

# Konfiguration einer Bereitstellung ohne Vertrauen für den Remote-Zugriff auf einer sicheren Firewall

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Erforderliche Konfiguration](#)

[Allgemeine Konfigurationen](#)

[Anwendungsgruppe konfigurieren](#)

[Anwendungsgruppe 1: Verwenden von Duo als IDp](#)

[Anwendungsgruppe 2: Microsoft Entra ID \(Azure AD\) als IDp verwenden](#)

[Anwendungen konfigurieren](#)

[Anwendung 1: Test FMC Web UI \(Mitglied der Anwendungsgruppe 1\)](#)

[Anwendung 2: CTB-Weboberfläche \(Mitglied der Anwendungsgruppe 2\)](#)

[Überprüfung](#)

[Überwachung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird der Prozess der Konfiguration einer Clientless-Bereitstellung mit Zero Trust Access und Remote Access auf einer sicheren Firewall beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Firepower Management Center (FMC)
- Grundlegendes ZTNA-Wissen
- Grundlegendes SAML-Wissen (Security Assertion Markup Language)

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Secure Firewall Version 7.4.1
- FirePOWER Management Center (FMC) Version 7.4.1
- Duo als Identitätsanbieter (IdP)
- Microsoft Entra ID (ehemals Azure AD) als IdP

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Die Zero Trust Access-Funktion basiert auf den Zero Trust Network Access (ZTNA)-Prinzipien. ZTNA ist ein Sicherheitsmodell ohne Vertrauen, das implizite Vertrauenswürdigkeit ausschließt. Das Modell gewährt den Zugriff mit den geringsten Rechten, nachdem der Benutzer, der Kontext der Anforderung und das Risiko, wenn der Zugriff gewährt wird, geprüft wurden.

Derzeit gelten für ZTNA folgende Anforderungen und Einschränkungen:

- Unterstützt von Secure Firewall Version 7.4.0+, verwaltet von FMC Version 7.4.0+ (Firepower 4200-Serie)
- Unterstützt auf Secure Firewall Version 7.4.1+, verwaltet von FMC Version 7.4.1+ (alle anderen Plattformen)
- Nur Webanwendungen (HTTPS) werden unterstützt. Szenarien, die eine Entschlüsselungsausnahme erfordern, werden nicht unterstützt.
- Unterstützt nur SAML-IDs
- Öffentliche DNS-Updates sind für den Remote-Zugriff erforderlich.
- IPv6 wird nicht unterstützt. Die Szenarien NAT66, NAT64 und NAT46 werden nicht unterstützt.
- Diese Funktion steht nur dann zur Abwehr von Bedrohungen zur Verfügung, wenn Snort 3 aktiviert ist.
- Alle Hyperlinks in geschützten Webanwendungen müssen einen relativen Pfad aufweisen.
- Geschützte Webanwendungen, die auf einem virtuellen Host oder hinter internen Load Balancern ausgeführt werden, müssen dieselbe externe und interne URL verwenden.
- Nicht unterstützt auf einzelnen Modusclustern

- Nicht unterstützt bei Anwendungen mit aktivierter strikter HTTP-Host-Header-Validierung
- Wenn der Anwendungsserver mehrere Anwendungen hostet und Inhalte auf der Grundlage des Headers "Servername Indication (SNI)" im TLS Client Hello bereitstellt, muss die externe URL der Anwendungskonfiguration mit Null-Vertrauensstellung mit der SNI der entsprechenden Anwendung übereinstimmen.
- Wird nur im Routing-Modus unterstützt
- Smart License erforderlich (funktioniert nicht im Evaluierungsmodus)

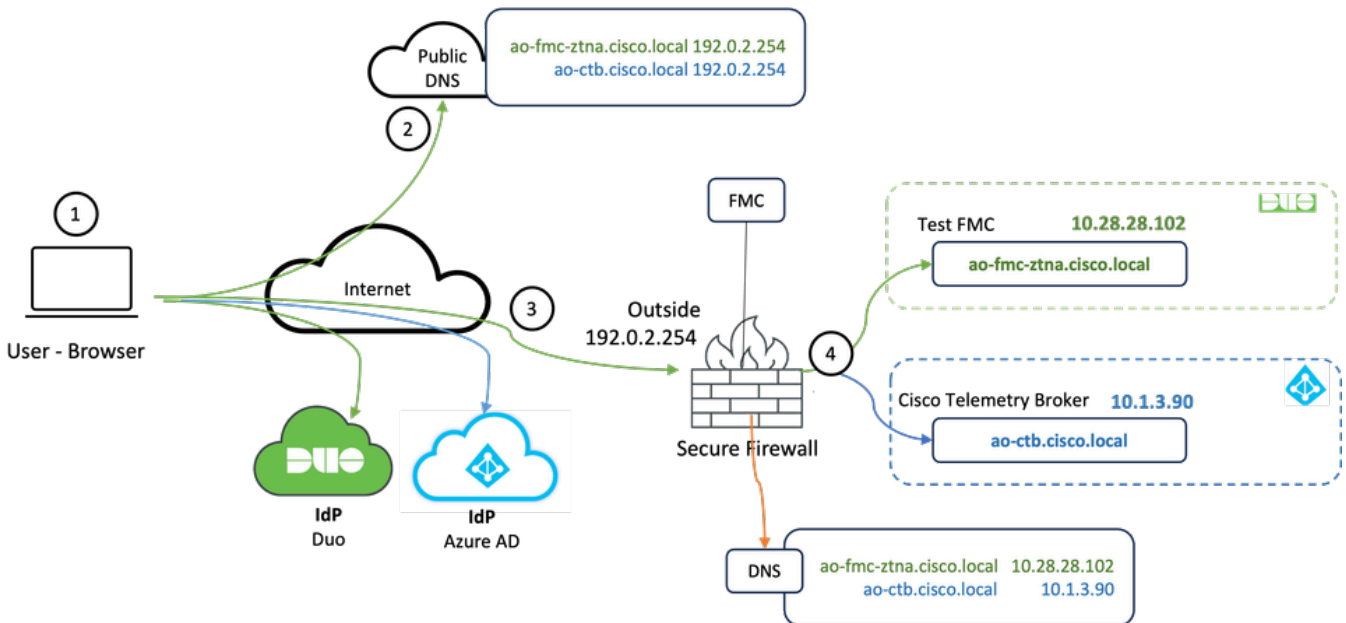
Weitere Informationen und Einzelheiten zu Zero Trust Access in Secure Firewall finden Sie im [Cisco Secure Firewall Management Center Device Configuration Guide, 7.4.](#)

## Konfigurieren

Das vorliegende Dokument behandelt eine Remote Access-Bereitstellung von ZTNA.

