

在安全防火墙上配置Azure Entra强制网络门户

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[图解](#)

[终端、FTD和Azure Entra之间的强制网络门户](#)

[配置](#)

[第 1 阶段：初始FMC和DNS配置](#)

[步骤 1：启用思科动态属性连接器\(CSDAC\)](#)

[步骤 2：创建代表FTD入口接口的完全限定域名网络对象](#)

[步骤 3：配置DNS A记录](#)

[第 2 阶段：公钥基础设施配置](#)

[步骤 1：将内部CA证书导入FMC](#)

[步骤 2：使用CA签署服务提供商证书](#)

[步骤 3：将SP证书部署到FTD](#)

[第 3 阶段：Azure配置](#)

[步骤 1：为SAML工具包创建Entra Enterprise应用程序](#)

[步骤 2：配置Entra ID应用注册](#)

[步骤3.为应用程序注册配置Microsoft Graph API权限。](#)

[步骤 4：配置事件中心\(EH\)命名空间](#)

[步骤 5：在事件中心名称空间中选择或创建共享访问策略](#)

[步骤 6：从EH命名空间收集并记录共享访问签名\(SAS\)信息](#)

[步骤 7：在事件中心名称空间内创建事件中心实例](#)

[步骤 8::在事件中心命名空间内创建事件中心实例使用者组](#)

[步骤 9：验证收集的值](#)

[步骤 10：配置Entra ID Audit Log Streaming到Event Hub](#)

[第 4 阶段：整合Azure和FMC/FTD主动身份验证配置](#)

[步骤 1：使用FMC向导配置Azure SAML/Entra ID领域](#)

[步骤 2：在Azure企业应用程序中实施FMC配置的SAML SP元数据](#)

[步骤 3：使用FMC向导配置Azure SAML/Entra ID领域 \(续\)](#)

[步骤 4：检查下载的用户](#)

[第 5 阶段：在FMC中配置策略](#)

[步骤 1：配置解密策略](#)

[步骤 2：配置解密策略规则](#)

[步骤 3：创建身份策略](#)

[步骤 4：配置身份策略规则](#)

[步骤 5：配置访问控制策略](#)

[步骤 6：将配置部署到思科安全防火墙设备](#)

[验证](#)

[GUI](#)

[CLI](#)

[故障排除](#)

[强制网络门户调试](#)

[用户身份转储](#)

[可能的问题](#)

[强制网络门户未知证书颁发机构](#)

[强制网络门户“找不到服务器”](#)

[相关信息](#)

简介

本文档介绍如何配置Microsoft Azure Entra ID以在Cisco安全防火墙上用于强制网络门户（主动身份验证）。

先决条件

要求

建议掌握下列主题的相关知识：

- 安全断言标记语言(SAML)
- Microsoft Azure
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

您必须在Azure for Event Hub创建中具有可用的标准定价层。此外，设备必须在启用智能许可和导出控制功能的情况下激活。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全FTD版本10.0
- 思科安全FMC版本10.0

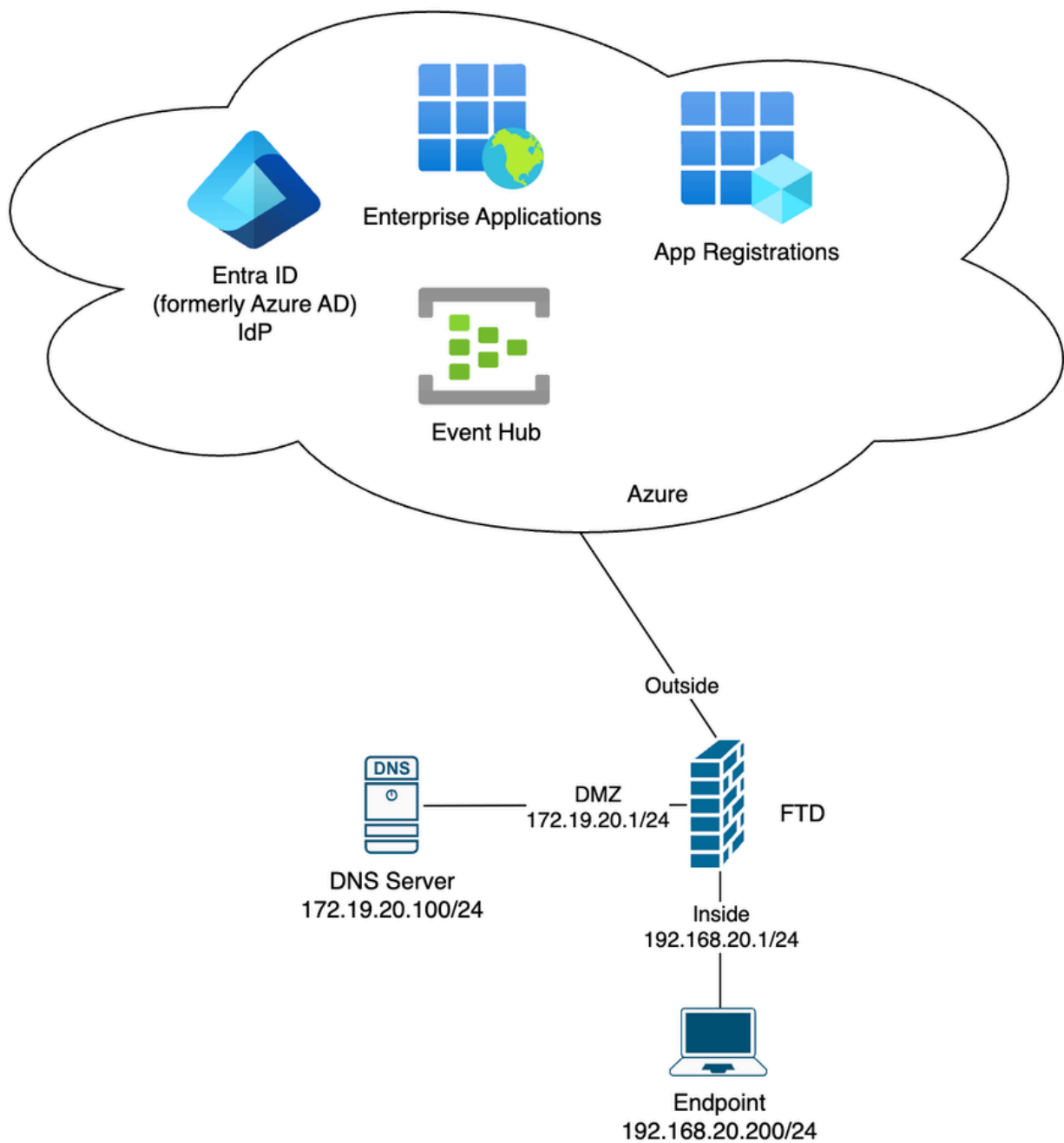
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

随着传统的基于IP的安全架构努力跟上动态混合工作环境的步伐，集成SAML的思科安全防火墙主动身份验证提供了一个以身份为中心的强大解决方案。通过将Microsoft Entra ID(Azure AD)作为集中身份提供程序，此配置使管理员能够超越静态网络规则，并根据经过验证的用户身份而不是易失性网络地址实施粒度访问控制。此集成通过无缝单点登录(SSO)和强制多重身份验证(MFA)简化用户体验，同时确保统一的安全状态，从而在无边界网络中保持严格的可视性和策略实施。

图解

终端、FTD和Azure Entra之间的强制网络门户



终端和Azure Entra之间的强制网络门户

配置

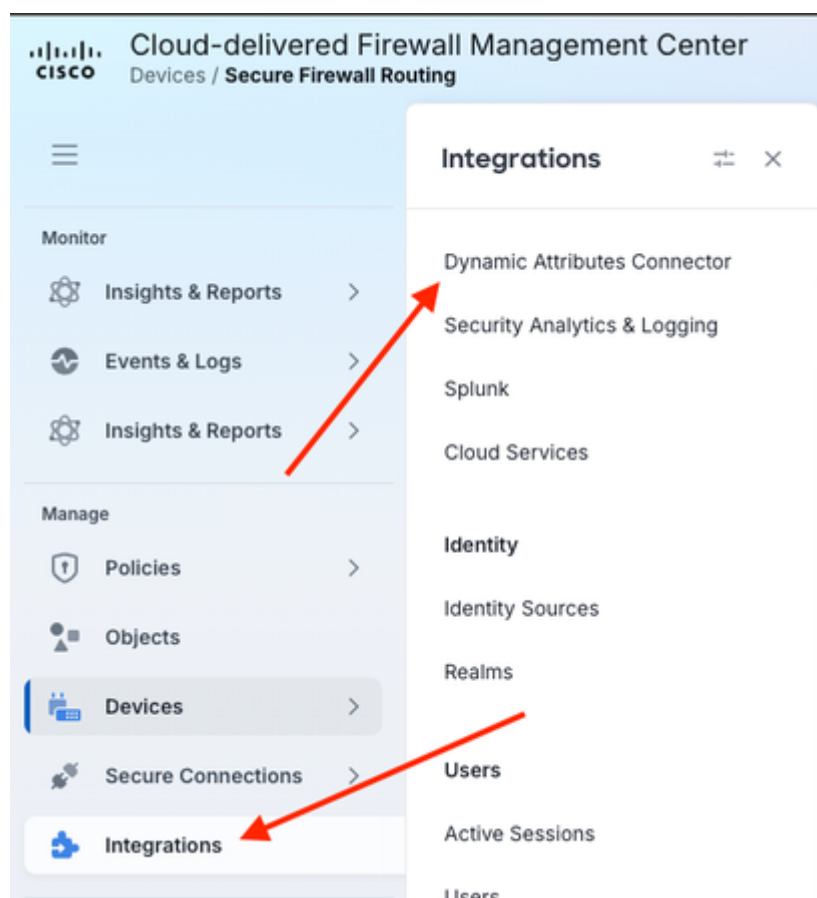
第 1 阶段：初始FMC和DNS配置



注意：本实验使用云交付的防火墙管理中心(cdFMC);但是，内部FMC的步骤保持不变。

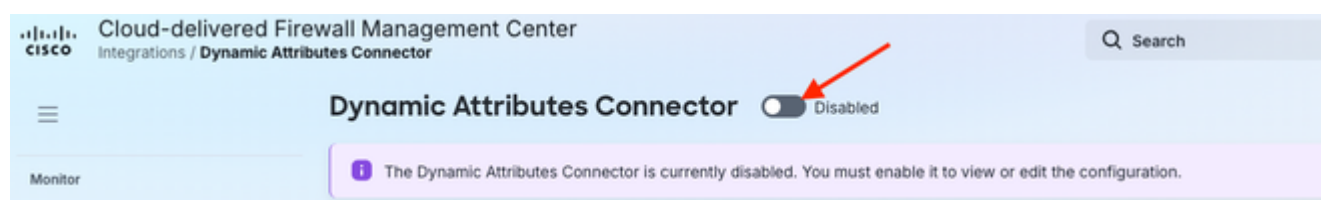
步骤 1：启用思科动态属性连接器(CSDAC)

1)选择Integrations > Dynamic Attributes Connector。



选择集成动态属性连接器

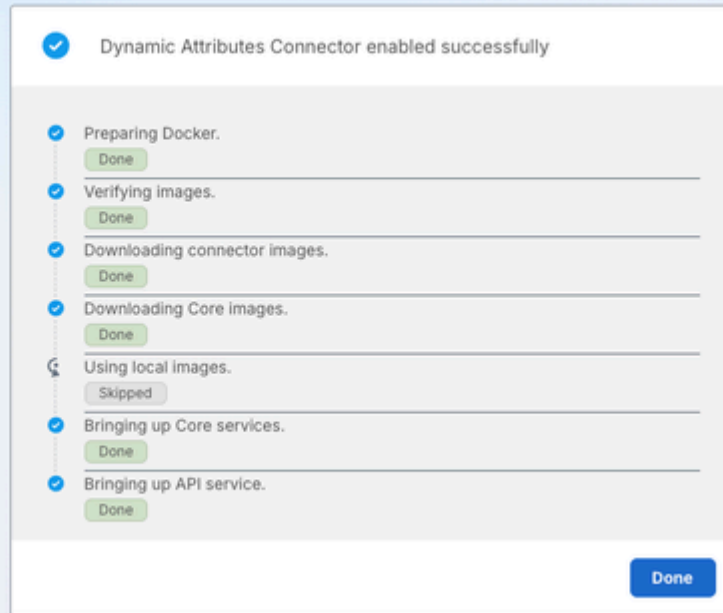
2)点击Disabled字符串旁的控件以启用CSDAC。



启用Cisco动态属性连接器

c)CSDAC启用完成后，单击Done。

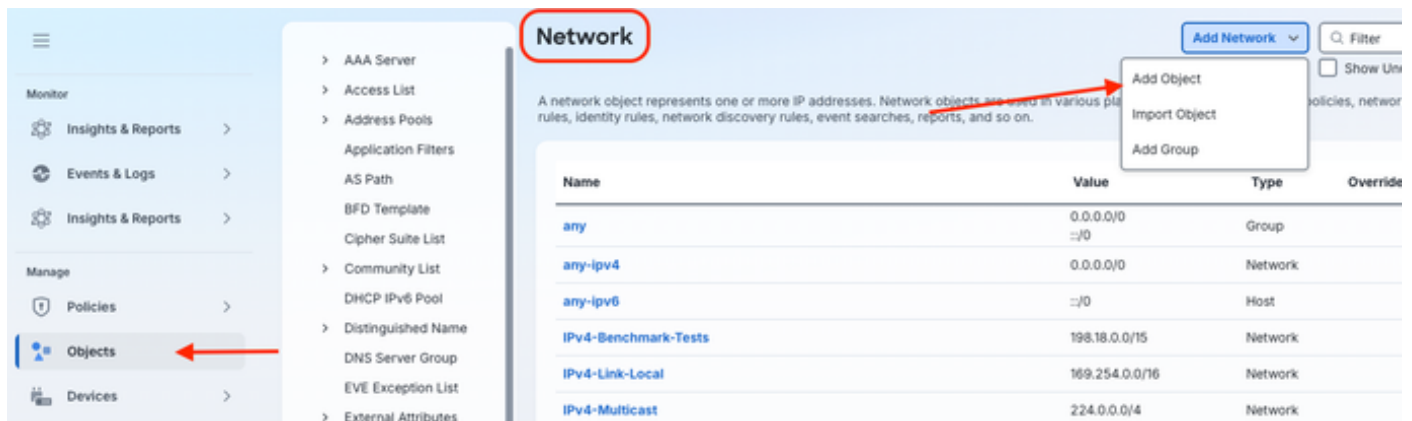
Dynamic Attributes Connector



启用思科动态属性连接器状态

步骤 2：创建代表FTD入口接口的完全限定域名网络对象

1)选择Objects > Add Network > Add Object.



创建新的完全限定域名网络对象

2)使用完全限定域名(FQDN)命名配置的网络对象。 输入FQDN，并通过点击适当的单选按钮将网络对象指定为FQDN类型。 Click Save.

Edit Network Object ?

