

Configurar o Portal do Azure Entra Captive no Firewall Seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama](#)

[Portal cativo entre endpoint, FTD e Azure Entra](#)

[Configurar](#)

[Fase 1: Configuração inicial do FMC e do DNS](#)

[Passo 1: Ativar o Cisco Dynamic Attributes Connector \(CSDAC\)](#)

[Passo 2: Crie um representante de objeto de rede de nome de domínio totalmente qualificado da interface de ingresso do FTD](#)

[Passo 3: Configurar o registro DNS A](#)

[Fase 2: Configuração da infraestrutura de chave pública](#)

[Passo 1: Importar o Certificado de CA Interno para o FMC](#)

[Passo 2: Assinar o certificado do provedor de serviços com a autoridade de certificação](#)

[Passo 3: Implantar o Certificado SP no FTD](#)

[Fase 3: Configuração do Azure](#)

[Passo 1: Criar o Aplicativo do Entra Enterprise para o Kit de Ferramentas SAML](#)

[Passo 2: Configurar registros do aplicativo de ID do Entra](#)

[Etapa 3. Configurar as permissões de API do Microsoft Graph para o registro do aplicativo.](#)

[Passo 4: Configurar o Namespace do Hub de Eventos \(EH\)](#)

[Passo 5: Escolha ou Crie Políticas de Acesso Compartilhado no Namespace do Hub de Eventos](#)

[Passo 6: Coletar e Anotar Informações de Assinatura de Acesso Compartilhado \(SAS\) do Namespace EH](#)

[Passo 7: Criar uma Instância do Hub de Eventos no Namespace do Hub de Eventos](#)

[Passo 8: Criar um Grupo de Consumidores de Instâncias do Hub de Eventos no Namespace do Hub de Eventos](#)

[Etapa 9: Verificar Valores Coletados](#)

[Etapa 10: Configurar o Streaming de Log de Auditoria do Entra ID para o Hub de Eventos](#)

[Fase 4: Consolidar a Configuração de Autenticação Ativa do Azure e do FMC/FTD](#)

[Passo 1: Configurar o Domínio SAML/Entra ID do Azure Usando o Assistente do FMC](#)

[Passo 2: Implementar os Metadados de SP SAML configurados pelo FMC no Aplicativo Azure Enterprise](#)

[Passo 3: Configurar o Domínio SAML/Entra ID do Azure Usando o Assistente do FMC \(Continuação\)](#)

[Passo 4: Verificar Usuários Baixados](#)

[Fase 5: Configurar políticas no FMC](#)

[Passo 1: Configurar Política de Criptografia](#)

[Passo 2: Configurar Regras de Política de Criptografia](#)

[Passo 3: Criar política de identidade](#)

[Passo 4: Configurar Regras de Política de Identidade](#)

[Passo 5: Configurar a Política de Controle de Acesso](#)

[Verificar](#)

[GUI](#)

[CLI](#)

[Troubleshooting](#)

[Depuração do portal cativo](#)

[Despejo de Identidade de Usuário](#)

[Possíveis problemas](#)

[Autoridade de Certificação Desconhecida do Portal Cativo](#)

[Portal cativo "Servidor não encontrado"](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração da ID do Microsoft Azure Entra para uso com o portal cativo (autenticação ativa) no Cisco Secure Firewall.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- SAML (Security Assertion Markup Language, Linguagem de marcação de asserção de segurança)
- Microsoft Azure
- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Secure Firewall

Você deve ter o tipo de preço Padrão disponível no Azure para a criação do Hub de Eventos. Além disso, os dispositivos devem ser ativados com o Smart Licensing habilitado com a funcionalidade de exportação controlada.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure FTD versão 10.0
- Cisco Secure FMC versão 10.0

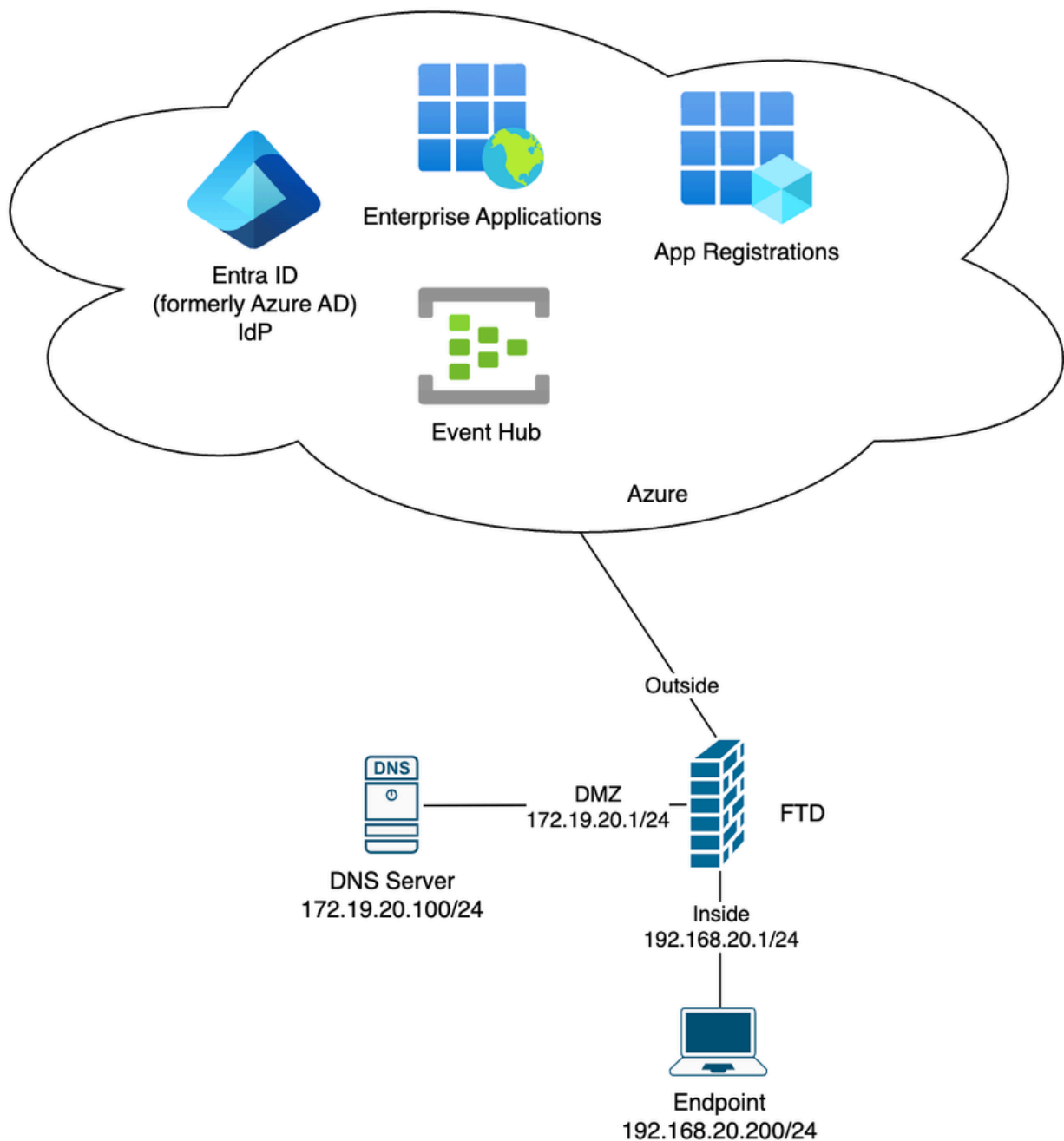
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Informações de Apoio

Como as arquiteturas de segurança tradicionais baseadas em IP lutam para acompanhar o ritmo dos ambientes de trabalho dinâmicos e híbridos, a autenticação ativa do Cisco Secure Firewall com integração SAML oferece uma solução robusta e centrada em identidade. Aproveitando o Microsoft Entra ID (Azure AD) como um provedor de identidade centralizado, essa configuração permite que os administradores vão além das regras de rede estática e apliquem controle de acesso granular com base na identidade do usuário verificada, em vez de endereços de rede voláteis. Essa integração otimiza a experiência do usuário por meio de Logon Único (SSO) e Autenticação Multifator (MFA) obrigatórios, ao mesmo tempo em que garante uma postura de segurança unificada que mantém visibilidade estrita e aplicação de políticas em uma rede sem perímetro.

Diagrama

Portal cativo entre endpoint, FTD e Azure Entra



Portal Cativo Entre EndPoint E Azure Entra

Configurar

Fase 1: Configuração inicial do FMC e do DNS

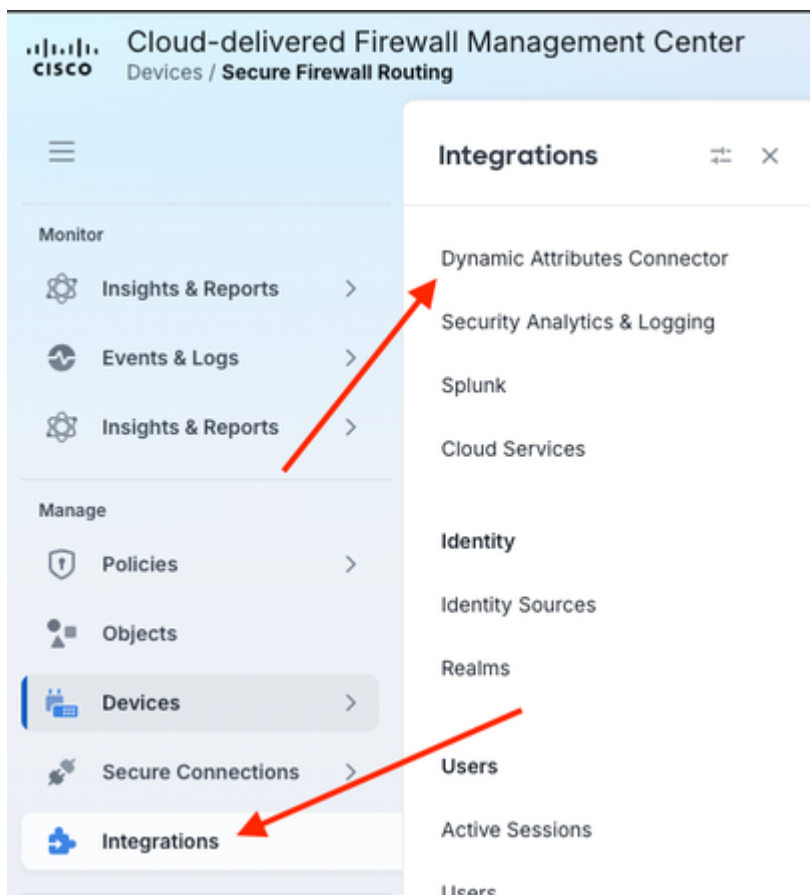


Note: Este laboratório usa o Centro de Gerenciamento de Firewall (cdFMC - Firewall Management Center) fornecido em nuvem; no entanto, as etapas continuam a ser as

mesmas para o CVP local.

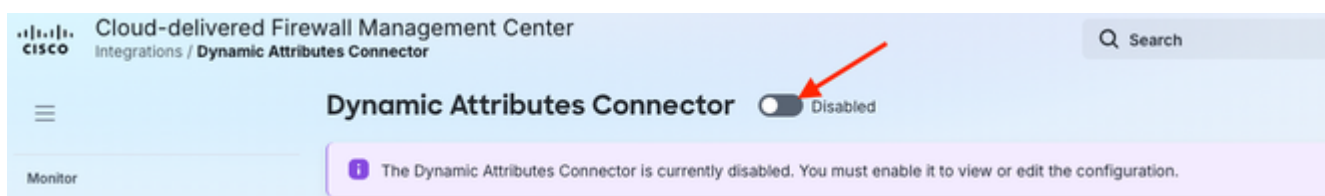
Passo 1: Ativar o Cisco Dynamic Attributes Connector (CSDAC)

1) Escolha Integrations > Dynamic Attributes Connector.



Escolher Conector de Atributos Dinâmicos de Integrações

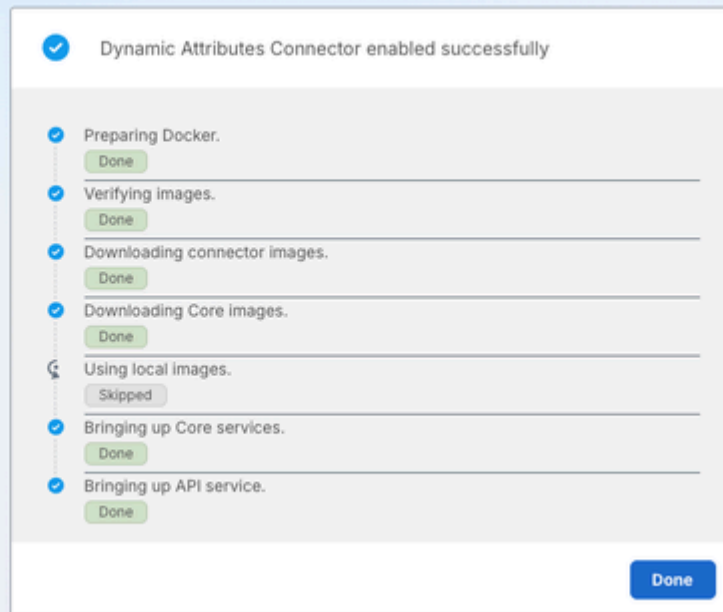
2) Clique no controle adjacente à string Disabled para ativar o CSDAC.



Ativar Conector de Atributos Dinâmicos Cisco

c) Clique em Concluído quando a ativação do CSDAC for concluída.

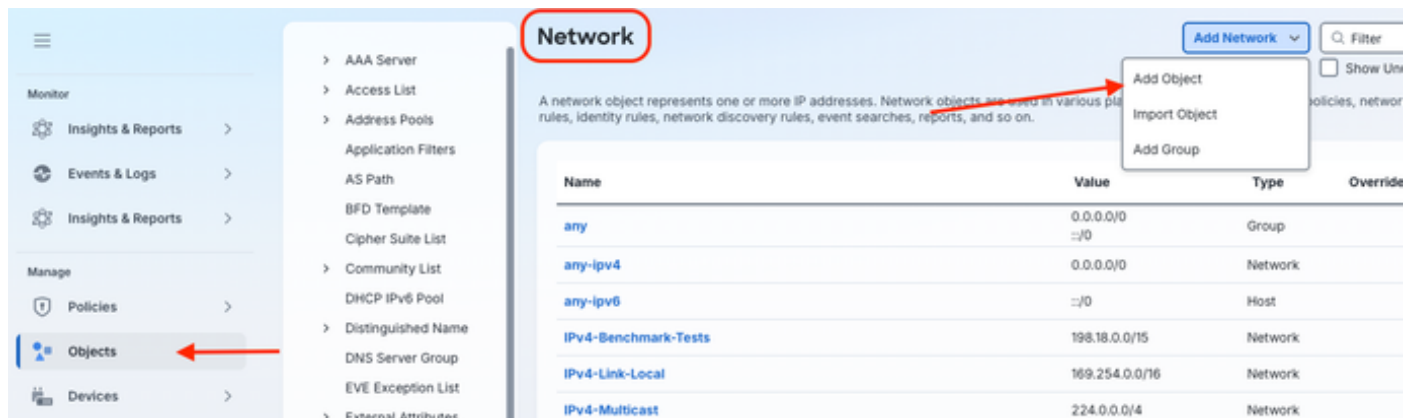
Dynamic Attributes Connector



Habilitar Status do Conector de Atributos Dinâmicos Cisco

Passo 2: Crie um representante de objeto de rede de nome de domínio totalmente qualificado da interface de ingresso do FTD

1) Escolha Objetos > Adicionar rede > Adicionar objeto.



