脅威の封じ込め

脅威中心型 NAC サービス

脅威中心型ネットワーク アクセス コントロール（TC-NAC）機能により、脅威および脆弱性のアダプタから受信する脅威と脆弱性の属性に基づいて、許可ポリシーを作成できます。

脅威のシビラティ（重大度）レベルと脆弱性評価の結果は、エンドポイントまたはユーザーのアクセス レベルを動的に制御するために使用できます。

忠実度の高い侵害の兆候（IoC）、脅威検出イベント、およびCVSS スコアを Cisco ISE に送信するように脆弱性および脅威のアダプタを設定できます。これにより、エンドポイントの権限とコンテキストを適宜変更するための脅威中心型アクセスポリシーを作成できます。

Cisco ISE では次のアダプタがサポートされています。

- SourceFire FireAMP（現在の Cisco Secure Endpoint）
- Cognitive Threat Analytics（CTA）アダプタ
- Qualys

（注） TC-NAC フローで現在サポートされているのは Qualys Enterprise Edition のみです。

- Rapid7 Nexpose
- Tenable Security Center

エンドポイントの脅威イベントが検出されたら、[侵害されたエンドポイント（Compromised Endpoints）] ウィンドウでエンドポイントの MAC アドレスを選択して ANC ポリシー（Quarantine など）を適用できます。Cisco ISE は、そのエンドポイントに対して CoA をトリガーし、対応する ANC ポリシーを適用します。ANC ポリシーが使用可能ではない場合、Cisco ISE はそのエンドポイントに対して CoA をトリガーし、元の許可ポリシーを適用します。[侵害されたエンドポイント（Compromised Endpoints）] ウィンドウの [脅威と脆弱性のクリア（Clear Threat and Vulnerabilities）] オプションを使用して、（Cisco ISE システムデータベースから）エンドポイントに関連付けられている脅威と脆弱性をクリアできます。

脅威ディクショナリには次の属性がリストされます。

- CTA-Course_Of_Action（値は Internal Blocking、Eradication、または Monitoring です。）
- Qualys-CVSS_Base_Score
- Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

Base Score 属性と Temporal Score 属性の有効な範囲は 0 ~ 10 です。

脆弱性イベントがエンドポイントに受信されると、Cisco ISE はそのエンドポイントの CoA をトリガーします。ただし、脅威イベントの受信時には CoA はトリガーされません。

脆弱性属性を使用して、属性の値に基づいて脆弱なエンドポイントを自動的に隔離する許可ポリシーを作成できます。次に例を示します。

```
Any Identity Group & Threat:Qualys-CVSS_Base_Score > 7.0 -> Quarantine
```

CoA イベント中に自動的に隔離されているエンドポイントのログを表示するには、**[操作（Operations）] > [脅威中心型NACのライブログ（Threat-Centric NAC Live Logs）]** を選択します。手動で隔離されているエンドポイントのログを表示するには、**[操作（Operations）] > [レポート（Reports）] > [監査（Audit）] > [変更構成監査（Change Configuration Audit）]** を選択します。

脅威中心型 NAC サービスを有効にする際には、次の点に注意してください。

- 脅威中心型 NAC サービスを使用するには、Cisco ISE Premier ライセンスが必要です。
- 脅威中心型 NAC サービスは、展開内の 1 つのノードでのみ有効にできます。
- 脆弱性アセスメント サービスでは、ベンダーあたり 1 つのアダプタ インスタンスだけを追加できます。ただし、FireAMP アダプタ インスタンスは複数追加できます。
- 設定を失わずにアダプタを停止、再開できます。アダプタの設定後は、任意の時点でアダプタを停止できます。ISE サービスの再起動時でもアダプタはこの状態のままになります。アダプタを再起動するには、アダプタを選択して [再起動（Restart）] をクリックします。

（注） アダプタが [停止（Stopped）] 状態の場合、アダプタ インスタンスの名前だけを編集できます。アダプタ設定や詳細設定は編集できません。

エンドポイントの脅威情報は次に示すページで確認できます。

- **[ホーム（Home）] ページ > [脅威（Threat）] ダッシュボード**
- **[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [侵害されたエンドポイント（Compromised Endpoints）]**

脅威中心型 NAC サービスによりトリガーされるアラームを次に示します。

- Adapter not reachable（syslog ID：91002）：アダプタに到達できないことを示します。
- Adapter Connection Failed（syslog ID：91018）：アダプタに到達できるが、アダプタとソースサーバーの間の接続がダウンしていることを示します。
- Adapter Stopped Due to Error（syslog ID：91006）：このアラームは、アダプタが必要な状態になっていない場合にトリガーされます。このアラームが表示されたら、アダプタ設定とサーバー接続を調べてください。詳細については、アダプタ ログを参照してください。
- Adapter Error（syslog ID：91009）：Qualys アダプタが Qualys サイトとの接続を確立できないか、またはこのサイトから情報をダウンロードできないことを示します。

脅威中心型 NAC サービスで使用できるレポートを次に示します。

- **[アダプタのステータス（Adapter Status）]**：アダプタのステータスレポートには、脅威と脆弱性のアダプタのステータスが表示されます。
- **[COA イベント（COA Events）]**：エンドポイントの脆弱性イベントを受信すると、Cisco ISE はそのエンドポイントについて CoA をトリガーします。CoA イベント レポートには、これらの CoA イベントのステータスが表示されます。また、これらのエンドポイントの新旧の認証ルールとプロファイルの詳細が表示されます。
- **[脅威イベント（Threat Events）]**：脅威イベントレポートには、設定したさまざまなアダプタから Cisco ISE が受信した脅威イベントがすべて表示されます。脆弱性アセスメントのイベントは、このレポートには含まれません。
- **[脆弱性アセスメント（Vulnerability Assessment）]**：脆弱性アセスメントレポートには、エンドポイントで実行中のアセスメントに関する情報が示されます。このレポートを表示して、設定されたポリシーに基づいてアセスメントが行われているかどうかを確認することができます。

[操作（Operations）] > [レポート（Reports）] > [診断（Diagnostics）] > [ISE カウンタ（ISE Counters）] > [しきい値カウンタのトレンド（Threshold Counter Trends）] で、次の情報を確認できます。

- 受信したイベントの総数

- 脅威イベントの総数
- 脆弱性イベントの総数
- （PSN に対して）発行された CoA の総数

これらの属性の値は 5 分おきに収集されるため、この値は直近 5 分間の数を表します。

[脅威（Threat）] ダッシュボードには次のダッシュレットが表示されます。

- [侵害されたエンドポイントの総数（Total Compromised Endpoints）] ダッシュレットには、ネットワーク上で現在影響を受けているエンドポイント（接続エンドポイントと切断エンドポイントの両方）の総数が表示されます。
- [特定期間における侵害されたエンドポイント（Compromised Endpoints Over Time）] ダッシュレットには、指定された期間におけるエンドポイントへの影響の履歴ビューが表示されます。
- [上位の脅威（Top Threats）] ダッシュレットには、影響を受けるエンドポイントの数と脅威のシビラティ（重大度）に基づく上位の脅威が表示されます。
- [脅威ウォッチリスト（Threats Watchlist）] ダッシュレットを使用して、選択したイベントのトレンドを分析できます。

[上位の脅威（Top Threats）] ダッシュレットでは、バブルのサイズが影響を受けるエンドポイントの数を示し、薄い影が付いている領域が切断されているエンドポイントの数を示します。色と縦方向の目盛りで脅威のシビラティ（重大度）を示します。脅威には、インディケータとインシデントという 2 つのカテゴリがあります。インディケータのシビラティ（重大度）属性は「Likely_Impact」、インシデントのシビラティ（重大度）属性は「Impact_Qualification」です。

[侵害されたエンドポイント（Compromised Endpoint）] ウィンドウには、影響を受けるエンドポイントのマトリックスビューと、各脅威カテゴリの影響のシビラティ（重大度）が示されます。エンドポイントの詳細な脅威情報を表示するには、デバイス リンクをクリックします。

[実行されたアクション（Course Of Action）] チャートには、CTA アダプタから受信した CTA-Course_Of_Action 属性に基づき、脅威インシデントに対して実行されたアクション（[内部ブロック（Internal Blocking）]、[撲滅（Eradication）]、または [モニタリング（Monitoring）]）が表示されます。

[ホーム（Home）] ページの [脆弱性（Vulnerability）] ダッシュボードには、次のダッシュレットが表示されます。

- [脆弱なエンドポイントの総数（Total Vulnerable Endpoints）] ダッシュレットには、指定された値よりも大きい CVSS スコアを持つエンドポイントの総数が表示されます。また、CVSS スコアが指定された値よりも大きい接続エンドポイントと切断エンドポイントの総数も表示されます。
- [上位の脆弱性（Top Vulnerability）] ダッシュレットには、影響を受けるエンドポイントの数または脆弱性のシビラティ（重大度）に基づく上位の脅威が表示されます。[上位の脆弱性（Top Vulnerability）] ダッシュレットでは、バブルのサイズが影響を受けるエンドポ

イントの数を示し、薄い影が付いている領域が切断されているエンドポイントの数を示します。色と縦方向の目盛りで脆弱性のシビラティ（重大度）を示します。

- [脆弱性ウォッチリスト（Vulnerability Watchlist）] ダッシュレットを使用して、一定期間にわたる選択した脆弱性のトレンドを分析できます。ダッシュレットで検索アイコンをクリックし、ベンダー固有の ID（Qualys の ID 番号の場合は「qid」）を入力して、その ID 番号の傾向を選択して表示します。
- [特定期間における脆弱なエンドポイント（Vulnerable Endpoints Over Time）] ダッシュレットには、一定期間におけるエンドポイントへの影響の履歴ビューが表示されます。

[脆弱なエンドポイント（Vulnerable Endpoints）] ウィンドウの [CVSS 別エンドポイント数（Endpoint Count By CVSS）] グラフには、影響を受けるエンドポイントの数とその CVSS スコアが表示されます。[脆弱なエンドポイント（Vulnerable Endpoints）] ウィンドウでは、影響を受けるエンドポイントのリストも表示されます。各エンドポイントの詳細な脆弱性情報を表示するには、デバイスリンクをクリックします。

脅威中心型 NAC サービスログはサポートバンドルに含まれています。脅威中心型 NAC サービスログは support/logs/TC-NAC/ にあります。

（注） Cisco ISE は、エンドポイントでのクレデンシャルを使用したオンデマンドスキャンをサポートしていません。

脅威中心型 NAC サービスの有効化

脆弱性と脅威のアダプタを設定するには、まず脅威中心型 NAC サービスを有効にする必要があります。このサービスは、導入内の 1 つのポリシーサービス ノードでのみ有効にできます。

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

ステップ 2 脅威中心型 NAC サービスを有効にする PSN の隣にあるチェック ボックスにマークを付けて、[編集（Edit）] をクリックします。

ステップ 3 [脅威中心型 NAC サービスの有効化（Enable Threat Centric NAC Service）] チェック ボックスにマークを付けます。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

SourceFire FireAMP アダプタの追加 （6 ページ）
Cognitive Threat Analytics アダプタの追加 （7 ページ）
CTA アダプタの許可プロファイルの設定 （9 ページ）
Course of Action 属性を使用した許可ポリシーの設定 （9 ページ）
脅威中心型 NAC サービス （1 ページ）

SourceFire FireAMP アダプタの追加

始める前に

- SourceFire FireAMP のアカウントが必要です。
- すべてのエンドポイントの FireAMP クライアントを導入する必要があります。
- 脅威中心型 NAC サービスを展開ノードで有効にする必要があります（脅威中心型 NAC サービスの有効化 （5 ページ）を参照）。
- FireAMP アダプタは REST API コール（AMP クラウドへ）、およびイベントを受信する AMQP に SSL を使用します。また、プロキシの使用をサポートしています。FireAMP アダプタは通信にポート 443 を使用します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから [AMP：脅威（AMP：Threat）] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ベンダーインスタンスのリストウィンドウを更新します。ベンダーインスタンスのリストウィンドウでアダプタのステータスが [設定準備完了（Ready to Configure）] に変更された後でのみ、アダプタを設定できます。

ステップ 7 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 8 （オプション）すべてのトラフィックをルーティングするように SOCKS プロキシ サーバーを設定した場合、プロキシ サーバーのホスト名とポート番号を入力します。

ステップ 9 接続するクラウドを選択します。US クラウドまたは EU クラウドを選択できます。

ステップ 10 サブスクライブするイベント ソースを選択します。次のオプションを使用できます。

- **[AMP イベントのみ（AMP events only）]**
- **[CTA イベントのみ（CTA events only）]**
- **[CTA と AMP のイベント（CTA and AMP events）]**

ステップ 11 FireAMP リンクをクリックし、admin として FireAMP にログインします。[アプリケーション（Applications）] ペインの [許可（Allow）] をクリックして、ストリーミング イベント エクスポート要求を許可します。
Cisco ISE にリダイレクトします。

ステップ 12 監視するイベントを選択します（たとえば、不審なダウンロード、疑わしいドメインへの接続、実行されたマルウェア、Java 侵害）。

詳細設定の変更またはアダプタの再設定時に、AMPクラウドに新しいイベントが追加されている場合、これらのイベントも [イベントリスト（Events Listing）] ウィンドウに表示されます。

アダプタ用のログ レベルを選択できます。選択可能なオプションは、[エラー（Error）]、[情報（Info）]、[デバッグ（Debug）] です。

アダプタインスタンスの設定の要約が [設定サマリー（Configuration Summary）] ウィンドウに表示されます。

Cognitive Threat Analytics アダプタの追加

始める前に

- 脅威中心型 NAC サービスを展開ノードで有効にする必要があります（脅威中心型 NAC サービスの有効化 （5 ページ）を参照）。
- http://cognitive.cisco.com/login から Cisco Cognitive Threat Analytics（CTA）ポータルにログインし、CTA STIX/TAXII サービスを要求します。詳細については、『Cisco ScanCenter Administrator Guide』を参照してください。
- Cognitive Threat Analytics（CTA）アダプタは、SSL とともに TAXII プロトコルを使用して、CTA クラウドをポーリングし、検出された脅威を確認します。また、プロキシの使用をサポートしています。
- 信頼できる証明書ストアにアダプタ証明書をインポートします。[管理（Administration）] >[システム（System）]>[証明書（Certificates）]>[信頼できる証明書（Trusted Certificates）] > [インポート（Import）] の順に選択し、証明書をインポートします。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[管理（Administration）] > [脅威中心型NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）]**。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから [CTA：脅威（CTA：Threat）] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ベンダー インスタンスのリスト ページを更新します。ベンダー インスタンスのリスト ページでアダプタのステータスが [設定準備完了（Ready to Configure）] に変更された後でのみ、アダプタを設定できます。

ステップ 7 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 8 次の詳細を入力します。

- [CTA STIX/TAXII サービスの URL（CTA STIX/TAXII service URL）]：CTA クラウドサービスの URL。デフォルトでは URL https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService/ が使用されます。
- [CTA フィード名（CTA feed name）]：CTA クラウドサービスのフィード名を入力します。
- [CTA ユーザー名とパスワード（CTA username and password）]：CTA クラウドサービスのユーザー名とパスワードを入力します。
- [プロキシホストとポート（Proxy host and port）]（オプション）：すべてのトラフィックをルーティングするようにプロキシサーバーを設定した場合、そのプロキシ サーバーのホスト名とポート番号を入力します。
- [ポーリング間隔（Polling interval）]：各ポーリング間の時間間隔。デフォルト値は 30 分です。
- [最初のポーリング期間（時間数）（First Poll Duration in hours）]：最初のポーリングで取得されるデータの経過時間。デフォルト値は 2 時間です。最大値は 12 時間です。
- [インシデントタイプ（Incident Type）]：次のオプションを使用できます。
  - **[CTA イベントのみ（CTA events only）]**
  - **[AMP イベントのみ（AMP events only）]**
  - **[CTA と AMP のイベント（CTA and AMP events）]**

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 次のオプションを設定するには、[詳細設定（Advanced Settings）] をクリックします。

- [影響の指定（Impact Qualification）]：ポーリングするインシデントのシビラティ（重大度）レベルを選択します。次のオプションを使用できます。
  - **[1 - 影響なし（1 - Insignificant）]**
  - **[2 - 妨害（2 - Distracting）]**
  - **[3 - 困難（3 - Painful）]**
  - **[4 - 損害発生（4 - Damaging）]**
  - **[5 - 壊滅的（5 - Catastrophic）]**

  [3 - 困難（3 - Painful）] を選択した場合、シビラティ（重大度）レベルが [3 - 困難（3 - Painful）] またはそれ以上（この場合 [4 - 損害発生（4 - Damaging）] と [5 - 壊滅的（5 - Catastrophic）]）のインシデントがポーリングされます。
- [ロギングレベル（Logging Level）]：アダプタのログ レベルを選択します。選択可能なオプションは、[エラー（Error）]、[情報（Info）]、[デバッグ（Debug）] です。

ステップ 11 [終了（Finish）] をクリックします。

（注） CTA は Web プロキシ ログに IP アドレスまたはユーザー名としてリストされているユーザー ID を処理します。具体的には、IP アドレスの場合、プロキシ ログで使用可能なデバイスの IP アドレスが、内部ネットワークの別のデバイスの IP アドレスと競合する可能性があります。たとえばエージェント経由で接続するローミングユーザーと、インターネットに直接接続するスプリットトンネルが獲得するローカル IP 範囲アドレス（例：10.0.0.X）が、内部ネットワークで使用されている重複するプライベート IP 範囲のアドレスと競合することがあります。不一致のデバイスに隔離アクションが適用されることを防ぐポリシーを定義するときには、論理ネットワーク アーキテクチャを考慮することが推奨されます。