Name

Description

Network
☐ Host ☐ Range ☐ Network ☒ FQDN

Note:
You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

Lookup:

☐ Allow Overrides

Cancel Save

配置FQDN网络对象变量

步骤 3：配置DNS A记录

1)此处显示的示例使用Windows Server 2025;根据需要查看特定名称解析服务器的文档。

	Name	Type	Data
DC	(same as parent folder)	Start of Authority (SOA)	[1], dc., hostmaster.
Forward Lookup Zones	(same as parent folder)	Name Server (NS)	dc.
example.com	ftd-inside	Host (A)	192.168.20.1
Reverse Lookup Zones			
Trust Points			

Windows Server DNS A记录配置



注意：执行主动身份验证的客户端必须能够解析此DNS A记录。

第 2 阶段：公钥基础设施配置

内部证书颁发机构(CA)可用作主动身份验证配置的公钥基础设施(PKI)。Cisco FMC和FTD要求将内部CA公钥和配对的私钥作为内部CA对象上载，以执行必要的SSL侦听和Decrypt-Resign操作。此外，内部CA必须在执行活动身份验证的客户端浏览器中受信任。请参阅客户端浏览器文档，检查如何确认浏览器信任证书。

步骤 1：将内部CA证书导入FMC

1)选择Objects > PKI > Internal CAs。单击Import CA。



注意：内部CA也可以直接在FMC上创建。

Import Internal Certificate Authority ⓘ

Name:

Certificate Data or, choose a file:

-----BEGIN CERTIFICATE-----
-----END PRIVATE KEY-----

Key or, choose a file:

-----BEGIN CERTIFICATE-----
-----END PRIVATE KEY-----

☒ Encrypted, and the password is:

将内部证书颁发机构导入防火墙管理中心



注意：在本文档的内容中，出现空白区域，涵盖图像中的各个字段值，这是本文档发布时

有意造成的。实际值会在您配置时反映您的环境。

步骤 2：使用CA签署服务提供商证书

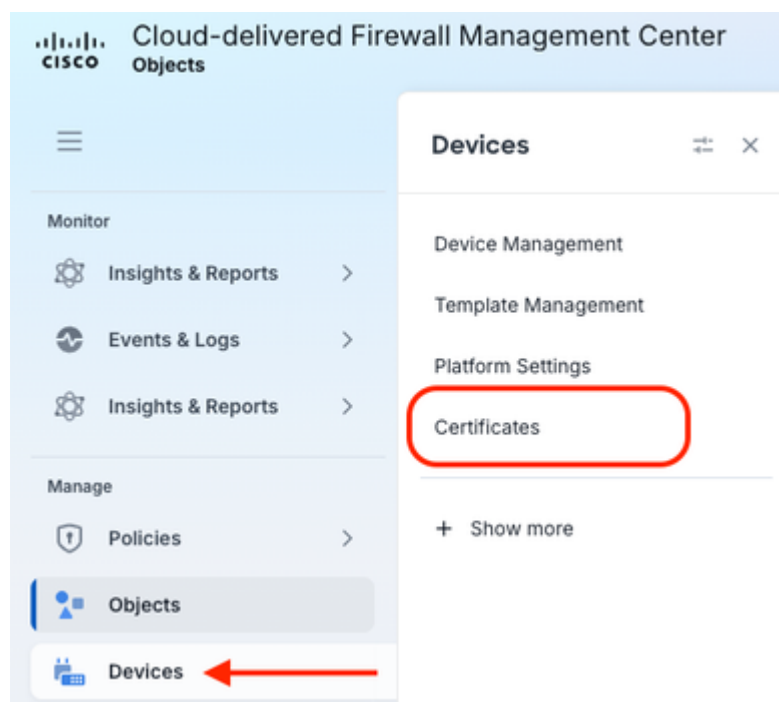
1)服务提供商(SP)证书必须由受信任的证书颁发机构(CA)签名并以PKCS#12(.p12)格式返回。



注意：此CA可以在内部签名。唯一的警告是内部CA必须受客户端设备的信任。

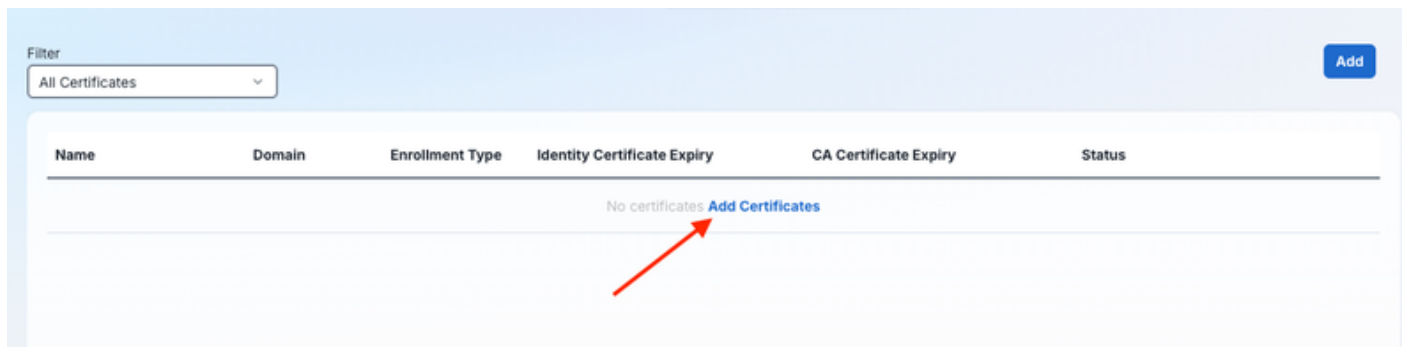
步骤 3：将SP证书部署到FTD

1)选择Devices > Certificates。



导航到Devices And Certificates

2)单击Add Certificates。



添加新设备证书

3)从执行Active Authentication的下拉列表中点击设备，然后点击+图标以创建新的Certificate Enrollment。

A screenshot of a dialog box titled 'Add New Certificate'. It contains a description: 'Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.' There are two dropdown menus: 'Device*' with 'FTD' selected, and 'Certificate Enrollment*'. A red arrow points to the 'FTD' selection in the 'Device*' dropdown. Another red arrow points to a '+' icon located to the right of the 'Certificate Enrollment*' dropdown. At the bottom right of the dialog are 'Cancel' and 'Add' buttons.

选择FTD并添加添加新证书注册(Add New Certificate Enrollment)

4)将证书注册命名为，并从注册类型下拉列表中选择PKCS12文件。

Add Certificate Enrollment

Name*

FTD-SP-Cert

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

SCEP

Enrollment URL:*

EST

Challenge Password:

SCEP

Confirm Password:

ACME

Retry Period:

Manual

Retry Count:

10

(Range 0-100)

Fingerprint:

Ex: e6f7d542 e355586c a758e7...

Validation Usage:

☒ IPsec Client

☒ SSL Client

☐ SSL Server

Cancel

Save

证书注册设置和类型

5)单击Browse PKCS12 File导入PKCS#12文件，然后输入所需的口令。Click Save.

Add Certificate Enrollment

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: SP.p12 [Browse PKCS12 File](#)

Passphrase*:

Validation Usage: ☒ IPsec Client ☒ SSL Client ☐ SSL Server

☐ Skip Check for CA flag in basic constraints of the CA Certificate

☒ Allow Overrides

> Override (0)

Cancel Save

浏览和导入PKCS12文件

6)确认注册详细信息是否正确，然后点击添加。

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD

Certificate Enrollment*: FTD-SP-Cert +

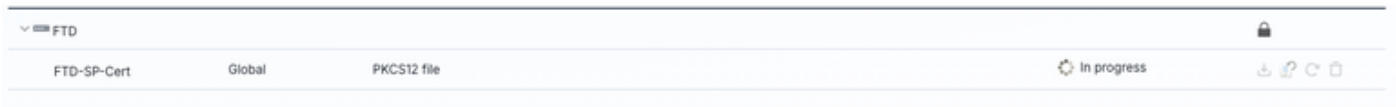
Certificate Enrollment Details:

Name:	FTD-SP-Cert
Enrollment Type:	PKCS12 file
Enrollment URL:	N/A

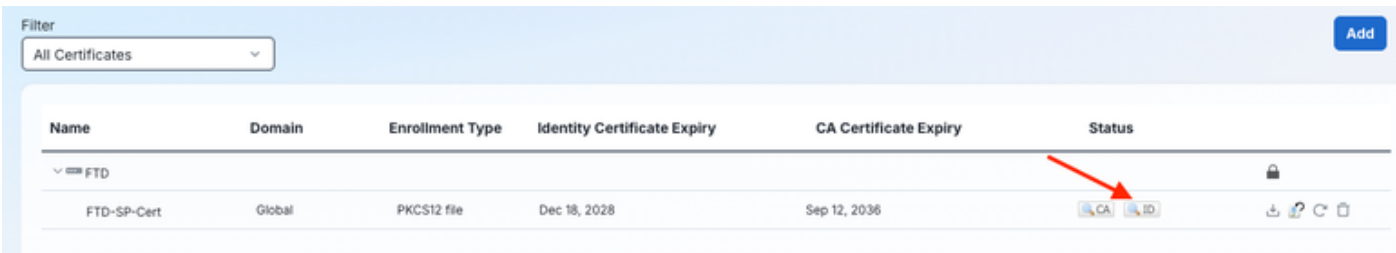
Cancel Add

确认证书注册详细信息

7)导入反映进行中。



导入完成后，可以通过点击已配置证书的ID图标来验证SP证书信息。

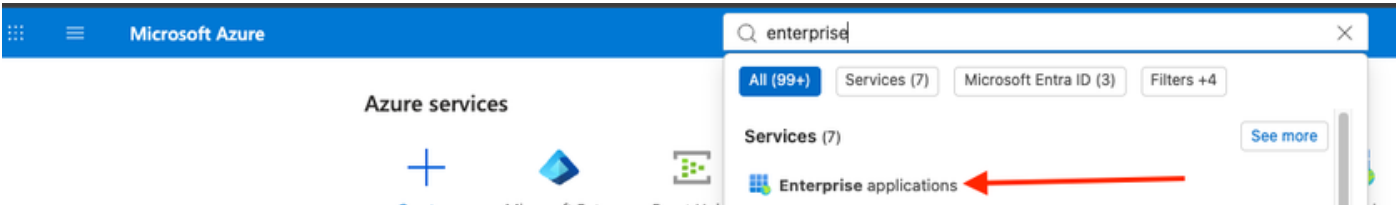


证书导入进行中状态

第 3 阶段:Azure配置

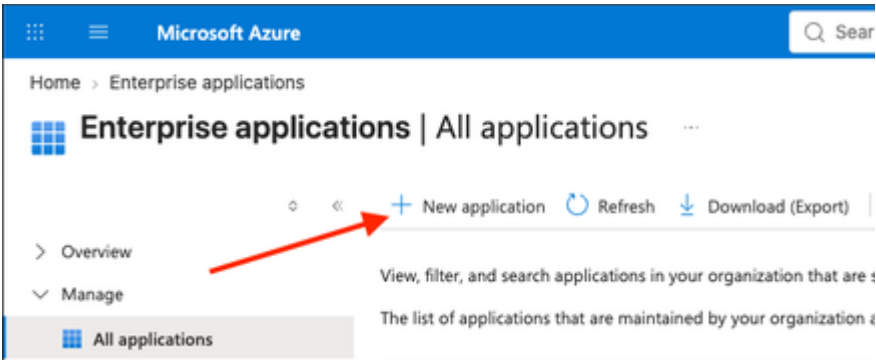
步骤 1：为SAML工具包创建Entra Enterprise应用程序

1)搜索并点击Enterprise Applications。



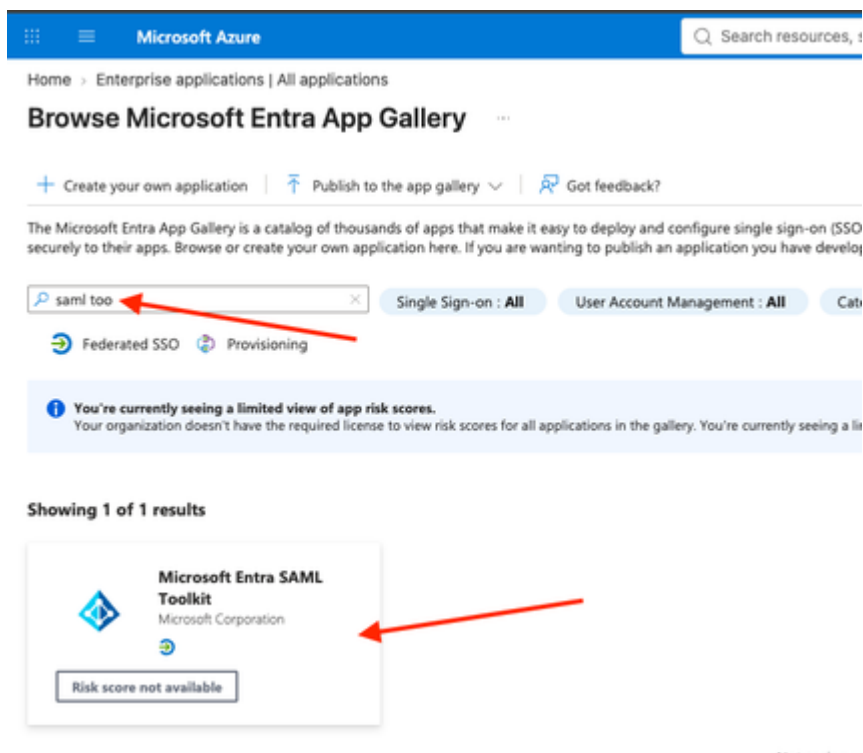
搜索和访问企业应用

2)单击+ New Application。



选择企业应用程序中的新应用程序

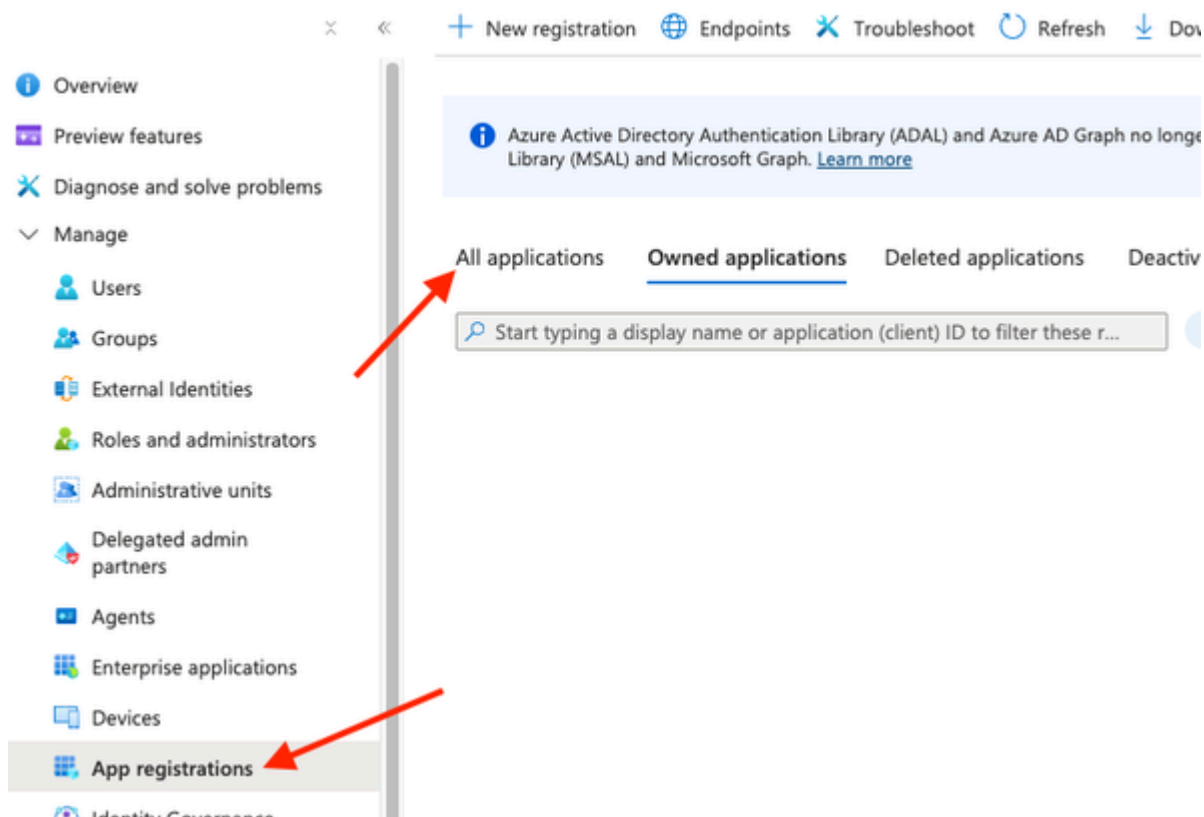
3)搜索Microsoft Entra SAML Toolkit，然后点击其缩略图。



