在安全防火墙上配置零信任远程访问部署

目录

简介

本文档介绍在安全防火墙上配置无客户端零信任访问远程访问部署的流程。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower Management Center (FMC)
- 基本ZTNA知识
- 基本安全断言标记语言(SAML)知识

使用的组件

本文档中的信息基于以下软件版本：

- 安全防火墙版本7.4.1
- Firepower管理中心(FMC)版本7.4.1

- Duo作为身份提供程序(IdP)
- Microsoft Entra ID（以前称为Azure AD）作为IdP

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

零信任访问功能基于零信任网络访问(ZTNA)原则。ZTNA是一种消除隐式信任的零信任安全模型。该模型在验证用户、请求上下文以及分析访问被授予的风险后授予最小权限访问权限。

ZTNA的当前要求和限制如下：

- 受FMC版本7.4.0+（Firepower 4200系列）管理的安全防火墙版本7.4.0+支持
- 受FMC版本7.4.1+管理的安全防火墙版本7.4.1+支持（所有其他平台）
- 仅支持Web应用(HTTPS)。不支持需要解密豁免的场景
- 仅支持SAML IdP
- 远程访问需要公共DNS更新
- 不支持IPv6。不支持NAT66、NAT64和NAT46场景
- 只有在启用Snort 3后，此功能才可用于威胁防御
- 受保护的Web应用程序中的所有超链接必须具有相对路径
- 在虚拟主机上运行或在内部负载平衡器后面运行的受保护的Web应用程序必须使用相同的外部和内部URL
- 在个别模式集群上不受支持
- 启用了严格HTTP主机报头验证的应用程序不支持
- 如果应用服务器托管多个应用并根据TLS客户端Hello中的服务器名称指示(SNI)信头提供内容，则零信任应用配置的外部URL必须与特定应用的SNI匹配
- 仅在路由模式下支持
- 需要智能许可证（不在评估模式下运行）

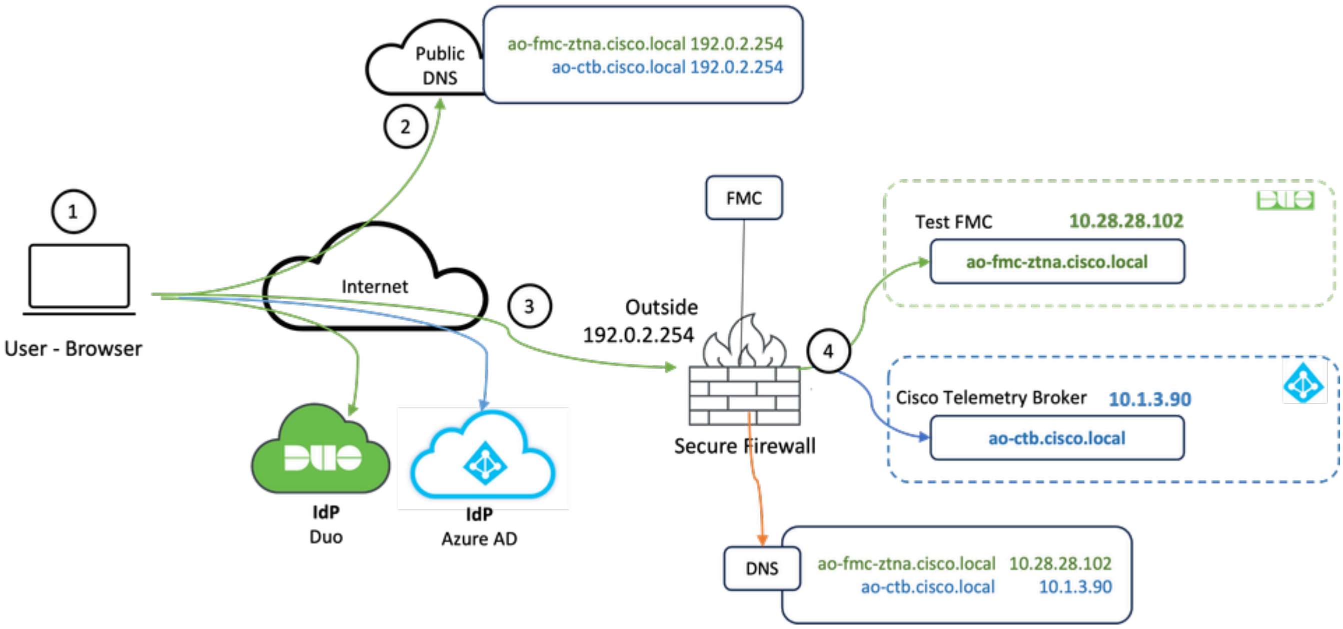
有关安全防火墙中的零信任访问的详细信息和详细信息，请参阅Cisco安全防火墙管理中心设备配置指南7.4。

配置

本文档重点介绍ZTNA的远程访问部署。

在此示例场景中，远程用户需要访问测试FMC的Web用户界面(UI)和思科遥测代理(CTB)，它们托管在安全防火墙之后。访问这些应用程序时，会分别通过两个不同的IdP授予：Duo和Microsoft Entra ID，如下图所示。

网络图



Public DNS
ao-fmc-ztna.cisco.local 192.0.2.254
ao-ctb.cisco.local 192.0.2.254
2
1
User - Browser
Internet
3
Outside
192.0.2.254
FMC
Test FMC 10.28.28.102
ao-fmc-ztna.cisco.local
4
Cisco Telemetry Broker 10.1.3.90
ao-ctb.cisco.local
Secure Firewall
IdP
Duo
IdP
Azure AD
DNS
ao-fmc-ztna.cisco.local 10.28.28.102
ao-ctb.cisco.local 10.1.3.90

拓扑图

1. 远程用户需要访问托管在安全防火墙之后的应用。
2. 每个应用程序在公共DNS服务器中必须有一个DNS条目。
3. 这些应用程序名称必须解析为Secure Firewall Outside接口的IP地址。
4. 安全防火墙解析为应用的实际IP地址，并使用SAML身份验证对每个应用验证每个用户。

前提条件配置

身份提供程序(IdP)和域名服务器(DNS)

- 必须在SAML身份提供程序(IdP)中配置应用程序或应用程序组，例如Duo、Okta或Azure AD。在本示例中，Duo和Microsoft Entra ID用作IdP。
- 在安全防火墙上配置应用时，使用IdP生成的证书和元数据

内部和外部DNS服务器

- 外部DNS服务器（供远程用户使用）必须具有应用程序的FQDN条目，并解析到安全防火墙外部接口IP地址
- 内部DNS服务器（由安全防火墙使用）必须具有应用程序的FQDN条目，并解析为应用程序的实际IP地址

证书

ZTNA策略配置需要以下证书：

- 身份/代理证书：由安全防火墙用于伪装应用。此处的安全防火墙充当SAML服务提供商(SP)。此证书必须是通配符或使用者可选名称(SAN)证书，该证书与专用应用的FQDN匹配（在预身份验证阶段代表所有专用应用的通用证书）
- IdP证书：用于身份验证的IdP为定义的每个应用或应用组提供证书。必须配置此证书，以便安全防火墙
  能够验证传入SAML断言上的IdP签名（如果这是针对应用组定义的，则同一证书用于整个应用组）
- 应用证书：从远程用户到应用的加密流量需要由安全防火墙解密，因此，每个应用的证书链和私钥必须添加到安全防火墙。

常规配置

要配置新的零信任应用，请执行以下步骤：

1. 导航到Policies > Access Control > Zero Trust Application，然后单击Add Policy。
2. 填写必填字段：

a)General：输入策略的名称和说明。

b)域名：这是添加到DNS的域名，必须解析到访问应用的威胁防御网关接口。

注：域名用于为应用组中的所有专用应用生成ACS URL。

c)身份证书：这是代表预身份验证阶段的所有专用应用的通用证书。

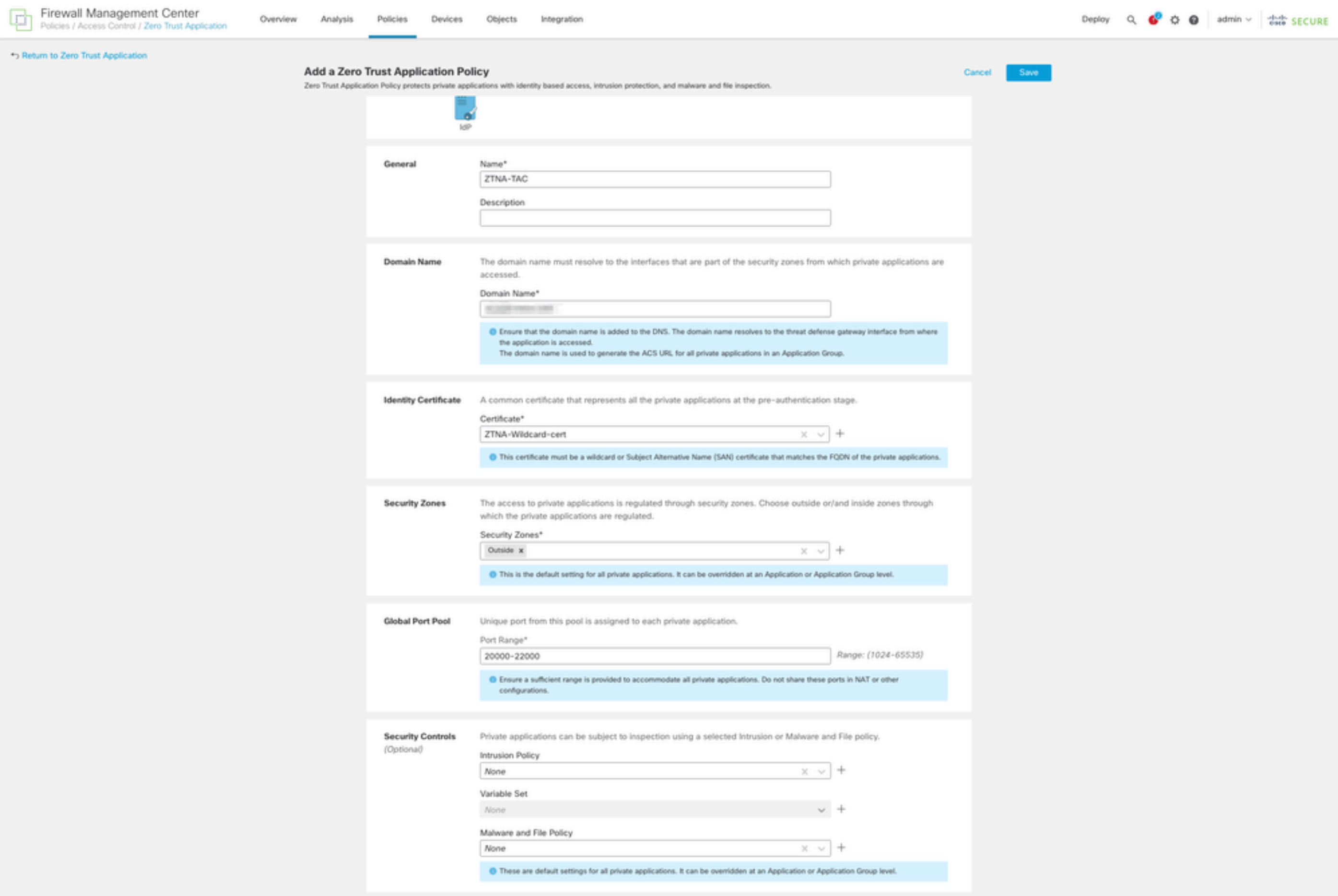
注意：此证书必须是通配符或与专用应用的FQDN匹配的主题备用名称(SAN)证书。

d)安全区域：选择用于管理专用应用的外部或/和内部区域。

e)全局端口池：此池中的唯一端口分配给每个专用应用。

f)安全控制（可选）：选择是否对私有应用进行检查。

在此示例配置中，输入了以下信息：



Firewall Management Center
Policies / Access Control / Zero Trust Application
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Return to Zero Trust Application
IdP
Cancel
Save

Add a Zero Trust Application Policy

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

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.

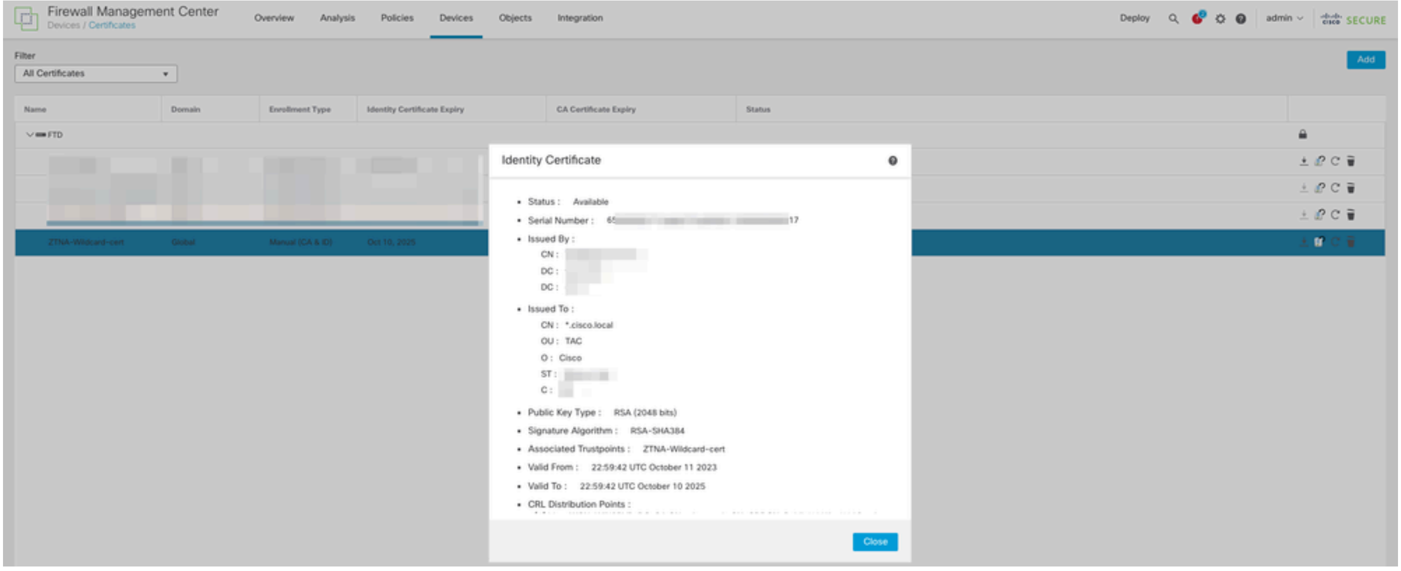
Intrusion Policy: *None*

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.

