

セキュアファイアウォールでのAzure Entraキャプティブポータルの構成

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[図](#)

[エンドポイント、FTD、Azure Entra間のキャプティブポータル](#)

[設定](#)

[フェーズ1:FMCとDNSの初期設定](#)

[ステップ1:Cisco Dynamic Attributes Connector\(CSDAC\)を有効にします](#)

[ステップ2:FTD入カインターフェイスを表す完全修飾ドメイン名\(FQDN\)ネットワークオブジェクトを作成します。](#)

[ステップ3:DNS Aレコードの設定](#)

[フェーズ2：公開キーインフラストラクチャの設定](#)

[ステップ1：内部CA証明書をFMCにインポートする](#)

[ステップ2：サービスプロバイダー証明書にCAで署名する](#)

[ステップ3:FTDへのSP証明書の導入](#)

[フェーズ3: Azure構成](#)

[ステップ1:SAMLツールキット用のエンタープライズアプリケーションを作成します](#)

[ステップ2：エントリIDのアプリケーション登録を設定します。](#)

[ステップ3：アプリケーション登録のためのMicrosoft Graph API権限の設定](#)

[ステップ4：イベントハブ\(EH\)名前空間を構成します](#)

[ステップ5：イベントハブの名前空間で共有アクセスポリシーを選択または作成する](#)

[ステップ6:EH名前空間から共有アクセスシグニチャ\(SAS\)情報を収集してメモする](#)

[ステップ7：イベントハブネームスペース内にイベントハブインスタンスを作成する](#)

[ステップ8：イベントハブネームスペース内にイベントハブインスタンスコンシューマグループを作成します](#)

[ステップ9：収集された値の確認](#)

[ステップ10：イベントハブへのエントリID監査ログストリーミングを設定します](#)

[フェーズ4: AzureとFMC/FTDのアクティブ認証構成を統合する](#)

[手順1: FMCウィザードを使用してAzure SAML/Entra IDレルムを構成する](#)

[手順2: FMCで構成されたSAML SPメタデータをAzure Enterpriseアプリケーションに実装する](#)

[手順3: FMCウィザードを使用してAzure SAML/Entra IDレルムを構成する（続き）](#)

[ステップ4：ダウンロードしたユーザの確認](#)

[フェーズ5:FMCでのポリシーの設定](#)

[ステップ1：復号ポリシーの設定](#)

[ステップ2：復号ポリシールールの設定](#)

[手順3：アイデンティティポリシーの作成](#)

[ステップ4：アイデンティティポリシールールの設定](#)

[ステップ5：アクセスコントロールポリシーの設定](#)

[ステップ6:Cisco Secure Firewallデバイスへの設定の導入](#)

[確認](#)

[GUI](#)

[CLI](#)

[トラブルシューティング](#)

[キャプティブポータルのデバッグ](#)

[ユーザIDダンプ](#)

[考えられる問題](#)

[キャプティブポータルの不明な認証局](#)

[キャプティブポータル「サーバが見つかりません](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Secure Firewallのキャプティブポータル (アクティブ認証) で使用するMicrosoft Azure Entra ID(MDL)の設定について説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

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

Event Hubを作成するには、Azureで利用できるStandard価格レベルが必要です。さらに、輸出規制機能を有効にしたスマートライセンスでデバイスを有効化する必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Secure FTDバージョン10.0
- Cisco Secure FMCバージョン10.0

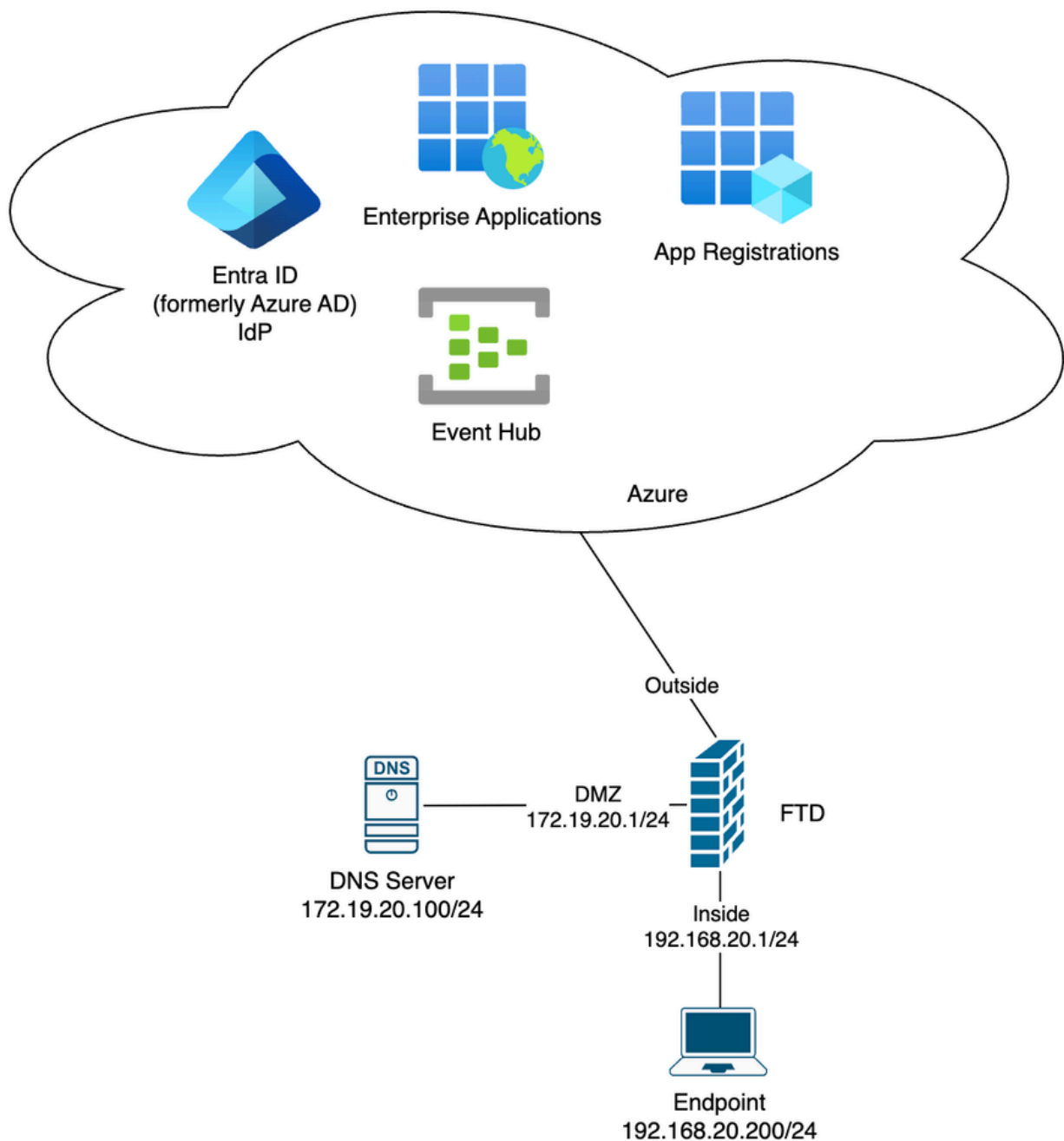
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

従来のIPベースのセキュリティアーキテクチャは、動的なハイブリッド作業環境への対応に苦慮しているため、Cisco Secure Firewall Active Authentication with SAML統合は、堅牢なアイデンティティ中心のソリューションを提供します。この構成では、一元化されたIDプロバイダーとしてMicrosoft Entra ID (Azure AD)を活用することで、管理者は静的なネットワークルールを超えて、揮発性ネットワークアドレスではなく検証済みのユーザーIDに基づいてきめ細かなアクセス制御を適用できます。この統合により、シームレスなシングルサインオン(SSO)と必須のMulti-Factor Authentication(MFA)を通じてユーザエクスペリエンスが合理化されます。また、境界のないネットワーク全体で厳格な可視性とポリシー適用を維持する統合されたセキュリティポスチャが確保されます。



エンドポイント、FTD、Azure Entra間のキャプティブポータル



エンドポイントとAzure Entra間のキャプティブポータル

設定

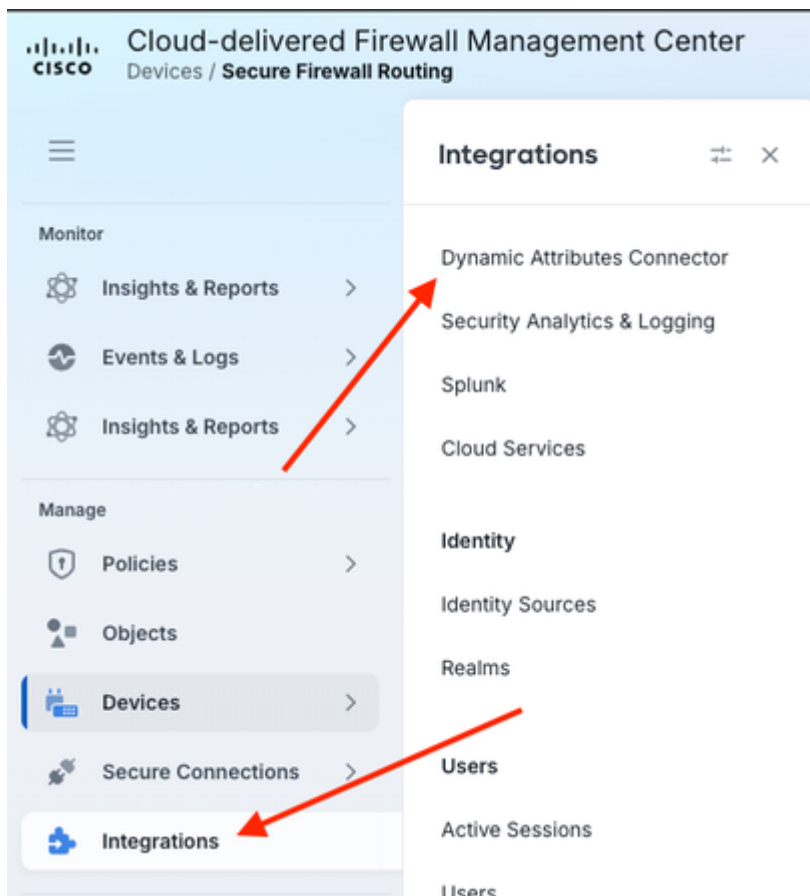
フェーズ1:FMCとDNSの初期設定



注：この実習では、クラウドで提供されるFirewall Management Center(cdFMC)を使用します。ただし、手順はオンプレミスFMCと同じです。

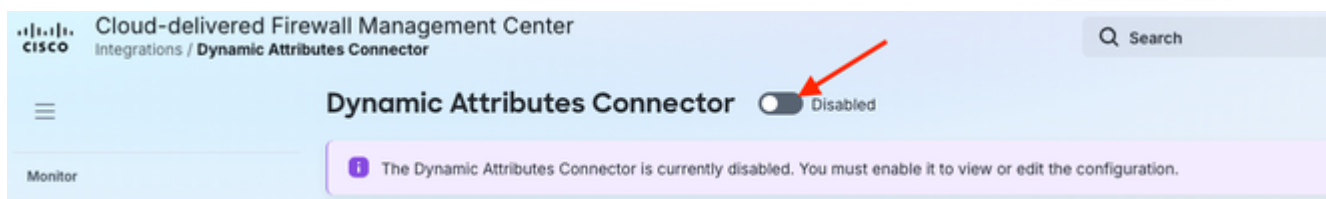
ステップ1: Cisco Dynamic Attributes Connector(CSDAC)を有効にします

1) Integrations > Dynamic Attributes Connectorの順に選択します。



統合の選択ダイナミック属性コネクタ

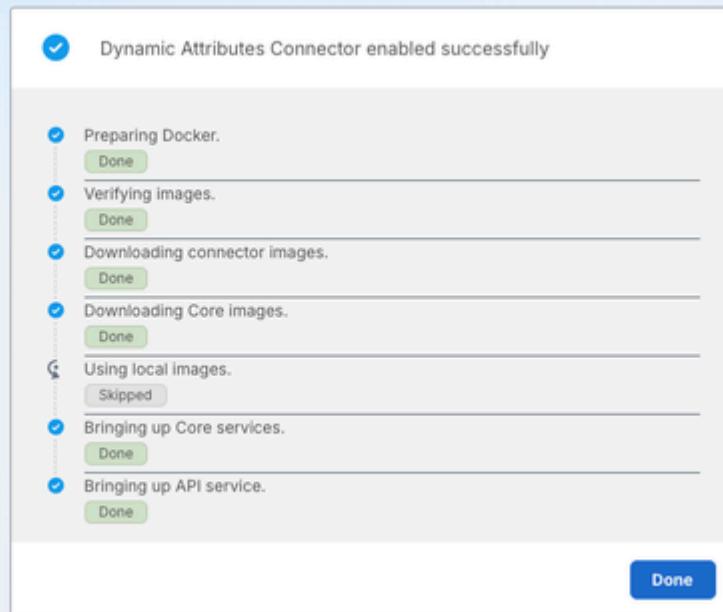
2) Disabled文字列の横にあるコントロールをクリックして、CSDACを有効にします。



