アイデンティティ ソース

アイデンティティ ソースは、ユーザ アカウントを定義するサーバおよびデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、Device Manager へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

ここでは、アイデンティティ ソースの定義方法について説明します。アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。

- アイデンティティ ソースについて （1 ページ）
- Active Directory（AD）アイデンティティ レルム （3 ページ）
- RADIUS サーバおよびグループ （10 ページ）
- Identity Services Engine（ISE） （16 ページ）
- SAMLサーバ （20 ページ）
- ローカル ユーザ （24 ページ）

アイデンティティ ソースについて

アイデンティティ ソースは、組織内のユーザのユーザ アカウントを定義する AAA サーバおよびデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、Device Manager へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

[オブジェクト（Objects）] > [アイデンティティ ソース（Identity Sources）] ページを使用して、ソースを作成および管理します。アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。

サポートされているアイデンティティ ソースとその使用方法は次のとおりです。

Active Directory（AD）アイデンティティ レルム

Active Directoryは、ユーザ アカウントおよび認証情報を提供します。Active Directory（AD）アイデンティティ レルム （3 ページ）を参照してください。

このソースは、次の目的で使用できます。

- リモートアクセスVPN（プライマリ アイデンティティ ソースとして）。ADはRADIUSサーバと組み合わせて使用できます。

- アイデンティティ ポリシー（アクティブ認証用、およびパッシブ認証で使用されるユーザ アイデンティティ ソースとして）。

AD（Active Directory）レルムシーケンス

AD レルムシーケンスは、AD レルムオブジェクトの番号付きリストです。レルムシーケンスは、ネットワーク内で複数の AD ドメインを管理する場合に役立ちます。AD レルムシーケンスの設定 （8 ページ）を参照してください。

このソースは、次の目的で使用できます。

- パッシブ認証で使用されるユーザ ID ソースとしての ID ポリシー。シーケンス内のレルムの順序によって、競合が発生しているまれな状況で、システムがユーザ ID を決定する方法が決まります。

Cisco Identity Services Engine（ISE）または Cisco Identity Services Engine Passive Identity Connector（ISE PIC）

ISE を使用している場合は、脅威に対する防御 デバイスと ISE 展開を統合できます。Identity Services Engine（ISE） （16 ページ）を参照してください。

このソースは、次の目的で使用できます。

- アイデンティティ ポリシー（ISE からユーザ アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

RADIUS サーバ、RADIUS サーバ グループ

RADIUS サーバーを使用している場合は、それらを Device Manager で使用することもできます。それぞれのサーバを個別のオブジェクトとして定義し、それらをサーバ グループ（特定グループ内のサーバは互いのコピー）に入れる必要があります。サーバ グループを機能に割り当て、個々のサーバは割り当てないでください。RADIUS サーバおよびグループ （10 ページ）を参照してください。

このソースは、次の目的で使用できます。

- 認証、および許可、アカウンティングのアイデンティティ ソースとしてのリモート アクセス VPN。ADはRADIUSサーバと組み合わせて使用できます。
- アイデンティティ ポリシー（リモート アクセス VPN ログインからユーザ アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。
- Device Manager または 脅威に対する防御 CLI 管理ユーザーの外部認証。許可レベルが異なる複数の管理ユーザをサポートできます。これらのユーザは、デバイスの設定とモニタリングのためにシステムにログインできます。

SAML サーバ

セキュリティ アサーション マークアップ言語 2.0（SAML 2.0）は、当事者間、特に ID プロバイダー（IdP）とサービスプロバイダー（SP）の間で認証および許可データを交換するためのオープン標準です。

このソースは、次の目的で使用できます。

- シングルサインオン（SSO）認証ソースとしてのリモートアクセス VPN。
- Device Manager ユーザーの外部認証。許可レベルが異なる複数の管理ユーザをサポートできます。これらのユーザは、デバイスの設定とモニタリングのためにシステムにログインできます。

LocalIdentitySource

これはローカル ユーザー データベースです。これには Device Manager で定義したユーザーが含まれます。このデータベースのユーザーアカウントを管理するには、**[オブジェクト（Objects）] > [ユーザー（Users）]** を選択します。ローカル ユーザ （24 ページ）を参照してください。

（注） ローカル アイデンティティ ソース データベースには、CLIアクセス用にCLIで設定するユーザは含まれません(**configure user add**コマンドを使用)。CLI ユーザーは、Device Manager で作成するユーザーとは完全に別のユーザーです。

このソースは、以下の目的で使用できます。

- リモート アクセス VPN（プライマリまたはフォールバック アイデンティティ ソースとして）。
- アイデンティティ ポリシー（リモート アクセス VPN ログインからユーザ アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

Active Directory（AD）アイデンティティ レルム

Microsoft Active Directory（AD）はユーザ アカウントを定義します。Active Directory ドメイン用に AD アイデンティティ レルムを作成できます。ここでは、AD アイデンティティ レルムの定義方法について説明します。

サポートされるディレクトリ サーバ

Windows Server 2012、2016、2019 で Microsoft Active Directory（AD）を使用できます。

サーバの構成については、次の点に注意してください。

- ユーザ グループまたはグループ内のユーザにユーザ制御を実施したい場合は、ディレクトリ サーバにおいてユーザ グループを設定する必要があります。サーバがオブジェクト階層でユーザを管理している場合、システムでユーザ グループ制御を実行できません。
- システムがサーバからユーザのメタデータを取得するには、ディレクトリ サーバで、次の表に示すフィールド名を使用する必要があります。

メタデータ	Active Directory フィールド
LDAP ユーザ名	samaccountname
名	givenname
姓	sn
電子メール アドレス	mail userprincipalname（mail に値が設定されていない場合）
department	department distinguishedname（department に値が設定されていない場合）
電話番号	telephonenumber

ユーザ数の制限

Device Manager はディレクトリサーバーから最大 50,000 人のユーザーに関する情報をダウンロードできます。

ディレクトリ サーバに 50,000 以上のユーザ アカウントが含まれる場合、アクセス ルールでユーザを選択するとき、またはユーザベースのダッシュボード情報を閲覧するときに、すべての可能な名前を確認することができません。ルールは、ダウンロードしたこれらの名前だけに書き込むことができます。

この制限は、グループに関連付けられた名前にも適用されます。グループに 50,000 を超えるメンバーが含まれている場合は、ダウンロードした 50,000 個の名前だけをグループメンバーシップと照合できます。

ディレクトリ ベース DN の決定

ディレクトリのプロパティを設定するときに、ユーザとグループに共通のベース識別名（DN）を指定する必要があります。ベースはディレクトリ サーバで定義され、ネットワークごとに異なります。アイデンティティ ポリシーが動作するためには、正しいベースを入力する必要があります。ベースが間違っている場合は、システムがユーザ名やグループ名を判別できないため、アイデンティティ ベースのポリシーが機能しません。

