

Azure Entra Captive-Portal auf sicherer Firewall konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Diagramm](#)

[Captive Portal zwischen Endgerät, FTD und Azure Entra](#)

[Konfigurieren](#)

[Phase 1: Erstkonfiguration von FMC und DNS](#)

[Schritt 1: Aktivieren des Cisco Dynamic Attributes Connectors \(CSDAC\)](#)

[Phase 2: Vollqualifizierter Domänenname des Netzwerkobjektvertreters der FTD-Eingangsschnittstelle erstellen](#)

[Schritt 3: Konfigurieren des DNS-A-Datensatzes](#)

[Phase 2: Konfiguration der Public Key-Infrastruktur](#)

[Schritt 1: Importieren des internen Zertifizierungsstellenzertifikats in das FMC](#)

[Phase 2: Signieren des Dienstanbieterzertifikats mit der Zertifizierungsstelle](#)

[Schritt 3: Bereitstellung des SP-Zertifikats für das FTD](#)

[Phase 3: Azure-Konfiguration](#)

[Schritt 1: Erstellen der Enterprise-Anwendung für das SAML-Toolkit](#)

[Phase 2: App-Registrierungen für Entra-ID konfigurieren](#)

[Schritt 3: Konfigurieren von Microsoft Graph API-Berechtigungen für die App-Registrierung](#)

[Schritt 4: Konfigurieren des EH-Namespaces \(Event Hub\)](#)

[Schritt 5: Auswählen oder Erstellen von Richtlinien für gemeinsamen Zugriff im Event Hub-Namespace](#)

[Schritt 6: Sammeln und Notieren von SAS-Informationen \(Shared Access Signature\) aus dem EH-Namespace](#)

[Schritt 7: Erstellen einer Event Hub-Instanz im Event Hub-Namespace](#)

[Schritt 8: Erstellen einer Ereignishub-Instanzverbrauchergruppe im Ereignishub-Namespace](#)

[Schritt 9: Erfasste Werte überprüfen](#)

[Phase 10: Konfigurieren des Streaming des Prüfprotokolls für die Entra-ID für den Event Hub](#)

[Phase 4: Azure und FMC/FTD Active Authentication-Konfiguration konsolidieren](#)

[Schritt 1: Konfigurieren des Azure SAML/Entra ID-Bereichs mithilfe des FMC-Assistenten](#)

[Phase 2: Implementieren der FMC-konfigurierten SAML SP-Metadaten in der Azure Enterprise-Anwendung](#)

[Schritt 3: Konfigurieren des Azure SAML-/Entra-ID-Bereichs mithilfe des FMC-Assistenten \(Fortsetzung\)](#)

[Schritt 4: Heruntergeladene Benutzer überprüfen](#)

[Phase 5: Konfigurieren von Richtlinien im FMC](#)

[Schritt 1: Entschlüsselungsrichtlinie konfigurieren](#)

[Phase 2: Entschlüsselungsrichtlinienregeln konfigurieren](#)

[Schritt 3: Identitätsrichtlinie erstellen](#)

[Schritt 4: Identitätsrichtlinien-Regeln konfigurieren](#)

[Schritt 5: Konfigurieren der Zugriffskontrollrichtlinie](#)

[Überprüfung](#)

[GUI](#)

[CLI](#)

[Fehlerbehebung](#)

[Captive Portal-Debugging](#)

[Benutzeridentitäts-Dump](#)

[Mögliche Probleme](#)

[Captive Portal Unbekannte Zertifizierungsstelle](#)

[Captive Portal "Server nicht gefunden"](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration der Microsoft Azure Entra-ID für die Verwendung mit dem Captive Portal (aktive Authentifizierung) in der Cisco Secure Firewall beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

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

Für die Erstellung des Event Hub muss in Azure die Standard-Preisebene verfügbar sein. Darüber hinaus müssen Geräte mit aktivierter Smart Licensing-Funktion und einer exportgesteuerten Funktion aktiviert werden.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure FTD Version 10.0
- Cisco Secure FMC Version 10.0

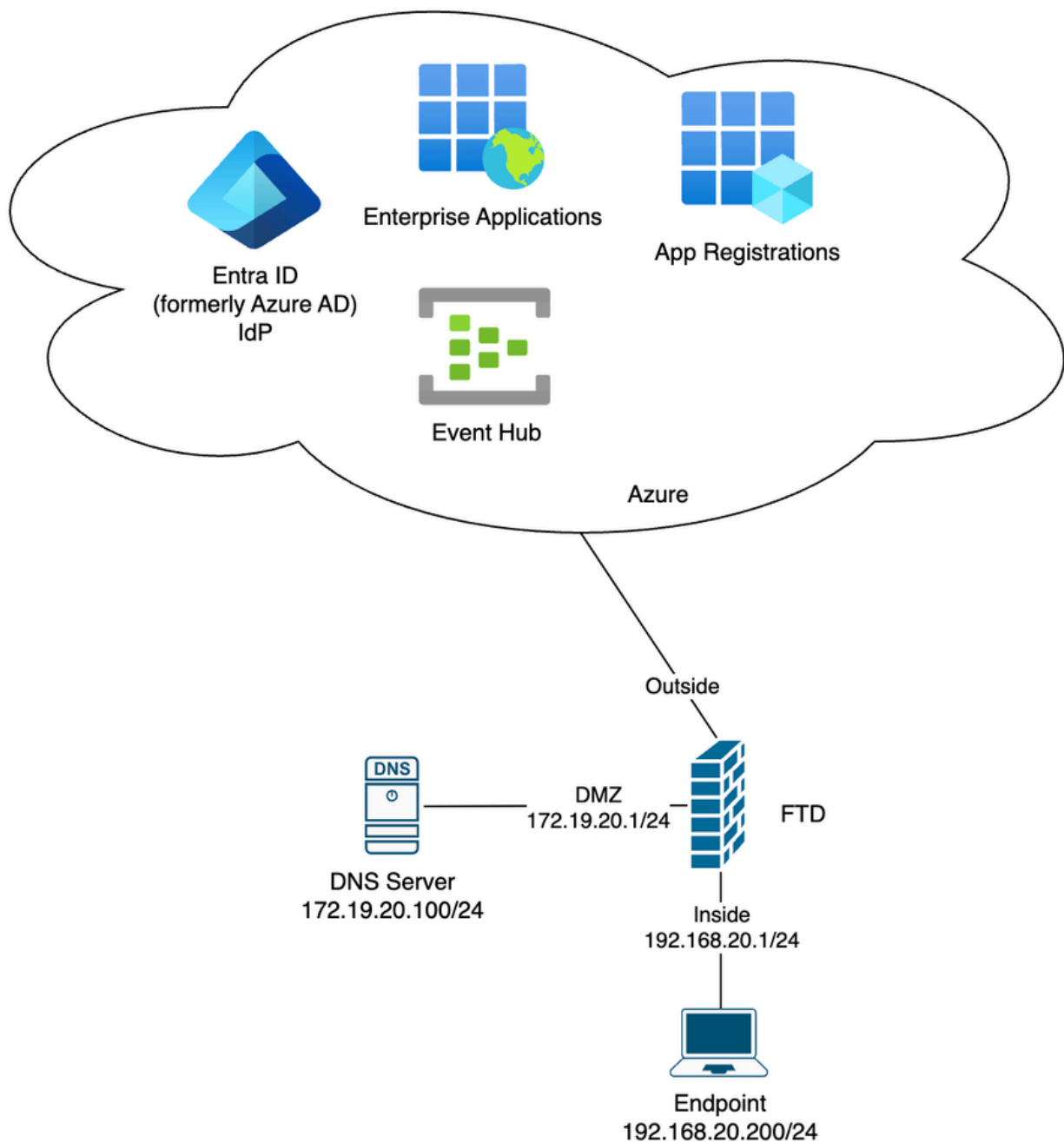
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Da herkömmliche IP-basierte Sicherheitsarchitekturen Schwierigkeiten haben, mit dynamischen, hybriden Arbeitsumgebungen Schritt zu halten, bietet Cisco Secure Firewall Active Authentication mit SAML-Integration eine robuste, identitätsbasierte Lösung. Durch die Nutzung von Microsoft Entra ID (Azure AD) als zentralisierter Identitätsanbieter ermöglicht diese Konfiguration Administratoren, über statische Netzwerkregeln hinauszugehen und eine granulare Zugriffskontrolle auf der Grundlage einer verifizierten Benutzeridentität anstelle von flüchtigen Netzwerkadressen durchzusetzen. Diese Integration optimiert die Benutzerumgebung durch die nahtlose einmalige Anmeldung (Single Sign-On, SSO) und die obligatorische Multi-Factor-Authentifizierung (MFA). Gleichzeitig wird ein einheitlicher Sicherheitsstatus sichergestellt, der in einem Netzwerk ohne Perimeter für strenge Transparenz und Richtliniendurchsetzung sorgt.

Diagramm

Captive Portal zwischen Endgerät, FTD und Azure Entra



Captive Portal zwischen EndPoint und Azure Entra

Konfigurieren

Phase 1: Erstkonfiguration von FMC und DNS

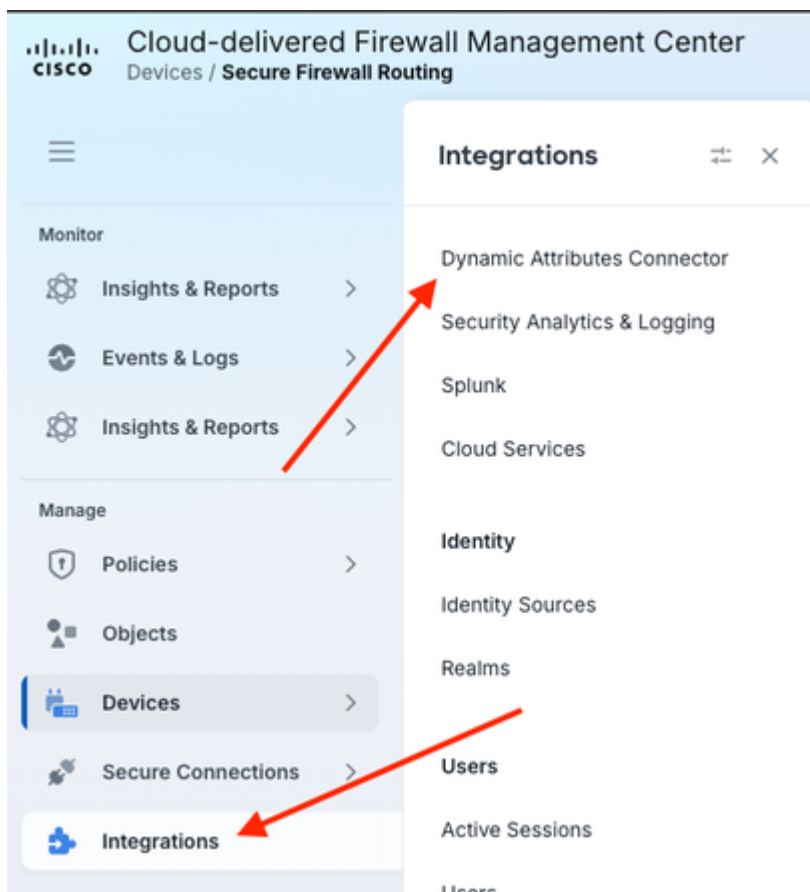


Anmerkung: Bei dieser Übung wird ein über die Cloud bereitgestelltes Firewall Management Center (cdFMC) verwendet. Bei standortbasiertem FÜZ bleiben die Schritte

jedoch unverändert.

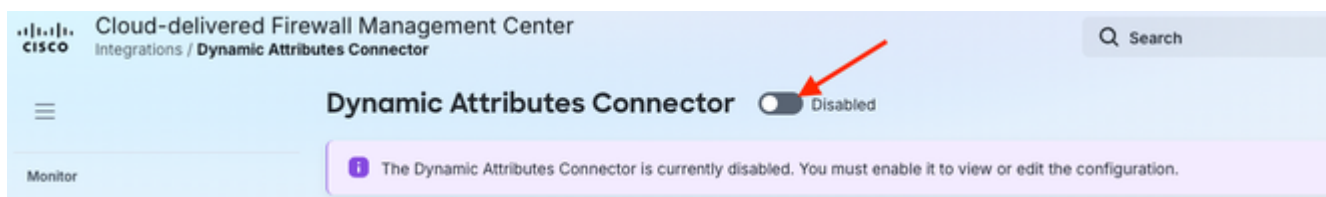
Schritt 1: Aktivieren des Cisco Dynamic Attributes Connectors (CSDAC)

1) Wählen Sie Integrationen > Dynamic Attributes Connector.



Integrationen auswählen Dynamic Attributes Connector

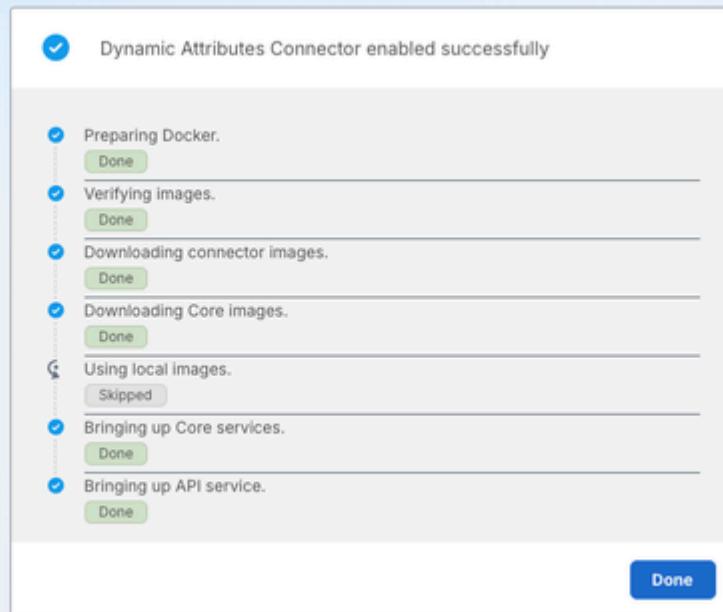
2) Klicken Sie auf das Steuerelement neben der Zeichenfolge Disabled (Deaktiviert), um CSDAC zu aktivieren.



