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 ID を提供したり、Firepower 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 ID を提供したり、Firepower 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 を RADIUS サーバと連携して使用することができます。

- 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）。

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、Firepower Threat Defense デバイスと ISE 展開を統合できます。Identity Services Engine（ISE） （14 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 サーバを使用している場合は、それらを Firepower 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 を RADIUS サーバと連携して使用することができます。
- 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）。
- FDM または FTD CLI 管理ユーザの外部認証。異なる認可レベルの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、システムにログインして、デバイスの設定とモニタリングを行うことができます。

LocalIdentitySource

これはローカル ユーザ データベースです。これには Firepower Device Manager で定義したユーザが含まれます。このデータベースのユーザ アカウントを管理するには、**[オブジェクト（Objects）]** > **[ユーザ（Users）]** を選択します。ローカル ユーザ （18 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（**configure user add** コマンドを使用）は含まれません。CLI ユーザは、Firepower Device Manager で作成するユーザとはまったく別になります。

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 サーバ 2008 および 2012 で Microsoft Active Directory（AD）を使用できます。

サーバの設定に関して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対してユーザ制御を実行する場合、ディレクトリ サーバでユーザ グループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、システムはユーザ グループ制御を実行できません。
- ディレクトリ サーバは、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からユーザ 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	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

ユーザ数の制限

Firepower Device Manager はディレクトリ サーバから最大 50,000 人のユーザ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 メンバーシップに照らして照合できます。

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 サーバとその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を許可されているユーザおよびユーザ 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 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 復号化：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に相談して、ディレクトリ サーバ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。

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、Firepower 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。作成可能なのは 1 つのレルムのみです。
- 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（Administrator だけでなく）などの完全修飾名である必要があります。

（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。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。サーバへの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。
- [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することができます。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 [テスト（Test）] ボタンをクリックして、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 サーバ接続のトラブルシューティング （8 ページ）を参照してください。

ステップ 7 [OK] をクリック

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、機能に応じて異なるプロセスを使用して、ディレクトリ サーバと通信します。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。

Directory ユーザの認証問題。

ユーザ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 サーバで有効なことを確認します。Active Directory では、昇格された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（Administrator だけでなく）などの完全修飾名である必要があります。

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 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と、ルーティングが成功します。
- 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 サーバへのルートが存在している必要があります。
- 仮想管理インターフェイスによって使用される物理インターフェイスである [診断（diagnostic）] インターフェイスで IP アドレスを設定する必要はありません。ただし、アドレスを設定する場合、ディレクトリ サーバに対するトラフィックを診断インターフェイスにリダイレクトするスタティック ルート（デフォルト ルートなど）も設定しないでください。
- 直接接続された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の間にルータがある場合、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 サーバには物理的な管理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 サーバが物理的な管理インターフェイス（Management0/0 など）に直接接続されているネットワークまたはその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、次の手順を実行する必要があります。

- 管理インターフェイスの IPv4 アドレス（論理名 **diagnostic**）を **[デバイス（Device）] > [インターフェイス（Interfaces）]** で設定します。IP アドレスは仮想管理アドレスと同じサブネット上にある必要があります（**[デバイス（Device）] > [システム設定（System Settings）] > [管理インターフェイス（Management Interface）]**）。
- ディレクトリ サーバと管理インターフェイスの間にルータがある場合、[診断（diagnostic）] インターフェイスの **[デバイス（Device）] > [ルーティング（Routing）]** で、ディレクトリ サーバ用のルートを設定します。
- 診断インターフェイスおよび管理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にあります。

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 サーバを使用して、リモート アクセス VPN 接続、および FDM と FTDCLI 管理ユーザ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 サーバも使用する場合は、Firepower Device Manager でそのサーバを使用できます。

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 サーバを使用してユーザを認証および認可すると、これらのサーバを Firepower 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 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。これによりトークンを取得して入力する時間が得られます。
- [サーバ秘密キー（Server Secret Key）]：（オプション）Firepower Threat Defense 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（Object）]** 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 の目的では、ISE がクライアント ポスチャを評価できるように、Cisco Identity Services Engine（ISE） を初期トラフィックに送信することです。ACL は HTTPS トラフィックを ISE に送信する必要がありますが、すでに宛先が ISE に指定されているトラフィック、または名前解決のために DNS サーバに送信されるトラフィックは除きます。例については、FTD 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（Resolve via Route Lookup）] を選択した場合、システムは常にルーティング 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。

  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。

サーバが管理アドレスと同じネットワーク上にある場合（これは診断インターフェイスを選択することを意味します）、診断インターフェイスで IP アドレスを設定する必要もあります。管理 IP アドレスを設定するだけでは不十分です。**[デバイス（Device）] > [インターフェイス（Interfaces）]** に移動し、管理 IP アドレスと同じサブネット上にある診断インターフェイスで IP アドレスを設定します。

FDM 管理アクセスにもこのサーバを使用する場合、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、管理 IP アドレスを通じて常に認証されます。

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。

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。デフォルト値は 10 分です。
- [最大失敗試行回数（Maximum Failed Attempts）]：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動的認可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：
  - テストでは、サーバに設定されているインターフェイスが無視され、常に管理インターフェイスが使用されるので注意してください。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、テストは失敗すると予想されます。
  - 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。
  - 秘密鍵、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。秘密鍵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。グループ内のすべての RADIUS サーバが失敗したときに、システムが最初のサーバ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。デフォルトは 10 分ですが、1440 分まで設定できます。
- 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 Firepower Threat Defense デバイスと統合することができます。

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に関するユーザ認識データを提供します。ただし、Firepower Threat Defense 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 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

- Firepower システムでは、システムによってデバイス認証がユーザと関連付けられることがないため、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（デバイスとユーザの両方）だけを報告するようにISEを設定します。このように設定すれば、デバイス ログインはシステムに 1 回だけ報告されます。
- 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。そうしないと、システムが予期しない間隔でユーザ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 グループをモニタするように 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 Firepower 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（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。

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 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）サーバが分かれていない場合、pxGridサーバ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 Firepower Threat Defense 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。
- [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 Firepower Threat Defense 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 サーバと Firepower Threat Defense 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 Administrator Guide*』の「Automatically approve new accounts」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。

- Firepower Threat Defense 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。Firepower 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、Firepower Threat Defense 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 データ

ISE または ISE-PIC によって報告されるユーザ 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 ユーザのアクティビティを検出すると、サーバからそれら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 コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。

- システムは、ISE ゲスト サービス ユーザのユーザ データを受信しません。

ローカル ユーザ

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

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（Firepower Device Manager ユーザ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 で使用するユーザ 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 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：Firepower Device Manager にログインできる管理ユーザ向け。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（edit）] 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（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。