In diesem Beispielszenario benötigen Remote-Benutzer Zugriff auf die Web-Benutzeroberflächen (UI) eines Test-FMC und eines Cisco Telemetry Brokers (CTB), die hinter einer sicheren Firewall gehostet werden. Der Zugriff auf diese Anwendungen wird durch zwei verschiedene IDs gewährt: Duo und Microsoft Entra ID, wie im nächsten Diagramm gezeigt.

## Netzwerkdiagramm



Topologiediagramm

1. Die Remote-Benutzer müssen auf Anwendungen zugreifen, die hinter der sicheren Firewall gehostet werden.
2. Jede Anwendung muss über einen DNS-Eintrag in den öffentlichen DNS-Servern verfügen.
3. Diese Anwendungsnamen müssen in die IP-Adresse der Secure Firewall Outside-Schnittstelle aufgelöst werden.

4. Die Secure Firewall löst die IP-Adressen der Anwendungen auf und authentifiziert jeden Benutzer für jede Anwendung mithilfe der SAML-Authentifizierung.

## Erforderliche Konfiguration

### Identity Provider (IdP) und Domain Name Server (DNS)

- Die Anwendungen oder Anwendungsgruppen müssen in einem SAML Identity Provider (IdP) wie Duo, Okta oder Azure AD konfiguriert werden. In diesem Beispiel werden Duo und Microsoft Entra ID als IdPs verwendet.
- Das von den IdPs generierte Zertifikat und die Metadaten werden bei der Konfiguration der Anwendung in der sicheren Firewall verwendet.

### Interne und externe DNS-Server

- Externe DNS-Server (die von Remote-Benutzern verwendet werden) müssen über den FQDN-Eintrag der Anwendungen verfügen und in die IP-Adresse der externen Schnittstelle der sicheren Firewall aufgelöst werden.
- Interne DNS-Server (die von der sicheren Firewall verwendet werden) müssen über den FQDN-Eintrag der Anwendungen verfügen und in die tatsächliche IP-Adresse der Anwendung aufgelöst werden

## Zertifikate

Die nächsten Zertifikate sind für die ZTNA-Richtlinienkonfiguration erforderlich:

- Identitäts-/Proxy-Zertifikat: Wird von der sicheren Firewall zum Masquerade der Anwendungen verwendet. Die Secure Firewall fungiert dabei als SAML Service Provider (SP). Bei diesem Zertifikat muss es sich um ein Platzhalter- oder SAN-Zertifikat (Subject Alternative Name) handeln, das mit dem FQDN der privaten Anwendungen übereinstimmt (ein gemeinsames Zertifikat, das alle privaten Anwendungen in der Phase vor der Authentifizierung darstellt).
- IdP-Zertifikat: Das zur Authentifizierung verwendete IdP stellt ein Zertifikat für jede definierte Anwendung oder Anwendungsgruppe bereit. Dieses Zertifikat muss so konfiguriert werden, dass die sichere Firewall  
Kann die Signatur der IdP bei eingehenden SAML-Assertionen überprüfen (wenn dies für eine Anwendungsgruppe definiert ist, wird dasselbe Zertifikat für die gesamte Anwendungsgruppe verwendet)
- Anwendungszertifikat: Der verschlüsselte Datenverkehr vom Remote-Benutzer zur Anwendung muss von der sicheren Firewall entschlüsselt werden. Aus diesem Grund müssen die Zertifikatskette und der private Schlüssel jeder Anwendung zur sicheren Firewall hinzugefügt werden.

## Allgemeine Konfigurationen


So konfigurieren Sie eine neue Anwendung ohne Vertrauenswürdigkeit:

1. Navigieren Sie zu Policies > Access Control > Zero Trust Application, und klicken Sie auf Add Policy.
2. Füllen Sie die erforderlichen Felder aus:

a) Allgemein: Geben Sie den Namen und die Beschreibung der Richtlinie ein.

b) Domain Name (Domänenname): Dieser Name wird dem DNS hinzugefügt und muss in die Threat Defence-Gateway-Schnittstelle aufgelöst werden, von der aus auf die Anwendungen zugegriffen wird.


---

 Hinweis: Der Domänenname wird zum Generieren der ACS-URL für alle privaten Anwendungen in einer Anwendungsgruppe verwendet.

---

c) Identitätszertifikat: Dies ist ein gemeinsames Zertifikat, das alle privaten Anwendungen in der Phase vor der Authentifizierung darstellt.

---

 Hinweis: Bei diesem Zertifikat muss es sich um ein Platzhalter- oder SAN-Zertifikat (Subject Alternative Name) handeln, das dem FQDN der privaten Anwendungen entspricht.

---

d) Sicherheitszonen: Wählen Sie Außen- oder/und Innenzonen aus, über die private Anwendungen reguliert werden.

e) Globaler Port-Pool: Jeder privaten Anwendung wird ein eindeutiger Port aus diesem Pool zugewiesen.

f) Sicherheitskontrollen (optional): Wählen Sie diese Option aus, wenn die privaten Anwendungen überprüft werden sollen.

In dieser Beispielkonfiguration wurden die nächsten Informationen eingegeben:

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\*  
[Redacted]

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.

Das in diesem Fall verwendete Identitäts-/Proxyzertifikat ist ein Platzhalterzertifikat, das mit dem FQDN der privaten Anwendungen übereinstimmt:

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[Redacted]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. Speichern Sie die Richtlinie.

#### 4. Erstellen Sie neue Anwendungsgruppen und/oder neue Anwendungen:

- Eine Anwendung definiert eine private Web-Anwendung mit SAML-Authentifizierung, Schnittstellenzugriff, Intrusion sowie Malware- und Dateirichtlinien.
- Mit einer Anwendungsgruppe können Sie mehrere Anwendungen gruppieren und allgemeine Einstellungen wie SAML-Authentifizierung, Schnittstellenzugriff und Sicherheitssteuerungseinstellungen gemeinsam nutzen.