Criar novo objeto de rede de nome de domínio totalmente qualificado

2) Nomeie o Objeto de Rede configurado com o Nome de Domínio Totalmente Qualificado (FQDN). Insira o FQDN e atribua o objeto de rede como um tipo de FQDN clicando no botão de opção apropriado. 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

Configurar Variáveis de Objeto de Rede FQDN

Passo 3: Configurar o registro DNS A

1) O exemplo mostrado aqui usa o Windows Server 2025; consulte a documentação do servidor de resolução de nomes específico conforme necessário.

	Name	Type	Data
	(same as parent folder)	Start of Authority (SOA)	[1], dc., hostmaster.
	(same as parent folder)	Name Server (NS)	dc.
	ftd-inside	Host (A)	192.168.20.1



Note: O cliente que executa a Autenticação Ativa deve ser capaz de resolver esse registro DNS A.

Fase 2: Configuração da infraestrutura de chave pública

Uma CA (Autoridade de Certificação) interna pode ser usada como PKI (Infraestrutura de Chave Pública) para a configuração de Autenticação Ativa. O FMC e o FTD da Cisco exigem que a chave pública da CA interna e a chave privada emparelhada sejam carregadas como um objeto de CA interna para executar as operações necessárias de interceptação SSL e Descriptografia-Renúncia. Além disso, a CA interna deve ser confiável no navegador do cliente a partir do qual a Autenticação Ativa é executada. Consulte a documentação do navegador do cliente para verificar como confirmar se o navegador confia no certificado.

Passo 1: Importar o Certificado de CA Interno para o FMC

1) Selecione Objects > PKI > Internal CAs. Clique em Importar CA.



Note: A CA interna também pode ser criada diretamente no FMC.

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:



Note: No conteúdo deste documento, aparece um espaço em branco cobrindo os vários valores de campo nas imagens e é intencional de acordo com a publicação deste documento. Os valores reais são refletidos para seu ambiente à medida que você configura.

Passo 2: Assinar o certificado do provedor de serviços com a autoridade de certificação

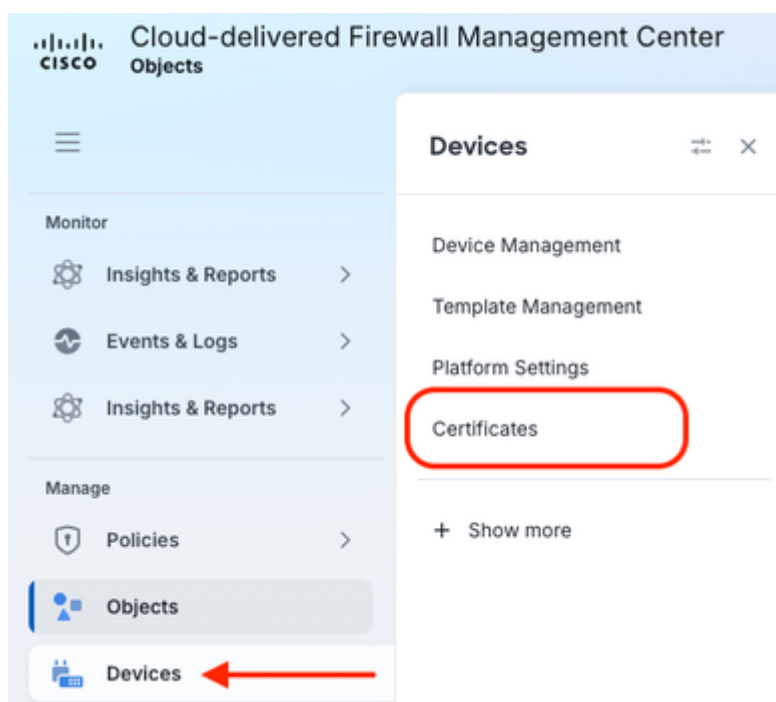
1) O certificado do provedor de serviços (SP) deve ser assinado por uma autoridade de certificação (CA) confiável e retornado em um formato PKCS#12 (.p12).



Note: Esta CA pode ser assinada internamente. A única advertência é que a CA interna deve ser confiável pelo dispositivo cliente.

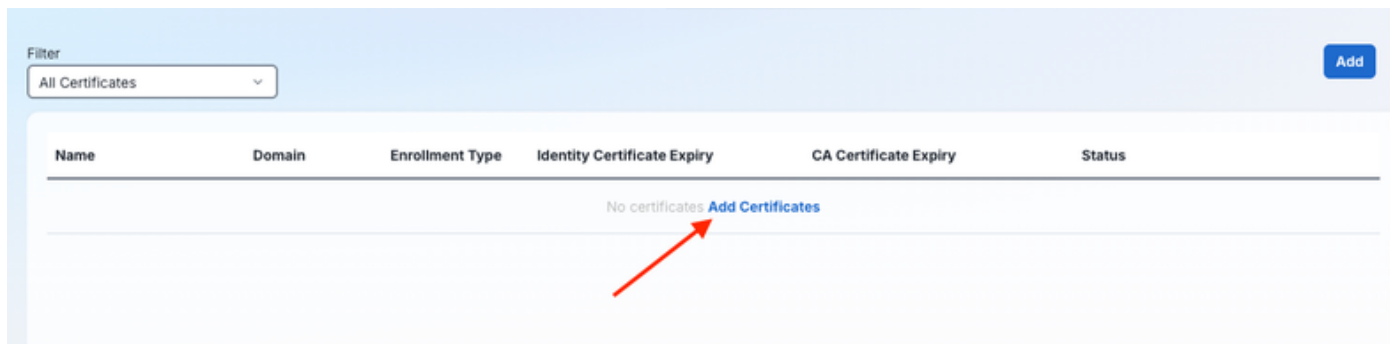
Passo 3: Implantar o Certificado SP no FTD

1) Selecione Devices > Certificates.



Navegue Até Dispositivos E Certificados

2) Clique em Add Certificates.



Adicionar novo certificado do dispositivo

3) Clique no dispositivo na lista suspensa que executa a Autenticação ativa e, em seguida, clique no ícone + para criar um novo Registro de certificado.

A screenshot of the "Add New Certificate" form. The form has a title "Add New Certificate" and a help icon. Below the title, there is 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*" and "Certificate Enrollment*". The "Device*" dropdown is set to "FTD". A red arrow points to the "FTD" option. To the right of the "Certificate Enrollment*" dropdown is a "+" icon, which is also pointed to by a red arrow. At the bottom right, there are two buttons: "Cancel" and "Add".

Selecione FTD E Adicione Adicionar Nova Inscrição De Certificado

4) Nomeie o Registro de certificado e, na lista suspensa Tipo de registro, escolha o arquivo PKCS12.

Add Certificate Enrollment

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:*

Challenge Password:

Confirm Password:

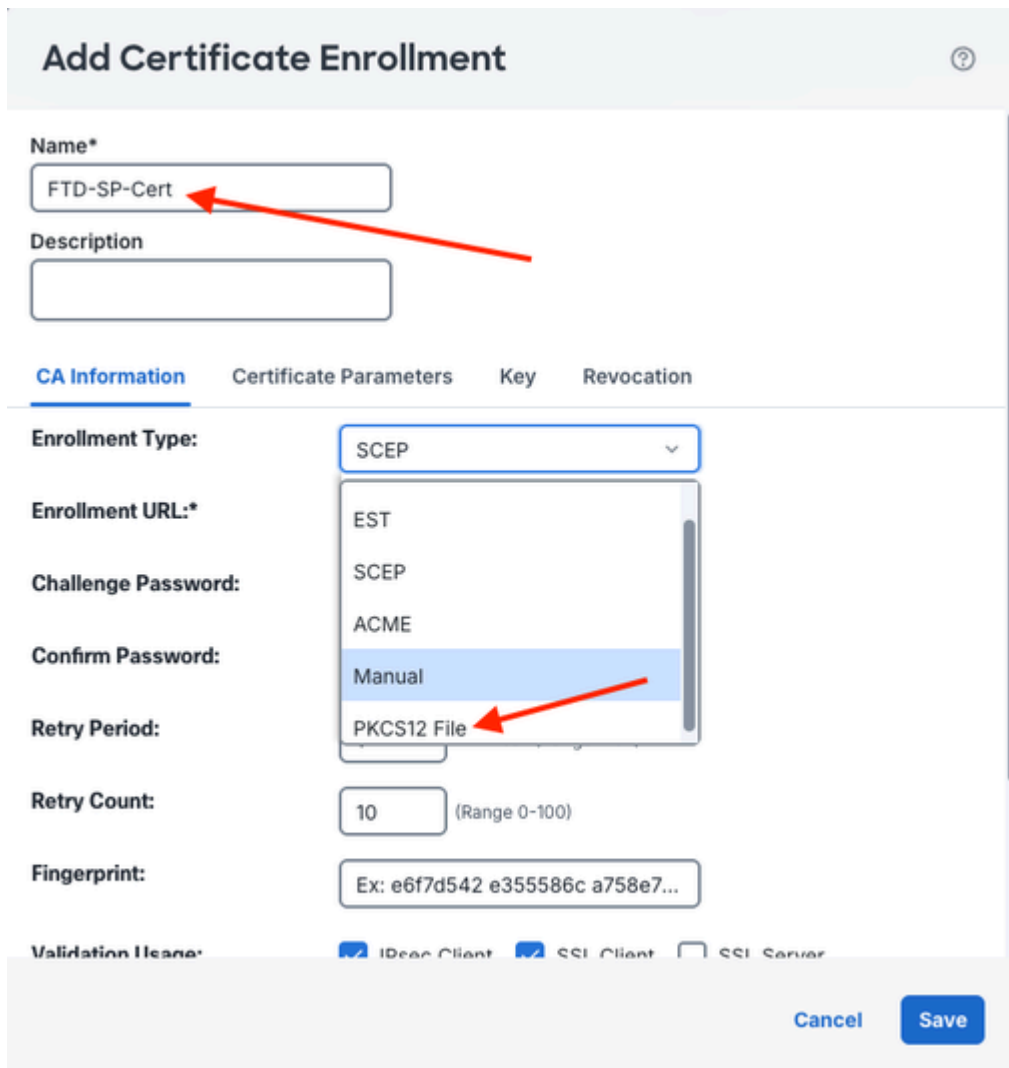
Retry Period:

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7...

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

Cancel Save



Tipo E Configurações De Registro De Certificado

5) Importe o arquivo PKCS#12 clicando em Browse PKCS12 File e insira a senha necessária. 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**

Procurar e importar o arquivo PKCS12

6) Confirme se os detalhes da inscrição estão corretos e clique em Adicionar.

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 +

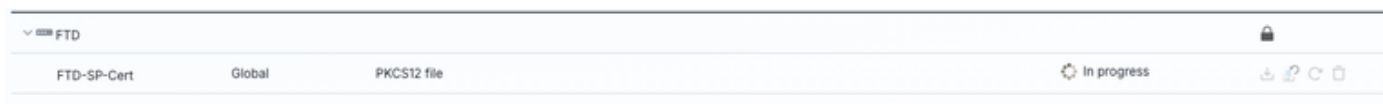
Certificate Enrollment Details:

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

Cancel **Add**

Confirmar detalhes da inscrição de certificado

7) A importação reflete Em andamento.



FTD-SP-Cert	Global	PKCS12 file	In progress
-------------	--------	-------------	-------------

Quando a importação for concluída, as informações do certificado SP poderão ser validadas clicando no ícone ID do certificado configurado.



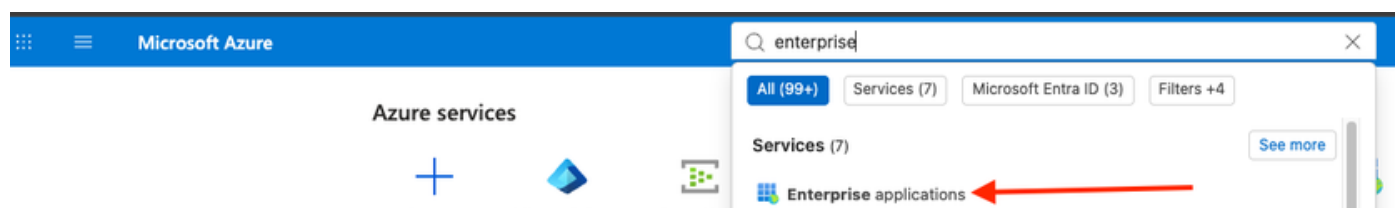
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
FTD-SP-Cert	Global	PKCS12 file	Dec 18, 2028	Sep 12, 2036	 

Status de Importação de Certificado em Andamento

Fase 3: Configuração do Azure

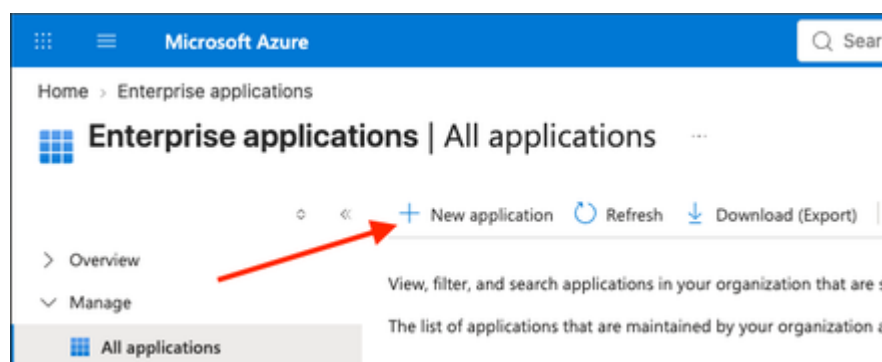
Passo 1: Criar o Aplicativo do Entra Enterprise para o Kit de Ferramentas SAML

1) Procure e clique em Enterprise Applications.