CTA アダプタの許可プロファイルの設定

脅威イベントごとに、CTA アダプタは Course of Action 属性の値「Internal Blocking」、「Monitoring」、または「Eradication」のいずれかを返します。これらの値に基づいて許可プロファイルを作成できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 許可プロファイルの名前および説明を入力します。

ステップ 4 アクセス タイプを選択します。

ステップ 5 必要な詳細を入力し、[送信（Submit）] をクリックします。

Course of Action 属性を使用した許可ポリシーの設定

脅威イベントが報告されたエンドポイントに対して許可ポリシーを設定するには、CTA-Course_Of_Action 属性を使用できます。この属性は [脅威（Threat）] ディレクトリで使用できます。

また、CTA-Course_Of_Action 属性に基づいて例外ルールを作成することもできます。

ステップ 1 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択します。
脅威イベントが発生したエンドポイントについて、既存のポリシー ルールを編集するか、または新しい例外ルールを作成することができます。

ステップ 2 CTA-Course_Of_Action 属性値を検査するための条件を作成し、適切な許可プロファイルを割り当てます。次に例を示します。

Network_Access_Authentication_Passed AND ThreatCTA-Course_Of_Action CONTAINS Internal Blocking then blocking (authorization profile)

（注） 「Internal Blocking」はエンドポイントの隔離に使用することが推奨される Course of Action 属性です。

ステップ 3 [保存（Save）] をクリックします。

エンドポイントの脅威イベントを受信すると、Cisco ISE は、そのエンドポイントに一致する許可ポリシーがあるかどうかを調べ、エンドポイントがアクティブな場合にのみ CoA をトリガーします。エンドポイントがオフラインの場合、脅威イベントの詳細が脅威イベント レポートに追加されます（[操作（Operations）] > [レポート（Reports）] > [脅威中心型 NAC（Threat Centric NAC] > [脅威イベント（Threat Events）]）。

（注） CTA が 1 つのインシデントで複数のリスクとそれらに関連付けられている Course of Action 属性を送信することがあります。たとえば 1 つのインシデントで「Internal Blocking」と「Monitoring」（Course of Action 属性）を送信することがあります。この場合、「equals」演算子を使用してエンドポイントを隔離する許可ポリシーが設定されていると、エンドポイントは隔離されません。次に例を示します。

```
CTA-Course_Of_Action EQUALS Internal Blocking then Quarantine_Systems (authorization profile)
```

この場合、エンドポイントを隔離するには許可ポリシーで「contains」演算子を使用する必要があります。次に例を示します。

```
CTA-Course_Of_Action CONTAINS Internal Blocking then Quarantine_Systems
```

Cisco ISE での脆弱性アセスメントのサポート

Cisco ISE は次の脆弱性アセスメント（VA）エコシステムパートナーと連携し、Cisco ISE ネットワークに接続するエンドポイントの脆弱性アセスメント結果を取得します。

- Qualys：Qualysは、ネットワークに導入されているスキャナアプライアンスを使用するクラウドベースの評価システムです。Cisco ISE では、Qualys と通信して VA 結果を取得するアダプタを設定できます。管理者ポータルからアダプタを設定できます。アダプタを設定するには、スーパー管理者権限を持つ Cisco ISE 管理者アカウントが必要です。Qualys アダプタは、Qualys クラウド サービスとの通信に REST API を使用します。REST API にアクセスするには、Qualys でマネージャ権限が付与されたユーザー アカウントが必要です。Cisco ISE は次の Qualys REST API を使用します。
  - [ホスト検出リストAPI（Host Detection List API）]：エンドポイントの最新スキャン結果を確認します。
  - [Scan API]：エンドポイントのオンデマンドスキャンをトリガーします。

  Qualys により、サブスクライブ ユーザーが実行できる API コールの数に制限が適用されます。デフォルトのレート制限カウントは、24 時間あたり 300 です。Cisco ISE は Qualys

API バージョン 2.0 を使用して Qualys に接続します。これらの API 機能の詳細については、『Qualys API V2 User Guide』を参照してください。

- [Rapid7 Nexpose]：Cisco ISE は脆弱性管理ソリューションである Rapid 7 Nexpose と連携して、脆弱性の検出を促進します。これにより、このような脅威に迅速に対応できるようになります。Cisco ISE は Nexpose から脆弱性データを受信し、ISE で設定したポリシーに基づいて、影響を受けるエンドポイントを隔離します。Cisco ISE ダッシュボードから、影響を受けるエンドポイントを確認し、適切なアクションを実行できます。

  Cisco ISE は Nexpose リリース 6.4.1 でテスト済みです。

- [Tenable SecurityCenter（Nessus スキャナ）（Tenable SecurityCenter (Nessus scanner)）]：Cisco ISE は Tenable SecurityCenter と連携し、（Tenable SecurityCenter により管理される）Tenable Nessus スキャナから脆弱性データを受信します。また、ISE で設定したポリシーに基づいて、影響を受けるエンドポイントを隔離します。Cisco ISE ダッシュボードから、影響を受けるエンドポイントを確認し、適切なアクションを実行できます。

  Cisco ISE リリース 3.4 は、Tenable SecurityCenter 6.4 で検証されます。

エコシステム パートナーからの結果は Structured Threat Information Expression（STIX）表現に変換され、この値に基づき、必要に応じて認可変更（CoA）がトリガーされ、適切なアクセスレベルがエンドポイントに付与されます。

エンドポイントの脆弱性に関する評価にかかる時間は、さまざまな要因に基づいて異なるため、VA をリアルタイムで実行することはできません。エンドポイントの脆弱性に関する評価にかかる時間に影響する要因を次に示します。

- 脆弱性アセスメント エコシステム
- スキャン対象の脆弱性のタイプ
- 有効なスキャンのタイプ
- エコシステムによりスキャナ アプライアンスに割り当てられるネットワーク リソースとシステム リソース

このリリースの Cisco ISE では、IPv4 アドレスを持つエンドポイントのみが脆弱性を評価できます。

脆弱性アセスメント サービスの有効化と設定

Cisco ISE で脆弱性アセスメント サービスを有効にして設定するには、次の作業を行います。

ステップ 1 脅威中心型 NAC サービスの有効化 （5 ページ）。

ステップ 2 次の設定を行います。

- Qualys アダプタ（Qualys アダプタの設定 （12 ページ）を参照）。
- Nexpose アダプタ（Nexpose アダプタの設定 （16 ページ）を参照）。
- Tenable アダプタ（Tenable アダプタの設定 （18 ページ）を参照）。

ステップ 3 認可プロファイルの設定 （21 ページ）。

ステップ 4 脆弱なエンドポイントを隔離する例外ルールの設定 （22 ページ）。

脅威中心型 NAC サービスの有効化

脆弱性と脅威のアダプタを設定するには、まず脅威中心型 NAC サービスを有効にする必要があります。このサービスは、導入内の 1 つのポリシー サービス ノードでのみ有効にできます。

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

ステップ 2 脅威中心型NACサービスを有効にするPSNの隣にあるチェック ボックスにマークを付けて、[編集（Edit）] をクリックします。

ステップ 3 [脅威中心型 NAC サービスの有効化（Enable Threat Centric NAC Service）] チェック ボックスにマークを付けます。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

SourceFire FireAMP アダプタの追加 （6 ページ）
Cognitive Threat Analytics アダプタの追加 （7 ページ）
CTA アダプタの許可プロファイルの設定 （9 ページ）
Course of Action 属性を使用した許可ポリシーの設定 （9 ページ）
脅威中心型 NAC サービス （1 ページ）

Qualys アダプタの設定

Cisco ISE は、Qualys 脆弱性アセスメント エコシステムをサポートしています。Cisco ISE 用の Qualys アダプタを作成して、Qualys と通信し、VA 結果を取得する必要があります。

始める前に

- 次のユーザー アカウントを準備する必要があります。
  - ベンダー アダプタを設定できる、スーパー管理者権限を持つ Cisco ISE の管理者ユーザー アカウント。
  - 管理者権限を持つ Qualys のユーザー アカウント
- 適切な Qualys ライセンス サブスクリプションがあることを確認します。Qualys レポート センター、ナレッジベース（KBX）、APIにアクセスする必要があります。詳細については、Qualys アカウント マネージャにお問い合わせください。
- Cisco ISE の信頼できる証明書ストアに Qualys サーバー証明書をインポートします（[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]）。適切なルートと中

間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている（または存在する）ことを確認します。

- Qualys API ガイドの次の設定を参照してください。
  - Qualys で CVSS スコアが有効になっていることを確認します（[レポート（Reports）] > [設定（Setup）] > [CVSS スコア（CVSS Scoring）] > [CVSS スコアの有効化（Enable CVSS Scoring）]）。
  - Qualys にエンドポイントの IP アドレスとサブネットマスクが追加されていることを確認します（[アセット（Assets）] > [ホストアセット（Host Assets）]）。
  - Qualys オプションプロファイルの名前があることを確認します。オプションプロファイルは、Qualys がスキャンのために使用するスキャナ テンプレートです。認証されたスキャンを含むオプション プロファイルを使用することを推奨します（このオプションは、エンドポイントの MAC アドレスも確認します）。
- HTTPS/SSL（ポート 443）を介して Qualys と通信する Cisco ISE。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから、[Qualys:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば、Qualys_Instance などです。

設定されているアダプタインスタンスのリストを含むリストウィンドウが表示されます。

ステップ 5 ベンダーインスタンスのリストウィンドウを更新します。新しく追加された Qualys_Instance アダプタのステータスが、[設定準備完了（Ready to Configure）] に変化します。

ステップ 6 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 7 Qualys の設定画面で次の値を入力し、[次へ（Next）] をクリックします。

フィールド名	説明
REST API ホスト（REST API Host）	Qualys クラウドをホストするサーバーのホスト名です。この情報については、Qualys の担当者にお問い合わせください。
REST API ポート（REST API Port）	443
ユーザー名（Username）	管理者権限を持つ Qualys のユーザー アカウントです。
パスワード（Password）	Qualys ユーザー アカウントのパスワードです。

フィールド名	説明
HTTP プロキシ ホスト（HTTP Proxy Host）	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバーがある場合は、プロキシ サーバーのホスト名を入力します。
HTTP プロキシ ポート（HTTP Proxy Port）	プロキシ サーバーが使用するポート番号を入力します。

Qualys サーバーへの接続が確立されると、Qualys スキャナのリストを含む[スキャナマッピング（Scanner Mappings）] ウィンドウが表示されます。ネットワークからの Qualys スキャナがこのウィンドウに表示されます。

ステップ 8 Cisco ISE がオンデマンド スキャンに使用するデフォルトのスキャナを選択します。

ステップ 9 [スキャナマッピングに対する PSN（PSN to Scanner Mapping）] 領域で、PSN ノードに対して 1 つ以上の Qualys スキャナアプライアンスを選択し、[次へ（Next）] をクリックします。

[詳細設定（Advanced Settings）] ポップアップウィンドウが表示されます。

ステップ 10 [詳細設定（Advanced Settings）] ウィンドウに次の値を入力します。このウィンドウの設定は、オンデマンドスキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド名	説明
オプション プロファイル（Option Profile）	Qualys がエンドポイントのスキャンのために使用するオプションプロファイルを選択します。デフォルト オプション プロファイルである、[初期オプション（Initial Options）] を選択できます。
最後のスキャン結果 - チェック設定	
分単位の最後のスキャン結果のチェック間隔（Last scan results check interval in minutes）	（ホスト検出リスト API のアクセス レートに影響します）経過後に最後のスキャン結果を再度チェックする必要がある、分単位の時間間隔です。有効な範囲は 1 ～ 2880 です。
最後のスキャン結果がチェックされる前の最大結果数（Maximum results before last scan results are checked）	（ホスト検出リスト API のアクセス レートに影響します）キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[分単位の最後のスキャン結果のチェック間隔（Last scan results check interval in minutes）] フィールドで指定された時間間隔の前に最後のスキャン結果がチェックされます。有効な範囲は 1 ～ 1000 です。

フィールド名	説明
MAC アドレスの確認（Verify MAC address）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Qualys からの最後のスキャン結果はエンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
分単位のスキャン トリガー間隔（Scan trigger interval in minutes）	（スキャン API のアクセス レートに影響します）経過後にオンデマンドスキャンがトリガーされる、分単位の時間間隔です。有効な範囲は 1 ～ 2880 です。
スキャンがトリガーされる前の最大要求数（Maximum requests before scan is triggered）	（スキャン API のアクセス レートに影響します）キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[分単位のスキャン トリガー間隔（Scan trigger interval in minutes）] フィールドで指定された時間間隔の前にオンデマンド スキャンがトリガーされます。有効な範囲は 1 ～ 1000 です。
分単位のスキャン ステータスのチェック間隔（Scan status check interval in minutes）	経過後に Cisco ISE が Qualys と通信してスキャンのステータスをチェックする、分単位の時間間隔です。有効な範囲は 1 ～ 60 です。
同時にトリガーできるスキャン数（Number of scans that can be triggered concurrently）	（このオプションは、[スキャナ マッピング（Scanner Mappings）] 画面で各 PSN にマッピングされているスキャナの数に依存しています）各スキャナは同時に 1 つの要求のみを処理できます。PSN に複数のスキャナをマッピングしている場合は、選択したスキャナの数に基づいてこの値を増やすことができます。有効な範囲は 1 ～ 200 です。
分単位のスキャン タイムアウト（Scan timeout in minutes）	経過後にスキャン要求がタイムアウトする、分単位の時間です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は 20 ～ 1440 です。
スキャナごとの送信される IP アドレスの最大数（Maximum number of IP addresses to be submitted per scanner）	処理のために Qualys に送信される単一の要求にキュー登録できる要求の数を示します。有効な範囲は 1 ～ 1000 です。
アダプタ ログ ファイル用のログ レベルの選択（Choose the log level for adapter log files）	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー（ERROR）]、[情報（INFO）]、[デバッグ（DEBUG）]、[トレース（TRACE）] です。

ステップ 11 [次へ（Next）] をクリックして、構成設定を確認します。

ステップ 12 [完了（Finish）] をクリックします。

Nexpose アダプタの設定

Cisco ISE 用の Nexpose アダプタを作成して、Nexpose と通信し、VA 結果を取得する必要があります。

始める前に

- Cisco ISE で脅威中心型 NAC サービスを有効にしていることを確認します。
- Nexpose Security Console にログインし、ユーザーアカウントを作成して次の権限をこのアカウントに付与します。
  - サイトの管理
  - レポートの作成
- Cisco ISE の信頼できる証明書ストアに Nexpose サーバー証明書をインポートします（**[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]**）。適切なルートと中間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている（または存在する）ことを確認します。
- HTTPS/SSL（ポート 3780）を介して Nexpose と通信する Cisco ISE。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウンリストから [Rapid7 Nexpose:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば Nexpose と入力します。

設定されているアダプタインスタンスのリストを含むリストウィンドウが表示されます。

ステップ 5 ベンダーインスタンスのリストウィンドウを更新します。新しく追加された Nexpose アダプタのステータスが、[設定準備完了（Ready to Configure）] に変化します。

ステップ 6 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 7 Nexpose の設定画面で次の値を入力し、[次へ（Next）] をクリックします。

フィールド名	説明
Nexpose ホスト（Nexpose Host）	Nexpose サーバーのホスト名。
Nexpose ポート（Nexpose Port）	3780。

フィールド名	説明
ユーザー名（**Username**）	Nexpose 管理者ユーザー アカウント。
パスワード（**Password**）	Nexpose管理者ユーザーアカウントのパスワード。
HTTP プロキシ ホスト（HTTP Proxy Host）	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバーがある場合は、プロキシ サーバーのホスト名を入力します。
HTTP プロキシ ポート（HTTP Proxy Port）	プロキシ サーバーが使用するポート番号を入力します。

ステップ 8 [次へ（Next）] をクリックして拡張設定を設定します。

ステップ 9 [詳細設定（Advanced Settings）] ウィンドウに次の値を入力します。このウィンドウの設定は、オンデマンドスキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド名	説明
最新スキャン結果のチェックの設定	
最新スキャン結果をチェックする間隔（分単位）（**Interval between checking the latest scan results in minutes**）	最新スキャン結果を再度確認するまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。
最新スキャン結果を確認するトリガーとなる保留要求数（**Number of pending requests that can trigger checking the latest scan results**）	[最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）] フィールドに指定した期間が経過していない場合でも、キューに登録されたスキャン要求の数がここで指定する最大数を超えると、最新スキャン結果が確認されます。有効な範囲は 1 ～ 1000 です。
MAC アドレスの確認（**Verify MAC address**）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Nexpose からの最後のスキャン結果はエンドポイントのMACアドレスを含む場合にのみ使用されます。
スキャンの設定	
各サイトのスキャン トリガー間隔（分単位）（**Scan trigger interval for each site in minutes**）	スキャンがトリガーされるまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。