搜索并选择Microsoft Entra SAML Toolkit

4)为Microsoft Entra SAML Toolkit Enterprise Application指定Name，然后单击Create。(来自Microsoft的参考：[请阅读我们的Microsoft Entra SAML Toolkit逐步集成教程](#))。

1)导航回Entra ID，然后从左侧导航菜单中选择App registrations。单击All applications过滤器并搜索为Enterprise Application指定的名称。点击适当的应用。



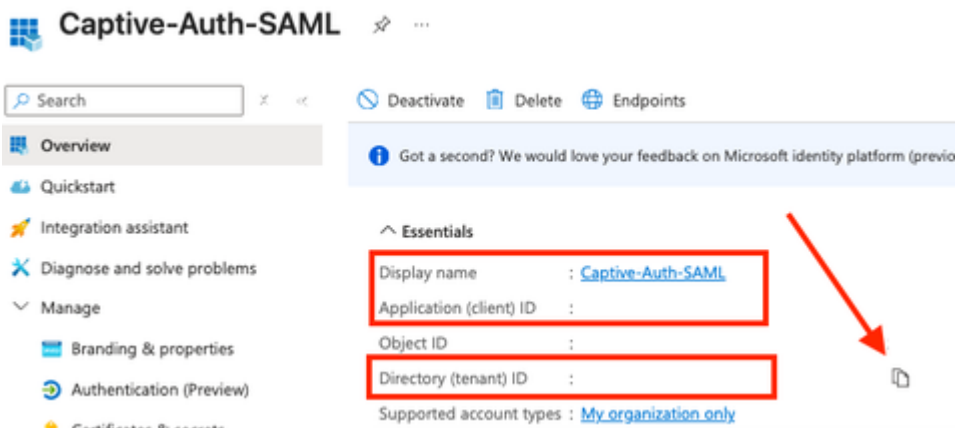
导航到应用注册和所有应用

2)收集并记录Enterprise App Registration下的Essentials值。



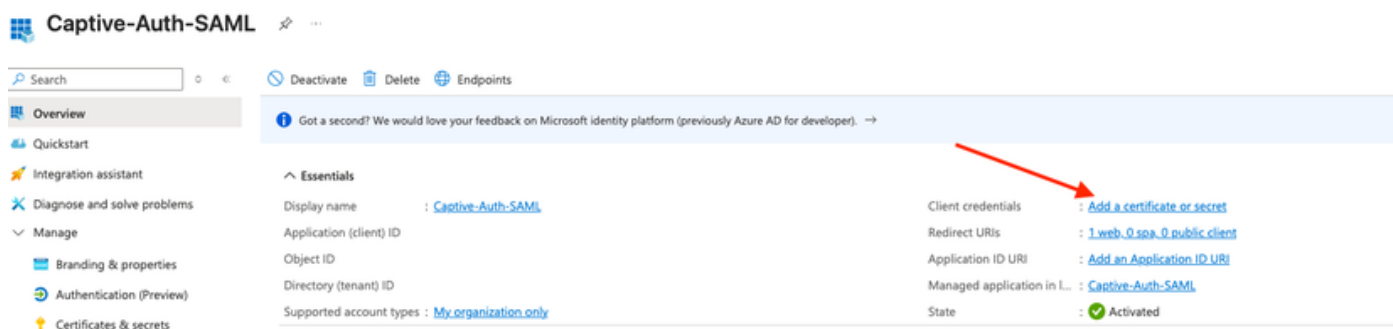
重要信息：将鼠标悬停在值上，以显示复制到剪贴板，并收集概述页面上Essentials下的值：

- 显示名称
- 应用（客户端）ID
- 目录（租户）ID



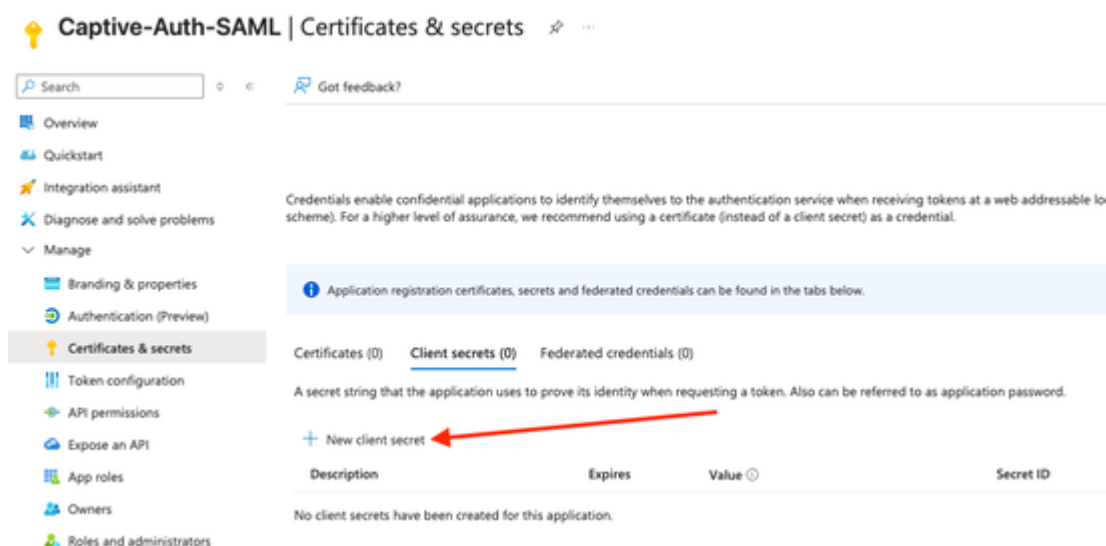
收集显示以及应用程序和目录ID值

3)单击Add a certificate or secret超链接。



添加证书或密钥超链接

4)单击+ New client secret。



添加新客户端密钥

5)提供密码说明，并根据需要调整过期。单击 Add。

Add a client secret

Description

saml-secret

Expires

Recommended: 180 days (6 months)

Add

Cancel

提供客户端密钥的说明

6)复制密钥。



重要信息：注意复制到剪贴板的加密值。

Captive-Auth-SAML | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

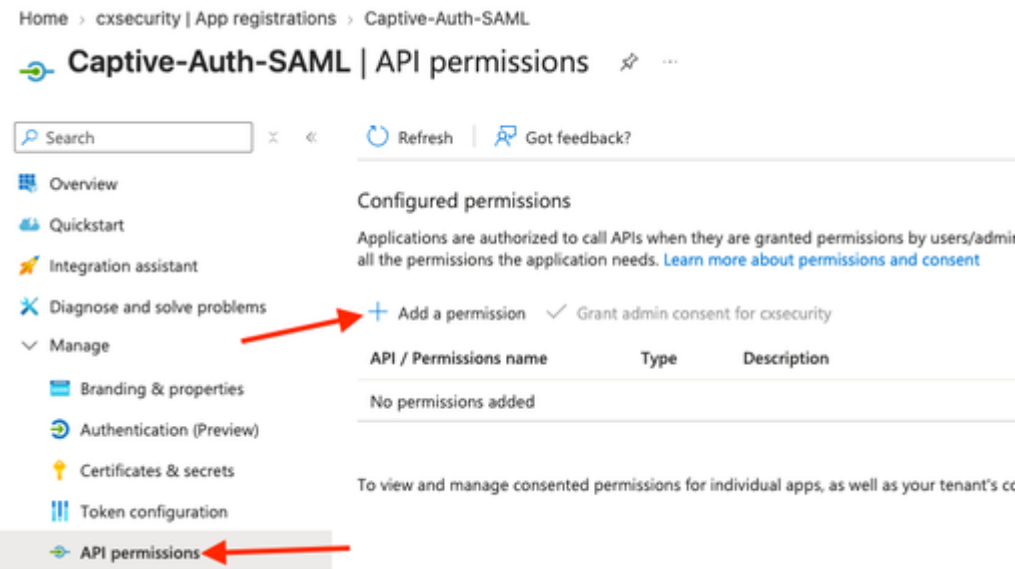
New client secret

Description	Expires	Value	Secret ID
saml-secret	3/14/2027		

复制客户端加密值

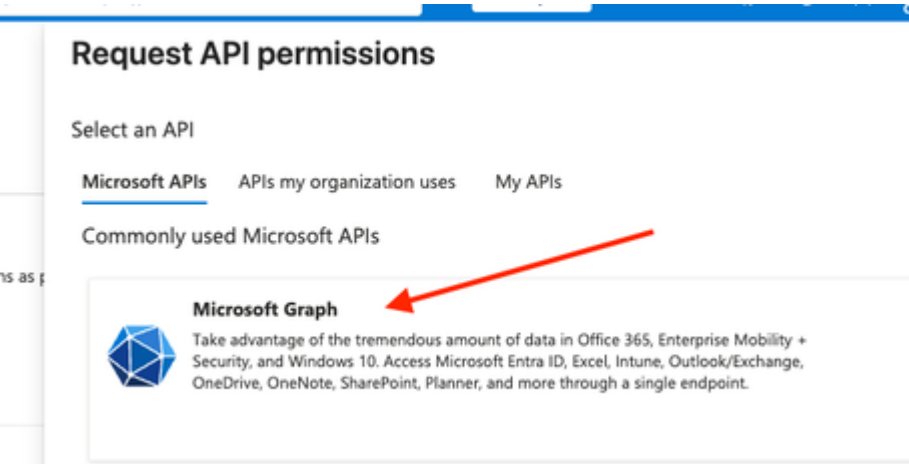
步骤3.为应用程序注册配置Microsoft Graph API权限。

1)从左侧导航菜单中选择API Permissions , 然后单击+添加权限。



配置API权限

2)单击Microsoft Graph API。



选择Microsoft Graph API

3)授予Delegated User.Read权限 , 然后单击Add permissions。

Request API permissions

[← All APIs](#)

 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

 User.Read

Permission	Admin consent required
> AgentIdUser	
> IdentityRiskyUser	
▼ User (1)	
☒ User.Read ⓘ Sign in and read user profile	No
☐ User.Read.All ⓘ Read all users' full profiles	Yes
☐ User.ReadBasic.All ⓘ Read all users' basic profiles	No

[Add permissions](#) [Discard](#)

授予授权用户读取权限

4)授予Application User.Read.All权限 (选中复选框)。

Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Permission	Admin consent required
> IdentityRiskyUser	
User (1)	
☒ User.Read.All ⓘ Read all users' full profiles	Yes

授予应用程序读取所有权限

5)搜索并选中Group.Read.All复选框以授予Group Read权限。单击添加权限。

Select permissions

[expand all](#)

Permission	Admin consent required
Group (1)	
☒ Group.Read.All ⓘ Read all groups	Yes

保存API权限

6)确认配置的权限是否一致，并授予其管理同意。

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for ...
User.Read	Delegated	Sign in and read user profile	No	...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for ...

授予权限管理同意

7)显示授予管理员同意后的输出。

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

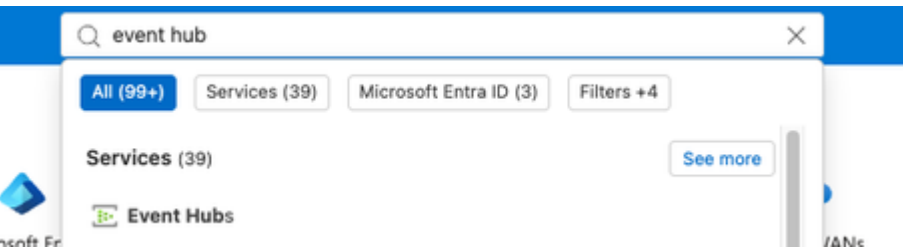
✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	✔ Granted for ...
User.Read	Delegated	Sign in and read user profile	No	✔ Granted for ...
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for ...

授予的管理同意输出

步骤 4：配置事件中心(EH)命名空间

1)搜索并点击Event Hub。



搜索事件中心配置

2)创建新的EH命名空间。



No event hubs namespaces to display

An Event Hubs namespace is a management container for event hubs which provides DNS-integrated network endpoints and a range of access control and network integration management.

[+ Create](#)

[Learn more about Event Hubs](#)

创建事件中心命名空间

3)配置EH命名空间。



注意：必须选择Standard定价层或更高版本。基本定价层阻止领域使用。

请参阅[Azure Event Hub文档](#)，以进一步评估Event Hub高级设置以及对特定需求的适用性。

单击Review + Create。



Create Namespace

Event Hubs

[Basics](#) [Advanced](#) [Networking](#) [Tags](#) [Review + create](#)

Project Details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *

[Create new](#)

Instance Details

Enter required settings for this namespace, including a price tier and configuring the number of units (capacity).

Namespace name * ☒ .servicebus.windows.net

Region * ☒
i The region selected supports Availability zones. Your namespace will have Availability Zones enabled. [Learn more](#)

Pricing tier * ☒
[Browse the available plans and their features](#)

Throughput Units *

Enable Auto-Inflate ? ☐

[Review + create](#)

< Previous

Next: Advanced >

配置事件中心命名空间设置

4)验证成功后，单击Create。

Home > Event Hubs

Create Namespace

Event Hubs

Validation succeeded.

