

Azure Entra Captive Portal op Secure Firewall configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Diagram](#)

[Captive Portal tussen Endpoint, FTD en Azure Entra](#)

[Configureren](#)

[Fase 1: Eerste FMC- en DNS-configuratie](#)

[Stap 1: De Cisco Dynamic Attributes Connector \(CSDAC\) inschakelen](#)

[Stap 2: Maak een volledig gekwalificeerd domeinnaam netwerk object vertegenwoordiger van de FTD Ingress Interface](#)

[Stap 3: Configureer de DNS A-record](#)

[Fase 2: Configuratie van infrastructuur met openbare sleutel](#)

[Stap 1: Importeer het interne CA-certificaat naar het VCC](#)

[Stap 2: Teken het Service Provider Certificate met de CA](#)

[Stap 3: Implementeer het SP-certificaat in de FTD](#)

[Fase 3: Azure Configuration](#)

[Stap 1: Maak de Entra Enterprise Application voor de SAML Toolkit](#)

[Stap 2: Inschrijvingen voor Entra ID-apps configureren](#)

[Stap 3: Configureer Microsoft Graph API-machtigingen voor de app-registratie.](#)

[Stap 4: Configureer de naamruimte Event Hub \(EH\)](#)

[Stap 5: Kies of maak beleid voor gedeelde toegang in de naamruimte van de gebeurtenishub](#)

[Stap 6: Verzamel en noteer informatie over gedeelde toegangshandtekeningen \(SAS\) uit de EH-naamruimte](#)

[Stap 7: Een instantie van de gebeurtenishub binnen de naamruimte van de gebeurtenishub maken](#)

[Stap 8: Maak een Event Hub Instance Consumer Group binnen de naamruimte van de Event Hub](#)

[Stap 9: Verzamelde waarden verifiëren](#)

[Stap 10: Intra ID Audit Log Streaming configureren naar de Event Hub](#)

[Fase 4: Configuratie van Azure en FMC/FTD Active Authentication consolideren](#)

[Stap 1: Configureer de Azure SAML/Entra ID Realm met behulp van de FMC Wizard](#)

[Stap 2: Implementeer de FMC-geconfigureerde SAML SP-metagegegevens in de Azure Enterprise-toepassing](#)

[Stap 3: Configureer het Azure SAML/Entra ID Realm met behulp van de FMC Wizard \(vervolg\)](#)

[Stap 4: Controleer gedownloade gebruikers](#)

[Fase 5: Beleid configureren in het VCC](#)

[Stap 1: Decryptiebeleid configureren](#)

[Stap 2: Decryptiebeleidsregels configureren](#)

[Stap 3: Creëer een identiteitsbeleid](#)

[Stap 4: Identiteitsbeleidsregels configureren](#)

[Stap 5: Configureer het toegangscontrolebeleid](#)

[Verifiëren](#)

[GUI](#)

[CLI](#)

[Problemen oplossen](#)

[Debug in captive-portaal](#)

[Dump van gebruikersidentiteit](#)

[Mogelijke problemen](#)

[Captive Portal Unknown Certificate Authority](#)

[Captive Portal "Server niet gevonden"](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de configuratie van Microsoft Azure Entra ID voor gebruik met een captive portal (actieve verificatie) op Cisco Secure Firewall.

Voorwaarden

Vereisten

Cisco adviseert kennis van deze onderwerpen:

- Security Assertion Markup Language (SAML)
- Microsoft Azure
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

U moet de standaard prijslaag beschikbaar hebben in Azure voor het maken van Event Hub. Daarnaast moeten apparaten worden geactiveerd met Smart Licensing ingeschakeld met exportgestuurde functionaliteit.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure FTD versie 10.0
- Cisco Secure FMC versie 10.0

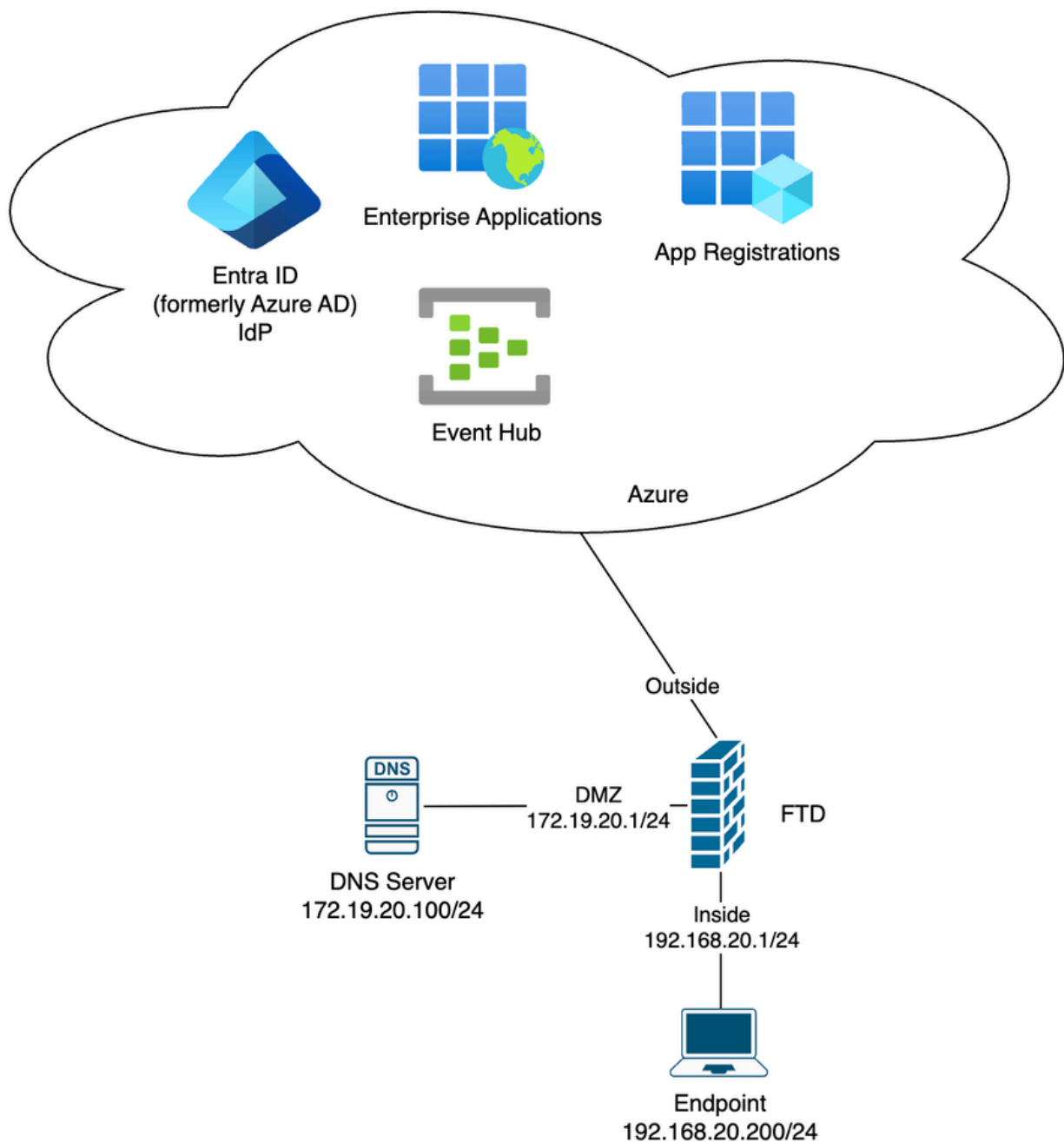
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Omdat traditionele IP-gebaseerde beveiligingsarchitecturen moeite hebben om gelijke tred te houden met dynamische, hybride werkomgevingen, biedt Cisco Secure Firewall Active Authentication met SAML-integratie een robuuste, identiteitsgerichte oplossing. Door gebruik te maken van Microsoft Entra ID (Azure AD) als een gecentraliseerde identiteitsprovider, stelt deze configuratie beheerders in staat om verder te gaan dan statische netwerkregels en granulaire toegangscontrole af te dwingen op basis van geverifieerde gebruikersidentiteit in plaats van vluchtige netwerkadressen. Deze integratie stroomlijnt de gebruikerservaring door middel van naadloze Single Sign-On (SSO) en verplichte Multi-Factor Authentication (MFA), terwijl ook wordt gezorgd voor een uniforme beveiligingspositie die strikte zichtbaarheid en beleidshandhaving in een perimeterloos netwerk behoudt.

Diagram

Captive Portal tussen Endpoint, FTD en Azure Entra



Captive Portal tussen EndPoint en Azure Entra

Configureren

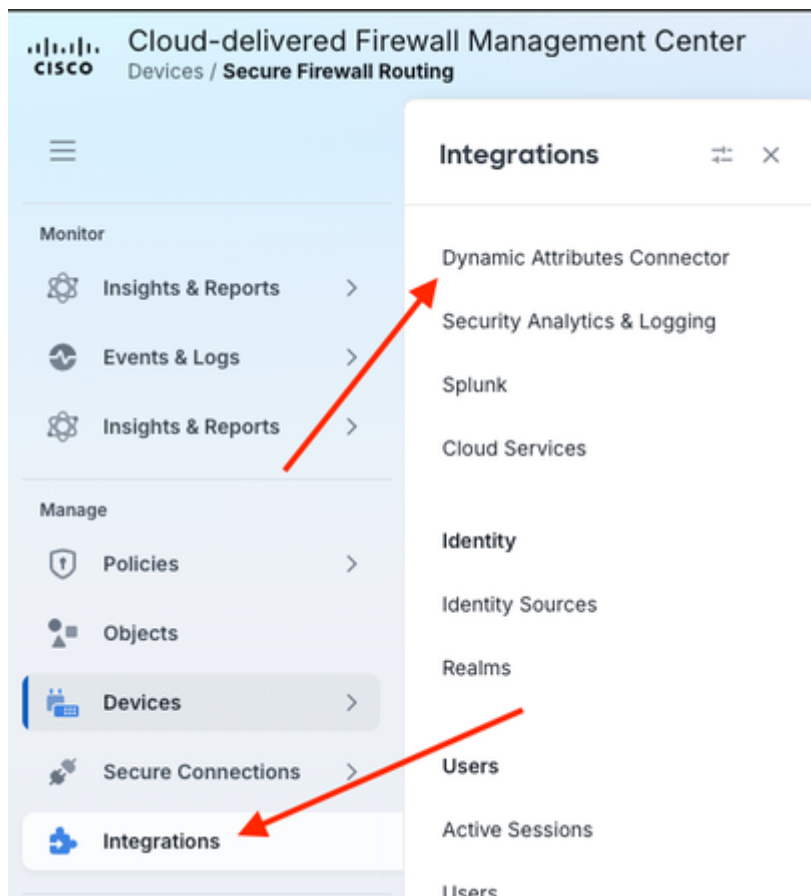
Fase 1: Eerste FMC- en DNS-configuratie



Opmerking: in dit lab wordt gebruikgemaakt van het door de cloud geleverde Firewall Management Center (cdFMC). De stappen blijven echter hetzelfde voor lokale FMC.

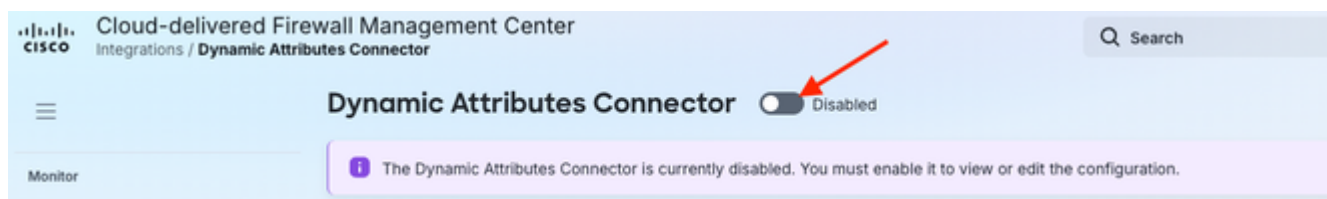
Stap 1: De Cisco Dynamic Attributes Connector (CSDAC) inschakelen

1) Kies Integraties > Dynamische Attributen Connector.



Kies Integraties Dynamische Attributen Connector

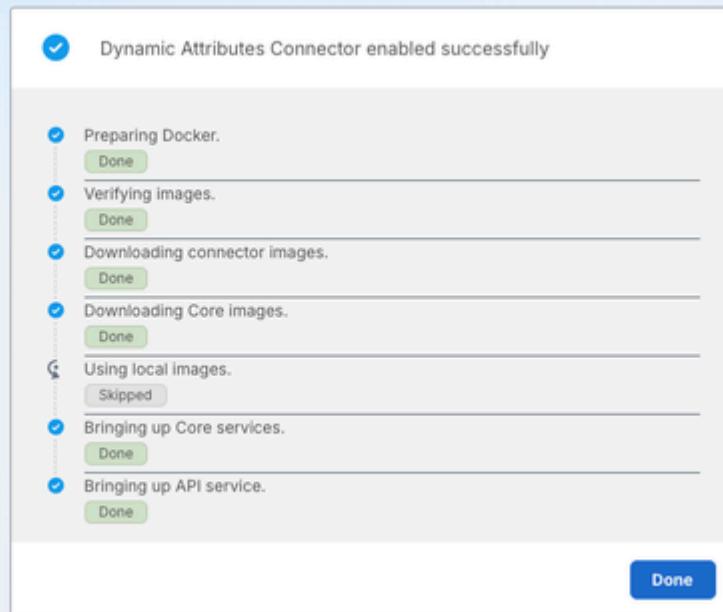
2) Klik op het besturingselement naast de tekenreeks Uitgeschakeld om CSDAC in te schakelen.



Cisco Dynamic Attributes Connector inschakelen

c) Klik op Gereed zodra de CSDAC-activering is voltooid.