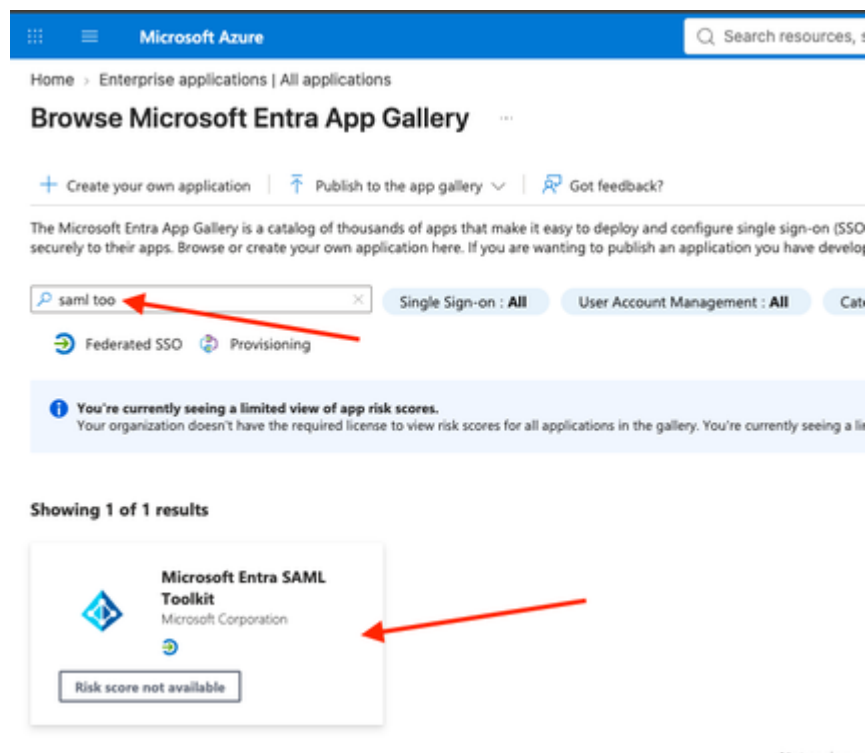
Pesquisar E Acessar Aplicativos Corporativos

2) Clique em + Novo aplicativo.



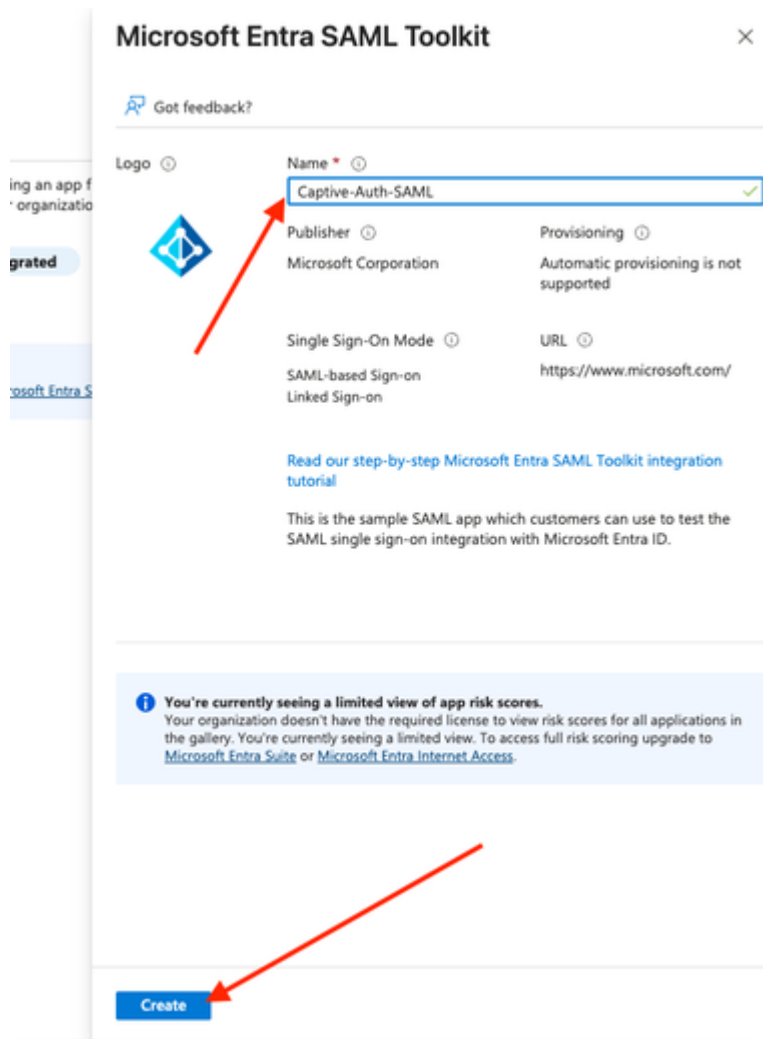
Selecionar Novo Aplicativo Nos Aplicativos Corporativos

3) Procure o Microsoft Entra SAML Toolkit e clique na miniatura dele.



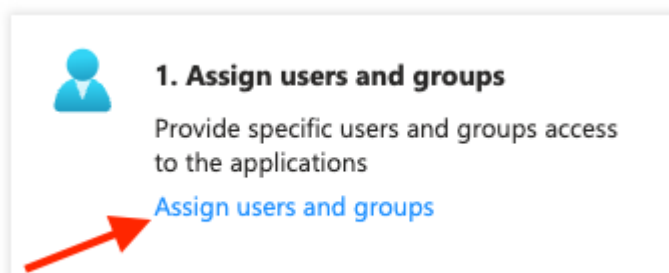
Pesquisar e Selecionar o Kit de Ferramentas Microsoft Entra SAML

4) Atribua um Nome ao Aplicativo Empresarial Microsoft Entra SAML Toolkit e clique em Criar.
(Referência da Microsoft: [Leia nosso tutorial de integração passo a passo do Microsoft Entra SAML Toolkit](#)).



Atribuir nome ao aplicativo Toolkit SAML

5) Na página Visão geral, atribua os usuários e grupos específicos à aplicação SAML Toolkit Enterprise. Neste exemplo, a conta de teste (ctive-portal-user) é um membro do grupo ative-auth-lab.

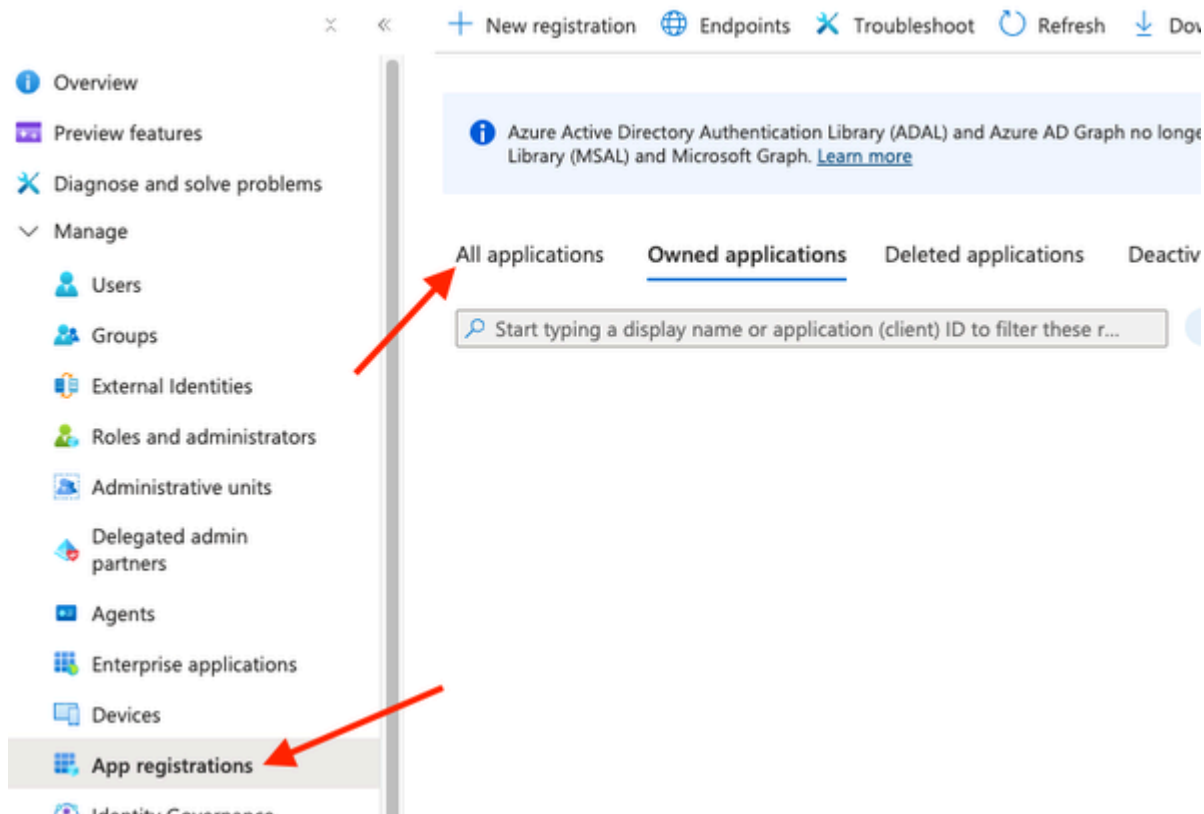


Atribuir Usuários E Grupos Ao Aplicativo

6) A configuração deste aplicativo empresarial continua nas etapas posteriores.

Passo 2: Configurar registros do aplicativo de ID do Entra

1) Navegue de volta para Entra ID e, no menu de navegação esquerdo, escolha Registros de aplicativo. Clique no filtro Todos os aplicativos e procure o nome fornecido ao aplicativo empresarial. Clique no aplicativo apropriado.



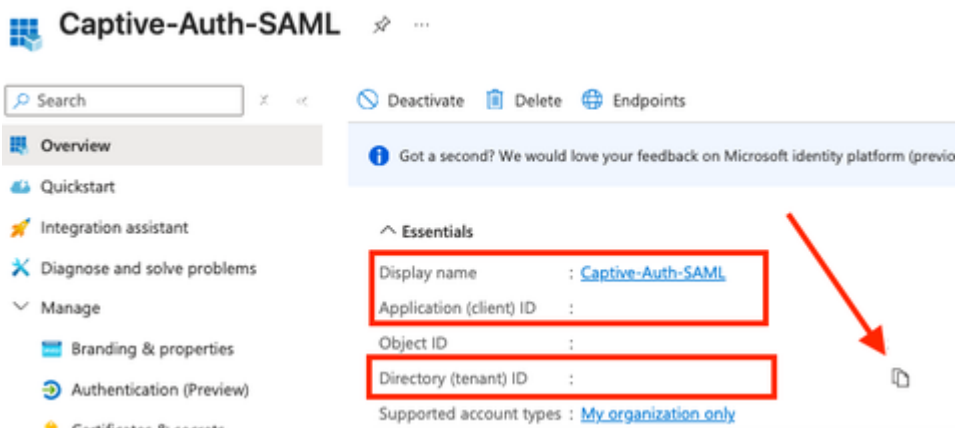
Navegue Até Registros De Aplicativo E Todos Os Aplicativos

2) Colete e anote os valores essenciais no Enterprise App Registration.



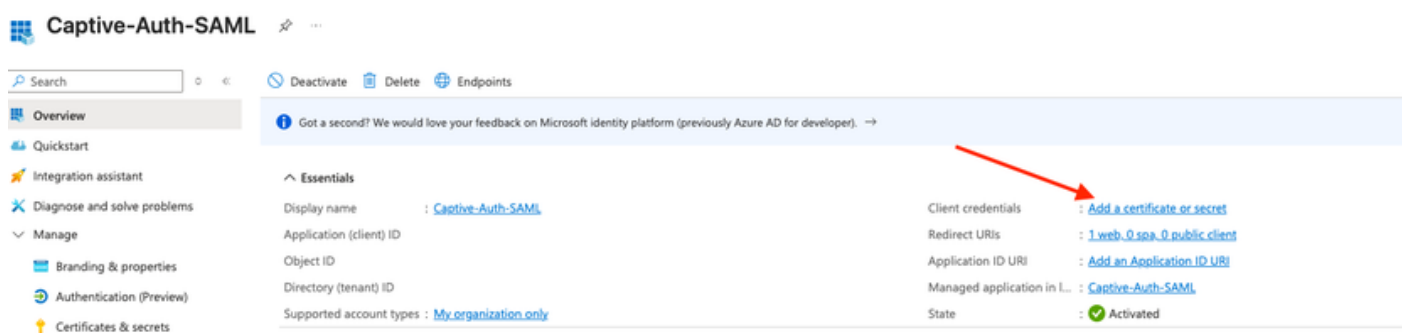
Importante: Passe o mouse sobre os valores para revelar Copiar para a área de transferência e coletar os valores em Essentials na página Visão geral:

- Nome de exibição
- ID do aplicativo (cliente)
- ID do Diretório (Locatário)



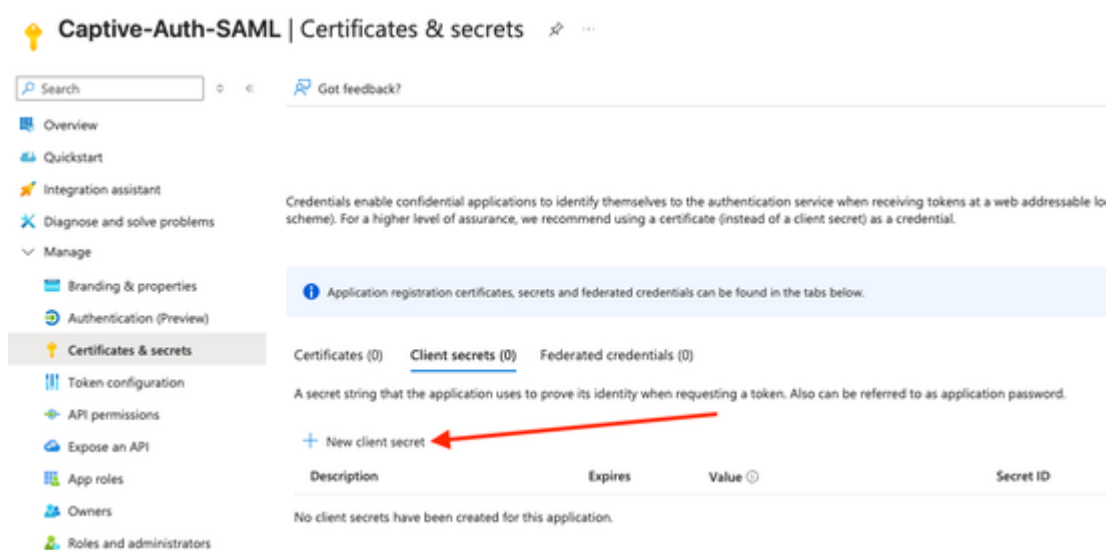
Coletar Valores De ID De Aplicativo E De Exibição E De Diretório

3) Clique no hiperlink Add a certificate or secret.



Adicionar Hiperlink De Certificado Ou Segredo

4) Clique em + Novo segredo do cliente.



Adicionar novo segredo do cliente

5) Forneça uma Descrição para o segredo e ajuste a expiração conforme necessário. Clique em

Add.

Add a client secret [X]

Description:

Expires: Recommended: 180 days (6 months) [v]

[Add] [Cancel]

Fornecer Descrição Do Segredo Do Cliente

6) Copie o segredo.



Importante: Anote o valor secreto copiado para a área de transferência.

Captive-Auth-SAML | Certificates & secrets [star] [menu]

Search [input] [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.