Basics Advanced Networking Tags Review + create

Event Hubs Namespace
by Microsoft

Basics

Namespace name	captive-auth-ad-eh
Subscription	
Resource group	
Region	East US
Pricing tier	Standard
Throughput Units	1
Availability Zones (Zone Redundancy)	Enabled
Auto-inflate Maximum Throughput Units	Disabled

Networking

Connectivity method	Public access
Network Protocol Preference	IPv4 only

Security

Minimum TLS version	1.2
Local Authentication	Enabled

Create < Previous Next >

创建事件中心命名空间部署

5)确认部署完成，然后单击Go to resource。

Home

captive-auth-ad-eh | Overview

Deployment

Search Delete Cancel Redeploy Download Refresh

Overview

- Inputs
- Outputs
- Template

Your deployment is complete

Deployment name : captive-auth-ad-eh
Subscription :
Resource group :

> Deployment details

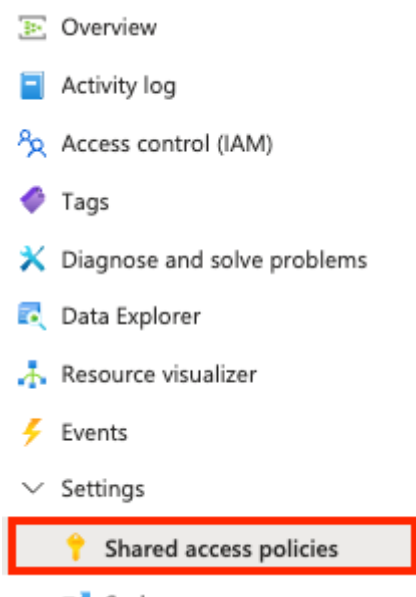
> Next steps

Go to resource

转到Event Hub命名空间资源

步骤 5：在事件中心名称空间中选择或创建共享访问策略

1)从左侧导航菜单中选择设置>共享访问策略。



导航到共享访问策略

2)点击+ Add并输入新的Policy name，然后选中Manage复选框。单击Add SAS Policy菜单面板底部的Create。



添加新的共享访问策略



创建共享访问策略

步骤 6：从EH命名空间收集并记录共享访问签名(SAS)信息

1)点击新的共享访问策略;eh SAS策略显示在右侧面板中。

Regenerate primary key

Regenerate secondary key

Delete

Event Hubs access control with Shared Access Signatures [Learn more](#)

Claims

☒ Manage

☐ Send

☐ Listen

Primary key

Secondary key

Primary connection string

Secondary connection string

Event Hubs Access Control (IAM)

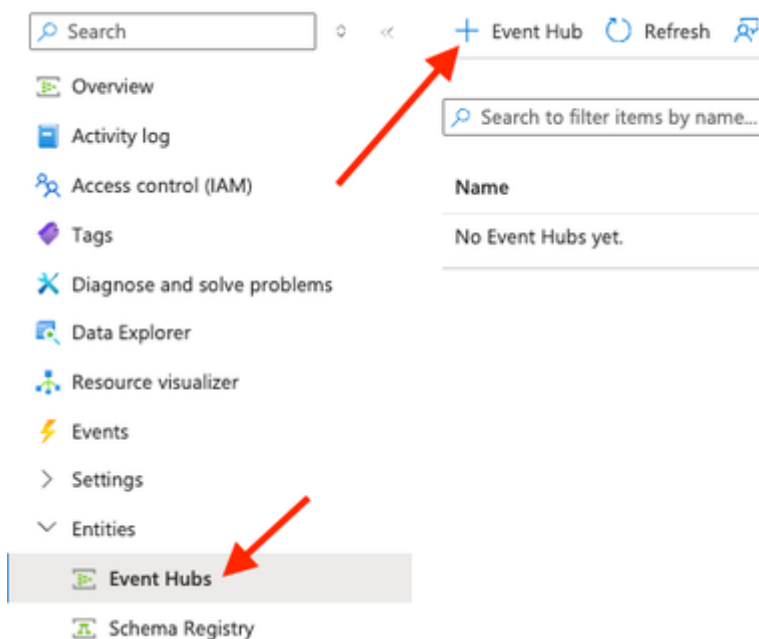
复制主连接字符串



重要信息：复制并记录Primary连接字符串。

步骤 7：在事件中心名称空间内创建事件中心实例

1)从Namespace菜单中，选择Entities > Event Hub。单击+ Event Hub以创建新的EH实例。



创建新的事件中心实例

2)为新EH实例分配名称，然后单击Review + create。

Home > Event Hubs > captive-auth-ad-eh | Event Hubs

Create Event Hub

Event Hubs

Basics Capture Review + create

Event Hub Details

Enter required settings for this event hub, including partition count and message retention.

Name * ⓘ captive-auth-ad-eh-1 ✓

Partition count ⓘ 1

Retention

Configure retention settings for this Event Hub. [Learn more](#)

Cleanup policy ⓘ Delete

Retention time (hrs) * ⓘ 1
min. 1 hour, max. 168 hours (7days)

Review + create < Previous Next: Capture >

为事件中心实例分配名称

3)验证成功后，单击Create以调配Event Hub实例。

Create Event Hub ...

Event Hubs

✓ Validation succeeded.

Basics Capture Review + create

Event Hubs Instance
by Microsoft

Basics

Name captive-auth-ad-eh-1
Partition count 1

Retention

Cleanup policy Delete
Retention time (hrs) 1

Capture

Capture Status Off

Create

< Previous

Next >

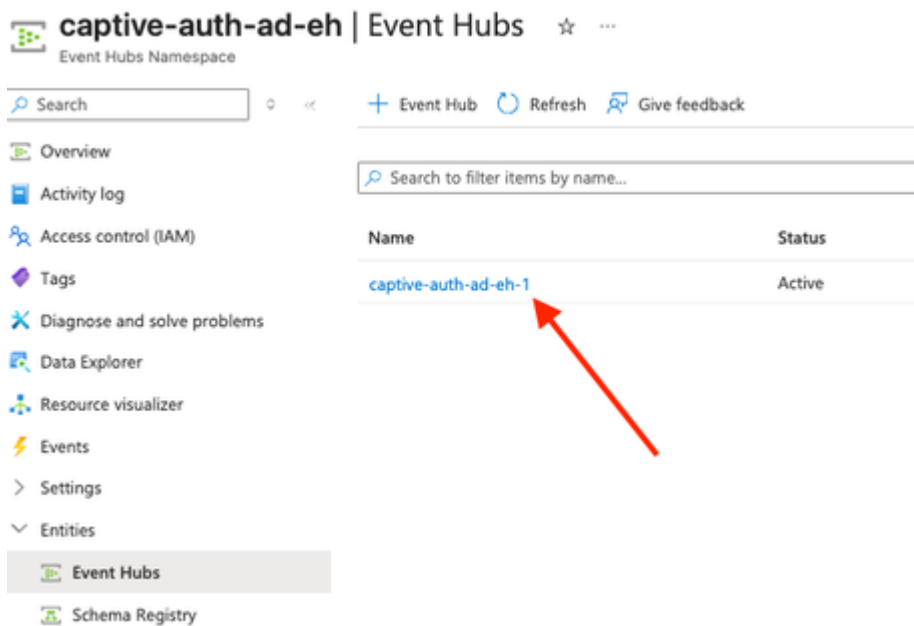
调配事件中心实例



重要信息：复制并记录Event Hub实例名称。

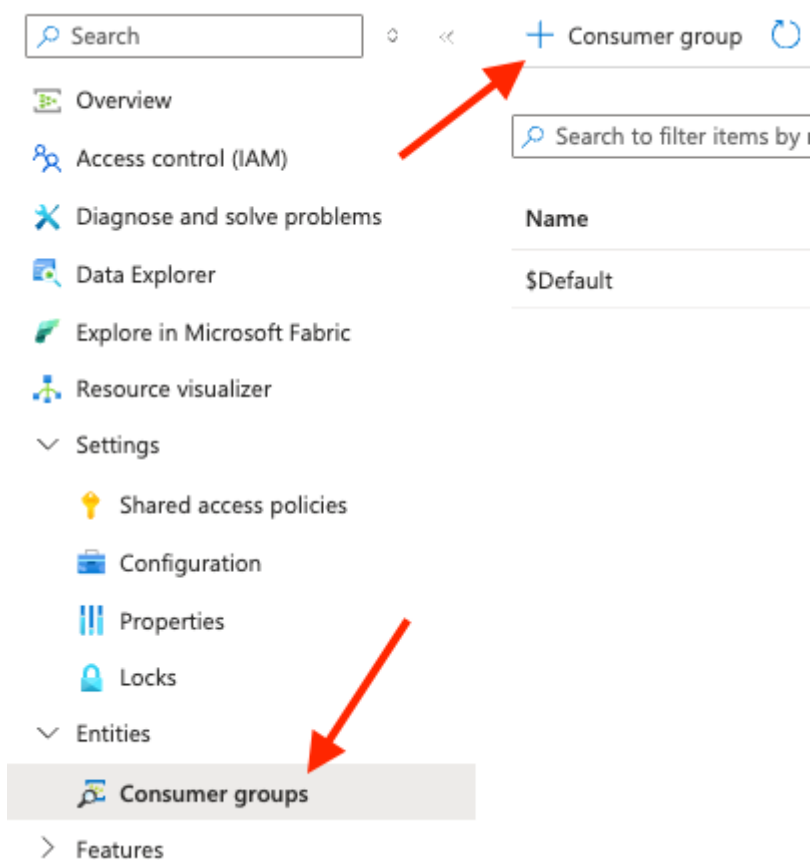
步骤 8::在事件中心命名空间内创建事件中心实例使用者组

1)点击上一步中配置的新EH实例。



访问事件中心实例配置

2)从EH实例中选择实体>消费者组，然后创建一个新的消费者组。



创建使用者组

3)为使用者组命名，然后单击创建。

Create consumer group

Consumer groups

Name *

captive-auth-ad-eh-cg

✓

Create

将名称分配给使用者组



重要信息：复制并记录Event Hub instance Consumer组名称。

步骤 9：验证收集的值

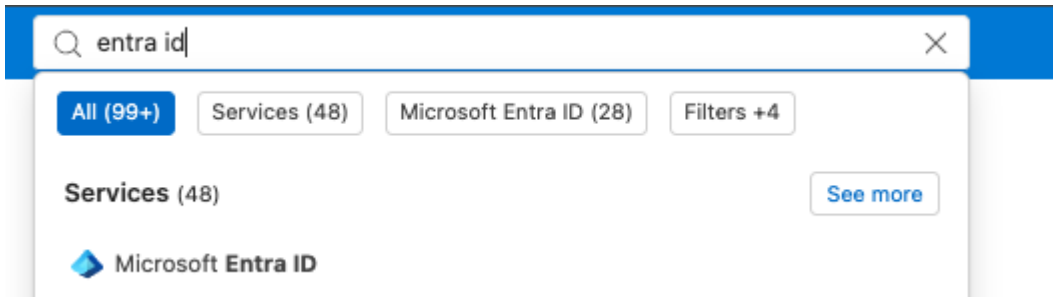
1)此时，应记录上述步骤中的这些值。如果没有记录任何值，请参考收集值的适用步骤：

- 第3阶段第2步 — 应用注册（针对此流程创建的企业应用，由收集的显示名称引用）
 - 步骤2，子步骤2
 - 显示名称
 - 应用（客户端）ID
 - 目录（租户）ID
 - 步骤2，子步骤6
 - 客户端密码
- 第3阶段第6步 — 事件中心
 - 第6步，子步骤1
 - EH命名空间
 - 主连接字符串
 - 步骤7，子步骤3
 - EH实例（事件中心）名称

- 第8步，子步骤3
 - EH使用者组名称

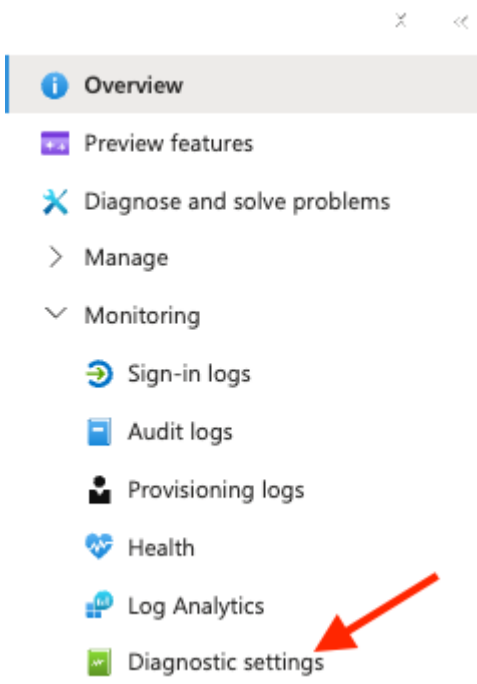
步骤 10：配置Entra ID Audit Log Streaming到Event Hub

1)导航回Entra ID租户配置。



搜索并导航至Entra ID租户配置

2)从左侧菜单中选择Monitoring > Diagnostic Settings。



诊断设置监控

3)选择Diagnostic settings > General，然后单击+ Add diagnostic setting。

<< Refresh Feedback

Diagnostic settings

General

Custom security attributes

Diagnostic settings are used to configure streaming export of platform logs

Diagnostic settings

Name	Storage account
	-
	-
	-

+ Add diagnostic setting

添加新诊断设置

4)为诊断设置分配所需的名称，选中AuditLogs复选框以记录，并选中Stream to an event hub复选框。参考之前配置中记录的值，完成后单击Save。

Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

captive-portal-auth

Logs

Categories

- ☒ AuditLogs
- ☐ SignInLogs
- ☐ NonInteractiveUserSignInLogs
- ☐ ServicePrincipalSignInLogs
- ☐ ManagedIdentitySignInLogs
- ☐ ProvisioningLogs
- ☐ ADFSSignInLogs
- ☐ RiskyUsers
- ☐ UserRiskEvents
- ☐ NetworkAccessTrafficLogs

Destination details

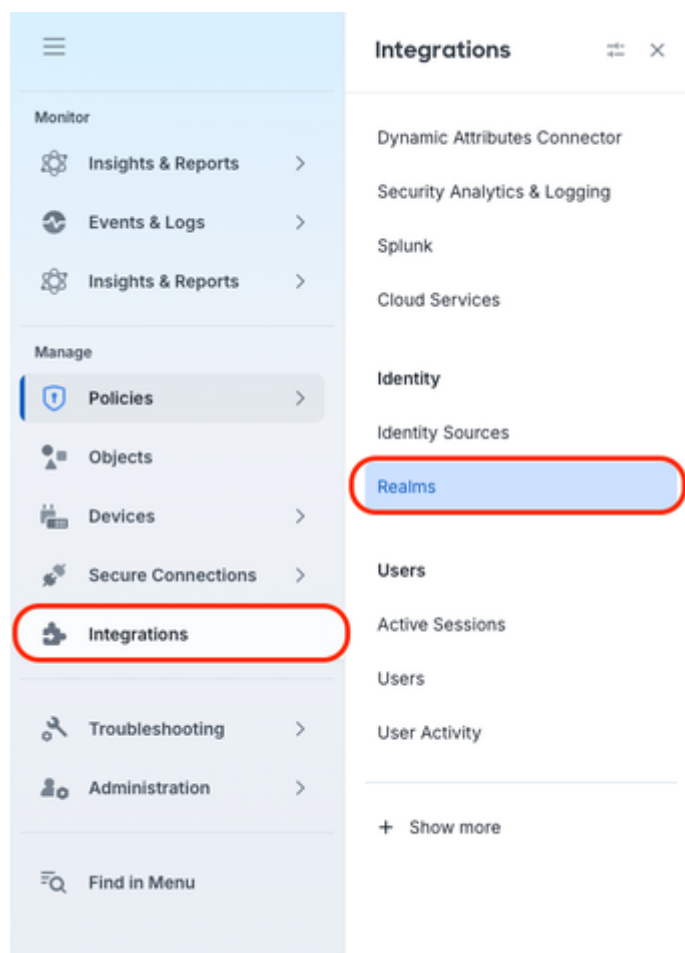
- ☐ Send to Log Analytics workspace
- ☐ Archive to a storage account
- ☒ Stream to an event hub
- For potential partner integrations, [click to learn more about event hub integration](#).
- Subscription
- Event hub namespace *
- captive-auth-ad-eh
- Event hub name (optional)
- captive-auth-ad-eh-1
- Event hub policy name
- ☐ Send to partner solution

