セグメンテーション

ポリシー セット

Cisco ISE はポリシーベースのネットワークアクセス制御ソリューションで、ネットワーク アクセスポリシーセットを提供し、ワイヤレス、有線、ゲスト、およびクライアントプロビジョニングなど、さまざまなネットワーク アクセスの使用例を管理できます。ポリシー セット（ネットワーク アクセスとデバイス管理の両方のセット）を使用すると、認証および許可ポリシーを論理的に同じセットにグループ化することができます。ロケーション、アクセスタイプ、類似パラメータに基づくポリシーセットなどの領域に基づいて、複数のポリシーセットを作成できます。Cisco ISE をインストールすると、デフォルトのポリシーセットであるポリシーセットが常に 1 つ定義され、デフォルトのポリシーセットには、事前定義されたデフォルトの認証、許可、および例外のポリシー規則が含まれています。

ポリシーセットを作成するときは、ネットワーク アクセス サービスはポリシーセット レベルで、ID ソースは認証ポリシー レベルで、ネットワーク許可は許可ポリシー レベルで選択するように、（条件および結果で設定された）これらのルールを設定できます。さまざまなベンダーに対し、Cisco ISE 対応ディクショナリからの属性のいずれかを使用して、1 つまたは複数の条件を定義できます。Cisco ISE では、再利用可能な個別のポリシー要素として条件を作成できます。

ネットワーク デバイスと通信するためにポリシー セットごとに使用されるネットワーク アクセス サービスは、そのポリシー セットの最上位レベルで定義されます。ネットワーク アクセス サービスには次のものがあります。

- 許可されたプロトコル：初期要求とプロトコルネゴシエーションを処理するように設定されたプロトコル
- プロキシサービス：処理のために外部 RADIUS サーバーに要求を送信します

（注） **[ワークセンター（Work Centers）]>[デバイス管理（Device Administration）]**から、ポリシーセットに関連する TACACS サーバー順序を選択することもできます。TACACS サーバー順序を使用して、一連の TACACS プロキシ サーバーを処理用に設定します。

[ポリシーセット（Policy Set）]テーブルから確認できるポリシーセットの最上位レベルのルールが、セット全体に適用され、残りのポリシーと例外のルールの前に一致している場合、ポリシーセットは階層的に構成されています。その後、セットのルールが次の順序で適用されます。

1. 認証ポリシー ルール
2. ローカル ポリシー例外
3. グローバル ポリシー例外
4. 許可ポリシー ルール

（注） ポリシーセットの機能は、ネットワークアクセスとデバイス管理ポリシーの場合と同じです。この章で説明するすべてのプロセスは、[ネットワークアクセス（Network Access）]および[デバイス管理（Device Administration）] ワークセンターの両方で作業する場合に適用できます。この章では、[ネットワーク アクセス（Network Access）] ワーク センターのポリシーセットについて具体的に説明します。**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）]** を選択します。

ISE コミュニティ リソース

WLC からの RADIUS 結果の使用については、「WLC Called-Station-ID（RADIUS 認証とアカウンティングの設定）（WLC Called-Station-ID (Radius Authentication and Accounting Config)）」を参照してください。

ポリシー セットの構成時の設定

次の表では、[ポリシーセット（Policy Sets）] ウィンドウのフィールドについて説明します。このフィールドから、認証、例外、および許可ポリシーを含むポリシーセットを設定できます。ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）]** を選択します。ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

Table 1: ポリシー セットの構成時の設定

フィールド名	使用上のガイドライン
[ステータス（Status）]	このポリシーのステータスを選択します。次のいずれかを設定できます。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニターのみ（Monitor Only）]：このポリシー条件は評価されません。
ポリシー セット名	このポリシー セットの一意の名前を入力します。

フィールド名	使用上のガイドライン
条件（**Conditions**）	新しいポリシー行から、プラス（+）アイコンをクリックするか、既存のポリシー行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
説明	ポリシーの一意の説明を入力します。
許可されているプロトコルまたはサーバー順序（**Allowed Protocols or Server Sequence**）	すでに作成した許可されているプロトコルを選択するか、または（+）記号をクリックして [新しい許可されているプロトコルを作成（Create a New Allowed Protocol）] するか、[新しい RADIUS 順序を作成（Create a New Radius Sequence）] するか、または [TACACS 順序を作成（Create a TACACS Sequence）] します。
条件（**Conditions**）	新しい例外行から、プラス（+）アイコンをクリックするか、既存の例外行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
ヒット数（**Hits**）	ヒット数は、条件が一致した回数を示す診断ツールです。このアイコンが最後に更新された時刻を表示し、ゼロにリセットし、更新の頻度を表示するには、アイコンにカーソルを合わせます。

フィールド名	使用上のガイドライン
アクション（**Actions**）	さまざまなアクションを表示して選択するには、[アクション（Actions）] 列の歯車アイコン をクリックします。 • [上に新しい行を挿入（Insert new row above）] : [アクション（Actions）] メニューを開いたポリシーの上に新しいポリシーを挿入します。 • [下に新しい行を挿入（Insert new row below）] : [アクション（Actions）] メニューを開いたポリシーの下に新しいポリシーを挿入します。 • [上に複製（Duplicate above）] : 元のセットの上に、[アクション（Actions）] メニューを開いたポリシーの上に複製ポリシーを挿入します。 • [下に複製（Duplicate below）] : 元のセットの下に、[アクション（Actions）] メニューを開いたポリシーの下に複製ポリシーを挿入します。 • [削除（Delete）] : ポリシーセットを削除します。
表示（**View**）	矢印アイコンをクリックすると、特定のポリシーセットの [設定（Set）] ビューが開き、認証、例外、および許可のサブポリシーが表示されます。

認証ポリシー

各ポリシーセットには、そのセットの認証ポリシーを表す複数の認証ルールを含めることができます。認証ポリシーの優先順位は、（[認証ポリシー（Authentication Policy）] 領域の [設定（Set）] ビュー ページから）ポリシー セット自体に表示されるポリシーに対する順序に基づいて決定されます。

Cisco ISE は、ポリシー セット レベルで設定された設定に基づいて、ネットワーク アクセス サービス（許可されたプロトコルまたはサーバー順序のいずれか）を動的に選択し、その後、認証ポリシー レベルおよび許可ポリシー レベルから ID ソースおよび結果をチェックします。複数の条件を、Cisco ISE ディクショナリ内の任意の属性を使用して定義できます。Cisco ISE

では、個々のポリシー要素として条件を作成し、ライブラリに保存してから、他のルールベースのポリシーに再利用することができます。

認証ポリシーの結果である ID 特定方法は、次のいずれかになります。

- アクセスを拒否：ユーザーへのアクセスは拒否され、認証は実行されません。
- ID データベース：次のいずれかの単一の ID データベース。
  - 内部ユーザー
  - ゲスト ユーザー
  - 内部エンドポイント
  - Active Directory
  - Lightweight Directory Access Protocol（LDAP）データベース
  - RADIUS トークン サーバー（RSA または SafeWord サーバー）
  - 証明書認証プロファイル
- ID ソース順序：認証に使用する ID データベースの順序。

最初の Cisco ISE インストール時に実装されるデフォルト ポリシー セットには、デフォルトの ISE 認証ルールおよび許可ルールが含まれています。デフォルト ポリシー セットには、認証と許可のための追加の柔軟な組み込みルール（デフォルトではない）も含まれています。これらのポリシーにルールを追加して、組み込みルールを削除および変更できますが、デフォルト ルールを削除することはできず、デフォルト ポリシー セットを削除することはできません。

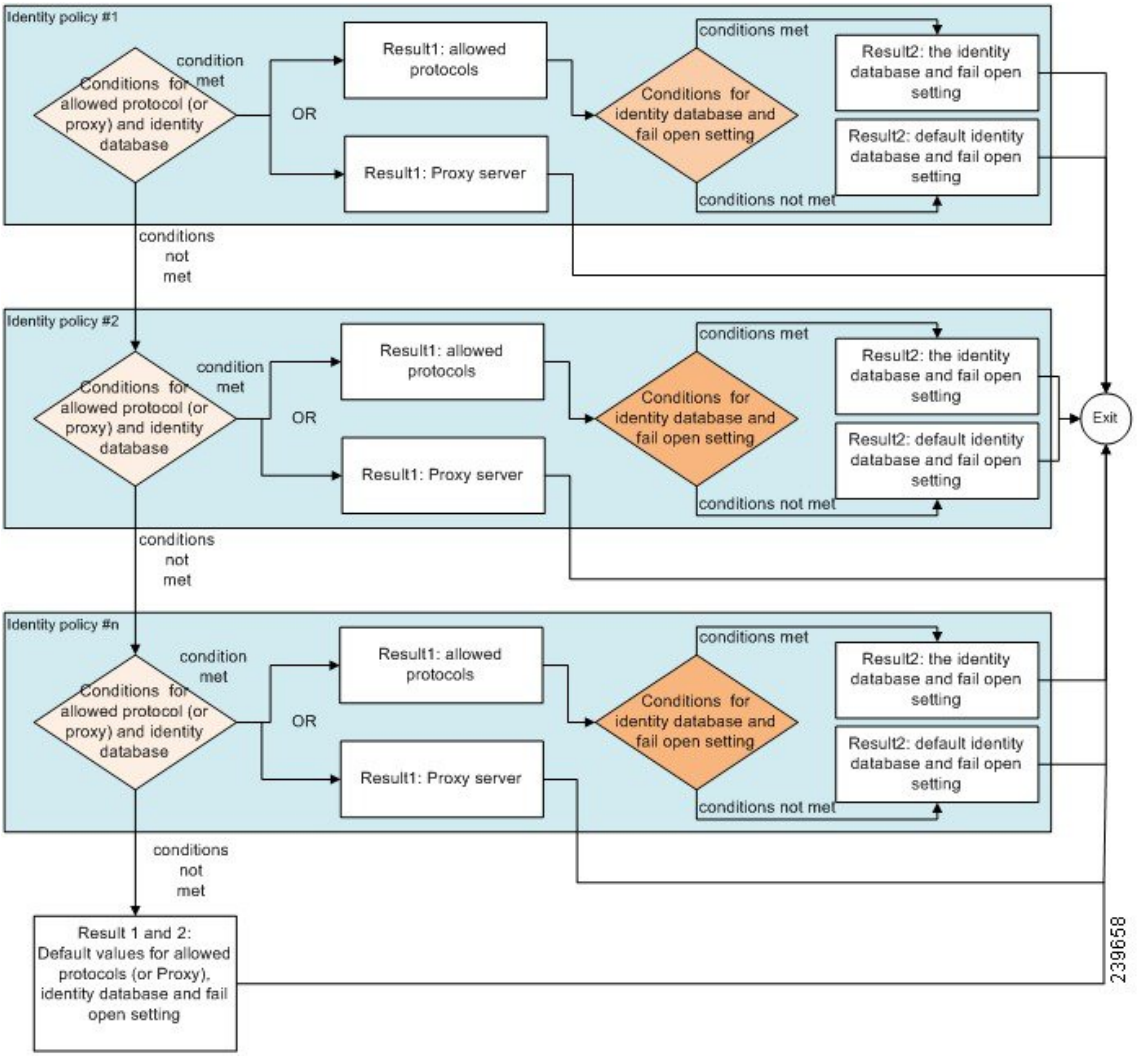
認証ポリシーのフロー

認証ポリシーでは、条件と結果で構成される複数のルールを定義できます。ISE は、指定された条件を評価し、評価結果に基づいて対応する結果を割り当てます。ID データベースは、基準に一致する最初のルールに基づいて選択されます。

異なるデータベースで構成される ID ソース順序を定義することもできます。Cisco ISE がデータベースを検索する順序を定義できます。Cisco ISE は、認証が成功するまで指定された順序でこれらのデータベースにアクセスします。1 つの外部データベースに同一ユーザーの複数のインスタンスが存在する場合、認証は失敗します。1 つの ID ソース内で、ユーザー レコードは重複できません。

ID ソース順序には、3 つのデータベース、または多くとも 4 つのデータベースを使用することを推奨します。

図 *1* : 認証ポリシーのフロー



認証失敗：ポリシー結果オプション

識別方法としてアクセス拒否を選択した場合、要求への応答として拒否メッセージが送信されます。ID データベースまたは ID ソース順序を選択して、認証が成功した場合、処理は同じポリシーセットに対して設定された許可ポリシーに対して続行されます。一部の認証は失敗し、その場合次のように分類されます。

- 認証の失敗：クレデンシャルが正しくない、無効なユーザーであることなどが原因で認証が失敗したことを示す明確な応答を受信します。アクションのデフォルト コースは拒否です。
- ユーザーが見つからない：どの ID データベースでもこのユーザーが見つかりませんでした。アクションのデフォルト コースは拒否です。

- 処理の失敗：ID データベース（複数の場合もある）にアクセスできません。アクションのデフォルト コースはドロップです。

Cisco ISE では、認証失敗に対して次のアクションのコースのいずれかを設定することができます。

- [拒否（Reject）]：拒否応答が送信されます。
- [ドロップ（Drop）]：応答は送信されません。
- [続行（Continue）]：許可ポリシーに従って Cisco ISE を継続します。

[続行（Continue）] オプションを選択した場合でも、使用されているプロトコルの制限により Cisco ISE が要求の処理を実行できない場合があります。PEAP、LEAP、EAP-FAST、EAP-TLS、または RADIUS MSCHAP を使用した認証では、認証に失敗したり、ユーザーが見つからなかったときには、要求の処理を続行することはできません。

認証に失敗した場合、PAP/ASCII または MAC 認証バイパス（MAB またはホスト ルックアップ）の許可ポリシーの処理を続行できます。その他のすべての認証プロトコルの場合、認証に失敗すると、次のいずれかの状態となります。

- 認証の失敗：拒否応答が送信されます。
- ユーザーまたはホストが見つからない：拒否応答が送信されます。
- 処理に問題が発生：応答は送信されず、要求はドロップされます。

認証ポリシーの設定

必要に応じて、複数の認証ルールを設定および管理することによって、ポリシーセットごとに認証ポリシーを定義します。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

ステップ 2 認証ポリシーを追加または更新するポリシーセットの行から、ポリシーセットの詳細のすべてにアクセスし、認証および許可ポリシーとポリシー例外を作成するために、[ポリシーセット（Policy Sets）]テーブルの [表示（View）] 列から › をクリックします。

ステップ 3 ページの認証ポリシー部分の横にある矢印アイコンをクリックして、テーブル内のすべての認証ポリシールールを展開して表示します。

ステップ 4 いずれかの行の[アクション（Actions）]列から、歯車アイコンをクリックします。ドロップダウンメニューから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して、新しい認証ポリシールールを挿入します。
[認証ポリシー（Authentication Policy）] テーブルに新しい行が表示されます。

ステップ 5 [ステータス（Status）] 列から、現在の [ステータス（Status）] アイコンをクリックし、ドロップダウンリストから必要に応じてポリシーセットのステータスを更新します。[ステータス（Status）]の詳細については、認証ポリシーの構成設定 （9 ページ）を参照してください。

ステップ 6 テーブル内のルールの場合は、[ルール名（Rule Name）] または [説明（Description）] のセルをクリックして、フリーテキストを変更します。

ステップ 7 条件を追加または変更するには、[条件（Conditions）] 列のセルにカーソルを合わせ、  をクリックします。[条件スタジオ（Conditions Studio）] が開きます。詳細については、特別なネットワーク アクセス条件（55 ページ）を参照してください。

選択するすべての属性に「Equals」、「Not Equals」、「In」、「Not In」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現（REGEX）をサポートし、使用します。

（注） 単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数値属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。リストの場合、「in」演算子は、特定の値がリスト内に存在するかどうかをチェックします。単一文字列の場合、「in」演算子は、文字列が「equals」演算子などと同じかどうかをチェックします。

ステップ 8 チェックして一致させる順序に従って、テーブル内のポリシーを編成します。ルールの順序を変更するには、行をドラッグして正しい位置にドロップします。

ステップ 9 [保存（Save）] をクリックすると、変更内容が保存されて実装されます。

次のタスク

1. 許可ポリシーの設定

認証ポリシーの構成設定

次の表では、[ポリシーセット（Policy Sets）] ウィンドウの [認証ポリシー（Authentication Policy）]セクションのフィールドについて説明します。これらのフィールドから、認証サブポリシーをポリシーセットの一部として構成できます。 ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ポリシーセット（Policy Sets）]**を選択します。デバイス管理ポリシーの場合は、**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]**を選択します。[ポリシーセット（Policy Sets）] ページから、**[表示（View）] > [認証ポリシー（Authentication Policy）]** を選択します。

Table 2: 認証ポリシーの構成設定

フィールド名	使用上のガイドライン
[ステータス（Status）]	このポリシーのステータスを選択します。次のいずれかを設定できます。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニターのみ（Monitor Only）]：このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証（Live Log authentication）]ページでこのポリシー条件の結果を照会できます。ここでは、モニターされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加する場合に、条件がもたらす結果が正しいかどうかを判断できないことがあります。この場合、モニター モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。
ルール名	この認証ポリシーの名前を入力します。
条件（Conditions）	新しいポリシー行から、プラス（+）アイコンをクリックするか、または既存のポリシー行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。
使用（Use）	認証に使用する ID ソースを選択します。ID ソース順序が設定済みである場合、これを選択することも可能です。 デフォルトの ID ソースを編集して、このルールで定義されたいずれの ID ソースも要求に一致しない場合に Cisco ISE が使用する ID ソースを指定できます。

フィールド名	使用上のガイドライン
オプション（**Options**）	認証失敗、ユーザーが見つからない、プロセス障害、の各イベントに対する今後のアクションのコースを定義します。次のいずれかのオプションを選択できます。 • [拒否（Reject）]：拒否応答が送信されます。 • [ドロップ（Drop）]：応答は送信されません。 • [続行（Continue）]：Cisco ISE は認証ポリシーの処理を続行します。
ヒット数（**Hits**）	ヒット数は、条件が一致した回数を示す診断ツールです。
アクション（**Actions**）	さまざまなアクションを表示して選択するには、[アクション（Actions）] 列の歯車アイコン をクリックします。 • [上に新しい行を挿入（Insert new row above）]：[アクション（Actions）] メニューを開いたポリシーの上に新しい認証ポリシーを挿入します。 • [下に新しい行を挿入（Insert new row below）]：[アクション（Actions）] メニューを開いたポリシーの下に新しい認証ポリシーを挿入します。 • [上に複製（Duplicate above）]：元のセットの上に、[アクション（Actions）] メニューを開いたポリシーの上に複製認証ポリシーを挿入します。 • [下に複製（Duplicate below）]：元のセットの下に、[アクション（Actions）] メニューを開いたポリシーの下に複製認証ポリシーを挿入します。 • [削除（Delete）]：ポリシーセットを削除します。

パスワード ベースの認証

認証とは、ユーザー情報を検証してユーザー ID を確認することです。従来の認証方式では、名前とある決まったパスワードが使用されていました。これは、最も一般的かつ単純で、低コストの認証方式です。この方式の欠点は、ユーザー名やパスワードの情報が簡単に第三者に伝えられたり、推測または不正に取得されたりする可能性がある点です。単純な暗号化されていないユーザー名とパスワードを使用する方法は、強力な認証方式とは考えられていませんが、インターネットアクセスなど、許可または特権レベルが低い場合は十分に要件を満たす可能性があります。

暗号化されたパスワードと暗号化技術を使用したセキュアな認証

ネットワーク上でパスワードが不正に取得される危険性を低減するには、暗号化を使用する必要があります。RADIUS などのクライアント/サーバー アクセス コントロール プロトコルでは、パスワードを暗号化することにより、ネットワーク内でパスワードが不正に取得される事態を防止します。ただし、RADIUS は認証、許可、およびアカウンティング（AAA）クライアントと Cisco ISE との間でだけ動作します。認証プロセスでは、このポイントの前で、許可されていないユーザーが次のような例で暗号化されていないパスワードを入手する可能性があります。

- 電話回線を介してダイヤルアップ接続を行うエンドユーザークライアントとの間の通信
- ネットワークアクセスサーバーで終了する ISDN 回線
- エンドユーザー クライアントとホスティング デバイスの間の Telnet セッションを介して行われる通信

さらに安全な方式では、チャレンジハンドシェイク認証プロトコル（CHAP）、ワンタイムパスワード（OTP）、および高度な EAP ベースのプロトコルの内部で使用されるような暗号化技術を使用します。Cisco ISE は、これらのさまざまな認証方式をサポートしています。

認証方式と許可特権

認証と許可には基本的な暗黙の関係があります。ユーザーに与えられる許可特権が多くなればなるほど、それに応じて認証を強化する必要があります。Cisco ISE では、さまざまな認証方式を提供することにより、この関係がサポートされています。

認証ダッシュレット

Cisco ISE のダッシュボードには、ネットワークとデバイスに対し行われたすべての認証の概要が表示されます。これには、[認証（Authentication）] ダッシュレットにある認証および許可の失敗についての概要情報が表示されます。

[RADIUS 認証（RADIUS Authentication）] ダッシュレットには、Cisco ISE が処理した認証に関する次の統計情報が表示されます。

- 認証成功、認証失敗、同一ユーザーによる同時ログインなど、Cisco ISE が処理した RADIUS 認証要求の総数。

- Cisco ISE が処理した、失敗した RADIUS 認証要求の総数。

また、TACACS+認証の概要を表示することもできます。TACACS+認証ダッシュレットには、デバイス認証の統計情報が表示されます。

デバイス管理認証の詳細については、TACACS ライブ ログを参照してください。RADIUS ライブ ログ設定の詳細については、RADIUS ライブ ログを参照してください。

> ISE コミュニティ リソース
>
> 認証と許可の失敗のトラブルシューティング方法については、「How To: Troubleshoot ISE Failed Authentications & Authorizations」を参照してください。

認証結果の表示

Cisco ISE にはリアルタイムで認証の概要を表示するさまざまな方法があります。

始める前に

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

ステップ 1 ネットワーク認証（RADIUS）の場合は、**[操作（Operations）] > [RADIUS] > [ライブログ（Live Logs）]** を選択し、デバイス認証（TACACS）の場合は **[操作（Operations）] > [TACACS] > [ライブログ（Live Logs）]** を選択して、リアルタイム認証の概要を表示します。

ステップ 2 認証の概要を表示するには、次のような方法があります。

- [ステータス（Status）]アイコンの上にマウス カーソルを移動すると、認証の結果と概要を表示できます。ステータスの詳細とともにポップアップが表示されます。
- 結果をフィルタリングするには、リストの最上部に表示される 1 つ以上の任意のテキスト ボックスに検索条件を入力して **Enter** を押します。
- 詳細なレポートを表示するには、[詳細（Details）] の虫眼鏡アイコンをクリックします。

（注） [認証概要（Authentication Summary）] レポートまたはダッシュボードが失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。

認証レポートおよびトラブルシューティング ツール

認証の詳細の他に、Cisco ISE では、ネットワークの効率的な管理に使用できるさまざまなレポートおよびトラブルシューティング ツールが提供されます。

ネットワーク内の認証の傾向およびトラフィックを把握するために実行できるさまざまなレポートがあります。現在のデータに加えて履歴のレポートを生成できます。認証レポートのリストは次のとおりです。

- AAA の診断
- RADIUS アカウンティング（RADIUS Accounting）
- RADIUS 認証
- 認証概要（Authentication Summary）

（注） Cisco Catalyst 4000 シリーズ スイッチで IPv6 スヌーピングを有効にする必要があります、有効にしないと、IPv6 アドレスが認証セッションにマッピングされず、show の出力に表示されません。IPv6 スヌーピングを有効にするには、次のコマンドを使用します。

```
vlan config <vlan-number>
 ipv6 snooping
 end
ipv6 nd raguard policy router
 device-role router
interface <access-interface>
  ipv6 nd raguard
interface <uplink-interface>
  ipv6 nd raguard attach-policy router
  end
```

認可ポリシー

許可ポリシーは、Cisco ISE ネットワーク許可サービスのコンポーネントです。このサービスを使用して、ネットワーク リソースにアクセスする特定のユーザーおよびグループの許可ポリシーを定義し、許可プロファイルを設定することができます。

許可ポリシーには条件付きの要件を含めることができ、この要件では、1つ以上の許可プロファイルを返すことができる許可チェックを含む複合条件を使用して、1 つ以上の ID グループを組み合わせます。さらに、条件付きの要件は、特定の ID グループの使用とは別に存在することがあります。

許可プロファイルは、Cisco ISE で許可ポリシーを作成するときに使用されます。許可ポリシーは許可ルールで構成されます。許可ルールには、名前、属性、および権限の3つの要素があります。権限要素は、許可プロファイルにマッピングされます。

Cisco ISE の許可プロファイル

許可ポリシーは、特定のユーザーおよびグループのIDにルールを関連付け、対応するプロファイルを作成します。これらのルールが設定された属性と一致する場合は、常に、権限を付与する、対応する許可プロファイルがポリシーによって返され、ネットワーク アクセスがこれに応じて許可されます。

たとえば、許可プロファイルには、次のタイプに含まれるさまざまな権限を含めることができます。

- 標準プロファイル
- 例外プロファイル
- デバイスベースのプロファイル

プロファイルは、利用可能なベンダー ディクショナリのいずれかに保存されているリソース セットから選択された属性で構成され、特定の許可ポリシーの条件が一致したときに返されます。許可ポリシーには単一のネットワーク サービス ルールにマッピングする条件を含めることができるため、許可チェックのリストを含めることもできます。

許可確認は、返される許可プロファイルに準拠する必要があります。許可確認は、通常、ライブラリに追加できるユーザー定義名を含む1つ以上の条件から構成され、他の許可ポリシーで再利用できます。

認証ポリシーの UDN プロファイル

Cisco ISE アカウントがユーザー定義ネットワークと呼ばれるソリューションの一部である場合、User Defined Network という名前の認証プロファイルが Cisco ISE のすべての認証ポリシーに追加されます。これにより、Cisco ISE と WLC 間でユーザー定義ネットワークデバイス構成を共有できます。

[ポリシー（Policy）]>[ポリシーセット（Policy Sets）]>[認証ポリシー（Authorization Policies）]を選択します。プロファイル **UDN** がリストのすべての認証ポリシーに表示されます。

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。 **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] > [認証ポリシー（Authorization Policies）]** を選択します。プロファイル **UDN** がリストのすべての認証ポリシーに表示されます。

Cisco ISE 管理者は、ユーザー定義ネットワークの目的で使用しないポリシーからユーザー定義ネットワークプロファイルを削除できます。ただし、認証ポリシーからはプロファイルのユーザー定義ネットワークを削除しないことを推奨します。

ユーザー定義ネットワークプロファイルだけでは、認証ポリシーを使用できません。

詳細については、ご使用のリリースの『*Cisco ISE Release Notes*』の「User Defined Network」のセクションを参照してください。

許可プロファイルの権限

許可プロファイルの権限設定を開始する前に、以下を確認します。

- 認証ポリシーおよび認証プロファイル間の関係を理解している。
- **[認証プロファイル（Authorization Profile）]** ページをよく理解している。
- ポリシーおよびプロファイルを設定する場合に必要な基本ガイドラインを知っている。
- 認証プロファイルの権限の構成を理解している。

認証プロファイルを使用するには、**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]**>**[結果（Results）]** を選択します。左側のメニューから、**[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** を選択します。

ネットワークでさまざまなタイプの認証プロファイルのポリシー要素権限を表示、作成、変更、削除、複製、または検索するプロセスの開始点として **[結果（Results）]** ナビゲーションウィンドウを使用します。**[結果（Results）]** ペインには、最初 [認証（Authentication）]、[許可（Authorization）]、[プロファイリング（Profiling）]、[ポスチャ（Posture）]、[クライアントプロビジョニング（Client Provisioning）]、および [TrustSec] のオプションが表示されています。

許可プロファイルでは、RADIUS 要求が受け入れられたときに返される属性を選択できます。Cisco ISE では、[共通タスク設定（Common Tasks Settings）] を設定して共通に使用される属性をサポートできるメカニズムが提供されます。Cisco ISE が基盤となる RADIUS 値に変換する [共通タスク属性（Common Tasks Attributes）] の値を入力する必要があります。

ISE コミュニティ リソース

802.1x サプリカント（Cisco AnyConnect Mobile Security）とオーセンティケータ（スイッチ）間の Media Access Control Security（MACsec）暗号化を設定する方法の例については、「MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example」を参照してください。

ロケーションに基づく認証

Cisco ISE は、Cisco モビリティ サービス エンジン（MSE）と統合し、物理ロケーション ベースの認証を導入します。Cisco ISE は、MSE からの情報を使用して、MSE によって報告されるユーザーの実際の位置に基づいて差別化されたネットワーク アクセスを提供します。

この機能を使用すると、エンドポイントのロケーション情報を使用して、ユーザーが適切なゾーンにいる場合にネットワーク アクセスを提供できます。また、エンドポイントのロケーションをポリシーの追加属性として追加して、デバイスのロケーションに基づいてより詳細なポリシー許可のセットを定義することもできます。次のように、ロケーションベースの属性を使用する許可ルール内で条件を設定できます。

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

ロケーション階層（キャンパス/ビルディング/フロア構造）を定義して、Cisco Prime Infrastructure のアプリケーションを使用してセキュアおよび非セキュアのゾーンを設定できます。ロケーション階層を定義した後、ロケーション階層データを MSE サーバーと同期する必要があります。Cisco Prime Infrastructure の詳細については、http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html を参照してください。

1 つまたは複数の MSE インスタンスを追加して、MSE ベースのロケーション データを許可プロセスに統合できます。これらの MSE からロケーション階層データを取得し、このデータを使用してロケーション ベースの許可ルールを設定できます。

エンドポイントの移動を追跡するには、許可プロファイルの作成時に [移動の追跡（Track Movement）] チェックボックスをオンにします。Cisco ISE は、5 分ごとにエンドポイント ロケーションの関連 MSE にクエリを行い、ロケーションが変更されたかどうかを確認します。

（注）
- Cisco ISE に MSE デバイスを追加する場合は、許可が簡単になるように MSE デバイスから ISE に証明書をコピーします。
- 複数のユーザーを追跡すると、頻繁な更新によってパフォーマンスに影響します。[移動の追跡（Track Movement）] オプションは、上位のセキュリティ ロケーションに使用できます。
- ロケーション ツリーは、MSE インスタンスから取得されたロケーション データを使用して作成されます。ロケーションツリーを使用して、許可ポリシーに公開するロケーション エントリを選択できます。
- ロケーションサービスを使用するには、Cisco ISE Plus ライセンスが必要です。

MSE サーバーの追加

始める前に

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

ステップ 1 [管理（Administration）]>[ネットワークリソース（Network Resources）]>[ロケーションサービス（Location Services）] > [ロケーションサーバー（Location Servers）] 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 サーバー名、ホスト名/IP アドレス、パスワードなど、MSE サーバーの詳細を入力します。

ステップ 4 指定したサーバーの詳細を使用して MSE の接続性をテストするには、[テスト（Test）] をクリックします。

ステップ 5 （任意）エンドポイントがこの MSE に現在接続されているかどうかを確認するには、[ロケーション検索（Find Location）] フィールドにエンドポイントの MAC アドレスを入力し、[検索（Find）] をクリックします。

エンドポイントのロケーションが見つかった場合は、*Campus:Building:Floor:Zone* の形式で表示されます。ロケーションの階層およびゾーンの設定によっては、複数のエントリが表示される場合があります。たとえば、*Campus1* という名前のキャンパス内のビルディング（*building1*）のすべてのフロアが非セキュア ゾーンとして定義され、最初のフロアのラボ エリアがセキュア ゾーンとして定義されている場合、エンドポイントがそのラボ エリアにある場合は、次のエントリが表示されます。

見つかった場所：

Campus1#building1#floor1#LabArea

Campus1#building1#floor1#NonSecureZone

ステップ 6 [送信（Submit）] をクリックします。

新しい MSE を追加したら、[ロケーションツリー（Location Tree）] ページに移動し、[更新の取得（Get Update）] をクリックして、ロケーション階層を取得し、それをロケーション ツリーに追加します。このツリーで定義されたフィルタがある場合、これらのフィルタは新しい MSE エントリにも適用されます。

ロケーション ツリー

ロケーション ツリーは、MSE インスタンスから取得されたロケーション データを使用して作成されます。[ロケーションツリー（Location Tree）] を表示するには、[管理（Administration）] >[ネットワークリソース（Network Resources）]>[ロケーションサービス（Location Services）] > [ロケーションツリー（Location Tree）] を選択します。

1 つのビルディングに複数の MSE がある場合、Cisco ISE はすべての MSE からロケーションの詳細を照合し、単一のツリーとして表示します。

ロケーション ツリーを使用して、許可ポリシーに公開するロケーション エントリを選択できます。また、要件に基づいて特定のロケーションを非表示にすることもできます。ロケーションを非表示にする前にロケーション ツリーを更新することを推奨します。非表示にされたロケーションは、ツリーが更新されても非表示のままになります。

許可ルールに関連するロケーション エントリが変更または削除された場合は、影響を受けるルールをディセーブルにし、これらのロケーションを [不明（Unknown）] として設定するか、または影響を受ける各ルールに代替ロケーションを選択する必要があります。変更を適用したり更新をキャンセルする前に新しいツリー構造を確認する必要があります。

すべての MSE から最新のロケーション階層構造を取得するには、[更新の取得（Get Update）] をクリックします。新しいツリー構造を確認したら、[保存（Save）] をクリックして変更を適用します。

ダウンロード可能 ACL

アクセス コントロール リスト（ACL）はアクセス コントロール エントリ（ACE）のリストで、ポリシー適用ポイント（スイッチなど）によってリソースに適用できます。各 ACE は、読み取り、書き込み、実行など、このオブジェクトに対してユーザーごとに許可された権限を識別します。たとえば、ある ACE で販売グループに書き込み権限を許可し、別の ACE で組織内の他のすべての従業員に読み取り権限を許可して、ネットワーク内の販売エリアを使用するように ACL を設定できます。RADIUS プロトコルの場合、送信元と宛先の IP アドレス、トランスポート プロトコル、および他のパラメータをフィルタリングして、ACL は許可を付与します。スタティック ACL はスイッチ上に配置されており、スイッチから直接設定でき、ISE GUI から許可ポリシーに適用できます。ダウンロード可能な ACL（DACL）は、ISE GUI から許可ポリシーで設定、管理、および適用できます。DACL は、カスタムユーザー属性と AD 属性を使用して設定することもできます。

ISE でネットワーク許可ポリシーに DACL を実装する場合：

1. **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ダウンロード可能なACL（Downloadable ACLs）]** から新規または既存の DACL を設定します。詳細については、ダウンロード可能 ACL に対する権限の設定 （19 ページ）を参照してください。

2. 設定済みの DACL を使用して、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可プロファイル（Authorization Profiles）]** から新規または既存の許可プロファイルを設定します。
3. **[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets]** から新規および既存のポリシー セットを作成および設定する場合は、設定済みの許可プロファイルを実装します。

ダウンロード可能 ACL に対する権限の設定

Cisco ISE の場合、ダウンロード可能な ACL（DACL）は、さまざまなユーザーおよびユーザー グループがネットワークにアクセスする方法を制御するために許可ポリシーで設定および導入できます。デフォルト許可 DACL は、次のデフォルト プロファイルを含む ISE のインストール時に使用できます。

- DENY_ALL_IPV4_TRAFFIC
- PERMIT_ALL_IPV4_TRAFFIC
- DENY_ALL_IPV6_TRAFFIC
- PERMIT_ALL_IPV6_TRAFFIC

DACL を使用する場合、これらのデフォルトは設定できませんが、他の同じような DACL を作成するために複製することはできます。

必要な DACL を設定した後に、ネットワーク上で関連する認証ポリシーにその DACL を適用できます。認証ポリシーで使用されている DACL は、編集または削除できません。その DACL を編集または削除するには、まずその DACL を認証ポリシーから削除する必要があります。DACL を更新した後に、必要に応じて、同じ DACL を認証ポリシーに再適用できます。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[ダウンロード可能 ACL（Downloadable ACLs）]** を選択します。

ステップ 2 [ダウンロード可能なACL（Downloadable ACLs）] テーブル上部の **[追加（Add）]** をクリックするか、既存の DACL を選択し、テーブル上部の **[複製（Duplicate）]** をクリックします。

ステップ 3 次のルールに留意しながら、DACL に適切な値を入力または編集します。

- [名前（Name）] フィールドのサポート対象の文字：英数字、ハイフン（-）、ドット（.）、アンダースコア（_）
- 次の DACL タイプを選択すると、IP 形式は選択した IP バージョンに基づいて処理されます。
  - IPv4 の法的な ACE のみを検証する [IPv4]。有効な IPv4 形式を入力する必要があります。
  - IPv6 の法的な ACE のみを検証する [IPv6]。有効な IPv6 形式を入力する必要があります。
  - 以前のリリースからリリース 2.6 にアップグレードされた DACL では、[IP バージョン（IP Version）] フィールドに DACL タイプとして [非依存（Agnostic）] オプションが表示されます。必要に応じて形式を入力します。シスコでサポートされていないデバイスの DACL を作成するには、[非依存（Agnostic）] を使用します。[非依存（Agnostic）] を選択すると、形式は検証されないため、DACL 構文をチェックすることはできません。

- キーワード **Any** が DACL のすべての ACE のソースである必要があります。DACL がプッシュされると、ソースの **Any** がスイッチに接続されているクライアントの IP アドレスで置き換えられます。

（注） **[IP バージョン（IP Version）]** フィールドは、DACL がいずれかの認証プロファイルにマッピングされている場合は編集できません。この場合、**[認証プロファイル（Authorization Profiles）]** から DACL 参照を削除し、IP バージョンを編集して、**[認証プロファイル（Authorization Profiles）]** の DACL を再マッピングします。

ステップ 4 必要に応じて、ACEのすべてのリストの作成が完了したら、[DACL構文のチェック（Check DACL Syntax）] をクリックしてリストを検証します。検証エラーが発生した場合、自動的に表示されるウィンドウで無効な構文を識別する特定の指示が返されます。

ステップ 5 [Submit] をクリックします。

Active Directory ユーザー許可のためのマシン アクセス制限

Cisco ISE には、Microsoft Active Directory 認証ユーザーの許可を制御する追加の方法を提供する、マシンアクセス制限（MAR）コンポーネントが含まれています。この形式の許可は、Cisco ISE ネットワークにアクセスするために使用されるコンピュータのマシン認証に基づきます。成功したマシン認証ごとに、Cisco ISE は、RADIUS Calling-Station-ID 属性（属性 31）で受信した値を、成功したマシン認証の証拠としてキャッシュします。

Cisco ISE は、[Active Directory の設定（Active Directory Settings）] ページの [存続可能時間（Time to Live）] パラメータで設定された時間が失効になるまで各 Calling-Station-ID 属性値をキャッシュに保持します。失効したパラメータは、Cisco ISE によってキャッシュから削除されます。

ユーザーをエンドユーザー クライアントから認証する場合、Cisco ISE は、成功したマシン認証の Calling-Station-ID 値のキャッシュを検索して、ユーザー認証要求で受信した Calling-Station-ID 値を見つけようとします。Cisco ISE が一致するユーザー認証 Calling-Station-ID 値をキャッシュで見つけた場合、これは、次の方法で認証を要求するユーザーに Cisco ISE が権限を割り当てる方法に影響します。

- Calling-Station-ID 値が Cisco ISE キャッシュで見つかった値と一致する場合、成功した許可の許可プロファイルを割り当てます。
- Calling-Station-ID 値が Cisco ISE キャッシュの値と一致しないことがわかった場合、マシン認証のない成功したユーザー認証の許可プロファイルを割り当てます。

許可ポリシーおよびプロファイルの設定のガイドライン

許可ポリシーおよびプロファイルを管理または運用する場合、次のガイドラインに従ってください。

- 作成するルール名は、サポートされている次の文字のみを使用する必要があります。
  - 記号：プラス（+）、ハイフン（-）、アンダースコア（_）、ピリオド（.）、およびスペース（ ）。

- アルファベット文字：A ～ Z、a ～ z。
- 数字：0 ～ 9。

- ID グループのデフォルトは「Any」です（このグローバル デフォルトを使用してすべてのユーザーに適用できます）。
- 条件では、1 つ以上のポリシー値を設定することが許可されています。ただし、条件はオプションであり、許可ポリシーを作成する場合に必須ではありません。次に、条件を作成する 2 つの方法を示します。
  - 選択肢の対応するディクショナリから既存の条件または属性を選択します。
  - 推奨値を選択またはテキストボックスを使用してカスタム値を入力できるカスタム条件を作成します。
- 作成する条件名は、サポートされている次の文字のみを使用する必要があります。
  - 記号：ハイフン（-）、アンダースコア（_）、およびピリオド（.）。
  - アルファベット文字：A ～ Z、a ～ z。
  - 数字：0 ～ 9。
- 認証プロファイルを作成または編集するときに、[クライアント プロビジョニング（ポリシー）（Client Provisioning (Policy)）] 以外のオプションで [Webリダイレクション（CWA、MDM、NSP、CPP）（Web Redirection (CWA, MDM, NSP, CPP)）] を有効にする場合、IPv6 アドレスをその許可ポリシーの [スタティックIP/ホスト名/FQDN（Static IP/Host name/FQDN）] として設定することはできません。これは、IPv6 のスタティック IP/ホスト名/FQDN が中央 Web 認証（CWA）、モバイル デバイス管理（MDM）リダイレクト、およびネイティブ サプリカント プロトコル（NSP）でサポートされていないためです。
- 権限は、ポリシーに使用する許可プロファイルを選択するときに重要です。権限は、特定のリソースへのアクセス権を付与したり、特定のタスクの実行を可能にしたりできます。たとえば、あるユーザーが特定の ID グループ（デバイス管理者など）に属しており、そのユーザーが定義済みの条件（サイトがボストンにあるなど）を満たしている場合、このユーザーは、そのグループに関連付けられた権限（特定のネットワーク リソースのセットへのアクセス権、デバイスへの特定の操作を実行する権限など）を付与されます。
- 認可条件で **radius** 属性 **Tunnel-Private-Group-ID** を使用する場合、**EQUALS** 演算子を使用するときに、条件にタグと値の両方を指定する必要があります。次に例を示します。

```
Tunnel-Private-Group-ID EQUALS (tag=0) 77
```

