

Configuración de Azure Entra Captive Portal en Secure Firewall

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama](#)

[Portal cautivo entre terminales, FTD y Azure Entra](#)

[Configurar](#)

[Fase 1: Configuración inicial de FMC y DNS](#)

[Paso 1: Habilitar el conector de atributos dinámicos de Cisco \(CSDAC\)](#)

[Paso 2: Creación de un Objeto de Red de Nombre de Dominio Totalmente Cualificado Representante de la Interfaz de Ingreso FTD](#)

[Paso 3: Configuración del registro A de DNS](#)

[Fase 2: Configuración de la infraestructura de clave pública](#)

[Paso 1: Importar el certificado de CA interna al FMC](#)

[Paso 2: Firmar el certificado de proveedor de servicios con la CA](#)

[Paso 3: Implementación del certificado SP en el FTD](#)

[Fase 3: Configuración de Azure](#)

[Paso 1: Crear la aplicación empresarial completa para el kit de herramientas de SAML](#)

[Paso 2: Configurar registros de aplicaciones de ID de entrada](#)

[Paso 3: Configure los permisos de la API de Microsoft Graph para el registro de la aplicación.](#)

[Paso 4: Configuración del espacio de nombres del Event Hub \(EH\)](#)

[Paso 5: Elija o cree políticas de acceso compartido en el espacio de nombres del centro de eventos](#)

[Paso 6: Recopilar y anotar información de firmas de acceso compartido \(SAS\) del espacio de nombres EH](#)

[Paso 7: Creación de una instancia del Event Hub en el espacio de nombres del Event Hub](#)

[Paso 8: Creación de un grupo de consumidores de instancias de Event Hub en el espacio de nombres del Event Hub](#)

[Paso 9: Verificar valores recopilados](#)

[Paso 10: Configuración de la transmisión del registro de auditoría de Intra ID al Event Hub](#)

[Fase 4: Consolidar configuración de autenticación activa de Azure y FMC/FTD](#)

[Paso 1: Configuración del rango de ID de Azure SAML/Entra mediante el Asistente de FMC](#)

[Paso 2: Implementar los metadatos SP de SAML configurados en FMC en la aplicación empresarial de Azure](#)

[Paso 3: Configuración del rango de ID de Azure SAML/Entra mediante el asistente de FMC \(continuación\)](#)

[Paso 4: Comprobar usuarios descargados](#)

[Fase 5: Configuración de políticas en el FMC](#)

[Paso 1: Configurar política de descifrado](#)

[Paso 2: Configurar reglas de directiva de descifrado](#)

[Paso 3: Crear política de identidad](#)

[Paso 4: Configurar reglas de directiva de identidad](#)

[Paso 5: Configuración de la política de control de acceso](#)

[Verificación](#)

[GUI](#)

[CLI](#)

[Troubleshoot](#)

[Depuración del portal cautivo](#)

[Volcado de identidad de usuario](#)

[Posibles problemas](#)

[Autoridad de certificados desconocida del portal cautivo](#)

[Portal cautivo "Servidor no encontrado"](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración de Microsoft Azure Entra ID para su uso con el portal cautivo (autenticación activa) en Cisco Secure Firewall.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Lenguaje de marcado de aserción de seguridad (SAML)
- Microsoft Azure
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)

Debe tener el nivel de precios Estándar disponible en Azure para la creación de Event Hub. Además, los dispositivos deben activarse con la licencia inteligente habilitada con funcionalidad de exportación controlada.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure FTD versión 10.0
- Cisco Secure FMC versión 10.0

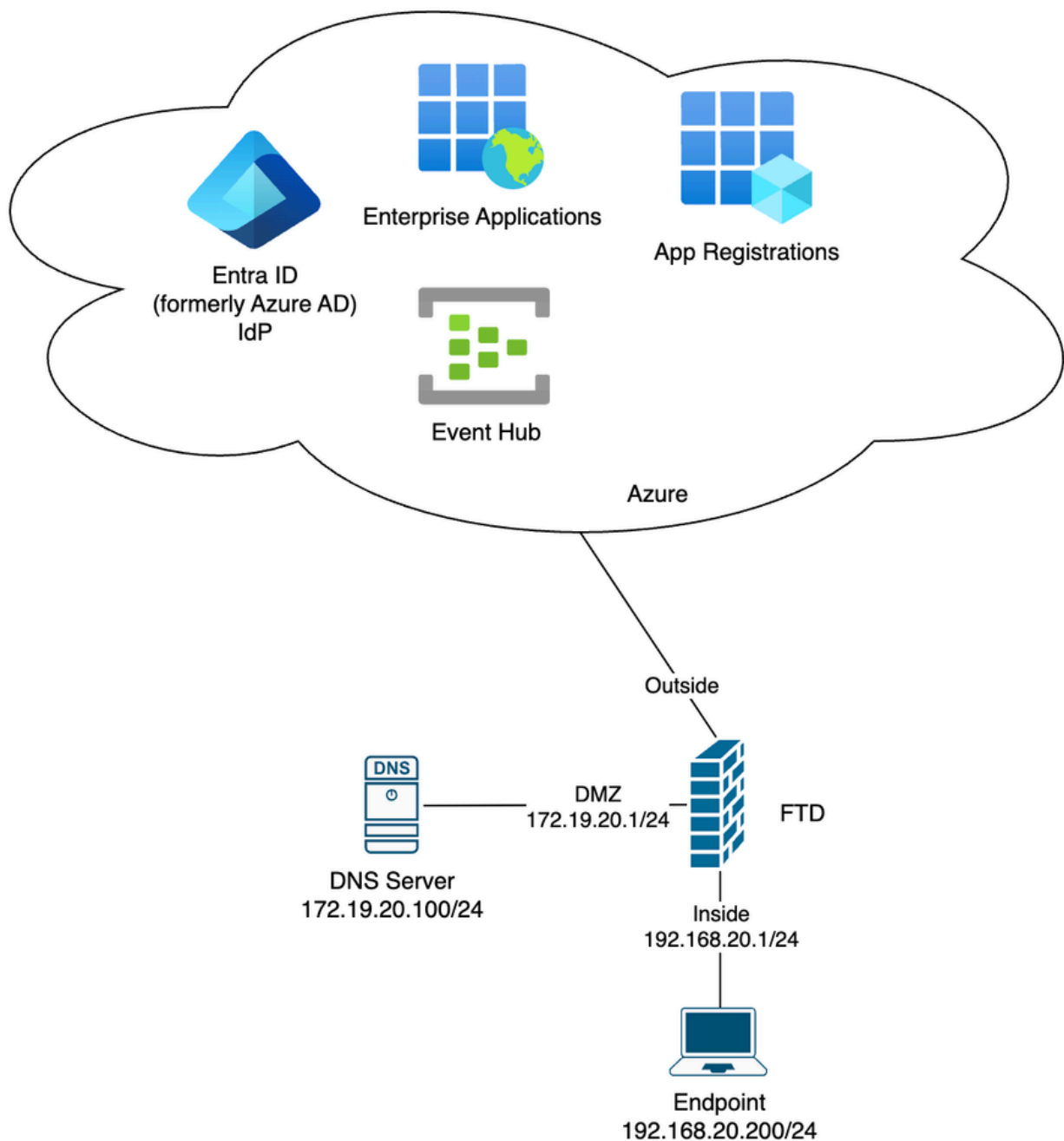
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

A medida que las arquitecturas de seguridad tradicionales basadas en IP se esfuerzan por seguir el ritmo de los entornos de trabajo dinámicos e híbridos, la autenticación activa de Cisco Secure Firewall con integración SAML ofrece una solución sólida centrada en la identidad. Al aprovechar Microsoft Entra ID (Azure AD) como proveedor de identidad centralizado, esta configuración permite a los administradores ir más allá de las reglas de red estáticas y aplicar un control de acceso granular basado en la identidad de usuario verificada en lugar de en direcciones de red volátiles. Esta integración optimiza la experiencia del usuario a través del inicio de sesión único (SSO) y la autenticación multifactor (MFA) obligatoria, a la vez que garantiza una condición de seguridad unificada que mantiene una estricta visibilidad y aplicación de políticas en una red sin perímetro.

Diagrama

Portal cautivo entre terminales, FTD y Azure Entra



Portal cautivo entre EndPoint y Azure Entra

Configurar

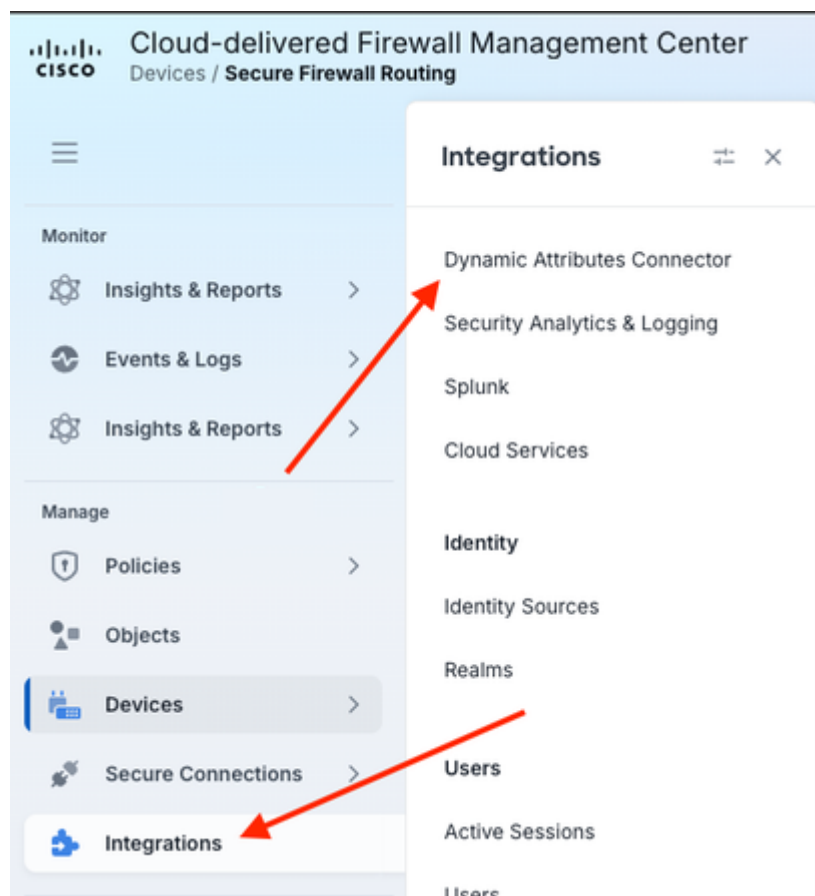
Fase 1: Configuración inicial de FMC y DNS



Nota: Este laboratorio utiliza el centro de gestión de firewall (cdFMC) proporcionado en la nube; sin embargo, los pasos siguen siendo los mismos para el FMC in situ.

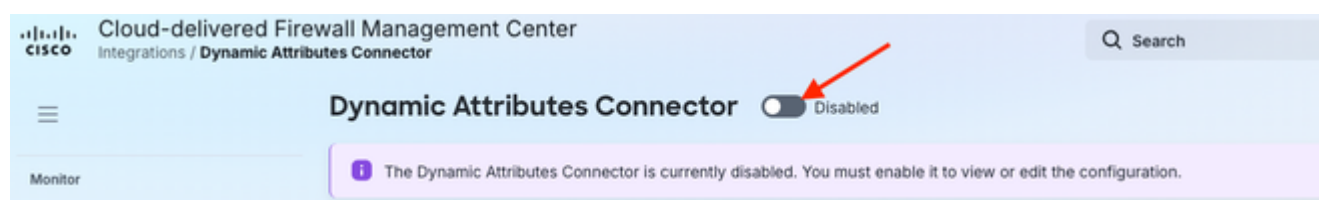
Paso 1: Habilitar el conector de atributos dinámicos de Cisco (CSDAC)

1) Elija Integraciones > Conector de atributos dinámicos.



Seleccione Integraciones Conector de atributos dinámicos

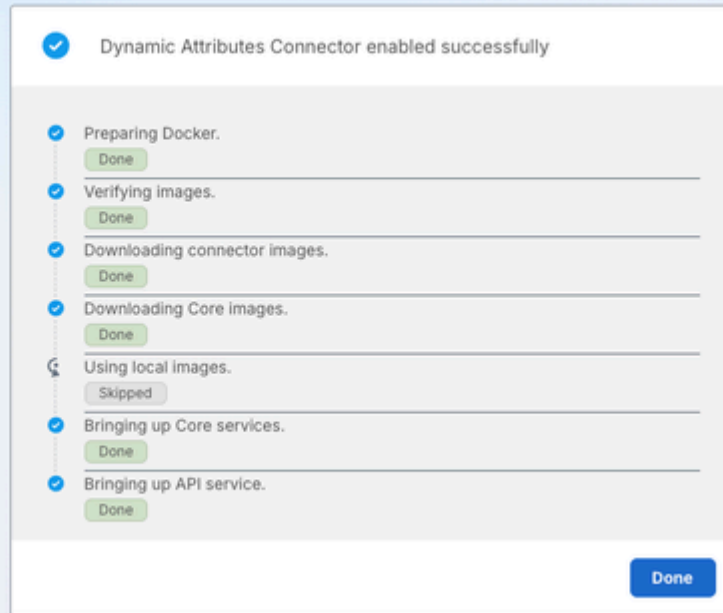
2) Haga clic en el control adyacente a la cadena Disabled para habilitar CSDAC.



