ポリシーの設定および管理

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。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 ルールが含まれています。

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 サーバに要求を送信します

（注） [デバイス管理（Device Administration）] ワーク センターから、ポリシー セットに関連する TACACS サーバ順序を選択することもできます。TACACS サーバ順序を使用して、一連の TACACS プロキシ サーバ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。このワーク センターをアクセスするには、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ポリシー セット（Policy Sets）]** を選択します。

新規ポリシー モデル

認証、認可、例外を含め、すべてのネットワーク アクセス ポリシーおよびポリシーセットは、Cisco ISE 2.3 以降では [ポリシーセット（Policy Sets）] ウィンドウの下に統合されます。各ポリシー セットは、ポリシー階層の最上位レベルで定義されたコンテナであり、その下にそのセットのすべての関連する認証および認可ポリシーおよびポリシー例外ルールが設定されます。

条件に基づいて、認証と認可の両方に複数のルールを定義できます。また、条件とその他の関連設定に簡単にアクセスして、新しいポリシー セット インターフェイスから直接再利用できるようになりました。ポリシー セットの照合順序は、新しい [ポリシーセット（Policy Set）] インタフェイスに表示される順序によって決まります。チェックは、**ポリシーセット**テーブルの最初の行から開始され、一致が見つかるまで続きます。一致するものが見つからない場合は、システムのデフォルト ポリシー セットが使用されます。同じ論理を使用して正しい認証ルールの照合と選択が行われ、次に正しい認可ルールの照合と選択が行われます。各**ポリシー**

セットテーブルの先頭からチェックが開始され、一致が見つかるまで各ルールがチェックされます。一致する他のルールがない場合は、デフォルト ルールが使用されます。

新しいポリシー モデルは、古いユーザ インターフェイスを使用して以前のバージョンで追加された可能性のあるすべてのポリシーを表しますが、ネットワーク アクセスを論理的に管理できる大幅に簡素化された改良済みのインターフェイスが提供されます。

スタンドアロンの認証および許可ポリシーの変更

スタンドアロンの認証ルールを使用する場合、ISE 2.2 以前のバージョンのルールは新しいポリシー モデルに変換されます。認証ルールに割り当てられている許可されたプロトコルに基づいて、2 つの個別のシナリオがあります。

1. システム内のすべての「外部パート」に、デフォルト パートを含む同じ許可されたプロトコルが割り当てられている場合、すべての元の認証ルールは次のように変換されます。

   すべての「外部パート」は、新しいポリシー モデルの単一のポリシー セットに変換されます。新しいポリシー セットはデフォルトと呼ばれ、ポリシー セット レベルでは条件が定義されず、統一された許可プロトコルが割り当てられます。すべての内部パートは、新しいデフォルト ポリシー セット内の認証ポリシーの一部としてルールに変換されます。

   次の表に、同じ許可プロトコルを使用する古いスタンドアロン認証ルールのセットの変換を示します（シナリオ 1）。この表では、各行の形式は次のとおりです。

   名前（条件/結果）

   たとえば認証外部パート 1（外部条件/許可されるプロトコル A）の場合：

   - 名前：認証外部パート 1
   - 条件：外部条件
   - 結果：許可されるプロトコル A

表 *1*: 同じ許可されたプロトコルを使用したスタンドアロン認証ポリシー

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
1. 認証外部パート1（外部条件1/許可されるプロトコル A） **1.** 認証内部パート1.1（内部条件1.1/IDストア A） **2.** 認証内部パート1.2（内部条件1.2/IDストア A） **3.** 認証内部パート1.3（内部条件1.3/IDストア A） **4.** 認証内部1デフォルト（条件なし/IDストア B） **2.** 認証外部パート2（外部条件2/許可されるプロトコル A） **1.** 認証内部パート2.1（内部条件2.1/IDストア A） **2.** 認証内部パート2.2（内部条件2.2/IDストア A） **3.** 認証内部パート2.3（内部条件2.3/IDストア A） **4.** 認証内部2デフォルト（条件なし/IDストア B） **3.** 認証外部パート3（外部条件3/許可されるプロトコル A） **1.** 認証内部3デフォルト（条件なし/IDストア B） **4.** デフォルト認証外部パート（条件なし/許可されるプロトコル A/デフォルト IDストア） **5.** 例外 1 **6.** 許可ルール 1 **7.** 許可ルール 2	

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
	1. デフォルト（条件なし/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. 認証外部パート 1：認証内部パート 1.1（外部条件 1＋内部条件 1.1/ID ストア A） 2. 認証外部パート 1：認証内部パート 1.2（外部条件 1＋内部条件 1.2/ID ストア A） 3. 認証外部パート 1：認証内部パート 1.3（外部条件 1＋内部条件 1.3/ID ストア A） 4. 認証外部パート 1：認証内部 1 デフォルト（外部条件 1/ID ストア B） 5. 認証外部パート 2：認証内部パート 2.1（外部条件 2＋内部条件 2.1/ID ストア A） 6. 認証外部パート 2：認証内部パート 2.2（外部条件 2＋内部条件 2.2/ID ストア A） 7. 認証外部パート 2：認証内部パート 2.3（外部条件 2＋内部条件 2.3/ID ストア A） 8. 認証外部パート 2：認証内部 2 デフォルト（外部条件 2/ID ストア B） 9. 認証外部パート 3：認証内部 3 デフォルト（外部条件 3/ID ストア B） 10. デフォルト認証外部パート（条件なし/デフォルト ID ストア） 2. 例外 1 3. 許可ポリシー（コンテナ）

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
	1. 許可ルール 1 2. 許可ルール 2

2. システム内の「外部パート」の少なくとも1つに、デフォルトパートなどの他の部分とは異なる許可されたプロトコルが割り当てられている場合、すべての元の認証ルールは次のように変換されます。

   各「外部パート」は、新しいポリシー モデルの個別のポリシー セットに変換されます。新しいポリシーセットは、その特定の新しいセットの元の外部パートの名前に基づいて名前が付けられます。各ポリシー セットのポリシー セット レベルでは、元の外部パートの条件と許可プロトコルが割り当てられます。各外部パートのすべての内部パートは、新しいポリシー セット内の認証ポリシーの一部として 1 対 1 で認証ルールに変換されます。

