに SNMP トラップ プローブを有効にする場合は、このチェックボックスをオンにします。次のいずれかを選択します。 • [リンクトラップクエリ（Link Trap Query）]：SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、このチェックボックスをオンにします。 • [MAC トラップクエリ（MAC Trap Query）]：SNMP トラップを介して受信する MAC 通知を受信して解釈するには、このチェックボックスをオンにします。 • [インターフェイス（Interface）]：ISE ノードのインターフェイスを選択します。 • [ポート（Port）]：使用するホストの UDP ポートを入力します。デフォルト ポートは 162 です。
Active Directory	定義された Active Directory サーバをスキャンして、Windows ユーザに関する情報を探します。
pxGrid	ISE で pxGrid を介してエンドポイント属性を収集（プロファイリング）できるようになります。

関連トピック

Cisco ISE プロファイリング サービス （748 ページ）
プロファイリング サービスによって使用されるネットワーク プローブ （751 ページ）
Cisco ISE ノードでのプロファイリング サービスの設定 （750 ページ）

証明書ストアの設定

[証明書ストア（Certificate Store）] ページでは、認証に使用できる証明書を Cisco ISE で設定することができます。

自己署名証明書の設定

次の表では、[自己署名証明書の生成（Generate Self Signed Certificate）] ページのフィールドについて説明します。このページでは、ノード間通信、EAP-TLS 認証、Cisco ISE Web ポータル、および pxGrid コントローラとの通信用のシステム証明書を作成できます。このページのナビゲーションパスは、**[管理（Administration）]>[システム（System）]>[証明書（Certificates）]>[システム証明書（System Certificates）] > [自己署名証明書の生成（Generate Self Signed Certificate）]** です。

表 *171 :* 自己署名証明書の設定

フィールド名	使用上のガイドライン
ノードの選択（Select Node）	（必須）システム証明書を生成するノード。
Common Name（CN）	（SAN を指定しない場合に必須）デフォルトでは、一般名は自己署名証明書を生成する ISE ノードの完全修飾ドメイン名です。
Organizational Unit（OU）	組織ユニット名。Engineering など。
組織（Organization）（O）	組織名。Cisco など。
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。
Country（C）	国名。2 文字の ISO 国番号を入力する必要があります。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	証明書に関連付けられた IP アドレス、DNS 名、または Uniform Resource Identifier（URI）。
キー タイプ	RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。

フィールド名	使用上のガイドライン
キーの長さ（**Key Length**）	公開キーのビット サイズを指定します。RSA には、次のオプションを使用できます。 • 512 • 1024 • 2048 • 4096 ECDSA には、次のオプションを使用できます。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。 パブリック CA 署名付き証明書を取得する場合、または FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は、2048 を選択します。
署名するダイジェスト（**Digest to Sign With**）	ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。
証明書ポリシー（**Certificate Policies**）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。
TTL 有効期限（**Expiration TTL**）	証明書が失効するまでの日数を指定します。
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ワイルドカード証明書の許可（**Allow Wildcard Certificates**）	自己署名したワイルドカード証明書（サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク（*）が含まれている証明書）を生成する場合は、このチェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。

フィールド名	使用上のガイドライン
Usage	このシステム証明書を使用する必要があるサービスを選択します。 • [管理者（Admin）]：管理者ポータルとの通信および展開内の ISE ノード間の通信の保護に使用されるサーバ証明書 • [EAP 認証（EAP Authentication）]：SSL/TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバ証明書 • [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバ証明書 • [pxGrid]：pxGrid クライアントとサーバの間の通信を保護するクライアントおよびサーバ証明書 • [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバ証明書

関連トピック

システム証明書 （157 ページ）
システム証明書の表示 （158 ページ）
自己署名証明書の生成 （162 ページ）

証明書署名要求の設定

Cisco ISE では、1 つの要求で、管理者ポータルから展開内のすべてのノードの CSR を生成することができます。また、展開内の単一ノードまたは複数両方のノードのどちらの CSR を生成するのか選択することもできます。単一ノードの CSR を生成する場合、ISE は証明書サブジェクトの [CN=] フィールドの特定ノードの完全修飾ドメイン名（FQDN）を自動的に置き換えます。証明書の [サブジェクト代替名（Subject Alternative Name (SAN)）] フィールドにエントリを含めることを選択した場合、他の SAN 属性に加えて ISE ノードの FQDN を入力する必要があります。展開内のすべてのノードの CSR を生成することを選択した場合は、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] チェックボックスをオンにして、[SAN] フィールド（DNS 名）にワイルドカード表記で FQDN を入力します（*.amer.example.com など）。EAP 認証に証明書を使用する場合は、[CN=] フィールドにワイルドカード値を入力しないでください。

ワイルドカード証明書を使用することにより、各 Cisco ISE ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用すると、展開内の複数の両方のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバ証明書を割り当てる場合よりも安全性が低いと見なされます。

次の表に、認証局（CA）が署名可能な証明書署名要求（CSR）の生成に使用できる [証明書署名要求（Certificate Signing Request）] ページのフィールドを示します。このページのナビゲーション パスは **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書管理（Certificate Management）]** > **[証明書署名要求（Certificate Signing Request）]** です。

表 *172 :* 証明書署名要求の設定

フィールド	使用上のガイドライン
証明書の用途（**Certificate(s) will be used for**）	

フィールド	使用上のガイドライン
	証明書を使用するサービスを選択します。 **Cisco ISE ID 証明書** • [複数使用（Multi-Use）]：複数のサービス（管理者、EAP-TLS 認証、pxGrid、およびポータル）に使用されます。複数使用の証明書は、クライアントとサーバ両方のキーの用途を使用します。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [管理者（Admin）]：サーバ認証に使用されます（管理者ポータルとの通信および展開内の ISE ノード間の通信を保護するため）。署名 CA の証明書テンプレートは、Web サーバ証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） • [EAP 認証（EAP Authentication）]：サーバ認証に使用されます。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） （注） EAP-TLS クライアント証明書にデジタル署名キー使用法を使用する必要があります。 • [RADIUS DTLS]：RADIUS DTLS サーバの認証に使用されます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） • [ポータル（Portal）]：サーバ認証に使用されます（すべての ISE Web

フィールド	使用上のガイドライン
	ポータルとの通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） • [pxGrid]：クライアント認証とサーバ認証の両方に使用されます（pxGrid クライアントとサーバ間の通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） （注） 拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用しないことをお勧めします。拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用する場合、証明書は無効と見なされ、次のエラー メッセージが表示されます。 `source=local ; type=fatal ; message="unsupported certificate"` **Cisco ISE 認証局証明書**

フィールド	使用上のガイドライン
	• [ISE ルート CA（ISE Root CA）]：（内部 CA サービスにのみ適用可能）プライマリ PAN のルート CA および PSN の下位 CA を含む内部 CA 証明書チェーン全体を再生成するために使用されます。 • [ISE 中間 CA（ISE Intermediate）]：（ISE が外部 PKI の中間 CA として機能する場合に内部 CA サービスにのみ適用可能）プライマリ PAN の中間 CA 証明書および PSN の下位 CA 証明書の生成に使用されます。署名 CA の証明書テンプレートは、下位認証局と呼ばれます。このテンプレートには、次のプロパティがあります。 • [基本制約（Basic Constraints）]：重要、認証局 • [キーの用途（Key Usage）]：証明書の署名、デジタル署名 • [キーの拡張用途（Extended Key Usage）]：OCSP 署名（1.3.6.1.5.5.7.3.9） • [ISE OCSP 応答側証明書の更新（Renew ISE OCSP Responder Certificates）]：（内部 CA サービスにのみ適用可能）展開全体の ISE OCSP 応答側証明書の更新に使用されます（証明書署名要求ではありません）。セキュリティ上の理由から、ISE OCSP 応答側証明書を 6 ヵ月ごとに更新することを推奨します。
ワイルドカード証明書の許可（Allow Wildcard Certificates）	証明書の [SAN] フィールドの CN/DNS 名にワイルドカード文字（*）を使用するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、展開内のすべてのノードが自動的に選択されます。左端のラベルの位置にアスタリスク（*）ワイルドカード文字を使用する必要があります。ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、セキュリティ問題が発生する可能性があります。
これらのノードの CSR の生成（Generate CSRs for these Nodes）	証明書を生成するノードの隣のチェックボックスをオンにします。展開内の選択されたノードの CSR を生成するには、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオフにします。
Common Name（CN）	デフォルトでは、一般名は CSR を生成する ISE ノードの FQDN です。$FQDN$ は ISE ノードの FQDN を意味します。展開内の複数ノードの CSR を生成すると、CSR の [一般名（Common Name）] フィールドは各 ISE ノードの FQDN に置き換えられます。
Organizational Unit（OU）	組織ユニット名。Engineering など。
Organization（O）	組織名。Cisco など。

フィールド	使用上のガイドライン
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。
Country（C）	国名。2 文字の ISO 国番号を入力する必要があります。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	証明書に関連付けられている IP アドレス、DNS 名、Uniform Resource Identifier（URI）、またはディレクトリ名。 • [DNS 名（DNS Name）]：DNS 名を選択した場合は、ISE ノードの完全修飾ドメイン名を入力します。[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオンにした場合は、ワイルドカード表記（ドメイン名の前にアスタリスクとピリオドを入力）を指定します。*.amer.example.com など。 • [IP アドレス（IP Address）]：証明書に関連付けられる ISE ノードの IP アドレス。 • [Uniform Resource Identifier]：証明書に関連付ける URI。 • [ディレクトリ名（Directory Name）]：RFC 2253 に従って定義される識別名（DN）の文字列表現。DN 間はカンマ（,）で区切ります。「dnQualifier」RDN の場合は、カンマをエスケープし、区切り文字としてバックスラッシュ カンマ「\,」を使用します。たとえば、CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL などです。
キー タイプ	RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。

フィールド	使用上のガイドライン
キーの長さ（Key Length）	公開キーのビット サイズを指定します。 RSA には、次のオプションを使用できます。 • 512 • 1024 • 2048 • 4096 ECDSA には、次のオプションを使用できます。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。 パブリック CA の署名付き証明書を取得するか、FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は 2048 以上を選択します。
署名するダイジェスト（Digest to Sign With）	ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。
証明書ポリシー（Certificate Policies）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。

関連トピック

証明書署名要求 （185 ページ）
証明書署名要求の作成と認証局への CSR の送信 （185 ページ）
CSR への CA 署名付き証明書のバインド （185 ページ）

発行および失効した証明書

次の表で、[発行および失効した証明書の概要（Overview of Issued and Revoked Certificates）] ページのフィールドについて説明します。展開内の PSN ノードがエンドポイントに証明書を発行します。このページでは、展開内の各 PSN ノードが発行するエンドポイント証明書に関する情報を示します。このページへのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[概要（Overview）]** です。

表 *173* : 発行された証明書と失効した証明書

フィールド	使用上のガイドライン
ノード名	証明書を発行したポリシー サービス ノード（PSN）の名前。
[発行された証明書（Certificates Issued）]	PSN ノードが発行したエンドポイント証明書の数。
[取り消された証明書（Certificates Revoked）]	失効したエンドポイント証明書（PSN ノードが発行した証明書）の数。
[証明書要求（Certificates Requests）]	PSN ノードが処理した証明書ベースの認証要求の数。
[失敗した証明書（Certificates Failed）]	PSN ノードが処理する失敗した認証要求の数。

関連トピック

発行された証明書 （209 ページ）
ユーザおよびエンドポイントの証明書の更新 （196 ページ）
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 （214 ページ）
ユーザによる証明書の更新を許可する Cisco ISE の設定 （197 ページ）
エンドポイント証明書の失効 （235 ページ）

証明書のステータス（OCSP または CRL）を確認します。

Cisco ISE は、証明書失効リスト（CRL）を定期的にチェックします。このページを使用して、自動的にダウンロードされた CRL に対して進行中のセッションをチェックするように Cisco ISE を設定できます。OCSP または CRL のチェックを毎日開始する時刻と、OCSP サーバまたは CRL を再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定できます。

次の表では、[証明書定期チェックの設定（Certificate Periodic Check Settings）] ページのフィールドについて説明します。このページを使用して、証明書（OCSP または CRL）のステータスをチェックする時間間隔を指定できます。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [証明書定期チェックの設定（Certificate Periodic Check Settings）]** です。

表 *174* : 証明書定期チェックの設定

フィールド名	使用上のガイドライン
証明書チェックの設定	

フィールド名	使用上のガイドライン
自動的に取得されたCRLに対する進行中のセッションのチェック（**Check ongoing sessions against automatically retrieved CRL**）	Cisco ISE が自動的にダウンロードされた CRL に対する進行中のセッションをチェックするようにするには、このチェックボックスをオンにします。
CRL/OCSP の定期的な証明書チェック	
最初のチェック時刻（**First check at**）	CRL または OCSP のチェックを毎日開始する時刻を指定します。00:00 ～ 23:59 の時間範囲の値を入力します。
チェック間隔（**Check every**）	CRL または OCSP サーバを再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定します。

関連トピック

OCSP サービス （235 ページ）
OCSP クライアント プロファイルの追加 （237 ページ）

システム証明書のインポート設定

次の表では、サーバ証明書をインポートするために使用できる [システム証明書のインポート（Import System Certificate）] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理（Administration）]** > > > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** > **[インポート（Import）]** です。

表 *175 :* システム証明書のインポート設定

フィールド名	説明
ノードの選択（**Select Node**）	（必須）システム証明書をインポートする Cisco ISE ノードを選択します。
証明書ファイル（**Certificate file**）	（必須）[参照（Browse）] をクリックして、ローカル システムから証明書ファイルを選択します。
秘密キー ファイル（**Private key file**）	（必須）[参照（Browse）] をクリックして、秘密キー ファイルを選択します。
[パスワード（Password）]	（必須）秘密キー ファイルを復号化するためのパスワードを入力します。

フィールド名	説明
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ワイルドカード証明書の許可（**Allow Wildcard Certificates**）	ワイルドカード証明書（サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク（*）が含まれている証明書）をインポートする場合は、このチェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。このチェックボックスをオンにすると、Cisco ISE は展開内の他のすべてのノードにこの証明書をインポートします。
証明書の拡張の検証（**Validate Certificate Extensions**）	Cisco ISE に証明書の拡張の検証を許可する場合は、このチェックボックスをオンにします。このチェックボックスをオンにし、かつインポートする証明書に CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。
Usage	このシステム証明書を使用する必要があるサービスを選択します。 • [管理者（Admin）]：管理者ポータルとの通信および展開内の ISE ノード間の通信の保護に使用されるサーバ証明書 （注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。 • [EAP 認証（EAP Authentication）]：SSL/TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバ証明書 • [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバ証明書 • [pxGrid]：pxGrid クライアントとサーバの間の通信を保護するクライアントおよびサーバ証明書 • [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバ証明書

関連トピック

システム証明書 （157 ページ）
システム証明書の表示 （158 ページ）
システム証明書のインポート （159 ページ）

[信頼できる証明書ストア（Trusted Certificate Store）] ページ

次の表では、管理ノードに追加された証明書を表示するために使用できる [信頼できる証明書ストア（Trusted Certificates Store）] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** です。

表 *176 :* 信頼できる証明書ページ

フィールド名	使用上のガイドライン
フレンドリ名（**Friendly Name**）	証明書の名前を表示します。
Status（ステータス）	有効または無効にします。[無効（Disabled）] の場合、ISEは信頼を確立するために証明書を使用しません。
信頼対象（**Trusted for**）	証明書を使用するサービスを表示します。
発行先（**Issued To**）	証明書のサブジェクトの一般名（CN）。
発行元（**Issued By**）	証明書の発行元の一般名（CN）。
有効期限の開始（**Valid From**）	「Not Before」証明書属性。
Expiration Date	「Not After」証明書属性。
有効期限ステータス（**Expiration Status**）	証明書の有効期限のステータスに関する情報です。このコラムに表示される情報メッセージには5つのアイコンとカテゴリがあります。 • **緑色**：期限切れまで 91 日以上 • **青色**：期限切れまで 90 日以内 • **黄色**：期限切れまで 60 日以内 • **オレンジ色**：期限切れまで 30 日以内 • **赤色**: 期限切れ

関連トピック

信頼できる証明書ストア （168 ページ）
信頼できるストア証明書の表示 （172 ページ）
信頼できる証明書ストアの証明書のステータス変更 （172 ページ）
信頼できる証明書ストアへの証明書の追加 （173 ページ）

証明書設定の編集

次の表では、認証局（CA）証明書属性を編集するために使用できる [証明書ストアの証明書編集（Certificate Store Edit Certificate）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [証明書（Certificate）] > [編集（Edit）]** です。

表 *177 :* 証明書ストア編集設定

フィールド名	使用上のガイドライン
証明書発行元（Certificate Issuer）	
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。
Status（ステータス）	[有効（Enabled）] または [無効（Disabled）] を選択します。[無効（Disabled）] の場合、ISE は信頼を確立するために証明書を使用しません。
説明	任意で説明を入力します。
使用方法	
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書で（他の ISE ノードまたは LDAP サーバから）サーバ証明書を検証する場合は、このチェックボックスをオンにします。
クライアント認証および **syslog** 用に信頼する（**Trust for client authentication and Syslog**）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した ISE に接続するエンドポイントの認証 • syslog サーバの信頼
シスコ サービスの認証用に信頼する（**Trust for authentication of Cisco Services**）	フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
証明書ステータスの検証（Certificate Status Validation）	ISEは、特定のCAが発行するクライアントまたはサーバ証明書の失効ステータスをチェックする2とおりの方法をサポートしています。1つは、Online Certificate Status Protocol（OCSP）を使用して証明書を検証することです（OCSPは、CAによって保持されるOCSPサービスに要求を行います）。もう1つは、ISEにCAからダウンロードした証明書失効リスト（CRL）に対して証明書を検証することです。両方の方法は、OCSPを最初に使用し、ステータスを判断できないときに限りCRLを使用する場合に使用できます。
OCSP サービスに対して検証する（Validate Against OCSP Service）	OCSP サービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まずOCSPサービスを作成する必要があります。
OCSP が不明なステータスを返した場合は要求を拒否する（Reject the request if OCSP returns UNKNOWN status）	認証ステータスがOCSPによって判別されなかった場合に要求を拒否するには、このチェックボックスをオンにします。このチェックボックスをオンにした場合、OCSPサービスによって不明のステータス値が返されると、ISEは現在評価されているクライアントまたはサーバ証明書を拒否します。
OCSP応答側が到達不能な場合は要求を拒否する（Reject the request if OCSP Responder is unreachable）	OCSP応答側が到達不能な場合にISEが要求を拒否するには、このチェックボックスをオンにします。
CRL のダウンロード（Download CRL）	Cisco ISEでCRLをダウンロードするには、このチェックボックスをオンにします。
CRL 配信 URL（CRL Distribution URL）	CA から CRL をダウンロードするための URL を入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URL は「http」、「https」、または「ldap」で始まる必要があります。
CRL の取得（Retrieve CRL）	CRL は、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。
ダウンロードが失敗した場合は待機する（If download failed, wait）	Cisco ISEがCRLを再度ダウンロードするまでに待機する時間間隔を設定します。

フィールド名	使用上のガイドライン
CRL を受信しない場合 CRL 検証をバイパスする（Bypass CRL Verification if CRL is not Received）	このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。
CRL がまだ有効でないか、または期限切れの場合は無視する（Ignore that CRL is not yet valid or expired）	Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。 Cisco ISE で [有効日（Effective Date）] フィールドの開始日と [次の更新（Next Update）] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRL がまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。

関連トピック

信頼できる証明書ストア （168 ページ）
信頼できる証明書の編集 （173 ページ）

信頼できる証明書のインポート設定

次の表では、認証局（CA）証明書を Cisco ISE に追加するために使用できる [信頼できる証明書のインポート（Trusted Certificate Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** です。

表 ***178 :*** 信頼できる証明書のインポート設定

フィールド	説明
証明書ファイル（Certificate file）	[参照（Browse）] をクリックして、ブラウザを実行しているコンピュータから証明書ファイルを選択します。

フィールド	説明
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE により <common name>#<issuer>#<nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書を（他の ISE ノードまたは LDAP サーバから）サーバ証明書の検証に使用する場合は、このチェックボックスをオンにします。
クライアント認証および syslog 用に信頼する（Trust for client authentication and Syslog）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した ISE に接続するエンドポイントの認証 • syslog サーバの信頼
シスコ サービスの認証用に信頼する（Trust for authentication of Cisco Services）	フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書の拡張の検証（Validate Certificate Extensions）	（[クライアント認証用に信頼する（Trust for client authentication）] オプションと [証明書拡張の検証を有効にする（Enable Validation of Certificate Extensions）] オプションの両方をオンにした場合のみ）「keyUsage」拡張が存在し、「keyCertSign」ビットが設定されていることと、CA フラグが true に設定された基本制約拡張が存在することを確認します。
説明	任意で説明を入力します。

関連トピック

信頼できる証明書ストア （168 ページ）
証明書チェーンのインポート （179 ページ）
信頼できる証明書ストアへのルート証明書のインポート （177 ページ）

OCSP クライアント プロファイル設定

次の表では、OCSP クライアント プロファイル設定を行うために使用できる [OCSP クライアント プロファイル（OCSP Client Profile）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [OCSP クライアント プロファイル（OCSP Client Profile）]** です。

表 *179 : OCSP* クライアント プロファイル設定

フィールド名	使用上のガイドライン
名前（**Name**）	OCSP クライアント プロファイル名。
説明	任意で説明を入力します。
OCSP応答側の設定（Configure OCSP Responder）	
セカンダリ サーバの有効化（**Enable Secondary Server**）	ハイ アベイラビリティのセカンダリ OCSP サーバを有効にするには、このチェックボックスをオンにします。
常にプライマリ サーバに最初にアクセスする（**Always Access Primary Server First**）	このオプションは、セカンダリ サーバへの移動を試行する前にプライマリ サーバをチェックする場合に使用します。プライマリが以前にチェックされ、応答しないことがわかっている場合にも、Cisco ISE はセカンダリ サーバに移動する前にプライマリ サーバへの要求の送信を試行します。
[n 分経過後にプライマリ サーバにフォールバック（Fallback to Primary Server After Interval *n* Minutes）]	このオプションは、Cisco ISE がセカンダリ サーバに移動してから、再度プライマリ サーバにフォールバックする場合に使用します。この場合、その他の要求はすべてスキップされ、テキスト ボックスで設定した時間セカンダリ サーバが使用されます。許可される時間の範囲は 1 ～ 999 分です。
プライマリ サーバとセカンダリ サーバ（Primary and Secondary Servers）	
URL	プライマリおよびセカンダリ OCSP サーバの URL を入力します。
ナンス拡張サポートの有効化（**Enable Nonce Extension Support**）	ナンスが OCSP 要求の一部として送信されるように設定できます。ナンスには、OCSP 要求の疑似乱数が含まれます。応答で受信される数値は要求に含まれる数値と同じであることが検証されています。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。

フィールド名	使用上のガイドライン
応答の署名の検証（**Validate Response Signature**）	OCSP レスポンダは、次のいずれかの証明書を使用して応答に署名します。 • CA 証明書 • CA 証明書とは別の証明書 Cisco ISE が応答の署名を検証するためには、OCSP 応答側が応答を証明書とともに送信する必要があります。そうでない場合、応答の検証は失敗し、証明書のステータスは利用できません。RFC に従い、OCSP は異なる証明書を使用して応答に署名できます。このことは、OCSP が Cisco ISE による検証用に応答に署名した証明書を送信する限り当てはまります。OCSP が Cisco ISE で設定されているものとは異なる証明書を使用して応答に署名した場合、応答の検証は失敗します。
Authority Information Access（**AIA**）に指定された**OCSP URL**を使用する（**Use OCSP URLs specified in Authority Information Access (AIA)**）	Authority Information Access の拡張で指定されている OCSP URL を使用するには、オプション ボタンをクリックします。
応答キャッシュ（**Response Cache**）	

フィールド名	使用上のガイドライン
[キャッシュ エントリの存続可能時間 n 分(Cache Entry Time To Live *n* Minutes)]	キャッシュ エントリが期限切れになる時間を分単位で入力します。OCSP サーバからの各応答には nextUpdate 値が含まれています。この値は、証明書のステータスがサーバで次にいつ更新されるかを示します。OCSP 応答がキャッシュされるとき、2 つの値（1 つは設定から、もう 1 つは応答から）が比較され、この 2 つの最小値の時間だけ応答がキャッシュされます。nextUpdate 値が 0 の場合、応答はまったくキャッシュされません。Cisco ISE は設定された時間 OCSP 応答をキャッシュします。キャッシュは複製されず、永続的でもないため、Cisco ISE が再起動するとキャッシュはクリアされます。次の理由により、OCSP キャッシュは OCSP 応答を保持するために使用されます。 • 既知の証明書に関する OCSP サーバからのネットワークトラフィックと負荷を低減するため • 既知の証明書のステータスをキャッシュすることによって Cisco ISE のパフォーマンスを向上させるため デフォルトでは、キャッシュは内部 CA OCSP クライアント プロファイルに対し 2 分に設定されています。エンドポイントが最初の認証から 2 分以内にもう一度認証すると、OCSP のキャッシュが使用され、OCSP レスポンダには問い合わせされません。エンドポイントの証明書がキャッシュ期間内に失効した場合、以前の OCSP のステータス [良好（Good）] が使用され、認証は成功します。キャッシュを 0 分に設定すると、応答はキャッシュされません。このオプションでは、セキュリティは向上しますが、認証のパフォーマンスは低下します。
キャッシュのクリア（Clear Cache）	OCSP サービスに接続されているすべての認証局のエントリをクリアするには、[キャッシュのクリア（Clear Cache）] をクリックします。 展開内で、[キャッシュのクリア（Clear Cache）] はすべてのノードと相互作用して、処理を実行します。このメカニズムでは、展開内のすべてのノードが更新されます。

関連トピック

OCSP サービス （235 ページ）
Cisco ISE CA サービスの Online Certificate Status Protocol レスポンダ （236 ページ）
OCSP 証明書のステータスの値 （236 ページ）
OCSP ハイ アベイラビリティ （236 ページ）
OCSP の障害 （237 ページ）
OCSP 統計情報カウンタ （241 ページ）

OCSP クライアント プロファイルの追加 （237 ページ）

内部 CA の設定

次の表では、内部 CA の設定ページのフィールドについて説明します。内部 CA の設定を表示し、このページから内部 CA サービスを無効にできます。このページへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [内部 CA の設定（Internal CA Settings）]** です。

表 *180 :* 内部 *CA* の設定

フィールド名	使用上のガイドライン
認証局の無効化（Disable Certificate Authority）	内部 CA サービスを無効にするには、このボタンをクリックします。
ホスト名（Host Name）	CA サービスを実行している Cisco ISE ノードのホスト名。
ペルソナ（Personas）	CA サービスを実行しているノードで有効な Cisco ISE ノードのペルソナ。たとえば、管理、ポリシー サービスなどです。
ロール（Role(s)）	CA サービスを実行する Cisco ISE ノードが担当するロール。たとえば、スタンドアロンまたはプライマリまたはセカンダリです。
CA、EST、および OCSP 応答側のステータス（CA, EST & OCSP Responder Status）	有効または無効
OCSP 応答側 URL（OCSP Responder URL）	OCSP サーバにアクセスするための Cisco ISE ノードの URL。
SCEP URL	SCEP サーバにアクセスするための Cisco ISE ノードの URL。

関連トピック

Cisco ISE CA サービス （201 ページ）
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 （214 ページ）

証明書テンプレートの設定

次の表に、クライアント プロビジョニング ポリシーで使用される SCEP RA プロファイルの定義に使用できる [CA 証明書テンプレート（CA Certificate Template）] ページのフィールドを示します。このページへのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > > **[証明書テンプレート（Certificate Templates）]** > **[追加（Add）]** です。

（注） 証明書テンプレート フィールド（[組織ユニット（Organizational Unit）]、[組織（Organization）]、[都市（City）]、[州（State）]、および [国（Country）]）の UTF-8 文字はサポートしていません。UTF-8 文字を証明書テンプレートで使用すると、証明書プロビジョニングが失敗します。

表 *181* : 証明書テンプレートの設定

フィールド名	使用上のガイドライン
名前（Name）	（必須）証明書テンプレートの名前を入力します。たとえば、Internal_CA_Template とします。
説明	（任意）説明を入力します。
Common Name（CN）	（表示のみ）一般名にはユーザ名が自動入力されます。
Organizational Unit（OU）	組織ユニット名。Engineering など。
Organization（O）	組織名。Cisco など。
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。
国（Country）（C）	国名。2 文字の ISO 国番号を入力する必要があります。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	（表示のみ）エンドポイントの MAC アドレス。
キー タイプ	RSA または ECC

フィールド名	使用上のガイドライン
キー サイズ	（RSA を選択した場合にのみ適用可能）1024 以上のキー サイズを指定します。
曲線タイプ（Curve Type）	（ECC を選択した場合にのみ適用可能）曲線のタイプを指定します（デフォルトは P-384 です）。
SCEP RA プロファイル（SCEP RA Profile）	ISE 内部 CA または作成した外部 SCEP RA プロファイルを選択します。
有効期限（Valid Period）	証明書の期限が切れるまでの日数を入力します。
拡張キーの使用状況	
クライアント認証	クライアント認証にこの証明書を使用する場合は、このチェック ボックスをオンにします。
サーバ認証（Server Authentication）	サーバ認証にこの証明書を使用する場合は、このチェック ボックスをオンにします。

関連トピック

証明書テンプレート （207 ページ）
証明書テンプレート名の拡張子 （207 ページ）
証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定 （214 ページ）
pxGrid コントローラ用の Cisco ISE CA 証明書の展開 （208 ページ）
許可ポリシー条件での証明書テンプレート名の使用 （207 ページ）

ロギングの設定

次の各ページでは、デバッグ ログの重大度の設定、外部ログ ターゲットの作成が可能です。また、Cisco ISE がこれらの外部ログ ターゲットにログ メッセージを送信できるようにできます。

リモート ロギング ターゲットの設定

次の表では、外部の場所（syslog サーバ）を作成してロギング メッセージを保存するために使用できる [リモート ロギング ターゲット（Remote Logging Targets）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** です。

表 *182 :* リモート ロギング ターゲットの設定

フィールド	使用上のガイドライン
名前（Name）	新しいターゲットの名前を入力します。
ターゲット タイプ（Target Type）	ターゲット タイプを選択します。デフォルトでは、[UDP Syslog] に設定されます。
説明	新しいターゲットの簡単な説明を入力します。
[IPアドレス（IP Address）]	ログを格納する宛先マシンの IP アドレスまたはホスト名を入力します。
[ポート（Port）]	宛先マシンのポート番号を入力します。
ファシリティ コード（Facility Code）	ロギングに使用する syslog ファシリティ コードを選択します。有効なオプションは、Local0 ～ Local7 です。
最大長（Maximum Length）	リモートログターゲットメッセージの最大長を入力します。有効なオプションは200～1024バイトです。
サーバダウン時のバッファ メッセージ（Buffer Message When Server Down）	TCP syslog ターゲットおよびセキュア syslog ターゲットが使用できないときに Cisco ISE に syslog メッセージをバッファするには、このチェックボックスをオンにします。ISEは、接続が再開されるとターゲットへのメッセージの送信を再試行します。接続が再開された後、メッセージは古いものから順に送信され、バッファ内のメッセージは常に新しいメッセージの前に送信されます。バッファがいっぱいになると、古いメッセージが廃棄されます。
バッファ サイズ（MB）（Buffer Size (MB)）	各ターゲットのバッファサイズを設定します。デフォルトでは、100 MB に設定されます。バッファ サイズを変更するとバッファがクリアされ、特定のターゲットのバッファリングされた既存のすべてのメッセージが失われます。
再接続タイムアウト（秒）（Reconnect Timeout (Sec)）	サーバがダウンしている場合に TCP およびセキュア syslog を廃棄する前に保持する期間を秒単位で指定します。
CA 証明書の選択（Select CA Certificate）	クライアント証明書を選択します。

フィールド	使用上のガイドライン
サーバ証明書有効性を無視（Ignore Server Certificate validation）	ISE でサーバ証明書認証が無視されるようにして、syslog サーバを許可するには、このチェックボックスをオンにします。デフォルトでは、このオプションが無効になっているときにシステムが FIPS モードでない限り、このオプションはオフに設定されます。

関連トピック

Cisco ISE ロギング メカニズム （291 ページ）
Cisco ISE システム ログ （292 ページ）
リモート syslog メッセージの形式
Cisco ISE メッセージ カタログ （295 ページ）
収集フィルタ （298 ページ）
イベント抑制バイパス フィルタ （298 ページ）
リモート syslog 収集場所の設定 （293 ページ）
収集フィルタの設定 （298 ページ）

ロギング カテゴリの設定

次の表では、[ロギング カテゴリ（Logging Categories）]ページのフィールドについて説明します。これらのフィールドを使用して、ログの重大度レベルを設定し、選択したカテゴリのログが保存されるロギング ターゲットを選択できます。このページへのナビゲーション パスは、[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギングカテゴリ（Logging Categories）] です。

表 *183*：ロギング カテゴリの設定

フィールド	使用上のガイドライン
名前（Name）	ロギング カテゴリの名前を表示します。

フィールド	使用上のガイドライン
ログの重大度レベル（Log Severity Level）	次のオプションから、診断ロギング カテゴリの重大度レベルを選択できます。 • [重大（FATAL）]：緊急事態。 このオプションは、Cisco ISE が使用できないため、緊急措置が必要であることを意味します • [エラー（ERROR）]：このオプションは深刻な状態またはエラー状態を示します。 • [警告（WARN）]：このオプションは、通常の状態ではあるが重大な状態を示します。 これがデフォルトの条件です。 • [情報（INFO）]：このオプションは、情報メッセージを示します。 • [デバッグ（DEBUG）]：このオプションは、診断バグ メッセージを示します。
ローカル ロギング（Local Logging）	ローカル ノードで上のこのカテゴリのロギング イベントを有効にするには、このチェックボックスをオンにします。
ターゲット（Target）	左アイコンと右アイコンを使用して[使用可能（Available）]と[選択済み（Selected）]のボックス間でターゲットを移動することによって、カテゴリのターゲットを変更できます。[使用可能（Available）]ボックスには、論理（事前定義済み）と外部（ユーザ定義）という両方の既存のロギング ターゲットが含まれています。最初は空の[選択済み（Selected）]ボックスには、特定のカテゴリの選択済みターゲットが含まれます。

関連トピック

リモート syslog メッセージの形式

Cisco ISE メッセージ コード （294 ページ）

リモート syslog 収集場所の設定 （293 ページ）

メッセージ コードの重大度レベルの設定 （294 ページ）

メンテナンスの設定

これらのページでは、バックアップ、復元、およびデータ消去機能を使用してデータを管理できます。

リポジトリの設定

次の表では、リポジトリを作成してバックアップ ファイルを保存するために使用できる [リポジトリ リスト（Repository List）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[メンテナンス（Maintenance）]** > **[リポジトリ（Repository）]** です。

表 *184 :* リポジトリの設定

フィールド	使用上のガイドライン
リポジトリ（Repository）	リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。
プロトコル	使用する使用可能なプロトコルの 1 つを選択します。
サーバ名（Server Name）	（TFTP、HTTP、HTTPS、FTP、SFTP、および NFS で必須）リポジトリの作成先サーバのホスト名または IPv4 アドレスを入力します。 （注） IPv6 アドレスを使用してリポジトリを追加する場合は、IPv6 アドレスを使用して ISE eth0 インターフェイスが設定されていることを確認します。
パス	リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。 この値は、サーバのルート ディレクトリを示す 2 つのスラッシュ（//）または単一のスラッシュ（/）で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ（/）はルート ディレクトリではなく FTP ユーザのホーム ディレクトリを示します。

フィールド	使用上のガイドライン
PKI 認証を有効にします。	（オプション：SFTP リポジトリにのみ適用）SFTP リポジトリで RSA 公開キー認証を有効にするには、このチェック ボックスをオンにします。
ユーザ名（User Name）	（FTP、SFTP、および NFS で必須）指定されたサーバに対する書き込み権限を持つユーザ名を入力します。使用できる文字は英数字のみです。
[パスワード（Password）]	（FTP、SFTP、および NFS で必須）指定されたサーバへのアクセスに使用するパスワードを入力します。パスワードに使用できる文字は、0 ～ 9、a ～ z、A ～ Z、-、.、|、@、#、$、%、^、&、*、,、+、および = です。

関連トピック

バックアップ/復元リポジトリ （265 ページ）
リポジトリの作成 （266 ページ）

オンデマンド バックアップの設定

次の表では、バックアップを任意の時点で取得するために使用できる [オンデマンド バックアップ（On-Demand Backup）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup & Restore）]** です。

表 *185* : オンデマンド バックアップの設定

フィールド	使用上のガイドライン
バックアップ名（Backup Name）	バックアップ ファイルの名前を入力します。
リポジトリ名（Repository Name）	バックアップファイルを保存するリポジトリ。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（Encryption Key）	このキーは、バックアップ ファイルの暗号化および解読に使用されます。

関連トピック

バックアップ データのタイプ （265 ページ）

スケジュール バックアップの設定

次の表では、フル バックアップまたは差分バックアップの復元に使用できる [スケジュール バックアップ（Scheduled Backup）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** です。

表 *186* : スケジュール バックアップの設定

フィールド	使用上のガイドライン
名前（Name）	バックアップ ファイルの名前を入力します。任意の説明的な名前を入力できます。Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加して、ファイルをリポジトリに格納します。一連のバックアップを設定しても、バックアップ ファイル名は一意になります。[スケジュール バックアップ（Scheduled Backup）] リスト ページでは、ファイルが **kron** occurrence ジョブであることを示すために、バックアップ ファイル名に「backup_occur」が付加されます。 .
説明	バックアップの説明を入力します。
リポジトリ名（Repository Name）	バックアップ ファイルを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（Encryption Key）	バックアップ ファイルを暗号化および復号化するためのキーを入力します。
スケジューリング オプション（Schedule Options）	スケジュール バックアップの頻度を選択し、適宜他のオプションに入力します。

関連トピック

バックアップ データのタイプ （265 ページ）
オンデマンドおよびスケジュール バックアップ （269 ページ）
バックアップ履歴 （277 ページ）
バックアップの失敗 （277 ページ）
Cisco ISE 復元操作 （278 ページ）
認証および許可ポリシー設定のエクスポート （285 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （286 ページ）
CLI を使用したバックアップ （277 ページ）
バックアップのスケジュール （273 ページ）

ポリシーのエクスポート設定のスケジュール

次の表では、[ポリシーのエクスポートのスケジュール（Schedule Policy Export）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）] > [ポリシーのエクスポート（Policy Export）]** です。

表 *187* : ポリシーのエクスポート設定のスケジュール

フィールド	使用上のガイドライン
暗号化（Encryption）	
暗号化キー（Encryption Key）	エクスポート データを暗号化および復号化するためのキーを入力します。このフィールドは、[暗号キーを使用したエクスポート（Export with Encryption Key）] オプションを選択した場合にのみ有効になります。
[接続先（Destination）]	
ローカルコンピュータにファイルをダウンロード（Download file to local computer）	ポリシー エクスポート ファイルをローカル システムにダウンロードできます。
[ファイルをメールで送信（Email file to）]	複数の電子メール アドレスをカンマで区切って入力します。
リポジトリ （Repository）	エクスポート データを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。ポリシーのエクスポートのスケジュールを設定する前に、リポジトリを作成してください。

フィールド	使用上のガイドライン
今すぐエクスポート（Export Now）	指定したリポジトリにデータをすぐにエクスポートするには、このオプションをクリックします。
スケジュール	
スケジューリング オプション（Schedule Options）	エクスポートのスケジュールの頻度を選択し、それに応じてその他の詳細を入力します。

管理者アクセスの設定

これらのページにより、管理者のアクセス設定を行うことができます。

管理者パスワード ポリシーの設定

次の表に、管理者パスワードが満たす必要のある基準を定義するために使用できる [管理者パスワード ポリシー（Administrator Password Policy）] ページのフィールドを示します。このページのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理アクセス（Admin Access）]** > **[認証（Authentication）]** > **[パスワード ポリシー（Password Policy）]** です。

表 *188 :* 管理者パスワード ポリシーの設定

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

フィールド	使用上のガイドライン
パスワードに使用できない文字（Password may not contain）	[管理者名またはその文字の逆順は使用できません（Admin name or its characters in reverse order）]：このチェックボックスをオンにして、管理者ユーザ名またはその文字の逆順での使用を制限します。
	[「cisco」またはその文字の逆順は使用できません（"cisco" or its characters in reverse order）]：このチェックボックスをオンにして、単語「cisco」またはその文字の逆順での使用を制限します。
	[この単語またはその文字の逆順は使用できません（This word or its characters in reverse order）]：このチェックボックスをオンにして、定義したすべての単語またはその文字の逆順での使用を制限します。
	[4 回以上連続する繰り返し文字は使用できません（Repeated characters four or more times consecutively）]：このチェックボックスをオンにして、4回以上連続する繰り返し文字の使用を制限します。

フィールド	使用上のガイドライン
	[辞書の単語、その文字の逆順、または文字の置き換えは使用できません（Dictionary words, their characters in reverse order or their letters replaced with other characters]：辞書の単語、単語の文字の逆順での使用、単語の文字の置き換えでの使用を制限します。 「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば Pa$$w0rd などです。 • [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。 デフォルトでは、このオプションが選択されています。 • [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択（Choose File）] をクリックし、カスタム辞書ファイルを選択します。このテキスト ファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。
必須の文字（Required Characters）	管理者パスワードに、次の選択肢から選択したタイプの文字が少なくとも 1 つ含まれている必要があることを指定します。 • 小文字の英文字 • 大文字の英文字 • 数字（Numeric characters） • 英数字以外の文字（Non-alphanumeric characters）

フィールド	使用上のガイドライン
パスワード履歴（Password History）	同じパスワードが繰り返し使用されるのを防ぐために、新しいパスワードと異なっている必要がある以前のパスワードの数を指定します。 また、以前のパスワードと異なる必要がある文字数を指定します。 ユーザがパスワードを再使用できない日数を入力します。
パスワードライフタイム（Password Lifetime）	次のオプションを指定して、指定した期間後にパスワードを変更するようユーザに強制します。 • パスワードが変更されなかった場合に管理者アカウントを無効にするまでの時間（日数）（Time (in days) before the administrator account is disabled if the password is not changed.）（使用可能な範囲は 0 ～ 2,147,483,647 日です）。 • 管理者アカウントが無効になるまでのリマインダ（日数）。（Reminder (in days) before the administrator account is disabled.）
ネットワーク デバイスの機密データの表示	
管理者パスワードが必要（Require Admin Password）	共有秘密やパスワードなどのネットワーク デバイスの機密データを表示するために管理者ユーザがログイン パスワードを入力するようにする場合には、このチェックボックスにマークを付けます。
パスワードのキャッシュ期間（Password cached for）	管理者ユーザによって入力されたパスワードは、この期間キャッシュされます。管理者ユーザはこの間、ネットワークデバイスの機密データを表示するためにパスワードの再入力を求められることはありません。有効な範囲は 1 ～ 60 分です。