フィールド名	説明
最新スキャン結果のチェックの設定	
各サイトのスキャンのトリガーとなる保留要求の数（**Number of pending requests before a scan is triggered for each site**）	キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[スキャン トリガー間隔（分単位）（Scan trigger interval in minutes）] フィールドで指定された時間間隔が経過する前にスキャンがトリガーされます。有効な範囲は1～1000です。
分単位のスキャン タイムアウト（**Scan timeout in minutes**）	経過後にスキャン要求がタイムアウトする、分単位の時間です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は20～1440です。
スキャンを同時にトリガーできるサイトの数（**Number of sites for which scans could be triggered concurrently**）	スキャンを同時に実行できるサイトの数。有効な範囲は 1 ～ 200 です。
タイムゾーン（**Timezone**）	Nexposeサーバーで設定されているタイム ゾーンに基づいてタイム ゾーンを選択します。
HTTP タイムアウト（秒単位）（Http timeout in seconds）	Cisco ISE が Nexpose からの応答を待機する時間間隔。有効な範囲は 5 ～ 1200 です。
アダプタ ログ ファイル用のログ レベルの選択（**Choose the log level for adapter log files**）	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー（ERROR）]、[情報（INFO）]、[デバッグ（DEBUG）]、[トレース（TRACE）] です。

ステップ 10 [次へ（Next）] をクリックして、構成設定を確認します。

ステップ 11 [完了（Finish）] をクリックします。

Tenable アダプタの設定

Cisco ISE が Tenable SecurityCenter（Nessus スキャナ）と通信し、VA 結果を取得するためには、Tenable アダプタを作成する必要があります。

始める前に

Cisco ISE で Tenable Adapter を設定する前に、Tenable SecurityCenter で次の項目を設定する必要があります。これらの設定については、Tenable SecurityCenter のマニュアルを参照してください。

- Tenable Security Center と Tenable Nessus Vulnerability Scanner がインストールされている必要があります。Tenable Nessus スキャナの登録時に、[登録（Registration）] フィールドで [SecurityCenter で管理（Managed by SecurityCenter）] を必ず選択します。
- Tenable SecurityCenter で Security Manager 権限を持つユーザー アカウントを作成します。
- SecurityCenter でリポジトリを作成します（管理者ログイン情報を使用して Tenable SecurityCenter にログインし、**[リポジトリ（Repository）] > [追加（Add）]** を選択します）。
- リポジトリにスキャン対象のエンドポイント IP 範囲を追加します。
- Nessus スキャナを追加します。
- スキャン ゾーンを作成し、作成したスキャン ゾーンと、これらのスキャン ゾーンにマッピングされているスキャナに、IP アドレスを割り当てます。
- ISE のスキャン ポリシーを作成します。
- アクティブなスキャンを追加し、ISE スキャン ポリシーに関連付けます。設定項目とターゲット（IP/DNS 名）を設定します。
- システム証明書とルート証明書を Tenable SecurityCenter からエクスポートし、Cisco ISE の信頼できる証明書ストアにインポートします（**[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]**）。適切なルートと中間証明書が、Cisco ISE の信頼できる証明書ストアにインポートされている（または存在する）ことを確認します。
- Tenable SecurityCenter 6.4 以降のリリースでは、**SCAN_DEFAULT_SCAN_TIMEOUT** パラメータ値（/opt/sc/src/ の下）を 43200 に設定する必要があります。

（注） HTTPS/SSL（ポート 443）を介して Tenable SecurityCenter と通信する Cisco ISE。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [脅威中心型 NAC（Threat Centric NAC）] > [サードパーティベンダー（Third Party Vendors）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ベンダー（Vendor）] ドロップダウン リストから、[Tenable Security Center:VA] を選択します。

ステップ 4 アダプタ インスタンスの名前を入力します。たとえば、Tenable。

設定されているアダプタインスタンスのリストを含むリストウィンドウが表示されます。

ステップ 5 ベンダーインスタンスのリストウィンドウを更新します。新しく追加された Tenable アダプタのステータスが、[設定準備完了（Ready to Configure）] に変化します。

ステップ 6 [設定準備完了（Ready to Configure）] リンクをクリックします。

ステップ 7 Tenable SecurityCenter の設定画面で次の値を入力し、[次へ（Next）] をクリックします。

フィールド名	説明
Tenable SecurityCenter ホスト（Tenable SecurityCenter Host）	Tenable SecurityCenter のホスト名。
Tenable SecurityCenter ポート（Tenable SecurityCenter Port）	443
ユーザー名（Username）	Tenable SecurityCenter でセキュリティ マネージャ権限を持つユーザー アカウントのユーザー名。
パスワード（Password）	Tenable SecurityCenter でセキュリティ マネージャ権限を持つユーザー アカウントのパスワード。
HTTP プロキシ ホスト（HTTP Proxy Host）	すべてのインターネット トラフィックをルーティングするように設定されたプロキシ サーバーがある場合は、プロキシ サーバーのホスト名を入力します。
HTTP プロキシ ポート（HTTP Proxy Port）	プロキシ サーバーが使用するポート番号を入力します。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [詳細設定（Advanced Settings）] ウィンドウに次の値を入力します。このウィンドウの設定は、オンデマンドスキャンがトリガーされるかどうかや、最後のスキャン結果が VA に使用されるかどうかを決定します。

フィールド名	説明
リポジトリ（Repository）	Tenable SecurityCenter で作成したリポジトリを選択します。
スキャン ポリシー（Scan Policy）	Tenable SecurityCenter で、ISE 用に作成したスキャン ポリシーを選択します。
最新スキャン結果のチェックの設定	
最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）	最新スキャン結果を再度確認するまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。
最新スキャン結果を確認するトリガーとなる保留要求数（Number of pending requests that can trigger checking the latest scan results）	[最新スキャン結果をチェックする間隔（分単位）（Interval between checking the latest scan results in minutes）] フィールドに指定した期間が経過していない場合でも、キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、最新スキャン結果が確認されます。有効な範囲は 1 ～ 1000 です。デフォルトは 10 です。

フィールド名	説明
MAC アドレスの確認（Verify MAC address）	[はい（True）] または [いいえ（False）] です。[はい（True）] に設定した場合、Tenable SecurityCenter からの最新スキャン結果は、エンドポイントの MAC アドレスを含む場合にのみ使用されます。
スキャンの設定	
各サイトのスキャン トリガー間隔（分単位）（Scan trigger interval for each site in minutes）	オンデマンド スキャンがトリガーされるまでの時間間隔（分単位）。有効な範囲は 1 ～ 2880 です。
スキャンのトリガーとなる保留要求の数（Number of pending requests before a scan is triggered）	キューに登録されたスキャン要求の数がここで指定された最大数を超えた場合、[スキャン トリガー間隔（分単位）（Scan trigger interval in minutes）] フィールドで指定された時間間隔が経過する前にオンデマンド スキャンがトリガーされます。有効な範囲は 1 ～ 1000 です。
分単位のスキャン タイムアウト（Scan timeout in minutes）	経過後にスキャン要求がタイムアウトする期間（分単位）です。スキャン要求がタイムアウトすると、アラームが生成されます。有効な範囲は 20 ～ 1440 です。
並列実行可能なスキャンの数（Number of scans that could run in parallel）	同時に実行できるスキャンの数。有効な範囲は 1 ～ 200 です。
HTTP タイムアウト（秒単位）（Http timeout in seconds）	Cisco ISE が Tenable SecurityCenter からの応答を待機する時間間隔。有効な範囲は 5 ～ 1200 です。
アダプタ ログ ファイル用のログ レベルの選択（Choose the log level for adapter log files）	アダプタ用のログ レベルを選択します。使用できるオプションは、[エラー（ERROR）]、[情報（INFO）]、[デバッグ（DEBUG）]、[トレース（TRACE）] です。

ステップ 10 [次へ（Next）] をクリックして、構成設定を確認します。

ステップ 11 [完了（Finish）] をクリックします。

認可プロファイルの設定

Cisco ISE の許可プロファイルに、脆弱性がないかエンドポイントをスキャンするオプションが含まれるようになりました。スキャンの定期的な実行を選択できます。また、これらのスキャンの時間間隔を指定することもできます。許可プロファイルを定義した後、既存の認可ポリシー ルールに適用するか、または新しい認可ポリシー ルールを作成できます。

始める前に

脅威中心型 NAC サービスを有効にし、ベンダー アダプタを設定する必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[許可（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 新規の許可プロファイルを作成するか、既存のプロファイルを編集します。

ステップ 3 [共通タスク（Common Tasks）] 領域で、[脆弱性を評価する（Assess Vulnerabilities）] チェックボックスをオンにします。

ステップ 4 [アダプタ インスタンス（Adapter Instance）] ドロップダウン リストから、設定したベンダー アダプタを選択します。たとえば、Qualys_Instance などです。

ステップ 5 最後のスキャンからの時間がテキスト ボックスよりも大きい場合は、トリガー スキャンのスキャン間隔を時間単位で入力します。有効な範囲は 1 ～ 9999 です。

ステップ 6 [上の間隔を使用して定期的に評価する（Assess periodically using above interval）] チェックボックスをオンにします。

ステップ 7 [送信（Submit）] をクリックします。

脆弱なエンドポイントを隔離する例外ルールの設定

例外ルールを設定し、脆弱なエンドポイントへのアクセスを制限するには、次の脆弱性アセスメント属性を使用できます。

- Threat:Qualys-CVSS_Base_Score
- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

これらの属性は [脅威（Threat）] ディレクトリで使用できます。有効な値の範囲は 0 ～ 10 です。

エンドポイントの隔離、アクセスの制限（別のポータルへのリダイレクト）、または要求の拒否のいずれかを選択できます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー セット（Policy Sets）]** を選択します。
既存のポリシー ルールを編集するか、または VA 属性のチェックについて新しい例外ルールを作成します。

ステップ 2 Qualys スコアを確認して適切な許可プロファイルを割り当てるための条件を作成します。次に例を示します。

Any Identity Group & Threat:Qualys-CVSS_Base_Score > 5 -> Quarantine (authorization profile)

ステップ 3 [保存（Save）] をクリックします。

脆弱性アセスメント ログ

Cisco ISE には、VA サービスのトラブルシューティングのための次のログがあります。

- vaservice.log：VA コア情報が含まれており、TC-NAC サービスを実行しているノードで使用可能です。
- varuntime.log：エンドポイントと VA フローに関する情報が含まれており、モニタリングノードと、TC-NAC サービスを実行しているノードで使用可能です。
- vaaggregation.log：1 時間ごとに収集されるエンドポイントの脆弱性に関する情報が含まれており、プライマリ管理ノードで使用可能です。

信頼できる証明書の設定

次の表では、信頼できる証明書の [編集（Edit）] ウィンドウのフィールドについて説明します。このウィンドウで CA 証明書の属性を編集します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** です。編集する信頼できる証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

表 *1*：信頼できる証明書の編集設定

フィールド名	使用上のガイドライン
証明書発行元（Certificate Issuer）	
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。これはオプションのフィールドです。フレンドリ名を入力しない場合は、次の形式でデフォルト名が生成されます。 *common-name#issuer#nnnnn*
ステータス（Status）	ドロップダウンリストから [有効（Enabled）] または [無効（Disabled）] を選択します。証明書が無効の場合、Cisco ISE は信頼を確立するために証明書を使用しません。
説明（Description）	（任意）説明を入力します。
使用方法（Usage）	

フィールド名	使用上のガイドライン
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書で（他の Cisco ISE ノードまたは LDAP サーバーからの）サーバー証明書を確認する場合は、このチェックボックスをオンにします。
クライアント認証および syslog 用に信頼する（Trust for client authentication and Syslog）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した Cisco ISE に接続するエンドポイントを認証します。 • syslog サーバーを信頼します。
証明書ベースの管理者認証用に信頼する（Trust for certificate based admin authentication）	このチェックボックスをオンにできるのは、[クライアント認証および Syslog 用に信頼する（Trust for client authentication and Syslog）] が選択されている場合のみです。 管理者アクセスの証明書ベースの認証の使用を有効にするには、このチェックボックスをオンにします。信頼できる証明書ストアに必要な証明書チェーンをインポートします。
シスコ サービスの認証用に信頼する（Trust for authentication of Cisco Services）	フィードサービスなどの外部シスコサービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書ステータスの検証（Certificate Status Validation）	Cisco ISE は、特定の CA が発行するクライアントまたはサーバー証明書の失効ステータスをチェックする 2 とおりの方法をサポートしています。1 つめの方法は、Online Certificate Status Protocol（OCSP）を使用して証明書を検証することです（OCSP は、CA によって保持される OCSP サービスに要求を行います）。2 つめの方法は、Cisco ISE に CA からダウンロードした証明書失効リスト（CRL）と照合して証明書を検証することです。どちらの方法も、OCSP を最初に使用してステータスを判断できないときに限り CRL を使用する場合に使用できます。
OCSP サービスに対して検証する（Validate Against OCSP Service）	OCSP サービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まず OCSP サービスを作成する必要があります。

フィールド名	使用上のガイドライン
OCSP が不明なステータスを返した場合は要求を拒否する（Reject the request if OCSP returns UNKNOWN status）	証明書ステータスがOCSPサービスによって判断されなかった場合に要求を拒否するには、このチェックボックスをオンにします。このチェックボックスをオンにした場合、OCSP サービスによって不明なステータス値が返されると、Cisco ISEは現在評価しているクライアントまたはサーバー証明書を拒否します。
OCSP応答側が到達不能な場合は要求を拒否する（Reject the request if OCSP Responder is unreachable）	OCSP 応答側が到達不能な場合に Cisco ISE が要求を拒否するには、このチェックボックスをオンにします。
CRL のダウンロード（Download CRL）	Cisco ISE で CRL をダウンロードするには、このチェックボックスをオンにします。
CRL 配信 URL（CRL Distribution URL）	CA から CRL をダウンロードするための URL を入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URL は「http」、「https」、または「ldap」で始まる必要があります。
CRL の取得（Retrieve CRL）	CRLは、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。
ダウンロードが失敗した場合は待機する（If download failed, wait）	Cisco ISE が CRL を再度ダウンロードするまでに Cisco ISE に必要な試行を待機する必要がある時間間隔を設定します。
CRL を受信しない場合 CRL 検証をバイパスする（Bypass CRL Verification if CRL is not Received）	このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。

フィールド名	使用上のガイドライン
CRL がまだ有効でないか、または期限切れの場合は無視する（Ignore that CRL is not yet valid or expired）	Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。 Cisco ISE で [有効日（Effective Date）] フィールドの開始日と [次の更新（Next Update）] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRL がまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。

関連トピック

信頼できる証明書ストア
信頼できる証明書の編集

メンテナンスの設定

これらのウィンドウでは、バックアップ、復元、およびデータ消去の機能を使用してデータを管理できます。

リポジトリの設定

次の表では、リポジトリを作成してバックアップ ファイルを保存するために使用できる [リポジトリリスト（Repository List）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）]**。

表 *2:* リポジトリの設定

フィールド	使用上のガイドライン
リポジトリ（Repository）	リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。
プロトコル（Protocol）	使用する使用可能なプロトコルの 1 つを選択します。
サーバー名（Server Name）	（TFTP、HTTP、HTTPS、FTP、SFTP、および NFS で必須）リポジトリの作成先サーバーのホスト名または IP アドレス（IPv4 または IPv6）を入力します。 （注） IPv6 アドレスを使用してリポジトリを追加する場合は、IPv6 アドレスを使用して ISE eth0 インターフェイスが設定されていることを確認します。

フィールド	使用上のガイドライン
パス（**Path**）	リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。 この値は、サーバーのルート ディレクトリを示す 2 つのスラッシュ（//）または単一のスラッシュ（/）で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ（/）はルートディレクトリではなく、ローカル デバイス ホーム ディレクトリの FTP を示します。
PKI認証の有効化（Enable PKI authentication）	（オプション：SFTP リポジトリにのみ適用）SFTP リポジトリで RSA 公開キー認証を有効にするには、このチェック ボックスをオンにします。
ユーザー名（User Name）	（FTP、SFTP で必須）指定されたサーバーに対する書き込み権限を持つユーザー名を入力します。ユーザー名には、英数字と _-. /@\$ 文字を含めることができます。
パスワード（Password）	（FTP、SFTP で必須）指定されたサーバーへのアクセスに使用するパスワードを入力します。パスワードに使用できる文字は、0 ～ 9、a ～ z、A ～ Z、-、.、|、@、#、$、^、&、*、,、+、および = です。 !、?、~ のような一部の特殊文字（上記のリストには含まれていません）は、GUI を介した FTP および SFTP パスワード設定で許可されていることに注意してください。ただし、これらの特殊文字は、CLI または Open API による設定には使用できません。

関連トピック

バックアップ/復元リポジトリ
リポジトリの作成

オンデマンド バックアップの設定

次の表では、バックアップを任意の時点で取得するために使用できる [オンデマンドバックアップ（On-Demand Backup）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup & Restore）]** です。

表 *3:* オンデマンド バックアップの設定

フィールド名	使用上のガイドライン
タイプ（**Type**）	次のいずれかを実行します。 • **[設定データのバックアップ（Configuration Data Backup）]**：アプリケーション固有およびCisco ADE オペレーティングシステム両方の構成データが含まれます。 • **[運用データのバックアップ（Operational Data Backup）]**：モニタリングおよびトラブルシューティング データが含まれます。
バックアップ名（**Backup Name**）	バックアップ ファイルの名前を入力します。
リポジトリ名（**Repository Name**）	バックアップ ファイルを保存するリポジトリ。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（**Encryption Key**）	このキーは、バックアップ ファイルの暗号化および解読に使用されます。

関連トピック

- バックアップ データのタイプ
- オンデマンドおよびスケジュール バックアップ
- バックアップ履歴
- バックアップの失敗
- Cisco ISE 復元操作
- 認証および許可ポリシー設定のエクスポート
- 分散環境でのプライマリ ノードとセカンダリ ノードの同期
- オンデマンド バックアップの実行