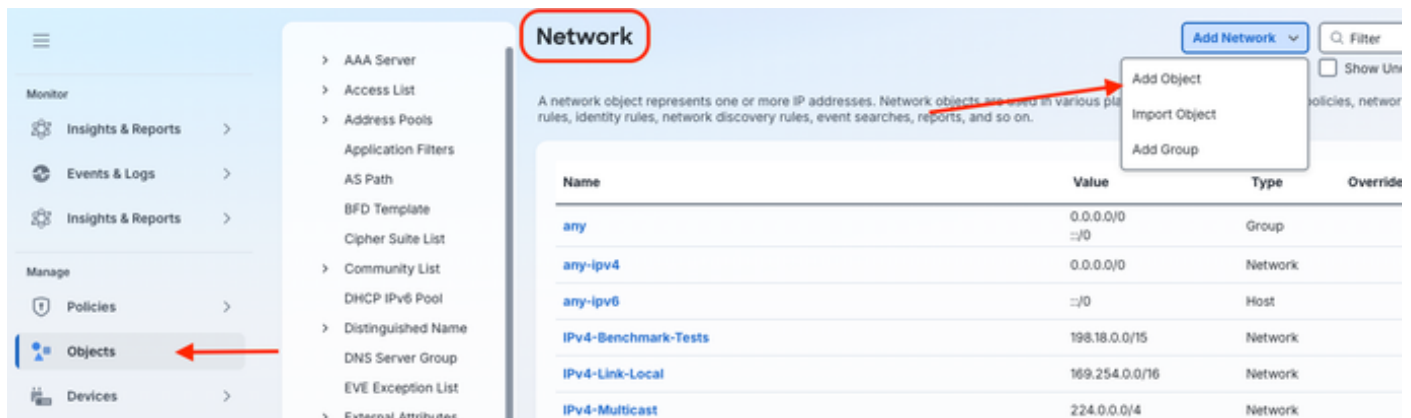
Dynamic Attributes Connector



Connectorstatus Cisco Dynamic Attributes inschakelen

Stap 2: Maak een volledig gekwalificeerd domeinnaam netwerk object vertegenwoordiger van de FTD Ingress Interface

1) Kies Objecten > Netwerk toevoegen > Object toevoegen.



Nieuw volledig gekwalificeerd domeinnaam netwerkobject maken

2) Noem het netwerkobject dat is geconfigureerd met de volledig gekwalificeerde domeinnaam (FQDN). Voer het FQDN in en wijs het netwerkobject toe als een FQDN-type door op de juiste keuzerondjes te klikken. Klik op Save (Opslaan).

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

FQDN-netwerkojectvariabelen configureren

Stap 3: Configureer de DNS A-record

1) Het hier getoonde voorbeeld maakt gebruik van Windows Server 2025; zie indien nodig de documentatie voor de specifieke naamoplossingsserver.

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



Opmerking: de client die actieve verificatie uitvoert, moet deze DNS A-record kunnen oplossen.

Fase 2: Configuratie van infrastructuur met openbare sleutel

Een interne Certificate Authority (CA) kan worden gebruikt als de Public Key Infrastructure (PKI) voor de Active Authentication-configuratie. Cisco FMC en FTD vereisen dat de interne CA public key en gekoppelde private key worden geüpload als een intern CA-object om de noodzakelijke SSL-interceptie en Decrypt-Resign-bewerkingen uit te voeren. Bovendien moet de interne CA worden vertrouwd in de clientbrowser van waaruit Active Authentication wordt uitgevoerd. Raadpleeg de documentatie van de clientbrowser om te controleren hoe u kunt bevestigen dat de browser het certificaat vertrouwt.

Stap 1: Importeer het interne CA-certificaat naar het VCC

1) Kies Objecten > PKI > Interne CA's. Klik op CA importeren.



Opmerking: de interne CA kan ook rechtstreeks op het FMC worden gemaakt.

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:



Opmerking: binnen de inhoud van dit document wordt een witruimte weergegeven die de verschillende veldwaarden in de afbeeldingen dekt en is deze opzettelijk per publicatie van dit document. De werkelijke waarden worden weergegeven voor uw omgeving tijdens het configureren.

Stap 2: Teken het Service Provider Certificate met de CA

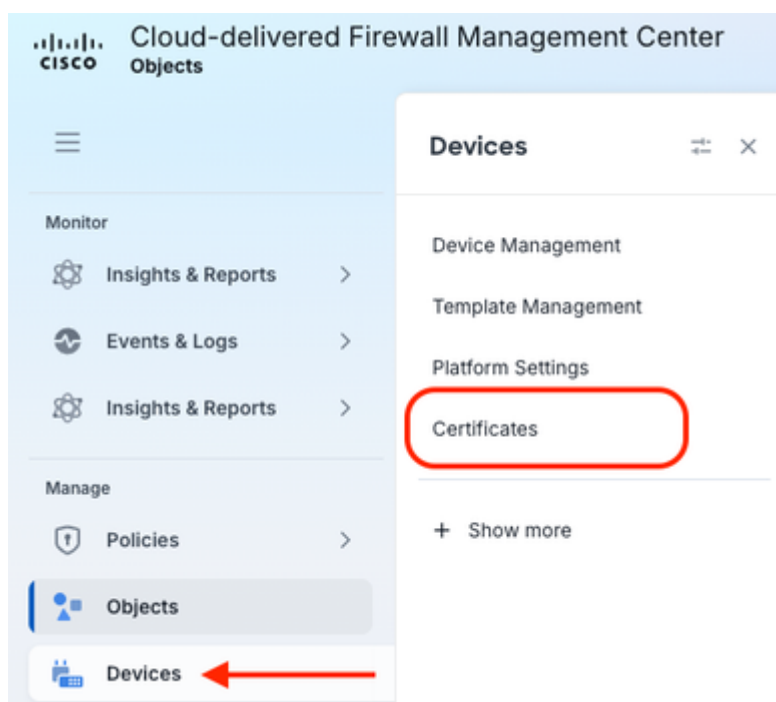
1) Het certificaat van de Serviceverlener (SP) moet worden ondertekend door een vertrouwde certificeringsinstantie (CA) en worden geretourneerd in een PKCS#12 (.p12)-indeling.



Opmerking: deze CA kan intern worden ondertekend. Het enige voorbehoud is dat de interne CA moet worden vertrouwd door het clientapparaat.

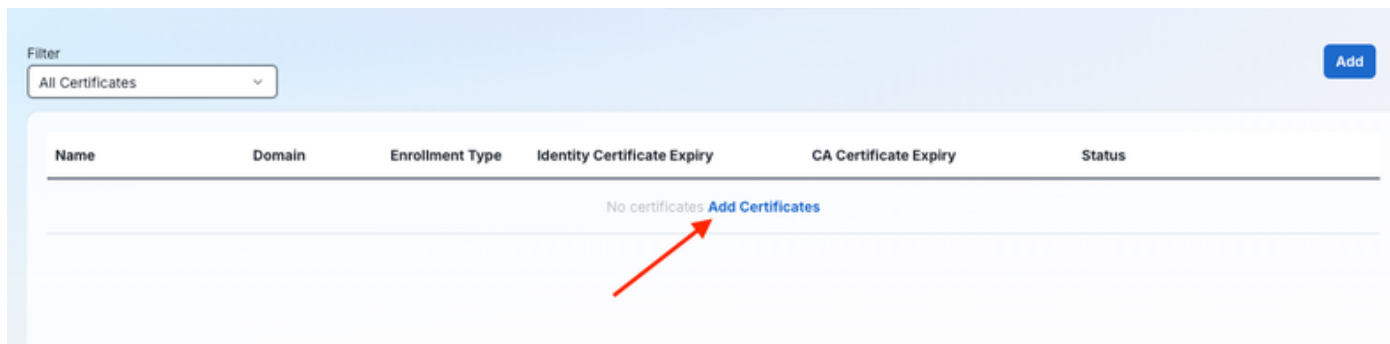
Stap 3: Implementeer het SP-certificaat in de FTD

1) Kies Apparaten > Certificaten.



Navigeer naar apparaten en certificaten

2) Klik op Certificaten toevoegen.



Nieuw apparaatcertificaat toevoegen

3) Klik op het apparaat in de vervolgkeuzelijst dat actieve verificatie uitvoert en klik vervolgens op het +-pictogram om een nieuwe certificaatinschrijving te maken.

A screenshot of the 'Add New Certificate' form. The title 'Add New Certificate' is at the top. Below it 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. Below the 'Certificate Enrollment*' dropdown is a '+' icon, with a red arrow pointing to it. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

Selecteer FTD en voeg nieuwe certificaatinschrijving toe

4) Noem de certificaatinschrijving en kies in de vervolgkeuzelijst Inschrijftype het PKCS12-bestand.

Add Certificate Enrollment ?

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:*

Challenge Password:

Confirm Password:

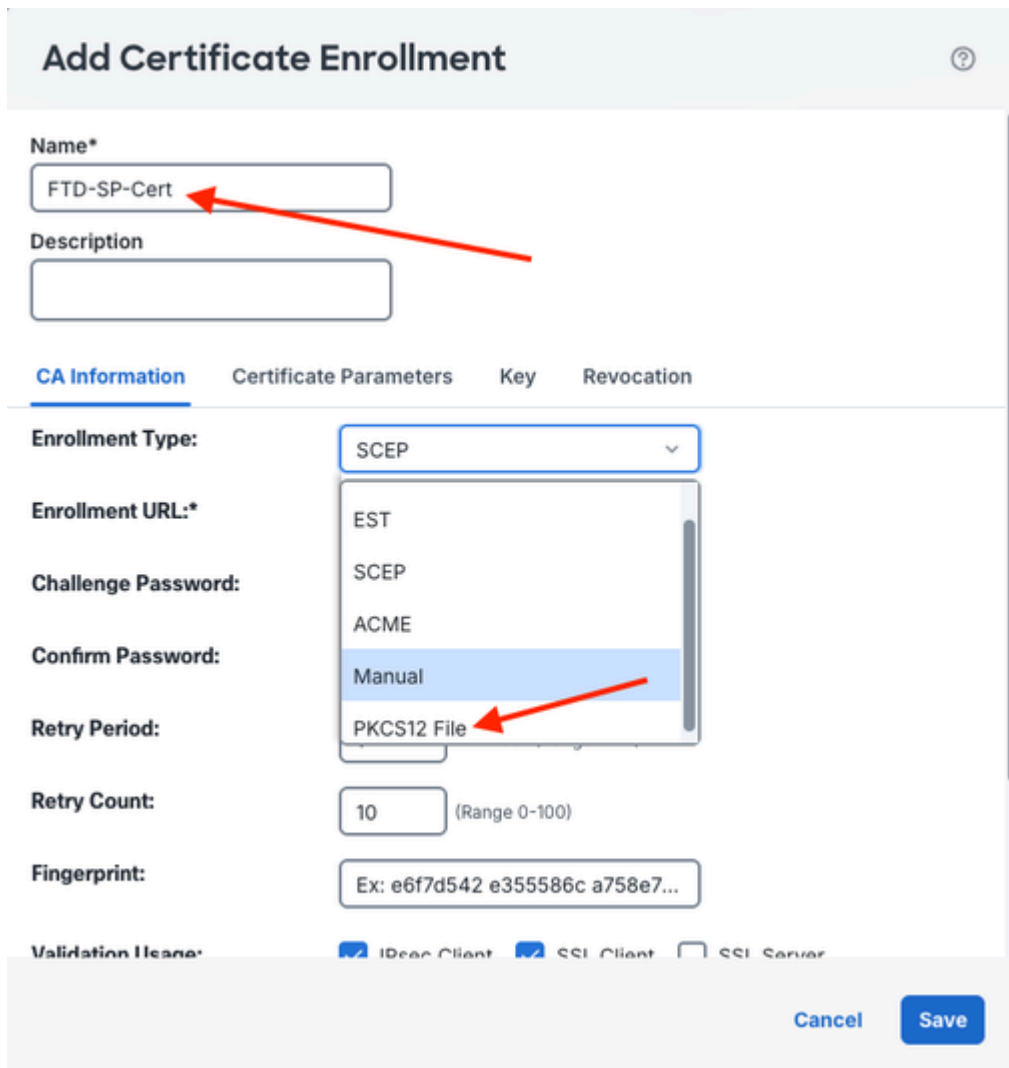
Retry Period:

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7...

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

Cancel Save



Instellingen en type certificaatschrijving

5) Importeer het PKCS#12-bestand door te klikken op Bladeren PKCS12-bestand en voer de vereiste wachtwoordzin in. Klik op Save (Opslaan).

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

Bladeren en importeren van PKCS12-bestand

6) Bevestig dat de inschrijvingsgegevens correct zijn en klik op Toevoegen.

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 +

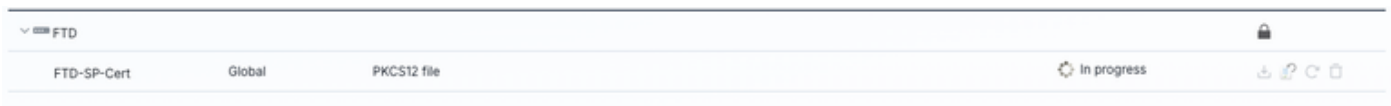
Certificate Enrollment Details:

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

Cancel Add

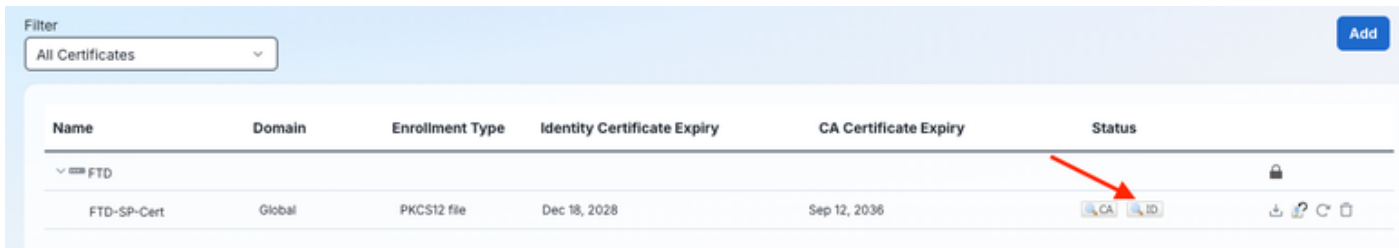
Inschrijvingsgegevens certificaat bevestigen

7) De invoer weerspiegelt In uitvoering.