Cisco Dynamic Attributes Connector aktivieren

c) Klicken Sie auf Fertig, sobald die CSDAC-Aktivierung abgeschlossen ist.

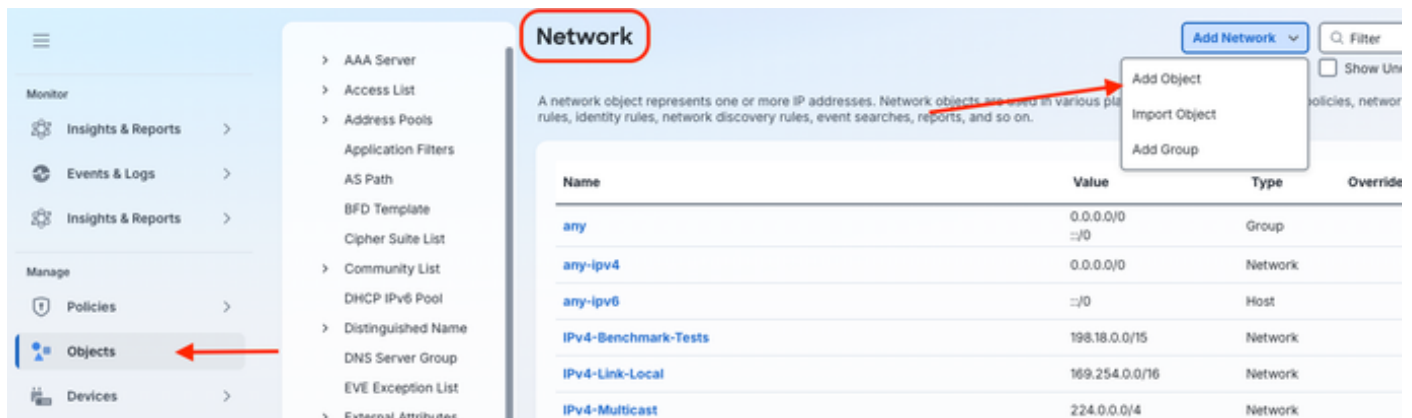
Dynamic Attributes Connector



Cisco Dynamic Attributes Connector-Status aktivieren

Phase 2: Vollqualifizierter Domänenname des Netzwerkobjektvertreters der FTD-Eingangsschnittstelle erstellen

1) Wählen Sie Objekte > Netzwerk hinzufügen > Objekt hinzufügen.



Neues vollständig qualifiziertes Domännennamennetzwerkobjekt erstellen

2) Nennen Sie das Netzwerkobjekt, das mit dem vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) konfiguriert wurde. Geben Sie den FQDN ein, und weisen Sie das Netzwerkobjekt als FQDN-Typ zu, indem Sie auf das entsprechende Optionsfeld klicken. Klicken Sie auf Speichern.

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

Konfigurieren von FQDN-Netzwerkobjektvariablen

Schritt 3: Konfigurieren des DNS-A-Datensatzes

1) Im hier gezeigten Beispiel wird Windows Server 2025 verwendet. bei Bedarf in der Dokumentation des jeweiligen Namensauflösungsservers nachsehen.

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



Anmerkung: Der Client, der die Active Authentication ausführt, muss in der Lage sein, diesen DNS-A-Eintrag aufzulösen.

Phase 2: Konfiguration der Public Key-Infrastruktur

Eine interne Zertifizierungsstelle (Certificate Authority, CA) kann als Public Key Infrastructure (PKI) für die Konfiguration der aktiven Authentifizierung verwendet werden. Cisco FMC und FTD erfordern, dass der interne öffentliche Schlüssel der CA und der gepaarte private Schlüssel als internes CA-Objekt hochgeladen werden, um die erforderlichen Vorgänge zum Abfangen und Entschlüsseln von SSL auszuführen. Darüber hinaus muss die interne CA innerhalb des Clientbrowsers, von dem aus die aktive Authentifizierung ausgeführt wird, vertrauenswürdig sein. In der Dokumentation des Client-Browsers finden Sie Informationen dazu, wie Sie überprüfen, ob der Browser dem Zertifikat vertraut.

Schritt 1: Importieren des internen Zertifizierungsstellenzertifikats in das FMC

1) Wählen Sie Objects > PKI > Internal CAs (Objekte > PKI > Interne Zertifizierungsstellen). Klicken Sie auf CA importieren.



Anmerkung: Die interne CA kann auch direkt auf dem FMC erstellt werden.

Import Internal Certificate Authority ⓘ

Name:
Internal-Lab-Network-CA

Certificate Data or, choose a file: [Browse..](#)

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

Key or, choose a file: [Browse..](#)

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

☒ Encrypted, and the password is:

[Cancel](#) [Save](#)

Interne Zertifizierungsstelle in Firewall-Verwaltungscenter importieren



Anmerkung: Innerhalb des Inhalts dieses Dokuments wird ein Leerraum angezeigt, der die verschiedenen Feldwerte in den Bildern abdeckt und gemäß der Veröffentlichung dieses Dokuments beabsichtigt ist. Die tatsächlichen Werte werden während der Konfiguration für die Umgebung übernommen.

Phase 2: Signieren des Dienstanbieterzertifikats mit der Zertifizierungsstelle

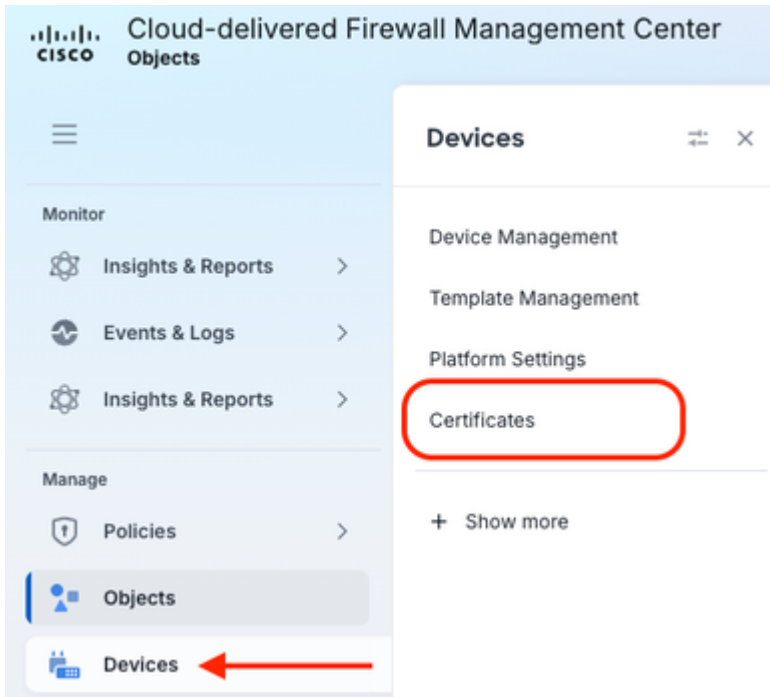
1) Das Service Provider-Zertifikat (SP-Zertifikat) muss von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) signiert und in einem PKCS#12-Format (.p12) zurückgegeben werden.



Anmerkung: Diese Zertifizierungsstelle kann intern signiert werden. Der einzige Vorbehalt besteht darin, dass die interne Zertifizierungsstelle vom Clientgerät als vertrauenswürdige eingestuft werden muss.

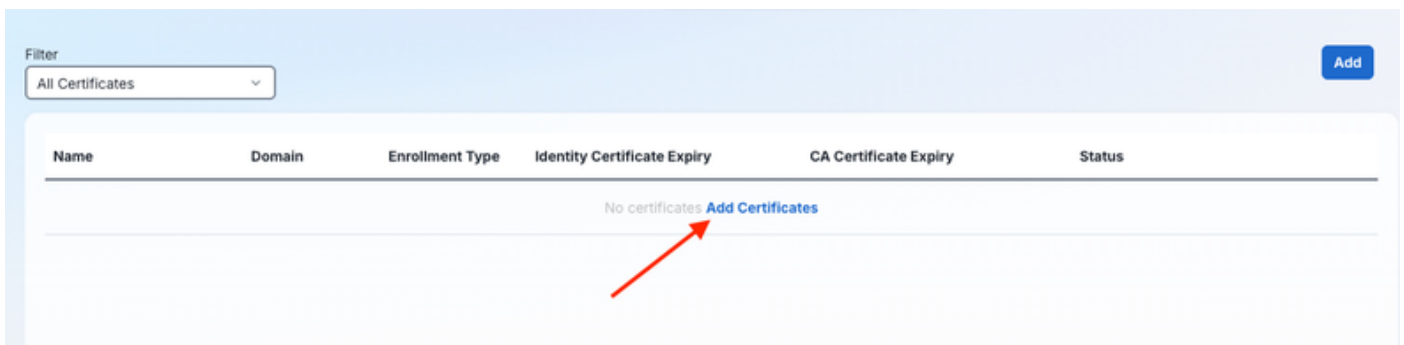
Schritt 3: Bereitstellung des SP-Zertifikats für das FTD

1) Wählen Sie Geräte > Zertifikate aus.



Navigieren zu Geräten und Zertifikaten

2) Klicken Sie auf Zertifikate hinzufügen.



Neues Gerätezertifikat hinzufügen

3) Klicken Sie auf das Gerät in der Dropdown-Liste, das die aktive Authentifizierung ausführt, und klicken Sie dann auf das + Symbol, um eine neue Zertifikatregistrierung zu erstellen.

Add New Certificate ?

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

Device*:

Certificate Enrollment*:

FTD auswählen und neue Zertifikatregistrierung hinzufügen

4) Nennen Sie die Zertifikatregistrierung, und wählen Sie in der Dropdown-Liste Registrierungstyp die Option PKCS12-Datei aus.

Add Certificate Enrollment ?

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

Enrollment URL:*

Challenge Password:

Confirm Password:

Retry Period: (Range 0-100)

Retry Count: (Range 0-100)

Fingerprint:

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

Einstellungen und Typ der Zertifikatregistrierung

5) Importieren Sie die PKCS#12-Datei, indem Sie auf PKCS12-Datei durchsuchen klicken und die erforderliche Passphrase eingeben. Klicken Sie auf Speichern.

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**

PKCS12-Datei durchsuchen und importieren

6) Bestätigen Sie, dass die Registrierungsdetails korrekt sind, und klicken Sie auf Hinzufügen.

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 +

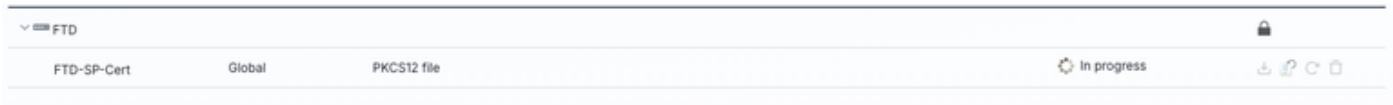
Certificate Enrollment Details:

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

Cancel **Add**

Zertifikatregistrierungsdetails bestätigen

7) Der Import spiegelt In Bearbeitung wider.



Wenn der Import abgeschlossen ist, können die SP-Zertifikatinformationen durch Klicken auf das ID-Symbol des konfigurierten Zertifikats validiert werden.

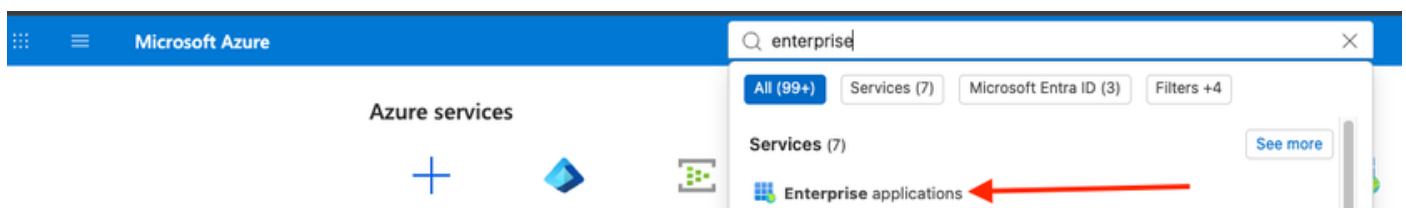


Status des Zertifikatimports wird ausgeführt

Phase 3: Azure-Konfiguration

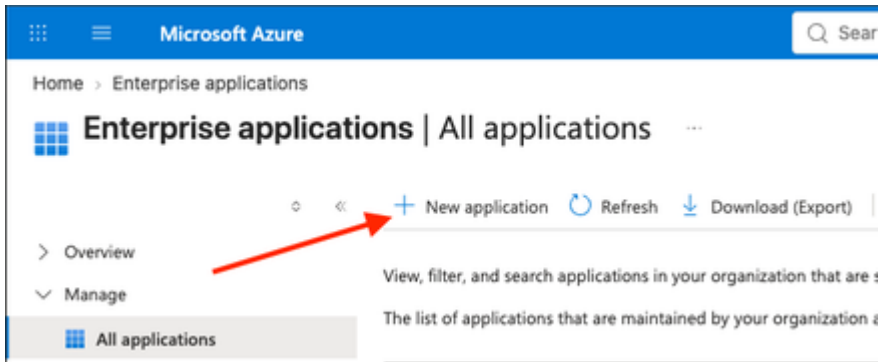
Schritt 1: Erstellen der Enterprise-Anwendung für das SAML-Toolkit

1) Suchen Sie nach Unternehmensanwendungen, und klicken Sie auf.