許可ポリシーの設定

[ポリシー（Policy）] メニューから許可ポリシーの属性および構成要素を作成したら、[ポリシーセット（Policy Sets）] メニューからポリシー セット内で許可ポリシーを作成します。

始める前に

この手順を開始する前に、ID グループと条件など、許可ポリシーの作成に使用されるさまざまなビルディング ブロックについて基本を理解しておく必要があります。

ステップ 1 ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

ステップ 2 [表示（View）]列から、 をクリックしてすべてのポリシーセットの詳細にアクセスし、認証および許可ポリシーとポリシー例外を作成します。

ステップ 3 ページの許可ポリシー部分の横にある矢印アイコンをクリックして、[許可ポリシー（Authorization Policy）] テーブルを展開して表示します。

ステップ 4 いずれかの行の [アクション（Actions）] 列から、歯車アイコンをクリックします。ドロップダウン メニューから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して、新しい許可ポリシー ルールを挿入します。
[許可ポリシー（Authorization Policy）] テーブルに新しい行が表示されます。

ステップ 5 ポリシーのステータスを設定するには、現在の [ステータス（Status）] アイコンをクリックし、ドロップダウンリストの [ステータス（Status）] 列から必要なステータスを選択します。ステータスの詳細については、許可ポリシーの設定 （25 ページ） を参照してください。

ステップ 6 テーブル内のポリシーの場合は、[ルール名（Rule Name）] のセルをクリックしてフリーテキストを変更し、一意のルール名を作成します。

ステップ 7 条件を追加または変更するには、[条件（Conditions）] 列のセルにカーソルを合わせ、 をクリックします。[条件スタジオ（Conditions Studio）] が開きます。詳細については、#unique_1052を参照してください。

選択するすべての属性に「Equals」、「Not Equals」、「In」、「Not In」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現（REGEX）をサポートし、使用します。

（注） 単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数値属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。リストの場合、「in」演算子は、特定の値がリスト内に存在するかどうかをチェックします。単一文字列の場合、「in」演算子は、文字列が「equals」演算子などと同じかどうかをチェックします。

ステップ 8 ネットワーク アクセス結果プロファイルの場合は、[結果プロファイル（Results Profiles）] ドロップダウンリストから関連する許可プロファイルを選択するか、または を選択またはクリックして、[新しい許可プロファイルの作成（Create a New Authorization Profile）] を選択し、[新しい標準プロファイルの追加（Add New Standard Profile）] 画面が開いたら、次の手順を実行します。

a) 必要に応じて値を入力して、新しい許可プロファイルを設定します。次の点を考慮してください。

- [名前（name）] フィールドでサポートされる文字は次のとおりです：スペース、! # $ % & ‘ ( ) * + , - . / ; = ? @ _ {。
- [共通タスク（Common Tasks）] の場合、DACL を入力し、次の関連する [DACL名（DACL Name）] オプションを選択して、動的なドロップダウン リストから必要な DACL を選択します。
  - IPv4 DACL を使用するには、[DACL名（DACL Name）] をオンにします。
  - IPv6 DACL を入力するには、[IPv6 DACL名（IPv6 DACL Name）] をオンにします。
  - 他の DACL 構文を入力するには、いずれかのオプションをオンにします。IPv4 と IPv6 の両方のドロップダウン リストに依存しない DACL が表示されます。

    （注） [DACL名（DACL Name）] を選択すると、DACL 自身が非依存でも、AVP タイプは IPv4 です。[IPv6 DACL名（IPv6 DACL Name）] の DACL を選択すると、DACL 自身が非依存でも、AVP タイプは IPv6 です。

- （注） ポリシーに ACL を使用する場合は、デバイスとこの機能に互換性があることを確認します。詳細については、『*Cisco Identity Services Engine Compatibility Guide*』を参照してください。

[共通タスク（Common Tasks）] の場合、ACL を入力するには、次のように関連する [ACL（フィルタID）（ACL (Filter-ID)）] オプションを選択し、フィールドに ACL 名を入力します。

- IPv4 ACL を使用するには、[ACL（フィルタID）（ACL (Filter-ID)）] をオンにします。
- IPv6 ACL を入力するには、[ACL IPv6（フィルタID）（ACL IPv6 (Filter-ID)）] をオンにします。

- Airespace デバイスで ACL を使用するには、必要に応じて [Airespace ACL名（Airespace ACL Name）] または [Airespace IPv6 ACL名（Airespace IPv6 ACL Name）] をオンにして、フィールドに ACL 名を入力します。
- 画面下部に動的に表示される [属性詳細（Attributes Details）] から許可プロファイル RADIUS 構文をダブルチェックできます。

b) [保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、許可プロファイルを作成します。

c) [ポリシーセット（Policy Sets）] 領域外のプロファイルを作成、管理、編集、および削除するには、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authorization）] > [認証プロファイル（Authorization Profiles）]** を選択します。

ステップ 9 ネットワーク アクセス結果のセキュリティ グループの場合は、[結果のセキュリティ グループ（Results Security Groups）] ドロップダウンリストから関連するセキュリティ グループを選択するか、または ➕ をクリックして、[新しいセキュリティ グループの作成（Create a New Security Group）] を選択し、[新しいセキュリティ グループの作成（Create New Security Group）] 画面が開いたら、次の手順を実行します。

a) 新規セキュリティ グループの名前と説明（オプション）を入力します。

b) この SGT を Cisco ACI に反映するには、[ACI に伝達（Propagate to ACI）] チェックボックスをオンにします。この SGT に関連する SXP マッピングは、Cisco ACI が [Cisco ACI の設定（Cisco ACI Settings）] ページで選択した VPN に所属している場合にのみ Cisco ACI に反映されます。

このオプションはデフォルトでは無効になっています。

c) タグ値を入力します。タグ値は、手動で入力したり、自動生成されるようにしたり設定できます。また SGT の範囲を予約できます。これは、から設定できます。[一般TrustSecの設定（General TrustSec Settings）] ページ（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）]）。

d) [送信（Submit）] をクリックします。

詳細については、セキュリティ グループの設定 （140 ページ）を参照してください。

ステップ 10 TACACS+ の結果については、[結果（Results）] ドロップダウンリストから関連するコマンド セットとシェル プロファイルを選択するか、または [コマンド セット（Command Sets）] または [シェル プロファイル（Shell Profiles）] 列で ✚ をクリックして、[コマンドの追加（Add Commands）] 画面または [シェルプロファイルの追加（Add Shell Profile）] をそれぞれ開きます。[新しいコマンドセットの作成（Create a New Command Set）] または [新しいシェル プロファイルの作成（Create a New Shell Profile）] を選択し、フィールドに入力します。

ステップ 11 テーブル内でポリシーをチェックして一致させる順序を編成します。

ステップ 12 [保存（Save）] をクリックして、変更を Cisco ISE システム データベースに保存し、この新しい許可ポリシーを作成します。

認証ポリシーの UDN プロファイル

Cisco ISE アカウントがユーザー定義ネットワークと呼ばれるソリューションの一部である場合、User Defined Network という名前の認証プロファイルが Cisco ISE のすべての認証ポリシーに追加されます。これにより、Cisco ISE と WLC 間でユーザー定義ネットワークデバイス構成を共有できます。

[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] > [認証ポリシー（Authorization Policies）] を選択します。プロファイル **UDN** がリストのすべての認証ポリシーに表示されます。

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。 **[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** > **[認証ポリシー（Authorization Policies）]** を選択します。プロファイル **UDN** がリストのすべての認証ポリシーに表示されます。

Cisco ISE 管理者は、ユーザー定義ネットワークの目的で使用しないポリシーからユーザー定義ネットワークプロファイルを削除できます。ただし、認証ポリシーからはプロファイルのユーザー定義ネットワークを削除しないことを推奨します。

ユーザー定義ネットワークプロファイルだけでは、認証ポリシーを使用できません。

詳細については、ご使用のリリースの『*Cisco ISE Release Notes*』の「User Defined Network」のセクションを参照してください。

許可ポリシーの設定

次の表では、[ポリシーセット（Policy Sets）] ウィンドウの [許可ポリシー（Authorization Policy）] セクションのフィールドについて説明します。このフィールドから、許可ポリシーをポリシーセットの一部として構成できます。ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。[ポリシーセット（Policy Sets）] ページから、**[表示（View）]** > **[認証ポリシー（Authorization Policy）]** を選択します。ネットワーク アクセス ポリシーの場合は、

表 *3:* 許可ポリシーの構成時の設定

フィールド名	使用上のガイドライン
[ステータス（Status）]	このポリシーのステータスを選択します。次のいずれかを設定できます。 • [有効（Enabled）]：このポリシー条件はアクティブです。 • [無効（Disabled）]：このポリシー条件は非アクティブであり、評価されません。 • [モニターのみ（Monitor Only）]：このポリシー条件は評価されますが、結果は実施されません。[ライブ ログ認証（Live Log authentication）] ページでこのポリシー条件の結果を照会できます。ここでは、モニターされる手順と属性を含む詳細レポートを参照してください。たとえば、新しいポリシー条件を追加する場合に、条件がもたらす結果が正しいかどうかを判断できないことがあります。この場合、モニター モードでポリシー条件を作成して、結果を確認できます。結果に問題がない場合はそのポリシー条件を有効化できます。
ルール名	このポリシーの一意の名前を入力します。
条件（Conditions）	新しいポリシー行から、プラス（+）アイコンをクリックするか、既存のポリシー行から [編集（Edit）] アイコンをクリックして [条件スタジオ（Conditions Studio）] を開きます。

フィールド名	使用上のガイドライン
結果またはプロファイル（**Results or Profiles**）	関連する許可プロファイルを選択します。これにより、構成されたセキュリティ グループに提供される権限のそれぞれのレベルが決まります。関連する許可プロファイルをまだ設定していない場合は、インラインで行うことができます。
結果またはセキュリティグループ（**Results or Security Groups**）	関連するセキュリティグループを選択します。これにより、特定のルールに関連するユーザーのグループが決まります。関連するセキュリティ グループをまだ設定していない場合は、インラインで行うことができます。
結果またはコマンドセット（**Results or Command Sets**）	コマンド セットは、デバイス管理者が実行できるコマンドの指定されたリストを適用します。デバイス管理者がネットワーク デバイスに対して操作コマンドを発行すると、その管理者がこれらのコマンドの発行を認可されているかどうかを判定する問い合わせが ISE に行われます。これは、コマンド認可とも呼ばれます。
結果またはシェルプロファイル（**Results or Shell Profiles**）	TACACS+ シェル プロファイルは、デバイス管理者の最初のログイン セッションを制御します。
ヒット数（**Hits**）	ヒット数は、条件が一致した回数を示す診断ツールです。

フィールド名	使用上のガイドライン
アクション（**Actions**）	さまざまなアクションを表示して選択するには、[アクション（Actions）] 列の歯車アイコン をクリックします。 • [上に新しい行を挿入（Insert new row above）] : [アクション（Actions）] メニューを開いたルールの上に新しい許可ルールを挿入します。 • [下に新しい行を挿入（Insert new row below）] : [アクション（Actions）] メニューを開いたルールの下に新しい許可ルールを挿入します。 • [上に複製（Duplicate above）] : 元のセットの上に、[アクション（Actions）] メニューを開いたルールの上に複製許可ルールを挿入します。 • [下に複製（Duplicate below）] : 元のセットの下に、[アクション（Actions）] メニューを開いたルールの下に複製許可ルールを挿入します。 • [削除（Delete）] : ルールを削除します。

許可プロファイルの設定

[許可プロファイル（Authorization Profiles）] ウィンドウの次のフィールドで、ネットワークアクセスの属性を定義します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]**> **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[認証プロファイル（Authorization Profiles）]** です。

Note シスコ以外のデバイスで Cisco ISE 2.x リリースから Cisco ISE 3.x リリースにアップグレードする場合、認証プロファイルに ACL 値が設定されたネットワーク デバイス プロファイルが含まれていると、アップグレードが失敗する可能性があります。これは、ネットワーク デバイス プロファイルに ACL が設定されるようになっていないためです。

この問題を回避するには、値を手動で削除するか、該当する認証プロファイル自体を削除します。

許可プロファイルの設定

- [名前（Name）]：この新しい認証プロファイルの名前を入力します。
- [説明（Description）]：許可プロファイルの説明を入力します。
- [アクセスタイプ（Access Type）]：アクセスタイプ（[ACCESS_ACCEPT] または [ACCESS_REJECT]）を選択します。
- [サービステンプレート（Service Template）]：SAnet 対応デバイスとのセッションをサポートするには、このオプションを有効にします。Cisco ISE は、許可プロファイルを「サービステンプレート」互換としてマークする特別なフラグを使用して、許可プロファイルにサービステンプレートを実装します。サービステンプレートは許可プロファイルでもあるため、SAnet デバイスと非 SAnet デバイスの両方をサポートする単一のポリシーとして機能します。
- [移動の追跡（Track Movement）]：Cisco Mobility Services Engine（MSE）を使用してユーザーの場所を追跡するには、このオプションを有効にします。

Note このオプションは、Cisco ISE のパフォーマンスに影響を与える可能性があります。これは、セキュリティレベルの高い場所を対象としています。

- [Passive Identity トラッキング（Passive Identity Tracking）]：ポリシーの適用とユーザートラッキングのために Passive Identity の Easy Connect 機能を使用するには、このオプションを有効にします。

一般的なタスク

一般的なタスクは、ネットワークアクセスに適用される特定の権限とアクションです。

- [DACL名（DACL Name）]：ダウンロード可能な ACL を使用するには、このオプションを有効にします。デフォルト値（**PERMIT_ALL_IPV4_TRAFFIC** 、**PERMIT_ALL_IPV6_TRAFFIC** 、**DENY_ALL_IPV4_TRAFFIC**、**DENY_ALL_IPV6_TRAFFIC**）を使用するか、次のディクショナリから属性を選択することができます。
  - 外部 ID ストア（属性）（External identity store (attributes)）
  - エンドポイント
  - 内部ユーザー
  - 内部エンドポイント

  DACL の追加、または既存の DACL の編集および管理の詳細については、ダウンロード可能 ACL, on page 18を参照してください。

- [セキュリティグループ（Security group）]：認証の一部としてセキュリティグループ（SGT）を割り当てるには、このオプションを有効にします。
  - Cisco ISE が Cisco DNA Center と統合されていない場合、Cisco ISE は VLAN ID 1 を割り当てます。
  - Cisco ISE が Cisco DNA Center と統合されている場合は、Cisco DNA Center が Cisco ISE と共有する仮想ネットワーク（VN）を選択し、[データタイプ（Data Type）] とサブネット/アドレスプールを選択します。

  セキュリティグループタスクには、セキュリティグループとオプションの VN が含まれています。セキュリティグループを設定する場合、別個に VLAN を設定することはできません。エンドポイントデバイスは、1 つの仮想ネットワークにのみ割り当てることができます。
- [VLAN]：仮想LAN（VLAN）IDを指定するには、このオプションを有効にします。VLAN ID には、整数または文字列値を入力できます。このエントリの形式は、Tunnel-Private-Group-ID:VLANnumber です。
- [音声ドメイン権限（Voice Domain Permission）]：ダウンロード可能な ACL を使用するには、このオプションを有効にします。`cisco-av-pair` のベンダー固有属性（VSA）を `device-traffic-class=voice` の値と関連付けます。複数ドメインの許可モードでは、ネットワークスイッチがこの VSA を受信した場合、エンドポイントは、許可後に音声ドメインに接続されます。
- [Webリダイレクション（CWA、DRW、MDM、NSP、CPP）（Web Redirection（CWA, DRW, MDM, NSP, CPP））]：認証後に Web リダイレクションを有効にするには、このオプションを有効にします。
  - リダイレクションのタイプを選択します。選択した Web リダイレクションのタイプには、次で説明する追加のオプションが表示されます。
  - Cisco ISE が NAD に送信するリダイレクションをサポートするための ACL を入力します。

    NAD に送信するために入力する ACL は、cisco-av ペアとして [属性の詳細（Attributes Details）] ペインに表示されます。たとえば、**acl119** と入力した場合、これは [属性の詳細（Attributes Details）] ペインには `cisco-av-pair = url-redirect-acl = acl119` と表示されます。
  - 選択した Web リダイレクションタイプのその他の設定を選択します。

  次のタイプの Web リダイレクションのいずれかを選択します。
  - [中央集中Web認証（Centralized Web Auth）]：[値（Value）] ドロップダウンから選択したポータルにリダイレクトします。
  - [クライアント プロビジョニング（ポスチャ）（Client Provisioning (Posture)）]：クライアントでポスチャを有効にするため、[値（Value）] ドロップダウンから選択したクライアント プロビジョニング ポータルにリダイレクトします。

- [ホットスポット: リダイレクト（Hot Spot: Redirect）]：[値（Value）] ドロップダウンから選択したホットスポットポータルにリダイレクトします。
- [MDM リダイレクト（MDM Redirect）]：指定した MDM サーバーの MDM ポータルにリダイレクトします。
- [ネイティブサプリカントのプロビジョニング（Native Supplicant Provisioning）]：[値（Value）] ドロップダウンから選択した BYOD にリダイレクトします。

Web リダイレクションタイプを選択し、必要なパラメータを入力したら、次のオプションを設定します。

- [証明書更新メッセージの表示（Display Certificates Renewal Message）]：証明書更新メッセージを表示するには、このオプションを有効にしますurl-redirect 属性値が変更され、この値に証明書が有効である日数が含まれます。このオプションは、中央集中型 Web 認証のみに使用できます。
- [スタティックIP/ホスト名/FQDN（Static IP/Host Name/FQDN）]：ユーザーを別の PSN にリダイレクトするには、このオプションを有効にします。ターゲットIPアドレス、ホスト名、またはFQDNを入力します。このオプションを設定しない場合、ユーザーはこの要求を受信したポリシーサービスノードの FQDN にリダイレクトされます。
- [論理プロファイルでエンドポイントのプロファイラCoAを抑制する（Suppress Profiler CoA for endpoints in Logical Profile）]：特定のタイプのエンドポイントデバイスのリダイレクトをキャンセルするには、このオプションを有効にします。

- [自動スマートポート（Auto smartport）]：自動スマートポート機能を使用するには、このオプションを有効にします。イベント名を入力します。これにより、この値を持つ VSA の cisco-av-pair が `auto-smart-port=event_name` として作成されます。この値は、[属性詳細（Attributes Details）] ペインに表示されます。
- [アクセスの脆弱性（Access Vulnerabilities）]：このオプションを有効にすると、このエンドポイントでの脅威中心型 NAC 脆弱性評価を許可の一環として実行できます。アダプタを選択し、スキャンを実行するタイミングを選択します。
- [再認証（Reauthentication）]：再認証中にエンドポイントを接続したままにするには、このオプションを有効にします。 [RADIUS要求（RADIUS-Request）]（1）を使用することを選択して、再認証中に接続を維持することを選択します。 デフォルトの [RADIUS要求（RADIUS-Request）]（0）では、既存のセッションを切断します。非アクティビティタイマーを設定することもできます。
- [MACSec ポリシー（MACSec Policy）]：MACSec 対応クライアントが Cisco ISE に接続するたびにMACSec暗号化ポリシーを使用するには、このオプションを有効にします。次のオプションのいずれかを選択します。[must-secure]、[should-secure]、または [must-not-secure]。 設定は [属性詳細（Attributes Details）] ペインに `cisco-av-pair = linksec-policy=must-secure` と表示されます。
- [NEAT]：ネットワーク間の ID 認識を拡張するネットワーク エッジ アクセス トポロジ（NEAT）を使用するには、このオプションを有効にします。このチェックボックスをオ

ンにすると、[属性の詳細（Attributes Details）] ペインに、`cisco-av-pair = device-traffic-class=switch` と表示されます。

- [Web認証（ローカルWeb認証）（Web Authentication（Local Web Auth））]：この許可プロファイルのローカル Web 認証を使用するには、このオプションを有効にします。この値では、Cisco ISE が DACL とともに VSA を送信することによって Web 認証の許可をスイッチが認識できます。VSA は `cisco-av-pair = priv-lvl=15` で、これは [属性の詳細（Attributes Details）] ペインに表示されます。
- [Airespace ACL名（Airespace ACL Name）]：Cisco Airespace ワイヤレスコントローラに ACL 名を送信するには、このオプションを有効にします。Airespace VSA はこの ACL を使用して、ローカルで定義された WLC 上の接続への ACL を許可します。たとえば、**rsa-1188** と入力した場合、これは [属性の詳細（Attributes Details）] ペインに `Airespace-ACL-Name = rsa-1188` と表示されます。
- [ASA VPN]：適応型セキュリティアプライアンス（ASA）VPN グループポリシーを割り当てるには、このオプションを有効にします。ドロップダウンリストから、VPN グループポリシーを選択します。
- [AVCプロファイル名（AVC Profile Name）]：このエンドポイントでアプリケーションの可視性を実行するには、このオプションを有効にします。使用する AVC プロファイルを入力します。
- [UPNルックアップ（UPN Lookup）]：未定

高度な属性設定（Advanced Attributes Settings）

- [ディクショナリ（Dictionaries）]：下矢印アイコンをクリックし、[ディクショナリ（Dictionaries）] ウィンドウに選択可能なオプションを表示します。最初のフィールドで設定する必要があるディクショナリと属性を選択します。
- [属性値（Attribute Values）]：下矢印アイコンをクリックし、[属性値（Attribute Values）] ウィンドウに選択可能なオプションを表示します。目的の属性グループと属性値を選択します。この値は、最初のフィールドで選択した値と一致します。設定する [高度な属性（Advanced Attributes）] が [属性の詳細（Attribute Details）] パネルに表示されます。
- [属性の詳細（Attributes Details）]：このペインには、[共通タスク（Common Tasks）] および [高度な属性（Advanced Attributes）] に設定した設定済みの属性値が表示されます。

  [属性の詳細（Attributes Details）] ペインに表示される値は読み取り専用です。

Note [属性の詳細（Attributes Details）] ペインに表示される読み取り専用の値を変更または削除するには、対応する [共通タスク（Common Tasks）] フィールド、または [高度な属性設定（Advanced Attributes Settings）] ペインの [属性値（Attribute Values）] で選択した属性でこれらの値を変更または削除します。

Related Topics

Cisco ISE の許可プロファイル （14 ページ）
許可プロファイルの権限 （15 ページ）
未登録のデバイスのリダイレクトのための許可プロファイルの設定
許可プロファイルの作成

許可ポリシーの例外

各ポリシー セット内では、通常の許可ポリシーの他に、ローカルの例外ルール（各ポリシー セットの [Set] ビューの [Authorization Policy Local Exceptions] パートから定義される）およびグローバル例外ルール（各ポリシー セットの [Set] ビューの [Authorization Policy Global Exceptions] パートから定義される）も定義できます。

グローバル許可例外ポリシーを使用すると、すべてのポリシー セット内のすべての許可ルールを上書きするルールを定義できます。グローバル許可例外ポリシーを設定すると、すべてのポリシー セットに追加されます。グローバル許可例外ポリシーは、現在設定されているポリシー セットのいずれかから更新できます。グローバル許可例外ポリシーを更新するたびに、それらの更新がすべてのポリシー セットに適用されます。

ローカル許可例外ルールは、グローバル例外ルールを上書きします。許可ルールは、許可ポリシーのローカル例外規則、グローバル例外規則、通常ルールの順番で処理されます。

認証例外ポリシールールは、認証ポリシールールと同じように設定されます。認証ポリシーについては、許可ポリシーの設定 （21 ページ）を参照してください。

（注） Cisco ISE では、認証ポリシーで % 文字を使用してセキュリティ問題を回避することはサポートできません。

ローカル例外およびグローバル例外の構成時の設定

ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。[ポリシーセット（Policy Sets）] ウィンドウから、**[表示（View）]** > **[ローカル例外ポリシー（Local Exceptions Policy）]** または [グローバル例外ポリシー（Global Exceptions Policy）] を選択します。929

許可例外設定は、許可ポリシー設定と同じで、許可ポリシーの設定 （25 ページ） で説明されています。

ポリシー条件

Cisco ISE はルールベースのポリシーを使用してネットワーク アクセスを提供します。ポリシーは、ルールが条件で構成されているルールと結果のセットです。Cisco ISE では、個々のポリシー要素として条件を作成し、システム ライブラリに保存してから、[条件スタジオ（Conditions Studio）] の他のルールベースのポリシーに再利用することができます。

条件では演算子（等しい、等しくない、より大きい、など）と値を使用し、必要に応じて単純にすることも、複雑にすることもできます。また、複数の属性、演算子、複雑な階層を含めることもできます。実行時に、Cisco ISE はポリシー条件を評価し、ポリシー評価が true または false 値のどちらを返すかに応じて、定義された結果を適用します。

条件を作成して一意の名前を割り当てた後、この条件を [条件スタジオ ライブラリ（Conditions Studio Library）] から選択することで、さまざまなルールとポリシーにわたって複数回再利用することができます。例を次に示します。

```
Network Conditions.MyNetworkCondition EQUALS true
```

ポリシーで使用されているか、または別の条件の一部である条件は [条件スタジオ（Conditions Studio）] から削除できません。

各条件は、オブジェクトのリストを定義します。このリストはポリシー条件に含めることができ、これにより、要求で示される定義と照合される定義セットになります。

演算子 `EQUALS true` を使用して、ネットワーク条件が true であるかどうか（要求に指定されている値がネットワーク条件の 1 つ以上のエントリと一致しているかどうか）を確認するか、または`EQUALS false` を使用して、ネットワーク条件が false であるかどうか（ネットワーク条件のどのエントリとも一致しないかどうか）を確認することができます。

Cisco ISE には、事前定義されたスマート条件も用意されています。この条件は、ポリシーで個別に使用したり、独自のカスタマイズされた条件で構成要素として使用でき、必要に応じて更新および変更できます。

次の固有のネットワーク条件を作成してネットワークへのアクセスを制限することができます。

- エンドステーション ネットワーク条件（Endstation Network Conditions）：接続が開始および終了されるエンドステーションに基づきます。

  Cisco ISE はリモート アドレスの [TO] フィールド（TACACS+ 要求または RADIUS 要求であるかに基づいて取得）を評価し、これがエンドポイントの IP アドレス、MAC アドレス、発信側回線 ID（CLI）、または着信番号識別サービス（DNIS）のいずれであるかを確認します。

  RADIUS 要求では、この ID は属性 31（Calling-Station-Id）で使用できます。

  TACACS+ 要求では、リモート アドレスにスラッシュ（/）が含まれている場合、スラッシュより前の部分は [FROM] の値として見なされ、スラッシュより後の部分は [TO] 値として見なされます。たとえば、要求に CLI/DNIS と指定されている場合、CLI は [FROM] の値と見なされ、DNIS は [TO] の値と見なされます。スラッシュが含まれていない場合

は、リモート アドレス全体が [FROM] の値として見なされます（IP アドレス、MAC アドレス、CLI いずれの場合でも）。

- デバイス ネットワーク条件（Device Network Conditions）：要求を処理する AAA クライアントに基づきます。

  ネットワーク デバイスは、IP アドレス、ネットワーク デバイス リポジトリで定義されているデバイス名、またはネットワーク デバイス グループによって識別されます。

  RADIUS 要求では、属性 4（NAS-IP-Address）が指定されている場合、Cisco ISE はこの属性から IP アドレスを取得します。属性 32（NAS-Identifier）が存在する場合、Cisco ISE は属性 32 から IP アドレスを取得します。これらの属性が存在しない場合は、受信したパケットから IP アドレスを取得します。

  デバイスディクショナリ（NDGディクショナリ）にはネットワーク デバイス グループ属性（Location、Device Type、または NDG を表すその他の動的に作成された属性など）が含まれています。これらの属性には、現在のデバイスに関連するグループが含まれています。

- [デバイス ポート ネットワーク条件（Device Port Network Conditions）]：デバイスの IP アドレス、名前、NDG、およびポート（エンドポイントが接続しているデバイスの物理ポート）に基づきます。

  RADIUS 要求では、属性 5（NAS-Port）が要求内に存在する場合、Cisco ISE はこの属性から値を取得します。属性 87（NAS-Port-Id）が要求内に存在する場合、Cisco ISE は属性 87 から要求を取得します。

  TACACS+ 要求では、Cisco ISE はその ID を（すべてのフェーズの）開始要求のポート フィールドから取得します。

これらの固有条件の詳細については、特別なネットワーク アクセス条件 （55 ページ） を参照してください。

ディクショナリおよびディクショナリ属性

ディクショナリは、ドメインのアクセス ポリシーの定義に使用できる属性と許容値のドメイン固有カタログです。個々のディクショナリは、属性タイプの同種の集合です。ディクショナリで定義された属性は同じ属性タイプを持ち、タイプは特定の属性のソースまたはコンテキストを示します。

属性タイプは次のいずれかになります。

- MSG_ATTR
- ENTITY_ATTR
- PIP_ATTR

属性と許容値に加えて、ディクショナリには名前と説明、データ型、デフォルト値などの属性に関する情報が含まれます。属性は、次のいずれかのデータ型となります。BOOLEAN、FLOAT、INTEGER、IPv4、IPv6、OCTET_STRING、STRING、UNIT32、および UNIT64。

Cisco ISE ではインストール中にシステム ディクショナリが作成され、ユーザー ディクショナリを作成できます。

属性は、異なるシステム ディクショナリに格納されます。属性を使用して、条件を構成します。属性は、複数の条件で再利用できます。

ポリシー条件を作成するときに、有効な属性を再利用するには、サポートされている属性を含むディクショナリから選択します。たとえば、Cisco ISE は、AuthenticationIdentityStore という属性を提供しています。これは NetworkAccess ディクショナリにあります。この属性は、ユーザーの認証中にアクセスされた最後の ID ソースを識別します。

- 認証中に単一の ID ソースが使用されると、この属性には認証が成功した ID ストアの名前が含まれます。
- 認証中に ID ソース順序を使用する場合、この属性にはアクセスされた最後の ID ソースの名前が含まれます。

AuthenticationStatus 属性を AuthenticationIdentityStore 属性と組み合わせて使用し、ユーザーが正常に認証された ID ソースを識別する条件を定義できます。たとえば、許可ポリシーで LDAP ディレクトリ（LDAP13）を使用してユーザーが認証された条件をチェックするために、次の再利用可能な条件を定義できます。

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

（注） AuthenticationIdentityStore は、条件にデータを入力できるテキストフィールドを表します。このフィールドには、名前を必ず正しく入力またはコピーします。ID ソースの名前が変更された場合は、ID ソースの変更と一致するように、この条件を変更する必要があります。

以前認証されたエンドポイント ID グループに基づく条件を定義するために、Cisco ISE では、エンドポイント ID グループ 802.1X 認証ステータスの間に定義された許可をサポートしています。Cisco ISE では、802.1X 認証を実行するとき、RADIUS 要求の「Calling-Station-ID」フィールドから MAC アドレスを抽出し、この値を使用して、デバイスのエンドポイント ID グループ（endpointIDgroup 属性として定義）のセッション キャッシュを検索して読み込みます。このプロセスによって、許可ポリシー条件の作成に endpointIDgroup 属性を使用できるようになり、ユーザー情報に加えてこの属性を使用して、エンドポイント ID グループ情報に基づく許可ポリシーを定義できます。

エンドポイント ID グループの条件は、[許可ポリシー設定（authorization policy configuration）] ページの [ID グループ（ID Groups）] カラムで定義できます。ユーザー関連情報に基づく条件は、許可ポリシーの [その他の条件（Other Conditions）] のセクションで定義する必要があります。ユーザー情報が内部ユーザー属性に基づいている場合は、内部ユーザー ディクショナリの ID グループ属性を使用します。たとえば、「User Identity Group:Employee:US」のような値を使用して、ID グループに完全な値のパスを入力できます。

ネットワーク アクセス ポリシーでサポートされるディクショナリ

Cisco ISE は、認証ポリシーと許可ポリシーの条件とルールを構築する際に必要なさまざまな属性を含む次のシステム格納ディクショナリをサポートしています。

- システム定義されたディクショナリ
  - CERTIFICATE
  - DEVICE
  - RADIUS
- RADIUS ベンダー ディクショナリ
  - Airespace
  - Cisco
  - Cisco-BBSM
  - Cisco-VPN3000
  - Microsoft
  - Network Access

許可ポリシータイプの場合、条件で設定された検証は、戻される許可プロファイルに従う必要があります。

確認には、通常、ライブラリに追加して他のポリシーで再利用できるユーザー定義名を含む 1 つ以上の条件が含まれます。

以下の項では、条件の設定に使用できるサポートされている属性とディクショナリについて説明します。

ディクショナリによってサポートされる属性

表に、ディクショナリでサポートされる固定属性を示します。これらの属性をポリシー条件内で使用できます。作成する条件のタイプによっては、使用できない属性もあります。

たとえば、認証ポリシー内でアクセス サービスを選択する条件を作成する場合、使用できるネットワーク アクセス属性は、Device IP Address、ISE Host Name、Network Device Name、Protocol、および Use Case のみです。

次の表に示す属性をポリシー条件に使用できます。

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
Device	Device Type（定義済みのネットワーク デバイス グループ）	対応	対応
	Device Location（定義済みのネットワーク デバイス グループ）		
	Other Custom Network Device Group		
	ソフトウェアバージョン（Software Version）		
	モデル名（Model Name）		
RADIUS	すべての属性	対応	対応
Network Access	ISE Host Name	対応	対応
	AuthenticationMethod	非対応	はい
	AuthenticationStatus	非対応	非対応
	CTSDeviceID	非対応	非対応
	Device IP Address（デバイス IP アドレス）	対応	対応
	EapAuthentication（マシンのユーザーの認証時に使用される EAP 方式）	非対応	はい
	EapTunnel（トンネルの確立に使用される EAP 方式）	非対応	はい
	プロトコル	対応	対応
	UseCase	対応	対応
	UserName	非対応	はい
	WasMachineAuthenticated	非対応	非対応

ディクショナリ	属性	許可されるプロトコルのルールおよびプロキシ	ID ルール
証明書	Common Name	非対応	はい
	国（Country）		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	シリアル番号（Serial Number）		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	発行元（Issuer）		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
	Issuer - Street Address		
	Issuer - Domain Component		
	Issuer - User ID		

システム定義のディクショナリとディクショナリ属性

Cisco ISE は、インストール中にシステム ディクショナリを作成します。これは、[システム ディクショナリ（System Dictionaries）] ページで確認できます。システム定義のディクショナリ属性は、読み取り専用の属性です。その特性のため、既存のシステム定義のディクショナリは表示することのみができます。システム定義の値またはシステムディクショナリ内の属性を作成、編集、削除することはできません。

システム定義のディクショナリ属性は、属性の記述名、ドメインによって認識される内部名、および許容値とともに表示されます。

また、Cisco ISE は Internet Engineering Task Force（IETF）で定義され、システム定義のディクショナリにも含まれる IETF RADIUS 属性セット用にディクショナリ デフォルトを作成します。ID を除くすべてのフリー IETF RADIUS 属性フィールドを編集できます。

システム ディクショナリおよびディクショナリ属性の表示

システムディクショナリ内のシステム定義の属性を作成、変更、削除することはできません。システム定義された属性は表示することのみができます。ディクショナリの名前と説明に基づくクイック検索またはユーザー定義の検索ルールに基づく高度な検索を実行できます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）]** を選択します。

ステップ 2 [システム ディクショナリ（System Dictionaries）] ページからシステム ディクショナリを選択して [表示（View）] をクリックします。

ステップ 3 [ディクショナリ属性（Dictionary Attributes）] をクリックします。

ステップ 4 リストからシステム ディクショナリを選択して [表示（View）] をクリックします。

ステップ 5 [システム ディクショナリ（System Dictionaries）] ページに戻るには、[ディクショナリ（Dictionaries）] リンクをクリックします。

ユーザー定義のディクショナリとディクショナリ属性

Cisco ISE では、[ユーザー ディクショナリ（User Dictionary）] ページで作成したユーザー定義ディクショナリが表示されます。システムで作成され、保存された既存のユーザーディクショナリの [ディクショナリ名（Dictionary Name）] または [ディクショナリ タイプ（Dictionary Type）] の値は変更できません。

[ユーザー ディクショナリ（User Dictionaries）] ページでは、次の操作を実行できます。

- ユーザー ディクショナリを編集および削除します。
- 名前および説明に基づいてユーザー ディクショナリを検索します。

- ユーザーディクショナリのユーザー定義のディクショナリ属性を追加、編集、および削除します。
- NMAP スキャン機能を使って、NMAP 拡張ディクショナリの属性を削除します。カスタム ポートが [NMAP スキャン アクション（NMAP Scan Actions）] ページで追加または削除されると、対応するカスタム ポート属性がディクショナリで追加、削除または更新されます。
- ディクショナリ属性の許容値を追加または削除します。

ユーザー定義のディクショナリの作成

ユーザー定義のディクショナリを作成、編集、または削除できます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [ユーザー（User）]** 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 ユーザー ディクショナリの名前、オプションの説明、およびバージョンを入力します。

ステップ 4 [ディクショナリ属性タイプ（Dictionary Attribute Type）] ドロップダウン リストから属性タイプを選択します。

ステップ 5 [Submit] をクリックします。

ユーザー定義のディクショナリ属性の作成

ユーザーディクショナリの、ユーザー定義のディクショナリ属性を追加、編集および削除したり、ディクショナリ属性に使用できる値を追加または削除したりすることができます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [ユーザー（User）]** を選択します。

ステップ 2 [ユーザーディクショナリ（User Dictionaries）] ページからユーザーディクショナリを選択して [編集（Edit）] をクリックします。

ステップ 3 [ディクショナリ属性（Dictionary Attributes）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 ディクショナリ属性の属性名、オプションの説明、および内部名を入力します。

ステップ 6 [データ型（Data Type）] ドロップダウン リストからデータ型を選択します。

ステップ 7 [追加（Add）] をクリックして、[使用できる値（Allowed Values）] テーブルで名前、使用できる値、およびデフォルト ステータスを設定します。

ステップ 8 [Submit] をクリックします。

RADIUS ベンダー ディクショナリ

Cisco ISE では、一連の RADIUS ベンダー ディクショナリを定義したり、それぞれの一連の属性を定義したりできます。リスト内の各ベンダー定義には、ベンダー名、ベンダー ID、および簡単な説明が含まれています。

Cisco ISE では、次の RADIUS ベンダー ディクショナリがデフォルトで提供されます。

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

RADIUSプロトコルは、これらのベンダーディクショナリと、許可プロファイルとポリシー条件で使用できるベンダー固有属性をサポートします。

RADIUS ベンダー ディクショナリの作成

RADIUSベンダーディクショナリを作成、編集、削除、エクスポート、およびインポートすることもできます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [Radius（Radius）] > [Radiusベンダー（Radius 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 RADIUS ベンダーの Internet Assigned Numbers Authority（IANA）で承認されている RADIUS ベンダー ディクショナリの名前、オプションの説明、およびベンダー ID を入力します。

ステップ 4 属性値から取得したバイト数を選択して、[ベンダー属性タイプ フィールド長（Vendor Attribute Type Field Length）] ドロップダウン リストから属性タイプを指定します。有効な値は、1、2、および4です。デフォルト値は 1 です。

ステップ 5 属性値から取得したバイト数を選択して、[ベンダー属性サイズ フィールド長（Vendor Attribute Size Field Length）] ドロップダウン リストから属性長を指定します。有効な値は 0 と 1 です。デフォルト値は 1 です。

ステップ 6 [Submit] をクリックします。

RADIUS ベンダー ディクショナリ属性の作成

CiscoISEがサポートするRADIUSベンダー属性を作成、編集、および削除できます。各RADIUSベンダー属性には、名前、データ型、説明、および方向（要求のみに関連する、応答のみに関連する、または両方に関連するかどうかを指定）が含まれています。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [Radius（Radius）] > [Radiusベンダー（Radius Vendors）]** を選択します。

ステップ 2 RADIUS ベンダーディクショナリ リストから RADIUS ベンダーディクショナリを選択して [編集（Edit）] をクリックします。

ステップ 3 [ディクショナリ属性（Dictionary Attributes）] をクリックし、[追加（Add）] をクリックします。

ステップ 4 RADIUS ベンダー属性の属性名とオプションの説明を入力します。

ステップ 5 [データ型（Data Type）] ドロップダウン リストからデータ型を選択します。

ステップ 6 [MAC オプションの有効化（Enable MAC option）] チェックボックスを選択します。

ステップ 7 RADIUS 要求のみ、RADIUS 応答のみ、またはその両方に適用される方向を [方向（Direction）] ドロップダウン リストから選択します。