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

Zodra het importeren is voltooid, kan de SP-certificaatinformatie worden gevalideerd door op het ID-pictogram van het geconfigureerde certificaat te klikken.



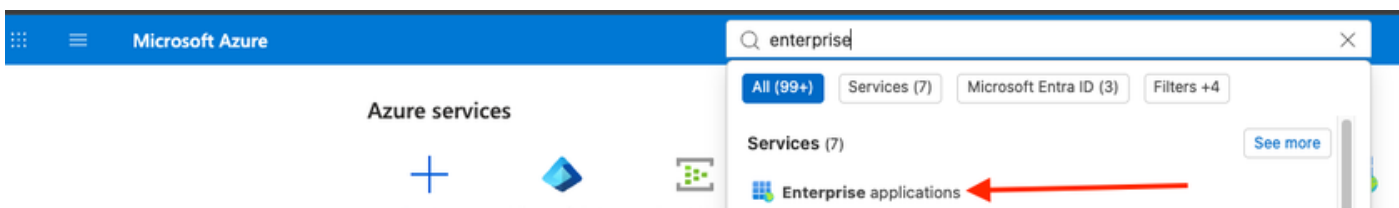
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
FTD-SP-Cert	Global	PKCS12 file	Dec 18, 2028	Sep 12, 2036	In progress

Status Certificaat importeren in uitvoering

Fase 3: Azure Configuration

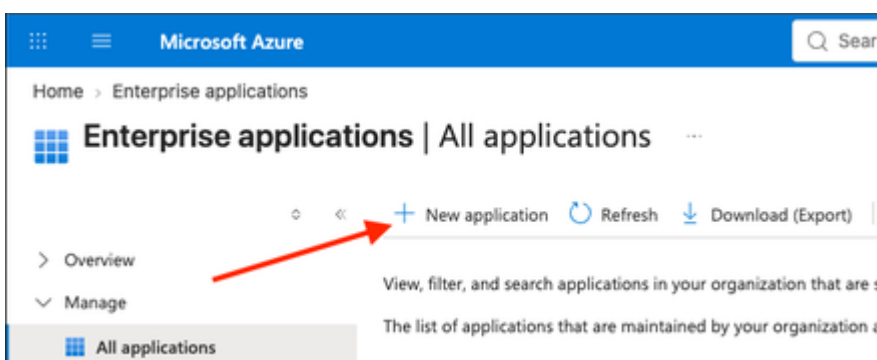
Stap 1: Maak de Entra Enterprise Application voor de SAML Toolkit

1) Zoeken naar en klikken op Enterprise Applications.



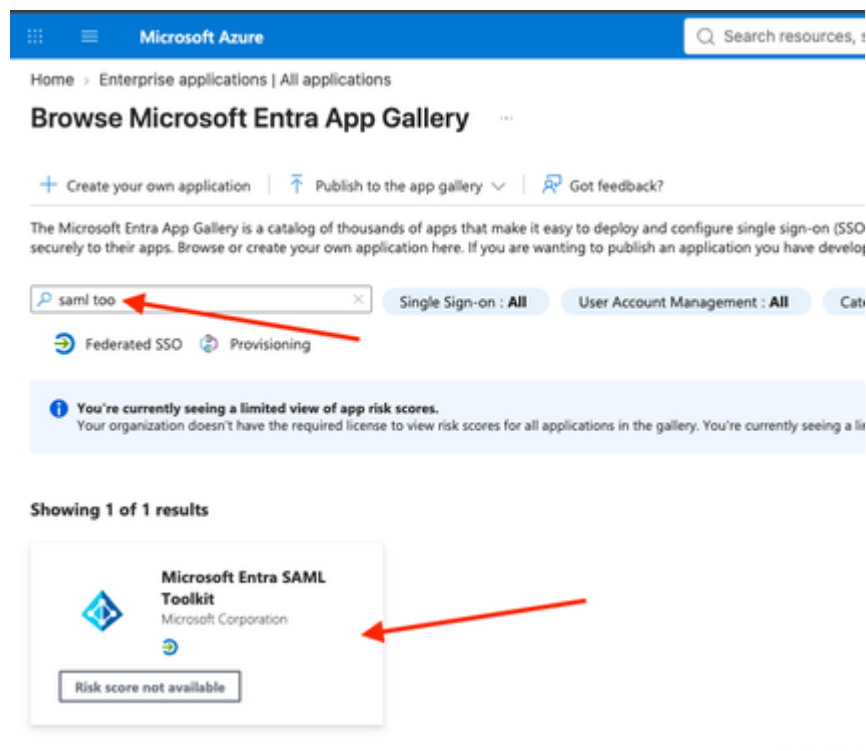
Zoeken naar en toegang krijgen tot bedrijfstoepassingen

2) Klik op + Nieuwe toepassing.



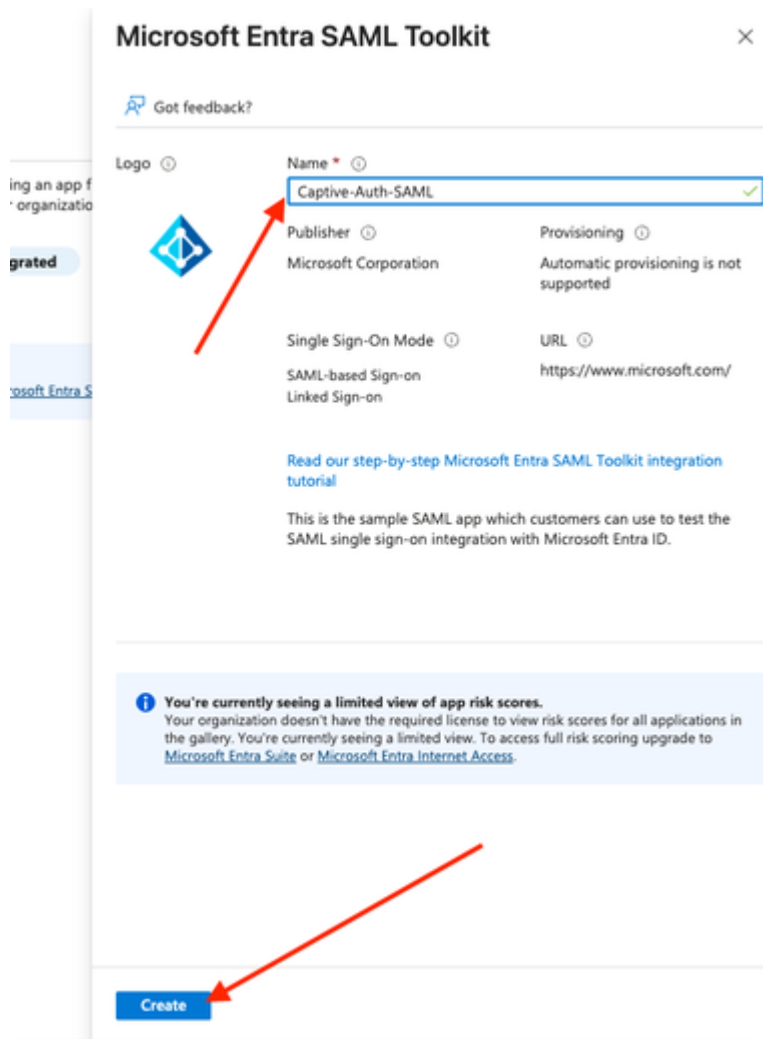
Nieuwe toepassing selecteren binnen bedrijfstoepassingen

3) Zoek naar de Microsoft Entra SAML Toolkit en klik op de thumbnail ervoor.



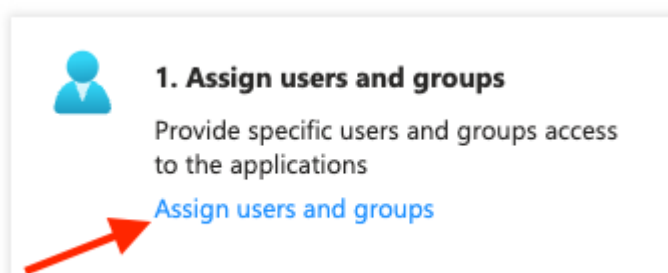
Zoeken en selecteren van Microsoft Entra SAML Toolkit

4) Wijs een naam toe aan de Microsoft Entra SAML Toolkit Enterprise Application en klik op Maken. (Referentie van Microsoft: [Lees onze stap-voor-stap Microsoft Entra SAML Toolkit integratie tutorial](#)).



Naam toewijzen aan SAML Toolkit-toepassing

5) Wijs op de pagina Overzicht de specifieke gebruikers en groepen toe aan de SAML Toolkit Enterprise Application. In dit voorbeeld is het testaccount (captive-portal-gebruiker) lid van de groep active-auth-lab.

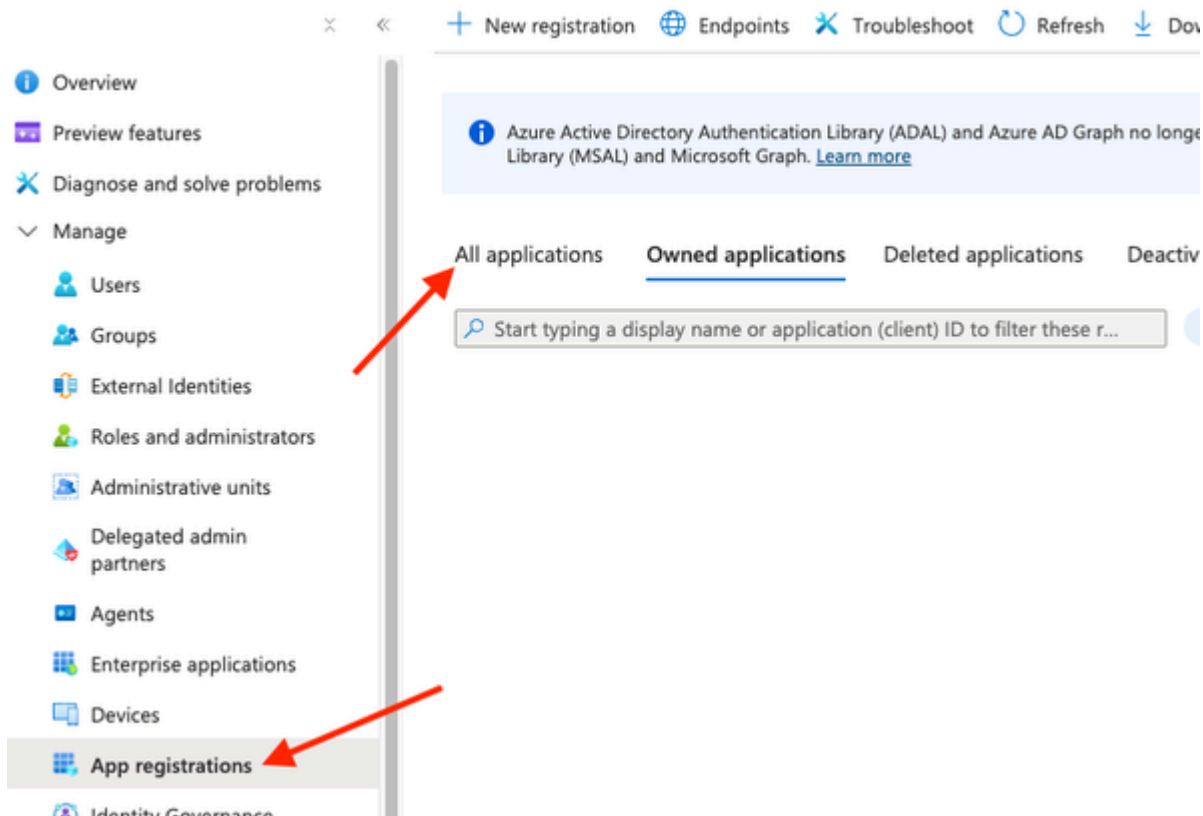


Gebruikers en groepen toewijzen aan toepassing

6) De configuratie van deze bedrijfstoeppassing wordt in latere stappen voortgezet.

Stap 2: Inschrijvingen voor Entra ID-apps configureren

1) Navigeer terug naar Entra ID en kies in het linkernavigatiemenu App-registraties. Klik op het filter Alle toepassingen en zoek naar de naam die aan de Enterprise-toepassing is gegeven. Klik op de juiste applicatie.



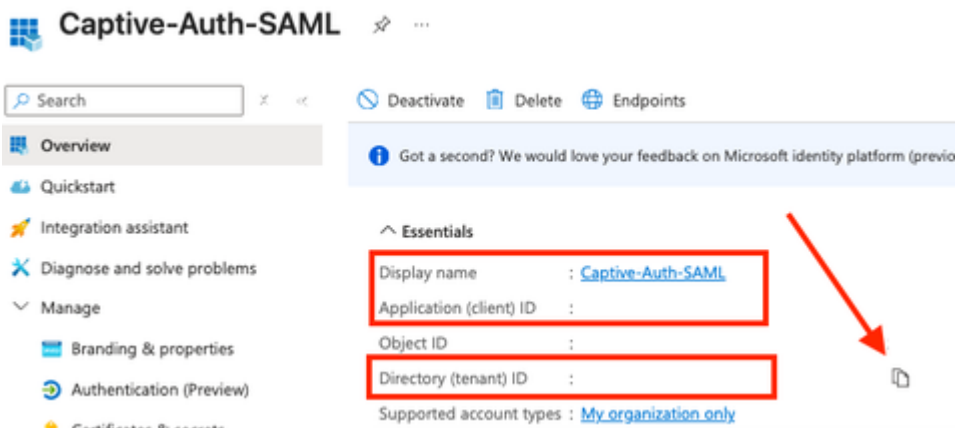
Navigeer naar app-registraties en alle toepassingen

2) Verzamel en noteer de essentiële waarden onder de registratie van de Enterprise App.



