管理アクセス用のユーザ アカウント

Firepower Management Center と管理対象デバイスには、管理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、サポートされているモデル用のカスタム ユーザ アカウントを作成する方法について説明します。ユーザ アカウントを使用して Firepower Management Center または管理対象デバイスにログインする方法の詳細については、「Firepower システムへのログイン」を参照してください。

この章では、Cisco Security Manager（CSM）で ASA を管理し、Firepower Management Center で FirePOWER サービス モジュールを管理する場合の、CSM シングル サインオンについても説明します。

ユーザ アカウントについて

内部ユーザとして、またはモデルでサポートされている場合は LDAP または RADIUS サーバの外部ユーザとして、Firepower Management Center および管理対象デバイスにカスタム ユーザ アカウントを追加できます。各 Firepower Management Center と各管理対象デバイスは、個別のユーザ アカウントを保持します。たとえば、Firepower Management Center にユーザを追加した場合は、そのユーザは FMC にのみアクセスできます。そのユーザ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を別途追加する必要があります。

内部および外部ユーザ

Firepower デバイスは次の 2 つのタイプのユーザをサポートしています。

- 内部ユーザ：デバイスは、ローカルデータベースでユーザ認証を確認します。内部ユーザの詳細については、「社内ユーザ アカウントの追加 （7 ページ）」を参照してください。
- 外部ユーザ：ユーザ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 の認証サーバに問い合わせます。外部ユーザの詳細については、「外部認証の設定 （12 ページ）」を参照してください。

Web インターフェイス、CLI またはシェルによるアクセス

ユーザ アカウントを設定する際に、Web インターフェイス アクセスと CLI またはシェル アクセスを個別に有効にします。 Firepower デバイスには、Linux の上部で実行する Firepower CLI が含まれます。CLI ユーザは、TAC の監督のもとで、または Firepower ユーザ マニュアルに明示的な手順がある場合、Linux シェルにアクセスすることもできます。管理 UI の詳細については、「Firepower Management Center 展開のユーザ インターフェイス」を参照してください。

⚠

注意 すべてのデバイス上で、CLI の Config レベルのアクセス権またはシェルへのアクセス権があるユーザは、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。

- 外部認証を確立した場合は、CLI またはシェルへのアクセス権があるユーザのリストを適切に制限してください。
- 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 マニュアルの明示的な手順による指示がない限り、Linux シェルや 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。

各デバイス タイプでサポートされているアクセス形式は異なります。次に詳細を示します。

- FTD、 ASA FirePOWER、および NGIPSv では、デバイスの直接管理に CLI アクセスを使用できます。
  - これらのデバイスでは CLI を使用して内部ユーザを作成できます。
  - Firepower Threat Defense デバイスでは外部ユーザを確立できます。

- 管理インターフェイスを通じてこれらのデバイスにログインしているユーザはCLIにアクセスします。CLI Config レベルのアクセス権を持つユーザは、CLI **expert** コマンドを使用して Linux シェルにアクセスできます。

  ⚠

  注意 Cisco TAC または Firepower ユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

- FMC にはデバイスを直接管理するための Web インターフェイス、CLI、および Linux シェルがあります。
  - FMC は 2 種類の内部 **admin** ユーザをサポートします。つまり Web インターフェイスのユーザと、 CLI またはシェル アクセス権が付与されたユーザが対象になります。これら 2 つの **admin** ユーザは異なるアカウントであり、同じパスワードを共有しません。システム初期化プロセスでは、これら 2 つの**admin** アカウントのパスワードが同期されるため、アカウントは同じように開始されますが、これらのアカウントは異なる内部メカニズムによって追跡され、初期設定後に分岐する場合があります。システム初期化の詳細については、ご使用のモデルの『*Getting Started Guide*』を参照してください。（Web インターフェイスの **admin** のパスワードを変更するには、**[System]** > **[Users]** > [ユーザ（Users）] を使用します。CLI またはシェルの **admin** のパスワードを変更するには、FMCCLI コマンド **configure password** を使用します）。
  - FMC Web インターフェイスで追加された内部ユーザには、Web インターフェイスのアクセス権のみが付与されます。
  - CLI またはシェルへのアクセス権を FMC の外部ユーザに付与できます。
  - FMC のデフォルトでは、シェルまたは CLI へのアクセス権を持つアカウントが管理インターフェイスにログインすると、そのアカウントは Linux シェルに直接アクセスします。FMC CLI を有効にすると、それらのユーザはログイン時にまず CLI へのアクセス権を取得すると、**expert** コマンドを使用してシェルへのアクセス権を取得できる場合があります。「Firepower Management Center のコマンド ライン リファレンス」を参照してください。
- 7000 および 8000 シリーズ デバイスには、デバイスを直接管理するための Web インターフェイスと CLI の両方が備わっています。
  - 7000 および 8000 シリーズ デバイスの内部ユーザには Web インターフェイスと CLI アクセス権があります。
  - 7000 および 8000 シリーズ デバイスの外部ユーザに対して CLI またはシェルへのアクセスを有効にできます。
  - 管理インターフェイスを通じてこれらのデバイスにログインしているユーザはCLIにアクセスします。CLI Config レベルのアクセス権を持つユーザは、シェルの **expert** コマンドを使用してシェルにアクセスできます。

注意 Cisco TAC またはFMC マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

ユーザの役割

ユーザ権限は、割り当てられたユーザ ロールに基づいています。たとえば、アナリストに対してセキュリティ アナリストや検出管理者などの事前定義ロールを付与し、デバイスを管理するセキュリティ管理者に対して管理者ロールを予約することができます。また、組織のニーズに合わせて調整されたアクセス権限を含むカスタム ユーザ ロールを作成できます。

Web インターフェイスのユーザ ロール

7000 および 8000 シリーズのデバイスは、管理者、メンテナンス ユーザ、およびセキュリティ アナリストのユーザ ロールへのアクセス権を持っています。

Firepower Management Center には、次の定義済みユーザ ロールが含まれています。

アクセス管理者

[ポリシー（Policies）] メニューでアクセス制御ポリシー機能や関連する機能へのアクセスが可能です。アクセス管理者は、ポリシーを展開できません。

管理者

管理者は製品内のすべてのものにアクセスできるため、セッションでセキュリティが侵害されると、高いセキュリティ リスクが生じます。このため、ログイン セッション タイムアウトから管理者を除外することはできません。

セキュリティ上の理由から、管理者ロールの使用を制限する必要があります。

検出管理者

[ポリシー（Policies）] メニューのネットワーク検出機能、アプリケーション検出機能、相関機能にアクセス可能です。検出管理者は、ポリシーを展開できません。

外部データベース ユーザ

JDBC SSL 接続に対応しているアプリケーションを用いて、Firepower System データベースに対して読取り専用のアクセスが可能です。Firepower システム アプライアンスの認証を行うサードパーティのアプリケーションについては、システム設定内でデータベースへのアクセスを有効にする必要があります。Web インターフェイスでは、外部データベース ユーザは、[ヘルプ（Help）] メニューのオンライン ヘルプ関連のオプションのみにアクセスできます。このロールの機能は、web インターフェイスに搭載されていないため、サポートやパスワードの変更を容易にするためにのみアクセスが可能です。

侵入管理者

[ポリシー（Policies）] メニューと [オブジェクト（Objects）] メニューの侵入ポリシー機能、侵入ルール機能、ネットワーク分析ポリシー機能のすべてにアクセスが可能です。侵入管理者は、ポリシーを展開できません。

メンテナンス ユーザ

監視機能やメインテナンス機能へのアクセスが可能です。メンテナンス ユーザは、[ヘルス（Health）] メニューや [システム（System）] メニューのメンテナンス関連オプションにアクセスできます。

ネットワーク管理者

[ポリシー（Policies）] メニューのアクセス制御機能、SSL インスペクション機能、DNS ポリシー機能、アイデンティティ ポリシー機能、および [デバイス（Devices）] メニューのデバイス設定機能へのアクセスが可能です。ネットワーク管理者は、デバイスへの設定の変更を展開できます。

セキュリティ アナリスト

セキュリティ イベント分析機能へのアクセスと [概要（Overview）] メニュー、[分析（Analysis）] メニュー、[ヘルス（Health）] メニュー、[システム（System）] メニューのヘルス イベントに対する読み取り専用のアクセスが可能です。

セキュリティ アナリスト（読み取り専用）

[概要（Overview）] メニュー、[分析（Analysis）] メニュー、[ヘルス（Health）] メニュー、[システム（System）] メニューのセキュリティ イベント分析機能とヘルス イベント機能への読み取り専用アクセスを提供します。

