

Configurare la distribuzione di Accesso remoto senza trust su un firewall protetto

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione prerequisiti](#)

[Configurazioni generali](#)

[Configura gruppo applicazioni](#)

[Gruppo applicazioni 1: utilizzo di Duo come IdP](#)

[Gruppo applicazioni 2: utilizzo di Microsoft Entra ID \(Azure AD\) come IdP](#)

[Configura applicazioni](#)

[Applicazione 1: interfaccia utente Web del CCP di test \(membro del gruppo di applicazioni 1\)](#)

[Applicazione 2: Interfaccia utente Web CTB \(membro del gruppo di applicazioni 2\)](#)

[Verifica](#)

[Monitor \(Monitora\)](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il processo di configurazione della distribuzione di Accesso remoto senza client con accesso zero trust su un firewall protetto.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Management Center (FMC)
- Conoscenze base di ZTNA
- Conoscenze base di SAML (Security Assertion Markup Language)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Secure Firewall versione 7.4.1
- Firepower Management Center (FMC) versione 7.4.1
- Duo as Identity Provider (IdP)
- ID Entra Microsoft (in precedenza Azure AD) come IdP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La funzionalità Accesso di protezione totale è basata sui principi ZTNA (Zero Trust Network Access). ZTNA è un modello di sicurezza con attendibilità zero che elimina la fiducia implicita. Il modello concede l'accesso con il privilegio minimo dopo aver verificato l'utente, il contesto della richiesta e dopo aver analizzato il rischio se l'accesso viene concesso.

I requisiti e le limitazioni attuali per lo ZTNA sono:

- Supportato su Secure Firewall versione 7.4.0+ gestito da FMC versione 7.4.0+ (Firepower serie 4200)
- Supportato su Secure Firewall versione 7.4.1+ gestito da FMC versione 7.4.1+ (tutte le altre piattaforme)
- Sono supportate solo le applicazioni Web (HTTPS). Gli scenari che richiedono l'esenzione dalla decrittografia non sono supportati
- Supporta solo ID SAML
- Per l'accesso remoto sono necessari aggiornamenti DNS pubblici
- IPv6 non supportato. Gli scenari NAT66, NAT64 e NAT46 non sono supportati
- La funzione è disponibile per la difesa dalle minacce solo se l'opzione Snort 3 è abilitata
- Tutti i collegamenti ipertestuali nelle applicazioni Web protette devono avere un percorso relativo
- Le applicazioni Web protette in esecuzione su un host virtuale o dietro i servizi di bilanciamento del carico interni devono utilizzare lo stesso URL esterno e interno
- Non supportato nei cluster in modalità singola
- Non supportato nelle applicazioni con la convalida rigorosa dell'intestazione host HTTP abilitata

- Se il server applicazioni ospita più applicazioni e fornisce contenuto basato sull'intestazione SNI (Server Name Indication) nel client TLS Hello, l'URL esterno della configurazione dell'applicazione con attendibilità zero deve corrispondere all'SNI di tale applicazione
- Supportato solo in modalità di routing
- Smart License richiesta (non funziona in modalità di valutazione)

Per ulteriori informazioni e dettagli su Zero Trust Access in Secure Firewall, vedere la [guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, versione 7.4](#).

Configurazione

Questo documento è incentrato sulla distribuzione ad accesso remoto di ZTNA.

In questo scenario di esempio, gli utenti remoti richiedono l'accesso alle interfacce utente Web (UI) di un CMC di test e di un Cisco Telemetry Broker (CTB) ospitati dietro un firewall protetto. L'accesso a queste applicazioni viene concesso da due diversi IdP: Duo e Microsoft Entra ID, rispettivamente, come illustrato nel diagramma seguente.

Esempio di rete

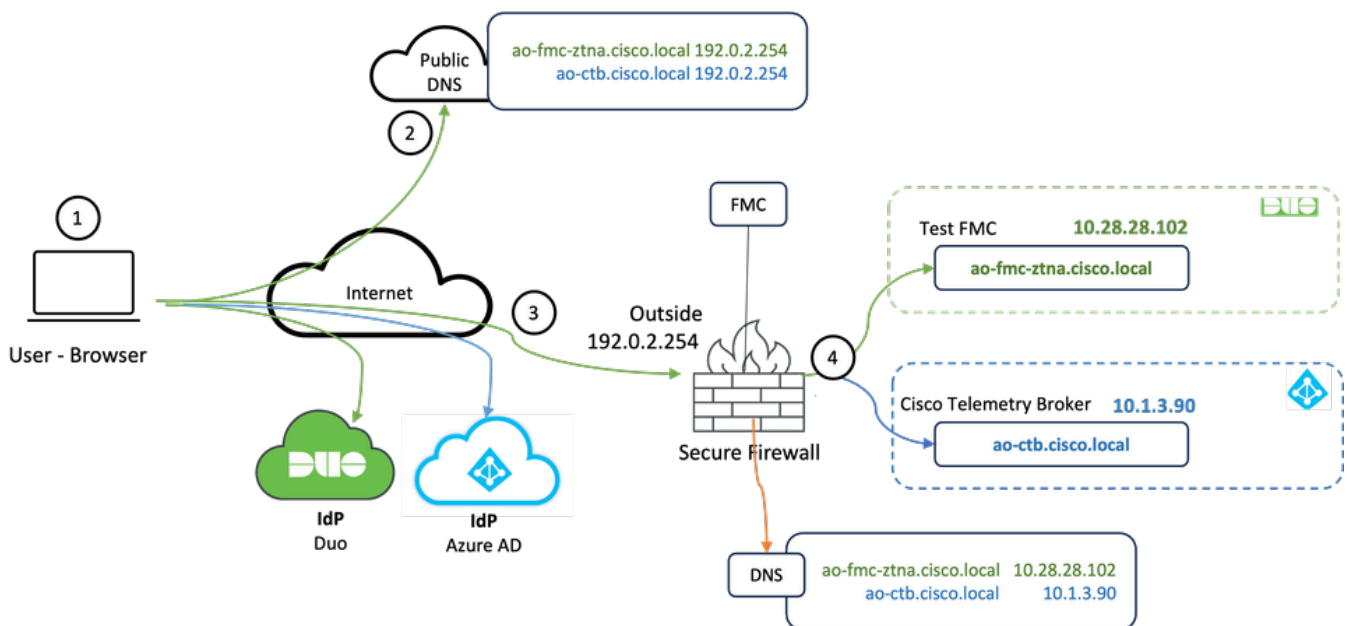


Diagramma topologico

1. Gli utenti remoti devono accedere alle applicazioni ospitate dietro Secure Firewall.
2. Ogni applicazione deve disporre di una voce DNS nei server DNS pubblici.
3. I nomi delle applicazioni devono essere risolti nell'indirizzo IP dell'interfaccia esterna del firewall protetto.
4. Secure Firewall si risolve negli indirizzi IP reali delle applicazioni e autentica ogni utente in ogni applicazione utilizzando l'autenticazione SAML.