本例中使用的身份/代理证书是通配符证书，用于匹配专用应用的FQDN:



Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
FTD					
[redacted]					
ZTNA-Wildcard-cert	Global	Manual (CA & ID)	Oct 10, 2025		

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 :

3.保存策略。

4.创建新应用组和/或新应用：

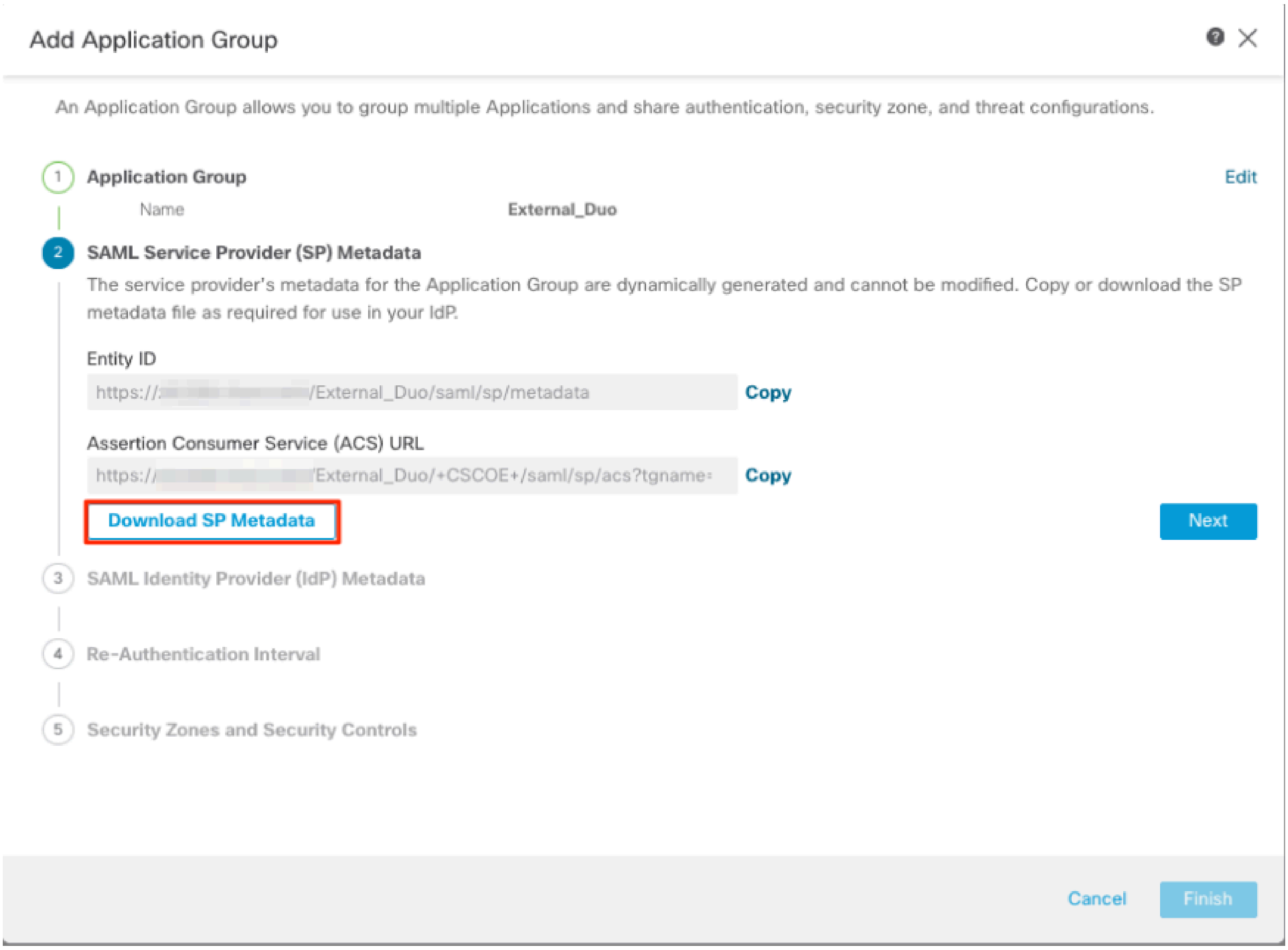
- 应用定义具有SAML身份验证、接口访问、入侵和恶意软件以及文件策略的专用Web应用。
- Application Group允许您对多个应用进行分组，并共享通用设置，例如SAML身份验证、接口访问和安全控制设置。

在本示例中，配置两个不同的应用程序组和两个不同的应用程序：一个用于要由Duo进行身份验证的应用程序（测试FMC Web UI），另一个用于要由Microsoft Entra ID(CTB Web UI)进行身份验证的应用程序。

配置应用组

应用组1：使用Duo作为IdP

a.输入Application Group Name，然后单击Next以显示SAML Service Provider(SP)元数据。



Add Application Group

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

1 Application Group — Edit

Name: External_Duo

2 SAML Service Provider (SP) Metadata

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

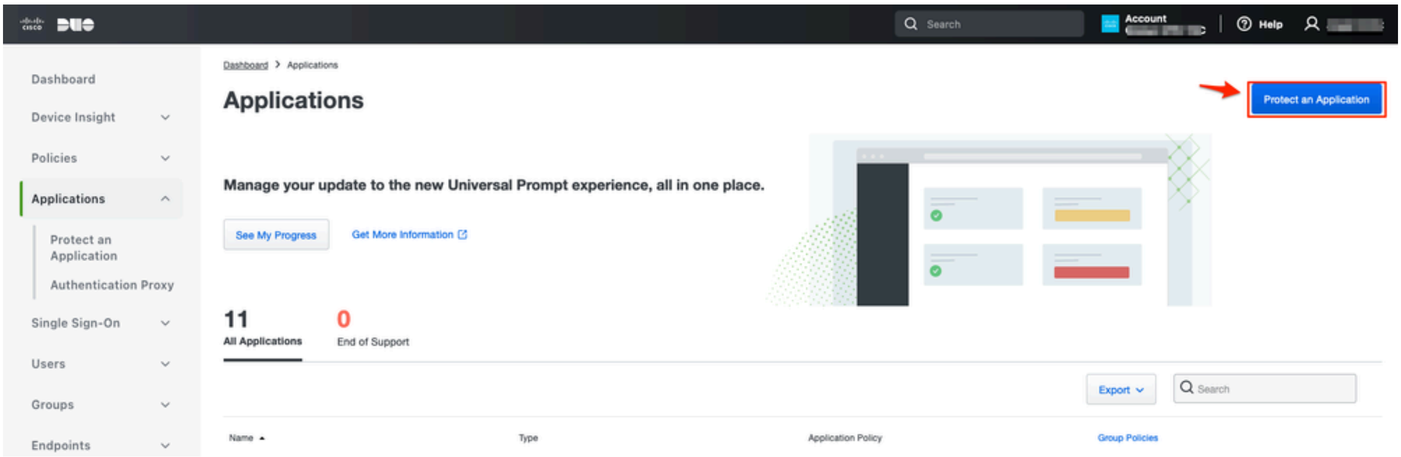
Entity ID: https://[redacted]/External_Duo/saml/sp/metadata — Copy

Assertion Consumer Service (ACS) URL: https://[redacted]External_Duo/+CSCOE+/saml/sp/acs?tgname= — Copy

Download SP Metadata
Next
3 SAML Identity Provider (IdP) Metadata
4 Re-Authentication Interval
5 Security Zones and Security Controls
Cancel
Finish

b.显示SAML SP元数据后，请转到IdP并配置新的SAML SSO应用程序。

c.登录到Duo，然后导航到Applications > Protect an an Application。



Dashboard > Applications

Applications

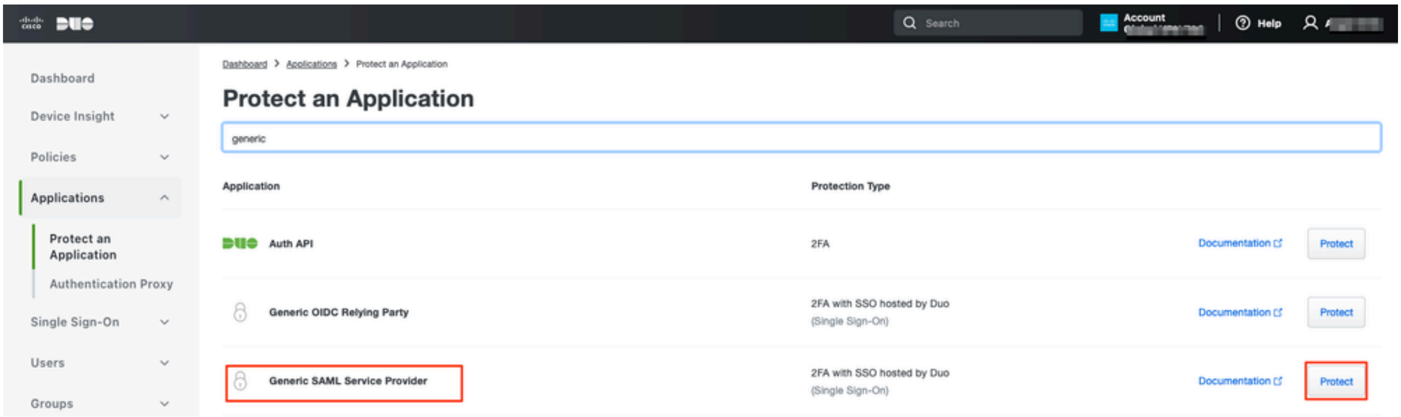
Manage your update to the new Universal Prompt experience, all in one place.

11 All Applications

0 End of Support

Name ▲	Type	Application Policy	Group Policies

d.查找通用SAML服务提供商，然后单击保护。



Dashboard > Applications > Protect an Application

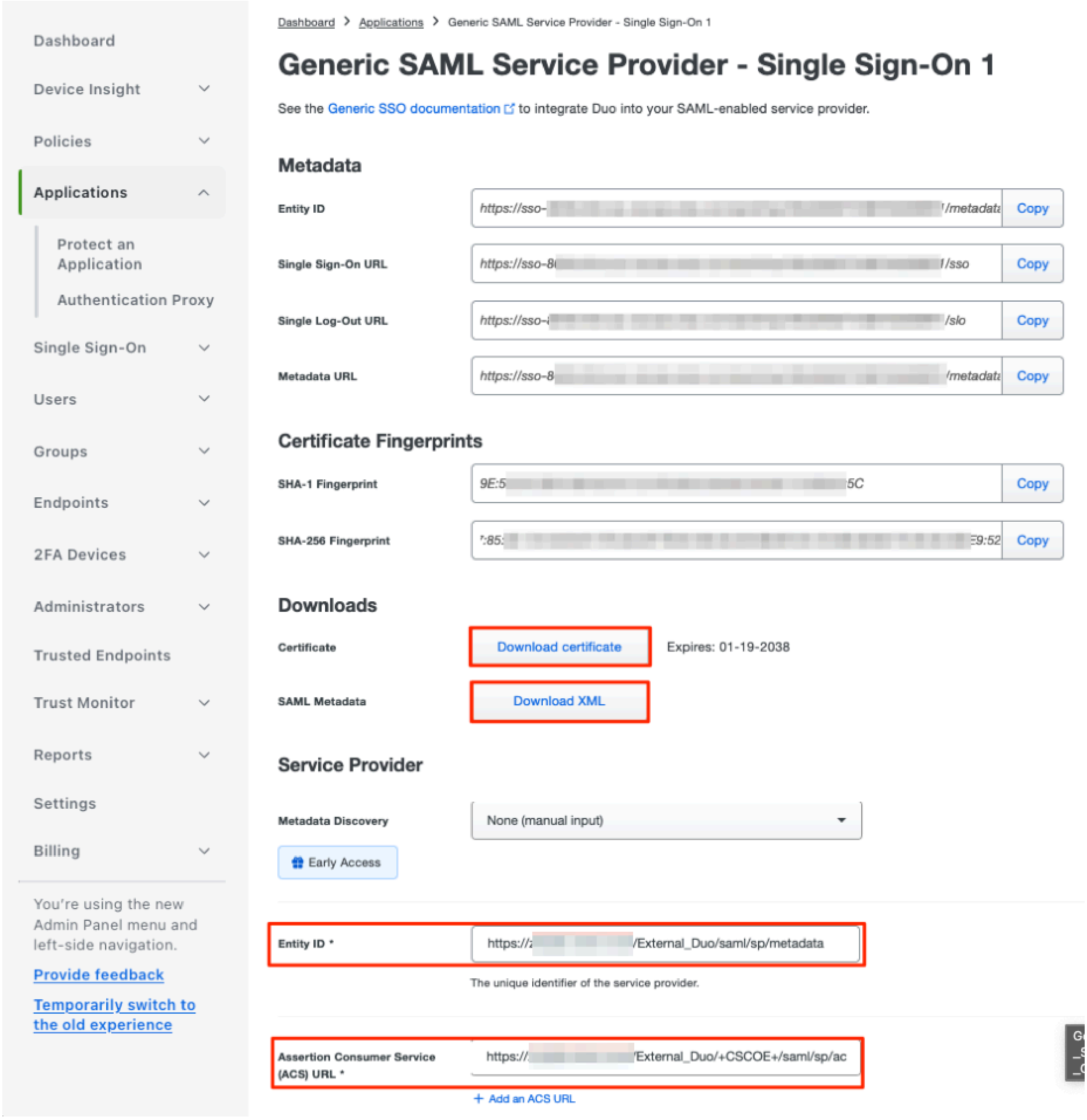
Protect an Application

generic

Application	Protection Type		
Auth API	2FA	Documentation	Protect
Generic OIDC Relying Party	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect
Generic SAML Service Provider	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect

e.从IdP下载证书和SAML元数据，因为继续安全防火墙上的配置需要该元数据。

f.从ZTNA应用组（在步骤a中生成）输入Entity ID和Assertion Consumer Service(ACS)。



Dashboard > Applications > Generic SAML Service Provider - Single Sign-On 1

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: https://sso-[redacted]/metadata Copy