セキュリティ承認者

[ポリシー（Policies）] メニューのアクセス制御ポリシーや関連のあるポリシー、ネットワーク検出ポリシーへの制限付きのアクセスが可能です。セキュリティ承認者はこれらのポリシーを表示し、展開できますが、ポリシーを変更することはできません。

Threat Intelligence Director (TID) ユーザ

[インテリジェンス（Intelligence）] メニューの Threat Intelligence Director 設定にアクセスできます。Threat Intelligence Director (TID) ユーザは、TID の表示および設定が可能です。

CLI ユーザ ロール

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

（注） FMC の CLI 外部ユーザにはユーザ ロールがありません。そのため、それらのユーザは使用可能なすべてのコマンドを使用できます。

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 レベルをユーザに割り当てるときには注意してください。

Basic

ユーザは、非設定コマンドにのみアクセスできます。

（注） 管理対象デバイス上の外部 CLI ユーザには常に Config ユーザ ロールが備わっています。

ユーザ アカウントの要件と前提条件

モデルのサポート

外部ユーザ認証は、次のモデルでサポートされています。

- Firepower Management Center
- Firepower Threat Defense
- 7000 および 8000 シリーズ

ユーザ アカウントの注意事項および制約事項

デフォルト

すべてのデバイスには、すべてのアクセス形式のローカルユーザアカウントとして**admin**ユーザが含まれています。**admin**ユーザは削除できません。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。システム初期化の詳細については、ご使用のモデルの『*Getting Started Guide*』を参照してください。

グローバル設定

デフォルトでは、Firepower Management Center のすべてのユーザ アカウントに次の設定が適用されます。

- パスワードの再利用に制限はありません。
- システムは正常なログインを追跡しません。
- システムは、不正なログイン クレデンシャルを入力したユーザに対して時間が指定された一時的なロックアウトを適用しません。

すべてのユーザのこれらの設定は、システム設定として変更できます（**[System]** > **[Configuration]**）。「グローバル ユーザ構成時の設定」を参照してください。

社内ユーザ アカウントの追加

各デバイスは、個別のユーザ アカウントを保持します。Firepower Management Center と 7000 および 8000 シリーズ の Web インターフェイスは似ています。Firepower Threat Defense、NGIPSv、およびASA FirePOWER では、CLI で社内ユーザを追加する必要があります。Firepower Management Center および 7000 および 8000 シリーズ では、CLI でユーザを追加することはできません。

Web インターフェイスでの内部ユーザの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FMC 7000 & 8000 シリーズ	任意	管理者

この手順では、Firepower Management Center または 7000 & 8000 シリーズ デバイスの Web インターフェイスでカスタム内部ユーザ アカウントを追加する方法について説明します。

[システム（System）] > [ユーザ（Users）] > [ユーザ（Users）] タブには、手動で追加した内部ユーザと、LDAP または RADIUS 認証でユーザがログインしたときに自動的に追加された外部ユーザの両方が表示されます。外部ユーザについては、より高い権限を持つロールを割り当てると、この画面のユーザ ロールを変更できます。パスワード設定を変更することはできません。

Firepower Management Center のマルチドメイン展開では、ユーザは作成されたドメインでのみ表示されます。グローバル ドメインにユーザを追加してから、リーフ ドメインのユーザ ロールを割り当てると、そのユーザがリーフ ドメインに「所属」していても、追加されたグローバル [ユーザ（Users）] ページにそのユーザが表示されることに注意してください。

デバイスでセキュリティ認定コンプライアンスまたは Lights-Out Management（LOM）を有効にすると、異なるパスワード制限が適用されます。セキュリティ認定コンプライアンスの詳細については、「セキュリティ認定準拠」を参照してください。

リーフ ドメインにユーザを追加した場合、そのユーザはグローバル ドメインからは表示されません。

手順

ステップ 1 **[System]** > **[Users]** を選択します。

[ユーザ（Users）] タブはデフォルトで表示されます。

ステップ 2 [Create User] をクリックします。

ステップ 3 [ユーザ名（User Name）] に入力します。

ユーザ名は、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

ステップ 4 LDAP または RADIUS によりログインしたときに自動的に追加されたユーザに対しては、[外部認証方式の使用（Use External Authentication Method）] チェックボックスがオンになっています。外部ユーザを事前設定する必要はないので、このフィールドは無視できます。外部ユーザについては、このチェックボックスをオフにすることで、そのユーザを内部ユーザに戻すことができます。

ステップ 5 [パスワード（Password）] および [パスワードの確認（Confirm Password）] フィールドに値を入力します。

この値は、このユーザに設定したパスワード オプションに準拠している必要があります。

ステップ 6 [ログイン失敗の最大回数（Maximum Number of Failed Logins）] を設定します。

各ユーザが、ログイン試行の失敗後に、アカウントがロックされるまでに試行できるログインの最大回数を示す整数を、スペースなしで入力します。デフォルト設定は5回です。ログイン失敗回数を無制限にするには、**0** を使用します。**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）。

ステップ 7 [パスワードの最小長（Minimum Password Length）] を設定します。

ユーザのパスワードの必須最小長（文字数）を示す整数を、スペースなしで入力します。デフォルト設定は **8** です。値 **0** は、最小長が必須ではないことを示します。

ステップ 8 [パスワードの有効期限までの日数（Days Until Password Expiration）] を設定します。

ユーザのパスワードの有効期限までの日数を入力します。デフォルト設定は、パスワードが期限切れにならないことを示す **0** です。デフォルトから変更すると、[ユーザ（Users）] リストの [パスワードのライフタイム（Password Lifetime）] 列に、各ユーザのパスワードの残っている日数が表示されます。

ステップ 9 [パスワードの有効期限を事前に警告する日数（Days Before Password Expiration Warning）] を設定します。

パスワードが実際に期限切れになる前に、ユーザがパスワードを変更する必要があるという警告が表示される日数を入力します。デフォルト設定は **0** 日間です。

ステップ 10 ユーザの [オプション（Options）] を設定します。

- [ログイン時にパスワードのリセットを強制（Force Password Reset on Login）]：次回のログイン時にユーザにパスワード変更を強制します。
- [パスワードの強度のチェック（Check Password Strength）]：強力なパスワードを必須にします。強力なパスワードは 8 文字以上の英数字からなり、大文字と小文字を使用し、1 つ以上の数字と 1 つ以上の特殊文字を使用する必要があります。辞書に記載されている単語や、同じ文字を連続して繰り返し使用することはできません。
- [ブラウザセッションタイムアウトの適用除外（Exempt from Browser Session Timeout）]：非アクティブ状態が原因で、ユーザのログイン セッションが終了しないようにします。Administrator ロールが割り当てられているユーザを除外することはできません。

ステップ 11 （7000 または 8000 シリーズ）「CLI ユーザ ロール （5 ページ）」の説明に従い、適切なレベルの [コマンドラインインターフェイスアクセス（Command-Line Interface Access）] を割り当てます。

（注） 7000 または 8000 シリーズ の場合とは異なり、Firepower Management Center 内部ユーザのシェル アクセスを有効にすることはできません（FMC では、外部ユーザのシェル アクセスを有効にできますが、システム セキュリティ上の理由から、有効にしないことを推奨します）。

ステップ 12 [ユーザロールの設定（User Role Configuration）] エリアで、ユーザ ロールを割り当てます。ユーザ ロールの詳細については、「Web インターフェイス用のユーザ ロールのカスタマイズ（31 ページ）」を参照してください。

外部ユーザについては、グループまたはリストのメンバーシップによってユーザ ロールが割り当てられている場合、最小限のアクセス権限を削除することはできません。ただし、追加の権限を割り当てることはできます。ユーザ ロールがデバイスで設定したデフォルトのユーザ ロールの場合は、ユーザ アカウントのロールを制限なしに変更できます。ユーザ ロールを変更すると、[ユーザ（Users）] タブの [認証方式（Authentication Method）] 列に、[外部-ローカル変更（External - Locally Modified）] のステータスが表示されます。

表示されるオプションは、デバイスが単一ドメイン展開かマルチドメイン展開（Firepower Management Center のみ）かによって異なります。

- 単一ドメイン：ユーザを割り当てるユーザ ロールをオンにします。
- マルチドメイン（Firepower Management Center のみ）：マルチドメイン展開では、管理者アクセス権限があるドメインでユーザアカウントを作成できます。ユーザは各ドメインで異なる権限を持つことができます。先祖ドメインと子孫ドメインの両方でユーザ ロールを割り当てることができます。たとえば、あるユーザにグローバル ドメインでは読み取り専用権限を割り当て、子孫ドメインでは管理者権限を割り当てることができます。次の手順を参照してください。

  1. [ドメインの追加（Add Domain）] をクリックします。
  2. [ドメイン（Domain）] ドロップダウン リストからドメインを選択します。
  3. ユーザを割り当てるユーザ ロールをオンにします。