将审核日志流式传输到事件中心

第 4 阶段：整合Azure和FMC/FTD主动身份验证配置

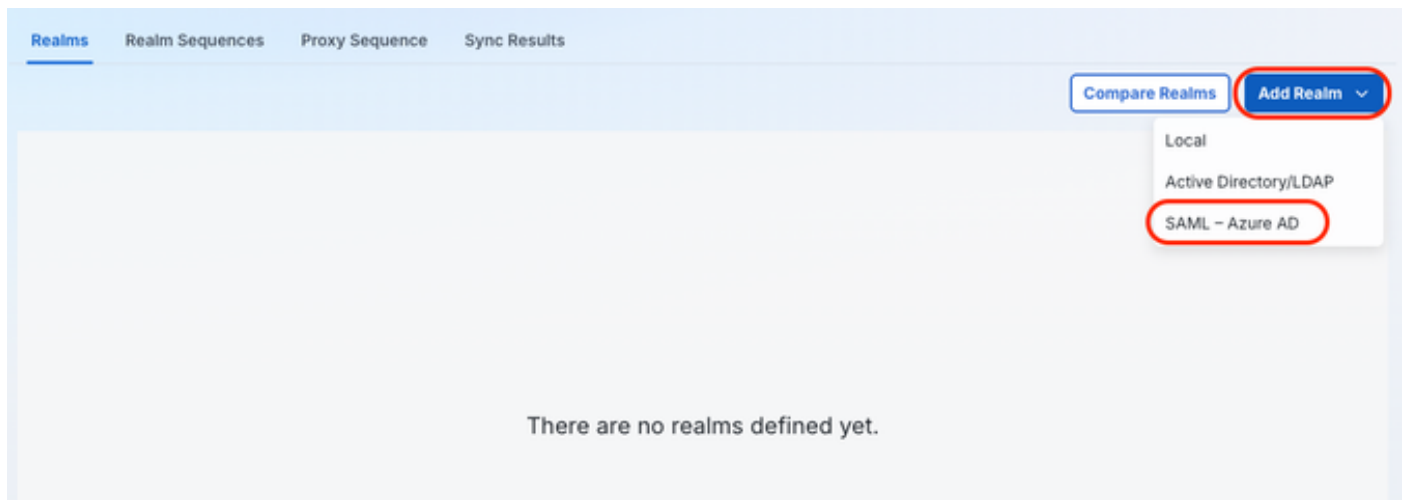
步骤 1：使用FMC向导配置Azure SAML/Entra ID领域

1)在FMC中，选择Integrations > Identity > Realms。



身份领域配置

2)单击Add Realm下拉列表，然后选择SAML - Azure AD。



添加SAML Azure AD领域

3)为Azure领域分配名称和说明以描述其使用，并确保从配置类型下拉列表中选择使用被动对Azure AD进行身份验证或使用强制网络门户对Azure AD。单击 Next。

配置Azure AD领域设置

4)选择先前配置的FQDN对象作为基本URL。输入带有所示字符串格式的实体ID:

`https://<fqdn-base-url>/<uniqueSuffix>`

- 配置SAML实体ID后缀（在下面的配置示例中用绿色下划线）时，请确保后缀在环境中的其他SSO实现中是唯一的。此值也必须与Azure SAML配置匹配。基本URL在整个配置中保持不变。
- Assertion Consumer Services(ACS)URL会自动填充且不可变。
- 在Devices > Certificates下，选择在FMC中之前的工作流程步骤中注册的服务提供商(SP)证书。
- 输入这些值后，单击下载服务提供商元数据以简化配置过程，并确认预期值已写入Azure。

Add SAML – Azure AD Realm

1 Realm Details Edit

Name	azure-entra-saml
Description	Active Authentication IdP
Identity Provider	Azure AD
Configuration Type	Authenticate passively with Azure AD or using captive portal with Azure AD

2 SAML Service Provider (SP) Metadata

Base URL *

active_auth_fqdn ⓧ +

Must resolve to the interface(s) of source security zones used in an identity policy.

Entity ID *

https://ftd-inside.example.com/saml/sp/metadata/activeAuthEntID 📋

Unique, alphanumeric identifier for a SAML entity.

Assertion Consumer Services (ACS) URL *

https://ftd-inside.example.com/+CSCOE+/saml/sp/acs?tname=azure-entra 📋

URL at which the service provider receives SAML assertions from Azure AD.

Service Provider Certificate *

FTD-SP-Cert ⓧ +

Certificate used for SAML authentication and TLS/SSL communication with the secure threat defense device. The certificate must have the value you specify for Base URL that must match the Common Name (CN) or Subject Alternative Name (SAN). The certificate, which must be in PKCS12 format, must be trusted by clients.

Download Service Provider Metadata

Next

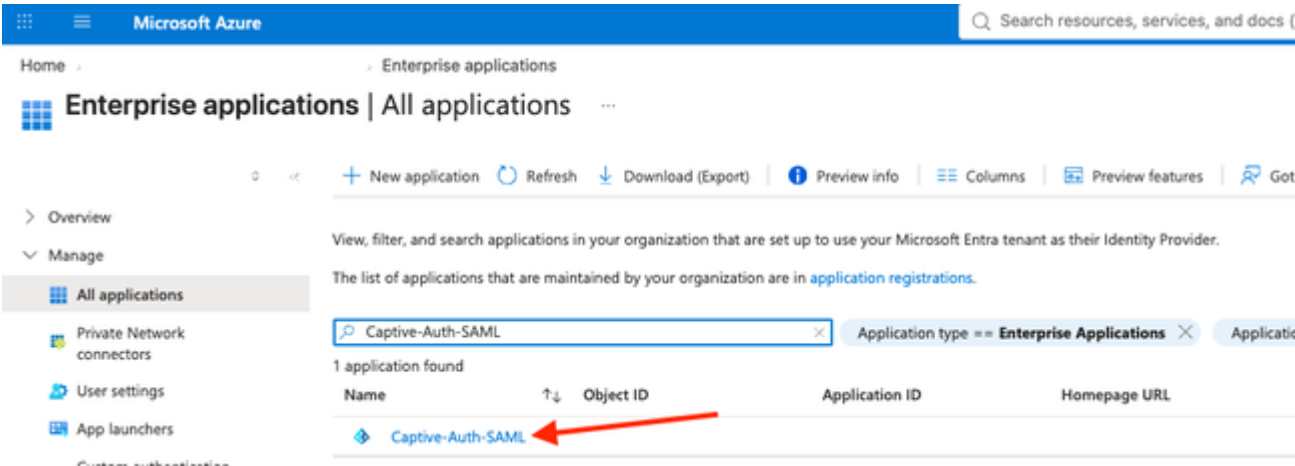
配置基本URL和实体ID并下载SAML元数据

5)单击Next转到Realm配置的Sequence 3。

步骤 2：在Azure企业应用程序中实施FMC配置的SAML SP元数据

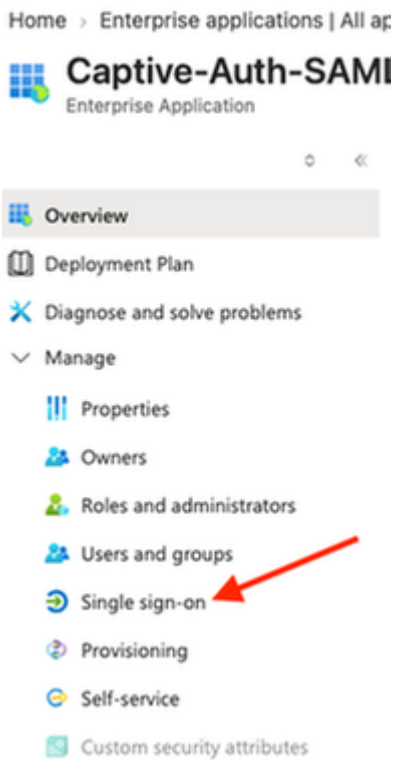
1)导航回Azure，然后选择Entra ID > Manage > Enterprise Applications。搜索以前创建的Microsoft

Entra SAML Toolkit Enterprise应用程序的实例。



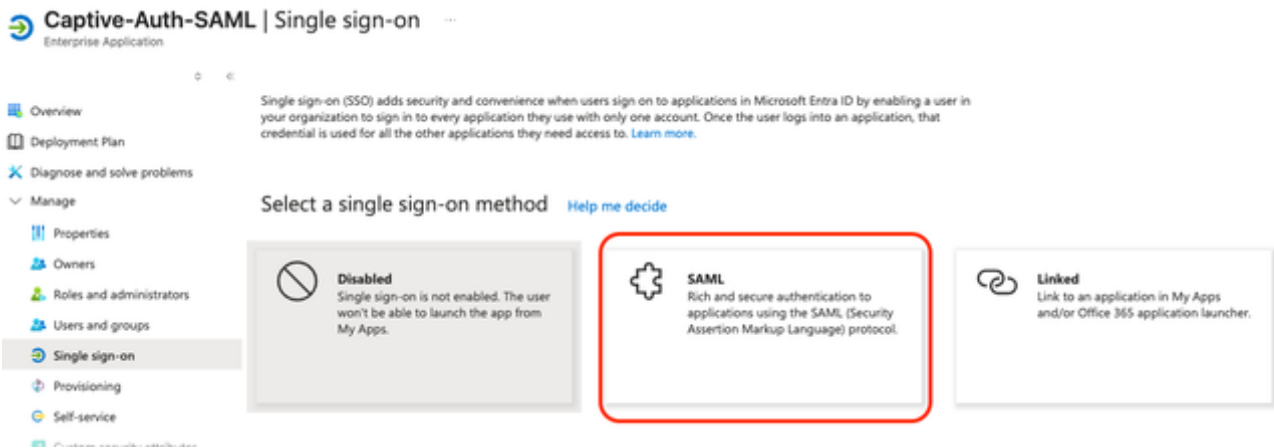
查找Microsoft Entra SAML Toolkit应用程序

2)从侧面导航菜单中选择管理>单点登录。



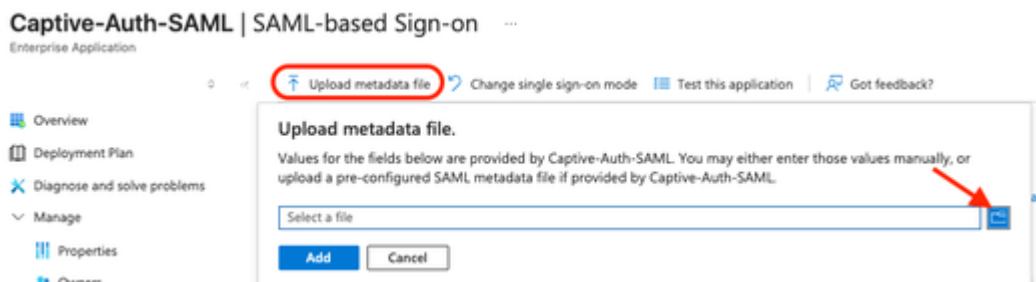
管理单点登录配置

3)点击SAML单点登录(SSO)模式。



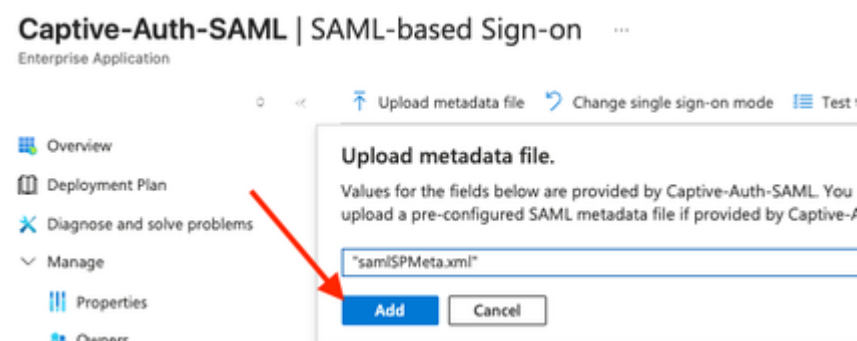
SAML单点登录模式选择

4)单击Upload metadata file，然后单击蓝色文件夹图标浏览本地文件系统，以查找从FMC下载的SAML元数据文件。



从防火墙管理中心上传元数据文件

5)上传完成后，单击Add。



添加SAML配置应用程序

6)系统将显示基本SAML配置的侧面板，并且从自动上传并应用的FMC源的SP元数据XML文件中提取标识符（实体ID）和ACS URL等值。但是，登录URL未填充，保存之前需要使用此登录URL。

Basic SAML Configuration

 Save |  Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default





[Add identifier](#)

Patterns: https://samltoolkit.azurewebsites.net

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default



0



[Add reply URL](#)

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

Patterns: https://samltoolkit.azurewebsites.net/

✗ Please enter a valid URL starting with "https://". If your URL has query parameters, ensure that there is a slash preceding the question mark (i.e. /?)

✗ This field is required

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.



基本SAML配置提取

7)使用给定的登录URL模式，复制并粘贴值，并在完成时点击顶部的Save。

Basic SAML Configuration



Save



Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default



[Add identifier](#)

Patterns: <https://samltoolkit.azurewebsites.net>

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default

0



[Add reply URL](#)

Patterns: <https://samltoolkit.azurewebsites.net/SAML/Consume>

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*



Patterns: <https://samltoolkit.azurewebsites.net/>

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.



登录URL配置条目

向下滚动到SAML Certificates，然后导出Azure生成的联合元数据XML文件，以便导入到Cisco Secure FMC。

3

SAML Certificates

Token signing certificate

Status

Active

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

Download

Download

Download

Edit

Verification certificates (optional)

Required

No

Active

0

Expired

0

Edit

导出联合元数据XML文件

步骤 3：使用FMC向导配置Azure SAML/Entra ID领域（续）

1)导航回FMC。在Sequence 3, SAML Identity Provider(IdP)Metadata下，将从Azure下载的已导出联合元数据XML文件上传到FMC以自动填充所需的值。

3

SAML Identity Provider (IdP) Metadata

Entity ID *

Unique, alphanumeric identifier for a SAML entity.

Single Sign-On (SSO) URL *

http(s)://

URL to your identity provider. You must include the scheme (e.g., https://).

IdP Certificate *

Select...

+

Choose a certificate from the list or upload a new certificate in manual format.

Click to upload or drag and drop a file.

Upload XML

Federation XML you downloaded from Azure AD. If you upload this, you don't have to enter the other values in this section.

上传联合元数据XML文件

2)上传后，这些值将按如下所示进行填充。

3 SAML Identity Provider (IdP) Metadata

Entity ID *

https://sts.windows.net/

Unique, alphanumeric identifier for a SAML entity.

Single Sign-On (SSO) URL *

https://login.microsoftonline.com/

URL to your identity provider. You must include the scheme (e.g., https://).

IdP Certificate *

Certificate-

Choose a certificate from the list or upload a new certificate in manual format.

