

Configure Azure Entra Captive Portal on Secure Firewall

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Diagram](#)

[Captive Portal Between Endpoint, FTD, and Azure Entra](#)

[Configure](#)

[Phase 1: Initial FMC and DNS Configuration](#)

[Step 1: Enable the Cisco Dynamic Attributes Connector \(CSDAC\)](#)

[Step 2: Create a Fully Qualified Domain Name Network Object Representative of the FTD Ingress Interface](#)

[Step 3: Configure the DNS A Record](#)

[Phase 2: Public Key Infrastructure Configuration](#)

[Step 1: Import the Internal CA Certificate to the FMC](#)

[Step 2: Sign the Service Provider Certificate with the CA](#)

[Step 3: Deploy the SP Certificate to the FTD](#)

[Phase 3: Azure Configuration](#)

[Step 1: Create the Entra Enterprise Application for the SAML Toolkit](#)

[Step 2: Configure Entra ID App Registrations](#)

[Step 3: Configure Microsoft Graph API Permissions for the App Registration](#)

[Step 4: Configure the Event Hub \(EH\) Namespace](#)

[Step 5: Choose or Create Shared Access Policies in the Event Hub Namespace](#)

[Step 6: Collect and Note Shared Access Signature \(SAS\) Information from the EH Namespace](#)

[Step 7: Create an Event Hub Instance Within the Event Hub Namespace](#)

[Step 8: Create an Event Hub Instance Consumer Group Within the Event Hub Namespace](#)

[Step 9: Verify Collected Values](#)

[Step 10: Configure Entra ID Audit Log Streaming to the Event Hub](#)

[Phase 4: Consolidate Azure and FMC/FTD Active Authentication Configuration](#)

[Step 1: Configure the Azure SAML/Entra ID Realm Using the FMC Wizard](#)

[Step 2: Implement the FMC-Configured SAML SP Metadata in the Azure Enterprise Application](#)

[Step 3: Configure the Azure SAML/Entra ID Realm Using the FMC Wizard \(Continued\)](#)

[Step 4: Check Downloaded Users](#)

[Phase 5: Configure Policies in the FMC](#)

[Step 1: Configure Decryption Policy](#)

[Step 2: Configure Decryption Policy Rules](#)

[Step 3: Create Identity Policy](#)

[Step 4: Configure Identity Policy Rules](#)

[Step 5: Configure the Access Control Policy](#)

[Step 6: Deploy Configurations to the Cisco Secure Firewall Devices](#)

[Verify](#)

[GUI](#)

[CLI](#)

[Troubleshoot](#)

[Captive Portal Debug](#)

[User Identity Dump](#)

[Possible Issues](#)

[Captive Portal Unknown Certificate Authority](#)

[Captive Portal "Server Not Found"](#)

[Related Information](#)

Introduction

This document describes the configuration of Microsoft Azure Entra ID for use with captive portal (active authentication) on Cisco Secure Firewall.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

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

You must have the *Standard* pricing tier available in Azure for Event Hub creation. Additionally, devices must be activated with Smart Licensing enabled with export-controlled functionality.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure FTD version 10.0
- Cisco Secure FMC version 10.0

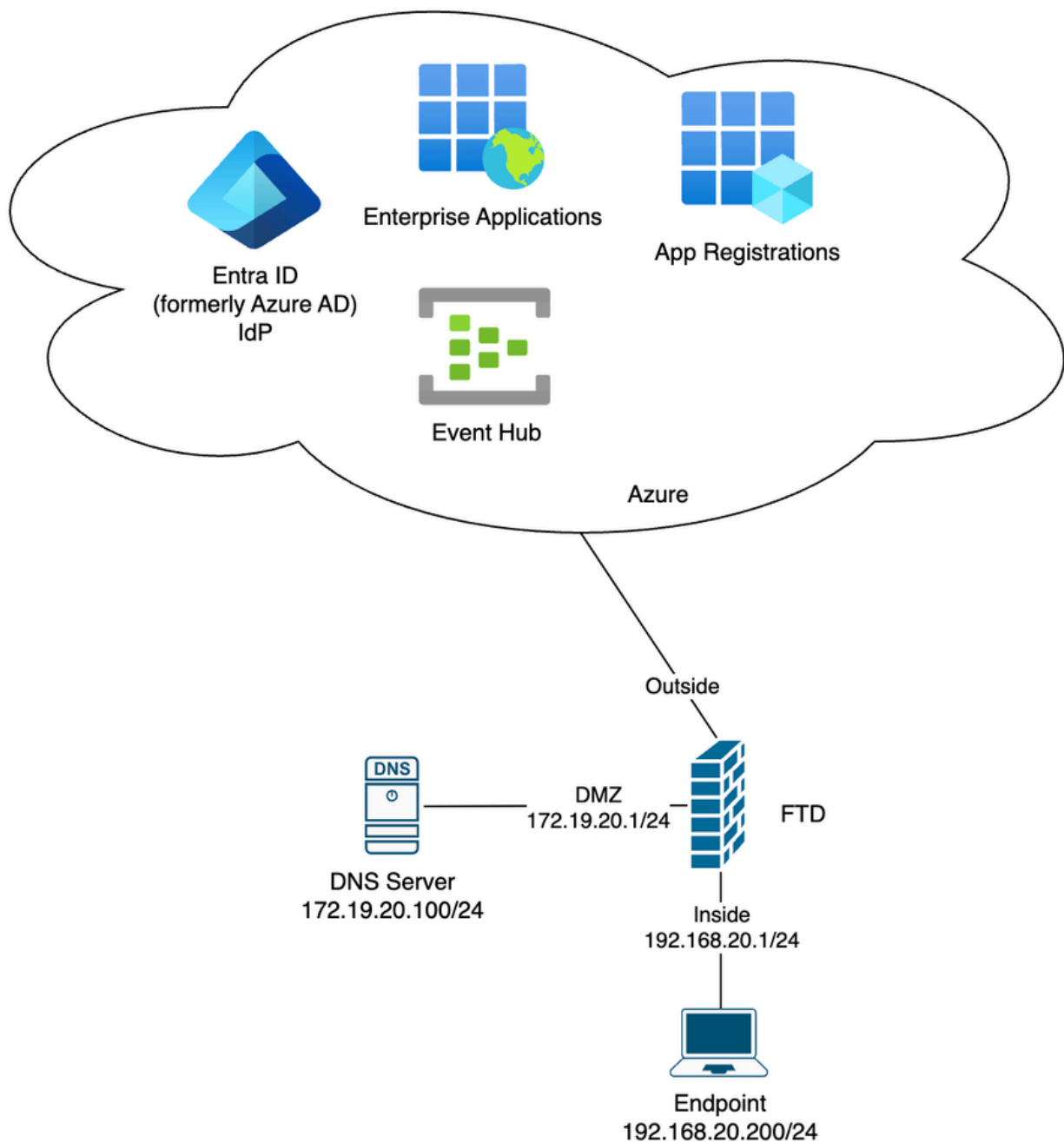
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

As traditional IP-based security architectures struggle to keep pace with dynamic, hybrid work environments, Cisco Secure Firewall Active Authentication with SAML integration offers a robust, identity-centric solution. By leveraging Microsoft Entra ID (Azure AD) as a centralized identity provider, this configuration enables administrators to move beyond static network rules and enforce granular access control based on verified user identity rather than volatile network addresses. This integration streamlines the user experience through seamless Single Sign-On (SSO) and mandatory Multi-Factor Authentication (MFA), while also ensuring a unified security posture that maintains strict visibility and policy enforcement across a perimeter-less network.

Diagram

Captive Portal Between Endpoint, FTD, and Azure Entra



Captive Portal Between EndPoint And Azure Entra

Configure

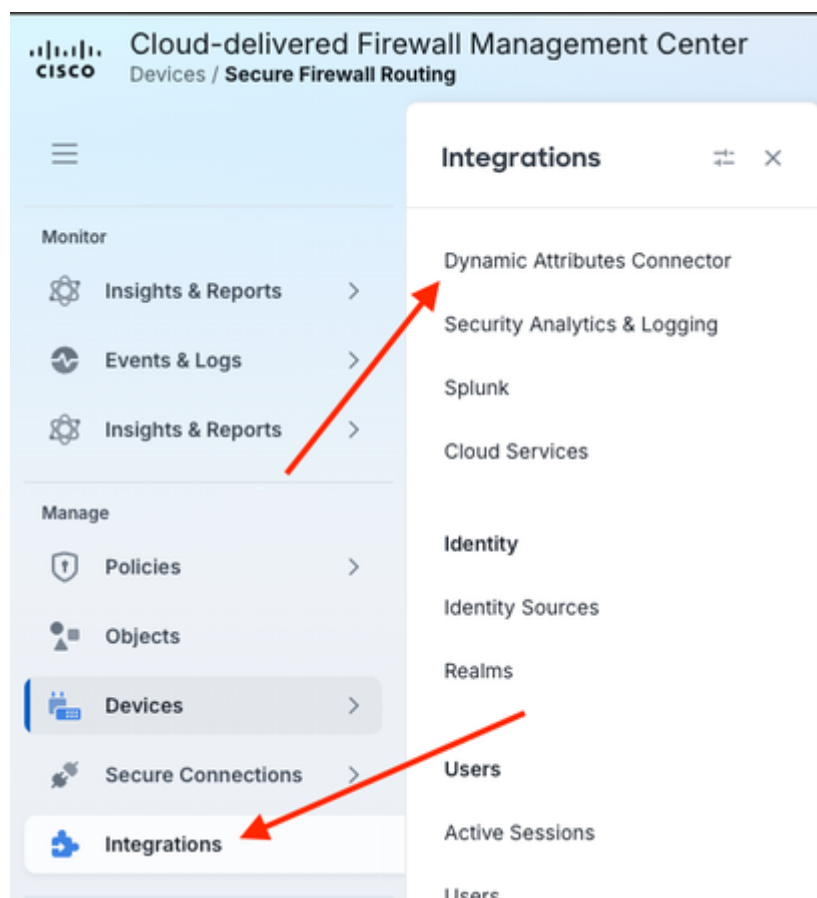
Phase 1: Initial FMC and DNS Configuration



Note: This lab uses cloud-delivered Firewall Management Center (cdFMC); however, the steps remain the same for on-premises FMC.

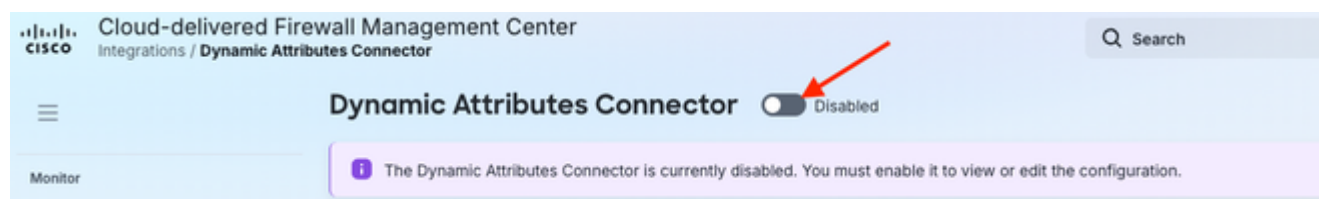
Step 1: Enable the Cisco Dynamic Attributes Connector (CSDAC)

1) Choose **Integrations** > **Dynamic Attributes Connector**.