4. [保存（Save）] をクリックします。

ステップ 13 [保存（Save）] をクリックします。

CLI での内部ユーザの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FTD ASA FirePOWER NGIPSv	任意	Config

CLI を使用して、FTD、ASA FirePOWER、および NGIPSv デバイスで内部ユーザを作成します。これらのデバイスには Web インターフェイスがないため、内部（および外部）ユーザは管理のために CLI にのみアクセスできます。

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 FTD 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 FTD 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*：ユーザ名を設定します。ユーザ名は、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に設定コマンドの入力を許可しません。
- **config**：ユーザに設定アクセス権を付与します。このロールはユーザ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 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に伝えます。

ステップ 3 （任意） セキュリティ要件を満たすようにアカウントの性質を調整します。

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。パスワードの最大有効日数と、有効期限が近づいたことをユーザに通知する警告を期限切れとなる何日前に発行するかを指定します。どちらの値も 1 ~ 9999 ですが、警告までの日数は最大日数以内にする必要があります。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。アカウントをロック解除するには、**configure user unlock** コマンドを使用します。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。

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

  パスワードの最小長を 1 ~ 127 までで設定します。

- **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。ユーザの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。

ユーザをアカウントからロックアウトしたり、アカウントを削除するか、またはその他の問題を修正したりしなければならない可能性があります。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。

- **configure user unlock** *username*

  ログイン試行の最大連続失敗回数の超過が原因でロックされたユーザアカウントをロック解除します。

外部認証の設定

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。

外部認証について

Firepowerシステムの管理ユーザの外部認証を有効にすると、デバイスにより外部認証オブジェクトで指定された LDAP または RADIUS サーバを使用してユーザ 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、Firepower Management Center、7000 および 8000 シリーズ、 および FTD 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。

FMC では、**[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** タブで外部認証オブジェクトを直接有効にします。この設定は、FMC の使用にのみ影響し、管理対象デバイスを使用する場合には、このタブで有効にする必要はありません。 7000 および 8000 シリーズおよびFTD のデバイスでは、デバイスに展開するプラットフォーム設定で外部認証オブジェクトを有効にする必要があります。

外部認証オブジェクト内の CLI/シェル ユーザから Web インターフェイスのユーザが個別に定義されます。 の RADIUS の CLI/シェル ユーザの場合、外部認証オブジェクト内に RADIUS

ユーザ名のリストを事前に設定しておく必要があります。LDAP では、LDAP サーバの CLI ユーザと一致するようにフィルタを指定できます。

CAC 認証用にも設定されている CLI/シェル アクセスの LDAP オブジェクトは使用できません。

（注） Linux シェルへのアクセス権があるユーザはルート権限を取得できるため、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 シェルへのアクセス権を持つユーザのリストを制限します。
- Linux シェル ユーザを作成しないでください。

Firepower Management Center および 7000 および 8000 シリーズ の外部認証

Webインターフェイスアクセス用に複数の外部認証オブジェクトを設定できます。たとえば、5 つの外部認証オブジェクトがある場合、いずれかのオブジェクトのユーザを Web インターフェイスにアクセスするために認証できます。

CLIまたはシェル アクセスに使用できる外部認証オブジェクトは1つのみです。複数の外部認証オブジェクトが有効になっている場合、ユーザはリスト内の最初のオブジェクトのみを使用して認証できます。7000 または 8000 シリーズ デバイス上の外部 CLI ユーザは常に Config 権限を持っています。他のユーザ ロールはサポートされません。

Firepower Threat Defense の外部認証

FTD では、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。

FTDSSH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。

外部ユーザは常に設定権限を持っています。他のユーザ ロールはサポートされません。

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。

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 サーバで、認証オブジェクトを作成できます。

FirePOWER デバイスは、SecurID トークンの使用をサポートします。SecurID を使用したサーバによる認証を設定した場合、そのサーバに対して認証されるユーザは、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、FirePOWER デバイスで追加の設定を行う必要はありません。

LDAP 外部認証オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FTD 7000 および 8000 シリーズ FMC	任意	管理者

デバイス管理用に外部ユーザをサポートするために、LDAP サーバを追加します。

FTD では、CLI アクセスには一部のフィールドのみが使用されます。どのフィールドが使用されるかについては、「SSH の外部認証の設定」を参照してください。

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。

始める前に

- デバイス上にドメイン名ルックアップの DNS サーバを指定する必要があります。この手順で LDAP サーバ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 サーバを追加するには「管理インターフェイスの設定」を参照してください。
- CAC 認証に使用する LDAP 認証オブジェクトを設定する場合は、コンピュータに挿入されている CAC を取り外さないでください。ユーザ証明書を有効にした後では、CAC が常に挿入された状態にしておく必要があります。

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 （任意） CAC 認証および認可にこの認証オブジェクトを使用する予定の場合は、[CAC] チェックボックスをオンにします。

CAC 認証および認可を完全に設定するには、「LDAP を使用した共通アクセス カード認証の設定 （30 ページ）」の手順にも従う必要があります。このオブジェクトは、CLI ユーザには使用できません。

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 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。

ヒント [デフォルトの設定（Set Defaults）] をクリックした場合は、デバイスにより [ユーザ名テンプレート（User Name Template）]、[UIアクセス属性（UI Access Attribute）]、[シェルアクセス属性（Shell Access Attribute）]、[グループメンバー属性（Group Member Attribute）]、および [グループメンバーURL属性（Group Member URL Attribute）] フィールドに、サーバ タイプのデフォルト値が入力されます。

ステップ 8 [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、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 9 （任意） [ポート（Port）] をデフォルトから変更します。

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

a) ユーザがアクセスする 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 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 支店のユーザだけを取得するには、`(physicalDeliveryOfficeName=NewYork)` 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、FTD 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。

- [ユーザ名テンプレート（User Name Template）]：[UIアクセス属性（UI Access Attribute）] に対応するテンプレートを入力します。たとえば、UI アクセス属性が `uid` である OpenLDAP サーバに接続し、Example 社のセキュリティ（Security）部門で働くすべてのユーザを認証するには、[ユーザ名テンプレート（User Name Template）] フィールドに `uid=%s,ou=security,dc=example,dc=com` と入力します。Microsoft Active Directory Server の場合は `%s@security.example.com` と入力します。

  CAC 認証では、このフィールドは必須です。

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

ステップ 12 （任意）[属性照合（Attribute Matching）] を設定して、属性に基づいてユーザを取得します。

- [UIアクセス属性（UI Access Attribute）] を入力するか、[属性の取得（Fetch Attrs）] をクリックして利用可能な属性のリストを取得します。たとえば Microsoft Active Directory Server では、Active Directory Server ユーザ オブジェクトに `uid` 属性がないため、[UI アクセス属性（UI Access Attribute）] を使用してユーザを取得することがあります。代わりに [UI アクセス属性（UI Access Attribute）] フィールドに `userPrincipalName` と入力して、`userPrincipalName` 属性を検索できます。

  CAC 認証では、このフィールドは必須です。

- ユーザ識別タイプ以外のシェル アクセス属性を使用する場合は、[シェルアクセス属性（Shell Access Attribute）] を設定します。たとえば、Microsoft Active Directory Server で、`sAMAccountName` シェル アクセス属性を使用して CLI/シェル アクセス ユーザを取得するには、`sAMAccountName` と入力します。

ステップ 13 （任意）[グループ制御アクセスロール（Group Controlled Access Roles）] を設定します。

グループ制御アクセス ロールを使用してユーザの権限を事前に設定していない場合、ユーザには、外部認証ポリシーでデフォルトで付与される権限だけが与えられています。

a) （任意）ユーザ ロールに対応するフィールドに、これらのロールに割り当てる必要があるユーザを含む LDAP グループの識別名を入力します。

   参照するグループはすべて LDAP サーバに存在している必要があります。スタティック LDAP グループまたはダイナミック LDAP グループを参照できます。スタティック LDAP

グループとは、特定のユーザを指し示すグループ オブジェクト属性によってメンバーシップが決定されるグループであり、ダイナミック LDAP グループとは、ユーザ オブジェクト属性に基づいてグループ ユーザを取得する LDAP 検索を作成することでメンバーシップが決定されるグループです。ロールのグループ アクセス権は、グループのメンバーであるユーザにのみ影響します。

ダイナミック グループを使用する場合、LDAP クエリは、LDAP サーバで設定されているとおりに使用されます。この理由から、検索構文エラーが原因で無限ループが発生することを防ぐため、FirePOWER デバイスでは検索の再帰回数が 4 回に制限されています。

