

Configure Zero Trust Remote Access Deployment on Secure Firewall

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Prerequisite Configuration](#)

[General Configurations](#)

[Configure Application Group](#)

[Application Group 1: Using Duo as IdP](#)

[Application Group 2: Using Microsoft Entra ID \(Azure AD\) as IdP](#)

[Configure Applications](#)

[Application 1: Test FMC Web UI \(Member of the Application Group 1\)](#)

[Application 2: CTB Web UI \(Member of the Application Group 2\)](#)

[Verify](#)

[Monitor](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the process of configuring Clientless Zero Trust Access Remote Access deployment on a Secure Firewall.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- Secure Firewall Management Center (FMC)
- Basic ZTNA Knowledge
- Basic Security Assertion Markup Language (SAML) knowledge

Components Used

The information in this document is based on these software versions:

- Secure Firewall version 7.4.1

- Firepower Management Center (FMC) version 7.4.1
- Duo as Identity Provider (IdP)
- Microsoft Entra ID (formerly, Azure AD) as IdP

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Zero Trust Access feature is based on Zero Trust Network Access (ZTNA) principles. ZTNA is a zero trust security model that eliminates implicit trust. The model grants the least privilege access after verifying the user, the context of the request, and after analyzing the risk if access is granted.

The current requirements and limitations for ZTNA are:

- Supported on Secure Firewall version 7.4.0+ managed by FMC version 7.4.0+ (Firepower 4200 Series)
- Supported on Secure Firewall version 7.4.1+ managed by FMC version 7.4.1+ (All other platforms)
- Only web applications (HTTPS) are supported. Scenarios requiring decryption exemption are not supported
- Supports only SAML IdPs
- Public DNS updates are required for remote access
- IPv6 is not supported. NAT66, NAT64, and NAT46 scenarios are not supported
- The feature is available on threat defense only if Snort 3 is enabled
- All hyperlinks in protected web applications must have a relative path
- Protected web applications running on a virtual host or behind internal load balancers must use the same external and internal URL
- Not supported on individual mode clusters
- Not supported on applications with strict HTTP Host Header validation enabled
- If the application server hosts multiple applications and serves content based on the Server Name Indication (SNI) header in the TLS Client Hello, the external URL of the zero trust application configuration must match the SNI of that specific application
- Supported only in Routed Mode
- Smart License required (does not work in evaluation mode)

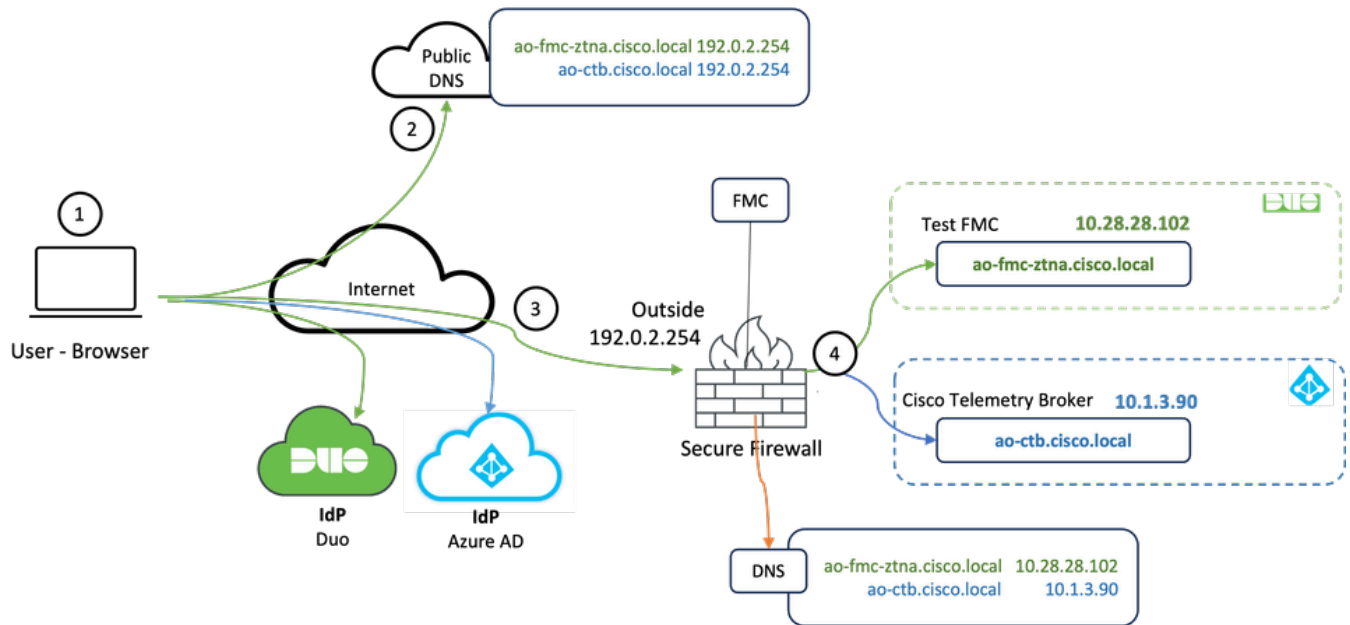
For more information and details about Zero Trust Access in Secure Firewall refer to the [Cisco Secure Firewall Management Center Device Configuration Guide, 7.4](#).

Configure

This document focuses on a Remote Access Deployment of ZTNA.

In this example scenario, remote users require access to the Web User Interfaces (UI) of a test FMC and a Cisco Telemetry Broker (CTB) which are hosted behind a Secure Firewall. Access to these applications is granted by two different IdPs: Duo & Microsoft Entra ID respectively, as shown in the next diagram.

Network Diagram



Topology diagram

1. The remote users need to access applications hosted behind the Secure Firewall.
2. Each application must have a DNS entry in the public DNS servers.
3. These application names must resolve to the IP address of the Secure Firewall Outside interface.
4. The Secure Firewall resolves to the real IP addresses of the applications and authenticates each user to each application using SAML authentication.