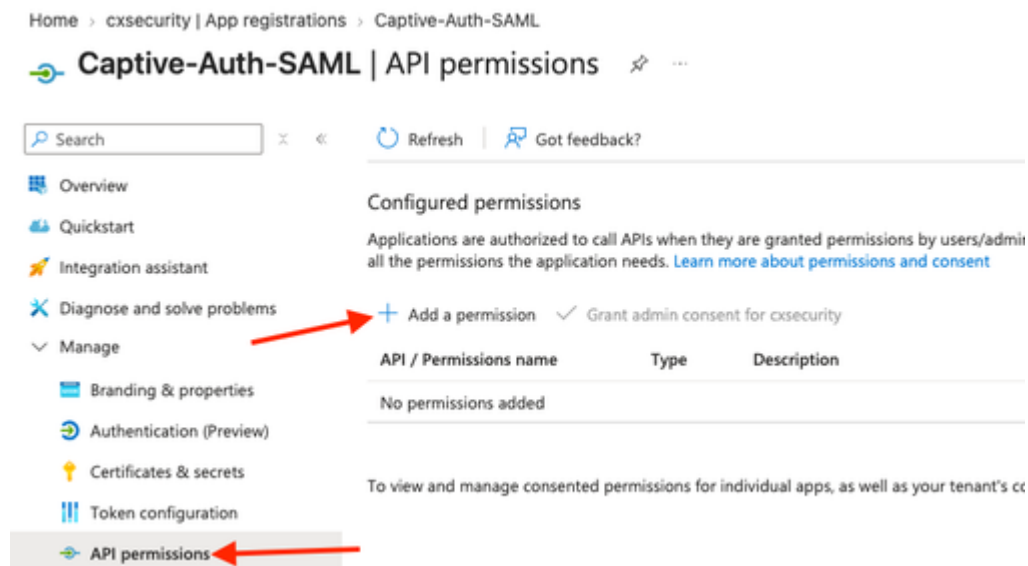
+ New client secret

Description	Expires	Value [i]	Secret ID
saml-secret	3/14/2027	[copy icon]	[copy icon]

Copiar valor do segredo do cliente

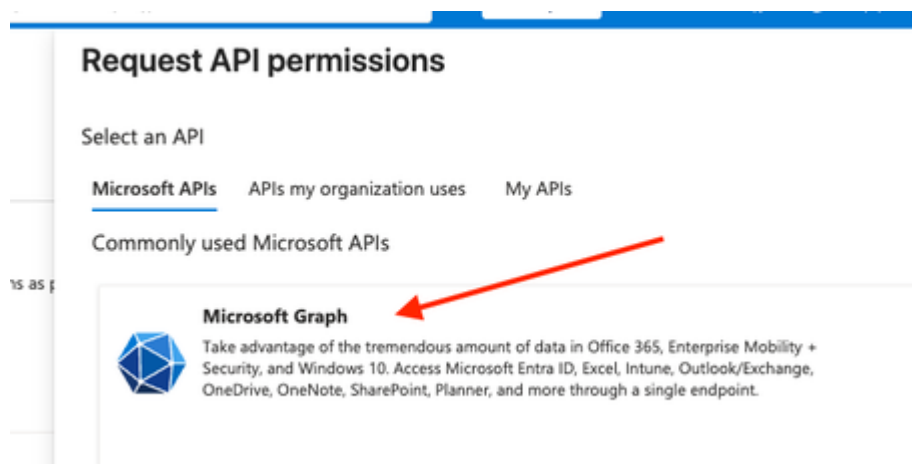
Etapa 3. Configurar as permissões de API do Microsoft Graph para o registro do aplicativo.

1) Escolha Permissões de API no menu de navegação esquerdo e clique em + Adicionar uma permissão.



Configurar Permissões de API

2) Clique em Microsoft Graph API.



Selecionar API do Microsoft Graph

3) Conceda permissões Delegated User.Read e clique em 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

Conceder Permissões de Leitura de Usuário Delegado

4) Conceder permissões User.Read.All do aplicativo (marque a caixa de seleção).

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

User.Read.All

Permission

Admin consent required

> IdentityRiskyUser

✓ User (1)

☒	User.Read.All ⓘ Read all users' full profiles	Yes
-------------------------------------	--	-----

Conceder ao Aplicativo Permissões Ler Tudo

5) Procure e marque a caixa de seleção Group.Read.All para conceder também permissões de Leitura do grupo. Clique em Adicionar permissões.

Select permissions

expand all

Group.Read.All

Permission

Admin consent required

✓ Group (1)

☒	Group.Read.All ⓘ Read all groups	Yes
-------------------------------------	-------------------------------------	-----

Add permissions Discard

Salvar Permissões de API

6) Confirme se as permissões configuradas estão alinhadas e conceda consentimento administrativo para elas.

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

Conceder Consentimento Administrativo Para Permissões

7) A saída, uma vez que o consentimento do administrador é concedido, é mostrada.

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

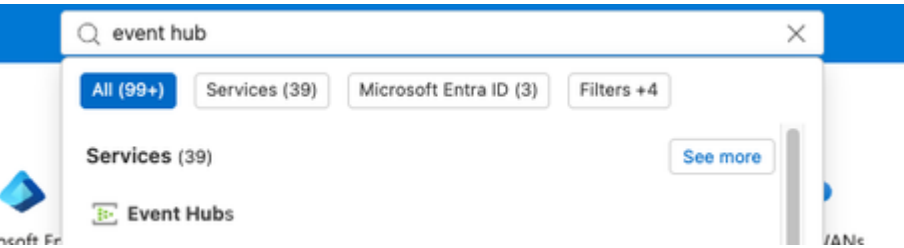
✓ Grant admin consent for

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

Saída de Consentimento Administrativo Concedido

Passo 4: Configurar o Namespace do Hub de Eventos (EH)

1) Procure e clique em Event Hubs.



Pesquisar Configuração do Hub de Eventos

2) Crie um novo namespace EH.



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.



[Learn more about Event Hubs](#)

Criar Namespace do Hub de Eventos

3) Configure o namespace EH.



Note: O tipo de preço Padrão ou superior deve ser escolhido. O tipo de preço básico impede o uso de realm.

Consulte a [Documentação do Hub de Eventos do Azure](#) para obter mais avaliações das Configurações Avançadas do Hub de Eventos e aplicabilidade a necessidades específicas.

Clique em Revisar + Criar.



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 >

Definir Configurações de Namespace do Hub de Eventos

4) Quando a validação for bem-sucedida, clique em Criar.

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 >](#)

Criar Implantação de Namespace do Hub de Eventos

5) Confirme se a implantação foi concluída e clique em Ir para o recurso.

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

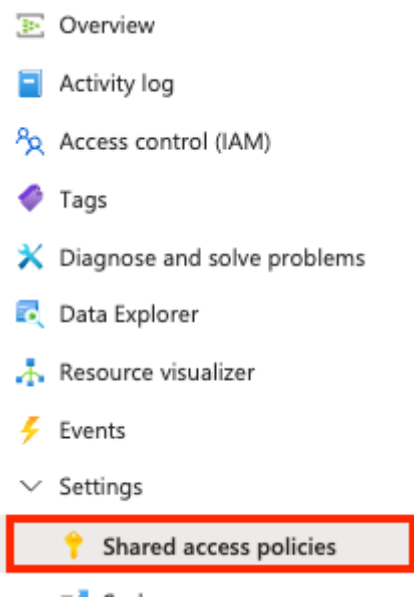
✓ Next steps

[Go to resource](#)

Ir para Recurso de Namespace do Hub de Eventos

Passo 5: Escolha ou Crie Políticas de Acesso Compartilhado no Namespace do Hub de Eventos

1) No menu de navegação à esquerda, escolha Settings > Shared access policies.



Navegue Até Shared Access Policies (Políticas De Acesso Compartilhado)

2) Clique em + Adicionar e insira o novo Nome da política e marque a caixa de seleção Gerenciar. Clique em Create na parte inferior do painel do menu Add SAS Policy.



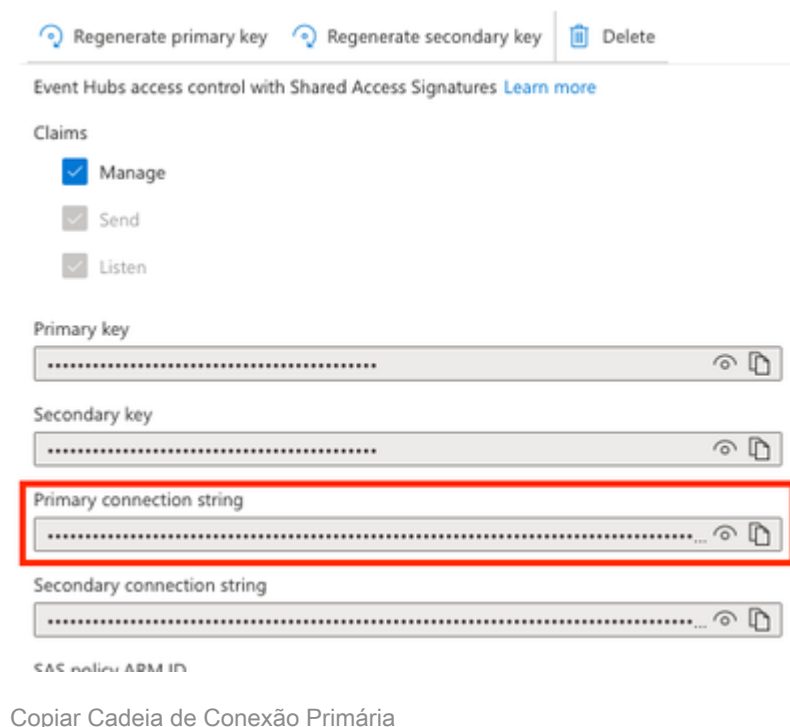
Adicionar nova política de acesso compartilhado



Criar política de acesso compartilhado

Passo 6: Coletar e Anotar Informações de Assinatura de Acesso Compartilhado (SAS) do Namespace EH

1) Clique na nova política de acesso compartilhado; a EH SAS Policy (Política de EH SAS) é exibida no painel lateral à direita.



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

SAS policy: ADP1 ID1

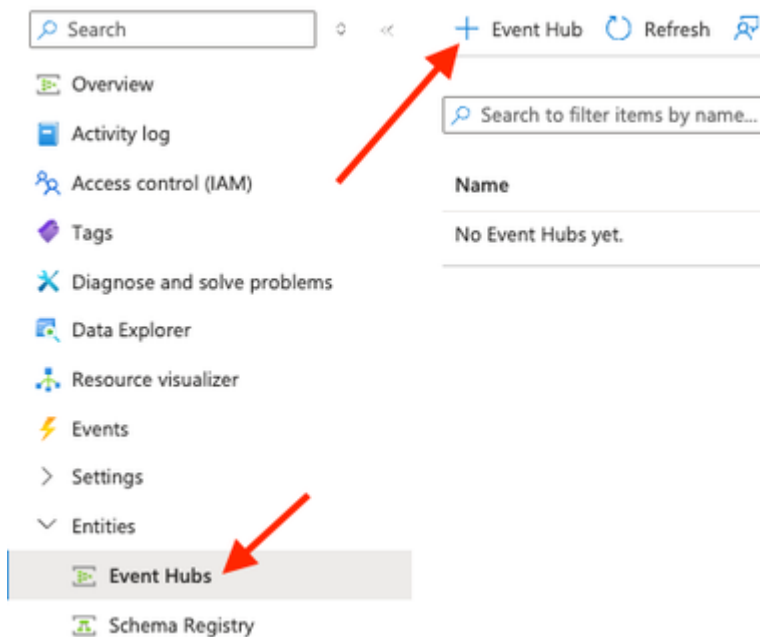
Copiar Cadeia de Conexão Primária



Importante: Copie e observe a cadeia de conexão Primária.

Passo 7: Criar uma Instância do Hub de Eventos no Namespace do Hub de Eventos

1) No menu Namespace, escolha Entidades > Hubs de Eventos. Clique em + Event Hub para criar uma nova instância de EH.



Criar Nova Instância do Hub de Eventos

2) Atribua um nome à nova instância de EH e clique em 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 * ⓘ ✓

Partition count ⓘ 1

Retention

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

Cleanup policy ⓘ

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

Review + create < Previous Next: Capture >

Atribuir Nome À Instância Do Hub De Eventos

3) Quando a validação for bem-sucedida, clique em Criar para provisionar a instância do Hub de Eventos.

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 >

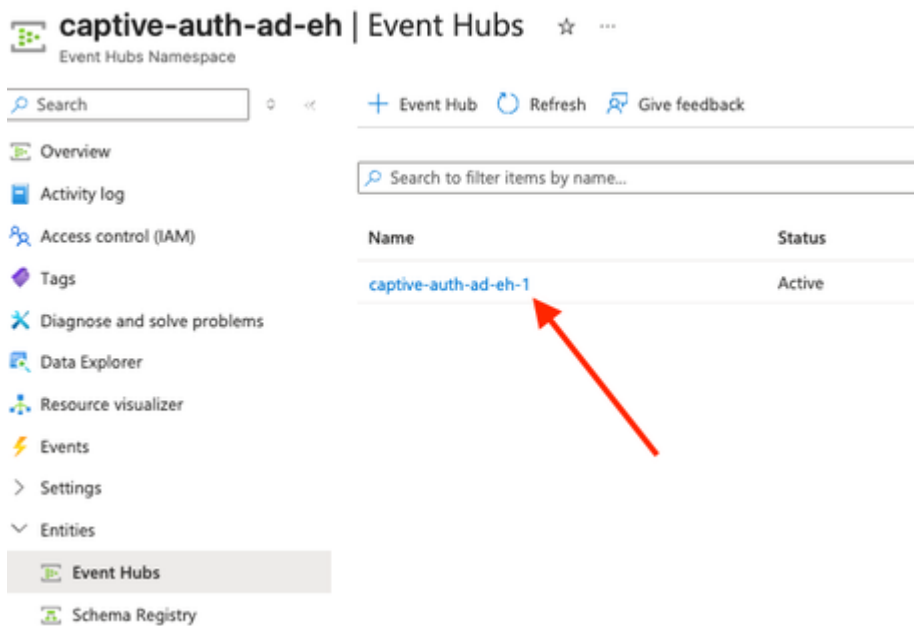
Provisionar Instância do Hub de Eventos



Importante: Copie e anote o nome da instância do Hub de Eventos.