関連トピック

Cisco ISE 管理者 （3 ページ）
新しい管理者の作成 （4 ページ）

セッション タイムアウトおよびセッション情報の設定

次の表では、セッションタイムアウトを定義し、アクティブな管理セッションを終了するために使用できる[セッション（Session）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** です。

表 *189*：セッション タイムアウトおよびセッション情報の設定

フィールド	使用上のガイドライン
セッションのタイムアウト（Session Timeout）	
セッション アイドル タイムアウト（Session Idle Timeout）	アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。
セッション情報（Session Info）	
無効化（Invalidate）	終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。

関連トピック

管理者アクセスの設定 （243 ページ）
管理者のセッション タイムアウトの設定 （247 ページ）
アクティブな管理セッションの終了 （247 ページ）

設定

これらのページでは、さまざまなサービスの全般設定を行うことができます。

ポスチャの全般設定

次の表では、修復時間およびポスチャ ステータスなどの一般的なポスチャ設定を行うために使用できる [ポスチャの全般設定（Posture General Settings）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]** です。

表 *190* : ポスチャの全般設定

フィールド	使用上のガイドライン
修復タイマー（Remediation Timer）	分単位で時間値を入力します。デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。
ネットワーク遷移遅延（Network Transition Delay）	秒単位で時間値を入力します。デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。
デフォルトのポスチャ ステータス（Default Posture Status）	準拠または非準拠を選択します。Linux のような非エージェント デバイスは、ネットワークに接続している間、このステータスを想定します。
一定時間（秒）経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After）	このチェックボックスをオンにすると、指定された時間後に、ログイン成功画面が自動的に閉じます。 チェックボックスの隣のフィールドに、時間値を秒単位で入力します。 0 ～ 300 秒にログイン画面が自動的に閉じるようにタイマーを設定できます。時間をゼロに設定した場合は、クライアント上のエージェントはログイン成功画面を表示しません。
連続モニタリング間隔（Continuous Monitoring Interval）	AnyConnect がモニタリング データの送信を開始するまでの時間間隔を指定します。アプリケーション条件の場合アプリケーションおよびハードウェア条件の場合、デフォルト値は 5 分です。
ステルス モードでの利用規約（Acceptable Use Policy in Stealth Mode）	会社のネットワーク使用条件が満たされていない場合、ステルス モードで [ブロック（Block）] を選択して、クライアントを非準拠ポスチャ ステータスに移行します。
ポスチャのリース	
ユーザがネットワークに接続するたびにポスチャ評価を行う（Perform posture assessment every time a user connects to the network）	ユーザがネットワークに接続するたびにポスチャ評価を開始するには、このオプションを選択します。
n 日おきにポスチャ評価を行う（Perform posture assessment every n days）	クライアントがすでにポスチャ準拠であるものの、指定された日数が経過したら、ポスチャ評価を開始する場合は、このオプションを選択します。

フィールド	使用上のガイドライン
最後の既知の良い状態をキャッシュする（Cache Last Known Good State）	ポスチャ評価の結果をキャッシュするには、Cisco ISE のこのチェックボックスをオンにします。デフォルトでは、このフィールドは無効です。
最後の既知の良い状態（Last Known Good State）	[最後の既知の良い状態をキャッシュする（Cache Last Known Good State）] チェックボックスをオンにしている場合のみ該当します。Cisco ISE は、このフィールドに指定した期間にわたり、ポスチャ評価の結果をキャッシュします。有効な値は、1 ～ 30 日、1 ～ 720 時間、または 1 ～ 43200 分です。

関連トピック

ポスチャ サービス （1166 ページ）
ポスチャ管理の設定 （1173 ページ）
ポスチャのリース （1178 ページ）
Cisco ISE でのポスチャ セッション サービスの有効化 （1172 ページ）
指定した時間内で修復するためのクライアントの修復タイマーの設定 （1177 ページ）
クライアントの遷移のためのネットワーク遷移遅延タイマーの設定 （1177 ページ）
ログイン成功ウィンドウを自動的に閉じる設定 （1177 ページ）
非エージェント デバイスへのポスチャ ステータスの設定 （1178 ページ）

ポスチャ再評価の構成設定

次の表では、ポスチャ再評価の設定に使用できる [ポスチャ再評価設定（Posture Reassessment Configurations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [再評価（Reassessments）]** です。

表 *191* : ポスチャ再評価の構成設定

フィールド	使用上のガイドライン
構成名	PRA 設定の名前を入力します。
設定の説明（Configuration Description）	PRA 設定の説明を入力します。
再評価適用を使用?（Use Reassessment Enforcement?）	ユーザ ID グループの PRA 設定を適用するには、チェックボックスをオンにします。

フィールド	使用上のガイドライン
適用タイプ（Enforcement Type）	適用する次のアクションを選択します。 • [続行（Continue）]：ユーザはポスチャ要件に関係なくクライアントを修復できるようにユーザ介入なしの特権アクセスが引き続き提供されます。 • [ログオフ（Logoff）]：クライアントが非準拠の場合、ユーザを強制的にネットワークからログオフします。 クライアントが再度ログインしたときのコンプライアンス ステータスは不明です。 • [修復（Remediate）]：クライアントが非準拠の場合、エージェントは修復のために指定の期間待機します。 クライアントが修復された後、エージェントはポリシーサービス ノードにPRA レポートを送信します。修復がクライアントで無視された場合、エージェントはクライアントにネットワークからログオフすることを強制するために、ポリシーサービス ノードにログオフ要求を送信します。 ポスチャ要件が [必須（mandatory）] に設定されている場合、RADIUS セッションはPRA 障害アクションの結果としてクリアされ、クライアントを再びポスチャするには新しい RADIUS セッションを開始する必要があります。 ポスチャ要件が [任意（Optional）] に設定されている場合、クライアント上のエージェントではユーザがエージェントから [続行（Continue）] オプションをクリックできます。ユーザは、制限なしで現在のネットワークにとどまることができます。
インターバル（Interval	最初のログイン成功後にクライアントで PRA を開始する間隔を分単位で入力します。 デフォルト値は 240 分です。最小値は 60 分、最大値は 1440 分です。

フィールド	使用上のガイドライン
猶予時間（Grace time）	クライアントが修復を完了することのできる時間間隔を分単位で入力します。猶予時間をゼロにすることはできません。また、PRA 間隔より大きくする必要があります。デフォルトの最小間隔（5 分）から最小 PRA 間隔までの範囲にすることができます。 最小値は 5 分、最大値は 60 分です。 （注） 猶予時間は、クライアントがポスチャの再評価に失敗した後、適用タイプが修復アクションに設定されている場合にだけ有効です。
ユーザ ID グループの選択（Select User Identity Groups）	PRA設定に対して一意のグループまたはグループの一意の組み合わせを選択します。
PRA の設定（PRA configurations）	既存の PRA 設定と PRA 設定に関連付けられたユーザ ID グループを表示します。

関連トピック

ポスチャのリース （1178 ページ）
定期的再評価 （1179 ページ）
ポスチャ評価オプション
ポスチャ修復オプション （1240 ページ）
ポスチャのカスタム条件 （1241 ページ）
カスタム ポスチャ修復アクション （1243 ページ）
定期的再評価の設定 （1180 ページ）

ポスチャの利用規定の構成設定

次の表では、ポスチャのアクセプタブルユース ポリシーを設定するために使用できるポスチャの [利用規定設定（Acceptable Use Policy Configurations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [利用規定（Acceptable Use Policy）]** です。

表 *192 :* ポスチャ *AUP* の設定

フィールド	使用上のガイドライン
構成名	ユーザが作成する AUP 設定の名前を入力します。

フィールド	使用上のガイドライン
設定の説明（Configuration Description）	ユーザが作成するAUP設定の説明を入力します。
エージェントユーザへの AUP の表示（Windows の場合のみ）	オンにした場合、[エージェントユーザへの AUP の表示（Show AUP to Agent users）] チェックボックスはユーザ（Windows のみ）にネットワークの利用規約へのリンクを表示し、それをクリックすると、認証およびポスチャ評価が成功したときにAUPが表示されます。
AUP メッセージの URL を使用（Use URL for AUP message）オプション ボタン	選択した場合、認証およびポスチャ評価が成功したときにクライアントがアクセスする必要がある AUP メッセージへの URL を AUP URL に入力する必要があります。
AUP メッセージのファイルを使用（Use file for AUP message）オプション ボタン	選択した場合、場所を参照し、トップ レベルに index.html を含む AUP ファイルにジップ形式のファイルをアップロードします。 .zip ファイルには、index.html ファイルに加えて、他のファイルおよびサブディレクトリを含めることができます。これらのファイルは、HTML タグを使用して相互に参照できます。
AUP URL	クライアントは認証およびポスチャ評価が成功したときにアクセスする必要があるAUPへの URL を入力します。
AUP ファイル（AUP File）	[AUP ファイル（AUP File）] で、ファイルを参照し、Cisco ISE サーバにアップロードします。これは zip 形式のファイルで、zip 形式のファイルではトップ レベルに index.html ファイルを含める必要があります。

フィールド	使用上のガイドライン
ユーザ ID グループの選択（Select User Identity Groups）	[ユーザ ID グループの選択（Select User Identity Groups）] ドロップダウン リストで、AUP 設定の一意のユーザ ID グループまたはユーザ ID グループの一意の組み合わせを選択します。 AUP 設定を作成する場合は、次の点に注意してください。 • ポスチャ AUP は、ゲスト フローには適用できません。 • 各設定には、一意のユーザ ID グループ、またはユーザ ID グループの一意の組み合わせが必要です。 • 2 つの設定が共通のユーザ ID グループを持つことはできません。 • ユーザ ID グループ「Any」で AUP 設定を作成する場合は、まず他のすべての AUP 設定を削除します。 • ユーザ ID グループ「Any」を使用して AUP 設定を作成した場合、一意のユーザ ID グループ、または複数のユーザ ID グループを使用して他の AUP 設定を作成することはできません。Any 以外のユーザ ID グループを使用して AUP 設定を作成するには、最初にユーザ ID グループ「Any」を使用した既存の AUP 設定を削除するか、ユーザ ID グループ「Any」を使用した既存の AUP 設定を一意のユーザ ID グループまたは複数のユーザの ID グループを使用して更新します。
利用規定設定 - 設定リスト（Acceptable use policy configurations—Configurations list）	既存の AUP 設定と AUP 設定に関連付けられたエンドユーザ ID グループを一覧表示します。

関連トピック

ポスチャ サービス （1166 ページ）
ポスチャ評価の利用規定の設定 （1188 ページ）

EAP-FAST 設定

次の表に、EAP-FAST、EAP-TLS、およびPEAPプロトコルを設定するために使用できる[プロトコル設定（Protocol Settings）]ページのフィールドを示します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-FAST]** > **[EAP-FAST 設定（EAP-FAST Settings）]** です。

表 *193 : EAP-FAST* の設定

フィールド	使用上のガイドライン
機関識別情報の説明（Authority Identity Info Description）	クレデンシャルをクライアントに送信する Cisco ISE ノードを説明したわかりやすい文字列を入力します。クライアントは、この文字列をタイプ、長さ、および値（TLV）の Protected Access Credentials（PAC）情報で認識できます。デフォルト値は、Identity Services Engine です。
マスター キー生成期間（Master Key Generation Period）	マスターキー生成期間を、秒、分、時間、日、または週単位で指定します。値は、1 ～ 2147040000 秒の正の整数である必要があります。デフォルトは 604800 秒で、これは 1 週間と同等です。
すべてのマスター キーおよび PAC の失効（Revoke all master keys and PACs）	すべてのマスターキーと PAC を失効させるには、[失効（Revoke）] をクリックします。
PAC なしセッション再開の有効化（Enable PAC-less Session Resume）	PAC ファイルなしで EAP-FAST を使用する場合は、このチェックボックスをオンにします。
PAC なしセッションのタイムアウト（PAC-less Session Timeout）	PAC なしセッションの再開がタイムアウトするまでの時間を秒単位で指定します。デフォルトは 7200 秒です。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
プロトコルとして EAP-FAST を使用するためのガイドライン （1046 ページ）
EAP-FAST の利点 （1095 ページ）
EAP-FAST の設定 （1047 ページ）

PAC の設定

次の表では、[PAC の生成（Generate PAC）] ページ上のフィールドについて説明します。これらのフィールドを使用して、EAP-FAST 認証用の Protected Access Credentials を設定します。このページのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定**

（**Settings**）] > **[プロトコル（Protocols）]** > **[EAP-FAST]** > **[PAC の生成（Generate PAC）]** です。

表 *194 : EAP-FAST* の *PAC* の生成の設定

フィールド	使用上のガイドライン
トンネル PAC（Tunnel PAC）	トンネル PAC を生成するには、このオプション ボタンをクリックします。
マシン PAC（Machine PAC）	マシン PAC を生成するには、このオプション ボタンをクリックします。
TrustSec PAC	TrustSec PAC を生成するには、このオプション ボタンをクリックします。
ID（Identity）	（トンネル PAC およびマシン PAC の ID フィールド用）EAP-FAST プロトコルによって「内部ユーザ名」として示されるユーザ名またはマシン名を指定します。ID 文字列がそのユーザ名と一致しない場合、認証は失敗します。これは、適応型セキュリティ アプライアンス（ASA）で定義されているホスト名です。ID 文字列は、ASA ホスト名に一致する必要があります。一致しない場合、ASA は生成された PAC ファイルをインポートできません。TrustSec PAC を生成する場合、[ID（Identity）] フィールドにより TrustSec ネットワーク デバイスのデバイス ID が指定され、EAP-FAST プロトコルによりイニシエータ ID とともに提供されます。ここに入力した ID 文字列がそのデバイス ID に一致しない場合、認証は失敗します。
PAC 存続可能時間（PAC Time To Live）	（トンネル PAC およびマシン PAC 用）PAC の有効期限を指定する値を秒単位で入力します。デフォルトは 604800 秒で、これは 1 週間と同等です。この値は、1 ～ 157680000 秒の正の整数である必要があります。TrustSec PAC に対しては、日、週、月、または年単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。
暗号化キー（Encryption Key）	暗号キーを入力します。キーの長さは 8 ～ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。

フィールド	使用上のガイドライン
期限日（Expiration Date）	（TrustSec PAC のみ）有効期限は、PAC 存続可能時間に基づいて計算されます。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
プロトコルとして EAP-FAST を使用するためのガイドライン （1046 ページ）
EAP-FAST の PAC の生成 （1048 ページ）

EAP-TTLS 設定

次の表では、[EAP-TTLS設定（EAP-TTLS Settings）]ページのフィールドについて説明します。このページへのナビゲーション パスは、[管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロトコル（Protocols）]>[EAP-TTLS] です。

表 *195 : EAP-TTLS* 設定

フィールド	使用上のガイドライン
EAP-TTLSセッションの再開を有効にする（Enable EAP-TTLS Session Resume）	このチェックボックスをオンにすると、Cisco ISE はユーザが EAP-TTLS 認証のフェーズ 2 で正常に認証された場合に限り、EAP-TTLS 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の EAP-TTLS セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、EAP-TTLS のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。 （注） EAP-TTLS セッションが再開されると、内部方式はスキップされます。
EAP-TTLSセッションタイムアウト（EAP-TTLS Session Timeout）	EAP-TTLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
認証プロトコルとしての EAP-TTLS の使用 （1050 ページ）
EAP-TLS の設定 （1051 ページ）

EAP-TLS 設定

次の表に、EAP-TLS プロトコル設定を行うために使用できる [EAP-TLS 設定（EAP-TLS Settings）] ページのフィールドを示します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-TLS]** です。

表 *196 : EAP-TLS* 設定

フィールド	使用上のガイドライン
EAP-TLS セッションの再開を有効にする（Enable EAP-TLS Session Resume）	完全な EAP-TLS 認証に成功したユーザの簡略化された再認証をサポートする場合にオンにします。この機能により、Secure Sockets Layer（SSL）ハンドシェイクのみでユーザの再認証が可能となり、証明書の適用が不要になります。EAP-TLS セッションは、タイムアウトしていない限り動作を再開します。
EAP-TLS セッション タイムアウト（EAP-TLS Session Timeout）	EAP-TLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。
[ステートレス セッション再開（Stateless Session Resume）]	
マスター キー生成期間（Master Key Generation Period）	マスターキー再生成までの時間を入力します。この値により、マスター キーがアクティブである期間が決定します。この値は秒、分、時、日数、または週数で入力できます。
[取り消し（Revoke）]	これまでに生成されたすべてのマスター キーとチケットをキャンセルするには、[取り消し（Revoke）] をクリックします。このオプションは、セカンダリ ノードでは無効です。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
EAP-TLS の設定 （1052 ページ）

PEAP 設定

次の表では、PEAP プロトコル設定を行うために使用できる [PEAP 設定（PEAP Settings）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[PEAP]** です。

表 *197 : PEAP* 設定

フィールド	使用上のガイドライン
PEAP セッションの再開を有効にする（Enable PEAP Session Resume）	このチェックボックスをオンにすると、Cisco ISE はユーザが PEAP 認証のフェーズ 2 で正常に認証された場合に限り、PEAP 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の PEAP セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、PEAP のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。PEAP セッション再開機能を動作させるには、PEAP セッション タイムアウト値を指定する必要があります。
PEAP セッション タイムアウト（PEAP Session Timeout）	PEAP セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。
高速再接続を有効にする（Enable Fast Reconnect）	このチェックボックスをオンにすると、セッション再開機能が有効な場合に、ユーザ クレデンシャルを確認しないで PEAP セッションが Cisco ISE で再開することが許可されます。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
PEAP の設定 （1053 ページ）
PEAP の使用の利点 （1094 ページ）
PEAP プロトコルでサポートされているサプリカント （1094 ページ）
PEAP プロトコルのフロー （1094 ページ）

RADIUS 設定

次の表に、[RADIUS 設定（RADIUS Settings）] ページにある各フィールドの説明を示します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS]** です。

[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）] オプションを有効にすると、認証が繰り返し失敗するクライアントは監査ログに出力されず、指定された期間にわたってこれらのクライアントからの要求が自動的に拒否されます。また、認証失敗回数を指定できます。失敗回数がこの回数を超えると、これらのクライアントからの要求は拒否されます。たとえばこの値を 5 に設定すると、クライアント認証が 5 回失敗した場合、指定された期間にわたってそのクライアントから受信する要求はすべて拒否されます。

（注） 認証失敗の原因が誤ったパスワードの入力である場合、クライアントは抑制されません。

表 *198 : RADIUS* 設定

フィールド	使用上のガイドライン
[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）]	
[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）]	同じ理由で繰り返し認証に失敗するクライアントを抑止するには、このチェックボックスをオンにします。これらのクライアントは監査ログに出力されず、また[繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）]オプションが有効な場合には、指定された期間にわたってこれらのクライアントからの要求が拒否されます。
[2 回の失敗を検出する期間（Detect Two Failures Within）]	分単位で時間間隔を入力します。クライアントがこの期間内に同じ理由で 2 回認証に失敗すると、監査ログに出力されず、また[繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] オプションが有効な場合には、指定された期間にわたってこのクライアントからの要求が拒否されます。
[失敗を報告する間隔（Report Failures Once Every）]	報告対象の認証失敗の時間間隔を分単位で入力します。たとえば、この値を 15 分に設定すると、繰り返し認証に失敗するクライアントが 15 分に 1 回だけ監査ログに報告されるため、報告の重複が防止されます。
[繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）]	認証が繰り返し失敗するクライアントからの RADIUS 要求を自動的に拒否するには、このチェック ボックスをオンにします。Cisco ISE による不要な処理を防ぎ、Denial of Service（DoS）攻撃から防御するには、このオプションを有効にします。

フィールド	使用上のガイドライン
[自動拒否前の失敗回数（Failures Prior to Automatic Rejection）]	認証失敗回数を入力します。認証失敗回数がこの値を超えると、繰り返し失敗するクライアントからの要求は自動的に拒否されます。設定されている期間（[要求を拒否する期間（Continue Rejecting Requests for）] で指定）にわたり、これらのクライアントから受信する要求はすべて自動的に拒否されます。この期間が経過した後では、これらのクライアントからの認証要求が処理されます。
[要求を拒否する期間（Continue Rejecting Requests for）]	繰り返し失敗するクライアントからの要求を拒否する時間間隔を分単位で入力します。
[繰り返し発生するアカウンティング更新を無視する期間（Ignore Repeated Accounting Updates Within）]	この期間内に繰り返し発生するアカウンティング更新は無視されます。
[成功レポートの抑制（Suppress Successful Reports）]	
繰り返される認証成功の抑制（Suppress Repeated Successful Authentications）	直近の 24 時間で、ID、ネットワーク デバイス、および許可のコンテキストに変更がない認証要求成功が繰り返し報告されないようにするには、このチェックボックスをオンにします。
[認証の詳細（Authentications Details）]	
[次よりも長いステップを強調表示（Highlight Steps Longer Than）]	ミリ秒単位で時間間隔を入力します。1つのステップの実行が指定のしきい値を超えると、認証詳細ページでそのステップがクロック アイコンでマークされます。
無効なユーザ名を開示する（Disclose Invalid Usernames）	このチェック ボックスをオンにすると、RADIUS ライブ ログに「USERNAME」または「INVALID」とラベル付けされたユーザ名が開示されます。認証概要レポートのように、RADIUS ライブ ログにもログイン済みのユーザ名を表示できます。このオプションは、30 分後に自動的に無効になります。
RADIUS UDP ポート	

フィールド	使用上のガイドライン
認証ポート（Authentication Port）	RADIUS UDP の認証フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1812 とポート 1645 が使用されます。値の範囲は 1024 ～ 65535 です。
アカウンティング ポート（Accounting Port）	RADIUS UDP のアカウンティング フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1813 とポート 1646 が使用されます。値の範囲は 1024 ～ 65535 です。 （注） これらのポートが他のサービスにより使用されていないことを確認します。
RADIUS DTLS	
認証およびアカウンティング ポート（Authentication and Accounting Port）	RADIUS DTLS の認証およびアカウンティング フローに使用するポートを指定します。デフォルトでは、ポート 2083 が使用されます。値の範囲は 1024 ～ 65535 です。 （注） このポートが他のサービスにより使用されていないことを確認します。
アイドル タイムアウト	パケットがネットワーク デバイスから届かなかったら、TLS セッションを終了する前に、Cisco ISE を待機する時間を秒単位で入力します。デフォルト値は 120 秒です。有効な範囲は 60 ～ 600 秒です。

フィールド	使用上のガイドライン
RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification）	Cisco ISE が DTLS ハンドシェイク中に RADIUS/DTLS クライアントの ID を確認するようにする場合は、このチェックボックスをオンにします。クライアント ID が有効でない場合、Cisco ISE はハンドシェイクに失敗します。デフォルトのネットワーク デバイスが設定されている場合、ID チェックはスキップされます。ID チェックは次の順序で実行されます。 1. クライアント証明書にサブジェクト代替名（SAN）属性が含まれている場合： • SAN に DNS 名が含まれている場合、証明書に指定されている DNS 名が Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。 • SAN に IP アドレスが含まれていて（DNS 名が含まれていない場合）、証明書で指定された IP アドレスが Cisco ISE で設定されているすべてのデバイス IP アドレスと比較されます。 2. 証明書に SAN が含まれていない場合、サブジェクト CN は Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。不一致の場合、Cisco ISE はハンドシェイクに失敗します。

関連トピック

ポリシー セット プロトコルの設定 （1046 ページ）
Cisco ISE の RADIUS プロトコルのサポート （1061 ページ）
RADIUS の設定 （1055 ページ）

一般 TrustSec の設定

Cisco ISE が TrustSec サーバとして機能したり、TrustSec サービスを提供したりするには、グローバル TrustSec 設定を定義します。次の表に、[TrustSec 設定（TrustSec Settings）] ウィンドウのフィールドの説明を示します（（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）]）。

TrustSec 展開の確認

このオプションを選択すると、すべてのネットワークデバイスに最新のTrustSecポリシーが展開されているかどうかを確認できます。Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合は [アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] および [ホーム（Home）] > [サマリ（Summary）]）にアラームが表示されます。TrustSec ダッシュ ボードに、以下のアラームが表示されます。

- 検証プロセスが開始または完了するたびに、[情報（Info）] アイコンとともにアラームが表示されます。
- 新しい展開要求により検証プロセスがキャンセルされた場合は、[情報（Info）] アイコンとともにアラームが表示されます。
- 検証プロセスがエラーで失敗した場合は、[警告（Warning）] アイコンとともにアラームが表示されます。たとえば、ネットワーク デバイスとの SSH 接続を開けない場合やネットワーク デバイスが使用できない場合、あるいは Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合などです。

[展開の検証（Verify Deployment）] オプションは、次のウィンドウでも使用できます。

- **[ワーク センター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティ グループ（Security Groups）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ ACL（Security Group ACLs）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [送信元ツリー（Source Tree）]**
- **[ワーク センター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [宛先ツリー（Destination Tree）]**

[すべての展開後に自動検証（Automatic Verification After Every Deploy）]：それぞれの展開後に、Cisco ISE ですべてのネットワーク デバイス上の更新を検証するには、このチェックボックスをオンにします。展開プロセスが完了したら、[展開プロセス後の時間（Time after Deploy Process）] フィールドに指定した時間が経過した後に、検証プロセスが開始されます。

[展開プロセス後の時間（Time after Deploy Process）]：展開プロセスが完了した後、検証プロセスを開始する前に Cisco ISE に待機させる時間を指定します。有効な範囲は、10 ～ 60 分です。

待機期間中に新しい展開が要求された場合や別の検証が進行中の場合は、現在の検証プロセスはキャンセルされます。

[今すぐ検証（Verify Now）]：検証プロセスをすぐに開始するには、このオプションをクリックします。

Protected Access Credential（PAC）

- [トンネル PAC の存続可能時間（Tunnel PAC Time to Live）]：

  PAC の有効期限を指定します。トンネル PAC は EAP-FAST プロトコル用のトンネルを生成します。時間を秒、分、時、日数、または週数で指定できます。デフォルト値は 90 日です。有効な範囲は次のとおりです。

  - 1 ～ 157680000 秒
  - 1 ～ 2628000 分
  - 1 ～ 43800 時間
  - 1 ～ 1825 日
  - 1 ～ 260 週間

- [プロアクティブ PAC 更新を次の後に実行する（Proactive PAC Update Will Occur After）]：Cisco ISE は、認証に成功した後、設定したパーセンテージのトンネル PAC TTL が残っているときに、新しい PAC をクライアントに予防的に提供します。PAC の期限が切れる前に最初の認証が正常に行われると、サーバはトンネル PAC の更新を開始します。このメカニズムにより、有効な PAC でクライアントが更新されます。デフォルト値は 10% です。

セキュリティグループタグ番号の割り当て

- [システムで SGT 番号を割り当てる（System will Assign SGT Numbers）]：Cisco ISE に SGT 番号を自動生成させる場合は、このオプションを選択します。
- [範囲内の番号を除外する（Except Numbers In range）]：手動設定用に SGT 番号の範囲を予約する場合は、このオプションを選択します。Cisco ISE は、SGT の生成時にこの範囲の数値を使用しません。
- [ユーザが手動で SGT 番号を入力する（User Must Enter SGT Numbers Manually）]：SGT 番号を手動で定義する場合は、このオプションを選択します。

APIC EPGのセキュリティグループタグのナンバリング（Security Group Tag Numbering for APIC EPGs）

[APIC EPG 用のセキュリティグループタグの番号付け（Security Group Tag Numbering for APIC EPGs）]：APIC から学習した EPG に基づいて SGT を作成する場合は、このチェックボックスをオンにし、使用する番号の範囲を指定します。

セキュリティグループの自動作成

[認証ルールを作成するときにセキュリティグループを自動作成する（Auto Create Security Groups When Creating Authorization Rules）]：認可ポリシーのルールを作成する際に SGT を自動的に作成する場合は、このチェックボックスをオンにします。

このオプションを選択した場合は、[認可ポリシー（Authorization Policy）] ウィンドウの上部に、「自動セキュリティグループの作成がオンです（Auto Security Group Creation is On）」というメッセージが表示されます。

自動作成された SGT は、ルール属性に基づいて命名されます。

（注） 自動作成された SGT は、それに対応する認可ポリシールールを削除しても削除されません。

デフォルトでは、新規インストールまたはアップグレードの後でこのオプションが無効になります。

- [自動命名オプション（Automatic Naming Options）]：自動作成される SGT の命名規則を定義するには、このオプションを使用します。

  （必須）[名前に次が含まれます（Name Will Include）]：次のオプションのいずれかを選択します。

  - **ルール名**
  - **SGT番号（SGT number）**
  - **ルール名およびSGT番号（Rule name and SGT number）**

  デフォルトでは、[ルール名（Rule name）] オプションが選択されます。

  オプションで、SGT 名に以下の情報を追加できます。

  - ポリシーセット名（Policy Set Name）（このオプションは [ポリシーセット（Policy Sets）] が有効な場合にのみ使用可能です）
  - プレフィックス（Prefix）（8 文字まで）
  - サフィックス（Suffix）（8 文字まで）

  Cisco ISE は、選択内容に応じて [サンプル名（Example Name）] フィールドにサンプル SGT 名を表示します。

  同じ名前の SGT が存在している場合、ISE は SGT 名に「*_x*」を付け加えます。*x* は（現在の名前に 1 が使用されていない場合は）1 から始まる最初の値です。新しい名前が 32 文字より長い場合、Cisco ISE によって最初の 32 文字に切り捨てられます。

ホスト名の IP SGT 静的マッピング

[ホスト名の IP SGT 静的マッピング（IP SGT Static Mapping of Hostnames）]：FQDN とホスト名が使用される場合、Cisco ISE はマッピングを展開して展開状態を検査する際に、PAN および PSN ノード内の対応する IP アドレスを検索します。DNS クエリによって返される IP アドレス用に作成されるマッピングの数を指定する場合は、このオプションを使用します。次のいずれかのオプションを選択できます。

- **DNS クエリによって返されるすべての IP アドレスに対してマッピングを作成する（Create mappings for all IP addresses returned by a DNS query）**
- **DNSクエリによって返される最初のIPv4アドレスおよび最初のIPv6アドレスに対してのみマッピングを作成する（Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query）**

関連トピック

TrustSec アーキテクチャ （1099 ページ）
TrustSec のコンポーネント （1100 ページ）
TrustSec のグローバル設定 （1107 ページ）

TrustSec マトリックスの設定

次の表に、[TrustSecマトリックスの設定（TrustSec Matrix Settings）] ページにある各フィールドの説明を示します。このページへのナビゲーション パスは、[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSecマトリックスの設定（TrustSec Matrix Settings）] です。

表 *199 : TrustSec* マトリックスの設定

フィールド	使用上のガイドライン
複数のSGACLを許可（Allow Multiple SGACLs）	セル内で複数のSGACLを許可するには、このチェックボックスをオンにします。このオプションが選択されていない場合、Cisco ISE はセル 1 つあたり 1 つの SGACL のみを許可します。 デフォルトでは、新たにインストールすると、このオプションはディセーブルになります。 アップグレード後、Cisco ISE は出力セルをスキャンし、複数の SGACL が割り当てられたセルを少なくとも 1 つ特定した場合、管理者に複数の SGACL をセルに追加することを許可します。それ以外の場合は、セル 1 つあたり 1 つの SGACL のみを許可します。 （注） 複数の SGACL を無効にする前に、複数の SGACL を含むセルを 1 つの SGACL のみを含めるように編集する必要があります。

フィールド	使用上のガイドライン
モニタリングの許可（Allow Monitoring）	マトリクス内のすべてのセルのモニタリングをイネーブルにする場合は、このチェックボックスをオンにします。モニタリングがディセーブルの場合、[セルの編集（Edit Cell）] ダイアログで、[すべてをモニタ（Monitor All）] アイコンはグレー表示され、[モニタ（Monitor）] オプションはディセーブルになります。 デフォルトでは、新たにインストールすると、モニタリングはディセーブルになります。 （注） マトリクス レベルでモニタリングをディセーブルにする前に、現在モニタされているセルのモニタリングをディセーブルにする必要があります。
SGT番号の表示（Show SGT Numbers）	マトリクス セルの SGT 値（10 進数および 16 進数の両方）を表示または非表示にするには、このオプションを使用します。 デフォルトでは、SGT 値はセルに表示されます。
アピアランス設定（Appearance Settings）	次のオプションを使用できます。 • [カスタム設定（Custom settings）] : デフォルトのテーマ（パターンなしの色）が最初に表示されます。独自の色とパターンを設定できます。 • [デフォルト設定（Default settings）] : パターンなしの色の定義済みリスト（編集不可）。 • [アクセシビリティ設定（Accessibility settings）] : パターンありの色の定義済みリスト（編集不可）。

フィールド	使用上のガイドライン
色/パターン（Color/Pattern）	マトリックスを読み取りやすくするために、セルの内容に基づいて、マトリックスセルに色とパターンを適用できます。 使用可能な表示タイプは、次のとおりです。 • [IPを許可/IPログを許可（Permit IP/Permit IP Log）]：セル内に設定されます • [IPを拒否/IPログを拒否（Deny IP/Deny IP Log）]：セル内に設定されます • [SGACL（SGACLs）]：セル内に設定されている SGACL 用 • [IPを許可/IPログを許可（継承）（Permit IP/Permit IP Log (Inherited)）]：デフォルト ポリシーから取得されます（設定されていないセル用） • [IPを拒否/IPログを拒否（継承）（Deny IP/Deny IP Log (Inherited)）]：デフォルト ポリシーから取得されます（設定されていないセル用） • [SGACL（継承）（SGACLs (Inherited)）]：デフォルトポリシーから取得されます（設定されていないセル用）

関連トピック

出力ポリシー （1125 ページ）
マトリクス ビュー （1126 ページ）
TrustSec マトリックスの設定 （1112 ページ）

SMS ゲートウェイ設定（SMS Gateway Settings）

電子メール サーバ経由でゲストとスポンサーに SMS メッセージを送信するように設定するには、次の設定を使用します。

表 *200 : SMS* 電子メール ゲートウェイの *SMS* ゲートウェイ設定

フィールド	使用上のガイドライン
SMS ゲートウェイ プロバイダー ドメイン（SMS Gateway Provider Domain）	プロバイダー ドメインと、ゲスト アカウントの携帯電話の番号を入力します。プロバイダーの SMS/MMS ゲートウェイにメッセージを送信するとき、前者が電子メール アドレスのホスト部として使用され、後者はユーザ部分として使用されます。
プロバイダー アカウント アドレス（Provider account address）	（オプション） アカウント アドレスを入力します。これは、電子メールの送信元アドレス（通常、アカウント アドレス）として使用され、**[ゲスト アクセス（Guest Access）] > [設定（Settings）]** の [デフォルトの電子メール アドレス（Default Email Address）] グローバル設定を上書きします。
SMTP API 宛先アドレス（SMTP API destination address）	（オプション） Clickatell SMTP API などの、特定のアカウント受信者アドレスを必要とする SMTP SMS API を使用する場合は、SMTP API 宛先アドレスを入力します。 これは、電子メールの送信先アドレスとして使用され、メッセージ本文のテンプレートはゲスト アカウントの携帯電話の番号に置き換えられます。
SMTP API 本文テンプレート（SMTP API body template）	（オプション） Clicketell SMTP API など、SMS の送信に特定の電子メール本文テンプレートを必要とする SMTP SMS API を使用する場合は、SMTP API 本文テンプレートを入力します。 サポートされる動的置換は $mobilenumber$、（形式 $YYYYMMDDHHHMISSmimi$ の）$timestamp$、および $message$ です。 URL に固有識別子が必要な SMS ゲートウェイには $timestamp$$mobilenumber$ を使用できます。

これらの設定へのナビゲーション パスは、**[ゲスト アクセス（Guest Access）] > [設定（Settings）] > [SMS ゲートウェイ（SMS Gateway）]** です。

HTTP API（GET 方式または POST 方式）でゲストとスポンサーに SMS メッセージを送信するように設定するには、次の設定を使用します。

表 *201 : SMS HTTP API* 用の *SMS* ゲートウェイ設定（*SMS Gateway Settings for SMS HTTP API*）

フィールド	使用上のガイドライン
URL	API の URL を入力します。 このフィールドは、符号化された URL ではありません。ゲスト アカウントの携帯電話の番号は、URL に置き換えられます。サポートされる動的置換は $mobilenumber$ および $message$ です。 HTTP API で HTTPS を使用した場合、HTTPS を URL 文字列に含め、Cisco ISE にプロバイダーの信頼できる証明書をアップロードします。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。
データ（URL エンコード部分）（Data (Url encoded portion)）	GET 要求または POST 要求のデータ（URL エンコード部分）を入力します。 このフィールドは、符号化された URL です。デフォルトの GET 方式を使用している場合、データが上で指定した URL に付加されます。
データ部分に HTTP POST 方式を使用（Use HTTP POST method for data portion）	POST 方式を使用する場合は、このオプションをオンにします。 上で指定したデータは、POST 要求の内容として使用されます。
HTTP POST データ コンテンツ タイプ（HTTP POST data content type）	POST 方式を使用する場合は、「plain/text」や「application/xml」などのコンテンツ タイプを指定します。
HTTPS ユーザ名（HTTPS Username） HTTPS パスワード（HTTPS Password） HTTPS ホスト名（HTTPS Host name） HTTPS ポート番号（HTTPS Port number）	この情報を入力します。

関連トピック

SMS プロバイダーおよびサービス （385 ページ）
ゲストに SMS 通知を送信するための SMS ゲートウェイの設定 （386 ページ）

DHCP および DNS サービス

これらの設定のためのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [DHCP および DNS サービス（DHCP & DNS Services）]** です。

認証 VLAN URL リダイレクトのシミュレーションを有効にするために、これらの設定を使用して、DHCP、およびオプションの DNS を設定します。さまざまな ISE ノードに適用するために、複数のスコープを作成できます。1 つの ISE ノードに複数のスコープを適用する場合、同じネットワーク インターフェイスで設定する必要があります。

（注） プロファイリングのために、DHCP プローブを必要とすることがあります。ISE DHCP プローブは認証 VLAN DHCP サービスと同じ UDP ポート 67 を使用します。そのため、DHCP プローブは、異なるインターフェイスで設定される必要があるか、またはこの ISE ノードで無効にすることができます。DHCP プローブの詳細については、DHCP プローブ （752 ページ）を参照してください。

表 *202 :* 認証 *VLAN URL* リダイレクトのシミュレーション用の *DHCP* と *DNS* サービスの設定

フィールド	使用上のガイドライン
スコープ名	このスコープの目的を容易に記憶できる名前を入力します。
ステータス	[有効（Enabled）] または [無効（Disabled）] を選択します。有効の場合、スコープは ISE ノードにのみ使用できます。
ISE ノード（ISE Node）	DHCP/DNS サーバとして機能するように ISE ノードを適用します。ドロップダウン リストから、このスコープを使用する ISE ノードを選択します。認証 VLAN は ISE ノード/ネットワーク インターフェイスごとに設定され、2 つのインターフェイスまたは 2 つのノードが同じ VLAN を共有することはできません。

フィールド	使用上のガイドライン
ネットワーク インターフェイス（Network Interface）	選択した ISE ノードで利用可能なネットワーク インターフェイスは、選択した ISE ノードに基づいて動的にこのドロップダウン リストに表示されます。認証 VLAN は ISE ノード/ネットワーク インターフェイスごとに設定され、2つのインターフェイスまたは2つのノードが同じVLANを共有することはできません。DHCP/DNS サーバがリスニングするインターフェイスを選択します。NAD の VLAN IP ヘルパーを設定することによって、複数のVLANが 1 つのネットワーク インターフェイス カードに接続される可能性があります。IPヘルパーの設定の詳細については、デバイス用のアドミニストレーション ガイドの指示を参照してください。
ドメイン名（Domain Name）	このスコープで使用する DHCP サーバのドメイン名を入力します。
DHCP アドレス範囲	ネットワーク定義に基づいて、このスコープに使用可能な DHCP アドレスの範囲を選択します。
サブネット マスク（Subnet mask）	ネットワーク定義に基づいて、このスコープに使用するネットワークマスクを選択します。
ネットワーク ID（Network ID）	入力した DHCP の属性に基づいて、Cisco ISE により自動的に決定されます。
除外アドレス範囲	ネットワーク定義に基づいて、このスコープに使用すべきでない DHCP アドレスの範囲を選択します。
デフォルト ゲートウェイ	デフォルト ゲートウェイの IP アドレスを入力します。
DHCP リース期間	DHCP リース期間を定義します。

フィールド	使用上のガイドライン
[DHCP オプション（DHCP options）]	これはオプションのフィールドです。 DHCP オプションは、DHCP サーバが DHCP クライアントに渡すことができる追加の設定パラメータです。DHCP オプションにより、ネットワークにアクセスするため、または最終認証前にデバイスをブートストラップする手段として、オプション値に指定されている情報を必要とするデバイス（カメラ、アクセス ポイント、電話）がサポートされます。DHCP サーバは、DHCP 要求メッセージをクライアントから受信すると、(通常）DHCP ACK パケットをクライアントに送信することで応答します。この時点で、サーバは DHCP ACK パケットで設定されているすべてのオプションを転送します。 詳細については、次の表の後に続く「DHCP オプション」の項を参照してください。
外部 DNS サーバ	すべての企業ネットワークにアクセスするための認証を受ける前に、ユーザが認証 VLAN 外の外部ドメインにアクセスできるようにする場合、外部 DNS 名を解決するために DNS サーバの IP アドレスを入力します。
外部ドメイン	すべての企業ネットワークにアクセスするための認証を受ける前に、ユーザが特定のサイトにアクセスできるようにする場合、これらのフィールドにそれらのサイトのドメイン名を入力します。 親ドメインとは別に、ユーザがアクセスする必要があるすべての子ドメインの名前を入力します。

DHCP オプション

ISE で DHCP サービスを設定すると、Auth VLAN に接続するクライアントに特定の DHCP オプションを割り当てることができます。定義する各範囲に複数の DHCP オプションを追加できます。

ドロップダウン リストで選択できるオプションは、RFC 2132 のものです。また、（RFC 2132 から）カスタマイズしたオプションを追加するには、ドロップダウン リストから [カスタム（Custom）] を選択し、オプション コードを入力します。

一般に、最もよく使用される DHCP オプションがいくつかあります。

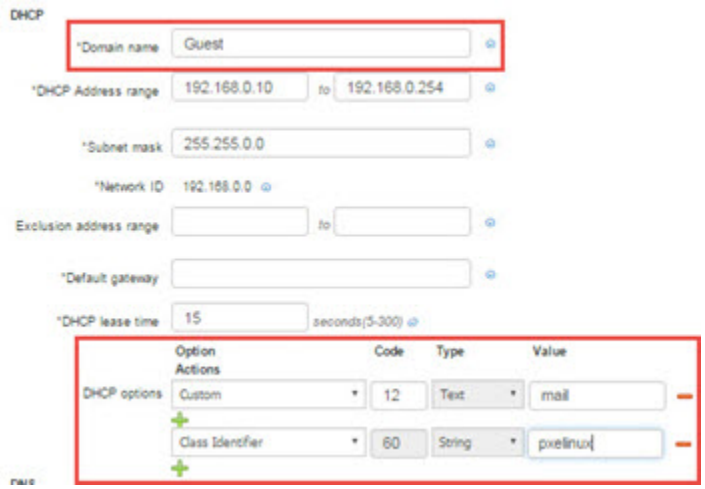
一般的なオプションとしては、次のようなものがあります。

- オプション 12（ホスト名）：ノードの完全修飾ドメイン名の「ホスト名」部分を渡すために使用されます。たとえば mail.ise.com の「mail」です。
- オプション 42（NTP サーバ）：ネットワークで使用される NTP サーバを渡します。
- オプション 66（TFTP サーバ）：IP アドレスまたはホスト名を渡すために使用されます。このオプションは、ドロップダウンリストから選択できます。
- オプション 82（DHCP リレー エージェント）：サーバ側 DHCP リレー サーバ情報のその他のサブオプションを渡すために使用されます。