Prerequisite Configuration

Identity Provider (IdP) and Domain Name Server (DNS)

- The applications or application groups must be configured in a SAML Identity Provider (IdP) such as Duo, Okta, or Azure AD. In this example, Duo and Microsoft Entra ID are used as IdPs.
- The certificate and metadata generated by the IdPs is used when configuring the application on the Secure Firewall

Internal and external DNS servers

- External DNS servers (used by remote users) must have the FQDN entry of the applications, and resolve to the Secure Firewall outside interface IP address
- Internal DNS servers (used by Secure Firewall) must have the FQDN entry of the applications, and resolve to the real IP address of the application

Certificates

The next certificates are required for the ZTNA Policy configuration:

- **Identity/Proxy certificate:** Used by the Secure Firewall to masquerade the applications. The Secure Firewall here acts as a SAML Service Provider (SP). This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications (a common certificate that represents all the private applications at the pre-authentication stage)
- **IdP certificate:** The IdP used for authentication provides a certificate for each application or application group defined. This certificate must be configured so that the Secure Firewall is able to verify the IdP's signature on incoming SAML assertions (if this is defined for an application group, the same certificate is used for the entire group of applications)
- **Application certificate:** The encrypted traffic from the remote user to the application needs to be decrypted by the Secure Firewall, therefore, the certificate chain and private key of each application must be added to the Secure Firewall.


General Configurations

To configure a new Zero Trust Application, perform the next steps:

1. Navigate to **Policies > Access Control > Zero Trust Application** and click on **Add Policy**.
2. Complete the required fields:

a) **General:** Enter the name and description of the policy.

b) **Domain Name:** This is the name that is added to the DNS and must resolve to the threat defense gateway interface from where the applications are accessed.

 **Note:** The domain name is used to generate the ACS URL for all private applications in an Application Group.

c) **Identity certificate:** this is a common certificate that represents all the private applications at the pre-authentication stage.

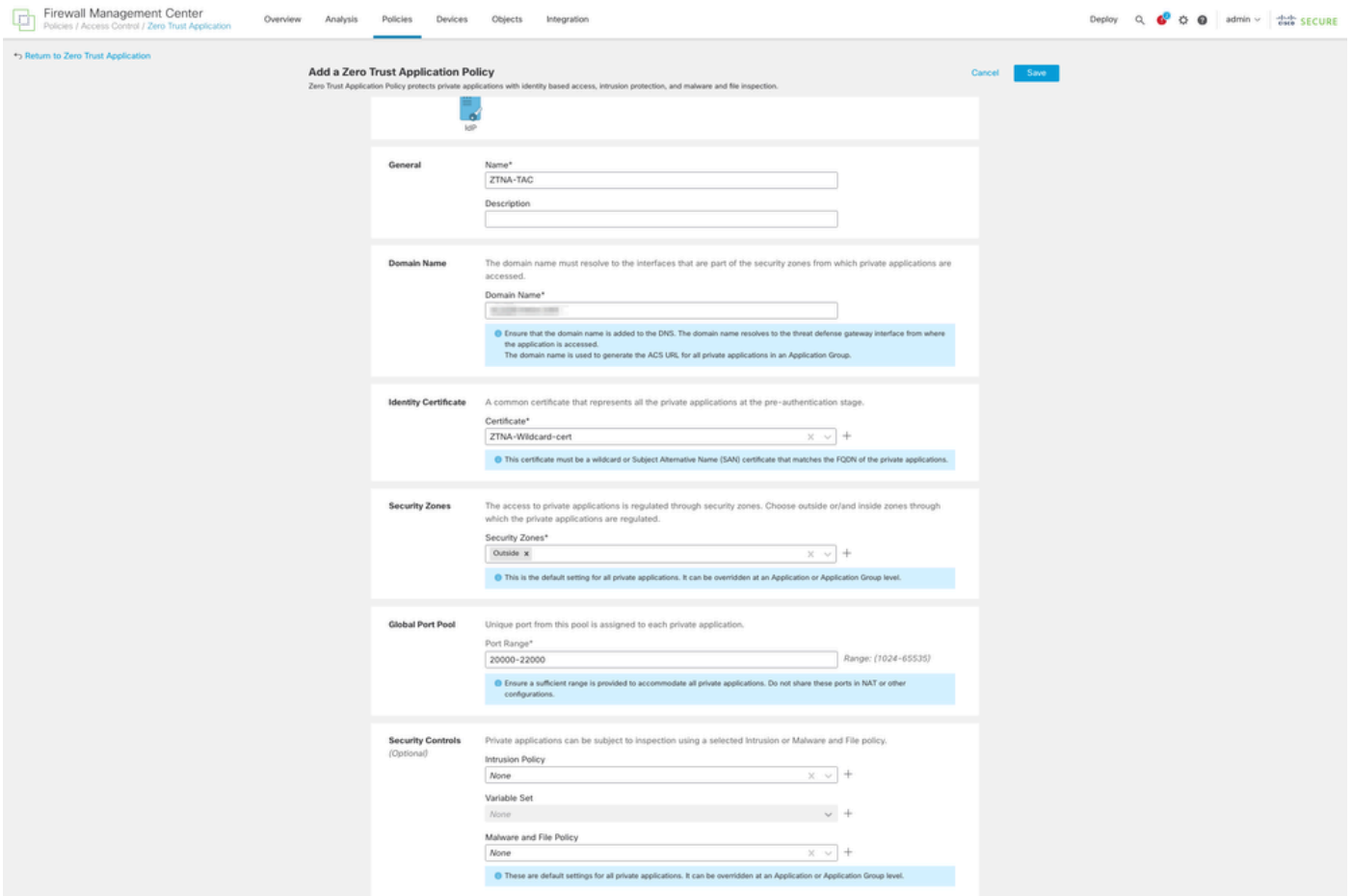
 **Note:** This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications.

d) **Security Zones:** Select outside or/and inside zones through which the private applications are regulated.