In diesem Beispiel werden zwei verschiedene Anwendungsgruppen und zwei verschiedene Anwendungen konfiguriert: eine für die Anwendung, die von Duo authentifiziert werden soll (Test FMC Web UI), und eine für die Anwendung, die von Microsoft Entra ID (CTB Web UI) authentifiziert werden soll.

### Anwendungsgruppe konfigurieren

Anwendungsgruppe 1: Verwenden von Duo als IDp

- a. Geben Sie den Anwendungsgruppennamen ein, und klicken Sie auf Weiter, damit die SAML Service Provider (SP)-Metadaten angezeigt werden.

## 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

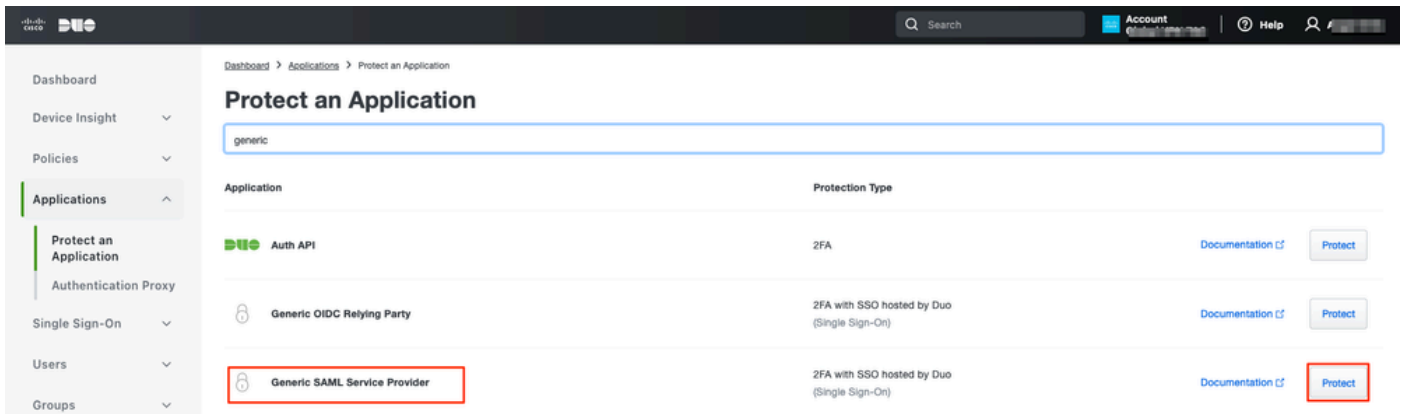
b. Sobald die SAML-SP-Metadaten angezeigt werden, wechseln Sie zur IdP, und konfigurieren Sie eine neue SAML SSO-Anwendung.

c. Melden Sie sich bei Duo an, und navigieren Sie zu Applications > Protect an Application.

The screenshot shows the 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 is titled 'Applications' and includes a sub-header 'Manage your update to the new Universal Prompt experience, all in one place.' Below this, there are two buttons: 'See My Progress' and 'Get More Information'. A summary section shows '11 All Applications' and '0 End of Support'. At the bottom right, there is an 'Export' dropdown and a search bar. A red arrow points to a 'Protect an Application' button in the top right corner of the main content area.



d. Suchen Sie nach einem generischen SAML-Dienstanbieter, und klicken Sie auf Schützen.



e. Laden Sie das Zertifikat und die SAML-Metadaten von der IdP herunter, wenn dies erforderlich ist, um die Konfiguration auf der sicheren Firewall fortzusetzen.

f. Geben Sie die Objektkennung und die ACS-URL (Assertion Consumer Service) aus der ZTNA-Anwendungsgruppe ein (wird in Schritt a generiert).

- 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>	<a href="#">Copy</a>
Single Sign-On URL	<code>https://sso-8.../sso</code>	<a href="#">Copy</a>
Single Log-Out URL	<code>https://sso-i.../slo</code>	<a href="#">Copy</a>
Metadata URL	<code>https://sso-8.../metadata</code>	<a href="#">Copy</a>

### Certificate Fingerprints

SHA-1 Fingerprint	<code>9E:5...5C</code>	<a href="#">Copy</a>
SHA-256 Fingerprint	<code>7:85:...E9:52</code>	<a href="#">Copy</a>

### Downloads

Certificate	<a href="#">Download certificate</a>	Expires: 01-19-2038
SAML Metadata	<a href="#">Download XML</a>	

### 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. Bearbeiten Sie die Anwendung entsprechend Ihren spezifischen Anforderungen, und gewähren Sie nur den beabsichtigten Benutzern Zugriff auf die Anwendung. Klicken Sie dann auf Speichern.

**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. Navigieren Sie zurück zum FMC, und fügen Sie die SAML-IdP-Metadaten mithilfe der von der IdP heruntergeladenen Dateien zur Anwendungsgruppe hinzu.

## Add Application Group



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

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

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

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

Import IdP Metadata  
 Manual Configuration  
 Configure Later

**Import IdP Metadata**

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

Entity ID\*

Single Sign-On URL\*

IdP Certificate

MIIDDTC[redacted]yDQYJKoZI

[redacted]

[redacted]

[redacted]

[Next](#)

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

i. Klicken Sie auf Weiter, und konfigurieren Sie das Intervall für die erneute Authentifizierung und die Sicherheitskontrollen gemäß Ihren Anforderungen. Überprüfen Sie die zusammenfassende Konfiguration, und klicken Sie auf Fertig stellen.

## Add Application Group



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

<b>1 Application Group</b>	Name	External_Duo	Edit
<b>2 SAML Service Provider (SP) Metadata</b>	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...	
<b>3 SAML Identity Provider (IdP) Metadata</b>	Entity ID	https://ssc [redacted]	Edit
	Single Sign-On URL	https://ssc [redacted]	
	IdP Certificate	External_Duo-1697063490514	
<b>4 Re-Authentication Interval</b>	Timeout Interval	1440 minutes	Edit
<b>5 Security Zones and Security Controls</b>	Security Zones	Inherited: (Outside)	Edit
	Intrusion Policy	Inherited: (None)	
	Variable Set	Inherited: (None)	
	Malware and File Policy	Inherited: (None)	

Cancel

Finish

## Anwendungsgruppe 2: Microsoft Entra ID (Azure AD) als IDp verwenden

a. Geben Sie den Anwendungsgruppennamen ein, und klicken Sie auf Weiter, damit die SAML Service Provider (SP)-Metadaten angezeigt werden.