Habilitar conector de atributos dinámicos de Cisco

c) Haga clic en Finalizado una vez que se complete la habilitación CSDAC.

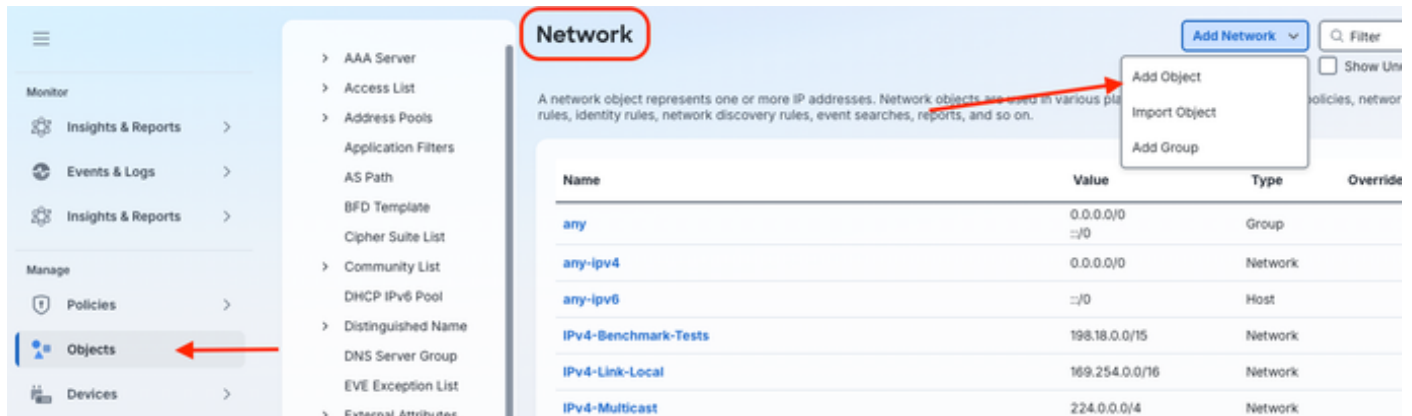
Dynamic Attributes Connector



Habilitar estado del conector de atributos dinámicos de Cisco

Paso 2: Creación de un Objeto de Red de Nombre de Dominio Totalmente Cualificado Representante de la Interfaz de Ingreso FTD

1) Elija Objects > Add Network > Add Object.



Crear nuevo objeto de red de nombre de dominio completamente calificado

2) Asigne al objeto de red un nombre configurado con el nombre de dominio completo (FQDN). Introduzca el FQDN y asigne el objeto de red como un tipo de FQDN haciendo clic en el botón de opción correspondiente. 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 variables de objeto de red FQDN

Paso 3: Configuración del registro A de DNS

1) El ejemplo que se muestra aquí utiliza Windows Server 2025; consulte la documentación del servidor de resolución de nombres específico según sea necesario.

	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



Nota: El cliente que realiza la autenticación activa debe poder resolver este registro A de DNS.

Fase 2: Configuración de la infraestructura de clave pública

Se puede utilizar una autoridad de certificación (CA) interna como la infraestructura de clave pública (PKI) para la configuración de autenticación activa. Cisco FMC y FTD requieren que la clave pública interna de la CA y la clave privada emparejada se carguen como un objeto de CA interna para realizar las operaciones de interceptación SSL y de descifrado y renuncia necesarias. Además, la CA interna debe ser de confianza en el explorador cliente desde el que se realiza la autenticación activa. Consulte la documentación del explorador cliente para comprobar cómo confirmar que el explorador confía en el certificado.

Paso 1: Importar el certificado de CA interna al FMC

1) Elija Objects > PKI > Internal CAs. Haga clic en Importar CA.



Nota: La CA interna también se puede crear directamente en el 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:



Nota: Dentro del contenido de este documento, aparece un espacio en blanco que cubre los diversos valores de campo en las imágenes y es intencional según la publicación de este documento. Los valores reales se reflejan para el entorno a medida que se configura.

Paso 2: Firmar el certificado de proveedor de servicios con la CA

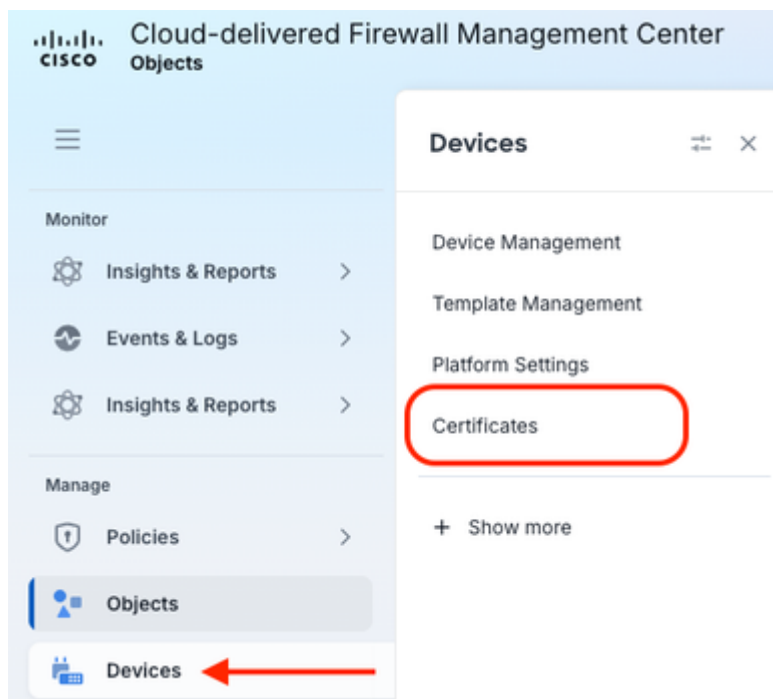
1) El certificado del proveedor de servicios (SP) debe estar firmado por una autoridad de certificación (CA) de confianza y devuelto en un formato PKCS#12 (.p12).



Nota: Esta CA se puede firmar internamente. La única advertencia es que el dispositivo cliente debe confiar en la CA interna.

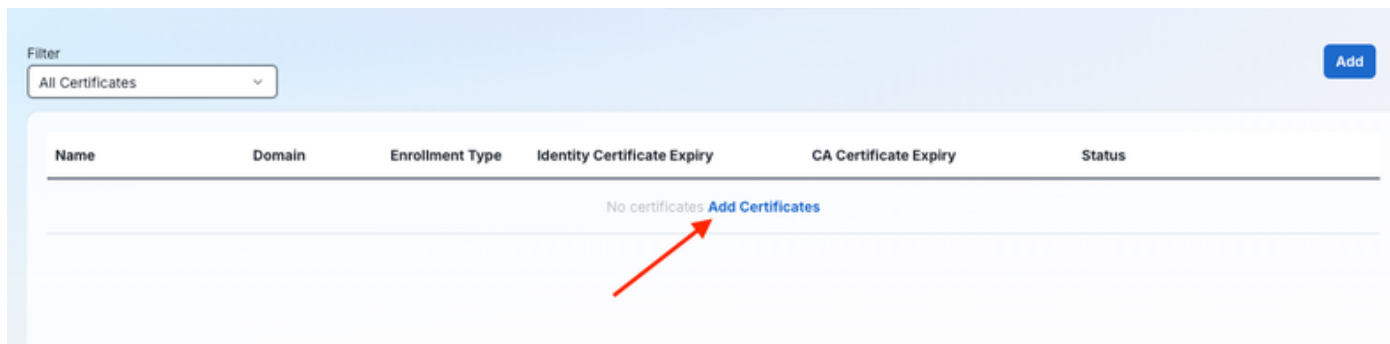
Paso 3: Implementación del certificado SP en el FTD

1) Elija Devices > Certificates.



Vaya A Dispositivos Y Certificados

2) Haga clic en Agregar certificados.



Agregar nuevo certificado de dispositivo

3) Haga clic en el dispositivo en la lista desplegable que ejecuta la autenticación activa y, a continuación, haga clic en el icono + para crear una nueva inscripción de certificados.

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 Y Agregar Inscripción de Nuevo Certificado

4) Asigne un nombre a la Inscripción de certificados y, en la lista desplegable Tipo de inscripción, seleccione Archivo PKCS12.

Add Certificate Enrollment ?

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:*

Challenge Password:

Confirm Password:

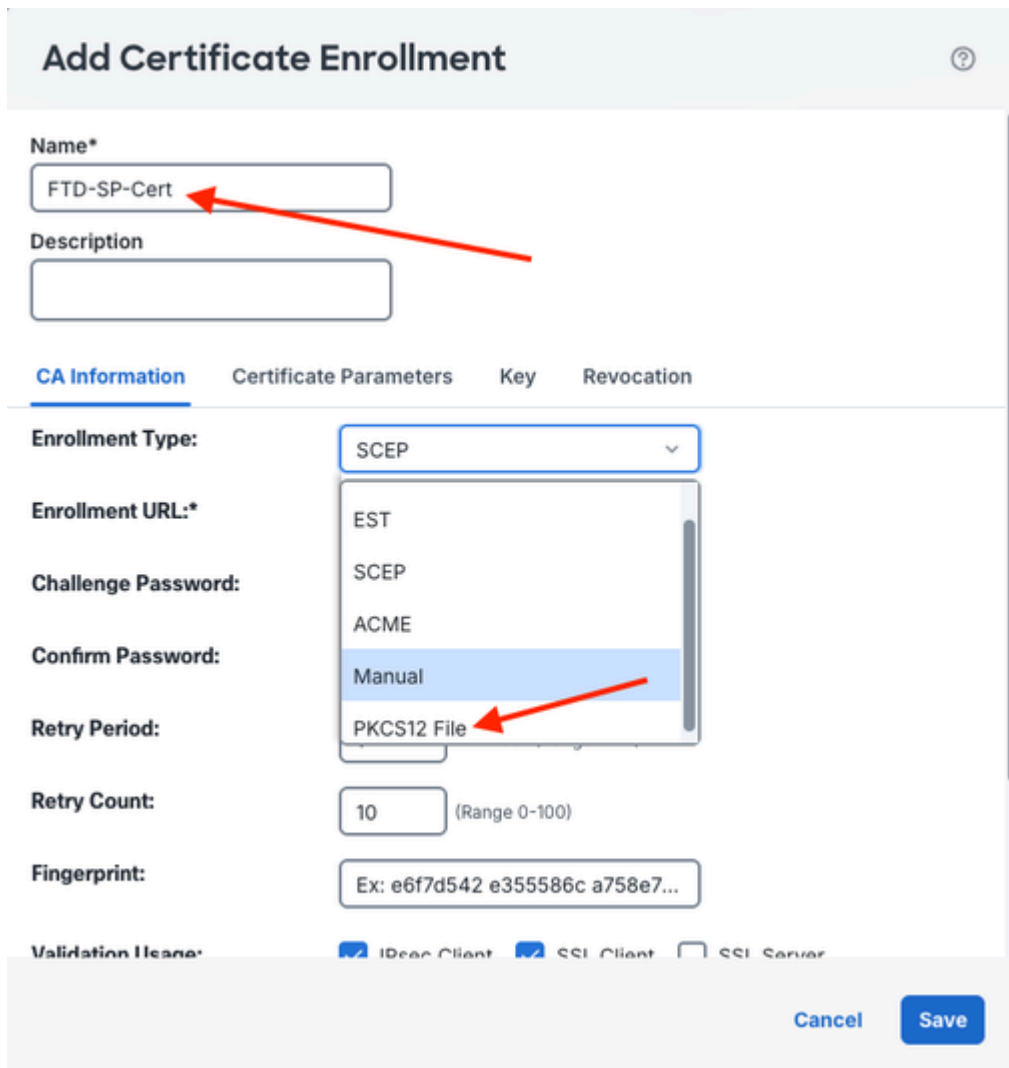
Retry Period:

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7...

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

Cancel Save



Configuración Y Tipo De Inscripción De Certificados

5) Importe el archivo PKCS#12 haciendo clic en Browse PKCS12 File e introduzca la frase de contraseña necesaria. 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

Examinar e importar archivo PKCS12

6) Confirme que los detalles de inscripción son correctos y haga clic en Agregar.

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 detalles de inscripción de certificados

7) La importación refleja En curso.

▼ FTD

FTD-SP-Cert

Global

PKCS12 file

In progress

Una vez completada la importación, la información del certificado SP se puede validar haciendo clic en el icono ID del certificado configurado.



A screenshot of a table showing certificate information. A red arrow points to the 'ID' icon in the 'Status' column for the 'FTD-SP-Cert' row.