ステップ 8 [ID] フィールドにベンダー属性 ID を入力します。

ステップ 9 [タグ付けの許可（Allow Tagging）] チェックボックスをオンにします。

ステップ 10 [プロファイルのこの属性の複数インスタンスを許可する（Allow multiple instances of this attribute in a profile）] チェックボックスをオンにします。

ステップ 11 [追加（Add）] をクリックして、[使用できる値（Allowed Values）] テーブルにベンダー属性の使用できる値を追加します。

ステップ 12 [Submit] をクリックします。

HP RADIUS IETF サービス タイプ属性

Cisco ISE では、RADIUS IETF サービス タイプ属性に 2 つの新しい値が導入されました。RADIUS IETF サービスタイプ属性は、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [RADIUS] > [IETF] で使用できます。ポリシーの条件で次の 2 つの値を使用できます。これら 2 つの値は、特に HP のデバイスがユーザーの権限を理解できるように設計されています。

列挙名	列挙値
HP-Oper	252
HP-User	255

RADIUS ベンダー ディクショナリ属性の設定

ここでは、Cisco ISE で使用される RADIUS ベンダーのディクショナリについて説明します。

次の表に、RADIUS ベンダーのディクショナリ属性を設定できるようにする RADIUS ベンダーの [ディクショナリ（Dictionary）] ウィンドウのフィールドを示します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy ）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [システム（System）] > [RADIUS] > [RADIUS ベンダー（RADIUS Vendors）]** です。

表 *4 : RADIUS* ベンダー ディクショナリ属性の設定

フィールド名	使用上のガイドライン
属性名（**Attribute Name**）	選択した RADIUS ベンダーのベンダー固有属性名を入力します。
説明	ベンダー固有属性のオプションの説明を入力します。
内部名	内部のデータベースで表されるベンダー固有属性の名前を入力します。
データ タイプ	ベンダー固有属性に対して、次のデータ型のいずれかを選択します。 • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4 • IPV6
MAC を有効にするオプション（Enable MAC option）	MACアドレスとしてのRADIUS属性の比較を有効にするには、このチェックボックスをオンにします。デフォルトで、RADIUS 属性 Calling-Station-ID に対して、このオプションは有効とマークされ、無効にできません。RADIUSベンダーディクショナリ内の別のディクショナリ属性（文字列型）の場合は、このオプションを有効または無効にできます。 このオプションを有効にした場合、認証および許可条件の設定中に、テキスト オプションを選択して比較をクリアな文字列にするか、またはMACアドレスオプションを選択して比較をMACアドレスにするかを定義できます。
方向（**Direction**）	RADIUS メッセージに適用するいずれかのオプションを選択します。
ID	ベンダー属性IDを入力します。有効な範囲は 0 ～ 255 です。

フィールド名	使用上のガイドライン
タギングの許可（**Allow Tagging**）	RFC2868 で定義するように、タグを持つことが許可されるものとして属性をマークするには、このチェック ボックスをオンにします。タグの目的は、トンネル化されたユーザーの属性のグループ化を許可することです。詳細については、RFC2868 を参照してください。 タグ付けされた属性のサポートでは、特定のトンネルに関するすべての属性のそれぞれのタグ フィールドに同じ値が含まれ、各セットに Tunnel-Preference 属性の適切に評価されたインスタンスが含まれていることが保証されます。これは、マルチベンダー ネットワーク環境に使用すべきトンネル属性に適合しているため、複数のベンダーで製造されたネットワーク アクセス サーバー（NAS）間の相互運用性の問題を解決します。
プロファイルでこの属性の複数のインスタンスを許可する（**Allow Multiple Instances of this Attribute in a Profile**）	プロファイルでこの RADIUS ベンダー固有属性の複数のインスタンスが必要な場合は、このチェックボックスをオンにします。

関連トピック

システム定義のディクショナリとディクショナリ属性 （39 ページ）
ユーザー定義のディクショナリとディクショナリ属性 （39 ページ）
RADIUS ベンダー ディクショナリ （41 ページ）
RADIUS ベンダー ディクショナリの作成 （41 ページ）

条件スタジオの操作

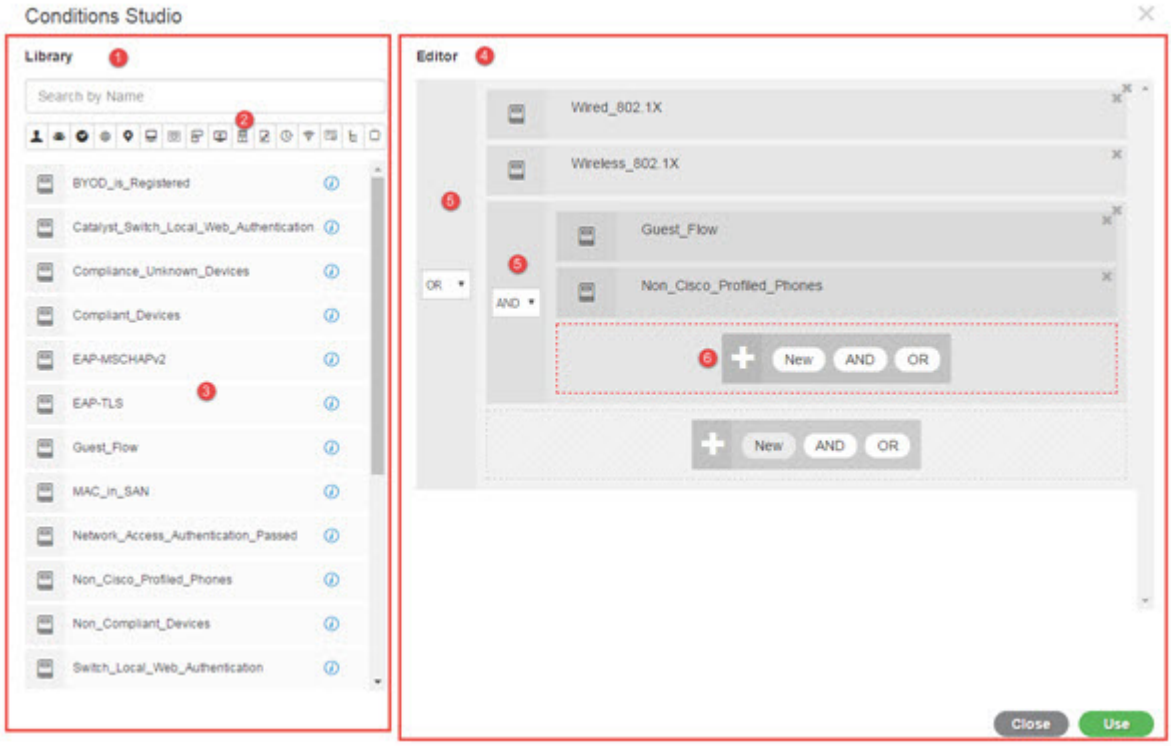
[条件スタジオ（Conditions Studio）]は、条件の作成、管理、および再利用に使用します。条件には複数のルールを含めることができ、1 つのみのレベルまたは複数の階層レベルを含む任意の複雑度で構築できます。[条件スタジオ（Conditions Studio）]を使用して新しい条件を作成する場合は、[ライブラリ（Library）]にすでに保存している条件ブロックを使用することができ、それらの保存された条件ブロックを更新および変更することもできます。後で条件を作成および管理する際に、クイック カテゴリ フィルタなどを使用して、必要なブロックと属性を簡単に見つけることができます。

ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

いずれかのポリシーセットの特定のルールにすでに適用されている条件を編集または変更するには、[条件（Conditions）]列のセルにカーソルを合わせ をクリックするか、または新しい条件を作成するには [ポリシーセット（Policy Set）] テーブルの [条件（Conditions）] 列のプラス記号 をクリックします。その条件は、すぐに同じポリシーセットに適用することができます。または、後で使用するために [ライブラリ（Library）] に保存することもできます。

次の図に、[条件スタジオ（Conditions Studio）] の主な要素を示します。

図 *2 : [条件スタジオ（Conditions Studio）]*



[条件スタジオ（Conditions Studio）] は、[ライブラリ（Library）] と [エディタ（Editor）] の 2 つの主要部分に分かれています。[ライブラリ（Library）] には再使用のために条件ブロックが保存され、[エディタ（Editor）] では保存されたブロックを編集したり新しいブロックを作成できます。

次の表では、[条件スタジオ（Conditions Studio）] のさまざまな部分について説明します。

フィールド	使用上のガイドライン
ライブラリ（Library）	再利用のためにISEデータベースで作成され保存されたすべての条件ブロックのリストを表示します。これらの条件ブロックを現在編集している条件の一部として使用するには、それらを[ライブラリ（Library）]から[エディタ（Editor）]の関連レベルにドラッグアンドドロップし、必要に応じて演算子を更新します。 条件は複数のカテゴリに関連付けることができるため、[ライブラリ（Library）]に保存されている条件はすべて[ライブラリ（Library）] アイコン  で表されます。 また、[ライブラリ（Library）]の各条件の横には、iアイコンがあります。このアイコンの上にカーソルを置くと、条件の完全な説明や、関連付けられているカテゴリが表示され、また、ライブラリから条件を完全に削除できます。ポリシーで使用されている条件は削除できません。 ライブラリ条件のいずれかを[エディタ（Editor）]にドラッグアンドドロップして、現在編集されているポリシーに単独で使用するか、または現在のポリシーで使用されるさらに複雑な条件の構成要素として使用するか、あるいは[ライブラリ（Library）]に新しい条件として保存します。[エディタ（Editor）]に条件をドラッグアンドドロップしてその条件を変更し、[ライブラリ（Library）]に同じ名前または新しい名前で保存することもできます。 インストール時には事前定義された条件もあります。これらの条件は、変更および削除することもできます。

フィールド	使用上のガイドライン
検索およびフィルタ（Search and filter）	名前で条件を検索したり、カテゴリ別にフィルタリングしたりできます。同様に、[エディタ（Editor）]の[クリックして属性を追加する（Click to add an attribute）] フィールドから属性を検索およびフィルタリングすることもできます。ツールバー上のアイコンは、件名や住所などの異なる属性カテゴリを表します。アイコンをクリックすると、特定のカテゴリに関連する属性が表示されます。カテゴリ ツールバーの強調表示されたアイコンをクリックすると、そのカテゴリが選択解除され、フィルタが削除されます。
条件リスト（Conditions List）	[ライブラリ（Library）] 内のすべての条件の完全なリスト、または検索またはフィルタの結果に基づく [ライブラリ（Library）] 内の条件のリスト。
エディタ（Editor）	すぐに使用する新しい条件を作成するだけでなく、今後使用するためにシステム ライブラリに条件を保存したり、既存の条件を編集して、即座に使用したり今後使用するためにその変更を [ライブラリ（Library）] に保存します。 新しい条件を作成するために [条件スタジオ（Conditions Studio）] を開くと（ポリシー セット テーブルのいずれかのプラス記号をクリック）、最初のルールを追加できる空白の行が 1 つだけ表示されます。 [エディタ（Editor）]が空のフィールドとともに表示される場合は、演算子アイコンは表示されません。

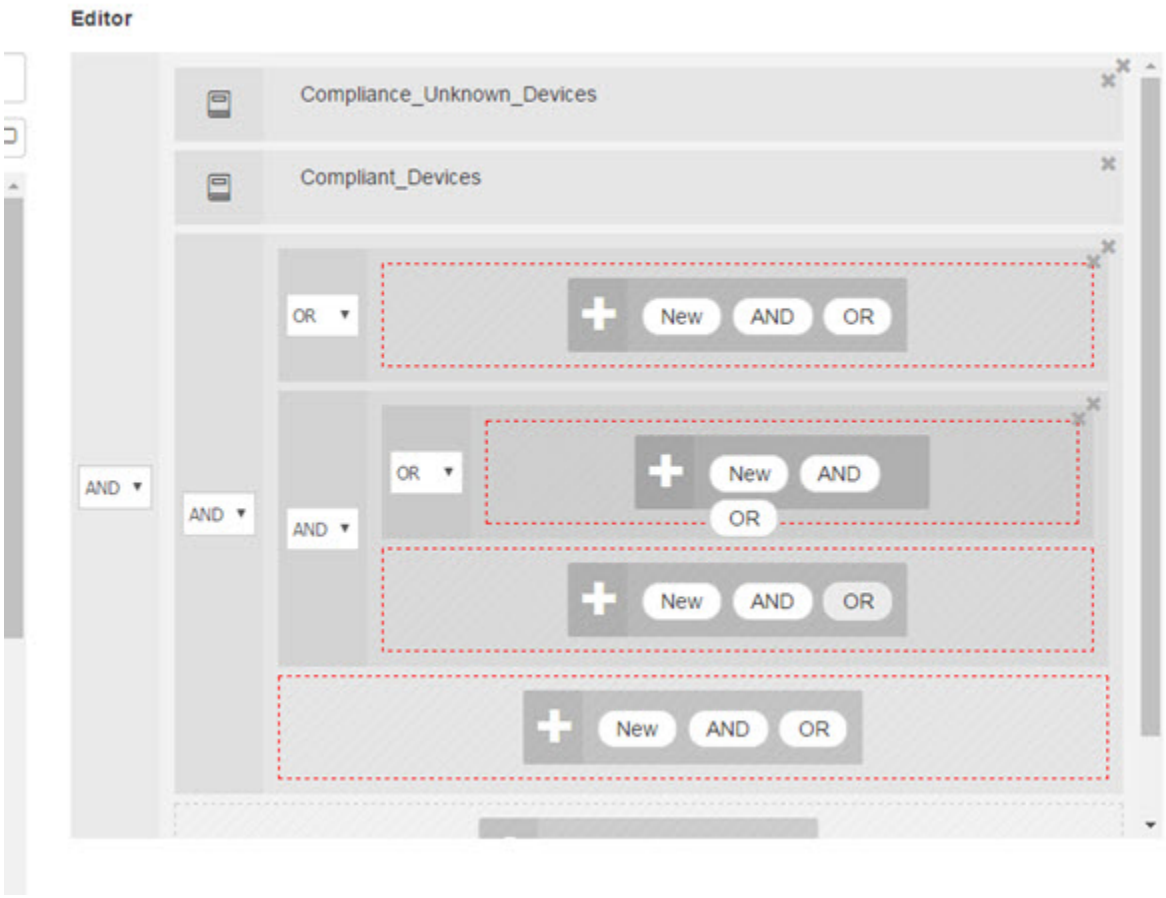
フィールド	使用上のガイドライン
	[エディタ（Editor）]は、さまざまな仮想列と行に分かれています。 列は異なる階層レベルを表し、各列は階層内の位置に基づいてインデントされます。行は個々のルールを表します。レベルごとに 1 つまたは複数のルールを作成し、複数のレベルを含めることができます。 上記のイメージの例は、構築または編集中の条件を示しており、ルールの階層を含んでいます。図の第 1 レベルと第 2 レベルの両方に番号 5 が付けられています。上位親レベルのルールは、演算子 OR を使用します。 演算子を選択して階層レベルを作成した後で演算子を変更するには、この列に表示されているドロップダウンリストから該当するオプションを選択するだけです。 演算子のドロップダウンリストに加えて、各ルールにはこの列に関連するアイコンがあり、そのルールが属するカテゴリが示されています。アイコンの上にカーソルを置くと、ツールチップにカテゴリの名前が示されます。 ライブラリに保存されると、すべての条件ブロックに [ライブラリ（Library）] アイコンが割り当てられ、[エディタ（Editor）] に表示されたカテゴリ アイコンが置き換えられます。 最後に、関連するすべての一致項目を**除外する**ルールが設定されている場合、Is-Not インジケータもこの列に表示されます。たとえば、London という値を持つロケーション属性が Is-Not に設定されている場合、ロンドンからのすべてのデバイスはアクセスが拒否されます。

フィールド	使用上のガイドライン
	この領域には、階層レベルで作業するときに使用できるオプションと、条件内の複数のルールが表示されます。 任意の列または行にカーソルを置くと、関連するアクションが表示されます。アクションを選択すると、そのアクションがそのセクションとすべての子セクションに適用されます。たとえば、階層 A の 5 つのレベルで、第 3 レベルの任意のルールから AND を選択すると、元のルールの下に新しい階層 B が作成され、元のルールが階層 B の親ルールになるように階層 A に埋め込まれます。 新しい条件を最初から作成するために [条件スタジオ（Condition Studio）] を最初に開くと、[エディタ（Editor）] 領域には、設定可能な単一ルールの 1 行のみと、関連する演算子を選択するオプション、または関連条件を [ライブラリ（Library）] からドラッグ アンド ドロップするオプションが含まれています。 **AND** および **OR** 演算子オプションを使用して、条件にレベルを追加できます。オプションをクリックしたときと同じレベルで新しいルールを作成するには、[新規（New）] を選択します。[新規（New）] オプションは、階層の最上位レベルに少なくとも 1 つのルールを設定した場合にのみ表示されます。

ポリシー条件の設定、編集および管理

[条件スタジオ（Conditions Studio）] は、条件の作成、管理、および再利用に使用します。条件には複数のルールを含めることができ、1 つのみのレベルまたは複数の階層レベルを含む任意の複雑度で構築できます。次の図のように、[条件スタジオ（Conditions Studio）] の [エディタ（Editor）] 側から条件階層を管理します。

図 *3 : [*エディタ（***Editor***）*]* : 条件階層



新しい条件を作成する場合は、[ライブラリ（Library）]にすでに保存している条件ブロックを使用することができ、それらの保存された条件ブロックを更新および変更することもできます。条件を作成および管理する際に、クイック カテゴリ フィルタなどを使用して、必要なブロックと属性を簡単に見つけることができます。

条件ルールを作成および管理する場合は、属性、演算子、および値を使用します。

Cisco ISE には、最も一般的な使用例の一部に関する事前定義された条件ブロックも含まれています。これらの事前定義された条件を要件に合わせて編集できます。設定済みブロックを含む、再使用のために保存された条件は、このタスクで説明するように、[条件スタジオ（Conditions Studio）] の [ライブラリ（Library）] に保存されます。

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 [ポリシーセット（Policy Sets）]領域にアクセスします。**[ポリシー（Policy）]** > **[ポリシーセット（Policy Sets）]** を選択します。

ステップ 2 [条件スタジオ（Conditions Studio）] にアクセスして新しい条件を作成したり、既存の条件ブロックを編集して、特定のポリシー セット（および関連するポリシーとルール）のために設定したルールの一部としてそれらの条件を使用したり、今後使用するために [ライブラリ（Library）] に保存します。

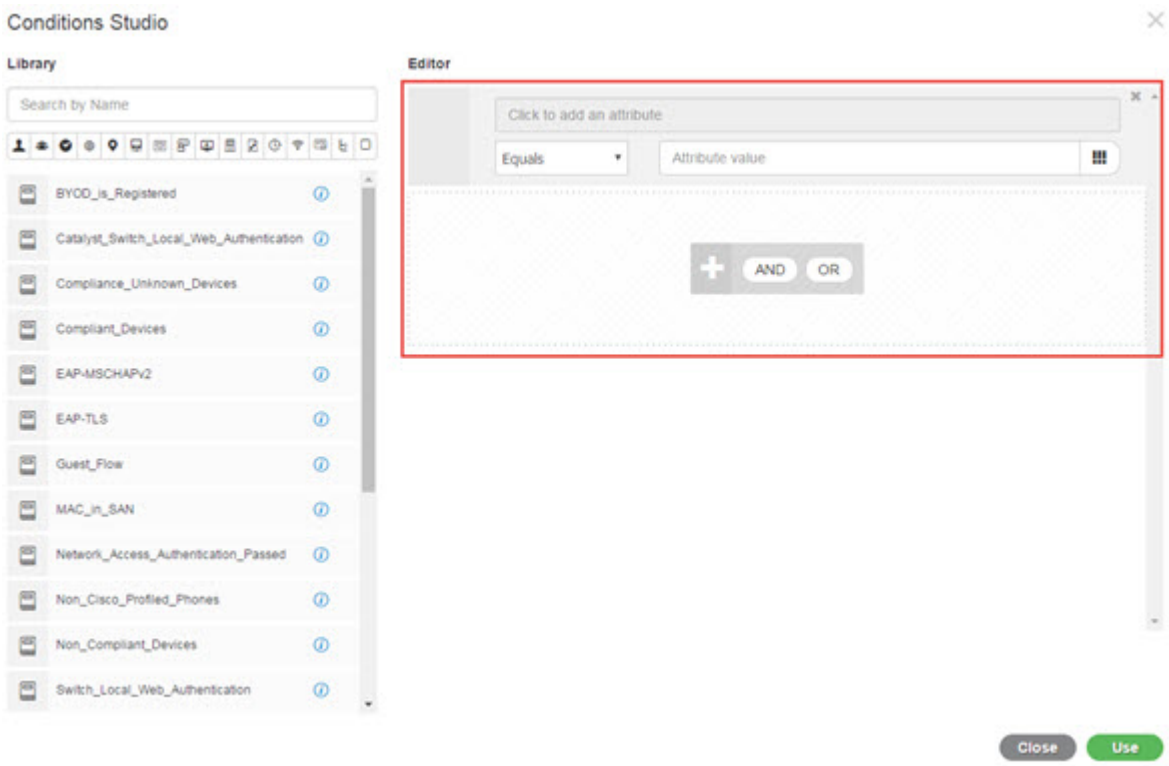
a) ポリシー セット全体（認証ポリシー ルールに照合する前にチェックされる条件）に関連する条件を作成するには、メインの [ポリシー セット（Policy Set）] ページで [ポリシー セット（Policy Set）] テーブルの [条件（Conditions）] 列から ✚ をクリックします。

b) または、認証および許可のすべてのルールを含む [設定（Set）] ビューを表示するには、特定のポリシー セットの行から › をクリックします。[設定（Set）] ビューから、ルールの表のいずれかの [条件（Conditions）] 列のセルにカーソルを合わせ、✚ をクリックして [条件スタジオ（Conditions Studio）] を開きます。

c) すでにポリシー セットに適用されている条件を編集する場合は、✎ をクリックして [条件スタジオ（Conditions Studio）] にアクセスします。

[条件スタジオ（Conditions Studio）] が開きます。新しい条件を作成するために開いた場合は、次の画像のように表示されます。フィールドの説明と、ポリシー セットに既に適用されている条件を編集するために開いた場合の [条件スタジオ（Conditions Studio）] の例を参照するには、条件スタジオの操作 （44 ページ） を参照してください。

図 4 : [条件スタジオ（*Conditions Studio*）] : 新しい条件の作成



ステップ 3 [ライブラリ（Library）] からの既存の条件ブロックを、作成または編集している条件のルールとして使用します。

a) [ライブラリ（Library）] のカテゴリ ツールバーから関連するカテゴリを選択してフィルタリングすると、選択したカテゴリの属性を含むすべてのブロックが表示されます。複数のルールを含むが、それらのルールの少なくとも 1 つに対して選択したカテゴリの属性を使用している条件ブロックも表示されます。追加のフィルタが追加されている場合、表示される結果には、特定のフィルタからの条件ブロックのみが含まれ、含まれている他のフィルタも照合されます。たとえば、ツールバーから [ポート（Ports）] カテゴリを選択し、[名前で検索（Search by Name）] フィールドにフリー テキストとして「auth」と入力すると、名前に「auth」が含まれているポートに関連するすべてのブロックが表示されます。カテゴリ ツールバーの強調表示されたアイコンを再度クリックすると選択解除され、そのフィルタが削除されます。

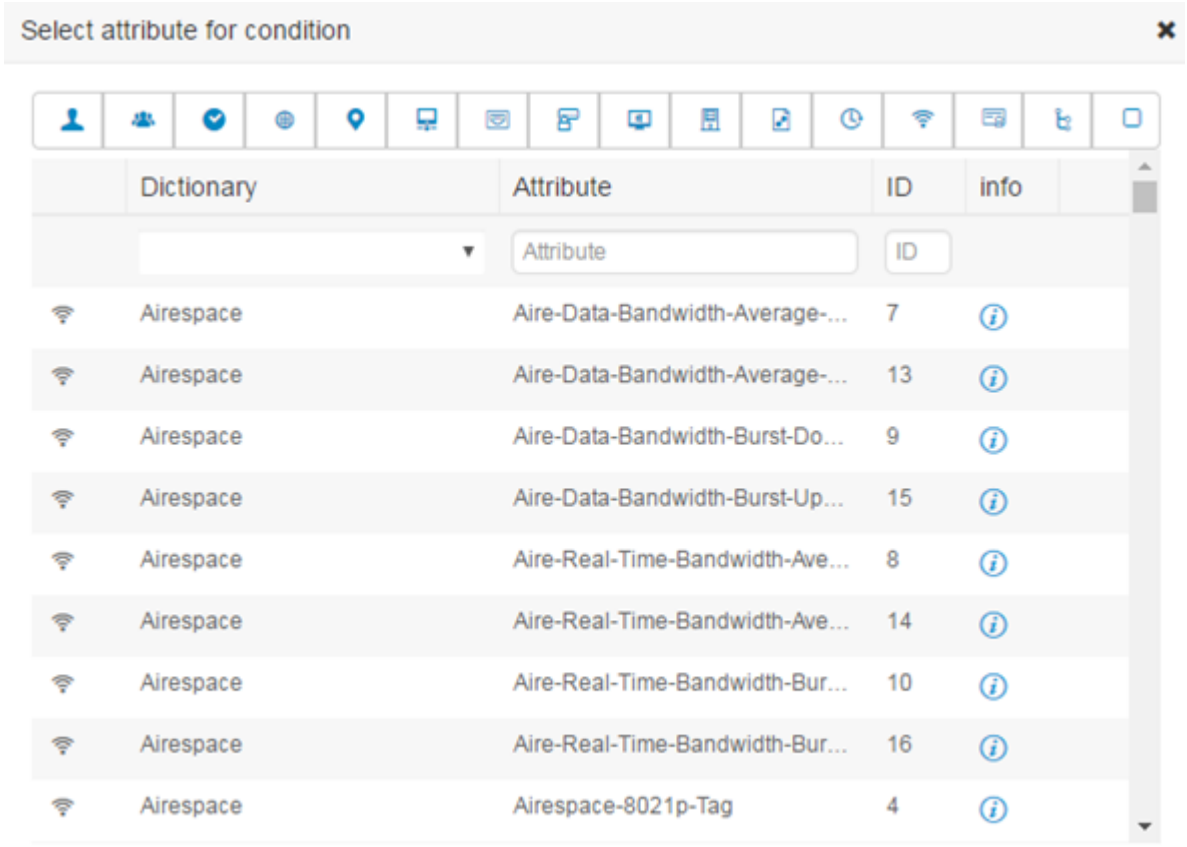
b) フリーテキストで条件ブロックを検索するには、検索しているブロックの名前に表示される [名前で検索（Search by Name）] フリー テキスト フィールドに、任意の用語または用語の一部を入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。カテゴリが選択されていない場合（いずれのアイコンも強調表示されていない場合）、結果にはすべてのカテゴリの条件ブロックが含まれます。カテゴリ アイコンがすでに選択されている場合（表示されているリストがすでにフィルタされている場合）、表示される結果には、特定のテキストを使用する特定のカテゴリのブロックのみが含まれます。

c) 条件ブロックを見つけたら、それを [エディタ（Editor）] にドラッグし、作成しているブロックの正しいレベルにドロップします。間違った場所にドロップした場合は、正しく配置されるまで [エディタ（Editor）] 内から再度ドラッグ アンド ドロップできます。

d) 作業中の条件に関連する変更を加えるには、[エディタ（Editor）] からブロックにカーソルを合わせ、[編集（Edit）] をクリックしてルールを変更し、[ライブラリ（Library）] のルールをその変更で上書きしたり、ルールを新しいブロックとして [ライブラリ（Library）] に保存します。
[エディタ（Editor）] にドロップされたときに読み込み専用であったブロックを編集できるようになりました。そのブロックには、[エディタ（Editor）] 内の他のすべてのカスタマイズされたルールと同じフィールド、構造、リスト、アクションがあります。このルールの編集の詳細については、次の手順に進みます。

ステップ 4 同じレベルでルールを追加するには、現在のレベルに演算子を追加します。[AND]、[OR]、または ['Is not' に設定（Set to 'Is not'）] を選択します。['Is not' に設定（Set to 'Is not'）] は、個々のルールにも適用できます。

ステップ 5 属性ディクショナリを使用してルールを作成および編集するには、[クリックして属性を追加する（Click to add an attribute）] フィールドをクリックします。次の画像のように、属性セレクタが開きます。



属性セレクタの要素を次の表で説明します。

フィールド	使用上のガイドライン
[属性カテゴリ（Attribute Category）] ツールバー	異なる属性カテゴリごとに固有のアイコンが含まれています。カテゴリ別に表示をフィルタ処理するには任意の属性カテゴリ アイコンを選択します。 強調表示されたアイコンをクリックすると選択解除され、フィルタが削除されます。
ディクショナリ	属性が格納されているディクショナリの名前を示します。ベンダー ディクショナリ別に属性をフィルタリングするには、ドロップダウンから特定のディクショナリを選択します。
属性（Attribute）	属性の名前を示します。属性をフィルタリングするには、使用可能なフィールドに属性名のフリー テキストを入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。

フィールド	使用上のガイドライン
ID	一意の属性 ID 番号を示します。属性をフィルタリングするには、使用可能なフィールドに ID 番号を入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。
情報（Info）	属性に関する詳細を表示するには、関連する属性の行にある情報アイコンの上にカーソルを置きます。

a) 属性セレクタ検索で、必要な属性をフィルタリングして検索します。属性セレクタの任意の部分でフリー テキストをフィルタリングまたは入力すると、他のフィルタがアクティブ化されていない場合、結果には選択されたフィルタのみに関連するすべての属性が含まれます。複数のフィルタを使用すると、表示される検索結果はすべてのフィルタに一致します。たとえば、ツールバーの[ポート（Port）] アイコンをクリックし、[属性（Attribute）] 列に「auth」と入力すると、名前に「auth」が含まれる [ポート（Ports）] カテゴリの属性のみが表示されます。カテゴリを選択すると、ツールバーのアイコンが青色で強調表示され、フィルタリングされたリストが表示されます。カテゴリ ツールバーの強調表示されたアイコンを再度クリックすると選択解除され、そのフィルタが削除されます。

b) 関連する属性をルールに追加するには、その属性を選択します。
属性セレクタが閉じ、選択した属性が [クリックして属性を追加する（Click to add an attribute）] フィールドに追加されます。

c) [等しい（Equals）] ドロップダウンリストから、関連する演算子を選択します。

選択するすべての属性に「Equals」、「Not Equals」、「Matches」、「Starts With」、「Not Starts With」の演算子オプションが含まれているわけではありません。

「Matches」演算子は、ワイルドカードなしの正規表現（REGEX）をサポートし、使用します。

単純比較の場合は、「equals」演算子を使用する必要があります。「Contains」演算子は、複数値属性に使用できます。正規表現の比較には、「Matches」演算子を使用する必要があります。「Matches」演算子を使用すると、正規表現は静的値と動的値の両方について解釈されます。

d) [属性値（Attribute value）] フィールドから、次のいずれかを実行します。

- フィールドにフリー テキスト値を入力します。
- リストから動的にロードする値を選択します（関連する場合は、前の手順で選択した属性によって異なります）。
- 条件ルールの値として別の属性を使用します。フィールドの横にあるテーブル アイコンを選択して、属性セレクタを開き、関連する属性を検索、フィルタリング、および選択します。属性セレクタが閉じ、選択した属性が [属性値（Attribute value）] フィールドに追加されます。

ステップ 6 条件ブロックとして [ライブラリ（Library）] にルールを保存します。

a) [ライブラリ（Library）] にブロックとして保存するルールまたはルールの階層の上にマウス カーソルを置きます。[重複（Duplicate）] ボタンと [保存（Save）] ボタンは、単一の条件ブロックとして保存できるルールまたはルールのグループに対して表示されます。ルールのグループをブロックとし

て保存する場合は、階層全体のブロックされた領域内の階層全体の下部からアクション ボタンを選択します。

b) [保存（Save）] をクリックします。[保存（Save）] 条件画面が表示されます。

c) 次のどちらかを選択します。

- [既存のライブラリ条件に保存（Save to Existing Library Condition）] : [ライブラリ（Library）] 内の既存の条件ブロックを作成した新しいルールで上書きし、[リストから選択（Select from list）] ドロップダウンリストから上書きする条件ブロックを選択するには、このオプションを選択します。
- [新しいライブラリ条件として保存（Save as a new Library Condition）] : [条件名（Condition Name）] フィールドにブロックの一意の名前を入力します。

d) 必要に応じて、[説明（Description）] フィールドに説明を入力します。この説明は、[ライブラリ（Library）]内の任意の条件ブロックの情報アイコン上にマウスを置いた場合に表示され、さまざまな条件ブロックとその用途をすばやく識別できます。

e) [保存（Save）] をクリックして、条件ブロックを [ライブラリ（Library）] に保存します。

ステップ 7 新しい子レベルに新しいルールを作成するには、[AND] または [OR] をクリックして、既存の親階層と作成している子階層の間に正しい演算子を適用します。選択した演算子を使用して、演算子を選択したルールまたは階層の子として、エディタ階層に新しいセクションが追加されます。

ステップ 8 現在の既存のレベルで新しいルールを作成するには、該当するレベルから [新規（New）] をクリックします。新しいルールの新しい空の行が、開始したレベルと同じレベルで表示されます。

ステップ 9 [X] をクリックして、[エディタ（Editor）] とそのすべての子から条件を削除します。

ステップ 10 [重複（Duplicate）] をクリックすると、階層内の特定の条件が自動的にコピー アンド ペーストされ、同じレベルで追加の同一の子が作成されます。[重複（Duplicate）]ボタンをクリックしたレベルに応じて、子の有無にかかわらず個々のルールを複製できます。

ステップ 11 ページ下部の [使用（Use）] をクリックして、[エディタ（Editor）] で作成した条件を保存し、その条件をポリシー セットに実装します。

（注） いずれかのポリシーセットで AD 属性が必要な場合は、対応する AD 条件を設定する必要があります。

特別なネットワーク アクセス条件

この項では、ポリシーセットを作成するときに役立つ固有条件について説明します。これらの条件は、[条件スタジオ（Conditions Studio）]から作成することはできず、独自のプロセスがあります。

デバイス ネットワーク条件の設定

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [デバイス ネットワーク条件（Device Network Conditions）] 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 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IP アドレス：IP アドレスまたはサブネットの一覧を、1 行に 1 つ追加できます。IP アドレス/サブネットは IPv4 または Ipv6 形式で指定できます。
- デバイス名（Device Name）：デバイス名の一覧を、1 行に 1 つ追加することができます。ネットワーク デバイス オブジェクトで設定されているものと同じデバイス名を入力する必要があります。
- [デバイス グループ（Device Groups）]：ルート NDG、カンマ、（ルート NDG 配下の）NDG の順でタプル一覧を追加できます。タプルは、1 行に 1 つにする必要があります。

ステップ 5 [Submit] をクリックします。

デバイス ポート ネットワーク条件の設定

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [デバイス ポート ネットワーク条件（Device Port Network Conditions）] 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 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IP アドレス（IP Addresses）：次の順序で詳細を入力します。IP アドレスまたはサブネット、カンマ、（デバイスによって使用される）ポート。タプルは、1 行に 1 つにする必要があります。
- デバイス（Devices）：次の順序で詳細を入力します。デバイス名、カンマ、ポート。タプルは、1 行に 1 つにする必要があります。ネットワーク デバイス オブジェクトで設定されているものと同じデバイス名を入力する必要があります。
- デバイス グループ（Device Groups）：次の順序で詳細を入力します。ルート NDG、カンマ、（ルート下の）NDG、ポート。タプルは、1 行に 1 つにする必要があります。

ステップ 5 [Submit] をクリックします。

エンドステーション ネットワーク条件の設定

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ネットワーク条件（Network Conditions）] > [エンドステーション ネットワーク条件（Endstation Network Conditions）] 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 ネットワーク条件の名前と説明を入力します。

ステップ 4 次の詳細を入力します。

- IP アドレス：IP アドレスまたはサブネットの一覧を、1 行に 1 つ追加できます。IP アドレス/サブネットは IPv4 または Ipv6 形式で指定できます。
- MAC アドレス：カンマ区切りのエンドステーション MAC アドレスと宛先 MAC アドレスの一覧を入力できます。各 MAC アドレスには 12 桁の 16 進数を含め、次の形式のいずれかで指定してください。nn:nn:nn:nn:nn:nn、nn-nn-nn-nn-nn-nn、nnnn.nnnn.nnnn、nnnnnnnnnnnn。

  エンドステーション MAC または宛先 MAC が必要でない場合は、代わりにトークン「-ANY-」を使用します。
- CLI/DNIS：カンマ区切りの発信者 ID（CLI）および受信者 ID（DNIS）の一覧を追加できます。発信者 ID（CLI）または受信者 ID（DNIS）が必要でない場合は、代わりにトークン「-ANY-」を使用します。

ステップ 5 [Submit] をクリックします。

時刻と日付の条件の作成

[ポリシー要素条件（Policy Elements Conditions）] ページを使用して、時刻と日付のポリシー要素条件を表示、作成、変更、削除、複製、および検索します。ポリシー要素は、設定した特定の時刻と日付の属性設定に基づく条件を定義する共有オブジェクトです。

時刻と日付の条件を使用すると、Cisco ISE システム リソースにアクセスする権限を、作成した属性設定で指定された特定の時刻と日付に設定または制限できます。

始める前に

次のタスクを実行するには、スーパー管理者またはポリシー管理者である必要があります。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [共通（Common）] > [時刻と日付（Time and Date）] > [追加（Add）]** を選択します。

ステップ 2 フィールドに適切な値を入力します。

- [標準設定（Standard Settings）] 領域で、アクセスを提供する日時を指定します。

• [例外（Exceptions）] 領域で、アクセスを制限する日時の範囲を指定します。

ステップ 3 [Submit] をクリックします。

許可ポリシーで IPv6 条件属性を使用する

Cisco ISE では、エンドポイントからの IPv6 トラフィックを検出、管理、保護できます。

IPv6 対応エンドポイントが Cisco ISE ネットワークに接続すると、IPv6 ネットワーク経由でネットワーク アクセス デバイス（NAD）と通信します。NAD は、アカウンティングおよびプロファイリングの情報をエンドポイント（IPv6 値を含む）から Cisco ISE に IPv4 ネットワークを介して伝達します。ルール条件で IPv6 属性を使用して、IPv6 対応エンドポイントからのそのような要求を処理し、エンドポイントが準拠していることを保証するための、認証プロファイルおよびポリシーを Cisco ISE で設定できます。

ワイルドカード文字は、IPv6 プレフィックスと IPv6 インターフェイスの値で使用できます。たとえば、2001:db8:1234::/48 です。

サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記：コロンで区切られた 4 つの 16 進数桁の 8 つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。
- 短縮表記：1 つのグループ内にある先行ゼロは除きます。ゼロのグループを 2 つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切りの 4 つの表記（IPv4 対応付けおよび IPv4 互換性 IPv6 アドレス）：たとえば、::ffff:192.0.2.128 です。

サポートされている IPv6 属性は次のとおりです。

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address
- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

サポートされるシスコの属性と値のペアおよび対応する IETF 属性を次の表に示します：

シスコの属性と値のペア	IETF 属性
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

[RADIUS ライブログ（RADIUS Live Logs）] ページ、RADIUS 認証レポート、RADIUS アカウンティングレポート、現在アクティブなセッションレポート、RADIUS エラーレポート、設定が誤っている NAS レポート、適応型ネットワーク制御の監査および設定が誤っているサプリカントレポートは、IPv6 アドレスをサポートしています。[RADIUS ライブログ（RADIUS Live Logs）] ページ、またはこれらのレポートのいずれかから、これらのセッションの詳細を表示できます。IPv4、IPv6、または MAC アドレスでレコードをフィルタリングできます。

（注） IPv6 対応の DHCPv6 ネットワークに Android デバイスを接続すると、そのデバイスは DHCP サーバーからリンクローカルの IPv6 アドレスのみを受信します。したがって、[ライブログ（Live Log）] と [エンドポイント（Endpoints）] ページ（**[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）]**）にはグローバル IPv6 アドレスは表示されません。

次の手順は、許可ポリシーに IPv6 属性を設定する方法を説明します。

始める前に

展開内の NAD が IPv6 による AAA をサポートしていることを確認します。NAD で IPv6 の AAA サポートをイネーブルにする方法については、『**AAA Support for IPv6**』を参照してください。

ステップ 1 ネットワーク アクセス ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[ネットワークアクセス（Network Access）]** > **[ポリシーセット（Policy Sets）]** を選択します。デバイス管理ポリシーの場合は、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** を選択します。

ステップ 2 許可ルールを作成します。

ステップ 3 許可ルールを作成するときは、[条件スタジオ（Conditions Studio）]から条件を作成します。[条件スタジオ（Conditions Studio）] で、RADIUS ディクショナリから、RADIUS IPv6 属性、演算子、および値を選択します。

