Firewall Management Centerユーザー

Firewall Management Center には、Web および 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。ユーザーアカウントを使用して Firewall Management Center にログインする方法の詳細については、Management Center へのログインを参照してください。

ユーザについて

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。

Web インターフェイスおよび CLI によるアクセス

Firewall Management Center には、Web インターフェイス、CLI（コンソール（シリアルポートまたはキーボードとモニターのいずれか）から、または管理インターフェイスへの SSH を使用してアクセス可能）、および Linux シェルがあります。管理 UI の詳細については、システム ユーザー インターフェイスを参照してください。

Firewall Management Center ユーザー タイプと、それらがアクセスできる UI に関する次の情報を参照してください。

- admin ユーザー：Firewall Management Center は 2 種類の内部 **admin** ユーザーをサポートしています。Web インターフェイスのユーザーと、CLI アクセス権が付与されたユーザーです。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、[システム（System）]（⚙）> **[ユーザー（Users）]** > [ユーザー（Users）] を使用します。CLI の **admin** のパスワードを変更するには、Firewall Management Center CLI コマンド **configure password** を使用します。）
- 内部ユーザー：Web インターフェイスで追加された内部ユーザーには、Web インターフェイスのアクセス権のみが付与されます。
- 外部ユーザー：外部ユーザーには Web インターフェイスのアクセス権が付与され、オプションで CLI のアクセス権を設定できます。
- SSO ユーザー：SSO ユーザーには Web インターフェイスのアクセス権のみが付与されます。

⚠

注意 CLI 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。Cisco TAC または Firewall Management Center 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。CLI ユーザーは Linux シェルで `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、次のことを強く推奨します。

- CLI アクセス権を持つ外部ユーザーのリストを適切に制限してください。
- 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。

ユーザ ロール

CLI ユーザロール

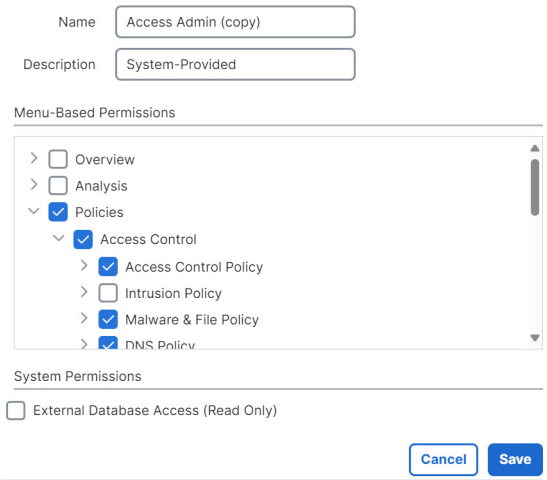
Firewall Management Center の CLI 外部ユーザにはユーザ ロールがありません。そのため、それらのユーザは使用可能なすべてのコマンドを使用できます。

Web インターフェイスのユーザ ロール

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。

定義済みのユーザーロールに割り当てられた権限を表示するには、定義済みのロールに基づいてカスタムロールを作成する場合と同様に、ロールの [コピー（Copy）] () をクリックします。これにより、割り当てられたすべての権限を確認できます。

図 *1*: ユーザーロール権限の表示



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

アクセス管理者（Access Admin）

[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

[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（読み取り専用）

JDBC SSL 接続をサポートするアプリケーションを使用したデータベースへの読み取り専用アクセスを提供します。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ーは、[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。このロールの機能には Web インターフェイスが含まれていないため、容易なサポートとパスワード変更の目的でのみアクセスが提供されます。

侵入管理者（Intrusion Admin）

[Policies] メニューと [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 ユーザー（Maintenance User）

監視機能と保守機能へのアクセスを提供します。メンテナンス ユーザーは、[Health] メニューや [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

[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 [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。

Security Analyst

セキュリティイベント分析機能へのアクセスと [Overview] メニュー、[Analysis] メニュー、[Health] メニュー、[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。

Security Analyst (Read Only)

[Overview] メニュー、[Analysis] メニュー、[Health] メニュー、[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。

このロールを持つユーザは、次のこともできます。

- 特定のデバイスのヘルスモニタのページから、トラブルシューティング ファイルを生成してダウンロードする。
- ユーザ設定で、ファイルのダウンロードの設定を行う。
- ユーザ設定で、イベントビューのデフォルトのタイムウィンドウを設定する（[Audit Log Time Window] を除く）。

セキュリティ承認者

[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。

脅威インテリジェンス ディレクタ（TID）ユーザー

[Intelligence] メニューの脅威インテリジェンスディレクタ設定にアクセスできます。Threat Intelligence Director（TID）ユーザーは、TID の表示および設定が可能です。

ユーザ パスワード

Firewall Management Center の内部ユーザーアカウントのパスワードには、Lights-Out Management（LOM）が有効な場合と無効な場合に応じて、次のルールが適用されます。外部認証されたアカウントまたはセキュリティ認定コンプライアンスが有効になっているシステムには、異なるパスワード要件が適用されます。詳細については、Firewall Management Center の外部認証の設定 （14 ページ）とセキュリティ認定準拠を参照してください。

Firewall Management Center の初期設定時に、**admin** ユーザーは、以下の表に記載されている強力なパスワード要件に準拠するようにアカウントパスワードを設定する必要があります。物理 Firewall Management Center の場合、LOM が有効になっている強力なパスワード要件が使用され、仮想 Management Center の場合、LOM が有効になっていない強力なパスワード要件が使用されます。この時点で、システムは web インターフェイスの **admin** と CLI アクセスの **admin** のパスワードを同期します。初期設定後、Web インターフェイスの **admin** は強力なパスワード要件を削除できますが、CLI アクセスの **admin** は、LOM が有効になっていない状態では、常に強力なパスワード要件に準拠している必要があります。

	LOM が有効になっていない	LOM が有効になっている
パスワードの強度チェックがオンになっている	パスワードには以下を含める必要があります。 • 8 文字以上または管理者がユーザーに設定した文字数のいずれか大きい方。 • 同じ文字が 3 文字以上連続していない • 1 つ以上の小文字 • 少なくとも 1 つの大文字 • 少なくとも 1 つの数字 • ! など、少なくとも 1 つの特殊文字@ # * - _ + システムは、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列も含まれる特殊なディクショナリと照合してパスワードをチェックします。	パスワードには以下を含める必要があります。 • 8 ～ 20 文字（MC 1000、MC 2500、および MC 4500 の場合、上限は 20 文字ではなく 14 文字） • 同じ文字が 3 文字以上連続していない • 1 つ以上の小文字 • 少なくとも 1 つの大文字 • 少なくとも 1 つの数字 • ! など、少なくとも 1 つの特殊文字@ # * - _ + 特殊文字のルールは、物理 Firewall Management Center のシリーズ間で異なります。特殊文字の選択を、上記の最後の箇条書きに記載されている特殊文字に制限することをお勧めします。 パスワードにユーザー名を含めないでください。 システムは、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列も含まれる特殊なディクショナリと照合してパスワードをチェックします。

	LOM が有効になっていない	LOM が有効になっている

パスワードの強度チェックがオフになっている	パスワードは、管理者がユーザーに対して設定した最小文字数以上である必要があります。（詳細については、内部ユーザーの追加または編集（11 ページ）を参照してください）。	パスワードには以下を含める必要があります。
		• 8 ～ 20 文字（MC 1000、MC 2500、および MC 4500 の場合、上限は 20 文字ではなく 14 文字）
		• 次の 4 つのカテゴリの少なくとも 3 つのカテゴリに属する文字：
		  • 大文字の英字
		  • 小文字の英字
		  • ディジット
		  • ! などの特殊文字@ # * - _ +
		特殊文字のルールは、物理 Firewall Management Center のシリーズ間で異なります。特殊文字の選択を、上記の最後の箇条書きに記載されている特殊文字に制限することをお勧めします。
		パスワードにユーザー名を含めないでください。

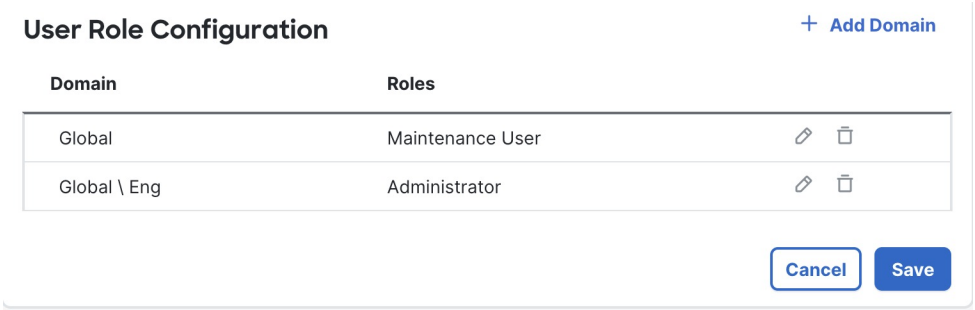
ユーザおよびドメイン

マルチドメイン型展開では、管理者アクセス権限があるドメインでユーザーアカウントを作成できます。

ドメイン内のユーザーロール

ユーザー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、あるユーザー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。

図 *2:* ドメインごとのユーザーロール



[ユーザー管理（User Management）]

ユーザーは作成されたドメインでのみ表示されます。

現在のドメインにユーザーを追加し、サブドメインでユーザーロールを割り当てた場合、そのユーザーはサブドメインでロールを持っていても、現在のドメインの[ユーザー（User）]ページにのみ表示されます。たとえば、グローバルドメインからユーザー **leaf** を追加して **Leaf1** のロールを割り当てる場合、ユーザーを追加したときにグローバルドメインにいたため、グローバルドメインに表示されます。

図 *3:* グローバルドメインのユーザー

Username	Real Name	Domains
admin		Global
leaf		Global \ Leaf1

ドメインを **Leaf1** に変更すると、ユーザー **leaf** は表示されませんが、Leaf1 サブドメインから直接追加されたユーザー **test** は表示されます。

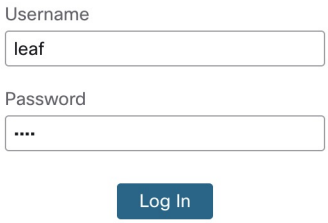
図 *4:* サブドメインユーザー

Username	Real Name	Domains
test		Global \ Leaf1

ログイン

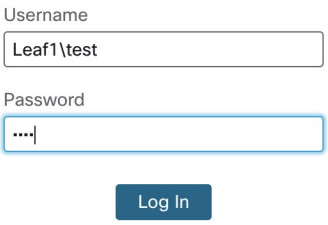
グローバルドメインから追加されたユーザーは、ロールがサブドメインのみにある場合でも、ユーザー名のみでログインできます。この例では、**leaf** には **Leaf1** サブドメインのユーザーロールのみがありますが、グローバルから追加されたため、ログインにサブドメインを含めないでください。

図 *5*：グローバルで追加されたユーザーのログイン



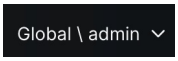
サブドメインに直接追加されたユーザーは、どのドメインにユーザーが追加されたかに応じて、サブドメインをログイン名の一部としてFirewall Management Centerにログインする必要があります。（サブドメイン*1*\サブドメイン*2*\ユーザー名）。**グローバル**親ドメインを入力する必要はありません。たとえば、**test** は **Leaf1** サブドメインから追加されたため、ログイン名にLeaf1 を含める必要があります。

図 *6*：グローバルドメインユーザーのログイン



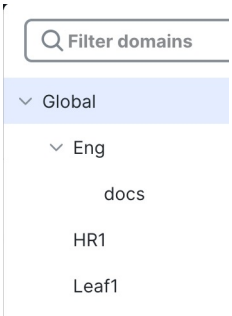
ログインすると、ユーザー名が追加されたドメインに配置されます。たとえば、管理者ユーザーはデフォルトでグローバルドメインに設定されます。

図 *7*：ログイン時のユーザードメイン



ただし、ログイン後に、下矢印をクリックしてサブドメインに変更できます。

図 *8*：サブドメインへの変更



Firewall Management Center のユーザーアカウントの注意事項と制約事項

- Firewall Management Center には、すべてのアクセス形式のローカルユーザーアカウントとして **admin** ユーザーが含まれています。**admin** ユーザーは削除できません。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。
- デフォルトでは、Firewall Management Center のすべてのユーザー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ー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。
  - 同時に開くことができる読み取り専用セッションと読み取り/書き込みセッションの数には、ユーザー定義の制限はありません。

  すべてのユーザーのこれらの設定は、システム設定として変更できます（[システム（System）]（⚙） > **[構成（Configuration）]** > **[ユーザー構成（User Configuration）]**）ユーザーの設定を参照してください。
- 初期設定時にデフォルトのアクセスロールをユーザーに割り当てる場合は、最小限の権限の原則に従うようにしてください。ユーザーがログイン情報を使用してシステムに初めてログインすると、アカウントにこのデフォルトのアクセスロールが割り当てられます。デフォルトのアクセスロールは、誰もがシステムにログインするために必要な最小限の権限にすることを推奨します。たとえば、共通ユーザーにはデフォルトのアクセスロールとしてセキュリティアナリスト（読み取り専用）ロールを付与し、管理者を別の管理者のグループに追加して完全な管理者権限を付与することができます。デフォルトのアクセスロールを割り当てるときに最小権限の原則に従わない場合、以降のログインでユーザーに意図しない権限レベルが割り当てられる可能性があります。これにより、必要なアクセスロールを超える権限がユーザーに付与される場合があります。このガイドラインは、すべてのユーザー（内部ユーザー、外部ユーザー、または CAC ユーザー）に適用されます。

  デフォルトのアクセスロールでログインしているユーザーが一時的に権限を昇格する必要がある場合、管理者権限を持つユーザーは、より高い権限を持つロールを割り当てることで、必要な高いレベルのアクセスを一時的にそのユーザーに提供できます。この権限は、非アクティブな状態が 24 時間続くと取り消され、ユーザーはデフォルトのアクセスロールに戻ります。

  ユーザーがより高い権限レベル（システム管理者など）に永続的なアクセスロールを再割り当てする必要がある場合は、グループ制御アクセスロール方式を使用して、管理者アクセス権をユーザーに付与します。この方法では、指定されたアクセスロールが 24 時間を

超えて保持され、ユーザーはグループ割り当てに従って正しい権限レベルを持つことが保証されます。グループ制御アクセスロールの設定の詳細については、「Add an LDAP External Authentication Object for Management Center」の項を参照してください。

FMC のユーザーアカウントの要件と前提条件

サポート モデル

Management Center

サポートされるドメイン

- SSO 設定：グローバルのみ。
- 他のすべての機能：すべて。

ユーザ ロール

- SSO設定：内部で認証された、またはLDAPまたはRADIUSによって認証された管理ロールを持つユーザーのみが SSO を設定できます。
- その他すべての機能：管理者ロールを持つすべてのユーザー。
- LDAP を使用した共通アクセス カード認証の設定 （32 ページ）もネットワーク管理者ロールをサポートしています。

内部ユーザーの追加または編集

この手順では、Firewall Management Center のカスタム内部ユーザー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）]>[ユーザー（Users）]>[ユーザー（Users）]には、手動で追加した内部ユーザーと、LDAPまたはRADIUS認証でユーザーがログインしたときに自動的に追加された外部ユーザーの両方が表示されます。外部ユーザーについては、より高い権限を持つロールを割り当てると、この画面のユーザー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。

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。

（注） 複数の管理者ユーザーがFirewall Management Centerで同時に新しいユーザーを作成することは避けてください。ユーザーデータベースアクセスの競合によってエラーが発生する可能性があります。

手順

ステップ1 [システム（System）]（⚙）>**[ユーザー（Users）]**を選択します。

ステップ2 新しいユーザを作成するには、以下の手順を実行します。

a) [Create User] をクリックします。

b) [ユーザー名（User Name）] に入力します。

ユーザー名は、次の制限に従う必要があります。

- 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。
- 文字は大文字と小文字を使用できます。
- ピリオド（.）、ハイフン（-）、アンダースコア（_）以外の句読点または特殊文字は使用できません。

ステップ3 既存のユーザーを編集するには、編集するユーザーレイヤの横にある [編集（Edit）]（✎）をクリックします。

ステップ4 [実際の名前（Real Name）]：アカウントが属しているユーザーまたは部門を識別するための説明情報を入力します。

ステップ5 （任意）[電子メールアドレス（Email Address）]：電子メールアドレスを入力します。シスコでは、商談や製品更新の案内、新しいリリースの導入に関するニュースレターの提供、その他の製品関連通信の共有を目的として、電子メールアドレスを収集し、使用しています。

ステップ6 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ーに対しては、[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。外部ユーザー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7 [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8 [ログイン失敗の最大回数（Maximum Number of Failed Logins）] を設定します。

各ユーザーが、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指定する整数を、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 9 [パスワードの最小長（Minimum Password Length）] を設定します。

ユーザーのパスワードの必須最小長（文字数）を指定する整数を、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 10 [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。

ユーザー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 **0** で、パスワードは期限切れにならないことを示します。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 11 [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何日前に、ユーザー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かを入力します。デフォルト設定は **0** 日間です。

ステップ 12 以下の**オプション**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ー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。パスワード強度チェックが有効になっている場合、パスワードは、ユーザ パスワード （5 ページ）で説明されている強力なパスワードの要件に従う必要があります。
- [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、ユーザーのログインセッションが終了しないようにします。管理者ロールが割り当てられているユーザーを除外することはできません。

ステップ 13 [ユーザーロールの設定（User Role Configuration）] エリアで、ユーザーロールを割り当てます。ユーザー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ー ロールのカスタマイズ （84 ページ）を参照してください。

外部ユーザーについては、ユーザーロールがグループメンバーシップ（LDAP）を介して、またはユーザー属性（RADIUS）に基づいて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。ユーザー ロールを変更すると、[ユーザー（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かによって異なります。

- 単一ドメイン：ユーザーを割り当てるユーザーロールをオンにします。

- マルチドメイン：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ーアカウントを作成できます。ユーザー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。ユーザーがサブドメインに追加された場合のログイン方法などの詳細については、「ユーザおよびドメイン （7 ページ）」を参照してください。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. ユーザーを割り当てるユーザーロールをオンにします。
  4. **[Save（保存）]** をクリックします。

ステップ 14 （任意、物理 Firewall Management Center のみ）ユーザーに管理者ロールを割り当てている場合は、[管理者オプション（Administrator Options）] が表示されます。[Allow Lights-Out Management Access] を選択すると、ユーザーに Lights-Out Management アクセスを許可できます。Lights-Out Management の詳細については、Lights-Out 管理の概要を参照してください。

ステップ 15 [保存（Save）] をクリックします。

Firewall Management Center の外部認証の設定

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。

Firewall Management Center の外部認証について

外部認証を有効にすると、Firewall 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 サーバーを使用してユーザー クレデンシャルが検証されます。

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ーを 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 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、ユーザー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。

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。

（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 Management Center では、**[システム（System）]** > **[ユーザー（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、Firewall Management Center 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。Firewall Threat Defense 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 ユーザーから Web インターフェイスのユーザーが個別に定義されます。RADIUS の CLI ユーザーの場合、外部認証オブジェクト内に RADIUS ユーザー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。

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

（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。

- 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。

Cisco 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、Cisco Secure Firewall デバイスで追加の設定を行う必要はありません。

Firewall Management Center 用の LDAP 外部認証オブジェクトの追加

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。

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 Management Center 管理インターフェイスの変更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。ユーザー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 [システム（System）]（⚙）>**[ユーザー（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 [追加（Add）] アイコン（＋） [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 （32 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 ユーザーには使用できません。

ステップ 6 [CAC環境変数（CAC Environment Variable）] フィールドに、ログインに使用するユーザー名を含む環境変数を入力します。[CAC] チェックボックスをオンにすると、このフィールドが表示

されます。CAC を有効にしてブラウザで使用してアプライアンスにアクセスすると、CAC 情報を含む環境変数をログインに使用できます。例：`SSL_CLIENT_S_DN_CN = last.first.1234567890`

ステップ 7 [CACユーザー名テンプレート（CAC User Name Template）] フィールドに、CAC 環境変数からユーザー名の部分を抽出するためのテンプレートを入力します。たとえば、CAC 環境変数文字列の最後の 10 桁を抽出する場合は、「`\.(\d{10})$`」と入力します。

ステップ 8 [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 9 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 **[ユーザー名テンプレート（User Name Template）]**、**[UI アクセス属性（UI Access Attribute）]**、**[CLI アクセス属性（CLI 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 10 [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 11 （任意） [ポート（Port）] をデフォルトから変更します。

ステップ 12 （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 13 [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。

CAC認証を使用している場合、アクティブなユーザーアカウント（無効なユーザーアカウントを除く）のみをフィルタ処理するには、`(!(userAccountControl:1.2.840.113556.1.4.803:=2))` と入力します。この条件は、`ldpgrp` グループに属し、`userAccountControl` 属性値が `2`（無効）ではない AD 内のユーザーアカウントを取得します。

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）] をクリックして完全な CA チェーン証明書を選択する必要があります。

  （注）
  バイナリ証明書（PKCS12、DER など）ファイルは Firewall Threat Defense でサポートされていないため、選択しないでください。

  アップロードされた証明書を削除するには、[ロードされた証明書のクリア（Clear load certificate ）] チェックボックスをオンにします。このオプションは、証明書をアップロード済みで、外部認証オブジェクトの編集モードの場合にのみ表示されます。

  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（完全な CA チェーン）を再アップロードし、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。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。

- [ユーザー名テンプレート（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。

- [シェルユーザー名テンプレート（Shell User Name Template）]：CLI ユーザーを認証するために [CLIアクセス属性（CLI Access Attribute）] に対応するテンプレートを入力します。たとえば、CLI アクセス属性が `sAMAccountName` である OpenLDAP サーバーに接続し、セキュリティ（Security）部門で働くすべてのユーザーを認証するには、[シェルユーザー名テンプレート（Shell User Name Template）] フィールドに `%s` と入力します。

- [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 1024 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 14 [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 ユーザーオブジェクトに `uid` 属性がないため、UI アクセス属性を使用してユーザー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。

- ユーザー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、[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。

ステップ 15 （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） ユーザー 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ーを含む 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 サーバー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、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。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です。

