



Management Center ユーザー

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 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](#) (1 ページ)
- [Management Center のユーザーアカウントの注意事項と制約事項](#) (7 ページ)
- [Management Center のユーザーアカウントの要件と前提条件](#) (8 ページ)
- [内部ユーザーの追加または編集](#) (9 ページ)
- [Management Center の外部認証の設定](#) (12 ページ)
- [SAML シングルサインオンの設定](#) (31 ページ)
- [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](#) (93 ページ)
- [LDAP 認証接続のトラブルシューティング](#) (99 ページ)
- [ユーザー設定の指定](#) (101 ページ)
- [Management Center ユーザーアカウントの履歴](#) (111 ページ)

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、Management Center にユーザーを追加した場合は、そのユーザーは 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ー

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

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。

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**：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 (⚙️) > [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、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 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。

ユーザーの役割

CLI ユーザーロール

Management Center の CLI 外部ユーザにはユーザー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ーロール

ユーザ権限は、割り当てられたユーザー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ーロールを作成できます。

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。



- (注) システムが同時セッション制限の目的で読み取り専用と見なす定義済みユーザーロールには、システム (⚙) > [ユーザー (Users)] > [ユーザー (Users)] と システム (⚙) > [ユーザー (Users)] > [ユーザーロール (User Roles)] でロール名に [(Read Only)] というラベルが付けられます。ユーザーロールのロール名に [(読み取り専用) ((Read Only))] が含まれていない場合、システムはそのロールを読み取り/書き込みと見なします。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。

アクセス管理者

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

管理者

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

セキュリティ上の理由から、管理者ロールの使用を制限する必要があります。

検出管理者 (Discovery Admin)

[ポリシー (Policies)] メニューのネットワーク検出機能、アプリケーション検出機能、関連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は、[ヘルプ (Help)] メニューのオンラインヘルプ関連のオプションのみにアクセスできます。このロールの機能は、webイ

ンターフェイスに搭載されていないため、サポートやパスワードの変更を容易にするためにのみアクセスが可能です。

侵入管理者 (Intrusion Admin)

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

メンテナンス ユーザ (Maintenance User)

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

ネットワーク管理者 (Network Admin)

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

セキュリティ アナリスト

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

セキュリティ アナリスト (読み取り専用) (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マニタのページから、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 (Security Approver)

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

脅威インテリジェンス ディレクタ (TID) ユーザー

[インテリジェンス (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

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、[Management Center の外部認証の設定 \(12 ページ\)](#)と [セキュリティ認定準拠](#)を参照してください。

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 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	<p>パスワードには以下を含める必要があります。</p> <ul style="list-style-type: none"> • 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 @ # * - _ + <p>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。</p>	<p>パスワードには以下を含める必要があります。</p> <ul style="list-style-type: none"> • 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 @ # * - _ + <p>特殊文字のルールは、物理 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。</p> <p>パスワードにユーザー名を含めないでください。</p> <p>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。</p>

	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 (9 ページ) を参照してください）。	<p>パスワードには以下を含める必要があります。</p> <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 大文字の英字 • 小文字の英字 • デジタル • ! などの特殊文字 @ # * - _ + <p>特殊文字のルールは、物理 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。</p> <p>パスワードにユーザー名を含めないでください。</p>

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

- 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、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 (⚙️) > [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、[ステップ 15](#)の項を参照してください。

Management Center 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 \(29 ページ\)](#) 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、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。

Management Center のマルチドメイン展開では、ユーザは作成されたドメインでのみ表示されます。グローバルドメインにユーザーを追加してからリーフドメインのユーザーロールを割り当てると、そのユーザーがリーフドメインに所属していても、追加されたグローバル[ユーザー (Users)] ページにそのユーザーが表示されます。

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

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



- (注) 複数の管理者ユーザーが 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 (⚙️) > [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) [ユーザの作成 (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** 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 6** [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 7** [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 8** [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 9** [パスワードの有効期限までの日数 (Days Until Password Expiration)] を設定します。
- ユーザのパスワードの有効期限までの日数を入力します。デフォルト設定は、パスワードが期限切れにならないことを示す **0**です。デフォルトから変更すると、[ユーザ (Users)] リストの [パスワードのライフタイム (Password Lifetime)] 列に、各ユーザのパスワードの残っている日数が表示されます。
- ステップ 10** [パスワードの有効期限を事前に警告する日数 (Days Before Password Expiration Warning)] を設定します。

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

ステップ 11 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 12 [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 \(93 ページ\)](#) 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。ユーザー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。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 13 (任意、物理 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 14 [保存 (Save)] をクリックします。

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。

Management Center の外部認証について

外部認証を有効にすると、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、Management Center および 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 Threat Defense と Management Center で異なるため、オブジェクトを共有する場合は、Threat Defense の小さなタイムアウト範囲 (LDAP の場合は 1 ~ 30 秒、RADIUS の場合は 1 ~ 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、Threat Defense 外部認証設定が機能しません。

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、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。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 箇所ですべての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、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、およびアカウント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。

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「[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 (⚙️) > [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** [外部認証オブジェクトの追加 (Add External Authentication Object)] [追加 (Add)] アイコン (➕) 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 \(29 ページ\)](#)」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を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 DN)] 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)] をクリックして証明書を選択する必要があります。

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、新しい証明書をアップロードし、設定をデバイスに再展開して、新しい証明書を上書きコピーします。

(注) TLS暗号化には、すべてのプラットフォームで証明書が必要です。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、[ユーザー名テンプレート (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 - 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 Threat Defense と Management Center で異なるため、オブジェクトを共有する場合は、Threat Defense の小さなタイムアウト範囲 (1 - 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、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)] [シェルアクセス属性 (Shell Access Attribute)] を設定します。たとえば、Microsoft Active Directory Server で、`sAMAccountName` 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。

- (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、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、Cisco Secure Firewall デバイスでは検索の再帰回数が 4 回に制限されています。

例：

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

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

- b) 指定したグループのいずれにも属していないユーザの [デフォルトユーザロール (Default User Role)] を選択します。
- c) スタティック グループを使用する場合は、[グループ メンバー属性 (Group Member Attribute)] を入力します。

例：

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

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

例：

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

ユーザ ロールを変更する場合は、変更した外部認証オブジェクトを保存/展開し、[ユーザ (Users)] 画面からユーザを削除する必要があります。次のログイン時に、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一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 Management Center ユーザーは **admin** である必要があります。**[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 \(99 ページ\)](#)」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ーのユーザー名とパスワードをテストすることもできます。**[ユーザー名 (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 **[追加のテストパラメータ (Additional Test Parameters)]** フィールドにユーザー情報を入力せずに **[テスト (Test)]** をクリックします。正常に完了した場合は、テストする特定ユーザーのユーザー名とパスワードを指定します。

例：

Example 社の `JSmith` ユーザー名とパスワード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。 [Management Center でのユーザーの外部認証の有効化 \(28 ページ\)](#) 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。

External Authentication Object

Authentication Method

CAC Use for CAC authentication and authorization

Name *

Description

Server Type [Set Defaults](#)

Primary Server

Host Name/IP Address * ex. IP or hostname

Port *

Backup Server (Optional)

Host Name/IP Address ex. IP or hostname

Port

LDAP-Specific Parameters

Base DN * ex. dc=sourcefire,dc=com [Fetch DNS](#)

Base Filter ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(cn=bsmith)(cn=csmith*))

User Name * ex. cn=jsmith,dc=sourcefire,dc=com

Password *

Confirm Password *

[▶ Show Advanced Options](#)

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。

The screenshot shows a configuration window for LDAP external authentication. It is divided into three main sections:

- Attribute Mapping:** Contains two input fields. The first is labeled "UI Access Attribute *" and contains the text "sAMAccountName". To its right is a "Fetch Attrs" button. The second is labeled "CLI Access Attribute *" and contains the text "sAMAccountName".
- Group Controlled Access Roles (Optional):** A section header.
- CLI Access Filter:** Contains a radio button labeled "CLI Access Filter" which is selected. Next to it is an unchecked checkbox labeled "Same as Base Filter". Below this is a text input field with the placeholder "(Mandatory for FTD devices)". To the right of the input field is an example filter string: "ex. (cn=jsmith), (cn=jsmith), (&(cn=jsmith))((cn=bsmith)(cn=csmith*))".
- Additional Test Parameters:** Contains two input fields: "User Name" and "Password".

At the bottom left, there is a note: "*Required Field". At the bottom right, there are three buttons: "Cancel", "Test", and "Save".

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、[CLI アクセス属性 (CLI Access Attribute)] が sAMAccountName の場合、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。

External Authentication Object

Authentication Method: LDAP

CAC Use for CAC authentication and authorization

Name: Advanced Configuration Example

Description:

Server Type: MS Active Directory Set Defaults

Primary Server

Host Name/IP Address: 10.11.3.4 ex. IP or hostname

Port: 636

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

LDAP-Specific Parameters

Base DN: OU=security,DC=it,DC=example,DC=com Fetch DNs ex. dc=sourcefire,dc=com

Base Filter: (cn=*smith) ex. (cn=jsmith), (cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))

User Name: CN=Admin,DC=example,DC=com ex. cn=jsmith,dc=sourcefire,dc=com

Password:

Confirm Password:

▼ Show Advanced Options

Encryption: SSL TLS None

SSL Certificate Upload Path: Choose File certificate.pem ex. PEM Format (base64 encoded version of DER)

User Name Template: %s ex. cn=%s,dc=sourcefire,dc=com

Shell User Name Template: %s ex. %s

Timeout (Seconds): 60

Attribute Mapping

UI Access Attribute: sAMAccountName Fetch Attrs

CLI Access Attribute: sAMAccountName

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、[CLIアクセス属性 (CLI Access Attribute)] が `sAMAccountName` の場合、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。

▼ Group Controlled Access Roles (Optional)

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role

Access Admin
 Administrator
 Discovery Admin
 External Database User

To specify the default user role if user is not found in any group

Group Member Attribute

Group Member URL Attribute

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。

CLI Access Filter

CLI Access Filter Same as Base Filter

(Mandatory for Firewall Threat Defense devices)

ex. (cn=jsmith), (tcn=jsmith), (&(cn=jsmith)(!(cn=bsmith)(cn=csmith*)))

Additional Test Parameters

User Name

Password

*Required Field

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 (⚙️) > [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 [プライマリサーバ (Primary Server)] の場合は、[ホスト名/IPアドレス (Host Name/IP Address)] を入力します。
- ステップ7 (任意) [ポート (Port)] をデフォルトから変更します。
- ステップ8 [RADIUS秘密キー (RADIUS Secret Key)] を入力します。
- ステップ9 (任意) [バックアップサーバ (Backup Server)] パラメータを入力します。
- ステップ10 (任意) [RADIUS固有のパラメータ (RADIUS-Specific Parameters)] を入力します。
- a) プライマリサーバを再試行するまでの [タイムアウト (Timeout)] を 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 Threat Defense と Management Center で異なるため、オブジェクトを共有する場合は、Threat Defense の短いタイムアウト範囲 (1 ~ 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、Threat Defense RADIUS 設定が機能しません。
- b) バックアップサーバにロールオーバーするまでの [再試行 (Retries)] を入力します。デフォルトは 3 です。
- c) ユーザ ロールに対応するフィールドに、各ユーザの名前を入力するか、またはこれらのロールに割り当てる必要がある属性と値のペアを指定します。
- ユーザ名と属性と値のペアは、カンマで区切ります。

例 :

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

例 :

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

例 :

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

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

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

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

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

- a) [属性名 (Attribute Name)] を入力します。

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

- b) [属性ID (Attribute ID)] を整数で入力します。

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

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

属性のタイプ (文字列、IP アドレス、整数、または日付) も指定します。

- d) [追加 (Add)] をクリックして、カスタム属性を追加します。

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

例：

シスコルータが接続しているネットワーク上で RADIUS サーバが使用される場合に、`Ascend-Assign-IP-Pool` 属性を使用して、特定の IP アドレス プールからログインするすべてのユーザ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 12 (任意) [CLIアクセスフィルタ (CLI Access Filter)] エリアの [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区切りで入力します。

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

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

例 :

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

ステップ 15 [保存 (Save)] をクリックします。

ステップ 16 このサーバーの使用を有効にします。Management Center でのユーザーの外部認証の有効化 (28 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。

External Authentication Object

Authentication Method:

Name *:

Description:

Primary Server

Host Name/IP Address *: ex. IP or hostname

Port *:

RADIUS Secret Key *:

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。

RADIUS-Specific Parameters

Timeout (Seconds)	<input type="text" value="30"/>
Retries	<input type="text" value="3"/>
Access Admin	<input type="text"/>
Administrator	<input type="text" value="swbaron.gand"/>
Discovery Admin	<input type="text"/>
External Database User	<input type="text"/>
Intrusion Admin	<input type="text"/>
Maintenance User	<input type="text" value="abronite"/>
Network Admin	<input type="text"/>
Security Analyst	<input type="text" value="jwstid"/>
Security Analyst (Read Only)	<input type="text"/>
Security Approver	<input type="text"/>
Threat Intelligence Director (TID) User	<input type="text"/>
Default User Role	<div style="border: 1px solid gray; padding: 2px;"> Discovery Admin External Database User Intrusion Admin Maintenance User </div> <small>To specify the default user role if user is not found in any group</small>

CLI Access Filter

(For FMC (all versions) and FTD (5.2.3 and 5.3), define users for CLI access. For FTD 5.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List	<input type="text" value="swbaron"/>
------------------------------------	--------------------------------------

ex. user1, user2, user3 (lowercase letters only).

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。

Security Analyst (Read Only) MS-RAS-Version=MSRASV5.00

Security Approver

Threat Intelligence Director (TID) User

Default User Role

External Database User

Intrusion Admin

Maintenance User

Network Admin

To specify the default user role if user is not found in any group

CLI Access Filter

(For FMC (all versions) and FTD (6.2.3 and 6.3), define users for CLI access. For FTD 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List ewharton

ex. user1, user2, user3 (lowercase letters only).