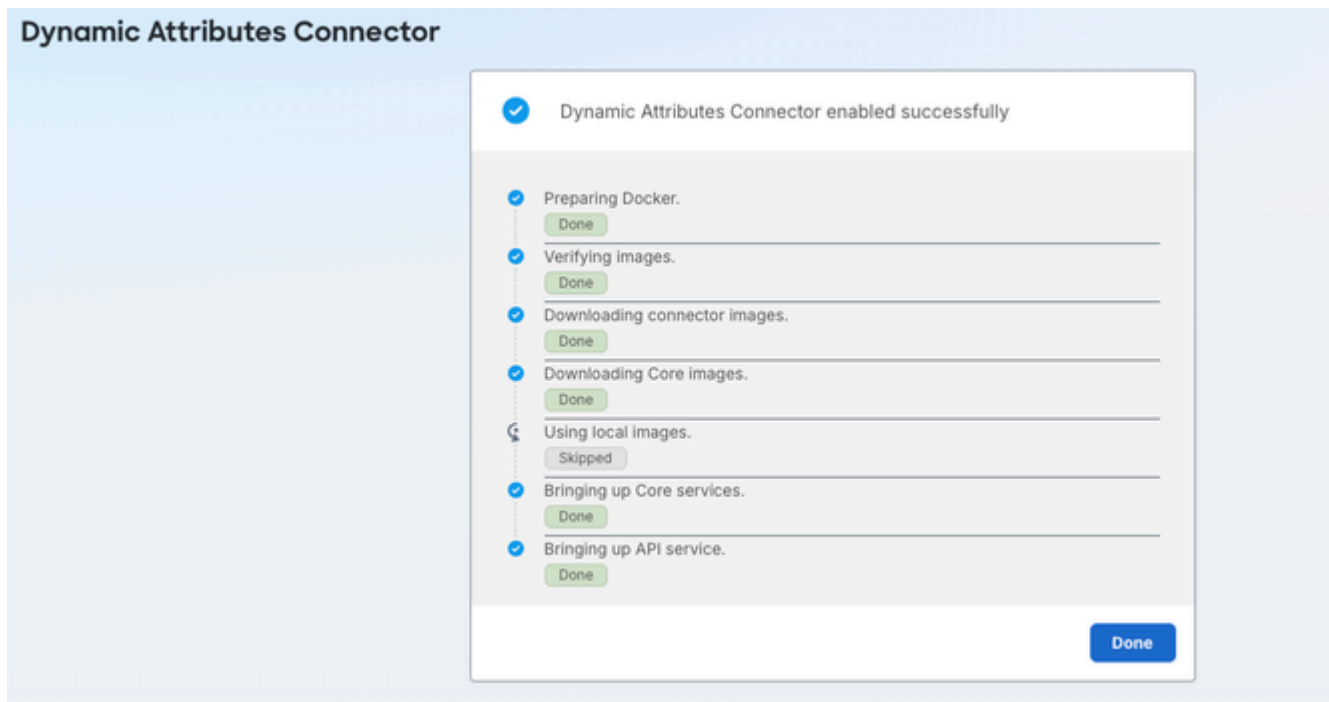
Choose Integrations Dynamic Attributes Connector

2) Click the **control** adjacent to the **Disabled** string to enable CSDAC.



Enable Cisco Dynamic Attributes Connector

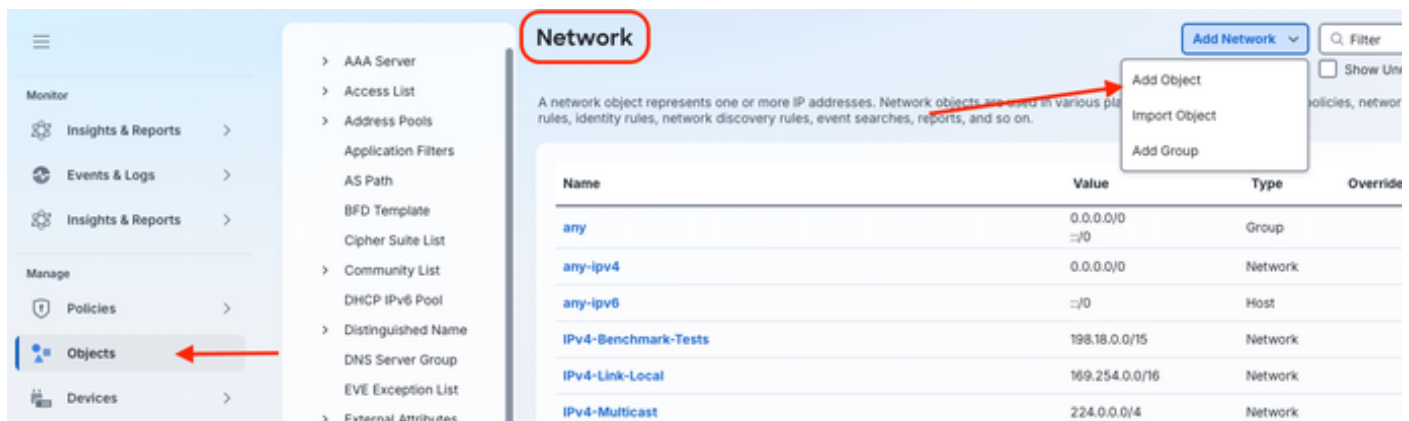
c) Click **Done** once CSDAC enablement completes.



Enable Cisco Dynamic Attributes Connector Status

Step 2: Create a Fully Qualified Domain Name Network Object Representative of the FTD Ingress Interface

1) Choose **Objects > Add Network > Add Object**.



Create New Fully Qualified Domain Name Network Object

2) Name the **Network Object** configured with the **Fully Qualified Domain Name (FQDN)**. Enter the **FQDN**, and assign the Network Object as an **FQDN type** by clicking the appropriate **radio button**. 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

Configure FQDN Network Object Variables

Step 3: Configure the DNS A Record

1) The example shown here uses Windows Server 2025; see the documentation for the specific name resolution server as needed.

The screenshot shows the Windows Server DNS console. In the left pane, the hierarchy is: DNS > DC > Forward Lookup Zones > example.com. The right pane displays a table of DNS records for the example.com zone.

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

Windows Server DNS A Record Configuration



Note: The client that performs Active Authentication must be able to resolve this DNS A record.

Phase 2: Public Key Infrastructure Configuration

An internal Certificate Authority (CA) can be used as the Public Key Infrastructure (PKI) for the Active Authentication configuration. Cisco FMC and FTD require the internal CA public key and paired Private Key to be uploaded as an Internal CA object to perform the necessary SSL interception and Decrypt-Resign operations. In addition, the internal CA must be trusted within the client browser from which Active Authentication is performed. See the client browser documentation to check how to confirm that the browser trusts the certificate.

Step 1: Import the Internal CA Certificate to the FMC

1) Choose **Objects > PKI > Internal CAs**. Click **Import CA**.



Note: The Internal CA can also be created directly on the FMC.

The screenshot shows the 'Import Internal Certificate Authority' form. It includes a 'Name' field with the value 'Internal-Lab-Network-CA'. Below it is a 'Certificate Data or, choose a file:' section with a 'Browse..' button. The text area contains '-----BEGIN CERTIFICATE-----' and '-----END PRIVATE KEY-----'. There is a similar section for the 'Key or, choose a file:' with another 'Browse..' button and the same placeholder text. At the bottom, there is a checkbox labeled 'Encrypted, and the password is:' which is checked, followed by a password field containing seven dots. 'Cancel' and 'Save' buttons are at the bottom right.

Import Internal Certificate Authority To Firewall Management Center



Note: Within the content of this document, white space appears covering the various field values in

the images and is intentional per the publishment of this document. Actual values are reflected for your environment as you configure.

Step 2: Sign the Service Provider Certificate with the CA

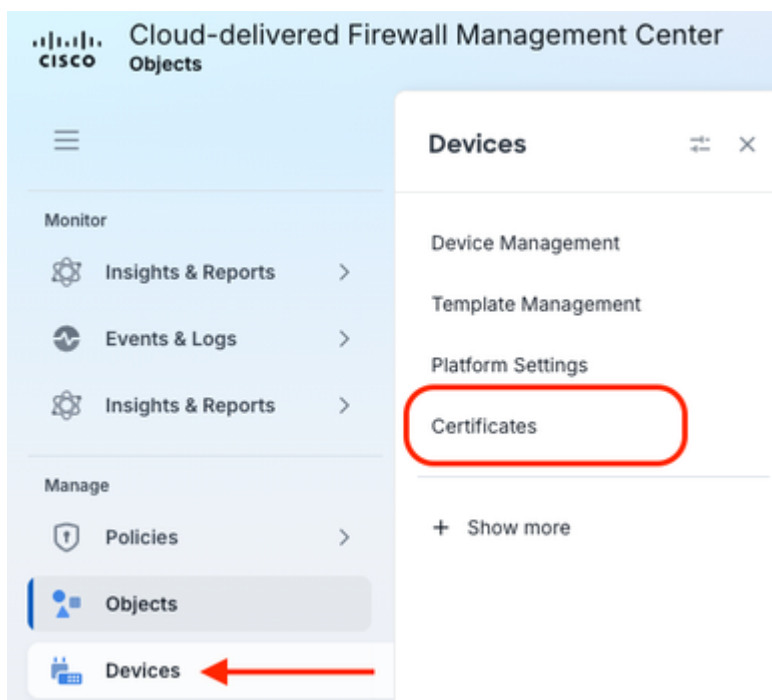
1) The Service Provider (SP) certificate must be signed by a trusted Certificate Authority (CA) and returned in a PKCS#12 (.p12) format.



Note: This CA can be internally signed. The only caveat is that the Internal CA must be trusted by the client device.

Step 3: Deploy the SP Certificate to the FTD

1) Choose **Devices > Certificates**.



Navigate To Devices And Certificates

2) Click **Add Certificates**.

Filter

All Certificates

Add

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
No certificates Add Certificates					

Add New Device Certificate

3) Click the **device** from the drop-down list that executes Active Authentication, then click the + **icon** to create a new **Certificate Enrollment**.

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*:

▼

+

Cancel

Add

Select FTD And Add Add New Certificate Enrollment

4) Name the **Certificate Enrollment**, and from the **Enrollment Type** drop-down list, choose **PKCS12 file**.

Add Certificate Enrollment ?

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:*

Challenge Password:

Confirm Password:

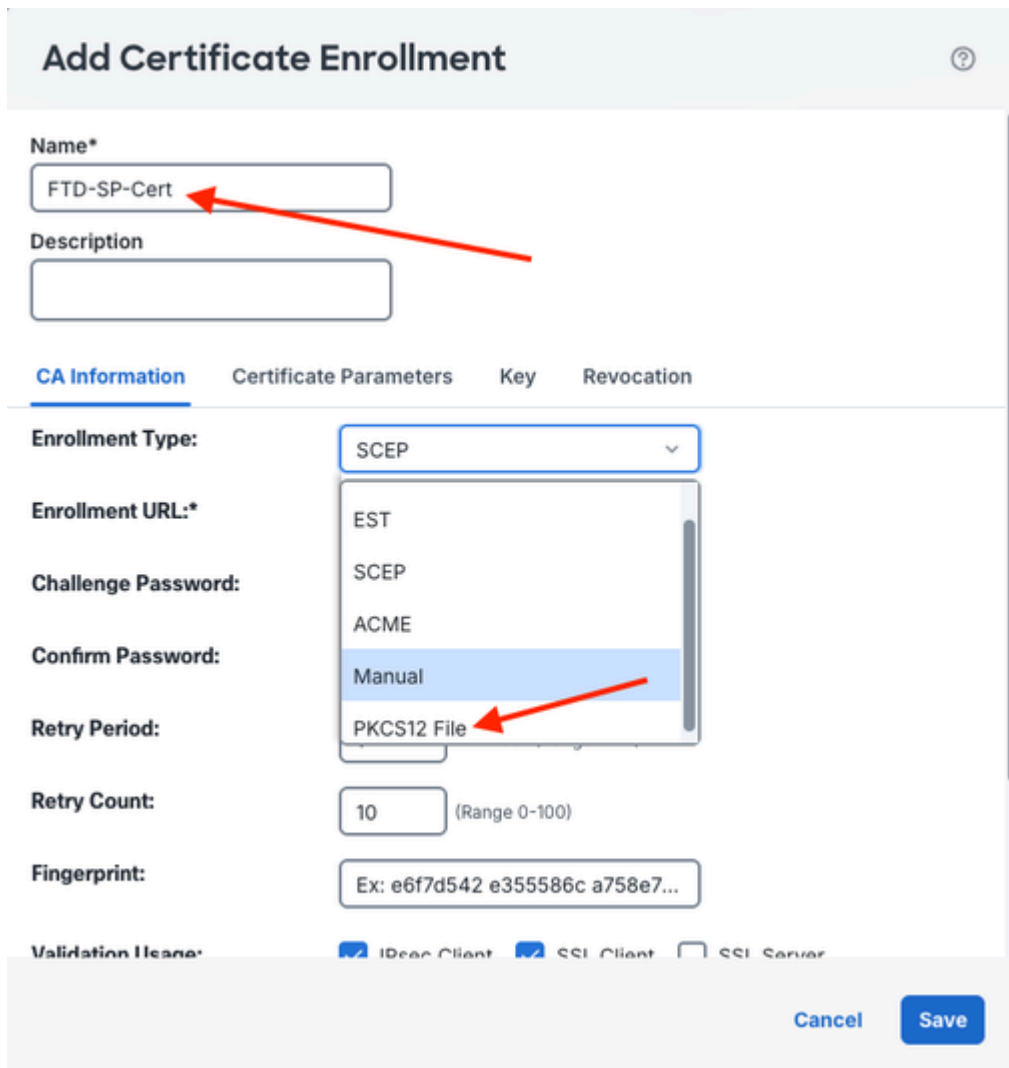
Retry Period:

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7...