例：

Example 社の情報テクノロジー（Information Technology）部門の名前を認証するには、[管理者（Administrator）] フィールドに次のように入力します。

```
cn=itgroup,ou=groups, dc=example,dc=com
```

b) 指定したグループのいずれにも属していないユーザの [デフォルトユーザロール（Default User Role）] を選択します。

c) スタティック グループを使用する場合は、[グループ メンバー属性（Group Member Attribute）] を入力します。

例：

デフォルトの Security Analyst アクセスのためのスタティック グループのメンバーシップを示すために `member` 属性を使用する場合は、`member` と入力します。

d) ダイナミック グループを使用する場合は、[グループ メンバー URL 属性（Group Member URL Attribute）] を入力します。

例：

デフォルトの管理者アクセスに対して指定したダイナミック グループのメンバーを取得する LDAP 検索が `memberURL` 属性に含まれている場合は、`memberURL` と入力します。

ユーザ ロールを変更する場合は、変更した外部認証オブジェクトを保存/展開し、[ユーザ（Users）] 画面からユーザを削除する必要があります。次回のログイン時に、ユーザが自動的に再度追加されます。

ステップ 14 （任意） CLI/シェル ユーザを許可するように [シェルアクセスフィルタ（Shell Access Filter）] を設定します。

CLI/シェル アクセスの LDAP 認証を防止するには、このフィールドを空白にします。CLI/シェル ユーザを指定するには、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）] を選択します。
- 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

（注） 7000 または 8000 シリーズ および Firepower Management Center では、[シェルアクセスフィルタ（Shell Access Filter）] に含まれているユーザと同じユーザ名を持つ内部ユーザを作成しないでください。唯一の内部 FMC ユーザは **admin** である必要があります。[シェルアクセスフィルタ（Shell Access Filter）] に **admin** ユーザを含めないでください。

FTD では、内部ユーザに同じユーザ名を以前に設定している場合、FTD は内部ユーザに対して最初にパスワードを確認し、失敗した場合はLDAP サーバを確認します。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。

ステップ 15 （任意） LDAP サーバへの接続をテストするには、[テスト（Test）] をクリックします。

テスト出力には、有効なユーザ名と無効なユーザ名が示されます。有効なユーザ名は一意のユーザ名であり、アンダースコア（_）、ピリオド（.）、ハイフン（-）、英数字を使用できます。UI のページ サイズ制限のため、ユーザ数が 1000 を超えているサーバへの接続をテストする場合、返されるユーザの数は 1000 であることに注意してください。テストが失敗した場合は、「LDAP 認証接続のトラブルシューティング （38 ページ）」を参照してください。

ステップ 16 （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）] `uid` 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。

Microsoft Active Directory Server に接続して `uid` の代わりに UI アクセス属性を指定する場合は、ユーザ名としてこの属性の値を使用します。ユーザの完全修飾識別名も指定できます。

ヒント テストユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。サーバ設定が正しいことを確認するには、最初に [追加のテストパラメータ（Additional Test Parameters）] フィールドにユーザ情報を入力せずに [テスト（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のユーザ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 17 [保存（Save）] をクリックします。

ステップ 18 このサーバの使用を有効にします。

- Firepower Management Center：Firepower Management Center でのユーザの外部認証の有効化（28 ページ）

- FTD：SSH の外部認証の設定
- 7000 および 8000 シリーズ：7000/8000 シリーズ デバイスの外部認証について

ステップ 19 LDAP サーバで後からユーザを追加または削除する場合は、ユーザ リストを更新し、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。Firepower Management Center では、この手順は必要ありません。

a) 各 LDAP サーバの横にある[refresh] アイコン（）をクリックします。

ユーザ リストが変更された場合は、デバイスの設定変更を展開するように促すメッセージが表示されます。

b) 7000 および 8000 シリーズ デバイスの場合は、プラットフォーム設定を少し変更して、設定が古いとマークされるようにします。LDAP シェルユーザ リストの更新のために、7000 および 8000 シリーズ のプラットフォーム設定が自動的に古いとマークされることはありません。

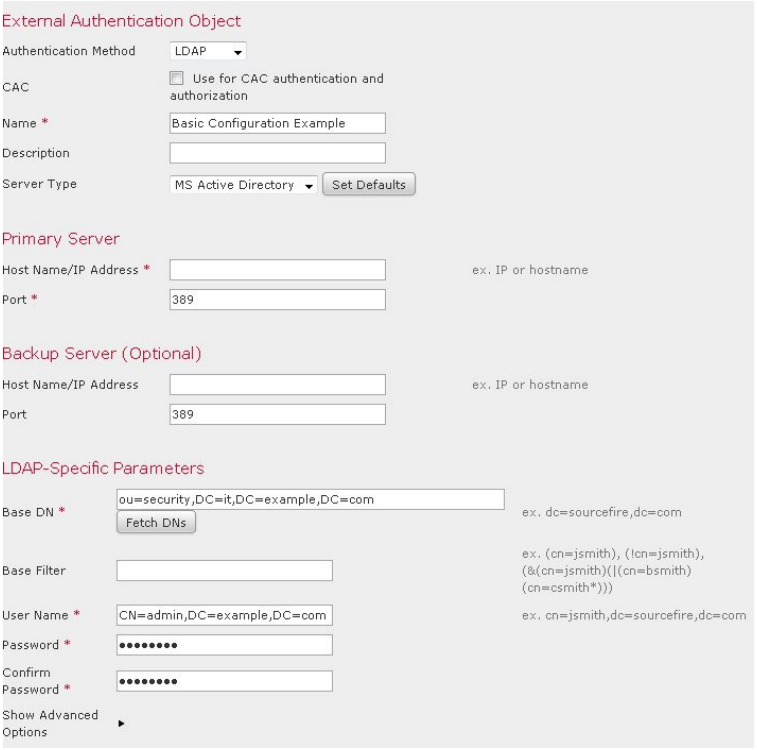
Firepower Threat Defense のプラットフォーム設定は自動的に古いとマークされるため、この回避策を実行する必要はありません。

c) 設定変更を展開します。「設定変更の展開」を参照してください。

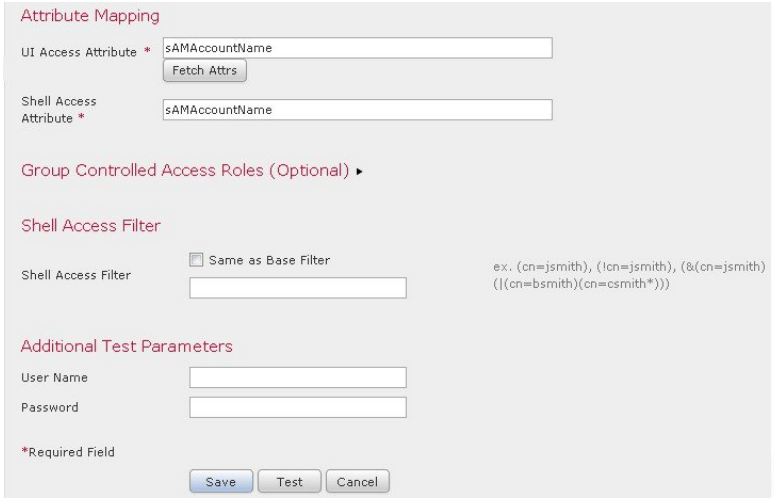
例

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。



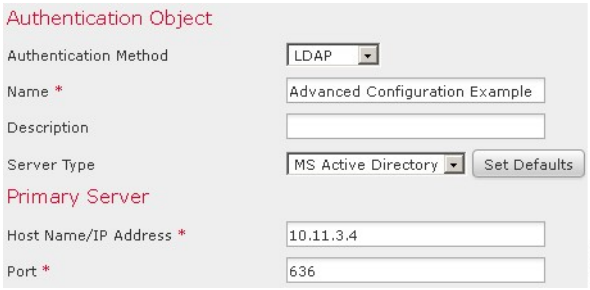
ただし、このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。サーバのタイプとして MS Active Directory を選択し、[デフォルトの設定（Set Defaults）] をクリックすると、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` に設定されます。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザ名を検索します。

また、[シェルアクセス属性（Shell Access Attribute）] が `sAMAccountName` の場合、ユーザがアプライアンスでシェル アカウントまたは CLI アカウントにログインすると、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。