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

Single Log-Out URL: https://sso-[redacted]/slo Copy

Metadata URL: https://sso-8[redacted]/metadata Copy

Certificate Fingerprints

SHA-1 Fingerprint: 9E:5[redacted]5C Copy

SHA-256 Fingerprint: :85:[redacted]E9:52 Copy

Downloads

Certificate: Download certificate Expires: 01-19-2038

SAML Metadata: Download XML

Service Provider

Metadata Discovery: None (manual input)

Early Access

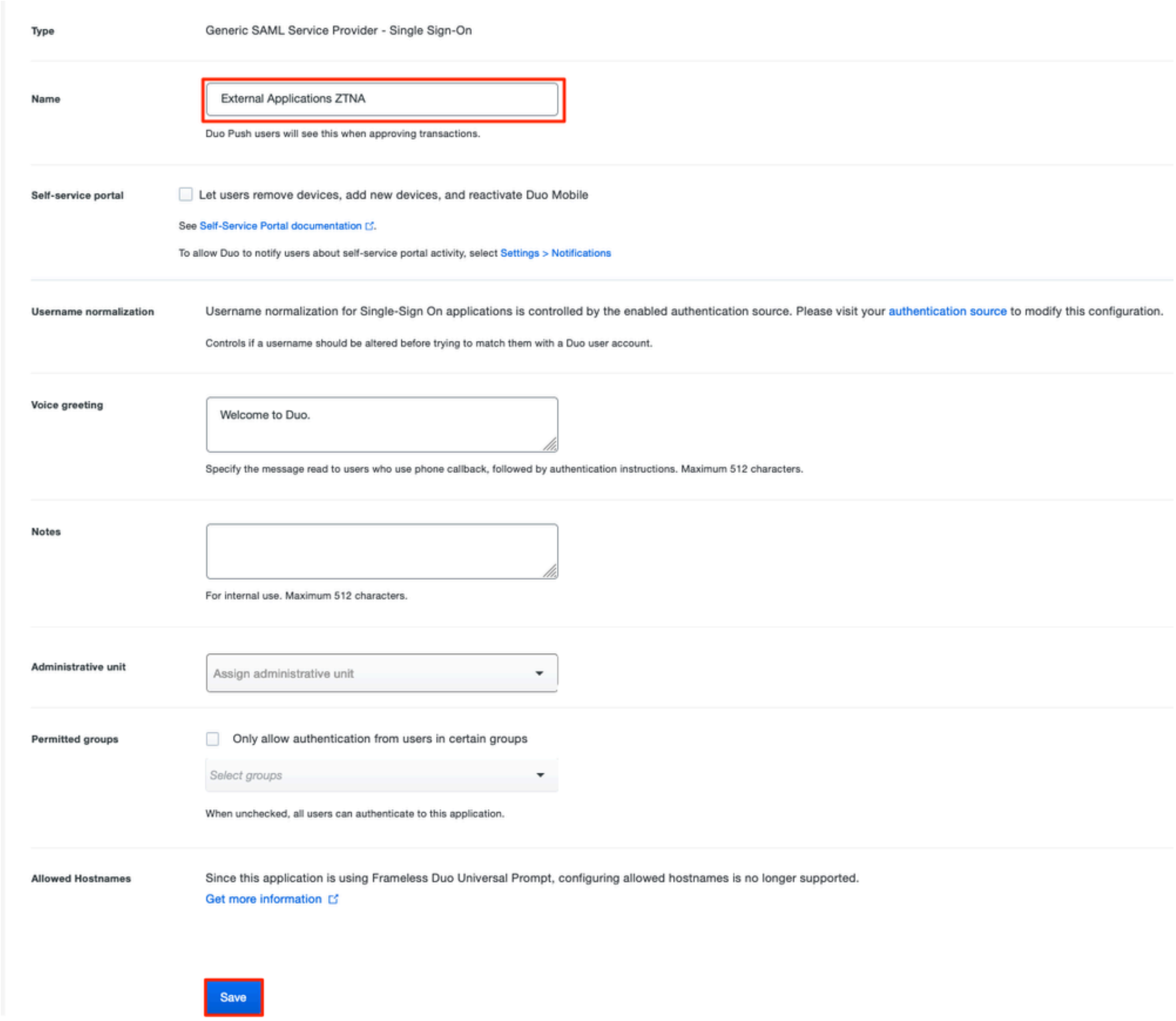
Entity ID *: https://[redacted]/External_Duo/saml/sp/metadata

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *: https://[redacted]External_Duo/+CSCOE+/saml/sp/ac

+ Add an ACS URL

g.根据您的特定要求编辑应用程序，只允许预期用户访问应用程序，然后单击Save。



Type Generic SAML Service Provider - Single Sign-On

Name External Applications ZTNA

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 Welcome to Duo.

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 Assign administrative unit

Permitted groups □ Only allow authentication from users in certain groups

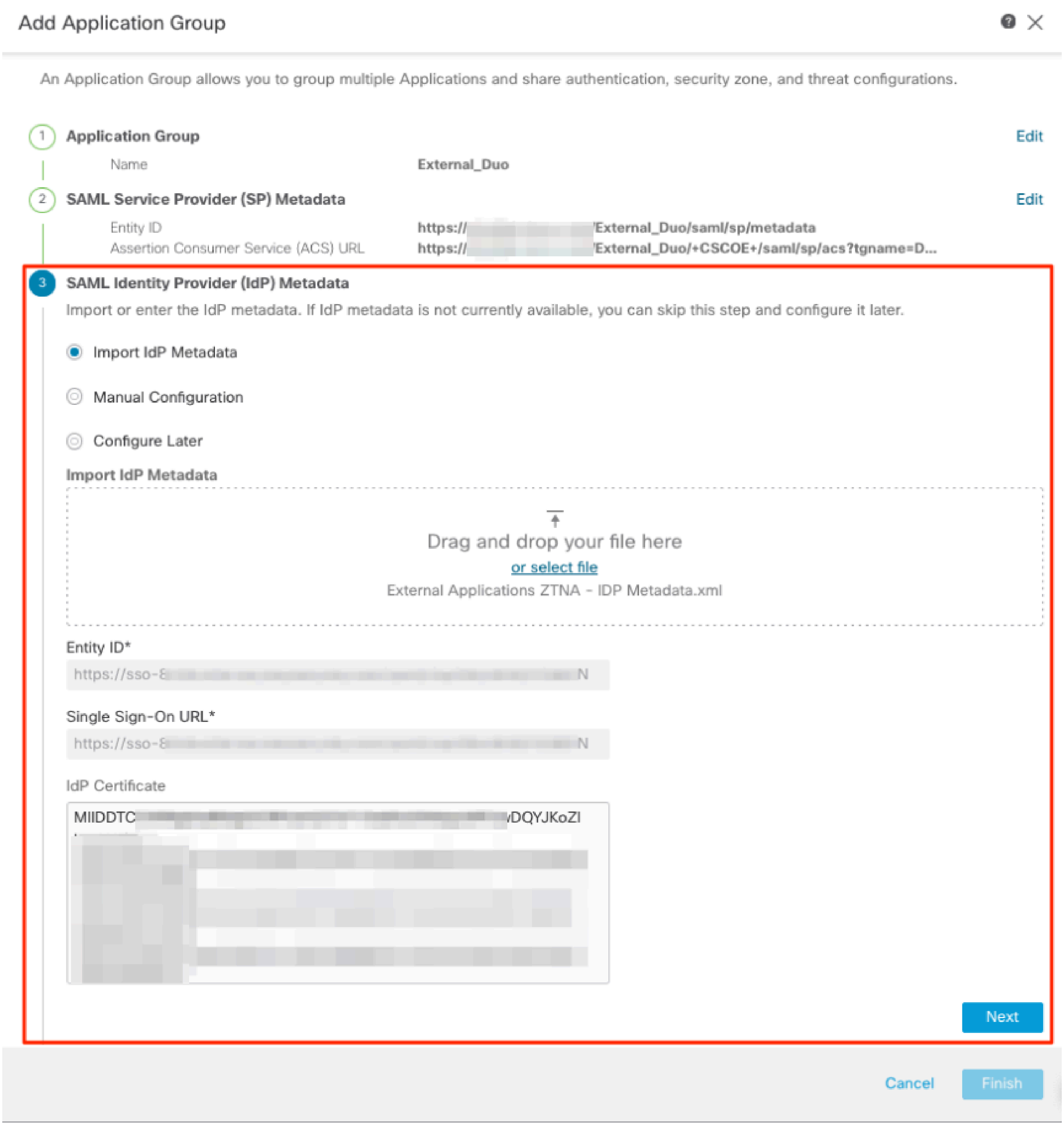
Select groups

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.使用从IdP下载的文件，导航回FMC并将SAML IdP元数据添加到应用程序组。



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

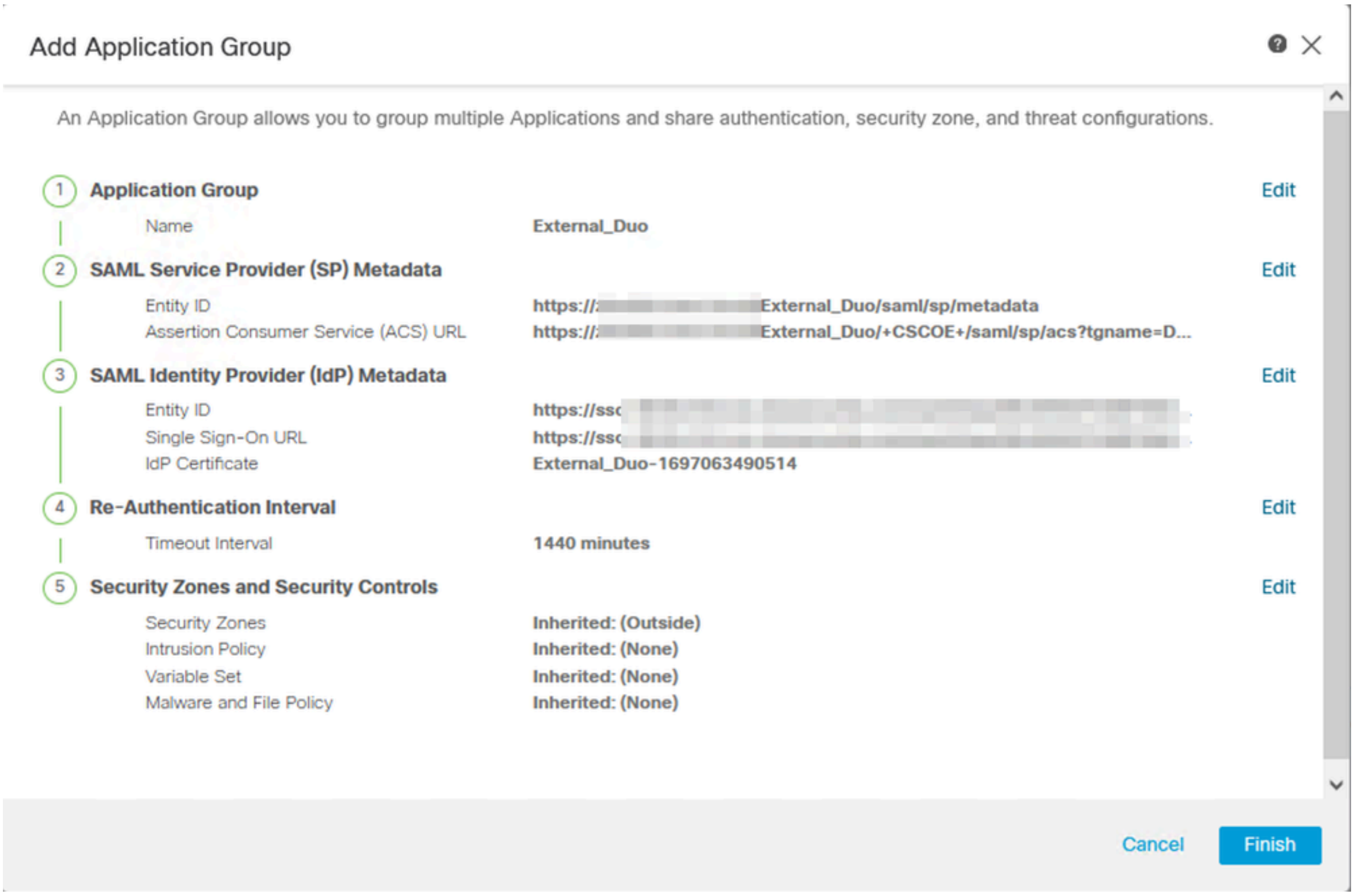
External Applications ZTNA - IDP Metadata.xml