Configurazione prerequisiti

Provider di identità (IdP) e DNS (Domain Name Server)

- Le applicazioni o i gruppi di applicazioni devono essere configurati in un provider di identità SAML (IdP), ad esempio Duo, Okta o Azure AD. Nell'esempio, Duo e Microsoft Entra ID vengono utilizzati come IdP.
- Il certificato e i metadati generati dagli IdP vengono utilizzati durante la configurazione dell'applicazione nel firewall protetto

Server DNS interni ed esterni

- I server DNS esterni (utilizzati da utenti remoti) devono avere la voce FQDN delle applicazioni e risolversi nell'indirizzo IP dell'interfaccia esterna Secure Firewall
- I server DNS interni (utilizzati da Secure Firewall) devono avere la voce FQDN delle applicazioni e risolversi nell'indirizzo IP reale dell'applicazione

Certificati

Per la configurazione dei criteri ZTNA sono necessari i certificati successivi:


- Certificato di identità/proxy: utilizzato dal firewall protetto per mascherare le applicazioni. Il firewall protetto funge da provider di servizi SAML (SP). Il certificato deve essere un carattere jolly o un certificato SAN (Subject Alternative Name) corrispondente al nome FQDN delle applicazioni private (un certificato comune che rappresenta tutte le applicazioni private nella fase di preautenticazione)
- Certificato IdP: l'IdP utilizzato per l'autenticazione fornisce un certificato per ogni applicazione o gruppo di applicazioni definito. Questo certificato deve essere configurato in modo che il firewall protetto
È in grado di verificare la firma del provider di identità sulle asserzioni SAML in ingresso (se è definita per un gruppo di applicazioni, lo stesso certificato viene utilizzato per l'intero gruppo di applicazioni)
- Certificato dell'applicazione: il traffico crittografato dall'utente remoto all'applicazione deve essere decrittografato dal firewall protetto, pertanto è necessario aggiungere al firewall protetto la catena di certificati e la chiave privata di ogni applicazione.

Configurazioni generali


Per configurare una nuova applicazione con attendibilità zero, eseguire la procedura seguente:

1. Selezionare Criteri > Controllo di accesso > Applicazione con attendibilità totale e fare clic su Aggiungi criterio.
2. Completare i campi obbligatori:
 - a) Generale: inserire il nome e la descrizione della polizza.
 - b) Nome di dominio: è il nome aggiunto al DNS e deve risolversi nell'interfaccia del gateway di

difesa delle minacce da cui si accede alle applicazioni.

 Nota: il nome di dominio viene utilizzato per generare l'URL ACS per tutte le applicazioni private in un gruppo di applicazioni.

c) Certificato di identità: si tratta di un certificato comune che rappresenta tutte le applicazioni private nella fase di preautenticazione.

 Nota: questo certificato deve essere un carattere jolly o un certificato SAN (Subject Alternative Name) corrispondente al nome di dominio completo (FQDN) delle applicazioni private.

d) Zone di sicurezza: selezionare all'esterno o/e all'interno delle zone in cui sono regolate le applicazioni private.

e) Pool globale di porte: a ciascuna applicazione privata viene assegnata una porta univoca di questo pool.

f) Controlli di sicurezza (facoltativi): selezionare se le applicazioni private sono soggette a ispezione.

In questa configurazione di esempio sono state immesse le informazioni seguenti:

Firewall Management Center
Policies / Access Control / Zero Trust Application

Overview Analysis Policies Devices Objects Integration

Deploy Q [admin] SECURE

Return to Zero Trust Application

Add a Zero Trust Application Policy

Zero Trust Application Policy protects private applications with identity based access, intrusion protection, and malware and file inspection.

Cancel Save

IP

General

Name*
ZTNA-TAC

Description

Domain Name

The domain name must resolve to the interfaces that are part of the security zones from which private applications are accessed.

Domain Name*

Ensure that the domain name is added to the DNS. The domain name resolves to the threat defense gateway interface from where the application is accessed.
The domain name is used to generate the ACS URL for all private applications in an Application Group.

Identity Certificate

A common certificate that represents all the private applications at the pre-authentication stage.

Certificate*

ZTNA-Wildcard-cert

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

Security Zones

The access to private applications is regulated through security zones. Choose outside or/and inside zones through which the private applications are regulated.

Security Zones*

Outside

This is the default setting for all private applications. It can be overridden at an Application or Application Group level.

Global Port Pool

Unique port from this pool is assigned to each private application.

Port Range*

20000-22000 Range: (1024-65535)

Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other configurations.

Security Controls (Optional)

Private applications can be subject to inspection using a selected Intrusion or Malware and File policy.

Intrusion Policy

None

Variable Set

None

Malware and File Policy

None

These are default settings for all private applications. It can be overridden at an Application or Application Group level.

Il certificato di identità/proxy utilizzato in questo caso è un certificato con caratteri jolly corrispondente al nome di dominio completo (FQDN) delle applicazioni private:

Firewall Management Center
Devices / Certificates

Overview Analysis Policies Devices Objects Integration

Deploy Q [admin] SECURE

Filter
All Certificates Add

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
ZTNA-Wildcard-cert	Global	Manual CA & EV	Oct 10, 2025		Available

Identity Certificate

- Status: Available
- Serial Number: 65-17
- Issued By:
 - CN: [redacted]
 - DC: [redacted]
 - DC: [redacted]
- Issued To:
 - CN: *.cisco.local
 - OU: TAC
 - O: Cisco
 - ST: [redacted]
 - C: [redacted]
- Public Key Type: RSA (2048 bits)
- Signature Algorithm: RSA-SHA384
- Associated Trustpoints: ZTNA-Wildcard-cert
- Valid From: 22:59:42 UTC October 11 2023
- Valid To: 22:59:42 UTC October 10 2025
- CRL Distribution Points:

Close

3. Salvare il criterio.

4. Creare i nuovi gruppi di applicazioni e/o le nuove applicazioni:

- Un'applicazione definisce un'applicazione Web privata con autenticazione SAML, accesso all'interfaccia, intrusione e criteri Malware e File.
- Un gruppo applicazioni consente di raggruppare più applicazioni e di condividere impostazioni comuni, ad esempio l'autenticazione SAML, l'accesso all'interfaccia e le impostazioni di controllo della protezione.

