

Configurer Azure Entra Captive Portal sur Secure Firewall

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme](#)

[Portail captif entre Endpoint, FTD et Azure Entra](#)

[Configurer](#)

[Phase 1 : Configuration initiale de FMC et DNS](#)

[Étape 1: Activer le connecteur d'attributs dynamiques Cisco \(CSDAC\)](#)

[Étape 2: Créer un objet réseau de nom de domaine complet représentatif de l'interface d'entrée FTD](#)

[Étape 3: Configuration de l'enregistrement DNS A](#)

[Phase 2 : Configuration d'infrastructure à clé publique](#)

[Étape 1: Importer le certificat CA interne dans le FMC](#)

[Étape 2: Signer le certificat du fournisseur de services avec l'autorité de certification](#)

[Étape 3: Déployer le certificat SP sur le FTD](#)

[Phase 3 : Configuration Azure](#)

[Étape 1: Création de l'application Entreprise Entra pour le kit d'outils SAML](#)

[Étape 2: Configurer les inscriptions d'application Entra ID](#)

[Étape 3 : configuration des autorisations de l'API Microsoft Graph pour l'enregistrement des applications](#)

[Étape 4: Configuration de l'espace de noms Event Hub \(EH\)](#)

[Étape 5: Choisir ou créer des politiques d'accès partagé dans l'espace de noms Event Hub](#)

[Étape 6: Collecter et noter les informations de signature d'accès partagé \(SAS\) de l'espace de noms EH](#)

[Étape 7: Création d'une instance Event Hub dans l'espace de noms Event Hub](#)

[Étape 8: Créer un groupe de consommateurs d'instances Event Hub dans l'espace de noms Event Hub](#)

[Étape 9: Vérifier les valeurs collectées](#)

[Étape 10: Configuration de la diffusion en continu du journal d'audit Entra ID vers Event Hub](#)

[Phase 4 : Consolider la configuration d'authentification active Azure et FMC/FTD](#)

[Étape 1: Configurer le domaine Azure SAML/Entra ID à l'aide de l'Assistant FMC](#)

[Étape 2: Implémenter les métadonnées SAML SP configurées par FMC dans l'application Azure Enterprise](#)

[Étape 3: Configurer le domaine Azure SAML/Entra ID à l'aide de l'Assistant FMC \(suite\)](#)

[Étape 4: Vérifier les utilisateurs téléchargés](#)

[Phase 5 : Configuration des stratégies dans le FMC](#)

[Étape 1: Configurer la stratégie de déchiffrement](#)

[Étape 2: Configurer les règles de stratégie de déchiffrement](#)

[Étape 3: Créer une stratégie d'identité](#)

[Étape 4: Configurer les règles de stratégie d'identité](#)

[Étape 5: Configurer la stratégie de contrôle d'accès](#)

[Vérifier](#)

[IUG](#)

[CLI](#)

[Dépannage](#)

[Débogage du portail captif](#)

[Vidage des identités utilisateur](#)

[Problèmes possibles](#)

[Autorité de certification inconnue du portail captif](#)

[Portail captif « Serveur introuvable »](#)

[Informations connexes](#)

Introduction

Ce document décrit la configuration de Microsoft Azure Entra ID pour une utilisation avec un portail captif (authentification active) sur Cisco Secure Firewall.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

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

Vous devez disposer du niveau tarifaire Standard dans Azure pour la création du hub d'événements. En outre, les périphériques doivent être activés avec Smart Licensing activé avec la fonctionnalité de contrôle des exportations.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

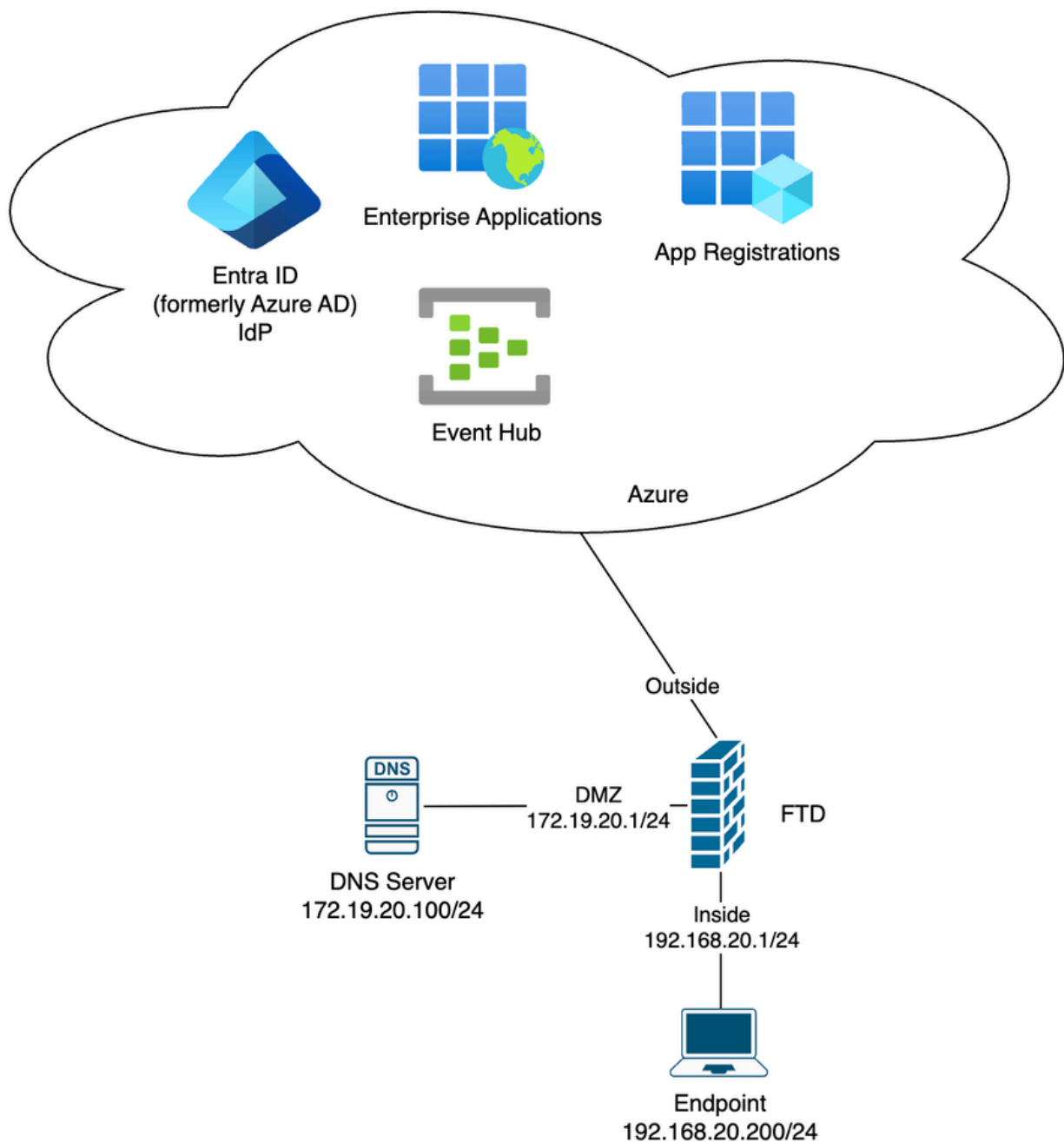
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Alors que les architectures de sécurité IP traditionnelles ont du mal à s'adapter aux environnements de travail hybrides et dynamiques, l'authentification active Cisco Secure Firewall avec intégration SAML offre une solution robuste et axée sur l'identité. En utilisant Microsoft Entra ID (Azure AD) comme fournisseur d'identité centralisé, cette configuration permet aux administrateurs de dépasser les règles réseau statiques et d'appliquer un contrôle d'accès granulaire basé sur l'identité vérifiée de l'utilisateur plutôt que sur des adresses réseau volatiles. Cette intégration rationalise l'expérience utilisateur grâce à l'authentification unique (SSO) transparente et à l'authentification multifacteur (MFA) obligatoire, tout en garantissant une position de sécurité unifiée qui maintient une visibilité et une application des politiques strictes sur un réseau sans périmètre.

Diagramme

Portail captif entre Endpoint, FTD et Azure Entra



Portail Captif Entre EndPoint Et Azure Entra

Configurer

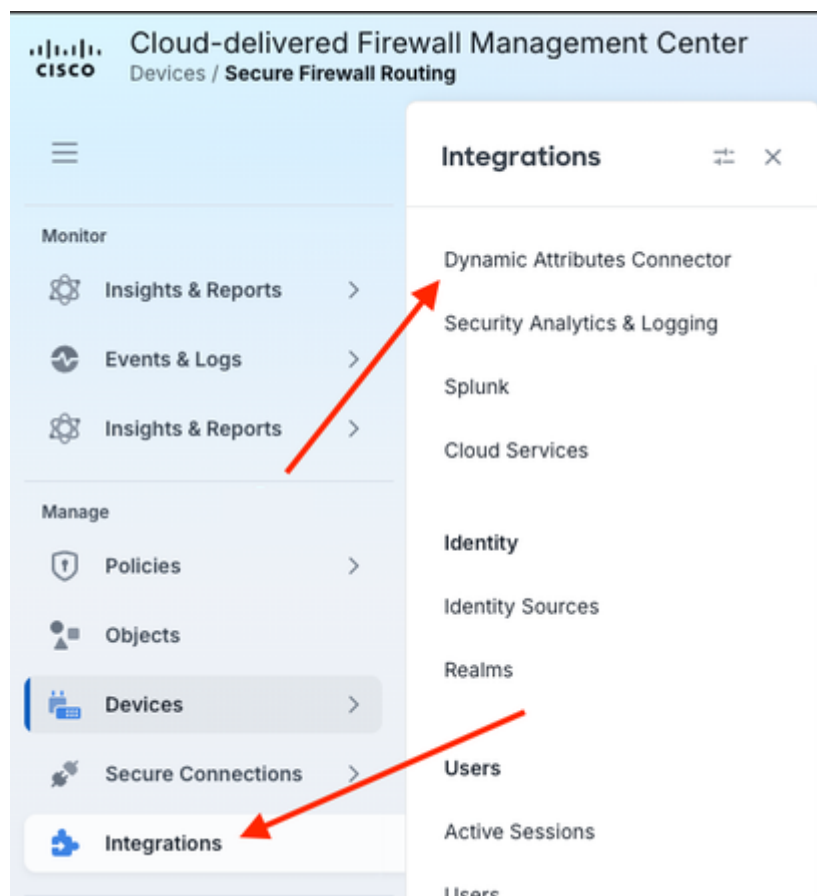
Phase 1 : Configuration initiale de FMC et DNS



Remarque : Ces travaux pratiques utilisent le centre de gestion des pare-feu (cdFMC) fourni dans le cloud ; toutefois, les étapes restent les mêmes pour le FMC sur site.

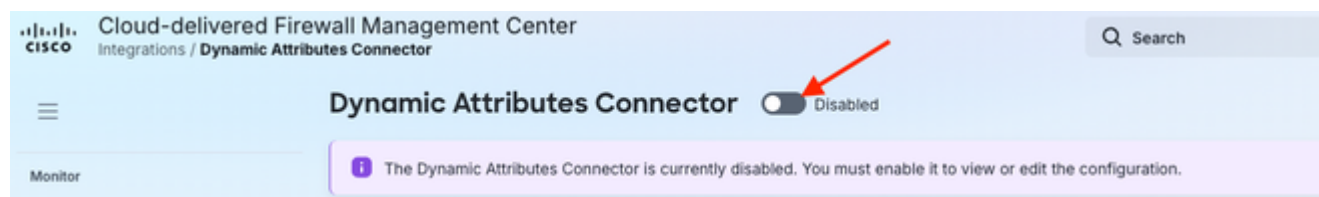
Étape 1: Activer le connecteur d'attributs dynamiques Cisco (CSDAC)

1) Choisissez Integrations > Dynamic Attributes Connector.



Choisir des intégrations Attributs dynamiques Connecteur

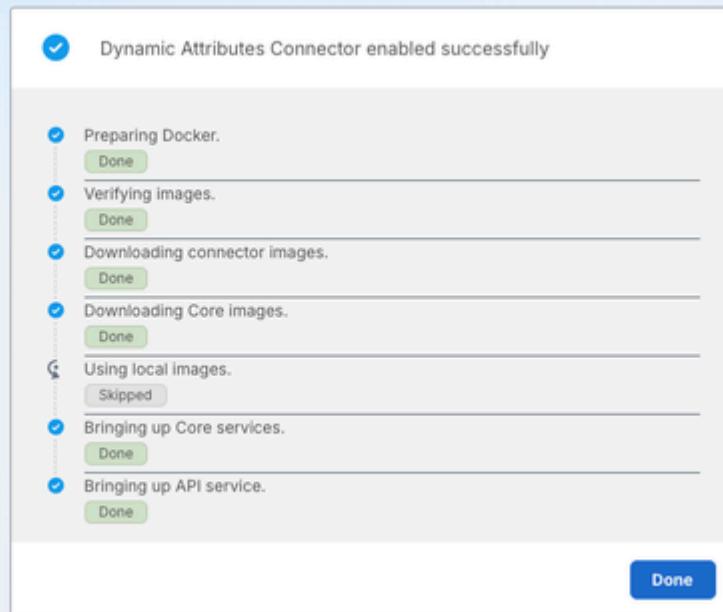
2) Cliquez sur le contrôle adjacent à la chaîne Disabled pour activer CSDAC.



Activer le connecteur d'attributs dynamiques Cisco

c) Cliquez sur Done une fois l'activation CSDAC terminée.