スケジュール バックアップの設定

次の表では、フルバックアップまたは増分バックアップの復元に使用できる[スケジュールバックアップ（Scheduled Backup）]ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup and Restore）]** です。

表 *4:* スケジュール バックアップの設定

フィールド名	使用上のガイドライン
タイプ（**Type**）	次のいずれかを実行します。 • **[設定データのバックアップ（Configuration Data Backup）]**：アプリケーション固有およびCisco ADE オペレーティングシステム両方の構成データが含まれます。 • **[運用データのバックアップ（Operational Data Backup）]**：モニタリングおよびトラブルシューティング データが含まれます。
名前（**Name**）	バックアップ ファイルの名前を入力します。任意のわかりやすい名前を入力できます。Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加して、ファイルをリポジトリに格納します。複数のバックアップを作成するように設定しても、一意なバックアップ ファイル名を得ることができます。[スケジュールバックアップ（Scheduled Backup）] リストウィンドウで、ファイル名の先頭に「backup_occur」が追加され、このファイルが **kron** ジョブであることを示します。
説明（**Description**）	バックアップの説明を入力します。
リポジトリ名（**Repository Name**）	バックアップ ファイルを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウンリストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
暗号化キー（**Encryption Key**）	バックアップ ファイルを暗号化および復号化するためのキーを入力します。
スケジューリング オプション（**Schedule Options**）	スケジュール バックアップの頻度を選択し、適宜他のオプションに入力します。

関連トピック

- バックアップ データのタイプ
- オンデマンドおよびスケジュール バックアップ
- バックアップ履歴
- バックアップの失敗
- Cisco ISE 復元操作
- 認証および許可ポリシー設定のエクスポート
- 分散環境でのプライマリ ノードとセカンダリ ノードの同期
- CLI を使用したバックアップ

バックアップのスケジュール

ポリシーのエクスポート設定のスケジュール

次の表では、[ポリシーのエクスポートのスケジュール（Schedule Policy Export）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]>[システム（System）]>[バックアップ/復元（Backup and Restore）] > [ポリシーのエクスポート（Policy Export）]** です。

表 *5:* ポリシーのエクスポート設定のスケジュール

フィールド名	使用上のガイドライン
暗号化（Encryption）	
暗号キー（Encryption Key）	エクスポートデータを暗号化および復号化するためのキーを入力します。このフィールドは、[暗号キーを使用したエクスポート（Export with Encryption Key）] オプションを選択した場合にのみ有効になります。
宛先（Destination）	
ローカル コンピュータにファイルをダウンロード（Download file to local computer）	ポリシー エクスポート ファイルをローカル システムにダウンロードできます。
ファイルをメールで送信（Email file to）	複数の電子メールアドレスは、カンマで区切ることで入力できます。
リポジトリ（Repository）	ポリシーデータをエクスポートするリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウンリストから利用可能なリポジトリのみを選択できます。ポリシーのエクスポートのスケジュールを設定する前に、リポジトリを作成してください。
今すぐエクスポート（Export Now）	データをローカルコンピュータにエクスポートするか、電子メールの添付ファイルとして送信するには、このオプションをクリックします。リポジトリにエクスポートすることはできません。リポジトリのエクスポートのみをスケジュールできます。
スケジュール（Schedule）	
スケジューリング オプション（Schedule Options）	エクスポートのスケジュールの頻度を選択し、それに応じてその他の詳細を入力します。

一般 TrustSec の設定

Cisco ISE が TrustSec サーバーとして機能したり、TrustSec サービスを提供したりするには、グローバル TrustSec 設定を定義します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSec の全般設定（General TrustSec Settings）]。

TrustSec 展開の確認

このオプションを選択すると、すべてのネットワークデバイスに最新の TrustSec ポリシーが展開されているかどうかを確認できます。Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合は [アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] および [ホーム（Home）] > [サマリ（Summary）]）にアラームが表示されます。TrustSec ダッシュ ボードに、以下のアラームが表示されます。

- 検証プロセスが開始または完了するたびに、[情報（Info）] アイコンとともにアラームが表示されます。
- 新しい展開要求により検証プロセスがキャンセルされた場合は、[情報（Info）] アイコンとともにアラームが表示されます。
- 検証プロセスがエラーで失敗した場合は、[警告（Warning）] アイコンとともにアラームが表示されます。たとえば、ネットワーク デバイスとの SSH 接続を開けない場合やネットワーク デバイスが使用できない場合、あるいは Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合などです。

[展開の検証（Verify Deployment）] オプションは、次のウィンドウでも使用できます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。：

- **[ワーク センター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティ グループ（Security Groups）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ ACL（Security Group ACLs）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [送信元ツリー（Source Tree）]**
- **[ワーク センター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [宛先ツリー（Destination Tree）]**

[すべての展開後に自動検証（Automatic Verification After Every Deploy）]：それぞれの展開後に、Cisco ISE ですべてのネットワーク デバイス上の更新を検証するには、このチェックボッ

クスをオンにします。展開プロセスが完了したら、[展開プロセス後の時間（Time after Deploy Process）] フィールドに指定した時間が経過した後に、検証プロセスが開始されます。

[展開プロセス後の時間（Time after Deploy Process）]：展開プロセスが完了した後、検証プロセスを開始する前に Cisco ISE に待機させる時間を指定します。有効な範囲は、10 ～ 60 分です。

待機期間中に新しい展開が要求された場合や別の検証が進行中の場合は、現在の検証プロセスはキャンセルされます。

[今すぐ検証（Verify Now）]：検証プロセスをすぐに開始するには、このオプションをクリックします。

Protected Access Credential（PAC）

- [トンネル PAC の存続可能時間（Tunnel PAC Time to Live）]：

  PAC の有効期限を指定します。トンネル PAC は EAP-FAST プロトコル用のトンネルを生成します。時間を秒、分、時、日数、または週数で指定できます。デフォルト値は 90 日です。有効な範囲は次のとおりです。

  - 1 ～ 157680000 秒
  - 1 ～ 2628000 分
  - 1 ～ 43800 時間
  - 1 ～ 1825 日
  - 1 ～ 260 週間

- [プロアクティブ PAC 更新を次の後に実行する（Proactive PAC Update Will Occur After）]：Cisco ISE は、認証に成功した後、設定したパーセンテージのトンネル PAC TTL が残っているときに、新しい PAC をクライアントに予防的に提供します。PAC の期限が切れる前に最初の認証が正常に行われると、サーバーはトンネル PAC の更新を開始します。このメカニズムにより、有効な PAC でクライアントが更新されます。デフォルト値は 10% です。

セキュリティグループタグ番号の割り当て

- [システムで SGT 番号を割り当てる（System will Assign SGT Numbers）]：Cisco ISE に SGT 番号を自動生成させる場合は、このオプションを選択します。
- [範囲内の番号を除外する（Except Numbers In range）]：手動設定用に SGT 番号の範囲を予約する場合は、このオプションを選択します。Cisco ISE は、SGT の生成時にこの範囲の数値を使用しません。
- [ユーザーが手動で SGT 番号を入力する（User Must Enter SGT Numbers Manually）]：SGT 番号を手動で定義する場合は、このオプションを選択します。

APIC EPGのセキュリティグループタグのナンバリング（Security Group Tag Numbering for APIC EPGs）

[APIC EPGのセキュリティグループタグのナンバリング（Security Group Tag Numbering for APIC EPGs）]：APIC から学習した EPG に基づいて SGT を作成する場合は、このチェックボックスをオンにし、使用する番号の範囲を指定します。

セキュリティグループの自動作成

[認証ルールを作成するときにセキュリティグループを自動作成する（Auto Create Security Groups When Creating Authorization Rules）]：認証ポリシーのルールを作成する際に SGT を自動的に作成する場合は、このチェックボックスをオンにします。

このオプションを選択した場合は、[認証ポリシー（Authorization Policy）] ウィンドウの上部に、`Auto Security Group Creation is On` というメッセージが表示されます。

自動作成された SGT は、ルール属性に基づいて命名されます。

（注） 自動作成された SGT は、それに対応する認可ポリシールールを削除しても削除されません。

デフォルトでは、新規インストールまたはアップグレードの後でこのオプションが無効になります。

- [自動命名オプション（Automatic Naming Options）]：自動作成される SGT の命名規則を定義するには、このオプションを使用します。

  （必須）[名前に次が含まれます（Name Will Include）]：次のオプションのいずれかを選択します。

  - **ルール名（Rule name）**
  - **SGT番号（SGT number）**
  - **ルール名およびSGT番号（Rule name and SGT number）**

  デフォルトでは、[ルール名（Rule name）] オプションが選択されます。

  オプションで、SGT 名に以下の情報を追加できます。

  - **ポリシーセット名（Policy Set Name）**（このオプションは [ポリシーセット（Policy Sets）] が有効な場合にのみ使用可能です）
  - **プレフィックス（Prefix）**（8 文字まで）
  - **サフィックス（Suffix）**（8 文字まで）

  Cisco ISE は、選択内容に応じて [サンプル名（Example Name）] フィールドにサンプル SGT 名を表示します。

同じ名前の SGT が存在している場合、ISE は SGT 名に「_x」を付け加えます。x は（現在の名前に 1 が使用されていない場合は）1 から始まる最初の値です。新しい名前が 32 文字より長い場合、Cisco ISE によって最初の 32 文字に切り捨てられます。

ホスト名の IP SGT 静的マッピング（IP SGT Static Mapping of Hostnames）

[ホスト名の IP SGT 静的マッピング（IP SGT Static Mapping of Hostnames）]：FQDN とホスト名が使用される場合、Cisco ISE はマッピングを展開して展開状態を検査する際に、PAN および PSN ノード内の対応する IP アドレスを検索します。DNS クエリによって返される IP アドレス用に作成されるマッピングの数を指定する場合は、このオプションを使用します。次のいずれかのオプションを選択できます。

- **DNS クエリによって返されるすべての IP アドレスに対してマッピングを作成する（Create mappings for all IP addresses returned by a DNS query）**
- **DNSクエリによって返される最初のIPv4アドレスおよび最初のIPv6アドレスに対してのみマッピングを作成する（Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query）**

ネットワークデバイス用TrustSec HTTPサービス

- [HTTP サービスを有効化（Enable HTTP Service）]：HTTPを使用して、ポート 9063 経由で TrustSec データをネットワークデバイスに転送します。
- [応答ペイロード本文を監査に含める（Include entire response payload body in Audit）]：監査ログに TrustSec HTTP 応答ペイロード本文全体を表示する場合は、このオプションを有効にします。このオプションを選択すると、パフォーマンスが大幅に低下する可能性があります。このオプションを無効にすると、HTTP ヘッダー、ステータス、および認証情報のみがログに記録されます。

関連トピック

TrustSec アーキテクチャ
TrustSec のコンポーネント
TrustSec のグローバル設定

ネットワーク リソース

セッション認識型ネットワーク（SAnet）のサポート

Cisco ISE は、セッション認識型ネットワーキング（SAnet）に対する限定的なサポートを提供します。SAnet は、多くのシスコスイッチで実行するセッション管理フレームワークです。SAnet は、可視性、認証、認可などのアクセスセッションを管理します。SAnet は、RADIUS 認可属性が含まれているサービステンプレートを使用します。Cisco ISE には、認証プロファイル内にサービステンプレートが含まれています。Cisco ISE は、プロファイルを「サービス

テンプレート」互換として識別するフラグを使用して認証プロファイルのサービステンプレートを識別します。

Cisco ISE 認証プロファイルには、属性のリストに変換される RADIUS 認可属性が含まれています。また、SAnet サービステンプレートには、RADIUS 認可属性も含まれていますが、これらの属性はリストに変換されません。

SAnetデバイスの場合、Cisco ISEはサービステンプレートの名前を送信します。キャッシュ内にそのコンテンツか、または静的に定義された設定が存在しない限り、デバイスはサービステンプレートのコンテンツをダウンロードします。サービステンプレートによってRADIUS属性が変更されると、Cisco ISE はデバイスに CoA 通知を送信します。

ネットワーク デバイス

後続の項で説明されているウィンドウを使用して、Cisco ISE でネットワークデバイスを追加および管理できます。

ネットワーク デバイス定義の設定

次の表では、Cisco ISE のネットワーク アクセス デバイスを設定するために使用できる [ネットワークデバイス（Network Devices）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** で、**[追加（Add）]** をクリックします。

ネットワーク デバイスの設定

次の表では、**[新しいネットワークデバイス（New Network Devices）]** ウィンドウのフィールドについて説明します。

表 *6:* ネットワーク デバイスの設定

フィールド名	説明
名前（Name）	ネットワークデバイスの名前を入力します。 ネットワークデバイスに、デバイスのホスト名とは異なるわかりやすい名前を指定できます。デバイス名は論理識別子です。 （注）　必要に応じて、設定後にデバイスの名前を変更できます。
説明（Description）	このデバイスの説明を入力します。

フィールド名	説明
IP アドレス（IP Address）または**IP 範囲（IP Range）**	ドロップダウンリストから次のいずれかを選択し、表示されるフィールドに必要な値を入力します。 • [IP アドレス（IP Address）]：単一の IP アドレス（IPv4 または IPv6 アドレス）とサブネットマスクを入力します。 • [IP 範囲（IP Ranges）]：必要な IPv4 アドレスの範囲を入力します。認証時に IP アドレスを除外するには、[除外（Exclude）] フィールドに IP アドレスまたは IP アドレスの範囲を入力します。 IP アドレスとサブネットマスクまたは IP アドレスの範囲を定義するためのガイドラインを次に示します。 • 特定の IP アドレスを定義するか、サブネットマスクを使用して IP 範囲を定義できます。デバイス A の IP アドレス範囲が定義されている場合、デバイス A に定義されている範囲の個別のアドレスを別のデバイス B に設定できます。 • すべてのオクテットの IP アドレス範囲を定義できます。IP アドレスの範囲を指定するときに、ハイフン（-）またはアスタリスク（*）をワイルドカードとして使用できます。たとえば、*.*.*.*、1-10.1-10.1-10.1-10 または 10-11.*.5.10-15 などです。 • サブセットがすでに追加されている場合は、設定された範囲からその IP アドレス範囲のサブセットを除外できます。例：10.197.65.*/10.197.65.1 または 10.197.65.* exclude 10.197.65.1。 • ネットワークデバイスごとに最大 40 の IP アドレス、または IP 範囲を設定できます。 • 同じ IP アドレスを持つ 2 台のデバイスを定義することはできません。 • 同じ IP 範囲を持つ 2 台のデバイスを定義することはできません。IP 範囲は、一部または全部が重複することはできません。 • IP アドレスを除外する場合は、重複する IP 範囲を使用しないでください。代わりに、独立した IP 範囲を除外してください。
デバイスプロファイル（Device Profile）	ドロップダウンリストから、ネットワークデバイスのベンダーを選択します。 選択したベンダーのネットワークデバイスがサポートしているフローおよびサービスを表示するには、ドロップダウンリストの横にあるツールのヒントを使用します。ツールのヒントには、デバイスが使用する URL リダイレクトの RADIUS 認可変更（CoA）ポートとタイプも表示されます。これらの属性は、デバイス タイプのネットワーク デバイス プロファイルで定義されます。

フィールド名	説明
モデル名（**Model Name**）	ドロップダウンリストからデバイスのモデルを選択します。 モデル名は、ルールベースのポリシーの条件をチェックするときに、パラメータの1つとして使用します。この属性は、デバイスディクショナリにあります。
ソフトウェアバージョン（**Software Version**）	ドロップダウンリストから、ネットワークデバイスで実行するソフトウェアのバージョンを選択します。 ソフトウェアバージョンは、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性は、デバイスディクショナリにあります。
ネットワーク デバイス グループ（**Network Device Group**）	[ネットワークデバイスグループ（Network Device Group）] 領域で、[ロケーション（Location）]、**[IPSec]**、および [デバイスタイプ（Device Type）] ドロップダウンリストから必要な値を選択します。 グループに明確にデバイスを割り当てないと、そのグループはデフォルトのデバイスグループ（ルート ネットワーク デバイス グループ）に含まれます。これにより、ロケーションは [すべてのロケーション（All Locations）]、デバイスタイプは [すべてのデバイスタイプ（All Device Types）] となります。

（注） フィルタを使用して Cisco ISE 展開からネットワーク アクセス デバイス（NAD）を選択して削除する場合は、ブラウザのキャッシュをクリアして、選択した NAD のみが削除されるようにします。

RADIUS 認証設定

次の表では、[RADIUS 認証設定（RADIUS Authentication Settings）] 領域のフィールドについて説明します。

表 *7 : [RADIUS* 認証設定（*RADIUS Authentication Settings***）*]* 領域**

フィールド名	使用上のガイドライン
RADIUS UDP の設定	
プロトコル（**Protocol**）	選択したプロトコルとして **RADIUS** を表示します。

