

보안 방화벽에서 Azure Entra 종속 포털 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[다이어그램](#)

[엔드포인트, FTD 및 Azure Entra 간의 종속 포털](#)

[구성](#)

[1단계: 초기 FMC 및 DNS 컨피그레이션](#)

[1단계: CSDAC\(Cisco Dynamic Attributes Connector\) 활성화](#)

[2단계: FTD 인그레스 인터페이스를 나타내는 정규화된 도메인 이름 네트워크 개체 만들기](#)

[3단계: DNS A 레코드 구성](#)

[2단계: 공개 키 인프라 컨피그레이션](#)

[1단계: FMC에 내부 CA 인증서 가져오기](#)

[2단계: CA로 서비스 공급자 인증서 서명](#)

[3단계: FTD에 SP 인증서 구축](#)

[3단계: Azure 구성](#)

[1단계: SAML 토크용 Centera 엔터프라이즈 애플리케이션 생성](#)

[2단계: Entra ID 앱 등록 구성](#)

[3단계: 앱 등록을 위한 Microsoft Graph API 권한을 구성합니다.](#)

[4단계: EH\(Event Hub\) 네임스페이스 구성](#)

[5단계: 이벤트 허브 네임스페이스에서 공유 액세스 정책 선택 또는 만들기](#)

[6단계: EH 네임스페이스에서 SAS\(Shared Access Signature\) 정보 수집 및 메모](#)

[7단계: 이벤트 허브 네임스페이스 내에서 이벤트 허브 인스턴스 만들기](#)

[8단계: 이벤트 허브 네임스페이스 내에서 이벤트 허브 인스턴스 소비자 그룹 만들기](#)

[9단계: 수집된 값 확인](#)

[10단계: 이벤트 허브에 대한 Entra ID 감사 로그 스트리밍 구성](#)

[4단계: Azure 및 FMC/FTD 활성 인증 컨피그레이션 통합](#)

[1단계: FMC 마법사를 사용하여 Azure SAML/Entra ID 영역 구성](#)

[2단계: Azure 엔터프라이즈 응용 프로그램에서 FMC 구성 SAML SP 메타데이터 구현](#)

[3단계: FMC 마법사를 사용하여 Azure SAML/Entra ID 영역 구성\(계속\)](#)

[4단계: 다운로드한 사용자 확인](#)

[5단계: FMC에서 정책 구성](#)

[1단계: 암호 해독 정책 구성](#)

[2단계: 암호 해독 정책 규칙 구성](#)

[3단계: ID 정책 생성](#)

[4단계: ID 정책 규칙 구성](#)

[5단계: 액세스 제어 정책 구성](#)

[6단계: Cisco Secure Firewall 장치에 컨피그레이션 구축](#)

[다음을 확인합니다.](#)

[GUI](#)

[CLI](#)

[문제 해결](#)

[종속 포털 디버그](#)

[사용자 ID 덤프](#)

[가능한 문제](#)

[종속 포털 알 수 없는 인증 기관](#)

[종속 포털 "서버를 찾을 수 없음](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Secure Firewall에서 종속 포털(활성 인증)과 함께 사용할 Microsoft Azure Entra ID의 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

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

이벤트 허브 생성을 위해 Azure에서 사용 가능한 표준 가격 책정 계층이 있어야 합니다. 또한 내보내기 제어 기능을 통해 활성화된 Smart Licensing으로 디바이스를 활성화해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure FTD 버전 10.0
- Cisco Secure FMC 버전 10.0

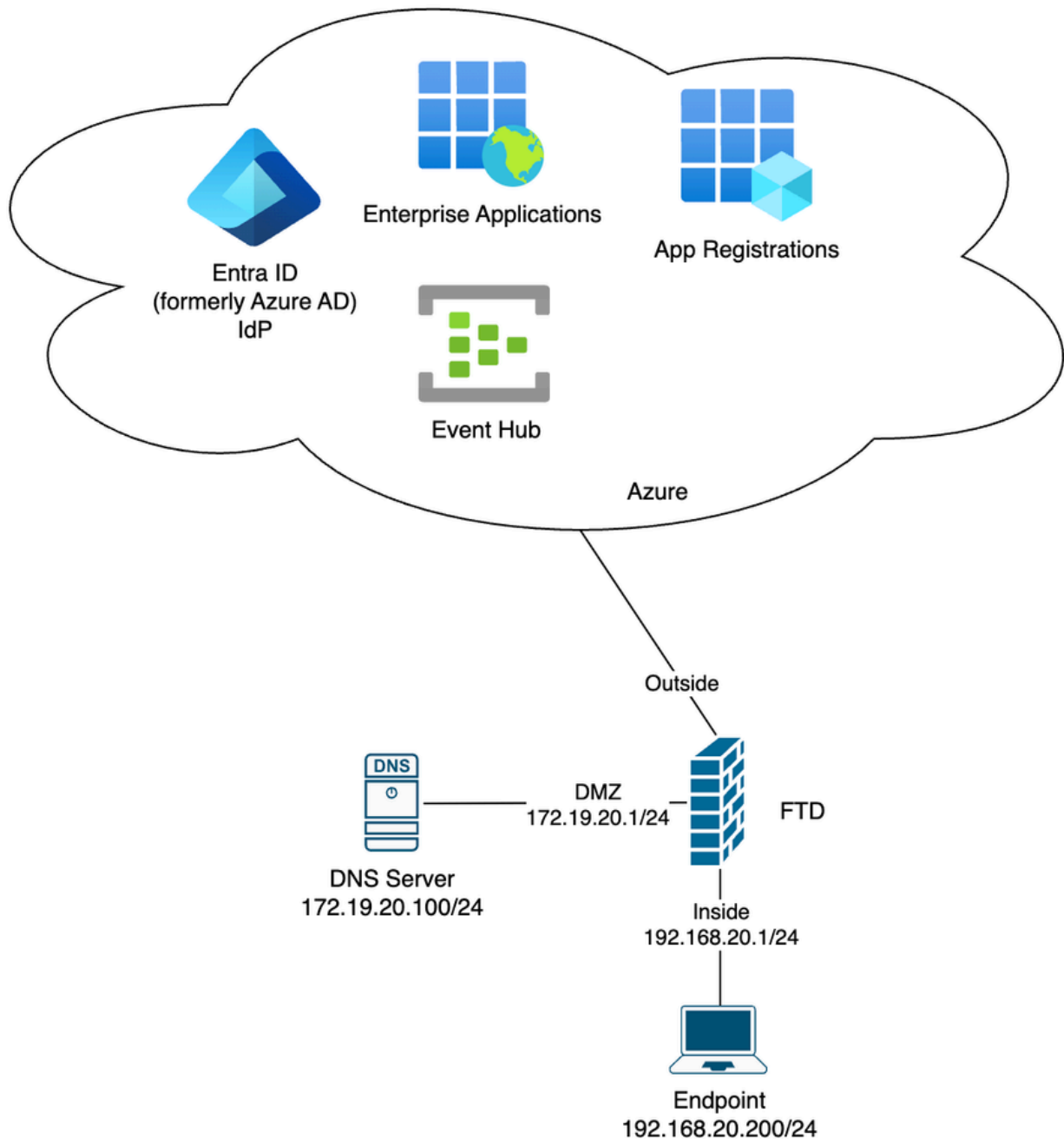
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

기존의 IP 기반 보안 아키텍처가 동적인 하이브리드 작업 환경에 발맞추는 데 어려움을 겪는 가운데 , SAML 통합을 지원하는 Cisco Secure Firewall Active Authentication은 강력한 ID 중심 솔루션을 제공합니다. Microsoft Azure AD(Entra ID)를 중앙 집중식 ID 공급자로 활용함으로써 관리자는 이 구성을 통해 정적 네트워크 규칙을 벗어나 휘발성 네트워크 주소보다는 확인된 사용자 ID를 기반으로 세분화된 액세스 제어를 시행할 수 있습니다. 이러한 통합은 원활한 SSO(Single Sign-On) 및 필수 MFA(Multi-Factor Authentication)를 통해 사용자 환경을 간소화하는 동시에 경계가 없는 네트워크에서 엄격한 가시성 및 정책 시행을 유지하는 통합된 보안 상태를 보장합니다.

다이어그램

엔드포인트, FTD 및 Azure Entra 간의 종속 포털



EndPoint와 Azure Entra 사이의 종속 포털

구성

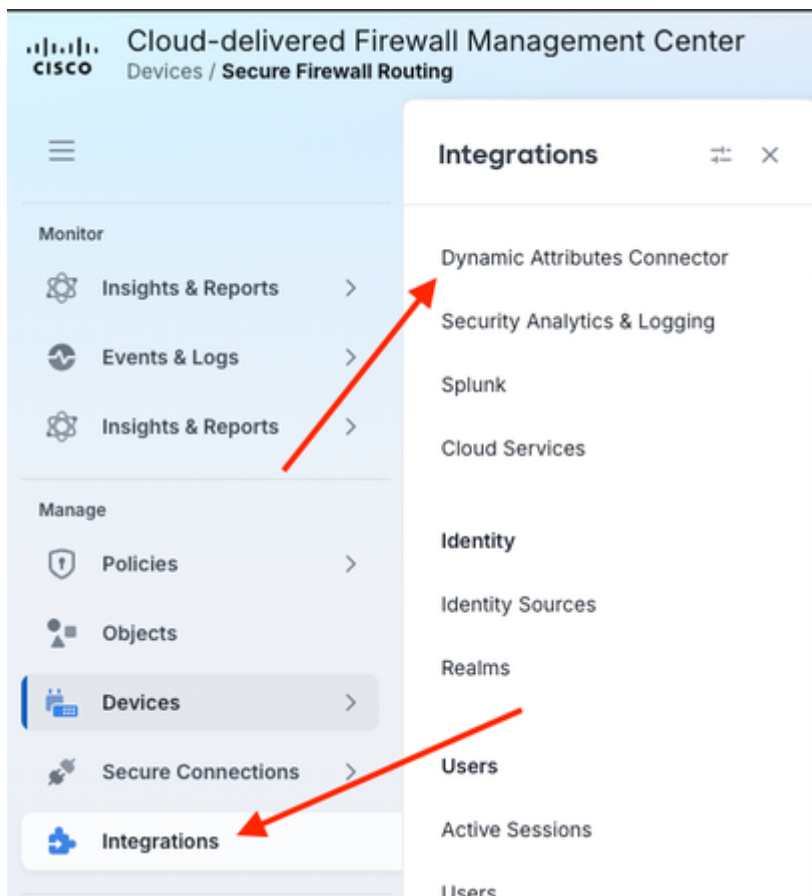
1단계: 초기 FMC 및 DNS 컨피그레이션



참고: 이 실습에서는 클라우드 기반 cdFMC(Firewall Management Center)를 사용합니다. 그러나 온프레미스 FMC의 단계는 동일합니다.

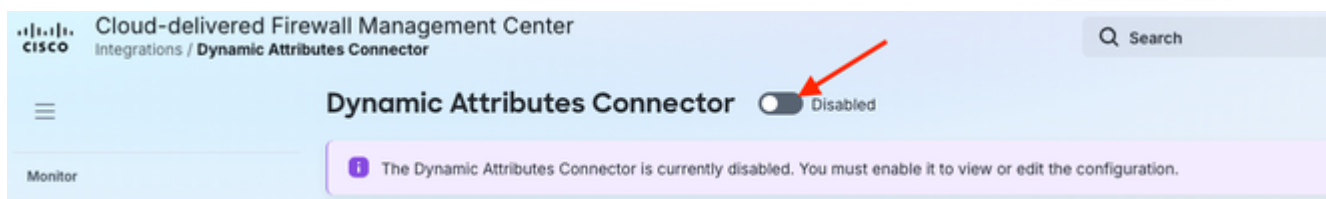
1단계: CSDAC(Cisco Dynamic Attributes Connector) 활성화

1) Integrations(통합) > Dynamic Attributes Connector(동적 특성 커넥터)를 선택합니다.



Integrations Dynamic Attributes Connector(통합 동적 특성 커넥터)를 선택합니다.

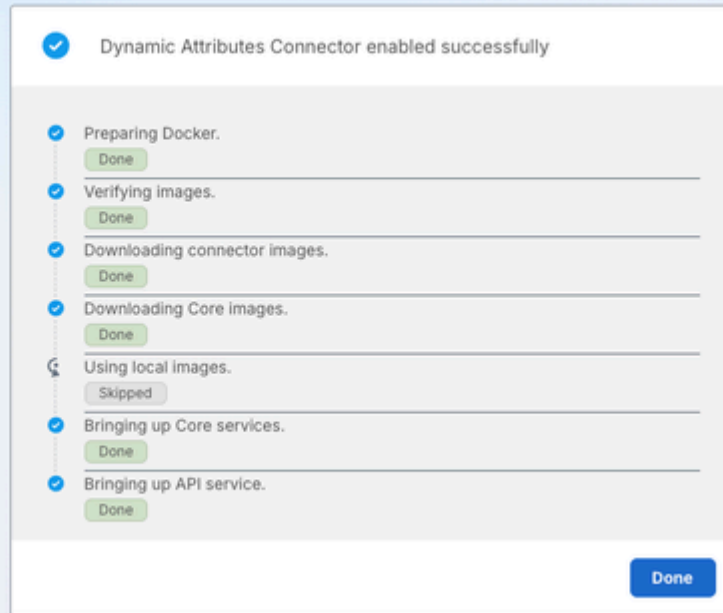
2) Disabled 문자열 옆에 있는 컨트롤을 클릭하여 CSDAC를 활성화합니다.



Cisco Dynamic Attributes 커넥터 활성화

c) CSDAC 활성화가 완료되면 Done(완료)을 클릭합니다.