ヒント 正しいベースを取得するには、ディレクトリ サーバを担当する管理者に確認してください。

Active Directory の場合は、ドメイン管理者として Active Directory サーバにログインし、コマンドプロンプトで **dsquery** コマンドを次のように使用することで、正しいベースを判別できます。

ユーザ検索ベース

dsquery user コマンドを入力し、ベース識別名を調べる既知のユーザ名（一部または全部）を指定します。たとえば次のコマンドでは、部分名「John*」を使用して、「John」で始まるすべてのユーザに対する情報を返します。

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

ベース DN は「DC=csc-lab,DC=example,DC=com」となります。

グループ検索ベース

dsquery group コマンドを入力し、ベース識別名を調べたい既知のグループ名を指定します。たとえば次のコマンドでは、グループ名「Employees」を使用して識別名を返します。

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

グループのベース DN は「DC=csc-lab,DC=example,DC=com」となります。

また、ADSI Edit プログラムを使用して、Active Directory 構造を参照することもできます（**Start** > **Run** > **adsiedit.msc**）。ADSI Edit で、組織単位（OU）、グループ、ユーザなど任意のオブジェクトを右クリックし、[プロパティ（Properties）] を選択すると、識別名が表示されます。DC 値の文字列をベースとしてコピーできます。

ベースが正しいことを確認するには、次のように操作します。

1. ディレクトリ プロパティの [Test Connection] ボタンをクリックして、接続を確認します。問題を解決し、ディレクトリ プロパティを保存します。
2. デバイスに対する変更をコミットします。
3. アクセス ルールを作成して、[ユーザ（Users）] タブを選択し、ディレクトリから既知のユーザ名とグループ名の追加を試みます。ディレクトリが含まれるレルム内のユーザおよびグループに入力が一致すると、自動コンプリートによる候補が表示されます。これらの候補がドロップダウン リストに表示された場合、システムがディレクトリを正常にクエリーできたことが分かります。候補が表示されない場合は、該当する検索ベースを修正する必要があります。

AD アイデンティティ レルムの設定

アイデンティティ レルムとは、認証サービスを提供するのに必要なディレクトリ サーバおよび他の属性のことです。ディレクトリ サーバには、ネットワークへのアクセスが許可されているユーザおよびユーザ グループに関する情報が格納されます。

Active Directoryの場合、レルムはActive Directoryドメインに相当します。サポートする必要があるADドメインごとに個別のレルムを作成します。

レルムは次のポリシーで使用されます。

- [アイデンティティ（Identity）]：レルムはユーザ アイデンティティおよびグループ メンバーシップ情報を提供します。この情報をアクセス制御ルールで使用することができます。システムはすべてのユーザおよびグループに関する更新された情報を、毎日最後の1時間（UTC）にダウンロードします。ディレクトリ サーバに管理インターフェイスから到達できる必要があります。
- [リモート アクセス VPN（Remote access VPN）]：レルムは認証サービスを提供します。これにより、接続を許可するかどうかが決まります。ディレクトリサーバにRA VPN外部インターフェイスから到達できる必要があります。
- アクセス制御、SSL復号：レルム内のすべてのユーザにルールを適用するため、ユーザの基準でレルムを選択することができます。

ディレクトリ管理者と協力して、ディレクトリ サーバのプロパティを設定するために必要な値を取得してください。

（注） 接続されたネットワーク上にディレクトリ サーバが存在しない場合やデフォルト ルート経由で使用可能でない場合は、そのサーバのスタティック ルートを作成します。**[デバイス]**>**[ルーティング]** > **[設定の表示]**の順に選択して、スタティックルートを作成します。 または、サーバを定義するときに適切なインターフェイスを選択します。

次の手順では、[オブジェクト（Objects）]ページからオブジェクトを直接作成および編集する方法を説明します。レルム プロパティの編集時に、オブジェクト リストに表示される [新しいアイデンティティ レルムの作成（Create New Identity Realm）] リンクをクリックして、アイデンティティ レルムを作成することもできます。

始める前に

ディレクトリサーバー、Threat Defense デバイス、およびクライアント間で、時刻設定が一致していることを確認します。これらのデバイス間で時刻にずれがあると、ユーザ認証が成功しない場合があります。「一致」とは、別のタイム ゾーンを使用できますが、たとえば、10 AM PST = 1 PM EST など、それらのゾーンに対して相対的に同じになっている必要があることを意味しています。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アイデンティティ レルム（Identity Realm）][アイデンティティ ソース（Identity Sources）] を選択します。

ステップ 2 次のいずれかを実行します。

- AD レルムを作成するには、**[+]** > **[AD]** をクリックします。
- レルムを編集するには、そのレルムの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 基本レルムのプロパティを設定します。

- [名前（Name）]：ディレクトリ レルムの名前。
- [タイプ（Type）]：ディレクトリ サーバのタイプ。サポートされているタイプは Active Directory のみのため、このフィールドは変更できません。
- [ディレクトリユーザ名（Directory Username）]、[ディレクトリパスワード（Directory Password）]：取得するユーザ情報に対して適切な権限を持つユーザの識別用ユーザ名とパスワード。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

  （注）
  この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=administrator,cn=users,dc=example,dc=com と変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [ベースDN（Base DN）]：ユーザおよびグループ情報、つまり、ユーザとグループの共通の親を検索またはクエリするためのディレクトリ ツリー。たとえば、cn=users,dc=example,dc=com となります。ベース DN の検索方法については、ディレクトリ ベース DN の決定 （4 ページ）を参照してください。
- [AD プライマリ ドメイン（AD Primary Domain）]：デバイスが参加する必要のある、完全修飾 Active Directory ドメイン名。たとえば、example.com のように指定します。

ステップ 4 ディレクトリ サーバのプロパティを設定します。

- [ホスト名/IP アドレス（Hostname/IP Address）]：ディレクトリ サーバのホスト名または IP アドレス。サーバに対して暗号化された接続を使用する場合、IP アドレスではなく、完全修飾ドメイン名を入力する必要があります。
- [インターフェイス]: ADサーバに到達するためのインターフェイス。インターフェイスを選択しない場合、データルーティングテーブルを使用して適切なインターフェイスが検索されます。管理専用インターフェイスを使用する場合は、そのインターフェイスを具体的に選択する必要があります。管理専用ルーティングテーブルからルートルックアップを使用することはできません。
- [ポート（Port）]：サーバとの通信に使用するポート番号。デフォルトは 389 です。LDAPS を暗号化方式に選択している場合は、ポート 636 を使用します。