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

Cancel Save



Certificate Enrollment Settings And Type

5) Import the **PKCS#12 file** by clicking **Browse PKCS12 File** and enter the **required passphrase**. 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

Browse And Import PKCS12 File

6) Confirm that the **enrollment details** are correct and click **Add**.

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 +

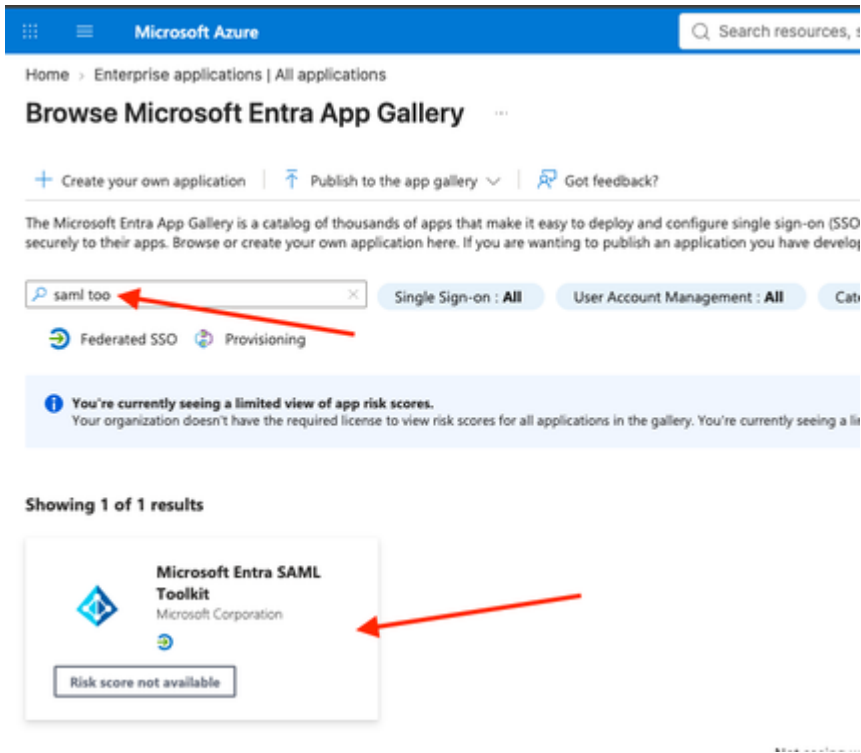
Certificate Enrollment Details:

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

Cancel Add

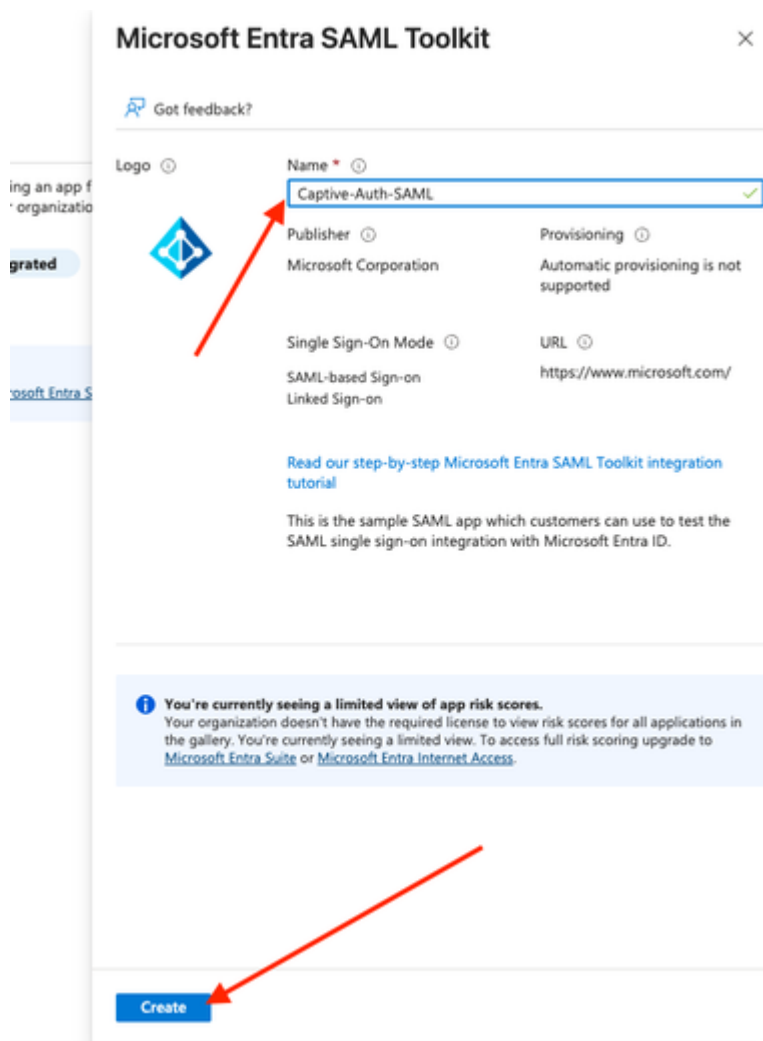
Confirm Certificate Enrollment Details

7) The import reflects **In progress**.



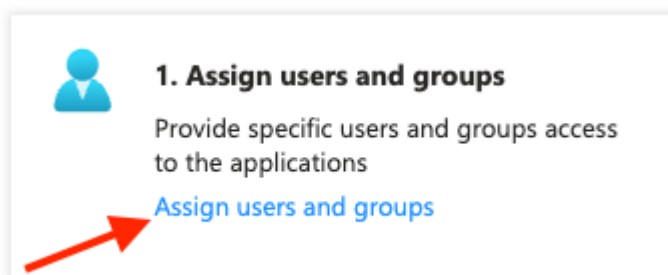
Search And Select Microsoft Entra SAML Toolkit

- 4) Assign a **Name** to the Microsoft Entra SAML Toolkit Enterprise Application and click **Create**.
(Reference from Microsoft: [Read our step-by-step Microsoft Entra SAML Toolkit integration tutorial](#)).



Assign Name To SAML Toolkit Application

5) On the **Overview** page, assign the **specific users and groups** to the SAML Toolkit Enterprise Application. In this example, the test account (captive-portal-user) is a member of the active-auth-lab group.

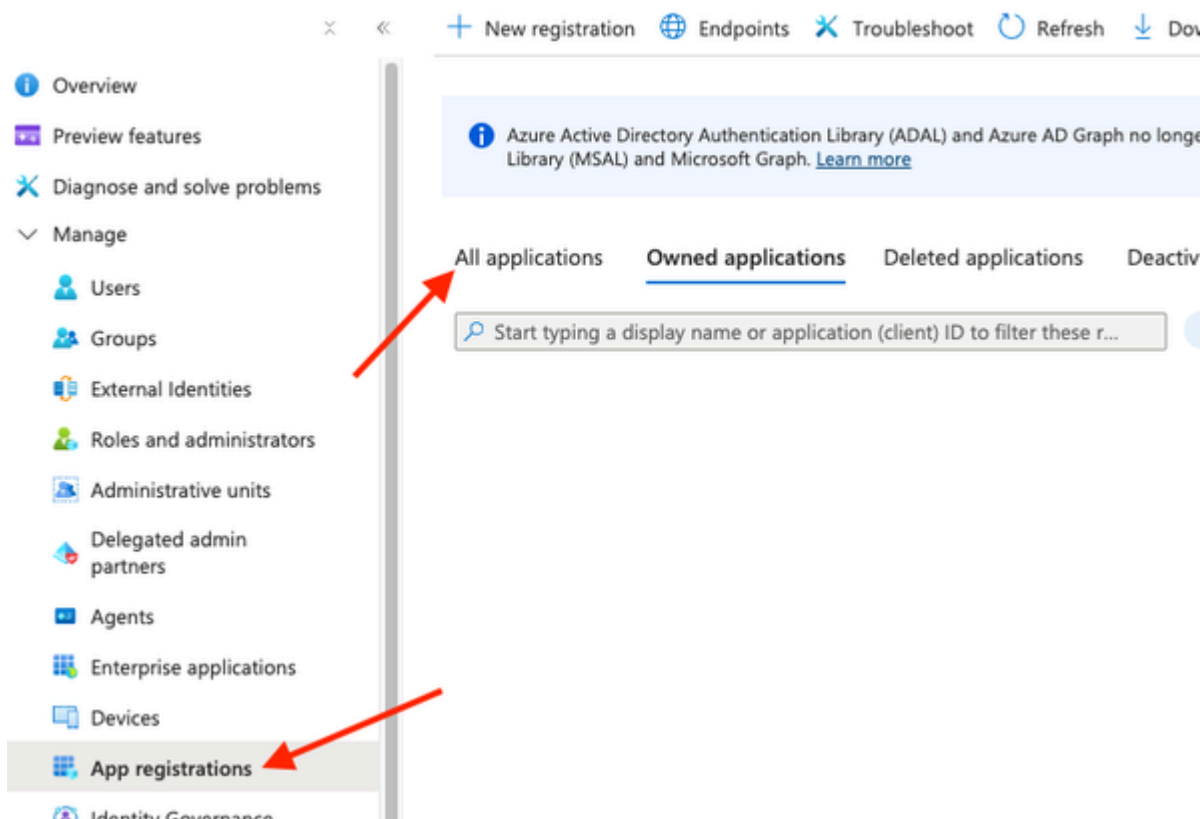


Assign Users And Groups To Application

6) Configuration of this Enterprise Application continues in later steps.

Step 2: Configure Entra ID App Registrations

1) Navigate back to **Entra ID** and from the left navigation menu, choose **App registrations**. Click the **All applications** filter and search for the name given to the Enterprise Application. Click the appropriate application.



Navigate To App Registrations And All Applications

2) Collect and Note the Essentials Values Under the **Enterprise App Registration**.



Important: Hover over the values to reveal **Copy to Clipboard** and collect the values under **Essentials** on the **Overview** page:

- Display Name
- Application (Client) ID
- Directory (Tenant) ID

Captive-Auth-SAML ✨ ...

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Essentials

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

Application (client) ID :

Object ID :

Directory (tenant) ID :

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

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

Collect Display And Application And Directory ID Values

3) Click the **Add a certificate or secret** hyperlink.

Captive-Auth-SAML ✨ ...

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

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 L... : [Captive-Auth-SAML](#)

State : Activated

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

Add Certificate Or Secret Hyperlink

4) Click + **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 location. 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.			

Add New Client Secret

5) Provide a **Description** for the secret and adjust the **expiration** as necessary. Click **Add**.

Add a client secret

Description:

Expires: Recommended: 180 days (6 months)

Add **Cancel**

Provide Description For Client Secret

6) Copy the **Secret**.



Important: Take note of the secret value copied to clipboard.

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.