Ciscoダイナミック属性コネクタを有効にする

c) CSDACの有効化が完了したら、Doneをクリックします。

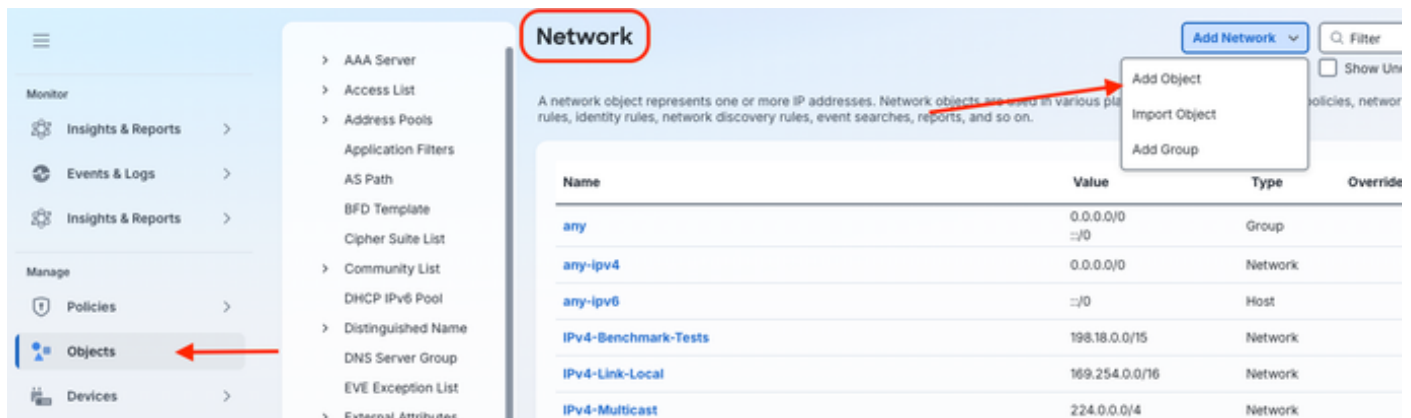
Dynamic Attributes Connector



Ciscoダイナミック属性コネクタのステータスを有効にする

ステップ2:FTD入力インターフェイスを表す完全修飾ドメイン名(FQDN)ネットワークオブジェクトを作成します。

1) Objects > Add Network > Add Objectの順に選択します。



新しい完全修飾ドメイン名(FQDN)ネットワークオブジェクトの作成

2)設定されているネットワークオブジェクトに完全修飾ドメイン名(FQDN)を使用して名前を付けます。 FQDNを入力し、該当するオプションボタンをクリックして、ネットワークオブジェクトをFQDNタイプとして割り当てます。[Save] をクリックします。

Edit Network Object ?

Name

Description

Network
☐ Host ☐ Range ☐ Network ☒ FQDN

Note:
You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

Lookup:

☐ Allow Overrides

Cancel Save

FQDNネットワークオブジェクト変数の設定

ステップ3:DNS Aレコードの設定

1)ここに示す例では、Windows Server 2025を使用しています。必要に応じて、特定の名前解決サーバのマニュアルを参照してください。

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



注：アクティブ認証を実行するクライアントは、このDNS Aレコードを解決できる必要があります。

フェーズ2：公開キーインフラストラクチャの設定

内部認証局(CA)は、アクティブ認証の設定の公開キーインフラストラクチャ(PKI)として使用できます。Cisco FMCとFTDでは、必要なSSL代行受信と復号化 – 再署名の操作を実行するために、内部CA公開キーとペア化された秘密キーが内部CAオブジェクトとしてアップロードされている必要があります。また、内部CAは、アクティブ認証が実行されるクライアントブラウザ内で信頼される必要があります。ブラウザが証明書を信頼していることを確認する方法については、クライアントブラウザのマニュアルを参照してください。

ステップ1：内部CA証明書をFMCにインポートする

1) Objects > PKI > Internal CAsの順に選択します。[Import CA] をクリックします。



注：内部CAは、FMC上で直接作成することもできます。

Import Internal Certificate Authority ?

Name:

Certificate Data or, choose a file:

-----BEGIN CERTIFICATE-----

-----END PRIVATE KEY-----

Key or, choose a file:

-----BEGIN CERTIFICATE-----

-----END PRIVATE KEY-----

☒ Encrypted, and the password is:



注：このドキュメントのコンテンツでは、イメージのさまざまなフィールド値をカバーする空白文字が表示されます。この空白文字は、このドキュメントの発行時に意図的に使用されています。実際の値は、設定時に環境に反映されます。

ステップ2：サービスプロバイダー証明書にCAで署名する

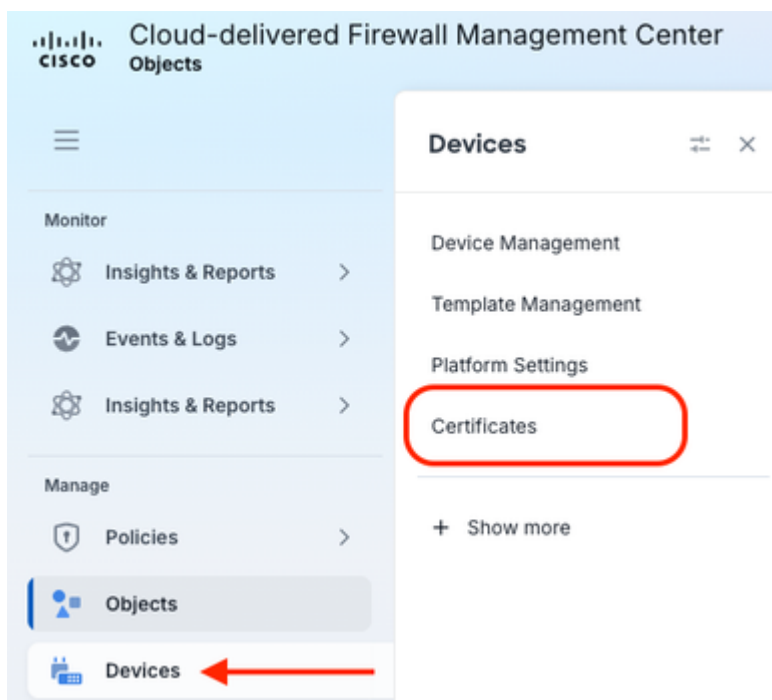
1) サービスプロバイダー(SP)証明書は、信頼できる認証局(CA)によって署名され、PKCS#12 (.p12)形式で返される必要があります。



注：このCAは内部署名が可能です。唯一の注意事項は、内部CAがクライアントデバイスによって信頼される必要があることです。

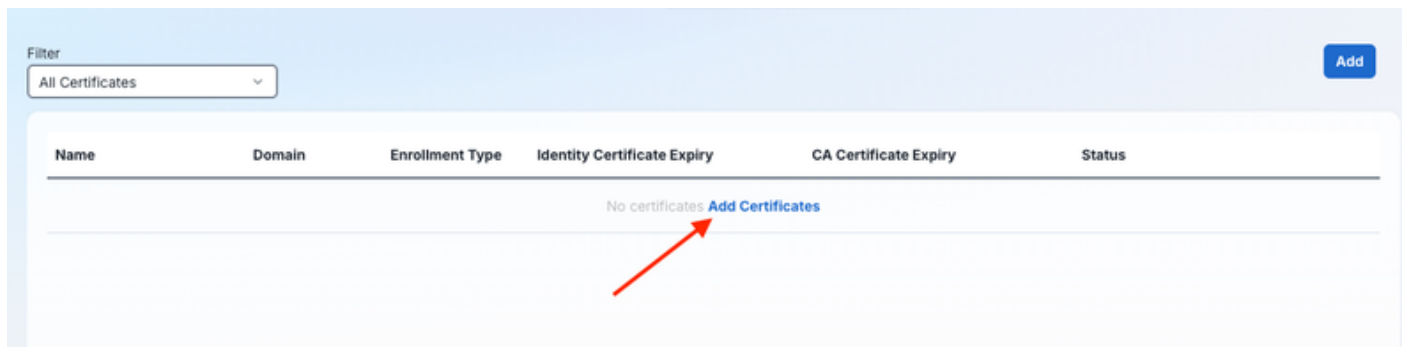
ステップ3:FTDへのSP証明書の導入

1) Devices > Certificatesの順に選択します。



Devices And Certificatesに移動します。

2) Add Certificatesをクリックします。



新しいデバイス証明書の追加

3) アクティブ認証を実行するドロップダウンリストからデバイスをクリックし、+アイコンをクリックして新しい証明書登録を作成します。

FTDを選択し、Add Add New Certificate Enrollmentを選択します

4) Certificate Enrollmentという名前を付け、Enrollment Typeドロップダウンリストから、PKCS12 fileを選択します。

Add Certificate Enrollment ?

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:*

Challenge Password:

Confirm Password:

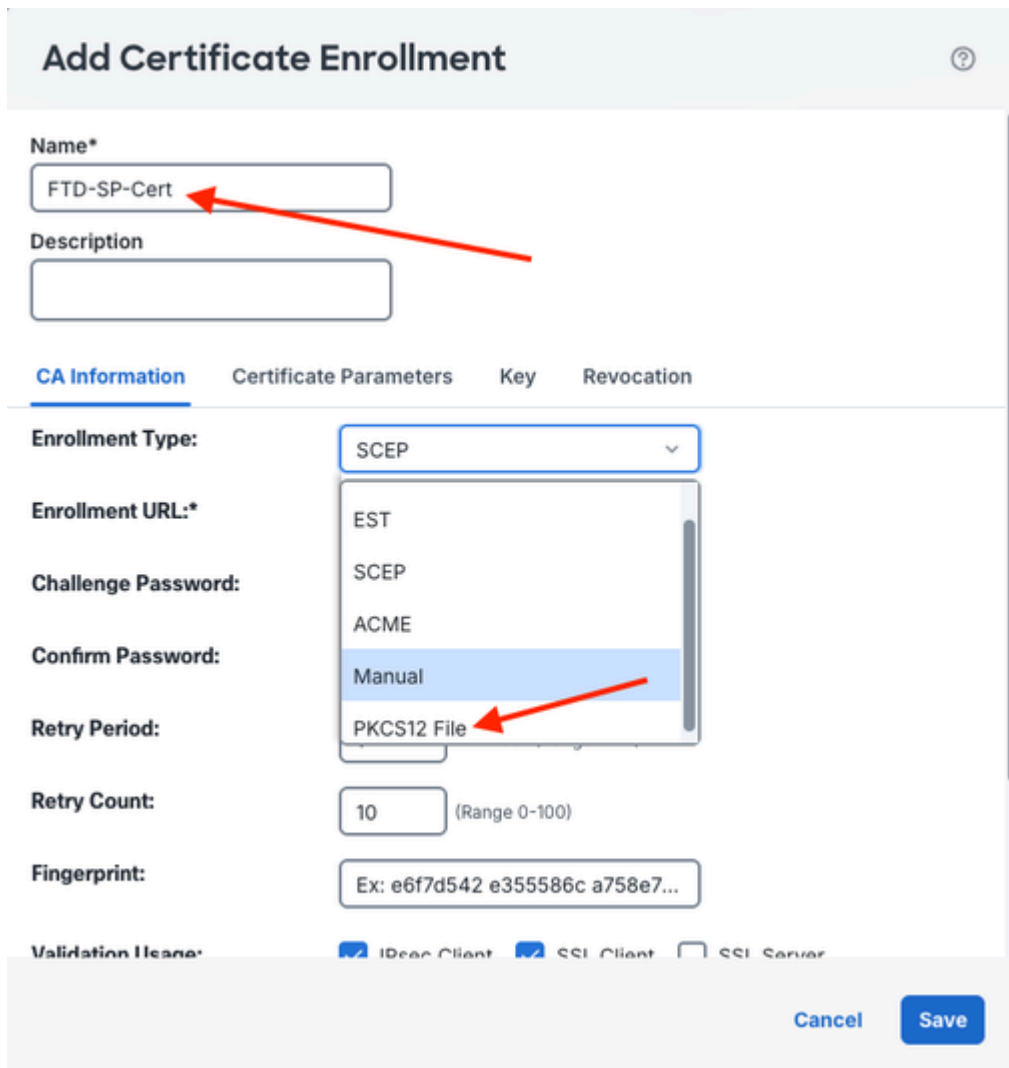
Retry Period:

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7...