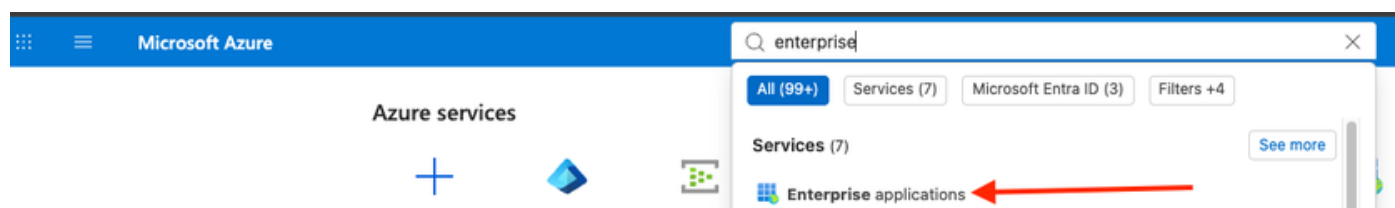
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
FTD-SP-Cert	Global	PKCS12 file	Dec 18, 2028	Sep 12, 2036	CA ID

Estado de importación de certificado en curso

Fase 3: Configuración de Azure

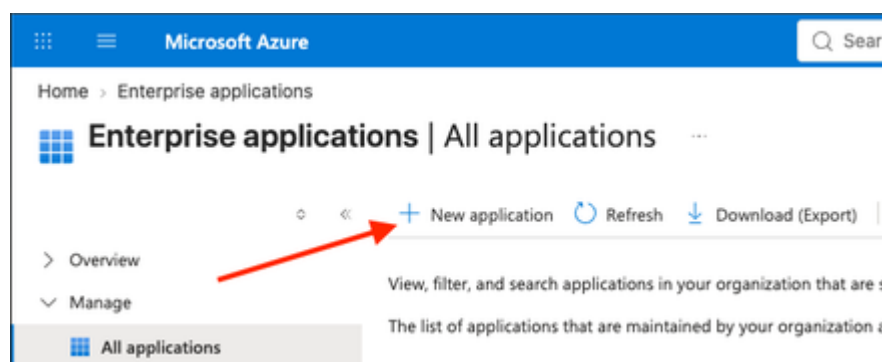
Paso 1: Crear la aplicación empresarial completa para el kit de herramientas de SAML

1) Busque y haga clic en Aplicaciones de empresa.



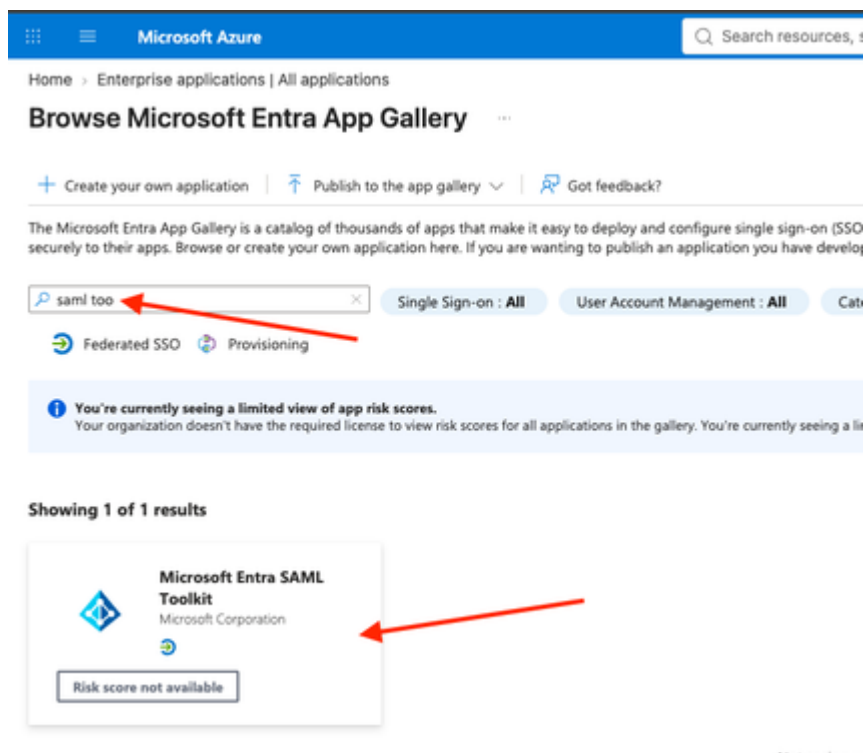
Búsqueda Y Acceso A Aplicaciones Empresariales

2) Haga clic en + Nueva aplicación.



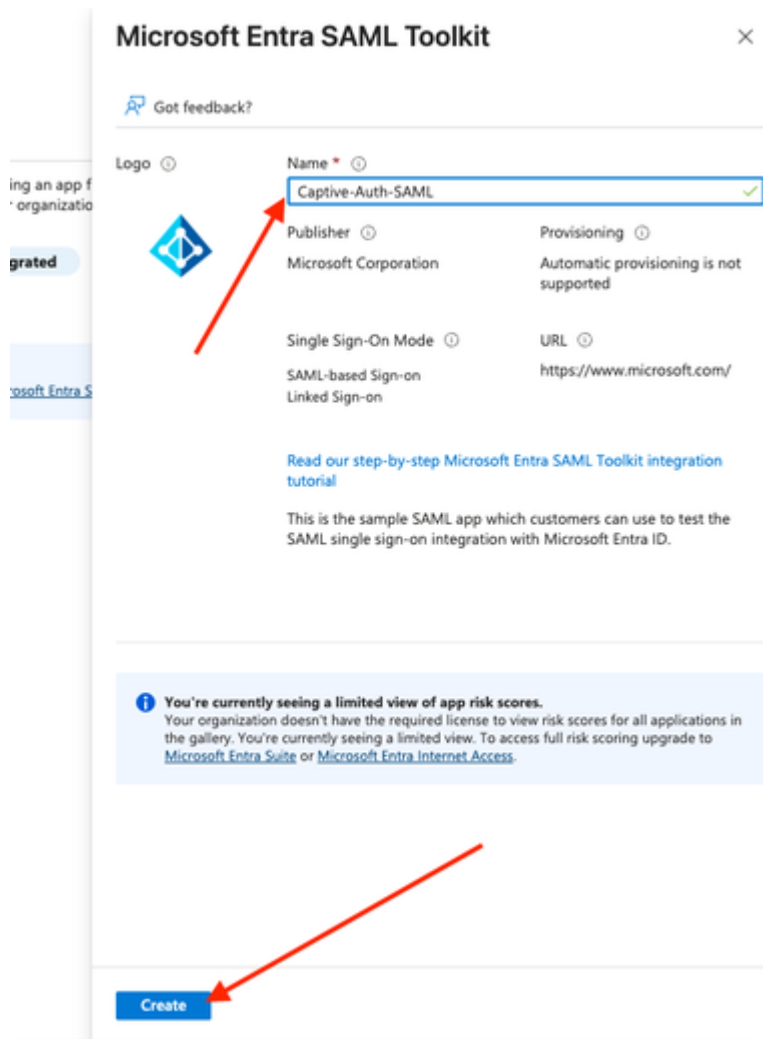
Seleccionar nueva aplicación en aplicaciones empresariales

3) Busque el Microsoft Entra SAML Toolkit y haga clic en la miniatura correspondiente.



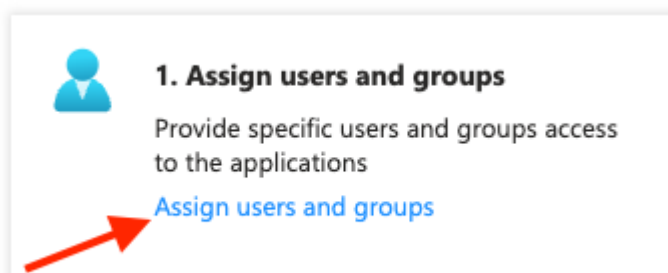
Busque y seleccione Microsoft Entra SAML Toolkit

4) Asigne un nombre a la aplicación Microsoft Entra SAML Toolkit Enterprise y haga clic en Create. (Referencia de Microsoft: [Lea nuestro tutorial paso a paso sobre la integración de Microsoft Entra SAML Toolkit](#)).



Asignar nombre a la aplicación SAML Toolkit

5) En la página Overview, asigne los usuarios y grupos específicos a la aplicación SAML Toolkit Enterprise. En este ejemplo, la cuenta de prueba (captive-portal-user) es miembro del grupo active-auth-lab.

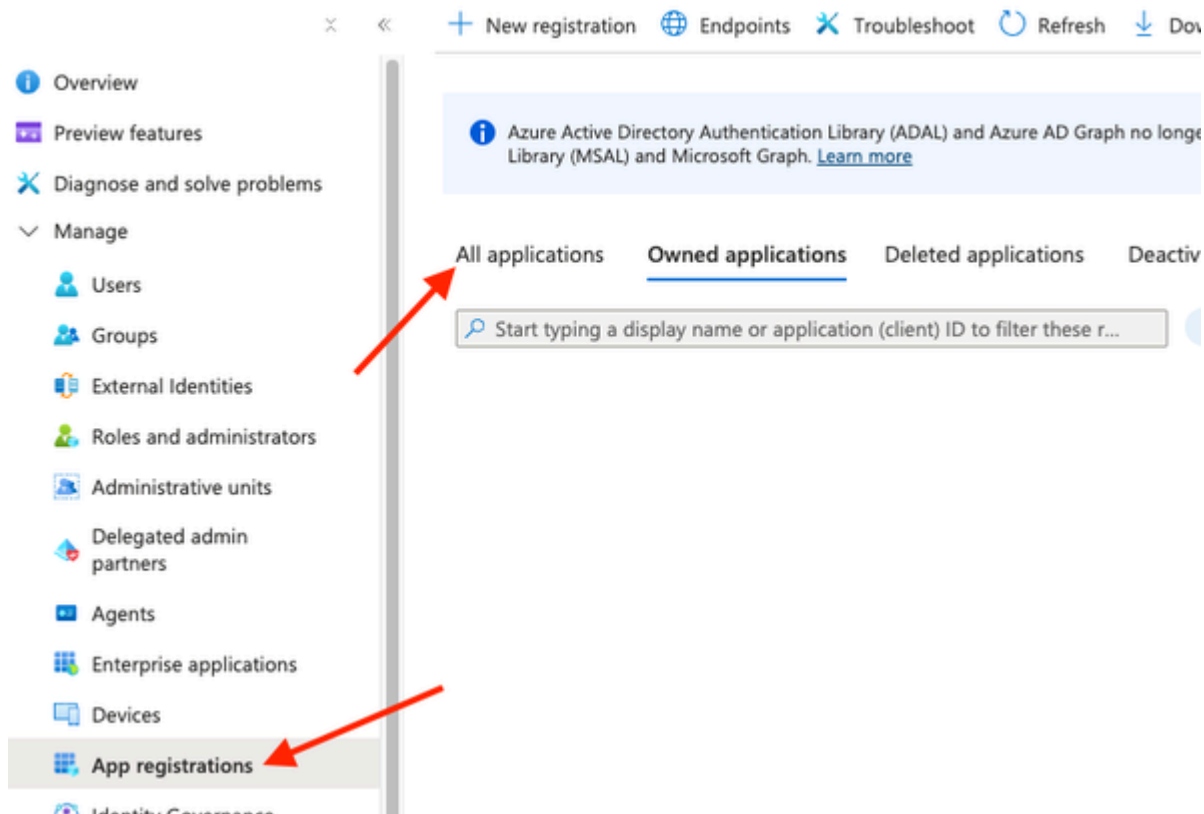


Asignar Usuarios Y Grupos A La Aplicación

6) La configuración de esta aplicación empresarial continúa en pasos posteriores.

Paso 2: Configurar registros de aplicaciones de ID de entrada

1) Navegue hasta Introducir ID y en el menú de navegación izquierdo, elija Registros de aplicaciones. Haga clic en el filtro Todas las aplicaciones y busque el nombre asignado a la aplicación de empresa. Haga clic en la aplicación correspondiente.



Desplácese Hasta Registros De Aplicaciones Y Todas Las Aplicaciones

2) Recopile y anote los valores esenciales en el registro de la aplicación empresarial.



Importante: Pase el ratón sobre los valores para mostrar Copiar al Portapapeles y recopile los valores en Essentials en la página Descripción general:

- Mostrar nombre:
- ID de aplicación (cliente)
- ID de directorio (arrendatario)

Captive-Auth-SAML

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previous)

Essentials

Display name : [Captive-Auth-SAML](#)

Application (client) ID :

Object ID :

Directory (tenant) ID :

Supported account types : [My organization only](#)

Recopilar Valores De Visualización E ID De Aplicación Y Directorio

3) Haga clic en el hipervínculo Agregar un certificado o secreto.

Captive-Auth-SAML

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : [Captive-Auth-SAML](#)

Application (client) ID :

Object ID :

Directory (tenant) ID :

Supported account types : [My organization only](#)

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [1 web, 0 spa, 0 public client](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in : [Captive-Auth-SAML](#)

State : [Activated](#)

Agregar certificado o hipervínculo secreto

4) Haga clic en + New client secret.

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

Roles and administrators

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable (scope). 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 (0) 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
No client secrets have been created for this application.			