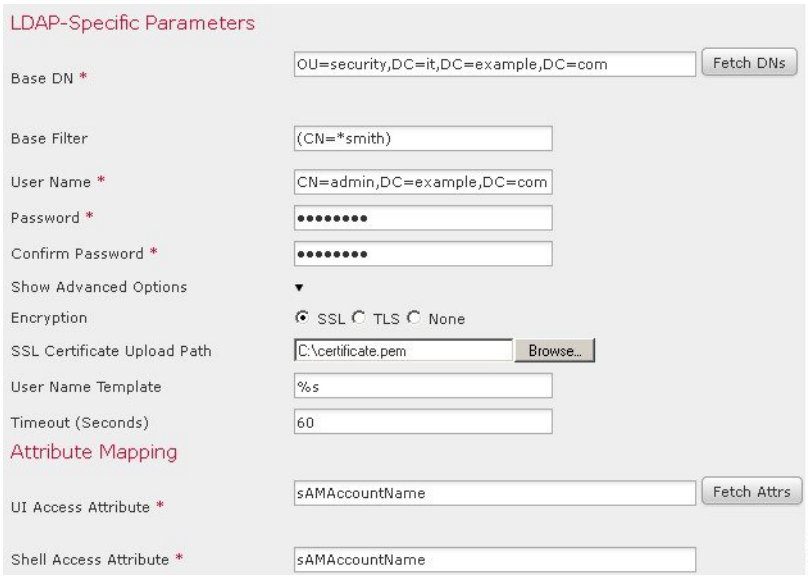
基本フィルタはこのサーバに適用されないため、Firepower システムはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバへの接続は、デフォルトの期間（または LDAP サーバで設定されたタイムアウト期間）の経過後にタイムアウトします。

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、サーバから取得するユーザを、一般名が `smith` で終わるユーザに限定します。

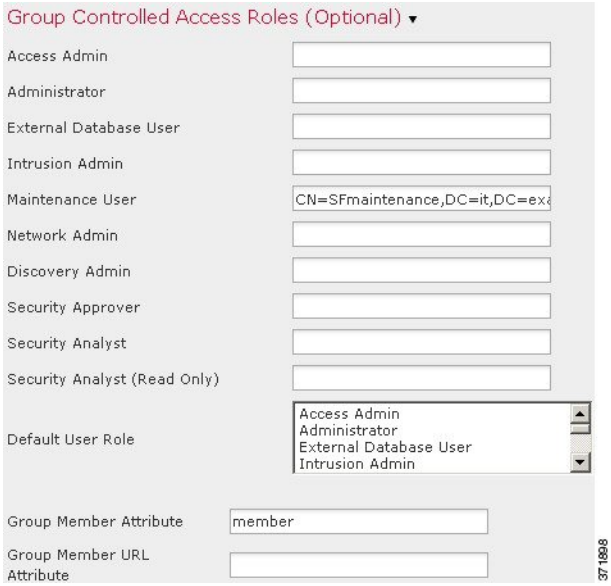


サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[タイムアウト（Timeout）] の設定により、60 秒経過後にサーバへの接続がタイムアウトします。

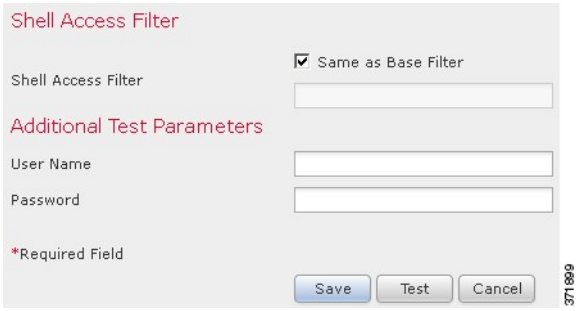
このサーバが Microsoft Active Directory Server であるため、ユーザ名の保存に `uid` 属性ではなく `sAMAccountName` 属性が使用されます。設定では、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` であることに注意してください。その結果、ユーザが Firepower システムへのログインを試行すると、Firepower システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザ名を検索します。

また、[シェルアクセス属性（Shell Access Attribute）] が `sAMAccountName` の場合、ユーザがアプライアンスで CLI/シェル アカウントにログインすると、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。

この例では、グループ設定も行われます。[メンテナンス ユーザ（Maintenance User）] ロールが、`member` グループ属性を持ち、ベース ドメイン名が `CN=SFmaintenance,=it,=example,=com` であるグループのすべてのメンバーに自動的に割り当てられます。



シェル アクセス フィルタは、基本フィルタと同一に設定されます。このため、同じユーザが Web インターフェイスを使用する場合と同様に、シェルまたは CLI を介してアプライアンスにアクセスできます。



RADIUS 外部認証オブジェクトの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FTD 7000 および 8000 シリーズ FMC	任意	管理者

デバイス管理用に外部ユーザをサポートするために、RADIUS サーバを追加します。

FTD では、CLI アクセスには一部のフィールドのみが使用されます。どのフィールドが使用されるかについては、「SSH の外部認証の設定」を参照してください。

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。

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 [RADIUS] 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 [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。

ステップ 7 （任意） [ポート（Port）] をデフォルトから変更します。

ステップ 8 [RADIUS秘密キー（RADIUS Secret Key）] を入力します。

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 （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 サーバを再試行するまでの [タイムアウト（Timeout）] を秒単位で入力します。デフォルトは 30 です。

b) バックアップ サーバ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。

c) ユーザ ロールに対応するフィールドに、各ユーザの名前を入力するか、またはこれらのロールに割り当てる必要がある属性と値のペアを指定します。

ユーザ名と属性と値のペアは、カンマで区切ります。

例：

セキュリティ アナリストとする必要があるすべてのユーザの `User-Category` 属性の値が `Analyst` である場合、これらのユーザにそのロールを付与するには、[セキュリティアナリスト（Security Analyst）] フィールドに `User-Category=Analyst` と入力します。

例：

ユーザ `jsmith` と `jdoe` に管理者ロールを付与する場合は、[管理者（Administrator）] フィールドに `jsmith, jdoe` と入力します。

例：

`User-Category` の値が `Maintenance` であるすべてのユーザにメンテナンス ユーザ ロールを付与するには、[メンテナンスユーザ（Maintenance User）] フィールドに `User-Category=Maintenance` と入力します。

d) 指定したグループのいずれにも属していないユーザの [デフォルトユーザロール（Default User Role）] を選択します。

ユーザ ロールを変更する場合は、変更した外部認証オブジェクトを保存/展開し、[ユーザ（Users）]画面からユーザを削除する必要があります。次回のログイン時に、ユーザが自動的に再度追加されます。

ステップ 11 （任意） [カスタムRADIUS属性を定義する（Define Custom RADIUS Attributes）]。

RADIUS サーバが、`/etc/radiusclient/` 内の `dictionary` ファイルに含まれていない属性の値を返し、これらの属性を使用してユーザにユーザ ロールを設定する予定の場合は、これらの属性を定義する必要があります。RADIUS サーバでユーザ プロファイルを調べると、ユーザについて返される属性を見つけることができます。

a) [属性名（Attribute Name）] を入力します。

属性を定義する場合は、英数字からなる属性名を指定します。属性名の中の単語を区切るには、スペースではなくダッシュを使用することに注意してください。

b) [属性ID（Attribute ID）] を整数で入力します。

属性 ID は整数にする必要があり、`etc/radiusclient/dictionary` ファイルの既存の属性 ID と競合していてはなりません。

c) ドロップダウン リストから [属性タイプ（Attribute Type）] を選択します。

属性のタイプ（文字列、IP アドレス、整数、または日付）も指定します。

d) [追加（Add）] をクリックして、カスタム属性を追加します。

RADIUS認証オブジェクトの作成時に、そのオブジェクトの新しいディクショナリ ファイルがデバイスの `/var/sf/userauth` ディレクトリに作成されます。追加したすべてのカスタム属性は、ディクショナリ ファイルに追加されます。

例：

シスコ ルータが接続しているネットワーク上で RADIUS サーバが使用される場合に、`Ascend-Assign-IP-Pool` 属性を使用して、特定の IP アドレス プールからログインするすべてのユーザに特定のロールを付与するとします。`Ascend-Assign-IP-Pool` は、ユーザがログインできるアドレス プールを定義する整数属性であり、割り当てられる IP アドレス プールの番号を示す整数が指定されます。

そのカスタム属性を宣言するには、属性名が `Ascend-IP-Pool-Definition`、属性 ID が `218`、属性タイプが `integer` のカスタム属性を作成します。

次に、`Ascend-IP-Pool-Definition` 属性値が `2` のすべてのユーザに対し、読み取り専用の Security Analyst 権限を付与するには、`Ascend-Assign-IP-Pool=2` 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。

ステップ 12 （任意）[シェルアクセスフィルタ（Shell Access Filter）] エリアの [管理者シェルアクセスユーザリスト（Administrator Shell Access User List）] フィールドに、CLI/シェルへのアクセス権を付与する必要があるユーザ名をカンマで区切って入力します。

これらのユーザ名がRADIUSサーバのユーザ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

このフィールドを空のままにするのは、に対して CLI/シェル アクセスの RADIUS 認証を防止するためです。

（注） 7000 または 8000 シリーズ および Firepower Management Center では、[シェルアクセスフィルタ（Shell Access Filter）] に含まれているユーザと同じユーザ名を持つ内部ユーザを削除します。Firepower Management Center の場合、内部 CLI/シェル ユーザのみが **admin** です。そのため、**admin** 外部ユーザを作成しないでください。