In questo esempio vengono configurati due diversi gruppi di applicazioni e due diverse applicazioni: una per l'applicazione che deve essere autenticata da Duo (test FMC Web UI) e una per l'applicazione che deve essere autenticata da Microsoft Entra ID (CTB Web UI).

Configura gruppo applicazioni

Gruppo applicazioni 1: utilizzo di Duo come IdP

a. Immettere il nome del gruppo di applicazioni e fare clic su Avanti per visualizzare i metadati del provider di servizi SAML (SP).

Add Application Group ? ×

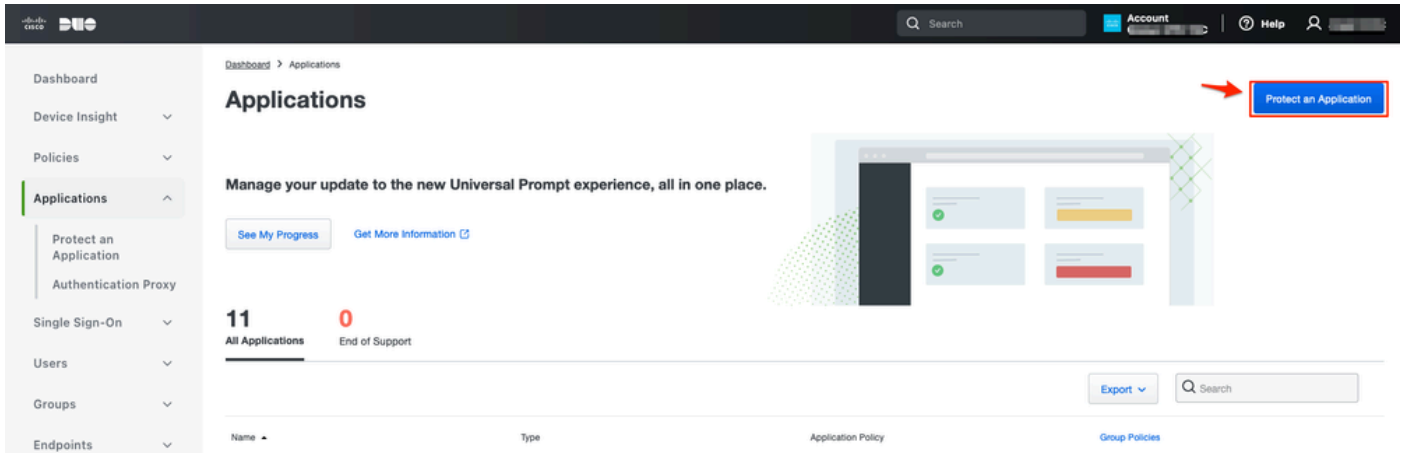
An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- 1 Application Group** Edit
Name: External_Duo
- 2 SAML Service Provider (SP) Metadata**
The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.
Entity ID: Copy
Assertion Consumer Service (ACS) URL: Copy
Download SP Metadata Next
- 3 SAML Identity Provider (IdP) Metadata**
- 4 Re-Authentication Interval**
- 5 Security Zones and Security Controls**

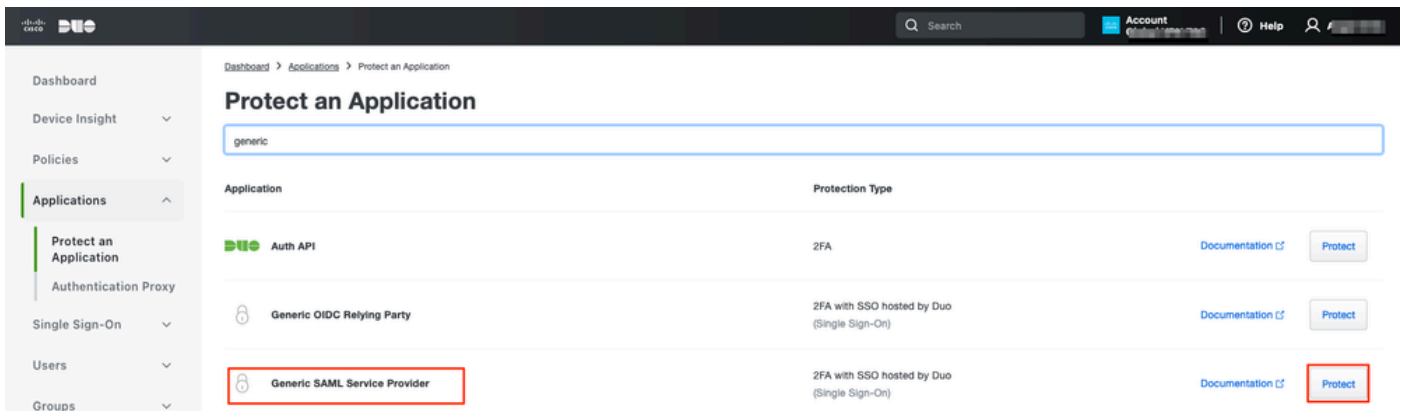
Cancel Finish

b. Una volta visualizzati i metadati dell'SP SAML, passare all'IdP e configurare una nuova applicazione SAML SSO.

c. Accedere a Duo e selezionare Applicazioni > Proteggi applicazione.



d. Cercare Generic SAML Service Provider e fare clic su Proteggi.



e. Scaricare il certificato e i metadati SAML dall'IdP poiché sono necessari per continuare la configurazione su Secure Firewall.

f. Inserire l'ID entità e l'URL del servizio consumer di asserzione (ACS) dal gruppo di applicazioni ZTNA (generato nel passo 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 *
The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *
[+ Add an ACS URL](#)

g. Modificare l'applicazione in base alle proprie esigenze specifiche e consentire l'accesso all'applicazione solo agli utenti desiderati, quindi fare clic su Salva.