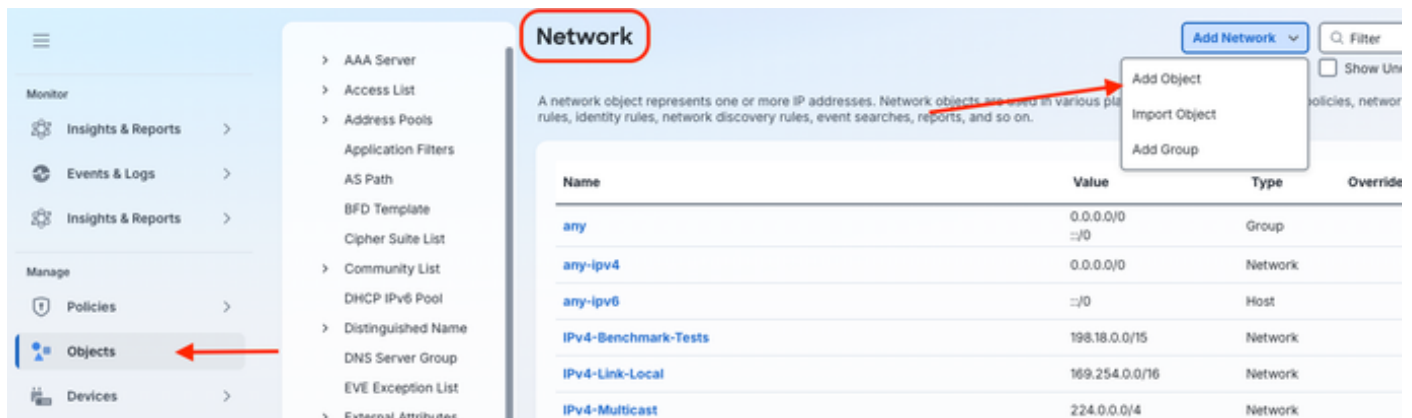
Dynamic Attributes Connector



État du connecteur Activer les attributs dynamiques Cisco

Étape 2: Créer un objet réseau de nom de domaine complet représentatif de l'interface d'entrée FTD

1) Choisissez Objects > Add Network > Add Object.



Créer un nouvel objet réseau de nom de domaine complet

2) Nommez l'objet réseau configuré avec le nom de domaine complet (FQDN). Saisissez le nom de domaine complet et affectez l'objet réseau comme type de nom de domaine complet en cliquant sur la case d'option appropriée. Cliquez sur 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

Configurer les variables d'objet réseau FQDN

Étape 3: Configuration de l'enregistrement DNS A

1) L'exemple présenté ici utilise Windows Server 2025 ; reportez-vous à la documentation du serveur de résolution de noms spécifique, si nécessaire.

	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			



Remarque : Le client qui effectue l'authentification active doit être en mesure de résoudre cet enregistrement DNS A.

Phase 2 : Configuration d'infrastructure à clé publique

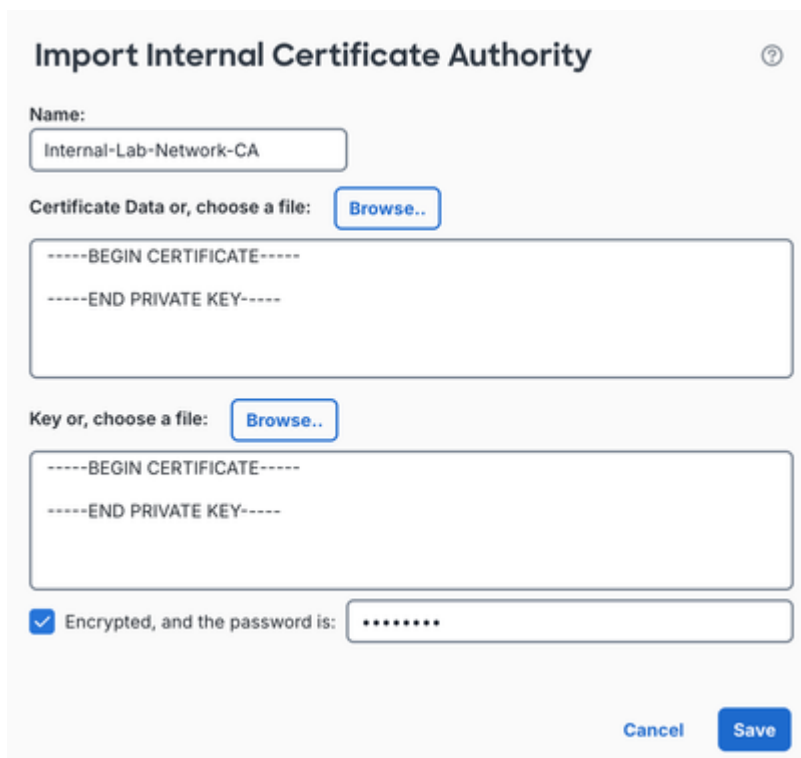
Une autorité de certification (CA) interne peut être utilisée comme infrastructure à clé publique (PKI) pour la configuration d'authentification active. Cisco FMC et FTD exigent que la clé publique d'autorité de certification interne et la clé privée appariée soient téléchargées en tant qu'objet d'autorité de certification interne pour effectuer les opérations d'interception SSL et de déchiffrement-déconnexion nécessaires. En outre, l'autorité de certification interne doit être approuvée dans le navigateur client à partir duquel l'authentification active est effectuée. Reportez-vous à la documentation du navigateur client pour vérifier comment confirmer que le navigateur approuve le certificat.

Étape 1: Importer le certificat CA interne dans le FMC

1) Choisissez Objects > PKI > Internal CAs. Cliquez sur Import CA.



Remarque : L'autorité de certification interne peut également être créée directement sur le FMC.



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](#)

Importer L'Autorité De Certification Interne Vers Le Centre De Gestion Du Pare-Feu



Remarque : Dans le contenu de ce document, un espace blanc apparaît couvrant les différentes valeurs de champ dans les images et est intentionnel par la publication de ce document. Les valeurs réelles sont reflétées pour votre environnement lors de la configuration.

Étape 2: Signer le certificat du fournisseur de services avec l'autorité de certification

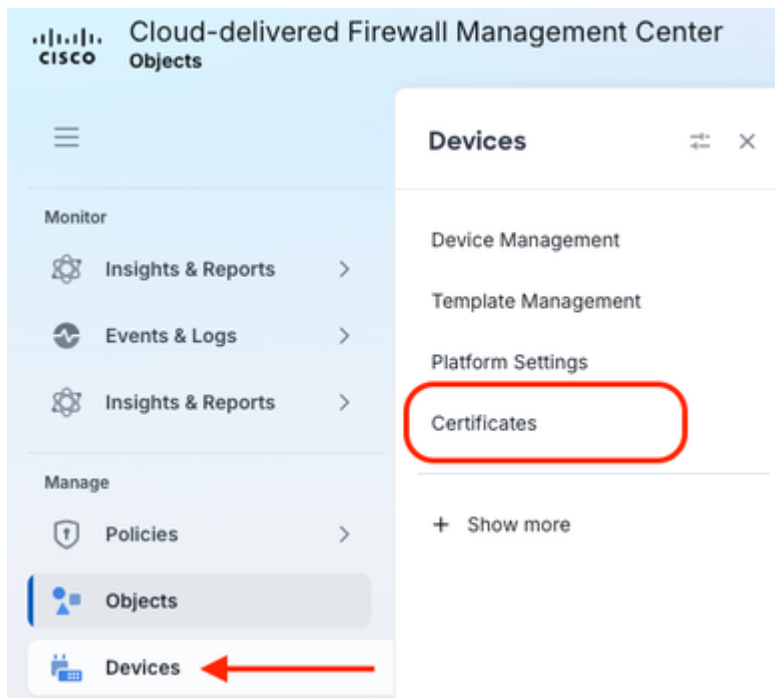
1) Le certificat du fournisseur de services (SP) doit être signé par une autorité de certification (CA) approuvée et renvoyé dans un format PKCS#12 (.p12).



Remarque : Cette CA peut être signée en interne. La seule mise en garde est que l'autorité de certification interne doit être approuvée par le périphérique client.

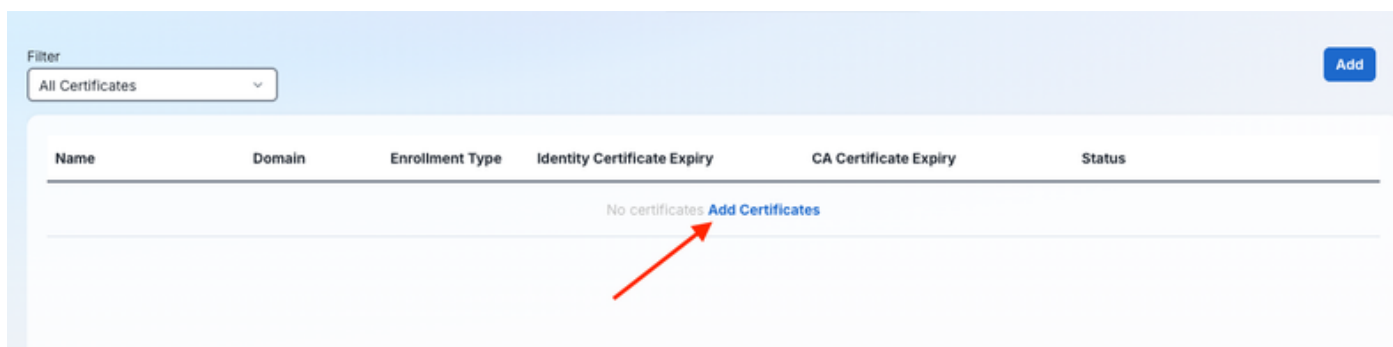
Étape 3: Déployer le certificat SP sur le FTD

1) Choisissez Devices > Certificates.



Accédez À Périphériques Et Certificats

2) Cliquez sur Add Certificates.



Ajouter un nouveau certificat de périphérique

3) Cliquez sur le périphérique dans la liste déroulante qui exécute l'authentification active, puis cliquez sur l'icône + pour créer une nouvelle inscription de certificat.

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

Sélectionner FTD et ajouter une nouvelle inscription de certificat

4) Attribuez un nom à l'inscription de certificat et, dans la liste déroulante Type d'inscription, sélectionnez Fichier PKCS12.

Add Certificate Enrollment ?

Name* FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:* EST

Challenge Password: SCEP

Confirm Password: ACME

Retry Period: Manual

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7...

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

Cancel Save

Paramètres Et Type D'Inscription De Certificat

5) Importez le fichier PKCS#12 en cliquant sur Browse PKCS12 File et en saisissant la phrase de passe requise. Cliquez sur 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

Parcourir et importer un fichier PKCS12

6) Confirmez que les détails de l'inscription sont corrects et cliquez sur 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 +

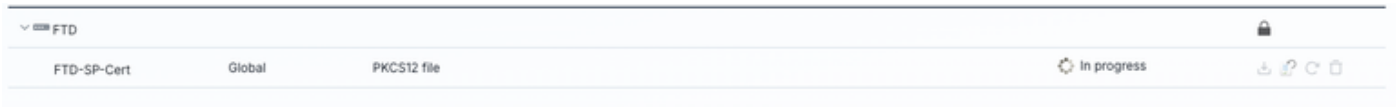
Certificate Enrollment Details:

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

Cancel Add

Confirmer les détails d'inscription de certificat

7) L'importation reflète En cours.



Une fois l'importation terminée, les informations de certificat SP peuvent être validées en cliquant sur l'icône ID du certificat configuré.

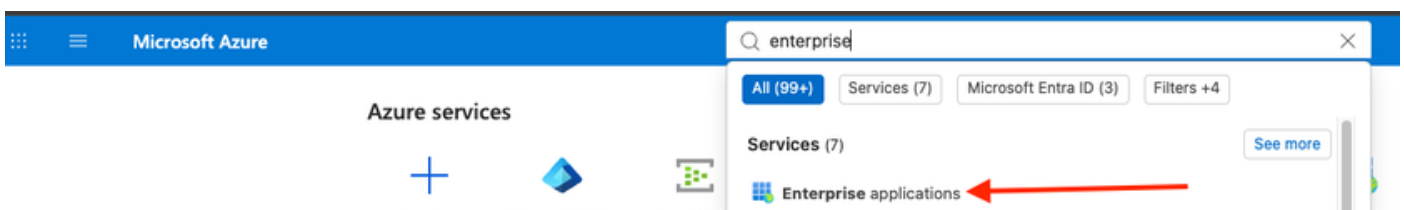


État d'importation de certificat en cours

Phase 3 : Configuration Azure

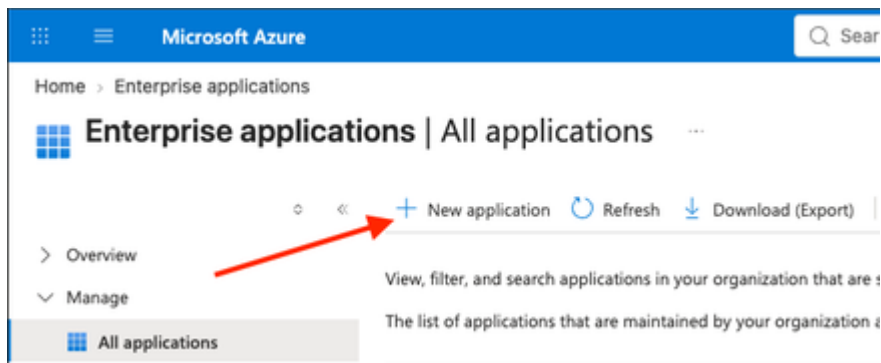
Étape 1: Création de l'application Entreprise Entra pour le kit d'outils SAML

1) Recherchez et cliquez sur Applications d'entreprise.



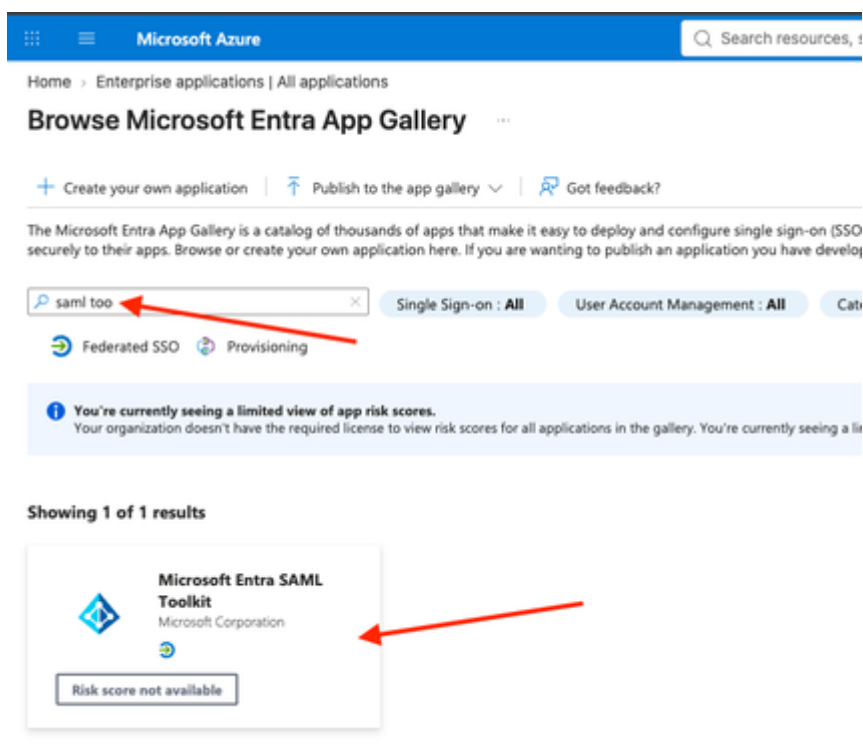
Rechercher Et Accéder Aux Applications D'Entreprise

2) Cliquez sur + Nouvelle application.