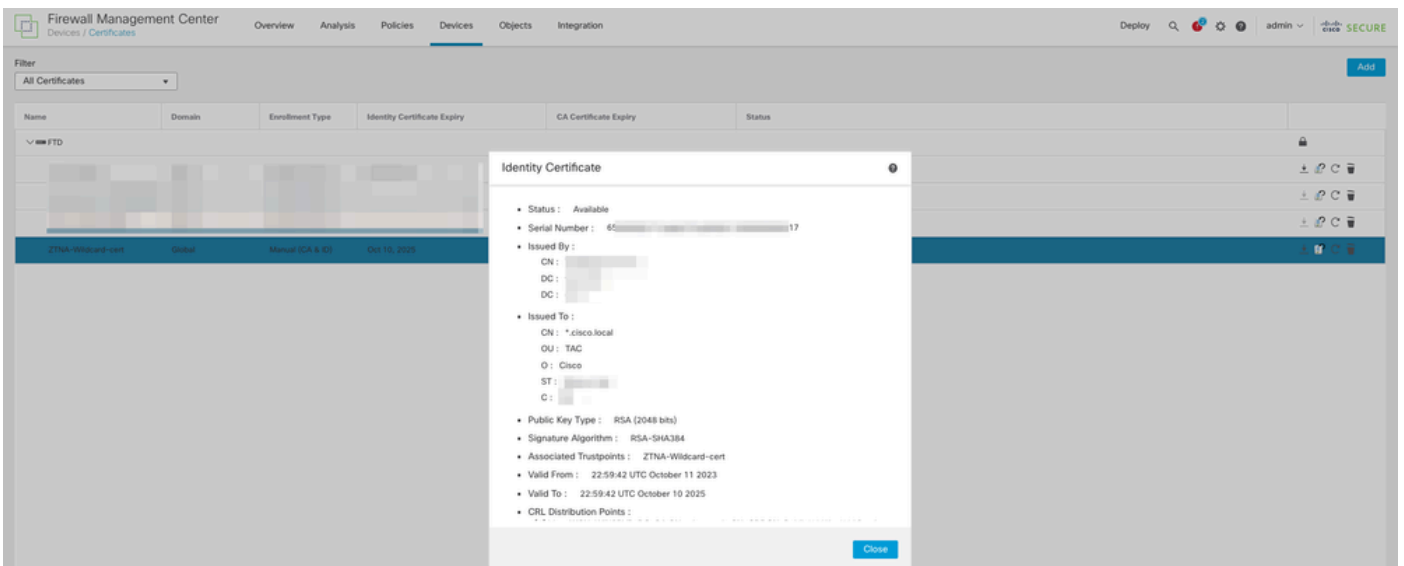
e) **Global Port Pool:** Unique port from this pool is assigned to each private application.

f) **Security Controls (optional):** Select if the private applications are subject to inspection.

In this sample configuration, the next information was entered:



The identity/proxy certificate used in this case is a wildcard certificate to match the FQDN of the private applications:



3. Save the policy.

4. Create the new Application Groups and/or new Applications:

- An **Application** defines a private web application with SAML authentication, interface access, Intrusion and Malware and File policies.
- An **Application Group** allows you to group multiple Applications, and share common settings such as SAML authentication, interface access, and security control settings.

In this example, two different application groups and two different applications are configured: one for the application to be authenticated by Duo (test FMC Web UI) & one for the application to be authenticated by Microsoft Entra ID (CTB Web UI).

Configure Application Group

Application Group 1: Using Duo as IdP

a. Enter the **Application Group Name** and click **Next** for the SAML Service Provider (SP) Metadata to be displayed.