- [暗号化（Encryption）]：ユーザとグループの情報をダウンロードするのに暗号化接続を使用する場合は、適切な方式を [STARTTLS] または [LDAPS] から選択します。デフォルトは [なし（None）] です。したがって、ユーザとグループ情報はクリア テキストでダウンロードされます。
  - [STARTTLS] は暗号化方式をネゴシエートし、ディレクトリ サーバでサポートされている最も強力な方式を使用します。ポート 389 を使用します。リモート アクセス VPN 用にレルムを使用する場合は、このオプションがサポートされません。
  - [LDAPS] では LDAP over SSL が必要です。ポート 636 を使用します。
- [信頼できる CA 証明書（Trusted CA Certificate）]：暗号化方式を選択した場合は、認証局（CA）証明書をアップロードして、システムとディレクトリ サーバの間で信頼できる接続を有効化します。認証に証明書を使用している場合、証明書のサーバ名とサーバのホスト名/IP アドレスが一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用するが、証明書では ad.example.com が指定されている場合、接続が失敗します。

ステップ 5 レルムの複数のサーバがある場合は、[別の設定の追加（Add Another Configuration）] をクリックし、追加サーバごとのプロパティを入力します。

最大 10 の AD サーバをレルムに追加できます。これらのサーバは互いの重複である必要があり、同じ AD ドメインをサポートする必要があります。

各サーバエントリは適宜折りたたんだり展開することができます。セクションには、ホスト名または IP アドレスとポートラベルが付けられます。

ステップ 6 システムがサーバと通信できるか確認するには、[テスト（Test）] ボタンをクリックします。

システムは別個のプロセスおよびインターフェイスを使用してサーバにアクセスします。このため、アイデンティティ ポリシーでは接続に成功してリモート アクセス VPN では失敗するなど、ある使用方法では接続が成功しても、別の方法では失敗したことを示すエラーが表示される場合があります。サーバにアクセスできない場合は、指定した IP アドレスとホスト名が正しく、DNS サーバにそのホスト名が入力されているかなどを確認します。サーバのスタティック ルートを設定する必要が生じることもあります。詳細については、ディレクトリ サーバ接続のトラブルシューティング （9 ページ）を参照してください。

ステップ 7 **[OK]** をクリックします。

AD レルムシーケンスの設定

パッシブ ID ルールで AD レルムシーケンスを使用すると、システムが複数の AD サーバでユーザの照合を試みることができるようになります。レルムシーケンスで、各 AD サーバが別個のレルムまたはドメイン（engineering.example.com や marketing.example.com など）を管理する AD レルムの番号付きリストを設定します。

レルムシーケンスは、複数の AD ドメインをサポートしていて、異なるドメインのユーザーが Threat Defense デバイスを介してトラフィックを送信する可能性がある場合にのみ役立ちます。

レルムは、受動的に認証されるユーザセッションの ID を検索するために使用されます。レルムの順序は、まれに競合が発生した場合に、ID の競合を解決するために使用されます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アイデンティティソース（Identity Sources）] を選択します。

ステップ 2 次のいずれかを実行します。

- AD レルムシーケンスを作成するには、**[+]**>**[AD レルムシーケンス（AD Realm Sequence）]** をクリックします。
- AD レルムシーケンスを編集するには、オブジェクトの編集アイコン（）をクリックします。

オブジェクトを削除するには、そのオブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 レルムシーケンスのプロパティを設定します。

- [Name]：オブジェクトの名前。
- [説明（Description）]：（任意）オブジェクトの説明。
- [AD レルム（AD Realms）]：[+] をクリックして、AD レルムオブジェクトをシーケンスに追加します。レルムを追加したら、目的の順序になるように、レルムをクリックしてドラッグアンドドロップします。

ステップ 4 [OK] をクリックします。

パッシブ ID ルールで AD レルムシーケンスを選択できるようになりました。

ディレクトリ サーバ接続のトラブルシューティング

システムは、機能に応じてディレクトリ サーバとの通信に異なるプロセスを使用します。そのため、アイデンティティ ポリシー用の接続は機能しますが、リモート アクセス VPN 用の接続は失敗します。

これらのプロセスでは、さまざまなインターフェイスを使用してディレクトリ サーバと通信します。次のインターフェイスからの接続を確認する必要があります。

- 管理インターフェイス（アイデンティティ ポリシーの場合）
- データ インターフェイス（リモート アクセス VPN（外部インターフェイス）の場合）

アイデンティティ レルムを設定する場合、[テスト（Test）] ボタンを使用して接続が機能することを確認します。エラー メッセージは、接続に問題のある機能を示す必要があります。次

に、認証属性およびルーティング/インターフェイス設定に基づいて、発生する可能性がある一般的な問題を示します。

ディレクトリユーザの認証の問題。

問題が、ユーザ名またはパスワードのため、ディレクトリ サーバにログインできなかったということである場合、名前とパスワードが正しく、ディレクトリ サーバで有効なことを確認します。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

また、システムは、ユーザ名とパスワードの情報から ldap-login-dn と ldap-login-password を生成します。たとえば、Administrator@example.com は cn=administrator,cn=users,dc=example,dc=com と変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

ディレクトリ サーバは、データ インターフェイスを介してアクセス可能です。

ディレクトリ サーバが、データ インターフェイスに直接接続されているネットワーク上にある（ギガビット イーサネット インターフェイスなど）か、直接接続されているネットワークからルーティング可能であるネットワーク上にある場合は、仮想管理インターフェイスとディレクトリ サーバ間のルートがあることを確認する必要があります。

- **data-interfaces** を管理ゲートウェイとして使用するには、ルーティングを成功させる必要があります。
- 管理インターフェイスに明示的なゲートウェイがある場合は、そのゲートウェイ ルータはディレクトリ サーバへのルートを持つ必要があります。
- 直接接続されているネットワークとディレクトリ サーバをホストするネットワーク間にルータがある場合は、ディレクトリ サーバのスタティック ルートを設定します（**[デバイス（Device）] > [ルーティング（Routing）]**）。
- データ インターフェイスの IP アドレスとサブネットマスクが正しいことを確認します。

ディレクトリ サーバは、外部ネットワーク上です。

ディレクトリ サーバが外部（アップリンク）インターフェイスの反対側のネットワーク上にある場合は、サイト間 VPN 接続を設定する必要があります。手順については、リモート アクセス VPN を使用した外部ネットワークでのディレクトリ サーバの使用法を参照してください。

RADIUS サーバおよびグループ

RADIUS サーバーを使用して、リモートアクセス VPN 接続、および Device Manager と脅威に対する防御 CLI 管理ユーザーの認証および認可を行うことができます。たとえば、Cisco Identity

Services Engine（ISE）とその RADIUS サーバーも使用する場合は、Device Manager でそのサーバーを使用できます。

RADIUS サーバを使用するように機能を設定する場合は、個別のサーバではなく RADIUS グループを選択します。RADIUS グループは、相互にコピーである RADIUS サーバの集合です。グループに複数のサーバがある場合は、それらは、1 つのサーバが使用できなくなった場合に冗長性を提供する一連のバックアップ サーバを形成します。ただし、サーバが 1 つしかない場合でも、機能の RADIUS サポートを設定するには、メンバーが 1 つのグループを作成する必要があります。

