CLI ユーザー

管理対象デバイスには、CLI アクセス用のデフォルトの**管理者**アカウントが含まれています。この章では、カスタムユーザーアカウントを作成する方法について説明します。

CLI ユーザーについて

内部ユーザーとして、または LDAP または RADIUS サーバーの外部ユーザーとして、管理対象デバイスにカスタムユーザーアカウントを追加できます。各管理対象デバイスは、個別のユーザーアカウントを保持します。たとえば、Firewall Management Center にユーザーを追加した場合は、そのユーザーは Firewall Management Center にのみアクセスできます。そのユーザー名を使用して管理対象デバイスに直接ログインすることはできません。管理対象デバイスにユーザーを別途追加する必要があります。

内部および外部ユーザ

管理対象デバイスは次の 2 つのタイプのユーザーをサポートしています。

- 内部ユーザー：デバイスは、ローカル データベースでユーザー認証を確認します。
- 外部ユーザー：ユーザーがローカル データベースに存在しない場合は、システムは外部 LDAP または RADIUS の認証サーバーに問い合わせます。

CLI アクセス

Firepower デバイスには、Linux の上部で実行する Firepower CLI が含まれます。デバイスでは CLI を使用して内部ユーザーを作成できます。Firewall Management Center を使用して Firewall Threat Defense デバイスで外部ユーザーを確立できます。

注意 CLI の Config レベルのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスでき、Linux シェルの `sudoers` 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。システムセキュリティ上の理由から、次の点を強くお勧めします。

- TAC の監督のもとで、または Firepower ユーザーマニュアルに明示的な手順がある場合に限り、Linux シェルを使用します。
- CLI アクセス権を持つユーザーのリストを適切に制限していることを確認します。
- CLI アクセス権限を付与する場合は、構成レベルのアクセス権を付与されたユーザーのリストを制限します。
- Linux シェルでユーザを直接追加しないでください。この章の手順のみを使用してください。
- Cisco TAC による指示または Firepower ユーザーマニュアルの明示的な手順による指示がない限り、CLI エキスパートモードを使用して Firepower デバイスにアクセスしないでください。

CLI ユーザー ロール

管理対象デバイスでは、CLI のコマンドへのユーザーのアクセス権は割り当てるロールによって異なります。

None

ユーザは、コマンド ラインでデバイスにログインすることはできません。

Config

ユーザは、設定コマンドを含むすべてのコマンドにアクセスできます。このアクセス レベルをユーザーに割り当てるときには注意してください。

Basic

ユーザーは、非設定コマンドにのみアクセスできます。使用できるコマンドは、dig、ping、traceroute です。内部ユーザーと Firewall Threat Defense 外部 RADIUS ユーザーのみが基本ロールをサポートします。

CLI ユーザーのガイドライン:

ユーザ名

- 内部ユーザーと外部ユーザーの両方に同じユーザー名を追加することはできません。外部サーバーが重複するユーザー名を使用している場合、デバイスへの展開は失敗します。
- ユーザー名は、次のように Linux に対して有効である必要があります。
  - 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
  - すべて小文字
  - 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

デフォルト

すべてのデバイスに、**admin**ユーザがローカルユーザアカウントとして含まれています。**admin** ユーザを削除することはできません。デフォルトの初期パスワードは **Admin123** です。初期化プロセス中に、この初期パスワードの変更が強制されます。エージェントは、変更されたログイン情報を Windows レジストリに保存し、 Firewall Management Centerと同じ暗号化、つまり暗号ブロック連鎖（CBC）を使用します。システム初期化の詳細については、ご使用のモデルのスタートアップガイドを参照してください。

ユーザー アカウント数

Cisco Firepower 1000 シリーズ デバイスでは、最大 43 のユーザーアカウントを作成できます。

CLI での内部ユーザーの追加

CLI を使用して、Firewall Threat Defense で内部ユーザーを作成します。

手順

ステップ 1 設定権限を持つアカウントを使用してデバイス CLI にログインします。

admin ユーザ アカウントには必要な権限がありますが、設定権限を持つ任意のアカウントで作業できます。SSH セッションまたはコンソール ポートを使用できます。

特定の Firewall Threat Defense モデルの場合、コンソール ポートで FXOS CLI に入ります。**connect ftd** を使用して Firewall Threat Defense の CLI にアクセスします。

ステップ 2 ユーザ アカウントを作成します。

configure user add *username* {**basic** | **config**}

- *username*：ユーザー名を設定します。ユーザー名は、次のように Linux に対して有効である必要があります。
  - 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
  - すべて小文字
  - 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可
- **basic**：ユーザーに基本的なアクセス権を付与します。このロールはユーザーに設定コマンドの入力を許可しません。使用できるコマンドは、dig、ping、traceroute です。
- **config**：ユーザーに設定アクセス権を付与します。このロールはユーザーにすべてのコマンドへの完全な管理者権限を与えます。

例：

次の例では、johncrichton という名前の設定アクセス権を持つユーザー アカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton      1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

（注）
自分のパスワードを **configure password** コマンドを使用して変更できることをユーザーに伝えます。

ステップ 3 （任意） セキュリティ要件を満たすアカウントの特性を調整します。

アカウントのデフォルト動作を変更するには、次のコマンドを使用できます。

- **configure user aging** *username max_days warn_days*

  ユーザパスワードの有効期限を設定します。パスワードが有効である最大日数に続いて、有効期限前にユーザに今後の期限切れを警告する日数を指定します。値は共に 1 から 9999 ですが、警告日数は最大日数よりも小さくなければなりません。アカウントを作成した場合、パスワードの有効期限はありません。

- **configure user forcereset** *username*

  次回ログイン時にユーザにパスワードを強制的に変更するよう要求します。

- **configure user maxfailedlogins** *username number*

  アカウントがロックされる前の連続したログイン失敗の最大回数を 1 ~ 9999 までで設定します。Use the **configure user unlock** command to unlock accounts. 新しいアカウントのデフォ

ルトは、5 回連続でのログインの失敗です。管理者アカウントは、ログイン失敗回数が最大数に達してもロックアウトされません（ただし、セキュリティ認定コンプライアンスを有効にした場合は除きます）。

