

セキュアファイアウォールでのゼロトラストのリモートアクセス展開の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[前提条件となる設定](#)

[一般的な設定](#)

[アプリケーショングループの設定](#)

[アプリケーショングループ1:DuoをIdPとして使用](#)

[アプリケーショングループ2: Microsoft Entra ID \(Azure AD\)をIdPとして使用する](#)

[アプリケーションの設定](#)

[アプリケーション1:FMC Web UIのテスト \(アプリケーショングループ1のメンバー\)](#)

[アプリケーション2:CTB Web UI \(アプリケーショングループ2のメンバー\)](#)

[確認](#)

[モニタ](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、セキュアなファイアウォールでクライアントレスゼロトラストアクセスリモートアクセス(SSL)導入を設定するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることを推奨しています。

- Firepower Management Center (FMC)
- ZTNAの基礎知識
- Security Assertion Markup Language(SAML)に関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Secure Firewallバージョン7.4.1
- Firepower Management Center (FMC) バージョン 7.4.1
- アイデンティティプロバイダー(IdP)としてのDuo
- Microsoft Entra ID (以前のAzure AD) (IdP)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ゼロトラストアクセス機能は、ゼロトラストネットワークアクセス(ZTNA)の原則に基づいています。ZTNAは、暗黙の信頼を排除するゼロトラストセキュリティモデルです。このモデルでは、ユーザと要求のコンテキストを確認し、アクセスが許可された場合にリスクを分析した後に、最小限の特権アクセスを許可します。

ZTNAの現在の要件と制限事項は次のとおりです。

- FMCバージョン7.4.0+ (Firepower 4200シリーズ) で管理されるセキュアファイアウォールバージョン7.4.0+でサポート
- FMCバージョン7.4.1+ (その他のすべてのプラットフォーム) で管理されるセキュアファイアウォールバージョン7.4.1+でサポート
- Webアプリケーション(HTTPS)のみがサポートされます。復号化の除外が必要なシナリオはサポートされていません
- SAML IdPのみをサポート
- リモートアクセスにはパブリックDNS更新が必要です
- IPv6はサポートされていません。NAT66、NAT64、およびNAT46のシナリオはサポートされていません
- この機能は、Snort 3が有効になっている場合にのみ脅威対策で使用できます
- 保護されたWebアプリケーションのすべてのハイパーリンクには、相対パスが必要です
- 仮想ホストまたは内部ロードバランサの背後で実行される保護されたWebアプリケーションは、同じ外部および内部URLを使用する必要があります
- 個々のモードクラスタではサポートされない
- 厳密なHTTPホストヘッダー検証が有効になっているアプリケーションではサポートされません

- アプリケーションサーバが複数のアプリケーションをホストし、TLS Client HelloのServer Name Indication(SNI)ヘッダーに基づいてコンテンツを提供する場合、ゼロトラストアプリケーション設定の外部URLは、その特定のアプリケーションのSNIと一致する必要があります
- ルーテッドモードでのみサポート
- スマートライセンスが必要 (評価モードでは機能しない)

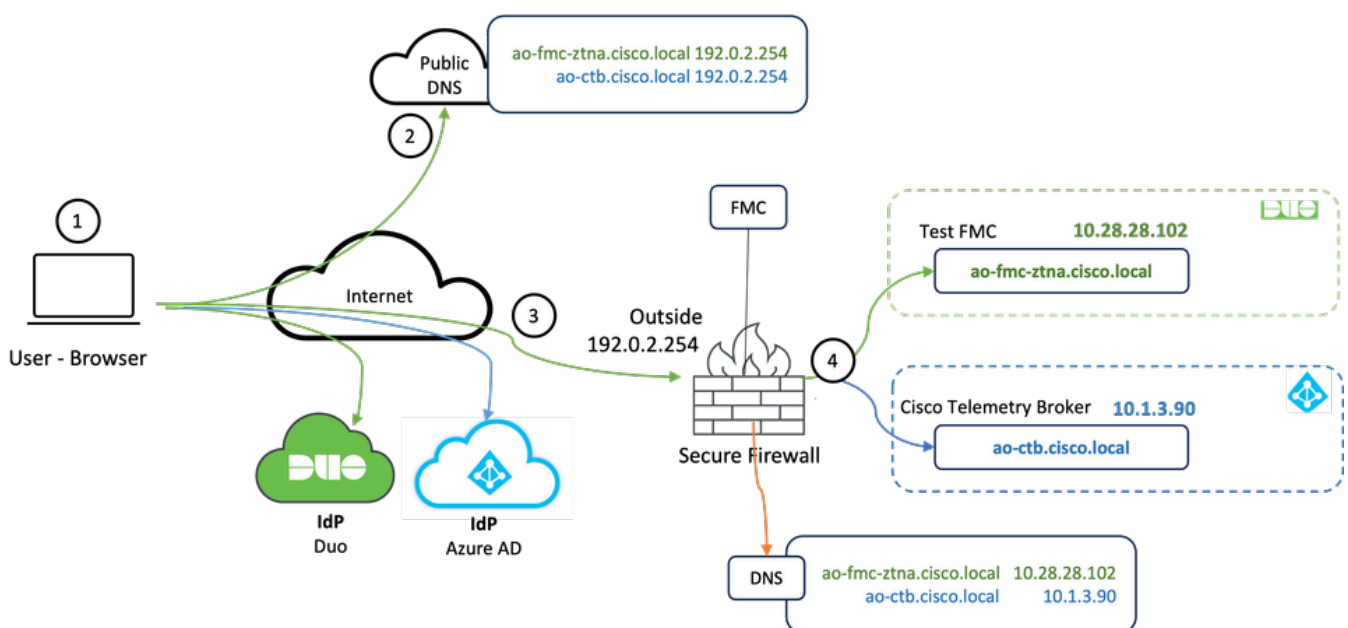
セキュアファイアウォールのゼロトラストアクセスの詳細については、『[Cisco Secure Firewall Management Centerデバイスコンフィギュレーションガイド、7.4](#)』を参照してください。

設定

このドキュメントでは、ZTNAのリモートアクセス導入について説明します。

この例のシナリオでは、リモートユーザは、テストFMCのWebユーザインターフェイス(UI)と、セキュアファイアウォールの背後でホストされているCisco Telemetry Broker(CTB)にアクセスする必要があります。これらのアプリケーションへのアクセスは、次の図に示すように、DuoとMicrosoft Entra IDの2つの異なるIdPによってそれぞれ許可されます。

