

Configurar a Implantação de Acesso Remoto Zero Trust no Firewall Seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração de pré-requisito](#)

[Configurações gerais](#)

[Configurar Grupo de Aplicativos](#)

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

[Grupo de Aplicativos 2: Usando o Microsoft Entra ID \(Azure AD\) como IdP](#)

[Configurar aplicativos](#)

[Aplicação 1: Testar a interface do usuário da Web do FMC \(membro do grupo de aplicação 1\)](#)

[Aplicação 2: IU da Web do CTB \(membro do grupo de aplicações 2\)](#)

[Verificar](#)

[Monitor](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o processo de configuração da implantação do Acesso Remoto sem Confiança Sem Cliente em um Firewall Seguro.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Firepower Management Center (FMC)
- Conhecimento básico da ZTNA
- Conhecimento de SAML (Basic Security Assertion Markup Language)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Secure Firewall versão 7.4.1
- Firepower Management Center (FMC) versão 7.4.1
- Duo como provedor de identidade (IdP)
- Microsoft Entra ID (anteriormente, Azure AD) como IdP

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O recurso Acesso Zero Trust é baseado nos princípios do Acesso à Rede Zero Trust (ZTNA). O ZTNA é um modelo de segurança de confiança zero que elimina a confiança implícita. O modelo concede o acesso de privilégio mínimo depois de verificar o usuário, o contexto da solicitação e depois de analisar o risco se o acesso for concedido.

Os requisitos e limitações atuais para a ZTNA são:

- Compatível com o Secure Firewall versão 7.4.0+ gerenciado pelo FMC versão 7.4.0+ (Firepower 4200 Series)
- Compatível com o Secure Firewall versão 7.4.1+ gerenciado pelo FMC versão 7.4.1+ (Todas as outras plataformas)
- Somente aplicativos da Web (HTTPS) são suportados. Não há suporte para cenários que requerem isenção de descryptografia
- Suporta somente IdPs SAML
- Atualizações de DNS público são necessárias para acesso remoto
- IPv6 sem suporte. Os cenários NAT66, NAT64 e NAT46 não são suportados
- O recurso estará disponível na defesa contra ameaças somente se o Snort 3 estiver habilitado
- Todos os hiperlinks em aplicativos da Web protegidos devem ter um caminho relativo
- Os aplicativos Web protegidos executados em um host virtual ou atrás de balanceadores de carga internos devem usar a mesma URL externa e interna
- Sem suporte em clusters de modo individual
- Não há suporte em aplicativos com validação de Cabeçalho de Host HTTP estrita habilitada
- Se o servidor de aplicativos hospedar vários aplicativos e fornecer conteúdo baseado no

cabeçalho SNI (Server Name Indication) no Hello do cliente TLS, a URL externa da configuração do aplicativo de confiança zero deverá corresponder ao SNI desse aplicativo específico

- Suportado somente no Modo Roteado
- Licença inteligente necessária (não funciona no modo de avaliação)

Para obter mais informações e detalhes sobre o Zero Trust Access no Secure Firewall, consulte o [Cisco Secure Firewall Management Center Device Configuration Guide, 7.4](#).

Configurar

Este documento se concentra em uma implantação de acesso remoto do ZTNA.

Neste cenário de exemplo, os usuários remotos exigem acesso às interfaces de usuário da Web (IU) de um FMC de teste e um Cisco Telemetry Broker (CTB) que são hospedados atrás de um firewall seguro. O acesso a esses aplicativos é concedido por dois IdPs diferentes: Duo e Microsoft Entra ID, respectivamente, como mostrado no próximo diagrama.

Diagrama de Rede

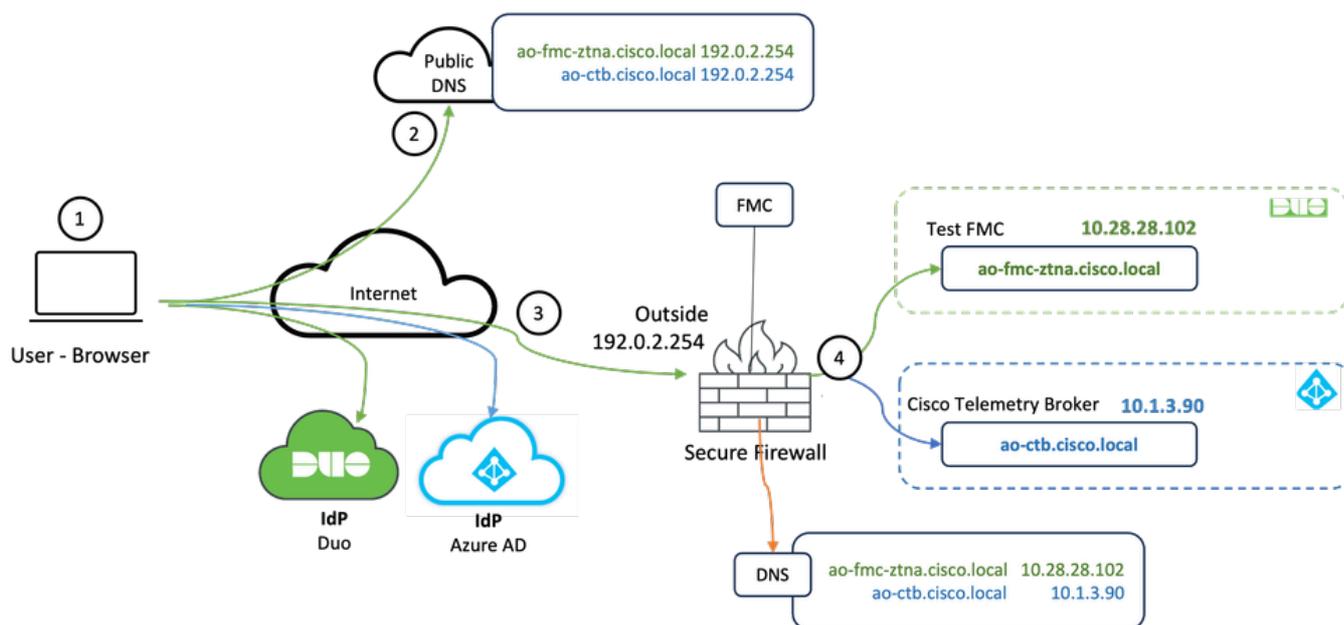


Diagrama de topologia

1. Os usuários remotos precisam acessar aplicativos hospedados por trás do Firewall Seguro.
2. Cada aplicativo deve ter uma entrada DNS nos servidores DNS públicos.
3. Esses nomes de aplicativos devem ser resolvidos para o endereço IP da interface externa do firewall seguro.
4. O Firewall Seguro resolve para os endereços IP reais dos aplicativos e autentica cada usuário para cada aplicativo usando a autenticação SAML.