▼ Define Custom RADIUS Attributes

Attribute Name	Attribute ID	Attribute Type
MS-Ras-Version	5	string

Add Delete

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、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


[Management Center 用の LDAP 外部認証オブジェクトの追加 \(13 ページ\)](#) および [Management Center 用の RADIUS 外部認証オブジェクトの追加 \(22 ページ\)](#) 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 (⚙️) > [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に対してのみ認証できます。

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

ステップ 6 外部ユーザーに 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 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、[ステップ 15](#)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、[ユーザ名 (Username)] フィールドと [パスワード (Password)] フィールドに、管理者権限を持つユーザとしてログインします。CAC クレデンシャルを使用してログインすることは、まだできません。
- ステップ 6** [システム (System)] > [ユーザ (Users)] > [外部認証 (External Authentication)] を選択します。
- ステップ 7** 「[Management Center 用の LDAP 外部認証オブジェクトの追加 \(13 ページ\)](#)」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 [Management Center でのユーザーの外部認証の有効化 \(28 ページ\)](#) 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 (⚙️) > [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 サーバ証明書のインポート](#)で説明する手順に従います。

使用する予定の CAC で、HTTPS サーバ証明書とユーザ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 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、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 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、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 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 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、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。

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。



-
- (注) 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。
-

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



-
- (注) Cisco Secure Sign On SSO 製品は、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。
-

Management Center の SSO ガイドライン

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。

- 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 Management Center を設定することはできません。
- 高可用性設定の 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 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 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 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 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 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 Management Center の SSO を設定する場合：
 - プライマリ Management Center で SSO を設定する場合、セカンダリ Management Center で SSO を設定する必要はありません。
 - セカンダリ Management Center で SSO を設定する場合は、プライマリ 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 Management Center にログインする前に、プライマリ 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）。
- マルチテナントを使用する Management Center では、SSO 設定はグローバルドメインレベルでのみ適用でき、グローバルドメインとすべてのサブドメインに適用されます。
- 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。
- Management Center は、IdP から開始された SSO をサポートしていません。
- 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 Management Center の監査ログに記録されます。

関連トピック

[ハイ アベイラビリティ](#)

[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 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、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。



- (注) 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 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、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 (⚙️) > [ユーザー (Users)] > [ユーザーの編集 (Edit User)] の下の 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、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。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して、ログイン時に SSO ユーザーに割り当てられる Management Center ユーザーロールを確立できます。

ユーザーロールマッピングでは、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、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 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 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 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)。Management Center では、そのロール属性の名前は SSO 構成の一部です。Management Center SSO 構成には、Management Center ユーザーロールのリストに割り当てられた式のリストも含まれています。ユーザーが SSO を使用して Management Center にログインすると、

Management Centerはそのユーザー（または構成によってはそのユーザーのグループ）のロール属性の値を各 Management Center ユーザーロールの式と比較します。Management Centerは、ユーザーが指定した属性値に式が一致するすべてのロールをユーザーに割り当てます。



- (注) 個人ユーザー権限またはグループ権限に基づいて 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 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。

Management Centerでのシングルサインオンの有効化

始める前に

- SAML SSO 管理アプリケーションで、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 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 Management Center サービス プロバイダー アプリケーションの設定 \(38 ページ\)](#) を参照してください。
 - OneLogin の 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 Management Center サービス プロバイダー アプリケーションの設定 \(52 ページ\)](#) を参照してください。
 - Azure の 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 Management Center サービス プロバイダー アプリケーションの設定 \(66 ページ\)](#) 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 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 Management Center サービス プロバイダー アプリケーションの設定 \(81 ページ\)](#) を参照してください。
 - SAML 2.0 準拠の SSO プロバイダーの 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 Management Center サービス プロバイダー アプリケーションの設定 \(87 ページ\)](#) を参照してください。

手順

- ステップ1 システム (⚙️) > [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。

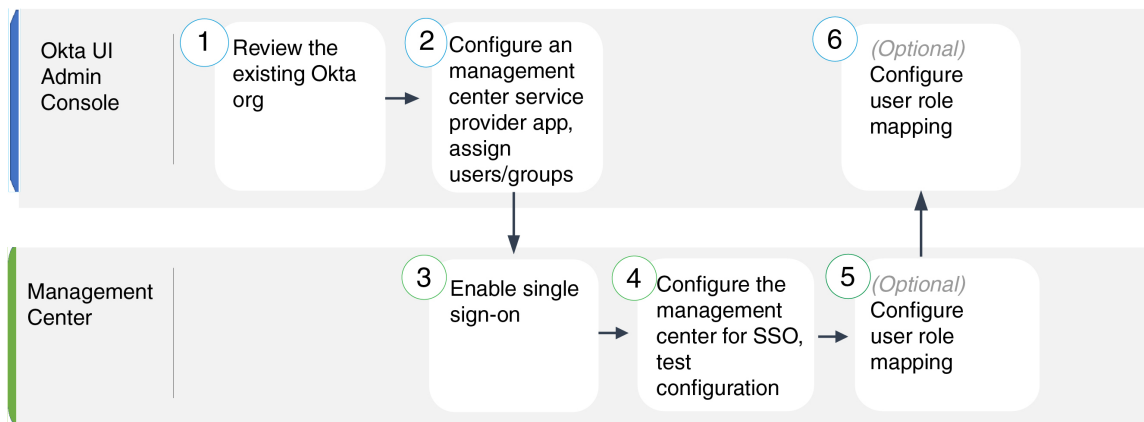
次のタスク

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 Management Center を設定するには、[Okta SSO 用の Management Center の設定 \(40 ページ\)](#) 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 Management Center を設定するには、[PingID PingOne for Customers を使用した SSO 用の Management Center の設定 \(83 ページ\)](#) を参照してください。
- Azure SSO 用に Management Center を設定するには、[Azure SSO 用の Management Center の設定 \(69 ページ\)](#) を参照してください。
- OneLogin SSO 用に Management Center を設定するには、[OneLogin SSO 用の Management Center の設定 \(54 ページ\)](#) 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 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 Management Center の設定 \(89 ページ\)](#) 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 (37 ページ)
②	Okta UI 管理コンソール	Okta の Management Center サービス プロバイダー アプリケーションの設定 (38 ページ)
③	Management Center	Management Centerでのシングルサインオンの有効化 (35 ページ)
④	Management Center	Okta SSO 用の Management Center の設定 (40 ページ)
⑤	Management Center	Management Center での Okta のユーザーロールマッピングの設定 (41 ページ)
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 (42 ページ)

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。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。

- 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。
- 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、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 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 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 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 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。



(注) 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。



(注) 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 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。

始める前に

- 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 \(37 ページ\)](#) 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。



(注) 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 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、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 Management Center のログイン URL を確認します (`https://ipaddress_or_hostname`) 。



- (注) 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 Management Center にアクセスする必要があります。

手順

ステップ 1 Okta クラシック UI 管理コンソールから、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 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 Management Center URL です。

文字列 `saml/acs` を 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 (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 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 Management Center アプリケーションに割り当てます。(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 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) Management Center での SSO セットアップを簡単にするために、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。

次のタスク

シングルサインオンを有効にします。Management Centerでのシングルサインオンの有効化 (35 ページ) を参照してください。

Okta SSO 用の Management Center の設定

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 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 Management Center サービス プロバイダー アプリケーションの設定 (38 ページ) 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。Management Centerでのシングルサインオンの有効化 (35 ページ) を参照してください

手順

ステップ 1 (このステップはManagement Centerでのシングルサインオンの有効化 (35 ページ) 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：
 1. [手動設定 (Manual Configuration)] オプションボタンをクリックします。
 2. 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 Management Center サービス プロバイダー アプリケーションの設定 (38 ページ) のステップ 4) 、ファイルを Management Center にアップロードできます。
 1. [XMLファイルのアップロード (Upload XMLFile)] オプションボタンをクリックします。
 2. 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、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。

次のタスク

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。[Management Center での Okta のユーザーロールマッピングの設定 \(41 ページ\)](#) 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、Management Center にログインするすべての SSO ユーザーに、[Management Center での Okta のユーザーロールマッピングの設定 \(41 ページ\)](#) 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。

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

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。

始める前に

- 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 \(37 ページ\)](#) を参照してください。
- 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。[Okta の Management Center サービスプロバイダーアプリケーションの設定 \(38 ページ\)](#) を参照してください。
- Management Center でシングルサインオンを有効にして設定します。[Management Center でのシングルサインオンの有効化 \(35 ページ\)](#) および[Okta SSO 用の Management Center の設定 \(40 ページ\)](#) を参照してください。

手順

- ステップ 1** システム (⚙️) > [ユーザー (Users)] を選択します。
- ステップ 2** [シングルサインオン (SSO) (Single Sign-On (SSO))] タブをクリックします。
- ステップ 3** [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 4** [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 Management Center ユーザーロールを選択します。
- ステップ 5** [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のユーザーロールマッピングのために Okta Management Center 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。(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 (43 ページ) 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 (44 ページ) のステップ 1 を参照)。

ステップ 6 SSO ユーザーに割り当てる各 Management Center ユーザーロールの横に、正規表現を入力します。(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を使用します。) Management Center は、これらの値を、IdP が SSO ユーザー情報とともに 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。Management Center は、一致が見つかったすべてのロールの和集合をユーザーに付与します。

次のタスク

- 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 (42 ページ) 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 (43 ページ) 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 (44 ページ) を参照してください。

SSO ユーザーが 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 Management Center に提示します。Management Center は、その属性値を SSO 設定で各 Management Center ユーザーロールに割り当てられた正規表現と比較し、一致が見つかったすべてのロールをユーザーに付与します。(一致するものが見つからない場合、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)。各 Management Center ユーザーロールに割り当てる式は、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必要があります。Management Center は、Okta から受け取った属性値を、Management Center ユーザーロール式との比較のために、同じ標準規格を使用する正規表現として扱います。



(注) 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。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、Management Center は、Okta で設定された 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 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、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 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。

始める前に

- [Okta の Management Center サービス プロバイダー アプリケーションの設定 \(38 ページ\)](#) の説明に従って、Okta IdP で 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。
- [Management Center での Okta のユーザーロールマッピングの設定 \(41 ページ\)](#) の説明に従って、Management Center で SSO ユーザーロールマッピングを設定します。

手順

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 Management Center に送信する変数名を指定します。この変数名は、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 ([Management Center での Okta のユーザーロールマッピングの設定 \(41 ページ\)](#) 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 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。

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。Management Center では、この文字列を、[Management Center での Okta のユーザーロールマッピングの設定 \(41 ページ\)](#) の手順 6 で各 Management Center ユーザーロールに割り当てた式と比較します (Management Center ユーザーロール式との比較のために、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 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 グループ属性を 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。Management Center は、Okta 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、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 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。

始める前に

- Okta IdP の 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 Management Center サービス プロバイダー アプリケーションの設定 \(38 ページ\)](#) を参照してください。
- Management Center でのユーザーロールマッピングの設定 [Management Center での Okta のユーザーロールマッピングの設定 \(41 ページ\)](#)

手順

Management Center サービス プロバイダー アプリケーションの新しい SAML グループ属性を作成します。

- [名前 (Name)]には、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一文字列を使用します。(Management Center での Okta のユーザーロールマッピングの設定 (41 ページ) のステップ 5 を参照してください)。
- [フィルタ (Filter)]には、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 Management Center に送信します。次に、Management Center では、これらのグループ名を、Management Center での Okta のユーザーロールマッピングの設定 (41 ページ) の手順 6 で各 Management Center ユーザーロールに割り当てた正規表現と比較します。

Okta ユーザーロールマッピングの例

次の例が示すように、ユーザーロールマッピングをサポートする Management Center での SSO 構成は、個々のユーザーとグループの両方で同じです。違いは、Okta の Management Center サービス プロバイダー アプリケーションの設定にあります。



- (注) 個人ユーザー権限またはグループ権限に基づいて 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 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。さらに、Management Center は、Okta で設定された 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せん。

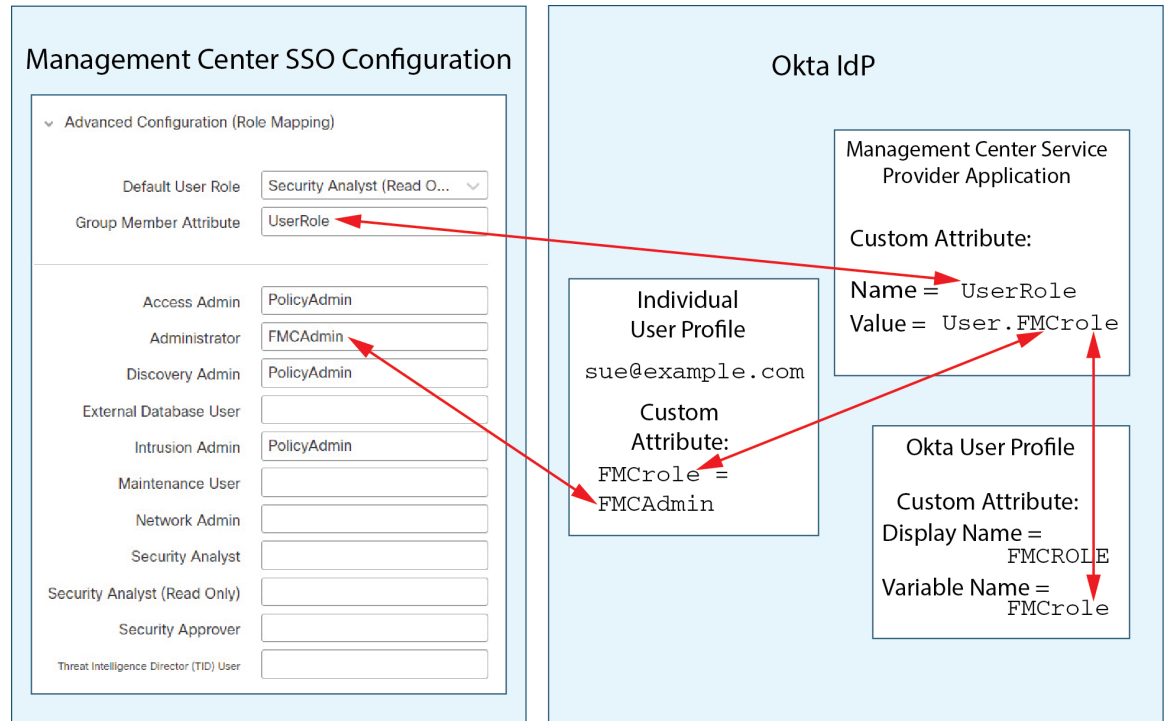
個人ユーザーアカウントの Okta ロールのマッピング例

個人ユーザーのロールマッピングでは、Okta Management Center サービスアプリケーションに、名前が Management Center でのグループメンバー属性の名前と一致するカスタム属性があります。(この例では、UserRole) 。Okta のユーザープロファイルには、カスタム属性もあります(この例では、FMCrole という名前の変数) 。アプリケーションのカスタム属性 UserRole の定義は、Okta がユーザーロールマッピング情報を Management Center に渡すときに、対象のユーザーに割り当てられたカスタム属性値を使用することを確立します。