## 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

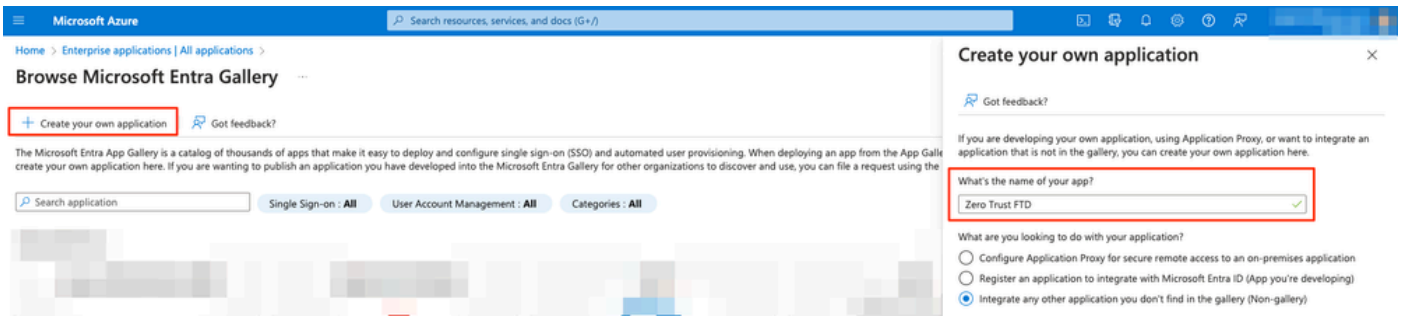
Finish

b. Sobald die SAML-SP-Metadaten angezeigt werden, wechseln Sie zur IdP, und konfigurieren Sie eine neue SAML SSO-Anwendung.

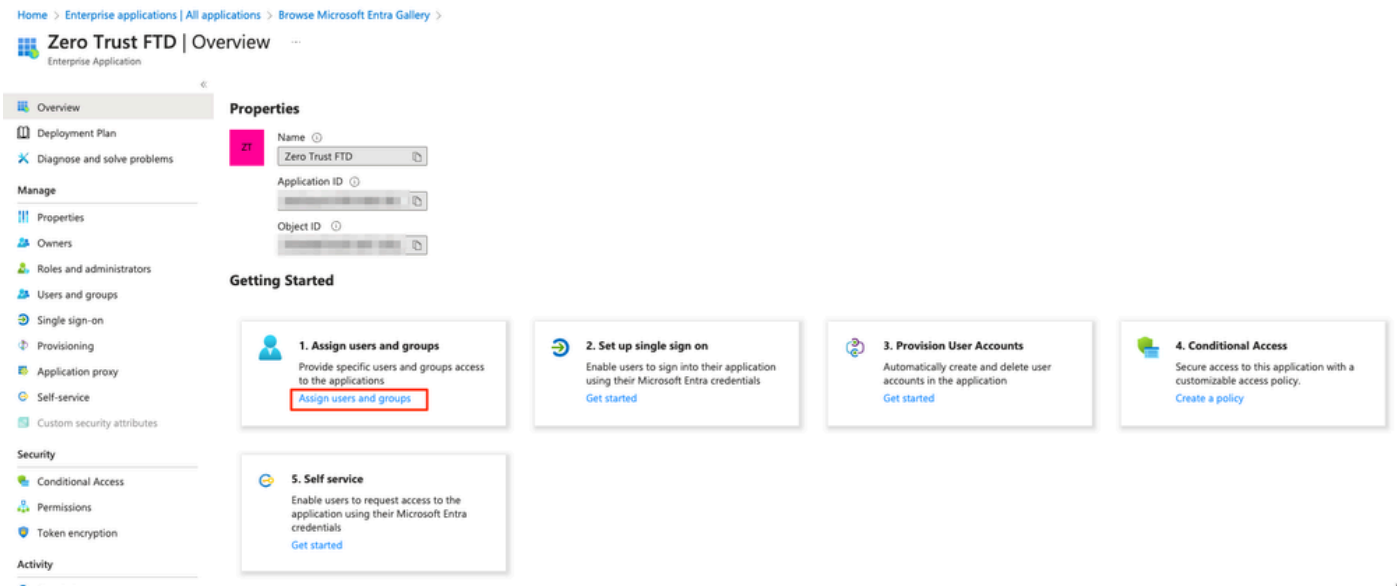
c. Melden Sie sich bei Microsoft Azure an, und navigieren Sie zu Enterprise-Anwendungen > Neue Anwendung.

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

d. Klicken Sie auf Eigene Anwendung erstellen > geben Sie den Namen der Anwendung ein > Erstellen



e. Öffnen Sie die Anwendung, und klicken Sie auf Benutzer und Gruppen zuweisen, um die Benutzer und/oder Gruppen zu definieren, die auf die Anwendung zugreifen dürfen.



f. Klicken Sie auf Benutzer/Gruppe hinzufügen > Wählen Sie die gewünschten Benutzer/Gruppen aus > Zuweisen. Sobald die richtigen Benutzer/Gruppen zugewiesen wurden, klicken Sie auf Single Sign-on (Einmalige Anmeldung).

## 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. Klicken Sie im Abschnitt zur einmaligen Anmeldung auf 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. Klicken Sie auf Metadatenfile hochladen, und wählen Sie die vom Service Provider (Secure Firewall) heruntergeladene XML-Datei aus, oder geben Sie die Entity ID and Assertion Consumer Service (ACS) URL aus der ZTNA Application Group (generiert in Schritt a) manuell ein.

Hinweis: Stellen Sie sicher, dass Sie auch die Verbundmetadaten-XML herunterladen oder das Zertifikat einzeln herunterladen (Basis 64) und die SAML-Metadaten aus der IDp (Anmelde- und Abmelde-URLs und Microsoft Entra-IDs) kopieren, da diese erforderlich sind, um die Konfiguration auf der sicheren Firewall fortzusetzen.