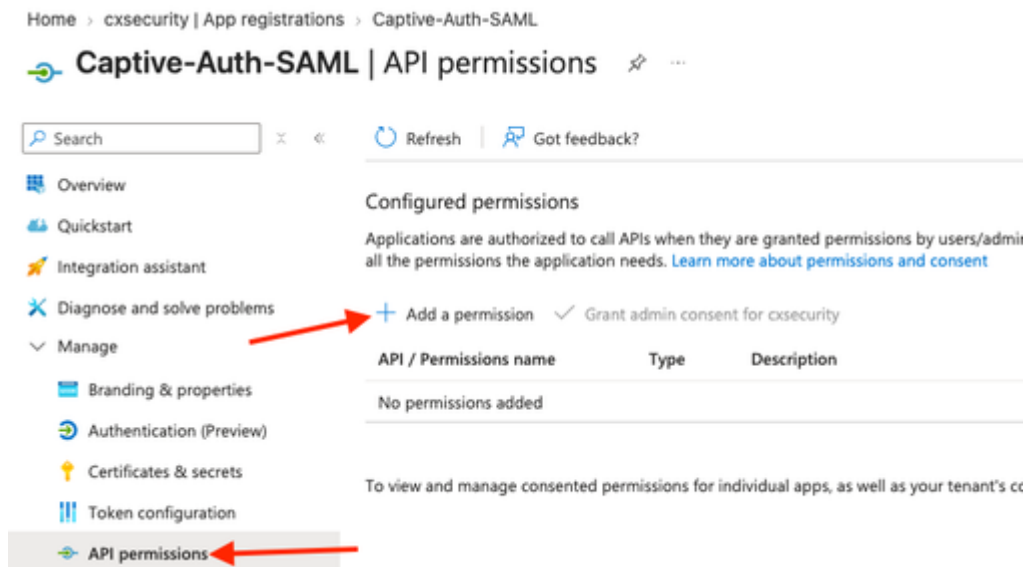
+ New client secret

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

Copy Client Secret Value

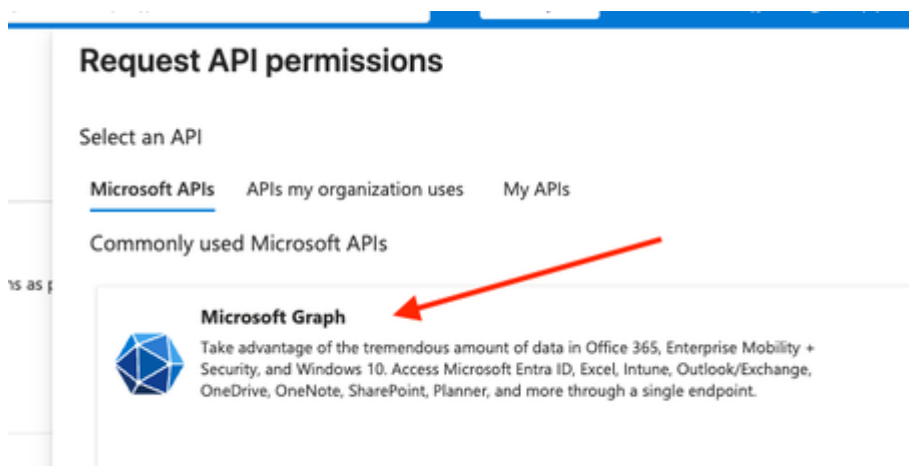
Step 3. Configure Microsoft Graph API Permissions for the App Registration.

1) Choose **API Permissions** from the left navigation menu, then click + **Add a permission**.



Configure API Permissions

2) Click **Microsoft Graph API**.



Select Microsoft Graph API

3) Grant **Delegated User.Read** permissions, then click **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](#)

Grant Delegated User Read Permissions

4) Grant Application **User.Read.All** permissions (check the check box).

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

Grant Application Read All Permissions

5) Search for and check the **Group.Read.All** check box to grant Group Read permissions as well. Click **Add permissions**.

Select permissions

[expand all](#)

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

Add permissions Discard

Save API Permissions

6) Confirm that the **configured permissions** align, and grant **administrative consent** for them.

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

Grant Administrative Consent For Permissions

7) The output, once admin consent is granted, is shown.

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

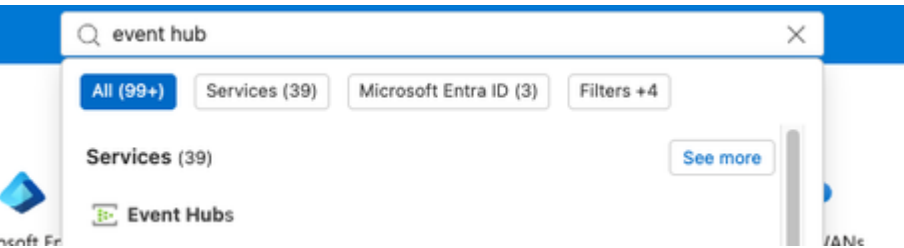
✓ Grant admin consent for

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

Administrative Consent Granted Output

Step 4: Configure the Event Hub (EH) Namespace

1) Search for and click **Event Hubs**.



Search Event Hub Configuration

2) Create a new **EH Namespace**.



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](#)

Create Event Hub Namespace

3) Configure the **EH Namespace**.



Note: The **Standard** pricing tier or higher must be chosen. **Basic** pricing tier prevents realm usage.

See the [Azure Event Hub Documentation](#) for further evaluation of Event Hub Advanced Settings and applicability to specific needs.

Click **Review + Create**.



Create Namespace

Event Hubs

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

Project Details

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

Subscription *

Resource group *

[Create new](#)

Instance Details

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

Namespace name * ☒ .servicebus.windows.net

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

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

Throughput Units *

Enable Auto-Inflate ? ☐

[Review + create](#)

< Previous

Next: Advanced >

Configure Event Hub Namespace Settings

4) Once validation succeeds, click **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 >

Create Event Hub Namespace Deployment

5) Confirm the deployment completes, then click **Go to resource**.

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

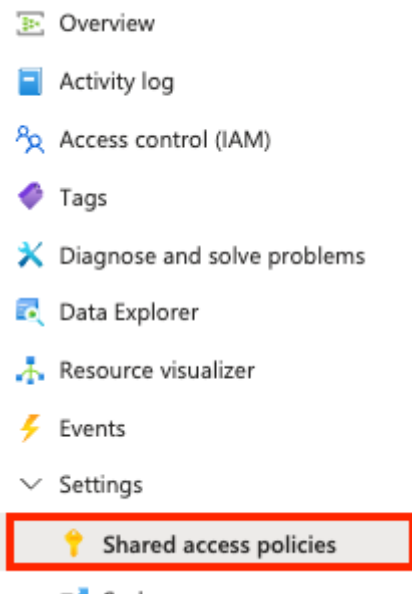
✓ Next steps

Go to resource

Go To Event Hub Namespace Resource

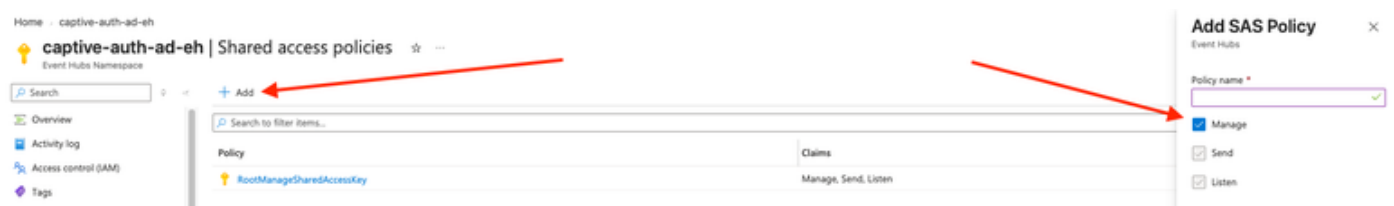
Step 5: Choose or Create Shared Access Policies in the Event Hub Namespace

1) From the left navigation menu, choose **Settings** > **Shared access policies**.



Navigate To Shared Access Policies

2) Click + **Add** and enter the new **Policy name**, and check the **Manage** check box. Click **Create** at the bottom of the **Add SAS Policy** menu panel.



Add New Shared Access Policy



Create Shared Access Policy

Step 6: Collect and Note Shared Access Signature (SAS) Information from the EH Namespace

1) Click the new **Shared access policy**; the EH SAS Policy appears in the side panel on the right.

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

Copy Primary Connection String



Important: Copy and note the Primary connection string.

Step 7: Create an Event Hub Instance Within the Event Hub Namespace

1) From the **Namespace** menu, choose **Entities > Event Hubs**. Click + **Event Hub** to create a new **EH instance**.

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Data Explorer

Resource visualizer

Events

Settings

Entities

Event Hubs

Schema Registry

+ Event Hub Refresh

Search to filter items by name...

Name

No Event Hubs yet.

2) Assign a **name** to the new EH instance, then click **Review + create**.

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

Create Event Hub

Event Hubs

Basics Capture Review + create

Event Hub Details

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

Name * ⓘ captive-auth-ad-eh-1 ✓

Partition count ⓘ 1

Retention

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

Cleanup policy ⓘ Delete

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

Review + create < Previous Next: Capture >

3) Once validation succeeds, click **Create** to provision the Event Hub instance.

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 >

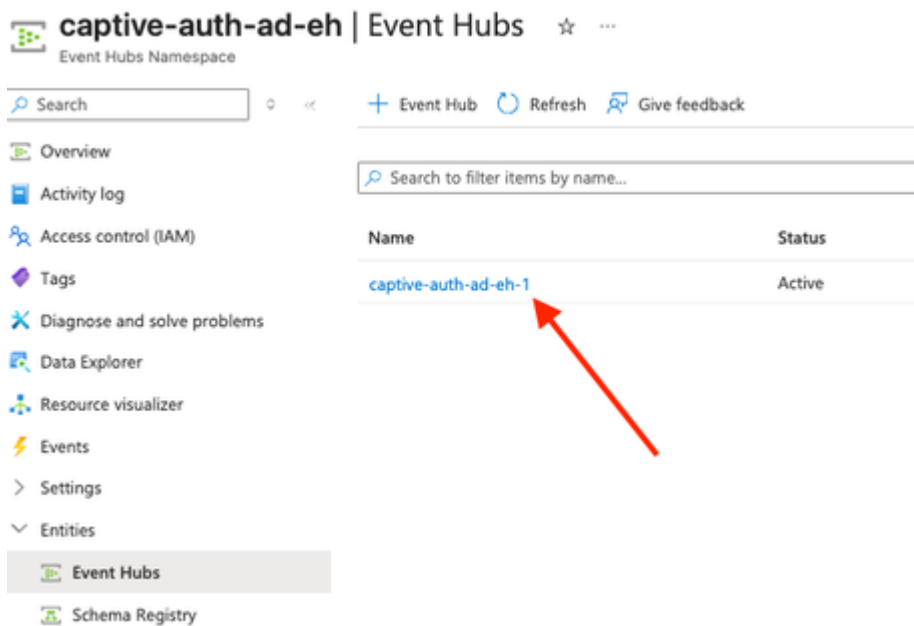
Provision Event Hub Instance



Important: Copy and note the Event Hub instance name.

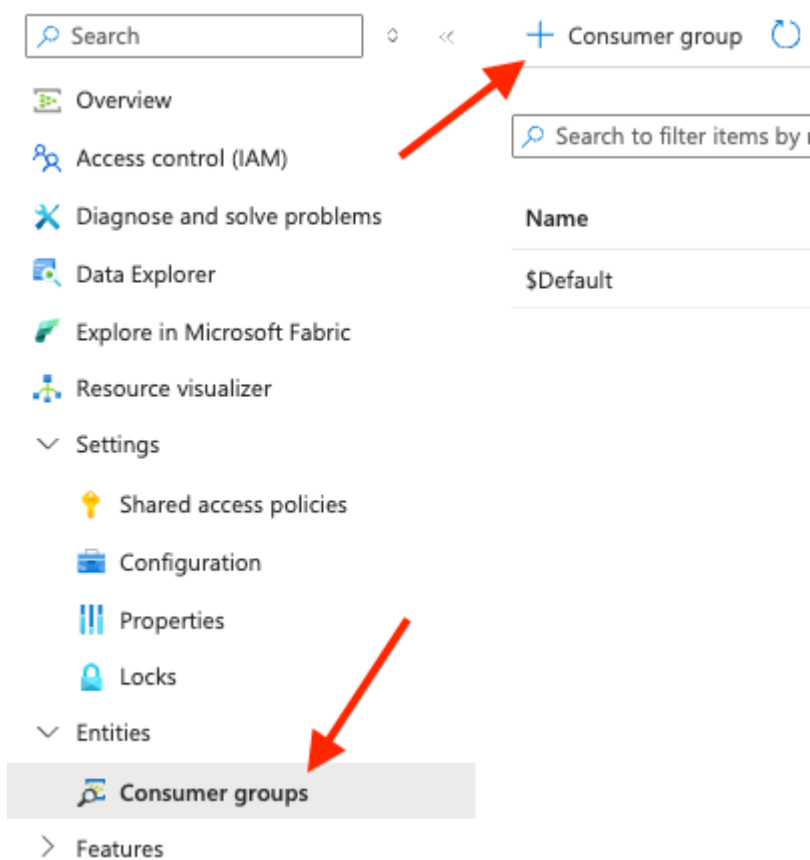
Step 8: Create an Event Hub Instance Consumer Group Within the Event Hub Namespace

1) Click the new **EH instance** configured in the previous step.