- **configure user minpasswdlen** *username number*

  パスワードの最小の長さを 1 から 127 に設定します。

- **configure user strengthcheck** ユーザ名 {**enable** | **disable**}

  パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

ステップ 4 必要に応じてユーザ アカウントを管理します。

ユーザのアカウントをロックアウトできます。そうしないとアカウントの削除やその他の問題の修正が必要な場合があります。システムのユーザアカウントを管理するには、次のコマンドを使用します。

- **configure user access** ユーザ名 {**basic** | **config**}

  ユーザ アカウントの権限を変更します。

- **configure user delete** *username*

  指定したアカウントを削除します。

- **configure user disable** *username*

  指定したアカウントを削除せずに無効にします。ユーザは、アカウントを有効にするまでログインできません。

- **configure user enable** *username*

  指定したアカウントを有効にします。

- **configure user password** *username*

  指定したユーザのパスワードを変更します。ユーザーは通常 **configure password** コマンドを使用して自分のパスワードを変更する必要があります。

  注意
  管理者ユーザーのパスワードを変更する場合、エキスパートモードで Linux の **passwd** コマンドを使用しないでください。このコマンドは、ファイルシステムの破損を引き起こす可能性があります。通常の Firewall Threat Defense CLI の **configure user password admin** コマンド（管理者でない場合）、または **configure password** コマンド（管理者である場合）のみを使用します。パスワードがわからなくなり、全くログインできない場合は、パスワードの回復手順を参照してください。

- **configure user unlock** *username*

連続して失敗したログイン試行が最大数を超えたためにロックされたユーザアカウントのロックを解除します。

（注）
Firewall Threat Defense は、ユーザー認証に着脱可能な認証モジュール（PAM）フレームワークを使用します。このフレームワーク内で、pam_unix.so モジュールは、SHA-512 アルゴリズムを使用してパスワードのハッシュ化と検証を処理します

パスワードは、 SHA-512 アルゴリズムを使用してハッシュされます。

FTD の外部認証の設定

FTD デバイスの外部認証を有効にするには、1 つ以上の外部認証オブジェクトを追加する必要があります。

Firewall Threat Defense の外部認証について

Firewall Threat Defense ユーザーの外部認証を有効にすると、Firewall Threat Defense により外部認証オブジェクトで指定された LDAP または RADIUS サーバーを使用してユーザークレデンシャルが検証されます。

外部認証オブジェクトは、Firewall Management Center および Firewall Threat Defense デバイスで使用できます。さまざまなアプライアンス/デバイスタイプで同じオブジェクトを共有することも、別々のオブジェクトを作成することもできます。Firewall Threat Defense では、デバイスに展開するプラットフォーム設定で 1 つの外部認証オブジェクトのみをアクティブ化できます。

（注） タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の小さめのタイムアウト範囲（LDAP の場合は 1 ー 30 秒、RADIUS の場合は 1 ー 300 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Firewall Threat Defense 外部認証設定が機能しません。

Firewall Threat Defense SSH アクセスでは、外部認証オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを他のデバイス タイプにも使用する場合は、それらのフィールドが使用されます。

LDAP ユーザーには常に Config 権限があります。RADIUS ユーザーは、Config ユーザーまたは Basic ユーザーとして定義できます。

RADIUS サーバーのユーザーを定義する（Service-Type 属性を使用）か、外部認証オブジェクト内にユーザーリストを事前に定義することができます。LDAP では、LDAP サーバーの CLI ユーザーと一致するようにフィルタを指定できます。

（注） CLI へのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Linux シェルユーザーは root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。次のことを実行してください。

- Linux シェルアクセスが付与されるユーザーのリストを制限します。
- Linux シェルユーザーを作成しないでください。

LDAP について

Lightweight Directory Access Protocol（LDAP）により、ユーザ クレデンシャルなどのオブジェクトをまとめるためのディレクトリをネットワーク上の一元化されたロケーションにセットアップできます。こうすると、複数のアプリケーションがこれらのクレデンシャルと、クレデンシャルの記述に使用される情報にアクセスできます。ユーザーのクレデンシャルを変更する必要がある場合も、常に 1 箇所でクレデンシャルを変更できます。

Microsoft 社は、2020 年に Active Directory サーバーで LDAP バインディングと LDAP 署名の適用を開始すると発表しました。Microsoft 社がこれらを要件にするのは、デフォルト設定で Microsoft Windows を使用する場合に権限昇格の脆弱性が存在するために、中間者攻撃者が認証要求を Windows LDAP サーバーに正常に転送できる可能性があるからです。詳細については、Microsoft 社のサポートサイトで「2020 LDAP channel binding and LDAP signing requirement for Windows」を参照してください。

まだ行っていない場合は、Active Directory サーバーによる認証で TLS/SSL 暗号化の使用を開始することをお勧めします。

RADIUS について

Remote Authentication Dial In User Service（RADIUS）は、ネットワーク リソースへのユーザ アクセスの認証、認可、およびアカウンティングに使用される認証プロトコルです。RFC 2865 に準拠するすべての RADIUS サーバーで、認証オブジェクトを作成できます。

Secure Firewall デバイスは、SecurID トークンの使用をサポートします。SecurID を使用したサーバーによる認証を設定した場合、そのサーバーに対して認証されるユーザーは、自身の SecurID PIN の末尾に SecurID トークンを追加したものをログイン時にパスワードとして使用します。SecurID をサポートするために、Secure Firewall デバイスで追加の設定を行う必要はありません。

注意事項

- デフォルトの RADIUS 認証ポート番号は 1812 です。
- デフォルトの RADIUS アカウンティング ポートは 1813（RADIUS 認証ポートよりも 1 つ大きい番号）です。

RADIUS 認証ポートを変更すると、それに応じて RADIUS アカウンティング ポートも変更されます。 Firewall Management Center が新しいアカウンティング ポートで RADIUS サーバに接続できることを確認します。そうしないと、認証遅延が発生する可能性があります。