ステップ 4 [完了（Done）][保存（Save）]をクリックして、許可ルールをポリシー セットに保存します。

ポリシー セット プロトコルの設定

これらのプロトコルを使用してポリシー セットを作成、保存、実装する前に、Cisco ISE でグローバル プロトコル設定を定義する必要があります。[プロトコル設定（Protocol Settings）] ページを使用して、ネットワーク内の他のデバイスと通信する Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）、Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）、および Protected Extensible Authentication Protocol（PEAP）の各プロトコルのグローバル オプションを定義できます。

サポートされているネットワーク アクセス ポリシー セット プロトコル

ネットワーク アクセス ポリシー セット ポリシーの定義時に選択可能なプロトコルを次に示します。

- Password Authentication Protocol（PAP）
- Protected Extensible Authentication Protocol（PEAP）
- Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）
- Extensible Authentication Protocol-Message Digest 5（EAP-MD5）
- Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）
- Extensible Authentication Protocol-Tunneled Transport Layer Security（EAP-TTLS; 拡張認証プロトコル - トンネル方式トランスポート層セキュリティ）
- Protected Extensible Authentication Protocol-Transport Layer Security（PEAP-TLS）

プロトコルとして EAP-FAST を使用するためのガイドライン

EAP-FAST を認証プロトコルとして使用する場合は、次のガイドラインに従ってください。

- EAP-FAST 受信クライアント証明書が認証されたプロビジョニングで有効な場合は、EAP-TLS 内部方式を有効にすることを強く推奨します。認証されたプロビジョニングの EAP-FAST 受信クライアント証明書は別の認証方式ではなく、ユーザーを認証するのと同じ証明書のクレデンシャルのタイプを使用した略式のクライアント証明書認証ですが、内部方式を実行する必要がありません。
- PAC なしの完全なハンドシェイクおよび認定 PAC プロビジョニングとの認証プロビジョニング作業に対するクライアント証明書を受け入れます。PAC なしのセッション再開、匿名 PAC プロビジョニング、PAC ベース認証には動作しません。

- EAP 属性は、認証の順序とは関係なく、ID ごとにモニタリング ツールの認証詳細に、まずユーザー順、次にマシン順に表示されます（したがって EAP チェーニングは 2 回表示されます）。
- EAP-FAST 認可 PAC が使用される場合、ライブ ログに表示される EAP 認証方式は完全認証に使用される認証方式と同じ（PEAP でのように）であり、参照としてではありません。
- EAP チェーン モードでは、トンネル PAC が期限切れになると、ISE がプロビジョニングにフォールバックし、AC 要求ユーザーおよびマシン認可 PAC（マシン許可 PAC）はプロビジョニングできません。後続の PAC ベースの認証通信で AC が要求したときにプロビジョニングされます。
- Cisco ISE がチェーンに、AC がシングル モードに設定されている場合は、AC は IdentityType TLV で ISE に応答しますただし、2 番目の ID 認証は失敗します。この通信から、クライアントのチェーニング実行は適切であるが、現在はシングル モードで構成されていることがわかります。
- Cisco ISE は AD にのみチェーンしている EAP-FAST のマシンとユーザーの両方の属性およびグループをサポートします。LDAP および内部 DB ISE に対しては、最新の ID 属性のみを使用します。

Note High Sierra、Mojave、または Catalina MAC OSX デバイスに EAP-FAST 認証プロトコルを使用すると、「EAP-FAST 暗号化バインドの検証に失敗しました（EAP-FAST cryptobinding verification failed）」というメッセージが表示される場合があります。これらの MAC OSX デバイスに EAP-FAST を使用する代わりに PEAP または EAP-TLS を使用するよう、[許可プロトコル（Allowed Protocols）] ページの [優先EAPプロトコル（Preferred EAP Protocol）] フィールドを設定することをお勧めします。

EAP-FAST の設定

始める前に

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

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-FAST]** > **[EAP-FAST の設定（EAP-FAST Settings）]** を選択します。

ステップ 2 EAP-FAST プロトコルの定義に必要な詳細を入力します。

ステップ 3 以前に生成されたプライマリキーと PAC をすべて失効させるには、[失効（Revoke）] をクリックします。

ステップ 4 EAP-FAST 設定を保存するには、[保存（Save）] をクリックします。

EAP-FAST の PAC の生成

Cisco ISE の [PAC の生成（Generate PAC）] オプションを使用して、EAP-FAST プロトコルのトンネル PAC またはマシン PAC を生成できます。

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）]** を選択します。
ステップ 2 左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。
ステップ 3 **[EAP-FAST] > [PAC の生成（Generate PAC）]** を選択します。
ステップ 4 EAP-FAST プロトコルのマシン PAC を生成する場合に必要な詳細を入力します。
ステップ 5 [PAC の生成（Generate PAC）] をクリックします。

EAP-FAST 設定

表 *5 : EAP-FAST* の設定

フィールド名	使用上のガイドライン
機関識別情報の説明（**Authority Identity Info Description**）	クレデンシャルをクライアントに送信する Cisco ISE ノードを説明したわかりやすい文字列を入力します。クライアントは、この文字列をタイプ、長さ、および値（TLV）の Protected Access Credentials（PAC）情報で認識できます。デフォルト値は、Identity Services Engine です。
マスター キー生成期間（**Master Key Generation Period**）	プライマリキー生成期間を、秒、分、時間、日、または週単位で指定します。値は、1 ～ 2147040000 秒の正の整数である必要があります。デフォルトは 604800 秒で、これは 1 週間と同等です。
すべてのマスター キーおよび PAC の失効（**Revoke all master keys and PACs**）	すべてのプライマリキーと PAC を失効させるには、[失効（Revoke）] をクリックします。
PAC なしセッション再開の有効化（**Enable PAC-less Session Resume**）	PAC ファイルなしで EAP-FAST 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。
PAC なしセッションのタイムアウト（**PAC-less Session Timeout**）	PAC なしセッションの再開がタイムアウトするまでの時間を秒単位で指定します。デフォルトは 7200 秒です。

関連トピック

ポリシー セット プロトコルの設定 （60 ページ）
プロトコルとして EAP-FAST を使用するためのガイドライン （60 ページ）
EAP-FAST の利点 （114 ページ）
EAP-FAST の設定 （61 ページ）

PAC の設定

次の表では、[PAC の生成（Generate PAC）] ウィンドウ上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、EAP-FAST 認証用の Protected Access Credentials を設定します。このページのナビゲーションパスは、このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します。**[管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロトコル（Protocols）]>[EAP-FAST]>[PAC の生成（Generate PAC）]** です。

表 *6 : EAP-FAST* の *PAC* の生成の設定

フィールド名	使用上のガイドライン
トンネル PAC（Tunnel PAC）	トンネル PAC を生成するには、このオプション ボタンをクリックします。
マシン PAC（Machine PAC）	マシン PAC を生成するには、このオプション ボタンをクリックします。
TrustSec PAC	TrustSec PAC を生成するには、このオプション ボタンをクリックします。
ID（Identity）	（トンネル PAC およびマシン PAC 用）EAP-FAST プロトコルによって「内部ユーザー名」として示されるユーザー名またはマシン名を指定します。ID 文字列がそのユーザー名と一致しない場合、認証は失敗します。 これは、適応型セキュリティ アプライアンス（ASA）で定義されているホスト名です。ID 文字列は、ASA ホスト名に一致する必要があります。一致しない場合、ASA は生成された PAC ファイルをインポートできません。 TrustSec PAC を生成する場合、[ID（Identity）] フィールドにより TrustSec ネットワーク デバイスのデバイス ID が指定され、EAP-FAST プロトコルによりイニシエータ ID とともに提供されます。ここに入力した ID 文字列がそのデバイス ID に一致しない場合、認証は失敗します。

フィールド名	使用上のガイドライン
PAC 存続可能時間（PAC Time To Live）	（トンネル PAC およびマシン PAC 用）PAC の有効期限を指定する値を秒単位で入力します。デフォルトは 604800 秒で、これは 1 週間と同等です。この値は、1 ～ 157680000 秒の正の整数である必要があります。TrustSec PAC に対しては、日、週、月、または年単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。
暗号化キー（Encryption Key）	暗号キーを入力します。キーの長さは 8 ～ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。
期限日（Expiration Date）	（TrustSec PAC のみ）有効期限は、PAC 存続可能時間に基づいて計算されます。

関連トピック

ポリシー セット プロトコルの設定 （60 ページ）
プロトコルとして EAP-FAST を使用するためのガイドライン （60 ページ）
EAP-FAST の PAC の生成 （62 ページ）

認証プロトコルとしての EAP-TTLS の使用

EAP-TTLS は、EAP-TLS プロトコルの機能を拡張する 2 フェーズ プロトコルです。フェーズ 1 では、セキュアなトンネルを構築し、フェーズ 2 で使用するセッション キーを導出し、サーバーとクライアント間で属性および内部方式データを安全にトンネリングします。フェーズ 2 中では、トンネリングされた属性を使用して、多数のさまざまなメカニズムを使用する追加認証を実行できます。

Cisco ISE は、次のようなさまざまな TTLS サプリカントから認証を処理できます。

- Windows 上の Network Access Manager（NAM）
- Windows 8.1 ネイティブ サプリカント
- セキュア W2（MultiOS で JoinNow とも呼ばれます）
- MAC OS X ネイティブ サプリカント
- IOS ネイティブ サプリカント
- Android ベースのネイティブ サプリカント
- Linux WPA サプリカント

（注） 暗号化バインドが必要な場合は、内部方式として EAP-FAST を使用する必要があります。

EAP-TLS の設定

始める前に

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

ステップ 1 [管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロトコル（Protocols）]>[EAP-TTLS] を選択します。

ステップ 2 [EAP-TTLS設定（EAP-TTLS Settings）] ページに必要な詳細を入力します。

ステップ 3 [Save] をクリックします。

EAP-TTLS 設定

表 *7 : EAP-TTLS* 設定

フィールド名	使用上のガイドライン
EAP-TTLSセッションの再開を有効にする（Enable EAP-TTLS Session Resume）	このチェックボックスをオンにすると、Cisco ISE はユーザーが EAP-TTLS 認証のフェーズ 2 で正常に認証された場合に限り、EAP-TTLS 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザーが再接続しようとする場合、元の EAP-TTLS セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、EAP-TTLS のパフォーマンスが向上し、AAA サーバーの負荷が軽減されます。 （注） EAP-TTLS セッションが再開されると、内部方式はスキップされます。
EAP-TTLSセッションタイムアウト（EAP-TTLS Session Timeout）	EAP-TTLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。

関連トピック

ポリシー セット プロトコルの設定 （60 ページ）
認証プロトコルとしての EAP-TTLS の使用 （64 ページ）
EAP-TLS の設定 （65 ページ）

EAP-TLS の設定

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [EAP-TLS]** を選択します。

ステップ 2 EAP-TLS プロトコルの定義に必要な詳細を入力します。

ステップ 3 EAP-TLS 設定を保存するには、[保存（Save）] をクリックします。

EAP-TLS 設定

関連トピック

ポリシー セット プロトコルの設定 （60 ページ）
EAP-TLS の設定 （66 ページ）

PEAP の設定

始める前に

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

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

ステップ 2 左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。

ステップ 3 [PEAP] を選択します。

ステップ 4 PEAP プロトコルの定義に必要な詳細を入力します。

ステップ 5 PEAP 設定を保存するには、[保存（Save）] をクリックします。

PEAP 設定

関連トピック

ポリシー セット プロトコルの設定 （60 ページ）
PEAP の設定 （66 ページ）
PEAP の使用の利点 （113 ページ）
PEAP プロトコルでサポートされているサプリカント （113 ページ）
PEAP プロトコルのフロー （113 ページ）

RADIUS の設定

認証に失敗、または認証成功のレポートの繰り返しの抑制に失敗したクライアントを検出するように RADIUS 設定を設定することができます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）]** を選択します。
ステップ 2 [設定（Settings）] ナビゲーション ペインで [プロトコル（Protocols）] をクリックします。
ステップ 3 [RADIUS] を選択します。
ステップ 4 RADIUS 設定の定義に必要な詳細を入力します。
ステップ 5 [保存（Save）] をクリックして、設定を保存します。

RADIUS 設定

[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）] オプションを有効にすると、認証が繰り返し失敗するクライアントは監査ログに出力されず、指定された期間にわたってこれらのクライアントからの要求が自動的に拒否されます。また、認証失敗回数を指定できます。失敗回数がこの回数を超えると、これらのクライアントからの要求は拒否されます。たとえばこの値を 5 に設定すると、クライアント認証が 5 回失敗した場合、指定された期間にわたってそのクライアントから受信する要求はすべて拒否されます。

Note

- エンドポイント認証失敗の原因が誤ったパスワードの入力であり、ユーザータイプが内部ユーザーである場合、エンドポイントは抑制され、拒否モードになります。

  ただし、Active Directory ユーザーの場合に誤ったパスワードが検出された場合、エンドポイントは抑制されますが、拒否モードにはなりません。

- Cisco ISE でのクライアント抑制は、クライアントの発信側ステーション ID に関連付けられた MAC アドレスがある場合にのみ機能します。

Note RADIUS 障害の抑制を設定すると、RADIUS ログの抑制を設定した後も、「5440エンドポイントが EAPセッションを放棄し、新しいセッションを開始しました（5440 Endpoint Abandoned EAP Session and started a new one）」というエラーを受信することがあります。詳細については、次の ISE コミュニティの投稿を参照してください。

https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944

***Table 8: RADIUS* 設定**

フィールド名	使用上のガイドライン
[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）]	
[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）]	同じ理由で繰り返し認証に失敗するクライアントを抑止するには、このチェックボックスをオンにします。これらのクライアントは監査ログに出力されず、また [繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] オプションが有効な場合には、指定された期間にわたってこれらのクライアントからの要求が拒否されます。 **Note** CTS 関連のログは、このオプションが有効になっている場合でも抑制されず、常にライブログに含まれます。
[2 回の失敗を検出する期間（Detect Two Failures Within）]	分単位で時間間隔を入力します。クライアントがこの期間内に同じ理由で 2 回認証に失敗すると、監査ログに出力されず、また [繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] オプションが有効な場合には、指定された期間にわたってこのクライアントからの要求が拒否されます。
[失敗を報告する間隔（Report Failures Once Every）]	報告対象の認証失敗の時間間隔を分単位で入力します。たとえば、この値を 15 分に設定すると、繰り返し認証に失敗するクライアントが 15 分に 1 回だけ監査ログに報告されるため、報告の重複が防止されます。

フィールド名	使用上のガイドライン
[繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）]	認証が繰り返し失敗するクライアントからの RADIUS 要求を自動的に拒否するには、このチェック ボックスをオンにします。Cisco ISE による不要な処理を防ぎ、Denial of Service（DoS）攻撃から防御するには、このオプションを有効にします。
[自動拒否前の失敗回数（Failures Prior to Automatic Rejection）]	認証失敗回数を入力します。認証失敗回数がこの値を超えると、繰り返し失敗するクライアントからの要求は自動的に拒否されます。設定されている期間（[要求を拒否する期間（Continue Rejecting Requests for）] で指定）にわたり、これらのクライアントから受信する要求はすべて自動的に拒否されます。この期間が経過した後では、これらのクライアントからの認証要求が処理されます。
[要求を拒否する期間（Continue Rejecting Requests for）]	繰り返し失敗するクライアントからの要求を拒否する時間間隔を分単位で入力します。
[繰り返し発生するアカウンティング更新を無視する期間（Ignore Repeated Accounting Updates Within）]	この期間内に繰り返し発生するアカウンティング更新は無視されます。
[成功レポートの抑制（Suppress Successful Reports）]	
繰り返される認証成功の抑制（Suppress Repeated Successful Authentications）	直近の 24 時間で、ID、ネットワーク デバイス、および許可のコンテキストに変更がない認証要求成功が繰り返し報告されないようにするには、このチェックボックスをオンにします。
[認証の詳細（Authentications Details）]	
[次よりも長いステップを強調表示（Highlight Steps Longer Than）]	ミリ秒単位で時間間隔を入力します。1つのステップの実行が指定のしきい値を超えると、認証詳細ページでそのステップがクロック アイコンでマークされます。
[高レートなRADIUS要求を検出する（Detect High Rate of RADIUS Requests）]	

フィールド名	使用上のガイドライン
[定常的に高レートなRADIUS要求を検出する（Detect Steady High Rate of Radius Requests）]	[RADIUS要求の期間（Duration of RADIUS requests）]および[RADIUS要求の合計数（Total number of RADIUS requests）]フィールドで指定した上限を超える場合に、高レートなRADIUS 要求負荷のアラームを発生させるには、このチェックボックスをオンにします。
[RADIUS要求の期間（Duration of RADIUS Requests）]	RADIUS のレートを計算するために使用する期間（秒単位）を入力します。デフォルトは60秒です。有効な範囲は20～86400秒です。
[RADIUS要求の合計数（Total Number of RADIUS Requests）]	RADIUS のレートを計算するために使用される要求の上限を入力します。デフォルトの要求数は 72000 です。要求数の有効な範囲は 24000 ～ 103680000 で d す。
RADIUS UDP ポート	
認証ポート（**Authentication Port**）	RADIUS UDP の認証フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1812 とポート 1645 が使用されます。値の範囲は 1024 ～ 65535 です。
アカウンティング ポート（**Accounting Port**）	RADIUS UDP のアカウンティング フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1813 とポート 1646 が使用されます。値の範囲は 1024 ～ 65535 です。 **Note** これらのポートが他のサービスにより使用されていないことを確認します。
RADIUS DTLS	
認証およびアカウンティング ポート（**Authentication and Accounting Port**）	RADIUS DTLS の認証およびアカウンティング フローに使用するポートを指定します。デフォルトでは、ポート 2083 が使用されます。値の範囲は 1024 ～ 65535 です。 **Note** このポートが他のサービスにより使用されていないことを確認します。

フィールド名	使用上のガイドライン
アイドル タイムアウト	パケットがネットワーク デバイスから届かなかったら、TLS セッションを終了する前に、Cisco ISE を待機する時間を秒単位で入力します。デフォルト値は 120 秒です。有効な範囲は 60 ～ 600 秒です。
RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification）	Cisco ISE が DTLS ハンドシェイク中に RADIUS/DTLS クライアントの ID を確認するようにする場合は、このチェックボックスをオンにします。クライアント ID が有効でない場合、Cisco ISE はハンドシェイクに失敗します。デフォルトのネットワーク デバイスが設定されている場合、ID チェックはスキップされます。ID チェックは次の順序で実行されます。 **1.** クライアント証明書にサブジェクト代替名（SAN）属性が含まれている場合： • SAN に DNS 名が含まれている場合、証明書に指定されている DNS 名が Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。 • SAN に IP アドレスが含まれていて（DNS 名が含まれていない場合）、証明書で指定された IP アドレスが Cisco ISE で設定されているすべてのデバイス IP アドレスと比較されます。 **2.** 証明書に SAN が含まれていない場合、サブジェクト CN は Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。不一致の場合、Cisco ISE はハンドシェイクに失敗します。

Related Topics

ポリシー セット プロトコルの設定 （60 ページ）
Cisco ISE の RADIUS プロトコルのサポート （75 ページ）
RADIUS の設定 （67 ページ）

セキュリティ設定の構成

次の手順を実行して、セキュリティ設定を構成します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]** を選択します。

ステップ 2 [セキュリティ設定（Security Settings）] ウィンドウで、次の必須オプションを選択します。

- TLS 1.0を許可（Allow TLS 1.0）：次のワークフローについて、従来のピアとの通信に TLS 1.0 を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
  - Cisco ISE は ERS サーバーとして設定されます

  また、次の Cisco ISE コンポーネントとの通信用に TLS 1.0 を許可します。
  - すべてのポータル
  - 認証局
  - MDM クライアント
  - pxGrid
  - PassiveID エージェント

  （注） セキュリティを強化するために、TLS の上位バージョンを使用するようにクライアントとサーバーでネゴシエートすることをお勧めします。

- TLS 1.1を許可（Allow TLS 1.1）：次のワークフローについて、従来のピアとの通信に TLS 1.1 を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
  - Cisco ISE は ERS サーバーとして設定されます

  また、次の Cisco ISE コンポーネントとの通信用に TLS 1.1 を許可します。
  - すべてのポータル

- 認証局
- 外部 RESTful サービス（ERS）
- MDM クライアント
- pxGrid

（注） セキュリティを強化するために、TLS の上位バージョンを使用するようにクライアントとサーバーでネゴシエートすることをお勧めします。

- [SHA-1暗号化を許可（Allow SHA-1 Ciphers）]：次のワークフローについて、ピアとの通信に SHA-1 暗号化を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます

  また、次の Cisco ISE コンポーネントとの通信用に SHA-1 暗号化を許可します。
  - 管理者アクセス UI
  - すべてのポータル
  - ERS
  - pxGrid
  - 管理者アクセス：443
  - Cisco ISE ポータル：9002、8443、8444、8445、8449
  - ERS：9060、9061、9063
  - pxGrid：8910

  （注） このオプションはデフォルトでは無効になっています。

  [SHA-1暗号化を許可（Allow SHA-1 Ciphers）] オプションを有効または無効にした後、展開内のすべてのノードを再起動する必要があります。再起動に失敗すると、設定の変更は適用されません。このようなシナリオでは、次のコマンドを使用して、すべてのノードを手動で再起動する必要があります。

  application stop ise および **application start ise**。

  レガシーピアとの通信用に SHA-1 暗号化を許可する際、次のオプションのいずれかを選択できます。
  - [Allow all SHA-1 Ciphers]：レガシーピアとの通信用にすべての SHA-1 暗号方式を許可します。

- [Allow only TLS_RSA_with_AES_128_CBC_SHA]：レガシーピアとの通信用に TLS_RSA_with_AES_128_CBC_SHA 暗号方式のみを許可します。

（注） セキュリティを強化するために、SHA-256 または SHA-384 暗号化を使用することを推奨します。

- [ECDHE-RSA 暗号化を許可（Allow ECDHE-RSA Ciphers）]：次のワークフローについて、ピアとの通信に ECDHE-RSA 暗号化を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- [3DES 暗号化を許可（Allow 3DES ciphers）]：次のワークフローについて、ピアとの通信に 3DES 暗号化を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバーとして設定されます
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- [Accept Certificates without Validating Purpose]：Cisco ISE が EAP または RADIUS DTLS サーバーとして機能している場合、クライアント証明書は次のことを確認せずに受け入れられます。
  - Key Usage 拡張に、ECDHE-ECDSA 暗号方式の keyAgreement ビットまたは他の暗号方式の keyEncipherment ビットが含まれている。
  - Extended Key Usage の属性値は ClientAuth である

  このオプションを無効にすると、Cisco ISE により、すべてのクライアント証明書の目的が検証されます。証明書は、次のいずれかの条件が満たされた場合にのみ有効と見なされます。
  - Extended Key Usage の属性値が存在しない場合：
    - cipherGroup が ECDHE-ECDSA の場合、Key Usage 拡張には KeyAgreement 値が含まれている必要があります。
    - cipherGroup が ECDHE-ECDSA 以外の場合、Key Usage 拡張には keyEncipherment 値と DigitalSignature 値が含まれている必要があります。

- Extended Key Usage の属性値が ClientAuth の場合：
  - cipherGroup が ECDHE-ECDSA の場合、Key Usage 拡張には KeyAgreement 値が含まれている必要があります。
  - cipherGroup が ECDHE-ECDSA 以外の場合、Key Usage 拡張には keyEncipherment 値と DigitalSignature 値が含まれている必要があります。

上記の条件のいずれも満たされない場合、証明書の検証は失敗します。

- [ISEのDSS暗号化をクライアントとして許可（Allow DSS ciphers for ISE as a client）]：次のワークフローについて、Cisco ISE がクライアントとして機能する場合、サーバーとの通信に DSS 暗号化を許可します。
  - Cisco ISE は、RADIUS DTLS クライアントとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- ISEの従来の安全でないTLS再ネゴシエーションをクライアントとして許可（Allow Legacy Unsafe TLS Renegotiation for ISE as a Client）：次のワークフローについて、安全な TLS 再ネゴシエーションをサポートしていない従来の TLS サーバーとの通信を許可します。
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- [無効なユーザー名を開示する（Disclose invalid usernamess）]：デフォルトでは、ユーザー名が正しくないために認証が失敗した場合に、Cisco ISE は `invalid` メッセージを表示します。デバッグをサポートするために、このオプションでは `invalid` メッセージの代わりに、Cisco ISE がレポートにユーザー名を表示するように強制します。ユーザー名が正しくないという理由以外で認証に失敗した場合、ユーザー名は常に表示されることに注意してください。

  この機能は、Active Directory、内部ユーザー、LDAP、および ODBC ID ソースでサポートされます。RADIUS トークン、RSA、または SAML など、他の ID ストアではサポートされません。

ステップ 3 [Save] をクリックします。

Cisco ISE の RADIUS プロトコルのサポート

RADIUS は、クライアント/サーバープロトコルです。リモートアクセスサーバーは、このプロトコルを使用して中央サーバーと通信してダイヤルインユーザーを認証し、要求されたシステムまたはサービスへのアクセスを許可します。RADIUS を使用すると、すべてのリモート

サーバーが共有できる中央データベースでユーザープロファイルを管理できます。このプロトコルはセキュリティを向上させます。また、このプロトコルを使用して、単一の管理ネットワーク ポイントで適用されるポリシーを設定できます。

RADIUS は、Cisco ISE の RADIUS クライアントとしても機能し、リモート RADIUS サーバーへの要求をプロキシ処理します。また、アクティブセッション中に許可変更（CoA）アクティビティを提供します。

Cisco ISE では、RFC 2865 と、その仕様および拡張仕様に記載されているすべての一般的な RADIUS 属性の包括的なサポートに従って、RADIUS プロトコルのフローがサポートされます。Cisco ISE では、Cisco ISE ディクショナリで定義されているベンダーだけを対象に、ベンダー固有属性の解析がサポートされます。

RADIUS インターフェイスでは、RFC 2865 で定義されている次の属性データ型がサポートされます。

- テキスト（Unicode Transformation Format（UTF））
- 文字列（バイナリ）
- アドレス（IP）
- 整数（Integer）
- 時刻（Time）

ISE コミュニティ リソース

Cisco ISE でサポートされるネットワーク アクセス属性については、「ISE Network Access Attributes」を参照してください。

許可されるプロトコル

次の表に、認証中に使用するプロトコルを設定できるようにする [許可されるプロトコル（Allowed Protocols）] ウィンドウのフィールドを示します。ナビゲーションパスは、次のとおりです。**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）]**。

Table 9: 許可されるプロトコル

フィールド名	使用上のガイドライン
[許可されているプロトコル（Allowed Protocols）] > [認証バイパス（Authentication Bypass）]	

フィールド名	使用上のガイドライン
ホスト ルックアップの処理（**Process Host Lookup**）	Cisco ISE がホスト ルックアップ要求を処理できるようにするには、このチェックボックスをオンにします。ホストルックアップ要求は、RADIUS Service-Type が 10（Call-Check）に等しく、ユーザー名が Calling-Station-ID に等しい場合は PAP/CHAP プロトコルに対して処理されます。ホスト ルックアップ要求は、Service-Type が 1（Framed）に等しく、ユーザー名が Calling-Station-ID に等しい場合は EAP-MD5 プロトコルに対して処理されます。Cisco ISE でホスト ルックアップ要求を無視し、認証にシステム ユーザー名属性の元の値を使用するには、このチェックボックスをオフにします。オフにすると、メッセージ処理はプロトコル（たとえば PAP）に従って行われます。 **Note** このオプションを無効にすると、既存の MAB 認証で障害が発生する可能性があります。
[許可されているプロトコル（Allowed Protocols）] > [認証プロトコル（Authentication Protocols）]	
PAP/ASCII を許可（Allow PAP/ASCII）	このオプションによって、PAP/ASCII が有効になります。PAP は、平文パスワード（つまり暗号化されていないパスワード）を使用する最も安全性の低い認証プロトコルです。
CHAP を許可（Allow CHAP）	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。
MS-CHAPv1 を許可（Allow MS-CHAPv1）	MS-CHAPv1 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。
MS-CHAPv2 を許可（Allow MS-CHAPv2）	MS-CHAPv2 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。
EAP-MD5 を許可（Allow EAP-MD5）	EAP ベースの MD5 パスワード 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。

フィールド名	使用上のガイドライン
EAP-TLS を許可（Allow EAP-TLS）	

フィールド名	使用上のガイドライン
	EAP-TLS 認証プロトコルを有効にする場合、およびEAP-TLS設定値を設定する場合は、このチェックボックスをオンにします。エンドユーザー クライアントからの EAP Identity 応答で提示されたユーザー ID を Cisco ISE が確認する方法を指定できます。ユーザーIDは、エンドユーザー クライアントによって提示された証明書の情報に照らして確認されます。この比較は、Cisco ISE とエンドユーザー クライアントとの間にEAP-TLS トンネルが確立された後に行われます。 **Note** EAP-TLSは、証明書ベースの認証プロトコルです。EAP-TLS認証が行われるのは、証明書の設定に必要な手順を完了した場合に限られます。 • [期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）]：ユーザーが証明書を更新できるようにする場合は、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すると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。 • [ステートレスセッション再開を有効にする（Enable Stateless Session Resume）]：セッション状態をサーバーに保存する必要なしでEAP-TLSセッションを再開できるようにするには、このチェックボックスをオンにします。Cisco ISE では RFC 5077 で記述されているセッション チケット拡張もサポートされます。Cisco ISE はチケットを作成してEAP-TLSクライアントにそのチケットを送信します。クライアントはセッションを再開するためにそのチケットを ISE に提示します。 • [プロアクティブセッションチケット更新（Proactive Session Ticket update）]：セッ

フィールド名	使用上のガイドライン
	ションチケットが更新される前に経過する必要がある存続可能時間（TTL）の量を示すパーセント値を入力します。たとえば、値に60を入力すると、セッションチケットはTTLの60パーセントが経過した後で更新されます。 • [セッションチケットの存続時間（Session ticket Time to Live）]：セッションチケットが期限切れになるまでの時間を入力します。この値は、セッション チケットがアクティブである期間を決定します。この値は秒、分、時、日数、または週数で入力できます。
LEAP を許可（Allow LEAP）	Lightweight Extensible Authentication Protocol（LEAP）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。

フィールド名	使用上のガイドライン
PEAP を許可（Allow PEAP）	

フィールド名	使用上のガイドライン
	PEAP認証プロトコルおよびPEAP設定値を有効にする場合は、このチェックボックスをオンにします。デフォルトの内部方式は、MS-CHAPv2 です。 [PEAP を許可（Allow PEAP）] チェックボックスをオンにすると、次の PEAP 内部方式を設定できます。 • [EAP-MS-CHAPv2を許可（Allow EAP-MS-CHAPv2）]：内部方式として EAP-MS-CHAPv2 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。 • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザークレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。 • [EAP-GTCを許可（Allow EAP-GTC）]：内部方式としてEAP-GTC 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。 • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザークレデンシャルを要求する回数を指定します。有効範囲は 0 ～ 3 です。 • [EAP-TLSを許可（Allow EAP-TLS）]：内部方式として EAP-TLS 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。 ユーザーによる証明書の更新を許可する

フィールド名	使用上のガイドライン
	場合は、[期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）] 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すると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。 • [暗号化バインドTLVを要求（Require cryptobinding TLV）]：EAP ピアと EAP サーバーの両方が PEAP 認証の内部および外部 EAP 認証に参加する場合、このチェックボックスをオンにします。 • [レガシークライアントにのみPEAPv0を許可（Allow PEAPv0 only for legacy clients）]：PEAP サプリカントが PEAPv0 を使用してネゴシエーションできるようにするには、このチェックボックスをオンにします。一部のレガシー クライアントは PEAPv1 プロトコル規格に準拠しません。そのような PEAP カンバセーションがドロップされないようにするには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
EAP-FAST を許可（Allow EAP-FAST）	

フィールド名	使用上のガイドライン
	EAP-FAST 認証プロトコルおよび EAP-FAST 設定を有効にする場合は、このチェックボックスをオンにします。EAP-FAST プロトコルは、同じサーバー上の複数の内部プロトコルをサポートできます。デフォルトの内部方式は、MS-CHAPv2 です。 [EAP-FAST を許可（Allow EAP-FAST）] チェックボックスをオンにすると、EAP-FAST を内部方式として設定できます。 • **EAP-MS-CHAPv2 を許可（Allow EAP-MS-CHAPv2）** • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザークレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。 • **EAP-GTC を許可（Allow EAP-GTC）** [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザークレデンシャルを要求する回数を指定します。有効な値は 0 ～ 3 です。 • [PACの使用（Use PACs）]：EAP-FAST クライアントに認可 Protected Access Credentials（PAC）をプロビジョニングするように Cisco ISE を設定する場合にこのオプションを選択します。追加の PAC オプションが表示されます。 • [PACを使用しない（Don’t use PACs）]：トンネルまたはマシン PAC を発行したり受け入れたりしないで EAP-FAST を使用するように Cisco ISE を設定する場合にこ

フィールド名	使用上のガイドライン
	のオプションを選択します。PAC のすべての要求は無視され、Cisco ISE は PAC を含まない Success-TLV で応答します。 このオプションを選択すると、マシン認証を実行するように Cisco ISE を設定できます。 • [EAP-TLSを許可（Allow EAP-TLS）]：内部方式として EAP-TLS 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。 ユーザーによる証明書の更新を許可する場合は、[期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）] 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すると、要求をさらに処理する前に証明書が更新されたかどうかをチェックするように適切な許可ポリシー ルールを設定します。

フィールド名	使用上のガイドライン
	• [EAPチェーンを有効化（Enable EAP Chaining）]：EAP チェーンを有効にするには、このチェックボックスをオンにします。 EAP チェーンによって、Cisco ISE はユーザー認証とマシン認証の結果を関連付け、EAPChainingResult 属性を使用して適切な許可ポリシーを適用することができます。 EAP チェーンには、クライアント デバイスで EAP チェーンをサポートするサプリカントが必要です。サプリカントで[ユーザー認証およびマシン認証（User and Machine Authentication）] オプションを選択します。 EAP チェーンは、EAP-FAST プロトコル（PAC ベース モードおよび PAC レス モードの両方）を選択するときに使用できます。 PAC ベースの認証では、ユーザー認可 PAC またはマシン認可 PAC のいずれかを使用するか、両方を使用して内部方式をスキップすることができます。 証明書ベースの認証では、（許可されるプロトコルサービスの）EAP-FAST プロトコルに対して [Accept Client Certificate for Provisioning] オプションが有効な場合、およびエンドポイント（AnyConnect）がトンネル内のユーザー証明書を送信するように設定されている場合、トンネルの確立中に、ISE が証明書を使用してユーザーを認証し（内部方式はスキップされます）、マシン認証は内部方式によって実行されます。これらのオプションが設定されていない場合、EAP-TLS が内部方式としてユーザー認証に使用されます。 EAP チェーンを有効にした後、許可ポリシーを更新し、NetworkAccess:EapChainingResult 属性を使用して条件を追加し、適切な権限を割り当てます。

フィールド名	使用上のガイドライン
EAP-TTLSを許可（Allow EAP-TTLS）	

フィールド名	使用上のガイドライン

	EAP-TTLS プロトコルを有効にする場合に、このチェックボックスをオンにします。
	
	次の内部方式を設定できます。
	
	• [PAP/ASCIIを許可（Allow PAP/ASCII）]：内部方式として PAP/ASCII 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。EAP-TTLS PAP は、トークンおよび OTP ベースの認証で使用できます。
	
	• [CHAPを許可（Allow CHAP）]：内部方式として CHAP 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。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。
	
	• [MS-CHAPv1を許可（Allow MS-CHAPv1）]：内部方式として MS-CHAPv1 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。
	
	• [MS-CHAPv2を許可（Allow MS-CHAPv2）]：内部方式として MS-CHAPv2 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。
	
	• [EAP-MD5を許可（Allow EAP-MD5）]：内部方式として EAP-MD5 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。
	
	• [EAP-MS-CHAPv2を許可（Allow EAP-MS-CHAPv2）]：内部方式として EAP-MS-CHAPv2 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。
	
	  • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。
	
	  • [再試行（Retry Attempts）]：Cisco ISE でログイン失敗を返す前にユーザークレデンシャルを要求する回数を指

フィールド名	使用上のガイドライン
	定します。有効な値は 0 ～ 3 です。

フィールド名	使用上のガイドライン
TEAP を許可（Allow TEAP）	

フィールド名	使用上のガイドライン
	Tunnel Extensible Authentication Protocol（TEAP）を有効にして TEAP を設定するには、このチェックボックスをオンにします。TEAP は、トンネルを確立するために Transport Layer Security（TLS）プロトコルを使用して、サーバーとピア間のセキュアな通信を可能にする、トンネルベースの EAP 方式です。TEAP トンネル内では、EAP ピアと EAP サーバー間の認証関連データを伝送するために、Type-Length-Value（TLV）オブジェクトが使用されます。 TEAP に次の内部方式を設定できます。 • [EAP-MS-CHAPv2を許可（Allow EAP-MS-CHAPv2）]：内部方式として EAP-MS-CHAPv2 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。 • [パスワード変更の許可（Allow Password Change）]：Cisco ISE でパスワード変更をサポートする場合は、このチェックボックスをオンにします。 • [再試行回数（Retries）]：ログイン失敗メッセージを返す前に、Cisco ISE がログイン情報の入力を許可する回数を入力します。有効範囲は 0 ～ 3 です。 • [EAP-TLSを許可（Allow EAP-TLS）]：内部方式として EAP-TLS 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。 • [期限切れ証明書の認証を許可して、許可ポリシーの証明書の更新を許可する（Allow authentication of expired certificates to allow certificate renewal in Authorization Policy）]：ユーザーが証明書を更新できるようにする場合は、このチェックボックスをオンにします。このオプションを有効にすると、認証要求をさらに処理する前に証明書が更新されたかどうかを確認する

フィールド名	使用上のガイドライン
	ように適切な許可ポリシールールを設定します。 • [MSKへのダウングレードの許可（Allow Downgrade to MSK）]：内部方式が拡張マスターセッションキー（EMSK）をサポートしているが、クライアントデバイスがマスターセッションキー（MSK）のみを提供している場合は、このチェックボックスをオンにします。EMSK はMSK よりも安全ですが、一部のクライアントデバイスでは EMSK がサポートされていない可能性があることに注意してください。 • [トンネル確立中のクライアント証明書の承認（Accept Client Certificate during Tunnel Establishment）]：TEAP トンネルの確立時に Cisco ISE がクライアント証明書を要求するようにするには、このチェックボックスをオンにします。証明書が指定されていない場合、Cisco ISE は設定された内部方式を認証に使用します。

フィールド名	使用上のガイドライン
	• [EAPチェーンを有効化（Enable EAP Chaining）]：EAP チェーンを有効にするには、このチェックボックスをオンにします。EAPチェーンを使用すると、Cisco ISEは、同じTEAPトンネル内でユーザーとマシンの両方の認証の内部方式を実行できます。これにより、Cisco ISE は認証の結果を関連付け、EAPChainingResult 属性を使用して適切な許可ポリシーを適用することができます。 EAP チェーンを有効にした後、許可ポリシーを更新し、NetworkAccess:EapChainingResult 属性を使用して条件を追加し、適切な権限を割り当てます。 **Note** EAPチェーンが有効になっていて、ユーザーとマシンの両方の認証を実行する場合は、ユーザーとマシンの証明書がサプリカントにコピーされていることを確認します。

フィールド名	使用上のガイドライン
	Note • Cisco ISE で EAP チェーンが有効になっている場合は、プライマリとセカンダリの両方の認証方式が Microsoft サプリカント用に設定されている必要があります。 • Cisco ISE で EAP チェーンが無効になっている場合は、プライマリの認証方式のみが Microsoft サプリカント用に設定されている必要があります。 • プライマリとセカンダリの両方の認証方式が [なし（None）] に設定されている場合、EAP ネゴシエーションが失敗し、次のメッセージが表示されることがあります。 `サプリカントが ISE に応答しなくなりました（upplicant stopped responding to ISE）`
優先 EAP プロトコル（Preferred EAP protocol）	EAP-FAST、PEAP、LEAP、EAP-TLS、EAP-TTLS、および EAP-MD5 から任意の優先 EAP プロトコルを選択するには、このチェックボックスをオンにします。優先プロトコルを指定しない場合、EAP-TLS がデフォルトで使用されます。
EAP-TLS L ビット（EAP-TLS L-bit）	デフォルトで、ISE からの TLS Change Cipher Spec メッセージと暗号化ハンドシェイクメッセージの長さの含まれるフラグ（L ビットフラグ）を予測するレガシー EAP サプリカントをサポートするには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
EAP の脆弱な暗号の許可（Allow Weak Ciphers for EAP）	このオプションを有効にすると、レガシー クライアントが脆弱な暗号（RSA_RC4_128_SHA、RSA_RC4_128_MD5 など）を使用してネゴシエートすることができます。レガシー クライアントが脆弱な暗号化だけをサポートしている場合に限り、このオプションを有効にすることを推奨します。 このオプションはデフォルトでは無効になっています。 **Note** Cisco ISE は、EDH_RSA_DES_64_CBC_SHA および EDH_DSS_DES_64_CBC_SHA をサポートしていません。
すべての RADIUS 要求にメッセージ オーセンティケータが必要（Require Message Authenticator for all RADIUS Requests）	このオプションを有効にすると、Cisco ISE は、RADIUS メッセージ オーセンティケータ属性が RADIUS メッセージがあるかどうかを検証します。メッセージ オーセンティケータ属性がない場合、RADIUS メッセージは破棄されます。 このオプションを有効にすると、スプーフィングされたアクセス要求メッセージおよび RADIUS メッセージの改ざんに対する保護が提供されます。 RADIUS メッセージ オーセンティケータ属性は、RADIUS メッセージ全体の Message Digest 5（MD5）ハッシュです。 **Note** EAP はメッセージ オーセンティケータ属性をデフォルトで使用するので、これを有効にする必要はありません。
5G を許可する（Allow 5G）	Cisco ISE での Cisco Private 5G 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。 **Note** Cisco ISE で 5G as a Service（5GaaS）を有効にする前に、ネットワークに Cisco Private 5G を展開しておく必要があります