Configuração de pré-requisito

Provedor de Identidade (IdP) e Servidor de Nome de Domínio (DNS)

- Os aplicativos ou grupos de aplicativos devem ser configurados em um Provedor de Identidade SAML (IdP), como Duo, Okta ou Azure AD. Neste exemplo, Duo e Microsoft Entra ID são usados como IdPs.
- O certificado e os metadados gerados pelos IdPs são usados ao configurar o aplicativo no Firewall Seguro

Servidores DNS internos e externos

- Os servidores DNS externos (usados por usuários remotos) devem ter a entrada FQDN dos aplicativos e devem ser resolvidos para o endereço IP da interface externa do Secure Firewall
- Servidores DNS internos (usados pelo Firewall Seguro) devem ter a entrada FQDN dos aplicativos e resolver para o endereço IP real do aplicativo

Certificados

Os próximos certificados são necessários para a configuração da Política ZTNA:

- Certificado de identidade/proxy: usado pelo Firewall seguro para mascarar os aplicativos. Aqui, o Firewall Seguro atua como um Provedor de Serviços (SP) SAML. Este certificado deve ser um curinga ou um certificado SAN (Nome Alternativo da Entidade) que corresponda ao FQDN dos aplicativos privados (um certificado comum que representa todos os aplicativos privados no estágio de pré-autenticação)
- Certificado IdP: o IdP usado para autenticação fornece um certificado para cada aplicativo ou grupo de aplicativos definido. Este certificado deve ser configurado para que o Firewall Seguro
É capaz de verificar a assinatura do IdP em asserções SAML de entrada (se isso for definido para um grupo de aplicativos, o mesmo certificado será usado para todo o grupo de aplicativos)
- Certificado do aplicativo: o tráfego criptografado do usuário remoto para o aplicativo precisa ser descriptografado pelo Secure Firewall; portanto, a cadeia de certificados e a chave privada de cada aplicativo devem ser adicionadas ao Secure Firewall.

Configurações gerais

Para configurar um novo aplicativo Zero Trust, execute as próximas etapas:

1. Navegue para Políticas > Access Control > Zero Trust Application e clique em Add Policy.
2. Preencha os campos obrigatórios:
 - a) Geral: Informe o nome e a descrição da política.
 - b) Nome do domínio: Este é o nome que é adicionado ao DNS e deve ser resolvido para a

interface do gateway de defesa contra ameaças a partir do qual os aplicativos são acessados.

 Observação: o nome de domínio é usado para gerar o URL do ACS para todos os aplicativos privados em um Grupo de Aplicativos.

c) Certificado de identidade: é um certificado comum que representa todos os aplicativos privados na fase de pré-autenticação.

 Observação: este certificado deve ser um curinga ou um certificado SAN (Nome Alternativo da Entidade) que corresponda ao FQDN dos aplicativos privados.

d) Zonas de segurança: Selecione fora ou/e dentro das zonas através das quais os aplicativos privados são regulados.

e) Pool de Portas Global: Uma porta exclusiva desse pool é atribuída a cada aplicação privada.

f) Controles de segurança (opcional): Selecione se os aplicativos privados estão sujeitos a inspeção.

Nesta configuração de exemplo, as próximas informações foram inseridas:

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.

O certificado de identidade/proxy usado neste caso é um certificado curinga para corresponder ao FQDN dos aplicativos privados:

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: *
 - 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. Salve a política.

4. Crie os novos Grupos de Requisições e/ou novas Requisições:

- Um Aplicativo define um aplicativo Web privado com autenticação SAML, acesso à interface, políticas de Intrusão e Malware e Arquivo.
- Um Grupo de Aplicativos permite agrupar vários Aplicativos e compartilhar configurações comuns, como autenticação SAML, acesso à interface e configurações de controle de segurança.

Neste exemplo, dois grupos de aplicativos diferentes e dois aplicativos diferentes são configurados: um para o aplicativo ser autenticado pelo Duo (teste da IU da Web do FMC) e um para o aplicativo ser autenticado pela ID do Microsoft Entra (IU da Web do CTB).

Configurar Grupo de Aplicativos

Grupo de aplicativos 1: Uso do Duo como IdP

a. Insira o Application Group Name e clique em Next para que os Metadados do provedor de serviços (SP) SAML sejam exibidos.