Firewall Threat Defense 用の LDAP 外部認証オブジェクトの追加

Firewall Threat DefenseF 管理用に外部ユーザーをサポートするために、LDAP サーバーを追加します。

マルチドメイン展開では、外部認証オブジェクトは作成されたドメインでのみ使用できます。

外部認証オブジェクトの共有

外部 LDAP オブジェクトは、Firewall Management Center および Firewall Threat Defense デバイスで使用できます。同じオブジェクトを Firewall Management Center とデバイス間で共有することも、別々のオブジェクトを作成することもできます。オブジェクトを共有していない場合でも、Firewall Threat Defense と Firewall Management Center の両方が LDAP サーバーに到達できることを確認します。Firewall Management Center は、ユーザーリストを取得してデバイスにダウンロードするために必要です。

（注） LDAP の場合、タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の短いタイムアウト範囲（1 ー 30 秒）を超えないようにしてください。タイムアウトをこれより高い値に設定すると、Firewall Threat Defense への展開が失敗します。

Firewall Threat Defense サポート対象フィールド

Firewall Threat Defense SSH アクセスでは、LDAP オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを Firewall Management Centerにも使用する場合は、それらのフィールドが使用されます。この手順は、Firewall Threat Defense でサポートされているフィールドのみを対象とします。その他のフィールドについては、Firewall Management Center 用の LDAP 外部認証オブジェクトの追加を参照してください。

ユーザー名

ユーザー名は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

外部認証に **admin** または **sshd** ユーザーを追加することはできません。

外部ユーザーは、Firewall Management Center で（外部認証オブジェクトの一部として）追加することしかできません。CLI では追加できません。内部ユーザーは、Firewall Management Center ではなく、CLI でしか追加できないことに注意してください。

内部ユーザーとして同じユーザー名が **configure user add** コマンドを使用して設定されていた場合は、Firewall Threat Defense は最初にその内部ユーザーのパスワードをチェックし、それが失敗した場合は LDAP サーバーをチェックします。後から外部ユーザと同じ名前の内部ユーザを追加できないことに注意してください。既存の内部ユーザしかサポートされません。

Privilege Level

LDAP ユーザーには常に Config 権限があります。

始める前に

デバイス上にドメイン名ルックアップの DNS サーバーを指定する必要があります。この手順で LDAP サーバーのホスト名ではなく IP アドレスを指定した場合、ホスト名に含めることができる認証用の URI を LDAP サーバーが返す場合があります。ホスト名を解決するには DNS ルックアップが必要です。DNS サーバーを追加するには「Firewall Threat Defense 管理インターフェイスの CLI での変更」を参照してください。

手順

ステップ 1 **System** (⚙) > **Users**を選択します。

ステップ 2 [外部認証（External Authentication）] タブをクリックします。

ステップ 3 (＋)**[外部認証オブジェクトの追加（Add External Authentication Object）]** をクリックします。

ステップ 4 [認証方式（Authentication Method）] を [LDAP] に設定します。

ステップ 5 [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 6 ドロップダウン リストから [サーバタイプ（Server Type）] を選択します。

ステップ 7 [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要がりあります。また、暗号化接続では IPv6 アドレスはサポートされていません。

ステップ 8 （任意） [ポート（Port）] をデフォルトから変更します。

ステップ 9 （任意） [バックアップサーバ（Backup Server）] パラメータを入力します。

ステップ 10 [LDAP固有のパラメータ（LDAP-Specific Parameters）] を入力します。

a) ユーザーがアクセスする LDAP ディレクトリの [ベースDN（Base DN）] を入力します。たとえば、Example 社のセキュリティ（Security）部門の名前を認証するには、`ou=security,dc=example,dc=com` と入力します。または、[DNの取得（Fetch DNs）] をクリックし、ドロップダウン リストから適切なベース識別名を選択します。

b) （任意） [基本フィルタ（Base Filter）] を入力します。

たとえば、ディレクトリ ツリー内のユーザー オブジェクトに `physicalDeliveryOfficeName` 属性が設定されており、New York 支店のユーザーに対しこの属性に値 `NewYork` が設定されている場合、New York 支店のユーザーだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` と入力します。

許可されていないユーザー admin および sshd を除き、すべての cn 名を取得するには、`(&(cn=*)(!( |(cn=sshd)(cn=admin)))` と入力します。

c) LDAP サーバを参照するために十分なクレデンシャルを持つユーザの [ユーザ名（User Name）] を入力します。たとえば、ユーザ オブジェクトに `uid` 属性が含まれている OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門の管理者のオブジェクトの `uid` に値 `NetworkAdmin` が設定されている場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力します。

d) [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドにユーザ パスワードを入力します。

e) （任意） [詳細オプションを表示（Show Advanced Options）] をクリックして、次の詳細オプションを設定します。

- **[暗号化（Encryption）]**：**[なし（None）]**、**[TLS]**、または **[SSL]** をクリックします。

  ポートを指定した後で暗号化方式を変更すると、ポートがその方式のデフォルト値にリセットされます。[なし（None）] または [TLS] の場合、ポートはデフォルト値の 389 にリセットされます。[SSL] 暗号化を選択した場合、ポートは 636 にリセットされます。

- [SSL証明書アップロードパス（SSL Certificate Upload Path）]：SSL または TLS 暗号化の場合は、[ファイルの選択（Choose File）] をクリックして証明書を選択する必要があります。

  以前にアップロードした証明書を置き換えるには、新しい証明書をアップロードし、設定をデバイスに再展開して、新しい証明書を上書きコピーします。

  （注）
  TLS 暗号化には、すべてのプラットフォームで証明書が必要です。SSL の場合、Firewall Threat Defense も証明書を必要とします。他のプラットフォームの場合、SSL は証明書を必要としません。ただし、中間者攻撃を防ぐため、SSL 証明書を常にアップロードしておくことをお勧めします。

- （未使用）[ユーザー名テンプレート（User Name Template）]：Firewall Threat Defense では使用されていません。

- [タイムアウト（秒）（Timeout (Seconds)）]：バックアップ接続にロールオーバーするまでの秒数（1 ー 30 秒）を入力します。デフォルトは 30 です。

  （注）
  タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の小さめのタイムアウト範囲（1 ー 30 秒）を超えないようにしてください。タイムアウトを高めの値に設定すると、Firewall Threat Defense LDAP 設定が機能しません。