Agregar nuevo secreto de cliente

5) Proporcione una descripción del secreto y ajuste la caducidad según sea necesario. Haga clic

en Add (Agregar).

Add a client secret

Description:

Expires: Recommended: 180 days (6 months)

Add **Cancel**

Proporcionar Descripción De Secreto De Cliente

6) Copie el secreto.



Importante: Tome nota del valor secreto copiado en el portapapeles.

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.

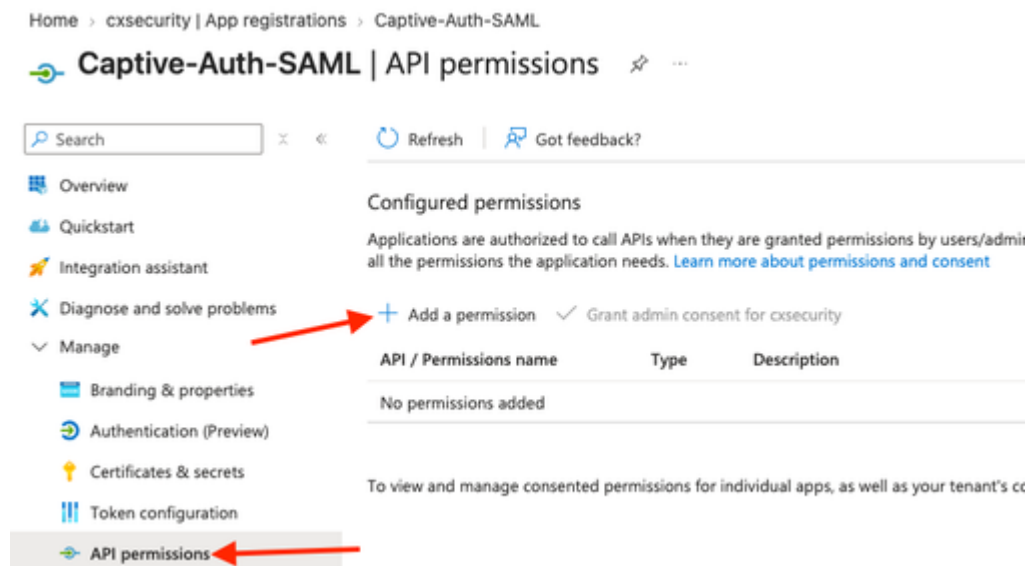
+ New client secret

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

Copiar valor secreto de cliente

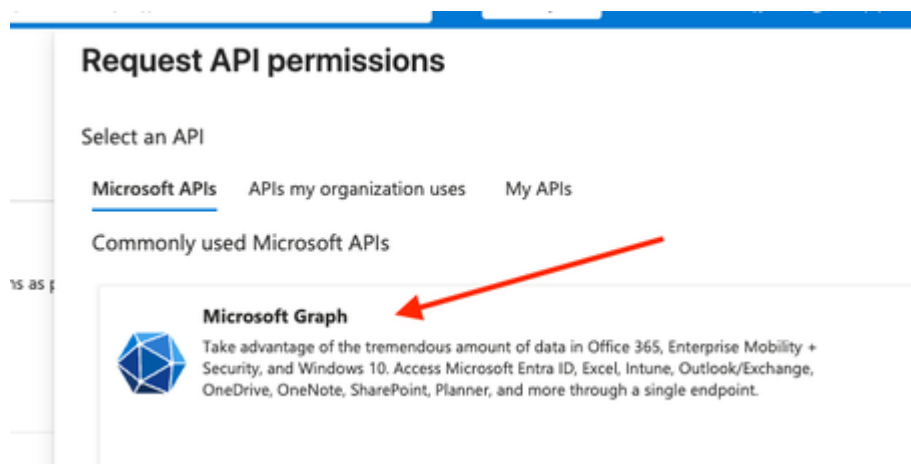
Paso 3. Configure los permisos de la API de Microsoft Graph para el registro de la aplicación.

1) Elija API Permissions en el menú de navegación izquierdo, luego haga clic en + Add a permission.



Configurar permisos de API

2) Haga clic en API de Microsoft Graph.



Seleccionar API de Microsoft Graph

3) Otorgue permisos Delegated User.Read y, a continuación, haga clic en 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 permisos de lectura de usuario delegado

4) Otorgar permisos User.Read.All a la aplicación (marque la casilla de verificación).

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

Conceder permisos de lectura de todos a una aplicación

5) Busque y marque la casilla de verificación Group.Read.All para conceder también permisos de lectura de grupo. Haga clic en Agregar permisos.

Select permissions

[expand all](#)

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

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

Guardar permisos de API

6) Confirme que los permisos configurados se alinean y conceda el consentimiento administrativo para ellos.

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 Consentimiento Administrativo Para Permisos

7) El resultado, una vez que se concede el consentimiento del administrador, se muestra.

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

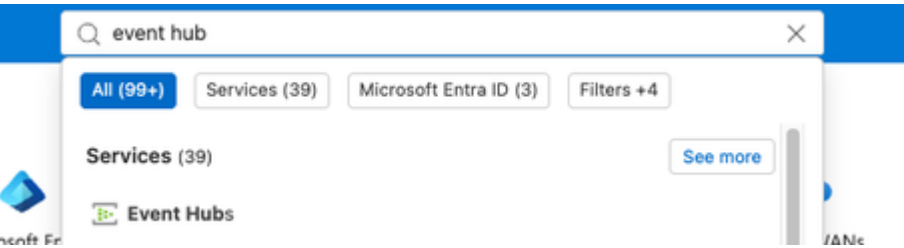
✓ Grant admin consent for

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

Resultado de consentimiento administrativo concedido

Paso 4: Configuración del espacio de nombres del Event Hub (EH)

1) Busque y haga clic en Event Hubs.



Buscar configuración de Event Hub

2) Crear un nuevo espacio de nombres 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](#)

Crear espacio de nombres de Event Hub

3) Configure el espacio de nombres EH.



Nota: Se debe elegir el nivel de precios Standard o superior. El nivel de precios básico impide el uso del dominio.

Consulte la [Documentación de Azure Event Hub](#) para obtener más información sobre la configuración avanzada de Event Hub y la aplicabilidad a necesidades específicas.

Haga clic en Revisar + Crear.



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 * ☒
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 >

Configuración de espacio de nombres de Event Hub

4) Una vez validada correctamente, haga clic en 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 >

Crear implementación de espacio de nombres de Event Hub

5) Confirme que la implementación se ha completado y, a continuación, haga clic en Ir al recurso.

Home

captive-auth-ad-eh | Overview

Deployment

Search x <<

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

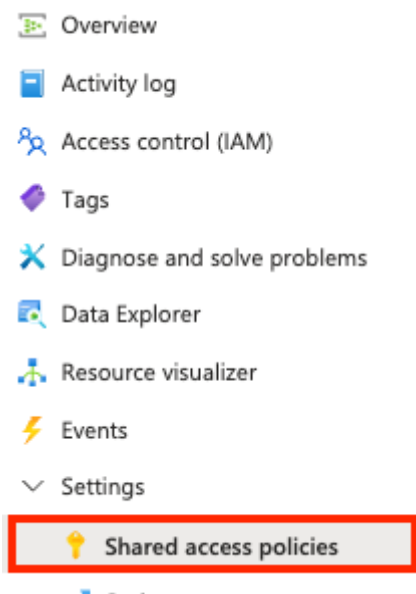
Go to resource

Ir al recurso de espacio de nombres del centro de eventos

Paso 5: Elija o cree políticas de acceso compartido en el espacio de nombres del centro de

eventos

1) En el menú de navegación izquierdo, elija Settings > Shared access policies.



Desplácese Hasta Políticas De Acceso Compartido

2) Haga clic en + Add e ingrese el nuevo nombre de la política, y marque la casilla de verificación Manage. Haga clic en Create en la parte inferior del panel de menú Add SAS Policy.



Agregar nueva directiva de acceso compartido



Crear directiva de acceso compartido

Paso 6: Recopilar y anotar información de firmas de acceso compartido (SAS) del espacio de

nombres EH

1) Haga clic en la nueva política de acceso compartido; la política EH SAS aparece en el panel lateral de la derecha.

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: ADM ID

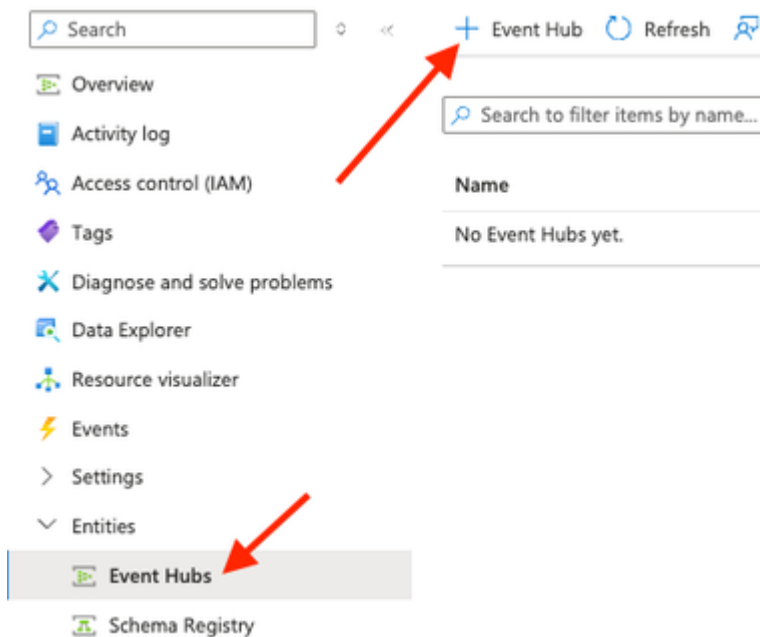
Copiar cadena de conexión principal



Importante: Copie y anote la cadena de conexión principal.

Paso 7: Creación de una instancia del Event Hub en el espacio de nombres del Event Hub

1) En el menú Namespace, elija Entities > Event Hubs. Haga clic en + Event Hub para crear una nueva instancia EH.



Crear nueva instancia de Event Hub

2) Asigne un nombre a la nueva instancia de EH y, a continuación, haga clic en Revisar + crear.

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 >

Asignar nombre a la instancia del centro de eventos

3) Una vez validada correctamente, haga clic en Create para aprovisionar la instancia del Event Hub.

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 >

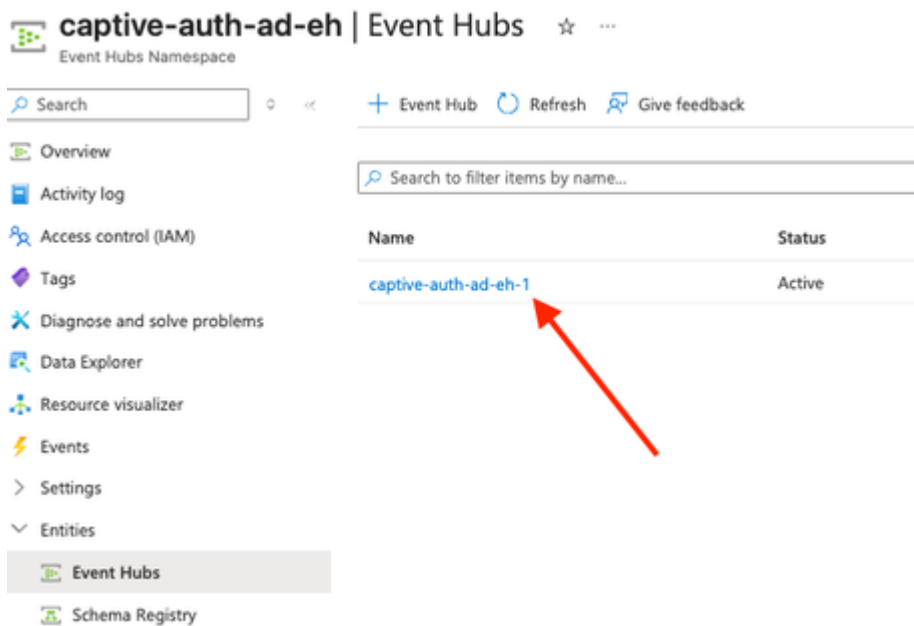
Aprovisionar instancia del Event Hub



Importante: Copie y anote el nombre de la instancia del Event Hub.

