Duo をアイデンティティ プロバイダーとして使用した Firewall Management Center での SAML SSO の有効化

改訂：2026 年 3 月 9 日

Duo を使用した Management Center での SAML SSO の有効化

対象読者

このガイドは、ネットワーク管理者がアイデンティティプロバイダー（IdP）として Duo を使用して Firewall Management Center でセキュリティアサーションマークアップ言語（SAML）シングルサインオン（SSO）を設定するのに役立ちます。

Firewall Management Center での SAML SSO の概要

Firewall Management Center で SSO を有効にすると、ログインページに SSO リンクが表示されます。SSO アクセスが可能なユーザーは、このリンクをクリックして、Firewall Management Center ログインページでユーザー名とパスワードを入力する代わりに、IdP（この場合は Duo）を介してサインインできます。Duo がユーザーを認証すると、ユーザーは Firewall Management Center Web インターフェイスにリダイレクトされ、自動的にログインします。Firewall Management Center と Duo 間のすべての通信はユーザーのブラウザを介して行われるため、Firewall Management Center では Duo への直接ネットワーク接続は必要ありません。

マルチテナント Firewall Management Center では、SAML ユーザーを特定のサブドメインに割り当てるように SSO を設定できます。これはグローバルドメインレベルでのみ設定できます。Duo と Firewall Management Center のロールが一致しない場合、デフォルトのロール（セキュリティアナリストのロール）がユーザーに割り当てられます。このデフォルトロールを使用すると、ユーザーはすべてのドメインにアクセスできます。

システム要件

表 1 に、この機能のプラットフォームとバージョン、およびこのドキュメントで示される例を一覧表示します。

製品	バージョン	このガイドで使用されるバージョン
Cisco Secure Firewall Management Center	6.7 以降	10.0
Cisco Secure Firewall Threat Defense	6.7 以降	10.0
Duo Admin Panel	—	Duo 75

Firewall Management Center で Duo を SSO 用に設定するにあたっての前提条件

- Duo 管理者アカウントを持っていることを確認します。
- Duo 管理者アカウントのログイン情報を使用して、https://admin.duosecurity.com/login で Duo Admin Panel にログインします。
- 二要素認証を完了します。
- ユーザーの二要素認証用デバイスに Duo Mobile をダウンロードします。
- Firewall Management Center が Duo IdP に到達できることを確認します。

Duo を使用した Firewall Management Center での SAML SSO の有効化のガイドライン

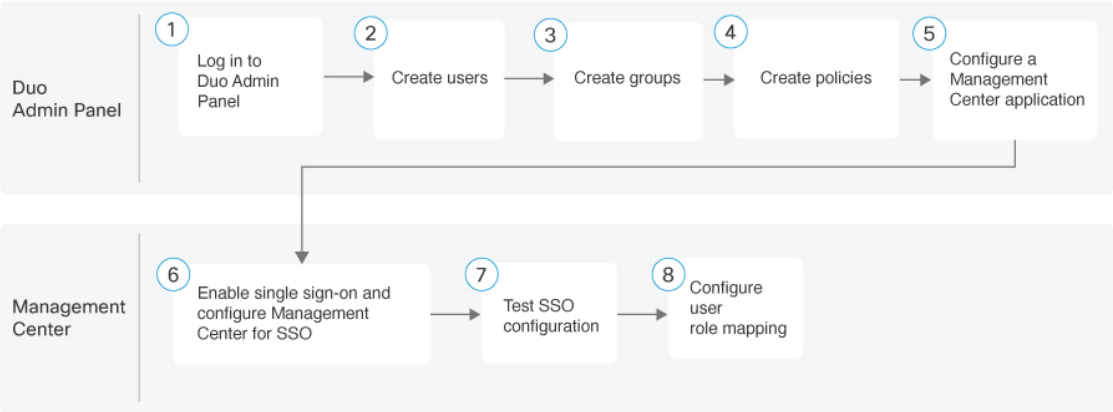
ガイドライン

- 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。
- Firewall Management Center 高可用性設定では、次のガイドラインに従ってください。
  - SSO 設定は高可用性ペアのメンバー間で同期されないため、ペアの各メンバーで個別に SSO を設定する必要があります。
  - 高可用性ペアの両方の Firewall Management Center は、SSO に同じ IdP を使用する必要があります。SSO 用に設定された各 Firewall Management Center の Duo 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。
  - ユーザーは、SSO を使用してセカンダリ Firewall Management Center に初めてアクセスする前に、まず SSO を使用してプライマリ Firewall Management Center に少なくとも 1 回ログインする必要があります。
- CC モードを使用して展開中に SSO を設定できません。

制限事項

- Firewall Management Center は、一度に 1 つの SSO プロバイダーのみを使用して SSO をサポートできます。たとえば、SSO に Duo と Okta の両方を使用するように Firewall Management Center を設定することはできません。
- Firewall Management Center は、Duo から開始された SSO をサポートしません。
- Firewall Management Center は、SSO アカウントの CAC クレデンシャルを使用したログインをサポートしません。

Firewall Management Center で Duo を使用して SAML SSO を有効にするためのワークフロー



ステップ	タスク	詳細情報
1	Duo Admin Panel にログインします。	—
2	Duo でユーザーを作成します。	Duo でのユーザーの作成 （4 ページ）
3	Duo でグループを作成します。	Duo でのグループの作成 （7 ページ）
4	Duo でポリシーを作成します。	ポリシーの作成 （9 ページ）
5	Duoで Firewall Management Center アプリケーションを設定します。	Duo での Firewall Management Center アプリケーションの作成 （10 ページ）
[6]	SSO を有効にし、SSO を使用できるように Firewall Management Center を設定します。	Duo SSO に向けた Firewall Management Center の設定 （13 ページ）
7	Firewall Management Center で SSO の設定をテストします。	—
8	Firewall Management Center でユーザーロールマッピングを設定します。	Duo SSO に向けた Firewall Management Center の設定 （13 ページ）