ステップ 11 [属性マッピング（Attribute Mapping）] を設定して、属性に基づいてユーザーを取得します。

- [UI アクセス属性（UI Access Attribute）] を入力します。**注**：このフィールドは、デバイスの CLI アクセスには使用されません。ただし、これは必須フィールドであるため、値を入力する必要があります。[CLIアクセス属性（CLI Access Attribute）] に入力する値と同じ値を入力できます。
- ユーザー識別タイプ以外の CLI アクセス属性を使用する場合は、[CLIアクセス属性（CLI Access Attribute）] を設定します。たとえば、Microsoft Active Directory Server で、`sAMAccountName` シェル CLI アクセス属性を使用して CLI アクセスユーザーを取得するには、`sAMAccountName` と入力します。

（注）
CLI へのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Linux シェルユーザーは root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。CLI または Linux シェルアクセスが付与されるユーザーのリストを制限してください。

（注）
CLI アクセス権を持つ多数のユーザーを許可する外部認証オブジェクトを展開すると、ユーザーの作成を待機している間に展開がタイムアウトし、失敗する可能性があります。

ステップ 12 [CLIアクセスフィルタ（CLI Access Filter）] を設定します。

次のいずれかの方法を選択します。

- 認証設定の設定時に指定したものと同じフィルタを使用するには、[基本フィルタと同じ（Same as Base Filter）] チェックボックスをオンにします。
- 属性値に基づいて管理ユーザ項目を取得するには、属性名、比較演算子、およびフィルタとして使用する属性値を、カッコで囲んで入力します。たとえば、すべてのネットワーク管理者の `manager` 属性に属性値 `shell` が設定されている場合は、基本フィルタ `(manager=shell)` を設定できます。

ユーザー名の注意事項については、この手順の最初にある 「ユーザー名」 を参照してください。

ステップ 13 [保存（Save）] をクリックします。

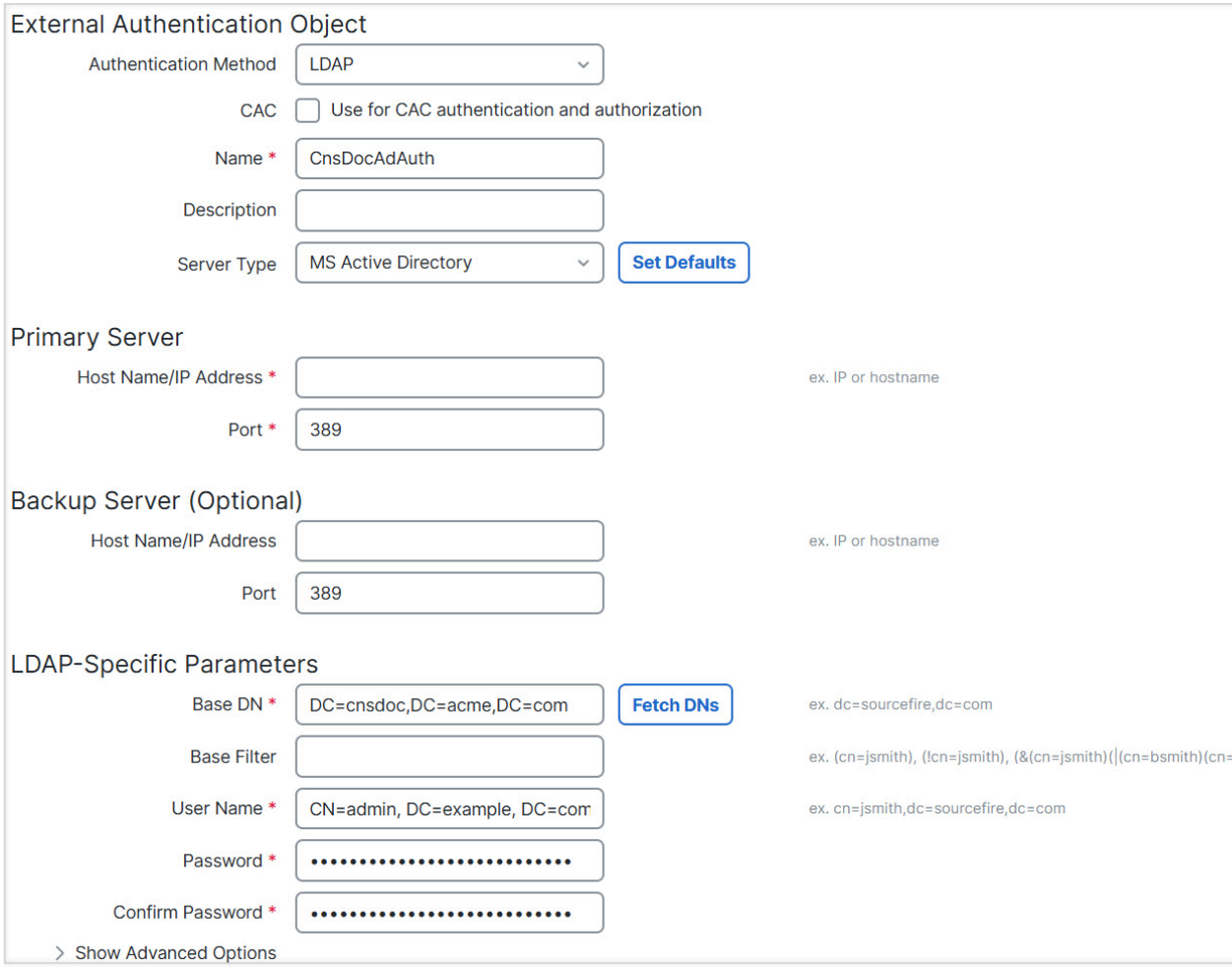
ステップ 14 このサーバーの使用を有効にします。外部認証 を参照してください。

ステップ 15 LDAP サーバーで後からユーザーを追加または削除する場合は、、管理対象デバイスのプラットフォーム設定を再展開する必要があります。Firewall Management Center はユーザーリストを再ダウンロードし、デバイスに展開します。「設定変更の展開」を参照してください。