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

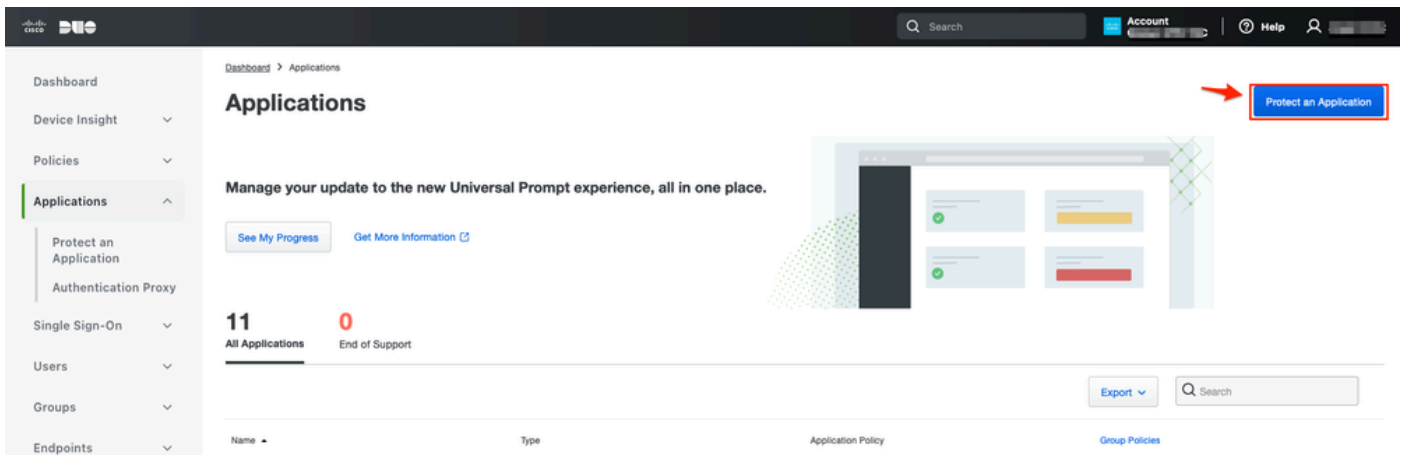
4 Re-Authentication Interval

5 Security Zones and Security Controls

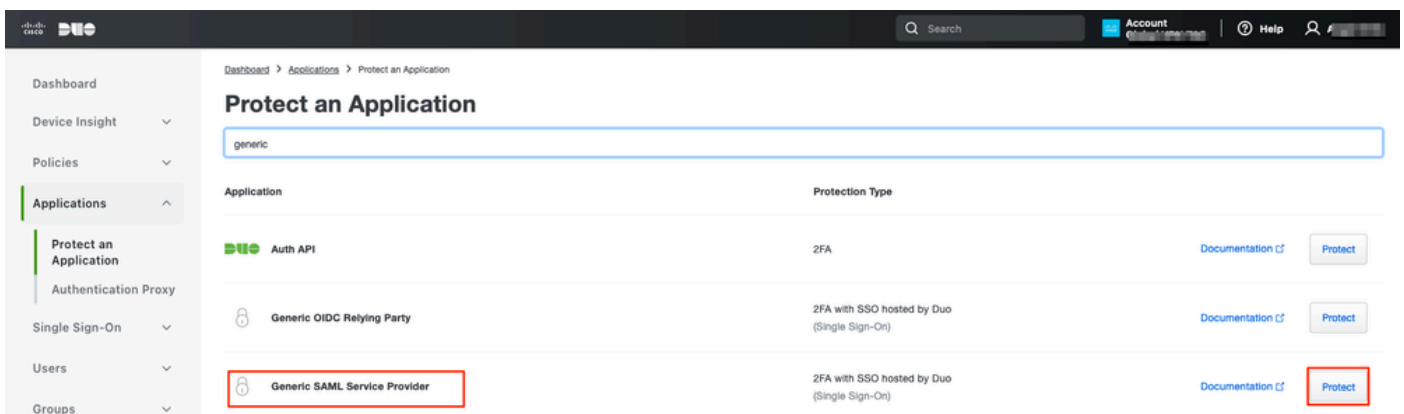
Cancel Finish

b. Once the SAML SP Metadata is displayed, go to the IdP and configure a new SAML SSO application.

c. Log in to Duo and navigate to **Applications > Protect an Application**.



d. Look for **Generic SAML Service Provider** and click **Protect**.



e. Download the Certificate and SAML Metadata from the IdP as it is required to continue the configuration on Secure Firewall.

f. Enter the **Entity ID** and **Assertion Consumer Service (ACS) URL** from the ZTNA Application Group (generated in **step 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. Edit the application in accordance to your specific requirements and allow access to the application only to the intended users and click **Save**.

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. Navigate back to the FMC and add the **SAML IdP Metadata** to the Application Group, using the files downloaded from the 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*
https://sso-8[redacted] N

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

IdP Certificate
MIIDDTC[redacted]yDQYJKoZI
[redacted]

Next

Cancel Finish

i. Click **Next** and configure the **Re-Authentication Interval** and **Security Controls** as per your requirements. Review the summary configuration and click **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

Application Group 2: Using Microsoft Entra ID (Azure AD) as IdP

a. Enter the **Application Group Name** and click **Next** for the SAML Service Provider (SP) Metadata to be displayed.

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

Cancel

Finish

b. Once the SAML SP Metadata is displayed, go to the IdP and configure a new SAML SSO application.

c. Log in to **Microsoft Azure** and navigate to **Enterprise applications > New Application**.

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.

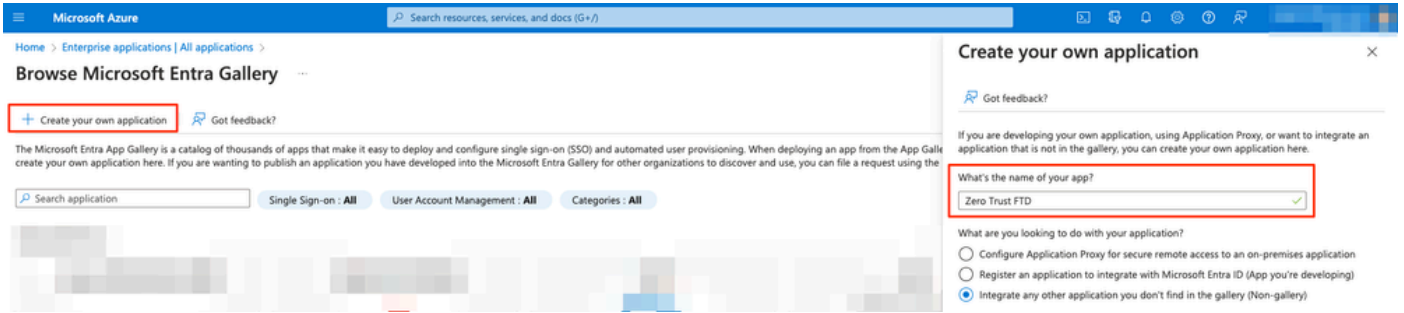
The list of applications that are maintained by your organization are in [application registrations](#).