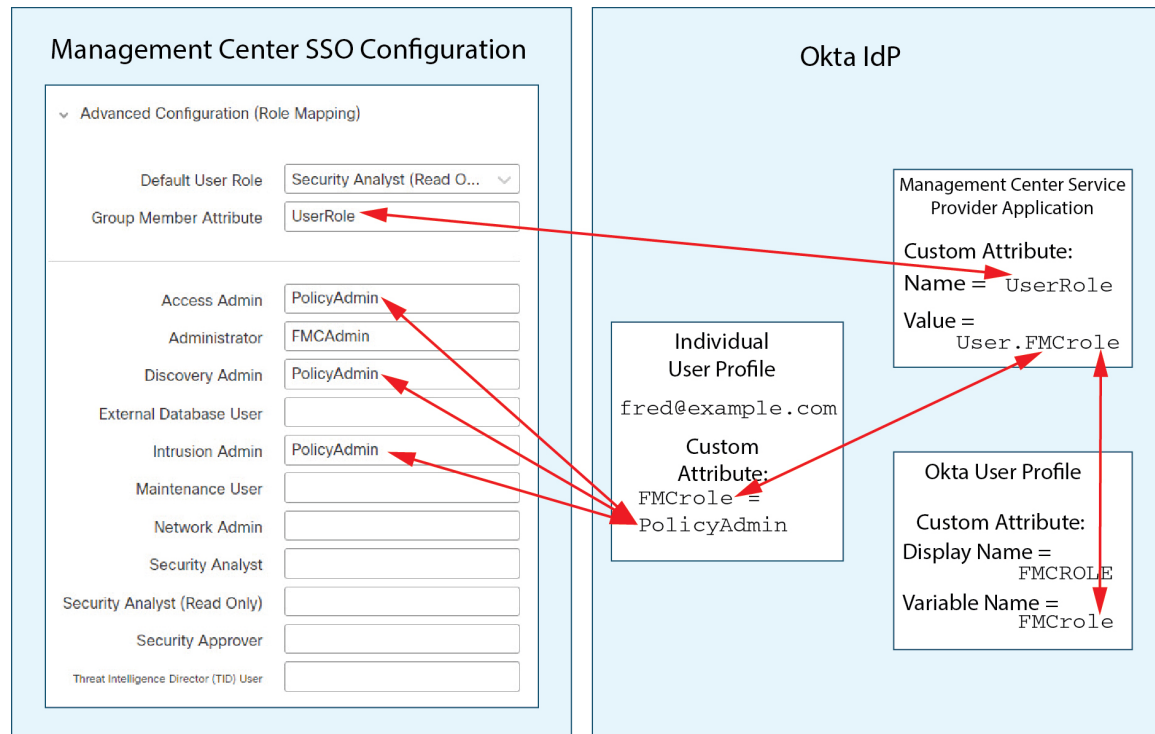
次の図は、Management Center および Okta 構成の関連するフィールドと値が、個人アカウントのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図では、Management Center と Okta UI 管理コンソールで同じ SSO 設定を使用していますが、Management

Center で各ユーザーに異なる役割を割り当てるために、Okta UI 管理コンソールでの各ユーザーの設定は異なります。

- この図では、sue@example.com では `FMCrole` 値 `FMCAdmin` が使用されていて、Management Center が彼女に管理者役割を割り当てます。



- この図では、fred@example.com では `FMCrole` 値 `PolicyAdmin` が使用されていて、Management Center が彼にアクセス管理者、検出管理者、侵入管理者の役割を割り当てます。



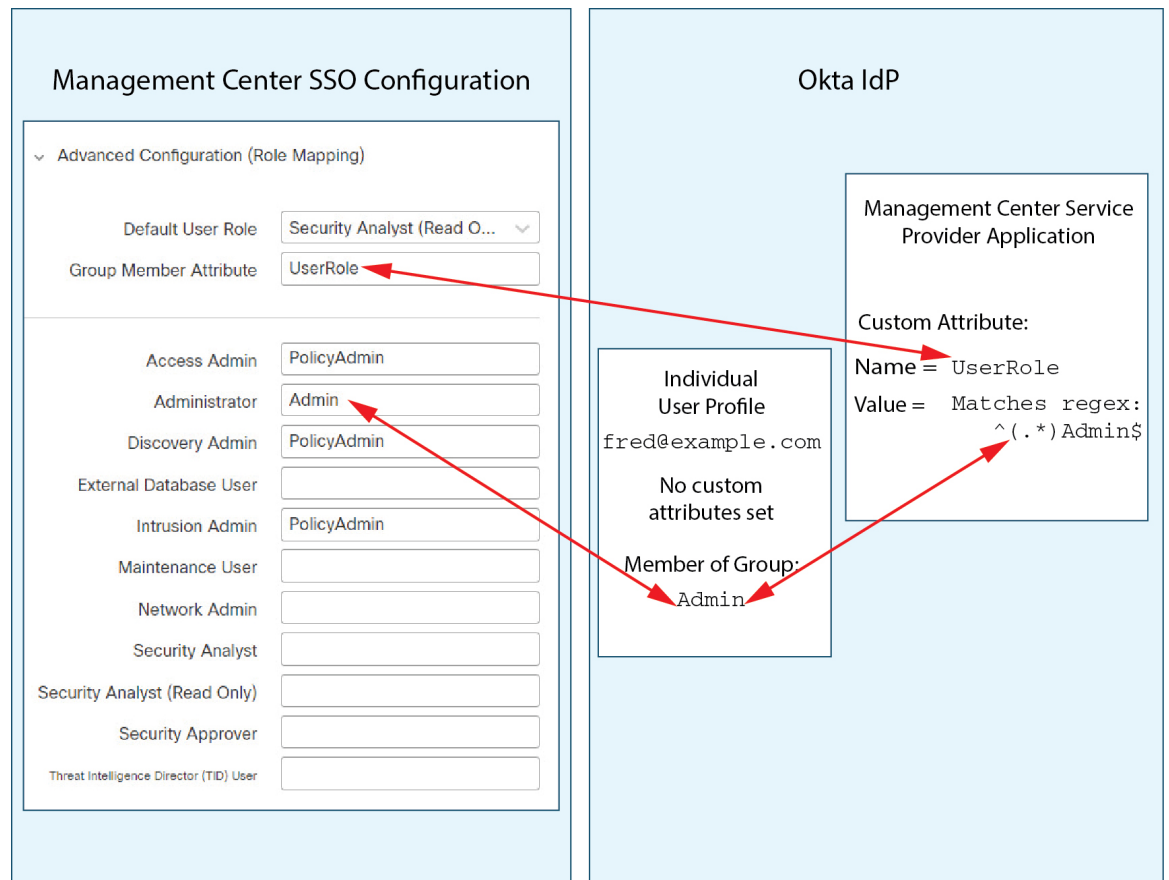
- この Management Center のために Okta サービスアプリケーションに割り当てられた他のユーザーには、次のいずれかの理由で、デフォルトのユーザーロールであるセキュリティアナリスト（読み取り専用）が割り当てられます。
 - Okta ユーザープロファイルの `FMCrole` 変数に値が割り当てられていません。
 - Okta ユーザープロファイルの `FMCrole` 変数に割り当てられた値が、Management Center の SSO 設定でユーザーロールに設定された式と一致しません。

グループの Okta ロールマッピングの例

グループのロールマッピングでは、Okta Management Center サービスアプリケーションに、名前が Management Center でのグループメンバー属性の名前と一致するカスタムグループ属性があります（この例では、`UserRole`）。Okta は Management Center の SSO ログインのリクエストを処理するときに、ユーザーのグループメンバーシップを Management Center サービスアプリケーショングループ属性に割り当てられた式と比較します（この例では、`^(.*)Admin$`）。Okta は、グループ属性に一致するユーザーのグループメンバーシップを Management Center に送信します。Management Center は、受信したグループ名を各ユーザーロールに設定された正規表現と比較し、それに応じてユーザーロールを割り当てます。

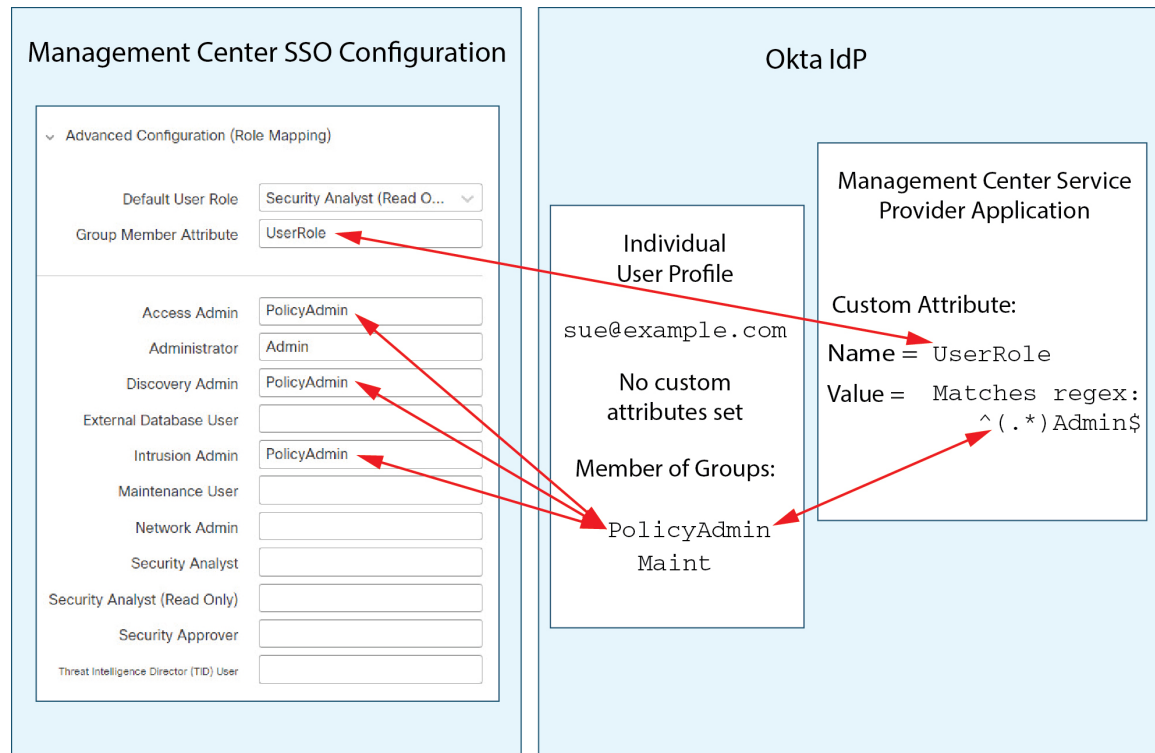
次の図は、Management Center および Okta 構成の関連するフィールドと値が、グループのユーザーロールマッピングで互いに対応しているかを示しています。各図では、Management Center と Okta UI 管理コンソールで同じ SSO 設定を使用していますが、Management Center で各ユーザーに異なるロールを割り当てるために、Okta UI 管理コンソールでの各ユーザーの設定は異なります。

- この図では、fred@example.com は Okta IdP グループの Admin のメンバーであり、式 $^(.*)Admin\$$ に一致します。Okta は Management Center に Fred の Admin グループメンバーシップを送信し、Management Center は彼に管理者ロールを割り当てます。

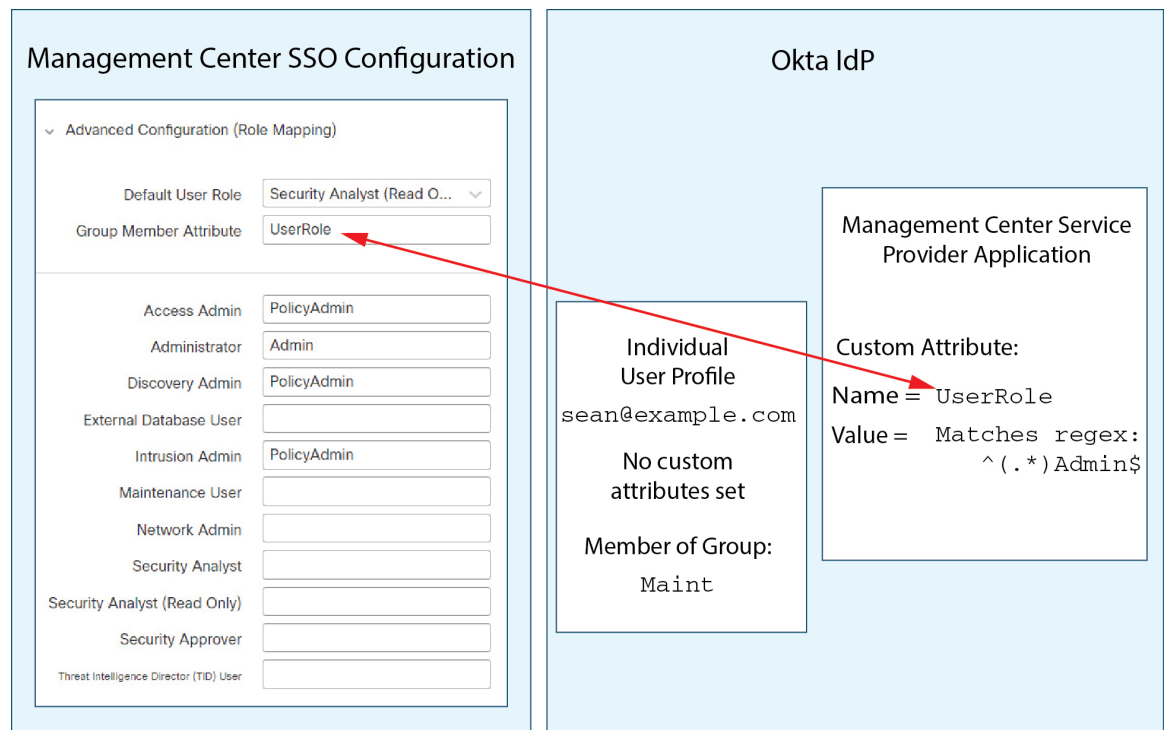


- この図では、sue@example.com は Okta IdP グループの PolicyAdmin のメンバーであり、式 $^(.*)Admin\$$ に一致します。Okta は Management Center に Sue の PolicyAdmin グループメンバーシップを送信し、Management Center は彼女にアクセス管理者、検出管理者、侵入管理者のロールを割り当てます。