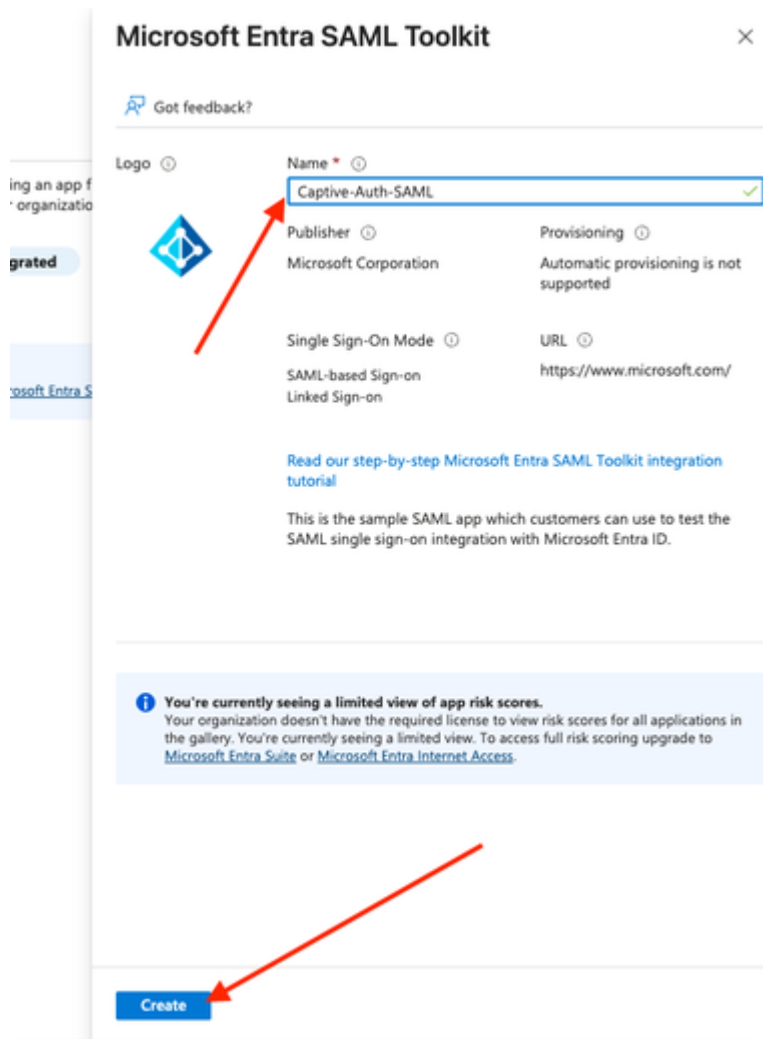
Sélectionner une nouvelle application dans les applications d'entreprise

3) Recherchez le Microsoft Entra SAML Toolkit et cliquez sur la miniature correspondante.



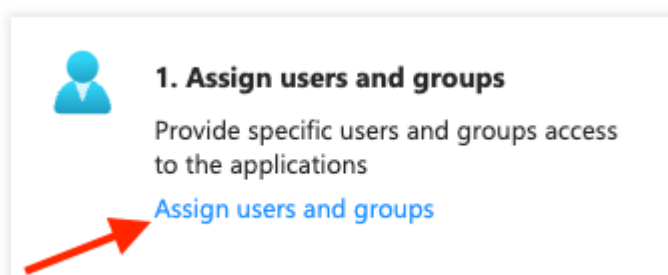
Rechercher et sélectionner Microsoft Entra SAML Toolkit

4) Attribuez un nom à l'application Microsoft Entra SAML Toolkit Enterprise et cliquez sur Créer. (Référence de Microsoft : [Lisez notre didacticiel détaillé sur l'intégration de Microsoft Entra SAML Toolkit](#)).



Attribuer un nom à l'application SAML Toolkit

5) Sur la page Overview, affectez les utilisateurs et groupes spécifiques à l'application d'entreprise SAML Toolkit. Dans cet exemple, le compte de test (captive-portal-user) est membre du groupe active-auth-lab.

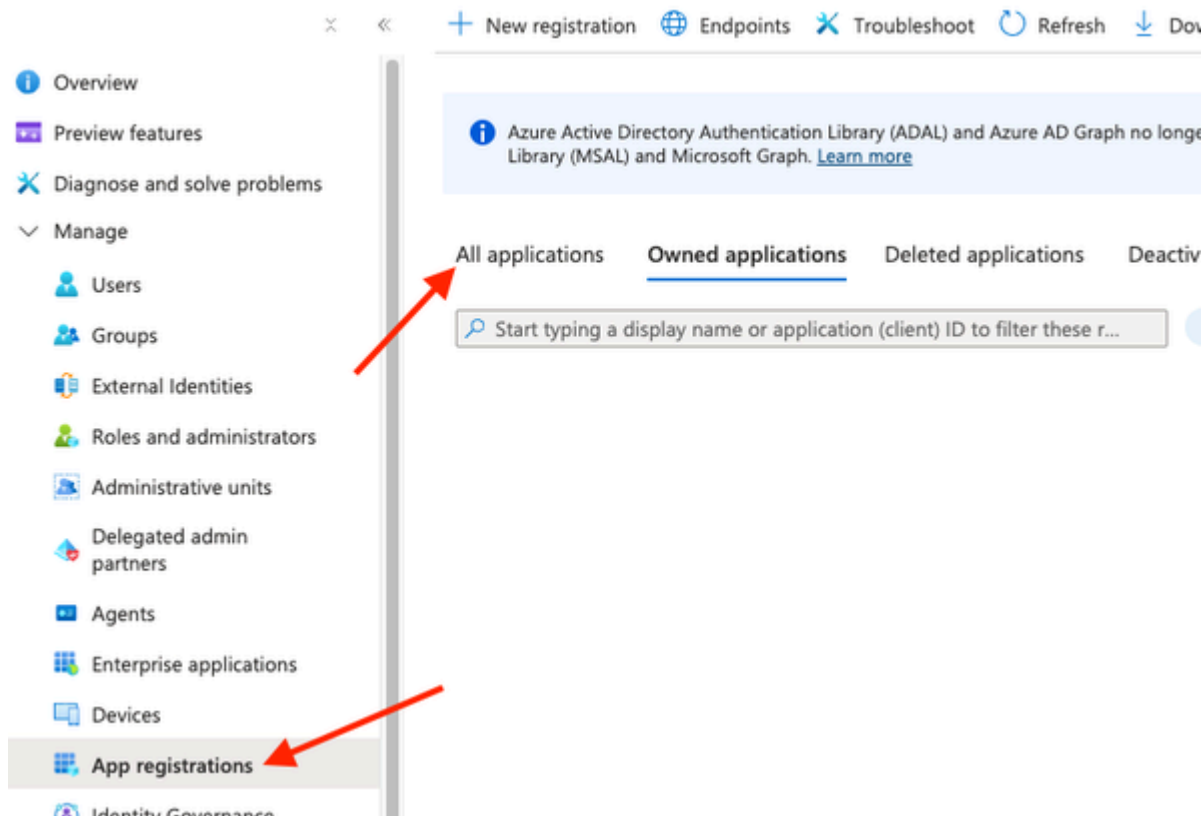


Affecter Des Utilisateurs Et Des Groupes À L'Application

6) La configuration de cette application d'entreprise se poursuit dans les étapes suivantes.

Étape 2: Configurer les inscriptions d'application Entra ID

1) Revenez à Entra ID et dans le menu de navigation de gauche, choisissez App registrations. Cliquez sur le filtre Toutes les applications et recherchez le nom donné à l'application d'entreprise. Cliquez sur l'application appropriée.



Accédez Aux Inscriptions D'Applications Et À Toutes Les Applications

2) Collectez et notez les valeurs Essentiels sous l'enregistrement de l'application d'entreprise.



Important : Passez le curseur sur les valeurs pour afficher Copier dans le Presse-papiers et collecter les valeurs sous Essentiels sur la page Overview :

- Nom d'affichage
- ID d'application (client)
- ID de répertoire (locataire)

Captive-Auth-SAML

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

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

Essentials

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

Application (client) ID :

Object ID :

Directory (tenant) ID :

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

Collecter Les Valeurs D'Affichage, D'Application Et D'ID Répertoire

3) Cliquez sur le lien hypertexte Ajouter un certificat ou un secret.

Captive-Auth-SAML

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

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

Essentials

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

Application (client) ID

Object ID

Directory (tenant) ID

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

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

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

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

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

State : [Activated](#)

Ajouter Un Lien Hypertexte Certificat Ou Secret

4) Cliquez sur + 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.			

Ajouter un nouveau secret client

5) Fournissez une description du secret et ajustez l'expiration si nécessaire. Cliquez sur Ajouter.

Add a client secret

Description:

Expires: Recommended: 180 days (6 months) ▼

Add Cancel

Fournir Une Description Pour Le Secret Client

6) Copiez le secret.



Important : Notez la valeur secrète copiée dans le Presse-papiers.

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

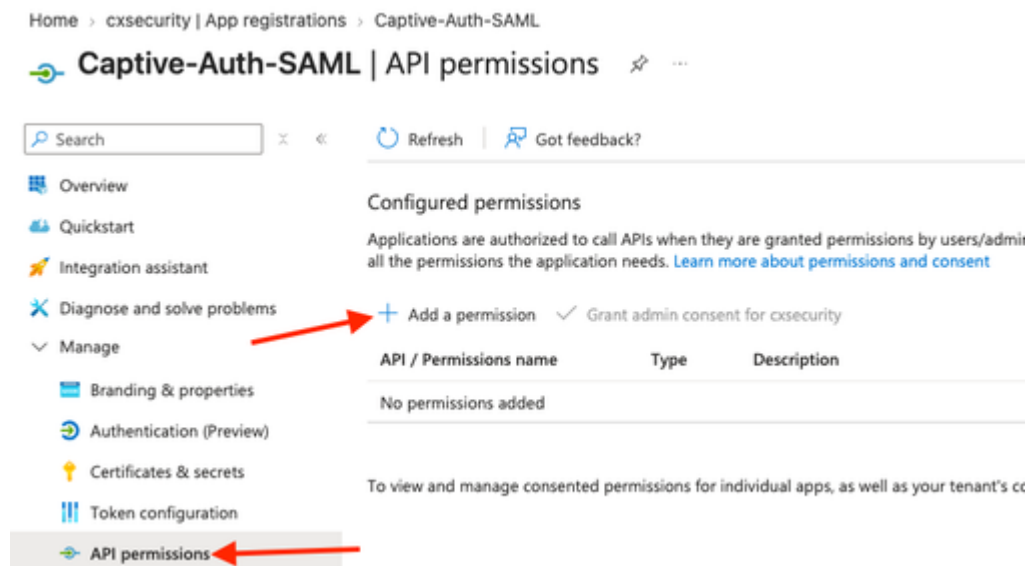
Description	Expires	Value	Secret ID
saml-secret	3/14/2027		

Copier la valeur secrète du client

Étape 3 : configuration des autorisations de l'API Microsoft Graph pour l'enregistrement des

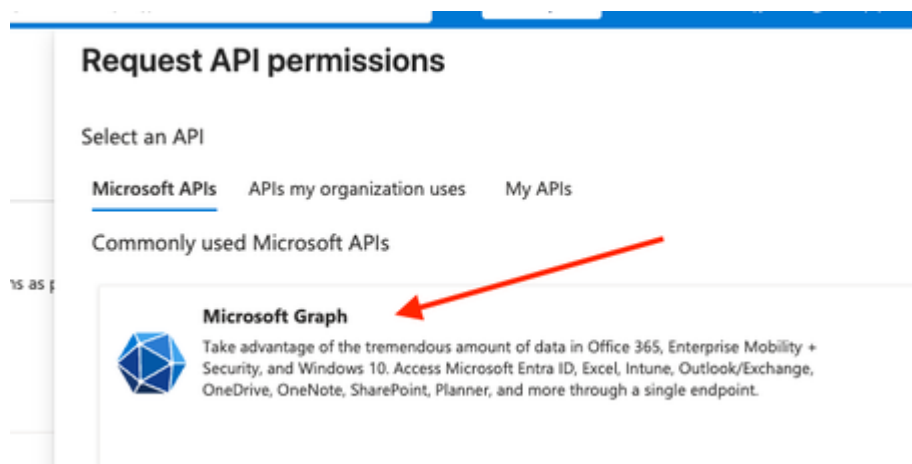
applications

1) Choisissez API Permissions dans le menu de navigation de gauche, puis cliquez sur + Add a permission.



Configurer les autorisations API

2) Cliquez sur Microsoft Graph API.



Sélectionnez l'API Microsoft Graph

3) Octroyer des autorisations d'utilisateur délégué. Lisez, puis cliquez sur Ajouter des autorisations.

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

Accorder des autorisations de lecture aux utilisateurs délégués

4) Accordez à Application User.Read.All les autorisations (cochez la case).

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

Accorder toutes les autorisations de lecture de demande

5) Recherchez et cochez la case Group.Read.All pour accorder également des autorisations de lecture au groupe. Cliquez sur Ajouter des autorisations.

Select permissions

[expand all](#)

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

Enregistrer les autorisations API

6) Confirmez que les autorisations configurées sont alignées et accordez-leur le consentement administratif.

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

Accorder Le Consentement Administratif Pour Les Autorisations

7) Le résultat, une fois le consentement de l'administrateur accordé, est affiché.

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

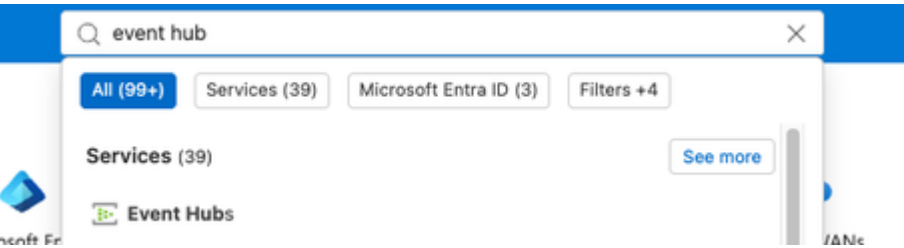
✓ Grant admin consent for

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

Résultat du consentement administratif accordé

Étape 4: Configuration de l'espace de noms Event Hub (EH)

1) Recherchez et cliquez sur Event Hubs.



