アセットの可視性

外部 ID ストアを使用した Cisco ISE への管理アクセス

Cisco ISE では、Active Directory、LDAP、RSA SecureID などの外部 ID ストアを介して管理者を認証できます。外部 ID ストアを介した認証の提供に使用できる次の 2 つのモデルがあります。

- 外部認証および許可：管理者に関してローカル Cisco ISE データベースで指定されたクレデンシャルはなく、許可は、外部 ID ストア グループ メンバーシップのみに基づきます。このモデルは、Active Directory および LDAP 認証で使用されます。
- 外部認証および内部許可：管理者の認証クレデンシャルは外部 ID ソースから取得され、許可および管理者ロール割り当てはローカル Cisco ISE データベースを使用して行われます。このモデルは、RSA SecurID 認証で使用されます。この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザー名を設定する必要があります。

認証プロセス時、Cisco ISE は、外部 ID ストアとの通信が確立されなかった場合や失敗した場合はフォールバックし、内部 ID データベースから認証の実行を試行するように設計されています。さらに、外部認証が設定されている管理者には、ブラウザを起動してログインセッションを開始するたびに、ログインダイアログボックスの [ID ストア（Identity Store）] ドロップダウンリストから [内部（Internal）] を選択すると Cisco ISE のローカルデータベースを介した認証を要求するオプションが依然として表示されます。

ネットワーク管理者グループに所属する管理者と、外部 ID ストアを使用して認証および認可するように設定されている管理者は、CLI（コマンドライン インターフェイス）アクセス用に外部 ID ストアを使用して認証することもできます。

（注） 外部管理者認証を提供するこの方法は、管理者ポータルを介してのみ設定できます。Cisco ISE CLI では、これらの機能は設定されません。

ネットワークに既存の外部 ID ストアがまだない場合は、必要な外部 ID ストアをインストールし、これらの ID ストアにアクセスするように Cisco ISE が設定されていることを確認します。

外部認証および許可

デフォルトでは、Cisco ISE によって内部管理者認証が提供されます。外部認証を設定するには、外部 ID ストアで定義している外部管理者アカウントのパスワード ポリシーを作成する必要があります。次に、結果的に外部管理者 RBAC ポリシーの一部となるこのポリシーを外部管理者グループに適用できます。

外部認証を設定するには、次の手順を実行する必要があります。

- 外部 ID ストアを使用してパスワード ベースの認証を設定します。
- 外部管理者グループを作成します。
- 外部管理者グループ用のメニュー アクセスとデータ アクセスの権限を設定します。
- 外部管理者認証の RBAC ポリシーを作成します。

ネットワークでは、外部 ID ストア経由の認証を提供するほかに、共通アクセス カード（CAC）認証デバイスを使用する必要もある場合があります。

外部 ID ストアを使用したパスワード ベースの認証の設定

最初に、Active Directory や LDAP などの外部 ID ストアを使用して認証を行う管理者のためのパスワード ベースの認証を設定する必要があります。

ステップ 1

ステップ 2 **[認証方式（Authentication Method）]** タブで、**[パスワードベース（Password Based）]** をクリックし、すでに設定されている外部 ID ソースの 1 つを選択します。たとえば、作成した Active Directory インスタンスを選択します。

ステップ 3 外部 ID ストアを使用して認証を行う管理者のためのその他の特定のパスワード ポリシーを設定します。

ステップ 4 [保存（Save）] をクリックします。

外部管理者グループの作成

外部 Active Directory または LDAP 管理者グループを作成する必要があります。これにより、Cisco ISE は外部 Active Directory または LDAP ID ストアで定義されているユーザー名を使用して、ログイン時に入力した管理者ユーザー名とパスワードを検証します。

Cisco ISE は、外部リソースから Active Directory または LDAP グループ情報をインポートし、それをディクショナリ属性として保存します。次に、この属性を、外部管理者認証方式用の RBAC ポリシーを設定するときのポリシー要素の 1 つとして指定できます。

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

[マッピングされた外部グループ（External Groups Mapped）] 列には、内部 RBAC ロールにマップされている外部グループの数が表示されます。管理者ロールに対応する番号をクリックすると、外部グループを表示できます（たとえば、[ネットワーク管理者（Super Admin）] に対して表示されている 2 をクリックすると、2 つの外部グループの名前が表示されます）。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 名前とオプションの説明を入力します。

ステップ 4 [外部（External）] をクリックします。

Active Directory ドメインに接続し、参加している場合は、Active Directory インスタンス名が [名前（Name）] フィールドに表示されます。

ステップ 5 [外部グループ（External Groups）] ドロップダウン リスト ボックスから、この外部管理者グループにマッピングする Active Directory グループを選択します。

追加の Active Directory グループをこの外部管理者グループにマッピングするために「+」記号をクリックします。

ステップ 6 [保存（Save）] をクリックします。

内部読み取り専用管理者の作成

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

ステップ 2 [追加（Add）] をクリックして、[管理ユーザーの作成（Create An Admin User）] を選択します。

ステップ 3 [読み取り専用（Read Only）] チェックボックスをオンにして読み取り専用管理者を作成します。

外部グループを読み取り専用管理者グループにマッピング

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択して、外部認証ソースを設定します。

ステップ 2 必要な外部 ID ソース（Active Directory や LDAP など）をクリックし、選択した ID ソースからグループを取得します。

ステップ 3 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）] を選択して、管理者アクセスの認証方式を ID ソースとマッピングします。

ステップ 4 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）] を選択し、[読み取り専用管理者（Read Only Admin）] グループを選択します。

ステップ 5 **[外部（External）]** チェックボックスをオンにして、読み取り専用権限を提供する必要のある外部グループを選択します。

ステップ 6 [保存（Save）] をクリックします。

読み取り専用管理者グループにマップされている外部グループは、他の管理者グループに割り当てることはできません。

外部管理者グループのメニューアクセス権限とデータアクセス権限の設定

外部管理者グループに割り当てることができるメニュー アクセス権限とデータ アクセス権限を設定する必要があります。

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

ステップ 2 次のいずれかをクリックします。

- **[メニューアクセス（Menu Access）]**：外部管理者グループに属するすべての管理者に、メニューまたはサブメニューレベルでの権限を付与することができます。メニュー アクセス権限によって、アクセスできるサブメニューまたはメニューが決定されます。

- **[データアクセス（Data Access）]**：外部管理者グループに属するすべての管理者に、データレベルでの権限を付与することができます。データ アクセス権限によって、アクセスできるデータが決定されます。

ステップ 3 外部管理者グループのメニュー アクセス権限とデータ アクセス権限を指定します。

ステップ 4 [保存（Save）] をクリックします。

外部管理者認証の RBAC ポリシーの作成

外部 ID ストアを使用して管理者を認証し、カスタムメニューアクセス権限とデータアクセス権限を指定するには、新しいRBACポリシーを設定する必要があります。このポリシーには、認証用の外部管理者グループ、および外部認証と許可を管理するための Cisco ISE メニュー アクセス権限とデータ アクセス権限が存在している必要があります。

（注） これらの新しい外部属性を指定するように既存（システムプリセット）のRBACポリシーを変更することはできません。テンプレートとして使用する既存のポリシーがある場合は、そのポリシーを複製し、名前を変更してから、新しい属性を割り当てる必要があります。

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

ステップ 2 ルール名、外部管理者グループ、および権限を指定します。

適切な外部管理者グループが正しい管理者ユーザーIDに割り当てられている必要があることに注意してください。管理者が正しい外部管理者グループに関連付けられていることを確認します。

ステップ 3 [保存（Save）] をクリックします。

管理者としてログインした場合、Cisco ISE RBAC ポリシーが管理者 ID を認証できないと、Cisco ISE では、「認証されていない」ことを示すメッセージが表示され、管理者ポータルにアクセスできません。

内部許可を伴う認証に対する外部IDストアを使用した管理アクセスの設定

この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザー名を設定する必要があります。外部 RSA SecurID ID ストアを使用して管理者認証を提供するように Cisco ISE を設定している場合、管理者のクレデンシャル認証が RSA ID ストアによって実行されます。ただし、許可（ポリシー アプリケーション）は、依然として Cisco ISE 内部データベースに従って行われます。また、外部認証と許可とは異なる、留意する必要がある次の2つの重要な要素があります。

- 管理者の特定の外部管理者グループを指定する必要はありません。
- 外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザー名を設定する必要があります。

ステップ 1

ステップ 2 外部 RSA ID ストアの管理者ユーザー名が Cisco ISE にも存在することを確認します。[パスワード（Password）] の下の [外部（External）] オプションをクリックします。

（注） 外部管理者ユーザー ID のパスワードを指定する必要はなく、特別に設定されている外部管理者グループを関連付けられている RBAC ポリシーに適用する必要もありません。

ステップ 3 [保存（Save）] をクリックします。

外部認証のプロセス フロー

管理者がログインすると、ログインセッションはそのプロセスにおいて次の手順で処理されます。

1. 管理者が RSA SecurID チャレンジを送信します。
2. RSA SecurID は、チャレンジ応答を返します。
3. 管理者は、ユーザー ID とパスワードを入力する場合と同様に、ユーザー名および RSA SecurID チャレンジ応答を Cisco ISE ログイン ダイアログに入力します。
4. 管理者は、指定した ID ストアが外部 RSA SecurID リソースであることを確認します。
5. 管理者は、[ログイン（Login）] をクリックします。

ログイン時、管理者には、RBAC ポリシーで指定されたメニュー アクセス項目とデータ アクセス項目のみが表示されます。

外部 ID ソース

これらのウィンドウでは、Cisco ISE が認証および認可に使用するユーザーデータが含まれている外部 ID ソースを設定および管理することができます。

LDAP ID ソースの設定

LDAP 一般設定

以下の表では、[一般（General）] タブのフィールドについて説明します。

表 *1: LDAP* 一般設定

フィールド名	使用上のガイドライン
名前（**Name**）	LDAP インスタンスの名前を入力します。この値は、サブジェクト DN および属性を取得するために検索で使用されます。この値は string 型で、最大長は 64 文字です。
説明（**Description**）	LDAP インスタンスの説明を入力します。この値は string 型で、最大長は 1024 文字です。
スキーマ（**Schema**）	次の組み込みのスキーマ タイプのいずれかを選択するか、カスタム スキーマを作成できます。 • Active Directory • Sun Directory Server • Novell eDirectory [スキーマ（Schema）] の隣の矢印をクリックすると、スキーマの詳細を表示できます。 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。
（注）　次のフィールドは、カスタム スキーマを選択した場合にのみ編集できます。	
サブジェクト オブジェクト クラス（**Subject Objectclass**）	サブジェクト DN および属性を取得するために検索で使用する値を入力します。この値は string 型で、最大長は 256 文字です。
サブジェクト名属性（**Subject Name Attribute**）	要求内のユーザー名を含む属性の名前を入力します。この値は string 型で、最大長は 256 文字です。 （注）　構成されているサブジェクト名属性は、外部 ID ストア内のインデックス付きのものである必要があります。
グループ名属性（**Group Name Attribute**）	• CN：共通名に基づいて LDAP ID ストア グループを取得します。 • DN：識別名に基づいて LDAP ID ストア グループを取得します。

フィールド名	使用上のガイドライン
証明書属性（**Certificate Attribute**）	証明書定義を含む属性を入力します。証明書ベースの認証の場合、クライアントによって提示された証明書を検証するために、これらの定義が使用されます。
グループ オブジェクト クラス（**Group Objectclass**）	グループとして認識されるオブジェクトを指定するために、検索に使用する値を入力します。この値は string 型で、最大長は 256 文字です。
グループ マップ属性（**Group Map Attribute**）	マッピング情報を含む属性を指定します。この属性は、選択した参照方向に基づいて、ユーザーまたはグループ属性を指定できます。
サブジェクト オブジェクトにグループへの参照が含まれる（**Subject Objects Contain Reference To Groups**）	所属するグループを指定する属性がサブジェクトオブジェクトに含まれている場合は、このオプションをクリックします。
グループ オブジェクトにサブジェクトへの参照が含まれる（**Group Objects Contain Reference To Subjects**）	サブジェクトを指定する属性がグループオブジェクトに含まれている場合は、このオプションをクリックします。この値はデフォルト値です。
グループ内のサブジェクトをメンバー属性に保存（**Subjects In Groups Are Stored In Member Attribute As**）	（[グループオブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）] オプションを有効にした場合に限り使用可能）グループメンバー属性にメンバーが供給される方法を指定します（デフォルトは DN）。

フィールド名	使用上のガイドライン
ユーザー情報属性（**User Info Attributes**）	デフォルトでは、事前設定された属性が次の組み込みのスキーマ タイプのユーザー情報（名、姓、電子メール、電話、地域など）を収集するために使用されます。 • Active Directory • Sun Directory Server • Novell eDirectory 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。 [スキーマ（Schema）] ドロップダウン リストから [カスタム（Custom）] オプションを選択し、要件に基づいてユーザー情報の属性を編集することもできます。

（注） 構成されているサブジェクト名属性は、外部 ID ストア内のインデックス付きのものである必要があります。

LDAP の接続設定

以下の表では、[接続設定（Connection Settings）] タブのフィールドについて説明します。

表 *2 : LDAP* の接続設定

フィールド名	使用上のガイドライン
セカンダリ サーバーの有効化（**Enable Secondary Server**）	プライマリ LDAP サーバーに障害が発生した場合にバックアップとして使用するセカンダリ LDAP サーバーを有効にする場合は、このオプションをオンにします。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバーの設定パラメータを入力する必要があります。
プライマリ サーバーとセカンダリ サーバー（**Primary and Secondary Servers**）	

フィールド名	使用上のガイドライン
ホスト名/IP（**Hostname/IP**）	LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。
ポート（**Port**）	LDAP サーバーがリッスンしている TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバーの管理者からポート番号を取得できます。
各 ISE ノードのサーバーの指定（**Specify server for each ISE node**）	プライマリおよびセカンダリ LDAP サーバーの hostnames/IP および各 PSN のポートを設定するには、このチェック ボックスをオンにします。 このオプションを有効にすると、導入のすべてのノードを表示するテーブルが表示されます。ノードを選択し、プライマリおよびセカンダリ LDAP サーバーの hostname/IP および選択したノードのポートを設定する必要があります。
アクセス（**Access**）	[匿名アクセス（Anonymous Access）]：LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバーではクライアントが区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへの、クライアント読み取りアクセスが許可されます。認証情報をサーバーに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。 [認証されたアクセス（Authenticated Access）]：LDAP ディレクトリの検索が管理者のログイン情報によって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。

フィールド名	使用上のガイドライン
管理者 DN（Admin DN）	管理者の DN を入力します。管理者 DN は、[ユーザー ディレクトリ サブツリー（User Directory Subtree）] 下のすべての必要なユーザーの検索およびグループの検索を行う権限を持つ LDAP アカウントです。指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、該当LDAPサーバーで認証されたユーザーのグループ マッピングは失敗します。
パスワード（Password）	LDAP 管理者アカウントのパスワードを入力します。
セキュアな認証（Secure Authentication）	SSL を使用して Cisco ISE とプライマリ LDAP サーバー間の通信を暗号化する場合にクリックします。[ポート（Port）] フィールドに LDAP サーバーでの SSL に使用されるポート番号が入力されていることを確認します。このオプションを有効にした場合は、ルートCAを選択する必要があります。
LDAP サーバーのルート CA（LDAP Server Root CA）	ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証を有効にします。
サーバー タイムアウト（Server timeout）	プライマリ LDAP サーバーでの接続または認証が失敗したと判断する前に Cisco ISE がプライマリ LDAP サーバーからの応答を待つ秒数を入力します。有効な値は 1 ～ 99 です。デフォルトは 10 です。
最大管理接続（Max. Admin Connections）	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、ユーザーディレクトリ サブツリーおよびグループ ディレクトリ サブツリーの下にあるユーザーおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です。デフォルトは 20 です。
N 秒ごとに再接続（Force reconnect every N seconds）	このチェックボックスをオンにし、[秒（Seconds）] フィールドに、サーバーを指定された間隔で LDAP 接続を更新するための適切な値を入力します。有効な範囲は 1 ～ 60 分です。

フィールド名	使用上のガイドライン
サーバーへのバインドをテスト（**Test Bind To Server**）	LDAP サーバーの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバーの詳細を編集して再テストします。
フェールオーバー（**Failover**）	
常にプライマリ サーバーに最初にアクセスする（**Always Access Primary Server First**）	Cisco ISE の認証と認可のために常にプライマリ LDAP サーバーに最初にアクセスするように設定するには、このオプションをクリックします。
経過後にプライマリ サーバーにフェールバック（**Failback to Primary Server After**）	Cisco ISE で接続しようとしたプライマリ LDAP サーバーが到達不可能な場合、Cisco ISE はセカンダリ LDAP サーバーへの接続を試行します。Cisco ISE に再びプライマリ LDAP サーバーを使用するように設定するには、このオプションをクリックし、テキスト ボックスに値を入力します。

[LDAP] の [ディレクトリ構成（Directory Organization）] タブ

次の表では、[ディレクトリ構成（Directory Organization）] タブのフィールドについて説明します。

表 *3 : [LDAP]* の *[*ディレクトリ構成（*Directory Organization*）*]* タブ

フィールド名	使用上のガイドライン
サブジェクト検索ベース（**Subject Search Base**）	すべてのサブジェクトを含むサブツリーの DN を入力します。次に例を示します。 o=corporation.com サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

フィールド名	使用上のガイドライン
グループ検索ベース（**Group Search Base**）	すべてのグループを含むサブツリーの DN を入力します。次に例を示します。 ou = 組織ユニット、ou = 次の組織ユニット、o = corporation.com グループを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。
形式での MAC アドレスの検索（**Search for MAC Address in Format**）	LDAPデータベースでの検索に使用する、Cisco ISE の MAC アドレス形式を入力します。内部 ID ソースの MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で供給されます。LDAPデータベースのMACアドレスは、異なる形式で供給できます。ただし、Cisco ISE でホスト ルックアップ要求が受信されると、MACアドレスは内部形式からこのフィールドで指定した形式に変換されます。 ドロップダウン リストを使用して、特定の形式でのMACアドレスの検索を有効にします。<*format*> は次のいずれかです。 • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 選択する形式は、LDAP サーバーに供給されているMACアドレスの形式と一致している必要があります。

フィールド名	使用上のガイドライン
サブジェクト名の先頭から最後に出現する区切り文字まで削除（**Strip start of subject name up to the last occurrence of the separator**）	ユーザー名からドメインプレフィックスを削除するための適切なテキストを入力します。 ユーザー名の中でこのフィールドに指定した区切り文字が Cisco ISE で検出されると、そのユーザー名の初めから区切り文字までのすべての文字が削除されます。ユーザー名に、<start_string> ボックスに指定した文字が複数含まれている場合は、Cisco ISE によって最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザー名が DOMAIN\user1 である場合、Cisco ISE によって user1 が LDAP サーバーに送信されます。 （注） <start_string> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザー名にこれらの文字を使用できません。
最初に出現する区切り文字からサブジェクト名の末尾まで削除（**Strip end of subject name from the first occurrence of the separator**）	ユーザー名からドメイン サフィックスを削除するための適切なテキストを入力します。 ユーザー名の中でこのフィールドに指定した区切り文字が Cisco ISE で検出されると、その区切り文字からユーザー名の末尾までのすべての文字が削除されます。ユーザー名に、このフィールドに指定した文字が複数含まれている場合は、Cisco ISE によって最初の区切り文字から文字が削除されます。たとえば、区切り文字が@で、ユーザー名が *user1@domain* であれば、Cisco ISE は *user1* を LDAP サーバーに送信します。 （注） *<end_string>* ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザー名にこれらの文字を使用できません。

LDAP グループ設定

表 *4: LDAP* グループ設定

フィールド名	使用上のガイドライン
追加（**Add**）	[追加（Add）]>[グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）] を選択して LDAP ディレクトリからグループを選択します。 グループの追加を選択した場合は、新しいグループの名前を入力します。ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。選択したグループが [グループ（Groups）] ウィンドウに表示されます。

LDAP 属性設定

表 *5: LDAP* 属性設定

フィールド名	使用上のガイドライン
追加（**Add** ）	[追加（Add）]>[属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）] を選択して LDAP サーバーから属性を選択します。 属性を追加する場合は、新しい属性の名前を入力します。ディレクトリから選択する場合は、ユーザー名を入力し、[属性の取得（Retrieve Attributes）] をクリックして属性を取得します。選択する属性の隣にあるチェック ボックスをオンにし、[OK] をクリックします。

LDAP 詳細設定

以下の表では、[詳細設定（Advanced Settings）] タブのフィールドについて説明します。

表 *6: LDAP* 詳細設定

フィールド名	使用上のガイドライン
[パスワードの変更を有効にする（Enable password change）]	デバイス管理に PAP プロトコルを使用し、ネットワーク アクセスに RADIUS EAP-GTC プロトコルを使用している場合に、パスワードが期限切れになるか、またはパスワードがリセットされるときに、ユーザーがパスワードを変更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。サポートされていないプロトコルでは、ユーザー認証が失敗します。このオプションでは、ユーザーが次回のログイン時にパスワードを変更できるようにすることもできます。

関連トピック

LDAP ディレクトリ サービス （145 ページ）
LDAP ユーザー認証 （146 ページ）
LDAP ユーザー ルックアップ （150 ページ）
LDAP ID ソースの追加 （151 ページ）

RADIUS トークン ID ソースの設定

関連トピック

RADIUS トークン ID ソース （170 ページ）
RADIUS トークン サーバーの追加 （174 ページ）

RSA SecurID ID ソースの設定

RSA プロンプトの設定

次の表では、[RSA プロンプト（RSA Prompts）] タブ内のフィールドについて説明します。

表 *7 : RSA* プロンプトの設定

フィールド名	使用上のガイドライン
パスコード プロンプトの入力（Enter Passcode Prompt）	パス コードを取得するテキスト文字列を入力します。
次のトークン コードの入力（Enter Next Token Code）	次のトークンを要求するテキスト文字列を入力します。
PIN タイプの選択（Choose PIN Type）	PIN タイプを要求するテキスト文字列を入力します。
システム PIN の受け入れ（Accept System PIN）	システム生成の PIN を受け付けるテキスト文字列を入力します。
英数字 PIN の入力（Enter Alphanumeric PIN）	英数字 PIN を要求するテキスト文字列を入力します。
数値 PIN の入力（Enter Numeric PIN）	数値 PIN を要求するテキスト文字列を入力します。
PIN の再入力（Re-enter PIN）	ユーザーに PIN の再入力を要求するテキスト文字列を入力します。

RSA メッセージ設定（RSA Message Settings）

次の表では、[RSA メッセージ（RSA Messages）] タブ内のフィールドについて説明します。

表 *8 : RSA* メッセージ設定（*RSA Messages Settings*）

フィールド名	使用上のガイドライン
システム PIN メッセージの表示（Display System PIN Message）	システム PIN メッセージのラベルにするテキスト文字列を入力します。
システム PIN 通知の表示（Display System PIN Reminder）	ユーザーに新しい PIN を覚えるように通知するテキスト文字列を入力します。
数字を入力する必要があるエラー（Must Enter Numeric Error）	PIN には数字のみを入力するようにユーザーに指示するメッセージを入力します。
英数字を入力する必要があるエラー（Must Enter Alpha Error）	PINには英数字のみを入力するようにユーザーに指示するメッセージを入力します。
PIN 受け入れメッセージ（PIN Accepted Message）	ユーザーの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
PIN 拒否メッセージ（PIN Rejected Message）	ユーザーの PIN がシステムによって拒否されたときに表示されるメッセージを入力します。
ユーザーの PIN が異なるエラー（User Pins Differ Error）	ユーザーが不正な PIN を入力したときに表示されるメッセージを入力します。
システム PIN 受け入れメッセージ（System PIN Accepted Message）	ユーザーの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
不正パスワード長エラー（Bad Password Length Error）	ユーザーが指定した PIN が、PIN 長ポリシーで指定されている範囲に収まらない場合に表示されるメッセージを入力します。

関連トピック

RSA ID ソース （176 ページ）
Cisco ISE と RSA SecurID サーバーの統合 （177 ページ）
RSA ID ソースの追加 （180 ページ）

Cisco ISE ユーザー

この章では、ユーザーという用語はネットワークに定期的にアクセスする従業員と請負業者に加え、スポンサーおよびゲストユーザーを意味します。スポンサーは、スポンサーポータルでゲストユーザーアカウントを作成および管理する組織の従業員または請負業者です。ゲストユーザーは、一定期間組織のネットワークリソースへのアクセスを必要とする外部ビジターです。

Cisco ISE ネットワーク上のリソースとサービスにアクセスするすべてのユーザーのアカウントを作成する必要があります。従業員、請負業者、およびスポンサーユーザーは、管理者ポータルから作成されます。

Cisco ISE リリース 3.2 から、[有効化日（Date Enabled）] 列（**[設定（Settings）] > [列（Columns）] > [有効化日（Date Enabled）]**）と [パスワードが期限切れになるまでの日数（Days Until Password Expires）] 列（**[接続（Settings）] > [列（Columns）] > [パスワードが期限切れになるまでの日数（Days Until Password Expires）]**）を [ネットワーク アクセス ユーザー（Network Access User）] ウィンドウ（**[管理（Administration）] > [ID管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]**）の [ネットワーク アクセス ユーザー（Network Access User）] テーブルに追加することを選択できます。この操作は、ネットワーク アクセス ユーザーをパスワードの期限切れに関する情報でソートするのに役立ちます。これらのフィールドは、デフォルトでは追加されません。ウィンドウのカスタマイズオプションを使用して、それらをテーブルに追加できます。

ユーザー ID

ユーザーIDは、ユーザーに関する情報を保持するコンテナに似ており、ユーザーのネットワーク アクセス クレデンシャルを形成します。各ユーザーの ID はデータにより定義され、ユーザー名、電子メールアドレス、パスワード、アカウントの説明、関連付けられている管理者グループ、ユーザー グループ、ロールなどが含まれます。

ユーザー グループ

ユーザー グループは、特定の一連の Cisco ISE サービスおよび機能へのアクセスを許可する共通の権限セットを共有する個々のユーザーの集合です。

ユーザー ID グループ

ユーザーのグループ ID は、同じグループに属している特定のユーザー グループを識別および説明する要素で構成されています。グループ名は、このグループのメンバーが持っている機能ロールの説明です。グループは、そのグループに属しているユーザーのリストです。

デフォルト ユーザー ID グループ

Cisco ISE には、次の事前定義されたユーザー ID グループが用意されています。

- All_Accounts
- 従業員
- Group_Accounts
- GuestType_Contractor
- GuestType_Daily
- GuestType_SocialLogin

- GuestType_Weekly
- Own_Accounts

ユーザー ロール

ユーザー ロールは、ユーザーが Cisco ISE ネットワークで実行できるタスクやアクセスできるサービスを決定する権限セットです。ユーザー ロールは、ユーザー グループに関連付けられています（ネットワーク アクセス ユーザーなど）。

ユーザー アカウントのカスタム属性

Cisco ISE では、ネットワーク アクセス ユーザーと管理者の両方に対して、ユーザー属性に基づいてネットワーク アクセスを制限することができます。Cisco ISE では、一連の事前定義されたユーザー属性が用意されており、カスタム属性を作成することもできます。両方のタイプの属性が認証ポリシーを定義する条件で使用できます。パスワードが指定された基準を満たすように、ユーザー アカウントのパスワード ポリシーも定義できます。

カスタム ユーザー属性

[ユーザーのカスタム属性（User Custom Attributes）] ウィンドウ（[管理（Administration）] > [ID 管理（Identity Management）] > [設定（Settings）] > [ユーザーのカスタム属性（User Custom Attributes）]）で、追加のユーザー アカウント属性を設定できます。このウィンドウに事前に定義済みのユーザー属性のリストを表示することもできます。事前定義済みユーザー属性を編集することはできません。

新しいカスタム属性を追加するには、[ユーザーのカスタム属性（User Custom Attributes）] ペインに必要な詳細を入力します。[ユーザーのカスタム属性（User Custom Attributes）] ウィンドウに追加するカスタム属性とデフォルト値が、ネットワークアクセスユーザー（[管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [追加（Add）] / [編集（Edit）]）または管理者ユーザー（[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）] > [追加（Add）]/[編集（Edit）]）の追加または編集時に表示されます。これらのデフォルト値は、ネットワーク アクセスまたは管理者ユーザーの追加または編集時に変更できます。

ユーザーが [ユーザーのカスタム属性（User Custom Attributes）] ウィンドウで、カスタム属性に対し次のデータ型を選択できます。

- [文字列（String）]：文字列の最大長（文字列属性値の最大許容長）を指定できます。
- [整数（Integer）]：最小値と最大値を設定できます（最小、最大の許容可能な整数値を指定します）。
- [Enum]：各パラメータに次の値を指定できます。
  - 内部値
  - 表示値

デフォルト パラメータを指定することもできます。ネットワーク アクセスまたは管理者ユーザーの追加または編集時に、[表示（Display）] フィールドに追加する値が表示されます。

- [浮動小数点数（Float）]
- [パスワード（Password）]：最大文字列の長さを指定できます。
- [Long 型（Long）]：最小値と最大値を設定できます。
- [IP]：デフォルトの IPv4 アドレスまたは IPv6 アドレスを指定できます。
- [ブール値（Boolean）]：デフォルト値として True または False を設定できます。
- [日付（Date）]：カレンダーから日付を選択し、デフォルト値として設定できます。日付は yyyy-mm-dd 形式で表示されます。

ネットワーク アクセスまたは管理者ユーザーの追加または編集時、これを必須属性とする場合は、[必須（Mandatory）] チェックボックスをオンにします。カスタム属性のデフォルト値を設定することもできます。

カスタム属性は、認証ポリシーで使用できます。カスタム属性に設定するデータ型と許容範囲は、ポリシー条件のカスタム属性の値に適用されます。

ユーザー認証の設定

すべての外部 ID ストアで、ネットワーク アクセス ユーザーが自分のパスワードを変更できるわけではありません。詳細については、各 ID ソースのセクションを参照してください。

ネットワーク使用パスワードルールは、**[管理（Administration）] > [IDの管理（Identity Management）] > [設定（Settings）] > [ユーザー認証設定（User Authentication Settings）]** で設定されます。

[パスワードポリシー（Password Policy）] タブの一部のフィールドに関する追加情報を次のセクションに示します。

- [必須の文字（Required Characters）]：大文字または小文字が必要なユーザーパスワードポリシーを設定するときに、ユーザーの言語でこれらの文字がサポートされていない場合、ユーザーはパスワードを設定できません。UTF-8 文字をサポートするには、次のチェックボックスをオフにします。
  - **小文字の英文字**
  - **大文字の英文字**
- [パスワード変更差分（Password Change Delta）]：現在のパスワードを新しいパスワードに変更するときに変更する必要がある最小文字数を指定します。Cisco ISE では、文字の位置を変更することは変更とみなされません。たとえば、パスワードの差分が 3 で、現在のパスワードが「?Aa1234?」の場合、「?Aa1567?」（「5」、「6」、「7」は 3 つの新しい文字です）は有効な新しいパスワードです。「?Aa1562?」は、「?」、「2」、および「?」

の文字が現在のパスワードに含まれているため無効です。文字位置が変更された場合でも、同じ文字が現在のパスワードに含まれているため、「Aa1234??」は無効になります。

また、パスワード変更差分では、以前の X パスワードが考慮されます。この X は、[パスワードは前のバージョンと異なっている必要があります（Password must be different from the previous versions）] の値です。パスワードの差分が 3 で、パスワードの履歴が 2 である場合は、過去 2 つのパスワードの一部ではない 4 文字を変更する必要があります。

- [辞書の単語（Dictionary words）]：辞書の単語、辞書の単語の逆順での使用、単語内の文字を別の文字で置き換えた単語の使用を制限する場合は、このチェックボックスをオンにします。

  「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば、「Pa$$w0rd」です。

  - [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。
  - [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択（Choose File）] をクリックし、カスタム辞書ファイルを選択します。このテキストファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。

- [パスワードの有効期間（Password Lifetime）] セクションを使用して、パスワードのリセット間隔と通知を更新できます。パスワードの有効期間を設定するには、[パスワードを__日ごとに変更する（有効範囲は1～3650）（Change password every __ days (valid range 1 to 3650)）] チェックボックスをオンにし、入力フィールドに日数を入力します。[ユーザーアカウントを無効にする（Disable User Account）] オプションを選択して、指定された時間内にユーザーがパスワードを変更しなかった場合にユーザーアカウントを無効にすることができます。[次回のログイン時にパスワードの変更が必要（Require password change on next login）] を選択して、次回 Cisco ISE にログインするときにパスワードを変更するようにユーザーに求めます。

  パスワードをリセットするためのリマインダ電子メールを送信するには、[パスワード有効期限の __ 日前にリマインダを表示する（Display Reminder __ Days Before to Password Expiration）] チェックボックスをオンにし、ネットワークアクセスユーザーに設定された電子メールアドレスにリマインダ電子メールを送信するまでの日数を入力します。ネットワークアクセスユーザーを作成するときに、[管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [ネットワークアクセスユーザーの追加（Add Network Access User）] ウィンドウで電子メールアドレスを追加して、パスワードのリセットに関する電子メール通知を送信できます。

（注）

- リマインダ電子メールは、iseadminportal@<ISE-Primary-FQDN>から送信されます。この送信者のアクセスを明示的に許可する必要があります。
- デフォルトでは、リマインダ電子メールには次の内容が含まれています。ネットワーク アクセスパスワードは、<*password expiry date and time*> に失効します。Please contact your system administrator for assistance.

  Cisco ISE リリース 3.2 以降では、電子メール通知の「システム管理者に連絡して支援を受けてください（Please contact your system administrator for assistance）」の部分の後の電子メールの内容をカスタマイズできます。

- [不正なログイン試行によるアカウントのロック/一時停止（Lock/Suspend Account with Incorrect Login Attempts）]：このオプションを使用して、ログイン試行が指定した回数失敗した場合にアカウントを一時停止またはロックできます。有効な範囲は、3～20です。
- [アカウント無効化ポリシー（Account Disable Policy）]：既存のユーザーアカウントを無効にするタイミングに関するルールを設定できます。詳細については、「グローバルにユーザー アカウントを無効にする」を参照してください。

関連トピック

ユーザー アカウントのカスタム属性 （20 ページ）
ユーザーの追加方法 （24 ページ）

ユーザーおよび管理者用の自動パスワードの生成

ユーザーおよび管理者の作成ウィンドウで [パスワードの生成（Generate Password）] オプションを使用して、Cisco ISE パスワードポリシーに従うインスタントパスワードを生成します。これにより、ユーザーまたは管理者は設定する安全なパスワードを考えるために時間を費やすことなく、Cisco ISE によって生成されたパスワードを使用することができます。

[パスワードの生成（Generate Password）] オプションは、次のウィンドウで使用できます。

- [管理（Administration）]>[ID 管理（Identity Management）]>[ID（Identities）]>[ユーザー（Users）]の順に選択します。
- [管理（Administration）]>[システム（System）]>[管理者アクセス（Admin Access）]>[管理者（Administrators）]>[管理者ユーザー（Admin Users）]の順に選択します。
- [設定（Settings）]>[アカウント設定（Account Settings）]>[パスワードの変更（Change Password）]の順に選択します。

内部ユーザー操作

ユーザーの追加方法

Cisco ISE では、Cisco ISE ユーザーの属性を表示、作成、編集、複製、削除、ステータス変更、インポート、エクスポート、または検索できます。

Cisco ISE 内部データベースを使用する場合、Cisco ISE ネットワークのリソースまたはサービスへのアクセスを必要とするすべての新規ユーザーのアカウントを作成する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** を選択します。

[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ID（Identities）] > [ユーザー（Users）] ウィンドウにアクセスすることによって、ユーザーを作成することもできます。

ステップ 2 新しいユーザーを作成するには、[追加（Add）]（+）をクリックします。

ステップ 3 すべてのフィールドに値を入力します。

（注） !、%、:、;、[、{、|、}、]、`、?、=、<、>、\、および制御文字をユーザー名に使用しないでください。スペースのみのユーザー名も許可されません。BYOD 用に Cisco ISE 内部認証局（CA）を使用する場合、ここに入力したユーザー名がエンドポイント証明書の共通名として使用されます。Cisco ISE 内部 CA は、「+」または「*」の文字を [共通名（Common Name）] フィールドでサポートしていません。

ステップ 4 [送信（Submit）] をクリックして、Cisco ISE 内部データベースに新しいユーザーを作成します。

Cisco ISE ユーザー データのエクスポート

Cisco ISE 内部データベースからユーザー データをエクスポートしなければならない場合があります。Cisco ISE では、パスワード保護された csv ファイル形式でユーザー データをエクスポートすることができます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** を選択します。

ステップ 2 データをエクスポートするユーザーに対応するチェックボックスをオンにします。

ステップ 3 [選択済みをエクスポート（Export Selected）] をクリックします。

ステップ 4 [キー（Key）] フィールドに、パスワードを暗号化するためのキーを入力します。

ステップ 5 [エクスポート開始（Start Export）] をクリックして、users.csv ファイルを作成します。

ステップ 6 [OK] をクリックして、users.csv ファイルをエクスポートします。

Cisco ISE 内部ユーザーのインポート

新しい内部アカウントを作成するために、CSV ファイルを使用して新しいユーザーデータを Cisco ISE にインポートできます。ユーザーアカウントのインポート中にテンプレートの CSV ファイルをダウンロードに使用できます。スポンサーはスポンサー ポータルでユーザーをインポートできます。スポンサーゲストアカウントが使用する情報タイプの設定に関する情報については、を参照してくださいスポンサー アカウント作成のためのアカウント コンテンツの設定 。

（注） CSV ファイルにカスタム属性が含まれている場合、カスタム属性に設定するデータタイプと許容範囲は、インポート時にカスタム属性の値に適用されます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** を選択します。

ステップ 2 [インポート（Import）] をクリックして、カンマ区切りテキスト ファイルからユーザーをインポートします。

カンマ区切りテキストファイルがない場合は、[テンプレートの生成（Generate a Template）] をクリックし、ヘッダー行に値が取り込まれている CSV ファイルを作成します。

ステップ 3 [ファイル（File）] テキスト ボックスに、インポートするユーザーが含まれたファイル名を入力するか、[参照（Browse）] をクリックして、ファイルが配置されている場所に移動します。

ステップ 4 新しいユーザーを作成して既存のユーザーを更新する場合は、[新しいユーザーの作成と新しいデータでの既存ユーザーの更新（Create new user(s) and update existing user(s) with new data）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

（注） すべてのネットワーク アクセス ユーザーを一度に削除しないことを推奨します。一度に削除すると、特に非常に大規模なデータベースを使用している場合は、CPU スパイクとサービスのクラッシュにつながる場合があるためです。

エンドポイント設定

表 *9:* エンドポイント設定

フィールド名	使用上のガイドライン
MAC アドレス	エンドポイントを静的に作成するには、MAC アドレスを 16 進数形式で入力します。 MAC アドレスは、Cisco ISE 対応のネットワークに接続するインターフェイスのデバイス ID です。
スタティック割り当て（Static Assignment）	[エンドポイント（Endpoints）] ウィンドウでエンドポイントを静的に作成する場合このチェックボックスをオンにすると、静的割り当てのステータスが static に設定されます。 エンドポイントのスタティック割り当てのステータスを静的から動的に、または動的から静的に切り替えできます。
ポリシー割り当て	（[スタティック割り当て（Static Assignment）] が選択されていない限り、デフォルトで無効）[ポリシー割り当て（Policy Assignment）] ドロップダウンリストから一致するエンドポイントポリシーを選択します。 次のいずれかを実行できます。 • 一致するエンドポイント ポリシーを選択しないで、デフォルトのエンドポイントポリシーである不明を使用する場合、スタティック割り当てステータスはエンドポイントに対して動的に設定され、それにより、エンドポイントの動的プロファイリングが可能になります。 • [不明（Unknown）] ではなく、一致するエンドポイントポリシーを選択する場合、スタティック割り当てのステータスはそのエンドポイントに対して静的に設定され、[スタティック割り当て（Static Assignment）] チェックボックスが自動的にオンになります。

フィールド名	使用上のガイドライン
スタティック グループ割り当て（Static Group Assignment）	エンドポイントをIDグループに静的に割り当てる場合はこのチェックボックスをオンにします。 このチェックボックスをオンにした場合、プロファイリング サービスは、前に他のエンドポイントIDグループに動的に割り当てられたエンドポイントの次のエンドポイントポリシーの評価時に、そのエンドポイントIDグループを変更しません。 このチェックボックスをオフにした場合、エンドポイントIDグループは、ポリシー設定に基づいてISEプロファイラにより割り当てられたダイナミック グループです。[スタティック グループ割り当て（Static Group Assignment）] オプションを選択しない場合、エンドポイントは、エンドポイント ポリシーの次回評価時に一致するIDグループに自動的に割り当てられます。

ID グループ割り当て	エンドポイントを割り当てるエンドポイントID グループを選択します。
	
	エンドポイントを静的に作成する場合、またはエンドポイントのエンドポイントポリシーの評価時に [一致する ID グループの作成（Create Matching Identity Group）] オプションを使用しない場合は、エンドポイントをIDグループに割り当てることができます。
	
	Cisco ISE には、次のシステムによって作成された次のエンドポイントIDグループがあります。
	• [ブラックリスト（Blacklist）]
	• GuestEndpoints
	• プロファイル済み
	  • Cisco IP-Phone
	  • ワークステーション
	• RegisteredDevices
	• 不明

関連トピック

識別されたエンドポイント （271 ページ）
ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 （265 ページ）

エンドポイントの LDAP からのインポートの設定

表 *10*：エンドポイントの、*LDAP* からのインポートの設定

フィールド名	使用上のガイドライン
接続の設定	
Host	LDAP サーバーのホスト名または IP アドレスを入力します。
[ポート（Port）]	LDAP サーバーのポート番号を入力します。デフォルト ポート 389 を使用して LDAP サーバーからインポートするか、デフォルト ポート 636 を使用して SSL を介して LDAP サーバーからインポートできます。 （注） Cisco ISE では、任意の設定済みポート番号をサポートします。設定済みの値は、LDAP サーバー接続詳細に一致する必要があります。
セキュア接続を有効にする（Enable Secure Connection）	SSL を介して LDAP サーバーからインポートするには、[セキュア接続を有効にする（Enable Secure Connection）] チェックボックスをオンにします。
ルート CA 証明書名	ドロップダウン矢印をクリックして、信頼できる CA 証明書を表示します。 ルート CA 証明書名は、LDAP サーバーに接続する場合に必要となる信頼できる CA 証明書を指します。Cisco ISE 内の CA 証明書は、追加（インポート）、編集、削除、およびエクスポートが可能です。
匿名バインド（Anonymous Bind）	[匿名バインド（Anonymous Bind）] チェックボックスをオンにするか、または slapd.conf コンフィギュレーション ファイルの LDAP 管理者クレデンシャルを入力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
管理者 DN（**Admin DN**）	slapd.conf コンフィギュレーション ファイルで LDAP 管理者に設定されている識別名（DN）を入力します。 管理者 DN フォーマット例：cn=Admin, dc=cisco.com, dc=com
パスワード	LDAP 管理者に設定されたパスワードを slapd.conf コンフィギュレーション ファイルに入力します。
ベース DN（**Base DN**）	親エントリの認定者名を入力します。 ベース DN フォーマット例：dc=cisco.com, dc=com
クエリ設定（**Query Settings**）	
MAC アドレス objectClass（**MAC Address objectClass**）	MACアドレスのインポートに使用されるクエリフィルタ（ieee802Device など）を入力します。
MAC アドレス属性名（**MAC Address Attribute Name**）	インポートに対して返される属性名（macAddress など）を入力します。

フィールド名	使用上のガイドライン
プロファイル属性名（**Profile Attribute Name**）	LDAP 属性の名前を入力します。この属性は、LDAP サーバーで定義されている各エンドポイント エントリのポリシー名を保持します。 [プロファイル属性名（Profile Attribute Name）] フィールドを設定する場合は、次の点を考慮してください。 • [プロファイル属性名（Profile Attribute Name）] フィールドでこの LDAP 属性を指定しない場合、またはこの属性を誤って設定した場合、インポート操作時にエンドポイントは [不明（Unknown）]としてマークされ、これらのエンドポイントは一致するエンドポイント プロファイリングポリシーに個別にプロファイリングされます。 • [プロファイル属性名（Profile Attribute Name）] フィールドで LDAP 属性を設定した場合、その属性値は、エンドポイントポリシーが Cisco ISE 内の既存のポリシーに一致することを確認するために検証され、エンドポイントがインポートされます。エンドポイント ポリシーが既存のポリシーと一致しない場合、それらのエンドポイントはインポートされません。
タイムアウト（**Time Out**）	この時間は秒数で入力します。有効な範囲は 1 ～ 60 秒です。

関連トピック

識別されたエンドポイント （271 ページ）
LDAP サーバーからのエンドポイントのインポート （270 ページ）

ID グループ操作

ユーザー ID グループの作成

ユーザー ID グループを追加する前に、ユーザー ID グループを作成する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [IDグループ（Identity Groups）] > [ユーザー ID グループ（User Identity Groups）] > [追加（Add）]** を選択します。

[ワークセンター（Work Centers）]>[デバイス管理（Device Administration）]>[ユーザーIDグループ（User Identity Groups）] > [IDグループ（Identity Groups）] > [ユーザーIDグループ（User Identity Groups）] > [追加（Add）] ページにアクセスして、ユーザー ID グループを作成することもできます。

ステップ 2 [名前（Name）] フィールドおよび [説明（Description）] フィールドに値を入力します。[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、# $ & ‘ ( ) * + - . / @ _。

ステップ 3 **[送信（Submit）]** をクリックします。

関連トピック

ユーザー ID グループ （19 ページ）

ユーザー ID グループのエクスポート

Cisco ISE では、ローカルに設定されたユーザー ID グループを csv ファイル形式でエクスポートすることができます。

ステップ 1 [管理（Administration）] > [ID 管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザー ID グループ（User Identity Groups）] を選択します。

ステップ 2 エクスポートするユーザー ID グループに対応するチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 [OK] をクリックします。

ユーザー ID グループのインポート

Cisco ISE では、ユーザー ID グループを csv ファイル形式でインポートすることができます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ID グループ（Identity Groups）] > [ユーザー ID グループ（User Identity Groups）]** を選択します。

ステップ 2 インポートファイルに使用するテンプレートを取得するには、[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 [インポート（Import）] をクリックして、カンマ区切りテキストファイルからネットワーク アクセス ユーザーをインポートします。

ステップ 4 新しいユーザー ID グループの追加、および既存のユーザー ID グループの更新の両方を実行する必要がある場合は、[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。

ステップ 5 [インポート（Import）] をクリックします。

ステップ 6 Cisco ISE データベースに変更を保存するには、[保存（Save）] をクリックします。

エンドポイント ID グループの設定

表 *11* : エンドポイント *ID* グループの設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するエンドポイント ID グループの名前を入力します。
説明（**Description**）	作成するエンドポイント ID グループの説明を入力します。
親グループ（**Parent Group**）	新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを、[親グループ（Parent Group）] ドロップダウンリストから選択します。

関連トピック

識別されたエンドポイントの、エンドポイント ID グループでのグループ化 （274 ページ）
エンドポイント ID グループの作成 （273 ページ）

最大同時セッション数の設定

最適なパフォーマンスを得るために、同時ユーザー セッション数を制限できます。ユーザー レベルまたはグループ レベルで制限を設定できます。最大ユーザー セッションの設定に応じて、セッション カウントはユーザーに適用されます。

ISE ノードごとに各ユーザーの同時セッションの最大数を設定できます。この制限を超えるセッションは拒否されます。

ステップ 1 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [最大セッション数（Max Sessions）] > [ユーザー（User）] を選択します。

ステップ 2 次のいずれかを実行します。

- 各ユーザーに許可される同時セッションの最大数を、[ユーザーごとの最大セッション数（Maximum Sessions per User）] フィールドに入力します。
- ユーザーのセッション数を無制限にするには、[セッション数無制限（Unlimited Sessions）] チェックボックスをオンにします。このオプションは、デフォルトで選択されます。

ステップ 3 [保存（Save）] をクリックします。

セッションの最大数がユーザー レベルとグループ レベルの両方で設定されている場合、小さい方の値が優先されます。たとえば、ユーザーの最大セッション値が 10 に設定されていて、

ユーザーが属するグループの最大セッション値が5に設定されている場合、ユーザーは最大で5 つのセッションのみを持つことができます。

（注） 最大同時セッション数は、設定されている PSN によって管理されます。このカウントは PSN 間で同期されません。ユーザーまたはグループごとの最大同時セッション数が設定されている Cisco ISE で認証が行われ、別のプロキシサーバーで許可が行われる場合、最大同時セッション制限は Cisco ISE にのみ適用され、プロキシサーバーには適用されません。

最大同時セッション数はランタイムプロセスで実装され、データはメモリにのみ保存されます。PSN が再起動されると、最大同時セッションカウンタがリセットされます。

最大同時セッション数は、使用されるネットワーク アクセス デバイスに関係なく、ユーザー名に関して大文字と小文字を区別しません（同じ PSN ノードが使用されている場合）。

グループの最大同時セッション数

ID グループの最大同時セッション数を設定できます。

グループ内の少人数のユーザーによってすべてのセッションが使用される場合があります。他のユーザーからの新しいセッションの作成要求は、セッション数がすでに最大設定値に達しているため、拒否されます。Cisco ISE では、グループ内の各ユーザーに最大セッション制限を設定できます。特定の ID グループに所属する各ユーザーは、同じグループの他のユーザーが開いているセッション数に関係なく、制限以上はセッションを開くことができません。特定のユーザーのセッション制限を計算する場合は、ユーザー1 人あたりのグローバルセッション制限、ユーザーが所属する ID グループあたりのセッション制限、グループ内のユーザー 1 人あたりのセッション制限のいずれかの最小設定値が優先されます。

ID グループの同時セッションの最大数を設定するには、次の手順に従います。

ステップ 1 [管理（Administration）]>[システム（System）]>[設定（Settings）]>[最大セッション数（Max Sessions）]>[グループ（Group）] の順に選択します。

設定した ID グループがすべて一覧表示されます。

ステップ 2 編集するグループの横にある [編集（Edit）] アイコンをクリックして、次の値を入力します。

- そのグループに許可される同時セッションの最大数。グループのセッションの最大数を 100 に設定した場合、グループのすべてのメンバーによって確立されたすべてのセッションの総数は 100 を超えることはできません。

  （注） グループ階層に基づいてグループ レベルのセッションが適用されます。

- そのグループの各ユーザーに許可される同時セッションの最大数。このオプションは、グループの最大セッション数を上書きします。

グループの同時セッションの最大数、またはグループ内のユーザーの同時セッションの最大数を [無制限（Unlimited）] に設定するには、[グループの最大セッション数/グループ内のユーザーの最大セッション数（Max Sessions for User in Group/Max Sessions for User in Group）] フィールドを空白にし、ティック アイコンをクリックし、[保存（Save）] をクリックします。デフォルトでは、両方の値が [無制限（Unlimited）] に設定されています。

ステップ 3 [保存（Save）] をクリックします。

カウンタの時間制限の設定

同時ユーザー セッションのタイムアウトを設定できます。

ステップ 1 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [最大セッション数（Max Sessions）] > [カウンタの時間制限（Counter Time Limit）] 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。

- [無制限（Unlimited）]：セッションのタイムアウトまたは時間制限を設定しない場合は、このチェックボックスをオンにします。
- [経過後にセッションを削除（Delete sessions after）]：日、時間、分の単位で同時セッションのタイムアウト値を入力できます。セッションが時間制限を超えると、Cisco ISE はカウンタからセッションを削除してセッション数を更新するため、新しいセッションが許可されます。ユーザーは、セッションの時間制限を超えた場合、ログアウトされません。

ステップ 3 [保存（Save）] をクリックします。

[RADIUS ライブログ（RADIUS Live Logs）] ウィンドウでセッションカウントをリセットできます。[ID（Identity）]、[ID グループ（Identity Group）]、[サーバー（Server）] 列に表示される [アクション（Actions）] アイコンをクリックして、セッション カウントをリセットします。セッションをリセットすると、セッションはカウンタから削除されます（これにより、新しいセッションが許可されます）。ユーザーのセッションがカウンタから削除されても、ユーザーの接続は切断されません。

アカウントの無効化ポリシー

ユーザーまたは管理者の認証または問い合わせ時に、Cisco ISE は **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザー認証設定（User Authentication Settings）]** でグローバルアカウント無効化ポリシー設定を確認し、その構成に基づいて認証または結果を返します。

Cisco ISE は、次の 3 つのポリシーを確認します。

- [指定した日付（yyyy-mm-dd）を超えたらユーザーアカウントを無効にする（Disable user accounts that exceed a specified date (yyyy-mm-dd)）]：設定された日付にユーザーアカウント

を無効にします。ただし、[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [アカウント無効化ポリシー（Account Disable Policy）] で設定された個々のネットワーク アクセス ユーザーのアカウント無効化ポリシー設定はグローバル設定よりも優先されます。

- [アカウント作成時または最後の有効化から *n* 日後にユーザーアカウントを無効にする（Disable user account after n days of account creation or last enable）] : アカウントの作成またはアカウントが有効になった最後の日から指定した日数後にユーザーアカウントを無効にします。[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] > [ステータス（Status）] でユーザーのステータスを確認できます。
- 非アクティブになってから *n* 日後にアカウントを無効にする（Disable accounts after n days of inactivity）] : 設定した連続日数、認証されなかった管理者およびユーザーアカウントを無効化します。

Cisco Secure ACS から Cisco ISE に移行する際、Cisco Secure ACS ではネットワーク アクセス ユーザー用に指定したアカウント無効化ポリシーの設定は Cisco ISE に移行されます。

個別のユーザー アカウントの無効化

Cisco ISE では、アカウントの無効日が管理者ユーザーによって指定された日付を超えた場合は、各個人ユーザーのユーザー アカウントを無効にすることができます。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] の順に選択します。

ステップ 2 [追加（Add）] をクリックして新しいユーザーを作成するか、既存のユーザーの横のチェックボックスをオンにして [編集（Edit）] をクリックして既存のユーザーの詳細を編集します。

ステップ 3 [日付を超えたらアカウントを無効化する（Disable account if the date exceeds）] チェックボックスをオンにして、日付を選択します。

このオプションによって、ユーザー レベルで設定した日付を超えたときに、ユーザー アカウントをディセーブルにすることができます。必要に応じて、異なるユーザーに異なる失効日を設定できます。このオプションは、個々のユーザーのグローバル コンフィギュレーションを無効にします。日付には、現在のシステム日付または将来の日付を設定できます。

（注） 現在のシステム日付よりも古い日付は入力できません。

ステップ 4 [送信（Submit）] をクリックして、個々のユーザーのアカウント無効化ポリシーを設定します。

グローバルにユーザー アカウントを無効にする

特定の日付、アカウントの作成日または最終アクセス日から数日後、およびアカウントが非アクティブになってから数日後に、ユーザー アカウントを無効にすることができます。

ステップ 1 [管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザー認証設定（User Authentication Settings）] > [アカウント無効化ポリシー（Account Disable Policy）] を選択します。

ステップ 2 次のいずれかの操作を実行します。

- [日付を超えるとアカウントを無効にする（Disable account if date exceeds）] チェック ボックスをオンにして、yyyy-mm-dd 形式の適切な日付を選択します。このオプションによって、設定した日付の後、ユーザー アカウントを無効にすることができます。ユーザー レベルでの [日付を超えるとアカウントを無効にする（Disable account if date exceeds）] オプションは、このグローバル設定よりも優先されます。
- [アカウントの作成または最後に有効になってから n 日後にアカウントを無効にする（Disable account after n days of account creation or last enable）] チェック ボックスをオンにして、日数を入力します。このオプションは、アカウントの作成日または最終アクセス日が指定した日数を超えたときにユーザー アカウントを無効にします。管理者は、無効化されたユーザー アカウントを手動で有効にでき、有効にすると、日数の数はリセットされます。
- [非アクティブになってから n 日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオンにして、日数を入力します。このオプションは、アカウントが指定した日数非アクティブのときにユーザー アカウントを無効にします。

ステップ 3 [送信（Submit）] をクリックし、グローバル アカウント無効化ポリシーを設定します。

（注） **[非アクティブ状態で n 日経過後のアカウントを無効化（Disable account after n days of inactivity）]** オプションを使用して、Cisco ISE の非アクティブユーザーを無効にすると、デバイスポータルにログインしたエンドポイントのアクティブな日数はリセットされません。これは、デバイスポータルがプロファイリングの更新やアカウンティング情報を送信しないためです。

内部 ID ソースと外部 ID ソース

アイデンティティ ソースは、ユーザー情報を保存するデータベースです。Cisco ISE は、アイデンティティ ソースのユーザー情報を使用して、認証時にユーザー クレデンシャルを検証します。ユーザー情報には、グループ情報と、そのユーザーに関連付けられているその他の属性が含まれます。ID ソースに対してユーザー情報の追加、編集、および削除を行うことができます。

Cisco ISE では内部 ID ソースと外部 ID ソースがサポートされます。スポンサーとゲストユーザーの認証に両方のソースを使用できます。

内部 ID ソース

Cisco ISE には、ユーザー情報を保存できる内部ユーザー データベースがあります。内部ユーザー データベースのユーザーは、内部ユーザーと呼ばれます。Cisco ISE には、Cisco ISE に接

続するすべてのデバイスおよびエンドポイントに関する情報を格納する内部エンドポイントデータベースもあります。

外部 ID ソース

Cisco ISE では、ユーザー情報を含む外部 ID ソースを設定することができます。Cisco ISE は外部 ID ソースに接続して、認証用のユーザー情報を取得します。外部 ID ソースには、Cisco ISE サーバーおよび証明書認証プロファイルの証明書情報も含まれます。Cisco ISE は外部 ID ソースとの通信に認証プロトコルを使用します。

内部ユーザーのポリシーを設定する際は、次の点に注意してください。

- 内部 ID ストアに対して内部ユーザーを認証するための認証ポリシーを設定します。
- 次のオプションを選択して、内部ユーザー グループの許可ポリシーを設定します。

```
Identitygroup.Name EQUALS User Identity Groups: Group_Name
```

次の表に、認証プロトコルおよびサポートされる外部 ID ソースを示します。

表 *12 :* 認証プロトコルとサポートされている外部 *ID* ソース

プロトコル（認証タイプ）	内部データベース	Active Directory	LDAP	RADIUS トークン サーバーまたは RSA	ODBC
EAP-GTC、PAP（プレーン テキスト パスワード）	対応	対応	対応	対応	対応
MS-CHAP パスワード ハッシュ： MSCHAPv1/v2 EAP-MSCHAPv2（PEAP、EAP-FAST、または EAP-TTLS の内部メソッドとして） LEAP	対応	対応	×	×	対応

プロトコル（認証タイプ）	内部データベース	Active Directory	LDAP	RADIUS トークンサーバーまたは RSA	ODBC
EAP-MD5 CHAP	対応	×	×	×	対応
EAP-TLS PEAP-TLS （証明書取得） （注） TLS 認証（EAP-TLS と PEAP-TLS）に ID ソースは必須ではありませんが、許可ポリシー条件のために任意で追加できます。	×	対応	対応	×	×

クレデンシャルを保存する方法は、外部データ ソースの接続タイプと使用される機能に応じて異なります。

- Active Directory ドメイン（パッシブ ID 用ではない）に参加する場合、参加に使用されるクレデンシャルは保存されません。Cisco ISE は、AD コンピュータ アカウントが存在しない場合はそのアカウントを作成し、そのアカウントを使用してユーザーを認証します。
- LDAP およびパッシブ ID の場合、外部データ ソースへの接続に使用されるクレデンシャルは、ユーザーの認証にも使用されます。

外部 ID ソースの作成

Cisco ISE では、Active Directory、LDAP、RADIUS トークン、RSA SecurID サーバーなどの外部 ID ソースに接続して、認証/許可のユーザー情報を取得できます。外部 ID ソースには、証明書ベースの認証に必要な証明書認証プロファイルも含まれています。

（注） 認証済みユーザー ID を受信して共有できるようにするパッシブ ID サービスを使用するには、その他の パッシブ ID サービス プロバイダ （98 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- 証明書認証プロファイル（Certificate Authentication Profile）：証明書ベースの認証の場合。
- [Active Directory]：外部 ID ソースとして Active Directory に接続する場合。詳細については、外部 ID ソースとしての Active Directory （41 ページ）を参照してください。
- LDAP：LDAP ID ソースを追加する場合。詳細については、LDAP （145 ページ）を参照してください。
- RADIUS トークン（RADIUS Token）：RADIUS トークン サーバーを追加する場合。詳細については、RADIUS トークン ID ソース （170 ページ）を参照してください。
- RSA SecurID：RSA SecurID サーバーを追加する場合。詳細については、RSA ID ソース （176 ページ）を参照してください。
- SAML IDプロバイダ（SAML Id Providers）：Oracle Access Manager などの ID プロバイダ（IdP）を追加する場合。詳細については、外部 ID ソースとしての SAMLv2 ID プロバイダ （184 ページ）を参照してください。
- [ソーシャルログイン（Social Login）]：Facebook などのソーシャルログインを外部 ID ソースとして追加する場合。詳細については、アカウント登録ゲストのソーシャル ログイン を参照してください。

外部 ID ストアパスワードに対する内部ユーザーの認証

Cisco ISE では、外部 ID ストア パスワードに対して内部ユーザーを認証できます。Cisco ISE では、[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）] ウィンドウから、内部ユーザーのパスワード ID ストアを選択するオプションが提供されます。管理者は、Cisco ISE の外部 ID ソースのリストから ID ストアを選択することができ、[ユーザー（Users）] ウィンドウでユーザーを追加するか、または編集します。内部ユーザーのデフォルトのパスワード ID ストアは内部 ID ストアです。Cisco Secure ACS ユーザーは、Cisco Secure ACS から Cisco ISE への移行中および移行後、同じパスワード ID ストアを維持します。

Cisco ISE はパスワード タイプに対し次の外部 ID ストアをサポートします。

- Active Directory
- LDAP
- ODBC
- RADIUS トークン サーバー
- RSA SecurID サーバー

（注） 現在の設計では、外部 ID ストアに対して認証が行われる場合、内部ユーザー ID グループ名は認証ポリシー内に設定できません。許可に内部ユーザー ID グループを使用するには、内部ユーザー ID ストアに対して認証するように認証ポリシーを設定する必要があります。また、ユーザー設定でパスワードタイプ（内部または外部）を選択する必要があります。

証明書認証プロファイル

プロファイルごとに、プリンシパルユーザー名として使用する証明書フィールドと、証明書のバイナリ比較を行うかどうかを指定する必要があります。

証明書認証プロファイルの追加

Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）証明書ベースの認証方式を使用する場合は、証明書認証プロファイルを作成する必要があります。従来のユーザー名とパスワードの方法で認証する代わりに、Cisco ISE はクライアントから受信した証明書をサーバー内の証明書と比較してユーザーの信頼性を確認します。

始める前に

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

ステップ 2 証明書認証プロファイルの名前と説明（任意）を入力します。

ステップ 3 ドロップダウン リストから ID ストアを選択します。

基本証明書のチェックは ID ソースを必要としません。証明書にバイナリ比較チェックが必要な場合は、ID ソースを選択する必要があります。ID ソースとして Active Directory を選択した場合は、サブジェクト名、一般名、およびサブジェクト代替名（すべての値）を使用してユーザーを検索できます。

ステップ 4 [証明書属性（Certificate Attribute）] または [証明書の任意のサブジェクトまたは代替名属性（Any Subject or Alternative Name Attributes in the Certificate）] から ID の使用を選択します。これは、ログで検索のために使用されます。

[証明書の任意のサブジェクトまたは代替名属性（Any Subject or Alternative Name Attributes in the Certificate）] を選択すると、Active Directory UPN がログ用のユーザー名として使用され、証明書のすべてのサブジェクト名および代替名がユーザーの検索に試行されます。このオプションは、ID ソースとして Active Directory を選択した場合にのみ使用できます。

ステップ 5 **クライアント証明書を ID ストアの証明書と照合する**場合に選択します。この場合、ID ソース（LDAP または Active Directory）を選択する必要があります。[Active Directory] を選択した場合は、ID のあいまいさを解決するためにのみ証明書を照合することを選択できます。

- [なし（Never）]：このオプションは、バイナリ比較を実行しません。
- [ID のあいまいさを解決する目的のみ（Only to resolve identity ambiguity）]：このオプションは、あいまいさが見つかった場合にのみ、クライアント証明書と Active Directory のアカウントの証明書とのバイナリ比較を実行します。たとえば、複数の Active Directory アカウントが証明書の識別名に一致することがあります。
- [常にバイナリ比較を実行する（Always perform binary comparison）]：このオプションは、クライアント証明書と ID ストア（Active Directory または LDAP）内のアカウントの証明書とのバイナリ比較を常に実行します。

ステップ 6 [送信（Submit）] をクリックして、証明書認証プロファイルを追加するか、変更を保存します。

外部 ID ソースとしての Active Directory

Cisco ISE は、ユーザー、マシン、グループ、属性などのリソースにアクセスするために、Microsoft Active Directory を外部 ID ソースとして使用します。Active Directory でのユーザーとマシンの認証では、Active Directory にリストされているユーザーとデバイスに対してのみネットワーク アクセスを許可します。

ISE コミュニティ リソース

ISE Administrative Portal Access with AD Credentials Configuration Example

Active Directory でサポートされる認証プロトコルおよび機能

Active Directory は、一部のプロトコルを使用したユーザーとマシンの認証、Active Directory ユーザー パスワードの変更などの機能をサポートしています。次の表に、Active Directory でサポートされる認証プロトコルおよびそれぞれの機能を示します。

表 *13 : Active Directory* でサポートされる認証プロトコル

認証プロトコル	機能
EAP-FAST およびパスワードベースの Protected Extensible Authentication Protocol（PEAP）	MS-CHAPv2 および EAP-GTC の内部方式で EAP-FAST と PEAP を使用するパスワード変更機能を備えたユーザーとマシンの認証
Password Authentication Protocol（PAP）	ユーザーおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol Version 1（MS-CHAPv1）	ユーザーおよびマシン認証
Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）	ユーザーおよびマシン認証

認証プロトコル	機能
Extensible Authentication Protocol-Generic Token Card（EAP-GTC）	ユーザーおよびマシン認証
Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）	• ユーザーおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling-Transport Layer Security（EAP-FAST-TLS）	• ユーザーおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Protected Extensible Authentication Protocol-Transport Layer Security（PEAP-TLS）	• ユーザーおよびマシン認証 • グループおよび属性取得 • 証明書のバイナリ比較
Lightweight Extensible Authentication Protocol（LEAP）	ユーザー認証

許可ポリシーで使用する Active Directory 属性およびグループの取得

Cisco ISE は、許可ポリシー ルールで使用するために Active Directory からユーザーまたはマシンの属性およびグループを取得します。これらの属性は Cisco ISE ポリシーで使用され、ユーザーまたはマシンの承認レベルを決定します。Cisco ISE は、認証が成功した後にユーザーおよびマシンの Active Directory 属性を取得します。認証とは別に、許可のために属性を取得することもできます。

Cisco ISE は、外部 ID ストア内のグループを使用してユーザーまたはコンピュータに権限を割り当てることがあります（たとえば、ユーザーをスポンサー グループにマップします）。Active Directory のグループ メンバーシップの次の制限事項に注意してください。

- ポリシー ルールの条件は、次のいずれかを参照します。ユーザーまたはコンピュータのプライマリ グループ、ユーザーまたはコンピュータが直接メンバーであるグループ、または間接的（ネストされた）グループ。
- ユーザーまたはコンピュータのアカウント ドメイン外のドメイン ローカル グループはサポートされません。

（注） Active Directory 属性の値 msRadiusFramedIPAddress を IP アドレスとして使用できます。この IP アドレスは、許可プロファイルのネットワーク アクセス サーバー（NAS）に送信できます。msRADIUSFramedIPAddress 属性は IPv4 アドレスだけをサポートします。ユーザー認証では、ユーザーに対し取得された msRadiusFramedIPAddress 属性値が IP アドレス形式に変換されます。

属性およびグループは、参加ポイントごとに取得され、管理されます。これらは許可ポリシーで使用されます（まず参加ポイントを選択し、次に属性を選択します）。許可のスコープごとに属性またはグループを定義することはできませんが、認証ポリシーでスコープを使用できます。認証ポリシーでスコープを使用する場合、ユーザーは 1 つの参加ポイントで認証されますが、ユーザーのアカウント ドメインへの信頼できるパスがある別の参加ポイント経由で属性またはグループを取得することができます。認証ドメインを使用して、1 つの範囲内にある 2 つの参加ポイントで認証ドメインが重複しないようにすることができます。

（注） マルチ参加ポイント設定の許可プロセス時に、Cisco ISE は、特定のユーザーが見つかるまで、認証ポリシーに記載されている順序で参加ポイントを検索します。ユーザーが見つかると、参加ポイント内のユーザーに割り当てられた属性とグループが、認証ポリシーを評価するために使用されます。

（注） 使用可能な Active Directory グループの最大数については、Microsoft の制限を参照してください。http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

ルールに、/、!、@、\、#、$、%、^、&、*、(、)、_、+、または~のような特殊文字を使用した Active Directory グループ名が含まれる場合、許可ポリシーは失敗します。

管理者ユーザー名に $ という文字が含まれている場合、Active Directory を介した管理者ユーザーのログインが失敗することがあります。

明示的な UPN の使用

ユーザー情報と Active Directory のユーザー プリンシパル名（UPN）属性を照合する場合の不確実性を減らすため、明示的な UPN を使用するように Active Directory を設定する必要があります。2 人のユーザーが同じ値 *sAMAccountName* を使用した場合、暗示的な UPN を使用すると、あいまいな結果が生成されます。

Active Directory で明示的な UPN を設定するには、[高度な調整（Advanced Tuning）] ページを開いて、属性 *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* を 1 に設定します。

ブール属性のサポート

Cisco ISE は、Active Directory および LDAP ID ストアからのブール属性の取得をサポートしています。

Active Directory または LDAP のディレクトリ属性を設定する際に、ブール属性を設定できます。これらの属性は、Active Directory または LDAP による認証時に取得されます。