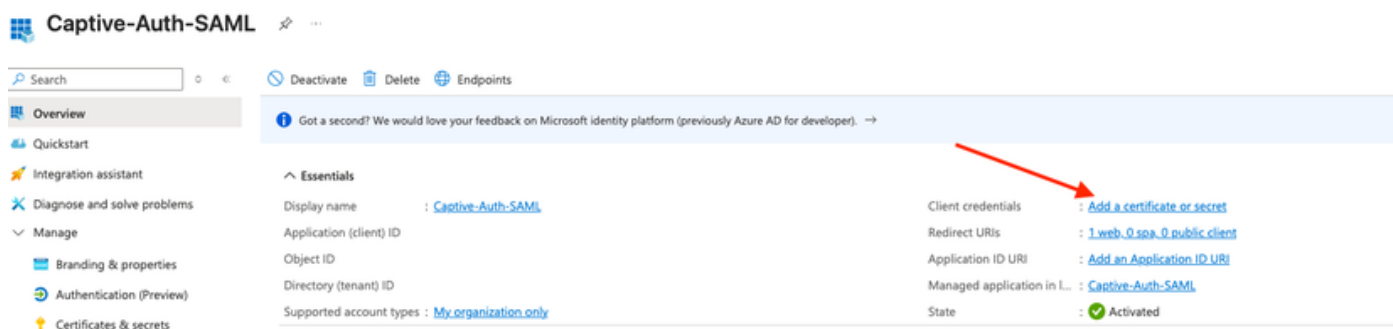
Belangrijk: Beweeg de muis over de waarden om Kopiëren naar klembord weer te geven en verzamel de waarden onder Essentials op de pagina Overzicht:

- Weergavenaam
- Applicatie-ID (client)
- Directory-ID (huurder)



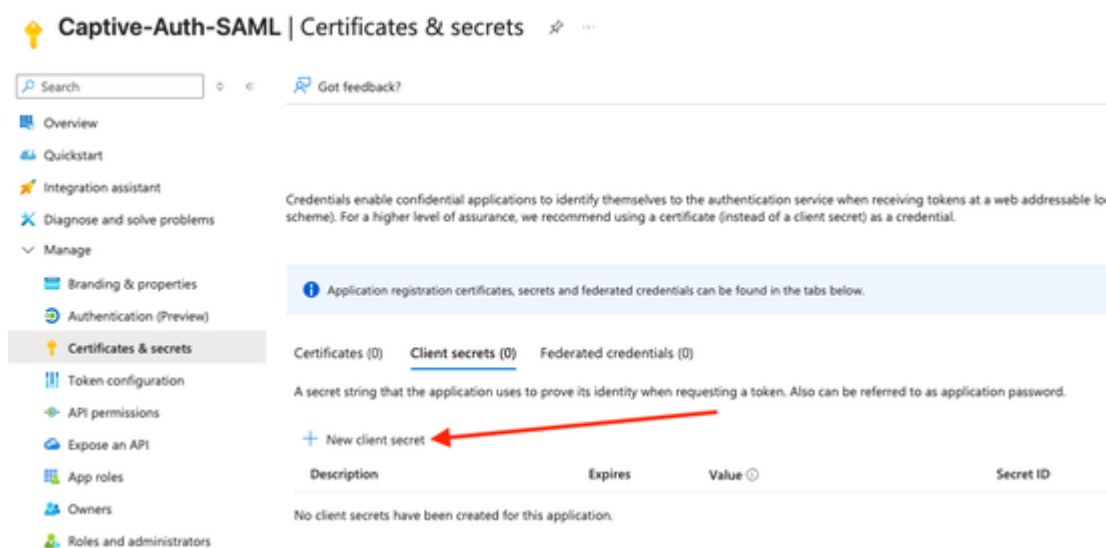
Weergave- en toepassings- en directory-ID-waarden verzamelen

3) Klik op Certificaat of geheime hyperlink toevoegen.



Certificaat of geheime hyperlink toevoegen

4) Klik op + Nieuw clientgeheim.



Nieuw clientgeheim toevoegen

5) Geef een beschrijving voor het geheim en pas de vervaldatum indien nodig aan. Klik op Add

(Toevoegen).

Add a client secret

Description:

Expires: Recommended: 180 days (6 months)

Add **Cancel**

Beschrijving voor clientgeheim opgeven

6) Kopieer het geheim.



Belangrijk: Let op de geheime waarde die naar het klembord is gekopieerd.

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.

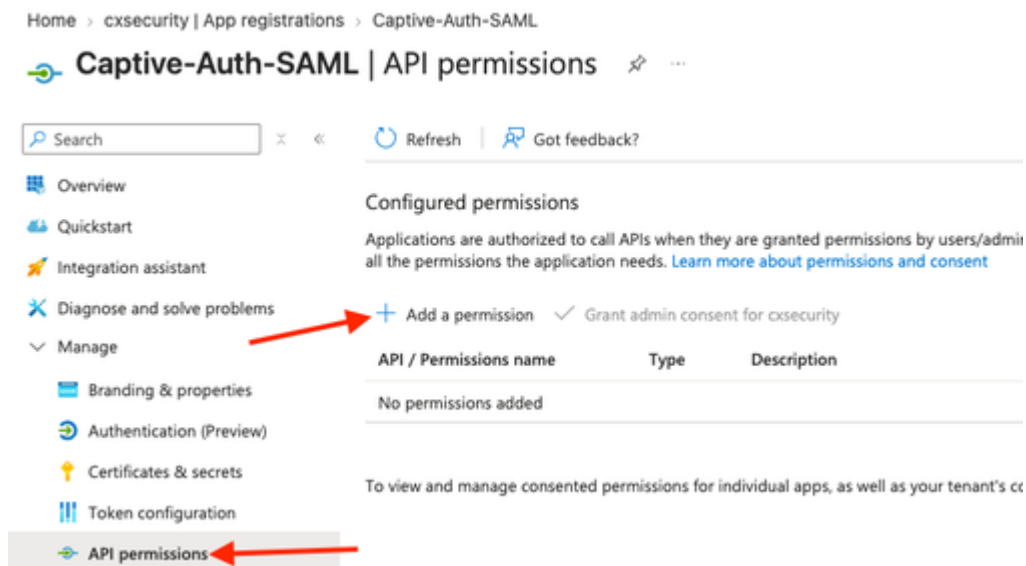
+ New client secret

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

Client Secret Value kopiëren

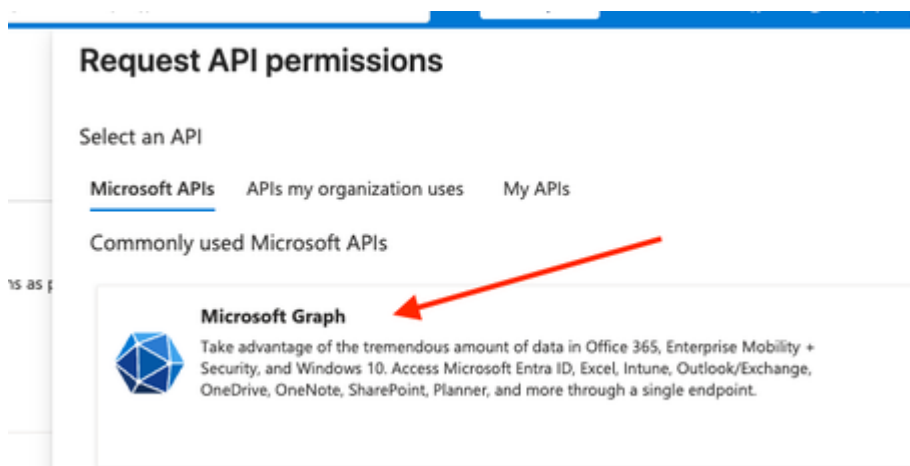
Stap 3. Configureer Microsoft Graph API-machtigingen voor de app-registratie.

1) Kies API-machtigingen in het linkernavigatiemenu en klik vervolgens op + Een machtiging toevoegen.



API-machtigingen configureren

2) Klik op Microsoft Graph API.



Selecteer Microsoft Graph API

3) Gedelegeerde gebruiker toekennen. Rechten lezen en klik vervolgens op Rechten toevoegen.

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

Toekenning van leest toestemmingen voor gedelegeerde gebruikers

4) Grant Application User.Read.All permissies (vink het selectievakje aan).

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

Toekenningaanvraag Alle machtigingen lezen

5) Zoek en vink het selectievakje Group.Read.All aan om ook machtigingen voor groepslezen toe te kennen. Klik op Rechten toevoegen.

Select permissions

[expand all](#)

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

API-machtigingen opslaan

6) Bevestig dat de geconfigureerde machtigingen overeenkomen en geef hiervoor administratieve toestemming.

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

Administratieve toestemming verlenen voor machtigingen

7) De output, zodra de admin toestemming is verleend, wordt weergegeven.

+ Add a permission

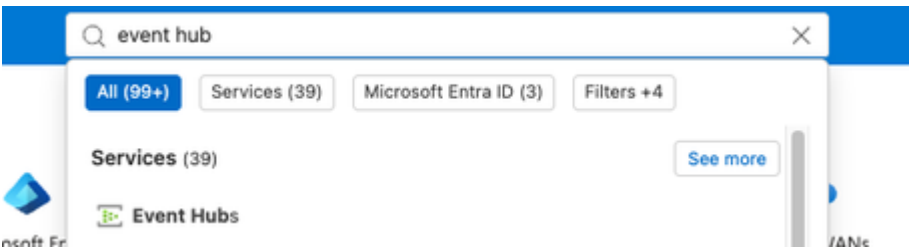
✓ Grant admin consent for

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

Toegegeven administratieve toestemming Output

Stap 4: Configureer de naamruimte Event Hub (EH)

1) Zoek en klik op Event Hubs.



Configuratie van de Hub voor zoekgebeurtenissen

2) Maak een nieuwe EH-naamruimte.



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](#)

Naamruimte van gebeurtenishub maken

3) Configureer de EH-naamruimte.



Opmerking: de standaard prijslaag of hoger moet worden gekozen. Het basisprijsniveau voorkomt gebruik in het domein.

Zie de [documentatie van Azure Event Hub](#) voor verdere evaluatie van Geavanceerde instellingen van Event Hub en toepasbaarheid op specifieke behoeften.

Klik op Beoordelen + Aanmaken.



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 >

Instellingen naamruimte gebeurtenishub configureren

4) Klik op Aanmaken zodra de validatie is geslaagd.

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 >

Gebeurtenishub-naamruimteimplementatie maken

5) Bevestig dat de implementatie is voltooid en klik vervolgens op Ga naar resource.

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

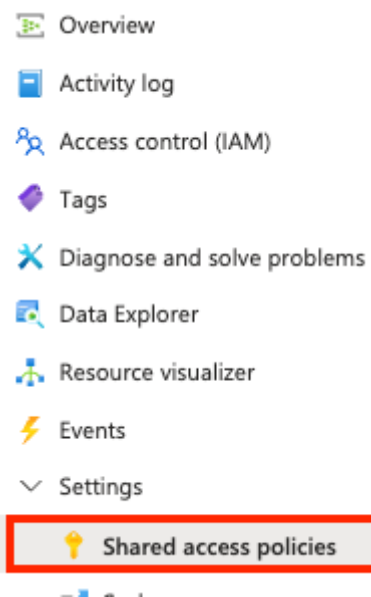
✓ Next steps

Go to resource

Ga naar Event Hub namespace resource

Stap 5: Kies of maak beleid voor gedeelde toegang in de naamruimte van de gebeurtenishub

1) Kies in het linkernavigatiemenu Instellingen > Gedeeld toegangsbeleid.



Navigeer naar beleid voor gedeelde toegang

2) Klik op + Toevoegen en voer de nieuwe beleidsnaam in en vink het selectievakje Beheren aan. Klik onderaan in het menupaneel SAS-beleid toevoegen op Aanmaken.



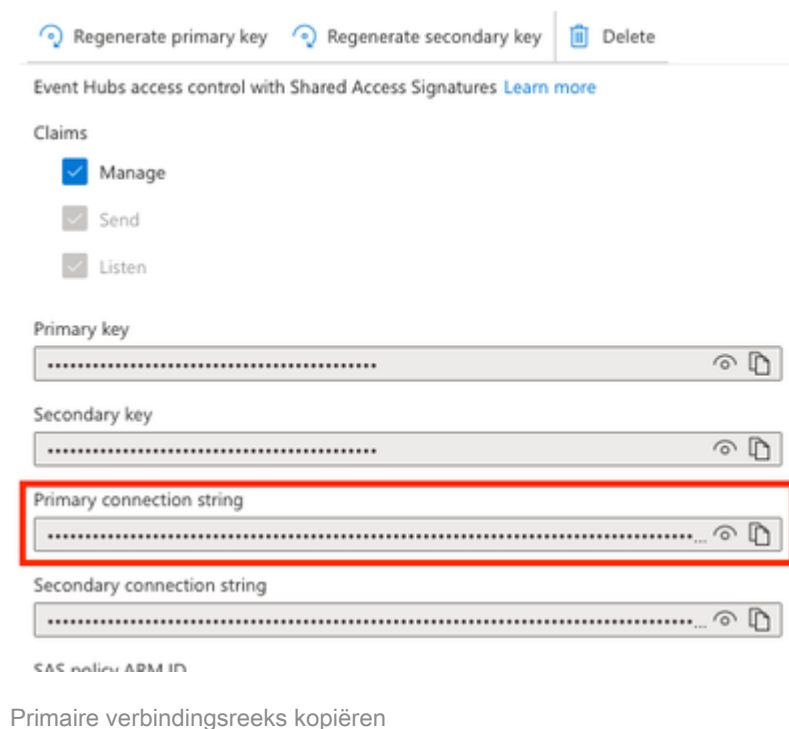
Nieuw beleid voor gedeelde toegang toevoegen



Beleid voor gedeelde toegang maken

Stap 6: Verzamel en noteer informatie over gedeelde toegangshandtekeningen (SAS) uit de EH-naamruimte

1) Klik op het nieuwe beleid voor gedeelde toegang; het EH SAS-beleid wordt weergegeven in het zijpaneel aan de rechterkant.