ここでは、サポートされている機能で使用できるように RADIUS サーバおよびグループを設定する方法について説明します。

RADIUS サーバの設定

RADIUSサーバは、AAA(認証、認可、アカウンティング)サービスを提供します。RADIUS サーバーを使用してユーザーを認証および認可すると、これらのサーバーを Device Manager と一緒に使用できます。

RADIUS サーバごとにオブジェクトを作成した後、重複サーバの各グループを含む RADIUS サーバ グループを作成します。

始める前に

RA VPN のリダイレクト ACL を設定する場合は、スマート CLI を使用して、サーバ オブジェクトを作成または編集する前に拡張 ACL を作成する必要があります。オブジェクトの編集中に ACL を作成することはできません。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アイデンティティ ソース（Identity Sources）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、**[+]** > **[RADIUSサーバ（RADIUS Server）]** をクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 次のプロパティを設定します。

- [Name]：オブジェクトの名前。 サーバで設定されているものと一致している必要はありません。

- [サーバ名またはIPアドレス（Server Name or IP Address）]：サーバの完全修飾ホスト名（FQDN）または IP アドレス。たとえば、radius.example.com または 10.100.10.10 などです。
- [認証ポート（Authentication Port）]：RADIUS 認証および認可が実行されるポート。デフォルトは 1812 です。
- [タイムアウト（Timeout）]：次のサーバに要求を送信する前にサーバからの応答を待機する時間の長さ（1～300秒）。デフォルトは 10 秒です。認証トークンの入力を求めるなどのために、このサーバをリモート アクセス VPN のセカンダリ認証ソースとして使用している場合は、このタイムアウトを少なくとも 60 秒に増やします。この間に、ユーザはトークンを取得して入力できます。
- [サーバ秘密キー（Server Secret Key）]：（任意）脅威に対する防御 デバイスと RADIUS サーバ間でデータを暗号化するために使用される共有秘密キー。キーは、大文字と小文字が区別される最大 64 文字の英数字文字列です。スペースは使用できません。キーは、英数字またはアンダースコアで開始する必要があります。次の特殊文字を含めることができます：$ & - _ .+ @。+ @ を使用できます。文字列は、RADIUS サーバで設定された文字列と一致している必要があります。秘密キーを設定していない場合、接続は暗号化されません。
- **RADIUS 応答にはメッセージオーセンティケータが必要です**：Message-Authenticator 属性は、Blast- RADIUS 攻撃を防ぐために使用されます。メッセージ オーセンティケータをサポートするようにRADIUS サーバーをアップグレードした場合は、このオプションを有効にして、Blast- RADIUS 攻撃を防御できます。有効にする場合は、すべての要求と応答にメッセージオーセンティケータが含まれている必要があります。含まれていなければ認証に失敗します。

ステップ 4 （オプション）リモートアクセスVPNの認可変更設定のためにサーバを使用している場合は、[RA VPNのみ（RA VPN Only）] リンクをクリックし、次のオプションを設定できます。

- [ACLのリダイレクト（Redirect ACL）]：RA VPN リダイレクト ACL を使用する拡張 ACL を選択します。**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** ページのスマート CLI 拡張アクセスリストオブジェクトを使用して、拡張 ACL を作成します。

  リダイレクト ACL の目的は、Cisco Identity Services Engine（ISE）がクライアントポスチャを評価できるように、初期トラフィックを ISE に送信することです。ACLはISEにHTTPSトラフィックを送信しますが、ISE宛てのトラフィックや、名前解決のためにDNSサーバに送信されるトラフィックは送信しません。例については、Threat Defense デバイスでの認可変更の設定を参照してください。
- [RADIUSサーバに接続するために使用されるインターフェイス（Interface Used to Connect to RADIUS Server）]：サーバと通信するときに使用するインターフェイス。[ルートルックアップ経由で解決する]を選択した場合、システムは常にデータルーティングテーブルを使用して、使用するインターフェイスを決定します。[インターフェイスの手動選択]を選択した場合、システムは常に選択したインターフェイスを使用します。管理専用インター

フェイスを使用する場合は、具体的に選択する必要があります。管理専用ルーティングテーブルにルートルックアップを使用することはできません。

認可変更を設定している場合、システムがインターフェイスでCoAリスナーを適切に有効化できるように、特定のインターフェイスを選択する必要があります。

Device Manager 管理アクセスにもこのサーバーを使用する場合、このインターフェイスは無視されます。管理アクセスの試行は、常に管理 IP アドレスを介して認証されます。

ステップ 5 （任意。オブジェクトを編集する場合のみ）[テスト（Test）]をクリックして、システムがサーバに接続できるかどうか確認します。

ユーザ名とパスワードの入力を求められます。テストでは、サーバを接続できるかどうか、接続できる場合はユーザ名が認証されるかどうかを確認します。

ステップ 6 **[OK]** をクリックします。

RADIUS サーバ グループの設定

RADIUS サーバ グループには、1 つまたは複数の RADIUS サーバ オブジェクトが含まれています。グループ内のサーバは、相互にコピーされる必要があります。これらのサーバはバックアップ サーバのチェーンを形成します。そのため、最初のサーバが利用できなくなると、システムはリスト上の次のサーバを試すことができます。

機能に RADIUS サポートを設定する場合、サーバ グループを選択する必要があります。したがって、RADIUS サーバが 1 台しかなくても、それを含むサーバ グループを作成する必要があります。

始める前に

グループに追加するすべてのサーバーには、**[すべての RADIUS 応答にメッセージ認証を要求（Require Message-Authenticator for all RADIUS Responses）]**の設定が同じである必要があります（有効か無効かのいずれか）。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アイデンティティ ソース（Identity Sources）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、**[+]** > **[RADIUSサーバグループ（RADIUS Server Group）]** をクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（ ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 次のプロパティを設定します。

- [Name]：オブジェクトの名前。 サーバで設定されているものと一致している必要はありません。
- [デッドタイム（Dead Time）]：失敗したサーバは、すべてのサーバが失敗した後にのみ再アクティブ化されます。デッドタイムは、最後のサーバが失敗した後にすべてのサーバを再アクティブ化するまで待機する時間の長さ(0～1440分)です。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。デフォルトは 10 分です。
- [最大失敗試行回数]:次のサーバを試行する前に、グループ内のRADIUSサーバに送信されたAAAトランザクションの失敗数(応答がなかった要求の数)。1 ～ 5 を指定できます。デフォルトは3 です。最大失敗試行数を超えると、システムはサーバを故障としてマークします。