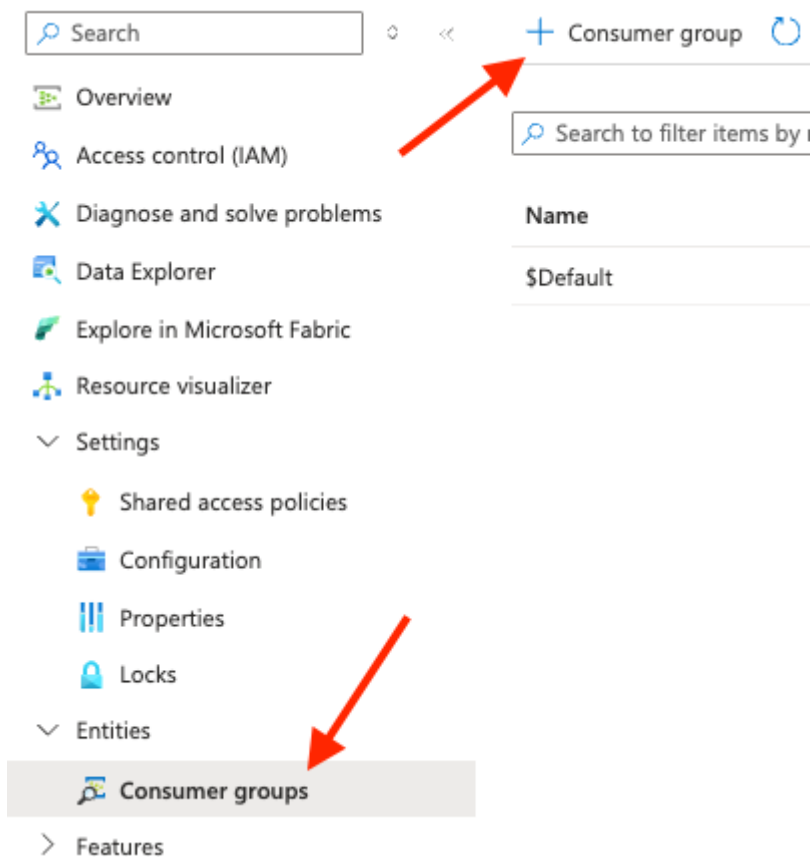
Paso 8: Creación de un grupo de consumidores de instancias de Event Hub en el espacio de nombres del Event Hub

1) Haga clic en la nueva instancia EH configurada en el paso anterior.



Configuración de instancia de Event Hub de acceso

2) En la instancia EH, elija Entities > Consumer groups, y cree un nuevo grupo Consumer.



Crear grupo de consumidores

3) Asigne un nombre al grupo de consumidores y haga clic en Crear.

Create consumer group ×

Consumer groups

Name *

captive-auth-ad-eh-cg



Create

Asignar nombre a grupo de consumidores



Importante: Copie y anote el nombre del grupo de consumidores de la instancia del Event Hub.

Paso 9: Verificar valores recopilados

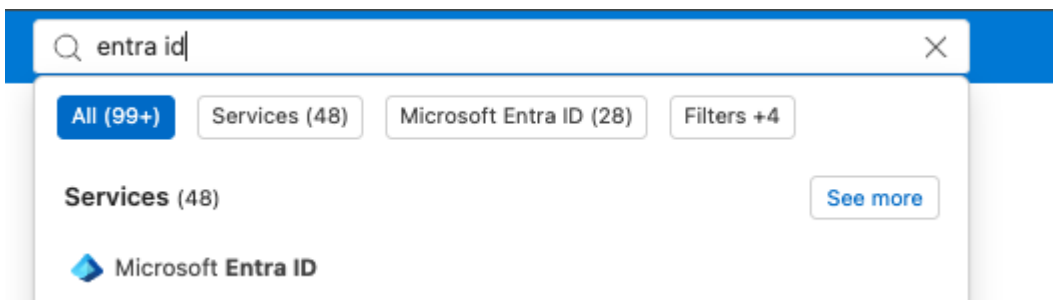
1) En este punto, deben anotarse estos valores de los pasos anteriores. Si no se ha registrado ningún valor, haga referencia al paso aplicable en el que se recopila:

- Fase 3 Paso 2 - Registro de aplicaciones (de la aplicación empresarial creada para este proceso, a la que hace referencia el nombre para mostrar recopilado)
 - Paso 2, subpaso 2
 - Mostrar nombre:
 - ID de aplicación (cliente)
 - ID de directorio (arrendatario)
 - Paso 2, subpaso 6
 - Secreto del cliente
- Fase 3 Paso 6: Event Hub
 - Paso 6, subpaso 1
 - Espacio de nombres EH

- Cadena de conexión principal
- Paso 7, subpaso 3
 - Nombre de instancia EH (Event Hub)
- Paso 8, subpaso 3
 - Nombre del grupo de consumidores EH

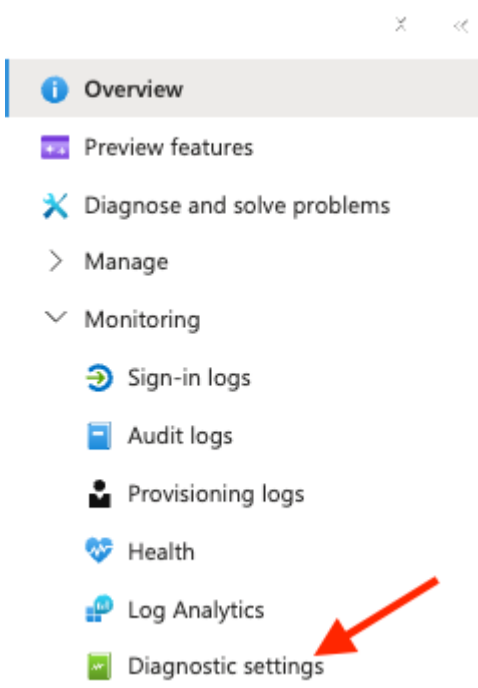
Paso 10: Configuración de la transmisión del registro de auditoría de Intra ID al Event Hub

1) Vuelva a la configuración de arrendatario de ID de entrada.



Busque Y Navegue Hasta Introducir La Configuración De Arrendatario De Id.

2) En el menú de la izquierda, elija Monitoring > Diagnostic Settings.



Supervisión de configuración de diagnóstico

3) Elija Diagnostic settings > General y haga clic en + Add diagnostic settings.



 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

Agregar nueva configuración de diagnóstico

4) Asigne el nombre necesario a la configuración de diagnóstico, marque la casilla de verificación AuditLogs para registrar y marque la casilla de verificación Stream to an event hub. Haga referencia a los valores indicados de las configuraciones anteriores y haga clic en Guardar cuando haya terminado.

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 *

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 *

Event hub name (optional)

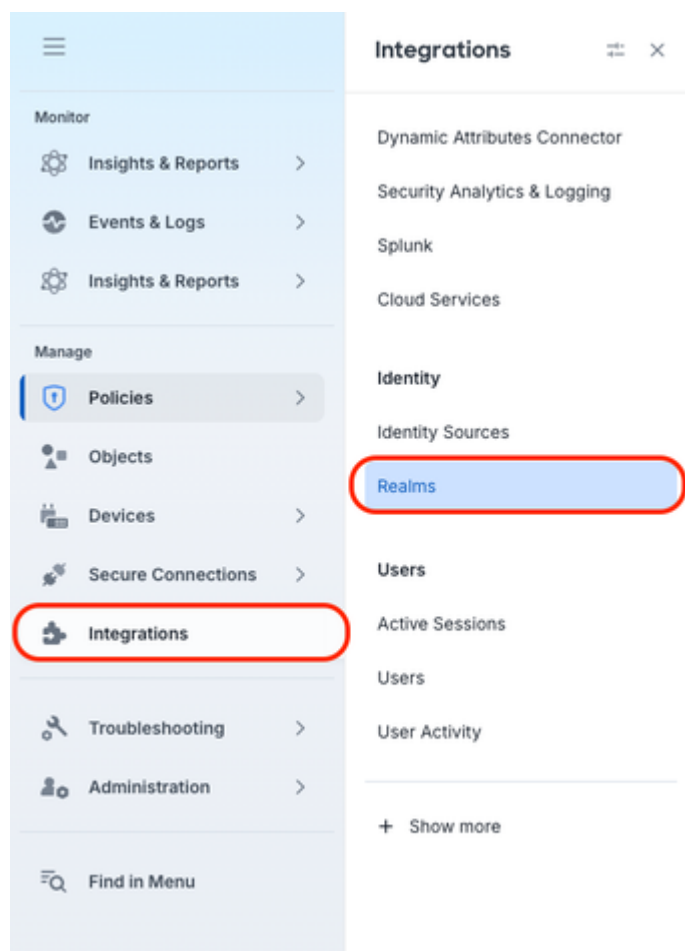
Event hub policy name

- ☐ Send to partner solution

Fase 4: Consolidar configuración de autenticación activa de Azure y FMC/FTD

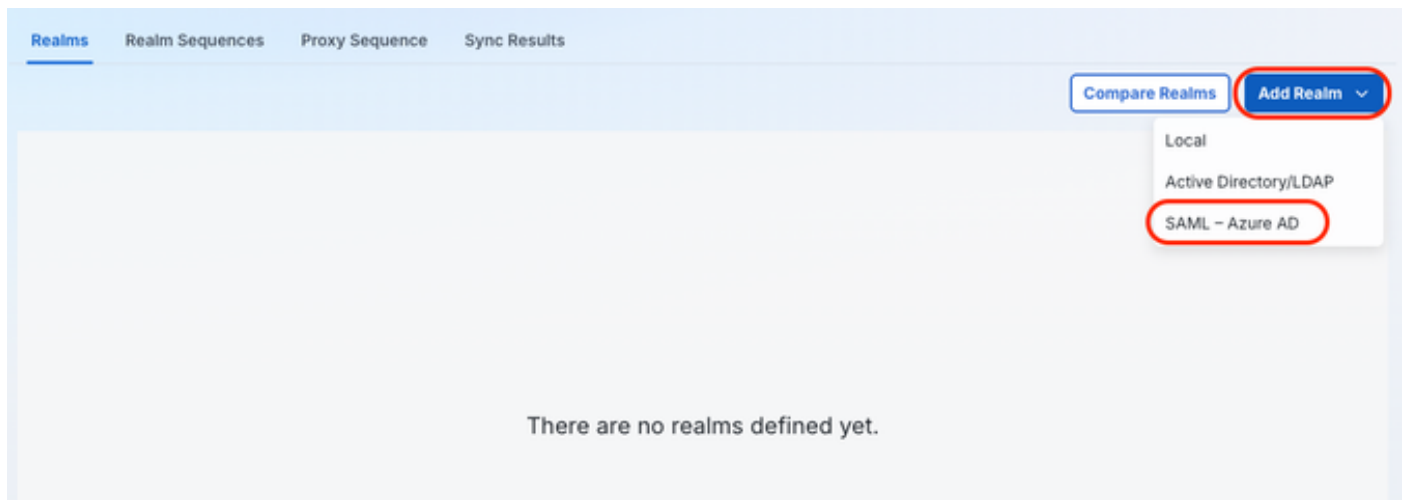
Paso 1: Configuración del rango de ID de Azure SAML/Entra mediante el Asistente de FMC

1) En el FMC, seleccione Integrations > Identity > Realms.



Configuración de rangos de identidad

2) Haga clic en Agregar rango lista desplegable, y elija SAML - Azure AD.



Agregar rango de SAML Azure AD

3) Asigne un nombre y una descripción al rango de Azure para describir su uso, y asegúrese de que Autenticar pasivamente con Azure AD o usando el portal cautivo con Azure AD se elija de la lista desplegable Tipo de configuración. Haga clic en Next (Siguiente).

Configurar Azure AD Realm Settings

4) Elija el objeto FQDN configurado anteriormente como URL base. Ingrese el Id. de entidad con el formato de cadena que se muestra:

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

- Cuando se configura el sufijo ID de entidad SAML (subrayado en verde en el siguiente ejemplo de configuración), asegúrese de que el sufijo sea único entre otras implementaciones de SSO dentro del entorno. Este valor también debe coincidir con la configuración SAML de Azure. La URL base permanece igual durante toda la configuración.
- La URL de Assertion Consumer Services (ACS) se rellena automáticamente y es inmutable.
- Elija el certificado de proveedor de servicios (SP) inscrito en los pasos anteriores del flujo de trabajo en FMC en Dispositivos > Certificados.
- Después de ingresar estos valores, haga clic en Descargar metadatos del proveedor de servicios para facilitar el proceso de configuración y confirmar que los valores esperados se escriben en 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

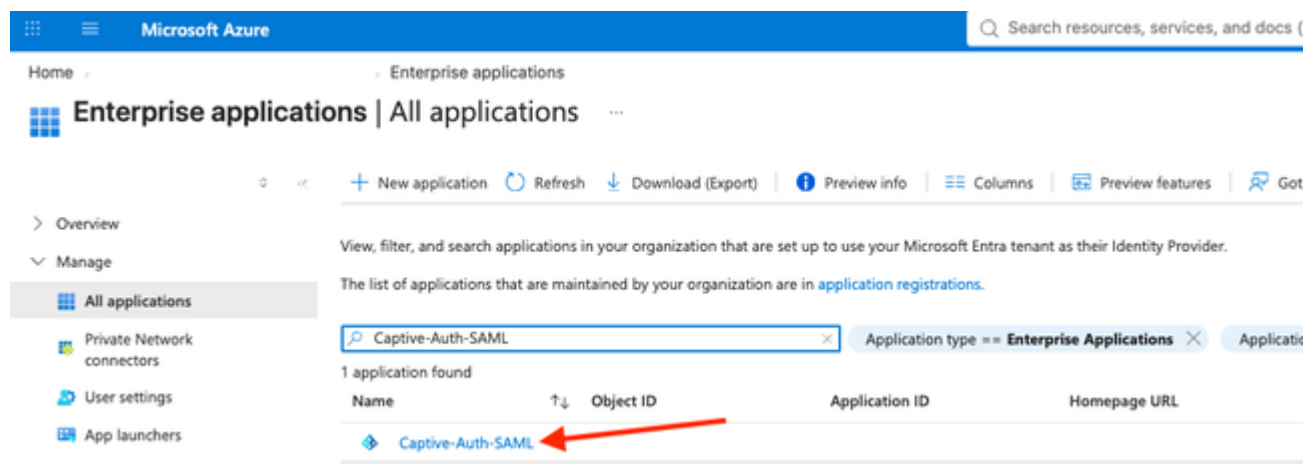
Next

Configuración de URL base e ID de entidad y descarga de metadatos SAML

5) Haga clic en Next para pasar a la secuencia 3 de la configuración de rango.