FTD では、内部ユーザに同じユーザ名を以前に設定している場合、FTD は内部ユーザに対して最初にパスワードを確認し、失敗した場合は RADIUS サーバを確認します。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。

ステップ 13 （任意） RADIUS サーバへの FMC 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サーバへのFMC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 テストユーザの名前とパスワードを誤って入力すると、サーバ設定が正しい場合でもテストが失敗します。サーバ設定が正しいことを確認するには、最初に [追加のテストパラメータ（Additional Test Parameters）] フィールドにユーザ情報を入力せずに [テスト（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のユーザ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 このサーバの使用を有効にします。

- Firepower Management Center：Firepower Management Center でのユーザの外部認証の有効化（28 ページ）
- FTD：SSH の外部認証の設定
- 7000 および 8000 シリーズ：7000/8000 シリーズ デバイスの外部認証について

例

単純なユーザ ロールの割り当て

次の図は、IP アドレスが 10.10.10.98 で FreeRADIUS が稼働しているサーバのサンプル RADIUS ログイン認証オブジェクトを示します。接続ではアクセスのためにポート 1812 が使用されること、および不使用期間が 30 秒を経過するとサーバ接続がタイムアウトになり、バックアップ認証サーバへの接続試行前に、サーバ接続が 3 回再試行されることに注意してください。

次の例は、RADIUS ユーザ ロール設定の重要な特徴を示します。

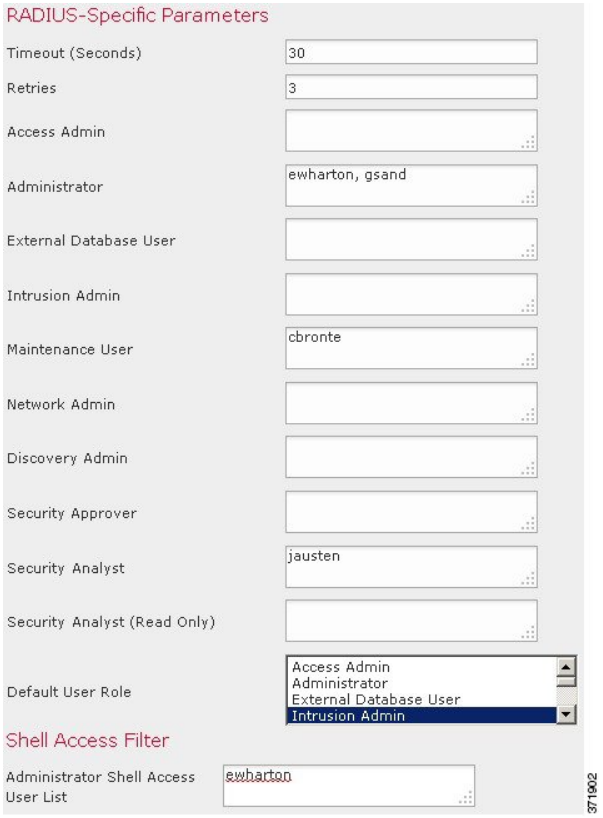
ユーザ `ewharton` および `gsand` には、Web インターフェイスの管理アクセスが付与されます。

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 `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 `ewharton` は、シェル 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。

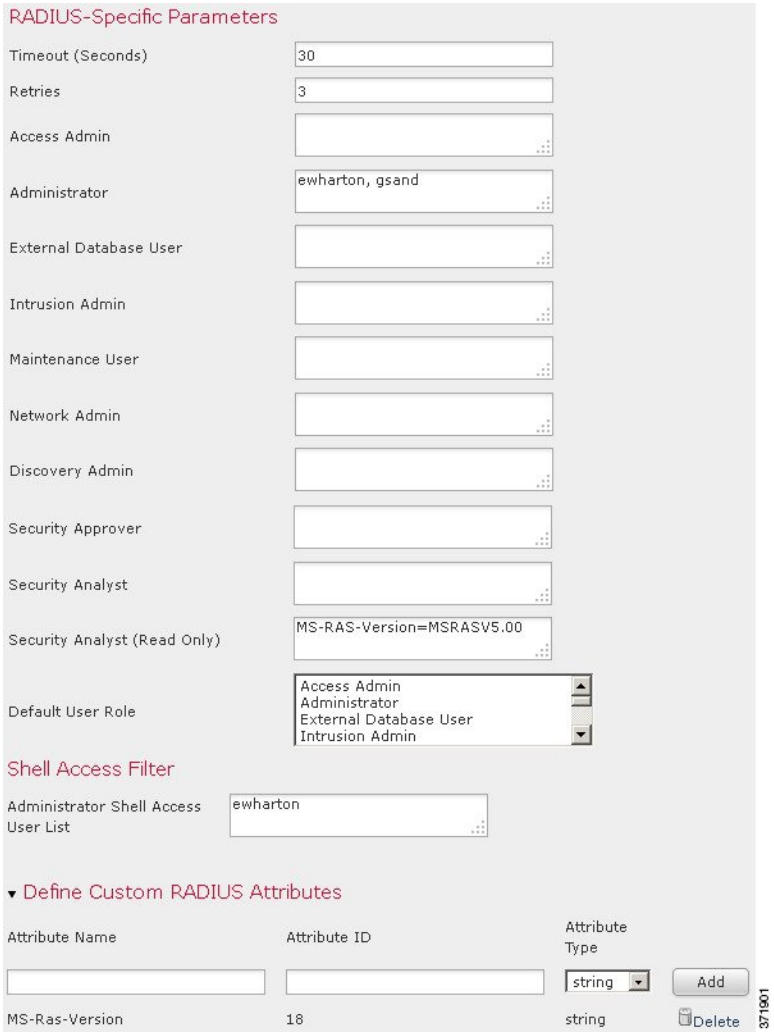


属性と値のペアに一致するユーザのロール

属性と値のペアを使用して、特定のユーザ ロールが付与される必要があるユーザ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 FreeRADIUS サーバのサンプル 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 サーバが使用されているため、1 つ以上のユーザの `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 サーバ経由で RADIUS にログインするすべてのユーザに対し、[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。



Firepower Management Center でのユーザの外部認証の有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FMC	任意	Admin

管理ユーザの外部認証を有効にすると、Firepower Management Center により外部認証オブジェクトで指定された LDAP または RADIUS サーバを使用してユーザ クレデンシャルが検証されます。

始める前に

「LDAP 外部認証オブジェクトの追加 （14 ページ）」および「RADIUS 外部認証オブジェクトの追加 （23 ページ）」に従って 1 つまたは複数の外部認証オブジェクトを追加します。

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 Web インターフェイスのユーザにデフォルトのユーザ ロールを設定します。

ロールがないユーザは、アクションを実行できません。外部認証オブジェクトで定義されたユーザ ロールは、このデフォルトのユーザ ロールをオーバーライドします。

a) [デフォルトのユーザ ロール（Default User Roles）] の値をクリックします（デフォルトでは何も選択されていません）。

a) [デフォルトのユーザロール設定（Default User Role Configuration）] ダイアログ ボックスで、使用するロールをオンにします。

b) [保存（Save）] をクリックします。

ステップ 4 使用する外部認証オブジェクトそれぞれの横にある スライダ（  ） をクリックします。複数のオブジェクトを有効にすると、ユーザは指定された順序でサーバと照合されます。サーバの順序を変更する場合は、次の手順を参照してください。

シェル認証を有効にする場合は、[シェルアクセスフィルタ（Shell Access Filter）] を含む外部認証オブジェクトを有効にする必要があります。また、CLI/シェル アクセスのユーザは、認証オブジェクトがリストの順序で最も高いサーバに対してのみ認証できます。

ステップ 5 （任意） 認証要求が行われたときに認証サーバがアクセスされる順序を、サーバをドラッグ アンド ドロップして変更できます。

ステップ 6 外部ユーザに CLI/シェル アクセスを許可する場合は、**[シェル認証（Shell Authentication）]** > **[有効（Enabled）]** を選択します。

1 番目の外部認証オブジェクト名は、CLI/シェル アクセスに使用されるのは 1 番目のオブジェクトだけであることを示すため、[有効（Enabled）] オプションの横に表示されます。

ステップ 7 [Save and Apply] をクリックします。

管理対象デバイスのユーザに対する外部認証の有効化

デバイスの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。使用している管理対象デバイス タイプに応じて、次の手順を参照してください。

- Firepower Threat Defense：SSH の外部認証の設定
- 7000 および 8000 シリーズ：7000/8000 シリーズ デバイスの外部認証について