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. Tornare al CCP e aggiungere i metadati IdP SAML al gruppo applicazioni, utilizzando i file scaricati dal provider di identità.

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. Fare clic su Avanti e configurare l'intervallo di riautenticazione e i controlli di sicurezza in base alle proprie esigenze. Esaminare la configurazione di riepilogo e fare clic su Fine.

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

Gruppo applicazioni 2: utilizzo di Microsoft Entra ID (Azure AD) come IdP

a. Immettere il nome del gruppo di applicazioni e fare clic su Avanti per visualizzare i metadati del provider di servizi SAML (SP).

Add Application Group



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

1 Application Group

Name **Azure_apps**

Edit

2 SAML Service Provider (SP) Metadata

The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.

Entity ID

https://[redacted]/Azure_apps/saml/sp/metadata

Copy

Assertion Consumer Service (ACS) URL

https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=[redacted]

Copy

Download SP Metadata

Next

3 SAML Identity Provider (IdP) Metadata

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

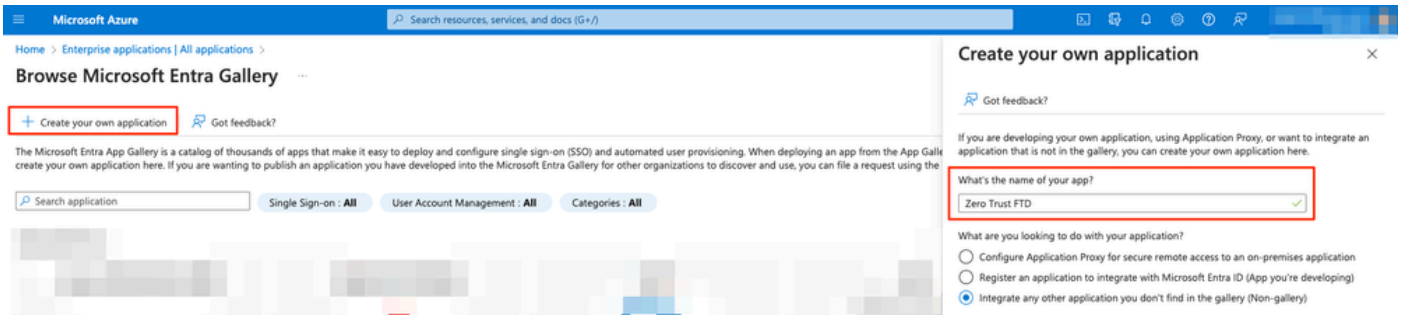
Finish

b. Una volta visualizzati i metadati dell'SP SAML, passare all'IdP e configurare una nuova applicazione SAML SSO.

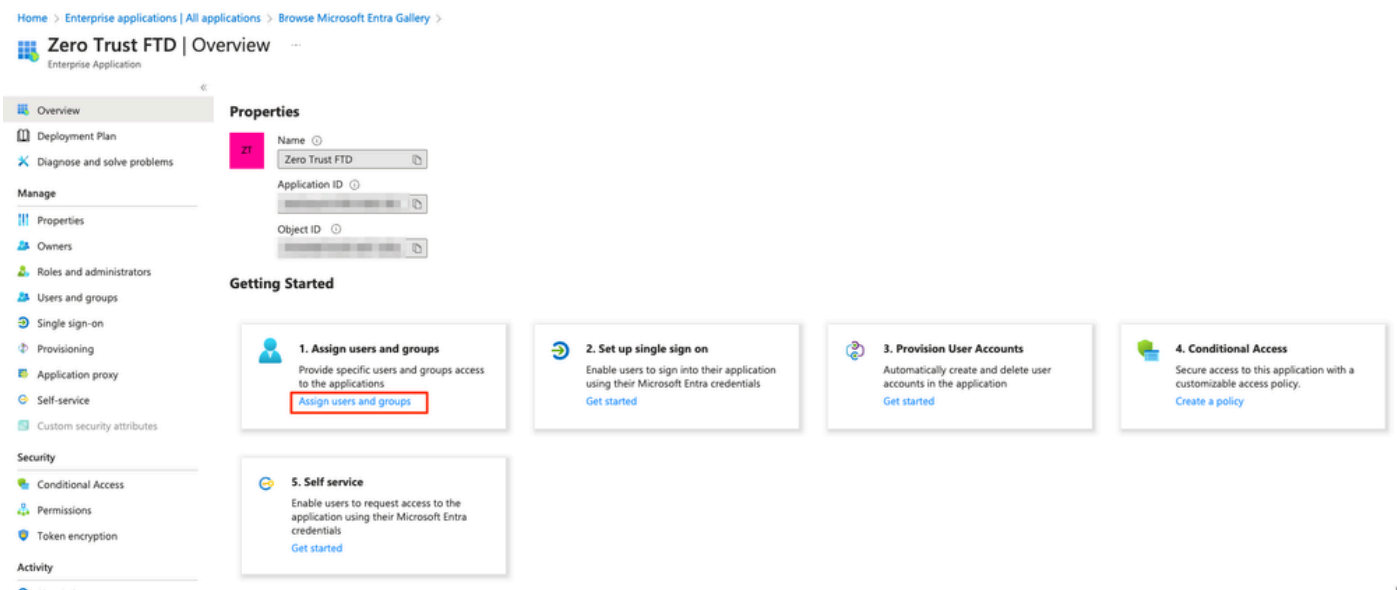
c. Accedere a Microsoft Azure e selezionare Applicazioni aziendali > Nuova applicazione.

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'. Below the heading, there is a search bar and several action buttons: '+ New application' (highlighted with a red box), 'Refresh', 'Download (Export)', 'Preview info', 'Columns', 'Preview features', and 'Got feedback?'. The left sidebar has a 'Manage' section with 'All applications' (highlighted with a red box) and 'Application proxy'. The main content area shows a table with 77 applications found, with columns for Name, Object ID, Application ID, Homepage URL, and Created on.

d. Fare clic su Create your own application > Enter the name of the application > Create



e. Aprire l'applicazione e fare clic su Assegna utenti e gruppi per definire gli utenti e/o i gruppi autorizzati ad accedere all'applicazione.



f. Fare clic su Add user/group > Select the needed users/groups > Assign (Aggiungi utente/gruppo > Seleziona gli utenti/gruppi necessari > Assegna). Una volta assegnati gli utenti/gruppi corretti, fare clic su Single Sign-On.