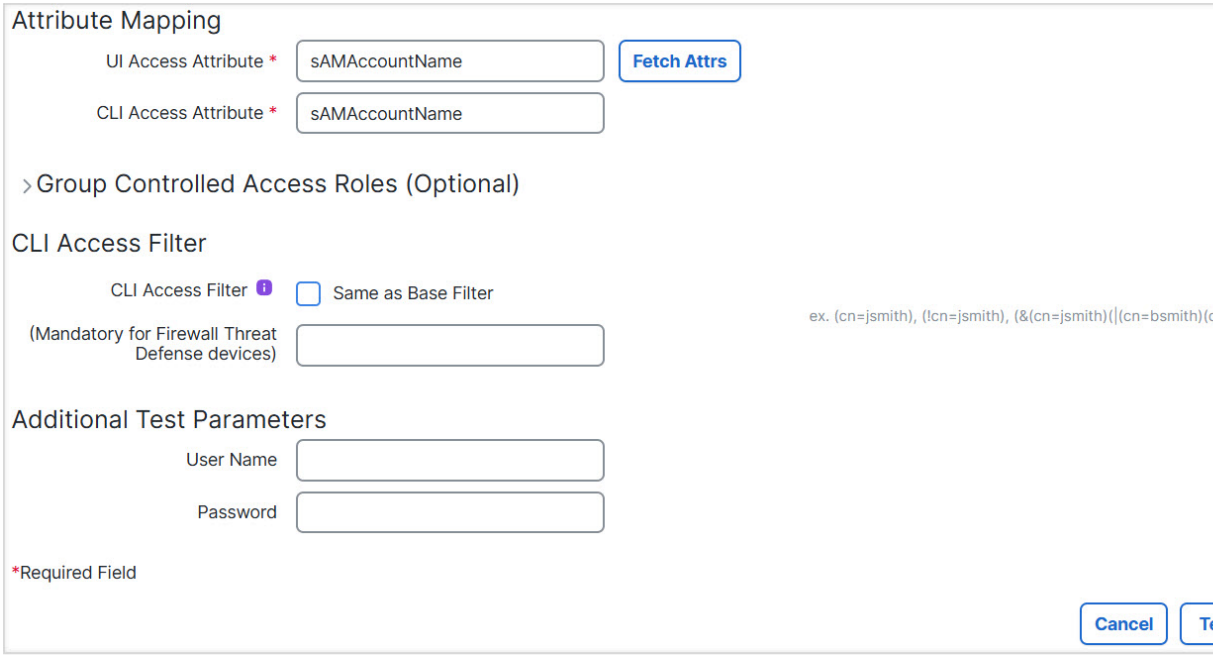
例

基本的な例

次の図は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの基本設定を示します。この例の LDAP サーバーの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 389 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。

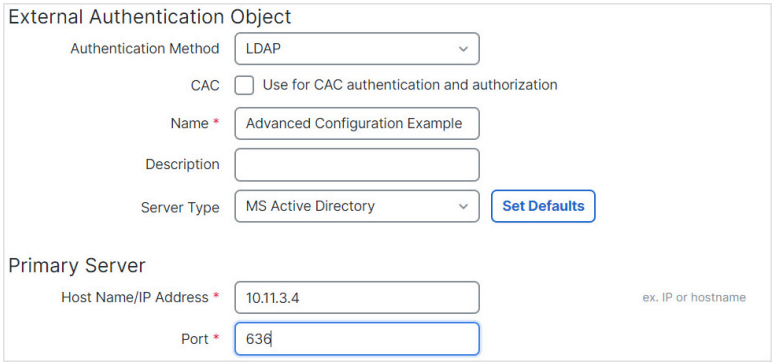


[CLIアクセス属性（CLI Access Attribute）] が `sAMAccountName` の場合、ユーザーが Firewall Threat Defense にログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

基本フィルタはこのサーバに適用されないため、Firewall Threat Defenseはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバーへの接続は、デフォルトの期間（または LDAP サーバーで設定されたタイムアウト期間）の経過後にタイムアウトします。

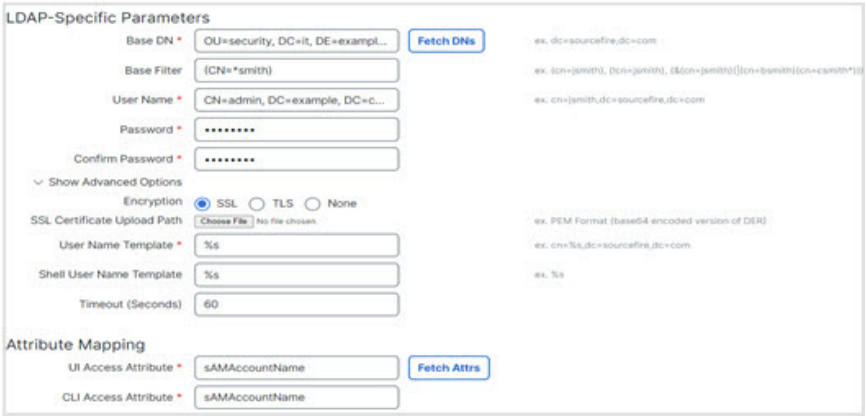
高度な例

次の例は、Microsoft Active Directory Server の LDAP ログイン認証オブジェクトの詳細設定を示します。この例の LDAP サーバーの IP アドレスは 10.11.3.4 です。接続ではアクセスのためにポート 636 が使用されます。



この例では、Example 社の情報テクノロジー ドメインで、セキュリティ部門のベース識別名として `OU=security,DC=it,DC=example,DC=com` を使用した接続を示しています。ただし、このサーバーに基本フィルタ `(cn=*smith)` が設定されていることに注意して

ください。このフィルタは、サーバーから取得するユーザーを、一般名が `smith` で終わるユーザーに限定します。

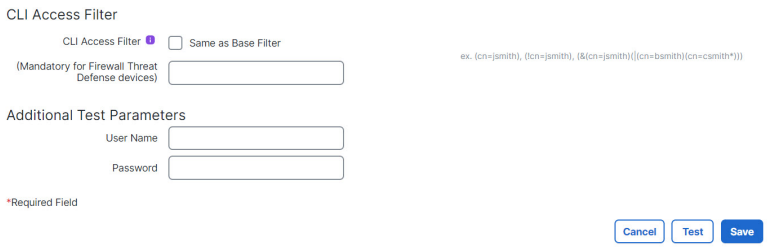


サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[タイムアウト（秒）（Timeout (Seconds)）] の設定により、60 秒経過後にサーバーへの接続がタイムアウトします。

このサーバーが Microsoft Active Directory Server であるため、ユーザー名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。