Click to upload or drag and drop a file.

Upload XML

Federation XML you downloaded from Azure AD. If you upload this, you don't have to enter the other values in this section.

Next

自动填充的SAML身份提供程序值



注意：部分输出如图所示。

3)输入截至此点的整个实施过程中收集的值：

- 应用注册
 - 应用（客户端）ID
 - 客户端密码
 - 目录（租户）ID
- 事件中心
 - EH命名空间主机名
 - EH命名空间主连接字符串
 - EH实例（事件中心）名称
 - EH使用者组名称

Add SAML – Azure AD Realm



4 Azure AD Details

Client ID * 851607f9-969f-4fed-90ec-829607c1c Application ID (also referred to as client ID you created in Azure AD).	Client Secret * Secret string that the application uses to prove its identity when requesting a token.
Tenant ID * af42bac0-52aa-429f-92db-9258199f Microsoft Entry ID entity that typically encompasses an organization. Displayed in Azure Entra ID → Properties.	Event Hubs Host Name * captive-auth-ad-eh.servicebus.windows.net Hostname of the Event Hub Namespace. Displayed in Event Hubs → Event Hubs Namespace.
Event Hub Name * captive-auth-ad-eh Name of your event hub. Displayed in Event Hubs Name Space → Overview.	Consumer Group Name * captive-auth-ad-eh-cg A view of an entire event hub. Consumer groups enable consuming applications to each have a separate view of the event stream.
Event Hub Connection String * Endpoint=sb://captive-auth-ad-eh.servicebus.windows.net;/SharedAccessKeyName=... Event Hub Connection String: Unique identifier for the event hub (also referred to as topic or endpoint). It is displayed on the Azure AD portal in Event Hubs → (name of your event hub) → Shared access policies → (name of policy).	
USER GROUPS ☒ ☐ Excluded User Groups ☒ Included User Groups Enter each group name on a separate line active-auth-lab Enter one or more groups from which to download users for identity control. Users in these groups will be available for use in access control policies.	

Test

Test connection succeeded

Next

输入应用和事件中心信息

输入后，单击测试检查连接，并使用提供的信息确认可以访问Azure。



注意：如果适用，请确保排除/包含的用户组与Entra配置保持一致

4)向导的最后一步允许您配置SAML强制网络门户用户超时。默认值为1440分钟。

5 User Session Timeout

SAML Captive Portal Users

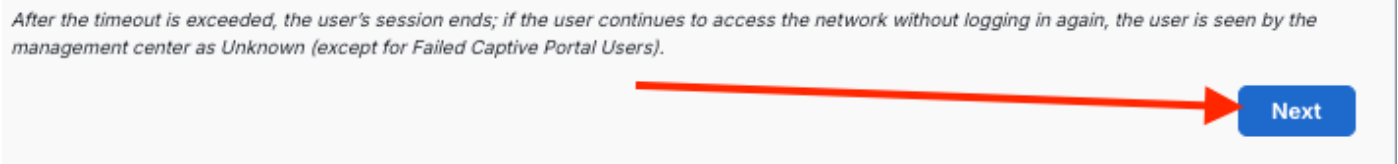
1440

Minutes

Range 0-35791394

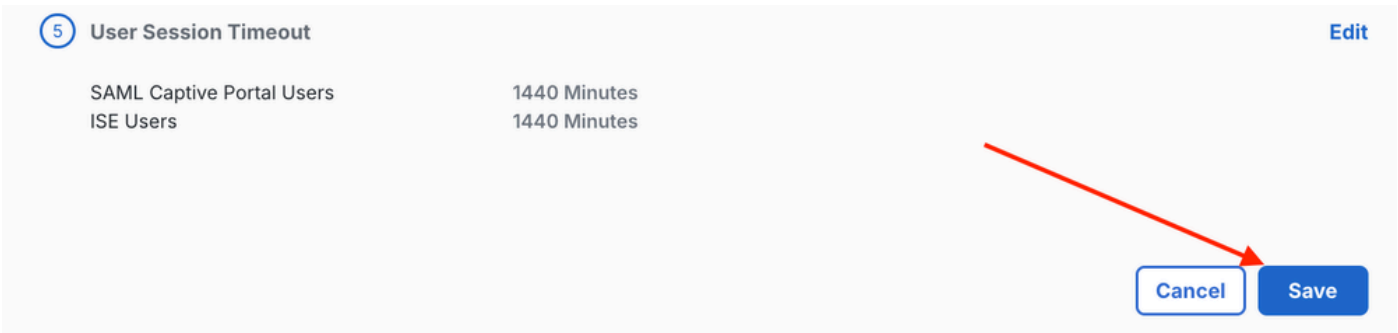
配置强制网络门户超时

5)单击Next继续。



使用Azure AD领域配置前进

6)向导提供已实施的配置的摘要。验证并确认输入的值后，在摘要末尾单击Save。



领域配置摘要保存按钮

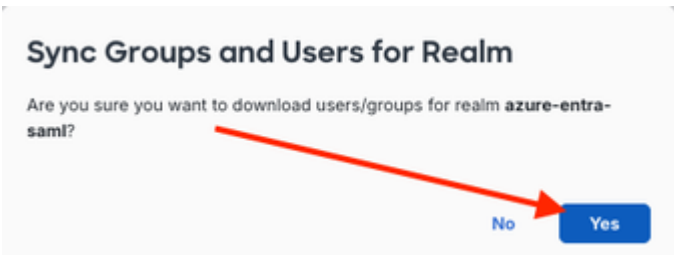
步骤 4：检查下载的用户

1)使用集成>身份>领域工作流程中的立即下载按钮，确认可以从Azure Entra下载用户。



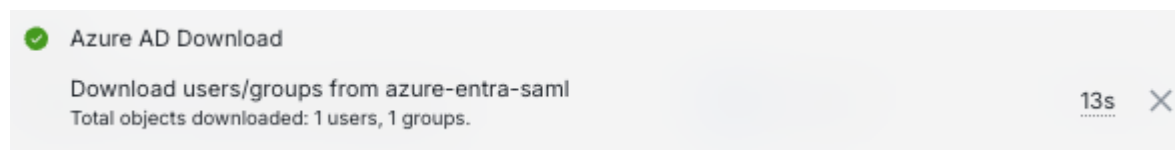
从Azure AD下载用户

2)响应对话框提示，单击Yes。



确认从Azure AD下载用户

3)下载任务会生成1个用户和1个已下载的组，如Notifications > Tasks下确认的。

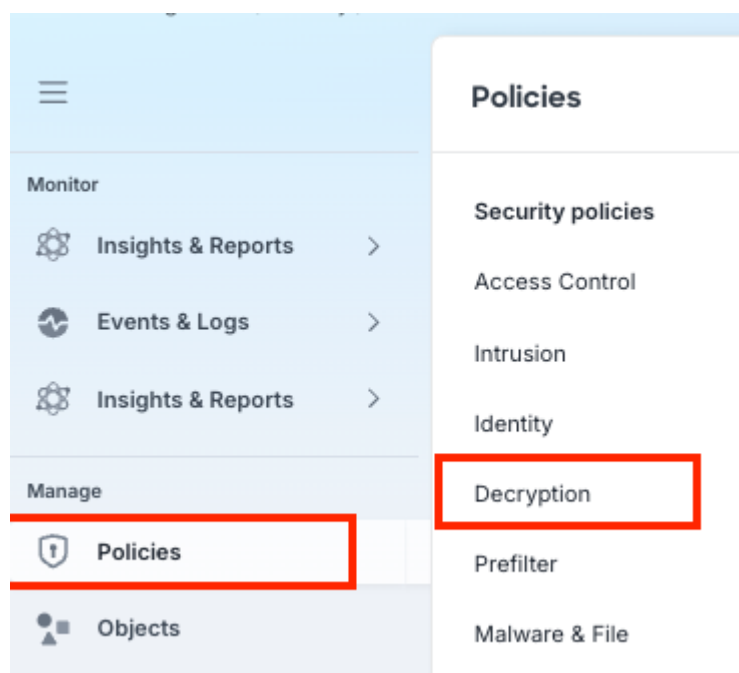


用于从Azure AD下载用户的通知条目

第 5 阶段：在FMC中配置策略

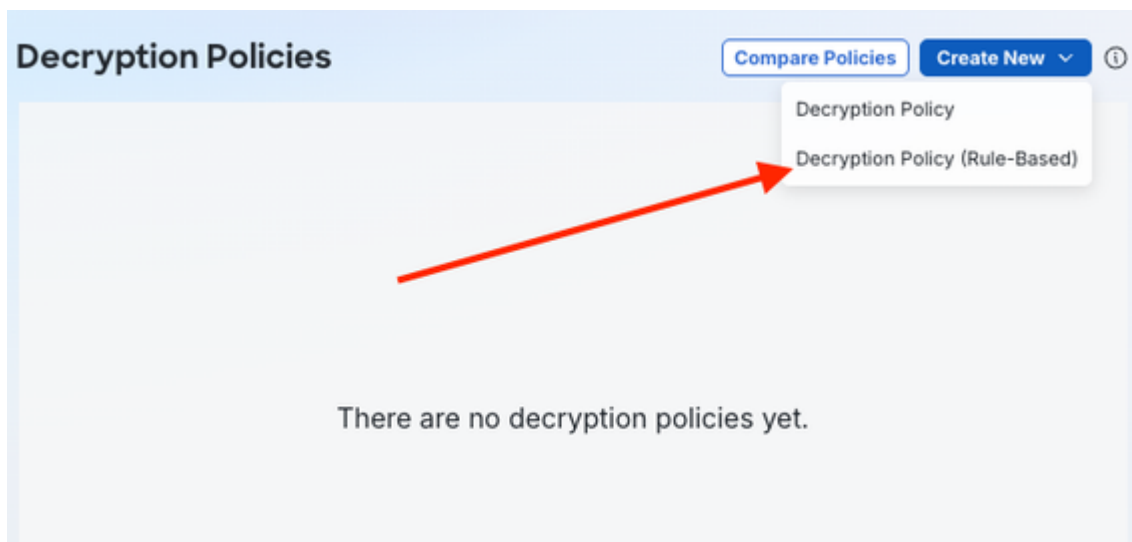
步骤 1：配置解密策略

1)在FMC中，选择Policies > Security Policies > Decryption。



导航到解密策略

2)点击Create New下拉列表，然后选择Decryption Policy(Rule-Based)。



创建新的基于规则的解密策略

3)为基于规则的新解密策略分配名称和说明（如果需要），然后单击Outbound Connections(User Protection)选项卡选项，以实施强制网络门户身份验证所需的Decrypt-Resign功能（主动身份验证）。

实施出站连接策略详细信息

4)从同一对话框中的适用下拉列表中选择之前应用的内部CA。单击 Next。

5)根据需要自定义选项。

Create Decryption Policy ?

1 **Policy Details**
Enter name, description, choose policy type and certificates.

2 **Blocking**
(Optional) Configure blocking based on TLS version and certificate status

3 **Decryption Exclusions**
(Optional) Configure exclusions for outbound connections.

☐ **Block inbound and outbound connections based on TLS version**
We recommend blocking the following because they are not secure. [Reset to default](#)
SSL v3.0 X TLS v1.0 X TLS v1.1 X

☐ **Block inbound and outbound connections based on server certificate status**
We recommend blocking the following because they are not secure. [Reset to default](#)
Invalid Signature X Expired X Not Yet Valid X

[Cancel](#) [Skip](#) [Back](#) [Next](#)

自定义解密策略选项

6)在本例中，使用缺省值，但所需的Policy Details除外。单击Create Policy完成配置向导。

Create Decryption Policy

1 Policy Details
Enter name, description, choose policy type and certificates.

2 Blocking
(Optional) Configure blocking based on TLS version and certificate status

3 Decryption Exclusions
(Optional) Configure exclusions for outbound connections.

Decryption Exclusions

☐ Bypass decryption for sensitive URL categories
In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Customize the list below to bypass inspection for designated categories.
Note: URL License is Required
URL Categories: Finance Online Trading Health and Medicine + Add

☒ Bypass decryption for undecryptable distinguished names
Bypass decryption based on Cisco's list of known undecryptable distinguished names.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported distinguished names.
[56 Distinguished names included](#)

☒ Bypass decryption for undecryptable applications
Certain applications are not supported for decryption due to a variety of reasons (certificate pinning, client certificate authentication, and so on). This option bypasses decryption based on Cisco's list of known undecryptable applications.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported applications.
[59 Applications included](#)

Intelligent Decryption Bypass

☐ Bypass decryption for very low-risk connections
Bypass decryption for very low-risk clients connecting to trusted servers.
Note: Do not decrypt traffic for very low-risk clients connecting to trusted servers, based on the threat confidence levels of clients