   次の表に、異なる許可プロトコルを使用する古いスタンドアロン認証ルールのセットの変換を示します（シナリオ 2）。この表では、各行の形式は次のとおりです。

   名前（条件/結果）

   たとえば認証外部パート 1（外部条件/許可されるプロトコル A）の場合：

   - 名前：認証外部パート 1
   - 条件：外部条件
   - 結果：許可されるプロトコル A

表 *2:* 異なる許可されたプロトコルを使用したスタンドアロン認証ポリシー

Cisco ISE 2.3 より前：デフォルト認証	**Cisco ISE 2.3** 以降へのアップグレード後：ポリシー セット
1. 認証外部パート 1（外部条件 1/許可されるプロトコル A） **1.** 認証内部パート 1.1（内部条件 1.1/ID ストア A） **2.** 認証内部パート 1.2（内部条件 1.2/ID ストア A） **3.** 認証内部パート 1.3（内部条件 1.3/ID ストア A） **4.** 認証内部 1 デフォルト（条件なし/ID ストア B） **2.** 認証外部パート 2（外部条件 2/許可されるプロトコル B） **1.** 認証内部パート 2.1（内部条件 2.1/ID ストア A） **2.** 認証内部パート 2.2（内部条件 2.2/ID ストア A） **3.** 認証内部パート 2.3（内部条件 2.3/ID ストア A） **4.** 認証内部 2 デフォルト（条件なし/ID ストア B） **3.** 認証外部パート 3（外部条件 3/許可されるプロトコル C） **1.** 認証内部 3 デフォルト（条件なし/ID ストア B） **4.** デフォルト認証外部パート（条件なし/許可されるプロトコル A/ID ストア C） **5.** 例外 1 **6.** 許可ルール 1 **7.** 許可ルール 2	

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
	1. デフォルト認証外部パート 1（外部条件 1/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. 認証内部パート 1.1（内部条件 1.1/ID ストア A） 2. 認証内部パート 1.2（内部条件 1.2/ID ストア A） 3. 認証内部パート 1.3（内部条件 1.3/ID ストア A） 4. 認証内部 1 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2 1. デフォルト認証外部パート 2（外部条件 2/許可されるプロトコル B） 1. 認証ポリシー（コンテナ） 1. 認証内部パート 2.1（内部条件 2.1/ID ストア A） 2. 認証内部パート 2.2（内部条件 2.2/ID ストア A） 3. 認証内部パート 2.3（内部条件 2.3/ID ストア A） 4. 認証内部 2 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
	1. デフォルト認証外部パート3（外部条件3/許可されるプロトコル C） 1. 認証ポリシー（コンテナ） 1. 認証内部 3 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2 1. デフォルト（条件なし/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. デフォルト認証ルール（条件なし/ID ストア C） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2

ポリシー セットの変更

以前のバージョンからISE2.3以降にアップグレードする場合、表示される新しいポリシーセットはここで説明する古い ISE バージョンの場合とは異なりますが、動作は同じままです。

次の図は、Cisco ISE 2.3 以降へのアップグレード後のポリシー セットの変更を示しています。

図 *1 : ISE 2.3* より前：ポリシー セット

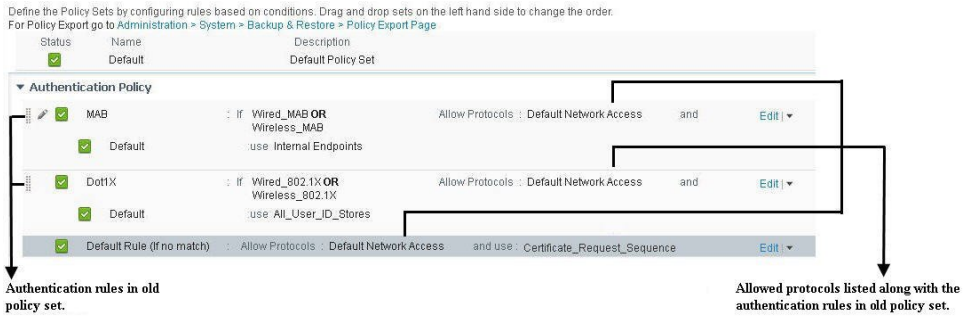
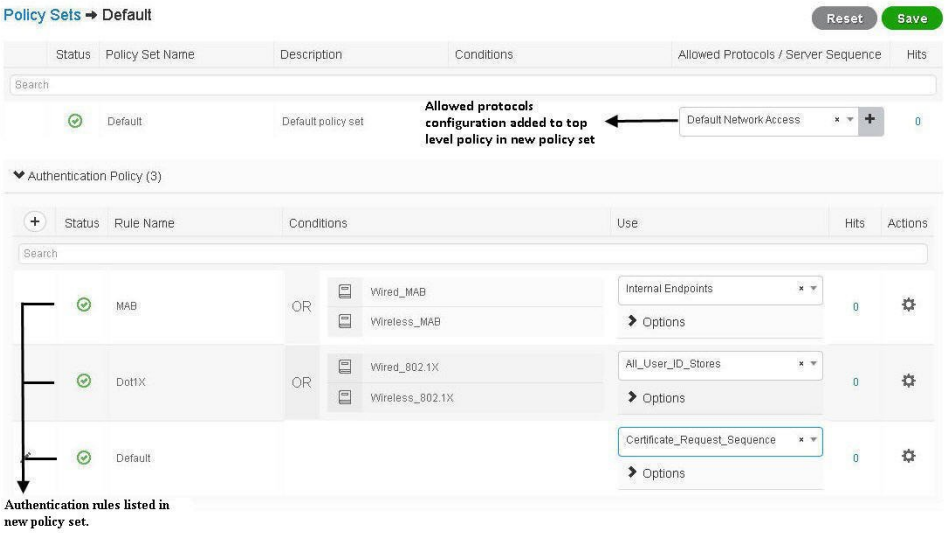


図 *2 : ISE 2.3* から：ポリシー セット



ISE 2.2 以前のバージョンのポリシーは、新しいポリシー モデルに変換されます。認証ルールに割り当てられている許可されたプロトコルに基づいて、2 つの個別のシナリオがあります。

1. 単一のポリシーセット内のすべての「外部パート」に同じ許可されたプロトコルが割り当てられている場合、元のポリシー セットはすべて次のように変換されます。

   - すべての「外部パート」は、新しいポリシー モデルの単一のポリシー セットに変換されます。新しいポリシー セットは、元のポリシー セットと同じ名前になります。たとえば、古いモデルでポリシーセットの名前が「全従業員」になっている場合、新しいモデルでも「全従業員」と呼ばれます。