Access Event Hub Instance Configuration

2) From the EH instance, choose **Entities > Consumer groups**, and create a new **Consumer group**.



Create Consumer Group

3) Name the **consumer group** and click **Create**.

Create consumer group ×

Consumer groups

Name *

captive-auth-ad-eh-cg



Create

Assign Name To Consumer Group



Important: Copy and note the Event Hub instance Consumer group name.

Step 9: Verify Collected Values

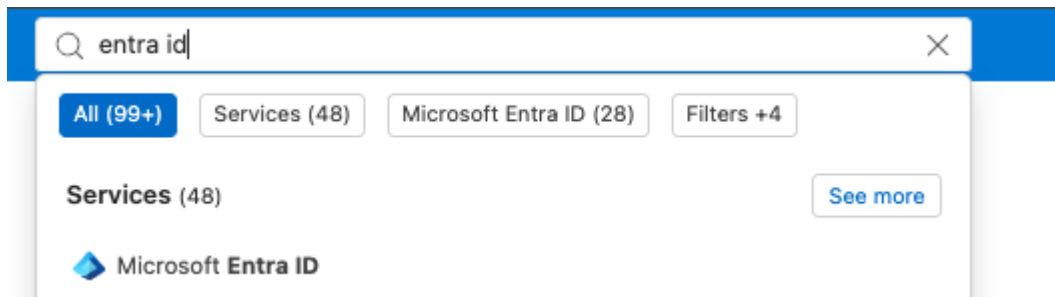
1) At this point, these values from the preceding steps are to be noted. If any value was not recorded, reference the applicable step where it is collected:

- Phase 3 Step 2 - App Registration (of the Enterprise App created for this process, referenced by the collected *Display Name*)
 - Step 2, Sub-Step 2
 - Display Name
 - Application (client) ID
 - Directory (tenant) ID
 - Step 2, Sub-Step 6
 - Client Secret
- Phase 3 Step 6 - Event Hub
 - Step 6, Sub-Step 1
 - EH Namespace
 - Primary Connection String
 - Step 7, Sub-Step 3
 - EH instance (Event Hub) name
 - Step 8, Sub-Step 3

- EH Consumer Group name

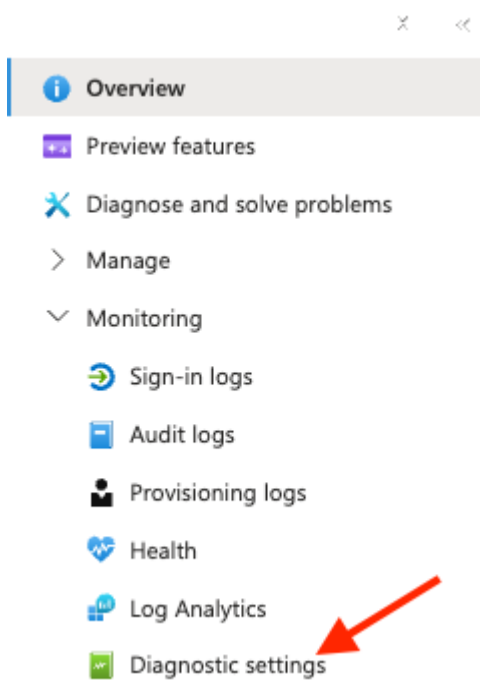
Step 10: Configure Entra ID Audit Log Streaming to the Event Hub

1) Navigate back to the **Entra ID tenant** configuration.



Search And Navigate To Entra ID Tenant Configuration

2) From the left menu, choose **Monitoring > Diagnostic Settings**.



Diagnostic Settings Monitoring

3) Choose **Diagnostic settings > General** and click + **Add diagnostic setting**.

Diagnostic settings

General

Custom security attributes

Refresh

Feedback

Diagnostic settings are used to configure streaming export of platform logs

Diagnostic settings

Name	Storage account
	-
	-
	-

+ Add diagnostic setting

Add New Diagnostic Setting

4) Assign the required **name** to the diagnostic setting, check the **AuditLogs** check box to log, and check the **Stream to an event hub** check box. Reference the values noted from the previous configurations, and click **Save** when complete.

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

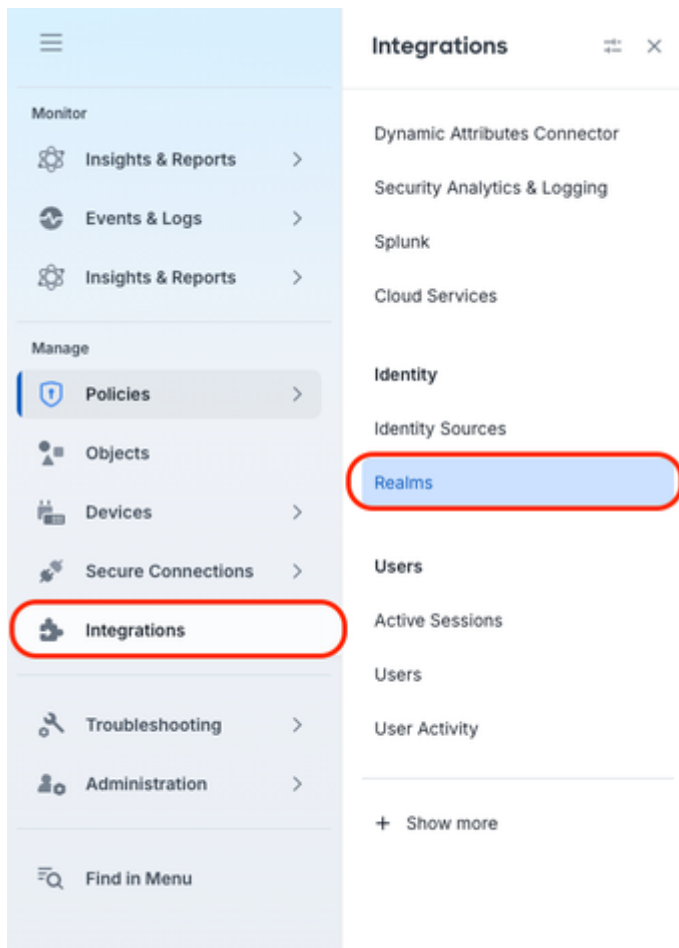
☐ Send to partner solution

Stream Audit Logs To Event Hub

Phase 4: Consolidate Azure and FMC/FTD Active Authentication Configuration

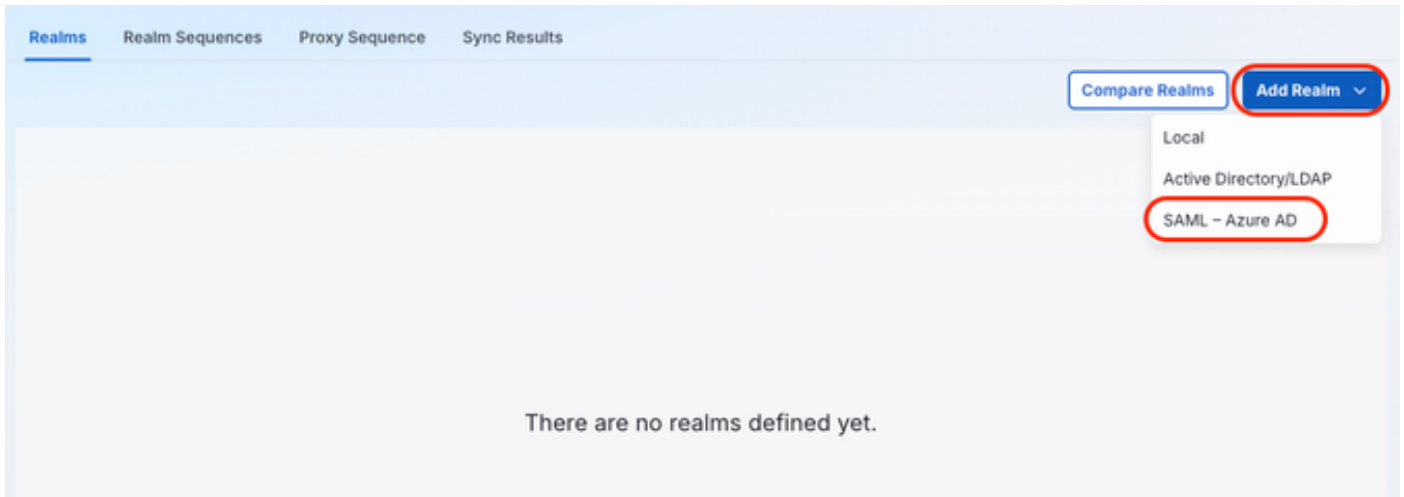
Step 1: Configure the Azure SAML/Entra ID Realm Using the FMC Wizard

1) Within the FMC, choose **Integrations > Identity > Realms**.



Identity Realms Configuration

2) Click **Add Realm** drop-down list, and choose **SAML - Azure AD**.



Add SAML Azure AD Realm

3) Assign a **name** and **description** to the Azure realm to describe its use, and ensure that **Authenticate passively with Azure AD or using captive portal with Azure AD** is chosen from the **Configuration Type** drop-down list. Click **Next**.

Add SAML - Azure AD Realm

1 Realm Details

Name *
azure-entra-saml

Description
Active Authentication IdP

Identity Provider *
Azure AD

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

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

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.

Next

Configure Azure AD Realm Settings

4) Choose the previously configured FQDN object as the **Base URL**. Enter the **Entity ID** with the string format shown:

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

- When the SAML Entity ID suffix is configured (underlined in green in the configuration example next), ensure that the suffix is unique among other SSO implementations within the environment. This value must match the Azure SAML configuration as well. The **Base URL** remains the same throughout the configuration.
- The **Assertion Consumer Services (ACS) URL** is populated automatically and is immutable.
- Choose the **Service Provider (SP) Certificate** enrolled in the previous workflow steps in FMC under **Devices > Certificates**.
- After these values are entered, click **Download Service Provider Metadata** to ease the configuration process and confirm that the **expected values** are written to 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

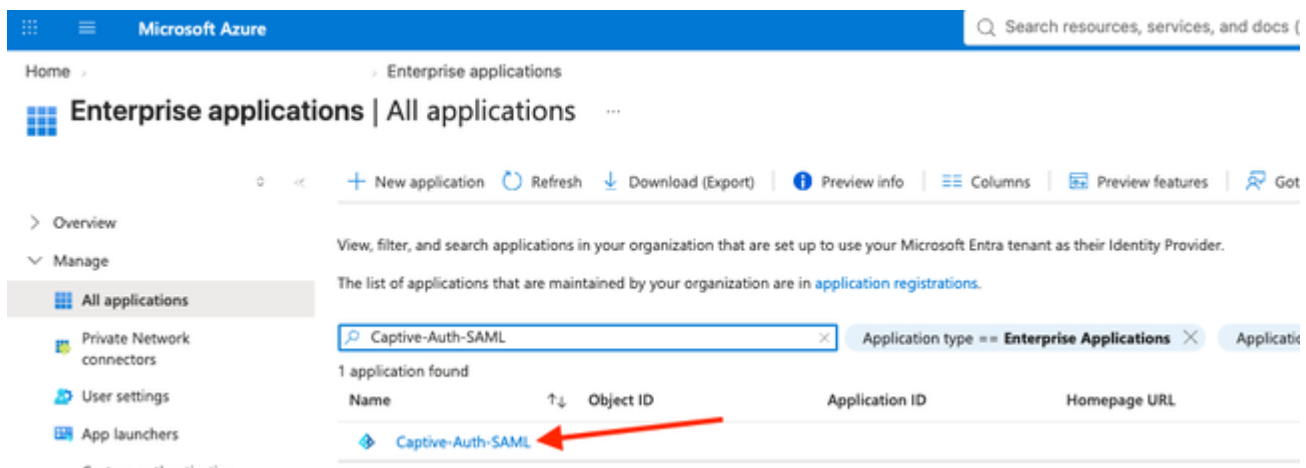
Next

Configure Base URL And Entity ID And Download SAML Metadata

5) Click **Next** to move to Sequence 3 of the Realm configuration.