ブール属性は、ポリシー ルール条件の設定に使用できます。

ブール属性値は、文字列型として Active Directory または LDAP サーバーから取得されます。Cisco ISE は、次のブール属性値をサポートしています。

ブール属性	サポートされる値
[はい（True）]	t、T、true、TRUE、True、1
いいえ（False）	f、F、false、FALSE、False、0

（注） 属性置換はブール属性ではサポートされません。

文字列型としてブール属性（たとえば、msTSAllowLogon）を設定すると、Active Directory または LDAP サーバーの属性のブール値は Cisco ISE の文字列属性に設定されます。属性タイプをブール型に変更したり、ブール型として属性を手動で追加できます。

証明書ベース認証の Active Directory 証明書の取得

Cisco ISE では、EAP-TLS プロトコルを使用するユーザーまたはマシン認証のための証明書取得がサポートされています。Active Directory 上のユーザーまたはマシン レコードには、バイナリ データ型の証明書属性が含まれています。この証明書属性に 1 つ以上の証明書を含めることができます。Cisco ISE ではこの属性は userCertificate として識別され、この属性に対して他の名前を設定することはできません。Cisco ISE はこの証明書を取得し、バイナリ比較の実行に使用します。

証明書認証プロファイルは、証明書の取得に使用する Active Directory のユーザーを検索するためにユーザー名を取得するフィールド（たとえば、サブジェクト代替名（SAN）または一般名）を決定します。Cisco ISE は、証明書を取得した後、この証明書とクライアント証明書とのバイナリ比較を実行します。複数の証明書が受信された場合、Cisco ISE は、いずれかが一致するかどうかをチェックするために証明書を比較します。一致が見つかった場合、ユーザーまたはマシン認証に合格します。

Active Directory ユーザー認証プロセス フロー

ユーザーの認証または問い合わせ時に、Cisco ISE は次のことをチェックします。

- MS-CHAP および PAP 認証では、ユーザーが無効かどうか、ロックアウトされているかどうか、期限切れかどうか、またはログイン時間外かどうかを確認します。これらの条件のいずれかが true の場合、認証が失敗します。
- EAP-TLS認証では、ユーザーが無効かどうか、ロックアウトされているかどうかを確認します。これらの条件のいずれかが一致する場合、認証が失敗します。

Active Directory マルチドメイン フォレストのサポート

Cisco ISE では、マルチドメイン フォレストの Active Directory がサポートされます。各フォレスト内で、Cisco ISE は単一のドメインに接続しますが、Cisco ISE が接続されているドメインと他のドメイン間に信頼関係が確立されている場合は、Active Directory フォレストの他のドメインからリソースにアクセスできます。

Active Directory サービスをサポートする Windows サーバー オペレーティング システムのリストについては、『Release Notes for Cisco Identity Services Engine』を参照してください。

（注） Cisco ISE は、ネットワーク アドレス トランスレータの背後にあり、ネットワーク アドレス変換（NAT）アドレスを持つMicrosoft Active Directory サーバーをサポートしません。

Active Directory と Cisco ISE の統合の前提条件

この項では、Cisco ISE と統合する Active Directory を設定するために必要な手動での作業手順について説明します。ただしほとんどの場合、Cisco ISE が Active Directory を自動的に設定するようにできます。次に、Cisco ISE と Active Directory を統合するための前提条件を示します。

- AD ドメイン設定の変更に必要な Active Directory ドメイン管理者クレデンシャルがあることを確認します。
- Cisco ISE でのネットワーク管理者またはシステム管理者の権限があることを確認します。
- Cisco ISE サーバーと Active Directory 間の時間を同期するために Network Time Protocol（NTP）サーバー設定を使用します。Cisco ISE CLI で NTP を設定できます。
- Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。特定の参加ポイントから他のドメインを照会する場合は、参加ポイントと、アクセスする必要があるユーザー情報およびマシン情報があるその他のドメインの間に信頼関係が確立されていることを確認します。信頼関係が確立されていない場合は、信頼できないドメインへの別の参加ポイントを作成する必要があります。信頼関係の確立の詳細については、Microsoft Active Directory のドキュメントを参照してください。
- Cisco ISE の参加先ドメインでは、少なくとも 1 つのグローバル カタログ サーバーが動作し、Cisco ISE からアクセス可能である必要があります。

さまざまな操作の実行に必要な Active Directory アカウント権限

参加操作	脱退処理	Cisco ISE マシン アカウント
参加操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシン アカウントがあるかどうかの確認） • ドメインに Cisco ISE マシン アカウントを作成する権限（マシン アカウントが存在しない場合） • 新しいマシン アカウントに属性を設定する権限（Cisco ISE マシン アカウント パスワード、SPN、dnsHostname など）	脱退操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシン アカウントがあるかどうかの確認） • ドメインから Cisco ISE マシンアカウントを削除する権限 強制脱退（パスワードなしの脱退）を実行する場合、ドメインからマシン アカウントは削除されません。	Active Directory 接続と通信する Cisco ISE マシン アカウントには、次の権限が必要です。 • パスワードを変更する。 • 認証されるユーザーおよびマシンに対応するユーザーおよびマシンオブジェクトを読み取る権限 • 情報を取得するために Active Directory をクエリする権限（信頼ドメイン、代替の UPN サフィックスなど） • tokenGroups 属性を読み取る権限 Active Directory でマシン アカウントを事前に作成できます。SAM の名前が Cisco ISE アプライアンスのホスト名と一致する場合は、参加操作中に検索して再利用します。 複数の参加操作が実行される場合、参加ごとに複数のマシン アカウントが Cisco ISE 内で保持されます。

（注） 参加操作または脱退操作に使用するクレデンシャルは Cisco ISE に保存されません。新規作成された Cisco ISE マシンアカウントのログイン情報のみが保存されます。

Microsoft Active Directory のセキュリティポリシー「**ネットワーク アクセス：SAM へのリモートの呼び出しを許可するクライアントを制限する**」が改訂されました。このため、Cisco ISE は 15 日ごとにマシンアカウントのパスワードを更新できない場合があります。マシンアカウントのパスワードが更新されない場合、Cisco ISE は Microsoft Active Directory を介してユーザーを認証しません。このイベントを通知するために、Cisco ISE ダッシュボードに [AD：ISE アカウントパスワードの更新に失敗（AD: ISE account password update failed）] アラームが表示されます。

（注） この問題は、Windows Server 2016 Active Directory 以降および Windows 10 バージョン 1607 の制限により発生します。この制限を克服するには、Windows Server 2016 Active Directory 以降または Windows 10 バージョン 1607 を Cisco ISE と統合する場合、レジストリ：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam のレジストリ値を non-zero から空白に設定して、すべてにアクセスを提供する必要があります。これにより、Cisco ISE がそのマシンのアカウントパスワードを更新できるようになります。

セキュリティポリシーにより、ユーザーはローカル セキュリティ アカウント マネージャ（SAM）データベース内と Microsoft Active Directory 内のユーザーとグループを列挙できます。Cisco ISE がマシンアカウントのパスワードを更新できるようにするには、Microsoft Active Directory の設定が正しいことを確認します。影響を受ける Windows オペレーティングシステムと Windows Server のバージョン、ネットワークにおけるこのセキュリティポリシーの意味、必要な変更の詳細については、以下を参照してください。

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

通信用に開放するネットワークポート

プロトコル	ポート（リモート ローカル）	ターゲット	認証	注記
DNS（TCP/UDP）	49152 以上の乱数	DNS サーバー/AD ドメイン コントローラ	いいえ	—
MSRPC	445	ドメイン コントローラ	対応	—
Kerberos（TCP/UDP）	88	ドメイン コントローラ	あり（Kerberos）	MS AD/KDC
LDAP（TCP/UDP）	389	ドメイン コントローラ	対応	—
LDAP（GC）	3268	グローバル カタログ サーバー	対応	—
NTP	123	NTP サーバー/ドメイン コントローラ	いいえ	—
IPC	80	展開内の他の ISE ノード	あり（RBAC クレデンシャルを使用）	—

DNS サーバー

DNS サーバーを設定する場合は、次の処理を実行します。

- Cisco ISE に設定されている DNS サーバーで、使用するドメインのすべての正引きおよび逆引き DNS クエリを解決できるようにする必要があります。
- DNS 再帰によって遅延が発生してパフォーマンスが重大な悪影響を受ける可能性があるので、権威 DNS サーバーで Active Directory レコードを解決することをお勧めします。
- すべての DNS サーバーで、追加サイト情報の有無に関係なく、DC、GC、および KDC の SRV クエリに回答できるようにする必要があります。
- パフォーマンスを向上させるために、SRV 応答にサーバー IP アドレスを追加することを推奨します。
- パブリック インターネットでクエリを実行する DNS サーバーを使用しないでください。不明な名前を解決する必要がある場合に、ネットワークの情報が漏洩する可能性があります。

外部 ID ソースとしての Active Directory の設定

Easy Connect や PassiveID ワーク センターなどの機能を設定する際に、Active Directory を外部 ID ソースとして設定します。これらの機能の詳細については、Easy Connect （83 ページ）と PassiveID ワーク センター （88 ページ）を参照してください。

外部 ID ソースとして Active Directory を設定する前に、次のことを確認します。

- Microsoft Active Directory サーバーがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないこと。
- 参加操作用の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更（Change Password on Next Login）] を使用して設定されていないこと。
- ISE のスーパー管理者またはシステム管理者の権限があること。

（注） Cisco ISE が Active Directory に接続されているときに操作に関する問題がある場合は、**[操作（Operations）] > [レポート（Reports）]** で AD コネクタ操作レポートを参照してください。

外部 ID ソースとして Active Directory を設定するには、次のタスクを実行する必要があります。

1. Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （49 ページ）
2. 認証ドメインの設定 （54 ページ）

3. Active Directory ユーザー グループの設定 （55 ページ）
4. Active Directory ユーザーとマシンの属性の設定 （56 ページ）
5. （オプション） パスワード変更、マシン認証、およびマシン アクセス制限の設定の変更 （57 ページ）

Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加

始める前に

Cisco ISE ノードが、NTP サーバー、DNS サーバー、ドメインコントローラ、グローバルカタログサーバーが配置されているネットワークと通信できることを確認します。ドメイン診断ツールを実行して、これらのパラメータをチェックできます。

Active Directory と、パッシブ ID ワーク センターのエージェント、syslog、SPAN、およびエンドポイントの各プローブを使用するには、参加ポイントを作成する必要があります。

Active Directory と統合する際に IPv6 を使用する場合は、関連する ISE ノードで IPv6 アドレスが設定されていることを確認する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [追加（Add）] をクリックして、[Active Directory 参加ポイント名（Active Directory Join Point Name）] の設定のドメイン名と ID ストア名を入力します。

ステップ 3 [送信（Submit）] をクリックします。

新しく作成された参加ポイントをドメインに参加させるかどうかを確認するポップアップ ウィンドウが表示されます。すぐに参加させる場合は [はい（Yes）] をクリックします。

[いいえ（No）] をクリックした場合、設定を保存すると、Active Directory ドメインの設定が（プライマリおよびセカンダリのポリシー サービス ノードに）グローバルに保存されますが、いずれの Cisco ISE ノードもまだドメインに参加しません。

ステップ 4 作成した新しい Active Directory 参加ポイントの横にあるチェックボックスをオンにして [編集（Edit）] をクリックするか、または左側のナビゲーションペインから新しい Active Directory 参加ポイントをクリックします。展開の参加/脱退テーブルに、すべての Cisco ISE ノード、ノードのロール、およびそのステータスが表示されます。

ステップ 5 参加ポイントがステップ 3 の間にドメインに参加しなかった場合は、関連する Cisco ISE ノードの横にあるチェックボックスをオンにし、[参加（Join）] をクリックして Active Directory ドメインに Cisco ISE ノードを参加させます。

設定を保存した場合も、これを明示的に実行する必要があります。1 回の操作で複数の Cisco ISE ノードをドメインに参加させるには、使用するアカウントのユーザー名とパスワードがすべての参加操作で同じである必要があります。各 Cisco ISE ノードを追加するために異なるユーザー名とパスワードが必要な場合は、Cisco ISE ノードごとに参加操作を個別に実行する必要があります。

ステップ 6 [ドメインへの参加（Join Domain）] ダイアログボックスで Active Directory のユーザー名とパスワードを入力します。

[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメインコントローラ（DC）に使用されます。

参加操作に使用するユーザーは、ドメイン自体に存在する必要があります。ユーザーが異なるドメインまたはサブドメインに存在する場合、ユーザー名は jdoe@acme.com のように、UPN 表記で表記する必要があります。

ステップ 7 （任意）[組織ユニットの指定（Specify Organizational Unit）] 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は、Cisco ISE ノードのマシンアカウントを CN=Computers,DC=someDomain,DC=someTLD 以外の特定の組織ユニットに配置する場合に、オンにする必要があります。Cisco ISE は、指定された組織ユニットの下にマシンアカウントを作成するか、またはマシン アカウントがすでにある場合は、この場所に移動します。組織ユニットが指定されない場合、Cisco ISE はデフォルトの場所を使用します。値は完全識別名（DN）形式で指定する必要があります。構文は、Microsoft のガイドラインに準拠する必要があります。特別な予約文字（/'+,;=<> など）、改行、スペース、およびキャリッジ リターンは、バックスラッシュ（\）によってエスケープする必要があります。たとえば、OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ や Workstations,DC=someDomain,DC=someTLD のようにします。マシン アカウントがすでに作成されている場合、このチェックボックスをオンにする必要はありません。Active Directory ドメインに参加したマシン アカウントのロケーションを後で変更することもできます。

ステップ 8 [OK] をクリックします。

Active Directory ドメインに参加する複数のノードを選択できます。

参加操作に失敗した場合、失敗メッセージが表示されます。各ノードの失敗メッセージをクリックして、そのノードの詳細なログを表示します。

（注） 参加が完了すると、Cisco ISE によりその AD グループと対応するセキュリティ識別子（SID）が更新されます。Cisco ISE は自動的に SID の更新プロセスを開始します。このプロセスを完了できるようにする必要があります。

（注） DNS サービス（SRV）レコードが欠落している（参加しようとしているドメインに対し、ドメインコントローラが SRV レコードをアドバタイズしない）場合は、Active Directory ドメインに Cisco ISE を参加させることができない可能性があります。トラブルシューティング情報については、次の Microsoft Active Directory のマニュアルを参照してください。

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

（注） ISE には最大 200 のドメイン コントローラのみを追加できます。制限を超えると、「エラー発生 <DC FQDN> - DC の数が最大許容数である 200 を超えています（Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200）」というエラーが表示されます。

ドメイン コントローラの追加

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから **[Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣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。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 （注） パッシブ ID サービスの新しいドメイン コントローラ（DC）を追加するには、その DC のログイン クレデンシャルが必要です。

[PassiveID] タブに移動し、[DC の追加（Add DCs）] をクリックします。

ステップ 4 モニター対象として参加ポイントに追加するドメイン コントローラの隣にあるチェックボックスをオンにし、[OK] をクリックします。
ドメイン コントローラが [PassiveID] タブの [ドメイン コントローラ（Domain Controllers）] リストに表示されます。

ステップ 5 ドメイン コントローラを設定します。

a) ドメイン コントローラをオンにし、[編集（Edit）] をクリックします。[アイテムの編集（Edit Item）] 画面が表示されます。
b) 必要に応じて、各種ドメイン コントローラ フィールドを編集します。
c) WMI プロトコルを選択した場合は、[設定（Configure）] をクリックして WMI を自動的に設定するか、または [テスト（Test）] をクリックして接続をテストします。

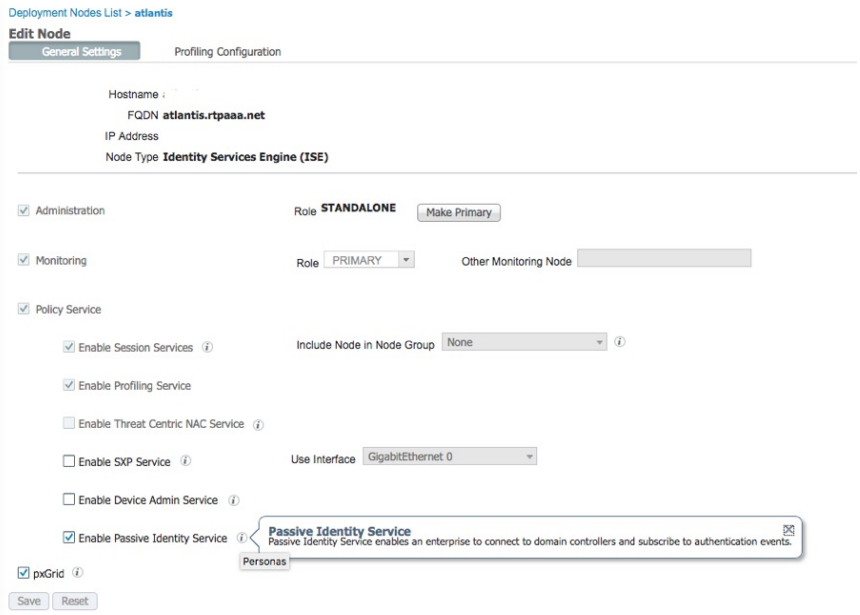
DC フェールオーバー メカニズムは DC 優先順位リストに基づいて管理されます。このリストは、フェールオーバーの発生時に DC が選択される順序を決定します。ある DC がオフラインであるか、何らかのエラーのため到達不能な場合には、優先順位リストにおける優先順位が下がります。DC がオンラインに戻ると、優先順位リストにおけるその優先順位が適宜調整されます（上がります）。

パッシブ ID 用の WMI の設定

始める前に

AD ドメイン設定の変更に必要な Active Directory ドメイン管理者クレデンシャルがあることを確認します。[管理（Administration）] > [システム（System）] > [展開（Deployment）] で、このノードのパッシブ ID が有効になっていることを確認します。

図 *1:*

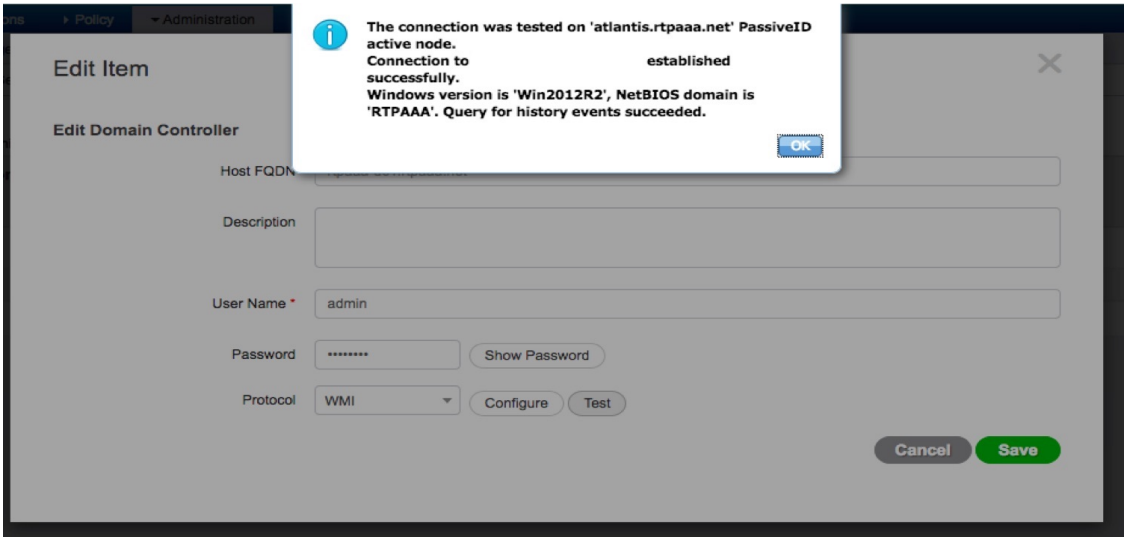


ステップ 1 **[管理（Administration）] > [IDの管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣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。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 [パッシブ ID（Passive ID）] タブに移動し、該当するドメイン コントローラの隣にあるチェックボックスをオンにし、[WMI の設定（Config WMI）] をクリックして、選択したドメイン コントローラが ISE により自動的に設定されるようにします。

図 *2 :*



Active Directory とドメイン コントローラを手動で設定する場合、または設定の問題のトラブルシューティングを行う場合は、Active Directory と Cisco ISE の統合の前提条件 （45 ページ）を参照してください。

図 *3 :*

（注） エージェントが Windows システムで正確な DC の詳細を取得できない場合は、DC と Cisco ISE 間の通信を再確立する必要があります。再確立するには、Cisco ISE IP アドレスと Cisco ISE FQDN（たとえば、Cisco ISE IP アドレス：https://10.0.0.0/ および Cisco ISE FQDN：https://ise1.cisco.com/）を Windows システム（**[このPC（This PC）]** > **[ローカルディスク（C:）（Local Disk (C:)）]** > **[Windows]** > **[System32]** > **[drivers]** > **[etc]**）の *hosts* ファイルに追加します。

Active Directory ドメインの脱退

この Active Directory ドメインまたはこの参加ポイントからユーザーとマシンを認証する必要がない場合は、Active Directory ドメインを脱退できます。

コマンドライン インターフェイスから Cisco ISE アプリケーション設定をリセットする場合、またはバックアップやアップグレードの後に設定を復元する場合、脱退操作が実行され、Cisco ISE ノードがすでに参加している場合は、Active Directory ドメインから切断されます。ただし、Cisco ISE ノードのアカウントは、Active Directory ドメインから削除されません。脱退操作では Active Directory ドメインからノード アカウントも削除されるため、脱退操作は管理者ポータルから Active Directory クレデンシャルを使用して実行することを推奨します。これは、Cisco ISE ホスト名を変更する場合にも推奨されます。

始める前に

Active Directory ドメインを脱退したが、認証の ID ソースとして（直接または ID ソース順序の一部として）Active Directory を使用している場合、認証が失敗する可能性があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣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。展開の参加/脱退テーブルが、すべての Cisco ISE ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 Cisco ISE ノードの隣にあるチェックボックスをオンにして [脱退（Leave）] をクリックします。

ステップ 4 Active Directory のユーザー名とパスワードを入力し、[OK] をクリックしてドメインを脱退し、Cisco ISE データベースからマシン アカウントを削除します。

Active Directory クレデンシャルを入力すると、Cisco ISE ノードは Active Directory ドメインを脱退し、Active Directory データベースから Cisco ISE マシン アカウントが削除されます。

（注） Active Directory データベースから Cisco ISE マシン アカウントを削除するには、ここに入力する Active Directory クレデンシャルに、ドメインからマシン アカウントを削除する権限がなければなりません。

ステップ 5 Active Directory クレデンシャルがない場合は、[使用可能なクレデンシャルなし（No Credentials Available）] チェックボックスをオンにして、[OK] をクリックします。

[クレデンシャルなしでドメインを脱退（Leave domain without credentials）] チェックボックスをオンにすると、プライマリ Cisco ISE ノードが Active Directory ドメインから脱退します。参加時に Active Directory で作成されたマシン アカウントは、Active Directory 管理者が手動で削除する必要があります。

認証ドメインの設定

Cisco ISE が参加しているドメインは、信頼関係を持つ他のドメインに対して可視性があります。デフォルトでは、Cisco ISE はこれらすべての信頼ドメインに対する認証を許可するように設定されます。認証ドメインのサブセットに対して、Active Directory 展開との相互作用を制限できます。ドメイン認証を設定することにより、接続ポイントごとに特定のドメインを選択して、選択されたドメインに対してのみ認証が実行されるようにできます。認証ドメインでは、接続ポイントから信頼されたすべてのドメインではなく、選択されたドメインのユーザーのみを認証するように Cisco ISE に指示するため、セキュリティが向上します。また、認証ドメインでは検索範囲（着信したユーザー名または ID に一致するアカウントの検索）が制限されるため、認証要求処理のパフォーマンスと遅延が改善されます。このことは、着信したユーザー名または ID にドメイン マークアップ（プレフィクスまたはサフィックス）が含まれていない場合に特に重要です。これらの理由から、認証ドメインを設定することをベスト プラクティスとして強く推奨します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 **Active Directory** の参加ポイントをクリックします。

ステップ 3 [認証ドメイン（Authentication Domains）] タブをクリックします。

表に、信頼ドメインのリストが表示されます。デフォルトでは、Cisco ISE はすべての信頼ドメインに対する認証を許可します。

ステップ 4 指定したドメインのみを許可するには、[認証にすべての Active Directory ドメインを使用する（Use all Active Directory domains for authentication）] チェックボックスをオフにします。

ステップ 5 認証を許可するドメインの隣にあるチェックボックスをオンにし、[選択対象の有効化（Enable Selected）] をクリックします。[認証（Authenticate）] カラムで、このドメインのステータスが [はい（Yes）] に変わります。

また、選択したドメインを無効にすることもできます。

ステップ 6 [使用できないドメインを表示（Show Unusable Domains）] をクリックして、使用できないドメインのリストを表示します。使用できないドメインは、単方向の信頼や選択的な認証などの理由により、Cisco ISE が認証に使用できないドメインです。

次のタスク

Active Directory ユーザー グループを設定します。

Active Directory ユーザー グループの設定

Active Directory ユーザー グループを許可ポリシーで使用できるように設定する必要があります。内部的には、Cisco ISE はグループ名のあいまいさの問題を解決し、グループ マッピングを向上させるためにセキュリティ ID（SID）を使用します。SID により、グループ割り当てが正確に一致します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [グループ（Groups）] タブをクリックします。

ステップ 3 次のいずれかを実行します。

a) **[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）]** を選択して、既存のグループを選択します。

b) **[追加（Add）] > [グループの追加（Add Group）]** を選択して、グループを手動で追加します。グループ名と SID の両方を指定するか、またはグループ名のみを指定し、[SID を取得（Fetch SID）] を押します。

ユーザー インターフェイス ログインのグループ名に二重引用符（"）を使用しないでください。

ステップ 4 グループを手動で選択する場合は、フィルタを使用してグループを検索できます。たとえば、**admin*** をフィルタ基準として入力し、[グループの取得（Retrieve Groups）] をクリックすると、admin で始まるユーザー グループが表示されます。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。一度に取得できるのは 500 グループのみです。

ステップ 5 許可ポリシーで使用可能にするグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 グループを手動で追加する場合は、新しいグループの名前と SID を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

（注） グループを削除し、そのグループと同じ名前で新しいグループを作成する場合は、[SID 値の更新（Update SID Values）] をクリックして、新しく作成したグループに新しい SID を割り当てる必要があります。アップグレードすると、最初の参加の後に SID が自動的に更新されます。

次のタスク

Active Directory のユーザー属性を設定します。

Active Directory ユーザーとマシンの属性の設定

許可ポリシーの条件で使用できるように Active Directory ユーザーとマシンの属性を設定する必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] >** [Active Directory] を選択します。

ステップ 2 [属性（Attributes）] タブをクリックします。

ステップ 3 **[追加（Add）] > [属性の追加（Add Attribute）]** を選択して属性を手動で追加するか、**[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）]** を選択してディレクトリから属性のリストを選択します。

Cisco ISE では、属性タイプ IP を手動で追加するときに、ユーザー認証に IPv4 または IPv6 アドレスを使用して AD を設定できます。

ステップ 4 ディレクトリからの属性の追加を選択した場合、ユーザーの名前を [サンプル ユーザー（Sample User）] フィールドまたは [マシン アカウント（Machine Account）] フィールドに入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザーの属性のリストを取得します。たとえば、管理者属性のリストを取得するには **administrator** を入力します。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。

（注） ユーザー名の例を入力する場合、Cisco ISE が接続されているアクティブな Active Directory ドメインからユーザーを選択します。マシン属性を取得するマシンの例を選択する場合、マシン名のプレフィックスとして「host/」を追加するか、SAM$ 形式を使用してください。たとえば、host/myhost を使用します。属性の取得時に表示される値の例は説明のみを目的としており、保存されません。

ステップ 5 選択する Active Directory の属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 属性を手動で追加する場合は、新しい属性の名前を入力します。

ステップ 7 [保存（Save）] をクリックします。

パスワード変更、マシン認証、およびマシン アクセス制限の設定の変更

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。詳細については、Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （49 ページ）を参照してください。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 該当する Cisco ISE ノードの隣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。

ステップ 3 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 4 必要に応じて、パスワード変更、マシン認証、およびマシンアクセス制限（MAR）の設定を変更します。

ステップ 5 [ダイヤルイン チェックを有効にする（Enable dial-in check）] チェックボックスをオンにして、認証中またはクエリ中にユーザーのダイヤルインアクセス権をチェックします。ダイヤルインアクセス権が拒否されている場合は、チェックの結果により認証拒否の原因になります。

ステップ 6 認証中またはクエリ中にサーバーからユーザーにコールバックするようにするには、[ダイヤルインクライアントのコールバック チェックを有効にする（Enable callback check for dial-in clients）] チェックボックスをオンにします。サーバーによって使用される IP アドレスまたは電話番号は、発信者またはネットワーク管理者によって設定されます。チェックの結果は、RADIUS 応答でデバイスに返されます。

ステップ 7 プレーン テキスト認証に Kerberos を使用する場合は、[プレーン テキスト認証に Kerberos を使用（Use Kerberos for Plain Text Authentications）] チェックボックスをオンにします。デフォルトの推奨オプションは MS-RPC です。

マシンアクセス制限キャッシュ

アプリケーションサービスを手動で停止すると、Cisco ISE はマシンアクセス制限（MAR）キャッシュコンテンツ、calling-station-ID リスト、および対応するタイムスタンプをローカルディスクのファイルに保存します。アプリケーションサービスを誤って再起動した場合、Cisco ISE はインスタンスの MAR キャッシュ エントリを保存しません。アプリケーション サービスが再起動すると、Cisco ISE はキャッシュエントリの存続時間に基づいて、ローカルディスクのファイルから MAR キャッシュエントリを読み取ります。再起動後にアプリケーションサービスが起動すると、Cisco ISE はそのインスタンスの現在の時刻と MAR キャッシュエントリの時刻を比較します。現在の時刻と MAR エントリの時刻の差が MAR キャッシュ エントリの存続時間よりも大きい場合は、Cisco ISE はディスクからそのエントリを取得しません。それ以外の場合、Cisco ISE は MAR キャッシュ エントリを取得し、MAR キャッシュ エントリ存続時間を更新します。

MAR キャッシュを設定するには、次の手順を実行します。

外部 ID に ソースで定義されている Active Directory の [詳細設定（Advanced Settings）] タブで、次のオプションがオンになっていることを確認します。

- [マシン認証の有効化（Enable Machine Authentication）]：マシン認証を有効にします。
- [マシンアクセス制限の有効化（Enable Machine Access Restriction）]：承認前にユーザーとマシン認証を組み合わせます。

認証で MAR キャッシュを使用するには、次の手順を実行します。

認証ポリシーで `WasMachineAuthenticated is True` を使用します。このルールとクレデンシャルルールを使用すると、デュアル認証を行うことができます。マシン認証は、AD クレデンシャルの前に実行する必要があります。

[システム（System）] > [展開（Deployment）] ページでノードグループを作成した場合は、MAR のキャッシュ配布を有効にします。MAR のキャッシュ配布は、同じノードグループ内のすべての PSN に MAR キャッシュを複製します。

詳細については、次の Cisco ISE コミュニティのページを参照してください。

- https://community.cisco.com/t5/policy-and-access/mar-why-is-it-useful/td-p/3213527
- https://community.cisco.com/t5/policy-and-access/ise-2-1-mar-aging-time-eap-tls/td-p/3209628

関連トピック

外部 ID ソースとしての Active Directory の設定 （48 ページ）

カスタム スキーマの設定

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 参加ポイントを選択します。

ステップ 3 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 4 [スキーマ（Schema）]セクションの[スキーマ（Schema）] ドロップダウンリストから[カスタム（Custom）] オプションを選択します。必要に応じて、ユーザー情報の属性を更新できます。これらの属性は、ユーザー情報（名、姓、電子メール、電話番号、地域など）の収集に使用されます。

事前設定された属性は、Active Directory スキーマ（組み込みのスキーマ）に使用されます。事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。

Active Directory の複数参加設定のサポート

Cisco ISE では、Active Directory ドメインへの複数参加がサポートされます。Cisco ISE では、50 までの Active Directory 参加がサポートされます。Cisco ISE は、双方向信頼がなく、相互の信頼がゼロである複数の Active Directory ドメインと接続できます。Active Directory の複数ドメイン参加は、各参加の独自のグループ、属性、および許可ポリシーを持つ個別の Active Directory ドメインのセットで構成されます。

同じフォレストに複数回参加できます。つまり、必要に応じて、同じフォレスト内の複数のドメインに参加できます。

Cisco ISE は、単方向の信頼があるドメインに参加できます。このオプションで、単方向の信頼によって生じる権限の問題を回避できます。いずれかの信頼ドメインに参加できるため、両方のドメインを確認できます。

- [参加ポイント（Join Point）]：Cisco ISE では、Active Directory ドメインへの個別参加は、参加ポイントと呼ばれます。Active Directory の参加ポイントは、Cisco ISE の ID ストアであり、認証ポリシーで使用できます。属性およびグループの関連ディクショナリがあり、許可条件で使用できます。

- [スコープ（Scope）]：グループ化された Active Directory の参加ポイントのサブセットは、スコープと呼ばれます。単一参加ポイントの代わりに、認証結果として認証ポリシーでスコープを使用できます。スコープは、複数の参加ポイントに対してユーザーを認証するために使用されます。各参加ポイントに複数のルールを使用する代わりにスコープを使用すると、単一のルールで同じポリシーを作成することができ、Cisco ISE で要求の処理やパフォーマンスの向上にかかる時間を短縮できます。参加ポイントには、複数のスコープが含まれる場合があります。スコープは、ID ソース順序に含まれる場合があります。スコープには関連するディクショナリがないため、許可ポリシー条件にスコープを使用することはできません。

  新しい Cisco ISE のインストールを実行する場合、デフォルトでスコープは存在しません。これは、ノー スコープ モードと呼ばれます。スコープを追加すると、Cisco ISE はマルチスコープモードになります。必要に応じて、ノースコープモードに戻すことができます。すべての参加ポイントは [Active Directory] フォルダに移動されます。

  - Initial_Scope は、ノー スコープ モードで追加された Active Directory 参加ポイントの格納に使用される暗黙のスコープです。マルチスコープモードを有効にすると、すべての Active Directory 参加ポイントが自動作成された Initial_Scope に移動します。Initial_Scope の名前を変更できます。

  - All_AD_Instances は組み込み型の疑似スコープで、Active Directory 設定には表示されません。これは、認証結果としてポリシーおよび ID 順序にのみ示されます。Cisco ISE で設定されたすべての Active Directory 参加ポイントを選択する場合は、このスコープを選択できます。

Active Directory 参加ポイントを追加する新しいスコープの作成

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [スコープモード（Scope Mode）] をクリックします。
Initial_Scope と呼ばれるデフォルトのスコープが作成され、現在のすべての参加ポイントがこのスコープに配置されます。

ステップ 3 より多くのスコープを作成するには、[追加（Add）] をクリックします。

ステップ 4 新しいスコープの名前と説明を入力します。

ステップ 5 **[送信（Submit）]** をクリックします。

ID 書き換え

ID 書き換えは、外部 Active Directory システムに渡される前に ID を操作するよう Cisco ISE に指示する拡張機能です。ID を必要な形式（任意のドメイン プレフィクスやサフィックスまたはその他の追加マークアップを含むまたは除く）に変更するためのルールを作成できます。

ID 書き換えルールは、サブジェクト検索、認証クエリー、許可クエリーなどの操作のために、クライアントから受信したユーザー名またはホスト名に対して Active Directory に渡される前に適用されます。Cisco ISE は条件のトークンを照合し、最初の 1 つが一致するとポリシーの処理を停止して、結果に応じて ID 文字列を書き換えます。

書き換え時、角カッコ [ ] で囲まれている（[IDENTITY] など）内容はすべて、評価側では評価されず、代わりに文字列内のその場所に一致する文字列が付加される変数です。角カッコなしはすべて、ルールの評価側と書き換え側の両方で、固定文字列として評価されます。

次に、ユーザーによって入力された ID が ACME\jdoe であるとした場合の ID 書き換えの例を示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**[IDENTITY]** に書き換えます。

  結果は jdoe です。このルールは、ACME プレフィクスを持つすべてのユーザー名を削除するよう Cisco ISE に指示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**[IDENTITY]@ACME.com** に書き換えます。

  結果は jdoe@ACME.com です。このルールは、形式をプレフィクス表記からサフィックス表記に、または NetBIOS 形式から UPN 形式に変更するよう Cisco ISE に指示します。

- ID が **ACME\[IDENTITY]** と一致する場合、**ACME2\[IDENTITY]** に書き換えます。

  結果は ACME2\jdoe です。このルールは、特定のプレフィクスを持つすべてのユーザー名を代替プレフィクスに変更するよう Cisco ISE に指示します。

- ID が **[ACME]\jdoe.USA** と一致する場合、**[IDENTITY]@[ACME].com** に書き換えます。

結果は jdoe\ACME.com です。このルールは、ドットの後の領域を削除するよう Cisco ISE に指示します。この場合は国名で、正しいドメインに置き換えられます。

- ID が **E=[IDENTITY]** と一致する場合、**[IDENTITY]** に書き換えます。

  結果は jdoe です。これは、ID が証明書から取得され、フィールドが電子メール アドレスで、Active Directory がサブジェクトで検索するように設定されている場合に作成可能なルールの例です。このルールは、「E=」を削除するように Cisco ISE に指示します。

- ID が **E=[EMAIL],[DN]** と一致する場合、**[DN]** に書き換えます。

  このルールは、証明書サブジェクトを、E=jdoe@acme.com、CN=jdoe、DC=acme、DC=com から単なる DN、CN=jdoe、DC=acme、DC=com に変換します。これは、ID が証明書サブジェクトから取得され、Active Directory が DN でユーザー検索するように設定されている場合に作成可能なルールの例です。このルールは、電子メール プレフィクスを削除し、DN を生成するよう Cisco ISE に指示します。

次に、ID 書き換えルールを記述する際によくある間違いを示します。

- ID が **[DOMAIN]\[IDENTITY]** と一致する場合、**[IDENTITY]@DOMAIN.com** に書き換えます。

  結果は jdoe@DOMAIN.com です。このルールは、ルールの書き換え側の角カッコ [ ] に [DOMAIN] がありません。

- ID が **DOMAIN\[IDENTITY]** と一致する場合、**[IDENTITY]@[DOMAIN].com** に書き換えます。

  この場合も、結果は jdoe@DOMAIN.com です。このルールは、ルールの評価側の角カッコ [ ] に [DOMAIN] がありません。

ID 書き換えルールは、常に、Active Directory 参加ポイントのコンテキスト内で適用されます。認証ポリシーの結果としてスコープが選択されている場合でも、書き換えルールは、各 Active Directory 参加ポイントに適用されます。EAP-TLS が使用されている場合、これらの書き換えルールは、証明書から取得される ID にも適用されます。

ID 書き換えの有効化

（注） この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE を参加させる必要があります。

ステップ 1 **[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[Active Directory]** を選択します。

ステップ 2 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 3 [ID 書き換え（Identity Rewrite）] セクションで、ユーザー名を変更する書き換えルールを適用するかどうかを選択します。

ステップ 4 一致条件および書き換え結果を入力します。表示されるデフォルトルールを削除し、要件に応じてルールを入力できます。Cisco ISE は順番にポリシーを処理し、要求ユーザー名に一致する最初の条件が適用されます。一致トークン（角カッコ内に含まれるテキスト）を使用して、元のユーザー名の要素を結果に転送できます。いずれのルールにも一致しない場合、識別名は変更されません。[テスト開始（Launch Test）] ボタンをクリックして、書き換え処理をプレビューできます。

ID 解決の設定

一部のタイプの ID には、プレフィクスまたはサフィックスのようなドメイン マークアップが含まれます。たとえば、ACME\jdoe などの NetBIOS ID では、「ACME」がドメイン マークアップのプレフィクスで、同様に jdoe@acme.com などの UPN ID では、「acme.com」がドメイン マークアップのサフィックスです。ドメイン プレフィクスは、組織内の Active Directory ドメインの NetBIOS（NTLM）名に一致し、ドメイン サフィックスは、組織内の Active Directory ドメインの DNS 名または代替 UPN サフィックスに一致する必要があります。たとえば、gmail.com は Active Directory ドメインの DNS 名ではないため、jdoe@gmail.com はドメイン マークアップなしとして処理されます。

ID 解決設定では、Active Directory 展開に一致するように、セキュリティおよびパフォーマンスのバランスを調整する重要な設定を指定できます。これらの設定を使用して、ドメインマークアップのないユーザー名およびホスト名の認証を調整できます。Cisco ISE でユーザーのドメインを認識できない場合、すべての認証ドメインでユーザーを検索するように設定できます。ユーザーが 1 つのドメインで見つかった場合でも、Cisco ISE は ID のあいまいさがないことを確実にするために、すべての応答を待ちます。この処理は、ドメインの数、ネットワークの遅延、負荷などに応じて、時間がかかる場合があります。

ID 解決問題の回避

認証時に、ユーザーおよびホストに完全修飾名（つまり、ドメインマークアップが含まれている名前）を使用することを強く推奨します。たとえば、ユーザーの UPN と NetBIOS 名、およびホストの FQDN SPN です。これは、複数の Active Directory アカウントが受信ユーザー名と一致する（たとえば、jdoe が jdoe@emea.acme.com および jdoe@amer.acme.com と一致する）など、あいまいエラーが頻繁に生じる場合に特に重要です。場合によっては、完全修飾名を使用することが、問題を解決する唯一の方法になります。また、ユーザーに一意のパスワードが設定されていることを保証するだけで十分な場合もあります。したがって、一意の ID を最初から使用すると、効率が向上し、パスワード ロックアウトの問題が減少します。

ID 解決の設定

（注） この設定タスクは任意です。あいまいな識別エラーなどのさまざまな理由で発生する認証失敗を減らすために実行できます。

始める前に

Active Directory ドメインに Cisco ISE ノードを参加させる必要があります。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [高度な設定（Advanced Settings）] タブをクリックします。

ステップ 3 [ID 解決（Identity Resolution）] セクションで、ユーザー名またはマシン名の ID 解決についての次の設定を定義します。この設定によって、ユーザーの検索と認証を詳細に制御できます。

最初に、マークアップなしの ID に対する設定を行います。このような場合、次のオプションのいずれかを選択できます。

- [要求を拒否する（Reject the request）]：このオプションを使用すると、SAM 名などのドメインマークアップがないユーザーの認証は失敗します。このことは、複数参加ドメインで、Cisco ISE がすべての参加グローバル カタログの ID を検索する必要があることによって、安全性が低下する可能性がある場合に役立ちます。このオプションによって、ドメイン マークアップを含むユーザー名を使用することがユーザーに対して強制されます。
- [結合されたフォレストの「認証ドメイン」のみで検索する（Only search in the “Authentication Domains” from the joined forest）]：このオプションを使用すると、認証ドメインのセクションで指定した、結合ポイントのフォレスト内のドメイン内のみで ID が検索されます。これはデフォルト オプションであり、SAM アカウント名に対する Cisco ISE 1.2 の動作と同じです。
- [すべての「認証ドメイン」セクションで検索する（Search in all the “Authentication Domains” sections）]：このオプションを使用すると、すべての信頼できるフォレストのすべての認証ドメイン内で ID が検索されます。これにより、遅延が増加し、パフォーマンスに影響する可能性があります。

Cisco ISE で認証ドメインがどのように設定されているかに基づいて選択します。特定の認証ドメインのみを選択した場合は、それらのドメインのみが検索されます（「結合されたフォレスト」と「すべてのフォレスト」のいずれを選択した場合も）。

2 番目の設定は、Cisco ISE が、[認証ドメイン（Authentication Domains）] セクションで指定された設定に準拠するために必要となるすべてのグローバル カタログ（GC）と通信できない場合に使用します。このような場合、次のオプションのいずれかを選択できます。

- [使用可能なドメインで続行する（Proceed with available domains）]：このオプションを使用すると、使用可能ないずれかのドメインで一致が見つかった場合に認証が続行されます。

- [要求をドロップする（Drop the request）]：このオプションを使用すると、ID 解決で到達不能または使用できないドメインが検出された場合に認証要求がドロップされます。

Active Directory 認証のためのユーザーのテスト

Active Directory からユーザー認証を検証するには、[ユーザーのテスト（Test User）] ツールを使用できます。グループおよび属性を取得して調査することもできます。単一の参加ポイントまたはスコープのテストを実行できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- すべての参加ポイントのテストを実行するには、**[拡張ツール（Advanced Tools）] > [すべての参加ポイントのユーザーをテスト（Test User for All Join Points）]** を選択します。
- 特定の参加ポイントのテストを実行するには、参加ポイントを選択し、[編集（Edit）] をクリックします。Cisco ISE ノードを選択し、[ユーザーのテスト（Test User）] をクリックします。

ステップ 3 Active Directory のユーザー（またはホスト）のユーザー名とパスワードを入力します。

ステップ 4 認証タイプを選択します。ステップ 3 のパスワード入力は、ルックアップ オプションを選択する場合には必要ありません。

ステップ 5 すべての参加ポイントに対してこのテストを実行する場合は、このテストを実行する Cisco ISE ノードを選択します。

ステップ 6 Active Directory からグループおよび属性を取得するには、[グループを取得（Retrieve Groups）] および [属性の取得（Retrieve Attributes）] チェック ボックスをオンにします。

ステップ 7 [テスト（Test）] をクリックします。
テスト操作の結果と手順が表示されます。手順で失敗の原因を特定し、トラブルシューティングできます。

また、Active Directory がそれぞれの処理手順（認証、参照、グループおよび属性の取得）を実行するのに要する時間（ミリ秒単位）を表示することもできます。操作にかかる時間がしきい値を超えると、Cisco ISE に警告メッセージが表示されます。

Active Directory の設定の削除

Active Directory を外部 ID ソースとして使用しない場合は、Active Directory の設定を削除する必要があります。別の Active Directory ドメインに参加する場合は、設定を削除しないでください。現在参加しているドメインから脱退し、新しいドメインに参加できます。

始める前に

Active Directory ドメインが残っていることを確認します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 設定された Active Directory の横のチェックボックスをオンにします。

ステップ 3 [ローカル ノード ステータス（Local Node Status）] が [参加していない（Not Joined）] としてリストされていることを確認します。

ステップ 4 [削除（Delete）] をクリックします。

Active Directory データベースから設定を削除しました。後で Active Directory を使用する場合は、有効な Active Directory の設定を再送信できます。

ノードの Active Directory の参加の表示

特定の Cisco ISE ノードのすべての Active Directory 参加ポイントのステータスまたはすべての Cisco ISE ノードのすべての参加ポイントのリストを表示するには、[Active Directory] ページの [ノード ビュー（Node View）] ボタンを使用できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [ノード ビュー（Node View）] をクリックします。

ステップ 3 [ISE Node（ISE ノード）] ドロップダウン リストからノードを選択します。
テーブルに、Active Directory のステータスがノード別に一覧されます。展開に複数の参加ポイントと複数の Cisco ISE ノードがある場合、このテーブルが更新されるまでに数分かかる場合があります。

ステップ 4 その Active Directory 参加ポイントのページに移動し、その他の特定のアクションを実行するには、参加ポイントの [名前（Name）] リンクをクリックします。

ステップ 5 [診断ツール（Diagnostic Tools）] ページに移動して特定の問題のトラブルシューティングを行うには、[診断概要（Diagnostic Summary）] 列のリンクをクリックします。診断ツールでは、ノードごとに各参加ポイントの最新の診断結果が表示されます。

Active Directory の問題の診断

診断ツールは、各 Cisco ISE ノードで実行されるサービスです。診断ツールを使用して、Active Directory 展開を自動的にテストおよび診断したり、Cisco ISE によって Active Directory が使用される場合に機能やパフォーマンスの障害の原因となる可能性がある問題を検出するための一連のテストを実行したりすることができます。

Cisco ISE が Active Directory に参加できない、または Active Directory に対して認証できない理由は、複数あります。このツールは、Cisco ISE を Active Directory に接続するための前提条件が正しく設定されていることを確認するのに役立ちます。また、ネットワーク、ファイアウォール設定、クロック同期、ユーザー認証などの問題の検出に役立ちます。このツールは、手順を

ステップごとに説明したガイドとして機能し、必要に応じて、中間の各レイヤの問題の修正を支援します。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。

ステップ 2 [拡張ツール（Advanced Tools）] ドロップダウン リストをクリックし、[診断ツール（Diagnostic Tools）] を選択します。

ステップ 3 診断を実行する Cisco ISE ノードを選択します。

Cisco ISE ノードを選択しない場合は、すべてのノードでテストが実行されます。

ステップ 4 特定の Active Directory 参加ポイントを選択します。

Active Directory 参加ポイントを選択しない場合は、すべての参加ポイントでテストが実行されます。

ステップ 5 オンデマンドで、またはスケジュールに基づいて診断テストを実行できます。

- テストをすぐに実行するには、[テストを今すぐ実行（Run Tests Now）] を選択します。
- スケジュールした間隔でテストを実行するには、[スケジュールしたテストを実行する（Run Scheduled Tests）] チェックボックスをオンにし、開始時刻とテストの実行間隔（時、日、週単位）を指定します。このオプションを有効にすると、すべての診断テストがすべてのノードとインスタンスに対して実行され、[ホーム（Home）] ダッシュボードの [アラーム（Alarms）] ダッシュレットに障害が報告されます。

ステップ 6 警告ステータスまたは失敗ステータスのテストの詳細を確認するには、[テストの詳細の表示（View Test Details）] をクリックします。
このテーブルを使用して、特定のテストの再実行、実行中のテストの停止、特定のテストのレポートの表示を行うことができます。

Active Directory デバッグ ログの有効化

Active Directory デバッグ ログはデフォルトでは記録されません。展開でポリシー サービス ペルソナを担当する Cisco ISE ノードでこのオプションを有効にする必要があります。Active Directory のデバッグ ログを有効にすると、ISE のパフォーマンスに影響する場合があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログの設定（Debug Log Configuration）]** を選択します。

ステップ 2 Active Directory のデバッグ情報を取得する Cisco ISE ポリシー サービス ノードの隣のオプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 3 [Active Directory] オプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 4 [Active Directory] の隣にあるドロップダウン リストから [DEBUG] を選択します。これにはエラー、警告、および verbose ログが含まれます。完全なログを取得するには、[TRACE] を選択します。

ステップ 5 [保存（Save）] をクリックします。

トラブルシューティング用の Active Directory ログ ファイルの入手

可能性がある問題をトラブルシューティングするには、Active Directory のデバッグ ログをダウンロードし、表示します。

始める前に

Active Directory のデバッグ ロギングを有効にする必要があります。

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [ログのダウンロード（Download Logs）]** を選択します。

ステップ 2 Active Directory のデバッグ ログ ファイルを取得するノードをクリックします。

ステップ 3 [デバッグ ログ（Debug Logs）] タブをクリックします。

ステップ 4 このページを下にスクロールして ad_agent.log ファイルを見つけます。このファイルをクリックしてダウンロードします。

Active Directory のアラームおよびレポート

Cisco ISE は、Active Directory に関連するアクティビティをモニターリングし、トラブルシューティングを実行するためのさまざまなアラームおよびレポートを提供します。

アラーム

Active Directory のエラーおよび問題に対して、次のアラームがトリガーされます。

- 構成済みネーム サーバーが使用不可（Configured nameserver not available）
- 参加しているドメインが使用不可（Joined domain is unavailable）
- 認証ドメインが使用不可（Authentication domain is unavailable）
- Active Directory フォレストが使用不可（Active Directory forest is unavailable）
- AD コネクタを再起動する必要があります（AD Connector had to be restarted）
- AD：ISE アカウント パスワードの更新に失敗（AD: ISE account password update failed）
- AD：マシン TGT のリフレッシュに失敗（AD: Machine TGT refresh failed）

レポート

次の 2 つのレポートで Active Directory に関連するアクティビティをモニターリングできます。

- RADIUS 認証レポート：このレポートには、Active Directory の認証と許可の詳細な手順が表示されます。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] > [RADIUS 認証（RADIUS Authentications）]** にあります。
- AD コネクタ操作レポート：AD コネクタ操作レポートには、AD コネクタが実行するバックグラウンド操作（Cisco ISE サーバーパスワードの更新、ケルベロスチケットの管理、DNS クエリ、DC 検出、LDAP、および RPC 接続管理など）のログが表示されます。Active Directory の障害が発生した場合は、考えられる原因を特定するために、このレポートで詳細を確認できます。このレポートは、**[操作（Operations）] > [レポート（Reports）] > [診断（Diagnostics）] > [AD コネクタ操作（AD Connector Operations）]** にあります。

Active Directory の高度な調整

高度な調整機能により、シスコのサポート担当者の管理下で、サポート操作に使用されるノード固有の設定が可能となり、システムのさらに深いレベルでパラメータを調整できるようになります。これらの設定は、通常の管理フローを対象としていません。ガイダンスに従って使用する必要があります。

Active Directory アイデンティティ検索属性

Cisco ISE は、SAM と CN のいずれか、または両方の属性を使用してユーザーを識別します。Cisco ISE リリース 2.2 パッチ 5 以降、および 2.3 パッチ 2 以降は、sAMAccountName 属性をデフォルトの属性として使用します。これ以前のリリースでは、SAM と CN の両方の属性がデフォルトで検索されていました。この動作はリリース 2.2 パッチ 5 以降と 2.3 パッチ 2 以降で、CSCvf21978 バグ修正の一部として変更されました。これらのリリースでは、sAMAccountName 属性のみがデフォルトの属性として使用されます。

実際の環境で必要に応じて、SAM と CN のいずれか、または両方を使用するように Cisco ISE を設定できます。SAM および CN が使用される場合、SAMAccountName 属性の値が一意でないと、Cisco ISE は CN 属性値も比較します。

（注） デフォルトでは、Cisco ISE 2.4 の ID 検索の動作は SAM アカウント名のみを検索するように変更されました。このデフォルトの動作を変更するには、「Active Directory アイデンティティ検索の属性の設定」のセクションで説明しているように「IdentityLookupField」フラグの値を変更します。

Active Directory アイデンティティ検索の属性の設定

1. **[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory]** を選択します。
2. [Active Directory] ウィンドウで、[拡張ツール（Advanced Tools）] をクリックし、[高度な調整（Advanced Tuning）] を選択します。次の詳細を入力します。

- [ISE ノード（ISE Node）]：Active Directory に接続される ISE ノードを選択します。
- [名前（Name）]：変更するレジストリキーを入力します。Active Directory 検索属性を変更するには、
  `REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`
  と入力します。
- [値（Value）]：ユーザーを識別するために ISE で使用する属性を入力します。
  - SAM：クエリで SAM のみを使用します（このオプションがデフォルトです）。
  - CN：クエリで CN のみを使用します。
  - SAMCN：クエリで CN と SAM を使用します。
- [コメント（Comment）]：変更内容を記述します（「デフォルト動作を SAM および CN に変更」など）。

3. [値の更新（Update Value）] をクリックしてレジストリを更新します。

   ポップアップウィンドウが表示されます。メッセージを読み取り、変更を受け入れます。ISE の AD コネクタサービスが再起動します。

検索文字列の例

次の例では、ユーザー名が *userd2only* であると想定します。

- SAM 検索文字列：

  ```
  filter=[(&(|(objectCategory=person)(objectCategory=computer))(|(cn=userd2only)(sAMAccountName=userd2only)))]
  ```

- SAM および CN 検索文字列：

  ```
  filter=[(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=userd2only))]
  ```

Active Directory が構成された Cisco ISE をセットアップするための補足情報

Active Directory が構成された Cisco ISE を設定するには、グループ ポリシーを設定し、マシン認証のサプリカントを設定する必要があります。

Active Directory のグループ ポリシーの設定

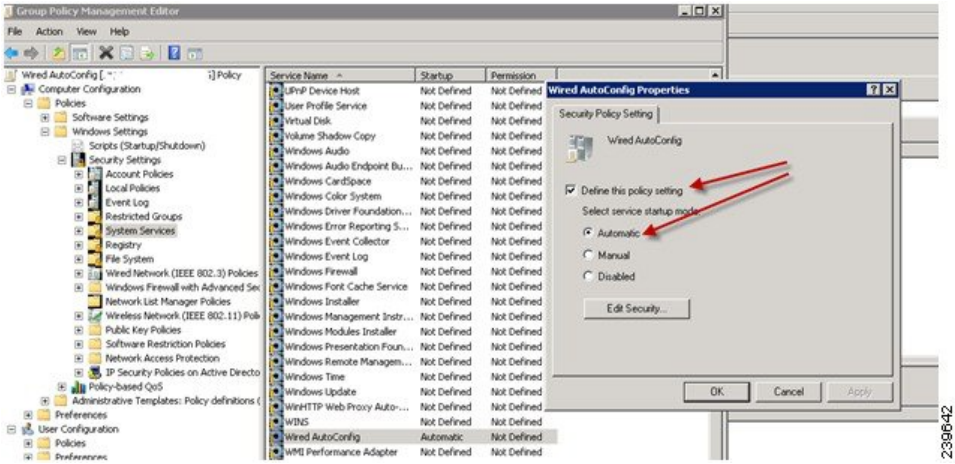
グループ ポリシー管理エディタにアクセスする方法の詳細については、Microsoft Active Directory のマニュアルを参照してください。

ステップ 1 次の図に示すように、グループ ポリシー管理エディタを開きます。

ステップ 2 新しいポリシーを作成し、その説明的な名前を入力するか、既存のドメイン ポリシーに追加します。

次の例では、ポリシー名に Wired Autoconfiguration を使用しています。

ステップ 3 次の図に示すように、[このポリシー設定を定義する（Define this policy setting）] チェックボックスをオンにして、サービス起動モードの [自動（Automatic）] オプション ボタンをクリックします。



ステップ 4 目的の組織ユニットまたはドメイン Active Directory レベルでポリシーを適用します。

Active Directory に対する EAP-TLS マシン認証のための Odyssey 5.X サプリカントの設定

Active Directory に対する EAP-TLS マシン認証に Odyssey 5.x サプリカントを使用している場合は、サプリカントで次の設定を行う必要があります。

ステップ 1 Odyssey アクセス クライアントを起動します。

ステップ 2 [ツール（Tools）] メニューから [Odyssey アクセス クライアント管理者（Odyssey Access Client Administrator）] を選択します。

ステップ 3 [マシン アカウント（Machine Account）] アイコンをダブルクリックします。

ステップ 4 [マシン アカウント（Machine Account）] ウィンドウから、EAP-TLS 認証のプロファイルを設定する必要があります。

a) **[設定（Configuration）]** > **[プロファイル（Profiles）]** を選択します。

b) EAP-TLS プロファイルの名前を入力します。

c) [認証（Authentication）] タブで、認証方式として [EAP-TLS] を選択します。

d) [証明書（Certificate）] タブで、[証明書を使用したログインを許可（Permit login using my certificate）] チェックボックスをオンにして、サプリカント マシンの証明書を選択します。

e) [ユーザー情報（User Info）] タブで、[マシン クレデンシャルを使用（Use machine credentials）] チェックボックスをオンにします。

このオプションが有効になっている場合、Odyssey サプリカントは host\<*machine_name*> の形式でマシン名を送信します。Active Directory は要求をマシンから送信されていると識別し、認証を実行するコンピュータ オブジェクトを検索します。このオプションが無効になっている場合、Odyssey サプリカントは host\ プレフィクスなしでマシン名を送信します。Active Directory はユーザー オブジェクトを検索し、認証は失敗します。

マシン認証のための AnyConnect エージェント

マシン認証のために AnyConnect エージェントを設定する場合、次のいずれかを実行できます。

- デフォルトのマシン ホスト名（プレフィクス「host/」を含む）を使用する。
- 新しいプロファイルを設定する。その場合、マシン名の前にプレフィクス「host/」を付加する必要があります。

Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件

Easy Connect および パッシブ ID サービスでは、Active Directory ドメイン コントローラによって生成される Active Directory ログイン監査イベントを利用して、ユーザー ログイン情報を収集します。ISE ユーザーが接続を行い、ユーザー ログイン情報を取得することができるように、Active Directory サーバーを適切に設定する必要があります。ここでは、Easy Connect および パッシブ ID サービス をサポートするように Active Directory ドメインコントローラを設定する方法（Active Directory 側からの設定）について説明します。

Easy Connect およびパッシブ ID サービスをサポートするように Active Directory ドメインコントローラを設定するには（Active Directory 側からの設定）、次の手順に従います：

（注） すべてのドメインのすべてのドメインコントローラを設定する必要があります。

1. ISE から Active Directory の参加ポイントとドメイン コントローラを設定します。Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （49 ページ）および#unique_678を参照してください。
2. ドメイン コントローラごとに WMI を設定します。#unique_679を参照してください。
3. Active Directory で次の操作を実行します。

• パッシブ ID サービス の Active Directory の設定 （72 ページ）
• Windows 監査ポリシーの設定 （76 ページ）

4. （オプション）Active Directory で ISE により実行された自動設定のトラブルシューティングを行うには、次の操作を実行します。

• Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定 （76 ページ）
• ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限 （77 ページ）
• ドメイン コントローラで DCOM を使用するための権限 （79 ページ）
• WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （80 ページ）
• AD ドメインコントローラのセキュリティイベントログへのアクセス権の付与 （81 ページ）

パッシブ ID サービス の Active Directory の設定

ISE Easy Connect およびパッシブ ID サービスでは、ユーザー ログイン情報を収集するため、Active Directory ドメイン コントローラにより生成される Active Directory ログイン監査イベントが使用されます。ISE は Active Directory に接続し、ユーザー ログイン情報を取得します。

次の手順は、Active Directory ドメイン コントローラから実行する必要があります。

ステップ 1 該当する Microsoft のパッチが Active Directory ドメイン コントローラにインストールされていることを確認します。

- Windows Server 2008 には次のパッチが必要です。
  - http://support.microsoft.com/kb/958124

    このパッチは Microsoft の WMI のメモリリークを修正し、ISE がドメインコントローラとの正常な接続を確立できないようにします。
  - http://support.microsoft.com/kb/973995

    このパッチは、Microsoft WMI の別のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザー ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。

- Windows Server 2008 R2 では、（SP1 がインストールされていない場合）次のパッチが必要です。
  - http://support.microsoft.com/kb/981314

    このパッチは、Microsoft WMI のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザー ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。

- http://support.microsoft.com/kb/2617858

  このパッチは、Windows Server 2008 R2 での予期しない起動やログイン プロセスの遅れを解消します。

- Windows プラットフォームの WMI 関連問題には、次のリンクにリストされているパッチが必要です。
  - http://support.microsoft.com/kb/2591403

  これらのホットフィックスは、WMI サービスおよび関連コンポーネントの動作と機能に関連付けられます。

ステップ 2 Active Directory がユーザー ログイン イベントを Windows セキュリティ ログに記録するのを確認します。

[監査ポリシー（Audit Policy ）]の設定（[グループポリシー管理（Group Policy Management）] の設定の一部）が、正常なログインによって Windows セキュリティログに必要なイベントが生成されるように設定されていることを確認します（これはデフォルトの Windows 設定ですが、この設定が適切であることを明示的に確認する必要があります）。

ステップ 3 ISE が Active Directory に接続するための十分な権限を持つ Active Directory ユーザーを設定する必要があります。次の手順では、管理ドメイン グループのユーザー、または管理ドメイン グループではないユーザーに対して権限を定義する方法を示します。

- Active Directory ユーザーが Domain Admin グループのメンバーである場合に必要な権限
- Active Directory ユーザーが Domain Admin グループのメンバーでない場合に必要な権限

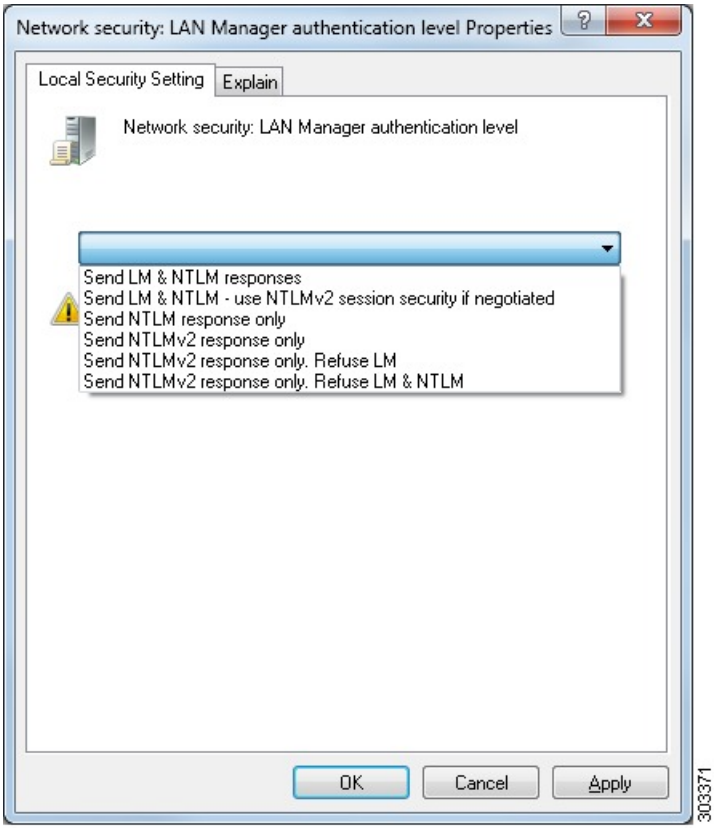
ステップ 4 ISE によって使用される Active Directory ユーザーは、NT Lan Manager（NTLM）v1 または v2 のいずれかによって認証を受けることができます。ISE と Active Directory ドメイン コントローラ間の正常な認証済み接続を確実に行うために、Active Directory NTLM の設定が ISE NTLM の設定と合っていることを確認する必要があります。次の表に、すべての Microsoft NTLM オプションと、サポート対象の ISE NTLM アクションを示します。ISE が NTLMv2 に設定される場合、記載されている 6 つのオプションがすべてサポートされます。NTLMv1 をサポートするように ISE が設定されている場合、最初の 5 つのオプションだけがサポートされます。

表 *14 : ISE* と *AD NTLM* のバージョン設定に基づいてサポートされる認証タイプ

ISE NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション（NTLMv1 NTLMv2）	**NTLMv1**	**NTLMv2**
LM & NTLM応答を送信接続を許可接続を許可（Send LM & NTLM responses connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます

ISE NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション（NTLMv1 NTLMv2）	NTLMv1	NTLMv2
LM & NTLMを送信：ネゴシエートされた接続が許可された場合にNTLMv2セッションセキュリティを使用接続を許可（Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみNTLM応答を送信接続を許可（Send NTLM response only connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみNTLMv2応答を送信接続を許可（Send NTLMv2 response only connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
NTLMv2応答のみを送信（Send NTLMv2 response only）。LMを拒否接続を許可接続を許可（Refuse LM connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
NTLMv2応答のみを送信（Send NTLMv2 response only）。LM & NTLMを拒否接続を拒否接続を許可（Refuse LM & NTLM connection is refused connection is allowed）	接続は拒否されます	接続が受け入れられます

図 *4 : MS NTLM* 認証タイプのオプション



ステップ 5 Active Directory ドメイン コントローラで `dllhost.exe` へのトラフィックを許可するファイアウォール ルールを作成していることを確認します。

ファイアウォールをオフにするか、または次のポートへの特定の IP（ISE IP アドレス）のアクセスを許可することができます。

- TCP 135：一般的な RPC ポート。非同期 RPC 発信をすると、このポートでリスニングしているサービスが、クライアントに、この要求を処理できるコンポーネントが使用しているポートを通知します。
- UDP 137：NetBIOS 名前解決
- UDP 138：NetBIOS データグラム サービス
- TCP 139：NetBIOS セッション サービス
- TCP 445：SMB

数値の大きいポートは動的に割り当てられ、手動で設定できます。ターゲットとして %SystemRoot%\System32\dllhost.exe を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォール ルールを、特定の IP アドレス（ISE IP）に割り当てることができます。

Windows 監査ポリシーの設定

監査ポリシー（**グループポリシー管理**設定の一部）が正常なログインを許可していることを確認します。これには、AD ドメイン コントローラ マシンの Windows セキュリティ ログに必要なイベントを生成する必要があります。これはデフォルトの Windows 設定ですが、この設定が正しいことを確認する必要があります。

ステップ 1 **[スタート]** > **[Programs]** > **[Administrative Tools]** > **[Group Policy Management]** を選択します。

ステップ 2 [Domains] で関連するドメインに移動し、ナビゲーション ツリーを展開します。

ステップ 3 [Default Domain Controller Policy] を選択し、右クリックして、[編集] を選択します。

グループ ポリシー管理エディターが表示されます。

ステップ 4 **[デフォルトのドメイン コントローラ ポリシー（Default Domain Controllers Policy ）]** > **[コンピュータ設定（Computer Configuration）]** > **[ポリシー（Policies）]** > **[Windows 設定（Windows Settings）]** > **[セキュリティ設定（Security Settings）]** の順に選択します。

- Windows Server 2003 または Windows Server 2008（R2 以外）の場合は **[ローカルポリシー（Local Policies）]** > **[監査ポリシー（Audit Policy）]** の順に選択します。2 つのポリシー項目（[Audit Account Logon Events] と [Audit Logon Events]）で、対応する [Policy Setting] に [Success] 状態が直接的または間接的に含まれていることを確認します。[Success] 状況を間接的に含めるには、[Policy Setting] に [Not Defined] を設定します。この場合、上位ドメインから有効値が継承されるため、[Success] 状態を明示的に含めるようにその上位ドメインの [Policy Setting] を設定する必要があります。
- Windows Server 2008 R2 および Windows 2012 の場合、**[Advanced Audit Policy Configuration]** > **[Audit Policies]** > **[Account Logon]** を選択します。2 つのポリシー項目（[Audit Kerberos Authentication Service] と [Audit Kerberos Service Ticket Operations]）に対応する [Policy Setting] に、前述のように [Success] 状態が直接または間接的に含まれていることを確認します。