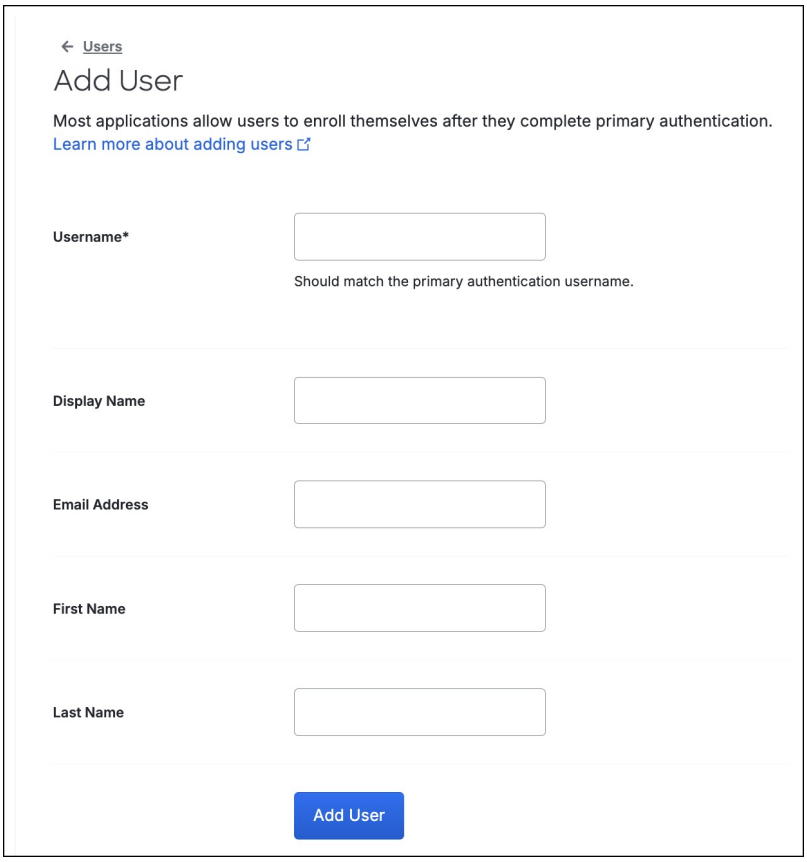
Duo でのユーザーの作成

Duo Admin Panel から Duo ユーザーアカウントを作成する必要があります。これらのユーザーアカウントを使用すると、エンドユーザーは、二要素認証を使用して Duo で保護されたサービスおよびアプリケーションにログインできます。

手順

ステップ 1 Duo Admin Panel から、[ユーザー] > [ユーザー] を選択します。

ステップ 2 [ユーザーの追加] をクリックします。



ステップ 3 [ユーザー名] フィールドに、ユーザー名を入力します。

ステップ 4 [表示名] フィールドに、ユーザーの表示名を入力します。

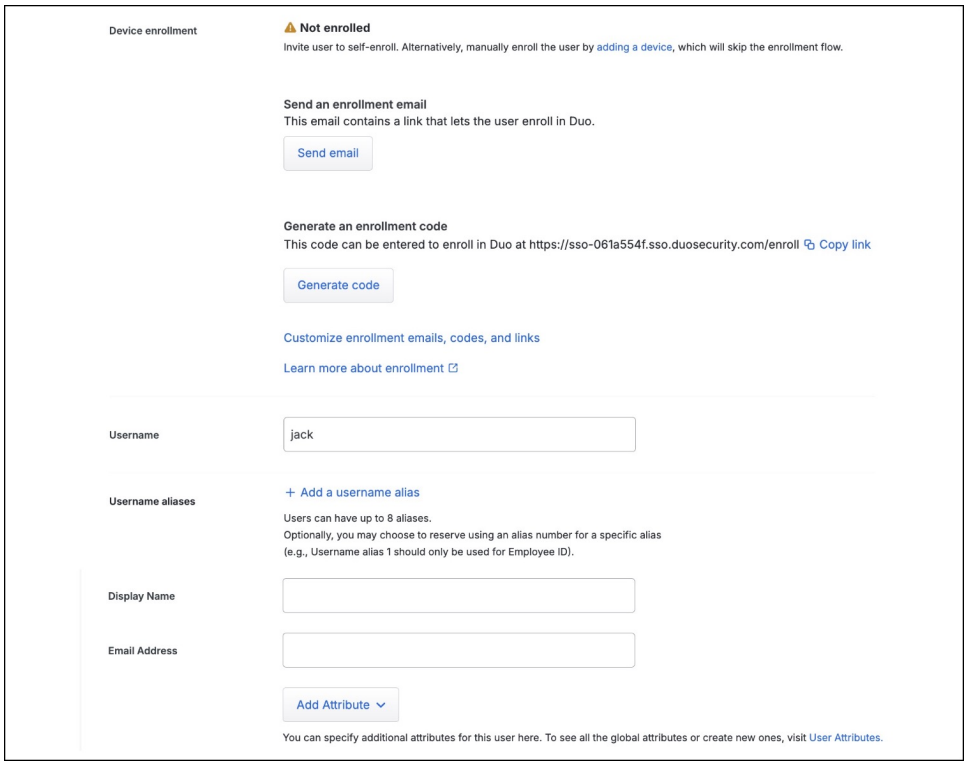
ステップ 5 [電子メール] フィールドに、ユーザーの電子メールアドレスを入力します。