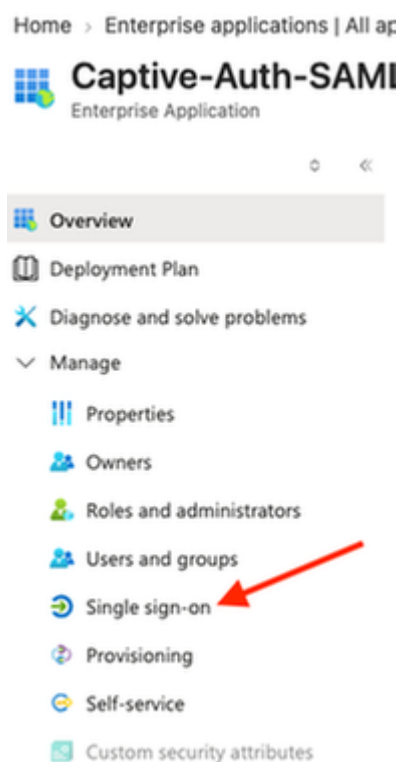
Step 2: Implement the FMC-Configured SAML SP Metadata in the Azure Enterprise Application

1) Navigate back to **Azure** and choose **Entra ID > Manage > Enterprise Applications**. Search for the previously created instance of the Microsoft Entra SAML Toolkit Enterprise Application.



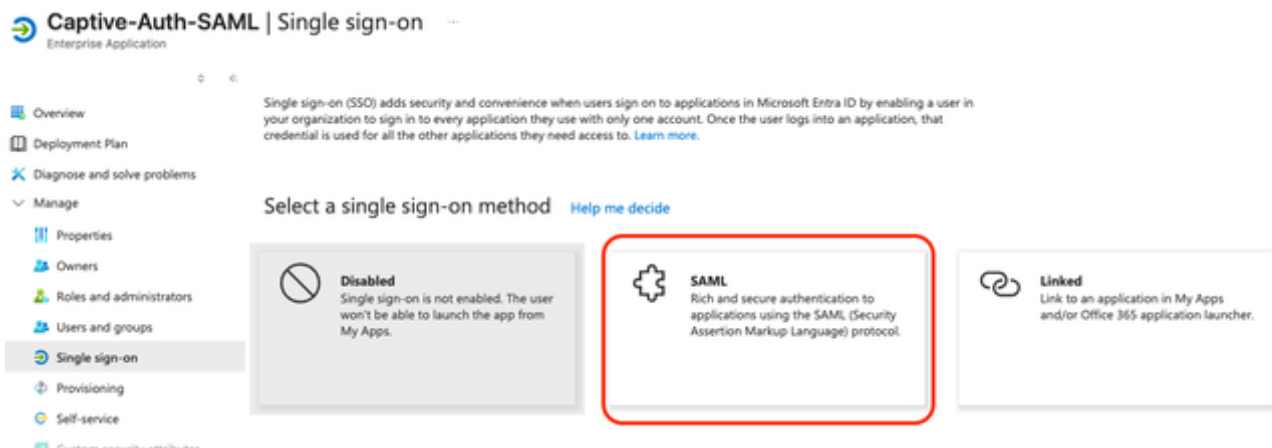
Locate Microsoft Entra SAML Toolkit Application

2) From the side navigation menu, choose **Manage > Single Sign-On**.



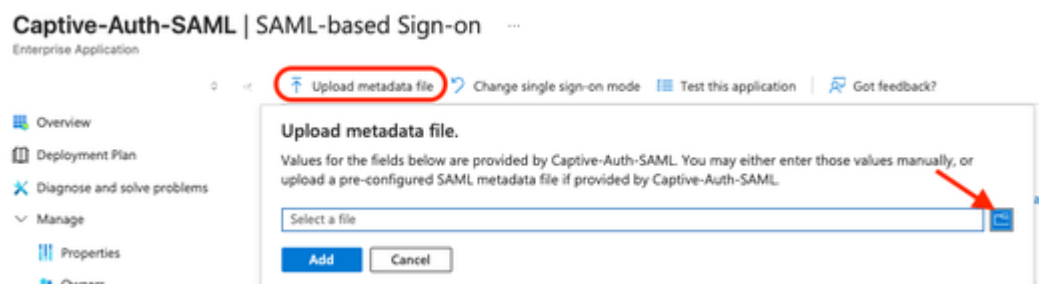
Manage Single Sign On Configuration

3) Click the **SAML** Single Sign-On (SSO) mode.



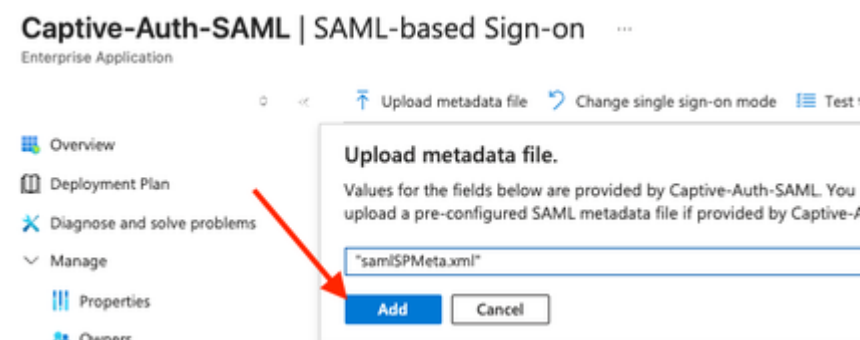
SAML Single Sign On Mode Selection

4) Click **Upload metadata file** and click the blue folder icon to browse your local filesystem for the **SAML metadata file** downloaded from the FMC.



Upload Metadata File From Firewall Management Center

5) Once the upload completes, click **Add**.



Add SAML Configuration Application

6) The side panel for Basic SAML Configuration appears, and values such as the **Identifier (Entity ID)** and the **ACS URL** are extracted from the FMC-originated SP metadata XML file uploaded and applied automatically. However, the **Sign on URL** is not populated and is required before saving.

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.



Basic SAML Configuration Extraction

7) Use the Sign-On URL pattern given, copy and paste the **value**, and click **Save** at the top when complete.

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.

✓

Sign On URL Configuration Entry

Scroll down to **SAML Certificates**, and export the Azure-generated **Federation Metadata XML** file for import into Cisco Secure FMC.

3 SAML Certificates

Token signing certificate		Edit
Status	Active	
Thumbprint		
Expiration		
Notification Email		
App Federation Metadata Url		Download
Certificate (Base64)		Download
Certificate (Raw)		Download
Federation Metadata XML		Download

Verification certificates (optional) [Edit](#)

Required	No
Active	0
Expired	0

Export Federation Metadata XML File

Step 3: Configure the Azure SAML/Entra ID Realm Using the FMC Wizard (Continued)

1) Navigate back to the FMC. Under Sequence 3, **SAML Identity Provider (IdP) Metadata**, upload the exported **Federation Metadata XML** file downloaded from Azure to the FMC to auto-populate the necessary values.

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.

[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.

Upload Federation Metadata XML File

2) Once uploaded, the values populate as shown.

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.



Auto Populated SAML Identity Provider Values



Note: Partial output is shown in the image.

3) Input the values collected throughout the implementation process up to this point:

- App Registration
 - Application (Client) ID
 - Client Secret
 - Directory (Tenant) ID
- Event Hub
 - EH Namespace Hostname
 - EH Namespace Primary Connection String
 - EH Instance (Event Hub) name
 - EH Consumer Group name

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

Enter Application And Event Hub Information

Once entered, click **Test** to check the connection and confirm that Azure is reachable with the information provided.



Note: If applicable, ensure the **Excluded/Included User Groups** align with your Entra configuration

4) The final step of the wizard allows you to configure **SAML Captive Portal Users** timeout. The default is 1440 minutes.

5 User Session Timeout

SAML Captive Portal Users

1440 Minutes Range 0-35791394

Configure Captive Portal Timeout

5) Click **Next** to continue.

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

Move Forward With Azure AD Realm Configuration

6) The wizard gives a summary of the configuration implemented. Click **Save** at the end of the summary after the entered values are validated and confirmed.

5 User Session Timeout Edit

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

Cancel Save

Realm Configuration Summary Save Button

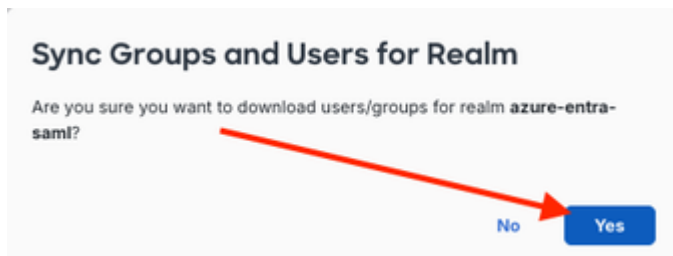
Step 4: Check Downloaded Users

1) Confirm that users can be **downloaded** from Azure Entra with the **Download Now** button within **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	Download Now

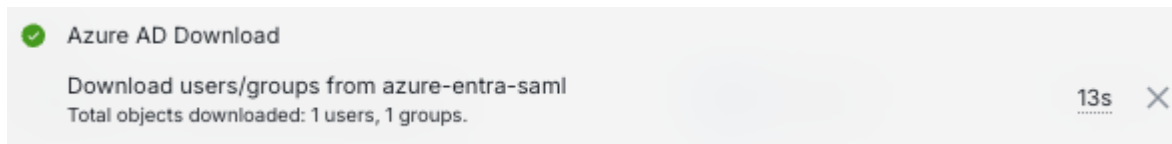
Download Users From Azure AD

2) Click **Yes** in response to the dialog prompt.



Confirm Download Of Users From Azure AD

3) The download task yields **1 user** and **1 group downloaded**, as confirmed under **Notifications > Tasks**.