Add Application Group ? ×

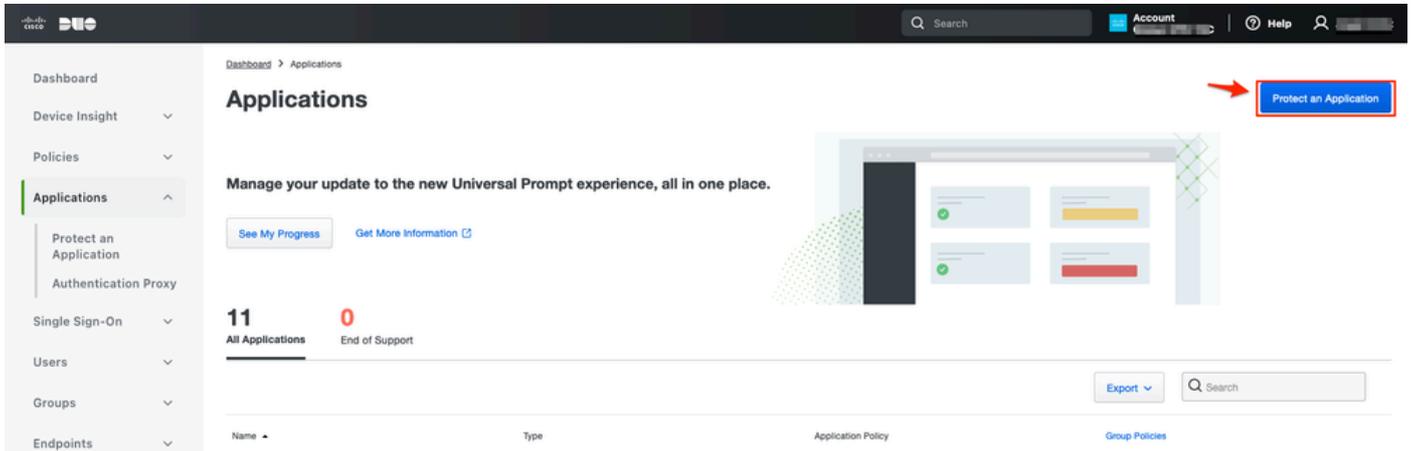
An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- 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**

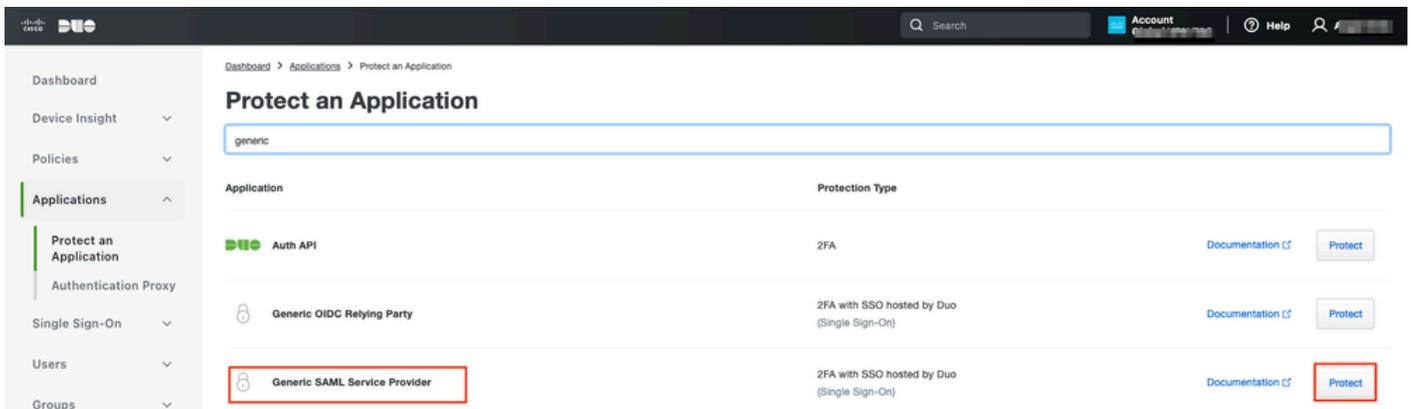
Cancel Finish

b. Quando os Metadados de SP SAML forem exibidos, vá para o IdP e configure um novo aplicativo SAML SSO.

c. Faça login no Duo e navegue até Applications > Protect an Application.



d. Procure Generic SAML Service Provider e clique em Protect.



e. Baixe o certificado e os metadados SAML do IdP, pois são necessários para continuar a configuração no Secure Firewall.

f. Insira o ID da entidade e o URL do serviço de consumidor de asserção (ACS) do grupo de aplicativos ZTNA (gerado na etapa 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. Edite o aplicativo de acordo com seus requisitos específicos e permita o acesso ao aplicativo somente aos usuários desejados e clique em Salvar.

Type Generic SAML Service Provider - Single Sign-On

Name
 Duo Push users will see this when approving transactions.

Self-service portal Let users remove devices, add new devices, and reactivate Duo Mobile
 See [Self-Service Portal documentation](#)
 To allow Duo to notify users about self-service portal activity, select [Settings > Notifications](#)

Username normalization Username normalization for Single-Sign On applications is controlled by the enabled authentication source. Please visit your [authentication source](#) to modify this configuration.
 Controls if a username should be altered before trying to match them with a Duo user account.

Voice greeting
 Specify the message read to users who use phone callback, followed by authentication instructions. Maximum 512 characters.

Notes
 For internal use. Maximum 512 characters.

Administrative unit

Permitted groups Only allow authentication from users in certain groups

 When unchecked, all users can authenticate to this application.

Allowed Hostnames Since this application is using Frameless Duo Universal Prompt, configuring allowed hostnames is no longer supported.
 [Get more information](#)

h. Navegue de volta para o FMC e adicione os metadados SAML IdP ao grupo de aplicativos, usando os arquivos baixados do IdP.

Add Application Group



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

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

3 SAML Identity Provider (IdP) Metadata

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

Import IdP Metadata
 Manual Configuration
 Configure Later

Import IdP Metadata

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

Entity ID*
https://sso-8[redacted] N

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

IdP Certificate
MIIDDTC[redacted]yDQYJKoZI
[redacted]

Next

Cancel Finish

i. Clique em Next e configure o Re-Authentication Interval e os Security Controls de acordo com seus requisitos. Revise a configuração de resumo e clique em Finish.

Add Application Group



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

1 Application Group	Name	External_Duo	Edit
2 SAML Service Provider (SP) Metadata	Entity ID	https://[redacted] External_Duo/saml/sp/metadata	Edit
	Assertion Consumer Service (ACS) URL	https://[redacted] External_Duo/+CSCOE+/saml/sp/acs?tgname=D...	
3 SAML Identity Provider (IdP) Metadata	Entity ID	https://ssc [redacted]	Edit
	Single Sign-On URL	https://ssc [redacted]	
	IdP Certificate	External_Duo-1697063490514	
4 Re-Authentication Interval	Timeout Interval	1440 minutes	Edit
5 Security Zones and Security Controls	Security Zones	Inherited: (Outside)	Edit
	Intrusion Policy	Inherited: (None)	
	Variable Set	Inherited: (None)	
	Malware and File Policy	Inherited: (None)	

Cancel

Finish

Grupo de Aplicativos 2: Usando o Microsoft Entra ID (Azure AD) como IdP

a. Insira o Application Group Name e clique em Next para que os Metadados do provedor de serviços (SP) SAML sejam exibidos.