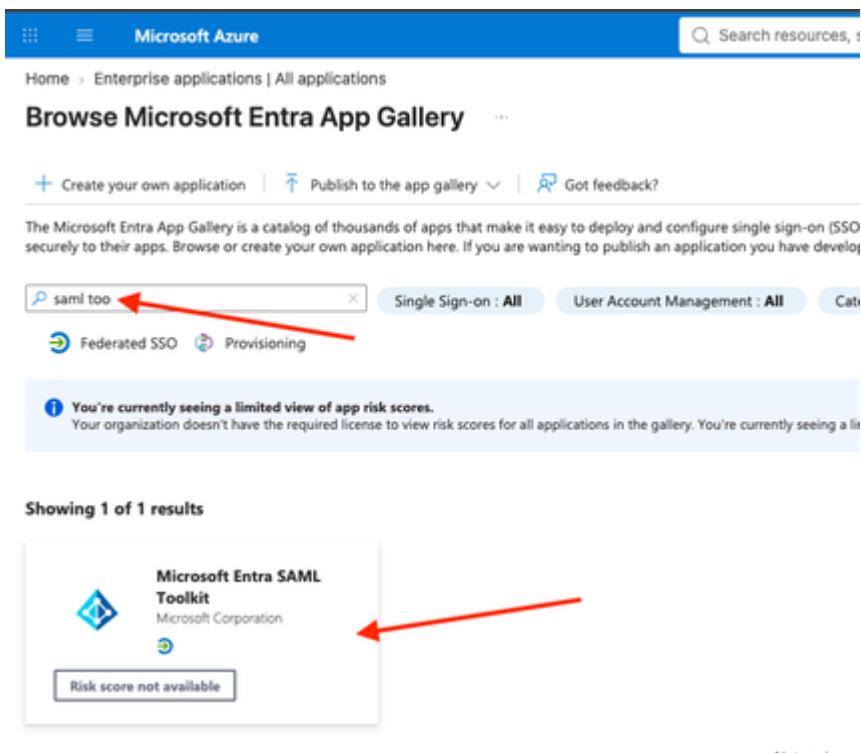
Suchen nach und Zugreifen auf Unternehmensanwendungen

2) Klicken Sie auf + Neue Anwendung.



Neue Anwendung in Unternehmensanwendungen auswählen

3) Suchen Sie nach dem Microsoft Entra SAML Toolkit und klicken Sie auf die Miniaturansicht dafür.



Suche und Auswahl des Microsoft Entra SAML-Toolkits

4) Weisen Sie der Microsoft Entra SAML Toolkit Enterprise Application einen Namen zu, und klicken Sie auf Erstellen. (Microsoft-Referenz: [Lesen Sie unser Schritt-für-Schritt-Tutorial zur Integration von Microsoft Entra SAML Toolkit](#)).

Microsoft Entra SAML Toolkit

Got feedback?

Logo

Name *

Publisher Microsoft Corporation

Provisioning Automatic provisioning is not supported

Single Sign-On Mode SAML-based Sign-on, Linked Sign-on

URL https://www.microsoft.com/

[Read our step-by-step Microsoft Entra SAML Toolkit integration tutorial](#)

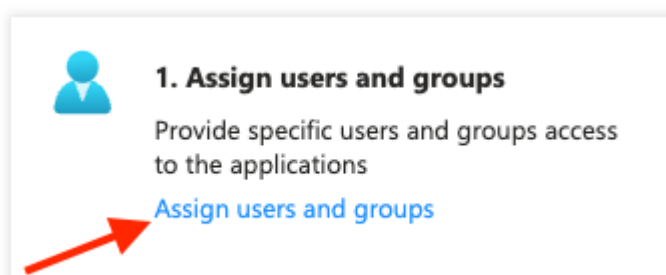
This is the sample SAML app which customers can use to test the SAML single sign-on integration with Microsoft Entra ID.

You're currently seeing a limited view of app risk scores.
Your organization doesn't have the required license to view risk scores for all applications in the gallery. You're currently seeing a limited view. To access full risk scoring upgrade to [Microsoft Entra Suite](#) or [Microsoft Entra Internet Access](#).

Create

Name der SAML-Toolkit-Anwendung zuweisen

5) Weisen Sie auf der Seite Overview (Übersicht) die spezifischen Benutzer und Gruppen der SAML Toolkit Enterprise Application (SAML-Toolkit-Enterprise-Anwendung) zu. In diesem Beispiel ist das Testkonto (captive-portal-user) ein Mitglied der Gruppe "active-auth-lab".

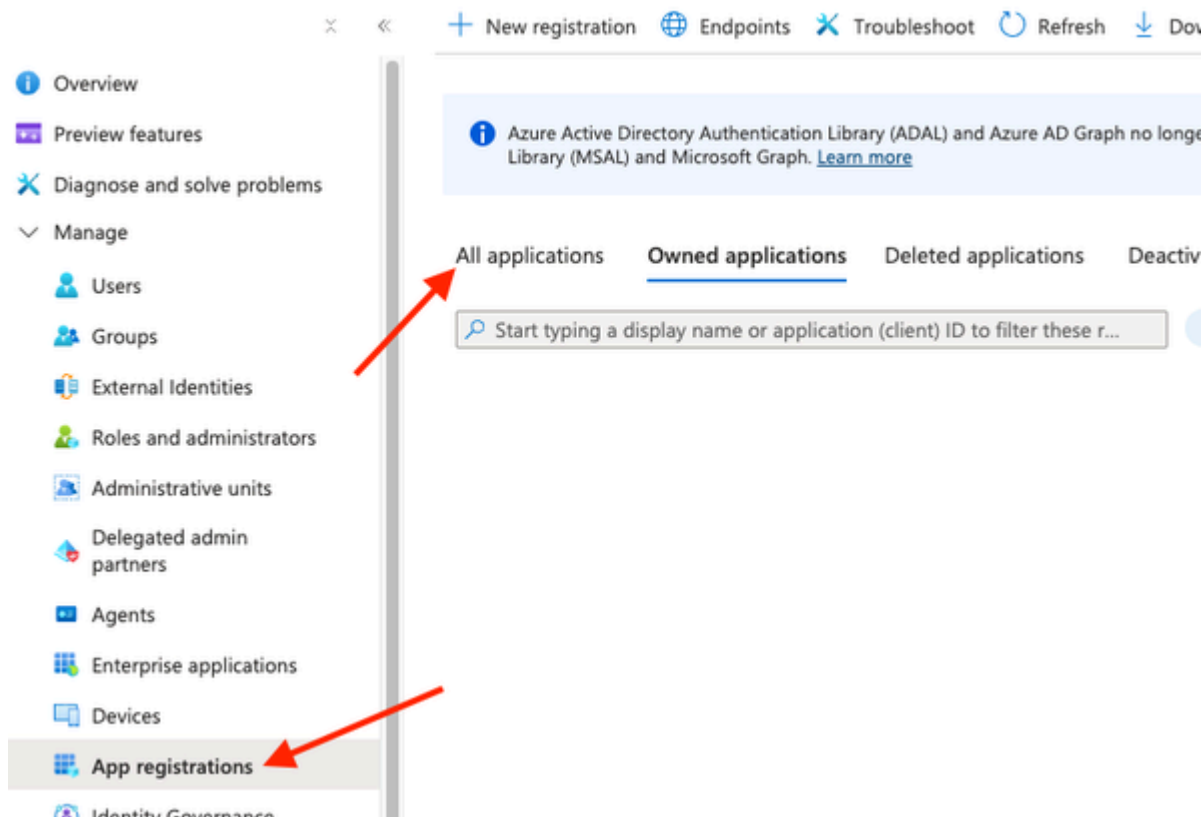


Zuweisen von Benutzern und Gruppen zu einer Anwendung

6) Die Konfiguration dieser Enterprise-Anwendung wird in späteren Schritten fortgesetzt.

Phase 2: App-Registrierungen für Entra-ID konfigurieren

1) Navigieren Sie zurück zu Entra ID, und wählen Sie im linken Navigationsmenü die Option App Registrations (App-Registrierungen). Klicken Sie auf den Filter Alle Anwendungen, und suchen Sie nach dem Namen, der der Enterprise-Anwendung zugewiesen wurde. Klicken Sie auf die entsprechende Anwendung.



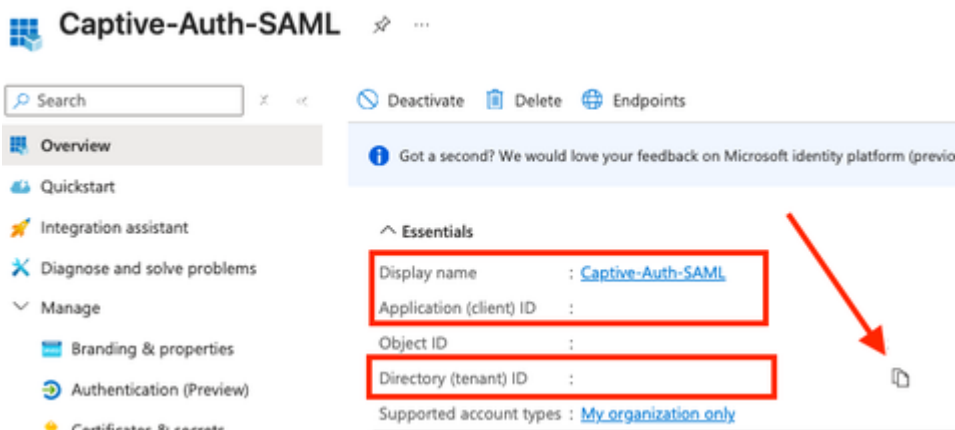
Navigieren Sie zu Anwendungsregistrierungen und allen Anwendungen.

2) Sammeln und notieren Sie die Essentials-Werte unter der Enterprise App-Registrierung.



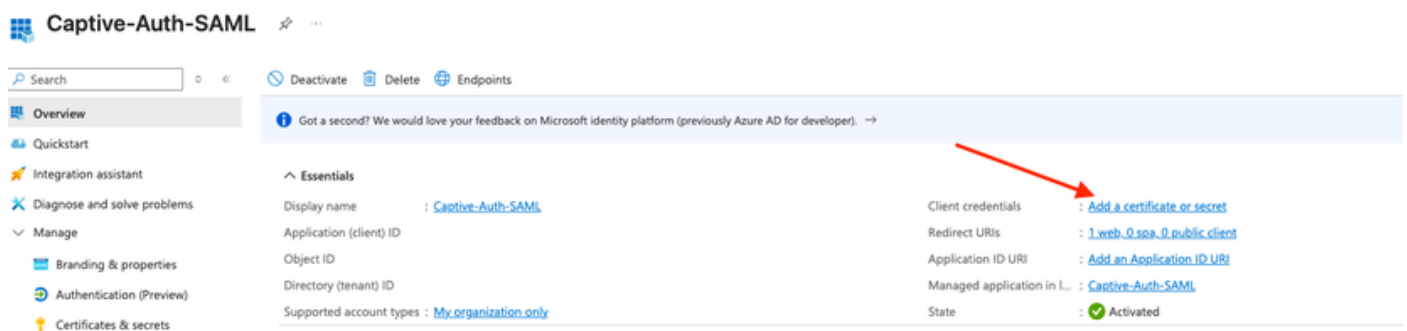
Wichtig: Bewegen Sie den Mauszeiger über die Werte, um In Zwischenablage kopieren anzuzeigen und die Werte unter Grundlagen auf der Seite Übersicht zu sammeln:

- Anzeigenname
- Anwendungs-ID (Client)
- Verzeichnis-ID (Tenant)



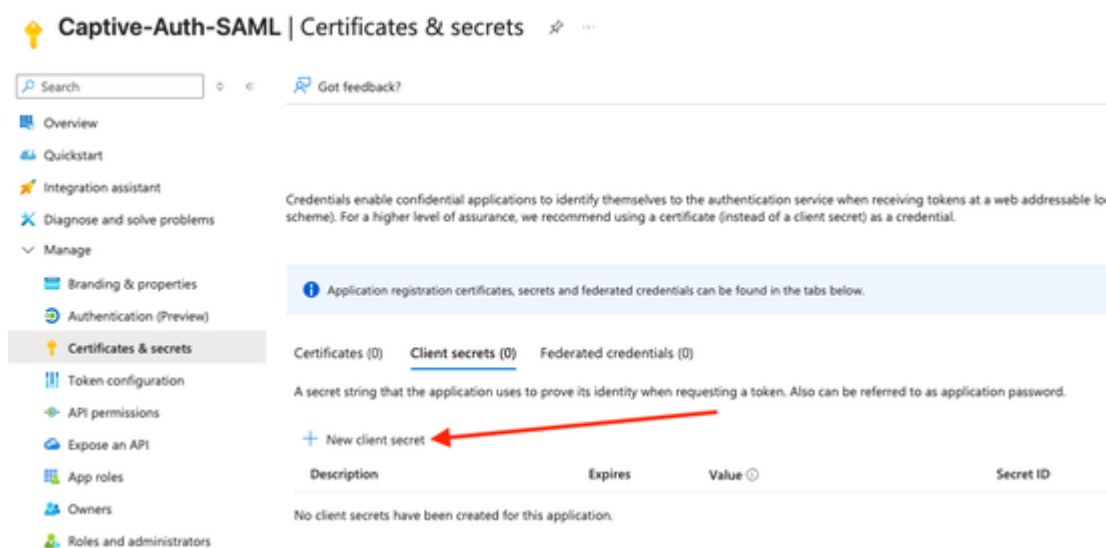
Anzeige-, Anwendungs- und Verzeichnis-ID-Werte erfassen

3) Klicken Sie auf den Hyperlink Zertifikat oder geheimen Schlüssel hinzufügen.



Zertifikat oder geheimen Hyperlink hinzufügen

4) Klicken Sie auf + New client secret.



Neuen Clientschlüssel hinzufügen

5) Geben Sie eine Beschreibung für den geheimen Schlüssel an, und passen Sie den Ablauf bei

Bedarf an. Klicken Sie auf Hinzufügen.

Add a client secret [X]

Description:

Expires:

[Add] [Cancel]

Beschreibung für geheimen Client bereitstellen

6) Kopieren Sie den Schlüssel.



Wichtig: Notieren Sie sich den geheimen Wert, der in die Zwischenablage kopiert wird.

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.