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、ユーザーが自動的に再度追加されます。

ステップ 16 （任意）**[CLI アクセスフィルタ（CLI Access Filter）]** を設定して CLI ユーザーを許可します。

CLI 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 ユーザーを指定するには、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）] 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、ピリオド（.）、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、アットマーク（@）やスラッシュ（/）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 アクセスフィルタ（CLI Access Filter）] に含まれているユーザーと同じユーザー名を持つ内部ユーザーを作成しないでください。唯一の内部 Firewall Management Center ユーザーは **admin** です。**[CLI アクセス フィルタ（CLI Access Filter）]** に **admin** ユーザーを含めないでください。

ステップ 17 （任意） LDAP サーバー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、有効なユーザー名と無効なユーザー名が示されます。有効なユーザー名は一意のユーザー名であり、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、ユーザー数が 1000 を超えているサーバーへの接続をテストする場合、返されるユーザーの数は 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 （90 ページ）」を参照してください。

ステップ 18 （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、ユーザー名としてこの属性の値を使用します。ユーザーの完全修飾識別名も指定できます。

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。

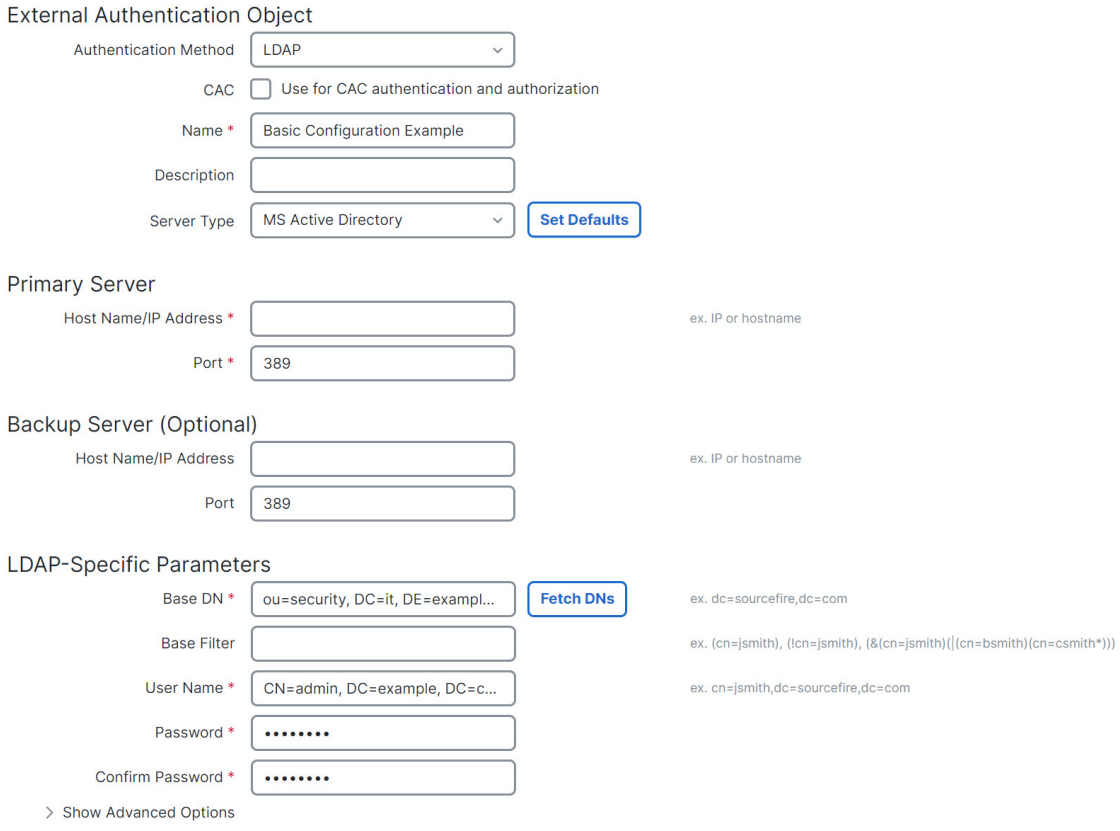
ステップ 19 [保存（Save）] をクリックします。

ステップ 20 このサーバーの使用を有効にします。Firewall Management Center でのユーザーの外部認証の有効化 （31 ページ） を参照してください。

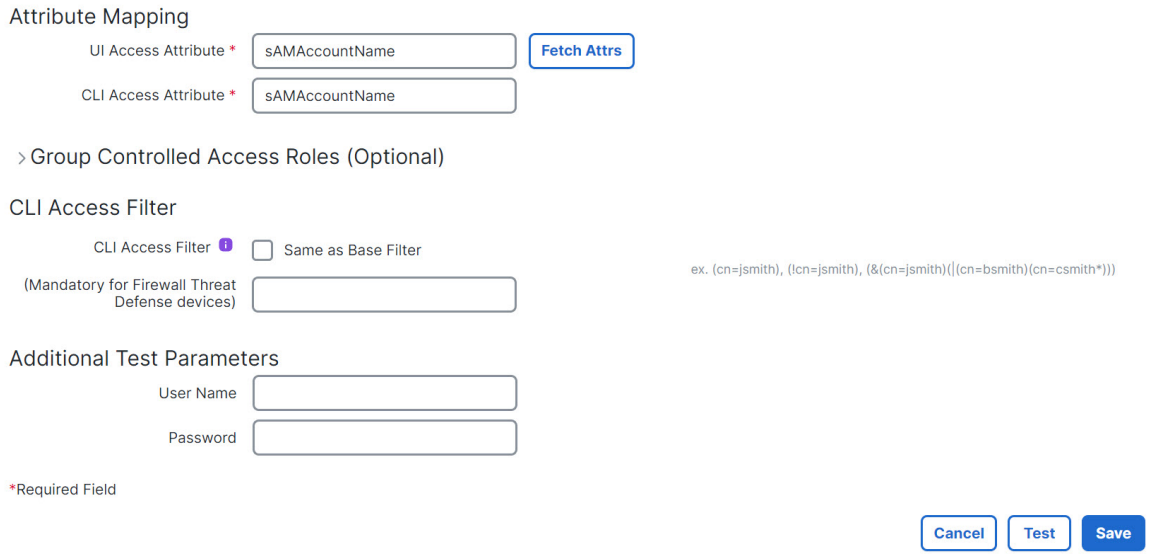
例

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。



ただし、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。サーバーのタイプとして

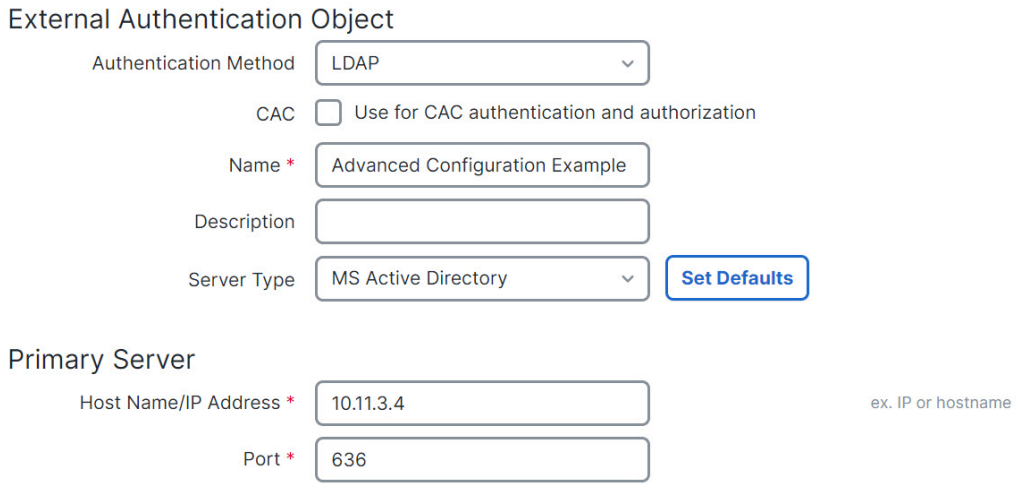
MS Active Directory を選択し、[デフォルトの設定（Set Defaults）] をクリックすると、[UI アクセス属性（UI Access Attribute）] が `sAMAccountName` に設定されます。その結果、ユーザーがシステムへのログインを試行すると、システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザー名を検索します。

また、`sAMAccountName` の **[CLI アクセス属性（CLI Access Attribute）]** は、ユーザーがアプライアンスで 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、一致が検索されるようにします。

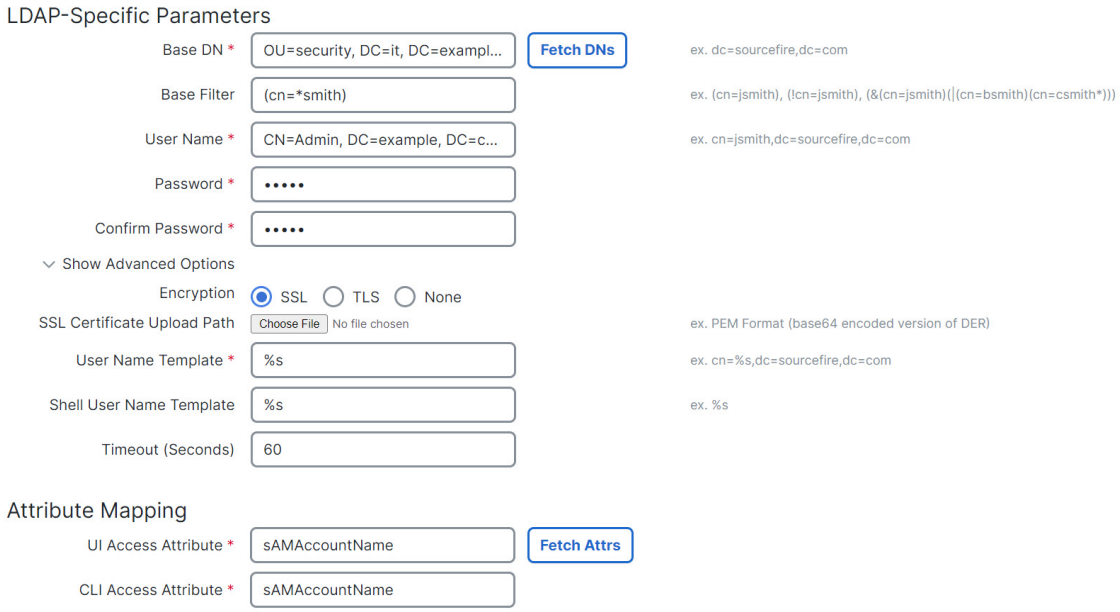
基本フィルタはこのサーバーに適用されないため、システムはベース識別名により示されるディレクトリ内のすべてのオブジェクトの属性を検査することに注意してください。サーバーへの接続は、デフォルトの期間（または LDAP サーバーで設定されたタイムアウト期間）の経過後にタイムアウトします。

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。

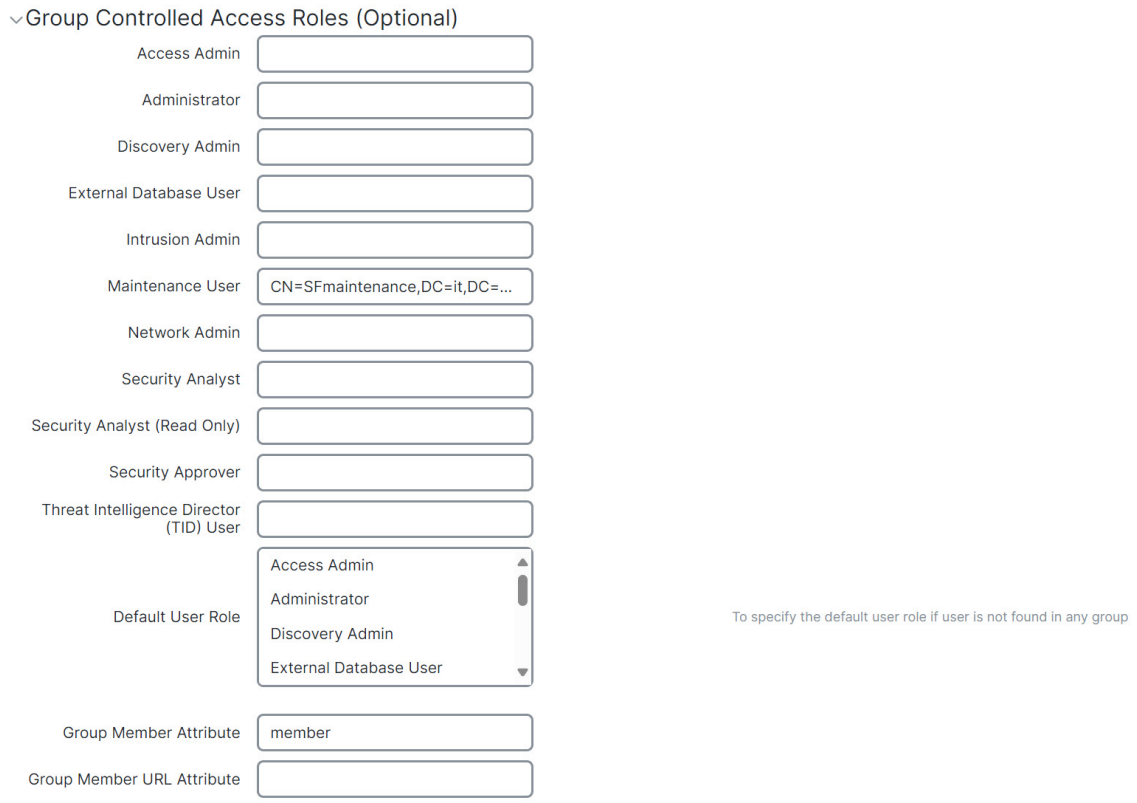


サーバへの接続が SSL を使用して暗号化され、`certificate.pem` という名前の証明書が接続に使用されます。また、[タイムアウト（秒）（Timeout (Seconds)）] の設定により、60 秒経過後にサーバーへの接続がタイムアウトします。

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。設定では、[UI Access Attribute] が `sAMAccountName` であることに注意してください。その結果、ユーザーがシステムへのログインを試行すると、システムは各オブジェクトの `sAMAccountName` 属性を検査し、一致するユーザー名を検索します。

また、`sAMAccountName` の **[CLI アクセス属性（CLI Access Attribute）]** は、ユーザーがアプライアンスで 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、一致が検索されるようにします。

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ー（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。



CLI 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、同じユーザーが Web インターフェイスを使用する場合と同様に、CLI を介してアプライアンスにアクセスできます。

Firewall Management Center 用の RADIUS 外部認証オブジェクトの追加

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。

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 [システム（System）]（⚙）>**[ユーザー（Users）]**を選択します。

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

ステップ 3 [追加（Add）] アイコン（＋） [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 すべての RADIUS 応答で Message-Authenticator 属性を要求するには、**[RADIUS サーバ対応メッセージ オーセンティケータ（RADIUS Server-Enabled Message Authenticator）]** チェックボックスをオンにして、RADIUS サーバーからのすべての応答が Firewall Threat Defense によって安全に検証されるようにします。

この機能は、新しい RADIUS サーバーではデフォルトで有効になっています。既存のサーバーではアップグレード後に有効にすることをお勧めします。メッセージオーセンティケータを無効にすると、ファイアウォールが攻撃にさらされる可能性があります。RADIUS サーバーでメッセージ オーセンティケータを構成してあることを確認してください。

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。

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（Timeout）] を 1 ～ 1024 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。

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、ユーザーが自動的に再度追加されます。

ステップ 12 （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 サーバー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ーに特定のロールを付与するとします。`Ascend-Assign-IP-Pool` は、ユーザーがログイ

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` のすべてのユーザーに対し、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 13 （任意）**[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。

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、ピリオド（.）、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、アットマーク（@）やスラッシュ（/）は使用不可

CLI アクセスの RADIUS 認証を防止するには、このフィールドを空白にします。

（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）
シェルアクセスフィルタに含まれているユーザーと同じユーザー名を持つ内部ユーザーを削除します。Firewall Management Center の場合、内部 CLI ユーザーのみが **admin** です。そのため、**admin** 外部ユーザーを作成しないでください。

ステップ 14 （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。

ステップ 15 （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。

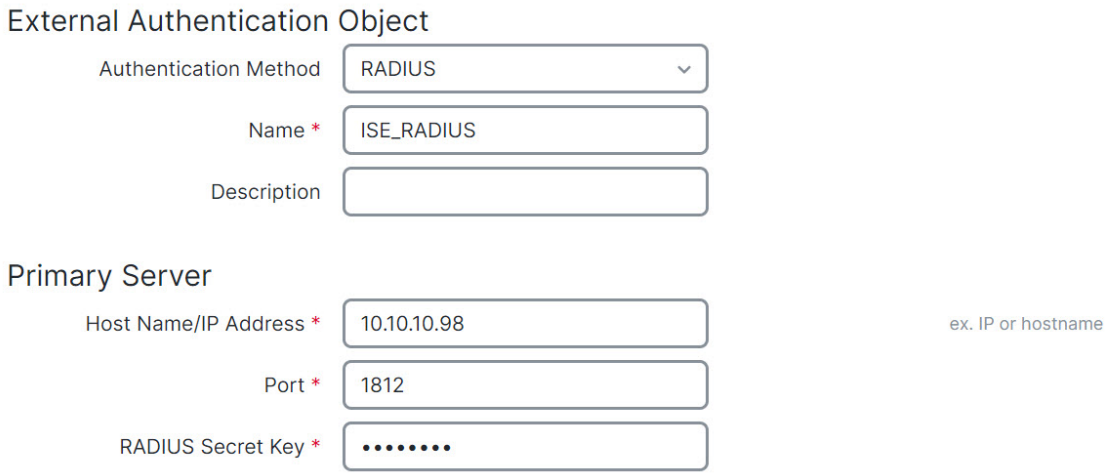
ステップ 16 [保存（Save）] をクリックします。

ステップ 17 このサーバーの使用を有効にします。Firewall Management Center でのユーザーの外部認証の有効化 （31 ページ） 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、Cisco Secure Firewall 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。

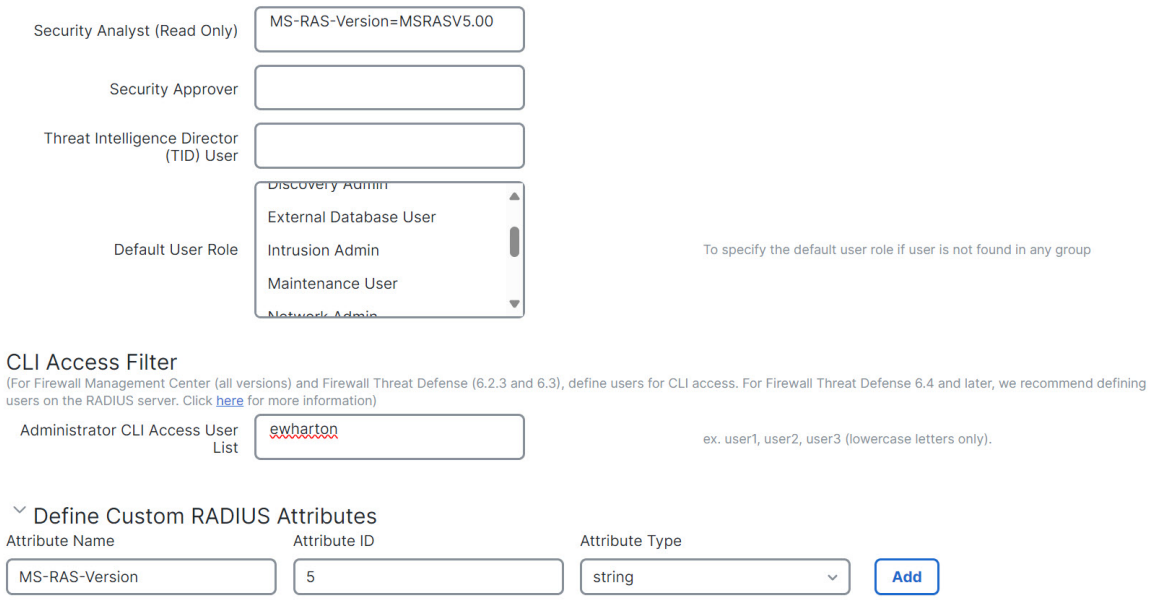
次の図に、この例のロール設定を示します。

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。



Firewall Management Center でのユーザーの外部認証の有効化

管理ユーザーの外部認証を有効にすると、Firewall 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 サーバーを使用してユーザー クレデンシャルが検証されます。

始める前に

Firewall Management Center 用の LDAP 外部認証オブジェクトの追加 （16 ページ）およびFirewall Management Center 用の RADIUS 外部認証オブジェクトの追加 （25 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 [システム（System）]（⚙）>**[ユーザー（Users）]**を選択します。

ステップ 2 [外部認証（External Authentication）] 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ーにデフォルトのユーザー ロールを設定します。

ロールがないユーザーは、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ー ロールは、このデフォルトのユーザー ロールをオーバーライドします。

a) [デフォルトのユーザーロール（Default User Role）] 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ーロール設定（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 [有効なスライダ（Slider enabled）]（）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。サーバー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、**[CLIアクセスフィルタ（CLI 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 アクセスのユーザーは、認証オブジェクトがリストの順序で最も高いサーバー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ーがアクセスされる順序を、サーバー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 外部ユーザーに CLI 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。

（注）
マルチドメイン機能は CLI ではサポートされていません。そのため、[シェル認証（Shell Authentication）] オプションは、グローバルドメインでのみ使用でき、サブドメインでは使用できません。

1 番目の外部認証オブジェクト名は、CLI 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。

LDAP を使用した共通アクセス カード認証の設定

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 Firewall Management Center ユーザーを認証するように LDAP 認証を設定できます。CAC 認証により、ユーザーは、デバイスに個別のユーザー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 認証ユーザーは、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ーが再度追加されますが、ユーザー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。

注意 LDAP を使用して CAC 認証を設定する場合は、ユーザーにデフォルトのアクセスロールを割り当てる際に、最小限の権限の原則に従うようにしてください。ユーザーが CAC ログイン情報を使用してシステムに初めてログインすると、アカウントにこのデフォルトのアクセスロールが割り当てられます。

デフォルトのアクセスロールを割り当てるときに最小権限の原則に従わない場合、以降のログインでユーザーに意図しない権限レベルが割り当てられる可能性があります。これにより、必要なアクセスロールを超える権限がユーザーに付与される場合があります。

デフォルトのアクセスロールでログインしているユーザーが一時的に権限を昇格する必要がある場合、管理者権限を持つユーザーは、より高い権限を持つロールを割り当てることで、必要な高いレベルのアクセスを一時的にそのユーザーに提供できます。この権限は、非アクティブな状態が 24 時間続くと取り消され、ユーザーはデフォルトのアクセスロールに戻ります。