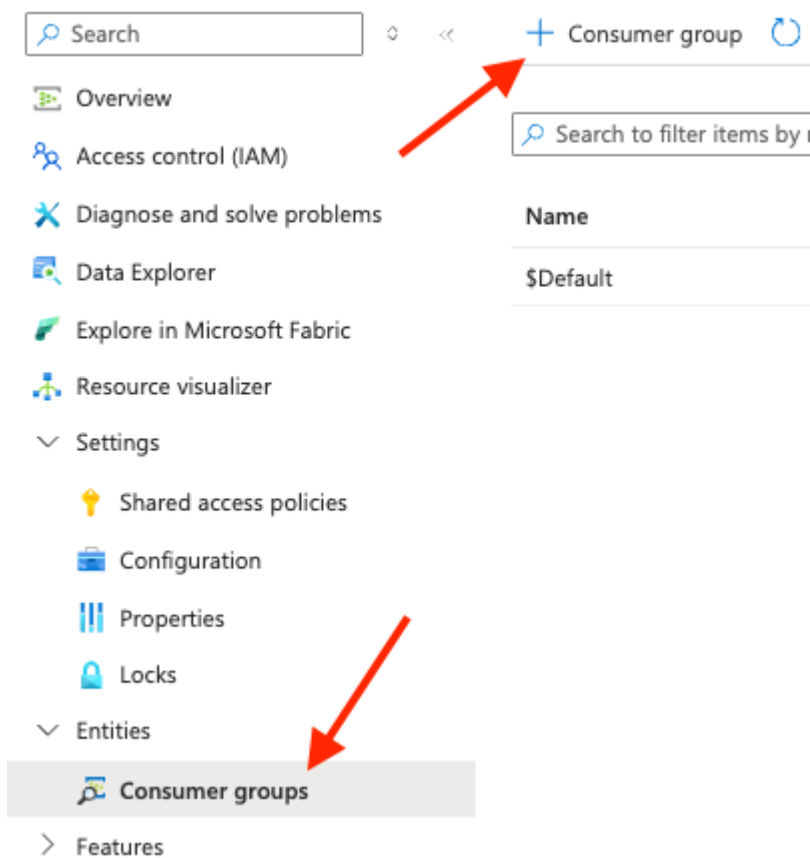
Passo 8: Criar um Grupo de Consumidores de Instâncias do Hub de Eventos no Namespace do Hub de Eventos

1) Clique na nova instância EH configurada na etapa anterior.



Acessar Configuração de Instância do Hub de Eventos

2) Na instância EH, escolha Entidades > Grupos de consumidores e crie um novo Grupo de consumidores.



Criar Grupo de Consumidores

3) Nomeie o grupo de consumidores e clique em Criar.

Create consumer group ×

Consumer groups

Name *

captive-auth-ad-eh-cg



Create

Atribuir Nome Ao Grupo De Consumidores



Importante: Copie e anote o nome do grupo de consumidores da instância do Hub de Eventos.

Etapa 9: Verificar Valores Coletados

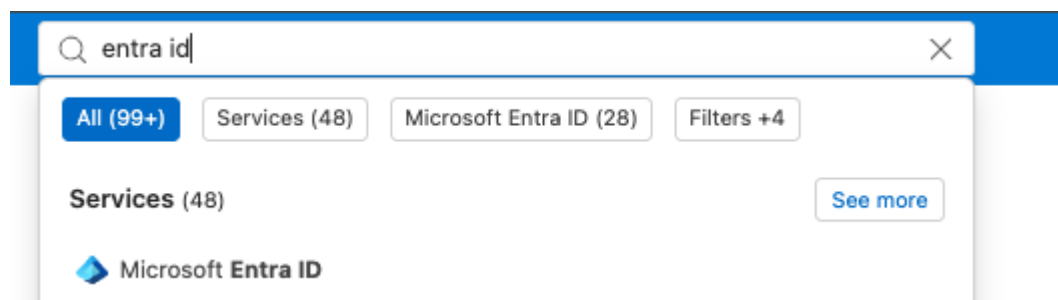
1) Neste ponto, os valores das etapas anteriores devem ser anotados. Se algum valor não tiver sido registrado, consulte a etapa aplicável onde ele é coletado:

- Fase 3 Etapa 2 - Registro do aplicativo (do aplicativo empresarial criado para esse processo, referenciado pelo nome de exibição coletado)
 - Etapa 2, Subetapa 2
 - Nome de exibição
 - ID do aplicativo (cliente)
 - ID do diretório (locatário)
 - Etapa 2, Subetapa 6
 - Segredo do cliente
- Fase 3 Etapa 6 - Hub de eventos
 - Etapa 6, Subetapa 1
 - Namespace EH

- Cadeia de Conexão Primária
- Etapa 7, Subetapa 3
 - Nome da instância EH (Hub de Eventos)
- Etapa 8, Subetapa 3
 - Nome do Grupo de Consumidores EH

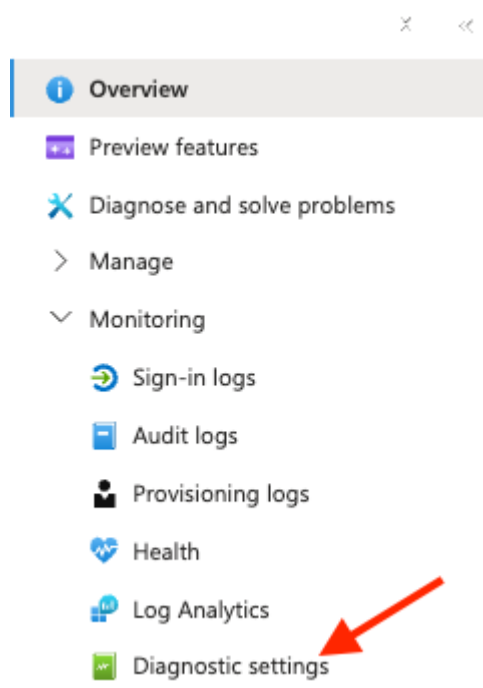
Etapa 10: Configurar o Streaming de Log de Auditoria do Entra ID para o Hub de Eventos

1) Navegue de volta para a configuração do locatário do Entra ID.



Pesquisar E Navegar Para A Configuração De Locatário Do Entra ID

2) No menu à esquerda, selecione Monitoring > Diagnostic Settings.



Monitoramento de Configurações de Diagnóstico

3) Escolha Diagnostic settings > General e clique em + 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

Adicionar nova configuração de diagnóstico

4) Atribua o nome necessário à configuração de diagnóstico, marque a caixa de seleção AuditLogs para registrar e marque a caixa de seleção Stream to an event hub. Consulte os valores observados nas configurações anteriores e clique em Save quando terminar.

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

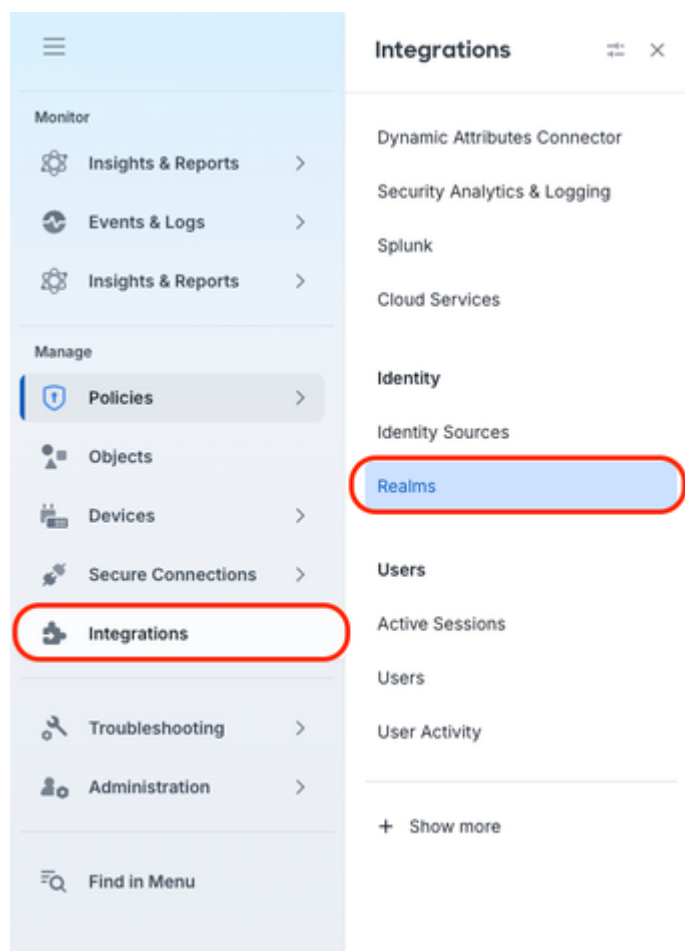
Event hub policy name

- ☐ Send to partner solution

Fase 4: Consolidar a Configuração de Autenticação Ativa do Azure e do FMC/FTD

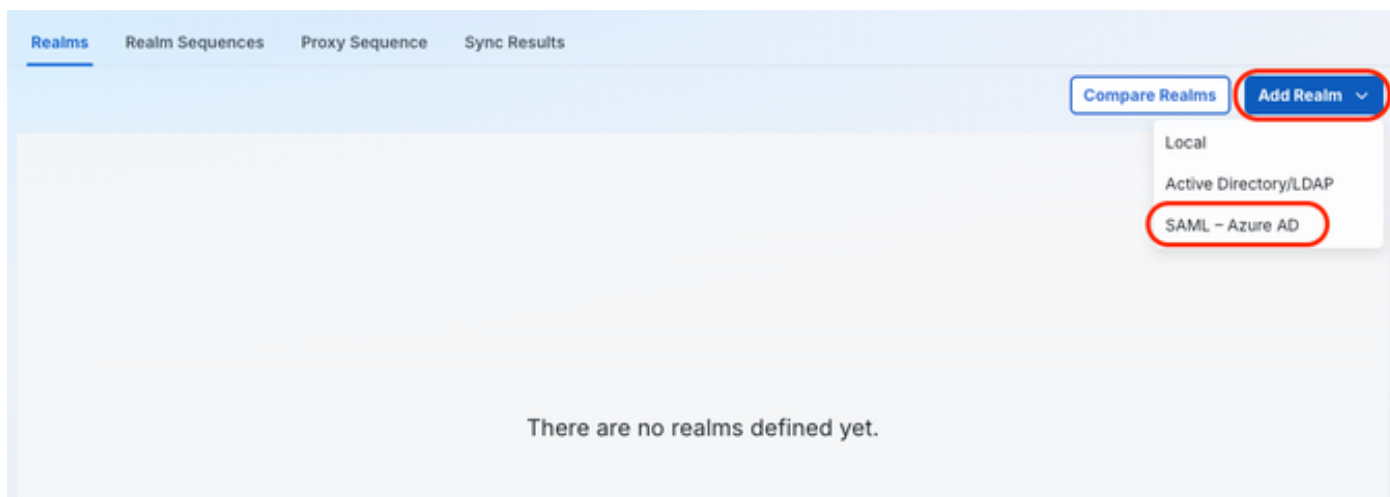
Passo 1: Configurar o Domínio SAML/Entra ID do Azure Usando o Assistente do FMC

1) No FMC, escolha Integrations > Identity > Realms.



Configuração de Realms de Identidade

2) Clique na lista suspensa Add Realm e escolha SAML - Azure AD.



Adicionar Domínio SAML Azure AD

3) Atribua um nome e descrição ao território do Azure para descrever seu uso e verifique se Autenticar passivamente com o Azure AD ou usar o portal cativo com o Azure AD é escolhido na lista suspensa Tipo de configuração. Clique em Next.

Add SAML - Azure AD Realm

1 Realm Details

Name *
azure-entra-saml

Description
Active Authentication IdP

Identity Provider *
Azure AD

Configuration Type
Authenticate passively with Azure AD or using captive portal with Az...

2 Authenticate with ISE
Download users and groups from an identity source like ISE for use in passive authentication rules.

3 Authenticate passively with Azure AD or using captive portal with Azure AD
Either download users and groups from Azure AD for use in passive authentication rules or download users and groups from Azure AD and use with captive portal active authentication rules.

4 Azure AD Details

Next

Configurar Definições de Realm do Azure AD

4) Escolha o objeto FQDN configurado anteriormente como a URL Base. Insira o ID da entidade com o formato de sequência de caracteres mostrado:

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

- Quando o sufixo da ID da entidade SAML estiver configurado (sublinhado em verde no exemplo de configuração a seguir), certifique-se de que o sufixo seja exclusivo entre outras implementações de SSO no ambiente. Este valor também deve corresponder à configuração SAML do Azure. O URL base permanece o mesmo durante toda a configuração.
- A URL de Serviços de Consumidor de Asserção (ACS) é preenchida automaticamente e é imutável.
- Escolha o Certificado do provedor de serviços (SP) registrado nas etapas de fluxo de trabalho anteriores no FMC em Dispositivos > Certificados.
- Depois que esses valores forem inseridos, clique em Baixar Metadados do Provedor de Serviços para facilitar o processo de configuração e confirmar que os valores esperados são gravados no 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 [ⓧ](#) [v](#) [+](#)

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 [v](#)

Unique, alphanumeric identifier for a SAML entity.

Assertion Consumer Services (ACS) URL *

https://ftd-inside.example.com/+CSCOE+/saml/sp/acs?tname=azure-entra [v](#)

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

Service Provider Certificate *

FTD-SP-Cert [ⓧ](#) [v](#) [+](#)

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](#)

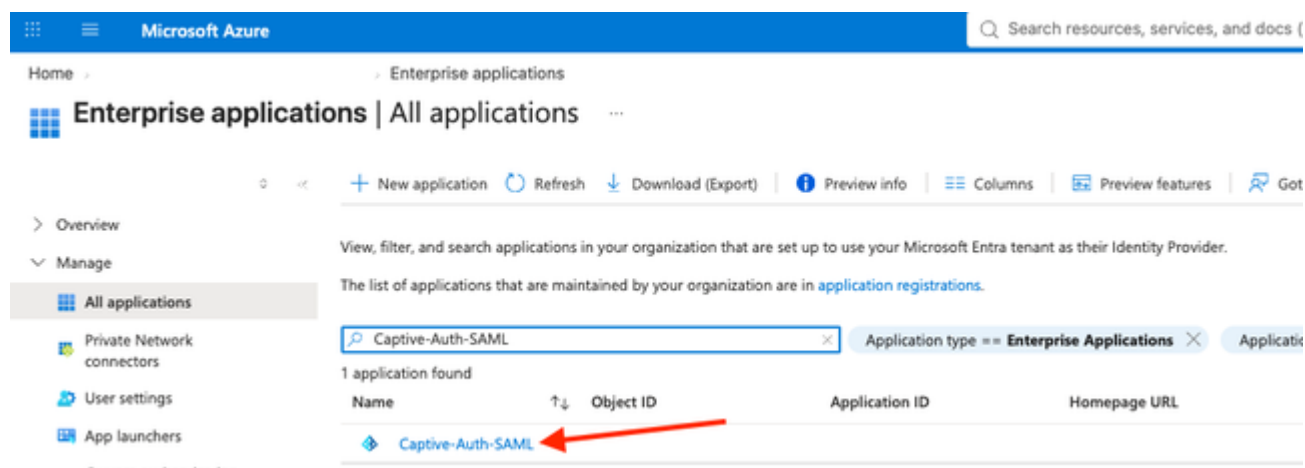
[Next](#)

Configurar URL Base e ID da Entidade e Baixar Metadados SAML

5) Clique em Próximo para ir para a Sequência 3 da configuração do Realm.

