アイデンティティ ソース

アイデンティティ ソースは、ユーザー アカウントを定義するサーバーとデータベースです。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

アイデンティティソースは、組織内のユーザーのユーザーアカウントを定義する AAA サーバー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、ユーザー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、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 アイデンティティ ソースとして）。AD は RADIUS サーバーと組み合わせて使用可能。

- 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ー 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、以下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ー 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、システムがユーザー 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） （15 ページ）を参照してください。

このソースは、以下の目的で使用できます。

- アイデンティティポリシー（ISE からユーザー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 サーバー、RADIUS サーバーグループ

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。それぞれのサーバーを個別のオブジェクトとして定義し、それらをサーバーグループ（特定グループ内のサーバーは互いのコピー）に入れる必要があります。サーバーグループを機能に割り当て、個々のサーバー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、以下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 サーバー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ー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ーをサポートできます。これらのユーザーは、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 サーバー

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、以下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ーをサポートできます。これらのユーザーは、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 ユーザー （23 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 で設定するユーザーは含まれません（**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ー 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）はユーザー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 サーバー

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

サーバーの設定に関して次の点に注意してください。

- ユーザー グループまたはグループ内のユーザーに対してユーザー制御を実行する場合、ディレクトリ サーバーでユーザー グループを設定する必要があります。サーバーが基本的なオブジェクト階層でユーザーを整理している場合、システムはユーザー グループ制御を実行できません。
- ディレクトリ サーバーは、次の表に示すフィールド名を使用して、システムがそのフィールドのサーバーからユーザー メタデータを取得できるようにする必要があります。

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

ユーザー数の制限

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 ベースの DN の決定

ディレクトリの各プロパティを設定する際、ユーザおよび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 サーバ内で定義され、ネットワークごとに異なります。アイデンティティ ポリシーが正しく機能するには、適切なベースを入力する必要があります。ベースが誤っていると、ユーザ名またはグループ名が特定されず、アイデンティティに基づくポリシーが機能しなくなります。

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。

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（**[スタート（Start）] > [ファイル名を指定して実行（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します。

正しいベースであることを確認するには、次の手順を実行します。

1. ディレクトリ プロパティの [テスト接続（Test Connection）] ボタンをクリックし、接続を確認します。問題があった場合には修正して、ディレクトリ プロパティを保存します。
2. 変更をデバイスに適用します。
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およびグループ名の追加を試みます。ディレクトリを含むレルム内の一致ユーザ名およびグループ名を入力すると、入力中にオートコンプリートによる候補が表示されます。ドロップダウンリストに候補が表示される場合は、システムがディレクトリに適切に照会できたことを意味します。入力した文字列がユーザ名またはグループ名として表示されることが確かであるにもかかわらず、候補が表示されない場合は、対応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、認証サービスの提供に必要なディレクトリ サーバーとその他の属性のことです。ディレクトリ サーバーには、ネットワークへのアクセスを許可されているユーザーおよびユーザー グループについての情報が含まれます。

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：レルムは、ユーザー アイデンティティ情報とグループ メンバーシップ情報を提供します。次いでそれらの情報をアクセス コントロール ルールで使用できます。システムは、毎日の最終時間（UTC）に、すべてのユーザーとグループに関する更新情報を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：レルムは、接続が許可されているかどうかを判断する認証サービスを提供します。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ーにルールを適用するため、ユーザー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に相談して、ディレクトリ サーバーのプロパティの設定に必要な値を取得します。

（注） ディレクトリ サーバーが接続済みネットワークに存在しない場合や、デフォルト ルートで使用できない場合には、サーバーのスタティック ルートを作成します。スタティック ルートを作成するには、**[デバイス（Device）]** > **[ルーティング（Routing）]** > **[表示設定（View Configuration）]** の順に選択します。 または、サーバー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。

次に、[オブジェクト（Objects）]ページで直接オブジェクトを作成および編集する方法について説明します。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 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。
- 既存の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。サポートされるタイプは Active Directory のみで、このフィールドを変更することはできません。
- [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 に変換されます。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。例、cn=users,dc=example,dc=com。ベース DN の検索の詳細については、ディレクトリ ベースの 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がある完全修飾 Active Directory ドメイン名。例、example.com。

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。

- [ホスト名または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（Interface）]：AD サーバー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。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。
- [暗号化（Encryption）]：ユーザおよびグループの情報のダウンロードに暗号化された接続を使用するには、希望の方法（[STARTTLS] または [LDAPS]）を選択します。デフォルト

では [なし（None）] になっており、ユーザおよびグループの情報がクリア テキストでダウンロードされます。

- [STARTTLS] では、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る最も強力な方式を使用します。ポート 389 を使用します。このオプションは、リモート アクセス VPN にレルムを使用する場合は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）]：暗号化方式を選択する場合、認証局（CA）の証明書をアップロードして、システムとディレクトリ サーバ間の信頼できる接続を有効にします。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IPアドレス（Hostname/IP Address）] と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 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