ユーザーがより高い権限レベル（システム管理者など）に永続的なアクセスロールを再割り当てする必要がある場合は、**グループ制御アクセスロール方式**を使用して、管理者アクセス権をユーザーに付与します。この方法では、指定されたアクセスロールが 24 時間を超えて保持され、ユーザーはグループ割り当てに従って正しい権限レベルを持つことが保証されます。グループ制御アクセスロールの設定の詳細については、「Add an LDAP External Authentication Object for Management Center」の項を参照してください。

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、[ユーザー名（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ー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 「Firewall Management Center 用の LDAP 外部認証オブジェクトの追加 （16 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）] > [ユーザー名テンプレート（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 Firewall Management Center でのユーザーの外部認証の有効化 （31 ページ）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 [システム（System）]（⚙）> **[構成（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 サーバー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 サーバー証明書とユーザー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 クライアント証明書設定（HTTPS Client Certificate Settings）] の [クライアント証明書を有効にする（Enable Client 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 Secure Firewall Management Center へのログイン に従い、デバイスにログインします。

SAML シングルサインオンの設定

シングルサインオンを使用するように Firewall Management Center を設定できます。これは、中央アイデンティティ プロバイダー（IdP）が、組織内の他のアプリケーションだけでなく、Firewall Management Center にログインするユーザーに認証と承認を提供するシステムです。このような SSO 構成に参加するように設定されたアプリケーションは、フェデレーテッド サービス プロバイダー アプリケーションと呼ばれます。SSO ユーザーは、一度ログインすると、同じフェデレーションのメンバーであるすべてのサービス プロバイダー アプリケーションにアクセスできるようになります。

SAML シングルサインオンについて

SSO 用に設定された Firewall Management Center では、ログインページにシングルサインオンのためのリンクが表示されます。SSO アクセス用に設定されたユーザーは、このリンクをクリックすると、Firewall Management Center のログインページでユーザー名とパスワードを入力せずに、認証と承認のために IdP にリダイレクトされます。IdP による認証に成功すると、SSO ユーザーは Firewall Management Center Web インターフェイスに再度リダイレクトされて、ロ

グインします。これを実現するための Firewall Management Center と IdP 間のすべての通信は、ブラウザを仲介として使用して行われます。そのため、Firewall Management Center はアイデンティティ プロバイダーに直接アクセスするためにネットワーク接続を必要としません。

マルチテナント Firewall Management Center では、SSO の設定により、SAML ユーザーを特定のサブドメインに割り当てることができます。この構成は、グローバル ドメイン レベルでのみ可能であることに注意してください。

Firewall Management Center は、認証および承認のために、セキュリティ アサーション マークアップ言語（SAML）2.0 オープンスタンダードに準拠する任意の SSO プロバイダーを使用した SSO をサポートしています。

Note Management Center は SAML 認証要求メッセージに署名できません。そのため、IdP が認証要求でサービスプロバイダーの署名を必要とする場合、Management Center での SSO は失敗します。

Firewall Management Center Web インターフェイスには、次の SSO プロバイダー用の設定オプションが用意されています。

- Okta
- OneLogin
- Azure
- お客様のクラウドソリューションの PingID の PingOne
- その他

Note Cisco Secure Sign On SSO 製品は、Firewall Management Center を事前統合サービスプロバイダーとして認識しません。

Firewall Management Center の SSO ガイドライン

Firewall Management Center を SSO フェデレーションのメンバーとして設定するときは、次の点に注意してください。

- Firewall Management Center は、一度に 1 つの SSO プロバイダーのみで SSO をサポートできます。たとえば、SSO に Okta と OneLogin の両方を使用するように Firewall Management Center を設定することはできません。
- 高可用性設定の Firewall Management Center Firewall Management Center では SSO をサポートできますが、次の考慮事項に留意する必要があります。
  - SSO設定は、高可用性ペアのメンバー間で同期されません。ペアの各メンバーで個別に SSO を設定する必要があります。

- 高可用性ペアの両方の Firewall Management Center は、SSO に同じ IdP を使用する必要があります。SSO 用に設定された各 Firewall Management Center の IdP で、サービスプロバイダー アプリケーションを設定する必要があります。
- 両方が SSO をサポートするように設定されている Firewall Management Center の高可用性ペアでは、ユーザーは SSO を使用してセカンダリ Firewall Management Center に初めてアクセスする前に、最初に SSO を使用してプライマリ Firewall Management Center に少なくとも 1 回ログインする必要があります。
- 高可用性ペアで Firewall Management Center の SSO を設定する場合：
  - プライマリ Firewall Management Center で SSO を設定する場合、セカンダリ Firewall Management Center で SSO を設定する必要はありません。
  - セカンダリ Firewall Management Center で SSO を設定する場合は、プライマリ Firewall Management Center でも SSO を設定する必要があります。（これは、SSO ユーザーがセカンダリ Firewall Management Center にログインする前に、プライマリ Firewall Management Center に少なくとも 1 回ログインする必要があるためです）。

- 内部で認証された、または LDAP または RADIUS によって認証された管理ロールを持つユーザーのみが SSO を構成できます。
- Firewall Management Center は、IdP から開始された SSO をサポートしていません。
- Firewall Management Center は、SSO アカウントの CAC クレデンシャルを使用したログインをサポートしていません。
- CC モードを使用して展開中に SSO を設定できません。
- SSO アクティビティは、[サブシステム（Subsystem）] フィールドで指定されたログインまたはログアウトを使用して Firewall Management Center の監査ログに記録されます。

Related Topics

高可用性
ドメイン
CAC クレデンシャルを使用した Secure Firewall Management Center へのログイン
セキュリティ認定準拠
監査レコード

SSO ユーザーアカウント

アイデンティティ プロバイダーは、ユーザーとグループの構成を直接サポートできます。また、多くの場合、Active Directory、RADIUS、LDAP などの他のユーザー管理アプリケーションからユーザーとグループをインポートできます。このドキュメントでは、IdP と連携して SSO をサポートするように Firewall Management Center を設定することに焦点を当てています。ただし、IdP ユーザーおよびグループがすでに確立されていることを前提としています。他の

ユーザー管理アプリケーションのユーザーとグループをサポートするようにIdPを設定するには、IdPベンダーのドキュメントを参照してください。

ユーザー名とパスワードを含む、SSOユーザーのほとんどのアカウント特性は、IdPで確立されます。SSOアカウントは、それらのアカウントが初めてログインするまで、Firewall Management Center Webインターフェイスの[ユーザー（Users）]ページに表示されません。

Note システムでは、SSOアカウントのユーザー名と、SAMLログインプロセス中にIdPがFirewall Management Centerに送信するNameID属性の両方が有効な電子メールアドレスである必要があります。多くのIdPは、ログインしようとしているユーザーのユーザー名をNameID属性として自動的に使用しますが、これがIdPに適しているかを確認する必要があります。IdPでサービス プロバイダー アプリケーションを設定し、Firewall Management CenterへのSSOアクセス権限を持つIdPユーザーアカウントを作成する場合は、このことに注意してください。

SSOユーザーの次のアカウント特性は、[システム（System）]（⚙）>**[ユーザー（Users）]**>**[ユーザーの編集（Edit User）]**の下のFirewall Management Center Webインターフェイスから設定できます。

- 実際の名前
- ブラウザ セッション タイムアウトから除外する（Exempt from Browser Session Timeout）

SSO ユーザーのユーザーロールマッピング

デフォルトでは、Firewall Management CenterへのSSOアクセスが許可されているすべてのユーザーに、セキュリティアナリスト（読み取り専用）ロールと、すべてのドメインへのアクセスが割り当てられます。このデフォルトを変更することも、特定のSSOユーザーまたはグループに対してユーザー ロール マッピングで上書きすることもできます。Firewall Management Center SSO構成を確立してテストに成功したら、ユーザーロールマッピングを構成できます。ユーザー ロールのマッピングとは、IdPロールを1つ以上のFirewall Management Centerロールに関連付けることを意味し、**グループ メンバー属性値**を使用して1つ以上のドメインへのアクセスを許可できます。

ユーザーロールマッピングでは、Firewall Management Centerの構成設定をSSO IdPアプリケーションの設定と調整する必要があります。ユーザーロールは、IdPアプリケーションで定義されたユーザーまたはグループに割り当てることができます。ユーザーはグループのメンバーである場合とそうでない場合があります。また、ユーザーまたはグループの定義は、Active Directoryなどの組織内の他のユーザー管理システムからIdPにインポートされる場合とインポートされない場合があります。このため、Firewall Management Center SSOユーザーロールマッピングを効果的に構成するには、SSOフェデレーションがどのように編成されているか、およびSSO IdPアプリケーションでユーザー、グループ、およびそれらのロールがどのように割り当てられているかを理解する必要があります。このドキュメントでは、IdPと連携してユーザーロールマッピングをサポートするようにFirewall Management Centerを構成することに焦点を当てています。IdP内にユーザーまたはグループを作成したり、ユーザー管理アプリケーションからIdPにユーザーまたはグループをインポートしたりするには、IdPベンダーのドキュメントを参照してください。

ユーザー ロール マッピングでは、IdP は Firewall Management Center サービス プロバイダー アプリケーションのロール属性を維持し、その Firewall Management Center にアクセスできる各ユーザーまたはグループは、ロール属性の文字列または式で構成されます。属性値の要件は IdP ごとに異なります。

Firewall Management Centerでは、**[グループ メンバーの属性（Group Member Attribute）]** フィールドで指定されたロール属性の名前、**[グループ メンバーの属性値（Group Member Attribute Value）]** フィールドで指定されたロール属性の値、割り当てられるロールとドメインは SSO 構成の一部です。ユーザーが SSO を使用して Firewall Management Center にログインすると、Firewall Management Center は、IdP のそのユーザー（またはそのユーザーのグループ）のロール属性の値をFirewall Management Centerのロール属性の値と比較し、1 つ以上のユーザー ロールを割り当て、1 つ以上のドメインへのアクセスを提供します。ロールに不一致がある場合、すべてのドメインへのアクセス権を持つデフォルト ロールがユーザーに割り当てられます。

Note 個人ユーザー権限またはグループ権限に基づいてFirewall Management Center ロールがマッピングされるように構成できますが、単一のFirewall Management Centerアプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできません。

Firewall Management Centerでのシングルサインオンの有効化

Before you begin

- SAML SSO 管理アプリケーションで、Firewall Management Center のサービス プロバイダー アプリケーションを設定し、ユーザーまたはグループをサービス プロバイダー アプリケーションに割り当てます。
  - Okta の Firewall Management Center サービス プロバイダー アプリケーションを設定するには、Okta の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 41を参照してください。
  - OneLogin の Firewall Management Center サービス プロバイダー アプリケーションを設定するには、OneLogin の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 52を参照してください。
  - Azure の Firewall Management Center サービス プロバイダー アプリケーションを設定するには、Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62を参照してください。
  - PingID の PingOne for Customers クラウドソリューションの Firewall Management Center サービス プロバイダー アプリケーションを設定するには、PingID PingOne for Customers の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 72を参照してください。
  - SAML 2.0 準拠の SSO プロバイダーの Firewall Management Center サービス プロバイダー アプリケーションを設定するには、SAML 2.0 準拠の SSO プロバイダー用の FMC サービス プロバイダー アプリケーションの設定, on page 77を参照してください。

Procedure

ステップ 1 [システム（System）]（⚙）>**[ユーザー（Users）]**>**[シングルサインオン（Single Sign-On）]**を選択します。

ステップ 2 [シングルサインオン（SSO）設定（Single Sign-On (SSO) Configuration）] スライダをクリックして、SSO を有効にします。

ステップ 3 [SSOの設定（Configure SSO）] ボタンをクリックします。

ステップ 4 [Firewall Management Center SAMLプロバイダーの選択（Select Firewall Management Center SAML Provider）] ダイアログボックスで、選択した SSO IdP のオプションボタンをクリックし、[次へ（Next）] をクリックします。

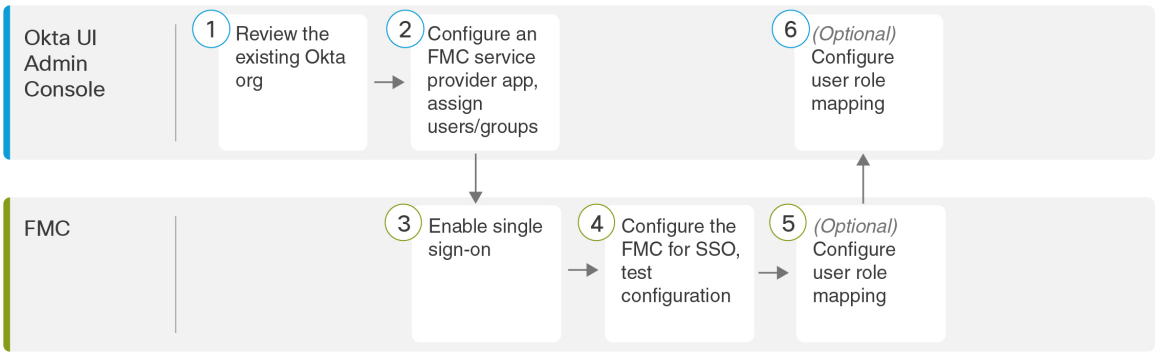
What to do next

選択した SSO プロバイダーに適した手順に進みます。

- Okta SSO 用に Firewall Management Center を設定するには、Okta SSO 用の Firewall Management Center の設定, on page 43を参照してください。
- PingID の PingOne for Customers クラウドソリューションを使用した SSO 用に Firewall Management Center を設定するには、PingID PingOne for Customers を使用した SSO 用の Firewall Management Center の設定, on page 74を参照してください。
- Azure SSO 用に Firewall Management Center を設定するには、Azure SSO 用の Firewall Management Center の設定, on page 64を参照してください。
- OneLogin SSO 用に Firewall Management Center を設定するには、OneLogin SSO 用の Firewall Management Center の設定, on page 54を参照してください。
- SAML 2.0 準拠のプロバイダーを使用した SSO 用に Firewall Management Center を設定するには、SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Firewall Management Center の設定, on page 80を参照してください。

Okta を使用したシングルサインオンの設定

Okta を使用して SSO を設定するには、次のタスクを参照してください。



1	Okta UI 管理コンソール	Okta Org の確認, on page 40
2	Okta UI 管理コンソール	Okta の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 41
3	Firewall Management Center	Firewall Management Centerでのシングルサインオンの有効化, on page 38
4	Firewall Management Center	Okta SSO 用の Firewall Management Center の設定, on page 43
5	Firewall Management Center	次における Okta のユーザーロールマッピングの設定： Firewall Management Center, on page 44
6	Okta UI 管理コンソール	Okta IdP におけるユーザーロールマッピングの設定, on page 46

Okta Org の確認

Okta では、ユーザーが同じ SSO アカウントでアクセスできるすべてのフェデレーションデバイスとアプリケーションを含むエンティティは、*org* と呼ばれます。Firewall Management Center を Okta org に追加する前に、その設定についてよく理解してください。次の質問を考慮してください。

- Firewall Management Center にアクセスできるユーザーは何人ですか？
- ユーザーは、グループの Okta org のメンバーですか？
- ユーザーとグループの定義は Okta にネイティブですか。それとも Active Directory、RADIUS、LDAP などのユーザー管理アプリケーションからインポートされますか。
- Firewall Management Center で SSO をサポートするために、Okta org にユーザーまたはグループを追加する必要がありますか。
- どのようなユーザーロールの割り当てを行いますか。（ユーザーロールを割り当てない場合は、Firewall Management Center が構成可能なデフォルトのユーザーロールをすべての SSO ユーザーに自動的に割り当てます）。

- 必要なユーザーロールマッピングをサポートするには、Okta org 内のユーザーとグループをどのように編成する必要がありますか？

個人ユーザー権限またはグループ権限に基づいてFirewall Management Centerロールがマッピングされるように構成できますが、単一のFirewall Management Centerアプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。

このドキュメントは、Okta クラシック UI 管理コンソールに精通していて、ネットワーク管理者権限を必要とする設定機能を実行できるアカウントを持っていることを前提としています。詳細が必要な場合は、オンラインで入手できる Okta のドキュメントを参照してください。

Okta の Firewall Management Center サービス プロバイダー アプリケーションの設定

Okta クラシック UI 管理コンソールでこれらの手順を使用して、Okta 内に Firewall Management Center サービス プロバイダー アプリケーションを作成し、そのアプリケーションにユーザーまたはグループを割り当てます。SAML SSO の概念と Okta 管理コンソールに精通している必要があります。このドキュメントでは、完全に機能する SSO 組織を確立するために必要なすべての Okta の機能について説明しているわけではありません。たとえば、ユーザーとグループを作成したり、別のユーザー管理アプリケーションからユーザーとグループの定義をインポートしたりするには、Okta のドキュメントを参照してください。

Note Firewall Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

Note Firewall Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、OneLogin から Firewall Management Center にユーザーロール情報を伝達する単一の属性を構成する必要があります。

Before you begin

- SSO フェデレーションとそのユーザーおよびグループについて理解します。Okta Org の確認, on page 40を参照してください。
- 必要に応じて、Okta org にユーザーアカウントやグループを作成します。

Note システムでは、SSO アカウントのユーザー名と、SAML ログイン プロセス中に IdP が Firewall Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービスプロバイダー アプリケーションを設定し、Firewall Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Firewall Management Center のログイン URL を確認します（`https://ipaddress_or_hostname`）。

Note Firewall Management Center Web インターフェイスに複数の URL（たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで構成するログイン URL を使用して Firewall Management Center にアクセスする必要があります。

Procedure

ステップ 1 Okta クラシック UI 管理コンソールから、Firewall Management Center のサービス プロバイダー アプリケーションを作成します。次の選択肢を使用して Firewall Management Center アプリケーションを設定します。

- [プラットフォーム（Platform）] に `Web` を選択します。
- [サインオン方式（Sign on method）] に `SAML 2.0` を選択します。
- [シングルサインオンURL（Single sign on URL）] を指定します。

  これは、ブラウザが IdP に代わって情報を送信する Firewall Management Center URL です。

  文字列 `saml/acs` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [受信者URLおよび接続先URLにこれを使用する（Use this for Recipient URL and Destination URL）] を有効にします。
- [オーディエンスURI（SPエンティティID）（Audience URI (SP Entity ID)）] を入力します。

  これは、サービスプロバイダー（Firewall Management Center）のグローバルに一意の名前であり、多くの場合、URL としてフォーマットされます。

文字列 `/saml/metadata` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/metadata`。

- [名前ID形式（Name ID Format）] に `Unspecified` を選択します。

ステップ 2 （グループをアプリケーションに割り当てる場合はオプション）個々のOktaユーザーをFirewall Management Centerアプリケーションに割り当てます。（Firewall Management Centerアプリケーションにグループを割り当てることを計画している場合は、それらのグループのメンバーであるユーザーを個人として割り当てないでください。）

ステップ 3 （個人ユーザーをアプリケーションに割り当てる場合はオプション）Okta グループを Firewall Management Center アプリケーションに割り当てます。

ステップ 4 （オプション）Firewall Management Center での SSO セットアップを簡単にするために、Firewall Management Center サービス プロバイダー アプリケーションの SAML XML メタデータファイルを Okta からローカルコンピュータにダウンロードできます。

What to do next

シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください。

Okta SSO 用の Firewall Management Center の設定

Firewall Management Center Web インターフェイスでこれらの手順を使用します。

はじめる前に

- Okta クラシック UI 管理コンソールで Firewall Management Center サービス プロバイダー アプリケーションを作成します。Okta の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 41を参照してください。
- シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください

Procedure

ステップ 1 （このステップはFirewall Management Centerでのシングルサインオンの有効化, on page 38から直接続きます）。[Oktaメタデータの設定（Configure Okta Metadata）] ダイアログボックスには、2 つの選択肢があります。

- SSO 構成情報を手動で入力するには：
  - **a.** [手動設定（Manual Configuration）] オプションボタンをクリックします。
  - **b.** Okta SSO サービス プロバイダー アプリケーションから次の値を入力します（Okta クラシック UI 管理コンソールからこれらの値を取得します）。
    - **アイデンティティ プロバイダーのシングルサインオン（SSO）URL**

- アイデンティティ プロバイダー発行元
- X.509 証明書

- Okta によって生成された XML メタデータファイルをローカルコンピュータに保存した場合（Okta の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 41のステップ 4）、ファイルを Firewall Management Center にアップロードできます。

  a. [XMLファイルのアップロード（Upload XML File）]オプションボタンをクリックします。

  b. 画面の指示に従って、ローカルコンピュータ上の XML メタデータファイルに移動して選択します。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）]ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Firewall Management Center の SSO 構成と Okta サービス プロバイダー アプリケーション構成を確認し、エラーを修正してから再試行します。

ステップ 5 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

What to do next

オプションで、SSO ユーザーのユーザーロールマッピングを構成できます。次における Okta のユーザーロールマッピングの設定： Firewall Management Center, on page 44を参照してください。ロールマッピングを構成しないことを選択した場合、デフォルトで、Firewall Management Center にログインするすべての SSO ユーザーに、次における Okta のユーザーロールマッピングの設定： Firewall Management Center, on page 44のステップ 4 で構成したユーザーロールが割り当てられます。

次における Okta のユーザーロールマッピングの設定： Firewall Management Center

Firewall Management Center Web インターフェイスでユーザー ロール マッピングを構成するフィールドは、SSOプロバイダーの選択に関係なく同じです。ただし、構成する値では、使用する SAML SSO プロバイダーのユーザー ロール マッピングの導入方法を考慮する必要があります。

Before you begin

- Okta ユーザーグループのマッピング情報を確認します。Okta Org の確認, on page 40を参照してください。

- Firewall Management Center を SSO サービス プロバイダー アプリケーションとして設定します。Okta の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 41を参照してください。
- Firewall Management Center でシングルサインオンを有効にして設定します。Firewall Management Centerでのシングルサインオンの有効化, on page 38およびOkta SSO 用の Firewall Management Center の設定, on page 43を参照してください。

Procedure

ステップ 1 [システム（System）]（⚙）>**[ユーザー（Users）]**>**[シングルサインオン（Single Sign-On）]**を選択します。

ステップ 2 **[詳細設定（Advanced Configuration）]**を展開します。

ステップ 3 **[デフォルトのユーザーロール（Default User Role）]**ドロップダウン リストから、ユーザーを割り当てるデフォルトの Firewall Management Center ユーザーロールを選択します。