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

Cancel Save



証明書の登録の設定と種類

5) Browse PKCS12 FileをクリックしてPKCS#12 fileをインポートし、必要なパスフレーズを入力します。[Save] をクリックします。

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ファイルの参照とインポート

6)登録の詳細が正しいことを確認し、Addをクリックします。

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

証明書の登録の詳細の確認

FTD				
FTD-SP-Cert	Global	PKCS12 file	In progress	

Filter

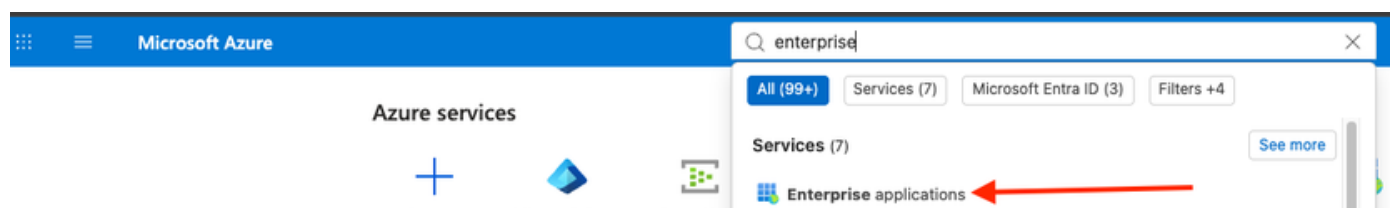
All Certificates

Add

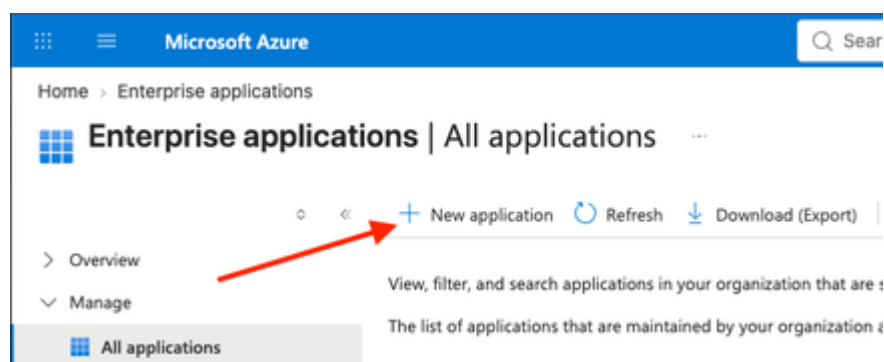
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
FTD					
FTD-SP-Cert	Global	PKCS12 file	Dec 18, 2028	Sep 12, 2036	CA ID

フェーズ3: Azure構成

1) Enterprise Applicationsを検索してクリックします。

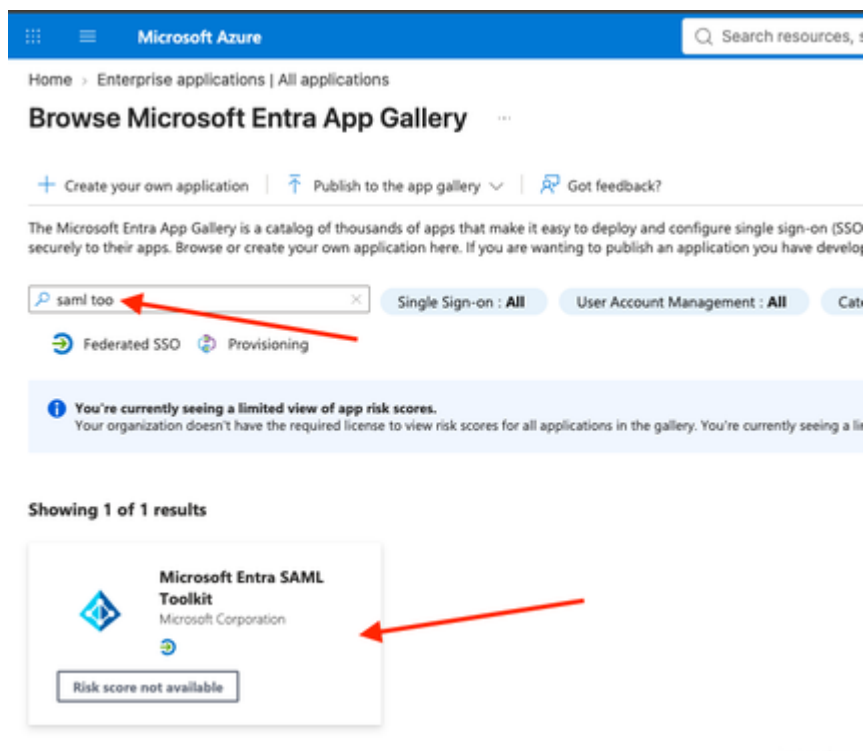


2) + New Applicationをクリックします。



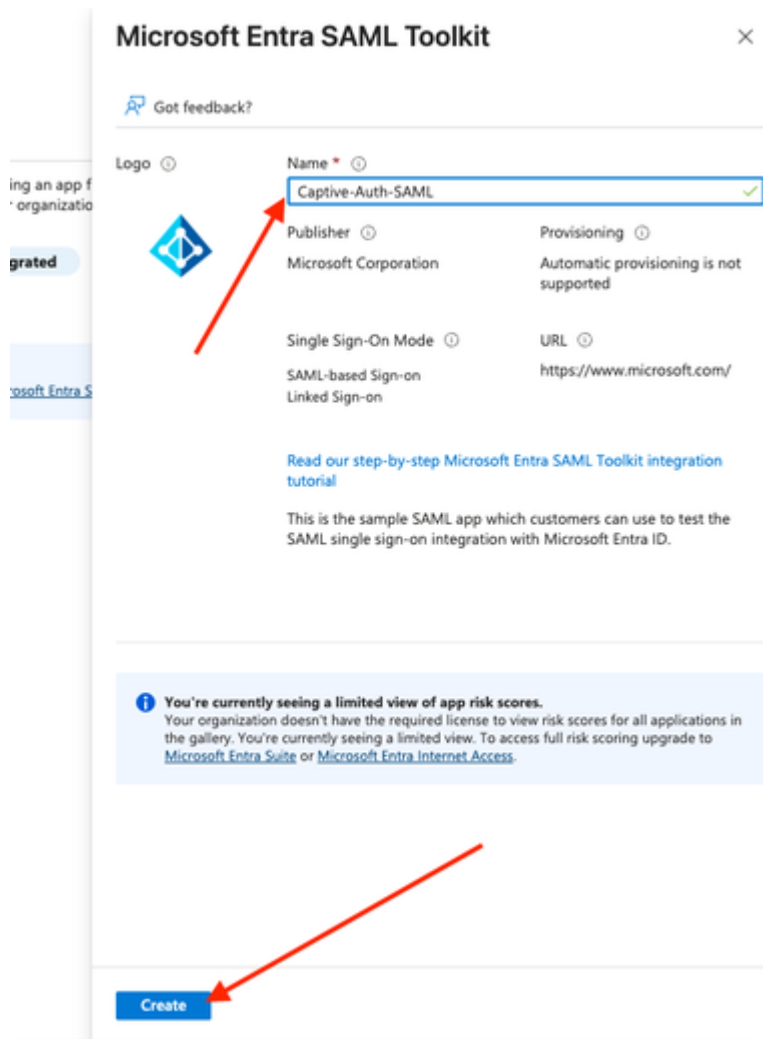
エンタープライズアプリケーション内の新しいアプリケーションの選択

3) Microsoft Entra SAML Toolkitを検索し、そのサムネイルをクリックします。



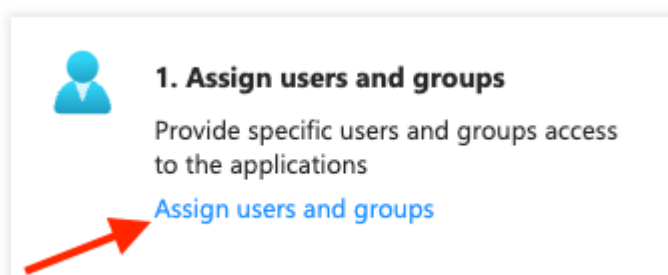
Microsoft Entra SAML Toolkitの検索と選択

4) Microsoft Entra SAML Toolkit Enterprise ApplicationにNameを割り当て、Createをクリックします。(Microsoftからの参照 : [Microsoft Entra SAML Toolkit統合チュートリアルの手順を読んでください](#))。



Samlツールキットアプリケーションへの名前の割り当て

5) Overviewページで、SAML Toolkitエンタープライズアプリケーションに特定のユーザとグループを割り当てます。この例では、テストアカウント(captive-portal-user)はactive-auth-labグループのメンバーです。

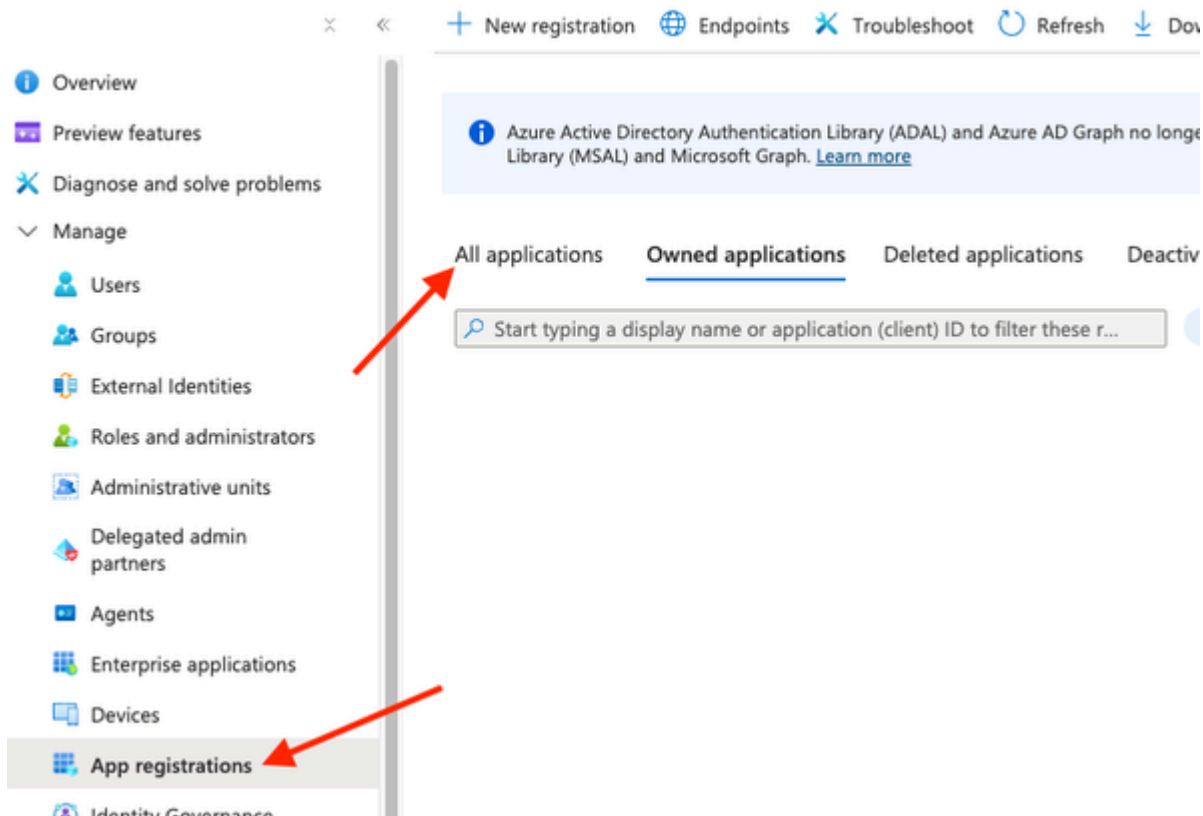


ユーザーとグループのアプリケーションへの割り当て

6)このエンタープライズアプリケーションの設定は、後の手順で続けます。

ステップ2：エントリIDのアプリケーション登録を設定します。

1) Entra IDに戻り、左側のナビゲーションメニューからApp registrationsを選択します。All applicationsフィルタをクリックして、Enterprise Applicationに指定された名前を検索します。該当するアプリケーションをクリックします。



アプリケーションの登録とすべてのアプリケーションに移動

2) Enterprise App RegistrationでEssentials値を収集してメモします。



重要：値の上にマウスのカーソルを置くと、「クリップボードにコピー」が表示され、「概要」ページの「Essentials」の下で値を収集できます。

- 表示名
- アプリケーション (クライアント) ID
- ディレクトリ (テナント) ID

Captive-Auth-SAML

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

- Branding & properties
- Authentication (Preview)
- Certificates & secrets

Essentials

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

Application (client) ID :

Object ID :

Directory (tenant) ID :

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

表示、アプリケーション、およびディレクトリIDの値の収集

3) Add a certificate or secretハイパーリンクをクリックします。

Captive-Auth-SAML

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

- Branding & properties
- Authentication (Preview)
- Certificates & secrets

Essentials

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

Application (client) ID :

Object ID :

Directory (tenant) ID :

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

Client credentials

- [Add a certificate or secret](#)
- [1 web, 0 spa, 0 public client](#)
- [Add an Application ID URI](#)
- Managed application in L... : [Captive-Auth-SAML](#)
- State : [Activated](#)

証明書またはシークレットハイパーリンクの追加

4) + New client secretをクリックします。

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.			

新しいクライアントシークレットの追加

5)シークレットの説明を指定し、必要に応じて有効期限を調整します。[Add] をクリックします。

Add a client secret

Description:

Expires: Recommended: 180 days (6 months) ▼

Add Cancel

クライアントシークレットの説明を入力してください

6) 秘密をコピーします。



重要：クリップボードにコピーされたシークレット値をメモします。

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

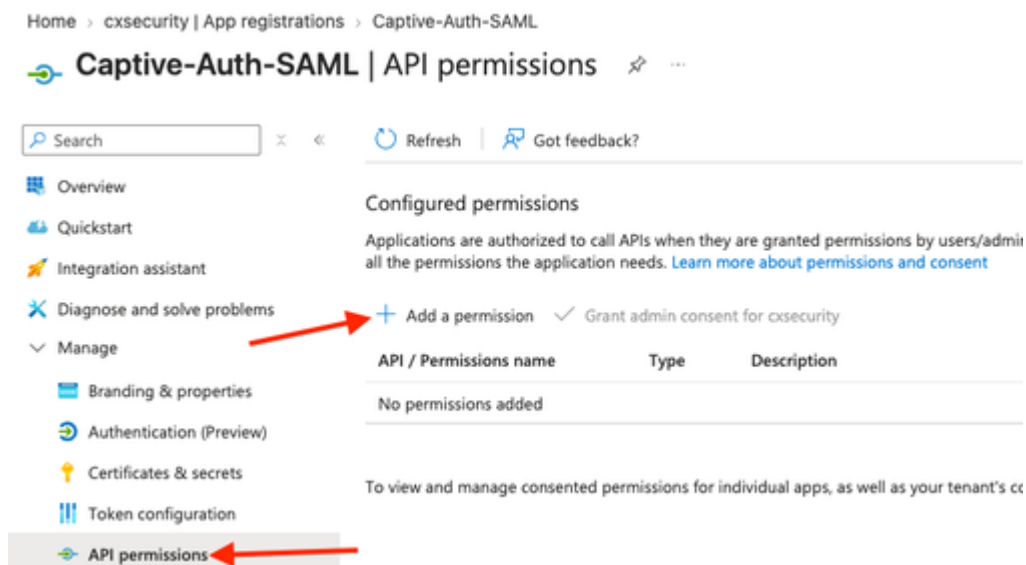
Description	Expires	Value	Secret ID
saml-secret	3/14/2027		

A red arrow points to the copy icon in the 'Secret ID' column for the 'saml-secret' entry.