  特定の機能について、ローカルデータベースを使用するフォールバック方式を設定していて、グループ内のすべてのサーバが応答に失敗した場合、グループは非応答と見なされ、フォールバック方式が試行されます。サーバ グループはデッド タイムの間非応答とマークされたままになるため、その期間内に追加の AAA 要求でサーバ グループへの接続は試行されず、フォールバック方式がすぐに使用されます。
- ダイナミック認証（RA VPNの場合のみ）、ポート：RADIUS サーバ グループ向けの RADIUS ダイナミック認証または認可変更（CoA）サービスを有効にすると、グループは CoA 通知用に登録され、Cisco Identity Services Engine（ISE）からの指定した CoA ポリシー更新用ポートをリッスンします。デフォルトのリスニングポートは 1700 ですが、1024 ～ 65535 の範囲で別のポートを指定することができます。このサーバ グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ、ダイナミック認証をイネーブルにします。
- [RADIUSサーバをサポートするレルム（Realm that Supports the RADIUS Server）]：AD サーバを使用してユーザを認証するように RADIUS サーバが設定されている場合は、この RADIUS サーバと組み合わせて使用される AD サーバを指定する AD レルムを選択します。レルムが存在していない場合は、リストの下部にある [新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックして作成します。
- [RADIUSサーバリスト（RADIUS Server list）]：グループのサーバを定義する RADIUS サーバ オブジェクトを最大 16 個選択します。優先順にこれらのオブジェクトを追加します。リストの最初のサーバが、非応答になるまで使用されます。オブジェクトを追加した後に、ドラッグ アンド ドロップで並び替えることができます。必要なオブジェクトがまだない場合は、[新規RADIUSサーバの作成（Create New RADIUS Server）] をクリックしてすぐに追加します。

  [テスト（Test）] リンクをクリックして、システムがサーバに接続できることを確認することもできます。ユーザ名とパスワードの入力を求められます。テストでは、サーバを接続できるかどうか、接続できる場合はユーザ名が認証されるかどうかを確認します。

ステップ 4 （オプション）[すべてのサーバをテスト（Test All Servers）] ボタンをクリックして、グループ内の各サーバへの接続を確認します。

ユーザ名とパスワードの入力を求められます。システムは、各サーバを接続できるかどうか、各サーバでユーザ名が認証されるかどうかを確認します。

ステップ 5 **[OK]** をクリックします。

RADIUS サーバおよびグループのトラブルシューティング

次に、外部認証が機能しない場合に確認する項目を示します。

- RADIUS サーバの [テスト（Test）] ボタンとサーバ グループ オブジェクトを使用して、デバイスからサーバに通信できることを確認します。テストする前に、必ずオブジェクトを保存してください。テストが失敗した場合：
  - テストは、サーバに設定されたインターフェイスを無視し、常に管理インターフェイスを使用することを理解しておいてください。RADIUS 認証プロキシが管理 IP アドレスからの要求に応答するように設定されていない場合、テストは失敗することが予想されます。
  - テスト中に正しいユーザ名/パスワードの組み合わせを入力していることを確認します。正しくない場合は、クレデンシャルが不正であるというメッセージが表示されます。
  - 秘密キー、ポート、およびサーバの IP アドレスを確認します。ホスト名を使用している場合は、DNS が管理インターフェイス用に設定されていることを確認します。秘密キーがデバイス設定ではなく RADIUS サーバで変更された可能性を考えます。
  - テストが引き続き失敗する場合は、RADIUS サーバへのスタティック ルートを設定する必要があります。CLI コンソールまたは SSH セッションからサーバに ping を試行して、到達できるかどうか確認します。
- 外部認証が機能していたのに機能しなくなった場合は、すべてのサーバがデッドタイムになっている可能性を考えます。ローカル認証へのフォールバックを設定する場合、グループ内のすべての RADIUS サーバーが失敗したときに、システムが最初のサーバーを再試行する前に待機する時間（分単位）がデッドタイムです。デッドタイム中は、ローカル認証が使用されるため、指定したユーザーのユーザー名とパスワードがローカルのユーザー名/パスワードになります。デフォルトは 10 分ですが、1440 分までの範囲で設定できます。
- HTTPS 外部認証が一部のユーザでしか機能しない場合は、各ユーザアカウントの RADIUS サーバで定義されている cisco-av-pair 属性を評価します。この属性の設定が正しくない可能性があります。属性が欠落しているか不正であると、そのユーザアカウントのすべての HTTS アクセスがブロックされます。
- SSH 外部認証が一部のユーザでしか機能しない場合は、各ユーザ アカウントの RADIUS サーバで定義されている Service-Type 属性を評価します。この属性の設定が正しくない可

能性があります。属性が欠落しているか不正であると、そのユーザアカウントのすべての SSH アクセスがブロックされます。

Identity Services Engine（ISE）

パッシブ認証に ISE/ISE-PIC を使用するために、Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）展開を 脅威に対する防御 デバイスと統合することができます。

ISE/ISE-PIC は権限を持つアイデンティティ ソースであり、Active Directory（AD）、LDAP、RADIUS、または RSA を使用して認証するユーザのユーザ認識データを提供します。ただし、脅威に対する防御 では、AD との組み合わせでのみユーザ アイデンティティ認識に ISE を使用できます。さまざまな監視ダッシュボードおよびイベントでユーザ情報を表示できるだけでなく、アクセス制御および SSL 復号ポリシーでユーザ アイデンティティを一致基準として使用できます。

Cisco ISE/ISE-PIC の詳細については、Cisco Identity Services Engine の管理者ガイド [英語]（https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html）と Identity Services Engine Passive Identity Connector（ISE-PIC）のインストールおよび管理者ガイド [英語]（https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html）を参照してください。

ISE に関する注意事項と制限事項

- ファイアウォールシステムでは、システムがデバイス認証をユーザーと関連付けないため、Active Directory 認証とともに 802.1x デバイス認証を使用することはできません。802.1x アクティブログインを使用する場合は、802.1xアクティブログインのみをレポートするようにISEを設定します(デバイスとユーザの両方)。この設定により、デバイスログインは一度だけシステムにレポートされます。
- ISE/ISE-PIC は、ISE ゲスト サービス ユーザのアクティビティをレポートしません。
- ISE/ISE-PIC サーバとデバイスの時刻を同期させます。同期していない場合、予期しない間隔でユーザ タイムアウトが実行される可能性があります。
- 多数のユーザ グループをモニタするように ISE/ISE-PIC を設定する場合、メモリ制限のためにシステムがグループに基づいてユーザマッピングをドロップする可能性があります。その結果、レルムまたはユーザ条件を持つルールが予期どおりに実行されない場合があります。
- システムのこのバージョンと互換性がある特定のバージョンの ISE/ISE-PIC については、『*Cisco Secure Firewall Compatibility Guide*』（https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html）を参照してください。
- ご使用のバージョンの ISE が IPv6 をサポートしていることを確認できないかぎり、ISE サーバの IPv4 アドレスを使用してください。