Sue は Okta グループの Maint のメンバーでもありますが、このグループ名は Okta Management Center サービスアプリケーションのグループメンバーシップ属性に割り当てられた式と一致しないため、Okta は Sue の Maint グループメンバーシップに関する情報を Management Center に送信しません。そのため、Maint グループでの彼女のメンバーシップは、Management Center が彼女に割り当てるロールには関与しません。



- この図では、sean@example.com は Okta IdP グループの Maint のメンバーです。このグループ名は式 $^(.*)Admin\$$ と一致しないため、sean@example.com が Management Center にログインしたときに、Okta は Sean の Maint グループメンバーシップに関する情報を Management Center に送信しません。そのため、Sean にはメンテナンスユーザーロールではなく、デフォルトのユーザーロール（セキュリティアナリスト（読み取り専用））が割り当てられます。

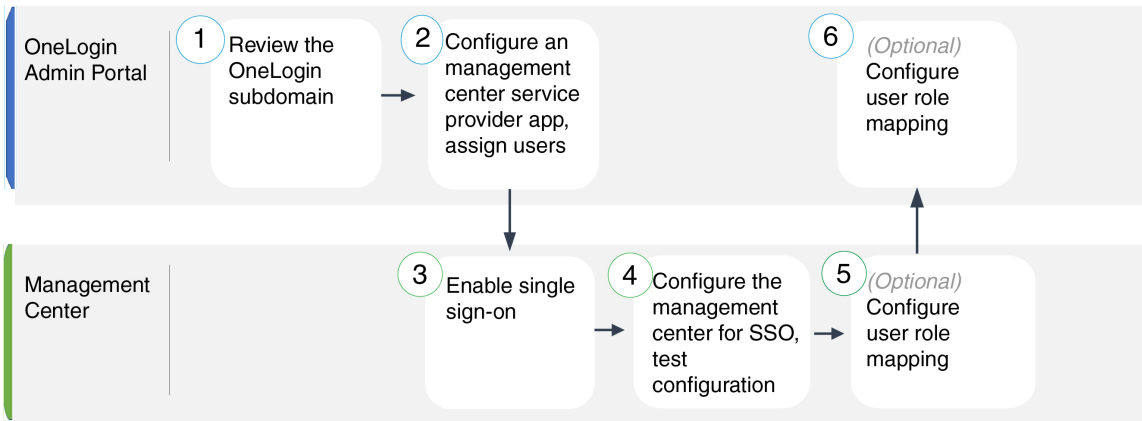


これらの図は、ロールマッピング戦略を確立する際の事前計画の重要性を示しています。この例では、Maint グループのみのメンバーである、この Management Center へのアクセス権を持つ Okta ユーザーには、デフォルトのユーザーロールのみを割り当てることができます。

Management Center は、Okta サービスアプリケーション設定で、1つのカスタムグループ属性のみの使用をサポートしています。その属性に割り当てる式と、その式と照合するために確立するグループ名は、慎重に作成する必要があります。Management Center SSO 設定のユーザーロール割り当て文字列で正規表現を使用することで、ロールマッピングをより柔軟に行うことができます。（各 Management Center ユーザーロールに割り当てる式は、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必要があります）。

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	Management Center	OneLogin サブドメインの確認 (51 ページ)
②	Management Center	OneLogin の Management Center サービス プロバイダー アプリケーションの設定 (52 ページ)
③	OneLogin 管理ポータル	Management Centerでのシングルサインオンの有効化 (35 ページ)
④	OneLogin 管理ポータル	OneLogin SSO 用の Management Center の設定 (54 ページ)
⑤	OneLogin 管理ポータル	Management Center における OneLogin のユーザーロールマッピングの設定 (55 ページ)
⑥	Management Center	OneLogin IdP におけるユーザーロールマッピングの設定 (56 ページ)

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。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。

- 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？
- 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 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、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 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 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 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 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。



-
- (注) 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。
-



-
- (注) 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 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。
-

始める前に

- 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 \(51 ページ\)](#) 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。



(注) 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 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、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 Management Center のログイン URL を確認します
(`https://ipaddress_or_hostname/`)。



(注) 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 Management Center にアクセスする必要があります。

手順

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、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 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 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 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 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 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 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) Management Center での SSO セットアップを簡単にするために、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。

次のタスク

シングルサインオンを有効にします。[Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) を参照してください。

OneLogin SSO 用の Management Center の設定

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

始める前に

- OneLogin 管理ポータルで 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 Management Center サービス プロバイダー アプリケーションの設定 \(52 ページ\)](#) 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。[Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) を参照してください。

手順

ステップ 1 (このステップは[Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) 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：
 1. [手動設定 (Manual Configuration)] オプションボタンをクリックします。
 2. 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 Management Center サービス プロバイダー アプリケーションの設定 \(52 ページ\)](#) のステップ 4) 、ファイルを Management Center にアップロードできます。
 1. [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。
 2. 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、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。

次のタスク

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。[Management Center における OneLogin のユーザーロールマッピングの設定 \(55 ページ\)](#) 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、Management Center にログインするすべての SSO ユーザーに、[Management Center における OneLogin のユーザーロールマッピングの設定 \(55 ページ\)](#) 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。

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

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。

始める前に

- 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 \(51 ページ\)](#) を参照してください。
- 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 Management Center サービスプロバイダーアプリケーションの設定 \(52 ページ\)](#) を参照してください。
- Management Center でシングルサインオンを有効にして設定します。[Management Center でのシングルサインオンの有効化 \(35 ページ\)](#) および[OneLogin の Management Center サービスプロバイダーアプリケーションの設定 \(52 ページ\)](#) を参照してください。

手順

-
- ステップ 1** システム (⚙) > [ユーザー (Users)] > [シングルサインオン (Single Sign-On)] [システム (System)] > [ユーザー (Users)] 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 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、OneLogin の Management Center サービスプロバイダーアプリケーションでロールマッピング用に定義するカスタムパラメータのフィールド名と一致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 \(57 ページ\)\)](#) 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 \(58 ページ\)\)](#) のステップ 1 を参照)。
- ステップ 5** SSO ユーザーに割り当てる各 Management Center ユーザーロールの横に、正規表現を入力します。Management Center は、これらの値を、IdP が SSO ユーザー情報とともに Management Center に送信するユーザーロールマッピング属性と比較します。Management Center は、一致が見つかったすべてのロールの和集合をユーザーに付与します。
-

次のタスク

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 \(56 ページ\)](#) 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 \(57 ページ\)](#) 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 \(58 ページ\)](#) を参照してください。

SSO ユーザーが 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 Management Center に提示します。Management Center はその属性値を SSO 設定で各 Management Center ユーザーロールに割り当てられた正規表現と比較し、一致が見つかったすべてのロールをユーザーに付与します。（一致するものが見つからない場合、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）。各 Management Center ユーザーロールに割り当てられる式は、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必要があります。Management Center は、OneLogin から受け取った属性値を、Management Center ユーザーロール式との比較のために、同じ標準規格を使用する正規表現として扱います。



- (注) 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。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。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 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、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 Management Center に渡す手段を提供します。

始める前に

- 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 \(51 ページ\)](#) を参照してください。
- OneLogin で 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 Management Center サービス プロバイダー アプリケーションの設定 \(52 ページ\)](#) を参照してください。
- [Management Center における OneLogin のユーザーロールマッピングの設定 \(55 ページ\)](#) 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。

手順

- ステップ 1** 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、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一名前を使用します ([Management Center における OneLogin のユーザーロールマッピングの設定 \(55 ページ\)](#) 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、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 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 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、Management Center が SSO 構成で 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 ([Management Center における OneLogin のユーザーロールマッピングの設定 \(55 ページ\)](#) のステップ 5 を参照してください)。

次のタスク

- さまざまなアカウントから SSO を使用して Management Center にログインし、期待どおりにユーザーに 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、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 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。

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。

始める前に

- 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 \(51 ページ\)](#) を参照してください。
- OneLogin で 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 Management Center サービス プロバイダー アプリケーションの設定 \(52 ページ\)](#) を参照してください。
- [Management Center における OneLogin のユーザーロールマッピングの設定 \(55 ページ\)](#) 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。

手順

ステップ 1 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、Management Center SSO 設定で [グループメンバーの属性 (Group Member Attribute)]に使用したのと同じ名前を使用します ([Management Center における OneLogin のユーザーロールマッピングの設定 \(55 ページ\)](#) 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、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 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。

Management Center では、この文字列を、[Management Center における OneLogin のユーザーロールマッピングの設定 \(55 ページ\)](#) の手順 5 で各 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。

次のタスク

- さまざまなアカウントから SSO を使用して Management Center にログインし、期待どおりにユーザーに 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 ユーザーロールマッピングの例

次の例が示すように、ユーザーロールマッピングをサポートする Management Center での SSO 構成は、個々のユーザーとグループの両方で同じです。違いは、OneLogin の Management Center サービス プロバイダー アプリケーションの設定にあります。



- (注) 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。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。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 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。

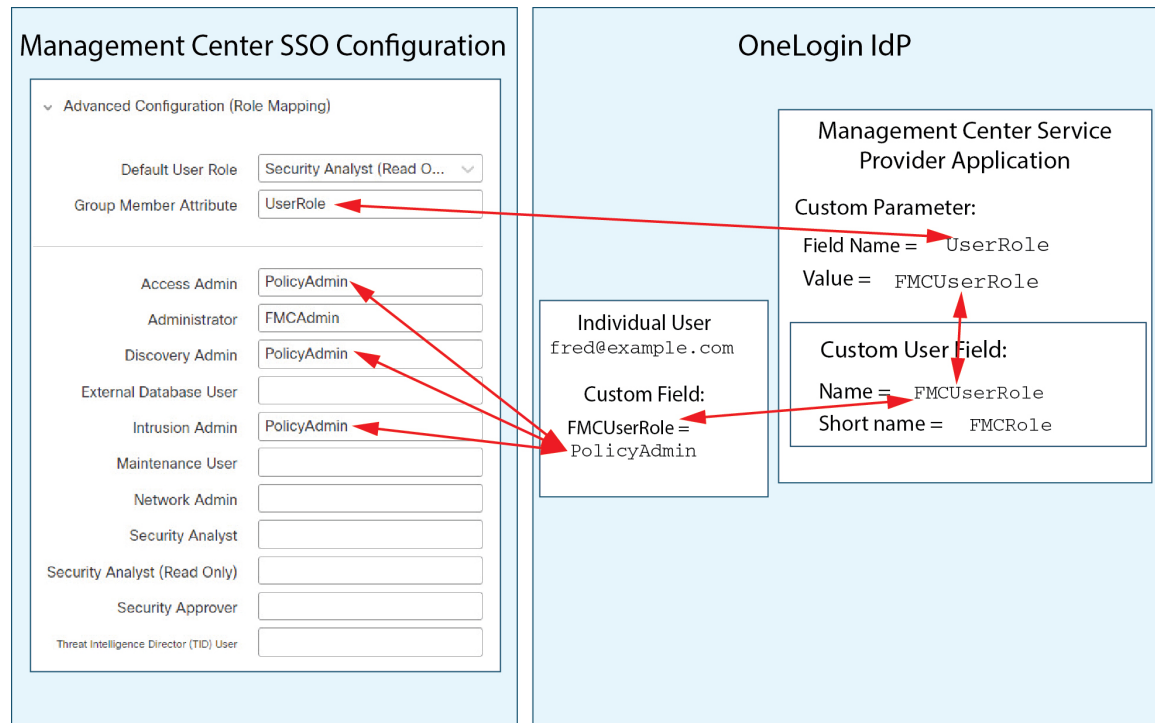
個人ユーザーアカウントの OneLogin ロールマッピングの例

個人ユーザーのロールマッピングでは、OneLogin Management Center サービスアプリケーションに、名前が Management Center でのグループメンバー属性の名前と一致するカスタムパラメー