Zero Trust FTD | Users and groups

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups

Single sign-on

+ Add user/group

1

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. Nella sezione Single Sign-on, fare clic su SAML.

Zero Trust FTD | Single sign-on

Enterprise Application


- 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. Fare clic su Upload metadata file (Carica file metadati) e selezionare il file XML scaricato dal provider di servizi (Secure Firewall) oppure immettere manualmente l'ID entità e l'URL del servizio consumer di asserzione (ACS) dal gruppo di applicazioni ZTNA (generato nel passaggio a).

 **Nota:** accertarsi di scaricare anche il file XML dei metadati federativi o di scaricare singolarmente il certificato (base 64) e copiare i metadati SAML dal provider di identità (URL di accesso e disconnessione e identificatori di accesso Microsoft) poiché sono necessari per continuare la configurazione sul firewall protetto.

Zero Trust FTD | SAML-based Sign-on

Enterprise Application

« [Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#) | [Got feedback?](#)

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Troubleshooting + Support

- New support request

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Zero Trust FTD.

- ### Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	https://[redacted]/Azure_apps/saml/sp/metadata
Reply URL (Assertion Consumer Service URL)	https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tgname=DefaultZeroTrustGroup
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- ### Attributes & Claims [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- ### SAML Certificates

Token signing certificate [Edit](#)

Status	Active
Thumbprint	[redacted]
Expiration	[redacted]
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) [Edit](#)

Required	No
Active	0
Expired	0
- ### Set up Zero Trust FTD

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://[redacted]
Microsoft Entra Identifier	https://[redacted]
Logout URL	https://[redacted]

i. Tornare al CCP e importare i metadati IdP SAML nel gruppo di applicazioni 2, utilizzando il file di metadati scaricato dal provider di identità o immettere manualmente i dati richiesti.

Add Application Group



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

1 Application Group

Name **Azure_apps**

Edit

2 SAML Service Provider (SP) Metadata

Entity ID **https://[redacted]/Azure_apps/saml/sp/metadata**
Assertion Consumer Service (ACS) URL **https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=Def...**

Edit

3 SAML Identity Provider (IdP) Metadata

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

Import IdP Metadata

Manual Configuration

Configure Later

Import IdP Metadata

Drag and drop your file here
or [select file](#)
Zero Trust FTD.xml

Entity ID*

https://[redacted]

Single Sign-On URL*

https://[redacted]

IdP Certificate

MIIc8DCCAdigAwIBAgIQdTt7Lwlj7aRGm1m212dU/DANBgkqhkiG9w0B

[Redacted certificate content]

Next

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

Finish

j. Fare clic su Avanti e configurare l'intervallo di riautenticazione e i controlli di sicurezza in base alle proprie esigenze. Esaminare la configurazione di riepilogo e fare clic su Fine.

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?tgname=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

Configura applicazioni


Dopo aver creato i gruppi di applicazioni, fare clic su **Aggiungi applicazione** per definire le applicazioni da proteggere e a cui accedere in remoto.

1. Immettere le impostazioni dell'applicazione:

a) Nome applicazione: identificatore dell'applicazione configurata.

b) URL esterno: URL pubblicato dell'applicazione nei record DNS pubblici/esterni. URL utilizzato dagli utenti per accedere all'applicazione in remoto.

c) URL applicazione: FQDN reale o IP di rete dell'applicazione. URL utilizzato da Secure Firewall per raggiungere l'applicazione.

 **Nota:** per impostazione predefinita, l'URL esterno viene utilizzato come URL applicazione. Deselezionare la casella di controllo per specificare un URL applicazione diverso.

d) Certificato applicazione: la catena di certificati e la chiave privata dell'applicazione a cui accedere (aggiunta dalla home page di FMC > Oggetti > Gestione oggetti > PKI > Certificati

interni)

e) Origine NAT IPv4 (opzionale): l'indirizzo IP di origine dell'utente remoto viene convertito negli indirizzi selezionati prima di inoltrare i pacchetti all'applicazione (sono supportati solo oggetti di rete/gruppi di oggetti di tipo Host e Range con indirizzi IPv4). Questa impostazione può essere configurata per garantire che le applicazioni dispongano di un percorso di ritorno agli utenti remoti tramite il firewall protetto

f) Gruppo applicazioni (facoltativo): selezionare questa opzione se l'applicazione viene aggiunta a un gruppo applicazioni esistente per utilizzare le impostazioni configurate per l'applicazione.

In questo esempio, le applicazioni a cui è possibile accedere utilizzando ZTNA sono un'interfaccia utente Web di test FMC e l'interfaccia utente Web di un CTB che si trova dietro il firewall protetto.

I certificati delle applicazioni devono essere aggiunti in Oggetti > Gestione oggetti > PKI > Certificati interni:

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:

 Nota: assicurarsi di aggiungere tutti i certificati per ogni applicazione a cui si accede con ZTNA.

Dopo aver aggiunto i certificati come certificati interni, continuare a configurare le restanti impostazioni.

Le impostazioni dell'applicazione configurate per questo esempio sono:

Applicazione 1: interfaccia utente Web del CCP di test (membro del gruppo di applicazioni 1)

Enabled **1 Application Settings**

Application Name*

FMC

External URL* ⓘ

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

Application URL (FQDN or Network IP)*

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

 Use External URL as Application URL

By default, External URL is used as Application URL. Uncheck the checkbox to specify a different URL. For e.g., https://10.72.34.57:8443

Application Certificate* ⓘ

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

IPv4 NAT Source ⓘ

Select... v +

Application Group

External_Duo x v

Next

2 SAML Service Provider (SP) Metadata

3 SAML Identity Provider (IdP) Metadata

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

Finish

Poiché l'applicazione è stata aggiunta al gruppo di applicazioni 1, le restanti impostazioni vengono ereditate per questa applicazione. È comunque possibile ignorare le aree di protezione e i controlli di protezione con impostazioni diverse.

Rivedere l'applicazione configurata e fare clic su Fine.

