

Configureer de implementatie van Zero Trust Remote Access op beveiligde firewall

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie voorwaarde](#)

[Algemene configuraties](#)

[Toepassingsgroep configureren](#)

[Toepassingsgroep 1: Duo gebruiken als IDp](#)

[Toepassingsgroep 2: Microsoft Entra ID \(Azure AD\) gebruiken als IDP](#)

[Toepassingen configureren](#)

[Toepassing 1: Test FMC Web UI \(Lid van de Toepassingsgroep 1\)](#)

[Toepassing 2: CTB Web UI \(lid van de Toepassingsgroep 2\)](#)

[Verifiëren](#)

[Monitor \(bewaken\)](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het proces van het configureren van de implementatie van Clientless Zero Trust Access Remote Access op een beveiligde firewall.

Voorwaarden

Vereisten

Cisco raadt u aan kennis van deze onderwerpen te hebben:

- Firepower Management Center (FMC)
- Basiskennis van ZTNA
- Basiskennis van Security Assertion Markup Language (SAML)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Secure Firewall versie 7.4.1
- Firepower Management Center (FMC) versie 7.4.1
- Duo als Identity Provider (IDP)
- Microsoft Entra ID (voorheen Azure AD) als IDP

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Nul Trust Access-functie is gebaseerd op Zero Trust Network Access (ZTNA)-principes. ZTNA is een zero trust security model dat impliciet vertrouwen elimineert. Het model verleent de minst bevoorrechte toegang na het verifiëren van de gebruiker, de context van het verzoek, en na het analyseren van het risico indien toegang wordt verleend.

De huidige eisen en beperkingen voor ZTNA zijn:

- Ondersteund op Secure Firewall versie 7.4.0+ beheerd door FMC versie 7.4.0+ (Firepower 4200 Series)
- Ondersteund op Secure Firewall versie 7.4.1+ beheerd door FMC versie 7.4.1+ (Alle andere platforms)
- Alleen webtoepassingen (HTTPS) worden ondersteund. Scenario's waarvoor decryptie-vrijstelling nodig is, worden niet ondersteund
- Ondersteunt alleen SAML IDps
- Voor externe toegang zijn openbare DNS-updates vereist
- IPv6 wordt niet ondersteund. NAT66, NAT64 en NAT46-scenario's worden niet ondersteund
- Deze optie is alleen beschikbaar bij bescherming tegen bedreigingen als Snort 3 is ingeschakeld
- Alle hyperlinks in beveiligde webtoepassingen moeten een relatief pad hebben
- Beschermd webtoepassingen die op een virtuele host of achter interne taakverdelers worden uitgevoerd, moeten dezelfde externe en interne URL gebruiken
- Niet ondersteund op clusters met afzonderlijke modus
- Niet ondersteund op toepassingen waarvoor strikte HTTP-hostheadervalidatie is ingeschakeld

- Als de applicatieserver meerdere toepassingen host en inhoud serveert op basis van de Server Name Indication (SNI) header in de TLS client Hello, moet de externe URL van de zero trust applicatie configuratie overeenkomen met de SNI van die specifieke toepassing
- Alleen ondersteund in Routed Mode
- Smart License vereist (werkt niet in evaluatiemodus)

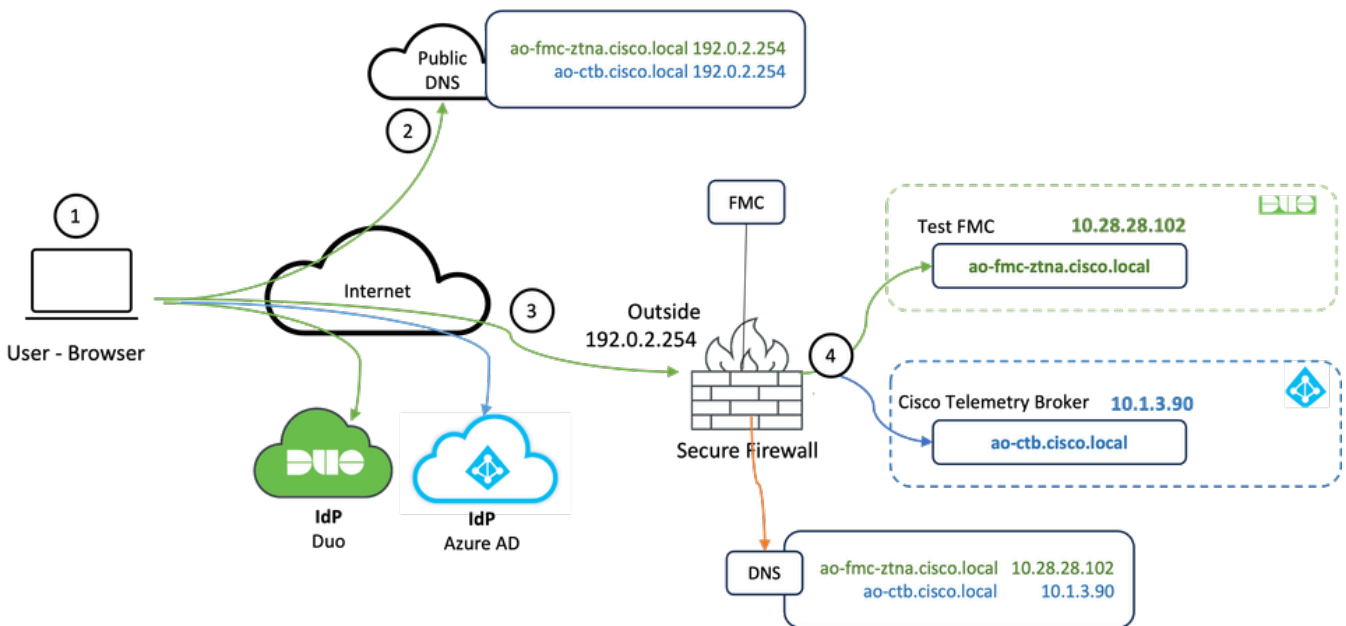
Raadpleeg voor meer informatie en informatie over Zero Trust Access in Secure Firewall de [Cisco Secure Firewall Management Center-configuratiehandleiding voor apparaten, 7.4](#).