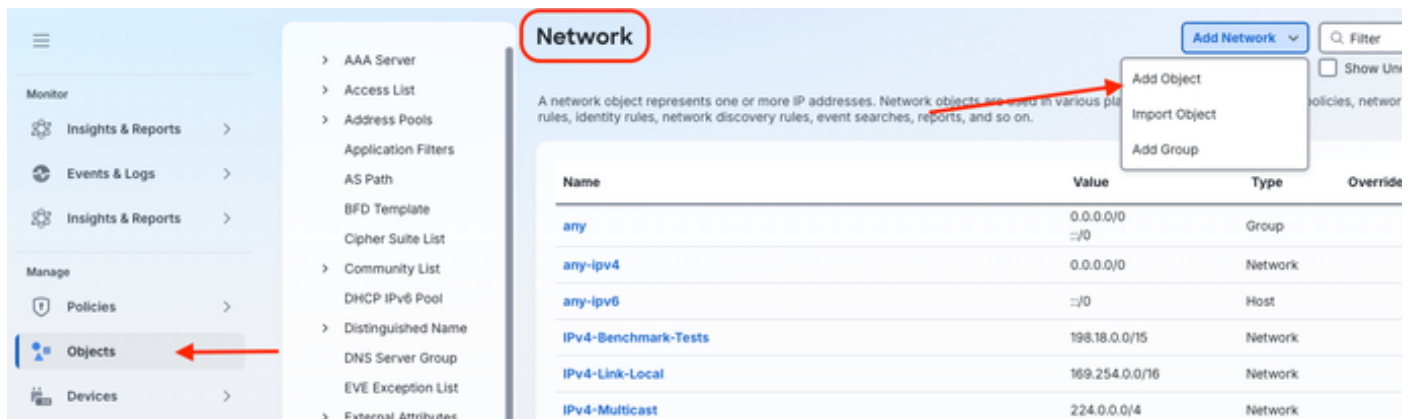
Dynamic Attributes Connector



Cisco Dynamic Attributes 커넥터 상태 활성화

2단계: FTD 인그레스 인터페이스를 나타내는 정규화된 도메인 이름 네트워크 개체 만들기

1) Objects(개체) > Add Network(네트워크 추가) > Add Object(개체 추가)를 선택합니다.



새 정규화된 도메인 이름 네트워크 개체 만들기

2) FQDN(Fully Qualified Domain Name)으로 구성된 네트워크 개체의 이름을 지정합니다. FQDN을 입력하고 적절한 라디오 버튼을 클릭하여 네트워크 개체를 FQDN 유형으로 할당합니다. 저장을 클릭합니다.

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

FQDN 네트워크 개체 변수 구성

3단계: DNS A 레코드 구성

1) 여기에 표시된 예에서는 Windows Server 2025를 사용합니다. 필요에 따라 특정 이름 확인 서버에 대한 설명서를 참조하십시오.

	Name	Type	Data
DNS ▼ DC ▼ Forward Lookup Zones example.com > Reverse Lookup Zones > Trust Points	(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



참고: 액티브 인증을 수행하는 클라이언트는 이 DNS A 레코드를 확인할 수 있어야 합니다.

2단계: 공개 키 인프라 컨피그레이션

내부 CA(Certificate Authority)를 활성 인증 컨피그레이션의 PKI(Public Key Infrastructure)로 사용할 수 있습니다. Cisco FMC 및 FTD는 필요한 SSL 가로채기 및 Decrypt-Resign 작업을 수행하기 위해 내부 CA 공개 키 및 페어링된 개인 키를 내부 CA 객체로 업로드해야 합니다. 또한 내부 CA는 활성 인증이 수행되는 클라이언트 브라우저 내에서 신뢰되어야 합니다. 브라우저에서 인증서를 신뢰하는지 확인하는 방법은 클라이언트 브라우저 설명서를 참조하십시오.

1단계: FMC에 내부 CA 인증서 가져오기

1) Objects(개체) > PKI > Internal CAs(내부 CA)를 선택합니다. Import CA(CA 가져오기)를 클릭합니다.



참고: 내부 CA는 FMC에서 직접 생성할 수도 있습니다.

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:

내부 인증 기관을 방화벽 관리 센터로 가져오기



참고: 이 문서의 내용 내에서 이미지의 다양한 필드 값을 다루는 공백이 나타나며 이 문서의 게시물별로 의도적입니다. 실제 값은 구성에 따라 환경에 반영됩니다.

2단계: CA로 서비스 공급자 인증서 서명

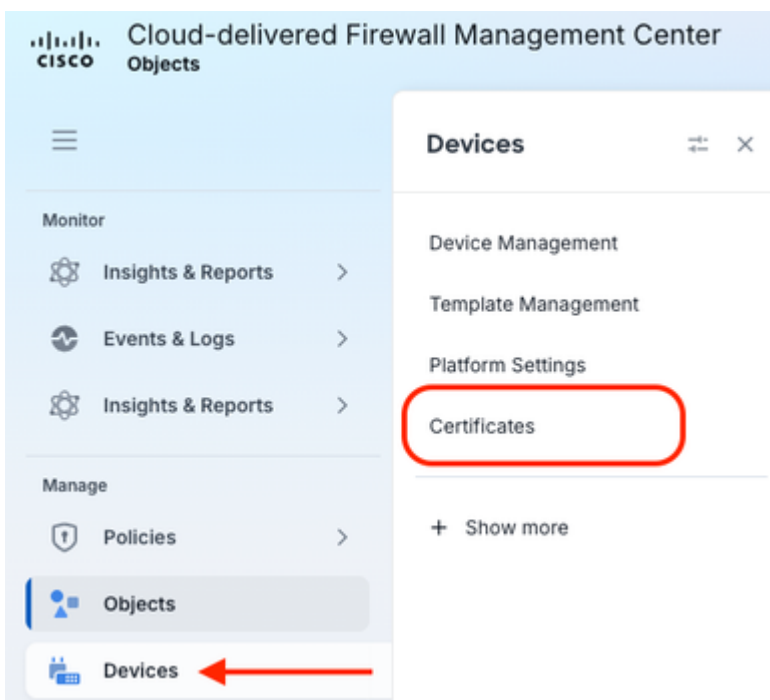
1) SP(서비스 공급자) 인증서는 신뢰할 수 있는 CA(Certificate Authority)에서 서명하고 PKCS#12(.p12) 형식으로 반환해야 합니다.



참고: 이 CA는 내부적으로 서명할 수 있습니다. 유일한 주의 사항은 클라이언트 디바이스에서 내부 CA를 신뢰해야 한다는 것입니다.

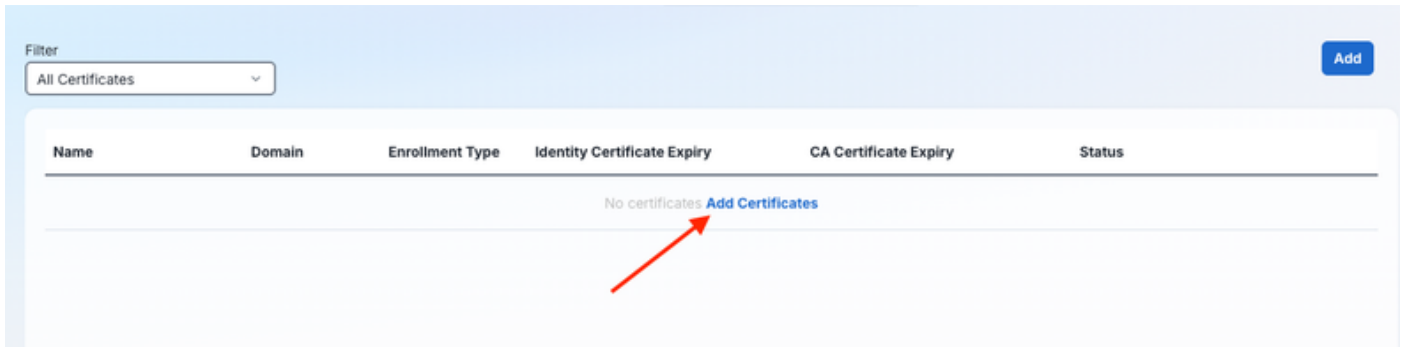
3단계: FTD에 SP 인증서 구축

1) Devices > Certificates를 선택합니다.



디바이스 및 인증서로 이동

2) Add Certificates(인증서 추가)를 클릭합니다.



새 디바이스 인증서 추가

3) Active Authentication(활성 인증)을 실행하는 드롭다운 목록에서 디바이스를 클릭한 다음 + 아이콘을 클릭하여 새 Certificate Enrollment(인증서 등록)을 생성합니다.

FTD를 선택하고 Add New Certificate Enrollment를 추가합니다.

4) Certificate Enrollment(인증서 등록)의 이름을 지정하고 Enrollment Type(등록 유형) 드롭다운 목록에서 PKCS12 파일을 선택합니다.

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

인증서 등록 설정 및 유형

5) Browse PKCS12 File(PKCS12 파일 찾아보기)을 클릭하여 PKCS#12 파일을 가져오고 필요한 암호를 입력합니다. 저장을 클릭합니다.

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 파일 찾아보기 및 가져오기

6) 등록 세부 정보가 정확한지 확인하고 Add(추가)를 클릭합니다.

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 +

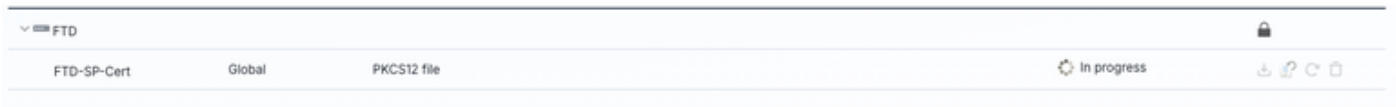
Certificate Enrollment Details:

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

Cancel Add

인증서 등록 세부 정보 확인

7) 가져오기에 진행 중이 반영됩니다.



가져오기가 완료되면 구성된 인증서의 ID 아이콘 을 클릭하여 SP 인증서 정보의 유효성을 검사할 수 있습니다.

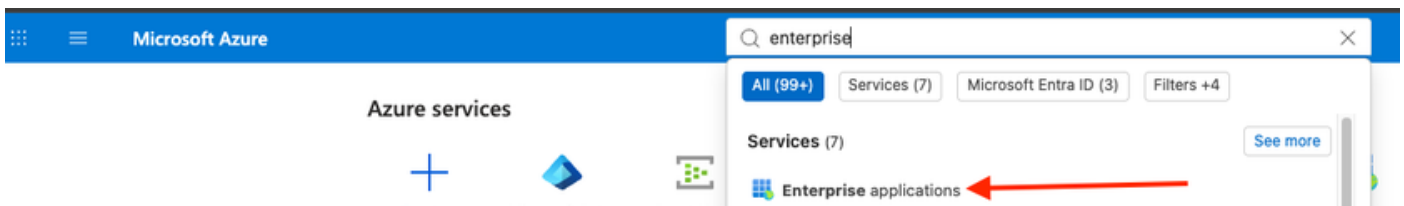


인증서 가져오기 진행 중 상태

3단계: Azure 구성

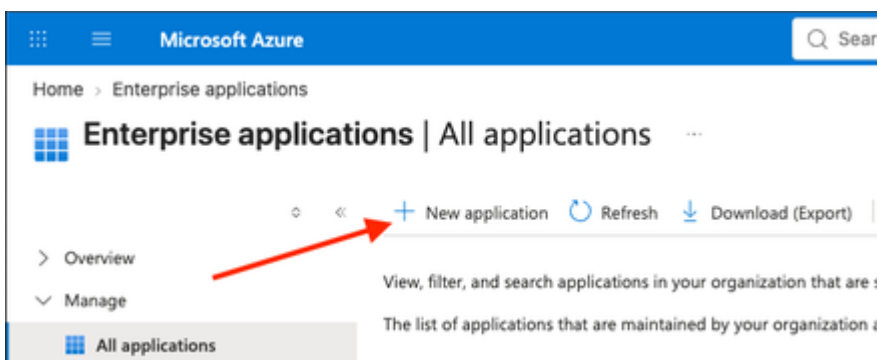
1단계: SAML 톨킷용 Centera 엔터프라이즈 애플리케이션 생성

1) Enterprise Applications를 검색하고 클릭합니다.



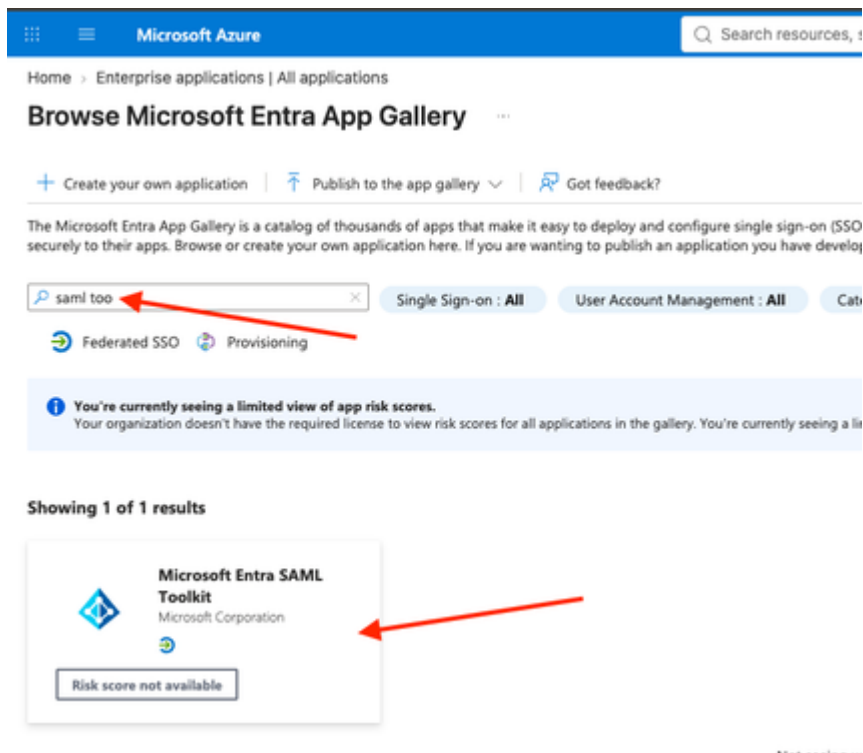
엔터프라이즈 애플리케이션 검색 및 액세스

2) + New Application을 클릭합니다.



