Cisco Secure Firewall Management Center を使用したリモートワーカーの Duo Single Sign-On 認証の設定

初版：2023 年 12 月 13 日

最終更新：2024 年 5 月 15 日

Cisco Secure Firewall Management Center を使用したリモートワーカーの Duo Single Sign-On の設定

Duo Single Sign-On について

Duo Single Sign-On（SSO）により、組織内のすべての重要なアプリケーションに簡単にアクセスでき、一貫したログインエクスペリエンスが得られます。Duo SSO を有効にすることで、複数のパスワードを覚える必要がなくなるため、ログイン情報の漏洩に関連するリスクが軽減され、パスワードレスの未来に向け大きく前進できます。

このガイドでは、クラウドホスト型の Duo SSO ソリューションを使用した、ローカルの Active Directory または SAML ID プロバイダーにおける、ユーザーの既存のログイン情報を使ったリモートアクセス VPN トンネルの保護手順を説明します。このガイドで説明する設定例では、認証ソースとして Microsoft Entra ID（旧称 Azure Active Directory）を使用します。

このガイドの対象読者

このガイドは、Secure Firewall Management Center を使用して組織内のリモートワーカー向けに Duo SSO ソリューションを統合するネットワーク管理者向けです。このユースケースを通じて、Microsoft Entra ID をプライマリ ID プロバイダーとして使用する Duo SSO 認証の設定手順を説明します。

シナリオ

大規模な組織の IT 管理者である Kit は、組織の IT インフラストラクチャの管理とセキュリティの確保を担当しています。Kit は、従業員が複数のユーザー名とパスワードを使用してさまざまなアプリケーションにアクセスしている状況を認識しており、脆弱なパスワードを使用したり、パスワードを再利用したりしている可能性があると考えています。サイバーセキュリティ

への脅威がエスカレートしていることから、Kitは組織のセキュリティ態勢を強化し、ITサポート業務を合理化したいと考えています。

リスクがあるもの

組織内のさまざまなアプリケーションにアクセスするためには複数のパスワードを覚える必要があることから、従業員が脆弱なパスワードを使用したり、パスワードを再利用したりすることで、悪意のある攻撃者による不正アクセスにつながりやすくなります。何度も認証を要求されると、ユーザー体験が低下し、従業員に不満を感じさせる恐れがあります。