ステップ 6 [ユーザーの追加] をクリックします。

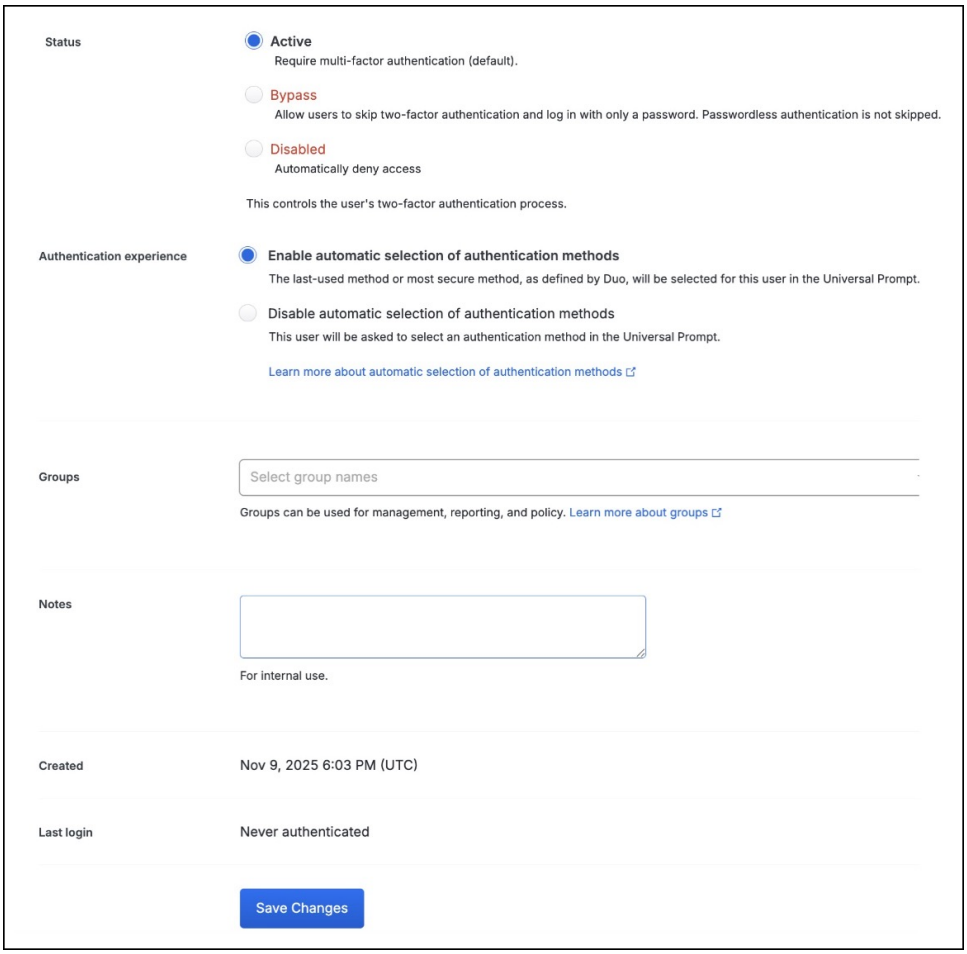
ユーザーが作成され、そのユーザーの編集モードが開始されます。

ステップ 7 [デバイスの登録] で、[電子メールの送信] をクリックします。

このメールには、ユーザーを Duo に登録するためのリンクが含まれています。



ステップ 8 [ステータス] で、[アクティブ] オプションボタンをクリックして、ユーザーに多要素認証（MFA）を要求します。



ステップ 9 [変更の保存] をクリックします。

ユーザーは Duo Security から Duo のユーザーアカウントを設定するための電子メールを受信します。ユーザーは電子メール内のリンクをクリックしてアカウントを作成する必要があります。

Duo でのグループの作成

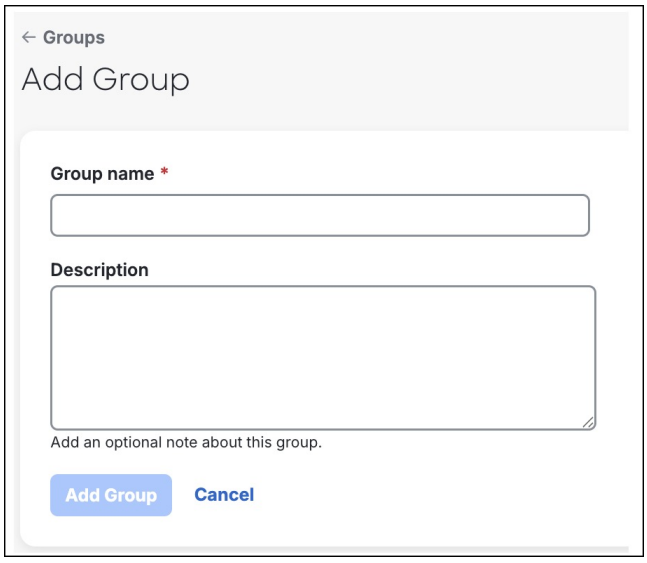
Duo では、グループを使用してユーザーを組織化して管理できます。

この例では、グループを作成して Firewall Management Center アプリケーションに関連付け、グループのメンバーであるユーザーのみが Firewall Management Center で認証を受けられるように設定します。