（注） Active Directory ドメイン コントローラの設定で RC4 暗号が無効になっている場合を除き、Cisco ISE は Active Directory との通信に Kerberos プロトコルで RC4 暗号を使用します。Active Directory で [ネットワークセキュリティ：Kerberosで許可される暗号タイプを設定（Network Security: Configure Encryption Types Allowed for Kerberos）] オプションを使用すると、Kerberos プロトコルで許可される暗号タイプを設定できます。

ステップ 5 [監査ポリシー] の項目設定が変更されている場合は、`gpupdate /force` を実行して新しい設定を強制的に有効にする必要があります。

Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows Server 2012 および Windows Server 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティングシステムの特定のレジストリ キーを完

全に制御することはできません。Microsoft Active Directory の管理者は、Microsoft Active Directory ユーザーに次のレジストリキーに対する完全制御権限を提供する必要があります。

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

次の Microsoft Active Directory バージョンでは、レジストリを変更する必要はありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、まず Microsoft Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーアイコンを右クリックし、[所有者（Owner）] タブを選択します。
ステップ 2 [アクセス許可（Permissions）] をクリックします。
ステップ 3 [詳細設定（Advanced）] をクリックします。

ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限

Windows 2012 R2 の場合は、Microsoft AD ユーザーに次のレジストリキーに対する完全制御権限を提供します。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell で次のコマンドを使用して、レジストリキーに完全な権限が付与されているかどうかを確認します。

- `get-acl -path "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`
- `get-acl -path "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`

Microsoft AD ユーザーがドメイン管理者グループではなく、ドメインユーザーグループに所属している場合は、次の権限が必要です。

- Cisco ISE がドメインコントローラに接続できるようにするには、レジストリキーを追加します。

- ドメイン コントローラで DCOM を使用するための権限 （79 ページ）
- WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （80 ページ）

これらの権限は、次のバージョンの Microsoft AD でのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ドメインコントローラへの Cisco ISE の接続を許可するためにレジストリキーを追加

Cisco ISE がドメインユーザーとして接続し、ログイン認証イベントを取得できるようにするには、ドメインコントローラにいくつかのレジストリ キーを手動で追加する必要があります。エージェントはドメインコントローラまたはドメイン内のマシンには必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

DllSurrogate キーの値には、2 つのスペースが含まれていることを確認します。レジストリを手動で更新する場合は、2 つのスペースのみを含める必要があり、引用符は含めないでください。レジストリを手動で更新する際は、AppID、DllSurrogate、およびその値に引用符が含まれていないことを確認してください。

前述のスクリプトに示すように、ファイルの末尾の空の行を含めて、空の行は保持します。

Windows コマンドプロンプトで次のコマンドを使用して、レジストリキーが作成され、正しい値が設定されているかどうかを確認します。

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

ドメイン コントローラで DCOM を使用するための権限

Cisco ISE パッシブ ID サービスに使用される Microsoft Active Directory ユーザーには、ドメイン コントローラ サーバーでDCOM を使用する権限が必要です。**dcomcnfg** コマンドラインツールを使用して権限を設定します。

ステップ 1 コマンド ラインから **dcomcnfg** ツールを実行します。

ステップ 2 [コンポーネントサービス（Component Services）] を展開します。

ステップ 3 **[コンピュータ（Computers）] > [マイコンピュータ（My Computer）]** を展開します。

ステップ 4 メニューバーで [アクション（Action）] を選択し、[プロパティ（Properties）] をクリックして [COM セキュリティ（COM Security）] をクリックします。

ステップ 5 Cisco ISE がアクセスと起動の両方に使用するアカウントには許可権限が必要です。4 つのオプション（[アクセス権限Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対する [制限の編集（Edit Limits）] と [デフォルトの編集（Edit Default）]）のすべてに Microsoft Active Directory ユーザーを追加します。

ステップ 6 [アクセス権限（Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対してローカルアクセスとリモートアクセスをすべて許可します。

図 *5 : [アクセス権限（Access Permissions）]* に対するローカルアクアセスとリモートアクセス

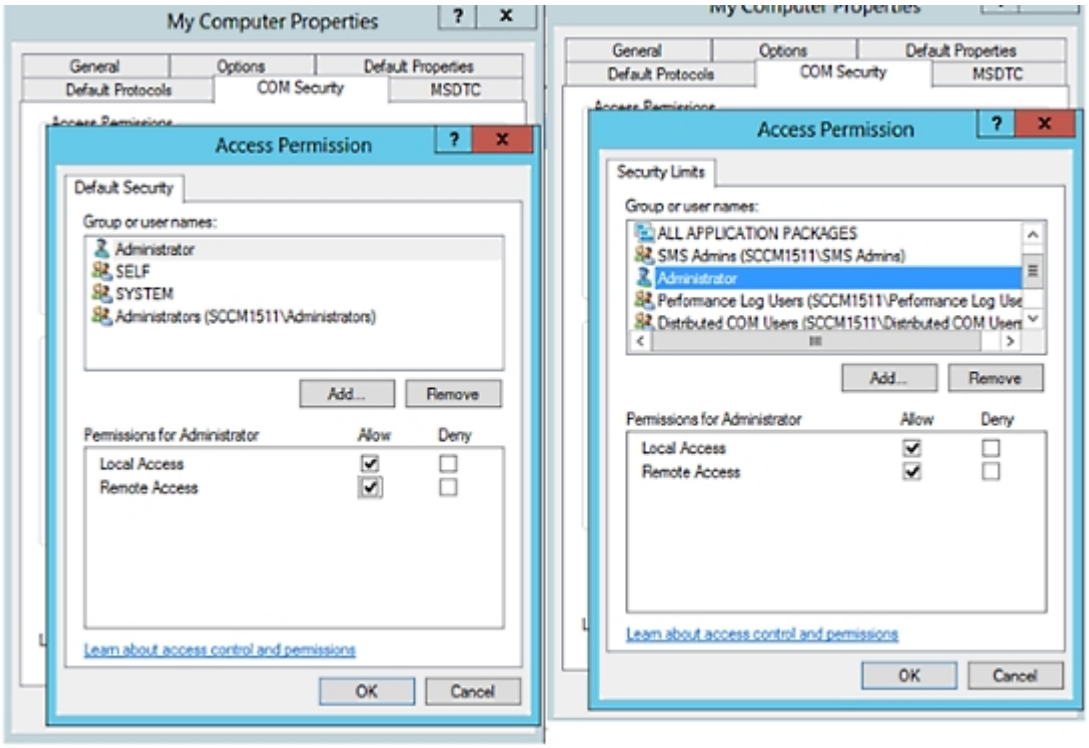
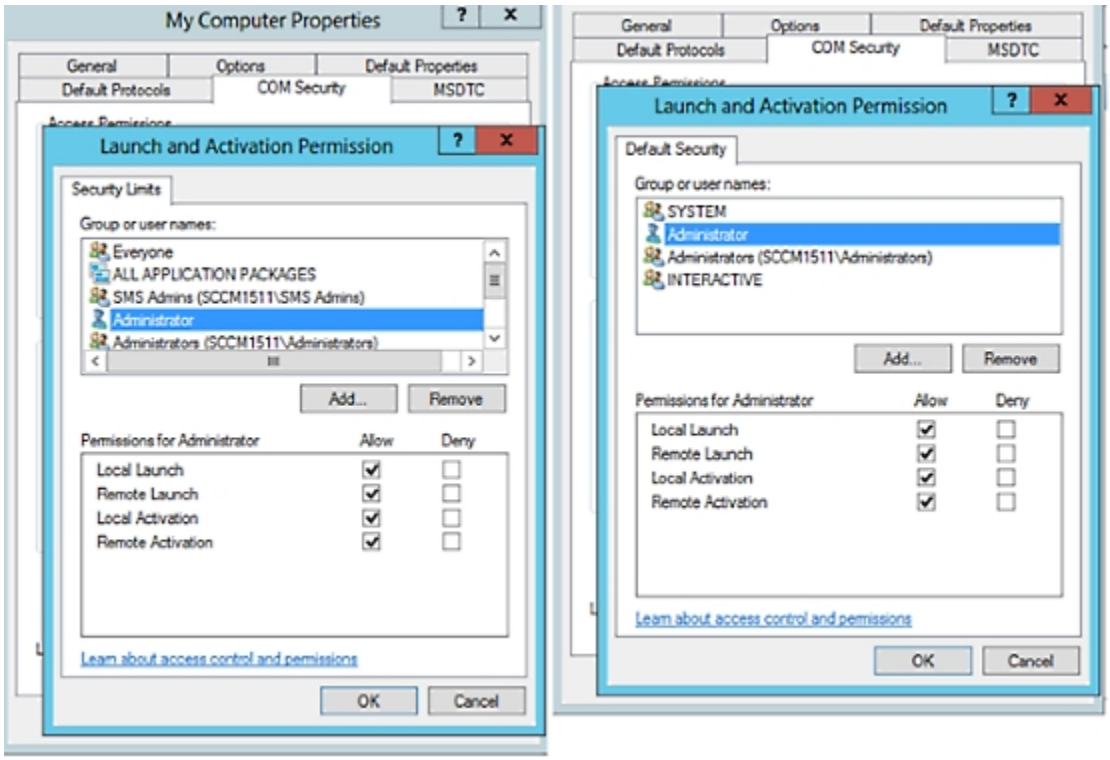


図 *6 :* [起動およびアクティブ化の権限（***Launch and Activation Permissions***）] のローカルアクセスとリモートアクセス



WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Microsoft Active Directory ユーザーには実行メソッドおよびリモートの有効化のための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

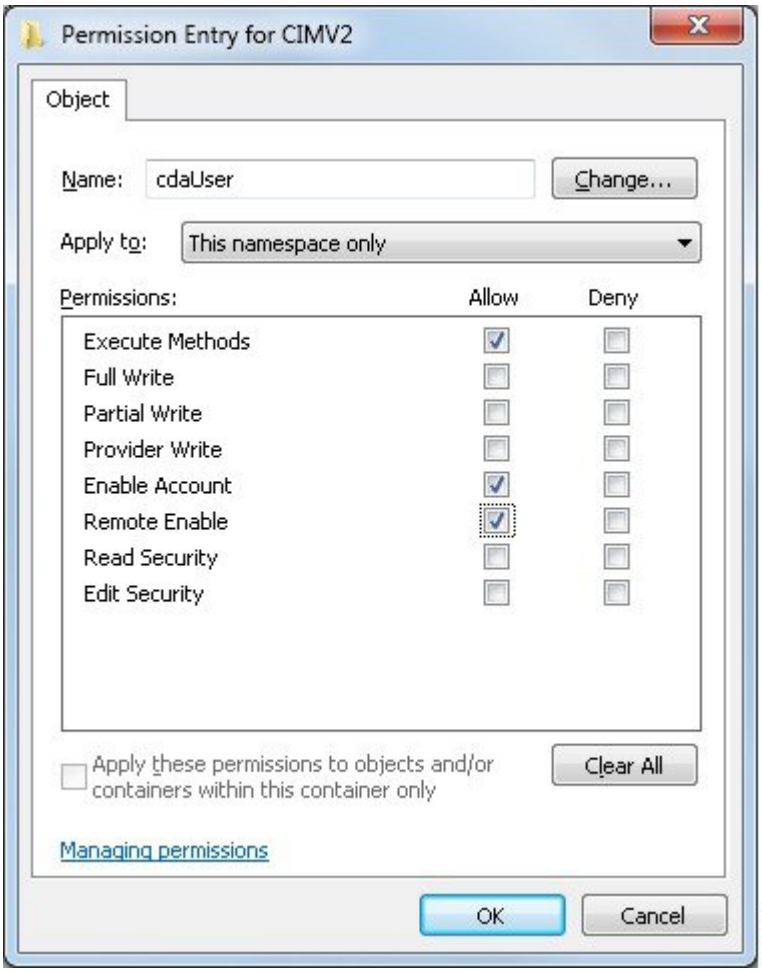
ステップ 1 **[スタート（Start）]** > **[実行（Run）]** を選択し、`wmimgmt.msc` と入力します。

ステップ 2 **[WMI Control]** を右クリックし、**[プロパティ（Properties）]** をクリックします。

ステップ 3 **[セキュリティ（Security）]** タブで、**[ルート（Root）]** を展開し、**[CIMV2]** を選択します。

ステップ 4 [セキュリティ（Security）] をクリックします。

ステップ 5 次のイメージに示すように、Microsoft Active Directory ユーザーを追加し、必要な権限を設定します。



AD ドメインコントローラのセキュリティイベントログへのアクセス権の付与

Windows 2008 以降では、ISE ID マッピング ユーザーを Event Log Reader と呼ばれるグループに追加することで、AD ドメイン コントローラのログへのアクセス権を付与できます。

Windows のすべての旧バージョンでは、次に示すようにレジストリ キーを編集する必要があります。

ステップ 1 セキュリティ イベント ログへのアクセス権を委任するには、アカウントの SID を検索します。

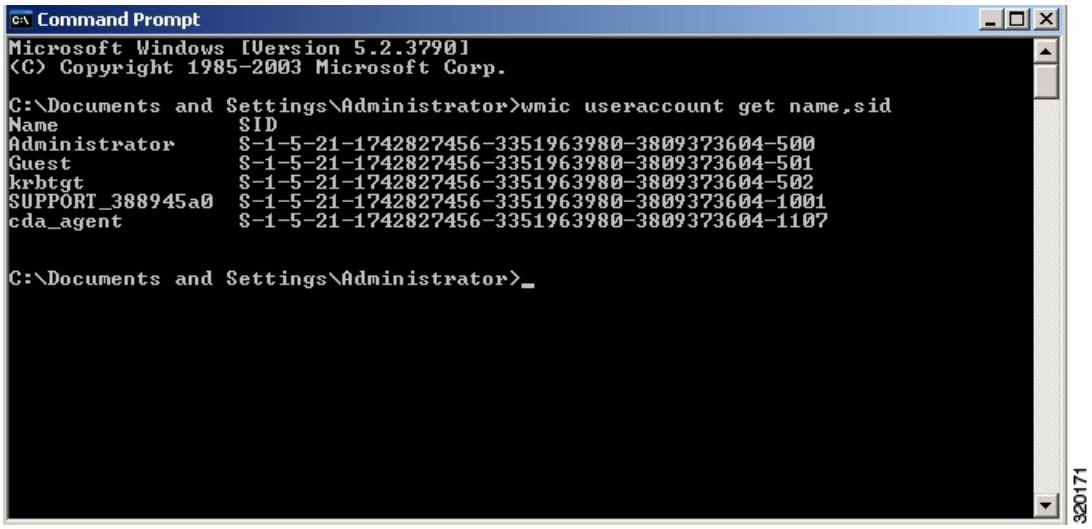
ステップ 2 すべての SID アカウントを表示するには、次の図に示すように、コマンド ラインから次のコマンドを使用します。

```
wmic useraccount get name,sid
```

特定のユーザー名とドメインに対して、次のコマンドを使用することもできます。

```
wmic useraccount where name="iseUser" get domain,name,sid
```

図 *7:* すべての *SID* アカウントの表示



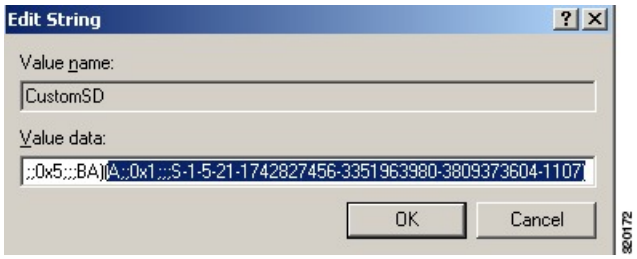
ステップ 3 SID を見つけ、レジストリ エディタを開き、次の場所を参照します。