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: ABM ID

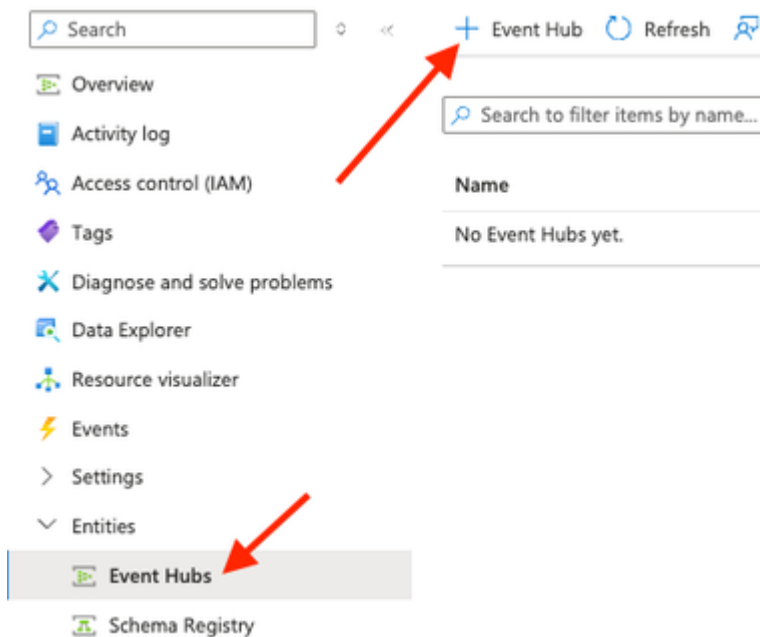
Primaire verbindingssreeks kopiëren



Belangrijk: Kopieer en noteer de primaire verbindingssreeks.

Stap 7: Een instantie van de gebeurtenishub binnen de naamruimte van de gebeurtenishub maken

1) Kies Entiteiten > Event Hubs in het menu Namespace. Klik op + Event Hub om een nieuwe EH-instantie te maken.



Nieuwe instantie van gebeurtenishub maken

2) Wijs een naam toe aan de nieuwe EH-instantie en klik vervolgens op 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 >

Naam toewijzen aan instantie Event Hub

3) Als de validatie is voltooid, klikt u op Aanmaken om de instantie Event Hub te openen.

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 >

instantie van gebeurtenishub voor provisioning



Belangrijk: Kopieer en noteer de instantienaam van de Event Hub.

Stap 8: Maak een Event Hub Instance Consumer Group binnen de naamruimte van de Event Hub

1) Klik op de nieuwe EH-instantie die in de vorige stap is geconfigureerd.

captive-auth-ad-eh | Event Hubs ☆ ...
Event Hubs Namespace

Search

+ Event Hub Refresh Give feedback

Search to filter items by name...

Name	Status
captive-auth-ad-eh-1	Active

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Data Explorer
Resource visualizer
Events
Settings
Entities
Event Hubs
Schema Registry

Configuratie van instantie van Access Event Hub

2) Kies Entiteiten > Consumentengroepen in de instantie EH en maak een nieuwe Consumentengroep.

Search

+ Consumer group Refresh

Search to filter items by name...

Name
\$Default

Overview
Access control (IAM)
Diagnose and solve problems
Data Explorer
Explore in Microsoft Fabric
Resource visualizer
Settings
Shared access policies
Configuration
Properties
Locks
Entities
Consumer groups
Features

Consumentengroep maken

3) Geef de consumentengroep een naam en klik op Maken.

Create consumer group ×

Consumer groups

Name *

captive-auth-ad-eh-cg



Create

Naam toewijzen aan consumentengroep



Belangrijk: Kopieer en noteer de naam van de instantie Event Hub Consumer group.

Stap 9: Verzamelde waarden verifiëren

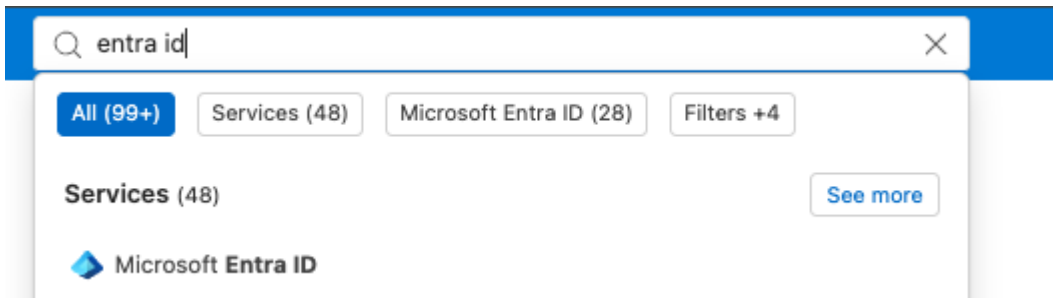
1) Op dit punt moeten deze waarden uit de voorgaande stappen worden genoteerd. Als er geen waarde is geregistreerd, verwijst u naar de toepasselijke stap waar deze wordt verzameld:

- Fase 3 Stap 2 - App-registratie (van de Enterprise App die voor dit proces is gemaakt, waarnaar wordt verwezen door de verzamelde weergavenaam)
 - Stap 2, substap 2
 - Weergavenaam
 - Toepassing (client)-ID
 - Directory (tenant)-ID
 - Stap 2, substap 6
 - Clientgeheim
- Fase 3 Stap 6 - Event Hub
 - Stap 6, substap 1
 - EH-naamruimte
 - Primaire verbindingssreeks

- Stap 7, substap 3
 - EH-instantie (Event Hub) naam
- Stap 8, substap 3
 - Naam EH Consumer Group

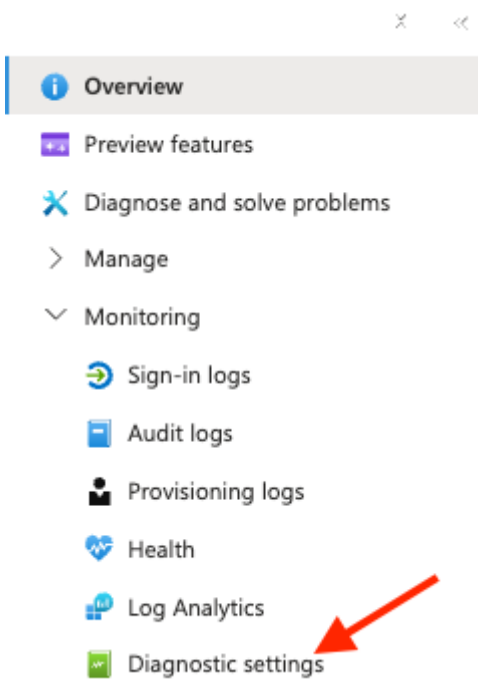
Stap 10: Intra ID Audit Log Streaming configureren naar de Event Hub

1) Navigeer terug naar de configuratie van de Entra ID-tenant.



Zoeken en navigeren naar de configuratie van de ID-tenant

2) Kies in het linkermenu Bewaking > Diagnostische instellingen.



Controle van diagnostische instellingen

3) Kies Diagnostische instellingen > Algemeen en klik op + Diagnostische instellingen toevoegen.



 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

Nieuwe diagnostische instelling toevoegen

4) Wijs de vereiste naam toe aan de diagnostische instelling, vink het selectievakje AuditLogs aan om te loggen en vink het selectievakje Stream to an event hub aan. Verwijs naar de waarden die zijn genoteerd in de vorige configuraties en klik op Opslaan wanneer u klaar bent.

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

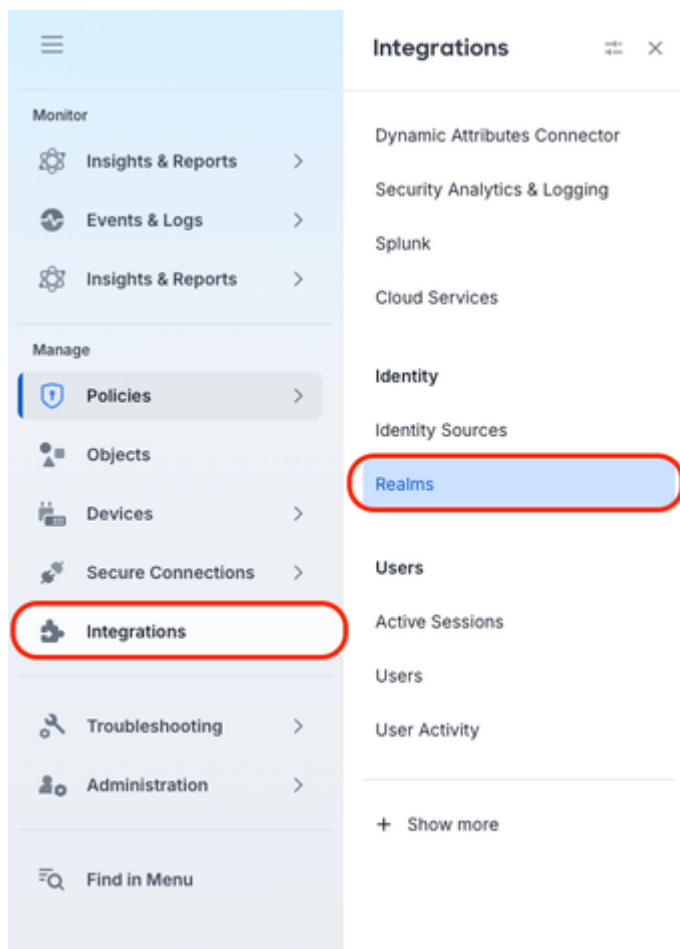
Destination details

- ☐ 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: Configuratie van Azure en FMC/FTD Active Authentication consolideren

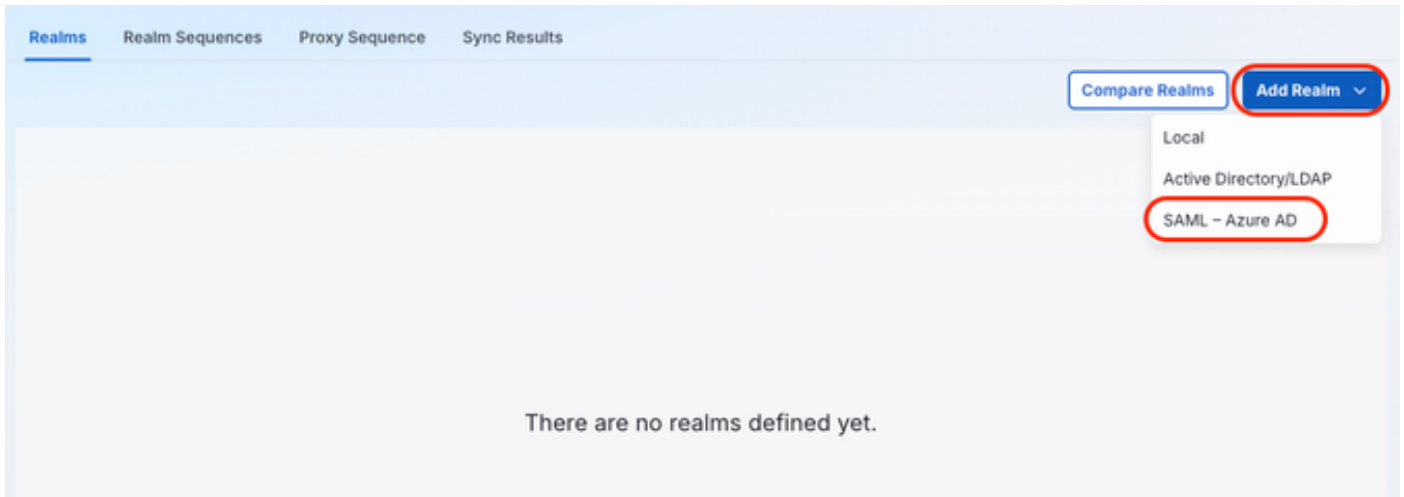
Stap 1: Configureer de Azure SAML/Entra ID Realm met behulp van de FMC Wizard

1) Kies binnen het VCC Integraties > Identiteit > Rijken.



Configuratie van identiteitsgebieden

2) Klik op de vervolgkeuzelijst Realm toevoegen en kies SAML - Azure AD.



SAML Azure AD Realm toevoegen

3) Wijs een naam en beschrijving toe aan het Azure-domein om het gebruik ervan te beschrijven en zorg ervoor dat Authenticate passief met Azure AD of het gebruik van een captive portal met Azure AD wordt gekozen uit de vervolgkeuzelijst Configuration Type. Klik op Next (Volgende).

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

Azure AD Realm-instellingen configureren

4) Kies het eerder geconfigureerde FQDN-object als de basis-URL. Voer de entiteit-ID in met de tekenreeksindeling die wordt weergegeven:

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

- Wanneer het achtervoegsel SAML Entity ID is geconfigureerd (groen onderstreept in het volgende configuratievoorbeeld), moet u ervoor zorgen dat het achtervoegsel uniek is voor andere SSO-implementaties in de omgeving. Deze waarde moet ook overeenkomen met de Azure SAML-configuratie. De basis-URL blijft gedurende de configuratie hetzelfde.
- De URL van de Assertion Consumer Services (ACS) wordt automatisch ingevuld en is onveranderlijk.
- Kies het Service Provider (SP)-certificaat dat is ingeschreven in de vorige werkstroomstappen in FMC onder Apparaten > Certificaten.
- Nadat deze waarden zijn ingevoerd, klikt u op Metagegevens van serviceprovider downloaden om het configuratieproces te vereenvoudigen en te bevestigen dat de verwachte waarden naar Azure zijn geschreven.