     次の表に、同じ許可プロトコルを使用する認証ルールを含む古いポリシーセットの変換を示します（シナリオ 1）。この表では、各行の形式は次のとおりです。

     名前（条件/結果）

たとえば認証外部パート 1（外部条件/許可されるプロトコル A）の場合：

- 名前：認証外部パート 1
- 条件：外部条件
- 結果：許可されるプロトコル A

表 *3 :* 同じ許可されたプロトコルを使用したポリシー セットの変換

Cisco ISE 2.2 以前からの古いポリシー セット	**Cisco ISE 2.3** 以降へのアップグレード後の新しいポリシー セット

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
1. ポリシー セット A（条件 A/結果なし） 1. 認証外部パート 1（外部条件 1/許可されるプロトコル A） 1. 認証内部パート 1.1（内部条件 1.1/ID ストア A） 2. 認証内部パート 1.2（内部条件 1.2/ID ストア A） 3. 認証内部パート 1.3（内部条件 1.3/ID ストア A） 4. 認証内部 1 デフォルト（条件なし/ID ストア B） 2. 認証外部パート 2（外部条件 2/許可されるプロトコル A） 1. 認証内部パート 2.1（内部条件 2.1/ID ストア A） 2. 認証内部パート 2.2（内部条件 2.2/ID ストア A） 3. 認証内部パート 2.3（内部条件 2.3/ID ストア A） 4. 認証内部 2 デフォルト（条件なし/ID ストア B） 3. 認証外部パート 3（外部条件 3/許可されるプロトコル A） 1. 認証内部 3 デフォルト（条件なし/ID ストア B） 4. デフォルト認証外部パート（条件なし/許可されるプロトコル A/ID ストア C） 5. 例外 1 6. 許可ルール 1 7. 許可ルール 2	

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
	1. ポリシー セット A（条件 A/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. 認証外部パート 1：認証内部パート 1.1（外部条件 1 + 内部条件 1.1/ID ストア A） 2. 認証外部パート 1：認証内部パート 1.2（外部条件 1 + 内部条件 1.2/ID ストア A） 3. 認証外部パート 1：認証内部パート 1.3（外部条件 1 + 内部条件 1.3/ID ストア A） 4. 認証外部パート 1：認証内部 1 デフォルト（外部条件 1/ID ストア B） 5. 認証外部パート 2：認証内部パート 2.1（外部条件 2 + 内部条件 2.1/ID ストア A） 6. 認証外部パート 2：認証内部パート 2.2（外部条件 2 + 内部条件 2.2/ID ストア A） 7. 認証外部パート 2：認証内部パート 2.3（外部条件 2 + 内部条件 2.3/ID ストア A） 8. 認証外部パート 2：認証内部 2 デフォルト（外部条件 2/ID ストア B） 9. 認証外部パート 3：認証内部 3 デフォルト（外部条件 3/ID ストア B） 10. デフォルト認証外部パート（条件なし/ID ストア C） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
	2. 許可ルール 2

- 新しくアップグレードされたポリシー セットには、元のポリシー セットからの外部条件と内部条件を組み合わせて変換される認証ルールのリストが含まれています。変換中に作成されるそれぞれの新しい認証ルールは、内部パートの名前を含むサフィックス付きの古い外部パートの名前に基づいて名前が付けられます。たとえば、上記の表のように、古いポリシーセットが「ポリシーセットA」と呼ばれ、その認証の「外部パート」の 1 つが外部パート 1 と呼ばれ、認証の「内部パート」の 1 つが内部パート 1 と呼ばれている場合、新しく作成された認証ルールは、ポリシー セット A 内で「外部パート 1：内部パート 1」と呼ばれます。同様に、古いポリシー セットが「全従業員」ポリシーセットと呼ばれ、その認証の「外部パート」の 1 つがロンドンと呼ばれ、認証の「内部パート」の 1 つが「有線 MAB」と呼ばれている場合、新しく作成された認証ルールは「全従業員」ポリシー セット内で「ロンドン：有線 MAB」と呼ばれます。認証ポリシーのデフォルトの外部パートは、デフォルトの認証ルールとして変換されます。システムのデフォルト ポリシー ルールは、作成または変換された他のルールに関係なく、認証テーブル全体の最後のルールとして表示され、このルールは移動または削除できません。
- 外部パートに定義された条件（それに基づいて認証ルールが照合されます）は、内部パートの条件（認証に使用される ID ストアを示す）と組み合わされます。新しい結合条件は、新しいモデルのポリシーセット内の単一の認証ルールで設定されます。ポリシー セット内の新しい個別ルールは、古いポリシー セットの個別の外部パートごとに作成されます。

2. ポリシーセット内の「外部パート」に対して 2 つ以上の許可プロトコルが選択されている場合、元のポリシー セットはすべて次のように変換されます。
   - 古いポリシーセット内の各認証ルールの各「外部パート」は、新しいモデルで新しい個別のポリシー セットに変換されます。この新しいポリシー セットは、新しいポリシー モデルの [認証ポリシー（Authentication Policy）] セクションの下にある同じ元の「外部パート」から「条件」を配置します。

     次の表に、ISE 2.2 以前のバージョンから ISE 2.3 以降への古いポリシー セットの変換を示します（シナリオ 2）。

表 *4 :* 異なる許可されたプロトコルを使用したポリシー セットの変換

Cisco ISE 2.2 以前からの古いポリシー セット	**Cisco ISE 2.3** 以降へのアップグレード後の新しいポリシー セット

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
1. ポリシー セット A（条件 A/結果なし） 1. 認証外部パート 1（外部条件 1/許可されるプロトコル A） 1. 認証内部パート 1.1（内部条件 1.1/ID ストア A） 2. 認証内部パート 1.2（内部条件 1.2/ID ストア A） 3. 認証内部パート 1.3（内部条件 1.3/ID ストア A） 4. 認証内部 1 デフォルト（条件なし/ID ストア B） 2. 認証外部パート 2（外部条件 2/許可されるプロトコル B） 1. 認証内部パート 2.1（内部条件 2.1/ID ストア A） 2. 認証内部パート 2.2（内部条件 2.2/ID ストア A） 3. 認証内部パート 2.3（内部条件 2.3/ID ストア A） 4. 認証内部 2 デフォルト（条件なし/ID ストア B） 3. 認証外部パート 3（外部条件 3/許可されるプロトコル C） 1. 認証内部 3 デフォルト（条件なし/ID ストア B） 4. デフォルト認証外部パート（条件なし/許可されるプロトコル A/ID ストア C） 5. 例外 1 6. 許可ルール 1 7. 許可ルール 2	

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
	1. ポリシー セット A：認証外部パート 1（条件 A + 外部条件 1/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. 認証内部パート 1.1（内部条件 1.1/ID ストア A） 2. 認証内部パート 1.2（内部条件 1.2/ID ストア A） 3. 認証内部パート 1.3（内部条件 1.3/ID ストア A） 4. 認証内部 1 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2 1. ポリシー セット A：認証外部パート 2（条件 A + 外部条件 2/許可されるプロトコル B） 1. 認証ポリシー（コンテナ） 1. 認証内部パート 2.1（内部条件 2.1/ID ストア A） 2. 認証内部パート 2.2（内部条件 2.2/ID ストア A） 3. 認証内部パート 2.3（内部条件 2.3/ID ストア A） 4. 認証内部 2 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
	2. 許可ルール 2 1. ポリシー セット A：デフォルト認証 外部パート 3（条件 A + 外部条件 3/許可されるプロトコル C） 1. 認証ポリシー（コンテナ） 1. 認証内部 3 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2 1. ポリシー セット A：デフォルト（条件 A/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. デフォルト認証ルール（条件なし/ID ストア C） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2