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

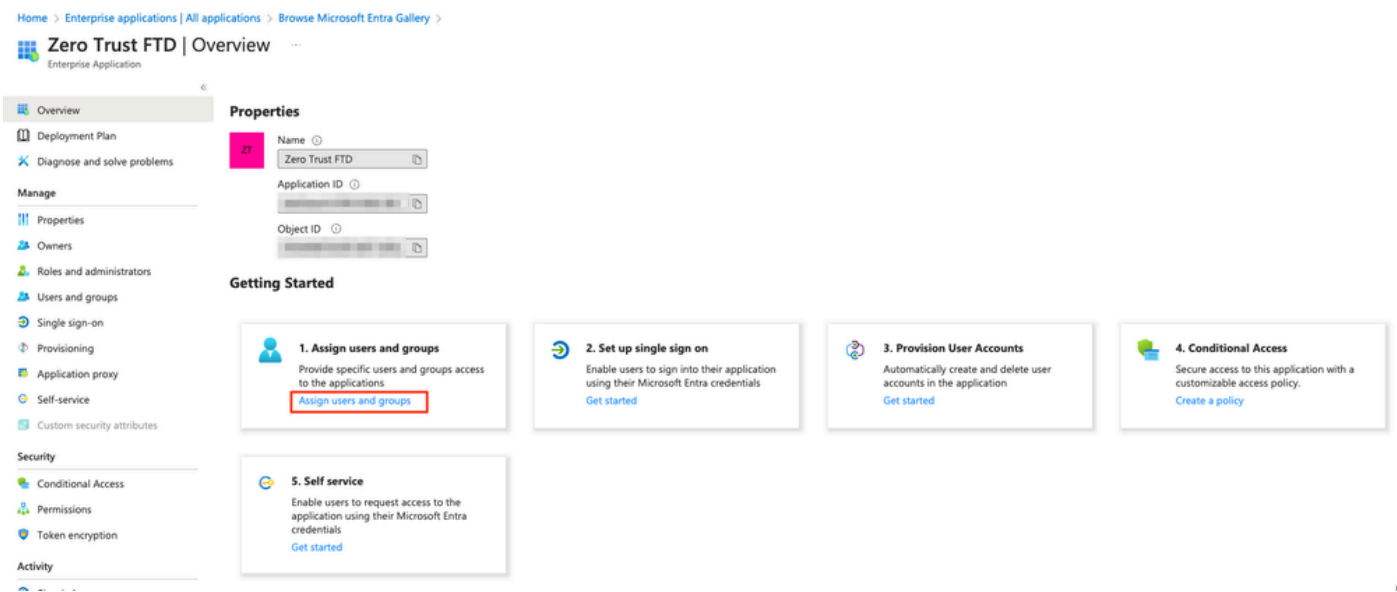
77 applications found

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

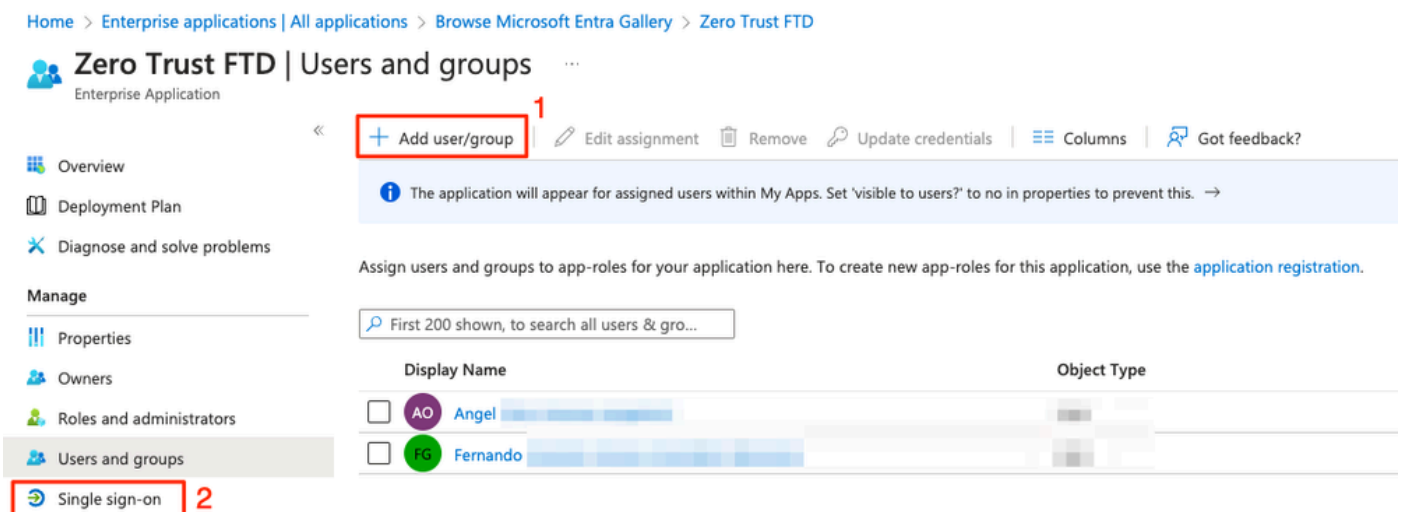
d. Click on **Create your own application > Enter the name of the application > Create**



e. Open the application and click on **Assign users and groups** to define the users and/or groups that are allowed to access the application.




f. Click on **Add user/group** > **Select the necessary users/groups** > **Assign**. Once the correct users/groups have been assigned, click on **Single sign-on**.



g. Once in the **Single sign-on** section, click on **SAML**.

The screenshot shows the Microsoft Entra ID console interface for configuring Single Sign-On (SSO) for an application named 'Zero Trust FTD'. The breadcrumb trail is: Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Zero Trust FTD. The page title is 'Zero Trust FTD | Single sign-on'. The left navigation pane includes: Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy). The main content area has a heading 'Select a single sign-on method' with a 'Help me decide' link. Below this are three options: 1. 'Disabled' (with a crossed-out circle icon) with the text: 'Single sign-on is not enabled. The user won't be able to launch the app from My Apps.' 2. 'SAML' (with a puzzle piece icon) which is highlighted with a red border, with the text: 'Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.' 3. 'Password-based' (with a lock icon) with the text: 'Password storage and replay using a web browser extension or mobile app.'

h. Click on **Upload metadata file** and select the XML file downloaded from the Service Provider (Secure Firewall) or manually enter the **Entity ID** and **Assertion Consumer Service (ACS) URL** from the ZTNA Application Group (generated in **step a**).

 **Note:** Ensure to also download the Federation Metadata XML or individually download the the Certificate (base 64) and copy the SAML Metadata from the IdP (Login & Logout URLs and Microsoft Entra Identifiers) as these are required to continue the configuration on the 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?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	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]	Download
Microsoft Entra Identifier	https://[redacted]	Download
Logout URL	https://[redacted]	Download

i. Navigate back to the FMC and import the **SAML IdP Metadata** to the Application Group 2, using the metadata file downloaded from the IdP or manually enter the required data.

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. Click **Next** and configure the **Re-Authentication Interval** and **Security Controls** as per your requirements. Review the summary configuration and click **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

Configure Applications

Now that the Application Groups have been created, click **Add Application** to define the applications to be protected and accessed remotely.

1. Enter the Application Settings:

a) **Application Name:** Identifier for the configured application.

b) **External URL:** Published URL of the application in the public/external DNS records. This is the URL used by users to access the application remotely.

c) **Application URL:** Real FQDN or Network IP of the application. This is the URL used by Secure Firewall to reach the application.

Note: By default, the External URL is used as Application URL. Uncheck the checkbox to specify a different Application URL.

d) **Application Certificate:** the certificate chain and private key of the application to be accessed (Added from **FMC Home Page > Objects > Object Management > PKI > Internal certs**)

e) **IPv4 NAT Source (optional):** The source IP address from the remote user is translated to the selected addresses before forwarding the packets to the application (only Host and Range type network objects/object-groups having IPv4 addresses are supported). This can be configured to ensure that the applications have a route back to the remote users through the Secure Firewall

f) **Application Group (optional):** Select if this Application is added to an existing Application Group to use the settings configured for it.

In this example, the applications to be accessed using ZTNA are a test FMC Web UI and the Web UI of a CTB located behind the Secure Firewall.

The certificates of the Applications must be added in **Objects > Object Management > PKI > Internal certs:**

Add Known Internal Certificate ?