クライアントシークレット値のコピー

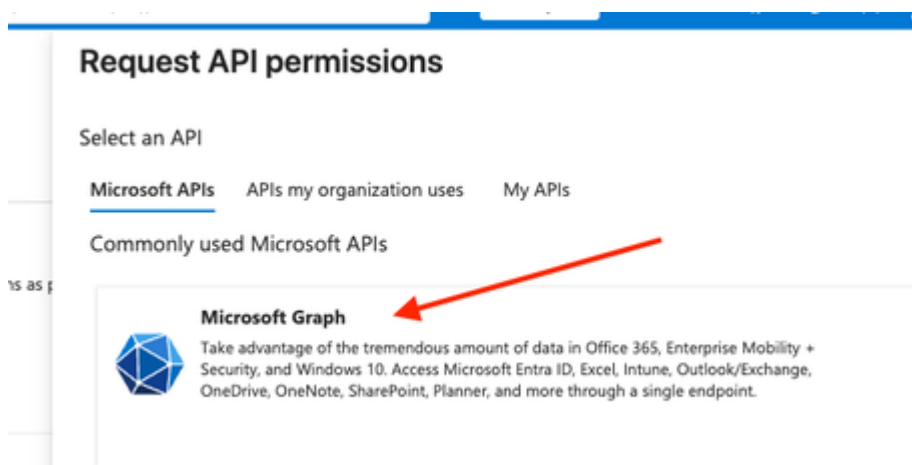
ステップ 3：アプリケーション登録のためのMicrosoft Graph API権限の設定

1) 左側のナビゲーションメニューからAPI Permissionsを選択し、+Add a permissionをクリックします。



APIアクセス許可の設定

2) Microsoft Graph APIをクリックします。



Microsoft Graph APIの選択

3) Delegated User.Read権限を付与し、Add permissionsをクリックします。

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

委任されたユーザーに読み取りアクセス許可を付与する

4)アプリケーションにUser.Read.All権限を付与します (チェックボックスをオンにします)。

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)

☒	User.Read.All ⓘ Read all users' full profiles	Yes
-------------------------------------	--	-----

アプリケーションに読み取り権限を付与

5)Group.Read.Allチェックボックスを検索してチェックし、グループに読み取り権限も付与します。Add permissionsをクリックします。

Select permissions

expand all

Group.Read.All

Permission

Admin consent required

▼ Group (1)

☒	Group.Read.All ⓘ Read all groups	Yes
-------------------------------------	-------------------------------------	-----

Add permissions

Discard

APIアクセス許可の保存

6)設定された権限が一致していることを確認し、それらに管理者の同意を与えます。

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 ...

アクセス許可に対する管理者の同意を許可する

7)管理者の同意が付与されると、出力が表示されます。

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

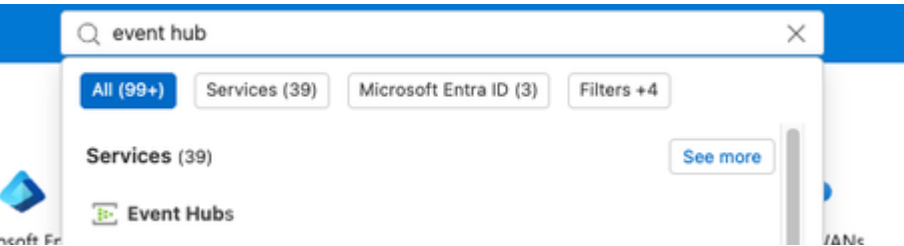
✓ Grant admin consent for

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 ...

許可された管理上の同意の出力

ステップ4：イベントハブ(EH)名前空間を構成します

1) Event Hubsを検索してクリックします。



検索イベントハブの構成

2)新しいEH名前空間を作成します。



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.

[+ Create](#)

[Learn more about Event Hubs](#)

イベントハブ名前空間の作成

3) EH名前空間を構成します。



注:Standard以上の価格レベルを選択する必要があります。Basic価格レベルでは、レルムの使用が禁止されます。

Event Hubの詳細設定と特定のニーズへの適用性の詳細な評価については、[Azure Event Hubドキュメント](#)を参照してください。

Review + Createをクリックします。



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 >

イベントハブの名前空間の設定を構成する

4)検証が成功したら、Createをクリックします。

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 >

イベントハブ名前空間の展開の作成

5)導入が完了したことを確認し、Go to resourceをクリックします。

Home

captive-auth-ad-eh | Overview

Deployment

Search x <

Delete Cancel Redeploy Download Refresh

Overview

- Inputs
- Outputs
- Template

Your deployment is complete

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

> Deployment details

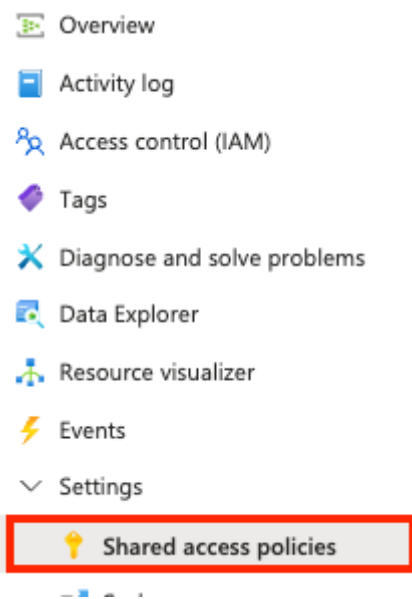
Next steps

Go to resource

イベントハブ名前空間リソースに移動

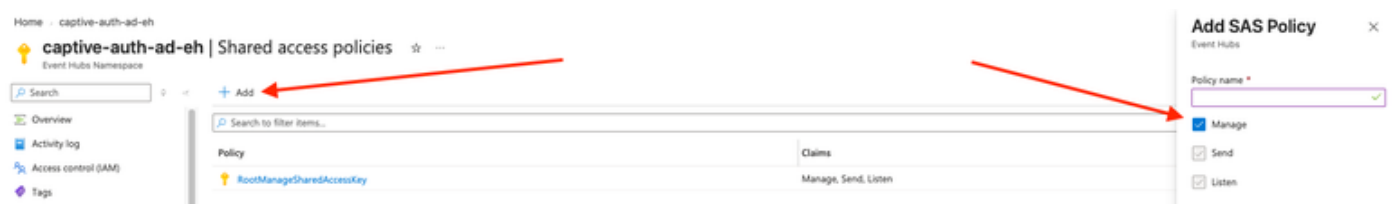
ステップ5：イベントハブの名前空間で共有アクセスポリシーを選択または作成する

1)左側のナビゲーションメニューから、Settings > Shared access policiesの順に選択します。



共有アクセスポリシーに移動

2) + Addをクリックして、新しいポリシー名を入力し、Manageチェックボックスにチェックマークを付けます。Add SAS Policyメニューパネルの下部にあるCreateをクリックします。



新しい共有アクセスポリシーの追加



共有アクセスポリシーの作成

ステップ6:EH名前空間から共有アクセスシグニチャ(SAS)情報を収集してメモする

1)新しい共有アクセスポリシーをクリックします。右側のサイドパネルにEH SASポリシーが表示

されます。

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 ADMIN ID

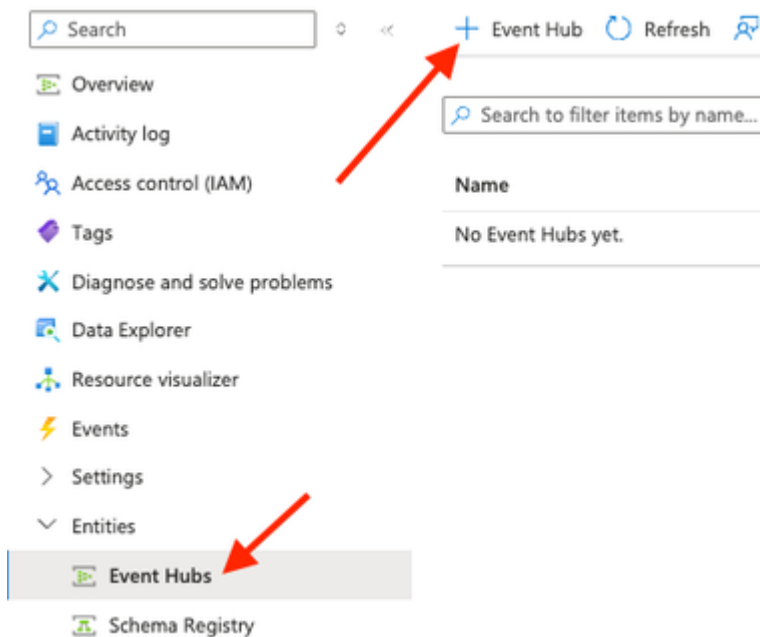
プライマリ接続文字列のコピー



重要：プライマリ接続文字列をコピーしてメモします。

ステップ7：イベントハブネームスペース内にイベントハブインスタンスを作成する

1) Namespaceメニューから、Entities > Event Hubsの順に選択します。+ Event Hubをクリックして、新しいEHインスタンスを作成します。



新しいイベントハブインスタンスの作成

2)新しいEHインスタンスに名前を割り当て、確認+作成をクリックします。

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 >

イベントハブインスタンスへの名前の割り当て

3)検証が成功したら、CreateをクリックしてEvent Hubインスタンスをプロビジョニングします。

Create Event Hub

Event Hubs

Validation succeeded.

Basics

Capture

Review + create

Event Hubs Instance by Microsoft

Basics

Retention

Capture

Name	captive-auth-ad-eh-1
Partition count	1
Cleanup policy	Delete
Retention time (hrs)	1
Capture Status	Off

Create

< Previous

Next >

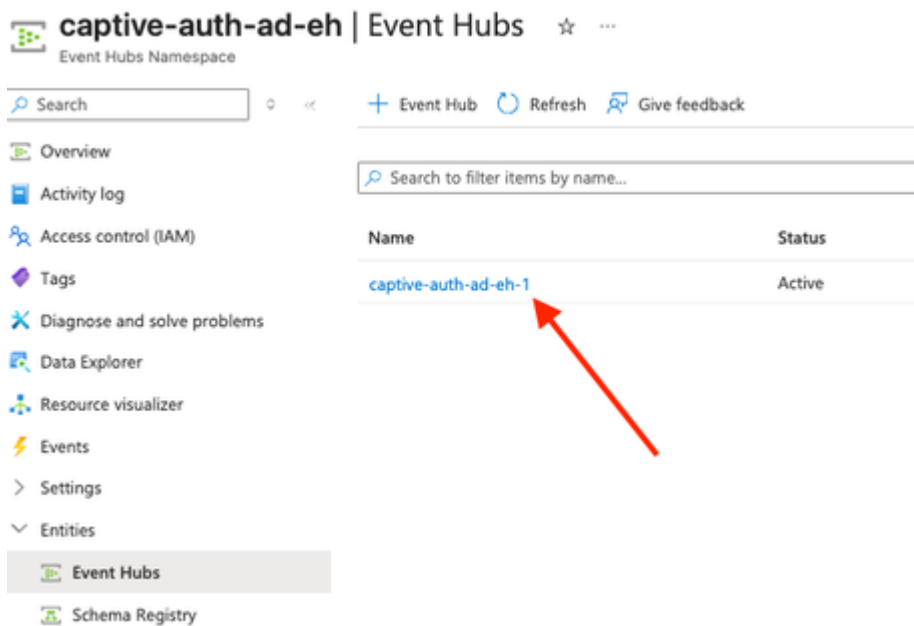
Provision Event Hubインスタンス



重要:Event Hubのインスタンス名をコピーしてメモします。

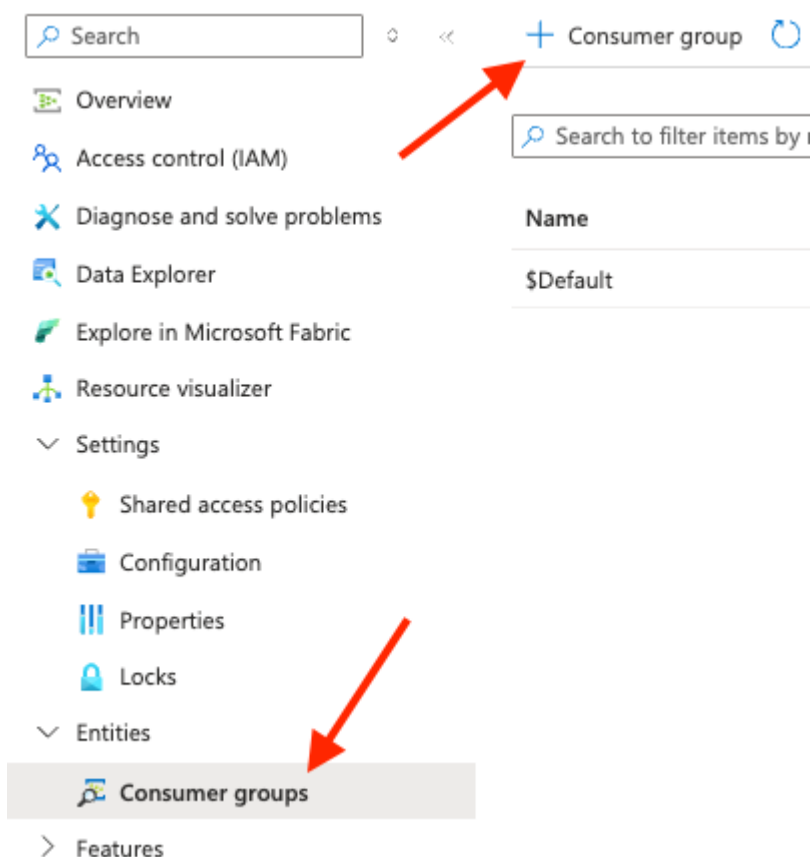
ステップ8： イベントハブネームスペース内にイベントハブインスタンスコンシューマグループを作成します