Related Topics

TACACS+ デバイス管理を許可された FIPS および非 FIPS モードのプロトコル
ネットワーク アクセスの許可されるプロトコルの定義 （107 ページ）

PAC オプション

次の表では、[許可されるプロトコルサービスリスト（Allowed Protocols Services List）] ウィンドウで [PACを使用（Use PAC）] を選択した後のフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authentication）]** > **[許可されるプロトコル（Allowed Protocols）]** です。

表 *10 : PAC* オプション

フィールド名	使用上のガイドライン
PAC を使用（Use PAC）	

フィールド名	使用上のガイドライン
	• [トンネルPACの存続可能時間（Tunnel PAC Time To Live）]：存続可能時間（TTL）の値によって PAC のライフタイムが制限されます。ライフタイム値と単位を指定します。デフォルトは 90 日です。範囲は 1 ～ 1825 日です。 • [プロアクティブPAC更新の条件：<n%>のPAC TTLが残っている場合（Proactive PAC Update When: <n%> of PAC TTL is Left）]：Update 値により、クライアントに有効な PAC が保持されます。Cisco ISE は、最初に認証が成功してから TTL によって設定された有効期限までに更新を開始します。update 値は、TTL の残り時間のパーセンテージです。デフォルトは 90% です。 • [匿名インバンドPACプロビジョニングを許可（Allow Anonymous In-band PAC Provisioning）]：Cisco ISE でクライアントとのセキュアな匿名 TLS ハンドシェイクを確立し、クライアントに PAC をプロビジョニングする場合にこのチェックボックスをオンにします。その際、EAP-FAST のフェーズ 0 と EAP-MSCHAPv2 が使用されます。匿名 PAC プロビジョニングを有効にするには、内部方式として EAP-MSCHAPv2 と EAP-GTC の両方を選択する必要があります。 • [認証付きインバンドPACプロビジョニングを許可（Allow Authenticated In-band PAC Provisioning）]：Cisco ISE は SSL サーバー側の認証を使用して、EAP-FAST のフェーズ 0 中にクライアントに PAC をプロビジョニングします。このオプションは匿名プロビジョニングよりもセキュアですが、サーバー証明書および信頼できるルート CA が Cisco ISE にインストールされている必要があります。 このオプションをオンにすると、認証された PAC プロビジョニングの成功後に Access-Accept メッセージをクライアントに返すように Cisco ISE を設定できます。

フィールド名	使用上のガイドライン
	• [認証されたプロビジョニングの後にサーバーからAccess-Acceptを返す（Server Returns Access Accept After Authenticated Provisioning）]：認証された PAC プロビジョニングの後に Cisco ISE から access-accept パッケージを返す場合にこのチェックボックスをオンにします。 • [マシン認証を許可（Allow Machine Authentication）]：Cisco ISE でエンドユーザークライアントにマシン PAC をプロビジョニングし、（マシンクレデンシャルを持たないエンドユーザークライアントに対して）マシン認証を実行する場合にこのチェックボックスをオンにします。マシン PAC は、要求（インバンド）によって、または管理者（アウトオブバンド）によって、クライアントにプロビジョニングできます。Cisco ISE がエンドユーザー クライアントから有効なマシン PAC を受信すると、その PAC からマシン ID の詳細が抽出され、Cisco ISE 外部 ID ソースで確認されます。マシン認証の外部 ID ソースとして Cisco ISE によってサポートされるのは、Active Directory だけです。その詳細が正しいことが確認されると、その後の認証は実行されません。 このオプションをオンにすると、マシン PAC を使用するために受け入れることができる期間の値を入力できます。Cisco ISE は、期限切れのマシン PAC を受け取ると、（エンドユーザー クライアントからの新規マシン PAC 要求を待たずに）エンドユーザー クライアントに新規マシン PAC を自動的に再プロビジョニングします。

フィールド名	使用上のガイドライン
	• [ステートレスセッション再開の有効化（Enable Stateless Session Resume）]：Cisco ISE で EAP-FAST クライアントに認可 PAC をプロビジョニングし、EAP-FAST のフェーズ 2 をスキップする場合にこのチェックボックスをオンにします（デフォルトはオン）。 このチェックボックスは次の場合にオフにします。 • Cisco ISE が EAP-FAST クライアントに認可 PAC をプロビジョニングしないようにする場合 • EAP-FAST のフェーズ 2 を常に実行する場合 このオプションをオンにすると、ユーザー認可 PAC の認可期間を入力できます。この期間の終了後、PAC は期限切れになります。Cisco ISE は期限切れの認可 PAC を受信すると、EAP-FAST 認証のフェーズ 2 を実行します。

関連トピック

OOB TrustSec PAC （135 ページ）
EAP-FAST の PAC の生成 （62 ページ）

RADIUS プロキシ サーバーとして機能する Cisco ISE

Cisco ISE は、RADIUS サーバーおよび RADIUS プロキシ サーバーとして機能できます。プロキシ サーバーとして機能する場合、Cisco ISE はネットワーク アクセス サーバー（NAS）から認証要求およびアカウンティング要求を受信し、これらの要求を外部 RADIUS サーバーに転送します。Cisco ISE は要求の結果を受け取り、NAS に返します。

Cisco ISE は、同時に複数の外部 RADIUS サーバーへのプロキシ サーバーとして動作できます。RADIUS サーバー順序で設定した外部 RADIUS サーバーを使用できます。次に説明する [外部 RADIUS サーバー（External RADIUS Server）] ページには、Cisco ISE で定義した外部 RADIUS サーバーがすべて表示されます。フィルタ オプションを使用して、名前または説明、またはその両方に基づいて特定の RADIUS サーバーを検索することができます。単純な認証ポリシーとルールベースの認証ポリシーの両方で、RADIUS サーバー順序を使用して要求を RADIUS サーバーにプロキシできます。

RADIUS サーバー順序は、RADIUS-Username 属性からドメイン名を抜き取り（ストリッピング）、RADIUS 認証に使用します。このドメイン ストリッピングは EAP 認証には使用できません。EAP 認証では EAP-Identity 属性が使用されます。RADIUS プロキシ サーバーは RADIUS-Username 属性からユーザー名を取得し、RADIUS サーバー順序の設定時に指定した文字列からユーザー名を抜き取ります。EAP 認証の場合は、RADIUS プロキシ サーバーはユーザー名を EAP-Identity 属性から取得します。RADIUS サーバー順序を使用する EAP 認証は、EAP-Identity 値と RADIUS-Username 値が同一である場合のみ成功します。

外部 RADIUS サーバーの設定

Cisco ISE で外部 RADIUS サーバーを設定して、要求を外部 RADIUS サーバーに送信できるようにする必要があります。タイムアウト時間および接続試行回数を定義できます。

始める前に

- この項で作成した外部 RADIUS サーバーは、それだけでは使用できません。RADIUS サーバー順序を作成して、この項で作成した RADIUS サーバーを使用するように設定する必要があります。これにより、RADIUS サーバー順序を認証ポリシーで使用できるようになります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[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）]** を選択します。

[RADIUS サーバー（RADIUS Servers）] ページが表示され、Cisco ISE で定義された外部 RADIUS サーバーのリストが示されます。

ステップ 2 外部 RADIUS サーバーを追加するには、[追加（Add）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信（Submit）] をクリックして、外部 RADIUS サーバーの設定を保存します。

RADIUS サーバー順序の定義

Cisco ISE の RADIUS サーバー順序を使用すると、NAD からの要求を外部 RADIUS サーバーにプロキシできます。外部 RADIUS サーバーは要求を処理して結果を Cisco ISE に返し、Cisco ISE はその応答を NAD に転送します。

[RADIUS サーバー順序（RADIUS Server Sequences）] ページに、Cisco ISE で定義したすべての RADIUS サーバーの順序が表示されます。このページを使用して、RADIUS サーバーの作成、編集、または複製が可能です。

始める前に

- この手順を開始する前に、プロキシサービスの基本を理解し、関連リンクの最初のエントリのタスクを正常に完了している必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[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）]** 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 必要に応じて値を入力します。

ステップ 4 [送信（Submit）] をクリックして、ポリシーに使用する RADIUS サーバー順序を保存します。

TACACS+ プロキシ クライアントとして機能する Cisco ISE

Cisco ISE は、外部 TACACS+ サーバーへのプロキシ クライアントとして機能できます。プロキシ クライアントとして機能する場合、Cisco ISE はネットワーク アクセス サーバー（NAS）から認証要求、許可要求およびアカウンティング要求を受信し、これらの要求を外部 TACACS+ サーバーに転送します。Cisco ISE は要求の結果を受け取り、NAS に返します。

[TACACS+外部サーバー（TACACS+ External Servers）] ページには、Cisco ISE で定義した外部 TACACS+ サーバーがすべて表示されます。フィルタ オプションを使用して、名前または説明、またはその両方に基づいて特定の TACACS+ サーバーを検索することができます。

Cisco ISE は、同時に複数の外部 TACACS+ サーバーへのプロキシ クライアントとして動作できます。複数の外部サーバーを設定するには、[TACACS+サーバーの順序（TACACS+ server sequence）] ページを使用できます。詳細については、「TACACS+ サーバー順序の設定」ページを参照してください。

外部 TACACS+ サーバーの設定

Cisco ISE で外部 TACACS サーバーを設定して、要求を外部 TACACS サーバーに送信できるようにする必要があります。タイムアウト時間および接続試行回数を定義できます。

始める前に

- この項で作成した外部 TACACS サーバーは、ポリシーに直接使用できません。TACACS サーバー順序を作成して、この項で作成した TACACS サーバーを使用するように設定する必要があります。これにより、TACACS サーバー順序をポリシー セットで使用できるようになります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[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）] > [TACACS外部サーバー（TACACS External Servers）]** の順に選択します。[TACACS外部サーバー（TACACS External Servers）] ページが表示され、Cisco ISE で定義された外部 TACACS サーバーのリストが示されます。

ステップ 2 外部 TACACS サーバーを追加するには、[追加（Add）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [送信（Submit）] をクリックして、外部 TACACS サーバーの設定を保存します。

TACACS+ 外部サーバーの設定

次の表では、[TACACS外部サーバー（TACACS External Servers）] ページのフィールドについて説明します。ナビゲーションパスは、次のとおりです。**[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）] > [TACACS 外部サーバー（TACACS External Servers）]**。

表 *11 : TACACS+* 外部サーバーの設定

フィールド	使用上のガイドライン
名前（Name）	TACACS+外部サーバーの名前を入力します。
説明	TACACS+外部サーバー設定の説明を入力します。
ホスト名/アドレス（Host IP）	リモート TACACS+ 外部サーバーの IP アドレス（IPv4 または IPv6 アドレス）を入力します。
接続ポート（Connection Port）	リモート TACACS+ 外部サーバーのポート番号を入力します。ポート番号は 49 です。
Timeout	ISE が外部 TACACS+ 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 1 ～ 120 です。
共有秘密鍵（Shared Secret）	TACACS+外部サーバーとの接続を保護するのに使用するテキスト文字列。正しく設定されていない場合、接続はTACACS+外部サーバーによって拒否されます。

フィールド	使用上のガイドライン
シングル接続を使用（Use Single Connect）	TACACS プロトコルは、接続にセッションを関連付けるための 2 つのモード、シングル接続と非シングル接続をサポートしています。シングル接続モードは、クライアントが開始する可能性がある多数の TACACS+ セッションに対し、単一の TCP 接続を再使用します。非シングル接続では、クライアントが開始するすべての TACACS+ セッションに対し、新しい TCP 接続が開かれます。TCP 接続は、各セッションの後に閉じられます。 トラフィックが多い環境では、[シングル接続を使用（Use Single Connect）] チェックボックスをオンにし、トラフィックが少ない環境ではオフにできます。

TACACS+ サーバー順序の定義

Cisco ISE の TACACS+ サーバー順序を使用すると、NAD からの要求を外部 TACACS+ サーバーにプロキシできます。外部 TACACS+ サーバーは要求を処理して結果を Cisco ISE に返し、Cisco ISE はその応答を NAD に転送します。[TACACS+サーバー順序（TACACS+ Server Sequences）] ページに、Cisco ISE で定義したすべての TACACS+ サーバーの順序が表示されます。このページを使用して、TACACS+ サーバー順序の作成、編集、または複製が可能です。

始める前に

- プロキシ サービス、Cisco ISE 管理者グループ、アクセス レベル、権限、および制限の基本を理解している必要があります。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- TACACS+ サーバー順序で使用する外部 TACACS+ サーバーがすでに定義されていることを確認します。

ステップ 1 **[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）] > [TACACS外部サーバー順序（TACACS External Server Sequence）]** 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 必要な値を入力します。

ステップ 4 [送信（Submit）] をクリックして、ポリシーに使用する TACACS+ サーバー順序を保存します。

TACACS+ サーバー順序の設定

次の表では、[TACACSサーバー順序（TACACS Server Sequence）] ページのフィールドについて説明します。ナビゲーションパスは、次のとおりです。**[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）]** > **[TACACS外部サーバー順序（TACACS External Server Sequence）]**。

表 *12 : TACACS+* サーバー順序の設定

フィールド	使用上のガイドライン
名前（Name）	TACACS プロキシ サーバー順序の名前を入力します。
説明	TACACS プロキシ サーバー順序の説明を入力します。
サーバー リスト（Server List）	[使用可能（Available）] リストから必要な TACACS プロキシ サーバーを選択します。[使用可能（Available）] リストには、[TACACS外部サービス（TACACS External Services）] ページで設定されている TACACS プロキシ サーバーのリストが含まれています。
ロギング制御（Logging Control）	ロギング制御を有効にするにはオンにします。 • ローカル アカウンティング：アカウンティング メッセージは、デバイスからの要求を処理するサーバーによってログに記録されます。 • リモート アカウンティング：アカウンティング メッセージは、デバイスからの要求を処理するプロキシ サーバーによってログに記録されます。

フィールド	使用上のガイドライン
ユーザー名の除去（Username Stripping）	ユーザー名のプレフィックス/サフィックスの除去 • [プレフィックスの除去（Prefix Strip）]：プレフィックスからユーザー名を取り除く場合にオンにします。たとえば、サブジェクト名が acme\smith、区切り文字が \ の場合、ユーザー名は smith になります。デフォルトの区切り文字は \ です。 • [サフィックスの除去（Suffix Strip）]：サフィックスからユーザー名を取り除く場合にオンにします。たとえば、サブジェクト名が smith@acme.com、区切り文字が @ の場合、ユーザー名は smith になります。デフォルトの区切り文字は @ です。

ネットワーク アクセス サービス

ネットワーク アクセス サービスには、要求に対する認証ポリシー条件が含まれています。たとえば有線 802.1X や有線 MAB など、さまざまな用途向けに個別のネットワーク アクセス サービスを作成することができます。ネットワーク アクセス サービスを作成するには、許可されているプロトコルまたはサーバー順序を設定します。その後、ネットワーク アクセス ポリシーのネットワーク アクセス サービスが [ポリシー セット（Policy Sets）] ページから構成されます。

ネットワーク アクセスの許可されるプロトコルの定義

許可されるプロトコルは、ネットワーク リソースへのアクセスを要求するデバイスとの通信に Cisco ISE が使用できるプロトコルのセットを定義します。許可されるプロトコル アクセス サービスは、認証ポリシーを設定する前に作成する必要がある独立したエントリです。許可されるプロトコル アクセス サービスは、特定の使用例に対して選択されたプロトコルが含まれているオブジェクトです。

[許可されるプロトコル サービス（Allowed Protocols Services）] ページには、作成した許可されるプロトコル サービスがすべて表示されます。Cisco ISE で事前に定義されたデフォルトのネットワーク アクセス サービスが存在します。

始める前に

この手順を開始する前に、認証に使用するプロトコル サービスの基本を理解している必要があります。

- この章の「Cisco ISE 認証ポリシー」の項を参照して、さまざまなデータベースでサポートされる認証タイプおよびプロトコルについて理解します。

- 「PAC オプション」を確認して、各プロトコル サービスの機能とオプションを理解し、使用しているネットワークに最適な選択ができるようにしてください。
- 手順を進める前に、グローバル プロトコル設定を必ず定義してください。

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

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されるプロトコル（Allowed Protocols）]** 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 必要な情報を入力します。

ステップ 4 ネットワークに適切な認証プロトコルとオプションを選択します。

ステップ 5 PAC の使用を選択した場合、適切な選択を行います。

匿名 PAC プロビジョニングを有効にするには、内部方式として EAP-MSCHAPv2 と Extensible Authentication Protocol-Generic Token Card（EAP-GTC）の両方を選択する必要があります。また Cisco ISE では、マシン認証の外部 ID ソースとしては Active Directory だけがサポートされる点に注意してください。

ステップ 6 [送信（Submit）] をクリックして、許可されるプロトコル サービスを保存します。

許可されるプロトコル サービスは、単純な認証ポリシーおよびルールベースの認証ポリシーのページで独立したオブジェクトとして表示されます。このオブジェクトは異なるルールに使用できます。

これで、単純な認証ポリシーおよびルールベースの認証ポリシーを作成できるようになります。

内部方式として EAP-MSCHAP を無効にし、PEAP または EAP-FAST の EAP-GTC と EAP-TLS 内部方式を有効にすると、ISE は内部方式のネゴシエーション中に EAP-GTC 内部方式を開始します。最初の EAP-GTC メッセージがクライアントに送信される前に、ISE は ID 選択のポリシーを実行して、ID ストアから GTC パスワードを取得します。このポリシーの実行中、EAP 認証は EAP-GTC と同じです。EAP-GTC 内部方式がクライアントによって拒否され、EAP-TLS がネゴシエートされても、ID ストア ポリシーが再び実行されることはありません。ID ストア ポリシーが EAP 認証属性に基づいている場合、本当の EAP 認証は EAP-TLS でありながら ID ポリシー評価後に設定されたため、予期しない結果になることがあります。

ユーザーのネットワーク アクセス

ネットワーク アクセスでは、ホストはネットワーク デバイスに接続し、ネットワーク リソースの使用を要求します。ネットワーク デバイスは、新しく接続されたホストを識別し、転送方式として RADIUS プロトコルを使用して、ユーザーの認証および許可を Cisco ISE に要求します。

Cisco ISE では、RADIUS プロトコルを使用して転送されるプロトコルに応じて、ネットワーク アクセス フローがサポートされます。

EAP を使用しない RADIUS ベースのプロトコル

EAP を含まない RADIUS ベースのプロトコルは、次のとおりです。

- Password Authentication Protocol（PAP）
- CHAP
- Microsoft Challenge Handshake Authentication Protocol version 1（MS-CHAPv1）
- MS-CHAP バージョン 2（MS-CHAPv2）

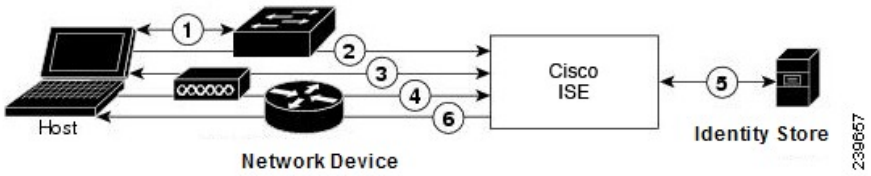
RADIUS-Based Non-EAP 認証フロー

ここでは、EAP 認証を使用しない RADIUS ベースのフローについて説明します。PAP 認証を使用する RADIUS ベースのフローは、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが RADIUS 要求（Access-Request）を Cisco ISE に送信します。この要求には、使用する特定のプロトコル（PAP、CHAP、MS-CHAPv1、または MS-CHAPv2）に適した RADIUS 属性が含まれます。
3. Cisco ISE では、ID ストアを使用してユーザー クレデンシャルを検証します。
4. RADIUS 応答（Access-Accept または Access-Reject）が、決定を適用するネットワーク デバイスに送信されます。

次の図は、EAP を使用しない RADIUS ベースの認証を示しています。

図 *5 : EAP* を使用しない *RADIUS* ベースの認証



Cisco ISE でサポートされる非 EAP プロトコルは次のとおりです。

パスワード認証プロトコル

PAP では、ユーザーが双方向ハンドシェイクを使用して ID を確立できる単純な方法が提供されます。PAP パスワードは共有秘密を使用して暗号化されるため、最もセキュリティ レベルの低い認証プロトコルです。PAP は、反復的な試行錯誤攻撃に対する保護がほとんどないため、確実な認証方式ではありません。

Cisco ISE の *RADIUS-Based PAP* 認証

Cisco ISE では、ID ストアに対してユーザー名とパスワードのペアをチェックし、最終的にその認証を確認するか、接続を終了します。

Cisco ISE では、異なるセキュリティ レベルを同時に使用して、さまざまな要件に対応できます。PAP は双方向ハンドシェイク手順を適用します。認証に成功した場合、Cisco ISE は確認

応答を返します。認証に失敗した場合、Cisco ISE は接続を終了するか、認証の要求元にもう一度チャンスを与えます。

認証の要求元が、試行の頻度とタイミングを総合的に制御します。したがって、より強力な認証方式を使用できるサーバーは、PAP よりも前にその方式のネゴシエーションを提案します。PAP は RFC 1334 で定義されています。

Cisco ISE では、RADIUS UserPassword 属性に基づく標準の RADIUS PAP 認証がサポートされます。RADIUS PAP 認証は、すべての ID ストアと互換性があります。

PAP 認証フローを使用する RADIUS には、試行の成功と失敗のロギングが含まれます。

チャレンジ ハンドシェイク認証プロトコル

CHAP は、応答時に一方向の暗号化を使用するチャレンジ/レスポンス方式です。CHAP を使用することで、Cisco ISE は、セキュリティ レベルの高い順からセキュリティ暗号化方式をネゴシエートし、プロセス中に伝送されるパスワードを保護します。CHAP パスワードは再利用が可能です。Cisco ISE 内部データベースを認証に使用する場合は、PAP または CHAP のどちらかを使用できます。CHAP は、Microsoft ユーザー データベースでは使用できません。RADIUS PAP と比較した場合、エンドユーザー クライアントから AAA クライアントに通信するときに CHAP を使用すると、パスワードが暗号化されるため、高いセキュリティ レベルを確保できます。

Cisco ISE では、RADIUS ChapPassword 属性に基づく標準の RADIUS CHAP 認証がサポートされます。Cisco ISE では、外部 ID ストアを使用した RADIUS CHAP 認証だけがサポートされます。

Microsoft Challenge Handshake Authentication Protocol Version 1

Cisco ISE では、RADIUS MS-CHAPv1 認証およびパスワード変更機能がサポートされます。RADIUS MS-CHAPv1 には、Change-Password-V1 と Change-Password-V2 の 2 つのバージョンのパスワード変更機能が含まれます。Cisco ISE は RADIUS MS-CHAP-CPW-1 属性に基づいた Change-Password-V1 パスワード変更をサポートせず、MS-CHAP-CPW-2 属性に基づいた Change-Password-V2 のみをサポートします。RADIUS MS-CHAPv1 認証およびパスワード変更機能は、次の ID ソースを使用してサポートされます。

- 内部 ID ストア
- Microsoft Active Directory ID ストア

Microsoft Challenge Handshake Authentication Protocol Version 2

RADIUS MS-CHAPv2 認証およびパスワード変更機能は、次の ID ソースでサポートされます。

- 内部 ID ストア
- Microsoft Active Directory ID ストア

RADIUS ベースの EAP プロトコル

EAP では、さまざまな認証タイプをサポートする拡張可能なフレームワークが提供されます。ここでは、Cisco ISE でサポートされる EAP 方式について説明します。次のトピックを扱います。

単純な EAP 方式

- EAP-Message Digest 5
- Lightweight EAP

認証に Cisco ISE サーバー証明書を使用する EAP 方式

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

上記にリストした方式とは別に、サーバー認証とクライアント認証の両方に証明書を使用する EAP 方式があります。

RADIUS-Based EAP 認証フロー

認証プロセスで EAP が使用される場合は常に、そのプロセスよりも、具体的にどの EAP 方式（および該当する場合は内部方式）を使用する必要があるかを決定するネゴシエーションフェーズが先行します。EAP ベースの認証は、次のプロセスで発生します。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが EAP 要求をホストに送信します。
3. ホストは、EAP 応答によって、ネットワーク デバイスに応答します。
4. ネットワーク デバイスは、ホストから受信した EAP 応答を RADIUS Access-Request 内に（EAP-Message RADIUS 属性を使用して）カプセル化し、RADIUS Access-Request を Cisco ISE に送信します。
5. Cisco ISE は、RADIUS パケットから EAP 応答を抽出して新しい EAP 要求を作成し、この EAP 要求を RADIUS Access-Challenge 内に（この場合も EAP-Message RADIUS 属性を使用して）カプセル化し、ネットワーク デバイスに送信します。
6. ネットワーク デバイスは、EAP 要求を抽出し、ホストへ送信します。

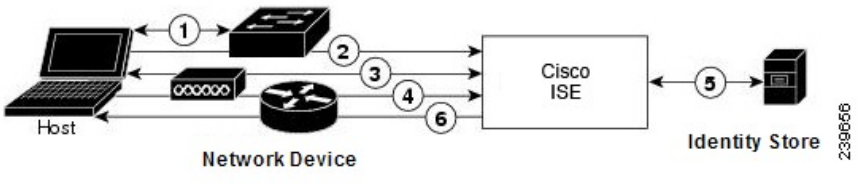
この方法で、ホストと Cisco ISE は間接的に EAP メッセージを交換します（EAP メッセージは、RADIUS を使用して転送され、ネットワーク デバイスを介して渡されます）。この方法で交換される EAP メッセージの最初のセットによって、特定の EAP 方式がネゴシエートされます。その後、認証を実行する場合に、この EAP 方式が使用されます。

その後交換される EAP メッセージは、実際の認証の実行に必要なデータを伝送するために使用されます。ネゴシエートされた特定の EAP 認証方式で必要な場合、Cisco ISE では ID ストアを使用してユーザー クレデンシャルを検証します。

Cisco ISE では、認証が成功か失敗かを決定した後、EAP-Success または EAP-Failure メッセージを、RADIUS Access-Accept または Access-Reject メッセージ内にカプセル化された状態で、ネットワーク デバイスに（最終的にはホストにも）送信します。

次の図は、EAP を使用する RADIUS ベースの認証を示しています。

***Figure 6: EAP* を使用する *RADIUS* ベースの認証**



Extensible Authentication Protocol-Message Digest 5

Extensible Authentication Protocol-Message Digest 5（EAP-MD5）では、一方向のクライアント認証が提供されます。サーバーは、クライアントにランダムチャレンジを送信します。クライアントは、チャレンジとそのパスワードを MD5 で暗号化することによって、応答でその ID を証明します。中間者がチャレンジと応答を見ることができるため、EAP-MD5 は、公開メディアで使用される場合にはディクショナリ攻撃に対して脆弱です。サーバー認証が行われないため、スプーフィングに対しても脆弱です。Cisco ISE では、Cisco ISE 内部 ID ストアに対する EAP-MD5 認証がサポートされます。EAP-MD5 プロトコルを使用している場合は、ホストルックアップもサポートされます。

Lightweight Extensible Authentication Protocol

Cisco ISE では現在、Lightweight Extensible Authentication Protocol（LEAP）を Cisco Aironet ワイヤレス ネットワーキングに対してだけ使用します。このオプションを有効にしないと、LEAP 認証を実行するように設定された Cisco Aironet エンドユーザー クライアントは、ネットワークにアクセスできなくなります。Cisco Aironet エンドユーザー クライアントすべてが Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）などの異なる認証プロトコルを使用する場合は、このオプションを無効にすることを推奨します。

（注） [ネットワーク デバイス（Network Devices）] セクションで RADIUS（Cisco Aironet）デバイスとして定義された AAA クライアントを使用してユーザーがネットワークにアクセスする場合は、LEAP、EAP-TLS、またはその両方を有効にする必要があります。これ以外の場合、Cisco Aironet ユーザーは認証を受けることができません。

保護拡張認証プロトコル

保護拡張認証プロトコル（PEAP）では、相互認証が提供され、脆弱なユーザー クレデンシャルの機密性と整合性が保証されます。またこのプロトコルでは、自身をパッシブ（盗聴）およ

びアクティブ（中間者）攻撃から保護し、セキュアに暗号キー関連情報を生成します。PEAP は、IEEE 802.1X 標準および RADIUS プロトコルと互換性があります。Cisco ISE では、Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol（EAP-MS-CHAP）、Extensible Authentication Protocol-Generic Token Card（EAP-GTC）、および EAP-TLS 内部方式で PEAP バージョン 0（PEAPv0）と PEAP バージョン 1（PEAPv1）がサポートされます。Cisco Secure Services Client（SSC）サプリカントでは、Cisco ISE でサポートされるすべての PEAPv1 内部方式がサポートされます。

PEAP の使用の利点

PEAP を使用すると、次のような利点があります。PEAP は、広く実装されセキュリティが細部にわたって確認された TLS に基づいています。キーを生成しない方式に対しては、キーを確立します。トンネル内で ID を送信します。内部方式の交換と結果メッセージを保護します。フラグメンテーションがサポートされます。

PEAP プロトコルでサポートされているサプリカント

PEAP では、次のサプリカントがサポートされます。

- Microsoft Built-In Clients 802.1X XP
- Microsoft Built-In Clients 802.1X Vista
- Cisco Secure Services Client（SSC）Release 4.0
- Cisco SSC リリース 5.1
- Funk Odyssey Access Client リリース 4.72
- Intel リリース 12.4.0.0

PEAP プロトコルのフロー

PEAP カンバセーションは、次の 3 つの部分に分かれます。

1. Cisco ISE とピアが TLS トンネルを構築します。Cisco ISE は自身の証明書を提示しますが、ピアは提示しません。ピアと Cisco ISE はキーを作成して、トンネル内のデータを暗号化します。
2. 内部方式によって、次のようにトンネル内のフローが決定されます。
   - EAP-MS-CHAPv2 内部方式：EAP-MS-CHAPv2 パケットは、ヘッダーなしでトンネル内を移動します。ヘッダーの先頭のバイトにタイプ フィールドが含まれます。EAP-MS-CHAPv2 内部方式では、パスワード変更機能がサポートされます。ユーザーが管理者ポータルでパスワードの変更を試行できる回数を設定できます。ユーザー認証の試行回数はこの数値によって制限されます。
   - EAP-GTC 内部方式：PEAPv0 と PEAPv1 の両方で、EAP-GTC 内部方式がサポートされます。サポートされるサプリカントでは、EAP-GTC 内部方式を使用する PEAPv0 はサポートされません。EAP-GTC では、パスワード変更機能がサポートされます。ユーザーが管理者ポータルでパスワードの変更を試行できる回数を設定できます。ユーザー認証の試行回数はこの数値によって制限されます。

- EAP-TLS 内部方式：Windows 組み込みサプリカントでは、トンネルが確立された後のメッセージのフラグメンテーションはサポートされず、このことは EAP-TLS 内部方式に影響を与えます。Cisco ISE では、トンネルが確立された後の外部 PEAP メッセージのフラグメンテーションはサポートされません。トンネルの確立中、フラグメンテーションは PEAP のマニュアルで指定されているとおりに動作します。PEAPv0 では EAP-TLS パケットのヘッダーが削除され、PEAPv1 では EAP-TLS パケットがそのまま送信されます。
- Extensible Authentication Protocol-type, length, value（EAP-TLV）拡張：EAP-TLV パケットはそのまま送信されます。EAP-TLV パケットは、トンネル内をヘッダー付きで移動します。

3. カンバセーションが内部方式に到達した場合、保護された成功と失敗の確認応答があります。

   クライアント EAP メッセージは常に RADIUS Access-Request メッセージで送信され、サーバー EAP メッセージは常に RADIUS Access-Challenge メッセージで送信されます。EAP-Success メッセージは、常に RADIUS Access-Accept メッセージで送信されます。EAP-Failure メッセージは、常に RADIUS Access-Reject メッセージで送信されます。クライアント PEAP メッセージをドロップすると、RADIUS クライアント メッセージがドロップされます。

（注） Cisco ISE は、PEAPv1 通信中に EAP-Success または EAP-Failure メッセージの確認を要求します。ピアは、成功または失敗メッセージの受信を確認するために空の TLS データ フィールドを含む PEAP パケットを返送する必要があります。

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）は、相互認証を提供する認証プロトコルであり、共有秘密を使用してトンネルを確立します。このトンネルは、パスワードに基づく弱い認証方式を保護するために使用されます。Protected Access Credentials（PAC）キーと呼ばれる共有秘密は、トンネルのセキュリティを確保するときにクライアントとサーバを相互認証するために使用されます。

EAP-FAST の利点

EAP-FAST は、他の認証プロトコルに比べて次の利点があります。

- 相互認証：EAP サーバーはピアの ID と信頼性を確認できる必要があり、ピアは EAP サーバーの信頼性を確認できる必要があります。
- パッシブ ディクショナリ攻撃に対する耐性：多くの認証プロトコルでは、ピアから EAP サーバーにパスワードがクリア テキストまたはハッシュとして明示的に提供される必要があります。
- 中間者攻撃に対する耐性：相互認証された保護トンネルの確立時に、プロトコルは、ピアと EAP サーバーとの間のカンバセーションに攻撃者が情報を挿入することを防ぐ必要があります。

- MS-CHAPv2 や汎用トークン カード（GTC）などの多くの異なるパスワード認証インターフェイスをサポートできる柔軟性：EAP-FAST は、同じサーバーで複数の内部プロトコルをサポートできる拡張可能なフレームワークです。
- 効率性：無線メディアを使用する場合、ピアは計算資源と電源リソースを制限されます。EAP-FAST では、ネットワーク アクセス通信の計算を軽量化できます。
- 認証サーバーのユーザーごとの認証状態要件の最小化：大規模な展開では、通常、多くのサーバーが多くのピアに対する認証サーバーとして機能する必要があります。ユーザー名とパスワードを使用してネットワークにアクセスするのと同じように、ピアが同じ共有秘密を使用してトンネルのセキュリティを確保することも強く推奨されます。EAP-FAST により、サーバーでキャッシュおよび管理する必要があるユーザーごとおよびデバイスごとの状態を最小にすることができ、ピアによる強力な単一共有秘密の使用が容易になります。

EAP-FAST フロー

EAP-FAST プロトコルのフローは常に、次のフェーズを組み合わせたものになります。

1. プロビジョニング フェーズ：これは EAP-FAST のフェーズ 0 です。このフェーズでは、Cisco ISE とピアとの間で共有される、PAC と呼ばれる一意の強力な秘密を使用して、ピアがプロビジョニングされます。
2. トンネル確立フェーズ：PAC を使用して新しいトンネル キーを確立することによって、クライアントとサーバーを相互認証します。トンネル キーはその後、残りのカンバセーションを保護するために使用され、メッセージの機密性と信頼性を提供します。
3. 認証フェーズ：認証がトンネル内で処理され、セッション キーの生成と保護された終了が行われます。Cisco ISE では、EAP-FAST バージョン 1 および 1a がサポートされます。

シスコ以外のデバイスからの MAB の有効化

次の設定を順番に設定して、シスコ以外のデバイスから MAB を設定します。

ステップ 1 認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。プロファイラ サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。

ステップ 2 シスコ以外のデバイス（PAP、CHAP、EAP-MD5）で使用される MAC 認証のタイプに基づいて、ネットワーク デバイス プロファイルを作成します。

a) [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）] の順に選択します。
b) [追加（Add）] をクリックします。
c) ネットワーク デバイス プロファイルの名前と説明を入力します。
d) [ベンダー（Vendor）] ドロップダウン リストからベンダー名を選択します。
e) デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスが RADIUS をサポートする場合は、ネットワーク デバイスで使用する RADIUS ディクショナリを選択します。

f) [認証/許可（Authentication/Authorization）]セクションを展開し、フロータイプ、属性エイリアシング、およびホスト ルックアップに関するデバイスのデフォルト設定を行います。

g) [ホスト ルックアップ（MAB）（Host Lookup (MAB)）] セクションで、次を実行します。

- [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、また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。

- [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。

- [EAP-MD5 経由（Via 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。

h) [アクセス許可（Permissions）]、[認可変更（CoA）（Change of Authorization (CoA)）]、[リダイレクト（Redirect）] のセクションで必要な詳細を入力して、[送信（Submit）] をクリックします。

カスタム NAD プロファイルを作成する方法については、『Network Access Device Profiles with Cisco Identity Services Engine』を参照してください。

ステップ 3 **[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）]** を選択します。

ステップ 4 MAB を有効にするデバイスを選択して、[編集（Edit）] をクリックします。

ステップ 5 [ネットワーク デバイス（Network Device）] ページの [デバイス プロファイル（Device Profile）] ドロップダウン リストから、手順 2 で作成したネットワーク デバイス プロファイルを選択します。

ステップ 6 [保存（Save）] をクリックします。

（注） Cisco NAD では、MAB および Web/ユーザー認証に使用する Service-Type 値は異なります。これにより、Cisco NAD を使用する場合に、ISE は MAB と Web 認証を区別できます。シスコ以外の一部の NAD では、MAB と Web/ユーザー認証に同じ値の Service-Type 属性を使用しています。この場合、アクセスポリシーでセキュリティ上の問題につながる場合があります。シスコ以外のデバイスで MAB を使用する場合は、ネットワーク セキュリティが侵害されないように、追加の許可ポリシー ルールを設定することを推奨します。たとえば、プリンタで MAB を使用する場合は、ACL のプリンタ プロトコル ポートに制限する許可ポリシー ルールを設定できます。

シスコ デバイスからの MAB の有効化

次の設定を順番に設定して、シスコ デバイスから MAB を設定します。

ステップ 1 認証されたエンドポイントの MAC アドレスが、エンドポイント データベースで使用可能なことを確認します。プロファイラ サービスによって、これらのエンドポイントを追加したり、自動的にプロファイリングしたりできます。

ステップ 2 シスコ デバイス（PAP、CHAP、EAP-MD5）で使用される MAC 認証のタイプに基づいて、ネットワーク デバイス プロファイルを作成します。

a) [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）] を 選択します。

b) [追加（Add）] をクリックします。

c) ネットワーク デバイス プロファイルの名前と説明を入力します。

d) デバイスがサポートするプロトコルのチェックボックスをオンにします。デバイスが RADIUS をサポートする場合は、ネットワーク デバイスで使用する RADIUS ディクショナリを選択します。

e) [認証/許可（Authentication/Authorization）] セクションを展開し、フロータイプ、属性エイリアシング、およびホスト ルックアップに関するデバイスのデフォルト設定を行います。

f) [ホスト ルックアップ（MAB）（Host Lookup (MAB)）] セクションで、次を実行します。

- [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。

  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、また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。

- [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。

- [EAP-MD5 経由（Via 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。

g) [アクセス許可（Permissions）]、[認可変更（CoA）（Change of Authorization (CoA)）]、[リダイレクト（Redirect）] のセクションで必要な詳細を入力して、[送信（Submit）] をクリックします。

カスタム NAD プロファイルを作成する方法については、『Network Access Device Profiles with Cisco Identity Services Engine』を参照してください。

ステップ 3 **[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）]** を選択します。

ステップ 4 MAB を有効にするデバイスを選択して、[編集（Edit）] をクリックします。

ステップ 5 [ネットワーク デバイス（Network Device）] ページの [デバイス プロファイル（Device Profile）] ドロップダウン リストから、手順 2 で作成したネットワーク デバイス プロファイルを選択します。

ステップ 6 [保存（Save）] をクリックします。

ISE コミュニティ リソース

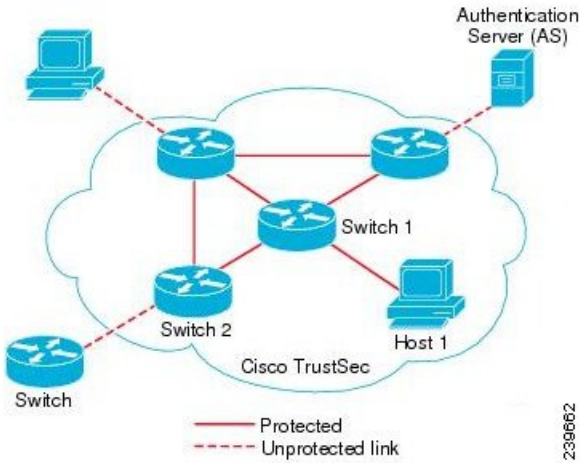
IP フォンの認証機能については、「Phone Authentication Capabilities」を参照してください。