オプション値を定義するには、ドロップダウン リストからオプションを選択します。事前定義の**オプション**を選択すると、コードとタイプが自動的に取り込まれます。

[カスタム（Custom）] を選択して**コード**を入力すると、[タイプ（Type）] が自動的に更新されます。オプションの値を入力します。

図 *71 : DHCP* オプション



次に例を示します。

- ホスト名の設定：[オプション（Option）] から [カスタム（Custom）] を選択します。[コード（Code）] に 15 と入力します。[タイプ（Type）] が自動的に [テキスト（Text）] に更新されます。[値（Value）] にホスト名（mail.ise.com の「mail」など）を入力します。
- TFTP サーバ名の設定：[オプション（Option）] から [TFTP サーバ名（TFTP Server Name）] を選択します。[コード（Code）] と [タイプ（Type）] がそれぞれ自動的に更新されます。[値（Value）] に TFTP サーバのホスト名を入力します。

（注） 一部の DHCP オプションは、ISE に対して自動的に定義されているため、手動で入力できません。たとえばオプション 15（ドメイン名）はカスタム オプションとして定義できません。これは、DHCP ドメイン名は、この画面で必須フィールドとして定義されており、上書きできないためです。

複数のオプションを入力するには、[アクション（Actions）]の下のプラス記号をクリックします。

関連トピック

Cisco ISE でのサードパーティ ネットワーク デバイスのサポート （910 ページ）
Cisco ISE でのサードパーティ製ネットワーク デバイスの設定 （915 ページ）
DHCP プローブ （752 ページ）

ID の管理

これらのページは、Cisco ISE の ID を設定し、管理することができます。

エンドポイント

これらのページでは、ネットワークに接続するエンドポイントを設定および管理することができます。

エンドポイント設定

次の表に、エンドポイントを作成し、エンドポイントにポリシーを割り当てるために使用できる [エンドポイント（Endpoints）] ページのフィールドを示します。このページへのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]** です。

表 *203* : エンドポイント設定

フィールド	使用上のガイドライン
MAC アドレス（MAC Address）	エンドポイントを静的に作成するには、MAC アドレスを 16 進数形式で入力します。 MAC アドレスは、Cisco ISE 対応のネットワークに接続するインターフェイスのデバイス ID です。

フィールド	使用上のガイドライン
スタティック割り当て（Static Assignment）	[エンドポイント（Endpoints）] ページでエンドポイントを静的に作成する場合このチェックボックスをオンにすると、静的割り当てのステータスが static に設定されます。 エンドポイントのスタティック割り当てのステータスを静的から動的に、または動的から静的に切り替えできます。
ポリシー割り当て	（スタティック割り当てが選択されていない限り、デフォルトで無効）[ポリシー割り当て（Policy Assignment）] ドロップダウン リストから一致するエンドポイント ポリシーを選択します。 次のいずれかを実行できます。 • 一致するエンドポイント ポリシーを選択しないで、デフォルトのエンドポイント ポリシーである不明を使用する場合、スタティック割り当てステータスはエンドポイントに対して動的に設定され、それにより、エンドポイントの動的プロファイリングが可能になります。 • 不明ではなく、一致するエンドポイント ポリシーを選択する場合、スタティック割り当てステータスはそのエンドポイントに対して静的に設定され、[スタティック割り当て（Static Assignment）] チェックボックスが自動的にオンにされます。

フィールド	使用上のガイドライン
スタティック グループ割り当て（Static Group Assignment）	（[スタティック グループ割り当て（Static Group Assignment）] が選択されていない限り、デフォルトで無効）エンドポイントを ID グループに静的に割り当てる場合、このチェックボックスをオンにします。 このチェックボックスをオンにした場合、プロファイリング サービスは、前に他のエンドポイント ID グループに動的に割り当てられたエンドポイントの次のエンドポイント ポリシーの評価時に、そのエンドポイント ID グループを変更しません。 このチェックボックスをオフにした場合、エンドポイント ID グループは、ポリシー設定に基づいて ISE プロファイラにより割り当てられたダイナミック グループです。[スタティック グループ割り当て（Static Group Assignment）] オプションを選択しない場合、エンドポイントは、エンドポイント ポリシーの次回評価時に一致する ID グループに自動的に割り当てられます。

フィールド	使用上のガイドライン

ID グループ割り当て	エンドポイントを割り当てるエンドポイント ID グループを選択します。
	
	エンドポイントを静的に作成する場合、またはエンドポイントのエンドポイント ポリシーの評価時に [一致する ID グループの作成（Create Matching Identity Group）] オプションを使用しない場合は、エンドポイントを ID グループに割り当てることができます。
	
	Cisco ISE には、次のシステムによって作成された次のエンドポイント ID グループがあります。
	• ブラックリスト
	• GuestEndpoints
	• プロファイル済み
	  • Cisco IP-Phone
	  • ワークステーション
	• RegisteredDevices
	• 不明

関連トピック

識別されたエンドポイント （822 ページ）

ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 （816 ページ）

エンドポイントの、LDAP からのインポートの設定

次の表では、LDAP サーバからのエンドポイントのインポートに使用できる [LDAP からのインポート（Import from LDAP）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** です。

表 *204* : エンドポイントの、*LDAP* からのインポートの設定

フィールド	使用上のガイドライン
接続の設定	
ホスト	LDAP サーバのホスト名または IP アドレスを入力します。

フィールド	使用上のガイドライン
[ポート（Port）]	LDAP サーバのポート番号を入力します。デフォルト ポート 389 を使用して LDAP サーバからインポートするか、デフォルトポート 636 を使用して SSL を介して LDAP サーバからインポートできます。 （注） Cisco ISE では、任意の設定済みポート番号をサポートします。設定済みの値は、LDAP サーバ接続詳細に一致する必要があります。
セキュア接続を有効にする（Enable Secure Connection）	SSL を介して LDAP サーバからインポートするには、[セキュア接続を有効にする（Enable Secure Connection）] チェックボックスをオンにします。
ルート CA 証明書名	ドロップダウン矢印をクリックして、信頼できる CA 証明書を表示します。 ルート CA 証明書名は、LDAP サーバに接続する場合に必要となる信頼できる CA 証明書を指します。Cisco ISE 内の CA 証明書は、追加（インポート）、編集、削除、およびエクスポートが可能です。
匿名バインド（Anonymous Bind）	匿名バインドを有効にするには、[匿名バインド（Anonymous Bind）] チェックボックスをオンにします。 [匿名バインド（Anonymous Bind）] チェックボックスをオンにするか、または slapd.conf コンフィギュレーション ファイルの LDAP 管理者クレデンシャルを入力する必要があります。
管理者 DN（Admin DN）	slapd.conf コンフィギュレーション ファイルで LDAP 管理者に設定されている識別名（DN）を入力します。 管理者 DN フォーマット例：cn=Admin, dc=cisco.com, dc=com
[パスワード（Password）]	LDAP 管理者に設定されたパスワードを slapd.conf コンフィギュレーション ファイルに入力します。

フィールド	使用上のガイドライン
ベース DN（Base DN）	親エントリの認定者名を入力します。 ベース DN フォーマット例：dc=cisco.com, dc=com
クエリ設定（Query Settings）	
MAC アドレス objectClass（MAC Address objectClass）	MACアドレスのインポートに使用するクエリフィルタを入力します。たとえば、ieee802Device です。
MAC アドレス属性名（MAC Address Attribute Name）	インポートに対して返される属性名を入力します。たとえば、macAddress です。
プロファイル属性名（Profile Attribute Name）	LDAP 属性の名前を入力します。この属性は、LDAP サーバで定義されている各エンドポイント エントリのポリシー名を保持します。 [プロファイル属性名（Profile Attribute Name）] フィールドを設定する場合は、次の点を考慮してください。 • [プロファイル属性名（Profile Attribute Name）] フィールドでこの LDAP 属性を指定しない場合、またはこの属性を誤って設定した場合、インポート操作時にエンドポイントは「不明」としてマークされ、これらのエンドポイントは一致するエンドポイント プロファイリング ポリシーに個別にプロファイリングされます。 • [プロファイル属性名（Profile Attribute Name）] フィールドで LDAP 属性を設定した場合、その属性値は、エンドポイント ポリシーが Cisco ISE 内の既存のポリシーに一致することを確認するために検証され、エンドポイントがインポートされます。エンドポイント ポリシーが既存のポリシーと一致しない場合、それらのエンドポイントはインポートされません。
タイムアウト（秒）（Time Out [seconds]）	時間を秒単位（1 ～ 60 秒）で入力します。

関連トピック

識別されたエンドポイント （822 ページ）
LDAP サーバからのエンドポイントのインポート （821 ページ）

グループ

これらのページでは、エンドポイント ID グループを設定および管理することができます。

エンドポイント ID グループの設定

次の表に、エンドポイント グループを作成するために使用できる [エンドポイント ID グループ（Endpoint Identity Groups）] ページのフィールドを示します。このページへのナビゲーション パスは、[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）] です。

表 *205* : エンドポイント *ID* グループの設定

フィールド	使用上のガイドライン
名前（Name）	作成するエンドポイント ID グループの名前を入力します。
説明	作成するエンドポイント ID グループの説明を入力します。
親グループ（Parent Group）	新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを、[親グループ（Parent Group）] ドロップダウン リストから選択します。

関連トピック

識別されたエンドポイントの、エンドポイント ID グループでのグループ化 （825 ページ）
エンドポイント ID グループの作成 （825 ページ）

外部 ID ソース

これらのページでは、Cisco ISE が認証および認可に使用するユーザ データが含まれる外部 ID ソースを設定および管理することができます。

LDAP ID ソースの設定

次の表では、[LDAP ID ソース（LDAP Identity Sources）] ページのフィールドについて説明します。これらのフィールドを使用して LDAP インスタンスを作成し、これに接続します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** です。

LDAP 一般設定

以下の表では、[一般（General）] タブのフィールドについて説明します。

表 *206 : LDAP* 一般設定

フィールド	使用上のガイドライン
名前（Name）	LDAP インスタンスの名前を入力します。この値は、サブジェクト DN および属性を取得するために検索で使用されます。この値は string 型で、最大長は 64 文字です。
説明（Description）	LDAP インスタンスの説明を入力します。この値は string 型で、最大長は 1024 文字です。
スキーマ（Schema）	次の組み込みのスキーマ タイプのいずれかを選択するか、カスタム スキーマを作成できます。 • Active Directory • Sun Directory Server • Novell eDirectory [スキーマ（Schema）] の隣の矢印をクリックすると、スキーマの詳細を表示できます。 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。
（注）　次のフィールドは、カスタム スキーマを選択した場合にのみ編集できます。	
サブジェクト オブジェクト クラス（Subject Objectclass）	サブジェクト DN および属性を取得するために検索で使用する値を入力します。この値は string 型で、最大長は 256 文字です。
サブジェクト名属性（Subject Name Attribute）	要求内のユーザ名を含む属性の名前を入力します。この値は string 型で、最大長は 256 文字です。
グループ名属性（Group Name Attribute）	[グループ名属性（Group Name Attribute）] フィールドに CN または DN またはサポートされる属性を入力します。 • CN：共通名に基づいて LDAP ID ストア グループを取得します。 • DN：識別名に基づいて LDAP ID ストア グループを取得します。

フィールド	使用上のガイドライン
証明書属性（Certificate Attribute）	証明書定義を含む属性を入力します。証明書ベースの認証の場合、クライアントによって提示された証明書を検証するために、これらの定義が使用されます。
グループ オブジェクト クラス（Group Objectclass）	グループとして認識されるオブジェクトを指定するために、検索に使用する値を入力します。この値は string 型で、最大長は 256 文字です。
グループ マップ属性（Group Map Attribute）	マッピング情報を含む属性を指定します。この属性は、選択した参照方向に基づいて、ユーザまたはグループ属性を指定できます。
サブジェクト オブジェクトにグループへの参照が含まれる（Subject Objects Contain Reference To Groups）	所属するグループを指定する属性がサブジェクト オブジェクトに含まれている場合は、このオプション ボタンをクリックします。
グループ オブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）	サブジェクトを指定する属性がグループ オブジェクトに含まれている場合は、このオプション ボタンをクリックします。この値はデフォルト値です。
グループ内のサブジェクトをメンバー属性に保存（Subjects In Groups Are Stored In Member Attribute As）	（[グループ オブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）] オプション ボタンの選択時に限り使用可能）グループ メンバー属性にメンバーが供給される方法を指定します（デフォルトは DN）。

フィールド	使用上のガイドライン
ユーザ情報属性（User Info Attributes）	デフォルトでは、事前設定された属性が次の組み込みのスキーマタイプのユーザ情報（名、姓、電子メール、電話、地域など）を収集するために使用されます。 • Active Directory • Sun Directory Server • Novell eDirectory 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。 [スキーマ（Schema）] ドロップダウン リストから [カスタム（Custom）] オプションを選択し、要件に基づいてユーザ情報の属性を編集することもできます。

LDAP の接続設定

以下の表では、[接続設定（Connection Settings）] タブのフィールドについて説明します。

表 *207 : LDAP* の接続設定

フィールド	使用上のガイドライン
セカンダリ サーバの有効化（Enable Secondary Server）	プライマリ LDAP サーバに障害が発生した場合にバックアップとして使用するセカンダリ LDAP サーバを有効にする場合は、このオプションをオンにします。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバの設定パラメータを入力する必要があります。
プライマリ サーバとセカンダリ サーバ（Primary and Secondary Servers）	
ホスト名/IP（Hostname/IP）	LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。

フィールド	使用上のガイドライン
ポート（Port）	LDAP サーバがリッスンしている TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバの管理者からポート番号を取得できます。
各 ISE ノードのサーバの指定（Specify server for each ISE node）	プライマリおよびセカンダリ LDAP サーバの hostnames/IP および各 PSN のポートを設定するには、このチェック ボックスをオンにします。 このオプションを有効にすると、導入のすべてのノードを表示するテーブルが表示されます。ノードを選択し、プライマリおよびセカンダリ LDAP サーバの hostname/IP および選択したノードのポートを設定する必要があります。
アクセス（Access）	[匿名アクセス（Anonymous Access）]：LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバではクライアントが区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへの、クライアント読み取りアクセスが許可されます。認証情報をサーバに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。 [認証されたアクセス（Authenticated Access）]：LDAP ディレクトリの検索が管理クレデンシャルによって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。

フィールド	使用上のガイドライン
管理者 DN（Admin DN）	管理者の DN を入力します。管理者 DN は、[ユーザ ディレクトリ サブツリー（User Directory Subtree）] 下のすべての必要なユーザの検索およびグループの検索を行う権限を持つ LDAP アカウントです。指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、該当 LDAP サーバで認証されたユーザのグループ マッピングは失敗します。
パスワード（Password）	LDAP 管理者アカウントのパスワードを入力します。
セキュアな認証（Secure Authentication）	SSL を使用して Cisco ISE とプライマリ LDAP サーバ間の通信を暗号化する場合にクリックします。[ポート（Port）] フィールドに LDAP サーバでの SSL に使用されるポート番号が入力されていることを確認します。このオプションを有効にした場合は、ルート CA を選択する必要があります。
LDAP サーバのルート CA（LDAP Server Root CA）	ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証を有効にします。
サーバ タイムアウト（Server timeout）	プライマリ LDAP サーバでの接続または認証が失敗したと判断する前に Cisco ISE がプライマリ LDAP サーバからの応答を待つ秒数を入力します。有効な値は 1 ～ 99 です。デフォルトは 10 です。
最大管理接続（Max. Admin Connections）	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、ユーザ ディレクトリ サブツリーおよびグループ ディレクトリ サブツリーの下にあるユーザおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です。デフォルトは 20 です。
N 秒ごとに再接続（Force reconnect every N seconds）	このチェック ボックスをオンにし、2 つ目のテキスト ボックスに、サーバを指定された間隔で LDAP 接続を更新するための適切な値を入力します。有効な範囲は 1 ～ 60 分です。

フィールド	使用上のガイドライン
サーバへのバインドをテスト（Test Bind To Server）	LDAP サーバの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバの詳細を編集して再テストします。
フェールオーバー	
常にプライマリ サーバに最初にアクセスする（Always Access Primary Server First）	Cisco ISE の認証と認可のために常にプライマリ LDAP サーバに最初にアクセスするように設定するには、このオプションをクリックします。
経過後にプライマリ サーバにフェールバック（Failback to Primary Server After）	Cisco ISE で接続しようとしたプライマリ LDAP サーバが到達不可能な場合、Cisco ISE はセカンダリ LDAP サーバへの接続を試行します。Cisco ISE に再びプライマリ LDAP サーバを使用するように設定するには、このオプションをクリックし、テキスト ボックスに値を入力します。

[LDAP] の [ディレクトリ構成（Directory Organization）] タブ

次の表では、[ディレクトリ構成（Directory Organization）] タブのフィールドについて説明します。

表 *208 : [LDAP] の [ディレクトリ構成（Directory Organization）] タブ*

フィールド	使用上のガイドライン
サブジェクト検索ベース（Subject Search Base）	すべてのサブジェクトを含むサブツリーの DN を入力します。次に例を示します。 o=corporation.com サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

フィールド	使用上のガイドライン
グループ検索ベース（Group Search Base）	すべてのグループを含むサブツリーの DN を入力します。次に例を示します。 ou = 組織ユニット、ou = 次の組織ユニット、o = corporation.com グループを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。
形式での MAC アドレスの検索（Search for MAC Address in Format）	LDAPデータベースでの検索に使用する、Cisco ISE の MAC アドレス形式を入力します。内部 ID ソースの MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で供給されます。LDAPデータベースのMACアドレスは、異なる形式で供給できます。ただし、Cisco ISE でホスト ルックアップ要求が受信されると、MACアドレスは内部形式からこのフィールドで指定した形式に変換されます。 ドロップダウン リストを使用して、特定の形式でのMACアドレスの検索を有効にします。<*format*> は次のいずれかです。 • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 選択する形式は、LDAP サーバに供給されているMACアドレスの形式と一致している必要があります。

フィールド	使用上のガイドライン
サブジェクト名の先頭から最後に出現する区切り文字まで削除（Strip start of subject name up to the last occurrence of the separator）	ユーザ名からドメインプレフィックスを削除するための適切なテキストを入力します。 ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、そのユーザ名の初めから区切り文字までのすべての文字が削除されます。ユーザ名に、<start_string> ボックスに指定した文字が複数含まれている場合は、Cisco ISE によって最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザ名が DOMAIN\user1 である場合、Cisco ISE によって user1 が LDAP サーバに送信されます。 （注） <start_string> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。
最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip end of subject name from the first occurrence of the separator）	ユーザ名からドメイン サフィックスを削除するための適切なテキストを入力します。 ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、その区切り文字からユーザ名の末尾までのすべての文字が削除されます。ユーザ名に、このフィールドに指定した文字が複数含まれている場合は、Cisco ISE によって最初の区切り文字から文字が削除されます。たとえば、区切り文字が@で、ユーザ名が *user1@domain* であれば、Cisco ISE は *user1* を LDAP サーバに送信します。 （注） *<end_string>* ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。

LDAP グループ設定

表 *209 : LDAP* グループ設定

フィールド	使用上のガイドライン
追加（Add）	[追加（Add）] > [グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）] を選択して LDAP ディレクトリからグループを選択します。 グループの追加を選択した場合は、新しいグループの名前を入力します。ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。選択したグループが [グループ（Groups）] ページに表示されます。

LDAP 属性設定

表 *210 : LDAP* 属性設定

フィールド	使用上のガイドライン
追加（Add）	[追加（Add）] > [属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）] を選択して LDAP サーバから属性を選択します。 属性を追加する場合は、新しい属性の名前を入力します。ディレクトリから選択する場合は、ユーザ名を入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザの属性を取得します。選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

LDAP 詳細設定

以下の表では、[詳細設定（Advanced Settings）] タブのフィールドについて説明します。

表 *211 : LDAP* 詳細設定

フィールド	使用上のガイドライン
[パスワードの変更を有効にする（Enable password change）]	デバイス管理に PAP プロトコルを使用し、ネットワーク アクセスに RADIUS EAP-GTC プロトコルを使用している場合に、パスワードが期限切れになるか、またはパスワードがリセットされるときに、ユーザがパスワードを変更できるようにするには、このチェックボックスをオンにします。サポートされていないプロトコルでは、ユーザ認証が失敗します。このオプションでは、ユーザが次回のログイン時にパスワードを変更できるようにすることもできます。

関連トピック

LDAP ディレクトリ サービス （696 ページ）
LDAP ユーザ認証 （697 ページ）
LDAP ユーザ ルックアップ （702 ページ）
LDAP ID ソースの追加 （703 ページ）

RADIUS トークン ID ソースの設定

次の表では、RADIUS 外部 ID ソースを設定し、それに接続するために使用できる [RADIUS トークン ID ソース（RADIUS Token Identity Sources）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）]** です。

表 *212 : RADIUS* トークン *ID* ソースの設定

フィールド	使用上のガイドライン
名前（Name）	RADIUS トークン サーバの名前を入力します。許容最大文字数は 64 文字です。
説明	RADIUS トークン サーバの説明を入力します。最大文字数は 1024 です。
SafeWord サーバ（SafeWord Server）	RADIUS ID ソースが SafeWord サーバである場合はこのチェックボックスをオンにします。

フィールド	使用上のガイドライン
セカンダリ サーバの有効化（Enable Secondary Server）	プライマリに障害が発生した場合にバックアップとして使用する Cisco ISE のセカンダリ RADIUS トークン サーバを有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにする場合は、セカンダリ RADIUS トークン サーバを設定する必要があります。
常にプライマリ サーバに最初にアクセスする（Always Access Primary Server First）	Cisco ISE が常にプライマリ サーバに最初にアクセスするには、このオプション ボタンをクリックします。
経過後にプライマリ サーバにフォールバック（Fallback to Primary Server after）	プライマリ サーバに到達できない場合に Cisco ISE がセカンダリ RADIUS トークン サーバを使用して認証できる時間（分単位）を指定するには、このオプション ボタンをクリックします。この時間を過ぎると、Cisco ISE はプライマリ サーバに対する認証を再試行します。
プライマリ サーバ（Primary Server）	
ホスト名/アドレス（Host IP）	プライマリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。
共有秘密鍵（Shared Secret）	この接続のプライマリ RADIUS トークン サーバで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	プライマリ RADIUS トークン サーバが受信しているポート番号を入力します。
サーバ タイムアウト（Server timeout）	プライマリ サーバがダウンしていると判断する前に Cisco ISE がプライマリ RADIUS トークン サーバからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	セカンダリ サーバ（定義されている場合）に移動する前、またはセカンダリ サーバが定義されていない場合は要求をドロップする前に、Cisco ISE がプライマリ サーバへの再接続を試行する回数を指定します。
セカンダリ サーバ（Secondary Server）	

フィールド	使用上のガイドライン
ホスト名/アドレス（Host IP）	セカンダリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。
共有秘密鍵（Shared Secret）	この接続のセカンダリ RADIUS トークン サーバで設定されている共有秘密を入力します。
認証ポート（Authentication Port）	セカンダリ RADIUS トークン サーバが受信しているポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは 1812 です。
サーバ タイムアウト（Server timeout）	セカンダリ サーバがダウンしていると判断する前に Cisco ISE がセカンダリ RADIUS トークン サーバからの応答を待つ時間（秒単位）を指定します。
接続試行回数（Connection Attempts）	要求をドロップする前に Cisco ISE がセカンダリ サーバへの再接続を試行する回数を指定します。

関連トピック

RADIUS トークン ID ソース （722 ページ）
RADIUS トークン サーバの追加 （728 ページ）

RSA SecurID ID ソースの設定

次の表では、RSA SecurID ID ソースを作成し、それに接続するために使用できる [RSA SecurID ID ソース（RSA SecurID Identity Sources）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[RSA SecurID]** です。

RSA プロンプトの設定

次の表では、[RSA プロンプト（RSA Prompts）] タブ内のフィールドについて説明します。

表 *213 : RSA* プロンプトの設定

フィールド	使用上のガイドライン
パスコード プロンプトの入力（Enter Passcode Prompt）	パス コードを取得するテキスト文字列を入力します。
次のトークン コードの入力（Enter Next Token Code）	次のトークンを要求するテキスト文字列を入力します。

フィールド	使用上のガイドライン
PIN タイプの選択（Choose PIN Type）	PIN タイプを要求するテキスト文字列を入力します。
システム PIN の受け入れ（Accept System PIN）	システム生成の PIN を受け付けるテキスト文字列を入力します。
英数字 PIN の入力（Enter Alphanumeric PIN）	英数字 PIN を要求するテキスト文字列を入力します。
数値 PIN の入力（Enter Numeric PIN）	数値 PIN を要求するテキスト文字列を入力します。
PIN の再入力（Re-enter PIN）	ユーザに PIN の再入力を要求するテキスト文字列を入力します。

RSA メッセージ設定（RSA Message Settings）

次の表では、[RSA メッセージ（RSA Messages）] タブ内のフィールドについて説明します。

表 *214 : RSA* メッセージ設定（*RSA Messages Settings*）

フィールド	使用上のガイドライン
システム PIN メッセージの表示（Display System PIN Message）	システム PIN メッセージのラベルにするテキスト文字列を入力します。
システム PIN 通知の表示（Display System PIN Reminder）	ユーザに新しい PIN を覚えるように通知するテキスト文字列を入力します。
数字を入力する必要があるエラー（Must Enter Numeric Error）	PIN には数字のみを入力するようにユーザに指示するメッセージを入力します。
英数字を入力する必要があるエラー（Must Enter Alpha Error）	PIN には英数字のみを入力するようにユーザに指示するメッセージを入力します。
PIN 受け入れメッセージ（PIN Accepted Message）	ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
PIN 拒否メッセージ（PIN Rejected Message）	ユーザの PIN がシステムによって拒否されたときに表示されるメッセージを入力します。
ユーザの PIN が異なるエラー（User Pins Differ Error）	ユーザが不正な PIN を入力したときに表示されるメッセージを入力します。

フィールド	使用上のガイドライン
システム PIN 受け入れメッセージ（System PIN Accepted Message）	ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
不正パスワード長エラー（Bad Password Length Error）	ユーザが指定した PIN が、PIN 長ポリシーで指定されている範囲に収まらない場合に表示されるメッセージを入力します。

関連トピック

RSA ID ソース （730 ページ）
Cisco ISE と RSA SecurID サーバの統合 （730 ページ）
RSA ID ソースの追加 （734 ページ）

ネットワーク リソース

ネットワーク デバイス

これらのページを使用すると、ネットワーク デバイスを追加し、管理することができます。

（注） IPv4 および IPv6 は、ネットワーク デバイス（TACACS および RADIUS）設定および外部 RADIUS サーバ設定でサポートされるようになりました。IPv4 アドレスを入力する場合は、範囲とサブネット マスクを使用できます。IPv6 では、範囲がサポートされていません。

ネットワーク デバイス定義の設定

次の表は、Cisco ISE のネットワーク アクセス デバイスを設定するために使用できる [ネットワーク デバイス（Network Devices）] ページのフィールドについて説明しています。このページへのナビゲーション パスは、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]** です。

ネットワーク デバイスの設定

次の表に、[ネットワーク デバイス（Network Device）] セクションのフィールドを示します。

表 *215 :* ネットワーク デバイスの設定

フィールド	説明
Name	ネットワーク デバイスの名前を入力します。 ネットワーク デバイスに、デバイスのホスト名とは異なるわかりやすい名前を指定できます。デバイス名は論理識別子です。 （注） 一度設定したデバイスの名前は編集できません。
説明	デバイスの説明を入力します。

フィールド	説明
IP アドレス/IP 範囲（IP Address/IP Ranges）	次のいずれかを実行します。 • [IP アドレス（IP Address）]：単一の IP アドレス（IPv4 または IPv6 アドレス）とサブネット マスクを入力します。 • [IP 範囲（IP Ranges）]：必要な IPv4 アドレス範囲を入力します。[除外（Exclude）] テキスト ボックスに IP アドレスまたは IP アドレス範囲を入力して、認証時に IP アドレスを除外することもできます。 IP アドレスとサブネットマスクまたは IP アドレス範囲を定義するときに従う必要があるガイドラインを次に示します。 • 特定の IP アドレスを定義するか、サブネット マスクを使用して範囲を定義できます。デバイス A の IP アドレス範囲が定義されている場合、デバイス A に定義されている範囲の個別のアドレスを別のデバイス B に設定できます。 • すべてのオクテットの IP アドレス範囲を定義できます。IP アドレスの範囲を指定するときに、ハイフン（-）またはアスタリスク（*）をワイルドカードとして使用できます。たとえば、*.*.*.*、1-10.1-10.1-10.1-10 または 10-11.*.5.10-15 などです。 • サブセットがすでに追加されている場合には、設定された範囲からその IP アドレス範囲のサブセットを除外できます。たとえば、10.197.65.*/10.197.65.1 または 10.197.65.* exclude 10.197.65.1 などです。 • 同じ IP アドレスを持つ 2 台のデバイスを定義することはできません。 • 同じ IP 範囲を持つ 2 台のデバイスを定義することはできません。IP 範囲は、一部または全部が重複することはできません。

フィールド	説明
デバイスタイプ（**Device Type**）	ドロップダウン リストをクリックして、ネットワーク デバイスのベンダーを選択します。 ドロップダウン リストの横にあるツールのヒントを使用して、選択したベンダーのネットワーク デバイスがサポートしているフローおよびサービスと、デバイスで使用されている RADIUS CoA ポートと URL リダイレクトのタイプを表示できます。これらの属性は、デバイス タイプのネットワーク デバイス プロファイルで定義されます。
モデル名（**Model Name**）	ドロップダウン リストをクリックして、デバイス モデルなどを選択します。 モデル名は、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性は、デバイスディクショナリにあります。
ソフトウェア バージョン（**Software Version**）	ドロップダウン リストをクリックして、ネットワーク デバイスで実行するソフトウェアのバージョンを選択します。 ソフトウェア バージョンは、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性は、デバイス ディクショナリにあります。
ネットワーク デバイス グループ（**Network Device Group**）	[ロケーション（Location）] および [デバイス タイプ（Device Type）] ドロップダウン リストをクリックし、ネットワーク デバイスに関連付けることができるロケーションとデバイス タイプを選択します。 グループを設定するときに、明確にデバイスをグループに割り当てないと、そのデバイスはデフォルトのデバイス グループ（ルート NDG）に含まれます。これにより、ロケーションはすべてのロケーション、デバイス タイプはすべてのデバイス タイプとなり、デフォルトのデバイス グループ（ルート NDG）が割り当てられます。たとえば、すべてのロケーションとすべてのデバイス グループなどです。

RADIUS 認証設定

次の表では、[RADIUS 認証設定（RADIUS Authentication Settings）] セクションのフィールドについて説明します。

表 *216 : RADIUS* 認証設定

フィールド	使用上のガイドライン
RADIUS UDP の設定	
Protocol	選択したプロトコルとして RADIUS を表示します。
共有秘密鍵（Shared Secret）	ネットワーク デバイスの共有秘密鍵を入力します。 共有秘密鍵は、**pac** オプションを指定した **radius-host** コマンドを使用してネットワーク デバイスに設定したキーです。 （注） 共有秘密鍵の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ページの [RADIUS 共有秘密鍵の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります（[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] > [デバイス セキュリティ設定（Device Security Settings）]）。 RADIUS サーバでのベスト プラクティスは、22 文字にすることです。新規インストールとアップグレードした展開の場合、デフォルトではこの値は 4 文字であることに注意してください。この値は[デバイスセキュリティ設定（Device Security Settings）] ページで変更できます。

フィールド	使用上のガイドライン
2 番目の共有秘密の使用	ネットワーク デバイスと Cisco ISE で使用される 2 つの共有秘密（鍵）を指定します。 （注） TrustSec デバイスには、デュアル共有秘密（鍵）の利点がありますが、Cisco ISE により送信される TrustSec CoA パケットは常に最初の共有秘密（鍵）を使用します。2 番目の共有秘密の使用を有効にするには、TrustSec デバイスに送信される必要のある TrustSec CoA パケットの送信元の ISE ノードを、**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [TrustSecの詳細設定（Advanced TrustSec Settings）]** ページの [送信元（Send From）] ドロップダウン リストから選択する必要があります。PAN または PSN ノードを選択できます。選択した PSN ノードがダウンした場合、PAN を使用して TrustSec デバイスに TrustSec CoA パケットが送信されます。 （注） RADIUS アクセス要求の 2 番目の共有秘密機能は、Message-Authenticator フィールドを含むパケットに対してのみ機能します。

フィールド	使用上のガイドライン
CoA ポート（CoA Port）	RADIUS CoA に使用するポートを指定します。 デバイスのデフォルトの CoA ポートはネットワーク デバイス プロファイルで定義されます。 （注） [RADIUS 認証設定（RADIUS Authentication Settings）] の [ネットワーク デバイス（Network Devices）] ページ（[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]）で指定した CoA ポートを変更する場合は、[ネットワーク デバイス プロファイル（Network Device Profile）] ページ（[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス プロファイル（Network Device Profiles）]）で対応するプロファイルに同じ CoA ポートを指定します。
RADIUS DTLS の設定	
必要な DTLS	このオプションを有効にすると、Cisco ISE ではこのデバイスからの DTLS 要求だけが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。
CoA ポート（CoA Port）	RADIUS DTLS CoA に使用するポートを指定します。
CoA の ISE 証明書の発行元 CA	ドロップダウン リストから RADIUS DTLS CoA に使用する認証局を選択します。

フィールド	使用上のガイドライン
DNS 名	ネットワーク デバイスの DNS 名を入力します。[RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification）] オプションが RADIUS 設定で有効になっている場合、Cisco ISE はこの DNS 名とクライアント証明書で指定されている DNS 名を比較して、ネットワーク デバイスの ID を確認します。
全般設定	
KeyWrap の有効化（Enable KeyWrap）	ネットワーク デバイスでサポートされる場合にのみ、このチェックボックスをオンにします。これにより、AES KeyWrap アルゴリズムによって RADIUS のセキュリティが強化されます。 （注） FIPS モードで Cisco ISE を実行する場合は、ネットワーク デバイス上で KeyWrap を有効にする必要があります。
キー暗号キー（Key Encryption Key）	（KeyWrap を有効にしている場合だけ表示されます）セッション暗号化（秘密）に使用される暗号キーを入力します。
メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）	（KeyWrap を有効にしている場合だけ表示されます）RADIUS メッセージのキー付き Hashed Message Authentication Code（HMAC）の計算に使用されるキーを入力します。

フィールド	使用上のガイドライン
キー入力形式（Key Input Format）	次の形式のいずれか 1 つを選択します。 • [ASCII]：キー暗号キーの長さは 16 文字（バイト）、メッセージ オーセンティケータ コード キーの長さは 20 文字（バイト）である必要があります。 • [16 進数（Hexadecimal）]：キー暗号キーの長さは 32 バイトであり、メッセージ オーセンティケータ コード キーの長さは 40 バイトである必要があります。 Cisco ISE FIPS 暗号キーの入力に使用するキー入力形式を指定します。これは、WLC の設定と一致する必要があります（指定する値はキーの正しい（全体の）長さにする必要があり、それよりも短い値は許可されません）。

TACACS+ 認証設定

次の表では、ネットワーク デバイスの TACACS+ 認証を設定するために使用できる [ネットワークデバイス（Network Devices）] ページのフィールドについて説明します。ナビゲーション パスは次のとおりです。

- （ネットワーク デバイスの場合）**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [TACACS認証設定（TACACS Authentication Settings）]**。
- （デフォルトのデバイスの場合）**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [デフォルトのデバイス（Default Devices）] > [TACACS認証設定（TACACS Authentication Settings）]**。詳細については、「Cisco ISE でのデフォルト ネットワーク デバイスの定義」を参照してください。

フィールド	使用上のガイドライン
共有秘密鍵（Shared Secret）	TACACS+ プロトコルがイネーブルのときにネットワーク デバイスに割り当てられたテキストの文字列。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前にテキストを入力する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。これは必須フィールドではありません。

フィールド	使用上のガイドライン
廃止された共有秘密がアクティブです（**Retired Shared Secret is Active**）	リタイアメント期間がアクティブな場合に表示されます。
廃止（**Retire**）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、メッセージ ボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。
残りの廃止期間（**Remaining Retired Period**）	（上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）次のナビゲーション パスで指定されたデフォルト値が表示されます。**[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）] > [接続設定（Connection Settings）] > [デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]**。デフォルト値は変更することができます。 これにより、新しい共有秘密を入力でき、古い共有秘密は指定された日数にわたってアクティブなままになります。
終了（**End**）	（上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。
シングル接続モードを有効にする（**Enable Single Connect Mode**）	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを実行します。 • [レガシーシスコデバイス（Legacy Cisco Devices）] • または、[TACACS+ドラフトコンプライアンスシングル接続のサポート（TACACS+ Draft Compliance Single Connect Support）]。シングル接続モードをディセーブルにすると、ISE はすべての TACACS+ 要求に対して新しい TCP 接続を使用します。

SNMP 設定

次の表では、[SNMP 設定（SNMP Settings）] セクションのフィールドについて説明します。

表 *217 : SNMP* 設定

フィールド	使用上のガイドライン
SNMP バージョン（SNMP Version）	[バージョン（Version）] ドロップダウン リストから要求に使用される SNMP のバージョンを選択します。 次のバージョンがあります。 • 1：SNMPv1 は informs をサポートしていません。 • 2c • 3：SNMPv3 は、[Priv] セキュリティ レベルを選択した場合にパケット暗号化が可能であるため、最もセキュアなモデルです。 （注） ネットワーク デバイスに SNMPv3 パラメータを設定した場合、モニタリング サービス（[操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] > [ネットワーク デバイス（Network Device）] > [セッション ステータス概要（Session Status Summary）]）によって提供されるネットワーク デバイス セッション ステータス概要レポートを生成できません。ネットワーク デバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。
SNMP RO コミュニティ（SNMP RO Community）	（SNMP バージョン 1 および 2c で選択された場合のみ）Cisco ISE にデバイスへの特定タイプのアクセスを提供する読み取り専用コミュニティ ストリングを入力します。 （注） キャレット記号（曲折アクセント付き^）を使用することはできません。

フィールド	使用上のガイドライン
SNMP ユーザ名（SNMP Username）	（SNMP バージョン 3 の場合のみ）SNMP ユーザ名を入力します。
セキュリティ レベル（Security Level）	（SNMP バージョン 3 の場合のみ）次からセキュリティ レベルを選択します。 • [Auth]：Message Digest 5 またはセキュア ハッシュ アルゴリズム（SHA）パケット認証をイネーブルにします • [No Auth]：認証なし、プライバシーなしのセキュリティ レベル。 • [Priv]：データ暗号規格（DES）パケットの暗号化をイネーブルにします
認証プロトコル（Auth Protocol）	（SNMP バージョン 3 でセキュリティ レベル Auth および Priv を選択した場合のみ）ネットワーク デバイスで使用する認証プロトコルを選択します。 認証プロトコルには、Auth および Priv のセキュリティ レベルに対して次のいずれかが含まれます。 • MD5 • SHA
認証パスワード（Auth Password）	（SNMP バージョン 3 でセキュリティ レベル Auth および Priv を選択した場合のみ）認証キーを入力します。このキーは 8 文字以上の長さにする必要があります。 デバイスにすでに設定されている認証パスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き ^）をパスワードで使用することはできません。

フィールド	使用上のガイドライン
プライバシー プロトコル（**Privacy Protocol**）	（SNMP バージョン 3 でセキュリティ レベル Priv を選択した場合のみ）ネットワーク デバイスで使用するプライバシー プロトコルを選択します。 プライバシープロトコルは次のいずれかです。 • DES • AES128 • AES192 • AES256 • 3DES
プライバシー パスワード（**Privacy Password**）	（SNMP バージョン 3 でセキュリティ レベル Priv を選択した場合のみ）プライバシー キーを入力します。 デバイスにすでに設定されているプライバシー パスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き ^）をパスワードで使用することはできません。
ポーリング間隔（**Polling Interval**）	ポーリング間隔を秒単位で入力します。デフォルトは 3600 秒です。
リンク トラップ クエリー（**Link Trap Query**）	SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、このチェックボックスをオンにします。
MAC トラップ クエリ（MAC Trap Query）	SNMP トラップを介して受信する MAC 通知を受信して解釈するには、このチェックボックスをオンにします。
送信元ポリシー サービス ノード（**Originating Policy Service Node**）	SNMP データのポーリングに使用される ISE サーバを示します。デフォルトでは自動ですが、別の値を割り当てて設定を上書きできます。

高度な TrustSec 設定

次の表は、[高度なTrustSec設定（Advanced TrustSec Settings）] セクションのフィールドについて説明しています。

表 *218* : 高度な *TrustSec* 設定

フィールド	使用上のガイドライン
HTTP REST API の設定	
TrustSec デバイスの通知および更新の設定	
TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）	[デバイスID（Device ID）] フィールドにデバイスIDとしてデバイス名をリストするには、このチェックボックスをオンにします。
デバイスID （Device ID）	[TrustSec IDにデバイスIDを使用（Use Device ID for TrustSec Identification）] チェックボックスがオンでない場合にのみ、このフィールドにデバイス ID を入力できます。
[パスワード（Password）]	TrustSec デバイスを認証するために TrustSec デバイス CLI で設定したパスワードを入力します。 TrustSecデバイスの認証に使用されるパスワードを表示するには、[表示（Show）] をクリックします。
環境データのダウンロード間隔 <...>（Download Environment Data Every <...>）	デバイスが Cisco ISE から環境データをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で指定できます。デフォルト値は 1 日です。
ピア許可ポリシーのダウンロード間隔 <...>（Download Peer Authorization Policy Every <...>）	デバイスが Cisco ISE からピア許可ポリシーをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で指定できます。デフォルト値は 1 日です。
再認証間隔 <...>（Reauthentication Every <...>）	最初の認証後、デバイスが Cisco ISE に対して自身を再認証する時間間隔を指定します。時間を秒、分、時、日、または週で設定できます。たとえば1000秒と入力すると、デバイスは 1000 秒ごとに Cisco ISE に対して自身を認証します。デフォルト値は 1 日です。