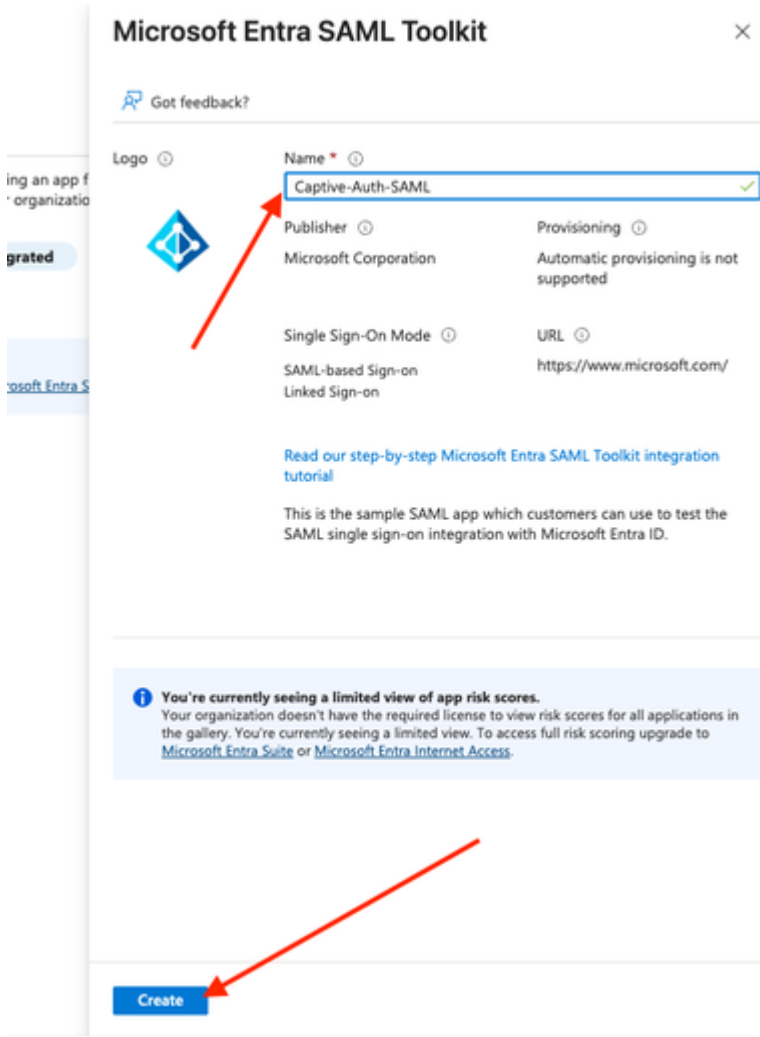
엔터프라이즈 애플리케이션 내에서 새 애플리케이션 선택

3) Microsoft Entra SAML Toolkit을 검색하고 축소판 그림을 클릭합니다.



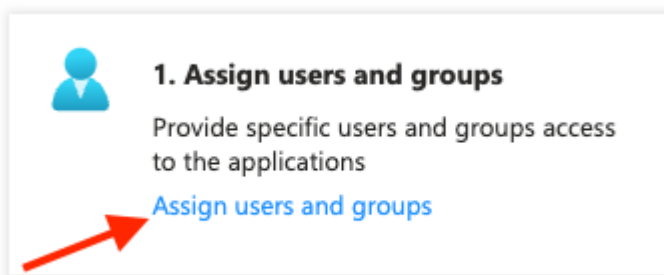
Microsoft Entra SAML 툴킷 검색 및 선택

4) Microsoft Entra SAML Toolkit Enterprise Application에 이름을 지정하고 Create를 클릭합니다.
(Microsoft 참조: [Microsoft Entra SAML Toolkit 통합 자습서를 읽어 보십시오.](#))



SAML 툴킷 애플리케이션에 이름 할당

5) 개요 페이지에서 특정 사용자 및 그룹을 SAML 툴킷 엔터프라이즈 애플리케이션에 할당합니다. 이 예에서 테스트 계정(captive-portal-user)은 active-auth-lab 그룹의 멤버입니다.

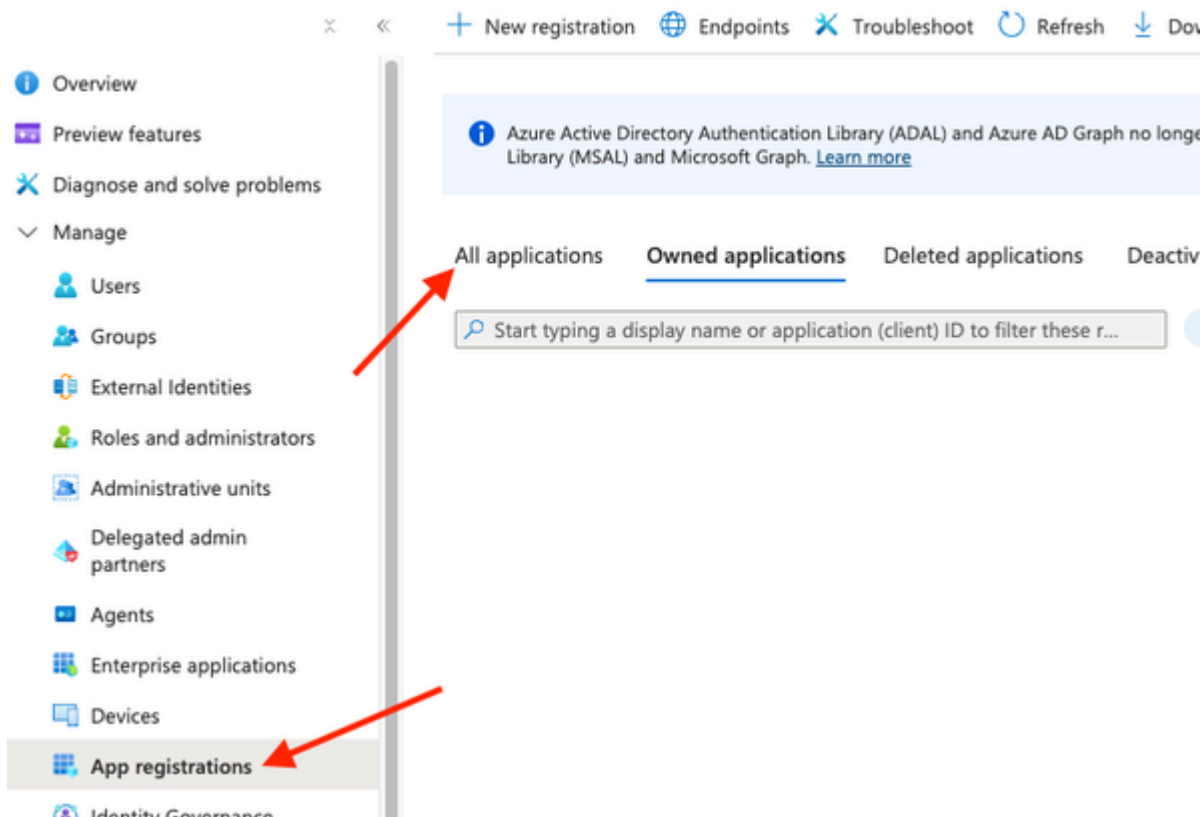


애플리케이션에 사용자 및 그룹 할당

6) 이 엔터프라이즈 애플리케이션 컨피그레이션은 이후 단계에서 계속됩니다.

2단계: Entra ID 앱 등록 구성

1) Entra ID로 다시 이동하고 왼쪽 탐색 메뉴에서 App registrations(앱 등록)를 선택합니다. All applications(모든 애플리케이션) 필터를 클릭하고 Enterprise Application(엔터프라이즈 애플리케이션)에 지정된 이름을 검색합니다. 적절한 애플리케이션을 클릭합니다.



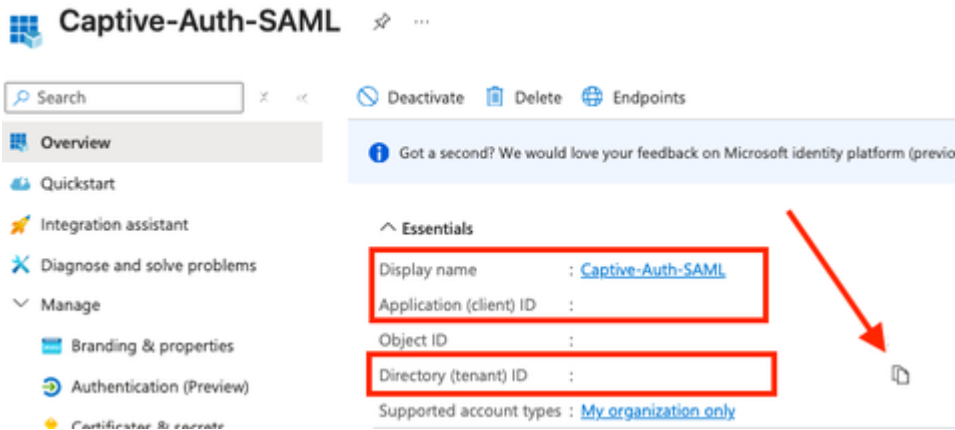
App Registrations And All Applications(앱 등록 및 모든 애플리케이션)로 이동합니다.

2) Enterprise App Registration 아래에서 Essentials 값을 수집하고 기록합니다.



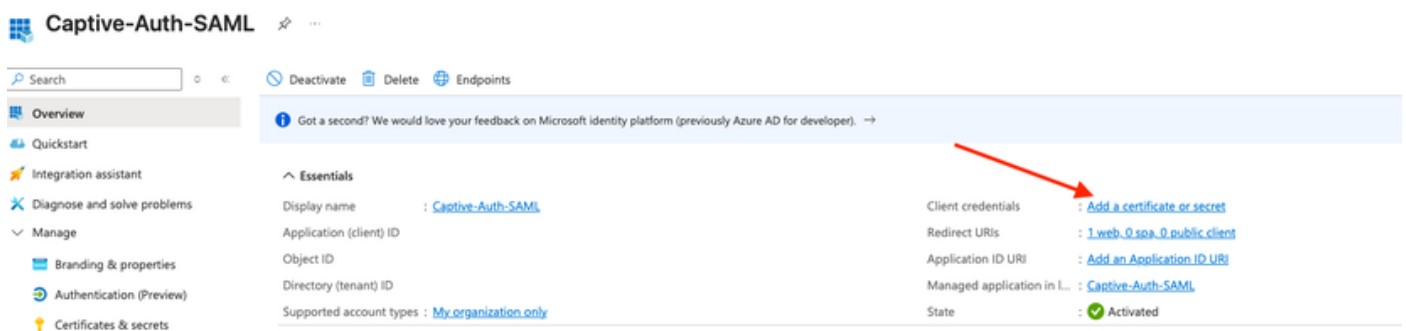
중요: 값 위에 마우스 커서를 올려 놓으면 클립보드에 복사가 표시되고 개요 페이지의 Essentials 아래에 값을 수집합니다.

- 표시 이름
- 애플리케이션(클라이언트) ID
- 디렉토리(테넌트) ID



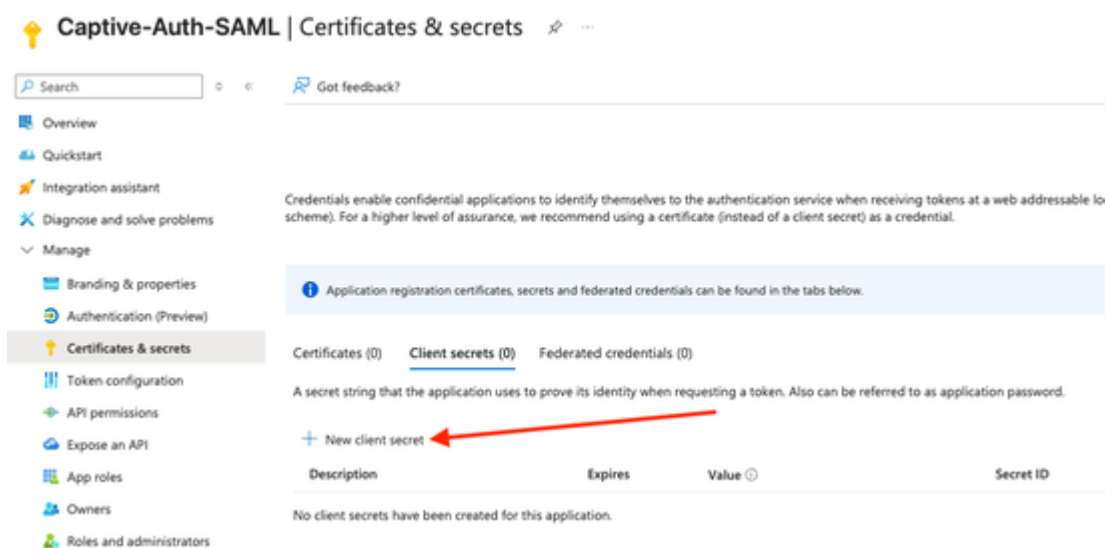
표시 및 응용 프로그램과 디렉터리 ID 값 수집

3) Add certificate or secret 하이퍼링크를 클릭합니다.



Add Certificate Or Secret 하이퍼링크

4) + 새 클라이언트 암호를 클릭합니다.