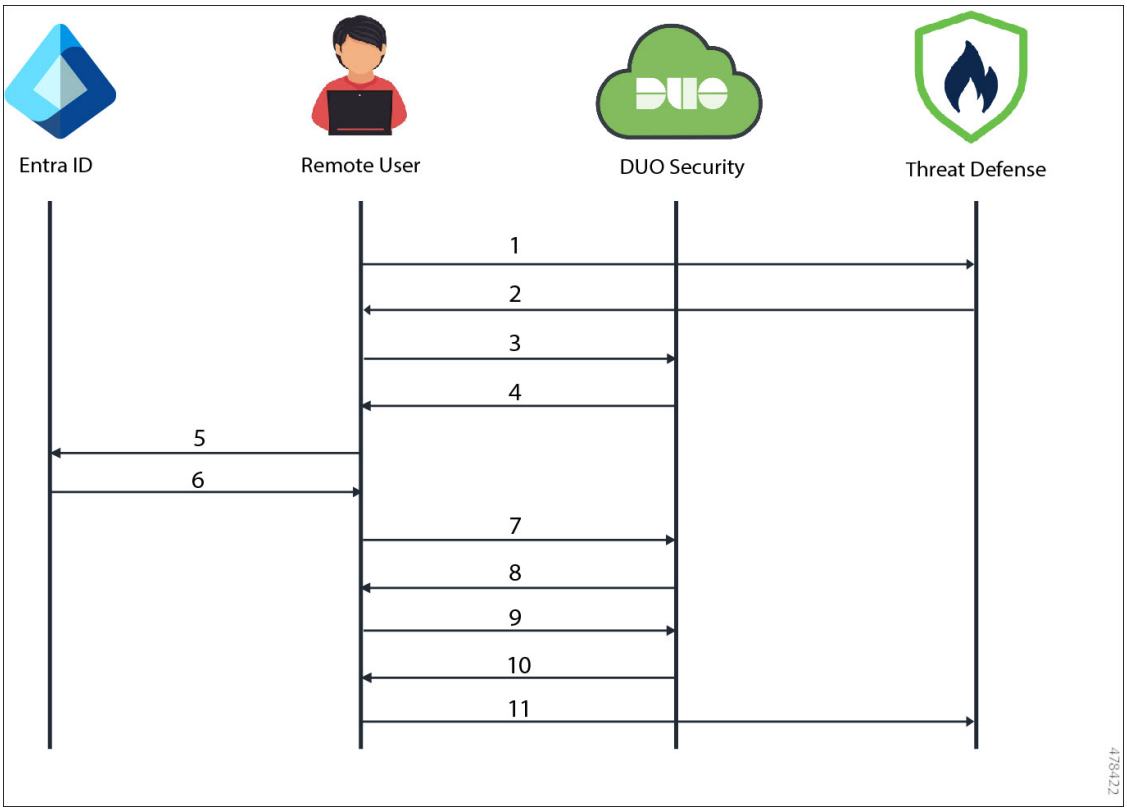
Duo SSO はこの問題をどう解決するのか

- セキュリティの向上：Duo SSOは、ユーザーが覚えておく必要があるパスワードの数を減らすことで、セキュリティを向上させられます。パスワードの数が少なくなると、脆弱なパスワードやパスワードの再利用など、パスワードに関連するセキュリティ侵害の可能性も下がります。
- シームレスなログイン体験：Duo SSOによって、ユーザーのログインプロセスがシンプルになります。一度認証すれば、複数のアプリケーションやサービスにアクセスできるので、アプリケーションやサービスごとにログイン情報を再入力する必要はありません。
- IT ヘルプデスクの業務負担の軽減：パスワード関連のトラブルが減ることで、IT ヘルプデスクチームの負担が減り、他のビジネスイニシアチブに力を入れられるようになります。

Duo Single-Sign-On の仕組み

次の図は、リモートユーザーによる Duo SSO を使ったリモートアクセス VPN へのアクセス認証時に発生するワークフローを示しています。

図 *1 : Duo SSO* 認証ワークフロー



ワークフロー

1. リモートユーザーが セキュアクライアント を使って、Threat Defense デバイスへのリモートアクセス VPN 接続要求を開始します。
2. Threat Defense デバイスが SAML 要求メッセージにより、ユーザーのブラウザを Duo SSO にリダイレクトします。
3. ユーザーのブラウザが Duo SSO にリダイレクトされます。
4. Duo SSO が SAML 要求メッセージにより、ユーザーのブラウザを Entra ID にリダイレクトします。
5. ユーザーのブラウザが Entra ID SSO ログインページにリダイレクトされます。
6. ユーザーがプライマリログイン情報を使用してログインします。Entra ID が SAML アサーションを生成し、この SAML アサーションによりユーザーのブラウザを Duo SSO にリダイレクトします。

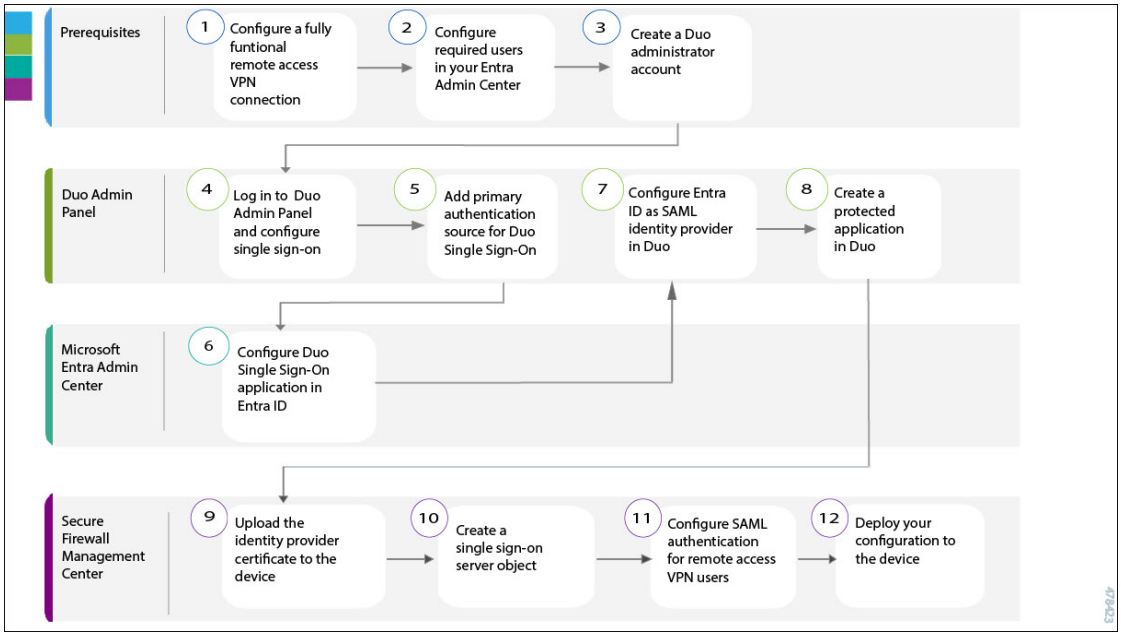
   SAML アサーションは、SAML ID プロバイダーと SAML サービスプロバイダー間で交換されるメッセージであり、リモートユーザーとリモートユーザーに許可されているアクセス先を秘密裏に識別します。SAML アサーションは、セキュリティ条件とアサーションの有効性のアシュアランスも指定します。