手順

ステップ 1 Duo Admin Panel から、[ユーザー] > [グループ] を選択します。

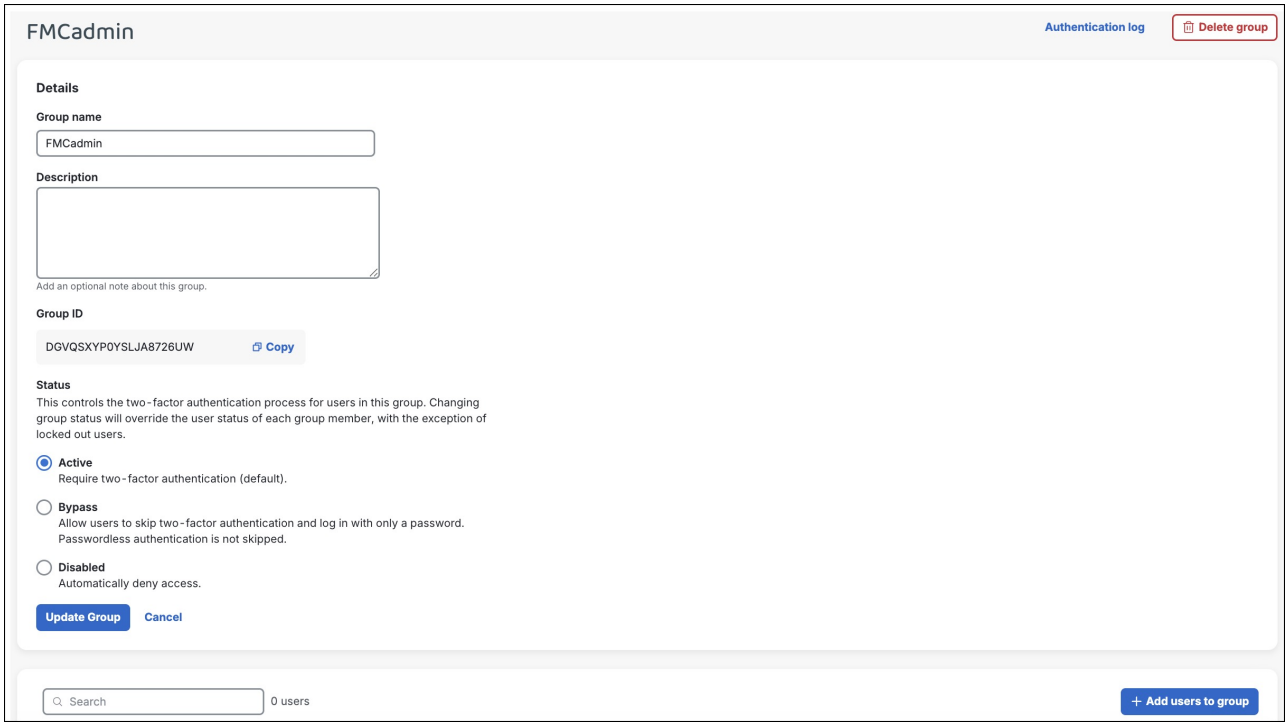
ステップ 2 [+グループの追加] をクリックします。



ステップ 3 [グループ名] フィールドにグループ名を入力します。

ステップ 4 [グループの追加] をクリックします。

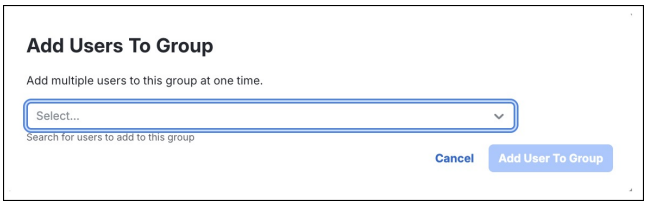
グループが作成され、グループの編集モードが開始されます。



ステップ 5 [ステータス] で [アクティブ] をクリックすると、グループ内のすべてのユーザーに二要素認証が要求されます。

ステップ 6 [+グループにユーザーを追加] をクリックします。

ステップ 7 [ユーザーをグループに追加] ダイアログボックスで、ドロップダウンリストから 1 人以上のユーザーを選択します。



ステップ 8 [ユーザーをグループに追加] をクリックします。

グループは [グループ] ページに一覧表示されます。この例のグループは以下のとおりです。

- FMCadmin
- FMCmaintenance
- FMCreadonly

ポリシーの作成

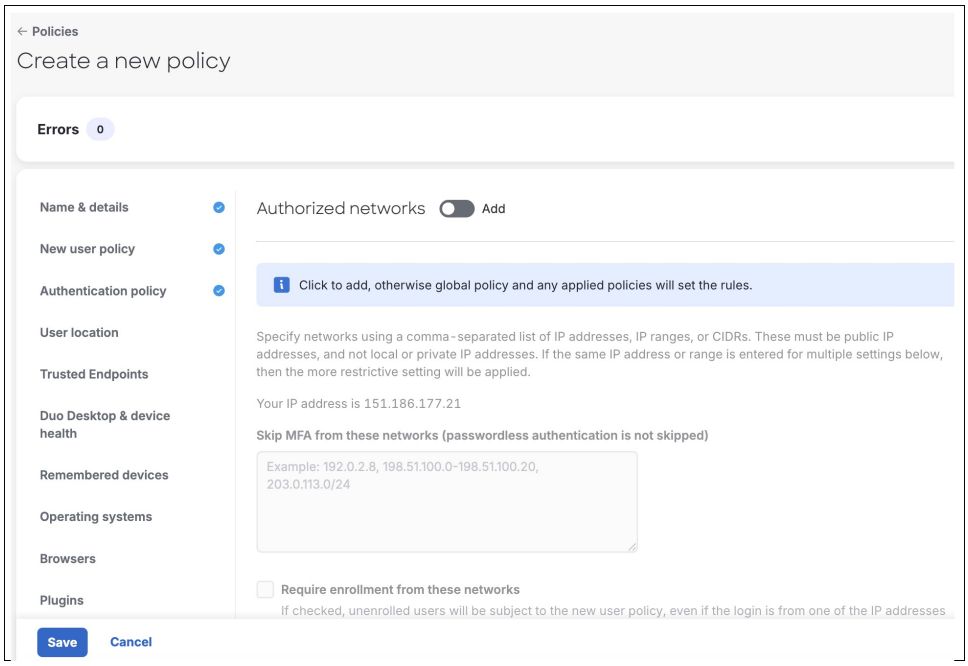
ポリシーを作成してグループに割り当てることで、ユーザーの認証方法を制御できます。