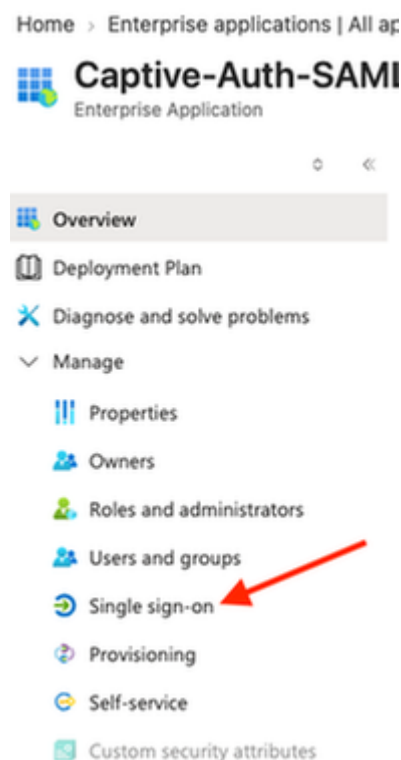
Passo 2: Implementar os Metadados de SP SAML configurados pelo FMC no Aplicativo Azure Enterprise

1) Navegue de volta para o Azure e escolha Entra ID > Gerenciar > Aplicativos Empresariais. Procure a instância criada anteriormente do Aplicativo Corporativo Microsoft Entra SAML Toolkit.



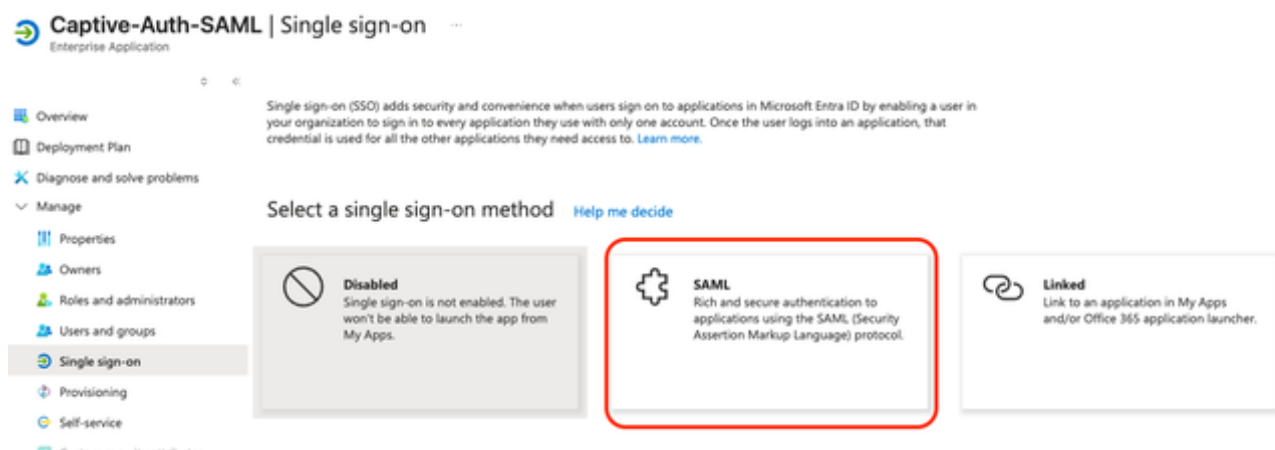
Localizar o Aplicativo Microsoft Entra SAML Toolkit

2) No menu de navegação lateral, escolha Gerenciar > Logon único.



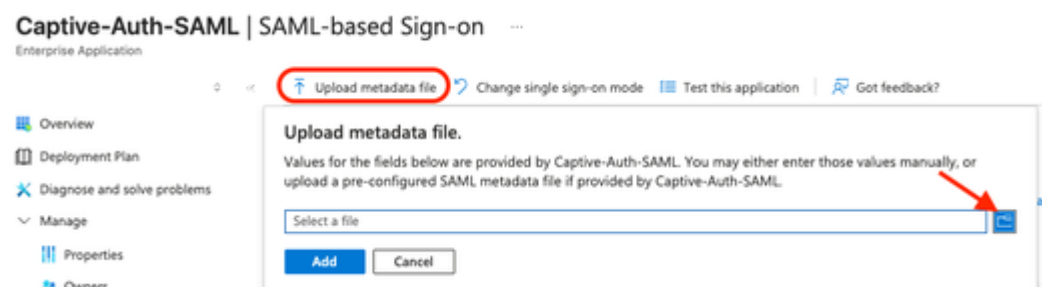
Gerenciar Configuração de Logon Único

3) Clique no modo SAML Single Sign-On (SSO).



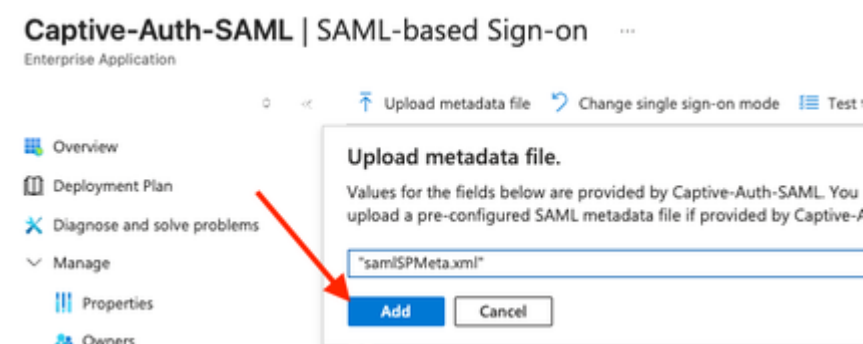
Seleção do Modo de Logon Único do SAML

4) Clique em Upload metadata file e clique no ícone de pasta azul para procurar no sistema de arquivos local o arquivo de metadados SAML baixado do FMC.



Carregar Arquivo De Metadados Do Centro De Gerenciamento De Firewall

5) Quando o carregamento for concluído, clique em Add.



Adicionar aplicativo de configuração SAML

6) O painel lateral para Configuração SAML básica é exibido e valores como Identificador (ID da entidade) e URL do ACS são extraídos do arquivo XML de metadados SP originado no FMC carregado e aplicado automaticamente. No entanto, a URL de início de sessão não é preenchida

e é necessária antes de salvar.

Save

Got feedback?

Basic SAML Configuration

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

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

✓

✓

ⓘ

🗑

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

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

✓

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.

*

Enter a sign on URL

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.

Enter a relay state

Logout Url (Optional)

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

Enter a logout url

✓

Extração de Configuração de SAML Básica

7) Use o padrão de URL de Logon fornecido, copie e cole o valor e clique em Salvar na parte superior quando terminar.

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

<https://ftd-inside.example.com/saml/sp/metadata/activeAuthEntID> ✓



[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

<https://ftd-inside.example.com/+CSCOE+/saml/sp/acs?tgname=azure-entra-saml>

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.

*

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

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.

Enter a relay state

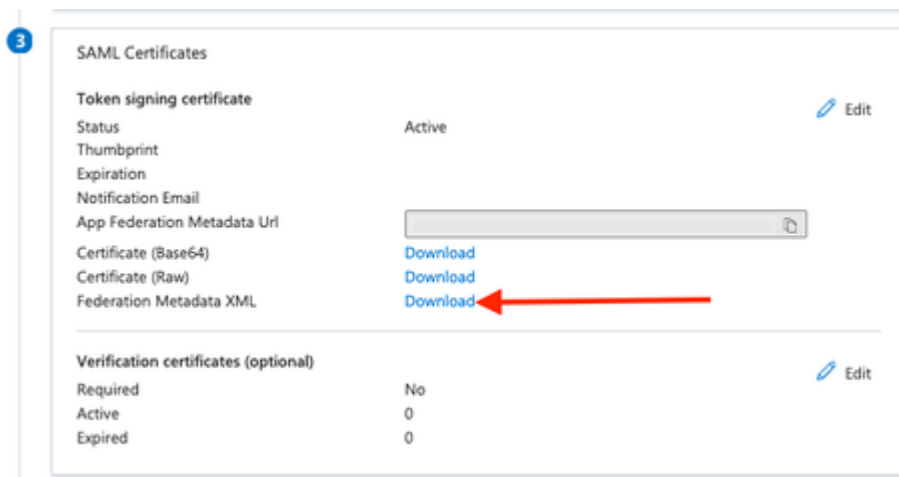
Logout Url (Optional)

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

Enter a logout url



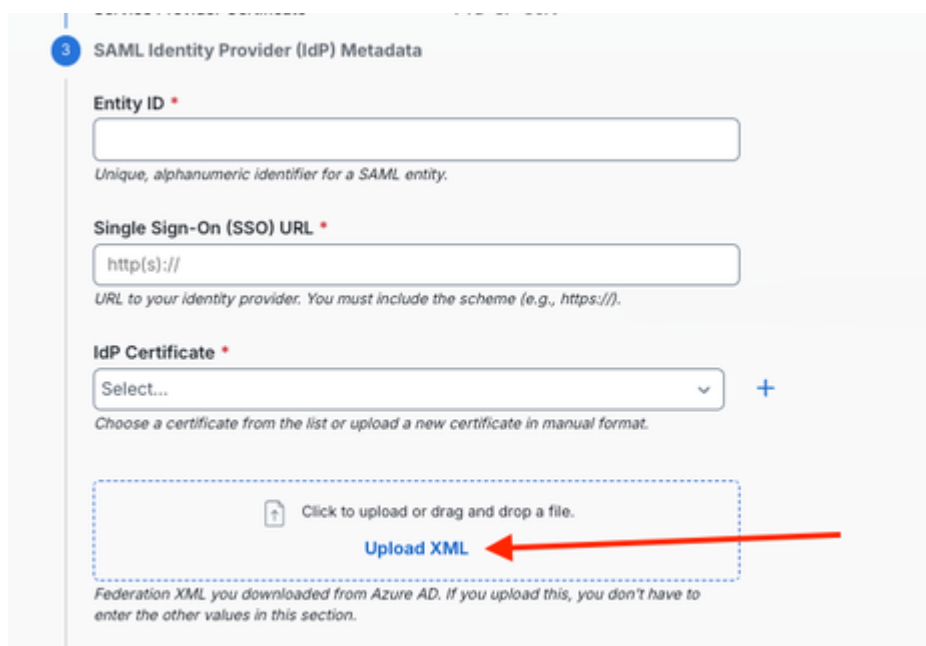
Role para baixo até Certificados SAML e exporte o arquivo XML de Metadados de Federação gerado pelo Azure para importar para o Cisco Secure FMC.



Exportar Arquivo XML de Metadados de Federação

Passo 3: Configurar o Domínio SAML/Entra ID do Azure Usando o Assistente do FMC (Continuação)

1) Volte para o FMC. Na Sequência 3, Metadados do Provedor de Identidade SAML (IdP), carregue o arquivo XML de Metadados de Federação exportado do Azure para o FMC para preencher automaticamente os valores necessários.



Carregar Arquivo XML de Metadados de Federação

2) Uma vez carregados, os valores são preenchidos conforme mostrado.

3 SAML Identity Provider (IdP) Metadata

Entity ID *

Unique, alphanumeric identifier for a SAML entity.

Single Sign-On (SSO) URL *

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

IdP 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](#)

Valores do Provedor de Identidade SAML Preenchidos Automaticamente



Note: A saída parcial é mostrada na imagem.

3) Insira os valores coletados durante o processo de implementação até este ponto:

- Registro do aplicativo
 - ID do aplicativo (cliente)
 - Segredo do cliente
 - ID do Diretório (Locatário)
- Hub de eventos
 - Nome de host do namespace EH
 - Cadeia de Conexão Primária do Namespace EH
 - Nome da Instância EH (Hub de Eventos)
 - Nome do Grupo de Consumidores EH

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

Inserir Informações Do Aplicativo E Do Hub De Eventos

Depois de inserir, clique em Testar para verificar a conexão e confirmar se o Azure está acessível com as informações fornecidas.



Note: Se aplicável, certifique-se de que os grupos de usuários excluídos/incluídos estejam de acordo com sua configuração do Entra

4) A etapa final do assistente permite configurar o tempo limite de usuários do portal cativo SAML. O padrão é 1440 minutos.

5 User Session Timeout

SAML Captive Portal Users

1440 Minutes Range 0-35791394

Configurar tempo limite do portal cativo

5) Clique em Avançar para continuar.

After the timeout is exceeded, the user's session ends; if the user continues to access the network without logging in again, the user is seen by the management center as Unknown (except for Failed Captive Portal Users).

Next

Avançar com a Configuração do Domínio do Azure AD

6) O assistente fornece um resumo da configuração implementada. Clique em Salvar no final do resumo depois que os valores inseridos forem validados e confirmados.

5 User Session Timeout Edit

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

Cancel Save

Botão Salvar Resumo da Configuração do Realm

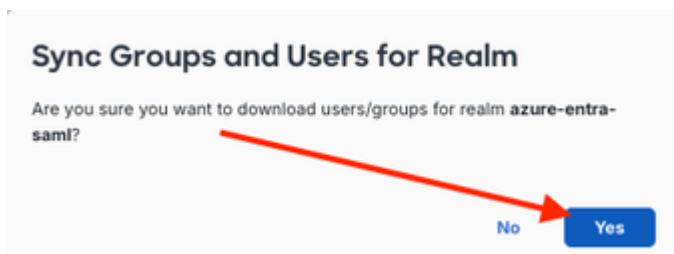
Passo 4: Verificar Usuários Baixados

1) Confirme se os usuários podem ser baixados do Azure Entra com o fluxo de trabalho Baixar Agora em Integrações > Identidade > Territórios.

Name	Type	Description	Proxy	Status	Value	
azure-entra-saml	SAML - Azure AD (captive portal)	Active Authentication IdP	Not Applicable	Ok	Tenant ID: af42bac0-5	Enabled Download Now

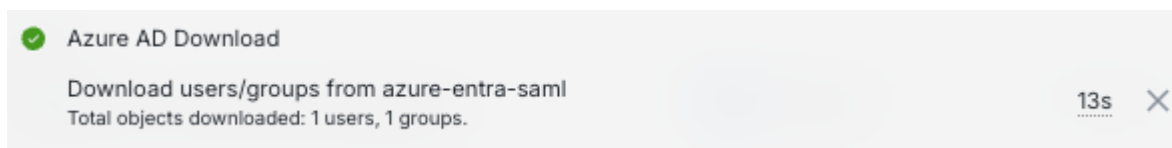
Baixar Usuários do Azure AD

2) Clique em Yes em resposta ao prompt do diálogo.



Confirmar Download de Usuários do Azure AD

3) A tarefa de download produz 1 usuário e 1 grupo baixado, como confirmado em Notificações > Tarefas.