새 클라이언트 암호 추가

5) 비밀에 대한 설명을 제공하고 필요에 따라 만료를 조정합니다. Add(추가)를 클릭합니다.

Add a client secret

Description:

Expires: Recommended: 180 days (6 months) ▼

Add Cancel

클라이언트 암호에 대한 설명 제공

6) 암호를 복사합니다.



중요: 클립보드에 복사된 비밀 값을 기록해 둡니다.

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.

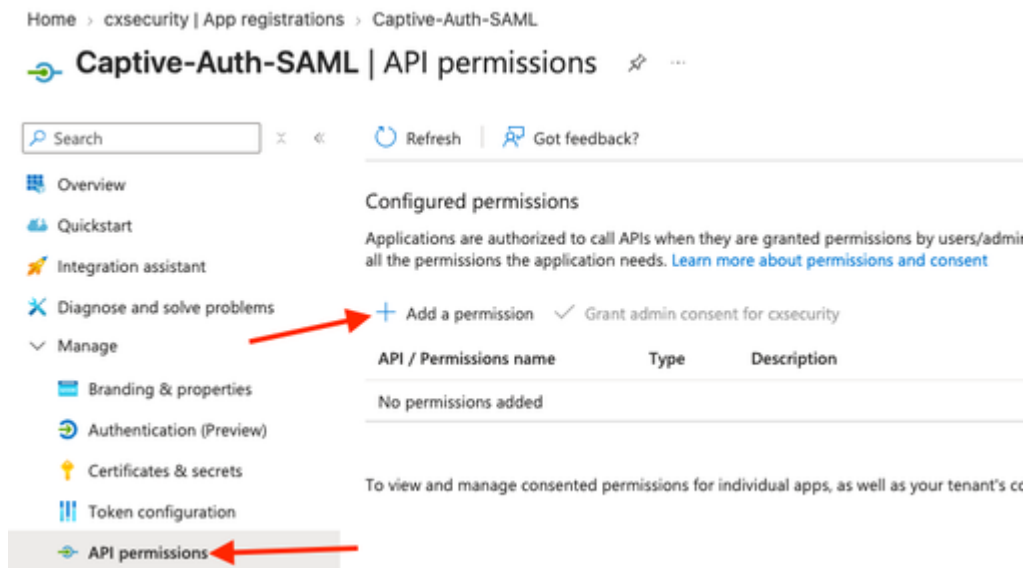
+ New client secret

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

클라이언트 암호 값 복사

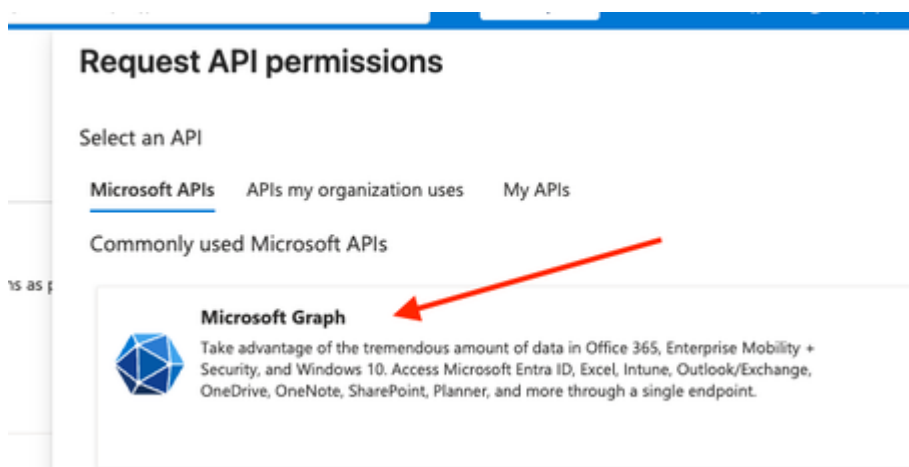
3단계. 앱 등록을 위한 Microsoft Graph API 권한을 구성합니다.

1) 왼쪽의 탐색 메뉴에서 API Permissions(API 권한)를 선택한 다음 + Add a permission(권한 추가)을 클릭합니다.



API 권한 구성

2) Microsoft Graph API를 클릭합니다.



Microsoft Graph API 선택

3) 위임된 사용자에게 권한을 부여합니다. 권한을 읽은 다음 권한 추가를 클릭합니다.

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

위임된 사용자에게 읽기 권한 부여

4) 응용 프로그램 User.Read.All 권한 부여(확인란 선택)

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
-------------------------------------	--	-----

응용 프로그램 읽기 모든 권한 부여

5) Group.Read.All 확인란을 검색하여 선택하면 Group Read 권한도 부여됩니다. Add permissions(권한 추가)를 클릭합니다.

Select permissions

expand all

Group.Read.All

Permission

Admin consent required

✓ Group (1)

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

Add permissions

Discard

API 권한 저장

6) 구성된 권한이 일치하는지 확인하고, 해당 권한에 대한 관리 동의를 부여합니다.

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 ...

권한에 대한 관리 동의 부여

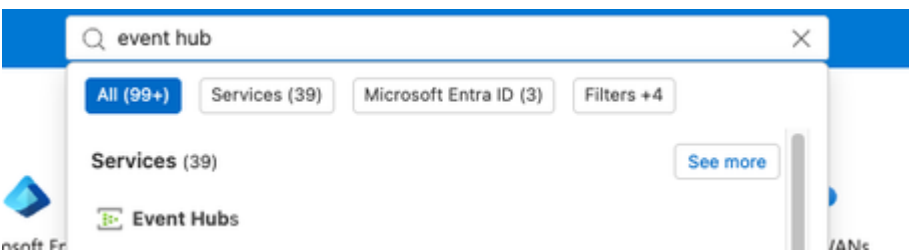
7) 관리자 동의가 부여되면 출력이 표시됩니다.

+ 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 ...

관리 동의가 부여된 출력

4단계: EH(Event Hub) 네임스페이스 구성

1) Event Hubs를 검색하고 클릭합니다.



이벤트 허브 구성 검색

2) 새 EH 네임스페이스를 만듭니다.



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](#)

이벤트 허브 네임스페이스 만들기

3) EH 네임스페이스를 구성합니다.



참고: 표준 가격 책정 계층 이상을 선택해야 합니다. 기본 가격 책정 계층은 영역 사용을 차단합니다.

이벤트 허브 고급 [설정](#) 및 특정 요구 사항에 대한 적용 가능성에 대한 자세한 내용은 [Azure](#) 이벤트 허브 설명서를 참조하십시오.

Review(검토) + Create(생성)를 클릭합니다.



Create Namespace

Event Hubs

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

Project Details

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

Subscription *

Resource group *

[Create new](#)

Instance Details

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

Namespace name * ☒ .servicebus.windows.net

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

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

Throughput Units *

Enable Auto-Inflate ? ☐

[Review + create](#)

< Previous

Next: Advanced >

이벤트 허브 네임스페이스 설정 구성

4) 검증이 성공하면 Create(생성)를 클릭합니다.



Create Namespace

Event Hubs

Validation succeeded.

Basics Advanced Networking Tags Review + createEvent 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 >

이벤트 허브 네임스페이스 배포 만들기

5) 구축이 완료되었는지 확인한 후 리소스로 이동을 클릭합니다.



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

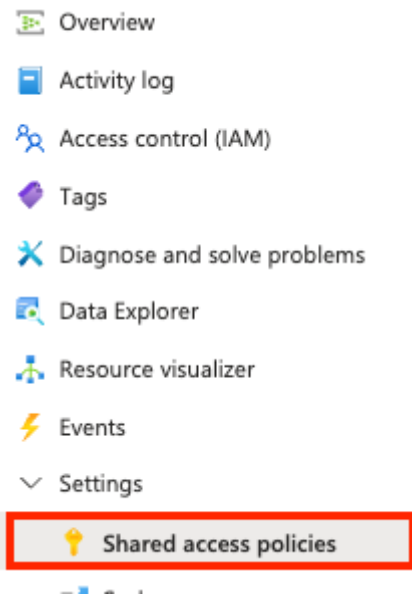
✓ Next steps

Go to resource

이벤트 허브 네임스페이스 리소스로 이동

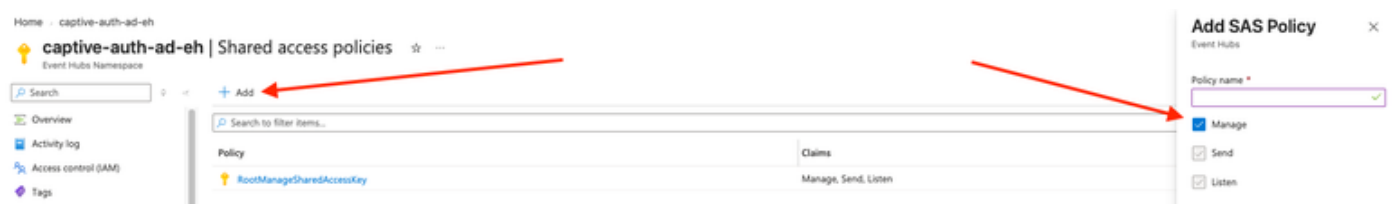
5단계: 이벤트 허브 네임스페이스에서 공유 액세스 정책 선택 또는 만들기

1) 왼쪽 탐색 메뉴에서 Settings(설정) > Shared access policies(공유 액세스 정책)를 선택합니다.



공유 액세스 정책으로 이동

2) + Add(추가)를 클릭하고 새 정책 이름을 입력한 다음 Manage(관리) 확인란을 선택합니다. Add SAS Policy(SAS 정책 추가) 메뉴 패널의 하단에서 Create(생성)를 클릭합니다.



새 공유 액세스 정책 추가



공유 액세스 정책 생성

6단계: EH 네임스페이스에서 SAS(Shared Access Signature) 정보 수집 및 메모

1) 새 공유 액세스 정책을 클릭합니다. eh SAS Policy(EH SAS 정책)가 오른쪽 측면 패널에 나타남

니다.

[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

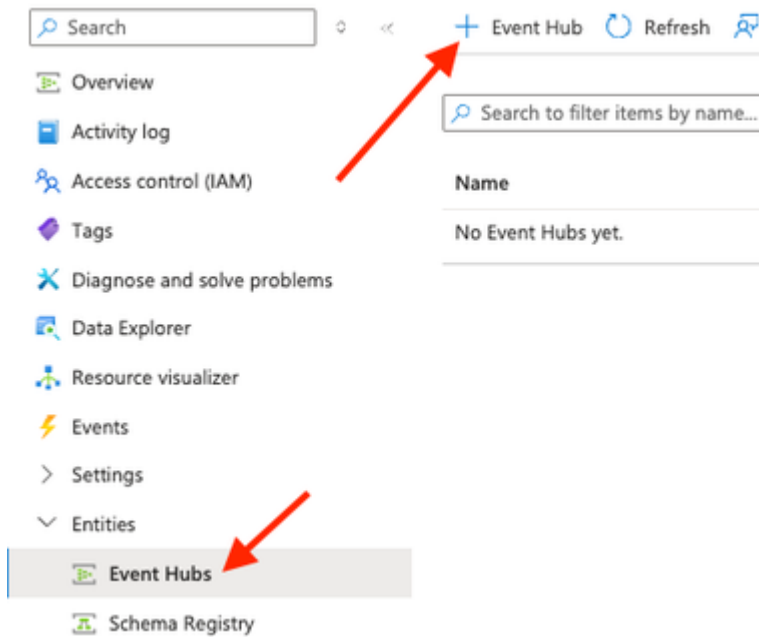
기본 연결 문자열 복사



중요: 기본 연결 문자열을 복사하여 기록합니다.

7단계: 이벤트 허브 네임스페이스 내에서 이벤트 허브 인스턴스 만들기

1) [네임스페이스] 메뉴에서 [엔터티] > [이벤트 허브]를 선택합니다. 새 EH 인스턴스를 생성하려면 + Event Hub를 클릭합니다.



새 이벤트 허브 인스턴스 만들기

2) 새 EH 인스턴스에 이름을 할당한 다음 Review + create를 클릭합니다.

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 >

이벤트 허브 인스턴스에 이름 할당

3) 검증이 성공하면 Create(생성)를 클릭하여 Event Hub 인스턴스를 프로비저닝합니다.

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 >

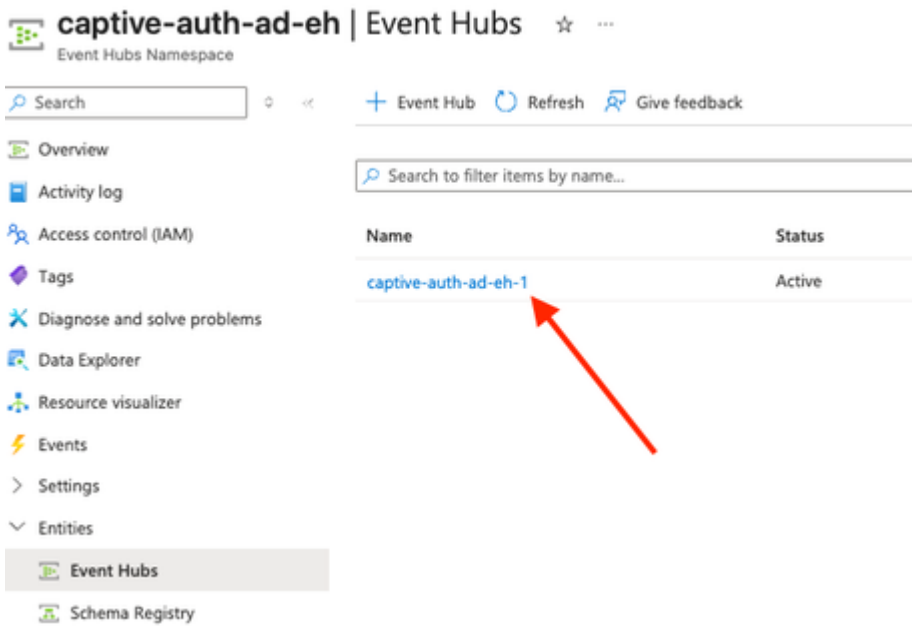
이벤트 허브 인스턴스 프로비전



중요: 이벤트 허브 인스턴스 이름을 복사하여 기록해 둡니다.