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

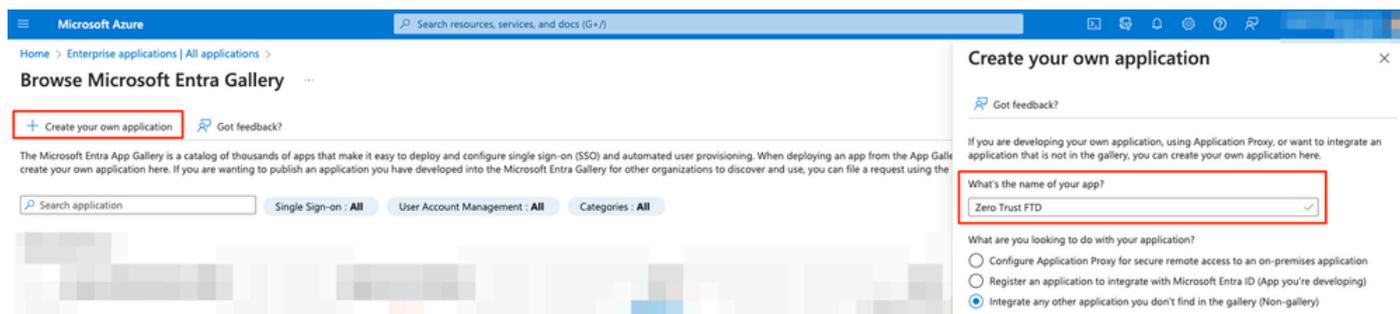
Finish

b. Quando os Metadados de SP SAML forem exibidos, vá para o IdP e configure um novo aplicativo SAML SSO.

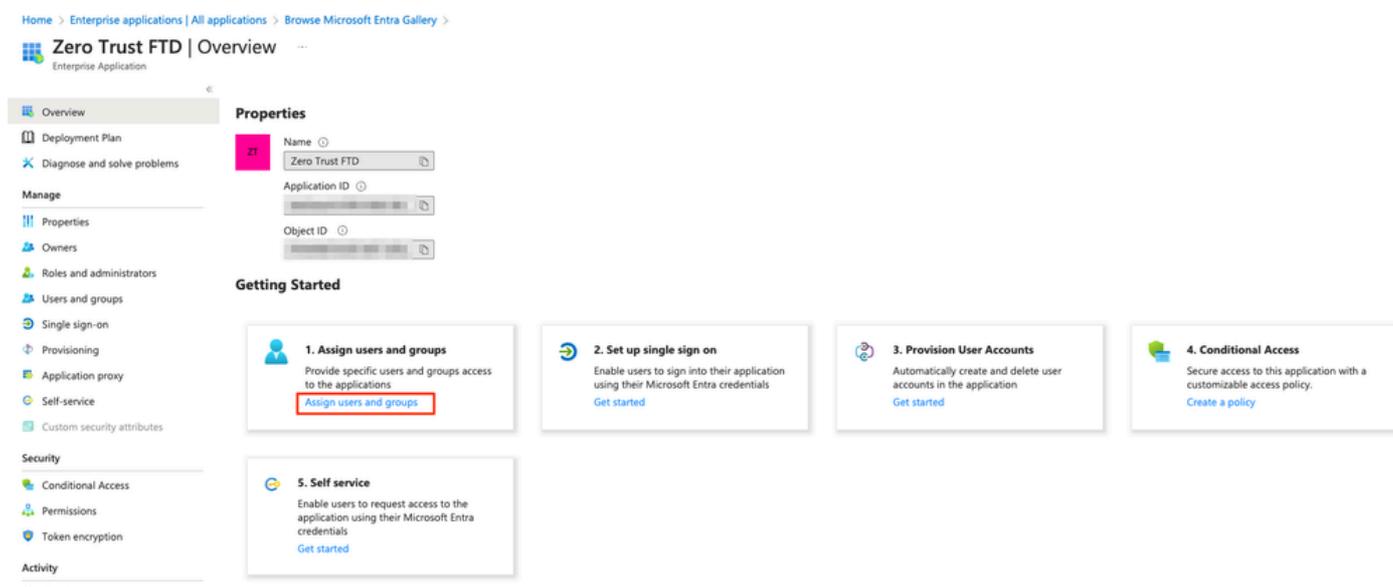
c. Faça login no Microsoft Azure e navegue para Aplicativos corporativos > Novo Aplicativo.

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and navigation links. The main heading is "Enterprise applications | All applications". Below this, there is a sidebar with navigation options: "Overview", "Diagnose and solve problems", and "Manage". Under "Manage", "All applications" is highlighted with a red box. The main content area shows a list of applications with columns for Name, Object ID, Application ID, Homepage URL, and Created on. A red box highlights the "+ New application" button. The page also includes a search bar for applications and several filters, such as "Application type == Enterprise Applications".

d. Clique em Create your own application > Insira o nome do aplicativo > Create



e. Abra o aplicativo e clique em Atribuir usuários e grupos para definir os usuários e/ou grupos que podem acessar o aplicativo.



f. Clique em Add user/group > Select the needed users/groups > Assign. Depois de atribuir os usuários/grupos corretos, clique em Logon único.

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. Na seção Single sign-on, clique em 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. Clique em Upload metadata file e selecione o arquivo XML baixado do Service Provider (Secure Firewall) ou insira manualmente a ID da entidade e a URL do Assertion Consumer Service (ACS) do Grupo de Aplicativos ZTNA (gerada na etapa a).