Configureren

Dit document concentreert zich op een implementatie van ZTNA voor externe toegang.

In dit voorbeeldscenario vereisen externe gebruikers toegang tot de Web User Interfaces (UI) van een test-VCC en een Cisco Telemetry Broker (CTB) die worden gehost achter een beveiligde firewall. Toegang tot deze applicaties wordt verleend door twee verschillende IDPs: Duo & Microsoft Entra ID, zoals in het volgende diagram wordt getoond.

Netwerkdigram



Topologiediagram

1. De externe gebruikers moeten toegang hebben tot toepassingen die worden gehost achter de Secure Firewall.
2. Elke toepassing moet een DNS-ingang in de openbare DNS-servers hebben.
3. Deze applicatienamen moeten worden opgelost op het IP-adres van de Secure Firewall Outside interface.
4. De Secure Firewall lost op naar de echte IP-adressen van de toepassingen en verifieert elke gebruiker naar elke toepassing met behulp van SAML-verificatie.

Configuratie voorwaarde

Identity Provider (IDP) en Domain Name Server (DNS)

- De toepassingen of toepassingsgroepen moeten worden geconfigureerd in een SAML Identity Provider (IDP) zoals Duo, Okta of Azure AD. In dit voorbeeld worden Duo en Microsoft Entra ID gebruikt als IDps.
- Het certificaat en de metagegevens die door de ID's worden gegenereerd, worden gebruikt bij het configureren van de toepassing op de beveiligde firewall

Interne en externe DNS-servers

- Externe DNS-servers (gebruikt door externe gebruikers) moeten beschikken over de FQDN-ingang van de toepassingen en worden opgelost in de Secure Firewall buiten het IP-adres van de interface
- Interne DNS-servers (gebruikt door Secure Firewall) moeten beschikken over de FQDN-ingang van de toepassingen en deze oplossen naar het echte IP-adres van de toepassing

Certificaten

De volgende certificaten zijn vereist voor de ZTNA Policy-configuratie:

- Identity/Proxy-certificaat: gebruikt door de beveiligde firewall om de toepassingen te maskeren. De Secure Firewall fungeert hier als een SAML Service Provider (SP). Dit certificaat moet een jokerteken of een certificaat van de Alternatieve Naam van het Onderwerp (SAN) zijn dat met FQDN van de privé toepassingen (een gemeenschappelijk certificaat dat alle privé toepassingen in de pre-authenticatiestadium vertegenwoordigt) aanpast
- IDp-certificaat: De IDp die gebruikt wordt voor authenticatie biedt een certificaat voor elke toepassing of toepassingsgroep die gedefinieerd is. Dit certificaat moet zo worden geconfigureerd dat de Secure Firewall Kan de handtekening van IdP op inkomende SAML-beweringen verifiëren (als dit is gedefinieerd voor een toepassingsgroep, wordt hetzelfde certificaat gebruikt voor de gehele groep toepassingen)
- Toepassingscertificaat: het versleutelde verkeer van de externe gebruiker naar de applicatie moet worden gedecodeerd door de Secure Firewall. Daarom moeten de certificaatketen en de privésleutel van elke toepassing worden toegevoegd aan de Secure Firewall.

Algemene configuraties


Voer de volgende stappen uit om een nieuwe Zero Trust-toepassing te configureren:

1. Navigeer naar **Beleid > Toegangsbeheer > Nulvertrouwen Toepassing** en klik op **Beleid toevoegen**.


2. Vul de vereiste velden in:

a) Algemeen: naam en beschrijving van het contract.

b) Domeinnaam: Dit is de naam die wordt toegevoegd aan de DNS en moet oplossen aan de interface van de bedreigingsdefensie gateway waar de toepassingen worden betreden.

 Opmerking: De domeinnaam wordt gebruikt om de ACS-URL te genereren voor alle privé-toepassingen in een Toepassingsgroep.

c) Identificatiecertificaat: dit is een gemeenschappelijk certificaat dat alle particuliere toepassingen vertegenwoordigt in de fase voorafgaand aan de authenticatie.

 Opmerking: dit certificaat moet een jokerteken of een certificaat van de alternatieve naam van het onderwerp (SAN) zijn dat overeenkomt met de FQDN van de particuliere toepassingen.

d) Security Zones: Selecteer buiten of/en binnen zones waar de private applicaties worden gereguleerd.

e) Wereldwijde poortpool: unieke poort uit deze pool wordt toegewezen aan elke private toepassing.

f) Beveiligingscontroles (facultatief): Selecteer deze als de particuliere toepassingen worden geïnspecteerd.

In deze voorbeeldconfiguratie is de volgende informatie ingevoerd:

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

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.

Het identiteit/proxy-certificaat dat in dit geval wordt gebruikt, is een wildcard-certificaat dat overeenkomt met de FQDN van de particuliere toepassingen:

Firewall Management Center
Devices / Certificates

Overview Analysis Policies Devices Objects Integration

Deploy Q [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. Sla het beleid op.