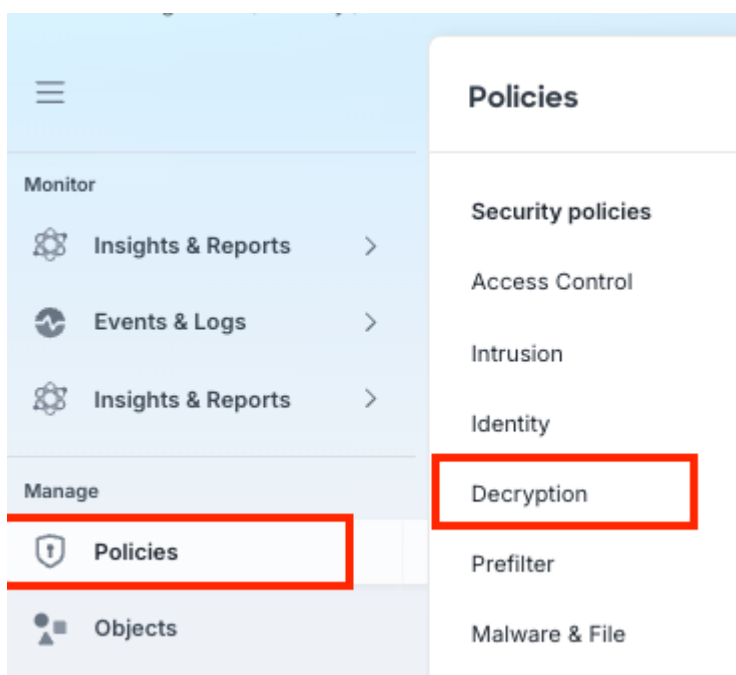


Entrada De Notificação Para Download De Usuários Do Azure AD

Fase 5: Configurar políticas no FMC

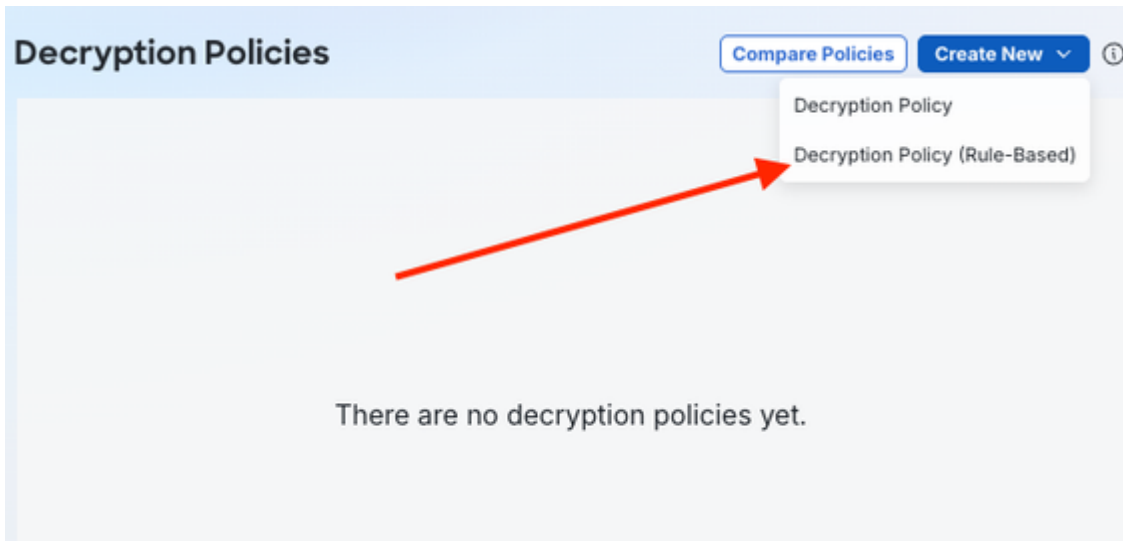
Passo 1: Configurar Política de Descriptografia

1) No FMC, escolha Policies > Security Policies > Decryption.



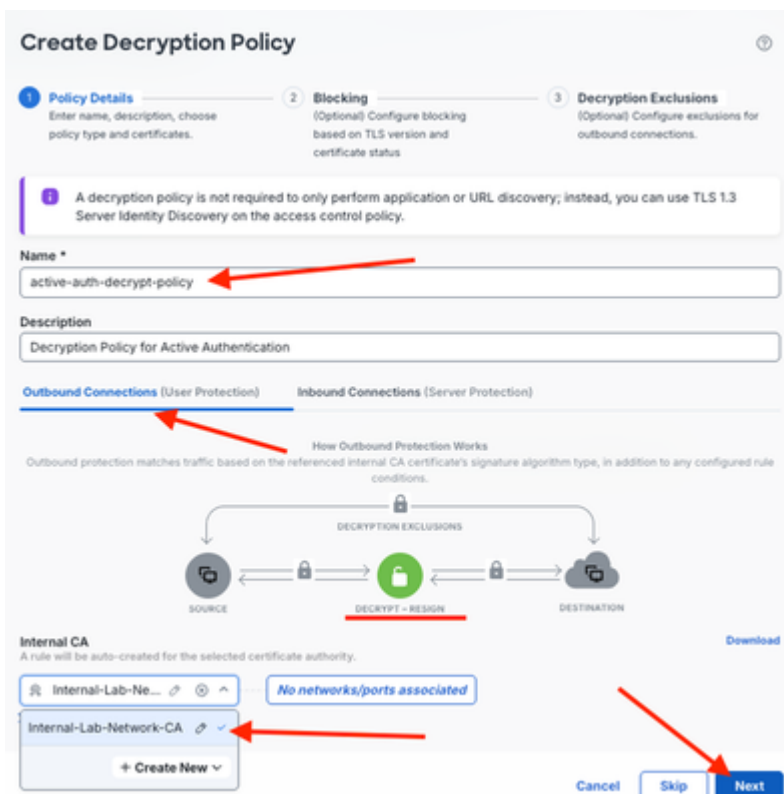
Navegar Para Política De Descriptografia

2) Clique na lista suspensa Create New e selecione Decryption Policy (Rule-Based).



Criar Nova Política de Descriptografia Baseada em Regras

3) Atribua um nome e, se desejado, uma descrição à nova Política de descriptografia baseada em regras e clique na opção da guia Conexões de saída (Proteção do usuário) para implementar a funcionalidade Descriptografar-Resign necessária para a autenticação do portal cativo (Autenticação ativa).



Implementar Detalhes da Política de Conexões de Saída

4) Escolha a CA interna anteriormente aplicada na lista suspensa aplicável na mesma caixa de

diálogo. Clique em Next.

5) Personalize as opções conforme necessário.

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](#)

Personalizar opções de política de descriptografia

6) Neste exemplo, os padrões são usados com exceção dos Detalhes da política necessários. Conclua o assistente de configuração clicando em Criar política.

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

[New](#)

[Cancel](#) [Skip](#) [Back](#) [Create Policy](#)

Criar política de descriptografia final

Passo 2: Configurar Regras de Política de Descriptografia

1) O layout padrão de uma política de descriptografia baseada em regras é mostrado aqui. O tráfego que não corresponde às regras ativadas padrão, como a regra 3 (que faz referência a uma lista pré-alocada de nomes de domínio não descriptografáveis) e a regra 6 (que faz referência a aplicativos marcados como não descriptografáveis), está sujeito à ação Descriptografar - Renunciar sob a Regra 7. Esses padrões, juntamente com a Ação padrão, podem ser modificados conforme necessário. Por padrão, o tráfego que não corresponde a nenhuma outra regra é configurado como Não descriptografar.

O tráfego do Serviço de Autenticação do Azure não deve ser descriptografado para inspeção, portanto, uma regra dedicada é criada para ele. Clique em + Adicionar regra para começar.

active-auth-decrypt-policy

Save

Cancel

Decryption Policy for Active Authentication

Rules

Trusted CA Certificates

Undecryptable Actions

Advanced Settings

+ 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
Administrator Rules													
This category is empty													
Standard Rules													
1	Auto-Rule-Certificate-Stz (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 Vers	Block with reset
3	Auto-Rule-Undecrypt	any	any	any	any	any	any	any	any	any	any	1 DN selection	Do not decrypt
4	Auto-Rule-Low-Risk-Con (Disabled)	any	any	any	any	any	any	any	any	any	any	Any (Except L 1 Client Threat	Do not decrypt
5	Auto-Rule-URL-Categoric (Disabled)	any	any	any	any	any	any	any	any	any	any	Finance (Any Health and M any Online Tradin	Do not decrypt
6	Auto-Rule-Undecryptabl	any	any	any	any	any	any	Tags: undecry	any	any	any	any	Do not decrypt
7	Auto-Rule-Internal-La	any	any	any	any	any	any	any	any	any	any	any	Decrypt - Resign
Root Rules													
This category is empty													
Default Action													Do not decrypt

Adicionar Regra E Mostrando Layout De Descriptografia Baseado Em Regra Padrão

2) Atribua um nome à nova entrada de regra da política de descriptografia, escolha Não descriptografar na lista suspensa Ação e coloque a regra na parte superior, com regras menos específicas. As zonas de Origem/Destino também são implementadas para restringir ainda mais a regra.

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

Available Zones

Search by name

Inside_Zone

Outside_Zone

DMZ_Zone

Add to Source

Add to Destination

Source Zones (1)

Inside_Zone

Destination Zones (1)

Outside_Zone

Cancel

Add

Configurar Regra Não Descriptografar

3) Antes da regra ser adicionada, clique na guia Aplicativos, procure e clique no aplicativo Azure Authentication Service. Clique em Adicionar à Regra e clique em Adicionar.

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 Available Applications (2)

Risks (Any Selected)

- ☐ Very Low 809
- ☐ Low 715
- ☐ Medium 2239
- ☐ High 1823
- ☐ Very High 609

Business Relevance (Any Selected)

- ☐ Very Low 009

All apps matching the filter

- Azure Arc
- Azure Authentication Service**

Selected Applications and Filters (0)

any

Adicionar Regra de Aplicativo do Serviço de Autenticação do Azure

4) Clique em Salvar.

active-auth-decrypt-policy

Decryption Policy for Active Authentication

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

You have unsaved changes

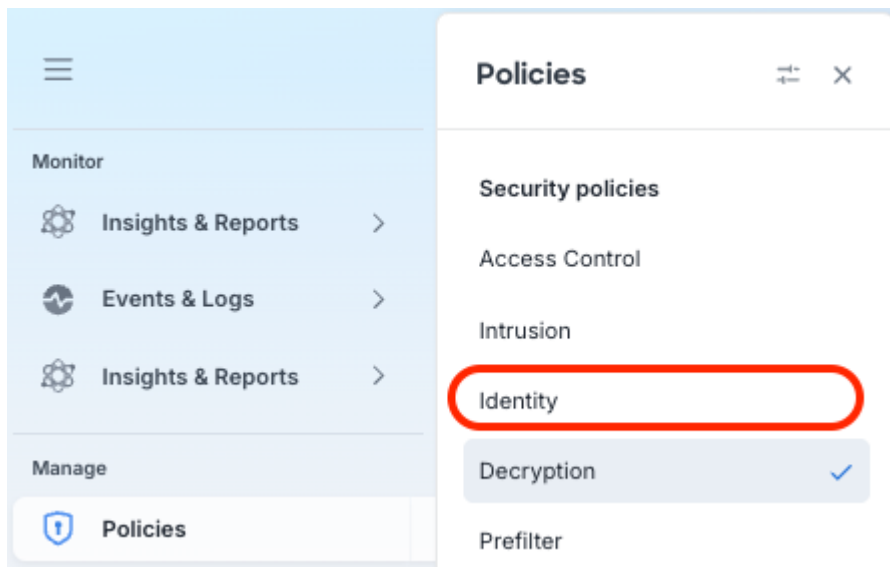
+ Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	Categories	SSL	Action
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 Vers	Block with reset
3	Azure-Auth-Service-	Inside_Zone	Outside_Zon	any	any	any	any	Azure Authen	any	any	any	any	Do not decrypt

Salvar política de descriptografia

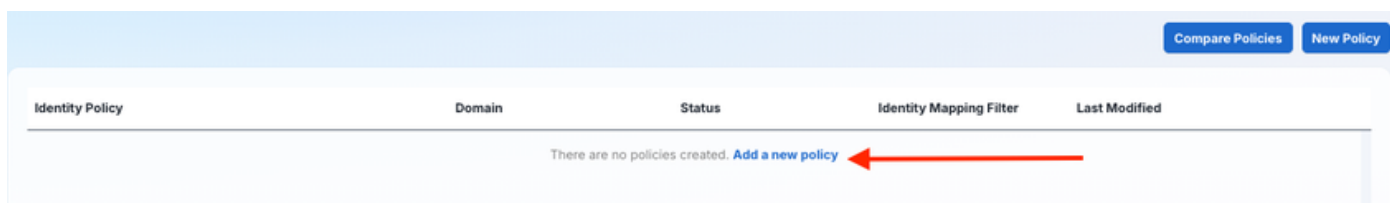
Passo 3: Criar política de identidade

1) Escolha Policies > Security Policies > Identity para criar uma política de identidade.



Criar política de identidade

2) Crie uma nova Política de identidade e clique em Adicionar uma nova política.



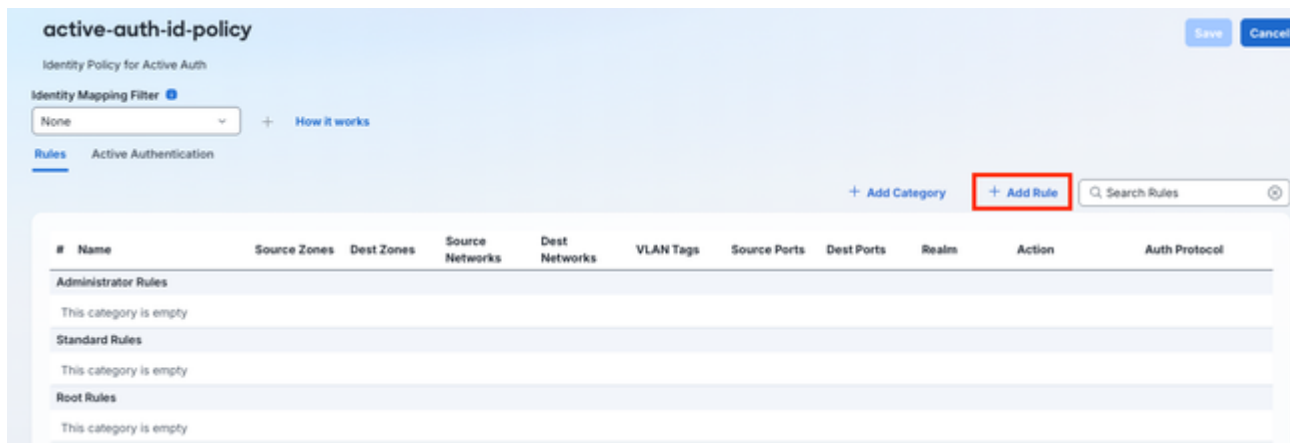
Adicionar nova configuração de política de identidade

3) Atribua um nome e, se aplicável, uma descrição à nova política de identidade. Click Save.