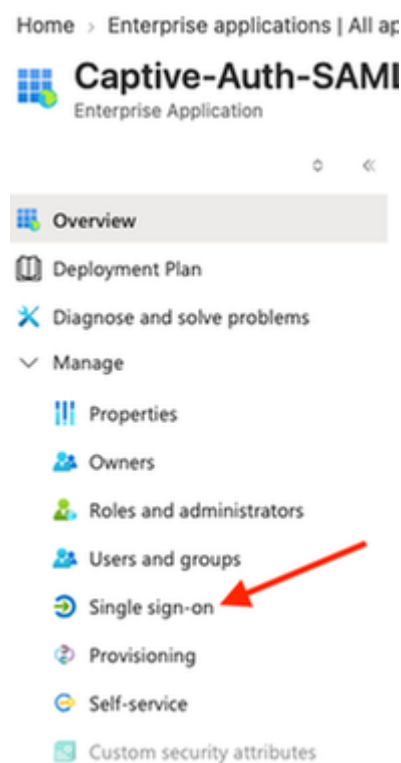
Paso 2: Implementar los metadatos SP de SAML configurados en FMC en la aplicación empresarial de Azure

1) Vuelva a Azure y elija Entra ID > Manage > Enterprise Applications. Busque la instancia creada anteriormente de la aplicación Microsoft Entra SAML Toolkit Enterprise.



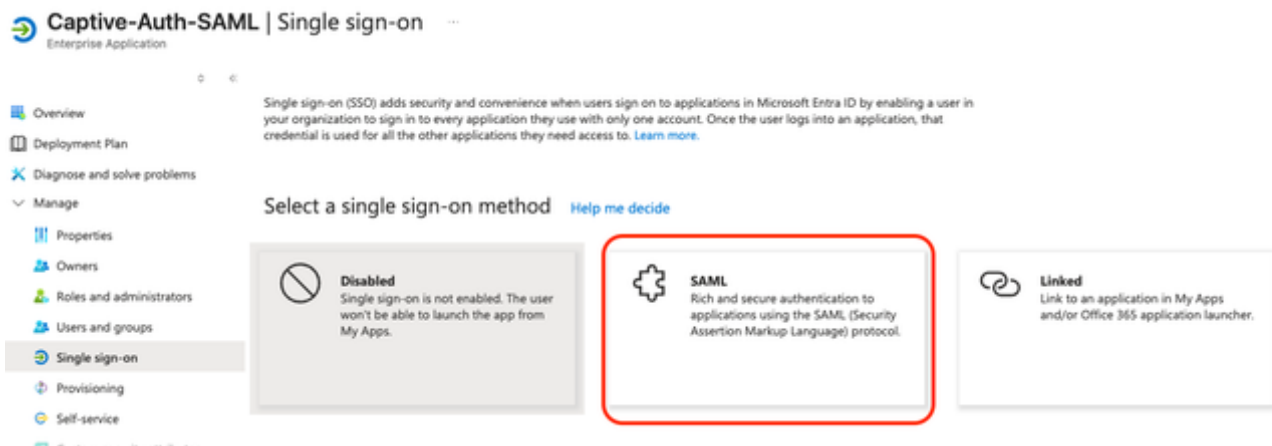
Localizar la aplicación Microsoft Entra SAML Toolkit

2) En el menú de navegación lateral, elija Manage > Single Sign-On.



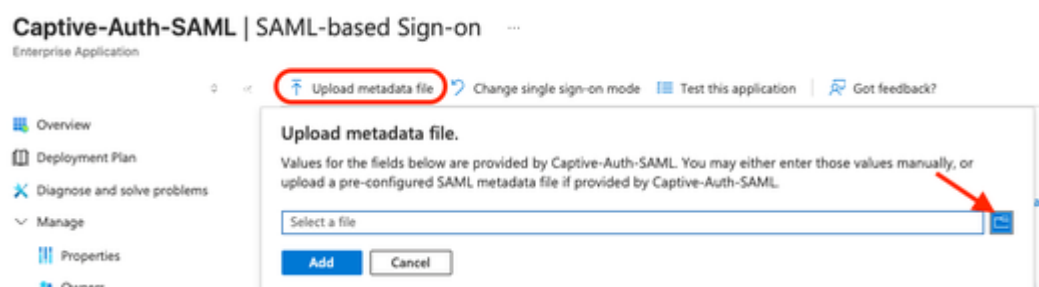
Administrar configuración de inicio de sesión único

3) Haga clic en el modo SAML Single Sign-On (SSO).



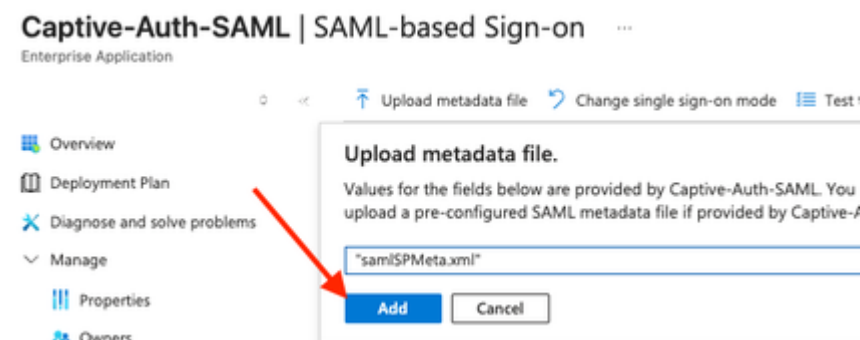
Selección del modo de inicio de sesión único SAML

4) Haga clic en Cargar archivo de metadatos y haga clic en el icono de carpeta azul para examinar el sistema de archivos local en busca del archivo de metadatos SAML descargado desde el FMC.



Cargar Archivo De Metadatos Desde Firewall Management Center

5) Una vez completada la carga, haga clic en Add.



Agregar aplicación de configuración SAML

6) Aparece el panel lateral para la configuración básica de SAML, y los valores como el identificador (Id. de entidad) y la URL ACS se extraen del archivo XML de metadatos SP originado en FMC y se cargan y aplican automáticamente. Sin embargo, la URL de inicio de sesión no se rellena y es necesaria antes de guardar.

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.



Extracción de configuración básica de SAML

7) Utilice el patrón de URL de inicio de sesión proporcionado, copie y pegue el valor y haga clic en

Guardar en la parte superior cuando haya terminado.

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.



Entrada de configuración de URL de inicio de sesión

Desplácese hasta SAML Certificates y exporte el archivo Federation Metadata XML generado por

Azure para importarlo a Cisco Secure FMC.

Exportar archivo XML de metadatos de federación

Paso 3: Configuración del rango de ID de Azure SAML/Entra mediante el asistente de FMC (continuación)

1) Vuelva al CSP. En Secuencia 3, Metadatos del proveedor de identidad SAML (IdP), cargue el archivo XML de metadatos de federación exportado y descargado de Azure en el FMC para rellenar automáticamente los valores necesarios.

Cargar archivo XML de metadatos de federación

2) Una vez cargados, los valores se rellenan como se muestra.

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

Valores del proveedor de identidad SAML rellenados automáticamente



Nota: La imagen muestra una salida parcial.

3) Introduzca los valores recopilados durante todo el proceso de implementación hasta este punto:

- Registro de aplicaciones
 - ID de aplicación (cliente)
 - Secreto del cliente
 - ID de directorio (arrendatario)
- Centro de eventos
 - EH Namespace Hostname
 - Cadena de conexión principal de espacio de nombres EH
 - Nombre de instancia EH (Event Hub)
 - Nombre del 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.windo

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/;SharedAccessKeyNi

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

Introducir Información De La Aplicación Y Del Centro De Eventos

Una vez ingresado, haga clic en Test para verificar la conexión y confirmar que Azure es accesible con la información proporcionada.



Nota: Si procede, asegúrese de que los grupos de usuarios excluidos/incluidos se corresponden con su configuración de Entrar

4) El paso final del asistente le permite configurar el tiempo de espera de los usuarios del portal cautivos de SAML. El valor predeterminado es 1440 minutos.

5 User Session Timeout

SAML Captive Portal Users

1440 Minutes Range 0-35791394

Configurar tiempo de espera del portal cautivo

5) Haga clic en Next 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

Avanzar con la configuración de Azure AD Realm

6) El asistente proporciona un resumen de la configuración implementada. Haga clic en Guardar al final del resumen una vez validados y confirmados los valores introducidos.

5 User Session Timeout Edit

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

Cancel Save

Botón Guardar Resumen de Configuración de Rango

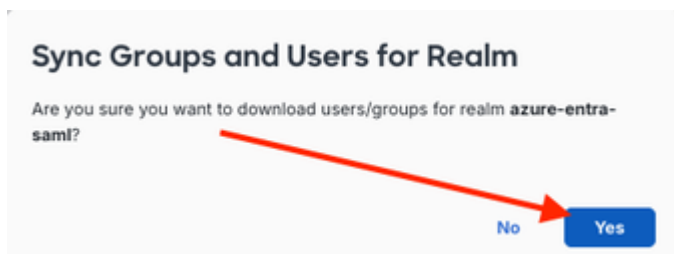
Paso 4: Comprobar usuarios descargados

1) Confirme que los usuarios se pueden descargar de Azure Entra con el botón Download Now dentro del flujo de trabajo de Integrations > Identity > Realms.

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

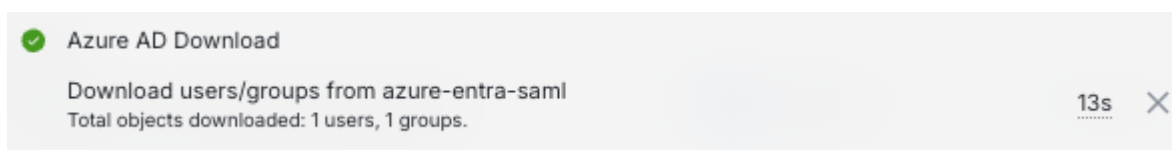
Descargar usuarios de Azure AD

2) Haga clic en Sí en respuesta al mensaje del cuadro de diálogo.



Confirmar La Descarga De Usuarios Desde Azure AD

3) La tarea de descarga produce 1 usuario y 1 grupo descargados, como se confirma en Notificaciones > Tareas.

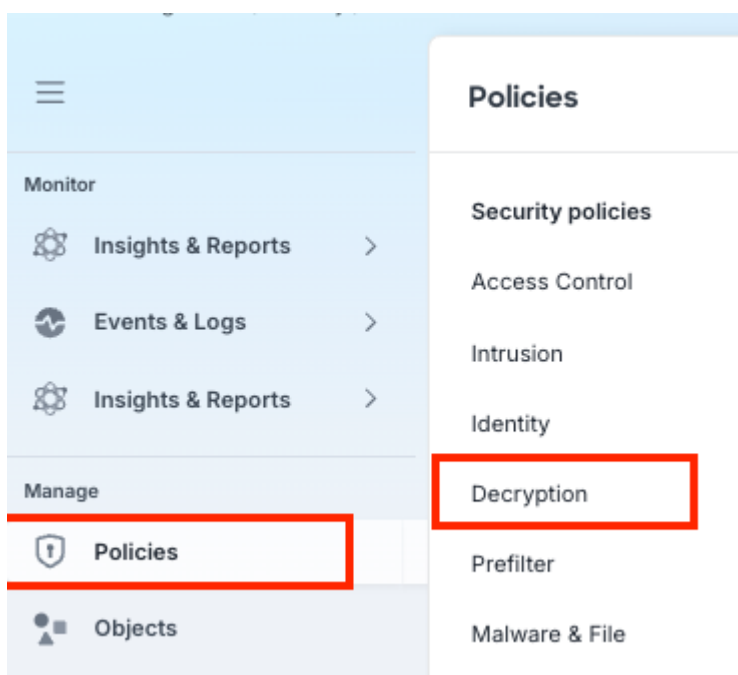


Entrada de notificación para la descarga de usuarios desde Azure AD

Fase 5: Configuración de políticas en el FMC

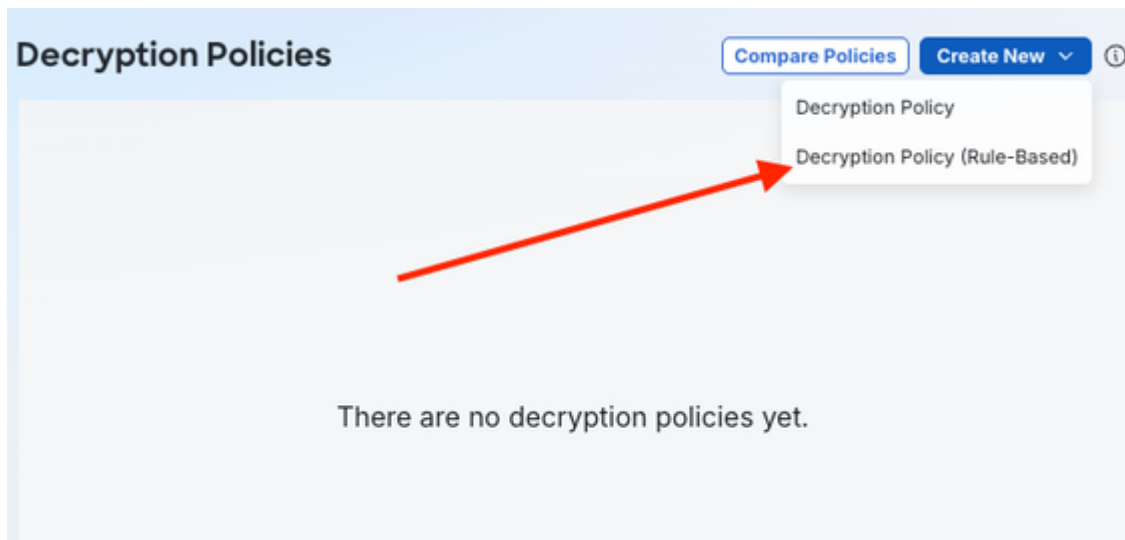
Paso 1: Configurar política de descifrado

1) En el FMC, seleccione Policies > Security Policies > Decryption.