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?tgname=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](#)

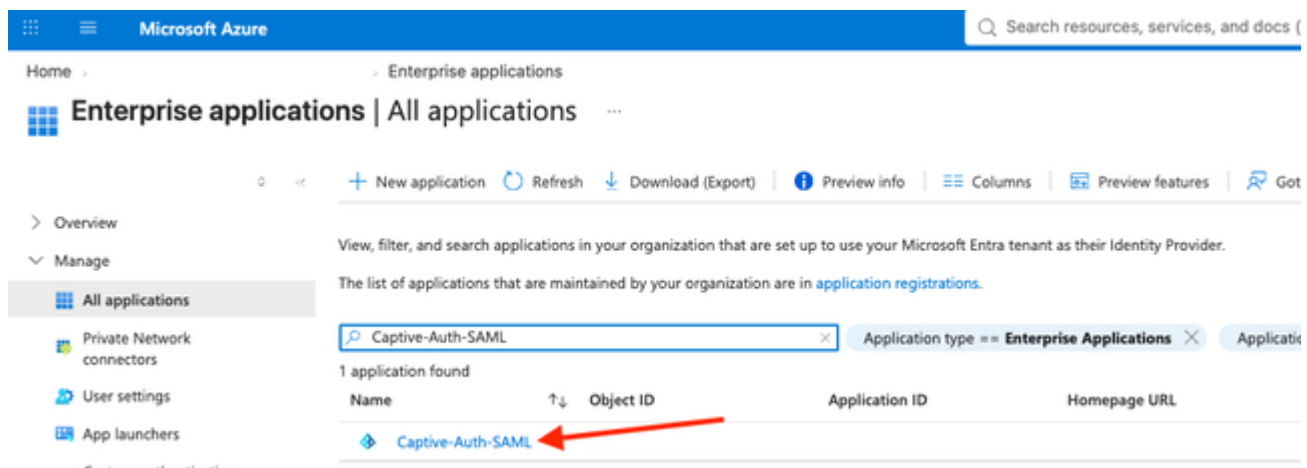
[Next](#)

BasisURL en entiteit-ID configureren en SAML-metagegevens downloaden

5) Klik op Volgende om naar Reeks 3 van de Realm-configuratie te gaan.

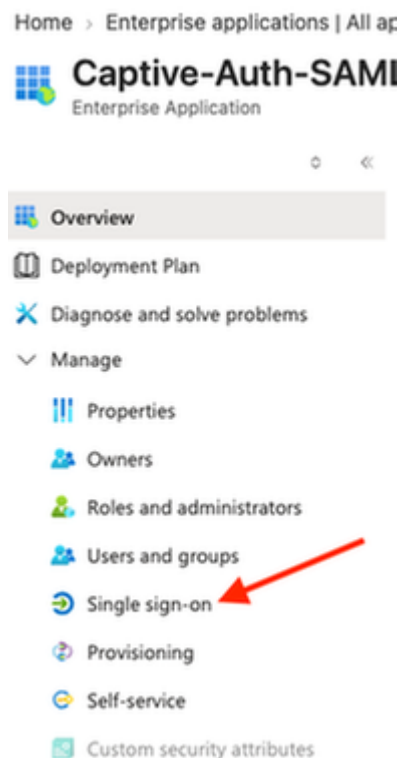
Stap 2: Implementeer de FMC-geconfigureerde SAML SP-metagegevens in de Azure Enterprise-toepassing

1) Navigeer terug naar Azure en kies Entra ID > Beheren > Enterprise Applications. Zoek naar de eerder gemaakte instantie van de Microsoft Entra SAML Toolkit Enterprise Application.



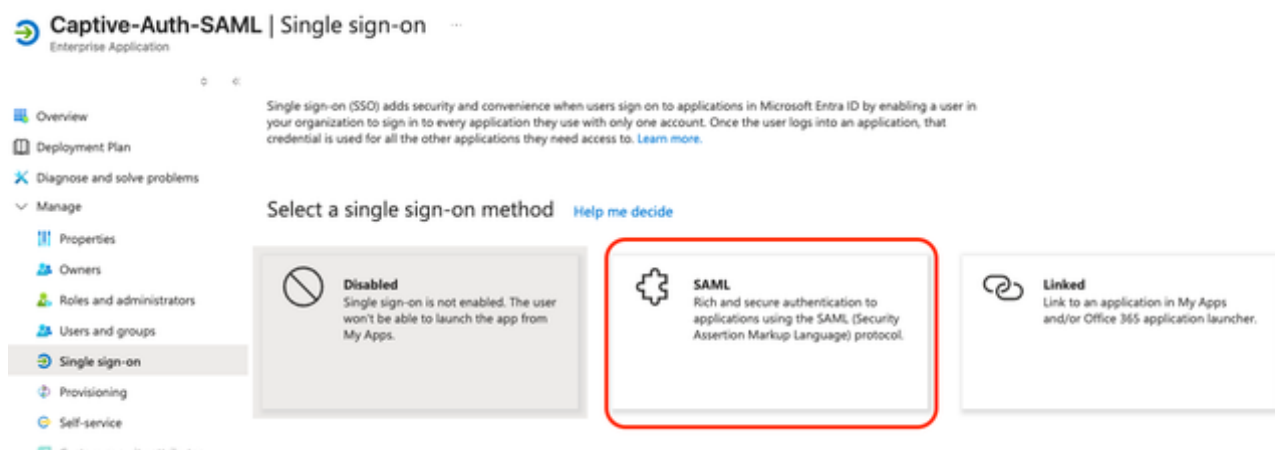
Microsoft Entra SAML Toolkit-toepassing zoeken

2) Kies in het navigatiemenu aan de zijkant Beheren > Eenmalige aanmelding.



Configuratie voor eenmalige aanmelding beheren

3) Klik op de modus SAML Single Sign-On (SSO).



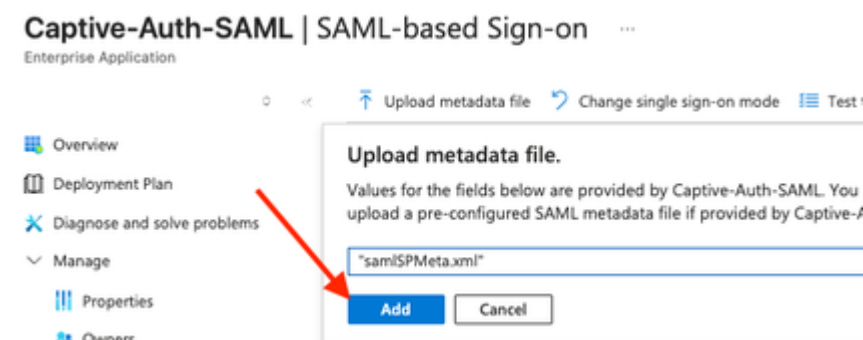
SAML Selectie van modus voor eenmalige aanmelding

4) Klik op Metagegevensbestand uploaden en klik op het blauwe mappictogram om door uw lokale bestandssysteem te bladeren naar het SAML-metagegevensbestand dat van het FMC is gedownload.



Metagegevensbestand uploaden vanuit Firewall Management Center

5) Als het uploaden is voltooid, klikt u op Toevoegen.



SAML-configuratie-toepassing toevoegen

6) Het zijpaneel voor Basic SAML Configuration verschijnt en waarden zoals de Identifier (Entity ID) en de ACS URL worden geëxtraheerd uit het SP-metadata XML-bestand dat door de FMC is

gemaakt en automatisch wordt geüpload en toegepast. De aanmeldings-URL is echter niet ingevuld en is vereist voordat u deze opslaat.

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?tname=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.

*

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.

7) Gebruik het opgegeven aanmeldings-URL-patroon, kopieer en plak de waarde en klik bovenaan op Opslaan wanneer u klaar bent.

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)

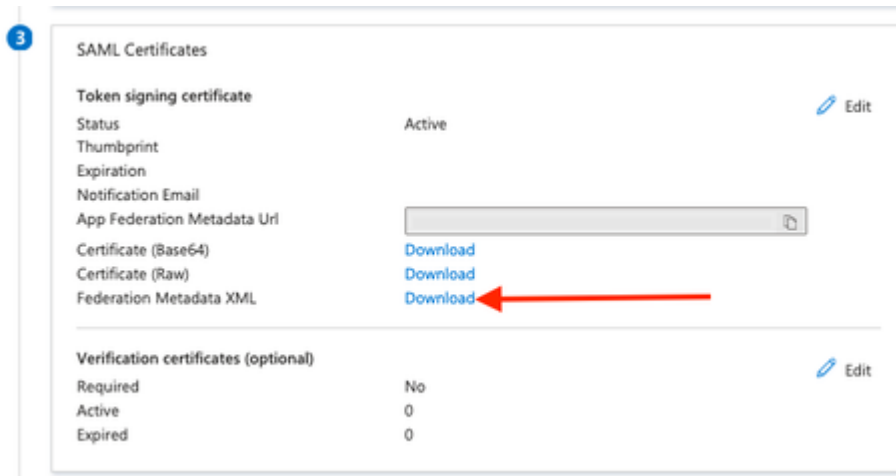
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional)

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



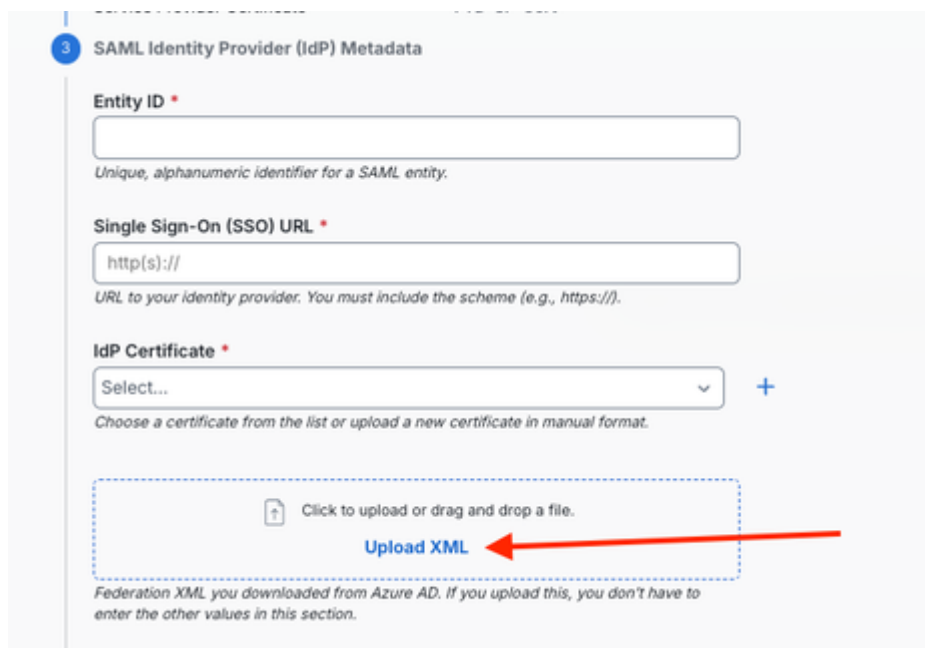
Blader omlaag naar SAML-certificaten en exporteer het Azure-gegenereerde Federation Metadata XML-bestand voor import in Cisco Secure FMC.



XML-bestand met metagegevens van federatie exporteren

Stap 3: Configureer het Azure SAML/Entra ID Realm met behulp van de FMC Wizard (vervolg)

1) Navigeer terug naar het VCC. Upload onder Volgorde 3, SAML Identity Provider (IdP) Metadata, het geëxporteerde Federation Metadata XML-bestand dat van Azure naar de FMC is gedownload om de benodigde waarden automatisch in te vullen.



Upload Federation Metadata XML-bestand

2) Eenmaal geüpload, vullen de waarden zoals weergegeven.

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

Automatisch ingevulde SAML-identiteitsproviderwaarden



Opmerking: Gedeeltelijke uitvoer wordt weergegeven in de afbeelding.

3) Voer de verzamelde waarden in tijdens het implementatieproces tot op dit punt:

- App-registratie
 - Applicatie-ID (client)
 - Clientgeheim
 - Directory-ID (huurder)
- Event Hub
 - EH-naamruimte-hostnaam
 - EH-naamruimte Primaire verbindingssreeks
 - Naam van instantie EH (Event Hub)
 - Naam EH Consumer Group

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

Voer de gegevens van de toepassing en de gebeurtenishub in

Eenmaal ingevoerd, klikt u op Test om de verbinding te controleren en te bevestigen dat Azure bereikbaar is met de verstrekte informatie.



Opmerking: zorg ervoor dat de Uitgesloten/Ingesloten gebruikersgroepen overeenkomen met uw Entra-configuratie

4) In de laatste stap van de wizard kunt u de time-out voor SAML Captive Portal-gebruikers configureren. De standaardwaarde is 1440 minuten.

5 User Session Timeout

SAML Captive Portal Users

1440 Minutes Range 0-35791394

Time-out voor captive portal configureren

5) Klik op Volgende om door te gaan.

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

Vooruit met Azure AD Realm Configuration

6) De wizard geeft een overzicht van de geïmplementeerde configuratie. Klik aan het einde van de samenvatting op Opslaan nadat de ingevoerde waarden zijn gevalideerd en bevestigd.

5 User Session Timeout Edit

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

Cancel Save

Overzicht Realm-configuratie Knop Opslaan

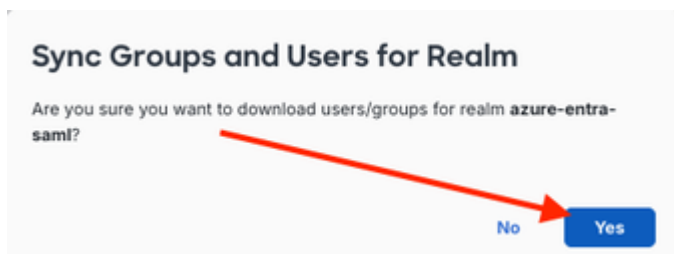
Stap 4: Controleer gedownloade gebruikers

1) Bevestig dat gebruikers kunnen worden gedownload van Azure Entra met de Download Now-knop binnen Integrations > Identity > Realms-workflow.