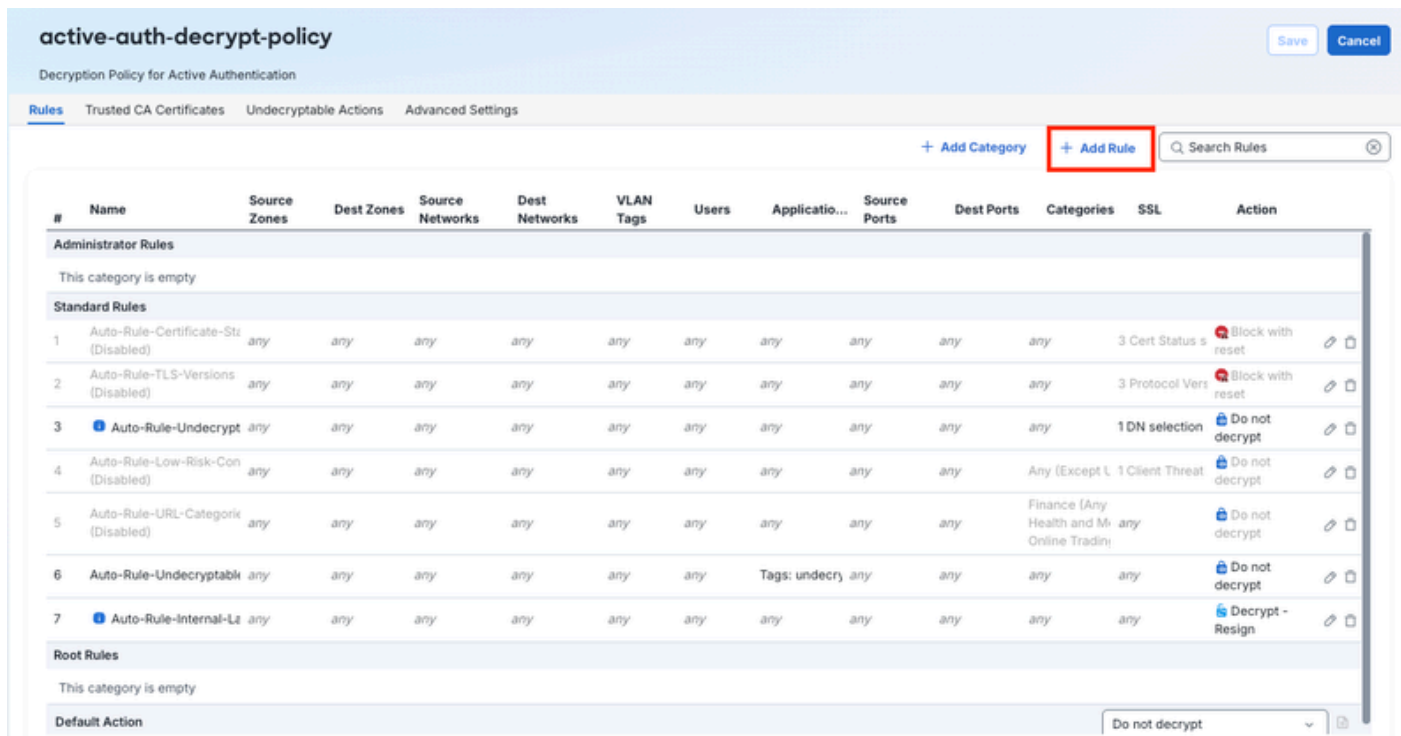
Cancel Skip Back Create Policy

创建最终解密策略

步骤 2：配置解密策略规则

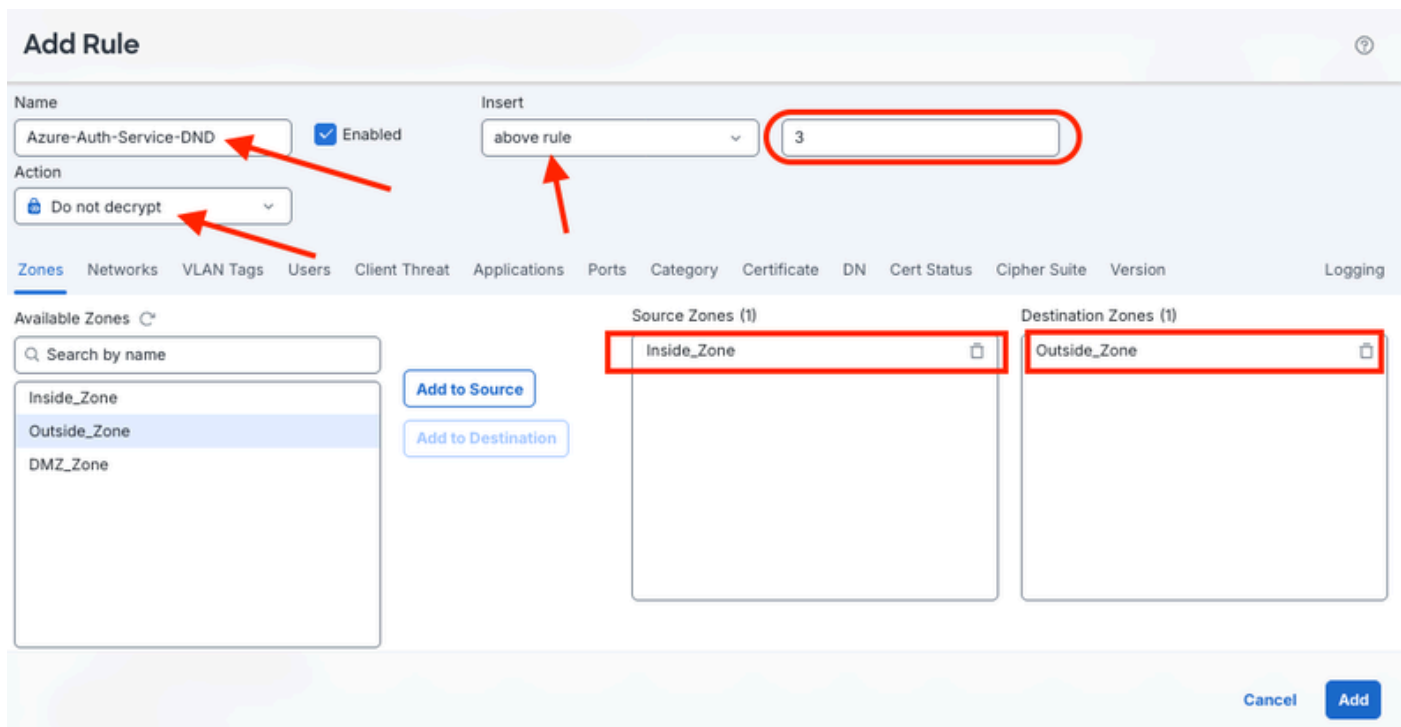
1)基于规则的解密策略的默认布局如下所示。与默认启用的规则不匹配的流量，例如规则3（引用无法解密的域名的预分配列表）和规则6（引用标记为无法解密的应用程序），将接受规则7下的“解密—重新签名”(Decrypt - Resign)操作。这些默认值以及“默认操作”(Default Action)可根据需要进行修改。默认情况下，不匹配其他规则的流量配置为Do Not Decrypt。

Azure Authentication Service流量不能解密以进行检查，因此为其创建专用规则。单击+ Add Rule开始。



添加规则并显示基于默认规则的解密布局

2)为新的解密策略规则条目分配名称，从“操作”(Action)下拉列表中选择不解密(Do not decrypt)，并将规则放在不太具体的规则顶部。还实施源/目标区域以进一步缩小规则范围。



配置不解密规则

3)在添加规则之前，单击Applications选项卡，搜索并点击Azure Authentication Service应用程序。单击Add to Rule，然后单击Add。

Add Rule

Name

Azure-Auth-Service-DND

Enabled

Insert

above rule

3

Action

Do not decrypt

Zones

Networks

VLAN Tags

Users

Client Threat

Applications

Ports

Category

Certificate

DN

Cert Status

Cipher Suite

Version

Logging

Application Filters

Clear All Filters

Search by name

Risks (Any Selected)

Very Low

809

Low

715

Medium

2239

High

1823

Very High

609

Business Relevance (Any Selected)

Very Low

809

Available Applications (2)

Search azure a

All apps matching the filter

Azure Arc

Azure Authentication Service

Add to Rule

Selected Applications and Filters (0)

any

Cancel

Add

添加Azure身份验证服务应用程序规则

4)单击Save。

active-auth-decrypt-policy

Decryption Policy for Active Authentication

Rules

Trusted CA Certificates

Undecryptable Actions

Advanced Settings

You have unsaved changes

Save

Cancel

+ Add Category

+ Add Rule

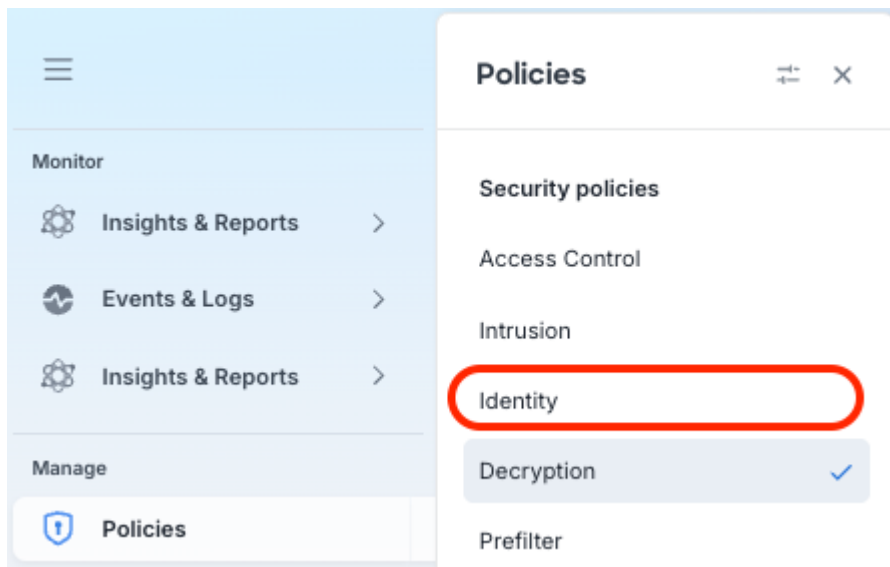
Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	Categories	SSL	Action
Standard Rules													
1	Auto-Rule-Certificate-St (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Cert Status s	Block with reset
2	Auto-Rule-TLS-Versions (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Protocol Ver	Block with reset
3	Azure-Auth-Service-	Inside_Zone	Outside_Zon	any	any	any	any	Azure Authent	any	any	any	any	Do not decrypt

保存解密策略

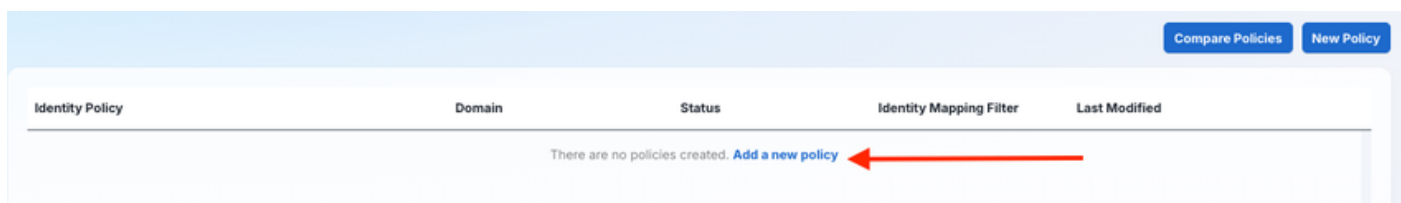
步骤 3：创建身份策略

1)选择Policies > Security Policies > Identity以创建身份策略。



创建身份策略

2)创建新的身份策略，然后点击Add a new policy。



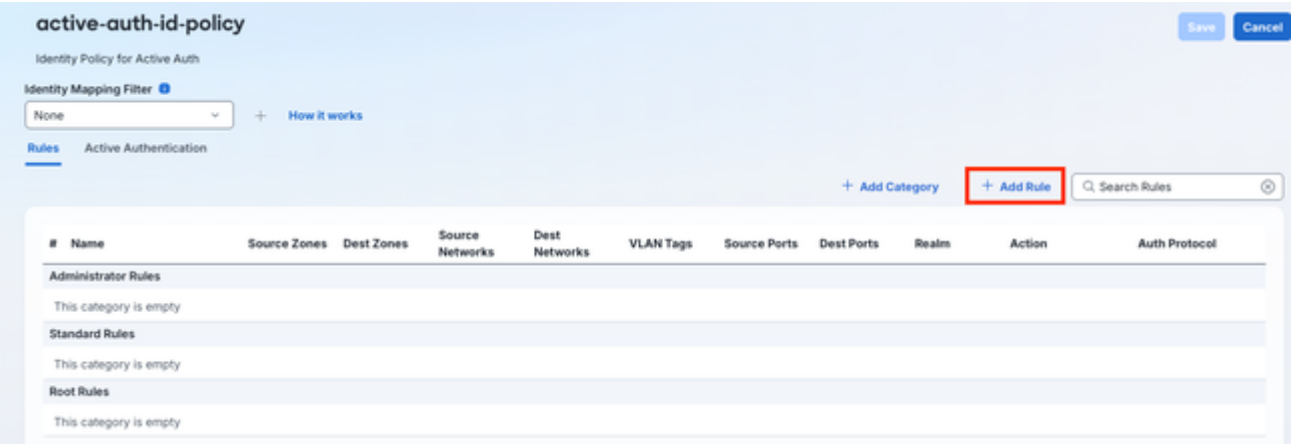
添加新身份策略配置

3)为新的身份策略分配名称和说明 (如果适用)。Click Save.

命名新身份策略

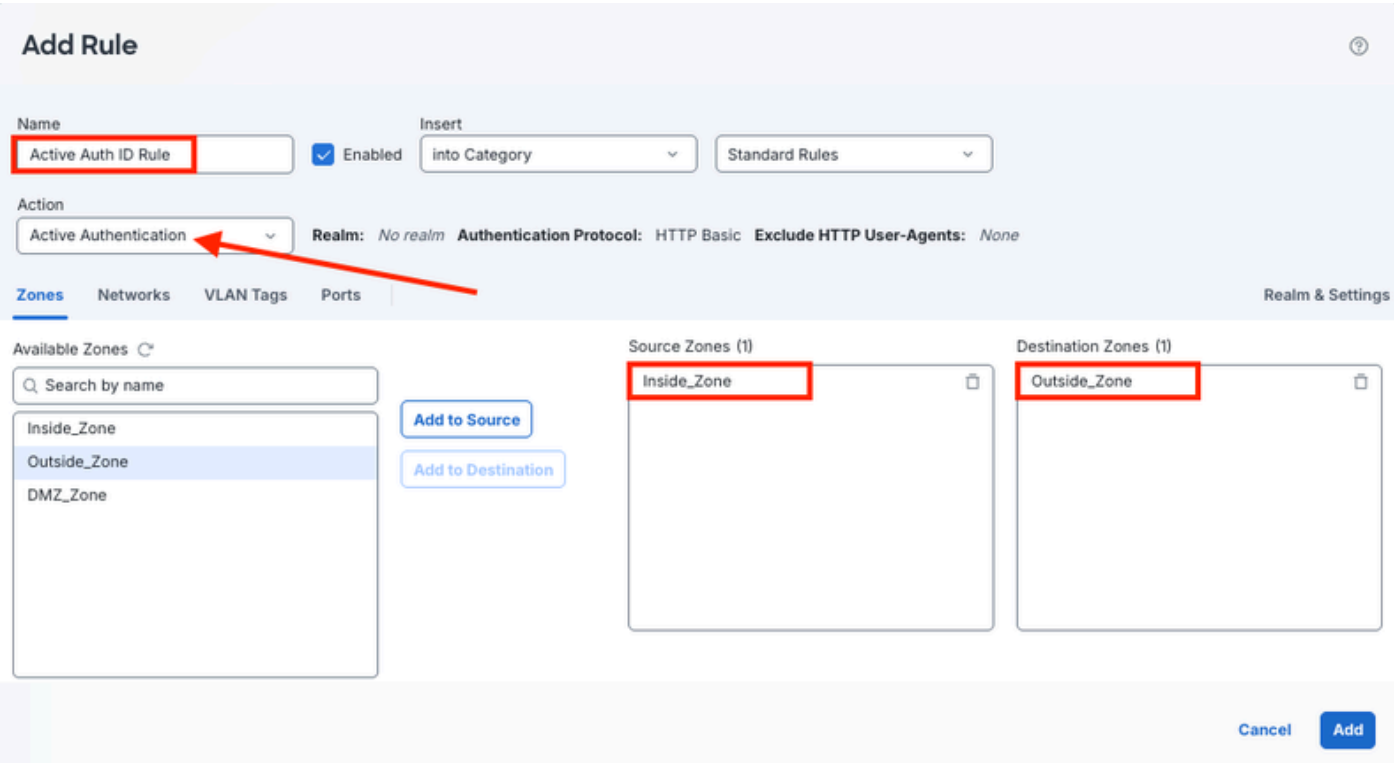
步骤 4：配置身份策略规则

1)通过点击+添加规则(Add Rule)添加新规则。



添加新身份策略规则

2)为新规则命名名称，从Action下拉列表中选择Active Authentication，并缩小与规则匹配才能执行Active Authentication的特定区域/网络。



配置主动身份验证规则设置

3)单击Add之前，请在规则编辑器内单击Realm and Settings选项卡。确认在前面的步骤中配置的领域被选为身份验证领域，然后单击添加。

Add Rule

Name: Active Auth ID Rule ☒ Enabled Insert: into Category Standard Rules

Action: Active Authentication **Realm:** azure-entra-saml (S... **Authentication Protocol:** SAML **Exclude HTTP User-Agents:** None

Zones Networks VLAN Tags Ports [Realm & Settings](#)

Authentication Realm *
azure-entra-saml (SAML)

☐ Use passive identity if available.
Active identity realm is going to be used as a passive identity realm.