# 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**

<b>Token signing certificate</b>	Active	<span>Edit</span>
Status		
Thumbprint	[redacted]	
Expiration	[redacted]	
Notification Email	[redacted]	
App Federation Metadata Url	[redacted]	<span>Download</span>
Certificate (Base64)		<span>Download</span>
Certificate (Raw)		<span>Download</span>
<b>Federation Metadata XML</b>		<span>Download</span>
<b>Verification certificates (optional)</b>		<span>Edit</span>
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]	<span>Copy</span>
Microsoft Entra Identifier	https://[redacted]	<span>Copy</span>
Logout URL	https://[redacted]	<span>Copy</span>

i. Navigieren Sie zurück zum FMC, und importieren Sie die SAML IdP-Metadaten in die Anwendungsgruppe 2. Verwenden Sie dabei die von der IdP heruntergeladene Metadatenfile, oder geben Sie die erforderlichen Daten manuell ein.

## 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/DANBqkqhkiG9w0B

[redacted]

Next

### 4 Re-Authentication Interval

### 5 Security Zones and Security Controls

Cancel

Finish

j. Klicken Sie auf Weiter, und konfigurieren Sie das Intervall für die erneute Authentifizierung und die Sicherheitskontrollen gemäß Ihren Anforderungen. Überprüfen Sie die zusammenfassende Konfiguration, und klicken Sie auf Fertig stellen.

### Add Application Group ? X

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

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

Cancel
Finish

## Anwendungen konfigurieren

Nachdem Sie die Anwendungsgruppen erstellt haben, klicken Sie auf Anwendung hinzufügen, um die zu schützenden Anwendungen zu definieren, auf die remote zugegriffen werden soll.

1. Geben Sie die Anwendungseinstellungen ein:

a) Anwendungsname: Kennung für die konfigurierte Anwendung.

b) Externe URL: Veröffentlichte URL der Anwendung in den öffentlichen/externen DNS-Datensätzen. Dies ist die URL, die von Benutzern für den Remote-Zugriff auf die Anwendung verwendet wird.

c) Anwendungs-URL: Echter FQDN oder Netzwerk-IP der Anwendung. Dies ist die URL, die von der sicheren Firewall verwendet wird, um die Anwendung zu erreichen.



Hinweis: Standardmäßig wird die externe URL als Anwendungs-URL verwendet. Deaktivieren Sie das Kontrollkästchen, um eine andere Anwendungs-URL anzugeben.

d) Anwendungszertifikat: Zertifikatskette und privater Schlüssel der Anwendung, auf die

zugegriffen werden soll (hinzugefügt von FMC-Startseite > Objekte > Objektverwaltung > PKI > Interne Zertifikate)

e) IPv4 NAT-Quelle (optional): Die IP-Quelladresse des Remote-Benutzers wird in die ausgewählten Adressen umgewandelt, bevor die Pakete an die Anwendung weitergeleitet werden (nur Netzwerkobjekte/Objektgruppen vom Host- und Bereichstyp mit IPv4-Adressen werden unterstützt). Dies kann konfiguriert werden, um sicherzustellen, dass die Anwendungen über die sichere Firewall eine Route zurück zu den Remote-Benutzern haben.

f) Anwendungsgruppe (optional): Wählen Sie aus, ob diese Anwendung zu einer vorhandenen Anwendungsgruppe hinzugefügt wird, um die dafür konfigurierten Einstellungen zu verwenden.

In diesem Beispiel sind die Anwendungen, auf die mit ZTNA zugegriffen werden soll, eine Test-FMC-Webbenutzeroberfläche und die Webbenutzeroberfläche einer CTB, die sich hinter der sicheren Firewall befindet.

Die Zertifikate der Anwendungen müssen unter Objekte > Objektverwaltung > PKI > Interne Zertifikate hinzugefügt werden:

## Add Known Internal Certificate



Name:

ao-fmc-ztna.cisco.local

Certificate Data or, choose a file:

Browse..

```
-----BEGIN CERTIFICATE-----  
[Redacted Certificate Data]  
-----END CERTIFICATE-----
```

Key or, choose a file:

Browse..

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

Encrypted, and the password is: .....

Cancel

Save

Hinweis: Fügen Sie alle Zertifikate für jede Anwendung hinzu, auf die mit ZTNA zugegriffen werden soll.

Sobald die Zertifikate als interne Zertifikate hinzugefügt wurden, fahren Sie mit der Konfiguration der übrigen Einstellungen fort.

Die für dieses Beispiel konfigurierten Anwendungseinstellungen sind:

Anwendung 1: Test FMC Web UI (Mitglied der Anwendungsgruppe 1)

**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

Wenn die Anwendung der Anwendungsgruppe 1 hinzugefügt wurde, werden die übrigen Einstellungen für diese Anwendung übernommen. Sie können die Sicherheitszonen und Sicherheitskontrollen weiterhin mit unterschiedlichen Einstellungen überschreiben.

Überprüfen Sie die konfigurierte Anwendung, und klicken Sie auf Fertig stellen.

## 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

Anwendung 2: CTB-Weboberfläche (Mitglied der Anwendungsgruppe 2)

Die Konfigurationsübersicht für diese Anwendung sieht wie folgt aus:

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

 Hinweis: Beachten Sie, dass für diese Anwendung ein Netzwerkobjekt "ZTNA\_NAT\_CTB" als IPv4-NAT-Quelle konfiguriert wurde. Bei dieser Konfiguration wird die Quell-IP-Adresse der Remote-Benutzer in eine IP-Adresse innerhalb des konfigurierten Objekts umgewandelt, bevor die Pakete an die Anwendung weitergeleitet werden. Dies wurde konfiguriert, da die Standardroute der Anwendung (CTB) auf ein anderes Gateway als die sichere Firewall verweist. Der zurückkehrende Datenverkehr wurde daher nicht an die Remote-Benutzer gesendet. Mit dieser NAT-Konfiguration wurde eine statische Route in der Anwendung konfiguriert, damit das Subnetz ZTNA\_NAT\_CTB über die sichere Firewall erreichbar ist.