4. De nieuwe toepassingsgroepen en/of nieuwe toepassingen maken:

- Een Applicatie definieert een private webapplicatie met SAML-verificatie, interfacetoegang, inbraakbeveiliging, malware- en bestandsbeleid.
- Een Toepassingsgroep stelt u in staat meerdere Toepassingen te groeperen en gemeenschappelijke instellingen te delen, zoals SAML-verificatie, interfacetoegang en instellingen voor beveiligingscontrole.

In dit voorbeeld worden twee verschillende toepassingsgroepen en twee verschillende toepassingen geconfigureerd: één voor de toepassing die moet worden geverifieerd door Duo (test FMC Web UI) en één voor de toepassing die moet worden geverifieerd door Microsoft Entra ID (CTB Web UI).

Toepassingsgroep configureren

Toepassingsgroep 1: Duo gebruiken als IDp

- a. Voer de naam van de toepassingsgroep in en klik op Volgende voor de weer te geven metagegevens van de SAML Service Provider (SP).

Add Application Group



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

- Application Group** Edit
Name: External_Duo
- 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

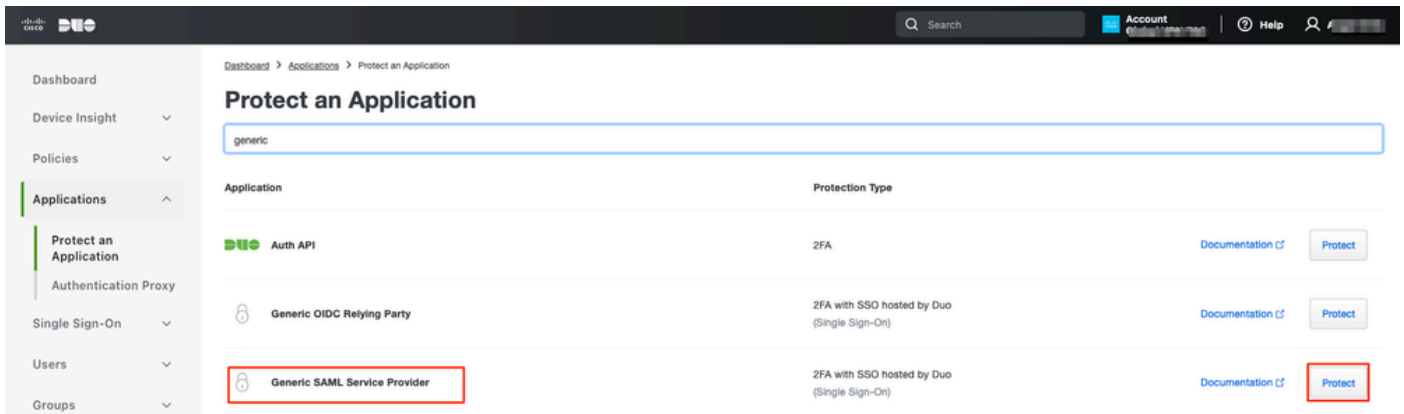
Cancel Finish

b. Zodra de metagegevens van SAML SP worden getoond, ga naar de IDp en vorm een nieuwe toepassing van SAML SSO.

c. Log in op Duo en navigeer naar Toepassingen > Bescherm een Toepassing.

The screenshot shows the Cisco Duo 'Applications' dashboard. The left sidebar contains navigation options: Dashboard, Device Insight, Policies, Applications (selected), Authentication Proxy, Single Sign-On, Users, Groups, and Endpoints. The main content area displays 'Applications' with a sub-header 'Manage your update to the new Universal Prompt experience, all in one place.' Below this, there are statistics: '11 All Applications' and '0 End of Support'. A 'Protect an Application' button is highlighted with a red box and an arrow. At the bottom, there is an 'Export' dropdown and a search bar.

d. Zoek naar Generic SAML Service Provider en klik op Protect.



e. Download het certificaat en de metagegevens van SAML van IDp aangezien het wordt vereist om de configuratie op Veilige Firewall voort te zetten.

f. Voer de URL van de entiteit-id en de ACS-URL (Assertion Consumer Service) in uit de ZTNA-toepassingsgroep (gegenereerd in stap 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. Bewerk de toepassing in overeenstemming met uw specifieke vereisten en geef alleen toegang tot de toepassing aan de beoogde gebruikers en klik op Opslaan.

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. Navigeer terug naar het VCC en voeg de metagegevens van SAML IDP toe aan de Toepassingsgroep met behulp van de bestanden die van de IDp zijn gedownload.

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. Klik op Volgende en configureer de herverificatie-interval en beveiligingscontroles volgens uw vereisten. Controleer de summiere configuratie en klik op Voltooien.

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

Toepassingsgroep 2: Microsoft Entra ID (Azure AD) gebruiken als IDP

a. Voer de naam van de toepassingsgroep in en klik op Volgende voor de weer te geven metagegevens van de SAML Service Provider (SP).

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**

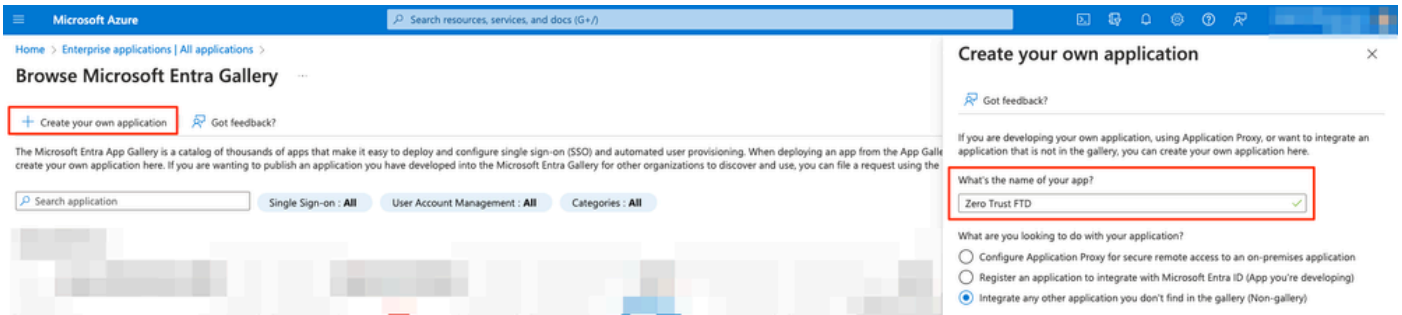
Cancel Finish

b. Zodra de metagegevens van SAML SP worden getoond, ga naar de IDp en vorm een nieuwe toepassing van SAML SSO.