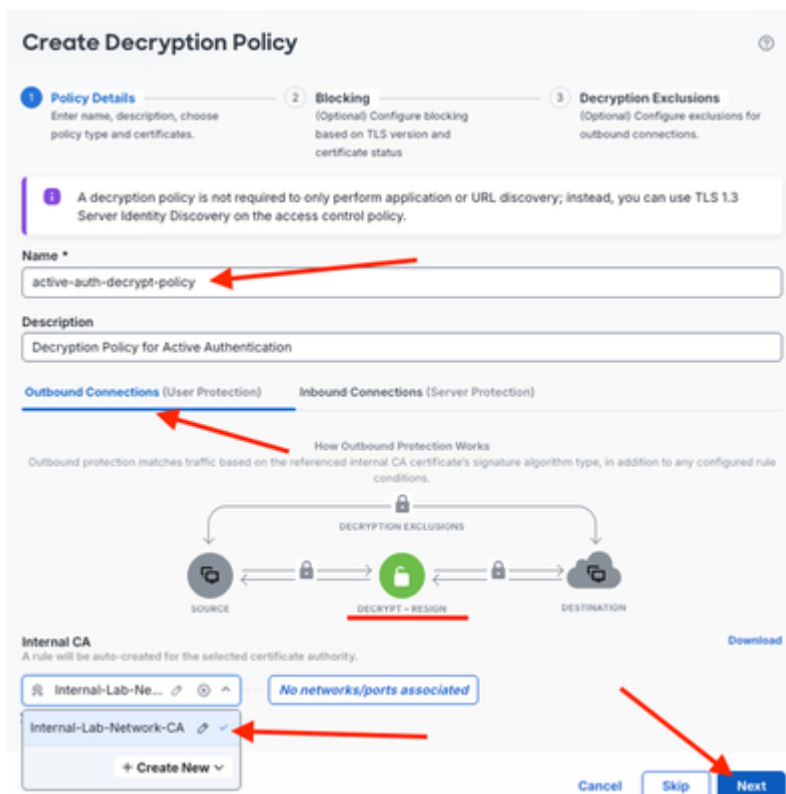
Desplazarse A La Política De Descifrado

2) Haga clic en la lista desplegable Create New y elija Decryption Policy (Rule-Based).



Crear nueva política de descifrado basada en reglas

3) Asigne un nombre y, si lo desea, una descripción a la nueva política de descifrado basada en reglas, y haga clic en la opción de pestaña Outbound Connections (User Protection) para implementar la funcionalidad Decrypt-Resign necesaria para la autenticación del portal cautivo (Active Authentication).



Implementar detalles de directiva de conexiones salientes

4) Elija la CA interna aplicada anteriormente de su lista desplegable aplicable en el mismo

diálogo. Haga clic en Next (Siguiente).

5) Personalice las opciones según sea necesario.

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 opciones de directiva de descifrado

6) En este ejemplo, se utilizan los valores por defecto, excepto los detalles de política necesarios. Complete el asistente de configuración haciendo clic en Create Policy.

Create Decryption Policy

1 Policy Details

2 Blocking

3 Decryption Exclusions

Enter name, description, choose policy type and certificates.

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

(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

Crear política de descifrado final

Paso 2: Configurar reglas de directiva de descifrado

1) Aquí se muestra el diseño predeterminado de una política de descifrado basada en reglas. El tráfico que no coincide con las reglas habilitadas predeterminadas, como la regla 3 (que hace referencia a una lista preasignada de nombres de dominio no descifrables) y la regla 6 (que hace referencia a aplicaciones etiquetadas como no descifrables), está sujeto a la acción Descifrar - Renunciar de la regla 7. Estos valores predeterminados, junto con la acción predeterminada, se pueden modificar según sea necesario. De forma predeterminada, el tráfico que no coincide con ninguna otra regla se configura como No descifrar.

El tráfico del Servicio de autenticación de Azure no se debe descifrar para inspección, por lo que se crea una regla dedicada para él. Haga clic en + Agregar regla para comenzar.

active-auth-decrypt-policy Save Cancel

Decryption Policy for Active Authentication

[Rules](#) [Trusted CA Certificates](#) [Undecryptable Actions](#) [Advanced Settings](#)

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

#	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

Agregar Regla Y Mostrar Diseño De Descifrado Basado En Regla Predeterminado

2) Asigne un nombre a la nueva entrada de regla de política de descifrado, elija No descifrar en la lista desplegable Acción y coloque la regla en la parte superior de las reglas menos específicas. Las zonas de origen y destino también se implementan para restringir aún más la regla.

Add Rule

Name: ☒ Enabled

Action:

Insert:

[Zones](#) [Networks](#) [VLAN Tags](#) [Users](#) [Client Threat](#) [Applications](#) [Ports](#) [Category](#) [Certificate](#) [DN](#) [Cert Status](#) [Cipher Suite](#) [Version](#) [Logging](#)

Available Zones

- Inside_Zone
- Outside_Zone
- DMZ_Zone

Source Zones (1):

Destination Zones (1):

Configurar regla de no descifrado

3) Antes de agregar la regla, haga clic en la pestaña Applications, busque y haga clic en la

aplicación Azure Authentication Service. Haga clic en Add to Rule y, a continuación, haga clic en 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 Available Applications (2) Search by name: azure a

Risks (Any Selected): Very Low (809), Low (715), Medium (2239), High (1823), Very High (609). Business Relevance (Any Selected): Very Low (609).

All apps matching the filter: Azure Arc, Azure Authentication Service

Add to Rule

Selected Applications and Filters (0): any

Cancel Add

Agregar regla de aplicación del Servicio de autenticación de Azure

4) Haga clic en Save.

active-auth-decrypt-policy

Decryption Policy for Active Authentication

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

You have unsaved changes Save Cancel

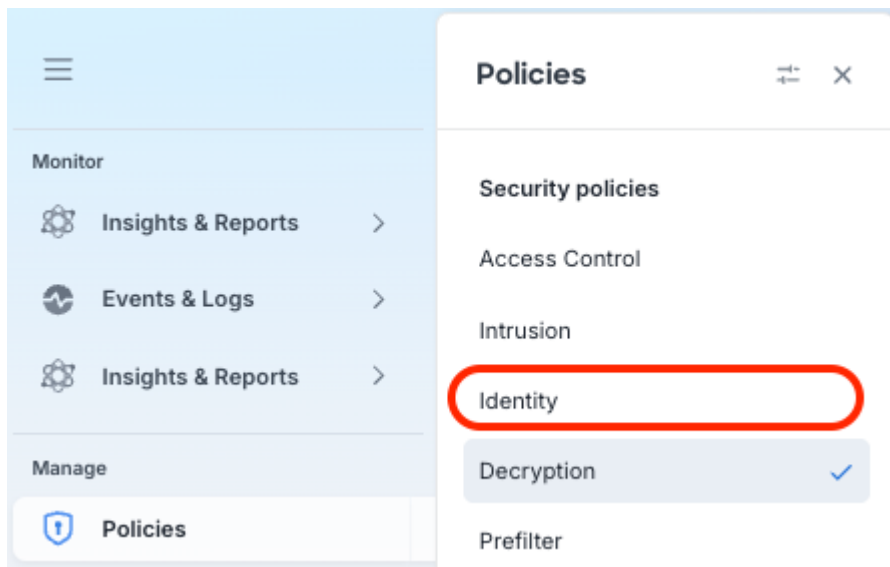
+ Add Category + Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	Categories	SSL	Action
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

Guardar política de descifrado

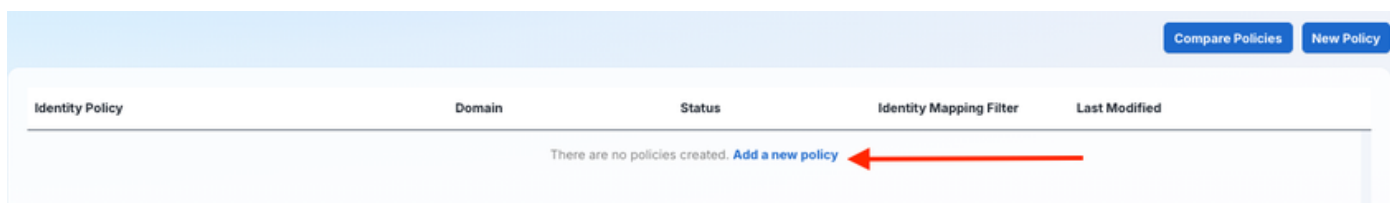
Paso 3: Crear política de identidad

1) Elija Policies > Security Policies > Identity para crear una política de identidad.



Crear política de identidad

2) Cree una nueva política de identidad y haga clic en Agregar una nueva política.



Agregar nueva configuración de política de identidad

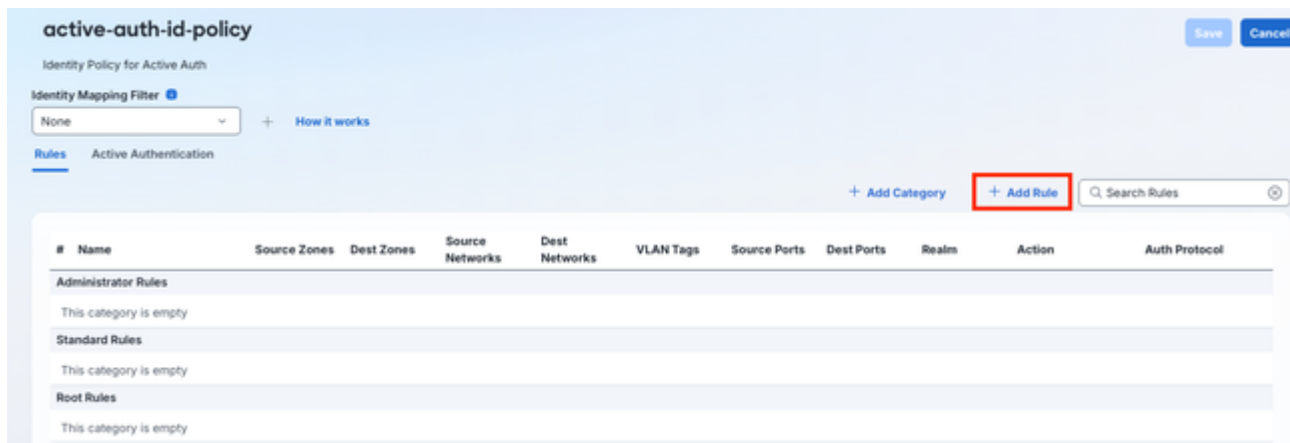
3) Asigne un nombre y, si procede, una descripción a la nueva política de identidad. Click Save.

A screenshot of a 'New Identity policy' form. It has two input fields: 'Name' with the value 'active-auth-id-policy' and 'Description' with the value 'Identity Policy for Active Auth'. At the bottom are 'Cancel' and 'Save' buttons. A red arrow points to the 'Save' button.

Nombre Nueva política de identidad

Paso 4: Configurar reglas de directiva de identidad

1) Agregue una nueva regla haciendo clic en + Add Rule.



Agregar nueva regla de política de identidad

2) Asigne un nombre a la nueva regla, elija Active Authentication en la lista desplegable Action y limite las zonas/redes específicas que deben coincidir con la regla para realizar la autenticación activa.