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

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

IdP Certificate: MIIDDTC[redacted]DQYJKoZI [redacted]

i.单击Next并根据要求配置Re-Authentication Interval和Security Controls。查看摘要配置，然后单击Finish。



Add Application Group

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

1 Application Group — Edit

Name	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 — Edit

Entity ID	https://ssc[redacted]
Single Sign-On URL	https://ssc
IdP Certificate	External_Duo-1697063490514

4 Re-Authentication Interval — Edit

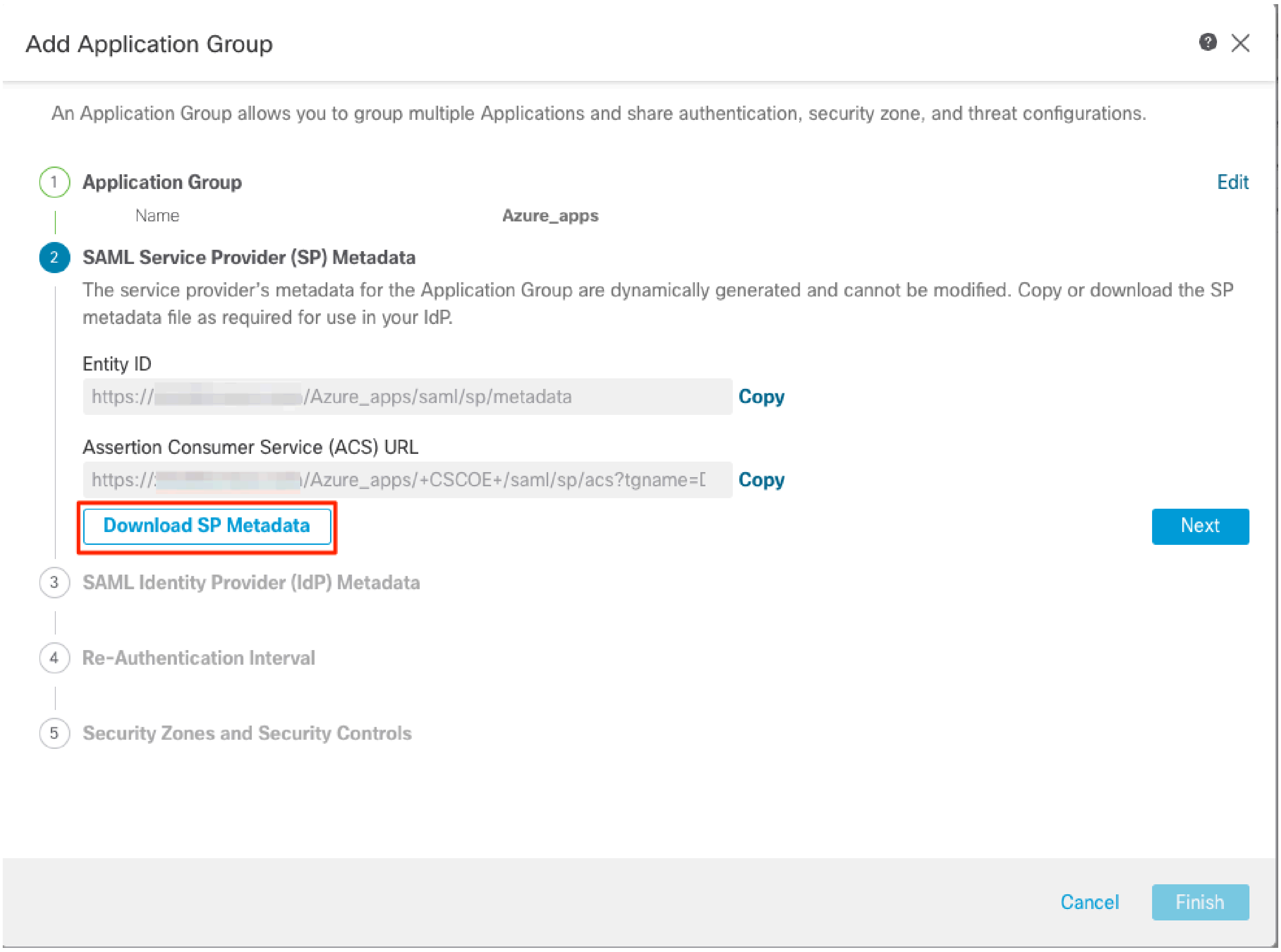
Timeout Interval	1440 minutes

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)

应用组2：使用Microsoft Entra ID(Azure AD)作为IdP

a.输入Application Group Name，然后单击Next以显示SAML Service Provider(SP)元数据。



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

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

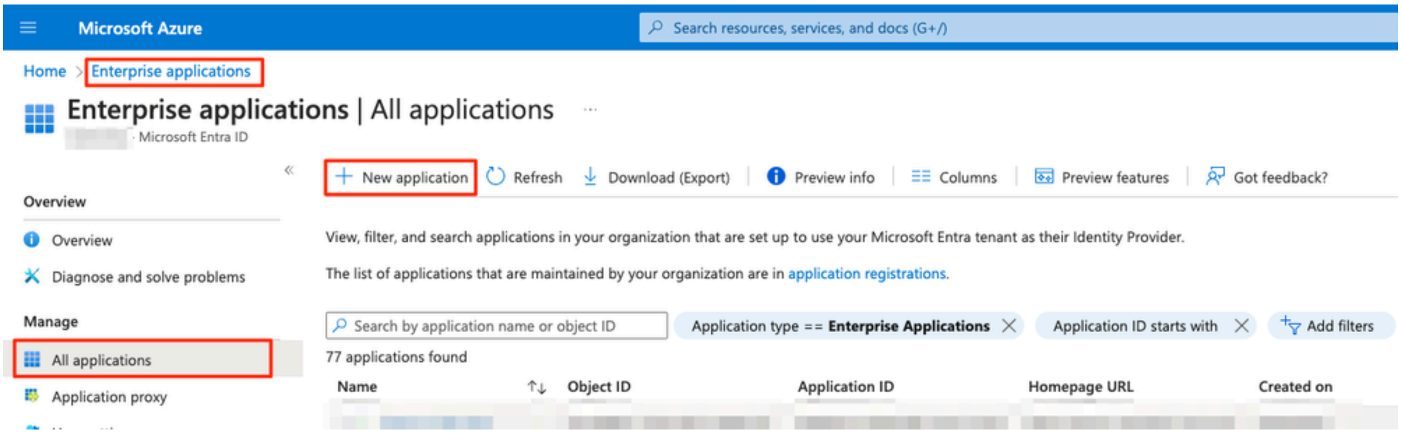
Assertion Consumer Service (ACS) URL

https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tgname=[— Copy

Download SP Metadata
Next
3 SAML Identity Provider (IdP) Metadata
4 Re-Authentication Interval
5 Security Zones and Security Controls
Cancel
Finish

b.显示SAML SP元数据后，请转到IdP并配置新的SAML SSO应用程序。

c.登录到Microsoft Azure，然后导航到企业应用程序>新建应用程序。



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications
Enterprise applications | All applications
[redacted] Microsoft Entra ID
New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

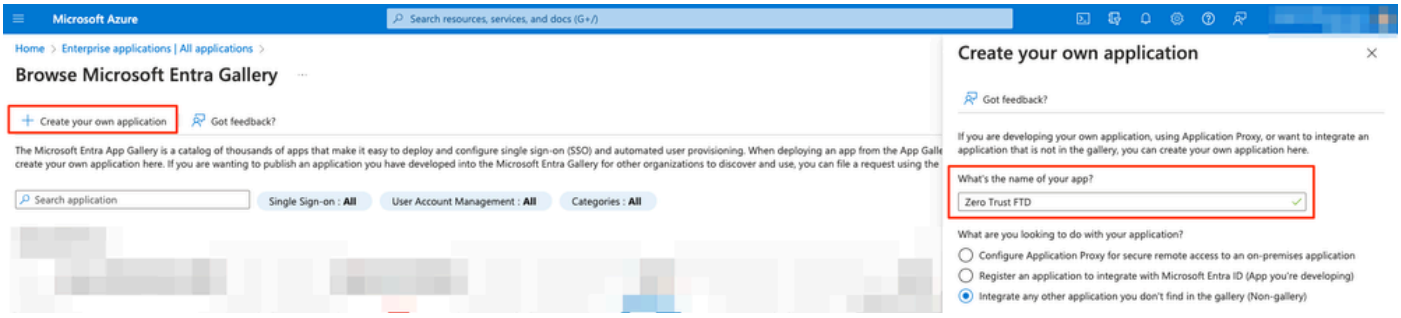
The list of applications that are maintained by your organization are in application registrations.

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

77 applications found

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

d.单击创建自己的应用程序>输入应用程序名称>创建



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery

＋ Create your own application   Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Galle create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the

Search application   Single Sign-on : **All**   User Account Management : **All**   Categories : **All**

[redacted]

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Zero Trust FTD ✓

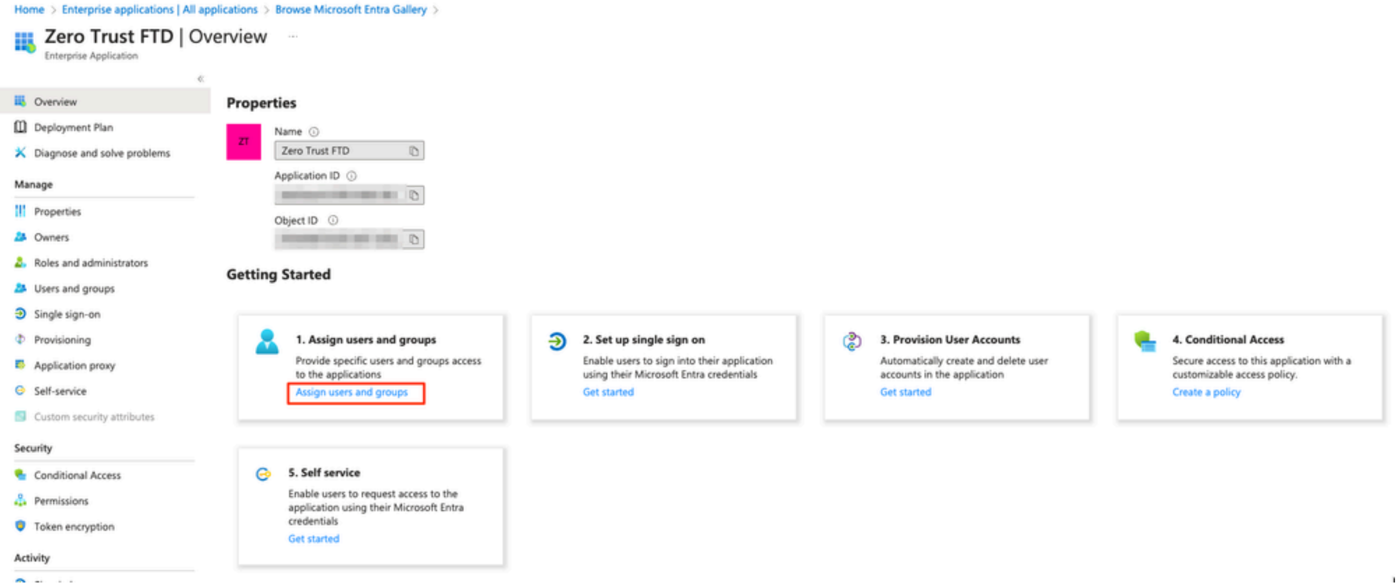
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Microsoft Entra ID (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

e.打开应用程序，然后单击分配用户和组，定义允许访问应用程序的用户和/或组。



Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery >

Zero Trust FTD | Overview

Enterprise Application

Properties

Name: Zero Trust FTD

Application ID: [redacted]

Object ID: [redacted]