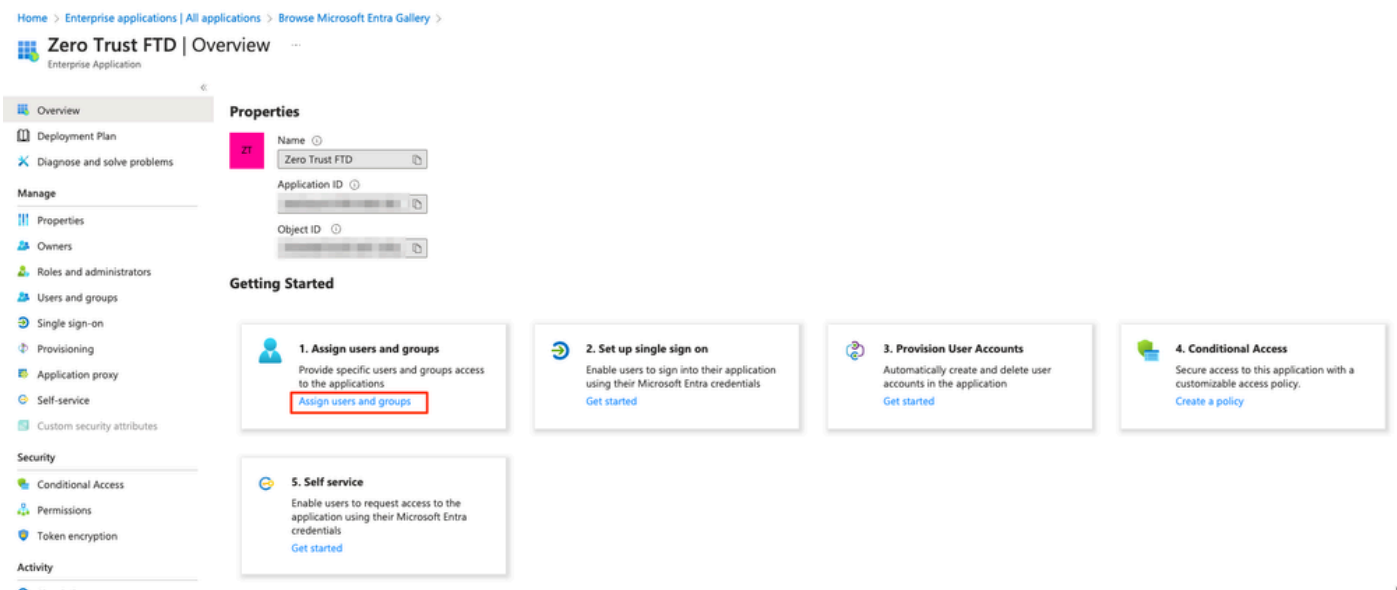
c. Log in op Microsoft Azure en navigeer naar Enterprise-toepassingen > Nieuwe toepassing.

The screenshot shows the Microsoft Azure portal interface for Enterprise applications. The breadcrumb navigation is 'Home > Enterprise applications'. The main heading is 'Enterprise applications | All applications'. The left sidebar has 'All applications' selected. The main content area shows a '+ New application' button (highlighted with a red box), 'Refresh', 'Download (Export)', 'Preview info', 'Columns', 'Preview features', and 'Got feedback?' options. Below this is a search bar and filter options: 'Application type == Enterprise Applications' and 'Application ID starts with'. A table header is visible with columns: Name, Object ID, Application ID, Homepage URL, and Created on. The table shows 77 applications found.

d. Klik op Uw eigen toepassing maken > De naam van de toepassing invoeren > Aanmaken



e. Open de toepassing en klik op Gebruikers en groepen toewijzen om de gebruikers en/of groepen te definiëren die toegang hebben tot de toepassing.



f. Klik op Gebruiker/groep toevoegen > De gewenste gebruikers/groepen selecteren > Toewijzen. Klik op Single sign-on zodra de juiste gebruikers/groepen zijn toegewezen.

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 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. Klik eenmaal in het gedeelte Enkelvoudige aanmelding op 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. Klik op Upload metagegevensbestand en selecteer het XML-bestand dat is gedownload van de Serviceprovider (Secure Firewall) of voer handmatig de URL van de entiteit-ID en de URL van de Assertion Consumer Service (ACS) in de ZTNA-toepassingsgroep (gegenereerd in stap a).

Opmerking: Zorg ervoor dat u ook de Federation Metadata XML downloadt of het certificaat afzonderlijk downloadt (basis 64) en de SAML Metadata kopieert van de IDp (Login & Logout URL's en Microsoft Entra Identifiers), aangezien deze nodig zijn om de configuratie op de Secure Firewall voort te zetten.

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	Active	
Thumbprint	[redacted]	
Expiration	[redacted]	
Notification Email	[redacted]	
App Federation Metadata Url	[redacted]	Download
Certificate (Base64)	[redacted]	Download
Certificate (Raw)	[redacted]	Download
Federation Metadata XML	[redacted]	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. Navigeer terug naar het VCC en importeer de metagegevens van SAML IDP naar de Toepassingsgroep 2, met behulp van het van de IDP gedownloade metagegevensbestand of voer de vereiste gegevens handmatig in.