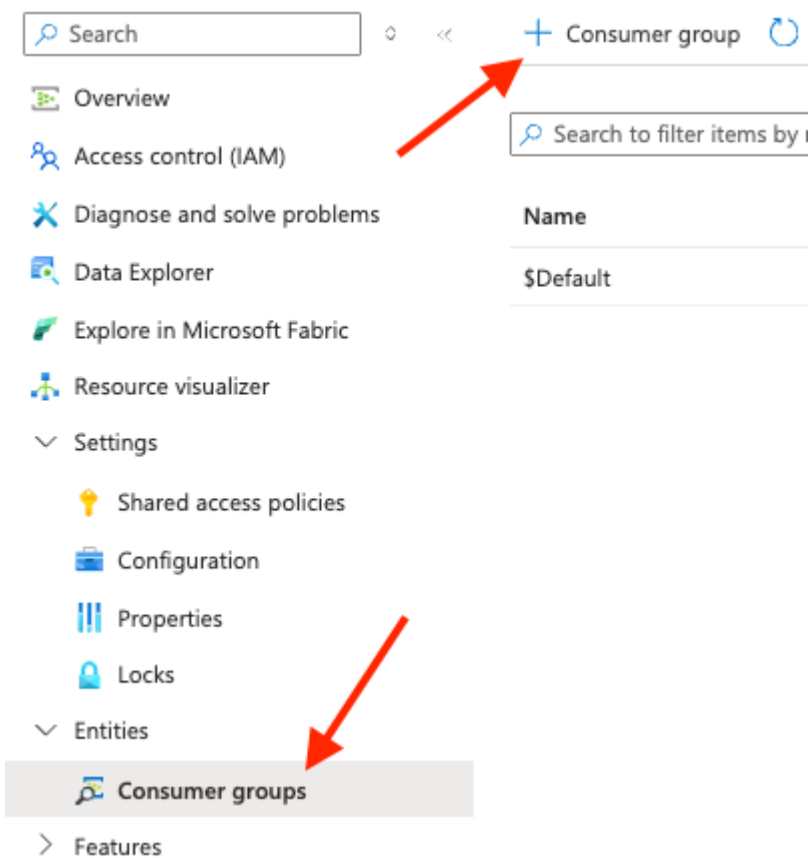
8단계: 이벤트 허브 네임스페이스 내에서 이벤트 허브 인스턴스 소비자 그룹 만들기

1) 이전 단계에서 구성한 새 EH 인스턴스를 클릭합니다.



액세스 이벤트 허브 인스턴스 컨피그레이션

2) EH 인스턴스에서 Entities(엔터티) > Consumer groups(소비자 그룹)를 선택하고 새 Consumer group(소비자 그룹)을 만듭니다.



소비자 그룹 생성

3) 소비자 그룹의 이름을 지정하고 Create(생성)를 클릭합니다.

Create consumer group ✕

Consumer groups

Name *

captive-auth-ad-eh-cg ✓

Create

소비자 그룹에 이름 할당



중요: Event Hub 인스턴스 Consumer 그룹 이름을 복사하여 기록합니다.

9단계: 수집된 값 확인

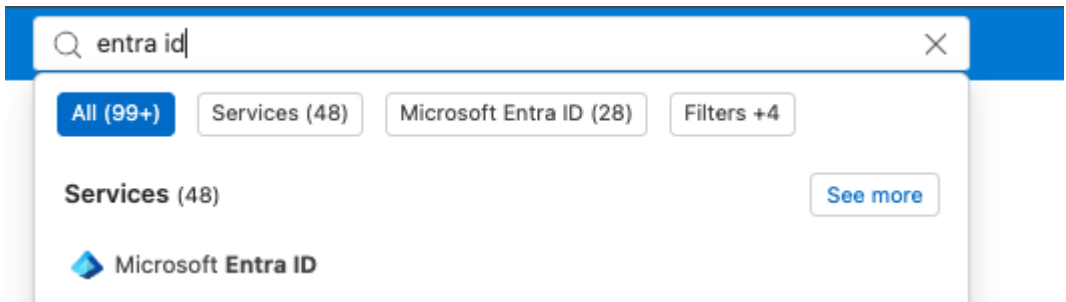
1) 이 시점에서, 이전 단계의 이 값을 기록한다. 값이 기록되지 않은 경우 해당 값이 수집되는 단계를 참조하십시오.

- 3단계 2단계 - 애플리케이션 등록(이 프로세스를 위해 생성된 엔터프라이즈 앱의 경우, 수집된 표시 이름이 참조함)
 - 2단계, 2단계 하위
 - 표시 이름
 - 애플리케이션(클라이언트) ID
 - 디렉토리(테넌트) ID
 - 2단계, 6단계
 - 클라이언트 암호
- 3단계 6단계 - 이벤트 허브
 - 6단계, 1단계
 - EH 네임스페이스
 - 기본 연결 문자열

- 7단계, 3단계 하위
 - EH 인스턴스(이벤트 허브) 이름
- 8단계, 3단계 하위
 - EH 소비자 그룹 이름

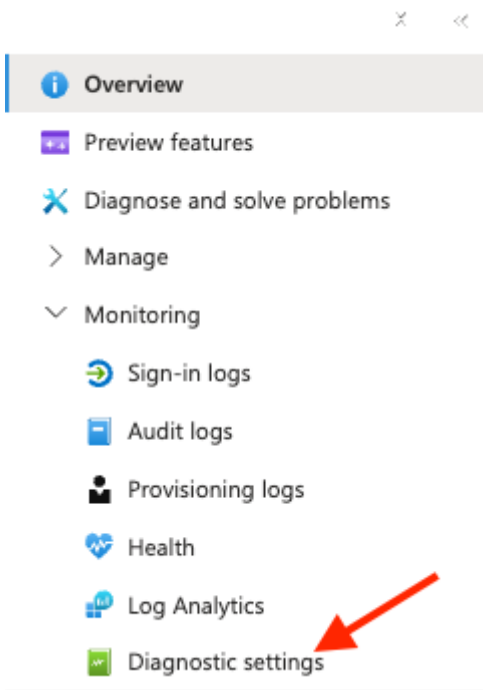
10단계: 이벤트 허브에 대한 Entra ID 감사 로그 스트리밍 구성

1) Entra ID 테넌트 구성으로 다시 이동합니다.



Entra ID Tenant Configuration(ID 테넌트 컨피그레이션)을 검색하고 탐색합니다.

2) 왼쪽 메뉴에서 Monitoring(모니터링) > Diagnostic Settings(진단 설정)를 선택합니다.



진단 설정 모니터링

3) Diagnostic settings(진단 설정) > General(일반)을 선택하고 + Add diagnostic settings(진단 설정 추가)를 클릭합니다.

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

새 진단 설정 추가

4) 진단 설정에 필요한 이름을 지정하고, AuditLogs(감사 로그) 확인란을 선택하여 로깅하고, Stream to an event hub(이벤트 허브에 스트림) 확인란을 선택합니다. 이전 컨피그레이션에서 명시한 값을 참조하고 완료되면 Save(저장)를 클릭합니다.

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

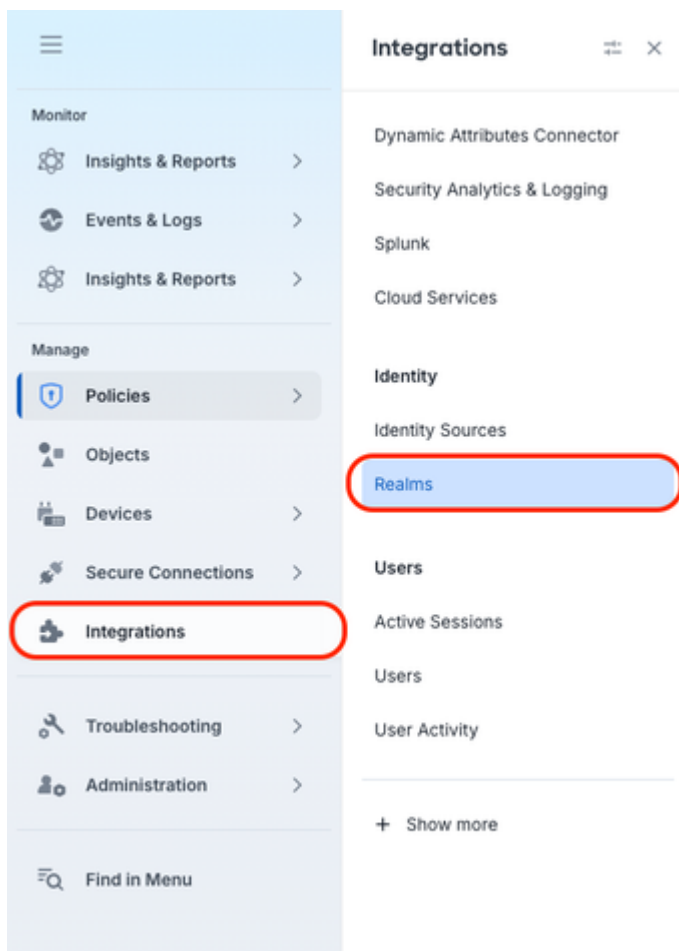
Event hub policy name

☐ Send to partner solution

4단계: Azure 및 FMC/FTD 활성 인증 컨피그레이션 통합

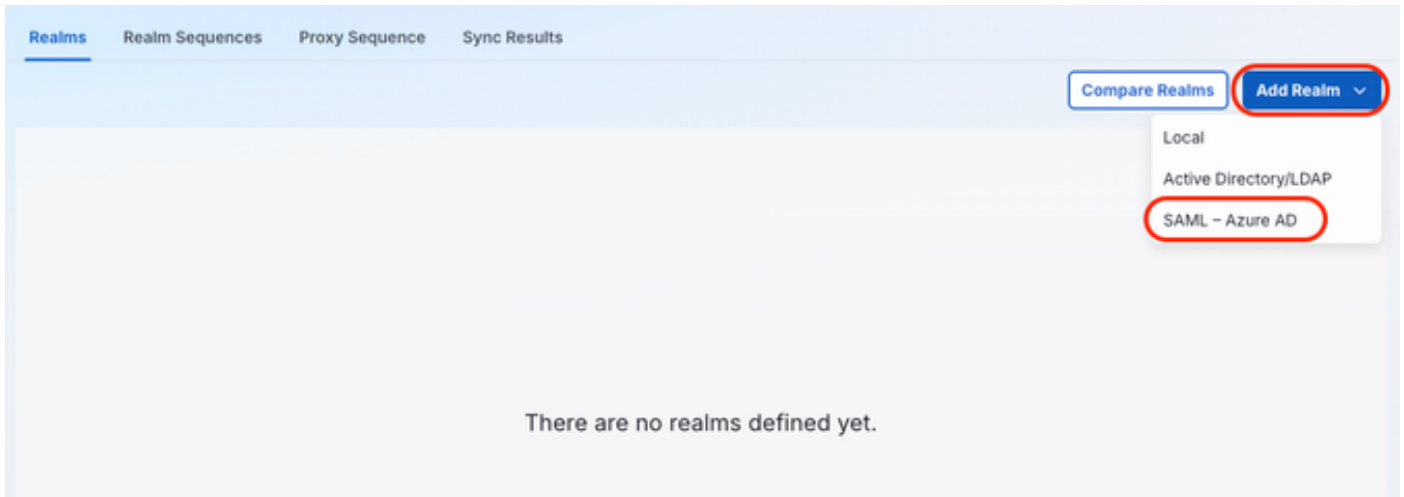
1단계: FMC 마법사를 사용하여 Azure SAML/Entra ID 영역 구성

1) FMC에서 Integrations(통합) > Identity(ID) > Realms(영역)를 선택합니다.



ID 영역 컨피그레이션

2) 영역 추가 드롭다운 목록을 클릭하고 SAML - Azure AD를 선택합니다.



SAML Azure AD 영역 추가

3) Azure 영역에 이름 및 설명을 할당하여 사용을 설명하고 Azure AD를 사용하여 수동으로 인증하거나 Azure AD를 사용하여 종속 포털을 사용하는 것이 구성 유형 드롭다운 목록에서 선택되었는지 확인합니다. Next(다음)를 클릭합니다.

Azure AD 영역 설정 구성

4) 이전에 구성한 FQDN 객체를 Base URL로 선택합니다. 다음과 같이 문자열 형식으로 엔티티 ID를 입력합니다.

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

- SAML 엔티티 ID 접미사가 구성된 경우(다음 구성 예에서 녹색으로 밑줄이 그어짐) 환경 내의 다른 SSO 구현 간에 접미사가 고유한지 확인합니다. 이 값은 Azure SAML 구성과도 일치해야 합니다. 기본 URL은 컨피그레이션 전체에서 동일하게 유지됩니다.
- ACS(Assertion Consumer Services) URL은 자동으로 채워지며 변경할 수 없습니다.
- FMC의 Devices(디바이스) > Certificates(인증서) 아래에서 이전 워크플로 단계에 등록된 서비스 공급자(SP) 인증서를 선택합니다.
- 이러한 값을 입력한 후 서비스 공급자 메타데이터 다운로드를 클릭하여 구성 프로세스를 간소화하고 예상 값이 Azure에 기록되었는지 확인합니다.