1)前のステップで設定した新しいEHインスタンスをクリックします。



Event Hubインスタンス構成へのアクセス

2) EHインスタンスから、Entities > Consumer groupsの順に選択し、新しいConsumer groupを作成します。



コンシューマグループの作成

3) コンシューマ・グループに名前を付けて、作成をクリックします。

Create consumer group ×

Consumer groups

Name *

captive-auth-ad-eh-cg



Create

コンシューマ・グループへの名前の割り当て



重要:Event Hubインスタンスのコンシューマ・グループ名をコピーしてメモします。

ステップ9：収集された値の確認

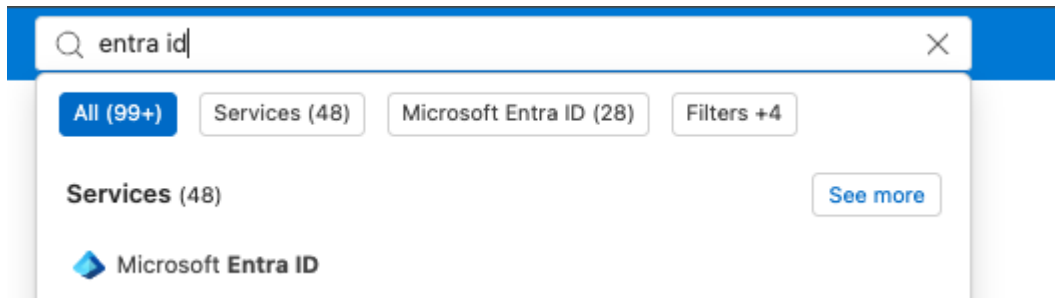
1)この時点では、前の手順の値に注意する必要があります。値が記録されていない場合は、収集された該当する手順を参照してください。

- フェーズ3ステップ2：アプリケーション登録（このプロセス用に作成されたエンタープライズアプリケーションの、収集された表示名で参照）
 - ステップ2、サブステップ2
 - 表示名
 - アプリケーション（クライアント）ID
 - ディレクトリ（テナント）ID
 - ステップ2、サブステップ6
 - クライアントシークレット
- フェーズ3ステップ6:Event Hub
 - ステップ6、サブステップ1
 - EH名前空間
 - プライマリ接続文字列

- ステップ7、サブステップ3
 - EHインスタンス(Event Hub)名
- ステップ8、サブステップ3
 - EHコンシューマグループ名

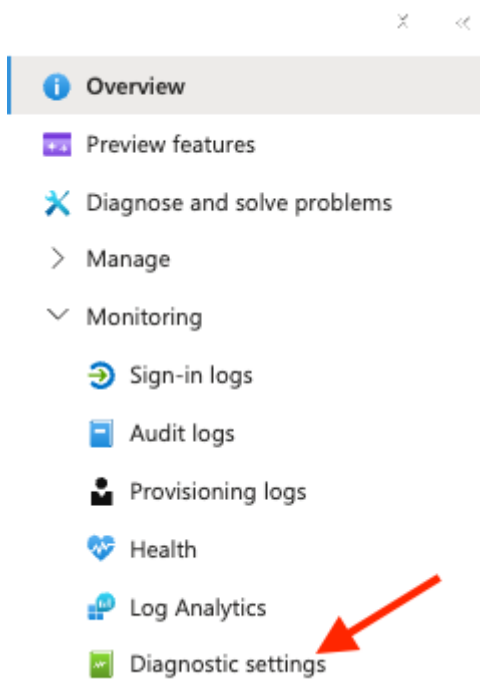
ステップ10：イベントハブへのエントリID監査ログストリーミングを設定します

1) Entra IDテナント設定に戻ります。



IDテナント設定の検索とエントリへの移動

2)左側のメニューから、Monitoring > Diagnostic Settingsの順に選択します。



診断設定の監視

3) Diagnostic settings > Generalの順に選択し、+Add diagnostic settingをクリックします。

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

新しい診断設定の追加

4)必要な名前を診断設定に割り当て、ログを記録するにはAuditLogsチェックボックスにチェックマークを入れ、さらにStream to an event hubチェックボックスにチェックマークを入れます。上記の設定でメモした値を参照し、完了したらSaveをクリックします。

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

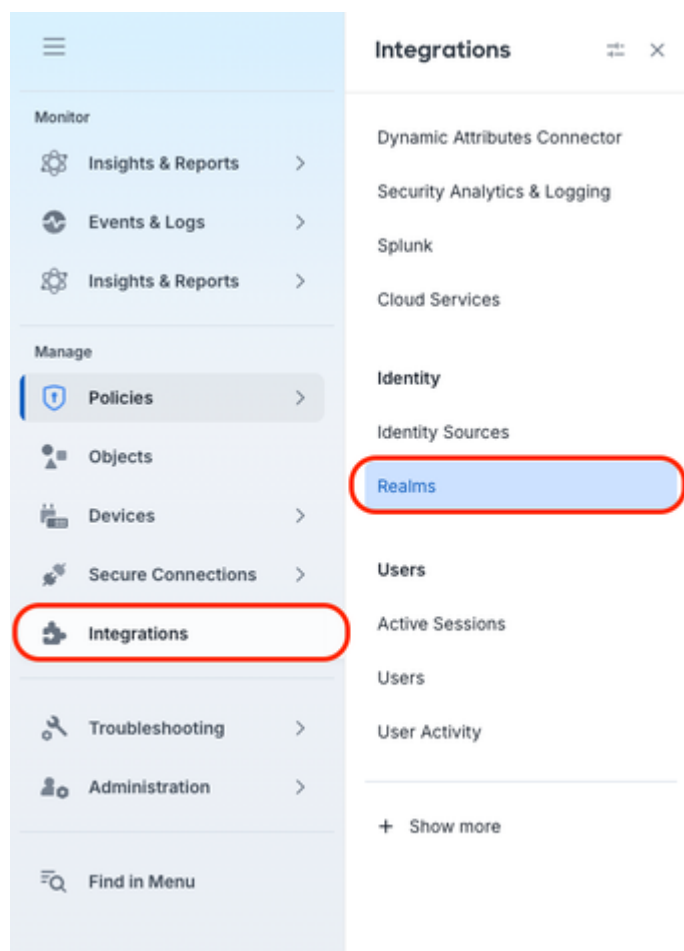
Event hub policy name

☐ Send to partner solution

フェーズ4: AzureとFMC/FTDのアクティブ認証構成を統合する

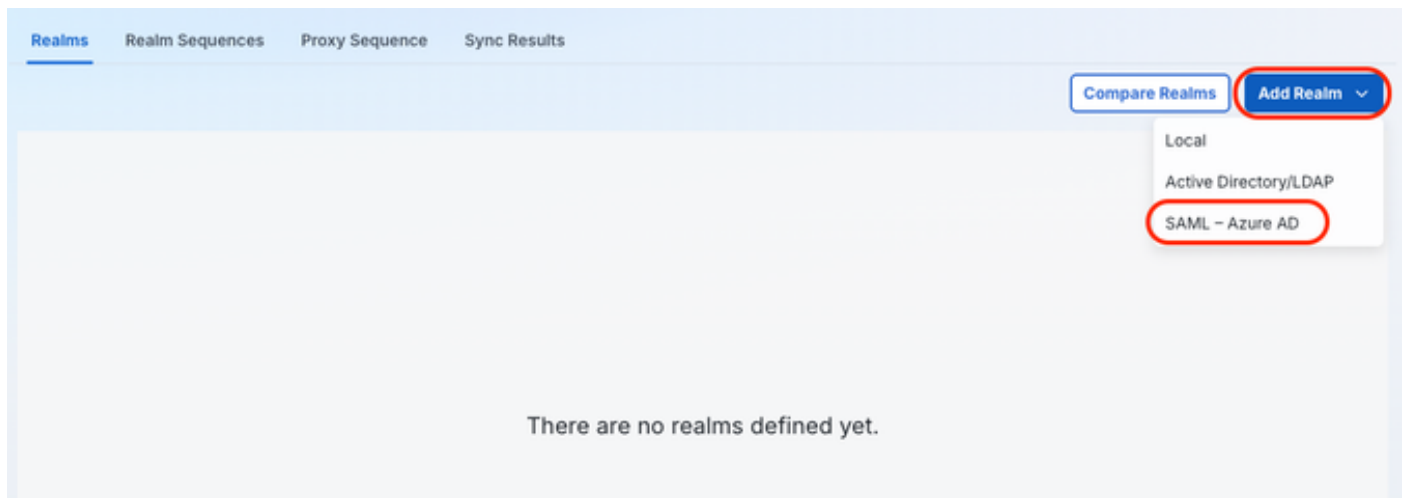
手順1: FMCウィザードを使用してAzure SAML/Entra IDレルムを構成する

1) FMC内で、Integrations > Identity > Realmsの順に選択します。



アイデンティティ・レルムの構成

2) Add Realmドロップダウンリストをクリックし、SAML - Azure ADを選択します。



SAML Azure ADレルムの追加

3) Azureレルムの用途を説明するために名前と説明を割り当て、構成の種類のドロップダウンリストからAzure ADを使用してパッシブに認証するか、Azure ADを使用してキャプティブポータルを使用するを選択してください。[next] をクリックします。

Azure ADレルム設定の構成

4) ベースURLとして、以前に設定したFQDNオブジェクトを選択します。次に示す文字列フォーマットでエンティティIDを入力します。

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

- SAMLエンティティIDサフィックス (次の構成例では緑色の下線) を設定する場合は、サフィックスが環境内の他のSSO実装間で一意であることを確認してください。この値は、Azure SAML構成とも一致している必要があります。ベースURLは設定全体を通じて同じままです。
- Assertion Consumer Services(ACS)URLは自動的に入力され、変更できません。
- FMCの前述のワークフローステップのDevices > Certificatesの下に登録されているService Provider (SP) Certificateを選択します。
- これらの値を入力したら、Download Service Provider Metadataをクリックして設定プロセスを簡単にし、予期される値がAzureに書き込まれていることを確認します。

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](#)

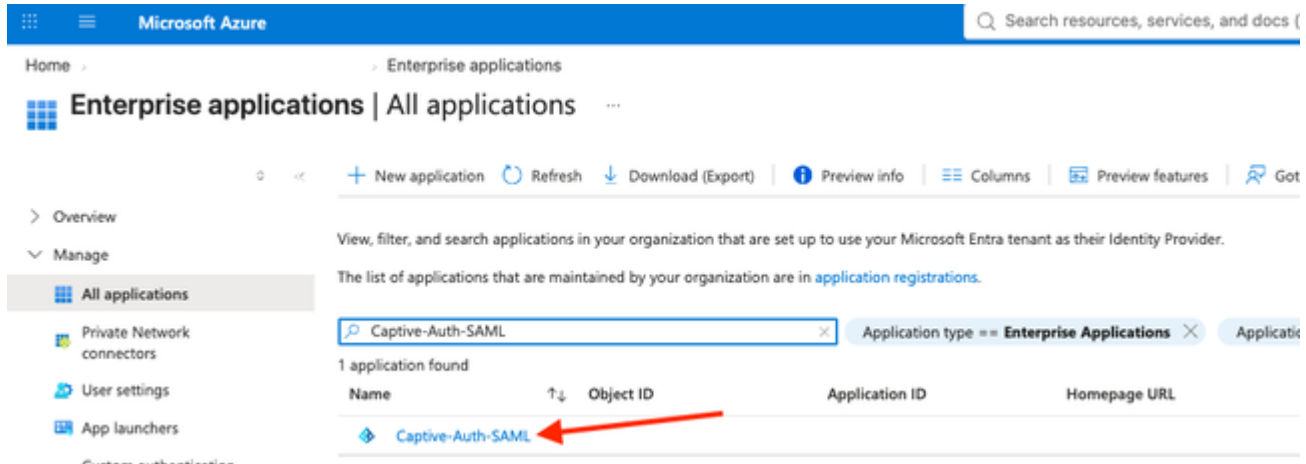
Next

ベースURLとエンティティIDの設定、およびSAMLメタデータのダウンロード

5) Nextをクリックして、レルム設定のシーケンス3に移動します。

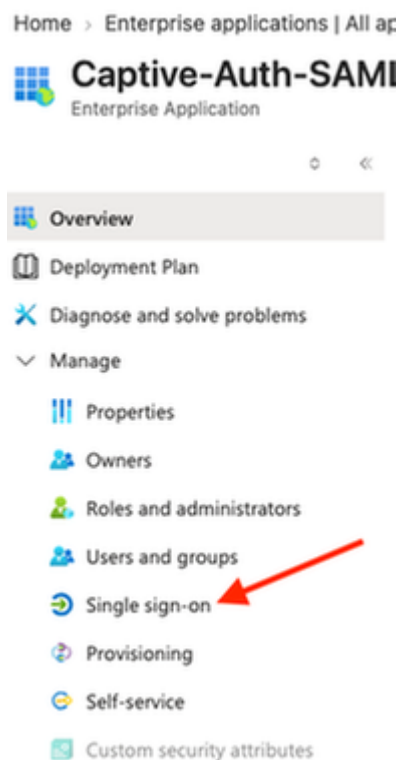
手順2: FMCで構成されたSAML SPメタデータをAzure Enterpriseアプリケーションに実装する