Nachdem die Anwendungen konfiguriert wurden, werden sie nun unter der entsprechenden Anwendungsgruppe angezeigt.

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.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
<input checked="" type="checkbox"/> 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

Speichern Sie abschließend die Änderungen, und stellen Sie die Konfiguration bereit.




# Überprüfung

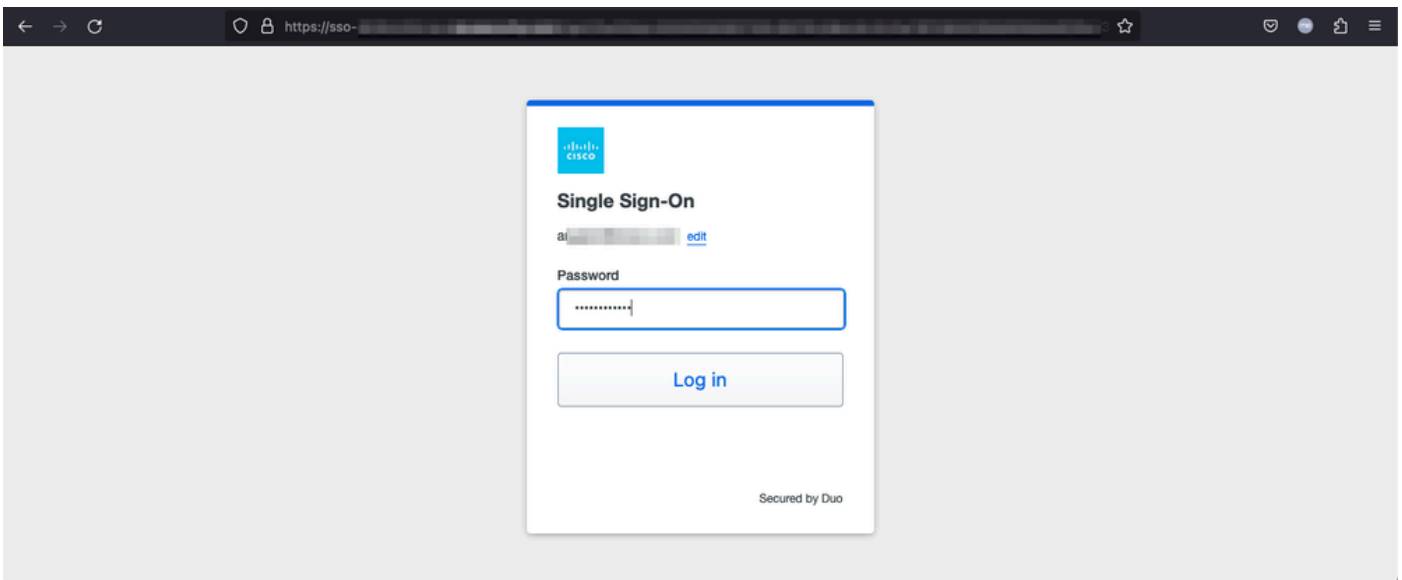
Nach der Konfiguration können Remote-Benutzer über die externe URL auf die Anwendungen zugreifen. Wenn sie über die entsprechende IDp zugelassen sind, haben sie Zugriff darauf.

## Anwendung 1

1. Der Benutzer öffnet einen Webbrowser und navigiert zur externen URL der Anwendung 1. In diesem Fall lautet die externe URL "https://ao-fmc-ztna.cisco.local/".

 Hinweis: Der externe URL-Name muss in die IP-Adresse der konfigurierten Secure Firewall-Schnittstelle aufgelöst werden. In diesem Beispiel wird die IP-Adresse der externen Schnittstelle (192.0.2.254) aufgelöst.

2. Da es sich um einen neuen Zugriff handelt, wird der Benutzer zum für die Anwendung konfigurierten IdP-Anmeldeportal umgeleitet.