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

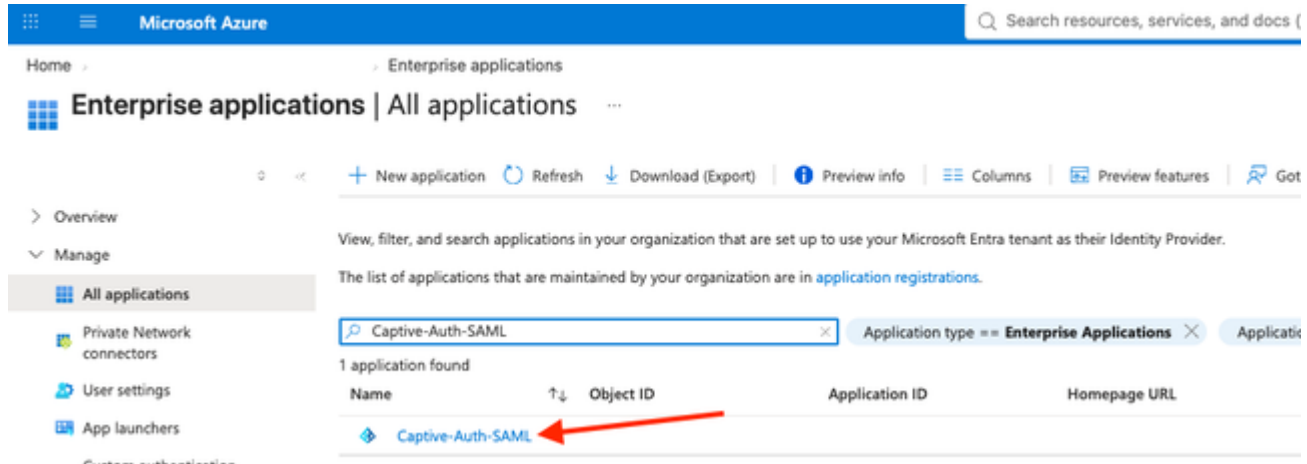
Next

기본 URL 및 엔티티 ID 구성, SAML 메타데이터 다운로드

5) Next(다음)를 클릭하여 Realm(영역) 컨피그레이션의 Sequence 3(시퀀스 3)으로 이동합니다.

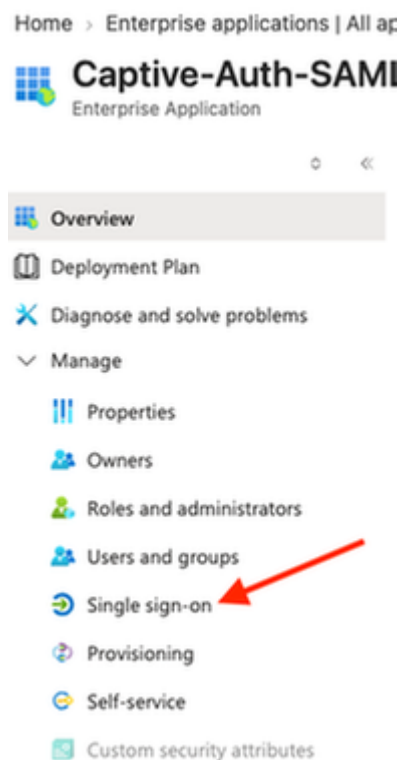
2단계: Azure 엔터프라이즈 응용 프로그램에서 FMC 구성 SAML SP 메타데이터 구현

1) 다시 Azure로 이동하고 Enterprise ID > 관리 > 엔터프라이즈 응용 프로그램을 선택합니다. 이전에 생성한 Microsoft Entra SAML Toolkit Enterprise Application 인스턴스를 검색합니다.



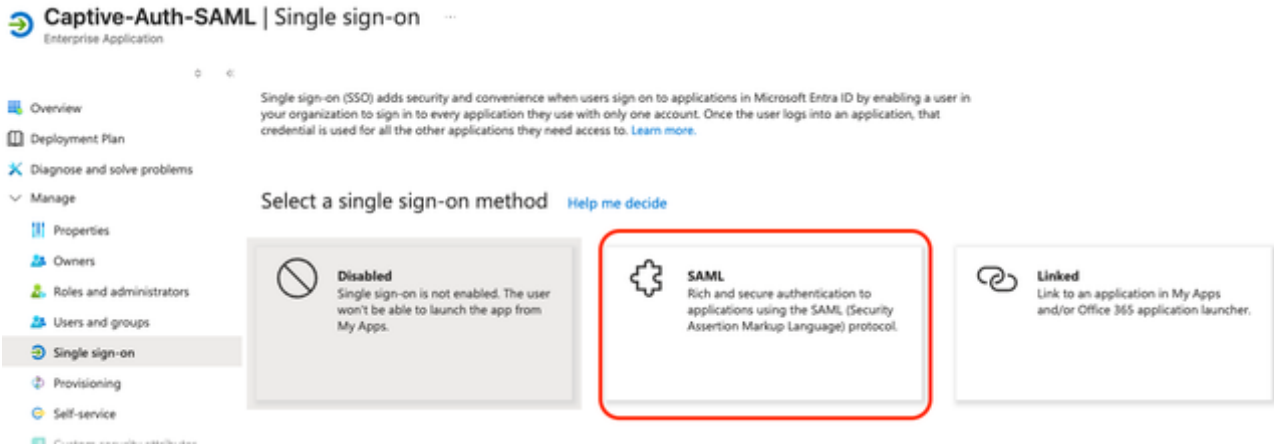
Microsoft Entra SAML 톨킷 애플리케이션 찾기

2) 측면 탐색 메뉴에서 Manage(관리) > Single Sign-On을 선택합니다.



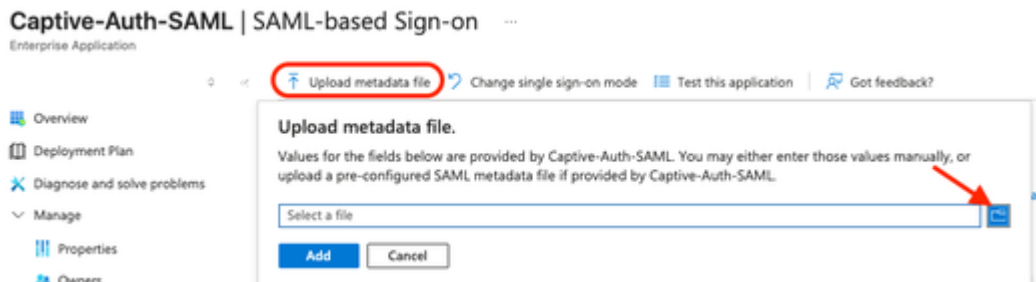
단일 사인은 구성 관리

3) SAML SSO(Single Sign-On) 모드를 클릭합니다.



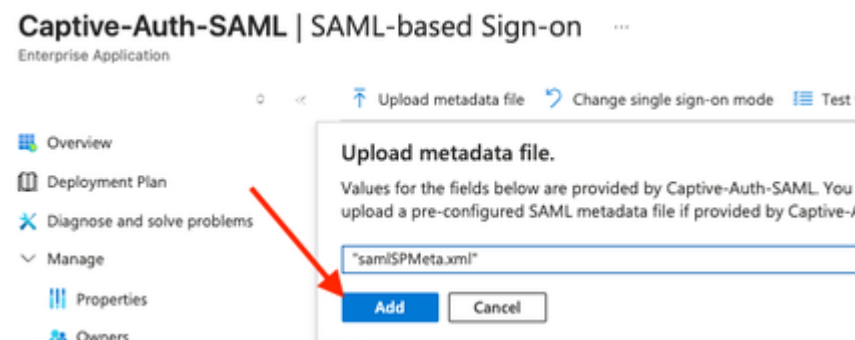
SAML 단일 사인온 모드 선택

4) Upload metadata file(메타데이터 파일 업로드)을 클릭하고 파란색 폴더 아이콘을 클릭하여 FMC에서 다운로드한 SAML 메타데이터 파일에 대한 로컬 파일 시스템을 찾습니다.



방화벽 관리 센터에서 메타데이터 파일 업로드

5) 업로드가 완료되면 Add를 클릭합니다.



SAML 컨피그레이션 애플리케이션 추가

6) Basic SAML Configuration(기본 SAML 컨피그레이션)의 측면 패널이 나타나고 업로드 및 자동으로 적용되는 FMC에서 생성된 SP 메타데이터 XML 파일에서 식별자(엔티티 ID) 및 ACS URL과 같은 값이 추출됩니다. 그러나 로그인 URL은 채워지지 않으며 저장하기 전에 필요합니다.

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.



기본 SAML 컨피그레이션 추출

7) 지정된 로그인 URL 패턴을 사용하여 값을 복사하여 붙여넣은 다음, 완료 시 상단의 저장을 클릭

합니다.

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.



로그온 URL 컨피그레이션 항목

아래로 스크롤하여 SAML 인증서로 이동하고 Cisco Secure FMC로 가져올 Azure 생성 페더레이션

메타데이터 XML 파일을 내보냅니다.

페더레이션 메타데이터 XML 파일 내보내기

3단계: FMC 마법사를 사용하여 Azure SAML/Entra ID 영역 구성(계속)

1) FMC로 다시 이동합니다. 시퀀스 3의 SAML IdP(Identity Provider) 메타데이터에서 Azure에서 다운로드한 내보낸 페더레이션 메타데이터 XML 파일을 FMC에 업로드하여 필요한 값을 자동으로 채웁니다.

페더레이션 메타데이터 XML 파일 업로드

2) 업로드되면 표시된 대로 값이 채워집니다.

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

자동으로 채워진 SAML ID 공급자 값



참고: 부분 출력이 이미지에 표시됩니다.

3) 이 시점까지 구현 프로세스 전반에 걸쳐 수집된 값을 입력합니다.

- 앱 등록
 - 애플리케이션(클라이언트) ID
 - 클라이언트 암호
 - 디렉토리(테넌트) ID
- 이벤트 허브
 - EH 네임스페이스 호스트 이름
 - EH 네임스페이스 기본 연결 문자열
 - EH 인스턴스(이벤트 허브) 이름
 - EH 소비자 그룹 이름

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

애플리케이션 및 이벤트 허브 정보 입력

입력을 마치면 테스트를 클릭하여 연결을 확인하고 제공된 정보로 Azure에 연결할 수 있는지 확인합니다.



참고: 해당되는 경우, Excluded/Included User Groups(제외된/포함된 사용자 그룹)가 Entra 컨피그레이션과 일치하는지 확인합니다

4) 마법사의 마지막 단계에서 SAML 종속 포털 사용자 시간 초과를 구성할 수 있습니다. 기본값은 1440분입니다.

5 User Session Timeout

SAML Captive Portal Users

Minutes Range 0-35791394

종속 포털 시간 초과 구성

5) Next(다음)를 클릭하여 계속 진행합니다.

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 영역 구성을 사용하여 앞으로 이동

6) 마법사가 구현된 구성에 대한 요약을 제공합니다. 입력한 값을 검증하고 확인한 후 요약 끝에 있는 저장을 누릅니다.

5 User Session Timeout [Edit](#)

SAML Captive Portal Users	1440 Minutes
ISE Users	1440 Minutes

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

영역 구성 요약 저장 버튼

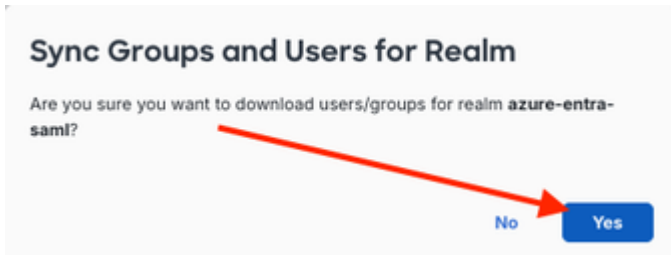
4단계: 다운로드한 사용자 확인

1) Integrations(통합) > Identity(ID) > Realms(영역) 워크플로의 Download Now(지금 다운로드) 버튼을 사용하여 Azure Entra에서 사용자를 다운로드할 수 있는지 확인합니다.

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

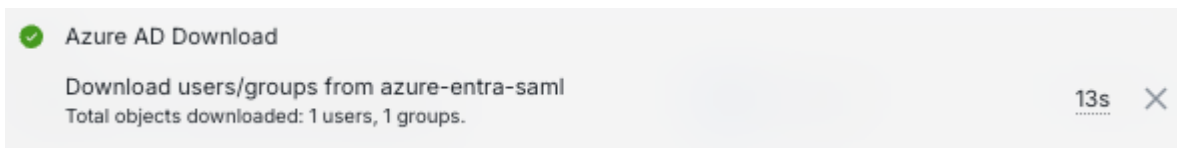
Azure AD에서 사용자 다운로드

2) 대화 프롬프트에 대한 응답으로 Yes(예)를 클릭합니다.



Azure AD에서 사용자 다운로드 확인

3) Notifications(알림) > Tasks(작업)에서 확인한 대로 다운로드 작업에서 사용자 1명과 그룹 1명이 다운로드됩니다.