[CLIアクセス属性（CLI Access Attribute）] が `sAMAccountName` の場合、ユーザーが Firewall Threat Defense にログインすると、ディレクトリ内のすべてのオブジェクトの各 `sAMAccountName` 属性が検査され、一致が検索されます。

次の例では、CLI アクセスフィルタが基本フィルタと同じように設定されています。



Firewall Threat Defense 用の RADIUS 外部認証オブジェクトの追加

Firewall Threat Defense 用に外部ユーザーをサポートするために、RADIUS サーバーを追加します。

外部認証オブジェクトの共有

同じオブジェクトを Firewall Management Center とデバイス間で共有することも、別々のオブジェクトを作成することもできます。Firewall Threat Defense は RADIUS サーバーでのユーザーの定義をサポートしますが、Firewall Management Center では外部認証オブジェクトのユーザーリストを事前定義する必要があることに注意してください。Firewall Threat Defense には事前に定義されているリスト方式を使用できますが、RADIUS サーバーでユーザーを定義する場合は

Firewall Threat Defense と Firewall Management Center に個別のオブジェクトを作成する必要があります。

（注） タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の短いタイムアウト範囲（1 ー 300 秒）を超えないようにしてください。タイムアウトをもっと長い値に設定すると、Firewall Threat Defense RADIUS 設定が機能しません。

Firewall Threat Defense サポート対象フィールド

Firewall Threat Defense SSH アクセスでは、RADIUS オブジェクト内のフィールドのサブセットのみが使用されます。その他のフィールドに値を入力しても無視されます。このオブジェクトを Firewall Management Centerにも使用する場合は、それらのフィールドが使用されます。この手順は、Firewall Threat Defense でサポートされているフィールドのみを対象とします。他のフィールドについては、*Cisco Secure Firewall Management Center Administration Guide*の「Add a RADIUS External Authentication Object for Firewall Management Center」を参照してください。

ユーザー名

外部認証に **admin** ユーザーを追加することはできません。外部ユーザーは、Firewall Management Center で（外部認証オブジェクトの一部として）追加することしかできません。CLI では追加できません。内部ユーザーは、Firewall Management Center ではなく、CLI でしか追加できないことに注意してください。

内部ユーザーとして同じユーザー名が **configure user add** コマンドを使用して設定されていた場合は、Firewall Threat Defense は最初にその内部ユーザーのパスワードをチェックし、それが失敗した場合は RADIUS サーバーをチェックします。後から外部ユーザーと同じ名前の内部ユーザーを追加できないことに注意してください。既存の内部ユーザーしかサポートされません。RADIUS サーバーで定義されているユーザーの場合は、内部ユーザーの権限レベルと同じに設定してください。そうしないと、外部ユーザーパスワードを使用してログインできません。

手順

ステップ 1 Service-Type 属性を使用して RADIUS サーバー上のユーザーを定義します。

次に、Service-Type 属性でサポートされている値を示します。

- Administrator (6)：CLI への config アクセス認証を提供します。これらのユーザーは、CLI ですべてのコマンドを使用できます。
- NAS Prompt (7) または 6 以外のレベル：CLI への基本的なアクセス認証を提供します。これらのユーザーは **show** コマンドなど、モニタリングやトラブルシューティングのための読み取り専用コマンドを使用できます。

名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、記号（@）やスラッシュ（/）は使用不可

または、外部認証オブジェクトにユーザーを事前定義できます（ステップ 12 （16 ページ） を参照）。Firewall Threat Defense に対して Service-Type 属性メソッドを使用しているときに Firewall Threat Defense および Firewall Management Center に同じ RADIUS サーバーを使用するには、同じ RADIUS サーバーを識別する外部認証オブジェクトを 2 つ作成します。一方のオブジェクトには事前に定義した [CLIアクセスフィルタ（CLI Access Filter）] ユーザーを含め（Firewall Management Center で使用）、もう一方のオブジェクトの [CLIアクセスフィルタ（CLI Access Filter）] は空のままにします（Firewall Threat Defense で使用）。

ステップ 2 Firewall Management Center で、**System** (⚙) > **Users** を選びます。

ステップ 3 [外部認証（External Authentication）] をクリックします。

ステップ 4 [外部認証オブジェクトの追加（Add External Authentication Object）] (＋) をクリックします。

ステップ 5 [認証方式（Authentication Method）] を [RADIUS] に設定します。

ステップ 6 [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 7 [プライマリサーバ（Primary Server）] の場合は、[ホスト名/IPアドレス（Host Name/IP Address）] を入力します。

IPv4 だけがサポートされます。

（注）
証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、このフィールドに入力するホスト名と一致している必要があります。

ステップ 8 （任意） [ポート（Port）] をデフォルトから変更します。

ステップ 9 [RADIUS秘密キー（RADIUS Secret Key）] を入力します。

ステップ 10 （任意） [バックアップサーバ（Backup Server）] パラメータを入力します。

ステップ 11 （任意） [RADIUS固有のパラメータ（RADIUS-Specific Parameters）] を入力します。

a) プライマリサーバーを再試行するまでの [タイムアウト（秒）（Timeout (Seconds)）] を 1 ～ 300 の秒単位で入力します。デフォルトは 30 です。

（注）
タイムアウト範囲は Firewall Threat Defense と Firewall Management Center で異なるため、オブジェクトを共有する場合は、Firewall Threat Defense の短いタイムアウト範囲（1 ー 300 秒）を超えないようにしてください。タイムアウトをもっと長い値に設定すると、Firewall Threat Defense RADIUS 設定が機能しません。

b) バックアップ サーバーにロールオーバーするまでの [再試行（Retries）] を入力します。デフォルトは 3 です。

ステップ 12 （任意） RADIUS 定義ユーザー（ステップ 1 （15 ページ） を参照）を使用する代わりに、[CLI アクセスフィルタ（CLI Access Filter）] 領域の [管理者CLIアクセスユーザーリスト（Administrator

CLI Access User List）] フィールドに、CLI アクセスが必要なユーザー名をカンマで区切って入力します。たとえば、**jchrichton, aerynsun, rygel** と入力します。

Firewall Threat Defense で [CLIアクセスフィルタ（CLI Access Filter）] メソッドを使用すると、Firewall Threat Defense およびその他のプラットフォームタイプで同一の外部認証オブジェクトを使用できます。