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

Applicazione 2: Interfaccia utente Web CTB (membro del gruppo di applicazioni 2)

Il riepilogo della configurazione per questa applicazione è il seguente:

Enabled

1 Application Settings Edit

Application Name: CTB
 External URL: https://ao-ctb.cisco.local
 Application URL: https://ao-ctb.cisco.local
 IPv4 NAT Source: ZTNA_NAT_CTB
 Application Certificate: ao-ctb.cisco.local
 Application Group: Azure_apps

2 SAML Service Provider (SP) Metadata
 Configurations are derived from Application Group 'Azure_apps'


3 SAML Identity Provider (IdP) Metadata
 Configurations are derived from Application Group 'Azure_apps'

4 Re-Authentication Interval
 Configurations are derived from Application Group 'Azure_apps'

5 Security Zones and Security Controls Edit

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

Cancel Finish

 Nota: per questa applicazione, un oggetto di rete "ZTNA_NAT_CTB" è stato configurato come origine NAT IPv4. Con questa configurazione, l'indirizzo IP di origine degli utenti remoti viene convertito in un indirizzo IP all'interno dell'oggetto configurato prima di inoltrare i pacchetti all'applicazione. Questa configurazione è stata eseguita perché il percorso predefinito dell'applicazione (CTB) punta a un gateway diverso dal firewall protetto, pertanto il traffico di ritorno non è stato inviato agli utenti remoti. Con questa configurazione NAT, è stata configurata nell'applicazione una route statica affinché la subnet ZTNA_NAT_CTB sia raggiungibile tramite il firewall protetto.

Una volta configurate, le applicazioni vengono visualizzate nel gruppo di applicazioni corrispondente.

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
<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


Infine, salvare le modifiche e distribuire la configurazione.

Verifica

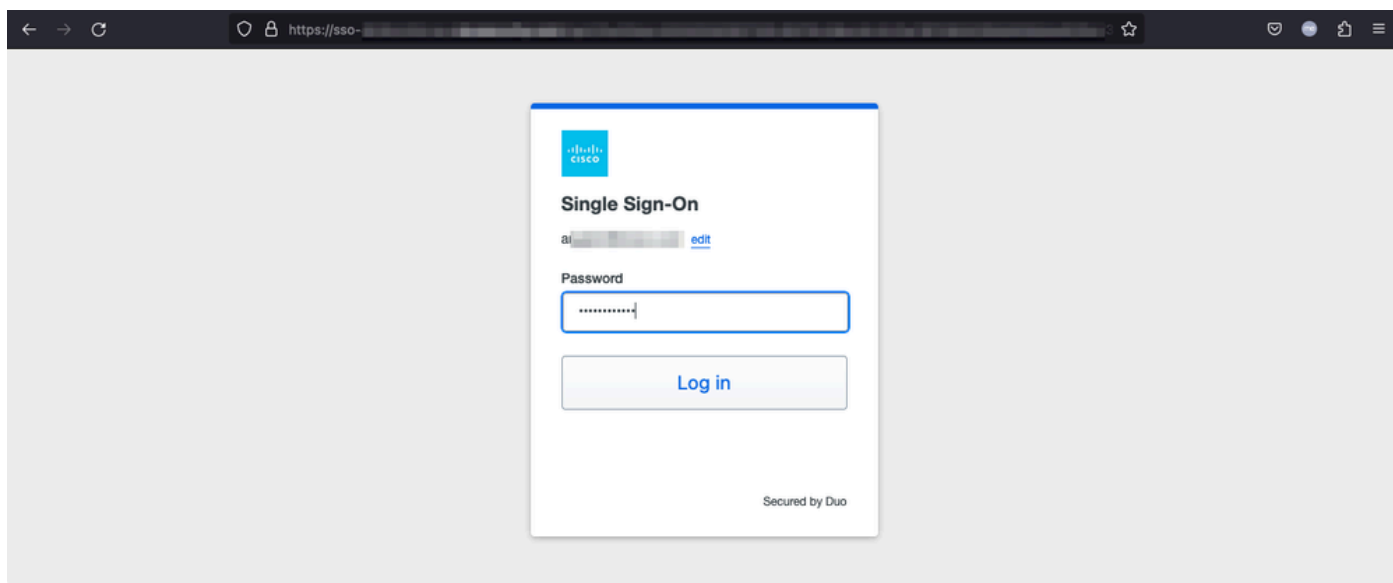
Una volta implementata la configurazione, gli utenti remoti possono raggiungere le applicazioni tramite l'URL esterno e, se autorizzati dal provider di identità corrispondente, possono accedervi.

Applicazione 1

1. L'utente apre un browser web e naviga all'URL esterno dell'applicazione 1. In questo caso, l'URL esterno è "https://ao-fmc-ztna.cisco.local/"

 Nota: il nome dell'URL esterno deve essere risolto nell'indirizzo IP dell'interfaccia del firewall protetto configurata. Nell'esempio, viene risolto nell'indirizzo IP dell'interfaccia esterna (192.0.2.254)

2. Poiché si tratta di un nuovo accesso, l'utente viene reindirizzato al portale di accesso IdP configurato per l'applicazione.

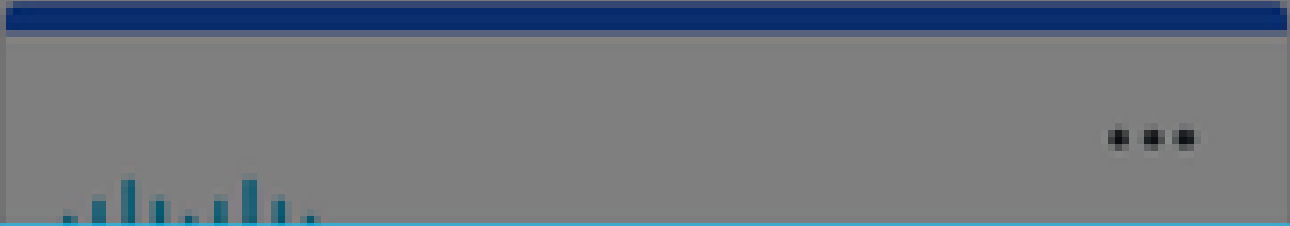


3. All'utente viene inviato un Push per l'autenticazione a più fattori (dipende dal metodo di autenticazione a più fattori configurato nell'IdP).