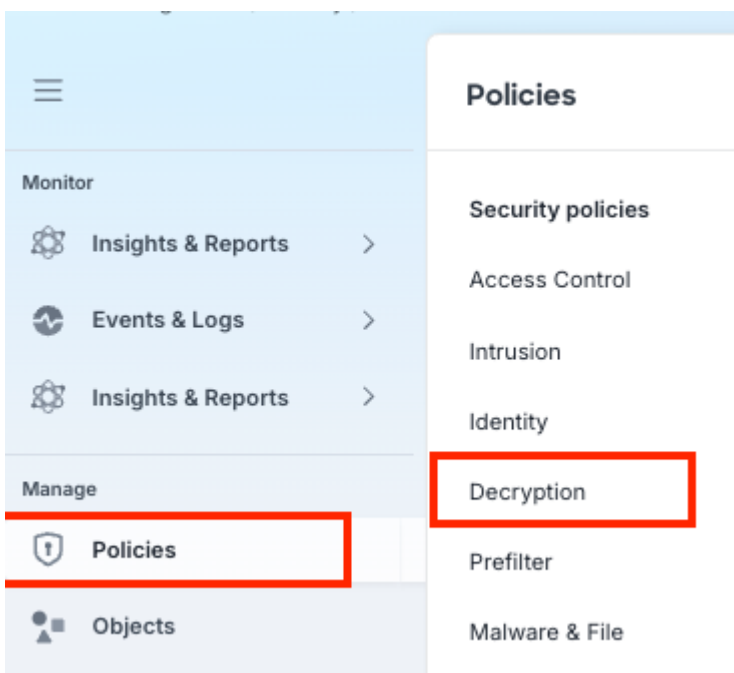


Azure AD에서 사용자 다운로드를 위한 알림 항목

5단계: FMC에서 정책 구성

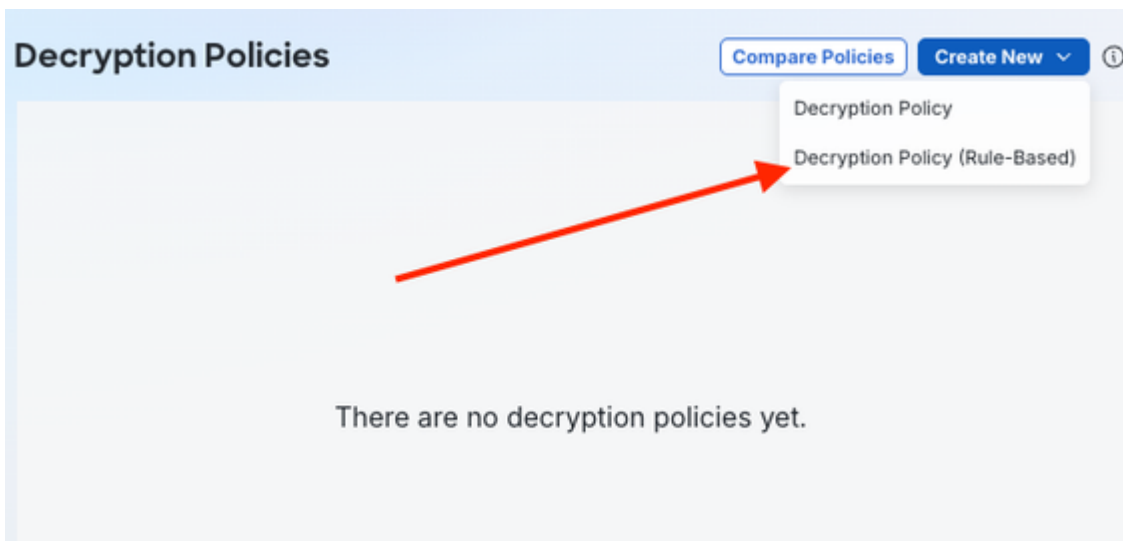
1단계: 암호 해독 정책 구성

1) FMC에서 Policies(정책) > Security Policies(보안 정책) > Decryption(해독)을 선택합니다.



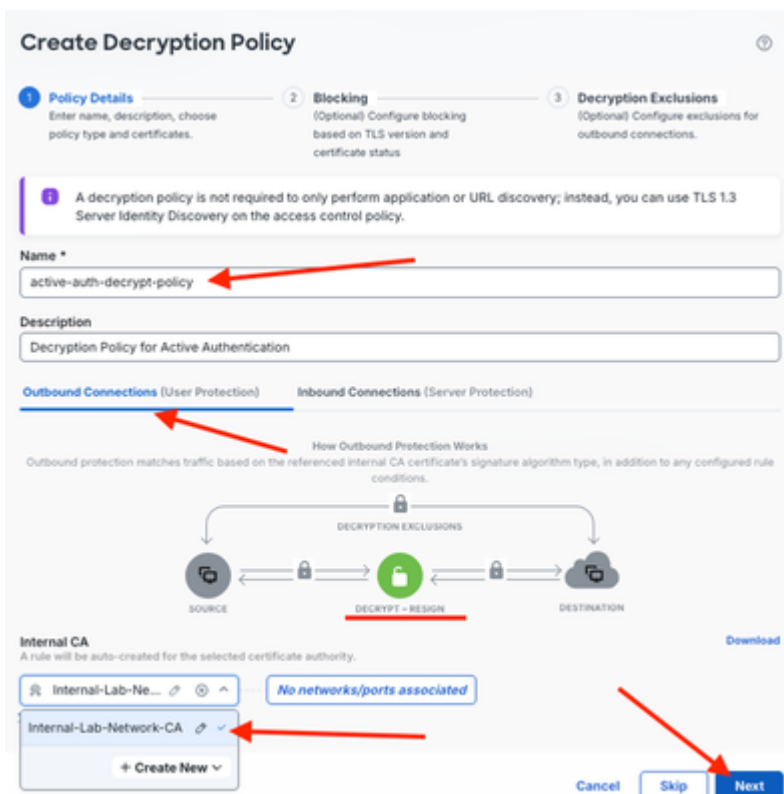
암호 해독 정책으로 이동

2) Create New(새로 만들기) 드롭다운 목록을 클릭하고 Decryption Policy (Rule-Based)(암호 해독 정책(규칙 기반))을 선택합니다.



새 규칙 기반 암호 해독 정책 생성

3) 새로운 규칙 기반 암호 해독 정책에 이름 및 설명(원하는 경우)을 지정하고 Outbound Connections (User Protection)(아웃바운드 연결(사용자 보호)) 탭 옵션을 클릭하여 종속 포털 인증(활성 인증)에 필요한 Decrypt-Resign 기능을 구현합니다.



아웃바운드 연결 정책 세부 정보 구현

4) 동일한 대화 상자의 해당 드롭다운 목록에서 이전에 적용된 내부 CA를 선택합니다. Next(다음

)를 클릭합니다.

5) 필요에 따라 옵션을 사용자 지정합니다.

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](#)

암호 해독 정책 옵션 사용자 지정

6) 이 예에서는 필수 Policy Details(정책 세부사항)를 제외하고 기본값이 사용됩니다. Create Policy(정책 생성)를 클릭하여 컨피그레이션 마법사를 완료합니다.

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

Cancel
Skip
Back
Create Policy

최종 암호 해독 정책 생성

2단계: 암호 해독 정책 규칙 구성

1) 규칙 기반 암호 해독 정책의 기본 레이아웃이 여기에 표시됩니다. 해독 불가 도메인 이름의 사전 할당 목록을 참조하는 규칙 3 및 해독 불가 태그가 지정된 애플리케이션을 참조하는 규칙 6과 같이 기본 활성화된 규칙과 일치하지 않는 트래픽은 규칙 7에서 Decrypt - Resign 작업을 받습니다. 이러한 기본값은 기본 작업과 함께 필요에 따라 수정할 수 있습니다. 기본적으로 다른 규칙과 매칭하지 않는 트래픽은 Do Not Decrypt로 구성됩니다.

검사를 위해 Azure 인증 서비스 트래픽의 암호를 해독해서는 안 되므로 이에 대한 전용 규칙이 만들어집니다. 시작하려면 + Add Rule을 클릭합니다.

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

규칙 추가 및 기본 규칙 기반 암호 해독 레이아웃 표시

2) 새 암호 해독 정책 규칙 항목에 이름을 지정하고 Action 드롭다운 목록에서 Do not decrypt를 선택한 다음, 덜 구체적인 규칙의 맨 위에 규칙을 놓습니다. 소스/대상 영역도 구현하여 규칙을 더 좁힙니다.

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 규칙 구성

3) 규칙을 추가하기 전에 [응용 프로그램] 탭을 클릭하고 Azure 인증 서비스 응용 프로그램을 검색

하여 클릭합니다. [규칙에 추가]를 클릭한 다음 [추가]를 클릭합니다.

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)

Search by name: azure a

Risks (Any Selected)

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

Business Relevance (Any Selected)

- ☐ Very Low 609

Available Applications (2)

All apps matching the filter

- Azure Arc
- Azure Authentication Service**

Selected Applications and Filters (0)

any

Azure 인증 서비스 응용 프로그램 규칙 추가

4) Save를 클릭합니다.

active-auth-decrypt-policy

Decryption Policy for Active Authentication

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

You have unsaved changes

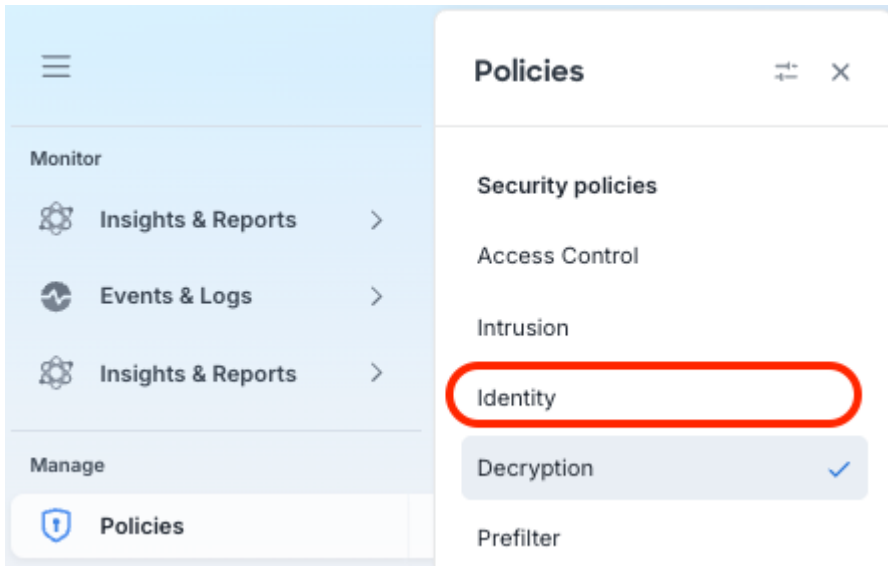
+ Add Category + Add Rule Search Rules

#	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	any	any	Azure Authen	any	any	any	any	Do not decrypt

암호 해독 정책 저장

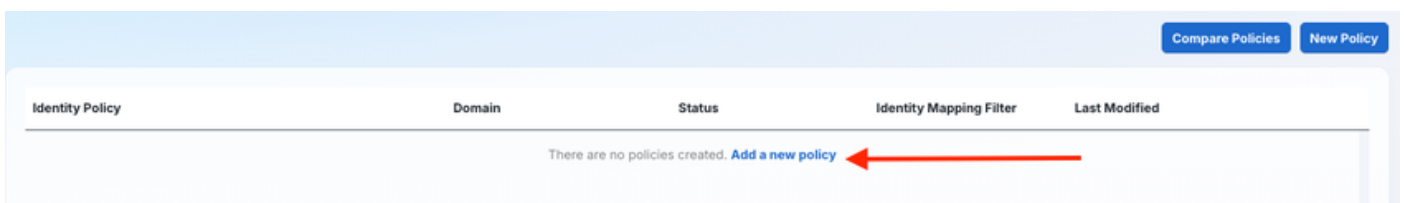
3단계: ID 정책 생성

1) ID 정책을 생성하려면 Policies > Security Policies > Identity를 선택합니다.



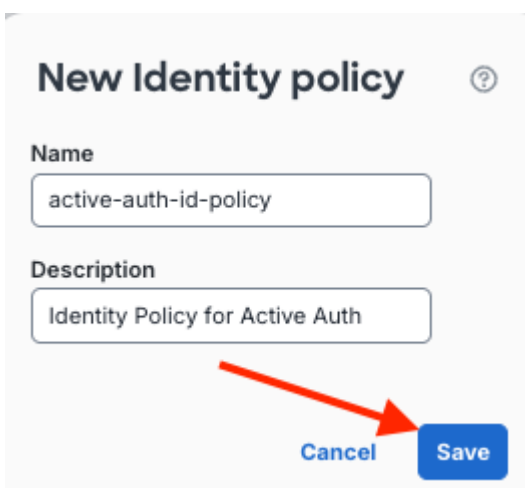
ID 정책 생성

2) 새 ID 정책을 만들고 Add a new policy(새 정책 추가)를 클릭합니다.



새 ID 정책 구성 추가

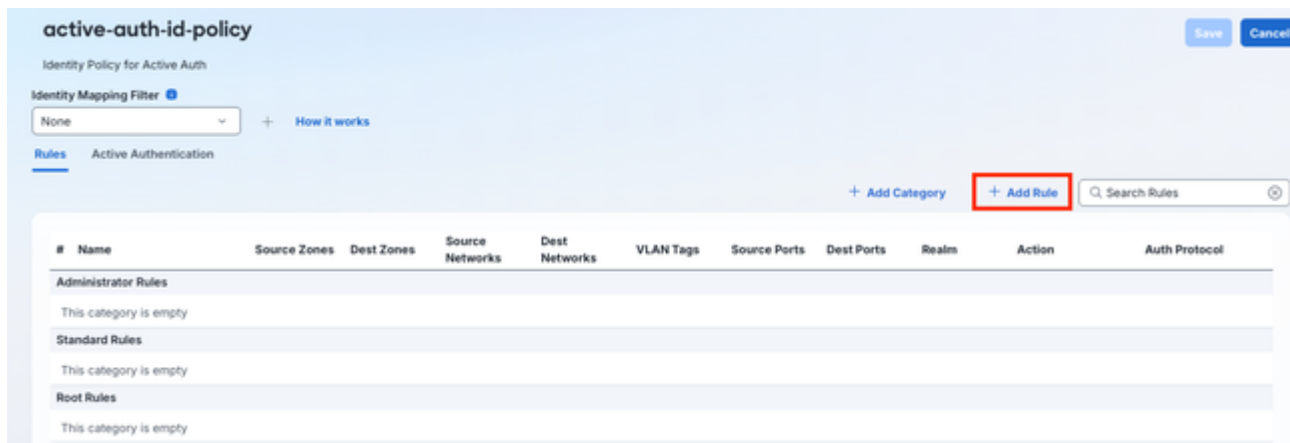
3) 이름을 할당하고, 해당되는 경우 새 ID 정책에 대한 설명을 할당합니다. 저장을 클릭합니다.