 **Observação:** certifique-se de também fazer download do XML de Metadados de Federação ou fazer download individual do Certificado (base 64) e copiar os Metadados SAML do IdP (URLs de Logon e Logoff e Identificadores Microsoft Entra), pois eles são necessários para continuar a configuração no Firewall Seguro.

Zero Trust FTD | SAML-based Sign-on

Enterprise Application

<< **Upload metadata file** >> Change single sign-on mode | Test this application | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs
 - Provisioning logs
 - Access reviews
- Troubleshooting + Support
 - New support request

Set up Single Sign-On with SAML

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

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

- Basic SAML Configuration** Edit

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

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

Token signing certificate	Active	Edit
Status		
Thumbprint	[redacted]	
Expiration	[redacted]	
Notification Email	[redacted]	
App Federation Metadata Url	[redacted]	Download
Certificate (Base64)		Download
Certificate (Raw)		Download
Federation Metadata XML		Download
Verification certificates (optional)		Edit
Required	No	
Active	0	
Expired	0	
- Set up Zero Trust FTD**

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

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

i. Navegue de volta para o FMC e importe os metadados IdP SAML para o grupo de aplicativos 2, usando o arquivo de metadados baixado do IdP ou insira manualmente os dados necessários.

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. Clique em Next e configure o Re-Authentication Interval e os Security Controls de acordo com seus requisitos. Revise a configuração de resumo e clique em Finish.

Add Application Group ? X

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

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

Cancel
Finish

Configurar aplicativos

Agora que os Grupos de Aplicativos foram criados, clique em Adicionar Aplicativo para definir os aplicativos a serem protegidos e acessados remotamente.

1. Insira as Configurações do aplicativo:

- a) Nome do aplicativo: identificador do aplicativo configurado.
- b) URL externa: URL publicada do aplicativo nos registros DNS públicos/externos. Este é o URL usado pelos usuários para acessar o aplicativo remotamente.
- c) URL do aplicativo: FQDN real ou IP de rede do aplicativo. Este é o URL usado pelo Firewall Seguro para acessar o aplicativo.

Observação: por default, o URL Externo é usado como URL do Aplicativo. Desmarque a caixa de seleção para especificar um URL de aplicativo diferente.

d) Application Certificate: a cadeia de certificados e a chave privada do aplicativo a ser acessado (Adicionado de FMC Home Page > Objects > Object Management > PKI > Internal

certs)

e) Origem NAT IPv4 (opcional): O endereço IP origem do usuário remoto é convertido para os endereços selecionados antes de encaminhar os pacotes para o aplicativo (somente objetos de rede do tipo Host e Intervalo/grupos de objetos com endereços IPv4 são suportados). Isso pode ser configurado para garantir que os aplicativos tenham uma rota de volta para os usuários remotos através do Firewall Seguro

f) Grupo de Aplicativos (opcional): Selecione se este Aplicativo for adicionado a um Grupo de Aplicativos existente para usar as configurações definidas para ele.

Neste exemplo, os aplicativos a serem acessados usando ZTNA são uma interface de usuário da Web do FMC de teste e a interface de usuário da Web de um CTB localizado atrás do Firewall seguro.

Os certificados dos Aplicativos devem ser adicionados em Objetos > Gerenciamento de objetos > PKI > Certificados internos:

Add Known Internal Certificate



Name:

ao-fmc-ztna.cisco.local

Certificate Data or, choose a file:

[Browse..](#)

```
-----BEGIN CERTIFICATE-----
[Redacted Certificate Data]
T
G
AY
```

Key or, choose a file:

[Browse..](#)

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

Encrypted, and the password is:

.....

[Cancel](#)

[Save](#)

Observação: certifique-se de adicionar todos os certificados para cada aplicativo a ser acessado com ZTNA.

Depois que os certificados tiverem sido adicionados como certificados internos, continue definindo as configurações restantes.

As configurações de Aplicativo definidas para este exemplo são:

Aplicação 1: Testar a interface do usuário da Web do FMC (membro do grupo de aplicação 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

Como o aplicativo foi adicionado ao Grupo de Aplicativos 1, as configurações restantes são herdadas para este aplicativo. Você ainda pode substituir as Zonas de segurança e os Controles de segurança por configurações diferentes.

Revise o aplicativo configurado e clique em Finish.

Add Application



Enabled

Edit

1 Application Settings

Application Name	FMC
External URL	https://ao-fmc-ztna.cisco.local
Application URL	https://ao-fmc-ztna.cisco.local
IPv4 NAT Source	-
Application Certificate	ao-fmc-ztna.cisco.local
Application Group	External_Duo

2 SAML Service Provider (SP) Metadata

Configurations are derived from Application Group 'External_Duo'

3 SAML Identity Provider (IdP) Metadata

Configurations are derived from Application Group 'External_Duo'

4 Re-Authentication Interval

Configurations are derived from Application Group 'External_Duo'

5 Security Zones and Security Controls

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

Edit

Cancel

Finish

Aplicação 2: IU da Web do CTB (membro do grupo de aplicações 2)

O resumo da configuração para este aplicativo é o seguinte:

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_CTBT
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

 **Observação:** observe que, para esse aplicativo, um objeto de rede "ZTNA_NAT_CTBT" foi configurado como origem de NAT IPv4. Com essa configuração, o endereço IP de origem dos usuários remotos é convertido em um endereço IP dentro do objeto configurado antes de encaminhar os pacotes para o aplicativo. Isso foi configurado porque a rota padrão do aplicativo (CTB) aponta para um gateway diferente do Firewall Seguro, portanto, o tráfego de retorno não foi enviado para os usuários remotos. Com essa configuração de NAT, uma rota estática foi configurada no aplicativo para que a sub-rede ZTNA_NAT_CTBT fosse alcançável através do Firewall Seguro.

Depois que os aplicativos forem configurados, eles serão exibidos no grupo de aplicativos correspondente.