ステップ 4 **[グループ メンバー属性（Group Member Attribute）]**フィールドに、ユーザーまたはグループの Firewall Management Center ユーザー ロール マッピング用に Okta で設定された属性を入力します。（Okta IdP におけるロールマッピングのためのユーザー属性の設定, on page 46のステップ 1 またはOkta IdP におけるロールマッピングのためのグループ属性の設定, on page 48のステップ 1 を参照）。

ステップ 5 1 つ以上のユーザー ロールマッピングを設定し、それらを 1 つ以上のドメインに関連付けます。

a) **[グループ メンバー属性値（Group Member Attribute Value）]**で、**[編集（Edit）]**ボタンをクリックし、IdP で定義されている属性値と一致する文字列または正規表現として属性値を入力します。複数の値をカンマで区切って入力することもできます。

b) **[ドメイン（Domain）]**ドロップダウンリストで、ドメインを選択します。

c) **[ロール（Roles）]**ドロップダウン リストから、1 つ以上のユーザー ロールを選択します。

Firewall Management Center は、属性値を、IdP が SSO ユーザー情報とともに Firewall Management Center に送信するユーザー ロールマッピング属性値と比較します。一致が見つかると、 Firewall Management Center は、構成されたドメインへのアクセスとともに、対応するロールをユーザーに付与します。

d) （オプション）**[ユーザー ロール マッピングの追加（Add User Role Mapping）]**をクリックして、ユーザー ロール マッピングをさらに追加します。

ステップ 6 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Firewall Management Center の SSO 構成と Okta サービス プロバイダー アプリケーション構成を確認し、エラーを修正してから再試行します。

ステップ 7 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

What to do next

サービス プロバイダー アプリケーションでユーザーロールマッピングを構成します。Okta IdP におけるユーザーロールマッピングの設定, on page 46を参照してください。

Okta IdP におけるユーザーロールマッピングの設定

個人ユーザーの権限またはグループの権限に基づいて、Okta クラシック UI 管理コンソールで SSO ユーザーロールマッピングを設定できます。

- 個人ユーザーの権限に基づいてマップするには、Okta IdP におけるロールマッピングのためのユーザー属性の設定, on page 46を参照してください。
- グループの権限に基づいてマップするには、Okta IdP におけるロールマッピングのためのグループ属性の設定, on page 48を参照してください。

SSO ユーザーが Firewall Management Center にログインすると、Okta は、Okta IdP で設定されたユーザーまたはグループロールの属性値を Firewall Management Center に提示します。Firewall Management Center は、その属性値を **[グループメンバーの属性値（Group Member Attribute Value）]** フィールドの正規表現と比較し、ユーザーに設定されたロールと、設定されたドメインへのアクセス権を付与します。（一致するものが見つからない場合、Firewall Management Centerは、すべてのドメインへアクセスできる、設定可能なデフォルトのユーザーロールをユーザーに付与します）。

Note Firewall Management Center 単一では、グループと個人ユーザーの両方のロールマッピングをサポートできません。Firewall Management Center サービス プロバイダー アプリケーションに対して 1 つのマッピング方法を選択し、それを一貫して使用する必要があります。さらに、Firewall Management Center は、Okta で設定された Firewall Management Center サービス プロバイダー アプリケーションごとに 1 つのグループ属性ステートメントのみを使用して、グループロールマッピングをサポートできます。一般に、グループベースのロールマッピングは、多数のユーザーがいる Firewall Management Center でより効率的です。Okta org 全体で確立されたユーザーとグループの定義を考慮する必要があります。

Okta IdP におけるロールマッピングのためのユーザー属性の設定

Okta クラシック UI 管理コンソールでこれらの手順を使用して、カスタムロールマッピング属性を Okta のデフォルト ユーザー プロファイルに追加します。

Okta サービス プロバイダー アプリケーションは、次の 2 種類のユーザープロファイルのいずれかを使用する場合があります。

- Okta ユーザープロファイル。カスタム属性で拡張できます。
- アプリのユーザープロファイル。サポートされている属性についてサードパーティのアプリケーションまたはディレクトリ（Active Directory、LDAP、Radius など）をクエリすることによって Okta が生成する事前定義されたリストの属性でのみ拡張できます。

Okta組織では、いずれかのタイプのユーザープロファイルを使用できます。それらの設定方法については、Oktaのドキュメントを参照してください。どのタイプのユーザープロファイルを使用しても、Firewall Management Center でユーザーロールマッピングをサポートするには、プロファイルでカスタム属性を設定して、各ユーザーのロールマッピング式をFirewall Management Center に伝える必要があります。

このドキュメントでは、Oktaユーザープロファイルを使用したロールマッピングについて説明します。アプリプロファイルを使用してマッピングするには、組織でカスタム属性を設定するために使用しているサードパーティのユーザー管理アプリケーションに精通している必要があります。詳細については、Okta のドキュメントを参照してください。

Before you begin

- Okta の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 41の説明に従って、Okta IdP で Firewall Management Center サービス プロバイダー アプリケーションを構成します。
- 次における Okta のユーザーロールマッピングの設定： Firewall Management Center, on page 44の説明に従って、Firewall Management Center で SSO ユーザーロールマッピングを設定します。

Procedure

ステップ 1 デフォルトの Okta ユーザープロファイルに新しい属性を追加します。

- [データ型（Data type）] では、`string` を選択します。
- ユーザーロールマッピングで照合する式が含まれる、Okta IdP が Firewall Management Center に送信する変数名を指定します。この変数名は、Firewall Management Center SSO 構成の [グループメンバー属性（Group Member Attribute）] で入力した文字列と一致する必要があります（次における Okta のユーザーロールマッピングの設定： Firewall Management Center, on page 44のステップ 5 を参照してください）。

ステップ 2 このプロファイルを使用して Firewall Management Center サービス プロバイダー アプリケーションに割り当てられた各ユーザーについて、先ほど作成したユーザーロール属性に値を割り当てます。

Firewall Management Center からユーザーに割り当てるロールを表すために式を使用します。Firewall Management Center では、この文字列を、次における Okta のユーザーロールマッピングの設定： Firewall Management Center, on page 44の手順 6 で各 Firewall Management Center ユーザーロールに割り当てた式と比較します（Firewall Management Center ユーザーロール式との比較のために、Firewall Management Center では Okta から受け取った属性値を、Golang と Perl でサポートされている Google の RE2 正規表現標準の制限バージョンに準拠した式として扱います）。

Okta IdP におけるロールマッピングのためのグループ属性の設定

Okta 管理コンソールでこれらの手順を使用して、カスタム ロール マッピング グループ属性を Firewall Management Center サービス プロバイダー アプリケーションに追加します。Firewall Management Center は、Okta Firewall Management Center サービス プロバイダー アプリケーションごとに 1 つのグループ属性ステートメントのみを使用して、グループロールマッピングをサポートできます。

Okta サービス プロバイダー アプリケーションは、次の 2 種類のグループのいずれかを使用する場合があります。

- Okta グループ。カスタム属性で拡張できます。
- アプリケーショングループ。サポートされている属性についてサードパーティのアプリケーションまたはディレクトリ（Active Directory、LDAP、Radius など）をクエリすることによって Okta が生成する事前定義されたリストの属性でのみ拡張できます。

Okta組織では、いずれかのタイプのグループを使用できます。それらの設定方法については、Okta のドキュメントを参照してください。どのタイプのグループを使用しても、Firewall Management Center でユーザーロールマッピングをサポートするには、グループのカスタム属性を設定して、ロールマッピング式を Firewall Management Center に伝える必要があります。

このドキュメントでは、Oktaグループを使用したロールマッピングについて説明します。アプリケーショングループを使用してマッピングするには、組織でカスタム属性を設定するために使用しているサードパーティのユーザー管理アプリケーションに精通している必要があります。詳細については、Okta のドキュメントを参照してください。

Before you begin

- Okta IdP の Firewall Management Center サービス プロバイダー アプリケーションを設定します。Okta の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 41を参照してください。
- Firewall Management Center でのユーザーロールマッピングの設定次における Okta のユーザーロールマッピングの設定： Firewall Management Center, on page 44

Procedure

ステップ 1 Okta 管理者コンソールの左ペインから、**[アプリケーション（Applications）]**を選択します。

ステップ 2 SAML アプリケーションをクリックします。

ステップ 3 [全般（General）] タブをクリックします。

ステップ 4 **[SAML設定（SAML Settings）]** セクションで **[編集（Edit）]** をクリックします。

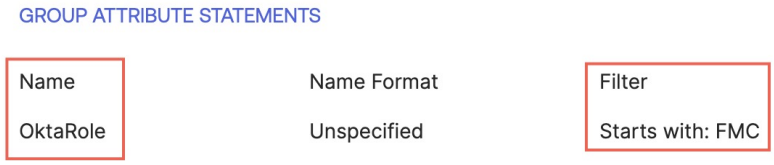
ステップ 5 **[グループ属性ステートメント（Group Attribute Statements）]** の下で、次のように操作します：

- **[名前（Name）]** には、Firewall Management Center SSO 設定で **[グループメンバーの属性（Group Member Attribute）]** に入力したものと同じ文字列を使用します（次における

Okta のユーザーロールマッピングの設定： Firewall Management Center, on page 44 のステップ 4 を参照）。

- [フィルタ（Filter）] には、Firewall Management Center からグループのメンバーに割り当てるロールを表す式を指定します。Okta は、この値をユーザーがメンバーであるグループの名前と比較し、一致するグループ名を Firewall Management Center に送信します。これらのグループでは、Firewall Management Center は指定したユーザロールとドメインを割り当てます。

次の例では、**OktaRole** が新しい SAML グループ属性の名前で、フィルタは「**Starts with FMC**」です。



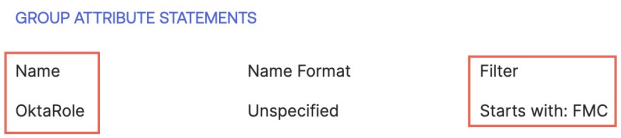
ステップ 6 [次へ（Next）] をクリックし、続けて [完了（Finish）] をクリックします。

グループの Okta ロールマッピングの例

次の例を考えてみます。

Okta のグループのロールマッピングでは、名前が Firewall Management Center の **グループメンバー属性** の名前と一致する必要があるカスタムグループ属性を作成できます。この例では、ロール マッピング用にグループ ロール属性 `OktaRole` が、名前が Firewall Management Centerで始まるすべてのグループに `OktaRole` 属性を使用するように指定するフィルタとともに作成されています。Oktaは、ログインアサーション中にグループ属性 `OktaRole` を Firewall Management Center に送信します。Okta でのグループ属性の設定の詳細については、Okta IdP におけるロールマッピングのためのグループ属性の設定, on page 48を参照してください。

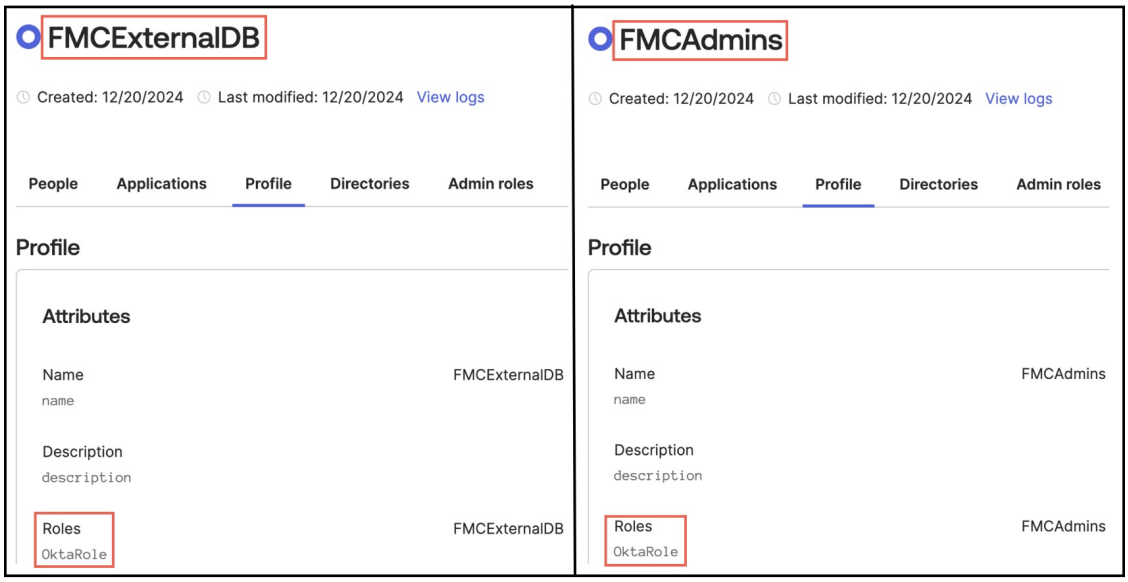
次の図は、Okta の**グループ属性ステートメント**を示しています。



Okta IdP には 2 つのグループがあります。

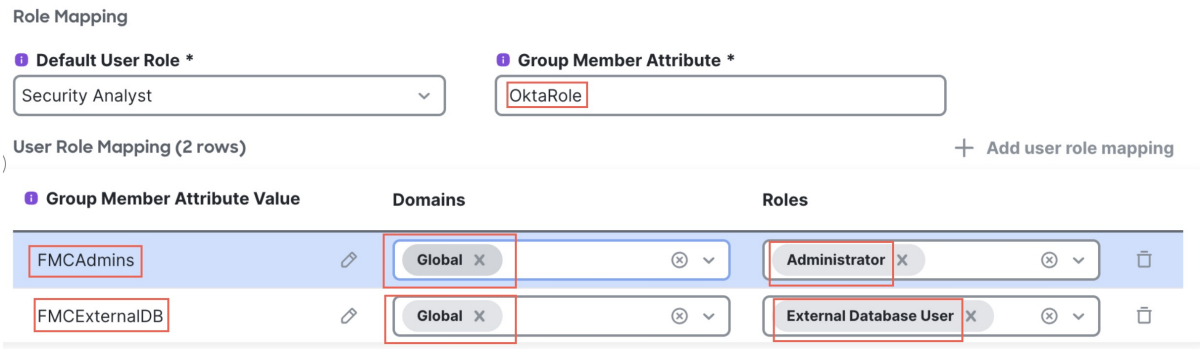
- FMCExternalDB：Firewall Management Centerで外部データベースのユーザーロールが割り当てられるユーザー用。
- FMCAdmins：Firewall Management Centerで 管理者ロールが割り当てられるユーザー用。

次の図は、2 つのグループを示しています。



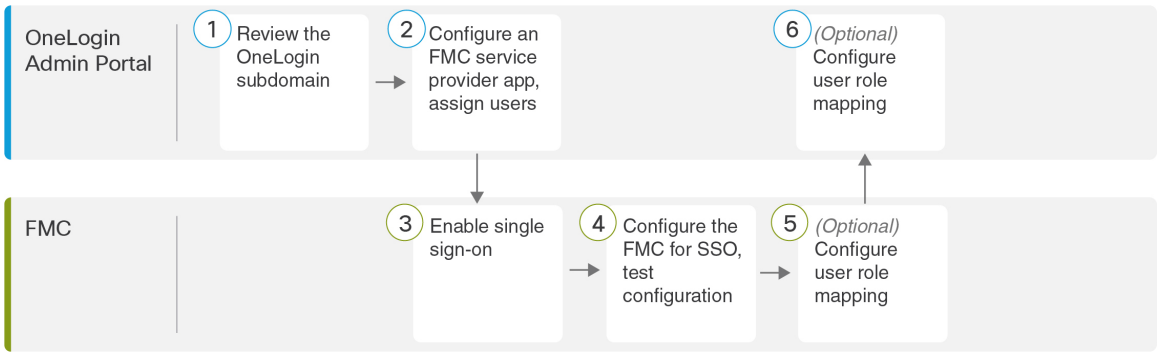
SSO ユーザーが Firewall Management Center にログインすると、Okta は、Firewall Management Center にグループ ロール属性`OktaRole` を提示します。Firewall Management Center は、この属性を、Firewall Management Centerで **グループメンバー属性**（`OktaRole`）として構成された文字列と比較します。Okta グループ属性フィルタに従って、名前が FMC で始まるすべてのグループが、**グループ メンバー属性値**の値として見なされます。Okta IdP グループ `FMCAdmins` および `FMCExternalDB` のメンバーであるユーザーは、構成済みドメインへのアクセス権を持つ構成済みロールにマッピングされます。一致するものが見つからない場合、Firewall Management Center は設定可能なデフォルトのユーザー ロールをユーザーに付与します。

次の図は、この例の Firewall Management Center でのユーザー ロール マッピングを示しています。



OneLogin を使用したシングルサインオンの設定

OneLogin を使用して SSO を設定するには、次のタスクを参照してください。



1	Firewall Management Center	OneLogin サブドメインの確認, on page 51
2	Firewall Management Center	OneLogin の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 52
3	OneLogin 管理ポータル	Firewall Management Centerでのシングルサインオンの有効化, on page 38
4	OneLogin 管理ポータル	OneLogin SSO 用の Firewall Management Center の設定, on page 54
5	OneLogin 管理ポータル	Firewall Management Center における OneLogin のユーザーロールマッピングの設定, on page 55
6	Firewall Management Center	OneLogin IdP におけるユーザーロールマッピングの設定, on page 57

OneLogin サブドメインの確認

OneLogin では、ユーザーが同じ SSO アカウントでアクセスできるすべてのフェデレーションデバイスとアプリケーションを含むエンティティは、サブドメインと呼ばれます。Firewall Management Center を OneLogin サブドメインに追加する前に、その設定についてよく理解してください。次の質問を考慮してください。

- Firewall Management Center にアクセスできるユーザーは何人ですか？
- ユーザーは、グループの OneLogin サブドメインのメンバーですか？
- Active Directory、Google Apps、LDAP などのサードパーティディレクトリのユーザーとグループは、OneLogin サブドメインと同期されていますか？
- Firewall Management Center で SSO をサポートするために、OneLogin サブドメインにユーザーまたはグループを追加する必要がありますか？
- どのような Firewall Management Center のユーザーロールの割り当てを行いますか？（ユーザーロールを割り当てない場合は、Firewall Management Center が構成可能なデフォルトのユーザーロールをすべての SSO ユーザーに自動的に割り当てます）。

- 必要なユーザーロールマッピングをサポートするには、OneLogin サブドメイン内のユーザーとグループをどのように編成する必要がありますか？

個人ユーザーまたはグループに基づいてFirewall Management Centerのロールがマッピングされるように構成できますが、単一のFirewall Management Centerのアプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。

このドキュメントは、ユーザーが OneLogin 管理ポータルに精通していて、スーパーユーザー権限を持つアカウントを持っていることを前提としています。ユーザーロールマッピングを構成するには、カスタムユーザーフィールドをサポートする OneLogin Unlimited プランへのサブスクリプションも必要です。詳細が必要な場合は、オンラインで入手できるOneLoginのドキュメントを参照してください。

OneLogin の Firewall Management Center サービス プロバイダー アプリケーションの設定

OneLogin 管理ポータルでこれらの手順を使用して、OneLogin 内に Firewall Management Center サービス プロバイダー アプリケーションを作成し、そのアプリケーションにユーザーまたはグループを割り当てます。SAML SSO の概念と OneLogin 管理ポータルに精通している必要があります。このドキュメントでは、完全に機能する SSO 組織を確立するために必要なすべての OneLogin の機能について説明しているわけではありません。たとえば、ユーザーとグループを作成したり、別のユーザー管理アプリケーションからユーザーとグループの定義をインポートしたりするには、OneLogin のドキュメントを参照してください。

Note Firewall Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

Note Firewall Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、OneLogin から Firewall Management Center にユーザーロール情報を伝達する単一の属性を構成する必要があります。

Before you begin

- OneLogin サブドメインとそのユーザーおよびグループについて理解します。OneLogin サブドメインの確認, on page 51を参照してください。
- 必要に応じて、OneLogin サブドメイン内にユーザーアカウントを作成します。

Note システムでは、SSO アカウントのユーザー名と、SAML ログイン プロセス中に IdP が Firewall Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービスプロバイダー アプリケーションを設定し、Firewall Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Firewall Management Center のログイン URL を確認します（`https://ipaddress_or_hostname/`）。

Note Firewall Management Center Web インターフェイスに複数の URL（たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで設定するログイン URL を使用して Firewall Management Center にアクセスする必要があります。

Procedure

ステップ 1 [SAMLテストコネクタ（詳細）（SAML Test Connector (Advanced)）] をベースとして使用して、Firewall Management Center サービス プロバイダー アプリケーションを作成します。

ステップ 2 次の設定を使用してアプリケーションを設定します。

- [対象者（エンティティID）（Audience (Entity ID)）] については、文字列 `/saml/metadata` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/metadata`。
- [受信者（Recipient）] については、文字列 `/saml/acs` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [ACS（コンシューマ）URL検証（ACS (Consumer) URL Validator）] については、OneLogin が正しい Firewall Management Center URL を使用していることを確認するために使用する式を入力します。ACS URL を使用して次のように変更することで、単純なバリデータを作成できます。
  - ACS URL の先頭に ^ を追加します。
  - ACS URL の末尾に $ を追加します。
  - ACS URL 内のすべての / と ? の前に \ を挿入します。

たとえば、ACS URL が `https://ExampleFMC/saml/acs` の場合、適切な URL バリデータは `^https:\/\/ExampleFMC\/saml\/acs$` になります。

- [ACS（コンシューマ）URL（ACS (Consumer) URL）] については、文字列 `/saml/acs` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [ログインURL（Login URL）] については、文字列 `/saml/acs` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [SAMLイニシエータ（SAML Initiator）] には、`Service Provider` を選択します。

ステップ 3 OneLogin ユーザーを Firewall Management Center サービス プロバイダー アプリケーションに割り当てます。

ステップ 4 （オプション）Firewall Management Center での SSO セットアップを簡単にするために、Firewall Management Center サービス プロバイダー アプリケーションの SAML XML メタデータを OneLogin からローカルコンピュータにダウンロードできます。

What to do next

シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください。

OneLogin SSO 用の Firewall Management Center の設定

Firewall Management Center Web インターフェイスでこれらの手順を使用します。

Before you begin

- OneLogin 管理ポータルで Firewall Management Center サービス プロバイダー アプリケーションを作成します。OneLogin の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 52を参照してください。
- シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください。