フィールド	使用上のガイドライン
SGACL リストのダウンロード間隔 <...>（Download SGACL Lists Every <...>）	デバイスが Cisco ISE から SGACL をダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で設定できます。デフォルト値は 1 日です。
その他の TrustSec デバイスでこのデバイスを信頼する（信頼できる TrustSec）（Other TrustSec Devices to Trust This Device (TrustSec Trusted)）	すべてのピア デバイスでこの TrustSec デバイスを信頼する場合は、このチェックボックスをオンにします。このチェックボックスをオフにした場合、ピア デバイスはこのデバイスを信頼せず、このデバイスから到着したすべてのパケットが適宜色付けまたはタグ付けされます。
設定変更のデバイスへの送信（Send Configuration Changes to Device）	Cisco ISE で CoA または CLI（SSH）を使用して TrustSec 設定変更を TrustSec デバイスに送信する場合は、このチェックボックスをオンにします。
CoA の使用（Using CoA）	Cisco ISE で CoA を使用して設定変更を TrustSec デバイスに送信する場合は、このオプションを選択します。
送信元（Send From）	設定変更を TrustSec デバイスに送る必要がある送信元 ISE ノードを、このドロップダウンリストから選択します。PAN または PSN ノードを選択できます。選択した PSN ノードがダウンした場合、PSN を使用して TrustSec デバイスに設定変更が送信されます。
Test Connection	TrustSec デバイスと選択した ISE ノード（PAN または PSN ノード）の間の接続をテストするには、このオプションを使用できます。
CLI（SSH）の使用（Using CLI (SSH)）	Cisco ISE で CLI を使用（SSH 接続を使用）して設定の変更を TrustSec デバイスに送信するには、このオプションを選択します。詳細については、非 CoA サポート デバイスへの設定変更のプッシュ（1148 ページ）を参照してください。

フィールド	使用上のガイドライン
SSH キー（SSH Key）	この機能を使用するには、Cisco ISE からネットワーク デバイスへの SSHv2 トンネルを開き、デバイスの CLI を使用して SSH キーを取得します。確認のために、このキーをコピーして [SSHキー（SSH Key）] フィールドに貼り付ける必要があります。詳細については、『』の「SSH キーの検証」のセクションSSH キーの検証 （1149ページ）を参照してください。
デバイス設定の展開設定	
セキュリティ グループ タグ マッピングの展開時にこのデバイスを含める（Include this device when deploying Security Group Tag Mapping Updates）	この TrustSec デバイスで、デバイス インターフェイス クレデンシャルを使用して IP と SGT の間のマッピングを取得するには、このチェックボックスをオンにします。
EXEC モード ユーザ名（EXEC Mode Username）	TrustSec デバイスへのログインに使用するユーザ名を入力します。
EXEC モード パスワード（EXEC Mode Password）	デバイス パスワードを入力します。
有効モード パスワード（Enable Mode Password）	（省略可能）特権モードで TrustSec デバイスの構成を編集するために使用する有効なパスワードを入力します。
アウト オブ バンド TrustSec PAC ディスプレイ（Out Of Band TrustSec PAC Display）	
発行日（Issue Date）	この TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行日を表示します。
期限日（Expiration Date）	この TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の有効期限を表示します。
発行元（Issued By）	このデバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行者（TrustSec 管理者）の名前を表示します。
PAC の生成（Generate PAC）	TrustSec デバイスのアウト オブ バンド TrustSec PAC を生成するには、このオプションをクリックします。

関連トピック

Cisco ISE でのネットワークデバイスの定義 （905 ページ）

Cisco ISE でのサードパーティ ネットワーク デバイスのサポート （910 ページ）
ネットワーク デバイス グループ（Network Device Groups） （918 ページ）
Cisco ISE でのネットワークデバイスの追加 （231 ページ）
Cisco ISE でのサードパーティ製ネットワーク デバイスの設定 （915 ページ）

デフォルトのネットワーク デバイス定義の設定

次の表に、Cisco ISE が RADIUS または TACACS+ 認証に使用できる、デフォルトのネットワーク デバイスを設定できるようにする [デフォルトのネットワーク デバイス（Default Network device）]ページのフィールドを示します。次のいずれかのナビゲーション パスを選択します。

- **[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デフォルトのデバイス（Default Devices）]**
- **[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク リソース（Network Resources）] > [デフォルトのデバイス（Default Devices）]**

表 *219* : デフォルトのネットワーク デバイス定義の設定

フィールド	使用上のガイドライン
デフォルトのネットワーク デバイスのステータス（Default Network Device Status）	デフォルトのネットワーク デバイス定義を有効にするには、[デフォルトのネットワーク デバイスのステータス（Default Network Device Status）] ドロップダウン リストから [有効化（Enable）] を選択します。 （注） デフォルトデバイスが有効になっている場合、RADIUS または TACACS+ で認証設定を有効にする必要があります。
デバイス プロファイル	デフォルトのデバイス ベンダーとしてシスコを表示します。
RADIUS 認証設定	
RADIUS の有効化	デバイスへの RADIUS 認証を有効にする場合は、このチェック ボックスをオンにします。
RADIUS UDP の設定	

フィールド	使用上のガイドライン
共有秘密鍵（Shared Secret）	共有秘密を入力します。共有秘密情報の長さは、最大 127 文字です。 共有秘密鍵は、**pac** オプションを指定した **radius-host** コマンドを使用してネットワーク デバイスに設定したキーです。 （注） 共有秘密鍵の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ページの [RADIUS 共有秘密鍵の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります（[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] > [デバイス セキュリティ設定（Device Security Settings）]）。デフォルトでは、この値は新規インストールとアップグレードされた展開用は 4 文字です。RADIUS サーバでのベスト プラクティスは、22 文字にすることです。
RADIUS DTLS の設定	
必要な DTLS	このオプションを有効にすると、Cisco ISE ではこのデバイスからの DTLS 要求だけが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。
CoA の ISE 証明書の発行元 CA	ドロップダウン リストから RADIUS DTLS CoA に使用する認証局を選択します。
全般設定	

フィールド	使用上のガイドライン
KeyWrap の有効化（Enable KeyWrap）	ネットワーク デバイスでサポートされる場合にのみ、このチェックボックスをオンにします。これにより、AES KeyWrap アルゴリズムによって RADIUS のセキュリティが強化されます。 FIPS モードで Cisco ISE を実行する場合は、ネットワーク デバイス上で KeyWrap を有効にする必要があります。
キー暗号キー（Key Encryption Key）	KeyWrap を有効にしているときに、セッションの暗号化（秘密）に使用される暗号キーを入力します。
メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）	KeyWrap を有効にしているときに、RADIUS メッセージに対するキー付き Hashed Message Authentication Code（HMAC）の計算に使用されるキーを入力します。
キー入力形式（Key Input Format）	次の形式のいずれか 1 つを選択します。 • [ASCII]：キー暗号キーの長さは 16 文字（バイト）、メッセージ オーセンティケータ コード キーの長さは 20 文字（バイト）である必要があります。 • [16 進数（Hexadecimal）]：キー暗号キーの長さは 32 バイトであり、メッセージ オーセンティケータ コード キーの長さは 40 バイトである必要があります。 Cisco ISE FIPS 暗号キーの入力に使用するキー入力形式を指定します。これは、WLC の設定と一致する必要があります指定する値はキーの正しい（全体の）長さにする必要があります。それよりも短い値は許可されません。
TACACS 認証設定	
共有秘密鍵（Shared Secret）	TACACS+ プロトコルがイネーブルのときにネットワーク デバイスに割り当てられたテキストの文字列。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前にテキストを入力する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。

フィールド	使用上のガイドライン
廃止された共有秘密がアクティブです（Retired Shared Secret is Active）	リタイアメント期間がアクティブな場合に表示されます。
廃止（Retire）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、メッセージ ボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。
残りの廃止期間（Remaining Retired Period）	（上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）次のナビゲーション パスで指定されたデフォルト値が表示されます。**[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）] > [接続設定（Connection Settings）] > [デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]**。デフォルト値は変更することができます。 これにより、新しい共有秘密を入力でき、古い共有秘密は指定された日数にわたってアクティブなままになります。
終了（End）	（上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。
シングル接続モードを有効にする（Enable Single Connect Mode）	ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを実行します。 • [レガシーシスコデバイス（Legacy Cisco Devices）] • または、[TACACS+ドラフトコンプライアンスシングル接続のサポート（TACACS+ Draft Compliance Single Connect Support）]。このオプションをディセーブルにすると、すべての TACACS+ 要求に対して新しい TCP 接続が ISE で使用されます。

デバイス セキュリティ設定

RADIUS 共有秘密の最小長を指定します。新規インストールとアップグレードした展開の場合、デフォルトではこの値は4 文字になります。RADIUS サーバでのベストプラクティスは、22 文字にすることです。

（注） [ネットワーク デバイス（Network Devices）] ページに入力した共有秘密の長さは、[デバイス セキュリティ設定（Device Security Settings）] ページの [RADIUS 共有秘密の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定した値以上でなければなりません。

関連トピック

ネットワーク デバイス定義の設定 （1429 ページ）

ネットワーク デバイスのインポート設定

次の表では、ネットワークデバイスの詳細をCisco ISEにインポートするために使用する [ネットワーク デバイス インポート（Network Device Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]** です。

表 *220 :* ネットワーク デバイスのインポート設定

フィールド	使用上のガイドライン
テンプレートの生成（Generate a Template）	カンマ区切り形式（.csv）テンプレート ファイルを作成するには、このリンクをクリックします。 同じ形式のネットワーク デバイス情報でテンプレートを更新し、それらのネットワーク デバイスをCisco ISE 展開にインポートするためにローカルで保存します。
ファイル（File）	作成したか、またはCisco ISE 展開から以前にエクスポートしたカンマ区切り形式ファイルの場所を参照するには、[参照（Browse）] をクリックします。 インポートを使用して、新しい、更新されたネットワーク デバイス情報を含むネットワーク デバイスを別のCisco ISE 展開にインポートできます。

フィールド	使用上のガイドライン
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	Cisco ISE で既存のネットワーク デバイスをインポート ファイル内のデバイスに置き換える場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポート ファイル内の新しいネットワーク デバイス定義がネットワーク デバイス リポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート中にエラーが発生したときに Cisco ISE にインポートを中止させる場合、このチェックボックスをオンにしますが、Cisco ISE はエラーのその時点までネットワーク デバイスをインポートします。 このチェックボックスがオフで、エラーが発生した場合は、エラーが報告され、Cisco ISE はデバイスを引き続きインポートします。

関連トピック

Cisco ISE でのネットワークデバイスの定義 （905 ページ）
Cisco ISE でのサードパーティ ネットワーク デバイスのサポート （910 ページ）
Cisco ISE へのネットワーク デバイスのインポート （908 ページ）

ネットワーク デバイス グループ（Network Device Groups）

これらのページを使用すると、ネットワーク デバイス グループを設定し、管理することができます。

ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用できる [ネットワーク デバイス グループ（Network Device Groups）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] > [グループ（Groups）]** です。

[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークデバイスグループ（Network Device Groups）] > [グループ（Groups）] ページでネットワーク デバイス グループを作成することもできます。

表 *221* : ネットワーク デバイス グループの設定

フィールド	使用上のガイドライン
名前（Name）	ルート ネットワーク デバイス グループ（NDG）の名前を入力します。ルート NDG の下の後続のすべての子ネットワーク デバイス グループに対して、新しいネットワーク デバイス グループの名前を入力します。 ルート ノードを含み、最大で 6 つのノードを NDG 階層に含めることができます。各 NDG 名は最大 32 文字です。
説明	ルートまたは子のネットワーク デバイス グループの説明を入力します。
親グループ（Parent Group）	親グループとして既存のグループを選択するか、ルートグループとして、この新しいグループを追加できます。

関連トピック

ネットワーク デバイス グループ（Network Device Groups） （918 ページ）
ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性 （919 ページ）
Cisco ISE でのネットワークデバイスの追加 （231 ページ）

ネットワーク デバイス グループのインポート設定

次の表では、Cisco ISE にネットワーク デバイス グループをインポートするために使用できる [ネットワーク デバイス グループ インポート（Network Device Group Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス グループ（Network Device Groups）]** > **[グループ（Groups）]** です。

表 *222* : ネットワーク デバイス グループのインポート設定

フィールド	使用上のガイドライン
テンプレートの生成（Generate a Template）	カンマ区切り形式（.csv）テンプレート ファイルを作成するには、このリンクをクリックします。 同じ形式のネットワーク デバイス グループ情報でテンプレートを更新し、それらのネットワーク デバイス グループを Cisco ISE 展開にインポートするためにローカルで保存します。

フィールド	使用上のガイドライン
ファイル（File）	作成したか、またはCisco ISE展開から以前にエクスポートしたカンマ区切り形式ファイルの場所を参照するには、[参照（Browse）] をクリックします。 インポートを使用して、新しい、更新されたネットワーク デバイス グループ情報を含むネットワーク デバイス グループを別の Cisco ISE 展開にインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	Cisco ISE で既存のネットワーク デバイス グループをインポート ファイル内のデバイス グループに置き換える場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポート ファイル内の新しいネットワーク デバイス グループがネットワーク デバイス グループ リポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート中にエラーが発生すると、Cisco ISE にインポートを中止させる場合、このチェックボックスをオンにしますが、Cisco ISE はエラーのその時点までネットワーク デバイス グループをインポートします。 このチェックボックスがオフで、エラーが発生した場合は、エラーが報告され、Cisco ISE はデバイス グループを引き続きインポートします。

関連トピック

ネットワーク デバイス グループ（Network Device Groups） （918 ページ）
ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性 （919 ページ）
Cisco ISE へのネットワーク デバイス グループのインポート （920 ページ）

セッション認識型ネットワーク（SAnet）のサポート

Cisco ISE は、セッション認識型ネットワーキング（SAnet）に対する限定的なサポートを提供します。SAnet は、多くのシスコスイッチで実行するセッション管理フレームワークです。SAnet は、可視性、認証、認可などのアクセスセッションを管理します。SAnet は、RADIUS 認可属性が含まれているサービステンプレートを使用します。Cisco ISE には、認証プロファイル内にサービステンプレートが含まれています。Cisco ISE は、プロファイルを「サービス

テンプレート」互換として識別するフラグを使用して認証プロファイルのサービステンプレートを識別します。

Cisco ISE 認証プロファイルには、属性のリストに変換される RADIUS 認可属性が含まれています。また、SAnet サービステンプレートには、RADIUS 認可属性も含まれていますが、これらの属性はリストに変換されません。

SAnetデバイスの場合、Cisco ISEはサービステンプレートの名前を送信します。キャッシュ内にそのコンテンツか、または静的に定義された設定が存在しない限り、デバイスはサービステンプレートのコンテンツをダウンロードします。サービステンプレートによってRADIUS属性が変更されると、Cisco ISE はデバイスに CoA 通知を送信します。

ネットワーク デバイス プロファイル設定

次の表は、[ネットワーク デバイス プロファイル（Network Device Profiles）] ページのフィールドについての説明です。このページを使用して、プロトコル、リダイレクトURLおよびCoA設定に対するデバイスのサポートなど、特定のベンダーからのネットワークデバイスのタイプに対するデフォルト設定を構成することができます。その後、プロファイルを使用して特定のネットワーク デバイスを定義します。

このページへのナビゲーション パスは、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス プロファイル（Network Device Profiles）]** です。

ネットワーク デバイス プロファイルの設定

次の表は、[ネットワークデバイスプロファイル（Network Device Profile）]セクションのフィールドについての説明です。

表 *223 :* ネットワーク デバイス プロファイルの設定

フィールド	説明
名前（Name）	ネットワークデバイスプロファイルの名前を入力します。
説明	ネットワークデバイスプロファイルの説明を入力します。
アイコン（Icon）	ネットワークデバイスプロファイルに使用するアイコンを選択します。このアイコンには、選択したベンダーのアイコンがデフォルトで設定されます。 選択するアイコンは 16 X 16 の PNG ファイルである必要があります。

フィールド	説明
ベンダー（Vendor）	ネットワーク デバイス プロファイルのベンダーを選択します。 選択可能なベンダーは、シスコ、Aruba、HP、Motorola、Brocade、Alcatel などです。
サポートされるプロトコル	
RADIUS	このネットワーク デバイス プロファイルが RADIUS をサポートしている場合は、このチェックボックスをオンにします。
TACACS+	このネットワーク デバイス プロファイルが TACACS+ をサポートしている場合は、このチェックボックスをオンにします。
TrustSec	このネットワーク デバイス プロファイルが TrustSec をサポートしている場合は、このチェックボックスをオンにします。
RADIUS ディクショナリ（RADIUS Dictionaries）	このプロファイルでサポートされる 1 つ以上の RADIUS ディクショナリを選択します。プロファイルを作成する前に、ベンダー固有の RADIUS ディクショナリをインポートします。

認証/許可テンプレートの設定

次の表は、[認証/許可（Authentication/Authorization）] セクションのフィールドについての説明です。

表 *224 :* 認証/許可の設定

フィールド	説明
フロータイプの条件（Flow Type Conditions）	Cisco ISE では、802.1X、MAC 認証バイパス（MAB）、およびブラウザベースの Web 認証ログインが、有線ネットワークと無線ネットワークの両方を介した基本的なユーザ認証およびアクセスでサポートされます。 このタイプのネットワーク デバイスがサポートする認証ログインのチェックボックスをオンにします。次の 1 つ以上の項目を指定できます。 • 有線 MAC 認証バイパス（MAB）（Wired MAC authentication bypass (MAB)） • 無線 MAB（Wireless MAB） • 有線 802.1x（Wired 802.1X） • 無線 802.1x（Wireless 802.1X） • 有線 Web 認証（Wired Web Authentication） • 無線 Web 認証（Wireless Web Authentication） ネットワーク デバイス プロファイルでサポートされる認証ログインをオンにした後、ログインの条件を指定します。
属性エイリアシング（Attribute Aliasing）	ポリシー ルールのフレンドリ名としてデバイスのサービスセット識別子（SSID）を使用する場合は、[SSID] チェックボックスをオンにします。これにより、ポリシー ルールで使用する一貫した名前を作成でき、その名前は複数のデバイスに適用されます。
ホスト ルックアップ（MAB）	

フィールド	説明
ホスト ルックアップの処理（Process Host Lookup）	ネットワーク デバイス プロファイルで使用されるホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。 さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。デバイス タイプに応じて、使用しているプロトコルの [パスワードを確認（Check Password）] チェックボックス、[Calling-Station-IdがMACアドレスと等しいかを確認（Checking Calling-Station-Id equals MAC Address）] チェックボックス、またはその両方をオンにします。
PAP/ASCII 経由（Via PAP/ASCII）	ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。
CHAP 経由（Via CHAP）	ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。 このオプションによって、CHAP 認証が有効になります。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。
EAP-MD5 経由（EAP-MD5）	ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。

権限テンプレートの設定

このネットワーク デバイス プロファイルに使用される VLAN および ACL の権限を定義できます。プロファイルを保存すると、Cisco ISE は設定された各権限に対し許可プロファイルを自動的に生成します。次の表は、[権限（Permissions）] セクションのフィールドについての説明です。

表 *225 :* 権限の設定

フィールド	説明
VLAN の設定（Set VLAN）	このネットワーク デバイス プロファイルに VLAN権限を設定するには、このチェックボックスをオンにします。次のいずれかのオプションを選択します。 • IETF 802.1X 属性（IETF 802.1X Attributes）：Internet Engineering Task Force で定義されたデフォルトの RADIUS 属性のセットです。 • 一意の属性（Unique Attributes）：複数の RADIUS 属性値のペアを指定できます。
ACL の設定（Set ACL）	RADIUS 属性をネットワーク デバイス プロファイルの ACL に設定する場合は、このチェックボックスをオンにします。

許可変更（CoA）テンプレートの設定

このテンプレートは、CoA がこのタイプのネットワーク デバイスにどのように送信されるかを定義します。次の表は、[許可変更（CoA）（Change of Authorization (CoA)）] セクションのフィールドについての説明です。

表 *226 :* 許可変更（*CoA*）の設定

フィールド	定義（Definition）
次による CoA（CoA by）	RADIUS により、または SNMP により、ネットワーク デバイス プロファイルに CoA パケットを送信するか、あるいはまったくしないかを選択します。
RADIUS による CoA（CoA by RADIUS）	
デフォルトの CoA ポート（Default CoA Port）	RADIUS CoA を送信するポート。シスコ デバイスのデフォルト ポートは 1700 で、他のベンダーのデバイスでは 3799 です。 [ネットワークデバイス（Network Device）] ページでこれを上書きできます。
タイムアウト間隔（Timeout Interval）	CoA の送信後に Cisco ISE が応答を待機する秒数。

フィールド	定義（Definition）
再試行回数（Retry Count）	最初のタイムアウト後に Cisco ISE が CoA の送信を試行する回数。
切断	これらのデバイスに接続解除要求を送信する方法を選択します。 • RFC 5176（RFC 5176）：標準のセッション終了の場合はこのチェックボックスをオンにし、RFC 5176 に従って定義されているように、ポートを新しいセッション用に残しておきます。 • ポート バウンス（Port Bounce）：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。 • ポートのシャットダウン（Port Shutdown）：セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。
再認証（Re-authenticate）	ネットワーク デバイスに再認証要求を送信する方法を選択します。これは現在、シスコ デバイスのみでサポートされています。 • 基本（Basic）：標準のセッション再認証の場合はこのチェックボックスをオンにします。 • 再実行（Rerun）：認証方式によって最初から実行する場合は、このチェックボックスをオンにします。 • 最後（Last）：最後に成功した認証方式をセッションに使用します。
CoA プッシュ（CoA Push）	ネットワーク デバイスがシスコの TrustSec CoA 機能をサポートしない場合は、このオプションを選択して、Cisco ISE が設定の変更をデバイスにプッシュできるようにします。
SNMP による CoA（CoA by SNMP）	
タイムアウト間隔（Timeout Interval）	CoA の送信後に Cisco ISE が応答を待機する秒数。

フィールド	定義（Definition）
再試行回数（Retry Count）	Cisco ISE が CoA の送信を試行する回数。
NAD ポートの検出	関連する RADIUS 属性は、現時点での唯一のオプションです。
関連する RADIUS 属性	NAD ポートを検出する方法を選択します。 • Nas-Port • Nas-Port-ID
切断	これらのデバイスに接続解除要求を送信する方法を選択します。 • 再認証します。セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。 • ポート バウンス（Port Bounce）：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。 • ポートのシャットダウン（Port Shutdown）：セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。

リダイレクト テンプレートの設定

ネットワークデバイスは、許可プロファイルで設定されている場合、クライアントのHTTP要求をリダイレクトできます。このテンプレートは、このネットワーク デバイス プロファイルがURLリダイレクトをサポートするかどうかを指定します。デバイス タイプに固有のURLパラメータ名を使用します。

次の表は、[リダイレクト（Redirect）] セクションのフィールドについての説明です。

表 *227:* リダイレクトの設定

フィールド	定義（**Definition**）
タイプ（Type）	ネットワーク デバイス プロファイルが静的または動的URL リダイレクトをサポートするかを選択します。 デバイスがどちらもサポートしていない場合、[未サポート（Not Supported）] を選択し、**[設定（Settings）] > [DHCPおよびDNSサービス（DHCP & DNS Services）]** から VLAN を設定します。
リダイレクト URL パラメータ名	
クライアント IP アドレス	ネットワーク デバイスがクライアントのIPアドレスに使用するパラメータ名を入力します。
クライアントMACアドレス（Client MAC Address）	ネットワーク デバイスがクライアントのMACアドレスに使用するパラメータ名を入力します。
元の URL（Originating URL）	ネットワーク デバイスが元のURLに使用するパラメータ名を入力します。
セッション ID	ネットワーク デバイスがセッション ID に使用するパラメータ名を入力します。
SSID	ネットワーク デバイスがサービス セット識別子（SSID）に使用するパラメータ名を入力します。
ダイナミック URL パラメータ	
パラメータ	動的URL リダイレクトを選択する場合は、これらのネットワーク デバイスがリダイレクト URL を作成する方法を指定する必要があります。また、リダイレクトURLがセッションIDまたはクライアントのMACアドレスを使用するかを指定できます。

詳細設定（Advanced Settings）

ネットワーク デバイス プロファイルを使用して、ネットワーク デバイスをポリシー ルールで使いやすくするために、多数のポリシー要素を生成できます。これらの要素には、複合条件、許可プロファイル、および許可されているプロトコルが含まれています。

これらの要素を作成するには、[ポリシー要素の作成（Generate Policy Elements）] ボタンをクリックします。

関連トピック

ネットワーク デバイス プロファイル （913 ページ）
Cisco ISE でのサードパーティ ネットワーク デバイスのサポート （910 ページ）
ネットワーク デバイス プロファイルの作成 （916 ページ）

外部 RADIUS サーバの設定

次の表では、[外部 RADIUS サーバ（External RADIUS Server）] ページのフィールドについて説明します。これらのフィールドを使用して、RADIUS サーバを設定できます。Cisco ISE が RADIUS サーバとして機能するためには、このページで設定する必要があります。このページのナビゲーション パスは、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [外部 RADIUS サーバ（External RADIUS Servers）]** です。

表 *228* : 外部 *RADIUS* サーバの設定

フィールド	使用上のガイドライン
名前（Name）	外部 RADIUS サーバの名前を入力します。
説明	外部 RADIUS サーバの説明を入力します。
ホスト名/アドレス（Host IP）	外部 RADIUS サーバの IP アドレスを入力します。 （注） IPv4 および IPv6 は、ネットワーク デバイス（TACACS および RADIUS）設定および外部 RADIUS サーバ設定でサポートされるようになりました。
共有秘密鍵（Shared Secret）	外部 RADIUS サーバの認証に使用される、Cisco ISE と外部 RADIUS サーバの間の共有秘密を入力します。共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証されるようにこれらの情報を提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。共有秘密情報の長さは、最大 128 文字です。
KeyWrap の有効化（Enable KeyWrap）	このオプションをオンにすると、Cisco ISE で FIPS 140-2 準拠が有効になり、AES KeyWrap アルゴリズムにより RADIUS プロトコルのセキュリティが強化されます。

フィールド	使用上のガイドライン
キー暗号キー（Key Encryption Key）	（[keyWrap を有効にする（Enable keyWrap）] チェックボックスをオンにした場合のみ）セッション暗号化（秘密）に使用される暗号キーを入力します。
メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）	（[keyWrap を有効にする（Enable keyWrap）] チェックボックスをオンにした場合のみ）RADIUS メッセージ上のキー付き HMAC 計算に使用されるキーを入力します。
キー入力形式（Key Input Format）	Cisco ISE 暗号キーの入力に使用する形式を指定します。これは、WLAN コントローラ上の設定と一致する必要があります。（指定する値の長さは、次に定義されているキーの最大長と正確に一致している必要があります。これより短い値は許可されません）。 • [ASCII]：キー暗号キーの長さは 16 文字（バイト）、メッセージ オーセンティケータ コード キーの長さは 20 文字（バイト）である必要があります。 • [16 進数（Hexadecimal）]：キー暗号キーの長さは 32 バイトであり、メッセージ オーセンティケータ コード キーの長さは 40 バイトである必要があります。
認証ポート（Authentication Port）	RADIUS 認証のポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1812 です。
アカウンティング ポート（Accounting Port）	RADIUS アカウンティングのポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1813 です。
サーバ タイムアウト（Server timeout）	Cisco ISE が外部 RADIUS サーバからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は 5 ～ 120 です。
接続試行回数（Connection Attempts）	Cisco ISE が外部 RADIUS サーバへの接続を試行する回数を入力します。デフォルトは 3 回に設定されています。有効な値は 1 ～ 9 です。

関連トピック

RADIUS プロキシ サーバとして機能する CIsco ISE （1082 ページ）

外部 RADIUS サーバの設定 （1083 ページ）

RADIUS サーバ順序

次の表では、RADIUS サーバ順序を作成するために使用する [RADIUS サーバ順序（RADIUS Server Sequences）] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [RADIUS サーバ順序（RADIUS Server Sequences）] > [追加（Add）]** です。

表 *229 : RADIUS* サーバ順序

フィールド	使用上のガイドライン
名前（Name）	RADIUS サーバ順序の名前を入力します。
説明	任意で説明を入力します。
ホスト名/アドレス（Host IP）	外部 RADIUS サーバの IP アドレスを入力します。
ユーザが選択したサービス タイプ（User Selected Service Type）	[使用可能（Available）] リスト ボックスで、ポリシー サーバとして使用する外部 RADIUS サーバを選択し、選択した外部 RADIUS サーバを [選択済み（Selected）] リスト ボックスに移動します。
リモート アカウンティング（Remote Accounting）	リモート ポリシー サーバでアカウンティングを有効にするには、このチェックボックスをオンにします。
ローカル アカウンティング（Local Accounting）	Cisco ISE でのアカウンティングを有効にするには、このチェックボックスをオンにします。
高度な属性設定（Advanced Attributes Settings）	
サブジェクト名の先頭から最後に出現する区切り文字まで削除（Strip Start of Subject Name up to the First Occurrence of the Separator）	プレフィクスからユーザ名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が acme\userA、区切り文字が \ の場合、ユーザ名は userA になります。

フィールド	使用上のガイドライン
最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip End of Subject Name from the Last Occurrence of the Separator）	サフィックスからユーザ名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が userA@abc.com、区切り文字が @ の場合、ユーザ名は userA になります。 • NetBIOS または User Principle Name（UPN）フォーマットのユーザ名（user@domain.com または /domain/user）からユーザ名を抽出するには、これらのストリップ オプションを有効にする必要があります。RADIUS サーバでユーザを認証するために、ユーザ名だけがRADIUS サーバに渡されるためです。 • \ および @ の両方のストリップ機能をアクティブ化し、Cisco AnyConnect を使用している場合、Cisco ISE は最初に出現する\を文字列から正確に取り除くことができません。ただし、各ストリップ機能は、Cisco AnyConnect を考慮して設計されているため、個別に使用する場合は動作します。
外部 RADIUS サーバへの要求に含まれる属性を変更する（Modify Attributes in the Request to the External RADIUS Server）	認証済みの RADIUS サーバとの間で送受信する属性の操作を Cisco ISE に許可するには、このチェックボックスをオンにします。 次の属性操作が可能です。 • [追加（Add）]：RADIUS 要求/応答全体に属性を追加します。 • [更新（Update）]：属性値（固定または静的）を変更します。または属性を別の属性値（動的）で置き換えます。 • [削除（Remove）]：属性または属性と値のペアを削除します。 • [すべて削除（RemoveAny）]：存在するすべての属性を削除します。

フィールド	使用上のガイドライン
認証ポリシーに進む（Continue to Authorization Policy）	ID ストア グループおよび属性の取得に基づいて、プロキシ フローを許可ポリシーの実行に誘導して、より詳細な意思決定を行うには、このチェックボックスをオンにします。このオプションを有効にすると、外部RADIUSサーバからの応答に含まれる属性が、認証ポリシーの選択に使用されます。このコンテキストの既存の属性は、AAAサーバの受け入れ応答属性の適切な値で更新されます。
Access-Accept の送信前に属性を変更する（Modify Attributes before send an Access-Accept）	応答をデバイスに返送する直前に属性を変更するには、このチェックボックスをオンにします。

関連トピック

RADIUS プロキシ サーバとして機能する CIsco ISE （1082 ページ）
RADIUS サーバ順序の定義 （1083 ページ）

NAC マネージャの設定

次の表では、NAC マネージャを追加するために使用できる [新規 NAC Manager（New NAC Manager）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [NAC Managers]** です。

表 *230 : NAC* マネージャの設定

フィールド	使用上のガイドライン
名前（Name）	Cisco Access Manager（CAM）の名前を入力します。
ステータス	CAM への接続を認証する Cisco ISE プロファイラからの REST API 通信を有効にする場合は、[ステータス（Status）] チェックボックスをオンにします。
説明	CAM の説明を入力します。

フィールド	使用上のガイドライン
[IPアドレス（IP Address）]	CAM の IP アドレスを入力します。Cisco ISE で CAM を作成して保存した後、CAM の IP アドレスを編集することはできません。 0.0.0.0 と 255.255.255.255 は、Cisco ISE で CAM の IP アドレスを検証するときに除外され、CAM の [IP アドレス（IP Address）] フィールドで使用できる有効な IP アドレスではないため、使用できません。 （注） ハイ アベイラビリティ構成で CAM のペアが共有する仮想サービス IP アドレスを使用できます。これで、ハイ アベイラビリティ構成で CAM のフェールオーバーをサポートできます。
[ユーザ名（Username）]	CAM のユーザインターフェイスにログオンできる CAM 管理者のユーザ名を入力します。
[パスワード（Password）]	CAM のユーザインターフェイスにログオンできる CAM 管理者のパスワードを入力します。

関連トピック

Cisco NAC アプライアンスとの Cisco ISE 統合

Cisco Clean Access Manager の追加

デバイス ポータルの管理

デバイス ポータルの設定

デバイス ポータルのグローバル設定

[ワーク センター（Work Centers）] > [BYOD] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）] または **[管理（Administration）] > [デバイス ポータルの管理（Device Portal Management）] > [設定（Settings）]** を選択します。

BYOD ポータルおよびデバイス ポータルの次の一般設定を設定できます。

- [従業員が登録するデバイス（Employee Registered Devices）]：[従業員を制限（Restrict employees to）] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は 5 デバイスに設定されています。

- [再試行 URL（Retry URL）]：デバイスを Cisco ISE にリダイレクトするために使用できる URL を [オンボードのための再試行 URL（Retry URL for onboarding）] に入力します。

これらの一般的な設定値を設定したら、これらの設定は会社に設定したすべて BYOD ポータルおよびデバイス ポータルに適用されます。

関連トピック

従業員が登録するパーソナル デバイス数の制限 （882 ページ）
BYOD 登録に再接続する URL の提供 （883 ページ）
分散環境のエンドユーザのデバイス ポータル （874 ページ）

デバイス ポータルのポータル ID 設定

これらの設定へのナビゲーションパスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [ブラックリスト ポータル（Blacklist Portal）]/[クライアント プロビジョニング ポータル（Client Provisioning Portals）]/[BYOD ポータル（BYOD Portals）]/[MDM ポータル（MDM Portals）]/[デバイス ポータル（My Device Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの設定およびカスタマイズ（Portals Settings and Customization）]** です。

- ポータル名（Portal Name）：このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル（ブラックリスト、個人所有デバイス持ち込み（BYOD）、クライアントプロビジョニング、モバイルデバイス管理（MDM）、またはデバイスの各ポータル）に使用しないでください。

  この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- **説明（Description）**：任意項目です。

- ポータルテスト URL（Portal test URL）：[保存（Save）] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

  リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

（注） テスト ポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアントプロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。

- 言語ファイル（Language File）：各ポータルタイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

  言語ファイルには、その言語のポータル全体のすべての文字列設定に加え、特定のブラウザのロケール設定（例：フランス語の場合は fr、fr-fr、fr-ca）へのマッピングが含まれています。1 つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

  1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイスポータルにも適用されます。

  [ポータルページのカスタマイズ（Portal Page Customizations）] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に 1 つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

-

関連トピック

許可ポリシー ルールの作成 （900 ページ）
許可プロファイルの作成 （899 ページ）
パーソナル デバイス ポータル （875 ページ）

ブラックリスト ポータルのポータル設定

この設定のナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [ブラックリスト ポータル（Blacklist Portal）] > [編集（Edit）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です

これらの設定を使用して、ユーザ（状況に応じてゲスト、スポンサー、または従業員）に表示される特定のポータルページではなく、ポータル全体に適用される値を指定したり動作を定義したりします。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

ポスチャ評価と修復についてのみ、クライアントプロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビットイーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。

- ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときのVMベースのものを含む、すべてのPSNで使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
- ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディングインターフェイスを設定しようとします。これが成功しない場合、おそらくは、そのPSNでボンディングが設定されていないために、PSNでエラーが記録されて終了します。PSNは物理インターフェイスでのポータルの開始を試みません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために2つの個別のNIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理NICと対応するボンディングされたNICの両方が設定されている場合：PSNがポータルを設定しようとすると、最初にボンディングインターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSNは物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- **表示言語**
  - [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語がISEでサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語がISEでサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

関連トピック

ブラックリスト ポータルの編集 （888 ページ）
ブラックリスト ポータル （876 ページ）
ブラックリスト ポータルの言語ファイルの HTML サポート （532 ページ）

BYOD と MDM ポータルのポータル設定

この設定のナビゲーションパスは、**[管理（Administration）]**>**[デバイス ポータル管理（Device Portal Management）]** > **[BYOD ポータルまたは MDM ポータル（BYOD Portals or MDM Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ポータル設定（Portal Settings）]** です。

これらを設定して、ポータル ページの動作を定義します。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアント プロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。

- スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
- スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディングインターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。

- 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- エンドポイント ID グループ（Endpoint identity group）：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。
- **表示言語**
  - [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

関連トピック

個人所有デバイスの持ち込みポータル （876 ページ）
BYOD ポータルの作成 （891 ページ）
モバイル デバイス管理ポータル （877 ページ）
MDM ポータルの作成 （896 ページ）
個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート （532 ページ）
モバイル デバイス管理ポータルの言語ファイルの HTML サポート （539 ページ）

BYOD ポータルの BYOD 設定

この設定のナビゲーションパスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[BYOD ポータル（BYOD Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[BYOD 設定（BYOD Settings）]** です。

この設定を使用して、パーソナル デバイスを使用する従業員の個人所有デバイスの持ち込み（BYOD）機能を有効にし、企業ネットワークにアクセスできるようにします。

フィールド	使用上のガイドライン
AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）	会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、またはAUPテキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
同意が必要（Require acceptance）	ユーザのアカウントが完全に有効になる前に、ユーザはAUPに同意する必要があります。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。ユーザがAUPに同意しない場合、ネットワークにアクセスできません。
AUPの最後までのスクロールが必要（Require scrolling to end of AUP）	このオプションは、[AUP をページに含める（Include an AUP on page）] が有効である場合のみ表示されます。 ユーザがAUPを最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。
登録時にデバイス ID フィールドを表示する（Display Device ID field during registration）	登録プロセス中に、デバイスIDをユーザに表示します。これは、デバイスIDが事前設定されており、BYOD ポータルを使用しているときに変更できない場合も含みます。

フィールド	使用上のガイドライン
元の URL（Originating URL）	ネットワークへの認証に成功すると、可能な場合はユーザのブラウザを、ユーザがアクセスしようとしていた元の Web サイトにリダイレクトします。リダイレクトできない場合は、認証成功ページが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。 Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザード アプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS（dot1X）およびサポート対象外のデバイス（ネットワーク アクセスが許可されている）では、この URL にリダイレクトされます。
成功ページ（Success page）	デバイスの登録が成功したことを示すページを表示します。
URL	ネットワークへの認証に成功すると、ユーザのブラウザを指定された URL（会社の Web サイトなど）にリダイレクトします。

（注） 認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。

関連トピック

個人所有デバイスの持ち込みポータル （876 ページ）
BYOD ポータルの作成 （891 ページ）
個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート （532 ページ）

証明書プロビジョニング ポータルのポータル設定

これらの設定へのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [証明書プロビジョニング ポータル（Certificate Provisioning Portal）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

  （注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は

PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

- イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
- ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
- ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- 認証方式（Authentication Method）ID ソース順序（Identity source sequence）：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP ディレクトリ などがあります。

  Cisco ISE には、スポンサー ポータル Sponsor_Portal_Sequence 用のデフォルトのスポンサー ID ソース順序が含まれています。

IdP を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

ID ソース順序を設定するには、[管理（Administration）] > [IDの管理（Identity Management）] > [IDソース順序（Identity Source Sequences）] の順に選択します。

- [承認済みグループの設定（Configure Authorized Groups）]：証明書を生成してそれを [選択済み（Chosen）] ボックスに移動するための権限を付与するユーザ ID グループを選択します。
- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：スポンサーまたはデバイス ポータルに対応する 1 つの固有の FQDN またはホスト名を入力します。たとえば、**sponsorportal.yourcompany.com,sponsor** と入力することで、ユーザはブラウザにこれらのいずれかを入力すると、スポンサー ポータルが表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

  デフォルトの FQDN を変更する場合は、次を実行します。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

- [アイドル タイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

ログイン ページの設定（Login Page Settings）

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザ セッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [AUPを含める（Include an AUP）]：フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
  - [同意が必要（require acceptance）]：フローを続行する前に、ユーザが AUP に同意するように強制します。
-

利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP ページを含める（Include an AUP page）]：会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [従業員に別の AUP を使用する（Use different AUP for employees）]：従業員専用に別の AUP およびネットワーク使用諸条件を表示します。このオプションを選択すると、[従業員用の AUP をスキップ（Skip AUP for employees）] は選択できません。
- [従業員用の AUP をスキップ（Skip AUP for employees）]：従業員は、ネットワークにアクセスする前に AUP に同意する必要はありません。このオプションを選択すると、[従業員に別の AUP を使用する（Use different AUP for employees）] は選択できません。
- [同意が必要（Require acceptance）]：ユーザのアカウントが完全に有効になる前に、ユーザは AUP に同意する必要があります。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。ユーザが AUP に同意しない場合、ネットワークにアクセスできません。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。

  ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。AUP がユーザに表示された場合に設定します。

  - [初回のログインのみ（On first login only）]：ユーザが初めてネットワークまたはポータルにログインしたときに AUP を表示します。
  - [ログインごと（On every login）]：ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
  - [__ 日ごと（初回のログインから）（Every __ days (starting at first login)）]：ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。
-

関連トピック

証明書プロビジョニング ポータル （876 ページ）
クライアント プロビジョニング ポータルの作成 （893 ページ）
証明書プロビジョニング ポータルの言語ファイルの HTML サポート （533 ページ）

クライアント プロビジョニング ポータルのポータル設定

これらの設定へのナビゲーション パスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[クライアント プロビジョニング ポータル（Client Provisioning Portals）]** > **[作成、編集、複製または削除（Create, Edit, Duplicate, or Delete）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** です。

ポータル設定

- HTTPS ポート（HTTPS Port）：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合、この制限に従うようにポート設定を変更する必要があります。
- 使用可能インターフェイス（Allowed interfaces）：ポータルを実行できる PSN インターフェイスを選択します。PSN で使用可能なインターフェイスを備えた PSN のみがポータルを作成できます。物理およびボンディングされたインターフェイスの任意の組み合わせを設定できます。これは PSN 全体の設定です。すべてのポータルはこれらのインターフェイスでのみ動作し、このインターフェイス設定はすべての PSN に適用されます。
  - 異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名は、インターフェイス IP に解決される必要があります。
  - ISE CLI の ip host x.x.x.x yyy.domain.com をセカンダリ インターフェイス IP と FQDN をマッピングするように設定します。これは証明書のサブジェクト名/サブジェクトの代替名を一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、その PSN にボンド セットがなかったことが原因である可能性があるので、PSN はエラーを記録して終了します。物理インターフェイスでポータルを開始しようとはしません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。
- 証明書グループ タグ（Certificate group tag）：ポータルの HTTPS トラフィックに使用する証明書グループのグループ タグを選択します。

- [認証方式（Authentication Method）]：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP などがあります。

  Cisco ISE には、クライアント プロビジョニング ポータル用のデフォルトのクライアント プロビジョニング ID ソース順序 Certificate_Portal_Sequence が含まれています。

- 完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）：クライアント プロビジョニング ポータル用に少なくとも 1 つの一意の FQDN、ホスト名、またはその両方を入力します。たとえば、「provisionportal.yourcompany.com」と入力した場合、ユーザはこれらのいずれかをブラウザに入力して証明書プロビジョニング ポータルに到達できます。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに確実に解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。