フィールド名	使用上のガイドライン
共有秘密鍵（Shared Secret）	ネットワーク デバイスの共有秘密鍵を入力します。 共有秘密鍵は、**pac** オプションを指定した **radius-host** コマンドを使用してネットワークデバイスに設定したキーです。 （注） 共有秘密鍵の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ウィンドウ（[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デバイスセキュリティ設定（Device Security Settings）]）の [RADIUS 共有秘密鍵の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります。 RADIUS サーバーでのベストプラクティスは、22 文字にすることです。新規インストールおよびアップグレードされた展開の場合、共有秘密鍵の長さはデフォルトで 4 文字です。この値は [デバイスセキュリティ設定（Device Security Settings）] ウィンドウで変更できます。
2 番目の共有秘密の使用（Use Second Shared Secret）	ネットワークデバイスと Cisco ISE で使用される 2 番目の共有秘密鍵を指定します。 （注） Cisco TrustSec デバイスには、デュアル共有秘密（鍵）の利点がありますが、Cisco ISE により送信される Cisco TrustSec CoA パケットは常に最初の共有秘密（鍵）を使用します。2 番目の共有秘密鍵の使用を有効にするには、Cisco TrustSec CoA パケットを Cisco TrustSec デバイスに送信する Cisco ISE ノードを選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources }] > [ネットワークデバイス（Network Devices）] > [追加（Add）] > [高度な TrustSec 設定（Advanced Trustsec Settings）]** ウィンドウの [送信元（Send From）] ドロップダウンリストで、このタスクに使用する Cisco ISE ノードを設定します。プライマリ管理ノード（PAN）またはポリシーサービスノード（PSN）を選択できます。選択した PSN ノードがダウンしている場合、PAN は Cisco TrustSec デバイスに Cisco TrustSec CoA パケットを送信します。 （注） RADIUS アクセス要求の 2 番目の共有秘密機能は、[Message-Authenticator] フィールドを含むパケットに対してのみ機能します。

フィールド名	使用上のガイドライン
CoA ポート（CoA Port）	RADIUS CoA に使用するポートを指定します。 デバイスのデフォルトの CoA ポートは、ネットワークデバイス用に設定されたネットワーク デバイス プロファイルで定義されます（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）]**）。デフォルト CoA ポートを使用するには、[デフォルトに設定（Set To Default）] をクリックします。 （注） [RADIUS 認証設定（RADIUS Authentication Settings）] の **[ネットワークデバイス（Network Devices）]** ウィンドウ（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]**）で指定した CoA ポートを変更する場合は、**[ネットワークデバイスプロファイル（Network Device Profile）]** ウィンドウ（**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）]**）で対応するプロファイルに同じ CoA ポートを指定します。
RADIUS DTLS の設定	
必要な DTLS（DTLS Required）	[必要な DTLS（DTLS Required）] チェックボックスをオンにすると、Cisco ISE ではこのデバイスからの DTLS 要求のみが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS はセキュアソケットレイヤ（SSL）トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、Message Digest 5（MD5）完全性チェックを計算するために使用されます。
CoA ポート（CoA Port）	RADIUS DTLS CoA に使用するポートを指定します。
CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）	ドロップダウンリストから RADIUS DTLS CoA に使用する認証局を選択します。

フィールド名	使用上のガイドライン
DNS 名（DNS Name）	ネットワーク デバイスの DNS 名を入力します。[RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification）] オプションが [RADIUS 設定（RADIUS Settings）] ウィンドウ（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[RADIUS]**）で有効になっている場合、Cisco ISE はこの DNS 名とクライアント証明書で指定されている DNS 名を比較して、ネットワークデバイスの ID を確認します。
全般設定	
KeyWrap の有効化（Enable KeyWrap）	KeyWrap アルゴリズムがネットワークデバイスでサポートされている場合にのみ、[KeyWrap の有効化（Enable KeyWrap）] チェックボックスをオンにします。ネットワークデバイスは、AES KeyWrap RFC（RFC 3394）と互換性がある必要があります。 このオプションは、AES KeyWrap アルゴリズムを介して RADIUS セキュリティを強化するために使用されます。
キー暗号キー（Key Encryption Key）	セッションの暗号化（秘密）に使用される暗号キーを入力します。
メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）	RADIUS メッセージに対するキー付きハッシュメッセージ認証コード（HMAC）の計算に使用されるキーを入力します。
キー入力形式（Key Input Format）	次のいずれかのオプション ボタンをクリックします。 • [ASCII] : [キー暗号キー（Key Encryption Key）] フィールドに入力する値の長さは16 文字（バイト）、[メッセージ認証コードキー（Message Authenticator Code Key）] フィールドに入力する値の長さは 20 文字（バイト）にする必要があります。 • [16 進数（Hexadecimal）] : [キー暗号キー（Key Encryption Key）] フィールドに入力する値の長さは 32 文字（バイト）、[メッセージ認証コードキー（Message Authenticator Code Key）] フィールドに入力する値の長さは 40 文字（バイト）にする必要があります。 ネットワークデバイスの設定と一致するように、キー暗号キーおよびメッセージ認証コードキーの入力に使用するキー入力形式を指定できます。指定する値はキーの正しい（全体の）長さにする必要があり、それよりも短い値は許可されません。

TACACS 認証設定

表 *8 : [TACACS* 認証設定（*TACACS Authentication Settings*）*]* 領域のフィールド

フィールド名	使用上のガイドライン
共有秘密鍵（**Shared Secret**）	TACACS+ プロトコルが有効のときにネットワークデバイスに割り当てられたテキストの文字列。ユーザーは、ネットワークデバイスによってユーザー名およびパスワードが認証される前にテキストを入力する必要があります。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。
廃止された共有秘密がアクティブです（**Retired Shared Secret is Active**）	リタイアメント期間がアクティブな場合に表示されます。
廃止（**Retire**）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、ダイアログボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。
残りの廃止期間（**Remaining Retired Period**）	（[廃止（Retire）] ダイアログボックスで [はい（Yes）] を選択した場合にのみ利用可能）**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[設定（Settings）]** > **[接続設定（Connection Settings）]** > **[デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]** で指定されたデフォルト値が表示されます。必要に応じて、デフォルト値を変更できます。 古い共有秘密は、指定された日数の間はアクティブなままになります。
終了（**End**）	（[廃止（Retire）] ダイアログボックスで [はい（Yes）] をクリックした場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。
シングル接続モードを有効にする（**Enable Single Connect Mode**）	[シングル接続モードを有効にする（Enable Single Connect Mode）] チェックボックスは、ネットワークデバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかのオプションボタンをクリックします。 • **[レガシーシスコデバイス（Legacy Cisco Devices）]** • **[TACACS ドラフトコンプライアンスシングル接続のサポート（TACACS Draft Compliance Single Connect Support）]** （注） [シングル接続モード（Single Connect Mode）] を無効にすると、Cisco ISE はすべての TACACS 要求に対して新しい TCP 接続を使用します。

SNMP 設定

次の表では、[SNMP 設定（SNMP Settings）] セクションのフィールドについて説明します。

表 *9 : [SNMP*設定（***SNMP Settings***）*]*領域のフィールド

フィールド名	使用上のガイドライン
SNMP バージョン（SNMP Version）	[SNMP バージョン（SNMP Version）] ドロップダウンリストから、次のいずれかのオプションを選択します。 • **1**：SNMPv1 は informs をサポートしていません。 • **2c** • 3：SNMPv3 は、[セキュリティレベル（Security Level）] フィールドで [Priv] を選択した場合にパケットの暗号化が可能であるため、最もセキュアなモデルです。 （注） ネットワークデバイスに SNMPv3 パラメータを設定した場合、モニタリングサービス（**[操作（Operations）] > （[レポート（Reports）] > [診断（Diagnostics）] > [ネットワークデバイスセッションステータス（Network Device Session Status）]**）によって提供される [ネットワーク デバイス セッション ステータス（Network Device Session Status）] 概要レポートを生成できません。ネットワークデバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。
SNMP RO コミュニティ（SNMP RO Community）	（SNMP バージョン 1 および 2c にのみ適用可能）Cisco ISE にデバイスへの特定タイプのアクセスを提供する読み取り専用コミュニティ文字列を入力します。 （注） キャレット記号（曲折アクセント付き^）は使用できません。
SNMP ユーザー名（SNMP Username）	（SNMP バージョン 3 の場合のみ）SNMP ユーザー名を入力します。
セキュリティ レベル（Security Level）	（SNMP バージョン 3 の場合のみ）[セキュリティレベル（Security Level）] ドロップダウンリストから次のオプションのいずれかを選択します。 • **[Auth]**：MD5 またはセキュア ハッシュ アルゴリズム（SHA）パケットの認証を有効にします。 • **[No Auth]**：認証なし、プライバシーなしのセキュリティレベル。 • **[Priv]**：Data Encryption Standard（DES; データ暗号規格）パケットの暗号化を有効にします。

フィールド名	使用上のガイドライン
認証プロトコル（**Auth Protocol**）	（SNMP バージョン 3 でセキュリティレベル [Auth] または [Priv] を選択した場合のみ）[認証プロトコル（Auth Protocol）] ドロップダウンリストから、ネットワークデバイスで使用する認証プロトコルを選択します。 • **[MD5]** • **[SHA]**
認証パスワード（**Auth Password**）	（SNMP バージョン 3 で [Auth] および [Priv] セキュリティレベルを選択した場合のみ）認証キーを入力します。8 文字以上の長さにする必要があります。 デバイスにすでに設定されている認証パスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き^）を使用することはできません。
プライバシー プロトコル（**Privacy Protocol**）	（SNMP バージョン 3 で [Priv] セキュリティレベルを選択した場合のみ）[プライバシープロトコル（Privacy Protocol）] ドロップダウンリストから次のいずれかのオプションを選択します。 • **DES** • **AES128** • **AES192** • **AES256** • **3DES**
プライバシー パスワード（**Privacy Password**）	（SNMP バージョン 3 で [Priv] セキュリティレベルを選択した場合のみ）プライバシーキーを入力します。 デバイスにすでに設定されているプライバシーパスワードを表示するには、[表示（Show）] をクリックします。 （注） キャレット記号（曲折アクセント付き^）を使用することはできません。
ポーリング間隔（**Polling Interval**）	ポーリング間隔を秒単位で入力します。デフォルト値は 3600 です。
リンク トラップ クエリー（**Link Trap Query**）	SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、[リンクトラップクエリ（Link Trap Query）] チェックボックスをオンにします。

フィールド名	使用上のガイドライン
MAC トラップ クエリ（MAC Trap Query）	SNMP トラップを介して受信する MAC 通知を受信して解釈するには、[MAC トラップクエリ（MAC Trap Query）] チェックボックスをオンにします。
送信元ポリシー サービス ノード（Originating Policy Services Node）	[送信元ポリシーサービスノード（Originating Policy Services Node）] ドロップダウンリストから、SNMP データのポーリングに使用する Cisco ISE サーバーを選択します。このフィールドのデフォルト値は [自動（Auto）] です。ドロップダウンリストから特定の値を選択して、設定を上書きします。

高度な TrustSec 設定

次の表は、[高度なTrustSec設定（Advanced TrustSec Settings）] セクションのフィールドについて説明しています。

表 *10 : [*高度な *TrustSec* 設定（*Advanced TrustSec Settings*）*]* 領域のフィールド

フィールド名	使用上のガイドライン
デバイスの認証設定	
TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）	[デバイスID（Device ID）] フィールドにデバイス ID としてデバイス名をリストするには、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスをオンにします。
デバイスID（Device ID）	このフィールドは、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスがオフになっている場合にのみ使用できます。
パスワード（Password）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
HTTP REST API の設定	
HTTP REST API の有効化（Enable HTTP REST API）	HTTP REST API を使用して、ネットワークデバイスに必要な Cisco TrustSec 情報を提供するには、[HTTP REST API の有効化（Enable HTTP REST API）]チェックボックスをオンにします。これにより、効率性と能力が向上し、RADIUS プロトコルと比較して、短時間で大規模な設定をダウンロードできます。また、UDP を介した TCP を使用することで、信頼性が向上します。

フィールド名	使用上のガイドライン
ユーザー名（**Username**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したユーザー名を入力します。ユーザー名にスペース、!%^:;、[{|}] ' "= <>? を含めることはできません
パスワード（**Password**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。
TrustSec デバイスの通知および更新	
デバイスID（**Device ID**）	このフィールドは、[TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）] チェックボックスがオフになっている場合にのみ使用できます。
パスワード（**Password**）	Cisco TrustSec デバイスを認証するために Cisco TrustSec デバイスの CLI で設定したパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
環境データのダウンロード間隔 <...>（**Download Environment Data Every <...>**）	この領域のドロップダウンリストから必要な値を選択して、デバイスが Cisco ISE から環境データをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で選択できます。デフォルト値は 1 日です。
ピア許可ポリシーのダウンロード間隔 <...>（**Download Peer Authorization Policy Every <...>**）	デバイスが Cisco ISE からピア認証ポリシーをダウンロードする必要がある時間間隔を、この領域のドロップダウンリストから必要な値を選択して指定します。時間間隔を秒、分、時、日数、または週数で指定できます。デフォルト値は 1 日です。
再認証間隔 <...>（**Reauthentication Every <...>**）	この領域のドロップダウンリストから必要な値を選択して、最初の認証後、デバイスが Cisco ISE に対して自身を再認証する時間間隔を指定します。時間間隔は秒、分、時、日、または週で設定できます。たとえば 1000 秒と入力すると、デバイスは 1000 秒ごとに Cisco ISE に対して自身を認証します。デフォルト値は 1 日です。
SGACL リストのダウンロード間隔 <...>（**Download SGACL Lists Every <...>**）	この領域のドロップダウンリストから必要な値を選択して、デバイスが Cisco ISE から SGACL リストをダウンロードする時間間隔を指定します。時間間隔は秒、分、時、日、または週で設定できます。デフォルト値は 1 日です。

フィールド名	使用上のガイドライン
その他の TrustSec デバイスでこのデバイスを信頼する（信頼できる TrustSec）（Other TrustSec Devices to Trust This Device (TrustSec Trusted)）	すべてのピアデバイスがこの Cisco TrustSec デバイスを信頼できるようにするには、[このデバイスを信頼する他の TrustSec デバイス（Other TrustSec Devices to Trust This Device）] チェックボックスをオンにします。このチェックボックスをオフにした場合、ピアデバイスはこのデバイスを信頼せず、このデバイスから到着したすべてのパケットが適宜色付けまたはタグ付けされます。
設定変更のデバイスへの送信（Send Configuration Changes to Device）	Cisco ISE で CoA または CLI（SSH）を使用して Cisco TrustSec 構成変更を Cisco TrustSec デバイスに送信する場合は、[構成変更のデバイスへの送信（Send Configuration Changes to Device）] チェックボックスをオンにします。必要に応じて、[CoA] または [CLI（SSH）（CLI (SSH)）] オプションボタンをクリックします。 Cisco ISE で CoA を使用して設定変更を Cisco TrustSec デバイスに送信する場合は、[CoA] オプションボタンをクリックします。 Cisco ISE で CLI を使用（SSH 接続を使用）して設定変更を Cisco TrustSec デバイスに送信するには、[CLI（SSH）（CLI (SSH)）] オプションボタンをクリックします。詳細については、非 CoA サポート デバイスへの設定変更のプッシュを参照してください。
送信元（Send From）	ドロップダウンリストから、設定変更を Cisco TrustSec デバイスに送信する必要がある送信元 Cisco ISE ノードを選択します。PAN または PSN を選択できます。選択した PSN がダウンした場合、PSN を使用して Cisco TrustSec デバイスに設定変更が送信されます。
テスト接続（Test Connection）	Cisco TrustSec デバイスと選択した Cisco ISE ノード（PAN または PSN ノード）の間の接続をテストするには、このオプションを使用できます。
SSH キー（SSH Key）	この機能を使用するには、Cisco ISE からネットワーク デバイスへの SSHv2 トンネルを開き、デバイスの CLI を使用して SSH キーを取得します。確認のために、このキーをコピーして [SSHキー（SSH Key）] フィールドに貼り付ける必要があります。詳細については、SSH キーの検証を参照してください。
デバイス構成の展開	

フィールド名	使用上のガイドライン
セキュリティ グループ タグ マッピングの展開時にこのデバイスを含める（**Include this device when deploying Security Group Tag Mapping Updates**）	Cisco TrustSec デバイスがデバイスインターフェイスのログイン情報を使用して IP-SGT マッピングを取得するには、[セキュリティ グループ タグ マッピングの更新の展開時にこのデバイスを含める（Include this device when deploying Security Group Tag Mapping Updates）] チェックボックスをオンにします。
EXEC モード ユーザー名（EXEC Mode Username）	Cisco TrustSec デバイスへのログインに使用するユーザー名を入力します。
EXEC モード パスワード（EXEC Mode Password）	デバイス パスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。 （注） セキュリティの脆弱性を回避するために、EXEC モードやイネーブルモードのパスワードを含むパスワードの文字に % を使用しないことを推奨します。
有効モード パスワード（Enable Mode Password）	（任意）特権 EXEC モードで Cisco TrustSec デバイスの設定を編集するために使用する有効なパスワードを入力します。 パスワードを表示するには、[表示（Show）] をクリックします。
アウトオブバンドTrustSec PAC	
発行日（Issue Date）	この Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の発行日を表示します。
期限日（Expiration Date）	この Cisco TrustSec デバイス用に Cisco ISE によって生成された最後の Cisco TrustSec PAC の期限日を表示します。
発行元（Issued By）	このデバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行者（Cisco TrustSec 管理者）の名前を表示します。
PAC の生成（Generate PAC）	Cisco TrustSec デバイスのアウトオブバンド Cisco TrustSec PAC を生成するには、[PACの生成（Generate PAC）] ボタンをクリックします。

デフォルトのネットワーク デバイス定義の設定

次の表では、Cisco ISE が RADIUS または TACACS+ 認証に使用できる、デフォルトのネットワークデバイスを設定できるようにする [デフォルトのネットワークデバイス（Default Network device）] ウィンドウのフィールドについて説明します。次のナビゲーションパスのいずれかを選択します。

- **[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [デフォルトのデバイス（Default Devices）]**
- **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク ソース（Network Resources）] > [デフォルトのデバイス（Default Devices）]**