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

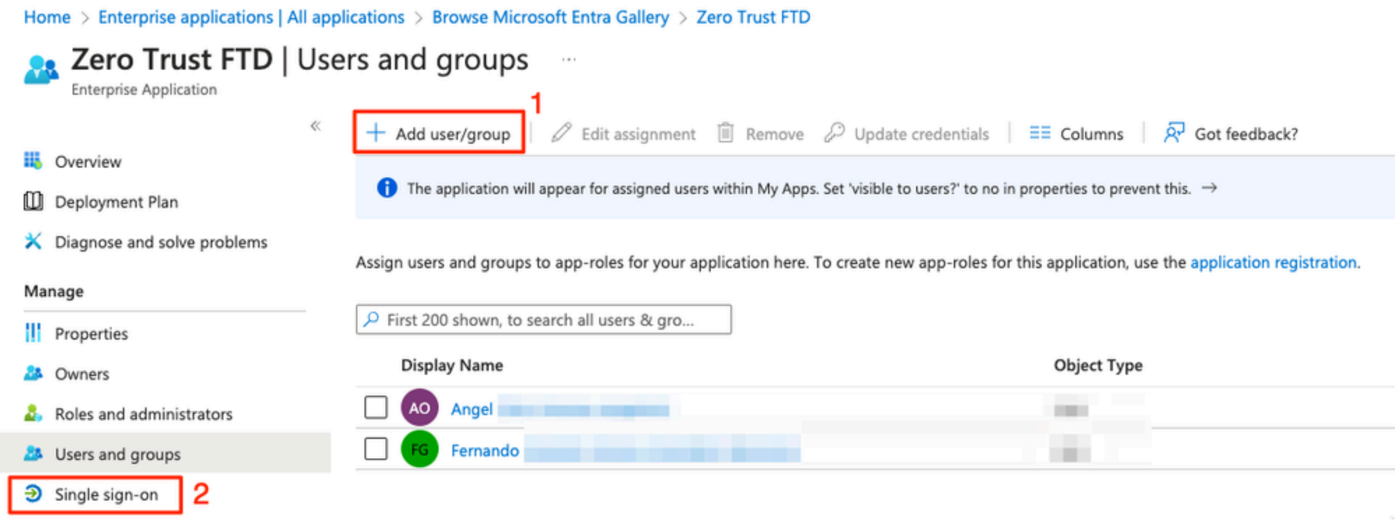
2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Microsoft Entra credentials
Get started

f.单击Add user/group > Select the necessary users/groups > Assign。分配正确的用户/组后，单击单点登录。



Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Zero Trust FTD

Zero Trust FTD | Users and groups

Enterprise Application

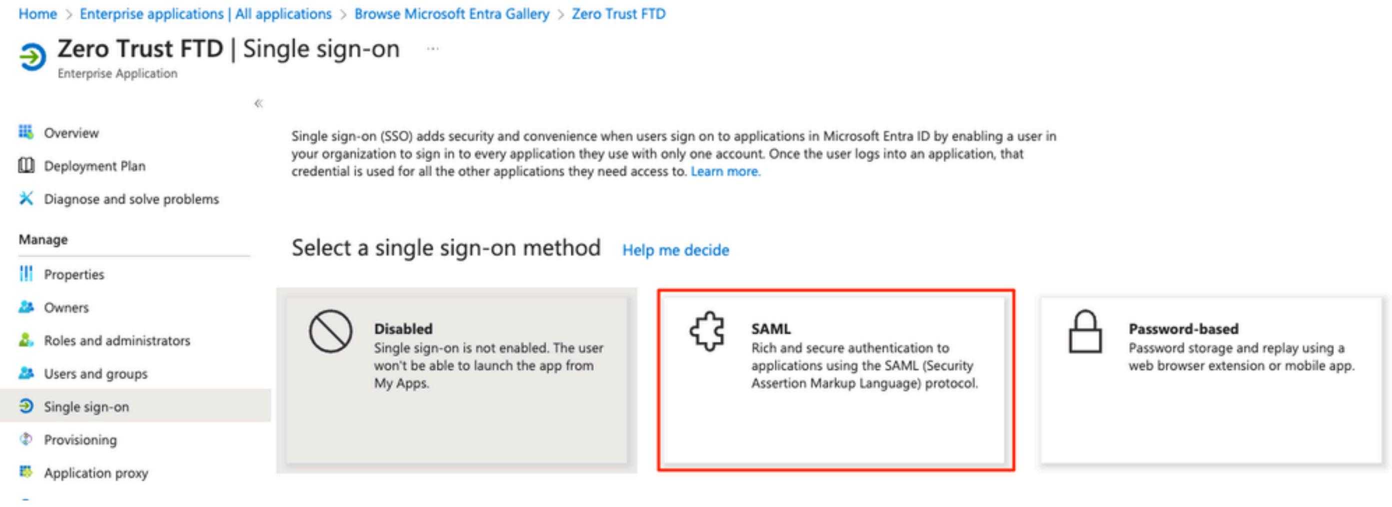
The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

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
□	AO Angel [redacted]	[redacted]
□	FG Fernando [redacted]	[redacted]

g.在单点登录部分中，单击SAML。


Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Zero Trust FTD

Zero Trust FTD | Single sign-on ...

Enterprise Application

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

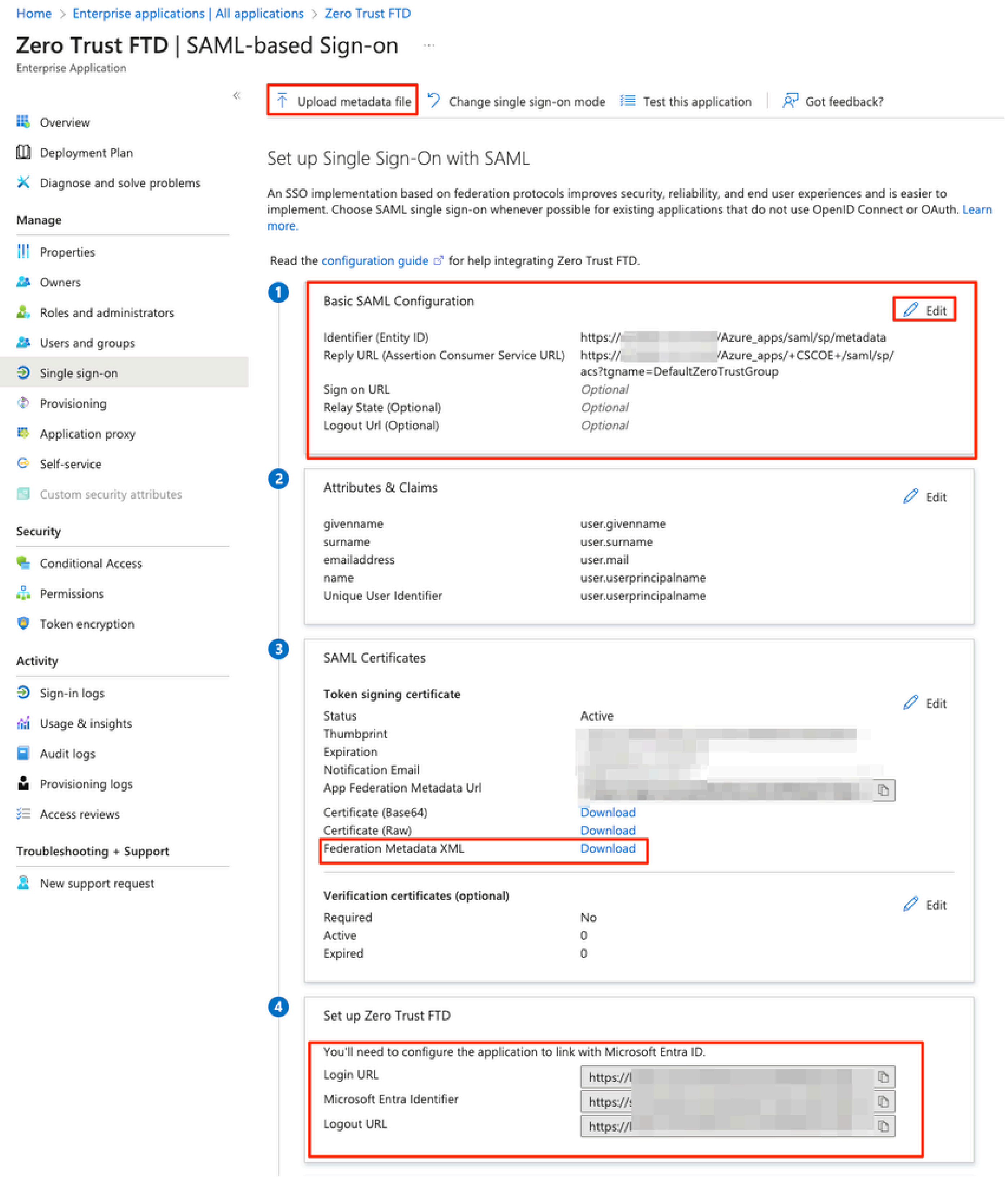
Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

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.单击Upload metadata file，然后选择从服务提供商（安全防火墙）下载的XML文件，或手动输入Entity ID和Assertion Consumer Service(ACS)URL，该地址来自ZTNA应用组(在步骤a中生成)。

注意：请确保也下载联合元数据XML或单独下载证书（以64为基数）并从IdP（登录和注销URL和Microsoft Entra标识符）复制SAML元数据，因为这些是继续安全防火墙上的配置所必需的。



Home > Enterprise applications | All applications > Zero Trust FTD

Zero Trust FTD | SAML-based Sign-on ...

Enterprise Application

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.

1 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*

2 Attributes & Claims — Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 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

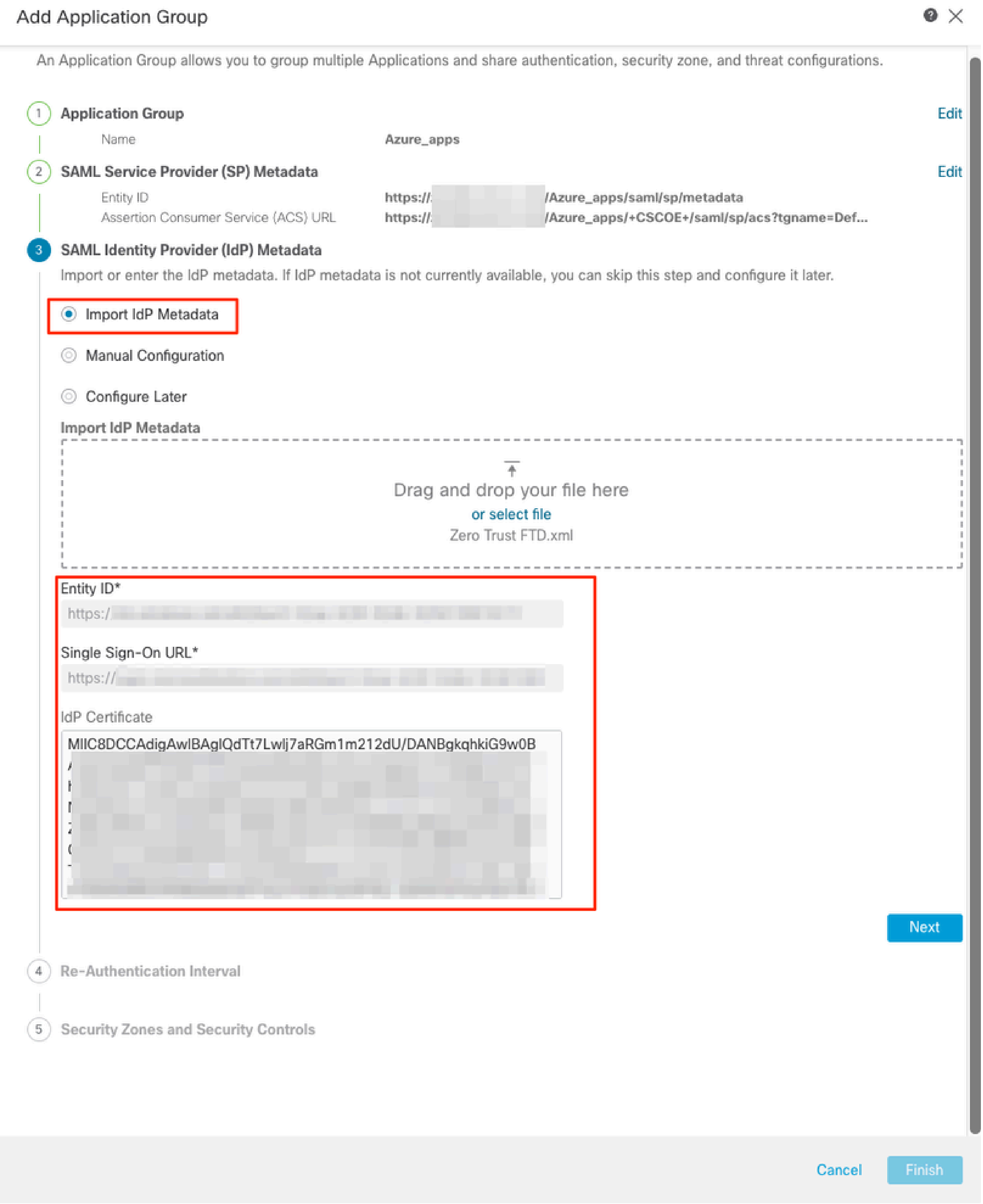
Required	No
Active	0
Expired	0

4 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.使用从IdP下载的元数据文件或手动输入所需数据，导航回FMC并将SAML IdP元数据导入到应用组2。