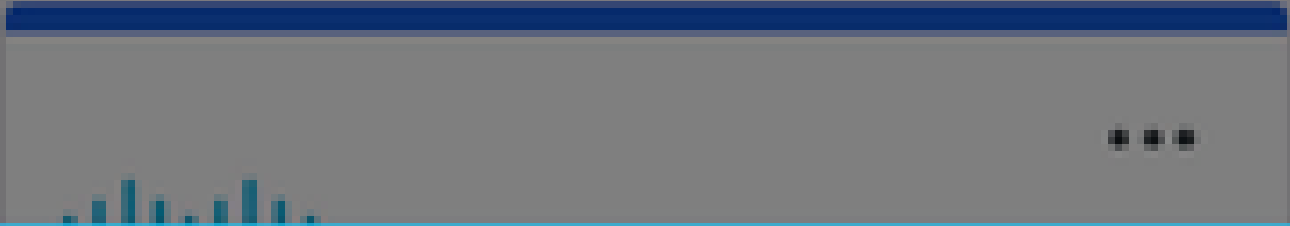


3. Dem Benutzer wird ein Push für MFA gesendet (dies hängt von der MFA-Methode ab, die für die IdP konfiguriert wurde).



## Accounts

Add




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

🌐 Global VPN TAC

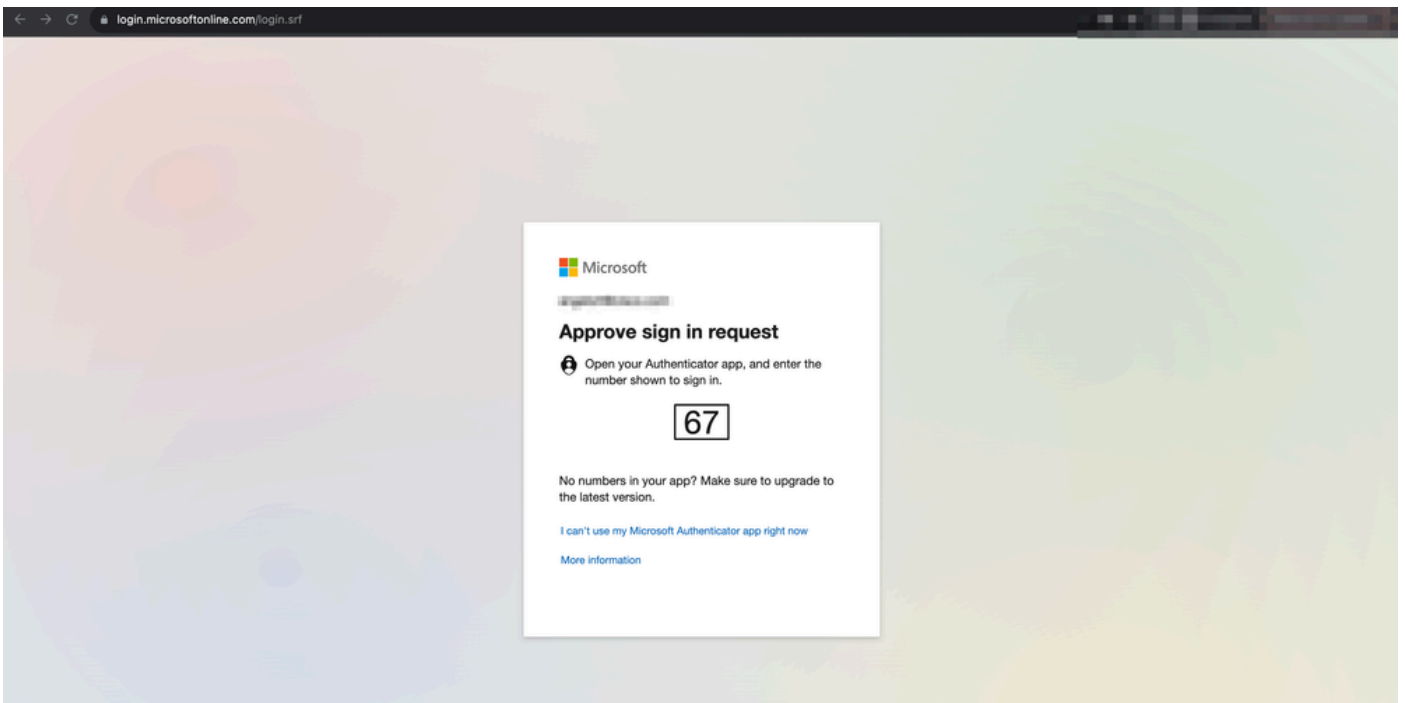
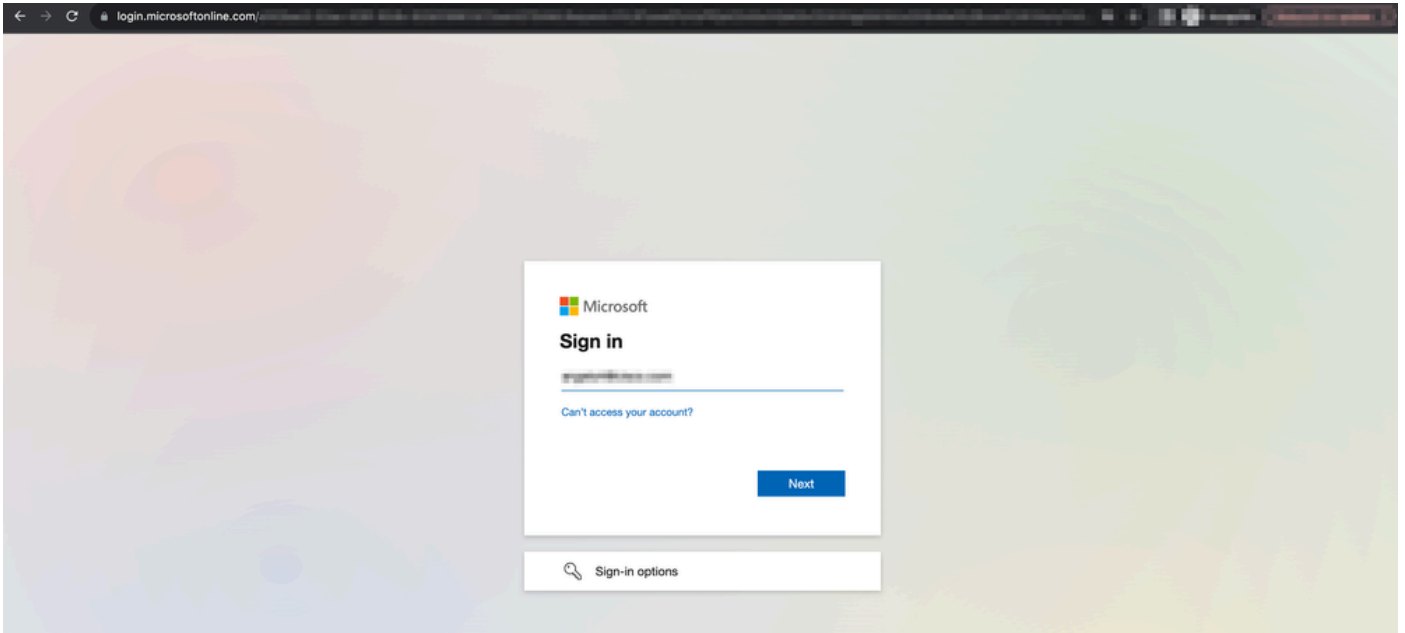
🌐 [Redacted]

🕒 1:13 p.m.

👤 [Redacted]

 : Der externe URL-Name muss in die IP-Adresse der konfigurierten Secure Firewall-Schnittstelle aufgelöst werden. In diesem Beispiel wird die IP-Adresse der externen Schnittstelle (192.0.2.254) aufgelöst.

2. Da es sich um einen neuen Zugriff handelt, wird der Benutzer zum für die Anwendung konfigurierten IdP-Anmeldeportal umgeleitet.

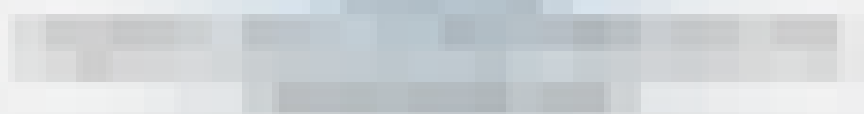


3. Dem Benutzer wird ein Push für MFA gesendet (dies hängt von der MFA-Methode ab, die für die IdP konfiguriert wurde).

4:24



**Are you trying to sign in?**



Enter the number shown to sign in.