- 変換時に作成される新しいポリシーセットは、外部パート名を含むサフィックスを使用して抽出された古いポリシーセットの名前に基づいて名前が付けられます。たとえば、上記の表のように、古いポリシーセットが「ポリシーセットA」と呼ばれ、その認証の「外部パート」の1つが外部パート1と呼ばれている場合、新しく作成されたポリシー セットは「ポリシー セットA：外部パート1」と呼ばれます。同じように、古いポリシーセットが「ロンドン」と呼ばれ、その認証の「外部パート」の1つが有線 MAB と呼ばれている場合、新しく作成されたポリシー セットは「ロンドン：有線 MAB」と呼ばれます。

古い各ポリシーセットのデフォルトの外部パートも、「ロンドン：デフォルト」などのように、他のすべての外部パートと同様に新しいポリシーセットに変換されます。システム デフォルト ポリシー セットは、作成または変換された他のポリシー セットに関係なく、テーブル全体の最後のポリシーセットとして表示され、移動または削除できません。

- 古いポリシーセットの最上位レベルで定義された条件は、許可された正しいプロトコルを選択するように設計された外部認証パート条件と組み合わされます。新しい結合条件は、新しいモデルの新しいポリシーセットごとに最上位レベルのルールで構成されます。古い各ポリシー セットの各外部パートごとに新しい個別のポリシー セットが作成されます。

許可ルール/例外の変更

グローバル例外とローカル例外に加えて、認可ルールもポリシーセット内から管理できるようになりました。古いポリシーセット内のすべての認可ルールおよび例外は、認証ポリシールールの変換の結果として生じるすべての新しいポリシーセットにも適用されます。許可ポリシーの変更は、外部パートに設定されている許可されたプロトコルに関係なく、アップグレードされるすべてのポリシー セットに適用されます。

ポリシー セットの評価

新しいインターフェイスでポリシーセットは、[ポリシーセット（Policy Set）]テーブルに表示される順序に従って一致の有無がチェックされます。たとえば、古い「ロンドン」ポリシーセットに、変換前にステータスが異なる3つの外部パートがあり、古い「ニューヨーク」セットにデフォルトの外部パートのみが含まれている場合、新しいポリシー セット インターフェイスのテーブルには新しいポリシー セットとシステムのデフォルト ポリシー セットが次の順序で表示されます。

ポリシー セット名
ロンドン：有線 MAB
ロンドン：ワイヤレス MAB
ロンドン：デフォルト
ニューヨーク：デフォルト
デフォルト

最初の2つのセットが一致しない場合、システムは「ロンドン：デフォルト」をチェックします。「ロンドン：デフォルト」が一致しない場合、システムは次に「ニューヨーク：デフォルト」をチェックします。「ニューヨーク：デフォルト」も一致しない場合、システムはポリシーとして「デフォルト」のみを使用します。

同じ論理を使用して正しい認証ルールの照合と選択が行われ、次に正しい許可ルールの照合と選択が行われます。各テーブルの先頭から開始し一致が見つかるまで各ルールがチェックされます。一致する他のルールがない場合は、デフォルト ルールが使用されます。

新しく変換されたポリシー セットのステータス

認証ルールに異なる許可されたプロトコルを使用するポリシーセットを変換する際に、新しく変換されたポリシーセットのステータスは、古いポリシーセットのステータスと古いポリシーセットの「外部パート」のステータスに基づいて次のように決定されます。

古いポリシー セットのステータス	古いポリシー セットの「外部パート」のステータス	新しいポリシー セットのステータス
無効	無効	無効
無効	モニタ	無効
無効	有効	無効
モニタ	無効	無効
モニタ	モニタ	モニタ
モニタ	有効	モニタ
有効	無効	無効
有効	モニタ	モニタ
有効	有効	有効

新しく変換された認証ルールのステータス

認証ルールに同じ許可されたプロトコルを使用するポリシーセットを変換する際に、新しく変換された認証ルールのステータスは、古い認証ルールの「外部パート」のステータスと対応する古い認証ルールの「内部パート」のステータスに基づいて次のように決定されます。

古い認証ルールの「外部パート」のステータス	対応する古い認証ルールの「内部パート」のステータス	変換された認証ルールのステータス
無効	無効	無効
無効	モニタ	無効
無効	有効	無効
モニタ	無効	無効
モニタ	モニタ	モニタ
モニタ	有効	モニタ
有効	無効	無効
有効	モニタ	モニタ

古い認証ルールの「外部パート」のステータス	対応する古い認証ルールの「内部パート」のステータス	変換された認証ルールのステータス
有効	有効	有効

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
  - ゲスト ユーザ
  - 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（RSA または SafeWord サーバ）
  - 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。