7. ユーザーのブラウザが Duo SSO にリダイレクトされます。
8. Duo が Duo 二要素認証を使用して認証するようにユーザーに要求します。
9. ユーザーが Duo 二要素認証を完了します。
10. Duo SSO が SAML 応答メッセージにより、ユーザーのブラウザを Threat Defense にリダイレクトします。
11. ユーザーのブラウザが SAML 応答により Threat Defense デバイスにリダイレクトされ、リモートアクセス VPN 認証が完了します。

エンドツーエンドの Duo Single Sign-On 設定手順

次のフローチャートは、リモートワーカーの Duo SSO 設定ワークフローをエンドツーエンドで示しています。

図 *2:* エンドツーエンドのワークフロー：***Duo SSO*** の設定



ステップ	アプリケーション	説明
1	前提条件	完全に機能するリモートアクセスVPN接続を設定します。「Duo Single Sign-On を設定するにあたっての要件」を参照してください。
2	前提条件	Entra 管理センターで必要なユーザーを設定します。「Duo Single Sign-On を設定するにあたっての要件」を参照してください。

ステップ	アプリケーション	説明
3	前提条件	Duo 管理者アカウントを作成します。「Duo Single Sign-On を設定するにあたっての要件」を参照してください。
4	Duo Admin Panel	Duo Admin Panel にログインし、シングルサインオンを設定します。「Duo Single Sign-On および認証ソースの設定（6 ページ）」を参照してください。
5	Duo Admin Panel	Duo SSO のプライマリ認証ソースを追加します。「Duo Single Sign-On および認証ソースの設定 （6 ページ）」を参照してください。
6	Microsoft Entra 管理センター	Entra ID での Duo Single Sign-On アプリケーションの設定（7 ページ）。
7	Duo Admin Panel	Duo で Entra ID を ID プロバイダーとして設定する （9 ページ）。
8	Duo Admin Panel	Duo で保護されたアプリケーションを作成する （11 ページ）。
9	Secure Firewall Management Center	Threat Defense デバイスへの ID プロバイダー証明書のアップロード （12 ページ）。
10	Secure Firewall Management Center	シングルサインオン サーバー オブジェクトの作成 （12 ページ）。
11	Secure Firewall Management Center	リモートアクセス VPN ユーザーの SAML 認証の設定 （14 ページ）。
12	Secure Firewall Management Center	Threat Defense デバイスへの設定の展開 （14 ページ）。

Duo Single Sign-On を設定するにあたっての要件

このガイドで説明する Duo SSO の設定を開始する前に、あらかじめ次の要件が満たされていることを確認してください。

- 必要なユーザー設定を済ませた有効な Entra ID サブスクリプション。Entra ID の使用開始にあたっての詳しい情報は、Microsoft Entra ID のドキュメントを参照してください。
- ロールが [所有者（Owner）] である Duo 管理者アカウント。詳細については、『Getting Started with Duo Security』を参照してください。
- Management Center によって管理される Threat Defense デバイス上の完全に機能するリモートアクセス VPN 設定。

- Secure Firewall Management Center バージョン 7.0.0 以降。
- 管理対象デバイスの Secure Firewall Threat Defense バージョン 6.7.0 以降。
- セキュアクライアント バージョン 4.6 以降。

システム要件

- Secure Firewall Management Center バージョン 7.0.0 以降。
- 管理対象デバイスの Secure Firewall Threat Defense バージョン 6.7.0 以降。
- セキュアクライアント バージョン 4.6 以降。

Duo Single Sign-On および認証ソースの設定

Duo SSO は、クラウドホスト型 SAML 2.0 ID プロバイダーであり、Entra ID などの既存のユーザーディレクトリを使用して Web アプリケーションへのセキュアなアクセスを可能にします。Duo SSO は、認証ソースとしてローカル Active Directory（AD）および SAML ID プロバイダー（IdP）をサポートします。この設定例では、Microsoft Entra ID をプライマリ認証ソースとして使用します。