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog
```

ステップ 4 [セキュ リティ（Security）] をクリックし、[CustomDS] をダブルクリックします。

たとえば、ise_agent アカウント（`SID：S-1-5-21-1742827456-3351963980-3809373604-1107`）への読み取りアクセスを許可するには、「`(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`」と入力します。

図 *8 : CustomSD* 文字列の編集



ステップ 5 ドメイン コントローラ上で WMI サービスを再起動します。次の 2 とおりの方法で WMI サービスを再起動できます。

a) CLI から次のコマンドを実行します。

net stop winmgmt

net start winmgmt

b) `Services.msc` を実行します。これにより、Windows サービス管理ツールが開きます。Windows サービス管理ウィンドウで、「**Windows Management Instrumentation**」サービスを検索し、右クリックして [再起動] を選択します。

Easy Connect

Easy Connect により、セキュアな方法で有線接続されたエンドポイントからネットワークにユーザーを簡単に接続し、Cisco ISE ではなく Active Directory ドメイン コントローラからユーザーを認証することで、それらのユーザーをモニターすることができます。Easy Connect により、Cisco ISE は Active Directory ドメインコントローラからユーザー認証情報を収集します。Easy Connect は MS WMI インターフェイスを使用して Windows システム（Active Directory）に接続し、Windows イベントメッセージからのログにクエリを行うため、現在は Windows がインストールされているエンドポイントのみをサポートしています。Easy Connect は MAB を使用した有線接続をサポートし、これは 802.1X よりもずっと設定が容易です。802.1X とは異なり、Easy Connect と MAB では、

- サプリカントを設定する必要がありません
- PKI を設定する必要がありません
- ISE は外部サーバー（AD）がユーザーを認証した後に CoA を発行します

Easy Connect は次の動作モードをサポートしています。

- 適用モード：ISE がユーザー クレデンシャルに基づいて、適用のために認証ポリシーをネットワークデバイスにアクティブにダウンロードします。
- 可視性モード：Cisco ISE がセッションマージをパブリッシュし、情報を pxGrid に送信するために NAD デバイスセンサーから受信した情報をアカウンティングします。

どちらの場合も、Active Directory（AD）で認証されたユーザーは、Cisco ISE のライブ セッション ビューに表示され、サードパーティ製アプリケーションによる Cisco pxGrid インターフェイスを使用してセッションディレクトリからクエリすることができます。既知の情報としては、ユーザー名、IP アドレス、AD DC ホスト名と AD DC NetBIOS 名があります。pxGrid の詳細については、Cisco pxGrid ノードを参照してください。

Easy Connect のセットアップが完了したら、ユーザーの名前または IP アドレスに基づいて特定ユーザーをフィルタリングできます。たとえば IT サービスの管理者が、そのエンドポイントの標準ユーザーを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して [ライブ セッション（Live Sessions）] に表示されないようにし、そのエンドポイントの標準ユーザーだけが表示されるようにできます。パッシブ ID サービスをフィルタリングするには、パッシブ ID サービスのフィルタリング （137 ページ）を参照してください。

Easy Connect の制限

- MAC 認証バイパス（MAB）は Easy Connect をサポートします。MAB と 802.1X の両方を同じポートで設定できますが、各サービス用に異なる ISE ポリシーが必要です。
- 現在は MAB 接続のみがサポートされています。許可ポリシーで定義されている Easy Connect 条件によって接続が許可され、権限が付与されるため、接続についての独自の認証ポリシーは不要です。
- Easy Connect はハイ アベイラビリティ モードでサポートされます。パッシブ ID を使用して、複数のノードを定義して有効にすることができます。ISE はその後自動的に 1 つの PSN を有効にしますが、その他のノードはスタンバイ状態のままです。
- シスコのネットワーク アクセス デバイス（NAD）のみがサポートされています。
- IPv6 はサポートされていません。
- ワイヤレス接続は現在サポートされていません。
- Kerberos 認証イベントのみが追跡されるため、Easy Connect はユーザー認証のみを有効にし、マシン認証をサポートしません。

Easy Connect は ISE で設定する必要があり、Active Directory ドメイン サーバーには Microsoft によって発行された指示とガイドラインに基づいた適切なパッチと設定が必要です。Cisco ISE の Active Directory ドメインコントローラの設定については、次の項を参照してください。Active Directory でEasy Connect およびパッシブ ID サービスをサポートするための要件 （71 ページ）

Easy Connect 適用モード

Easy Connect により、ユーザーは MAC アドレス バイパス（MAB）プロトコルを使用し、認証のための Active Directory（AD）にアクセスすることで、Windows オペレーティング システムを備えた有線接続されたエンドポイント（通常は PC）からセキュアなネットワークにログオンすることができます。Easy Connect は、認証されるユーザーに関する情報のために Active Directory サーバーからの Windows Management Instrumentation（WMI）イベントをリッスンします。AD がユーザーを認証すると、ドメインコントローラがユーザーに割り当てられたユーザー名と IP アドレスを含むイベント ログを生成します。Cisco ISE が AD からログインの通知を受信し、RADIUS の認可変更（CoA）を発行します。

（注） RADIUS サービス タイプが call-check に設定されている場合、MAC アドレス ルックアップは MAB 要求のために行われません。そのため、この要求への応答は access-accept です。これはデフォルトの設定です。

Easy Connect 適用モードのプロセス フロー

Easy Connect 適用モードのプロセスは次のとおりです。

1. ユーザーが有線接続されたエンドポイント（PC など）から NAD に接続します。

2. NAD（MAB 用に設定）はアクセス要求を Cisco ISE に送信します。Cisco ISE がアクセスに応答し、ユーザー設定に基づいて、ユーザーに AD へのアクセスを許可します。設定では、少なくとも DNS、DHCP、および AD へのアクセスを許可する必要があります。
3. ユーザーがドメインにログインし、セキュリティ監査イベントが Cisco ISE に送信されます。
4. ISE は RADIUS から MAC アドレスを収集し、セキュリティ監査イベントから IP アドレス、ドメイン名、ユーザーに関するアカウンティング情報（ログイン情報）を収集します。
5. セッションディレクトリですべてのデータが収集されてマージされると、（ポリシーサービスノードで管理されている適切なポリシーに基づいて）Cisco ISE が NAD に CoA を発行し、そのポリシーに基づいて NAD によりユーザーにネットワークへのアクセスが提供されます。

図 *9 : Easy Connect* 適用モードの基本フロー

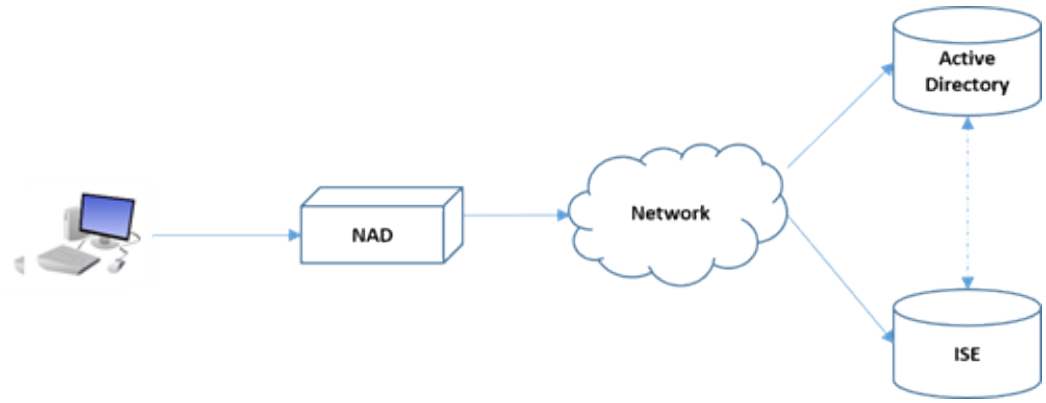
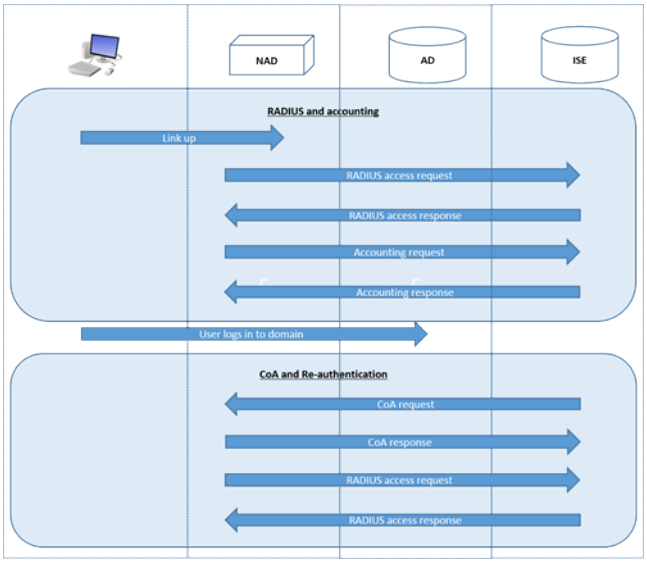


図 *10 : Easy Connect* 適用モードの詳細フロー

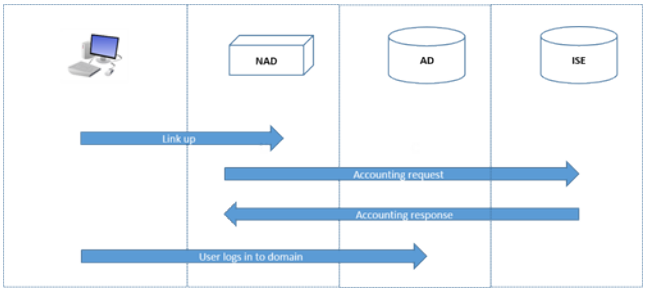


適用モードの設定の詳細については、Easy Connect 適用モードの設定 （86 ページ）を参照してください。

Easy Connect 可視性モード

可視性モードでは、Cisco ISE は RADIUS からのアカウンティング情報のみをモニターし（NAD のデバイスセンサー機能の一部）、認証は行いません。Easy Connect は RADIUS アカウンティングと WMI イベントをリッスンし、ログとレポート（およびオプションで pxGrid）にその情報をパブリッシュします。pxGrid が設定されている場合、Active Directory を使用したユーザーログイン中に RADIUS のアカウンティング開始とセッション終了の両方が pxGrid にパブリッシュされます。

図 *11 : Easy Connect* 可視性モードのフロー



Easy Connect 可視性モードの設定の詳細については、Easy Connect 可視性モードの設定 （88 ページ）を参照してください。

Easy Connect 適用モードの設定

始める前に

- 最適なパフォーマンスを得るには、WMI イベントを受け取るための専用の PSN を導入します。
- AD ログイン イベントを受け取る、WMI ノードの Active Directory ドメイン コントローラのリストを作成します。
- Active Directory からユーザーグループを取得するために Cisco ISE が参加する必要がある Microsoft ドメインを決定します。
- 認証ポリシーでリファレンスとして使用される Active Directory グループを決定します。
- pxGrid を使用してネットワーク デバイスからのセッション データを他の pxGrid 対応システムと共有する場合は、展開内で pxGrid ペルソナを定義します。pxGrid の詳細については、次を参照してください。 Cisco pxGrid ノード
- MAB が成功した後、NAD は、そのポートのユーザーが Active Directory サーバーにアクセスできるようにする、制限付きアクセスプロファイルを提供する必要があります。

（注） パッシブ ID サービスは複数のノードで有効にできますが、Easy Connect は一度に 1 つのノードでのみ操作できます。複数のノードのサービスを有効にすると、ISE はアクティブな Easy Connect セッションのために使用するノードを自動的に決定します。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択してノードを開き、[全般設定（General Settings）] で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] を有効にします。

ステップ 2 Easy Connect が使用する Active Directory 参加ポイントとドメイン コントローラを設定します。詳細については、Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件 （71 ページ）を参照してください。

ステップ 3 （オプション）**[管理（Administration）]** > **[ID 管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > [Active Directory] を選択します。[グループ（Groups）] タブをクリックし、認証ポリシーで使用する Active Directory グループを追加します。
ドメイン コントローラ用にマッピングした Active Directory グループは PassiveID ディクショナリで動的に更新され、ポリシー条件ルールを設定するときに使用することができます。

ステップ 4 （注） Easy Connect プロセスが適切に実行され、ISE が有効にされて CoA が発行できるように、Easy Connect 認証に使用されるすべてのプロファイルで [パッシブ ID 追跡（Passive Identity Tracking）] を有効にする必要があります。

[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）]** を選択します。Easy Connect によって使用されるプロファイルについて、プロファイルを開いて [パッシブ ID 追跡（Passive Identify Tracking）] を有効にします。

ステップ 5 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[条件（Conditions）]** > **[許可（Authorization）]** > **[単純条件（Simple Conditions）]** を選択し、Easy Connect 用のルールを作成します。[追加（Add）] をクリックして条件を定義します。

a) 名前と説明を入力します。
b) [属性（Attribute）] から PassiveID ディクショナリに移動し、PassiveID_Groups を選択してドメイン コントローラ グループ用の条件を作成するか、PassiveID_user を選択して個々のユーザー用の条件を作成します。
c) 正しい操作を入力します。
d) ポリシーに含めるユーザー名またはグループ名を入力します。

ステップ 6 **[送信（Submit）]** をクリックします。

Easy Connect 可視性モードの設定

始める前に

- 最適なパフォーマンスを得るには、WMI イベントを受け取るための専用の PSN を導入します。
- AD ログイン イベントを受け取る、WMI ノードの Active Directory ドメイン コントローラのリストを作成します。
- Active Directory からユーザーグループを取得するために Cisco ISE が参加する必要がある Microsoft ドメインを決定します。
- pxGrid を使用してネットワーク デバイスからのセッション データを他の pxGrid 対応システムと共有する場合は、展開内で pxGrid ペルソナを定義します。pxGrid の詳細については、次を参照してください。 Cisco pxGridノード

ステップ 1 **[管理（Administration）]>[システム（System）]>[展開（Deployment）]** を選択してノードを開き、[全般設定（General Settings）] で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] を有効にします。

ステップ 2 Easy Connect が使用する Active Directory 参加ポイントとドメイン コントローラを設定します。詳細については、Active Directory でEasy Connect およびパッシブ ID サービスをサポートするための要件 （71 ページ）を参照してください。

PassiveID ワーク センター

パッシブ ID コネクタ（PassiveID ワーク センター）は一元的なワンストップ インストールおよび実装を提供します。これにより、ユーザー ID 情報を受信してさまざまなセキュリティ製品（Cisco Firepower Management Center（FMC）や Stealthwatch など）のサブスクライバと共有するように、ネットワークを容易に設定できます。パッシブ ID の完全なブローカとして、PassiveID ワーク センター はさまざまなプロバイダ ソース（Active Directory ドメイン コントローラ（AD DC）など）からユーザー ID を収集し、ユーザー ログイン情報を使用中の該当するIPアドレスにマッピングし、そのマッピング情報を、設定されているサブスクライバセキュリティ製品と共有します。

パッシブ ID について

認証、許可、およびアカウンティング（AAA）サーバーを提供し、802.1X や Web 認証などのテクノロジーを使用する Cisco Identity Services Engine（ISE）で提供される標準フローは、ユーザーまたはエンドポイントと直接通信し、ネットワークへのアクセスを要求し、ログインクレデンシャルを使用して ID を検証およびアクティブに認証します。

パッシブ ID サービスはユーザーを直接認証するのではなく、プロバイダと呼ばれる Active Directory などの外部認証サーバーからユーザー ID および IP アドレスを収集し、サブスクライバとこの情報を共有します。まず初めに、PassiveID ワーク センターは、通常、ユーザーのログインとパスワードに基づいてプロバイダからユーザー ID 情報を受信し、ユーザー ID および関連する IP アドレスを照合するために必要な確認とサービスを実行し、認証済み IP アドレスをサブスクライバに提供します。

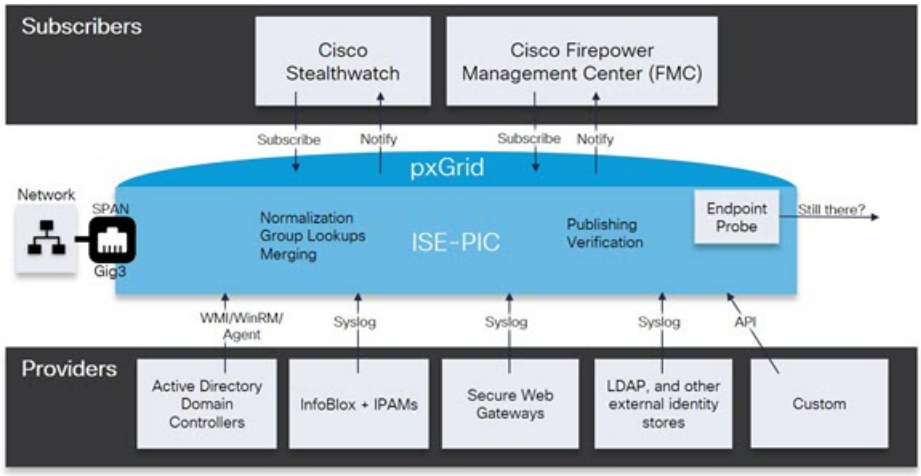
Passive Identity Connector（PassiveID ワーク センター）のフロー

PassiveID ワーク センター のフローは次のとおり。

1. プロバイダがユーザーまたはエンドポイントの認証を実行します。
2. プロバイダが認証済みのユーザー情報を Cisco ISE に送信します。
3. Cisco ISE によりユーザー情報の正規化、ルックアップ、マージ、解析、および IP アドレスへのマッピングが行われ、マッピングされた詳細情報が pxGrid に対して公開されます。
4. pxGrid サブスクライバはマッピングされたユーザーの詳細情報を受信します。

次の図に、Cisco ISE の全体的なフローを示します。

図 *12 :* 全体的なフロー



初期セットアップと設定

Cisco PassiveID ワーク センターをすぐに使用できるようにするには、次のフローに従います。

1. DNS サーバーを適切に設定していることを確認します。これには、Cisco ISE からのクライアントマシンの逆引きの設定も含まれます。詳細については、DNS サーバー （48 ページ）を参照してください。
2. いずれかのパッシブ ID サービスに使用する専用ポリシーサーバー（PSN）で、パッシブ ID サービスと pxGrid サービスを有効にします。**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択して該当するノードを開き、[全般設定（General

Settings）] で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] と [pxGrid] を有効にします。

3. NTP サーバーのクロック設定を同期します。
4. ISE パッシブ ID セットアップで、最初のプロバイダを設定します。詳細については、PassiveID セットアップの使用を開始する （92 ページ）を参照してください。
5. 1 つまたは複数のサブスクライバを設定します。詳細については、サブスクライバ （140 ページ）を参照してください。

最初のプロバイダとサブスクライバの設定が完了したら、追加のプロバイダを容易に作成できます（その他の パッシブ ID サービス プロバイダ （98 ページ）を参照）。また PassiveID ワーク センター。

PassiveID ワーク センター ダッシュボード

Cisco PassiveID ワーク センター ダッシュボードには、効果的なモニターリングおよびトラブルシューティングに必要不可欠な、統合され、関連付けられた概要と統計データが表示されます。ダッシュボードはリアルタイムに更新されます。特に指定がない限り、ダッシュレットには過去 24 時間のアクティビティが表示されます。ダッシュボードにアクセスするには、**[ワークセンター（Work Centers）] > [PassiveID]** を選択し、左側のパネルで [ダッシュボード（Dashboard）] を選択します。Cisco PassiveID ワーク センター ダッシュボードはプライマリ管理ノード（PAN）でのみ表示できます。

- [メイン（Main）] ビューには、線形の [メトリクス（Metrics）] ダッシュボード、チャート ダッシュレット、およびリストダッシュレットが含まれています。PassiveID ワーク センターでは、ダッシュレットは設定できません。使用可能なダッシュレットには次のものがあります。
  - [パッシブ ID メトリック（Passive Identity Metrics）] では、現在追跡中の固有のライブ セッションの総数、システムに設定されている ID プロバイダの総数、ID データをアクティブに配信しているエージェントの総数、および現在設定されているサブスクライバの総数が表示されます。
  - [プロバイダ（Providers）] : プロバイダはユーザー ID 情報を PassiveID ワーク センター に提供します。ISE プローブ(特定のソースからデータを収集するメカニズム）を設定します。プローブを介してプロバイダ ソースからの情報を受信します。たとえば、Active Directory（AD）プローブとエージェント プローブはいずれも ISE-PIC による AD からのデータ収集を支援しますが、syslog プローブは、syslog メッセージを読み取るパーサーからデータを収集します。
  - [サブスクライバ（Subscribers）] : サブスクライバは ISE に接続し、ユーザー ID 情報を取得します。
  - [OS タイプ（OS Types）] : 表示できる唯一の OS タイプは Windows です。Windows のタイプが Windows バージョン別に表示されます。プロバイダは OS タイプを報告しませんが、ISE はこの情報を取得するため Active Directory を照会できます。ダッシュレットに表示できるエントリの最大数は 1000 です。

• [アラーム（Alarms）]：ユーザー ID 関連のアラーム。

プローブおよびプロバイダとしての Active Directory

Active Directory（AD）は、ユーザー ID 情報（ユーザー名、IP アドレス、ドメイン名など）の取得元である安全性が高く正確なソースです。

AD プローブ（パッシブ ID サービス）は、WMI テクノロジーを使用して AD からユーザー ID 情報を収集しますが、その他のプローブはその他のテクノロジーや手法で AD をユーザー ID プロバイダとして使用します。ISE のその他のプローブとプロバイダ タイプの詳細については、その他の パッシブ ID サービス プロバイダ （98 ページ）を参照してください。

Active Directory プローブを設定すると、次の（ソースとして Active Directory を使用する）その他のプローブも迅速に設定して有効にできます。

- Active Directory エージェント （101 ページ）

（注） Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。

- SPAN （112 ページ）
- エンドポイント プローブ （138 ページ）

また、ユーザー情報の収集時に AD ユーザー グループを使用するために Active Directory プローブを設定します。AD、エージェント、SPAN、および syslog プローブで AD ユーザーグループを使用できます。AD グループの詳細については、Active Directory ユーザー グループの設定（55 ページ）を参照してください。

Active Directory（WMI）プローブのセットアップ

パッシブ ID サービス向けに Active Directory と WMI を設定するには、パッシブ ID ワークセンターウィザードを使用するか（PassiveID セットアップの使用を開始する （92 ページ）を参照）、または次の手順に従います。

1. Active Directory プローブを設定します。Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （49 ページ）を参照してください。
2. AD ログイン イベントを受信する 1 つ以上の WMI 設定ノードの Active Directory ドメインコントローラのリストを作成します。#unique_678を参照してください。
3. Active Directory を ISE と統合するため Active Directory を設定します。#unique_679を参照してください。
4. （オプション）Active Directory プロバイダの管理 （94 ページ）。

詳細については、Active Directory でEasy Connect および パッシブ ID サービスをサポートするための要件 （71 ページ）を参照してください。

PassiveID セットアップの使用を開始する

ISE-PIC には、Active Directory からユーザー ID を受信するために、Active Directory を最初のユーザー ID プロバイダとして容易に設定できるウィザードがあります。ISE-PIC に Active Directory を設定することで、後でその他のプロバイダ タイプを設定するプロセスも簡素化されます。Active Directory を設定したら、ユーザーデータを受信するクライアントを定義するため、サブスクライバ（Cisco Firepower Management Center（FMC）や Stealthwatch など）を設定する必要があります。サブスクライバの詳細については、サブスクライバ（140 ページ） を参照してください。

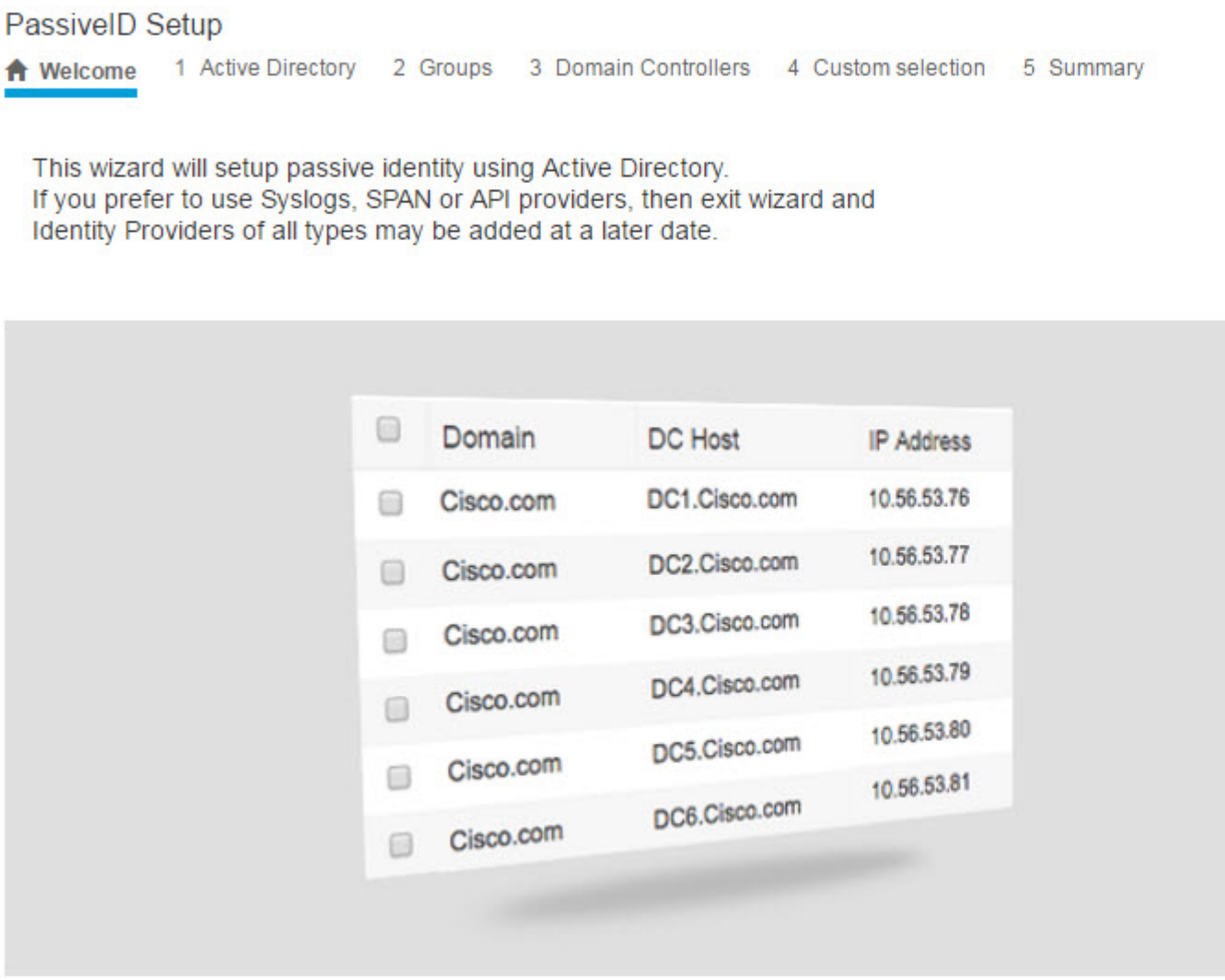
始める前に

- Microsoft Active Directory サーバーがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないことを確認します。
- 参加操作用の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更（Change Password on Next Login）] を使用して設定されていないことを確認します。
- ISE でのスーパー管理者またはシステム管理者の権限があることを確認します。
- いずれかのパッシブ ID サービスに使用する専用ポリシーサーバー（PSN）で、パッシブ ID サービスと pxGrid サービスを有効にします。**[管理（Administration）]** > **[システム（System）]**>**[展開（Deployment）]** を選択して該当するノードを開き、[全般設定（General Settings）] で [パッシブ ID サービスの有効化（Enable Passive Identity Service）] と [pxGrid] を有効にします。
- ISE のエントリがドメイン ネーム サーバー（DNS）にあることを確認します。ISE からのクライアントマシンの逆引き参照を適切に設定していることを確認します。詳細については、DNS サーバー （48 ページ）を参照してください。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** を選択します。[パッシブ ID コネクタの概要（Passive Identity Connector Overview）] 画面で [パッシブ ID ウィザード（Passive Identity Wizard）] をクリックします。

[PassiveID セットアップ（PassiveID Setup）] ウィンドウが表示されます。

図 *13 : [PassiveID* セットアップ（*PassiveID Setup*）*]*



ステップ 2 [次へ（Next）] をクリックしてウィザードを開始します。

ステップ 3 この Active Directory の参加ポイントの一意の名前を入力します。このノードが接続されている Active Directory ドメインのドメイン名を入力し、Active Directory 管理者のユーザー名とパスワードを入力します。

[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメインコントローラ（DC）に使用されます。

ステップ 4 [次へ（Next）] をクリックし、Active Directory グループを定義し、追加してモニターするユーザー グループをすべてオンにします。

前のステップで設定した Active Directory 参加ポイントに基づいて Active Directory ユーザー グループが自動的に表示されます。

ステップ 5 [次へ（Next）] をクリックします。モニターする DC を選択します。[カスタム（Custom）] を選択した場合は、次の画面でモニターする特定の DC を選択します。完了したら、[次へ（Next）] をクリックします。

ステップ 6 [終了（Exit）] をクリックして、ウィザードを終了します。

次のタスク

最初のプロバイダとして Active Directory の設定を完了したら、追加のプロバイダ タイプも容易に設定できます。詳細については、その他のパッシブ ID サービス プロバイダ （98 ページ）を参照してください。さらに、定義したいずれかのプロバイダが収集したユーザー ID 情報を受信するためのサブスクライバも設定できるようになりました。詳細については、サブスクライバ （140 ページ）を参照してください。

Active Directory プロバイダの管理

Active Directory 参加ポイントの作成と設定が完了したら、次の作業を行い Active Directory プローブを管理します。

- Active Directory 認証のためのユーザーのテスト （64 ページ）
- ノードの Active Directory の参加の表示 （65 ページ）
- Active Directory の問題の診断 （65 ページ）
- Active Directory ドメインの脱退 （53 ページ）
- Active Directory の設定の削除 （64 ページ）
- Active Directory デバッグ ログの有効化 （66 ページ）

Active Directory の設定

Active Directory（AD）は、安全性が高く正確なソースであり、ここからユーザー情報（ユーザー名、IP アドレスなど）が取得されます。

参加ポイントを作成、編集することで Active Directory のプローブを作成し、管理するには、**[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダ（Providers）] > [Active Directory]** を選択します。

詳細については、Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE ノードの参加 （49 ページ）を参照してください。

表 *15 : Active Directory* 参加ポイント名の設定と *[ドメインへの参加（Join Domain）]* ウィンドウ

フィールド名	説明
参加ポイント名（Join Point Name）	設定したこの参加ポイントを容易に区別できる一意の名前。

フィールド名	説明
Active Directory ドメイン（Active Directory Domain）	このノードが接続している Active Directory ドメインのドメイン名。
ドメイン管理者（Domain Administrator）	管理者権限を持つ Active Directory ユーザーのユーザープリンシパル名またはユーザーアカウント名。
パスワード（Password）	Active Directory で設定されているドメイン管理者のパスワード。
組織単位の指定（Specifiy Organizational Unit）	管理者の組織単位の情報を入力します。
クレデンシャルの保存（Store Credentials）	[クレデンシャルの保存（Store Credentials）] を選択することを強く推奨します。これにより、管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメインコントローラ（DC）に使用されます。 エンドポイントプローブの場合は、[クレデンシャルの保存（Store Credentials）] を選択する必要があります。

表 *16 : [Active Directory* 参加/脱退（*Active Directory Join/Leave*）*]* ウィンドウ

フィールド名	説明
ISEノード（ISE Node）	インストール環境での特定のノードの URL。
ISE ノードのロール（ISE Node Role）	インストール環境でそのノードがプライマリノードまたはセカンダリ ノードのいずれであるかを指定します。
ステータス（Status）	ノードが Active Directory ドメインにアクティブに参加しているかどうかを示します。
ドメインコントローラ（Domain Controller）	Active Directory に参加しているノードの場合、この列には Active Directory ドメインでノードが接続している特定のドメイン コントローラが示されます。
サイト（Site）	Active Directory フォレストが ISE に参加する場合、このフィールドには、[Active Directory サイトとサービス（Active Directory Sites and Services）] 領域に示されるフォレスト内の特定の Active Directory サイトが示されます。

表 *17 : [*パッシブ *ID* ドメイン コントローラ（*DC*）（*Passive ID Domain Controllers (DC)*）*]* リスト

フィールド	説明
ドメイン（**Domain**）	ドメインコントローラが存在しているサーバーの完全修飾ドメイン名。
DC ホスト（DC Host）	ドメインコントローラが存在しているホスト。
サイト（**Site**）	Active Directory フォレストが ISE に参加する場合、このフィールドには、[Active Directory サイトとサービス（Active Directory Sites and Services）] 領域に示されるフォレスト内の特定の Active Directory サイトが示されます。
IP アドレス（IP Address）	ドメイン コントローラの IP アドレス。
モニター方法（**Monitor Using**）	次のいずれかの方法で、ユーザー ID 情報を取得するため Active Directory ドメイン コントローラをモニターします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニターします。 • [エージェント名（Agent name）]：ユーザー情報を取得するために Active Directory をモニターするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウンリストから使用するエージェントを選択します。エージェントの詳細については、Active Directory エージェント（101 ページ） を参照してください。

表 *18 : [*パッシブ *ID* ドメインコントローラ（*DC*）（*Passive ID Domain Controllers (DC)*）*]* 編集ウィンドウ

フィールド名	説明
ホスト FQDN（Host FQDN）	ドメインコントローラが存在しているサーバーの完全修飾ドメイン名を入力します。
説明（**Description**）	このドメイン コントローラを容易に特定できるように、一意の説明を入力します。
ユーザー名（User Name）	Active Directory にアクセスするための管理者のユーザー名。
パスワード（**Password**）	Active Directory にアクセスするための管理者のパスワード。

フィールド名	説明
プロトコル（**Protocol**）	次のいずれかの方法で、ユーザーID情報を取得するため Active Directory ドメイン コントローラをモニターします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニターします。 • [エージェント名（Agent name）]：ユーザー情報を取得するためにActive Directoryをモニターするエージェントを定義している場合は、Agentプロトコルを選択し、ドロップダウンリストから使用するエージェントを選択します。エージェントの詳細については、Active Directoryエージェント（101ページ）を参照してください。

Active Directoryグループは Active Directoryから定義および管理されます。このノードに参加している Active Directoryのグループは、このタブで確認できます。Active Directoryの詳細については、https://msdn.microsoft.com/en-us/library/bb742437.aspxを参照してください。

表 *19 : Active Directory* の詳細設定

フィールド名	説明
履歴期間（History interval）	すでに発生したユーザー ログインの情報を パッシブ ID サービスが読み取る期間。これは、パッシブ ID サービスの起動時または再起動時に、このサービスが使用不可であった間に生成されたイベントを確認するために必要となります。エンドポイント プローブがアクティブな場合、この期間の頻度が維持されます。
ユーザーセッションのエージングタイム（User session aging time）	ユーザーがログインできる時間です。パッシブ ID サービスでは、DC からの新しいユーザー ログイン イベントが識別されますが、DC はユーザーがログオフする時点を報告しません。エージング タイムを使用すると、Cisco ISE で、ユーザーがログインする時間間隔を決定できます。
NTLM プロトコル設定（NTLM Protocol settings）	Cisco ISE と DC の間の通信プロトコルとして [NTLMv1] または [NTLMv2] を選択できます。推奨されるデフォルトは [NTLMv2] です。

その他の パッシブ ID サービス プロバイダ

ISE が ID 情報（パッシブ ID サービス）を、サービスをサブスクライブするコンシューマ（サブスクライバ）に提供できるようにするため、最初に ISE プローブを設定する必要があります。このプローブは ID プロバイダに接続します。

次の表に、ISE で使用可能なすべてのプロバイダとプローブタイプの詳細を示します。Active Directory の詳細については、プローブおよびプロバイダとしての Active Directory （91 ページ）を参照してください。

定義できるプロバイダ タイプを次に示します。

表 *20* : プロバイダ タイプ

プロバイダ タイプ（プローブ）	説明	送信元システム（プロバイダ）	テクノロジー	収集されるユーザー ID 情報	ドキュメント リンク
Active Directory（AD）	ユーザー情報の取得元である安全性が高く正確で最も一般的なソース。 プローブとして機能する場合、AD は WMI テクノロジーを使用して認証済みユーザー ID を送信します。 また AD 自体が、プローブではなく、その他のプローブがユーザー データを取得するソース システム（プロバイダ）として機能します。	Active Directory ドメイン コントローラ	WMI	• ユーザー名（User name） • IP アドレス • ドメイン	プローブおよびプロバイダとしての Active Directory （91 ページ）
エージェント（Agents）	Active Directory ドメイン コントローラまたはメンバー サーバーにインストールされているネイティブ 32 ビット アプリケーション。エージェント プローブは、ユーザー ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。		ドメイン コントローラまたはメンバー サーバーにインストールされているエージェント。	• ユーザー名（User name） • IP アドレス • ドメイン	Active Directory エージェント （101 ページ）
エンドポイント（Endpoint）			WMI	ユーザーが接続しているかどうか	エンドポイント プローブ （138 ページ）

プロバイダ タイプ（プローブ）	説明	送信元システム（プロバイダ）	テクノロジー	収集されるユーザー ID 情報	ドキュメント リンク
	設定されているその他のプローブに加えて、ユーザーが接続しているかどうかを確認するため、常にバックグラウンドで実行されます。				
SPAN	ネットワーク トラフィックをリッスンし、Active Directory データに基づいてユーザー ID 情報を抽出するため、ネットワーク スイッチに導入されています。		SPAN（スイッチにインストール）と Kerberos メッセージ	• ユーザー名（User name） • IP アドレス • ドメイン	SPAN （112 ページ）
API プロバイダ	ISE が提供する RESTful API サービスを使用して、RESTful API クライアントと通信するようにプログラミングされている任意のシステムから、ユーザー ID 情報を収集します。	REST API クライアントと通信するようにプログラミングされている任意のシステム。	RESTful API。JSON 形式でサブスクライバに送信されるユーザー ID。	• ユーザー名（User name） • IP アドレス • ポート範囲（Port range） • ドメイン（Domain）	API プロバイダ （106 ページ）
Syslog	syslog メッセージを解析し、ユーザー ID（MAC アドレスを含む）を取得します。	• 標準 syslog メッセージ プロバイダ • DHCP サーバー	syslog メッセージ	• ユーザー名（User name） • IP アドレス • MAC アドレス • ドメイン	syslog プロバイダ （114 ページ）

（注） pxGrid は、セッショントピックに対して 1 秒あたり 200 イベントを送信して、クライアントのオーバーロードを回避します。パブリッシャが 200 を超えるイベントを送信すると、追加のイベントはキューに入り、次のバッチで送信されます。

pxGrid が長時間にわたって 1 秒あたり 200 を超えるイベントを継続的に受信する場合、バックログイベントを保存するために通常よりも多くのメモリが消費される可能性があり、pxGrid のパフォーマンスに影響を与える場合があります。

Active Directory エージェント

パッシブ ID サービス ワーク センターから、ネイティブ 32 ビット アプリケーション、ドメイン コントローラ（DC）エージェントを、（設定に応じて）Active Directory（AD）ドメイン コントローラ（DC）またはメンバー サーバー上の任意の場所にインストールし、AD からユーザー ID 情報を取得して、設定したサブスクライバにこれらの ID を送信します。エージェント プローブは、ユーザー ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。エージェントは個別のドメインまたは AD ドメインにインストールできます。インストールされたエージェントは、1 分ごとに ISE にステータス更新情報を提供します。

エージェントは ISE が自動的にインストールおよび設定するか、またはユーザーが手動でインストールすることができます。インストールが完了すると、次のようになります。

- エージェントとその関連ファイルはパス **Program Files/Cisco/Cisco ISE PassiveID Agent** にインストールされています。
- エージェントのロギング レベルを指定する **PICAgent.exe.config** という設定ファイルがインストールされます。この設定ファイル内でロギング レベルを手動で変更できます。
- CiscoISEPICAgent.log ファイルにはすべてのロギング メッセージが保存されます。
- nodes.txt ファイルには、展開内でエージェントが通信できるすべてのノードのリストが含まれています。エージェントはリストの最初のノードと通信します。このノードと通信できない場合、エージェントはリストのノード順序に従ってノードとの通信を試行します。手動でのインストールの場合、このファイルを開き、ノード IP アドレスを入力する必要があります。（手動または自動での）インストールの完了後にこのファイルを変更するには、このファイルを手動で更新する必要があります。ファイルを開き、ノード IP アドレスを必要に応じて追加、変更、または削除します。
- Cisco ISE PassiveID Agent サービスはマシン上で稼働します。このサービスは [Windows サービス（Windows Services）] ダイアログボックスから管理できます。
- ISE は最大 100 個のドメイン コントローラをサポートでき、それぞれのエージェントは最大 10 個のドメイン コントローラをモニターできます。100 個のドメイン コントローラをモニターするには、10 個のエージェントを設定する必要があります。
- Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。エージェントをインストールできない場合、パッシブ ID サービスには Active Directory プロー

ブを使用します。詳細については、プローブおよびプロバイダとしての Active Directory（91 ページ）を参照してください。

（注） メンバーサーバーで AD エージェントを実行している場合でも、Active Directory にログイン要求をクエリします。

Active Directory エージェントの自動インストールおよび展開

ユーザー ID についてドメイン コントローラをモニターするようにエージェント プロバイダを設定するときには、エージェントがメンバー サーバーまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE が自動的にインストールするか、またはユーザーが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニターするように設定する必要があります。このプロセスでは、自動インストールを有効にし、ドメイン コントローラをモニターするようにエージェントを設定する方法について説明します。

始める前に

始める前に：

- サーバー側からの関連 DNS サーバーの逆引き参照を設定します。ISE の DNS サーバー設定要件の詳細については、DNS サーバー （48 ページ）を参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/framework を参照してください。
- アクティブなパッシブ ID および pxGrid サービス。詳細については、初期セットアップと設定 （89 ページ）を参照してください。
- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダとしての Active Directory （91 ページ）を参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザー グループを使用します。AD グループの詳細については、Active Directory ユーザー グループの設定 （55 ページ）を参照してください。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダ（Providers）]** を選択し、左側のパネルから **[エージェント（Agents）]** を選択します。

ステップ 2 新しいエージェントを追加するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 新しいエージェントを作成し、この設定で指定するホストに自動的にインストールするには、[新規エージェントの展開（Deploy New Agent）] を選択します。

ステップ 4 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、Active Directory エージェントの設定 （105 ページ）を参照してください。

ステップ 5 [展開（Deploy）] をクリックします。
設定で指定したドメインに基づいてエージェントが自動的にホストにインストールされ、設定が保存されます。エージェントは [エージェント（Agents）] テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 6 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダ（Providers）]** を選択し、左側のパネルから [Active Directory] を選択して、現在設定されているすべての参加ポイントを表示します。

ステップ 7 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 8 前提条件の一部として追加したドメインコントローラを設定するには、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 9 作成したエージェントを使用してモニターするドメインコントローラを選択し、[編集（Edit）] をクリックします。

ステップ 10 [プロトコル（Protocol）] ドロップダウンリストから [エージェント（Agent）] を選択します。

ステップ 11 **作成したエージェントを [エージェント（Agent）]** ドロップダウンリストから選択します。作成したエージェントのユーザー名とパスワードのログイン情報を入力し、**[保存（Save）]** をクリックします。

ユーザー名とパスワードのログイン情報は、ドメインコントローラにエージェントをインストールするために使用されます。最後に、[展開する（Deploy）] をクリックすると、*picagent.exe* が */opt/pbis/bin* から指定した Windows マシンにコピーされます。

Active Directory エージェントの手動インストールおよび展開

ユーザー ID についてドメイン コントローラをモニターするようにエージェント プロバイダを設定するときには、エージェントがメンバー サーバーまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントはISE が自動的にインストールするか、またはユーザーが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニターするように設定する必要があります。このプロセスでは、エージェントを手動でインストールし、ドメイン コントローラをモニターするように設定する方法について説明します。

始める前に

始める前に：

- サーバー側からの関連 DNS サーバーの逆引き参照を設定します。ISE の DNS サーバー設定要件の詳細については、DNS サーバー （48 ページ）を参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/framework を参照してください。
- アクティブなパッシブ ID および pxGrid サービス。詳細については、初期セットアップと設定 （89 ページ）を参照してください。

- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダとしての Active Directory （91 ページ）を参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザー グループを使用します。AD グループの詳細については、Active Directory ユーザー グループの設定 （55 ページ）を参照してください。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダ（Providers）]** を選択し、左側のパネルから **[エージェント（Agents）]** を選択します。

ステップ 2 [エージェントのダウンロード（Download Agent）] をクリックし、手動でインストールするための **`picagent-installer.zip`** ファイルをダウンロードします。
このファイルは Windows の標準ダウンロード フォルダにダウンロードされます。

ステップ 3 ZIP ファイルを指定のホスト マシンに保存してインストールを実行します。

ステップ 4 ISE GUI から **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** をもう一度選択し、左側のパネルから **[エージェント（Agents）]** を選択します。

ステップ 5 新しいエージェントを設定するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 6 すでにホストマシンにインストールしているエージェントを設定するには、[既存のエージェントの登録（Register Existing Agent）] を選択します。

ステップ 7 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、Active Directory エージェントの設定 （105 ページ）を参照してください。

ステップ 8 [保存（Save）] をクリックします。
エージェント設定が保存されます。エージェントは[エージェント（Agents）]テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 9 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、左側のパネルから **[Active Directory]** を選択して、現在設定されているすべての参加ポイントを表示します。

ステップ 10 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 11 前提条件の一部として追加したドメインコントローラを設定するには、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 12 作成したエージェントを使用してモニターするドメインコントローラを選択し、[編集（Edit）]をクリックします。

ステップ 13 [プロトコル（Protocol）] ドロップダウンリストから [エージェント（Agent）] を選択します。

ステップ 14 作成したエージェントを[エージェント（Agent）] ドロップダウンリストから選択します。エージェントに接続するためのユーザー名とパスワードを入力し、[保存（Save）] をクリックします。

ユーザーアカウントには、セキュリティイベントを読み取るために必要な権限が必要です。WMIベースのエージェントのユーザーアカウントには、WMI/DCOM 権限が必要です。

エージェントのアンインストール

自動または手動でインストールされたエージェントは、Windowsから直接（手動で）簡単にアンインストールできます。

ステップ 1 [Windows] ダイアログで [プログラムと機能（Programs and Features）] に移動します。

ステップ 2 インストールされているプログラムのリストで [Cisco ISE PassiveID エージェント（Cisco ISE PassiveID Agent）] を見つけて選択します。

ステップ 3 [アンインストール（Uninstall）] をクリックします。

Active Directory エージェントの設定

ISE が、さまざまなドメイン コントローラ（DC）からユーザー ID 情報を取得し、その情報をパッシブ ID サービス サブスクライバに配信するために、ネットワーク内の指定されたホストにエージェントを自動的にインストールすることを許可します。

エージェントを作成および管理するには、**[プロバイダー（Providers）]** > **[エージェント（Agents）]** を選択します。Active Directory エージェントの自動インストールおよび展開 （102 ページ）を参照してください。

表 *21 : [*エージェント（*Agents*）*]* ウィンドウ

フィールド名	説明
Name	設定したエージェント名。
ホスト（Host）	エージェントがインストールされているホストの完全修飾ドメイン名。
モニターリング（Monitoring）	指定されたエージェントがモニターするドメインコントローラのカンマ区切りリストです。

表 *22 :* 新規エージェント（*Agents New*）

フィールド	説明
新規エージェントの展開（Deploy New Agent）または既存のエージェントの登録（Register Existing Agent）	• 新規エージェントの展開（Deploy New Agent）：指定されたホストに新規エージェントをインストールします。 • 既存のエージェントの登録（Register Existing Agent）：ホストにエージェントを手動でインストールし、パッシブ ID サービス がサービスを有効にできるようにするため、この画面でそのエージェントを設定します。

フィールド	説明
名前（**Name**）	エージェントを容易に把握できる名前を入力します。
説明（**Description**）	エージェントを容易に把握できる説明を入力します。
ホスト **FQDN**（**Host FQDN**）	エージェントがインストールされているホスト(既存のエージェントの登録の場合）またはインストールされるホスト（自動展開の場合）の完全修飾ドメイン名です。
ユーザー名（**User Name**）	エージェントをインストールするホストにアクセスするためのユーザー名を入力します。パッシブ ID サービスはこれらのクレデンシャルを使用してエージェントを自動的にインストールします。 ユーザーアカウントには、リモートで接続して PIC エージェントをインストールするための権限が必要です。
パスワード	エージェントをインストールするホストにアクセスするためのパスワードを入力します。パッシブ ID サービスはこれらのクレデンシャルを使用してエージェントを自動的にインストールします。

API プロバイダ

Cisco ISE の API プロバイダ機能では、カスタマイズしたプログラムまたはターミナル サーバー（TS）エージェントから組み込み ISE パッシブ ID サービス REST API サービスにユーザー ID 情報をプッシュできます。これにより、ネットワークからプログラミング可能なクライアントをカスタマイズして、任意のネットワーク アクセス制御（NAC）システムから収集されたユーザー ID をこのサービスに送信するようにできます。さらに Cisco ISE API プロバイダにより、すべてのユーザーの IP アドレスが同一であるが、各ユーザーに固有のポートが割り当てられるネットワーク アプリケーション（Citrix サーバーの TS-Agent など）と対話できます。

たとえば、Active Directory（AD）サーバーに対して認証されたユーザーの ID マッピングを提供する Citrix サーバーで稼働するエージェントは、新しいユーザーがログインまたはログオフするたびに、ユーザー セッションを追加または削除する REST 要求を ISE に送信できます。ISE は、クライアントから送信されたユーザー ID 情報（IP アドレス、割り当てられたポートなど）を取得し、事前に設定されているサブスクライバ（Cisco Firepower Management Center（FMC）など）に送信します。

ISE REST API フレームワークは、HTTPS プロトコルを介した REST サービスを実装し（クライアント証明書の検証は不要）、ユーザー ID 情報が JSON（JavaScript Object Notation）形式で送信されます。JSON の詳細については、http://www.json.org/ を参照してください。

ISE REST API サービスは、1 つのシステムに同時にログインしている複数のユーザーを区別するため、ユーザー ID を解析し、その情報をポート範囲にマッピングします。ポートがユーザーに割り当てられるたびに、API がメッセージを ISE に送信します。

REST API プロバイダのフロー

カスタマイズしたクライアントを ISE のプロバイダとして宣言し、そのカスタマイズした特定のプログラム（クライアント）が RESTful 要求を送信できるようにして、ISE からカスタマイズしたクライアントへのブリッジを設定している場合、ISE REST サービスは次のように機能します。

1. Cisco ISE はクライアント認証のために認証トークンを必要とします。通信開始時と、ISE から以前のトークンの期限が切れたことが通知されるたびに、クライアントマシンのカスタマイズしたプログラムから認証トークンを求める要求が送信されます。この要求への応答としてトークンが返されます。これによりクライアントと ISE サービス間の継続的な通信が可能になります。
2. ユーザーがネットワークにログインすると、クライアントはユーザー ID 情報を取得し、API Add コマンドを使用してこの情報を ISE REST サービスに送信します。
3. Cisco ISE はユーザー ID 情報を受信してマッピングします。
4. Cisco ISE はマッピングされたユーザー ID 情報をサブスクライバに送信します。
5. 必要な場合は常に、カスタマイズされたマシンはユーザー情報削除要求を送信できます。このためには、Remove API コールを送信し、Add コールの送信時に応答として受信したユーザー ID を含めます。

ISE での REST API プロバイダの操作

ISE で REST サービスをアクティブにするには、次の手順に従います。

1. クライアント側を設定します。詳細については、クライアント ユーザー マニュアルを参照してください。
2. パッシブ ID サービスと pxGrid サービスをアクティブにします。詳細については、初期セットアップと設定 （89 ページ）を参照してください。
3. DNS サーバーを適切に設定していることを確認します。これには、ISE からのクライアント マシンの逆引きの設定も含まれます。 の DNS サーバー設定要件の詳細については、DNS サーバー （48 ページ）を参照してください。
4. パッシブ ID サービス の ISE REST サービスへのブリッジの設定 （108 ページ）を参照してください。

（注） TS-Agent と連携するように API プロバイダを設定するには、ISE からそのエージェントへのブリッジの作成時に TS-Agent 情報を追加します。その後、TS-Agent のマニュアルで API コールの送信について確認してください。

5. 認証トークンを生成し、追加要求と削除要求を API サービスに送信します。

パッシブ ID サービス の ISE REST サービスへのブリッジの設定

ISE REST API サービスが特定のクライアントから情報を受信できるようにするには、まず Cisco ISE でその特定のクライアントを定義する必要があります。異なる IP アドレスを使用して複数の REST API クライアントを定義できます。

始める前に

始める前に：

- パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。詳細については、初期セットアップと設定 （89 ページ）を参照してください。
- DNS サーバーを適切に設定していることを確認します。これには、Cisco ISE からのクライアントマシンの逆引きの設定も含まれます。Cisco ISE の DNS サーバー設定要件の詳細については、DNS サーバー （48 ページ）を参照してください。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダ（Providers）]** を選択し、次に左側のパネルから [API プロバイダ（API Providers）] を選択します。
[API プロバイダ（API Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しいクライアントを追加するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、API プロバイダの設定 （109 ページ）を参照してください。

ステップ 4 [送信（Submit）] をクリックします。
クライアント設定が保存され、更新された [API プロバイダ（API Providers）] テーブルが画面に表示されます。これで、クライアントは ISE REST サービスにポストを送信できるようになりました。

次のタスク

認証トークンとユーザー ID を ISE REST サービスに送信するように、カスタマイズしたクライアントをセットアップします。パッシブ ID REST サービスへの API コールの送信 （109 ページ） を参照してください。

パッシブ ID REST サービスへの API コールの送信

始める前に

パッシブ ID サービス の ISE REST サービスへのブリッジの設定 （108 ページ）

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

ステップ 2 [API プロバイダ（API Providers）] ウィンドウで指定および設定したユーザー名とパスワードを入力します。詳細については、パッシブ ID サービス の ISE REST サービスへのブリッジの設定 （108 ページ）を参照してください。

ステップ 3 Enter キーを押します。

ステップ 4 ターゲットノードの [URL アドレス（URL Address）] フィールドに API コールを入力します。

ステップ 5 [送信（Send）] をクリックして API コールを発行します。

次のタスク

さまざまな API コールとそのスキーマおよび結果の詳細については、API コール （110 ページ）を参照してください。

API プロバイダの設定

（注） 次のようにリクエスト コールを使用して完全な API 定義とオブジェクト スキーマを取得できます。

- 完全な API の指定（wadl）：https://YOUR_ISE:9094/application.wadl
- API モデルとオブジェクト スキーマ：https://YOUR_ISE:9094/application.wadl/xsd0.xsd

表 *23 : API* プロバイダの設定

フィールド	説明
名前	このクライアントを他のクライアントから容易に区別できる一意の名前を入力します。
説明（Description）	このクライアントのわかりやすい説明を入力します。
ステータス（Status）	設定完了後すぐにクライアントが REST サービスとやりとりできるようにするには、[有効（Enabled）] を選択します。

フィールド	説明
ホスト/IP（Host/ IP）	クライアント ホスト マシンの IP アドレスを入力します。DNS サーバーを適切に設定していることを確認します。これには、ISEからのクライアント マシンの逆引きの設定も含まれます。
ユーザー名（User name）	REST サービスへの送信時に使用する一意のユーザー名を作成します。
パスワード（Password）	REST サービスへの送信時に使用する一意のパスワードを作成します。

API コール

Cisco ISE で パッシブ ID サービスのユーザー ID イベントを管理するには、次の API コールを使用します。

目的：認証トークンの生成

- **要求**

  POST

  https://<PIC IP アドレス>:9094/api/fmi_platform/v1/identityauth/generatetoken

  要求には BasicAuth 認証ヘッダーが含まれている必要があります。ISE-PIC GUI から以前に作成した API プロバイダのログイン情報を入力します。詳細については、API プロバイダの設定 （109 ページ）を参照してください。

- **応答ヘッダー**

  このヘッダーには X-auth-access-token が含まれています。これは、追加の REST 要求を送信するときに使用するトークンです。

- **応答本文**

  HTTP 204 No Content

目的：ユーザーの追加

- **要求**

  POST

  https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity

  POST 要求のヘッダーに X-auth-access-token を追加します（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）。

- **応答ヘッダー**

201 Created

- **応答本文**

{

"user": "<ユーザー名>",

"srcPatRange": {

"userPatStart": <ユーザー PAT 開始値>,

"userPatEnd": <ユーザー PAT 終了値>,

"patRangeStart": <PAT 範囲開始値>

},

"srcIpAddress": "<src IP アドレス>",

"agentInfo": "<エージェント名>",

"timestamp": "<ISO_8601 形式、例：“YYYY-MM-DDTHH:MM:SSZ" >",

"domain": "<ドメイン>"

}

- **注記**
  - 上記の JSON で 1 つの IP ユーザー バインディングを作成するには srcPatRange を削除します。
  - 応答本文には「ID」（作成されたユーザーセッションバインディングの固有識別子）が含まれています。削除するユーザーを指定する DELETE 要求を送信するときに、この ID を使用してください。
  - この応答には、新たに作成されたユーザー セッション バインディングの URL であるセルフ リンクも含まれています。

目的：ユーザーの削除

- **要求**

DELETE

https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity/<id>

<id> に、Add 応答で受信した ID を入力します。

DELETE 要求のヘッダーに X-auth-access-token を追加します（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）。

- **応答ヘッダー**

200 OK

- **応答本文**

応答本文には、削除されたユーザーセッションバインディングの詳細が含まれています。

SPAN

SPAN は、Cisco ISE がネットワークをリッスンし、ユーザー情報を取得できるようにユーザーが容易に設定できるようにする、パッシブ ID サービスです。このとき、Active Directory が Cisco ISE と直接連携するように設定する必要はありません。SPAN はネットワーク トラフィックをスニフィングし、特に Kerberos メッセージを調べ、Active Directory により保存されているユーザー ID 情報を抽出し、その情報を ISE に送信します。ISE は次にその情報を解析し、最終的にはユーザー名、IP アドレス、およびドメイン名を、ISE からすでに設定しているサブスクライバに送信します。

SPAN がネットワークをリッスンし、Active Directory ユーザー情報を抽出できるようにするには、ISE と Active Directory の両方がネットワーク上の同一スイッチに接続している必要があります。これにより、SPAN は Active Directory からすべてのユーザー ID データをコピーおよびミラーリングできます。

SPAN により、ユーザー情報は次のように取得されます。

1. ユーザーエンドポイントがネットワークにログインします。
2. ログイン データとユーザー データは Kerberos メッセージに保存されます。
3. ユーザーがログインし、ユーザーデータがスイッチを通過すると、SPAN がネットワークデータをミラーリングします。
4. Cisco ISE は、ユーザー情報を取得するためネットワークをリッスンし、ミラーリングされたデータをスイッチから取得します。
5. Cisco ISE はユーザー情報を解析し、パッシブ ID マッピングを更新します。
6. Cisco ISE は解析後のユーザー情報をサブスクライバに送信します。

SPAN の使用

始める前に

ISE がネットワーク スイッチから SPAN トラフィックを受信できるようにするには、最初にそのスイッチをリッスンするノードとノードインターフェイスを定義する必要があります。インストールされている複数の ISE ノードをリッスンするには、SPAN を設定します。ネットワークをリッスンするように設定できるインターフェイスは、ノードごとに 1 つのみです。また、リッスンするために使用するインターフェイスは SPAN 専用である必要があります。

開始する前に、パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。SPAN の設定に使用可能なインターフェイスのリストには、パッシブ ID が有効なノードだけが表示されます。詳細については、初期セットアップと設定 （89 ページ）を参照してください。

また、次の操作を行う必要があります。

- ネットワークで Active Directory が設定されていることを確認します。
- スイッチが ISE と通信できることを確認するために、Active Directory に接続しているネットワーク上のスイッチで CLI を実行します。
- AD からネットワークをミラーリングするようにスイッチを設定します。
- SPAN 専用の ISE ネットワーク インターフェイス カード（NIC）を設定します。この NIC は SPAN トラフィック専用で使用されます。
- SPAN 専用の NIC が、コマンドライン インターフェイスからアクティブにされていることを確認します。
- Kerberos トラフィックのみを SPAN ポートに送信する VACL を作成します。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダー（Providers）]** を選択し、次に左側のパネルから **[SPAN]** を選択して SPAN を設定します。

ステップ 2 （注） GigabitEthernet0 ネットワーク インターフェイス カード（NIC）は使用可能なままにし、SPAN の設定には使用可能な別の NIC を選択することを推奨します。GigabitEthernet0 は、システム管理の目的で使用されます。

わかりやすい説明を入力し（オプション）、[有効（Enabled）] ステータスを選択し、ネットワーク スイッチのリッスンに使用する関連 NIC とノードを選択します。詳細については、SPAN 設定 （113 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックします。
SPAN 設定が保存され、ISE-PIC ISE がネットワーク トラフィックをアクティブにリッスンします。

SPAN 設定

SPAN をクライアント ネットワークにインストールすることで、展開した各ノードから、 ISE がユーザー ID を受信することを簡単に設定できます。

表 *24 : SPAN* 設定

フィールド	説明
説明（**Description**）	現在有効なノードとインターフェイスがわかる固有の説明を入力します。
ステータス（**Status**）	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。

フィールド	説明
インターフェイス NIC（**Interface NIC**）	ISE にインストールされている 1 つ以上のノードを選択してから、選択したノードごとに、ネットワークをリッスンして情報を得るノード インターフェイスを選択します。 （注） GigabitEthernet0 NIC を引き続き使用可能にし、SPAN の設定には他の使用可能な NIC を選択することを推奨します。GigabitEthernet0 は、システム管理の目的で使用されます。

syslog プロバイダ

パッシブ ID サービスは syslog メッセージを配信する任意のクライアント（ID データプロバイダ）からの syslog メッセージを解析し、MAC アドレスなどのユーザー ID 情報を送信します。syslog メッセージには、通常の syslog メッセージ（InfoBlox、Blue Coat、BlueCat、Lucent などのプロバイダからのメッセージ）と DHCP syslog メッセージがあります。このマッピングされたユーザー ID データがサブスクライバに配信されます。

ユーザー ID データを受信する syslog クライアントを指定できます（syslog クライアントの設定 （115 ページ）を参照）。プロバイダの設定時に、接続方法（TCP または UDP）および解析に使用する syslog テンプレートを指定する必要があります。

（注） 設定されている接続タイプが TCP であり、メッセージヘッダーに問題があるためにホスト名を解析できない場合、 ISE はパケットで受信した IP アドレスを、ISE で設定されている syslog メッセージのプロバイダリストにあるすべてのプロバイダの IP アドレスと照合しようとします。このリストを表示するには、**[ワーク センター（Work Centers）] > [パッシブ ID（Passive ID）] > [プロバイダ（Providers）] > [syslog プロバイダ（Syslog Providers）]** を選択します。メッセージヘッダーを確認し、必要に応じて、解析が正常に実行されるようにカスタマイズすることをお勧めします。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （122 ページ） を参照してください。

syslog プローブが受信した syslog メッセージを ISE パーサーに送信します。パーサーはユーザー ID 情報をマッピングし、その情報を ISE に公開します。次に ISE が、解析およびマッピングされたユーザー ID 情報を パッシブ ID サービス サブスクライバに配信します。

ISE-PIC ISE からの syslog メッセージを解析してユーザー ID を取得するには、次の手順を実行します。

- ユーザー ID データの送信元 syslog クライアントを設定します。syslog クライアントの設定 （115 ページ）を参照してください。
- 1 つのメッセージヘッダーをカスタマイズします。syslog ヘッダーのカスタマイズ （122 ページ）を参照してください。

- テンプレートを作成してメッセージ本文をカスタマイズします。syslog メッセージ本文のカスタマイズ （120 ページ）を参照してください。
- 解析に使用するメッセージテンプレートとして syslog クライアントを設定する場合には、ISE で事前に定義されているメッセージテンプレートを使用します。あるいは、これらの事前に定義されたテンプレートに基づいてヘッダーまたは本文のテンプレートをカスタマイズします。Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照してください。

syslog クライアントの設定

Cisco ISE が特定のクライアントからの syslog メッセージをリッスンできるようにするには、最初に Cisco ISE でそのクライアントを定義する必要があります。異なる IP アドレスを使用して複数のプロバイダを定義できます。

始める前に

開始する前に、パッシブ ID サービスと pxGrid サービスをアクティブにしていることを確認します。詳細については、初期セットアップと設定 （89 ページ）を参照してください。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダ（Providers）]** を選択し、次に左側のパネルから [syslog プロバイダ（Syslog Providers）] を選択します。
[syslog プロバイダ（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを設定するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドを入力し（詳細についてはSyslog の設定 （115 ページ）を参照）、必要に応じてメッセージテンプレートを作成します（詳細についてはsyslog メッセージ本文のカスタマイズ （120 ページ）を参照）。

ステップ 4 **[送信（Submit）]** をクリックします。

Syslog の設定

特定のクライアントからの syslog メッセージを介してユーザー ID（MAC アドレスを含む）を受信するように Cisco ISE を設定します。異なる IP アドレスを使用して複数のプロバイダを定義できます。

表 25 : syslog プロバイダ

フィールド名	説明
Name	設定したこのクライアントを容易に区別できる一意の名前を入力します。
説明（Description）	この syslog プロバイダのわかりやすい説明。

フィールド名	説明
ステータス（Status）	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。
Host	ホスト マシンの FQDN を入力します。
接続タイプ（Connection Type）	ISE が syslog メッセージをリッスンするチャネルを指定するため、UDP または TCP を入力します。 （注） TCP が設定されている接続タイプである場合で、メッセージヘッダーとホスト名が解析できない問題がある場合は、Cisco ISE は syslog メッセージに設定されているプロバイダのリストにあるいずれかのプロバイダの IP アドレス宛のパケットで受信した IP アドレスと照合しようとします。 このリストを表示するには、**[ワークセンター（Work Centers）] > [パッシブ ID（Passive ID）] > [プロバイダ（Providers）] > [syslog プロバイダ（Syslog Providers）]** を選択します。メッセージヘッダーを確認し、必要に応じて、解析が正常に実行されるようにカスタマイズすることをお勧めします。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （122 ページ）を参照してください。

フィールド名	説明
テンプレート（**Template**）	

フィールド名	説明
	テンプレートにより正確な本文メッセージ構造が指定されます。これにより、パーサーは syslog メッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。 たとえば、テンプレートでは正確なユーザー名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザー名を検出できます。 このフィールドでは、syslog メッセージを認識して正しく解析するために使用される（syslog メッセージの本文の）テンプレートを指定します。 事前定義のドロップダウンリストから選択するか、または [新規（New）] をクリックして独自のカスタム テンプレートを作成します。新しいテンプレートの作成の詳細については、syslog メッセージ本文のカスタマイズ （120 ページ）を参照してください。ほとんどの事前定義テンプレートでは正規表現が使用されています。カスタム テンプレートでも正規表現を使用する必要があります。 （注） 編集または削除できるのはカスタム テンプレートだけであり、ドロップダウンの事前定義システム テンプレートは変更できません。 現在 ISE に含まれている事前定義 DHCP プロバイダ テンプレートを次に示します。 • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP （注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより Cisco ISE はユーザー ID 情報を正しく解析して配信するために、最初

フィールド名	説明
	にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合しようとします。 DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。 Cisco ISE には次の事前定義の標準 syslog プロバイダテンプレートがあります。 • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN テンプレートについては、Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照してください。
デフォルト ドメイン（**Default Domain**）	syslog メッセージで特定のユーザーに対してドメインが指定されていない場合、このデフォルト ドメインが自動的にそのユーザーに割り当てられます。これにより、すべてのユーザーにドメインが割り当てられます。 デフォルト ドメインまたはメッセージから解析されたドメインにユーザー名が付加され、username@domain となります。したがって、ユーザーとユーザーグループに関する詳細情報を取得するためには、ドメインを含めます。

syslog メッセージ構造のカスタマイズ（テンプレート）

テンプレートは正確なメッセージ構造を指定します。これにより、パーサーはsyslogメッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。たとえば、テンプレートでは正確なユーザー名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザー名を検出できます。テンプレートにより、新規マッピングメッセージとマッピング削除メッセージの両方に対応する構造が決定します。

Cisco ISE では、パッシブ ID パーサーが使用する 1 つのメッセージ ヘッダーと複数の本文構造をカスタマイズできます。

パッシブ ID パーサーが、メッセージがユーザー ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザーの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザー名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

メッセージテンプレートをカスタマイズするときに、事前定義オプションで使用されている正規表現とメッセージ構造を調べ、ISE-PICISE の事前定義メッセージ テンプレートに基づいてカスタマイズを行うかどうかを決定できます。事前定義テンプレートの正規表現、メッセージ構造、例などの詳細については、Syslog事前定義メッセージテンプレートの使用 （126ページ）を参照してください。

次の内容をカスタマイズできます。

- 1 つのメッセージ ヘッダー：syslog ヘッダーのカスタマイズ （122 ページ）
- 複数のメッセージ本文：syslog メッセージ本文のカスタマイズ （120 ページ）。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより Cisco ISE は ユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）]で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合しようとします。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

DHCP メッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCP メッセージ テンプレートをカスタマイズすることは推奨されません。代わりに、事前定義の DHCP テンプレートを使用してください。

syslog メッセージ本文のカスタマイズ

Cisco ISE では、パッシブ ID パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます（メッセージ本文のカスタマイズ）。テンプレートには、ユーザー名、IP ア

ドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE はユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

DHCP メッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCP メッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義の DHCP テンプレートを使用してください。

syslog クライアント設定画面から、syslog メッセージ本文テンプレートを作成および編集します。

（注） 各自でカスタマイズしたテンプレートだけを編集できます。システムに用意されている事前定義テンプレートは変更できません。

ステップ 1 **[ワークセンター（Work Centers）]** > **[PassiveID]** > **[プロバイダ（Providers）]** を選択し、次に左側のパネルから [syslog プロバイダ（Syslog Providers）] を選択します。
[syslog プロバイダ（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを追加するには [追加（Add）] をクリックし、すでに設定されているクライアントを更新するには [編集（Edit）] をクリックします。syslog クライアントの設定と更新については、syslog クライアントの設定 （115 ページ）を参照してください。

ステップ 3 [syslog プロバイダ（Syslog Providers）] ウィンドウで、[新規（New）] をクリックして新しいメッセージテンプレートを作成します。既存のテンプレートを編集するには、ドロップダウンリストからテンプレートを選択して [編集（Edit）] をクリックします。

ステップ 4 必須フィールドをすべて指定します。

値を正しく入力する方法の詳細については、syslog カスタマイズ テンプレートの設定と例 （123 ページ）を参照してください。

ステップ 5 [テスト（Test）] をクリックして、入力した文字列に基づいてメッセージが正しく解析されていることを確認します。

ステップ 6 [保存（Save）] をクリックします。

syslog ヘッダーのカスタマイズ

syslog ヘッダーには、メッセージの送信元のホスト名も含まれています。syslog メッセージが Cisco ISE メッセージパーサーで認識されない場合は、ホスト名の後に続く区切り文字を設定し、Cisco ISE がホスト名を認識してメッセージを正しく解析できるようにすることで、メッセージヘッダーをカスタマイズする必要がある場合があります。この画面のフィールドの詳細については、syslog カスタマイズテンプレートの設定と例（123 ページ）を参照してください。カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダー タイプにこの設定が追加されます。

（注） 1 つのヘッダーだけをカスタマイズできます。ヘッダーをカスタマイズした後、[カスタムヘッダー（Custom Header）] をクリックしてテンプレートを作成すると、最新の設定のみが保存されます。

ステップ 1 **[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダ（Providers）]** を選択し、次に左側のパネルから [syslog プロバイダ（Syslog Providers）] を選択します。
[syslog プロバイダ（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 [カスタム ヘッダー（Custom Header）] をクリックして [syslog カスタム ヘッダー（Syslog Custom Header）] 画面を開きます。

ステップ 3 [サンプル syslog を貼り付ける（Paste sample syslog）] に、syslog メッセージのヘッダー形式の例を入力します。たとえば、メッセージの 1 つからヘッダー **`<181>Oct 10 15:14:08 Cisco.com`** をコピーして貼り付けます。

ステップ 4 [区切り文字（Separator）] フィールドで、単語をスペースとタブのいずれで区切るかを指定します。

ステップ 5 [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドで、ヘッダーのどの位置がホスト名であるかを指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。

[ホスト名（Hostname）] フィールドに、最初の 3 つのフィールドに示される詳細情報に基づいてホスト名が表示されます。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。

<181>Oct 10 15:14:08 Cisco.com

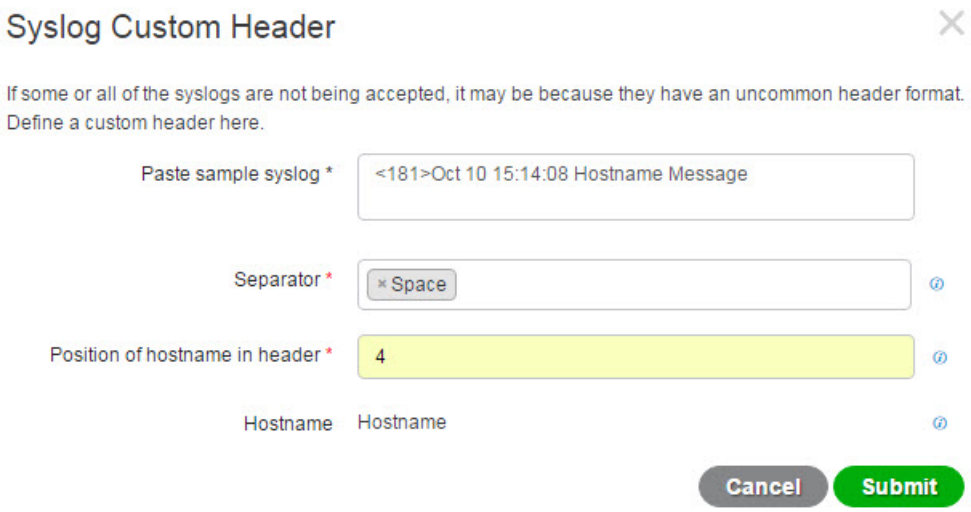
区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。

[ホスト名（Hostname）] には自動的に Cisco.com と表示されます。これは、[syslog の例を貼り付ける（Paste sample syslog）] フィールドに貼り付けたヘッダー フレーズの 4 番目の単語です。

ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

この例を次のスクリーン キャプチャに示します。

図 *14 : syslog* ヘッダーのカスタマイズ



ステップ 6 [送信（Submit）] をクリックします。
カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダータイプにこの設定が追加されます。

syslog カスタマイズ テンプレートの設定と例

Cisco ISE では、パッシブ ID パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます。カスタマイズされたテンプレートは、新規マッピング メッセージとマッピング削除メッセージの両方に対応する構造を決定します。パッシブ ID パーサーが、メッセージがユーザー ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザーの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザー名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されます。カスタマイズテンプレートでも正規表現を使用してください。

syslog ヘッダーの各部分

ホスト名の後に続く区切り文字を設定することで、syslog プローブが認識する単一ヘッダーをカスタマイズできます。

次の表に、カスタムsyslogヘッダーに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 28 : カスタマイズ テンプレートの正規表現（126 ページ）を参照してください。

表 *26 : syslog* カスタム ヘッダー

フィールド	説明
syslog の例を貼り付ける（Paste sample syslog）	syslog メッセージにヘッダー形式の例を入力します。たとえば、次のヘッダーをコピーして貼り付けます。 `<181>Oct 10 15:14:08 Hostname Message`
区切り文字（Separator）	単語をスペースまたはタブのいずれで区切るかを指定します。
ヘッダーのホスト名の位置（Position of hostname in header）	ヘッダーでのホスト名の位置を指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。
ホストネーム	最初の 3 つのフィールドに示される詳細情報に基づいて、ホスト名を表示します。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。 <181>Oct 10 15:14:08 Hostname Message 区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。 [ホスト名（Hostname）] には Hostname が自動的に表示されます。 ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

メッセージ本文の syslog テンプレートの各部分と説明

次の表に、カスタマイズ syslog メッセージ テンプレートに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 28 : カスタマイズ テンプレートの正規表現 （126 ページ）を参照してください。

表 *27 : syslog* テンプレート

パート	フィールド	説明
	名前	このテンプレートの目的がわかる一意の名前。
マッピング操作	新規マッピング	新しいユーザーを追加するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、F5 VPN にログインした新しいユーザーを示すには、このフィールドに「logged on from」と入力します。
	削除されたマッピング	ユーザーを削除するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、削除する必要がある ASA VPN のユーザーを示すには、このフィールドに「session disconnect」と入力します。
ユーザーデータ	IPアドレス	キャプチャする IP アドレスを示す正規表現。 たとえば Bluecat メッセージの場合、この IP アドレス範囲内のユーザーの ID をキャプチャするには、次のように入力します。 (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))
	ユーザー名	キャプチャするユーザー名形式を示す正規表現。
	ドメイン	キャプチャするドメインを示す正規表現。
	MAC アドレス	キャプチャする MAC アドレスの形式を示す正規表現。

正規表現の例

メッセージを解析するため、正規表現を使用します。ここでは、IPアドレス、ユーザー名、およびマッピング追加メッセージを解析する正規表現の例を示します。

たとえば、正規表現を使用して次のメッセージを解析します。

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

次の表に、正規表現の定義を示します。

表 *28*：カスタマイズ テンプレートの正規表現

パート	正規表現
IP アドレス	Address <([^\s]+)>|address ([^\s]+)
ユーザー名（User name）	User <([^\s]+)>| Username = ([^\s]+)
マッピング追加メッセージ（Add mapping message）	(%ASA-4-722051|%ASA-6-713228)

Syslog 事前定義メッセージテンプレートの使用

syslog メッセージには、ヘッダーとメッセージ本文を含む標準構造があります。

ここでは、メッセージの送信元に基づいてサポートされているヘッダーの内容の詳細や、サポートされている本文の構造など、Cisco ISE が提供する事前定義テンプレートについて説明します。

また、システムで事前に定義されていないソース用に、カスタマイズした本文コンテンツを使用した独自のテンプレートも作成できます。ここでは、カスタムテンプレートでサポートされる構造について説明します。メッセージの解析時には、システムで事前定義されているヘッダーに加えて、使用する 1 つのカスタマイズヘッダーを設定できます。また、メッセージ本文には、複数のカスタマイズテンプレートを設定できます。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ（122 ページ）を参照してください。本文のカスタマイズの詳細については、syslog メッセージ本文のカスタマイズ（120 ページ）を参照してください。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されており、カスタマイズテンプレートでも正規表現を使用する必要があります。

メッセージ ヘッダー

パーサーで認識されるヘッダータイプには、すべてのクライアントマシンのすべてのメッセージタイプ（新規および削除）について認識される 2 つのタイプがあります。これらのヘッダーは次のとおりです。

- <171>Host message
- <171>Oct 10 15:14:08 Host message

受信されたヘッダーはホスト名を検出するため解析されます。ホスト名は、IPアドレス、ホスト名、または完全 FQDN のいずれかです。

ヘッダーもカスタマイズできます。ヘッダーをカスタマイズするには、syslog ヘッダーのカスタマイズ （122 ページ）を参照してください。

syslog ASA VPN 事前定義テンプレート

ASA VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

本文メッセージ	解析例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	

本文メッセージ	解析例
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] （注） このメッセージタイプから解析されるIPアドレスは、メッセージに示されているようにプライベートIPアドレスです。
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] （注） このメッセージタイプから解析されたIPアドレスはIPv4アドレスです。

マッピング削除本文メッセージ

ここではパーサーでASA VPNのためにサポートされているマッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,10.1.1.1]

本文メッセージ
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.

本文メッセージ
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

syslog Bluecat 事前定義テンプレート

Bluecat でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング本文メッセージ

ここでは、Bluecat syslog で新規マッピングとしてサポートされるメッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

本文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

マッピング削除メッセージ

Bluecat のマッピング削除メッセージはありません。

syslog F5 VPN 事前定義テンプレート

F5 VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな F5 VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[user=UserA,ip=172.16.0.12]

本文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

マッピング削除メッセージ

現在、F5 VPN でサポートされている削除メッセージはありません。

syslog Infoblox 事前定義テンプレート

Infoblox でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

本文メッセージ
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

マッピング削除メッセージ

受信された本文が解析され、次のようにユーザーの詳細が判明します。

- MAC アドレスが含まれている場合：

  [00:0c:29:a2:18:34,10.0.10.100]

- MAC アドレスが含まれていない場合：

  [10.0.10.100]

本文メッセージ
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

syslog Linux DHCPd3 事前定義テンプレート

Linux DHCPd3 でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング メッセージ

次の表では、パーサーが認識するさまざまな Linux DHCPd3 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

マッピング削除本文メッセージ

ここではパーサーで Linux DHCPd3 のためにサポートされているマッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[00:0c:29:a2:18:34 ,10.0.10.100]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

syslog MS DHCP 事前定義テンプレート

MS DHCP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな MS DHCP 本文メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0

マッピング削除本文メッセージ

ここではパーサーで MS DHCP のためにサポートされているマッピング削除メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

syslog SafeConnect NAC 事前定義テンプレート

SafeConnect NAC でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな SafeConnect NAC 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

本文メッセージ
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

マッピング削除メッセージ

現在、Safe Connect でサポートされている削除メッセージはありません。

syslog Aerohive 事前定義テンプレート

Aerohive でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Aerohive 本文メッセージについて説明します。

本文で解析される詳細には、ユーザー名と IP アドレスがあります。解析に使用される正規表現の例を次に示します。

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,10.5.50.52]

本文メッセージ
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

マッピング削除メッセージ

現在、Aerohive からのマッピング削除メッセージはサポートされていません。

syslog Blue Coat 事前定義テンプレート：Main Proxy、Proxy SG、Squid Web Proxy

Blue Coat の次のメッセージ タイプがサポートされています。

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

BlueCoat メッセージでサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Blue Coat 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,192.168.10.24]

本文メッセージ（この例は、**BlueCoat** プロキシ **SG** メッセージからの引用です）
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

次の表では、新規マッピング メッセージに使用されるクライアント別の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:){1,7}[a-zA-Z0-9]{1,}| ユーザー名（User name） **\s\-\s([a-zA-Z0-9_]+)\s\-\s**
BlueCoat Proxy SG	新規マッピング **(\-\sPROXIED){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:){1,7}[a-zA-Z0-9]{1,}|[a-zA-Z0-9_]+\s-** ユーザー名（User name） **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid Web Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:){1,7}[a-zA-Z0-9]{1,}|TCP** ユーザー名（User name） **\s([a-zA-Z0-9\._]+)\s\-\/**

マッピング削除メッセージ

Blue Coat クライアントではマッピング削除メッセージがサポートされていますが、現在利用できる例はありません。

次の表では、マッピング削除メッセージに使用されるクライアント別の既知の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	現在利用できる例はありません。
BlueCoat Squid Web Proxy	**(TCP_MISS|TCP_NC_MISS){1}**

syslog ISE および ACS 事前定義テンプレート

パーサーは ISE または ACS クライアントをリッスンするときに、次のメッセージ タイプを受信します。

- 認証成功：ユーザーが ISE または ACS により認証されると、認証が成功したことを通知し、ユーザーの詳細情報を記述した認証成功メッセージが発行されます。このメッセージが解析され、このメッセージのユーザーの詳細とセッション ID が保存されます。
- アカウンティング開始およびアカウンティング更新メッセージ（新規マッピング）：アカウンティング開始メッセージまたはアカウンティング更新メッセージは、認証成功メッセージから保存されたユーザーの詳細とセッション ID を使用して解析され、ユーザーがマッピングされます。
- アカウンティング終了（マッピング削除）：システムからユーザーマッピングが削除されます。

ISE および ACS でサポートされる syslog メッセージの形式とタイプについて説明します。

認証成功メッセージ

認証成功メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- **解析例**

  ユーザー名とセッション ID だけが解析されます。

  [UserA,5]

アカウンティング開始/更新（新規マッピング）メッセージ

新規マッピング メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザー名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

マッピング削除メッセージ

マッピング削除では次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザー名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

syslog Lucent QIP 事前定義テンプレート

Lucent QIP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （126 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまなLucent QIP本文メッセージについて説明します。

これらのメッセージの正規表現構造を次に示します。

DHCP_GrantLease|:DHCP_RenewLease

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[00:0C:29:91:2E:5D,10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

マッピング削除本文メッセージ

これらのメッセージの正規表現構造を次に示します。

Delete Lease:|DHCP Auto Release:

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

パッシブ ID サービスのフィルタリング

特定のユーザーを名前やIPアドレスに基づいてフィルタリングできます。たとえばITサービスの管理者が、そのエンドポイントの標準ユーザーを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して[ライブセッション（Live Sessions）]に表示されないようにし、そのエンドポイントの標準ユーザーだけが表示されるようにできます。[ライブ セッション（Live Session）] には、マッピング フィルタでフィルタリングされていないパッシブ ID サービス コンポーネントが表示されます。フィルタは必要なだけ追加できます。「OR」論理演算子をフィルタの間に適用します。両方のフィールドを 1 つのフィルタで指定する場合は、「AND」論理演算子をこれらのフィールドの間に適用します。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[プロバイダ（Providers）]** を選択し、左側のパネルから [マッピング フィルタ（Mapping Filters）] を選択します。

ステップ 2 **[プロバイダ（Providers）]** > **[マッピング フィルタ（Mapping Filters）]** を選択します。

ステップ 3 [追加（Add）] をクリックし、フィルタするユーザーのユーザー名や IP アドレスを入力して、[送信（Submit）] をクリックします。

ステップ 4 現在モニターリング セッション ディレクトリにログインしてしているフィルタリングされていないユーザーを表示するには、**[操作（Operations）]** > **[RADIUSライブログ（RADIUS Livelog）]** を選択します。

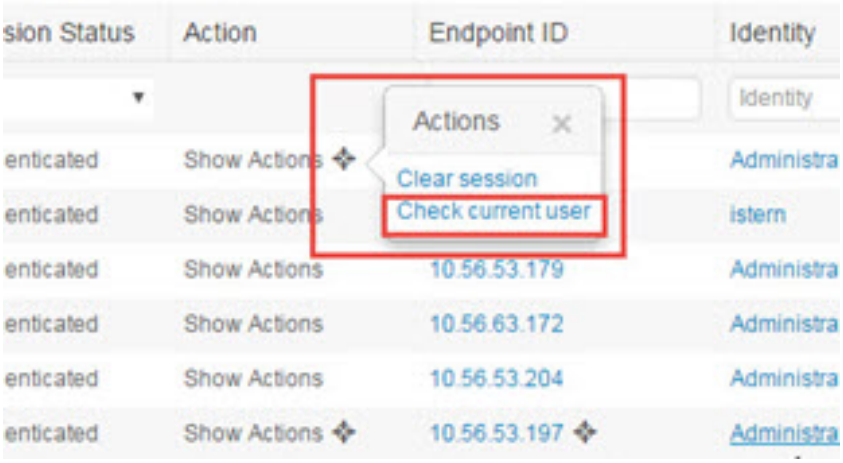
エンドポイント プローブ

設定可能なカスタム プロバイダの他に、パッシブ ID サービス がアクティブになると ISE でエンドポイント プローブが有効になります。エンドポイント プローブは、特定の各ユーザーがまだシステムにログインしているかどうかを定期的にチェックします。

（注） エンドポイントがバックグラウンドで実行されることを確認するには、まず最初の Active Directory 参加ポイントを設定し、[クレデンシャルの保存（Store Credentials）] を選択していることを確認します。エンドポイント プローブの設定の詳細については、エンドポイント プローブの使用 （139 ページ）を参照してください。

エンドポイントのステータスを手動で確認するには、**[アクション（Actions）]** 列から **[ライブセッション（Live Sessions）]** に移動し、**[アクションを表示（Show Actions）]** をクリックし、次の図に示すように **[現在のユーザーを確認（Check current user）]** を選択します。

図 *15*：現在のユーザーの確認



エンドポイント ユーザーのステータスと手動でのチェックの実行の詳細については、RADIUS ライブ セッションを参照してください。

エンドポイントプローブはユーザーが接続していることを認識します。特定のエンドポイントのセッションが最後に更新された時点から 4 時間経過している場合には、ユーザーがまだログインしているかどうかを確認し、次のデータを収集します。

- MAC アドレス
- オペレーティング システムのバージョン

このチェックに基づいてプローブは次の操作を実行します。

- ユーザーがまだログインしている場合、プローブは Cisco ISE を [アクティブユーザー（Active User）] ステータスで更新します。
- ユーザーがログアウトしている場合、セッション状態は[終了（Terminated）]に更新され、15 分経過後にユーザーはセッション ディレクトリから削除されます。
- ユーザーと通信できない場合、たとえばファイアウォールによって通信が防止されているか、エンドポイントがシャットダウンしている場合などには、ステータスが [到達不可能（Unreachable）]として更新され、サブスクライバポリシーによってユーザーセッションの処理方法が決定します。エンドポイントは引き続きセッション ディレクトリに残ります。

エンドポイント プローブの使用

始める前に

サブネット範囲に基づいてエンドポイント プローブを作成および有効にできます。PSN ごとに1つのエンドポイントプローブを作成できます。エンドポイントプローブを使用するには、次のように設定していることを確認してください。

- エンドポイントはポート 445 とのネットワーク接続が必要です。
- ISE から 1 番目の Active Directory 参加ポイントを設定し、プロンプトが表示されたら [クレデンシャルの選択（Select Credentials）] を選択してください。参加ポイントの詳細については、プローブおよびプロバイダとしての Active Directory （91 ページ）を参照してください。

（注） エンドポイントがバックグラウンドで実行するようにするため、最初に 1 番目の Active Directory 参加ポイントを設定する必要があります。これにより、Active Directory プローブが完全に設定されていない場合でもエンドポイント プローブを実行できるようになります。

ステップ 1 **[ワーク センター（Work Centers）] > [パッシブ ID（Passive ID）] > [プロバイダ（Providers）]** を選択し、[エンドポイント プローブ（Endpoint Probes）] を選択します。

ステップ 2 新しいエンドポイント プローブを作成するには、[追加（Add）] をクリックします。

ステップ 3 必須フィールドに入力し、[ステータス（Status）] フィールドで [有効化（Enable）] を選択していることを確認してから、[送信（Submit）]をクリックします。詳細については、エンドポイントプローブ設定 （140 ページ）を参照してください。

エンドポイント プローブ設定

サブネット範囲に基づいて PSN ごとに 1 つのエンドポイント プローブを作成します。展開で複数の PSN を使用している場合は、個別のサブネットのセットに各 PSN を割り当てることができます。

表 *29 :* エンドポイント プローブ設定

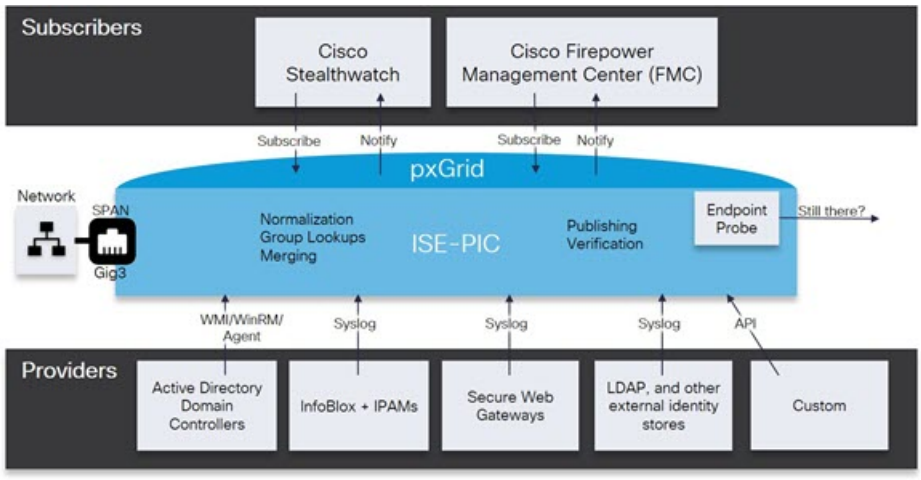
フィールド名	説明
Name	このプローブの用途を示す一意の名前を入力します。
説明（Description）	このプローブの用途を示す一意の説明を入力します。
ステータス（Status）	このプローブをアクティブにするには[有効化（Enable）] を選択します。
ホスト名（Host Name）	展開で使用可能な PSN のリストから、このプローブの PSN を選択します。
サブネット（Subnets）	このプローブがチェックする必要があるエンドポイントのグループのサブネット範囲を入力します。標準のサブネット マスク範囲と、カンマで区切ったサブネット アドレスを使用します。 例： 10.56.14.111/32,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 各範囲は一意である必要があり、相互に重複していてはなりません。たとえば、範囲 2.2.2.0/16,2.2.3.0/16 は相互に重複しているため、同一プローブに対して入力できません。

サブスクライバ

パッシブ ID サービス は、さまざまなプロバイダから収集し、Cisco ISE セッション ディレクトリにより保存された認証済みユーザー ID を、Cisco Stealthwatch や Cisco Firepower Management Center（FMC）などのその他のネットワーク システムに送信するため、Cisco pxGrid サービスを使用します。

次の図では、pxGrid ノードが外部プロバイダからユーザー ID を収集しています。これらの ID は解析、マッピング、およびフォーマットされます。pxGrid はこれらのフォーマット済みのユーザー ID を取得し、パッシブ ID サービス サブスクライバに送信します。

図 *16* : パッシブ *ID* サービス フロー



Cisco ISE に接続するサブスクライバは、pxGrid サービスの使用を登録する必要があります。サブスクライバは、クライアントになるために pxGrid SDK を介してシスコから使用可能な pxGrid クライアント ライブラリを採用する必要があります。サブスクライバは、一意の名前と証明書ベースの相互認証を使用して pxGrid にログインできます。Cisco pxGrid サブスクライバは、有効な証明書を送信すると、ISE により自動的に承認されます。

サブスクライバは設定されている pxGrid サーバーのホスト名または IP アドレスのいずれかに接続できます。不必要なエラーが発生することを防ぎ、DNS クエリが適切に機能するようにするため、ホスト名を使用することが推奨されます。公開および登録するためにサブスクライバの pxGrid で作成される、情報トピックまたはチャネル機能があります。Cisco ISE では SessionDirectory と IdentityGroup だけがサポートされています。機能情報は、公開、ダイレクトクエリ、または一括ダウンロードクエリによりパブリッシャから取得でき、[Capabilities] タブの [Subscribers] で確認できます。

サブスクライバが ISE から情報を受信できるようにするには、次の操作を行います。

1. 必要に応じて、サブスクライバ側から証明書を生成します。
2. PassiveID ワーク センターからサブスクライバの pxGrid 証明書の生成 （141 ページ）を参照してください。
3. サブスクライバの有効化 （143 ページ）。サブスクライバが ISE からユーザー ID を受信できるようにするため、このステップを実行するか、承認を自動的に有効にします。サブスクライバの設定 （144 ページ） を参照してください。

サブスクライバの pxGrid 証明書の生成

始める前に

pxGrid とサブスクライバの間の相互信頼を保証するため、pxGrid サブスクライバの証明書を生成できます。これにより、ISE からサブスクライバにユーザー ID を渡すことが可能になりま

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）]** > **[PassiveID]** > **[サブスクライバ（Subscribers）]** を選択し、[証明書（Certificates）] タブに移動します。

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

- [単一の証明書の生成（証明書署名要求なし）（Generate a single certificate without a certificate signing request）]：このオプションを選択した場合は、共通名（CN）を入力する必要があります。[コモンネーム（Common Name）] フィールドに、pxGrid をプレフィックスとして含む pxGrid FQDN を入力します。たとえば www.pxgrid-ise.ise.net です。あるいはワイルドカードを使用します。たとえば *.ise.net です。
- [単一の証明書の生成（証明書署名要求あり）（Generate a single certificate with a certificate signing request）]：このオプションを選択した場合は、証明書署名要求の詳細を入力する必要があります。
- [一括証明書の生成（Generate bulk certificates）]：必要な詳細を含む CSV ファイルをアップロードすることができます。
- [ルート証明書チェーンのダウンロード（Download root certificate chain）]：pxGrid クライアントの信頼できる証明書ストアに追加するために、ISE 公開ルート証明書をダウンロードします。ISE pxGrid ノードは、新規に署名された pxGrid クライアント証明書だけを信頼します（あるいはこの逆）。これにより、外部の認証局を使用する必要がなくなります。

ステップ 3 （オプション）この証明書の説明を入力できます。

ステップ 4 この証明書のベースとなる pxGrid 証明書テンプレートを表示または編集します。証明書テンプレートには、そのテンプレートに基づいて認証局（CA）によって発行されたすべての証明書に共通のプロパティが含まれています。証明書テンプレートは、件名、サブジェクト代替名（SAN）、キー タイプ、キー サイズ、使用する必要がある SCEP RA プロファイル、証明書の有効期間、証明書がクライアントまたはサーバーの認証またはその両方に使用される必要があるかどうかを指定した拡張キーの使用状況（EKU）を定義します。内部 Cisco ISE CA（ISE CA）は、証明書テンプレートを使用し、そのテンプレートに基づいて証明書を発行します。このテンプレートを編集するには、**[管理（Administration）]** > **[証明書（Certificates）]** > **[認証局（Certificate Authority）]** > **[証明書テンプレート（Certificate Templates）]** を選択します。

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

- [FQDN]：ISE ノードの完全修飾ドメイン名を入力します。たとえば www.isepic.ise.net です。あるいは FQDN にワイルドカードを使用します。たとえば *.ise.net です。

  pxGrid FQDN も入力できる追加の行を FQDN に追加できます。これは [コモンネーム（Common Name）] フィールドで使用する FQDN と同一である必要があります。
- [IP アドレス（IP address）]：この証明書に関連付ける ISE ノードの IP アドレスを入力します。サブスクライバが FQDN ではなく IP アドレスを使用する場合には、この情報を入力する必要があります。

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

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

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

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成（Create）] をクリックします。

サブスクライバの有効化

サブスクライバが Cisco ISE からユーザー ID を受信できるようにするため、このタスクを実行するか、または承認を自動的に有効にする必要があります。サブスクライバの設定 （144 ページ）を参照してください。

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
- パッシブ ID サービスを有効にします。詳細については、Easy Connect （83 ページ）を参照してください。

ステップ 1 **[ワーク センター（Work Centers）]** > **[PassiveID]** > **[サブスクライバ（Subscribers）]** を選択し、[クライアント（Clients）] タブが表示されることを確認します。

ステップ 2 サブスクライバの隣にあるチェックボックスをオンにして [承認（Approve）] をクリックします。

ステップ 3 [リフレッシュ（Refresh）] をクリックすると、最新のステータスが表示されます。

ライブ ログからのサブスクライバ イベントの表示

[ライブ ログ（Live Logs）] ページにはすべてのサブスクライバ イベントが表示されます。イベント情報には、イベント タイプ、タイムスタンプ、サブスクライバ名、機能名が含まれています。

[サブスクライバ（Subscribers）] に移動し、[ライブ ログ（Live Log）] タブを選択し、イベント リストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

サブスクライバの設定

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）]** > **[pxGrid サービス（pxGrid Services）]** > **[設定（Settings）]** を選択します。

ステップ 2 必要に応じて、次のオプションを選択します。

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

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

ステップ 3 [保存（Save）] をクリックします。

PassiveID ワーク センター でのサービスのモニターリングとトラブルシューティング

モニターリング、トラブルシューティング、およびレポーティングの各ツールを使用して PassiveID ワーク センター を管理する方法について説明します。

- RADIUS ライブ セッション
- 『』の「レポート」のセクションを参照してください。 Cisco ISE レポート
- 着信トラフィックを検証する TCP ダンプユーティリティ

LDAP

Lightweight Directory Access Protocol（LDAP）は、RFC 2251 で定義されている、TCP/IP 上で動作するディレクトリ サービスの問い合わせおよび変更のためのネットワーキング プロトコルです。LDAP は、X.500 ベースのディレクトリ サーバーにアクセスするためのライトウェイト メカニズムです。

Cisco ISE は、LDAP プロトコルを使用して LDAP 外部データベース（ID ソースとも呼ばれる）と統合します。

LDAP ディレクトリ サービス

LDAP ディレクトリ サービスは、クライアント/サーバー モデルに基づきます。クライアントは、LDAP サーバーに接続し、操作要求をサーバーに送信することで、LDAP セッションを開始します。サーバーは、応答を送信します。1 台以上の LDAP サーバーに、LDAP ディレクトリ ツリーまたは LDAP バックエンド データベースからのデータが含まれています。

ディレクトリ サービスは、情報を保持するデータベースであるディレクトリを管理します。ディレクトリ サービスは、情報を保存するために分散モデルを使用します。その情報は、通常はディレクトリ サーバー間で複製されます。

LDAP ディレクトリは、単純なツリー階層で編成されており、数多くのサーバー間で分散できます。各サーバーには、定期的に同期化されるディレクトリ全体の複製バージョンを配置できます。

ツリーのエントリには属性のセットが含まれており、各属性には名前（属性タイプまたは属性の説明）と 1 つ以上の値があります。属性はスキーマに定義されます。

各エントリには、固有識別情報、つまり識別名（DN）があります。この名前には、エントリ内の属性で構成されている相対識別名（RDN）と、それに続く親エントリの DN が含まれています。DN は完全なファイル名、RDN はフォルダ内の相対ファイル名と考えることができます。

複数の LDAP インスタンス

IP アドレスまたはポートの設定が異なる複数の LDAP インスタンスを作成することにより、異なる LDAP サーバーを使用するか、または同じ LDAP サーバー上の異なるデータベースを使用して認証を行うように、Cisco ISE を設定できます。プライマリ サーバーの各 IP アドレスおよびポートの設定は、セカンダリ サーバーの IP アドレスおよびポートの設定とともに、Cisco ISE LDAP ID ソース インスタンスに対応する LDAP インスタンスを形成します。

Cisco ISE では、個々の LDAP インスタンスが一意の LDAP データベースに対応している必要はありません。複数の LDAP インスタンスを、同一のデータベースにアクセスするように設定できます。この方法は、LDAP データベースにユーザーまたはグループのサブツリーが複数含まれている場合に役立ちます。各 LDAP インスタンスでは、ユーザーとグループに対してそれぞれ単一のサブツリー ディレクトリだけをサポートするため、Cisco ISE が認証要求を送信す

るユーザー ディレクトリとグループ ディレクトリのサブツリーの組み合わせごとに、別々の LDAP インスタンスを設定する必要があるからです。

LDAP フェールオーバー

Cisco ISE は、プライマリ LDAP サーバーとセカンダリ LDAP サーバー間でのフェールオーバーをサポートします。フェールオーバーは、LDAP サーバーがダウンしているかまたは到達不可能なために Cisco ISE で LDAP サーバーに接続できないことが原因で認証要求が失敗した場合に発生します。

フェールオーバー設定が指定され、Cisco ISE で接続しようとした最初の LDAP サーバーが到達不可能な場合、Cisco ISE は常に 2 番目の LDAP サーバーへの接続を試行します。再度、Cisco ISE で最初の LDAP サーバーを使用する場合は、[フェールバック再試行の遅延（Failback Retry Delay）] テキスト ボックスに値を入力する必要があります。

（注） Cisco ISE では、常にプライマリ LDAP サーバーを使用して、認証ポリシーで使用するグループと属性を管理者ポータルから取得します。このため、プライマリ LDAP サーバーはこれらの項目を設定するときにアクセス可能である必要があります。Cisco ISE では、フェールオーバーの設定に従って、実行時に認証と許可にのみセカンダリ LDAP サーバーを使用します。

LDAP 接続管理

Cisco ISE では、複数の同時 LDAP 接続がサポートされます。接続は、最初の LDAP 認証時にオンデマンドで開かれます。最大接続数は、LDAP サーバーごとに設定されます。事前に接続を開いておくと、認証時間が短縮されます。同時バインディング接続に使用する最大接続数を設定できます。開かれる接続の数は、LDAP サーバー（プライマリまたはセカンダリ）ごとに異なる場合があり、サーバーごとに設定される最大管理接続数に基づいて決まります。

Cisco ISE は、Cisco ISE で設定されている LDAP サーバーごとに、開いている LDAP 接続（バインディング情報を含む）のリストを保持します。認証プロセス中に、Connection Manager は開いている接続をプールから検索しようとします。開いている接続が存在しない場合、新しい接続が開かれます。

LDAP サーバーが接続を閉じた場合、Connection Manager はディレクトリを検索する最初のコールでエラーをレポートし、接続を更新しようとします。認証プロセスが完了した後、Connection Manager は接続を解放します。

LDAP ユーザー認証

LDAP を外部 ID ストアとして設定できます。Cisco ISE はプレーン パスワード認証を使用します。ユーザー認証には次の処理が含まれます。

- LDAP サーバーでの、要求のユーザー名に一致するエントリの検索

- ユーザー パスワードと、LDAP サーバーで見つかったパスワードとの照合
- ポリシーで使用するグループ メンバーシップ情報の取得
- ポリシーおよび許可プロファイルで使用するように指定された属性の値の取得

ユーザーを認証するために、Cisco ISE は LDAP サーバーにバインド要求を送信します。バインド要求には、ユーザーの DN およびユーザー パスワードがクリア テキストで含まれています。ユーザーの DN およびパスワードが LDAP ディレクトリ内のユーザー名およびパスワードと一致した場合に、ユーザーは認証されます。

Active Directory が LDAP として使用されている場合は、UPN 名がユーザー認証に使用されます。Sun ONE Directory Server が LDAP として使用されている場合は、SAM 名がユーザー認証に使用されます。

（注）
- Cisco ISE は、ユーザー認証ごとに 2 つの searchRequest メッセージを送信します。これは、Cisco ISE の許可またはネットワークのパフォーマンスに影響しません。2 番目の LDAP 要求では、Cisco ISE が正しい ID と通信していることを確認します。
- DNS クライアントとしての Cisco ISE は、DNS 応答で返された最初の IP のみを使用して、LDAP バインドを実行します。

Secure Sockets Layer（SSL）を使用して LDAP サーバーへの接続を保護することを推奨します。

（注） パスワードの変更は、パスワードの有効期限が切れた後にアカウントの残りの猶予ログインがあるときにのみ、LDAP でサポートされます。パスワードが正常に変更された場合、LDAP サーバーの bindResponse は LDAP_SUCCESS であり、bindResponse メッセージに残りの猶予ログインの制御フィールドが含まれます。bindResponse メッセージにさらなる制御フィールド（残りの猶予ログイン以外）が含まれる場合は、Cisco ISE がメッセージを復号できない可能性があります。

許可ポリシーで使用する LDAP グループおよび属性の取得

Cisco ISE は、ディレクトリ サーバーでバインド操作を実行し、サブジェクトを検索および認証することによって、LDAP ID ソースに対してサブジェクト（ユーザーまたはホスト）を認証できます。認証が成功した後、Cisco ISE は、要求された場合、常にサブジェクトに所属するグループおよび属性を取得できます。Cisco ISE 管理者ポータルで取得されるように属性を設定するには、**[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [LDAP]** を選択します。Cisco ISE は、これらのグループおよび属性を使用してサブジェクトを許可できます。

ユーザーの認証または LDAP ID ソースの問い合わせを行うために、Cisco ISE は LDAP サーバーに接続し、接続プールを保持します。

Active Directory が LDAP ストアとして設定されている場合は、グループ メンバーシップに関する次の制限事項に注意する必要があります。

- ユーザーまたはコンピュータは、ポリシー条件でポリシー ルールに一致するように定義されたグループの直接的なメンバーである必要があります。
- 定義されたグループは、ユーザーまたはコンピュータのプライマリ グループではない可能性があります。この制限は、Active Directory が LDAP ストアとして設定されている場合にのみ適用されます。

LDAP グループ メンバーシップ情報の取得

ユーザー認証、ユーザー ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからグループ メンバーシップ情報を取得する必要があります。LDAP サーバーは、サブジェクト（ユーザーまたはホスト）とグループ間の関連付けを次の方法のいずれかで表します。

- [グループがサブジェクトを参照（Groups Refer to Subjects）]：グループオブジェクトには、サブジェクトを指定する属性が含まれています。サブジェクトの識別子は、次のものとしてグループに供給できます。
  - 識別名
  - プレーン ユーザー名
- [サブジェクトがグループを参照（Subjects Refer to Groups）]：サブジェクトオブジェクトには、所属するグループを指定する属性が含まれています。

LDAP ID ソースには、グループ メンバーシップ情報の取得のために次のパラメータが含まれています。

- [参照方向（Reference direction）]：このパラメータは、グループメンバーシップを決定するときに使用する方法を指定します（グループからサブジェクトへまたはサブジェクトからグループへ）。
- [グループマップ属性（Group Map Attribute）]：このパラメータは、グループメンバーシップ情報を含む属性を示します。
- [グループオブジェクトクラス（Group Object Class）]：このパラメータは、特定のオブジェクトがグループとして認識されることを決定します。
- [グループ検索サブツリー（Group Search Subtree）]：このパラメータは、グループ検索の検索ベースを示します。
- [メンバータイプオプション（Member Type Option）]：このパラメータは、グループメンバー属性にメンバーが保存される方法を指定します（DN またはプレーンユーザー名のいずれかとして）。

LDAP 属性の取得

ユーザー認証、ユーザー ルックアップ、および MAC アドレス ルックアップのために、Cisco ISE は LDAP データベースからサブジェクト属性を取得する必要があります。LDAP ID ソースのインスタンスごとに、ID ソース ディクショナリが作成されます。これらのディレクトリでは、次のデータ型の属性がサポートされています。

- 文字列
- 符号なし 32 ビット整数
- IPv4 アドレス

符号なし整数および IPv4 属性の場合、Cisco ISE は取得した文字列を対応するデータ型に変換します。変換が失敗した場合、または属性の値が取得されなかった場合、Cisco ISE ではデバッグ メッセージをロギングしますが、認証またはルックアップ プロセスは失敗しません。

変換が失敗した場合、または Cisco ISE で属性の値が取得されない場合に、Cisco ISE で使用できるデフォルトの属性値を任意で設定できます。

LDAP 証明書の取得

ユーザー ルックアップの一部として証明書取得を設定した場合、Cisco ISE は証明書属性の値を LDAP から取得する必要があります。証明書属性の値を LDAP から取得するには、LDAP ID ソースの設定時に、アクセスする属性のリストで証明書属性をあらかじめ設定しておく必要があります。

LDAP サーバーによって返されるエラー

次のエラーが認証プロセス中に発生する可能性があります。

- 認証エラー：Cisco ISE は、認証エラーを Cisco ISE ログ ファイルに記録します。

  LDAP サーバーがバインディング（認証）エラーを返す理由で考えられるのは、次のとおりです。

  - パラメータ エラー：無効なパラメータが入力された
  - ユーザーアカウントが制限されている（無効、ロックアウト、期限切れ、パスワード期限切れなど）
  - 初期化エラー：LDAP サーバーのタイムアウト設定を使用して、LDAP サーバーでの接続または認証が失敗したと判断する前に Cisco ISE が LDAP サーバーからの応答を待つ秒数を設定します。

    LDAP サーバーが初期化エラーを返す理由で考えられるのは、次のとおりです。

    - LDAP がサポートされていない。
    - サーバーがダウンしている。
    - サーバーがメモリ不足である。

- ユーザーに特権がない。
- 間違った管理者クレデンシャルが設定されている。

外部リソースエラーとして次のエラーがロギングされ、LDAPサーバーで考えられる問題が示されます。

- 接続エラーが発生した
- タイムアウトが期限切れになった
- サーバーがダウンしている
- サーバーがメモリ不足である

未知ユーザー エラーとして次のエラーがロギングされます。

- データベースにユーザーが存在しない

ユーザーは存在するが送信されたパスワードが無効である場合、無効パスワードエラーとして次のエラーがロギングされます。

- 無効なパスワードが入力された

LDAP ユーザー ルックアップ

Cisco ISE は LDAP サーバーを使用したユーザー ルックアップ機能をサポートしています。この機能を使用すると、認証なしでLDAPデータベース内のユーザーを検索し、情報を取得できます。ユーザー ルックアップ プロセスには次のアクションが含まれます。

- LDAP サーバーでの、要求のユーザー名に一致するエントリの検索
- ポリシーで使用するユーザー グループ メンバーシップ情報の取得
- ポリシーおよび許可プロファイルで使用するように指定された属性の値の取得

LDAP MAC アドレス ルックアップ

Cisco ISE はMACアドレスルックアップ機能をサポートしています。この機能を使用すると、認証なしで LDAP データベース内の MAC アドレスを検索し、情報を取得できます。MAC アドレス ルックアップ プロセスには次のアクションが含まれます。

- デバイスの MAC アドレスと一致するエントリの LDAP サーバーを検索する
- ポリシーで使用するデバイスの MAC アドレス グループ情報の取得
- ポリシーで使用する指定された属性の値の取得

LDAP ID ソースの追加

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。
- Cisco ISE は、許可ポリシーで使用するグループおよび属性を取得するためにプライマリ LDAP サーバーを常に使用します。このため、プライマリ LDAP サーバーはこれらの項目を設定するときに到達可能である必要があります。

ステップ 1 **[管理（Administration）] > [ID 管理（Identity Management）] > [外部IDソース（External Identity Sources）]** > [LDAP] > [追加（Add）] を選択します。

ステップ 2 値を入力します。

ステップ 3 [送信（Submit）] をクリックして、LDAP インスタンスを作成します。

LDAP ID ソースの設定

LDAP 一般設定

以下の表では、[一般（General）] タブのフィールドについて説明します。

表 *30 : LDAP* 一般設定

フィールド名	使用上のガイドライン
名前（**Name**）	LDAP インスタンスの名前を入力します。この値は、サブジェクト DN および属性を取得するために検索で使用されます。この値は string 型で、最大長は 64 文字です。
説明（**Description**）	LDAP インスタンスの説明を入力します。この値は string 型で、最大長は 1024 文字です。

フィールド名	使用上のガイドライン
スキーマ（**Schema**）	次の組み込みのスキーマ タイプのいずれかを選択するか、カスタム スキーマを作成できます。 • Active Directory • Sun Directory Server • Novell eDirectory [スキーマ（Schema）]の隣の矢印をクリックすると、スキーマの詳細を表示できます。 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。
（注） 次のフィールドは、カスタム スキーマを選択した場合にのみ編集できます。	
サブジェクト オブジェクト クラス（**Subject Objectclass**）	サブジェクト DN および属性を取得するために検索で使用する値を入力します。この値は string 型で、最大長は 256 文字です。
サブジェクト名属性（**Subject Name Attribute**）	要求内のユーザー名を含む属性の名前を入力します。この値は string 型で、最大長は 256 文字です。 （注） 構成されているサブジェクト名属性は、外部 ID ストア内のインデックス付きのものである必要があります。
グループ名属性（**Group Name Attribute**）	• CN：共通名に基づいて LDAP ID ストア グループを取得します。 • DN：識別名に基づいて LDAP ID ストア グループを取得します。
証明書属性（**Certificate Attribute**）	証明書定義を含む属性を入力します。証明書ベースの認証の場合、クライアントによって提示された証明書を検証するために、これらの定義が使用されます。

フィールド名	使用上のガイドライン
グループ オブジェクト クラス（**Group Objectclass**）	グループとして認識されるオブジェクトを指定するために、検索に使用する値を入力します。この値は string 型で、最大長は 256 文字です。
グループ マップ属性（**Group Map Attribute**）	マッピング情報を含む属性を指定します。この属性は、選択した参照方向に基づいて、ユーザーまたはグループ属性を指定できます。
サブジェクト オブジェクトにグループへの参照が含まれる（**Subject Objects Contain Reference To Groups**）	所属するグループを指定する属性がサブジェクトオブジェクトに含まれている場合は、このオプションをクリックします。
グループ オブジェクトにサブジェクトへの参照が含まれる（**Group Objects Contain Reference To Subjects**）	サブジェクトを指定する属性がグループオブジェクトに含まれている場合は、このオプションをクリックします。この値はデフォルト値です。
グループ内のサブジェクトをメンバー属性に保存（**Subjects In Groups Are Stored In Member Attribute As**）	（[グループオブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）] オプションを有効にした場合に限り使用可能）グループメンバー属性にメンバーが供給される方法を指定します（デフォルトは DN）。
ユーザー情報属性（**User Info Attributes**）	デフォルトでは、事前設定された属性が次の組み込みのスキーマ タイプのユーザー情報（名、姓、電子メール、電話、地域など）を収集するために使用されます。 • Active Directory • Sun Directory Server • Novell eDirectory 事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。 [スキーマ（Schema）] ドロップダウン リストから [カスタム（Custom）] オプションを選択し、要件に基づいてユーザー情報の属性を編集することもできます。

（注） 構成されているサブジェクト名属性は、外部 ID ストア内のインデックス付きのものである必要があります。

LDAP の接続設定

以下の表では、[接続設定（Connection Settings）] タブのフィールドについて説明します。

表 *31 : LDAP* の接続設定

フィールド名	使用上のガイドライン
セカンダリ サーバーの有効化（**Enable Secondary Server**）	プライマリ LDAP サーバーに障害が発生した場合にバックアップとして使用するセカンダリ LDAP サーバーを有効にする場合は、このオプションをオンにします。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバーの設定パラメータを入力する必要があります。
プライマリ サーバーとセカンダリ サーバー（**Primary and Secondary Servers**）	
ホスト名/IP（**Hostname/IP**）	LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。
ポート（**Port**）	LDAP サーバーがリッスンしている TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP 仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバーの管理者からポート番号を取得できます。

フィールド名	使用上のガイドライン
各 ISE ノードのサーバーの指定（Specify server for each ISE node）	プライマリおよびセカンダリ LDAP サーバーの hostnames/IP および各 PSN のポートを設定するには、このチェック ボックスをオンにします。 このオプションを有効にすると、導入のすべてのノードを表示するテーブルが表示されます。ノードを選択し、プライマリおよびセカンダリ LDAP サーバーの hostname/IP および選択したノードのポートを設定する必要があります。
アクセス（Access）	[匿名アクセス（Anonymous Access）]：LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバーではクライアントが区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへの、クライアント読み取りアクセスが許可されます。認証情報をサーバーに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。 [認証されたアクセス（Authenticated Access）]：LDAP ディレクトリの検索が管理者のログイン情報によって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。
管理者 DN（Admin DN）	管理者の DN を入力します。管理者 DN は、[ユーザー ディレクトリ サブツリー（User Directory Subtree）] 下のすべての必要なユーザーの検索およびグループの検索を行う権限を持つ LDAP アカウントです。指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、該当 LDAP サーバーで認証されたユーザーのグループ マッピングは失敗します。
パスワード（Password）	LDAP 管理者アカウントのパスワードを入力します。

フィールド名	使用上のガイドライン
セキュアな認証（**Secure Authentication**）	SSL を使用して Cisco ISE とプライマリ LDAP サーバー間の通信を暗号化する場合にクリックします。[ポート（Port）] フィールドに LDAP サーバーでの SSL に使用されるポート番号が入力されていることを確認します。このオプションを有効にした場合は、ルート CA を選択する必要があります。
LDAP サーバーのルート CA（LDAP Server Root CA）	ドロップダウンリストボックスから信頼できるルート認証局を選択して、証明書による安全な認証を有効にします。
サーバー タイムアウト（**Server timeout**）	プライマリ LDAP サーバーでの接続または認証が失敗したと判断する前に Cisco ISE がプライマリ LDAP サーバーからの応答を待つ秒数を入力します。有効な値は 1 ～ 99 です。デフォルトは 10 です。
最大管理接続（**Max. Admin Connections**）	特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、ユーザーディレクトリ サブツリーおよびグループディレクトリ サブツリーの下にあるユーザーおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です。デフォルトは 20 です。
N 秒ごとに再接続（Force reconnect every N seconds）	このチェックボックスをオンにし、[秒（Seconds）] フィールドに、サーバーを指定された間隔で LDAP 接続を更新するための適切な値を入力します。有効な範囲は 1 ～ 60 分です。
サーバーへのバインドをテスト（**Test Bind To Server**）	LDAP サーバーの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバーの詳細を編集して再テストします。
フェールオーバー（**Failover**）	
常にプライマリ サーバーに最初にアクセスする（**Always Access Primary Server First**）	Cisco ISE の認証と認可のために常にプライマリ LDAP サーバーに最初にアクセスするように設定するには、このオプションをクリックします。

フィールド名	使用上のガイドライン
経過後にプライマリ サーバーにフェールバック（**Failback to Primary Server After**）	Cisco ISE で接続しようとしたプライマリ LDAP サーバーが到達不可能な場合、Cisco ISE はセカンダリ LDAP サーバーへの接続を試行します。Cisco ISE に再びプライマリ LDAP サーバーを使用するように設定するには、このオプションをクリックし、テキスト ボックスに値を入力します。

[LDAP] の [ディレクトリ構成（Directory Organization）] タブ

次の表では、[ディレクトリ構成（Directory Organization）] タブのフィールドについて説明します。

表 *32 : [LDAP]* の *[*ディレクトリ構成（*Directory Organization*）*]* タブ

フィールド名	使用上のガイドライン
サブジェクト検索ベース（**Subject Search Base**）	すべてのサブジェクトを含むサブツリーの DN を入力します。次に例を示します。 o=corporation.com サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。

フィールド名	使用上のガイドライン
グループ検索ベース（**Group Search Base**）	すべてのグループを含むサブツリーの DN を入力します。次に例を示します。 ou = 組織ユニット、ou = 次の組織ユニット、o = corporation.com グループを含むツリーがベース DN である場合は、LDAP 設定に応じて o=corporation.com または dc=corporation,dc=com と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。
形式での **MAC** アドレスの検索（**Search for MAC Address in Format**）	LDAPデータベースでの検索に使用する、Cisco ISE の MAC アドレス形式を入力します。内部 ID ソースの MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で供給されます。LDAPデータベースのMACアドレスは、異なる形式で供給できます。ただし、Cisco ISE でホスト ルックアップ要求が受信されると、MACアドレスは内部形式からこのフィールドで指定した形式に変換されます。 ドロップダウン リストを使用して、特定の形式でのMACアドレスの検索を有効にします。<*format*> は次のいずれかです。 • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 選択する形式は、LDAP サーバーに供給されているMACアドレスの形式と一致している必要があります。

フィールド名	使用上のガイドライン
サブジェクト名の先頭から最後に出現する区切り文字まで削除（Strip start of subject name up to the last occurrence of the separator）	ユーザー名からドメインプレフィックスを削除するための適切なテキストを入力します。 ユーザー名の中でこのフィールドに指定した区切り文字が Cisco ISE で検出されると、そのユーザー名の初めから区切り文字までのすべての文字が削除されます。ユーザー名に、<start_string> ボックスに指定した文字が複数含まれている場合は、Cisco ISE によって最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザー名が DOMAIN\user1 である場合、Cisco ISE によって user1 が LDAP サーバーに送信されます。 （注） <start_string> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザー名にこれらの文字を使用できません。
最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip end of subject name from the first occurrence of the separator）	ユーザー名からドメイン サフィックスを削除するための適切なテキストを入力します。 ユーザー名の中でこのフィールドに指定した区切り文字が Cisco ISE で検出されると、その区切り文字からユーザー名の末尾までのすべての文字が削除されます。ユーザー名に、このフィールドに指定した文字が複数含まれている場合は、Cisco ISE によって最初の区切り文字から文字が削除されます。たとえば、区切り文字が@で、ユーザー名が *user1@domain* であれば、Cisco ISE は *user1* を LDAP サーバーに送信します。 （注） *<end_string>* ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザー名にこれらの文字を使用できません。

LDAP グループ設定

表 *33 : LDAP* グループ設定

フィールド名	使用上のガイドライン
追加（**Add**）	[追加（Add）]>[グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）] を選択して LDAP ディレクトリからグループを選択します。 グループの追加を選択した場合は、新しいグループの名前を入力します。ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。選択したグループが [グループ（Groups）] ウィンドウに表示されます。

LDAP 属性設定

表 *34 : LDAP* 属性設定

フィールド名	使用上のガイドライン
追加（**Add** ）	[追加（Add）]>[属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）] を選択して LDAP サーバーから属性を選択します。 属性を追加する場合は、新しい属性の名前を入力します。ディレクトリから選択する場合は、ユーザー名を入力し、[属性の取得（Retrieve Attributes）] をクリックして属性を取得します。選択する属性の隣にあるチェック ボックスをオンにし、[OK] をクリックします。

LDAP 詳細設定

以下の表では、[詳細設定（Advanced Settings）] タブのフィールドについて説明します。

表 *35 : LDAP* 詳細設定

フィールド名	使用上のガイドライン
[パスワードの変更を有効にする（Enable password change）]	デバイス管理に PAP プロトコルを使用し、ネットワーク アクセスに RADIUS EAP-GTC プロトコルを使用している場合に、パスワードが期限切れになるか、またはパスワードがリセットされるときに、ユーザーがパスワードを変更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。サポートされていないプロトコルでは、ユーザー認証が失敗します。このオプションでは、ユーザーが次回のログイン時にパスワードを変更できるようにすることもできます。

関連トピック

LDAP ディレクトリ サービス （145 ページ）
LDAP ユーザー認証 （146 ページ）
LDAP ユーザー ルックアップ （150 ページ）
LDAP ID ソースの追加 （151 ページ）

LDAP スキーマの設定

ステップ 1

ステップ 2 LDAP インスタンスを選択します。

ステップ 3 [全般（General）] タブをクリックします。

ステップ 4 [スキーマ（Schema）] オプションの近くにあるドロップダウン矢印をクリックします。

ステップ 5 [スキーマ（Schema）] ドロップダウン リストから必要なスキーマを選択します。[カスタム（Custom）] オプションを選択して、要件に基づいて属性を更新できます。

事前定義属性は、組み込みスキーマ（Active Directory、Sun directory Server、Novell eDirectory など）に使用されます。事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。

プライマリおよびセカンダリ LDAP サーバーの設定

LDAP インスタンスを作成したら、プライマリ LDAP サーバーに対する接続を設定する必要があります。セカンダリ LDAP サーバーの設定は、オプションです。

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、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集する LDAP インスタンスの隣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。

ステップ 3 [接続（Connection）] タブをクリックして、プライマリおよびセカンダリ サーバーを設定します。

ステップ 4 「LDAP ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 [送信（Submit）] をクリックして接続パラメータを保存します。

LDAP サーバーからの属性を取得するための Cisco ISE の有効化

Cisco ISE で LDAP サーバーからユーザーとグループのデータを取得するには、Cisco ISE で LDAP ディレクトリの詳細を設定する必要があります。LDAP ID ソースでは、次の 3 つの検索が適用されます。

- 管理のためのグループ サブツリーのすべてのグループの検索
- ユーザーを特定するためのサブジェクト サブツリーのユーザーの検索

- ユーザーが所属するグループの検索

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、**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** > [LDAP] を選択します。

ステップ 2 編集する LDAP インスタンスの隣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。

ステップ 3 [ディレクトリ構成（Directory Organization）] タブをクリックします。

ステップ 4 「LDAP ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 [送信（Submit）] をクリックして設定を保存します。

LDAP サーバーからのグループ メンバーシップ詳細の取得

新しいグループを追加するか、LDAP ディレクトリからグループを選択できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集する LDAP インスタンスの隣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。

ステップ 3 [グループ（Groups）] タブをクリックします。

ステップ 4 **[追加（Add）]>[グループの追加（Add Group）]** を選択して新しいグループを追加するか、**[追加（Add）]> [ディレクトリからグループを選択（Select Groups From Directory）]** を選択して LDAP ディレクトリからグループを選択します。

a) グループの追加を選択した場合は、新しいグループの名前を入力します。

b) ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。検索条件には、アスタリスク（*）ワイルドカード文字を含めることができます。

ステップ 5 選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

選択したグループが [グループ（Groups）] ページに表示されます。

ステップ 6 グループ選択を保存するには、[送信（Submit）] をクリックします。

（注） Active Directory の組み込みグループは、Active Directory が Cisco ISE の LDAP ID ストアとして設定されているときにはサポートされません。

LDAP サーバーからのユーザー属性の取得

許可ポリシーで使用する LDAP サーバーからユーザー属性を取得できます。

ステップ 1 **[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** を選択します。

ステップ 2 編集する LDAP インスタンスの隣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。

ステップ 3 [属性（Attributes）] タブをクリックします。

ステップ 4 **[追加（Add）] > [属性の追加（Add Attribute）]** を選択して新しい属性を追加するか、**[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）]** を選択して LDAP サーバーから属性を選択します。

a) 属性を追加する場合は、新しい属性の名前を入力します。

b) ディレクトリから選択する場合は、例のユーザーを入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザーの属性を取得します。アスタリスク（*）ワイルドカード文字を使用できます。

Cisco ISE では、属性タイプ IP を手動で追加するときに、ユーザー認証に IPv4 または IPv6 アドレスを使用して LDAP サーバーを設定できます。

ステップ 5 選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 属性選択を保存するには、[送信（Submit）] をクリックします。

LDAP ID ソースによるセキュア認証の有効化

LDAP 設定ページで [セキュア認証（Secure Authentication）] オプションを選択すると、Cisco ISE は LDAP ID ソースとのセキュアな通信に SSL を使用します。LDAP ID ソースへのセキュアな接続は以下を使用して確立されます。

- SSL トンネル：SSL v3 または TLS v1（LDAP サーバーでサポートされる最も強力なバージョン）を使用
- サーバー認証（LDAP サーバーの認証）：証明書ベース
- クライアント認証（Cisco ISE の認証）：なし（管理者のバインドは SSL トンネル内で使用されます）
- 暗号スイート：Cisco ISE でサポートされるすべての暗号スイート

最も強力な暗号化と Cisco ISE がサポートする暗号方式を備えている TLS v1 を使用することを推奨します。

Cisco ISE が LDAP ID ソースと安全に通信できるようにするには、次の手順を実行します。

始める前に

- Cisco ISE は、LDAP サーバーに接続する必要があります
- TCP ポート 636 を開く必要があります

ステップ 1 LDAP サーバーにサーバー証明書を発行した CA の認証局（CA）チェーン全体を Cisco ISE にインポートします（**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**）。

完全な CA チェーンは、ルート CA 証明書および中間 CA 証明書を参照し、LDAP サーバー証明書は参照しません。

ステップ 2 LDAP ID ソースとの通信時にセキュア認証を使用するように Cisco ISE を設定します（**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]**の順に選択します。[接続設定（Connection Settings）] タブで [セキュア認証（Secure Authentication）] チェックボックスを必ずオンにしてください）。

ステップ 3 LDAP ID ストアでルート CA 証明書を選択します。

ODBC ID ソース

オープン データベース コネクティビティ（ODBC）準拠データベースは、ユーザーとエンドポイントを認証する外部 ID ソースとして使用できます。ODBC ID ストアは、ID ストアの順序で、ゲストおよびスポンサーの認証に使用できます。また、BYOD フローにも使用できます。

サポートされているデータベース エンジンは次のとおりです。

- MySQL
- Oracle
- PostgreSQL
- Microsoft SQL Server
- Sybase

ODBC 準拠データベースに対して認証するように Cisco ISE を設定しても、データベースの設定には影響を与えません。データベースを管理するには、データベースのマニュアルを参照してください。

（注） Cisco ISE は ODBC による暗号化をサポートしていません。したがって、ODBC 接続は保護されていません。

ODBC データベースのクレデンシャルチェック

Cisco ISE は、ODBC データベースに対する 3 つの異なるタイプのクレデンシャルチェックをサポートしています。それぞれのクレデンシャル チェック タイプに適切な SQL ストアドプロシージャを設定する必要があります。ストアドプロシージャは、ODBC データベースで適切な

テーブルをクエリし、ODBCデータベースから出力パラメータやレコードセットを受信するために使用されます。データベースは、ODBCクエリに応答してレコードセットまたは名前付きパラメータのセットを返すことができます。

パスワードは、クリアテキストまたは暗号化形式でODBCデータベースに保存できます。Cisco ISEによって呼び出された場合は、ストアドプロシージャでパスワードをクリアテキストに復号化できます。

クレデンシャルチェックタイプ	ODBC 入力パラメータ	ODBC 出力パラメータ	クレデンシャルチェック	認証プロトコル
ODBC データベースのプレーンテキストパスワード認証	ユーザ名 パスワード	結果 グループ アカウント情報 エラー文字列	ユーザー名とパスワードが一致すると、関連するユーザー情報が返されます。	PAP EAP-GTC（PEAP または EAP-FAST の内部メソッドとして） TACACS
ODBC データベースから取得したプレーンテキストパスワード	[ユーザー名（Username）]	結果 グループ アカウント情報 エラー文字列 パスワード	ユーザー名が見つかった場合、そのパスワードと関連するユーザー情報がストアドプロシージャによって返されます。Cisco ISE は、認証方式に基づいてパスワードハッシュを計算し、クライアントから受信したものと比較します。	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2（PEAP または EAP-FAST の内部メソッドとして） TACACS
ルックアップ	[ユーザー名（Username）]	結果 グループ アカウント情報 エラー文字列	ユーザー名が見つかった場合、該当するユーザー情報が返されます。	MAB PEAP、EAP-FAST、EAP-TTLS の高速再接続

（注） 承認の参照元として ODBC を使用する場合は、ODBC データベースと着信要求 MAB 形式が同じであることを確認します。

出力パラメータで返されるグループは、Cisco ISE では使用されません。グループの取得ストアドプロシージャによって取得されたグループのみが Cisco ISE で使用されます。アカウント情報は、認証の監査ログにのみ含まれています。

次の表に、ODBC データベース ストアド プロシージャと Cisco ISE 認証結果コードによって返される、結果コード間のマッピングを示します。

（ストアド プロシージャによって返される）結果コード	説明	Cisco ISE 認証結果コード
[0]	CODE_SUCCESS	該当なし（認証成功）
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	失敗しました（Failed）
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	エラー（Error）
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired

（注） Cisco ISE は、このマッピングされた認証結果コードに基づいて実際の認証またはルックアップ操作を実行します。

ODBC データベースからグループと属性を取得するためにストアド プロシージャを使用できます。

次は、プレーンテキストパスワード認証用のレコードセットを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset]
        @username varchar(64), @password varchar(255)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

次は、プレーンテキストパスワード取得用のレコードセットを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset]
        @username varchar(64)
AS
BEGIN
```

```
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error',password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

次は、ルックアップ用のレコードセットを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

次は、プレーンテキストパスワード認証用のパラメータを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters]
        @username varchar(64), @password varchar(255), @result INT OUTPUT, @group
varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc',  @errorString='ODBC Authen Error'
END
```