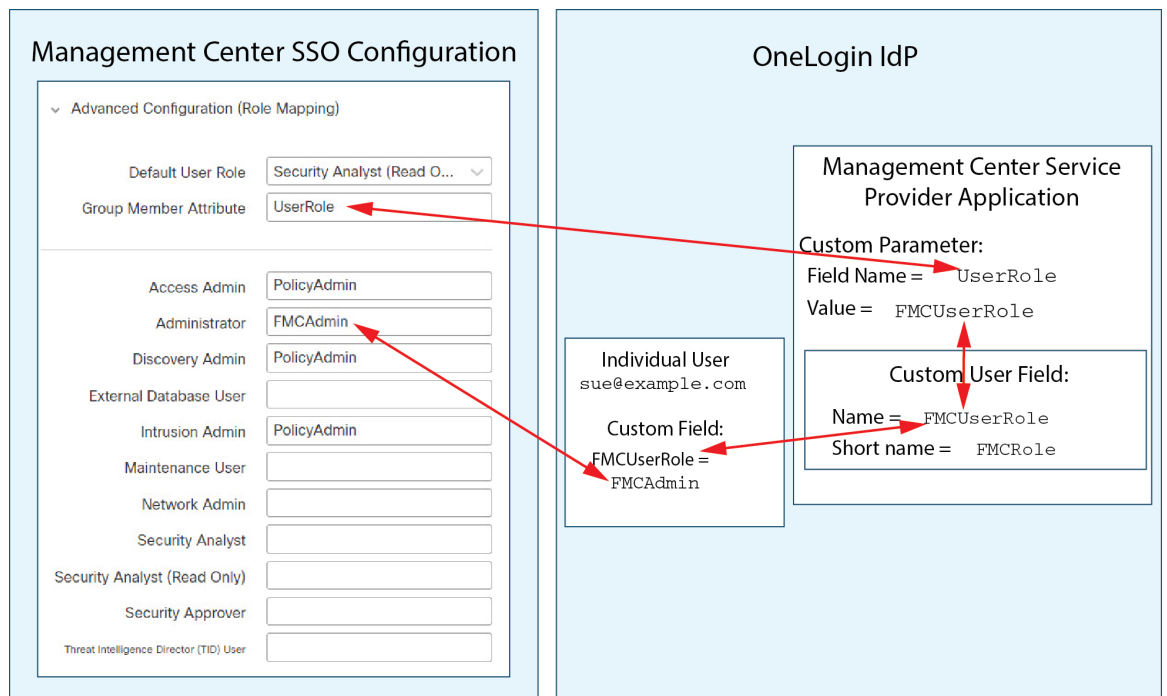
タがあります（この例では、UserRole）。OneLoginには、カスタムユーザーフィールドも定義されています（この例ではFMCUserRole）。アプリケーションのカスタムパラメータ UserRole の定義により、OneLogin がユーザーロールマッピング情報を Management Center に渡すときに、問題のユーザーのカスタムユーザーフィールド FMCUserRole の値を使用することが確立されます。

次の図は、Management Center および OneLogin 構成の関連するフィールドと値が、個人アカウントのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図は、Management Center と OneLogin Admin ポータルで同じ SSO 構成を使用していますが、OneLogin Admin ポータルでの各ユーザーの構成は、Management Center で各ユーザーに異なるロールを割り当てるために異なります。

- この図では、fred@example.com では FMCUserRole 値 PolicyAdmin が使用されていて、Management Center が彼にアクセス管理者、検出管理者、侵入管理者のロールを割り当てます。



- この図では、sue@example.com では FMCUserRole 値 FMCAdmin が使用されていて、Management Center が彼女に管理者ロールを割り当てます。



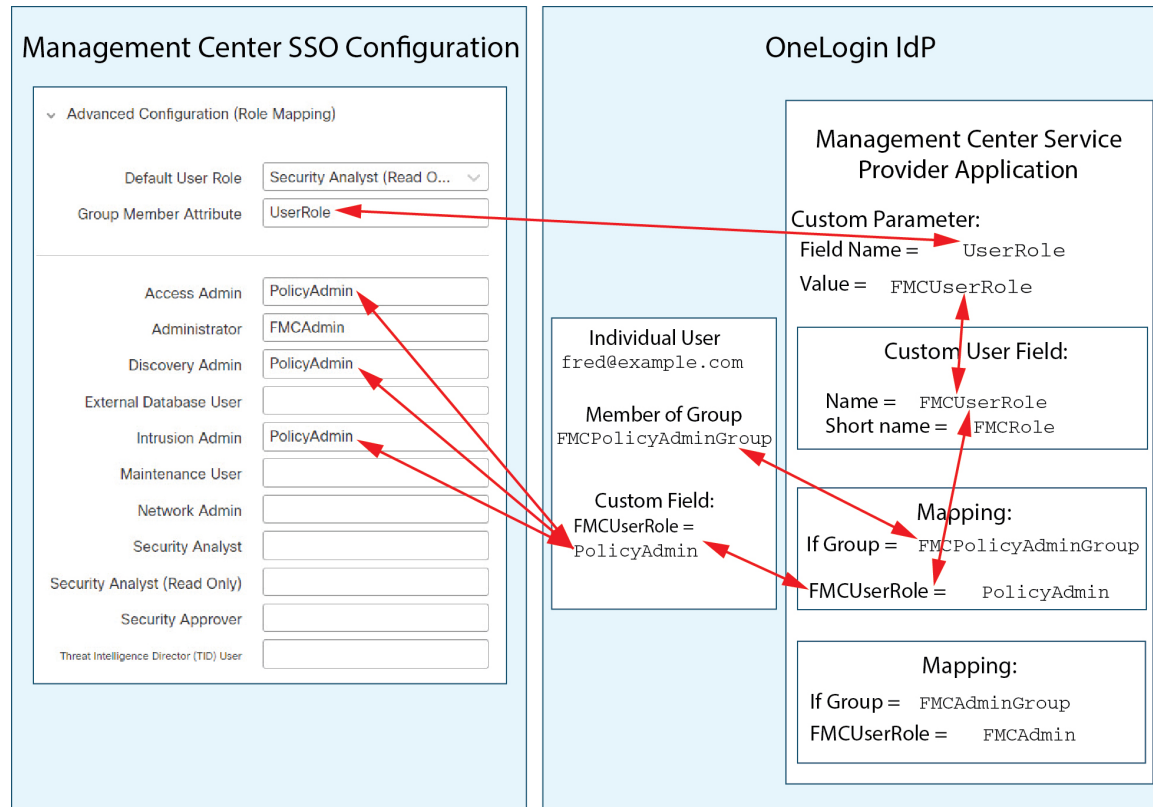
- この Management Center のために OneLogin サービスアプリケーションに割り当てられた他のユーザーには、次のいずれかの理由で、デフォルトのユーザーロールであるセキュリティアナリスト（読み取り専用）が割り当てられます。
 - FMCUserRole カスタムユーザーフィールドに値が割り当てられていません。
 - FMCUserRole カスタムユーザーフィールドに割り当てられた値が、Management Center の SSO 設定でユーザーロールに設定された式と一致しません。

グループの OneLogin ロールマッピングの例

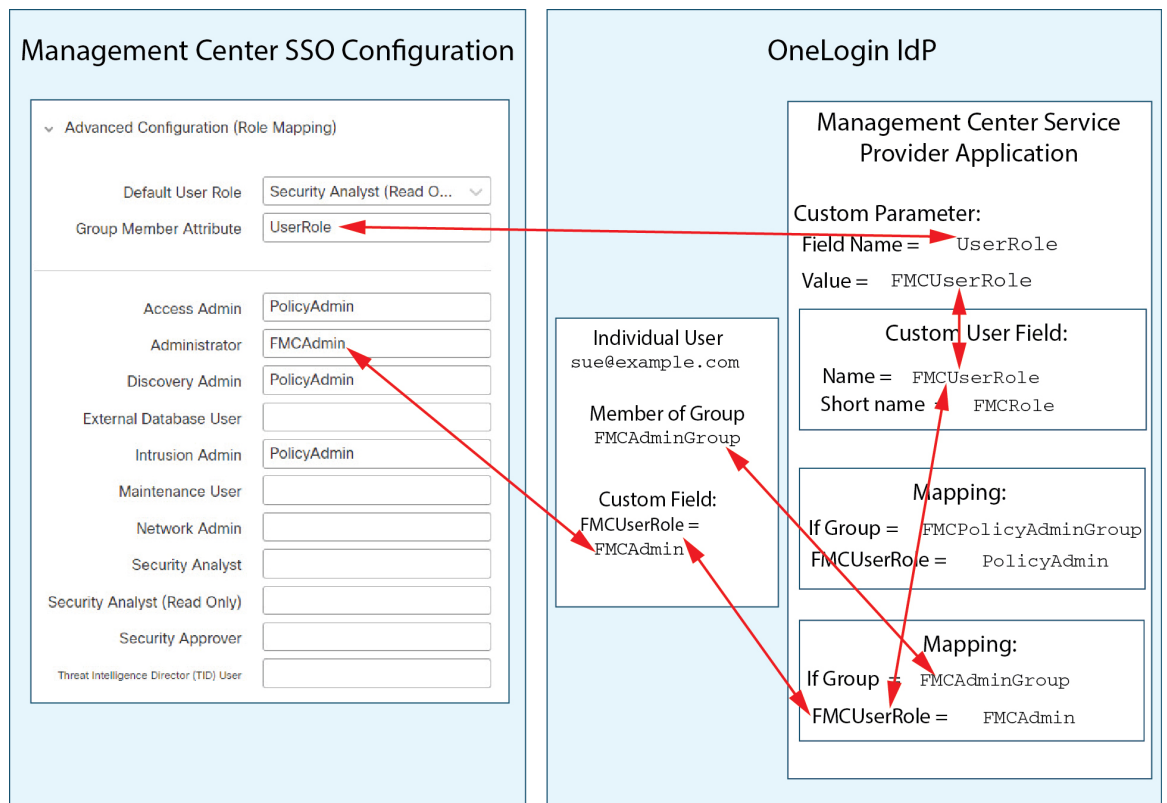
グループのロールマッピングでは、OneLogin Management Center サービスアプリケーションに、名前が Management Center でのグループメンバー属性の名前と一致するカスタムパラメータがあります（この例では、UserRole）。OneLogin には、カスタムユーザーフィールドも定義されています（この例では FMCUserRole）。アプリケーションのカスタムパラメータ UserRole の定義により、OneLogin がユーザーロールマッピング情報を Management Center に渡すときに、問題のユーザーのカスタムユーザーフィールド FMCUserRole の値を使用することが確立されます。ユーザーグループマッピングをサポートするには、OneLogin 内でマッピングを確立して、そのユーザーの OneLogin グループメンバーシップに基づいて各ユーザーの FMCUserRole フィールドに値を割り当てる必要があります。

次の図は、Management Center および OneLogin 構成の関連するフィールドと値が、グループのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図は、Management Center と OneLogin Admin ポータルで同じ SSO 構成を使用していますが、OneLogin Admin ポータルでの各ユーザーの構成は、Management Center で各ユーザーに異なるロールを割り当てるために異なります。

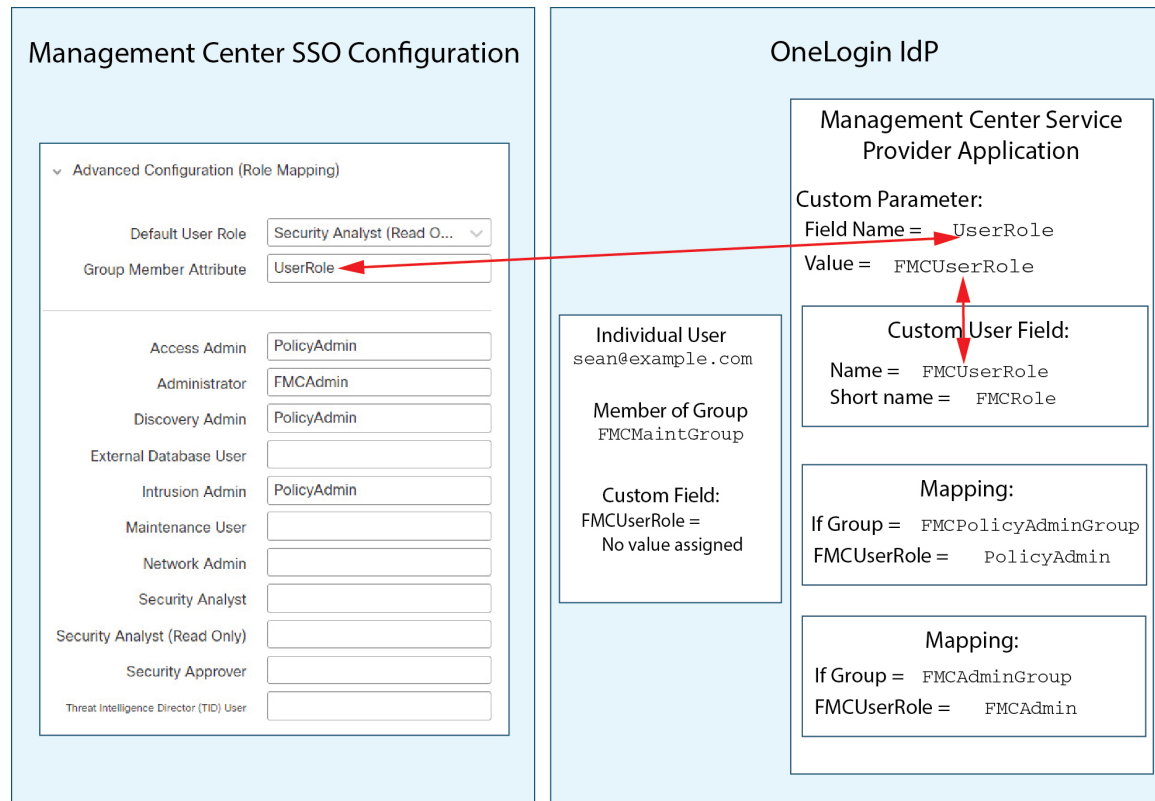
- この図では、fred@example.com は OneLogin IdP グループ FMCPolicyAdminGroup のメンバーです。OneLogin マッピングは、値 PolicyAdmin を FMCPolicyAdminGroup のメンバーのカスタムユーザーフィールド FMCUserRole に割り当てます。Management Center は Fred および FMCPolicyAdminGroup の他のメンバーにアクセス管理者、検出管理者、侵入管理者のロールを割り当てます。



- この図では、sue@example.com は OneLogin IdP グループの FMCAdminGroup のメンバーです。OneLogin マッピングは、値 FMCAdmin を FMCAdminGroup のメンバーのカスタムユーザーフィールド FMCUserRole に割り当てます。Management Center は、Sue と FMCAdminGroup の他のメンバーに管理者ロールを割り当てます。