（注）
RADIUS 定義ユーザーを使用する場合は、[CLIアクセスフィルタ（CLI Access Filter）] を空のままにする必要があります。

これらのユーザー名が RADIUS サーバーのユーザー名と一致していることを確認します。名前は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アットマーク（@）、またはスラッシュ（/）は使用不可

（注）
CLI へのアクセス権を持つユーザーは、**expert** コマンドを使用して Linux シェルにアクセスできます。Linux シェルユーザーは root 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。CLI または Linux シェルアクセスが付与されるユーザーのリストを制限してください。

（注）
CLI アクセス権を持つ多数のユーザーを許可する外部認証オブジェクトを展開すると、ユーザーの作成を待機している間に展開がタイムアウトし、失敗する可能性があります。

ステップ 13 （任意） RADIUS サーバーへの Firewall Management Center 接続をテストするには、[テスト（Test）] をクリックします。

この機能は、RADIUS サーバーへの Firewall Management Center 接続のみをテストできます。管理対象デバイスの RADIUS サーバーへの接続をテストする機能はありません。

ステップ 14 （任意） [追加のテストパラメータ（Additional Test Parameters）] を入力して、認証できるようにするユーザのユーザ クレデンシャルをテストすることもできます。[ユーザ名（User Name）] と [パスワード（Password）] を入力してから、[テスト（Test）] をクリックします。

ヒント
テストユーザーの名前とパスワードを誤って入力すると、サーバー設定が正しい場合でもテストが失敗します。サーバー設定が正しいことを確認するには、最初に [Additional Test Parameters] フィールドにユーザー情報を入力せずに [Test] をクリックします。正常に完了した場合は、テストする特定ユーザーのユーザー名とパスワードを指定します。

例：

Example 社の `JSmith` ユーザ クレデンシャルを取得できるかどうかをテストするには、`JSmith` と正しいパスワードを入力します。

ステップ 15 [保存（Save）] をクリックします。

ステップ 16 このサーバーの使用を有効にします。外部認証を参照してください

例

単純なユーザー ロールの割り当て

次の図は、IP アドレスが 10.10.10.98 のポート 1812 で Cisco Identity Services Engine（ISE）が稼働しているサーバーのサンプル RADIUS ログイン認証オブジェクトを示します。バックアップサーバーは定義されていません。

次の例は、システムがバックアップサーバー（存在する場合）への接続を試みるまでのタイムアウト（30 秒）と失敗した再試行の数を含む、RADIUS 固有のパラメータを示しています。

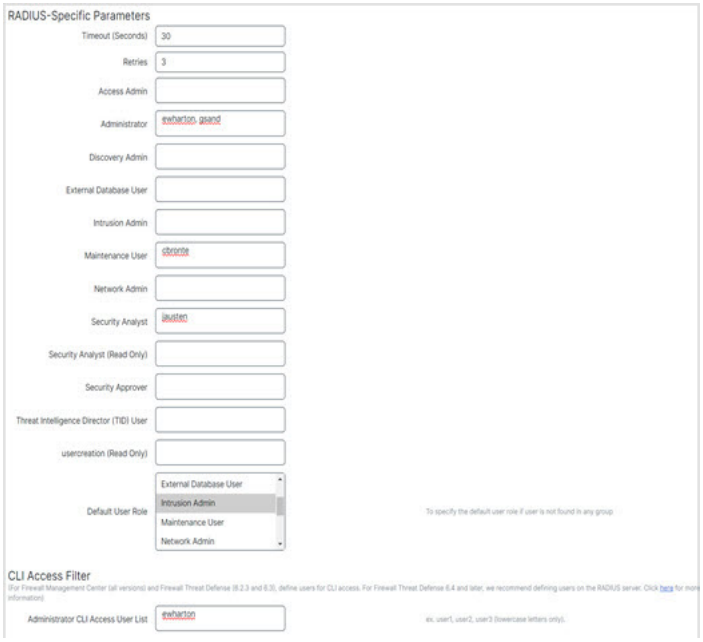
次の例は、RADIUS ユーザー ロール設定の重要な特徴を示します。

ユーザ `ewharton` および `gsand` には、Web インターフェイスの管理アクセスが付与されます。

ユーザ `cbronte` には、Web インターフェイスのメンテナンス ユーザ アクセスが付与されます。

ユーザー `jausten` には、Web インターフェイスのセキュリティ アナリスト アクセスが付与されます。

ユーザー `ewharton` は、CLI アカウントを使用してデバイスにログインできます。



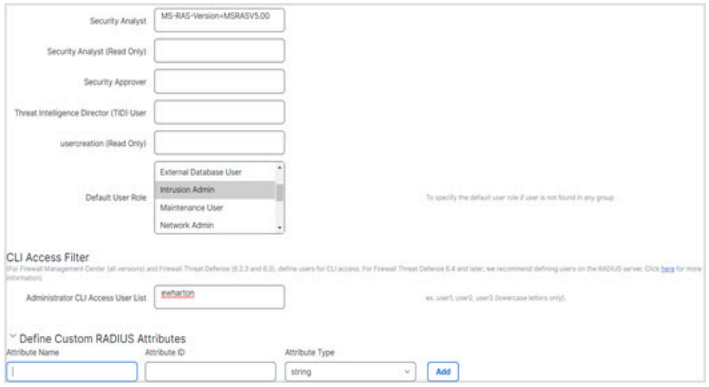
次の図に、この例のロール設定を示します。

属性と値のペアに一致するユーザーのロール

属性と値のペアを使用して、特定のユーザー ロールが付与される必要があるユーザーを示すこともできます。使用する属性がカスタム属性の場合、そのカスタム属性を定義する必要があります。

次の図は、前述の例と同じ ISE サーバーのサンプル RADIUS ログイン認証オブジェクトでのロール設定とカスタム属性の定義を示します。

ただしこの例では、Microsoft リモート アクセス サーバーが使用されているため、1 つ以上のユーザーの `MS-RAS-Version` カスタム属性が返されます。`MS-RAS-Version` カスタム属性は文字列であることに注意してください。この例では、Microsoft v. 5.00 リモート アクセス サーバー経由で RADIUS にログインするすべてのユーザーに対し、[セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] ロールが付与される必要があります。このため、属性と値のペア `MS-RAS-Version=MSRASV5.00` を [セキュリティ アナリスト（読み取り専用）（Security Analyst (Read Only)）] フィールドに入力します。