Procedure

ステップ 1 （このステップはFirewall Management Centerでのシングルサインオンの有効化, on page 38から直接続きます）。[OneLoginメタデータの設定（Configure OneLogin Metadata）] ダイアログには、2 つの選択肢があります。

- SSO 構成情報を手動で入力するには：
  - **a.** [手動設定（Manual Configuration）] オプションボタンをクリックします。
  - **b.** OneLogin サービス プロバイダー アプリケーションから次の SSO 構成値を入力します。

- [アイデンティティプロバイダーのシングルサインオンURL（Identity Provider Single Sign-On URL）]：OneLogin からの **SAML 2.0 エンドポイント（HTTP）**を入力します。
- [アイデンティティプロバイダー発行元（Identity Provider Issuer）]：OneLogin からの**発行元 URL** を入力します。
- [X.509証明書（X.509 Certificate）]：OneLogin からの **X.509 証明書**を入力します。

- OneLogin によって生成された XML メタデータファイルをローカルコンピュータに保存した場合（OneLogin の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 52のステップ 4）、ファイルを Firewall Management Center にアップロードできます。
  a. [XMLファイルのアップロード（Upload XML File）]オプションボタンをクリックします。
  b. 画面の指示に従って、ローカルコンピュータ上の XML メタデータファイルに移動して選択します。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）]ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Firewall Management Center の SSO 構成と OneLogin サービス プロバイダー アプリケーション構成を確認し、エラーを修正してから再試行します。

ステップ 5 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

What to do next

オプションで、SSOユーザーのユーザーロールマッピングを構成できます。Firewall Management Center における OneLogin のユーザーロールマッピングの設定, on page 55を参照してください。ロールマッピングを構成しないことを選択した場合、デフォルトで、Firewall Management Center にログインするすべての SSO ユーザーに、Firewall Management Center における OneLogin のユーザーロールマッピングの設定, on page 55のステップ 4 で構成したユーザーロールが割り当てられます。

Firewall Management Center における OneLogin のユーザーロールマッピングの設定

Firewall Management Center Web インターフェイスでユーザーロールマッピングを構成するフィールドは、SSO プロバイダーの選択に関係なく同じです。ただし、構成する値では、使用する SAML SSO プロバイダーのユーザーロールマッピングの導入方法を考慮する必要があります。

Before you begin

- OneLogin のユーザーとグループを確認します。OneLogin サブドメインの確認, on page 51 を参照してください。
- Firewall Management Center の SSO サービス プロバイダー アプリケーションを設定します。OneLogin の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 52を参照してください。
- Firewall Management Center でシングルサインオンを有効にして設定します。Firewall Management Centerでのシングルサインオンの有効化, on page 38およびOneLogin の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 52を参照してください。

Procedure

ステップ 1 [システム（System）]（⚙） > **[ユーザー（Users）]** > **[シングルサインオン（Single Sign-On）]** を選択します。

ステップ 2 **[詳細設定（Advanced Configuration）]** を展開します。

ステップ 3 **[デフォルトのユーザーロール（Default User Role）]** ドロップダウン リストから、ユーザーを割り当てるデフォルトの Firewall Management Center ユーザーロールを選択します。

ステップ 4 **[グループメンバー属性（Group Member Attribute）]** フィールドに、ユーザーまたはグループの Firewall Management Center ユーザー ロール マッピング用に OneLogin で設定された属性を入力します。OneLogin IdP における個人ユーザーのユーザーロールマッピングの設定, on page 57 のステップ 1 または OneLogin IdP におけるグループのユーザーロールマッピングの設定, on page 59 のステップ 1 を参照してください。

ステップ 5 1 つ以上のユーザー ロールマッピングを設定し、それらを 1 つ以上のドメインに関連付けます。

a) **[グループ メンバー属性値（Group Member Attribute Value）]**で、**[編集（Edit）]** ボタンをクリックし、IdP で定義されている属性値と一致する文字列または正規表現として属性値を入力します。複数の値をカンマで区切って入力することもできます。

b) **[ドメイン（Domain）]** ドロップダウンリストで、ドメインを選択します。

c) **[ロール（Roles）]** ドロップダウン リストから、1つ以上のユーザー ロールを選択します。

Firewall Management Center は、属性値を、IdP が SSO ユーザー情報とともに Firewall Management Center に送信するユーザー ロールマッピング属性値と比較します。一致が見つかると、 Firewall Management Center は、構成されたドメインへのアクセスとともに、対応するロールをユーザーに付与します。

d) （オプション）**[ユーザー ロール マッピングの追加（Add User Role Mapping）]** をクリックして、ユーザー ロール マッピングをさらに追加します。

ステップ 6 [Test Configuration] をクリックします。システムに エラーメッセージが表示された場合は、Firewall Management Center の SSO 構成と Okta サービス プロバイダー アプリケーション構成を確認し、エラーを修正してから再試行します。

ステップ 7 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

What to do next

サービスプロバイダーアプリケーションでユーザーロールマッピングを構成します。OneLogin IdP におけるユーザーロールマッピングの設定, on page 57を参照してください。

OneLogin IdP におけるユーザーロールマッピングの設定

個々の権限またはグループの権限に基づいて、Onelogin 管理ポータルで SSO ユーザーロールマッピングを設定できます。

- 個人ユーザーの権限に基づいてマップするには、OneLogin IdP における個人ユーザーのユーザーロールマッピングの設定, on page 57を参照してください。
- グループの権限に基づいてマップするには、OneLogin IdP におけるグループのユーザーロールマッピングの設定, on page 59を参照してください。

SSO ユーザーが Firewall Management Center にログインすると、OneLogin は、OneLogin IdP で設定されたカスタムユーザーフィールドから値を取得するユーザーまたはグループロールの属性値を Firewall Management Center に提示します。.Firewall Management Center は、その属性値を **[グループメンバーの属性値（Group Member Attribute Value）]** フィールドの正規表現と比較し、ユーザーに設定されたロールと、設定されたドメインへのアクセス権を付与します。（一致するものが見つからない場合、Firewall Management Center は設定可能なデフォルトのユーザー ロールをユーザーに付与しますをユーザーに付与します）。

Note Firewall Management Center 単一では、グループと個人ユーザーの両方のロールマッピングをサポートできません。Firewall Management Center サービス プロバイダー アプリケーションに対して 1 つのマッピング方法を選択し、それを一貫して使用する必要があります。Firewall Management Center は、OneLogin で設定された 1 つのカスタムユーザーフィールドのみを使用してロールマッピングをサポートできます。一般に、グループベースのロールマッピングは、多数のユーザーがいる Firewall Management Center でより効率的です。OneLogin サブドメイン全体で確立されたユーザーとグループの定義を考慮する必要があります。

OneLogin IdP における個人ユーザーのユーザーロールマッピングの設定

OneLogin 管理ポータルを使用して、Firewall Management Center サービス プロバイダー アプリケーションのカスタムパラメータとカスタムユーザーフィールドを作成します。これらは、SSO ログインプロセス中に OneLogin がユーザーロール情報を Firewall Management Center に渡す手段を提供します。

Before you begin

- OneLogin サブドメインとそのユーザーとグループを確認します。OneLogin サブドメインの確認, on page 51を参照してください。

- OneLogin で Firewall Management Center サービス プロバイダー アプリケーションを作成して設定します。OneLogin の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 52を参照してください。
- Firewall Management Center における OneLogin のユーザーロールマッピングの設定, on page 55の説明に従って、SSO ユーザーロールマッピングを設定します。

Procedure

ステップ 1 Firewall Management Center サービス プロバイダー アプリケーションのカスタムパラメータを作成します。

- [フィールド名（Field Name）] には、Firewall Management Center SSO 設定で [グループメンバーの属性（Group Member Attribute）] に使用したものと同じ名前を使用します（Firewall Management Center における OneLogin のユーザーロールマッピングの設定, on page 55のステップ 4 を参照）。
- [値（Value）] には、`FMCUserRole` などのニーモニック名を指定します。これは、この手順のステップ 2 で構成する顧客ユーザーフィールドの名前と一致する必要があります。

ステップ 2 カスタムユーザーフィールドを作成して、Firewall Management Center のアクセス権を持つ各 OneLogin ユーザーのユーザーロール情報を含めます。

- フィールド [名前（Name）] には、`FMCUserRole` などのニーモニック名を指定します。これは、この手順のステップ 1 で説明されているアプリケーション カスタム パラメータに指定された値と一致する必要があります。
- [短縮名（Short name）] には、フィールドの省略された代替名を指定します（これは OneLogin プログラマチック インターフェイスに使用されます）。

ステップ 3 Firewall Management Center サービス プロバイダー アプリケーションへのアクセス権を持つ各ユーザーについて、この手順のステップ 2 で作成したカスタムユーザーフィールドに値を割り当てます。

ユーザーが SSO を使用して Firewall Management Center にログインする場合、そのユーザーに対してこのフィールドに割り当てる値は、Firewall Management Center が SSO 構成で Firewall Management Center ユーザーロールに割り当てた式と比較する値になります（Firewall Management Center における OneLogin のユーザーロールマッピングの設定, on page 55のステップ 5 を参照してください）。

What to do next

- さまざまなアカウントから SSO を使用して Firewall Management Center にログインし、期待どおりにユーザーに Firewall Management Center ユーザーロールが割り当てられることを確認することで、ロールマッピングスキームをテストします。

OneLogin IdP におけるグループのユーザーロールマッピングの設定

OneLogin 管理ポータルを使用して、Firewall Management Center サービス プロバイダー アプリケーションのカスタムパラメータとカスタムユーザーフィールドを作成します。OneLoginユーザーをグループに割り当てます。次に、カスタムユーザーフィールドとユーザーグループの間に 1 つ以上のマッピングを作成し、OneLogin がユーザーのグループメンバーシップに基づいてカスタムユーザーフィールドに値を割り当てるようにします。これらは、SSO ログインプロセス中に OneLogin がグループベースのユーザーロール情報を Firewall Management Center に渡す手段を提供します。

OneLogin サービス プロバイダー アプリケーションは、次の 2 種類のグループのいずれかを使用する場合があります。

- OneLogin にネイティブなグループ。
- Active Directory、Google Apps、LDAP などのサードパーティ アプリケーションから同期されたグループ。

Firewall Management Center グループロールマッピングには、いずれかのタイプのグループを使用できます。このドキュメントでは、OneLogin グループを使用したロールマッピングについて説明します。サードパーティのアプリケーショングループを使用するには、組織で使用しているサードパーティのユーザー管理アプリケーションに精通している必要があります。詳細については、OneLogin のドキュメントを参照してください。

Before you begin

- OneLogin サブドメインとそのユーザーとグループを確認します。OneLogin サブドメインの確認, on page 51を参照してください。
- OneLogin で Firewall Management Center サービス プロバイダー アプリケーションを作成して設定します。OneLogin の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 52を参照してください。
- Firewall Management Center における OneLogin のユーザーロールマッピングの設定, on page 55の説明に従って、SSO ユーザーロールマッピングを設定します。

Procedure

ステップ 1 Firewall Management Center サービス プロバイダー アプリケーションのカスタムパラメータを作成します。

- [フィールド名（Field Name）] には、Firewall Management Center SSO 設定で [グループメンバーの属性（Group Member Attribute）] に使用したものと同じ名前を使用します（Firewall Management Center における OneLogin のユーザーロールマッピングの設定, on page 55のステップ 4 を参照）。
- [値（Value）] には、`FMCUserRole` などのニーモニック名を指定します。これは、この手順のステップ 2 で構成する顧客ユーザーフィールドの名前と一致する必要があります。

ステップ 2 カスタムユーザーフィールドを作成して、Firewall Management Center のアクセス権を持つ各 OneLogin ユーザーのユーザーロール情報を含めます。

- フィールド[名前（Name）]には、`FMCUserRole` などのニーモニック名を指定します。これは、この手順のステップ 1 で説明されているアプリケーション カスタム パラメータに指定された値と一致する必要があります。
- [短縮名（Short name）] には、フィールドの省略された代替名を指定します（これは OneLogin プログラマチック インターフェイスに使用されます）。

ステップ 3 1 つ以上のユーザー フィールド マッピングを作成して、この手順のステップ 2 で作成したカスタムユーザーフィールドにグループベースの値を割り当てます。各 OneLogin ユーザーグループに正しい Firewall Management Center ユーザーロールを割り当てるために必要な数のマッピングを作成します。

- ユーザーの [グループ（Group）] フィールドをグループ名と比較して、マッピングの**条件**を 1 つ以上作成します。
- 複数の**条件**を作成する場合は、マッピングを行うために、ユーザーのグループが条件の*一部*または*すべて*に一致する必要があるかどうかを選択します。
- マッピングの**アクション**を作成して、この手順のステップ 2 で作成したカスタムユーザーフィールドに値を割り当てます。フィールド [名前（Name）] と、指定した**条件**に一致するすべてのユーザーに対して OneLogin がこのカスタムユーザーフィールドに割り当てる文字列を指定します。

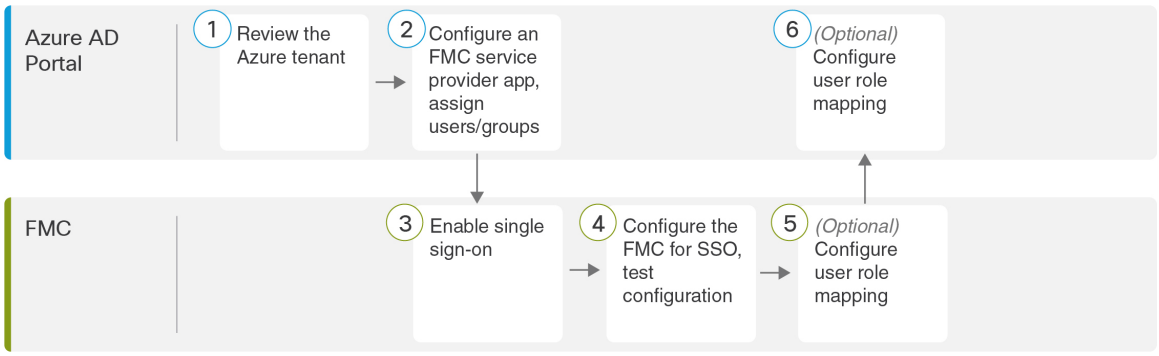
  Firewall Management Center では、この文字列を、Firewall Management Center における OneLogin のユーザーロールマッピングの設定, on page 55の手順 5 で各 Firewall Management Center ユーザーロールに割り当てた式と比較します。
- 変更が完了したら、**すべてのマッピングを再適用**します。

What to do next

- さまざまなアカウントから SSO を使用して Firewall Management Center にログインし、期待どおりにユーザーに Firewall Management Center ユーザーロールが割り当てられることを確認することで、ロールマッピングスキームをテストします。

Azure AD を使用したシングルサインオンの設定

Azure を使用して SSO を構成するには、次のタスクを参照してください。



1	Azure AD ポータル	Azure テナントの確認, on page 61
2	Azure AD ポータル	Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62
3	Firewall Management Center	Firewall Management Centerでのシングルサインオンの有効化, on page 38
4	Firewall Management Center	Azure SSO 用の Firewall Management Center の設定, on page 64
5	Firewall Management Center	Firewall Management Center での Azure のユーザーロールマッピングの設定, on page 66
6	Azure AD ポータル	Azure IdP におけるユーザーロールマッピングの設定, on page 67

Azure テナントの確認

Azure AD は、Microsoft のマルチテナント クラウド ベースのアイデンティティおよびアクセス管理サービスです。Azure では、ユーザーが同じ SSO アカウントでアクセスできるすべてのフェデレーテッドデバイスが含まれているエンティティをテナントと呼びます。Firewall Management Center を Azure テナントに追加する前に、その組織についてよく理解してください。次の質問を考慮してください。

- Firewall Management Center にアクセスできるユーザーは何人ですか？
- ユーザーは、グループの Azure テナントのメンバーですか？
- 別のディレクトリ製品からのユーザーとグループですか？
- Firewall Management Center で SSO をサポートするために、Azure テナントにユーザーまたはグループを追加する必要がありますか？
- どのような Firewall Management Center のユーザーロールの割り当てを行いますか？（ユーザーロールを割り当てない場合は、Firewall Management Center が構成可能なデフォルトのユーザーロールをすべての SSO ユーザーに自動的に割り当てます）。

- 必要なユーザーロールマッピングをサポートするには、Azure テナント内のユーザーとグループをどのように編成する必要がありますか？
- 個人ユーザーまたはグループに基づいて Firewall Management Center のロールがマッピングされるように構成できますが、単一の Firewall Management Center のアプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。

このドキュメントは、ユーザーがすでに Azure Active Directory ポータルに精通していて、Azure AD テナントのアプリケーション管理者権限を持つアカウントを持っていることを前提としています。Firewall Management Center は、テナント固有のシングルサインオンおよびシングルサインアウトのエンドポイントでのみ Azure SSO をサポートしていることに注意してください。Azure AD Premium P1 以上のライセンスとグローバル管理者権限が必要です。詳細については、Azure のドキュメントを参照してください。

Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定

Azure Active Directory ポータルを使用して、Azure Active Directory テナント内に Firewall Management Center サービス プロバイダー アプリケーションを作成し、基本的な構成設定を確立します。

Note Firewall Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

Note Firewall Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、OneLogin から Firewall Management Center にユーザーロール情報を伝達する単一の属性を構成する必要があります。

Before you begin

- Azure テナントとそのユーザーおよびグループについて理解します。Azure テナントの確認, on page 61を参照してください。
- 必要に応じて、Azure テナントにユーザーアカウントやグループを作成します。

Note システムでは、SSO アカウントのユーザー名と、SAML ログイン プロセス中に IdP が Firewall Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービスプロバイダー アプリケーションを設定し、Firewall Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Firewall Management Center のログイン URL を確認します（`https://ipaddress_or_hostname`）

Note Firewall Management Center Web インターフェイスに複数の URL（たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで構成するログイン URL を使用して Firewall Management Center にアクセスする必要があります。

Procedure

ステップ 1 Azure AD SAML Toolkit をベースとして使用して、Firewall Management Center サービス プロバイダー アプリケーションを作成します。

ステップ 2 [基本的なSAML設定（Basic SAML Configuration）] の次の設定を使用してアプリケーションを設定します。

- [識別子（エンティティID）（Identifier (Entity ID)）] については、文字列 `/saml/metadata` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/metadata`。
- [応答URL（Assertion Consumer Service URL）（Reply URL (Assertion Consumer Service URL)）] については、文字列 `/saml/acs` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [サインオンURL（Sign on URL）] については、文字列 `/saml/acs` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。

ステップ 3 アプリケーションの**一意ユーザー識別子名（名前 ID）**請求を編集して、Firewall Management Center でのサインオンのユーザー名をユーザーアカウントに関連付けられた電子メールアドレスに強制します。

- [ソース（Source）] で `Attribute` を選択します。
- [ソース属性（Source attribute）]：`user.mail` を選択します。

ステップ 4 Firewall Management Center で SSO を保護するための証明書を生成します。証明書には次のオプションを使用します。

- [署名オプション（Signing Option）] で [SAML応答とアサーションに署名（Sign SAML Response and Assertion）] を選択します。
- [署名アルゴリズム（Signing Algorithm）] に [SHA-256] を選択します。

ステップ 5 Base-64バージョンの証明書をローカルコンピュータにダウンロードします。Firewall Management Center Web インターフェイスで Azure SSO を構成するときに必要になります。

ステップ 6 アプリケーションの SAML ベースのサインオン情報で、次の値をメモします。

- **[ログイン URL（Login URL）]**
- [Azure AD識別子（Azure AD Identifier）]

Firewall Management Center Web インターフェイスで Azure SSO を構成するときに、これらの値が必要になります。

ステップ 7 （オプション）Firewall Management Center での SSO セットアップを簡単にするために、Firewall Management Center サービス プロバイダー アプリケーションの SAML XML メタデータファイル（Azure Portal では**フェデレーションメタデータ XML** と呼ばれます）をローカルコンピュータにダウンロードできます。

ステップ 8 既存の Azure ユーザーとグループを Firewall Management Center サービスアプリケーションに割り当てます。

Note
Firewall Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

Note
ユーザーのロールマッピングを構成する場合、個人ユーザー権限またはグループ権限に基づいてロールがマッピングされるように構成できますが、単一の Firewall Management Center のアプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。

What to do next

シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください。

Azure SSO 用の Firewall Management Center の設定

Firewall Management Center Web インターフェイスでこれらの手順を使用します。

Before you begin

- Azure AD ポータルで Firewall Management Center サービス プロバイダー アプリケーションを作成します。Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62を参照してください。
- シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください。

Procedure

ステップ 1 （このステップはFirewall Management Centerでのシングルサインオンの有効化, on page 38から直接続きます）。[Azureメタデータの設定（Configure Azure Metadata）] ダイアログには、2 つの選択肢があります。

- SSO 構成情報を手動で入力するには：
  - **a.** [手動設定（Manual Configuration）] オプションボタンをクリックします。
  - **b.** Azure SSO サービス プロバイダー アプリケーションから取得した値を入力します。
    - [アイデンティティプロバイダーのシングルサインオンURL（Identity Provider Single Sign-On URL）] には、Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62のステップ 6 で書き留めた**ログイン URL** を入力します。
    - [アイデンティティプロバイダー発行元（Identity Provider Issuer）] には、Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62のステップ 6 で書き留めた **Azure AD 識別子**を入力します。
    - [X.509証明書（X.509 Certificate）] には、Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62のステップ 5 で Azure からダウンロードした証明書を使用します。（テキストエディタを使用して証明書ファイルを開き、内容をコピーして [X.509証明書（X.509 Certificate）] フィールドに貼り付けます。）
- Azure によって生成された XML メタデータファイルをローカルコンピュータに保存した場合（Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62のステップ 7）、ファイルを Firewall Management Center にアップロードできます。
  - **a.** [XMLファイルのアップロード（Upload XML File）] オプションボタンをクリックします。
  - **b.** 画面の指示に従って、ローカルコンピュータ上の XML メタデータファイルに移動して選択します。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）] ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Firewall Management Center の SSO 設定と Azure サービス プロバイダー アプリケーションを確認し、エラーを修正してから再試行します。

ステップ 5 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

What to do next

オプションで、SSO ユーザーのロールマッピングを設定できます。Firewall Management Center での Azure のユーザーロールマッピングの設定, on page 66を参照してください。ロールマッピングを設定しないことを選択した場合、デフォルトで、Firewall Management Center にログインするすべての SSO ユーザーに、Firewall Management Center での Azure のユーザーロールマッピングの設定, on page 66のステップ 4 で設定したデフォルトユーザーロールが割り当てられます。