Name:


Certificate Data or, choose a file:

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

Key or, choose a file:

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

Encrypted, and the password is:

 **Note:** Ensure to add all the certificates for each application to be accessed with ZTNA.

Once the certificates have been added as **Internal Certs**, continue to configure the remaining settings.

The Application settings configured for this example are:

Application 1: Test FMC Web UI (Member of the Application Group 1)

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* ?
 x v +

IPv4 NAT Source ?
 v +

Application Group
 x v

[Next](#)
- SAML Service Provider (SP) Metadata
- SAML Identity Provider (IdP) Metadata
- Re-Authentication Interval
- Security Zones and Security Controls

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

As the Application was added to the Application Group 1, the remaining settings are inherited for this application. You can still override the Security Zones and Security Controls with different settings.

Review the configured Application and click **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: CTB Web UI (Member of the Application Group 2)

The configuration summary for this application is the next:

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

 **Note:** Notice that for this application, a network object "ZTNA_NAT_CTB" was configured as IPv4 NAT Source. With this configuration, the source IP address from the remote users is translated to an IP address within the configured object before forwarding the packets to the application. This was configured because the application (CTB) default route points to a gateway other than the Secure Firewall, therefore the return traffic was not sent to the remote users. With this NAT configuration, a static route was configured on the application for the subnet ZTNA_NAT_CTB to be reachable through the Secure Firewall.

After the applications have been configured, they are now displayed under the corresponding Application Group.

ZTNA-TAC Targeted: 1 device

Groups: 3 Applications:

Applications Settings

Bulk Actions Add Application Group Add Application

Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled
<input checked="" type="checkbox"/> Azure_apps (1 Application)			https://sts.cisco.local	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
<input checked="" type="checkbox"/> External_Duo (1 Application)			https://sso.cisco.local	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


Finally, save the changes and deploy the configuration.

Verify

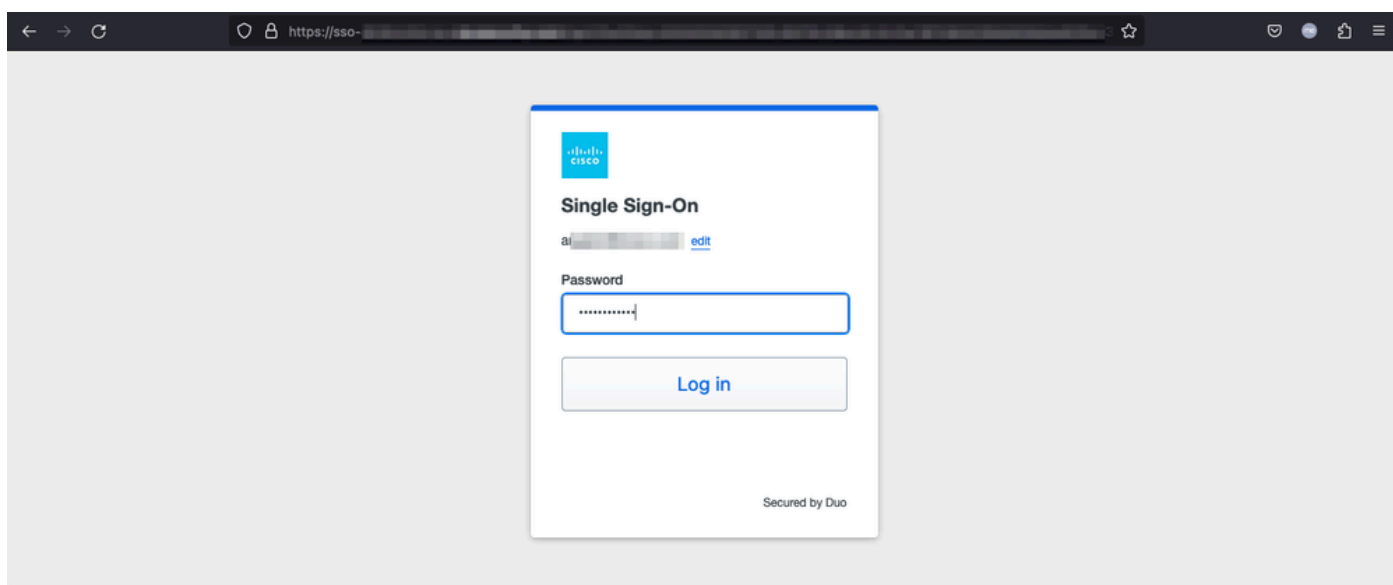
Once the configuration is in place, remote users can reach the applications through the external URL and if they are allowed by the corresponding IdP, have access to it.

Application 1

1. The user opens a web browser and navigates to the external URL of the application 1. In this case, the external URL is "https://ao-fmc-ztna.cisco.local/"

 **Note:** The external URL name must resolve to the IP address of the Secure Firewall interface that was configured. In this example, it resolves to the Outside interface IP address (192.0.2.254)