Duo SSO と認証ソースの設定の詳細については、Duo のドキュメントを参照してください。

手順

ステップ 1 Duo Admin Panel にログインし、[シングルサインオン（Single Sign-On）] をクリックします。

ステップ 2 （オプション）Duo Single Sign-On を初めて設定する場合は、[シングルサインオン（Single Sign-On）] ページの情報と Duo プライバシーステートメントを確認してください。利用規約に同意し、[アクティブ化して設定を開始（Activate and Start Setup）] をクリックします。

ステップ 3 [SSOサブドメインをカスタマイズする（Customize your SSO subdomain）] ページで、Duo SSO によるログイン時にユーザーに表示するサブドメインを指定します。たとえば、*example* と入力すると、Duo SSO へのログイン時に、URL に *example.login.duosecurity.com* と表示されます。

[保存して続行（Save and Continue）] をクリックしてサブドメインを使用するか、[今はスキップ（Skip for now）] をクリックして後でサブドメインをカスタマイズします。

ステップ 4 [認証ソースの追加（Add Authentication Source）] ページで、[SAML IDプロバイダーの追加（Add SAML Identity Provider）] をクリックします。

SAML ID プロバイダーに提供する必要がある Duo SSO メタデータ情報は、[SAML IDプロバイダーの設定（Configure the SAML Identity Provider）] セクションに表示されます。

Entra ID での Duo Single Sign-On アプリケーションの設定

SAML は、サービスプロバイダーから ID プロバイダーに認証を委任します。この設定では、Duo SSO は、プライマリ認証の SAML ID プロバイダーとして Microsoft Entra ID を使用する SAML サービスプロバイダーとして機能します。詳細については、Duo のドキュメントの「SAML Identity Provider」 セクションに記載されている Entra ID の使用手順を参照してください。

始める前に

あらかじめ必要なユーザー設定を済ませた Microsoft Entra ID アカウントを用意します。

手順

ステップ 1 Microsoft Azure ポータルにログインし、[Microsoft Entra ID] をクリックします。

ステップ 2 左側のペインの [エンタープライズアプリケーション（Enterprise Applications）] をクリックし、[+新しいアプリケーション（+ New Application）] をクリックします。

ステップ 3 [+独自のアプリケーションの作成（+ Create your own application）] をクリックして、Duo SSO 設定用の新しいアプリケーションを作成します。

ステップ 4 アプリケーションを一意に識別する表示名（*Duo SSO* など）を指定します。

ステップ 5 [ギャラリーにない他のアプリケーションを統合する（Integrate any other application you not find in the gallery）] オプションを選択し、[作成（Create）] をクリックします。

ステップ 6 *Duo SSO* アプリケーションの [概要（Overview ）] ページで、[ユーザーとグループ（ Users and groups）] をクリックします。

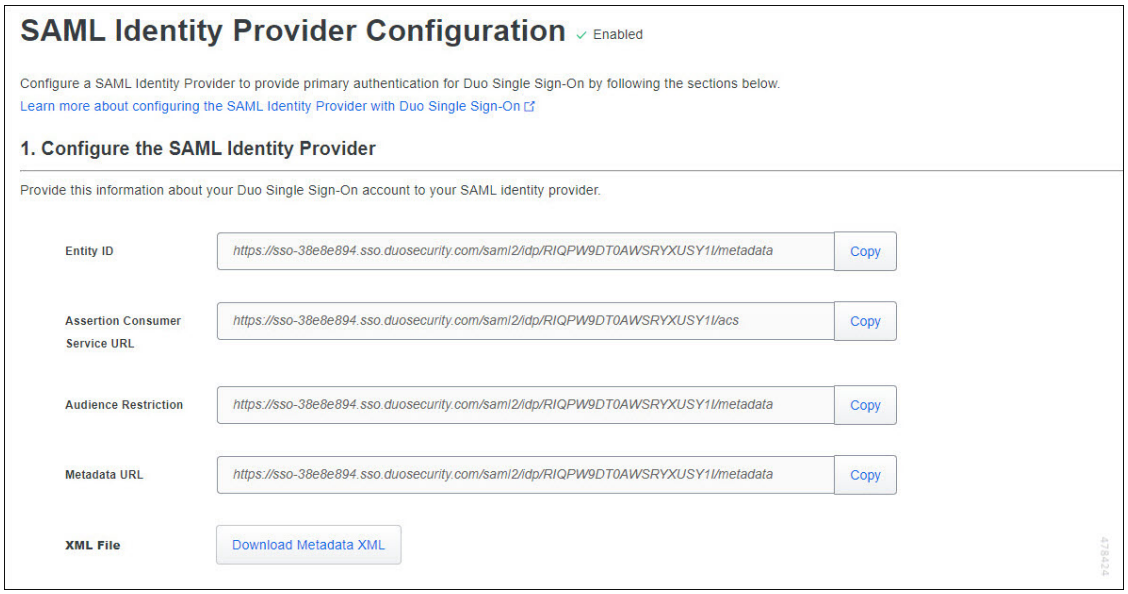
ステップ 7 [+ユーザー/グループの追加（+ Add user/group ）] をクリックし、Entra ID ログイン情報を使って Duo SSO にログインするためのアクセス権を付与するユーザーとグループを選択します。ユーザーとグループを選択したら、ページの下部にある [割り当て（Assign）] をクリックします。