Name	Type	Description	Proxy	Status	Value	
azure-entra-saml	SAML - Azure AD (captive portal)	Active Authentication IdP	Not Applicable	Ok	Tenant ID: af42bac0-1	Enabled Download Now

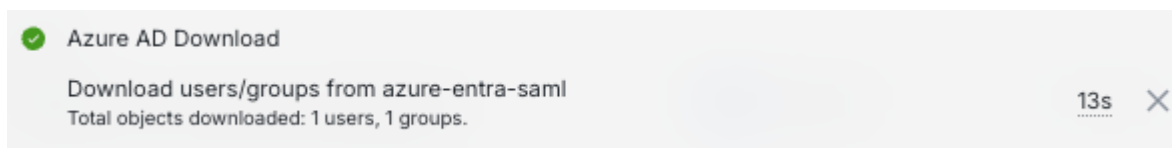
Gebruikers downloaden van Azure AD

2) Klik op Ja als reactie op de dialoogprompt.



Bevestig het downloaden van gebruikers van Azure AD

3) De downloadtaak levert 1 gebruiker en 1 groep gedownload, zoals bevestigd onder Meldingen > Taken.

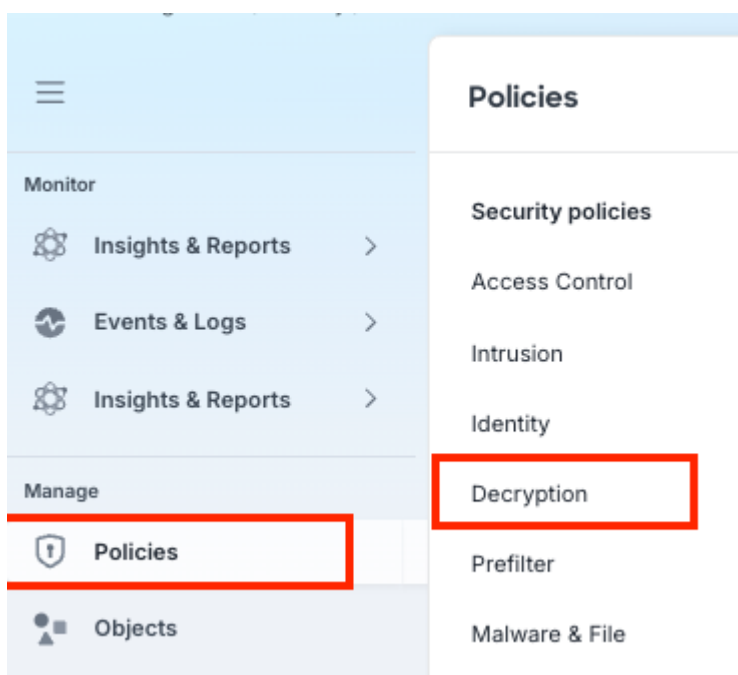


Melding voor het downloaden van gebruikers van Azure AD

Fase 5: Beleid configureren in het VCC

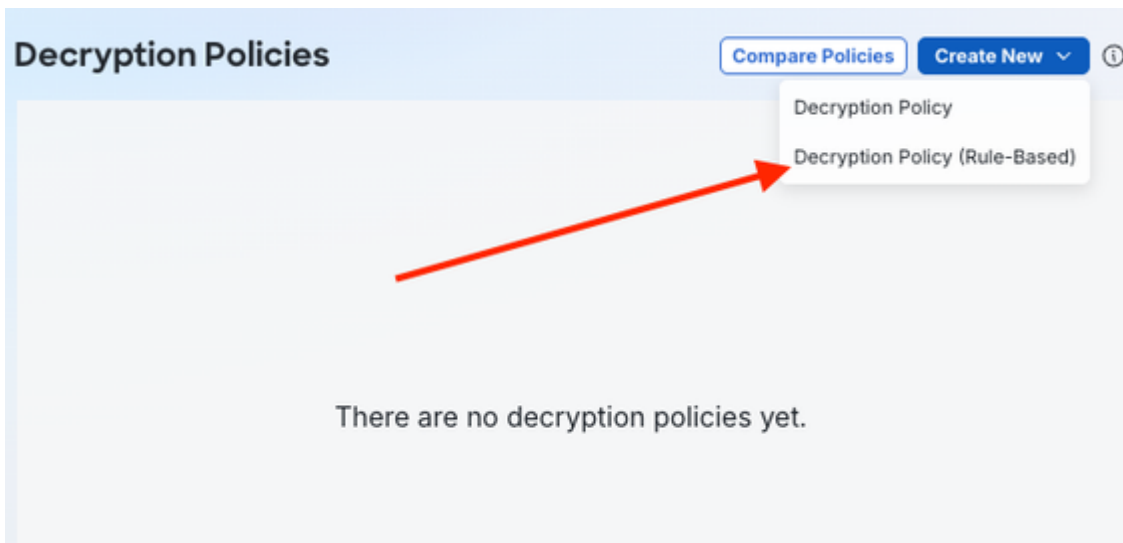
Stap 1: Decryptiebeleid configureren

1) Kies in het VCC Beleid > Beveiligingsbeleid > Decryptie.



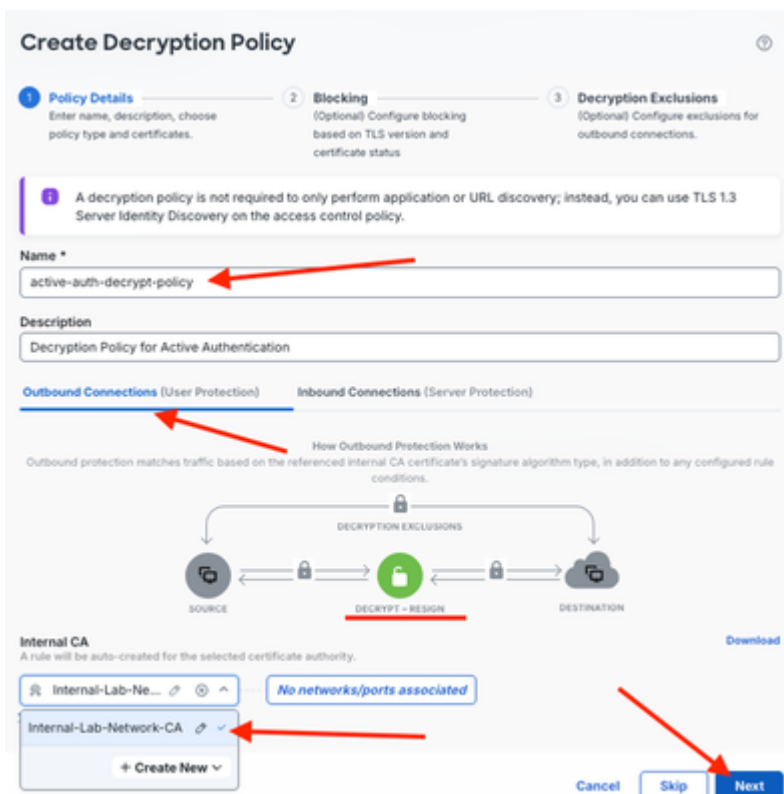
Navigeer naar decoderingsbeleid

2) Klik op de vervolgkeuzelijst Nieuw maken en kies Decryptiebeleid (op regels gebaseerd).



Nieuw op regels gebaseerd decoderingsbeleid maken

3) Wijs een naam en, indien gewenst, een beschrijving toe aan het nieuwe op regels gebaseerde decoderingsbeleid en klik op de taboptie Uitgaande verbindingen (Gebruikersbescherming) om de functionaliteit Decrypt-Resign te implementeren die vereist is voor interne portaalverificatie (Active Authentication).



Beleidsdetails voor uitgaande verbindingen implementeren

4) Kies de eerder toegepaste interne CA uit de toepasselijke vervolgkeuzelijst in hetzelfde

dialogovenster. Klik op Next (Volgende).

5) Pas de opties zo nodig aan.

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](#)

Opties voor decoderingsbeleid aanpassen

6) In dit voorbeeld worden standaardwaarden gebruikt, met uitzondering van de vereiste beleidsgegevens. Vul de configuratiewizard in door op Beleid maken te klikken.

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** New
 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

Definitief decoderingsbeleid maken

Stap 2: Decryptiebeleidsregels configureren

1) De standaardlay-out van een op regels gebaseerd decoderingsbeleid wordt hier weergegeven. Verkeer dat niet overeenkomt met de standaard ingeschakelde regels, zoals regel 3 (die verwijst naar een vooraf toegewezen lijst met niet-decodeerbare domeinnamen) en regel 6 (die verwijst naar toepassingen die zijn getagd als niet-decodeerbaar), is onderworpen aan de actie Decrypt - Ontslag onder regel 7. Deze standaardinstellingen kunnen, samen met de standaardactie, indien nodig worden gewijzigd. Standaard wordt verkeer dat overeenkomt met geen andere regel geconfigureerd als Niet decoderen.

Het verkeer van de Azure Authentication Service mag niet worden ontsleuteld voor inspectie, dus er wordt een speciale regel voor gemaakt. Klik op + Regel toevoegen om te beginnen.

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

Regel toevoegen en decoderingslay-out op basis van standaardregel weergeven

2) Wijs een naam toe aan de nieuwe regel voor het decoderingsbeleid, kies Niet decoderen uit de vervolgkeuzelijst Actie en plaats de regel bovenaan, minder specifieke regels. Bron-/bestemmingszones worden ook geïmplementeerd om de regel verder te beperken.

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

Regel Niet decoderen configureren

3) Voordat de regel wordt toegevoegd, klikt u op het tabblad Toepassingen, zoekt u naar en klikt u

op de toepassing Azure Authentication Service. Klik op Toevoegen aan regel en klik vervolgens op Toevoegen.

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

All apps matching the filter

- Azure Arc
- Azure Authentication Service**

Selected Applications and Filters (0)

any

Azure Authentication Service Application Rule toevoegen

4) Klik op Opslaan.

active-auth-decrypt-policy

Decryption Policy for Active Authentication

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

You have unsaved changes

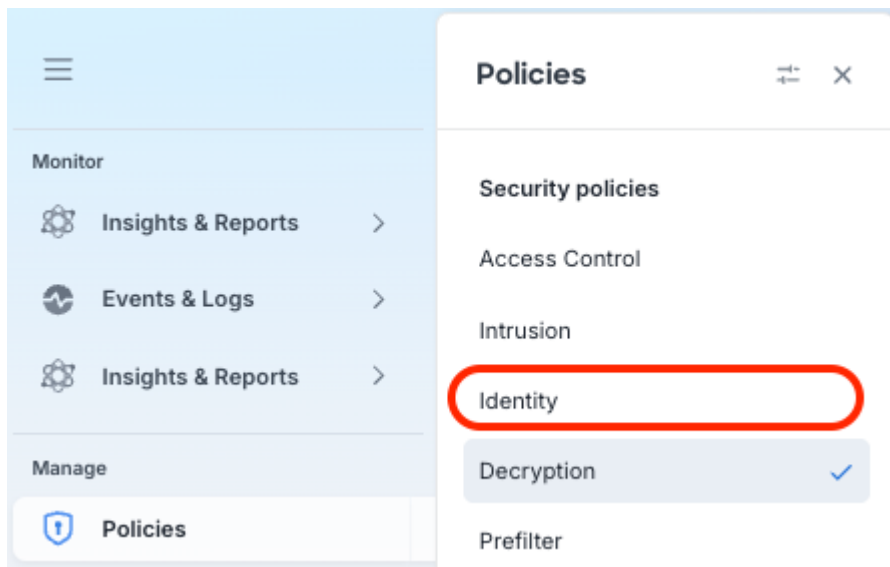
+ Add Category + Add Rule

#	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

Decryptiebeleid opslaan

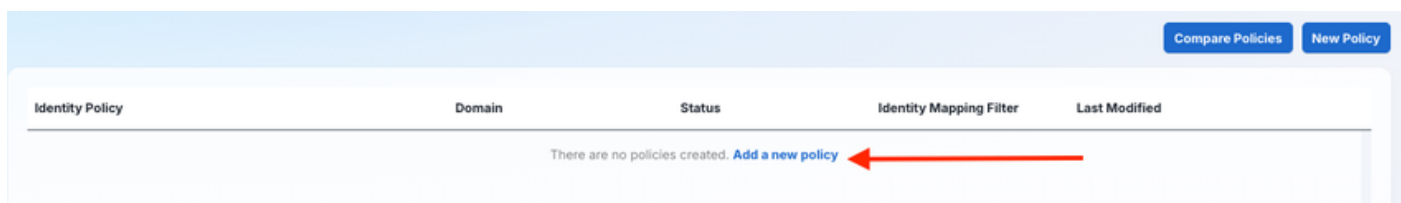
Stap 3: Creëer een identiteitsbeleid

1) Kies Beleid > Beveiligingsbeleid > Identiteit om een Identiteitsbeleid te maken.



Identiteitsbeleid maken

2) Maak een nieuw identiteitsbeleid en klik op Een nieuw beleid toevoegen.



Configuratie nieuw identiteitsbeleid toevoegen

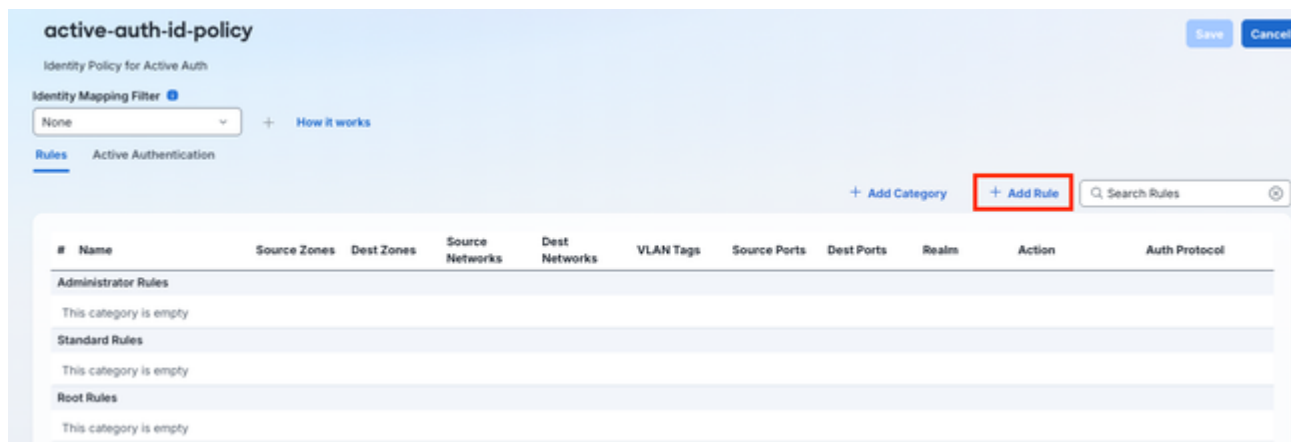
3) Wijs een naam en, indien van toepassing, een beschrijving toe aan het nieuwe identiteitsbeleid. Klik op Save (Opslaan).