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. Klik op Volgende en configureer de herverificatie-interval en beveiligingscontroles volgens uw vereisten. Controleer de summiere configuratie en klik op Vervolgens.

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

Toepassingen configureren

Nu de Toepassingsgroepen zijn gemaakt, klikt u op Add Application om de toepassingen te definiëren die op afstand moeten worden beveiligd en benaderd.

1. Voer de toepassingsinstellingen in:

a) Toepassingsnaam: Identificatiecode voor de geconfigureerde toepassing.

b) Externe URL: gepubliceerde URL van de toepassing in de openbare/externe DNS-records. Dit is de URL die door gebruikers wordt gebruikt om de applicatie op afstand te benaderen.

c) Application URL: Real FQDN of Network IP van de applicatie. Dit is de URL die door Secure Firewall wordt gebruikt om de applicatie te bereiken.

Opmerking: standaard wordt de externe URL gebruikt als applicatie-URL. Schakel het selectievakje uit om een andere URL voor de toepassing op te geven.

d) Toepassingscertificaat: de certificaatketen en de privésleutel van de aanvraag die toegankelijk is (Toegevoegd vanaf FMC Home Page > Objecten > Objectbeheer > PKI > Interne

certs)

e) IPv4 NAT-bron (optioneel): Het IP-bronadres van de externe gebruiker wordt vertaald naar de geselecteerde adressen voordat de pakketten naar de applicatie worden doorgestuurd (alleen netwerkobjecten/objectgroepen met IPv4-adressen van het type Host en Range worden ondersteund). Dit kan zo worden geconfigureerd dat de toepassingen via de Secure Firewall een route naar de externe gebruikers hebben

f) Toepassingsgroep (optioneel): Selecteer als deze toepassing wordt toegevoegd aan een bestaande Toepassingsgroep om de instellingen te gebruiken die ervoor zijn geconfigureerd.

In dit voorbeeld zijn de toepassingen die met ZTNA worden benaderd een test-FMC Web UI en de Web UI van een CTB die zich achter de Secure Firewall bevindt.

De certificaten van de Toepassingen moeten worden toegevoegd in Objecten > Objectbeheer > PKI > Interne certs:

Add Known Internal Certificate



Name:

ao-fmc-ztna.cisco.local

Certificate Data or, choose a file:

Browse..

```
-----BEGIN CERTIFICATE-----
[Redacted Certificate Data]
T
G
3Y
```

Key or, choose a file:


Browse..

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

Encrypted, and the password is:

Cancel

Save

 Opmerking: Zorg ervoor dat u alle certificaten toevoegt voor elke toepassing die u met ZTNA kunt benaderen.

Nadat de certificaten zijn toegevoegd als interne certificaten, blijft u de resterende instellingen configureren.


De toepassingsinstellingen die bij dit voorbeeld zijn geconfigureerd, zijn:

Toepassing 1: Test FMC Web UI (Lid van de Toepassingsgroep 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   +IPv4 NAT Source Select...  +

Application Group

External_Duo  

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

Aangezien de toepassing werd toegevoegd aan Toepassingsgroep 1, worden de resterende instellingen geërfd voor deze toepassing. U kunt de Security Zones en Security Controls nog steeds negeren met verschillende instellingen.

Controleer de geconfigureerde toepassing en klik op Voltooien.

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

Toepassing 2: CTB Web UI (lid van de Toepassingsgroep 2)

De configuratiesamenvatting voor deze toepassing is de volgende:

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

 **Opmerking:** Merk op dat voor deze toepassing een netwerkobject "ZTNA_NAT_CTB" is geconfigureerd als IPv4 NAT-bron. Met deze configuratie wordt het IP-bronadres van de externe gebruikers vertaald naar een IP-adres binnen het geconfigureerde object voordat de pakketten naar de applicatie worden doorgestuurd. Dit werd geconfigureerd omdat de standaard applicatie (CTB) routepunten naar een gateway anders dan de Secure Firewall, daarom werd het retourverkeer niet verzonden naar de externe gebruikers. Met deze NAT configuratie, werd een statische route geconfigureerd op de applicatie voor het subnetnetwerk ZTNA_NAT_CTB om bereikbaar te zijn via de Secure Firewall.

Nadat de toepassingen zijn geconfigureerd, worden ze nu weergegeven onder de corresponderende toepassingsgroep.

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


Sla tot slot de wijzigingen op en implementeer de configuratie.