表 *11 : [*デフォルトのネットワークデバイス（***Default Network Device***）*]* ウィンドウのフィールド

フィールド名	使用上のガイドライン
デフォルトのネットワーク デバイスのステータス（Default Network Device Status）	デフォルトのネットワークデバイスの定義を有効にするには、[デフォルトのネットワークデバイスのステータス（Default Network Device Status）] ドロップダウンリストから [有効化（Enable）] を選択します。 （注） デフォルトのデバイスが有効になっている場合は、ウィンドウ内の関連するチェックボックスをオンにすることで、RADIUS または TACACS+ の認証設定を有効にする必要があります。
デバイス プロファイル（Device Profile）	デフォルトのデバイスベンダーとして [シスコ（Cisco）] が表示されます。
RADIUS 認証設定	
RADIUS の有効化（Enable RADIUS）	デバイスの RADIUS 認証を有効にするには、[RADIUS の有効化（Enable RADIUS）] チェックボックスをオンにします。
RADIUS UDP の設定	

フィールド名	使用上のガイドライン
共有秘密鍵（Shared Secret）	共有秘密を入力します。共有秘密情報の長さは、最大 127 文字です。 共有秘密鍵は、pac キーワードを指定した radius-host コマンドを使用してネットワークデバイスに設定したキーです。 （注） 共有秘密の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ウィンドウ（**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイス（Network Devices）]** > **[デバイスのセキュリティ設定（Device Security Settings）]**）の [RADIUS 共有秘密の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります。デフォルトでは、この値は新規インストールとアップグレードされた展開の場合は 4 文字です。RADIUS サーバーでのベストプラクティスは、22 文字にすることです。
RADIUS DTLS の設定	
必要な DTLS（DTLS Required）	[必要な DTLS（DTLS Required）] チェックボックスをオンにすると、Cisco ISE ではこのデバイスからの DTLS 要求のみが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。 RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。
共有秘密鍵（Shared Secret）	RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。
CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）	RADIUS DTLS CoA に使用する認証局を [CoA の ISE 証明書の発行元 CA（Issuer CA of ISE Certificates for CoA）] ドロップダウンリストから選択します。
全般設定	
KeyWrap の有効化（Enable KeyWrap）	（任意）KeyWrap アルゴリズムがネットワークデバイスでサポートされている場合にのみ [KeyWrap の有効化（Enable KeyWrap）] チェックボックスをオンにします。これにより AES KeyWrap アルゴリズムを介した RADIUS のセキュリティが強化されます。
キー暗号キー（Key Encryption Key）	KeyWrap を有効にした場合は、セッションの暗号化（秘密）に使用する暗号キーを入力します。

フィールド名	使用上のガイドライン
メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）	KeyWrapを有効にしているときに、RADIUSメッセージに対するキー付きHashed Message Authentication Code（HMAC）の計算に使用されるキーを入力します。
キー入力形式（Key Input Format）	対応するオプションボタンをクリックして次のいずれかの形式を選択し、[キー暗号化キー（Key Encryption Key）]フィールドと[メッセージ認証コードキー（Message Authenticator Code Key）]フィールドに値を入力します。 • [ASCII]：**キー暗号化キー**の長さは16文字（バイト）、**メッセージ オーセンティケータ コード キー**の長さは20文字（バイト）である必要があります。 • [16進数（Hexadecimal）]：キー暗号化キーの長さは32バイト、メッセージ オーセンティケータ コード キーの長さは40バイトである必要があります。 ネットワークデバイスの設定と一致するように、キー暗号キーおよびメッセージ認証コードキーの入力に使用するキー入力形式を指定します。指定する値はキーの正しい（全体の）長さにする必要があります。それよりも短い値は許可されません。
TACACS 認証設定	
共有秘密鍵（Shared Secret）	TACACS+プロトコルが有効のときにネットワークデバイスに割り当てるテキスト文字列を入力します。ユーザーはネットワークデバイスによってユーザー名およびパスワードが認証される前にテキストを入力する必要があることに注意してください。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。
廃止された共有秘密がアクティブです（Retired Shared Secret is Active）	リタイアメント期間がアクティブな場合に表示されます。
廃止（Retire）	既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）]をクリックすると、ダイアログボックスが表示されます。[はい（Yes）]または[いいえ（No）]をクリックします。

フィールド名	使用上のガイドライン
残りの廃止期間（Remaining Retired Period）	（任意）[廃止（Retire）] ダイアログボックスで [はい（Yes）] をクリックした場合にのみ使用できます。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）] > [接続設定（Connection Settings）] > [デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]** ウィンドウで指定されたデフォルト値が表示されます。デフォルト値は変更することができます。 これにより、新しい共有秘密を入力できます。古い共有秘密は、指定された日数の間はアクティブなままになります。
終了（End）	（任意）[残りの廃止期間（Remaining Retired Period）] ダイアログボックスで [はい（Yes）] を選択した場合にのみ使用できます。廃止期間が終了し、古い共有秘密の設定は解除されます。
シングル接続モードを有効にする（Enable Single Connect Mode）	[シングル接続モードを有効にする（Enable Single Connect Mode）] チェックボックスは、ネットワークデバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかのオプションボタンをクリックします。 • [レガシーシスコデバイス（Legacy Cisco Devices）] • [TACACS ドラフト コンプライアンス シングル接続のサポート（TACACS Draft Compliance Single Connect Support）] （注） このフィールドを無効にすると、Cisco ISE はすべての TACACS+ 要求に新しい TCP 接続を使用します。

デバイス セキュリティ設定

RADIUS 共有秘密の最小長を指定します。新規インストールとアップグレードした展開の場合、デフォルトではこの値は 4 文字になります。RADIUS サーバーでのベスト プラクティスは、22 文字にすることです。

（注） [ネットワーク デバイス（Network Devices）] ページに入力した共有秘密の長さは、[デバイス セキュリティ設定（Device Security Settings）] ページの [RADIUS 共有秘密の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定した値以上でなければなりません。

関連トピック

ネットワーク デバイス定義の設定

ネットワーク デバイスのインポート設定

次の表では、ネットワークデバイスの詳細を Cisco ISE にインポートするために使用できる [ネットワークデバイスのインポート（Import Network Devices）] ウィンドウのフィールドにつ

いて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）]**。[ネットワークデバイス（Network Devices）] ウィンドウで、[インポート（Import）] をクリックします。

表 *12 :* ネットワークデバイスのインポート設定

フィールド名	使用上のガイドライン
テンプレートの生成（Generate a Template）	カンマ区切りの値（CSV）テンプレートファイルを作成するには、[テンプレートの生成（Generate a Template）] をクリックします。 CSV形式のネットワークデバイス情報でテンプレートを更新し、ローカルに保存します。次に、編集したテンプレートを使用して、Cisco ISE展開にネットワークデバイスをインポートします。
ファイル（File）	最近作成したか、またはCisco ISE 展開から以前にエクスポートしたCSVファイルを選択するには、**[ファイルの選択（Choose File）]** をクリックします。 [インポート（Import）]オプションを使用して、新規および更新されたネットワークデバイスの情報を含む別のCisco ISE 展開にネットワークデバイスをインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワークデバイスをインポートファイル内のデバイスに置き換えるには、[既存のデータを新しいデータで上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポートファイル内の新しいネットワーク デバイス定義がネットワーク デバイス リポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生したときにCisco ISE にインポートを中止する場合は、[最初のエラー時にインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。Cisco ISE は、エラーが発生するまでネットワークデバイスをインポートします。 このチェックボックスがオンになっておらず、エラーが発生した場合は、エラーが報告され、Cisco ISEは残りのデバイスを引き続きインポートします。

ネットワーク デバイス グループの管理

次のウィンドウを使用すると、ネットワークデバイスグループを設定し、管理することができます。

ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用する [ネットワークデバイスグループ（Network Device Groups）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] > [すべてのグループ（All Groups）]**。

ネットワーク デバイス グループは、**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] > [すべてのグループ（All Groups）]** ウィンドウでも作成できます。

表 *13 : [ネットワーク デバイス グループ（Network Device Group）] ウィンドウのフィールド*

フィールド名	使用上のガイドライン
名前（Name）	ルート ネットワーク デバイス グループの名前を入力します。このルート ネットワークデバイス グループに追加される後続のすべての子ネットワーク デバイス グループに対して、新たに作成したこのネットワーク デバイス グループの名前を入力します。 ネットワーク デバイス グループ階層内には、ルートノードを含めて、最大で 6 つのノードを含めることができます。各ネットワーク デバイス グループの名前には最大で 32 文字を使用できます。
説明（Description）	ルートまたは子のネットワーク デバイス グループの説明を入力します。
ネットワークデバイスの数（No. of Network Devices）	ネットワークグループ内のネットワークデバイスの数がこの列に表示されます。

ネットワーク デバイス グループのインポート設定

次の表では、[ネットワークデバイスグループ（Network Device Group）] ウィンドウの [インポート（Import）] ダイアログボックスのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）]**。

表 *14 : [*ネットワーク デバイス グループのインポート（***Network Device Groups Import***）*]*ウィンドウのフィールド

フィールド名	使用上のガイドライン
テンプレートの生成（Generate a Template）	CSVテンプレートファイルをダウンロードするには、このリンクをクリックします。 同じ形式のネットワーク デバイス グループ情報でテンプレートを更新します。そのテンプレートをローカルに保存し、ネットワーク デバイス グループを Cisco ISE 展開にインポートします。
ファイル（File）	**[ファイルの選択（Choose File）]** をクリックして、アップロードするCSVファイルの場所に移動します。そのファイルは、新規ファイル、または別の Cisco ISE 展開からエクスポートされたファイルである可能性があります。 更新されたネットワーク デバイス グループ情報を使用して、ある Cisco ISE展開から別の展開にネットワークデバイスグループをインポートできます。
新しいデータで既存のデータを上書き（Overwrite existing data with new data）	既存のネットワーク デバイス グループをインポートファイル内のデバイスグループに置き換える場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合、インポートファイル内の新しいネットワーク デバイス グループのみがネットワーク デバイス グループリポジトリに追加されます。重複エントリは無視されます。
最初のエラーでインポートを停止（Stop Import on First Error）	インポート時にエラーが発生した最初のインスタンスでインポートを中止するには、このチェックボックスをオンにします。 このチェックボックスをオンにしていないためにエラーが発生した場合は、Cisco ISE はエラーを報告し、残りのデバイスグループを引き続きインポートします。

ネットワーク デバイス プロファイル設定

次の表は、[ネットワークデバイスプロファイル（Network Device Profiles）] ウィンドウのフィールドについての説明です。このページを使用して、プロトコル、リダイレクトURLおよびCoA設定に対するデバイスのサポートなど、特定のベンダーからのネットワークデバイスのタイプに対するデフォルト設定を構成することができます。その後、プロファイルを使用して特定のネットワーク デバイスを定義します。

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[ネットワークデバイスプロファイル（Network Device Profiles）]** です。

ネットワーク デバイス プロファイルの設定

次の表は、[ネットワーク デバイス プロファイル（Network Device Profile）] セクションのフィールドについての説明です。

表 *15*：ネットワーク デバイス プロファイルの設定

フィールド名	説明
名前（**Name**）	ネットワーク デバイス プロファイルの名前を入力します。
説明（**Description**）	ネットワーク デバイス プロファイルの説明を入力します。
アイコン（**Icon**）	ネットワーク デバイス プロファイルに使用するアイコンを選択します。このアイコンには、選択したベンダーのアイコンがデフォルトで設定されます。 選択するアイコンは 16 X 16 の PNG ファイルである必要があります。
ベンダー（**Vendor**）	ネットワーク デバイス プロファイルのベンダーを選択します。
サポートされるプロトコル	
RADIUS	このネットワーク デバイス プロファイルが RADIUS をサポートしている場合は、このチェックボックスをオンにします。
TACACS+	このネットワーク デバイス プロファイルが TACACS+ をサポートしている場合は、このチェックボックスをオンにします。
TrustSec	このネットワーク デバイス プロファイルが TrustSec をサポートしている場合は、このチェックボックスをオンにします。
RADIUS ディクショナリ（RADIUS Dictionaries）	このプロファイルでサポートされる 1 つ以上の RADIUS ディクショナリを選択します。プロファイルを作成する前に、ベンダー固有の RADIUS ディクショナリをインポートします。

認証/許可テンプレートの設定

次の表は、[認証/許可（Authentication/Authorization）] セクションのフィールドについての説明です。

表 *16 :* 認証/許可の設定

フィールド名	説明
フロータイプの条件（**Flow Type Conditions**）	Cisco ISE では、802.1X、MAC 認証バイパス（MAB）、およびブラウザベースの Web 認証ログインが、有線ネットワークと無線ネットワークの両方を介した基本的なユーザー認証およびアクセスでサポートされます。 このタイプのネットワーク デバイスがサポートする認証ログインのチェックボックスをオンにします。次の 1 つ以上の項目を指定できます。 • 有線 MAC 認証バイパス（MAB）（Wired MAC authentication bypass (MAB)） • 無線 MAB（Wireless MAB） • 有線 802.1x（Wired 802.1X） • 無線 802.1x（Wireless 802.1X） • 有線 Web 認証（Wired Web Authentication） • 無線 Web 認証（Wireless Web Authentication） ネットワーク デバイス プロファイルでサポートされる認証ログインをオンにした後、ログインの条件を指定します。
属性エイリアシング（**Attribute Aliasing**）	ポリシー ルールのフレンドリ名としてデバイスのサービス セット識別子（SSID）を使用する場合は、[SSID] チェックボックスをオンにします。これにより、ポリシールールで使用する一貫した名前を作成できます。
ホスト ルックアップ（**MAB**）	
ホスト ルックアップの処理（**Process Host Lookup**）	ネットワーク デバイス プロファイルで使用されるホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。 さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。デバイスタイプに応じて、使用しているプロトコルの [パスワードを確認（Check Password）] チェックボックス、または [Calling-Station-IdがMACアドレスと等しいかを確認（Checking Calling-Station-Id equals MAC Address）] チェックボックス、あるいはその両方をオンにします。
PAP/ASCII 経由（**Via PAP/ASCII**）	ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。

フィールド名	説明
CHAP 経由（Via CHAP）	ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。 このオプションによって、CHAP 認証が有効になります。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。
EAP-MD5 経由（EAP-MD5）	ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。

権限

このネットワーク デバイス プロファイルに使用される VLAN および ACL の権限を定義できます。プロファイルを保存すると、Cisco ISE は設定された各権限に対し許可プロファイルを自動的に生成します。

表 *17* : 権限

フィールド名	説明
VLAN の設定（Set VLAN）	このネットワーク デバイス プロファイルに VLAN 権限を設定するには、このチェックボックスをオンにします。次のいずれかのオプションを選択します。 • IETF 802.1X 属性（IETF 802.1X Attributes）：Internet Engineering Task Force で定義されたデフォルトの RADIUS 属性のセットです。 • 一意の属性（Unique Attributes）：複数の RADIUS 属性値のペアを指定できます。
ACL の設定（Set ACL）	RADIUS 属性をネットワーク デバイス プロファイルの ACL に設定する場合は、このチェックボックスをオンにします。

許可変更（CoA）テンプレートの設定

このテンプレートは、CoA がこのタイプのネットワーク デバイスにどのように送信されるかを定義します。次の表は、[許可変更（CoA）（Change of Authorization (CoA)）] セクションのフィールドについての説明です。

表 *18 :* 許可変更（*CoA*）の設定

フィールド名	定義
次による CoA（CoA by）	次のオプションのいずれかを選択します。 • RADIUS • SNMP • サポート対象外
RADIUS による CoA（CoA by RADIUS）	
デフォルトの CoA ポート（Default CoA Port）	RADIUS CoA を送信するポート。シスコ デバイスのデフォルト ポートは 1700 で、他のベンダーのデバイスでは 3799 です。 [ネットワークデバイス（Network Device）] ウィンドウでこれを上書きできます。
タイムアウト間隔（Timeout Interval）	CoA の送信後に Cisco ISE が応答を待機する秒数。
再試行回数（Retry Count）	最初のタイムアウト後に Cisco ISE が CoA の送信を試行する回数。
切断（Disconnect）	これらのデバイスに接続解除要求を送信する方法を選択します。 • **[RFC 5176]**：標準のセッション終了の場合はこのチェックボックスをオンにし、RFC 5176 に従って定義されているように、ポートを新しいセッション用に残しておきます。 • **[ポートバウンス（Port Bounce）]**：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。 • **[ポートのシャットダウン（Port Shutdown）]**：セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。
再認証（Re-authenticate）	ネットワーク デバイスに再認証要求を送信する方法を選択します。これは現在、シスコ デバイスのみでサポートされています。 • **[基本（Basic）]**：標準のセッション再認証の場合はこのチェックボックスをオンにします。 • **[再実行（Rerun）]**：認証方式によって最初から実行する場合は、このチェックボックスをオンにします。 • **[最後（Last）]**：最後に成功した認証方式をセッションに使用します。

フィールド名	定義
CoA プッシュ（CoA Push）	ネットワーク デバイスがシスコの TrustSec CoA 機能をサポートしない場合は、このオプションを選択して、Cisco ISE が設定の変更をデバイスにプッシュできるようにします。
SNMP による CoA（CoA by SNMP）	
タイムアウト間隔（Timeout Interval）	CoA の送信後に Cisco ISE が応答を待機する秒数。
再試行回数（Retry Count）	Cisco ISE が CoA の送信を試行する回数。
NAD ポートの検出（NAD Port Detection）	関連する RADIUS 属性は、現時点での唯一のオプションです。
関連する RADIUS 属性	NAD ポートを検出する方法を選択します。 • Nas-Port • Nas-Port-ID
切断（Disconnect）	これらのデバイスに接続解除要求を送信する方法を選択します。 • **[再認証（Reauthenticate）]**：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。 • **[ポートバウンス（Port Bounce）]**：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。 • **[ポートのシャットダウン（Port Shutdown）]**：セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。