Firewall Management Center での Azure のユーザーロールマッピングの設定

Firewall Management Center Web インターフェイスでユーザーロールマッピングを構成するフィールドは、SSO プロバイダーの選択に関係なく同じです。ただし、構成する値では、使用する SAML SSO プロバイダーのユーザーロールマッピングの導入方法を考慮する必要があります。

Before you begin

- 既存の Azure ユーザーとグループを確認します。Azure テナントの確認, on page 61を参照してください。
- Firewall Management Center の SSO サービス プロバイダー アプリケーションを設定します。Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62を参照してください。
- Firewall Management Center でシングルサインオンを有効にして設定します。Firewall Management Centerでのシングルサインオンの有効化, on page 38およびAzure SSO 用の Firewall Management Center の設定, on page 64を参照してください。

Procedure

ステップ 1 [システム（System）]（⚙）>**[ユーザー（Users）]**>**[シングルサインオン（Single Sign-On）]** を選択します。

ステップ 2 **[詳細設定（Advanced Configuration）]** を展開します。

ステップ 3 **[デフォルトのユーザーロール（Default User Role）]** ドロップダウン リストから、ユーザーを割り当てるデフォルトの Firewall Management Center ユーザーロールを選択します。

ステップ 4 **[グループ メンバー属性（Group Member Attribute）]** フィールドに、ユーザーまたはグループの Firewall Management Center ユーザー ロール マッピングのために Azure で設定された属性を入力します。Azure IdP における個人ユーザーのユーザーロールマッピングの設定, on page 68 のステップ 1 または Azure IdP におけるグループのユーザーロールマッピングの設定, on page 69 のステップ 1 を参照してください。

ステップ 5 1 つ以上のユーザー ロールマッピングを設定し、それらを 1 つ以上のドメインに関連付けます。

a) **[グループ メンバー属性値（Group Member Attribute Value）]**で、**[編集（Edit）]** ボタンをクリックし、IdP で定義されている属性値と一致する文字列または正規表現として属性値を入力します。複数の値をカンマで区切って入力することもできます。

b) **[ドメイン（Domain）]** ドロップダウンリストで、ドメインを選択します。

c) **[ロール（Roles）]** ドロップダウンリストから、1 つ以上のユーザー ロールを選択します。

Firewall Management Center は、属性値を、IdP が SSO ユーザー情報とともに Firewall Management Center に送信するユーザー ロールマッピング属性値と比較します。一致が見つかると、 Firewall Management Center は、構成されたドメインへのアクセスとともに、対応するロールをユーザーに付与します。

d) （オプション）**[ユーザー ロール マッピングの追加（Add User Role Mapping）]** をクリックして、ユーザー ロール マッピングをさらに追加します。

ステップ 6 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Firewall Management Center の SSO 構成と Okta サービス プロバイダー アプリケーション構成を確認し、エラーを修正してから再試行します。

ステップ 7 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

What to do next

サービス プロバイダー アプリケーションでユーザーロールマッピングを構成します。Azure IdP におけるユーザーロールマッピングの設定, on page 67を参照してください。

Azure IdP におけるユーザーロールマッピングの設定

個人ユーザーの権限またはグループの権限に基づいて、Azure AD ポータルで SSO ユーザーロールマッピングを設定できます。

- 個人ユーザーのアクセス許可に基づいてマップするには、「Azure IdP における個人ユーザーのユーザーロールマッピングの設定」を参照してください。
- グループのアクセス許可に基づいてマップするには、「Azure IdP におけるグループのユーザーロールマッピングの設定」を参照してください。

SSO ユーザーが Firewall Management Center にログインすると、Azure は、Azure AD ポータルで設定されたアプリケーションロールから値を取得するユーザーまたはグループロールの属性値を Firewall Management Center に提示します。Firewall Management Center は、その属性値を **[グループメンバーの属性値（Group Member Attribute Value）]** フィールドの正規表現と比較

し、ユーザーに設定されたロールと、設定されたドメインへのアクセス権を付与します。（一致するものが見つからない場合、Firewall Management Center は設定可能なデフォルトのユーザー ロールをユーザーに付与しますをユーザーに付与します）。

Note Firewall Management Center 単一では、グループと個人ユーザーの両方のロールマッピングをサポートできません。Firewall Management Center サービス プロバイダー アプリケーションに対して 1 つのマッピング方法を選択し、それを一貫して使用する必要があります。Firewall Management Center は、Azure で構成された 1 つの要求のみを使用してロールマッピングをサポートできます。一般に、グループベースのロールマッピングは、多数のユーザーがいる Firewall Management Center でより効率的です。Azure テナント全体で確立されたユーザーとグループの定義を考慮する必要があります。

Azure IdP における個人ユーザーのユーザーロールマッピングの設定

Azure で Firewall Management Center サービスアプリケーションの個人ユーザーのロールマッピングを確立するには、Azure AD ポータルを使用してアプリケーションに要求を追加し、アプリケーションの登録マニフェストにロールを追加して、ロールをユーザーに割り当てます。

Before you begin

- Azure テナントを確認します。Azure テナントの確認, on page 61を参照してください。
- Azure で Firewall Management Center サービス プロバイダー アプリケーションを作成して設定します。Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62を参照してください。
- Firewall Management Center での Azure のユーザーロールマッピングの設定, on page 66の説明に従って、SSO ユーザーロールマッピングを設定します。

Procedure

ステップ 1 次の特性を使用して、Firewall Management Center サービスアプリケーションの SSO 設定にユーザー要求を追加します。

- [名前（Name）]：Firewall Management Center SSO 設定で [グループメンバーの属性（Group Member Attribute）] に入力したものと同じ文字列を使用します。（Firewall Management Center での Azure のユーザーロールマッピングの設定, on page 66のステップ 5 を参照してください）。
- [名前識別子の形式（Name identifier format）]：[永続（Persistent）] を選択します。
- [ソース（Source）]：`Attribute` を選択します。
- [ソース属性（Source attribute）]：`user.assignedroles` を選択します。

ステップ 2 Firewall Management Center サービスアプリケーションのマニフェスト（JSON 形式）を編集し、アプリケーションロールを追加して、SSO ユーザーに割り当てる Firewall Management Center ユーザーロールを表します。最も簡単な方法は、既存のアプリケーションロール定義をコピーして、次のプロパティを変更することです。

- `displayName`：AD Azure ポータルで表示されるロールの名前。
- `description`：ロールの簡単な説明。
- `Id`：マニフェスト内の ID プロパティの中で一意である必要がある英数字。
- `value`：1 つ以上の Firewall Management Center ユーザーロールを表す文字列。（注：Azure では、この文字列にスペースを含めることはできません）。

ステップ 3 Firewall Management Center サービスアプリケーションに割り当てられたユーザーごとに、そのアプリケーションのマニフェストに追加したアプリケーションロールの 1 つを割り当てます。ユーザーが SSO を使用して Firewall Management Center にログインする場合、そのユーザーに割り当てるアプリケーションロールは、Azure がサービスアプリケーションの要求で Firewall Management Center に送信する値です。Firewall Management Center は、SSO 設定で Firewall Management Center ユーザーロールに割り当てた式と要求を比較し（Firewall Management Center での Azure のユーザーロールマッピングの設定, on page 66のステップ 6 を参照）、一致するすべての Firewall Management Center ユーザーロールをユーザーに割り当てます。

What to do next

- さまざまなアカウントから SSO を使用して Firewall Management Center にログインし、期待どおりにユーザーに Firewall Management Center ユーザーロールが割り当てられることを確認することで、ロールマッピングスキームをテストします。

Azure IdP におけるグループのユーザーロールマッピングの設定

Azure で Firewall Management Center サービスアプリケーションのユーザーグループのロールマッピングを確立するには、Azure AD ポータルを使用してアプリケーションに要求を追加し、アプリケーションの登録マニフェストにロールを追加して、ロールをグループに割り当てます。

Before you begin

- Azure テナントを確認します。Azure テナントの確認, on page 61を参照してください。
- Azure で Firewall Management Center サービス プロバイダー アプリケーションを作成して設定します。Azure の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 62を参照してください。
- Firewall Management Center での Azure のユーザーロールマッピングの設定, on page 66の説明に従って、SSO ユーザーロールマッピングを設定します。

Procedure

ステップ 1 次の特性を使用して、Firewall Management Center サービスアプリケーションの SSO 設定にユーザー要求を追加します。

- [名前（Name）]：Firewall Management Center SSO 設定で [グループメンバーの属性（Group Member Attribute）] に入力したものと同じ文字列を使用します。（Firewall Management Center での Azure のユーザーロールマッピングの設定, on page 66のステップ 5 を参照してください）。
- [名前識別子の形式（Name identifier format）]：[永続（Persistent）] を選択します。
- [ソース（Source）]：`Attribute` を選択します。
- [ソース属性（Source attribute）]：`user.assignedroles` を選択します。

ステップ 2 Firewall Management Center サービスアプリケーションのマニフェスト（JSON 形式）を編集し、アプリケーションロールを追加して、SSO ユーザーに割り当てる Firewall Management Center ユーザーロールを表します。最も簡単な方法は、既存のアプリケーションロール定義をコピーして、次のプロパティを変更することです。

- `displayName`：Ad Azure ポータルで表示されるロールの名前。
- `description`：ロールの簡単な説明。
- `Id`：マニフェスト内の ID プロパティの中で一意である必要がある英数字。
- `value`：1 つ以上の Firewall Management Center ユーザーロールを表す文字列。（Azure では、この文字列にスペースを含めることはできません）。

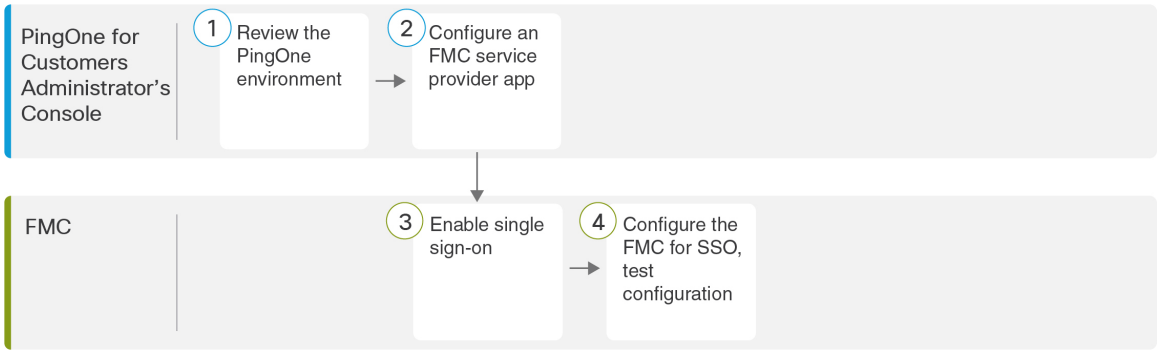
ステップ 3 Firewall Management Center サービスアプリケーションに割り当てられたグループごとに、そのアプリケーションのマニフェストに追加したアプリケーションロールの 1 つを割り当てます。ユーザーが SSO を使用して Firewall Management Center にログインする場合、そのユーザーのグループに割り当てるアプリケーションロールは、Azure がサービスアプリケーションの要求で Firewall Management Center に送信する値です。Firewall Management Center は、SSO 設定で Firewall Management Center ユーザーロールに割り当てた式と要求を比較し（Firewall Management Center での Azure のユーザーロールマッピングの設定, on page 66のステップ 6 を参照）、一致するすべての Firewall Management Center ユーザーロールをユーザーに割り当てます。

What to do next

さまざまなアカウントから SSO を使用して Firewall Management Center にログインし、期待どおりにユーザーに Firewall Management Center ユーザーロールが割り当てられることを確認することで、ロールマッピングスキームをテストします。

PingID を使用したシングルサインオンの設定

PingID の PingOne for Customers 製品を使用して SSO を設定するには、次のタスクを参照してください。



1	PingOne for Customers 管理者コンソール	PingID PingOne for Customers 環境の確認, on page 71。
2	PingOne for Customers 管理者コンソール	PingID PingOne for Customers の Firewall Management Center サービスプロバイダー アプリケーションの設定, on page 72。
3	Firewall Management Center	Firewall Management Centerでのシングルサインオンの有効化, on page 38。
4	Firewall Management Center	PingID PingOne for Customers を使用した SSO 用の Firewall Management Center の設定, on page 74。

PingID PingOne for Customers 環境の確認

PingOne for Customers は、PingID のクラウドでホストされる Identity-as-a-Service（IDaaS）製品です。PingOne for Customers では、ユーザーが同じ SSO アカウントでアクセスできるすべてのフェデレーテッドデバイスが含まれているエンティティを環境と呼びます。Firewall Management Center を PingOne 環境に追加する前に、その組織についてよく理解してください。次の質問を考慮してください。

- Firewall Management Center にアクセスできるユーザーは何人ですか？
- Firewall Management Center で SSO をサポートするために、ユーザーを追加する必要がありますか。

このドキュメントは、PingOne for Customers 管理者コンソールに精通していて、組織管理者ロールを持つアカウントを持っていることを前提としています。

PingID PingOne for Customers の Firewall Management Center サービス プロバイダー アプリケーションの設定

PingOne for Customers 管理者コンソールを使用して、PingOne for Customers 環境内に Firewall Management Center サービス プロバイダー アプリケーションを作成し、基本的な構成設定を確立します。このドキュメントでは、完全に機能する SSO 環境を確立するために必要な PingOne for Customers のすべての機能について説明しているわけではありません。たとえば、ユーザーを作成するには、PingOne for Customers のドキュメントを参照してください。

Before you begin

- PingOne for Customers 環境とそのユーザーについてよく理解してください。
- 必要に応じて、追加のユーザーを作成します。

Note システムでは、SSO アカウントのユーザー名と、SAML ログインプロセス中に IdP が Firewall Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービスプロバイダーアプリケーションを設定し、Firewall Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Firewall Management Center のログイン URL を確認します（`https://ipaddress_or_hostname`）

Note Firewall Management Center Web インターフェイスに複数の URL（たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで構成するログイン URL を使用して Firewall Management Center にアクセスする必要があります。

Procedure

ステップ 1 PingOne for Customer 管理者コンソールを使用して、次の設定を使用して環境内にアプリケーションを作成します。

- [Webアプリケーション（Web App）] のアプリケーションタイプを選択します。
- [SAML] の接続タイプを選択します。

ステップ 2 SAML 接続に次の設定を使用してアプリケーションを設定します。

- [ACS URL] については、文字列 `/sam/acs` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/acs`。
- [署名証明書（Signing Certificate）] で、[アサーションと応答の署名（Sign Assertion & Response）] を選択します。
- [署名アルゴリズム（Signing Algorithm）] には、RSA_SHA256 を選択します。
- [エンティティID（Entity ID）] については、文字列 `/saml/metadata` を Firewall Management Center ログイン URL に追加します。例：`https://ExampleFMC/saml/metadata`。
- [SLOバインド（SLO Binding）] で [HTTP POST] を選択します。
- [アサーション有効期間（Assertion Validity Duration）] には、300 と入力します。

ステップ 3 アプリケーションの SAML 接続情報にある、次の値に注目してください。

- シングルサインオンサービス（Single Sign-On Service）
- 発行者 ID（Issuer ID）

これらの値は、Firewall Management Center Web インターフェイスで PingID の PingOne for Customers 製品を使用して SSO を設定するときに必要になります。

ステップ 4 [SAML属性（SAML ATTRIBUTES）] で、単一の必須属性に対して次の選択を行います。

- [PINGONEユーザー属性（PINGONE USER ATTRIBUTE）]：`Email Address`
- [アプリケーション属性（APPLICATION ATTRIBUTE）]：`saml_subject`

ステップ 5 署名証明書を X509 PEM（`.crt`）形式でダウンロードし、ローカルコンピュータに保存します。

ステップ 6 （オプション）Firewall Management Center での SSO セットアップを簡単にするために、Firewall Management Center サービス プロバイダー アプリケーションの SAML XML メタデータファイルをローカルコンピュータにダウンロードできます。

ステップ 7 アプリケーションを有効にします。

What to do next

シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください。

PingID PingOne for Customers を使用した SSO 用の Firewall Management Center の設定

Before you begin

- PingOne for Customers 管理者コンソールで Firewall Management Center サービス プロバイダー アプリケーションを作成します。PingID PingOne for Customers の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 72を参照してください。
- シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください

Procedure

ステップ 1 （このステップはFirewall Management Centerでのシングルサインオンの有効化, on page 38から直接続きます）。[PingIDメタデータの設定（Configure PingID Metadata）] ダイアログには、2つの選択肢があります。

- SSO 構成情報を手動で入力するには：
  - **a.** [手動設定（Manual Configuration）] オプションボタンをクリックします。
  - **b.** PingOne for Customers 管理者コンソールから取得した値を入力します。
    - [アイデンティティプロバイダーのシングルサインオンURL（Identity Provider Single Sign-On URL）] には、PingID PingOne for Customers の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 72のステップ 3 で書き留めた**シングルサインオンサービス**を入力します。
    - [アイデンティティプロバイダー発行元（Identity Provider Issuer）] には、PingID PingOne for Customers の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 72のステップ 3 で書き留めた**発行者 ID** を入力します。
    - [X.509証明書（X.509 Certificate）] には、PingID PingOne for Customers の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 72のステップ 5 で PingOne for Customers からダウンロードした証明書を使用します。（テキストエディタを使用して証明書ファイルを開き、内容をコピーして [X.509証明書（X.509 Certificate）] フィールドに貼り付けます。）
- PingOne for Customers によって生成された XML メタデータファイルをローカル コンピュータに保存した場合（PingID PingOne for Customers の Firewall Management Center サービス プロバイダー アプリケーションの設定, on page 72のステップ 6）、**[XML ファイルのアップロード（Upload XML File）]** ラジオ ボタンをクリックして、ファイルを Firewall Management Center にアップロードできます。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）] ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 **[詳細設定（Advanced Configuration）]** を展開します。

ステップ 5 **[デフォルトのユーザーロール（Default User Role）]** ドロップダウン リストから、ユーザーを割り当てるデフォルトの Firewall Management Center ユーザーロールを選択します。

ステップ 6 **[グループ メンバー属性（Group Member Attribute）]** フィールドに、ユーザーまたはグループの Firewall Management Center ユーザー ロール マッピングのために PingID PingOne で設定した属性を入力します。

ステップ 7 1 つ以上のユーザー ロールマッピングを設定し、それらを 1 つ以上のドメインに関連付けます。

a) **[グループ メンバー属性値（Group Member Attribute Value）]**で、**[編集（Edit）]** ボタンをクリックし、IdP で定義されている属性値と一致する文字列または正規表現として属性値を入力します。複数の値をカンマで区切って入力することもできます。

b) **[ドメイン（Domain）]** ドロップダウンリストで、ドメインを選択します。

c) **[ロール（Roles）]** ドロップダウンリストから、1 つ以上のユーザー ロールを選択します。

Firewall Management Center は、属性値を、IdP が SSO ユーザー情報とともに Firewall Management Center に送信するユーザー ロールマッピング属性値と比較します。一致が見つかると、 Firewall Management Center は、構成されたドメインへのアクセスとともに、対応するロールをユーザーに付与します。

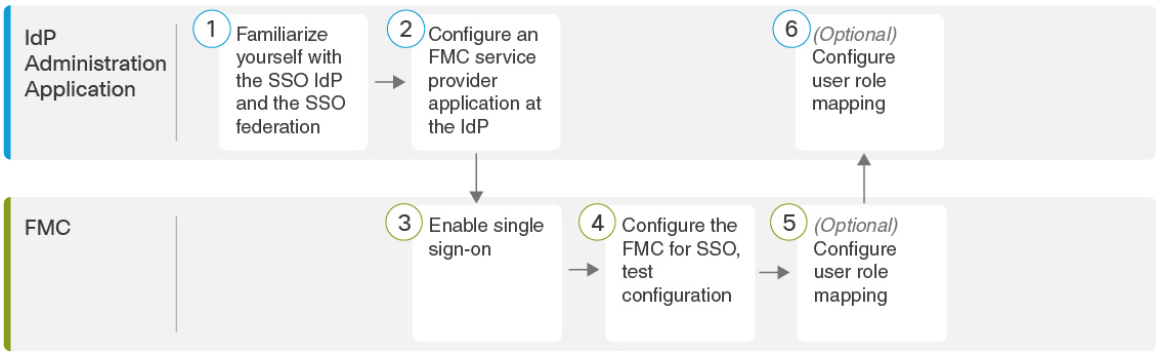
d) （オプション）**[ユーザー ロール マッピングの追加（Add User Role Mapping）]** をクリックして、ユーザー ロール マッピングをさらに追加します。

ステップ 8 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Firewall Management Center の SSO 構成と PingOne for Customers サービス プロバイダー アプリケーションを確認し、エラーを修正してから再試行します。

ステップ 9 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

SAML 2.0 準拠の SSO プロバイダーでのシングルサインオンの設定

Firewall Management Center は、SAML 2.0 SSO プロトコル準拠の SSO アイデンティティ プロバイダー（IdP）によるシングルサインオンをサポートしています。幅広い SSO プロバイダーを使用するための一般的な手順では、実行するタスクの概要を扱う必要があります。このドキュメントで具体的に扱われていないプロバイダーを使用して SSO を確立するには、選択した IdP に習熟している必要があります。これらのタスクは、SAML 2.0 準拠の SSO プロバイダーを使用したシングルサインオンのために Firewall Management Center を設定する手順を判断するために役立ちます。



1	IdP 管理アプリケーション	SSO アイデンティティ プロバイダーおよび SSO フェデレーションの理解, on page 76。
2	IdP 管理アプリケーション	SAML 2.0 準拠の SSO プロバイダー用の FMC サービス プロバイダー アプリケーションの設定, on page 77。
3	Firewall Management Center	Firewall Management Centerでのシングルサインオンの有効化, on page 38。
4	Firewall Management Center	SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Firewall Management Center の設定, on page 80。
5	Firewall Management Center	SAML 2.0 準拠の SSO プロバイダー向け Firewall Management Center でのユーザー ロールマッピングの設定, on page 81。
6	IdP 管理アプリケーション	SAML 2.0 準拠の SSO プロバイダーの IdP での Firewall Management Center ユーザー ロールマッピングの設定, on page 83。