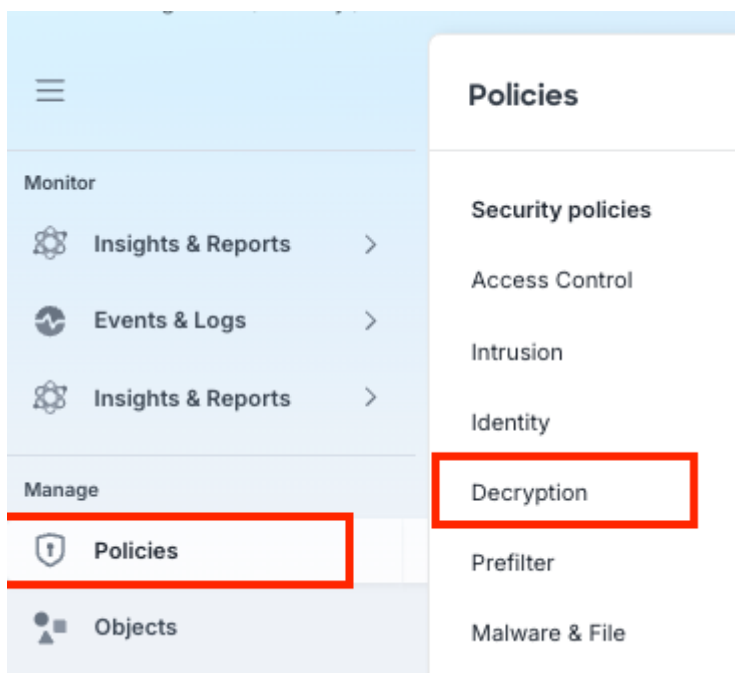


Notification Entry For Download Of Users From Azure AD

Phase 5: Configure Policies in the FMC

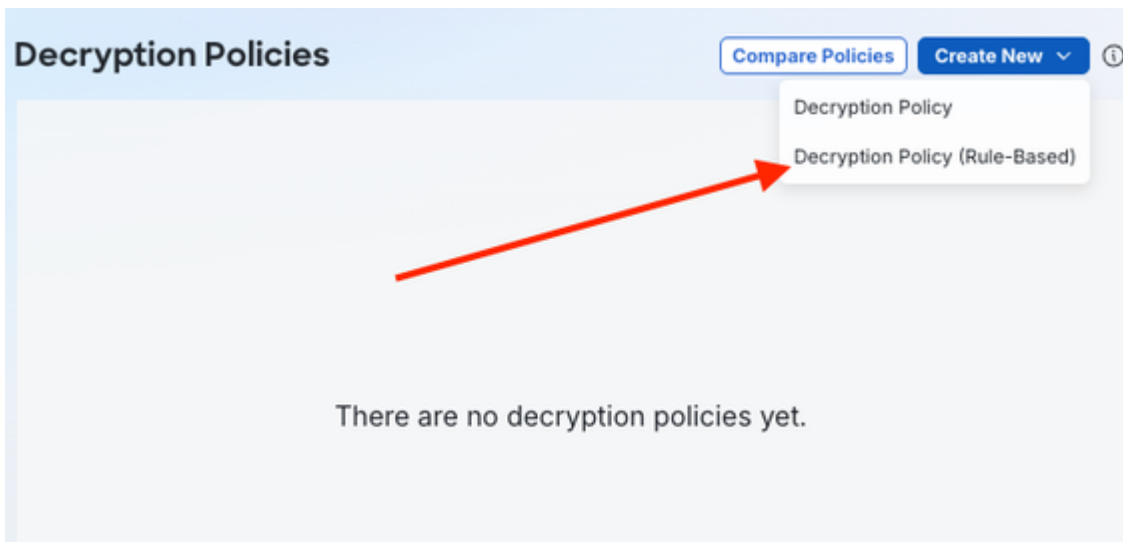
Step 1: Configure Decryption Policy

1) In the FMC, choose **Policies > Security Policies > Decryption**.



Navigate To Decryption Policy

2) Click the **Create New** drop-down list and choose **Decryption Policy (Rule-Based)**.



Create New Rule Based Decryption Policy

3) Assign a **name** and, if desired, a **description** to the new rule-based Decryption Policy, and click the **Outbound Connections (User Protection)** tab option to implement the **Decrypt-Resign** functionality required for captive portal authentication (Active Authentication).

Implement Outbound Connections Policy Details

4) Choose the **previously applied Internal CA** from its applicable drop-down list in the same dialog. Click **Next**.

5) Customize options as needed.

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](#)

Customize Decryption Policy Options

6) In this example, defaults are used with the exception of the required Policy Details. Complete the configuration wizard by clicking **Create Policy**.

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**

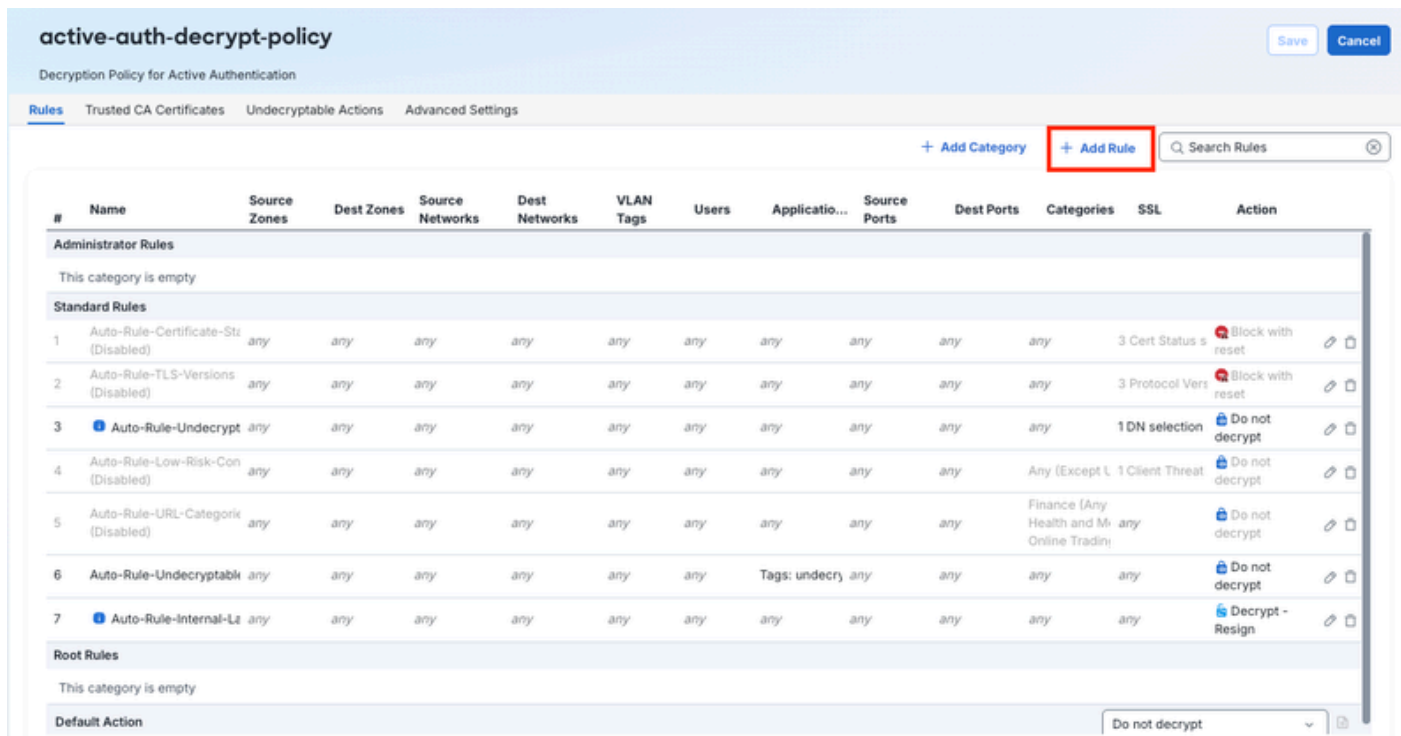
Cancel Skip Back Create Policy

Create Final Decryption Policy

Step 2: Configure Decryption Policy Rules

1) The default layout of a rule-based Decryption Policy is shown here. Traffic that does not match the default enabled rules, such as rule 3 (which references a pre-allocated list of undecryptable domain names) and rule 6 (which references applications tagged as undecryptable), is subject to the Decrypt - Resign action under Rule 7. These defaults, along with the Default Action, can be modified as needed. By default, traffic that matches no other rule is configured as Do Not Decrypt.

The **Azure Authentication Service** traffic must not be decrypted for inspection, so a dedicated rule is created for it. Click + **Add Rule** to begin.



Add Rule And Showing Default Rule Based Decryption Layout

2) Assign a **name** to the new Decryption Policy **rule entry**, choose **Do not decrypt** from the Action drop-down list, and place the rule at the top, less-specific rules. Source/Destination zones are also implemented to narrow the rule further.

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is set to 'Azure-Auth-Service-DND'. The 'Action' dropdown is set to 'Do not decrypt'. The 'Insert' dropdown is set to 'above rule'. The 'Source Zones' field is set to 'Inside_Zone' and the 'Destination Zones' field is set to 'Outside_Zone'. The 'Add Rule' button is highlighted.

Configure Do Not Decrypt Rule

3) Before the rule is added, click the **Applications** tab, search for and click the **Azure Authentication Service** application. Click **Add to Rule**, then click **Add**.

Add Rule

Name: ☒ Enabled Insert:

Action:

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 809

Available Applications (2)

Search:

All apps matching the filter

- Azure Arc
- Azure Authentication Service**

Selected Applications and Filters (0)

Add Azure Authentication Service Application Rule

4) Click **Save**.

active-auth-decrypt-policy

Decryption Policy for Active Authentication

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

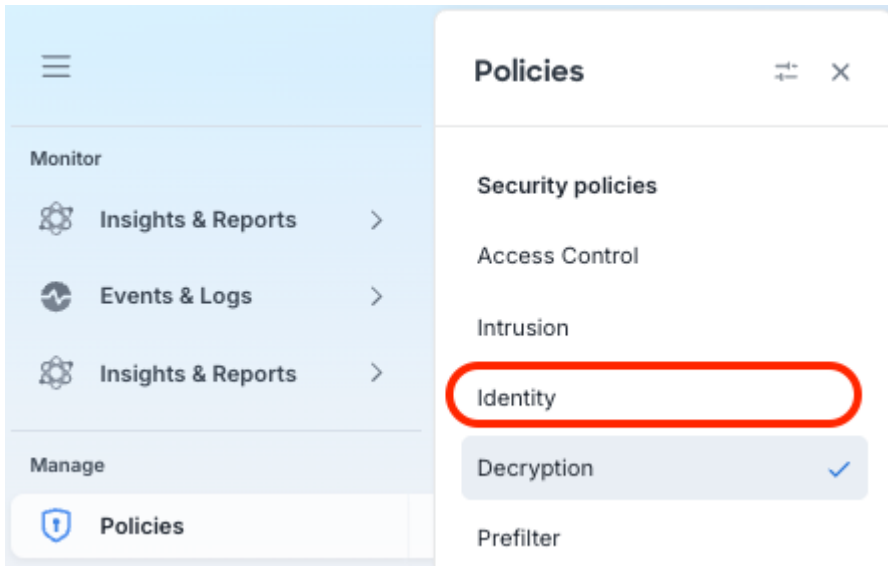
You have unsaved changes

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Application...	Source Ports	Dest Ports	Categories	SSL	Action
Standard Rules													
1	Auto-Rule-Certificate-St (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Cert Status s	Block with reset
2	Auto-Rule-TLS-Versions (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Protocol 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

Save Decryption Policy

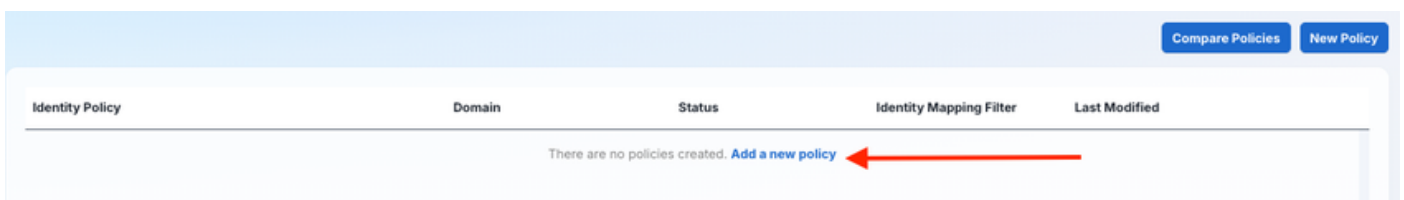
Step 3: Create Identity Policy

1) Choose **Policies > Security Policies > Identity** to create an **Identity Policy**.



Create Identity Policy

2) Create a new Identity Policy and click **Add a new policy**.