1) Azureに戻り、Enter ID > Manage > Enterprise Applicationsの順に選択します。以前に作成したMicrosoft Entra SAML Toolkitエンタープライズアプリケーションのインスタンスを検索します。



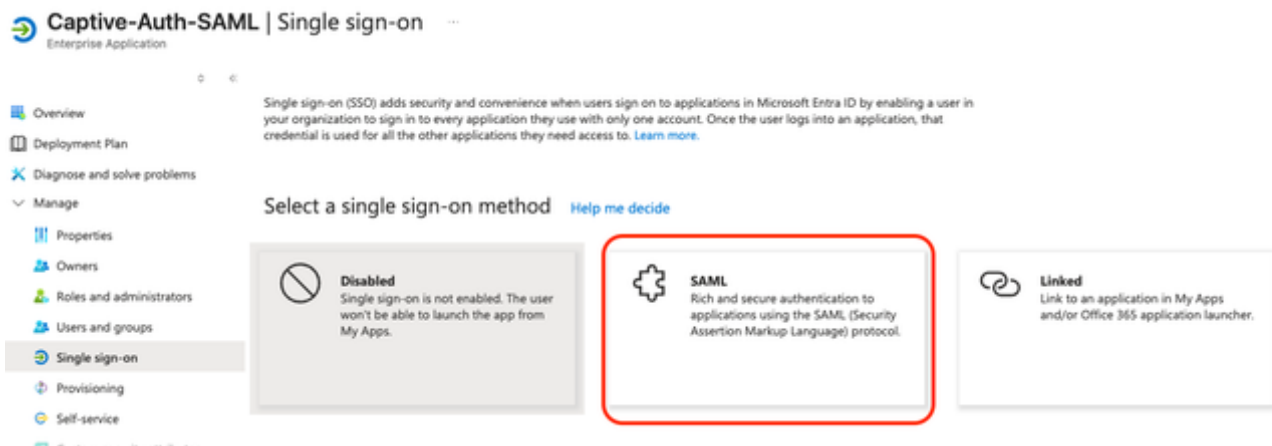
Microsoft Entra SAMLツールキットアプリケーションの検索

2) サイドのナビゲーションメニューから、管理>シングルサインオンを選択します。



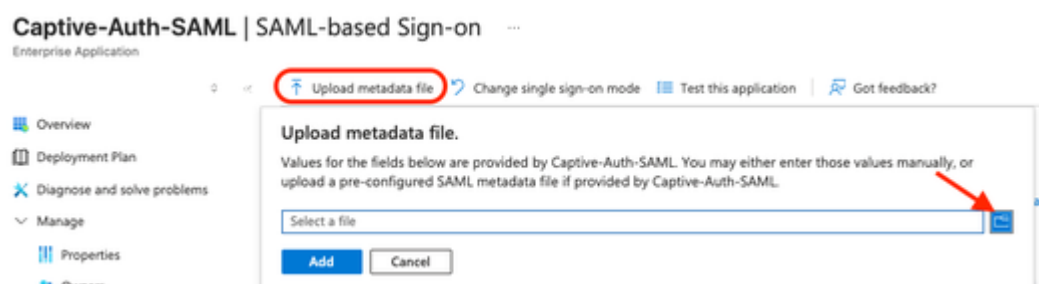
シングルサインオン構成の管理

3) SAMLシングルサインオン(SSO)モードをクリックします。



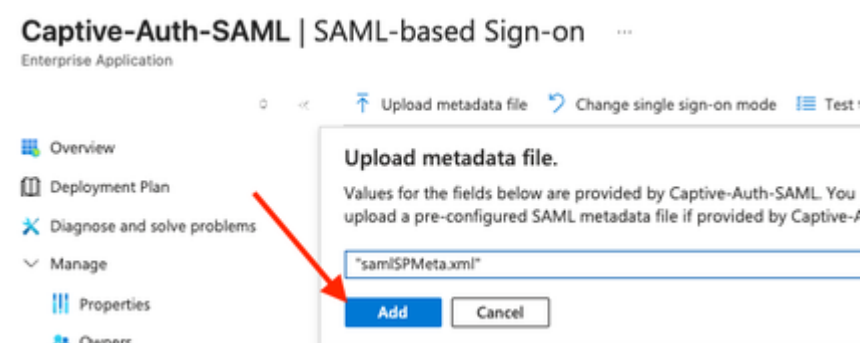
SAMLシングルサインオンモードの選択

4) Upload metadata fileをクリックし、青色のフォルダアイコンをクリックして、ローカルファイルシステムを参照し、FMCからダウンロードしたSAMLメタデータファイルを探します。



ファイアウォール管理センターからのメタデータファイルのアップロード

5)アップロードが完了したら、Addをクリックします。



SAML構成アプリケーションの追加

6)基本SAML設定のサイドパネルが表示され、自動的にアップロードされて適用されたFMC生成のSPメタデータXMLファイルから、識別子 (エンティティID) やACS URLなどの値が抽出されます。ただし、サインオンURLは入力されないため、保存する前に入力する必要があります。

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.



基本的なSAML構成の抽出

7)表示されたサインオンURLパターンを使用し、値をコピーアンドペーストして、完了したら上

部のSaveをクリックします。

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)

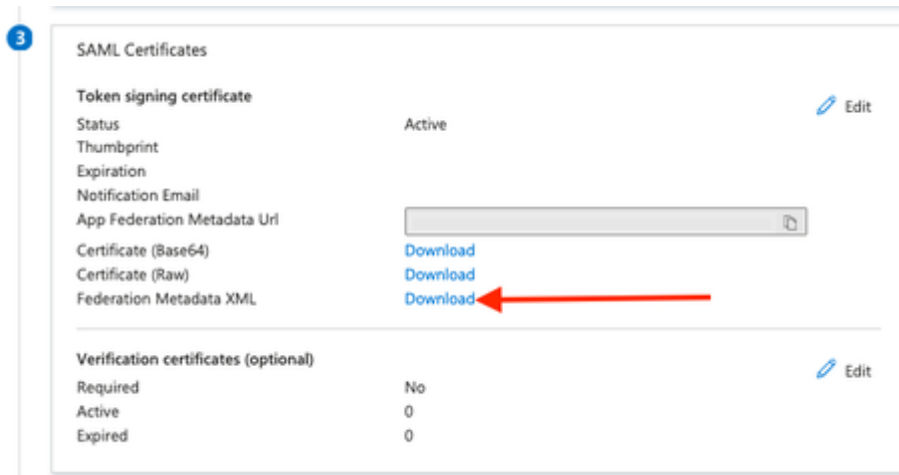
This URL is used to send the SAML logout response back to the application.



サインオンURL構成エントリ

SAML Certificatesまでスクロールダウンして、Azureで生成されたフェデレーションメタデータ

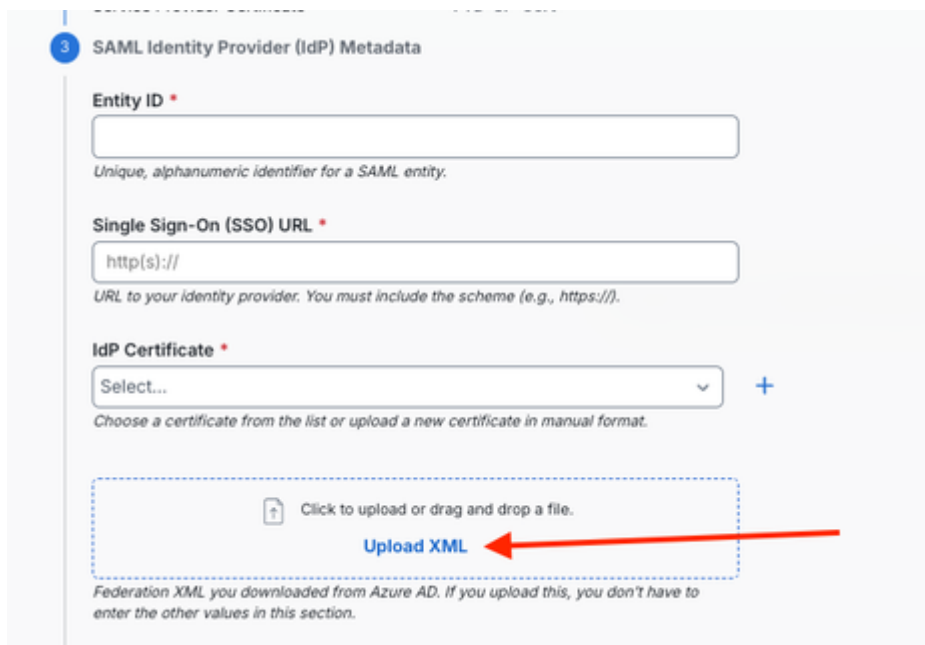
XMLファイルをエクスポートし、Cisco Secure FMCにインポートします。



フェデレーションメタデータXMLファイルのエクスポート

手順3: FMCウィザードを使用してAzure SAML/Entra IDレルムを構成する (続き)

1) FMCに戻ります。シーケンス3、SAML Identity Provider (IdP) Metadataの下で、AzureからダウンロードしたエクスポートしたフェデレーションメタデータXMLファイルをFMCにアップロードし、必要な値を自動入力します。



フェデレーションメタデータXMLファイルのアップロード

2)アップロードされると、次に示すように値が入力されます。

3 SAML Identity Provider (IdP) Metadata

Entity ID *

https://sts.windows.net/

Unique, alphanumeric identifier for a SAML entity.

Single Sign-On (SSO) URL *

https://login.microsoftonline.com/

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

IdP Certificate *

Certificate-

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

Click to upload or drag and drop a file.

Upload XML

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

Next

自動入力されたSAML IDプロバイダー値



注：出力の一部を図に示します。

3)実装プロセス全体で収集した値を、次の時点までに入力します。

- アプリの登録
 - アプリケーション (クライアント) ID
 - クライアントシークレット
 - ディレクトリ (テナント) ID
- イベントハブ
 - EH名前空間ホスト名
 - EH名前空間のプライマリ接続文字列
 - EHインスタンス (イベントハブ) 名
 - EHコンシューマグループ名

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

アプリケーションおよびイベント・ハブ情報の入力

入力したら、Testをクリックして接続を確認し、提供された情報でAzureに到達できることを確認します。



注：該当する場合は、除外/含めるユーザグループとエントリ設定が一致していることを確認してください

4)ウィザードの最後の手順では、SAMLキャプティブポータルユーザのタイムアウトを設定できます。デフォルトは 1440 分です。

5 User Session Timeout

SAML Captive Portal Users

1440 Minutes Range 0-35791394

キャプティブポータルタイムアウトの設定

5) Nextをクリックして続行します。

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

Azure ADレルムの構成を進める

6)ウィザードは、実装された設定の概要を示します。 入力した値を検証して確認したら、要約の最後にあるSaveをクリックします。

5 User Session Timeout Edit

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

Cancel Save

レルム構成のサマリーの保存ボタン

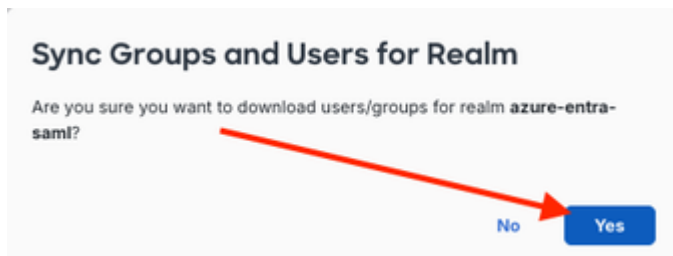
ステップ4：ダウンロードしたユーザの確認

1) Azure Entraからユーザーをダウンロードできることを確認します。これには、Integrations > Identity > Realms ワークフローでDownload Nowボタンをクリックします。