Nome Nova Política de Identidade

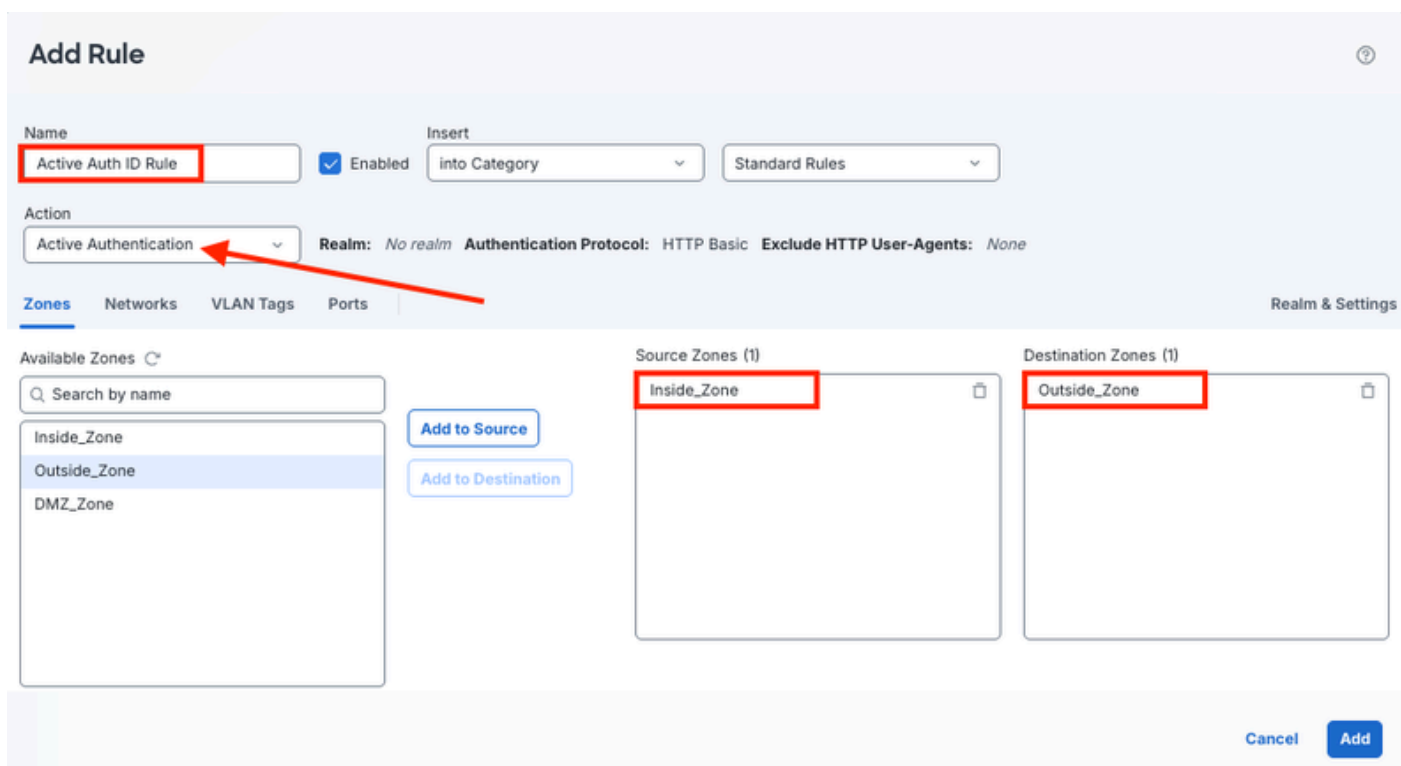
Passo 4: Configurar Regras de Política de Identidade

1) Adicione uma nova regra clicando em + Adicionar regra.



Adicionar nova regra de política de identidade

2) Nomeie a nova regra, escolha Autenticação ativa na lista suspensa Ação e restrinja as zonas/redes específicas que devem corresponder à regra para executar a Autenticação ativa.



Add Rule

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

Action: **Active Authentication** Realm: No realm Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Zones Networks VLAN Tags Ports **Realm & Settings**

Available Zones

- Inside_Zone
- Outside_Zone**
- DMZ_Zone

Add to Source **Add to Destination**

Source Zones (1): **Inside_Zone** Destination Zones (1): **Outside_Zone**

Cancel **Add**

Definir Configurações de Regra de Autenticação Ativa

3) Antes de clicar em Adicionar, clique na guia Realm and Settings no Editor de regras. Confirme se o território configurado nas etapas anteriores foi escolhido como o território de autenticação e clique em Adicionar.

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

Definir Território E Configurações Para Regra De Identidade

4) A regra é adicionada e configurada. 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](#)

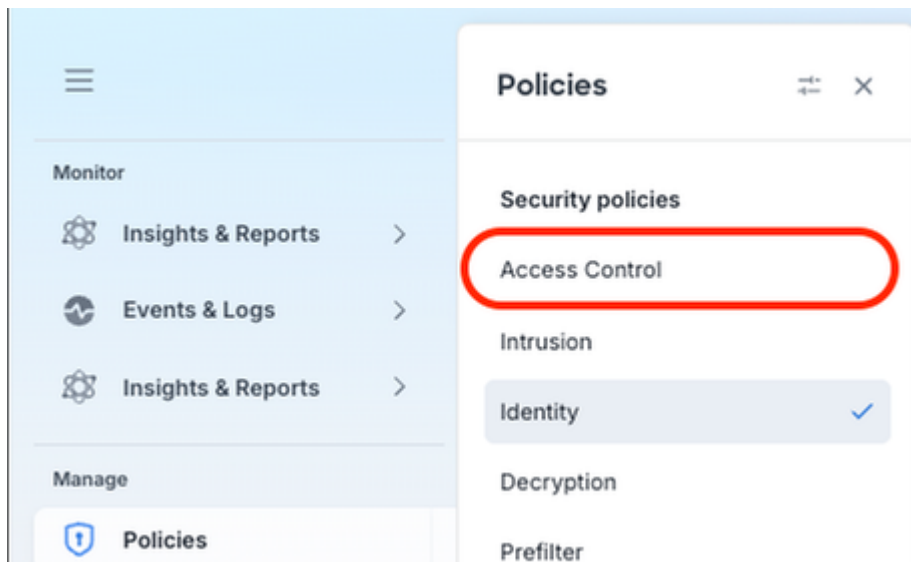
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	Active Auth ID Rule	Inside_Zone (Ro	Outside_Zone (f	any	any	any	any	any	azure-entra-san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

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

Salvar Configuração de Regra de Política de Identidade

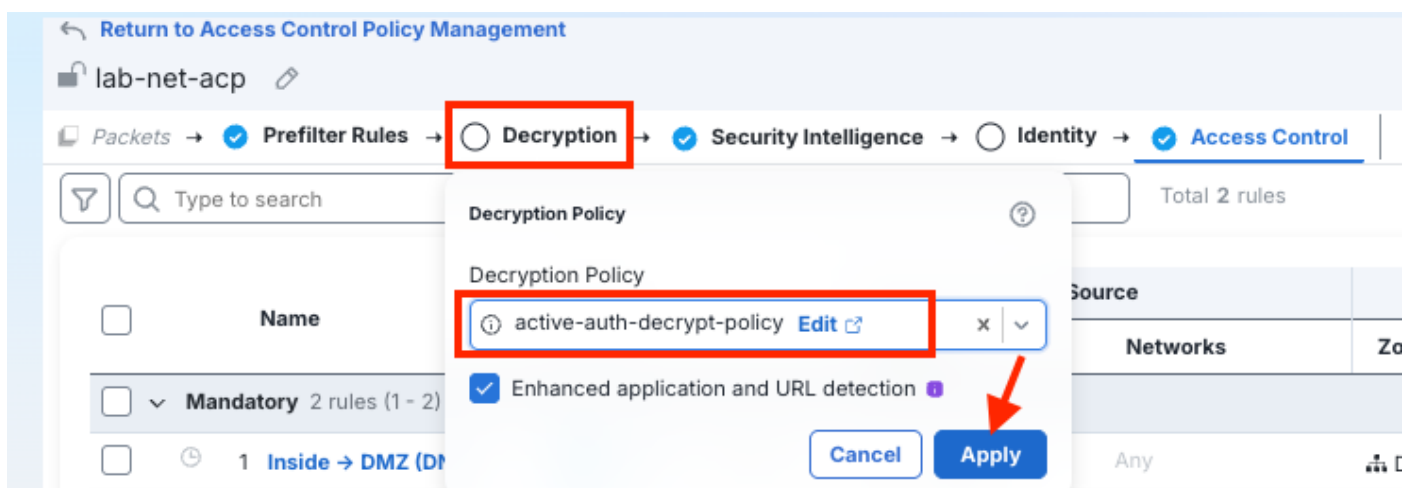
Passo 5: Configurar a Política de Controle de Acesso

1) Escolha Policies > Security Policies > Access Control e clique na Access Control Policy à qual o FTD está atribuído.



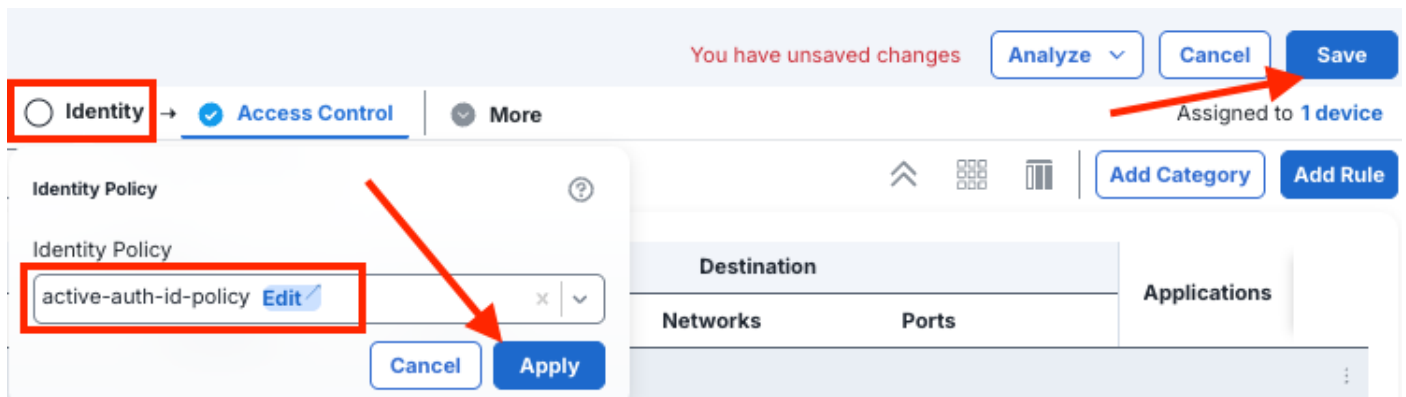
Configuração da Política de Controle de Acesso

2) Confirme se a política de descryptografia configurada nas etapas anteriores foi aplicada à política de controle de acesso.



Aplicar Política De Descryptografia Ao Controle De Acesso

3) Confirme se a política de identidade configurada nas etapas anteriores também é aplicada à política de controle de acesso. Salve as alterações da política.



Aplicar Política De Identidade Ao Controle De Acesso

4) Confirme se existem regras que permitem o tráfego do plano de dados do cliente através do Firewall Seguro após a Autenticação Ativa bem-sucedida. O exemplo mostrado aqui usa um conjunto de regras mais amplo, dado o ambiente de laboratório.

☐	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)								

Conjunto de Regras de Tráfego de Plano de Dados do Usuário

Passo 6: Implante configurações nos dispositivos Cisco Secure Firewall

Uma vez implantados, os clientes que enviam tráfego são solicitados com uma página da Web de Entrada da Microsoft para executar a Autenticação Ativa com o Azure Entra.

Para obter contexto adicional sobre o processo documentado aqui, consulte [Criar um realm do Microsoft Azure AD \(SAML\) para autenticação ativa \(portal cativo\) - Capítulo: Territórios no Guia de configuração de dispositivo FMC 10.x](#).

Verificar

Use esta seção para ajudar a confirmar se a configuração funciona corretamente.

GUI

Validar as sessões e atividades do usuário no FMC:

- Escolha Integrations > Users > Active Sessions.

The screenshot shows the Cisco FMC interface with the breadcrumb 'Integrations / Users / Active Sessions'. A table displays one active session for the user 'captive-portal-user' in the 'azure-entra-saml' realm. The session duration is 1 min 40 sec, and it was last seen on 2026-10-07 at 02:10:02.

☐	Login Time	RealmUsername	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

Saída de Sessões Ativas do FMC

- Escolha Integrations > Users > User Activity.

The screenshot shows the Cisco FMC interface with the breadcrumb 'Integrations / Users / User Activity'. A table displays two user login activities for the user 'captive-portal-user' in the 'azure-entra-saml' realm, both using 'Microsoft Azure' as the discovery application.

☐	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		

Saída da atividade do usuário do FMC

No Azure, navegue para o Centro de Administração do Microsoft Entra:

- Filtrar aplicativos corporativos, pesquisar/clicar no aplicativo aplicável.

The screenshot displays the Microsoft Entra admin center interface. On the left, the navigation pane lists various sections, with 'Enterprise apps' highlighted by a red box. The main content area is titled 'Enterprise applications | All applications'. It features a search bar with the text 'captive-' and a list of applications. A red arrow points from the 'Custom authentication extensions' section in the left pane to the 'Captive-Auth...' application in the list. The list has columns for 'Name', 'Obj', and 'efda'.

Name	Obj	efda
Captive-Auth...		

Navegação de Aplicativos Empresariais do Centro de Administração do Azure Entra

- Escolha Activity > Sign-in logs.

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

Logs de Atividades de Entrada do Aplicativo Azure Enterprise

CLI

- Na CLI do FTD, você pode ver estatísticas relacionadas à SAML e respostas do portal cativo:

<#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
```

Troubleshooting

Depuração do portal cativo

- O comando `system support captive-portal-debug` pode ser usado no FTD. A saída mostra como habilitar a depuração e também observa segmentos-chave da saída para ajudar a entender o fluxo do Portal Cativo.

```
<#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
...

```

Despejo de Identidade de Usuário

- Para obter um instantâneo dos dados do estado de identidade do usuário atual no FTD, execute o comando `system support firewall-engine-dump-user-identity-data` na CLI do FTD:

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

```
Successfully commanded snort.
```

```
>
```

- Na CLI do modo expert , ao fazer login com as credenciais de administrador local do dispositivo FTD, visualize o conteúdo do arquivo despejado em /ngfw/var/sf/user_enforcement/user_identity.dump

```
<#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:
```

```
-----
```

```
...
```

Possíveis problemas

Autoridade de Certificação Desconhecida do Portal Cativo

Problema: O navegador do cliente retorna um erro de emissor desconhecido quando há uma tentativa de autenticação.

Causa provável: A Autoridade de Certificação interna não é confiável no navegador do cliente.

Resolução: Confirme se a autoridade de certificação é confiável no navegador. O exemplo mostrado aqui confirma que o certificado interno da CA é confiável.

Portal cativo "Servidor não encontrado"

Problema: Quando o navegador do cliente tenta carregar o portal cativo, ele retorna "Servidor não encontrado" para o URL base ao tentar alcançar o URL base ou similar.

Causa provável: Acessibilidade de DNS ou configuração incorreta de DNS.

Resolução: Confirme se o cliente tem o servidor DNS apropriado configurado para resolver o registro A. Confirme se o servidor tem um registro A mapeado para o FQDN e se ele está acessível e responde.

Informações Relacionadas

- [Criar um domínio do Microsoft Azure AD \(SAML\) para autenticação ativa \(portal cativo\) - Guia de Configuração de Dispositivo do FMC 10.x](#)
- [Documentação do Hub de Eventos do Azure](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

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.