  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

（注） URL リダイレクトなしのクライアント プロビジョニングの場合、[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）] フィールドに入力するポータル名は、DNS 設定で設定されている必要があります。URL リダイレクトなしのクライアント プロビジョニングを有効にするため、この URL をユーザに通知する必要があります。

- アイドル タイムアウト（Idle timeout）：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

（注） クライアント プロビジョニング ポータルではポート番号と証明書を定義できます。これにより、ホストはクライアント プロビジョニングとポスチャに同じ証明書をダウンロードすることを許可します。ポータル証明書が正式な認証局により署名されている場合、セキュリティ警告は表示されません。自己署名証明書の場合、ポータルと Cisco AnyConnect Posture コンポーネントの両方でセキュリティ警告を受け取ります。

ログイン ページの設定（Login Page Settings）

- [ログインの有効化（Enable Login）]：クライアント プロビジョニング ポータルのログイン手順を有効にするには、このチェック ボックスを選択します

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：単一のブラウザ セッションからのログイン試行失敗回数を指定します。この回数を超過すると、Cisco ISE はログイン試行を実行できる頻度を意図的に低下させて、追加のログイン試行を防ぎます。ログイン失敗がこの回数に達した後のログイン試行の間隔は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で指定されます。
- [頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）]：[頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間を分単位で設定します。
- [AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）]：会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
- [同意が必要（Require acceptance）]：ポータルにアクセスする前にユーザが AUP を受け入れることを要求します。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。AUP を受け入れないユーザは、ポータルにアクセスできません。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。

利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP を含める（Include an AUP）]：会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：ユーザが AUP を完全に読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。
- [初回のログインのみ（On first login only）]：ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
- [ログインごと（On every login）]：ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [_ 日ごと（初回のログインから）（Every _____ days (starting at first login)）]：ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。

ポストログイン バナー ページ設定（Post-Login Banner Page Settings）

[ポストログイン バナー ページを含める（Include a Post-Login Banner page）]：ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

パスワード変更設定（Change Password Settings）

[内部ユーザに自身のパスワードの変更を許可する（Allow internal users to change their own passwords）]：従業員がクライアントプロビジョニング ポータルにログインして、自分のパスワードを変更できるようにします。これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

関連トピック

クライアント プロビジョニング ポータル （877 ページ）
クライアント プロビジョニング ポータルの作成 （894 ページ）
クライアントプロビジョニング ポータルの言語ファイルの HTML サポート （534 ページ）

MDM ポータルの従業員のモバイル デバイス管理設定

これらの設定へのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [MDM ポータル（MDM Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [従業員のモバイル デバイス管理設定（Employee Mobile Device Management Settings）]** です。

これらの設定を使用して、MDM ポータルを使用する従業員のモバイルデバイス管理（MDM）機能を有効にし、AUP エクスペリエンスを定義します。

フィールド	使用上のガイドライン
AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）	会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
同意が必要（Require acceptance）	ユーザのアカウントが完全に有効になる前に、ユーザは AUP に同意する必要があります。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。ユーザが AUP に同意しない場合、ネットワークにアクセスできません。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	このオプションは、[AUP をページに含める（Include an AUP on page）] が有効である場合のみ表示されます。 ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。

関連トピック

モバイル デバイス管理ポータル （877 ページ）
MDM ポータルの作成 （896 ページ）
Mobile Device Manager と Cisco ISE との相互運用性

デバイス ポータルのポータル設定

これらの設定へのナビゲーション パスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[デバイス ポータル（My Devices Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ポータル設定（Portal Settings）]** です。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**

  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディングインターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディングインターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：スポンサーまたはデバイス ポータルに対応する 1 つの固有の FQDN またはホスト名を入力します。たとえば、**sponsorportal.yourcompany.com,sponsor** と入力することで、ユーザはブラウザにこれらのいずれかを入力すると、スポンサー ポータルが表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

  デフォルトの FQDN を変更する場合は、次を実行します。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

- 認証方式（Authentication Method）IDソース順序（Identity source sequence）：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP ディレクトリ などがあります。

  Cisco ISE には、スポンサー ポータル Sponsor_Portal_Sequence 用のデフォルトのスポンサー ID ソース順序が含まれています。

  IdP を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

  ID ソース順序を設定するには、[管理（Administration）] > [IDの管理（Identity Management）] > [IDソース順序（Identity Source Sequences）] の順に選択します。

- エンドポイント ID グループ（Endpoint identity group）：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

- __日に達した場合にこの ID グループ内のエンドポイントを消去する（Purge endpoints in this identity group when they reach __ days）：Cisco ISE データベースから消去されるまでの、ユーザのデバイスの登録からの日数を変更します。消去は毎日実行され、消去アクティビティは全体的な消去タイミングと同期されます。変更は、このエンドポイント ID グループ全体に適用されます。

その他のポリシー条件に基づいてエンドポイント消去ポリシーに変更が加えられた場合、この設定は使用できなくなります。

- [アイドル タイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。
- **表示言語**
  - [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

関連トピック

デバイス ポータル （878 ページ）
デバイス ポータルの作成 （898 ページ）

デバイス ポータルのログイン ページ設定

デバイス ポータルのログイン ページ設定

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザ セッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザ セッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [AUPを含める（Include an AUP）]：フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。

- [同意が必要（require acceptance）]：フローを続行する前に、ユーザが AUP に同意するように強制します。

-

関連トピック

デバイス ポータル （878 ページ）
デバイス ポータルの作成 （898 ページ）
デバイス ポータルおよびエンドポイント アクティビティのモニタ （903 ページ）

デバイス ポータルの利用規定ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]** です。

これらの設定を使用して、ユーザ（状況に応じてゲスト、スポンサーまたは従業員）に対して AUP エクスペリエンスを定義します。

フィールド	使用上のガイドライン
AUP ページを含める（Include an AUP page）	会社のネットワーク使用諸条件を、別のページでユーザに表示します。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。
初回のログインのみ（On first login only）	ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUPを表示します。
ログインごと（On every login）	ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
__日ごと（初回のログインから）（Every __ days (starting at first login)）	ユーザがネットワークまたはポータルに初めてログインした後に、定期的にAUPを表示します。

関連トピック

デバイス ポータル （878 ページ）
デバイス ポータルの作成 （898 ページ）

デバイス ポータルのポストログイン バナー ページ設定

このページへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集ま**

または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポストログイン バナー ページ設定（Post-Login Banner Page Settings）] です。

これらの設定を使用して、正常なログイン後にユーザ（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

フィールド	使用上のガイドライン
ポストログイン バナー ページを含める（Include a Post-Login Banner page）	ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

関連トピック

デバイス ポータル （878 ページ）
デバイス ポータルの作成 （898 ページ）

デバイス ポータルの従業員によるパスワード変更の設定

このページへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [従業員のパスワード変更設定（Employee Change Password Settings）]** です。これらの設定を使用して、デバイス ポータルを使用している従業員のパスワード要件を定義します。

従業員のパスワード ポリシーを設定するには、**[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザ名パスワード ポリシー（Username Password Policy）]** を選択します。

フィールド	使用上のガイドライン
内部ユーザにパスワードの変更を許可する（Allow internal users to change password）	従業員が、デバイス ポータルにログインした後で、自分のパスワードを変更することを許可します。 これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

関連トピック

デバイス ポータルの作成 （898 ページ）
ポータルでの UTF-8 文字のサポート （121 ページ）

デバイス ポータルのデバイス管理設定

これらの設定へのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集ま**

たは複製（Create, Edit or Duplicate）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [デバイスの管理（Manage Device）] です。

[ページのカスタマイズ（Page Customizations）] で、デバイス ポータルの [アカウントの管理（Manage Accounts）] タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

[設定（Settings）] では、このデバイス ポータルを使用する従業員が各自の登録されたパーソナル デバイスで実行可能なアクションを指定できます。

表 *231* : デバイス ポータルのデバイス管理設定

フィールド	使用上のガイドライン
紛失（Lost）	すべてのデバイス。 デバイスを紛失したことを従業員が示すことができるようにします。このアクションは、デバイス ポータルのデバイスのステータスを [紛失（Lost）] に更新し、ブラックリストのエンドポイントの ID グループにそのデバイスを追加します。
復元（Reinstate）	すべてのデバイス。 このアクションでは、ブラックリストに記載されているか、紛失したか、または盗難されたデバイスを復元し、そのステータスを最後の既知の値にリセットします。このアクションでは、ネットワークに接続する前に追加プロビジョニングを実行する必要があるため、盗難デバイスのステータスを [未登録（Not Registered）] にリセットします。 ブラックリストに記載されているデバイスを従業員が復元できないようにする場合は、デバイス ポータルでこのオプションを有効にしないでください。

フィールド	使用上のガイドライン
削除（Delete）	すべてのデバイス。 登録済みデバイスの最大数に到達した場合、従業員が、登録されたデバイスをデバイス ポータルから削除したり、未使用のデバイスを削除して新しいデバイスを追加したりできるようにします。このアクションによって、デバイス ポータルに表示されるデバイス リストからデバイスが削除されますが、デバイスはCisco ISEデータベースに残り、エンドポイントのリストに表示されます。 BYOD またはデバイス ポータルを使用して従業員が登録できるパーソナル デバイスの最大数を定義するには、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員登録済みデバイス（Employee Registered Devices）]** を選択します。 Cisco ISE データベースからデバイスを完全に削除するには、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。
盗難（Stolen）	すべてのデバイス。 デバイスが盗まれたことを従業員が示すことができるようにします。このアクションは、デバイス ポータルのデバイスのステータスを [盗難（Stolen）] に更新し、ブラックリストのエンドポイントのIDグループにそのデバイスを追加し、証明書を削除します。
デバイス ロック	MDM 登録デバイスのみ。 デバイスの紛失または盗難が発生した場合、従業員がすぐにデバイス ポータルからリモートでデバイスをロックできるようにします。このアクションによって、デバイスの不正使用が防止されます。 ただし、デバイス ポータルではPINを設定できないため、従業員が事前にモバイル デバイスに設定しておく必要があります。

フィールド	使用上のガイドライン
登録解除（Unenroll）	MDM 登録デバイスのみ。 職場でデバイスを使用する必要がなくなった場合に、従業員がこのオプションを選択できるようにします。このアクションでは、会社がインストールしているアプリケーションと設定のみが削除され、従業員のモバイルデバイス上の他のアプリケーションおよびデータは維持されます。
完全消去（Full wipe）	MDM 登録デバイスのみ。 デバイスを紛失したり、新しいものに交換したりした場合に、従業員がこのオプションを選択できるようにします。このアクションでは、従業員のモバイル デバイスを工場出荷時のデフォルト設定にリセットし、インストール済みのアプリケーションとデータを削除します。

関連トピック

従業員が追加するパーソナル デバイスの管理 （901 ページ）
デバイス ポータル （878 ページ）

デバイス ポータルのデバイス カスタマイズの追加、編集、および検索

これらの設定へのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [デバイスの追加、デバイスの編集またはデバイスの検索（Add Devices, Edit Devices or Locate Devices）]** です。

[ページのカスタマイズ（Page Customizations）] で、デバイス ポータルの [追加（Add）]、[編集（Edit）]、および [検索（Locate）] の各タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

関連トピック

デバイス ポータル （878 ページ）
デバイス ポータルの作成 （898 ページ）

デバイス ポータルのサポート情報ページの設定

この設定へのナビゲーションパスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [BYOD ポータル（BYOD Portals）]/[クライアント プロビジョニング ポータル（Client Provisioning Portals）]/[MDM ポータル（MDM Portals）]/[デバイス ポータル（My Device Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [サポート情報ページの設定（Support Information Page Settings）]** です。

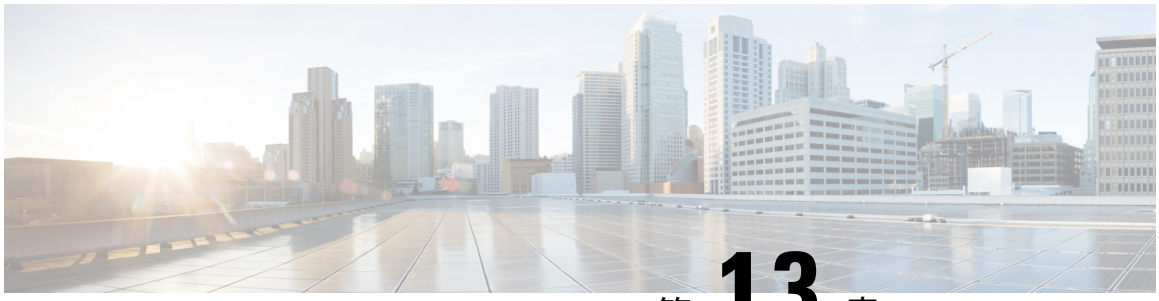
これらの設定を使用して、ヘルプデスクがユーザ（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

フィールド	使用上のガイドライン
サポート情報ページを含める（Include a Support Information Page）	該当ポータルのすべての有効なページ上で、**問い合わせ先**などの情報へのリンクを表示します。
MAC アドレス	[サポート情報（Support Information）] ページにデバイスの MAC アドレスを含めます。
IP アドレス	[サポート情報（Support Information）] ページにデバイスの IP アドレスを含めます。
ブラウザのユーザ エージェント（Browser user agent）	[サポート情報（Support Information）] ページに、要求の発信元のユーザ エージェントの製品名とバージョン、レイアウトエンジン、バージョンなど、ブラウザの詳細を含めます。
ポリシー サーバ（Policy server）	[サポート情報（Support Information）] ページに、このポータルを提供している ISE ポリシー サービス ノード（PSN）の IP アドレスを含めます。
障害コード（Failure code）	可能な場合は、ログ メッセージ カタログ内の対応する番号を含めます。メッセージ カタログにアクセスしてこれを表示するには、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージ カタログ（Message Catalog）]** に移動します。
フィールドを隠す（Hide field）	含める情報が存在しない場合、[サポート情報（Support Information）] ページ上の該当するフィールドラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード（Failure code）] は、選択されている場合でも表示されません。
値のないラベルを表示（Display label with no value）	含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを [サポート情報（Support Information）] ページに表示します。たとえば、障害コードが不明な場合、[障害コード（Failure code）] は空白であっても表示されます。

フィールド	使用上のガイドライン
デフォルト値でラベルを表示（Display label with default value）	[サポート情報（Support Information）] ページ上の選択されているフィールドに含まれる情報が存在しない場合、このテキストがこれらのすべてのフィールドに表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード（Failure code）] に [使用できません（Not Available）] と表示されます。

関連トピック

デバイス ポータルおよびエンドポイント アクティビティのモニタ （903 ページ）
デバイス ポータルへのアクセス （875 ページ）



第 13 章

pxGrid

pxGrid ノード

Cisco pxGrid を使用すると、Cisco ISE セッション ディレクトリからの状況依存情報を、ISE エコ システムのパートナー システムなどの他のネットワーク システムや他のシスコ プラットフォームと共有できます。また、pxGrid フレームワークは、Cisco ISE とサード パーティのベンダー間でのタグおよびポリシー オブジェクトの共有のように、ノード間でのポリシーおよび設定データの交換に使用でき、その他の情報交換にも使用できます。また、pxGrid では、サードパーティ システムが適応型ネットワーク制御アクション（EPS）を起動して、ネットワーク イベントまたはセキュリティ イベントに応答してユーザ/デバイスを隔離できます。タグ定義、値、および説明のような TrustSec 情報は、TrustSec トピックを通して Cisco ISE から別のネットワークに渡すことができます。完全修飾名（FQN）を持つエンドポイント プロファイルは、エンドポイント プロファイル メタ トピックを通して Cisco ISE から他のネットワークに渡すことができます。Cisco pxGrid は、タグおよびエンドポイント プロファイルの一括ダウンロードもサポートしています。

pxGrid 経由で SXP バインディング（IP-SGT マッピング）を発行および受信登録できます。SXP バインディングの詳細については、セキュリティ グループ タグの交換プロトコル （1157 ページ）を参照してください。

ハイ アベイラビリティ設定で、Cisco pxGrid サーバは、PAN を通してノード間で情報を複製します。PAN がダウンすると、pxGrid サーバは、クライアントの登録およびサブスクリプション処理を停止します。pxGrid サーバの PAN をアクティブにするには、手動で昇格する必要があります。[pxGrid サービス（pxGrid Services）] ページ（[管理（Administration）] > [pxGrid サービス（pxGrid Services）]）を調べ、pxGrid ノードが現在アクティブであるか、スタンバイ状態であるかを確認できます。

XMPP（Extensible Messaging and Presence Protocol）クライアントの場合、pxGrid ノードはアクティブ/スタンバイの高可用性モードで動作します。つまり、pxGrid サービスはアクティブ ノード上では「実行中」状態で、スタンバイ ノードでは「無効」状態です。

セカンダリ pxGrid ノードへの自動フェールオーバーが開始された後、元のプライマリ pxGrid ノードがネットワークに戻された場合、元のプライマリ pxGrid ノードは引き続きセカンダリ

ロールを持ち、現在のプライマリ ノードがダウンしない限り、プライマリ ロールに昇格されません。

（注） 時々、元のプライマリ pxGrid ノードがプライマリ ロールに自動的に昇格されることがあります。

ハイ アベイラビリティ展開では、プライマリ pxGrid ノードがダウンすると、セカンダリ pxGrid ノードに切り替えるのに約 3 ～ 5 分かかることがあります。プライマリ pxGrid ノードに障害が発生した場合は、キャッシュ データを消去する前に、クライアントはスイッチオーバーが完了するまで待機することを推奨します。

pxGrid ノードでは、次のログを使用できます。

- pxgrid.log：状態変更通知。
- pxgrid-cm.log：パブリッシャ/サブスクライバおよびクライアントとサーバ間のデータ交換アクティビティの更新。
- pxgrid-controller.log：クライアント機能、グループ、およびクライアント許可の詳細を表示します。
- pxgrid-jabberd.log：システムの状態と認証に関連するすべてのログ。
- pxgrid-pubsub.log：パブリッシャとサブスクライバのイベントに関する情報。

（注） ノードで pxGrid サービスが無効になっている場合、ポート 5222 はダウンしますが、（Web クライアントで使用される）ポート 8910 は機能し、引き続き要求に応答します。

（注） Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。また、 のアップグレード ライセンスを最近インストールしている場合には、Base インストールで特定の拡張 pxGrid サービスが使用可能である可能性があります。

（注） パッシブ ID ワーク センターを使用するには pxGrid を定義する必要があります。詳細については、 PassiveID ワークセンター （637 ページ）を参照してください。

pxGrid クライアントおよび機能の管理

Cisco ISE に接続するクライアントは、pxGrid サービスを使用する前に、アカウントを登録し、承認を受ける必要があります。pxGrid クライアントは、クライアントになるために pxGrid SDK を介してシスコから利用可能な pxGrid クライアントライブラリを使用します。Cisco ISE は、

自動および手動承認の両方をサポートします。クライアントは、一意の名前と証明書ベースの相互認証を使用して pxGrid にログインできます。スイッチの AAA 設定と同様に、クライアントは設定された pxGrid サーバのホスト名または IP アドレスに接続できます。

pxGrid の「機能」は、クライアントの pxGrid 上の情報トピックまたはチャネルであり、これらは公開および登録されます。Cisco ISE では、ID、適応型ネットワーク制御、SGA などの機能のみがサポートされます。クライアントが新しい機能を作成すると、その機能は **[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [機能別に表示（View by Capabilities）]** に表示されます。機能は個別に有効または無効にできます。機能情報は、発行、ダイレクト クエリー、または一括ダウンロード クエリーでパブリッシャから入手してください。

（注） pxGrid セッション グループが EPS グループの一部であるため、EPS ユーザ グループに割り当てられたユーザはセッション グループで操作を実行できます。ユーザが EPS グループに割り当てられると、ユーザは pxGrid クライアントのセッションのグループに加入できます。

関連トピック

pxGrid 証明書の生成 （82 ページ）

pxGrid クライアントの有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- パッシブ ID サービスを有効にします。**[管理（Administration）] > [展開（Deployment）]** を選択し、必要なノードにチェックマークを付け、[編集（Edit）] をクリックします。設定画面で [パッシブ ID サービスを有効にする（Enable Passive Identity Service）] をオンにします。

ステップ 1 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）]** を選択します。

ステップ 2 クライアントの隣にあるチェックボックスをオンにして [承認（Approve）] をクリックします。

ステップ 3 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

pxGrid 機能の有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。

• pxGrid クライアントをイネーブルにします。

ステップ 1 **[管理（Administration）] > [pxGrid サービス（pxGrid Services）]** を選択します。

ステップ 2 右上の [機能別に表示（View by Capabilities）] をクリックします。

ステップ 3 有効にする機能を選択し、[有効（Enable）] をクリックします。

ステップ 4 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

ISE pxGrid ノードの展開

スタンドアロン ノードと分散展開ノードの両方で、Cisco pxGrid ペルソナを有効にできます。

始める前に

- Base ライセンスを使用して pxGrid を有効にできますが、pxGrid ペルソナを有効にするには Plus ライセンスが必要です。
- Cisco pxGrid サービスは、Cisco ISE SNS 3415/3495 アプライアンス上または VMware で実行されます。
- すべてのノードは、pxGrid 用に CA 証明書を使用するように設定されています。アップグレード前にデフォルトの証明書を pxGrid に使用する場合、アップグレード後にこの証明書は内部 CA 証明書に置き換えられます。
- 分散展開を使用しているか、または Cisco ISE 1.2 からアップグレードする場合は、証明書で [pxGrid 使用（pxGrid Usage）] オプションを有効にする必要があります。[pxGrid 使用（pxGrid Usage）] オプションを有効にするには、**[管理（Administration）] > [証明書（Certificates）] > [システム証明書（Certificates）]** に移動します。展開に使用される証明書を選択し、[編集（Edit）] をクリックします。pxGrid を確認します。[pxGrid コントローラ（pxGrid Controller）] チェックボックスの証明書を使用します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 [展開ノード（Deployment Nodes）] ページで、pxGrid サービスを有効にするノードの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 [全般設定（General Settings）] タブをクリックし、[pxGrid] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

以前のバージョンからアップグレードするとき、[保存（Save）] オプションが無効になる場合があります。このことは、ブラウザ キャッシュが旧バージョンの Cisco ISE の古いファイルを参照する場合に発生します。[保存（Save）] オプションを有効にするには、ブラウザ キャッシュを消去します。

pxGrid の設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）] を選択します。

ステップ 2 必要に応じて、次のオプションを選択します。

- 新しいアカウントの自動承認（Automatically Approve New Accounts）：このチェック ボックスにマークを付けると、新しい pxGrid クライアントからの接続要求が自動的に承認されます。
- パスワード ベースのアカウント作成の許可（Allow Password Based Account Creation）：このチェック ボックスにマークを付けると、pxGrid クライアントのユーザ名/パスワードベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

  pxGrid クライアントは、REST API を介してユーザ名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

ステップ 3 [保存（Save）] をクリックします。

[pxGrid の設定（pxGrid Settings ）] ページで [テスト（Test）] オプションを使用して、pxGrid ノードでヘルス チェックを実行します。pxgrid/pxgrid-test.log ファイルで詳細を確認できます。

pxGrid 証明書の生成

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- pxGrid 証明書はプライマリ PAN から生成する必要があります。
- PxGrid 証明書がサブジェクト代替名（SAN）の拡張を使用する場合、DNS 名のエントリとしてサブジェクト ID の FQDN が含まれるようにします。

ステップ 1 [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [設定（Settings）] の順に選択します。

ステップ 2 [処理の選択（I want to）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- 単一の証明書の生成（証明書署名要求なし）（Generate a single certificate without a certificate signing request）：このオプションを選択すると、コモン ネーム（CN）を入力する必要があります。
- 単一の証明書の生成（証明書署名要求あり）（Generate a single certificate with a certificate signing request）：このオプションを選択すると、証明書署名要求の詳細を入力する必要があります。

- 一括証明書の生成（Generate bulk certificates）：必要な詳細を含む CSV ファイルをアップロードすることができます。
- ルート証明書チェーンのダウンロード（Download root certificate chain）：ルート証明書をダウンロードして、信頼できる証明書ストアに追加できます。ホスト名と証明書のダウンロード形式を指定する必要があります。

[証明書テンプレート（Certificate Templates）] リンクから証明書テンプレートをダウンロードし、必要に応じて、テンプレートを編集できます。

ステップ 3 （[単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）] オプションを選択した場合は必須）pxGrid クライアントの FQDN を入力します。

ステップ 4 （オプション）この証明書の説明を入力できます。

ステップ 5 サブジェクト代替名（SAN）を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- IP アドレス（IP address）：この証明書に関連付ける pxGrid クライアントの IP アドレスを入力します。
- FQDN：pxGrid の完全修飾ドメイン名を入力します。

（注） このフィールドは、[一括証明書の生成（Generate bulk certificates）] オプションを選択している場合には表示されません。

ステップ 6 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- Private Enhanced Electronic Mail（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY----」タグで終わります。
- PKCS12 形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル）：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンド エンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成（Create）] をクリックします。

作成した証明書は、ISE の **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [発行された証明書（Issued Certificates）]** に表示され、ブラウザのダウンロード ディレクトリにダウンロードされます。

pxGrid クライアントの権限の制御

pxGrid クライアントの権限を制御するために、pxGrid 許可ルールを作成できます。これらのルールを使用して、pxGrid クライアントに提供されるサービスを制御します。

さまざまな種類のグループを作成し、pxGrid クライアントに提供されるサービスをこれらのグループにマッピングできます。[権限（Permissions）] ウィンドウの [グループの管理（Manage Groups）] オプションを使用して、新しいグループを追加します。[権限（Permissions）] ウィンドウで、事前定義されたグループ（EPS や ANC など）を使用する事前定義された許可ルールを表示できます。事前定義されたルールでは [操作（Operations）] フィールドだけを更新できることに注意してください。

pxGrid クライアントの許可ルールを作成するには、以下の手順を実行します。

ステップ 1 [管理（Administration）] タブから、[pxGridサービス（pxGrid Services）] > [権限（Permissions）] を選択します。

ステップ 2 [サービス（Service）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

ステップ 3 [操作（Operations）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- **<ANY>**
- **パブリッシュ**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**

（注） このオプションを選択すると、カスタム操作を指定できます。

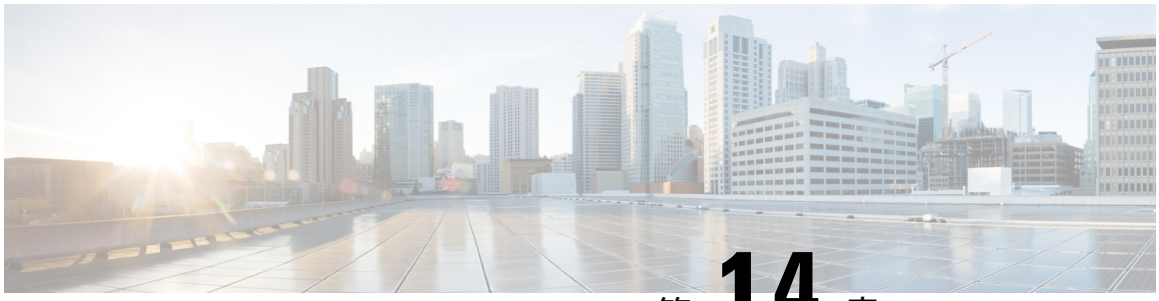
ステップ 4 [グループ（Groups）] ドロップダウン リストから、このサービスにマッピングするグループを選択します。

（EPS や ANC などの）事前定義されたグループ、および（[権限（Permissions）] ウィンドウの [グループの管理（Manage Groups）] オプションを使用して）手動で追加されたグループが、このドロップダウン リストに表示されます。

Cisco pxGrid ライブ ログ

[ライブ ログ（Live Logs）] ページには、すべての pxGrid 管理イベントが表示されます。イベント情報には、クライアント名と機能名、およびイベント タイプとタイムスタンプが含まれています。

[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [ライブ ログ（Live Log）] の順に移動して、イベント リストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。



第 14 章

統合

- iOS サプリカント プロビジョニングのためのワイヤレス LAN コントローラ設定（1527 ページ）
- MDM Interoperability のためのワイヤレス LAN コントローラでの ACL の設定（1528 ページ）

Wireless Setup について

Wireless Setup では、802.1x、ゲスト、および BYOD のワイヤレス フローを容易にセットアップできます。また、適切な場合にはゲスト向けのポータルと BYOD 向けのポータルを設定およびカスタマイズするためのワークフローも提供されます。これらのワークフローでは、最も一般的な推奨設定が提供されるため、ISE で関連ポータル フローを設定するよりもシンプルです。Wireless Setup では、ISE と WLC でユーザが実行する必要のあるステップの多くが自動的に処理されるため、迅速に作業環境を構築できます。

フローのテストと開発に、Wireless Setup により作成された環境を使用できます。Wireless Setup 環境が稼働したら、ISE に切り替えることができます。これにより、より多くの拡張設定に対応できるようになります。ISE でのゲストの設定についての詳細は、お使いの ISE バージョンの『ISE Administrators Guide』と Cisco コミュニティ サイト（https://community.cisco.com/t5/security-documents/ise-guest-amp-web-authentication/ta-p/3657224）を参照してください。ISE の Wireless Setup の設定と使用の詳細については、https://community.cisco.com/t5/security-documents/cisco-ise-secure-access-wizard-saw-guest-byod-and-secure-access/ta-p/3636602 を参照してください。

（注） ISE Wireless Setup はベータ ソフトウェアです。実稼働ネットワークでは ISE Wireless Setup を使用しないでください。

- Wireless Setup は、Cisco ISE の新規インストール後はデフォルトで**無効**になっています。Wireless Setup は、ISE CLI から **application configure ise** コマンド（オプション 17 を選択）を使用するか、または ISE GUI の [ホーム（Home）] ページで [ワイヤレスのセットアップ（Wireless Setup）] オプションを使用して有効にすることができます。
- ISE を以前のバージョンからアップグレードした場合、Wireless Setup は機能しません。Wireless Setup は、新規の ISE インストールでのみサポートされています。
- Wireless Setup は、スタンドアロン ノードでのみ機能します。
- Wireless Setup インスタンスは一度に 1 つだけ実行してください。また、Wireless Setup を実行できるユーザは一度に 1 人だけです。
- Wireless Setup を使用するには、ポート 9103 と 9104 が開いている必要があります。これらのポートを閉じるには、CLI を使用して Wireless Setup を無効にします。
- 一部のフローの実行後に Wireless Setup の新規インストールを開始する場合には、CLI コマンド **application reset-config ise** を使用できます。このコマンドは ISE 設定をリセットして ISE データベースをクリアしますが、ネットワーク定義を維持します。したがって、ISE

と Wireless Setup をリセットするときに、ISE を再インストールしてセットアップを実行する必要はありません。

Wireless Setup を再び使用開始するには、次の手順に従って ISE と Wireless Setup の両方の設定をリセットできます。

- CLI で **application reset-config** を実行し、ISE 設定をすべてリセットします。新規インストールで Wireless Setup をテストしていた場合、このコマンドを実行すると、ISE で Wireless Setup によって行われた設定が削除されます。
- CLI で **application configure ise** を実行し、**[18]Reset Config Wi-Fi Setup** を選択します。これにより、Wireless Setup 設定データベースの内容が消去されます。
- WLC で、Wireless Setup により WLC に追加された設定を削除します。WLC での Wireless Setup の設定内容については、「Wireless Setup による ISE と WLC の変更 （1515 ページ）」を参照してください。

ISE の新規インストール完了後に VM のスナップショットを取得しておくと、この手順を行わずに済みます。

CLI の詳細については、お使いの ISE バージョンの『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

- Wireless Setup を使用するには、ISE スーパー管理者ユーザである必要があります。
- Wireless Setup を使用するには、少なくとも 2 つの CPU コアと 8GB のメモリが必要です。
- Active Directory グループとユーザだけがサポートされています。Wireless Configuration で 1 つ以上のフローを作成すると、Wireless Setup でその他のタイプのユーザ、グループ、認証を使用できますが、これらを ISE で設定する必要があります。
- ISE で Active Directory をすでに定義しており、この AD を Wireless Setup に使用する予定の場合は、次の要件を満たしている必要があります。
  - 参加名とドメイン名が同一である必要があります。これらの名前が同一でない場合は、Wireless Setup でその AD を使用する前に、ISE で名前を同一にしてください。
  - ISE で WLC がすでに設定されている場合、その WLC には共有秘密が設定されている必要があります。WLC 定義に共有秘密がない場合は、Wireless Setup でその WLC を設定する前に、共有秘密を追加するか、または ISE から WLC を削除してください。
- Wireless Setup では ISE コンポーネントを設定できますが、フローの開始後に ISE コンポーネントを削除または変更することはできません。ISE の Wireless Setup で設定するすべての項目のリストについては、お使いの ISE バージョンの『Cisco Identity Services Engine CLI Reference Guide』を参照してください。
- 開始したフローは完了する必要があります。フローでトピック パスをクリックすると、フローが停止します。フローをステップに従って進むと、ISE 設定が動的に変更されます。Wireless Setup では設定変更のリストが表示されるので、手動で変更を元に戻すことができます。1 つの例外を除いて、フローで前に戻って追加の変更を行うことはできません。例

外として、ゲスト ポータルまたは BYOD ポータルのカスタマイズ内容を変更する場合には戻ることができます。

- 複数の WLC と Active Directory ドメインがサポートされていますが、各フローでは 1 つの WLC と 1 つの Active Directory だけがサポートされています。
- Wireless Setup が動作するためには、ISE Basic ライセンスが必要です。BYOD には Plus ライセンスが必要です。
- Wireless Setup の設定前に ISE リソースを設定している場合、Wireless Setup が既存のポリシーと矛盾することがあります。この状況では、Wireless Setup から、ツールの実行後に認証ポリシーをレビューするよう指示されます。Wireless Setup の実行時には、正常にセットアップされた ISE を使用して開始することが推奨されます。Wireless Setup と ISE の混合設定のサポートは限定されています。
- Wireless Setup は英語でのみ提供されており、他の言語では提供されていません。ポータルで他の言語を使用する場合には、Wireless Setup の実行後に ISE でその言語を設定してください。
- BYOD ではデュアル SSID がサポートされています。この設定で使用されるオープン SSID では、競合のためゲスト アクセスはサポートされません。ゲストと BYOD の両方に対応したポータルが必要な場合、Wireless Setup は使用できません。これについてはこのマニュアルでは説明しません。
- **電子メール通知と SMS 通知**
  - アカウント登録ゲストの場合、SMS 通知と電子メール通知がサポートされています。これらの通知は、ポータル カスタマイズ通知セクションで設定します。SMS 通知と電子メール通知をサポートするように SMTP サーバを設定する必要があります。ISE に組み込まれているセルラープロバイダー（AT&T、T Mobile、Sprint、Orange、Verizon など）は、事前に設定されている無料の電子メール/SMS ゲートウェイです。
  - ゲストはポータルで各自のセルラープロバイダーを選択します。プロバイダーがリストにない場合は、メッセージを受信できません。グローバルプロバイダーも設定できますが、これについてはこのマニュアルでは説明しません。ゲスト ポータルで SMS 通知と電子メール通知が設定されている場合、ゲストは両方のサービスの値を入力する必要があります。
  - Sponsored Guest フローでは、Wireless Setup での SMS 通知または電子メール通知の設定は行いません。このフローについては、ISE で通知サービスを設定する必要があります。
  - ポータルで通知を設定するときには、SMS プロバイダー *Global Default* を選択しないでください。（デフォルトでは）このプロバイダーは設定されていません。
- Wireless Setup では、HA を使用しないスタンドアロン セットアップだけがサポートされています。認証のために追加の PSN を使用する場合は、それらの PSN の ISE IP アドレスを WLC の RADIUS 設定に追加してください。

Wireless Setup での Apple ミニブラウザ（Captive Network Assistant）のサポート

- **ゲスト フロー**：Apple擬似ブラウザの自動ポップアップは、すべてのゲストフローで機能します。ゲストは Apple の Captive Network Assistant ブラウザを使用してフローを通過することができます。Apple ユーザが OPEN ネットワークに接続すると、ミニブラウザが自動的に表示されます。これにより、ユーザはAUP（ホットスポット）を受け入れるか、または各自のクレデンシャルを使用してアカウント登録またはログインを実行できます。
- **BYOD**
  - **シングル SSID**：ISE 2.2 では Apple ミニブラウザのサポートが追加されました。ただし Apple デバイスで SSID フローの問題が発生する可能性を抑えるため、リダイレクション ACL に captive.apple.com を追加してミニブラウザが表示されないようにしました。これにより、Apple デバイスはインターネットにアクセスできると想定します。ユーザは、Web 認証またはデバイス オンボーディングのためにポータルにリダイレクトされるように、Safari を手動で起動する必要があります。
  - **デュアル SSID**：ゲスト アクセスを開始するか、または従業員がデバイス オンボーディング（BYOD）を実行できるようにするために、最初の OPEN ネットワーク WLAN で開始し、セキュア SSID にリダイレクトされるデュアル SSID フローの場合にも、ミニブラウザが表示されなくなります。

Apple CAN ミニブラウザの詳細については、https://communities.cisco.com/docs/DOC-71122 を参照してください。

ワイヤレス ネットワークの WLC の設定

Wireless Setup に初めてログインしてフローを選択すると、ワイヤレス コントローラを設定するように促されます。Wireless Setup は設定するフローのタイプに対応するため、必要な設定を WLC にプッシュします。

- WLC は、AireOS 8.x 以降が稼働する Cisco WLC でなければなりません。
- vWLC は ACL ベースの DNS をサポートしません
- Wireless Setup 展開で使用する予定のインターフェイス VLANS（ネットワーク）用に WLC を設定します。デフォルトでは、WLC には管理インターフェイスがありますが、ゲストおよびセキュアアクセス（従業員）ネットワーク用に別のインターフェイスを設定することが推奨されます。
- ゲスト フローの場合、AUP の受け入れ（ホットスポット）、ログイン、またはクレデンシャルの作成のために、ACL_WEBAUTH_REDIRECT ACL を使用して、ゲスト デバイスがホットスポットまたはクレデンシャルを持つゲストポータルのいずれかにリダイレクトされます。承認されたゲストには、アクセスが許可されます（ACCESS-ACCEPT）。WLC で ACL を使用してゲストの権限を制限することができます。WLC で ACL を作成し、その ACL をゲスト権限 authz プロファイルで使用します。ISE 成功ページへのアクセスを許可するには、この ACL を WLC に追加します。限定的な ACL の作成の詳細については、https://communities.cisco.com/docs/DOC-68169 を参照してください。

- Wireless Setup ではフローごとに WLAN が設定されます。フローに WLAN を設定したら、その WLAN は他のフローには使用できません。唯一の例外は、アカウント登録フロー用に WLAN を設定しており、後でこの WLAN を Sponsored Guest フロー（ゲストのアカウント登録とスポンサー処理の両方を扱うフロー）に使用することに決定した場合です。

  実稼働環境で Wireless Setup を実行する場合、設定によって一部の既存ユーザの接続が切断されることがあります。

- Wireless Setup で WLC を使用してフローを設定したら、ISE ではその WLC を削除しないでください。

- ISE ですでに WLC を設定しているが、RADIUS オプションで共有秘密を設定していない場合、Wireless Setup で WLC を使用する前に共有秘密を追加する必要があります。

- ISE で WLC をすでに設定しており、共有秘密を設定している場合は、Wireless Setup で異なる共有秘密を設定しないでください。Wireless Setup と ISE のシークレット パスワードが一致している必要があります。選択する WLAN はフローで無効にされますが、フローの終わりで [本番稼働（Go Live）] ボタンをクリックすると再度有効にできます。

- **リモート LAN**：ネットワークにリモート LAN が含まれている場合、Wireless Setup はリモート LAN にすでに割り当てられている VLAN ID を使用しようとすると失敗します。この回避策として、リモート LAN を削除するか、または Wireless Setup を使用する前に WLC で使用する予定の VLAN を作成しておきます。Wireless Setup では、フローに対してこれらの既存の VLAN を有効にできます。

- **FlexConnect**：Flexconnect ローカル スイッチおよび Flexconnect ACL は、Wireless Setup によって設定されますが、使用されず、サポートされていません。Wireless Setup は、Flexconnect 集中型またはローカル モード Ap および SSID でのみ動作します。

ワイヤレス設定の例

次に示す WLC ログの一部分には、フローの設定時に Wireless Setup により行われる設定の例が示されています。

```
"config radius auth add 1 192.168.201.228 1812 ascii cisco"
"config radius auth disable 1"
"config radius auth rfc3576 enable 1"
"config radius auth management 1 disable"
"config radius auth enable 1"
"config radius acct add 1 192.168.201.228 1813 ascii cisco"
"config radius acct enable 1"
"config acl create ACL_WEBAUTH_REDIRECT"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
```

```
"config acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255"
"config acl apply ACL_WEBAUTH_REDIRECT"
"show flexconnect acl summary"
"config flexconnect acl create ACL_WEBAUTH_REDIRECT"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
 255.255.255.255"
"config flexconnect acl apply ACL_WEBAUTH_REDIRECT"
```

Active Directory と Wireless Setup

Sponsored Guest、802.1x、および BYOD のフローを作成するには、Active Directory ドメインが必要です。Active Directory は、スポンサー ポータル、802.1x セキュア アクセスおよび関連 VLAN、BYOD およびデバイス オンボーディングにアクセスできるスポンサー グループのユーザを指定します。Wireless Setup でいずれかのフローを設定したら、必要に応じて [ISE ID（ISE Identities）] に移動して次の項目を追加できます。

- スポンサー グループにマッピングされている内部スポンサー アカウント（ALL_ACCOUNTS など）。Active Directory を使用している場合は、これは不要です。
- ISE 内部従業員グループに含まれている従業員。内部従業員グループが許可ポリシーと ISE 内部従業員グループに追加されていることを確認してください。

Wireless Setup でのゲスト ポータル

企業の訪問者が企業のネットワークを使用してインターネットまたはネットワーク上のリソースおよびサービスにアクセスしようとしている場合、ゲスト ポータルを使用してネットワーク アクセスを提供することができます。設定すると、従業員はゲスト ポータルを使用して会社のネットワークにアクセスできます。

3 つのデフォルトのゲスト ポータルがあります。

- ホットスポット ゲスト ポータル：ネットワーク アクセスはクレデンシャルを必要とせずに許可されます。通常、ネットワーク アクセスを許可する前にユーザ ポリシーの認可（AUP）が承認される必要があります。

- Sponsored-Guest ポータル：ゲストのアカウントを作成したスポンサーによりネットワークアクセスが許可され、ゲストにログイン クレデンシャルが提供されます。
- アカウント登録ゲスト ポータル：ゲストは各自のアカウント クレデンシャルを作成できます。ネットワーク アクセスが付与される前に、スポンサー承認が必要となることがあります。

Cisco ISE は、事前に定義されたデフォルト ポータルなど、複数のゲスト ポータルをホストすることができます。

デフォルトのポータル テーマには、管理者ポータルからカスタマイズできる標準のシスコ ブランドが適用されています。

Wireless Setup には独自のデフォルト テーマ（CSS）があります。ロゴ、バナー、背景画像、色、フォントなどの基本的な設定の一部を変更できます。ISE では、他の設定を変更することでポータルをさらにカスタマイズでき、高度なカスタマイズを行うこともできます。