次は、プレーンテキストパスワード取得用のパラメータを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters]
       @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
 varchar(255) OUTPUT, @errorString varchar(255) OUTPUT, @password varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error', @password=password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
```

```
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

次は、ルックアップ用のパラメータを返すサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters]
       @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
 varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No
Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

次は、Microsoft SQL Server からグループを取得するサンプルのプロシージャです。

```
CREATE PROCEDURE [dbo].[ISEGroupsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                select 'accountants', 'engineers', 'sales','test_group2'
        end
        else
                set @result = 1
END
```

次は、ユーザー名が「*」の場合にすべてのユーザーの全グループを取得するサンプルのプロシージャ（Microsoft SQL Server 用）です。

```
ALTER PROCEDURE [dbo].[ISEGroupsH]
                @username varchar(64), @result int output
AS
BEGIN
                if @username = '*'
                begin
                                -- if username is equal to '*' then return all existing
 groups
                                set @result = 0
                                select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4'
                end
                else
                if exists (select * from NetworkUsers where username = @username)
                begin
                                set @result = 0
                                select 'accountants'
                end
                else
                                set @result = 1
END
```

次は、Microsoft SQL Server から属性を取得するサンプルのプロシージャです。

```
CREATE PROCEDURE [dbo].[ISEAttrsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                                select phone as phone, username as username, department
 as department, floor as floor, memberOf as memberOf, isManager as isManager from
NetworkUsers where username = @username
        end
        else
                set @result = 1
END
```

ODBC 設定のその他の例

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/211581-Configure-ODBC-on-ISE-2-3-with-Oracle-Da.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200644-Configure-ODBC-on-ISE-2-1-with-PostgreSQ.html

ODBC ID ソースの追加

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 **[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）]** を選択します。

ステップ 2 [ODBC] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [一般（General）] タブで、ODBC ID ソースの名前と説明を入力します。

ステップ 5 [接続（Connection）] タブで、次の詳細情報を入力します。

- ODBC データベースのホスト名または IP アドレス。データベースに非標準 TCP ポートが使用されている場合は、「ホスト名または IP アドレス:ポート」の形式でポート番号を指定できます。
- ODBC データベースの名前
- 管理者のユーザー名およびパスワード（Cisco ISE がこれらのクレデンシャルを使用してデータベースに接続します）
- 秒単位のサーバーのタイムアウト（デフォルトは 5 秒）
- 接続の試行（デフォルトは 1）
- データベース タイプ。次のいずれかを実行します。
  - **MySQL**
  - **Oracle**

- **PostgreSQL**
- **Microsoft SQL Server**
- **Sybase**

ステップ 6 [テスト接続（Test Connection）] をクリックして ODBC データベースとの接続を確認し、設定された使用例用のストアドプロシージャの存在を確認します。

ステップ 7 [ストアドプロシージャ（Stored Procedures）] タブで、次の詳細情報を入力します。

ステップ 8 [属性（Attributes）] タブに必要な属性を追加します。属性の追加時に、属性名が認証ポリシールールでどのように表示されるかを指定できます。

ステップ 9 [グループ（Groups）] タブにユーザーグループを追加します。また、ユーザー名または MAC アドレスを指定して ODBC データベースからグループを取得することもできます。これらのグループは、認証ポリシーで使用できます。

グループおよび属性の名前を変更できます。デフォルトでは、[ISE の名前（Name in ISE）] フィールドに表示される名前は ODBC データベースの名前と同じですが、この名前は変更できます。この名前が認証ポリシーで使用されます。

ステップ 10 [送信（Submit）] をクリックします。

（注） 入力属性を設定した場合は、ODBC ID ストアを複製するときに次の手順を実行する必要があります。保存しない場合は、複製した ODBC ID ストアで入力パラメータが失われる可能性があります。

1. [詳細設定（Advance Settings）] をクリックします。
2. 入力パラメータが正しく設定されているかどうかを確認します。
3. [OK] をクリックして、複製した ODBC ID ストアにこれらの入力パラメータを保存します。

RADIUS トークン ID ソース

RADIUS プロトコルをサポートし、ユーザーおよびデバイスに認証、許可、アカウンティング（AAA）サービスを提供するサーバーは、RADIUS サーバーと呼ばれます。RADIUS ID ソースは、サブジェクトとそのクレデンシャルの集合を含み、通信に RADIUS プロトコルを使用する外部 ID ソースです。たとえば、Safeword トークン サーバーは、複数のユーザーおよびそのクレデンシャルをワンタイム パスワードとして含めることができる ID ソースであり、Safeword トークン サーバーによって提供されるインターフェイスでは、RADIUS プロトコルを使用して問い合わせることができます。

Cisco ISE では、RADIUS RFC 2865 準拠のいずれかのサーバーが外部 ID ソースとしてサポートされています。Cisco ISE では、複数の RADIUS トークン サーバー ID がサポートされています。たとえば、RSA SecurID サーバーや SafeWord サーバーなどです。RADIUS ID ソースは、ユーザーを認証するために使用される任意の RADIUS トークン サーバーと連携できます。

（注） MAB認証では、プロセス ホスト ルックアップ オプションを有効にする必要があります。MAB 認証を使用するデバイスは OTP または RADIUS トークン（RADIUS トークン サーバー認証に必要）を生成できないため、MAB 認証用に外部 ID ソースとして使用される RADIUS トークン サーバーを設定しないことをお勧めします。そのため、認証は失敗します。MAB 要求の処理には、外部 RADIUS サーバー オプションを使用できます。

RADIUS トークンサーバーでサポートされる認証プロトコル

Cisco ISE では、RADIUS ID ソースに対して次の認証プロトコルがサポートされています。

- RADIUS PAP
- 内部拡張認証プロトコル汎用トークン カード（EAP-GTC）を含む保護拡張認証プロトコル（PEAP）
- 内部 EAP-GTC を含む EAP-FAST

RADIUS トークンサーバーで通信に使用されるポート

RADIUS ID トークン サーバーでは、認証セッションに UDP ポートが使用されます。このポートはすべての RADIUS 通信に使用されます。Cisco ISE で RADIUS ワンタイム パスワード（OTP）メッセージを RADIUS 対応トークン サーバーに送信するには、Cisco ISE と RADIUS 対応トークン サーバーの間のゲートウェイ デバイスが、UDP ポートを介した通信を許可するように設定されている必要があります。UDP ポートは、管理者ポータルを介して設定できます。

RADIUS 共有秘密

Cisco ISE で RADIUS ID ソースを設定するときに、共有秘密を指定する必要があります。この共有秘密情報は、RADIUSトークンサーバー上で設定されている共有秘密情報と同一である必要があります。

RADIUS トークン サーバーでのフェールオーバー

Cisco ISE では、複数の RADIUS ID ソースを設定できます。各 RADIUS ID ソースには、プライマリとセカンダリの RADIUS サーバーを指定できます。Cisco ISE からプライマリ サーバーに接続できない場合は、セカンダリ サーバーが使用されます。

RADIUS トークン サーバーの設定可能なパスワード プロンプト

RADIUS ID ソースでは、パスワード プロンプトを設定できます。パスワード プロンプトは、管理者ポータルを介して設定できます。

RADIUS トークン サーバーのユーザー認証

Cisco ISE は、ユーザー クレデンシャル（ユーザー名とパスコード）を取得し、RADIUS トークン サーバーに渡します。また、Cisco ISE は RADIUS トークン サーバー認証処理の結果をユーザーに中継します。

RADIUS トークン サーバーのユーザー属性キャッシュ

RADIUS トークン サーバーでは、デフォルトではユーザー ルックアップはサポートされていません。ただし、ユーザー ルックアップは次の Cisco ISE 機能に不可欠です。

- PEAP セッション再開：この機能によって、認証の成功後、EAP セッションの確立中に PEAP セッションを再開できます。
- EAP/FAST 高速再接続：この機能によって、認証の成功後、EAP セッションの確立中に高速再接続が可能になります。
- TACACS+ 許可：TACACS+ 認証に成功すると発生します。

Cisco ISE では、これらの機能のユーザー ルックアップ要求を処理するために、成功した認証の結果がキャッシュされます。成功した認証すべてについて、認証されたユーザーの名前と取得された属性がキャッシュされます。失敗した認証はキャッシュに書き込まれません。

キャッシュは、実行時にメモリで使用可能であり、分散展開の Cisco ISE ノード間で複製されません。管理者ポータルを介してキャッシュの存続可能時間（TTL）制限を設定できます。ISE 2.6 以降、ID キャッシング オプションを有効にして、エージング タイムを分単位で設定する場合があります。デフォルトでは、このオプションは無効です。有効にすると、指定した期間、メモリでキャッシュが使用できるようになります。

ID 順序での RADIUS ID ソース

ID ソース順序で認証順序用の RADIUS ID ソースを追加できます。ただし、属性取得順序用の RADIUS ID ソースを追加することはできません。これは、認証しないで RADIUS ID ソースを問い合わせることはできないためです。RADIUS サーバーによる認証中、Cisco ISE では異なるエラーを区別できません。すべてのエラーに対して RADIUS サーバーから Access-Reject メッセージが返されます。たとえば、RADIUS サーバーでユーザーが見つからない場合、RADIUS サーバーからは User Unknown ステータスの代わりに Access-Reject メッセージが返されます。

RADIUS サーバーがすべてのエラーに対して同じメッセージを返す

RADIUS サーバーでユーザーが見つからない場合、RADIUS サーバーからは Access-Reject メッセージが返されます。Cisco ISE では、管理者ポータルを使用してこのメッセージを [認証失敗（Authentication Failed）] メッセージまたは [ユーザーが見つからない（User Not Found）] メッセージとして設定するためのオプションを使用できます。ただし、このオプションを使用すると、ユーザーが未知の状況だけでなく、すべての失敗状況に対して「ユーザーが見つからない（User Not Found）」メッセージが返されます。

次の表は、RADIUS ID サーバーで発生するさまざまな失敗状況を示しています。

表 *36 :* エラー処理

失敗状況	失敗の理由
認証に失敗	• ユーザーが未知である。 • ユーザーが不正なパスコードでログインしようとしている。 • ユーザー ログイン時間が期限切れになった。
プロセスの失敗	• RADIUS サーバーが Cisco ISE で正しく設定されていない。 • RADIUS サーバーが使用できない。 • RADIUS パケットが偽装として検出されている。 • RADIUS サーバーとのパケットの送受信の問題。 • タイムアウト。
不明なユーザー	認証が失敗し、[拒否で失敗（Fail on Reject）] オプションが false に設定されている。

Safeword サーバーでサポートされる特別なユーザー名の形式

Safeword トークン サーバーでは、次のユーザー名フォーマットでの認証がサポートされています。

ユーザー名：Username, OTP

Cisco ISE では、認証要求を受信するとすぐにユーザー名が解析され、次のユーザー名に変換されます。

ユーザー名：Username

Safeword トークン サーバーでは、これらの両方のフォーマットがサポートされています。Cisco ISE はさまざまなトークン サーバーと連携します。SafeWord サーバーを設定する場合、Cisco ISE でユーザー名を解析して指定のフォーマットに変換するには、管理者ポータルで [SafeWord サーバー（SafeWord Server）] チェックボックスをオンにする必要があります。この変換は、要求が RADIUS トークン サーバーに送信される前に、RADIUS トークン サーバー ID ソースで実行されます。

RADIUS トークン サーバーでの認証要求と応答

Cisco ISE が RADIUS 対応トークン サーバーに認証要求を転送する場合、RADIUS 認証要求には次の属性が含まれます。

- User-Name（RADIUS 属性 1）
- User-Password（RADIUS 属性 2）
- NAS-IP-Address（RADIUS 属性 4）

Cisco ISE は次の応答のいずれかを受信すると想定されます。

- [Access-Accept]：属性は必要ありませんが、応答には RADIUS トークンサーバーの設定に基づいてさまざまな属性が含まれる場合があります。
- [Access-Reject]：属性は必要ありません。
- Access-Challenge：RADIUS RFC ごとに必要な属性は次のとおりです。
  - State（RADIUS 属性 24）
  - Reply-Message（RADIUS 属性 18）
  - 次の 1 つ以上の属性：Vendor-Specific、Idle-Timeout（RADIUS 属性 28）、Session-Timeout（RADIUS 属性 27）、Proxy-State（RADIUS 属性 33）

    Access-Challenge ではそれ以外の属性は使用できません。

RADIUS トークン ID ソースの設定

関連トピック

RADIUS トークン ID ソース （170 ページ）
RADIUS トークン サーバーの追加 （174 ページ）

RADIUS トークン 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）] > [追加（Add）]** を選択します。

ステップ 2 [一般（General）] タブおよび [接続（Connection）] タブに値を入力します。

ステップ 3 [認証（Authentication）] タブをクリックします。

このタブでは、RADIUS トークン サーバーからの Access-Reject メッセージへの応答を制御できます。この応答は、クレデンシャルが無効であること、またはユーザーが不明であることのいずれかを意味する場合があります。Cisco ISE は、認証失敗か、またはユーザーが見つからないかのいずれかの応答を受け入れます。このタブでは、ID キャッシングを有効にし、キャッシュのエージング タイムを設定することもできます。パスワードを要求するプロンプトを設定することもできます。

a) RADIUS トークン サーバーからの Access-Reject 応答を認証失敗として処理する場合は、[拒否を「認証失敗」として処理（Treat Rejects as 'authentication failed'）] オプション ボタンをクリックします。

b) RADIUS トークン サーバーからの Access-Reject 応答を未知ユーザー エラーとして処理する場合は、[拒否を「ユーザーが見つからない」として処理（Treat Rejects as 'user not found'）] オプション ボタンをクリックします。

ステップ 4 RADIUS トークン サーバーとの最初の認証の成功の後、Cisco ISE でキャッシュにパスコードを保存し、設定された期間内に発生した後続の認証に対しキャッシュされたユーザーのクレデンシャルを使用する場合、[パスコード キャッシングの有効化（Enable Passcode Caching）] チェック ボックスをオンにします。

パスコードをキャッシュ内に保存する必要がある秒数を [エージング タイム（Aging Time）] フィールドに入力します。この期間内にユーザーは同じパスコードで複数回の認証を行うことができます。デフォルト値は 30 秒です。有効な範囲は 1 ～ 300 秒です。

（注） Cisco ISE は、認証が初めて失敗した後でキャッシュをクリアします。ユーザーは新しい有効なパスコードを入力する必要があります。

（注） EAP-FAST-GTC などの、パスコードの暗号化をサポートするプロトコルを使用する場合にのみこのオプションを有効にすることを強く推奨します。RADIUS トークン サーバーでサポートされている認証プロトコルについては、次を参照してください。RADIUS トークンサーバーでサポートされる認証プロトコル （171 ページ）

ステップ 5 サーバーに対する認証を実行しない要求の処理を許可する場合は、[ID キャッシングの有効化（Enable Identity Caching）] チェックボックスをオンにします。

ID キャッシング オプションを有効にし、エージング タイムを分単位で設定できます。デフォルト値は 120 分です。有効な範囲は、1 ～ 1440 分です。最後に成功した認証から取得された結果と属性が、指定した時間、キャッシュ内に保持されます。

このオプションはデフォルトでは無効になっています。

ステップ 6 [許可（Authorization）] タブをクリックします。

このタブでは、Cisco ISE への Access-Accept 応答を送信中に RADIUS トークン サーバーによって返されるこの属性に対して表示される名前を設定できます。この属性は、許可ポリシー条件で使用できます。デフォルト値は CiscoSecure-Group-Id です。

（注） 外部 ID ソースから Access-Accept で属性を送信する場合、外部 ID ソースは属性名および値として <ciscoavpair> を ACS 形式（<attrname>=<attrvalue>）で送信する必要があります。<attrname> は [許可（Authorization）] タブで設定します。

ステップ 7 **[送信（Submit）]** をクリックします。

RADIUS トークン サーバーの削除

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。
- ID ソース順序に含まれる RADIUS トークン サーバーを選択していないことを確認します。ID ソース順序に含まれる RADIUS トークン サーバーを削除用に選択した場合、削除操作は失敗します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[ID 管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[RADIUS トークン（RADIUS Token）]** を選択します。

ステップ 2 削除する RADIUS トークン サーバーの隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして、選択した RADIUS トークン サーバーを削除します。

削除する RADIUS トークン サーバーを複数選択し、その 1 つが ID ソース順序で使用されている場合、削除操作は失敗し、いずれの RADIUS トークン サーバーも削除されません。

RSA ID ソース

Cisco ISE では、外部データベースとして RSA SecurID サーバーがサポートされています。RSA SecurID の 2 要素認証は、ユーザーの PIN と、タイム コード アルゴリズムに基づいて使い捨てのトークン コードを生成する個別に登録された RSA SecurID トークンで構成されます。異なるトークン コードが固定間隔（通常は 30 または 60 秒ごと）で生成されます。RSA SecurID サーバーでは、この動的な認証コードが検証されます。各 RSA SecurID トークンは固有であり、過去のトークンに基づいて将来のトークンの値を予測することはできません。そのため、正しいトークン コードが PIN とともに提示された場合、その人が有効なユーザーである確実性が高くなります。したがって、RSA SecurID サーバーでは、従来の再利用可能なパスワードよりも信頼性の高い認証メカニズムが提供されます。

Cisco ISE では、次の RSA ID ソースがサポートされています。

- RSA ACE/Server 6.x シリーズ
- RSA Authentication Manager 7.x および 8.0 シリーズ

次のいずれかの方法で、RSA SecurID 認証テクノロジーと統合できます。

- RSA SecurID エージェントの使用：ユーザーは、RSA のネイティブプロトコルによってユーザー名とパスコードで認証されます。
- RADIUS プロトコルの使用：ユーザーは、RADIUS プロトコルによってユーザー名とパスコードで認証されます。

Cisco ISE の RSA SecurID トークン サーバーは、RSA SecurID 認証テクノロジーと RSA SecurID エージェントを使用して接続します。

Cisco ISE では、1 つの RSA 領域だけがサポートされています。

Cisco ISE と RSA SecurID サーバーの統合

Cisco ISE と RSA SecurID サーバーを接続するには、次の 2 つの管理ロールが必要です。

- RSA サーバー管理者：RSA システムおよび統合を設定および維持します。
- Cisco ISE 管理者：Cisco ISE を RSA SecurID サーバーに接続するように設定し、設定を維持します。

ここでは、Cisco ISE に RSA SecurID サーバーを外部 ID ソースとして接続するために必要なプロセスについて説明します。RSA サーバーについての詳細は、RSA に関するドキュメントを参照してください。

Cisco ISE の RSA 設定

RSA 管理システムでは sdconf.rec ファイルが生成されます。このファイルは RSA システム管理者によって提供されます。このファイルを使用すると、Cisco ISE サーバーを領域内の RSA SecurID エージェントとして追加できます。このファイルを参照して Cisco ISE に追加する必要があります。プライマリ Cisco ISE サーバーは、複製のプロセスによってこのファイルをすべてのセカンダリ サーバーに配布します。

RSA SecurID サーバーに対する RSA エージェント認証

sdconf.rec ファイルがすべての Cisco ISE サーバーにインストールされると、RSA エージェント モジュールが初期化され、RSA 生成のクレデンシャルによる認証が各 Cisco ISE サーバーで実行されます。展開内の各 Cisco ISE サーバー上のエージェントが正常に認証されると、RSA サーバーとエージェント モジュールは securid ファイルをダウンロードします。このファイルは Cisco ISE ファイル システムに存在し、RSA エージェントによって定義された既知の場所にあります。

分散 Cisco ISE 環境の RSA ID ソース

分散 Cisco ISE 環境で RSA ID ソースを管理するには、次の操作が必要です。

- sdconf.rec および sdopts.rec ファイルのプライマリ サーバーからセカンダリ サーバーへの配布。
- securid および sdstatus.12 ファイルの削除。

Cisco ISE 展開の RSA サーバーの更新

Cisco ISE で sdconf.rec ファイルを追加した後、RSA サーバーを廃止する場合、または新しい RSA セカンダリ サーバーを追加する場合、RSA SecurID 管理者は sdconf.rec ファイルを更新することがあります。更新されたファイルは RSA SecurID 管理者によって提供されます。更新されたファイルによって Cisco ISE を再設定できます。Cisco ISE では、更新されたファイルが複製プロセスによって展開内のセカンダリ Cisco ISE サーバーに配布されます。Cisco ISE では、まずファイル システムのファイルを更新し、RSA エージェント モジュールに合わせて調整して再起動プロセスを適切に段階的に行います。sdconf.rec ファイルが更新されると、sdstatus.12 および securid ファイルがリセット（削除）されます。

自動 RSA ルーティングの上書き

領域内に複数の RSA サーバーを持つことができます。sdopts.rec ファイルはロード バランサの役割を果たします。Cisco ISE サーバーと RSA SecurID サーバーはエージェント モジュールを介して動作します。Cisco ISE に存在するエージェント モジュールは、領域内の RSA サーバーを最大限に利用するためにコストベースのルーティング テーブルを保持します。ただし、領域の各 Cisco ISE サーバーの手動設定を使用してこのルーティングを上書きするには、管理者ポータルで sdopts.rec と呼ばれるテキスト ファイルを使用します。このファイルの作成方法については、RSA に関するドキュメントを参照してください。

RSA ノード秘密リセット

securid ファイルは秘密ノード キー ファイルです。RSA が最初に設定されると、RSA では秘密を使用してエージェントが検証されます。Cisco ISE に存在する RSA エージェントが RSA サーバーに対して初めて正常に認証されると、securid と呼ばれるファイルがクライアント マシン上に作成され、このファイルを使用して、マシン間で交換されるデータが有効であることが確認されます。展開内の特定の Cisco ISE サーバーまたはサーバーのグループから securid ファイルを削除する必要がある場合があります（たとえば、RSA サーバーでのキーのリセット後など）。領域に対する Cisco ISE サーバーからこのファイルを削除するには、Cisco ISE 管理者ポータルを使用できます。Cisco ISE の RSA エージェントが次回正常に認証されたとき、新しい securid ファイルが作成されます。

（注） Cisco ISE の最新リリースへのアップグレード後に認証が失敗した場合は、RSA 秘密をリセットします。

RSA の自動可用性のリセット

sdstatus.12 ファイルは、領域内の RSA サーバーのアベイラビリティに関する情報を提供します。たとえば、いずれのサーバーがアクティブで、いずれのサーバーがダウンしているかに関する情報を提供します。エージェント モジュールは領域内の RSA サーバーと連携して、このアベイラビリティ ステータスを維持します。この情報は、sdstatus.12 ファイルに連続的に表示されます。このファイルは、Cisco ISE ファイル システムの既知の場所に供給されます。このファイルは古くなり、現在のステータスが反映されていないことがあります。その場合、現在のステータスが反映されるように、このファイルを削除する必要があります。特定の領域に対する固有の Cisco ISE サーバーからファイルを削除するには、管理者ポータルを使用できます。Cisco ISE は RSA エージェントに合わせて調整して、再起動が正しく段階的に行われるようにします。

sdstatus.12 ファイルは、securid ファイルがリセットされるか、あるいは sdconf.rec ファイルまたは sdopts.rec ファイルが更新されるたびに削除されます。

RSA SecurID ID ソースの設定

RSA プロンプトの設定

次の表では、[RSA プロンプト（RSA Prompts）] タブ内のフィールドについて説明します。

表 *37 : RSA* プロンプトの設定

フィールド名	使用上のガイドライン
パスコード プロンプトの入力（**Enter Passcode Prompt**）	パス コードを取得するテキスト文字列を入力します。
次のトークン コードの入力（**Enter Next Token Code**）	次のトークンを要求するテキスト文字列を入力します。
PIN タイプの選択（**Choose PIN Type**）	PIN タイプを要求するテキスト文字列を入力します。
システム PIN の受け入れ（**Accept System PIN**）	システム生成の PIN を受け付けるテキスト文字列を入力します。
英数字 PIN の入力（**Enter Alphanumeric PIN**）	英数字 PIN を要求するテキスト文字列を入力します。
数値 PIN の入力（**Enter Numeric PIN**）	数値 PIN を要求するテキスト文字列を入力します。
PIN の再入力（**Re-enter PIN**）	ユーザーに PIN の再入力を要求するテキスト文字列を入力します。

RSA メッセージ設定（RSA Message Settings）

次の表では、[RSA メッセージ（RSA Messages）] タブ内のフィールドについて説明します。

表 *38 : RSA* メッセージ設定（*RSA Messages Settings*）

フィールド名	使用上のガイドライン
システム PIN メッセージの表示（Display System PIN Message）	システム PIN メッセージのラベルにするテキスト文字列を入力します。
システム PIN 通知の表示（Display System PIN Reminder）	ユーザーに新しい PIN を覚えるように通知するテキスト文字列を入力します。
数字を入力する必要があるエラー（Must Enter Numeric Error）	PIN には数字のみを入力するようにユーザーに指示するメッセージを入力します。
英数字を入力する必要があるエラー（Must Enter Alpha Error）	PINには英数字のみを入力するようにユーザーに指示するメッセージを入力します。
PIN 受け入れメッセージ（PIN Accepted Message）	ユーザーの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
PIN 拒否メッセージ（PIN Rejected Message）	ユーザーの PIN がシステムによって拒否されたときに表示されるメッセージを入力します。
ユーザーの PIN が異なるエラー（User Pins Differ Error）	ユーザーが不正な PIN を入力したときに表示されるメッセージを入力します。
システム PIN 受け入れメッセージ（System PIN Accepted Message）	ユーザーの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。
不正パスワード長エラー（Bad Password Length Error）	ユーザーが指定した PIN が、PIN 長ポリシーで指定されている範囲に収まらない場合に表示されるメッセージを入力します。

関連トピック

RSA ID ソース （176 ページ）
Cisco ISE と RSA SecurID サーバーの統合 （177 ページ）
RSA ID ソースの追加 （180 ページ）

RSA ID ソースの追加

RSA ID ソースを作成するには、RSA コンフィギュレーション ファイル（sdconf.rec）をインポートする必要があります。RSA 管理者から sdconf.rec ファイルを取得する必要があります。こ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。

RSA ID ソースを追加するには、次のタスクを実行します。

RSA コンフィギュレーション ファイルのインポート

Cisco ISE に RSA ID ソースを追加するには、RSA コンフィギュレーション ファイルをインポートする必要があります。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[ID 管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[RSA SecurID]** > **[追加（Add）]** を選択します。

ステップ 2 [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新しい sdconf.rec ファイルまたは更新された sdconf.rec ファイルを選択します。

初めて RSA ID ソースを作成する場合、[新しい sdconf.rec ファイルのインポート（Import new sdconf.rec file）] フィールドは必須フィールドです。これ以降は、既存の sdconf.rec ファイルを更新されたファイルで置き換えることができますが、既存のファイルの置き換えは任意です。

ステップ 3 サーバーのタイムアウト値を秒単位で入力します。Cisco ISE はタイムアウトになる前に、指定された秒数 RSA サーバーからの応答を待ちます。この値には、1 ～ 199 の任意の整数を指定できます。デフォルト値は 30 秒です。

ステップ 4 PIN が変更された場合に強制的に再認証するには、[変更 PIN で再認証（Reauthenticate on Change PIN）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

Cisco ISE は、次のシナリオもサポートします。

- Cisco ISE サーバーのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット。
- RSA ID ソースの認証制御オプションの設定。

Cisco ISE サーバーのオプション ファイルの設定および SecurID ファイルと sdstatus.12 ファイルのリセット

ステップ 1 Cisco ISE サーバーにログインします。

ステップ 2 **[管理（Administration）]** > **[ID の管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[RSA SecurID]** > **[追加（Add）]** を選択します。

ステップ 3 [RSA インスタンス ファイル（RSA Instance Files）] タブをクリックします。

このページには、展開内のすべての Cisco ISE サーバーの sdopts.rec servers ファイルが一覧表示されます。

ユーザーが RSA SecurID トークン サーバーに対して認証されると、ノードのシークレット ステータスは [作成済み（Created）] と表示されます。ノードのシークレット ステータスは、[作成済み（Created）] また

は [未作成（Not Created）] のどちらかになります。消去されると、ノードのシークレット ステータスは [未作成（Not Created）] と表示されます。

ステップ 4 特定の Cisco ISE サーバーの sdopts.rec ファイルの横にあるオプション ボタンをクリックし、[オプション ファイルの更新（Update Options File）] をクリックします。

[現在のファイル（Current File）] 領域に既存のファイルが表示されます。

ステップ 5 次のいずれかを実行します。

- [RSA エージェントが保持する自動ロード バランシング ステータスを使用（Use the Automatic Load Balancing status maintained by the RSA agent）]：RSA エージェントでロード バランシングを自動的に管理する場合は、このオプションを選択します。
- [次で選択された sdopts.rec ファイルで自動ロード バランシング ステータスを上書き（Override the Automatic Load Balancing status with the sdopts.rec file selected below）]：特定のニーズに基づいて手動でロード バランシングを設定する場合は、このオプションを選択します。このオプションを選択する場合は、[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新しい sdopts.rec ファイルを選択する必要があります。

ステップ 6 [OK] をクリックします。

ステップ 7 Cisco ISE サーバーに対応する行をクリックして、そのサーバーの securid および sdstatus.12 ファイルをリセットします。

a) ドロップダウン矢印をクリックし、[securid ファイルのリセット（Reset securid File）] 列と [sdstatus.12 ファイルのリセット（Reset sdstatus.12 File）] 列の [送信で削除（Remove on Submit）] を選択します。

（注） [sdstatus.12 ファイルのリセット（Reset sdstatus.12 File）] フィールドはユーザーのビューから非表示になっています。このフィールドを表示するには、最も内側のフレームで垂直および水平スクロール バーを使用して、下にスクロールし、次に右にスクロールします。

b) この行で [保存（Save）] をクリックして変更を保存します。

ステップ 8 [保存（Save）] をクリックします。

RSA ID ソースの認証制御オプションの設定

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、**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID] > [追加（Add）]** を選択します。

ステップ 2 [認証制御（Authentication Control）] タブをクリックします。

ステップ 3 次のいずれかを実行します。

- [拒否を「認証失敗」として処理（Treat Rejects as "authentication failed"）]：拒否された要求を認証失敗として処理する場合は、このオプションを選択します。

- [拒否を「ユーザーが見つからない」として処理（Treat Rejects as "user not found"）]：拒否された要求をユーザーが見つからないエラーとして処理する場合は、このオプションを選択します。

ステップ 4 最初に認証が成功した後にCisco ISEがキャッシュにパスコードを保存し、設定された期間内に認証が行われた場合にキャッシュされたユーザー クレデンシャルを後続の認証のために使用するようにする場合は、[パスコード キャッシュの有効化（Enable Passcode Caching）] チェック ボックスにマークを付けます。

パスコードをキャッシュ内に保存する必要がある秒数を [エージング タイム（Aging Time）] フィールドに入力します。この期間内にユーザーは同じパスコードで複数回の認証を行うことができます。デフォルト値は 30 秒です。有効な範囲は 1 ～ 300 秒です。

（注） Cisco ISE は、認証が初めて失敗した後でキャッシュをクリアします。ユーザーは新しい有効なパスコードを入力する必要があります。

（注） EAP-FAST-GTC などの、パスコードの暗号化をサポートするプロトコルを使用する場合にのみこのオプションを有効にすることを強く推奨します。

ステップ 5 サーバーに対する認証を実行しない要求の処理を許可する場合は、[ID キャッシングの有効化（Enable Identity Caching）] チェックボックスをオンにします。

ID キャッシング オプションを有効にし、エージング タイムを分単位で設定できます。デフォルト値は 120 分です。有効な範囲は、1 ～ 1440 分です。最後に成功した認証から取得された結果と属性が、指定した時間、キャッシュ内に保持されます。

このオプションはデフォルトでは無効になっています。

ステップ 6 [**保存（Save**）] をクリックして、設定を保存します。

RSA プロンプトの設定

Cisco ISE では、RSA SecurID サーバーに送信される要求の処理中にユーザーに表示される RSA プロンプトを設定できます。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[ID 管理（Identity Management）]** > **[外部 ID ソース（External Identity Sources）]** > **[RSA SecurID]** を選択します。

ステップ 2 [プロンプト（Prompts）] をクリックします。

ステップ 3 「RSA SecurID ID ソースの設定」の説明に従って、値を入力します。

ステップ 4 **[送信（Submit）]** をクリックします。

RSA メッセージの設定

Cisco ISE では、RSA SecurID サーバーに送信される要求の処理中にユーザーに表示されるメッセージを設定できます。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID]** を選択します。

ステップ 2 [プロンプト（Prompts）] をクリックします。

ステップ 3 [メッセージ（Messages）] タブをクリックします。

ステップ 4 「RSA SecurID ID ソースの設定」の説明に従って、値を入力します。

ステップ 5 **[送信（Submit）]** をクリックします。

外部 ID ソースとしての SAMLv2 ID プロバイダ

Security Assertion Markup Language（SAML）は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のアプリケーションにシームレスにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。SAML により、ID プロバイダ（IdP）とサービス プロバイダ（この場合は ISE）の間で、セキュリティ認証情報を交換できます。

SAML シングル サインオン（SSO）は、IdP とサービス プロバイダの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。サービス プロバイダは IdP のユーザー情報を信頼して、さまざまなサービスやアプリケーションにアクセスできるようにします。

SAML SSO を有効にすると、次のようないくつかの利点が得られます。

- 異なるユーザー名とパスワードの組み合わせを入力する必要がなくなるため、パスワードの劣化が軽減します。
- 同じ ID に資格情報を再入力する時間が省けるため、生産性が向上します。
- アプリケーションをホストしているお使いのシステムからサードパーティのシステムに、認証を転送します。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

IdPは、ユーザー、システム、またはサービスのID情報を作成、維持、管理する認証モジュールです。IdPは、ユーザークレデンシャルを保管、検証し、ユーザーがサービスプロバイダの保護リソースにアクセスできる SAML 応答を生成します。

（注） IdPサービスをよく理解している必要があります。現在インストールされていて、操作可能であることを確認してください。

SAML SSO は次のポータルでサポートされます。

- ゲスト ポータル（スポンサー付きおよびアカウント登録）
- スポンサー ポータル
- デバイス ポータル
- 証明書プロビジョニング ポータル

（注） セッションサービスは、SAML SSO を有効にするノードで有効にする必要があります。このオプションを有効にするには、次の手順を実行します。

1. [管理（Administration）] > [システム（System）] > [展開（Deployment）] の順に選択します。
2. ノードを選択して、[編集（Edit）] をクリックします。
3. [全般設定（General Settings）] タブで [ポリシーサービス（Policy Service）] トグルボタンを有効にします。
4. [セッションサービスの有効化（Enable Session Services）] チェックボックスをオンにして、[保存（Save）] をクリックします。

BYOD ポータルでは外部 ID ソースとして IdP を選択できませんが、ゲスト ポータルでは IdP を選択し、BYOD フローをイネーブルにできます。

Cisco ISE は SAMLv2 に準拠しており、Base64 でエンコードされた証明書を使用するすべての SAMLv2 準拠 IdP をサポートしています。次に示す IdP が Cisco ISE でテストされました。

- Oracle Access Manager（OAM）
- Oracle Identity Federation（OIF）
- SecureAuth
- PingOne
- PingFederate
- Azure Active Directory

IdP は、ID ソース順序に追加できません。

指定された時間（デフォルトでは5分）にアクティビティがない場合は、SSOセッションが終了し、セッション タイムアウトのエラー メッセージが表示されます。

ポータルの [エラー（Error）] ページに [再度サインオン（Sign On Again）] ボタンを追加する場合は、[ポータルエラー（Portal Error）] ページの [オプションコンテンツ（Optional Content）] フィールドに次の JavaScript を追加します。

