

Configurer un déploiement d'accès à distance sans confiance sur Secure Firewall

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration requise](#)

[Configurations générales](#)

[Configurer le groupe d'applications](#)

[Groupe d'applications 1 : utilisation de Duo comme fournisseur d'identités](#)

[Groupe d'applications 2 : utilisation de Microsoft Entra ID \(Azure AD\) comme fournisseur d'identité](#)

[Configuration des applications](#)

[Application 1 : tester l'interface utilisateur Web de FMC \(membre du groupe d'applications 1\)](#)

[Application 2 : interface utilisateur Web de CTB \(membre du groupe d'applications 2\)](#)

[Vérifier](#)

[Monitor](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus de configuration du déploiement de l'accès à distance sans confiance sans client sur un pare-feu sécurisé.

Conditions préalables

Exigences

Cisco recommande de posséder des connaissances sur ces sujets :

- Firepower Management Center (FMC)
- Connaissances ZTNA de base
- Connaissance du langage SAML (Basic Security Assertion Markup Language)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Secure Firewall version 7.4.1
- Firepower Management Center (FMC) version 7.4.1
- Duo en tant que fournisseur d'identité (IdP)
- Microsoft Entra ID (anciennement Azure AD) en tant que fournisseur d'identité

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La fonctionnalité Zero Trust Access est basée sur les principes ZTNA (Zero Trust Network Access). ZTNA est un modèle de sécurité de confiance zéro qui élimine la confiance implicite. Le modèle accorde le privilège d'accès le plus faible après vérification de l'utilisateur, du contexte de la demande et après analyse du risque si l'accès est accordé.

Les exigences et limites actuelles de ZTNA sont les suivantes :

- Pris en charge sur Secure Firewall version 7.4.0+ géré par FMC version 7.4.0+ (Firepower 4200 Series)
- Pris en charge sur Secure Firewall version 7.4.1+ géré par FMC version 7.4.1+ (toutes les autres plates-formes)
- Seules les applications Web (HTTPS) sont prises en charge. Les scénarios nécessitant une exemption de déchiffrement ne sont pas pris en charge
- Prend en charge uniquement les IDp SAML
- Des mises à jour DNS publiques sont nécessaires pour l'accès distant
- IPv6 n'est pas pris en charge. Les scénarios NAT66, NAT64 et NAT46 ne sont pas pris en charge
- La fonction est disponible pour la défense contre les menaces uniquement si Snort 3 est activé
- Tous les liens hypertexte des applications Web protégées doivent avoir un chemin d'accès relatif
- Les applications Web protégées exécutées sur un hôte virtuel ou derrière des équilibreurs de charge internes doivent utiliser la même URL externe et interne
- Non pris en charge sur les clusters en mode individuel
- Non pris en charge sur les applications avec validation d'en-tête HTTP stricte activée

- Si le serveur d'applications héberge plusieurs applications et fournit du contenu basé sur l'en-tête SNI (Server Name Indication) dans Hello du client TLS, l'URL externe de la configuration d'application de confiance zéro doit correspondre au SNI de cette application spécifique
- Pris en charge uniquement en mode routé
- Licence Smart requise (ne fonctionne pas en mode évaluation)

Pour plus d'informations et de détails sur Zero Trust Access dans Secure Firewall, reportez-vous au [Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.4](#).

Configurer

Ce document se concentre sur un déploiement d'accès à distance de ZTNA.

Dans cet exemple de scénario, les utilisateurs distants ont besoin d'accéder aux interfaces utilisateur Web d'un FMC de test et d'un Cisco Telemetry Broker (CTB) qui sont hébergés derrière un pare-feu sécurisé. L'accès à ces applications est accordé par deux IDp différents : Duo et Microsoft Entra ID respectivement, comme indiqué dans le schéma suivant.

Diagramme du réseau

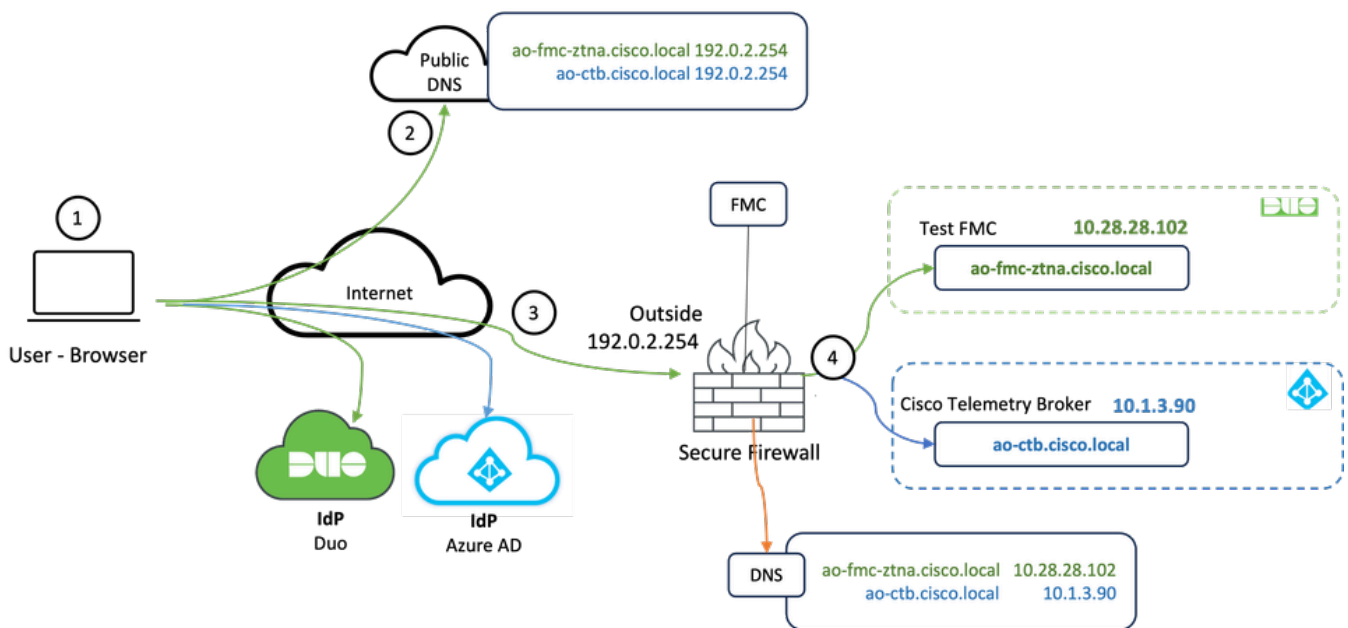


Diagramme topologique

1. Les utilisateurs distants doivent accéder aux applications hébergées derrière le pare-feu sécurisé.
2. Chaque application doit avoir une entrée DNS dans les serveurs DNS publics.
3. Ces noms d'application doivent correspondre à l'adresse IP de l'interface externe du pare-feu sécurisé.
4. Le pare-feu sécurisé convertit les adresses IP réelles des applications et authentifie chaque utilisateur pour chaque application à l'aide de l'authentification SAML.

Configuration requise

Fournisseur d'identités (IdP) et serveur de noms de domaine (DNS)

- Les applications ou les groupes d'applications doivent être configurés dans un fournisseur d'identité SAML (IdP) tel que Duo, Okta ou Azure AD. Dans cet exemple, les ID Duo et Microsoft Entra sont utilisés comme IDp.
- Le certificat et les métadonnées générés par les IdP sont utilisés lors de la configuration de l'application sur le pare-feu sécurisé

Serveurs DNS internes et externes

- Les serveurs DNS externes (utilisés par les utilisateurs distants) doivent disposer de l'entrée FQDN des applications et être résolus en adresse IP de l'interface externe Secure Firewall
- Les serveurs DNS internes (utilisés par le pare-feu sécurisé) doivent avoir l'entrée FQDN des applications et être résolus en adresse IP réelle de l'application

Certificats

Les certificats suivants sont requis pour la configuration de la politique ZTNA :


- Certificat d'identité/proxy : utilisé par le pare-feu sécurisé pour usurper les applications. Le pare-feu sécurisé agit ici en tant que fournisseur de services SAML. Ce certificat doit être un certificat générique ou un certificat SAN correspondant au nom de domaine complet des applications privées (un certificat commun qui représente toutes les applications privées au stade de la pré-authentification)
- Certificat IdP : le fournisseur d'ID utilisé pour l'authentification fournit un certificat pour chaque application ou groupe d'applications défini. Ce certificat doit être configuré de sorte que le pare-feu sécurisé
Peut vérifier la signature du fournisseur d'identité sur les assertions SAML entrantes (si cette signature est définie pour un groupe d'applications, le même certificat est utilisé pour l'ensemble du groupe d'applications)
- Certificat d'application : le trafic chiffré de l'utilisateur distant vers l'application doit être déchiffré par le pare-feu sécurisé. Par conséquent, la chaîne de certificats et la clé privée de chaque application doivent être ajoutées au pare-feu sécurisé.

Configurations générales


Pour configurer une nouvelle application Zero Trust, procédez comme suit :

1. Accédez à Politiques > Access Control > Zero Trust Application et cliquez sur Add Policy.
2. Renseignez les champs obligatoires :
 - a) Général : saisissez le nom et la description de la stratégie.

b) Domain Name : il s'agit du nom ajouté au DNS et qui doit être résolu en interface de passerelle de défense contre les menaces à partir de laquelle les applications sont accessibles.

 Remarque : le nom de domaine est utilisé pour générer l'URL ACS pour toutes les applications privées d'un groupe d'applications.

c) Certificat d'identité : il s'agit d'un certificat commun qui représente toutes les applications privées au stade de la pré-authentification.

 Remarque : ce certificat doit être un certificat générique ou un certificat SAN correspondant au nom de domaine complet des applications privées.

d) Zones de sécurité : sélectionnez les zones externes et/ou internes par lesquelles les applications privées sont réglementées.

e) Pool de ports global : un port unique de ce pool est attribué à chaque application privée.

f) Contrôles de sécurité (facultatif) : sélectionnez cette option si les applications privées sont soumises à une inspection.

Dans cet exemple de configuration, les informations suivantes ont été saisies :

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*

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.

Le certificat d'identité/proxy utilisé dans ce cas est un certificat générique correspondant au nom de domaine complet des applications privées :

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. Enregistrez la règle.

4. Créez les nouveaux groupes d'applications et/ou les nouvelles applications :

- Une application définit une application Web privée avec authentification SAML, accès à l'interface, stratégies contre les intrusions, les programmes malveillants et les fichiers.
- Un groupe d'applications vous permet de regrouper plusieurs applications et de partager des paramètres communs tels que l'authentification SAML, l'accès à l'interface et les paramètres de contrôle de sécurité.

Dans cet exemple, deux groupes d'applications différents et deux applications différentes sont configurés : un pour l'application à authentifier par Duo (tester l'interface utilisateur Web de FMC) et un pour l'application à authentifier par Microsoft Entra ID (interface utilisateur Web de CTB).

Configurer le groupe d'applications

Groupe d'applications 1 : utilisation de Duo comme fournisseur d'identités

a. Entrez le nom du groupe d'applications et cliquez sur Next pour afficher les métadonnées du fournisseur de services SAML.

Add Application Group [Close]

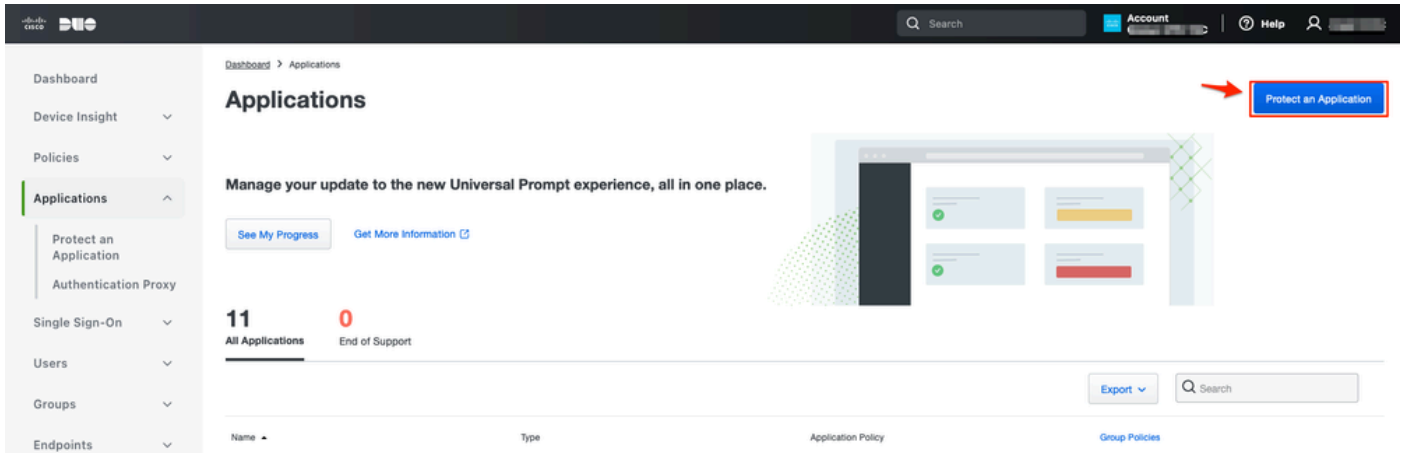
An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- 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**

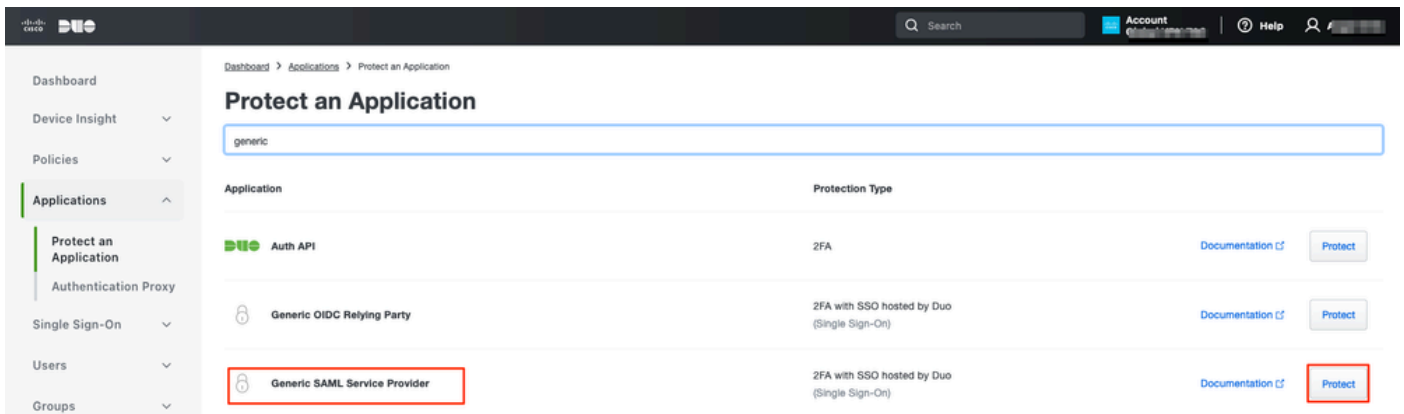
Cancel Finish

b. Une fois que les métadonnées SAML SP sont affichées, accédez à l'IdP et configurez une nouvelle application SAML SSO.

c. Connectez-vous à Duo et accédez à Applications > Protect an Application.



d. Recherchez Generic SAML Service Provider et cliquez sur Protect.



e. Téléchargez le certificat et les métadonnées SAML à partir du fournisseur d'identité, car ils sont nécessaires pour poursuivre la configuration sur Secure Firewall.

f. Saisissez l'ID d'entité et l'URL ACS (Assertion Consumer Service) à partir du groupe d'applications ZTNA (généré à l'étape a).

- 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 * `https://.../External_Duo/saml/sp/metadata`

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL * `https://.../External_Duo/+CSCOE+/saml/sp/ac`

[+ Add an ACS URL](#)

g. Modifiez l'application en fonction de vos besoins spécifiques et autorisez l'accès à l'application uniquement aux utilisateurs prévus, puis cliquez sur Enregistrer.

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. Revenez au FMC et ajoutez les métadonnées SAML IdP au groupe d'applications, à l'aide des fichiers téléchargés à partir de l'IdP.

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** 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*

Single Sign-On URL*

IdP Certificate

[Next](#)

[Cancel](#) [Finish](#)

i. Cliquez sur Next et configurez l'intervalle de réauthentification et les contrôles de sécurité selon vos besoins. Vérifiez la configuration récapitulative et cliquez sur Finish.

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?tname=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

Groupe d'applications 2 : utilisation de Microsoft Entra ID (Azure AD) comme fournisseur d'identité

a. Entrez le nom du groupe d'applications et cliquez sur Next pour afficher les métadonnées du fournisseur de services SAML.

Add Application Group



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

- Application Group** Edit
Name: **Azure_apps**
- 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
- SAML Identity Provider (IdP) Metadata**
- Re-Authentication Interval**
- Security Zones and Security Controls**

Cancel

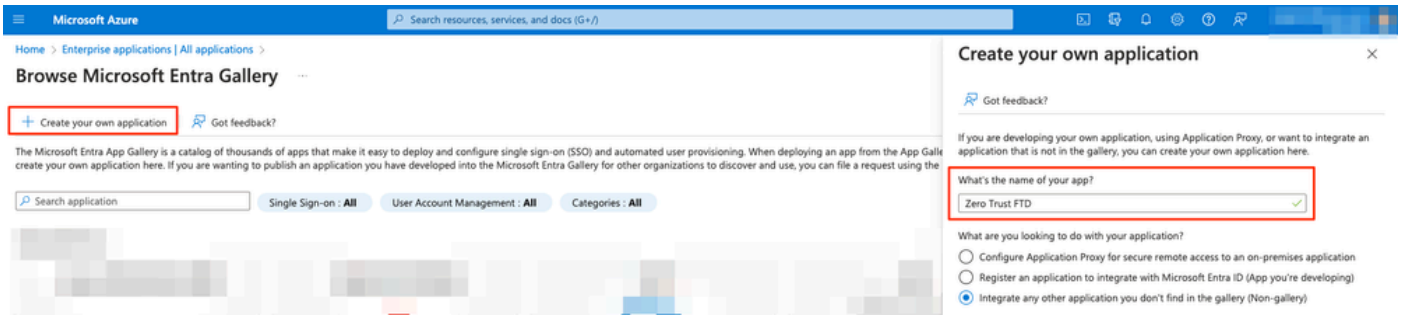
Finish

b. Une fois que les métadonnées SAML SP sont affichées, accédez à l'IdP et configurez une nouvelle application SAML SSO.

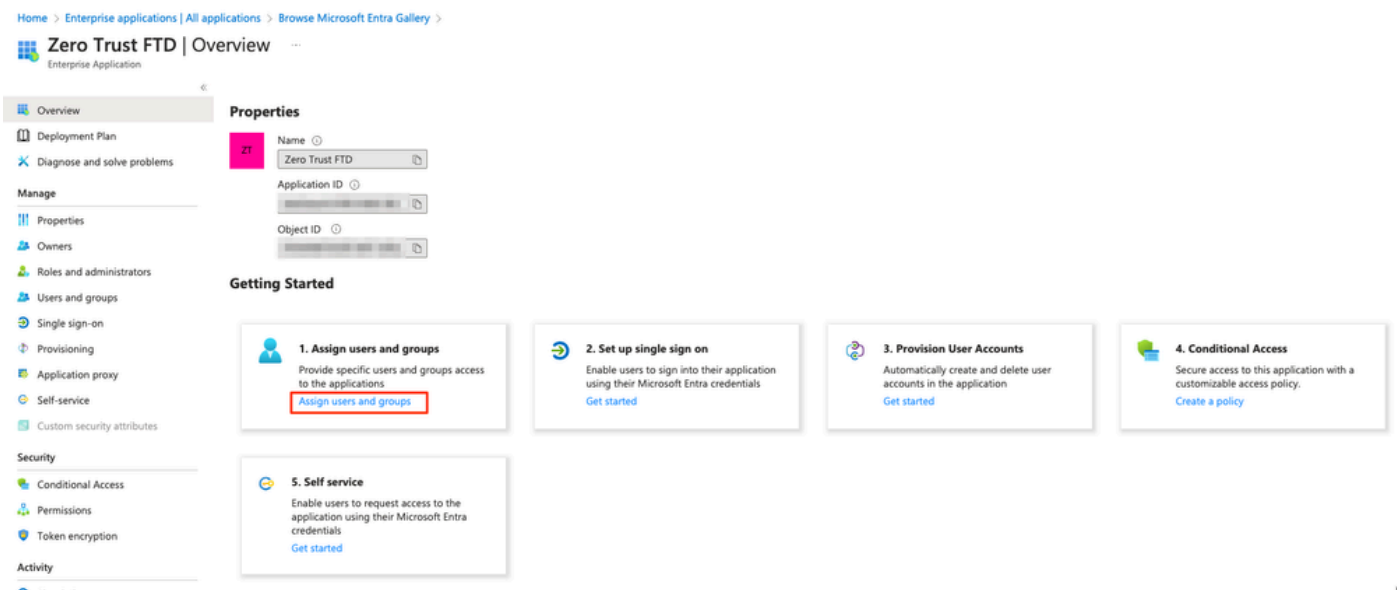
c. Connectez-vous à Microsoft Azure et accédez à Applications d'entreprise > Nouvelle application.

The screenshot shows the Microsoft Azure portal interface for Enterprise applications. The breadcrumb navigation is 'Home > Enterprise applications', with 'Enterprise applications' highlighted. The main heading is 'Enterprise applications | All applications'. Below this, there are several action buttons: '+ New application' (highlighted with a red box), 'Refresh', 'Download (Export)', 'Preview info', 'Columns', 'Preview features', and 'Got feedback?'. The 'Overview' section contains the text: 'View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider. The list of applications that are maintained by your organization are in application registrations.' Below this is a search bar with the text 'Search by application name or object ID' and two filter buttons: 'Application type == Enterprise Applications' and 'Application ID starts with'. It also shows '77 applications found' and a table with columns: Name, Object ID, Application ID, Homepage URL, and Created on.

d. Cliquez sur Create your own application > Saisissez le nom de l'application > Create



e. Ouvrez l'application et cliquez sur Affecter des utilisateurs et des groupes pour définir les utilisateurs et/ou les groupes autorisés à accéder à l'application.



f. Cliquez sur Add user/group > Sélectionnez les utilisateurs/groupes nécessaires > Assign. Une fois que les utilisateurs/groupes corrects ont été attribués, cliquez sur Authentification unique.

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

1

2

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

Display Name	Object Type
AO Angel	
FG Fernando	

g. Une fois dans la section Single sign-on, cliquez sur SAML.

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

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. Cliquez sur Upload metadata file et sélectionnez le fichier XML téléchargé à partir du fournisseur de services (Secure Firewall) ou saisissez manuellement l'ID d'entité et l'URL ACS (Assertion Consumer Service) du groupe d'applications ZTNA (généralisé à l'étape a).

Remarque : assurez-vous de télécharger également le fichier XML de métadonnées de fédération ou de télécharger individuellement le certificat (base 64) et de copier les métadonnées SAML à partir de l'IdP (URL de connexion et de déconnexion et identificateurs supplémentaires Microsoft), car ceux-ci sont nécessaires pour poursuivre la configuration sur le pare-feu sécurisé.

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?tgname=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. Revenez au FMC et importez les métadonnées SAML IdP dans le groupe d'applications 2, à l'aide du fichier de métadonnées téléchargé à partir de l'IdP ou saisissez manuellement les données requises.

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 certificate content]

Next

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

Finish

j. Cliquez sur Next et configurez l'intervalle de réauthentification et les contrôles de sécurité selon vos besoins. Vérifiez la configuration récapitulative et cliquez sur Finish.

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	Azure_apps	
2	SAML Service Provider (SP) Metadata		Edit
	Entity ID	https://[redacted]/Azure_apps/saml/sp/metadata	
	Assertion Consumer Service (ACS) URL	https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=Def...	
3	SAML Identity Provider (IdP) Metadata		Edit
	Entity ID	https://[redacted]	
	Single Sign-On URL	https://[redacted]	
	IdP Certificate	[redacted]	
4	Re-Authentication Interval		Edit
	Timeout Interval	1440 minutes	
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

Configuration des applications

Maintenant que les groupes d'applications ont été créés, cliquez sur Add Application pour définir les applications à protéger et auxquelles vous souhaitez accéder à distance.

1. Saisissez les paramètres de l'application :

a) Nom de l'application : Identificateur de l'application configurée.

b) URL externe : URL publiée de l'application dans les enregistrements DNS publics/externes. Il s'agit de l'URL utilisée par les utilisateurs pour accéder à l'application à distance.

c) URL de l'application : FQDN réel ou IP réseau de l'application. Il s'agit de l'URL utilisée par Secure Firewall pour accéder à l'application.

Remarque : par défaut, l'URL externe est utilisée comme URL d'application. Décochez la case pour spécifier une autre URL d'application.

d) Certificat d'application : la chaîne de certificats et la clé privée de l'application à laquelle accéder (ajouté depuis la page d'accueil FMC > Objets > Gestion des objets > ICP > Certificats)

internes)

e) IPv4 NAT Source (facultatif) : l'adresse IP source de l'utilisateur distant est traduite en adresses sélectionnées avant de transférer les paquets à l'application (seuls les objets/groupes d'objets réseau de type Hôte et Plage ayant des adresses IPv4 sont pris en charge). Cette option peut être configurée pour garantir que les applications disposent d'une route vers les utilisateurs distants via le pare-feu sécurisé

f) Groupe d'applications (facultatif) : sélectionnez cette option si l'application est ajoutée à un groupe d'applications existant pour utiliser les paramètres configurés.

Dans cet exemple, les applications accessibles à l'aide de ZTNA sont une interface utilisateur Web FMC de test et l'interface utilisateur Web d'un CTB situé derrière le pare-feu sécurisé.

Les certificats des applications doivent être ajoutés dans Objets > Gestion des objets > ICP > Certificats internes :

Add Known Internal Certificate ?

Name:

Certificate Data or, choose a file:

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

T


G

3Y

Key or, choose a file:

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

Encrypted, and the password is:

 Remarque : assurez-vous d'ajouter tous les certificats pour chaque application à laquelle ZTNA doit accéder.

Une fois que les certificats ont été ajoutés en tant que certificats internes, continuez à configurer les paramètres restants.

Les paramètres d'application configurés pour cet exemple sont les suivants :

Application 1 : tester l'interface utilisateur Web de FMC (membre du groupe d'applications 1)

Enabled **1 Application Settings**

Application Name*

FMC

External URL* ⓘ

https://ao-fmc-ztna.cisco.local

Application URL (FQDN or Network IP)*

https://ao-fmc-ztna.cisco.local

 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* ⓘ

ao-fmc-ztna.cisco.local x v +

IPv4 NAT Source ⓘ

Select... v +

Application Group

External_Duo x v

Next

2 SAML Service Provider (SP) Metadata

3 SAML Identity Provider (IdP) Metadata

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

Finish

Comme l'application a été ajoutée au groupe d'applications 1, les paramètres restants sont hérités pour cette application. Vous pouvez toujours remplacer les zones de sécurité et les contrôles de sécurité avec des paramètres différents.

Vérifiez l'application configurée et cliquez sur Finish.

Add Application



Enabled

Edit

1 Application Settings

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

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

Edit

Cancel

Finish

Application 2 : interface utilisateur Web de CTB (membre du groupe d'applications 2)

Le résumé de la configuration de cette application est le suivant :

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_CTB
 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

 Remarque : notez que pour cette application, un objet réseau « ZTNA_NAT_CTB » a été configuré comme source NAT IPv4. Avec cette configuration, l'adresse IP source des utilisateurs distants est traduite en une adresse IP dans l'objet configuré avant de transférer les paquets à l'application.

Cette configuration a été effectuée car la route par défaut de l'application (CTB) pointe vers une passerelle autre que le pare-feu sécurisé. Par conséquent, le trafic de retour n'a pas été envoyé aux utilisateurs distants. Avec cette configuration NAT, une route statique a été configurée sur l'application pour que le sous-réseau ZTNA_NAT_CTB soit accessible via le pare-feu sécurisé.

Une fois les applications configurées, elles s'affichent sous le groupe d'applications correspondant.

ZTNA-TAC Targeted: 1 device

Applications Settings Groups: 3 Applications:

Bulk Actions Add Application Group Add Application

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


Enfin, enregistrez les modifications et déployez la configuration.

Vérifier

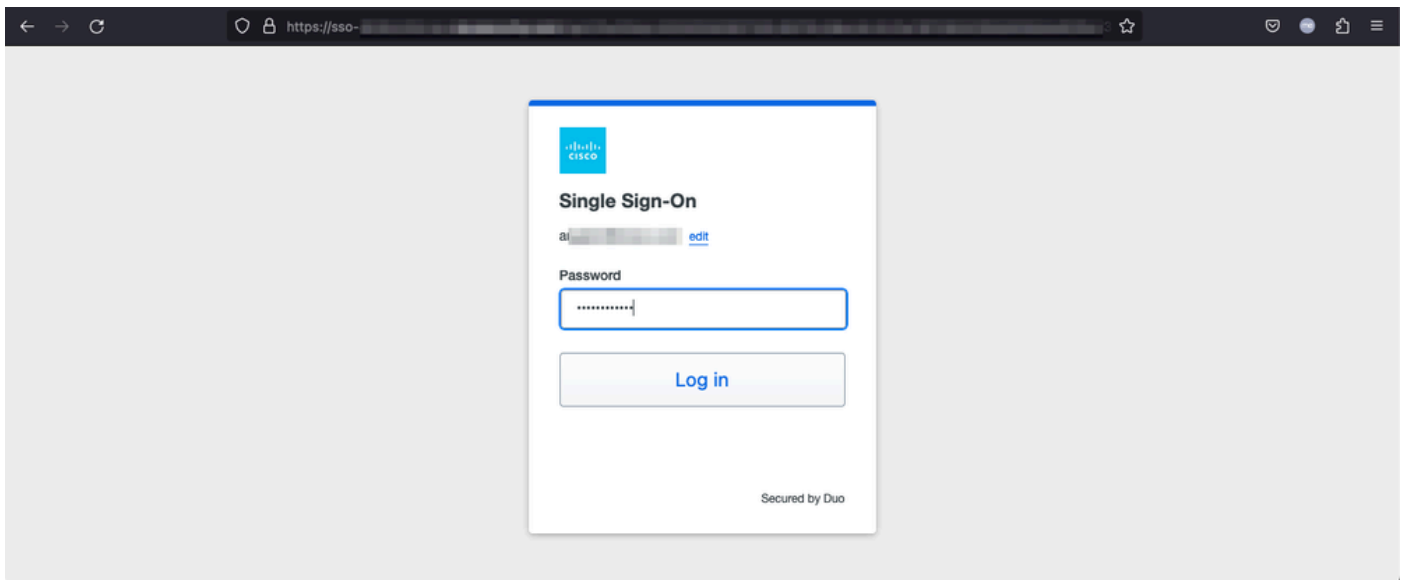
Une fois la configuration en place, les utilisateurs distants peuvent accéder aux applications via l'URL externe et, s'ils sont autorisés par le fournisseur d'identité correspondant, y accéder.

Application 1

1. L'utilisateur ouvre un navigateur Web et accède à l'URL externe de l'application 1. Dans ce cas, l'URL externe est "https://ao-fmc-ztna.cisco.local/"

 Remarque : le nom de l'URL externe doit correspondre à l'adresse IP de l'interface Secure Firewall configurée. Dans cet exemple, il correspond à l'adresse IP de l'interface externe (192.0.2.254)

2. Comme il s'agit d'un nouvel accès, l'utilisateur est redirigé vers le portail de connexion IdP configuré pour l'application.

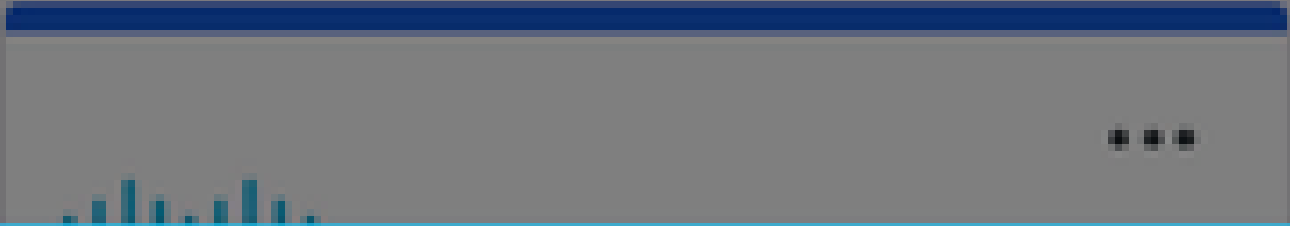


3. L'utilisateur reçoit une transmission Push pour MFA (cela dépend de la méthode MFA configurée sur l'IdP).



Accounts

Add




Are you logging in to External Applications ZTNA?

🌐 Global VPN TAC

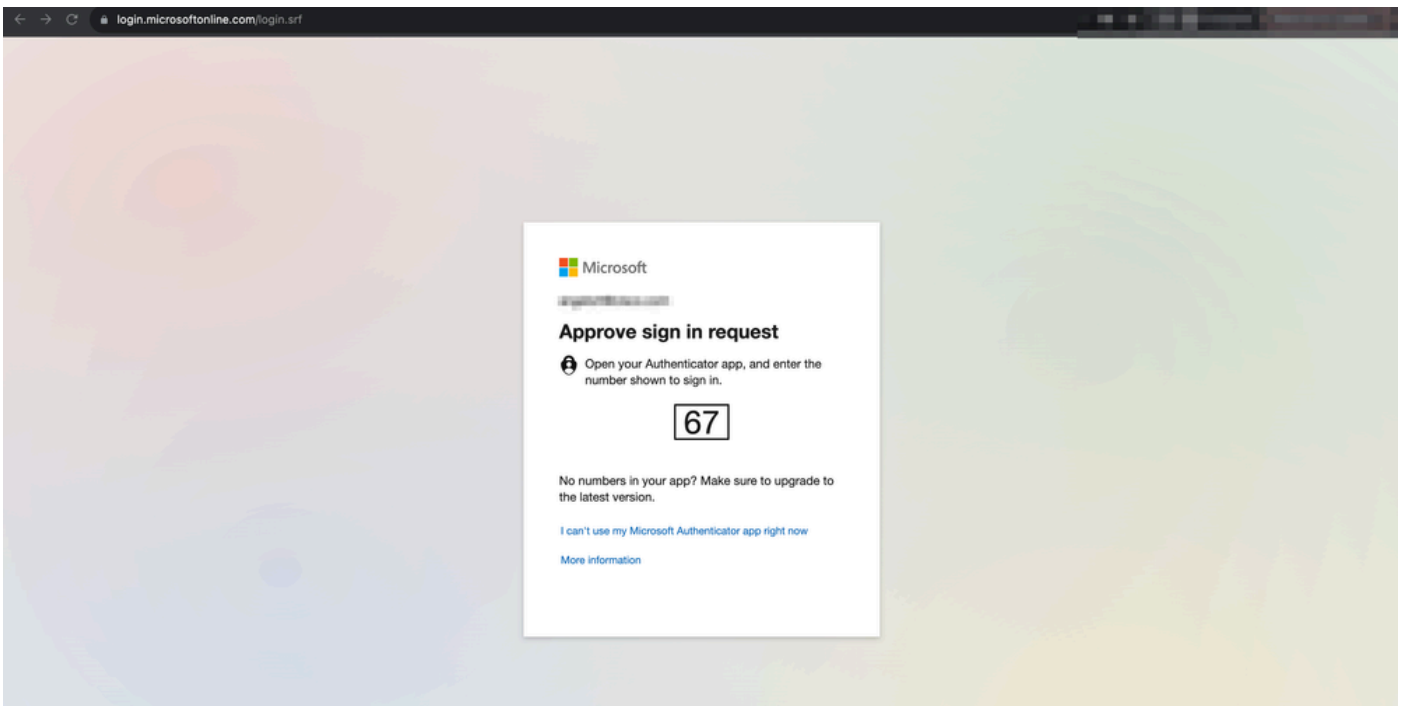
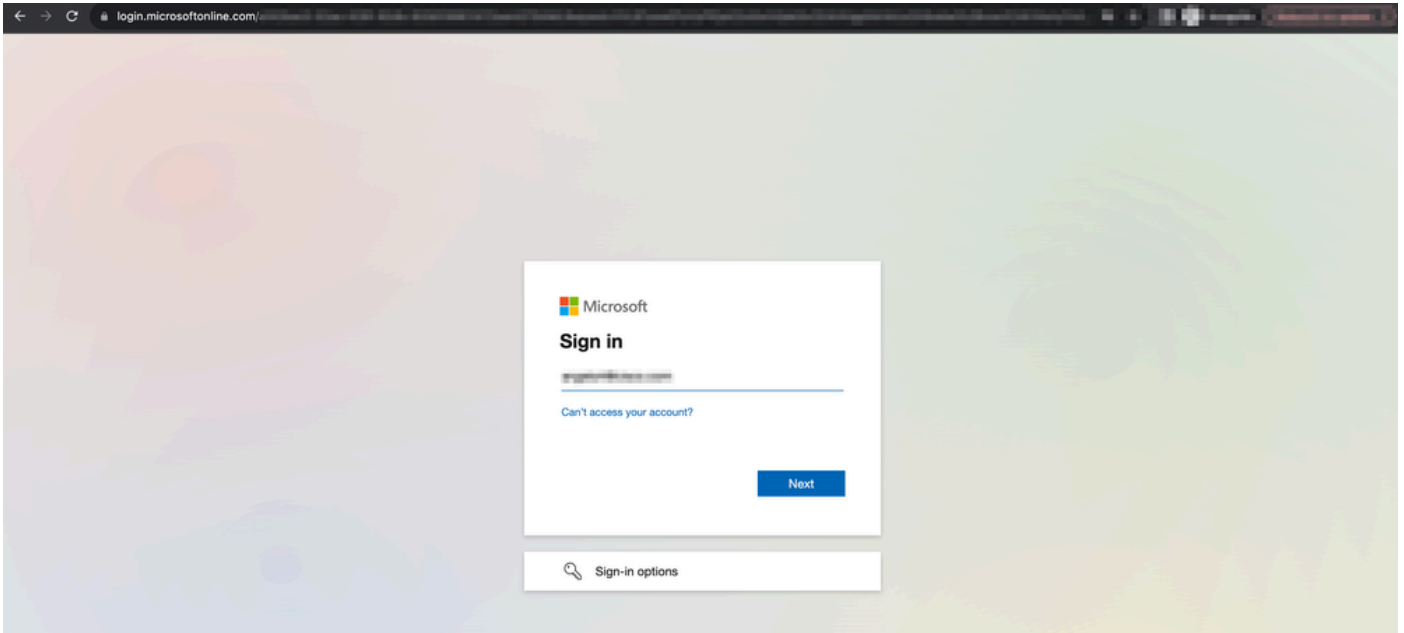
🌐 [Redacted]

🕒 1:13 p.m.

👤 [Redacted]

 : le nom de l'URL externe doit correspondre à l'adresse IP de l'interface Secure Firewall configurée. Dans cet exemple, il correspond à l'adresse IP de l'interface externe (192.0.2.254)

2. Comme il s'agit d'un nouvel accès, l'utilisateur est redirigé vers le portail de connexion IdP configuré pour l'application.

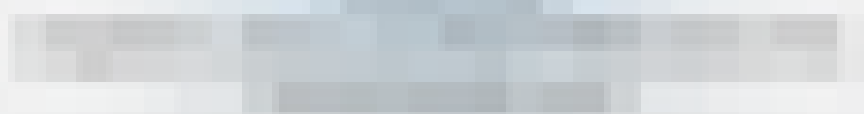


3. L'utilisateur reçoit une transmission Push pour MFA (cela dépend de la méthode MFA configurée sur l'IdP).

4:24



Are you trying to sign in?



Enter the number shown to sign in.

Enter number

No, it's not me

Yes

- Les diagnostics fournissent une analyse globale (OK ou non) et collectent des journaux détaillés qui peuvent être analysés pour résoudre les problèmes

Les diagnostics spécifiques à l'application permettent de détecter :



- Problèmes liés au DNS
- Mauvaise configuration, par exemple, socket non ouvert, règles de classification, règles NAT
- Problèmes dans la stratégie d'accès Zero Trust
- Problèmes liés à l'interface, par exemple, interface non configurée ou interface désactivée

Diagnostics génériques à détecter :

- Si une licence de chiffrement fort n'est pas activée
- Si le certificat d'application n'est pas valide
- Si la méthode d'authentification n'est pas initialisée à SAML dans le groupe de tunnels par défaut
- Problèmes de synchronisation en masse haute disponibilité et cluster
- Obtenez des informations des compteurs Snort pour diagnostiquer les problèmes, tels que ceux liés aux jetons ou au déchiffrement
- Problème d'épuisement du pool PAT dans la traduction source.

Pour exécuter les tests de diagnostic :

1. Accédez à l'icône diagnostics présente pour chaque application ZTNA.

Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled	
Azure_apps (1 Application)				Outside (Inherited)	None (Inherited)	None (Inherited)		
<input type="checkbox"/> CTB				Outside (Inherited)	None (Inherited)	None (Inherited)	True	
External_Duo (1 Application)				Outside (Inherited)	None (Inherited)	None (Inherited)		
<input type="checkbox"/> FMC				Outside (Inherited)	None (Inherited)	None (Inherited)	True	

2. Sélectionnez un périphérique et cliquez sur Exécuter.

Select Device

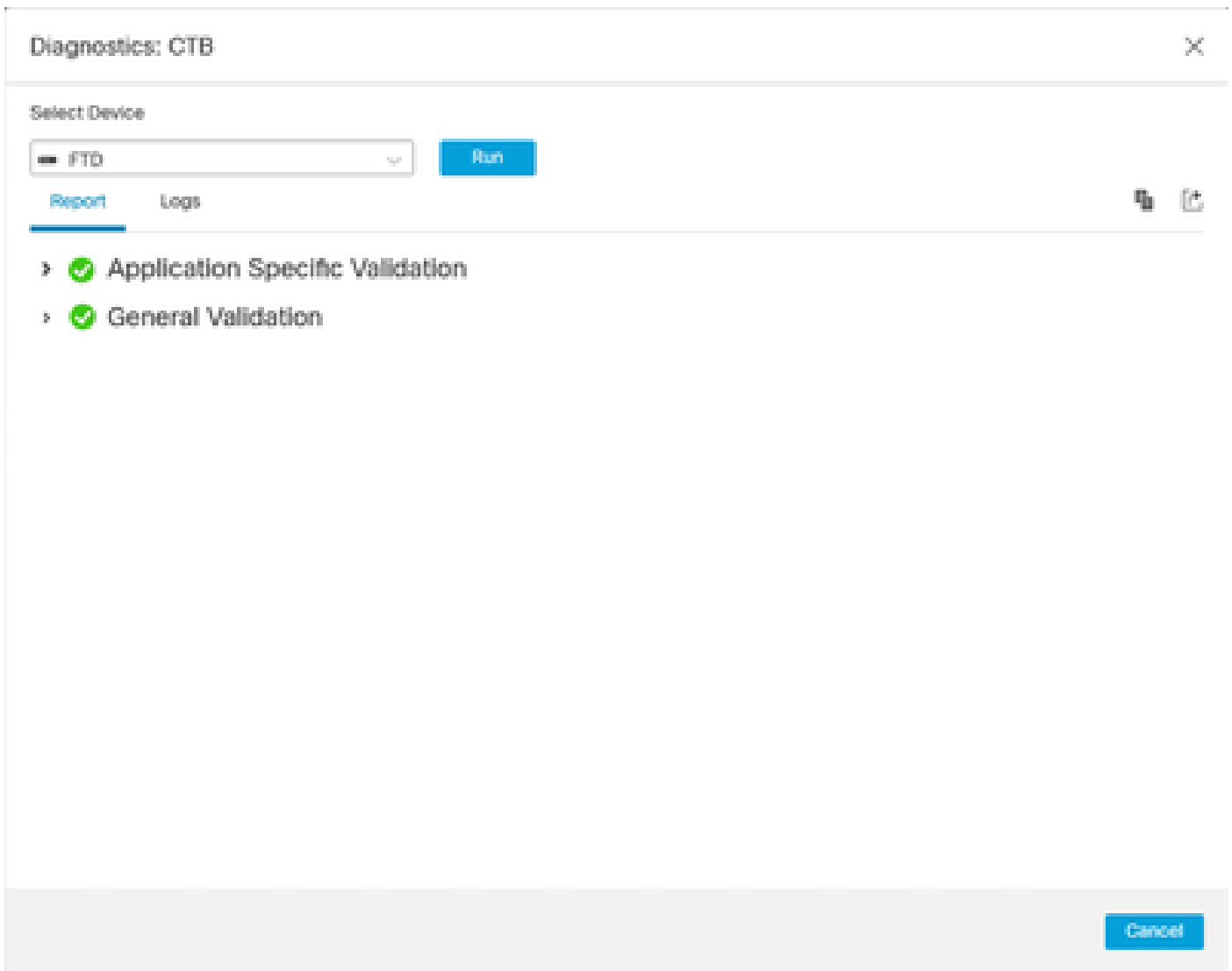
Select...

FTD

Run

Cancel

3. Affichez les résultats dans l'état.



Les commandes show et clear sont disponibles dans l'interface de ligne de commande FTD pour afficher la configuration de confiance zéro, ainsi que les statistiques et les informations de session.

```
<#root>
```

```
firepower# show running-config zero-trust
```

```
application      Show application configuration information
application-group Show application group configuration
|                Output modifiers
<cr>
```

```
firepower# show zero-trust
```

```
sessions  Show zero-trust sessions
statistics Show zero-trust statistics
```

```
firepower# show zero-trust sessions
```

```
application      show zero-trust sessions for application
application-group show zero-trust sessions for application group
count            show zero-trust sessions count
user            show zero-trust sessions for user
detail          show detailed info for the session
|              Output modifiers
<cr>
```

```
firepower# clear zero-trust
```

```
sessions  Clear all zero-trust sessions
statistics Clear all zero-trust statistics
```

```
firepower# clear zero-trust sessions
```

```
application Clear zero-trust sessions for application
user        Clear zero-trust sessions for user
<cr>
```

Pour activer les débogages de module de confiance zéro et webvpn, utilisez les commandes suivantes à l'invite Lina :

- firepower# debug zero-trust 255
- firepower# debug webvpn request 255
- firepower# debug webvpn response 255
- firepower# debug webvpn saml 255

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le centre d'assistance technique (TAC). Un contrat d'assistance valide est requis : [Cisco Worldwide Support Contacts](#).
- Vous pouvez également visiter la communauté VPN Cisco [ici](#).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.