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.cisco.local	Outside (Inherited)	None (Inherited)	None (Inherited)	True
<input type="checkbox"/> CTB	https://ao-ctb.cisco.local	https://ao-ctb.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True
<input checked="" type="checkbox"/> External_Duo (1 Application)			https://sso.cisco.local	Outside (Inherited)	None (Inherited)	None (Inherited)	True
<input type="checkbox"/> FMC	https://ao-fmc-ztna.cisco.local	https://ao-fmc-ztna.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True

Finalmente, salve as alterações e implante a configuração.

Verificar

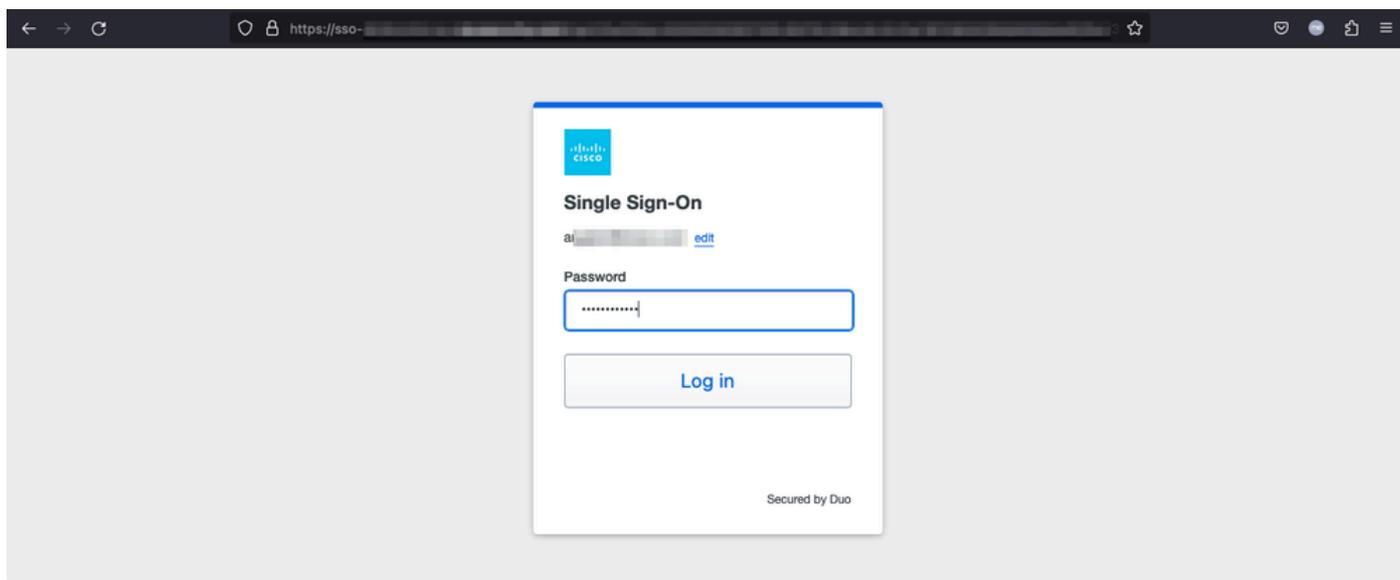
Uma vez que a configuração esteja em vigor, os usuários remotos podem acessar os aplicativos através da URL externa e, se eles forem permitidos pelo IdP correspondente, ter acesso a ela.

Aplicativo 1

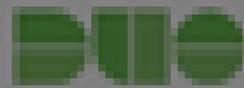
1. O usuário abre um navegador da Web e navega até o URL externo do aplicativo 1. Nesse caso, o URL externo é "https://ao-fmc-ztna.cisco.local/"

 Observação: o nome da URL externa deve ser resolvido para o endereço IP da interface do Firewall Seguro que foi configurada. Neste exemplo, ele resolve para o endereço IP da interface externa (192.0.2.254)