TrustSec アーキテクチャ

Cisco TrustSec ソリューションでは、信頼ネットワーク デバイスのクラウドを確立して、セキュアなネットワークを構築します。Cisco TrustSec クラウド内の個々のデバイスは、そのネイバー（ピア）によって認証されます。TrustSec クラウド内のデバイス間の通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。TrustSec ソリューションでは、認証中に取得したデバイスおよびユーザー ID 情報を使用して、ネットワークに入ってきたパケットを分類（色付け）します。このパケット分類は、パケットが TrustSec ネットワークに入ってきたときに、そのパケットにタグ付けすることによって維持されます。これにより、パケットはデータ パス全体で正しく識別され、セキュリティおよびその他のポリシー基準が適用されるようになります。このタグは、セキュリティ グループ タグ（SGT）と呼ばれることもあります。エンドポイント デバイスで SGT に応じてトラフィックをフィルタリングできるようにすることにより、Cisco ISE でアクセス コントロール ポリシーを適用できるようになります。

次の図に、TrustSec ネットワーク クラウドの例を示します。

図 7: *TrustSec* アーキテクチャ



ISE コミュニティ リソース

Cisco TrustSec を使用してネットワーク セグメンテーションを簡素化、セキュリティを強化する方法については、「Simplify Network Segmentation with Cisco TrustSec」と「Policy-Based Software Defined Segmentation and Cisco TrustSec Improve Security White Paper」を参照してください。

Cisco TrustSec プラットフォーム サポート マトリックスのリストについては、「Cisco TrustSec Platform Support Matrix」を参照してください。

利用可能な TrustSec のサポート ドキュメントのリストについては、「Cisco TrustSec」を参照してください。

TrustSec コミュニティ リソースのリストについては、TrustSec Communityを参照してください。

TrustSec のコンポーネント

主な TrustSec のコンポーネント：

- ネットワーク デバイス アドミッション コントロール（NDAC）：信頼ネットワークでは、認証中に、TrustSec クラウド内にある各ネットワーク デバイス（イーサネット スイッチなど）のクレデンシャルおよび信頼性が、そのピア デバイスによって検証されます。NDAC は IEEE 802.1X ポートベース認証を使用し、その拡張認証プロトコル（EAP）方式として Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）を使用します。NDAC プロセスの認証および許可が成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションが実行されます。Cisco ISE では、IOS XE 17.1 以降のスイッチング プラットフォームおよび IOS XE 17.6 以降のルーティング プラットフォームのための CTS プロビジョニング（EAP-FAST）TLSv1.2 のサポートが用意されています。
- エンドポイント アドミッション コントロール（EAC）：TrustSec クラウドに接続しているエンドポイント ユーザーまたはデバイスの認証プロセス。EAC は一般的にアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可が成功すると、ユーザーまたはデバイスに対する SGT 割り当てが実行されます。認証および許可の EAC アクセス方法には次のものがあります。
  - 802.1X ポートベースの認証
  - MAC 認証バイパス（MAB）
  - Web 認証（WebAuth）
- セキュリティ グループ（SG）：アクセス コントロール ポリシーを共有するユーザー、エンドポイント デバイス、およびリソースのグループ。SG は、管理者が Cisco ISE で定義します。新規ユーザーおよびデバイスが TrustSec ドメインに追加されると、Cisco ISE では、これらの新規エントリを適切なセキュリティ グループに割り当てます。

- セキュリティ グループ タグ（SGT）：TrustSec サービスは各セキュリティ グループに、その範囲が TrustSec ドメイン内でグローバルな一意のセキュリティ グループ番号（16 ビット）を割り当てます。スイッチ内のセキュリティ グループの数は、認証されたネットワーク エンティティの数に制限されます。セキュリティ グループ番号を手動で設定する必要はありません。これらは自動的に生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。
- セキュリティ グループ アクセス コントロール リスト（SGACL）：SGACL では、割り当てられている SGT に基づいてアクセスおよび権限を制御できます。権限をロールにまとめることにより、セキュリティ ポリシーの管理が容易になります。デバイスを追加するときに、1 つ以上のセキュリティ グループを割り当てるだけで、即座に適切な権限が付与されます。セキュリティ グループを変更することにより、新しい権限を追加したり、現在の権限を制限することもできます。
- セキュリティ交換プロトコル（SXP）：SGT 交換プロトコル（SXP）は、TrustSec サービス用に開発されたプロトコルで、SGT 対応ハードウェアをサポートしていないネットワーク デバイス間で、SGT/SGACL をサポートしているハードウェアに IP-SGT バインディングを伝播します。
- 環境データのダウンロード：TrustSec デバイスは、初めて信頼ネットワークに参加するときに、その環境データを Cisco ISE から取得します。デバイス上の一部のデータは、手動で設定することもできます。デバイスでは、期限切れになる前に環境データを更新する必要があります。TrustSec デバイスは、次の環境データを Cisco ISE から取得します。
  - サーバー リスト：クライアントがその後の RADIUS 要求に使用できるサーバーのリスト（認証および許可の両方）
  - デバイス SG：そのデバイス自体が属しているセキュリティ グループ
  - 有効期間：TrustSec デバイスが環境データをダウンロードまたはリフレッシュする頻度を制御する期間
- ID とポートとのマッピング：エンドポイントの接続先のポートでスイッチが ID を定義するための方法で、この ID を使用して Cisco ISE サーバー内の特定の SGT 値が検索されます。

TrustSec の用語

次の表は、TrustSec ソリューションで使用される一般的な用語の一部と、TrustSec 環境でのその意味を示しています。

***Table 13: TrustSec* の用語**

用語	意味
サプリカント	信頼ネットワークへの参加を試行するデバイス。

用語	意味
認証	信頼ネットワークへの参加を許可する前に、各デバイスの ID を検証するプロセス。
許可	信頼ネットワーク上のリソースへのアクセスを要求しているデバイスに対し、デバイスの認証IDに基づいてアクセスのレベルを決定するプロセス。
アクセス コントロール	各パケットに割り当てられている SGT に基づいて、パケットごとにアクセス コントロールを適用するプロセス。
セキュアな通信	信頼ネットワーク内の各リンクを経由して流れるパケットをセキュリティで保護するための、暗号化、整合性、データパス リプレイ保護のプロセス。
TrustSec デバイス	TrustSec ソリューションをサポートする Cisco Catalyst 6000 シリーズまたは Cisco Nexus 7000 シリーズのスイッチ。
TrustSec 対応デバイス	TrustSec 対応デバイスは、TrustSec 対応のハードウェアとソフトウェアを備えています。たとえば、Nexus オペレーティング システムを搭載した Nexus 7000 シリーズ スイッチなどです。
TrustSec シード デバイス	Cisco ISE サーバーに対して直接認証を行う TrustSec デバイス。オーセンティケータとサプリカントの両方として機能します。
受信側	Cisco TrustSec ソリューションが有効になっているネットワーク内の TrustSec 対応デバイスにパケットが初めて到達すると、SGT を使用してパケットにタグが付けられます。この信頼ネットワークへの入り口点を入力と呼びます。
送信側	Cisco TrustSec ソリューションが有効になっているネットワーク内の最後の TrustSec 対応デバイスをパケットが通過すると、タグが解除されます。この信頼ネットワークからの出口点を出力と呼びます。

TrustSec のサポートされるスイッチと必要なコンポーネント

Cisco TrustSec ソリューションが有効になった Cisco ISE ネットワークを設定するには、TrustSec ソリューションおよび他のコンポーネントをサポートするスイッチが必要です。スイッチ以外に、IEEE 802.1X プロトコルを使用した ID ベースのユーザー アクセス コントロールには、その他のコンポーネントも必要です。TrustSec をサポートするシスコ スイッチのプラットフォームおよび必要なコンポーネントの完全な最新のリストについては、「Cisco TrustSec-Enabled Infrastructure」を参照してください。

Cisco Catalyst Center との統合

Catalyst Center は、Cisco ISE との信頼された通信リンクを作成するメカニズムを備えており、Cisco ISE と安全な方法でデータを共有できます。Cisco ISE が Catalyst Center に登録されると、Catalyst Center が検出したすべてのデバイスが、関連する設定やその他のデータとともに Cisco ISE にプッシュされます。Catalyst Center を使用してデバイスを検出し、Catalyst Center と Cisco ISE の両方の機能を検出されたデバイスに適用できます。これは、検出されたデバイスが両方のアプリケーションに表示されるためです。Catalyst Center デバイスと Cisco ISE デバイスは、すべてそのデバイス名で一意に識別されます。

Cisco ISE への Catalyst Center の接続

Cisco ISE 用の Catalyst Center の設定の詳細については、『Cisco Catalyst Center Installation Guide』[英語] を参照してください。

このセクションでは、Catalyst Center 向けの Cisco ISE 設定に関する追加情報について説明します。

- パスワード：Catalyst Center は、Cisco ISE に接続するときに、Cisco ISE 管理者のユーザー名とパスワードを使用します。システムパスワードの詳細については、Cisco ISE への管理アクセスを参照してください。

（注） 2.2.1.0 より前の Catalyst Center バージョンでは、Cisco ISE CLI を使用して初期統合手順を実行していたため、Cisco ISE CLI と管理者のユーザー名およびパスワードは同じである必要がありました。Catalyst Center リリース 2.2.1.0 以降では、Cisco ISE CLI の使用が廃止されているため、Cisco ISE CLI と管理者のユーザー名およびパスワードを同じにする必要はありません。

- API：Cisco ISE で外部 RESTful サービス（ERS）API を有効にする必要があります。Cisco ISE で [セキュリティの強化に CSRF チェックを使用する（Use CSRF Check for Enhanced Security）] オプションが無効になっていることを確認してください。
- pxGrid：Cisco ISE は pxGrid コントローラで、Catalyst Center はサブスクライバです。Cisco ISE と Catalyst Center の両方で、SGT と SGACL 情報が含まれる Trustsec（SD-Access）コ

ンテンツをモニターします。Cisco ISE と Catalyst Center 間でシステムクロックを同期してください。Cisco ISE の pxGrid の詳細については、Cisco pxGridノードを参照してください。

（注） Cisco ISE 2.4 以降では、pxGrid 2.0 および pxGrid 1.0 がサポートされています。pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Catalyst Center は現在 2 つを超える pxGrid ノードをサポートしていません。

- Cisco ISE IP アドレス：Cisco ISE PAN と Catalyst Center 間は直接接続する必要があります。プロキシ、ロードバランサ、または仮想 IP アドレスを使用することはできません。

  Cisco ISE がプロキシを使用していないことを確認します。使用している場合は、プロキシから Catalyst Center の IP を除外してください。

- SXP：Catalyst Center に SXP は必要ありません。Cisco ISE と Catalyst Center 管理対象ネットワークを接続する場合に SXP を有効にすると、Cisco ISE は Trustsec（SD-Access）がハードウェアでサポートされないネットワークデバイスと通信できます。

（注） TrustSec をサポートするように Cisco ISE 展開を設定する場合、または Cisco ISE が Catalyst Center と統合されている場合は、ポリシーサービスノードを SXP 専用として設定しないでください。SXP は、TrustSec デバイスと非 Trustsec デバイス間のインターフェイスです。TrustSec 対応ネットワークデバイスとは通信しません。

- Cisco ISE との接続用の証明書：
  - Cisco ISE 管理証明書では、件名または SAN に Cisco ISE IP または FQDN を含める必要があります。
  - ECDSA は、SSH キー、ISE SSH アクセス、または Catalyst Center と Cisco ISE の接続用の証明書ではサポートされません。
  - Catalyst Centerの自己署名証明書では、cA:TRUE (RFC5280 section-4.2.19) の Basic Constraints 拡張を使用する必要があります。

（注） 2.2.1.0 より前の Catalyst Center リリースでは、SSH を有効にする必要がありました。Catalyst Center リリース 2.2.1.0 以降、SSH の使用は廃止されたため、SSH を有効にする必要はありません。

TrustSec ダッシュボード

TrustSec ダッシュボードは、TrustSec ネットワークの一元化されたモニタリング ツールです。

TrustSec ダッシュボードには次のダッシュレットが含まれています。

- [メトリック（Metrics）] : [メトリック（Metrics）] ダッシュレットには、TrustSec ネットワークの動作に関する統計情報が表示されます。
- [アクティブなSGTセッション（Active SGT Sessions）] : [アクティブなSGTセッション（Active SGT Sessions）] ダッシュレットには、ネットワークで現在アクティブな SGT セッションが表示されます。[アラーム（Alarms）] ダッシュレットには、TrustSec セッション関連のアラームが表示されます。
- アラーム
- [NAD/SGTクイックビュー（NAD / SGT Quick View）] : [クイックビュー（Quick View）] ダッシュレットには、NAD および SGT の TrustSec 関連情報が表示されます。
- TrustSecセッション/NADアクティビティライブログ（TrustSec Sessions / NAD Activity Live Log）：アクティブな TrustSec セッションを表示するには、[ライブログ（Live Log）] ダッシュレットの [TrustSecセッション（TrustSec Sessions）] リンクをクリックします。また、NAD から Cisco ISE への TrustSec プロトコル データ要求と応答に関する情報を表示することもできます。

メトリック

このセクションには、TrustSec ネットワークの動作に関する統計情報が表示されます。タイムフレーム（たとえば、過去 2 時間、過去 2 日 など）とチャート タイプ（たとえば、棒、折れ線、スプラインなど）を選択できます。

最新のバー値がグラフに表示されます。また、前のバーからのパーセンテージの変化も表示されます。バー値に増加がある場合、プラス記号付きの緑色で表示されます。値に減少がある場合、マイナス記号付きの赤色で表示されます。

値が計算された時刻とその正確な値を <Value:xxxx Date/Time: xxx> 形式で表示するには、グラフのバーにカーソルを置きます。

次のメトリックを表示できます。

SGTセッション（SGT sessions）	選択された時間内に作成された SGT セッションの総数が表示されます。 （注） SGT セッションは、認証フローの一部として SGT を受信したユーザー セッションです。

使用中のSGT（SGTs in use）	選択された時間内に使用された固有の SGT の総数が表示されます。たとえば、1 時間で 200 の TrustSec セッションがあったが、ISE が認証応答で 6 つのタイプの SGT でしか応答しなかった場合、グラフにはこの時間に値 6 が表示されます。
アラーム	選択された時間内に発生したアラームおよびエラーの総数が表示されます。エラーは赤色で表示され、アラームは黄色で表示されます。
使用中のNAD（NADs in use）	選択された時間内に TrustSec 認証に参加した固有の NAD の数が表示されます。

現在のネットワーク ステータス

このダッシュボードの中間部分には、TrustSec ネットワークの現在のステータスに関する情報が表示されます。グラフに表示される値は、ページがロードされると更新され、[ダッシュボードの更新（Refresh Dashboard）] オプションを使用して更新できます。

アクティブな SGT セッション

このダッシュレットには、ネットワークで現在アクティブなSGTセッションが表示されます。上位 10 個の最もよく使用されている SGT または最も使用頻度の低い SGT を表示できます。X 軸には SGT 使用率が表示され、Y 軸には SGT の名前が表示されます。

SGT の TrustSec セッションの詳細を表示するには、その SGT に対応するバーをクリックします。その SGT に関連する TrustSec セッションの詳細が [ライブログ（Live Log）] ダッシュレットに表示されます。

アラーム

このダッシュレットには、TrustSec セッション関連のアラームが表示されます。次の詳細情報を表示できます。

- [アラームのシビラティ（重大度）（Alarm Severity）]：アラームのシビラティ（重大度）レベルを示すアイコンが表示されます。
  - [高（High）]：TrustSec ネットワーク内の障害を示すアラームが含まれます（たとえば、PAC の更新が失敗したデバイスなど）。赤色のアイコンが付いています。
  - [中（Medium）]：ネットワーク デバイスの誤った設定を示す警告が含まれます（たとえば、CoA メッセージの受け入れを失敗したデバイスなど）。黄色でマークされます。
  - [低（Low）]：ネットワーク動作の一般情報および更新が含まれます（たとえば、TrustSec の設定変更など）。青色でマークされます。

- アラームの説明
- このアラーム カウンタが最後にリセットされてからアラームが発生した回数。
- アラームが最後に発生した時刻

クイック ビュー

[クイックビュー（Quick View）] ダッシュレットには、NAD の TrustSec 関連情報が表示されます。SGT の TrustSec 関連情報を表示することもできます。

NAD クイック ビュー

[検索（Search）] ボックスに詳細を表示する TrustSec ネットワーク デバイスの名前を入力し、**Enter** を押します。検索ボックスには自動入力機能があり、ユーザーがテキストボックスに入力すると、ドロップダウンに一致するデバイス名がフィルタされ表示されます。

次の情報がこのダッシュレットに表示されます。

- **[NDG（NDGs）]**：このネットワークデバイスが属するネットワーク デバイス グループ（NDG）がリストされます。
- **[IP アドレス（IP Address）]**：ネットワークデバイスの IP アドレスを表示します。[ライブログ（Live Logs）] ダッシュレットに NAD アクティビティの詳細を表示するには、このリンクをクリックします。
- **[アクティブセッション（Active sessions）]**：このデバイスに接続されているアクティブな TrustSec セッションの数がリストされます。
- **[PACの有効期限（PAC expiry）]**：PAC の失効日が表示されます。
- **[最後のポリシー更新（Last Policy Refresh）]**：ポリシーを最後にダウンロードした日付が表示されます。
- **[最後の認証（Last Authentication）]**：このデバイスの最後の認証レポートのタイムスタンプを表示します。が表示されます。
- **[アクティブSGT（Active SGTs）]**：このネットワークデバイスに関連するアクティブセッションで使用されている SGT がリストされます。カッコ内に表示される数字は、現在この SGT を使用しているセッションの数を示します。[ライブ ログ（Live Log）] ダッシュレットに TrustSec セッションの詳細を表示するには、SGT のリンクをクリックします。

[最新ログの表示（Show Latest Logs）] オプションを使用して、デバイスの NAD アクティビティのライブ ログを表示できます。

SGT クイック ビュー

[検索（Search）] ボックスに詳細を表示する SGT の名前を入力し、**Enter** を押します。

次の情報がこのダッシュレットに表示されます。

- **[値（Value）]**：SGT 値（10 進数と 16 進数の両方）が表示されます。

- **[アイコン（Icon）]**：この SGT に割り当てられているアイコンが表示されます。
- **[アクティブセッション（Active sessions）]**：現在この SGT を使用しているアクティブなセッションの数がリストされます。
- **[固有ユーザー（Unique users）]**：この SGT をアクティブセッションに保持する固有ユーザー名の数がリストされます。
- **[更新されたNAD（Updated NADs）]**：この SGT のポリシーをダウンロードした NAD の数がリストされます。

ライブ ログ

アクティブな TrustSec セッション（応答の一部として SGT があるセッション）を表示するには [TrustSecセッション（TrustSec Sessions）]リンクをクリックします。

NAD から Cisco ISE への TrustSec プロトコルデータ要求と応答に関する情報を表示するには、[NAD アクティビティ（NAD Activity）] リンクをクリックします。

[ACI エンドポイント アクティビティ（ACI endpoint Activity）] リンクをクリックして、Cisco ISE が Cisco ACI から学習した IP-SGT 情報を表示します。

TrustSec のグローバル設定

Cisco ISE が TrustSec サーバーとして機能して TrustSec サービスを提供するには、いくつかのグローバル TrustSec 設定を定義する必要があります。

始める前に

- TrustSec グローバル設定を設定する前に、グローバル EAP-FAST 設定が定義されていることを確認します（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-FAST]** > **[EAP-FAST 設定（EAP-FAST Settings）]** を選択）。

  [機関識別情報の説明（Authority Identity Info Description）] を Cisco ISE サーバー名に変更することができます。この説明は、クレデンシャルをエンドポイントクライアントに送信する Cisco ISE サーバーを説明したわかりやすい文字列にします。Cisco TrustSec アーキテクチャのクライアントには、IEEE 802.1X 認証の EAP 方式として EAP-FAST を実行するエンドポイント、または Network Device Access Control（NDAC）を実行するサプリカント ネットワーク デバイスのいずれも使用できます。クライアントは、この文字列を Protected Access Credentials（PAC）Type-Length-Value（TLV）情報で認識できます。デフォルト値は、Identity Services Engine です。NDAC 認証時に、ネットワーク デバイスで Cisco ISE PAC 情報が一意に識別されるように、この値を変更する必要があります。

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

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）] の順に選択します。

ステップ 2 フィールドに値を入力します。フィールドの詳細については、次を参照してください。 一般 TrustSec の設定 （128 ページ）

ステップ 3 [Save] をクリックします。

次のタスク

- TrustSec デバイスの設定 （134 ページ）

一般 TrustSec の設定

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。

- **[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 用のセキュリティグループタグの番号付け（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、「 自動セキュリティグループの作成がオンです（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**
  - **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

[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 （118 ページ）
TrustSec のコンポーネント （119 ページ）
TrustSec のグローバル設定 （127 ページ）

TrustSec マトリックスの設定

始める前に

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

ステップ 1 [ワークセンター（Work Centers）]>[TrustSec]>[設定（Settings）]>[TrustSecマトリックスの設定（TrustSec Matrix Settings）] の順に選択します。

ステップ 2 [TrustSecマトリックスの設定（TrustSec Matrix Settings）] ページに必要な詳細を入力します。

ステップ 3 [Save] をクリックします。

TrustSec マトリックスの設定

***Table 14: TrustSec* マトリックスの設定**

フィールド名	使用上のガイドライン
複数のSGACLを許可（Allow Multiple SGACLs）	セル内で複数の SGACL を許可するには、このチェックボックスをオンにします。このオプションが選択されていない場合、Cisco ISE はセル 1 つあたり 1 つの SGACL のみを許可します。 デフォルトでは、新たにインストールすると、このオプションはディセーブルになります。 アップグレード後、Cisco ISE は出力セルをスキャンし、複数の SGACL が割り当てられたセルを少なくとも 1 つ特定した場合、管理者に複数の SGACL をセルに追加することを許可します。それ以外の場合は、セル 1 つあたり 1 つの SGACL のみを許可します。 **Note** 複数の SGACL を無効にする前に、複数の SGACL を含むセルを 1 つの SGACL のみを含めるように編集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
モニタリングの許可（**Allow Monitoring**）	マトリクス内のすべてのセルのモニタリングをイネーブルにする場合は、このチェックボックスをオンにします。モニタリングがディセーブルの場合、[セルの編集（Edit Cell）] ダイアログで、[すべてをモニター（Monitor All）] アイコンはグレー表示され、[モニター（Monitor）] オプションはディセーブルになります。 デフォルトでは、新たにインストールすると、モニタリングはディセーブルになります。 **Note** マトリクス レベルでモニタリングをディセーブルにする前に、現在モニターされているセルのモニタリングをディセーブルにする必要があります。
SGT番号の表示（Show SGT Numbers）	マトリクス セルの SGT 値（10 進数および 16 進数の両方）を表示または非表示にするには、このオプションを使用します。 デフォルトでは、SGT 値はセルに表示されます。
アピアランス設定（**Appearance Settings**）	次のオプションを使用できます。 • [カスタム設定（Custom settings）] : デフォルトのテーマ（パターンなしの色）が最初に表示されます。独自の色とパターンを設定できます。 • [デフォルト設定（Default settings）] : パターンなしの色の事前に定義されたリスト（編集不可）。 • [アクセシビリティ設定（Accessibility settings）] : パターンありの色の事前に定義されたリスト（編集不可）。

フィールド名	使用上のガイドライン
色/パターン（Color/Pattern）	マトリックスを読み取りやすくするために、セルの内容に基づいて、マトリックス セルに色とパターンを適用できます。 使用可能な表示タイプは、次のとおりです。 • [IP を許可/IP ログを許可（Permit IP/Permit IP Log）]：セル内に設定されます。 • [IP を拒否/IP ログを拒否（Deny IP/Deny IP Log）]：セル内に設定されます。 • [SGACL（SGACLs）]：セル内に設定されている SGACL の場合。 • [IP を許可/IP ログを許可（継承）（Permit IP/Permit IP Log (Inherited)）]：デフォルトポリシーから取得されます（設定されていないセルの場合）。 • [IP を拒否/IP ログを拒否（継承）（Deny IP/Deny IP Log (Inherited)）]：デフォルトポリシーから取得されます（設定されていないセルの場合）。 • [SGACL（継承）（SGACLs (Inherited)）]：デフォルトポリシーから取得されます（設定されていないセルの場合）。

Related Topics

出力ポリシー （149 ページ）
マトリクス ビュー （150 ページ）
TrustSec マトリックスの設定 （132 ページ）

TrustSec デバイスの設定

Cisco ISE で TrustSec 対応デバイスからの要求を処理するには、これらの TrustSec 対応デバイスを Cisco ISE で定義しておく必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）] 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 [ネットワーク デバイス（Network Devices）] セクションで、必要な情報を入力します。

ステップ 4 TrustSec 対応デバイスを設定するために [高度な TrustSec 設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 5 [Submit] をクリックします。

OOB TrustSec PAC

すべての TrustSec ネットワーク デバイスで、EAP-FAST プロトコルの一部として TrustSec PAC が保持されています。これはセキュアなRADIUSプロトコルでも使用され、ここではRADIUS共有秘密が PAC で伝送されるパラメータから作成されます。これらのパラメータの 1 つである発信側 ID には、TrustSec ネットワーク デバイス ID、つまりデバイス ID が保持されます。

デバイスが TrustSec PAC を使用して識別される場合、Cisco ISE でそのデバイス用に設定されているデバイス ID と、PAC の発信側 ID が一致していない場合、認証に失敗します。

一部の TrustSec デバイス（Cisco ASA ファイアウォールなど）では EAP-FAST プロトコルをサポートしていません。したがって、Cisco ISE ではこれらのデバイスを EAP-FAST を介した TrustSec PAC でプロビジョニングできません。代わりに、TrustSec PAC は Cisco ISE 上で生成され、手動でデバイスにコピーされます。そのため、これをアウトオブバンド（OOB）TrustSec PAC 生成と呼びます。

Cisco ISE で PAC を生成すると、暗号キーで暗号化された PAC ファイルが生成されます。

ここでは、次の内容について説明します。

[設定（Settings）] 画面からの TrustSec PAC の生成

[設定（Settings）] 画面から TrustSec PAC を生成できます。

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

ステップ 2 左側の [設定（Settings）] ナビゲーション ペインの [プロトコル（Protocols）] をクリックします。

ステップ 3 **[EAP-FAST]** > **[PAC の生成（Generate PAC）]** を選択します。

ステップ 4 TrustSec PAC を生成します。

[ネットワーク デバイス（Network Devices）] 画面からの TrustSec PAC の生成

[ネットワーク デバイス（Network Devices）] 画面から TrustSec PAC を生成できます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 [追加（Add）] をクリックします。[ネットワーク デバイス（Network Devices）] ナビゲーション ペインのアクション アイコンから [新規デバイスの追加（Add new device）] をクリックすることもできます。

ステップ 3 新規デバイスを追加する場合は、デバイス名を入力します。

ステップ 4 TrustSec デバイスを設定するために [高度な TrustSec 設定（Advanced Trustsec Settings）] チェックボックスをオンにします。

ステップ 5 [アウトオブバンド（OOB）TrustSec PAC（Out of Band (OOB) TrustSec PAC）] サブ セクションで、[PAC の生成（Generate PAC）] をクリックします。

ステップ 6 次の詳細事項を入力します。

- [PAC 存続可能時間（PAC Time to Live）]：日、週、月、および年の単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。
- [暗号化キー（Encryption Key）]：暗号キーを入力します。キーの長さは 8 ～ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。

  暗号キーを使用して、生成されるファイルの PAC が暗号化されます。このキーは、デバイスで PAC ファイルを復号化する場合にも使用されます。したがって、後で使用できるように管理者が暗号キーを保存しておくことを推奨します。

  [ID（Identity）] フィールドは TrustSec ネットワーク デバイスのデバイス ID を示し、このフィールドには EAP-FAST プロトコルによって発信側 ID が提供されます。ここに入力した ID 文字列がネットワーク デバイスの作成ページの [TrustSec] セクションで定義されたデバイス ID と一致しない場合、認証は失敗します。

  有効期限は、PAC 存続可能時間に基づいて計算されます。

ステップ 7 [PAC の生成（Generate PAC）] をクリックします。

[ネットワーク デバイス リスト（Network Devices List）] 画面からの TrustSec PAC の生成

[ネットワーク デバイス リスト（Network Devices list）] 画面から TrustSec PAC を生成できます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [ネットワークデバイス（Network Devices）] の順に選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] をクリックします。

ステップ 3 TrustSec PAC を生成するデバイスの隣にあるチェックボックスをオンにし、[PAC の生成（Generate PAC）] をクリックします。

ステップ 4 フィールドで詳細を提供します。

ステップ 5 [PAC の生成（Generate PAC）] をクリックします。

[プッシュ（Push）] ボタン

出力ポリシーの [プッシュ（Push）] オプションは CoA 通知を開始します。この通知は、Cisco ISE からの出力ポリシー設定変更に関する更新を、ただちに要求するよう TrustSec デバイスに伝えます。

Cisco TrustSec AAA サーバーの設定

AAA サーバーリスト内に、Cisco Trustsec が有効になっている Cisco ISE サーバーのリストを設定すると、Cisco TrustSec デバイスの認証が、これらのサーバーのいずれに対しても実行されます。[プッシュ（Push）] をクリックすると、このリスト内の新しいサーバーが TrustSec デバイスにダウンロードされます。Cisco TrustSec デバイスは、認証を試行するときに、このリストから Cisco ISE サーバーを選択します。最初のサーバーがダウン状態またはビジー状態の場合、Cisco TrustSec デバイスはこのリストにある別の任意のサーバーに対してデバイス自体を認証できます。デフォルトでは、プライマリ Cisco ISE サーバーが Cisco TrustSec AAA サーバーです。より信頼性の高い Cisco TrustSec 環境を構築するために、より多くの Cisco ISE サーバーを設定することをお勧めします。

このページには、展開内の Cisco TrustSec AAA サーバーとして設定した Cisco ISE サーバーが一覧表示されます。

始める前に

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

ステップ 1 [Workcenters] > [TrustSec] > [Components] > [Trustsec Servers] > [Trustsec AAA Servers] 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 説明に従って値を入力します。

- [名前（Name）]：この AAA サーバーリスト内で Cisco ISE サーバーに割り当てる名前。この名前は、Cisco ISE サーバーのホスト名と異なっていてもかまいません。
- [説明（Description）]：任意の説明。
- [IP]：AAA サーバーリストに追加する Cisco ISE サーバーの IP アドレス。
- [ポート（Port）]：Cisco TrustSec デバイスとサーバー間の通信が行われるポート。デフォルトは 1812 です。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 表示される [AAA サーバー（AAA Servers）] ウィンドウで、[プッシュ（Push）] をクリックします。

次のタスク

セキュリティ グループを設定します。

TrustSec HTTPS サーバー

デフォルトでは、Cisco ISE が RADIUS を使用して Cisco ISE と TrustSec NAD 間で TrustSec 環境データを交換します。HTTPS を使用するように Cisco ISE を設定できます。これにより、RADIUS より高速で信頼性が高くなります。Cisco ISE は、REST API を使用して HTTP 転送を実装します。

HTTPS 転送には次が必要です。

- HTTPS サーバーと TrustSec ネットワークデバイス間でポート 9603 が開いていること。
- PSN に接続するすべてのネットワークデバイス上の HTTPS サーバーのクレデンシャルが一意であること。
- シスコのスイッチがバージョン16.12.2、17.1.1 以降を実行していること。

HTTPS 転送を設定するには、次の手順を実行します。

1. 各ネットワークデバイスで HTTP ファイル転送を有効にし、クレデンシャルを要求します。
2. Cisco ISE で、[TrustSec の全般設定（General TrustSec Settings）] で [ネットワークデバイスの TrustSec REST API サービス] を有効にします。
3. Cisco ISE で、各 PSN のネットワークデバイス定義を編集し、[HTTP REST API を有効にする（Enable HTTP REST API）] をオンにし、ネットワークデバイスの HTTP サーバーへのクレデンシャルを入力します。
4. Cisco ISE で、[TrustSec] > [コンポーネント（Components）] の下でそのネットワークデバイスを TrustSec HTTPs サーバーとして追加します。

（注） HTTPS に対して設定したノードが 1 つのみの場合は、HTTPS 用に設定されていない TrustSec サーバーは [TrustSec サーバー（TrustSec Servers）] リストに表示されません。展開内の他のすべての TrustSec 対応ノードを HTTPS 用に設定する必要があります。HTTPS 用に PSN が設定されていない場合は RADIUS が使用され、すべての Cisco ISE がこの TrustSec 展開のすべての PSN ノードをリストします。

設定が完了すると、Cisco ISE は [TrustSec] > [ネットワークデバイス（Network Devices）] で TrustSec 環境データに設定されているサーバーのリストを返します。

デバッグ

デバッグでの ERS を有効にします。この設定により、すべての ERS トラフィックがログに記録されます。ログファイルのオーバーロードを回避するために、この設定は 30 分以上有効にしたままにしないでください。

追加の監査情報を有効にするには、[TrustSec]>[設定（Settings）]>[TrustSec の全般設定（General TrustSec Settings）] の [ネットワークデバイス用 TrustSec REST API サービス（TrustSec REST API Service for Network Devices）] の下にある [要求ペイロードの本文を含める（Include request payload body）] をオンにします。一般 TrustSec の設定

Cisco ISE TrustSec HTTPS サーバーへの外部サーバーの追加

HTTPS サーバーリストに 1 つ以上の外部サーバーを追加することで、HTTPS TrustSec サービスのロードバランシングを実現できます。

外部サーバーは、次のいずれかの方法でロードバランサとして機能できます。

- **SSL ターミネーション**

  このセットアップでは、外部サーバーは、TrustSec 対応ネットワークデバイスによって開始された SSL 接続のターミネーションポイントです。同時に、サーバーは PSN ノードとの独自の SSL セッションを確立し、ネットワークデバイスと特定の PSN ノードの間で情報をリレーするプロキシとして機能します。したがって外部サーバーは、その IP アドレス、FQDN、またはその両方を含む証明書をホストする必要があります。この証明書は、ネットワークデバイスによって信頼されている必要があります。

  外部サーバーと PSN ノード間の SSL セッションの場合、外部サーバーは PSN ノードからの証明書を信頼する必要があります。この信頼の確立は、この目的で使用される製品に応じて、外部サーバーのデバイス固有設定の側面になります。

- **SSL パススルー**

  このセットアップでは、外部サーバーは IP アドレス変換デバイスとして機能し、ネットワークデバイスと PSN ノード間の通信を通過させるだけです。結果として外部サーバーには証明書が存在しないため、ネットワークデバイスと PSN ノードの間で証明書の信頼を確立させる必要があります。

  ネットワークデバイスは外部サーバーの IP アドレスを使用して SSL セッションを確立するため、この目的で PSN ノードが使用する証明書には、外部サーバーの IP アドレスが含まれている必要があります。これは、ワイルドカード証明書またはユニバーサル証明書を使用することで実現できます。ユニバーサル証明書の SAN エントリとして、複数の FQDN、IP アドレス、またはその両方を追加できます。

選択した展開オプションに関係なく、外部サーバーがネットワークデバイスから特定の PSN ノードへの通信を行う際は常に、その接続の永続性を確保する必要があります。つまり、その通信のすべてを、そのネットワークデバイスとその特定の PSN ノード間のみで行う必要があります。

始める前に

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

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。 [Work Centers] > [TrustSec] > [Components] > [TrustSec Servers] > [HTTPS Servers]

ステップ 2 [外部サーバーの追加（Add External Server）] をクリックします。

ステップ 3 次の詳細を入力します。

- [Name]：Cisco ISE HTTPS サーバーリストに追加する外部サーバーの名前。
- [Hostname (FQDN)]：外部サーバーのホスト名。

  （注） 外部サーバーのホスト名または IP アドレスのどちらを指定するか選択できます。

- [説明（Description）]：任意の説明。
- [Port]：Cisco TrustSec デバイスと外部サーバー間の通信が行われるポート。
- [IP Address]：Cisco ISE HTTPS サーバーリストに追加する外部サーバーの IP アドレス。

ステップ 4 [Add Certificate] をクリックします。

外部サーバーでロードバランシング操作とセキュア通信を有効にするには、SSL 証明書が必要です。ルート証明書から始まる信頼チェーンの順序に従って、証明書を追加します。

ステップ 5 [Certificate name] フィールドに名前を入力します。

ステップ 6 [Certificate] フィールドに SSL 証明書を追加します。これを行うには、ファイルを添付するか、クリップボードから証明書を貼り付けます。

ステップ 7 [Save] をクリックします。

通知バーに、次のメッセージを含むダイアログボックスが表示されます。

```
There are TrustSec configuration changes that have not been notified to network devices. To notify
the relevant network devices about these changes, click the push button.
```

ステップ 8 [プッシュ（Push）] をクリックします。

関連するネットワークデバイスに、これらの設定変更が通知されます。

これで、Cisco ISE HTTPS サーバーリストに外部サーバーが表示されるようになります。

セキュリティ グループの設定

セキュリティ グループ（SG）またはセキュリティ グループ タグ（SGT）は、TrustSec ポリシー設定で使用される要素です。SGT は、パケットが信頼ネットワーク内を移動する場合に付加さ

れます。これらのパケットは、信頼ネットワークに入ったとき（入力）にタグ付けされ、信頼ネットワークから離れるとき（出力）にタグ解除されます。

SGT は順次的な方法で生成されますが、IP と SGT とのマッピング用に SGT の範囲を予約しておくことができます。Cisco ISE は、SGT の生成時に予約済みの番号をスキップします。

TrustSec サービスはこれらの SGT を使用して、出力時に TrustSec ポリシーを適用します。

管理者ポータルで次のページからセキュリティ グループを設定できます。

- [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）]。
- **[設定（Configure）] > [新規セキュリティ グループの作成（Create New Security Group）]** の出力ポリシーページから直接。

[プッシュ（Push）] ボタンをクリックすると、複数の SGT を更新した後に、環境 CoA 通知を開始できます。この環境 CoA 通知はすべての TrustSec ネットワーク デバイスに送信され、ポリシー/データ リフレッシュ要求を開始することを強制します。

（注） [プッシュ（Push）] または [展開（Deploy）] ボタンを頻繁に使用することは推奨されません。マトリックスまたは SGACL に変更がある場合、次の展開操作を実行する前に、保留中の展開要求の通知バーを確認します。

Cisco ISE でのセキュリティグループの管理

前提条件

セキュリティグループを作成、編集、または削除するには、ネットワーク管理者またはシステム管理者である必要があります。

セキュリティグループの追加

1. **[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）]** を選択しますCisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。。
2. [追加（Add）] をクリックして新規セキュリティ グループを追加します。
3. 新規セキュリティ グループの名前と説明（オプション）を入力します。
4. この SGT を Cisco ACI に反映するには、[ACI に伝達（Propagate to ACI）] チェックボックスをオンにします。この SGT に関連する SXP マッピングは、Cisco ACI が [Cisco ACI の設定（Cisco ACI Settings）] ページで選択した VPN に所属している場合にのみ Cisco ACI に反映されます。

   このオプションはデフォルトでは無効になっています。

5. タグ値を入力します。タグ値は、手動で入力したり、自動生成されるようにしたり設定できます。またSGTの範囲を予約できます。これは、から設定できます。[一般TrustSecの設定（General TrustSec Settings）] ページ（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）]）。
6. [保存（Save）] をクリックします。

セキュリティグループの削除

送信元または宛先で使用中のセキュリティグループは削除できません。Cisco ISE の機能にマッピングされるデフォルトグループも削除できません。

- BYOD
- ゲスト
- TrustSec デバイス

Cisco ISE へのセキュリティ グループのインポート

カンマ区切り形式（CSV）ファイルを使用して Cisco ISE ノードにセキュリティ グループをインポートできます。Cisco ISE にセキュリティ グループをインポートする前に、テンプレートを更新する必要があります。同じリソースタイプのインポートを同時に実行できません。たとえば、2つの異なるインポートファイルから同時にセキュリティグループをインポートできません。

管理者ポータルからCSVテンプレートをダウンロードし、テンプレートにセキュリティグループの詳細を入力し、Cisco ISE にインポート可能な CSV ファイルとしてテンプレートを保存できます。

セキュリティ グループのインポート中、Cisco ISE で最初のエラーが発生した場合、インポート プロセスを停止できます。

ステップ 1 **[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）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 5 [インポート（Import）] をクリックします。

Cisco ISE からのセキュリティ グループのエクスポート

Cisco ISE で設定されたセキュリティ グループを CSV ファイル形式でエクスポートし、これを使用して別の Cisco ISE ノードにそれらのセキュリティ グループをインポートできます。

ステップ 1 [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）] を選択します。

ステップ 2 [エクスポート（Export）] をクリックします。

ステップ 3 セキュリティ グループをエクスポートするには、次のいずれかを実行できます。

- エクスポートするグループの隣にあるチェックボックスをオンにし、**[エクスポート（Export）] > [選択済みをエクスポート（Export Selected）]** を選択します。
- **[エクスポート（Export）] > [すべてエクスポート（Export All）]** を選択して、定義されたすべてのセキュリティ グループをエクスポートします。