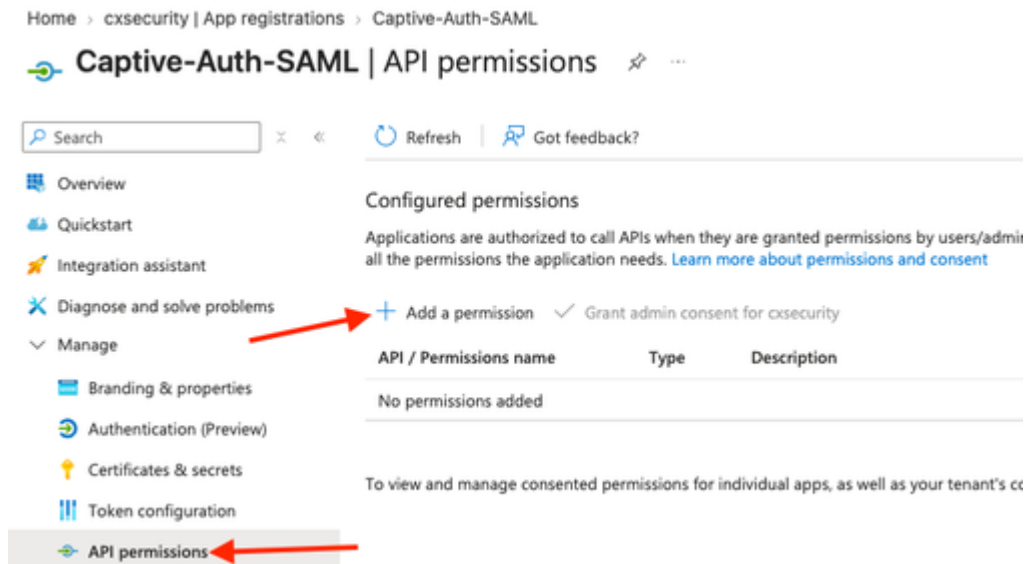
+ New client secret

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

Geheimen Wert des Clients kopieren

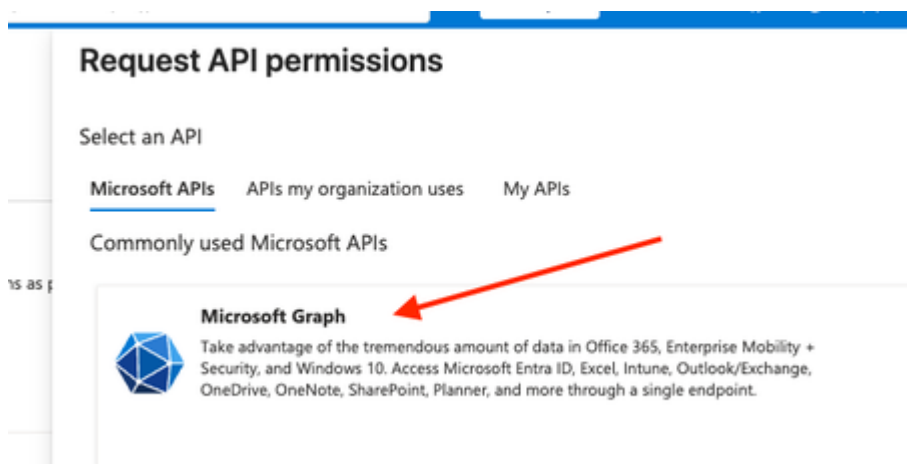
Schritt 3: Konfigurieren von Microsoft Graph API-Berechtigungen für die App-Registrierung

1) Wählen Sie API Permissions aus dem linken Navigationsmenü und klicken Sie dann auf + Add a Permission.



Konfigurieren von API-Berechtigungen

2) Klicken Sie auf Microsoft Graph API.



Microsoft Graph API auswählen

3) Gewähren Sie delegierten Benutzer.Read-Berechtigungen, und klicken Sie dann auf Berechtigungen hinzufügen.

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

Delegierten Benutzern Leseberechtigungen erteilen

4) Gewähren von Berechtigungen für Application User.Read.All (Aktivieren Sie das Kontrollkästchen).

Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

expand all

User.Read.All

Permission

Admin consent required

> IdentityRiskyUser

▼ User (1)

Permission	Admin consent required
☒ User.Read.All ⓘ Read all users' full profiles	Yes

Anwendung zum Lesen aller Berechtigungen gewähren

5) Suchen Sie nach dem Kontrollkästchen Group.Read.All, und aktivieren Sie es, um auch Group Read-Berechtigungen zu erteilen. Klicken Sie auf Berechtigungen hinzufügen.

Select permissions

expand all

Group.Read.All

Permission

Admin consent required

▼ Group (1)

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

Add permissions Discard

API-Berechtigungen speichern

6) Bestätigen Sie, dass die konfigurierten Berechtigungen übereinstimmen, und erteilen Sie die administrative Zustimmung dazu.

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

Administratorzustimmung für Berechtigungen erteilen

7) Die Ausgabe wird angezeigt, sobald die Zustimmung des Administrators erteilt wurde.

+ Add a permission

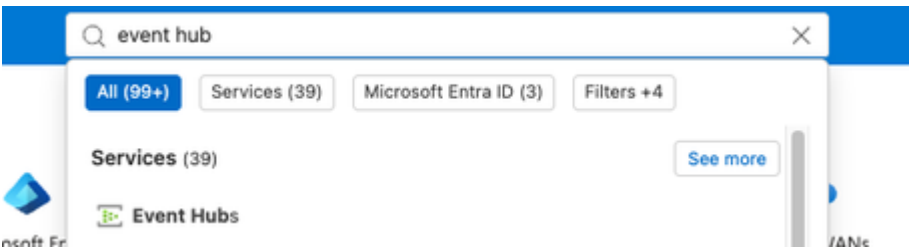
✓ Grant admin consent for

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

Verwaltungszustimmung erteilt Ausgabe

Schritt 4: Konfigurieren des EH-Namespaces (Event Hub)

1) Suchen Sie nach Event Hubs, und klicken Sie auf Event Hubs.



Hub-Konfiguration für Suchereignisse

2) Erstellen Sie einen neuen EH-Namespaces.



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](#)

Ereignis-Hub-Namespace erstellen

3) Konfigurieren Sie den EH-Namespace.



Anmerkung: Wählen Sie die Standard-Preisstufe oder höher aus. Die einfache Preisstufe verhindert die Nutzung von Realms.

Weitere Informationen zur Bewertung der erweiterten Einstellungen des Event Hub und der Anwendbarkeit auf bestimmte Anforderungen finden Sie in der [Azure Event Hub-Dokumentation](#).

Klicken Sie auf Prüfen + Erstellen.



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 >

Konfigurieren der Ereignis-Hub-Namespaceeinstellungen

4) Klicken Sie nach der erfolgreichen Validierung auf Erstellen.



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 >

Bereitstellung des Event Hub-Namespace erstellen

5) Bestätigen Sie, dass die Bereitstellung abgeschlossen ist, und klicken Sie dann auf Zur Ressource wechseln.



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

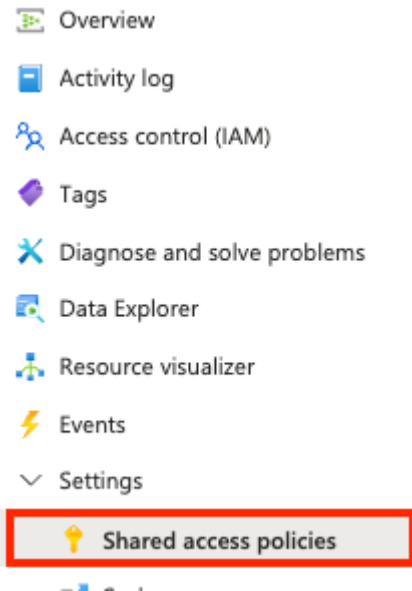
✓ Next steps

Go to resource

Gehe zu Ereignishub-Namespace Ressource

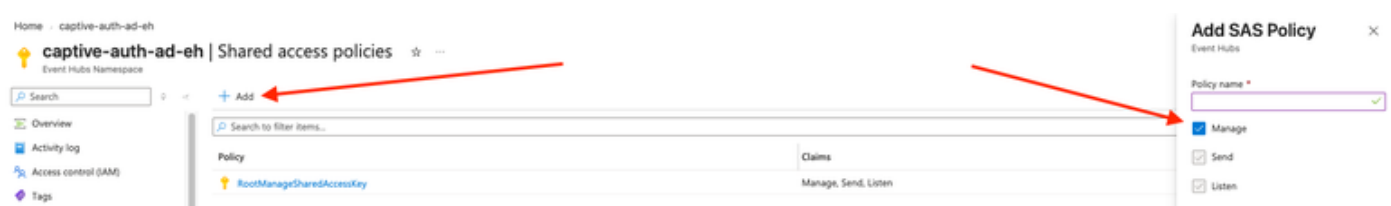
Schritt 5: Auswählen oder Erstellen von Richtlinien für gemeinsamen Zugriff im Event Hub-Namespace

1) Wählen Sie im linken Navigationsmenü Einstellungen > Richtlinien für gemeinsamen Zugriff aus.



Navigieren zu Richtlinien für gemeinsamen Zugriff

2) Klicken Sie auf + Hinzufügen, geben Sie den neuen Richtliniennamen ein, und aktivieren Sie das Kontrollkästchen Verwalten. Klicken Sie unten im Menübereich SAS-Richtlinie hinzufügen auf Erstellen.



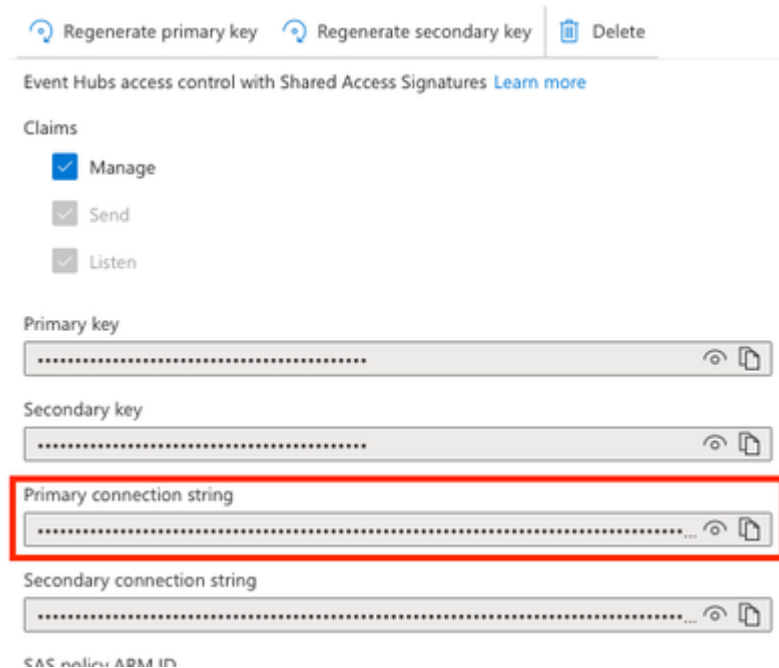
Neue Richtlinie für gemeinsamen Zugriff hinzufügen



Erstellen einer gemeinsam genutzten Zugriffsrichtlinie

Schritt 6: Sammeln und Notieren von SAS-Informationen (Shared Access Signature) aus dem EH-Namespace

1) Klicken Sie auf die neue Richtlinie für gemeinsamen Zugriff. wird die EH SAS Policy (EH-SAS-Richtlinie) in der Seitenleiste rechts angezeigt.



Regenerate primary key Regenerate secondary key Delete

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

Claims

- ☒ Manage
- ☐ Send
- ☐ Listen

Primary key

Secondary key

Primary connection string

Secondary connection string

SAS policy: ADM ID

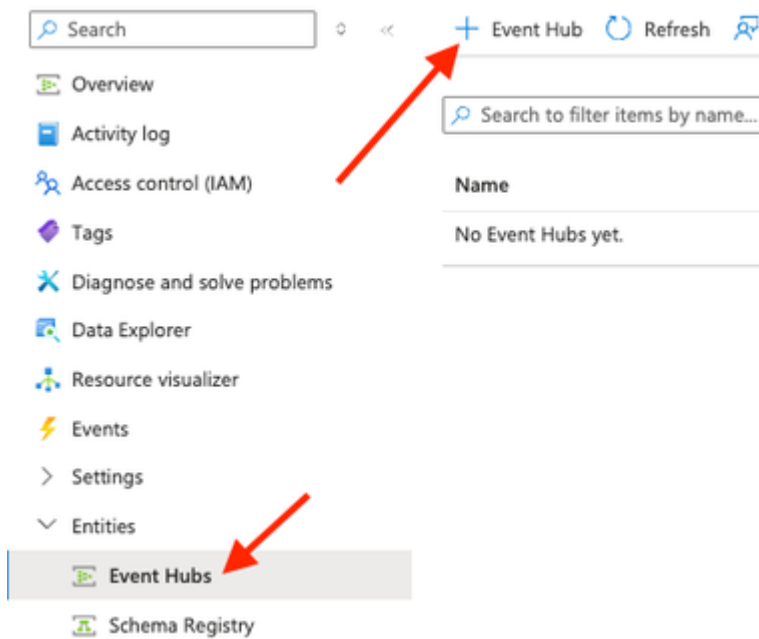
Primäre Verbindungszeichenfolge kopieren



Wichtig: Kopieren Sie die primäre Verbindungszeichenfolge, und notieren Sie sie.

Schritt 7: Erstellen einer Event Hub-Instanz im Event Hub-Namespace

1) Wählen Sie im Menü Namespace die Option Entities > Event Hubs aus. Klicken Sie auf + Event Hub, um eine neue EH-Instanz zu erstellen.



Neue Ereignis-Hub-Instanz erstellen

2) Weisen Sie der neuen EH-Instanz einen Namen zu, und klicken Sie dann auf Prüfen + Erstellen.

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 >

Name der Ereignis-Hub-Instanz zuweisen

3) Klicken Sie nach erfolgreicher Validierung auf Erstellen, um die Event Hub-Instanz bereitzustellen.

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 >

Hub-Instanz des Bereitstellungsereignisses



Wichtig: Kopieren Sie den Event Hub-Instanznamen, und notieren Sie ihn.

Schritt 8: Erstellen einer Ereignishub-Instanzverbrauchergruppe im Ereignishub-Namespace

1) Klicken Sie auf die neue EH-Instanz, die im vorherigen Schritt konfiguriert wurde.

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

Konfiguration der Access Event Hub-Instanz

2) Wählen Sie in der EH-Instanz Entities > Consumer groups, und erstellen Sie eine neue Consumer-Gruppe.

Search

+ Consumer group

Search to filter items by

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

Verbrauchergruppe erstellen

3) Nennen Sie die Verbrauchergruppe, und klicken Sie auf Erstellen.