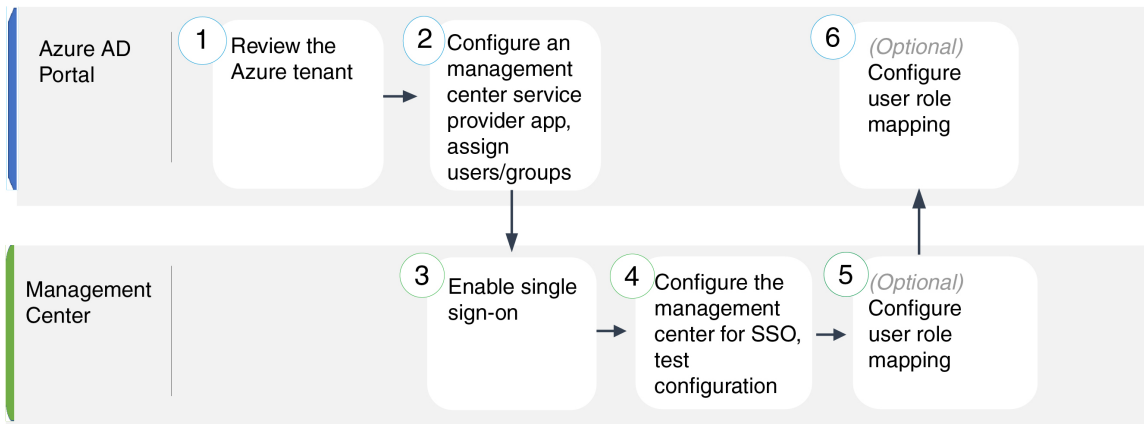


- この図では、sean@example.com は Idp グループ FMCMaintGroup のメンバーです。このグループには OneLogin マッピングが関連付けられていないため、OneLogin は Sean のカスタムユーザーフィールド FMCUserRole に値を割り当てません。Management Center は、メンテナンスユーザーロールではなく、デフォルトのユーザーロール（セキュリティアナリスト（読み取り専用））を Sean に割り当てます。



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 (66 ページ)
2	Azure AD ポータル	Azure の Management Center サービス プロバイダー アプリケーションの設定 (66 ページ)

3	Management Center	Management Centerでのシングルサインオンの有効化 (35 ページ)
4	Management Center	Azure SSO 用の Management Center の設定 (69 ページ)
5	Management Center	Management Center における Azure のユーザーロールマッピングの設定 (70 ページ)
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 (71 ページ)

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。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。

- 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？
- 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 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、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 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 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。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 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 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。



- (注) 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。



- (注) 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 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。

始める前に

- 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 \(66 ページ\)](#) 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。



- (注) 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 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、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 Management Center のログイン URL を確認します (`https://ipaddress_or_hostname`)



- (注) 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 Management Center にアクセスする必要があります。

手順

- ステップ 1** Azure AD SAML Toolkit をベースとして使用して、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 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 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 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、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 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。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)]

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) Management Center での SSO セットアップを簡単にするために、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 Management Center サービスアプリケーションに割り当てます。

(注) 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。

(注) 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 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。

次のタスク

シングルサインオンを有効にします。 [Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) を参照してください。

Azure SSO 用の Management Center の設定

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

始める前に

- Azure AD ポータルで 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 Management Center サービス プロバイダー アプリケーションの設定 \(66 ページ\)](#) 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。 [Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) を参照してください。

手順

ステップ 1 (このステップは [Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) 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：
 1. [手動設定 (Manual Configuration)] オプションボタンをクリックします。
 2. 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 Management Center サービス プロバイダー アプリケーションの設定 \(66 ページ\)](#) 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 Management Center サービス プロバイダー アプリケーションの設定 \(66 ページ\)](#) 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 Management Center サービス プロバイダー アプリケーションの設定 \(66 ページ\)](#) のステップ 5 で Azure からダウンロード

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 Management Center サービス プロバイダー アプリケーションの設定 \(66 ページ\)](#) のステップ 7）、ファイルを Management Center にアップロードできます。
 1. [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。
 2. 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、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実行します。

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。

次のタスク

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。[Management Center における Azure のユーザーロールマッピングの設定 \(70 ページ\)](#) 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、Management Center にログインするすべての SSO ユーザーに、[Management Center における Azure のユーザーロールマッピングの設定 \(70 ページ\)](#) 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。

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

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。

始める前に

- 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 \(66 ページ\)](#) を参照してください。
- 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 Management Center サービス プロバイダー アプリケーションの設定 \(66 ページ\)](#) を参照してください。

- Management Center でシングルサインオンを有効にして設定します。Management Center でのシングルサインオンの有効化 (35 ページ) および Azure SSO 用の Management Center の設定 (69 ページ) を参照してください。

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 [Single Sign-On] タブをクリックします。
- ステップ 3 [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 4 [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 Management Center ユーザーロールを選択します。
- ステップ 5 [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、Azure の Management Center サービス プロバイダー アプリケーション用に作成するユーザーの請求の名前と一致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 (72 ページ) 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 (73 ページ) のステップ 1 を参照してください。
- ステップ 6 SSO ユーザーに割り当てる各 Management Center ユーザーロールの横に、正規表現を入力します。(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を使用します。) Management Center は、これらの値を、IdP が SSO ユーザー情報とともに 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。Management Center は、一致が見つかったすべてのロールの和集合をユーザーに付与します。

次のタスク

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 (71 ページ) 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 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 Management Center に提示します。Management Center はその属性値を SSO 設定で各 Management Center ユーザーロールに割り当てられた正規表現と比較し、一致が見つかったすべてのロール

をユーザーに付与します。（一致するものが見つからない場合、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）。各 Management Center ユーザーロールに割り当てる式は、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必要があります。Management Center は、Azure から受け取った属性値を、Management Center ユーザーロール式との比較のために、同じ標準規格を使用する正規表現として扱います。



- (注) 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。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。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 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 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。

始める前に

- Azure テナントを確認します。[Azure テナントの確認 \(66 ページ\)](#) を参照してください。
- Azure で 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 Management Center サービス プロバイダー アプリケーションの設定 \(66 ページ\)](#) を参照してください。
- [Management Center における Azure のユーザーロールマッピングの設定 \(70 ページ\)](#) 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。

手順

ステップ 1 次の特性を使用して、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)] : 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一文字列を使用します。（[Management Center における Azure のユーザーロールマッピングの設定 \(70 ページ\)](#) 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 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 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 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 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 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 Management Center に送信する値です。Management Center は、SSO 設定で Management Center ユーザーロールに割り当てた式と要求を比較し ([Management Center における Azure のユーザーロールマッピングの設定 \(70 ページ\)](#)) のステップ 6 を参照)、一致するすべての Management Center ユーザーロールをユーザーに割り当てます。

次のタスク

- さまざまなアカウントから SSO を使用して Management Center にログインし、期待どおりにユーザーに 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 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。

始める前に

- Azure テナントを確認します。[Azure テナントの確認 \(66 ページ\)](#) を参照してください。
- Azure で 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 Management Center サービス プロバイダー アプリケーションの設定 \(66 ページ\)](#) を参照してください。
- [Management Center における Azure のユーザーロールマッピングの設定 \(70 ページ\)](#) 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。

手順

ステップ 1 次の特性を使用して、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)] : 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一文字列を使用します。 ([Management Center における Azure のユーザーロールマッピングの設定 \(70 ページ\)](#) 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 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 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 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 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 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 Management Center に送信する値です。Management Center は、SSO 設定で Management Center ユーザーロールに割り当てた式と要求を比較し ([Management Center における Azure のユーザーロールマッピングの設定 \(70 ページ\)](#) のステップ 6 を参照) 、一致するすべての Management Center ユーザーロールをユーザーに割り当てます。

次のタスク

さまざまなアカウントから SSO を使用して Management Center にログインし、期待どおりにユーザーに 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 ユーザーロールマッピングの例

次の例が示すように、ユーザーロールマッピングをサポートする Management Center での SSO 構成は、個々のユーザーとグループの両方で同じです。違いは、Azure の Management Center サービス プロバイダー アプリケーションの設定にあります。



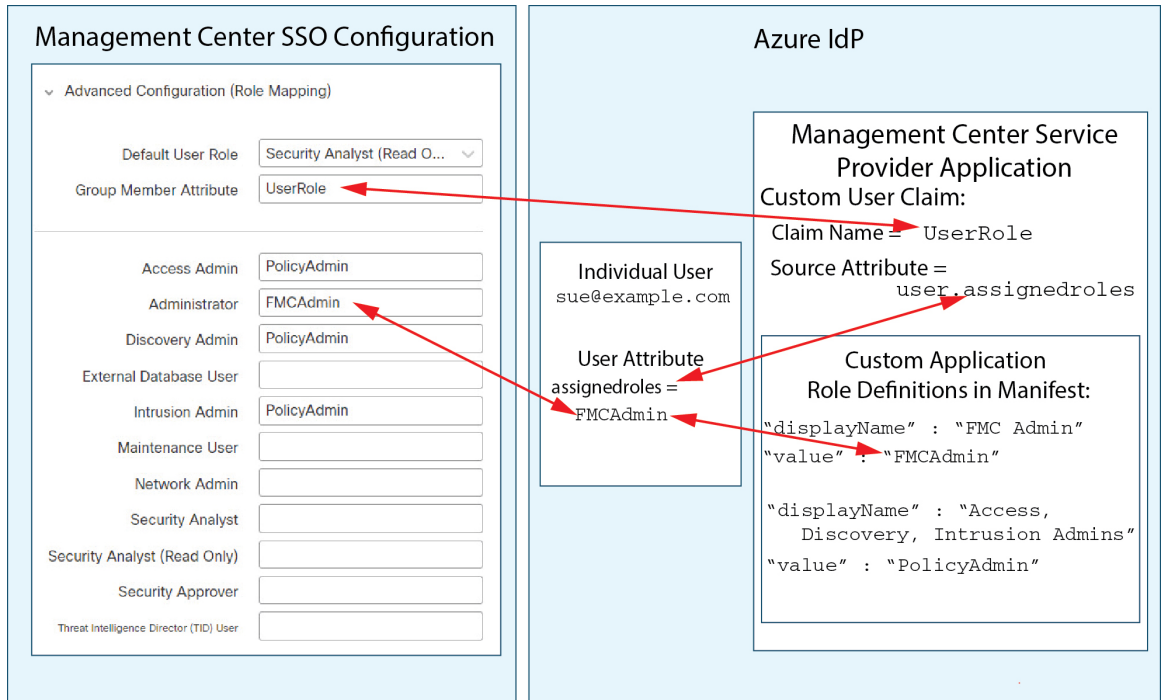
- (注) 個別の権限またはグループ権限に基づいて Management Center ロールがマッピングされるように構成できますが、単一の Management Center アプリケーションでは、グループと個人ユーザーの両方のロールマッピングはサポートできないことに注意してください。Management Center は、Azure で構成された 1 つの要求のみを使用してロールマッピングをサポートできます。

個人ユーザーアカウントの Azure ロールマッピングの例

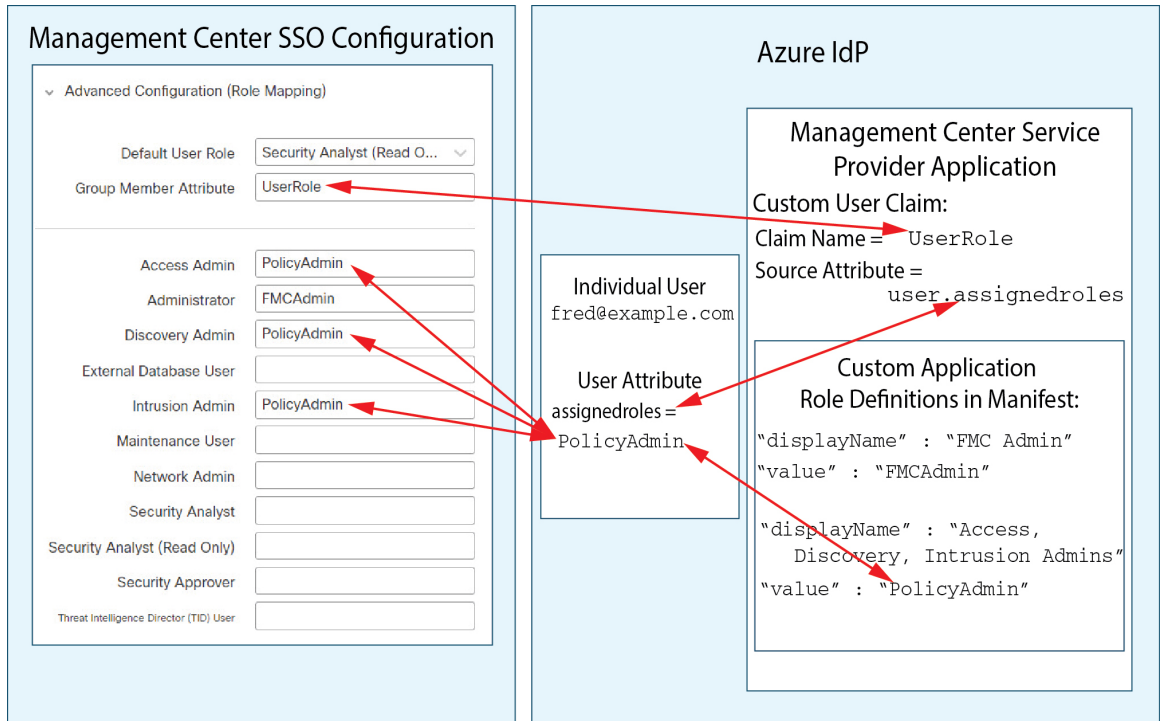
個人ユーザーのロールマッピングでは、Azure Management Center サービスアプリケーションのマニフェスト内にカスタムロールが定義されています（この場合、FMCAdmin と PolicyAdmin です）。これらのロールはユーザーに割り当てることができます。Azure は、各ユーザーのロールの割り当てをそのユーザーの `assignedroles` 属性に保存します。アプリケーションにはカスタムユーザークレームも定義されていて、このクレームは、SSO を使用して Management Center にログインしているユーザーに割り当てられたユーザーロールから値を取得するように構成されています。Azure は SSO ログインプロセス中にクレーム値を Management Center に渡し、Management Center はクレーム値を Management Center SSO 構成の各 Management Center ユーザーロールに割り当てられた文字列と比較します。

次の図は、Management Center および Azure 構成の関連するフィールドと値が、個人アカウントのユーザーロールマッピングで互いにどのように対応しているかを示しています。各図は、Management Center と Azure AD ポータルで同じ SSO 構成を使用していますが、Azure AD ポータルでの各ユーザーの構成は、Management Center で各ユーザーに異なるロールを割り当てるために異なります。

- この図では、`sue@example.com` では `assignedroles` 属性値 `FMCAdmin` が使用されていて、Management Center が彼女に Management Center 管理者ロールを割り当てます。