Authentication Protocol
SAML

▶ HTTP User Agent Exclusions

Cancel Add

配置身份规则的领域和设置

4)添加并配置规则。Click Save.

active-auth-id-policy

Identity Policy for Active Auth

Identity Mapping Filter: None [How it works](#)

[Rules](#) Active Authentication

[+ Add Category](#) [+ Add Rule](#)

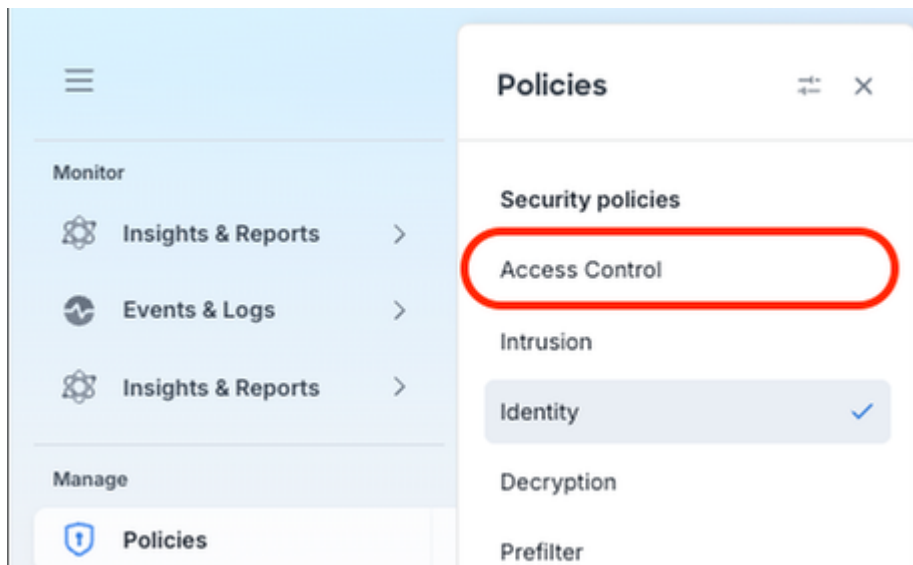
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	Active Auth ID Rule	Inside_Zone (Ro	Outside_Zone (f	any	any	any	any	any	azure-entra-san	Active Authentication	SAML
Root Rules											
This category is empty											

You have unsaved changes [Save](#) [Cancel](#)

保存身份策略规则配置

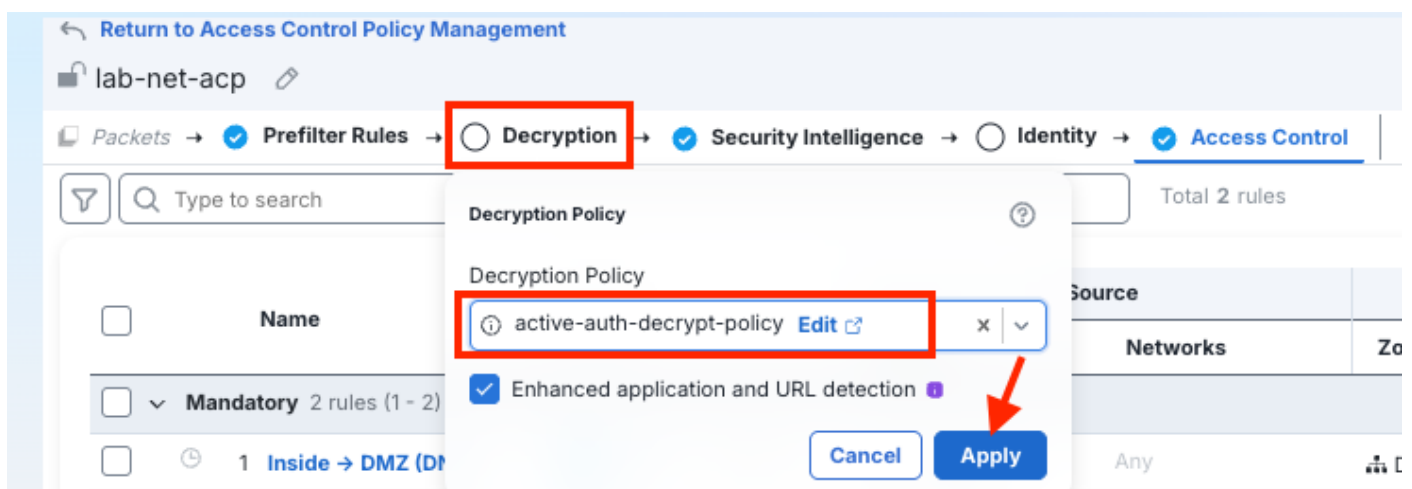
步骤 5：配置访问控制策略

1)选择Policies > Security Policies > Access Control，然后点击FTD分配到的Access Control Policy。



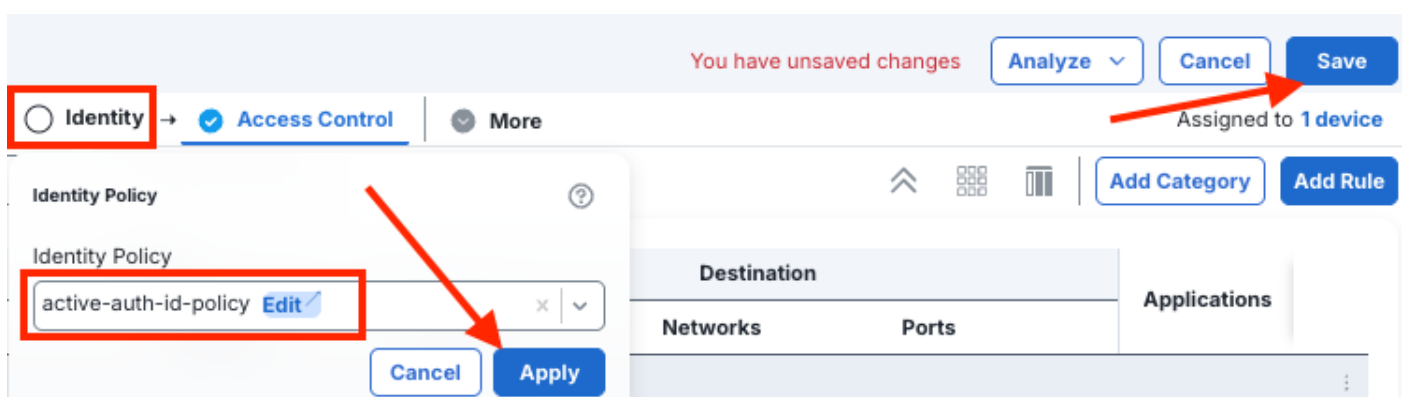
访问控制策略配置

2)确认之前步骤中配置的解密策略已应用于访问控制策略。



将解密策略应用于访问控制

3)确认之前步骤中配置的身份策略也应用于访问控制策略。保存策略更改。



将身份策略应用于访问控制

4)确认存在允许客户端数据平面流量在成功进行主动身份验证后通过安全防火墙的规则。此处显示的示例使用给定实验环境的较宽规则集。

☐	Name	Action	Source		Destination			Applications
			Zones	Networks	Zones	Networks	Ports	
☐ Mandatory 2 rules (1 - 2)								
☐	1 Inside → DMZ (DNS)	Allow	Inside_Zone	Any	DMZ_Zone	Any	Application Default	DNS
☐	2 DMZ-Inside → Outside	Allow	DMZ_Zone Inside_Zone	Any	Outside_Zone	Any	Any	Any
☐ Default (No rules)								

用户数据平面流量规则集

步骤 6：将配置部署到思科安全防火墙设备

部署后，发送流量的客户端将通过Microsoft登录网页进行提示，以使用Azure Entra执行主动身份验证。

有关此处记录的进程的其他上下文，请参阅[创建用于主动身份验证（强制网络门户）的Microsoft Azure AD\(SAML\)领域 — 章节：FMC设备配置指南10.x中的领域。](#)

验证

使用此部分可帮助确认配置是否正常工作。

GUI

验证FMC中的用户会话和活动：

- 选择Integrations > Users > Active Sessions。

Cloud-delivered Firewall Management Center									
Integrations / Users / Active Sessions									
Showing the 1 and only session									
Login Time	Realm/Username	Last Seen ↓	Authentication Type	Current IP	Session Duration	Realm	Username		
2026-10-07 02:10:02	azure-entra-saml/captive-pc	2026-10-07 02:10:02	Active Authentication		1 min 40 sec	azure-entra-saml	captive-portal-user		

FMC活动会话输出

- 选择Integrations > Users > User Activity。

Time	Username	Event	Realm	Discovery Application	Authentication Type	IP Address	Start Port
2026-10-07 02:10:02	captive-portal-user	User Login	azure-entra-saml	Microsoft Azure	Active Authentication		
2026-10-07 02:10:01	captive-portal-user	User Login	azure-entra-saml	Microsoft Azure	Active Authentication		

FMC用户活动输出

在Azure上，导航到Microsoft Entra管理中心：

- 过滤企业应用，搜索/单击适用的应用。

Microsoft Entra admin center

Home > Enterprise applications

Enterprise applications | All applications

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Private Network connectors
- User settings
- App launchers
- Custom authentication extensions

Security

- Conditional Access
- Consent and permissions
- Application policies

Search resources, services

Search: captive-

Name	Obj
Captive-Auth...	efda

Azure Entra管理中心企业应用导航

- 选择活动>登录日志。

Home > Enterprise applications | All applications > Captive-Auth-SAML



Captive-Auth-SAML | Sign-in logs

Enterprise Application

«

Download

Export data Settings

Troubleshoot

Refresh

Manage view

Got feedback?

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Want to switch back to the legacy signin logs experience? Click here to leave the preview.

Add filter

Show dates as: UTC

Date range: 10/7/2026 - 10/7/2026

Application contains

User sign-ins (interactive)

User sign-ins (non-interactive)

Service principal sign-ins

Managed identity sign-ins

Date ↓	Request ID	User principal name	Application	Status
2026-10-07T06:10:02Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:00Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:59Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:58Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:52Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:51Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:29Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted

Azure企业应用程序登录活动日志

CLI

- 在FTD CLI中，您可以查看与SAML和强制网络门户响应相关的统计信息：

<#root>

>

debug menu captive-portal 6

```
SAML passed requests captive-portal 14
SAML failed requests captive-portal 0
SAML passed responses captive-portal 4
SAML failed responses captive-portal 0
Total captive-portal bee-client messages processed 4
Total captive-portal bee-client messages successful 4
Total captive-portal bee-client messages failed 0
Total bee-client reconnects 0
```

故障排除

强制网络门户调试

- `system support captive-portal-debug`命令可用于FTD。输出显示如何启用调试，并记录输出的关键数据段，以帮助了解强制网络门户流量。

```
<#root>
```

```
>
```

```
system support captive-portal-debug
```

```
Enable firewall-debug too? [n]:
```

```
y
```

```
Enable identity-debug too? [n]:
```

```
y
```

```
Please specify an IP protocol:
```

```
tcp
```

```
Please specify a client IP address:
```

```
192.168.20.200
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Enable daq-debug too? (WARNING: current packet debug configs and logs will be overwritten) [n]:
```

```
Monitoring captive_portal and firewall and identity debug messages
```

```
!---
```

```
Baseline output pending user Captive Portal authentication
```

```
...
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 match rule order 1, id 1 action Captive por
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 didn't find active binding, initiating capt
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 captive portal authentication started
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 defer trust until captive portal redirect i
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 Current state = S_INIT, Event = EVT_CP_RULE
```

```
...
```

```
!---
```

```
Captive Portal probe intercepted and redirected to SAML IdP (generate_204)
```

```

...
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 AppID session with service_id: 676, url: http
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 Current state = S_PENDING_USER, Event = EVT_
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 app event changes: service, client, host, ur
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 using ipv4 address 192.168.20.1 for redirect
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 encrypted redirect url: https://ftd-inside.e
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 Current state = S_REDIRECTING, Event = EVT_F
...
!---

```

SAML authentication completes, identity binding created

```

...
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 looked for user_id with realm_id 2 auth_type
192.168.20.200 54023 -> 198.51.100.280 6 AS=0 ID=2 GR=1-1 found active binding for user_id 0 usernames
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 IdentityFlowSetupEventHandler Retrieved iden
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 New firewall session
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 allow action
...
!---

```

Authenticated binding persists across subsequent, unrelated destinations (no further redirects)

```

...
192.168.20.200 54024 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 found active binding for user_id 0 usernames
192.168.20.200 54025 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 54026 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 54027 -> 198.51.100.3 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 19935 -> 198.51.100.4 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
...

```

用户身份转储

- 要获取FTD上当前用户身份状态数据的快照，请在FTD CLI上运行system support firewall-engine-dump-user-identity-data命令：

```
> system support firewall-engine-dump-user-identity-data
```

```
Successfully commanded snort.
```

```
>
```

- 在expert模式的CLI中，使用FTD设备的本地管理员凭证登录时，在
/ngfw/var/sf/user_enforcement/user_identity.dump中查看转储文件的内容

```
<#root>
```

```
>
```

```
expert
```

```
admin@ftd:~$
```

```
sudo su
```

```
Password:
```

```
root@ftd:/home/admin#
```

```
root@ftd:/home/admin#
```

```
ls -lah /ngfw/var/sf/user_enforcement/user_identity.dump
```

```
-rw----- 1 root root 5.6K Oct  7 07:51 /ngfw/var/sf/user_enforcement/user_identity.dump
```

```
root@ftd:/home/admin#
```

```
root@ftd:/home/admin#
```

```
less /ngfw/var/sf/user_enforcement/user_identity.dump
```

```
...
```

```
-----  
IP:USER  
-----
```

```
!--- Host IP is aligned with the user authenticated via Captive Portal/Active Authentication  
-----
```

```
Host ::ffff:192.168.20.200  
-----
```

```
::ffff:192.168.20.200:0 realm 2 type 8, username azure-entra-saml\captive-portal-user@onmicrosoft.examp
```

```
::ffff:192.168.20.200: SXP initialized 0 sgt 0
```

```
ABP values: None
```

```
-----  
SXP MAPPING:  
-----
```

```
...
```

可能的问题

强制网络门户未知证书颁发机构

问题：尝试进行身份验证时，客户端浏览器返回未知的颁发者错误。

可能的原因:在客户端浏览器中，内部证书颁发机构不受信任。

解决方案：确认浏览器中信任CA。此处显示的示例确认内部CA证书是受信任的。

强制网络门户“找不到服务器”

问题：当客户端浏览器尝试加载强制网络门户时，它会针对基本URL返回“Server Not Found”，同时尝试访问基本URL或类似地址。

可能的原因:DNS可达性或DNS配置错误。

解决方案：确认客户端配置了用于解析A记录的相应DNS服务器。确认服务器具有映射到FQDN的A记录，并且服务器可访问并响应。

相关信息

- [创建用于主动身份验证（强制网络门户）的Microsoft Azure AD\(SAML\)领域 — FMC设备配置指南10.x](#)
- [Azure Event Hub文档](#)
- [技术支持和文档 - Cisco Systems](#)

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）。