2. Como este é um novo acesso, o usuário é redirecionado para o portal de login IdP configurado para o aplicativo.



3. O usuário recebe uma mensagem Push for MFA (isso depende do método MFA configurado no IdP).



Accounts

Add



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

🌐 Global VPN TAC

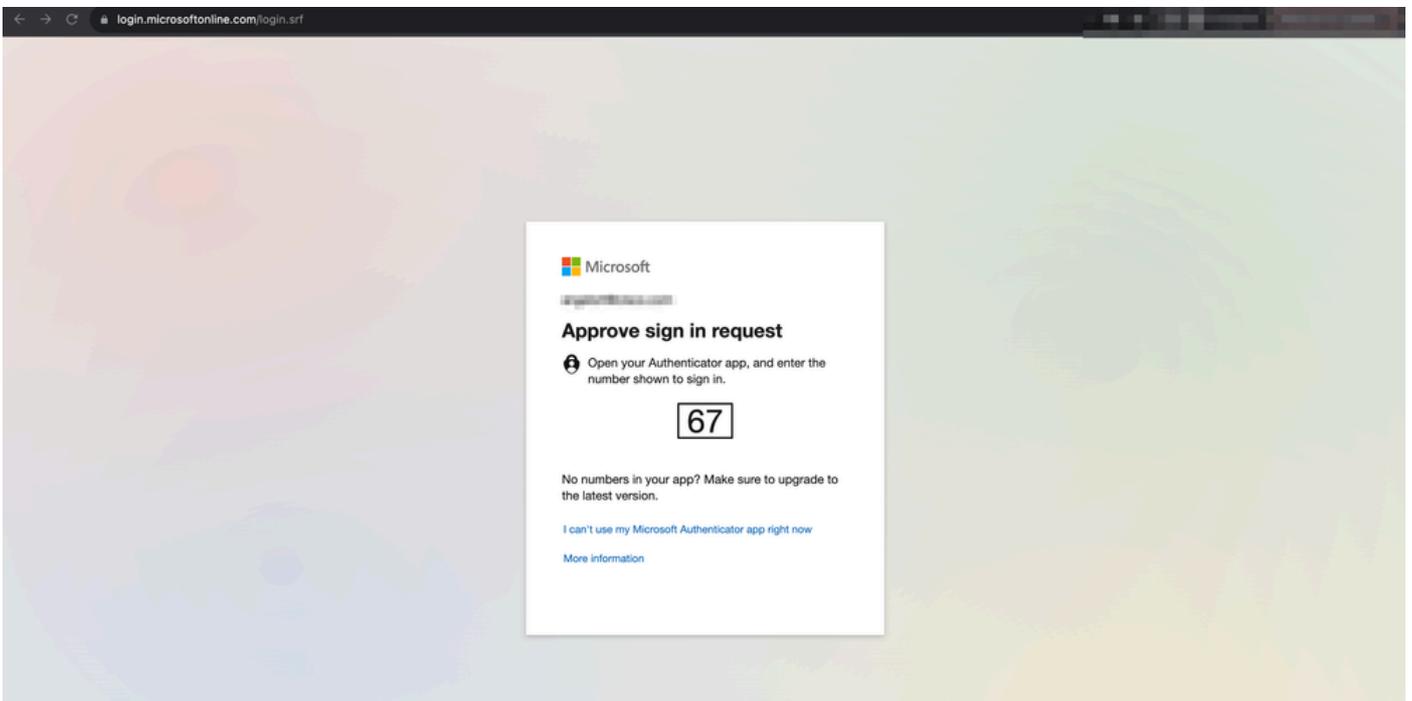
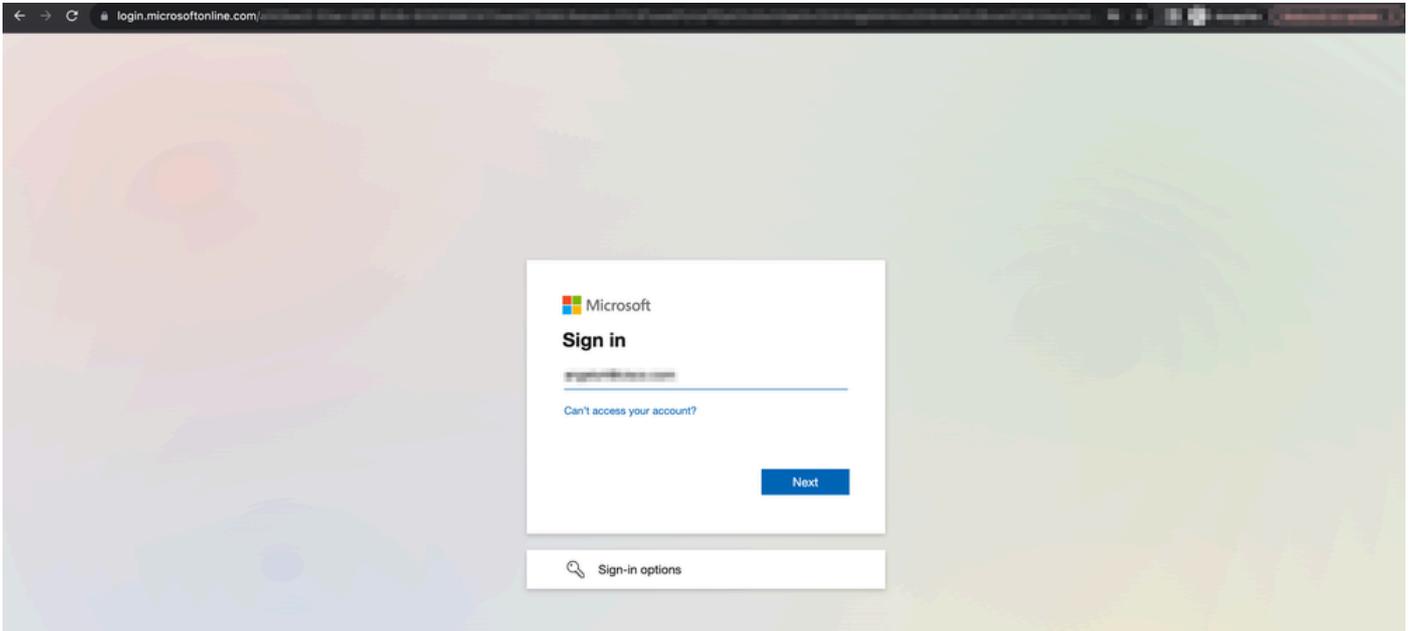
🌐 [Redacted]

🕒 1:13 p.m.

👤 [Redacted]

 : o nome da URL externa deve ser resolvido para o endereço IP da interface do Firewall Seguro que foi configurada. Neste exemplo, ele resolve para o endereço IP da interface externa (192.0.2.254)

2. Como este é um novo acesso, o usuário é redirecionado para o portal de login IdP configurado para o aplicativo.



3. O usuário recebe uma mensagem Push for MFA (isso depende do método MFA configurado no IdP).

4:24



Are you trying to sign in?



Enter the number shown to sign in.

Enter number

No, it's not me

Yes

- O diagnóstico fornece uma análise geral (OK ou não) e coleta registros detalhados que podem ser analisados para solucionar problemas

O Diagnóstico específico do aplicativo é usado para detectar:

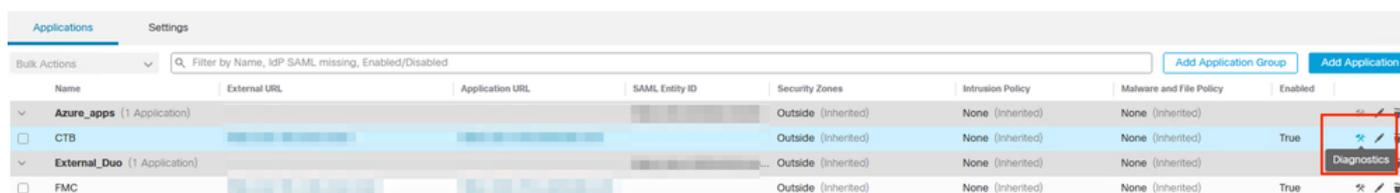
- Problemas relacionados ao DNS
- Configuração incorreta, por exemplo, soquete não aberto, regras de classificação, regras de NAT
- Problemas na Política de Acesso de Confiança Zero
- Problemas relacionados à interface, por exemplo, interface não configurada ou interface inoperante

Diagnóstico genérico a ser detectado:

- Se uma licença de codificação forte não estiver habilitada
- Se o certificado do aplicativo não for válido
- Se o método de autenticação não for inicializado para SAML no grupo de túnel padrão
- Problemas de sincronização em massa de alta disponibilidade e cluster
- Obtenha informações dos contadores de snort para diagnosticar problemas, como aqueles relacionados a tokens ou descriptografia
- Problema de esgotamento do pool PAT na tradução de origem.