Verifiëren

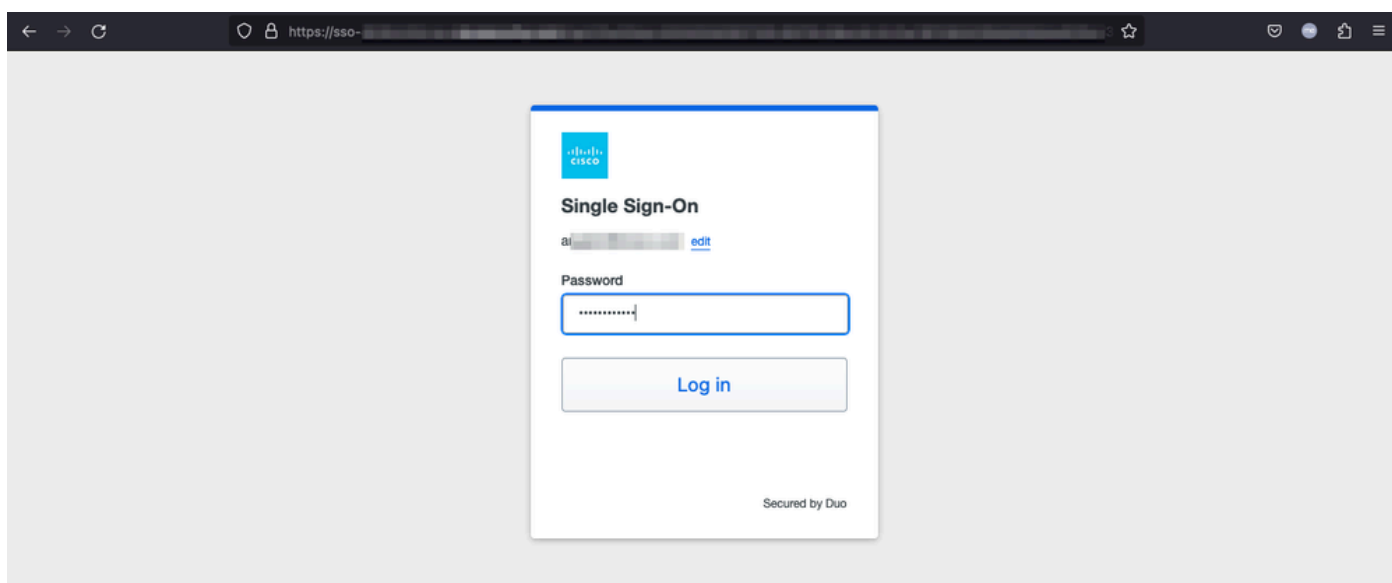
Zodra de configuratie is geïnstalleerd, kunnen externe gebruikers de toepassingen bereiken via de externe URL en als ze zijn toegestaan door de bijbehorende IDp, hebben ze toegang tot het.

Toepassing 1

1. De gebruiker opent een webbrowser en navigeert naar de externe URL van de toepassing 1. In dit geval is de externe URL "https://ao-fmc-ztna.cisco.local/"

 **Opmerking:** de externe URL moet worden aangepast naar het IP-adres van de beveiligde firewall-interface die is geconfigureerd. In dit voorbeeld, lost het aan het BuiteninterfacelP adres (192.0.2.254) op

2. Aangezien dit een nieuwe toegang is, wordt de gebruiker omgeleid naar het IDP-inlogportal dat voor de toepassing is geconfigureerd.

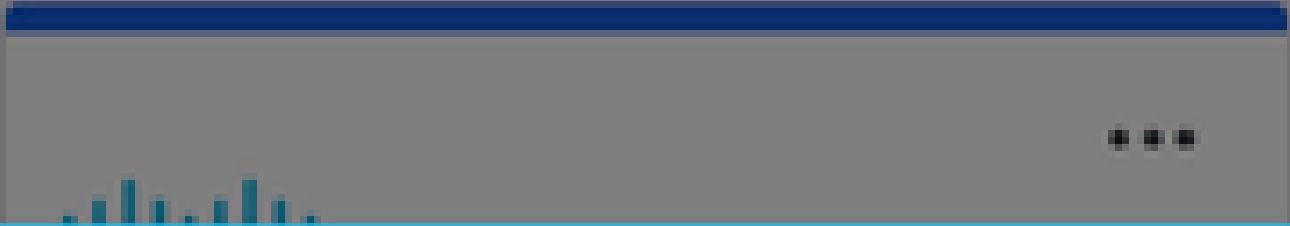


3. De gebruiker wordt een Push voor MFA (dit is afhankelijk van de MFA-methode die op de IDp is geconfigureerd) gestuurd.