Configuración de la regla de autenticación activa

3) Antes de hacer clic en Add, haga clic en la pestaña Realm and Settings en el Editor de reglas. Confirme que el rango configurado en los pasos anteriores se elija como el rango de autenticación, luego haga clic en Agregar.

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

Configurar El Rango Y La Configuración De La Regla De Identidad

4) Se agrega y configura la regla. 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](#)

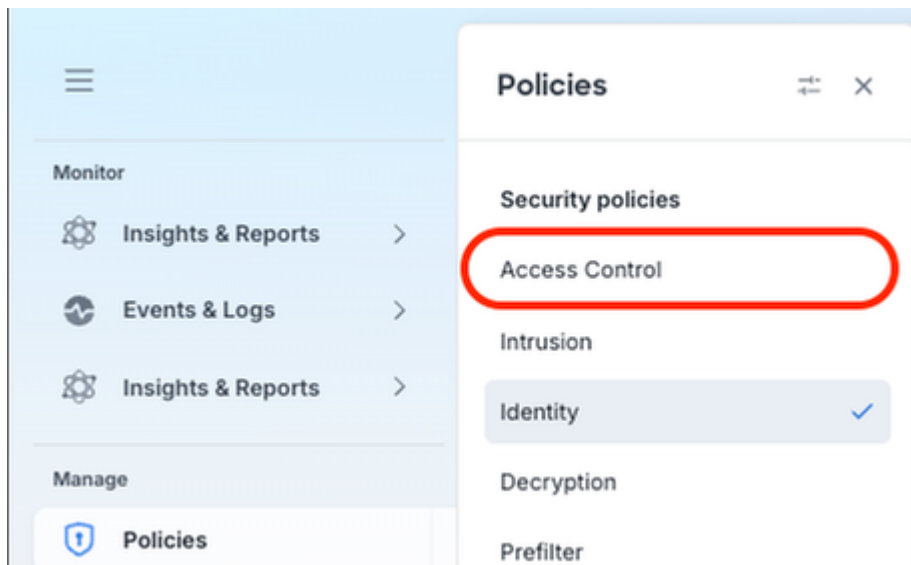
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	Active Auth ID Rule	Inside_Zone (Ro	Outside_Zone (f	any	any	any	any	any	azure-entra-san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

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

Guardar configuración de regla de política de identidad

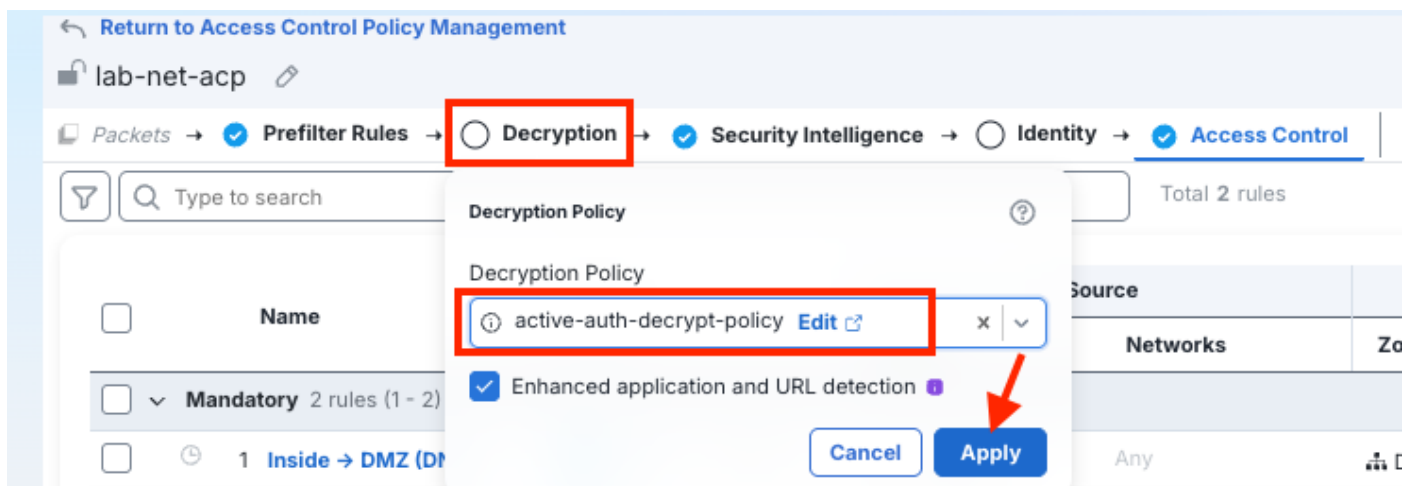
Paso 5: Configuración de la política de control de acceso

1) Elija Policies > Security Policies > Access Control, y haga clic en la Access Control Policy a la que se asigna el FTD.



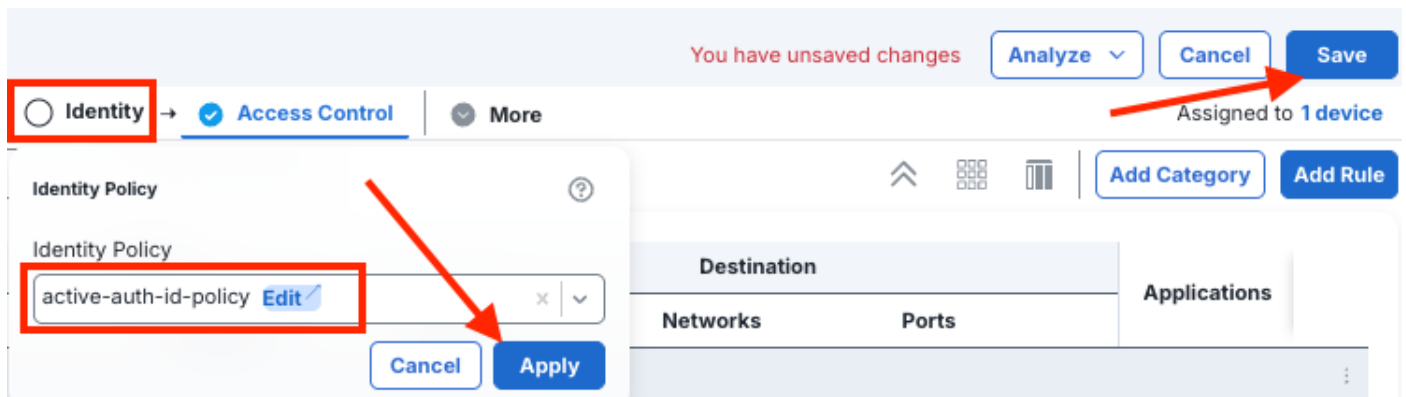
Configuración de política de control de acceso

2) Confirme que la política de descifrado configurada en los pasos anteriores se aplica a la política de control de acceso.



Aplicar Política De Descifrado Al Control De Acceso

3) Confirme que la política de identidad configurada en los pasos anteriores también se aplica a la política de control de acceso. Guarde los cambios de directiva.



Aplicar Política De Identidad Al Control De Acceso

4) Confirme que existen reglas que permiten el tráfico del plano de datos del cliente a través de Secure Firewall después de la autenticación activa exitosa. El ejemplo que se muestra aquí utiliza un conjunto de reglas más amplio dado el entorno de laboratorio.

☐	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 reglas de tráfico del plano de datos de usuario

Paso 6: Implemente configuraciones en los dispositivos Cisco Secure Firewall

Una vez implementados, a los clientes que envían tráfico se les pide una página web de inicio de sesión de Microsoft que realicen la autenticación activa con Azure Entra.

Para obtener información adicional sobre el proceso documentado aquí, vea [Crear un dominio de Microsoft Azure AD \(SAML\) para la autenticación activa \(portal cautivo\) - Capítulo: Realms in FMC Device Config Guide 10.x](#).

Verificación

Utilice esta sección para confirmar que la configuración funciona correctamente.

GUI

Validar las sesiones de usuario y la actividad en el FMC:

- Elija Integrations > Users > Active Sessions.

CISCO

Cloud-delivered Firewall Management Center

Integrations / Users / Active Sessions

Search

Switch to legacy UI

Refresh

Delete

Showing the 1 and only session

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

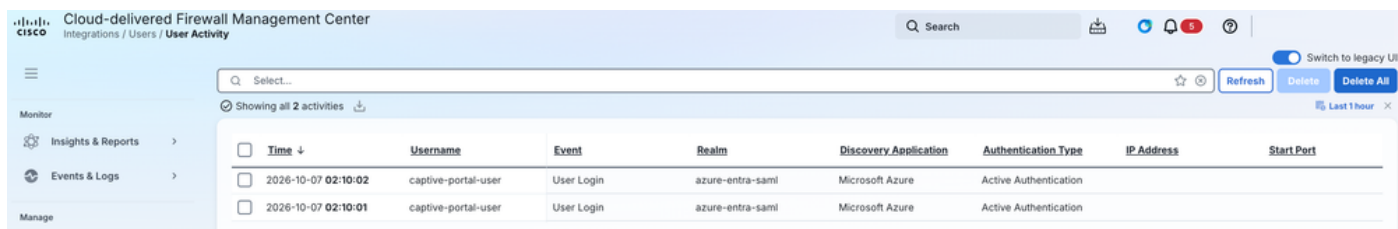
1 min 40 sec

azure-entra-saml

captive-portal-user

Salida de sesiones activas de FMC

- Elija Integrations > Users > User Activity.



The screenshot shows the Cisco Cloud-delivered Firewall Management Center (FMC) interface. The breadcrumb navigation is "Integrations / Users / User Activity". The left sidebar has "Monitor" selected. The main content area shows a table of user activity. A search bar at the top right has a "Switch to legacy UI" toggle. Below the search bar, it says "Showing all 2 activities". The table has columns: Time, Username, Event, Realm, Discovery Application, Authentication Type, IP Address, and Start Port. Two activities are listed, both with a time of 2026-10-07 02:10:02, username of captive-portal-user, event of User Login, realm of azure-entra-saml, discovery application of Microsoft Azure, authentication type of Active Authentication, and IP address of 1 min 40 sec.

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	1 min 40 sec	
2026-10-07 02:10:01	captive-portal-user	User Login	azure-entra-saml	Microsoft Azure	Active Authentication	1 min 40 sec	

Salida de actividad de usuario de FMC

En Azure, desplácese al Centro de administración de Microsoft Entra:

- Filtre Aplicaciones empresariales, busque/haga clic en la aplicación correspondiente.

The screenshot displays the Microsoft Entra admin center interface. On the left, the navigation pane is visible with the 'Enterprise apps' option highlighted by a red rectangle. The main content area shows the 'Enterprise applications | All applications' page. A search bar at the top right contains the text 'captive-'. Below the search bar, a list of applications is shown, with 'Captive-Auth...' highlighted by a red arrow. The 'All applications' link in the 'Manage' section is also highlighted by a red rectangle.

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

Home

Favorites

Entra ID

Overview

Users

Groups

Devices

Agents

Enterprise apps

App registrations

Roles & admins

Delegated admin partners

Tenant governance

New application

View, filter, and search applications

The list of applications that are

Search

captive-

Name	↑↓	Obj
Captive-Auth...		efda

Azure Entra Admin Center Enterprise Apps Navigation

- Elija 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

Registros de actividad de inicio de sesión de aplicación de Azure Enterprise

CLI

- En la CLI de FTD, puede ver las estadísticas relacionadas con las respuestas de SAML y del portal cautivo:

<#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
```

Troubleshoot

Depuración del portal cautivo

- El comando `system support captive-portal-debug` se puede utilizar en el FTD. El resultado muestra cómo habilitar el debug y también anota los segmentos clave del resultado para ayudar a comprender el flujo del portal cautivo.

```
<#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
...

```

Volcado de identidad de usuario

- Para tomar una instantánea de los datos de estado de identidad del usuario actual en el FTD, ejecute el comando `system support firewall-engine-dump-user-identity-data` en la CLI del FTD:

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

Successfully commanded snort.

>

- En el modo experto CLI, mientras se inicia sesión con las credenciales de administración local del dispositivo FTD, vea el contenido del archivo volcado en
/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:

...

Posibles problemas

Autoridad de certificados desconocida del portal cautivo

Problema: El explorador del cliente devuelve un error de emisor desconocido cuando se intenta la autenticación.

Causa probable: La autoridad de certificados interna no es de confianza en el explorador del cliente.

Resolución: Confirme que la CA es de confianza dentro del navegador. El ejemplo que se muestra aquí confirma que el certificado de la CA interna es de confianza.

Portal cautivo "Servidor no encontrado"

Problema: Cuando el navegador del cliente intenta cargar el portal cautivo, devuelve "Server Not Found" (Servidor no encontrado) para la URL base mientras intenta alcanzar la URL base o similar.

Causa probable: Alcance de DNS o configuración incorrecta de DNS.

Resolución: Confirme que el cliente tiene el servidor DNS adecuado configurado para resolver el registro A. Confirme que el servidor tiene un registro A asignado al FQDN y que es accesible y responde.

Información Relacionada

- [Crear un dominio de Microsoft Azure AD \(SAML\) para la autenticación activa \(portal cautivo\): Guía de configuración de dispositivos FMC 10.x](#)
- [Documentación de Azure Event Hub](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).