Configuration du concentrateur d'événements

2) Créez un nouvel espace de noms EH.



No event hubs namespaces to display

An Event Hubs namespace is a management container for event hubs which provides DNS-integrated network endpoints and a range of access control and network integration management.



[Learn more about Event Hubs](#)

Créer un espace de noms Event Hub

3) Configurez l'espace de noms EH.



Remarque : Le niveau de tarification Standard ou supérieur doit être sélectionné. Le niveau de tarification de base empêche l'utilisation du domaine.

Consultez la documentation [Azure Event Hub](#) pour plus d'informations sur les paramètres avancés du hub d'événements et leur applicabilité à des besoins spécifiques.

Cliquez sur Vérifier + Créer.



Create Namespace

Event Hubs

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

Project Details

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

Subscription *

Resource group *

[Create new](#)

Instance Details

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

Namespace name * ☒ .servicebus.windows.net

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

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

Throughput Units *

Enable Auto-Inflate ☐

[Review + create](#)

< Previous

Next: Advanced >

Configuration des paramètres d'espace de noms Event Hub

4) Une fois la validation réussie, cliquez sur Créer.

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 >

Déploiement de l'espace de noms Event Hub

5) Confirmez que le déploiement est terminé, puis cliquez sur Accéder à la ressource.

Home

captive-auth-ad-eh | Overview

Deployment

Search ✕ <<

Delete Cancel Redeploy Download Refresh

Overview

- Inputs
- Outputs
- Template

✓ Your deployment is complete

Deployment name : captive-auth-ad-eh
Subscription :
Resource group :

> Deployment details

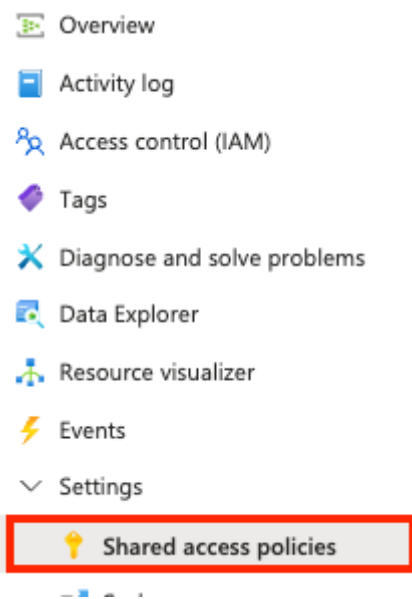
✓ Next steps

Go to resource

Accéder à la ressource Espace de noms Event Hub

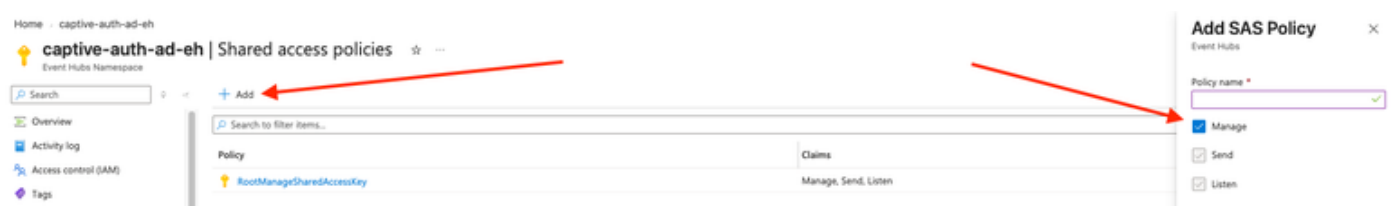
Étape 5: Choisir ou créer des politiques d'accès partagé dans l'espace de noms Event Hub

1) Dans le menu de navigation de gauche, choisissez Settings > Shared access policies.



Accéder Aux Stratégies D'Accès Partagé

2) Cliquez sur + Add et entrez le nouveau nom de stratégie, puis cochez la case Manage. Cliquez sur Create au bas du panneau de menu Add SAS Policy.



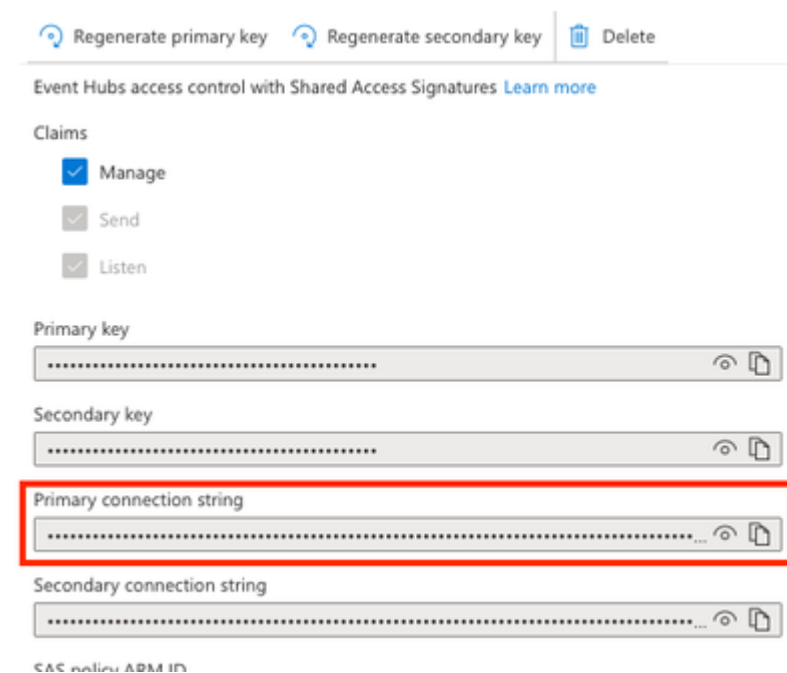
Ajouter une nouvelle stratégie d'accès partagé



Créer une stratégie d'accès partagé

Étape 6: Collecter et noter les informations de signature d'accès partagé (SAS) de l'espace de noms EH

1) Cliquez sur la nouvelle politique d'accès partagé ; la politique EH SAS apparaît dans le panneau latéral de droite.



The screenshot shows the 'Event Hubs access control with Shared Access Signatures' interface. At the top, there are buttons for 'Regenerate primary key', 'Regenerate secondary key', and 'Delete'. Below this is a link to 'Learn more'. The 'Claims' section has three checkboxes: 'Manage' (checked), 'Send', and 'Listen'. The 'Primary key' and 'Secondary key' fields are shown with masked text and icons to toggle visibility or copy. The 'Primary connection string' field is highlighted with a red box, showing masked text and similar icons. The 'Secondary connection string' field is also visible below it. At the bottom left, the text 'SAS policy ABM ID:' is partially visible.

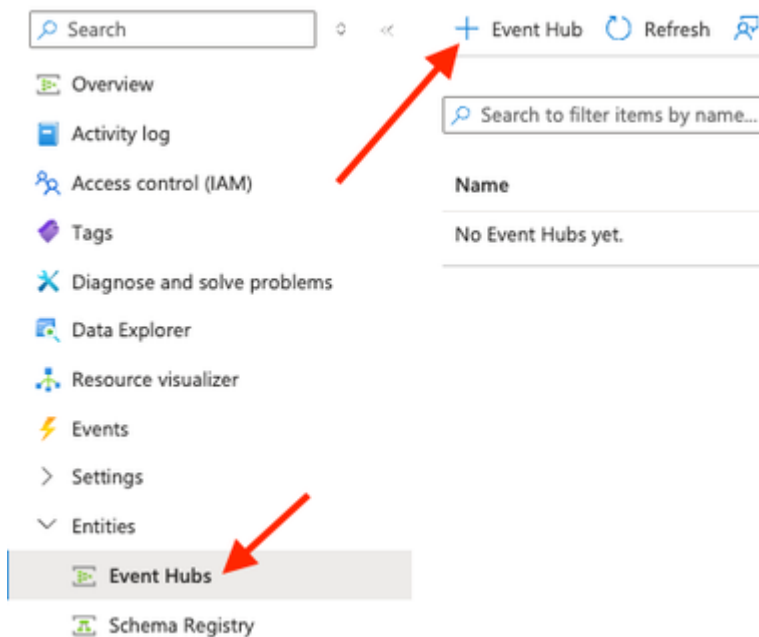
Copier la chaîne de connexion principale



Important : Copiez et notez la chaîne de connexion principale.

Étape 7: Création d'une instance Event Hub dans l'espace de noms Event Hub

1) Dans le menu Namespace, choisissez Entities > Event Hubs. Cliquez sur + Event Hub pour créer une nouvelle instance EH.



Créer une nouvelle instance Event Hub

2) Attribuez un nom à la nouvelle instance EH, puis cliquez sur Vérifier + créer.

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 >

Attribuer un nom à l'instance Event Hub

3) Une fois la validation réussie, cliquez sur Create pour provisionner l'instance Event Hub.

Create Event Hub ...

Event Hubs

✓ Validation succeeded.

Basics Capture Review + create

Event Hubs Instance
by Microsoft

Basics

Name	captive-auth-ad-eh-1
Partition count	1

Retention

Cleanup policy	Delete
Retention time (hrs)	1

Capture

Capture Status	Off
----------------	-----

Create < Previous Next >

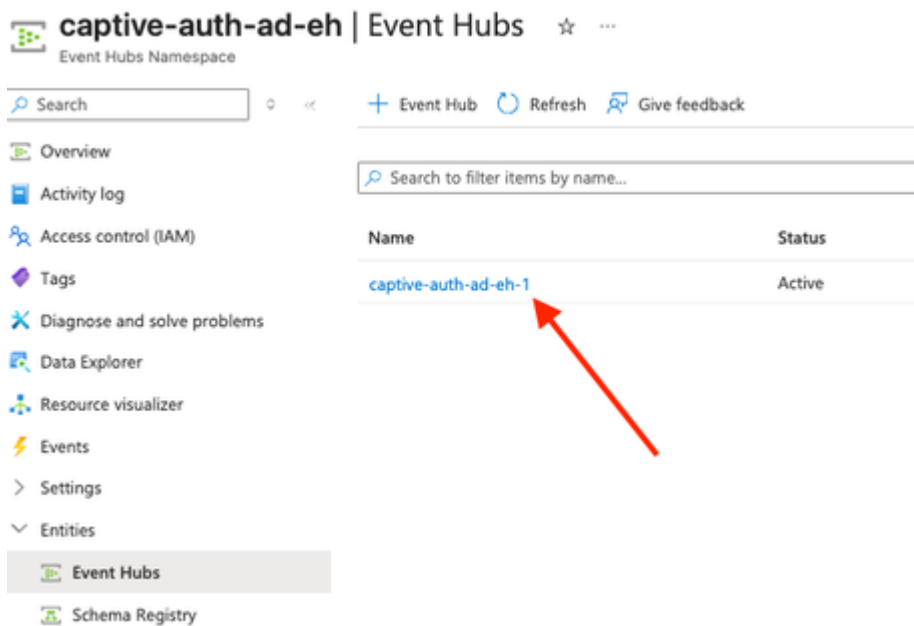
Provisionner l'instance Event Hub



Important : Copiez et notez le nom de l'instance Event Hub.

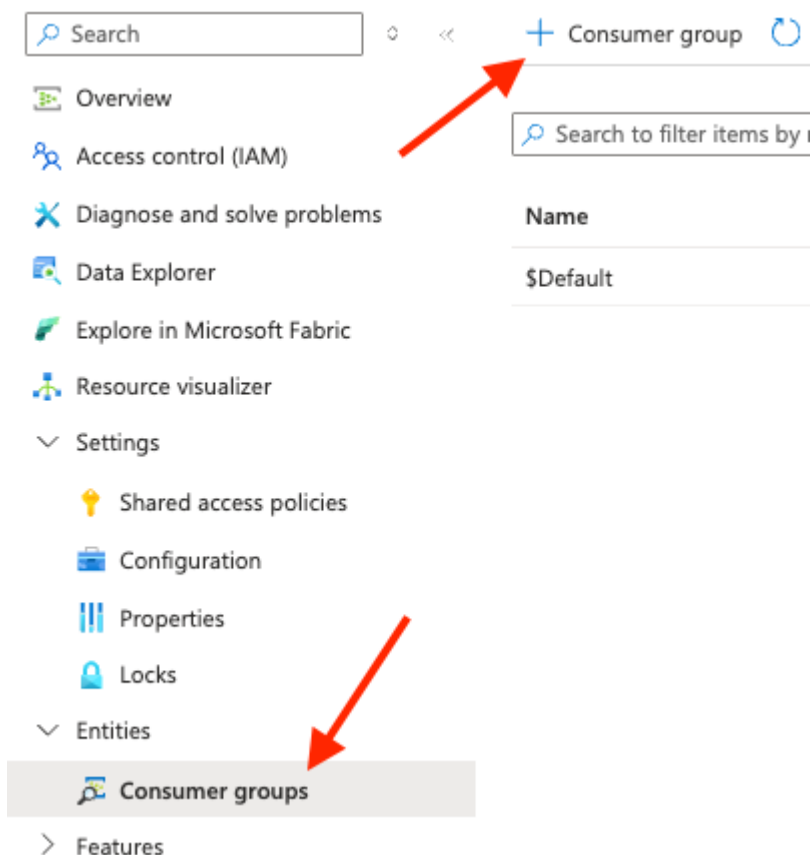
Étape 8: Créer un groupe de consommateurs d'instances Event Hub dans l'espace de noms Event Hub

1) Cliquez sur la nouvelle instance EH configurée à l'étape précédente.



Configuration de l'instance du concentrateur d'événements Access

2) Dans l'instance EH, choisissez Entités > Groupes de consommateurs, puis créez un nouveau groupe de consommateurs.



Créer un groupe de consommateurs

3) Nommez le groupe de consommateurs et cliquez sur Créer.

Create consumer group ×

Consumer groups

Name *

captive-auth-ad-eh-cg



Create

Attribuer un nom au groupe de consommateurs



Important : Copiez et notez le nom du groupe de consommateurs de l'instance Event Hub.