Accounts

Add




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

🌐 Global VPN TAC

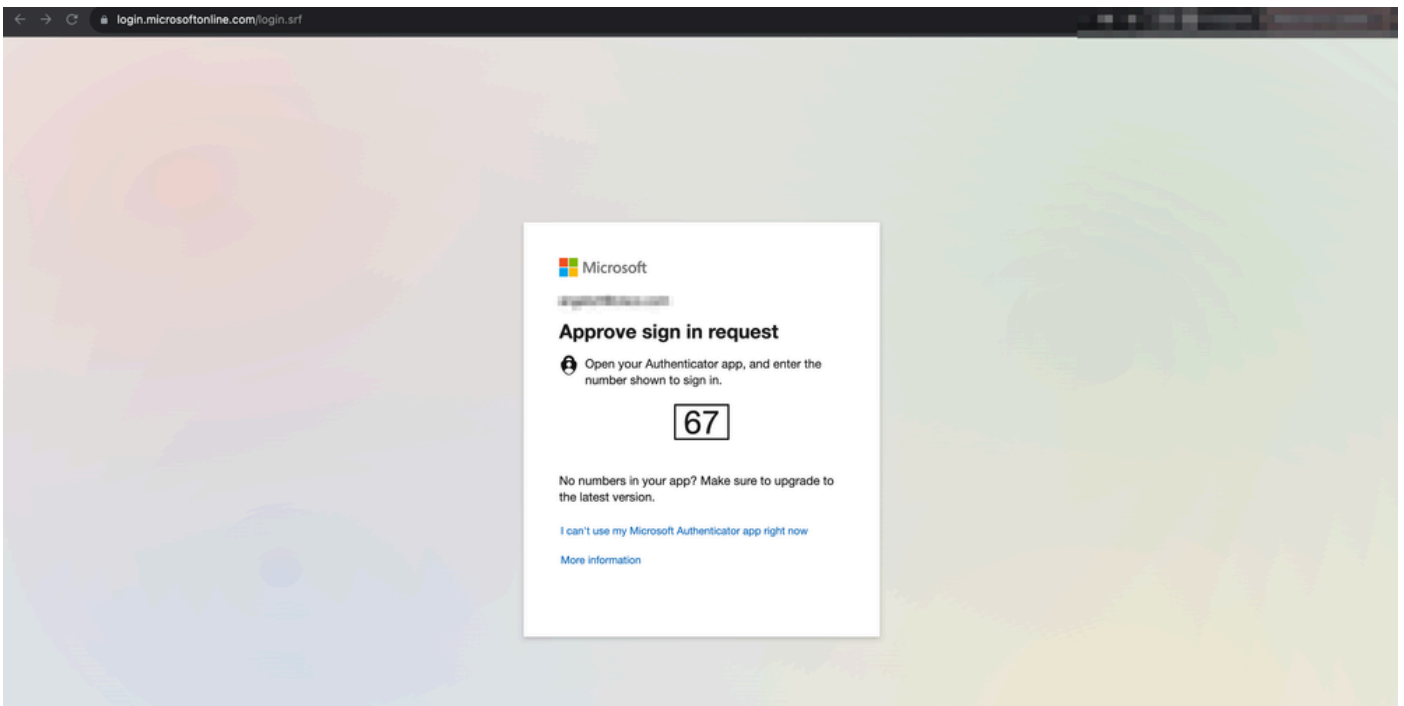
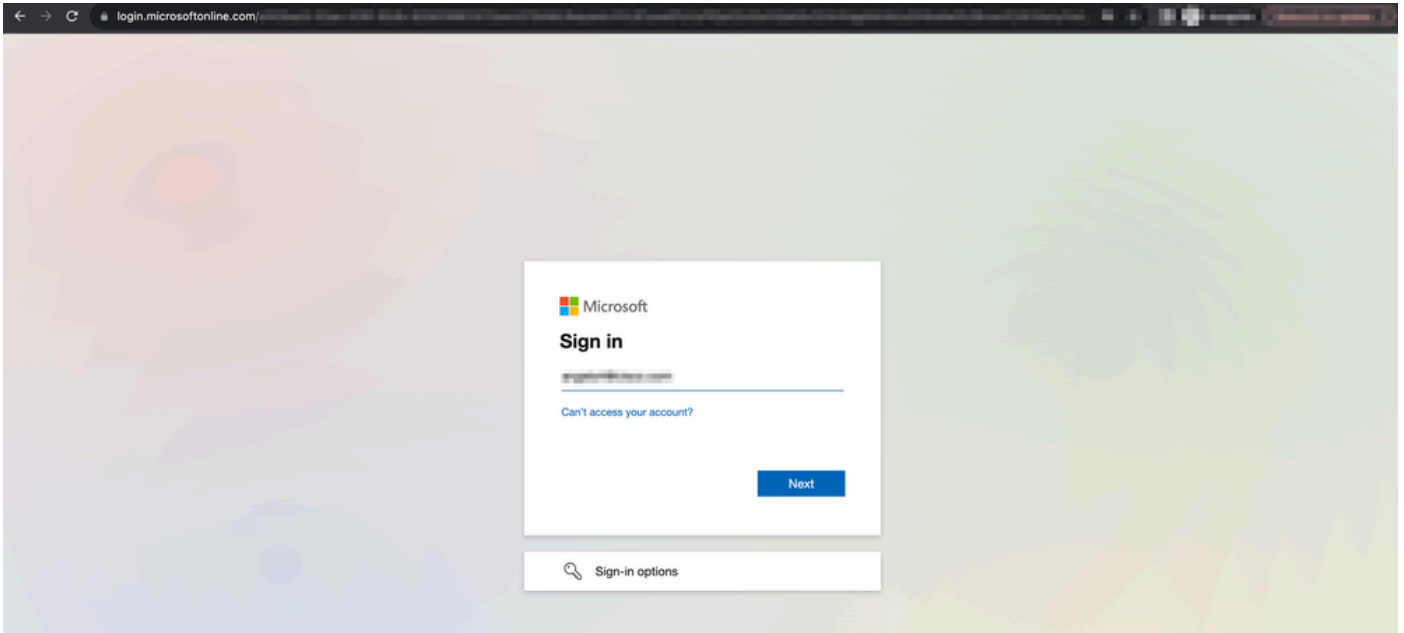
🌐 [Redacted]

🕒 1:13 p.m.

👤 [Redacted]

 : de externe URL moet worden aangepast naar het IP-adres van de beveiligde firewall-interface die is geconfigureerd. In dit voorbeeld, lost het aan het BuiteninterfaceIP adres (192.0.2.254) op

2. Aangezien dit een nieuwe toegang is, wordt de gebruiker omgeleid naar het IDP-inlogportal dat voor de toepassing is geconfigureerd.

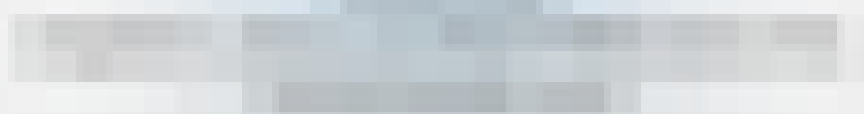


3. De gebruiker wordt een Push voor MFA (dit is afhankelijk van de MFA-methode die op de IDp is geconfigureerd) gestuurd.

4:24



Are you trying to sign in?



Enter the number shown to sign in.