ステップ 8 左側のペインで、[シングルサインオン（Single sign-on）] をクリックし、[シングルサインオン方式の選択（Select a single sign-on method ）] ページで [SAML] をクリックします。

ステップ 9 [SAMLによるシングルサインオンの設定（Set up Single Sign-On with SAML）] ページで、[SAML の基本設定（Basic SAML Configuration）] の横にある [編集（Edit）] をクリックします。

ステップ 10 Duo Admin Panel の [SAML IDプロバイダーの設定（ Configure the SAML Identity Provider ）] セクションから取得できる Duo SSO メタデータ情報を入力します。

図 *3 : Duo SSO* メタデータ



a) Duo Admin Panel から [エンティティID（Entity ID）] をコピーし、Entra 管理センターの [識別子（エンティティID）（Identifier (Entity ID)）] フィールドに貼り付けます。

b) Duo Admin Panel から [Assertion Consumer ServiceのURL（Assertion Consumer Service URL）] をコピーし、Entra 管理センターの [応答URL（Assertion Consumer ServiceのURL）（Reply URL (Assertion Consumer Service URL)）] フィールドに貼り付けます。

c) 他のフィールドはすべて空白のままにして、[保存（Save）] をクリックします。

ステップ 11 [属性と要求（Attributes & Claims）] セクションの横にある [編集（Edit）] をクリックして、Duo への SAML 応答送信時に使用する属性名を設定します。

SAML 応答でこれらの属性名を使用することで、ユーザーがアプリケーションにサインインする際に、Duo により自動的に正しい属性が選択されます。SAML アプリケーションの設定時に、これらの 5 つのブリッジ属性と追加で設定したカスタムブリッジ属性（ある場合）の中からいずれかを選択できます。Duo Admin Panel のアプリケーションの設定ページでブリッジ属性を選択すると、有効な認証ソースの適切な属性に自動的にマッピングされます。

a) [追加の要求（Additional Claims）] に設定されているすべてのデフォルト要求を削除します。

b) [+新しい要求の追加（+ Add new claim）] をクリックし、次のブリッジ属性を使用して、合計 5 つの要求を追加します。

属性名では大文字と小文字が区別されます。

表 *1 : Microsoft Entra ID* 属性名

名前	名前空間	ソース	ソース属性
Email	空白のままにする	属性	user.mail

名前	名前空間	ソース	ソース属性
Username	空白のままにする	属性	user.userprincipalename
FirstName	空白のままにする	属性	user.givenname
LastName	空白のままにする	属性	user.surname
DisplayName	空白のままにする	属性	user.displayname