Accounts

Add




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

🌐 Global VPN TAC

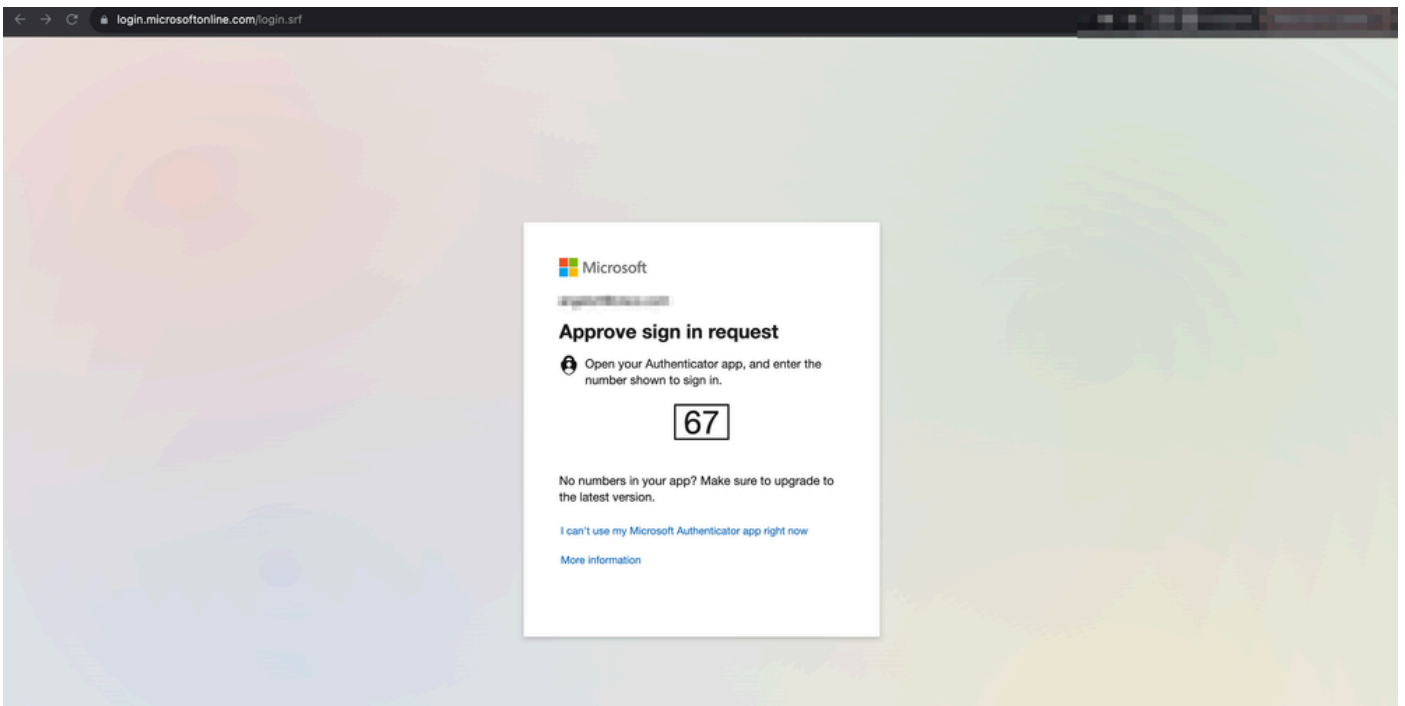
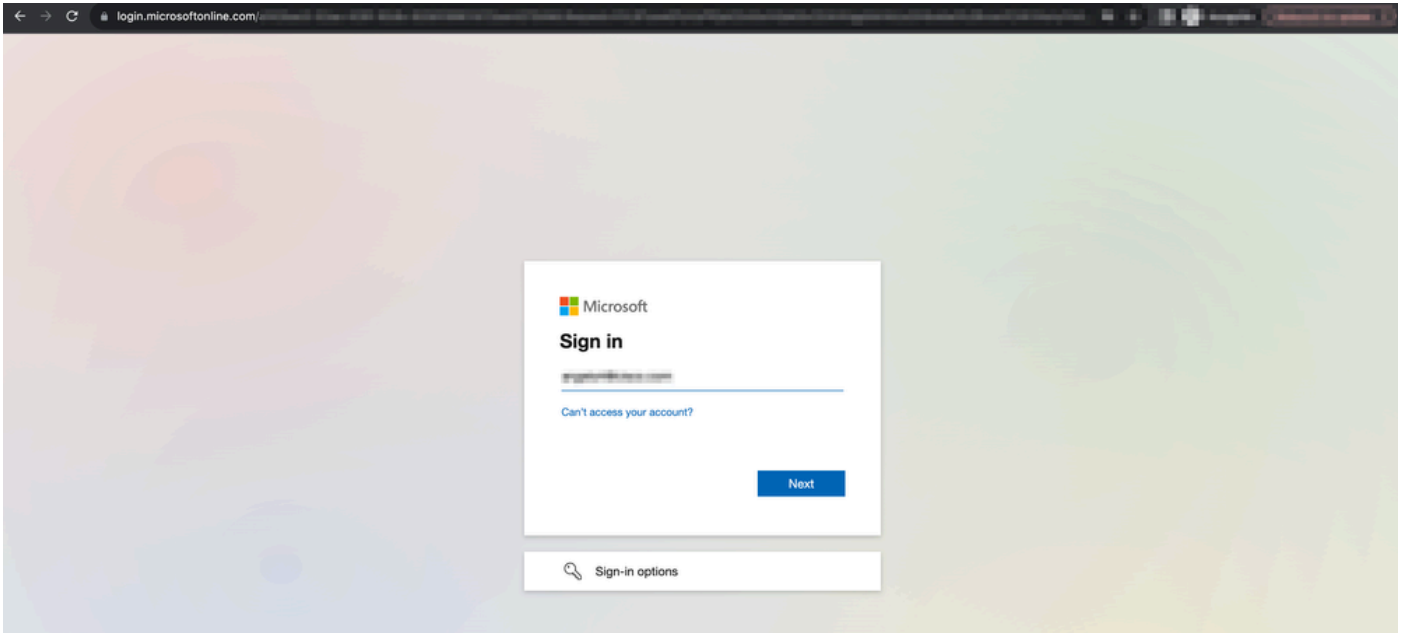
🌐 [Redacted]

🕒 1:13 p.m.

👤 [Redacted]

 : il nome dell'URL esterno deve essere risolto nell'indirizzo IP dell'interfaccia del firewall protetto configurata. Nell'esempio, viene risolto nell'indirizzo IP dell'interfaccia esterna (192.0.2.254)

2. Poiché si tratta di un nuovo accesso, l'utente viene reindirizzato al portale di accesso IdP configurato per l'applicazione.