Create consumer group ×

Consumer groups

Name *

captive-auth-ad-eh-cg



Create

Namen der Verbrauchergruppe zuweisen



Wichtig: Kopieren Sie den Namen der Consumer-Gruppe der Event Hub-Instanz, und notieren Sie ihn.

Schritt 9: Erfasste Werte überprüfen

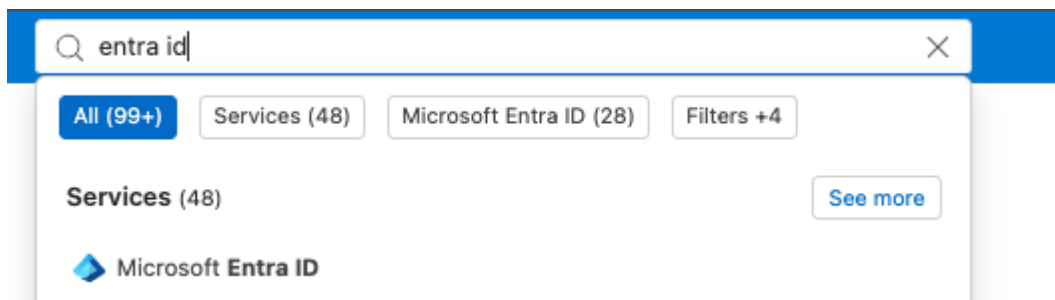
1) An dieser Stelle sind diese Werte aus den vorhergehenden Schritten zu beachten. Wenn kein Wert erfasst wurde, verweisen Sie auf den entsprechenden Schritt, in dem der Wert erfasst wird:

- Phase 3 - Schritt 2 - App-Registrierung (der für diesen Prozess erstellten Enterprise-App, auf die der erfasste Anzeigename verweist)
 - Schritt 2, Unterschritt 2
 - Anzeigename
 - Anwendungs-ID (Client)
 - Verzeichnis-ID (Tenant)
 - Schritt 2, Unterschritt 6
 - Client-Schlüssel
- Phase 3 - Schritt 6 - Event Hub
 - Schritt 6, Unterschritt 1
 - EH-Namespace

- Primäre Verbindungszeichenfolge
- Schritt 7, Unterschritt 3
 - EH-Instanzname (Event Hub)
- Schritt 8, Unterschritt 3
 - Name der EH-Verbrauchergruppe

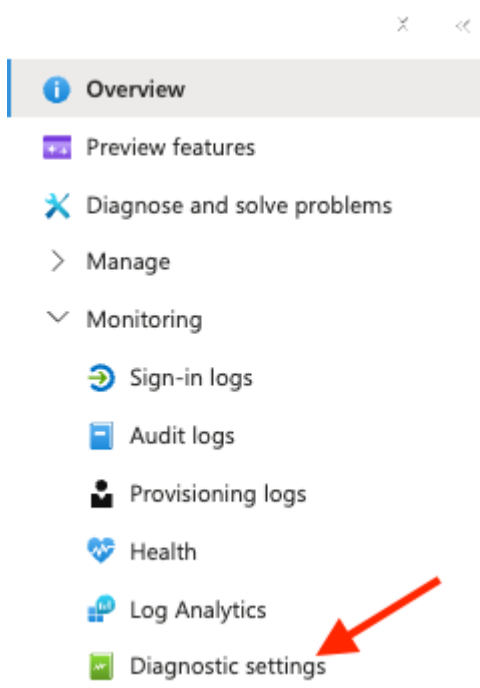
Phase 10: Konfigurieren des Streaming des Prüfprotokolls für die Entra-ID für den Event Hub

1) Navigieren Sie zurück zur Tenant-Konfiguration für die Entra-ID.



Suchen Sie nach der Tenant-Konfiguration für die Eingabe-ID, und navigieren Sie zu dieser.

2) Wählen Sie im Menü links Monitoring > Diagnostic Settings.



Überwachung der Diagnoseeinstellungen

3) Wählen Sie Diagnoseeinstellungen > Allgemein aus, und klicken Sie auf + Diagnoseeinstellung hinzufügen.

Diagnostic settings | General



Can you explain how to send diagnostic logs

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

Neue Diagnoseeinstellung hinzufügen

4) Weisen Sie der Diagnoseeinstellung den erforderlichen Namen zu, aktivieren Sie das Kontrollkästchen AuditLogs (Überwachungsprotokolle) für die Protokollierung, und aktivieren Sie das Kontrollkästchen Stream to an einen Ereignishub (Stream an einen Ereignishub). Verweisen Sie auf die Werte aus den vorherigen Konfigurationen, und klicken Sie abschließend auf Speichern.

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

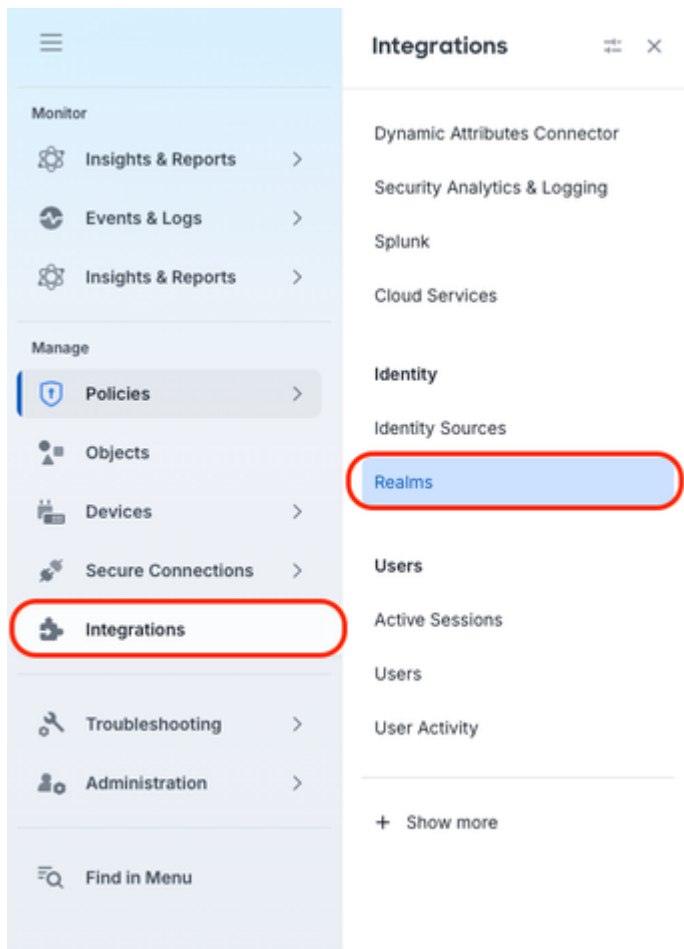
- ☐ Send to partner solution

Überwachungsprotokolle an den Ereignis-Hub streamen

Phase 4: Azure und FMC/FTD Active Authentication-Konfiguration konsolidieren

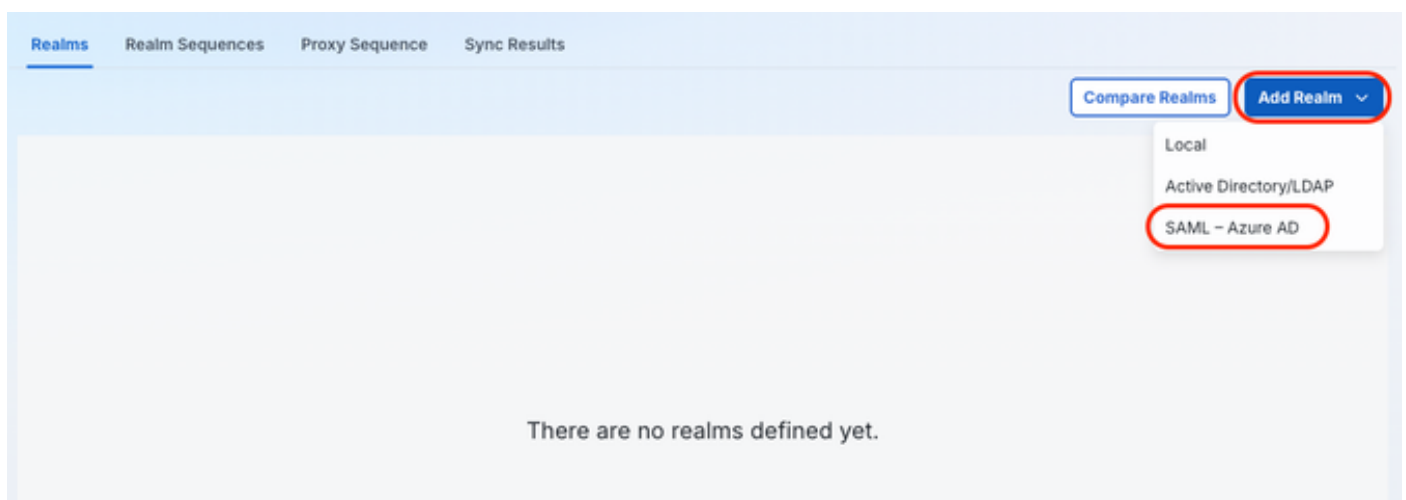
Schritt 1: Konfigurieren des Azure SAML/Entra ID-Bereichs mithilfe des FMC-Assistenten

1) Wählen Sie im FMC "Integrations" > "Identity" > "Realms".



Konfiguration der Identitätsbereiche

2) Klicken Sie auf die Dropdown-Liste Add Realm (Bereich hinzufügen), und wählen Sie SAML - Azure AD aus.



SAML Azure AD-Bereich hinzufügen

3) Weisen Sie dem Azure-Bereich einen Namen und eine Beschreibung zu, um dessen Verwendung zu beschreiben, und stellen Sie sicher, dass die passive Authentifizierung mit Azure AD oder die Verwendung des Captive Portals mit Azure AD aus der Konfigurationstyp-Dropdown-

Liste ausgewählt wird. Klicken Sie auf Next (Weiter).

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

Azure AD-Bereichseinstellungen konfigurieren

4) Wählen Sie das zuvor konfigurierte FQDN-Objekt als Basis-URL aus. Geben Sie die Entitäts-ID im angezeigten Zeichenfolgenformat ein:

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

- Wenn das Suffix "SAML Entity ID" konfiguriert ist (im nächsten Konfigurationsbeispiel grün unterstrichen), stellen Sie sicher, dass das Suffix bei anderen SSO-Implementierungen in der Umgebung eindeutig ist. Dieser Wert muss auch mit der Azure SAML-Konfiguration übereinstimmen. Die Basis-URL bleibt während der gesamten Konfiguration unverändert.
- Die ACS-URL (Assertion Consumer Services) wird automatisch ausgefüllt und ist unveränderlich.
- Wählen Sie das Service Provider (SP)-Zertifikat aus, das in den vorherigen Workflow-Schritten in FMC unter Geräte > Zertifikate registriert wurde.
- Klicken Sie nach der Eingabe dieser Werte auf Download Service Provider Metadata (Dienstanbieter-Metadaten herunterladen), um den Konfigurationsprozess zu vereinfachen und zu bestätigen, dass die erwarteten Werte in Azure geschrieben werden.

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

Basis-URL und Entitäts-ID konfigurieren und SAML-Metadaten herunterladen

5) Klicken Sie auf Weiter, um zu Sequenz 3 der Realm-Konfiguration zu gelangen.

Phase 2: Implementieren der FMC-konfigurierten SAML SP-Metadaten in der Azure Enterprise-Anwendung

1) Navigieren Sie zurück zu Azure, und wählen Sie Entra ID > Manage > Enterprise Applications. Suchen Sie nach der zuvor erstellten Instanz der Microsoft Entra SAML Toolkit Enterprise-Anwendung.

Microsoft Azure

Home > Enterprise applications

Enterprise applications | All applications

+ New application Refresh Download (Export) Preview info Columns Preview features Got it

Overview

Manage

- All applications
- Private Network connectors
- User settings
- App launchers

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Search: Captive-Auth-SAML Application type == Enterprise Applications

1 application found

Name	Object ID	Application ID	Homepage URL
Captive-Auth-SAML			

Suche nach Microsoft Entra SAML Toolkit-Anwendung

2) Wählen Sie im seitlichen Navigationsmenü Verwalten > Single Sign-On.

Home > Enterprise applications | All ap

Captive-Auth-SAML

Enterprise Application

Overview

Deployment Plan

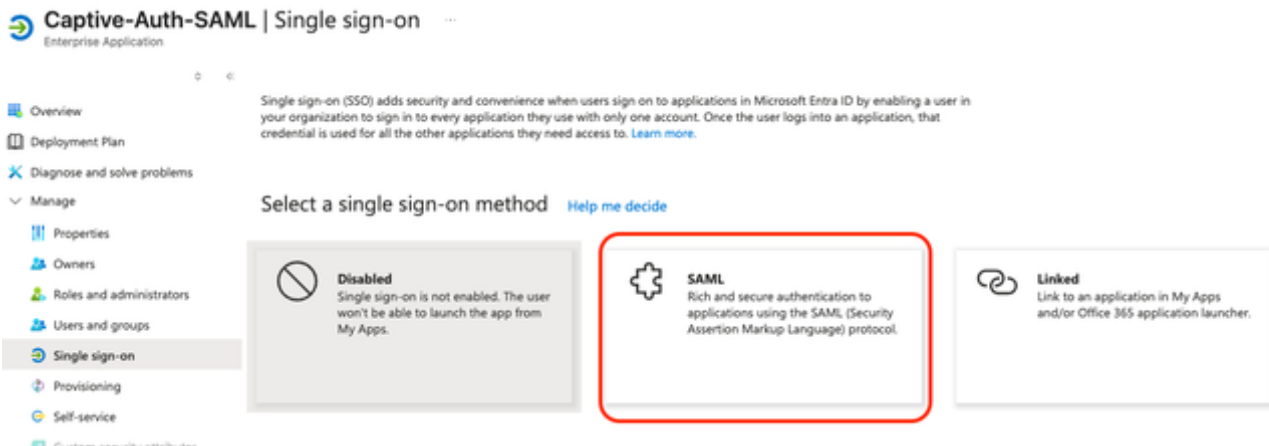
Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes

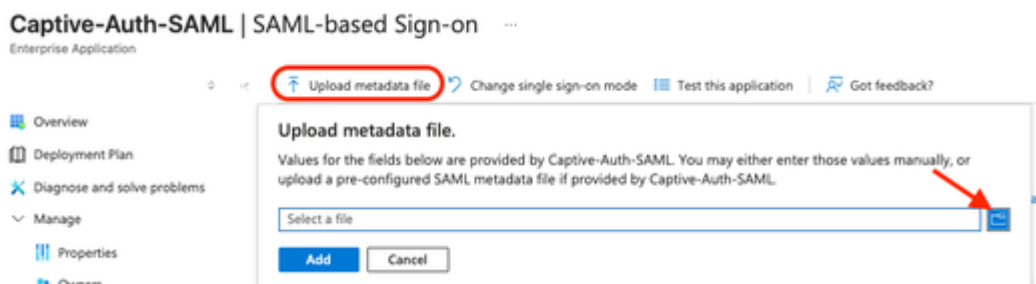
Konfiguration für einmaliges Anmelden verwalten

3) Klicken Sie auf den Modus SAML Single Sign-On (SSO).