ネットワーク図



トポロジ ダイアグラム

1. リモートユーザは、セキュアファイアウォールの背後でホストされているアプリケーションにアクセスする必要があります。
2. 各アプリケーションは、パブリックDNSサーバにDNSエントリを持つ必要があります。
3. これらのアプリケーション名は、Secure Firewall OutsideインターフェイスのIPアドレスに解決される必要があります。
4. セキュアファイアウォールは、アプリケーションの実際のIPアドレスに解決し、SAML認証を使用して各アプリケーションに対して各ユーザを認証します。

前提条件となる設定

アイデンティティプロバイダー(IdP)およびドメインネームサーバ(DNS)

- アプリケーションまたはアプリケーショングループは、Duo、Okta、Azure ADなどのSAML Identity Provider(IdP)で構成する必要があります。この例では、DuoおよびMicrosoft Entra IDがIdPとして使用されます。
- IdPsによって生成された証明書とメタデータは、セキュアファイアウォールでアプリケーションを設定するときに使用されます

内部および外部DNSサーバ

- (リモートユーザによって使用される) 外部DNSサーバは、アプリケーションのFQDNエントリを持ち、セキュアファイアウォール外部インターフェイスのIPアドレスに解決される必要があります
- 内部DNSサーバ (セキュアファイアウォールで使用) は、アプリケーションのFQDNエントリを持ち、アプリケーションの実際のIPアドレスに解決される必要があります

証明書

次の証明書は、ZTNAポリシーの設定に必要です。

- ID/プロキシ証明書：アプリケーションをマスカレードするためにセキュアファイアウォールによって使用されます。ここでのセキュアファイアウォールは、SAMLサービスプロバイダー(SP)として機能します。この証明書は、プライベートアプリケーションのFQDN (事前認証段階ですべてのプライベートアプリケーションを表す共通の証明書) に一致するワイルドカードまたはサブジェクトの別名(SAN)証明書である必要があります
- IdP証明書：認証に使用されるIdPは、定義された各アプリケーションまたはアプリケーショングループの証明書を提供します。この証明書は、セキュアファイアウォールが着信SAMLアサーションのIdPの署名を検証できる (アプリケーショングループに対して定義されている場合は、アプリケーションのグループ全体で同じ証明書が使用されます)
- アプリケーション証明書：リモートユーザからアプリケーションへの暗号化されたトラフィックは、セキュアファイアウォールで復号化する必要があります。したがって、各アプリケーションの証明書チェーンと秘密キーをセキュアファイアウォールに追加する必要があります。


一般的な設定

新しいゼロトラストアプリケーションを設定するには、次の手順を実行します。


1. Policies > Access Control > Zero Trust Applicationの順に移動し、Add Policyをクリックします。
2. 次の必須フィールドに入力します。

a) General: ポリシーの名前と説明を入力します。

b) ドメイン名 : これはDNSに追加される名前で、アプリケーションがアクセスされる場所から脅威対策ゲートウェイインターフェイスに解決される必要があります。

 注 : ドメイン名は、アプリケーショングループ内のすべてのプライベートアプリケーションのACS URLを生成するために使用されます。

c) ID証明書 : これは、事前認証段階ですべてのプライベートアプリケーションを表す一般的な証明書です。

 注 : この証明書は、プライベートアプリケーションのFQDNと一致するワイルドカードまたはサブジェクトの別名(SAN)証明書である必要があります。

d) セキュリティゾーン : プライベートアプリケーションを規制する外側または内側のゾーンを選択します。

e) グローバルポートプール : このプールからの一意のポートが各プライベートアプリケーションに割り当てられます。

f) Security Controls (オプション) : プライベートアプリケーションが検査の対象かどうかを選択します。

この設定例では、次の情報が入力されています。

Firewall Management Center
Policies / Access Control / Zero Trust Application

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Return to Zero Trust Application

Add a Zero Trust Application Policy

Zero Trust Application Policy protects private applications with identity based access, intrusion protection, and malware and file inspection.

Cancel Save

General

Name*
ZTNA-TAC

Description

Domain Name

The domain name must resolve to the interfaces that are part of the security zones from which private applications are accessed.

Domain Name*
ztna-tac.com

Ensure that the domain name is added to the DNS. The domain name resolves to the threat defense gateway interface from where the application is accessed.
The domain name is used to generate the ACS URL for all private applications in an Application Group.

Identity Certificate

A common certificate that represents all the private applications at the pre-authentication stage.

Certificate*
ZTNA-Wildcard-cert

This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications.

Security Zones

The access to private applications is regulated through security zones. Choose outside or/and inside zones through which the private applications are regulated.

Security Zones*
Outside

This is the default setting for all private applications. It can be overridden at an Application or Application Group level.

Global Port Pool

Unique port from this pool is assigned to each private application.

Port Range*
20000-22000 Range: (1024-65535)

Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other configurations.

Security Controls (Optional)

Private applications can be subject to inspection using a selected Intrusion or Malware and File policy.

Intrusion Policy
None

Variable Set
None

Malware and File Policy
None

These are default settings for all private applications. It can be overridden at an Application or Application Group level.

この場合に使用されるID/プロキシ証明書は、プライベートアプリケーションのFQDNに一致するワイルドカード証明書です。

Firewall Management Center
Devices / Certificates

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Filter
All Certificates

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
ZTNA-Wildcard-cert	Global	Manual CA & EV	Oct 10, 2025		Available

Identity Certificate

- Status: Available
- Serial Number: 65-17
- Issued By:
 - CN: *
 - DC: *
 - DC: *
- Issued To:
 - CN: *.cisco.local
 - OU: TAC
 - O: Cisco
 - ST: *
 - C: *
- Public Key Type: RSA (2048 bits)
- Signature Algorithm: RSA-SHA384
- Associated Trustpoints: ZTNA-Wildcard-cert
- Valid From: 22:59:42 UTC October 11 2023
- Valid To: 22:59:42 UTC October 10 2025
- CRL Distribution Points:

Close

3.ポリシーを保存します。

4.新しいアプリケーショングループまたは新しいアプリケーションを作成します。

- アプリケーションは、SAML認証、インターフェイスアクセス、侵入ポリシー、マルウェアおよびファイルポリシーを使用するプライベートWebアプリケーションを定義します。
- アプリケーショングループを使用すると、複数のアプリケーションをグループ化し、SAML認証、インターフェイスアクセス、セキュリティ制御設定などの共通の設定を共有できます。

この例では、2つの異なるアプリケーショングループと2つの異なるアプリケーションが設定されています。1つはDuoによって認証されるアプリケーション(test FMC Web UI)用、もう1つはMicrosoft Entra IDによって認証されるアプリケーション(CTB Web UI)用です。

アプリケーショングループの設定

アプリケーショングループ1:DuoをIdPとして使用

- a. アプリケーショングループ名を入力し、SAMLサービスプロバイダー(SP)メタデータが表示されるようにNextをクリックします。

Add Application Group ⓘ ✕

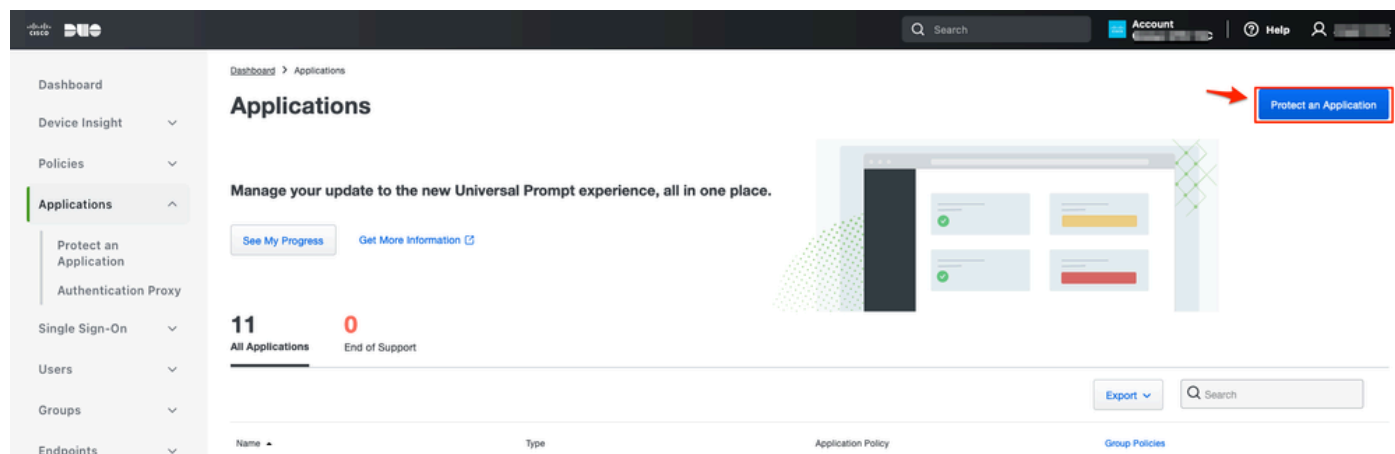
An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- 1 Application Group Edit
Name External_Duo
- 2 **SAML Service Provider (SP) Metadata**
The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.
Entity ID
https://[redacted]/External_Duo/saml/sp/metadata Copy
Assertion Consumer Service (ACS) URL
https://[redacted]/External_Duo/+CSCOE+/saml/sp/acs?tgname= Copy
Download SP Metadata Next
- 3 SAML Identity Provider (IdP) Metadata
- 4 Re-Authentication Interval
- 5 Security Zones and Security Controls

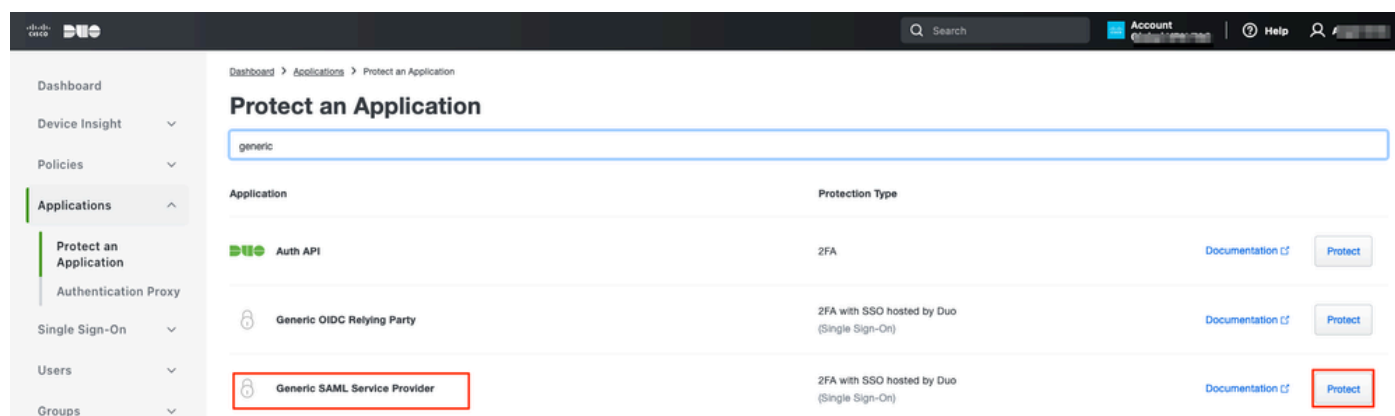
Cancel Finish

b. SAML SPメタデータが表示されたら、IdPに移動し、新しいSAML SSOアプリケーションを設定します。

c. Duoにログインし、Applications > Protect an Applicationの順に選択します。



d. Generic SAML Service Providerを探し、Protectをクリックします。



e. Secure Firewallで設定を続行する必要があるため、IdPから証明書とSAMLメタデータをダウンロードします。

f. ZTNAアプリケーショングループ(ステップaで生成)のエンティティIDとアサーションコンシューマサービス(ACS)URLを入力します。

- Dashboard
- Device Insight
- Policies
- Applications**
- Protect an Application
- Authentication Proxy
- Single Sign-On
- Users
- Groups
- Endpoints
- 2FA Devices
- Administrators
- Trusted Endpoints
- Trust Monitor
- Reports
- Settings
- Billing

You're using the new Admin Panel menu and left-side navigation.

[Provide feedback](#)

[Temporarily switch to the old experience](#)

Generic SAML Service Provider - Single Sign-On 1

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<code>https://sso-.../metadata</code>	Copy
Single Sign-On URL	<code>https://sso-8.../sso</code>	Copy
Single Log-Out URL	<code>https://sso-i.../slo</code>	Copy
Metadata URL	<code>https://sso-8.../metadata</code>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<code>9E:5...5C</code>	Copy
SHA-256 Fingerprint	<code>?:85:...E9:52</code>	Copy

Downloads

Certificate	Download certificate	Expires: 01-19-2038
SAML Metadata	Download XML	

Service Provider

Metadata Discovery: None (manual input)

[Early Access](#)

Entity ID *

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

[+ Add an ACS URL](#)

g. 特定の要件に従ってアプリケーションを編集し、目的のユーザのみにアプリケーションへのアクセスを許可して、Saveをクリックします。

Type Generic SAML Service Provider - Single Sign-On

Name
 Duo Push users will see this when approving transactions.

Self-service portal Let users remove devices, add new devices, and reactivate Duo Mobile
 See [Self-Service Portal documentation](#).
 To allow Duo to notify users about self-service portal activity, select [Settings > Notifications](#)

Username normalization Username normalization for Single-Sign On applications is controlled by the enabled authentication source. Please visit your [authentication source](#) to modify this configuration.
 Controls if a username should be altered before trying to match them with a Duo user account.

Voice greeting
 Specify the message read to users who use phone callback, followed by authentication instructions. Maximum 512 characters.

Notes
 For internal use. Maximum 512 characters.

Administrative unit

Permitted groups Only allow authentication from users in certain groups

 When unchecked, all users can authenticate to this application.

Allowed Hostnames Since this application is using Frameless Duo Universal Prompt, configuring allowed hostnames is no longer supported.
 [Get more information](#)

h. FMCに戻り、IdPからダウンロードしたファイルを使用して、アプリケーショングループに SAML IdPメタデータを追加します。

An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- 1 **Application Group** Edit
Name External_Duo
- 2 **SAML Service Provider (SP) Metadata** Edit
Entity ID https://[redacted]/External_Duo/saml/sp/metadata
Assertion Consumer Service (ACS) URL https://[redacted]/External_Duo/+CSCOE+/saml/sp/acs?tgname=D...

3 **SAML Identity Provider (IdP) Metadata**

Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.

Import IdP Metadata
 Manual Configuration
 Configure Later

Import IdP Metadata

Drag and drop your file here
[or select file](#)
External Applications ZTNA - IDP Metadata.xml

Entity ID*
https://sso-8[redacted] N

Single Sign-On URL*
https://sso-8[redacted] N

IdP Certificate
MIIDDTC[redacted]yDQYJKoZI
[redacted]

Next

Cancel Finish

i. Nextをクリックし、要件に従ってRe-Authentication IntervalとSecurity Controlsを設定します。サマリ設定を確認し、Finishをクリックします。

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group	Name	External_Duo	Edit
2 SAML Service Provider (SP) Metadata	Entity ID	https://[redacted] External_Duo/saml/sp/metadata	Edit
	Assertion Consumer Service (ACS) URL	https://[redacted] External_Duo/+CSCOE+/saml/sp/acs?tgname=D...	
3 SAML Identity Provider (IdP) Metadata	Entity ID	https://ssc [redacted]	Edit
	Single Sign-On URL	https://ssc [redacted]	
	IdP Certificate	External_Duo-1697063490514	
4 Re-Authentication Interval	Timeout Interval	1440 minutes	Edit
5 Security Zones and Security Controls	Security Zones	Inherited: (Outside)	Edit
	Intrusion Policy	Inherited: (None)	
	Variable Set	Inherited: (None)	
	Malware and File Policy	Inherited: (None)	

Cancel

Finish

アプリケーショングループ2: Microsoft Entra ID (Azure AD)をIdPとして使用する

- アプリケーショングループ名を入力し、SAMLサービスプロバイダー(SP)メタデータが表示されるようにNextをクリックします。

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group

Name **Azure_apps**

Edit

2 SAML Service Provider (SP) Metadata

The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.

Entity ID

https://[redacted]/Azure_apps/saml/sp/metadata

Copy

Assertion Consumer Service (ACS) URL

https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=[redacted]

Copy

Download SP Metadata

Next

3 SAML Identity Provider (IdP) Metadata

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

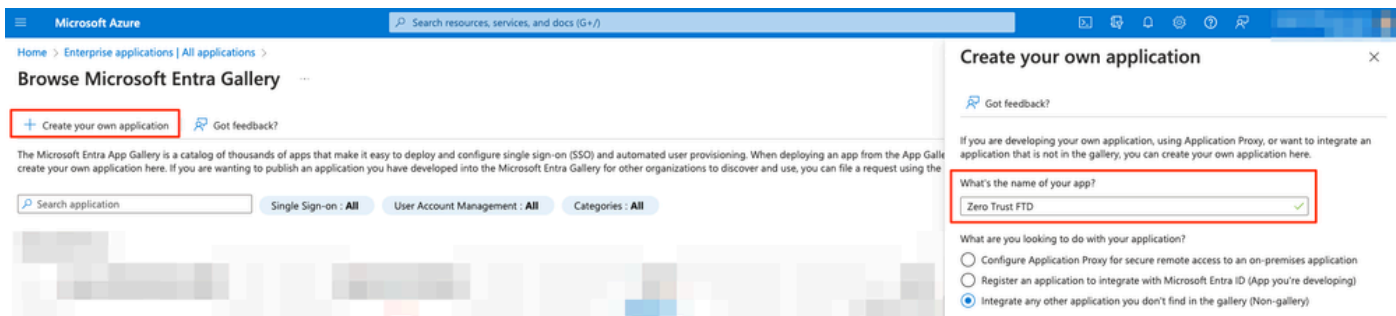
Finish

b. SAML SPメタデータが表示されたら、IdPに移動し、新しいSAML SSOアプリケーションを設定します。

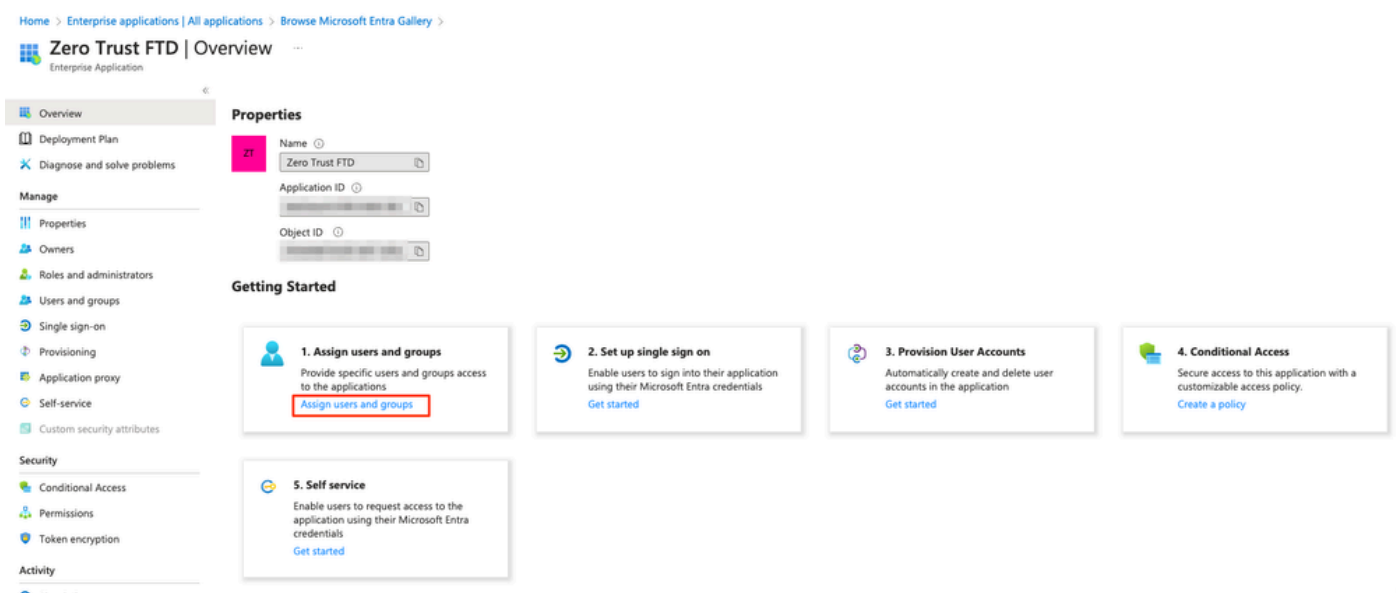
c. Microsoft Azureにログインし、Enterprise applications > New Applicationの順に移動します。

The screenshot shows the Microsoft Azure portal interface for managing Enterprise applications. The breadcrumb navigation is 'Home > Enterprise applications'. The main heading is 'Enterprise applications | All applications'. The left sidebar has a 'Manage' section with 'All applications' highlighted. The main content area includes a '+ New application' button (highlighted with a red box), a search bar, and a table of 77 applications. The table has columns for Name, Object ID, Application ID, Homepage URL, and Created on. The 'Application type' filter is set to 'Enterprise Applications'.

d. Create your own applicationをクリック>アプリケーションの名前を入力> Create



e. アプリケーションを開き、ユーザとグループの割り当てをクリックして、アプリケーションへのアクセスを許可するユーザやグループを定義します。



f. Add user/group > Select the necessary users/groups > Assignの順にクリックします。正しいユーザまたはグループが割り当てられたら、シングルサインオンをクリックします。

Zero Trust FTD | Users and groups

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on

+ Add user/group

Edit assignment Remove Update credentials Columns Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & gro...

Display Name	Object Type
AO Angel	
FG Fernando	

g. シングルサインオンセクションが表示されたら、SAMLをクリックします。

Zero Trust FTD | Single sign-on

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).

Select a single sign-on method [Help me decide](#)

- Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
- Password-based**
Password storage and replay using a web browser extension or mobile app.

h. Upload metadata fileをクリックして、サービスプロバイダー（セキュアファイアウォール）からダウンロードしたXMLファイルを選択するか、ZTNA Application Group(ステップaで生成)から Entity IDとAssertion Consumer Service(ACS)URLを手動で入力します。

注：また、フェデレーションメタデータXMLをダウンロードするか、証明書(Base 64)を個別にダウンロードして、IdP（ログインおよびログアウトURLとMicrosoft Entra Identifier）からSAMLメタデータをコピーしてください。これは、セキュアファイアウォールで設定を続行するために必要です。

Zero Trust FTD | SAML-based Sign-on

Enterprise Application

<< **Upload metadata file** >> Change single sign-on mode | Test this application | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs
 - Provisioning logs
 - Access reviews
- Troubleshooting + Support
 - New support request

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Zero Trust FTD.

- Basic SAML Configuration** Edit

Identifier (Entity ID)	https://[redacted]/Azure_apps/saml/sp/metadata
Reply URL (Assertion Consumer Service URL)	https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=DefaultZeroTrustGroup
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims** Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates**

Token signing certificate Edit	Active
Status	Active
Thumbprint	[redacted]
Expiration	[redacted]
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download
Verification certificates (optional) Edit	
Required	No
Active	0
Expired	0
- Set up Zero Trust FTD**

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://[redacted]
Microsoft Entra Identifier	https://[redacted]
Logout URL	https://[redacted]

i. FMCに戻り、IdPからダウンロードしたメタデータファイルを使用するか、必要なデータを手動で入力して、SAML IdPメタデータをアプリケーショングループ2にインポートします。

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group

Name Azure_apps

Edit

2 SAML Service Provider (SP) Metadata

Entity ID https://[redacted]/Azure_apps/saml/sp/metadata

Assertion Consumer Service (ACS) URL https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=Def...

Edit

3 SAML Identity Provider (IdP) Metadata

Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.

Import IdP Metadata

Manual Configuration

Configure Later

Import IdP Metadata

Drag and drop your file here
or select file

Zero Trust FTD.xml

Entity ID*

https://[redacted]

Single Sign-On URL*

https://[redacted]

IdP Certificate

MIIC8DCCAdigAwIBAgIQdTt7Lwlj7aRGm1m212dU/DANBgkqhkiG9w0B

[redacted]

Next

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

Finish

j. Nextをクリックし、要件に従ってRe-Authentication IntervalとSecurity Controlsを設定します。サマリ設定を確認し、Finishをクリックします。

Add Application Group

An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group	Name	Azure_apps	Edit
2 SAML Service Provider (SP) Metadata	Entity ID	https://[redacted]/Azure_apps/saml/sp/metadata	Edit
	Assertion Consumer Service (ACS) URL	https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=Def...	
3 SAML Identity Provider (IdP) Metadata	Entity ID	https://[redacted]	Edit
	Single Sign-On URL	https://[redacted]	
	IdP Certificate	[redacted]	
4 Re-Authentication Interval	Timeout Interval	1440 minutes	Edit
5 Security Zones and Security Controls	Security Zones	Inherited: (Outside)	Edit
	Intrusion Policy	Inherited: (None)	
	Variable Set	Inherited: (None)	
	Malware and File Policy	Inherited: (None)	

Cancel **Finish**

アプリケーションの設定


アプリケーショングループが作成されたので、Add Applicationをクリックして、保護してリモートでアクセスするアプリケーションを定義します。

1. アプリケーション設定を入力します。

a)アプリケーション名：設定されたアプリケーションの識別子。

b)外部URL:パブリック/外部DNSレコード内のアプリケーションの公開URL。これは、アプリケーションにリモートでアクセスするためにユーザが使用するURLです。

c)アプリケーションURL:アプリケーションの実際のFQDNまたはネットワークIP。これは、アプリケーションに到達するためにセキュアファイアウォールによって使用されるURLです。

 注：デフォルトでは、外部URLはアプリケーションURLとして使用されます。別のアプリケーションURLを指定するには、このチェックボックスをオフにします。

d)アプリケーション証明書：アクセスされるアプリケーションの証明書チェーンおよび秘密キー(FMCホームページ>オブジェクト>オブジェクト管理>PKI>内部証明書から追加)

e) IPv4 NAT送信元 (オプション) : パケットをアプリケーションに転送する前に、リモートユーザからの送信元IPアドレスが選択したアドレスに変換されます (IPv4アドレスを持つホストおよび範囲タイプのネットワークオブジェクト/オブジェクトグループのみがサポートされます)。これは、アプリケーションがセキュアファイアウォールを介してリモートユーザに戻るルートを持つように設定できます

f) アプリケーショングループ (オプション) : このアプリケーションを既存のアプリケーショングループに追加して、設定済みの設定を使用するかどうかを選択します。

この例では、ZTNAを使用してアクセスされるアプリケーションは、テスト用のFMC Web UIと、セキュアファイアウォールの背後にあるCTBのWeb UIです。

アプリケーションの証明書は、Objects > Object Management > PKI > Internal certsで追加する必要があります。

Add Known Internal Certificate ?

Name:

Certificate Data or, choose a file:


-----BEGIN CERTIFICATE-----

T
G
AY

Key or, choose a file:

-----BEGIN RSA PRIVATE KEY-----

Encrypted, and the password is:

 注:ZTNAでアクセスする各アプリケーションのすべての証明書を追加してください。

証明書が内部証明書として追加されたら、残りの設定を続行します。

この例で設定するアプリケーション設定は次のとおりです。

アプリケーション1:FMC Web UIのテスト (アプリケーショングループ1のメンバー)

Add Application ? ×

Enabled

- Application Settings**
 - Application Name*
 - External URL* ?
 - Application URL (FQDN or Network IP)*
 - Use External URL as Application URL
By default, External URL is used as Application URL. Uncheck the checkbox to specify a different URL. For e.g., https://10.72.34.57:8443
 - Application Certificate* ?
 × ▼ +
 - IPv4 NAT Source ?
 ▼ +
 - Application Group
 × ▼
- SAML Service Provider (SP) Metadata
- SAML Identity Provider (IdP) Metadata
- Re-Authentication Interval
- Security Zones and Security Controls

Next

Cancel Finish

アプリケーションがアプリケーショングループ1に追加されたため、このアプリケーションの残りの設定が継承されます。ただし、セキュリティゾーンとセキュリティ制御は異なる設定で上書きできます。

設定したアプリケーションを確認し、Finishをクリックします。

Add Application ? ×

Enabled

1 Application Settings Edit

Application Name	FMC
External URL	https://ao-fmc-ztna.cisco.local
Application URL	https://ao-fmc-ztna.cisco.local
IPv4 NAT Source	-
Application Certificate	ao-fmc-ztna.cisco.local
Application Group	External_Duo

2 SAML Service Provider (SP) Metadata
Configurations are derived from Application Group 'External_Duo'

3 SAML Identity Provider (IdP) Metadata
Configurations are derived from Application Group 'External_Duo'

4 Re-Authentication Interval
Configurations are derived from Application Group 'External_Duo'

5 Security Zones and Security Controls Edit

Security Zones	Inherited: (Outside)
Intrusion Policy	Inherited: (None)
Variable Set	Inherited: (None)
Malware and File Policy	Inherited: (None)

Cancel Finish

アプリケーション2:CTB Web UI (アプリケーショングループ2のメンバー)

このアプリケーションの設定の概要は次のとおりです。

Enabled

1 Application Settings Edit

Application Name	CTB
External URL	https://ao-ctb.cisco.local
Application URL	https://ao-ctb.cisco.local
IPv4 NAT Source	ZTNA_NAT_CTBT
Application Certificate	ao-ctb.cisco.local
Application Group	Azure_apps

2 SAML Service Provider (SP) Metadata
Configurations are derived from Application Group 'Azure_apps'


3 SAML Identity Provider (IdP) Metadata
Configurations are derived from Application Group 'Azure_apps'

4 Re-Authentication Interval
Configurations are derived from Application Group 'Azure_apps'

5 Security Zones and Security Controls Edit

Security Zones	Inherited: (Outside)
Intrusion Policy	Inherited: (None)
Variable Set	Inherited: (None)
Malware and File Policy	Inherited: (None)

Cancel Finish

 注：このアプリケーションでは、ネットワークオブジェクト「ZTNA_NAT_CTBT」がIPv4 NATソースとして設定されていることに注意してください。この設定では、パケットをアプリケーションに転送する前に、リモートユーザからの送信元IPアドレスが、設定されたオブジェクト内のIPアドレスに変換されます。

これは、アプリケーション(CTB)のデフォルトルートがセキュアファイアウォール以外のゲートウェイを指しているため、リターントラフィックがリモートユーザに送信されなかったために設定されました。このNAT設定では、セキュアファイアウォールを介してサブネットZTNA_NAT_CTBTに到達できるように、アプリケーション上にスタティックルートが設定されています。

アプリケーションが設定されると、対応するアプリケーショングループの下に表示されます。

ZTNA-TAC / Targeted: 1 device
Groups: 3 Applications:

Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled
▼ Azure_apps (1 Application)			https://sts.v...	Outside (Inherited)	None (Inherited)	None (Inherited)	
<input type="checkbox"/> CTB	https://ao-ctb.cisco.local	https://ao-ctb.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True
▼ External_Duo (1 Application)			https://sso-...	Outside (Inherited)	None (Inherited)	None (Inherited)	
<input type="checkbox"/> FMC	https://ao-fmc-ztna.cisco.local	https://ao-fmc-ztna.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True


最後に、変更を保存し、設定を展開します。

確認

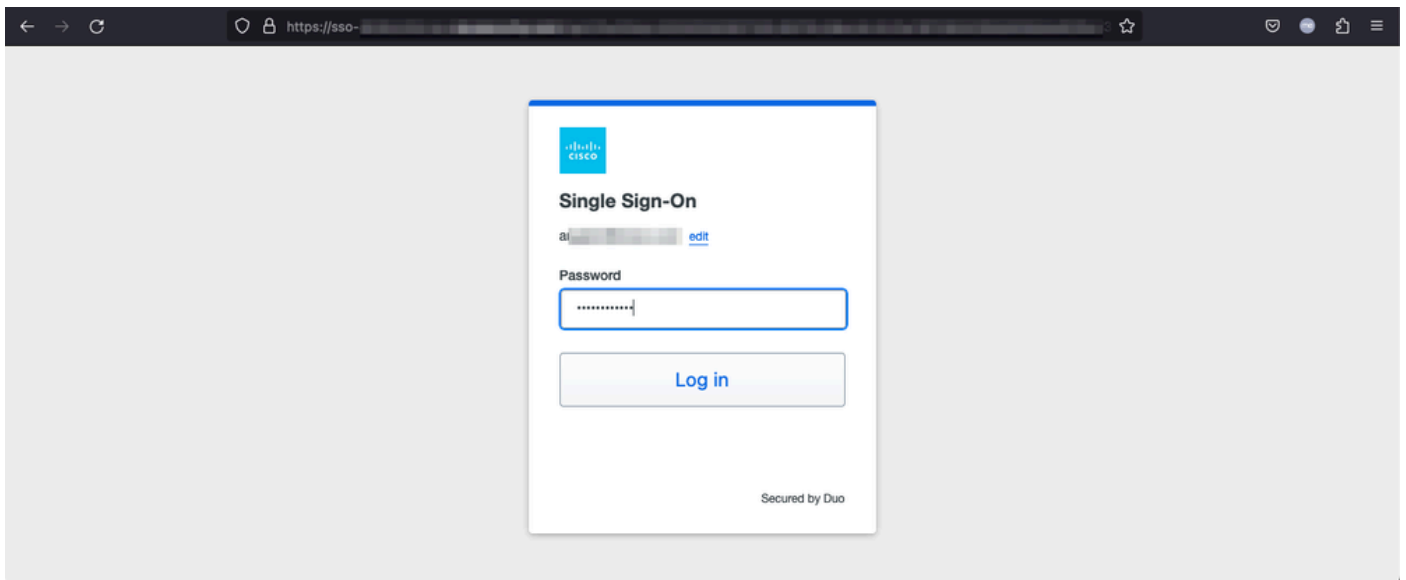
設定が完了すると、リモートユーザは外部URLを介してアプリケーションに到達でき、対応するIdPによって許可されている場合は、そのアプリケーションにアクセスできます。

アプリケーション 1

1.ユーザがWebブラウザを開き、アプリケーション1の外部URLに移動します。この場合、外部URLは「https://ao-fmc-ztna.cisco.local/」です

 注：外部URL名は、設定されたセキュアファイアウォールインターフェイスのIPアドレスに解決される必要があります。この例では、外部インターフェイスのIPアドレス (192.0.2.254)に解決されます

2.これは新しいアクセスであるため、ユーザはアプリケーション用に設定されたIdPログインポータルにリダイレクトされます。

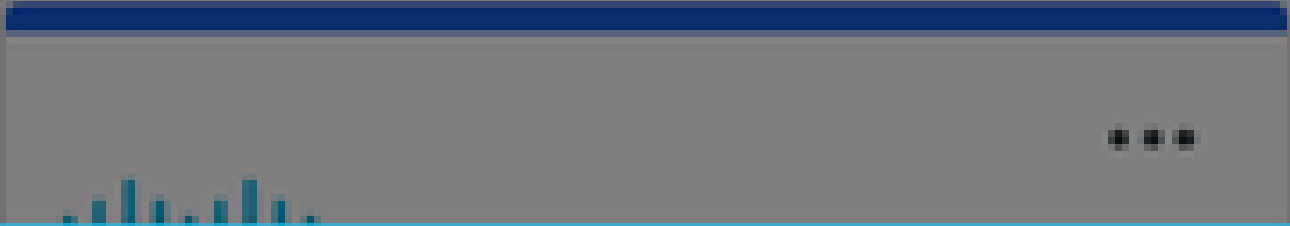


3.ユーザにMFAのプッシュが送信されます (これは、IdPで設定されているMFA方式によって異なります)。



Accounts

Add



Are you logging in to **External Applications ZTNA?**

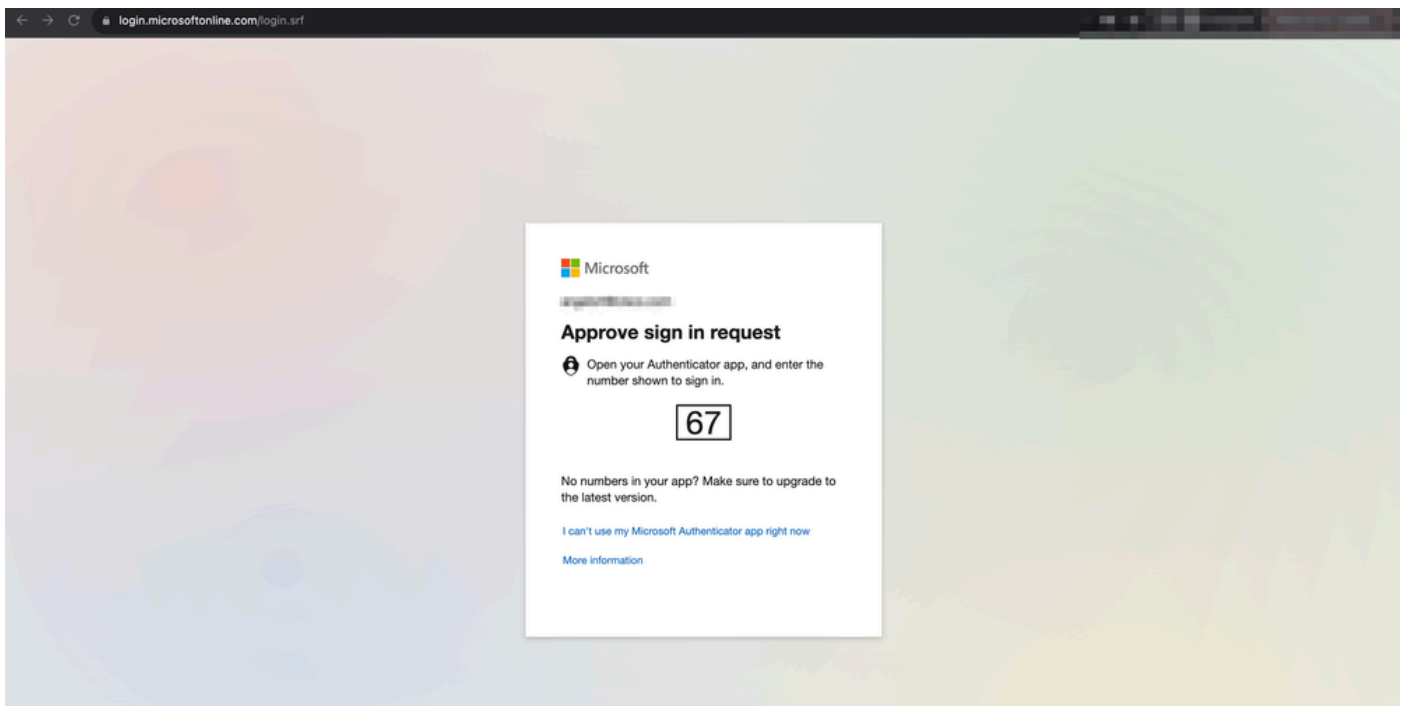
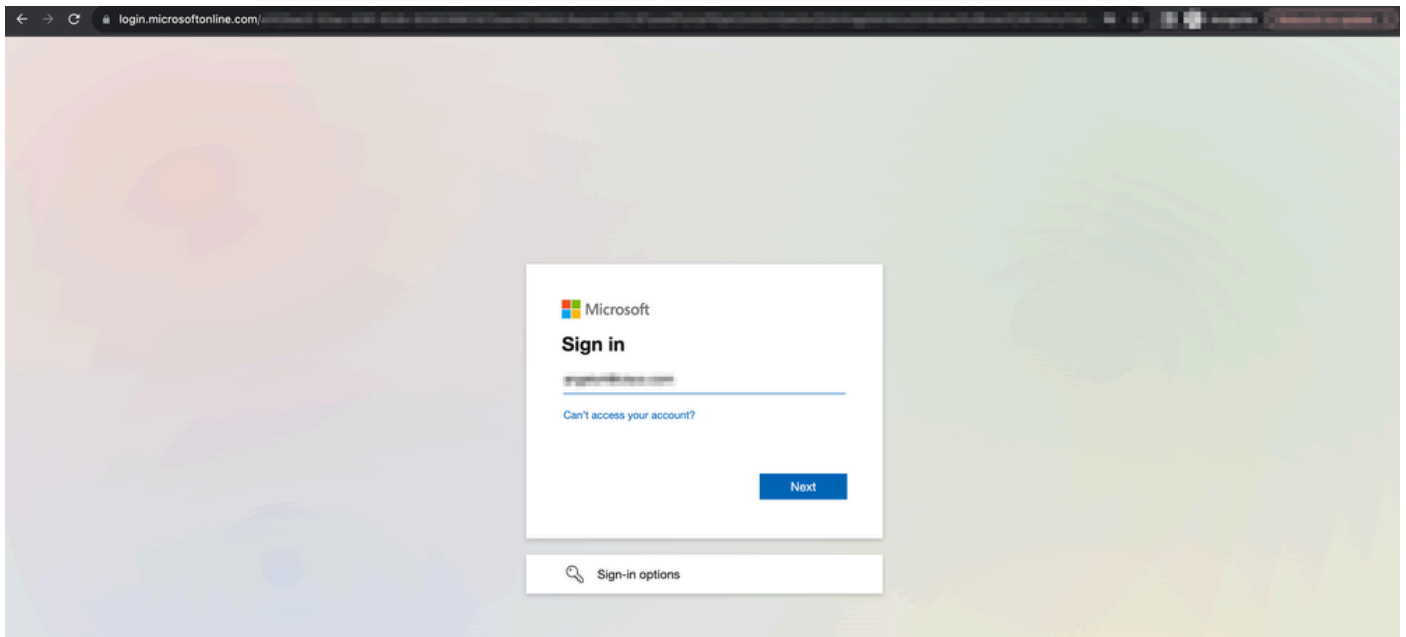
 Global VPN TAC

 [Redacted]

 1:13 p.m.

 [Redacted]

2.これは新しいアクセスであるため、ユーザはアプリケーション用に設定されたIdPログインポータルにリダイレクトされます。

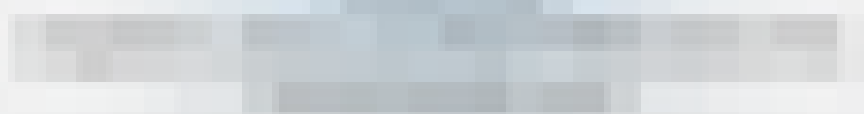


3.ユーザにMFAのプッシュが送信されます (これは、IdPで設定されているMFA方式によって異なります)。

4:24



Are you trying to sign in?



Enter the number shown to sign in.

No, it's not me

Yes

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。