c) 5 つすべての要求を追加したら、右上にある [閉じる（x）（Close (x)）] アイコンをクリックしてビューを閉じます。

（注） Duo SSO は、Entra ID からシングルサインオン接続をテストするオプションをサポートしていません。

Duo で Entra ID を ID プロバイダーとして設定する

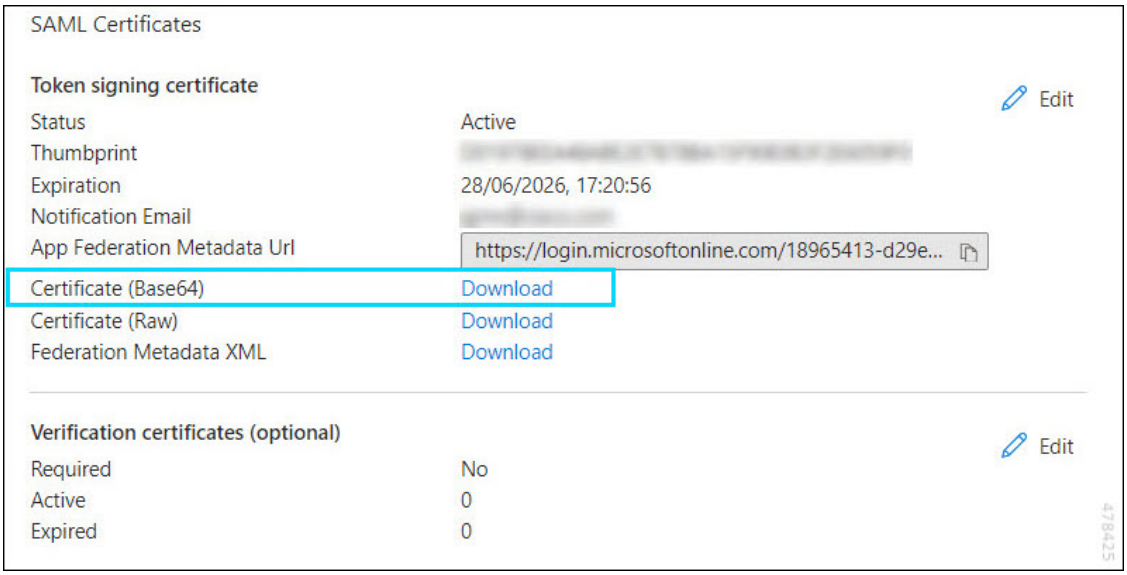
手順

ステップ 1 ユーザーが SAML を使用して Microsoft Entra ID で認証を行うと、Entra ID から Duo にトークンが発行されます。Duo は、ユーザーにユーザー名とパスワードの入力を求める代わりに、このトークンを使用してユーザーをサインインします。Microsoft Entra ID は、一意の証明書を使用してこれらの SAML トークンに署名します。次の手順に従って、Duo によるトークンの復号に使用できる SAML 証明書を Entra ID からダウンロードします。

a) Microsoft Entra 管理センターで、Duo 用に作成したアプリケーション [Duo SSO] を選択し、[シングルサインオン（Single Sign-on）] をクリックします。

b) [SAML証明書（SAML Certificates）] セクションで、[証明書（Base64）（Certificate (Base64)）] の横にある [ダウンロード（Download）] をクリックして SAML 証明書をダウンロードします。

図 *4 : SAML* 証明書のダウンロード



ステップ 2 [Duo SSOの設定（Set up Duo SSO）] から取得できる Entra ID（または指定した名前）のメタデータ情報をコピーします。

図 *5 : Entra ID* メタデータ

ステップ 3 Duo Admin Panel に戻り下にスクロールして、[SAML IDプロバイダーの設定（SAML Identity Provider Configuration）] ページの [Duo Single Sign-Onの設定（Configure Duo Single Sign-On）] セクションを表示します。

ステップ 4 SAML ID プロバイダーを識別する一意の表示名（*Entra ID*など）を指定します。

ステップ 5 Entra ID から [Microsoft Entra ID識別子（Microsoft Entra ID Identifier）] をコピーし、Duo Admin Panel の [識別子（エンティティID）（Identifier (Entity ID)）] フィールドに貼り付けます。

ステップ 6 Entra ID から [ログインURL（Login URL）] をコピーして、Duo Admin Panel の [シングルサインオンURL（Single Sign-On URL）] フィールドに貼り付けます。

ステップ 7 Entra ID からダウンロードした SAML 証明書を Duo Admin Panel の [証明書（Certificate）] セクションにアップロードします。

ステップ 8 [ユーザー名の正規化（Username Normalization）] オプションは [簡易（Simple）] のままにします。ユーザー名の正規化は、プライマリ認証で入力されたユーザー名を Duo ユーザーアカウントとの照合前に変更する必要があるかどうかを決める設定です。

ステップ 9 [保存（Save）] をクリックします。

Duo で保護されたアプリケーションを作成する

Duo の保護されたアプリケーションとは、Duo と Threat Defense リモートアクセス VPN を統合するサービスです。Duo でのアプリケーションの保護と追加のアプリケーションオプションの詳細については、「Protecting Applications」を参照してください。