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

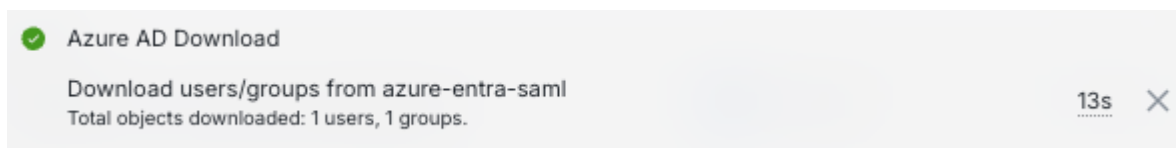
Azure ADからのユーザーのダウンロード

2)ダイアログプロンプトに対して、Yesをクリックします。



Azure ADからのユーザーのダウンロードの確認

3)ダウンロードタスクで1人のユーザと1つのグループがダウンロードされます。これは Notifications > Tasksで確認できます。

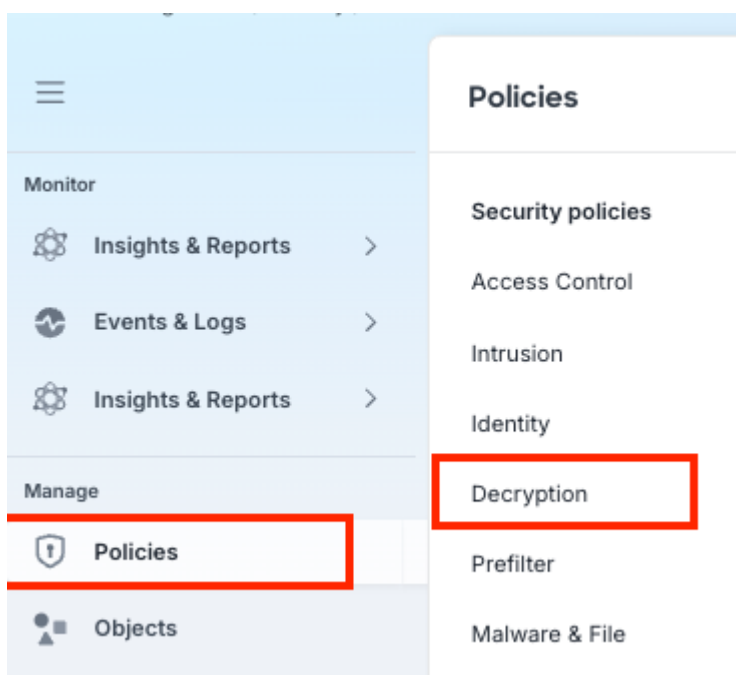


Azure ADからユーザーをダウンロードするための通知エントリ

フェーズ5:FMCでのポリシーの設定

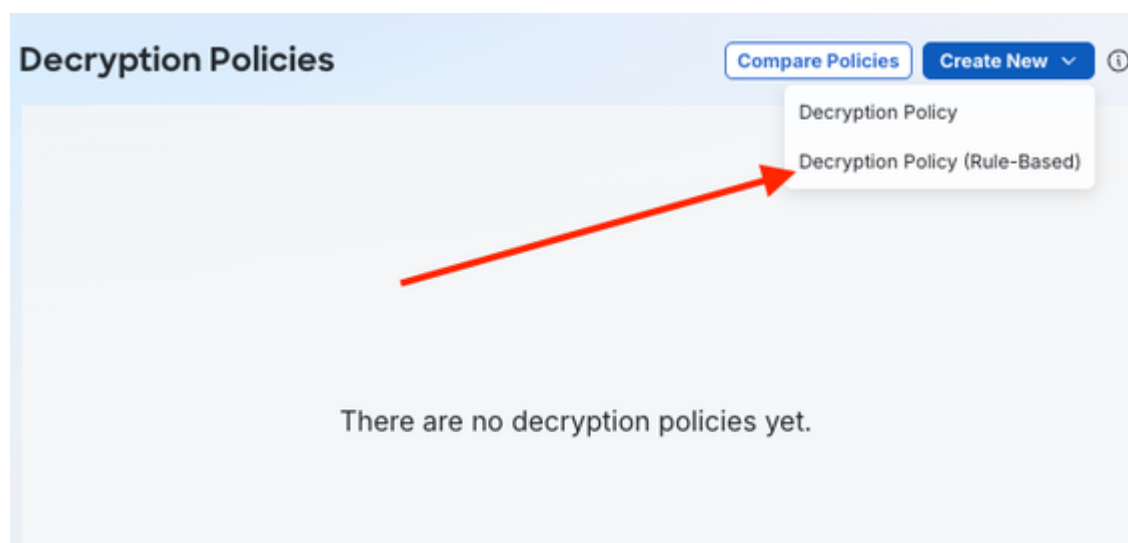
ステップ1：復号ポリシーの設定

1) FMCで、Policies > Security Policies > Decryptionの順に選択します。



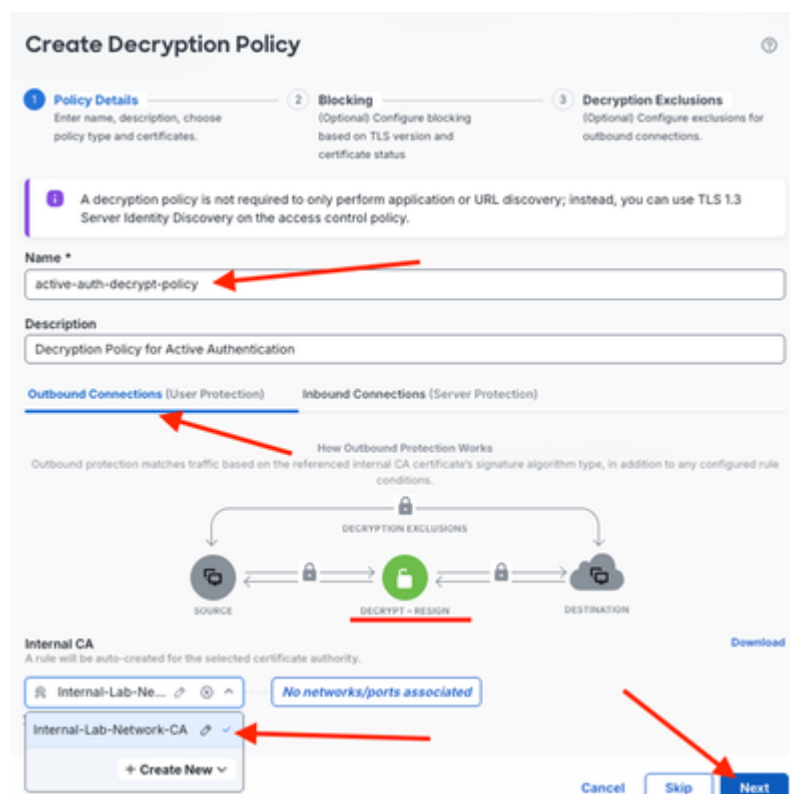
復号化ポリシーに移動

2) Create Newドロップダウンリストをクリックして、Decryption Policy (Rule-Based)を選択します。



新しいルールベースの暗号化解除ポリシーの作成

3)新しいルールベースの復号化ポリシーに名前を割り当て、必要に応じて説明を割り当て（必要な場合）、発信接続（ユーザ保護）タブオプションをクリックして、キャプティブポータル認証（アクティブ認証）に必要な復号化－再署名機能を実装します。



アウトバウンド接続ポリシーの実装の詳細

4)同じダイアログ内の該当するドロップダウンリストから、以前適用した内部CAを選択します。

[next] をクリックします。

5)必要に応じてオプションをカスタマイズします。

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](#)

復号ポリシーオプションのカスタマイズ

6)この例では、必要なPolicy Detailsを除いて、デフォルトが使用されます。Create Policyをクリックして、設定ウィザードを完了します。

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**

New

Create Policy

最終的な復号化ポリシーの作成

ステップ2：復号ポリシールールを設定

1)ルールベースの復号ポリシーのデフォルトレイアウトを次に示します。ルール3（非復号可能なドメイン名の事前に割り当てられたリストを参照）やルール6（非復号可能としてタグ付けされたアプリケーションを参照）などのデフォルトの有効なルールに一致しないトラフィックは、ルール7の下でDecrypt - Resignアクションの対象となります。これらのデフォルトは、デフォルトアクションとともに、必要に応じて変更できます。デフォルトでは、他のルールと一致しないトラフィックはDo Not Decryptとして設定されます。

Azure Authentication Serviceのトラフィックは検査のために暗号化を解除してはならず、専用のルールが作成されます。+ルールの追加をクリックして開始します。

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

規則を追加し、既定の規則に基づく復号化レイアウトを表示する

2)新しい復号ポリシールールエントリに名前を割り当て、ActionドロップダウンリストからDo not decryptを選択し、ルールを最も具体的でないルールに配置します。送信元/宛先ゾーンも、ルールをさらに絞り込むために実装されます。

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

Do Not Decryptルールの設定

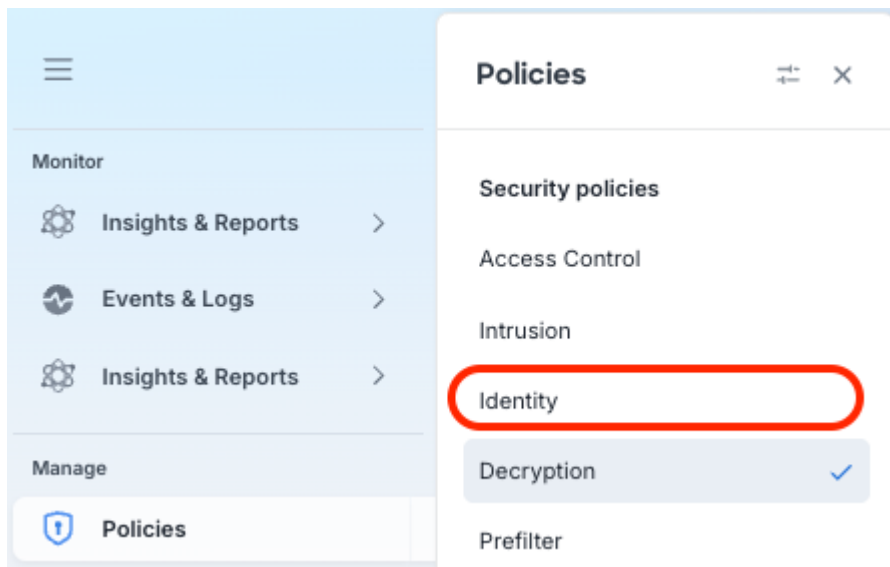
3)ルールを追加する前に、アプリケーションタブをクリックし、Azure Authentication Serviceア

Q

Azure 認証サービスアプリケーションルールの追加

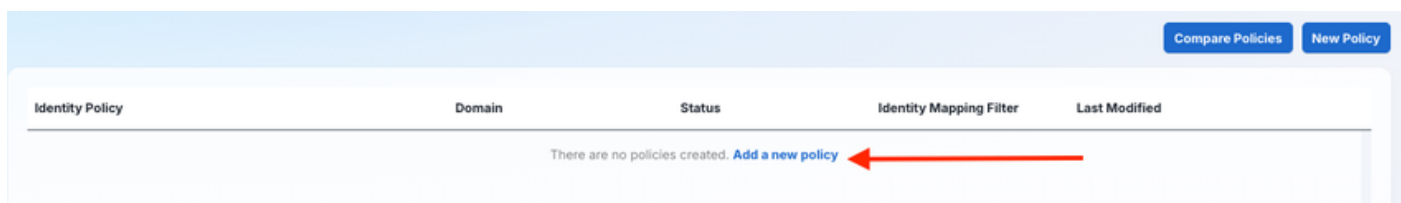
復号化ポリシーの保存

Q



アイデンティティポリシーの作成

2)新しいアイデンティティポリシーを作成し、Add a new policyをクリックします。



新しいアイデンティティポリシー設定の追加

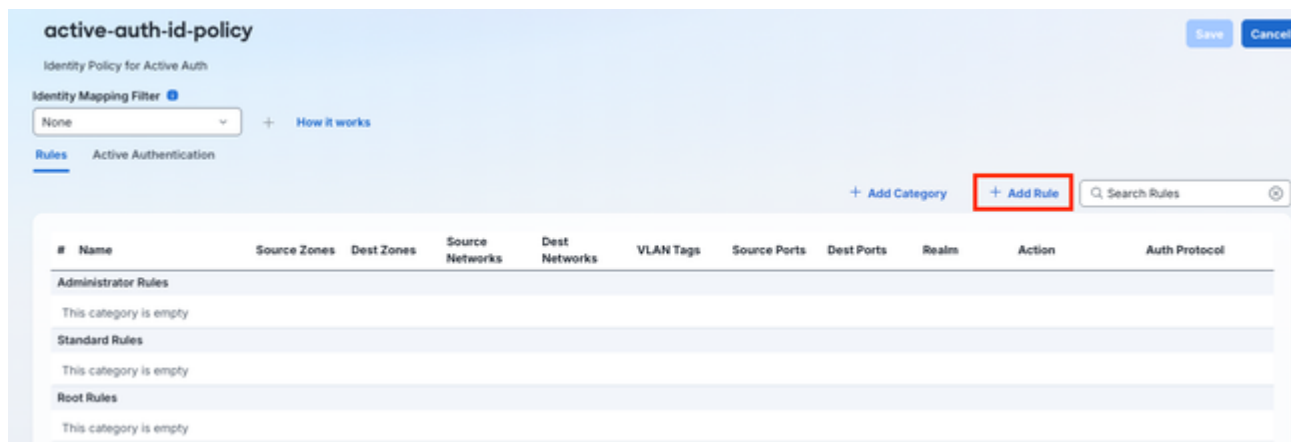
3)新しいアイデンティティポリシーに名前と、必要に応じて説明を割り当てます。[Save] をクリックします。