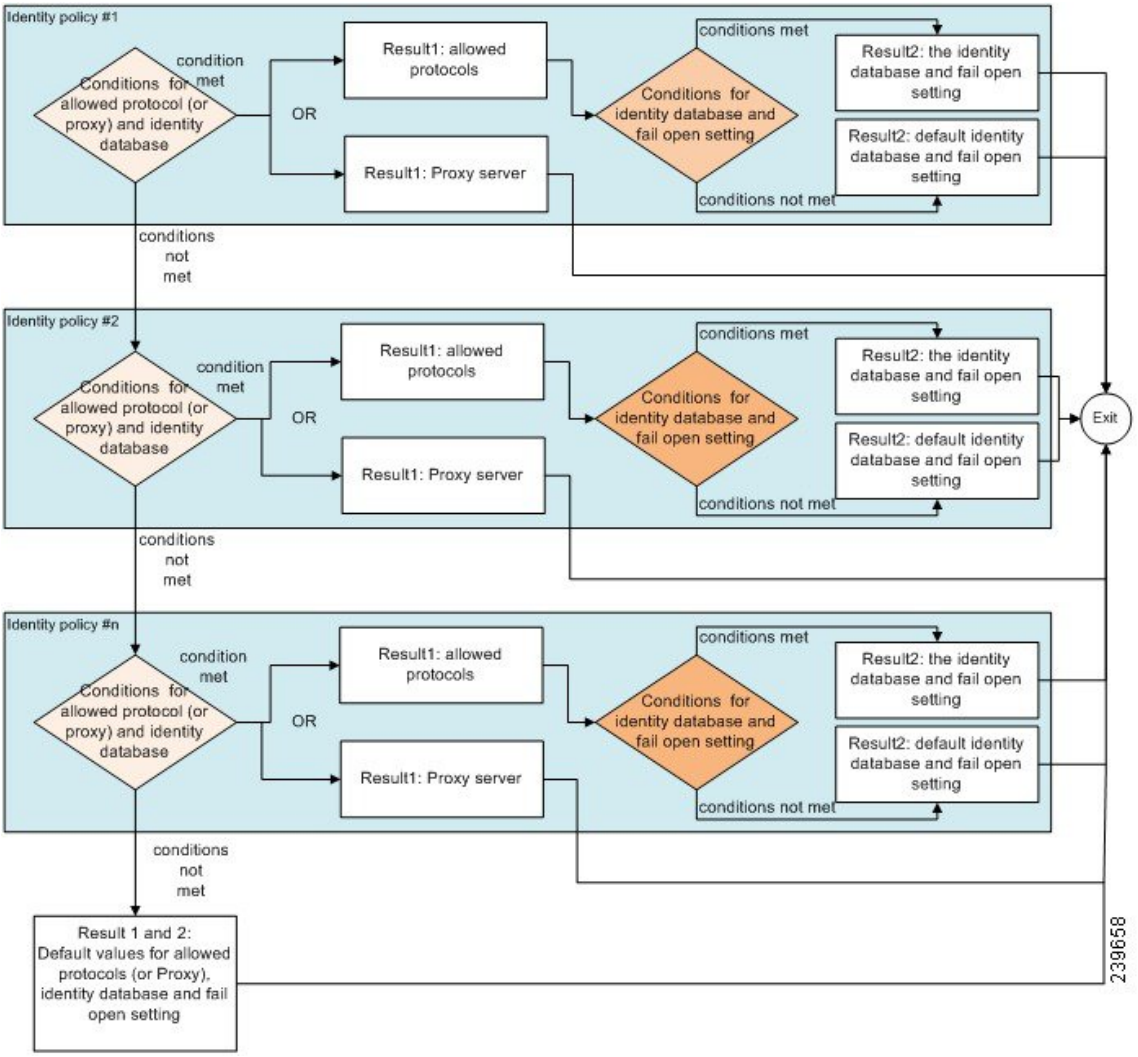
認証ポリシーのフロー

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、指定した条件を評価し、評価の結果に基づいて、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 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 *3:* 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。
- ユーザが見つからない：どの ID データベースでもこのユーザ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 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、ポリシー条件 （37 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、リアルタイムの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。
- 詳細レポートを表示するには、[詳細（Details）] カラムにある虫眼鏡アイコンをクリックします。

（注） 認証概要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。

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。

- 許可ポリシーおよび許可プロファイル間の関係を理解している
- 許可プロファイル 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
- 許可プロファイルの権限の構成を理解している

許可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、**[認証（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許可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 ペインを使用します。[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（Common Tasks）] 設定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（Common Tasks）] 属性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。

（注） 複数のユーザを追跡すると、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。

（注） ロケーション サービスを使用するには、ISE Plus ライセンスが必要です。

MSE サーバの追加

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（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 サーバ名、ホスト名/IP アドレス、パスワードなど、MSE サーバの詳細を入力します。

ステップ 4 指定したサーバの詳細を使用して 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（Downloadable ACLs）

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。

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 （32 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

ISE の場合、ダウンロード可能な ACL（DACL）は、さまざまなユーザおよびユーザ 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実装できます。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 を設定すると、ネットワーク上で関連する許可ポリシーにこの DACL を適用できます。DACL を許可ポリシーに適用すると、そのタイプを変更したり、ISE から削除したりできなくなります。ポリシーですでに使用されている DACL タイプを変更するには、DACL を複製し、その複製を更新するか、ポリシーから DACL を削除して、DACL を更新し、該当する場合に再適用します。

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。
  - 必要な形式を入力する [非依存（Agnostic）]。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。

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 [送信（Submit）] をクリックします。

Active Directory ユーザ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。

ユーザをエンドユーザ 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。

- 許可ポリシー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。

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 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、ポリシー条件 （37 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 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）] > [許可プロファイル（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 ACI に反映するには、[ACI に伝播（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、ACI が [ACI の設定（ACI Settings）] ページで選択した VPN に属するときのみ 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。

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 [設定（Set）] ビューの [許可ポリシーのローカル例外（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 [設定（Set）] ビューの [許可ポリシーのグローバル例外（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。

許可例外ポリシー ルールは、許可ポリシー ルールと同じように設定されます。例外ポリシーを設定するには、上記の通常の許可ポリシーの設定手順を参照してください。許可ポリシーの設定 （34 ページ）

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 （54 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 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。

（注） Calling-Station-ID は Cisco ISE2.3 以降の AA:BB:CC:DD:EE:FF 形式でのみ受け入れられます。したがって、承認条件は、Calling-Station-ID が AA-BB-CC-DD-EE-FF 形式で提供されていると失敗する可能性があります。

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。ユーザ情報が内部ユーザ属性に基づいている場合は、内部ユーザ 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（**Attributes**）	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）	Yes	Yes
	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	Yes	Yes

ディクショナリ	属性（**Attributes**）	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
Network Access	ISE Host Name	Yes	Yes
	AuthenticationMethod	×	○
	AuthenticationStatus	×	×
	CTSDeviceID	×	×
	Device IP Address（デバイス IP アドレス）	Yes	Yes
	EapAuthentication（マシンのユーザの認証時に使用される EAP 方式）	×	○
	EapTunnel（トンネルの確立に使用される EAP 方式）	×	○
	プロトコル	Yes	Yes
	UseCase	Yes	Yes
	UserName	×	○
	WasMachineAuthenticated	×	×

ディクショナリ	属性（**Attributes**）	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	×	○
	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		