Para executar o diagnóstico:

1. Navegue até o ícone diagnostics presente para cada ZTNA Application.



Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled	
▼ Azure_apps (1 Application)				Outside (Inherited)	None (Inherited)	None (Inherited)		
<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. Selecione um dispositivo e clique em Executar.

Select Device

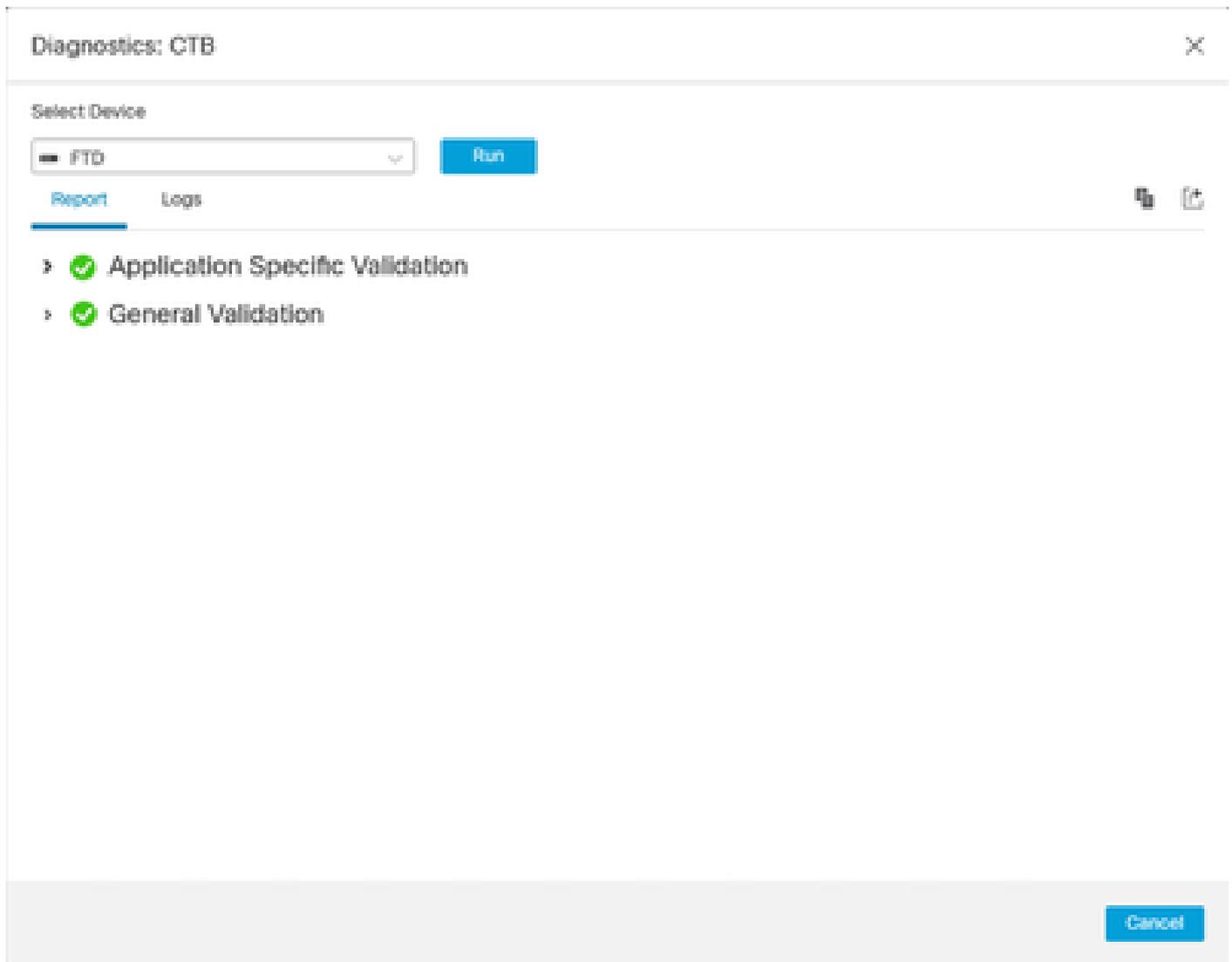
Select...

FTD

Run

Cancel

3. Exiba os resultados no relatório.



Os comandos show e clear estão disponíveis na CLI do FTD para exibir a configuração zero-trust e exibir estatísticas e informações de sessão.

```
<#root>
```

```
firepower# show running-config zero-trust
```

```
application      Show application configuration information
application-group Show application group configuration
|                Output modifiers
<cr>
```

```
firepower# show zero-trust
```

```
sessions  Show zero-trust sessions
statistics Show zero-trust statistics
```

```
firepower# show zero-trust sessions
```

```
application      show zero-trust sessions for application
application-group show zero-trust sessions for application group
count            show zero-trust sessions count
user            show zero-trust sessions for user
detail          show detailed info for the session
|              Output modifiers
<cr>
```

```
firepower# clear zero-trust
```

```
sessions  Clear all zero-trust sessions
statistics Clear all zero-trust statistics
```

```
firepower# clear zero-trust sessions
```

```
application Clear zero-trust sessions for application
user        Clear zero-trust sessions for user
<cr>
```

Para ativar as depurações do módulo zero-trust e webvpn, use os comandos seguintes no prompt do Lina:

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

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Centro de Assistência Técnica (TAC). É necessário um contrato de suporte válido: [Cisco Worldwide Support Contacts](#).
- Você também pode visitar a Cisco VPN Community [aqui](#).

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.