FTD デバイスのユーザーに対する外部認証の有効化

Firepower Threat Defense プラットフォーム設定で外部認証を有効にして、管理対象デバイスに設定を展開します。詳細については、外部認証を参照してください。

LDAP 認証接続のトラブルシューティング

LDAP認証オブジェクトを作成したが、選択したサーバーへの接続が失敗したか、または必要なユーザーのリストが取得されなかった場合は、そのオブジェクトの設定を調整できます。

接続のテストで接続が失敗する場合は、設定のトラブルシューティングに関する次の推奨手順を試してください。

- Web インターフェイス画面上部とテスト出力に示されるメッセージから、問題の原因となっているオブジェクトの部分を確認します。
- オブジェクトに使用したユーザー名とパスワードが有効であることを確認します。
  - サードパーティのLDAPブラウザを使用してLDAPサーバーに接続し、ベース識別名に示されているディレクトリを参照する権限があることを確認します。
  - ユーザー名が、LDAPサーバーのディレクトリ情報ツリーで一意であることを確認します。
  - テスト出力にLDAPバインドエラー49が示される場合は、ユーザーのユーザーバインディングが失敗しています。サードパーティアプリケーションを使用してサーバー認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。
  - LDAP認証を設定する場合、バインディングパスワードにバックスラッシュ（「\」）を使用しないでください。パスワードにバックスラッシュが含まれていると、LDAPバインドプロセスが失敗し、外部認証が失敗します。
- サーバーを正しく指定していることを確認します。

- サーバーの IP アドレスまたはホスト名が正しいことを確認します。
- ローカル アプライアンスから、接続する認証サーバーに TCP/IP でアクセスできることを確認します。
- サーバーへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。
- 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、サーバーに使用されているホスト名と一致している必要があります。
- CLI アクセスを認証する場合は、サーバー接続に IPv6 アドレスを使用していないことを確認します。
- サーバ タイプのデフォルトを使用している場合は、正しいサーバ タイプであることを確認し、[デフォルトを設定（Set Default）] をもう一度クリックしてデフォルト値をリセットします。

- ベース識別名を入力した場合は、[DNを取得（Fetch DNs）] をクリックし、サーバーで使用可能なすべてのベース識別名を取得し、リストから名前を選択します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、それぞれが有効であり正しく入力されていることを確認します。
- フィルタ、アクセス属性、または詳細設定を使用している場合は、各設定を削除し、設定なしでオブジェクトをテストしてみます。
- 基本フィルタまたは CLI アクセスフィルタを使用している場合は、フィルタがカッコで囲まれていて、有効な比較演算子を使用していることを確認します（囲み用のカッコを含めて最大 450 文字）。
- より制限された基本フィルタをテストするには、特定のユーザーだけを取得するため、フィルタにそのユーザーのベース識別名を設定します。
- 暗号化接続を使用する場合：
  - 証明書の LDAP サーバーの名前が、接続に使用するホスト名と一致していることを確認します。
  - 暗号化されたサーバー接続で IPv6 アドレスを使用していないことを確認します。
- テストユーザーを使用する場合、ユーザー名とパスワードが正しく入力されていることを確認します。
- テストユーザーを使用する場合、ユーザー資格情報を削除してオブジェクトをテストします。
- LDAP サーバーに接続し、次の構文を使用して、使用しているクエリをテストします。

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

たとえば、domainadmin@myrtle.example.com ユーザーと基本フィルタ (cn=*) を使用して myrtle.example.com のセキュリティ ドメインに接続する場合は、次のステートメントを使用して接続をテストできます。

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

接続のテストが正常に完了したが、プラットフォーム設定ポリシーの適用後に認証が機能しない場合は、使用する認証とオブジェクトの両方が、デバイスに適用されるプラットフォーム設定ポリシーで有効になっていることを確認します。

正常に接続したが、接続で取得されたユーザーリストを調整する必要がある場合は、基本フィルタまたはCLIアクセスフィルタを追加または変更するか、ベースDNをさらに制限するか制限を緩めて使用することができます。

Active Directory（AD）サーバーへの接続を認証しているときに、ADサーバーへの接続が成功しても、接続イベントログにブロックされたLDAPトラフィックが示されることはほとんどありません。この不正な接続ログは、ADサーバーが重複したリセットパケットを送信したときに発生します。Firewall Threat Defenseデバイスは、2番目のリセットパケットを新しい接続要求の一部として識別し、ブロックアクションを使用して接続をログに記録します。

CLI ユーザーの履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Limited user privileges for Threat Defense CLI Basic user.	7.7.0	7.7.0	The scope of the Threat Defense CLI Basic user privilege is now limited to the following commands: dig, ping, traceroute. If you have created users with the Basic privilege, evaluate whether you need to change them to the Config privilege. You can change a user's privilege level using the **configure user access** command. See: *Cisco Secure Firewall Threat Defense Command Reference*

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
RADIUS サーバーに定義されている Firewall Threat Defense ユーザーの Service-Type 属性のサポート	6.4.0	いずれか	Firewall Threat Defense CLI ユーザーの RADIUS の認証では、以前は RADIUS 外部認証オブジェクトにユーザー名を定義してから、RADIUS サーバーに認証されているユーザー名とリストが一致していることを手動で確認する必要がありました。Service-Type 属性を使用して RADIUS サーバーで CLI ユーザーを定義できるようになりました。また、Basic と Config の両方のユーザー ロールも定義できます。このメソッドを使用するには、外部認証オブジェクトのシェルアクセスフィルタを空白のままにしてください。 新規/変更された画面：**[システム（System）] > [ユーザー（Users）] > [外部認証（External Authentication）] > [外部認証オブジェクトの追加（Add External Authentication Object）] > [シェルアクセスフィルタ（Shell Access Filter）]**
Firewall Threat Defense SSH アクセスの外部認証	6.2.3	いずれか	LDAP または RADIUS認証を使用して Firewall Threat Defense への SSH の外部認証を設定できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [外部認証（External Authentication）]**

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。