ゲスト ポータル ワークフロー

1. ポータルのタイプを選択すると、使用するコントローラを選択するよう求められます。フローごとに新しいワイヤレス ネットワークを設定します。Wireless Setup でまだ使用していない既存の WLAN を選択するか、または新しい WLAN を作成することができます。

   リダイレクトが必要なフローには、元の URL、正常完了ページ、または特定の URL（例：www.cisco.com）にユーザをリダイレクトするオプションがあります。元の URL を使用する場合は、WLC からのサポートが必要です。

（注） WLC バージョン 8.4 のリリースまでは、元の URL はサポートされていません。

2. ポータルの外観をカスタマイズし、基本設定を変更します。
3. カスタマイズが完了したら、テスト ポータルへの URL リンクをたどります。テスト ポータルに、ポータルのテストバージョンのプレビューが表示されます。フローを通過し、必要に応じてさらに変更を行うことができます。[成功（Success）]ページへのリダイレクトだけが成功することに注意してください。元の URL とスタティック URL は、リダイレクトをサポートするためにワイヤレスセッションが必要であるため、機能しません。テスト ポータルは RADIUS セッションをサポートしていません。そのため、ポータルフロー全体は表示されません。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。
4. 設定が完了しました。ワークフローにおいて Wireless Setup により ISE と WLC で実行されたステップをダウンロードして確認できます。

（注） Wireless Setup では基本ゲスト アクセスにはロケーションは使用されません。ローカル時刻に基づいてアクセスを制御する場合に、ロケーションが必要となります。ISE でのタイムゾーンの設定については、SMS プロバイダーおよびサービス （385 ページ）。

ワイヤレス ネットワーク アカウント登録ポータル

アカウント登録ゲストポータルでは、ゲストが自分自身を登録し、自分のアカウントを作成して、ネットワークにアクセスできるようにすることができます。

ログオン成功ページではユーザに対して画面にログオン クレデンシャルが表示されるため、ログオン成功ページを選択しないことが推奨されます。ベストプラクティスは、ユーザにクレデンシャルを電子メールまたは SMS で受信することを要求することです。これにより、クレデンシャルが監査目的に特有の内容に関連付けられます。

ワイヤレス ネットワーク Sponsored Guest フロー

スポンサーはスポンサー ポータルを使用して、承認ユーザ用の一時アカウントを作成および管理し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲスト アカウントを作成した後、スポンサーは、スポンサー ポータルを使用して、印刷、電子メール送信、または携帯電話による送信を行ってゲストにアカウントの詳細を提供することもできます。アカウント登録ゲストに企業ネットワークへのアクセス権を提供する前に、スポンサーはゲスト アカウントを承認するように電子メールで要求されることがあります。

スポンサー フローで、Wireless Setup がスポンサー ポータルと Sponsored Guest ポータルを設定します。

承認フローは Wireless Setup ではサポートされていません。

ワークフローで Active Directory をスポンサー グループにマッピングします。ワークフローにより、選択された AD グループが ALL_ACCOUNTS スポンサー グループにマッピングされます。GROUP または OWN アカウント スポンサー グループは設定されません。必要に応じて、他の ID ソース（内部設定や LDAP 設定など）を追加するには、ISE 管理 UI を使用して追加します。詳細については、スポンサー グループを参照してください。

Wireless Setup BYOD フロー：ネイティブ サプリカントおよび証明書のプロビジョニング

個人所有デバイスの持ち込み（BYOD）ポータルでは、従業員が各自のパーソナルデバイスを登録できます。ネイティブ サプリカント、証明書プロビジョニングはネットワークへのアクセスを許可する前にすることができます。従業員はBYODポータルに直接アクセスできません。パーソナルデバイスを登録するときにこのポータルにリダイレクトされます。従業員がパーソナルデバイスを使用してネットワークへ初めてアクセスしようとすると、（iOS以外のデバイスの場合）手動でNetwork Setup Assistant（NSA）ウィザードをダウンロードして起動するように促されることがあります。NSA では、ネイティブ サプリカントの登録とインストールを順を追って実行できます。デバイスを登録すると、デバイス ポータルを使用して、それを管理できます。

Wireless Setup は ISE とコントローラでネイティブ サプリカントと証明書のプロビジョニングを設定します。ユーザはコントローラにPEAP接続し、証明書を提供します。接続がEAP-TLS（証明書）に切り替わります。

Wireless Setup でサポートされるデバイスは、Apple デバイス（MAC および iOS）、Windows デスクトップ OS（モバイル以外）、および Android です。Chrome OS オンボーディングは、Wireless Setup ではサポートされていません。

Android デバイスの場合は、シングルまたはデュアル EAP-TLS ベースの BYOD フローが正常に動作するために、基本認証アクセス ポリシーが有効になっていることを確認します。**[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] > [デフォルト（Default）] > [許可ポリシー（Authorization Policy）]** に移動し、[Basic_Authenticated_Access] ルールがアクティブになっていることを確認します。

（注） デュアル SSID フローは、オンボーディング用のオープン ネットワークと、認証済みアクセス用の TLS 証明書ベースのセキュア ネットワークで構成されます。デバイスはオンボーディングなしでセキュア ネットワークに接続できます。これは、basic_authenticated_access デフォルト ルールにより、有効な認証はすべて通過できるためです。デバイスがセキュア ネットワークに接続する際に、BYOD セキュア許可ルールに一致しないと、basic_authenticated_access のリストの下部に一致が移動します。

この対策として、許可ポリシーで Basic_Authenticated_Access ルールを無効にするか、特定の SSID（WLAN）に一致するようにこのルールを編集します。いずれの変更でも、許可しないデバイスへの PEAP 接続がブロックされます。

（注） Wireless Setup には、ロストとマークされたデバイスをリダイレクトする許可ルールはありません。これはブラックリストと呼ばれ、ブラックリスト ポータルによって管理されます。ロストしたデバイスや盗まれたデバイスの管理については、http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.pdf を参照してください。

Wireless Setup での BYOD フロー

Wireless Setup での BYOD 設定は次のステップで構成されます。

1. ワイヤレス LAN コントローラの選択または登録
2. ワイヤレス ネットワークの追加：デュアル SSID の場合、この手順が 2 回実行されます。

（注） 新しいISEインストールには、デフォルトのワイヤレス ネットワークが含まれます。デュアル SSID BYOD では、ユーザが 2 番目の SSID にリダイレクトされると、ユーザのネットワーク プロファイルにデフォルトのネットワーク SSID が示されます。デフォルト SSID を削除するか、またはユーザにこの SSID を無視するように通知できます。

3. Active Directory（AD）の選択または AD への参加：オンボーディング VLAN と最終アクセス VLAN の両方のデフォルト VLAN 設定を上書きできます。最終アクセス VLAN は Active Directory グループにマッピングされます。

4. BYOD ポータルのカスタマイズ：BOYD ポータルとデバイス ポータルをここでカスタマイズできます。このステップでは、ISE がサポートするすべてのページをカスタマイズできます。このステップでは、すべてのポータル カスタマイズ内容が送信され、ポリシーが作成され、プロファイルが関連するポリシーにリンクされます。

（注） デバイス ポータルでは、BYOD ポータルのカスタマイズの基本カスタマイズが使用されます。Wireless Setup ではデバイス ポータルをカスタマイズできません。

5. 行った設定変更をプレビューして [完了（Done）] を選択します。

デュアル SSID BYOD の場合

デュアル SSID BYOD をサポートするには、Fast SSID が有効になっている必要があります。ワイヤレス コントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間を高速で移動できます。高速 SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。Cisco WLC での高速 SSID の設定に関する詳細については、『Cisco Wireless Controller Configuration Guide』を参照してください。

推奨される WLC タイマー設定

Wireless Setup で使用する予定の WLC で、次のタイマーを設定しておくことが推奨されます。この設定は CLI に表示されます。

```
config radius auth retransmit-timeout {SERVER_INDEX} 5
config radius aggressive-failover disable
config radius fallback-test mode passive
config wlan exclusionlist {WLAN ID} 180
config wlan exclusionlist {WLAN ID} enabled
```

802.1X ワイヤレス フロー

Wireless Setup フローにより、802.1x ワイヤレス LAN コントローラが PEAP（ユーザ名とパスワードのクレデンシャル）を使用して設定されます。

このフローの一部で、Active Directory（AD）を指定するように求められます。従業員 AD グループを VLAN にマッピングできます。VLAN によってグループを分ける場合は、異なる従業員グループを異なる VLAN に設定することができます。[アクセス（Access）] の横のドロップダウンをクリックすると、設定した AD で使用可能な AD グループが表示されます。

Wireless Setup で AD グループを選択すると、各グループが VLAN にマッピングされます。AD グループが VLAN にマッピングされていない場合は、有効な AD ユーザに対してログインを許可する基本アクセス ポリシーにユーザが一致します。

従業員がネットワークに接続する

1. **従業員のクレデンシャルが認証される**：Cisco ISE は、社内 Active Directory と照合して従業員を認証し、許可ポリシーを提供します。
2. **デバイスが BYOD ポータルにリダイレクトされる**：デバイスが BYOD ポータルにリダイレクトされます。デバイスの [MACアドレス（MAC address）] フィールドが入力され、ユーザはデバイス名と説明を追加できます。
3. **ネイティブ サプリカントが設定される（MacOS、Windows、iOS、Android）**：ネイティブ サプリカントが設定されます。ただしこのプロセスはデバイスに応じて異なります。
   - MacOS および Windows デバイス：従業員は BYOD ポータルで [登録（Register）] をクリックして、サプリカント プロビジョニング ウィザードをダウンロードしてインストールします。このウィザードは、サプリカントを設定し、EAP-TLS 証明書ベースの認証用の証明書をインストールします。デバイスの MAC アドレスと従業員のユーザ名が発行済み証明書に組み込まれます。

     （注） MacOS の場合、Apple 証明書を除き、証明書は Mac に [未署名（unsigned）] と表示されます。これは BYOD フローには影響しません。

   - iOS デバイス：Cisco ISE ポリシー サーバは Apple の iOS ワイヤレス機能を使用して新しいプロファイルを IOS デバイスに送信します。このプロファイルには次の情報が含まれます。
     - 発行された証明書が、IOS デバイスの MAC アドレスおよび従業員のユーザ名と共に保存されます。
     - 802.1X 認証の MSCHAPv2 または EAP-TLS の使用を強制できる Wi-Fi サプリカント プロファイル。
   - Android デバイス：Cisco ISE は、従業員に Google Play ストアから Cisco Network Setup Assistant（NSA）をダウンロードするように要求し、ルーティングします。アプリのインストール後に、従業員は NSA を開いてセットアップ ウィザードを開始できます。スタートアップ ウィザードでは、サプリカントの設定と、デバイスの設定に使用される発行済み証明書が生成されます。
   - **認可変更が発行される**：ユーザがオンボーディング フローを通過すると、Cisco ISE は認可変更（CoA）を開始します。これにより、MacOS X、Windows、および Android デバイスは EAP-TLS を使用してセキュアな 802.1X ネットワークに再接続します。シングル SSID の場合、iOS デバイスも自動的に接続されますが、デュアル SSID の場合、ウィザードは iOS ユーザに手動で新しいネットワークに接続するように要求します。

ネイティブ サプリカントは、次のオペレーティング システムでサポートされます。

- Android（Amazon Kindle、B&N Nook を除く）
- Mac OS X（Apple Mac コンピュータの場合）
- Apple iOS デバイス（Apple iPod、iPhone、および iPad）
- Microsoft Windows 7、8（RT を除く）、Vista、および 10

Wireless Setup による ISE と WLC の変更

Wireless Setup では、フローをステップに従って進むことで ISE とコントローラが設定されます。Wireless Setup は、行った変更のリストを各フローの終わりで表示します。各フローの変更内容がここで参考のために表示されます。これにより、Wireless Setup が ISE に対して行ったすべての変更を確認し、変更内容をレビューまたは変更できます。

- ホットスポット
  - **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [ホットスポットポータル（Hotspot Portal）]**
  - **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）]**
  - **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシーセット（Policy Sets）]**
- アカウント登録
  - **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [自己登録ポータル（Self-reg Portal）]**
  - **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストタイプ（Guest Types）] > [ゲストタイプ（Guest Types）]**
  - **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]**
  - **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシーセット（Policy Sets）]**
  - **[管理（Aministration）] > [システム（System）] > [設定（Settings）] > [SMTPサーバ（SMTP Server）]**
  - **[管理（Aministration）] > [システム（System）] > [設定（Settings）] > [SMTPゲートウェイ（SMTP Gateway）]**
- スポンサー

- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [スポンサーゲストポータル（Sponsored Guest Portal）] >**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > > [スポンサーポータル（Sponsor Portal）] >**
- **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [許可ポリシー（Authorization Policy）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー（Sponsor）] > [スポンサーグループ（Sponsor Groups）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストタイプ（Guest Types）] > [ゲストタイプ（Guest Types）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [外部IDソース（Ext ID Sources）] > [Active Directory]**

- **BYOD**
  - **[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [BYODポータル（BYOD Portals）] > [BYODポータル（BYOD Portal）]**
  - **[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [デバイスポータル（My Devices Portals）] > [デバイスポータル（My Devices Portal）]**
  - **[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]**
  - **[ワークセンター（Work Centers）] > [BYOD] > [許可ポリシー（Authorization Policy）]**
  - **[ワークセンター（Work Centers）] > [BYOD] > [外部IDソース（Ext ID Sources）] > [Active Directory]**
  - **[ワーク センター（Work Centers）] > [BYOD] > [外部 ID ソース（Ext ID Sources）] > [Active Directory]** を選択し、AD を選択し、[グループ（Groups）] タブを選択します。

- セキュアなアクセス
  - **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]**
  - **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]**

- **[ワーク センター（Work Centers）] > [ゲスト アクセス（Guest Access）] > [外部 ID ソース（Ext ID Sources）] > [Active Directory]** を選択し、AD を選択し、[グループ（Groups）] タブを選択します。

- ワイヤレス LAN コントローラ
  - **WLAN**
  - **[セキュリティ（Security）] > [アクセス制御リスト（Access Control Lists）]**：Wireless Setup では次の ACL が作成されます。
    - ゲストと BYOD 用のリダイレクト ACL
  - Wireless Setup により、**[セキュリティ（Security）] > [AAA] > [認証およびアカウンティング（Authentication and Accounting）]** にもエントリが作成されます。

スイッチでの標準 Web 認証のサポートの有効化

認証時の URL リダイレクションのプロビジョニングなど、Cisco ISE 用の標準 Web 認証機能を有効にするには、次のコマンドをスイッチのコンフィギュレーションに含めます。

```
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443
ip http secure-server
```

代理 RADIUS トランザクション用のローカル ユーザ名とパスワードの定義

スイッチがこのネットワーク セグメントの RADIUS サーバであるかのように Cisco ISE ノードと通信するには、次のコマンドを入力します。

```
username test-radius password 0 abcde123
```

ログとアカウンティングのタイムスタンプの正確性を保証するための NTP サーバ設定

次のコマンドを入力して、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [システム時刻（System Time）]** で Cisco ISE に設定したのと同じ NTP サーバを指定していることを確認してください。

ntp server *<IP_address>|<domain_name>*

AAA 機能を有効にするコマンド

802.1X および MAB 認証機能など、スイッチと Cisco ISE との間でさまざまな AAA 機能を有効にするには、次のコマンドを入力します。

```
aaa new-model

! Creates an 802.1X port-based authentication method list

aaa authentication dot1x default group radius

! Required for VLAN/ACL assignment

aaa authorization network default group radius

! Authentication & authorization for webauth transactions

aaa authorization auth-proxy default group radius

! Enables accounting for 802.1X and MAB authentications

aaa accounting dot1x default start-stop group radius

!

aaa session-id common

!

aaa accounting update periodic 5


! Update AAA accounting information periodically every 5 minutes


aaa accounting system default start-stop group radius

!
```

スイッチ上の RADIUS サーバの設定

Cisco ISE とやり取りし、RADIUS ソース サーバとして動作するようスイッチを設定するには、次のコマンドを入力します。

```
!
radius-server <ISE Name>

! ISE Name is the name of the ISE PSN

address ipv4 <ip address> auth-port 1812 acct-port 1813

! IP address is the address of the PSN. This example uses the standard RADIUS ports.

key <passwd>

! passwd is the secret password confiugured in Cisco ISE

exit
```

（注） 3 回の再試行を含む 30 秒のデッド基準時間を設定し、Active Directory を認証に使用する RADIUS 要求に対して、より長い応答時間を提供することを推奨します。

RADIUS 許可変更（CoA）を有効にするコマンド

スイッチが RADIUS 許可変更動作を適切に処理し、Cisco ISE のポスチャ機能をサポートできるようにするための設定を指定するには、次のコマンドを入力します。

```
aaa server radius dynamic-author

client <ISE-IP> server-key 0 abcde123
```

（注）

- Cisco ISE では、RFC の CoA 用デフォルト ポート 3799 に対して、ポート 1700（Cisco IOS ソフトウェアのデフォルト）を使用します。既存の Cisco Secure ACS 5.x ユーザは、既存の ACS の実装の一部として CoA を使用している場合、すでにこれをポート 3799 に設定している可能性があります。
- 共有秘密キーは、ネットワークデバイスの追加時に Cisco ISE で設定したものと同じである必要があり、IP アドレスは PSN IP アドレスである必要があります。

デバイス トラッキングと DHCP スヌーピングを有効にするコマンド

セキュリティに関連する Cisco ISE のオプション機能を提供できるようにするには、次のコマンドを入力することによって、デバイス トラッキングと DHCP スヌーピングを有効にし、スイッチ ポートのダイナミック ACL 内で IP 置換を実現します。

```
! Optional

ip dhcp snooping

! Required!

! Configure Device Tracking Policy!
device-tracking policy <DT_POLICY_NAME>
no protocol ndp
tracking enable

! Bind it to interface!
interface <interface_id>
device-tracking attach-policy<DT_POLICY_NAME>
```

RADIUS アカウンティングでは、DHCP スヌーピングが有効になっていても、DHCP 属性は IOS センサーによって Cisco ISE に送信されません。このような場合、DHCP スヌーピングを VLAN で有効にして DHCP をアクティブにする必要があります。

VLAN で DHCP スヌーピングを有効にするには、次のコマンドを使用します。

```
ip dhcp snooping

ip dhcp snooping vlan 1-100
```

（データおよび VLAN に使用する範囲を含める必要があります）

802.1X ポートベースの認証を有効にするコマンド

スイッチ ポートに対してグローバルに 802.1X 認証を有効にするには、次のコマンドを入力します。

```
dot1x system-auth-control
```

クリティカルな認証の EAP を有効にするコマンド

サプリカントによる LAN 経由での認証要求をサポートするには、次のコマンドを入力することによって、EAP をクリティカルな認証（アクセスできない認証バイパス）に対して有効にします。

```
dot1x critical eapol
```

リカバリ遅延を使用してAAA要求をスロットリングするコマンド

クリティカルな認証リカバリ イベントが発生した場合、次のコマンドを入力することによって、自動的に遅延（秒単位）を発生させるようスイッチを設定し、Cisco ISE がリカバリ後にサービスを再起動できるようにすることが可能です。

```
authentication critical recovery delay 1000
```

適用状態に基づく VLAN の定義

ネットワーク内の既知の適用状態に基づいて VLAN 名、番号、および SVI を定義するには、次のコマンドを入力します。ネットワーク間のルーティングを有効にするには、それぞれの VLAN インターフェイスを作成します。これは特に、同じネットワーク セグメントを経由して渡される、複数のソースからのトラフィックを処理する場合に役立ちます。たとえば、PC とその PC がネットワークへの接続時に経由する IP 電話の両方からのトラフィックが考えられます。

```
vlan <VLAN_number>

name ACCESS!

vlan <VLAN_number>

name VOICE

!

interface <VLAN_number>

description ACCESS

ip address 10.1.2.3 255.255.255.0

ip helper-address <DHCP_Server_IP_address>

ip helper-address <Cisco_ISE_IP_address>

!

interface <VLAN_number>

description VOICE
```

```
ip address 10.2.3.4 255.255.255.0

ip helper-address <DHCP_Server_IP_address>
```

スイッチのローカル（デフォルト）ACL 定義

このような機能を古いバージョンのスイッチ（Cisco IOS ソフトウェア リリースのバージョンが 12.2(55)SE よりも前）で有効にし、Cisco ISE が認証と許可に必要なダイナミック ACL の更新を実行できるようにするには、次のコマンドを入力します。

```
ip access-list extended ACL-ALLOW

 permit ip any any

!

ip access-list extended ACL-DEFAULT

  remark DHCP

  permit udp any eq bootpc any eq bootps

  remark DNS

  permit udp any any eq domain

  remark Ping

  permit icmp any any

  remark Ping

  permit icmp any any

  remark PXE / TFTP

  permit udp any any eq tftp

  remark Allow HTTP/S to ISE and WebAuth portal


permit tcp any host <Cisco_ISE_IP_address> eq www


permit tcp any host <Cisco_ISE_IP_address> eq 443
```

```
permit tcp any host <Cisco_ISE_IP_address> eq 8443

permit tcp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8906

permit tcp any host <Cisco_ISE_IP_address> eq 8080

permit udp any host <Cisco_ISE_IP_address> eq 9996

remark Drop all the rest
  deny ip any any log
!
! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
```

（注） WLC でこの設定を行うと、CPU 使用率が増加し、システムが不安定になるリスクが高まります。これは IOS の問題で、Cisco ISE は悪影響を受けません。

802.1X および MAB のスイッチ ポートを有効にする

802.1X および MAB のスイッチ ポートを有効にするには、以下の手順を実行します。

ステップ 1 すべてのアクセス スイッチ ポートのコンフィギュレーション モードを開始します。
interface range FastEthernet0/1-8

ステップ 2 次のように、（トランク モードではなく）アクセス モードのスイッチ ポートを有効にします。

switchport mode access

ステップ 3 静的にアクセス VLAN を設定します。アクセス VLAN のローカル プロビジョニングを提供するこの手順は、オープン モード認証に必要となります。

switchport access vlan <*VLAN_number*>

ステップ 4 静的に音声 VLAN を設定します。

switchport voice vlan <*VLAN_number*>

ステップ 5 オープン モード認証を有効にします。オープン モードを使用すると、認証が完了する前に、トラフィックをデータおよび音声 VLAN 上にブリッジングできます。実稼働環境では、ポートベースの ACL を使用して不正アクセスを防ぐことを強く推奨します。

! Enables pre-auth access before AAA response; subject to port ACL

authentication open

ステップ 6 ポートベースの ACL を適用して、認証されていないエンドポイントからアクセス VLAN 上にデフォルトでどのトラフィックをブリッジングするかを決定します。最初にすべてのアクセスを許可してからポリシーを適用する必要があるため、ACL-ALLOW を適用して、スイッチ ポートを通過するすべてのトラフィックを許可する必要があります。すでに現時点のすべてのトラフィックを許可するデフォルトの ISE 許可を作成しましたが、この理由は、完全な可視性を実現し、既存のエンドユーザ環境にはまだ影響を与えないようにするためです。

! An ACL must be configured to prepend dACLs from AAA server.

ip access-group ACL-ALLOW in

（注） DSBU スイッチ上に Cisco IOS Release 12.2(55)SE ソフトウェアを用意する前に、RADIUS AAA サーバからのダイナミック ACL を適用するためのポート ACL が必要です。デフォルトの ACL を用意できなかった場合、割り当てられた dACL はスイッチによって無視されます。Cisco IOS Release12.2(55)SE ソフトウェアでは、デフォルトの ACL が自動的に生成および適用されます。

（注） テストの現段階では、ポートベースの 802.1X 認証を有効にし、さらに既存のネットワークへの影響を避けるために、ACL-ALLOW を使用しています。今後のテストでは、実稼働環境に必要のないトラフィックをブロックする、異なる ACL-DEFAULT を適用する予定です。

ステップ 7 マルチ認証ホスト モードを有効にします。マルチ認証は、基本的には複数ドメイン認証（MDA）のスーパーセットです。MDA では、データ ドメイン内の単一のエンドポイントだけが許可されます。マルチ認証を設定すると、音声ドメイン内では認証された単一の電話が（MDA の場合と同じように）許可されますが、データ ドメイン内では認証できるデータ デバイスの数に制限がありません。

! Allow voice + multiple endpoints on same physical access port

authentication host-mode multi-auth

（注） IP 電話の背後で複数のデータ デバイス（仮想デバイスであるかハブに接続されている物理デバイスであるかにかかわらず）を使用すると、アクセス ポートの物理リンク ステート認識度が低下する可能性があります。

ステップ 8 次のように、さまざまな認証方式オプションを有効にします。

! Enable re-authentication

authentication periodic
! Enable re-authentication via RADIUS Session-Timeout
authentication timer reauthenticate server
authentication event fail action next-method
! デッドサーバの場合のクリティカル認証 VLAN メソッドの設定
authentication event server dead action reinitialize vlan *<VLAN_number>*
authentication event server alive action reinitialize
! IOS Flex-Auth 認証 802.1X と MAB
authentication order dot1x mab
authentication priority dot1x mab

ステップ 9 次のように、スイッチ ポートで 802.1X ポート制御を有効にします。
! Enables port-based authentication on the interface
authentication port-control auto
authentication violation restrict

ステップ 10 次のように、MAC 認証バイパス（MAB）を有効にします。
! Enable MAC Authentication Bypass (MAB)
mab

ステップ 11 次のように、スイッチ ポートで 802.1X を有効にします。
! Enables 802.1X authentication on the interface
dot1x pae authenticator

ステップ 12 次のように、再送信時間を 10 秒に設定します。
dot1x timeout tx-period *10*

（注） dot1x tx-period のタイムアウトは、10 秒に設定する必要があります。この値を変更する場合は、その影響を理解したうえで行ってください。

ステップ 13 次のように、PortFast 機能を有効にします。
spanning-tree portfast

EPM ロギングを有効にするコマンド

Cisco ISE の機能について発生する可能性があるトラブルシューティングや記録をサポートするには、次のように、スイッチに標準のロギング機能を設定します。

```
epm logging
```

SNMP トラップを有効にするコマンド

次のように、スイッチがこのネットワーク セグメント内の適切な VLAN を経由して、Cisco ISE から SNMP トラップ転送を受信できるようにします。

```
snmp-server community public RO

snmp-server trap-source <VLAN_number>
```

プロファイリング用の SNMP v3 クエリーを有効にするコマンド

SNMP v3 ポーリングが正常に発生し、Cisco ISE プロファイリング サービスがサポートされるように、スイッチを設定します。まず、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] > [追加（Add）]|[編集（Edit）] > [SNMP 設定（SNMP Settings）]** を選択して、Cisco ISE の SNMP 設定を設定します。

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>

snmp-server group  <group> v3 priv

snmp-server group <group> v3 priv context vlan-1
```

（注） **snmp-server group** *<group>* **v3 priv context** *vlan-1* コマンドは、コンテキストごとに設定する必要があります。**snmp show context** コマンドでは、すべてのコンテキスト情報がリストされます。

SNMP要求がタイムアウトになり、接続の問題が発生していない場合は、タイムアウト値を増加させることができます。

プロファイラによる収集を可能にするためのMAC通知トラップを有効にするコマンド

次のように、適切な MAC 通知トラップを送信するようスイッチを設定し、Cisco ISE のプロファイラ機能がネットワーク エンドポイントで情報を収集できるようにします。

```
mac address-table notification change
```

```
mac address-table notification mac-move

snmp trap mac-notification change added

snmp trap mac-notification change removed
```

スイッチ上での RADIUS Idle-timeout の設定

スイッチに RADIUS Idle-timeout を設定するには、次のコマンドを使用します。

```
Switch(config-if)# authentication timer inactivity
```

inactivity は、クライアントアクティビティが不正と見なされるまでの非アクティブ間隔を秒単位で表したものです。

Cisco ISE では、そのようなセッションの非アクティブ タイマーを適用する必要がある許可ポリシーに対して、**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]**>**[結果（Results）]**>**[許可（Authorization）]**>**[許可プロファイル（Authorization Profiles）]** からこのオプションを有効にできます。

iOS サプリカント プロビジョニングのためのワイヤレス LAN コントローラ設定

シングル SSID の場合

同じワイヤレス アクセス ポイントで、Apple iOS ベースのデバイス（iPhone/iPad）が、ある SSID から別の SSID に切り替えることができるようにするには、「FAST SSID の変更」機能を有効にするようワイヤレス LAN コントローラ（WLC）を設定します。この機能によって、iOS ベースのデバイスがより迅速に SSID 間の切り替えを行うことができます。

デュアル SSID BYOD の場合

デュアル SSID BYOD をサポートするには、Fast SSID が有効になっている必要があります。ワイヤレス コントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間を高速で移動できます。高速 SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。Cisco WLC での高速 SSID の設定に関する詳細については、『Cisco Wireless Controller Configuration Guide』を参照してください。

WLC の設定例