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

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

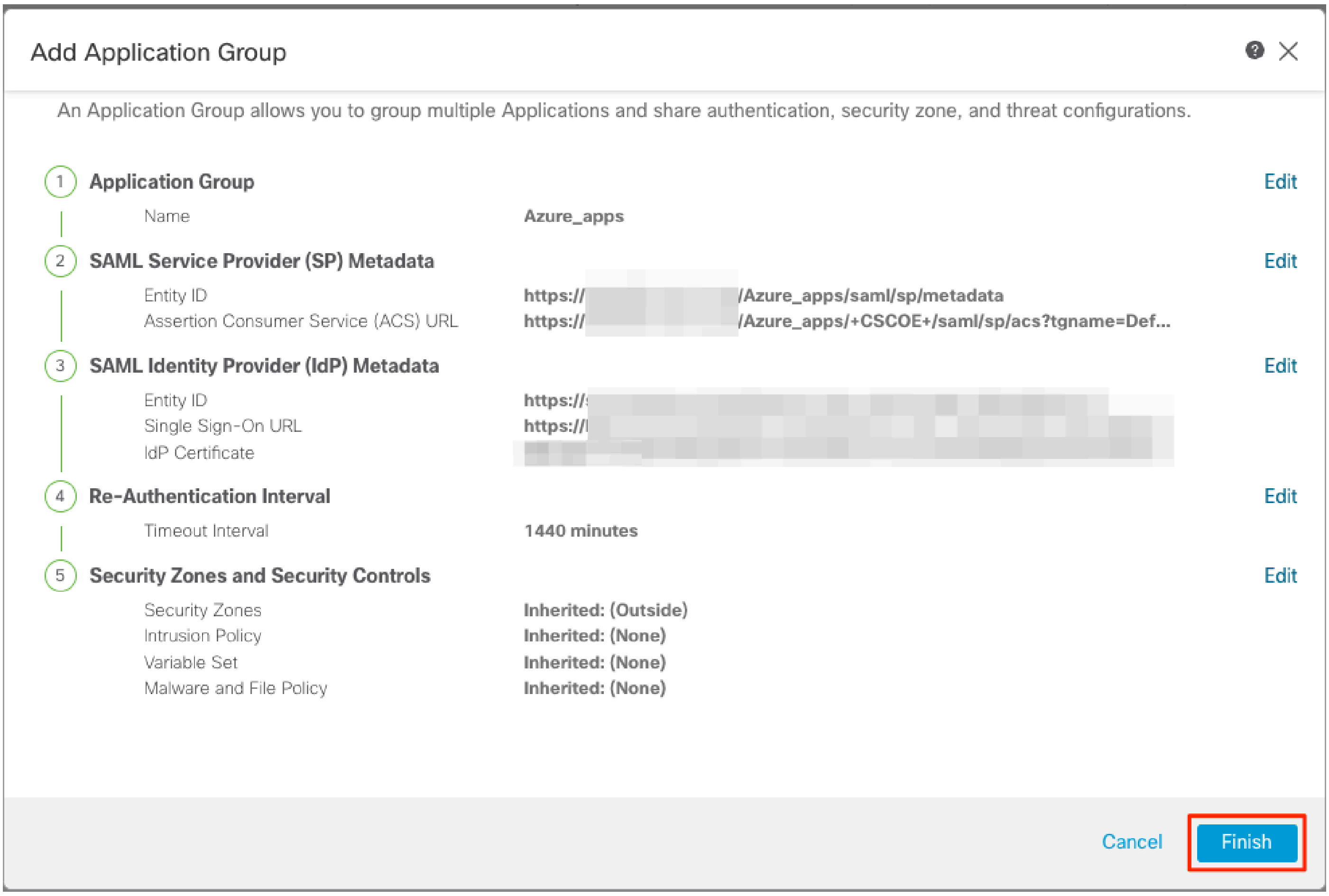
Entity ID*: https:/[redacted]

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.单击Next并根据要求配置Re-Authentication Interval和Security Controls。查看摘要配置，然后单击Finish。



Add Application Group

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

1 Application Group — Edit

Name: Azure_apps

2 SAML Service Provider (SP) Metadata — Edit

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

3 SAML Identity Provider (IdP) Metadata — Edit

Entity ID: https://[redacted]
Single Sign-On URL: https://
IdP Certificate:

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)

配置应用

创建应用程序组后，单击Add Application以定义要保护和远程访问的应用程序。

1. 输入应用设置：

a)应用程序名称：已配置应用的标识符。

b)外部URL：公共/外部DNS记录中应用的已发布URL。这是用户用于远程访问应用程序的URL。

c)应用程序URL：应用的实际FQDN或网络IP。这是Secure Firewall用于访问应用程序的URL。

注：默认情况下，外部URL用作应用URL。取消选中此复选框可指定其他应用URL。

d)应用证书：要访问的应用的证书链和私钥(从FMC主页>对象>对象管理> PKI >内部证书添加的)

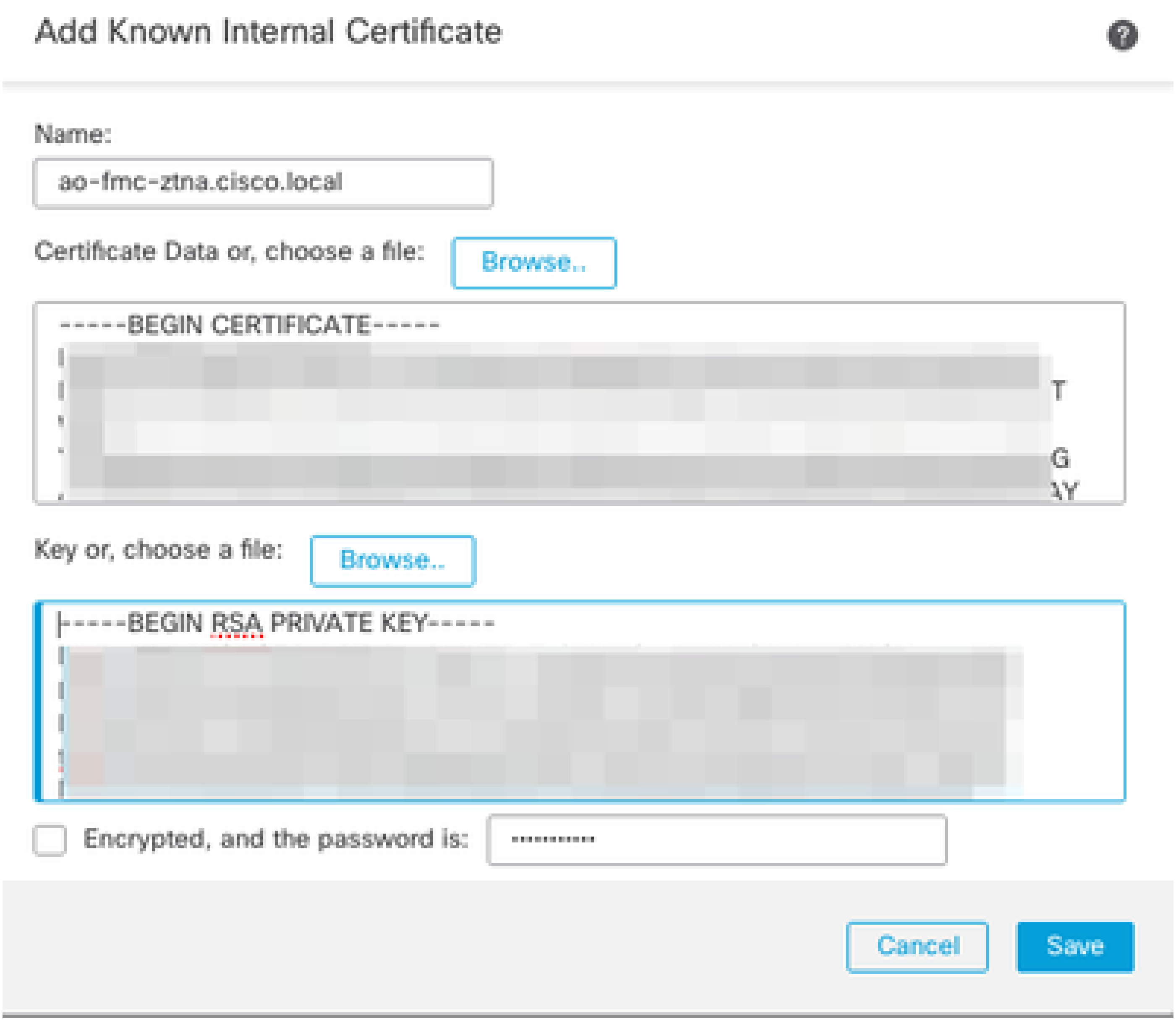
e)IPv4 NAT源(可选)：在将数据包转发到应用之前，会将远程用户的源IP地址转换为所选地址（仅支持具有IPv4地址的主机和范围类型网络对象/对象组）。可以对此进行配置，以确保应用程序

具有通过安全防火墙返回远程用户的路由

f)应用程序组（可选）：选择是否将此应用程序添加到现有应用程序组，以使用为其配置的设置。

在本示例中，要使用ZTNA访问的应用程序是测试FMC Web UI和位于安全防火墙后面的CTB的Web UI。

应用的证书必须添加到对象>对象管理> PKI >内部证书:



Add Known Internal Certificate

Name:

ao-fmc-ztna.cisco.local

Certificate Data or, choose a file: Browse..

-----BEGIN CERTIFICATE-----
[redacted]

Key or, choose a file: Browse..

-----BEGIN RSA PRIVATE KEY-----
[redacted]

□ Encrypted, and the password is: ••••••••••

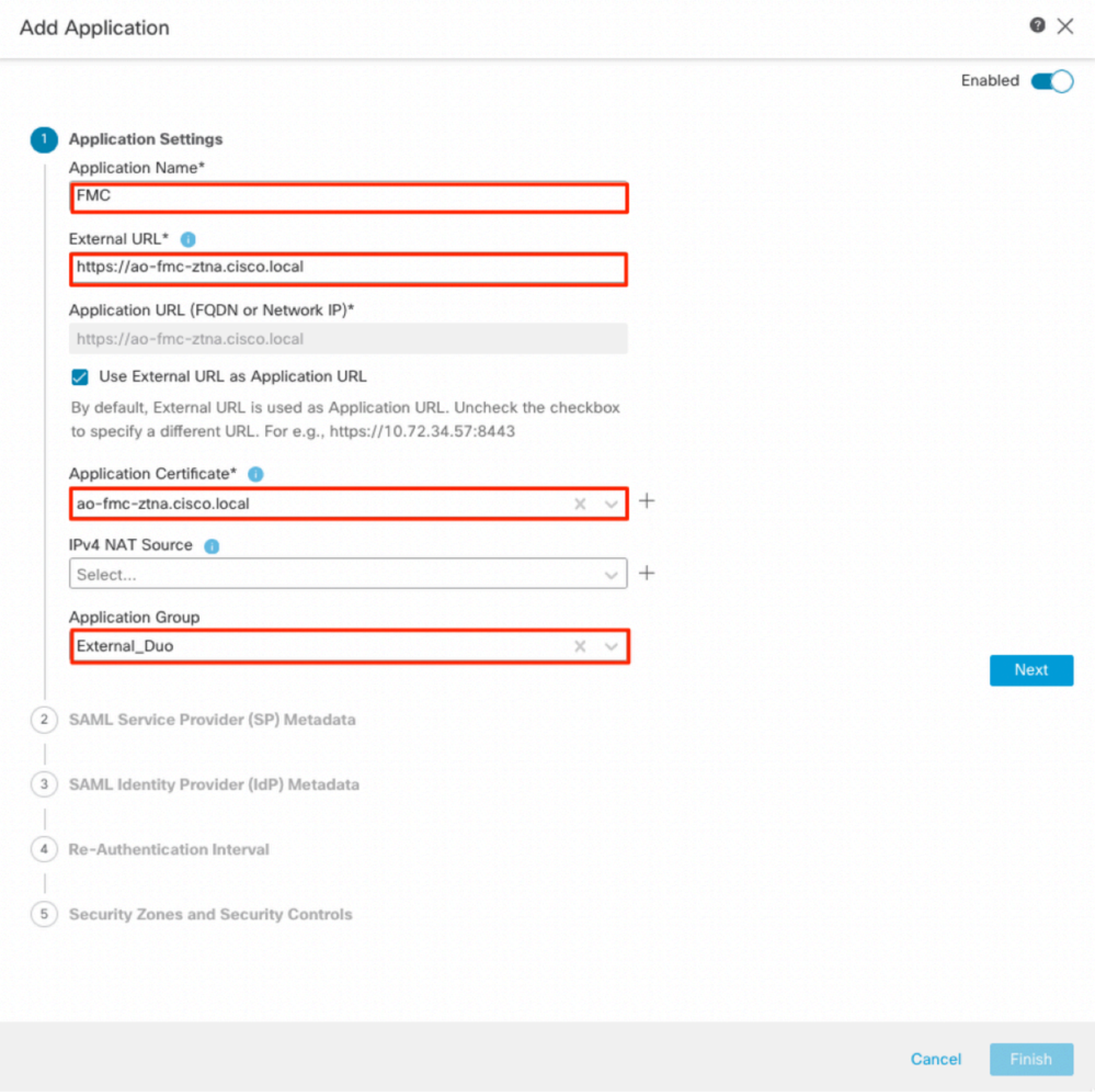
Cancel Save

注意：确保为每个要通过ZTNA访问的应用程序添加所有证书。

将证书添加为内部证书后，继续配置其余设置。

本示例中配置的应用设置如下：

应用1：测试FMC Web UI（应用组1的成员）



Add Application

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...