Identity Services Engine の設定

Cisco Identity Services Engine（ISE）または Cisco Identity Services Engine Passive Identity Connector（ISE PIC）をパッシブ アイデンティティ ソースとして使用するには、ISE Platform Exchange Grid（pxGrid）サーバへの接続を設定する必要があります。

始める前に

- ISEからpxGridサーバおよびMNTサーバの証明書をエクスポートします。たとえば、ISE PIC 2.2 では、**[証明書（Certificates）]** > **[証明書の管理（Certificate Management）]** > **[システム証明書（System Certificates）]** ページにあります。MNT (モニタリングおよびトラブルシューティング ノード)は、証明書リストの[使用者]列に[管理者]として表示されます。これらは、**[オブジェクト（Objects）]** > **[証明書（Certificates）]** ページで信頼できる CA 証明書としてアップロードするか、次の手順でアップロードすることができます。これらのノードは、同じ証明書を使用することがあります。
- AD アイデンティティ レルムを設定する必要もあります。システムは、AD からユーザのリストを取得し、ISE から user-to-IP アドレス マッピングに関する情報を取得します。
- 静的セキュリティ グループ タグ マッピングの有無にかかわらず、アクセス制御にセキュリティグループタグ（SGT）を使用し、SXP トピックをリッスンする場合は、ISE で SXP とこれらのマッピングも設定する必要があります。ISE でのセキュリティグループと SXP パブリッシングの設定を参照してください。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アイデンティティ ソース（Identity Sources）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、**[+]** > **[Identity Services Engine]** をクリックします。最大で 1 つの ISE オブジェクトを作成できます。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 次のプロパティを設定します。

- [Name]：オブジェクトの名前。
- [ステータス（Status）]：クリックしてオブジェクトを有効または無効にします。無効にすると、アイデンティティ ルールでISEをアイデンティティ ソースとして使用できません。
- [説明（Description）]：（任意）オブジェクトの説明。

- [プライマリノードホスト名/IPアドレス（Primary Node Hostname/IP Address）]：プライマリ pxGrid ISE サーバのホスト名または IP アドレス。ISE バージョンが IPv6 をサポートしていることを確認しない限り、IPv6 アドレスを指定しないでください。
- [セカンダリノードのホスト名/IPアドレス（Secondary Node Hostname/IP Address）]：ハイアベイラビリティ向けにセカンダリ ISE サーバを設定している場合、[セカンダリノードのホスト名/IPアドレスの追加（Add Secondary Node Hostname/IP Address）] をクリックし、セカンダリ pxGrid ISE サーバのホスト名または IP アドレスを入力します。
- [pxGridサーバCA証明書]: pxGridフレームワークの信頼された証明機関の証明書。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- [MNTサーバCA証明書]: 一括ダウンロードを実行する場合に使用するISE証明書用の信頼された証明機関の証明書。これは、MNT（モニタリングおよびトラブルシューティング）サーバが分かれていない場合、pxGrid サーバ証明書と同じにすることができます。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- [サーバ証明書（Server Certificate）]：ISE への接続時または一括ダウンロードの実行時に脅威に対する防御 デバイスが ISE に提供する必要がある内部アイデンティティ証明書。
- [登録（Subscribe To）]：登録する必要がある ISE pxGrid トピックを選択します。トピックを登録すると、そのトピックに関連するデータがダウンロードされます。
  - [セッション ディレクトリ トピック（Session Directory Topic）]：ユーザセッションの SGT マッピングを含む、ユーザセッションに関する情報を取得するかどうか。このオプションは、デフォルトで有効です。セキュリティポリシーで使用するためや、監視ダッシュボードで表示するためにパッシブユーザ ID を取得する場合は、このオプションを選択する必要があります。
  - [SXPトピック（SXP Topic）]：SGT から IP アドレスへの静的マッピングを取得するかどうか。セキュリティグループタグ（SGT）に基づくアクセス制御ルールを作成する場合は、このトピックを選択します。
- [ISEネットワークフィルタ（ISE Network Filters）]：ISE がシステムに報告するデータを制限するように設定できる任意のフィルタ。ネットワーク フィルタを指定すると、ISE はフィルタ内のネットワークからのみデータを報告します。[+] をクリックして、ネットワークを識別するネットワーク オブジェクトを選択し、[OK] をクリックします。オブジェクトを作成する必要がある場合は、[新しいネットワークの作成（Create New Network）] をクリックします。IPv4 ネットワーク オブジェクトのみを設定します。

ステップ 4 [テスト（Test）] ボタンをクリックして、システムが ISE サーバに接続できることを確認します。

テストが失敗した場合は、[ログの表示（See Logs）] リンクをクリックして、詳細なエラーメッセージを確認します。たとえば、次のメッセージはシステムが必要なポートでサーバに接続できなかったことを示しています。問題はホストへのルートが存在しないことである可能性