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

新しいアイデンティティポリシーの命名

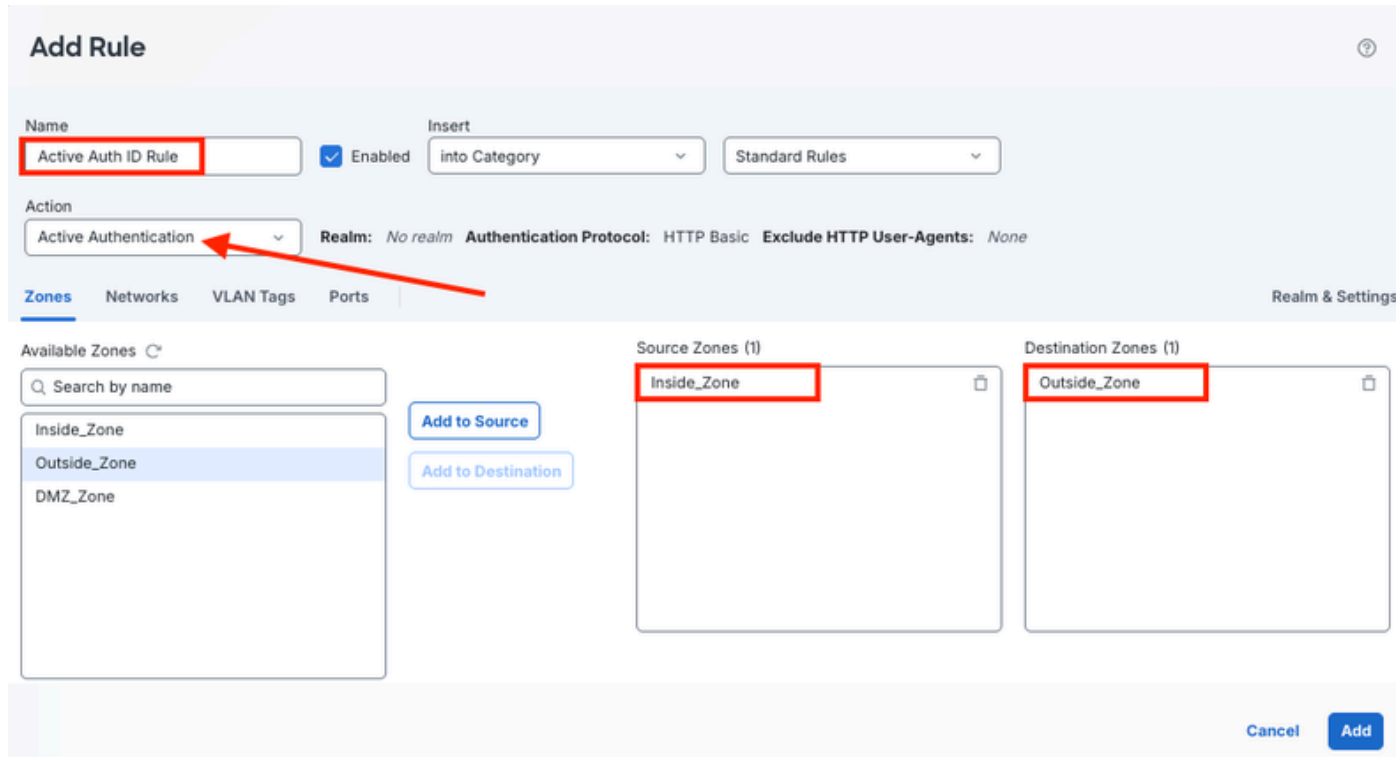
ステップ4：アイデンティティポリシールールの設定

1)+ルールの追加をクリックして、新しいルールを追加します。



新しいアイデンティティポリシールールの追加

2)新しいルールに名前を付け、ActionドロップダウンリストからActive Authenticationを選択して、アクティブ認証を実行するためにルールに一致する必要がある特定のゾーン/ネットワークを絞り込みます。



アクティブ認証ルールの設定の構成

3) Addをクリックする前に、Rule EditorでRealm and Settingsタブをクリックします。前のステップで設定したルールが認証ルールとして選択されていることを確認し、Addをクリックします

o

Add Rule

Name: Active Auth ID Rule ☒ Enabled Insert into Category: Standard Rules

Action: Active Authentication **Realm:** azure-entra-saml (SAML) **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

アイデンティティルールのレルムと設定の構成

4)ルールが追加され、設定されます。[Save] をクリックします。

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											

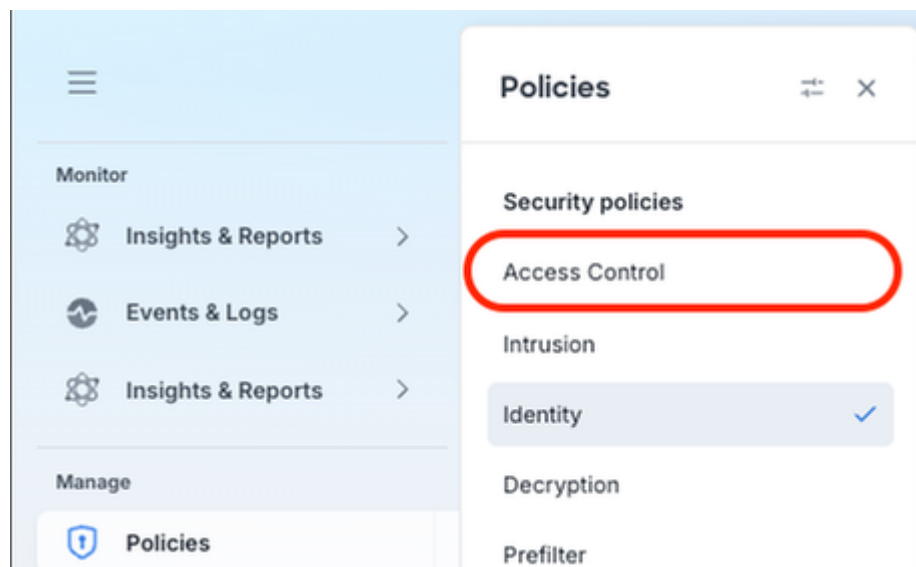
You have unsaved changes [Save](#) [Cancel](#)

アイデンティティポリシールール設定の保存

ステップ5：アクセスコントロールポリシーの設定

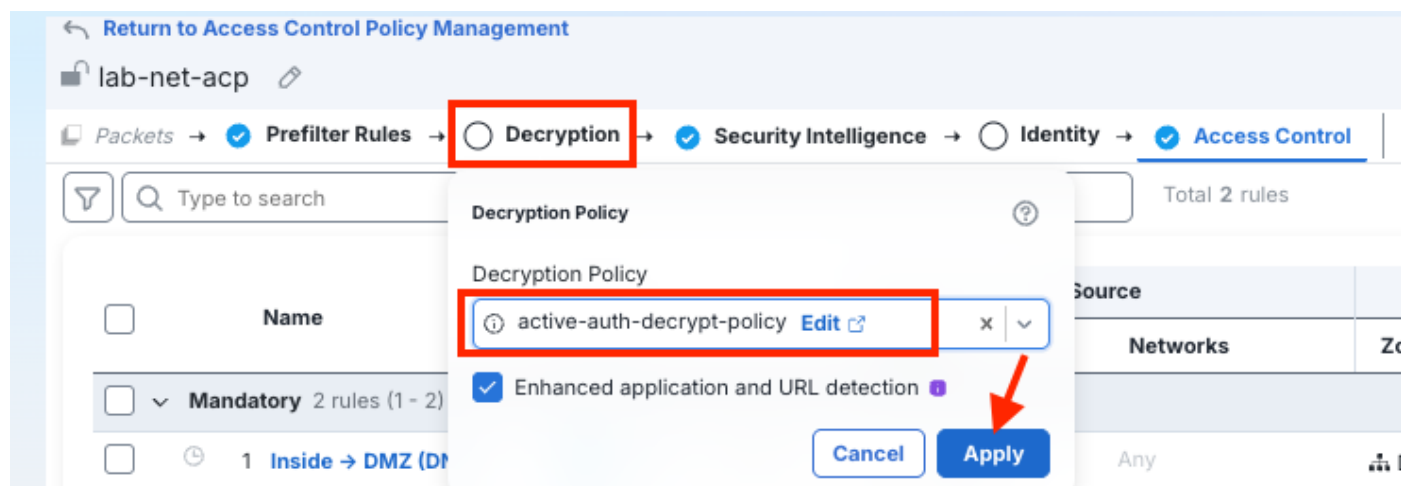
1) Policies > Security Policies > Access Controlの順に選択し、FTDが割り当てられているAccess

Control Policyをクリックします。



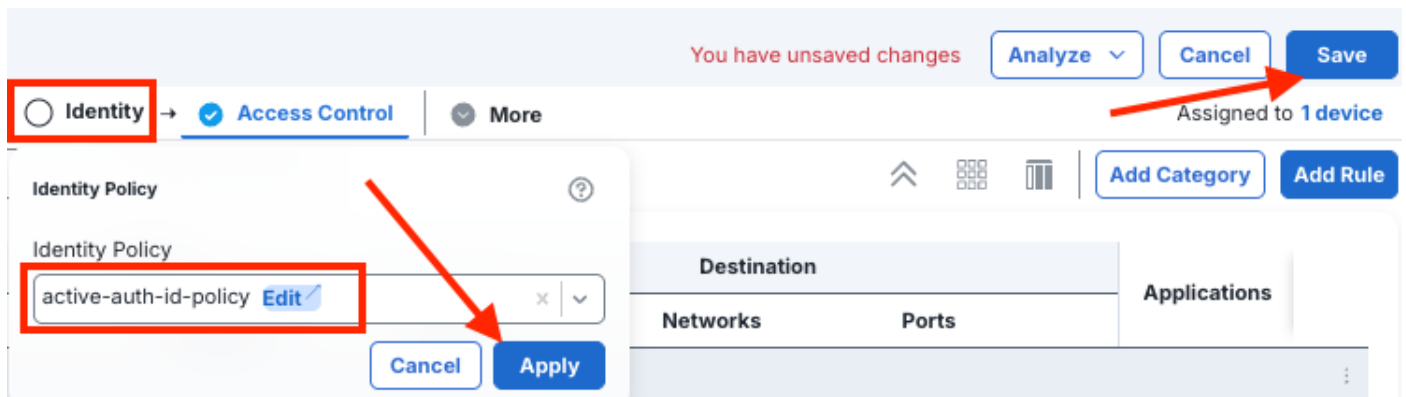
アクセスコントロールポリシーの設定

2)前の手順で設定した復号化ポリシーがアクセスコントロールポリシーに適用されていることを確認します。



アクセス制御への復号化ポリシーの適用

3)前の手順で設定したアイデンティティポリシーがアクセスコントロールポリシーにも適用されていることを確認します。ポリシーの変更を保存します。



アクセスコントロールへのアイデンティティポリシーの適用

4)アクティブ認証が成功した後に、クライアントのデータプレーントラフィックがセキュアファイアウォールを通過することを許可するルールが存在することを確認します。次の例では、ラボ環境に基づき、より幅広いルールセットを使用しています。

☐	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)								

ユーザデータプレーントラフィックルールセット

ステップ6:Cisco Secure Firewallデバイスへの設定の導入

デプロイが完了すると、トラフィックを送信するクライアントは、Azure Entraでアクティブ認証を実行するようにMicrosoftサインインWebページで求められます。

ここで説明するプロセスの詳細については、「[アクティブ認証用のMicrosoft Azure AD \(SAML\)レールの作成 \(キャプティブポータル\) – 章：FMC Device Config Guide 10.xのレール](#)」を参照してください。

確認

このセクションでは、設定が正常に動作していることを確認します。

GUI

FMCでユーザセッションとアクティビティを検証します。

- Integrations > Users > Active Sessionsの順に選択します。

The screenshot shows the Cisco FMC interface with the breadcrumb 'Integrations / Users / Active Sessions'. The left sidebar has 'Monitor' selected. The main content area shows a table of active sessions. The table has columns: Login Time, RealmUsername, 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	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アクティブセッションの出力

- Integrations > Users > User Activityの順に選択します。

The screenshot shows the Cisco FMC interface with the breadcrumb 'Integrations / Users / User Activity'. The left sidebar has 'Monitor' selected. The main content area shows a table of user activities. The table has columns: Time, Username, Event, Realm, Discovery Application, Authentication Type, IP Address, and Start Port. Two activities are listed, both with a time of 2026-10-07 02:10:02, username '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		

FMCユーザアクティビティ出力

Azureで、Microsoft Entra Admin Center:

- エンタープライズアプリケーションをフィルタリングし、該当するアプリケーションを検索またはクリックします。

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation pane has 'Enterprise apps' highlighted with a red box. The main content area is titled 'Enterprise applications | All applications'. It features a search bar with 'captive-' entered, also highlighted with a red box. Below the search bar, there is a list of applications. The first application in the list is 'Captive-Auth...', which is highlighted with a red box and has a red arrow pointing to it from the 'Custom authentication extensions' link in the 'Manage' section. The 'Manage' section also has 'All applications' highlighted with a red box. The 'Overview' section shows 'Overview' and 'Diagnose and solve problems' links. The 'Security' section shows 'Conditional Access', 'Consent and permissions', and 'Application policies' links.

Azure Entra Admin Center Enterprise Appsのナビゲーション

- Activity > Sign-in logsの順に選択します。

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?

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

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

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アプリケーションサインインアクティビティログ

CLI

- FTD CLIでは、SAMLおよびキャプティブポータルの応答に関する統計情報を確認できます

<#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
```

トラブルシューティング

キャプティブポータルのデバッグ

- `system support captive-portal-debug` コマンドをFTDで使用できます。次の出力では、デバッグを有効にする方法を示しています。また、キャプティブポータルのフローを理解しやすいように、出力の主要なセグメントも示しています。

```
<#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
...
```

ユーザIDダンプ

- FTDで現在のユーザID状態データのスナップショットを取得するには、FTD CLIでsystem support firewall-engine-dump-user-identity-dataコマンドを実行します。

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

```
Successfully commanded snort.
```

```
>
```

- expertモードのCLIで、FTDデバイスのローカル管理者クレデンシャルでログインし、
/ngfw/var/sf/user_enforcement/user_identity.dumpにあるダンプされたファイルの内容を表示
します。

```
<#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:  
-----
```

```
...
```

考えられる問題

キャプティブポータルの不明な認証局

問題：認証が試行されると、クライアントブラウザが「unknown issuer」エラーを返します。

原因：内部の証明機関がクライアントブラウザ内で信頼されていない。

解決策：ブラウザ内でCAが信頼できることを確認します。次の例は、内部CA証明書が信頼されていることを示しています。

キャプティブポータル「サーバが見つかりません

問題：クライアントブラウザがキャプティブポータルをロードしようとする、ベースURLに到達しようとしているときに、ベースURLに「Server Not Found」が返されます または類似しています。

考えられる原因:DNS到達可能性またはDNSの設定ミス。

解決策：クライアントに、Aレコードを解決するように設定された適切なDNSサーバがあることを確認します。サーバにFQDNにマッピングされたAレコードがあること、およびサーバが到達可能で応答できることを確認します。

関連情報

- [アクティブ認証用のMicrosoft Azure AD \(SAML\)レルムの作成 \(キャプティブポータル \) - FMCデバイス構成ガイド10.x](#)
- [Azure Event Hubドキュメント](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。