手順

ステップ 1 Duo Admin Panel から、[ポリシー] > [ポリシー] の順に選択します。

ステップ 2 [+ポリシーを追加] をクリックします。

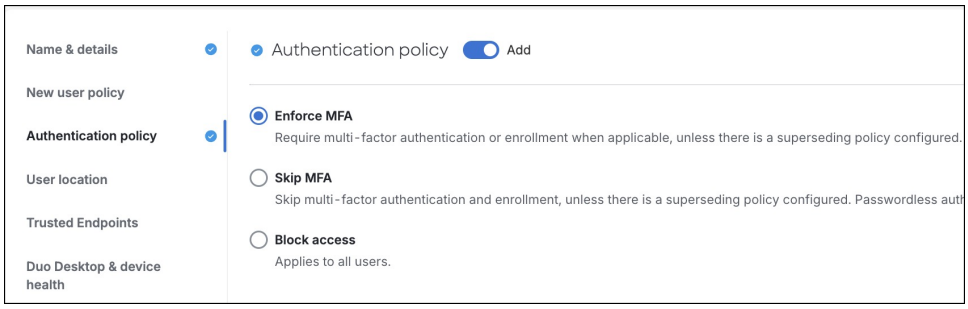
[新しいポリシーの作成] ダイアログボックスが表示され、左側のペインにはルールが表示されます。



ステップ 3 左側のペインから必要なルールを選択します。これらのルールに対応するパラメータが右側のペインに表示されます。

ステップ 4 会社のユーザー認証要件を有効にするルールを設定します。

[MFAの適用] を選択した場合、この例の [認証ポリシー] では、すべてのユーザーが MFA を使用する必要があります。



ステップ 5 [保存] をクリックします。

Duo での Firewall Management Center アプリケーションの作成

Firewall Management Center の SAML SSO を有効にするには、Duo で Firewall Management Center アプリケーションを作成します。