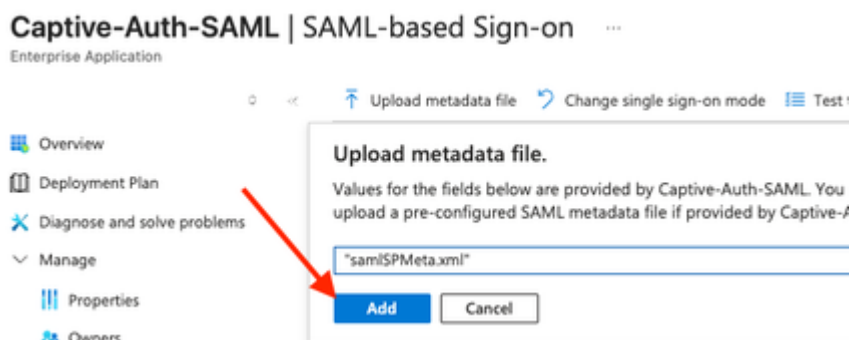
Auswahl des SAML Single Sign On-Modus

4) Klicken Sie auf Metadatendatei hochladen und dann auf das blaue Ordnersymbol, um das lokale Dateisystem nach der SAML-Metadatendatei zu durchsuchen, die vom FMC heruntergeladen wurde.



Hochladen der Metadatendatei vom Firewall Management Center

5) Klicken Sie nach Abschluss des Uploads auf Hinzufügen.



SAML-Konfigurationsanwendung hinzufügen

6) Die Seite für die grundlegende SAML-Konfiguration wird angezeigt, und Werte wie der Identifier (Entity ID) und die ACS-URL werden aus der XML-Datei mit den FMC-Metadaten extrahiert, die automatisch hochgeladen und angewendet wird. Die Anmelde-URL wird jedoch nicht ausgefüllt und ist vor dem Speichern erforderlich.

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.



Extraktion der grundlegenden SAML-Konfiguration

7) Verwenden Sie das angegebene Muster für die Anmelde-URL, kopieren Sie den Wert, fügen

Sie ihn ein, und klicken Sie nach Abschluss des Vorgangs oben auf Speichern.

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)

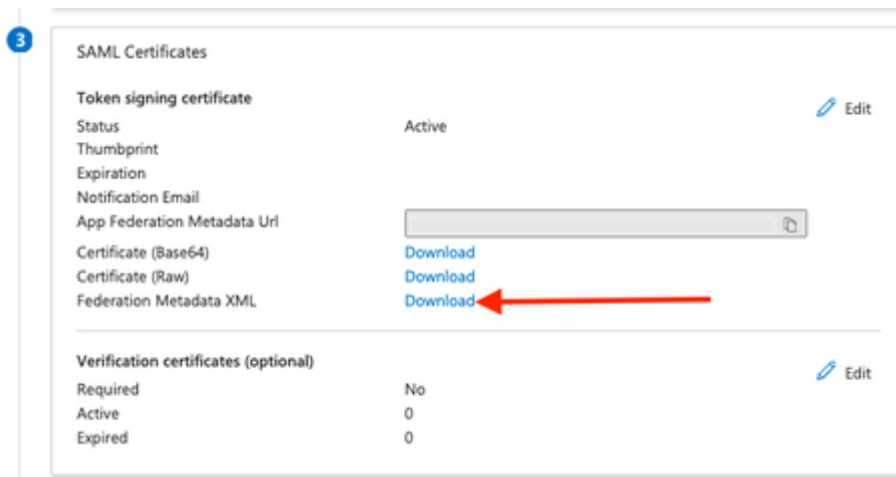
This URL is used to send the SAML logout response back to the application.

✓

URL-Konfigurationseintrag für die Anmeldung

Blättern Sie nach unten zu SAML-Zertifikate, und exportieren Sie die Azure-generierte

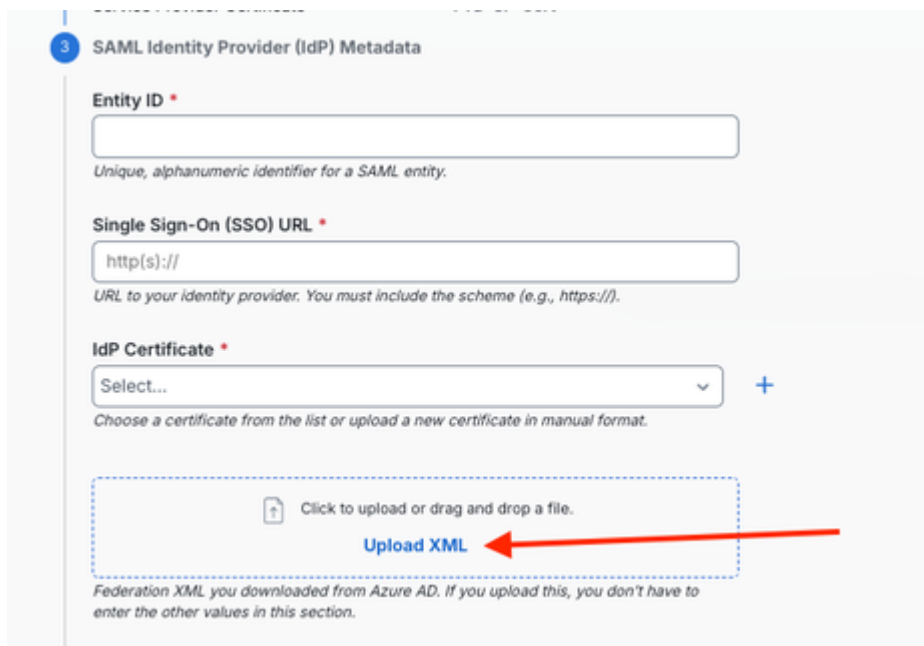
Verbundmetadaten-XML-Datei zum Importieren in Cisco Secure FMC.



Verbundmetadaten-XML-Datei exportieren

Schritt 3: Konfigurieren des Azure SAML-/Entra-ID-Bereichs mithilfe des FMC-Assistenten (Fortsetzung)

1) Navigieren Sie zurück zum FMC. Laden Sie unter "Sequence 3, SAML Identity Provider (IdP) Metadata" die exportierte Verbundmetadaten-XML-Datei, die von Azure heruntergeladen wurde, in das FMC hoch, um die erforderlichen Werte automatisch aufzufüllen.



Verbundmetadaten-XML-Datei hochladen

2) Nach dem Hochladen werden die Werte wie dargestellt angezeigt.

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.



Automatisch ausgefüllte SAML-Identitätsanbieterwerte



Anmerkung: Eine teilweise Ausgabe wird im Bild angezeigt.

3) Geben Sie die während des gesamten Implementierungsprozesses gesammelten Werte bis zu diesem Punkt ein:

- App-Registrierung
 - Anwendungs-ID (Client)
 - Client-Schlüssel
 - Verzeichnis-ID (Tenant)
- Event-Hub
 - Hostname des EH-Namespaces
 - EH-Namespace Primäre Verbindungszeichenfolge
 - Name der EH-Instanz (Event Hub)
 - Name der EH-Verbrauchergruppe

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

Anwendungs- und Ereignis-Hub-Informationen eingeben

Klicken Sie nach der Eingabe auf Test, um die Verbindung zu überprüfen und zu bestätigen, dass Azure mit den bereitgestellten Informationen erreichbar ist.



Anmerkung: Stellen Sie ggf. sicher, dass die ausgeschlossenen/eingeschlossenen Benutzergruppen auf Ihre Entra-Konfiguration ausgerichtet sind.

4) Im letzten Schritt des Assistenten können Sie das Timeout für SAML Captive Portal Users konfigurieren. Der Standardwert ist 1440 Minuten.

5 User Session Timeout

SAML Captive Portal Users

Minutes Range 0-35791394

Captive Portal-Timeout konfigurieren

5) Klicken Sie auf Weiter, um fortzufahren.

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**

Vorwärts mit Azure AD Realm-Konfiguration

6) Der Assistent bietet eine Zusammenfassung der implementierten Konfiguration. Klicken Sie am Ende der Zusammenfassung auf Speichern, nachdem die eingegebenen Werte validiert und bestätigt wurden.

5 User Session Timeout Edit

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

 **Cancel** **Save**

Schaltfläche zum Speichern der Bereichskonfigurationsübersicht

Schritt 4: Heruntergeladene Benutzer überprüfen

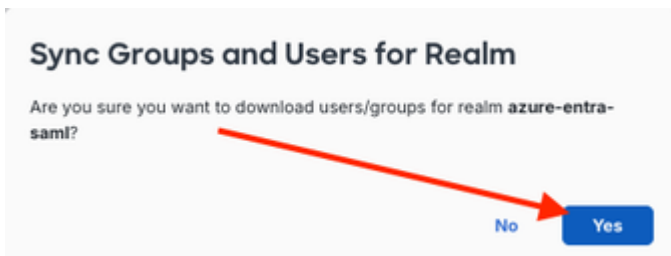
1) Bestätigen Sie, dass Benutzer von Azure Entra heruntergeladen werden können, indem Sie im Workflow "Integrations > Identity > Realms" auf die Schaltfläche Jetzt herunterladen klicken.

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

 **Download Now**

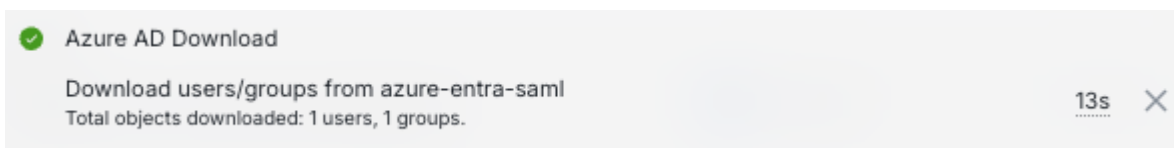
Benutzer aus Azure AD herunterladen

2) Klicken Sie auf Ja als Antwort auf die Dialogfeldaufforderung.



Download von Benutzern aus Azure AD bestätigen

3) Die Download-Aufgabe ergibt 1 Benutzer und 1 Gruppe heruntergeladen, wie unter Benachrichtigungen > Aufgaben bestätigt.

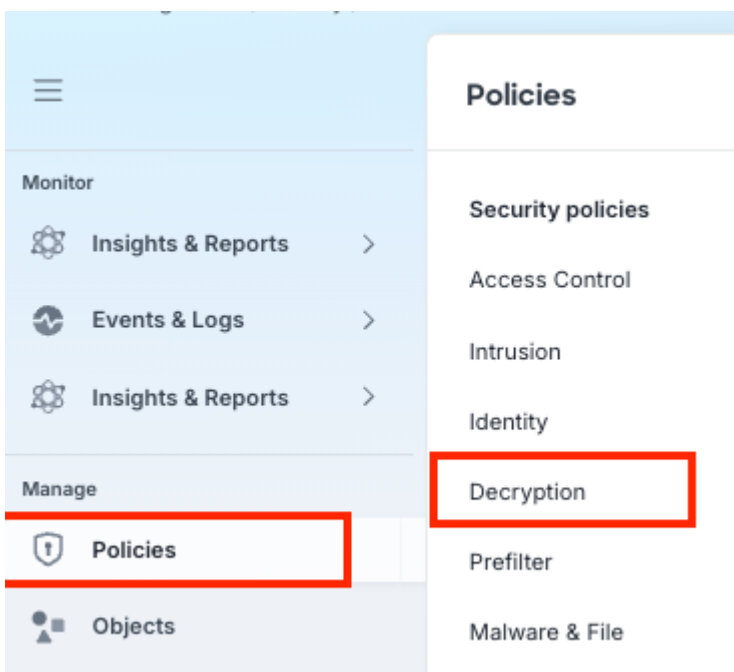


Benachrichtigungseintrag für den Download von Benutzern aus Azure AD

Phase 5: Konfigurieren von Richtlinien im FMC

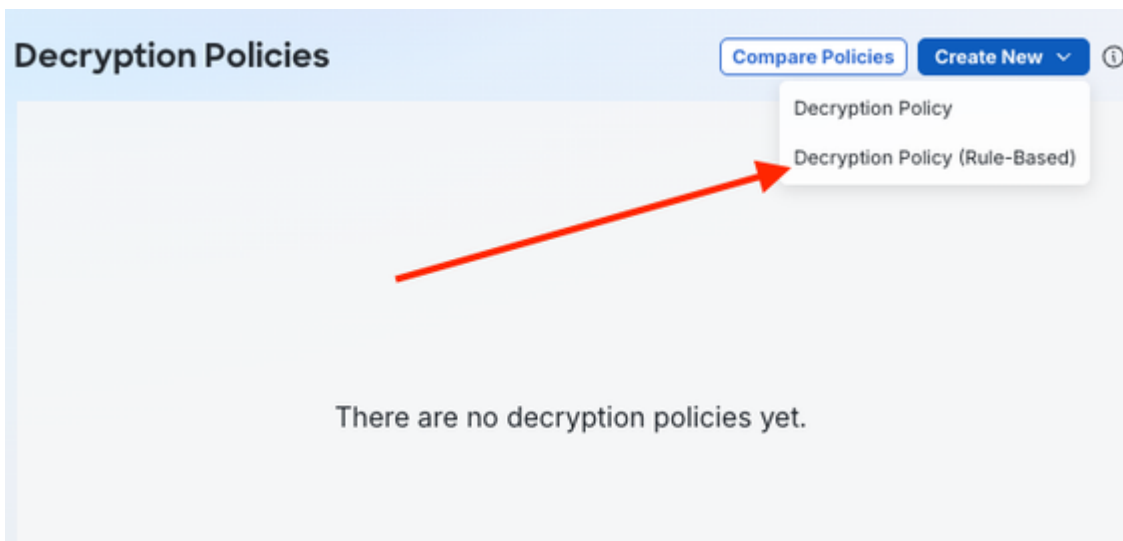
Schritt 1: Entschlüsselungsrichtlinie konfigurieren

1) Wählen Sie im FMC Policies > Security Policies > Decryption (Richtlinien > Sicherheitsrichtlinien > Entschlüsselung).