Étape 9: Vérifier les valeurs collectées

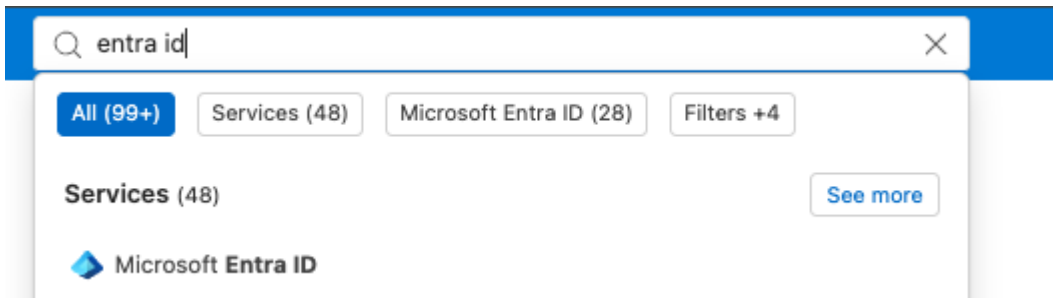
1) A ce stade, ces valeurs des étapes précédentes sont à noter. Si aucune valeur n'a été enregistrée, veuillez indiquer l'étape applicable où elle est collectée :

- Phase 3 Étape 2 - Enregistrement de l'application (de l'application d'entreprise créée pour ce processus, référencée par le nom d'affichage collecté)
 - Étape 2, sous-étape 2
 - Nom d'affichage
 - ID d'application (client)
 - ID du répertoire (locataire)
 - Étape 2, sous-étape 6
 - Secret client
- Phase 3 Étape 6 - Event Hub
 - Étape 6, sous-étape 1
 - Espace de noms EH
 - Chaîne de connexion principale

- Étape 7, sous-étape 3
 - Nom de l'instance EH (Event Hub)
- Étape 8, sous-étape 3
 - Nom du groupe de consommateurs EH

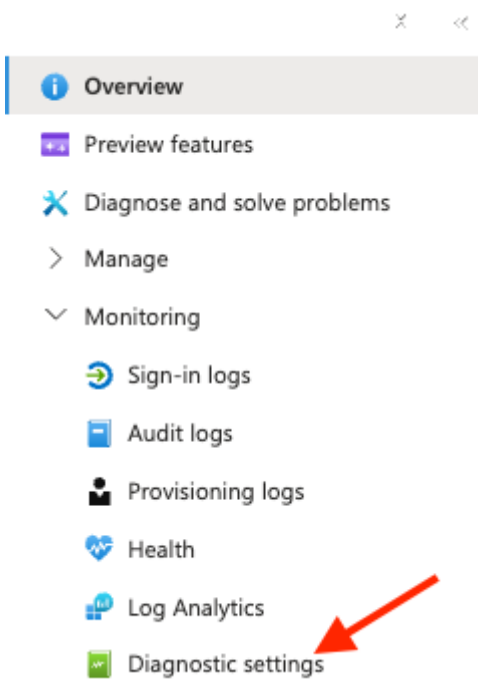
Étape 10: Configuration de la diffusion en continu du journal d'audit Entra ID vers Event Hub

1) Revenez à la configuration du client Entra ID.



Rechercher Et Accéder À La Configuration De L'ID Client

2) Dans le menu de gauche, choisissez Monitoring > Diagnostic Settings.



Surveillance des paramètres de diagnostic

3) Choisissez Diagnostic settings > General et cliquez sur + Add diagnostic setting.

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

Ajouter un nouveau paramètre de diagnostic

4) Attribuez le nom requis au paramètre de diagnostic, cochez la case AuditLogs pour consigner et la case Stream to an event hub. Référez-vous aux valeurs notées dans les configurations précédentes et cliquez sur Save lorsque vous avez terminé.

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

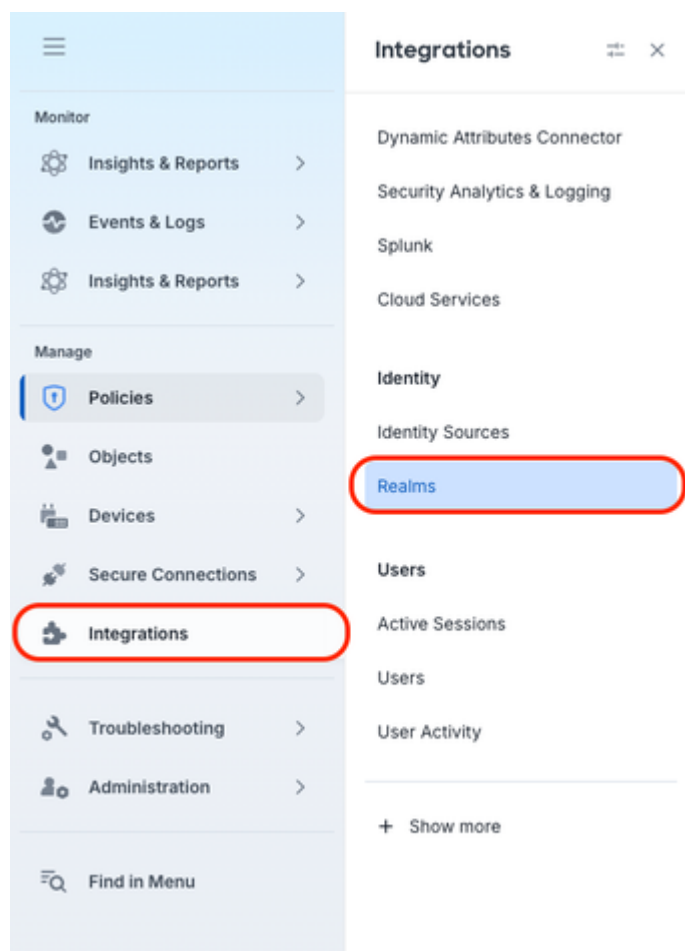
Event hub policy name

- ☐ Send to partner solution

Phase 4 : Consolider la configuration d'authentification active Azure et FMC/FTD

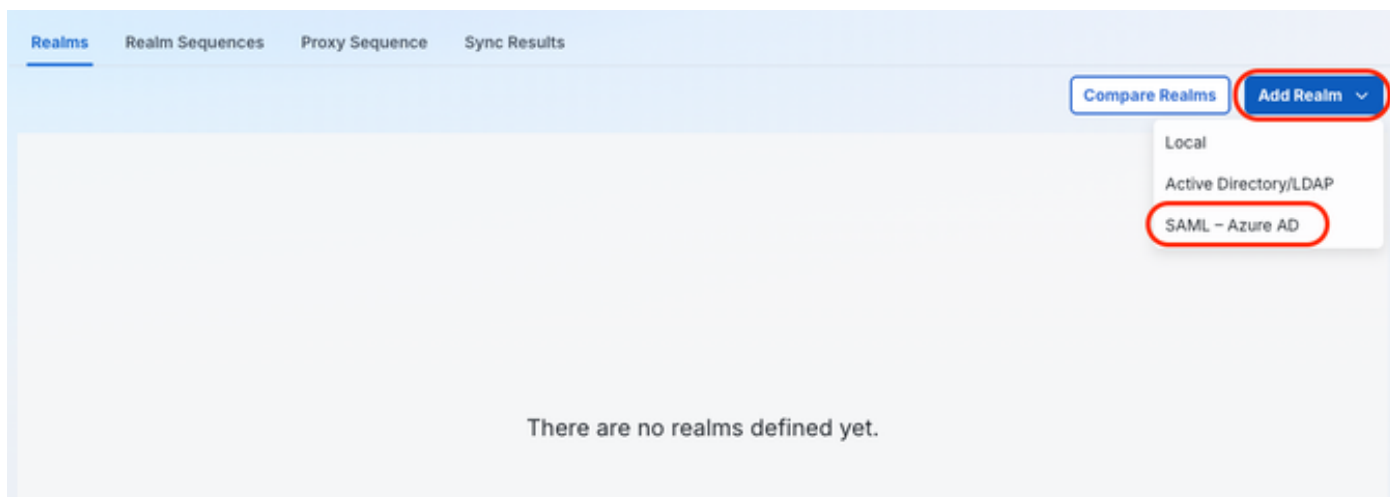
Étape 1: Configurer le domaine Azure SAML/Entra ID à l'aide de l'Assistant FMC

1) Dans FMC, choisissez Integrations > Identity > Realms.



Configuration des domaines d'identité

2) Cliquez sur la liste déroulante Ajouter un domaine, et choisissez SAML - Azure AD.



Ajouter un domaine SAML Azure AD

3) Attribuez un nom et une description au domaine Azure pour décrire son utilisation et assurez-vous que l'option S'authentifier passivement avec Azure AD ou utiliser un portail captif avec Azure AD est sélectionnée dans la liste déroulante Type de configuration. Cliquez sur Suivant.

Add SAML - Azure AD Realm

1 Realm Details

Name *
azure-entra-saml

Description
Active Authentication IdP

Identity Provider *
Azure AD

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

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

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

4 Azure AD Details

Next

Configurer les paramètres du domaine Azure AD

4) Sélectionnez l'objet FQDN précédemment configuré comme URL de base. Entrez l'ID d'entité avec le format de chaîne affiché :

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

- Lorsque le suffixe ID d'entité SAML est configuré (souligné en vert dans l'exemple de configuration suivant), assurez-vous que le suffixe est unique parmi les autres implémentations SSO de l'environnement. Cette valeur doit également correspondre à la configuration Azure SAML. L'URL de base reste la même dans toute la configuration.
- L'URL ACS (Assertion Consumer Services) est renseignée automatiquement et est immuable.
- Sélectionnez le certificat de fournisseur de services (SP) inscrit aux étapes précédentes du workflow dans FMC sous Périphériques > Certificats.
- Une fois ces valeurs entrées, cliquez sur Download Service Provider Metadata pour faciliter le processus de configuration et confirmer que les valeurs attendues sont écrites dans 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?tgname=azure-entra 📋

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

Service Provider Certificate *

FTD-SP-Cert ⓧ +

Certificate used for SAML authentication and TLS/SSL communication with the secure threat defense device. The certificate must have the value you specify for Base URL that must match the Common Name (CN) or Subject Alternative Name (SAN). The certificate, which must be in PKCS12 format, must be trusted by clients.

Download Service Provider Metadata

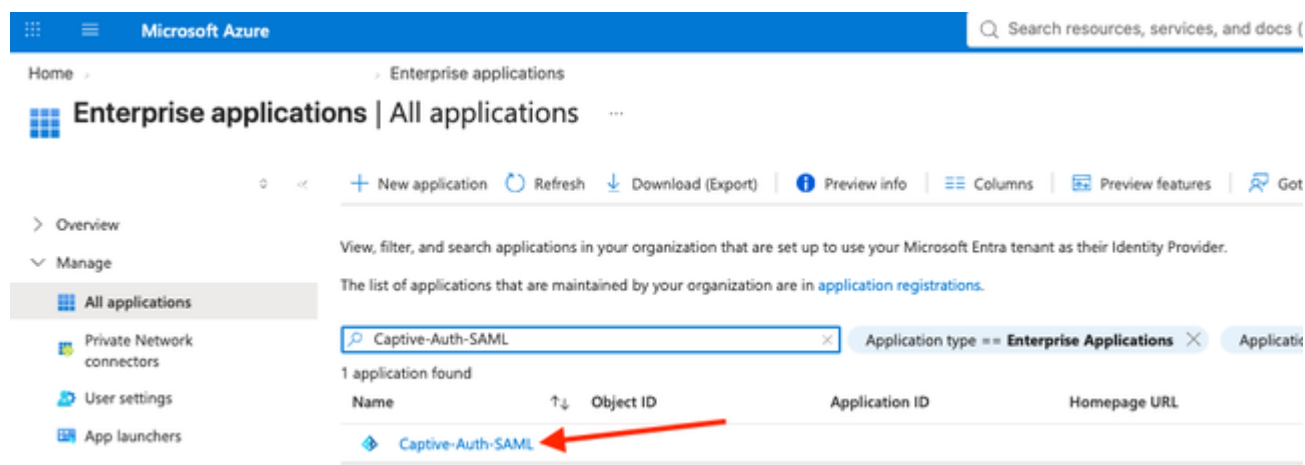
Next

Configurer l'URL de base et l'ID d'entité et télécharger les métadonnées SAML

5) Cliquez sur Next pour passer à la séquence 3 de la configuration du domaine.

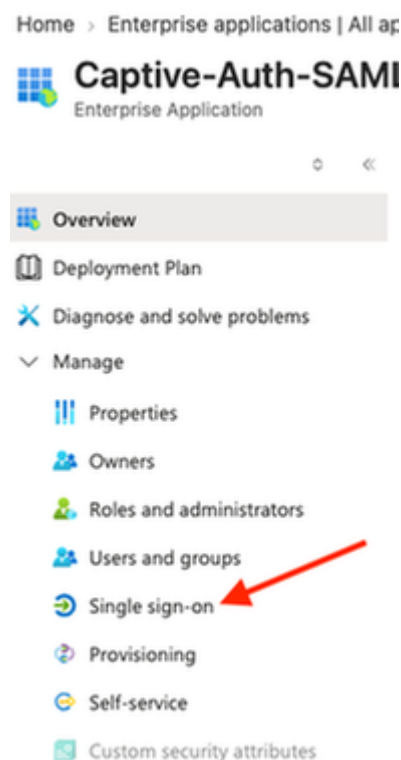
Étape 2: Implémenter les métadonnées SAML SP configurées par FMC dans l'application Azure Enterprise

1) Revenez à Azure et choisissez Entra ID > Manage > Enterprise Applications. Recherchez l'instance précédemment créée de l'application d'entreprise Microsoft Entra SAML Toolkit.



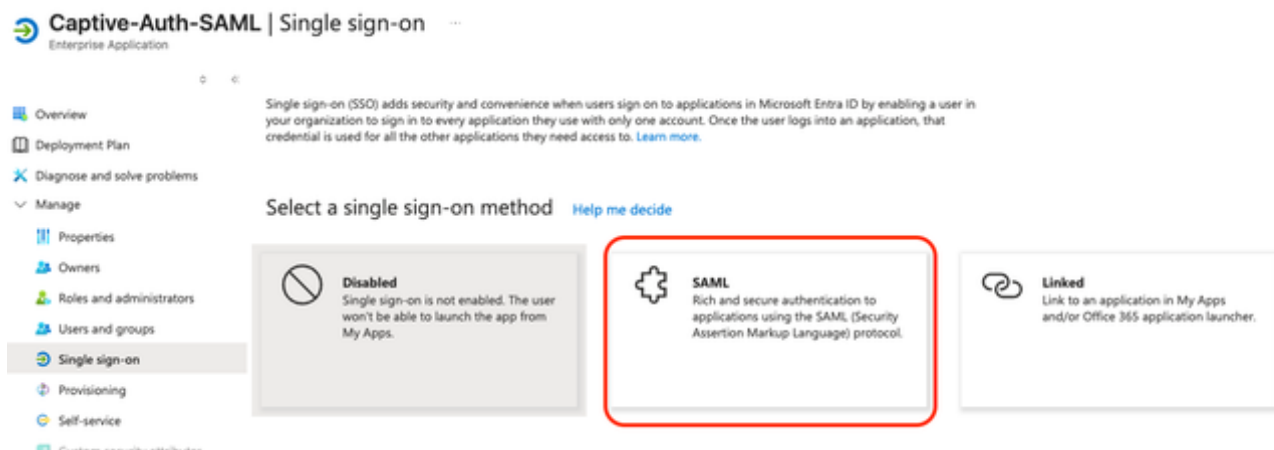
Localiser l'application Microsoft Entra SAML Toolkit

2) Dans le menu de navigation latérale, sélectionnez Manage > Single Sign-On.