があります。つまり、ISE サーバが予期されたポートを使用していないか、接続を妨げるアクセス制御ルールが存在します。

```
Captured Jabberwerx log:2018-05-11T16:10:30 [   ERROR]: connection timed out while
trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

ステップ 5 [OK] をクリックしてオブジェクトを保存します。

次のタスク

ISE を設定したら、アイデンティティ ポリシーを有効にして、パッシブ認証ルールを設定し、その設定を展開します。その後、ISE/ISE PIC に移動して、デバイスをサブスクライバとして許可する必要があります。サブスクライバを自動的に許可するよう ISE/ISE PIC を設定している場合、サブスクリプションを手動で許可する必要はありません。

ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング

ISE/ISE-PIC 接続

ISE 接続または ISE-PIC 接続で問題が発生している場合、次の項目を確認します。

- ISE 脅威に対する防御 デバイスを正常に統合するには、ISE の pxGrid アイデンティティ マッピング機能を有効にする必要があります。
- ISE サーバと 脅威に対する防御 デバイスの間の接続を成功させるには、ISE のクライアントを手動で承認する必要があります。

  または、『*Cisco Identity Services Engine* 管理者ガイド』の「ユーザおよび外部 ID ソースの管理」の章にある説明に従って、ISE で [新しいアカウントの自動承認（Automatically approve new accounts）] を有効にできます。
- 脅威に対する防御 デバイス（サーバ）証明書には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、他の拡張キー使用値を含むことはできません。clientAuth 拡張キーの使用が設定されている場合は、キーの使用も設定されていないか、デジタル署名キー使用値が設定されている必要があります。Device Manager を使用して作成できる自己署名アイデンティティ証明書は、これらの要件を満たしています。
- ISE サーバの時間は、脅威に対する防御 デバイスの時間と同期する必要があります。アプライアンスが同期していないと、システムは予期しない間隔でユーザ タイムアウトを実行することがあります。

ISE/ISE-PIC ユーザ データ

ISE または ISE-PIC によって報告されたユーザ データに問題がある場合は、次の項目に注意します。

- システムは、データベース にデータがない ISE ユーザのアクティビティを検出すると、サーバからそのユーザに関する情報を取得します。ISE ユーザによるアクティビティは、アクセス制御ルールで処理されず、システムがユーザ ダウンロードでそのユーザに関する情報を正常に取得するまでダッシュボードに表示されません。
- LDAP、RADIUS、または RSA ドメイン コントローラによって認証された ISE ユーザについてユーザ制御を実行することはできません。
- システムは、ISE ゲスト サービス ユーザのユーザ データを受信しません。

SAMLサーバ

セキュリティ アサーション マークアップ言語 2.0（SAML 2.0）サーバーを設定して、リモートアクセス VPN 接続およびデバイスマネージャユーザーのシングルサインオン（SSO）認証ソースとして使用することができます。SAML は、当事者間、特に ID プロバイダー（IdP）とサービスプロバイダー（SP）の間で認証および許可データを交換するためのオープン標準です。

SAML サーバの設定

セキュリティ アサーション マークアップ言語 2.0（SAML 2.0）サーバーを設定して、リモートアクセス VPN 接続およびデバイスマネージャユーザーのシングルサインオン（SSO）認証ソースとして使用することができます。たとえば、Duo Access Gateway（DAG）は SAML サーバーです。

SAML サーバーを認証方法として使用する場合、SAML サーバーはアイデンティティ プロバイダー（IdP）として機能し、Threat Defense デバイスはサービスプロバイダー（SP）として機能します。

RA VPN の場合、SAML サーバーをプライマリ認証ソースとして使用できますが、セカンダリ認証ソースを設定したり、フォールバック ソースを設定したりすることはできません。

デバイスマネージャのログインでは、SAML サーバーをサポートするように設定している場合、SAML サーバーを使用するときに Common Access Card（CAC）をログインに使用できます。

始める前に

SAML サーバー アイデンティティ プロバイダーから次の情報を取得します。可能であれば、簡単にアップロードできるように XML ファイルでユーザーから情報をダウンロードします。

- エンティティ ID URL（SAML サーバメタデータを提供）
- サインイン URL
- サインアウト URL
- アイデンティティ プロバイダー証明書

SAML 属性に対して複数の値が返された場合、システムは最初に見つかった有効な値を使用します。たとえば、RA VPN で SAML を使用し、Cisco のグループポリシー属性に複数の値を指定した場合、最初の有効なグループポリシーが使用されます。どの値が使用されるかを制御しなければならない場合は、返される各属性に対して 1 つの値を提供するように SAML サーバーが構成されていることを確認してください。

手順

ステップ 1 [SAMLサーバ（SAML Servers）] ページに移動するには、次のいずれかを実行します。

- [オブジェクト（Objects）] を選択し、目次から [アイデンティティ ソース（Identity Sources）] を選択します。
- **[デバイス（Device）] > [リモートアクセスVPN（Remote Access VPN）] > [SAMLサーバ（SAML Servers）]** を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、**[+] > [SAMLサーバ（SAML Server）]** をクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 次のプロパティを設定します。

- [Name]：オブジェクトの名前。
- [説明（Description）]：（任意）オブジェクトの説明。
- [アイデンティティ プロバイダー（IDP）エンティティ ID URL（Identity Provider (IDP) Entity ID URL）]：SAML 発行元が要求に応答する方法を記述したメタデータ XML を提供するページの URL。これは、一部の SAML サーバ製品ではエンティティ ID と呼ばれ、他の製品ではメタデータ URL と呼ばれます。この URL は、プロトコル（https://）を含めて 4 ～ 256 文字である必要があります。たとえば、https://191.168.2.21/dag/saml2/idp/metadata.php のようになります。

  （注）
  SAML サーバーから XML ファイルで情報をダウンロードした場合は、[XMLファイルから読み込む（Populate from XML file）] をクリックし、ファイルを選択します。このフィールドと [サインインURL（Sign-In URL）] と [アイデンティティプロバイダー証明書（Identity Provider Certificate）] は、XML ファイルから読み込むことができます。

- [サインインURL（Sign-In URL）]：アイデンティティ プロバイダー SAML サーバにサインインするための URL。この URL は、プロトコルを含めて 4 ～ 500 文字である必要があります。http:// と https:// の両方を使用できます。たとえば、https://191.168.2.21/dag/saml2/idp/SSOService.php のようになります。

- [サインアウトURL（Sign-Out URL）]：アイデンティティ プロバイダー SAML サーバからサインアウトするための URL。この URL は、プロトコルを含めて 4 ー 500 文字である必要があります。http:// と https:// の両方を使用できます。たとえば、https://191.168.2.21/dag/saml2/idp/SingleLogoutService.php のようになります。
- [サービスプロバイダー証明書（Service Provider Certificate）]：Threat Defense デバイスに使用する内部証明書。認定済みのサードパーティによって署名された証明書がすでにアップロードされていると理想的であり、ここでそれを選択できます。組み込みの DefaultInternalCertificate を使用することや、ここで [新しい内部証明書の作成（Create New Internal Certificate）] をクリックして署名済みの証明書をアップロードすることもできます。SAML サーバ アイデンティティ プロバイダーはこの証明書を信頼する必要があるため、証明書を SAML サーバにアップロードする必要がある場合があります。証明書をアップロードする方法や、その他の方法でサービスプロバイダーとの信頼関係を有効にする方法については、SAML サーバのマニュアルを参照してください。