ステップ 4 ローカル ハード ディスクに export.csv ファイルを保存します。

IP SGT スタティック マッピングの追加

IP-SGT スタティック マッピングを使用して、TrustSec デバイスと SXP ドメインに統一された方法でマッピングを展開することができます。新しい IP-SGT スタティック マッピングを作成するときに、このマッピングを展開する SXP ドメインとデバイスを指定できます。また、IP-SGT マッピングをマッピング グループに関連付けることもできます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）] 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 表示される [新規（New）] 領域で、ドロップダウンリストから [IP アドレス（IP Address）] または [ホスト名（Hostname）] を選択し、その横のフィールドに対応する値を入力します。

次の手順の [SGT に個別にマッピング（Map to SGT individually）] オプションで、マッピング先の SXP ドメインを指定できます。ただし、この手順で [ホスト名（Hostname）] を選択した場合、[SXP ドメインに送信（Send to SXP Domain）] フィールドにはアクセスできません。次の手順で SXP ドメインを追加するには、ここで [IP アドレス（IP Address）] を選択する必要があります。

ステップ 4 既存のマッピング グループを使用する場合は、[マッピング グループに追加（Add to a Mapping Group）] をクリックして、[マッピング グループ（Mapping Group）] ドロップダウン リストから必要なグループを選択します。

この IP アドレス/ホスト名を SGT に個別にマッピングする場合は、[SGT に個別にマッピング（Map to SGT Individually）] をクリックして以下を実行します。

- [SGT] ドロップダウン リストから SGT を選択します。

-
- マッピングを展開する必要がある SXP VPN グループを選択します。
- このマッピングを展開するデバイスを指定します。すべての TrustSec デバイス、選択されたネットワーク デバイス グループ、または選択されたネットワーク デバイスにマッピングを展開できます。

ステップ 5 [Save] をクリックします。

IP SGT スタティック マッピングの展開

マッピングを追加した後、[展開（Deploy）] オプションを使用して、対象のネットワーク デバイスでこのマッピングを展開します。マッピングをすでに保存している場合でも、これを明示的に行う必要があります。デバイスの展開ステータスを確認するには、[ステータスを確認（Check Status）] をクリックします。

ステップ 1 [ワークセンター（Work Centers）] タブから、[TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）] を選択します。

ステップ 2 展開するマッピングの近くにあるチェックボックスをオンにします。すべてのマッピングを展開する場合は、一番上のチェックボックスをオンにします。

ステップ 3 [展開（Deploy）] をクリックします。

すべての TrustSec デバイスが [IP SGTスタティックマッピングの展開（Deploy IP SGT Static Mapping）] ウィンドウにリストされます。

ステップ 4 選択したマッピングの展開先となる適切なデバイスまたはデバイス グループの横にあるチェックボックスをオンにします。

- すべてのデバイスを選択する場合は、一番上のチェックボックスをオンにします。
- フィルタリング オプションを使用して、特定のデバイスを検索します。
- デバイスを何も選択しない場合は、選択したマッピングがすべての TrustSec デバイスに展開されます。
- 新しいマッピングを展開するデバイスを選択すると、新しいマッピングの影響を受ける**すべて**のデバイスが ISE によって選択されます。

ステップ 5 [展開（Deploy）] をクリックします。[展開（Deploy）] ボタンをクリックすると、新しいマップによって影響を受けるすべてのデバイスのマッピングが更新されます。

[展開ステータス（Deployment Status）] ウィンドウに、デバイスが更新される順序と、エラーのために（またはデバイスが到達不能なために）更新されないデバイスが示されます。展開が完了すると、このウィンドウに、正常に更新されたデバイスの合計数と更新されないデバイスの数が表示されます。

[IP SGTスタティックマッピング（IP SGT Static Mapping）] ページの [ステータスを確認（Check Status）] オプションを使用して、特定のデバイスの同じ IP アドレスに複数の異なる SGT が割

り当てられているかどうかを確認します。このオプションを使用すると、競合するマッピングがあるデバイス、複数の SGT にマッピングされている IP アドレス、および同じ IP アドレスに割り当てられている複数の SGT を見つけることができます。展開でデバイス グループ、FQDN、ホスト名、または IPv6 アドレスが使用される場合でも、[ステータスを確認（Check Status）] オプションを使用できます。競合するマッピングを展開する前に、それらのマッピングを削除するか、展開の範囲を変更する必要があります。

IP SGT 静的マッピングでは IPv6 アドレスを使用できます。SSH または SXP を使用して、特定のネットワーク デバイスまたはネットワーク デバイス グループにこれらのマッピングを伝達できます。

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ステータスを検査する際に、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。

[一般TrustSecの設定（General TrustSec Settings）] ウィンドウの [ホスト名のIP SGTスタティックマッピング（IP SGT Static Mapping of Hostnames）] オプションを使用して、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数を指定します。次のオプションのいずれかを選択します。

- 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 returned by a DNS query）。

Cisco ISE への IP SGT スタティック マッピングのインポート

CSV ファイルを使用して IP SGT マッピングをインポートできます。

また、管理者ポータルからCSVテンプレートをダウンロードし、マッピングの詳細を入力し、CSV ファイルとしてテンプレートを保存して、Cisco ISE にインポートすることができます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）] の順に選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから CSV ファイルを選択します。

ステップ 4 [Upload] をクリックします。

Cisco ISE からの IP SGT スタティック マッピングのエクスポート

IP SGT マッピングを CSV ファイルの形式でエクスポートできます。このファイルを使用して、これらのマッピングを別の Cisco ISE ノードにインポートできます。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGTスタティックマッピング（IP SGT Static Mapping）] の順に選択します。

ステップ 2 次のいずれかを実行します。

- エクスポートするマッピングの隣にあるチェックボックスをオンにし、[エクスポート（Export）]>[選択済み（Selected）] を選択します。
- [エクスポート（Export）]>[すべて（All）] を選択して、すべてのマッピングをエクスポートします。

ステップ 3 ローカル ハード ディスクに mappings.csv ファイルを保存します。

SGT マッピング グループの追加

始める前に

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

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGT スタティックマッピング（IP SGT Static Mapping）] > [グループ管理（Manage Groups）] 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 マッピング グループの名前と説明を入力します。

ステップ 4 次の手順を実行します。

- [SGT] ドロップダウン リストから SGT を選択します。
-
- マッピングを展開する必要がある SXP VPN グループを選択します。
- マッピングを展開するデバイスを指定します。すべての TrustSec デバイス、選択されたネットワークデバイス グループ、または選択されたネットワーク デバイスにマッピングを展開できます。

ステップ 5 [保存（Save）] をクリックします。

あるマッピング グループから別のマッピング グループに IP SGT マッピングを移動できます。

また、マッピングおよびマッピング グループを更新または削除できます。マッピングまたはマッピング グループを更新するには、更新するマッピングまたはマッピング グループの横にあるチェック ボックスにマークを付けてから、[編集（Edit）] をクリックします。マッピングまたはマッピング グループを削除するには、削除するマッピングまたはマッピング グループの横にあるチェック ボックスにマークを付けてから、[ごみ箱（Trash）]>[選択済み（Selected）] の順にクリックします。マッピング グループが削除されると、そのグループ内の IP SGT マッピングも削除されます。

セキュリティ グループ アクセス コントロール リストの追加

始める前に

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

ステップ 1 **[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）]** を選択します。

ステップ 2 [追加（Add）] をクリックして新規セキュリティ グループ ACL を作成します。

ステップ 3 次の情報を入力します。

- [名前（Name）]：SGACL の名前
- [説明（Description）]：SGACL の説明（任意）
- [IP バージョン（IP Version）]：この SGACL でサポートされる IP バージョン：
  - [IPv4]：IP バージョン 4（IPv4）がサポートされます
  - [IPv6]：IP バージョン 6（IPv6）がサポートされます
  - [非認識（Agnostic）]：IPv4 と IPv6 の両方がサポートされます
- セキュリティ グループ ACL の内容：アクセス コントロール リスト（ACL）コマンド。次に例を示します。

  permit icmp

  deny ip

  ISE 内では SGACL 入力の構文が検査されません。スイッチ、ルータ、アクセス ポイントをエラーなく適用できるように、正しい構文を確実に使用してください。デフォルト ポリシーを **permit IP**、**permit ip log**、**deny ip**、または **deny ip log** として設定できます。TrustSec ネットワーク デバイスでは、デフォルト ポリシーを特定セルのポリシーの最後に付加します。

  参考用に SGACL の 2 つの例を示します。どちらにも最終的な catch-all ルールが含まれています。最初の例では、最終的な catch-all ルールとして拒否し、2 番目の例では許可します。

  Permit_Web_SGACL

  ```
  permit tcp dst eq 80
  permit tcp dst eq 443
  deny ip
  ```

  Deny_JumpHost_Protocols

  ```
  deny tcp dst eq 23
  deny tcp dst eq 23
  deny tcp dst eq 3389
  permit ip
  ```

  次の表に、IOS、IOS XE、NS OS オペレーティング システム用の SGACL の構文を示します。

SGACL CLI と ACE	IOS、IOS XE、NX OS で共通の構文
config acl	deny、exit、no、permit
拒否 許可	ahp、eigrp、gre、icmp、igmp、ip、nos、ospf、pcp、pim、tcp、udp
deny tcp deny tcp src deny tcp dst	dst、log、src
deny tcp dst eq deny tcp src eq	範囲は 0 ～ 65535
deny udp deny udp src deny udp dest	Dst、log、src
deny tcp dst eq www deny tcp src eq www	範囲は 0 ～ 65535

（注） Hypens は一部のシスコのスイッチでは許可されていません。したがって、`permit dst eq 32767-65535` は有効ではありません。`permit dst eq range 32767 65535` を使用します。一部の Cisco スイッチでは、コマンド構文に eq を含める必要がありません。したがって、それらのスイッチでは permit dst eq 32767-65535 は無効です。代わりに、permit dst 32767-65535 または permit dst range 32767 65535 を使用します。

ステップ 4 [プッシュ（Push）] をクリックします。
[プッシュ（Push）] オプションは CoA 通知を開始します。この通知は、Cisco ISE からの設定変更に関する更新をただちに要求するよう TrustSec デバイスに伝えます。

（注） Cisco ISE では次の事前定義済み SGACL を使用します：許可 IP、許可 IP ログ、拒否 IP、または拒否 IP ログ。これらの SGACL で GUI または ERS API を使用すると、TrustSec マトリックスを設定できます。これらの SGACL は GUI のセキュリティ グループ ACL リストのページに表示されませんが、ERS API を使用して利用可能な SGACL（ERS getAll 呼び出し）を表示すると表示されます。

出力ポリシー

出力テーブルには、送信元 SGT および宛先 SGT が、予約済みのものもそうでないものもあわせてリストされます。また、このページでは、出力テーブルをフィルタリングして特定のポリシーを表示することや、これらのプリセットフィルタを保存することもできます。送信元SGTから宛先SGTに到達しようとすると、TrustSec対応デバイスは、出力ポリシーで定義されているTrustSecポリシーに基づいてSGACLを適用します。Cisco ISEはポリシーを作成してプロビジョニングします。

TrustSecポリシーの作成に必要な基本的構築ブロックであるSGTおよびSGACLを作成した後に、SGACL を送信元 SGT および宛先 SGT に割り当てることによって、それらの関係を確立できます。

送信元 SGT と宛先 SGT のそれぞれの組み合わせが、出力ポリシーのセルになります。

出力ポリシーは、[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）] ページで表示できます。

それぞれ異なる 3 つの方法で出力ポリシーを表示できます。

- 送信元ツリー ビュー
- 宛先ツリー ビュー
- マトリクス ビュー

送信元ツリー ビュー

送信元ツリー ビューには、簡潔で組織化された送信元 SGT のビューが折りたたまれた状態で表示されます。送信元 SGT を展開すると、選択した送信元 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、宛先 SGT にマッピングされている送信元SGTのみが表示されます。特定の送信元SGTを展開すると、この送信元SGTにマッピングされているすべての宛先 SGT とその対応するポリシー（SGACL）がテーブルに表示されます。

一部のフィールドの横には、3 つのドット（...）が表示されます。これは、セルにより多くの情報が含まれていることを示しています。カーソルを 3 個のドットの上に置くと、クイック ビュー ポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

宛先ツリー ビュー

宛先ツリー ビューには、簡潔で組織化された宛先 SGT のビューが折りたたまれた状態で表示されます。宛先 SGT を展開すると、選択した宛先 SGT に関連するすべての情報が含まれた内部テーブルを表示できます。このビューには、送信元 SGT にマッピングされている宛先 SGT

のみが表示されます。特定の宛先 SGT を展開すると、この宛先 SGT にマッピングされているすべての送信元 SGT と対応するポリシー（SGACL）が表に示されます。

一部のフィールドの横には、3 つのドット（...）が表示されます。これは、セルにより多くの情報が含まれていることを示しています。カーソルを 3 個のドットの上に置くと、クイック ビュー ポップアップに残りの情報が表示されます。カーソルを SGT 名または SGACL 名の上に置くと、クイック ビュー ポップアップが開き、その特定の SGT または SGACL の内容が表示されます。

マトリクス ビュー

出力ポリシーのマトリクス ビューは、スプレッドシートに似ています。ここには2つの軸があります。

- 送信元軸：垂直軸にはすべての送信元 SGT がリストされます。
- 宛先軸：水平軸にはすべての宛先 SGT がリストされます。

送信元 SGT と宛先 SGT のマッピングが、セルとして示されます。セルにデータが含まれている場合、対応する送信元 SGT と宛先 SGT 間にマッピングがあるということになります。マトリクス ビューには 2 つのタイプのセルがあります。

- マッピングされたセル：送信元SGTと宛先SGTのペアが、順序付けされたSGACLのセットに関連付けられ、特定のステータスになっている場合。
- マッピングされていないセル：送信元 SGT と宛先 SGT のペアが、SGACL に関連付けられてなく、特定のステータスになっていない場合。

出力ポリシー セルには、送信元 SGT、宛先 SGT、最終的な catch-all ルールが 1 つのリストとして SGACL の下にカンマで区切られて表示されます。最終的な catch-all ルールは、[なし（None）] に設定されている場合には表示されません。マトリクス内の空のセルは、マッピングされていないセルを示します。

出力ポリシーのマトリクス ビューでは、マトリクスをスクロールして目的のセルのセットを表示できます。ブラウザがマトリクスデータ全体を一度にロードすることはありません。ブラウザは、ユーザーがスクロールした領域に移入されるデータをサーバーに要求します。これにより、メモリのオーバーフローとパフォーマンスの問題が回避されます。

[表示（View）] ドロップダウン リストで次のオプションを使用して、マトリックス ビューを変更できます。

- [SGACL名ありで簡易設定（Condensed with SGACL names）]：このオプションを選択すると、空のセルは非表示になり、SGACL 名がセルに表示されます。
- [SGACL名なしで簡易設定（Condensed without SGACL names）]：空のセルは非表示になり、SGACL 名はセルに表示されません。このビューは、より多くのマトリックス セルを表示し、色、パターンおよびアイコン（セルのステータス）を使用して、セルの内容を区別する場合に便利です。

- [SGACL名ありでフル（Full with SGACL names）]：このオプションを選択すると、左側と上側のメニューは非表示になり、SGACL 名がセルに表示されます。
- [SGACL名なしでフル（Full without SGACL names）]：このオプションを選択すると、マトリックスは全画面モードで表示され、SGACL 名はセルに表示されません。

ISE では、カスタム ビューを作成し、名前を付け、保存できます。カスタム ビューを作成するには、[表示（Show）] > [カスタムビューの作成（Create Custom View）] の順に選択します。また、ビューの条件を更新したり、未使用のビューを削除することもできます。

[マトリックス（Matrix）] ビューは、[ソース（Source）] ビューおよび [送信先（Destination）] ビューと同じ GUI 要素を持っています。ただし、次の追加要素を含みます。

マトリクスの次元

次元ビューの [次元（Dimension）] ドロップダウン リストでは、マトリクスの次元を設定することができます。

カスタム ビューの作成

始める前に

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

ステップ 1 [マトリックスビュー（Matrix View）] ページで、[表示（Show）] ドロップダウン リストから [カスタム ビューの作成（Create Custom View）] オプションを選択します。

ステップ 2 [ビューの編集（Edit View）] ダイアログボックスで、次の詳細情報を入力します。

- [ビュー名（View Name）]：カスタム ビューの名前を入力します。
- [送信元セキュリティグループ（Source Security Groups）]：カスタム ビューに含める SGT を [表示（Show）] 転送ボックスに移動します。
- [着信先関連の表示（Show Relevant for Destination）]：[送信元セキュリティグループの表示（Source Security Group Show）] 転送ボックスの選択内容を上書きして、[送信元セキュリティグループの非表示（Source Security Group Hide）] 転送ボックス内のすべてのエントリをコピーするには、このチェックボックスをオンにします。200 を超えるエントリがある場合、データはコピーされず、警告メッセージが表示されます。
- [着信先セキュリティグループ（Destination Security Groups）]：カスタム ビューに含める SGT を [表示（Show）] 転送ボックスに移動します。
- [送信元関連の表示（Show Relevant for Source）]：[送信元セキュリティグループの表示（Source Security Group Show）] 転送ボックス内での選択内容を上書きして、[送信元セキュリティグループの非表示（Source Security Group Hide）] 転送ボックスのすべてのエントリをコピーするには、このチェックボックスをオンにします。
- [次によってマトリックスをソートする（Sort Matrix By）]：次のいずれかのオプションを選択します。
  - 手動順序（Manual Order）

- タグ番号（Tag Number）
- SGT名（SGT Name）

ステップ 3 [Save] をクリックします。

マトリクス操作

マトリクスでの移動

カーソルでマトリクス コンテンツ領域をドラッグするか、または水平および垂直スクロール バーを使用して、マトリクス内を移動できます。セルをクリックしたままにし、マトリクス コンテンツ全体を任意の方向にドラッグできます。送信元および宛先のバーがセルと一緒に移動します。セルを選択すると、マトリクス ビューによってそのセルと対応する行（送信元SGT）およびカラム（宛先 SGT）が強調表示されます。選択したセルの座標（送信元 SGT および宛先 SGT）がマトリクス コンテンツ領域の下に表示されます。

マトリクスでのセルの選択

マトリクス ビューでセルを選択するには、該当のセルをクリックします。選択したセルが別の色で表示され、送信元 SGT および宛先 SGT が強調表示されます。セルをもう一度クリックするか、または別のセルを選択することで、セルの選択を解除できます。複数セルの選択は、マトリクス ビューでは許可されていません。セルをダブルクリックして、セルの設定を編集します。

出力ポリシーの SGACL の設定

[出力ポリシー（Egress Policy）] ページでセキュリティ グループ ACL を直接作成できます。

ステップ 1 [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）] の順に選択します。

ステップ 2 [送信元ツリービュー（Source Tree View）] または [宛先ツリービュー（Destination Tree View）] ページから、[設定（Configure）] > [新しいセキュリティグループACLの作成（Create New Security Group ACL）] を選択します。

ステップ 3 必要な詳細を入力し、[送信（Submit）] をクリックします。

ワーク プロセスの設定

始める前に

次のタスクを実行するには、スーパー管理者である必要があります。

ステップ 1 [ワーク センター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ワーク プロセスの設定（Work Process Settings）] の順に選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 単一マトリックス（Single Matrix）：TrustSec ネットワーク上のすべてのデバイスに対してポリシー マトリックスを 1 つのみ作成するには、このオプションを選択します。
- 複数マトリックス（Multiple Matrices）：さまざまなシナリオで複数のポリシーマトリックスを作成できるようにします。これらのマトリックスを使用して、さまざまなネットワーク デバイスに異なるポリシーを展開できます。

  （注） マトリックスは独立していて、各ネットワーク デバイスを 1 つのマトリックスのみに割り当てることができます。

- 承認プロセス付き実稼働およびステージング マトリックス（Production and Staging Matrices with Approval Process）：ワークフロー モードを有効にするには、このオプションを選択します。エディタ ロールおよび承認者ロールに割り当てられるユーザーを選択します。ユーザーは、ポリシー管理者グループおよびスーパー管理者グループからのみ選択できます。ユーザーはエディタ ロールおよび承認者ロールの両方に割り当てることはできません。

  エディタまたは承認者ロールが割り当てられたユーザーの電子メール アドレスが設定されていることを確認します。設定されていないと、ワークフロー プロセスに関する電子メール通知がこれらのユーザーに送信されません。

  ワークフロー モードを有効にすると、エディタのロールが割り当てられたユーザーは、ステージング マトリックスを作成し、ステージング ポリシーを展開するデバイスを選択して、承認者に承認を求めるステージング ポリシーを送信できます。承認者ロールが割り当てられたユーザーは、ステージング ポリシーを確認し、要求を承認または拒否することができます。ステージング ポリシーが承認者によって確認され、承認された後でのみ、ステージング ポリシーを選択したネットワーク デバイスに展開できます。

ステップ 3 DEFCON マトリックスを作成する場合は、[DEFCON を使用する（Use DEFCONS）] チェックボックスをオンにします。

DEFCONS マトリックスは、ネットワーク セキュリティ侵害の発生時に簡単に展開できるスタンバイ ポリシー マトリックスです。

シビラティ（重大度）レベル [重大（Critical）]、[深刻（Severe）]、[実質的（Substantial）]、および [適度（Moderate）] の DEFCON マトリックスを作成できます。

DEFCON マトリックスがアクティブになると、対応する DEFCON ポリシーがすべての TrustSec ネットワーク デバイスにすぐに展開されます。ネットワーク デバイスから DEFCON ポリシーを削除するには、非アクティブ化オプションを使用できます。

ステップ 4 [Save] をクリックします。

[マトリックス登録（Matrices Listing）] ページ

TrustSec ポリシーマトリックスと DEFCON マトリックスは、[マトリックス登録（Matrices Listing）] ページに表示されます（[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）] > [マトリックス登録（Matrices List）]）。各マトリックスに割り当てられているデバイスの数を確認することもできます。

（注） [マトリックス登録（Matrices Listing）] ページは、単一マトリックス モードが有効であり、DEFCON マトリックス オプションが無効な場合は表示されません。

[マトリックス登録（Matrices Listing）] ページからは、次のことが行えます。

- 新しいマトリックスの追加
- 既存のマトリックスの編集
- マトリックスの削除
- 既存のマトリックスの複製
- マトリックスへの NAD の割り当て

[NAD の割り当て（Assign NADs）] オプションを使用して、マトリックスに NAD を割り当てることができます。手順は次のとおりです。

1. [ネットワーク デバイスの割り当て（Assign Network Devices）] ウィンドウで、マトリックスに割り当てるネットワーク デバイスを選択します。フィルタ オプションを使用してネットワーク デバイスを選択することもできます。
2. [マトリックス（Matrix）] ドロップダウン リストから、マトリックスを選択します。既存のすべてのマトリックスとデフォルトのマトリックスがこのドロップダウン リストに表示されます。

デバイスをマトリックスに割り当てたら、[プッシュ（Push）] をクリックし、TrustSec の設定変更を該当するネットワーク デバイスに通知します。

[マトリックス登録（Matrices Listing）] ページで作業を行うときは、次の点に注意してください。

- デフォルトのマトリックスを編集、削除、名前変更することはできません。
- 新しいマトリックスを作成する際は、空のマトリックスから開始することや、既存のマトリックスからポリシーをコピーすることができます。
- マトリックスを削除すると、そのマトリックスに割り当てられている NAD が自動的にデフォルトのマトリックスに移動します。
- 既存のマトリックスをコピーするとマトリックスのコピーが作成されますが、デバイスはコピーされたマトリックスに自動的に割り当てられません。

- 複数マトリックス モードでは、すべてのデバイスが初期段階でデフォルトのマトリックスに割り当てられます。
- 複数マトリックス モードでは、一部の SGACL がマトリックス間で共有されることがあります。この場合、SGACL コンテンツを変更すると、セルにその SGACL が含まれているすべてのマトリックスに影響します。
- 複数マトリックスは、ステージングが進行中のときに有効にすることはできません。
- 複数マトリックス モードから単一マトリックス モードに変更すると、すべての NAD が自動的にデフォルトのマトリックスに割り当てられます。
- 現在有効になっている場合は、DEFCON マトリックスを削除することはできません。

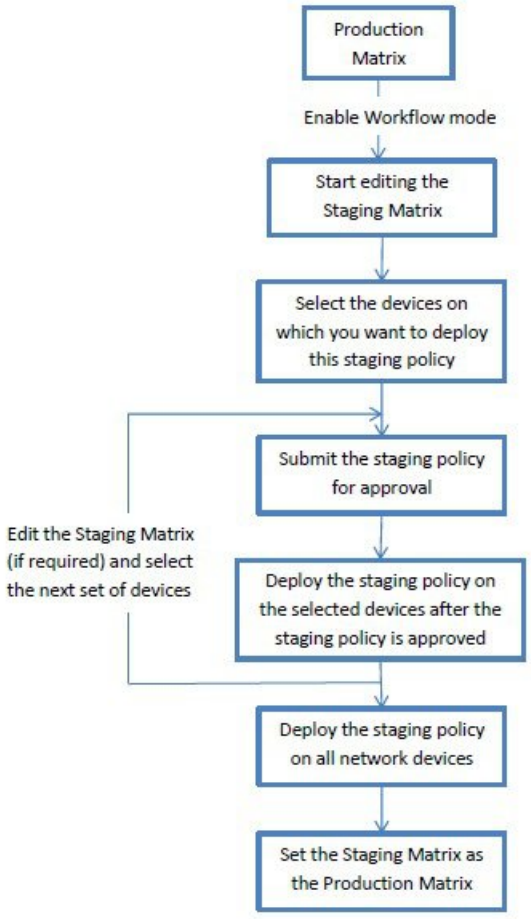
TrustSec マトリックス ワークフロー プロセス

マトリクスのワークフロー機能は、すべてのネットワーク デバイスにポリシーを導入する前に、このマトリックスのドラフト版（ステージング マトリックスとも呼ばれます）を使用して、デバイスの制限されたセットで新しいポリシーをテストできます。承認のためのステージング ポリシーを送信し、承認されると、選択したネットワーク デバイスにステージング ポリシーを導入できます。この機能により、必要に応じて、デバイスの制限されたセットへの新しいポリシーの導入、適切に機能しているかの確認、変更を行うことができます。次の一連のデバイスまたはすべてのデバイスにポリシーを適用し続けることもできます。ステージング ポリシーがすべてのネットワーク デバイスに導入されると、ステージング マトリックスは新たな実稼働マトリックスとして設定できます。

ワークフロー モードを有効にすると、エディタ ロールに割り当てられたユーザーは、ステージングマトリクスを作成し、マトリクスセルを編集できます。ステージングマトリックスは、TrustSec ネットワークに現在展開されている実稼働マトリックスのコピーです。エディタは、ステージング ポリシーを展開し、承認のために承認者にステージング ポリシーを送信するデバイスを選択できます。承認者ロールが割り当てられたユーザーは、ステージング ポリシーを確認し、要求を承認または拒否することができます。ステージング ポリシーが承認者によって確認され、承認された後でのみ、ステージング ポリシーを選択したネットワーク デバイスに展開できます。

次の図で、ワークフロー プロセスについて説明します。

図 *8 :* マトリックス ワークフロー プロセス



上級管理ユーザーは、ワークフロープロセスの設定ページ（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ワークフロー プロセス（Workflow Process）]）で、エディタおよび承認者ロールに割り当てられたユーザーを選択できます。

ステージング ポリシーが選択されたデバイスに導入された後では、SGT および SGACL を編集できませんが、マトリクスセルは編集できます。設定の差分レポートを使用して、実稼働マトリックスとステージングマトリックスの違いを追跡できます。また、ステージング処理中にそのセルへの変更を表示するには、セルで [デルタ（Delta）] アイコンをクリックします。

次の表では、ワークフローのさまざまな段階を説明します。

ステージ	説明
ステージングを編集中（Staging in Edit）	エディタがステージング マトリックスの編集を開始すると、マトリックスは[ステージングを編集中（Staging in Edit）] 状態に移行します。ステージングマトリックスを編集したら、エディタは、新しいステージング ポリシーを導入するデバイスを選択できます。
ステージングの承認待ち（Staging Awaiting Approval）	マトリックスの編集後、エディタは確認および承認を受けるために承認者にステージング マトリックスを送信します。 承認のためにステージング マトリックスを送信する時に、エディタは承認者に送信される電子メールにコメントを追加できます。 承認者は、ステージング ポリシーを確認し、要求を承認または拒否することができます。承認者は、選択したネットワーク デバイスと設定の差分レポートを表示できます。要求の承認または拒否時に、承認者はエディタに送信される電子メールにコメントを追加できます。 エディタはステージング ポリシーがどのネットワーク デバイスにも導入されていなければ承認リクエストをキャンセルできます。
展開の承認取得済み（Deploy Approved）	承認者が要求を承認すると、ステージング マトリックスは [展開の承認取得済み（Deploy Approved）] 状態に移行します。要求が拒否された場合、マトリックスは[ステージングを編集中（Staging in Edit）] 状態に戻されます。 エディタはステージング ポリシーが承認者によって承認された後でのみ、ステージング ポリシーを選択したネットワーク デバイスに導入できます。

ステージ	説明
一部展開済み（Partially deployed）	ステージング マトリックスが選択したデバイスに展開された後、マトリックスは[一部展開済み（Partially deployed）]状態に移行します。マトリックスは、ステージング ポリシーがすべてのネットワーク デバイスに導入されるまで、[一部展開済み（Partially deployed）]ステージのままです。 このステージでは、SGT および SGACL を編集できませんが、マトリクス セルは編集できます。 最新のポリシーが導入されていないデバイス（同期していないデバイス）は、[ネットワーク デバイスの導入（Network Device Deployment）]ウィンドウにオレンジ色（イタリック体）で表示されます。このステータスは、導入の進捗状況のステータス バーにも表示されます。エディタはこれらのデバイスを選択し、さまざまな導入サイクルで更新されたデバイスを同期するように承認を要求できます。
完全に展開済み（Fully deployed）	上記の手順は、ステージング ポリシーがすべてのネットワーク デバイスに展開されるまで繰り返されます。ステージング マトリックスをすべてのネットワーク デバイスに展開する場合、承認者はステージング マトリックスを実稼働マトリックスとして設定できます。 実稼働マトリックスをステージング マトリックスに置き換えた後では、実稼働マトリックスの以前のバージョンへのロールバックはできないため、新たな実稼働マトリクスとしてステージング マトリクスを設定する前に実稼働マトリクスのコピーを取得しておくことをお勧めします。

[ワークフロー（Workflow）]ドロップダウン リストに表示されるオプションは、ワークフローの状態とユーザー ロール（エディタまたは承認者）によって異なります。次の表に、エディタおよび承認者に表示されるメニュー オプションを示します。

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
ステージングを編集中（Staging in Edit）		• ネットワークデバイスの表示（View network devices） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	• ネットワークデバイスの選択（Select network devices） 次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • 選択したデバイスの承認要求（Request approval for selected devices） • すべての/フィルタリングされたステージングリストの承認要求（Request approval for all/filtered Staging list） • すべての/フィルタリングされた実稼働リストの承認要求（Request approval for all/filtered Production list） • すべての/フィルタリングされたデバイスの承認要	

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	求（Request approval for all/filtered devices） • 選択したデバイスの承認要求（Request approval for selected devices） • ステージングの破棄（Discard staging） • デルタの表示（View deltas）	
ステージングの承認待ち（Staging Awaiting Approval）	• 承認要求のキャンセル（Cancel approval request） • ネットワークデバイスの表示（View network devices） 次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • 承認要求のキャンセル（Cancel approval request） • デルタの表示（View deltas）	• 展開の承認（Approve deploy） • 展開の拒否（Reject deploy） • ネットワークデバイスの表示（View network devices） 次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • 展開の承認（Approve deploy） • 展開の拒否（Reject deploy） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー

承認済み：展開の準備完了（Approved - ready to deploy）	• [展開（Deploy）]
	• 承認要求のキャンセル（Cancel approval request）
	• ネットワークデバイスの表示（View network devices）
	次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。
	  • [展開（Deploy）]
	  • 承認要求のキャンセル（Cancel approval request）
	• デルタの表示（View deltas）
		• 展開の拒否（Reject deploy）
		• ネットワークデバイスの表示（View network devices）
		次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。
		  • 展開の拒否（Reject deploy）
		• デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
一部展開済み（Partially deployed）		• ネットワークデバイスの表示（View network devices） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	• ネットワークデバイスの選択（Select network devices） 次のオプションが [ネットワーク デバイスの導入（Network Device Deployment）] ウィンドウで使用できます。 • 選択したデバイスの承認要求（Request approval for selected devices） • すべての/フィルタリングされたステージングリストの承認要求（Request approval for all/filtered Staging list） • すべての/フィルタリングされた実稼働リストの承認要求（Request approval for all/filtered Production list） • すべての/フィルタリングされたデバイスの承認要	

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	求（Request approval for all/filtered devices） • 選択したデバイスの承認要求（Request approval for selected devices） • デルタの表示（View deltas）	

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
完全に展開済み（Fully deployed）		• 実稼働として設定（Set as production） • ネットワークデバイスの表示（View network devices） • デルタの表示（View deltas）

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	• ネットワークデバイスの選択（Select network devices） 次のオプションが[ネットワーク デバイスの導入（Network Device Deployment）]ウィンドウで使用できます。 • 選択したデバイスの承認要求（Request approval for selected devices） • すべての/フィルタリングされたステージングリストの承認要求（Request approval for all/filtered Staging list） • すべての/フィルタリングされた実稼働リストの承認要求（Request approval for all/filtered Production list） • すべての/フィルタリングされたデバイスの承認要	

ワークフローの状態	エディタに表示されるメニュー	承認者に表示されるメニュー
	求（Request approval for all/filtered devices） • 選択したデバイスの承認要求（Request approval for selected devices） • デルタの表示（View deltas）	

ワークフロー オプションは、[送信元ツリービュー（Source Tree View）] と [宛先ツリービュー（Destination Tree View）] でも使用できます。

TrustSec ポリシーのダウンロード レポート（[ワーク センター（Work Centers）] > [TrustSec] > [レポート（Reports）]）を使用して、ステージング/実稼働ポリシーをダウンロードしたデバイスのリストを表示できます。TrustSec ポリシーのダウンロードは、ポリシー（SGT/SGACL）のダウンロードのために、ネットワーク デバイスによって送信された要求と ISE によって送信された詳細を示します。ワークフローモードを有効にしている場合、要求を実稼働マトリックスまたはステージング マトリックスに対してフィルタ処理することができます。

出力ポリシー テーブル セルの設定

Cisco ISE では、ツールバーで使用可能なさまざまなオプションを使用して、セルを設定できます。Cisco ISE では、選択した送信元 SGT および宛先 SGT がマッピングされたセルと同一である場合には、セルを設定できません。

出力ポリシー セルのマッピングの追加

[ポリシー（Policy）] ページから出力ポリシーのマッピング セルを追加できます。

ステップ 1 **[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）]** を選択します。

ステップ 2 マトリクス セルを選択するには、次の手順を実行します。

- マトリクス ビューで、セルをクリックして選択します。
- 送信元ツリー ビューおよび宛先ツリー ビューで、内部テーブル内の行のチェックボックスをオンにして選択します。

ステップ 3 新しいマッピング セルを追加するには [追加（Add）] をクリックします。

ステップ 4 次の項目について適切な値を選択します。

- 送信元セキュリティ グループ（Source Security Group）
- 宛先セキュリティグループ
- ステータス（Status）、セキュリティ グループ ACL（Security Group ACLs）
- 最終的な catch-all ルール（Final Catch All Rule）

ステップ 5 [Save] をクリックします。

出力ポリシーのエクスポート

ステップ 1 [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）] > [エクスポート（Export）] を選択します。

ステップ 2 エクスポートしたファイルに空のセル（SGACL が設定されていないセル）を含める場合は、[空のセルを含める（Include Empty Cells）] チェック ボックスにマークを付けます。

このオプションが有効になっている場合、マトリックス全体がエクスポートされ、空のセルは[SGACL]列に「空（Empty）」キーワードでマークされます。

（注） エクスポートされたファイルに500000を超える行が含まれていないことを確認してください。そうでない場合、エクスポートが失敗する場合があります。

ステップ 3 次のオプションのいずれかを選択します。

- [Local Disk]：コンピュータのローカルドライブにファイルをエクスポートする場合は、このオプションを選択します。
- [リポジトリ（Repository）]：リモート リポジトリにファイルをエクスポートする場合は、このオプションを選択します。

  ファイルをエクスポートする前にリポジトリを設定する必要があります。リポジトリを設定するには、[管理（Administration）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）] の順に選択します。読み取りおよび書き込みアクセス権が選択したリポジトリに提供されていることを確認します。

  暗号キーを使用してエクスポートされたファイルを暗号化できます。

  ファイル名は変更することができます。ファイル名は、50 文字以内でなければなりません。デフォルトでは、ファイル名には現在の時刻が含まれていますが、同じファイル名がリモート リポジトリに存在する場合は、ファイルが上書きされます。

ステップ 4 [エクスポート（Export）] をクリックします。

出力ポリシーのインポート

出力ポリシーをオフラインで作成し、Cisco ISE にインポートすることができます。セキュリティ グループ タグの数が多い場合、セキュリティ グループ ACL マッピングを 1 つずつ作成すると、時間がかかることがあります。代わりに、出力ポリシーをオフラインで作成し、Cisco ISE にインポートすることにより、時間を節約できます。インポート中、Cisco ISE は CSV ファイルのエントリを出力ポリシー マトリクスに追加し、データは上書きしません。

次の場合、出力ポリシーのインポートは失敗します。

- 送信元または宛先 SGT が存在しない
- SGACL が存在しない
- モニター ステータスが、そのセルについて Cisco ISE で現在設定されているものと異なる

ステップ 1 [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）] > [インポート（Import）] を選択します。

ステップ 2 [テンプレートの生成（Generate a Template）] をクリックします。

ステップ 3 [出力ポリシー（Egress Policy）] ページからテンプレート（CSV ファイル）をダウンロードし、CSV ファイルに次の情報を入力します。

- 送信元 SGT（Source SGT）
- 宛先 SGT（Destination SGT）
- SGACL
- モニター ステータス（有効、無効、またはモニター対象）

ステップ 4 インポートするポリシーで既存のポリシーが上書きされるようにする場合は、[新しいデータで既存のデータを上書き（Overwrite Existing Data with New Data）] チェックボックスをオンにします。空セル（「Empty」キーワードでマークされた、[SGACL] 列のセル）がインポートされたファイルに含まれていると、対応するマトリックスのセルの既存のポリシーが削除されます。

イーグレス ポリシーをエクスポートする際に空セルを含めるには、[空のセルを含める（Include Empty Cells）] チェックボックスをオンにします。詳細については、出力ポリシーのエクスポート （169 ページ）を参照してください。

ステップ 5 [ファイルの検証（Validate File）] をクリックして、インポートされたファイルを検証します。Cisco ISE は、ファイルをインポートする前に CSV 構造、SGT 名、SGACL、およびファイル サイズを検証します。

ステップ 6 エラーが発生した場合に Cisco ISE でインポートを取り消すには、[最初のエラーでインポートを停止（Stop Import on First Error）] チェックボックスをオンにします。

ステップ 7 **[インポート (Import)]** をクリックします。

出力ポリシーの SGT の設定

[出力ポリシー（Egress Policy）] ページでセキュリティ グループを直接作成できます。

ステップ 1 **[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）]** を選択します。

ステップ 2 [送信元ツリービュー（Source Tree View）] または [宛先ツリービュー（Destination Tree View）] ページから、[設定（Configure）] > [新しいセキュリティグループの作成（Create New Security Group）] を選択します。

ステップ 3 必要な詳細を入力し、[送信（Submit）] をクリックします。

モニターモード

出力ポリシーの [すべてをモニター（Monitor All）] オプションを使用すると、出力ポリシー設定ステータス全体を 1 回のクリックでモニターモードに変更できます。[出力ポリシー（egress policy）] ページの [すべてをモニター（Monitor All）] チェックボックスをオンにして、すべてのセルの出力ポリシー設定ステータスをモニター モードに変更します。[すべてをモニター（Monitor All）] チェックボックスをオンにすると、設定ステータスが次のように変更されます。

- ステータスが [有効（Enabled）] であるセルはモニター対象として動作しますが、有効であるかのように表示されます。
- ステータスが [無効（Disabled）] であるセルは何も影響を受けません。
- ステータスが [モニター（Monitor）] であるセルは、[モニター対象（Monitored）] のままになります。

[すべてをモニター（Monitor All）] チェックボックスをオフにすると、元の設定ステータスに戻ります。データベース内の実際のセルのステータスは変更されません。[すべてをモニター（Monitor All）] をオフにすると、出力ポリシーのそれぞれのセルが元の設定ステータスに戻ります。