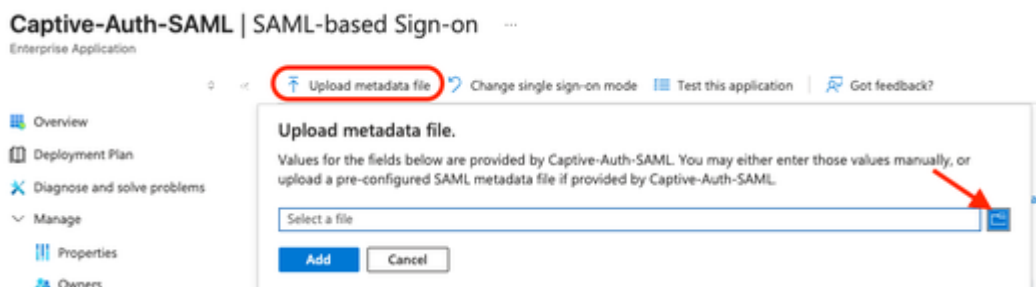
Gérer la configuration SSO

3) Cliquez sur le mode SSO (Single Sign-On) SAML.



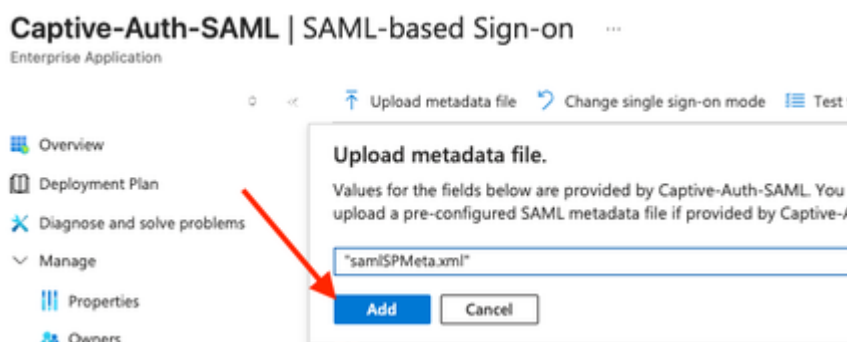
Sélection du mode d'authentification unique SAML

4) Cliquez sur Upload metadata file et cliquez sur l'icône de dossier bleue pour parcourir votre système de fichiers local et rechercher le fichier de métadonnées SAML téléchargé depuis FMC.



Télécharger un fichier de métadonnées depuis Firewall Management Center

5) Une fois le téléchargement terminé, cliquez sur Add.



Ajouter une application de configuration SAML

6) Le panneau latéral de la configuration SAML de base s'affiche et des valeurs telles que l'identificateur (ID d'entité) et l'URL ACS sont extraites du fichier XML de métadonnées SP généré par FMC et téléchargées et appliquées automatiquement. Cependant, l'URL de connexion n'est

pas renseignée et est requise avant l'enregistrement.

Save

Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

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

✓

✓

ⓘ

🗑

Add identifier

Patterns: https://samltoolkit.azurewebsites.net

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default

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

✓

0

✓

✓

ⓘ

🗑

Add reply URL

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

Enter a sign on URL

Patterns: https://samltoolkit.azurewebsites.net/

✗ Please enter a valid URL starting with "https://". If your URL has query parameters, ensure that there is a slash preceding the question mark (i.e. /?)

✗ This field is required

Relay State (Optional)

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

Enter a relay state

Logout Url (Optional)

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

Enter a logout url

✓

Extraction de la configuration SAML de base

7) Utilisez le modèle d'URL de connexion fourni, copiez et collez la valeur, puis cliquez sur Save en haut lorsque vous avez terminé.

Basic SAML Configuration



Save



Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

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



[Add identifier](#)

Patterns: https://samltoolkit.azurewebsites.net

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default

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

0



[Add reply URL](#)

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

https://samltoolkit.azurewebsites.net/ ✓

Patterns: https://samltoolkit.azurewebsites.net/

Relay State (Optional) ⓘ

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

Enter a relay state

Logout Url (Optional)

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

Enter a logout url ✓

Faites défiler jusqu'à Certificats SAML, et exportez le fichier XML de métadonnées de fédération généré par Azure pour l'importer dans Cisco Secure FMC.

SAML Certificates

Token signing certificate

Status: Active [Edit](#)

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)

Federation Metadata XML [Download](#)

Verification certificates (optional) [Edit](#)

Required: No

Active: 0

Expired: 0

Exporter le fichier XML des métadonnées de fédération

Étape 3: Configurer le domaine Azure SAML/Entra ID à l'aide de l'Assistant FMC (suite)

1) Revenez au FMC. Sous Sequence 3, Métadonnées du fournisseur d'identité SAML (IdP), téléchargez le fichier XML de métadonnées de fédération exporté téléchargé depuis Azure vers le FMC pour remplir automatiquement les valeurs nécessaires.

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 *

Select... [+](#)

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.

Télécharger le fichier XML de métadonnées de fédération

2) Une fois téléchargées, les valeurs sont renseignées comme indiqué.

3 SAML Identity Provider (IdP) Metadata

Entity ID *

Unique, alphanumeric identifier for a SAML entity.

Single Sign-On (SSO) URL *

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

IdP Certificate *



Choose a certificate from the list or upload a new certificate in manual format.

 Click to upload or drag and drop a file.

[Upload XML](#)

Federation XML you downloaded from Azure AD. If you upload this, you don't have to enter the other values in this section.

[Next](#)

Valeurs du fournisseur d'identité SAML renseignées automatiquement



Remarque : Une sortie partielle est affichée dans l'image.

3) Entrez les valeurs collectées tout au long du processus de mise en oeuvre jusqu'à ce point :

- Enregistrement des applications
 - ID d'application (client)
 - Secret client
 - ID de répertoire (locataire)
- Event Hub
 - Espace de noms EH Hostname
 - Espace de noms EH Chaîne de connexion principale
 - Nom de l'instance EH (Event Hub)
 - Nom du groupe de consommateurs EH

Add SAML – Azure AD Realm



4 Azure AD Details

Client ID *
851607f9-969f-4fed-90ec-829607c1c
Application ID (also referred to as client ID you created in Azure AD).

Client Secret *
.....
Secret string that the application uses to prove its identity when requesting a token.

Tenant ID *
af42bac0-52aa-429f-92db-9258199f
Microsoft Entry ID entity that typically encompasses an organization. Displayed in Azure Entra ID → Properties.

Event Hubs Host Name *
captive-auth-ad-eh.servicebus.windows.net
Hostname of the Event Hub Namespace. Displayed in Event Hubs → Event Hubs Namespace.

Event Hub Name *
captive-auth-ad-eh
Name of your event hub. Displayed in Event Hubs Name Space → Overview.

Consumer Group Name *
captive-auth-ad-eh-cg
A view of an entire event hub. Consumer groups enable consuming applications to each have a separate view of the event stream.

Event Hub Connection String *
Endpoint=sb://captive-auth-ad-eh.servicebus.windows.net/;SharedAccessKeyName=...
Event Hub Connection String: Unique identifier for the event hub (also referred to as topic or endpoint). It is displayed on the Azure AD portal in Event Hubs → (name of your event hub) → Shared access policies → (name of policy).

USER GROUPS ☒
☐ Excluded User Groups
☒ Included User Groups
Enter each group name on a separate line
active-auth-lab
Enter one or more groups from which to download users for identity control. Users in these groups will be available for use in access control policies.

Test

Test connection succeeded

Next

Saisir Les Informations Application Et Event Hub

Une fois entré, cliquez sur Test pour vérifier la connexion et confirmer qu'Azure est accessible avec les informations fournies.



Remarque : Le cas échéant, assurez-vous que les groupes d'utilisateurs exclus/inclus correspondent à votre configuration d'entrée

4) La dernière étape de l'assistant vous permet de configurer le délai d'expiration SAML Captive Portal Users. La valeur par défaut est 1 440 minutes.

5 User Session Timeout

SAML Captive Portal Users

Minutes Range 0-35791394

Configuration du délai du portail captif

5) Cliquez sur Next pour continuer.

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**

Avancer avec la configuration du domaine Azure AD

6) L'assistant fournit un résumé de la configuration implémentée. Cliquez sur Enregistrer à la fin du résumé une fois que les valeurs entrées ont été validées et confirmées.

5 User Session Timeout Edit

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

 **Cancel** **Save**

Bouton Enregistrer le résumé de la configuration du domaine

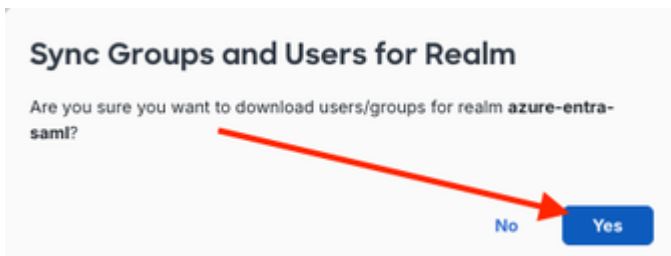
Étape 4: Vérifier les utilisateurs téléchargés

1) Vérifiez que les utilisateurs peuvent être téléchargés à partir d'Azure Entra à l'aide du bouton Télécharger maintenant dans le workflow Intégrations > Identité > Domaines.

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

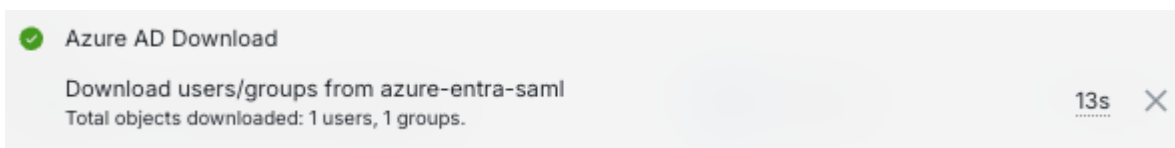
Télécharger des utilisateurs à partir d'Azure AD

2) Cliquez sur Yes en réponse à l'invite de dialogue.



Confirmer le téléchargement des utilisateurs à partir d'Azure AD

3) La tâche de téléchargement génère 1 utilisateur et 1 groupe téléchargés, comme le confirme la section Notifications > Tâches.

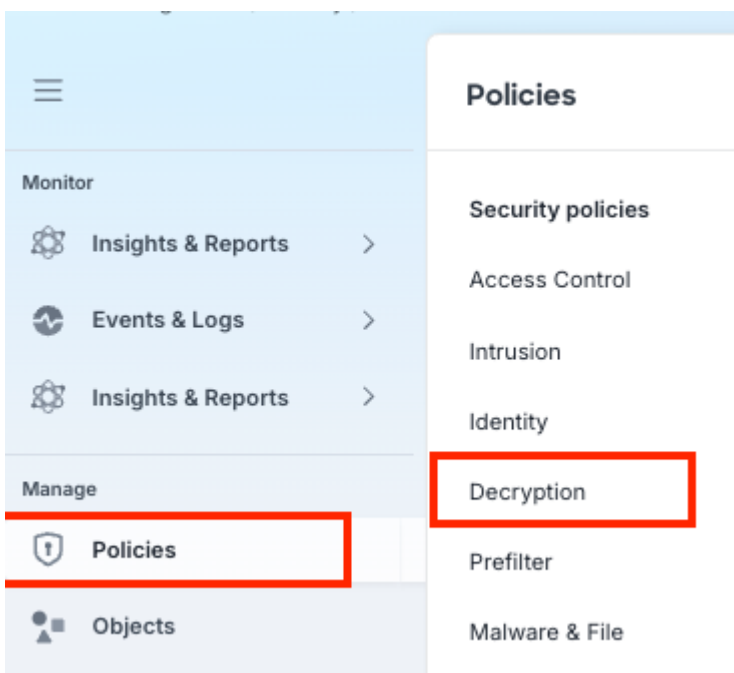


Entrée de notification pour le téléchargement d'utilisateurs à partir d'Azure AD

Phase 5 : Configuration des stratégies dans le FMC

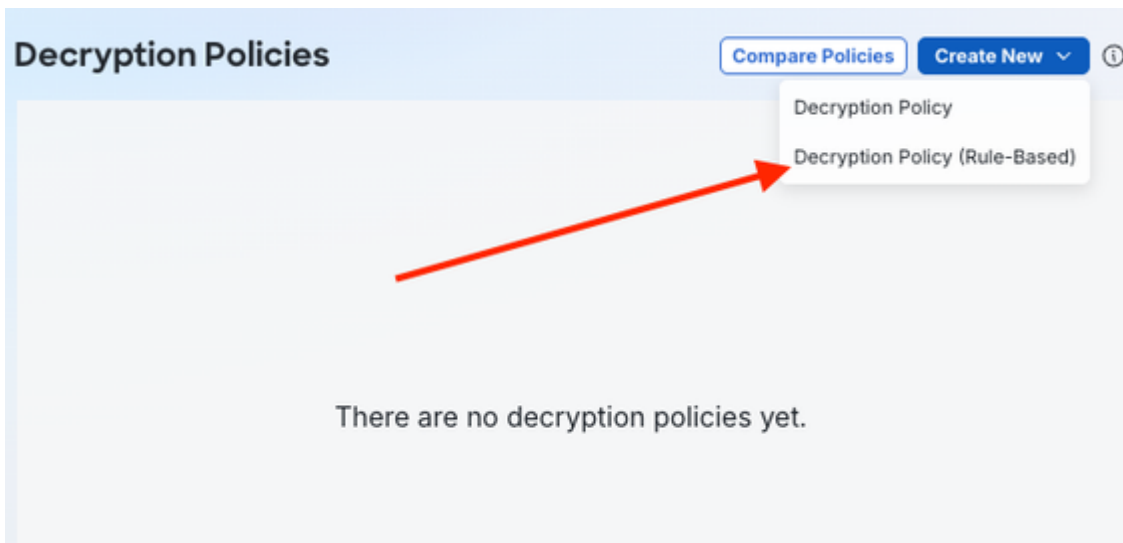
Étape 1: Configurer la stratégie de déchiffrement

1) Dans le FMC, choisissez Policies > Security Policies > Decryption.