SSO アイデンティティ プロバイダーおよび SSO フェデレーションの理解

次の点を考慮して、IdP ベンダーのドキュメントを読んでください。

- SSO プロバイダーは、ユーザーが IdP を使用する前にサービスにサブスクライブまたは登録することを要求していますか。

- SSOプロバイダーは、一般的なSSOの概念にどのような用語を使用しますか。たとえば、フェデレーテッドサービスプロバイダーアプリケーションのグループを参照するために、Okta は「組織」を使用しますが、Azure は「テナント」を使用します。
- SSO プロバイダーは SSO のみをサポートしていますか、それとも一連の機能（多要素認証やドメイン管理など）をサポートしていますか（これは、機能間で共有される一部の要素、特にユーザーとグループの構成に影響を与える可能性があります）。
- SSO を構成するために IdP ユーザーアカウントに必要な権限は何ですか。
- SSO プロバイダーは、サービス プロバイダー アプリケーションに対してどのような構成を確立する必要がありますか。たとえば、Okta は Firewall Management Center との通信を保護するために X509 証明書を自動的に生成しますが、Azure では Azure portal インターフェイスを使用してその証明書を生成する必要があります。
- ユーザーとグループはどのように作成および構成されますか。ユーザーはどのようにグループに割り当てられますか。ユーザーおよびグループは、サービス プロバイダー アプリケーションへのアクセスをどのように許可されますか。
- SSOプロバイダーは、SSO接続をテストする前に、サービスプロバイダーアプリケーションに少なくとも 1 人のユーザーを割り当てる必要がありますか。
- SSOプロバイダーはユーザーグループをサポートしていますか。ユーザー属性とグループ属性はどのように構成されますか。SSO構成で属性をFirewall Management Centerユーザーロールにマップするにはどうすればよいですか。
- Firewall Management Center で SSO をサポートするために、フェデレーションにユーザーまたはグループを追加する必要がありますか。
- ユーザーはグループのフェデレーションメンバーですか。
- ユーザーとグループの定義はIdPにネイティブですか。それともActive Directory、RADIUS、LDAP などのユーザー管理アプリケーションからインポートされますか。
- どのようなユーザーロールの割り当てを行いますか。（ユーザーロールを割り当てない場合は、Firewall Management Center が、ユーザーによる設定が可能なデフォルトのユーザーロールを、すべての SSO ユーザーに自動的に割り当てます）。
- 必要なユーザーロールマッピングをサポートする計画において、フェデレーション内のユーザーとグループをどのように編成する必要がありますか。

SAML 2.0 準拠の SSO プロバイダー用の FMC サービス プロバイダー アプリケーションの設定

通常、SSO プロバイダーでは、フェデレーション アプリケーションごとに IdP でサービス プロバイダー アプリケーションを設定する必要があります。SAML 2.0 SSO をサポートするすべての IdP では、サービス プロバイダー アプリケーションに同一の構成情報が必要になりますが、一部の IdP では構成設定が自動的に生成され、他の IdP ではすべての設定を自分で構成する必要があります。

Note Firewall Management Center アプリケーションにユーザーグループを割り当てることを計画している場合は、それらのグループ内のユーザーを個人として割り当てないでください。

Note Firewall Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、単一の属性を構成して、IdP からのユーザーロール情報を Firewall Management Center に伝達する必要があります。

Before you begin

- SSO フェデレーションとそのユーザーおよびグループについて理解します。SSO アイデンティティ プロバイダーおよび SSO フェデレーションの理解, on page 76を参照してください。
- IdP アカウントに、このタスクを実行するために必要な権限があることを確認します。
- 必要に応じて、SSO フェデレーションにユーザーアカウントやグループを作成します。

Note システムでは、SSO アカウントのユーザー名と、SAML ログイン プロセス中に IdP が Firewall Management Center に送信する NameID 属性の両方が有効な電子メールアドレスである必要があります。多くの IdP は、ログインしようとしているユーザーのユーザー名を NameID 属性として自動的に使用しますが、これが IdP に適しているかを確認する必要があります。IdP でサービスプロバイダー アプリケーションを設定し、Firewall Management Center への SSO アクセス権限を持つ IdP ユーザーアカウントを作成する場合は、このことに注意してください。

- ターゲット Firewall Management Center のログイン URL を確認します（`https://ipaddress_or_hostname`）

Note Firewall Management Center Web インターフェイスに複数の URL（たとえば、完全修飾ドメイン名と IP アドレス）でアクセスできる場合、SSO ユーザーは、一貫してこのタスクで設定するログイン URL を使用して Firewall Management Center にアクセスする必要があります。

Procedure

ステップ 1 IdP で新しいサービス プロバイダー アプリケーションを作成します。

ステップ 2 IdP に必要な値を設定します。Firewall Management Center で SAML 2.0 SSO 機能をサポートするために必要な、以下のフィールドを必ず含めてください。（SAML の概念には、さまざまな SSO サービスプロバイダーでさまざまな用語が使用されているため、このリストでは、IdP アプリケーションで適切な設定を見つけるために役立つこれらのフィールドの代替名を示しています）。

- サービスプロバイダーのエンティティ ID、サービスプロバイダー識別子、オーディエンス URI：サービスプロバイダー（Firewall Management Center）のグローバルに一意の名前で、URL としてフォーマットされます。これを作成するには、`https://ExampleFMC/saml/metadata` のように、Firewall Management Center ログイン URL に文字列 `/saml/metadata` を追加します。
- シングルサインオン URL、受信者 URL、アサーション コンシューマ サービス URL：ブラウザが IdP の代わりに情報を送信するサービスプロバイダー（Firewall Management Center）のアドレス。これを作成するには、`https://ExampleFMC/saml/acs` のように、Firewall Management Center ログイン URL に文字列 `saml/acs` を追加します。
- X.509 証明書：Firewall Management Center と IdP の間の通信を保護するための証明書。IdP の中には、証明書を自動的に生成するものもあれば、IDP インターフェイスを使用して明示的に生成する必要があるものもあります。

ステップ 3 （アプリケーションにグループを割り当てる場合はオプション）個人ユーザーを Firewall Management Center アプリケーションに割り当てます。（Firewall Management Center アプリケーションにグループを割り当てることを計画している場合は、それらのグループのメンバーを個人として割り当てないでください）。

ステップ 4 （個人ユーザーをアプリケーションに割り当てる場合はオプション）Firewall Management Center アプリケーションにユーザーグループを割り当てます。

ステップ 5 （オプション）一部の IdP には、SAML 2.0 標準に準拠するようにフォーマットされた、このタスクで設定した情報を含む SAML XML メタデータファイルを生成する機能があります。IdP にこの機能がある場合は、Firewall Management Center で SSO 設定プロセスを簡単に行うことができるように、ローカルコンピュータにこのファイルをダウンロードすることができます。

What to do next

シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください。

SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Firewall Management Center の設定

Firewall Management Center Web インターフェイスでこれらの手順を使用します。SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用に Firewall Management Center を設定するには、IdP からの情報が必要です。

Before you begin

- SSO フェデレーションの組織と、そのユーザーとグループを確認します。
- IdP の Firewall Management Center サービス プロバイダー アプリケーションを設定します。SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Firewall Management Center の設定, on page 80を参照してください。
- IdP から、サービス プロバイダー アプリケーションの次の SSO 設定情報を収集します。SAML の概念には、さまざまな SSO サービスプロバイダーでさまざまな用語が使用されているため、このリストでは、IdP アプリケーションで適切な値を見つけるために役立つこれらのフィールドの代替名を示しています。
  - アイデンティティ プロバイダーのシングルサインオン URL、ログイン URL：ブラウザが Firewall Management Center の代わりに情報を送信する IdP URL。
  - アイデンティティプロバイダー発行元、アイデンティティプロバイダー発行元URL、発行元 URL：多くの場合 URL としてフォーマットされる、IdP のグローバルに一意の名前。
  - Firewall Management Center と IdP の間の通信を保護するための X.509 デジタル証明書。
- シングルサインオンを有効にします。Firewall Management Centerでのシングルサインオンの有効化, on page 38を参照してください。

Procedure

ステップ 1 （このステップはFirewall Management Centerでのシングルサインオンの有効化, on page 38から直接続きます）。[SAMLメタデータの設定（Configure SAML Metadata）] ダイアログには、2 つの選択肢があります。

- SSO 構成情報を手動で入力するには：
  - **a.** [手動設定（Manual Configuration）] オプションボタンをクリックします。
  - **b.** SSO サービス プロバイダー アプリケーションから、以前に取得した次の値を入力します。
    - **アイデンティティ プロバイダーのシングルサインオン URL**
    - **アイデンティティ プロバイダー発行元**

- **X.509 証明書**

- IdP で生成された XML メタデータファイルを保存した場合（SAML 2.0 準拠の SSO プロバイダー用の FMC サービス プロバイダー アプリケーションの設定, on page 77のステップ 5）、ファイルを Firewall Management Center にアップロードできます。

  a. [XMLファイルのアップロード（Upload XML File）]オプションボタンをクリックします。

  b. 画面の指示に従って、ローカルコンピュータ上の XML メタデータファイルに移動して選択します。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 [メタデータの検証（Verify Metadata）]ダイアログで、構成パラメータを確認し、[保存（Save）] をクリックします。

ステップ 4 [Test Configuration] をクリックします。システムにエラーメッセージが表示された場合は、Firewall Management Center の SSO 設定と IdP でのサービス プロバイダー アプリケーション設定を確認し、エラーを修正してから再試行します。

ステップ 5 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

What to do next

オプションで、SSO ユーザーのユーザーロールマッピングを構成できます。SAML 2.0 準拠の SSO プロバイダー向け Firewall Management Center でのユーザー ロール マッピングの設定, on page 81を参照してください。ロールマッピングを設定しないことを選択した場合、デフォルトで、Firewall Management Center にログインするすべての SSO ユーザーに、SAML 2.0 準拠の SSO プロバイダー向け Firewall Management Center でのユーザー ロール マッピングの設定, on page 81のステップ 4 で設定したデフォルトユーザーロールが割り当てられます。

SAML 2.0 準拠の SSO プロバイダー向け Firewall Management Center でのユーザー ロール マッピングの設定

SAML SSO ユーザーロールマッピングを導入するには、IdP および Firewall Management Center で調整設定を確立する必要があります。

- IdP で、ユーザーまたはグループの属性を確立して、ユーザーロール情報を伝達し、それらに値を割り当てます。IdP は、SSO ユーザーを認証および承認すると、これらを Firewall Management Center に送信します。

- Firewall Management Center で、ユーザーに割り当てる各 Firewall Management Center ユーザーロールに値を関連付けます。

IdP が承認ユーザーに関連付けられたユーザーまたはグループ属性を Firewall Management Center に送信すると、Firewall Management Center は属性値を各 Firewall Management Center ユーザーロールに関連付けられた値と比較し、ユーザーを一致するすべてのロールに割り当て、ユー

ザーが構成済みドメインにアクセスできるようにします。Firewall Management Center は、Golang と Perl でサポートされている Google の RE2 正規表現標準規格の制限付きバージョンに準拠している正規表現として両方の値を扱うことにより、この比較を実行します。

Firewall Management Center Web インターフェイスでユーザーロールマッピングを構成するフィールドは、SSO プロバイダーの選択に関係なく同じです。ただし、構成する値では、使用する SAML SSO プロバイダーのユーザーロールマッピングの導入方法を考慮する必要があります。IdP は、ユーザーまたはグループ属性に構文制限を適用する場合があります。その場合、ロール名とそれらの要件と互換性のある正規表現を使用して、ユーザー ロール マッピング スキームを考案する必要があります。

Before you begin

- Firewall Management Center の SSO サービス プロバイダー アプリケーションを設定します。SAML 2.0 準拠の SSO プロバイダー用の FMC サービス プロバイダー アプリケーションの設定, on page 77を参照してください。
- Firewall Management Center でシングルサインオンを有効にして設定します。Firewall Management Centerでのシングルサインオンの有効化, on page 38およびSAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Firewall Management Center の設定, on page 80を参照してください。

Procedure

ステップ 1 [システム（System）]（⚙）>**[ユーザー（Users）]**>**[シングルサインオン（Single Sign-On）]**を選択します。

ステップ 2 [詳細設定（ロールマッピング）（Advanced Configuration (Role Mapping)）] を展開します。

ステップ 3 [デフォルトのユーザーロール（Default User Role）] ドロップダウンから、ユーザーをデフォルト値として割り当てる Firewall Management Center ユーザーロールを選択します。

ステップ 4 [グループメンバーの属性（Group Member Attribute）] を入力します。この文字列は、ユーザーまたはグループのいずれかを使用するユーザーロールマッピングのために IdP Firewall Management Center サービス プロバイダー アプリケーションで設定された属性名と一致する必要があります。（SAML 2.0 準拠の SSO プロバイダーの IdP での Firewall Management Center ユーザーロールマッピングの設定, on page 83のステップ 1 を参照。）

ステップ 5 1 つ以上のユーザー ロールマッピングを設定し、それらを 1 つ以上のドメインに関連付けます。

a) **[グループ メンバー属性値（Group Member Attribute Value）]**で、**[編集（Edit）]** ボタンをクリックし、IdP で定義されている属性値と一致する文字列または正規表現として属性値を入力します。複数の値をカンマで区切って入力することもできます。

b) **[ドメイン（Domain）]** ドロップダウンリストで、ドメインを選択します。

c) **[ロール（Roles）]** ドロップダウンリストから、1 つ以上のユーザーロールを選択します。

Firewall Management Center は、属性値を、IdP が SSO ユーザー情報とともに Firewall Management Center に送信するユーザー ロールマッピング属性値と比較します。一致が見

つかると、 Firewall Management Center は、構成されたドメインへのアクセスとともに、対応するロールをユーザーに付与します。

d) （オプション）**[ユーザー ロール マッピングの追加（Add User Role Mapping）]** をクリックして、ユーザー ロール マッピングをさらに追加します。

ステップ 6 [Test Configuration] をクリックします。システムに エラーメッセージが表示された場合は、Firewall Management Center の SSO 構成と Okta サービス プロバイダー アプリケーション構成を確認し、エラーを修正してから再試行します。

ステップ 7 システムが構成テストの成功を報告したら、[適用（Apply）] をクリックします。

What to do next

サービス プロバイダー アプリケーションでユーザーロールマッピングを構成します。SAML 2.0 準拠の SSO プロバイダーの IdP での Firewall Management Center ユーザーロールマッピングの設定, on page 83を参照してください。

SAML 2.0 準拠の SSO プロバイダーの IdP での Firewall Management Center ユーザーロールマッピングの設定

ユーザーロールマッピングを構成するための詳細な手順は、IdP ごとに異なります。サービスプロバイダーアプリケーションのカスタムユーザーまたはグループ属性を作成する方法を決定し、IdP で各ユーザーまたはグループの属性に値を割り当てて、ユーザーまたはグループの特権を Firewall Management Center に伝える必要があります。次の点を考慮してください。

- IdP がサードパーティのユーザー管理アプリケーション（Active Directory、LDAP、Radius など）からユーザーまたはグループプロファイルをインポートする場合、これはロールマッピングの属性の使用方法に影響を与える可能性があります。
- SSO フェデレーション全体でユーザーとグループのロール定義を考慮してください。
- Firewall Management Center は、複数の SSO 属性を使用したロールマッピングをサポートできません。ユーザーロールマッピングまたはグループロールマッピングのいずれかを選択し、単一の属性を構成して、IdP からのユーザーロール情報を Firewall Management Center に伝達する必要があります。
- 一般に、グループロールマッピングは、多数のユーザーがいる Firewall Management Center でより効率的です。
- Firewall Management Center アプリケーションにユーザーグループを割り当てる場合は、それらのグループ内のユーザーを個人として割り当てないでください。
- Firewall Management Center ユーザーロール式との一致を判断するために、Firewall Management Center では IdP から受け取ったユーザーおよびグループロール属性値を、Golang と Perl でサポートされている Google の RE2 正規表現標準の制限バージョンに準拠した正規表現として扱います。IdP は、ユーザーまたはグループ属性に特定の構文制限を適用する場合があります。その場合、ロール名とそれらの要件と互換性のある正規表現を使用して、ユーザー ロール マッピング スキームを考案する必要があります。

Before you begin

- IdP アカウントに、このタスクを実行するために必要な権限があることを確認します。
- IdP の Firewall Management Center サービス プロバイダー アプリケーションを設定します（SAML 2.0 準拠の SSO プロバイダー用の FMC サービス プロバイダー アプリケーションの設定, on page 77を参照してください）。

Procedure

ステップ 1 IdP で、Firewall Management Center に送信する属性を作成または指定して、各ユーザーサインインのロールマッピング情報を含めます。これは、ユーザー属性、グループ属性、または IdP またはサードパーティのユーザー管理アプリケーションによって維持されるユーザーまたはグループ定義などのソースから値を取得する別の属性である場合があります。

ステップ 2 属性がその値を取得する方法を構成します。取り得る値を、Firewall Management Center SSO 構成のユーザーロールに関連付けられた値と調整します。

Webインターフェイス用のユーザー 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。ユーザー ロールの詳細については、「ユーザ ロール （3 ページ）」を参照してください。

カスタム ユーザー ロールの作成

カスタムユーザーロールには、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、定義済みのユーザーロールまたは別のカスタムユーザーロールからコピーすることや、別のFirewall Management Centerからインポートすることができます。

（注） 製品をアップグレードすることなくコンテンツの更新へのアクセスを有効にすることはできますが、その逆（コンテンツのない製品）はお勧めできません。つまり、カスタムユーザーロールで [製品のアップグレード（Product Upgrades）] を有効にする場合は、[コンテンツの更新（Content Updates）] も有効にしてください。そうしないと、アップグレードパッケージを手動でアップロードする際に問題が発生する可能性があります。

手順

ステップ 1 [システム（System）]（⚙）>**[ユーザー（Users）]**を選択します。

ステップ 2 [ユーザー ロール（User Roles）] 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ー 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[コピー（Copy）]（🗐）をクリックします。
- 別のFirewall Management Centerからカスタムユーザーロールをインポートします。
  1. 別のFirewall Management Centerで、[エクスポート（Export）]（⬆）をクリックしてロールをコンピュータに保存します。
  2. 新しいFirewall Management Center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ーロールを新しいFirewall Management Center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。説明は 128 文字に制限されています。

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ー 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。

カスタムユーザー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（読み取り専用）（External Database Access (Read Only)）] 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。Firewall Management Center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）新しいユーザー 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 （88 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。
カスタムロールが保存されます。読み取り専用ロールであるとシステムが判断した場合は、そのロールに「(Read Only)」というラベルが付けられます。これは、読み取り専用ユーザーと読み取り/書き込みユーザーの同時セッション数を設定する場合に関連します。「(Read Only)」をロール名に手動で追加してロールを読み取り専用にすることはできません。同時セッション制限の詳細については、ユーザーの設定を参照してください。

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、侵入設定を除くアクセス コントロール ポリシーのすべての側面を設定できる必要があるネットワーク管理者と、侵入関連機能のみを設定できる必要がある侵入管理者を区別する方法を示します。[脅威設定の変更（Modify Threat Configuration）] 権限では、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、アクセス コントロール ポリシーのセキュリティ インテリジェンス ポリシーの設定、およびポリシーのデフォルトアクションの侵入アクションを選択できます。[残りのアクセス コントロール ポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] 権限は、ポリシーとルールの他のすべての側面（作成と削除を含む）をカバーします。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サンプル

メニューベースのアクセス許可	ロールの例		
	アクセス制御エディタ	侵入およびネットワーク分析エディタ	ポリシー承認者
アクセス制御	○	○	○
アクセス コントロール ポリシー	○	○	○
アクセス コントロール ポリシーの変更	×	○	×

メニューベースのアクセス許可	ロールの例		
	アクセス制御エディタ	侵入およびネットワーク分析エディタ	ポリシー承認者
脅威設定の変更（Modify Threat Configuration）	×	○	×
残りのアクセス コントロール ポリシー設定の変更（Modify Remaining Access Control Policy Configuration）	○	×	×
侵入ポリシー	×	○	○
侵入ポリシーの変更	×	○	×
設定をデバイスに展開	×	×	○

ユーザ ロールの非アクティブ化

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ーから、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 [システム（System）]（⚙）>**[ユーザー（Users）]**を選択します。

ステップ 2 [ユーザー ロール（User Roles）] 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ー 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ー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、またはユーザーのログイン セッション中にバックアップからユーザーまたはユーザー ロールを復元する場合、その

ユーザーは 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

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、あるユーザーが不在であるときにそのユーザーを別のユーザーに容易に置き換えることや、拡張ユーザー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。ユーザー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ー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ーのための 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 （88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 ユーザー ロールの設定 （89 ページ）。

ステップ 3 （ログイン後のユーザーの場合）ユーザー ロールのエスカレーション （90 ページ）

エスカレーション ターゲット ロールの設定

各自のユーザー 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 [システム（System）]（⚙）>**[ユーザー（Users）]**を選択します。

ステップ 2 [ユーザー 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ーには、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 ユーザー ロールの設定

エスカレーションを有効にするユーザーは、エスカレーションを有効にしたカスタムユーザーロールに属している必要があります。この手順では、カスタムユーザー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 （88 ページ）」に従って対象ユーザー ロールを設定します。

手順

ステップ 1 「カスタム ユーザー ロールの作成 （84 ページ）」の説明に従って、カスタム ユーザー 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）] で、[このロールをエスカレーションする：メンテナンスユーザー（Set this role to escalate to: Maintenance User）] 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つのオプションから選択できます。

- 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）
別のユーザーのパスワードで認証するときには、任意のユーザー名（非アクティブなユーザーまたは存在しないユーザーを含む）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。

ユーザー ロールのエスカレーション

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ー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 ユーザー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。

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。

- 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。

ユーザー設定の指定

ユーザーロールに応じて、ユーザーアカウントの特定の設定を指定できます。

マルチドメイン展開では、ユーザー設定は、アカウントでアクセスできるすべてのドメインに適用されます。ホームページ設定とダッシュボード設定を指定した場合、特定のページとダッシュボード ウィジェットがドメインから制約を受けることに留意してください。

パスワードの変更

すべてのユーザーアカウントはパスワードで保護されています。パスワードはいつでも変更することができ、ユーザアカウントの設定によっては定期的にパスワードを変更しなければならない場合もあります。

パスワード強度チェックが有効になっている場合、パスワードは、Firewall Management Centerのユーザーアカウントの注意事項と制約事項 （10 ページ）で説明されている強力なパスワードの要件に従う必要があります。