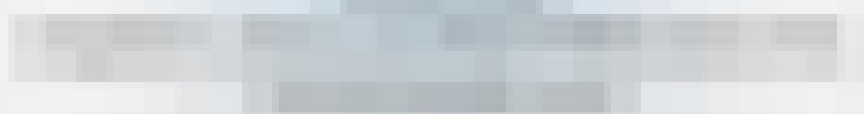


3. All'utente viene inviato un Push per l'autenticazione a più fattori (dipende dal metodo di autenticazione a più fattori configurato nell'IdP).

4:24



Are you trying to sign in?



Enter the number shown to sign in.

Enter number

No, it's not me

Yes

- La diagnostica fornisce un'analisi globale (OK o meno) e raccoglie i registri dettagliati che possono essere analizzati per risolvere i problemi

La diagnostica specifica dell'applicazione viene utilizzata per rilevare:



- Problemi relativi al DNS
- Configurazione errata, ad esempio socket non aperto, regole di classificazione, regole NAT
- Problemi nei criteri di accesso con attendibilità totale
- Problemi relativi all'interfaccia, ad esempio interfaccia non configurata o interfaccia non attiva

Diagnostica generica da rilevare:

- Se non è abilitata una licenza di cifratura avanzata
- Se il certificato dell'applicazione non è valido
- Se il metodo di autenticazione non è inizializzato su SAML nel gruppo di tunnel predefinito
- Problemi di sincronizzazione globale cluster e disponibilità elevata
- Ottieni informazioni dai contatori degli snort per diagnosticare problemi, ad esempio quelli relativi ai token o alla decrittografia
- Problema di esaurimento del pool PAT nella traduzione di origine.

Per eseguire la diagnostica:

1. Passare all'icona di diagnostica presente per ciascuna applicazione ZTNA.

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

2. Selezionare una periferica e fare clic su Esegui.

Select Device

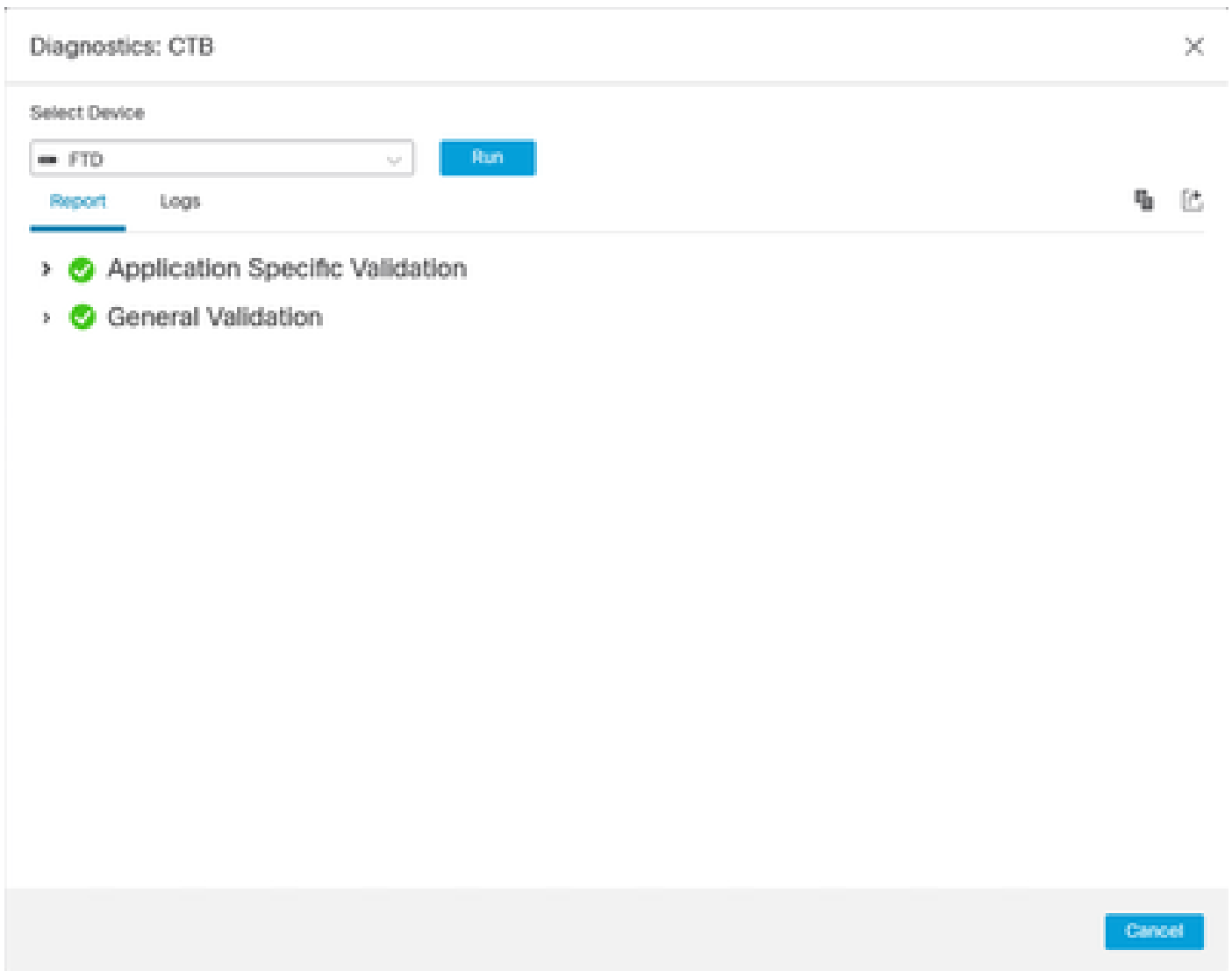
Select...

FTD

Run

Cancel

3. Visualizzare i risultati nel rapporto.



I comandi show e clear sono disponibili nella CLI FTD per visualizzare la configurazione con attendibilità zero e le statistiche e le informazioni sulla sessione.

```
<#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>
```

Per abilitare i debug di attendibilità zero e del modulo webvpn, usare i comandi successivi nel prompt di Lina:

- firepower# debug zero-trust 255
- firepower# debug webvpn richiesta 255
- firepower# debug webvpn risposta 255
- firepower# debug webvpn saml 255

Informazioni correlate

- Per ulteriore assistenza, contattare il Technical Assistance Center (TAC). È necessario un contratto di supporto valido: [Contatti del supporto Cisco internazionali](#).
- [Qui](#) è possibile anche visitare la Cisco VPN Community.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).