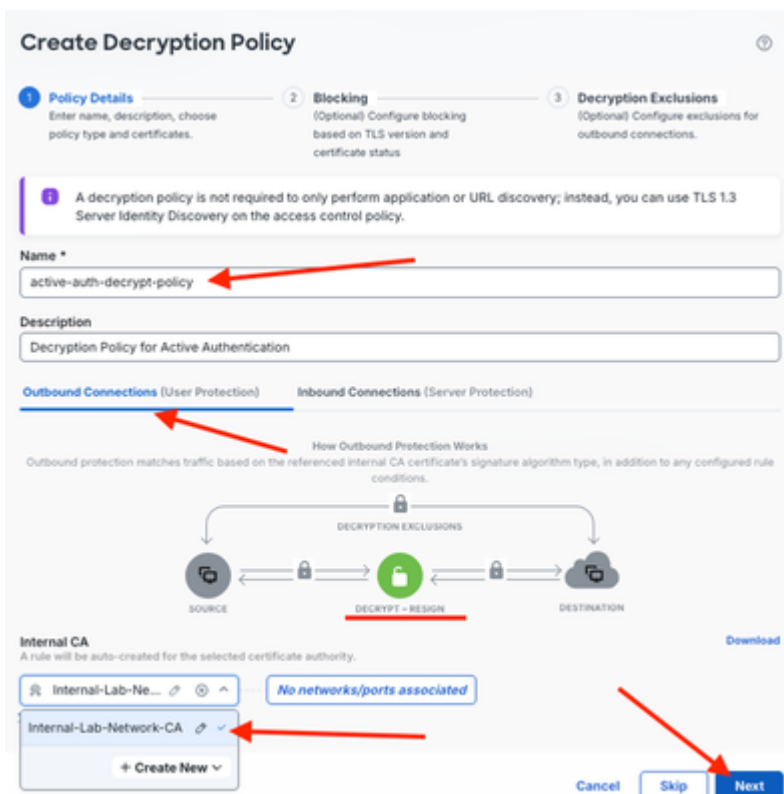
Accéder À La Stratégie De Décryptage

2) Cliquez sur la liste déroulante Create New et choisissez Decryption Policy (Rule-Based).



Créer une nouvelle stratégie de décodage basée sur des règles

3) Attribuez un nom et, si vous le souhaitez, une description à la nouvelle stratégie de décodage basée sur des règles, puis cliquez sur l'option de l'onglet Connexions sortantes (Protection de l'utilisateur) pour implémenter la fonctionnalité de décodage-résignation requise pour l'authentification du portail captif (Authentication active).



Implémenter les détails de stratégie de connexions sortantes

4) Choisissez l'autorité de certification interne précédemment appliquée dans la liste déroulante

correspondante de la même boîte de dialogue. Cliquez sur Suivant.

5) Personnalisez les options selon vos besoins.

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](#)

Personnaliser les options de stratégie de décodage

6) Dans cet exemple, les valeurs par défaut sont utilisées à l'exception des détails de stratégie requis. Terminez l'assistant de configuration en cliquant sur Create Policy.

Create Decryption Policy

1 Policy Details

2 Blocking

3 Decryption Exclusions

Enter name, description, choose policy type and certificates.

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

(Optional) Configure exclusions for outbound connections.

Decryption Exclusions

☐ Bypass decryption for sensitive URL categories

In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Customize the list below to bypass inspection for designated categories.

Note: URL License is Required

URL Categories: Finance Online Trading Health and Medicine [+ Add](#)

☒ Bypass decryption for undecryptable distinguished names

Bypass decryption based on Cisco's list of known undecryptable distinguished names.

Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported distinguished names.

[56 Distinguished names included](#)

☒ Bypass decryption for undecryptable applications

Certain applications are not supported for decryption due to a variety of reasons (certificate pinning, client certificate authentication, and so on). This option bypasses decryption based on Cisco's list of known undecryptable applications.

Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported applications.

[59 Applications included](#)

Intelligent Decryption Bypass

☐ Bypass decryption for very low-risk connections

Bypass decryption for very low-risk clients connecting to trusted servers.

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

[New](#)

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

Créer une politique de déchiffrement final

Étape 2: Configurer les règles de stratégie de déchiffrement

1) La disposition par défaut d'une politique de décodage basée sur des règles est indiquée ici. Le trafic qui ne correspond pas aux règles activées par défaut, telles que la règle 3 (qui fait référence à une liste pré-allouée de noms de domaine non déchiffrables) et la règle 6 (qui fait référence à des applications étiquetées comme non déchiffrables), est soumis à l'action Déchiffrer - Désigner sous la règle 7. Ces valeurs par défaut, ainsi que l'action par défaut, peuvent être modifiées si nécessaire. Par défaut, le trafic qui ne correspond à aucune autre règle est configuré comme Ne pas déchiffrer.

Le trafic Azure Authentication Service ne doit pas être déchiffré pour inspection, de sorte qu'une règle dédiée est créée pour lui. Cliquez sur + Ajouter une règle pour commencer.

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-Categoric (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

Ajouter Une Règle Et Afficher La Disposition De Déchiffrement Basée Sur Une Règle Par Défaut

2) Attribuez un nom à la nouvelle entrée de règle de stratégie de déchiffrement, choisissez Ne pas déchiffrer dans la liste déroulante Action, et placez la règle en haut des règles moins spécifiques. Des zones source/destination sont également implémentées pour affiner la règle.

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):

Cancel Add

Configurer la règle Ne pas déchiffrer

3) Avant d'ajouter la règle, cliquez sur l'onglet Applications, recherchez et cliquez sur l'application

Azure Authentication Service. Cliquez sur Ajouter à la règle, puis cliquez sur Ajouter.

Add Rule

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

Action: Do not decrypt

Zones Networks VLAN Tags Users Client Threat **Applications** Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Application Filters Available Applications (2)

Risks (Any Selected)

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

Business Relevance (Any Selected)

- ☐ Very Low 609

All apps matching the filter

- Azure Arc 1
- Azure Authentication Service 1**

Selected Applications and Filters (0)

any

Ajouter une règle d'application Azure Authentication Service

4) Cliquez sur Enregistrer.

active-auth-decrypt-policy

Decryption Policy for Active Authentication

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

You have unsaved changes

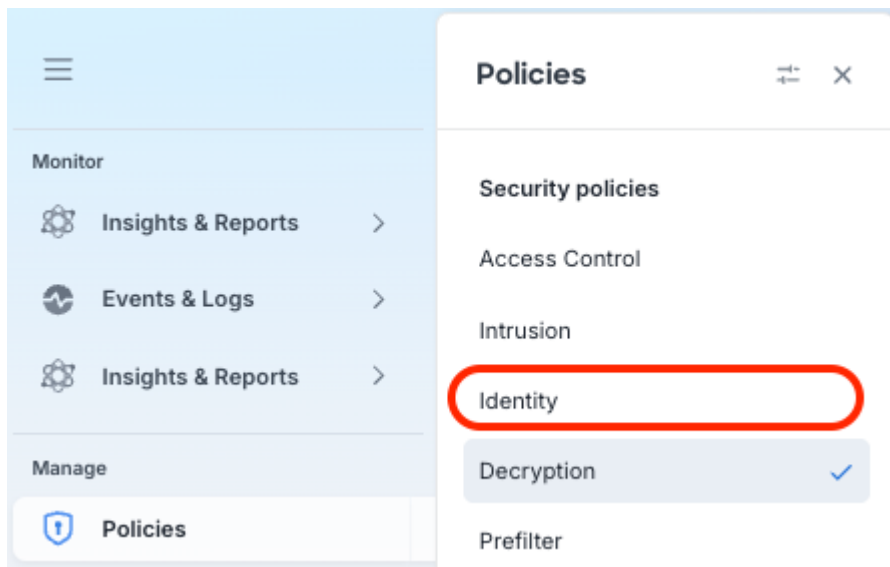
+ Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	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

Enregistrer la stratégie de décodage

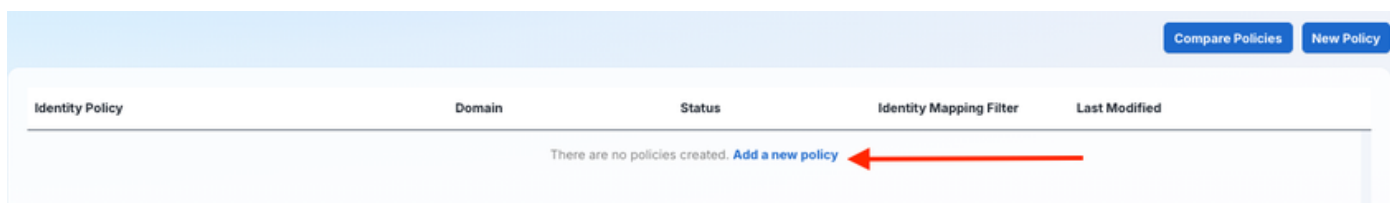
Étape 3: Créer une stratégie d'identité

1) Choisissez Politiques > Security Policies > Identity pour créer une politique d'identité.



Créer une stratégie d'identité

2) Créez une nouvelle stratégie d'identité et cliquez sur Add a new policy.



Ajouter une nouvelle configuration de stratégie d'identité

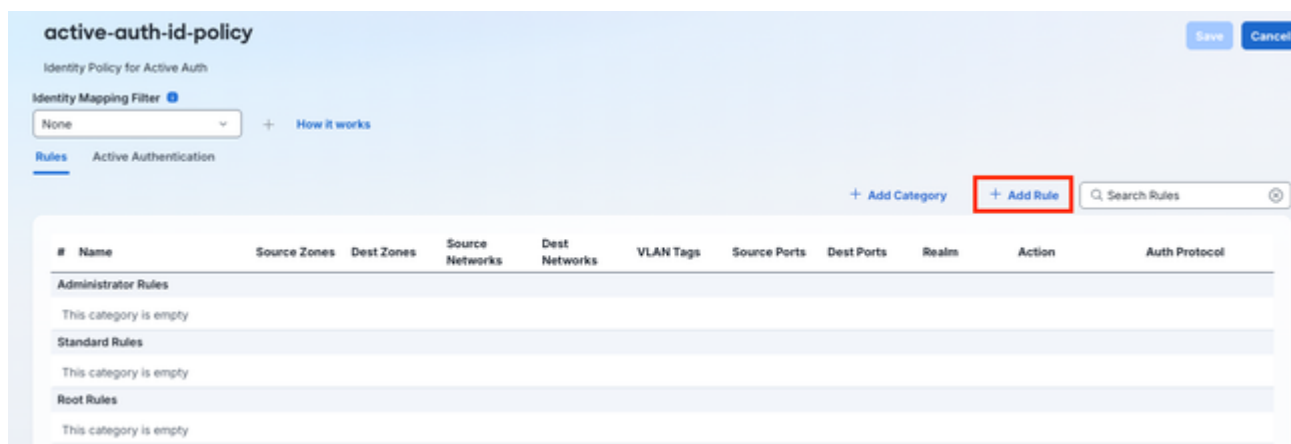
3) Attribuez un nom et, le cas échéant, une description à la nouvelle politique d'identité. Cliquez sur Save.

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

Nommer la nouvelle stratégie d'identité

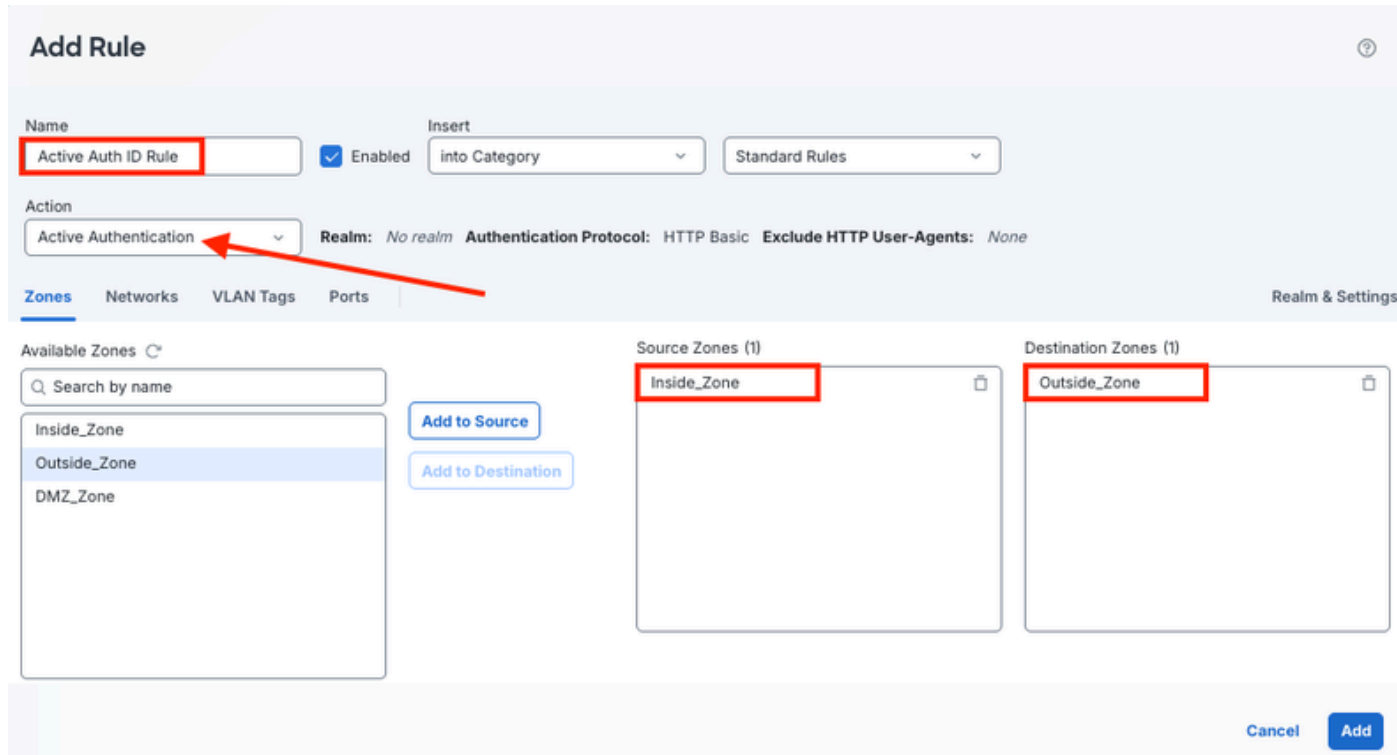
Étape 4: Configurer les règles de stratégie d'identité

1) Ajoutez une nouvelle règle en cliquant sur + Ajouter une règle.