LDAP を使用した共通アクセス カード認証の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FMC 7000 および 8000 シリーズ	任意	管理者（Administrator） Network Admin

組織で共通アクセス カード（CAC）を使用している場合は、Web インターフェイスにログインしている FMC ユーザまたは 7000 および 8000 シリーズ ユーザを認証するように LDAP 認証を設定できます。CAC 認証により、ユーザは、デバイスに個別のユーザ名とパスワードを指定せずに直接ログインすることができます。

CAC 認証ユーザは、Electronic Data Interchange Personal Identifier（EDIPI）番号により識別されます。

非アクティブ状態が 24 時間続くと、デバイスにより CAC 認証ユーザが [ユーザ（Users）] タブから削除されます。その後のログインのたびにユーザが再度追加されますが、ユーザ ロールに対する手動の変更は再設定する必要があります。

始める前に

CAC 設定プロセスの一部としてユーザ証明書を有効にするには、ブラウザに有効なユーザ証明書（この場合は CAC を介してユーザのブラウザに渡される証明書）が存在している必要があります。CAC 認証および認可の設定後に、ネットワーク上のユーザはブラウズ セッション期間にわたって CAC 接続を維持する必要があります。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

手順

ステップ 1 組織の指示に従い CAC を挿入します。

ステップ 2 ブラウザで **https://***ipaddress_or_hostname***/** に移動します。ここで、*ipaddress* または *hostname* は使用しているデバイスに対応します。

ステップ 3 プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。

ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ステップ 5 ログインページで、[ユーザ名（Username）] フィールドと [パスワード（Password）] フィールドに、管理者権限を持つユーザとしてログインします。CAC クレデンシャルを使用してログインすることは、まだ**できません**。

ステップ 6 **[システム（System）] > [ユーザ（Users）] > [外部認証（External Authentication）]** を選択します。

ステップ 7 「LDAP 外部認証オブジェクトの追加 （14 ページ）」の手順に従い、CAC 専用の LDAP 認証オブジェクトを作成します。次の設定を行う必要があります。

- **[CAC]** チェックボックス。
- **[LDAP固有のパラメータ（LDAP-Specific Parameters）] > [詳細オプションを表示（Show Advanced Options）] > [ユーザ名テンプレート（User Name Template）]**。
- **[属性マッピング（Attribute Mapping）] > [UIアクセス属性（UI Access Attribute）]**。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 「Firepower Management Center でのユーザの外部認証の有効化 （28 ページ）」または「7000/8000 シリーズ デバイスへの外部認証の有効化」の説明に従って、外部認証と CAC 認証を有効にします。

ステップ 10 **[System] > [Configuration]** を選択し、[HTTPS証明書（HTTPS Certificate）] をクリックします。

ステップ 11 HTTPS サーバ証明書をインポートし、必要に応じて「HTTPS サーバ証明書のインポート」で説明する手順に従います。

使用する予定の CAC で、HTTPS サーバ証明書とユーザ証明書が同じ認証局（CA）により発行される必要があります。

ステップ 12 [HTTPS ユーザ証明書設定（HTTPS User Certificate Settings）] の [ユーザ証明書を有効にする（Enable User Certificates）] を選択します。詳細については、「有効な HTTPS クライアント証明書の強制」を参照してください。

ステップ 13 「CAC クレデンシャルを使用した Firepower Management Center へのログイン」または「CAC クレデンシャルを使用した 7000 または 8000 シリーズ デバイスへのログイン」に従い、デバイスにログインします。

Webインターフェイス用のユーザ ロールのカスタマイズ

各ユーザ アカウントは、ユーザ ロールで定義する必要があります。このセクションでは、ユーザ ロールを管理する方法と、Web インターフェイス アクセス用のカスタム ユーザ ロールを設定する方法について説明します。ユーザ ロールの詳細については、「Web インターフェイスのユーザ ロール （4 ページ）」を参照してください。

（注） 管理対象デバイスの CLI/シェル ユーザ ロールは、設定ロールと基本ロールに制限されています。詳細については、「CLI ユーザ ロール （5 ページ）」を参照してください。

カスタム ユーザ ロールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FMC 7000 & 8000 シリーズ	任意	管理者

カスタム ユーザ ロールには、メニューベースのアクセス許可とシステム アクセス許可の任意のセットを持たせることができます。また、完全にオリジナルのものを作成することや、定義済みのユーザ ロールまたは別のカスタム ユーザ ロールからコピーすることや、別のデバイスからインポートすることができます。

手順

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [ユーザロール（User Roles）] タブをクリックします。

ステップ 3 次のいずれかの方法で新しいユーザ ロールを追加します。

- [ユーザ ロールの作成（Create User Role）] をクリックします。
- コピーするユーザ ロールの横にある[copy] アイコン（）をクリックします。
- 別のデバイスからカスタム ユーザ ロールをインポートします。
  1. 古いデバイスで、[export] アイコン（）をクリックしてロールを PC に保存します。
  2. 新しいデバイスで、**[システム（System）]** > **[ツール（Tools）]** > **[インポート/エクスポート（Import/Export）]** を選択します。
  3. [パッケージのアップロード（Upload Package）] をクリックし、指示に従って保存したユーザ ロールを新しいデバイスにインポートします。

ステップ 4 新しいユーザ ロールの [名前（Name）] を入力します。ユーザ ロール名では、大文字と小文字が区別されます。

ステップ 5 （任意） [説明（Description）] を追加します。

ステップ 6 新しいロールの [メニューベースのアクセス許可（Menu-Based Permissions）] を選択します。

アクセス許可を選択すると、その下位にあるアクセス許可もすべて選択され、複数値を持つアクセス許可では最初の値が使用されます。上位のアクセス許可をクリアすると、下位のアクセス許可もすべてクリアされます。アクセス許可を選択しても、下位のアクセス許可を選択しない場合、アクセス許可がイタリックのテキストで表示されます。

カスタム ロールのベースとして使用する事前定義ユーザ ロールをコピーすると、その事前定義ロールに関連付けられているアクセス許可が事前選択されます。

カスタム ユーザ ロールに制限付き検索を適用できます。これらの検索では、[分析（Analysis）] メニューの下にあるテーブルやページでユーザが確認できるデータが制限されます。制限付き検索を設定するには、最初に、プライベートの保存済み検索を作成し、該当するメニューベースのアクセス許可の下で [制限付き検索（Restrictive Search）] ドロップダウン メニューからその検索を選択します。

ステップ 7 （任意）新しいロールのデータベース アクセス権限を設定するには、[外部データベース アクセス（External Database Access）] チェックボックスをオンにします。

このオプションにより、JDBC SSL 接続に対応しているアプリケーションを用いて、データベースに対して読み取り専用アクセスが可能になります。デバイスの認証を行うサードパーティのアプリケーションについては、システム設定内でデータベース アクセスを有効にする必要があります。

ステップ 8 （任意）新しいユーザ ロールのエスカレーション権限を設定するには、「ユーザ ロール エスカレーションの有効化 （34 ページ）」を参照してください。

ステップ 9 [保存（Save）] をクリックします。

例

アクセス コントロール関連機能のカスタム ユーザ ロールを作成して、ユーザのアクセス コントロールおよび関連付けられたポリシーの表示、変更権限の有無を指定できます。

次の表に、作成可能なカスタム ロールと例として挙げたロールでそれぞれ与えられるユーザ権限を示します。表にはそれぞれのカスタム ロールに必要な権限が記載されています。この例では、ポリシー承認者（Policy Approver）はアクセス コントロール ポリシーと侵入ポリシーの表示が可能です（変更はできません）。また、ポリシー承認者は設定の変更をデバイスに展開することもできます。

表 *1*: アクセス制御のカスタム ロールの例

カスタム ロールの権限	例：アクセス コントロール編集者	例：侵入およびネットワーク分析編集者	例：ポリシー承認者
アクセス制御	可	不可	可
アクセス コントロール ポリシー	可	不可	可
アクセス制御ポリシーの変更	可	不可	不可
侵入ポリシー	不可	可	可
侵入ポリシーの変更	不可	可	不可
設定をデバイスに展開	不可	不可	可

ユーザ ロールの非アクティブ化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FMC 7000 & 8000 シリーズ	任意	管理者

ロールを非アクティブにすると、そのロールが割り当てられているすべてのユーザから、そのロールと関連するアクセス許可が削除されます。事前定義ユーザ ロールは削除できませんが、非アクティブにすることができます。

マルチドメイン展開では、現在のドメインで作成されたカスタム ユーザ ロールが表示されます。これは編集できます。先祖ドメインで作成されたカスタム ユーザ ロールも表示されますが、これは編集できません。下位のドメインのカスタム ユーザ ロールを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [ユーザロール（User Roles）] タブをクリックします。