手順

ステップ 1 Duo Admin Panel から、[アプリケーション] > [アプリケーション] を選択します。

ステップ 2 [+アプリケーションの追加] をクリックします。

ステップ 3 検索バーで [アプリケーションカタログの汎用SAMLサービスプロバイダー] を検索します。

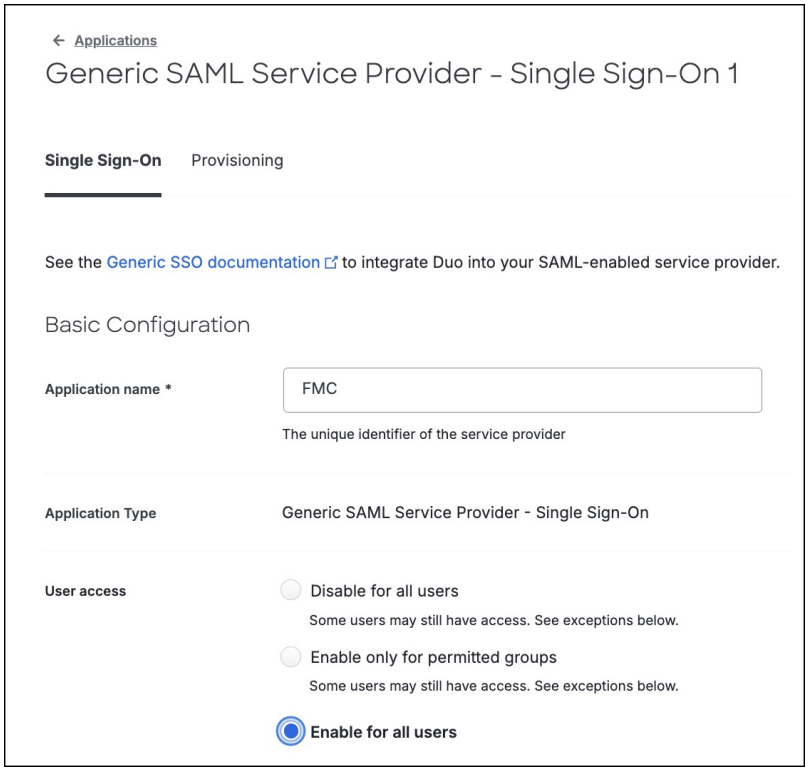
ステップ 4 **[+ 追加]** をクリックします。

ステップ 5 [シングルサインオン] タブをクリックします。

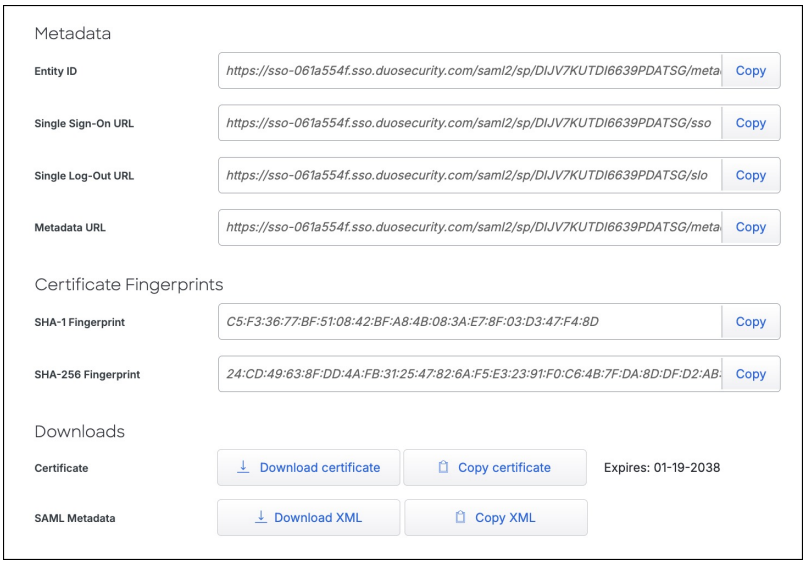
ステップ 6 [アプリケーション名] フィールドに、アプリケーションの名前を入力します。

ステップ 7 [ユーザーアクセス] で、[すべてのユーザーに対して有効化] または [許可されたグループに対してのみ有効化] オプションボタンをクリックします。

（注）
デフォルトでは、すべてのユーザーが無効になっています。許可されたグループまたはすべてのユーザーを有効にしたことを確認します。



ステップ 8 [メタデータ] では、[エンティティID]、[シングルサインオンURL]、および [メタデータURL] フィールドは自動的に入力されます。

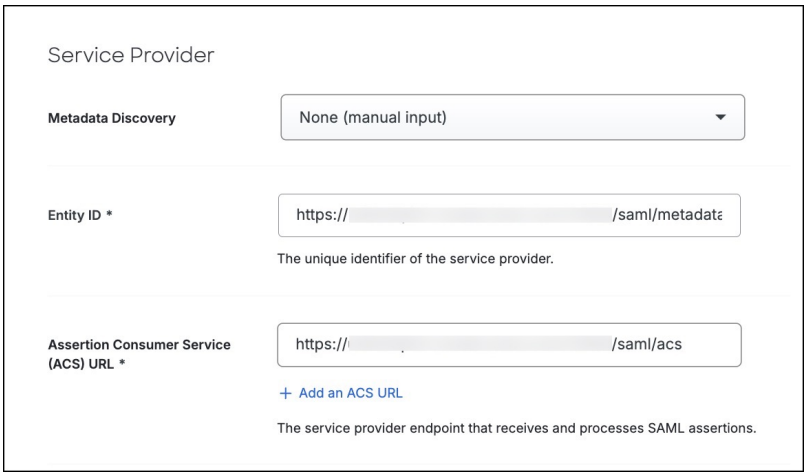


ステップ 9 このメタデータ情報をダウンロードするには、[XMLのダウンロード] をクリックします。

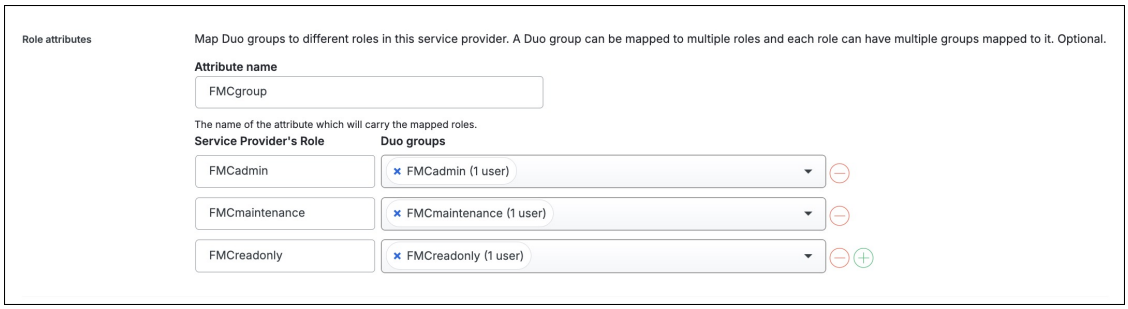
Duo SSO に向けた Firewall Management Center の設定 （13 ページ）のステップ 5 で Duo メタデータを設定するには、この XML をアップロードする必要があります。

ステップ 10 [エンティティID] フィールドに、Firewall Management Center の FQDN または IP アドレスを入力し、文字列 `/saml/metadata` を追加します（たとえば https://*xxxxxxxxx-xxxxxxx.xxxxx*.com/saml/metadata）。

ステップ 11 [Assertion Consumer Service (ACS) URL] フィールドに、Firewall Management Center の FQDN または IP アドレスを入力し、文字列 `/saml/acs` を追加します（たとえばhttps://*xxxxxxxxx-xxxxxxx.xxxxx*.com/saml/acs）。



ステップ 12 [ロール属性] を設定します。



a) [属性名] フィールドに属性名を入力します。

この例では、[属性名] は [FMCgroup] です。Firewall Management Center では、この値を [グループメンバーの属性] の値として使用する必要があります（Duo SSO に向けた Firewall Management Center の設定 （13 ページ）のステップ 10）。

b) [サービスプロバイダーのロール] フィールドに Firewall Management Center ロールを入力します。

この例で設定されているロールは、[FMCadmin]、[FMCmaintenance]、および [FMCreadonly] です。

c) [Duoグループ] ドロップダウンリストから、Firewall Management Center ロールに対応する Duo グループを選択します。

ステップ 13 [ポリシー] で、[ユーザーのグループにポリシーを適用] をクリックします。

ステップ 14 [保存] をクリックします。

Duo SSO に向けた Firewall Management Center の設定

Firewall Management Center で SSO を有効にし、SSO パラメータとユーザーロールマッピングを設定します。

始める前に

Duo Admin Panel で Firewall Management Center サービス プロバイダー アプリケーションを作成します。詳細については、「Duo での Firewall Management Center アプリケーションの作成 （10 ページ）」を参照してください。