[条件スタジオ（Conditions Studio）] の操作

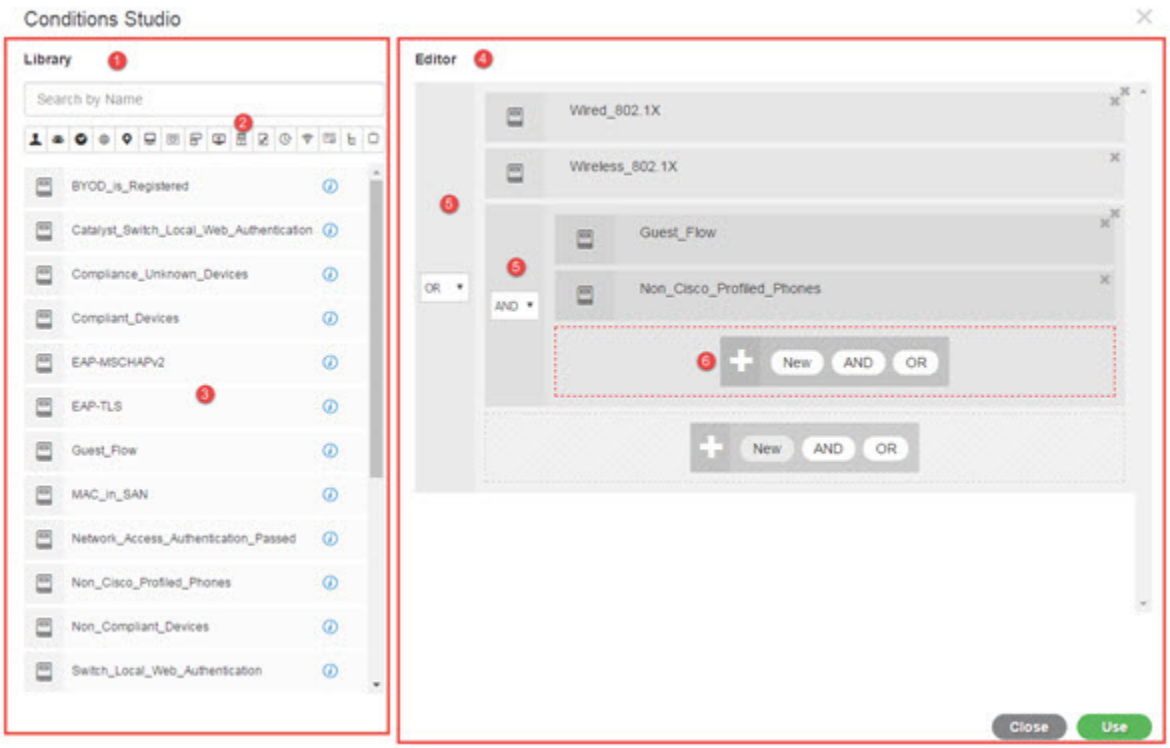
[条件スタジオ（Conditions Studio）] は、条件の作成、管理、および再利用に使用します。条件には複数のルールを含めることができ、1 つのみのレベルまたは複数の階層レベルを含む任意の複雑度で構築できます。[条件スタジオ（Conditions Studio）] を使用して新しい条件を作成する場合は、[ライブラリ（Library）] にすでに保存している条件ブロックを使用することができ、それらの保存された条件ブロックを更新および変更することもできます。後で条件を作成および管理する際に、クイック カテゴリ フィルタなどを使用して、必要なブロックと属性を簡単に見つけることができます。

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 *4 : [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。

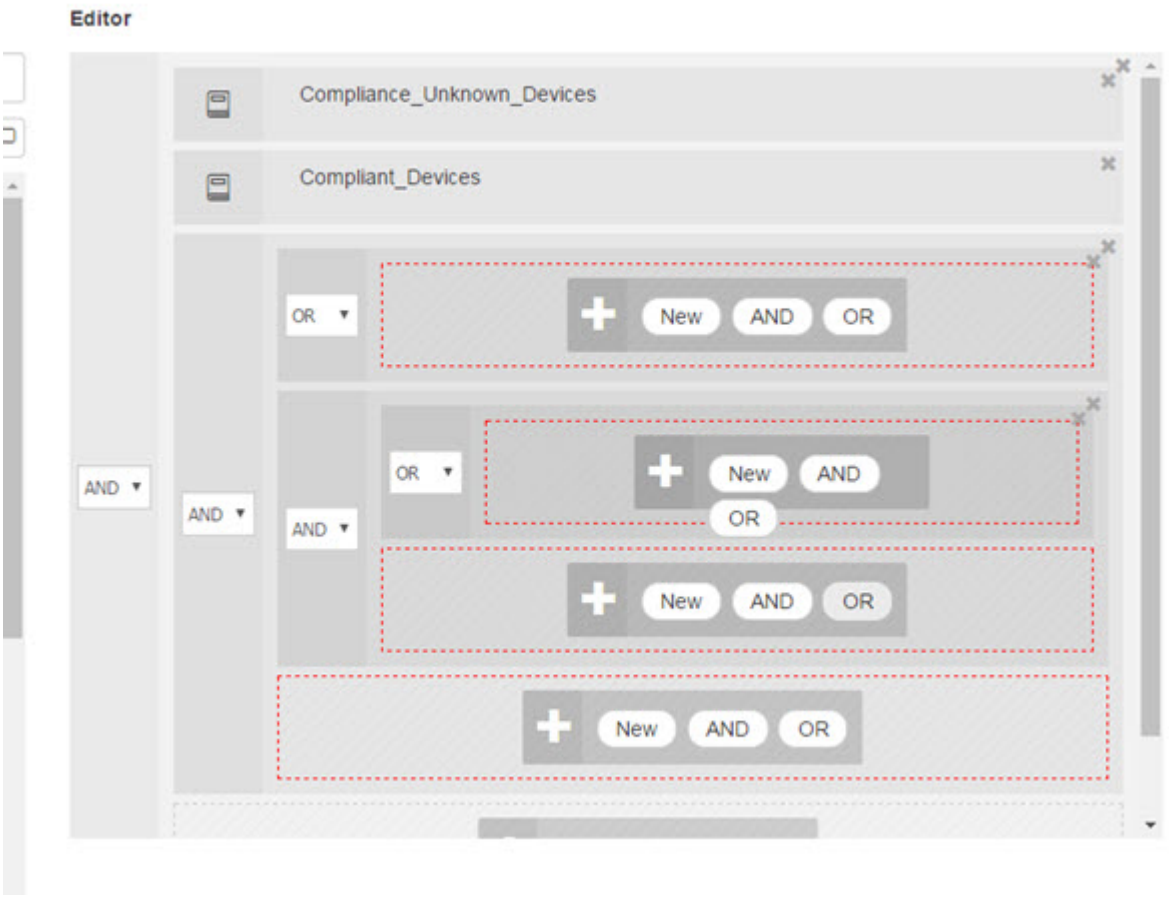
フィールド	使用上のガイドライン
	[エディタ（Editor）] は、さまざまな仮想列と行に分かれています。 列は異なる階層レベルを表し、各列は階層内の位置に基づいてインデントされます。行は個々のルールを表します。レベルごとに 1 つまたは複数のルールを作成し、複数のレベルを含めることができます。 上記のイメージの例は、構築または編集中の条件を示しており、ルールの階層を含んでいます。図の第 1 レベルと第 2 レベルの両方に番号 5 が付けられています。上位親レベルのルールは、演算子 OR を使用します。 演算子を選択して階層レベルを作成した後で演算子を変更するには、この列に表示されているドロ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 *5 : [*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。