ステップ 3 アクティブまたは非アクティブにするユーザ ロールの横にあるスライダをクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

Lights-Out Management を含むロールが割り当てられているユーザがログインしているときに、このロールを非アクティブにしてから再度アクティブにする場合、またはユーザのログイン セッション中にバックアップからユーザまたはユーザ ロールを復元する場合、そのユーザは Web インターフェイスに再度ログインして、IPMItool コマンドへのアクセスを再度取得する必要があります。

ユーザ ロール エスカレーションの有効化

Firepower Management Center の場合、カスタム ユーザ ロールにアクセス許可を付与し、パスワードを設定することで、ベース ロールの特権に加え、他のターゲット ユーザ ロールの特権を一時的に取得できます。この機能により、あるユーザが不在であるときにそのユーザを別のユーザに容易に置き換えることや、拡張ユーザ特権の使用状況を緊密に追跡することができます。デフォルトのユーザ ロールでは、エスカレーションはサポートされません。

たとえば、ユーザのベース ロールに含まれている特権が非常に限られている場合、そのユーザは管理アクションを実行するために管理者ロールにエスカレーションできます。ユーザが各自のパスワードを使用するか、または指定された別のユーザのパスワードを使用することができ

るように、この機能を設定できます。2 番目のオプションでは、該当するすべてのユーザのための 1 つのエスカレーション パスワードを容易に管理できます。

ユーザ ロール エスカレーションを設定するには、次のワークフローを参照してください。

手順

ステップ 1 エスカレーション ターゲット ロールの設定 （35 ページ）。エスカレーション ターゲット ロールにすることができるユーザ ロールは一度に 1 つだけです。

ステップ 2 エスカレーション用のカスタム ユーザ ロールの設定 （36 ページ）。

ステップ 3 （ログイン後のユーザの場合）ユーザ ロールのエスカレーション （37 ページ）

エスカレーション ターゲット ロールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FMC	任意	管理者

各自のユーザ ロール（事前定義またはカスタム）をシステム全体でのエスカレーション ターゲット ロールとして機能するように割り当てることができます。これは、カスタム ロールのエスカレーション先となるロールです（エスカレーションが可能な場合）。エスカレーション ターゲット ロールにすることができるユーザ ロールは一度に 1 つだけです。各エスカレーションはログイン セッション期間中保持され、監査ログに記録されます。

手順

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [ユーザ ロール（User Roles）] をクリックします。

ステップ 3 [アクセス許可エスカレーションの設定（Configure Permission Escalation）] をクリックします。

ステップ 4 [エスカレーションターゲット（Escalation Target）] ドロップダウン リストからユーザ ロールを選択します。

ステップ 5 [OK] をクリックして変更を保存します。

エスカレーション ターゲット ロールの変更は即時に反映されます。エスカレーションされたセッションのユーザには、新しいエスカレーション ターゲットのアクセス許可が付与されます。

エスカレーション用のカスタム ユーザ ロールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FMC	任意	管理者

エスカレーションを有効にするユーザは、エスカレーションを有効にしたカスタムユーザ ロールに属している必要があります。この手順では、カスタム ユーザ ロールのエスカレーションを有効にする方法について説明します。

カスタム ロールのエスカレーション パスワードを設定するときには、部門のニーズを考慮してください。多数のエスカレーションユーザを容易に管理するには、別のユーザを選択し、そのユーザのパスワードをエスカレーション パスワードとして使用することができます。そのユーザのパスワードを変更するか、またはそのユーザを非アクティブにすると、そのパスワードを必要とするすべてのエスカレーションユーザが影響を受けます。この操作により、特に一元管理できる外部認証ユーザを選択した場合に、ユーザ ロール エスカレーションをより効率的に管理できます。

始める前に

「エスカレーション ターゲット ロールの設定 （35 ページ）」に従って対象ユーザ ロールを設定します。

手順

ステップ 1 「カスタム ユーザ ロールの作成 （32 ページ）」の説明に従って、カスタム ユーザ ロールの設定を開始します。

ステップ 2 [システム権限（System Permissions）] エリアで、[このロールをエスカレーションする：（Set this role to escalate to:）] チェック ボックスをオンにします。

現在のエスカレーション ターゲット ロールは、チェックボックスの横に表示されます。

ステップ 3 このロールがエスカレーションするときに使用するパスワードを選択します。次の2つの対処法があります。

- このロールを持つユーザがエスカレーション時に自分のパスワードを使用するようにするには、[割り当てられたユーザのパスワードを使用して認証（Authenticate with the assigned user’s password）] を選択します。
- このロールを持つユーザが別のユーザのパスワードを使用するようにするには、[指定したユーザのパスワードを使用して認証（Authenticate with the specified user’s password）] を選択して、そのユーザ名を入力します。

（注） 別のユーザのパスワードで認証するときには、任意のユーザ名（非アクティブなユーザまたは存在しないユーザを含む）を入力できます。エスカレーションにパスワードが使用されるユーザを非アクティブにすると、そのパスワードを必要とするロールが割り当てられているユーザのエスカレーションが不可能になります。この機能を使用して、必要に応じてエスカレーション機能をただちに削除できます。

ステップ 4 [保存（Save）] をクリックします。

ユーザ ロールのエスカレーション

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	FMC	任意	任意

エスカレーション権限のあるカスタムユーザ ロールを割り当てられたユーザは、いつでもターゲット ロールの権限にエスカレーションできます。エスカレーションはユーザ設定に影響しないことに注意してください。

手順

ステップ 1 ユーザ名の下にあるドロップダウン リストから、[アクセス許可のエスカレーション（Escalate Permissions）] を選択します。

このオプションが表示されない場合は、管理者はユーザ ロールのエスカレーションを有効にしていません。

ステップ 2 認証パスワードを入力します。

ステップ 3 [エスカレーション（Escalate）] をクリックします。これで、現行ロールに加え、エスカレーション ターゲット ロールのすべてのアクセス許可が付与されました。

エスカレーションはログイン セッションの残り期間にわたって保持されます。ベース ロールの特権だけに戻すには、ログアウトしてから新しいセッションを開始する必要があります。

Cisco Security Manager のシングル サインオンの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意	任意	ASA FirePOWER	任意	管理者

シングル サインオンにより、Cisco Security Manager（CSM）バージョン 4.7 以上と Firepower Management Center を統合して、ログインの追加認証なしで CSM から Firepower Management Center にアクセスできるようにすることができます。ASA FirePOWER モジュールを使用して ASA を管理するときは、モジュールに展開したポリシーの変更が必要となる場合もあります。CSM でFirepower Management Centerを管理することを選択し、Web ブラウザで起動します。

（注） 組織で認証に CAC が使用されている場合は、シングル サインオンでログインできません。

始める前に

- NAT 環境では、Firepower Management Centerと CSM は NAT 境界の同じ側に存在している必要があります。

手順

ステップ 1 CSMから、接続を識別するシングルサインオン共有暗号キーを生成します。詳細については、CSM のマニュアルを参照してください。

ステップ 2 Firepower Management Center から、**[System]** > **[Users]** を選択します。

ステップ 3 [CSM シングル サインオン（CSM Single Sign-on）] を選択します。

ステップ 4 CSM ホスト名または IP アドレスとサーバのポートを入力します。

ステップ 5 CSM から生成した**共有キー**を入力します。

ステップ 6 （任意） Firepower Management Center のプロキシ サーバを使用して CSM と通信する場合は、[接続にプロキシを使用（Use Proxy For Connection）] チェックボックスをクリックします。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 [証明書の確認（Confirm Certificate）] をクリックして証明書を保存します。

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、選択したサーバへの接続が失敗したか、または必要なユーザ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ユーザにあることを確認します。
- ユーザ名が、LDAP サーバ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、ユーザのユーザ 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。

- サーバを正しく指定していることを確認します。
  - サーバの 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に TCP/IP でアクセスできることを確認します。
  - サーバ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。
  - シェル アクセスを認証する場合は、サーバ接続に 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シェル 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おり、有効な比較演算子を使用していることを確認します。
- より制限された基本フィルタをテストするには、特定のユーザだけを取得するため、フィルタにそのユーザ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。

- テストユーザを使用する場合、ユーザ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。
- テストユーザを使用する場合、ユーザ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 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シェル 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または制限を緩めて使用することができます。

ユーザ アカウントの履歴

機能	バージョン	詳細
FTD SSH アクセスの外部認証	6.2.3	LDAP または RADIUS認証を使用して FTD への SSH の外部認証を設定できるようになりました。 新しい/変更された画面： **[デバイス（Devices）] > [プラットフォームの設定（Platform Settings）] > [外部認証（External Authentication）]** サポートされるプラットフォーム FTD