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

最大 10 の AD サーバーをレルムに追加できます。これらのサーバーは互いに複製である必要があり、同じ AD ドメインをサポートする必要があります。

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

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。サーバーに到達できない場合は、正しい IP アドレスとホスト名を指定していること、DNS サーバーに当該ホスト名のエントリなどが設定されていることを確認します。サーバーにスタティック ルートを設定する必要があるかもしれません。詳細については、ディレクトリ サーバー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 サーバーでユーザー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 サーバー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ーセッションの 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。

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 レルムシーケンスのプロパティを設定します。

- [名前（Name）]：オブジェクトの名前。
- [説明（Description）]：（オプション）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

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 サーバー接続のトラブルシューティング

システムは、機能に応じて異なるプロセスを使用して、ディレクトリ サーバーと通信します。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。障害メッセージによって、接続上の問題がある機能が示されます。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ーの認証の問題。

ユーザー名またはパスワードが原因でシステムがディレクトリ サーバーにログインできない問題の場合、名前とパスワードが正しく、ディレクトリ サーバー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、システムはユーザー名とパスワードの情報から ldap-login-dn と ldap-login-password も生成します。たとえば、Administrator@example.com は cn=administrator,cn=users,dc=example,dc=com に変換されます。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ーは、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 サーバーにはデータ インターフェイスを介してアクセスできます。

ディレクトリ サーバーがデータ インターフェイス（GigabitEthernet インターフェイスなど）に直接接続されているネットワークまたは直接接続されたネットワークからルーティング可能なネットワーク上にある場合、仮想管理インターフェイスとディレクトリ サーバーの間に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上に明示的なゲートウェイがある場合、そのゲートウェイ ルータにディレクトリ サーバーへのルートが存在している必要があります。
- 直接接続されたネットワークとディレクトリ サーバーをホストするネットワークの間にルータがある場合、ディレクトリ サーバーのスタティック 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 サーバーは外部ネットワークにあります。

ディレクトリ サーバーが外部（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にある場合、サイト間 VPN 接続を設定する必要がある場合があります。詳細な手順については、リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバーを使用する方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 サーバーの設定

RADIUS サーバーは、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 サーバーごとにオブジェクトを作成した後、重複サーバーの各グループを含む RADIUS サーバー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、サーバー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サーバー（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。

- [名前（Name）]：オブジェクトの名前。 サーバー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。

- [サーバー名またはIPアドレス（Server Name or IP Address）]：サーバー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 とします。
- [認証ポート（Authentication Port）]：RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [タイムアウト（Timeout）]：次のサーバーに要求を送信する前にサーバー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、このサーバー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、ユーザーはトークンを取得して入力できます。
- [サーバー秘密キー（Server Secret Key）]：（オプション）脅威に対する防御 デバイスと RADIUS サーバー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、英数字または下線で開始する必要があります。特殊文字 $ & - _ . + @ を使用できます。文字列は、RADIUS サーバー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。

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ー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 サーバー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サーバー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）]：サーバー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（Resolve via Route Lookup）] 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。[インターフェイスを手動で選択する（Manually Choose Interface）] を選択すると、システムは常に選択され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、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。

  認可変更を設定する場合、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にできるように、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、システムがサーバーに接続できるかどうか確認します。

ユーザー名とパスワードの入力を求められます。テストでは、サーバーを接続できるかどうか、接続できる場合はユーザー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 サーバー グループの設定

RADIUS サーバーグループには、1 つまたは複数の RADIUS サーバーオブジェクトが含まれています。グループ内のサーバーは、相互にコピーされる必要があります。グループ内のサーバーでバックアップサーバーのチェーンが形成されるため、最初のサーバーが利用できなった場合、システムはリスト上の次のサーバーを試すことができます。

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

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。

- オブジェクトを作成するには、**[+]** > **[RADIUSサーバーグループ（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。

- [名前（Name）]：オブジェクトの名前。 サーバー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）]：失敗したサーバーは、すべてのサーバー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、最後のサーバーが失敗した後にすべてのサーバー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（Maximum Failed Attempts）]：次のサーバーを試行する前に、グループ内の RADIUS サーバーに送信された 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。最大失敗試行回数を超えると、システムはそのサーバー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ーが応答に失敗した場合、その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。サーバー 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 要求でサーバー 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 サーバー 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。このサーバー 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動的認可をイネーブルにします。
- [RADIUSサーバーをサポートするレルム（Realm that Supports the RADIUS Server）]：AD サーバーを使用してユーザーを認証するように RADIUS サーバーが設定されている場合は、この RADIUS サーバーと組み合わせて使用される AD サーバーを指定する 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サーバーリスト（RADIUS Server list）]：グループのサーバーを定義する RADIUS サーバー 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ーが、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サーバーの作成（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、システムがサーバーに接続できることを確認することもできます。ユーザー名とパスワードの入力を求められます。テストでは、サーバーを接続できるかどうか、接続できる場合はユーザー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）[すべてのサーバーをテスト（Test All Servers）] ボタンをクリックして、グループ内の各サーバーへの接続を確認します。