```
WLC (config)# FAST SSID change
```

一部の Apple iOS ベースのデバイスでは、ワイヤレス ネットワークに接続しようとすると、次のエラー メッセージが表示される場合があります。

ワイヤレスネットワークをスキャンできませんでした。（Could not scan for Wireless Networks.）

デバイス認証に影響しないため、このエラー メッセージは無視できます。

MDM Interoperability のためのワイヤレス LAN コントローラでの ACL の設定

未登録のデバイスおよび証明書プロビジョニングをリダイレクトするために許可ポリシーで使用する ACL をワイヤレス LAN コントローラで設定します。ACL は次の順序にする必要があります。

ステップ 1 サーバからクライアントへのすべての発信トラフィックを許可します。

ステップ 2 （任意）トラブルシューティングのためにクライアントからサーバへの ICMP 着信トラフィックを許可します。

ステップ 3 未登録および非準拠のデバイスが MDM エージェントをダウンロードし、コンプライアンス チェックに進むように MDM サーバへのアクセスを許可します。

ステップ 4 Web ポータルおよびサプリカント用 ISE、および証明書プロビジョニング フローに対するクライアントからサーバへのすべての着信トラフィックを許可します。

ステップ 5 名前解決のためにクライアントからサーバへの着信 DNS トラフィックを許可します。

ステップ 6 IP アドレスのためにクライアントからサーバへの着信 DHCP トラフィックを許可します。

ステップ 7 ISE へのリダイレクションのための、クライアントからサーバへの企業リソースに対するすべての着信トラフィックを（会社のポリシーに応じて）拒否します。

ステップ 8 （任意）残りのトラフィックを許可します。

例

次の例では、未登録のデバイスを BYOD フローにリダイレクトするための ACL を示しています。この例では、Cisco ISE IP アドレスは 10.35.50.165 で、社内ネットワークの IP アドレスは 192.168.0.0 および 172.16.0.0（リダイレクト用）で、MDM サーバ サブネットは 204.8.168.0 です。

図 *72 :* 登録されていないデバイスをリダイレクトするための *ACL*

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

第 15 章

トラブルシューティング

Cisco ISE のモニタリングとトラブルシューティング サービス

モニタリングおよびトラブルシューティング（MnT）サービスは、すべての Cisco ISE 実行時サービスを対象とした包括的なアイデンティティ ソリューションです。[操作（Operations）] メニューには次のコンポーネントが表示されます。このメニューはポリシー管理ノード（PAN）からのみ表示できます。[操作（Operations）] メニューはプライマリ モニタリング ノードに表示されないことに注意してください。

- モニタリング：ネットワーク上のアクセスアクティビティの状態を表す意味のあるデータをリアルタイムに表示します。これを把握することにより、操作の状態を簡単に解釈し、作用することができます。

- トラブルシューティング：ネットワーク上のアクセスの問題を解決するための状況に応じたガイダンスを提供します。また、ユーザの懸念に対応してタイムリーに解決策を提供できます。
- レポート：トレンドを分析し、システムパフォーマンスおよびネットワークアクティビティをモニタするために使用できる、標準レポートのカタログを提供します。レポートをさまざまな方法でカスタマイズし、今後使用するために保存できます。[ID（Identity）]、[エンドポイントID（Endpoint ID）]、および [ISE ノード（ISE Node）]（正常性の概要レポートは除く）のすべてのレポートで、ワイルドカードおよび複数値を使用してレコードを検索できます。

ISE コミュニティ リソース

トラブルシューティングに関するテクニカル ノートのリストについては、「ISE Troubleshooting TechNotes」を参照してください。

Network Privilege Framework のイベントフロープロセス

Network Privilege Framework（NPF）認証および許可イベント フローでは、次の表に記載されているプロセスが使用されます。

プロセス ステージ	説明
1	ネットワーク アクセス デバイス（NAD）によって通常の許可またはフレックス許可のいずれかが実行されます。
2	未知のエージェントレス ID が Web 許可を使用してプロファイリングされます。
3	RADIUS サーバによって ID が認証および許可されます。
4	許可がポートでアイデンティティに対してプロビジョニングされます。
5	許可されないエンドポイント トラフィックはドロップされます。

モニタリングおよびトラブルシューティング機能のユーザロールと権限

モニタリングおよびトラブルシューティング機能は、デフォルトのユーザ ロールに関連付けられます。実行を許可されるタスクは、割り当てられているユーザ ロールに直接関係します。

各ユーザロールに設定されている権限と制約事項については、Cisco ISE 管理者グループ （5 ページ）を参照してください。

モニタリングデータベースに格納されているデータ

Cisco ISE モニタリング サービスでは、データが収集され、特化したモニタリング データベースに格納されます。ネットワーク機能のモニタリングに使用されるデータのレートおよび量によっては、モニタリング専用のノードが必要な場合があります。Cisco ISE ネットワークによって、ポリシーサービスノードまたはネットワークデバイスからロギングデータが高いレートで収集される場合は、モニタリング専用の Cisco ISE ノードを推奨します。

モニタリングデータベースに格納される情報を管理するには、データベースの完全バックアップおよび差分バックアップを実行します。これには、不要なデータの消去とデータベースの復元が含まれます。

Smart Call Home

Smart Call Home（SCH）は、ネットワーク内の Cisco ISE デバイスを監視し、重大なイベントに関して電子メールで知らせます。電子メールには、環境情報と修復に関するアドバイスが記載されたリアルタイムのアラートが含まれています。

Cisco ISE のスマート ライセンスをアクティブにすると、SCH の機能はデフォルトで有効になります。それ以外の場合で、SCH を有効にするには、SCH サービス用に Cisco ISE を登録する必要があります。SCH 機能を有効にする方法の詳細については、Smart Call Home サービスの登録 （1534 ページ）を参照してください。

スマート ライセンスを有効にするか、SCH サービスを登録すると、次のいずれかを選択することができます。

- 匿名レポートのみを有効にします。SCH の匿名レポート機能は、ネットワーク内の Cisco ISE デバイスの最小限の状態に関する情報を提供します。
- SCH が提供するすべての機能セットを有効にします。

SCH機能の有効化については、Smart Call Home サービスの登録 （1534 ページ）を参照してください。

Smart Call Home プロファイル

Smart Call Home プロファイルは、デバイスでモニタされるイベントのタイプを決定します。Cisco ISE には、次のデフォルト プロファイルがあります。

- ciscotac-1：匿名レポートのために使用されます
- isesch-1：Smart Call Home 機能のために使用されます

匿名レポートのために使用されるデフォルト プロファイル（ciscotac-1）を編集することはできません。

Anonymous Reporting

Cisco ISE は、ユーザの展開、ネットワーク アクセス デバイス、プロファイラ、およびその他に使用しているサービスに関する非機密情報を安全に収集します。このデータは、Cisco ISE の使用状況をより詳しく把握し、製品と製品が提供するさまざまなサービスを向上させる目的で収集されます。

デフォルトでは、anonymous reporting は有効になっています。anonymous reporting を使用不可にするには、ISE 管理者ポータル（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [Smart Call Home]）で行うことができます。

Smart Call Home サービスの登録

（注） Cisco ISE のスマート ライセンスを有効にしている場合、Smart Call Home（SCH）サービスに登録する必要はありません。スマートライセンスにより、SCH機能はデフォルトで有効になっています。[Smart Call Home] ページの登録ステータスはアクティブになっています。匿名レポートのみを有効にすることや、SCH が提供する機能一式を有効にすることができます。

スマート ライセンスを使用せずに SCH サービスを有効にするには、まず SCH サービス用に Cisco ISE を登録する必要があります。これは、スタンドアロン ノードまたはプライマリ管理ノードからのみ行うことができます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [Smart Call Home]** の順に選択します。

ステップ 2 次のいずれかを実行します。

- SCH のすべての機能をオンにする（Turn on full SCH capability）
- デフォルト SCH テレメトリ設定を保持して匿名データのみを送信する（Keep the default SCH telemetry settings and send only anonymous data）
- すべて無効にする（Disable everything）

ステップ 3 （[SCH のすべての機能をオンにする（Turn on full SCH capability）] オプションを選択した場合のみ）[登録ステータス（Registration Status）] エリアに電子メール アドレスを入力します。

ステップ 4 （オプション）[Transport Gateway] チェックボックスをオンにして、Transport Gateway の URL を入力します。

ステップ 5 [保存（Save）] をクリックします。

SCH のすべての機能を有効にしている場合は、アクティベーション リンクが記載された電子メールを受信します。アクティベーション リンクをクリックして記載されている指示に従い、登録を完了します。

Cisco ISE をモニタする SNMP トラップ

Cisco ISE の汎用 SNMP トラップ

SNMP トラップは、Cisco ISE のステータスをモニタできます。Cisco ISE サーバにアクセスせずに Cisco ISE をモニタする場合は、Cisco ISE の SNMP ホストとして MIB ブラウザを設定できます。その後、MIB ブラウザから Cisco ISE のステータスをモニタすることもできます。

snmp-server host および **snmp-server trap** コマンドの詳細については、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

Cisco ISE は、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。

CLI から SNMP ホストを設定した場合は、Cisco ISE は次の汎用システム トラップを送信します。

- Cold start：デバイスをリブートするとき
- Linkup：イーサネット インターフェイスを起動するとき
- Linkdown：イーサネット インターフェイスをダウンするとき
- Authentication failure：コミュニティ ストリングが一致しないとき

Cisco ISE では、デフォルトで次の汎用 SNMP トラップが生成されます。

表 *232 : Cisco ISE* でデフォルトで生成される汎用 *SNMP* トラップ

OID	説明	トラップの例
.1.3.6.1.4.1.8072.4.0.3 NET SNMP エージェント MIB::nsNotifyRestart	エージェントが再起動されたことを示します。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.4.1.8072.4.0.2 NET SNMP エージェント MIB::nsNotifyShutdown	エージェントがシャットダウン中であることを示します。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix

OID	説明	トラップの例
.1.3.6.1.6.3.1.1.5.4 IF-MIB::linkUp	linkUp トラップは、エージェントロールで動作している SNMP エンティティで、いずれかの通信リンクの ifOperStatus オブジェクトが、ダウン状態から（notPresent 状態以外の）他の状態に遷移したことが検出されたことを示します。This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.3 IF-MIB::linkDown	linkDown トラップは、エージェントロールで動作している SNMP エンティティで、いずれかの通信リンクの ifOperStatus オブジェクトが、（notPresent 状態以外の）他の状態からダウン状態に遷移しようとしていることが検出されたことを示します。This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.1 SNMPv2-MIB::coldStart	coldStart トラップは、通知発信元アプリケーションをサポートする SNMP エンティティが自動的に再初期化され、このエンティティの設定は変更された可能性があることを示します。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

Cisco ISE のプロセス モニタリング SNMP トラップ

Cisco ISE では、Cisco ISE CLI から SNMP ホストを設定する場合、Cisco ISE プロセス ステータスの hrSWRunName トラップを SNMP マネージャに送信できます。Cisco ISE は cron ジョブを使用してこれらのトラップをトリガーします。cron ジョブは Cisco ISE プロセス ステータスを Monit から取得します。CLI から **SNMP-Server Host** コマンドを設定した後、5 分ごとに cron ジョブを実行して Cisco ISE をモニタします。

（注） 管理者が ISE プロセスを手動で停止した場合は、プロセスの Monit が停止しても、SNMP マネージャにトラップは送信されません。プロセスが不意にシャットダウンし、自動的に復活しない場合のみ、プロセス停止 SNMP トラップは SNMP マネージャに送信されます。

表 *233 : Cisco ISE* のプロセス モニタリング *SNMP* トラップ

OID	説明	トラップの例
.1.3.6.1.2.1.25.4.2.1.2 HOST-RESOURCES-MIB::hrSWRunName	A textual description of this running piece of software, including the manufacturer, revision, and the name by which it is commonly known. このソフトウェアがローカルにインストールされた場合は、対応する hrSWInstalledName で使用されているものと同じ文字列である必要があります。検討する必要のあるサービスは、app-server、rsyslog、redis-server、ad-connector、mnt-collector、mnt-processor、ca-server est-server、および elasticsearch です。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (63692139) 7 days, 8:55:21.39 SNMPv2-MIB::snmpTrapOID.0 = OID: HOSTRESOURCES-MIB::hrSWRunName HOSTRESOURCES-MIB::hrSWRunName = STRING: "redis-server:Running"

Cisco ISE は、次のステータスのトラップを設定済みの SNMP サーバに送信します。

- Process Start（監視状態）
- Process Stop（監視されていない状態）
- Execution Failed：プロセスの状態が「*Monitored*」から「*Execution failed*」に変更されるとトラップが送信されます。
- Does Not Exists：プロセスの状態が「*Monitored*」から「*Does not exists*」に変更されるとトラップが送信されます。

SNMPサーバで、すべてのオブジェクトについて一意のオブジェクトID（OID）が生成され、値が OID に割り当てられます。SNMP サーバの OID 値でオブジェクトを検索できます。実行中のトラップの OID 値は「*running*」で、監視されないトラップ、存在しないトラップ、実行に失敗したトラップの OID 値は「*stopped*」です。

Cisco ISE は、HOST-RESOURCES MIB に属している hrSWRunName の OID を使用してトラップを送信し、< *PROCESS NAME* > - < *PROCESS STATUS* > として OID 値を設定します。たとえば、runtime - running として設定します。

Cisco ISE が SNMP トラップを SNMP サーバに送信するのを停止させるには、Cisco ISE CLI からSNMP設定を削除します。この操作によって、SNMPトラップの送信と、SNMPマネージャからのポーリングが停止されます。

Cisco ISE のディスク使用状況 SNMP トラップ

Cisco ISE のパーティションのディスク使用率がしきい値に到達し、設定された空きディスク領域の量に達すると、ディスク使用状況トラップが送信されます。

（注） ISE には、プロセス ステータスまたはディスク使用状況の MIB はありません。Cisco ISE は SNMP トラップの送信に OID HOST-RESOURCES-MIB::hrSWRunName を使用します。プロセス ステータスまたはディスク使用状況の照会には snmp walk または snmp get コマンドは使用できません。

Cisco ISE では、次のディスク使用状況 SNMP トラップを設定できます。

表 *234 : Cisco ISE* のディスク使用状況 *SNMP* トラップ

OID	説明	トラップの例
.1.3.6.1.4.1.2021.9.1.9 UCD-SNMP-MIB::dskPercent	使用されているディスク容量の割合。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198297) 13 days, 16:19:42.97 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPercent UCD-SNMP-MIB::dskPercent = INTEGER: 13
.1.3.6.1.4.1.2021.9.1.2 UCD-SNMP-MIB::dskPath	ディスクがマウントされている場所のパス。 dskPath は、ISE 管理コマンド **show disks** の出力ですべてのマウント ポイントのトラップを送信できます。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198304) 13 days, 16:19:43.04 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPath UCD-SNMP-MIB::dskPath = STRING: /opt

Cisco ISE アラーム

アラームは、ネットワークの重大な状態を通知し、[アラーム（Alarms）] ダッシュレットに表示されます。データ消去イベントなど、システムアクティビティの情報も提供されます。システムアクティビティについてどのように通知するかを設定したり、それらを完全に無効にしたりできます。また、特定のアラームのしきい値を設定できます。

大半のアラームには関連付けられているスケジュールがなく、イベント発生後即時に送信されます。その時点で最新の 15,000 件のアラームのみが保持されます。

イベントが繰り返し発生した場合、同じアラームは約 1 時間抑制されます。イベントが繰り返し発生する間は、トリガーに応じて、アラームが再び表示されるのに約 1 時間かかる場合があります。

次の表に、すべての Cisco ISE アラームおよびその説明と解決方法を示します。

表 *235 : Cisco ISE* アラーム

アラーム名	アラームの説明	アラームの解決方法
管理および操作の監査の管理		
展開のアップグレードの失敗（Deployment Upgrade Failure）	ISE ノードでアップグレードに失敗しました。	アップグレードが失敗した原因と修正措置について、失敗したノードの ADE.ログを確認します。
アップグレード バンドルのダウンロードの失敗（Upgrade Bundle Download failure）	アップグレード バンドルのダウンロードが ISE ノードで失敗しました。	アップグレードが失敗した原因と修正措置について、失敗したノードの ADE.ログを確認します。
SXP 接続障害（SXP Connection Failure）	SXP 接続に失敗しました。	SXP サービスが実行していることを確認します。ピアに互換性があることを確認します。
シスコ プロファイルの全デバイスへの適用（Cisco profile applied to all devices）	ネットワーク デバイス プロファイルによって、MAB、Dot1X、CoA、Web Redirect などのネットワーク アクセス デバイスの機能が定義されます。ISE 2.0 へのアップグレードにより、デフォルトのシスコ ネットワーク デバイス プロファイルがすべてのネットワーク デバイスに適用されました。	シスコ以外のネットワーク デバイスの設定を必要に応じて編集し、適切なプロファイルを割り当てます。
CRL で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続（Secure LDAP connection reconnect due to CRL found revoked certificate）	CRL チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。LDAP サーバ証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバにインストールします。

アラーム名	アラームの説明	アラームの解決方法
OCSP で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続（Secure LDAP connection reconnect due to OCSP found revoked certificate）	OCSP チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。LDAP サーバ証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバにインストールします。
CRL で失効した証明書が見つかったことによるセキュア syslog 接続の再接続（Secure syslog connection reconnect due to CRL found revoked certificate）	CRL チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。syslog サーバ証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバにインストールします。
OCSP で失効した証明書が見つかったことによるセキュアな syslog 接続の再接続（Secure syslog connection reconnect due to OCSP found revoked certificate）	OCSP チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。syslog サーバ証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバにインストールします。
管理者アカウントがロック/無効（Administrator account Locked/Disabled）	パスワードの失効または不正なログイン試行のために、管理者アカウントがロックされているか、または無効になっています。詳細については、管理者パスワード ポリシーを参照してください。	管理者パスワードは、GUI または CLI を使用して、他の管理者によってリセットできます。
ERS が非推奨の URL を検出（ERS identified deprecated URL）	ERS が非推奨の URL を検出しました。	要求された URL が非推奨であるため、使用しないでください。
ERS が古い URL を検出（ERS identified out-dated URL）	ERS が古い URL を検出しました。	要求された URL が古いため、新しいものを使用してください。この URL は今後のリリースで削除されません。

アラーム名	アラームの説明	アラームの解決方法
ERS 要求 Content-Type ヘッダーが古い（ERS request content-type header is outdated）	ERS 要求 Content-Type ヘッダーが最新ではありません。	要求 Content-Type ヘッダーで指定された要求のリソースバージョンが最新ではありません。これはリソース スキーマが変更されたことを意味します。いくつかの属性が追加または削除された可能性があります。古いスキーマをこのまま処理するために、ERS エンジンでデフォルト値が使用されます。
ERS XML 入力が XSS またはインジェクション攻撃の原因です（ERS XML input is a suspect for XSS or Injection attack）	ERS XML 入力が XSS またはインジェクション攻撃の原因になっています。	XML 入力を確認してください。
バックアップに失敗（Backup Failed）	ISEバックアップ操作に失敗しました。	Cisco ISE とリポジトリ間のネットワーク接続を確認します。次の点を確認します。 • リポジトリに使用するクレデンシャルが正しいこと。 • リポジトリに十分なディスク領域があること。 • リポジトリ ユーザが書き込み特権を持っていること。
CA サーバがダウン（CA Server is down）	CA サーバがダウンしています。	CA サービスが CA サーバで稼働中であることを確認します。
CA サーバが稼働中（CA Server is Up）	CA サーバは稼働中です。	CA サーバが稼働中であることを管理者に通知します。

アラーム名	アラームの説明	アラームの解決方法
証明書の有効期限（Certificate Expiration）	この証明書はまもなく有効期限が切れます。これが失効すると、Cisco ISE がクライアントとのセキュアな通信を確立しないようにします。	証明書を交換します。信頼できる証明書の場合、発行元の認証局（CA）にお問い合わせください。CA署名付きローカル証明書の場合、CSR を生成し、CAに新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書が失効（Certificate Revoked）	管理者は、内部 CA がエンドポイントに発行した証明書を取り消しました。	BYOD フローに従って最初から新しい証明書を使用してプロビジョニングします。
証明書プロビジョニング初期化エラー（Certificate Provisioning Initialization Error）	証明書プロビジョニングの初期化に失敗しました。	複数の証明書でサブジェクトのCN（CommonName）属性が同じ値になっており、証明書チェーンを構築できません。SCEPサーバからそれらを含むシステムのすべての証明書を確認します。
証明書の複製に失敗（Certificate Replication Failed）	セカンダリ ノードへの証明書の複製に失敗しました。	証明書がセカンダリ ノードで無効であるか、他の永続的なエラー状態があります。セカンダリ ノードに矛盾する証明書が存在しないかどうかを確認します。見つかった場合、セカンダリ ノードに存在するその証明書を削除し、プライマリの新しい証明書をエクスポートしてから削除し、その後インポートすることによって複製を再試行します。
証明書の複製に一時的に失敗（Certificate Replication Temporarily Failed）	セカンダリ ノードへの証明書の複製に一時的に失敗しました。	証明書は、ネットワークの停止などの一時的な条件によりセカンダリ ノードに複製されませんでした。複製は、成功するまで再試行されます。

アラーム名	アラームの説明	アラームの解決方法
証明書が失効（Certificate Expired）	この証明書の期限が切れています。Cisco ISE がクライアントとのセキュアな通信を確立しないようにします。ノードツーノード通信も影響を受ける場合があります。	証明書を交換します。信頼できる証明書の場合、発行元の認証局（CA）にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書要求転送に失敗（Certificate Request Forwarding Failed）	証明書要求転送に失敗しました。	受信する証明書要求が送信者からの属性に一致することを確認します。
設定が変更（Configuration Changed）	Cisco ISE 設定が更新されています。このアラームは、ユーザとエンドポイントに設定変更があってもトリガーされません。	設定変更が想定どおりであるかどうかを確認します。
CRL の取得に失敗（CRL Retrieval Failed）	サーバから CRL を取得できません。これは、指定した CRL が使用できない場合に発生することがあります。	ダウンロード URL が正しく、サービスに使用可能であることを確認します。
DNS 解決に失敗（DNS Resolution Failure）	ノードで DNS 解決に失敗しました。	コマンド **ip name-server** で設定した DNS サーバが到達可能であることを確認してください。 「CNAME <hostname of the node> に対する DNS 解決が失敗しました（DNS Resolution failed for CNAME <hostname of the node>）」というアラームが表示された場合は、各 Cisco ISE ノードの A レコードとともに CNAME RR を作成できることを確認します。

アラーム名	アラームの説明	アラームの解決方法
ファームウェアの更新が必要（Firmware Update Required）	このホスト上でファームウェアの更新が必要です。	Cisco Technical Assistance Center に問い合わせてファームウェア アップデートを入手してください。
仮想マシン リソースが不十分（Insufficient Virtual Machine Resources）	このホストでは、CPU、RAM、ディスク容量、IOPS などの仮想マシン（VM）リソースが不十分です。	Cisco ISE Hardware Installation Guide に指定されている VM ホストの最小要件を確認します。
NTP サービスの障害（NTP Service Failure）	NTP サービスがこのノードでダウンしています。	これは、NTP サーバと Cisco ISE ノードとの間に大きな時間差（1000 秒を超える）があるために発生することがあります。NTP サーバが正しく動作していることを確認し、**ntp server <servername>** CLI コマンドを使用して NTP サービスを再起動して、時間を同期します。
NTP 同期に失敗（NTP Sync Failure）	このノードに構成されているすべての NTP サーバが到達不能です。	CLI で **show ntp** コマンドを実行してトラブルシューティングを行います。Cisco ISE から NTP サーバに到達可能であることを確認します。NTP 認証が設定されている場合、キー ID と値がサーバの対応する値に一致することを確認します。
スケジュールされた設定バックアップなし（No Configuration Backup Scheduled）	Cisco ISE 設定バックアップがスケジュールされていません。	設定バックアップのスケジュールを作成します。
操作 DB 消去に失敗（Operations DB Purge Failed）	操作データベースから古いデータを消去できません。このことは、M&T ノードがビジー状態である場合に発生する可能性があります。	[データ消去の監査（Data Purging Audit）] レポートをチェックし、used_space が threshold_space を下回ることを確認します。CLI を使用して M&T ノードにログインし、消去操作を手動で実行します。

アラーム名	アラームの説明	アラームの解決方法
プロファイラ SNMP 要求に失敗（Profiler SNMP Request Failure）	SNMP 要求がタイム アウトしたか、または SNMP コミュニティまたはユーザ認証データが不正です。	SNMP が NAD で動作していることを確認し、Cisco ISE の SNMP 設定が NAD に一致していることを確認します。
複製に失敗（Replication Failed）	セカンダリ ノードは複製されたメッセージを消費できませんでした。	Cisco ISE GUI にログインし、展開ページから手動同期を実行します。影響を受ける Cisco ISE ノードを登録解除してから登録します。
復元に失敗（Restore Failed）	Cisco ISE 復元操作に失敗しました。	Cisco ISE とリポジトリ間のネットワーク接続を確認します。リポジトリに使用するクレデンシャルが正しいことを確認します。バックアップ ファイルが破損していないことを確認します。CLI で **reset-config** コマンドを実行して、正常な既知の最終バックアップを復元します。
パッチに失敗（Patch Failure）	パッチ プロセスがサーバで失敗しました。	サーバにパッチ プロセスを再インストールします。
パッチに成功（Patch Success）	パッチ プロセスがサーバで成功しました。	-
外部 MDM サーバ API バージョンが不一致（External MDM Server API Version Mismatch）	外部 MDM サーバ API バージョンが Cisco ISE に設定されたものと一致しません。	MDM サーバ API バージョンが Cisco ISE に設定されたものと同じであることを確認します。Cisco ISE MDM サーバ設定を更新します（必要な場合）。
外部 MDM サーバ接続に失敗（External MDM Server Connection Failure）	外部 MDM サーバへの接続に失敗しました。	MDM サーバが稼働し、Cisco ISE-MDM API サービスが MDM サーバで稼働していることを確認します。
外部 MDM サーバ応答エラー（External MDM Server Response Error）	外部 MDM サーバ応答エラーです。	Cisco ISE-MDM API サービスが MDM サーバで適切に動作していることを確認します。

アラーム名	アラームの説明	アラームの解決方法
複製が停止（Replication Stopped）	ISE ノードが PAN から設定データを複製できませんでした。	Cisco ISE GUI にログインして展開ページから手動同期を実行するか、または影響を受けた ISE ノードを登録解除してから必須フィールドで再登録します。
エンドポイント証明書が期限切れ（Endpoint certificates expired）	エンドポイント証明書が日次スケジュール ジョブで期限切れとマークされました。	エンドポイント デバイスを再登録して新しいエンドポイント証明書を取得してください。
エンドポイント証明書が消去（Endpoint certificates purged）	期限切れのエンドポイント証明書が日次スケジュール ジョブによって消去されました。	アクションは必要ありません。これは、管理者が開始したクリーンアップ操作です。
エンドポイントのアクティビティ消去（Endpoints Purge Activities）	過去 24 時間のエンドポイントのアクティビティを消去します。このアラームは、真夜中にトリガーされます。	**[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザ（Endpoints and Users）] > [エンドポイントのアクティビティ消去（Endpoints Purge Activities）]** で消去アクティビティを確認します。
複製低速エラー（Slow Replication Error）	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
複製低速情報（Slow Replication Info）	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
複製低速警告（Slow Replication Warning）	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
PAN 自動フェールオーバー：フェールオーバーが失敗しました（PAN Auto Failover - Failover Failed）	セカンダリ管理ノードへのプロモーション要求が失敗しました。	解決方法については、アラームの詳細を参照してください。
PAN 自動フェールオーバー：フェールオーバーがトリガーされました（PAN Auto Failover - Failover Triggered）	プライマリ ロールにセカンダリ管理ノードのフェールオーバーが正常にトリガーされました。	セカンダリ PAN のプロモーションが完了するまで待機し、古いプライマリ PAN を起動してください。

アラーム名	アラームの説明	アラームの解決方法
PAN 自動フェールオーバー：ヘルスチェックの非アクティビティ（PAN Auto Failover - Health Check Inactivity）	PAN がモニタリング ノードからヘルス チェックのモニタリング要求を受け取りませんでした。	報告されたモニタリング ノードがダウンまたは同期していないかどうかを確認し、必要な場合は手動で同期してください。
PAN 自動フェールオーバー：無効なヘルスチェック（PAN Auto Failover - Invalid Health Check）	自動フェールオーバーで無効なヘルス チェック モニタリング要求が受信されました。	ヘルス チェック モニタリング ノードが同期していることを確認し、必要な場合は手動で同期してください。
PAN 自動フェールオーバー：プライマリ管理ノードのダウン（PAN Auto Failover - Primary Administration Node Down）	プライマリ管理ノードがダウンしているか、またはモニタリング ノードから到達不能です。	PAN を起動して、フェールオーバーが発生するまで待機します。
PAN 自動フェールオーバー：フェールオーバーの試行が拒否されました（PAN Auto Failover - Rejected Failover Attempt）	ヘルス チェック モニタ ノードによって行われたプロモーション要求をセカンダリ管理ノードが拒否しました。	解決方法については、アラームの詳細を参照してください。
EST サービスの停止	EST サービスが停止しています。	CA および EST サービスが稼働しており、証明書サービスのエンドポイント サブ CA 証明書チェーンが完了したことを確認します。
EST サービスの稼働	EST サービスが稼働しています。	EST サービスが稼働中であることを管理者に通知します。
Smart Call Home の通信障害	Smart Call Home メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間でネットワーク接続があることを確認します。
テレメトリ メッセージの障害	テレメトリ メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間でネットワーク接続があることを確認します。
アダプタに接続できない	Cisco ISE は、アダプタに接続できません。	エラーの詳細はアダプタ ログを確認してください。
アダプタのエラー	アダプタにエラーが生じています。	アラームの説明を確認してください。

アラーム名	アラームの説明	アラームの解決方法
アダプタ接続の失敗	アダプタは、送信元のサーバに接続できません。	送信元のサーバがアクセス可能であることを確認してください
エラーによるアダプタの停止	アダプタにエラーが発生し、望ましい状態ではありません。	アダプタの設定が正しく、送信元サーバがアクセス可能であることを確認してください。エラーの詳細はアダプタログを確認してください。
サービス コンポーネントのエラー	サービス コンポーネントにエラーが生じています。	アラームの説明を確認してください。
サービス コンポーネントの情報	サービス コンポーネントが情報を送信しました。	なし。
ISE サービス		
過剰な TACACS 認証試行（Excessive TACACS Authentication Attempts）	ISE ポリシー サービス ノードで TACACS 認証の割合が想定よりも多くなっています。	ネットワーク デバイスの再認証タイマーをチェックします。ISEインフラストラクチャのネットワーク接続を確認します。
過剰な TACACS 認証の失敗した試行（Excessive TACACS Authentication Failed Attempts）	ISE ポリシー サービス ノードで失敗した TACACS 認証の割合が想定よりも多くなっています。	根本原因を特定するために認証手順を確認します。ID と秘密の不一致がないか、ISE/NAD 設定を確認します。
MSE ロケーション サーバへのアクセス回復（MSE Location Server accessible again）	MSE ロケーション サーバへのアクセスが回復しました。	なし。
MSE ロケーション サーバにアクセス不能（MSE Location Server not accessible.）	MSE ロケーション サーバはアクセス不能でダウンしています。	MSE ロケーション サーバが稼働中で、ISE ノードからアクセスできるかどうかを確認します。
AD コネクタを再起動する必要があります（AD Connector had to be restarted）	AD コネクタが突然シャットダウンし、再起動が必要となりました。	この問題が連続して発生する場合は、Cisco TAC にお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
Active Directory フォレストが使用不可（Active Directory forest is unavailable）	Active Directory フォレスト GC（グローバル カタログ）が使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
認証ドメインが使用不可（Authentication domain is unavailable）	認証ドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
ISE の認証非アクティビティ（ISE Authentication Inactivity）	Cisco ISE ポリシー サービス ノードは、ネットワーク デバイスから認証要求を受け取っていません。	ISE/NAD 設定を確認します。ISE/NAD インフラストラクチャのネットワーク接続を確認します。
ID マッピングの認証非アクティビティ（ID Map. Authentication Inactivity）	ユーザ認証イベントが過去 15 分に ID マッピング サービスによって収集されませんでした。	これがユーザ認証が想定される時間（たとえば、勤務時間）である場合は、Active Directory ドメイン コントローラへの接続を確認します。
CoA 失敗（COA Failed）	ネットワーク デバイスが、Cisco ISE ポリシー サービス ノードによって発行された許可変更（CoA）要求を拒否しました。	Cisco ISE から許可変更（CoA）を受け入れるようにネットワーク デバイスが設定されていることを確認します。CoA が有効なセッションに対して発行されているかどうかを確認します。
設定されたネーム サーバがダウン（Configured nameserver is down）	設定されたネーム サーバがダウンしているか、使用できません。	DNS 設定とネットワーク接続を確認します。

アラーム名	アラームの説明	アラームの解決方法
サプリカントが応答停止（Supplicant Stopped Responding）	Cisco ISE がクライアントに最後のメッセージを 120 秒前に送信しましたが、クライアントから応答がありません。	サプリカントが Cisco ISE との完全な EAP カンバセーションを行えるように適切に設定されていることを確認します。サプリカントとの間で EAP メッセージを転送するように NAS が正しく設定されていることを確認します。サプリカントまたはNAS で、EAP カンバセーションのタイムアウトが短くないことを確認します。
過剰な認証試行（Excessive Authentication Attempts）	Cisco ISE ポリシー サービス ノードで認証の割合が想定よりも多くなっています。	ネットワーク デバイスの再認証タイマーをチェックします。Cisco ISE インフラストラクチャのネットワーク接続を確認します。 しきい値が満たされた場合、[過剰な認証試行（Excessive Authentication Attempts）] および [過剰な失敗試行（Excessive Failed Attempts）] アラームがトリガーされます。[説明（Description）] カラムの横に表示される数値は、過去 15 分間で Cisco ISE に対して認証されたか失敗した認証の合計数です。

アラーム名	アラームの説明	アラームの解決方法
過剰な失敗試行（Excessive Failed Attempts）	Cisco ISE ポリシー サービス ノードで認証失敗の割合が想定よりも多くなっています。	根本原因を特定するために認証手順を確認します。ID と秘密の不一致がないか、Cisco ISE/NAD 設定を確認します。 しきい値が満たされた場合、[過剰な認証試行（Excessive Authentication Attempts）] および [過剰な失敗試行（Excessive Failed Attempts）] アラームがトリガーされます。[説明（Description）] カラムの横に表示される数値は、過去 15 分間で Cisco ISE に対して認証されたか失敗した認証の合計数です。
AD：マシン TGT のリフレッシュに失敗（AD: Machine TGT refresh failed）	ISE サーバ TGT（チケット認可チケット）のリフレッシュに失敗しました。これは AD 接続とサービスに使用されます。	ISE マシン アカウントが存在し、有効であることを確認します。また、クロック スキュー、複製、Kerberos 設定やネットワーク エラーも確認します。
AD：ISE アカウント パスワードの更新に失敗（AD: ISE account password update failed）	ISE サーバは、AD マシン アカウント パスワードを更新できませんでした。	ISE マシン アカウント パスワードが変更されていないことと、マシン アカウントが無効でなく制限もされていないことを確認します。KDC への接続を確認します。
参加しているドメインが使用不可（Joined domain is unavailable）	参加しているドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
ID ストアが使用不可（Identity Store Unavailable）	Cisco ISE ポリシー サービス ノードは設定された ID ストアに到達できません。	Cisco ISE と ID ストア間のネットワーク接続を確認します。
正しく設定されていないネットワーク デバイスを検出（Misconfigured Network Device Detected）	Cisco ISE は、NAS から多すぎる RADIUS アカウンティング情報を検出しました。	非常に多くの重複する RADIUS アカウンティング情報が、NAS から ISE に送信されました。正確なアカウンティング頻度で NAS を設定します。

アラーム名	アラームの説明	アラームの解決方法
正しく設定されていないサプリカントを検出（Misconfigured Supplicant Detected）	Cisco ISE は、ネットワーク上で正しく設定されていないサプリカントを検出しました。	サプリカントの設定が正しいことを確認します。
アカウンティングの開始なし（No Accounting Start）	Cisco ISE ポリシー サービス ノードではセッションを許可していますが、ネットワーク デバイスからアカウンティング開始を受信しませんでした。	RADIUS アカウンティングがネットワーク デバイス上に設定されていることを確認します。ローカル許可に対するネットワーク デバイス設定を確認します。
NAD が不明な（Unknown NAD）	Cisco ISE ポリシー サービス ノードは、Cisco ISE に設定されていないネットワーク デバイスから認証要求を受信しています。	ネットワーク デバイスが正規の要求であるかどうかを確認してから、それを設定に追加します。シークレットが一致することを確認します。
SGACL がドロップ（SGACL Drops）	セキュリティ グループ アクセス（SGACL）ドロップが発生しました。これは、SGACL ポリシーの違反により、TrustSec 対応デバイスがパケットをドロップすると発生します。	RBACL ドロップ概要レポートを実行し、SGACL ドロップを引き起こしているソースを確認します。攻撃ソースに CoA を発行してセッションを再許可または切断します。
RADIUS 要求がドロップ（RADIUS Request Dropped）	NAD からの認証とアカウンティング要求がサイレントに廃棄されています。これは、NAD が不明であるか、共有秘密鍵が不一致であるか、RFC ごとのパケット内容が無効であるために発生することがあります。	NAD/AAA クライアントについて Cisco ISE に有効な設定があることを確認します。NAD/AAA クライアントと Cisco ISE の共有秘密鍵が一致しているかどうかを確認します。AAA クライアントとネットワーク デバイスにハードウェアの問題または RADIUS 互換性の問題がないことを確認します。また、Cisco ISE にデバイスを接続するネットワークにハードウェア上の問題がないことを確認します。
EAP セッションの割り当てに失敗（EAP Session Allocation Failed）	RADIUS 要求は EAP セッションの制限に達したためにドロップされました。この状態の原因として、並列 EAP 認証要求が多すぎることが考えられます。	新しい EAP セッションで別の RADIUS 要求を呼び出す前に数秒間待ちます。システムのオーバーロードが発生する場合は、ISE サーバの再起動を試してください。

アラーム名	アラームの説明	アラームの解決方法
RADIUS コンテキストの割り当てに失敗（RADIUS Context Allocation Failed）	RADIUS 要求はシステムのオーバーロードのためにドロップされました。この状態の原因として、並列認証要求が多すぎることが考えられます。	新しい RADIUS 要求を呼び出す前に数秒間待ちます。システムのオーバーロードが発生する場合は、ISE サーバの再起動を試してください。
AD：ISE のマシン アカウントにグループを取得するために必要な権限がない	Cisco ISE のマシン アカウントにグループを取得するために必要な権限がありません。	Cisco ISE のマシン アカウントに Active Directory のユーザ グループを取得する権限があるかどうかを確認します。
システムの状態（System Health）		
ディスク I/O 使用率が高い（High Disk I/O Utilization）	Cisco ISE システムは、ディスク I/O 使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
ディスク領域の使用率が高い（High Disk Space Utilization）	Cisco ISE システムは、ディスク領域の使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。

アラーム名	アラームの説明	アラームの解決方法
負荷平均が高い（High Load Average）	Cisco ISE システムは、不可平均が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。 プライマリおよびセカンダリ MNT ノードの 2:00 a.m. タイムスタンプに対して [負荷平均が高い（High Load Average）] アラームが表示される場合、この時刻に実行している DBMS 統計が原因で CPU 使用率が高い可能性があります。DBMS 統計が完了すると、CPU 使用率は通常に戻ります。
メモリ使用率が高い（High Memory Utilization）	Cisco ISE システムは、メモリ使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。
操作DBの使用率が高い（High Operations DB Usage）	ノードをモニタする Cisco ISE は、syslog データの量が想定よりも多くなっています。	操作データの消去設定ウィンドウを確認して削減します。
認証待ち時間が長い（High Authentication Latency）	Cisco ISE システムは、認証待ち時間が長くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバを追加します。

アラーム名	アラームの説明	アラームの解決方法
ヘルス ステータスが使用不可（Health Status Unavailable）	モニタリング ノードは Cisco ISE ノードからヘルス ステータスを受信しませんでした。	Cisco ISE ノードが稼働中であることを確認します。Cisco ISE ノードがモニタリング ノードと通信できることを確認します。
プロセスがダウン（Process Down）	Cisco ISE プロセスの 1 つが動作していません。	Cisco ISE アプリケーションを再起動します。
プロファイラ キューサイズの制限に到達（Profiler Queue Size Limit Reached）	ISE プロファイラ キュー サイズの制限に到達しました。キュー サイズの制限に達した後に受信されたイベントはドロップされます。	システムに十分なリソースがあることを確認し、エンドポイント属性フィルタが有効になっていることを確認します。
OCSP トランザクションしきい値に到達	OCSP トランザクションしきい値に到達しました。このアラームは、内部 OCSP サービスが大量のトラフィックに到達するとトリガーされます。	システムに十分なリソースがあるかどうかを確認してください。
ライセンシング		
ライセンスがまもなく期限切れ（License About to Expire）	Cisco ISE ノードにインストールされたライセンスがまもなく期限切れになります。	Cisco ISE の [ライセンシング（Licensing）] ページを参照してライセンスの使用状況を確認します。
ライセンスが期限切れ（License Expired）	Cisco ISE ノードにインストールされたライセンスの期限が切れました。	シスコ アカウント チームに問い合わせて、新しいライセンスを購入してください。
ライセンス違反（License Violation）	Cisco ISE ノードは、許可されたライセンス数を超過しているか、まもなく超過することを検出しました。	シスコ アカウント チームに問い合わせて、追加のライセンスを購入してください。

アラーム名	アラームの説明	アラームの解決方法
スマート ライセンスの認証の期限切れ	スマート ライセンスの認証の有効期限が切れました。	[Cisco ISE ライセンス管理（Cisco ISE License Administration）]ページを参照して、手動でスマート ライセンスの登録を更新するか、Cisco Smart Software Manager とのネットワーク接続を確認してください。問題が続くようであれば、シスコ パートナーまでお問い合わせください。
スマート ライセンスの認証の更新の失敗	Cisco Smart Software Manager を使用した認証の更新に失敗しました。	[Cisco ISE ライセンス管理（Cisco ISE License Administration）]ページを参照し、[ライセンス（Licenses）]テーブルの [更新（Refresh）]ボタンを使用して、Cisco Smart Software Manager で、手動で認証を更新します。問題が続くようであれば、シスコ パートナーまでお問い合わせください。
スマート ライセンスの認証の更新の成功	Cisco Smart Software Manager を使用した認証の更新に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の認証の更新が完了したことを通知します。
スマート ライセンスの通信障害	Cisco Smart Software Manager と Cisco ISE の通信が失敗しました。	Cisco Smart Software Manager とのネットワーク接続を確認します。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコ パートナーまでお問い合わせください。
復元されたスマート ライセンスの通信	Cisco Smart Software Manager と Cisco ISE の通信が復元されました。	Cisco Smart Software Manager とのネットワーク接続が復元されたことを通知します。

アラーム名	アラームの説明	アラームの解決方法
スマート ライセンスの登録解除の障害	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に失敗しました。	詳細については、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ページを参照してください。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコ パートナーまでお問い合わせください。
スマート ライセンスの登録解除の成功	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の登録解除に成功したことを通知します。
スマート ライセンスの無効化	スマート ライセンスは Cisco ISE で無効になり、従来のライセンスが使用されています。	スマート ライセンスを再度有効にするには、[ライセンスの管理（License Administration）] ページを参照してください。Cisco ISE のスマート ライセンスの使用の詳細については、管理ガイドを参照するか、シスコ パートナーにお問い合わせください。
スマート ライセンスの評価期間の期限切れ	スマート ライセンスの評価期間が終了しました。	Cisco Smart Software Manager を使用して Cisco ISE を登録するには、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ページを参照してください。
スマート ライセンスの HA 役割の変更	スマート ライセンスの使用中に、ハイ アベイラビリティの役割の変更が発生しました。	Cisco ISE でのハイ アベイラビリティの役割が変化したことを通知します。
スマート ライセンス ID 証明書の期限切れ	スマート ライセンス証明書の期限が切れました。	手動でスマート ライセンスの登録を更新するには、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ページを参照してください。問題が続くようであれば、シスコ パートナーまでお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
スマート ライセンス ID 証明書の更新の失敗	Cisco Smart Software Manager を使用したスマート ライセンスの登録の更新が失敗しました。	手動でスマート ライセンスの登録を更新するには、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ページを参照してください。問題が続くようであれば、シスコ パートナーまでお問い合わせください。
スマート ライセンス ID 証明書の更新の成功	Cisco Smart Software Manager を使用したスマート ライセンスの登録の更新が成功しました。	Cisco Smart Software Manager を使用した登録の更新が成功したことを通知します。
スマート ライセンスの無効な要求	無効な要求が Cisco Smart Software Manager に送信されました。	詳細については、[Cisco ISE ライセンス管理（Cisco ISE License Administration）] ページを参照してください。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコ パートナーまでお問い合わせください。
コンプライアンスに準拠していないスマート ライセンス	Cisco ISE ライセンスがコンプライアンスに準拠していません。	詳細については、[ISE ライセンス管理（ISE License Administration）] ページを参照してください。新しいライセンスを購入するには、パートナーまたはシスコ アカウント チームにお問い合わせください。
スマート ライセンスの登録の障害	Cisco Smart Software Manager を使用した Cisco ISE の登録が失敗しました。	詳細については、[ISE ライセンス管理（ISE License Administration）] ページを参照してください。問題が続くようであれば、Cisco Smart Software Manager にログインするか、またはシスコ パートナーまでお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
スマート ライセンスの登録の成功	Cisco Smart Software Manager を使用した Cisco ISE の登録に成功しました。	Cisco Smart Software Manager を使用した Cisco ISE の登録が成功したことを通知します。
システム エラー		
ログ収集エラー（Log Collection Error）	コレクタ プロセスをモニタする Cisco ISE が、ポリシー サービス ノードから生成された監査ログを保持できません。	これは、ポリシー サービス ノードの実際の機能に影響を与えません。その他の解決のために TAC に連絡してください。
スケジュールされているレポートのエクスポートに失敗（Scheduled Report Export Failure）	設定されたリポジトリにエクスポートされたレポート（CSV ファイル）をコピーできません。	設定されたリポジトリを確認します。それが削除されていた場合は、再度追加します。それが使用できないか、またはそれに到達できない場合は、リポジトリを再設定して有効にします。
TrustSec		
不明な SGT のプロビジョニング（Unknown SGT was provisioned）	不明な SGT がプロビジョニングされました。	ISE は承認フローの一部として不明な SGT をプロビジョニングしました。不明な SGT は既知のフローの一部として割り当てることはできません。
一部の TrustSec ネットワーク デバイスに最新の ISE IP-SGT マッピング設定がありません（Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration）	一部の TrustSec ネットワーク デバイスに最新の ISE IP-SGT マッピング設定がありません。	ISE が異なる IP-SGT マッピング セットを持ついくつかのネットワーク デバイスを検出しました。[IP-SGT マッピング展開（IP-SGT mapping Deploy）] オプションを使用してデバイスを更新します。

アラーム名	アラームの説明	アラームの解決方法
TrustSec SSH 接続の失敗（TrustSec SSH connection failed）	TrustSec SSH 接続に失敗しました。	ISE がネットワーク デバイスへの SSH 接続を確立できませんでした。[ネットワーク デバイス（Network Device）] ページでネットワーク デバイスの SSH クレデンシャルがネットワーク デバイス上のクレデンシャルと類似していることを確認します。ネットワーク デバイスで ISE（IP アドレス）からの SSH 接続が有効になっていることを確認します。
TrustSec で識別された ISE は 1.0 以外の TLS バージョンで動作するよう設定されました（TrustSec identified ISE was set to work with TLS versions other then 1.0）	TrustSec で識別された ISE は 1.0 以外の TLS バージョンで動作するよう設定されています。	TrustSec は TLS バージョン 1.0 のみをサポートします。
TrustSec PAC の検証の失敗（Trustsec PAC validation failed）	TrustSec PAC の検証に失敗しました。	ISE がネットワーク デバイスから送信された PAC を検証できませんでした。[ネットワーク デバイス（Network Device）] ページとデバイスの CLI で、Trustsec デバイス クレデンシャルを確認します。デバイスが ISE サーバによってプロビジョニングされた有効な pac を使用していることを確認します。
TrustSec 環境データのダウンロードの失敗	TrustSec 環境データのダウンロードに失敗しました	Cisco ISE は不正な環境データ要求を受信しました。 次のことを確認してください。 • 要求に PAC が存在し有効である。 • すべての属性が要求に存在している。

アラーム名	アラームの説明	アラームの解決方法
TrustSec CoA メッセージの無視	TrustSec CoA メッセージは無視されました	Cisco ISE は、TrustSec CoA メッセージを送信し、応答を受信しませんでした。ネットワーク デバイスが CoA 対応であることを確認してください。ネットワーク デバイス設定を確認してください。