始める前に

Duo アカウントの Duo SSO を有効にし、「Duo Single Sign-On および認証ソースの設定」の説明に従って、有効な認証ソースを設定します。

手順

ステップ 1 Duo Admin Panel にログインし、[アプリケーション（Applications）] を選択します。

ステップ 2 [アプリケーションの保護（Protect an Application）] をクリックします。

ステップ 3 下にスクロールして、アプリケーションリストから保護タイプが [DuoがホストするSSOによる2FA（シングルサインオン）（2FA with SSO hosted by Duo (Single Sign-On)）] である [Cisco Firepower Threat Defense VPN] を探して、アプリケーションの横にある [保護（Protect）] をクリックします。

図 *6 : Cisco Firepower Threat Defense VPN* アプリケーション

ステップ 4 Cisco Secure Firewall Threat Defense のパブリックに解決可能なホスト名を [Cisco FirepowerベースURL（Cisco Firepower Base URL）] に入力します。

ステップ 5 SSO を設定するリモートアクセス VPN の接続プロファイル名を [接続プロファイル名（Connection Profile Name）] に入力します。

ステップ 6 ページの一番下までスクロールし、[Save] をクリックします。

Threat Defense デバイスへの ID プロバイダー証明書のアップロード

手順

ステップ 1 Duo Admin Panel にログインし、[アプリケーション（Applications）] を選択します。

ステップ 2 Duo で保護されたアプリケーションを作成する （11 ページ）の説明に従って、アプリケーションリストから、設定済みの [Cisco Firepower Threat Defense VPN] アプリケーションを選択します。

ステップ 3 アプリケーションの詳細ページで、[ダウンロード （Downloads）] にある [IDプロバイダー証明書（Identity Provider Certificate）] の横の [証明書のダウンロード（Download certificate）] をクリックします。

ステップ 4 Management Center にログインし、**[デバイス（Devices）]** > **[証明書（Certificates）]**をクリックします。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 Duo SSO を設定する Threat Defense デバイスを選択します。

ステップ 7 [証明書の登録（Cert Enrollment）] の横にある [+] をクリックします。

ステップ 8 証明書の名前（*duo_sso_cert* など）を指定します。

ステップ 9 [登録タイプ（Enrollment Type）] ドロップダウンリストから、[手動（Manual）] を選択します。

ステップ 10 [CAのみ（CA Only）] チェックボックスをオンにします。

ステップ 11 メモ帳などのテキストエディタで先ほどダウンロードした証明書ファイルを開き、BEGIN CERTIFICATE と END CERTIFICATE の行を含むテキストの内容をすべてコピーします。Management Center の [CA証明書（CA Certificate）] フィールドに証明書ファイルのテキストを貼り付けます。

ステップ 12 [CA証明書の基本的な制約のCAフラグチェックをスキップする（Skip Check for CA flag in basic constraints of the CA Certificate）] チェックボックスをオンにし、トラストポイント証明書の基本的な制約の拡張と CA フラグのチェックをスキップします。

ステップ 13 **[Save]** をクリックします。

ステップ 14 [追加（Add）] をクリックします。

シングルサインオン サーバー オブジェクトの作成

始める前に

あらかじめ Duo Admin Panel から次の情報を取得しておきます。

表 *2 : Duo SSO* サーバーメタデータ

メタデータ	説明
ID プロバイダーエンティティ ID	サービスプロバイダーを一意に識別するために SAML IdP で定義される URL。 例： *https://sso-rbdef4.sso.duosecurity.com/saml2/sp/DIABC1367234567/metadata*
SSO URL	SAML ID プロバイダーサーバーにサインインするための URL。 例：*https://sso-rbdef4.sso.duosecurity.com/saml2/sp/DIABC1367234567/sso*
ログアウト URL	このフィールドは任意です。ユーザーが Duo SSO からログアウトすると、このフィールドの URL にリダイレクトされます。
アイデンティティ プロバイダの証明書	IdP によって署名されたメッセージを検証するために Threat Defense に登録される IdP の証明書。

手順

ステップ 1 Management Center で**[オブジェクト（Object）]**>**[オブジェクト管理（Object Management）]**>**[AAAサーバー（AAA Server）]**>**[シングルサインオンサーバー（Single Sign-on Server）]**を選択します。

ステップ 2 [シングルサインオンサーバーの追加（Add Single Sign-on Server）] をクリックします。

ステップ 3 [名前（Name）] フィールドの名前に **Duo SSO** を入力します。

ステップ 4 [Duo Admin Panelメタデータ（Duo Admin Panel Metadata）] セクションから [IDプロバイダーエンティティID（Identity Provider Entity ID）] をコピーし、Management Center の [IDプロバイダーエンティティID（Identity Provider Entity ID）] フィールドに貼り付けます。