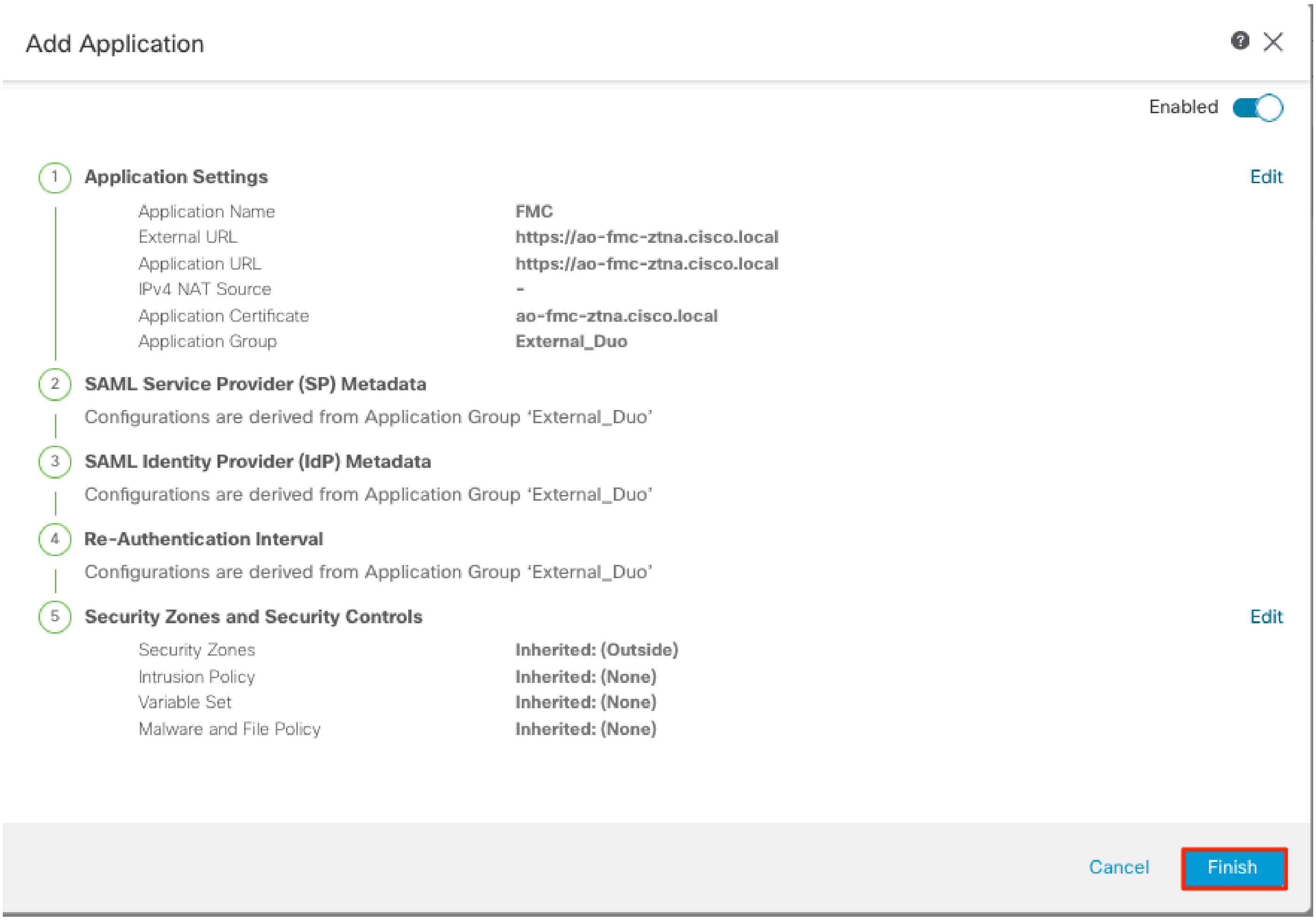
Application Group

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

应用程序添加到应用程序组1后，将继承此应用程序的其余设置。您仍然可以使用不同的设置覆盖安全区域和安全控制。

查看已配置的应用程序，然后单击Finish。



Add Application

Enabled

1 Application Settings

Edit

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’

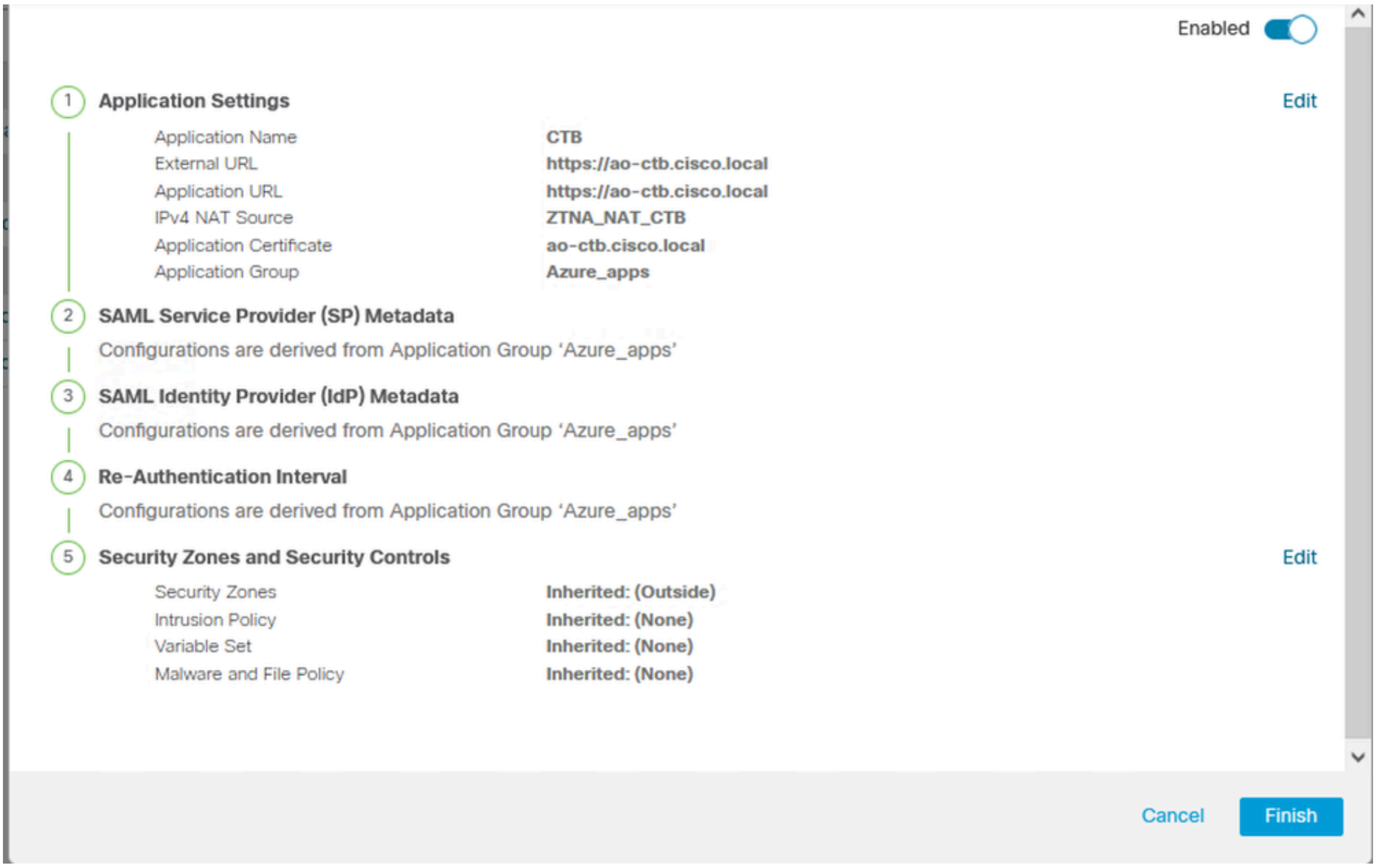
5 Security Zones and Security Controls

Edit

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

应用2:CTB Web UI（应用组2的成员）

此应用程序的配置摘要是下一个：



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**

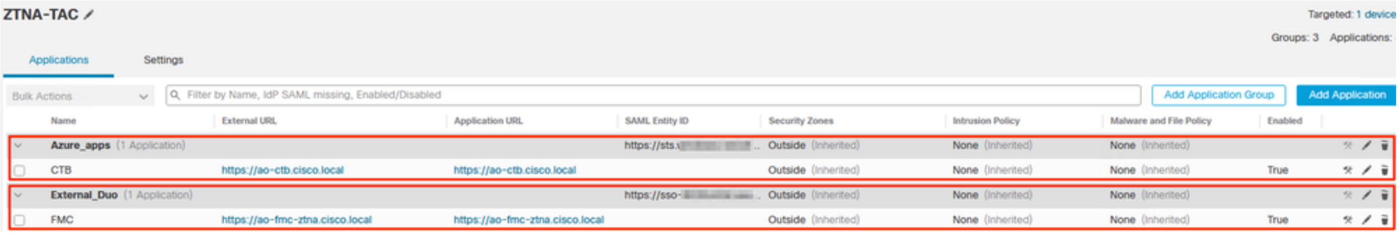
Configurations are derived from Application Group ‘Azure_apps’

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)

注意：请注意，对于此应用程序，网络对象“ZTNA_NAT_CTB”配置为IPv4 NAT源。使用此配置时，在将数据包转发到应用程序之前，会将远程用户的源IP地址转换为已配置对象中的IP地址。
配置此路由是因为应用(CTB)默认路由指向除安全防火墙之外的网关，因此返回流量未发送到远程用户。使用此NAT配置，已在应用上配置静态路由，使子网ZTNA_NAT_CTB可通过安全防火墙访问。

配置应用后，它们现在显示在相应的应用组下。



ZTNA-TAC

Targeted: 1 device

Groups: 3 Applications:

Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled
Azure_apps (1 Application)			https://sts.[redacted] ..	Outside (Inherited)	None (Inherited)	None (Inherited)	
CTB	https://ao-ctb.cisco.local	https://ao-ctb.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True
External_Duo (1 Application)			https://sso-[redacted] ..	Outside (Inherited)	None (Inherited)	None (Inherited)	
FMC	https://ao-fmc-ztna.cisco.local	https://ao-fmc-ztna.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True

最后，保存更改并部署配置。

验证

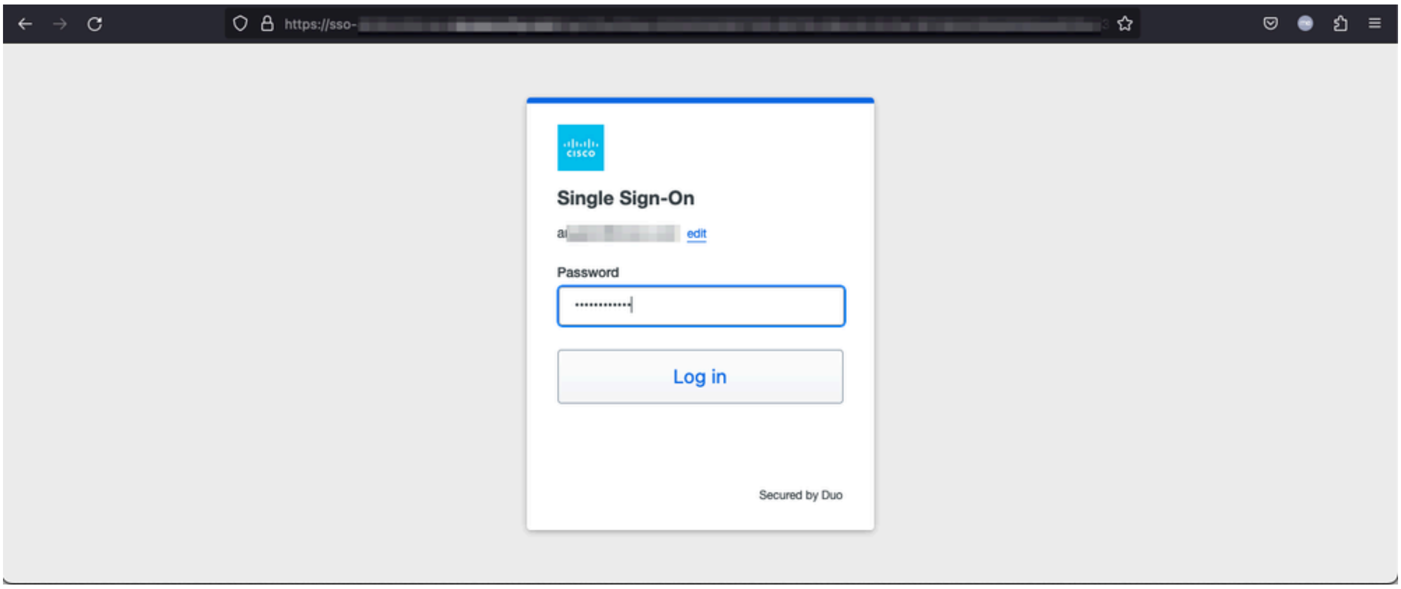
配置到位后，远程用户可以通过外部URL访问应用，并且如果相应IdP允许他们访问。