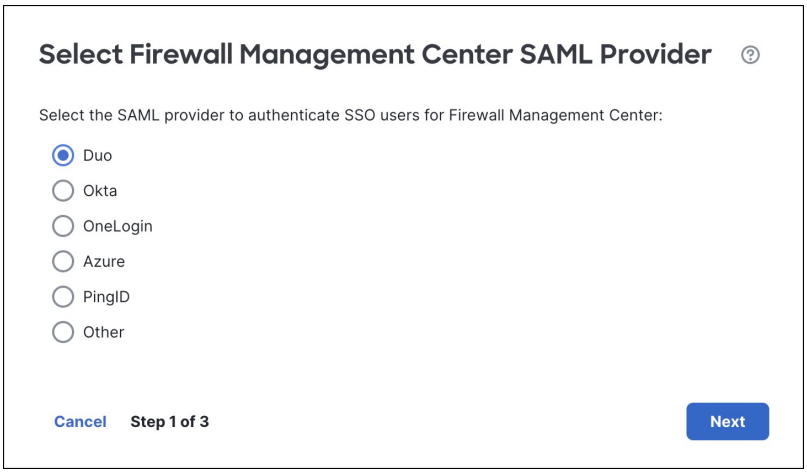
手順

ステップ 1 Firewall Management Center から [管理（Administration）] > [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）] トグルボタンをクリックして、SSO を有効にします。

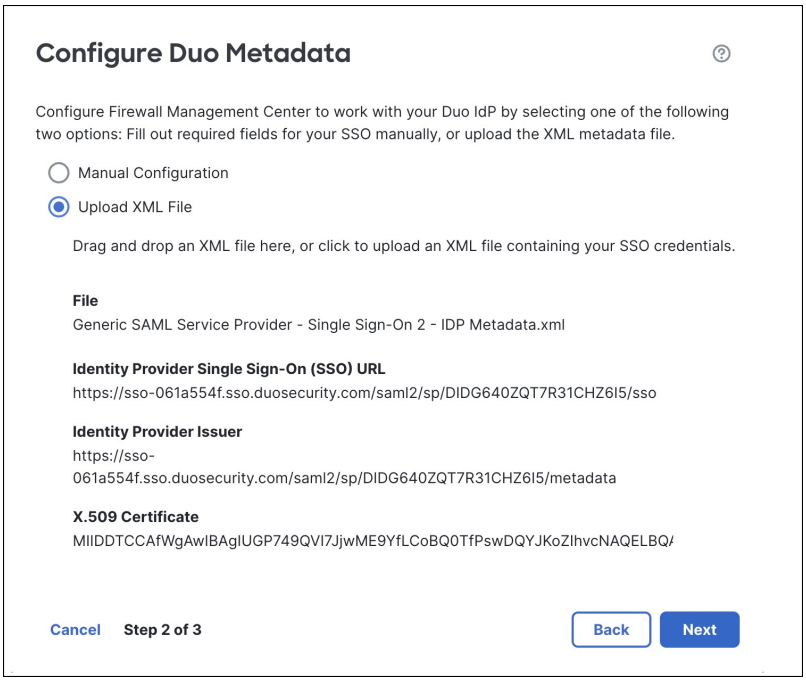
ステップ 3 [SSOの設定（Configure SSO）] をクリックします。

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、[Duo] オプションボタンをクリックして、[次へ（Next）] をクリックします。



ステップ 5 [Duoメタデータの設定（Configure Duo Metadata）] ダイアログボックスで、[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て、Duo のメタデータファイルをアップロードします。

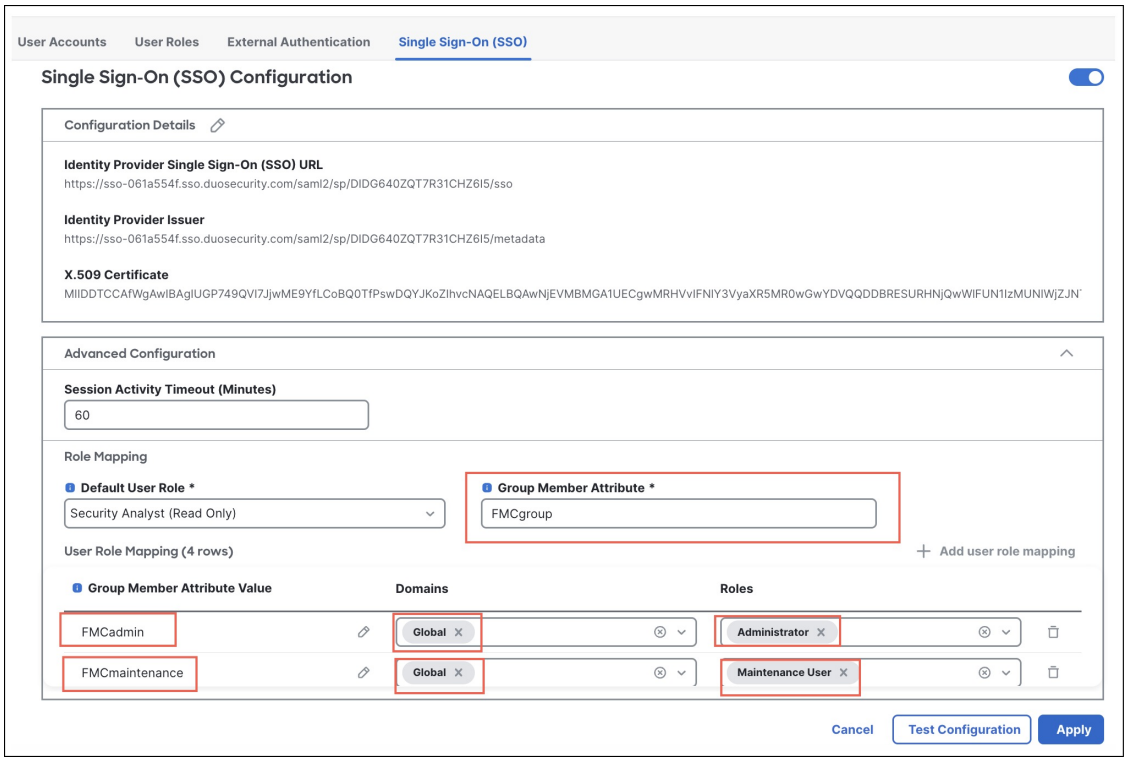
この XML ファイルは、Duo での Firewall Management Center アプリケーションの作成 （10 ページ）のステップ 9 で Duo からダウンロードしたメタデータ XML ファイルです。XML ファイルをアップロードすると、[Duoメタデータの設定（Configure Duo Metadata）] ダイアログボックスにメタデータが自動入力されます。



ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 Duo メタデータを確認し、[保存（Save）] をクリックします。

ステップ 8 [詳細設定（Advanced Configuration）] を展開します。



ステップ 9 [デフォルトのユーザーロール（Default User Role）] ドロップダウンリストから、他のロールが設定されていない場合に割り当てられるデフォルトの Firewall Management Center ユーザーロールを選択します。

ステップ 10 [グループメンバーの属性（Group Member Attribute）] フィールドに、ユーザーまたはグループの Firewall Management Center ロールマッピング用に Duo で設定された [属性名（Attribute name）] を入力します（Duo での Firewall Management Center アプリケーションの作成 （10 ページ）のステップ 12a）。

この例では、グループメンバーの属性は [FMCgroup] です。

ステップ 11 1 つ以上のユーザーロールマッピングを設定し、それらを 1 つ以上のドメインに関連付けます。

a) [グループメンバーの属性値（Group Member Attribute Value）] で、編集アイコンをクリックし、Duo で定義されている属性値と一致する文字列または正規表現として属性値を入力します。

b) [+ユーザーロールマッピングの追加（+ Add user role mapping）] をクリックして、新しいグループを作成します。

この例では、グループメンバーの属性値は [FMCadmin]、[FMCmaintenance]、および [FMCreadonly] です。

c) [ドメイン（Domain）] ドロップダウンリストで、1 つ以上のドメインを選択します。

この例では、すべてのグループメンバー属性値のドメインは [Global] です。

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

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

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

この例では、[FMCadmin]、[FMCmaintenance]、[FMCreadonly] のグループメンバー属性値に割り当てられるロールは、それぞれ [管理者（Administrator）]、[メンテナンスユーザー（Maintenance User）]、[セキュリティアナリスト（Security Analyst）] です。

e) （任意）[ユーザーロールマッピングの追加（Add User Role Mapping）] をクリックして、ユーザーロールマッピングをさらに追加します。

f) [Test Configuration] をクリックします。

（注）
システムにエラーメッセージが表示された場合は、Firewall Management Center の SSO 設定と Duo アプリケーション設定を確認してください。エラーを修正してから再試行します。エラーが解消されない場合は、Cisco Technical Assistance Center に連絡してください。

g) 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。

Duo を使用した Firewall Management Center での SAML SSO の検証

SSO を使用して Firewall Management Center にログインします。

1. Firewall Management Center Web インターフェイスのログインページで、[シングルサインオン（SSO）（Single Sign-On (SSO)）] リンクをクリックします。

2. Duo Security に二要素認証用の電子メールアドレスを入力します。
3. [次へ] をクリックすると、モバイルデバイスの Duo モバイルアプリケーションにプッシュ構成が表示されます。
4. 二要素認証の後、Firewall Management Center Web インターフェイスにログインします。

Firewall Management Center のロールとドメインは、Duo のユーザーロールマッピングによって異なります。各 Firewall Management Center ロールは、Duo 内のグループにマッピングされています。

Firewall Management Center でのユーザーの表示

管理者は、SSO を使用して Firewall Management Center にログインしたユーザーを確認できます。

1. Firewall Management Center Web インターフェイスに管理者ログイン情報でログインします。
2. [管理（Administration）] > [ユーザー（Users）] > [ユーザーアカウント（User Accounts）] を選択します。

Firewall Management Center の監査ログを表示してユーザーアクティビティをモニターする

Firewall Management Center は、ユーザーアクティビティに関する監査情報を監査ログとしてログに記録します。これらのログを表示するには、[イベントとログ（Events & Logs）] > [分析（Analysis）]、[監査ログ（Audit Logs）] の順に選択します。

Firewall Management Center での SAML SSO のトラブルシュート

- **症状**：ユーザーが Firewall Management Center にログインできません。

  解決策：Firewall Management Center と Duo の間の接続を確認します。

- **症状**：ユーザーが Firewall Management Center の正しいドメインにログインできません。

  解決策：Firewall Management Center と Duo のユーザーロールマッピングを確認します。

- **症状**：Firewall Management Center [シングルサインオン（SSO）（Single Sign-On (SSO)）] ページにサーバーエラーメッセージが表示されます。

  解決策：Firewall Management Center と Duo の間の接続を確認します。問題が解決しない場合は、Cisco TACに連絡してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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。