- この図では、fred@example.com では assignedroles 属性値 PolicyAdmin が使用されていて、Management Center が彼にアクセス管理者、検出管理者、侵入管理者のロールを割り当てます。



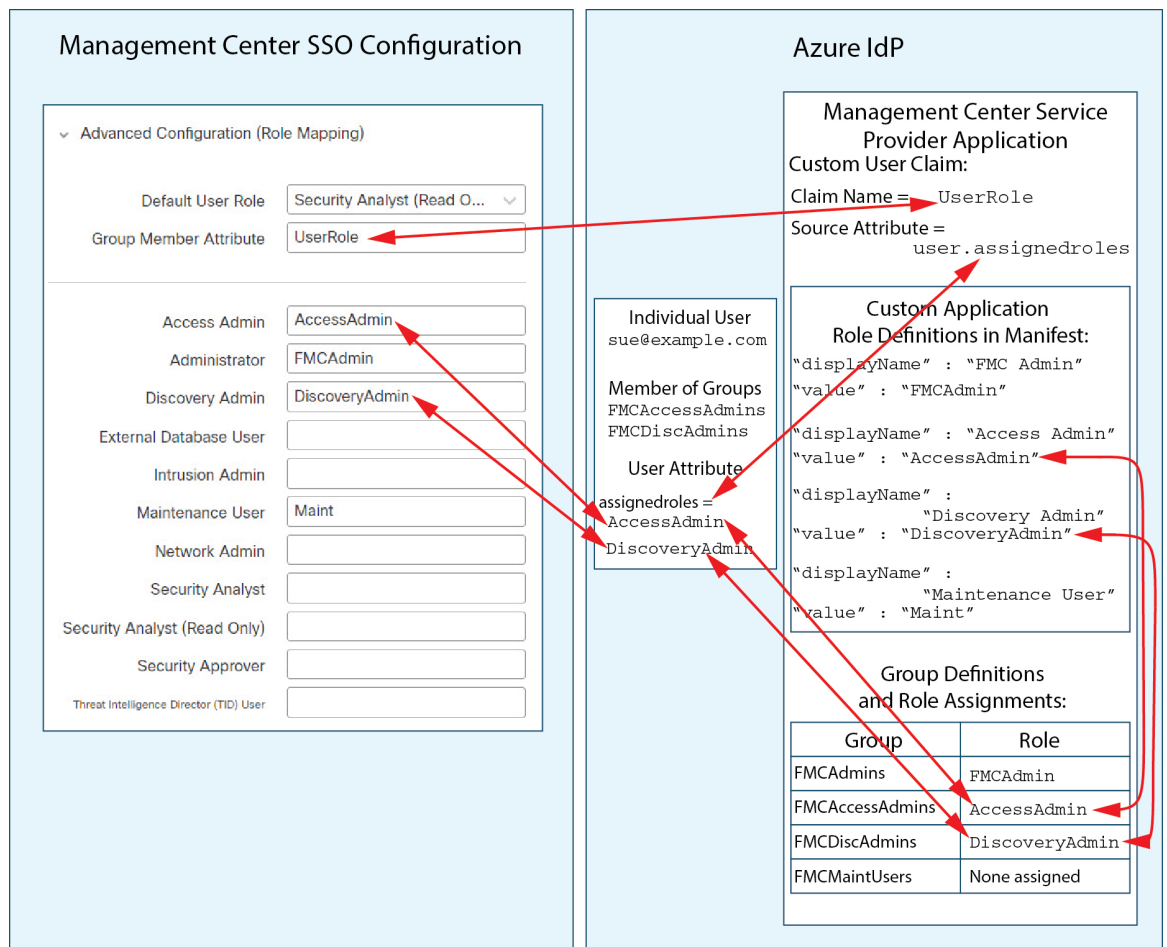
- この Management Center のために Azure サービスアプリケーションに割り当てられた他のユーザーには、次のいずれかの理由で、デフォルトのユーザーロールであるセキュリティアナリスト（読み取り専用）が割り当てられます。
 - これらには、assignedroles 属性に割り当てられた値がありません。
 - assignedroles 属性に割り当てられた値が、Management Center の SSO 設定でユーザーロールに設定された式と一致しません。

グループの Azure ロールマッピングの例

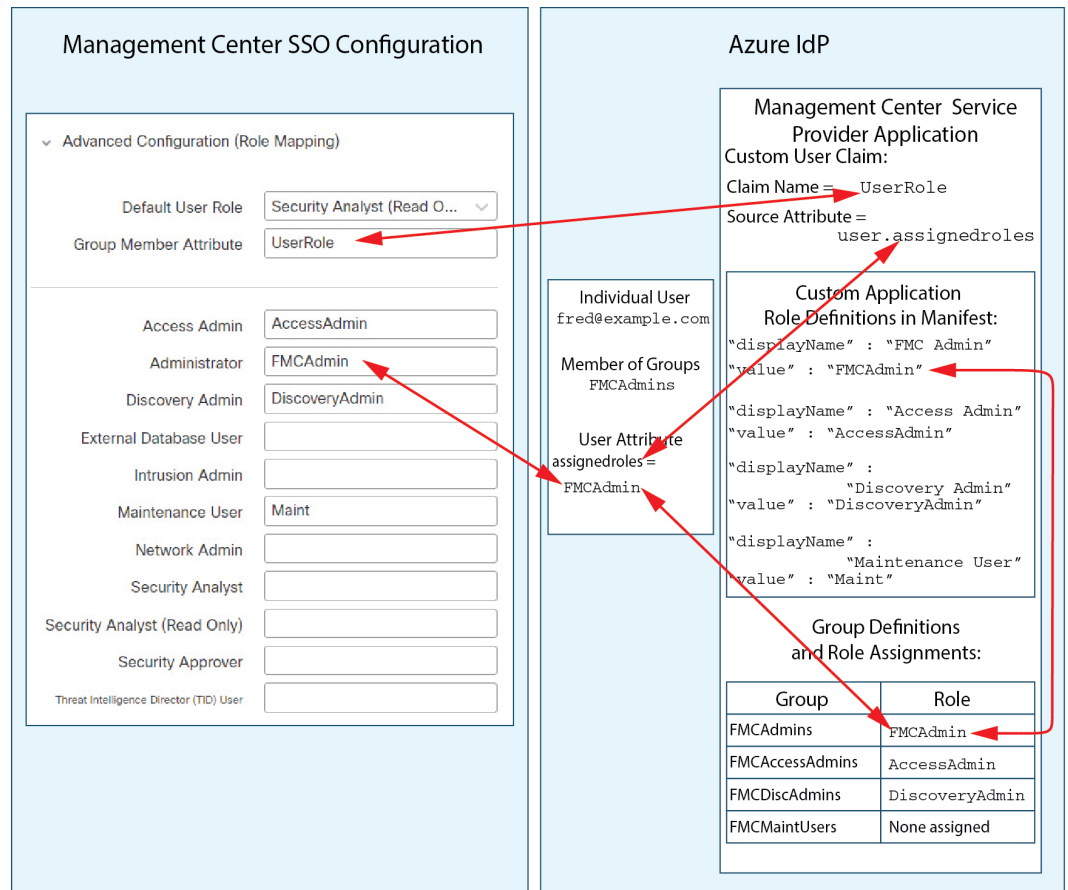
グループのロールマッピングでは、Azure Management Center サービスアプリケーションのマニフェスト内にカスタムロールが定義されています（この場合、FMCAdmin、AccessAdmin、Discovery Admin、Maint です）。これらのロールはグループに割り当てることができます。Azure は、各グループのロールの割り当てをグループメンバーの assignedroles 属性に渡します。アプリケーションにはカスタムユーザークレームも定義されていて、このクレームは、SSO を使用して Management Center にログインしているユーザーに割り当てられたユーザーロールから値を取得するように構成されています。Azure は SSO ログインプロセス中にクレーム値を Management Center に渡し、Management Center はクレーム値を Management Center SSO 構成の各 Management Center ユーザーロールに割り当てられた文字列と比較します。

次の図は、Management Center および Azure 構成の関連するフィールドと値が、グループのユーザーロールマッピングで互いに対応しているかを示しています。各図は、Management Center と Azure AD ポータルで同じ SSO 構成を使用していますが、Azure AD ポータルでの各ユーザーの構成は、Management Center で各ユーザーに異なるロールを割り当てるために異なります。

- この図では、sue@example.com は FMCAccessAdmins および FMCDiscoveryAdmins グループのメンバーです。これらのグループから、Sue はカスタムロール AccessAdmin および DiscoveryAdmin を継承します。Sue が SSO を使用して Management Center にログインすると、Management Center によってアクセス管理者および検出管理者のロールが割り当てられます。

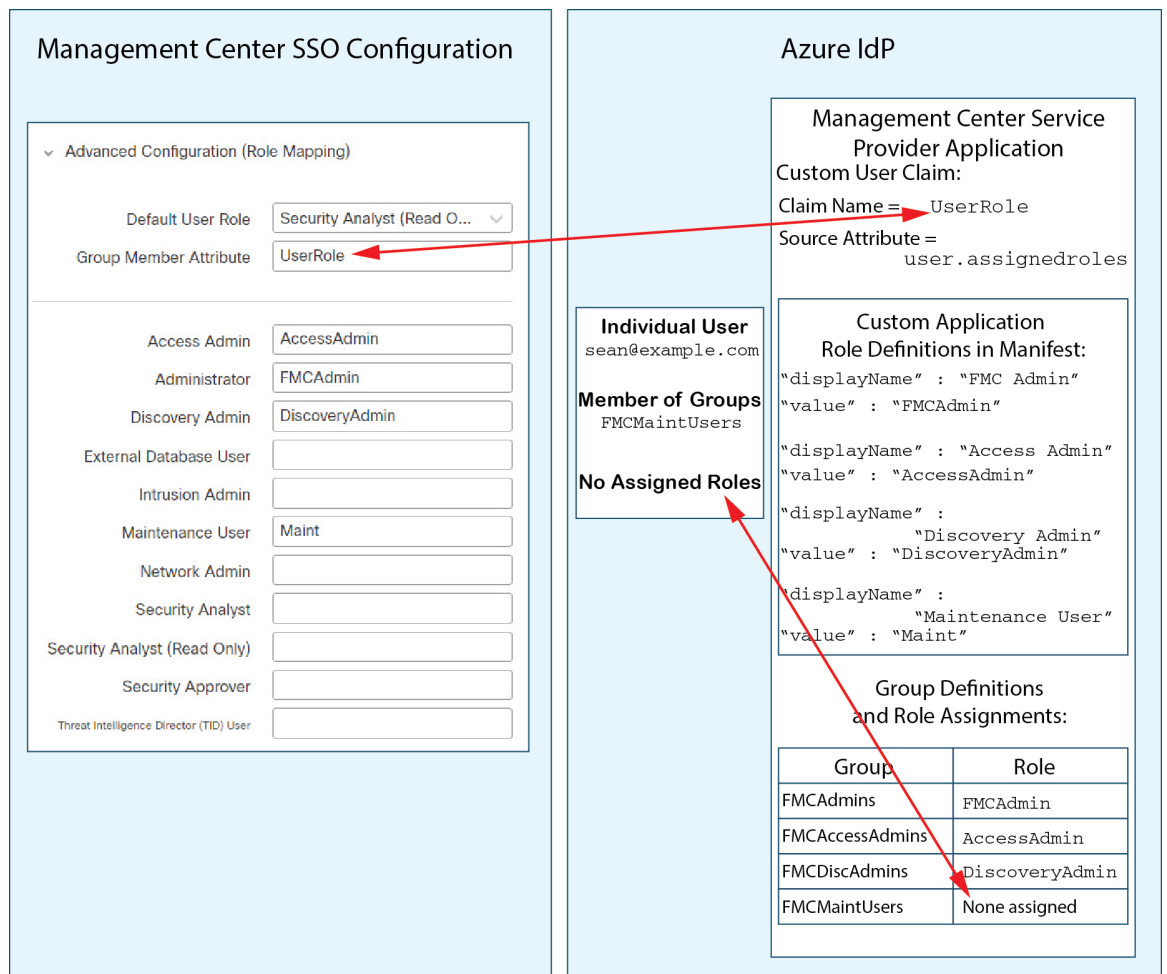


- この図では、fred@example.com は FMCAAdmins グループのメンバーであり、そこからカスタムロール FMCAAdmin を継承しています。Fred が SSO を使用して Management Center にログインすると、Management Center によって管理者ロールが割り当てられます。



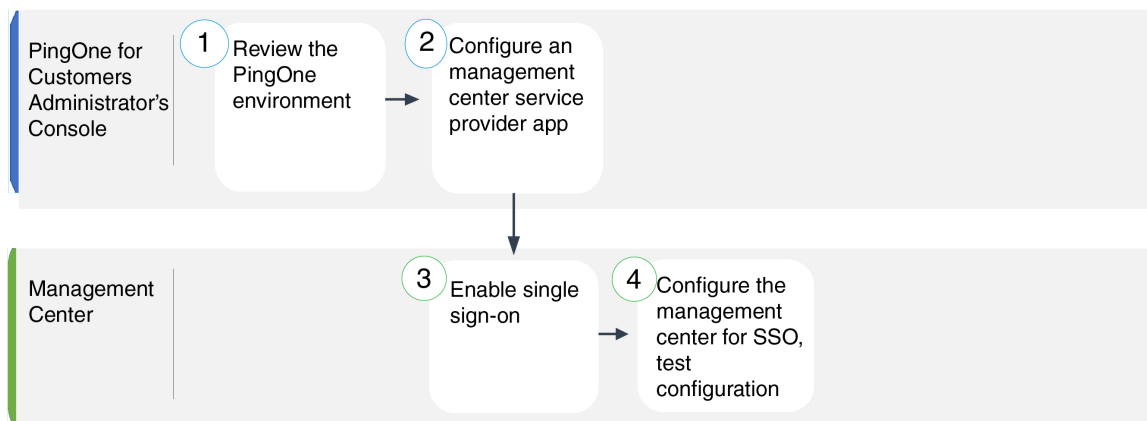
- この図では、sean@example.com は FMCMaintUsers グループのメンバーですが、Azure Management Center サービス プロバイダー アプリケーション内で FMCMaintUsers にカスタムロールが割り当てられていないため、Sean にはロールが割り当てられていません。このため、SSO を使用して Management Center にログインすると、Management Center によってデフォルトロールのセキュリティアナリスト（読み取り専用）が割り当てられます。