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'"
type="button">再サインオン</button>
```

SAML ID プロバイダの追加

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 証明書が IdP で自己署名されていない場合は、信頼できる証明書ストアに認証局（CA）証明書をインポートします。[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）] の順に選択し、CA 証明書をインポートします。

ステップ 2 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）][ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [外部 ID ソース（External Identity Sources）] を選択します。

ステップ 3 [SAML ID プロバイダ（SAML Id Providers）] 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 [SAML ID プロバイダ（SAML Identity Provider）] ページで、次の詳細情報を入力します。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 [ポータル設定（Portal Settings）] ページ（ゲスト ポータル、証明書プロビジョニングまたはデバイス ポータル）に移動して、[認証方式（Authentication Method）] フィールドでそのポータルにリンクする IdP を選択します。

[ポータル設定（Portal Settings）] ページにアクセスするには、次の手順を実行します。

- ゲスト ポータル：**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals and Components）] > [ゲストポータル（Guest Portals）] > [作成、編集または複製（Create, Edit, or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** の順に選択します（『』の「クレデンシャルを持つゲスト ポータルのポータル設定」のセクションクレデンシャルを持つゲスト ポータルのポータル設定を参照してください）。

- スポンサー ポータル：**[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals and Components）] > [スポンサーポータル（Sponsor Portals）] > [作成、編集または複製（Create, Edit, or Duplicate）] > [ポータルの動作およびフローの設定（Portal**

Behavior and Flow Settings）] > [ポータル設定（Portal Settings）] の順に選択します（スポンサーポータルのポータル設定を参照してください）。

- デバイス ポータル：**[ワークセンター（Work Centers）] > [BYOD] > [設定（Configure）] > [デバイスポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit, or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** [管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [デバイス（My Devices）] > [作成、編集または複製（Create, Edit, or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]を選択します（デバイスポータルのポータル設定を参照してください）。
- 証明書プロビジョニング ポータル：[管理（Administration）] > [デバイスポータル管理（Device Portal Management）] > [証明書プロビジョニング（Certificate Provisioning）] > [作成、編集または複製（Create, Edit, or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）] の順に選択します（「証明書プロビジョニング ポータルのポータル設定」を参照してください）。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [SAML ID プロバイダ（SAML Id Providers）][ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [外部 ID ソース（External Identity Sources）] > [SAML ID プロバイダ（SAML Id Providers）] を選択します。そのポータルにリンクする IdP を選択し、[編集（Edit）] をクリックします。

ステップ 10 （オプション）[サービス プロバイダ情報（Service Provider Info）] タブで、ロード バランサの詳細を追加します。ISE ノードの前にロード バランサを追加することで、ID プロバイダの設定を簡素化し、ISE ノードの負荷を最適化できます。

ロード バランサはソフトウェアベースまたはハードウェアベースのアプライアンスである可能性があります。導入の ISE ノードに要求を転送できる必要があります（[ポータル設定（Portal Settings）] ページで指定されたポートを使用して）。

ロード バランサを使用する場合は、ロード バランサの URL のみがサービス プロバイダのメタデータ ファイルで提供されます。ロードバランサが追加されていない場合は、複数の AssertionConsumerService URL がサービス プロバイダのメタデータ ファイルに含まれます。

（注） ポータル FQND 設定でロード バランサに同じ IP アドレスを使用しないようにすることが推奨されます。

ステップ 11 [サービスプロバイダ情報（Service Provider Info）] タブで、[エクスポート（Export）] をクリックして、サービス プロバイダのメタデータ ファイルをエクスポートします。

エクスポートされたメタデータには、Cisco ISE の署名証明書が含まれています。署名証明書は、選択したポータルの証明書と同一です。

エクスポートされたメタデータの ZIP ファイルには、各 IdP の設定に関する基本的な説明を含む Readme ファイルが含まれています（Azure Active Directory、PingOne、PingFederate、SecureAuth、OAM など）。

（注） ロードバランサが設定されていない、または次のようなポータル設定に変更がある場合は、サービス プロバイダのメタデータを再度エクスポートする必要があります。

- 新しい ISE ノードが登録された場合
- ノードのホスト名または IP アドレスが変更された場合
- デバイス、スポンサー、または証明書プロビジョニング ポータルの完全修飾ドメイン名（FQDN）が変わりました
- ポートまたはインターフェイス設定が変更された

更新されたメタデータが再エクスポートされない場合、ユーザー認証が IdP 側で失敗する可能性があります。

ステップ 12 ダイアログボックスで [参照（Browse）] をクリックして、圧縮ファイルをローカルに保存します。メタデータ ファイルのフォルダを解凍します。フォルダを解凍すると、ポータルの名前が付いたメタデータ ファイルを取得します。メタデータ ファイルには、プロバイダ ID とバインディング URI が含まれています。

ステップ 13 管理ユーザーとして IdP にログインし、サービス プロバイダのメタデータ ファイルをインポートします。サービス プロバイダのメタデータ ファイルをインポートする方法の詳細については、ID プロバイダのメタデータ ファイルをインポートする方法の詳細については、ID プロバイダのユーザーユーザーマニュアルを参照してください。

ステップ 14 [グループ（Groups）] タブで、必要なユーザー グループを追加します。

[グループ メンバーシップ属性（Group Membership Attribute）] フィールドにユーザーのグループ メンバーシップを指定するアサーション属性を入力します。

ステップ 15 [属性（Attributes）] タブにユーザー属性を追加します。属性を追加するときに、属性が IdP から返されたアサーションでどのように表示されるかを指定できます。[ISE の名前（Name in ISE）] フィールドに指定した名前はポリシー ルールに表示されます。属性でサポートされているのは、次のデータ型です。

- 文字列
- 整数（Integer）
- IPv4
- ブール値

（注） グループと属性の追加は必須ではありません。これらのグループと属性は、ポリシーとルールの設定に使用できます。スポンサー ポータルを使用している場合は、グループを追加してこれらのグループを選択し、スポンサー グループの設定を構成することができます。

ステップ 16 [詳細設定（Advanced Settings）] タブで、次のオプションを設定します。

- [ID属性（Identity Attribute）] : 認証中のユーザーの ID を指定する属性を選択します。[属性（Attribute）] ドロップダウン リストからサブジェクト名属性または属性を選択できます。

（注） Cisco ISE は、件名（NameID）が一時的なまたは永続的な形式で含まれる SAML IdP 応答をサポートしていません。このような方法が使用され、認証が失敗する場合、Cisco ISE は SAML IdP 応答からユーザー名属性アサーションを取得できません。

- [メール属性（Email attribute）]：スポンサーの電子メール アドレスを含む属性を選択します。これには、セルフサービスのゲストの要求とスポンサーが一致する必要があります。
- [メール属性（Email attribute）]：ユーザーの電子メール アドレスを返すアサーション属性を選択します。スポンサー付きゲストのリストが 1 人のスポンサーに承認されるようにフィルタリング（制限）する場合は、メール属性を設定する必要があります。
- 複数値属性の場合は、次のいずれかのオプションを選択します。
  - [個別のXML要素で各値（Each value in a separate XML element）]：個別の XML 要素で同じ属性の複数の値を IdP が返すには、このオプションをクリックします。
  - [単一の XML 要素で複数の値（Multiple values in a single XML element）]：単一の XML 要素で複数値を IdP が返すには、このオプションをクリックします。テキスト ボックスにデリミタを指定できます。
- ログアウト設定（Logout Settings）
  - [ログアウト要求の署名（Sign Logout Requests）]：ログアウト要求に署名され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。このオプションは、OAMおよびOIFでは表示されません。

    （注） SecureAuth は SAML ログアウトをサポートしていません。

  - [ログアウト URL（Logout URL）]：ロード バランサが設定されていなければ、このオプションは OAM および OIF だけに表示されます。ユーザーがスポンサー ポータルまたはデバイス ポータルからログアウトすると、ユーザーは SSO セッションを終了するために IdP でログアウト URL にリダイレクトされ、その後、ログイン ページにリダイレクトされます。
  - [リダイレクト パラメータ名（Redirect Parameter Name）]：ロード バランサが設定されていなければ、このオプションは OAM および OIF だけに表示されます。リダイレクト パラメータは、ユーザーがログアウト後にリダイレクトされる必要があるログインページのURLを渡すために使用されます。リダイレクト パラメータ名は、IdP に基づいて異なる場合があります（たとえば end_url や returnURL）。このフィールドは大文字と小文字が区別されます。

    ログアウトが正常に動作しない場合は、ログアウトURLおよびリダイレクトパラメータ名について、ID プロバイダのマニュアルを確認してください。マニュアルを確認してください。

ステップ 17 [送信（Submit）] をクリックします。

例

Ping Federate の設定の例については、『**Configure ISE 2.1 Guest Portal with PingFederate SAML SSO**』を参照してください。

ID プロバイダの削除

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。

削除する IdP がいずれのポータルにもリンクされていないことを確認します。IdP がポータルにリンクされている場合、削除操作は失敗します。

ステップ 1

ステップ 2 削除する IdP の隣のチェックボックスをオンにして、[削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして、選択した IdP を削除します。

認証失敗ログ

SAML ID ストアに対する認証が失敗し、IdP がユーザーを ISE ポータルに（SAML 応答を通じて）リダイレクトすると、ISE は認証ログに障害の理由を報告します。ゲスト ポータルで（BYOD フローの有効無効に関係なく）、認証の失敗の原因を知るために、RADIUS Livelog（[操作（Operations）] > [RADIUS] > [ライブ ログ（Live Logs）]）を確認できます。ポータルおよびスポンサー ポータル認証失敗の原因を把握するためには、デバイス ポータルおよびスポンサー ポータルで、デバイス ログイン/監査レポートとスポンサー ログイン/監査レポート（[操作（Operations）] > [レポート（Reports）] > [ゲスト（Guest）]）を確認できます。

ログアウトで障害が発生した場合、My Devices、スポンサーおよびゲスト ポータルの障害の原因を知るためにレポートおよびログを確認することができます。

認証が失敗する原因には次のものが考えられます。

- SAML 応答の解析エラー
- SAML 応答の検証エラー（不正な発行者など）
- SAML アサーションの検証エラー（誤った対象者など）
- SAML 応答署名の検証エラー（不正な署名など）
- IdP 署名証明書のエラー（失効した証明書など）

（注） Cisco ISEは、暗号化されたアサーションを含むSAML応答をサポートしていません。IdPで設定すると、ISEに次のエラーメッセージが表示されます：`FailureReason=24803 Unable to find 'username' attribute assertion`。

認証に失敗した場合は、認証ログの「DetailedInfo」属性を確認することを推奨します。この属性では、障害理由に関する追加情報が提供されます。

ID ソース順序

ID ソース順序は、Cisco ISE がそれぞれ異なるデータベース内でユーザー クレデンシャルを検索する順序を定義します。

Cisco ISE に接続されている 2 つ以上のデータベースにユーザー情報がある場合、Cisco ISE でこれらの ID ソース内の情報を検索する順序を定義できます。一致が見つかると、Cisco ISE はそれ以上の検索を行いませんが、クレデンシャルを評価し、ユーザーに結果を返します。このポリシーは最初の一致ポリシーです。

ID ソース順序の作成

始める前に

Cisco ISE に外部 ID ソースを設定していることを確認します。

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。

ゲストユーザーがローカル WebAuth を使用して認証できるようにするには、ゲストポータル認証ソースと ID ソース順序の両方に同じ ID ストアが含まれるように設定する必要があります。

ステップ 1 **[管理（Administration）] > [ID 管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）] >** [追加（Add）] を選択します。

ステップ 2 ID ソース順序の名前を入力します。また、任意で説明を入力できます。

ステップ 3 [証明書認証プロファイル（Certificate Authentication Profile）] チェックボックスをオンにし、証明書ベースの認証のための証明書認証プロファイルを選択します。

ステップ 4 [選択済み（Selected）] リストフィールドの ID ソース順序に含めるデータベースを選択します。

ステップ 5 Cisco ISE がデータ ベースを検索する順序に [選択済み（Selected）] リストフィールドのデータベースを並べ替えます。

ステップ 6 選択したアイデンティティストアに認証のためにアクセスできない場合は、[高度な検索リスト（Advanced Search List）] 領域で次のいずれかのオプションを選択します。

- [順序内の他のストアにアクセスせず、AuthenticationStatus属性をProcessErrorに設定（Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError）]

- [ユーザーが見つからなかったとして処理し、順序内の次のストアに進む（Treat as if the user was not found and proceed to the next store in the sequence）]

  Cisco ISE では、要求の処理中にこれらの ID ソースが順番に検索されます。[選択済み（Selected）] リストフィールドに Cisco ISE が ID ソースを検索する順序で ID ソースが表示されていることを確認します。

ステップ 7 [送信（Submit）] をクリックして ID ソース順序を作成すると、その後この ID ソース順序をポリシーで使用できます。

ID ソース順序の削除

ポリシーで今後使用しない ID ソース順序を削除できます。

始める前に

- 削除する ID ソース順序がいずれの認証ポリシーでも使用されていないことを確認してください。
- 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 **[管理（Administration）] > [ID の管理（Identity Management）] > [ID ソース順序（Identity Source Sequences）]** を選択します。

ステップ 2 削除する ID ソース順序の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

ステップ 3 [OK] をクリックして ID ソース順序を削除します。

レポートでの ID ソースの詳細

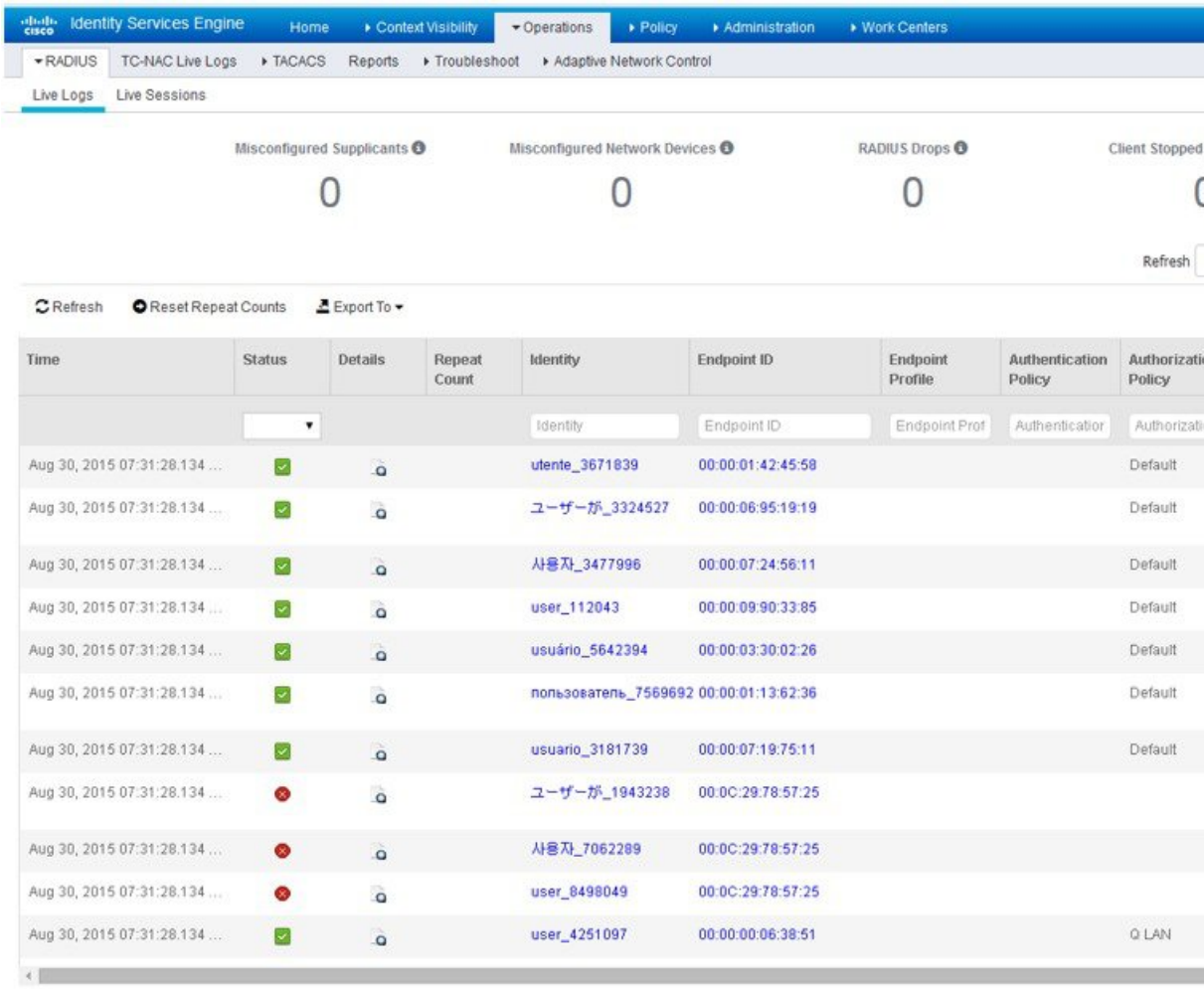
Cisco ISE は認証ダッシュレットおよび ID ソース レポートで ID ソースに関する情報を提供します。

[認証（Authentications）] ダッシュレット

[認証（Authentications）] ダッシュレットから、障害の理由などの詳細情報にドリルダウンできます。

[操作（Operations）] > [RADIUS ライブログ（RADIUS Livelog）] の順に選択して、リアルタイムで認証の概要を表示します。RADIUS ライブ ログの詳細については、RADIUS ライブ ログを参照してください。

図 *17 : RADIUS* ライブ ログ



ID ソース レポート

Cisco ISE は ID ソースに関する情報を含むさまざまなレポートを提供します。これらのレポートの詳細については、「使用可能なレポート」の項を参照してください。

ネットワークのプロファイリングされたエンドポイント

プロファイラ サービスは、ネットワーク上にあるすべてのエンドポイントの機能（Cisco ISE では ID とも呼ばれる）を、デバイス タイプにかかわらず識別、検索、および特定して、企業ネットワークへの適切なアクセスを保証および維持するのに役立ちます。Cisco ISE プロファ

イラ機能では、さまざまなプローブを使用して、ネットワーク上にあるすべてのエンドポイントの属性を収集し、それらを既知のエンドポイントが関連ポリシーおよびIDグループに従って分類されるプロファイラ アナライザに渡します。

プロファイラ フィード サービスによって、管理者は、新規および更新されたエンドポイントプロファイリングポリシーや更新されたOUIデータベースを、指定されたCiscoフィードサーバーからの、サブスクリプションを介したCisco ISEへのフィードとして取得できます。

プロファイラ条件の設定

次の表では、[プロファイラ条件（Profiler Condition）]ウィンドウのフィールドについて説明します。このウィンドウ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）]** > **[条件（Conditions）]** > **[プロファイリング（Profiling）]** です。

表 *39 :* プロファイラ条件の設定

フィールド名	使用上のガイドライン
名前（Name）	プロファイラ条件の名前。
説明（Description）	プロファイラ条件の説明。
タイプ（Type）	事前定義済みタイプのいずれかを選択します。
属性名（Attribute Name）	プロファイラ条件が基づく属性を選択します。
演算子（Operator）	演算子を選択します。
属性値（Attribute Value）	選択した属性の値を入力します。事前定義された属性値を含む属性名の場合、事前定義された値のドロップダウン リストが表示され、値を選択できます。
システム タイプ（System Type）	プロファイリング条件は、次のいずれかのタイプになります。 • [シスコ提供（Cisco Provided）]：シスコ提供として識別され、展開時にCisco ISEによって提供されるプロファイリング条件。システムから編集したり削除したりすることはできません。 • [管理者作成（Administrator Created）]：管理者作成として識別され、Cisco ISEの管理者として作成したプロファイリング条件。

関連トピック

Cisco ISE プロファイリング サービス （195 ページ）
プロファイラ条件 （226 ページ）
プロファイラ フィード サービス （277 ページ）
プロファイラ条件の作成 （246 ページ）

Cisco ISE プロファイリング サービス

Cisco Identity Services Engine（ISE）のプロファイリング サービスは、ネットワークに接続されているデバイスおよびその場所を識別します。エンドポイントは Cisco ISE に設定されたエンドポイント プロファイリング ポリシーに基づいてプロファイリングされます。次に、Cisco ISE では、ポリシー評価の結果に基づいてネットワークのリソースにアクセスする権限がエンドポイントに付与されます。

プロファイリング サービス：

- IEEE 規格 802.1X ポートベースの認証アクセス コントロール、MAC 認証バイパス（MAB）認証、およびネットワーク アドミッション コントロール（NAC）をさまざまな規模および複雑度の企業ネットワークに使用して、認証の効率的かつ効果的な展開および継続的な管理を容易にします。
- デバイス タイプにかかわらず、接続されたすべてのネットワーク エンドポイントの機能を特定、検索、および決定します。
- 一部のエンドポイントへのアクセスを誤って拒否しないようにします。

ISE Community Resource

ISE Endpoint Profiles

How To: ISE Profiling Design Guide

プロファイラ ワーク センター

[プロファイラ ワーク センター（Profiler Work Center）] メニュー（[ワーク センター（Work Centers）]>[プロファイラ（Profiler）]）には、すべてのプロファイラ ページが含まれ、ISE の管理者向けの単一の窓口として機能します。[プロファイラ ワーク センター（Profiler Work Center）] メニューには次のオプションがあります：[概要（Overview）]、[外部 ID ストア（Ext ID Stores）]、[ネットワーク デバイス（Network Devices）]、[エンドポイント分類（Endpoint Classification）]、[ノード設定（Node Config）]、[フィード（Feeds）]、[手動スキャン（Manual Scans）]、[ポリシー要素（ポリシーの要素）]、[プロファイリング ポリシー（Profiling Policies）]、[許可ポリシー（Authorization Policy）]、[トラブルシューティング（Troubleshoot）]、[レポート（Reports）]、[設定（Settings）] および [ディクショナリ（Dictionaries）]。

[プロファイラ（Profiler）] ダッシュボード

[プロファイラ（Profiler）] ダッシュボード（[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [エンドポイント分類（Endpoint Classification）]）は、ネットワーク内のプロファイル、エンドポイント、アセットの集中型モニターリング ツールです。このダッシュボードには、グラフと表の形式でデータが表示されます。[プロファイル（Profiles）] ダッシュレットには、ネットワークで現在アクティブな論理プロファイルとエンドポイント プロファイルが表示されます。[エンドポイント（Endpoints）] ダッシュレットには、ネットワークに接続するエンドポイントの ID グループ、PSN、OS タイプが表示されます。[アセット（Assets）] ダッシュレットには、ゲスト、BYOD、企業などのフローが表示されます。表には接続されたさまざまなエンドポイントが表示され、新しいエンドポイントを追加することもできます。

プロファイリング サービスを使用したエンドポイント インベントリ

プロファイリング サービスを使用して、ネットワークに接続されたすべてのエンドポイントの機能を検出、特定、および決定することができます。デバイスのタイプに関係なく、エンドポイントの企業ネットワークへの適切なアクセスを、保障し、保持できます。

プロファイリング サービスでは、エンドポイントの属性をネットワーク デバイスとネットワークから収集し、エンドポイントをそのプロファイルに従って特定のグループに分類します。一致したプロファイルを持つエンドポイントがCisco ISEデータベースに保存されます。プロファイリング サービスで処理されるすべての属性は、プロファイラ ディクショナリに定義されている必要があります。

プロファイリング サービスは、ネットワークの各エンドポイントを識別し、そのプロファイルに従ってシステム内の既存のエンドポイントの ID グループ、またはシステム内で作成できる新しいグループにそれらのエンドポイントをグループ化します。エンドポイントをグループ化して既存の ID グループにエンドポイント プロファイリング ポリシーを適用することで、エンドポイントと対応するエンドポイント プロファイリング ポリシーのマッピングを決定できます。

Cisco ISE プロファイラ キュー制限の設定

Cisco ISE プロファイラは、ネットワークから大量のエンドポイント データを短時間で収集します。それにより、一部の遅い Cisco ISE コンポーネントがプロファイラによって生成されるデータを処理するときにバックログが蓄積されるため、Java 仮想マシン（JVM）のメモリ使用率が増大し、パフォーマンスの低下および安定性の問題が生じます。

プロファイラが JVM メモリ使用率を増やさず、また、JVM がメモリ不足になり、再起動しないように、プロファイラの次の内部コンポーネントに制限が適用されます。

- エンドポイントキャッシュ：内部キャッシュのサイズは制限され、サイズが制限を超えると定期的に消去する必要があります（最長時間未使用方式に基づく）。
- フォワーダ：プロファイラによって収集されたエンドポイント情報のメイン入力キュー。

- イベントハンドラ：高速コンポーネントを接続解除する内部キューで、（通常、データベースクエリーに関連する）低速処理コンポーネントにデータを提供します。

エンドポイント キャッシュ

- maxEndPointsInLocalDb = 100000（キャッシュ内のエンドポイント オブジェクト）
- endPointsPurgeIntervalSec = 300（秒単位のエンドポイント キャッシュ消去スレッド間隔）
- numberOfProfilingThreads = 8（スレッド数）

制限は、すべてのプロファイラ内部イベント ハンドラに適用されます。キュー サイズ制限に達すると、モニターリング アラームがトリガーされます。

Cisco ISE プロファイラのキュー サイズの制限

- forwarderQueueSize = 5000（エンドポイント収集イベント）
- eventHandlerQueueSize = 10000（イベント）

イベント ハンドラ

- NetworkDeviceEventHandler：すでにキャッシュされているネットワーク アクセス デバイス（NAD）の重複 IP アドレスのフィルタリングのほか、ネットワークデバイスのイベント用。
- ARPCacheEventHandler：ARP キャッシュのイベント用。

Martian IP アドレス

Martian IP アドレスは、RADIUS パーサーがプロファイリングサービスに到達する前にそのようなアドレスを削除するため、**[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** と **[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[エンドポイントの分類（Endpoint Classification）]** ウィンドウには表示されません。Martian IP アドレスは攻撃に対して脆弱であるため、セキュリティ上の懸念事項です。ただし、Martian IP アドレスは監査目的で MnT ログに表示されます。この動作は、マルチキャスト IP アドレスの場合にも当てはまります。Martian IP アドレスの詳細については、https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/250/index.html#page/tesla_250_olh/martian_addresses.html を参照してください。

Cisco ISE ノードでのプロファイリング サービスの設定

Cisco ISE 対応のネットワークでネットワーク リソースを使用しているすべてのエンドポイントのコンテキスト インベントリを提供するプロファイリング サービスを設定できます。

デフォルトですべての管理、モニターリング、およびポリシー サービスのペルソナを担当する単一の Cisco ISE ノードで実行されるようにプロファイリング サービスを設定できます。

分散展開では、プロファイリング サービスは、ポリシー サービス ペルソナを担当する Cisco ISE ノードでのみ実行され、管理ペルソナとモニターリング ペルソナを担当する他の Cisco ISE ノードでは実行されません。

ステップ 1

ステップ 2 ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。

ステップ 3 [展開ノード（Deployment Nodes）] ページで [編集（Edit）] をクリックします。

ステップ 4 [全般設定（General Settings）] タブで [ポリシー サービス（Policy Service）] チェックボックスをオンにします。[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 次の作業を実行します。

a) [セッション サービスの有効化（Enable Session Services）] チェックボックスをオンにして、ネットワーク アクセス セッション サービス、ポスチャ セッション サービス、ゲスト セッション サービス、およびクライアント プロビジョニング セッション サービスを実行します。

b) [プロファイリング サービスの有効化（Enable Profiling Service）] チェックボックスをオンにして、プロファイリング サービスを実行します。

c) デバイス管理サービスを実行し、企業のネットワーク デバイスを制御および監査するには、[デバイス管理サービスの有効化（Enable Device Admin Service）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックしてノード設定を保存します。

プロファイリング サービスによって使用されるネットワーク プローブ

ネットワーク プローブは、ネットワーク上のエンドポイントから属性を収集するために使用される方法です。プローブを使用して、エンドポイントを Cisco ISE データベース内の一致するプロファイルで作成または更新できます。

Cisco ISE では、ネットワーク デバイスの動作を分析してデバイス タイプを決定する多数のネットワーク プローブを使用して、デバイスをプロファイリングすることができます。ネットワーク プローブは、ネットワーク可視性の向上に役立ちます。

IP アドレスと MAC アドレスのバインディング

エンドポイントを作成または更新するには、企業ネットワークの MAC アドレスのみを使用できます。ARP キャッシュにエントリが見つからない場合は、Cisco ISE で HTTP パケットの L2 MAC アドレスと NetFlow パケットの IN_SRC_MAC を使用してエンドポイントを作成または更新できます。エンドポイントが 1 ホップだけ離れている場合、プロファイリング サービスは

L2 隣接関係に依存します。エンドポイントに L2 隣接関係がある場合、エンドポイントの IP アドレスと MAC アドレスはすでにマッピングされているため、IP-MAC キャッシュ マッピングは必要ありません。

エンドポイントにL2隣接関係が存在せず、エンドポイントが複数ホップ離れている場合、マッピングは信頼できない場合があります。収集する NetFlow パケットの既知の属性には、PROTOCOL、L4_SRC_PORT、IPV4_SRC_ADDR、L4_DST_PORT、IPV4_DST_ADDR、IN_SRC_MAC、OUT_DST_MAC、IN_SRC_MAC、OUT_SRC_MAC などがあります。エンドポイントに L2 隣接関係が存在せず、L3 ホップに関して複数ホップ離れている場合は、IN_SRC_MAC 属性で L3 ネットワーク デバイスの MAC アドレスのみが伝送されます。Cisco ISE で HTTP プローブが有効になっている場合は、HTTP 要求メッセージによってペイロード データでエンドポイントの IP アドレスと MAC アドレスが伝送されないため、HTTP パケットの MAC アドレスを使用してのみエンドポイントを作成できます。

Cisco ISE では、プロファイリング サービスで ARP キャッシュが実装されるため、エンドポイントの IP アドレスと MAC アドレスを確実にマッピングできます。ARP キャッシュを機能させるには、DHCP プローブまたは RADIUS プローブを有効にする必要があります。DHCP プローブと RADIUS プローブは、ペイロード データでエンドポイントの IP アドレスと MAC アドレスを伝送します。DHCP プローブの dhcp-requested address 属性と RADIUS プローブの Framed-IP-address 属性によって、エンドポイントの IP アドレスがその MAC アドレスとともに伝送されます。これらのアドレスは、マッピングして ARP キャッシュに格納できます。

NetFlow プローブ

Cisco ISE プロファイラは Cisco IOS NetFlow Version 9 を実装しています。NetFlow Version 9 には、Cisco ISE プロファイリング サービスをサポートするためのプロファイラの拡張に必要な追加機能があるため、これを使用することを推奨します。

NetFlow Version 9 の属性を NetFlow 対応のネットワーク アクセス デバイスから収集して、エンドポイントを作成したり、Cisco ISE データベース内の既存のエンドポイントを更新できます。NetFlow Version 9 は、エンドポイントの送信元 MAC アドレスと宛先 MAC アドレスを割り当てて、更新するように設定できます。NetFlow 属性のディクショナリを作成して NetFlow ベースのプロファイリングに対応することもできます。

NetFlow Version 9 レコード フォーマットの詳細については、『NetFlow Version 9 Flow-Record Format』マニュアルの表 6「NetFlow Version 9 Field Type Definitions」を参照してください。

さらに、Cisco ISE は Version 5 以前の NetFlow バージョンをサポートします。ネットワークで NetFlow Version 5 を使用する場合は、Version 5 をアクセス レイヤのプライマリ ネットワーク アクセス デバイス（NAD）でのみ使用できます。他のデバイスでは動作しません。

Cisco IOS NetFlow Version 5 パケットには、エンドポイントの MAC アドレスが含まれません。NetFlow Version 5 から収集された属性は、Cisco ISE データベースに直接追加できません。IP アドレスを使用してエンドポイントを検出し、エンドポイントに NetFlow Version 5 の属性を付加できます。このことは、ネットワーク アクセス デバイスの IP アドレスと NetFlow Version 5 属性から抽出される IP アドレスを組み合わせることによって実行できます。ただし、これらのエンドポイントを RADIUS または SNMP プローブで事前に検出しておく必要があります。

NetFlow Version 5 以前のバージョンでは、MAC アドレスは IP フローの一部ではありません。このため、エンドポイントのキャッシュにあるネットワーク アクセス デバイスから収集された属性情報を関連付けることにより、エンドポイントの IP アドレスをプロファイリングすることが必要となります。

NetFlow Version 5 レコードフォーマットの詳細については、『NetFlow Services Solutions Guide』の表 2「Cisco IOS NetFlow Flow Record and Export Format Content Information」を参照してください。

DHCP プローブ

Cisco ISE 展開内のダイナミック ホスト コンフィギュレーション プロトコル プローブを使用すると、Cisco ISE プロファイリングサービスで INIT-REBOOT および SELECTING のメッセージタイプの新しい要求だけに基づいてエンドポイントを再プロファイリングできます。RENEWING や REBINDING などの他の DHCP メッセージ タイプは処理されますが、エンドポイントのプロファイリングには使用されません。DHCP パケットから解析された属性は、エンドポイント属性にマッピングされます。

INIT-REBOOT 状態中に生成された DHCPREQUEST メッセージ

DHCP クライアントが前に割り当てられてキャッシュされた設定を確認する場合、クライアントはサーバー識別子（server-ip）オプションを入力できません。代わりに、前に割り当てられた IP アドレスを要求された IP アドレス（requested-ip）オプションに入力する必要があります。また、DHCPREQUEST メッセージの Client IP Address（ciaddr）フィールドをゼロで埋める必要があります。要求された IP アドレスが正しくない場合、またはクライアントが誤ったネットワークに配置されている場合、DHCP サーバーは DHCPNAK メッセージをクライアントに送信します。

SELECTING 状態中に生成された DHCPREQUEST メッセージ

DHCP クライアントは、サーバー識別子（server-ip）オプションで選択された DHCP サーバーの IP アドレスを挿入し、要求された IP アドレス（requested-ip）オプションにクライアントによって選択された DHCPOFFER の Your IP Address（yiaddr）フィールドの値を入力します。また、「ciaddr」フィールドをゼロで埋めます。

表 *40:* さまざまな状態からの *DHCP* クライアント メッセージ

—	INIT-REBOOT	SELECTING	RENEWING	REBINDING
ブロードキャスト/ユニキャスト	broadcast	broadcast	ユニキャスト	broadcast
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP アドレス	IP アドレス

DHCP ブリッジ モードのワイヤレス LAN コントローラ設定

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）ブリッジ モードでワイヤレス LAN コントローラ（WLC）を設定することを推奨します。このモードでは、ワイヤレスクライアントから Cisco ISE にすべての DHCP パケットを転送できます。WLC Web インターフェイスの **[コントローラ（Controller）] > [詳細設定（Advanced）] > [DHCPマスターコントローラモード（DHCP Master Controller Mode）] > [DHCPパラメータ（DHCP Parameters）]** で使用可能な [DHCPプロキシの有効化（Enable DHCP Proxy）] チェックボックスをオフにする必要があります。DHCP IP ヘルパー コマンドが Cisco ISE ポリシー サービス ノードを指していることも確認する必要があります。

DHCP SPAN プローブ

DHCP スイッチド ポート アナライザ（SPAN）プローブは、Cisco ISE ノードで初期化されると、特定インターフェイス上のネットワーク アクセス デバイスからのネットワーク トラフィックをリッスンします。DHCP SPAN パケットを DHCP サーバーから Cisco ISE プロファイラに転送するようにネットワーク アクセス デバイスを設定する必要があります。プロファイラはこれらの DHCP SPAN パケットを受信して解析し、エンドポイントのプロファイリングに使用できるエンドポイント属性を取得します。

次に例を示します。

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

HTTP プローブ

HTTP プローブでは、識別文字列が HTTP 要求ヘッダー フィールド User-Agent を使って転送されます。このフィールドは、IP タイプのプロファイリング条件の作成、および Web ブラウザ情報の確認に使用される属性です。プロファイラは Web ブラウザ情報を User-Agent 属性および要求メッセージの他の HTTP 属性から取得し、エンドポイント属性のリストに追加します。

Cisco ISE はポート 80 およびポート 8080 で Web ブラウザからの通信をリッスンします。Cisco ISE には、多くのデフォルト プロファイルが用意されています。これらのプロファイルはシステムに組み込まれ、User-Agent 属性に基づいてエンドポイントを識別します。

HTTP はデフォルトで有効になっています。CWA、Hotspot、BYOD、MDM、およびポスチャなどの複数の ISE サービスは、クライアントの Web ブラウザの URL リダイレクトに依存しています。リダイレクトされるトラフィックには、接続されたエンドポイントの RADIUS セッション ID が含まれています。PSN でこれらの URL リダイレクトフローを終端すると、復号化された HTTPS データが可視化されます。HTTP プローブが PSN で無効になっている場合でも、ノードは Web トラフィックからブラウザのユーザーエージェント文字列を解析し、関連付けられたセッション ID に基づいてエンドポイントにデータを関連付けます。この方法でブラウザ文字列が収集されると、データのソースが HTTP プローブではなく、ゲストポータルまたは CP（クライアント プロビジョニング）としてリストされます。

HTTP SPAN プローブ

Cisco ISE 展開の HTTP プローブをスイッチド ポート アナライザ（SPAN）プローブとともに有効にすると、プロファイラは指定されたインターフェイスからの HTTP パケットをキャプチャできます。SPAN 機能は、Cisco ISE サーバーが Web ブラウザからの通信をリッスンするポート 80 で使用できます。

HTTP SPAN は、HTTP 要求ヘッダー メッセージの HTTP 属性を IP ヘッダー（L3 ヘッダー）の IP アドレスとともに収集し、L2 ヘッダーのエンドポイントの MAC アドレスに基づいてエンドポイントに関連付けることができます。この情報は、Appleデバイスやさまざまなオペレーティング システムのコンピュータなどの各種モバイルおよびポータブル IP 対応デバイスを識別するのに役立ちます。ゲスト ログインまたはクライアント プロビジョニング ダウンロード時に Cisco ISE サーバーでキャプチャをリダイレクトするため、各種モバイルおよびポータブル IP 対応デバイスの識別の信頼性が向上しました。これにより、プロファイラは User-Agent 属性とその他の HTTP 属性を要求メッセージから取得し、Apple デバイスなどのデバイスを識別できます。

VMware で実行中の Cisco ISE の HTTP 属性の収集の無効化

Cisco ISE を ESX サーバー（VMware）に展開している場合、Cisco ISE プロファイラはダイナミック ホスト コンフィギュレーション プロトコル トラフィックを収集しますが、vSphere クライアント上の設定の問題により HTTP トラフィックを収集しません。VMware セットアップで HTTP トラフィックを収集するには、Cisco ISE プロファイラのために作成する仮想スイッチの無差別モードを Accept から Reject（デフォルト）に変更して、セキュリティを設定します。DHCP および HTTP のスイッチド ポート アナライザ（SPAN）プローブが有効になっている場合は、Cisco ISE プロファイラによって DHCP トラフィックと HTTP トラフィックの両方が収集されます。

pxGrid プローブ

PxGrid プローブは、外部ソースからエンドポイントコンテキストを受信するために Cisco pxGrid を利用します。Cisco ISE 2.4 より前は、Cisco ISE はパブリッシャおよび共有されたさまざまなコンテキスト情報（セッション id、グループ情報、外部サブスクライバへの設定要素など）のみを提供していました。Cisco ISE 2.4 での pxGrid プローブの導入により、パブリッシャおよび Cisco ISE ポリシーサービスノードがサブスクライバになるという他のソリューションが提供されます。

pxGrid プローブは、エンドポイントアセットのトピック /topic/com.cisco.endpoint.asset、サービス名 com.cisco.endpoint.asset を使用する pxGrid v2 仕様に基づいています。次の表に、プレフィックス asset が先行するすべてのトピック属性を示します。

表 *41 :* エンドポイントアセットのトピック

属性名	タイプ	説明
assetId	長整数型	アセット ID
assetName	文字列	アセット名

assetIpAddress	文字列	IP アドレス
assetMacAddress	文字列	MAC アドレス
assetVendor	文字列	製造元
assetProductId	文字列	製品コード
assetSerialNumber	文字列	シリアル番号
assetDeviceType	文字列	デバイスタイプ
assetSwRevision	文字列	S/W リビジョン番号
assetHwRevision	文字列	H/W リビジョン番号
assetProtocol	文字列	プロトコル
assetConnectedLinks	配列	ネットワーク リンク オブジェクトの配列
assetCustomAttributes	配列	カスタム名と値のペアの配列

デバイスの MAC アドレス（assetMacAddress）や IP アドレス（assetIpAddress）などのネットワーク資産を追跡するために一般的に使用される属性に加えて、このトピックでは、ベンダーが固有のエンドポイント情報をカスタム属性（assetCustomAttributes）として公開することができます。Cisco ISE でエンドポイントカスタム属性を使用すると、pxGrid で共有される一意のベンダー属性セットごとにスキーマの更新を必要とせずに、さまざまな使用例に関するトピックを拡張できます。

RADIUS プローブ

Cisco ISE で認証に RADIUS を使用するように設定し、クライアント サーバー トランザクションで使用できる共有秘密を定義できます。RADIUS サーバーから RADIUS 要求および応答メッセージを受信すると、プロファイラはエンドポイントのプロファイリングに使用できる RADIUS 属性を収集できます。

Cisco ISE は RADIUS サーバーおよび他の RADIUS サーバーに対する RADIUS プロキシ クライアントとして動作できます。プロキシ クライアントとして動作する場合は、外部の RADIUS サーバーを使用して RADIUS 要求および応答メッセージを処理します。

また、RADIUS プローブは、デバイスセンサーによって RADIUS アカウンティングパケットで送信された属性も収集します。詳細については、Cisco IOS センサー組み込みスイッチからの属性の収集 （219 ページ）およびCisco IOS センサー組み込みネットワーク アクセス デバイスの設定チェックリスト （220 ページ）を参照してください。

RADIUS プローブは、プロファイルサービス用に設定されていないシステムであっても、デフォルトで実行し、ISE がコンテキスト可視性サービスで使用するエンドポイント認証および認可の詳細を追跡できるようにします。また、RADIUS プローブサービスおよびプロファイリングサービスは、消去操作のために登録されたエンドポイントの作成および更新の時間を追跡するためにも使用されます。

表 *42 : RADIUS* プローブを使用して収集した共通属性

ユーザー名	発信側ステーションID（Calling Station ID）	着信側ステーションID	フレーム IP アドレス
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
デバイスタイプ（NAD）	ロケーション（NAD）	認証ポリシー（Authentication policy）	許可ポリシー

（注） Cisco ISE がアカウンティング終了を受信すると、エンドポイントが最初に IP アドレスでプロファイルされた場合、対応するエンドポイントを再プロファイルするように Cisco ISE がトリガーされます。したがって、IP アドレスを使用してプロファイルされたエンドポイントのカスタム プロファイルがある場合、これらのプロファイルの確実度係数の合計を満たす唯一の方法は、プロファイルが対応する IP アドレスで一致することです。

ネットワーク スキャン（NMAP）プローブ

Cisco ISE では、NMAP セキュリティ スキャナを使用して、サブネット内のデバイスを検出できます。プロファイリング サービスの実行が有効になっているポリシー サービス ノードで NMAP プローブをイネーブルにします。エンドポイント プロファイリング ポリシーでそのプローブからの結果を使用します。

NMAP の各手動サブネット スキャンには、エンドポイント ソース情報をそのスキャン ID で更新するために使用される一意の数値 ID があります。エンドポイント検出時に、エンドポイント ソース情報を更新して、ネットワーク スキャン プローブで検出されたことを示すこともできます。

NMAP の手動サブネット スキャンは、静的な IP アドレスが割り当てられたプリンタなど、常に Cisco ISE ネットワークに接続されているために、他のプローブで検出できないデバイスを検出する場合に便利です。

NMAP スキャンの制限

サブネットのスキャンには非常に多くのリソースを消費します。サブネットのスキャンは時間のかかるプロセスです。これは、サブネットのサイズや密度によって異なります。アクティブなスキャンの数は常に 1 つに制限されるため、同時にスキャンできるサブネットは 1 つだけです。また、サブネット スキャンの進行中にいつでもサブネット スキャンをキャンセルできます。[クリック（Click）] を使用して、最新のスキャン結果のリンクを表示できます。これにより、**[ワーク センター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[手動スキャン（Manual Scans）]** > **[手動 NMAP スキャンの結果（Manual NMAP Scan Results）]** に保存されている最新のネットワーク スキャン結果を表示できます。

手動 NMAP スキャン

次の NMAP コマンドを使用すると、サブネットがスキャンされ、nmapSubnet.log に出力が送信されます。

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

表 *43* : 手動サブネット スキャンの *NMAP* コマンド

-O	OS 検出の有効化
-sU	UDP スキャン
-p <port ranges>	特定のポートのみスキャンします。たとえば、U:161, 162 と指定します。
oN	通常の出力
oX	XML 出力

NMAP の手動サブネット スキャンの SNMP 読み取り専用コミュニティ ストリング

NMAP の手動サブネット スキャンは、エンドポイントで UDP ポート 161 が開かれ、その結果、より多くの属性が収集されることを検出したときには、SNMP クエリーで拡張されます。NMAP 手動サブネット スキャン中は、ネットワーク スキャン プローブによって、デバイスで SNMP ポート 161 が開いているかどうかが検出されます。ポートが開いている場合は、SNMP バージョン 2c のデフォルトのコミュニティ ストリング（public）を使用して SNMP クエリがトリガーされます。

デバイスで SNMP がサポートされ、デフォルトの読み取り専用コミュニティ ストリングが public に設定されている場合は、デバイスの MAC アドレスを MIB 値「ifPhysAddress」から取得できます。

さらに、[プロファイラ設定（Profiler Configuration）] ウィンドウでは、NMAP の手動ネットワークスキャン用として、カンマで区切られた追加の SNMP 読み取り専用コミュニティ文字列を設定できます。また、SNMP バージョン 1 および 2c の SNMP MIB ウォーク用に新しい読み取り専用コミュニティ文字列を指定できます。SNMP 読み取り専用コミュニティ文字列の設定については、CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定 （212 ページ）を参照してください。

手動 NMAP スキャンの結果

最新のネットワーク スキャン結果は、[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャンの結果（Manual NMAP Scan Results）] に保存されます。[手動 NMAP スキャンの結果（Manual NMAP Scan Results）] ページには、任意のサブネットに対して手動でのネットワーク スキャンを実行し、その結果として検出された最新のエンドポイントのみが、関連付けられたエンドポイント プロファイル、MAC アドレス、およびスタティック割り当てステータスとともに表示されます。このページでは、必要に応じて、エンドポイント サブネットで検出されたポイントをより適切に分類するために編集できます。

Cisco ISE を使用すると、プロファイリング サービスの実行が有効になっている [ポリシー サービス（Policy Service）] ノードで手動でのネットワーク スキャンを実行できます。展開内のプライマリ管理 ISE ノード ユーザー インターフェイスでポリシー サービス ノードを選択し、そのポリシー サービス ノードで手動でのネットワーク スキャンを実行する必要があります。任意のサブネットに対する手動でのネットワーク スキャン時に、ネットワーク スキャン プローブにより、指定されたサブネット上のエンドポイントとそのオペレーティング システムが検出され、SNMP サービス用の UDP ポート 161 および 162 がチェックされます。

手動での NMAP スキャンの結果に関する追加情報を以下に示します。

- 不明なエンドポイントを検出するには、NMAP が NMAP スキャンまたはサポートする SNMP スキャンを介して IP/MAC バインディングを学習できる必要があります。
- ISE は、RADIUS 認証または DHCP プロファイリングを使用して、既知のエンドポイントの IP/MAC バインディングを学習します。
- IP/MAC バインディングは、展開内の PSN ノード間で複製されません。したがって、ローカル データベースに IP/MAC バインディングがある PSN（たとえば、MAC アドレスが最後に認証された PSN）から手動スキャンを開始する必要があります。
- NMAP スキャンの結果には、手動または自動にかかわらず、NMAP が以前にスキャンしたエンドポイントに関する情報は表示されません。

DNS プローブ

Cisco ISE 展開のドメイン ネーム サーバー（DNS）プローブを使用すると、プロファイラはエンドポイントを検索し、完全修飾名（FQDN）を取得できます。Cisco ISE 対応のネットワークでエンドポイントが検出されたら、エンドポイント属性のリストが NetFlow、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP プローブから収集されます。

Cisco ISE をスタンドアロンで展開する場合、または初めて分散環境に展開する場合は、セットアップ ユーティリティを実行して Cisco ISE アプライアンスを設定するように求められます。セットアップ ユーティリティを実行するときに、ドメイン ネーム システム（DNS）ドメインとプライマリ ネームサーバー（プライマリ DNS サーバー）を設定します。設定時には、1 つ以上のネームサーバーを設定できます。Cisco ISE の展開後に、CLI コマンドを使用して DNS ネームサーバーを変更または追加することもできます。

DNS FQDN ルックアップ

DNS ルックアップを実行する前に、DHCP、DHCP SPAN、HTTP、RADIUS、または SNMP のいずれかのプローブを DNS プローブとともに起動する必要があります。これにより、プロファイラの DNS プローブは、Cisco ISE 展開に定義されている、指定されたネームサーバーに対して逆引き DNS ルックアップ（FQDN ルックアップ）を実行できます。新しい属性がエンドポイントの属性リストに追加され、エンドポイント プロファイリング ポリシーの評価に使用できます。FQDN は、システム IP ディクショナリに存在する新しい属性です。エンドポイント プロファイリング条件を作成して、FQDN 属性およびそのプロファイリング用の値を検証できます。次は、DNS ルックアップ、およびこれらの属性を収集するプローブに必要な特定のエンドポイント属性です。

- dhcp-requested-address 属性：DHCP プローブと DHCP SPAN プローブによって収集される属性
- SourceIP 属性：HTTP プローブによって収集される属性
- Framed-IP-Address 属性：RADIUS プローブによって収集される属性
- cdpCacheAddress 属性：SNMP プローブによって収集される属性

WLC Web インターフェイスでの呼出端末 ID タイプの設定

WLC Web インターフェイスを使用して、呼出端末 ID タイプ情報を設定できます。WLC Web インターフェイスの [セキュリティ（Security）] タブに移動すると、[RADIUS RADIUS 認証サーバー（Authentication Servers）] ページで発信側ステーション ID を設定できます。[MAC デリミタ（MAC Delimiter）] フィールドは、WLC ユーザー インターフェイスのデフォルトでは、[コロン（Colon）] に設定されます。

WLC Web インターフェイスで設定する方法の詳細については、『Cisco Wireless LAN Controller Configuration Guide, Release 7.2』の第 6 章「Configuring Security Solutions」を参照してください。

config radius callStationIdType コマンドを使用して WLC CLI で設定する方法の詳細については、『Cisco Wireless LAN Controller Command Reference Guide, Release 7.2』の第 2 章「Controller Commands」を参照してください。

ステップ 1 ワイヤレス LAN コントローラのユーザー インターフェイスにログインします。

ステップ 2 [セキュリティ（Security）] をクリックします。

ステップ 3 [AAA] を展開して、**[RADIUS]** > **[認証（Authentication）]** を選択します。

ステップ 4 [呼出端末 ID タイプ（Call Station ID Type）] ドロップダウン リストから [システム MAC アドレス（System MAC Address）] を選択します。

ステップ 5 FIPS モードで Cisco ISE を実行する場合は、[AES キー ラップ（AES Key Wrap）] チェックボックスをオンにします。

ステップ 6 [MAC 区切り文字（MAC Delimiter）] ドロップダウン リストから [コロン（Colon）] を選択します。

SNMP クエリ プローブ

[ノードの編集（Edit Node）] ページでの SNMP クエリー プローブの設定に加えて、**[管理（Administration）]** > **[ネットワーク リソース（Network Resources）]** > **[ネットワーク デバイス（Network Devices）]** でその他の Simple Management Protocol 設定を行う必要があります。

[ネットワーク デバイス（Network Devices）] リスト ページで新しいネットワーク アクセス デバイス（NAD）の SNMP 設定を行うことができます。ネットワーク アクセス デバイスの SNMP クエリー プローブまたは SNMP 設定に指定したポーリング間隔で、NAD に定期的にクエリーを実行します。

次の設定に基づいて、特定の NAD の SNMP クエリーをオンおよびオフにすることができます。

- [リンクアップ時に SNMP クエリー（SNMP Query on Link up）] および [新しい MAC の通知（New MAC notification）] のオンまたはオフ
- Cisco Discovery Protocol 情報の [リンクアップ時に SNMP クエリー（SNMP Query on Link up）] および [新しい MAC の通知（New MAC notification）] のオンまたはオフ
- SNMP クエリー タイマーをデフォルトでスイッチごとに 1 時間に 1 回

iDevice および SNMP をサポートしないその他のモバイル デバイスでは、ARP テーブルによって MAC アドレスを検出でき、SNMP クエリー プローブによってネットワーク アクセス デバイスからクエリーを実行できます。

SNMP クエリに関する Cisco Discovery Protocol のサポート

ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスのすべてのポートで Cisco Discovery Protocol を有効（デフォルト）にする必要があります。ネットワーク デバイスのいずれかのポートで Cisco Discovery Protocol を無効にすると、接続されているすべてのエンドポイントの Cisco Discovery Protocol 情報が失われるため、正しくプロファイリングを実行できなくなる可能性があります。ネットワーク デバイスで cdp run コマンドを使用して Cisco Discovery Protocol をグローバルに有効にし、ネットワーク アクセス デバイスのインターフェイスで cdp enable コマンドを使用して Cisco Discovery Protocol を有効にします。ネットワーク デバイスとインターフェイスで Cisco Discovery Protocol を無効にするには、コマンドの先頭に no キーワードを使用します。

SNMP クエリに関する Link Layer Discovery Protocol のサポート

Cisco ISE プロファイラは LLDP の属性を収集するために SNMP クエリーを使用します。RADIUS プローブを使用して、ネットワーク デバイスに組み込まれている Cisco IOS センサーから LLDP 属性を収集することもできます。次に、ネットワーク アクセス デバイスでの LLDP グローバル コンフィギュレーション コマンドと LLDP インターフェイス コンフィギュレーション コマンドの設定に使用できるデフォルトの LLDP 構成設定を示します。

表 *44 :* デフォルトの *LLDP* 設定

属性	設定
LLDP グローバル ステート	無効
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	有効（すべての TLV の送受信が可能）
LLDP インターフェイス ステート	[有効（Enabled）]

属性	設定
LLDP 受信	[有効（Enabled）]
LLDP 転送	[有効（Enabled）]
LLDP med-tlv-select	有効（すべての LLDP-MED TLV の送信が可能）

単一文字で表示される CDP および LLDP の機能コード

エンドポイントの属性リストには、lldpCacheCapabilities 属性と lldpCapabilitiesMapSupported 属性の 1 文字の値が表示されます。値は、CDP と LLDP を実行するネットワーク アクセス デバイスに対して表示される機能コードです。

例 1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

例 2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

例 3

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

SNMP トラップ プローブ

SNMP トラップは、MAC 通知、linkup、linkdown、および informs をサポートする特定のネットワーク アクセス デバイスから情報を受信します。SNMP トラップ プローブは、ポートが起動するかダウンし、エンドポイントがネットワークから切断されるかネットワークに接続すると、特定のネットワーク アクセス デバイスから情報を受信します。

SNMP トラップを完全に機能させ、エンドポイントを作成するには、トラップを受信したときに SNMP クエリー プローブがネットワーク アクセス デバイスの特定のポートでポーリング イベントをトリガーするように SNMP クエリーを有効にする必要があります。この機能を完全に動作させるには、ネットワーク アクセス デバイスと SNMP トラップを設定する必要があります。

（注） Cisco ISE では、ワイヤレス LAN コントローラ（WLC）とアクセス ポイント（AP）から受信した SNMP トラップはサポートされません。

Active Directory プローブ

Active Directory（AD）のプローブは以下を実現します。

- Windows エンドポイントの OS 情報の明瞭度を向上させます。Microsoft AD はバージョンとサービス パックのレベルを含む、AD に参加しているコンピュータの OS の詳細情報を追跡します。AD のプローブは、AD のランタイム コネクタを使用してこの情報を直接取得し、クライアント OS 情報の信頼性の高いソースを提供します。
- 社内および社外の資産を区別するのに役立ちます。AD のプローブで使用される基本的ですが重要な属性は、エンドポイントが AD にあるかどうかです。この情報は AD に含まれるエンドポイントを管理対象デバイスまたは企業資産として分類するために使用できます。

[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [プロファイリング設定（Profiling Configuration）] で AD プローブを有効化できます。このプローブを有効にすると、Cisco ISE はホスト名を受信するとすぐに、新しいエンドポイントの AD 属性を取得します。ホスト名は通常 DHCP または DNS プローブから正常に学習されます。正常に取得すると、ISE は再スキャンがタイムアウトになるまで、同じエンドポイントに対し AD を再度問い合わせようとはしません。これにより属性の問い合わせに対する AD の負荷が制限されます。再スキャン タイマーは、**[再スキャンまでの日数（Days Before Rescan）]** フィールド（[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [プロファイリング設定（Profiling Configuration）] > [Active Directory] ）で設定できます。エンドポイントでの追加のプロファイリング アクティビティがあれば、AD はもう一度クエリーされます。

次の AD プローブの属性は ACTIVEDIRECTORY 条件を使用して、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [プロファイリング（Profiling）]** でマッチングさせることができます。AD のプローブを使用して集められた AD 属性は、[コンテキストの可視性（Context Visibility）]>[エンドポイント（Endpoints）] ウィンドウのエンドポイントの詳細にプレフィックス「AD」が付いて表示されます。

- AD-Host-Exists
- AD-Join-Point
- AD-Operating-System
- AD-OS-Version

- AD-Service-Pack

Cisco ISE ノードごとのプローブの設定

ポリシー サービス ペルソナを担当する展開の Cisco ISE ノードごとに、[プロファイリング設定（Profiling Configuration）] タブで次のプローブを 1 つ以上設定できます。

- [スタンドアロンノード（A standalone node）]：デフォルトですべての管理、モニターリング、およびポリシー サービスのペルソナを担当する単一のノードに Cisco ISE を展開した場合。
- [複数ノード（Multiple nodes）]：展開でポリシーサービスペルソナを担当するノードを複数登録した場合。

（注） デフォルトでは、すべてのプローブが有効になっているわけではありません。一部のプローブは、チェックマークで明示的に有効にされていない場合でも部分的に有効になります。プロファイリングの設定は、現在、各 PSN に固有です。展開内の各 PSN は、同一のプロファイラ構成設定を使用して設定することを推奨します。

始める前に

Cisco ISE ノードごとのプローブは、管理ノードからのみ設定できます。管理ノードは、分散展開のセカンダリ管理ノードで使用できません。

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、**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** の順に選択します。

ステップ 2 ポリシー サービス ペルソナを担当する Cisco ISE ノードを選択します。

ステップ 3 [展開ノード（Deployment Nodes）] ページで [編集（Edit）] をクリックします。

ステップ 4 [全般設定（General Settings）] タブで [ポリシー サービス（Policy Service）] チェックボックスをオンにします。[ポリシー サービス（Policy Service）] チェックボックスがオフになっている場合は、セッション サービスとプロファイリング サービスの両方のチェックボックスが無効になります。

ステップ 5 [プロファイリング サービスの有効化（Enable Profiling Service）] チェックボックスをオンにします。

ステップ 6 [プロファイリング設定（Profiling Configuration）] タブをクリックします。

ステップ 7 各プローブの値を設定します。

ステップ 8 [保存（Save）] をクリックしてプローブ設定を保存します。

CoA、SNMP RO コミュニティおよびエンドポイント属性フィルタの設定

Cisco ISE では、グローバル コンフィギュレーションで、[プロファイラ設定（Profiler Configuration）] ページで許可変更（CoA）を発行し、プロファイリング サービスを有効にしてすでに認証されているエンドポイントに対する制御を拡張することができます。

さらに、[プロファイラ設定（Profiler Configuration）] ページでは、NMAP の手動でのネットワーク スキャンのために、カンマで区切られた追加の SNMP 読み取り専用コミュニティ ストリングを設定できます。SNMP RO コミュニティ ストリングは、[現在のカスタム SNMP コミュニティ ストリング（Current custom SNMP community strings）] フィールドに表示されるのと同じ順序で使用されます。

[プロファイラ設定（Profiler Configuration）] ページでは、エンドポイント属性のフィルタリングを設定することもできます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）]** を選択します。

ステップ 2 次のいずれかの設定を選択して、CoA タイプを設定します。

- [CoA なし（No CoA）]（デフォルト）：このオプションを使用して、CoA のグローバル コンフィギュレーションを無効にできます。この設定は、エンドポイント プロファイリング ポリシーごとに設定された CoA を上書きします。目的が可視性のみの場合は、デフォルト値 の [CoA なし（No CoA）] のままにします。
- [ポート バウンス（Port Bounce）]：スイッチ ポートのセッションが 1 つだけである場合は、このオプションを使用できます。ポートに複数のセッションがある場合は、[再認証（Reauth）] オプションを使用します。プロファイルの変更に基づいてアクセスポリシーをすぐに更新することが目的の場合は、[ポートバウンス（Port Bounce）] オプションを選択します。これにより、クライアントレス エンドポイントが再認可され、必要に応じて、IP アドレスが更新されます。
- [再認証（Reauth）]：このオプションを使用して、すでに認証されているエンドポイントをプロファイリング時に再認証できます。 現在のセッションの再認可に従った VLAN またはアドレスの変更が予期されていない場合は、[再認証（Reauth）] オプションを選択します。

  （注） 1 つのポートに複数のアクティブなセッションがある場合は、CoA に [ポートバウンス（Port Bounce）] オプションを設定しても、プロファイリングサービスによって [再認証（Reauth）] オプションが指定された CoA が発行されます。この機能を使用すると、[ポート バウンス（Port Bounce）] オプションの場合のように他のセッションが切断されるのを回避できます。

ステップ 3 NMAP の手動でのネットワークスキャンのために、カンマで区切られた新しい SNMP コミュニティ文字列を [カスタム SNMP コミュニティ文字列の変更（Change Custom SNMP Community Strings）] フィールドに入力し、[カスタム SNMP コミュニティ文字列の確認（Confirm Custom SNMP Community Strings）] フィールドに文字列を再入力します。

デフォルトの SNMP コミュニティ文字列は「public」です。これを確認するには、[現在のカスタム SNMP コミュニティ文字列（Current Custom SNMP Community Strings）] セクションの [表示（Show）] をクリックします。

ステップ 4 [エンドポイント属性フィルタ（Endpoint Attribute Filter）] チェックボックスをオンにして、エンドポイント属性のフィルタリングを有効にします。

[エンドポイント属性フィルタ（EndPoint Attribute Filter）] を有効にすると、Cisco ISE プロファイラは、重要な属性のみを保持し、その他の属性をすべて廃棄します。詳細については、エンドポイント属性をフィルタリングするグローバル設定 （217 ページ）およびISE データベースの持続性とパフォーマンスの属性フィルタ （216ページ）の項を参照してください。ベストプラクティスとして、実稼働展開では [エンドポイント属性フィルタ（Endpoint Attribute Filter）] を有効にすることを推奨します。

ステップ 5 [プローブデータパブリッシャの有効化（Enable Probe Data Publisher）] チェックボックスをオンにして、Cisco ISE でエンドポイント プローブ データを、ISE でのエンドポイント オンボーディングの分類にこのデータが必要な pxGrid サブスクライバにパブリッシュします。PxGrid サブスクライバは、初期導入フェーズ中に一括ダウンロードを使用して、Cisco ISE からエンドポイントレコードをプルできます。Cisco ISE は、PAN で更新されるたびに、エンドポイントレコードを pxGrid サブスクライバに送信します。このオプションはデフォルトでは無効になっています。

このオプションを有効にする場合は、導入環境で pxGrid ペルソナが有効になっていることを確認します。

（注） このオプションは、Cisco ISE 2.4 パッチ 10 以降で使用できます。

ステップ 6 [保存（Save）] をクリックします。

認証されたエンドポイントに対する許可変更のグローバル設定

デフォルトの [CoA なし（No CoA）] オプションを使用して認可変更（CoA）を無効にするか、またはポートバウンスと再認証オプションを使用して CoA を有効にするグローバル コンフィギュレーション機能を使用できます。Cisco ISE の CoA でポート バウンスを設定している場合は、「CoA 免除」の項で説明されているように、プロファイリング サービスにより他の CoA が発行されることがあります。

選択したグローバル コンフィギュレーションでは、より具体的な設定がない場合のみ、デフォルトの CoA 動作が規定されます。エンドポイント プロファイリング ポリシーごとの認可変更の設定 （257 ページ）を参照してください。

RADIUS プローブまたはモニターリング ペルソナの REST API を使用して、エンドポイントの認証できます。RADIUS プローブを有効にして、パフォーマンスを向上させることができます。CoA を有効にした場合は、Cisco ISE アプリケーションで CoA 設定と合わせて RADIUS プローブを有効にしてパフォーマンスを向上させることを推奨します。これにより、プロファイリング サービスは収集された RADIUS 属性を使用して、エンドポイントに適切な CoA を発行できます。

Cisco ISE アプリケーションで RADIUS プローブを無効にした場合は、モニターリング ペルソナの REST API を使用して CoA を発行できます。これにより、プロファイリング サービスは

幅広いエンドポイントをサポートできます。分散展開では、モニターリング ペルソナの REST API を使用して CoA を発行するために、モニターリング ペルソナを担当する Cisco ISE ノードがネットワークに少なくとも 1 つ存在している必要があります。

プライマリおよびセカンダリ モニターリング ノードは同一のセッション ディレクトリ情報を持つため、Cisco ISE は、分散展開内の REST クエリーのデフォルトの宛先としてプライマリおよびセカンダリ モニターリング ノードを適宜指定します。

許可変更の発行の使用例

次の場合に、プロファイリング サービスによって許可変更が発行されます。

- エンドポイントが削除される：エンドポイントが [エンドポイント（Endpoints）] ページから削除され、そのエンドポイントがネットワークから接続解除または排除された場合。
- 例外アクションが設定される：エンドポイントに異常または許容できないイベントをもたらす例外アクションがプロファイルごとに設定されている場合。プロファイリング サービスは、CoA を発行して対応するスタティック プロファイルにエンドポイントを移動します。
- エンドポイントが初めてプロファイリングされる：エンドポイントがスタティックに割り当てられておらず、初めてプロファイリングされる場合（たとえば、プロファイルが不明プロファイルから既知のプロファイルに変更された場合）。
    - エンドポイント ID グループが変更される：エンドポイントが認証ポリシーで使用されるエンドポイント ID グループに対して追加または削除された場合。

      エンドポイント ID グループが変更され、エンドポイント ID グループが次のために許可ポリシーで使用されている場合、プロファイリング サービスは CoA を発行します。

        - 動的にプロファイリングされる場合のエンドポイントに対するエンドポイント ID グループの変更
        - ダイナミック エンドポイントに対してスタティック割り当てフラグが true に設定されている場合のエンドポイント ID グループの変更

- エンドポイント プロファイリングのポリシーが変更され、ポリシーが認証ポリシーで使用される：エンドポイント プロファイリング ポリシーが変更され、認証ポリシーで使用される論理的なプロファイルにそのポリシーが含まれる場合。エンドポイント プロファイリング ポリシーは、プロファイリング ポリシーの一致のため、または、エンドポイントが論理的なプロファイルに関連付けられたエンドポイント プロファイリング ポリシーにスタティックに割り当てられるときに、変更される場合があります。両方の場合で、エンドポイント プロファイリング ポリシーが許可ポリシーで使用される場合のみ、プロファイリング サービスは CoA を発行します。

許可変更の発行の免除

エンドポイントIDグループが変更され、スタティック割り当てがすでにtrueの場合、プロファイリング サービスはCoAを発行しません。

Cisco ISEは次の理由でCoAを発行しません。

- エンドポイントがネットワークから切断されている：ネットワークから切断されているエンドポイントが検出された場合。
- 有線（Extensible Authentication Protocol）EAP対応エンドポイントが認証された：認証された有線EAP対応エンドポイントが検出された場合。
- ポートごとに複数のアクティブセッション：1つのポートに複数のアクティブなセッションがある場合は、CoAに[ポート バウンス（Port Bounce）]オプションを設定しても、プロファイリング サービスによって[再認証（Reauth）]オプションが指定されたCoAが発行されます。
- ワイヤレス エンドポイント検出時のパケット オブ ディスコネクトCoA（セッションの終了）：エンドポイントがワイヤレスとして検出されて、パケットオブディスコネクトCoA（セッション終了）がポート バウンスCoAの代わりに送信された場合。この変更の利点は、ワイヤレスLANコントローラ（WLC）CoAがサポートされていることです。
- プロファイラ CoAは、許可プロファイルで設定された論理プロファイルに対して、[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）]オプションを使用すると抑制されます。デフォルトでは、プロファイラ CoAは他のすべてのエンドポイントに対してトリガーされます。
- グローバルな[CoAなし（No CoA）]設定がポリシー CoAを上書きする：グローバルな[CoAなし（No CoA）]は、エンドポイント プロファイリング ポリシーのすべての構成設定を上書きします。エンドポイント プロファイリングポリシーごとに設定されたCoAに関係なく、Cisco ISEでCoAが発行されないためです。

（注） [CoAなし（No CoA）]および[再認証（Reauth）]CoA設定は影響を受けません。また、プロファイラ サービスは有線およびワイヤレス エンドポイントに同じCoAの設定を適用します。

CoA 設定の各タイプに発行される許可変更

表 *45 : CoA* 設定の各タイプに発行される許可変更

シナリオ	CoA なし設定	ポート バウンス設定	再認証設定	その他の情報
Cisco ISE における CoA グローバル コンフィギュレーション（一般的な設定）	CoA なし（No CoA）	ポート バウンス	再認証（Reauthentication）	—
エンドポイントがネットワークで検出された場合	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	許可変更は、RADIUS 属性の Acct -Status -Type 値 Stop で判別されます。
同じスイッチ ポートで複数のアクティブ セッションと有線接続	CoA なし（No CoA）	再認証（Reauthentication）	再認証（Reauthentication）	再認証は、他のセッションの切断を回避します。
ワイヤレス エンドポイント	CoA なし（No CoA）	切断パケット CoA（セッション終了）	再認証（Reauthentication）	ワイヤレス LAN コントローラに対するサポート。
不完全な CoA データ	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	原因は RADIUS 属性の欠落。

ISE データベースの持続性とパフォーマンスの属性フィルタ

Cisco ISE は、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP ヘルパーと DHCP SPAN の両方）、HTTP、RADIUS、およびシンプル ネットワーク管理プロトコルの各プローブのフィルタを実装しています。ただし、パフォーマンスの低下に対処するために NetFlow は除外されています。各プローブ フィルタには、一時的でエンドポイント プロファイルとは関係のない属性のリストが含まれ、これらの属性はプローブによって収集された属性から削除されます。

isebootstrap ログ（isebootstrap-yyyymmdd-xxxxxx.log）には、辞書からの属性がフィルタリングされた状態で、辞書の作成を処理するメッセージが含まれます。エンドポイントがフィルタリ

ング フェーズを通過するときに、フィルタリングが行われたことを示すデバッグ メッセージをログに記録するように設定することもできます。

Cisco ISE プロファイラは、次のエンドポイント属性フィルタを呼び出します。

- DHCP ヘルパーと DHCP SPAN の両方の DHCP フィルタには、不要なすべての属性が含まれ、これらの属性は DHCP パケットの解析後に削除されます。フィルタリング後の属性は、エンドポイントのエンドポイント キャッシュ内にある既存の属性とマージされます。
- HTTP フィルタは、HTTP パケットからの属性のフィルタリングに使用され、フィルタリング後の属性セットに大幅な変更はありません。
- RADIUS フィルタは、syslog 解析が完了すると使用され、エンドポイント属性がプロファイリングのためにエンドポイント キャッシュにマージされます。
- SNMP クエリー用の SNMP フィルタには、CDP および LLDP フィルタが含まれています。これらのフィルタはすべて SNMP クエリー プローブに使用されます。

エンドポイント属性をフィルタリングするグローバル設定

収集ポイントで頻繁には変わらないエンドポイント属性の数を減らして、永続性イベントおよび複製イベントの数を減らすことができます。[エンドポイント属性フィルタ（EndPoint Attribute Filter）] を有効にすると、Cisco ISE プロファイラは、重要な属性のみを保持し、その他の属性をすべて廃棄します。重要な属性とは、Cisco ISE システムによって使用される属性またはエンドポイント プロファイリング ポリシーやルールで明確に使用される属性です。

[エンドポイント属性フィルタ（EndPoint Attribute Filter）] を有効にするには、CoA、SNMP ROコミュニティおよびエンドポイント属性フィルタの設定（212ページ）の項を参照してください。

許可されたリストは、カスタム エンドポイント プロファイリング ポリシー内でエンドポイントのプロファイリングに使用される属性のセットであり、認可変更（CoA）、個人所有デバイスの持ち込み（BYOD）、デバイス登録 WebAuth（DRW）などが Cisco ISE で期待どおりに機能するために不可欠です。許可されたリストは、無効になっている場合でも、エンドポイントの所有権が変わった場合に（属性が複数のポリシーのサービスノードによって収集されている場合）、常に基準として使用されます。

デフォルトでは許可されたリストは無効で、属性は、属性フィルタが有効になっている場合にのみドロップされます。許可されたリストは、フィードからの変更など、エンドポイントプロファイリングポリシーが変更されると、プロファイリングポリシーに新しい属性を含めるように、動的に更新されます。許可されたリストにない属性は収集時に即座にドロップされ、属性はプロファイリングエンドポイントには使用されません。バッファリングと組み合わせると、永続性イベントの数を減らすことができます。

許可されたリストに次の2つのソースから決定された属性のセットが含まれていることを確認する必要があります。

- エンドポイントをプロファイルに適合させるためにデフォルトプロファイルで使用される属性のセット。

- 許可変更（CoA）、個人所有デバイスの持ち込み（BYOD）、デバイス登録 WebAuth（DRW）などが Cisco ISE で期待どおりに機能するために不可欠な属性のセット。

（注） 許可されたリストに新しい属性を追加するには、管理者がその属性を使用する新しいプロファイラ条件とポリシーを作成する必要があります。この新しい属性は、保存された属性と複製された属性の許可されたリストに自動的に追加されます。

表 *46* : 許可属性

AAA-Server	BYODRegistration
Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	説明
DestinationIPAddress	Device Identifier
デバイス名（Device Name）	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
[FQDN]	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	製品
RegistrationTimeStamp	—
StaticAssignment	StaticGroupAssignment

TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

Cisco IOS センサー組み込みスイッチからの属性の収集

Cisco IOS センサーの統合により、スイッチから送信された任意またはすべての属性を Cisco ISE ランタイムと Cisco ISE プロファイラで収集できます。RADIUS プロトコルを使用して、DHCP、CDP、およびLLDP属性をスイッチから直接収集できます。DHCP、CDP、およびLLDPについて収集された属性は、解析され、（**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]**>**[ディクショナリ（Dictionaries）]**）にあるプロファイラディクショナリの属性にマッピングされます。

デバイス センサー用にサポートされている Catalyst プラットフォームについては、https://communities.cisco.com/docs/DOC-72932 を参照してください。

Cisco IOS センサー組み込みネットワーク アクセス デバイス

Cisco IOS センサー組み込みネットワーク アクセス デバイスと Cisco ISE の統合では、次のコンポーネントが含まれます。

- Cisco IOS センサー
- DHCP、CDPおよびLLDPのデータを収集するためにネットワーク アクセスデバイス（スイッチ）に組み込まれているデータ コレクタ
- データを処理し、エンドポイントのデバイス タイプを決定するアナライザ

  アナライザを展開するには次の 2 つの方法がありますが、2 つを組み合わせて使用することは想定されていません。

  - アナライザを Cisco ISE に展開する

- アナライザをセンサーとしてスイッチに組み込む

Cisco IOS センサー組み込みネットワーク アクセス デバイスの設定チェックリスト

ここでは、スイッチから直接 DHCP、CDP、および LLDP の属性を収集するために、Cisco IOS センサー対応スイッチと Cisco ISE で設定する必要がある作業のリストの概要について説明します。

- RADIUS プローブが Cisco ISE で有効になっていることを確認します。
- ネットワーク アクセス デバイスで DHCP、CDP、および LLDP 情報を収集するための IOS センサーがサポートされていることを確認します。
- ネットワーク アクセス デバイスで、エンドポイントから CDP 情報と LLDP 情報を取得するために次の CDP コマンドと LLDP コマンドが実行されていることを確認します。

```
cdp enable
lldp run
```

- 標準の AAA コマンドと RADIUS コマンドを使用して、セッション アカウンティングが個別に有効になっていることを確認します。

  コマンドの使用例を示します。

```
aaa new-model
aaa accounting dot1x default start-stop group radius

radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
radius-server vsa send accounting
```

- IOS センサー固有のコマンドを実行していることを確認します。
  - アカウンティング拡張の有効化

    ネットワーク アクセス デバイスで Cisco IOS センサープロトコルデータを RADIUS アカウンティングメッセージに追加したり、新しいセンサープロトコルデータの検出時に追加のアカウンティングイベントを生成したりできるようにする必要があります。つまり、RADIUS アカウンティング メッセージには、すべての CDP、LLDP、および DHCP 属性が含まれている必要があります。

    次のグローバル コマンドを入力します。

    device-sensor accounting

  - アカウンティング拡張の無効化

    （アカウンティング機能がグローバルに有効になっている場合）（アカウンティング）ネットワーク アクセス デバイスで、特定のポートでホストされているセッションについて Cisco IOS センサープロトコルデータを RADIUS アカウンティングメッセージに追加できないようにするには、適切なポートで次のコマンドを入力します。

no device-sensor accounting

- TLV 変更のトラッキング

  デフォルトでは、サポートされている各ピアプロトコルでクライアント通知とアカウンティングイベントが生成されるのは、特定のセッションのコンテキストで前に受信したことのないタイプ、長さ、値（TLV）が着信パケットに含まれている場合だけです。

  新しい TLV が存在するか、または前に受信した TLV の値が異なる場合は、すべての TLV 変更に対するクライアント通知とアカウンティング イベントを有効にする必要があります。次のコマンドを入力します。

  device-sensor notify all-changes

- ネットワーク アクセス デバイスで Cisco IOS Device Classifier（ローカルアナライザ）が無効になっていることを確認します。

  次のコマンドを入力します。