TrustSec のデフォルトの出力ポリシーの変更	TrustSec のデフォルトの出力ポリシーが変更されました。	TrustSec のデフォルトの出力ポリシーのセルが変更されました。セキュリティ ポリシーに合致していることを確認します。

アラームは、Cisco ISE にユーザまたはエンドポイントを追加する場合にはトリガーされません。

アラーム設定

次の表に、[アラーム設定（Alarm Settings）] ページのフィールドの説明を示します。（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarm Settings）]**）

フィールド	説明
アラーム タイプ（Alarm Type）	ドロップダウンリストからアラーム タイプを選択します。
アラーム名	アラームの名前を入力します。
説明	アラームの説明を入力します。
推奨されるアクション（Suggested Actions）	アラームがトリガーされるときに実行する推奨アクションを入力します。
ステータス	ステータスとして、アラーム ルールの [有効化（Enable）] または [無効化（Disable）] を選択します。

フィールド	説明
重大度（Severity）	ドロップダウン リスト ボックスを使用して、アラームの重大度レベルを選択します。有効なオプションは次のとおりです。 • [重大（Critical）]：重大なエラーの条件を示します。 • [警告（Warningi）]：正常ではあるものの重要な状態を示します。これがデフォルトの条件です。 • [情報（Info）]：情報メッセージを示します。
syslog メッセージを送信（Send Syslog Message）	Cisco ISE で生成される各システム アラームの syslog メッセージを送信する場合に、このチェックボックスをオンにします。
複数の電子メール アドレスをカンマで区切って入力（Enter Multiple Emails Separated with Comma）	電子メール アドレスまたは ISE 管理者名あるいはその両方のカンマ区切りリストを入力します。
電子メールのカスタム テキスト（Custom Text in Email）	システム アラームに関連付けるカスタム テキスト メッセージを入力します。

カスタム アラームの追加

Cisco ISE には [メモリ使用率が高い（High Memory Utilization）]、[設定変更（Configuration Change）] など 12 種類のデフォルト アラームがあります。Cisco によって定義されるシステム アラームは [アラーム設定（Alarms Settings）] ページに表示されます（[管理（(Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarms Settings）]）。システム アラームだけを編集できます。

既存のシステム アラームの他に、既存のアラーム タイプでカスタム アラームを追加、編集、削除できます。

各アラーム タイプで最大 5 つのアラームを作成でき、アラームの合計数は 200 に制限されます。

アラームを追加するには、次の手順を実行します。

ステップ 1 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarm Settings）] を選択します。

ステップ 2 [アラームの設定（Alarm Configuration）] タブで、[追加（Add）] をクリックします。

ステップ 3 次の必須詳細情報を入力します。詳細については、「アラーム設定」の項を参照してください。

アラーム タイプに基づいて（[メモリ使用率が高い（High Memory Utilization）]、[過剰な RADIUS 認証試行（Excessive RADIUS Authentication Attempts）]、[過剰な TACACS 認証試行（Excessive TACACS Authentication Attempts）] など）、追加の属性が [アラーム設定（Alarm Configuration）] ページに表示されます。たとえば、設定変更アラームには、[オブジェクト名（Object Name）]、[オブジェクト タイプ（Object Types）] および [管理者名（Admin Name）] フィールドが表示されます。さまざまな基準で同じアラームの複数のインスタンスを追加できます。

ステップ 4 [送信（Submit）] をクリックします。

Cisco ISE アラーム通知およびしきい値

Cisco ISE アラームを有効または無効にし、重大な状態を通知するようにアラーム通知動作を設定できます。特定のアラームに対して、過剰な失敗試行アラームの最大失敗試行数、または高ディスク使用量アラームの最大ディスク使用量などのしきい値を設定できます。

アラームごとに通知設定を設定できます。各アラームに対し通知する必要があるユーザの電子メール ID を入力できます（システム定義およびユーザ定義アラームの両方）。

（注） アラーム ルール レベルで指定された受信者の電子メール アドレスは、グローバルの受信者の電子メール アドレスより優先されます。

アラームの有効化および設定

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarm Settings）]** を選択します。

ステップ 2 デフォルト アラームのリストからアラームを選択して [編集（Edit）] をクリックします。

ステップ 3 [有効（Enable）] または [無効（Disable）] を選択します。

ステップ 4 アラームしきい値を必要に応じて設定します。

ステップ 5 [送信（Submit）] をクリックします。

モニタリング用の Cisco ISE アラーム

Cisco ISE は、重大なシステム状態が発生するたびに通知するシステム アラームを提供します。Cisco ISE によって生成されたアラームは [アラーム（Alarm）] ダッシュレットに表示されます。これらの通知は、自動的にアラーム ダッシュレットに表示されます。

アラーム ダッシュレットには最近のアラームのリストが表示され、ここから選択してアラームの詳細を表示できます。電子メールおよびsyslogメッセージを介してアラームの通知を受信することもできます。

モニタリング アラームの表示

ステップ 1 Cisco ISE **ダッシュボード**に進みます。

ステップ 2 [アラーム（Alarm）]ダッシュレットでアラームをクリックします。アラームの詳細および推奨アクションが表示された新しいウィンドウが開きます。

ステップ 3 アラームをリフレッシュするには、[リフレッシュ（Refresh）] をクリックします。

ステップ 4 選択したアラームを確認するには、[確認（Acknowledge）]をクリックします。タイムスタンプの前で使用可能なチェックボックスをクリックしてアラームを選択できます。これにより、読み取りとマークされているときに、アラーム カウンタ（アラームが発生した回数）が減少します。

ステップ 5 選択したアラームに対応する [詳細（Details）] リンクをクリックします。選択したアラームに対応する詳細が表示された新しいウィンドウが開きます。

（注） ペルソナの変更前に生成された以前のアラームに対応する [詳細（Details）] リンクに、データは表示されません。

ログ収集

モニタリング サービスはログと設定データを収集し、そのデータを保存してから、レポートおよびアラームを生成するために処理します。展開内の任意のサーバから収集されたログの詳細を表示できます。

アラーム syslog 収集場所

システム アラーム通知を syslog メッセージとして送信するようにモニタリング機能を設定した場合は、通知を受信する syslog ターゲットが必要です。アラーム syslog ターゲットは、アラーム syslog メッセージが送信される宛先です。

syslog メッセージを受信するには、syslog サーバとして設定されたシステムも必要です。アラーム syslog ターゲットを作成、編集、および削除できます。

（注） Cisco ISE モニタリングでは、logging-source interface の設定にネットワーク アクセス サーバ（NAS）の IP アドレスを使う必要があります。Cisco ISE モニタリング用のスイッチを設定する必要があります。

RADIUS ライブ ログ

次の表では、最近の RADIUS 認証を表示する [RADIUS ライブ ログ（RADIUS Live Logs）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）] > [RADIUS] > [ライブ ログ（Live Logs）]** です。RADIUS ライブ ログはプライマリ PAN だけで表示されます。

表 *236 : RADIUS* ライブ ログ

オプション	使用上のガイドライン
時刻（Time）	モニタリングおよび収集エージェントがログを受信した時刻を表示します。このカラムは必須です。選択解除することはできません。
ステータス（Status）	認証が成功したか失敗したかを示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。

オプション	使用上のガイドライン
詳細（Details）	[詳細（Details）] 列の下にあるアイコンをクリックすると、新しいブラウザウィンドウに [認証詳細レポート（Authentication Detail Report）] が表示されます。このレポートには、認証と関連属性のほか、認証フローに関する情報が記載されています。[認証の詳細（Authentications Details）] ボックスの [応答時間（Response Time）] には、Cisco ISE で認証フローを処理するのにかかった合計時間が示されます。たとえば、認証が 3 つのラウンドトリップメッセージで構成されている場合（最初のメッセージには300ミリ秒、次のメッセージには150ミリ秒、最後のメッセージには100ミリ秒かかる）、応答時間は、300＋150＋100 = 550 750 ミリ秒になります。 （注） 48時間を超えるアクティブになっているエンドポイントの詳細を表示することはできません。48時間を超えるアクティブになっているエンドポイントの詳細アイコンをクリックすると、次のメッセージがページに表示される場合があります：`No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.`
繰り返し回数（Repeat Count）	ID、ネットワークデバイス、および許可のコンテキストで変更がなく、直近の24時間で認証要求が繰り返された回数を表示します。

オプション	使用上のガイドライン
ID（Identity）	ログイン済みの認証に関連付けられているユーザ名を示します。 ユーザ名が ID ストアに存在しない場合は、「無効（INVALID）」と表示されます。その他の原因で認証に失敗した場合は、「ユーザ名（USERNAME）」と表示されます。 デバッグをサポートするために、無効なユーザ名の開示をISEに強制することもできます。[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS] > [抑制とレポート（Suppression & Reports）] > [認証の詳細（Authentication Details）] で [無効なユーザ名を開示する（Disclose invalid usernames）] チェックボックスをオンにします。このオプションは、30分後に自動的に無効になります。
エンドポイント ID（Endpoint ID）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。
エンドポイント プロファイル（Endpoint Profile）	プロファイリングされるエンドポイントのタイプを示します（たとえば、iPhone、Android、MacBook、Xbox になるようにプロファイリングされます）。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（Authorization Policy）	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル（Authorization Profiles）	認証に使用された許可プロファイルを表示します。
IP アドレス（IP Address）	エンドポイントデバイスの IP アドレスを表示します。
ネットワークデバイス（Network Device）	ネットワーク アクセス デバイスの IP アドレスを表示します。
デバイスポート（Device Port）	エンドポイントが接続されているポート番号を表示します。

オプション	使用上のガイドライン
ID グループ（Identity Group）	ログの生成対象となるユーザまたはエンドポイントに割り当てられる ID グループを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
サーバ（Server）	ログの生成元になったポリシーサービスが示されます。
MDMサーバ名（MDM Server Name）	MDM サーバの名前を表示します。
イベント（Event）	イベントステータスを表示します。
失敗の理由（Failure Reason）	認証が失敗した場合、その失敗の詳細な理由を表示します。
認証方式（Auth Method）	Microsoft チャレンジハンドシェイク認証プロトコルバージョン 2（MS-CHAPv2）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（Authentication Protocol）	Protected Extensible Authentication Protocol（PEAP）や拡張認証プロトコル（EAP）など、使用される認証プロトコルを表示します。
セキュリティ グループ（Security Group）	認証ログによって識別されるグループを表示します。
セッション ID（Session ID）	セッション ID を表示します。

（注） [RADIUS ライブ ログ（RADIUS Live Logs）] と [TACACS+ ライブ ログ（TACACS+ Live Logs）] 詳細ペインでは、各ポリシー許可ルールの 1 番目の属性として [照会済み PIP（Queried PIP）] が表示されます。許可ルール内のすべての属性が、以前のルールについてすでに照会されているディクショナリに関連している場合、これ以外に [照会済み PIP（Queried PIP）] エントリは表示されません。

[RADIUS ライブ ログ（RADIUS Live Logs）] ページで、次を実行できます。

- データを csv または pdf ファイル形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタリングします。後で使用するためにフィルタを保存することもできます。

- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） すべてのユーザのカスタマイズは、ユーザ設定として保存されます。

関連トピック

ライブ認証のモニタ （1570 ページ）
ライブ認証 （1569 ページ）

ライブ認証

[ライブ認証（Live Authentications）] ページから、発生した最近の RADIUS 認証をモニタできます。このページには、直近の 24 時間での上位 10 件の RADIUS 認証が表示されます。この項では、[ライブ認証（Live Authentications）] ページの機能について説明します。

[ライブ認証（Live Authentications）] ページには、認証イベントの発生時に、その認証イベントに対応するライブ認証エントリが表示されます。認証エントリに加えて、このページには、そのイベントに対応するライブ セッション エントリも表示されます。また、目的のセッションをドリルダウンして、そのセッションに対応する詳細レポートを表示することもできます。

[ライブ認証（Live Authentications）] ページには、最近の RADIUS 認証が発生順に表形式で表示されます。[ライブ認証（Live Authentications）] ページの下部に表示される最終更新には、サーバ日付、時刻、およびタイムゾーンが示されます。

（注） アクセス要求パケット内のパスワード属性が空の場合は、エラーメッセージがトリガーされ、アクセス要求は失敗します。

1 つのエンドポイントが正常に認証されると、2 つのエントリが [ライブ認証（Live Authentications）]ページに表示されます。1 つは認証レコードに対応し、もう 1 つは（セッション ライブ ビューからプルされた）セッション レコードに対応しています。その後、デバイスで別の認証が正常に実行されると、セッション レコードに対応する繰り返しカウンタの数が増えます。[ライブ認証（Live Authentications）] ページに表示される繰り返しカウンタには、抑制されている重複した RADIUS 認証成功メッセージの数が示されます。

「最近の RADIUS 認証」の項で説明されているデフォルトで表示されるライブ認証データ カテゴリを参照してください。

すべてのカラムを表示するか、選択したデータ カラムのみを表示するように選択できます。表示するカラムを選択した後で、選択を保存できます。

ライブ認証のモニタ

ステップ 1 **[操作（Operations）]** > **[RADIUSライブログ（RADIUS Livelog）]** の順に選択します。

ステップ 2 データ リフレッシュ レートを変更するには、[更新（Refresh）] ドロップダウン リストから時間間隔を選択します。

ステップ 3 データを手動で更新するには、[更新（Refresh）] アイコンをクリックします。

ステップ 4 表示されるレコードの数を変更するには、[表示（Show）] ドロップダウンリストからオプションを選択します。

ステップ 5 時間間隔を指定するには、[次の範囲内（Within）] ドロップダウン リストからオプションを選択します。

ステップ 6 表示されるカラムを変更するには、[カラムの追加または削除（Add or Remove Columns）] をクリックし、ドロップダウン リストからオプションを選択します。

ステップ 7 ドロップダウン リストの下部にある [保存（Save）] をクリックして、変更を保存します。

ステップ 8 ライブ RADIUS セッションを表示するには、[ライブ セッションの表示（Show Live Sessions）] をクリックします。

アクティブな RADIUS セッションを動的に制御できるライブ セッションの動的な許可変更（CoA）機能を使用できます。ネットワーク アクセス デバイス（NAD）に再認証または接続解除要求を送信できます。

[ライブ認証（Live Authentications）] ページでのデータのフィルタリング

[ライブ認証（Live Authentications）] ページのフィルタを使用して、必要な情報をフィルタリングし、ネットワーク認証の問題を迅速にトラブルシューティングできます。[認証（ライブログ）（Authentication (live logs)）] ページのレコードをフィルタして、目的のレコードのみを表示できます。認証ログには多数の詳細が含まれており、特定のユーザまたはロケーションから認証をフィルタリングすると、データをすばやくスキャンするために役立ちます。[ライブ認証（Live Authentications）]ページの各種フィールドで使用できる複数の演算子を使用して、検索基準に基づいてレコードをフィルタリングできます。

- 「abc」：「abc」を含む
- 「!abc」：「abc」を含まない
- 「{}」：空
- 「!{}」：空でない
- 「abc*」：「abc」で開始する
- 「*abc」：「abc」で終了する
- 「\!」、「*」、「\{」、「\\」：エスケープ

エスケープオプションを使用すると、特殊文字を含むテキストをフィルタリングできます（フィルタとして使用される特殊文字を含む）。特殊文字の前にバック スラッシュ（\）を付ける必要があります。たとえば、「Employee!」という ID を持つユーザの認証レコードを確認する場

合は、ID フィルタ テキスト ボックスに "Employee\!" と入力します。この例では、Cisco ISE は感嘆符（!）を特殊文字ではなくリテラル文字と見なします。

また、[ステータス（Status）] フィールドでは、成功した認証レコード、失敗した認証、ライブ セッションなどのみをフィルタリングできます。緑色のチェック マークは以前発生したすべての成功した認証をフィルタリングします。赤い十字マークはすべての失敗した認証をフィルタリングします。青い [i] アイコンはすべてのライブ セッションをフィルタリングします。これらのオプションの組み合わせを表示することも選択できます。

ステップ 1 **[操作（Operations）]** > **[RADIUS ライブログ（RADIUS Livelog）]** の順に選択します。

ステップ 2 [ライブ認証の表示（Show Live Authentications）] ページのいずれかのフィールドに基づいてデータをフィルタリングします。

成功または失敗した認証、あるいはライブ セッションに基づいて結果をフィルタリングできます。

RADIUS ライブ セッション

次の表では、ライブ認証が表示される [RADIUS ライブ セッション（RADIUS live sessions）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[操作（Operations）]** > **[RADIUS]** > **[ライブセッション（Live Sessions）]** です。RADIUS ライブ セッションはプライマリ PAN だけで表示されます。

表 *237 : RADIUS* ライブ セッション

フィールド	説明
開始（Initiated）	セッション開始時のタイムスタンプを表示します。
更新しました	何らかの変更のためにセッションが最後に更新された時点のタイムスタンプを表示します。
アカウント セッション時間（Account Session Time）	ユーザ セッションの期間（秒単位）を表示します。
セッション ステータス（Session Status）	エンドポイント デバイスの現在のステータスを表示します。
アクション（CoA Action）	アクティブな RADIUS セッションを再認証するか、またはアクティブな RADIUS セッションを切断するには、[アクション（Actions）] アイコンをクリックします。
繰り返し回数（Repeat Count）	ユーザまたはエンドポイントの再認証回数を示します。

フィールド	説明
エンドポイント ID（Endpoint ID）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。
ID（Identity）	エンドポイント デバイスのユーザ名を表示します。
[IPアドレス（IP Address）]	エンドポイントデバイスのIPアドレスを表示します。
監査セッション ID（Audit Session ID）	固有のセッション ID を表示します。
アカウント セッション ID（Account Session ID）	ネットワーク デバイスから提供された固有IDを表示します。
エンドポイント プロファイル（Endpoint Profile）	デバイスのエンドポイント プロファイルを表示します。
ポスチャ ステータス（Posture Status）	ポスチャ検証のステータスと認証の詳細を表示します。
セキュリティ グループ（Security Group）	認証ログによって識別されるグループを表示します。
サーバ	ログを生成したポリシー サービス ノードを示します。
認証方式（Auth Method）	パスワード認証プロトコル（PAP）、チャレンジ ハンドシェイク認証プロトコル（CHAP）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。
認証プロトコル（Authentication Protocol）	Protected Extensible Authentication Protocol（PEAP）や拡張認証プロトコル（EAP）など、使用される認証プロトコルを表示します。
認証ポリシー（Authentication policy）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー	特定の許可に選択されているポリシーの名前を表示します。
認証プロファイル	認証に使用された許可プロファイルを表示します。
NAS IP アドレス	ネットワーク デバイスのIPアドレスを表示します。

フィールド	説明
デバイス ポート（Device Port）	ネットワーク デバイスに接続されたポートを表示します。
PRA アクション（PRA Action）	ネットワークでのコンプライアンスのためにクライアントが正常にポスチャされた後、そのクライアントで実行される定期的な再評価アクションを表示します。
ANCステータス（ANC Status）	[隔離（Quarantine）]、[隔離解除（Unquarantine）]、または [シャットダウン（Shutdown）] としてデバイスの適応型ネットワーク制御のステータスを表示します。
WLC ローミング（WLC Roam）	エンドポイントがローミング中にWLC間でハンドオフされたことを追跡するために使用されるブール値（Y/N）を表示します。cisco-av-pair=nas-update の値は Y または N です。 （注） セッションの状態がローミングであるかどうかを判断する場合、Cisco ISE は WLC の nas-update=true 属性に依存しています。元の WLC が nas-update=true のアカウンティング停止属性を送信する場合、再認証を回避するために ISE のセッションは削除されません。何らかの理由でローミングが失敗する場合、ISE は何も操作しない期間が 5 日経過するとセッションを消去します。
パケット入力	受信したパケットの数を表示します。
パケット出力	送信したパケットの数を表示します。
受信バイト数（Bytes In）	受信したバイト数を表示します。
送信バイト数（Bytes Out）	送信したバイト数を表示します。
セッション送信元（Session Source）	RADIUS セッションまたは PassiveID セッションのいずれであるかを示します。
ユーザドメイン名（User Domain Name）	ユーザの登録済み DNS 名を示します。
ホストドメイン名（Host Domain Name）	ホストの登録済み DNS 名を示します。
ユーザNetBIOS名（User NetBIOS Name）	ユーザの NetBIOS 名を示します。

フィールド	説明
ホストNetBIOS名（Host NetBIOS Name）	ホストの NetBIOS 名を示します。
ライセンスのタイプ（License Type）	使用されているライセンスのタイプ（Base、Plus、Apex、または Plus and Apex）を表示します。
ライセンスの詳細（License Details）	ライセンスの詳細を表示します。
プロバイダー	エンドポイント イベントはさまざまな syslog ソースから学習されます。これらの syslog ソースはプロバイダーと呼ばれます。 • Windows Management Instrumentation（WMI）：WMI は、オペレーティング システム、デバイス、アプリケーション、およびサービスに関する管理情報にアクセスするための共通インターフェイスとオブジェクト モデルを提供する Windows サービスです。 • エージェント：クライアントまたは別のプログラムの代わりにクライアントで実行されるプログラム。 • syslog：クライアントがイベント メッセージを送信するロギング サーバ。 • REST：クライアントはターミナル サーバで認証されます。この syslog ソースの場合、[TS エージェント ID（TS Agent ID）]、[開始送信元ポート（Source Port Start）]、[終了送信元ポート（Source Port End）]、[最初の送信元ポート（Source First Port）] の値が表示されます。 • SPAN：ネットワーク情報は SPAN プローブを使用して検出されます。 • DHCP：DHCP イベント。 • エンドポイント（Endpoint） 異なるプロバイダーからの 2 つのイベントがエンドポイントセッションから学習されると、ライブ セッション ページにこれらのプロバイダーがカンマ区切り値として表示されます。
MAC アドレス	クライアントの MAC アドレスを表示します。

フィールド	説明
[エンドポイントチェック時刻（Endpoint Check Time）]	エンドポイント プローブによってエンドポイントが最後にチェックされた時刻を表示します。
[エンドポイントチェック結果（Endpoint Check Result）]	エンドポイント プローブの結果が表示されます。設定可能な値は次のとおりです。 • 到達不要 • [ユーザ ログアウト（User Logout）] • [アクティブ ユーザ（Active User）]
[送信元ポートの開始（Source Port Start）]	（RESTプロバイダーの場合にのみ値が表示されます。）ポート範囲の最初のポートの番号を示します。
[送信元ポートの終了（Source Port End）]	（RESTプロバイダーの場合にのみ値が表示されます。）ポート範囲の最後のポート番号を示します。
[最初の送信元ポート（Source First Port）]	（RESTプロバイダーの場合にのみ値が表示されます。）ターミナルサーバ（TS）エージェントにより割り当てられた最初のポートを示します。 ターミナルサーバ（TS）は、複数のエンドポイントがモデムまたはネットワーク インターフェイスなしで接続でき、複数エンドポイントがLANネットワークに接続できるようにするサーバまたはネットワーク デバイスです。複数のエンドポイントに同一 IP アドレスが割り当てられている場合は、特定ユーザの IP アドレスを識別することが困難になります。このため、特定ユーザを識別する目的でTSエージェントがサーバにインストールされ、各ユーザにポート範囲が割り当てられます。これにより、IP アドレス - ポート - ユーザのマッピングが作成されます。
[TS エージェント ID（TS Agent ID）]	（RESTプロバイダーの場合にのみ値が表示されます。）エンドポイントにインストールされているターミナルサーバ（TS）エージェントの一意の ID を表示します。

フィールド	説明
[AD ユーザ解決 ID（AD User Resolved Identities）]	（AD ユーザの場合にのみ値が表示されます。）一致したアカウントの候補が表示されます。
[AD ユーザ解決 DN（AD User Resolved DNs）]	（AD ユーザの場合にのみ値が表示されます。）AD ユーザの識別名（例：CN=chris,CN=Users,DC=R1,DC=com）を表示します。

関連トピック

RADIUS セッションの許可の変更 （305 ページ）
Cisco ISE のアクティブな RADIUS セッション （304 ページ）

認証概要レポート

認証要求に関連する属性に基づいて、特定のユーザ、デバイス、または検索条件についてネットワーク アクセスをトラブルシューティングできます。このことは、認証概要レポートを実行して行います。

ネットワーク アクセスの問題のトラブルシューティング

ステップ 1 **[操作（Operations）] > [レポート（Reports）] > [認証概要レポート（Authentication Summary Report）]** を選択します。

ステップ 2 失敗の理由でレポートをフィルタリングします。

ステップ 3 レポートの [失敗の理由別の認証（Authentication by Failure Reasons）] セクションのデータを確認し、ネットワーク アクセスの問題をトラブルシューティングします。

（注） 認証概要レポートが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。

診断トラブルシューティング ツール

診断ツールは、Cisco ISE ネットワークの問題の診断およびトラブルシューティングに役立ち、問題解決方法の詳細な手順を提供します。これらのツールを使用して、認証をトラブルシューティングし、TrustSec デバイスなどのネットワーク上のネットワーク デバイスの設定を評価できます。

RADIUS 認証のトラブルシューティング ツール

このツールを使用すると、予期せぬ認証結果がある場合に、RADIUS 認証または RADIUS 認証に関連する Active Directory を検索および選択して、トラブルシューティングを実行することができます。認証が成功すると予想していたのに失敗した場合、またはユーザやマシンが特定の特権レベルを持っていると予想したのにユーザやマシンがこれらの特権を持っていなかった場合は、このツールを使用できます。

- トラブルシューティングのために、ユーザ名、エンドポイント ID、ネットワーク アクセス サービス（NAS）の IP アドレス、および認証失敗理由に基づいて RADIUS 認証を検索すると、Cisco ISE はシステム（現在）の日付の認証だけを表示します。
- トラブルシューティングのために NAS ポートに基づいて RADIUS 認証を検索すると、Cisco ISE は前月の初めから現在までのすべての NAS ポート値を表示します。

（注） NAS IP アドレスおよび [エンドポイント ID（Endpoint ID）] フィールドに基づいて RADIUS 認証を検索する場合、検索はまず運用データベースで実行され、その後設定データベースで実行されます。

予期せぬ RADIUS 認証結果のトラブルシューティング

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > > [一般ツール（General Tools）] > [RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）]** を選択します。

ステップ 2 必要に応じてフィールドに検索基準を指定します。

ステップ 3 [検索（Search）] をクリックして、検索条件に一致する RADIUS 認証を表示します。

AD 関連の認証を検索する際に、展開に Active Directory サーバが設定されていない場合は、「AD が設定されていない」ことを示すメッセージが表示されます。

ステップ 4 テーブルから RADIUS 認証レコードを選択し、[トラブルシューティング（Troubleshoot）] をクリックします。

AD 関連の認証をトラブルシューティングする必要がある場合は、[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] > [AD ノード（AD node）] で、診断ツールに移動します。

ステップ 5 [ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更して、[送信（Submit）] をクリックします。

ステップ 6 [完了（Done）] をクリックします。

ステップ 7 トラブルシューティングが完了したら、[結果概要の表示（Show Results Summary）] をクリックします。

ステップ 8 診断、問題を解決するための手順、およびトラブルシューティング概要を表示するには、[完了（Done）] をクリックします。

Execute Network Device Command 診断ツール

Execute Network Device Command 診断ツールを使用すると、ネットワーク デバイスに対して **show** コマンドを実行することができます。結果は、コンソールに表示される場合とまったく同じ形式であり、デバイスの設定における問題を特定するために使用できます。設定が間違っていると思われる場合や、設定を検証したい場合、または単にどのように設定されているか関心がある場合に、使用することができます。

設定を確認する IOS show コマンドの実行

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [ネットワーク デバイス コマンドの実行（Execute Network Device Command）]** を選択します。

ステップ 2 該当するフィールドに情報を入力します。

ステップ 3 [実行（Run）] をクリックして、指定したネットワーク デバイスでコマンドを実行します。

ステップ 4 [ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更します。

ステップ 5 [送信（Submit）] をクリックして、ネットワーク デバイス上でコマンドを実行し、出力を表示します。

設定バリデータ ツールの評価

この診断ツールを使用して、ネットワーク デバイスの設定を評価し、設定の問題を特定できます。Expert Troubleshooter によって、デバイスの設定が標準設定と比較されます。

ネットワーク デバイス設定の問題のトラブルシューティング

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [設定バリデータの評価（Evaluate Configuration Validator）]** を選択します。

ステップ 2 設定を評価するデバイスのネットワーク デバイス IP アドレスを入力し、必要に応じて他のフィールドを指定します。

ステップ 3 推奨テンプレートと比較する設定オプションを選択します。

ステップ 4 [実行（Run）] をクリックします。

ステップ 5 [ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更します。

ステップ 6 分析するインターフェイスの隣のチェックボックスをオンにして、[送信（Submit）] をクリックします。

ステップ 7 [結果概要の表示（Show Results Summary）] をクリックします。

エンドポイント ポスチャの障害のトラブルシューティング

ステップ 1 **[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般ツール（General Tools）]** > **[ポスチャのトラブルシューティング（Posture Troubleshooting）]** を選択します。

ステップ 2 該当するフィールドに情報を入力します。

ステップ 3 [検索（Search）] をクリックします。

ステップ 4 説明を見つけ、イベントの解決策を決定するには、リストでイベントを選択し、[トラブルシューティング（Troubleshoot）] をクリックします。

セッション トレース テスト ケース

このツールでは、予測できる方法でポリシー フローをテストし、実際のトラフィックを実際のデバイスから発信することなく、ポリシーの設定方法を確認、検証できます。

テスト ケースで使用する属性と値のリストを設定できます。この詳細情報を使用して、ポリシー システムとのやりとりが行われ、実行時のポリシー呼び出しがシミュレートされます。

属性はディクショナリを使用して設定できます。[属性（Attributes）] フィールドに、単純な RADIUS 認証で使用可能なディクショナリがすべて示されます。

（注） 単純な RADIUS 認証のテスト ケースのみを設定できます。

セッション トレース テスト ケースの設定

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [セッション トレース テスト ケース（Session Trace Test Cases）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [テストの詳細（Test Details）] タブで、テスト ケースの名前と説明を入力します。

ステップ 4 事前定義テスト ケースを 1 つ選択するか、または必須属性とその値を設定します。使用可能な事前定義テスト ケースを次に示します。

- [基本認証済みアクセス（Basic Authenticated Access）]
- [プロファイリングされている Cisco Phone（Profiled Cisco Phones）]
- [準拠デバイス アクセス（Compliant Devices Access）]
- [Wi-Fi ゲスト（リダイレクト）（Wi-Fi Guest (Redirect)）]
- [Wi-Fi ゲスト（アクセス）（Wi-Fi Guest (Access)）]

事前定義テスト ケースを選択すると、Cisco ISE によりそのテスト ケースの関連する属性に自動的に値が取り込まれます。これらの属性のデフォルト値を使用するか、または表示されるオプションから目的の値を選択することができます。また、テスト ケースにカスタム属性を追加することもできます。

テスト ケースに追加する属性と値は、（[カスタム属性（Custom Attributes）] フィールドの下の）[テキスト（Text）] フィールドに示されます。[テキスト（Text）] フィールドの内容を編集すると、Cisco ISE により更新後の内容の有効性と構文がチェックされます。

[テストの詳細（Test Details）] ページの下部に、すべての属性の概要が表示されます。

ステップ 5 [送信（Submit）] をクリックして、テスト ケースを作成します。

Cisco ISE はテストの詳細を保存する前に、属性とその値を検証してエラーがある場合はエラーを表示します。

ステップ 6 [テスト ビジュアライザ（Test Visualizer）] タブで、このテスト ケースを実行するノードを選択します。

[ISE ノード（ISE Node）] ドロップダウン リストには、ポリシー サービス ペルソナを担当するノードだけが表示されます。

[ユーザ グループ/属性（User Groups/Attributes）] をクリックして、外部 ID ストアからユーザのグループと属性を取得します。

ステップ 7 [実行（Execute）] をクリックします。

Cisco ISE はテスト ケースを実行し、テスト ケースのステップごとの結果を表形式で表示します。ポリシー ステージ、一致ルール、結果オブジェクトが表示されます。緑色のアイコンをクリックして各ステップの詳細を表示します。

ステップ 8 [以前のテスト実行（Previous Test Executions）] タブをクリックし、以前のテスト実行結果を表示します。また、2 つのテスト ケースを選択して比較することもできます。Cisco ISE では、各テスト ケースの属性の比較ビューが表形式で表示されます。

[RADIUS ライブ ログ（RADIUS Live Logs）] ページから [セッション トレース テスト ケース（Session Trace Test Case）] ツールを起動できます。[セッション トレース テスト ケース（Session Trace Test Case）] ツールを起動するには、[ライブ ログ（Live Logs）] ページでエントリを選択し、（[詳細（Details）] 列の）[アクション（Actions）] アイコンをクリックします。Cisco

ISEにより、対応するログエントリから関連する属性と値が抽出されます。必要に応じてこれらの属性と値を変更してから、テスト ケースを実行できます。

高度なトラブルシューティングのテクニカルサポートのトンネル

Cisco ISE は、Cisco IronPort トンネル インフラストラクチャを使用して、ISE サーバに接続してシステムの問題をトラブルシューティングするための、シスコ テクニカル サポート エンジニア用のセキュア トンネルを作成します。Cisco ISE は SSH を使用して、トンネル経由のセキュアな接続を作成します。

管理者として、トンネル アクセスを制御できます。サポート エンジニアにアクセス権を付与する時期と期間を選択できます。シスコ カスタマー サポートは、ユーザの介入なしにトンネルを確立できません。サービス ログインに関する通知を受信します。任意の時点でトンネル接続をディセーブルにできます。デフォルトでは、テクニカル サポート トンネルは 72 時間開いたままになりますが、すべてのトラブルシューティング作業が完了したら、ご自身またはサポート エンジニアがトンネルを閉じることを推奨します。必要に応じて、72 時間を超えてトンネルを延長することもできます。

tech support-tunnel enable コマンドを使用して、トンネル接続を開始できます。

tech support-tunnel status コマンドでは、接続のステータスが表示されます。このコマンドでは、接続が確立されたかどうか、または認証エラーがあるかどうか、あるいはサーバが到達不能であるかどうかに関する情報が提示されます。トンネル サーバは到達可能であるが ISE が認証できない場合、ISE は 30 分にわたり 5 分ごとに再認証を試行し、その後トンネルは無効になります。

tech support-tunnel disable コマンドを使用して、トンネル接続を無効にできます。このコマンドでは、サポートエンジニアが現在ログインしている場合も既存のトンネルが切断されます。

ISE サーバからのトンネル接続をすでに確立している場合は、生成される SSH キーを ISE サーバで使用できます。後でサポート トンネルをイネーブルにしようとすると、システムによって、以前に生成された SSH キーを再使用するよう指示されます。同じキーを使用するか、または新しいキーを生成するかを選択できます。また、**tech support-tunnel resetkey** コマンドを使用してキーを手動でリセットすることもできます。トンネル接続が有効な場合にこのコマンドを実行すると、先に接続をディセーブルにするよう求めるプロンプトが表示されます。既存の接続を続け、無効にしないことを選択した場合、キーは既存の接続が無効になった後でリセットされます。接続を無効にすることを選択した場合、トンネル接続はドロップされ、キーは即座にリセットされます。

トンネル接続の確立後に、**tech support-tunnel extend** コマンドを使用して拡張することができます。

tech support-tunnel コマンドの使用上のガイドラインについては、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

テクニカル サポート トンネルの確立

Cisco ISE コマンドライン インターフェイス（CLI）からセキュア トンネルを確立できます。

ステップ 1 Cisco ISE CLI から、次のコマンドを入力します。

tech support-tunnel enable

トンネルのパスワードとニックネームの入力が求められます。

ステップ 2 パスワードを入力します。

ステップ 3 （任意）トンネルのニックネームを入力します。

システムによって SSH キーが生成され、パスワード、デバイスのシリアル番号および SSH キーが表示されます。サポート エンジニアがシステムに接続できるように、この情報をシスコ カスタマー サポートに渡す必要があります。

ステップ 4 パスワード、デバイスのシリアル番号および SSH キーをコピーし、シスコ カスタマー サポートに送信します。

これで、サポート エンジニアが ISE サーバに安全に接続できるようになります。サービス ログに関する定期的な通知を受信します。

着信トラフィックを検証する TCP ダンプ ユーティリティ

これは、予想されたパケットが実際にノードに到達したことを調査する場合に、パケットをスニッフィングするツールです。たとえば、レポートに示されている着信認証またはログがない場合、着信トラフィックがないのではないか、または着信トラフィックが Cisco ISE に到達できないのではないかと疑われる場合があります。このような場合、検証するためにこのツールを実行できます。

TCP ダンプ オプションを設定し、ネットワーク トラフィックからデータを収集して、ネットワークの問題をトラブルシューティングすることができます。

⚠

注意 TCP ダンプを起動すると、以前のダンプ ファイルは自動的に削除されます。以前のダンプ ファイルを保存するには、新しい TCP ダンプ セッションを開始する前に、「TCP ダンプ ファイルの保存」の項の説明に従ってタスクを実行します。

ネットワーク トラフィックのモニタリングでの TCP ダンプの使用

始める前に

- [TCP ダンプ（TCP Dump）] ページの [ネットワーク インターフェイス（Network Interface）] ドロップダウン リストには、IPv4 または IPv6 アドレスが設定されているネットワーク インターフェイス カード（NIC）のみが表示されます。デフォルトでは、すべての NIC は VMware に接続されるため、NIC は、IPv6 アドレスを使用して設定され、[ネットワーク インターフェイス（Network Interface）] ドロップダウン リストに表示されます。

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [TCP ダンプ（TCP Dump）]** を選択します。

ステップ 2 TCP ダンプ ユーティリティのソースとして [ホスト名（Host Name）] を選択します。

ステップ 3 モニタする [ネットワーク インターフェイス（Network Interface）] をドロップダウン リストから選択します。

ステップ 4 オプション ボタンをクリックして、オンかオフにして、無差別モードを設定します。デフォルトは [オン（On）] です。

無差別モードは、ネットワーク インターフェイスがシステムの CPU にすべてのトラフィックを渡すデフォルト パケット スニッフィング モードです。[オン（On）] のままにしておくことを推奨します。

ステップ 5 [フィルタ（Filter）] テキスト ボックスに、フィルタリングのもとになるブール演算式を入力します。

サポートされている標準 tcpdump フィルタ式 :

ip host 10.77.122.123

ip host 10.77.122.123 and not 10.77.122.119

ip host ISE123

ステップ 6 [開始（Start）] をクリックして、ネットワークのモニタリングを開始します。

ステップ 7 十分な量のデータが収集された時点で [停止（Stop）] をクリックするか、最大パケット数（500,000）が累積されてプロセスが自動的に終了するまで待機します。

（注） Cisco ISE は、1500 より大きいフレーム（ジャンボ フレーム）の MTU をサポートしません。

TCP ダンプ ファイルの保存

始める前に

「ネットワーク トラフィックのモニタリングでの TCP ダンプの使用」の項の説明に従って、タスクを完了しておく必要があります。

（注） Cisco ISE CLI を使用して TCPdump にアクセスすることもできます。詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [TCP ダンプ（TCP Dump）]** を選択します。

ステップ 2 [形式（Format）] をドロップダウン リストから選択します。[可読（Human Readable）] がデフォルトです。

ステップ 3 [ダウンロード（Download）] をクリックし、必要な場所に移動して、[保存（Save）] をクリックします。

ステップ 4 最初に以前のダンプ ファイルを保存しないで除去するには、[削除（Delete）] をクリックします。

エンドポイントまたはユーザの予期しない SGACL の比較

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [TrustSec ツール（Trustsec Tools）] > [出力（SGACL）ポリシー（Egress (SGACL) Policy）]** を選択します。

ステップ 2 SGACL ポリシーを比較する TrustSec デバイスのネットワーク デバイス IP アドレスを入力します。

ステップ 3 [実行（Run）] をクリックします。

ステップ 4 [ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更します。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 [結果概要の表示（Show Results Summary）] をクリックして、診断および推奨される解決手順を表示します。

出力ポリシー診断フロー

出力ポリシー診断ツールでは、次の表に示すプロセスを使用して比較が行われます。

プロセス ステージ	説明
1	指定した IP アドレスを使用してデバイスに接続し、送信元 SGT と宛先 SGT の各ペアに対するアクセス コントロール リスト（ACL）を取得します。
2	Cisco ISE に設定された出力ポリシーをチェックし、送信元 SGT と宛先 SGT の各ペアに対する ACL を取得します。

プロセス ステージ	説明
3	ネットワーク デバイスから取得された SGACL ポリシーと、Cisco ISE から取得された SGACL ポリシーを比較します。
4	ポリシーが一致しない送信元 SGT と宛先 SGT のペアを表示します。また、追加情報として、一致するエントリも表示します。

SXP-IP マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [TrustSec ツール（Trustsec Tools）] > [SXP-IP マッピング（SXP-IP Mappings）]** を選択します。

ステップ 2 ネットワーク デバイスのネットワーク デバイス IP アドレスを入力し、[選択（Select）] をクリックします。

ステップ 3 [実行（Run）] をクリックし、[ユーザ入力必須（User Input Required）] をクリックして、必要なフィールドを変更します。

Expert Troubleshooter によって、ネットワーク デバイスから TrustSec SXP 接続が取得されて、ピア SXP デバイスを選択するように再度要求するプロンプトが表示されます。

ステップ 4 [ユーザ入力必須（User Input Required）] をクリックし、必要な情報を入力します。

ステップ 5 SXP マッピングを比較するピア SXP デバイスのチェックボックスをオンにして、共通接続パラメータを入力します。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 [結果概要の表示（Show Results Summary）] をクリックして、診断および解決手順を表示します。

IP-SGT マッピングを持つ TrustSec 対応ネットワークの接続問題のトラブルシューティング

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [TrustSec ツール（Trustsec Tools）] > [IP ユーザ SGT（IP User SGT）]** を選択します。

ステップ 2 必要に応じてフィールドに情報を入力します。

ステップ 3 [実行（Run）] をクリックします。

追加入力が要求されます。

ステップ 4 [ユーザ入力必須（User Input Required）] をクリックし、必要に応じてフィールドを変更して、[送信（Submit）] をクリックします。

ステップ 5 [結果概要の表示（Show Results Summary）] をクリックして、診断および解決手順を表示します。

デバイス SGT ツール

TrustSec ソリューションが有効なデバイスの場合、RADIUS 認証によって各ネットワーク デバイスに SGT 値が割り当てられます。デバイス SGT 診断ツールは、（提供された IP アドレスを使用して）ネットワーク デバイスに接続し、ネットワーク デバイス SGT 値を取得します。次に RADIUS 認証レコードをチェックして、割り当てられた最新の SGT 値を特定します。最後に、デバイス SGT ペアを表形式で表示して、SGT 値が同じであるかどうかを特定します。

デバイス SGT マッピングの比較による TrustSec 対応ネットワークの接続問題のトラブルシューティング

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [TrustSec ツール（Trustsec Tools）] > [デバイス SGT（Device SGT）]** を選択します。

ステップ 2 必要に応じてフィールドに情報を入力します。

デフォルトのポート番号は、Telnet は 23、SSH は 22 です。

ステップ 3 [実行（Run）] をクリックします。

ステップ 4 [結果概要の表示（Show Results Summary）] をクリックして、デバイス SGT 比較の結果を表示します。

その他のトラブルシューティング情報の入手

Cisco ISE を使用すると、管理者ポータルから、サポートおよびトラブルシューティング情報をダウンロードできます。サポート バンドルを使用して、Cisco Technical Assistance Center（TAC）が Cisco ISE の問題をトラブルシューティングするための診断情報を準備できます。

（注） サポート バンドルおよびデバッグ ログにより、高度なトラブルシューティング情報が TAC に提供されます。サポート バンドルおよびデバッグ ログは解釈が困難です。Cisco ISE で提供されるさまざまなレポートおよびトラブルシューティング ツールを使用して、ネットワークで直面している問題を診断およびトラブルシューティングできます。

Cisco ISE のサポート バンドル

サポートバンドルに含めるログを設定できます。たとえば、特定のサービスのログをデバッグログに含めるように設定できます。また、日付に基づいてログをフィルタリングできます。

ダウンロードできるログは、次のように分類されます。

- 完全な設定データベース：Cisco ISE 設定データベースは、人間が読み取れる XML 形式でダウンロードされます。問題をトラブルシューティングしようとするときに、このデータベース設定を別の Cisco ISE ノードにインポートして、シナリオを再現できます。
- デバッグログ：ブートストラップ、アプリケーション設定、ランタイム、展開、公開キーインフラストラクチャ（PKI）情報、およびモニタリングとレポートが取得されます。

  デバッグ ログによって、特定の Cisco ISE コンポーネントのトラブルシューティング情報が提供されます。デバッグ ログを有効にするには、第 11 章「ログ」を参照してください。デバッグ ログを有効にしない場合、情報メッセージ（INFO）はすべてサポート バンドルに含まれます。詳細については、Cisco ISE デバッグ ログ （1589 ページ）を参照してください。
- ローカル ログ：Cisco ISE で実行されるさまざまなプロセスからの syslog メッセージが含まれています。
- コア ファイル：クラッシュの原因の特定に役立つ重要な情報が含まれています。これらのログは、アプリケーションがクラッシュし、アプリケーションにヒープ ダンプが含まれている場合に作成されます。
- モニタリングおよびレポート ログ：アラートおよびレポートに関する情報が含まれています。
- システム ログ：Cisco Application Deployment Engine（ADE）関連の情報が含まれています。
- ポリシー設定：Cisco ISE で設定されたポリシーが人間が読み取れる形式で含まれます。

これらのログは、Cisco ISE CLI から **backup-logs** コマンドを使用してダウンロードできます。詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

（注） インライン ポスチャ ノードの場合、管理者ポータルからサポート バンドルをダウンロードできません。Cisco ISE CLI から **backup-logs** コマンドを使用して、インライン ポスチャ ノードのログをダウンロードする必要があります。

これらのログを管理者ポータルからダウンロードすることを選択した場合、次の操作を実行できます。

- デバッグ ログやシステム ログなどのログ タイプに基づいて、ログのサブセットのみをダウンロードします。

- 選択したログタイプの最新の「*n*」個のファイルのみをダウンロードします。このオプションによって、サポート バンドルのサイズとダウンロードにかかる時間を制御できます。

モニタリング ログによって、モニタリング、レポート、およびトラブルシューティング機能に関する情報が提供されます。ログのダウンロードの詳細については、Cisco ISE ログ ファイルのダウンロード （1588 ページ）を参照してください。

サポート バンドル

サポート バンドルは、単純な tar.gpg ファイルとしてローカル コンピュータにダウンロードできます。サポート バンドルは、日付とタイム スタンプを使用して、ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg という形式で名前が付けられます。ブラウザに、適切な場所にサポートバンドルを保存するように要求するプロンプトが表示されます。サポート バンドルの内容を抽出し、README.TXT ファイルを表示できます。このファイルには、サポートバンドルの内容と、ISE データベースがサポートバンドルに含まれている場合はその内容をインポートする方法が示されています。

Cisco ISE ログ ファイルのダウンロード

ネットワークでの問題のトラブルシューティング時に、Cisco ISE ログ ファイルをダウンロードして、詳細情報を確認できます。

インストールとアップグレードに関する問題のトラブルシューティングを行うには、ADE-OS および他のログ ファイルを含む、システム ログをダウンロードすることもできます。

サポートバンドルをダウンロードする際には、暗号化キーを手動で入力する代わりに、暗号化用の公開キーを使用するように選択できるようになりました。このオプションを選択すると、Cisco PKI はサポート バンドルの暗号化および復号化に使用されます。Cisco TAC は、公開キーと秘密キーを保持します。Cisco ISE はサポート バンドルの暗号化に公開キーを使用します。Cisco TAC は、秘密キーを使用してサポート バンドルを復号化できます。このオプションは、トラブルシューティング用に Cisco TAC にサポート バンドルを提供する場合に使用します。オンプレミスの問題をトラブルシューティングしている場合、共有キー暗号化を使用します。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者の権限が必要です。
- デバッグ ログとデバッグ ログ レベルを設定します。

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）] > > [アプライアンス ノード リスト（Appliance node list）]** を選択します。

ステップ 2 サポート バンドルをダウンロードするノードをクリックします。

ステップ 3 [サポート バンドル（Support Bundle）] タブでは、サポート バンドルに入力するパラメータを選択します。

すべてのログを含めると、サポート バンドルが大きくなりすぎて、ダウンロードに時間がかかります。ダウンロード プロセスを最適化するには、最新の *n* ファイルのみをダウンロードするように選択します。

ステップ 4 サポート バンドルを生成する開始日と終了日を入力します。

ステップ 5 次のいずれかを実行します。

- 公開キー暗号化（Public Key Encryption）：このオプションは、トラブルシューティング用に Cisco TAC にサポート バンドルを提供する場合に選択します。
- 共有キー暗号化（Shared Key Encryption）：このオプションは、オンプレミスでローカルで問題をトラブルシューティングする場合に選択します。このオプションを選択すると、サポート バンドル用の暗号キーを入力する必要があります。

ステップ 6 サポート バンドルの暗号キーを入力し、再入力します。

ステップ 7 [サポート バンドルの作成（Create Support Bundle）] をクリックします。

ステップ 8 [ダウンロード（Download）] をクリックして、新しく作成されたサポート バンドルをダウンロードします。

サポート バンドルは、アプリケーション ブラウザを実行しているクライアント システムにダウンロードされる tar.gpg ファイルです。

次のタスク

特定のコンポーネントのデバッグ ログをダウンロードします。

Cisco ISE デバッグ ログ

デバッグ ログには、さまざまな Cisco ISE コンポーネントのトラブルシューティング情報が含まれています。デバッグ ログには、過去 30 日間に生成された重大な警告アラームと、過去 7 日間に生成された情報アラームが含まれています。問題を報告しているときに、これらのデバッグ ログを有効にして、問題の診断と解決のためにこれらのログを送信するよう求められる場合があります。

デバッグ ログの入手

ステップ 1 [デバッグ ログの設定（Debug Log Configuration）] ページで、デバッグ ログを取得するコンポーネントを設定します。

ステップ 2 デバッグ ログをダウンロードします。

Cisco ISE コンポーネントおよび対応するデバッグ ログ

表 *238 :* コンポーネントおよび対応するデバッグ ログ

コンポーネント	デバッグ ログ
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
ライセンス	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
クライアント	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
ゲスト アクセス管理	guest.log
ゲスト アクセス	guest.log
MyDevices	guest.log
ポータル（Portal）	guest.log

コンポーネント	デバッグ ログ
ポータル セッション マネージャ	guest.log
ポータル Web アクション	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
ポスチャ	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

デバッグ ログのダウンロード

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[ログのダウンロード（Download Logs）]** > > **[アプライアンス ノード リスト（Appliance node list）]** を選択します。

ステップ 2 [アプライアンス ノード リスト（Appliance node list）] で、デバッグ ログをダウンロードするノードをクリックします。

ステップ 3 [デバッグ ログ（Debug Logs）] タブをクリックします。

デバッグ ログ タイプとデバッグ ログのリストが表示されます。このリストは、デバッグ ログの設定に基づいています。

ステップ 4 ダウンロードするログ ファイルをクリックし、クライアント ブラウザを実行しているシステムに保存します。

必要に応じて、このプロセスを繰り返して他のログ ファイルをダウンロードできます。次に示すのは、[デバッグ ログ（Debug Logs）] ページからダウンロードできるその他のデバッグ ログです。

- isebootstrap.log：ブートストラップ ログ メッセージを提供します
- monit.log：ウォッチドッグ メッセージを提供します
- pki.log：サードパーティの暗号ライブラリ ログを提供します
- iseLocalStore.log：ローカル ストア ファイルに関するログを提供します
- ad_agent.log：Microsoft Active Directory サードパーティ ライブラリ ログを提供します
- catalina.log：サードパーティ ログを提供します