Enter number

No, it's not me

Yes

- Diagnostiek biedt algemene analyse (OK of niet) en verzamelt gedetailleerde logbestanden die kunnen worden geanalyseerd om problemen op te lossen

Toepassings specifieke diagnostiek wordt gebruikt voor de detectie van:

- DNS-gerelateerde problemen
- Misconfiguratie, bijvoorbeeld, socket niet geopend, classificatieregels, NAT-regels
- Problemen in het beleid voor vertrouwenstoegang op nul
- Op interfaces betrekking hebbende kwesties, bijvoorbeeld, interface niet geconfigureerd, of interface is down

Generieke diagnostiek voor detectie:

- Als een sterk algoritme niet is ingeschakeld
- Indien het aanvraagcertificaat niet geldig is
- Als de verificatiemethode niet is geïnitieerd naar SAML in de standaardtunnelgroep
- Problemen met HA en clusterbulk synchroniseren
- Krijg inzicht van snortellers om kwesties, zoals die met betrekking tot tekenen of decryptie te diagnosticeren
- Probleem met PAT-pooluitputting bij bronvertaling.

U voert de diagnostiek als volgt uit:

1. Navigeer naar het pictogram diagnostiek dat voor elke ZTNA-toepassing aanwezig is.

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. Selecteer een apparaat en klik op Uitvoeren.

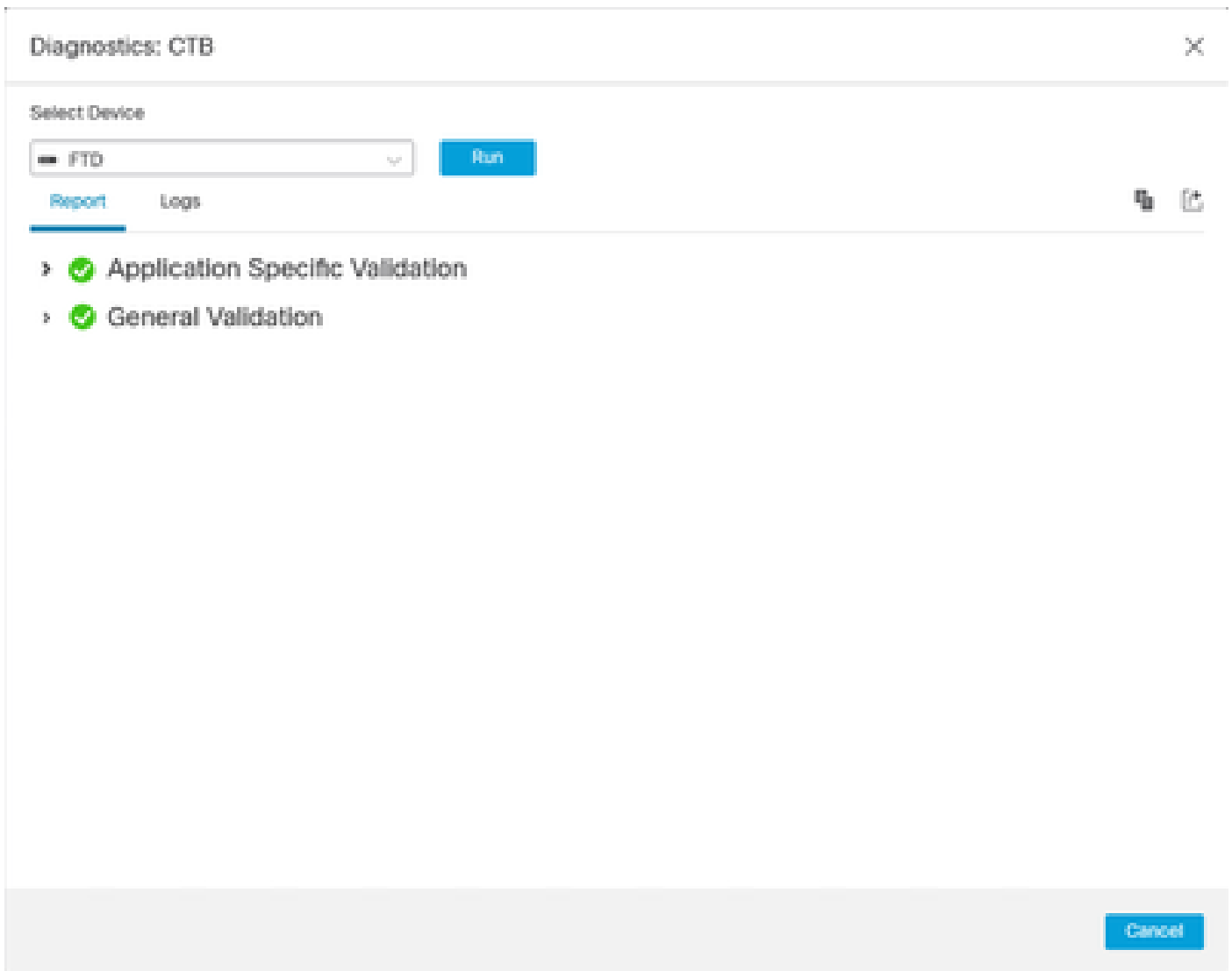
Select Device

Select...
FTD

Run

Cancel

3. Bekijk de resultaten in het rapport.



Toon en duidelijke bevelen zijn beschikbaar in FTD CLI om de nul-vertrouwen configuratie en de vertoningsstatistieken en zittingsinformatie te bekijken.

```
<#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>
```

Om nul-vertrouwen en webvpn module debugs toe te laten gebruik de volgende opdrachten in Lina prompt:

- firepower# debug zero-trust 255
- firepower# debug webvpn-verzoek 25
- firepower# debug webvpn-respons 25
- firepower# debug webvpn saml 255

Gerelateerde informatie

- Voor extra assistentie kunt u contact opnemen met het Technical Assistance Center (TAC). Er is een geldig ondersteuningscontract vereist: [Cisco's wereldwijde contactgegevens voor ondersteuning](#).
- U kunt [hier](#) ook de Cisco VPN-community bezoeken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.