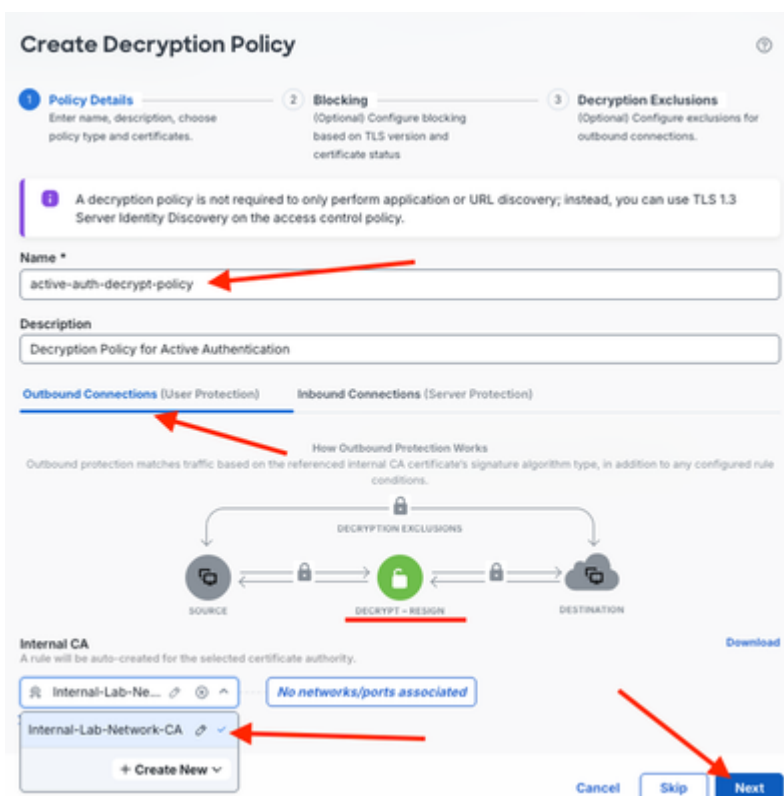
Zur Entschlüsselungsrichtlinie navigieren

2) Klicken Sie auf die Dropdown-Liste Neu erstellen, und wählen Sie Entschlüsselungsrichtlinie (regelbasiert).



Neue regelbasierte Entschlüsselungsrichtlinie erstellen

3) Weisen Sie der neuen regelbasierten Entschlüsselungsrichtlinie einen Namen und, falls gewünscht, eine Beschreibung zu, und klicken Sie auf die Registerkarte Outbound Connections (User Protection), um die für die Captive Portal-Authentifizierung (Active Authentication) erforderliche Entschlüsseln-Zurückweisen-Funktion zu implementieren.



Richtliniendetails für ausgehende Verbindungen implementieren

4) Wählen Sie die zuvor angewendete interne Zertifizierungsstelle aus der entsprechenden Dropdown-Liste im selben Dialogfeld aus. Klicken Sie auf Next (Weiter).

5) Passen Sie die Optionen nach Bedarf an.

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**

Entschlüsselungsrichtlinienoptionen anpassen

6) In diesem Beispiel werden mit Ausnahme der erforderlichen Richtliniendetails Standardwerte verwendet. Schließen Sie den Konfigurationsassistenten durch Klicken auf Richtlinie erstellen ab.

Create Decryption Policy ?

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

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

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

Decryption Exclusions

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

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

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

Intelligent Decryption Bypass

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

Cancel Skip Back Create Policy

Endgültige Entschlüsselungsrichtlinie erstellen

Phase 2: Entschlüsselungsrichtlinienregeln konfigurieren

1) Hier sehen Sie das Standardlayout einer regelbasierten Entschlüsselungsrichtlinie. Datenverkehr, der nicht mit den standardmäßig aktivierten Regeln übereinstimmt, z. B. Regel 3 (die auf eine vorab zugewiesene Liste nicht verschlüsselbarer Domännennamen verweist) und Regel 6 (die auf Anwendungen verweist, die als nicht verschlüsselbar gekennzeichnet sind), unterliegt der Aktion Entschlüsseln - Zuweisen gemäß Regel 7. Diese Standardwerte können zusammen mit der Standardaktion nach Bedarf geändert werden. Standardmäßig wird Datenverkehr, der keiner anderen Regel entspricht, mit der Option "Nicht entschlüsseln" konfiguriert.

Der Datenverkehr des Azure-Authentifizierungsdiensts darf nicht zur Überprüfung entschlüsselt werden. Daher wird eine dedizierte Regel dafür erstellt. Klicken Sie zum Starten auf + Regel hinzufügen.

active-auth-decrypt-policy Save Cancel

Decryption Policy for Active Authentication

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

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

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	Auto-Rule-Certificate-Stz (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Cert Status s	Block with reset
2	Auto-Rule-TLS-Versions (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Protocol Vers	Block with reset
3	Auto-Rule-Undecrypt	any	any	any	any	any	any	any	any	any	any	1 DN selection	Do not decrypt
4	Auto-Rule-Low-Risk-Con (Disabled)	any	any	any	any	any	any	any	any	any	Any (Except L	1 Client Threat	Do not decrypt
5	Auto-Rule-URL-Categoris (Disabled)	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 hinzufügen und standardmäßiges regelbasiertes Entschlüsselungslayout anzeigen

2) Weisen Sie dem neuen Eintrag der Entschlüsselungsrichtlinie einen Namen zu, wählen Sie Nicht entschlüsseln aus der Dropdown-Liste Aktion, und platzieren Sie die Regel an der Spitze der weniger spezifischen Regeln. Source/Destination-Zonen werden ebenfalls implementiert, um die Regel weiter einzugrenzen.

Add Rule

Name: ☒ Enabled

Action:

Insert:

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

Available Zones

- Inside_Zone
- Outside_Zone
- DMZ_Zone

Source Zones (1):

Destination Zones (1):

Konfigurieren der Regel "Nicht entschlüsseln"

3) Klicken Sie vor dem Hinzufügen der Regel auf die Registerkarte Anwendungen, suchen Sie nach der Azure-Authentifizierungsdienst-Anwendung, und klicken Sie auf Zur Regel hinzufügen, und klicken Sie dann auf Hinzufügen.

Add Rule

Name: Azure-Auth-Service-DND ☒ Enabled Insert: above rule 3

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 009

Available Applications (2)

Search by name: azure a

All apps matching the filter

- Azure Arc
- Azure Authentication Service**

Selected Applications and Filters (0)

any

Anwendungsregel für Azure-Authentifizierungsdienst hinzufügen

4) Klicken Sie auf Speichern.

active-auth-decrypt-policy

Decryption Policy for Active Authentication

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

You have unsaved changes

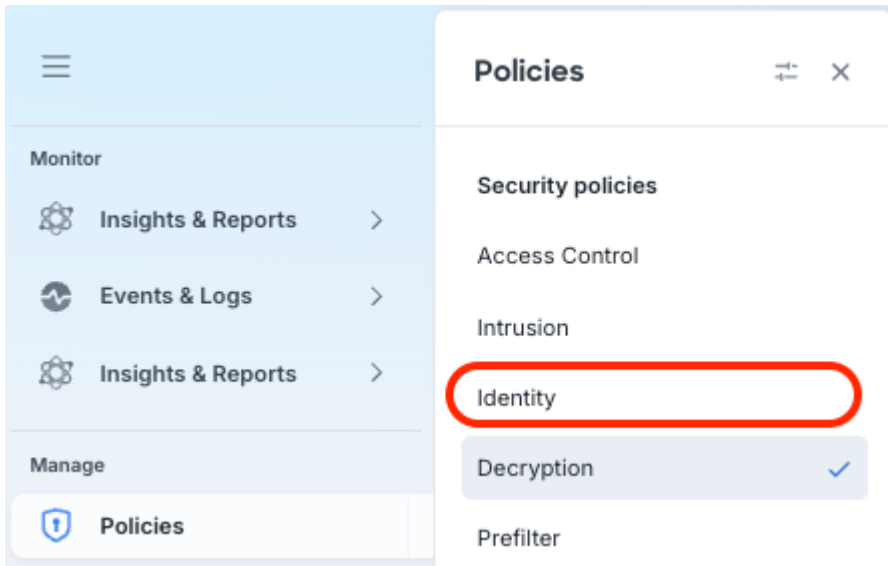
+ Add Category + Add Rule

#	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 Ver	Block with reset
3	Azure-Auth-Service-Inside_Zone_Outside_Zon	any	any	any	any	any	any	Azure Authen	any	any	any	any	Do not decrypt

Entschlüsselungsrichtlinie speichern

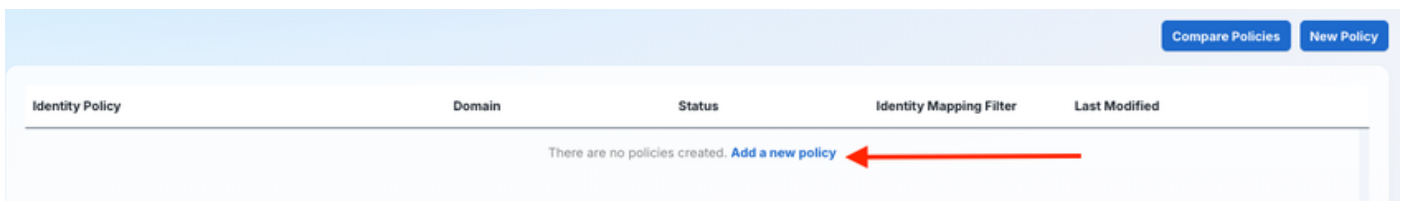
Schritt 3: Identitätsrichtlinie erstellen

1) Wählen Sie Policies > Security Policies > Identity (Richtlinien > Sicherheitsrichtlinien > Identität), um eine Identitätsrichtlinie zu erstellen.



Identitätsrichtlinie erstellen

2) Erstellen Sie eine neue Identitätsrichtlinie, und klicken Sie auf Neue Richtlinie hinzufügen.



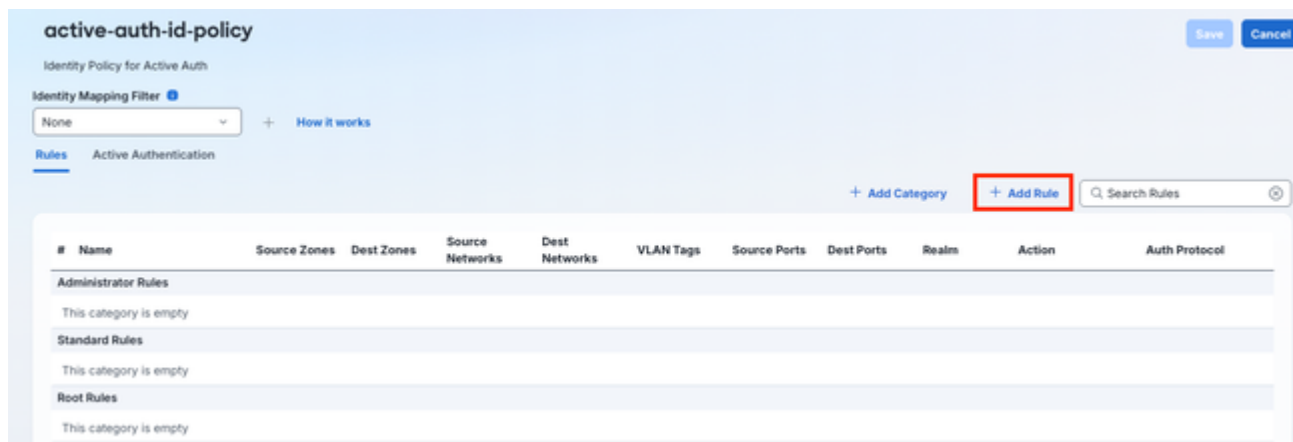
Neue Identitätsrichtlinienkonfiguration hinzufügen

3) Weisen Sie der neuen Identitätsrichtlinie einen Namen und gegebenenfalls eine Beschreibung zu. Klicken Sie auf Speichern.

Neue Identitätsrichtlinie benennen

Schritt 4: Identitätsrichtlinien-Regeln konfigurieren

1) Fügen Sie eine neue Regel hinzu, indem Sie auf + Regel hinzufügen klicken.



Neue Identitätsrichtlinienregel hinzufügen

2) Benennen Sie die neue Regel, wählen Sie Aktive Authentifizierung aus der Dropdown-Liste Aktion, und schränken Sie die spezifischen Zonen/Netzwerke ein, die der Regel entsprechen müssen, um die aktive Authentifizierung auszuführen.

Einstellungen für aktive Authentifizierungsregeln konfigurieren

3) Bevor Sie auf Hinzufügen klicken, klicken Sie im Regel-Editor auf die Registerkarte Bereich und Einstellungen. Bestätigen Sie, dass der in den vorherigen Schritten konfigurierte Bereich als

Authentifizierungsbereich ausgewählt ist, und klicken Sie dann auf Hinzufügen.