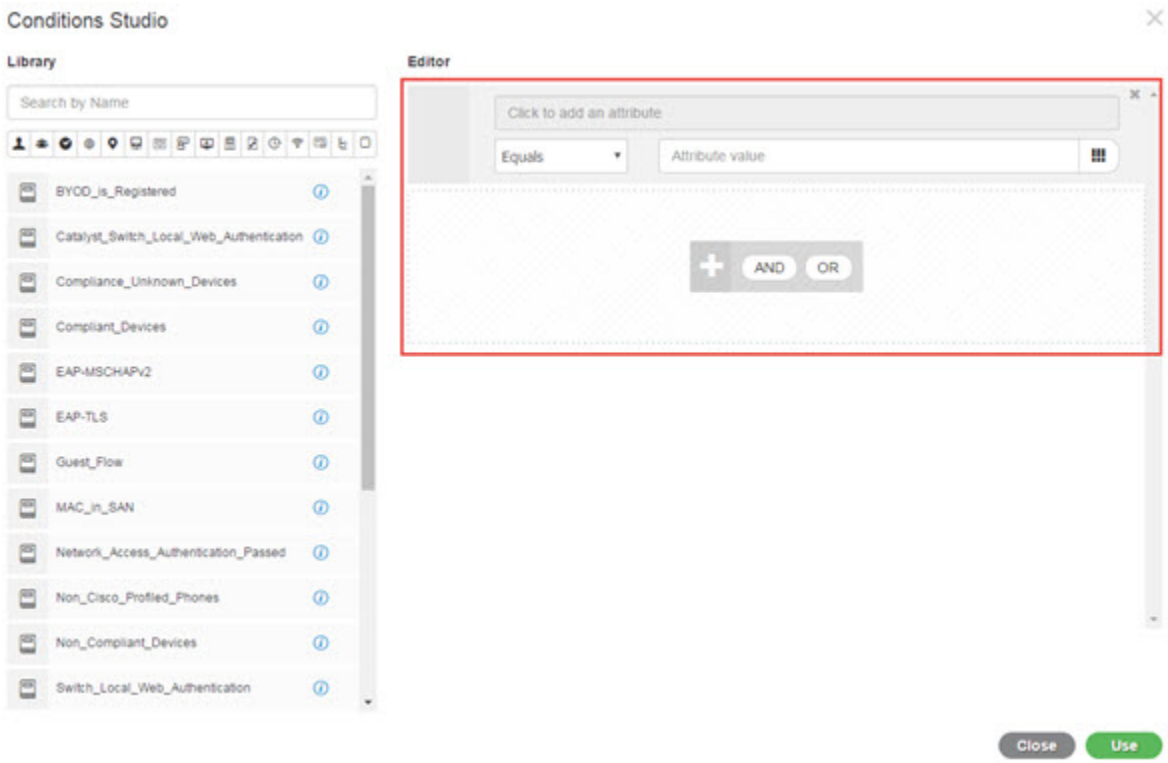
a) ポリシー セット全体（認証ポリシー ルールに照合する前にチェックされる条件）に関連する条件を作成するには、メインの [ポリシー セット（Policy Set）] ページで [ポリシー セット（Policy Set）] テーブルの [条件（Conditions）] 列から ✚ をクリックします。

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（Conditions Studio）] の操作 （44 ページ） を参照してください。

図 *6 : [*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。

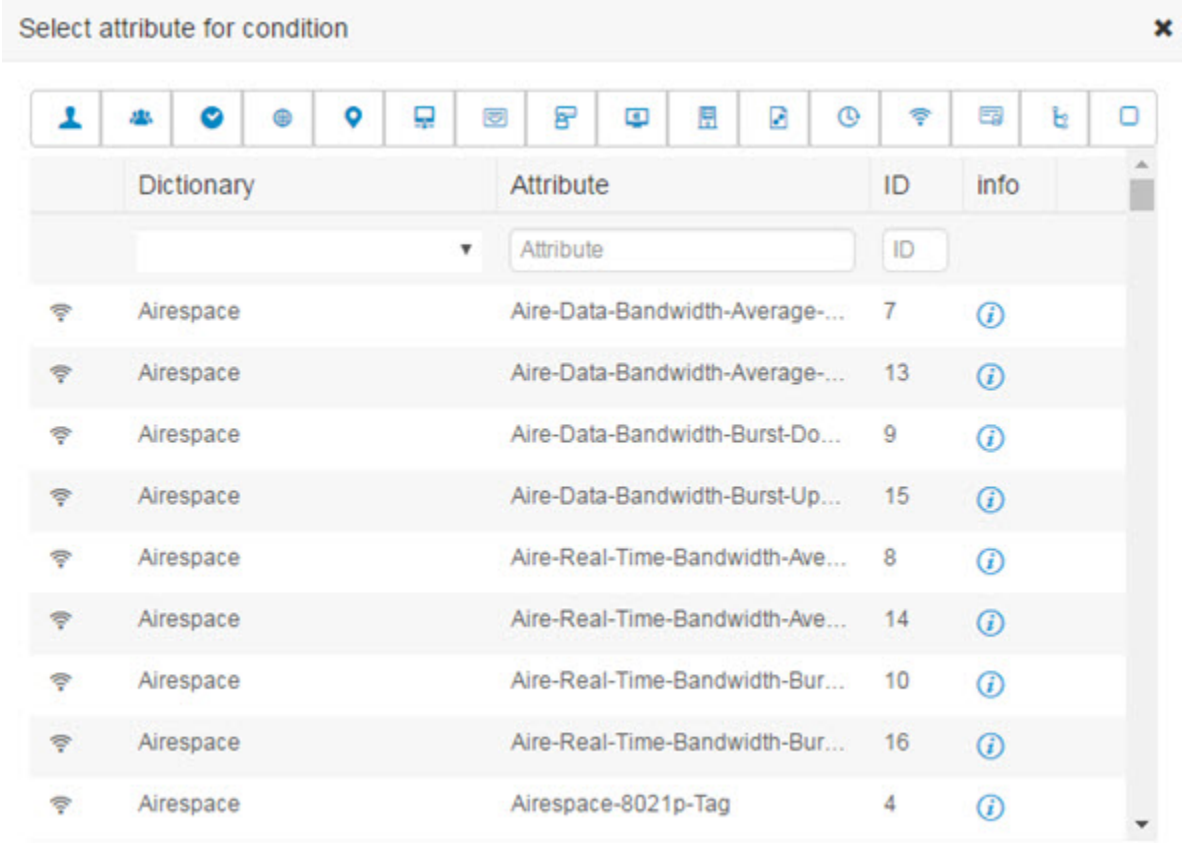
b) フリーテキストで条件ブロックを検索するには、検索しているブロックの名前に表示される [名前で検索（Search by Name）] フリー テキスト フィールドに、任意の用語または用語の一部を入力します。入力すると、システムは関連のリアルタイムの結果を動的に検索します。カテゴリが選択されていない場合（いずれのアイコンも強調表示されていない場合）、結果にはすべてのカテゴリの条件ブロックが含まれます。カテゴリ アイコンがすでに選択されている場合（表示されているリストがすでにフィルタされている場合）、表示される結果には、特定のテキストを使用する特定のカテゴリのブロックのみが含まれます。