새 ID 정책 이름 지정

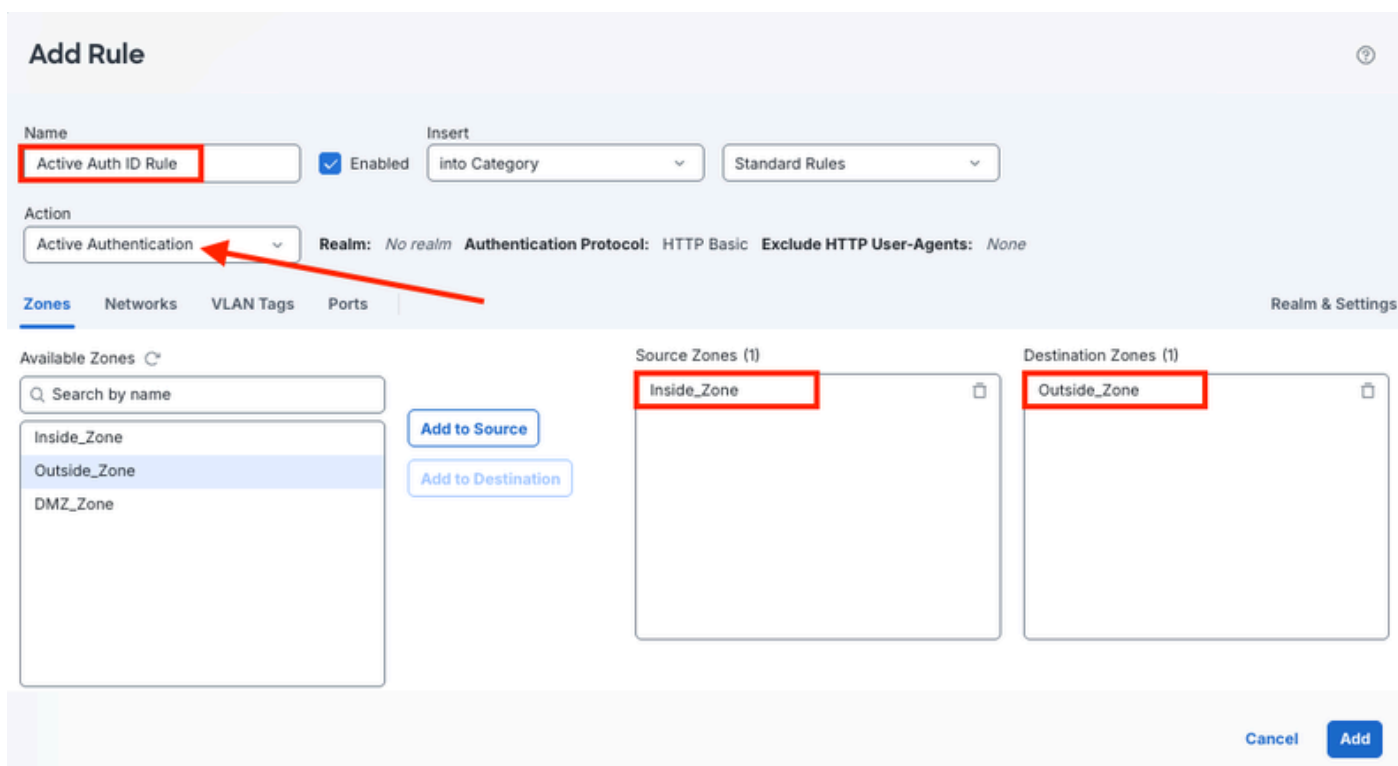
4단계: ID 정책 규칙 구성

1) + Add Rule을 클릭하여 새 규칙을 추가합니다.



새 ID 정책 규칙 추가

2) 새 규칙의 이름을 지정하고, Action 드롭다운 목록에서 Active Authentication을 선택하고, Active Authentication을 수행하기 위해 규칙과 일치해야 하는 특정 영역/네트워크의 범위를 좁힙니다.



활성 인증 규칙 설정 구성

3) Add(추가)를 클릭하기 전에 Rule Editor(규칙 편집기)에서 Realm and Settings(영역 및 설정) 탭을 클릭합니다. 이전 단계에서 구성된 영역이 인증 영역으로 선택되었는지 확인한 다음 Add를 클릭합니다.

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

Id 규칙에 대한 영역 및 설정 구성

4) 규칙이 추가 및 구성됩니다. 저장을 클릭합니다.

active-auth-id-policy

Identity Policy for Active Auth

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

[Rules](#) Active Authentication

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

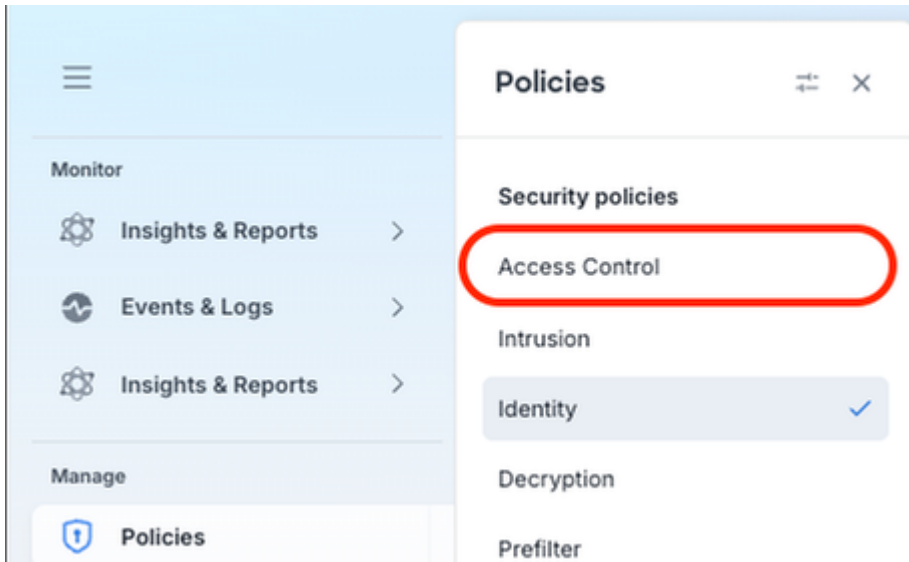
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	Active Auth ID Rule	Inside_Zone (Ro	Outside_Zone (f	any	any	any	any	any	azure-entra-san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

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

ID 정책 규칙 컨피그레이션 저장

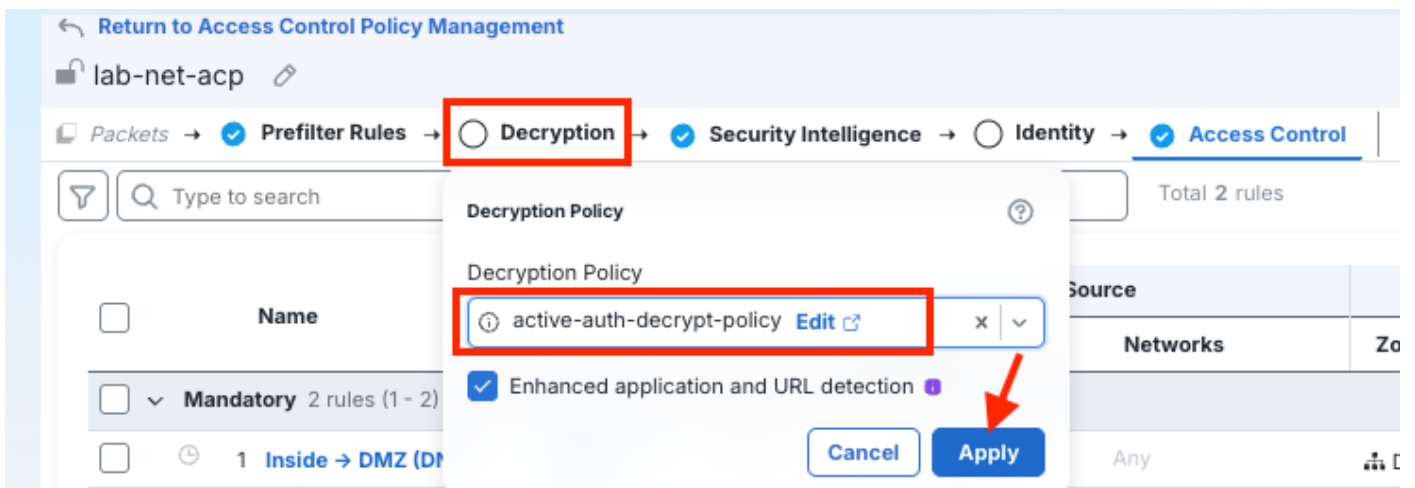
5단계: 액세스 제어 정책 구성

1) Policies > Security Policies > Access Control을 선택하고 FTD가 할당된 Access Control Policy를 클릭합니다.



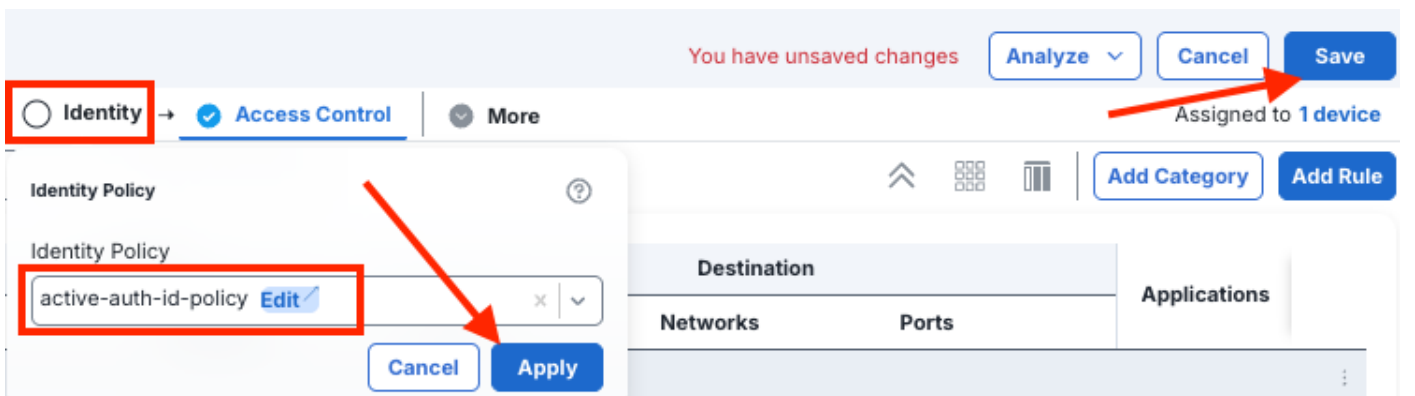
액세스 제어 정책 컨피그레이션

2) 이전 단계에서 구성한 암호 해독 정책이 액세스 제어 정책에 적용되는지 확인합니다.



액세스 제어에 암호 해독 정책 적용

3) 이전 단계에서 구성한 ID 정책이 액세스 제어 정책에도 적용되는지 확인합니다. 정책 변경 사항을 저장합니다.



4) 액티브 인증에 성공한 후 보안 방화벽을 통과하는 클라이언트 데이터 플레인 트래픽을 허용하는 규칙이 있는지 확인합니다. 여기에 표시된 예에서는 랩 환경에 따라 더 넓은 규칙 집합을 사용합니다.

☐	Name	Action	Source		Destination			Applications		
			Zones	Networks	Zones	Networks	Ports			
☐	Mandatory 2 rules (1 - 2)									
☐	1	Inside → DMZ (DNS)	Allow		Inside_Zone	Any	DMZ_Zone	Any	Application Default	DNS
☐	2	DMZ-Inside → Outside	Allow		DMZ_Zone	Any	Outside_Zone	Any	Any	Any
	Default (No rules)									

사용자 데이터 플레인 트래픽 규칙 집합

6단계: Cisco Secure Firewall 장치에 컨피그레이션 구축

배포되면 트래픽을 전송하는 클라이언트에 Microsoft 로그인 웹 페이지를 통해 Azure Entra를 통한 활성 인증을 수행하도록 프롬프트가 표시됩니다.

여기에 설명된 프로세스에 대한 추가 컨텍스트는 [활성 인증\(종속 포털\)을 위한 Microsoft Azure AD\(SAML\) 영역 만들기 - 장을 참조하십시오. FMC 디바이스 컨피그레이션 가이드 10.x의 영역.](#)

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인하십시오.

GUI

FMC에서 사용자 세션 및 활동을 검증합니다.

- Integrations(통합) > Users(사용자) > Active Sessions(활성 세션)를 선택합니다.

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

FMC 활성 세션 출력

- Integrations(통합) > Users(사용자) > User Activity(사용자 활동)를 선택합니다.

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 사용자 활동 출력

Azure에서 Microsoft Entra 관리 센터로 이동합니다.

- 엔터프라이즈 앱을 필터링하고 해당 앱을 검색/클릭합니다.

Microsoft Entra admin center

Search resources, services

Home > Enterprise applications

Enterprise applications | All applicatio

Overview

- Overview
- Diagnose and solve problems

Manage

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

Security

- Conditional Access
- Consent and permissions
- Application policies

Home Favorites Entra ID Overview Users Groups Devices Agents Enterprise apps App registrations Roles & admins Delegated admin partners Tenant governance

« + New application ