

Configuración de la implementación de acceso remoto sin confianza en un firewall seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de Prerrequisitos](#)

[Configuraciones generales](#)

[Configurar grupo de aplicaciones](#)

[Grupo de aplicaciones 1: Uso de Duo como IdP](#)

[Grupo de aplicaciones 2: usar Microsoft Entra ID \(Azure AD\) como IdP](#)

[Configurar aplicaciones](#)

[Aplicación 1: interfaz de usuario web de prueba FMC \(miembro del grupo de aplicaciones 1\)](#)

[Aplicación 2: interfaz de usuario web de CTB \(miembro del grupo de aplicaciones 2\)](#)

[Verificación](#)

[Monitor](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso de configuración de la implementación de Acceso Remoto de Confianza Cero sin Cliente en un Firewall Seguro.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Centro de administración Firepower (FMC)
- Conocimiento básico de ZTNA
- Conocimiento del lenguaje básico de marcado de aserción de seguridad (SAML)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Secure Firewall versión 7.4.1
- Firepower Management Center (FMC) versión 7.4.1
- Duo como proveedor de identidad (IdP)
- ID de Microsoft Entry (anteriormente, Azure AD) como IdP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La función Zero Trust Access se basa en los principios de Zero Trust Network Access (ZTNA). ZTNA es un modelo de seguridad de confianza cero que elimina la confianza implícita. El modelo concede el acceso con menos privilegios después de verificar el usuario, el contexto de la solicitud y después de analizar el riesgo si se concede el acceso.

Los requisitos y limitaciones actuales de ZTNA son:

- Compatible con Secure Firewall versión 7.4.0+ gestionado por FMC versión 7.4.0+ (Firepower serie 4200)
- Compatible con Secure Firewall versión 7.4.1+ gestionada por FMC versión 7.4.1+ (todas las demás plataformas)
- Solo se admiten aplicaciones web (HTTPS). No se admiten escenarios que requieran una exención de descifrado
- Sólo admite IDp de SAML
- Se requieren actualizaciones de DNS públicas para el acceso remoto
- No se admite IPv6. No se admiten los escenarios NAT66, NAT64 y NAT46
- Esta función solo está disponible en Threat Defence si Snort 3 está activado
- Todos los hipervínculos de las aplicaciones Web protegidas deben tener una ruta de acceso relativa
- Las aplicaciones web protegidas que se ejecutan en un host virtual o detrás de equilibradores de carga internos deben utilizar la misma URL externa e interna
- No compatible con clústeres de modo individual
- No compatible con aplicaciones con validación estricta de encabezado de host HTTP habilitada

- Si el servidor de aplicaciones aloja varias aplicaciones y sirve contenido basado en el encabezado de indicación de nombre de servidor (SNI) en el saludo del cliente de TLS, la URL externa de la configuración de la aplicación de confianza cero debe coincidir con el SNI de esa aplicación específica
- Sólo se admite en modo enrutado
- Se requiere licencia inteligente (no funciona en modo de evaluación)

Para obtener más información y detalles sobre el acceso de confianza cero en Secure Firewall, consulte la [Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.4.](#)

Configurar

Este documento se centra en una implementación de acceso remoto de ZTNA.

En este ejemplo, los usuarios remotos requieren acceso a las interfaces de usuario web (UI) de un CSP de prueba y un Cisco Telemetry Broker (CTB) alojados detrás de un firewall seguro. El acceso a estas aplicaciones se concede mediante dos idPs diferentes: Duo y Microsoft Entra ID respectivamente, como se muestra en el siguiente diagrama.

Diagrama de la red

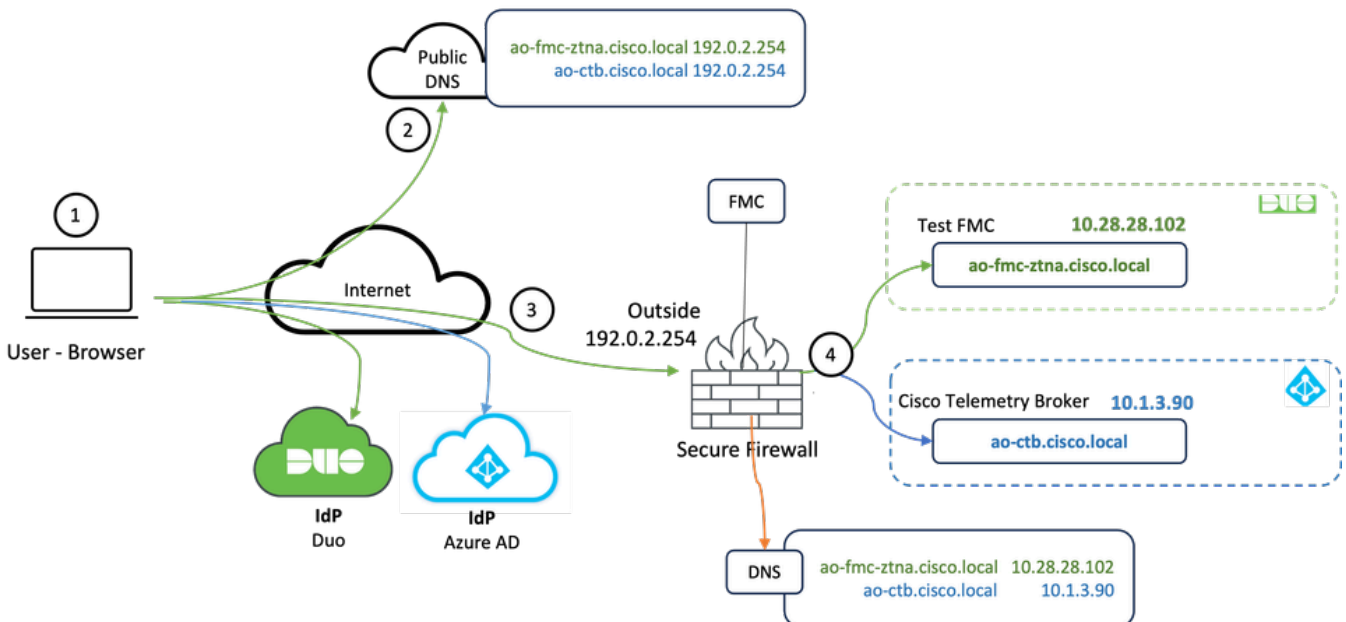


Diagrama de topología

1. Los usuarios remotos necesitan acceder a las aplicaciones alojadas detrás de Secure Firewall.
2. Cada aplicación debe tener una entrada DNS en los servidores DNS públicos.
3. Estos nombres de aplicación se deben resolver en la dirección IP de la interfaz externa de Secure Firewall.
4. Secure Firewall se resuelve en las direcciones IP reales de las aplicaciones y autentica a

cada usuario en cada aplicación mediante la autenticación SAML.

Configuración de Prerrequisitos

Proveedor de identidad (IdP) y servidor de nombres de dominio (DNS)

- Las aplicaciones o grupos de aplicaciones deben configurarse en un proveedor de identidad SAML (IdP) como Duo, Okta o Azure AD. En este ejemplo, Duo y Microsoft Entra ID se utilizan como IdPs.
- El certificado y los metadatos generados por los IdPs se utilizan al configurar la aplicación en Secure Firewall

Servidores DNS internos y externos

- Los servidores DNS externos (utilizados por usuarios remotos) deben tener la entrada FQDN de las aplicaciones y resolverse en la dirección IP de la interfaz externa de Secure Firewall
- Los servidores DNS internos (utilizados por Secure Firewall) deben tener la entrada FQDN de las aplicaciones y resolver la dirección IP real de la aplicación

Certificados

Los siguientes certificados son necesarios para la configuración de la política ZTNA:

- Certificado de identidad/proxy: utilizado por Secure Firewall para enmascarar las aplicaciones. El firewall seguro actúa aquí como proveedor de servicios SAML (SP). Este certificado debe ser un comodín o un certificado de nombre alternativo del sujeto (SAN) que coincida con el FQDN de las aplicaciones privadas (un certificado común que representa todas las aplicaciones privadas en la fase de autenticación previa)
- Certificado IdP: El IdP utilizado para la autenticación proporciona un certificado para cada aplicación o grupo de aplicaciones definido. Este certificado debe configurarse de modo que el firewall seguro
Es capaz de verificar la firma del IdP en las afirmaciones SAML entrantes (si esto se define para un grupo de aplicaciones, el mismo certificado se utiliza para todo el grupo de aplicaciones)
- Certificado de aplicación: el tráfico cifrado desde el usuario remoto a la aplicación debe ser descifrado por Secure Firewall, por lo tanto, la cadena de certificados y la clave privada de cada aplicación deben agregarse a Secure Firewall.

Configuraciones generales

Para configurar una nueva aplicación de confianza cero, lleve a cabo los siguientes pasos:

1. Navegue hasta Políticas > Control de acceso > Aplicación de confianza cero y haga clic en

Agregar política.

2. Complete los campos obligatorios:

a) General: Introduzca el nombre y la descripción de la política.

b) Nombre de dominio: Nombre que se agrega al DNS y que debe resolverse en la interfaz del gateway de defensa contra amenazas desde la que se accede a las aplicaciones.



Nota: El nombre de dominio se utiliza para generar la URL de ACS para todas las aplicaciones privadas de un grupo de aplicaciones.

c) Certificado de identidad: se trata de un certificado común que representa todas las aplicaciones privadas en la fase previa a la autenticación.



Nota: este certificado debe ser un comodín o un certificado de nombre alternativo del sujeto (SAN) que coincida con el FQDN de las aplicaciones privadas.

d) Zonas de seguridad: Seleccione las zonas exteriores y/o interiores a través de las cuales se regulan las aplicaciones privadas.

e) Conjunto de puertos global: el puerto único de este conjunto se asigna a cada aplicación privada.

f) Controles de seguridad (opcional): seleccione esta opción si las aplicaciones privadas están sujetas a inspección.

En esta configuración de ejemplo, se ingresó la siguiente información:

Firewall Management Center
Policies / Access Control / Zero Trust Application

Overview Analysis Policies Devices Objects Integration

Deploy Q [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

IP

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.

El certificado de identidad/proxy utilizado en este caso es un certificado comodín para coincidir con el FQDN de las aplicaciones privadas:

Firewall Management Center
Devices / Certificates

Overview Analysis Policies Devices Objects Integration

Deploy Q [admin] SECURE

Filter: All Certificates Add

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: [redacted]
 - DC: [redacted]
 - DC: [redacted]
- Issued To:
 - CN: *.cisco.local
 - OU: TAC
 - O: Cisco
 - ST: [redacted]
 - C: [redacted]
- 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. Guarde la directiva.

4. Cree los nuevos grupos de aplicaciones y/o las nuevas aplicaciones:

- Una Aplicación define una aplicación web privada con autenticación SAML, acceso a la interfaz, intrusión y políticas de Malware y Archivo.
- Un grupo de aplicaciones permite agrupar varias aplicaciones y compartir configuraciones comunes como la autenticación SAML, el acceso a la interfaz y la configuración de control de seguridad.

En este ejemplo, se configuran dos grupos de aplicaciones diferentes y dos aplicaciones diferentes: una para que Duo autentique la aplicación (interfaz de usuario web de prueba de FMC) y otra para que Microsoft Entra ID (interfaz de usuario web de CTB) autentique la aplicación.

Configurar grupo de aplicaciones

Grupo de aplicaciones 1: Uso de Duo como IdP

a. Introduzca el nombre del grupo de aplicaciones y haga clic en Siguiente para que se muestren los metadatos del proveedor de servicios (SP) de SAML.

Add Application Group ⓘ ✕

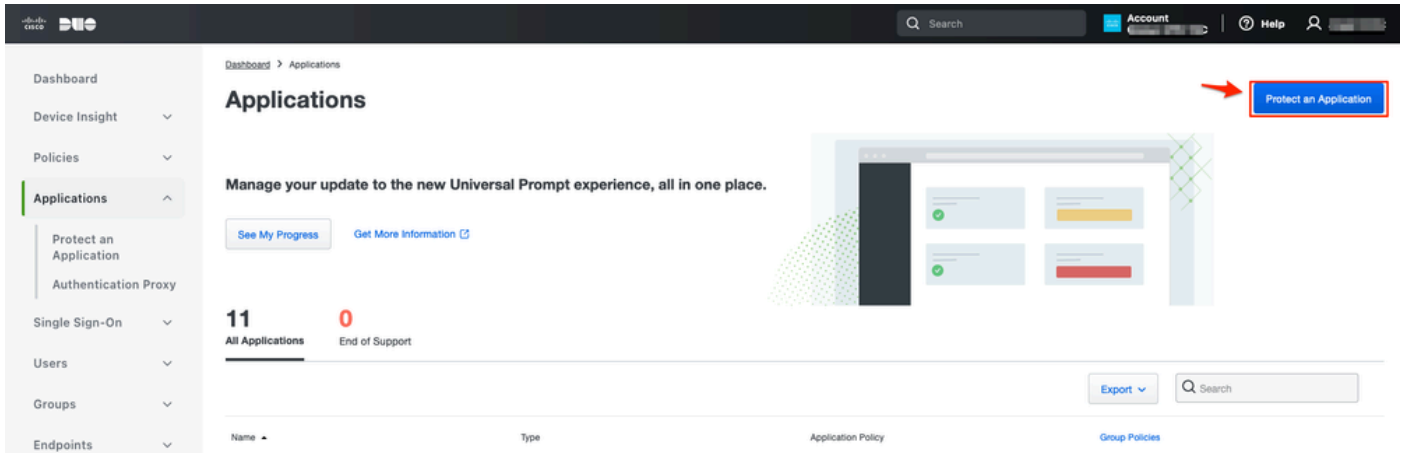
An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- 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: Copy
Assertion Consumer Service (ACS) URL: Copy
Download SP Metadata Next
- 3 SAML Identity Provider (IdP) Metadata**
- 4 Re-Authentication Interval**
- 5 Security Zones and Security Controls**

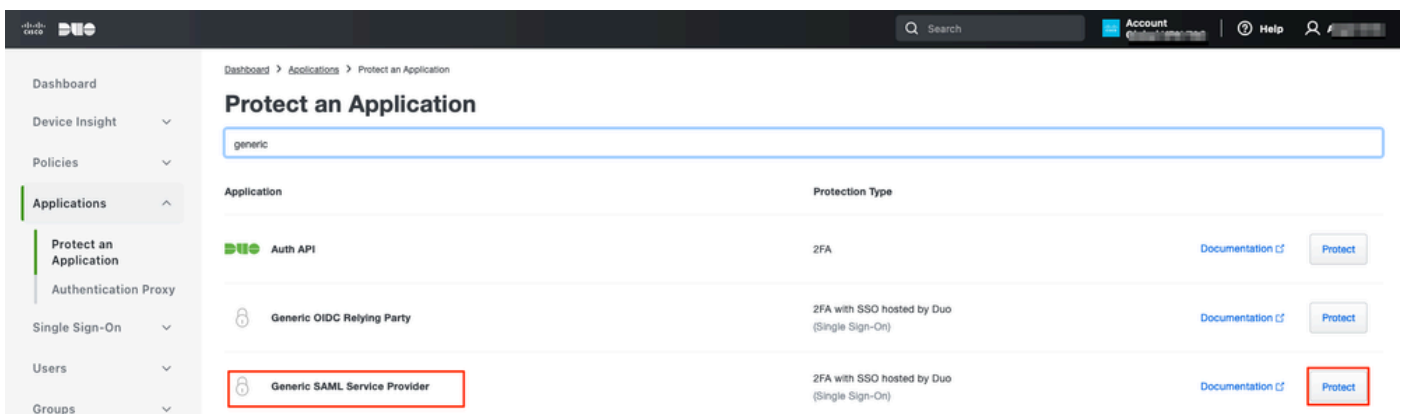
Cancel Finish

b. Una vez que se muestre los metadatos SP de SAML, vaya al IdP y configure una nueva aplicación SSO de SAML.

c. Inicie sesión en Duo y navegue hasta Aplicaciones > Proteger una aplicación.



d. Busque el proveedor de servicios SAML genérico y haga clic en Proteger.



e. Descargue el certificado y los metadatos SAML del IdP, ya que es necesario para continuar la configuración en Secure Firewall.

f. Introduzca la ID de entidad y la URL de servicio de consumo de aserción (ACS) del grupo de aplicaciones ZTNA (generado en el paso 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	<input type="text" value="https://sso-.../metadata"/>	Copy
Single Sign-On URL	<input type="text" value="https://sso-8.../sso"/>	Copy
Single Log-Out URL	<input type="text" value="https://sso-i.../slo"/>	Copy
Metadata URL	<input type="text" value="https://sso-8.../metadata"/>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<input type="text" value="9E:5...5C"/>	Copy
SHA-256 Fingerprint	<input type="text" value="7:85:...E9:52"/>	Copy

Downloads

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

Service Provider

Metadata Discovery

[Early Access](#)

Entity ID *

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

[+ Add an ACS URL](#)

g. Edite la aplicación de acuerdo con sus requisitos específicos y permita el acceso a la aplicación solo a los usuarios previstos y haga clic en Guardar.

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. Navegue de nuevo al FMC y agregue los metadatos de IdP de SAML al grupo de aplicaciones, usando los archivos descargados del 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?tname=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. Haga clic en Next y configure el Intervalo de Reautenticación y los Controles de Seguridad según sus requisitos. Revise la configuración del resumen y haga clic en 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?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

Grupo de aplicaciones 2: usar Microsoft Entra ID (Azure AD) como IdP

a. Introduzca el nombre del grupo de aplicaciones y haga clic en Siguiente para que se muestren los metadatos del proveedor de servicios (SP) de SAML.

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. Una vez que se muestre los metadatos SP de SAML, vaya al IdP y configure una nueva aplicación SSO de SAML.

c. Inicie sesión en Microsoft Azure y navegue hasta Aplicaciones empresariales > Nueva aplicación.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Enterprise applications

Enterprise applications | All applications

Microsoft Entra ID

+ New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Application proxy

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

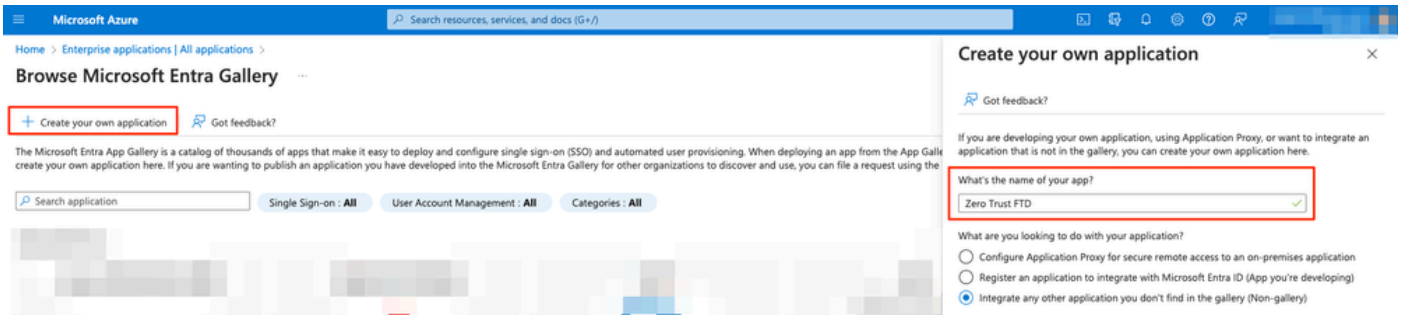
The list of applications that are maintained by your organization are in [application registrations](#).

Search by application name or object ID Application type == Enterprise Applications Application ID starts with Add filters

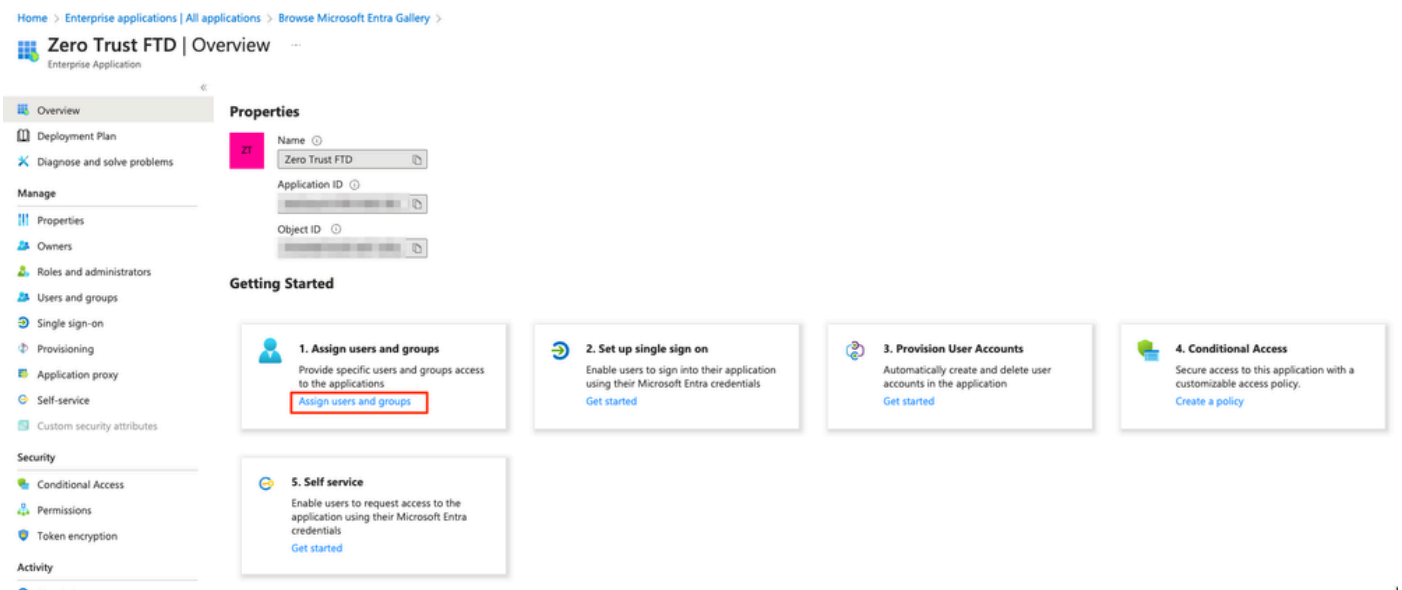
77 applications found

Name	Object ID	Application ID	Homepage URL	Created on
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

d. Haga clic en Create your own application > Enter the name of the application > Create



e. Abra la aplicación y haga clic en Asignar usuarios y grupos para definir los usuarios y/o grupos que tienen permiso para acceder a la aplicación.



f. Haga clic en Add user/group > Select the needed users/groups > Assign. Una vez que se hayan asignado los usuarios/grupos correctos, haga clic en Inicio de sesión único.

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
<input type="checkbox"/>	AO Angel	
<input type="checkbox"/>	FG Fernando	

g. Una vez en la sección Single Sign-on, haga clic en 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

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. Haga clic en Cargar archivo de metadatos y seleccione el archivo XML descargado del proveedor de servicios (Secure Firewall) o introduzca manualmente la ID de entidad y la URL de servicio de consumidor de afirmación (ACS) del grupo de aplicaciones ZTNA (generado en el paso a).

Nota: Asegúrese de descargar también el XML de metadatos de federación o de descargar individualmente el certificado (base 64) y de copiar los metadatos SAML del IdP (URL de inicio de sesión y cierre de sesión e identificadores de Microsoft Entra), ya que son necesarios para continuar la configuración en Secure Firewall.

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	Active	Edit
Status		
Thumbprint	[redacted]	
Expiration	[redacted]	
Notification Email	[redacted]	
App Federation Metadata Url	[redacted]	Download
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]	Copy
Microsoft Entra Identifier	https://[redacted]	Copy
Logout URL	https://[redacted]	Copy

i. Vuelva al FMC e importe los metadatos del IdP de SAML al grupo de aplicaciones 2, utilizando el archivo de metadatos descargado del IdP o introduzca manualmente los datos necesarios.

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. Haga clic en Next y configure el Intervalo de Reautenticación y los Controles de Seguridad según sus requisitos. Revise la configuración del resumen y haga clic en Finish.

Add Application Group ? X

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

Configurar aplicaciones

Ahora que se han creado los grupos de aplicaciones, haga clic en Add Application para definir las aplicaciones que se protegerán y a las que se accederá de forma remota.

1. Introduzca la configuración de la aplicación:

a) Nombre de la aplicación: Identificador de la aplicación configurada.

b) URL externa: URL publicada de la aplicación en los registros de DNS público/externo. Se trata de la URL que utilizan los usuarios para acceder a la aplicación de forma remota.

c) URL de la aplicación: FQDN real o IP de red de la aplicación. Se trata de la URL que utiliza Secure Firewall para acceder a la aplicación.

Nota: de forma predeterminada, la dirección URL externa se utiliza como dirección URL de la aplicación. Desmarque la casilla de verificación para especificar una URL de aplicación diferente.

d) Certificado de aplicación: la cadena de certificados y la clave privada de la aplicación a la

que se va a acceder (agregado desde la página de inicio de FMC > Objetos > Gestión de objetos > PKI > Certificados internos)

e) Origen NAT IPv4 (opcional): La dirección IP de origen del usuario remoto se traduce a las direcciones seleccionadas antes de reenviar los paquetes a la aplicación (solo se admiten objetos de red de tipo Host y Range o grupos de objetos con direcciones IPv4). Esto se puede configurar para garantizar que las aplicaciones tengan una ruta de vuelta a los usuarios remotos a través de Secure Firewall

f) Grupo de aplicaciones (opcional): seleccione esta opción si la aplicación se agrega a un grupo de aplicaciones existente para utilizar los parámetros configurados para ella.

En este ejemplo, las aplicaciones a las que se accederá mediante ZTNA son una interfaz de usuario Web de prueba de FMC y la interfaz de usuario Web de un CTB situado detrás de Secure Firewall.

Los certificados de las aplicaciones deben agregarse en Objetos > Administración de objetos > PKI > Certificados internos:

Add Known Internal Certificate



Name:

ao-fmc-ztna.cisco.local

Certificate Data or, choose a file:

Browse..

```
-----BEGIN CERTIFICATE-----  
[Redacted Certificate Data]  
T  
G  
1Y
```

Key or, choose a file:

Browse..

```
|-----BEGIN RSA PRIVATE KEY-----  
[Redacted Private Key Data]
```

Encrypted, and the password is:

.....

Cancel

Save

Nota: Asegúrese de agregar todos los certificados para cada aplicación a la que se vaya a acceder con ZTNA.

Una vez que los certificados se han agregado como certificados internos, continúe configurando los valores restantes.

Los valores de configuración de la aplicación configurados para este ejemplo son:

Aplicación 1: interfaz de usuario web de prueba FMC (miembro del grupo de aplicaciones 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

Cuando la aplicación se agregó al grupo de aplicaciones 1, el resto de la configuración se hereda para esta aplicación. Aún puede anular las zonas de seguridad y los controles de seguridad con parámetros diferentes.

Revise la aplicación configurada y haga clic en 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

Aplicación 2: interfaz de usuario web de CTB (miembro del grupo de aplicaciones 2)

El resumen de configuración de esta aplicación es el siguiente:

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





 Nota: Observe que para esta aplicación, un objeto de red "ZTNA_NAT_CTB" se configuró como origen NAT IPv4. Con esta configuración, la dirección IP de origen de los usuarios remotos se traduce a una dirección IP dentro del objeto configurado antes de reenviar los paquetes a la aplicación. Esto se configuró porque la ruta predeterminada de la aplicación (CTB) apunta a un gateway que no es el firewall seguro, por lo que el tráfico de retorno no se envió a los usuarios remotos. Con esta configuración de NAT, se configuró una ruta estática en la aplicación para que la subred ZTNA_NAT_CTB fuera accesible a través de Secure Firewall.

Una vez configuradas las aplicaciones, ahora se muestran en el grupo de aplicaciones correspondiente.

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	 


Por último, guarde los cambios e implemente la configuración.

Verificación

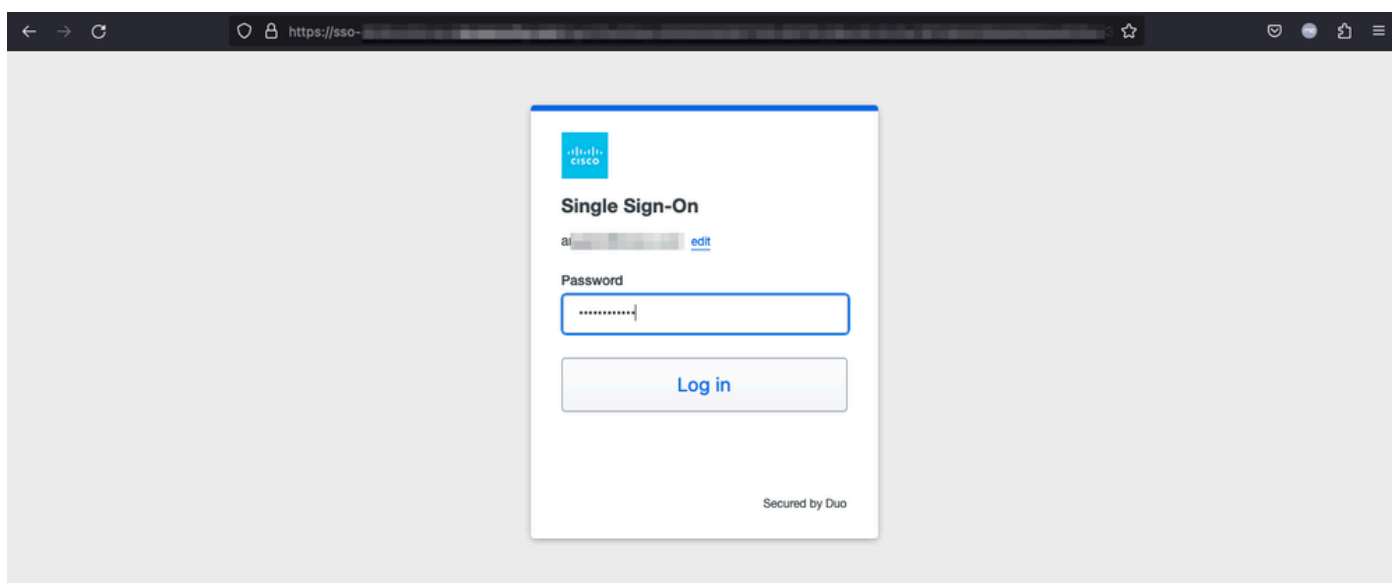
Una vez implementada la configuración, los usuarios remotos pueden acceder a las aplicaciones a través de la URL externa y, si el IdP correspondiente lo permite, tienen acceso a ella.

Aplicación 1

1. El usuario abre un navegador web y se desplaza a la URL externa de la aplicación 1. En este caso, la URL externa es "https://ao-fmc-ztna.cisco.local/"

 Nota: el nombre de URL externo debe resolverse en la dirección IP de la interfaz de Secure Firewall que se configuró. En este ejemplo, se resuelve en la dirección IP de la interfaz externa (192.0.2.254)

2. Como se trata de un nuevo acceso, el usuario es redirigido al portal de login IdP configurado para la aplicación.

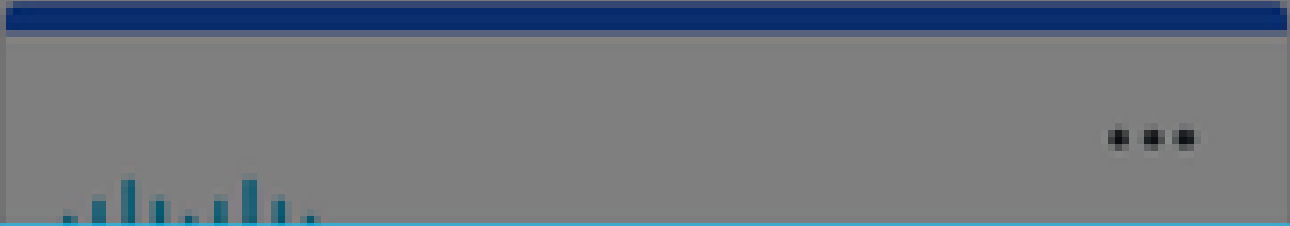


3. Se envía al usuario una transferencia para MFA (esto depende del método MFA configurado en el IdP).



Accounts

Add




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

 Global VPN TAC

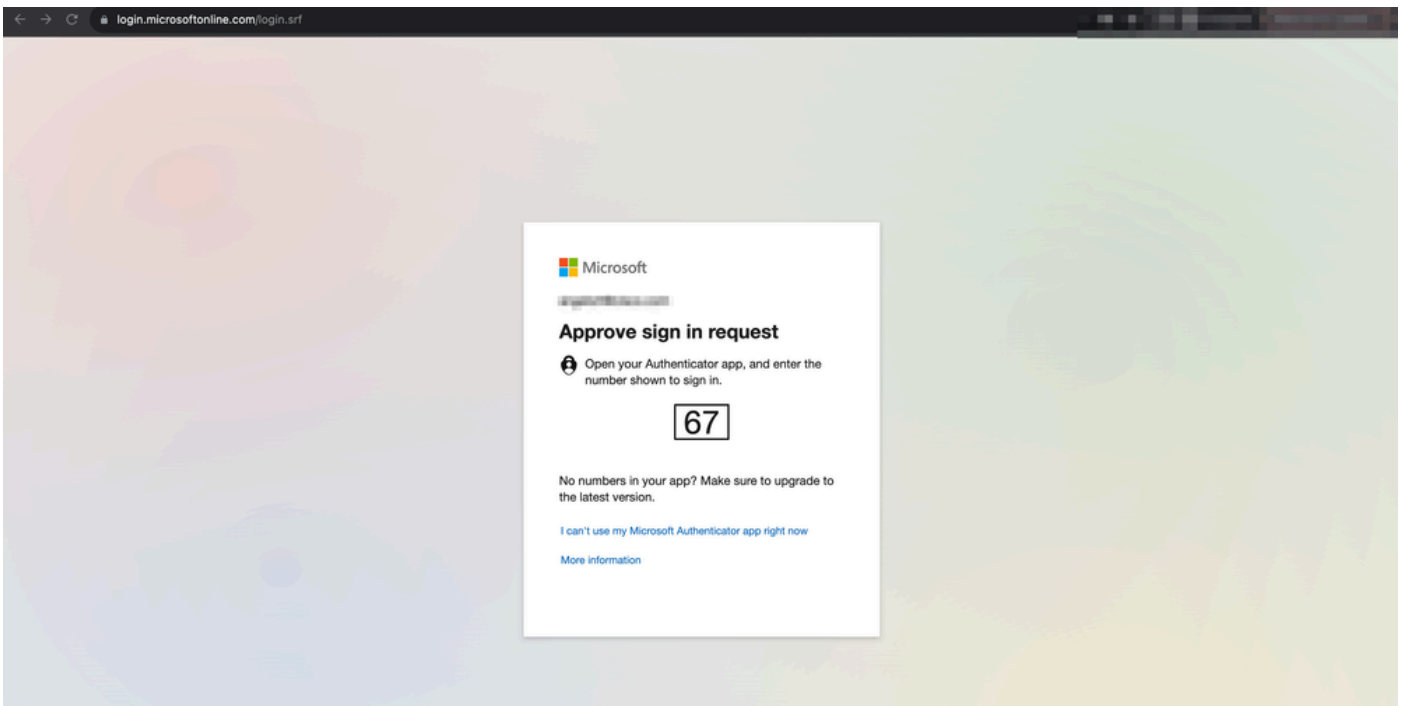
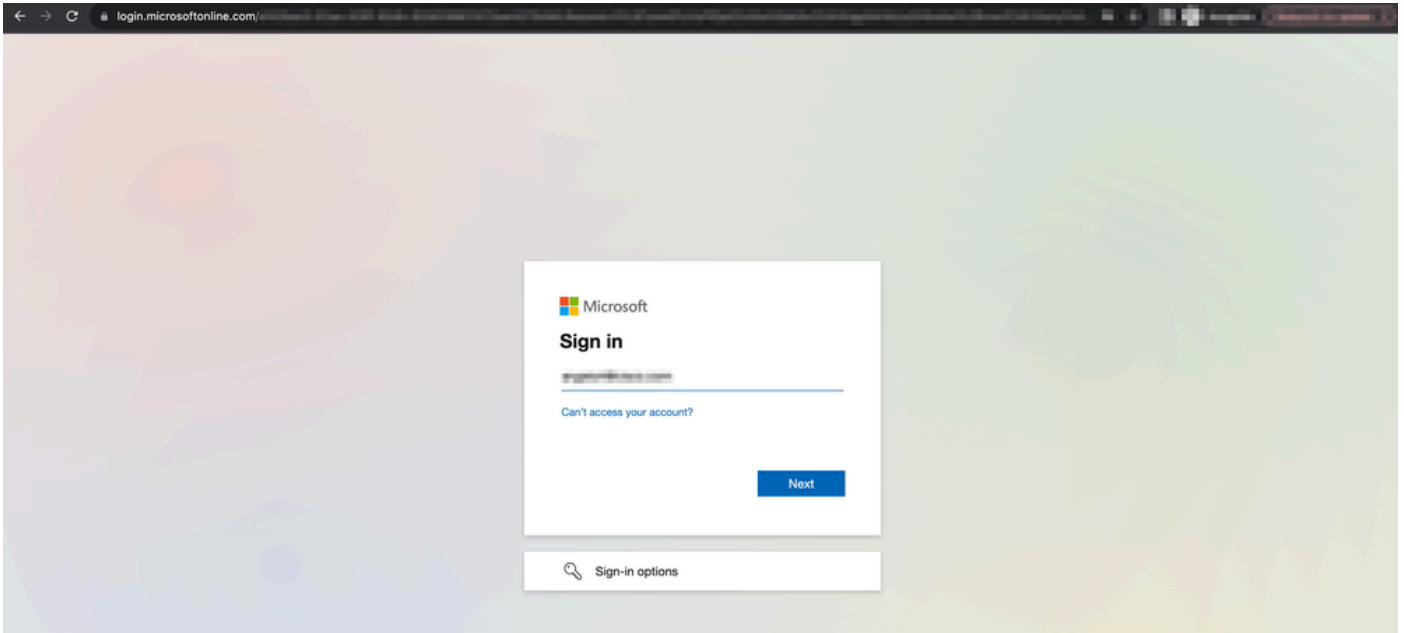
 [Redacted]

 1:13 p.m.

 [Redacted]

 : el nombre de URL externo debe resolverse en la dirección IP de la interfaz de Secure Firewall que se configuró. En este ejemplo, se resuelve en la dirección IP de la interfaz externa (192.0.2.254)

2. Como se trata de un nuevo acceso, el usuario es redirigido al portal de login IdP configurado para la aplicación.

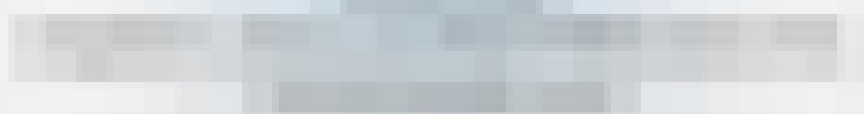


3. Se envía al usuario una transferencia para MFA (esto depende del método MFA configurado en el IdP).

4:24



Are you trying to sign in?



Enter the number shown to sign in.

Enter number

No, it's not me

Yes

- Los diagnósticos proporcionan un análisis general (correcto o no) y recopilan registros detallados que se pueden analizar para solucionar problemas

El diagnóstico específico de la aplicación se utiliza para detectar:



- Problemas relacionados con DNS
- Configuración incorrecta, por ejemplo, socket no abierto, reglas de clasificación, reglas NAT
- Problemas en la política de acceso de confianza cero
- Problemas relacionados con la interfaz, por ejemplo, interfaz no configurada o interfaz inactiva

Diagnósticos genéricos para detectar:

- Si no está habilitada una licencia de cifrado seguro
- Si el certificado de aplicación no es válido
- Si el método de autenticación no se inicializa en SAML en el grupo de túnel predeterminado
- Problemas de sincronización masiva de clústeres y HA
- Obtenga información de los contadores de snort para diagnosticar problemas, como los relacionados con tokens o descifrado
- Problema de agotamiento del grupo PAT en la traducción de origen.

Para ejecutar el diagnóstico:

1. Acceda al icono de diagnóstico presente para cada aplicación 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. Seleccione un dispositivo y haga clic en Ejecutar.

Select Device

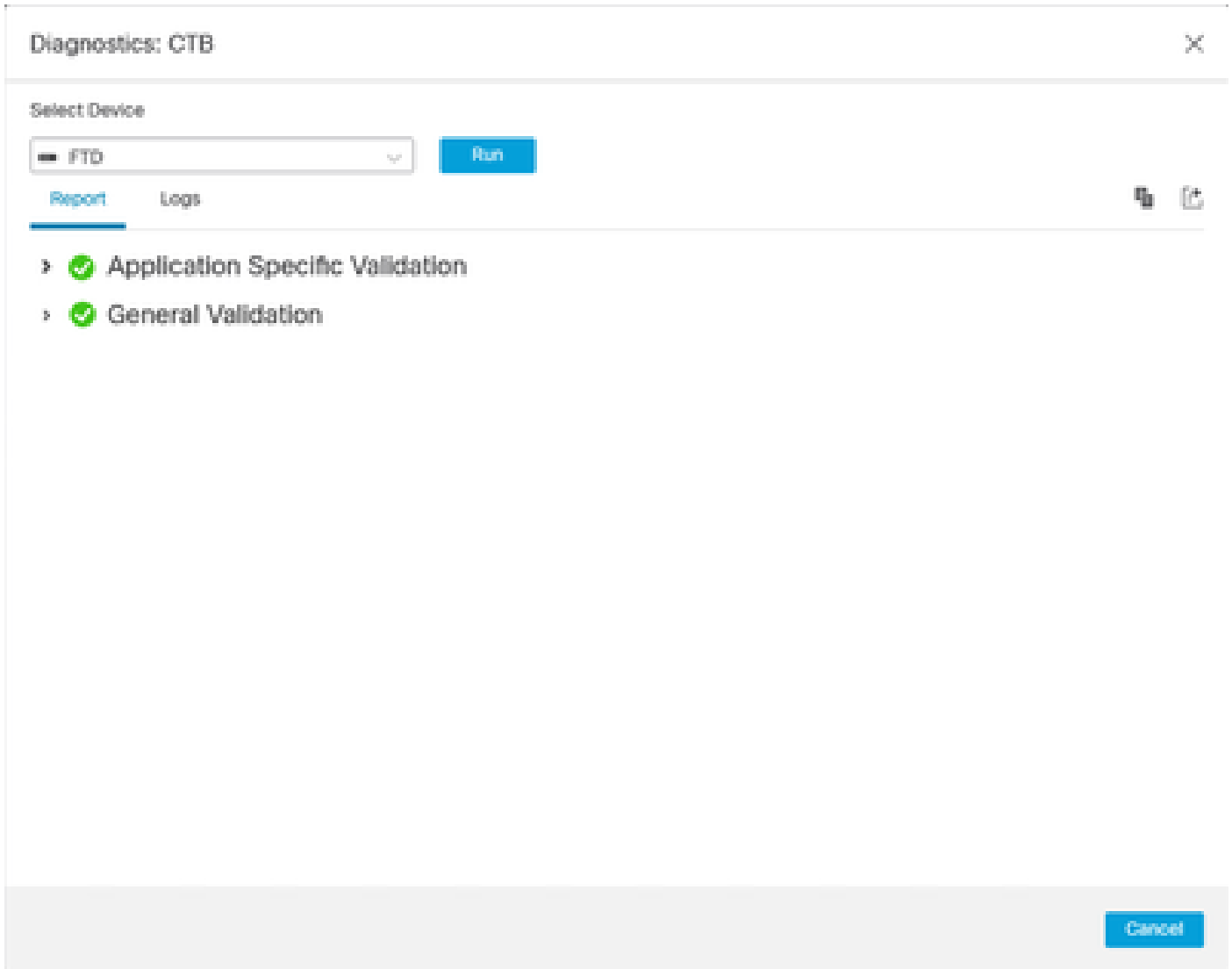
Select...

FTD

Run

Cancel

3. Consulte los resultados del informe.



Los comandos show y clear están disponibles en la CLI de FTD para ver la configuración de confianza cero y mostrar estadísticas e información de sesión.

```
<#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>
```

Para habilitar los debugs de módulo de confianza cero y webvpn, utilice los siguientes comandos en el prompt de línea:

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

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el centro de asistencia técnica (TAC). Se necesita un contrato de asistencia válido: [Contactos de asistencia globales de Cisco](#).
- También puede visitar la Comunidad VPN de Cisco [aquí](#).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).