```
no macro auto monitor
```

（注） このコマンドにより、ネットワーク アクセス デバイスは変更ごとに 2 つの同じ RADIUS アカウンティング メッセージを送信できなくなります。

ISE プロファイラによる Cisco IND コントローラのサポート

Cisco ISE は、Cisco Industrial Network Director（IND）に接続されたデバイスの状態をプロファイル化して表示できます。PxGrid は、Cisco ISE と Cisco Industrial Network Director を接続してエンドポイント（IoT）データの通信を行います。Cisco ISE の pxGrid は Cisco IND イベントを消費し、Cisco IND に照会してエンドポイント タイプを更新します。

Cisco ISE プロファイラには、IoT デバイス用のディクショナリ属性があります。**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[ディクショナリ（Dictionaries）]** を選択し、システムディクショナリのリストから *IOTASSET* を選択してディクショナリ属性を確認します。

ガイドラインと推奨事項

プロファイル用に複数の ISE ノードが設定されている場合、1 つのノードのみで IND の Cisco pxGrid を有効にすることを推奨します。

複数の Cisco IND デバイスを単一の ISE に接続できます。

複数のパブリッシャ（Cisco IND）から同じエンドポイントを受信した場合、Cisco ISE は最後のパブリッシャのデータのみをそのエンドポイント用に保持します。

Cisco ISE は pxGrid のサービス名 *com.cisco.endpoint.asset* と */topic/com.cisco.endpoint.asset.* から Cisco IND データを受け取ります。

Cisco IND プロファイリング プロセス フロー

Cisco IND アセットディスカバリでは IoT デバイスを検出し、そのデバイスのエンドポイントデータを pxGrid にパブリッシュします。Cisco ISE は、pxGrid 上のイベントを認識し、エンドポイントデータを取得します。Cisco ISE のプロファイラポリシーは、ISE プロファイラ ディクショナリ内の属性にデバイスデータを割り当て、これらの属性を Cisco ISE のエンドポイントに適用します。

Cisco ISE の既存の属性を満たさない IoT エンドポイントデータは保存されません。ただし、Cisco ISE でさらに属性を作成して Cisco IND に登録することができます。

Cisco ISE は、pxGrid を介した Cisco IND への接続が最初に確立されるときにエンドポイントの一括ダウンロードを行います。ネットワークに障害があると、Cisco ISE は蓄積されたエンドポイント変更を再び一括ダウンロードします。

IND プロファイル用の Cisco ISE と Cisco IND の設定

（注） Cisco INDで pxGrid をアクティブ化する前に、Cisco IND に Cisco ISE 証明書をインストールし、ISE に Cisco IND 証明書をインストールする必要があります。

1. **[管理（Administration）]** > **[展開（Deployment）]** を選択します。pxGrid コンシューマとして使用する予定の PSN を編集し、pxGrid を有効にします。この PSN は、Cisco IND およびプロファイリングによってパブリッシュされた pxGrid データからエンドポイントを作成します。
2. **[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** を選択して pxGrid が実行していることを確認します。次に **[証明書（Certificates）]** タブをクリックし、証明書フィールドに入力します。[作成（Create）] をクリックして証明書を発行し、その証明書をダウンロードします。
   - [処理の選択（I want to）] では [単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）] を選択し、接続する Cisco IND の名前を入力します。
   - [証明書のダウンロード形式（Certificate Download Format）] では、**PKS12 形式**を選択します。
   - [証明書のパスワード（Certificate Password）] では、パスワードを作成します。

（注） ISE 内部 CA を有効にする必要があります。ご使用のブラウザでポップアップをブロックしている場合は、証明書をダウンロードできません。証明書を解凍して、この次の手順で PEM ファイルを使用できるようにします。

3. Cisco INDで、**[設定（Settings）]** > **[pxGrid]** を選択し、[.pem IND 証明書のダウンロード（Download .pem IND certificate）] をクリックします。このウィンドウを開いたままにします。
4. Cisco ISE で、**[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** > **[すべてのクライアント（All Clients）]** を選択します。Cisco IND pxGrid クライアントが表示されたら、それを承認します。
5. Cisco IND でスライダを移動して pxGrid を有効にします。別の画面が開き、そこで ISE ノードの場所、ISE で pxGrid サーバー用に入力した証明書の名前、指定したパスワードを定義します。**[証明書のアップロード（Upload Certificate）]** をクリックして、ISE pxGrid PEM ファイルを検索します。
6. ISE で、**[管理（Administration）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。[インポート（Import）] をクリックし、Cisco IND から取得した証明書へのパスを入力します。
7. Cisco INDで、[アクティブ化（Activate）] をクリックします。
8. Cisco ISE で、[管理（Adminstration）] > [展開（Deployment）] を選択します。Cisco IND 接続に使用する PSN を選択し、[プロファイリング（Profiling）] ウィンドウを選択して pxGrid プローブを有効にします。
9. ISE と Cisco IND の間の pxGrid 接続がアクティブになりました。それを確認するには、Cisco IND が検出した IoT エンドポイントを表示します。

IND プロファイリング用の属性の追加

Cisco IND は、ISE ディクショナリに含まれていない属性を返す場合があります。Cisco ISE に属性をさらに追加することによって、その IoT デバイスをより正確にプロファイルすることができます。新しい属性を追加するには、Cisco ISE でカスタム属性を作成し、pxGrid を介してその属性を Cisco IND に送信します。

1. **[管理（Administration）]** > **[ID 管理（Identity Management）]** > **[設定（Settings）]** > **[エンドポイントカスタム属性（Endpoint Custom Attributes）]** を選択します。属性のエンドポイント属性を作成します。
2. これで、プロファイラポリシーでこの属性を使用して、新しい属性でアセットを識別できるようになります。**[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** を選択し、新しいプロファイラポリシーを作成します。[ルール（Rule）] セクションで、新しいルールを作成します。**属性/値**を追加した場合は、**CUSTOMATTRIBUTE** フォルダを選択し、作成したカスタム属性を選択します。

MUD の Cisco ISE サポート

製造元使用率記述子（MUD）は IETF 標準で、オンボード IoT デバイスに対する方法を定義します。IoTデバイスのシームレスな可視化とセグメンテーションの自動化を提供します。MUD はIETFプロセスで承認されており、RFC8520 としてリリースされています。詳細については、https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/ を参照してください。

Cisco ISE リリース 2.6 以降では、IoT デバイスの識別がサポートされています。Cisco ISE は、プロファイリングポリシーとエンドポイント ID グループを自動的に作成します。MUD は、IoT デバイスのプロファイリング、プロファイリングポリシーの動的作成、ポリシーとエンドポイント ID グループの作成プロセス全体の自動化をサポートします。管理者はこれらのプロファイリングポリシーを使用して、許可ポリシーおよびプロファイルを手動で作成できます。DHCP と LLDP のパケットで MUD URL を送信する IoT デバイスは、これらのプロファイルとポリシーを使用して登録されています。

Cisco ISE は IoT デバイスを符号なしで分類します。Cisco ISE は MUD 属性を保存しません。属性は現在のセッションのみで使用されます。[コンテキストと可視性（Context and Visibility）] >[エンドポイント（Endpoints）] ウィンドウの [エンドポイントプロファイル（Endpoint Profile）] フィールドで、IoT デバイスをフィルタリングできます。

次のデバイスは、Cisco ISE への MUD データの送信をサポートしています。

- Cisco IOS XE バージョン 16.9.1 と 16.9.2 を実行している Cisco Catalyst 3850 シリーズ スイッチ
- Cisco IOS バージョン 15.2(6)E2 を実行している Cisco Catalyst デジタル ビルディング シリーズ スイッチ
- Cisco IOS バージョン 15.2(6)E2 を実行している Cisco Industrial Ethernet 4000 シリーズ スイッチ
- MUD 機能が組み込まれた Internet of Things（IoT）デバイス

Cisco ISE は、次のプロファイリングプロトコルおよびプロファイリングプローブをサポートします。

- LLDP と Radius - TLV 127
- DHCP - オプション 161

両方のフィールドが IOS デバイスセンサーで Cisco ISE に送信できます。

MUD での ISE の設定

1. **[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [プロファイラの設定（Profiler Settings）]** を選択し、[MUD のプロファイリングの有効化（Enable profiling for MUD）] チェックボックスをオンにします。

2. MUD URI を送信可能なネットワーク アクセス デバイスを ISE に追加します。ネットワークデバイスを追加するには、**[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。
3. MUD-URL 接続が機能していることを確認します。
    1. **[コンテキストの可視性（Visibility）]** > **[エンドポイント（Endpoints）]** を選択し、ISE が正常に分類されている IoT エンドポイントを見つけます。IoT デバイスはエンドポイントプロファイル名でフィルタリングできます。`IOT-MUD` から始まります。
    2. いずれかの IoT デバイスのエンドポイント MAC アドレスをクリックし、属性タグを選択します。属性のリストに mud-url があることを確認します。
    3. **[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** を選択し、[システムタイプ（System Type）] に [作成した IOT（IOT Created）] を選択してリストをフィルタ処理します。
4. 必要に応じて、新しい IoT デバイスのデバッグ ロギングを設定します。
    1. **[システム（System）]** > **[ロギング（Logging）]** > **[デバッグログの設定（Debug Log Configuration）]** を選択し、MUD が設定された ISE ノードを選択します。
    2. 左側のメニューで [デバッグログの設定（Debug Log Configuration）] を選択し、プロファイラを選択します。

分類する IoT デバイスが増えると、同じ MUD-URL を持つ同じカテゴリまたはグループ内のすべてのデバイスが同じエンドポイントグループに割り当てられます。たとえば、Molex ライトを接続し、分類すると、この Molex ライトにプロファイラグループが作成されます。同じタイプの（同じ MUD-URL を持つ）Molex ライトが増え、分類されると、同じ分類またはエンドポイント ID グループを継承します。

ISE とスイッチで MUD トラフィックフローを確認

1. IoT デバイスをオンにする前に、ポートを接続するか、インターフェイスのシャットダウンを解除します。
    1. ISE でパケットキャプチャを開始します。
    2. スイッチポートでパケットキャプチャを開始します。
2. スイッチに関する次のコマンドの出力を確認します。
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**
3. IoT デバイスをオンにします。
4. 1 分ごとに次のコマンドを繰り返し実行します。

1. **show device-sensor cache all**
2. **show access-session**
3. **show radius statistics**

5. ISE のすべてのデバイスが表示されるまで 3 ～ 5 分間待機します。
6. ISE とスイッチパケットの両方のキャプチャを停止します。
7. 1 分ごとに次のコマンドを繰り返し実行します。
   1. **show device-sensor cache all**
   2. **show access-session**
   3. **show radius statistics**

プロファイラ条件

プロファイラ条件はポリシー要素であり、他の条件とほとんど同じです。ただし、認証、許可、およびゲスト条件とは異なり、プロファイリング条件は限られた数の属性に基づいています。[プロファイラ条件（Profiler Conditions）] ページに Cisco ISE で使用できる属性とその説明が表示されます。

プロファイラ条件は次のとおりです。

- シスコ提供：Cisco ISE には展開時に事前定義されたプロファイリング条件が含まれており、[プロファイラ条件（Profiler Conditions）] ウィンドウでシスコ提供の条件として識別されます。シスコ提供のプロファイリング条件を削除することはできません。

  [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）] からアクセスできる場所にあるシステム プロファイラ ディクショナリにもシスコ提供条件があります。

  たとえば、MAC ディクショナリです。一部の製品では、OUI（固有識別子情報）がデバイスの製造組織を識別するために最初に使用できる固有属性です。これはデバイスの MAC アドレスのコンポーネントです。MAC ディクショナリには、MACAddress および OUI 属性が含まれています。

- 管理者作成：ユーザーが Cisco ISE の管理者として作成するプロファイラ条件、複製された事前定義済みのプロファイリング条件は管理者作成として識別されます。[プロファイラ条件（Profiler Conditions）] ウィンドウでプロファイラディクショナリを使用して、DHCP、MAC、SNMP、IP、RADIUS、NetFlow、CDP、LLDP、および NMAP タイプのプロファイラ条件を作成できます。

プロファイリング ポリシーの数の推奨上限は 1000 ですが、最高 2000 までプロファイリング ポリシーを拡張できます。

プロファイリング ネットワーク スキャン アクション

エンドポイント スキャン アクションは、エンドポイント プロファイリング ポリシーで参照できる設定可能なアクションであり、ネットワーク スキャン アクションに関連付けられている条件が満たされるとトリガーされます。

Cisco ISE システムにおけるリソース使用量を制限するために、エンドポイントをスキャンする場合はエンドポイント スキャンが使用されます。ネットワーク スキャン アクションでは、リソースを大量に消費するネットワーク スキャンとは異なり、1 つのエンドポイントをスキャンします。これにより、エンドポイントの全体的な分類が向上し、エンドポイントのエンドポイント プロファイルが再定義されます。エンドポイント スキャンは、1 度に 1 つずつしか処理できません。

1 つのネットワーク スキャン アクションをエンドポイント プロファイリング ポリシーに関連付けることができます。Cisco ISE には、ネットワーク スキャン アクションに 3 つの走査方式が事前定義されています。たとえば、OS-scan、SNMPPortsAndOS-scan、および CommonPortsAndOS-scan といった 3 つの走査方式のいずれか、またはすべてを含めることができます。OS-scan、SNMPPortsAndOS-scan、および CommonPortsAndOS-scans を編集または削除できません。これらは、Cisco ISE の事前定義済みネットワーク スキャン アクションです。独自の新しいネットワーク スキャン アクションを作成することもできます。

エンドポイントを適切にプロファイリングしたら、設定済みのネットワーク スキャン アクションをエンドポイントに対して使用できません。たとえば、Apple-Device をスキャンすると、スキャンされたエンドポイントを Apple デバイスに分類できます。OS-scan によってエンドポイントで実行されているオペレーティング システムが特定されたら、Apple-Device プロファイルに一致しなくなりますが、Apple デバイスの適切なプロファイルに一致します。

新しいネットワーク スキャン アクションの作成

エンドポイント プロファイリング ポリシーに関連付けられたネットワーク スキャン アクションでは、エンドポイントのオペレーティング システム、簡易ネットワーク管理プロトコル（SNMP）ポート、および一般ポートがスキャンされます。シスコでは、最も一般的な NMAP スキャンのためのネットワーク スキャン アクションを提供していますが、独自のものを作成することもできます。

新しいネットワーク スキャンを作成する場合は、NMAP プローブがスキャンする情報のタイプを定義します。

始める前に

ネットワーク スキャン（NMAP）プローブは、ネットワーク スキャン アクションをトリガーするルールを定義する前にイネーブルにする必要があります。その手順は、「Cisco ISE ノードごとのプローブの設定」で説明します。

ステップ 1 **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[プロファイリング（Profiling）]** > **[ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）]** を選択します。または、**[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[ポリシー要素（Policy Elements）]** > **[NMAPスキャンアクション（NMAP Scan Actions）]** を選択することもできます。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 作成するネットワーク スキャン アクションの名前と説明を入力します。

ステップ 4 次のエンドポイントをスキャンする場合、1 つ以上のチェックボックスをオンにします。

- [OSのスキャン（Scan OS）]：オペレーティングシステムをスキャンする場合。
- [SNMP ポートのスキャン（Scan SNMP Port）]：SNMP ポート（161、162）をスキャンする場合。
- [一般ポートのスキャン（Scan Common Port）]：一般ポートをスキャンする場合。
- [カスタムポートのスキャン（Scan Custom Ports）]：カスタムポートをスキャンする場合。
- [サービスバージョン情報を含むスキャン（Scan Include Service Version Information）]：デバイスの詳細な説明を含むことがあるバージョン情報をスキャンする場合。
- [SMB 検出スクリプトの実行（Run SMB Discovery Script）]：SMB ポート（445 および 139）をスキャンして、OS やコンピュータ名などの情報を取得する場合。
- [NMAP ホスト検出のスキップ（Skip NMAP Host Discovery）]：NMAP スキャンの最初のホスト検出ステージをスキップする場合。

  （注） [NMAP ホスト検出のスキップ（Skip NMAP Host Discovery）] オプションは自動 NMAP スキャンではデフォルトでオンになっていますが、手動 NMAP スキャンを実行する場合は選択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。

NMAP オペレーティング システム スキャン

オペレーティング システム スキャン（OS-scan）タイプでは、エンドポイントで実行されているオペレーティング システム（および OS バージョン）がスキャンされます。これはリソースを大量に消費するスキャンです。

NMAP ツールには、信頼できない結果をまねく可能性がある OS-scan 上の制限があります。たとえば、スイッチやルータなどのネットワークデバイスのオペレーティング システムをスキャンすると、NMAP OS-scan から、それらのデバイスについて正しくない operating-system 属性が返されることがあります。Cisco ISE は精度が 100% ではない場合でも、operating-system 属性を表示します。

ルールで NMAP operating-system 属性を使用するエンドポイント プロファイリング ポリシーに低い確実度値の条件（確実度係数の値）を設定する必要があります。NMAP:operating-system 属性に基づいてエンドポイント プロファイリング ポリシーを作成するときは、NMAP からの不正な結果をフィルタリングする AND 条件を含めることを推奨します。

[OSのスキャン（Scan OS）]をエンドポイントプロファイリングポリシーに関連付けた場合、次の NMAP コマンドはオペレーティング システムをスキャンします。

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

次のNMAPコマンドを使用すると、サブネットがスキャンされ、nmapSubnet.logに出力が送信されます。

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

表 *47*：手動サブネット スキャンの *NMAP* コマンド

-O	OS 検出の有効化
-sU	UDP スキャン
-p <port ranges>	特定のポートのみスキャンします。たとえば、U:161, 162 と指定します。
oN	通常の出力
oX	XML 出力

オペレーティング システム ポート

次の表に、NMAP が OS のスキャンに使用する TCP ポートを示します。また、NMAP は ICMP および UDP ポート 51824 を使用します。

1	3	4	6	7	9	13	17	19
20	21	22	23	24	25	26	30	32
33	37	42	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808

843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
[1000]	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040 ～ 1100
1102	1104	1105	1106	1107	1108	1110	1111	1112
1113	1114	1117	1119	1121	1122	1123	1124	1126
1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720
1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972	1974	1984	1998 ～ 2010	2013	2020	2021
2022	2030	2033	2034	2035	2038	2040 ～ 2043	2045 ～ 2049	2065
2068	2099	2100	2103	2105 ～ 2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381 ～ 2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875

2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000 ～ 4006	4045	4111	4125	4126	4129	4224	4242
4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000 ～ 5004	5009	5030
5033	5050	5051	5054	[5060]	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900 ～ 5907	5910	5911	5915	5922	5925	5950	5952	5959
5960 ～ 5963	5987 ～ 5989	5998 ～ 6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565 ～ 6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911

7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080 ～ 8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9,000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616
10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774
32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389

50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

NMAP SNMP ポート スキャン

SNMP ポート（161 および 162）が開いている場合、SNMPPortsAndOS-scan タイプは、エンドポイントが実行中のオペレーティング システム（およびOSバージョン）をスキャンし、SNMP クエリーをトリガーします。さらに分類するために、識別されて不明プロファイルと最初に一致したエンドポイントに使用できます。

[SNMP ポートのスキャン（Scan SNMP Port）] をエンドポイント プロファイリング ポリシーに関連付けた場合、次の NMAP コマンドは SNMP ポート（UDP 161 と 162）をスキャンします。

nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>

表 *48 :* エンドポイントの *SNMP* ポート スキャンの *NMAP* コマンド

-sU	UDP スキャン。
-p <port-ranges>	特定のポートのみスキャンします。たとえば、UDP ポート 161 と 16.2 をスキャンします
oN	通常の出力。
oX	XML 出力。
IP-address	スキャン対象のエンドポイントの IP アドレス。

NMAP 一般ポート スキャン

CommonPortsAndOS-scan タイプでは、エンドポイントで実行されているオペレーティングシステム（および OS バージョン）がスキャンされ、SNMP ポートではなく共通ポート（TCP と UDP）もスキャンされます。[一般ポートのスキャン（Scan Common Port）] をエンドポイント プロファイリング ポリシーに関連付けると、次の NMAP コマンドが一般ポートをスキャンします。nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>

表 *49 :* エンドポイントの一般ポート スキャンの *NMAP* コマンド

-sTU	TCP 接続スキャンと UDP スキャンの両方。

-p <port ranges>	TCP ポート 21、22、23、25、53、80、110、135、139、143、443、445、3306、3389、8080、および UDP ポート 53、67、68、123、135、137、138、139、161、445、500、520、631、1434、1900 をスキャンします。
oN	通常の出力。
oX	XML 出力。
IP アドレス	スキャン対象のエンドポイントの IP アドレス。

一般ポート

次の表に、NMAP がスキャンのために使用する一般的なポートを示します。

表 *50 :* 一般ポート

TCP ポート（TCP Ports）		**UDP ポート**	
ポート	**サービス**	**ポート**	**サービス**
21/tcp	FTP	53/udp	ドメイン
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	ドメイン	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	ルート
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

NMAP カスタム ポート スキャン

一般的なポートに加えて、カスタム ポートを使用して（**[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[ポリシー要素（Policy Elements）]** > **[NMAP スキャン アクション（NMAP Scan Actions）]** または **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** >

[結果（Results）] > **[プロファイリング（Profiling）]** > **[ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）]**）、自動および手動 NMAP スキャン動作を指定できます。NMAP プローブが、指定した開いているカスタム ポートを通じてエンドポイントから属性を収集します。これらの属性は、[ISE ID（ISE Identity）] ページのエンドポイントの属性で更新されます（**[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）]**）。各スキャン動作に、最大で 10 個の UDP および 10 個の TCP ポートを指定することができます。一般ポートとして指定されているものと同じポート番号を使用できません。詳細については、「McAfee ePolicy Orchestrator を使用したプロファイリング ポリシーの設定」を参照してください。

サービス バージョン情報を含む NMAP スキャン

サービス バージョン情報を含む NMAP プローブは、デバイスで実行されているサービスに関する情報を収集することによる、より優れた分類のためにエンドポイントを自動的にスキャンします。このサービス バージョン オプションは、一般ポートまたはカスタム ポートと組み合わせることができます。

例：

CLI コマンド：nmap -sV -p T:8083 172.21.75.217

出力：

[ポート（Port）]	状態	サービス	バージョン
8083/tcp	open	http	McAfee ePolicy Orchestrator Agent 4.8.0.1500 (ePOServerName: WIN2008EPO, AgentGuid: {[illegible]})

NMAP SMB 検出スキャン

NMAP SMB 検出スキャンにより、Windows バージョンを区別し、よりよいエンドポイントのプロファイリングが得られます。NMAP が提供する SMB 検出スクリプトを実行するように NMAP スキャン アクションを設定できます。

NMAP スキャン アクションは Windows のデフォルト ポリシーに組み込まれ、エンドポイントがポリシーおよびスキャン ルールに一致すると、そのエンドポイントでスキャンされ、結果は、正確な Windows バージョンの決定に役立ちます。さらに、ポリシーは、フィード サービスで設定され、新しい事前定義済 NMAP スキャンが SMB の検出オプションで作成されます。

NMAP スキャン アクションは Microsoft ワークステーション ポリシーにより呼び出され、スキャンの結果は、オペレーティング システムの属性の下のエンドポイントに保存され、Windows ポリシーに活用されます。また、サブネットの手動スキャンの SMB 検出スクリプト オプションも用意されています。

（注） SMB 検出では、エンドポイントで Windows ファイル共有オプションを有効にしてください。

SMB 検出属性

SMB 検出スクリプトがエンドポイントで実行されるときに、新しい SMB 検出属性（SMB.Operating-system など）がエンドポイントに追加されます。これらの属性は、フィードサービスの Windows エンドポイント プロファイリング ポリシーの更新に対して考慮されます。SMB 検出スクリプトが実行されるときに、SMB 検出属性には SMB.operating-system、SMB.lanmanager、SMB.server、SMB.fqdn、SMB.domain、SMB.workgroup、SMB.cpe などのように、SMB が前に追加されます。

NMAP ホスト検出のスキップ

それぞれの IP アドレスのすべてのポートをスキャンすることは時間のかかるプロセスです。スキャンの目的によって、アクティブなエンドポイントの NMAP ホストの検出を省略できます。

NMAP スキャンがエンドポイントの分類の後にトリガーされると、プロファイラはエンドポイントのホストの検出を常にスキップします。ただし、手動スキャン アクションが NMAP ホスト検出のスキップ スキャンを有効にした後でトリガーされると、ホストの検出がスキップされます。

NMAP スキャン ワークフロー

NMAP スキャンを実行するための手順：

始める前に

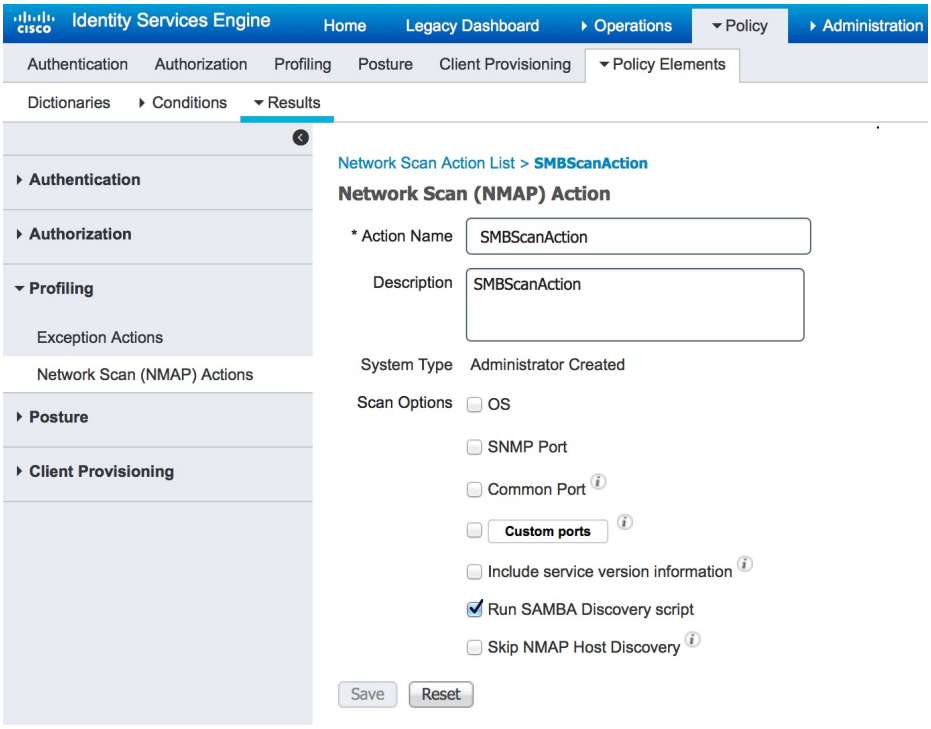
NMAP SMB 検出スクリプトを実行するには、そのシステムでファイル共有を有効にする必要があります。例については、「NMAP SMB 検出スクリプトを実行するためのファイル共有の有効化」トピックを参照してください。

ステップ 1 SMB スキャン アクションの作成。
ステップ 2 SMB スキャン アクションを使用したプロファイラ ポリシーの設定。
ステップ 3 SMB 属性を使用した新しい条件の追加。

SMB スキャン アクションの作成

ステップ 1
ステップ 2 [アクション名（Action Name）] と [説明（Description）] に入力します。
ステップ 3 [SMB 検出スクリプトの実行（Run SMB Discovery Script）] チェックボックスをオンにします。

ステップ 4 [追加（Add）] をクリックして、ネットワーク アクセス ユーザーを作成します。



次のタスク

SMB スキャン アクションを使用してプロファイラ ポリシーを設定する必要があります。

SMB スキャン アクションを使用したプロファイラ ポリシーの設定

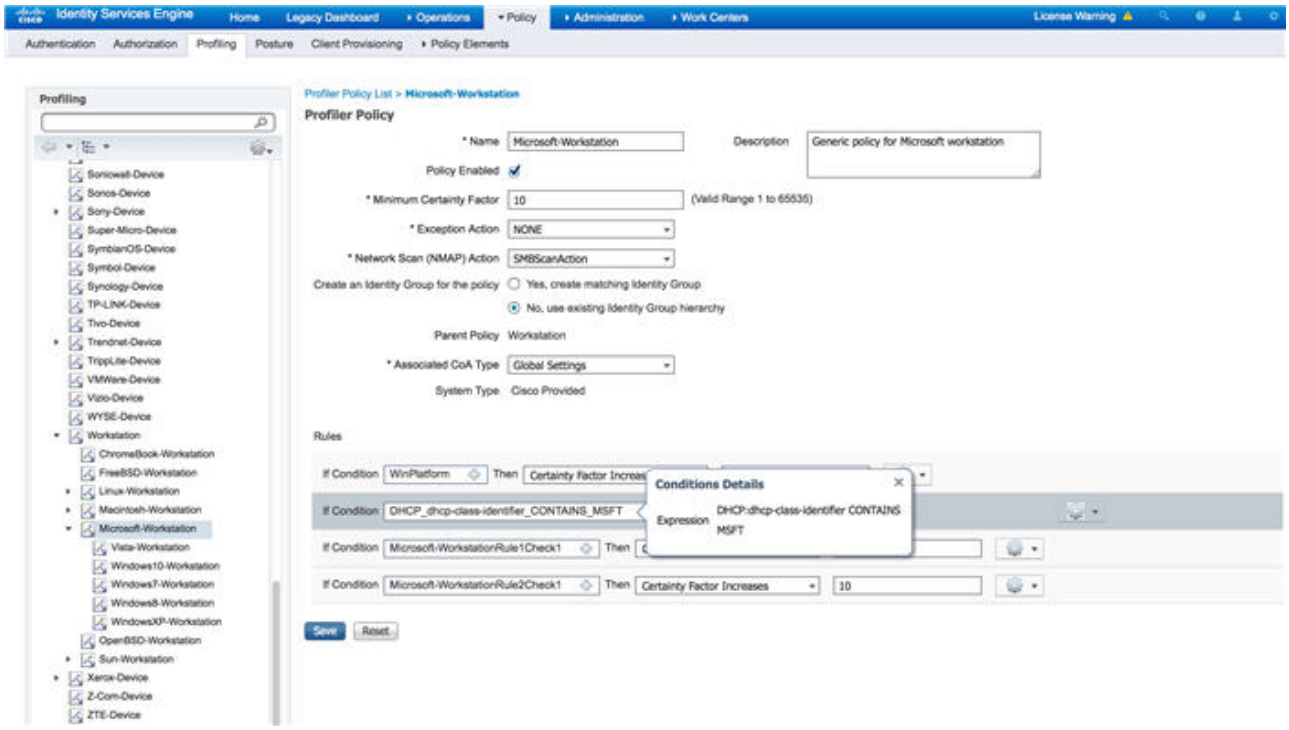
始める前に

SMB スキャン アクションを使用してエンドポイントをスキャンするための新しいプロファイラ ポリシーを作成する必要があります。たとえば、DHCP クラス ID に MSFT 属性が含まれている場合にネットワーク アクションを実行する必要があるルールを指定して、Microsoft Workstation をスキャンすることができます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [プロファイリング（Profiling）] > [追加（Add）]** の順に選択します。

ステップ 2 [名前（Name）] と [説明（Description）] に入力します。

ステップ 3 ドロップダウンで、作成したスキャン アクション（SMBScanAction など）を選択します。**ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Action）**



次のタスク

SMB 属性を使用して新しい条件を追加する必要があります。

SMB 属性を使用した新しい条件の追加

始める前に

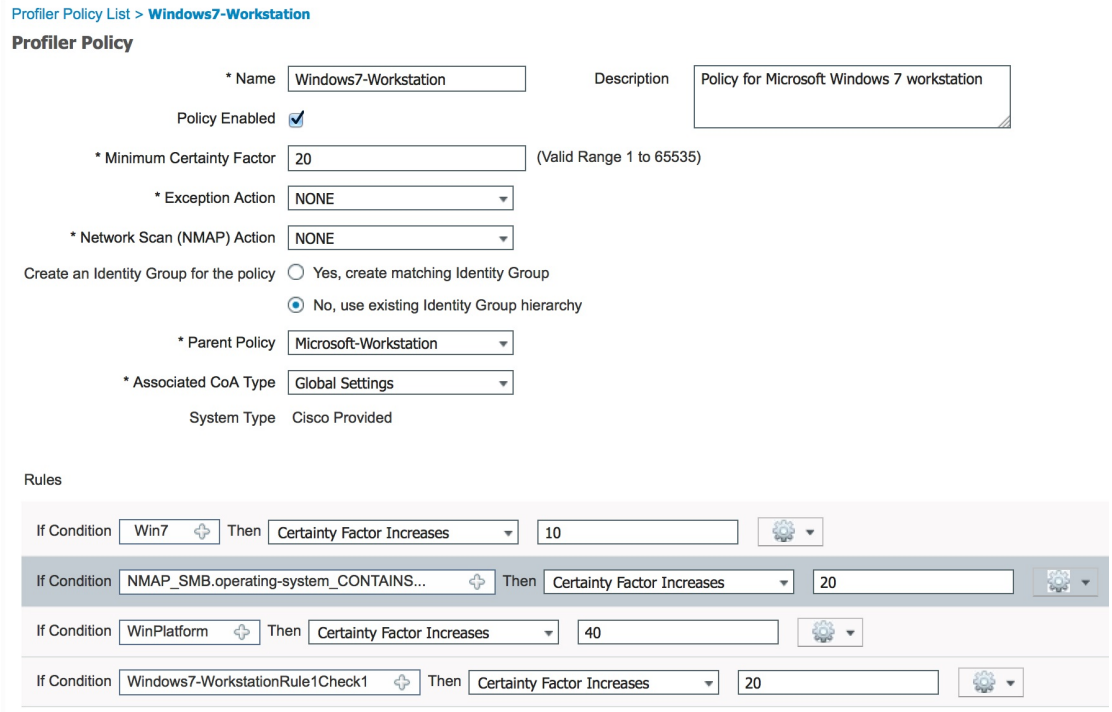
エンドポイントのバージョンをスキャンするには新しいプロファイラ ポリシーを作成する必要があります。たとえば、Microsoft ワークステーション親ポリシーの下で Windows 7 をスキャンできます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）] > [プロファイリング（Profiling）] > [追加（Add）]** の順に選択します。

ステップ 2 [名前（Name）]（たとえば Windows-7Workstation）と [説明（Description）] を入力します。

ステップ 3 [ネットワーク スキャン（NMAP）アクション（Network Scan（NMAP）Action）] ドロップダウンでは [なし（None）] を選択します。

ステップ 4 [親ポリシー（Parent Policy）] ドロップダウンでは Microsoft ワークステーション ポリシーを選択します。



NMAP SMB 検出スクリプトを実行するためのファイル共有の有効化

NMAP SMB 検出スクリプトを実行するために、Windows OS バージョン 7 のファイル共有を有効にする例を次に示します。

ステップ 1 [コントロール パネル] > [ネットワークとインターネット] の順に選択します。

ステップ 2 [ネットワークと共有センター（Network and Sharing Center）] をクリックします。

ステップ 3 [共有の詳細設定の変更（Change Advanced Sharing Settings）] をクリックします。

ステップ 4 [ファイルとプリンタを共有する（Turn on File and Printer Sharing）] をクリックします。

ステップ 5 [40 ビット暗号化または 56 ビット暗号化を使用するデバイスのファイル共有を有効にする（Enable File Sharing for Devices That Use 40- or 56-bit Encryption）] オプションと [パスワード保護共有を有効にする（Turn on Password Protected Sharing）] オプションを有効にします。

ステップ 6 [変更の保存（Save Changes）] をクリックします。

ステップ 7 ファイアウォール設定を設定します。

a) コントロール パネルで、**[システムとセキュリティ]** > **[Windows ファイアウォール]** > **[Windows ファイアウォールによるプログラムの許可]** の順に選択します。

b) [ファイルとプリンターの共有（File and Printer Sharing）] チェックボックスをオンにします。

c) [OK] をクリックします。

ステップ 8 共有フォルダを設定します。

a) 接続先フォルダを右クリックし、[プロパティ（Properties）] を選択します。

b) [共有（Sharing）] タブをクリックし、[共有（Share）] をクリックします。
c) [ファイルの共有（File Sharing）] ダイアログボックスで、必要な名前を追加して、[共有（Share）] をクリックします。
d) 選択したフォルダを共有した後で、[完了（Done）] をクリックします。
e) [詳細な共有（Advanced Sharing）] をクリックし、[このフォルダーの共有（Share This Folders）] チェックボックスをオンにします。
f) [アクセス許可（Permissions）] をクリックします。
g) [スキャンのアクセス許可（Permissions for Scans）] ダイアログボックスで、[全員（Everyone）] を選択し、[フル コントロール（Full Control）] チェックボックスをオンにします。
h) [OK] をクリックします。

NMAP スキャンからのサブネットの除外

エンドポイントの OS または SNMP ポートを特定するために NMAP スキャンを実行できます。

NMAP スキャンを実行するときに、NMAP でスキャンしないサブネット全体または IP 範囲を除外できます。[NMAPスキャンサブネット除外（NMAP Scan Subnet Exclusions）] ウィンドウ（[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）] > [NMAP スキャンサブネット除外（NMAP Scan Subnet Exclusions）]）でサブネットまたは IP 範囲を設定できます。これにより、ネットワークの負荷が制限され、相当の時間を節約できます。

手動 NMAP スキャンの場合は、[手動 NMAP スキャンの実行（Run Manual NMAP Scan）] ウィンドウ（[ワークセンター（Work Centers）]>[プロファイラ（Profiler）]>[手動スキャン（Manual Scans）] > [手動 NMAP スキャン（Manual NMAP Scan）] > [NMAP スキャンサブネット除外の設定（Configure NMAP Scan Subnet Exclusions At）]）を使用してサブネットまたは IP 範囲を指定できます。

手動 NMAP スキャンの設定

自動 NMAP スキャンに使用可能なオプションを使用して手動 NMAP スキャン（**[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [手動スキャン（Manual Scans）] > [手動 NMAP スキャン（Manual NMAP Scan）]**）を実行できます。スキャン オプションまたは事前定義されているオプションを選択できます。

表 *51* : 手動 *NMAP* スキャンの設定

フィールド名	使用上のガイドライン
ノード（**Node**）	NMAP スキャンが実行する ISE ノードを選択します。
サブネットの手動スキャン（**Manual Scan Subnet**）	NMAP スキャンを実行するエンドポイントのサブネットの IP アドレスの範囲を入力します。

フィールド名	使用上のガイドライン
NMAP スキャン サブネット除外の設定（Configure NMAP Scan Subnet Exclusions At）	**[ワークセンター（Work Centers）]>[プロファイラ（Profiler）]>[設定（Settings）]>[NMAP スキャンサブネット除外（NMAP Scan Subnet Exclusions）]** ウィンドウに誘導されます。除外するIPアドレスとサブネットマスクを指定します。一致が見つかると、NMAP スキャンは実行されません。
NMAP スキャン サブネット（NMAP Scan Subnet）	次のいずれかを実行できます。 • スキャン オプションの指定 • 既存の NMAP スキャンを選択します
スキャン オプションの指定（Specify Scan Options）	必要なスキャン オプションを選択します（OS、SNMP ポート、共通ポート、カスタム ポート、サービス バージョン情報を含む、SMB検出スクリプトの実行、NMAPホスト検出のスキップ）。詳細については、「新しいネットワーク スキャン アクションの作成」を参照してください。
既存の NMAP スキャンを選択（Select an Existijng NMAP Scan）	[既存の NMAP スキャンアクション（Existing NMAP Scan Actions）] ドロップダウンリストが表示され、デフォルトのプロファイラNMAP スキャンアクションが表示されます。
デフォルトのスキャン オプションにリセット（Reset to Default Scan Options）	このボタンをクリックしてデフォルト設定を復元します（すべてのスキャンオプションをオンにします）。
名前を付けてNMAPスキャンアクションを保存（Save as NMAP Scan Action）	アクション名と説明を入力します。

手動 NMAP スキャンの実行

ステップ 1

ステップ 2 [ノード（Node）] ドロップダウンリストで、NMAP スキャンを実行する予定の ISE ノードを選択します。

ステップ 3 [サブネットの手動スキャン（Manual Scan Subnet）] テキスト ボックスに、オープン ポートをチェックする予定のエンドポイントのサブネット アドレスを入力します。

ステップ 4 次のいずれかを選択します。

a) [スキャン オプションの指定（Specify Scan Options）] を選択し、ページの右側で、必要なスキャン オプションを選択します。詳細については、「新しいネットワーク スキャン アクションの作成」ページを参照してください。

b) [既存の NMAP スキャンアクションの選択（Select An Existing NMAP Scan Action）] を選択し、MCAFeeEPOOrchestratorClientScan などのデフォルトの NMAP アクションを選択します。

ステップ 5 [スキャンの実行（Run Scan）] をクリックします。

McAfee ePolicy Orchestrator を使用したプロファイリング ポリシーの設定

サービスのプロファイリングを行うCisco ISEは、McAfee ePolicy Orchestrator （McAfee ePO）クライアントをエンドポイントに登録するかどうかが検出されます。これにより、特定のエンドポイントが組織に属しているかどうかを確認する上で役立ちます。

このプロセスに関与するエンティティは、次のとおりです。

- ISEサーバー
- McAfee ePOサーバー
- McAfee ePO Agent

Cisco ISEは、オンボードNMAPスキャン動作（）をMCAFeeEPOOrchestratorClientscan McAfeeのエージェントが設定されているポート上でNMAP McAfeeのスクリプトを使用して、エンドポイントで実行されているかどうかを確認できます。また、カスタムポートマップを使用して新しいNMAPスキャン オプション作成できます（たとえば、8082）。McAfee ePOソフトウェアを使用して、次の手順に従って、新しいNMAPスキャン動作を設定可能:

ステップ 1 McAfee ePo NMAP スキャン アクションの設定。

ステップ 2 McAfee ePO Agent の設定。

ステップ 3 McAfee ePO NMAP スキャン アクションを使用したプロファイラ ポリシーの設定。

McAfee ePo NMAP スキャン アクションの設定

ステップ 1 **[ワークセンター（Work Centers）]** > **[プロファイラ（Profiler）]** > **[ポリシー要素（Policy Elements）]** > **[ネットワークスキャン（NMAP）アクション（Network Scan（NMAP）Actions）]** 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 [アクション名（Action Name）] と [説明（Description）] に入力します。

ステップ 4 **[スキャンオプション（Scan Options）]** では、**[カスタムポート（Custom Ports）]** を選択します。

ステップ 5 [カスタム ポート（Custom Ports）] ダイアログボックスで、必要な TCP ポートを追加します。TCP ポート 8080 は、McAfee ePO に対してデフォルトで有効になっています。

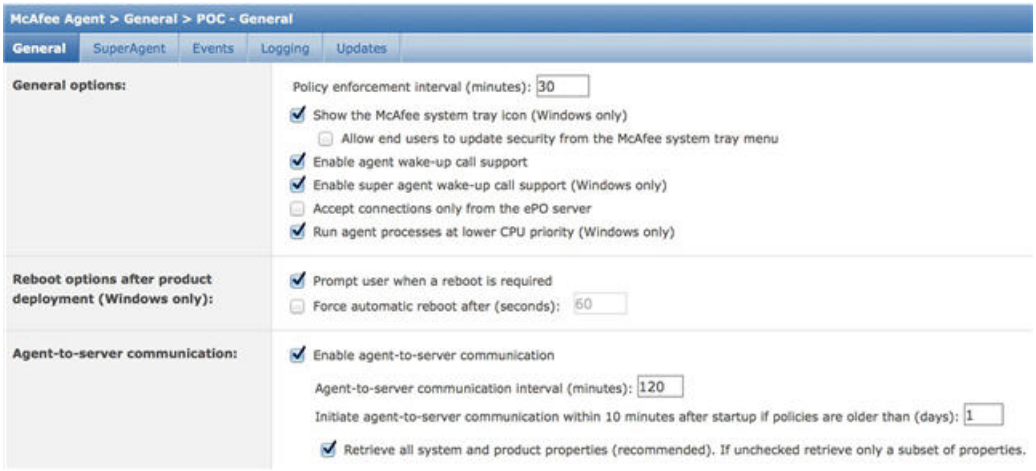
ステップ 6 [サービス バージョン情報を含む（Include Service Version Information）] チェック ボックスをオンにします。

ステップ 7 **[送信（Submit）]** をクリックします。

McAfee ePO Agent の設定

ステップ 1 McAfee ePO サーバーで、McAfee ePO Agent と ISE サーバー間の通信を容易にするために推奨される設定を確認します。

図 *18 : McAfee ePO Agent* の推奨されるオプション



ステップ 2 [ePO サーバーからのみ接続を受け入れる（Accept Connections Only From The ePO Server）] のマークが外されていることを確認します。

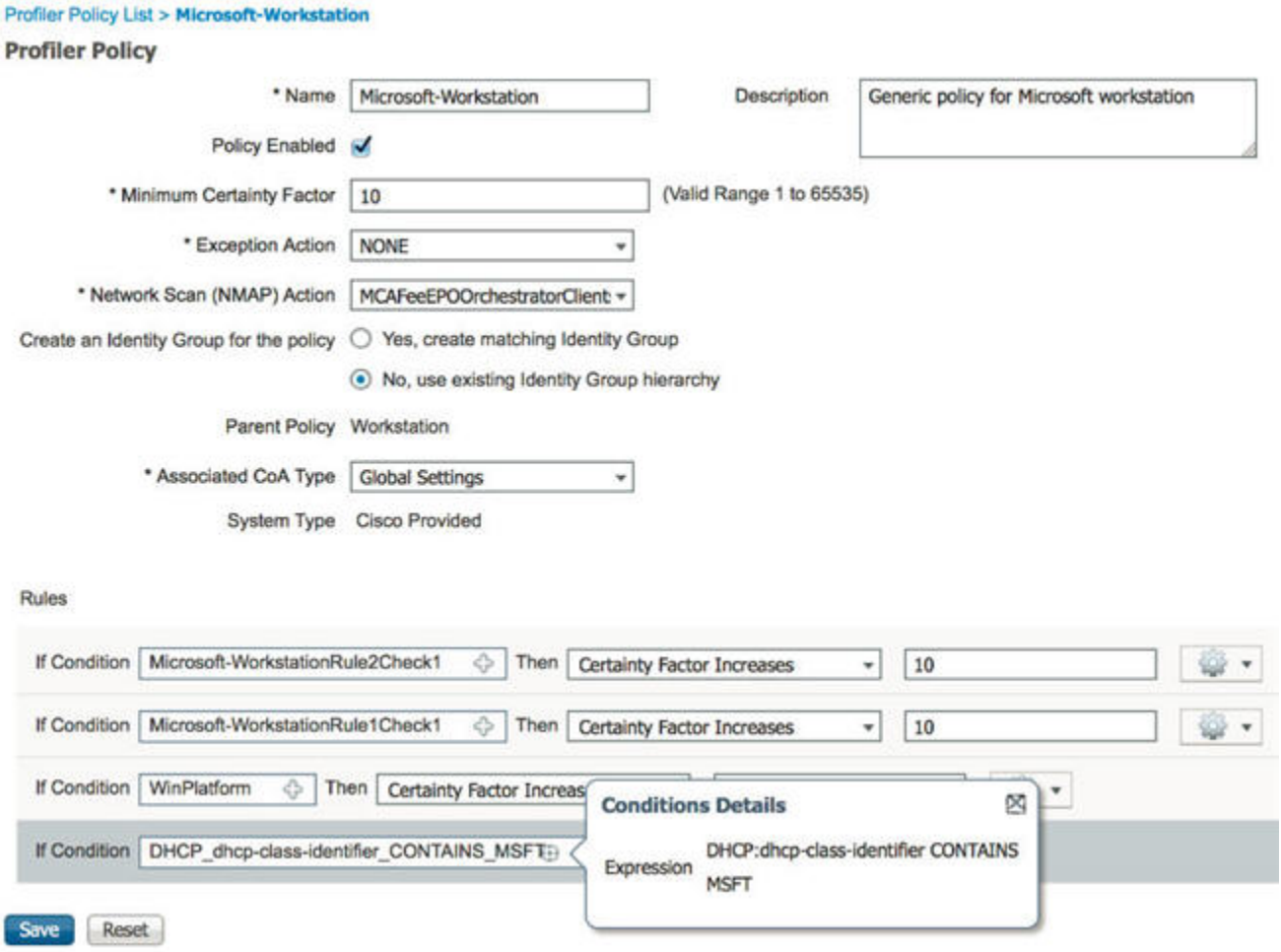
McAfee ePO NMAP スキャン アクションを使用したプロファイラ ポリシーの設定

ステップ 1 **[ポリシー（Policy）] > [プロファイリング（Profiling）] > [追加（Add）]** の順に選択します。

ステップ 2 [名前（Name）] と [説明（Description）] に入力します。

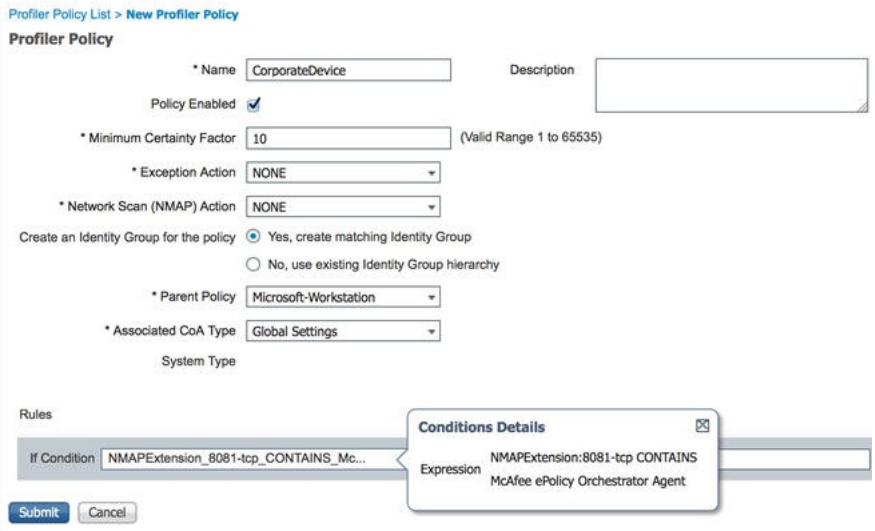
ステップ 3 **[ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Action）]** ドロップダウンで、必要なアクション（MCAFeeEPOOrchestratorClientscan など）を選択します。

ステップ 4 親プロファイラ ポリシー（DHCP クラス ID に MSFT 属性が含まれているかどうかを確認するルールを含む Microsoft-Workstation など）を作成します。



ステップ 5 McAfee ePO Agent がエンドポイントにインストールされているかどうかを確認するために、親 NMAP McAfee ePO ポリシー（Microsoft-Workstation など）内に新しいポリシー（CorporateDevice など）を作成します。

条件を満たすエンドポイントが会社のデバイスとしてプロファイルされます。このポリシーを使用して、McAfee ePO Agent によってプロファイルされたエンドポイントを新しい VLAN に移動することができます。



プロファイラ エンドポイント カスタム属性

エンドポイントがプローブから収集する属性に加えて、他の属性をエンドポイントに割り当てるには、**[管理（Administration）]** > **[ID 管理（Identity Management）]** > **[設定（Settings）]** > **[エンドポイントカスタム属性（Endpoint Custom Attributes）]** を選択します。エンドポイントのカスタム属性は、認可ポリシーでエンドポイントのプロファイルを作成するために使用できます。

最大100個のエンドポイントのカスタム属性を作成できます。サポートされるエンドポイントのカスタム属性の型は次のとおりです：Int、String、Long、Boolean および Float。

[コンテキストディレクトリ（Context Directory）] > **[エンドポイント（Endpoints）]** > **[エンドポイント分類（Endpoint Classification）]** ウィンドウで、エンドポイントのカスタム属性の値を追加できます。

エンドポイントのカスタム属性に対する使用例には、特定の属性に基づくデバイスの許可またはブロック、あるいは認証に基づく特定の権限の割り当てが含まれています。

認証ポリシーでのエンドポイント カスタム属性の使用

[エンドポイントカスタム属性（Endpoint Custom Attributes）]セクションを使用すると、追加の属性を設定できます。各定義は属性とタイプ（String、Int、Boolean、Float、Long）で構成されます。エンドポイントカスタム属性を使用して、デバイスのプロファイリングを行うことができます。

（注） エンドポイントにカスタム属性を追加するには、Plus 以上 のライセンスが必要です。

エンドポイント カスタム属性を使用して許可ポリシーを作成する手順を以下に示します。

ステップ 1 エンドポイント カスタム属性を作成し、値を割り当てます。

a) **[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント カスタム属性（Endpoint Custom Attributes）]** の順に選択します。

b) [エンドポイント カスタム属性（Endpoint Custom Attributes）] 領域で、[属性名（Attribute Name）]（たとえば、deviceType）と [データ型（Data Type）]（たとえば、String）とパラメータを入力します。

c) [保存（Save）] をクリックします。

d) **[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [概要（Summary）]** の順に選択します。

e) カスタム属性値を割り当てます。

- 必要な MAC アドレスのチェックボックスをオンにし、[編集（Edit）] をクリックします。
- または、必要な MAC アドレスをクリックして、[エンドポイント（Endpoints）] ページで、[編集（Edit）] をクリックします。

f) [エンドポイントの編集（Edit Endpoint）] ダイアログボックスの [カスタム属性（Custom Attribute）] 領域に、必須の属性値（たとえば、deviceType = Apple-iPhone）を入力します。

g) [保存（Save）] をクリックします。

ステップ 2 カスタム属性と値を使用して許可ポリシーを作成します。

a) **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]** を選択します。

b) エンドポイントの辞書からカスタム属性を選択することで、許可ポリシーを作成します（たとえば、Rule Name: Corporate Devices, Conditions:EndPoints:deviceType Contains Apple-iPhone, Permissions: then PermitAccess）。

c) [保存（Save）] をクリックします。

関連トピック

プロファイラ エンドポイント カスタム属性 （245 ページ）

プロファイラ条件の作成

Cisco ISE のエンドポイント プロファイリング ポリシーを使用すると、ネットワーク上で検出されたエンドポイントを分類し、特定のエンドポイント ID グループに割り当てることができます。これらのエンドポイント プロファイリング ポリシーは、エンドポイントを分類し、グループ化するために Cisco ISE が評価するプロファイリング条件から構成されます。

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）] > [プロファイリング（Profiling）] > [追加（Add）]** を選択します。

ステップ 2 エンドポイント プロファイリング ポリシーの設定（248 ページ）の説明に従って、フィールドに値を入力します。

ステップ 3 [送信（Submit）] をクリックして、プロファイラ条件を保存します。

ステップ 4 さらに多くの条件を作成するには、この手順を繰り返します。

エンドポイント プロファイリング ポリシー ルール

ルールを定義すると、すでにポリシー要素ライブラリに作成および保存されているライブラリから 1 つ以上のプロファイリング条件を選択し、確実度係数の整数値を各条件に関連付けるか、例外アクションまたはネットワーク スキャン アクションをその条件に関連付けることができます。例外アクションまたはネットワーク スキャン アクションは、Cisco ISE がエンドポイントの分類全体に関するプロファイリング ポリシーを評価しているときに、設定可能なアクションをトリガーするために使用します。

特定のポリシー内のルールが OR 演算子で個別に評価されると、各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。エンドポイント プロファイリング ポリシーのルールが一致した場合、そのプロファイリング ポリシーおよび一致するポリシーは、それらがネットワーク上で動的に検出された場合のエンドポイントと同じです。

ルール内で論理的にグループ化される条件

エンドポイント プロファイリング ポリシー（プロファイル）には、単一の条件または AND 演算子や OR 演算子を使用して論理的に結合された複数の単一条件の組み合わせが含まれ、これらの条件と照合して、ポリシー内の特定のルールについてエンドポイントをチェック、分類、およびグループ化することができます。

条件は、収集されたエンドポイント属性値をエンドポイントの条件に指定されている値と照合するために使用されます。複数の属性をマッピングする場合は、条件を論理的にグループ化して、ネットワーク上のエンドポイントの分類に使用できます。ルールで対応する確実度メトリック（定義済みの整数値）が関連付けられている 1 つ以上の条件とエンドポイントを照合するか、または、条件に関連付けられた例外アクション、または条件に関連付けられたネットワーク スキャン アクションをトリガーすることができます。

確実度係数

プロファイリング ポリシーの最小確実度メトリックは、エンドポイントの一致するプロファイルを評価します。エンドポイント プロファイリング ポリシーの各ルールには、プロファイリング条件に関連付けられた最小確実度メトリック（整数値）があります。確実度メトリックは、エンドポイント プロファイリング ポリシー内のすべての有効ルールに対して追加される尺度で、エンドポイント プロファイリング ポリシー内の各条件がエンドポイントの全体的な分類の改善にどの程度役立つかを測定します。

各ルールの確実度メトリックは、エンドポイント プロファイルからエンドポイント カテゴリを決定するための全体的な照合の計算に使用されます。すべての有効なルールの確実度メト

リックが合計され、照合の確実度が求められます。この値は、エンドポイントプロファイリング ポリシーに定義されている最小の確実度係数を超えている必要があります。デフォルトでは、すべての新しいプロファイリング ポリシー ルールおよび事前に定義されたプロファイリング ポリシーで、最小の確実度係数は 10 です。

エンドポイント プロファイリング ポリシーの設定

表 *52 :* エンドポイント プロファイリング ポリシーの設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するエンドポイントプロファイリング ポリシーの名前を入力します。
説明（**Description**）	作成するエンドポイントプロファイリング ポリシーの説明を入力します。
ポリシー有効（**Policy Enabled**）	デフォルトでは [ポリシー有効（Policy Enabled）] チェックボックスはオンになっており、エンドポイントのプロファイリング時に、一致するプロファイリング ポリシーが関連付けられます。 オフになっている場合、エンドポイントのプロファイリング時に、エンドポイントプロファイリング ポリシーは除外されます。
最小確実度計数（**Minimum Certainty Factor**）	プロファイリング ポリシーに関連付ける最小値を入力します。デフォルト値は 10 です。
例外アクション（**Exception Action**）	プロファイリング ポリシー内のルールを定義するときに条件に関連付ける例外アクションを選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [例外アクション（Exception Actions）] で定義されます。

フィールド名	使用上のガイドライン
ネットワーク スキャン（NMAP）アクション（**Network Scan (NMAP) Action**）	必要に応じて、プロファイリング ポリシー内のルールを定義するときに条件に関連付けるネットワーク スキャン アクションをリストから選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）]>[ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Actions）] で定義されます。
ポリシーの ID グループの作成（**Create an Identity Group for the policy**）	エンドポイント ID グループを作成するには、次のオプションのいずれかをオンにします。 • はい、一致する ID グループを作成します（**Yes, create matching Identity Group**） • いいえ、既存の ID グループ階層を使用します（**No, use existing Identity Group hierarchy**）
はい、一致する ID グループを作成します（**Yes, create matching Identity Group**）	既存のプロファイリング ポリシーを使用する場合、このオプションを選択します。 このオプションは、これらのエンドポイントの一致する ID グループを作成します。エンドポイント プロファイルが既存のプロファイリング ポリシーと一致した場合に、ID グループは Profiled エンドポイント ID グループの子になります。 たとえば、ネットワーク上で検出されたエンドポイントが Xerox-Device プロファイルに一致する場合は、[エンドポイント ID グループ（Endpoint Identity Groups）] ページで Xerox-Device エンドポイント ID グループが作成されます。

フィールド名	使用上のガイドライン
いいえ、既存の ID グループ階層を使用します（**No, use existing Identity Group hierarchy**）	プロファイリング ポリシーおよび ID グループの階層構造を使用して、一致する親エンドポイント ID グループにエンドポイントを割り当てるには、このチェックボックスをオンにします。 このオプションを使用すると、エンドポイントプロファイリングポリシー階層を利用することができ、エンドポイントはいずれかの一致する親エンドポイント ID グループ、さらに、親 ID グループに関連付けられたエンドポイント ID グループに割り当てられます。 たとえば、既存のプロファイルに一致するエンドポイントは、適切な親エンドポイント ID グループの下にグループ化されます。ここで、不明プロファイルに一致するエンドポイントは、[不明（Unknown）] の下にグループ化され、既存のプロファイルに一致するエンドポイントは、プロファイリングされたエンドポイント ID グループの下にグループ化されます。次の例を参考にしてください。 • エンドポイントが Cisco-IP-Phone プロファイルに一致する場合、これらのエンドポイントは Cisco-IP-Phone エンドポイント ID グループの下でグループ化されます。 • エンドポイントが Workstation プロファイルに一致する場合、これらのエンドポイントは、Workstation エンドポイント ID グループの下でグループ化されます。 Cisco-IP-Phone および Workstation エンドポイント ID グループは、システム内の Profiled エンドポイント ID グループに関連付けられます。
親ポリシー（**Parent Policy**）	新しいエンドポイントプロファイリングポリシーを関連付ける、システムで定義されている親プロファイリングポリシーを選択します。 子にルールと条件を継承できる親プロファイリング ポリシーを選択できます。

フィールド名	使用上のガイドライン
関連 CoA タイプ（**Associated CoA Type**）	エンドポイントプロファイリングポリシーと関連付ける次のいずれかの CoA タイプを選択します。 • CoA なし（No CoA） • ポート バウンス • 再認証（Reauth） • [グローバル設定（Global Settings）] : [管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）] で設定されたプロファイラ設定から適用されます。
ルール（**Rule**）	エンドポイントプロファイリングポリシーで定義された 1 つ以上のルールにより、エンドポイントの一致するプロファイリングポリシーが決定されます。これにより、プロファイルに応じたエンドポイントのグループ化が可能になります。 ポリシー要素ライブラリからの 1 つ以上のプロファイリング条件がルールに使用され、エンドポイント属性およびその値が、全体的な分類用に検証されます。

フィールド名	使用上のガイドライン
条件（**Conditions**）	

フィールド名	使用上のガイドライン
	プラス（+）記号をクリックして、条件の固定オーバーレイを展開します。マイナス（-）記号をクリックするか、固定オーバーレイの外側をクリックして条件を閉じます。 [既存の条件をライブラリから選択（Select Existing Condition from Library）] または [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] をクリックします。 [既存の条件をライブラリから選択（Select Existing Condition from Library）]：ポリシー要素ライブラリからシスコによって事前定義された条件を選択して、式を定義できます。 [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）]：さまざまなシステム辞書またはユーザー定義辞書から属性を選択して、式を定義できます。 プロファイリング条件と次のいずれかとを関連付けることができます。 • 各条件の確実度係数の整数値 • その条件の例外アクションまたはネットワーク スキャン アクション プロファイリング条件と関連付ける、次のいずれかの定義済み設定を選択します。 • [確実度計数が増加する（Certainty Factor Increases）]：各ルールの確実度値を入力します。この値は、全体的な分類に関するすべての一致ルールに対して追加されます。 • [例外の操作を行う（Take Exception Action）]：このエンドポイント プロファイリング ポリシーの [例外アクション（Exception Action）] フィールドで設定された例外アクションがトリガーされます。 • [ネットワークスキャンを行う（Take Network Scan Action）]：このエンドポイント プロファイリング ポリシーの [ネットワークスキャン（NMAP）アクション

フィールド名	使用上のガイドライン
	（Network Scan (NMAP) Action）] フィールドで設定されたネットワーク スキャン アクションがトリガーされます。
既存の条件をライブラリから選択（Select Existing Condition from Library）	次を実行できます。 • ポリシー要素ライブラリに存在するシスコによって事前定義された条件を選択できます。AND または OR 演算子を使用して複数の条件を追加できます。 • [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。 • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます • [複製（Duplicate）]：選択した条件のコピーを作成します • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます • [削除（delete）]：選択した条件を削除します。

フィールド名	使用上のガイドライン
新しい条件の作成（高度なオプション）（**Create New Condition (Advance Option)**）	次を実行できます。 • 式にアドホック属性/値の組み合わせを追加し、AND または OR 演算子を使用すると、複数の条件を追加できます。 • [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。 • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます • [複製（Duplicate）]：選択した条件のコピーを作成します • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます • [削除（delete）]：選択した条件を削除します。 AND または OR 演算子を使用できます

関連トピック

Cisco ISE プロファイリング サービス （195 ページ）
エンドポイント プロファイリング ポリシーの作成 （255 ページ）
UDID 属性を使用するエンドポイント コンテキストの可視性 （298 ページ）

エンドポイント プロファイリング ポリシーの作成

新しいプロファイリングポリシーを作成して、エンドポイントをプロファイリングするには、[新しいプロファイラ ポリシー（New Profiler Policy）]ページで次のオプションを使用します。

- ポリシー有効（Policy Enabled）
- [ID グループの作成（Create an Identity Group）]：一致するエンドポイント ID グループを作成するか、またはエンドポイント ID グループ階層を使用するポリシーの場合
- 親ポリシー（Parent Policy）

- 関連 CoA タイプ（Associated CoA Type）

（注） [プロファイリングポリシー（Profiling Policies）] ウィンドウでエンドポイントポリシーを作成する場合は、Webブラウザの停止ボタンを使用しないでください。このアクションによって、[新しいプロファイラポリシー（New Profiler Policy）] ウィンドウでのロードが停止され、アクセス時にリストページ内のその他のリストページおよびメニューがロードされ、リストページ内のフィルタメニュー以外のすべてのメニューでの操作を実行できなくなります。リスト ページ内ですべてのメニューの操作を実行するには、Cisco ISE からログアウトし、再度ログインする必要がある場合があります。

類似した特性のプロファイリング ポリシーを作成するには、すべての条件を再定義して新しいプロファイリング ポリシーを作成するのではなく、エンドポイント プロファイリング ポリシーを複製して変更することができます。

ステップ 1 **[ポリシー（Policy）]>[プロファイリング（Profiling）]>[プロファイリングポリシー（Profiling Policies）]** 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 作成する新しいエンドポイント ポリシーの名前と説明を入力します。[ポリシー有効（Policy Enabled）] チェックボックスはデフォルトでオンになっており、エンドポイントのプロファイリング時に検証するエンドポイント プロファイリング ポリシーが含まれます。

ステップ 4 有効範囲 1 ～ 65535 の最小の確実度係数の値を入力します。

ステップ 5 [例外アクション（Exception Action）] ドロップダウン リストの隣にある矢印をクリックして、例外アクションを関連付けるか、[ネットワーク スキャン（NMAP）アクション（Network Scan (NMAP) Actions）] ドロップダウン リストの隣にある矢印をクリックして、ネットワーク スキャン アクションを関連付けます。

ステップ 6 [ポリシーの ID グループの作成（Create an Identity Group for the policy）] で次のオプションのいずれか 1 つを選択します。

- **はい、一致する ID グループを作成します（Yes, create matching Identity Group）**
- **いいえ、既存の ID グループ階層を使用します（No, use existing Identity Group hierarchy）**

ステップ 7 [親ポリシー（Parent Policy）] ドロップダウン リストの隣の矢印をクリックして、新しいエンドポイント ポリシーに親ポリシーを関連付けます。

ステップ 8 [関連付ける CoA タイプ（Associated CoA Type）] ドロップダウン リストで、関連付ける CoA タイプを選択します。

ステップ 9 ルールをクリックし、条件を追加して、各条件の確実度係数の整数値を関連付けるか、エンドポイントの全体的な分類のその条件の例外アクションまたはネットワーク スキャン アクションを関連付けます。

ステップ 10 [送信（Submit）] をクリックしてエンドポイント ポリシーを追加するか、または [新しいプロファイラ ポリシー（New Profiler Policy）] ページの [プロファイラ ポリシー リスト（Profiler Policy List）] リンクをクリックして [プロファイリング ポリシー（Profiling Policies）] ページに戻ります。

エンドポイント プロファイリング ポリシーごとの認可変更の設定

Cisco ISE の許可変更（CoA）タイプのグローバル コンフィギュレーションに加えて、各エンドポイント プロファイリング ポリシーに関連付けられた特定のタイプの CoA も発行するように設定できます。

グローバル CoA なしタイプの設定は、エンドポイント プロファイリング ポリシーで設定された各 CoA タイプを上書きします。グローバル CoA タイプが CoA なしタイプ以外に設定されている場合、各エンドポイント プロファイリング ポリシーはグローバル CoA の設定を上書きできます。

CoA がトリガーされると、各エンドポイント プロファイリング ポリシーは、次のように実際の CoA タイプを決定できます。

- [全般設定（General Settings）]：これは、グローバル コンフィギュレーションごとに CoA を発行するすべてのエンドポイントプロファイリングポリシーのデフォルトの設定です。
- [CoA なし（No CoA）]：この設定はグローバル コンフィギュレーションを上書きし、そのプロファイルの CoA を無効にします。
- [ポート バウンス（Port Bounce）]：この設定は、グローバル ポート バウンスおよび再認証設定タイプを上書きし、ポート バウンス CoA を発行します。
- [再認証（Reauth）]：この設定は、グローバル ポート バウンスおよび再認証設定タイプを上書きし、再認証 CoA を排出します。

（注） プロファイラ グローバル CoA 設定がポート バウンス（または再認証）に設定されている場合は、モバイル デバイスの BYOD フローが切断されないように、対応するエンドポイント プロファイリング ポリシーを [CoA なし（No CoA）]、[ポリシーごとの CoA（per-policy CoA）] オプションを指定して設定していることを確認します。

グローバルおよびエンドポイント プロファイリング ポリシー設定に基づいて各場合に発行されたすべての CoA タイプと実際の CoA タイプが組み合わされた設定については、次の概要を参照してください。

表 *53 :* 設定のさまざまな組み合わせに発行された *CoA* タイプ

グローバル **CoA** タイプ	ポリシーごとに設定されたデフォルトの **CoA** タイプ	ポリシーごとの **CoA** なしタイプ	ポリシーごとのポート バウンス タイプ	ポリシーごとの再認証タイプ
CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）	CoA なし（No CoA）
ポート バウンス	ポート バウンス	CoA なし（No CoA）	ポート バウンス	再認証（Re-Auth）
再認証（Reauth）	再認証（Reauth）	CoA なし（No CoA）	ポート バウンス	再認証（Re-Auth）

エンドポイント プロファイリング ポリシーのインポート

エクスポート機能で作成できる同じ形式を使用して、XML ファイルからエンドポイント プロファイリング ポリシーをインポートできます。親ポリシーが関連付けられている、新しく作成されたプロファイリング ポリシーをインポートする場合は、子ポリシーを定義する前に親ポリシーを定義しておく必要があります。

インポート ファイルでは、エンドポイント プロファイリング ポリシーが階層構造になっており、最初に親ポリシー、次にポリシーに定義されているルールとチェックとともにインポートしたプロファイルが含まれます。

ステップ 1 **[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[プロファイリング（Profiling）]** > **[プロファイリングポリシー（Profiling Policies）]** 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、前にエクスポートしてこれからインポートするファイルを特定します。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 **[プロファイリングポリシー（Profiling Policies）]** ウィンドウに戻るには、**[プロファイラポリシーリスト（Profiler Policy List）]** リンクをクリックします。

エンドポイント プロファイリング ポリシーのエクスポート

他の Cisco ISE 展開にエンドポイント プロファイリング ポリシーをエクスポートできます。または、XML ファイルを独自のポリシーを作成するためのテンプレートとして使用してインポートできます。ファイルをシステムのデフォルトの場所にダウンロードして、後でインポートに使用することもできます。

エンドポイント プロファイリング ポリシーをエクスポートする際にダイアログが表示され、適切なアプリケーションで profiler_policies.xml を開くか、保存するように要求されます。これ

は XML 形式のファイルで、Web ブラウザまたは他の適切なアプリケーションで開くことができます。

ステップ 1 **[ポリシー（Policy）] > [プロファイリング（Profiling）] > [プロファイリング（Profiling）] > [プロファイリングポリシー（Profiling Policies）]** を選択します。

ステップ 2 [エクスポート（Export）] を選択し、次のいずれかを選択します。

- [選択済みをエクスポート（Export Selected）] : [プロファイリングポリシー（Profiling Policies）] ウィンドウでは、選択済みのエンドポイント プロファイリングのポリシーだけをエクスポートできます。
- [選択済みとエンドポイントをエクスポート（Export Selected with Endpoints）] : 選択済みのエンドポイントプロファイリング ポリシーと、選択済みのエンドポイントプロファイリング ポリシーでプロファイリングされたエンドポイントをエクスポートできます。
- [すべてエクスポート（Export All）] : デフォルトでは、[プロファイリングポリシー（Profiling Policies）] ウィンドウのすべてのプロファイリングポリシーをエクスポートできます。

ステップ 3 [OK] をクリックして、profiler_policies.xml ファイルのエンドポイント プロファイリング ポリシーをエクスポートします。

事前定義されたエンドポイント プロファイリング ポリシー

Cisco ISE を展開するとき、Cisco ISE には事前定義されたデフォルトのプロファイリング ポリシーが含められます。その階層構造を使用して、ネットワーク上の識別されたエンドポイントを分類し、それらを一致するエンドポイント ID グループに割り当てることができます。エンドポイント プロファイリング ポリシーは階層的であるため、[プロファイリング ポリシー（Profiling Policies）] ウィンドウにはデバイスの汎用（親）ポリシーと、それらの親ポリシーが [プロファイリング ポリシー（Profiling Policies）] リストウィンドウに関連付けられている子ポリシーが表示されます。

[プロファイリング ポリシー（Profiling Policies）] ウィンドウには、エンドポイント プロファイリング ポリシーとともに、その名前、タイプ、説明、およびステータス（検証が有効になっているかどうか）が表示されます。

エンドポイント プロファイリング ポリシー タイプは、次のように分類されます。

- シスコ提供：Cisco ISE で事前に定義されたエンドポイント プロファイリング ポリシーはシスコ提供タイプとして識別されます。
    - 管理者による変更：事前に定義されたエンドポイント プロファイリング ポリシーを変更したときに、エンドポイント プロファイリング ポリシーは管理者による変更タイプとして識別されます。Cisco ISE では、事前定義されたエンドポイント プロファイリング ポリシーに行った変更がアップグレード時に上書きされます。

- 管理者作成：作成したエンドポイント プロファイリング ポリシー、またはシスコ提供のエンドポイント プロファイリング ポリシーを複製したときのエンドポイント プロファイリング ポリシーは、管理者作成タイプとして識別されます。

一連のエンドポイントの一般的なポリシー（親）を作成して、その子がルールと条件を継承できるようにすることを推奨します。エンドポイントを分類する必要がある場合は、エンドポイントをプロファイリングするときに、まずエンドポイントプロファイルを親ポリシーと、次にその子孫（子）ポリシーと照合する必要があります。

たとえば、Cisco-Deviceは、すべてのシスコ デバイスの一般的なエンドポイントプロファイリングのポリシーであり、シスコ デバイスの他のポリシーは、Cisco-Deviceの子です。エンドポイントをCisco-IP-Phone 7960として分類する必要がある場合は、まずこのエンドポイントのエンドポイント プロファイルを親のCisco-Deviceポリシー、その子のCisco-IP-Phoneポリシーと照合する必要があり、その後さらに分類するためにCisco-IP-Phone 7960 プロファイリング ポリシーと照合します。

（注） Cisco ISE では、管理者によって変更されたポリシーや子ポリシーは、シスコ提供のラベルが付いていても上書きされません。管理者が変更したポリシーが削除されると、以前のシスコ提供のポリシーに戻ります。次にフィードの更新が発生すると、すべての子ポリシーが更新されます。

アップグレード中に上書きされる事前定義されたエンドポイントプロファイリング ポリシー

[プロファイリング ポリシー（Profiling Policies）] ページで既存のエンドポイント プロファイリング ポリシーを編集できます。また、事前定義されたエンドポイント プロファイリング ポリシーを変更するときは、事前定義されたエンドポイントプロファイルのコピーにすべての設定を保存する必要があります。

アップグレード時に、事前定義されたエンドポイントプロファイルに保存した設定が上書きされます。

エンドポイント プロファイリング ポリシーを削除できない

[プロファイリングポリシー（Profiling Policies）] ウィンドウで選択したエンドポイント プロファイリング ポリシーまたはすべてのエンドポイント プロファイリング ポリシーを削除できます。デフォルトでは、**[プロファイリングポリシー（Profiling Policies）]** ウィンドウからすべてのエンドポイント プロファイリング ポリシーを削除できます。**[プロファイリングポリシー（Profiling Policies）]** ウィンドウですべてのエンドポイント プロファイリング ポリシーを選択して削除しようとしても、エンドポイント プロファイリング ポリシーが他のエンドポイント プロファイリング ポリシーにマッピングされるか、または認証ポリシーにマッピングされる場合、そのエンドポイント プロファイリング ポリシーは削除できません。

- シスコ提供のエンドポイント プロファイリング ポリシーは削除できません。

- エンドポイントプロファイルが他のエンドポイントプロファイルの親として定義されている場合は、**[プロファイリングポリシー（Profiling Policies）]** ウィンドウで親プロファイルを削除できません。たとえば、Cisco-Device は、シスコ デバイスの他のエンドポイント プロファイリング ポリシーの親です。
- 許可ポリシーにマッピングされているエンドポイントプロファイルは削除できません。たとえば、Cisco-IP-Phone は Profiled Cisco IP Phones 許可ポリシーにマッピングされ、Cisco IP Phone の他のエンドポイント プロファイリング ポリシーの親です。

Draeger 医療機器用の事前定義済みプロファイリング ポリシー

Cisco ISE のデフォルトのエンドポイント プロファイルには、Draeger 医療機器用の一般的なポリシー、Draeger-Delta 医療機器用のポリシー、および Draeger-M300 医療機器用のポリシーが含まれます。両方の医療機器にポート 2050 と 2150 があるため、デフォルトの Draeger エンドポイント プロファイリング ポリシーを使用しても、Draeger-Delta 医療機器と Draeger-M300 医療機器を分類できません。

使用中の環境では、これらの Draeger デバイスにポート 2050 と 2150 があるため、デフォルトの Draeger-Delta and Draeger-M300 エンドポイント プロファイリング ポリシーでデバイスの宛先 IP アドレスのチェックに加えて、これらの医療機器を区別できるようにルールを追加する必要があります。

Cisco ISE には、Draeger 医療機器のエンドポイント プロファイリング ポリシーで使用される次のプロファイリング条件があります。

- ポート 2000 が含まれる Draeger-Delta-PortCheck1
- ポート 2050 が含まれる Draeger-Delta-PortCheck2
- ポート 2100 が含まれる Draeger-Delta-PortCheck3
- ポート 2150 が含まれる Draeger-Delta-PortCheck4
- ポート 1950 が含まれる Draeger-M300PortCheck1
- ポート 2050 が含まれる Draeger-M300PortCheck2
- ポート 2150 が含まれる Draeger-M300PortCheck3

不明なエンドポイントのエンドポイント プロファイリング ポリシー

既存のプロファイルに一致せず、Cisco ISE でプロファイリングできないエンドポイントは、不明なエンドポイントです。不明プロファイルは、エンドポイントについて収集された属性が Cisco ISE の既存のプロファイルと一致しない場合にそのエンドポイントに割り当てられるデフォルトのシステム プロファイリング ポリシーです。

不明プロファイルは次のシナリオで割り当てられます。

- エンドポイントが Cisco ISE で動的に検出され、そのエンドポイントに一致するエンドポイント プロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。
- エンドポイントが Cisco ISE で静的に追加され、静的に追加されたエンドポイントに一致するエンドポイント プロファイリング ポリシーがない場合、エンドポイントは不明プロファイルに割り当てられます。

  ネットワークにエンドポイントを静的に追加した場合、そのエンドポイントは Cisco ISE のプロファイリング サービスによってプロファイリングされません。不明プロファイルを適切なプロファイルに後で変更できます。割り当てたプロファイリング ポリシーは、Cisco ISE によって再プロファイリングされることはありません。

静的に追加されたエンドポイントのエンドポイントプロファイリングポリシー

静的に追加されたエンドポイントをプロファイリングするために、プロファイリング サービスは、新しい MATCHEDPROFILE 属性をエンドポイントに追加することによって、エンドポイントのプロファイルを計算します。計算されたプロファイルは、そのエンドポイントが動的にプロファイリングされるときのエンドポイントの実際のプロファイルです。これにより、静的に追加されたエンドポイントの計算されたプロファイルと動的にプロファイリングされたエンドポイントに一致するプロファイルの間の不一致を見つけることができます。

スタティックIPデバイスのエンドポイントプロファイリングポリシー

静的に割り当てられた IP アドレスを持つエンドポイントがある場合、そのスタティック IP デバイスのプロファイルを作成できます。

スタティック IP アドレスが割り当てられているエンドポイントをプロファイリングするには、RADIUS プローブまたは SNMP クエリー プローブと SNMP トラップ プローブを有効にする必要があります。

エンドポイント プロファイリング ポリシーの一致

1 つ以上のルールで定義されているプロファイリング条件がプロファイリング ポリシーに一致する場合、Cisco ISE は、エンドポイント用に選択されたポリシーを、評価されたポリシーではなく、一致したポリシーであると常に見なします。ここで、そのエンドポイントのスタティック割り当てのステータスがシステムで false に設定されます。ただし、エンドポイントの編集時にスタティック割り当て機能を使用して、システム内の既存のプロファイリング ポリシーに静的に再割り当てした後は、true に設定されることがあります。

次は、エンドポイントの一致したポリシーに適用されます。

- スタティックに割り当てられたエンドポイントでは、プロファイリング サービスは MATCHEDPROFILE を計算します。

- 動的に割り当てられたエンドポイントでは、MATCHEDPROFILEは一致するエンドポイント プロファイルと同じです。

ダイナミック エンドポイントに一致するプロファイリング ポリシーは、プロファイリング ポリシーで定義された1つ以上のルールを使用して特定できます。また、分類のために、必要に応じてエンドポイント ID グループを割り当てることができます。

エンドポイントが既存のポリシーにマッピングされる場合、プロファイリング サービスは、一連のポリシーが一致する最も近い親プロファイルをプロファイリング ポリシーの階層で検索し、エンドポイントを適切なエンドポイント ポリシーに割り当てます。