リダイレクト テンプレートの設定

ネットワーク デバイスは、許可プロファイルで設定されている場合、クライアントの HTTP 要求をリダイレクトできます。このテンプレートは、このネットワーク デバイス プロファイルが URL リダイレクトをサポートするかどうかを指定します。デバイス タイプに固有の URL パラメータ名を使用します。

次の表は、[リダイレクト（Redirect）] セクションのフィールドについての説明です。

表 *19:* リダイレクトの設定

フィールド名	定義
タイプ（Type）	ネットワーク デバイス プロファイルが静的または動的 URL リダイレクトをサポートするかを選択します。 デバイスがどちらもサポートしていない場合、[未サポート（Not Supported）] を選択し、**[設定（Settings）] > [DHCPおよびDNSサービス（DHCP & DNS Services）]** から VLAN を設定します。
リダイレクト URL パラメータ名	
クライアントIPアドレス（Client IP Address）	ネットワーク デバイスがクライアントの IP アドレスに使用するパラメータ名を入力します。
クライアントMACアドレス（Client MAC Address）	ネットワーク デバイスがクライアントの MAC アドレスに使用するパラメータ名を入力します。
元の URL（Originating URL）	ネットワーク デバイスが元のURLに使用するパラメータ名を入力します。
セッションID（Session ID）	ネットワーク デバイスがセッション ID に使用するパラメータ名を入力します。
SSID	ネットワーク デバイスがサービス セット識別子（SSID）に使用するパラメータ名を入力します。
ダイナミック URL パラメータ	
パラメータ（Parameter）	動的 URL リダイレクトを選択する場合は、これらのネットワーク デバイスがリダイレクトURLを作成する方法を指定する必要があります。また、リダイレクト URL がセッション ID またはクライアントの MAC アドレスを使用するかを指定できます。

詳細設定（Advanced Settings）

ネットワーク デバイス プロファイルを使用して、ネットワーク デバイスをポリシー ルールで使いやすくするために、多数のポリシー要素を生成できます。これらの要素には、複合条件、許可プロファイル、および許可されているプロトコルが含まれています。

これらの要素を作成するには、[ポリシー要素の作成（Generate Policy Elements）] をクリックします。

外部 RADIUS サーバーの設定

次の表では、[外部 RADIUS サーバー（External RADIUS Server）] ウィンドウのフィールドについて説明します。これらのフィールドを使用して、RADIUS サーバーを設定できます。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [外部 RADIUS サーバー（External RADIUS Servers）]**。

表 *20 :* 外部 *RADIUS* サーバーの設定

フィールド名	使用上のガイドライン
名前（**Name**）	外部 RADIUS サーバーの名前を入力します。
説明（**Description**）	外部 RADIUS サーバーの説明を入力します。
ホスト名/アドレス（**Host IP**）	外部 RADIUS サーバーの IP アドレスを入力します。IPv4 アドレスを入力する場合は、範囲とサブネット マスクを使用できます。IPv6 では、範囲がサポートされていません。
共有秘密鍵（**Shared Secret**）	外部 RADIUS サーバーの認証に使用される、Cisco ISE と外部 RADIUS サーバーの間の共有秘密を入力します。共有秘密情報は、予期されるテキスト文字列です。ユーザーは、ネットワーク デバイスによってユーザー名およびパスワードが認証されるようにこれらの情報を提示する必要があります。ユーザーが共有秘密情報を提示するまで、接続は拒否されます。共有秘密情報の長さは、最大 128 文字です。
KeyWrap の有効化（**Enable KeyWrap**）	このオプションを有効にすると、AES KeyWrap アルゴリズムにより RADIUS プロトコルのセキュリティが強化され、Cisco ISE で FIPS 140 に準拠可能になります。
キー暗号キー（**Key Encryption Key**）	（[keyWrap を有効にする（Enable keyWrap）] チェックボックスをオンにした場合のみ）セッション暗号化（秘密）に使用される暗号キーを入力します。
メッセージ オーセンティケータ コード キー（**Message Authenticator Code Key**）	（[keyWrap を有効にする（Enable keyWrap）] チェックボックスをオンにした場合のみ）RADIUS メッセージ上のキー付き HMAC 計算に使用されるキーを入力します。

フィールド名	使用上のガイドライン
キー入力形式（Key Input Format）	Cisco ISE 暗号キーの入力に使用する形式を指定します。これは、WLAN コントローラ上の設定と一致する必要があります。指定する値の長さは、次に定義されているキーの（最大の）長さと正確に一致している必要があります。これより短い値は許可されません。 • [ASCII]：キー暗号キーの長さは 16 文字（バイト）、メッセージ オーセンティケータ コード キーの長さは 20 文字（バイト）である必要があります。 • [16 進数（Hexadecimal）]：キー暗号キーの長さは 32 バイトであり、メッセージ オーセンティケータ コード キーの長さは 40 バイトである必要があります。
認証ポート（Authentication Port）	RADIUS 認証のポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1812 です。
アカウンティング ポート（Accounting Port）	RADIUS アカウンティングのポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1813 です。
サーバー タイムアウト（Server timeout）	Cisco ISE が外部 RADIUS サーバーからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は 5 ～ 120 です。
接続試行回数（Connection Attempts）	Cisco ISE が外部 RADIUS サーバーへの接続を試行する回数を入力します。デフォルトは 3 回に設定されています。有効な値は 1 ～ 9 です。
RADIUS プロキシ フェールオーバーの有効期限（RADIUS Proxy Failover Expiration）	接続に失敗してから、このサーバーに再び接続を試みるまでの経過時間を入力します。有効な範囲は 1 ～ 600 です。 サーバータイムアウトをスキップし、フェールオーバーに直接移動するには、このパラメータを設定します。

RADIUS サーバー順序

次の表では、RADIUS サーバー順序を作成するために使用する [RADIUS サーバー順序（RADIUS Server Sequences）] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[ネットワークリソース（Network Resources）]** > **[RADIUSサーバー順序（RADIUS Server Sequences）]** > [追加（Add）]。

表 *21 : RADIUS* サーバー順序

フィールド名	使用上のガイドライン
名前（**Name**）	RADIUS サーバー順序の名前を入力します。
説明（**Description**）	任意で説明を入力します。
ホスト名/アドレス（**Host IP**）	外部 RADIUS サーバーの IP アドレスを入力します。
ユーザーが選択したサービス タイプ（**User Selected Service Type**）	[使用可能（Available）] リスト ボックスで、ポリシー サーバーとして使用する外部 RADIUS サーバーを選択し、選択した外部 RADIUS サーバーを [選択済み（Selected）] リスト ボックスに移動します。
リモート アカウンティング（**Remote Accounting**）	リモート ポリシー サーバーでアカウンティングを有効にするには、このチェックボックスをオンにします。
ローカル アカウンティング（**Local Accounting**）	Cisco ISE でのアカウンティングを有効にするには、このチェックボックスをオンにします。
高度な属性設定（**Advanced Attributes Settings**）	
サブジェクト名の先頭から最後に出現する区切り文字まで削除（**Strip Start of Subject Name up to the First Occurrence of the Separator**）	プレフィクスからユーザー名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が acme\userA、区切り文字が \ の場合、ユーザー名は userA になります。

フィールド名	使用上のガイドライン
最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip End of Subject Name from the Last Occurrence of the Separator）	サフィックスからユーザー名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が userA@abc.com、区切り文字が @ の場合、ユーザー名は userA になります。 • NetBIOS または User Principle Name（UPN）フォーマットのユーザー名（user@domain.com または /domain/user）からユーザー名を抽出するには、これらのストリップオプションを有効にする必要があります。RADIUS サーバーでユーザーを認証するために、ユーザー名だけが RADIUS サーバーに渡されるためです。 • \ および @ の両方のストリップ機能をアクティブ化し、エージェントを使用している場合、Cisco ISE は最初に出現する \ を文字列から正確に取り除くことができません。ただし、各ストリップ機能は、エージェントを考慮して設計されているため、個別に使用する場合は動作します。
外部 RADIUS サーバーへの要求に含まれる属性を変更する（Modify Attributes in the Request to the External RADIUS Server）	認証済みの RADIUS サーバーとの間で送受信する属性の操作を Cisco ISE に許可するには、このチェックボックスをオンにします。 次の属性操作が可能です。 • [追加（Add）]：RADIUS 要求/応答全体に属性を追加します。 • [更新（Update）]：属性値（固定または静的）を変更します。または属性を別の属性値（動的）で置き換えます。 • [削除（Remove）]：属性または属性と値のペアを削除します。 • [すべて削除（RemoveAny）]：存在するすべての属性を削除します。
認証ポリシーに進む（Continue to Authorization Policy）	ID ストア グループおよび属性の取得に基づいて、プロキシ フローを許可ポリシーの実行に誘導して、より詳細な意思決定を行うには、このチェックボックスをオンにします。このオプションを有効にすると、外部RADIUS サーバーからの応答に含まれる属性が、認証ポリシーの選択に使用されます。このコンテキストの既存の属性は、AAA サーバーの受け入れ応答属性の適切な値で更新されます。
Access-Accept の送信前に属性を変更する（Modify Attributes before send an Access-Accept）	応答をデバイスに返送する直前に属性を変更するには、このチェックボックスをオンにします。

デバイス ポータルの管理

デバイス ポータルの設定

デバイス ポータルのポータル ID 設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータルの管理（Device Portal Managment）] > [ブロックリストポータル（Blocked List Portal）]/[クライアントプロビジョニングポータル（Client Provisioning Portals）]/[BYOD ポータル（BYOD Portals）]/[MDM ポータル（MDM Portals）]/[デバイスポータル（My Device Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの設定およびカスタマイズ（Portals Settings and Customization）]** です。

- [ポータル名（Portal Name）]：このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル（[ブロック済みリスト（Blocked List）]、[個人所有デバイス持ち込み（BYOD）（Bring Your Own Device (BYOD)）]、[クライアント プロビジョニング（Client Provisioning）]、[モバイルデバイス管理（MDM）（Mobile Device Management (MDM)）]、または [デバイス（My Devices）] の各ポータル）に使用しないでください。

  この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- [説明（Description）]：オプションです。

- [ポータルテスト URL（Portal test URL）]：[保存（Save）] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

  リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

（注） テストポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアントプロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

- [言語ファイル（Language File）]：各ポータルタイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

  言語ファイルには、特定のブラウザロケール設定へのマッピングと、その言語でのポータル全体のすべての文字列設定が含まれています。1つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

  1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザー Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイスポータルにも適用されます。

  [ポータルページのカスタマイズ（Portal Page Customizations）] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に1つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

BYOD と MDM ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [BYOD ポータルまたは MDM ポータル（BYOD Portals or MDM Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]**。

これらを設定して、ポータル ページの動作を定義します。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで8443です。ただし、ブロックリストポータルは8444です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート8905および8909も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

  同じHTTPSポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートと

インターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。

- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- NIC チーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループタグ（Certificate Group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループタグを選択します。
- [エンドポイント ID グループ（Endpoint Identity Group）]：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

- **表示言語**
  - [ブラウザのロケールを使用する（Use Browser Locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語（Fallback Language）] が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback Language）]：ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。

- [常に使用（Always Use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する（User Browser Locale）] オプションを上書きします。

BYOD ポータルの BYOD 設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [BYOD ポータル（BYOD Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [BYOD 設定（BYOD Settings）]**。

この設定を使用して、パーソナル デバイスを使用する従業員の個人所有デバイスの持ち込み（BYOD）機能を有効にし、企業ネットワークにアクセスできるようにします。

フィールド名	使用上のガイドライン
AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）	会社のネットワーク使用の諸条件を、現在ユーザーに表示されているウィンドウ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
同意が必要（Require Acceptance）	ユーザーのアカウントが完全に有効になる前に、ユーザーは AUP に同意する必要があります。[ログイン（Login）] ボタンは、ユーザーが AUP を受け入れない場合は有効になりません。ユーザーが AUP に同意しない場合、ネットワークにアクセスできません。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	このオプションは、[AUP をページに含める（Include an AUP on page）] が有効である場合のみ表示されます。 ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールすると有効になります。
登録時にデバイス ID フィールドを表示する（Display Device ID Field During Registration）	登録プロセス中に、デバイス ID をユーザーに表示します。これは、デバイス ID が事前設定されており、BYOD ポータルを使用しているときに変更できない場合も含みます。

フィールド名	使用上のガイドライン
元の URL（Originating URL）	ネットワークへの認証に成功すると、可能な場合はユーザーのブラウザを、ユーザーがアクセスしようとしていた元の Web サイトにリダイレクトします。使用できない場合は、[認証成功（Authentication Success）] ウィンドウが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の Cisco ISE で設定された認証プロファイルにより、PSN のポート 8443 で動作することを確認します。 Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザード アプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS（dot1X）およびサポート対象外のデバイス（ネットワーク アクセスが許可されている）では、この URL にリダイレクトされます。
成功ページ（Success page）	デバイスの登録が成功したことを示すページを表示します。
URL	ネットワークへの認証に成功すると、ユーザーのブラウザを指定された URL（会社の Web サイトなど）にリダイレクトします。

（注） 認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。

証明書プロビジョニング ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[証明書プロビジョニング ポータル（Certificate Provisioning Portal）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ポータル設定（Portal Settings）]**。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで 8443 です。ただし、ブロックリストポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。こ

れは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。

- ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- NIC チーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループタグ（Certificate Group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループタグを選択します。
- **[認証方式（AuthenticationMethod）]**：ユーザー認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ID ソース順序は、ユーザークレデンシャルを確認するために順番に検索される ID ストアのリストです。

  Cisco ISE には、スポンサーポータル Sponsor_Portal_Sequence 用のデフォルトの ID ソース順序が含まれています。

  IdP を設定するには、**[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

  ID ソース順序を設定するには、[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] を選択します。
- [承認済みグループの設定（Configure Authorized Groups）]：証明書を生成してそれを [選択済み（Chosen）] ボックスに移動するための権限を付与するユーザー ID グループを選択します。
- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：[スポンサー（Sponsor）] ポータルまたは [デバイス（MyDevices）] ポータルの固有の FQDN またはホスト名を 1 つの以上入力します。たとえば、

sponsorportal.yourcompany.com,sponsor と入力することで、ユーザーはブラウザにこれらのいずれかを入力すると、が表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

デフォルトの FQDN を変更する場合は、次を実行します。

- DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
- 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカルサーバー証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。[Kerberos SSO を許可（Allow Kerberos SSO）] オプションがスポンサーポータルで有効になっている場合は、ポータルで使用されるローカルサーバー証明書の SAN 属性に Cisco ISE PSN の FQDN またはワイルドカードを含める必要があります。

- [アイドルタイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザーをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

ログイン ページの設定（Login Page Settings）

- [レート制限までの最大ログイン試行失敗数（Maximum Failed Login Attempts Before Rate Limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [AUP を含める（Include an AUP）]：フローにアクセプタブル ユース ポリシー ウィンドウを追加します。AUP をウィンドウに追加したり、別のウィンドウへのリンクを設定することができます。

利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP ページを含める（Include an AUP Page）]：会社のネットワーク使用諸条件を、別のページでユーザーに表示します。
- [従業員に別の AUP を使用する（Use Different AUP for Employees）]：従業員専用に別の AUP およびネットワーク使用諸条件を表示します。このオプションを選択すると、[従業員用の AUP をスキップ（Skip AUP for employees）] は選択できません。
- [従業員用の AUP をスキップ（Skip AUP for Employees）]：従業員は、ネットワークにアクセスする前に AUP に同意する必要はありません。このオプションを選択すると、[従業員に別の AUP を使用する（Use different AUP for employees）] は選択できません。
- [同意が必要（Require Acceptance）]：ユーザーのアカウントが完全に有効になる前に、ユーザーは AUP に同意する必要があります。[ログイン（Login）] ボタンは、ユーザーが AUP

を受け入れない場合は有効になりません。ユーザーがAUPに同意しない場合、ネットワークにアクセスできません。

- [AUP の最後までのスクロールが必要（Require Scrolling to End of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。

  ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。AUP がユーザーに表示された場合に設定します。

  - [初回のログインのみ（On First Login only）]：ユーザーが初めてネットワークまたはポータルにログインしたときに AUP を表示します。
  - [ログインごと（On Every Login）]：ユーザーがネットワークまたはポータルにログインするごとに、AUP を表示します。
  - [__ 日ごと（初回のログインから）（Every __ Days (starting at first login)）]：ネットワークやポータルにユーザーが初めてログインした後は、AUP を定期的に表示します。

クライアント プロビジョニング ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）]** > **[デバイスポータル管理（Device Portal Management）]** > **[クライアントプロビジョニングポータル（Client Provisioning Portals）]** > **[作成、編集、複製または削除（Create, Edit, Duplicate, or Delete）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** です。