- [アイデンティティ プロバイダー証明書（Identity Provider Certificate）]：SAML サーバ アイデンティティ プロバイダーの信頼できる CA 証明書。この証明書は SAML サーバからダウンロードします。まだアップロードしていない場合は、ここで [新しい信頼できる CA 証明書の作成（Create New Trusted CA Certificate）] をクリックしてアップロードしてください。
- [要求の署名（Request Signature）]：ログイン要求の署名時に使用する暗号化アルゴリズム。暗号化を無効にする場合は、[なし（None）] を選択します。それ以外の場合は、[SHA1]、[SHA256]、[SHA384]、または [SHA512] のいずれか（後のものほど強力）を選択してください。
- [要求タイムアウト（Request Timeout）]：SAML アサーションには有効な期間があります。ユーザは、有効な期間内にシングルサインオン要求を完了する必要があります。この期間を変更するために、秒単位でタイムアウトを設定できます。アサーションの NotOnOrAfter 条件よりも長いタイムアウトを設定すると、タイムアウトは無視され、NotOnOrAfter が使用されます。指定できる範囲は 1 ～ 7200 秒です。デフォルトは 300 秒です。
- [このSAMLアイデンティティ プロバイダー（IDP）は内部ネットワーク上にある（This SAML identity provider (IDP) is on an internal network）]：SAML サーバが、保護されたネットワークへの内部ネットワーク（外部ネットワークではなく）上で動作しているかどうか。
- [ログイン時のIDP再認証の要求（Request IDP re-authentication at login）]：SAML サーバに以前の認証セッションを再利用させるのではなく、ログインごとにユーザが再認証されるようにするには、このオプションを選択します。このオプションは、デフォルトで有効です。

ステップ 4 [ユーザーロール（User Roles）] をクリックし、外部ユーザーの RBAC 許可ロールを設定します。

- [デフォルトユーザーロール（Default User Role）]：このページの設定で決定できない場合にユーザーに割り当てる許可ロール。

- [グループメンバー属性（Group Member Attribute）]：ユーザーの RBAC 許可ロールを定義する SAML サーバーのユーザー属性。
- [ロールマッピング（Role Mapping）]：ロールごとに、ロールに対応する SAML ユーザーレコードのグループメンバー属性に表示される文字列を入力します。
  - [管理者（Administrator）]：アプリケーションのすべての側面に対する完全な読み取り/書き込みアクセス権を持つユーザー。
  - [暗号管理者（Cryptographic Admin）]：証明書、復号ポリシー、秘密キーなどの暗号化関連機能を設定できるユーザー。他の機能への読み取り専用アクセス。
  - [監査管理者（Audit Admin）]：ユーザーのログイン履歴と監査ログを表示し、監査関連のアクションを実行できるユーザー。設定機能への読み取り専用アクセス。
  - [読み取り/書き込み（Read-Write）]：読み取り専用ユーザーが実行できることをすべて実行でき、設定を編集および展開することもできるユーザー。アップグレードのインストール、バックアップの作成と復元、監査ログの表示、他の Device Manager ユーザーセッションの終了など、システムクリティカルなアクションに対してのみ制限があります。
  - [読み取り専用（Read-Only）]：ダッシュボードおよび設定を表示できますが、変更することはできないユーザー。変更しようとすると、権限がないことを示すエラーメッセージが表示されます。

ステップ 5 [OK] をクリック

次のタスク

通信を暗号化するために [署名の要求（Request Signature）] を有効にした場合は、デバイスマネージャ情報を SAML サーバーにアップロードする必要があります。ID ソースのリストから、サーバーの [ダウンロード（Download）]（）ボタンをクリックし、XML ファイルを保存します。次に、SAML サーバーにログインし、情報をアップロードします。詳細については、SAML プロバイダーのマニュアルを参照してください。

デバイスマネージャのログインにサーバーを使用しているのに機能しない場合は、SAML サーバーの設定を確認します。

- SAML IdP にログインし、デバイスマネージャの SAML 応答コンシューマが正しく設定されていることを確認します。次の値である必要があります：https://<FDM_URL>/api/fdm/latest/fdm/token
- SAML サーバーオブジェクトで署名が有効になっている場合は、デバイスマネージャのパブリック証明書が SAML アプリケーションにアップロードされ、暗号化が有効になっていることを確認します。デバイスマネージャの XML ファイルをアップロードすると、証明書が SAML サーバーに追加されます。FDM API を使用してデバイスマネージャ証明書を取得することもできます：https://<FDM_URL>/saml/metadata

ローカル ユーザ

ローカル ユーザー データベース（LocalIdentitySource）には Device Manager で定義したユーザーが含まれます。

ローカル定義ユーザは、次の目的で使用できます。

- リモートアクセス VPN（プライマリまたはフォールバック アイデンティティ ソースとして）。
- 管理アクセス（Device Manager ユーザーのプライマリまたはセカンダリ ソースとして）。

  管理者ユーザはシステム定義のローカル ユーザです。ただし、管理者ユーザはリモートアクセス VPN にログインできません。追加のローカル管理者ユーザは作成できません。

  管理アクセスの外部認証を定義すると、デバイスにログインしている外部ユーザがローカル ユーザのリストに表示されます。
- アイデンティティ ポリシー（indirectly）（リモート アクセス VPN ログインからユーザ アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

ここでは、ローカル ユーザの設定方法について説明します。

ローカル ユーザの設定

リモートアクセス VPN とともに使用するために、デバイスでユーザ アカウントを直接作成できます。外部認証ソースの代わりに（または外部認証ソースに加えて）ローカル ユーザ アカウントを使用できます。

リモート アクセス VPN のフォールバック認証方式としてローカル ユーザ データベースを使用する場合、必ず外部データベースの名前と同じユーザ名/パスワードをローカル データベースで設定します。そうしなければ、フォールバック メカニズムは効果を発揮しません。

ここで定義されたユーザは、デバイスCLIにはログインできません。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[ユーザ（Users）]** を選択します。

リストに、次のようなユーザ名とサービスタイプが表示されます。

- MGMT：Device Manager にログインできる管理ユーザー向け。管理者ユーザが常に定義されており、削除することはできません。また、追加の MGMT ユーザを設定することもできません。ただし、管理アクセス用の外部認証を定義すると、デバイスにログインする外部ユーザが MGMT ユーザとしてローカル ユーザ リストに表示されます。

- RA VPN：デバイスに設定されたリモートアクセスVPNにログインできるユーザ向け。プライマリ ソースまたはセカンダリ（フォールバック）ソースのローカル データベースも選択する必要があります。

ステップ 2 次のいずれかを実行します。

- ユーザを追加するには、[+] をクリックします。
- ユーザを編集するには、そのユーザの編集アイコン（  ）をクリックします。

特定のユーザ アカウントが必要なくなったら、そのユーザの削除アイコン（  ）をクリックします。

ステップ 3 ユーザ プロパティを設定します。

名前とパスワードには、印刷可能ASCII英数字または特殊文字（スペースと疑問符を除く）を使用できます。印刷可能文字は ASCII コード 33 ～ 126 です。

- [名前（Name）]：リモート アクセス VPN にログインするためのユーザ名。名前には 4 ～ 64 文字を使用できますが、スペースは使用できません（例：johndoe）。
- [パスワード（Password）]、[パスワードの確認（Confirm Password）]：アカウントのパスワードを入力します。パスワードの長さは、8～16文字にする必要があります。同じ文字を連続して使用することはできません。数字、大文字、小文字、および特殊文字をそれぞれ 1 文字以上使用する必要もあります。

（注）
ユーザは、自分のパスワードを変更できません。ユーザにパスワードを通知します。パスワードを変更する必要がある場合は、ユーザ アカウントを編集する必要があります。また、外部MGMTユーザのパスワードは更新しないでください。パスワードは外部AAAサーバによって制御されています。

ステップ 4 **[OK]** をクリックします。

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