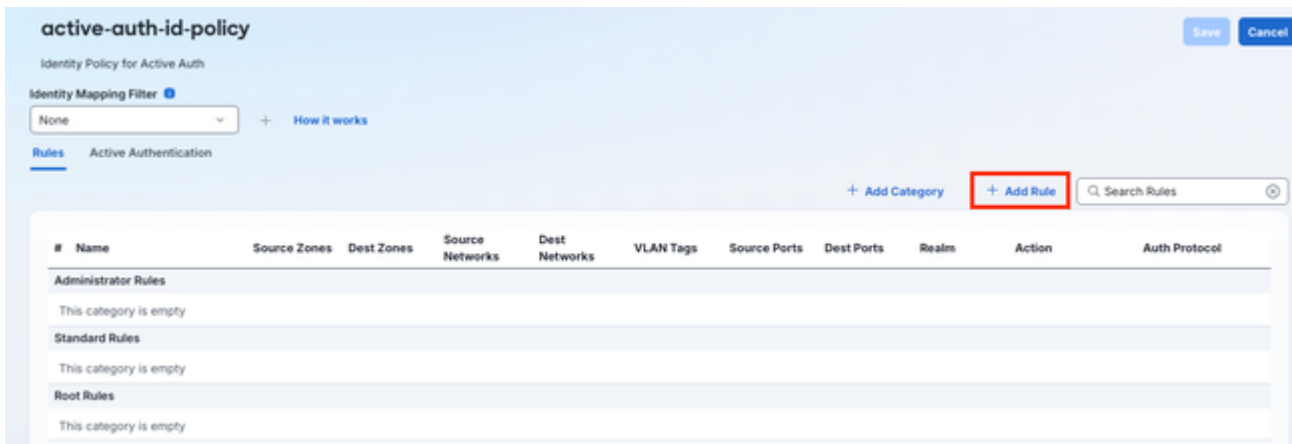
Add New Identity Policy Configuration

3) Assign a **name** and, if applicable, a **description** to the new Identity Policy. Click **Save**.

Name New Identity Policy

Step 4: Configure Identity Policy Rules

1) Add a new rule by clicking + **Add Rule**.



Add New Identity Policy Rule

2) Name the **new rule**, choose **Active Authentication** from the **Action** drop-down list, and narrow the **specific zones/networks** that must match the rule to perform Active Authentication.

The screenshot shows the 'Add Rule' configuration form. The 'Name' field is 'Active Auth ID Rule' (highlighted with a red box). The 'Enabled' checkbox is checked. The 'Insert' dropdown is set to 'into Category' and 'Standard Rules'. The 'Action' dropdown is set to 'Active Authentication' (indicated by a red arrow). Below the action dropdown, the 'Realm' is 'No realm', 'Authentication Protocol' is 'HTTP Basic', and 'Exclude HTTP User-Agents' is 'None'. A tab bar at the bottom shows 'Zones' (selected), 'Networks', 'VLAN Tags', and 'Ports'. On the left, under 'Available Zones', there is a search bar and a list with 'Inside_Zone', 'Outside_Zone' (highlighted), and 'DMZ_Zone'. In the center, 'Source Zones (1)' contains 'Inside_Zone' (highlighted with a red box). On the right, 'Destination Zones (1)' contains 'Outside_Zone' (highlighted with a red box). Buttons for 'Add to Source' and 'Add to Destination' are present. At the bottom right are 'Cancel' and 'Add' buttons.

Configure Active Authentication Rule Settings

3) Before clicking **Add**, click the **Realm and Settings** tab within the Rule Editor. Confirm that the realm configured in the previous steps is chosen as the **Authentication Realm**, then click **Add**.

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

Configure Realm And Settings For Identity Rule

4) The rule is added and configured. 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](#)

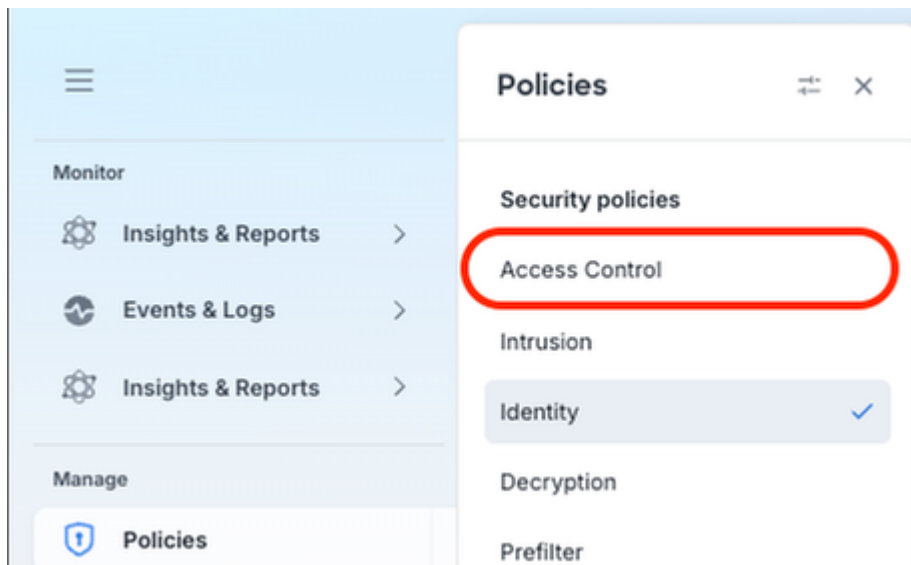
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	Active Auth ID Rule	Inside_Zone (Ro	Outside_Zone (F	any	any	any	any	any	azure-entra-san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

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

Save Identity Policy Rule Configuration

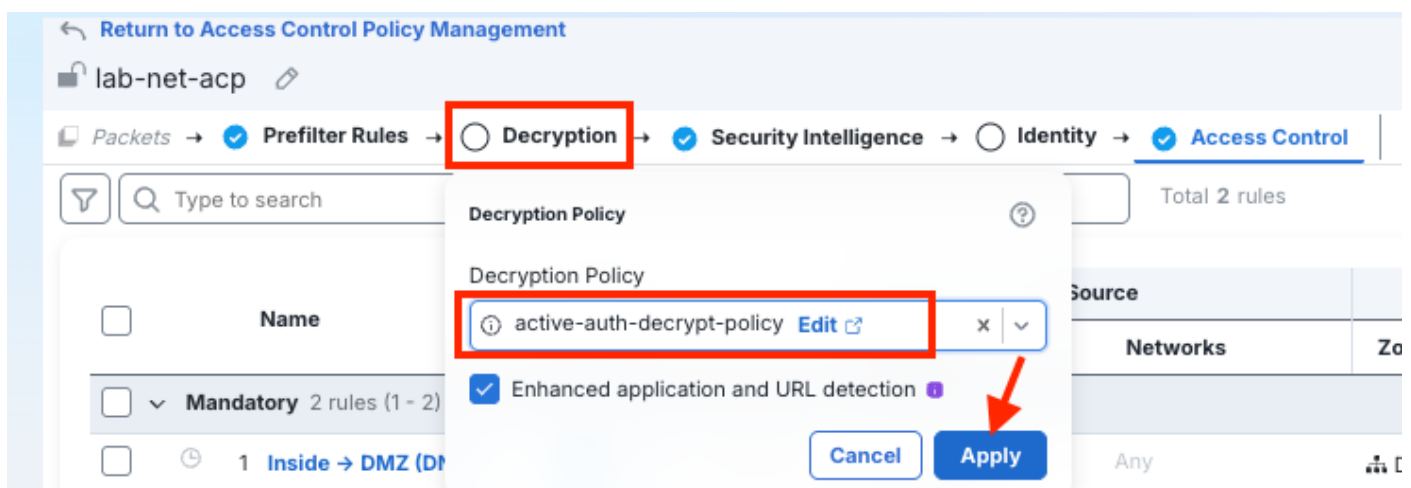
Step 5: Configure the Access Control Policy

1) Choose **Policies > Security Policies > Access Control**, and click the **Access Control Policy** to which the FTD is assigned.



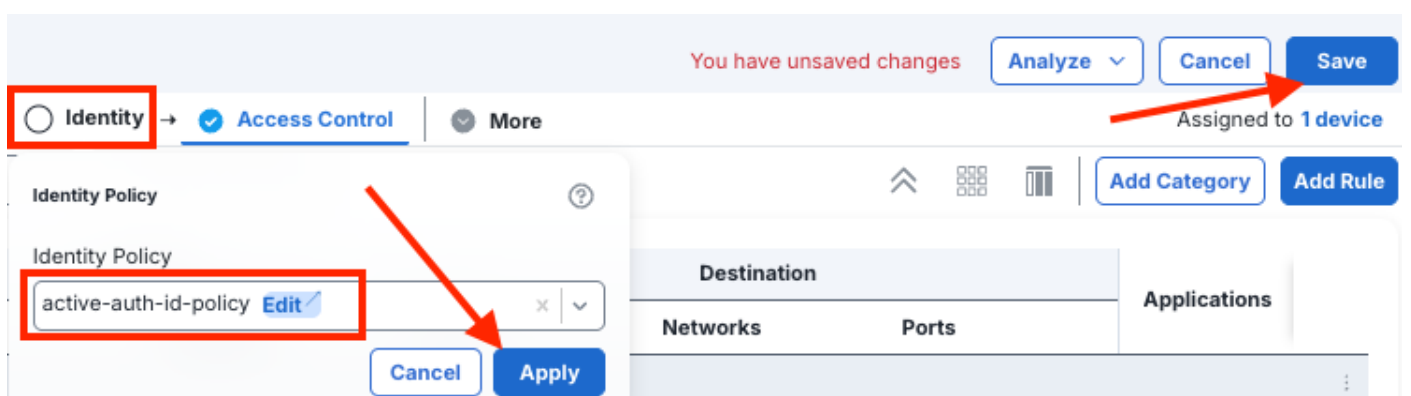
Access Control Policy Configuration

2) Confirm that the **Decryption Policy** configured in the previous steps is applied to the Access Control Policy.



Apply Decryption Policy To Access Control

3) Confirm that the **Identity Policy** configured in the previous steps is also applied to the Access Control Policy. **Save** the policy changes.



4) Confirm that rules **exist** that allow client data plane traffic through the Secure Firewall after successful Active Authentication. The example shown here uses a wider rule set given the lab environment.

☐	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)								

User Data Plane Traffic Rule Set

Step 6: Deploy Configurations to the Cisco Secure Firewall Devices

Once deployed, clients that send traffic are prompted with a Microsoft Sign-in webpage to perform Active Authentication with Azure Entra.

For additional context on the process documented here, see [Create a Microsoft Azure AD \(SAML\) realm for active authentication \(captive portal\) - Chapter: Realms in FMC Device Config Guide 10.x.](#)

Verify

Use this section to help confirm that the configuration works properly.

GUI

Validate user sessions and activity in the FMC:

- Choose **Integrations > Users > Active Sessions**.

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

FMC Active Sessions Output

- Choose **Integrations > Users > User Activity**.

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

FMC User Activity Output

On Azure, navigate to the **Microsoft Entra Admin Center**:

- Filter **Enterprise Apps**, search for/click the **applicable app**.

Microsoft Entra admin center

Home > Enterprise applications

Enterprise applications | All applications

Overview

- Overview
- Diagnose and solve problems

Manage

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

Security

- Conditional Access
- Consent and permissions
- Application policies

Search resources, services

Search: captive-

Name	Obj
Captive-Auth...	efda

Azure Entra Admin Center Enterprise Apps Navigation

- Choose **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

Azure Enterprise Application Sign In Activity Logs

CLI

- In the FTD CLI, you can see statistics related to SAML and captive portal responses:

```
<#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

Captive Portal Debug

- The **system support captive-portal-debug** command can be used on the FTD. The output shows how to enable the debug and also notes key segments of the output to help understand Captive Portal flow.

```
<#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: htt
```

```
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
...

```

User Identity Dump

- To take a snapshot of the current user identity state data on the FTD, run the **system support firewall-engine-dump-user-identity-data** command on the FTD CLI:

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

Successfully commanded snort.

```
>
```

- In **expert** mode CLI, while logging in with local admin credentials of the FTD device, view the contents of the dumped file 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:

...

Possible Issues

Captive Portal Unknown Certificate Authority

Issue: The client browser returns an unknown issuer error when authentication is attempted.

Likely Cause: The internal Certificate Authority is untrusted within the client browser.

Resolution: Confirm that the CA is trusted within the browser. The example shown here confirms that the

internal CA certificate is trusted.

Captive Portal "Server Not Found"

Issue: When the client browser attempts to load the captive portal, it returns "Server Not Found" for the base URL while attempting to reach base URL or similar.

Likely Cause: DNS reachability or DNS misconfiguration.

Resolution: Confirm that the client has the appropriate DNS server configured to resolve the A record. Confirm that the server has an A record mapped to the FQDN and that it is reachable and responsive.

Related Information

- [Create a Microsoft Azure AD \(SAML\) realm for active authentication \(captive portal\) - FMC Device Config Guide 10.x](#)
- [Azure Event Hub Documentation](#)
- [Technical Support & Documentation - Cisco Systems](#)