ポータル設定

- **[HTTPS ポート（HTTPS Port）]**：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで 8443 です。ただし、**[ブロックリスト（Blocked List）]** ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合、この制限に従うようにポート設定を変更する必要があります。
- **[使用可能インターフェイス（Allowed interfaces）]**：ポータルを実行できる PSN インターフェイスを選択します。PSN で使用可能なインターフェイスを備えた PSN のみがポータルを作成できます。物理およびボンディングされたインターフェイスの任意の組み合わせを設定できます。これはPSN全体の設定です。すべてのポータルはこれらのインターフェイスでのみ動作し、このインターフェイス設定はすべての PSN に適用されます。
  - 異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときのVMベースのものを含む、すべてのPSNで使用できるものでなければなりません。こ

れは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。

- ポータルの証明書のサブジェクト名とサブジェクトの代替名は、インターフェイス IP に解決される必要があります。
- ISE CLI の ip host x.x.x.x yyy.domain.com をセカンダリ インターフェイス IP と FQDN をマッピングするように設定します。これは証明書のサブジェクト名/サブジェクトの代替名を一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合は、PSN はポータルの設定時に、最初にボンディング インターフェイスの設定を試みます。これが成功しない場合、その PSN にボンドセットがなかったことが原因である可能性があるので、PSN はエラーを記録して終了します。物理インターフェイスでポータルを開始しようとはしません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- **[証明書グループタグ（Certificate group tag）]**：ポータルの HTTPS トラフィックに使用する証明書グループのグループタグを選択します。
- **[認証方式（Authentication Method）]**：ユーザー認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザー クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザー、内部ユーザー、Active Directory、LDAP などがあります。

  Cisco ISE には、クライアント プロビジョニング ポータル用のデフォルトのクライアント プロビジョニング ID ソース順序 Certificate_Portal_Sequence が含まれています。
- **[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]**：クライアント プロビジョニング ポータル用に少なくとも 1 つの一意の FQDN、ホスト名、またはその両方を入力します。たとえば、「provisionportal.yourcompany.com」と入力した場合、ユーザーはこれらのいずれかをブラウザに入力して証明書プロビジョニング ポータルに到達できます。
  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに確実に解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。

- 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバー証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

（注） URL リダイレクトなしのクライアント プロビジョニングの場合、[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）] フィールドに入力するポータル名は、DNS 設定で設定されている必要があります。URL リダイレクトなしのクライアント プロビジョニングを有効にするため、この URL をユーザーに通知する必要があります。

- **[アイドルタイムアウト（Idle timeout）]**：ポータルでアクティビティがない場合にユーザーをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

（注） クライアント プロビジョニング ポータルではポート番号と証明書を定義できます。これにより、ホストはクライアント プロビジョニングとポスチャに同じ証明書をダウンロードすることを許可します。ポータル証明書が正式な認証局により署名されている場合、セキュリティ警告は表示されません。自己署名証明書の場合、ポータルと Cisco エージェント ポスチャ コンポーネントの両方でセキュリティ警告を受け取ります。

ログイン ページの設定（Login Page Settings）

- [ログインの有効化（Enable Login）]：クライアント プロビジョニング ポータルのログイン手順を有効にするには、このチェックボックスを選択します
- [レート制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：単一のブラウザセッションからのログイン試行失敗回数を指定します。この回数を超過すると、Cisco ISE はログイン試行を実行できる頻度を意図的に低下させて、追加のログイン試行を防ぎます。ログイン失敗がこの回数に達した後のログイン試行の間隔は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で指定されます。
- [頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）]：[レート制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザーが再度ログインを試行するまでに待機する必要がある時間を分単位で設定します。
- [AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）]：会社のネットワーク使用の契約条件を、現在ユーザーに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。

- [同意が必要（Require acceptance）]：ポータルにアクセスする前にユーザーが AUP を受け入れることを要求します。[ログイン（Login）] ボタンは、ユーザーが AUP を受け入れない場合は有効になりません。AUP を受け入れないユーザーは、ポータルにアクセスできません。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。

利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP を含める（Include an AUP）]：会社のネットワーク使用の契約条件を、別のページでユーザーに表示します。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：ユーザーが AUP を完全に読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールするとアクティブになります。
- [初回のログインのみ（On first login only）]：ユーザーがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
- [ログインごと（On every login）]：ユーザーがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [_ 日ごと（初回のログインから）（Every _____ days (starting at first login)）]：ネットワークやポータルにユーザーが初めてログインした後は、AUP を定期的に表示します。

ポストログイン バナー ページ設定（Post-Login Banner Page Settings）

[ポストログインバナーページを含める（Include a Post-Login Banner page）]：ユーザーが正常にログインした後、ネットワークアクセスを付与される前に追加情報を表示します。

パスワード変更設定（Change Password Settings）

[内部ユーザーに自身のパスワードの変更を許可する（Allow internal users to change their own passwords）]：従業員がクライアントプロビジョニング ポータルにログインして、自分のパスワードを変更できるようにします。これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

MDM ポータルの従業員のモバイル デバイス管理設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [MDM ポータル（MDM Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] > [従業員のモバイル デバイス管理設定（Employee Mobile Device Management Settings）]**。

これらの設定を使用して、MDMポータルを使用する従業員のモバイルデバイス管理（MDM）機能を有効にし、AUP エクスペリエンスを定義します。

フィールド名	使用上のガイドライン
AUPをページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）	会社のネットワーク使用の諸条件を、現在ユーザーに表示されているウィンドウ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
同意が必要（Require Acceptance）	ユーザーのアカウントが完全に有効になる前に、ユーザーは AUP に同意する必要があります。[ログイン（Login）] ボタンは、ユーザーが AUP を受け入れない場合は有効になりません。ユーザーが AUP に同意しない場合、ネットワークにアクセスできません。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	このオプションは、[AUP をページに含める（Include an AUP on page）] が有効である場合のみ表示されます。 ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールすると有効になります。

デバイス ポータルのポータル設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作とフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]**。

- [HTTPS ポート（HTTPS Port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルトポータルで8443です。ただし、ブロックリストポータルは8444です。この範囲外のポート値を使用してアップグレードした場合は、このウィンドウで変更を加えるまで維持されます。このウィンドウを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲストポータルに非ゲストポータル（[デバイス（My Devices）] など）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート8905および8909も使用します。それ以外の場合は、ゲストポータルへの割り当てと同じポートを使用します。

  同じHTTPSポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。

- スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
- スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
- スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**

- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブロック済みリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストサービスにインターフェイス 0 を使用することを推奨します。[ポータル設定（Portal Settings）] ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed Interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名またはサブジェクトの代替名はインターフェイス IP アドレスに解決する必要があります。

- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリインターフェイスの IP アドレスを FQDN にマッピングします。これは、証明書のサブジェクト名、またはサブジェクトの代替名と一致させるために使用されます。
- ボンディングされたNICのみが選択されている場合は、PSNはポータルの設定時に、最初にボンディングインターフェイスの設定を試みます。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- NICチーミングまたはボンディングは、ハイアベイラビリティ（耐障害性）を実現するために 2 つの個別の NIC を設定できる 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方のNICは、接続を続行します。1 つの NIC が [ポータル設定（Portal Settings）] に基づいてポータルに選択されます。物理 NIC と対応するボンディングされた NIC の両方が設定されている場合は、PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSNは物理インターフェイスでポータルを開始しようとします。

- [証明書グループタグ（Certificate Group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループタグを選択します。
- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：[スポンサー（Sponsor）] ポータルまたは [デバイス（MyDevices）] ポータルの固有の FQDN またはホスト名を 1 つの以上入力します。たとえば、**sponsorportal.yourcompany.com,sponsor** と入力することで、ユーザーはブラウザにこれらのいずれかを入力すると、が表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

  デフォルトの FQDN を変更する場合は、次を実行します。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバー証明書のサブジェクト代替名（SAN）属性に、カスタマイズされたURLの FQDN またはワイルドカードを含めます。[Kerberos SSO を許可（Allow Kerberos SSO）] オプションがスポンサーポータルで有効になっている場合は、ポータルで使用されるローカルサーバー証明書の SAN 属性に Cisco ISE PSN の FQDN またはワイルドカードを含める必要があります。

- **[認証方式（AuthenticationMethod）]**：ユーザー認証に使用する ID ソース順序（ISS）またはIDプロバイダー（IdP）を選択します。ID ソース順序は、ユーザーク レデンシャルを確認するために順番に検索される ID ストアのリストです。

  Cisco ISE には、スポンサーポータル Sponsor_Portal_Sequence 用のデフォルトの ID ソース順序が含まれています。

IdP を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

ID ソース順序を設定するには、[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] を選択します。

- [エンドポイント ID グループ（Endpoint Identity Group）]：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

- [__日に達した場合にこの ID グループ内のエンドポイントを消去する（Purge Endpoints in this Identity Group when they Reach __ Days）]：Cisco ISE データベースからデバイスが消去されるまでの日数を指定します。消去は毎日実行され、消去アクティビティは全体的な消去タイミングと同期されます。変更は、このエンドポイント ID グループ全体に適用されます。

  その他のポリシー条件に基づいてエンドポイント消去ポリシーに変更が加えられた場合、この設定は使用できなくなります。

- [アイドルタイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザーをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

- **表示言語**

  - [ブラウザのロケールを使用する（Use Browser Locale）]：クライアントブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザのロケールの言語が Cisco ISE でサポートされていない場合は、[フォールバック言語（Fallback Language）] が言語ポータルとして使用されます。

  - [フォールバック言語（Fallback Language）]：ブラウザロケールから言語を取得できない場合、またはブラウザロケール言語が Cisco ISE でサポートされていない場合に使用する言語を選択します。

  - [常に使用（Always Use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザーの [ブラウザのロケールを使用する（User Browser Locale）] オプションを上書きします。

デバイス ポータルのログイン ページ設定

- [レート制限までの最大ログイン試行失敗数（Maximum Failed Login Attempts Before Rate Limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッ

ションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。

- [レート制限までの最大ログイン試行失敗数（Maximum Failed Login Attempts Before Rate Limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザセッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [AUP を含める（Include an AUP）]：フローにアクセプタブル ユース ポリシー ウィンドウを追加します。AUPをウィンドウに追加したり、別のウィンドウへのリンクを設定することができます。

デバイス ポータルの利用規定ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [アクセプタブルユースポリシー（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]** です。

これらの設定を使用して、ユーザー（状況に応じてゲスト、スポンサーまたは従業員）に対して AUP エクスペリエンスを定義します。

フィールド	使用上のガイドライン
AUP ページを含める（Include AUP Page）	会社のネットワーク使用諸条件を、別のページでユーザーに表示します。
AUP の最後までのスクロールが必要（Require scrolling to end of AUP）	ユーザーが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザーが AUP の最後までスクロールすると有効になります。
初回ログイン時のみ（On First Login only）	ユーザーがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
ログインごと（On Every Login）	ユーザーがネットワークまたはポータルにログインするごとに、AUP を表示します。

フィールド	使用上のガイドライン
__日ごと（初回のログインから）（Every __ Days (starting at first login)）	ユーザーがネットワークまたはポータルに初めてログインした後に、定期的に AUP を表示します。

デバイス ポータルのポストログイン バナー ページ設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポストログイン バナー ページ設定（Post-Login Banner Page Settings）]**。

これらの設定を使用して、正常なログイン後にユーザー（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

フィールド名	使用上のガイドライン
ポストログインバナーページを含める（Include a Post-Login Banner page）	ユーザーが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

デバイス ポータルの従業員によるパスワード変更の設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [従業員のパスワード変更設定（Employee Change Password Settings）]**。これらの設定を使用して、デバイス ポータルを使用している従業員のパスワード要件を定義します。

従業員のパスワードポリシーを設定するには、**[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザー名パスワード ポリシー（Username Password Policy）]** を選択します。

フィールド名	使用上のガイドライン
内部ユーザーにパスワードの変更を許可する（Allow internal users to change password）	従業員が、デバイス ポータルにログインした後で、自分のパスワードを変更することを許可します。 これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

デバイス ポータルのデバイス管理設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [マイデバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [デバイスの管理（Manage Device）]**。

[ページのカスタマイズ（Page Customizations）] で、マイデバイスポータルの [アカウントの管理（Manage Accounts）] タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

[設定（Settings）] では、このポータルを使用する従業員が各自の登録されたパーソナルデバイスで実行可能なアクションを指定できます。

表 *22*：デバイス ポータルのデバイス管理設定

フィールド名	使用上のガイドライン
紛失（Lost）	デバイスを紛失したことを従業員が示すことができるようにします。このアクションは、マイデバイスポータルのデバイスのステータスを [紛失（Lost）] に更新し、ブロック済みリストのエンドポイントの ID グループにそのデバイスを追加します。
復元（Reinstate）	このアクションでは、ブロックリストに記載されているか、紛失したか、または盗難されたデバイスを復元し、そのステータスを最後の既知の値にリセットします。このアクションでは、ネットワークに接続する前に追加プロビジョニングを実行する必要があるため、盗難デバイスのステータスを [未登録（Not Registered）] にリセットします。 ブロックリストに記載されているデバイスを従業員が復元できないようにする場合は、デバイスポータルでこのオプションを有効にしないでください。
削除（Delete）	登録済みデバイスの最大数に到達した場合、従業員が、登録されたデバイスをデバイスポータルから削除したり、未使用のデバイスを削除して新しいデバイスを追加したりできるようにします。このアクションによって、デバイス ポータルに表示されるデバイス リストからデバイスが削除されますが、デバイスは Cisco ISE データベースに残り、エンドポイントのリストに表示されます。 BYOD またはマイデバイスポータルを使用して従業員が登録できるパーソナルデバイスの最大数を定義するには、**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員登録済みデバイス（Employee Registered Devices）]** を選択します。 Cisco ISE データベースからデバイスを完全に削除するには、**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

フィールド名	使用上のガイドライン
盗難（**Stolen**）	デバイスが盗まれたことを従業員が示すことができるようにします。このアクションは、マイデバイスポータルのデバイスのステータスを [盗難（Stolen）] に更新し、ブロック済みリストのエンドポイントの ID グループにそのデバイスを追加し、証明書を削除します。
デバイスロック（**Device lock**）	MDM 登録デバイスのみ。 デバイスの紛失または盗難が発生した場合、従業員がすぐにデバイス ポータルからリモートでデバイスをロックできるようにします。このアクションによって、デバイスの不正使用が防止されます。 ただし、デバイス ポータルでは PIN を設定できないため、従業員が事前にモバイル デバイスに設定しておく必要があります。
登録解除（**Unenroll**）	MDM 登録デバイスのみ。 職場でデバイスを使用する必要がなくなった場合に、従業員がこのオプションを選択できるようにします。このアクションでは、会社がインストールしているアプリケーションと設定のみが削除され、従業員のモバイル デバイス上の他のアプリケーションおよびデータは維持されます。
完全消去（**Full wipe**）	MDM 登録デバイスのみ。 デバイスを紛失したり、新しいものに交換したりした場合に、従業員がこのオプションを選択できるようにします。このアクションでは、従業員のモバイル デバイスを工場出荷時のデフォルト設定にリセットし、インストール済みのアプリケーションとデータを削除します。

デバイス ポータルのデバイス カスタマイズの追加、編集、および検索

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルページのカスタマイズ（Portal Page Customization）] > [デバイスの追加、デバイスの編集またはデバイスの検索（Add Devices, Edit Devices or Locate Devices）]** です。

[ページのカスタマイズ（Page Customizations）] で、デバイス ポータルの [追加（Add）]、[編集（Edit）]、および [検索（Locate）] の各タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

デバイス ポータルのサポート情報ページの設定

このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [BYOD ポータル（BYOD Portals）]/[クライアントプロビジョニングポータル（Client Provisioning Portals）]/[MDM ポータル（MDM Portals）]/[デバイスポータル（My Device Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフ**

ローの設定（Portal Behavior and Flow Settings）] > [サポート情報ページの設定（Support Information Page Settings）] です。

これらの設定を使用して、ヘルプデスクがユーザー（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

フィールド名	使用上のガイドライン
サポート情報ページを含める（Include a Support Information Page）	該当ポータルのすべての有効なページ上で、[問い合わせ先（Contact Us）] などの情報へのリンクを表示します。
MAC アドレス（MAC Address）	[サポート情報（Support Information）] ウィンドウにデバイスの MAC アドレスを含めます。
IP アドレス（IP Address）	[サポート情報（Support Information）] ウィンドウにデバイスの IP アドレスを含めます。
ブラウザのユーザーエージェント（Browser User Agent）	[サポート情報（Support Information）] ページに、要求の発信元の製品名とバージョン、レイアウトエンジン、ユーザーエージェントのバージョンなど、ブラウザの詳細を含めます。
ポリシーサーバー（Policy Server）	[サポート情報（Support Information）] ウィンドウに、このポータルを提供している ISE ポリシーサービスノード（PSN）の IP アドレスを含めます。
障害コード（Failure code）	可能な場合は、ログ メッセージ カタログ内の対応する番号を含めます。メッセージカタログを表示するには、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージカタログ（Message Catalog）]** を選択します。
フィールドを非表示にする（Hide Field）	含める情報が存在しない場合、[サポート情報（Support Information）] ウィンドウ上の該当するフィールドのラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード（Failure Code）] は、選択されている場合でも表示されません。
値のないラベルを表示（Display label with no value）	含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを [サポート情報（Support Information）] ウィンドウに表示します。たとえば、障害コードが不明な場合、[障害コード（Failure Code）] は空白であっても表示されます。

フィールド名	使用上のガイドライン
デフォルト値でラベルを表示（Display Label with Default Value）	含める情報が存在しない場合、[サポート情報（Support Information）] ウィンドウ上の選択されているすべてのフィールドにこのテキストが表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード（Failure code）] に [使用できません（Not Available）] と表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。