2. As this is a new access, the user is redirected to the IdP login portal configured for the application.

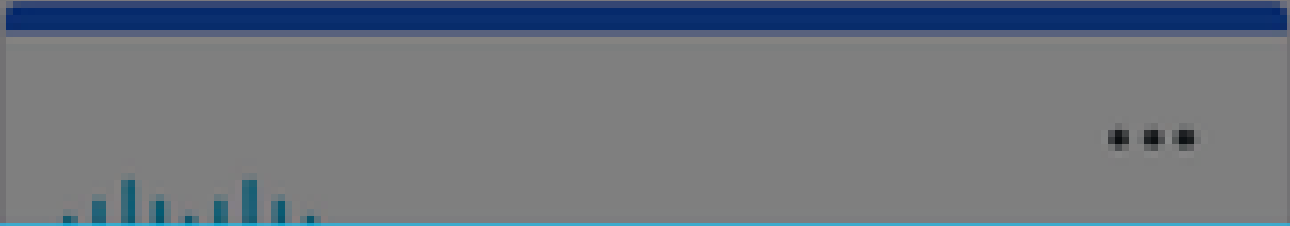


3. The user is sent a Push for MFA (this depends on the MFA method configured on the IdP).



Accounts

Add




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

 Global VPN TAC

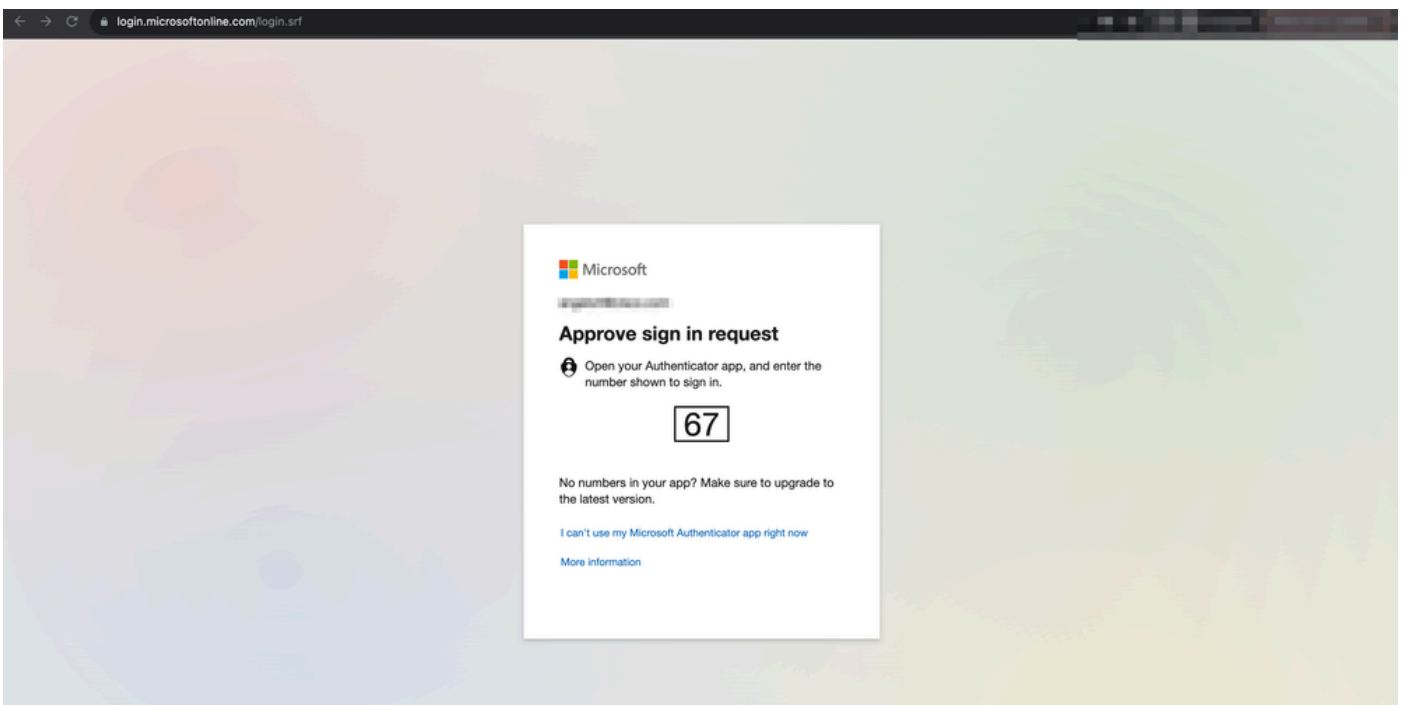
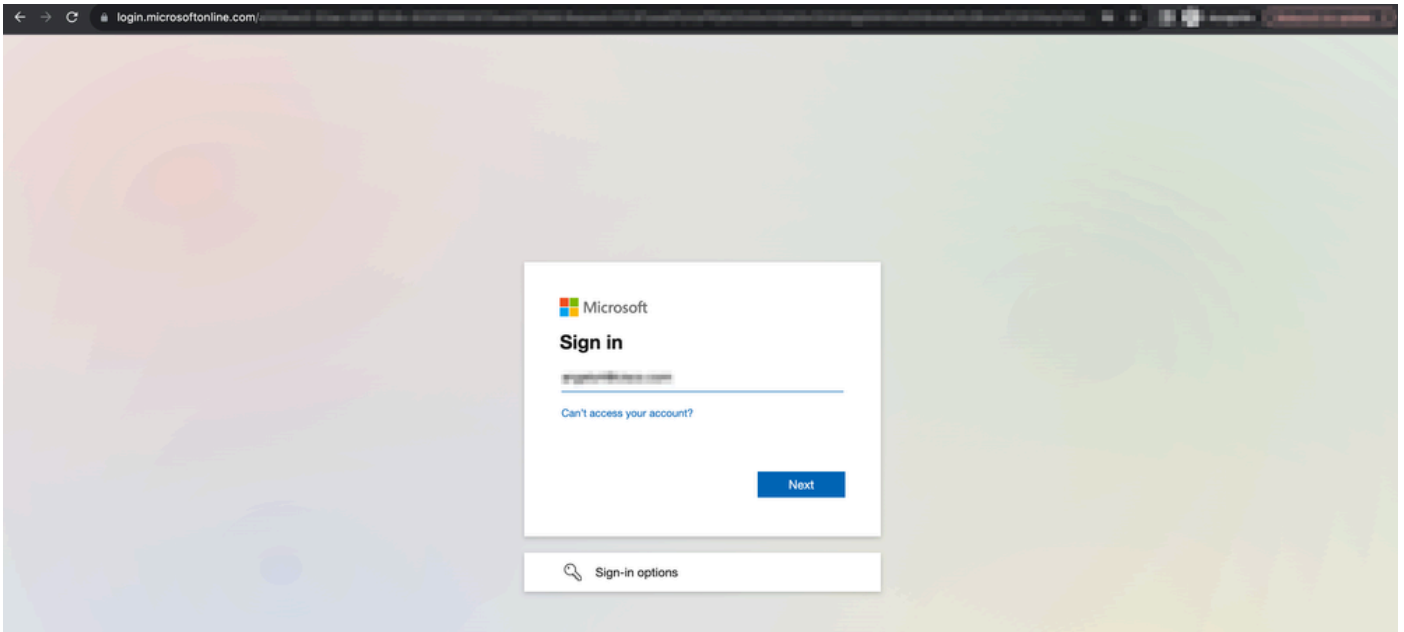
 [Redacted]

 1:13 p.m.