許可に使用するエンドポイント プロファイリング ポリシー

許可ルールにエンドポイント プロファイリング ポリシーを使用できます。このとき、エンドポイント プロファイリング ポリシーのチェックを含めるように属性として新しい条件を作成できます。属性値は、エンドポイント プロファイリング ポリシーの名前になります。エンドポイント プロファイリング ポリシーを、エンドポイント辞書から選択できます。エンドポイント プロファイリング ポリシーには、属性 PostureApplicable、EndPointPolicy、LogicalProfile および BYODRegistration が含まれています。

PostureApplicable の属性値は、オペレーティング システムに基づいて自動設定されます。この値は、IOSおよびAndroidデバイスでは[なし（No）]に設定されます。これらのプラットフォームでは、ポスチャを実行するためのAnyConnectがサポートされていないためです。この値は、Mac OSX および Windows デバイスでは [はい（Yes）] に設定されます。

EndPointPolicy、BYODRegistration および ID グループの組み合わせを含む許可ルールを定義できます。

エンドポイント プロファイリング ポリシーの論理プロファイルによるグループ化

論理プロファイルは、エンドポイント プロファイリング ポリシーがシスコ提供か、管理者作成かに関係なく、プロファイルまたは関連付けられているプロファイルのカテゴリのコンテナです。エンドポイント プロファイリング ポリシーは、複数の論理プロファイルに関連付けることができます。

許可ポリシー条件で論理プロファイルを使用して、プロファイルのカテゴリでネットワーク全体のアクセス ポリシーの作成に役立てることができます。許可の単純条件を作成して、許可ルールに含めることができます。許可条件で使用できる属性と値のペアは、論理プロファイル（属性）および論理プロファイルの名前（値）であり、エンドポイント システム ディクショナリ内にあります。

たとえば、カテゴリに一致するエンドポイント プロファイリング ポリシーを論理プロファイルに割り当てることによって、Android、Apple iPhone、Blackberry などのすべてのモバイル デバイスの論理プロファイルを作成できます。Cisco ISE には、すべての IP フォンのデフォルト

の論理プロファイルである IP-Phone が含まれ、IP-Phone には、IP-Phone、Cisco IP-Phone、Nortel-IP-Phone-2000-Series、および Avaya-IP-Phone プロファイルが含まれます。

論理プロファイルの作成

エンドポイント プロファイリング ポリシーのカテゴリをグループ化するために使用できる論理プロファイルを作成でき、それにより、プロファイルまたは関連付けられているプロファイルのカテゴリ全体を作成できます。エンドポイント プロファイリング ポリシーを割り当てられたセットから削除して、使用可能なセットに戻すこともできます。ロジカルプロファイルの詳細については、エンドポイントプロファイリングポリシーの論理プロファイルによるグループ化 （263 ページ）を参照してください。

ステップ 1 **[ポリシー（Policy）]** > **[プロファイリング（Profiling）]** > **[プロファイリング（Profiling）]** > **[論理プロファイル（Logical Profiles）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] のテキスト ボックスに新しい論理プロファイルの名前と説明を入力します。

ステップ 4 [使用可能なポリシー（Available Policies）] からエンドポイント プロファイリング ポリシーを選択して、論理プロファイルに割り当てます。

ステップ 5 右矢印をクリックして、選択したエンドポイント プロファイリング ポリシーを [割り当てられたポリシー（Assigned Policies）] に移動します。

ステップ 6 **[送信（Submit）]** をクリックします。

プロファイリング例外アクション

例外アクションは、エンドポイント プロファイリング ポリシーで参照できる単一の設定可能なアクションであり、アクションに関連付けられている例外条件が満たされるとトリガーされます。

例外アクションのタイプは次のいずれかになります。

- シスコ提供：シスコ提供の例外アクションは削除できません。Cisco ISE では、Cisco ISE のエンドポイントをプロファイリングするときに、次の編集不能なプロファイリング例外アクションがトリガーされます。
  - 許可変更：エンドポイントが許可ポリシーで使用されるエンドポイント ID グループに対して追加または削除される場合、プロファイリング サービスは許可変更を発行します。
  - エンドポイント削除：エンドポイントが [エンドポイント（Endpoints）] ページでシステムから削除されるか、Cisco ISE ネットワーク上で編集ページから不明プロファイルに再割り当てされると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。

- FirstTimeProfiled：エンドポイントが Cisco ISE で初めてプロファイリングされ、そのエンドポイントのプロファイルが不明プロファイルから既存のプロファイルに変更されて、そのエンドポイントが Cisco ISE ネットワーク上で認証に失敗すると、Cisco ISE で例外アクションがトリガーされ、CoA が発行されます。

- 管理者作成：Cisco ISE では、作成したプロファイリング例外アクションがトリガーされます。

例外アクションの作成

1 つ以上の例外ルールを定義し、1 つのプロファイリング ポリシーに関連付けることができます。この関連付けにより、Cisco ISE でエンドポイントをプロファイリングする際にプロファイリング ポリシーが一致し、少なくとも 1 つの例外ルールが一致する場合、例外アクション（単一の設定可能なアクション）がトリガーされます。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [例外アクション（Exception Actions）]** 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 [名前（Name）] と [説明（Description）] のテキスト ボックスに例外アクションの名前と説明を入力します。

ステップ 4 [CoA アクション（CoA Action）] チェックボックスをオンにします。

ステップ 5 [ポリシー割り当て（Policy Assignment）] ドロップダウン リストをクリックしてエンドポイント ポリシーを選択します。

ステップ 6 **[送信（Submit）]** をクリックします。

ポリシーおよびIDグループのスタティック割り当てによるエンドポイントの作成

[エンドポイント（Endpoints）] ページでエンドポイントの MAC アドレスを使用して、新しいエンドポイントを静的に作成できます。また、スタティック割り当ての [エンドポイント（Endpoints）] ページで、エンドポイント プロファイリング ポリシーおよび ID グループを選択できます。

通常のモバイルデバイス（MDM）エンドポイントは、[エンドポイント ID（Endpoints Identities）] リストに表示されます。リストページには、[ホスト名（Hostname）]、[デバイス タイプ（Device Type）]、[デバイス ID（Device ID）] など、MDM エンドポイントの属性のカラムが表示されます。[スタティック割り当て（Static Assignment）]、[スタティック グループ割り当て（Static Group Assignment）] などのその他のカラムは、デフォルトでは表示されません。

（注） このページを使用して、MDMエンドポイントを追加、編集、削除、インポートまたはエクスポートすることはできません。

ステップ 1 **[ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 エンドポイントの MAC アドレスをコロンで区切られた 16 進表記で入力します。

ステップ 4 [ポリシー割り当て（Policy Assignment）] ドロップダウン リストから一致するエンドポイント ポリシーを選択して、スタティック割り当てステータスをダイナミックからスタティックに変更します。

ステップ 5 [スタティック割り当て（Static Assignment）] チェックボックスをオンにして、エンドポイントに割り当てられたスタティック割り当てのステータスをダイナミックからスタティックに変更します。

ステップ 6 [ID グループ割り当て（Identity Group Assignment）] ドロップダウン リストから、新しく作成されたエンドポイントを割り当てるエンドポイント ID グループを選択します。

ステップ 7 エンドポイント ID グループのダイナミック割り当てをスタティックに変更するには、[スタティック グループ割り当て（Static Group Assignment）] チェックボックスをオンにします。

ステップ 8 **[送信（Submit）]** をクリックします。

CSV ファイルを使用したエンドポイントのインポート

Cisco ISE テンプレートから作成した CSV ファイルからエンドポイントをインポートし、エンドポイントの詳細を使用して更新することができます。Cisco ISE からエクスポートされたエンドポイントには約 90 個の属性が含まれているため、別の ISE 展開には直接インポートできません。インポートが許可されていない列が CSV ファイルにある場合は、インポートできない属性のリストを含むメッセージが表示されます。ファイルを再度インポートする前に、指定された列を削除する必要があります。

インポートできる属性は約 31 個あります。このリストには、MACAddress、EndPointPolicy、IdentityGroup が含まれています。オプション属性は次のとおりです。

説明	PortalUser	LastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	デバイスタイプ（Device Type）	host-name
PortalUser.GuestStatus	StaticAssignment	参照先
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion

PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<custom attribute name>	—	—

ファイル ヘッダーは、デフォルトのインポート テンプレートで指定されている形式にして、エンドポイントのリストが次の順序で表示されるようにする必要があります。MACAddress、EndpointPolicy、IdentityGroup、<オプション属性として上に記載されている属性のリスト>。次のファイル テンプレートを作成できます。

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <オプション属性として上に記載されている属性のリスト>

MAC アドレスを除くすべての属性値は、CSV ファイルからエンドポイントをインポートする際に省略可能です。特定の値のないエンドポイントをインポートする場合も、値はカンマで区切られます。次の例を参考にしてください。

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser, など

CSV ファイルを使用してエンドポイントをインポートするには、次の手順を実行します。

ステップ 1 **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** の順に選択します。

ステップ 2 [ファイルからインポート（Import from File）] をクリックします。

ステップ 3 [参照（Browse）] をクリックして、作成済みの CSV ファイルを見つけます。

ステップ 4 **[送信（Submit）]** をクリックします。

エンドポイントのカスタム属性をインポートするには、**[管理（Administration）]** > **[ID 管理（Identity Management）]** > **[設定（Settings）]** > **[エンドポイントカスタム属性（Endpoint Custom Attributes）]** ウィンドウで、正しいデータタイプを使用して CSV ファイルと同じカスタム属性を作成する必要があります。それらの属性には、CUSTOM というプレフィックスを付けてエンドポイント属性と区別する必要があります。

エンドポイントで使用可能なデフォルトのインポート テンプレート

エンドポイントのインポートに使用できるエンドポイントを更新できるテンプレートを生成できます。デフォルトで、[テンプレートの生成（Generate a Template）] リンクを使用して、Microsoft Office Excel アプリケーションで CSV ファイルを作成し、このファイルをシステム上にローカルに保存できます。ファイルは **[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]>[インポート（Import）]>[ファイルからインポート（Import from File）]** にあります。[テンプレートの生成（Generate a Template）] リンクを使用してテンプレートを作成でき、Cisco ISE サーバーは、[template.csv を開く（Opening template.csv）] ダイアログを表示します。このダイアログを使用すると、デフォルトの template.csv ファイルを開いたり、template.csv ファイルをシステム上にローカルに保存できます。このダイアログで template.csv ファイルを開くことを選択した場合、このファイルは Microsoft Office Excel アプリケーションで開かれます。デフォルトの template.csv ファイルには、MAC アドレス、エンドポイント ポリシー、エンドポイント ID グループ、およびその他のオプション属性が表示されるヘッダー行が含まれています。

エンドポイントの MAC アドレス、エンドポイント プロファイリング ポリシー、エンドポイント ID グループを、インポートするオプションの属性値とともに更新し、新しいファイル名を使用してファイルを保存します。このファイルをエンドポイントのインポートのために使用できます。[テンプレートの生成（Generate a Template）] リンクを使用したときに作成される template.csv ファイルのヘッダー行を参照してください。

表 *54 : CSV* テンプレート ファイル

MAC	EndPointPolicy	IdentityGroup	その他のオプションの属性
11:11:11:11:11:11	Android	プロファイル済み	<Empty>/<Value>

インポート中の不明なエンドポイントの再プロファイリング

インポートに使用するファイルに、MAC アドレスを持つエンドポイントがあり、それらに割り当てられているエンドポイントプロファイリング ポリシーが不明プロファイルである場合、これらのエンドポイントはインポート中に Cisco ISE でただちに一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。ただし、不明プロファイルに静的に割り当てられることはありません。エンドポイントに割り当てられているエンドポイント プロファイリング ポリシーが CSV ファイルにない場合、これらのエンドポイントは不明プロファイルに割り当てられ、一致するエンドポイント プロファイリング ポリシーに再プロファイリングされます。次に、Cisco ISE が、インポート中に Xerox_Device プロファイルに一致する不明プロファイルをどのように再プロファイリングするか、および割り当てられていないエンドポイントをどのように再プロファイリングするかを示します。

表 *55 :* 不明プロファイル：ファイルからのインポート

MACアドレス（MAC Address）	Cisco ISE でのインポート前に割り当てられたエンドポイントプロファイリングポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイントプロファイリングポリシー
00:00:00:00:01:02	不明（Unknown）	Xerox-Device
00:00:00:00:01:03	不明（Unknown）	Xerox-Device
00:00:00:00:01:04	不明（Unknown）	Xerox-Device
00:00:00:00:01:05	プロファイルがエンドポイントに割り当てられていない場合、そのエンドポイントは不明プロファイルに割り当てられ、一致するプロファイルに再プロファイリングされます。	Xerox-Device

インポートされない無効な属性を持つエンドポイント

CSV ファイルに存在するエンドポイントのいずれかに無効な属性がある場合、エンドポイントはインポートされず、エラー メッセージが表示されます。

たとえば、エンドポイントがインポートに使用されるファイル内で無効なプロファイルに割り当てられている場合、それらのエンドポイントは、Cisco ISE には一致するプロファイルがないためインポートされません。エンドポイントが CSV ファイル内の無効なプロファイルに割り当てられている場合、それらのエンドポイントがインポートされない仕組みを下に示します。

表 *56 :* 無効なプロファイル：ファイルからのインポート

MACアドレス（MAC Address）	Cisco ISE でのインポート前に割り当てられたエンドポイントプロファイリングポリシー	Cisco ISE でのインポート後に割り当てられたエンドポイントプロファイリングポリシー
00:00:00:00:01:02	不明（Unknown）	Xerox-Device
00:00:00:00:01:05	00:00:00:00:01:05 などのエンドポイントが Cisco ISE 使用可能なプロファイル以外の無効なプロファイルに割り当てられている場合、Cisco ISE では、ポリシー名が無効で、エンドポイントがインポートされないことを示す警告メッセージが表示されます。	エンドポイントは、Cisco ISE 内に一致するプロファイルがないためインポートされません。

LDAP サーバーからのエンドポイントのインポート

エンドポイントの MAC アドレス、関連するプロファイル、およびエンドポイント ID グループを LDAP サーバーからセキュアにインポートできます。

始める前に

エンドポイントをインポートする前に、LDAP サーバーがインストールされていることを確認します。

LDAP サーバーからインポートするには、接続設定値およびクエリー設定値を設定する必要があります。接続設定値またはクエリー設定値が Cisco ISE で間違って設定されていると、「LDAP インポートが失敗：（LDAP import failed:）」エラー メッセージが表示されます。

ステップ 1 **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** > **[インポート（Import）]** > **[LDAP からのインポート（Import From LDAP）]** の順に選択します。

ステップ 2 接続設定の値を入力します。

ステップ 3 クエリー設定の値を入力します。

ステップ 4 **[送信（Submit）]** をクリックします。

CSV ファイルを使用したエンドポイントのエクスポート

CSV ファイルを使用して、すべてのエンドポイントまたは選択したエンドポイントのみをエクスポートできます。エンドポイントは MAC アドレス、エンドポイント プロファイリング ポリシー、およびエンドポイント ID グループと、約 90 属性とともに一覧表示されます。カスタム属性は、CSV ファイルにもエクスポートされ、CUSTOM というプレフィクスが付けられて、他のエンドポイント属性と区別されます。

（注） 1 つの展開からエクスポートされたエンドポイントのカスタム属性を別の展開にインポートするには、**[管理（Administration）]** > **[ID 管理（Identity Management）]** > **[設定（Settings）]** > **[エンドポイントカスタム属性（Endpoint Custom Attributes）]** ウィンドウで同じカスタム属性を作成し、元の展開で指定したのと同じデータタイプを使用する必要があります。

[すべてエクスポート（Export All）] では Cisco ISE のすべてのエンドポイントがエクスポートされ、**[選択済みをエクスポート（Export Selected）]** ではユーザーが選択したエンドポイントのみがエクスポートされます。デフォルトでは、profiler_endpoints.csv が CSV ファイルであり、Microsoft Office Excel が CSV ファイルを開くデフォルトのアプリケーションです。

CSV ファイルを使用してエンドポイントをエクスポートするには、次の手順を実行します。

ステップ 1 **[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]** を選択します。

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

ステップ 3 [OK] をクリックして CSV ファイルを保存します。

エクスポートされたスプレッドシート内の属性のほとんどはシンプルなものです。属性の説明は次のとおりです。

- *UpdateTime*：エンドポイント属性の変更により、プロファイラがエンドポイントを最後に更新した時間。エンドポイント セッションの開始以降、更新がない場合、値は 0 です。更新中、一時的に空白になります。
- *InactivityTime*：エンドポイントがアクティブになってからの時間。

識別されたエンドポイント

Cisco ISE では、ネットワークに接続してネットワーク リソースを使用する識別されたエンドポイントが、[エンドポイント（Endpoints）] ウィンドウに表示されます。エンドポイントは、通常、有線および無線のネットワーク アクセス デバイスと VPN を介してネットワークに接続するネットワーク対応デバイスです。エンドポイントとして、パーソナル コンピュータ、ラップトップ、IP Phone、スマート フォン、ゲーム コンソール、プリンタ、ファクス機などがあります。

16 進数形式で表したエンドポイントの MAC アドレスは、常にエンドポイントの一意の表現ですが、それらに関連付けられた属性と値のさまざまなセット（属性と値のペアと呼ばれる）でエンドポイントを識別することもできます。エンドポイントの属性のさまざまなセットは、エンドポイント機能、ネットワーク アクセス デバイスの機能と設定、およびこれらの属性の収集に使用する方法（プローブ）に基づいて収集できます。

動的にプロファイリングされるエンドポイント

エンドポイントは、ネットワークで検出されると、設定されているプロファイリング エンドポイントのプロファイリング ポリシーに基づいて動的にプロファイリングされ、プロファイルに応じて一致するエンドポイント ID グループに割り当てられます。

静的にプロファイリングされるエンドポイント

MAC アドレスを使用してエンドポイントを作成し、Cisco ISE のエンドポイント ID グループとともにプロファイルをそのエンドポイントに割り当てると、エンドポイントを静的にプロファイリングすることができます。Cisco ISE では、静的に割り当てられたエンドポイントに対して、プロファイリング ポリシーおよび ID グループを再割り当てしません。

不明なエンドポイント

エンドポイントに対して一致するプロファイリング ポリシーがない場合、不明なプロファイリング ポリシー（「不明」）を割り当てることで、エンドポイントを不明としてプロファイリングできます。不明なエンドポイント ポリシーにプロファイリングされたエンドポイントの場合、そのエンドポイントに対して収集された属性または属性セットを使用してプロファイルを作成する必要があります。いずれのプロファイルにも一致しないエンドポイントは、不明なエンドポイント ID グループにグループ化されます。

識別されたエンドポイントの、ポリシー サービス ノード データベースへのローカル保存

Cisco ISE は識別されたエンドポイントをポリシー サービス ノードのデータベースにローカルに書き込みます。エンドポイントをデータベースにローカル保存した後は、それらのエンドポイントは、重要な属性がエンドポイントで変更され、他のポリシー サービス ノード データベースに複製されているときにのみ、管理ノード データベースで使用できる（リモート書き込み）ようになります。

重要な属性は次のとおりです。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

Cisco ISE でエンドポイント プロファイル定義を変更した場合、すべてのエンドポイントを再プロファイリングする必要があります。エンドポイント属性を収集するポリシー サービス ノードが、これらのエンドポイントの再プロファイリングを担当します。

あるポリシー サービス ノードが、最初は別のポリシー サービス ノードによって属性が収集されていたエンドポイントに関する属性を収集し始めると、エンドポイントの所有権が現在のポリシー サービス ノードに移ります。新しいポリシー サービス ノードは、前のポリシー サービス ノードから最新の属性を取得して、すでに収集されている属性と調整します。

重要な属性がエンドポイントで変更されると、エンドポイントの属性は管理ノード データベースに自動的に保存され、エンドポイントの最新の重要な変更を使用できます。エンドポイントを所有するポリシー サービス ノードが何らかの理由で使用できない場合、管理 ISE ノードが

所有者を失ったエンドポイントを再プロファイリングします。また、このようなエンドポイントに対して新しいポリシー サービス ノードを設定する必要があります。

クラスタのポリシー サービス ノード

Cisco ISE では、ポリシー サービス ノード グループをクラスタとして使用するため、クラスタ内の複数のノードが同じエンドポイントの属性を収集するときに、エンドポイント属性を交換できます。1 つのロード バランサの背後に存在する、すべてのポリシー サービス ノードに対するクラスタを作成することを推奨します。

現在のオーナー以外の別のノードが同じエンドポイントの属性を受信した場合、属性をマージし、所有権の変更が必要かどうかを決定するために、現在のオーナーから最新の属性を要求するメッセージをクラスタ全体に送信します。Cisco ISE でノード グループを定義していない場合は、すべてのノードが 1 つのクラスタ内にあると想定されます。

Cisco ISE でエンドポイントの作成と複製への変更は行われません。エンドポイントの所有権の変更のみが、プロファイリングに使用される、静的属性と動的属性で構成される属性の許可されたリストに基づいて決定されます。

次のいずれかの属性が変更された場合、後続の属性の収集時に、エンドポイントは管理ノードで更新されます。

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

エンドポイントが管理ノードで編集および保存されている場合、この属性はエンドポイントの現在のオーナーから取得されます。

エンドポイント ID グループの作成

Cisco ISE では、検出したエンドポイントを、対応するエンドポイント ID グループにグループ化します。Cisco ISE では、システム定義された複数のエンドポイントの ID グループが事前に用意されています。[エンドポイントIDグループ（Endpoint Identity Groups）] ウィンドウでは、追加のエンドポイント ID グループも作成できます。作成したエンドポイント ID グループを編

集または削除できます。システムで定義されたエンドポイント ID グループの説明のみを編集できます。これらのグループの名前を編集または削除することはできません。

ステップ 1 **[管理（Administration）] > [ID 管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity 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 作成するエンドポイント ID グループの [名前（Name）] に入力します（エンドポイント ID グループの名前にはスペースを入れないでください）。

ステップ 4 作成するエンドポイント ID グループの [説明（Description）] に入力します。

ステップ 5 [親グループ（Parent Group）] ドロップダウン リストをクリックして、新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを選択します。

ステップ 6 **[送信（Submit）]** をクリックします。

識別されたエンドポイントの、エンドポイントIDグループでのグループ化

Cisco ISE では、エンドポイント プロファイリング ポリシーに基づいて、検出されたエンドポイントを対応するエンドポイント ID グループにグループ化します。プロファイリング ポリシーは階層構造になっており、Cisco ISE のエンドポイント ID グループ レベルで適用されます。エンドポイントをエンドポイント ID グループにグループ化し、プロファイリング ポリシーをエンドポイント ID グループに適用すると、Cisco ISE により、対応するエンドポイント プロファイリング ポリシーを確認してエンドポイント プロファイルへのエンドポイントのマッピングを決定できます。

Cisco ISE によってエンドポイント ID グループのセットがデフォルトで作成され、これを使用して、エンドポイントを動的または静的に割り当てできる独自の ID グループを作成できます。エンドポイント ID グループを作成し、システムが作成した ID グループの 1 つにその ID グループを関連付けることができます。また、自分が作成したエンドポイントをシステム内のいずれかの ID グループに静的に割り当てることができ、ID グループがプロファイリング サービスで再割り当てされることはありません。

エンドポイントに対して作成されるデフォルトのエンドポイントIDグループ

Cisco ISE は次のエンドポイント ID グループを作成します。

- [ブラックリスト（blacklist）][ブロック済みリスト（Blocked List）]：このエンドポイント ID グループには、Cisco ISE でこのグループに静的に割り当てられたエンドポイント、およびデバイス登録ポータルでブロックされたエンドポイントが含まれます。許可プロファイルを Cisco ISE で定義して、このグループのエンドポイントへのネットワーク アクセスを許可または拒否できます。

- [GuestEndpoints]：このエンドポイント ID グループには、ゲストユーザーが使用するエンドポイントが含まれます。
- [プロファイル済み（Profiled）]：このエンドポイント ID グループには、Cisco ISE の Cisco IP 電話およびワークステーションを除くエンドポイント プロファイリング ポリシーに一致するエンドポイントが含まれます。
- [RegisteredDevices（登録済みデバイス）]：このエンドポイント ID グループには、デバイス登録ポータルを介して従業員が追加した登録済みデバイスであるエンドポイントが含まれます。プロファイリング サービスは通常、これらのデバイスがこのグループに割り当てられている場合、これらのデバイスを引き続きプロファイリングします。エンドポイントは Cisco ISE のこのグループに静的に割り当てられ、プロファイリング サービスがこれらのエンドポイントを他の ID グループに割り当てることはできません。これらのデバイスは、エンドポイント リストの他のエンドポイントと同様に表示されます。デバイス登録ポータルを介して追加されたこれらのデバイスは、Cisco ISE の [エンドポイント（Endpoints）] ウィンドウのエンドポイントリストで編集、削除、およびブロックできます。デバイス登録ポータルでブロックされているデバイスは、[ブラックリスト（blacklist）] エンドポイント ID グループに割り当てられ、Cisco ISE に存在する認証プロファイルは、ブロックされたデバイスを URL（「無許可ネットワークアクセス」と表示される、ブロックされたデバイスのデフォルトポータルページ）にリダイレクトします。
- 不明：このエンドポイント ID グループには、Cisco ISE のプロファイルに一致しないエンドポイントが含まれます。

上記のシステムで作成されたエンドポイント ID グループに加えて、Cisco ISE ではプロファイル済み（親）ID グループに関連付けられる次のエンドポイント ID グループが作成されます。親グループは、システムに存在するデフォルトの ID グループです。

- Cisco-IP-Phone：ネットワーク上のすべてのプロファイル済み Cisco IP 電話 が含まれる ID グループです。
- [ワークステーション（Workstation）]：ネットワーク上のすべてのプロファイル済みワークステーションが含まれる ID グループです。

一致するエンドポイント プロファイリング ポリシーに対して作成されるエンドポイント ID グループ

既存のポリシーと一致するエンドポイント ポリシーがある場合、プロファイリング サービスは一致するエンドポイント ID グループを作成できます。この ID グループは、プロファイル済みエンドポイント ID グループの子になります。エンドポイント ポリシーを作成する場合、[プロファリング ポリシー（Profiling Policies）] ページの [一致する ID グループの作成（Create Matching Identity Group）] チェックボックスをオンにして、一致するエンドポイント ID グループを作成できます。プロファイルのマッピングが削除されない限り、一致する ID グループは削除できません。

エンドポイント ID グループでの静的なエンドポイントの追加

エンドポイント ID グループの静的に追加されたエンドポイントを追加または削除できます。

[エンドポイント（Endpoints）] ウィジェットのエンドポイントのみを特定の ID グループに追加できます。エンドポイントを特定のエンドポイント ID グループに追加した場合、そのエンドポイントは、前に動的にグループ化されたエンドポイント ID グループから移動されます。

エンドポイントを最近追加したエンドポイント ID グループから削除すると、そのエンドポイントは、適切な ID グループに再プロファイリングされます。エンドポイントは、システムから削除されませんが、エンドポイントの ID グループからのみ削除されます。

ステップ 1 **[管理（Administration）] > [ID 管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]** を選択します。

ステップ 2 エンドポイント ID グループを選択して [編集（Edit）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [エンドポイント（Endpoints）] ウィジェットでエンドポイントを選択して、選択したエンドポイントをエンドポイント ID グループに追加します。

ステップ 5 [エンドポイント グループ リスト（Endpoint Group List）] リンクをクリックして、[エンドポイント ID グループ（Endpoint Identity Groups）] ページに戻ります。

ダイナミックエンドポイントの、IDグループへの追加または削除後の再プロファイリング

エンドポイント ID グループが静的に割り当てられていない場合、エンドポイント ID グループに追加した、またはエンドポイント ID グループから削除したエンドポイントは、再プロファイリングされます。ISE プロファイラにより動的に識別されたエンドポイントは、適切なエンドポイント ID グループに表示されます。動的に追加されたエンドポイントをエンドポイント ID グループから削除した場合、Cisco ISE では、エンドポイント ID グループからエンドポイントを正常に削除したが、それらのエンドポイントをエンドポイント ID グループに再プロファイリングして戻すことを示すメッセージが表示されます。

許可ルールで使用されるエンドポイント ID グループ

エンドポイント ID グループを許可ポリシーで効率的に使用して、検出されたエンドポイントに適切なネットワーク アクセス権限を付与することができます。たとえば、すべてのタイプの Cisco IP Phone 用の許可ルールが、デフォルトで、Cisco ISE の **[ポリシー セット（Policy Sets）] > [デフォルト（Default）] > [許可ポリシー（Authorization Policy）]** で使用できます。

エンドポイント プロファイリング ポリシーがスタンドアロン ポリシー（他のエンドポイント プロファイリング ポリシーの親でない）であるか、またはエンドポイント プロファイリング ポリシーの親ポリシーが無効でないことを確認する必要があります。

エニーキャストおよびプロファイラサービス

エニーキャストは、同じ IP アドレスが 2 つ以上のホストに割り当てられ、データを受信する最適なターゲットを決定するためにルーティングが許可されるネットワーキング技術です。データをプロファイリングする単一のターゲット（RADIUS、DHCP リレー、SNMP トラップ、および NetFlow）を提供するロードバランサの使用例と同様に、エニーキャストでは、複数の宛先に同じデータを送信しないように、単一の IP ターゲットで送信元を設定できます。

エニーキャスト IP アドレスを実際の PSN インターフェイス IP アドレスまたはロードバランサの仮想 IP アドレスに割り当てて、データセンター間の冗長性をサポートできます。エニーキャスト IP アドレスを ISE ギガビットイーサネット 0 管理インターフェイスに割り当てないでください。

エニーキャストに使用されるインターフェイスは、プロファイラプローブで使用される専用インターフェイスである必要があります。エニーキャスト IP アドレスがロードバランサの仮想 IP アドレスに割り当てられている場合、同じ要件は適用されません。

エニーキャストを使用する場合、ノード障害が自動的に検出され、障害が発生したノードまでの該当するルートがルーティングテーブルから削除されることが不可欠です。エニーキャストのターゲットがリンクまたは VLAN の唯一のホストの場合、障害が発生するとルートを自動的に削除できます。

IP エニーキャストを展開する場合、各ターゲットまでのルートメトリックに有意な重み付けやバイアスを確実に持たせることがきわめて重要になります。エニーキャストターゲットまでのルートがフラッピングする場合や、結果的に等コストマルチパス（ECMP）ルーティングのシナリオになる場合、所定のサービス（RADIUS AAA、DHCP または SNMP トラッププロファイリング、HTTPS ポータル）に関するトラフィックが各ターゲットに分散されることがあります。その場合、過剰なトラフィックやサービスの障害が発生したり（RADIUS AAA および HTTPS ポータル）、最適とは言えないプロファイリングやデータベース レプリケーションになります（プロファイリングサービス）。

IP エニーキャストの主要な利点は、アクセス デバイス、プロファイル データ ソース、DNS の設定が大幅に簡単になることです。また、特定のエンドポイントに関するデータのみ単一の PSN に送信されることが保証されるため、ISE プロファイリングが最適化されます。追加のルート設定を慎重に計画し、適切なモニターリングによって管理する必要があります。ただし、明確なサブネットワークおよび IP アドレスが使用されないため、トラブルシューティングも困難になります。

プロファイラ フィード サービス

プロファイラ条件、例外アクション、および NMAP スキャン アクションは、シスコ提供または管理者作成として分類され、システム タイプ属性に表示されます。エンドポイント プロファイリング ポリシーは、シスコ提供、管理者作成、または管理者による変更として分類されます。これらの分類は、システム タイプ属性に表示されます。

システム タイプ属性によって、プロファイラ条件、例外アクション、NMAP スキャン アクション、およびエンドポイント プロファイリング ポリシーに対して異なる操作を実行できます。シスコ提供の条件、例外アクション、NMAP スキャン アクションは編集または削除できません。シスコが提供するエンドポイント ポリシーは削除できません。ポリシーを編集すると、管理者による変更と見なされます。フィード サービスによってポリシーが更新されると、管理者によって変更されたポリシーは、それが基づいていたシスコ提供ポリシーの最新のバージョンに置き換えられます。

新規および更新されたエンドポイント プロファイリング ポリシーと更新された OUI データベースは、Cisco フィード サーバーから取得できます。Cisco ISE へのサブスクリプションが必要です。また、適用、成功、および失敗のメッセージに関する電子メール通知を受信することもできます。シスコによるフィード サービスの改善のため、フィード サービス アクションに関する匿名の情報をシスコに返信することができます。

OUI データベースには、ベンダーに割り当てられた MAC OUI が含まれています。OUI リストは、次の URL から入手できます。 http://standards.ieee.org/develop/regauth/oui/oui.txt

Cisco ISE は毎日ローカル Cisco ISE サーバーのタイム ゾーンの午前 1:00 にポリシーと OUI データベースの更新をダウンロードします。Cisco ISE は、これらのダウンロードされたフィード サーバー ポリシーを自動的に適用し、また、以前の状態に復元できるように変更内容を保存します。以前の状態に復元すると、新しいエンドポイント プロファイリング ポリシーは削除され、更新されたエンドポイント プロファイリング ポリシーは以前の状態に復元されます。さらに、プロファイラ フィード サービスは自動的に無効になります。

また、オフライン モードで手動でフィード サービスを更新することもできます。ISE 展開をシスコ フィード サービスに接続できない場合には、このオプションを使用して更新プログラムを手動でダウンロードすることができます。

（注） 60 日間のうち、ライセンスがコンプライアンス外（OOC）となっている日数が 45 日間に達すると、フィード サービスからの更新が許可されなくなります。ライセンスがコンプライアンス外になるのは、ライセンスの有効期限が切れるか、または使用が許可されているセッション数を超えた時点です。

プロファイラ フィード サービスの設定

プロファイラ フィード サービスは、Cisco フィード サーバーから新規および更新されたエンドポイント プロファイリング ポリシーと MAC OUI データベース更新を取得します。フィード サービスが使用できない場合、またはその他のエラーが発生した場合は、操作監査レポートで報告されます。

匿名のフィード サービス使用レポートをシスコに返信するように Cisco ISE を設定できます。そのレポートでは、次の情報がシスコに送信されます。

- Hostname：Cisco ISE のホスト名
- MaxCount：エンドポイントの合計数

- ProfiledCount：プロファイリングされたエンドポイントの数
- UnknownCount：不明なエンドポイントの数
- MatchSystemProfilesCount：シスコ提供のプロファイルの数
- UserCreatedProfiles：ユーザーが作成したプロファイルの数

シスコから提供されるプロファイリング ポリシーの CoA タイプを変更できます。フィード サービスがそのポリシーを更新すると、CoA タイプは変更されませんが、そのポリシーの残りの属性は引き続き更新されます。

始める前に

分散展開またはスタンドアロン ISE ノードでは、Cisco ISE 管理者ポータルからのみプロファイラ フィード サービスを設定できます。

フィード更新について管理者ポータルから電子メール通知を送信する場合は、Simple Mail Transfer Protocol（SMTP）サーバーを設定します（**[管理（Administration）] > [システム（System）] > [設定（Settings）]**）。

フィード サービスをオンラインで更新するには、次の手順に従います。

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 Certificates）]** を選択し、[QuoVadis Root CA 2] が有効になっているかを確認します。

ステップ 2 **[ワーク センター（Work Centers）] > [プロファイラ（Profiler）] > [フィード（Feeds）]** の順に選択します。
[管理（Administration）] > [フィードサービス（FeedService）] > [プロファイラ（Profiler）] ページでこのオプションにアクセスすることもできます。

ステップ 3 [オンライン サブスクリプションの更新（Online Subscription Update）] タブをクリックします。

ステップ 4 [フィードサービス接続のテスト（Test Feed Service Connection）] ボタンをクリックして、Cisco フィード サービスへの接続があり、証明書が有効であることを確認します。

ステップ 5 [オンライン サブスクリプション更新の有効化（Enable Online Subscription Update）] チェック ボックスをオンにします。

ステップ 6 HH:MM形式で時刻（Cisco ISE サーバーのローカル タイム ゾーン）を入力します。デフォルトでは、Cisco ISE フィード サービスは毎日午前 1 時にスケジュールされます。

ステップ 7 [ダウンロードが行われたら管理者に通知（Notify administrator when download occurs）] チェック ボックスをオンにして、[管理者の電子メール アドレス（Administrator email address）] テキスト ボックスに電子メール アドレスを入力します。Cisco ISE が非機密情報（今後のリリースでよりよいサービスと追加機能を提供するために使用される）を収集することを許可する場合、[プロファイリング精度を上げるために Cisco 匿名情報を提供する（Provide Cisco anonymous information to help improve profiling accuracy）] チェック ボックスをオンにします。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 [今すぐ更新（Update Now）] をクリックします。

最後のフィードサービス更新以降に作成された新規および更新されたプロファイルをチェックするために Cisco フィード サーバーに連絡するように Cisco ISE に指示します。これによりシステム内のすべてのエンドポイントが再プロファイリングされ、システム負荷が増加する可能性があります。エンドポイント プロファイリング ポリシーの更新のため、現在 Cisco ISE に接続している一部のエンドポイントの許可ポリシーが変更される場合があります。

最後のフィード サービス以降に作成された新規および更新されたプロファイルを更新すると [今すぐ更新（Update Now）] ボタンは無効になり、ダウンロードの完了後にのみ有効になります。[プロファイラ フィード サービス設定（Profiler Feed Service Configuration）] ウィンドウから別の場所に移動し、このウィンドウに戻る必要があります。

関連トピック

オフラインでのプロファイラ フィード サービスの設定 （280 ページ）

オフラインでのプロファイラ フィード サービスの設定

Cisco ISE と Cisco フィード サーバーが直接接続されていないときに、フィード サービスをオフラインで更新できます。Cisco フィード サーバーからオフライン更新プログラム パッケージをダウンロードし、Cisco ISE にオフライン フィード更新プログラムを使用してアップロードできます。またフィードサーバーに追加される新しいポリシーに関する電子メール通知を設定することもできます。

オフラインでのプロファイラ フィード サービス設定には、次のタスクが含まれます。

1. オフライン更新プログラム パッケージのダウンロード
2. オフライン フィード更新の適用

オフライン更新プログラム パッケージのダウンロード

ステップ 1 **[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [フィード（Feeds）]** の順に選択します。
[管理（Administration）] > [フィードサービス（FeedService）] > [プロファイラ（Profiler）] ページでこのオプションにアクセスすることもできます。

ステップ 2 [オフライン手動更新（Offline Manual Update）] タブをクリックします。

ステップ 3 [更新されているプロファイル ポリシーのダウンロード（Download Updated Profile Policies）] リンクをクリックします。フィード サービス パートナー ポータルにリダイレクトされます。
また、ブラウザから https://ise.cisco.com/partner/ にアクセスして、フィード サービス パートナー ポータルに直接アクセスすることもできます。

ステップ 4 初めてのユーザーは、各種条件および契約に同意します。
要求を承認するフィードサービス管理者に電子メールが送信されます。承認されると、確認用の電子メールが届きます

ステップ 5 Cisco.com のクレデンシャルを使用してパートナー ポータルにログインします。

ステップ 6 [オフライン フィード（Offline Feed）] > [パッケージのダウンロード（Download Package）] の順に選択します。

ステップ 7 [パッケージの生成（Generate Package）] をクリックします。

ステップ 8 [オフライン 更新プログラム パッケージの内容を表示するにはクリックしてください（Click to View the Offline Update Package contents）] リンクをクリックして、生成したパッケージに含まれるすべてのプロファイルと OUI を表示します。

- [フィード プロファイラ 1（Feed Profiler 1）] と [フィード OUI（Feed OUI）] の下のポリシーは Cisco ISE の全バージョンにダウンロードされます。
- [フィード プロファイラ 2（Feed Profiler 2）] の下のポリシーは Cisco ISE リリース 1.3 以降のみにダウンロードされます。
- [フィード プロファイラ 3（Feed Profiler 2）] の下のポリシーは Cisco ISE リリース 2.1 以降のみにダウンロードされます。

ステップ 9 [パッケージのダウンロード（Download Package）] をクリックして、ローカル システムにファイルを保存します。
保存したファイルを Cisco ISE サーバーにアップロードして、ダウンロードしたパッケージのフィード更新プログラムを適用できます。

オフライン フィード更新の適用

始める前に

フィード更新を適用する前に、オフライン更新プログラム パッケージをダウンロードしている必要があります。

ステップ 1 **[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [フィード（Feeds）]** を選択します。
[管理（Administration）] > [フィードサービス（FeedService）] > [プロファイラ（Profiler）] ウィンドウでこのオプションにアクセスすることもできます。

ステップ 2 [オフライン手動更新（Offline Manual Update）] タブをクリックします。

ステップ 3 [参照（Browse）] をクリックして、ダウンロードしたプロファイラ フィード パッケージを選択します。

ステップ 4 [更新の適用（Apply Update）] をクリックします。

プロファイルと OUI の更新に関する電子メール通知の設定

プロファイルと OUI の更新通知を受信する電子メール アドレスを設定できます。

ステップ 1 オフライン更新プログラム パッケージのダウンロードセクションの手順 1 ～ 5 を実行し、フィード サービス パートナー ポータルに移動します。

ステップ 2 [オフライン フィード（Offline Feed）] > [電子メール設定（Email Preferences）] を選択します。

ステップ 3 通知を受信するには、[通知の有効化（Enable Notifications）] チェック ボックスをオンにします。

ステップ 4 新しい更新通知を受信する頻度を設定するには、[日数（days）] ドロップダウン リストから日数を選択します。

ステップ 5 電子メール アドレスまたはアドレスを入力し、[保存（Save）] をクリックします。

フィード更新の取り消し

前回の更新で更新されたエンドポイント プロファイリング ポリシーに戻り、プロファイラ フィード サービスの前回の更新により新しく追加されたが、エンドポイント プロファイリング ポリシーおよび OUI を削除できます。

エンドポイント プロファイリング ポリシーは、フィード サーバーからの更新後に変更された場合、システムで変更されません。

ステップ 1 **[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [フィード（Feeds）]** を選択します。

ステップ 2 変更設定監査レポートで設定変更を表示する場合は、[更新レポート ページに移動（Go to Update Report Page）] をクリックします。

ステップ 3 [最新を元に戻す（Undo Latest）] をクリックします。

プロファイラ レポート

Cisco ISE には、エンドポイント プロファイリングに関するさまざまなレポートと、ネットワークの管理に使用できるトラブルシューティング ツールが用意されています。現在のデータに加えて履歴のレポートを生成できます。レポートの一部をドリルダウンして詳細を表示できます。大規模なレポートの場合、レポートをスケジュールし、さまざまな形式でダウンロードすることもできます。

[操作（Operations）] > [レポート（Reports）] > [エンドポイントとユーザー（Endpoints and Users）] からエンドポイントに関する次のレポートを実行できます。

- エンドポイント セッション履歴
- プロファイリングされたエンドポイントの概要
- エンドポイント プロファイルの変更
- エンドポイントによる上位承認
- 登録済みエンドポイント

エンドポイントの異常な動作の検出

Cisco ISE により、不正な MAC アドレスの使用からネットワークが保護されます。Cisco ISE は MAC アドレススプーフィングに関与しているエンドポイントを検出し、疑わしいエンドポイントの権限を制限できます。

プロファイラ設定ページには、異常な動作に関する次の 2 つのオプションがあります。

- 異常な動作の検出を有効にする（Enable Anomalous Behavior Detection）
- 異常な動作の適用を有効にする（Enable Anomalous Behavior Enforcement）

異常な動作の検出を有効にすると、Cisco ISE はデータを調査し、NAS ポート タイプ、DHCP クラス ID、およびエンドポイント ポリシーに関連する属性の変更について、既存のデータとの矛盾がないかどうかを確認します。該当する場合、**AnomalousBehavior** 属性が True に設定され、エンドポイントに追加されます。これは、[可視性のコンテキスト（Visibility Context）] ページでエンドポイントをフィルタリングおよび表示する際に役立ちます。該当する MAC アドレスの監査ログも生成されます。

異常な動作の検出を有効にすると、Cisco ISE は、既存のエンドポイントの次の属性が変更されたかどうかを検査します。

1. ポートタイプ—エンドポイントのアクセス方式が変更されたかどうかを判断します。これは、有線 Dot1x 経由で接続したものと同じ MAC アドレスがワイヤレス Dot1x にも使用されていた場合（およびその逆の場合）に適用されます。
2. DHCP クラス ID—エンドポイントのクライアントまたはベンダーのタイプが変更されたかどうかを判断します。これは、DHCP クラス ID 属性に特定の値が入力された後で別の値に変更された場合にのみ当てはまります。エンドポイントが静的 IP アドレスで構成されている場合、Cisco ISE での DHCP クラス ID 属性は空です。後で別のデバイスがこのエンドポイントの MAC アドレスをスプーフィングして DHCP を使用すると、クラス ID が空の値から特定の文字列に変更されます。これによって異常な動作の検出がトリガーされることはありません。
3. エンドポイント ポリシー—重要なプロファイル変更があったかどうかを判断します。これは、エンドポイントのプロファイルが [電話（Phone）] または [プリンタ（Printer）] から [ワークステーション（Workstation）] に変更されたときに適用されます。

[異常な動作の適用（Anomalous Behavior Enforcement）] を有効にすると、異常な動作が検出された時点で CoA が発行されます。これは、[プロファイラ設定（Profiler Configuration）] ウィンドウで設定した許可ルールに基づいて、疑わしいエンドポイントを再許可するために使用できます。

異常な動作が発生しているエンドポイントに関する許可ポリシールールの設定

異常な動作が発生しているエンドポイントに対して実行するアクションを選択するには、[許可ポリシー（Authorization Policy）] ページで対応するルールを設定します。

ステップ 1 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択します。

ステップ 2 デフォルト ポリシーに対応する [表示（View）] 列から矢印アイコン をクリックすると、[設定（Set）] ビュー画面が開き、デフォルト許可ポリシーを表示および管理できます。

ステップ 3 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、ドロップダウン リストから、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ルールを挿入します。
[ポリシー セット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 4 [ルール名（Rule Name）] に入力します。

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性を選択します（たとえば、Endpoints.AnomalousBehaviorEqualsTrue）。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップすることもできます。

ステップ 7 [使用（Use）] をクリックして、異常な動作を伴うエンドポイントの許可ポリシー ルールを設定します。

ステップ 8 [完了（Done）] をクリックします。

異常な動作が発生しているエンドポイントの表示

次のいずれかのオプションを使用して、異常な動作が発生しているエンドポイントを表示できます。

- [ホーム（Home）] > [概要（Summary）] > [メトリック（Metrics）] から [異常な動作（Anomalous Behavior）] をクリックします。この操作により、ウィンドウ下部のペインに [異常な動作（Anomalous Behavior）] 列がある新しいタブが表示されます。
- [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [エンドポイントの分類（Endpoint Classification）] を選択します。ウィンドウ下部のペインで [異常な動作（Anomalous Behavior）] 列を表示できます。
- 次の手順で説明するように、[コンテキストの可視性（Context Visibility）] ウィンドウの [認証（Authentication）] ビューまたは [侵害されたエンドポイント（Compromised Endpoints）] ビューで新しい [異常な動作（Anomalous Behavior）] 列を作成できます。

ステップ 1 [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [認証（Authentication）] または [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [侵害されたエンドポイント（Compromised Endpoints）] を選択します。

ステップ 2 ウィンドウ下部のペインにある [設定（Settings）] アイコンをクリックし、[異常な動作（ Anomalous Behavior）] チェックボックスをオンにします。

ステップ 3 [移動（Go）] をクリックします。
[認証（Authentication）] ビューまたは [侵害されたエンドポイント（Compromised Endpoints）] ビューで [異常な動作（Anomalous Behavior）] 列を表示できます。

クライアントマシン上のエージェントのダウンロードの問題

問題

ユーザーの認証と許可の後、クライアント マシン ブラウザに「ポリシーが一致しません（no policy matched）」のエラー メッセージが表示されます。この問題は、認証のクライアント プロビジョニング フェーズ中のユーザー セッションに該当します。

考えられる原因

クライアント プロビジョニング ポリシーに必要な設定が欠落している可能性があります。

ポスチャ エージェントのダウンロードの問題

ポスチャ エージェントのインストーラをダウンロードするには、次のものが必要があることに注意してください。

- エージェントを初めてクライアントマシンにインストールする場合、ユーザーはブラウザセッションでActiveXインストーラを許可する必要がありますクライアントプロビジョニング ダウンロード ページで、この情報の指定を求められます。
- クライアント マシンには、インターネット アクセスが必要です。

解像度

- クライアント プロビジョニング ポリシーが Cisco ISE に存在することを確認します。存在する場合は、ポリシー内に定義されているポリシー ID グループ、条件およびエージェントのタイプを確認します。また、すべてのデフォルト値のプロファイルも含め、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）] > [NAC または AnyConnect ポスチャプロファイル（NAC or AnyConnect Posture Profile）]>[AnyConnect

ポスチャプロファイル（AnyConnect Posture Profile）] で設定されたエージェントプロファイルが存在するかどうかについても確認します。

- アクセス スイッチのポートをバウンスすることにより、クライアント マシンの再認証を試行します。

エンドポイント

これらのウィンドウでは、ネットワークに接続するエンドポイントを設定および管理することができます。

エンドポイント設定

表 *57:* エンドポイント設定

フィールド名	使用上のガイドライン
MAC アドレス	エンドポイントを静的に作成するには、MAC アドレスを 16 進数形式で入力します。 MAC アドレスは、Cisco ISE 対応のネットワークに接続するインターフェイスのデバイス ID です。
スタティック割り当て（Static Assignment）	[エンドポイント（Endpoints）] ウィンドウでエンドポイントを静的に作成する場合このチェックボックスをオンにすると、静的割り当てのステータスが static に設定されます。 エンドポイントのスタティック割り当てのステータスを静的から動的に、または動的から静的に切り替えできます。

フィールド名	使用上のガイドライン
ポリシー割り当て	（[スタティック割り当て（Static Assignment）] が選択されていない限り、デフォルトで無効）[ポリシー割り当て（Policy Assignment）] ドロップダウンリストから一致するエンドポイントポリシーを選択します。 次のいずれかを実行できます。 • 一致するエンドポイント ポリシーを選択しないで、デフォルトのエンドポイントポリシーである不明を使用する場合、スタティック割り当てステータスはエンドポイントに対して動的に設定され、それにより、エンドポイントの動的プロファイリングが可能になります。 • [不明（Unknown）] ではなく、一致するエンドポイントポリシーを選択する場合、スタティック割り当てのステータスはそのエンドポイントに対して静的に設定され、[スタティック割り当て（Static Assignment）] チェックボックスが自動的にオンになります。
スタティック グループ割り当て（**Static Group Assignment**）	エンドポイントをIDグループに静的に割り当てる場合はこのチェックボックスをオンにします。 このチェックボックスをオンにした場合、プロファイリング サービスは、前に他のエンドポイントIDグループに動的に割り当てられたエンドポイントの次のエンドポイントポリシーの評価時に、そのエンドポイントIDグループを変更しません。 このチェックボックスをオフにした場合、エンドポイントIDグループは、ポリシー設定に基づいてISEプロファイラにより割り当てられたダイナミック グループです。[スタティック グループ割り当て（Static Group Assignment）] オプションを選択しない場合、エンドポイントは、エンドポイント ポリシーの次回評価時に一致するIDグループに自動的に割り当てられます。

フィールド名	使用上のガイドライン

ID グループ割り当て	エンドポイントを割り当てるエンドポイント ID グループを選択します。
	
	エンドポイントを静的に作成する場合、またはエンドポイントのエンドポイントポリシーの評価時に [一致する ID グループの作成（Create Matching Identity Group）] オプションを使用しない場合は、エンドポイントを ID グループに割り当てることができます。
	
	Cisco ISE には、次のシステムによって作成された次のエンドポイント ID グループがあります。
	• [ブラックリスト（Blacklist）]
	• GuestEndpoints
	• プロファイル済み
	  • Cisco IP-Phone
	  • ワークステーション
	• RegisteredDevices
	• 不明

関連トピック

識別されたエンドポイント （271 ページ）

ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成 （265 ページ）

エンドポイントの LDAP からのインポートの設定

表 *58 :* エンドポイントの、*LDAP* からのインポートの設定

フィールド名	使用上のガイドライン
接続の設定	
Host	LDAP サーバーのホスト名または IP アドレスを入力します。

フィールド名	使用上のガイドライン
[ポート（Port）]	LDAP サーバーのポート番号を入力します。デフォルト ポート 389 を使用して LDAP サーバーからインポートするか、デフォルト ポート 636 を使用して SSL を介して LDAP サーバーからインポートできます。 （注） Cisco ISE では、任意の設定済みポート番号をサポートします。設定済みの値は、LDAP サーバー接続詳細に一致する必要があります。
セキュア接続を有効にする（Enable Secure Connection）	SSL を介して LDAP サーバーからインポートするには、[セキュア接続を有効にする（Enable Secure Connection）] チェックボックスをオンにします。
ルート CA 証明書名	ドロップダウン矢印をクリックして、信頼できる CA 証明書を表示します。 ルート CA 証明書名は、LDAP サーバーに接続する場合に必要となる信頼できる CA 証明書を指します。Cisco ISE 内の CA 証明書は、追加（インポート）、編集、削除、およびエクスポートが可能です。
匿名バインド（Anonymous Bind）	[匿名バインド（Anonymous Bind）] チェックボックスをオンにするか、または slapd.conf コンフィギュレーション ファイルの LDAP 管理者クレデンシャルを入力する必要があります。
管理者 DN（Admin DN）	slapd.conf コンフィギュレーション ファイルで LDAP 管理者に設定されている識別名（DN）を入力します。 管理者 DN フォーマット例：cn=Admin, dc=cisco.com, dc=com
パスワード	LDAP 管理者に設定されたパスワードを slapd.conf コンフィギュレーション ファイルに入力します。
ベース DN（Base DN）	親エントリの認定者名を入力します。 ベース DN フォーマット例：dc=cisco.com, dc=com
クエリ設定（Query Settings）	

フィールド名	使用上のガイドライン
MAC アドレス objectClass（MAC Address objectClass）	MACアドレスのインポートに使用されるクエリフィルタ（ieee802Device など）を入力します。
MAC アドレス属性名（MAC Address Attribute Name）	インポートに対して返される属性名（macAddress など）を入力します。
プロファイル属性名（Profile Attribute Name）	LDAP 属性の名前を入力します。この属性は、LDAP サーバーで定義されている各エンドポイント エントリのポリシー名を保持します。 [プロファイル属性名（Profile Attribute Name）] フィールドを設定する場合は、次の点を考慮してください。 • [プロファイル属性名（Profile Attribute Name）] フィールドでこの LDAP 属性を指定しない場合、またはこの属性を誤って設定した場合、インポート操作時にエンドポイントは [不明（Unknown）]としてマークされ、これらのエンドポイントは一致するエンドポイント プロファイリングポリシーに個別にプロファイリングされます。 • [プロファイル属性名（Profile Attribute Name）] フィールドで LDAP 属性を設定した場合、その属性値は、エンドポイントポリシーが Cisco ISE 内の既存のポリシーに一致することを確認するために検証され、エンドポイントがインポートされます。エンドポイント ポリシーが既存のポリシーと一致しない場合、それらのエンドポイントはインポートされません。
タイムアウト（Time Out）	この時間は秒数で入力します。有効な範囲は 1 ～ 60 秒です。

関連トピック

識別されたエンドポイント （271 ページ）
LDAP サーバーからのエンドポイントのインポート （270 ページ）

エンドポイント プロファイリング ポリシーの設定

表 *59 :* エンドポイント プロファイリング ポリシーの設定

フィールド名	使用上のガイドライン
名前（**Name**）	作成するエンドポイントプロファイリング ポリシーの名前を入力します。
説明（**Description**）	作成するエンドポイントプロファイリング ポリシーの説明を入力します。
ポリシー有効（**Policy Enabled**）	デフォルトでは [ポリシー有効（Policy Enabled）] チェックボックスはオンになっており、エンドポイントのプロファイリング時に、一致するプロファイリング ポリシーが関連付けられます。 オフになっている場合、エンドポイントのプロファイリング時に、エンドポイントプロファイリング ポリシーは除外されます。
最小確実度計数（**Minimum Certainty Factor**）	プロファイリング ポリシーに関連付ける最小値を入力します。デフォルト値は 10 です。
例外アクション（**Exception Action**）	プロファイリング ポリシー内のルールを定義するときに条件に関連付ける例外アクションを選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）] > [例外アクション（Exception Actions）] で定義されます。
ネットワーク スキャン（**NMAP**）アクション（**Network Scan (NMAP) Action**）	必要に応じて、プロファイリング ポリシー内のルールを定義するときに条件に関連付けるネットワーク スキャン アクションをリストから選択します。 デフォルトは [なし（NONE）] です。例外アクションは、[ポリシー（Policy）]>[ポリシー要素（Policy Elements）] > [結果（Results）] > [プロファイリング（Profiling）]>[ネットワークスキャン（NMAP）アクション（Network Scan (NMAP) Actions）] で定義されます。

フィールド名	使用上のガイドライン
ポリシーの ID グループの作成（**Create an Identity Group for the policy**）	エンドポイントIDグループを作成するには、次のオプションのいずれかをオンにします。 • はい、一致する ID グループを作成します（**Yes, create matching Identity Group**） • いいえ、既存の ID グループ階層を使用します（**No, use existing Identity Group hierarchy**）
はい、一致する ID グループを作成します（**Yes, create matching Identity Group**）	既存のプロファイリング ポリシーを使用する場合、このオプションを選択します。 このオプションは、これらのエンドポイントの一致するIDグループを作成します。エンドポイント プロファイルが既存のプロファイリング ポリシーと一致した場合に、IDグループは Profiled エンドポイント ID グループの子になります。 たとえば、ネットワーク上で検出されたエンドポイントが Xerox-Device プロファイルに一致する場合は、[エンドポイント ID グループ（Endpoint Identity Groups）] ページで Xerox-Device エンドポイント ID グループが作成されます。

フィールド名	使用上のガイドライン
いいえ、既存の ID グループ階層を使用します（**No, use existing Identity Group hierarchy**）	プロファイリング ポリシーおよび ID グループの階層構造を使用して、一致する親エンドポイント ID グループにエンドポイントを割り当てるには、このチェックボックスをオンにします。 このオプションを使用すると、エンドポイントプロファイリング ポリシー階層を利用することができ、エンドポイントはいずれかの一致する親エンドポイント ID グループ、さらに、親 ID グループに関連付けられたエンドポイント ID グループに割り当てられます。 たとえば、既存のプロファイルに一致するエンドポイントは、適切な親エンドポイント ID グループの下にグループ化されます。ここで、不明プロファイルに一致するエンドポイントは、[不明（Unknown）] の下にグループ化され、既存のプロファイルに一致するエンドポイントは、プロファイリングされたエンドポイント ID グループの下にグループ化されます。次の例を参考にしてください。 • エンドポイントが Cisco-IP-Phone プロファイルに一致する場合、これらのエンドポイントは Cisco-IP-Phone エンドポイント ID グループの下でグループ化されます。 • エンドポイントが Workstation プロファイルに一致する場合、これらのエンドポイントは、Workstation エンドポイント ID グループの下でグループ化されます。 Cisco-IP-Phone および Workstation エンドポイント ID グループは、システム内の Profiled エンドポイント ID グループに関連付けられます。
親ポリシー（**Parent Policy**）	新しいエンドポイントプロファイリング ポリシーを関連付ける、システムで定義されている親プロファイリングポリシーを選択します。 子にルールと条件を継承できる親プロファイリング ポリシーを選択できます。

フィールド名	使用上のガイドライン
関連 CoA タイプ（Associated CoA Type）	エンドポイントプロファイリングポリシーと関連付ける次のいずれかの CoA タイプを選択します。 • CoA なし（No CoA） • ポート バウンス • 再認証（Reauth） • [グローバル設定（Global Settings）] : [管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロファイリング（Profiling）] で設定されたプロファイラ設定から適用されます。
ルール（Rule）	エンドポイントプロファイリングポリシーで定義された 1 つ以上のルールにより、エンドポイントの一致するプロファイリングポリシーが決定されます。これにより、プロファイルに応じたエンドポイントのグループ化が可能になります。 ポリシー要素ライブラリからの 1 つ以上のプロファイリング条件がルールに使用され、エンドポイント属性およびその値が、全体的な分類用に検証されます。

フィールド名	使用上のガイドライン
条件（**Conditions**）	

フィールド名	使用上のガイドライン
	プラス（+）記号をクリックして、条件の固定オーバーレイを展開します。マイナス（-）記号をクリックするか、固定オーバーレイの外側をクリックして条件を閉じます。 [既存の条件をライブラリから選択（Select Existing Condition from Library）] または [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] をクリックします。 [既存の条件をライブラリから選択（Select Existing Condition from Library）]：ポリシー要素ライブラリからシスコによって事前定義された条件を選択して、式を定義できます。 [新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）]：さまざまなシステム辞書またはユーザー定義辞書から属性を選択して、式を定義できます。 プロファイリング条件と次のいずれかとを関連付けることができます。 • 各条件の確実度係数の整数値 • その条件の例外アクションまたはネットワーク スキャン アクション プロファイリング条件と関連付ける、次のいずれかの定義済み設定を選択します。 • [確実度計数が増加する（Certainty Factor Increases）]：各ルールの確実度値を入力します。この値は、全体的な分類に関するすべての一致ルールに対して追加されます。 • [例外の操作を行う（Take Exception Action）]：このエンドポイント プロファイリング ポリシーの [例外アクション（Exception Action）] フィールドで設定された例外アクションがトリガーされます。 • [ネットワークスキャンを行う（Take Network Scan Action）]：このエンドポイント プロファイリング ポリシーの [ネットワークスキャン（NMAP）アクション

フィールド名	使用上のガイドライン
	（Network Scan (NMAP) Action）] フィールドで設定されたネットワーク スキャン アクションがトリガーされます。

既存の条件をライブラリから選択（Select Existing Condition from Library）	次を実行できます。
	• ポリシー要素ライブラリに存在するシスコによって事前定義された条件を選択できます。AND または OR 演算子を使用して複数の条件を追加できます。
	• [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。
	  • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます
	  • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます
	  • [複製（Duplicate）]：選択した条件のコピーを作成します
	  • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます
	  • [削除（delete）]：選択した条件を削除します。

フィールド名	使用上のガイドライン

新しい条件の作成（高度なオプション）（**Create New Condition (Advance Option)**）	次を実行できます。
	• 式にアドホック属性/値の組み合わせを追加し、AND または OR 演算子を使用すると、複数の条件を追加できます。
	• [操作（Action）] アイコンをクリックして、後続のステップで次を実行します。
	  • [属性または値の追加（Add Attribute or Value）]：アドホック属性または値の組み合わせを追加できます
	  • [ライブラリから条件を追加（Add Condition from Library）]：シスコによって事前定義された条件を追加できます
	  • [複製（Duplicate）]：選択した条件のコピーを作成します
	  • [ライブラリに条件を追加（Add Condition to Library）]：作成したアドホック属性/値の組み合わせをポリシー要素ライブラリに保存できます
	  • [削除（delete）]：選択した条件を削除します。 AND または OR 演算子を使用できます

関連トピック

Cisco ISE プロファイリング サービス （195 ページ）
エンドポイント プロファイリング ポリシーの作成 （255 ページ）
UDID 属性を使用するエンドポイント コンテキストの可視性 （298 ページ）

UDID 属性を使用するエンドポイント コンテキストの可視性

固有識別子（UDID）は、特定のエンドポイントの MAC アドレスを識別するエンドポイント属性です。エンドポイントは複数の MAC アドレスを持つことがあります。たとえば、有線インターフェイスに 1 つ、ワイヤレスインターフェイス用にもう 1 つの MAC アドレスがある場合があります。AnyConnect エージェントはそのエンドポイントの UDID を生成し、それをエンドポイント属性として保存します。UDID は承認クエリ内に使用できます。エンドポイントの UDID は一定であり、AnyConnect のインストールまたはアンインストールに伴って変更されることはありません。UDID を使用すると、[コンテキストの可視性（Context Visibility）] ウィンドウ（[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] >

[コンプライアンス（Compliance）]）では、複数の NIC が装着されているエンドポイントの場合は複数のエントリではなく 1 つのエントリが表示されます。MAC アドレスではなく特定のエンドポイントに対してポスチャ制御を行うことができます。

（注） UDID を作成するには、エンドポイントの AnyConnect が 4.7 以上である必要があります。

IF-MIB

オブジェクト	OID
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

SNMPv2-MIB

オブジェクト	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

IP-MIB

オブジェクト	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToPhysicalPhysAddress	1.3.6.1.2.1.4.35.1.4

CISCO-CDP-MIB

オブジェクト	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17

オブジェクト	OID
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

CISCO-VTP-MIB

オブジェクト	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

CISCO-STACK-MIB

オブジェクト	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

BRIDGE-MIB

オブジェクト	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

OLD-CISCO-INTERFACE-MIB

オブジェクト	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

CISCO-LWAPP-AP-MIB

オブジェクト	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.2
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.1.9
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20

オブジェクト	OID
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

CISCO-LWAPP-DOT11-CLIENT-MIB

オブジェクト	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10

オブジェクト	OID
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

CISCO-AUTH-FRAMEWORK-MIB

オブジェクト	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

EEE8021-PAE-MIB: RFC IEEE 802.1X

オブジェクト	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

HOST-RESOURCES-MIB

オブジェクト	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

LLDP-MIB

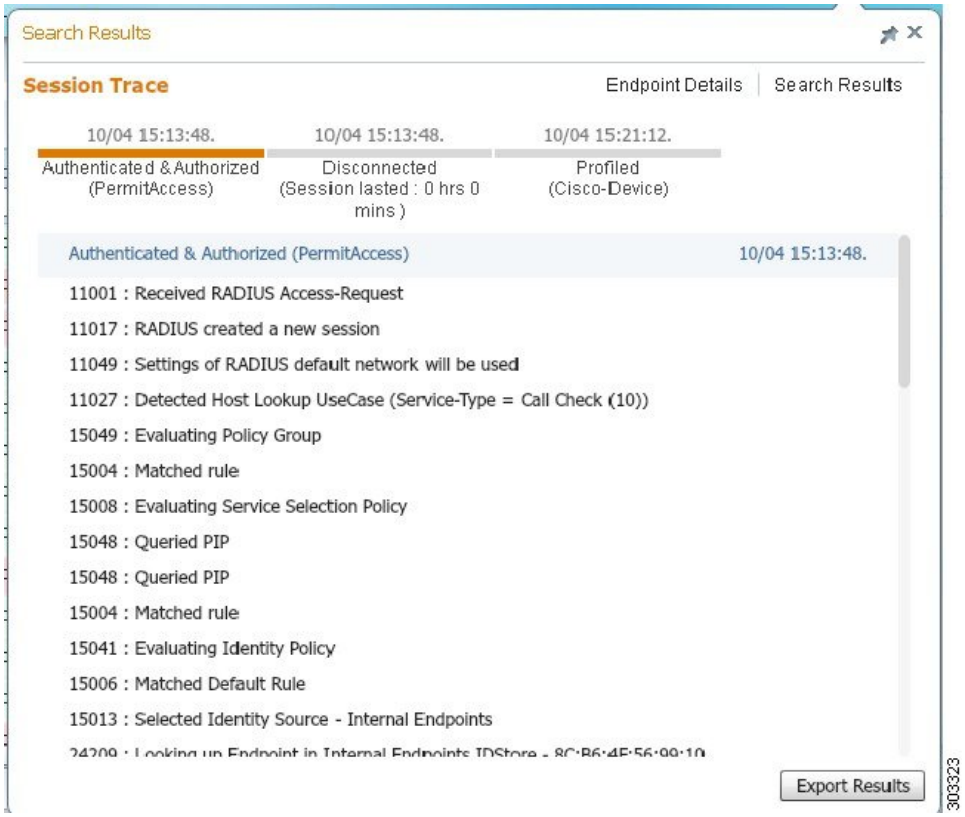
オブジェクト	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
ldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

エンドポイントのセッションのトレース

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用して、特定のエンドポイントのセッション情報を取得できます。基準に基づいて検索する場合は、エンドポイントのリストを取得します。エンドポイントのセッション トレース情報を表示するには、そのエンドポイントをクリックします。次の図に、エンドポイントに表示されるセッション トレース情報の例を示します。

（注） 検索に使用されるデータセットは、インデックスとしてのエンドポイントIDに基づいています。したがって、認証が行われる場合、検索結果セットにそれらを含めるには、認証にエンドポイントのエンドポイントIDが必要です。

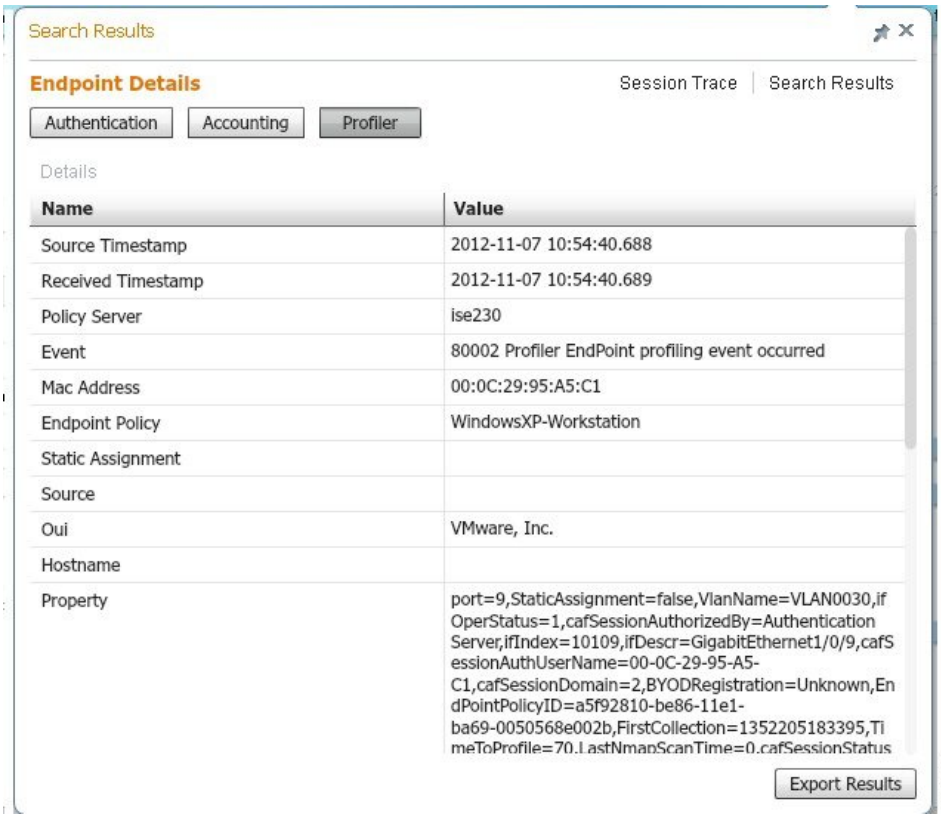
図 *19 :* エンドポイントのセッションのトレース



上部にあるクリック可能なタイムラインを使用すると、主な許可の遷移を確認できます。**[結果のエクスポート（Export Results）]** オプションを使用して、.csv 形式で結果をエクスポートすることもできます。レポートはブラウザにダウンロードされます。

特定のエンドポイントの認証、アカウンティング、およびプロファイラの詳細情報を表示するには、**[エンドポイントの詳細（Endpoint Details）]** リンクをクリックします。次の図に、エンドポイントに対して表示されたエンドポイントの詳細情報の例を示します。

図 *20 :* エンドポイントの詳細



ディレクトリからのセッションの削除

次のように、セッションが、モニターリングおよびトラブルシューティング ノード上のセッション ディレクトリから削除されます。

- 終了したセッションは、終了後 15 分で削除されます。
- 認証はあるがアカウンティングがない場合、このようなセッションは 1 時間後に削除されます。
- すべての非アクティブ セッションは 5 日後に消去されます。

エンドポイントのグローバル検索

Cisco ISE ホーム ページの上部にあるグローバル検索ボックスを使用して、エンドポイントを検索できます。次の条件を使用してエンドポイントを検索できます。

- ユーザー名（User name）
- MAC アドレス（MAC Address）

- IPアドレス（IP Address）
- 許可プロファイル
- エンドポイント プロファイル
- 失敗の理由
- ID グループ
- ID ストア
- ネットワーク デバイス名
- ネットワーク デバイス タイプ
- オペレーティング システム
- ポスチャ ステータス
- 参照先
- セキュリティ グループ（Security Group）
- ユーザー タイプ（User Type）

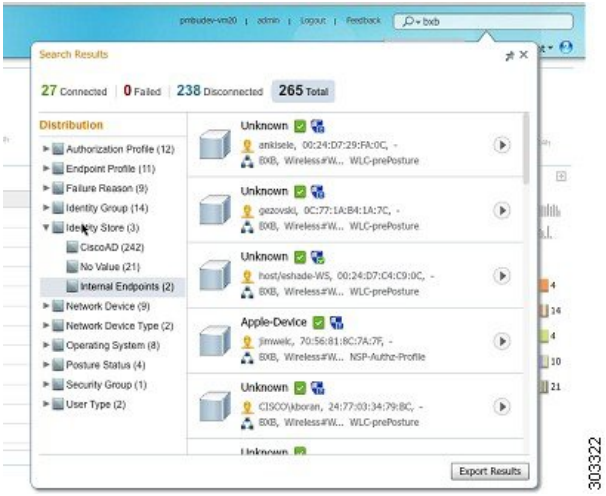
データを表示するには、[検索（Search）] フィールドに任意の検索条件の少なくとも 3 文字以上を入力する必要があります。

（注） エンドポイントが Cisco ISE によって認証された場合、またはそのアカウンティングの更新が受信された場合は、グローバル検索で確認できます。手動で追加され、Cisco ISE による認証または考慮がされていないエンドポイントは、検索結果に表示されません。

検索結果には、エンドポイントの現在のステータスに関する詳細および概要の情報が表示され、これをトラブルシューティングに使用することができます。検索結果には、上位 25 のエントリのみが表示されます。結果を絞り込むためにフィルタを使用できます。

次の図は、検索結果の例を示しています。

図 *21* : エンドポイントの検索結果



左パネルの任意のプロパティを使用して、結果をフィルタリングします。エンドポイントをクリックして、エンドポイントに関する次のような詳細情報を表示することもできます。

- セッションのトレース
- 認証の詳細
- アカウンティングの詳細
- ポスチャの詳細
- プロファイラの詳細
- クライアント プロビジョニングの詳細
- ゲスト アカウンティングおよびアクティビティ

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。