A screenshot of a form titled 'New Identity policy'. 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.

Naam Nieuw identiteitsbeleid

Stap 4: Identiteitsbeleidsregels configureren

1) Voeg een nieuwe regel toe door op + Regel toevoegen te klikken.



Nieuwe regel voor identiteitsbeleid toevoegen

2) Geef de nieuwe regel een naam, kies Actieve verificatie in de vervolgkeuzelijst Actie en vernauw de specifieke zones/netwerken die moeten overeenkomen met de regel om Actieve verificatie uit te voeren.

Instellingen voor actieve verificatieregels configureren

3) Voordat u op Toevoegen klikt, klikt u op het tabblad Realm en instellingen in de Regeleditor. Bevestig dat het rijk dat in de vorige stappen is geconfigureerd, is gekozen als het verificatierijk en

klik vervolgens op Toevoegen.

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

Realm en instellingen voor identiteitsregel configureren

4) De regel wordt toegevoegd en geconfigureerd. Klik op Save (Opslaan).

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											

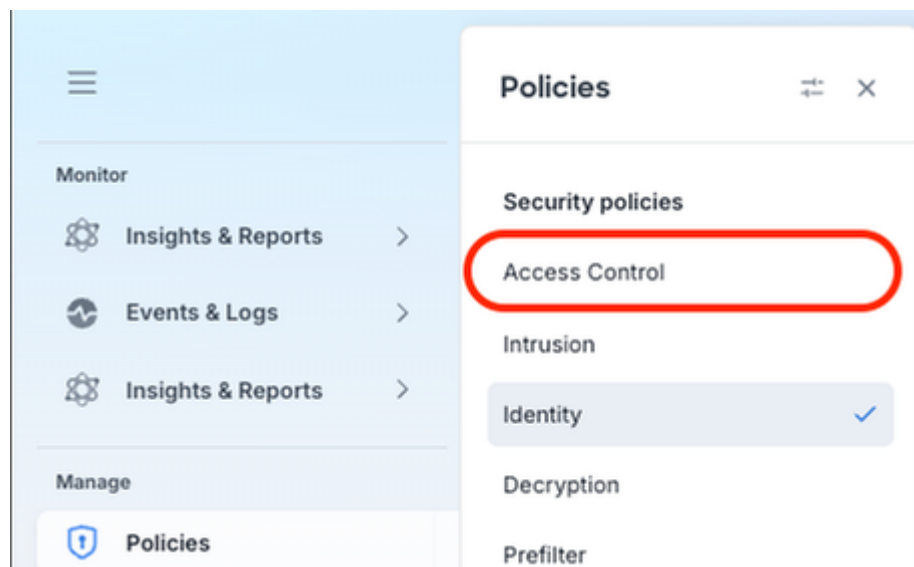
You have unsaved changes [Save](#) [Cancel](#)

Configuratie van regel voor identiteitsbeleid opslaan

Stap 5: Configureer het toegangscontrolebeleid

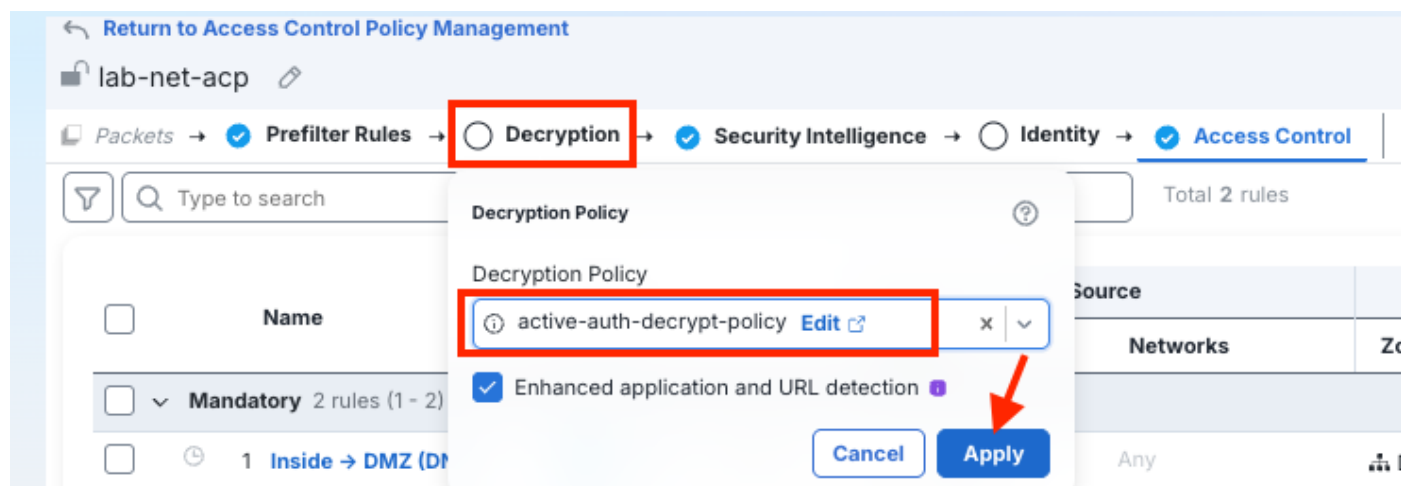
1) Kies Beleid > Beveiligingsbeleid > Toegangsbeheer en klik op het Toegangsbeheerbeleid

waaraan de FTD is toegewezen.



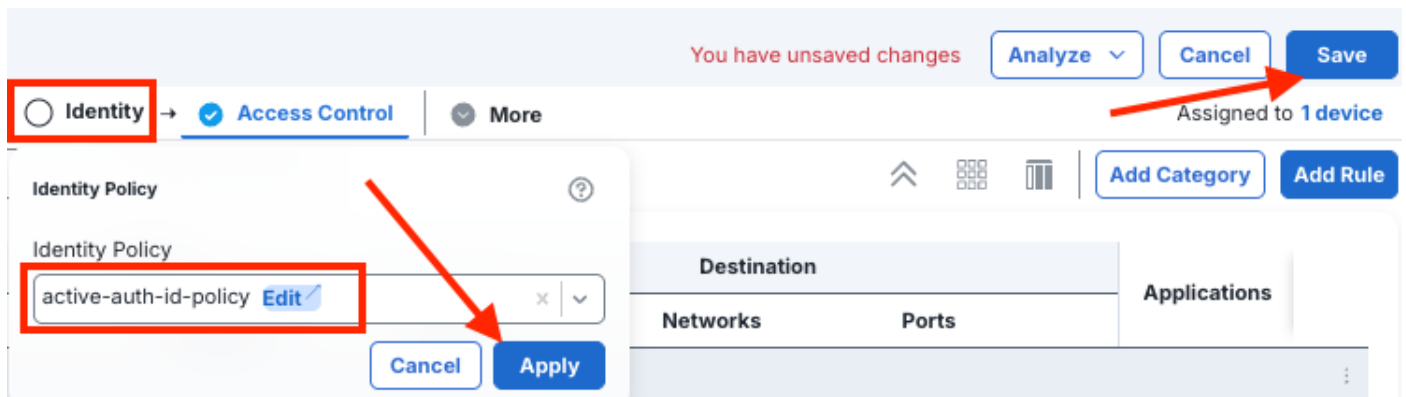
Configuratie toegangscontrolebeleid

2) Bevestig dat het decoderingsbeleid dat in de vorige stappen is geconfigureerd, wordt toegepast op het toegangscontrolebeleid.



Het decoderingsbeleid toepassen op toegangscontrole

3) Bevestig dat het identiteitsbeleid dat in de vorige stappen is geconfigureerd, ook wordt toegepast op het toegangscontrolebeleid. Sla de beleidswijzigingen op.



Identiteitsbeleid toepassen op toegangscontrole

4) Bevestig dat er regels bestaan die het verkeer van clientgegevens via de Secure Firewall toestaan na succesvolle actieve verificatie. Het voorbeeld dat hier wordt getoond, gebruikt een bredere regelset gezien de laboratoriumomgeving.

	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	Any	Outside_Zone	Any	Any	Any
Default (No rules)								

Verkeersregelset voor gebruikersgegevensvlak

Stap 6: Configuraties implementeren op de Cisco Secure Firewall-apparaten

Eenmaal geïmplementeerd, worden clients die verkeer verzenden, gevraagd met een Microsoft Sign-in-webpagina om Active Authentication met Azure Entra uit te voeren.

Zie [Een Microsoft Azure AD \(SAML\)-domein maken voor actieve verificatie \(captive portal\) - Hoofdstuk: Realms in FMC Device Config Guide 10.x voor](#) meer context over het hier gedocumenteerde proces.

Verifiëren

Gebruik deze sectie om te bevestigen dat de configuratie goed werkt.

GUI

Gebruikerssessies en -activiteiten in het VCC valideren:

- Kies Integraties > Gebruikers > Actieve sessies.

The screenshot shows the Cisco FMC interface with the 'Active Sessions' view selected. The left sidebar contains 'Monitor', 'Insights & Reports', 'Events & Logs', and 'Manage'. The main content area displays a table of active sessions. The table has columns: Login Time, Realm/Username, Last Seen, Authentication Type, Current IP, Session Duration, Realm, and Username. A single session is listed with a login time of 2026-10-07 02:10:02, realm/username of azure-entra-saml/captive-pc, last seen at 2026-10-07 02:10:02, authentication type of Active Authentication, current IP, session duration of 1 min 40 sec, realm of azure-entra-saml, and username of captive-portal-user. The interface includes a search bar, a 'Switch to legacy UI' toggle, and buttons for 'Refresh' and 'Delete'.

☐	Login Time	Realm/Username	Last Seen ↓	Authentication Type	Current IP	Session Duration	Realm	Username
☐	2026-10-07 02:10:02	azure-entra-saml/captive-pc	2026-10-07 02:10:02	Active Authentication		1 min 40 sec	azure-entra-saml	captive-portal-user

FMC Active Sessions-uitvoer

- Kies Integraties > Gebruikers > Gebruikersactiviteit.

The screenshot shows the Cisco FMC interface with the 'User Activity' view selected. The left sidebar contains 'Monitor', 'Insights & Reports', 'Events & Logs', and 'Manage'. The main content area displays a table of user 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 start port. The interface includes a search bar, a 'Switch to legacy UI' toggle, and buttons for 'Refresh', 'Delete', and 'Delete All'.

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

FMC-gebruikersactiviteitsuitvoer

Navigeer op Azure naar het Microsoft Entra Admin Center:

- Filter Enterprise Apps, zoek naar/klik op de toepasselijke app.

The screenshot displays the Microsoft Entra admin center interface. On the left, the navigation pane includes sections like Home, Favorites, and Entra ID. The 'Enterprise apps' option is highlighted with 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' category in the 'Manage' section to the 'Captive-Auth...' application in the list. The list has columns for Name, sort order (up/down arrows), and Object ID (Obj).

Name	Sort	Obj
Captive-Auth...	↑↓	efda

Azure Entra Admin Center Enterprise Apps Navigation

- Kies Activiteit > Aanmeldingslogs.

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

Activiteitenlogboeken voor aanmelding bij Azure Enterprise Application

CLI

- In de FTD CLI ziet u statistieken met betrekking tot SAML en captive portal reacties:

<#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
```

Problemen oplossen

Debug in captive-portaal

- De opdracht `captive-portal-debug` voor systeemondersteuning kan op de FTD worden gebruikt. De uitvoer laat zien hoe u de foutopsporing kunt inschakelen en noteert ook belangrijke segmenten van de uitvoer om de Captive Portal-stroom te helpen begrijpen.

```
<#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
...
```

Dump van gebruikersidentiteit

- Als u een momentopname wilt maken van de huidige gegevens over de gebruikersidentiteitsstatus op de FTD, voert u de opdracht **Systeemondersteuning firewall-engine-dump-user-identity-data** uit op de FTD CLI:

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

Successfully commanded snort.

>

- In expert mode CLI, terwijl u inlogt met lokale admin referenties van het FTD-apparaat, bekijk de inhoud van het gedumpte bestand in
/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:

...

Mogelijke problemen

Captive Portal Unknown Certificate Authority

Probleem: de clientbrowser geeft een onbekende fout van de uitgever terug wanneer de verificatie wordt geprobeerd.

Waarschijnlijke oorzaak: de interne certificeringsinstantie is niet vertrouwd in de clientbrowser.

Resolutie: Bevestig dat de CA vertrouwd is in de browser. Het hier getoonde voorbeeld bevestigt dat het interne CA-certificaat vertrouwd is.

Captive Portal "Server niet gevonden

Probleem: Wanneer de clientbrowser probeert het captive-portaal te laden, retourneert het "Server Not Found" voor de basis-URL terwijl het probeert de basis-URL of iets dergelijks te bereiken.

Waarschijnlijke oorzaak: DNS-bereikbaarheid of verkeerde DNS-configuratie.

Resolutie: Bevestig dat de client de juiste DNS-server heeft geconfigureerd om de A-record op te lossen. Bevestig dat de server een A-record heeft dat is toegewezen aan het FQDN en dat deze bereikbaar en responsief is.

Gerelateerde informatie

- [Een Microsoft Azure AD \(SAML\)-domein maken voor actieve verificatie \(captive portal\) - FMC Device Config Guide 10.x](#)
- [Documentatie Azure Event Hub](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.