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。

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 [送信（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 [送信（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 [送信（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 [送信（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、許可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サポートされています。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

シスコの属性と値のペア	IETF 属性
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、EPS 監査レポート、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 アドレスに基づいて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。

（注） 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 以前に生成されたマスター キーおよび 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。

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 AnyConnect 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 [保存（Save）] をクリックします。

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-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。

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。

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。

セキュリティ設定の構成

セキュリティ設定を構成するには、次の手順を実行します。

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）] ページで、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 サーバとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバから 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
- 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 サーバとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバから 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
- SHA1暗号化を許可（Allow SHA1 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 サーバとして設定されます

- Cisco ISE は、RADIUS DTLS サーバ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

（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 サーバとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバ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 サーバとして設定されます
  - Cisco ISE は、RADIUS DTLS サーバ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
- 目的の検証なしで証明書を受け入れる（Accept Certificates without Validating Purpose）：ISE が EAP または RADIUS DTLS サーバとして機能する場合、キー使用拡張に ECDHE-ECDSA 暗号化の keyAgreement ビットまたは他の暗号化の keyEncipherment ビットが含まれているかどうかを確認することなく、クライアント証明書が受け入れられます。
- 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

ステップ 3 無効なユーザ名を開示する（Disclose Invalid Usernames）：デフォルトでは、ユーザ名が無効な場合に ISE は認証失敗に無効と表示します。デバッグをサポートするために、このオプションが ISE に適用され、無効の代わりにレポートにユーザ名が開示（表示）されます。このオプションを選択するかどうかに関係なく、無効なユーザ名が原因ではない認証の失敗にユーザ名が常に表示されます。

[無効なユーザ名を開示する（Disclose Invalid Usernames）] を有効にする場合は、[無効なユーザ名を常に表示する（Always show invalid usernames）] または [無効なユーザ名を指定した期間表示する（Show invalid usernames for a specific tim）] を選択する必要があります。時間オプションを選択する場合は、時間を分単位で選択します（最大 1 か月（43,200 分））。

この機能は、Active Directory、内部ユーザ、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。このような ID ストアの場合、誤って入力されたユーザ名は常に「無効」として報告されます。

ステップ 4 [保存（Save）] をクリックします。

RADIUS プロキシ サーバとして機能する Cisco ISE

Cisco ISE は、RADIUS サーバおよび RADIUS プロキシ サーバとして機能できます。プロキシ サーバ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（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 サーバへのプロキシ サーバとして動作できます。RADIUS サーバ順序で設定した外部 RADIUS サーバを使用できます。次に説明する [外部 RADIUS サーバ（External RADIUS Server）] ページには、Cisco ISE で定義した外部 RADIUS サーバ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 サーバ順序を使用して要求を RADIUS サーバにプロキシできます。

RADIUS サーバ順序は、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 サーバは RADIUS-Username 属性からユーザ名を取得し、RADIUS サーバ順序の設定時に指定した文字列からユーザ名を抜き取ります。EAP 認証の場合は、RADIUS プロキシ サーバはユーザ名を EAP-Identity 属性から取得します。RADIUS サーバ順序を使用する 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 サーバの設定

Cisco ISE で外部 RADIUS サーバを設定して、要求を外部 RADIUS サーバ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サーバは、それだけでは使用できません。RADIUSサーバ順序を作成して、この項で作成したRADIUSサーバ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（External RADIUS Servers）]** を選択します。

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

ステップ 2 外部 RADIUS サーバを追加するには、[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 サーバの設定を保存します。

RADIUS サーバ順序の定義

Cisco ISE の RADIUS サーバ順序を使用すると、NAD からの要求を外部 RADIUS サーバにプロキシできます。外部 RADIUS サーバ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 サーバ順序（RADIUS Server Sequences）] ページに、Cisco ISE で定義したすべての RADIUS サーバの順序が表示されます。このページを使用して、RADIUS サーバの作成、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（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（TACACS+ External Servers）] ページには、Cisco ISE で定義した外部 TACACS+ サーバ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。複数の外部サーバを設定するには、[TACACS+サーバの順序（TACACS+ server sequence）] ページを使用できます。詳細については、「TACACS+ サーバ順序の設定」ページを参照してください。

TACACS+ 外部サーバの設定

次の表では、[TACACS外部サーバ（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、**[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（TACACS External Servers）]** ページです。

表 *5 : TACACS+* 外部サーバの設定

フィールド	使用上のガイドライン
[名前（Name）]	TACACS+ 外部サーバの名前を入力します。
説明	TACACS+ 外部サーバ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+ 外部サーバの IP アドレス（IPv4 または IPv6 アドレス）を入力します。

フィールド	使用上のガイドライン
接続ポート（Connection Port）	リモート TACACS+ 外部サーバ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+ 外部サーバによって拒否されます。
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。

外部 TACACS+ サーバの設定

Cisco ISE で外部 TACACS サーバを設定して、要求を外部 TACACS サーバ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 サーバは、ポリシーに直接使用できません。TACACS サーバ順序を作成して、この項で作成した TACACS サーバ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（TACACS External Servers）]** の順に選択します。
[TACACS外部サーバ（TACACS External Servers）] ページが表示され、Cisco ISE で定義された外部 TACACS サーバのリストが示されます。

ステップ 2 外部 TACACS サーバを追加するには、[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 サーバの設定を保存します。

TACACS+ サーバ順序の設定

次の表では、[TACACSサーバ順序（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、**[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サーバ順序（TACACS Server Sequence）]** ページです。

表 *6 : TACACS+* サーバ順序の設定

フィールド	使用上のガイドライン
[名前（Name）]	TACACS プロキシ サーバ順序の名前を入力します。
説明	TACACS プロキシ サーバ順序の説明を入力します。
サーバ 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
ユーザ名の除去（Username Stripping）	ユーザ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、ユーザ名は smith になります。デフォルトの区切り文字は @ です。

TACACS+ サーバ順序の定義

Cisco ISE の TACACS+ サーバ順序を使用すると、NAD からの要求を外部 TACACS+ サーバにプロキシできます。外部 TACACS+ サーバ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+サーバ順序（TACACS+ Server Sequences）] ページに、Cisco ISE で定義したすべての TACACS+ サーバの順序が表示されます。このページを使用して、TACACS+ サーバ順序の作成、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+ サーバ順序で使用する外部 TACACS+ サーバ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外部サーバ順序（TACACS External Server Sequence）]** 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 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+ サーバ順序を保存します。

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。

Cisco ISE が FIPS モードで動作するように設定されている場合は、一部のプロトコルがデフォルトで無効になり、それらのプロトコルを設定できません。

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。

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）] の順に選択します。

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）] 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) 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）] の順に選択します。

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。