ステップ 5 [Duo Admin Panelメタデータ（Duo Admin Panel Metadata）] セクションから SSO URL をコピーし、Management Center の [SSO URL] フィールドに貼り付けます。

ステップ 6 （オプション）[Duo Admin Panelメタデータ（Duo Admin Panel Metadata）] セクションからログアウト URL をコピーし、Management Center の [ログアウトURL（Logout URL）] フィールドに貼り付けます

ステップ 7 Threat Defense のパブリックに解決可能なホスト名を [ベースURL（Base URL）] として指定します。この URL は、ID プロバイダー認証が完了すると、ユーザーを再び Secure Firewall Threat Defense にリダイレクトします。

ステップ 8 [IDプロバイダー証明書（Identity Provider Certificate）] ドロップダウンリストから ID プロバイダー証明書 *duo_sso_cert* を選択します。

ステップ 9 [署名を要求（Request Signature）] の設定は [署名なし（No Signature）] のままにします。

ステップ 10 [ログイン時にIdPの再認証を要求する（Request IdP re-authentication on Login）] チェックボックスをオフにします。

ステップ 11 他のオプションはすべてデフォルト設定のままにして、[保存（Save）] をクリックします。

リモートアクセス VPN ユーザーの SAML 認証の設定

手順

ステップ 1 Management Center で、**[デバイス（Devices）]** > **[リモートアクセス（Remote Access）]**を選択します。

ステップ 2 更新するリモートアクセス VPN の横にある **[編集（Edit）]**（） アイコンをクリックします。

ステップ 3 Duo Single Sign-On を使用する接続プロファイルの横にある **[編集（Edit）]**（） アイコンをクリックします。

ステップ 4 [AAA] タブをクリックします。

ステップ 5 [認証方式（Authentication Method）] ドロップダウンリストから [SAML] を選択します。

ステップ 6 [認証サーバー（Authentication Server）] ドロップダウンリストから Duo Single Sign-On サーバーである [Duo SSO] を選択します。

ステップ 7 [エイリアス（Aliases）] タブをクリックし、この接続プロファイルのエイリアス名を追加して、接続をこの接続プロファイルにマッピングします。Secure Client に表示されるドロップダウンリストにこのエイリアス名が表示されます。

ステップ 8 変更を保存します。

Threat Defense デバイスへの設定の展開

すべての設定が完了したら、管理対象デバイスに設定を展開します。

手順

ステップ 1 Management Center メニューバーで、[展開（Deploy）] をクリックします。

ステップ 2 [高度な展開（Advanced Deploy）] をクリックします。

ステップ 3 設定を展開する Threat Defense デバイスの横にあるチェックボックスをオンにし、[展開（Deploy）] をクリックします。

詳細については、『Cisco Secure Firewall Management Center Device Configuration Guide』の「Configuration Deployment」セクションを参照してください。

設定の確認

手順

ステップ 1 セキュアクライアント を開き、SAML SSO 認証を使用する VPN 接続プロファイルを選択して、[接続（Connect）] をクリックします。

ステップ 2 セキュアクライアント により、プライマリ認証用の Microsoft Entra ID ログインページにリダイレクトされます。ログイン情報を使用してログインします。

ステップ 3 ユーザーログイン情報の検証が正常に完了すると、二要素認証のためにDuoにリダイレクトされます。プロンプトが表示されたら、Duo 二要素認証を完了します。

認証が正常に完了すると、VPN トンネルに接続されます。

Duo Single Sign-On 設定のトラブルシュート

展開後は、次の CLI を使用して、Secure Firewall Threat Defense デバイスの Duo SSO 認証設定に関連する問題に対応します。

⚠

注意 実稼働環境の Threat Defense デバイスで **debug**コマンドを実行する場合は、注意して進めてください。デバイスでさまざまなデバッグレベルを設定できるため、詳細な出力が行われる可能性があります。デフォルトでは、レベル 1 が使用されます。

表 *3 : Duo SSO* の障害対応

障害対応タスク	コマンド
リモートアクセス VPN 関連の情報をデバッグします。	**debug webvpn 255**
リモートアクセス VPN Secure Client 関連の情報をデバッグします。	**debug webvpn anyconnect 255**
リモートアクセス VPN セッション関連の情報をデバッグします。	**debug webvpn session 255**
一般的な IKE 関連のトランザクションをデバッグします。	**debug webvpn request 255**
SAML 認証関連の情報をデバッグします。	**debug aaa authentication**

【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。

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。