モニター モードの機能

モニター モードのモニタリング機能は次の操作に役立ちます。

- フィルタリングされているけれども、モニターモードではモニターされているトラフィックの量の確認
- SGT-DGT ペアがモニター モードであるか強制モードであるかの確認と、ネットワーク内で異常なパケット ドロップが発生していないかどうかの観察
- SGACL ドロップが実際に強制モードによって強制されているのか、またはモニター モードによって許可されているのかの確認
- モードのタイプ（モニター、強制、または両方）に基づいたカスタム レポートの作成
- NAD に適用されている SGACL、および表示の不一致（ある場合）の識別

不明セキュリティ グループ

不明セキュリティ グループは事前に設定されているセキュリティ グループで、変更不可能であり、タグ値 0 の TrustSec を表します。

Ciscoセキュリティ グループのネットワーク デバイスは、送信元または宛先のいずれかのSGTがない場合に不明 SGT を参照するセルを要求します。送信元のみが不明の場合、要求は <不明, 宛先 SGT> セルに適用されます。宛先のみが不明の場合、要求は <source SGT, unknown> セルに適用されます。送信元および宛先の両方が不明の場合、要求は<不明, 不明>セルに適用されます。

デフォルト ポリシー

デフォルト ポリシーは、<ANY,ANY> セルを参照します。任意の送信元 SGT が任意の宛先 SGT にマッピングされています。ここでは、ANY SGT は変更不可能であり、送信元 SGT にも宛先 SGT にも表示されません。ANY SGT は ANY SGT とのみペアにできます。他の SGT とはペアにできません。TrustSec ネットワーク デバイスでは、デフォルト ポリシーを特定セルのポリシーの最後に付加します。

- つまり、セルが空白の場合は、デフォルト ポリシーのみが含まれることになります。
- セルにポリシーが含まれる場合、結果のポリシーは、セル固有のポリシーとその後に続くデフォルト ポリシーの組み合わせになります。

Cisco ISE では、セル ポリシーおよびデフォルト ポリシーは 2 つの別々の SGACL セットになり、デバイスは 2 つの別々のポリシー クエリーの応答としてこれらのセットを取得します。

デフォルト ポリシーの設定は、他のセルと次の点で異なります。

- ステータスは [有効（Enabled）] または [モニター対象（Monitored）] の 2 つの値しかとることができません。
- セキュリティ グループ ACL は、デフォルト ポリシーでは任意のフィールドであるため、空白のままにできます。
- 最終的な catch-all ルールは次のいずれかになります。許可 IP、拒否 IP、許可 IP ログ、または拒否IP ログ。デフォルト ポリシーを上回る安全策はないため、ここで [なし（None）] オプションを使用できないことは明らかです。

SGT の割り当て

Cisco ISE では、デバイスのホスト名または IP アドレスがわかっている場合に、TrustSec デバイスに SGT を割り当てることができます。特定のホスト名または IP アドレスを持つデバイスがネットワークに参加すると、Cisco ISE によって認証前に SGT が割り当てられます。

次の SGT がデフォルトで作成されています。

- SGT_TrustSecDevices
- SGT_NetworkServices

- SGT_Employee
- SGT_Contractor
- SGT_Guest
- SGT_ProductionUser
- SGT_Developer
- SGT_Auditor
- SGT_PointofSale
- SGT_ProductionServers
- SGT_DevelopmentServers
- SGT_TestServers
- SGT_PCIServers
- SGT_BYOD
- SGT_Quarantine

セキュリティ グループ タグをエンドポイントにマップするようにデバイスを手動で設定する必要がある場合もあります。このマッピングは [セキュリティ グループ マッピング（Security Group Mappings）] ページから作成できます。この操作を実行する前に、SGT の範囲が予約済みであることを確認します。

ISE では、最大 10,000 の IP-to-SGT マッピングを作成できます。IP-to-SGT マッピング グループを作成して、このような大規模なマッピングを論理的にグループ化することができます。各 IP-to-SGT マッピング グループには、IP アドレスのリスト、マップ先の単一のセキュリティ グループ、およびこれらのマッピングの展開対象であるネットワーク デバイスまたはネットワーク デバイス グループが含まれています。

NDAC 許可

デバイスに SGT を割り当てることで TrustSec ポリシーを設定できます。TrustSec デバイスの ID 属性に基づいて、デバイスにセキュリティ グループを割り当てることができます。

NDAC 許可の設定

始める前に

- ポリシーで使用するためのセキュリティ グループを作成します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [ネットワークデバイス認証（Network Device Authorization）] を選択します。

ステップ 2 [デフォルト ルール（Default Rule）] 行の右側にある [操作（Action）] アイコンをクリックし、[新規行を上に挿入（Insert New Row Above）] をクリックします。

ステップ 3 このルールの名前を入力します。

ステップ 4 [条件（Conditions）] の隣にあるプラス記号（+）をクリックして、ポリシー条件を追加します。

ステップ 5 [新しい条件の作成（高度なオプション）（Create New Condition (Advance Option)）] をクリックすると、新しい条件を作成できます。

ステップ 6 [セキュリティ グループ（Security Group）] ドロップダウン リストから、この条件の評価が true になった場合に割り当てる SGT を選択します。

ステップ 7 この行の [操作（Action）] アイコンをクリックして、現在のルールの上または下に、デバイス属性に基づいた別のルールを追加します。このプロセスを繰り返して、TrustSec ポリシーに必要なすべてのルールを作成できます。ルールをドラッグ アンド ドロップし、  アイコンをクリックすることでこれらの順序を変更できます。既存の条件を複製することもできますが、ポリシー名は必ず変更してください。

評価が true になる最初のルールによって、評価の結果が決まります。いずれのルールも一致しなかった場合、デフォルト ルールが適用されます。デフォルト ルールを編集して、いずれのルールも一致しなかった場合にデバイスに適用される SGT を指定できます。

ステップ 8 [保存（Save）] をクリックして TrustSec ポリシーを保存します。

ネットワーク デバイス ポリシーを設定した後に、TrustSec デバイスで認証を行おうとすると、デバイスはその SGT およびそのピアの SGT を取得し、関連するすべての詳細をダウンロードできるようになります。

エンドユーザーの許可の設定

Cisco ISE では、許可ポリシー評価の結果としてセキュリティ グループを割り当てることができます。このオプションを使用すると、ユーザーおよびエンドポイントにセキュリティ グループを割り当てることができます。

始める前に

- 許可ポリシーについての情報を参照してください。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [認証ポリシー（Authorization Policy）] を選択します。

ステップ 2 新しい許可ポリシーを作成します。

ステップ 3 権限のセキュリティ グループを選択します。

あるユーザーまたはエンドポイントについて、この許可ポリシーで指定した条件がtrueの場合、このセキュリティ グループがそのユーザーまたはエンドポイントに割り当てられ、このユーザーまたはエンドポイントによって送信されたすべてのデータ パケットにこの特定の SGT でタグが付けられます。

TrustSec の設定およびポリシー プッシュ

Cisco ISE では、許可変更（CoA）がサポートされています。これを使用すると、Cisco ISE で TrustSec の設定およびポリシーの変更を TrustSec デバイスに通知でき、デバイスでは関連データの取得要求でこれに応答できるようになります。

CoA 通知では、TrustSec ネットワーク デバイスをトリガーし、環境 CoA またはポリシー CoA のいずれかを送信できます。

また、基本的にTrustSec CoA機能をサポートしないデバイスに設定変更をプッシュできます。

CoA でサポートされるネットワーク デバイス

Cisco ISE は次のネットワーク デバイスに CoA 通知を送信します。

- 単一の IP アドレスを持つネットワーク デバイス（サブネットはサポートされません）
- TrustSec デバイスとして設定されているネットワーク デバイス
- CoA サポート対象として設定されているネットワーク デバイス

複数のセカンダリが存在する分散環境に Cisco ISE が展開されており、これらのセカンダリがそれぞれ異なるデバイス セットと相互運用している場合、CoA 要求は Cisco ISE プライマリ ノードからすべてのネットワーク デバイスに送信されます。そのため、TrustSec ネットワーク デバイスは、Cisco ISE プライマリ ノードで CoA クライアントとして設定されている必要があります。

デバイスは、Cisco ISE プライマリ ノードに CoA NAK または ACK を返します。ただし、ネットワーク デバイスからの次の TrustSec セッションは、ネットワーク デバイスが他の AAA 要求をすべて送信する Cisco ISE ノードに送信され、必ずしもプライマリ ノードに送信されるわけではありません。

非 CoA サポート デバイスへの設定変更のプッシュ

一部のプラットフォームでは、許可変更（CoA）について Cisco ISE の「プッシュ」機能はサポートされていません。例：Nexus ネットワーク デバイスの一部のバージョン。この場合、ISEはネットワーク デバイスに接続し、ISEに対して更新された設定要求をデバイスがトリガーするようにします。これを行うために、ISE はネットワーク デバイスへの SSHv2 トンネルを開き、TrustSecポリシーマトリクスのリフレッシュをトリガーするコマンドを送信します。この方法は、CoA プッシュをサポートするネットワーク プラットフォームでも実行できます。

ステップ 1 **[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）]** の順に選択します。

ステップ 2 必要なネットワーク デバイスの横にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ネットワーク デバイスの名前、IP アドレス、RADIUS および TrustSec 設定が正しく設定されていることを確認します。

ステップ 3 [高度な TrustSec 設定（Advanced TrustSec Settings）] まで下にスクロールし、[TrustSec 通知および更新（TrustSec Notifications and Updates）] セクションで、[デバイスに設定変更を送信（Send configuration changes to device）] チェックボックスをオンにして [CLI（SSH）（CLI (SSH)）] オプション ボタンをクリックします。

ステップ 4 （任意） SSH キーを指定します。

ステップ 5 デバイス インターフェイスのクレデンシャルを使用して IP-SGT マッピングを取得するには、この SGA デバイスに対して [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）] チェックボックスをオンにします。

ステップ 6 EXEC モードでデバイス設定を編集する権限を持つユーザーのユーザー名とパスワードを入力します。

ステップ 7 （任意） 設定を編集できるデバイスの EXEC モード パスワードを有効にするためのパスワードを入力します。[表示（Show）] をクリックして、このデバイスにすでに設定されている EXEC モード パスワードを表示できます。

ステップ 8 ページの下部にある [送信（Submit）] をクリックします。

ネットワーク デバイスは、TrustSec の変更をプッシュするように設定されました。Cisco ISE ポリシーを変更した後で、ネットワーク デバイスに新規設定を反映させるには、[プッシュ（Push）] をクリックします。

SSH キーの検証

SSH キーを使用してセキュリティを強化することもできます。Cisco ISE では、SSH キー検証機能によってこれをサポートします。

この機能を使用するには、Cisco ISE からネットワーク デバイスに SSHv2 トンネルを開いて、ネットワーク デバイスの独自の CLI を使用して SSH キーを取得します。このキーをコピーし、検証のために Cisco ISE に貼り付けます。SSH キーが誤っている場合、Cisco ISE は接続を終了します。

制限：現在、Cisco ISE が検証できるのは 1 つの IP のみです（IP の範囲、または IP 内のサブネットは検証できません）

始める前に

次のものが必要です。

- ログイン クレデンシャル
- SSH キーを取得する CLI コマンド

（Cisco ISE とセキュアに通信できるようにするネットワーク デバイスのもの）

ステップ 1 ネットワーク デバイス上：

a) Cisco ISE が SSH キー検証を使用して通信するネットワーク デバイスにログインします。

b) デバイスの CLI を使用して SSH キーを表示します。

例：

Catalyst デバイスの場合、コマンドは次のとおりです。`sho ip ssh`。

c) 表示された SSH キーをコピーします。

ステップ 2 Cisco ISE ユーザー インターフェイスから、次の手順を実行します。

a) **[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）]** を選択し、必要なネットワーク デバイス名、IP アドレス、RADIUS および TrustSec 設定が正しく設定されていることを確認します。

b) [高度な TrustSec 設定（Advanced TrustSec Settings）] まで下にスクロールし、[TrustSec 通知および更新（TrustSec Notifications and Updates）] セクションで、[デバイスに設定変更を送信（Send configuration changes to device）] チェックボックスをオンにして [CLI（SSH）（CLI (SSH)）] オプション ボタンをクリックします。

c) [SSH キー（SSH Key）] フィールドに、ネットワーク デバイスから取得した SSH キーを貼り付けます。

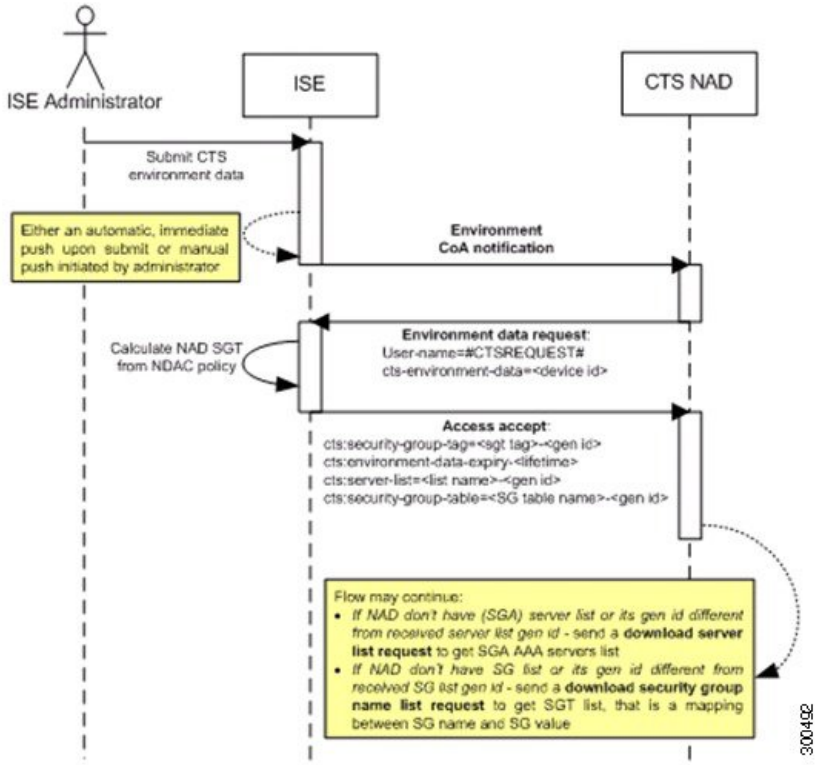
d) ページの下部にある [送信（Submit）] をクリックします。

ネットワーク デバイスは、SSH キー検証を使用して Cisco ISE と通信するようになりました。

環境 CoA 通知のフロー

次の図は、環境 CoA 通知のフローを示しています。

図 *9:* 環境 *CoA* 通知のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに環境 CoA 通知を送信します。
2. デバイスは、環境データ要求を返します。
3. 環境データ要求への応答で、Cisco ISE は次の情報を返します。

   要求を送信したデバイスの環境データ：これには、（NDAC ポリシーから推測される）TrustSec デバイスの SGT およびダウンロード環境 TTL が含まれます。

   TrustSec AAA サーバー リストの名前および生成 ID。

   （複数の可能性がある）SGT テーブルの名前および生成 ID：これらのテーブルには SGT 名と SGT 値がリストされ、一緒に SGT の完全リストも保持されます。
4. デバイスが TrustSec AAA サーバー リストを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、AAA サーバー リストの内容を取得します。
5. デバイスが応答にリストされている SGT テーブルを保持していない場合、または生成 ID が受信した生成 ID と異なる場合、デバイスは別の要求を送信して、その SGT テーブルの内容を取得します。

環境 CoA トリガー

環境 CoA は次のものに関して開始できます。

- ネットワーク デバイス
- セキュリティ グループ
- AAA サーバー

ネットワーク デバイスの環境 CoA のトリガー

ネットワーク デバイスに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [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）]**[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）]** を選択します。

ステップ 2 ネットワーク デバイスを追加または編集します。

ステップ 3 [高度な TrustSec 設定（Advanced TrustSec Settings）] セクションで、[TrustSec 通知および更新（TrustSec Notifications and Updates）] パラメータを更新します。

環境属性の変更は、変更が発生した特定の TrustSec ネットワーク デバイスにのみ通知されます。

単一のデバイスのみが影響を受けるため、環境 CoA 通知は送信直後に送信されます。結果として、そのデバイスの環境属性が更新されます。

セキュリティ グループの環境 CoA のトリガー

セキュリティ グループに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [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）] を選択しますCisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。。

ステップ 2 [セキュリティ グループ（Security Group）] ページで、SGT の名前を変更します。これにより、その SGT のマッピング値の名前が変更されます。これで環境変更がトリガーされます。

ステップ 3 複数の SGT の名前を変更した後、[プッシュ（Push）] ボタンをクリックして、環境 CoA 通知を開始します。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、変更されたすべての SGT の更新が提供されます。

TrustSec AAA サーバーの環境 CoA のトリガー

TrustSec AAA サーバーに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 **[ワークセンター（Work Centers）]** > **[TrustSec]** > **[コンポーネント（Components）]** > **[TrustSec AAA サーバー（TrustSec AAA Servers）]** を選択します。

ステップ 2 [TrustSec AAA サーバー（TrustSec AAA Servers）] ページで、TrustSec AAA サーバーの設定を作成、削除、または更新します。これで環境変更がトリガーされます。

ステップ 3 複数の TrustSec AAA サーバーを設定した後、[プッシュ（Push）] ボタンをクリックして、環境 CoA 通知を開始します。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、変更されたすべての TrustSec AAA サーバーの更新を提供します。

NDAC ポリシーの環境 CoA のトリガー

NDAC ポリシーに関する環境 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [ワークセンター（Work Centers）]>[TrustSec]>[ポリシー（Policy）]>[ネットワークデバイス許可（Network Device Authorization）] の順に選択します。

[NDAC ポリシー（NDAC policy）] ページで、NDAC ポリシーのルールを作成、削除、または更新できます。これらの環境変更は、すべてのネットワーク デバイスに通知されます。

ステップ 2 [ワークセンター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [ネットワークデバイス認証（Network Device Authorization）] を選択します。

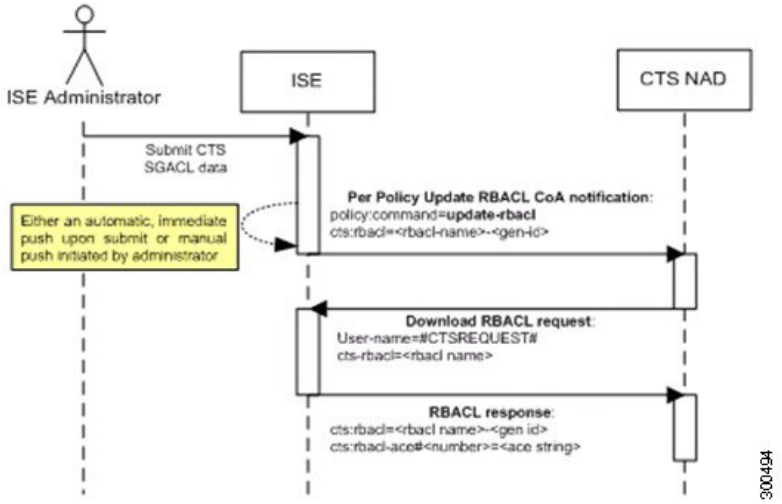
[NDAC ポリシー（NDAC policy）] ページで、NDAC ポリシーのルールを作成、削除、または更新できます。これらの環境変更は、すべてのネットワーク デバイスに通知されます。

ステップ 3 [NDAC ポリシー（NDAC policy）] ページで [プッシュ（Push）] ボタンをクリックすることで、環境 CoA 通知を開始できます。この環境 CoA 通知は、すべての TrustSec ネットワーク デバイスに送信され、ネットワーク デバイス自体の SGT の更新を提供します。

SGACL コンテンツ更新のフロー

次の図に、SGACL コンテンツ更新のフローを示します。

図 *10 : SGACL* コンテンツ更新のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに SGACL 名前付きリストの更新 CoA 通知を送信します。通知には、SGACL 名と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGACL データ要求で応答できます。

   SGACLが、デバイスが保持する出力セルに含まれている場合。デバイスには出力ポリシーデータのサブセットが保持されます。これらは、そのネイバーデバイスおよびエンドポイントの SGT に関連するセルです（選択した宛先 SGT の出力ポリシー カラム）。

   CoA 通知内の生成 ID が、この SGACL 用にデバイスが保持している生成 ID と異なっている。
3. SGACL データ要求への応答で、Cisco ISE は SGACL のコンテンツ（ACE）を返します。

SGACL 名前付きリストの更新 CoA の開始

SGACL 名前付きリストの更新 CoA をトリガーするには、次の手順を実行します。

ステップ 1 [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）] を選択します。

ステップ 2 SGACL のコンテンツを変更します。SGACL を送信すると、SGACL の生成 ID が変更されます。

ステップ 3 複数の SGACL のコンテンツを変更した後、[プッシュ（Push）] ボタンをクリックして、SGACL 名前付きリストの更新 CoA 通知を開始します。この通知は、すべての TrustSec ネットワーク デバイスに送信され、関連するデバイスのその SGACL コンテンツの更新が提供されます。

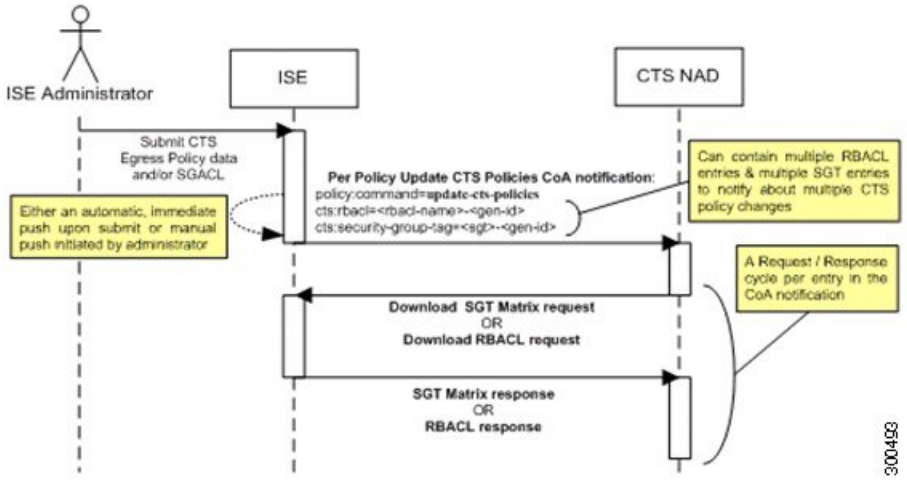
SGACL の名前または IP バージョンを変更しても、その生成 ID は変更されません。そのため、SGACL 名前付きリストの更新 CoA 通知を送信する必要はありません。

ただし、出力ポリシーで使用中の SGACL の名前または IP バージョンを変更することは、その SGACL を含むセルが変更されることを意味するため、この変更でそのセルの宛先 SGT の生成 ID が変更されます。

ポリシーの更新 CoA 通知のフロー

次の図に、ポリシーの CoA 通知のフローを示します。

図 *11* : ポリシーの *CoA* 通知のフロー

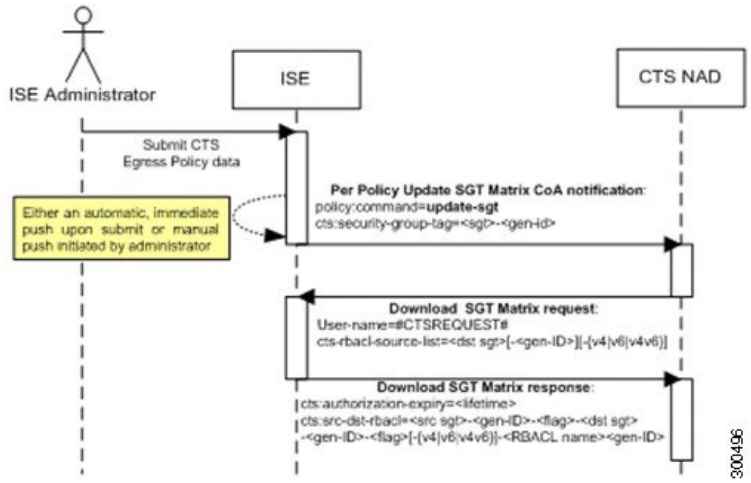


1. Cisco ISE は、TrustSec ネットワーク デバイスにポリシーの更新 CoA 通知を送信します。通知には、複数の SGACL 名とその生成 ID、および複数の SGT 値とその生成 ID が含まれることがあります。
2. デバイスは、複数の SGACL データ要求か複数の SGT データ、またはその両方で応答できます。
3. 各 SGACL データ要求または SGT データ要求に対する応答で、Cisco ISE は関連するデータを返します。

SGT マトリクスの更新 CoA のフロー

次の図に、SGT マトリクスの更新 CoA のフローを示します。

図 *12 : SGT* マトリクスの更新 *CoA* のフロー



1. Cisco ISE は、TrustSec ネットワーク デバイスに SGT マトリクスの更新 CoA 通知を送信します。通知には、SGT 値と生成 ID が含まれます。
2. デバイスは、次の両方の条件が満たされた場合に、SGT データ要求で応答できます。

   SGT がネイバーデバイスまたはエンドポイントの SGT である場合。デバイスは、ネイバーデバイスおよびエンドポイントの SGT に関連するセルをダウンロードして保持します（宛先 SGT）。

   CoA 通知内の生成 ID が、この SGT 用にデバイスが保持している生成 ID と異なっている。
3. SGT データ要求に対する応答で、Cisco ISE は、送信元および宛先 SGT、セルのステータス、そのセルに設定されている SGACL 名の順序リストなど、すべての出力セルのデータを返します。

出力ポリシーからの、SGT マトリクスの更新 CoA の開始

ステップ 1 **[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）]** を選択します。

ステップ 2 [出力ポリシー（Egress Policy）] ページで、セルの内容（ステータス、SGACL）を変更します。

ステップ 3 変更を送信すると、そのセルの宛先 SGT の生成 ID が変更されます。

ステップ 4 複数の出力セルの内容を変更した後、[プッシュ（Push）] ボタンをクリックして、SGT マトリクスの更新 CoA 通知を開始します。この通知は、すべての TrustSec ネットワーク デバイスに送信され、関連するデバイスのセルの内容の更新が提供されます。

TrustSec CoA の概要

次の表に、TrustSec CoA の開始を要求するさまざまなシナリオ、各シナリオで使用される CoA のタイプ、および関連する UI ページの概要を示します。

***Table 15: TrustSec CoA* の概要**

UI ページ	CoA をトリガーする操作	トリガー方法	CoA タイプ	送信先
ネットワーク デバイス（Network Device）	ページの [TrustSec] セクションでの環境 TTL の変更	TrustSec ネットワーク デバイスで正常に送信が行われたとき	環境	特定のネットワーク デバイス
TrustSec AAA サーバー（TrustSec AAA Server）	TrustSec AAA サーバーの変更（作成、更新、削除、順序変更）	[TrustSec AAA サーバー（TrustSec AAA servers）] リストページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス
セキュリティ グループ（Security Group）	SGT の変更（作成、名前変更、削除）	[SGT] リストページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス
NDAC ポリシー（NDAC Policy）	NDAC ポリシーの変更（作成、更新、削除）	[NDAC ポリシー（NDAC policy）] ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	環境	すべての TrustSec ネットワーク デバイス

UI ページ	CoA をトリガーする操作	トリガー方法	CoA タイプ	送信先
SGACL	SGACL ACE の変更	[SGACL] リストページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	RBACL 名前付きリストの更新	すべての TrustSec ネットワーク デバイス
	SGACL 名または IP バージョンの変更	[SGACL] リストページの [プッシュ（Push）] ボタンまたは出力テーブルのポリシー プッシュ ボタンをクリックすると、累積された変更をプッシュできます。	更新 SGT マトリクス	すべての TrustSec ネットワーク デバイス
出力ポリシー（Egress Policy）	SGT の生成 ID を変更するすべての操作	[出力ポリシー（egress policy）] ページの [プッシュ（Push）] ボタンをクリックすると、累積された変更をプッシュできます。	更新 SGT マトリクス	すべての TrustSec ネットワーク デバイス

セキュリティ グループ タグの交換プロトコル

セキュリティ グループ タグ（SGT）の交換プロトコル（SXP）は、TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播するために使用されます。SXP は、ある SGT 対応ネットワーク デバイスから別のデバイスに IP アドレスとともにエンドポイントの SGT を転送するために使用されます。SXP が転送するデータは、IP-SGT マッピングと呼ばれます。エンドポイントが属する SGT は静的または動的に割り当てることができ、SGT はネットワーク ポリシーで分類子として使用できます。

ノードで SXP サービスをイネーブルにするには、[ノードの一般設定（General Node Settings）] ページで [SXPサービスの有効化（Enable SXP Service）] チェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。

SXP はトランスポート プロトコルとして TCP を使用して、2 つの個別のネットワーク デバイス間に SXP 接続をセットアップします。各 SXP 接続には、SXP スピーカーとして指定されたピアと、SXP リスナーとして指定されたピアがあります。ピアは双方向モードで設定することもでき、そのモードでは、それぞれがスピーカーとリスナーの両方として機能します。接続はいずれかのピアによって開始できますが、マッピング情報は常にスピーカーからリスナーに伝播されます。

（注） セッションのバインディングは常にデフォルトの SXP ドメインに伝播されます。

次の表には、SXP 環境で使用される一般的な用語のいくつかを示しています。

IP-SGT マッピング	SXP 接続を介して交換される SGT マッピングへの IP アドレス。 SXP デバイスで学習されたすべてのマッピング（スタティック マッピングおよびセッション マッピングを含む）を表示するには、[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [すべてのSXPマッピング（All SXP Mappings）] の順に選択します。
SXP スピーカー	SXP 接続を介して IP-SGT マッピングを送信するピア。
SXP リスナー	SXP 接続を介して IP-SGT マッピングを受信するピア。

Cisco ISE に追加された SXP ピア デバイスを表示するには、[ワークセンター（Work centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）] の順に選択します。

（注） SXP サービスはスタンドアロン ノードで実行することを推奨します。

SXP サービスを使用する際は、次の点に注意してください。

- SXP ノードを登録解除して、既存の展開に再登録すると、そのノードに接続されている SXP デバイスが展開から削除されます。これらのデバイスは、**[SXPデバイス（SXP Devices）]** ウィンドウ（**[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）]**）には表示されません。SXP ノードを展開に再登録した後、これらのデバイスを手動で再追加する必要があります。ただし、SXP ノードの SXP サービスが無効になっている場合、SXP デバイスは削除されません。
- Cisco ISE は、同じ IP アドレスを持つ複数の SXP セッション バインディングをサポートしていません。

- RADIUS アカウンティング更新の頻度が高すぎる（数秒に約 6 から 8 のアカウンティング更新）場合、アカウンティング更新パケットがドロップされる可能性があり、SXP が IP-SGT バインディングを受信できないことがあります。
- 以前のバージョンの ISE からアップグレードした後は、SXP は自動的に起動しません。アップグレード後に、SXP パスワードを変更し、SXP プロセスを再起動する必要があります。

SXP デバイスの追加

始める前に

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

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）] 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 デバイスの詳細を入力します。

- CSV ファイルを使用して SXP デバイスを追加するには、[CSVファイルからアップロード（Upload from a CSV file）] をクリックします。CSV ファイルを参照して選択し、[アップロード（Upload）] をクリックします。

  また、CSV テンプレート ファイルをダウンロードして、追加するデバイスの詳細を入力し、CSV ファイルをアップロードすることもできます。

- 各 SXP デバイスのデバイスの詳細を手動で追加するには、[単一デバイスの追加（Add Single Device）] をクリックします。

  ピア デバイスの名前、IP アドレス、SXP ロール（リスナー、スピーカー、または両方）、パスワード タイプ、SXP バージョン、および接続されている PSN を入力します。また、ピア デバイスが接続されている SXP ドメインも指定する必要があります。

ステップ 4 （任意）[詳細設定（Advanced Settings）] をクリックし、次の詳細を入力します。

- [最小許容ホールドタイマー（Minimum Acceptable Hold Timer）]：スピーカーが接続状態を保持するためにキープアライブ メッセージを送信する時間を秒単位で指定します。値の範囲は 1 ～ 65534 です。
- [キープアライブタイマー（Keep Alive Timer）]：アップデート メッセージによって他の情報がエクスポートされないインターバル期間にキープアライブ メッセージのディスパッチをトリガーするためにスピーカーによって使用されます。値の範囲は 0 ～ 64000 です。

ステップ 5 [Save] をクリックします。

SXP ドメイン フィルタの追加

SXP デバイスで学習されたすべてのマッピング（スタティック マッピングおよびセッション マッピングを含む）は、[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [すべての SXP マッピング（All SXP Mappings）] ページで表示できます。

デフォルトでは、ネットワークデバイスから学習したセッションマッピングは、デフォルトの VPN グループ（default と呼ばれる）にのみ送信されます。SXP ドメインフィルタを作成して、異なる SXP ドメイン（VPN）にマッピングを送信できます。

SXP ドメイン フィルタを追加するには、次の手順を実行します。

始める前に

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

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [すべての SXP マッピング（All SXP Mappings）] を選択します。

ステップ 2 [SXP ドメイン フィルタの追加（Add SXP Domain Filter）] をクリックします。

ステップ 3 次の手順を実行します。

- サブネットの詳細を入力します。このサブネットからの IP アドレスを持つネットワーク デバイスのセッション マッピングは、[SXP ドメイン（SXP Domain）] フィールドで選択された SXP ドメイン（VPN）に送信されます。
- [SGT] ドロップダウン リストから SGT を選択します。この SGT に関連するセッションマッピングは、[SXP ドメイン（SXP Domain）] フィールドで選択された SXP ドメインに送信されます。

  サブネットと SGT の両方を指定した場合、このフィルタに一致するセッション マッピングは、[SXP ドメイン（SXP Domain）] フィールドで選択した SXP ドメインに送信されます。
- マッピングを送信する必要がある SXP ドメインを選択します。

ステップ 4 [保存（Save）] をクリックします。

SXP ドメインフィルタを更新または削除することもできます。フィルタを更新するには、[SXP ドメイン フィルタの管理（Manage SXP Domain Filter）] をクリックし、更新するフィルタ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。フィルタを削除するには、削除するフィルタの横にあるチェックボックスをオンにして、[ごみ箱（Trash）] > [選択済み（Selected）] をクリックします。

SXP の設定

始める前に

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

ステップ 1 [ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [SXP 設定（SXP Settings）] を選択します。

ステップ 2 [SXP設定（SXP Settings）] ページに必要な詳細を入力します。

[SXP バインディングを PxGrid で公開（Publish SXP Bindings on PxGrid）] チェックボックスをオフにすると、IP-SGT マッピングはネットワーク デバイス全体に伝達されません。

ステップ 3 [保存（Save）] をクリックします。

（注） SXP 設定が変更されると、SXP サービスが再起動されます。

シスコ アプリケーション セントリック インフラストラクチャと Cisco ISE の接続

Cisco ISE では、SGT および SXP マッピングを内部エンドポイントグループ（IEPG）、外部エンドポイントグループ（EEPG）、シスコ アプリケーション セントリック インフラストラクチャ（Cisco ACI）のエンドポイント（EP）設定と同期することができます。

Cisco ISE は、ISE で IEPG を同期して関連する読み取り専用の SGT を作成することで、Cisco ACI ドメインから TrustSec ドメインに着信するパケットをサポートします。これらの SGT は、Cisco ACI に設定されたエンドポイントをマッピングし、ISE で関連 SXP マッピングを作成します。SGT は [セキュリティグループ（Security Groups）] ページに表示されます（[学習元（Learned From）] フィールドに値 [Cisco ACI] が入った状態）。[すべての SXP マッピング（All SXP Mappings）] ページで SXP マッピングを表示できます。これらのマッピングは、（[Cisco ACI の設定（Cisco ACI Settings）] ページで）[ポリシープレーン（Policy Plane）] オプションが選択され、SXP デバイスが [Cisco ACI の設定（Cisco ACI Settings）] ページで設定した SXP ドメインに属している場合にのみ、ACI に送信されます。

（注） 読み取り専用 SGT は、IP-SGT マッピング、マッピンググループ、および SXP ローカルマッピングでは使用できません。

セキュリティ グループを追加する際には、[ACI に伝達（Propagate to ACI）] オプションを使用して、SGT を Cisco ACI に送信する必要があるかどうかを指定できます。このオプションを有

効にすると、この SGT に関連する SXP マッピングが Cisco ACI に送信されます。ただし、（[Cisco ACI の設定（Cisco ACI Settings）] ページで）[ポリシープレーン（Policy Plane）] オプションが選択され、SXP デバイスが [Cisco ACI の設定（Cisco ACI Settings）] ページで設定した SXP ドメインに所属している場合にのみに、Cisco ACI に送信されます。

Cisco ACI は SGT を同期して関連する EEPG を作成することで、TrustSec ドメインから Cisco ACI ドメインに送信されるパケットをサポートします。Cisco ACI は、Cisco ISE からの SXP マッピングに基づいて EEPG でサブネットを作成します。これらのサブネットは、対応する SXP マッピングが Cisco ISE で削除されるときに、Cisco ACI から削除されません。

IEPG が Cisco ACI で更新されると、対応する SGT 設定が Cisco ISE で更新されます。SGT が Cisco ISE に追加されると、新しい EEPG が Cisco ACI に作成されます。SGT が削除されると、対応する EEPG が Cisco ACI で削除されます。エンドポイントが Cisco ACI で更新されると、対応する SXP マッピングは Cisco ISE で更新されます。

Cisco ACI サーバーとの接続が失われると、接続が再確立されるときに、Cisco ISE は再びデータを再同期します。

（注） Cisco ACI の統合機能を使用するには、SXP サービスを有効にする必要があります。

Cisco ISE と Cisco ACI を正常に統合するには、署名付き証明書に適切な SAN フィールドが必要です。Cisco ISE は、APIC サーバーによって提示される証明書の SAN 拡張プロパティで指定された値を使用します。

（注） Cisco ISE で現在サポートされているのは、Cisco ACI との IPv4-SXP バインディングのみです。Cisco ACI からの IPv6-SGT バインディングはサポートされていません。

Cisco ACI の設定

始める前に

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificate）] > [インポート（Import）]** を選択します。

ステップ 2 Cisco ACI 証明書のインポート詳細については、信頼できる証明書ストアへのルート証明書のインポートを参照してください。

ステップ 3 **[ワークセンター（Work Centres）] > [TrustSec] > [設定（Settings）] > [ACI 設定（ACI Settings）]** を選択します。

ステップ 4 Cisco ACI からエンドポイントを学習し、SXP を使用してそれらを伝播するには、[ACI 統合の有効化（Enable ACI Integration）] チェックボックスをオンにします。

ステップ 5 [ポリシープレーン（Policy Plane）] オプションを選択した場合は、次の詳細を入力します。

- **[IP アドレス/ホスト名（IP address / Host name）]**：ACI サーバーの IP アドレスまたはホスト名を入力します。カンマで区切った 3 つの IP アドレスまたはホスト名を入力できます。
- [管理者名（Admin name）]：Cisco ACI 管理者ユーザーのユーザー名を入力します。
- [管理者パスワード（Admin password）]：Cisco ACI 管理者ユーザーのユーザー名を入力します。
- [テナント名（Tenant name）]：Cisco ACI で設定されているテナントの名前を入力します。
- **L3 ルートネットワーク名（L3 Route network name）**：ポリシー要素を同期させるために Cisco ACI で設定されているレイヤ 3 ルートネットワークの名前を入力します。
- [テスト設定（Test Settings）] をクリックして、Cisco ACI サーバーとの接続性を確認します。
- [新規SGTサフィックス（New SGT Suffix）]：このサフィックスは、ACI から学習された EPG に基づいて新規に作成された SGT に追加されます。

  （注） EPG 名が 32 文字を超える場合は切り捨てられます。ただし、[セキュリティ グループ（Security Groups）] リスト ページの [説明（Description）] フィールドで EPG のフルネーム、アプリケーション プロファイル名、SGT サフィックスの詳細を確認できます。

- [新規EPGサフィックス（New EPG Suffix）]：このサフィックスは、Cisco ISE から学習された SGT に基づいて Cisco ACI で新規に作成された EPG に追加されます。
- [SXP伝達（SXP Propagation）] エリアで、すべての SXP ドメインを選択するか、または Cisco ACI とマッピングを共有する SXP ドメインを指定することができます。

ステップ 6 [Save] をクリックします。

ユーザー レポート別上位 N 個の RBACL ドロップの実行

ユーザー レポート別上位 N 個の RBACL ドロップを実行して、特定のユーザーによるポリシー違反（パケット ドロップに基づく）を表示できます。

ステップ 1 [操作（Operations）] > [レポート（Reports）] > [TrustSec] を選択します。

ステップ 2 [ユーザー別上位 N 個の RBACL ドロップ（Top N RBACL Drops by User）] をクリックします。

ステップ 3 [フィルタ（Filters）] ドロップダウン メニューから、必要なモニター モードを追加します。

ステップ 4 選択したパラメータの値をこれに応じて入力します。[強制モード（Enforcement mode）] ドロップダウン リストから、[強制（Enforce）]、[モニター（Monitor）]、または [両方（Both）] としてモードを指定できます。

ステップ 5 [時間範囲（Time Range）] ドロップダウン メニューから、レポート データを収集する期間を選択します。

ステップ 6 [実行（Run）] をクリックして、選択したパラメータとともに特定の期間のレポートを実行します。

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。