LDAP またはRADIUS ユーザーの場合、Web インターフェイスを介してパスワードを変更することはできません。

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、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [パスワードの変更] をクリックします。

ステップ 3 必要に応じて、[パスワードの表示（Show password）] チェックボックスをオンにして、このダイアログの使用中にパスワードを確認します。

ステップ 4 [現在のパスワード（Current Password）] フィールドに入力します。

ステップ 5 次の 2 つの対処法があります。

- [新しいパスワード（New Password）] と [パスワードの確認（Confirm Password）] に新しいパスワードを入力します。
- [パスワードの生成（Generate Password）] をクリックして、リストされた条件に準拠したパスワードをシステムで作成します（生成されるパスワードはニーモニックではありません。このオプションを選択した場合は、念のためにパスワードをメモしてください）。

ステップ 6 [適用（Apply）] をクリックします。

失効パスワードの変更

ユーザー アカウントの設定によっては、パスワードが期限切れになることがあります。パスワードの有効期間は、アカウントが作成されたときに設定されます。パスワードが期限切れになった場合、[パスワードの有効期限の警告（Password Expiration Warning）] ページが表示されます。

手順

パスワードの有効期限の警告のページには 2 つの選択肢があります。

- すぐにパスワードを変更するには、[パスワードの変更（Change Password）] をクリックします。残りの警告日数がゼロの場合は、パスワードを変更する**必要があります**。

  ヒント
  パスワード強度チェックが有効になっている場合、パスワードは、Firewall Management Center のユーザーアカウントの注意事項と制約事項 （10 ページ）で説明されている強力なパスワードの要件に従う必要があります。

- 後でパスワードを変更するには、[後で（Skip）] をクリックします。

Web インターフェイス表示の変更

Web インターフェイスの表示方法を変更できます。

手順

ユーザー名の下にあるドロップダウンリストから、テーマを選択します。

- **低**
- **ダーク**
- **レガシー**

ホームページの指定

Webインターフェイス内のページをアプライアンスのホームページに指定できます。ダッシュボードへのアクセス権がないユーザーアカウント（外部データベースユーザーなど）を除いて、デフォルトのホームページは、デフォルトダッシュボード（**[概要（Overview）] > [ダッシュボード（Dashboards）]**）です（デフォルト ダッシュボードの設定については、「デフォルト ダッシュボードの指定 （101 ページ）」を参照してください）。

マルチドメイン環境では、選択したデフォルトのホームページは、ユーザーアカウントがアクセスできるすべてのドメインに適用されます。複数のドメインに頻繁にアクセスするアカウントのホームページを選択する際、特定のページはグローバルドメインに制限される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、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [ホームページ（Home Page）] をクリックします。

ステップ 3 ホーム ページとして使用するページをドロップダウン リストから選択します。

ドロップダウン リスト内のオプションは、ユーザ アカウントのアクセス権限に基づいて表示されます。詳細については、「ユーザ ロール （3 ページ）」を参照してください。

ステップ 4 [保存（Save）] をクリックします。

イベント ビュー設定の設定

[イベント ビュー設定（Event View Settings）] ページを使用して、Firewall Management Center のイベント ビューの特性を設定します。イベント ビュー設定は、特定のユーザー ロールでのみ使用可能であることに注意してください。External Database User ロールを持つユーザーは、イベント ビュー設定のユーザー インターフェイスの一部を表示できますが、それらの設定を変更しても意味のある結果は生じません。

手順

ステップ 1 ユーザー名の下にあるドロップダウン リストから、[ユーザー設定（User Preferences）] を選択します。

ステップ 2 [イベント ビュー設定（Event View Settings）] をクリックします。

ステップ 3 [イベント設定（Event Preferences）] セクションで、イベントビューの基本特性を設定します。イベント ビュー設定 （95 ページ）を参照してください。

ステップ 4 [ファイル設定（File Preferences）] セクションで、ファイルダウンロードを設定します。ファイル ダウンロード設定 （97 ページ）を参照してください。

ステップ 5 [デフォルト時間帯（Default Time Windows）] セクションで、デフォルトの時間帯を設定します。デフォルト時間枠 （98 ページ）を参照してください。

ステップ 6 [デフォルトワークフロー（Default Workflow）] セクションで、デフォルトワークフローを設定します。デフォルト ワークフロー （100 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

イベント ビュー設定

[イベント ビュー設定（Event View Settings）] ページの [イベント設定（Event Preferences）] セクションを使用して、Firepower システムのイベント ビューの基本特性を設定します。このセクションはすべてのユーザ ロールで使用可能ですが、イベントを表示できないユーザには、ほとんどまたはまったく意味がありません。

以下のフィールドが [イベント設定（Event Preferences）] セクションに表示されます。

- [「すべて」の操作を確認（Confirm “All” Actions）] フィールドは、イベント ビューのすべてのイベントに影響を与える操作について、アプライアンスがユーザーに確認を要求するかどうかを制御します。

  たとえば、この設定が有効な状態でイベント ビューの [すべて削除（Delete All）] をクリックした場合、アプライアンスがデータベースからこれらを削除する前に、現在の制約を満たすすべてのイベント（現在のページに表示されていないイベントを含む）を削除することをユーザーが確認する必要があります。

- [IP アドレスの解決（Resolve IP Addresses）] フィールドを使用すると、可能な場合には常に、アプライアンスで IP アドレスの代わりにホスト名がイベント ビューに表示されるようになります。

  多数の IP アドレスが含まれている場合、このオプションを有効にすると、イベント ビューの表示に時間がかかる可能性があることに注意してください。また、この設定を有効にするには、管理インターフェイス設定を使用して、システム設定で DNS サーバを確立する必要があることにも注意してください。

- [パケット ビューの展開（Expand Packet View）] フィールドでは、侵入イベントのパケット ビューをどのように表示するかを設定できます。デフォルトでは、アプライアンスによるパケット ビューの表示は折りたたまれた状態になっています。
  - [なし（None）] : パケット ビューの [パケット情報（Packet Information）] セクションのサブセクションをすべて折りたたんだ状態にします。
  - [パケット テキスト（Packet Text）] : [パケット テキスト（Packet Text）] サブセクションだけを展開します。
  - [パケット バイト（Packet Bytes）] : [パケット バイト（Packet Bytes）] サブセクションだけを展開します。
  - [すべて（All）] : すべてのセクションを展開します。

デフォルト設定に関係なく、パケット ビューのセクションを手動で展開することで、キャプチャされたパケットに関する詳細情報を常に表示することができます。

- [1 ページあたりの行数（Rows Per Page）] フィールドは、ドリル ダウン ページとテーブル ビューに表示する、ページごとのイベントの行数を制御します。
- [更新間隔（Refresh Interval）] フィールドは、イベント ビューの更新間隔を分単位で設定します。「0」を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [統計情報の更新間隔（Statistics Refresh Interval）] は、[侵入イベント統計（Intrusion Event Statistics）] や [ディスカバリ統計（Discovery Statistics）] ページなどのイベントのサマリー ページの更新間隔を制御します。「0」を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。

- [ルールの非アクティブ化（Deactivate Rules）] フィールドは、標準テキスト ルールによって生成される侵入イベントのパケット ビューに、どのリンクを表示させるかを次のように制御します。
  - [すべてのポリシー（All Policies）] : すべてのローカルで定義されたカスタム侵入ポリシーで標準テキスト ルールを非アクティブにする単一リンク
  - [現在のポリシー（Current Policy）] : 現在展開中の侵入ポリシーだけで標準テキスト ルールを非アクティブにする単一リンク。デフォルトのポリシーのルールは非アクティブにできないことに注意してください。
  - [質問（Ask）] : これらの個々のオプションへのリンク

パケット ビューでこれらのリンクを表示するには、Administrator または Intrusion Admin のアクセス権があるユーザー アカウントが必要です。

ファイル ダウンロード設定

[イベント ビュー設定（Event View Settings）] ページの [ファイル設定（File Preferences）] セクションを使用して、ローカル ファイル ダウンロードの基本特性を設定します。このセクションは、Administrator、Security Analyst、または Security Analyst（読み取り専用）ユーザー ロールを持つユーザーのみが利用できます。

キャプチャされたファイルのダウンロードをアプライアンスがサポートしていない場合、これらのオプションは無効になることに注意してください。

以下のフィールドが [ファイル設定（File Preferences）] セクションに示されます。

- [「ファイルのダウンロード」アクションを確認する（Confirm 'Download File' Actions）] チェックボックスは、ファイルをダウンロードするたびに [ファイル ダウンロード（File Download）] ポップアップ ウィンドウが表示され、警告が示されて続行するかキャンセルするかを選択するためのプロンプトが出されるようにするかどうかを制御します。

⚠

注意 シスコでは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

ファイルをダウンロードする際には、いつでもこのオプションを無効にできることに注意してください。

- キャプチャされたファイルをダウンロードすると、そのファイルを含むパスワード保護された .zip アーカイブがシステムによって作成されます。[zip ファイル パスワード（Zip File Password）] フィールドは、.zip ファイルへのアクセスを制限するためにユーザーが使用するパスワードを定義します。このフィールドを空欄にすると、パスワードなしのアーカイブ ファイルがシステムによって作成されます。

- [Zip ファイル パスワードの表示（Show Zip File Password）] チェック ボックスで、[Zip ファイルのパスワード（Zip File Password）] フィールドにプレーン テキストを表示するか不明瞭な文字を表示するかを切り替えます。このフィールドをオフにすると、[zip ファイル パスワード（Zip File Password）] には不明瞭な文字が表示されます。

デフォルト時間枠

時間枠（時間範囲と呼ばれることもある）は、任意のイベント ビューでイベントに時間制約を課します。[Event View Settings] ページの [Default Time Windows] セクションを使用して、時間枠のデフォルトの動作を制御します。

このセクションへのユーザー ロール アクセスは以下のとおりです。

- Administrators と Maintenance Users は、セクション全体にアクセスできます。
- Security Analysts と Security Analysts（読み取り専用）は、[Audit Log Time Window] 以外のすべてのオプションにアクセスできます。
- Access Admins、Discovery Admins、External Database Users、Intrusion Admins、Network Admins、および Security Approvers は、[Events Time Window] オプションにのみアクセスできます。

デフォルトの時間枠設定に関係なく、イベントの分析中にいつでも手動で個別のイベント ビューの時間枠を変更できることに注意してください。また、時間枠の設定は、現在のセッションにだけ有効であることにも注意してください。ログアウトしてから再びログインすると、時間枠は、このページで設定したデフォルトにリセットされます。

以下のように、デフォルトの時間枠を設定できる 3 つのタイプのイベントがあります。

- [Events Time Window] は、時間で制約できるほとんどイベントのために単一のデフォルトの時間枠を設定します。
- [Audit Log Time Window] は、監査ログのためにデフォルトの時間枠を設定します。
- [ヘルス モニタリングの時間枠（Health Monitoring Time Window）] は、ヘルス イベント用のデフォルトの時間枠を設定します。

時間枠は、ユーザー アカウントがアクセスできるイベント タイプにのみ設定できます。すべてのユーザー タイプは、イベントの時間枠を設定できます。Administrators、Maintenance Users、および Security Analysts は、ヘルス モニタリングの時間枠を設定できます。Administrators と Maintenance Users は、監査ログの時間枠を設定できます。

すべてのイベント ビューが時間で制約できるとは限らないので、時間枠の設定によって、ホスト、ホスト属性、アプリケーション、クライアント、脆弱性、ユーザーの ID、コンプライアンス allow リスト違反を表示するイベント ビューは影響を受けないことに注意してください。

複数の時間枠を使用して、上記の各タイプのイベントに 1 つずつ適用するか、または**単一の**時間枠を使用して、それをすべてのイベントに適用することができます。単一の時間枠を使用すると、3 つのタイプの時間枠用の設定が非表示になり、新しく [Global Time Window] 設定が表示されます。

以下の 3 つのタイプの時間枠があります。

- 静的は、特定の開始時刻から特定の終了時刻までに生成されたすべてのイベントを表示します
- 拡張は、特定の開始時刻から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠が拡張され、新しいイベントがイベント ビューに追加されます。
- スライディングは、特定の開始時刻（たとえば1日前）から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠は「スライド」し、設定した範囲内（この例では直前の 1 日）のイベントだけが表示されます。

すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。

次のオプションは、[Time Window Settings] ドロップダウン リストに表示されます。

- [Show the Last - Sliding] オプションにより、指定した長さのスライドするデフォルトの時間枠を設定できます。

  アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベントビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。

- [Show the Last - Static/Expanding] により、指定した長さのデフォルトの時間枠を静的または拡張のどちらかに設定できます。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、特定の開始時間（1 時間前など）から現在までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、特定の開始時刻（たとえば1時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。

- [Current Day - Static/Expanding] オプションにより、現在の日付のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の日付は、現行セッションのタイムゾーン設定に基づいて午前 0 時に始まります。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、午前0時からユーザーがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、午前0時から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。

- [Current Week - Static/Expanding] オプションにより、現在の週のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の週は、現行セッションのタイムゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。

  静的時間枠にするには、[Use End Time] チェック ボックスをオンにします。アプライアンスは、午前0時からユーザーがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベントビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[Use End Time] チェック ボックスをオフにします。アプライアンスは、日曜日の午前0時から現在までに生成されたすべてのイベントを表示します。イベントビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に1週間を超えて分析を続けた場合、この時間枠は1週間よりも長くなる可能性があることに注意してください。

デフォルト ワークフロー

ワークフローは、アナリストがイベントの評価に使用するデータが示された一連のページです。アプライアンスには、各イベントタイプに少なくとも1つの定義済みのワークフローが付属しています。たとえば、セキュリティアナリストの場合、実行する分析のタイプに応じて、それぞれが侵入イベントのデータを別の形式で示している、10の異なる侵入イベントのワークフローから選択できます。

アプライアンスには、イベント タイプごとにデフォルト ワークフローが設定されます。たとえば、[優先順位および分類に基づいたイベント（Events by Priority and Classification）] ワークフローが、侵入イベントのデフォルトになります。つまり、侵入イベント（確認済みの侵入イベントを含む）を表示するたびに、アプライアンスは [優先順位および分類に基づいたイベント（Events by Priority and Classification）] ワークフローを表示します。

ただし、イベント タイプごとにデフォルト ワークフローは変更できます。設定可能なデフォルトのワークフローは、ユーザ ロールによって異なります。たとえば、侵入イベントのアナリストがデフォルトのディスカバリ イベント ワークフローを設定することはできません。

デフォルト タイム ゾーンの設定

この設定は、タスクスケジュールやダッシュボードの表示などについて、自分のユーザーアカウントの Web インターフェイスにのみ表示される時間を決定します。この設定は、システム時刻を変更したり、他のユーザーに影響を与えたりせず、システムに保存されているデータ（通常は UTC を使用）にも影響を与えません。

警告 タイムゾーン機能（[ユーザー設定（User Preferences）]）は、システムクロックが UTC 時間に設定されていることを前提としています。システム時刻を変更しようとしないでください。システム時刻の UTC からの変更はサポートされていません。また、システム時刻を変更した場合はデバイスを再イメージ化してサポートされていない状態から回復させる必要があります。

（注） この機能は、時間ベースのポリシーの適用に使用されるタイムゾーンには影響しません。[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] でデバイスのタイムゾーンを設定します。

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、[ユーザ プリファレンス（User Preferences）] を選択します。

ステップ 2 [タイムゾーン（Time Zone）] ドロップダウンをクリックします。

ステップ 3 使用するタイムゾーンに対応する大陸または国と州の名前を選択します。

デフォルト ダッシュボードの指定

[概要（Overview）] > [ダッシュボード（Dashboards）] を選択すると、デフォルトのダッシュボードが表示されます。変更しない限り、すべてのユーザーのデフォルトダッシュボードは、[サマリー（Summary）] ダッシュボードです。ユーザーロールが管理者、メンテナンス、またはセキュリティアナリストの場合は、デフォルトダッシュボードを変更できます。

マルチドメイン環境では、選択したデフォルトのダッシュボードは、ユーザーアカウントがアクセスできるすべてのドメインに適用されます。複数のドメインに頻繁にアクセスするアカウントのダッシュボードを選択する際、ドメインが特定のダッシュボードウィジェットを制限する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、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 [ダッシュボード設定（Dashboard Settings）] をクリックします。

ステップ 3 デフォルトとして使用するダッシュボードをドロップダウン リストから選択します。

ステップ 4 [保存（Save）] をクリックします。

[How To] の設定の指定

How To は、Firewall Management Center 上でタスク間を移動するためのウォークスルーを提供するウィジェットです。ウォークスルーでは、タスクを実行するために移動する必要があるかもしれない各種 UI 画面かどうかを問わず、各ステップを順次体験することでタスクを完遂す

るために必要なステップを実行します。[How To] ウィジェットはデフォルトで有効になっています。

Firewall Management Center でサポートされている機能ウォークスルーのリストについては、「Feature Walkthroughs Supported in Secure Firewall Management Center」を参照してください。

（注）
- 通常、ウォークスルーはすべての UI ページで利用でき、ユーザ ロールは区別されていません。ただし、ユーザーの権限によってはFirewall Management Centerインターフェイスに表示されないメニュー項目もあります。そのため、そのようなページではウォークスルーは実行されません。

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、[ユーザ設定（User Preferences）] を選択します。

ステップ 2 **[How-To の設定（How-To Settings）]** タブをクリックします。

ステップ 3 [How Toの有効化（Enable How-To）] チェックボックスをオンにして [How To] を有効にします。

ステップ 4 **[Save（保存）]** をクリックします。

次のタスク

[How To] ウィジェットを開くには、**[ヘルプ（Help）]** > **[How-Tos]**を選択します。関心のあるタスクに対処する How-To ウォーク スルーを検索できます。詳細については、How To ウォークスルーの検索を参照してください。

Firewall Management Center ユーザーアカウントの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firewall Management Centerの新しいテーマ。	7.6.0	任意（Any）	Firewall Management Center に新しい左側のナビゲーションテーマを導入しました。お試しいただくには、右上隅にあるユーザー名をクリックし、[新しいテーマ（New theme）] を選択します。また、クラシックテーマも廃止されました。クラシックテーマを使用していた場合、アップグレードによりライトテーマに切り替わります。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
シスコのニュースレターおよびその他の製品関連の情報を購読します。	7.6.0	任意（Any）	シスコからの販売および製品更新に関する情報、新しいリリース導入のニュースレター、およびその他の製品関連の情報を受信するための電子メールアドレスを提供します。各 Firewall Management Center 内部ユーザーは、独自の電子メールアドレスを持つことができます。 新規/変更された画面：**[システム（System）]**>**[ユーザー（Users）]**>**[編集（Edit）]** > **[電子メール アドレス（Email Address）]**。
アクセス コントロール ポリシーとルールを変更するための詳細なアクセス許可。	7.4.0	任意（Any）	カスタムユーザーロールを定義して、アクセス コントロール ポリシーおよびルールの侵入設定と、その他のアクセス コントロール ポリシーおよびルールを区別できます。これらのアクセス許可を使用すると、ネットワーク管理チームと侵入管理チームの責任を分離できます。 ユーザーロールを定義するときに、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]**>**[アクセスコントロールポリシー（Access Control Policy）]** > **[アクセスコントロールポリシーの変更（Modify Access Control Policy）]** > **[脅威設定の変更（Modify Threat Configuration）]**オプションを選択して、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、アクセス コントロール ポリシーのセキュリティ インテリジェンス ポリシーの構成、およびポリシーのデフォルトアクションの侵入アクションを選択できるようにします。[残りのアクセスコントロールポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] を使用して、ポリシーの他のすべての側面を編集する機能を制御できます。アクセス コントロール ポリシーの変更権限を含む既存の事前定義されたユーザーロールは、引き続きすべてのサブ権限をサポートします。詳細な権限を適用する場合は、独自のカスタムロールを作成する必要があります。
シェルユーザー名テンプレートを割り当てるための新しいフィールドの追加。	7.0.0	いずれか	LDAP 外部認証用の CLI アクセス属性のテンプレートを指定するプロビジョニング：シェルユーザー名テンプレートが導入されました。したがって、CLI 属性には、LDAP CLI ユーザーを識別するための独自のテンプレートがあります。 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）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
SAML 2.0 準拠の SSO プロバイダーを使用したシングルサインオンのサポートが追加されました。	6.7.0	いずれか	サードパーティの SAML 2.0 準拠アイデンティティ プロバイダー（IdP）で設定された外部ユーザーのシングルサインオンのサポートが追加されました。これには、IdP のユーザーまたはグループロールを Firewall Management Center ユーザーロールにマッピングする機能が含まれます。 内部で認証された、または LDAP または RADIUS によって認証された管理ロールを持つユーザーのみが SSO を構成できます。 新規/変更された画面： **[システム（System）] > [ユーザー（Users）] > [シングル サインオン（Single Sign-On）]**
Webインターフェイスのテーマ。	6.6.0	任意（Any）	Web インターフェイスのルックアンドフィールを選択できます。ライトまたはDuskテーマを選択するか、以前のリリースに登場したクラシックテーマを使用します。 新規/変更された画面： **[ユーザー名（User Name）] > [ユーザー設定（User Preferences）] > [一般（General）] > [UI テーマ（UI Theme）]**
ユーザーアカウントの名前用に新しいフィールドを追加しました。	6.6.0	任意（Any）	内部ユーザーアカウントを担当するユーザーまたは部門を識別できるフィールドを追加しました。 新規/変更された画面： **[システム（System）] > [ユーザー（Users）] > [ユーザー（Users）][> 実際の名前（Real Name）]** フィールド
Cisco Security Manager シングルサインオンのサポートは終了しました。	6.5.0	いずれか	Firewall Management Center と Cisco Security Manager 間のシングルサインオンは、Firepower 6.5 ではサポートされなくなりました。 新規/変更された画面： **[システム（System）] > [ユーザー（Users）][> CSM シングル サインオン（CSM Single Sign-On]。**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
強化されたパスワードセキュリティ。	6.5.0	いずれか	この章内の 1 箇所に強力なパスワードの新しい要件が記載されるようになり、他の章から相互参照されます。 パスワード変更インターフェイスの追加された新しいフィールド：[パスワードの表示（Show Password）] および [パスワードの生成（Generate Password）] 新規/変更された画面： **[ユーザー名（User Name）] > [ユーザー設定（User Preferences）] > [一般（General）] > [パスワードの変更（Change Password）]**。

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。