ユーザー名とパスワードの入力を求められます。システムは、各サーバーに接続できるかどうか、各サーバーでユーザー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 サーバー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 サーバーの [テスト（Test）] ボタンとサーバーグループオブジェクトを使用して、デバイスからサーバー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、サーバー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ー名/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、ログイン情報が不正であるというメッセージが表示されます。
  - 秘密鍵、ポート、およびサーバーの 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。秘密鍵がデバイス設定ではなく RADIUS サーバー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 サーバー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ーに 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、すべてのサーバー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ーでしか機能しない場合は、各ユーザーアカウントの RADIUS サーバーで定義されている 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、そのユーザー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ーでしか機能しない場合は、各ユーザーアカウントの RADIUS サーバーで定義されている 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、そのユーザー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）

Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）の展開を 脅威に対する防御 デバイスと統合して、ISE/ISE-PIC をパッシブ認証に使用できます。

ISE/ISE-PIC は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、または RSA を使用して認証するユーザーに関するユーザー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ー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ー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ー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 Administrator Guide*』（https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html）および『*Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Administrator Guide*』（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（デバイスとユーザーの両方）。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ーのアクティビティをレポートしません。
- ISE/ISE-PIC サーバーとデバイスの時刻を同期させます。そうしないと、システムが予期しない間隔でユーザーのタイムアウトを実行する可能性があります。
- 多数のユーザー グループをモニターするように ISE/ISE-PIC を設定した場合、システムはメモリ制限のためにグループに基づいてユーザーマッピングをドロップすることがあります。その結果、レルムまたはユーザー条件を使用するルールが想定どおりに実行されない可能性があります。
- 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 サーバーの 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（Used By）] 列に [管理者

（Admin）] 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。

- [名前（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）]：（オプション）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 サーバー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 サーバーのホスト名または IP アドレスを入力します。
- [pxGrid サーバ CA 証明書（pxGrid Server CA Certificate）]：pxGrid フレームワークの信頼できる認証局の証明書。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（MNT Server CA Certificate）]：一括ダウンロードを実行する場合に使用するISE証明書の信頼できる認証局の証明書。これは、MNT（モニタリングおよびトラブルシューティング）サーバーが分かれていない場合、pxGridサーバー証明書と同じものにできます。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）]：ユーザーセッションのSGTマッピングを含む、ユーザー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ー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 または ISE-PIC 接続に問題が起こった場合は、次のことを確認してください。

- ISE を脅威に対する防御デバイスに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 サーバーと脅威に対する防御デバイスの間の接続を確立するには、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「ユーザーおよび外部 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（サーバー）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 サーバーの時間は、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されていないと、予想外の間隔でユーザーのタイムアウトが実行される可能性があります。

ISE/ISE-PIC ユーザーデータ

ISE または ISE-PIC によって報告されるユーザー データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにない ISE ユーザーのアクティビティを検出すると、サーバーからそれらに関する情報を取得します。ISE ユーザー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、システムがユーザーダウンロードでそのユーザー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 コントローラで認証された ISE ユーザーに対するユーザー制御は実行できません。
- システムは、ISE ゲストサービスユーザーのユーザーデータを受信しません。

SAML サーバー

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 サーバーの設定

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 サーバーメタデータを提供）
- 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

手順

ステップ 1 [SAMLサーバー（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サーバー（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サーバー（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。

- [名前（Name）]：オブジェクトの名前。
- [説明（Description）]：（オプション）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 サーバー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 サーバー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 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/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 サーバー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 サーバー 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 サーバー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 サーバー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 サーバー 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 サーバー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。ユーザーは、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 サーバーが、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 サーバー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ー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 ユーザー

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ーは、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）。

管理者ユーザーはシステム定義のローカルユーザーです。ただし、管理者ユーザー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ーは作成できません。

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ーがローカルユーザーのリストに表示されます。

- アイデンティティポリシー（間接的）（リモートアクセス VPN ログインからユーザー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、ローカルユーザーの設定方法について説明します。

ローカル ユーザーの設定

リモート アクセス VPN で使用するユーザー アカウントをデバイスで直接作成できます。外部認証ソースの代わりに、またはそれに加えて、ローカルユーザー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ー向け。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。
- ユーザーを編集するには、そのユーザーの [編集（edit）] アイコン（  ）をクリックします。

特定のユーザー アカウントが必要なくなったら、そのユーザーの [削除（delete）] 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。