Ajouter une nouvelle règle de stratégie d'identité

2) Attribuez un nom à la nouvelle règle, choisissez Active Authentication dans la liste déroulante Action, et limitez les zones/réseaux spécifiques qui doivent correspondre à la règle pour effectuer l'authentification active.



Configurer les paramètres de règle d'authentification active

3) Avant de cliquer sur Ajouter, cliquez sur l'onglet Domaine et paramètres dans l'Éditeur de règles. Vérifiez que le domaine configuré dans les étapes précédentes est sélectionné comme

domaine d'authentification, puis cliquez sur Ajouter.

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

Configurer Le Domaine Et Les Paramètres De La Règle D'Identité

4) La règle est ajoutée et configurée. Cliquez sur 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											

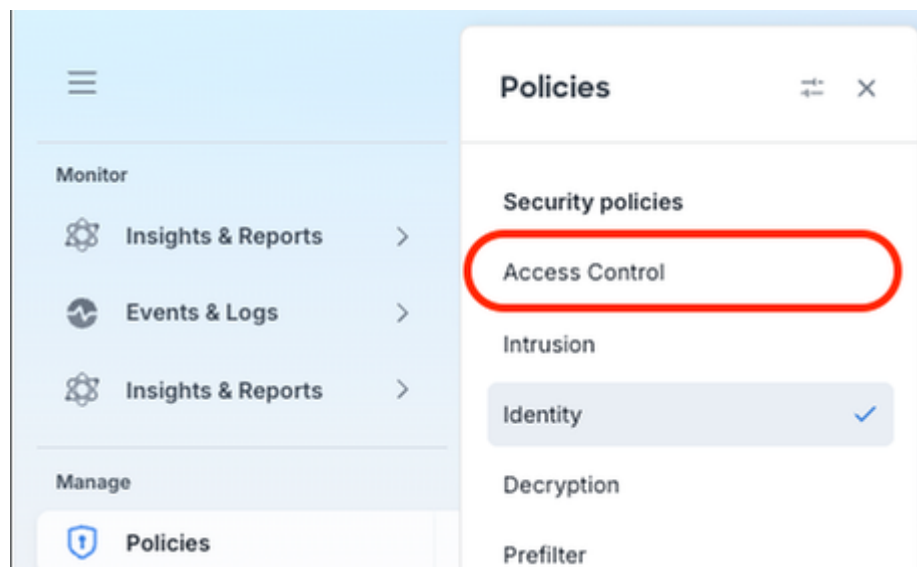
You have unsaved changes [Save](#) [Cancel](#)

Enregistrer la configuration de règle de stratégie d'identité

Étape 5: Configurer la stratégie de contrôle d'accès

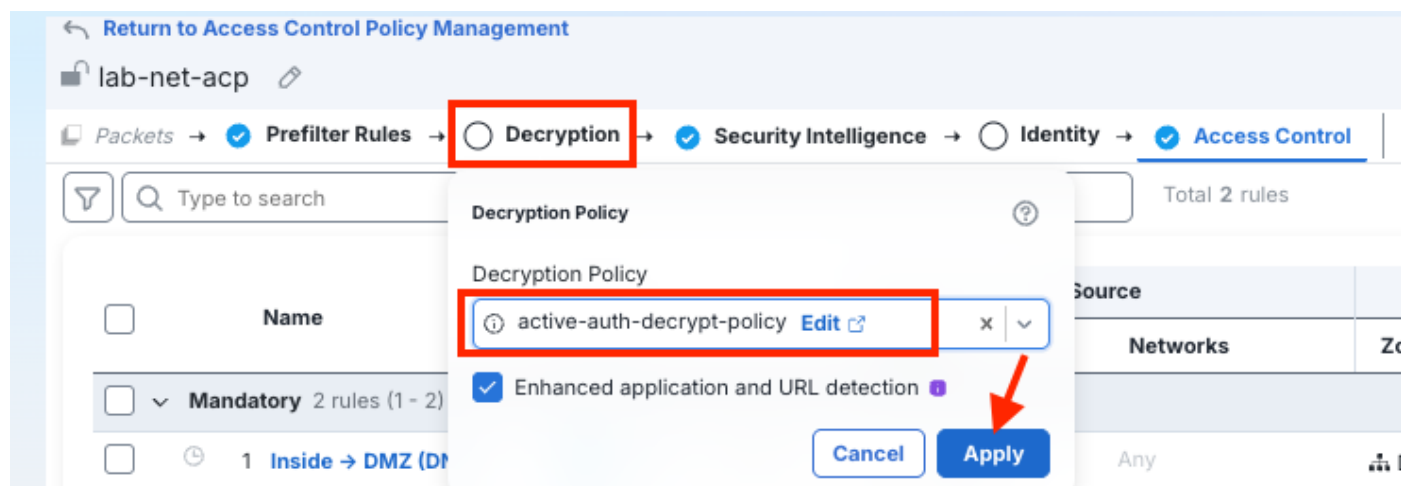
1) Choisissez Politiques > Security Policies > Access Control, puis cliquez sur la politique de

contrôle d'accès à laquelle le FTD est affecté.



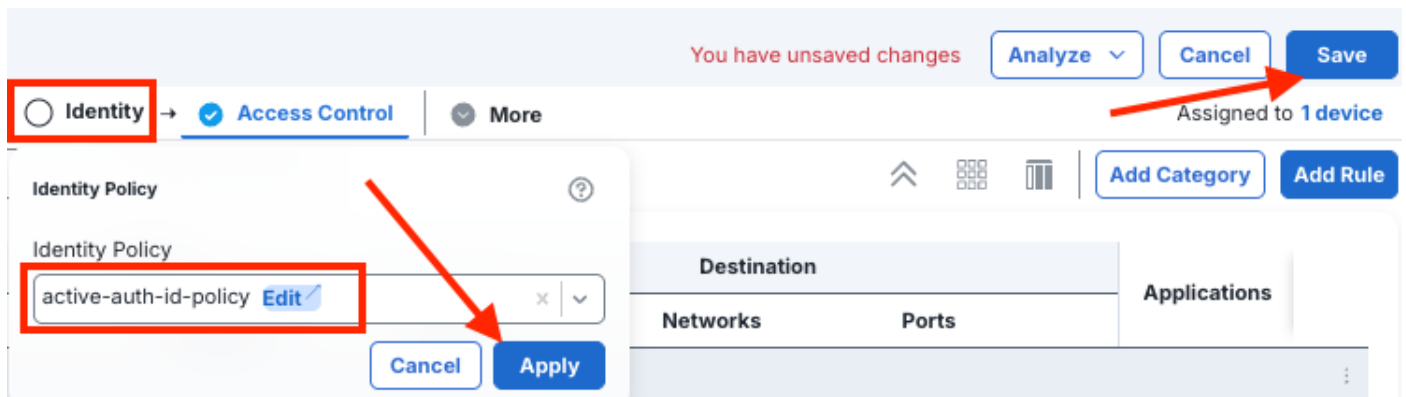
Configuration de la stratégie de contrôle d'accès

2) Vérifiez que la stratégie de décodage configurée dans les étapes précédentes est appliquée à la stratégie de contrôle d'accès.



Appliquer La Stratégie De Déchiffrement Au Contrôle D'Accès

3) Vérifiez que la stratégie d'identité configurée dans les étapes précédentes est également appliquée à la stratégie de contrôle d'accès. Enregistrez les modifications de stratégie.



Appliquer Une Stratégie D'Identité Au Contrôle D'Accès

4) Vérifiez qu'il existe des règles qui autorisent le trafic du plan de données client via le pare-feu sécurisé après une authentification active réussie. L'exemple ci-dessous utilise un ensemble de règles plus large dans l'environnement des travaux pratiques.

☐	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)								

Ensemble de règles de trafic du plan de données utilisateur

Étape 6: Déployer des configurations sur les périphériques Cisco Secure Firewall

Une fois déployés, les clients qui envoient du trafic sont invités à utiliser une page Web de connexion Microsoft pour effectuer l'authentification active avec Azure Entra.

Pour plus d'informations sur le processus décrit ici, consultez [Créer un domaine Microsoft Azure AD \(SAML\) pour l'authentification active \(portail captif\) - Chapitre : Domaines du Guide de configuration des périphériques FMC 10.x](#).

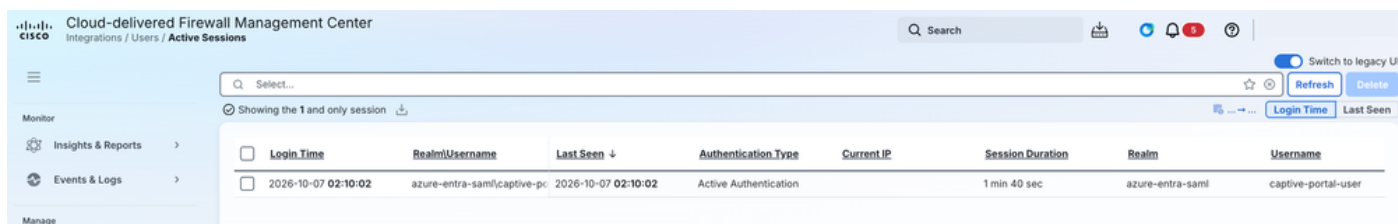
Vérifier

Utilisez cette section pour vérifier que la configuration fonctionne correctement.

IUG

Validez les sessions utilisateur et l'activité dans FMC :

- Choisissez Integrations > Users > Active Sessions.

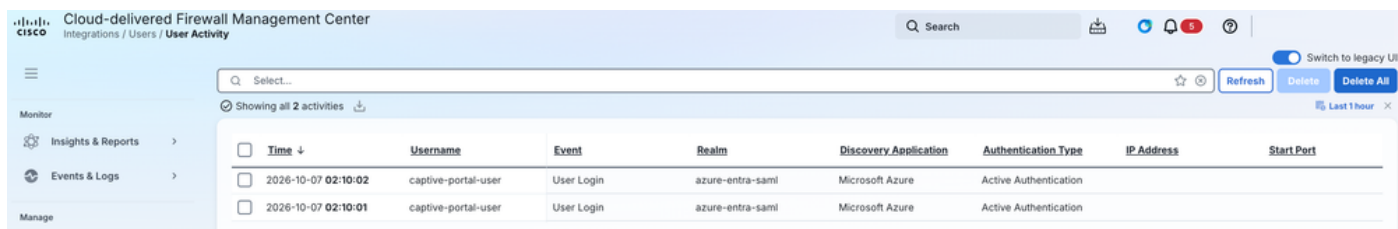


The screenshot shows the Cisco Cloud-delivered Firewall Management Center interface. The breadcrumb navigation is 'Integrations / Users / Active Sessions'. The left sidebar has 'Monitor' selected. The main content area shows a table of active sessions. A search bar at the top right has a 'Switch to legacy UI' toggle. Below the search bar, it says 'Showing the 1 and only session'. The table has columns: Login Time, Realm/Username, Last Seen, Authentication Type, Current IP, Session Duration, Realm, and Username. One session is listed with a login time of 2026-10-07 02:10:02, realm 'azure-entra-saml', and username 'captive-portal-user'.

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

Sortie des sessions actives FMC

- Choisissez Integrations > Users > User Activity.



The screenshot shows the Cisco Cloud-delivered Firewall Management Center interface. The breadcrumb navigation is 'Integrations / Users / User Activity'. The left sidebar has 'Monitor' selected. The main content area shows a table of user activities. A search bar at the top right has a 'Switch to legacy UI' toggle. Below the search bar, it says 'Showing all 2 activities'. The table has columns: Time, Username, Event, Realm, Discovery Application, Authentication Type, IP Address, and Start Port. Two activities are listed, both with a time of 2026-10-07 02:10:02, username 'captive-portal-user', and event 'User Login'.

☐	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		

Résultat de l'activité utilisateur FMC

Sur Azure, accédez au Centre d'administration Microsoft Entra :

- Filtrez les applications d'entreprise, recherchez/cliquez sur l'application appropriée.

Microsoft Entra admin center

Search resources, services

Home > Enterprise applications

Enterprise applications | All applicatio

« + New application ↻ R

Overview

- Overview View, filter, and search applica
- Diagnose and solve problems The list of applications that are

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 des applications d'Azure Entra Admin Center Enterprise

- Choisissez Exercice > Journaux de connexion.

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 filterShow dates as: UTCDate range: 10/7/2026 - 10/7/2026Application contains

User sign-ins (interactive)User sign-ins (non-interactive)Service principal sign-insManaged 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

Journaux d'activité de connexion aux applications Azure Enterprise

CLI

- Dans l'interface de ligne de commande FTD, vous pouvez voir les statistiques relatives aux réponses SAML et au portail captif :

<#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
```

Dépannage

Débogage du portail captif

- La commande `system support captive-portal-debug` peut être utilisée sur le FTD. Le résultat montre comment activer le débogage et note également des segments clés du résultat pour aider à comprendre le flux Captive Portal.

```
<#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
...

```

Vidage des identités utilisateur

- Pour prendre un instantané des données d'état d'identité d'utilisateur actuelles sur le FTD, exécutez la commande `system support firewall-engine-dump-user-identity-data` sur l'interface de ligne de commande du FTD :

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

Successfully commanded snort.

>

- En mode expert CLI, lors de la connexion avec les identifiants d'administration locaux du périphérique FTD, affichez le contenu du fichier vidé dans `/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:

...

Problèmes possibles

Autorité de certification inconnue du portail captif

Problème : Le navigateur client renvoie une erreur d'émetteur inconnu lorsque l'authentification est tentée.

Cause probable : L'autorité de certification interne n'est pas approuvée dans le navigateur client.

Résolution : Vérifiez que l'autorité de certification est approuvée dans le navigateur. L'exemple présenté ici confirme que le certificat d'autorité de certification interne est approuvé.

Portail captif « Serveur introuvable »

Problème : Lorsque le navigateur client tente de charger le portail captif, il renvoie « Serveur introuvable » pour l'URL de base lors de la tentative d'accès à l'URL de base ou similaire.

Cause probable : Accessibilité DNS ou configuration DNS incorrecte.

Résolution : Vérifiez que le client dispose du serveur DNS approprié configuré pour résoudre l'enregistrement A. Vérifiez que le serveur dispose d'un enregistrement A mappé au nom de domaine complet et qu'il est accessible et réactif.

Informations connexes

- [Créer un domaine Microsoft Azure AD \(SAML\) pour l'authentification active \(portail captif\) - Guide de configuration du périphérique FMC 10.x](#)
- [Documentation Azure Event Hub](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.