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

Bereich und Einstellungen für Identitätsregel konfigurieren

4) Die Regel wird hinzugefügt und konfiguriert. Klicken Sie auf Speichern.

active-auth-id-policy

Identity Policy for Active Auth

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

Rules Active Authentication

+ Add Category + Add Rule Search Rules

#	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											

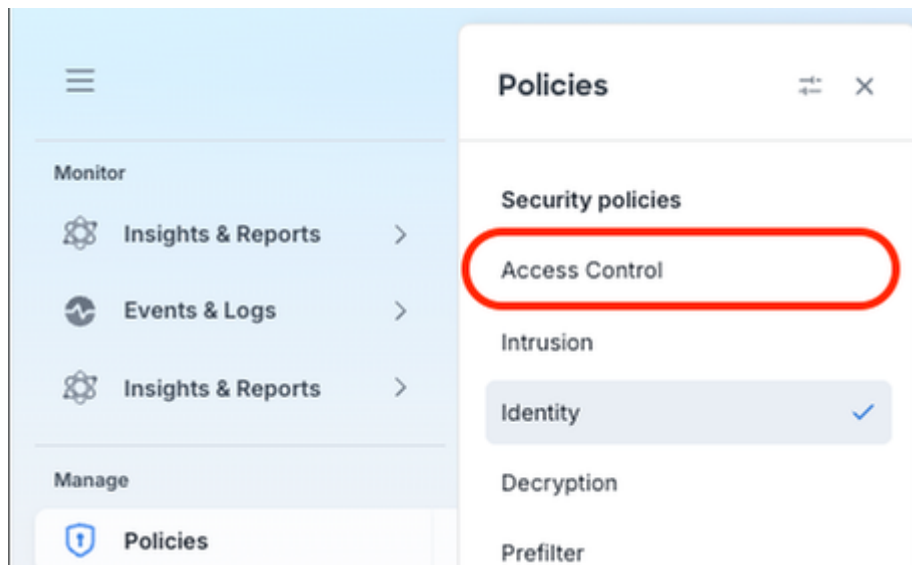
You have unsaved changes Save Cancel

Identitätsrichtlinienregelkonfiguration speichern

Schritt 5: Konfigurieren der Zugriffskontrollrichtlinie

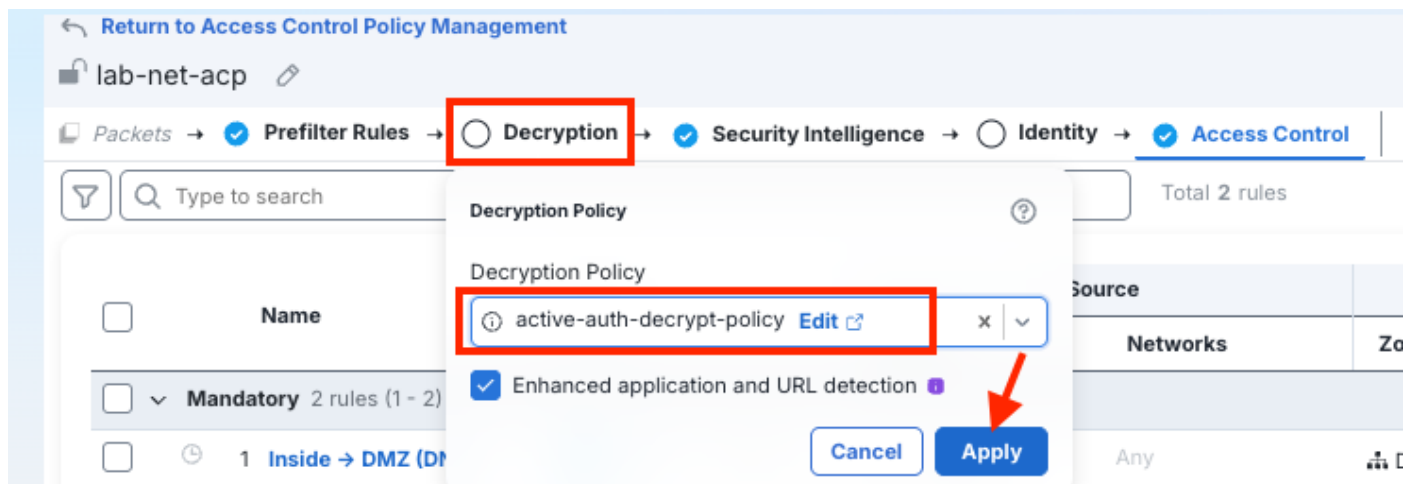
1) Wählen Sie Policies > Security Policies > Access Control aus, und klicken Sie auf die Access

Control Policy, der das FTD zugewiesen ist.



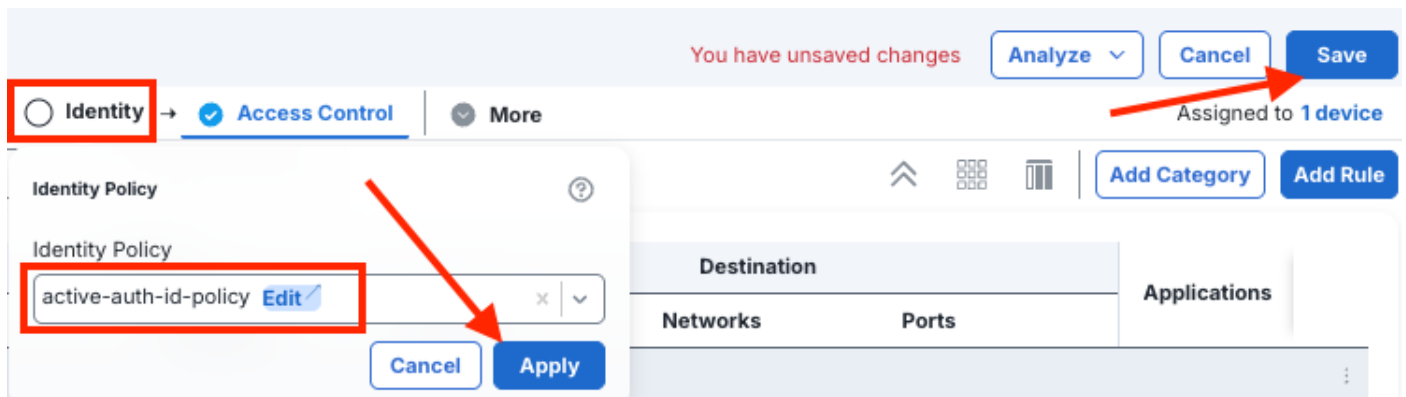
Konfiguration der Zugriffskontrollrichtlinie

2) Vergewissern Sie sich, dass die in den vorherigen Schritten konfigurierte Entschlüsselungsrichtlinie auf die Zugriffskontrollrichtlinie angewendet wird.



Anwenden der Entschlüsselungsrichtlinie auf die Zugriffskontrolle

3) Vergewissern Sie sich, dass die in den vorherigen Schritten konfigurierte Identitätsrichtlinie auch auf die Zugriffskontrollrichtlinie angewendet wird. Speichern Sie die Richtlinienänderungen.



Anwendung der Identitätsrichtlinie auf die Zugriffskontrolle

4) Bestätigen Sie, dass Regeln vorhanden sind, die Datenverkehr auf Client-Datenebene durch die sichere Firewall nach erfolgreicher aktiver Authentifizierung zulassen. Im vorliegenden Beispiel wird ein breiterer Regelsatz verwendet, der auf die Laborumgebung abgestimmt ist.

☐	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)								

Regelsatz für Datenverkehr auf Benutzerdatenebene

Schritt 6: Bereitstellung von Konfigurationen auf den Cisco Secure Firewall-Geräten

Nach der Bereitstellung werden Clients, die Datenverkehr senden, von einer Microsoft-Anmelde-Webseite aufgefordert, eine aktive Authentifizierung mit Azure Entra durchzuführen.

Weitere Informationen zum hier dokumentierten Prozess finden Sie unter [Erstellen eines Microsoft Azure AD-Bereichs \(SAML\) für die aktive Authentifizierung \(Captive Portal\) - Kapitel: Bereiche im Konfigurationsleitfaden 10.x für FMC-Geräte](#).

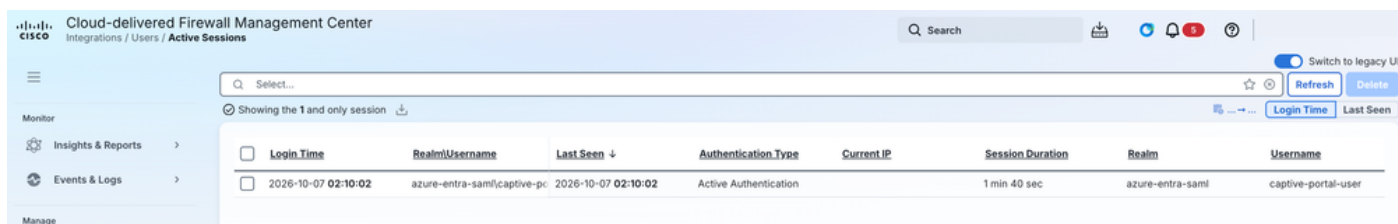
Überprüfung

In diesem Abschnitt können Sie überprüfen, ob die Konfiguration ordnungsgemäß funktioniert.

GUI

Benutzersitzungen und -aktivitäten im FMC validieren:

- Wählen Sie Integrationen > Benutzer > Aktive Sitzungen aus.

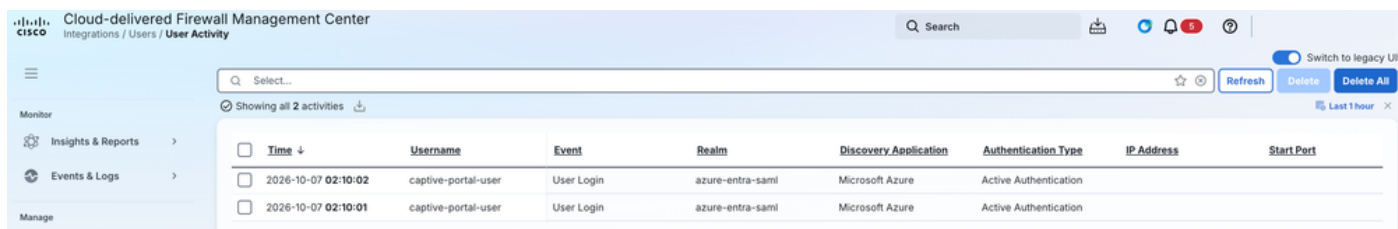


The screenshot shows the Cisco Cloud-delivered Firewall Management Center (FMC) interface. The breadcrumb navigation is 'Integrations / Users / Active Sessions'. The left sidebar has 'Monitor' selected. The main content area shows a table with one session. The table has columns: Login Time, RealmUsername, Last Seen, Authentication Type, Current IP, Session Duration, Realm, and Username. The session is for 'captive-portal-user' from 'azure-entra-saml' at '2026-10-07 02:10:02'.

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

FMC-Ausgabe für aktive Sitzungen

- Wählen Sie Integrationen > Benutzer > Benutzeraktivität aus.



The screenshot shows the Cisco FMC 'User Activity' page. The breadcrumb navigation is 'Integrations / Users / User Activity'. The left sidebar has 'Monitor' selected. The main content area shows a table with two activities. The table has columns: Time, Username, Event, Realm, Discovery Application, Authentication Type, IP Address, and Start Port. Both activities are 'User Login' events for 'captive-portal-user' from 'azure-entra-saml' using 'Microsoft Azure' at '2026-10-07 02:10:02' and '2026-10-07 02:10:01'.

☐	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		

Ausgabe der FMC-Benutzeraktivität

Navigieren Sie auf Azure zum Microsoft Entra-Admin-Center:

- Filtern Sie nach Enterprise-Apps, suchen Sie nach der entsprechenden App, und klicken Sie darauf.

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: captive-

Name	Obj
Captive-Auth...	efda

Navigation zu Azure Entra Admin Center Enterprise-Anwendungen

- Wählen Sie Aktivität > Anmeldeprotokolle aus.

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-Anwendung Anmelde-Aktivitätsprotokolle

CLI

- In der FTD-CLI werden Statistiken zu SAML- und Captive Portal-Antworten angezeigt:

<#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
```

Fehlerbehebung

Captive Portal-Debugging

- Der Befehl `system support captive-portal-debug` kann auf dem FTD verwendet werden. Die Ausgabe zeigt, wie das Debuggen aktiviert wird, und stellt wichtige Segmente der Ausgabe fest, um den Captive Portal-Fluss besser zu verstehen.

```
<#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
...

```

Benutzeridentitäts-Dump

- Führen Sie den Befehl `system support firewall-engine-dump-user-identity-data` in der FTD-CLI aus, um einen Snapshot des aktuellen Status der Benutzeridentität auf dem FTD zu erstellen:

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

Successfully commanded snort.

>

- Wenn Sie sich in der CLI des Expertenmodus mit den lokalen Administratoranmeldeinformationen des FTD-Geräts anmelden, zeigen Sie den Inhalt der gespeicherten Datei unter `/ngfw/var/sf/user_enforcement/user_identity.dump` an.

<#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:

...

Mögliche Probleme

Captive Portal Unbekannte Zertifizierungsstelle

Problem: Der Client-Browser gibt einen unbekannten Ausstellerfehler zurück, wenn eine Authentifizierung versucht wird.

Mögliche Ursache: Die interne Zertifizierungsstelle im Clientbrowser ist nicht vertrauenswürdig.

Auflösung: Bestätigen Sie, dass die Zertifizierungsstelle im Browser vertrauenswürdig ist. Das hier gezeigte Beispiel bestätigt, dass das interne CA-Zertifikat vertrauenswürdig ist.

Captive Portal "Server nicht gefunden"

Problem: Wenn der Client-Browser versucht, das Captive Portal zu laden, gibt er "Server Not Found" für die Basis-URL zurück, während er versucht, die Basis-URL oder Ähnliches zu erreichen.

Mögliche Ursache: DNS-Erreichbarkeit oder fehlerhafte DNS-Konfiguration

Auflösung: Vergewissern Sie sich, dass der entsprechende DNS-Server für die Auflösung des A-Eintrags auf dem Client konfiguriert ist. Vergewissern Sie sich, dass dem FQDN ein A-Eintrag zugeordnet ist und dass der Server erreichbar ist und reagiert.

Zugehörige Informationen

- [Erstellen eines Microsoft Azure AD \(SAML\)-Bereichs für die aktive Authentifizierung \(Captive Portal\) - FMC Device Config Guide 10.x](#)
- [Azure Event Hub-Dokumentation](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.