 [Redacted]

 : The external URL name must resolve to the IP address of the Secure Firewall interface that was configured. In this example, it resolves to the Outside interface IP address (192.0.2.254)

2. As this is a new access, the user is redirected to the IdP login portal configured for the application.

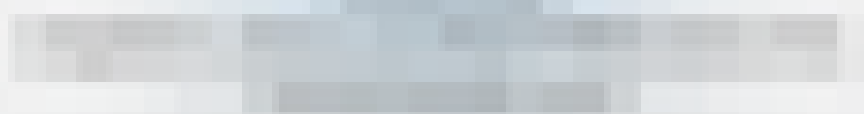


3. The user is sent a Push for MFA (this depends on the MFA method configured on the IdP).

4:24



Are you trying to sign in?



Enter the number shown to sign in.

No, it's not me

Yes

- Diagnostics provide overall analysis (OK or not) and collects detailed logs that can be analysed to solve issues

Application-specific Diagnostics is used to detect:

- DNS-related issues
- Misconfiguration, for example, socket not opened, classification rules, NAT rules
- Issues in Zero Trust Access Policy
- Interface-related issues, for example, interface not configured, or interface is down

Generic Diagnostics to detect:

- If a strong cipher license is not enabled
- If the application certificate is not valid
- If the authentication method is not initialised to SAML in the default tunnel group
- HA and cluster bulk sync issues
- Get insights from snort counters to diagnose issues, such as those related to tokens or decryption
- PAT pool exhaustion issue in source translation.

To run the diagnostics:

1. Navigate to the **diagnostics** icon present for each ZTNA Application.

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)		
CTB				Outside (Inherited)	None (Inherited)	None (Inherited)	True	Diagnostics
External_Duo (1 Application)				Outside (Inherited)	None (Inherited)	None (Inherited)		
FMC				Outside (Inherited)	None (Inherited)	None (Inherited)	True	

2. Select a device and click **Run**.

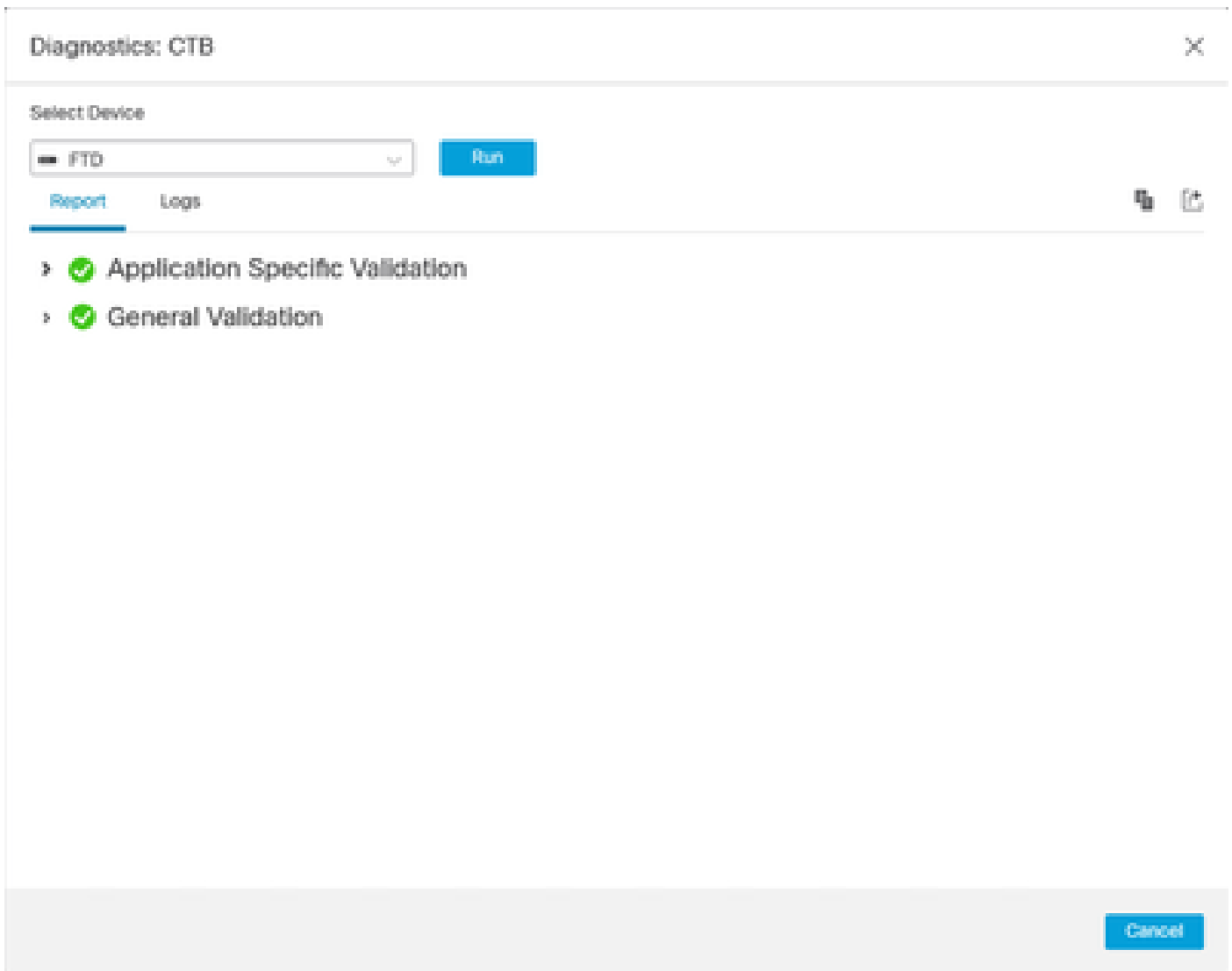
Select Device

Select...
FTD

Run

Cancel

3. View the results in the report.



If you need to work with Cisco Technical Assistance Center (TAC) for troubleshooting purposes, please collect the output of the next debug and show commands:

- **show counters protocol zero-trust**
- **debug zero-trust 255**
- **debug webvpn request 255**
- **debug webvpn response 255**
- **debug webvpn saml 255**

Related Information

- For additional assistance, please contact TAC. A valid support contract is required: [Cisco Worldwide Support Contacts](#).
- You can also visit the Cisco VPN Community [here](#).