应用 1

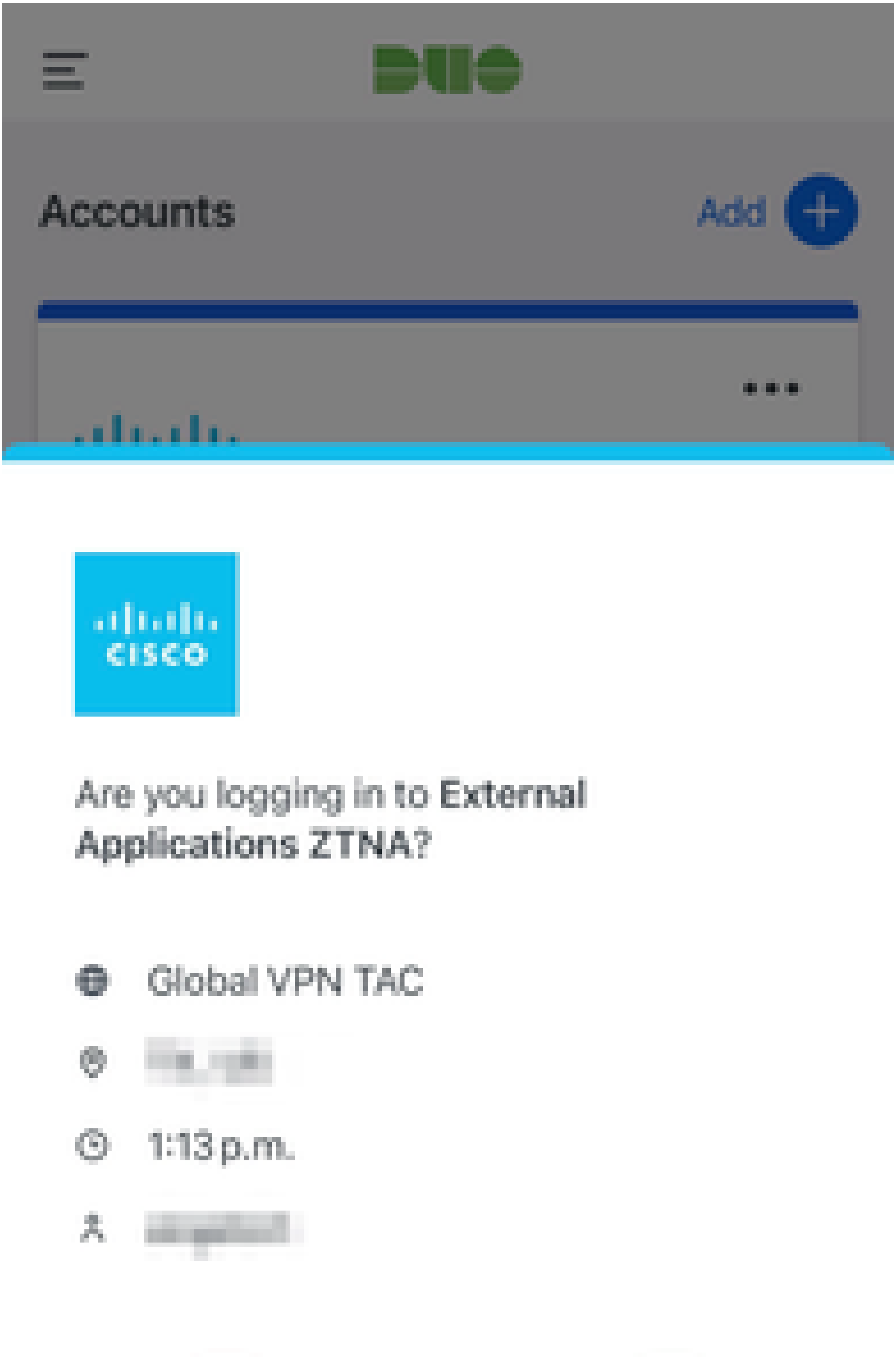
1.用户打开Web浏览器并导航至应用程序1的外部URL。在本例中，外部URL为“https://ao-fmc-ztna.cisco.local/”

> 注意：外部URL名称必须解析为已配置的安全防火墙接口的IP地址。在本示例中，它解析为外部接口IP地址(192.0.2.254)

2.由于这是新访问，因此用户被重定向到为应用程序配置的IdP登录门户。



3.向用户发送Push for MFA（这取决于IdP上配置的MFA方法）。



Are you logging in to External Applications ZTNA?

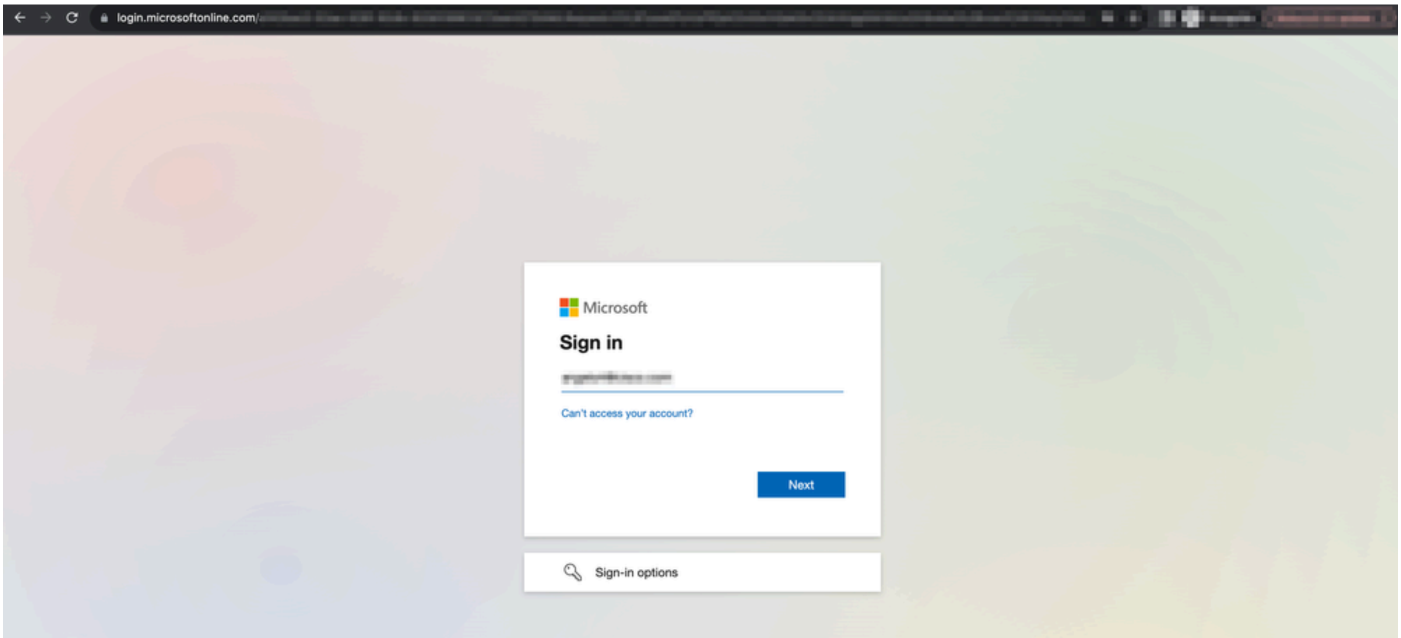
Global VPN TAC

[redacted]

1:13 p.m.

[redacted]

2.由于这是新访问，因此用户被重定向到为应用程序配置的IdP登录门户。



login.microsoftonline.com/[redacted]

Microsoft

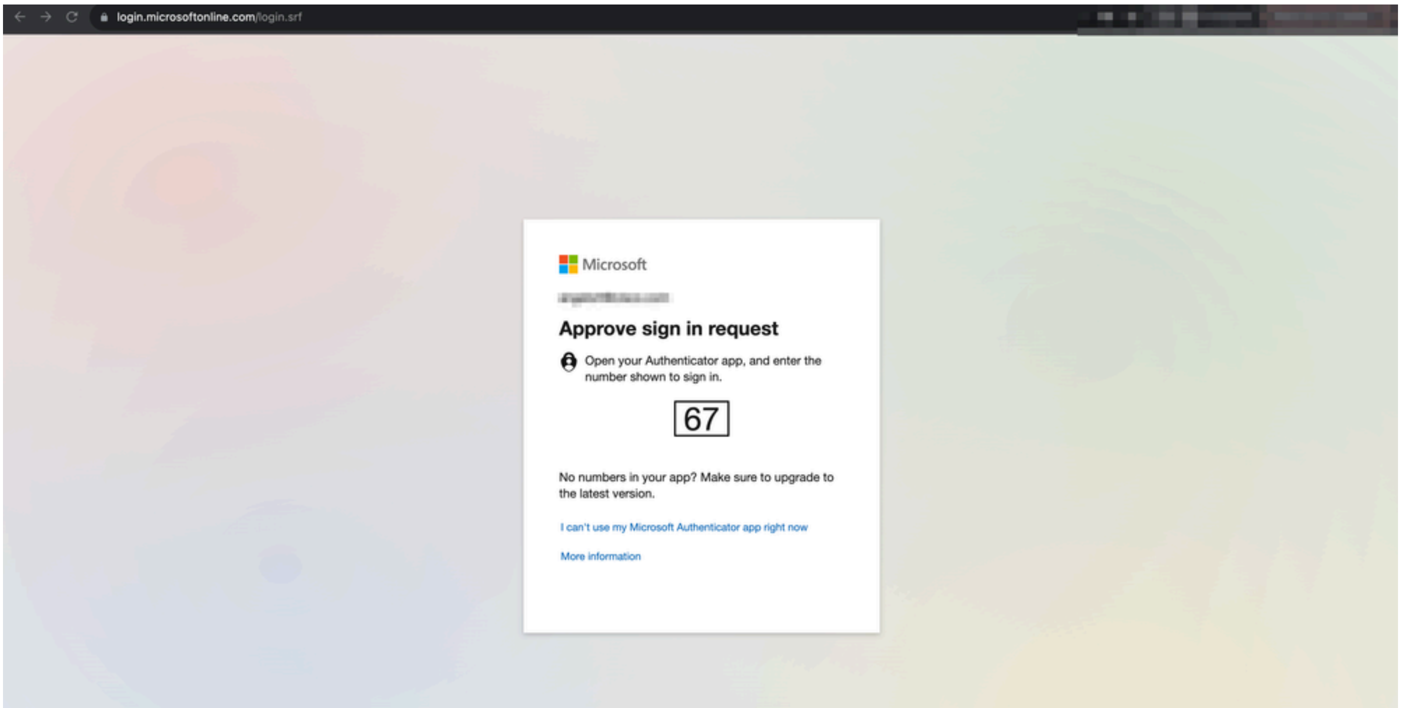
Sign in

[redacted]

Can't access your account?

Next

Sign-in options



login.microsoftonline.com/login.srf

Microsoft

[redacted]

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

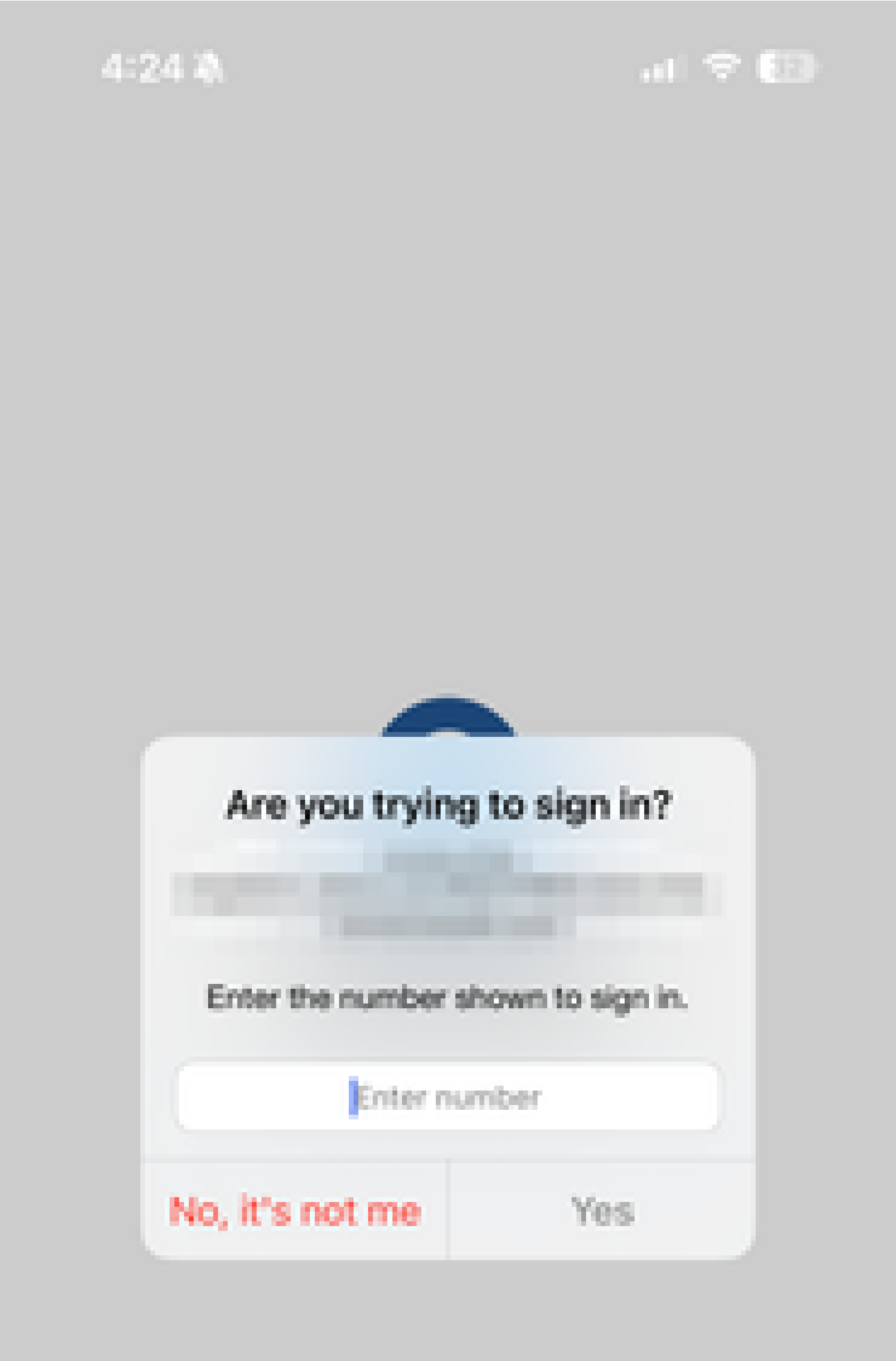
67

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

More information

3.向用户发送Push for MFA（这取决于IdP上配置的MFA方法）。



Are you trying to sign in?

[redacted]

Enter the number shown to sign in.

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。