**No, it's not me**

Yes

- Die Diagnose ermöglicht eine Gesamtanalyse (OK oder nicht) und sammelt detaillierte Protokolle, die zur Problembhebung analysiert werden können.

Die anwendungsspezifische Diagnose dient zum Erkennen von:

- DNS-bezogene Probleme
- Fehlkonfiguration, z. B. nicht geöffneter Socket, Klassifizierungsregeln, NAT-Regeln
- Probleme bei der Richtlinie für den nicht vertrauenswürdigen Zugriff
- Schnittstellenbezogene Probleme, z. B. nicht konfigurierte Schnittstelle oder ausgefallene Schnittstelle

Generic Diagnostics zur Erkennung:

- Wenn keine Lizenz für starke Verschlüsselung aktiviert ist
- Wenn das Anwendungszertifikat ungültig ist
- Wenn die Authentifizierungsmethode in der Standardtunnelgruppe nicht für SAML initialisiert ist
- Massensynchronisierungsprobleme bei HA und Clustern
- Einblicke in Snort-Zähler zur Diagnose von Problemen, z. B. Token oder Entschlüsselung
- PAT-Pool-Erschöpfungsproblem bei der Quellübersetzung.

So führen Sie die Diagnose aus:

1. Navigieren Sie zum Symbol Diagnostics (Diagnose) für jede ZTNA-Anwendung.

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	Diagnostics
▼ External_Duo (1 Application)				Outside (Inherited)	None (Inherited)	None (Inherited)		
<input type="checkbox"/> FMC				Outside (Inherited)	None (Inherited)	None (Inherited)	True	

2. Wählen Sie ein Gerät aus, und klicken Sie auf Ausführen.

Select Device

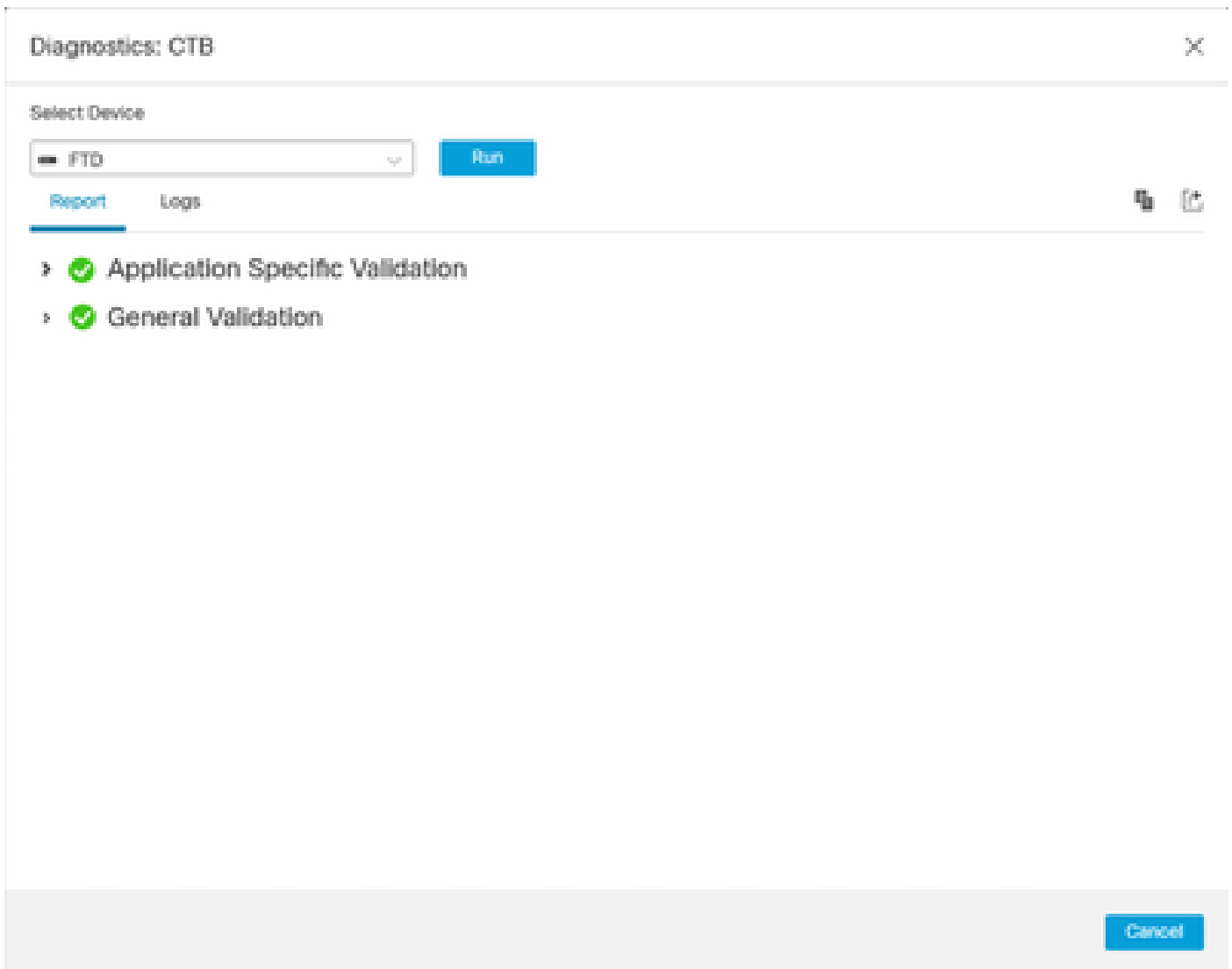
Select...

FTD

Run

Cancel

3. Zeigen Sie die Ergebnisse im Bericht an.



Befehle zum Anzeigen und Löschen sind in der FTD-CLI verfügbar, um die Konfiguration ohne Vertrauensstellung anzuzeigen und Statistiken und Sitzungsinformationen anzuzeigen.

```
<#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>
```

Verwenden Sie die folgenden Befehle in der Lina-Eingabeaufforderung, um das Debuggen von Zero-Trust- und WebVPN-Modulen zu aktivieren:

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

## Zugehörige Informationen

- Wenden Sie sich für zusätzliche Unterstützung an das Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: [Cisco Worldwide Support Contacts](#).
- Besuchen Sie auch die Cisco VPN Community [hier](#).



## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.