PingID を使用したシングルサインオンの設定



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 (81 ページ)。
②	PingOne for Customers 管理者コンソール	PingID PingOne for Customers の Management Center サービス プロバイダー アプリケーションの設定 (81 ページ)。
③	Management Center	Management Centerでのシングルサインオンの有効化 (35 ページ)。
④	Management Center	PingID PingOne for Customers を使用した SSO 用の Management Center の設定 (83 ページ)。

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。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。

- Management Center にアクセスできるユーザーは何人ですか？
- 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 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 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。

始める前に

- 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。



(注) 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 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、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 Management Center のログイン URL を確認します (`https://ipaddress_or_hostname`)



(注) 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 Management Center にアクセスする必要があります。

手順

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 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 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、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なになります。

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) Management Center での SSO セットアップを簡単にするために、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。

次のタスク

シングルサインオンを有効にします。 [Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) を参照してください。

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

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

始める前に

- PingOne for Customers 管理者コンソールで 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 Management Center サービスプロバイダーアプリケーションの設定 \(81 ページ\)](#) 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。 [Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) を参照してください。

手順

ステップ1 (このステップは [Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) 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 :

1. [手動設定 (Manual Configuration)] オプションボタンをクリックします。
2. 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 Management Center サービスプロバイダー アプリケーションの設定 \(81 ページ\)](#) 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 Management Center サービスプロバイダー アプリケーションの設定 \(81 ページ\)](#) 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 Management Center サービスプロバイダー アプリケーションの設定 \(81 ページ\)](#) 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 Management Center サービスプロバイダー アプリケーションの設定 \(81 ページ\)](#) のステップ 6)、ファイルを Management Center にアップロードできます。
 1. [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。
 2. 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 [詳細設定 (ロールマッピング) (Advanced Configuration (Role Mapping))] を展開します。

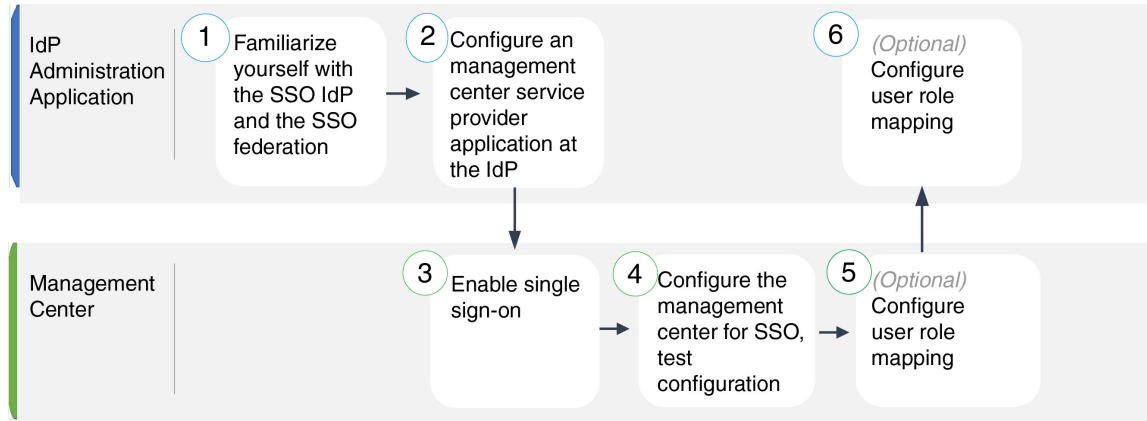
ステップ 5 [デフォルトのユーザーロール (Default User Role)] ドロップダウンから、ユーザーをデフォルト値として割り当てる Management Center ユーザーロールを選択します。

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、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 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。

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

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 に習熟する必要があります。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 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 (86 ページ)。
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 Management Center サービスプロバイダーアプリケーションの設定 (87 ページ)。
③	Management Center	Management Centerでのシングルサインオンの有効化 (35 ページ)。
④	Management Center	SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Management Center の設定 (89 ページ)。
⑤	Management Center	SAML 2.0 準拠の SSO プロバイダーの Management Center でのユーザーロールマッピングの設定 (90 ページ)。

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 Management Center ユーザーロールマッピングの設定 (92 ページ)。
---	----------------	---

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 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 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。
- 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、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 Management Center 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。



- (注) 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。



- (注) 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 Management Center に伝達する必要があります。

始める前に

- 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 \(86 ページ\)](#) 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。



- (注) 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 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、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 Management Center のログイン URL を確認します (`https://ipaddress_or_hostname`)



- (注) 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 Management Center にアクセスする必要があります。

手順

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。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 (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、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 (Management Center) のアドレス。これを作成するには、`https://ExampleFMC/saml/acs` のように、Management Center ログイン URL に文字列 `saml/acs` を追加します。
- X.509 証明書 : 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 Management Center アプリケーションに割り当てます。(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) 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、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。

次のタスク

シングルサインオンを有効にします。[Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) 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 Management Center の設定

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 Management Center を設定するには、IdP からの情報が必要です。

始める前に

- 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 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 Management Center の設定 \(89 ページ\)](#) 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 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。
 - 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。[Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) を参照してください。

手順

ステップ 1 (このステップは[Management Centerでのシングルサインオンの有効化 \(35 ページ\)](#) 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 :
 1. [手動設定 (Manual Configuration)] オプションボタンをクリックします。
 2. 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 Management Center サービス プロバイダー アプリケーションの設定](#)（87 ページ）のステップ 5）、ファイルを Management Center にアップロードできます。
 1. [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。
 2. 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、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。

次のタスク

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 プロバイダーの Management Center でのユーザーロールマッピングの設定](#)（90 ページ）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、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 プロバイダーの Management Center でのユーザーロールマッピングの設定](#)（90 ページ）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 プロバイダーの 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 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 Management Center に送信します。
- Management Center で、ユーザーに割り当てる各 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 Management Center に送信すると、Management Center は属性値を各 Management Center ユーザーロールに関連付けられた値と比較し、一致するすべてのロールをユーザーに割り当てます。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い、この比較を実行します。

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。

始める前に

- 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 Management Center サービス プロバイダー アプリケーションの設定 \(87 ページ\)](#) を参照してください。
- Management Center でシングルサインオンを有効にして設定します。[Management Center でのシングルサインオンの有効化 \(35 ページ\)](#) および[SAML 2.0 準拠の SSO プロバイダーを使用した SSO 用の Management Center の設定 \(89 ページ\)](#) を参照してください。

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 [Single Sign-On] タブをクリックします。
 - ステップ 3 [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 4 [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 Management Center ユーザーロールを選択します。
 - ステップ 5 [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 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 Management Center ユーザーロールマッピングの設定 \(92 ページ\)](#) のステップ 1 を参照。)
 - ステップ 6 SSO ユーザーに割り当てる各 Management Center ユーザーロールの横に、正規表現を入力します。(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を使用します。) Management Center は、これらの値を、IdP が SSO ユーザー情報とともに 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。Management Center は、一致が見つかったすべてのロールの和集合をユーザーに付与します。
-

次のタスク

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 Management Center ユーザーロールマッピングの設定 \(92 ページ\)](#) 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 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、ユーザーまたはグループの特権を 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。
- 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 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 Management Center でより効率的です。
- 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。
- Management Center ユーザーロール式との一致を判断するために、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。

始める前に

- 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 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 Management Center サービス プロバイダー アプリケーションの設定 \(87 ページ\)](#) を参照してください）。

手順

- ステップ1 IdP で、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、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

各ユーザーアカウントは、ユーザーロールで定義する必要があります。このセクションでは、ユーザー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ー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、「[ユーザの役割 \(3 ページ\)](#)」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 Management Center からインポートすることができます。



- (注) (バージョン 7.4.1 以降が必要) 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せんが、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したり、古い ASA FirePOWER および NGIPSv デバイスをアップグレードしたり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 (⚙️) > [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Management Centerで、  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Management Centerで、システム () > [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。

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

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

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

カスタムユーザ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。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 \(96 ページ\)](#)」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

ルール名に手動で追加してル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ーロールを作成して、ユーザー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	はい	はい	はい
アクセスコントロールポリシー (Access Control Policy)	はい	はい	はい
アクセス制御ポリシーの変更 (Modify Access Control Policy)	いいえ	はい	いいえ
脅威設定の変更	いいえ	はい	いいえ
残りのアクセスコントロールポリシー設定の変更	はい	いいえ	いいえ
侵入ポリシー	いいえ	はい	はい
侵入ポリシーの変更 (Modify Intrusion Policy)	いいえ	はい	いいえ

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
設定をデバイスに展開	いいえ	いいえ	はい

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 (⚙️) > [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 \(97ページ\)](#)。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 \(97ページ\)](#)。
- 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 \(98ページ\)](#)

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 (⚙️) > [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せん。

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 \(97 ページ\)](#)」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 \(93 ページ\)](#)」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使用するパスワードを選択します。次の2つの対処法があります。
- このロールを持つユーザがエスカレーション時に自分のパスワードを使用するには、[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には、[指定したユーザのパスワードを使用して認証 (Authenticate with the specified user's password)] を選択して、そのユーザ名を入力します。
- (注) 別のユーザのパスワードで認証するときには、任意のユーザ名 (非アクティブなユーザまたは存在しないユーザを含む) を入力できます。エスカレーションにパスワードが使用されるユーザを非アクティブにすると、そのパスワードを必要とするロールが割り当てられているユーザのエスカレーションが不可能になります。この機能を使用して、必要に応じてエスカレーション機能をただちに削除できます。
- ステップ 4** [保存 (Save)] をクリックします。
-

ユーザー 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 ユーザー ロールを割り当てられたユーザーは、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、ユーザのユーザ バインディングが失敗しています。サードパーティアプリケーションを使用してサーバ認証を試行し、その接続でも同様にバインディングが失敗するかどうかを確認します。
- サーバを正しく指定していることを確認します。
 - サーバの IP アドレスまたはホスト名が正しいことを確認します。
 - ローカル アプライアンスから、接続する認証サーバに TCP/IP でアクセスできることを確認します。
 - サーバへのアクセスがファイアウォールによって妨げられないこと、およびオブジェクトで設定されているポートがオープンしていることを確認します。

- 証明書を使用して TLS または SSL 経由で接続する場合は、証明書のホスト名が、サーバ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 DN)] 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 サーバの名前が、接続に使用するホスト名と一致していることを確認します。
 - 暗号化されたサーバ接続で IPv6 アドレスを使用していないことを確認します。
- テストユーザを使用する場合、ユーザ名とパスワードが正しく入力されていることを確認します。
- テストユーザーを使用する場合、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。脅威に対する防御デバイスは、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、ユーザー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、[Management Center のユーザーアカウントの注意事項と制約事項 \(7 ページ\)](#) 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** [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 [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、[Management Center のユーザーアカウントの注意事項と制約事項 \(7 ページ\)](#) 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
- Dusk

- **Classic** (バージョン 6.6 以前の外観と操作性)

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 \(109 ページ\)](#)」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、[ユーザの役割 \(3 ページ\)](#) 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。

イベントビューの設定

[イベントビュー設定 (Event View Settings)] ページを使用して、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は、イベントビュー設定のユーザ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** [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 \(104 ページ\)](#) 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 \(105 ページ\)](#) 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。[デフォルト時間帯 \(106 ページ\)](#) 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 \(108 ページ\)](#) 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、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 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ため注意してください。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。[イベント ビュー設定 (Event View Settings)]ページの [デフォルト時間枠 (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 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、[監査ログの時間枠 (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、[イベントの時間枠 (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は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ます。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。

- [イベントの時間枠 (Events Time Window)] は、時間で制約できるほとんどの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。
- [監査ログの時間枠 (Audit Log Time Window)] は、監査ログ用の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 [グローバルな時間枠 (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 (static)] : 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 (expanding)] : 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。
- [スライド (sliding)] : 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、[時間枠の設定 (Time Window Settings)] ドロップダウンリストに表示されます。

- [最後を表示 - スライディング (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。

- [最後を表示 (静的/拡張) (Show the Last - Static/Expanding)] : このオプションで、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。

静的時間枠の場合は、[終了時刻を使用 (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、[終了時刻を使用 (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。

- [現在の日付 (静的/拡張) (Current Day - Static/Expanding)]: このオプションで、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。

静的時間枠の場合は、[終了時刻を使用 (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、[終了時刻を使用 (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。

- [現在の週 (静的/拡張) (Current Week - Static/Expanding)]: このオプションで、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。

静的時間枠の場合は、[終了時刻を使用 (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、[終了時刻を使用 (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を含む大陸または地域を選択します。
- ステップ 4** 使用するタイムゾーンに対応する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、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。

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、ユーザー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 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。
 - この機能は、クラシックテーマでは使用できません。
-

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** [How To の設定 (How-To Settings)] 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。

Management Center ユーザーアカウントの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
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	いずれか	<p>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。</p> <p>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。</p>
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	<p>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。</p> <p>新規/変更された画面：</p> <p>システム (⚙) > [ユーザー (Users)] > [外部認証 (External Authentication)]</p>

機能	最小 Management Center	最小 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	<p>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 Management Center ユーザーロールにマッピングする機能が含まれません。</p> <p>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。</p> <p>新規/変更された画面： システム (⚙️) > [ユーザー (Users)] > [シングルサインオン (Single Sign-On)]</p>
Web インターフェイスのテーマ。	6.6.0	任意 (Any)	<p>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。</p> <p>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)]</p>
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)	<p>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。</p> <p>新規/変更された画面： システム (⚙️) > [ユーザー (Users)] > [ユーザー (Users)] > [本名 (Real Name)] フィールド</p>
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	<p>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。</p> <p>新規/変更された画面： システム (⚙️) > [ユーザー (Users)] ([System] > [Users]) > [CSM シングルサインオン (CSM Single Sign-on)]</p>
強化されたパスワードセキュリティ。	6.5.0	いずれか	<p>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。</p> <p>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)]</p> <p>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)]</p>

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。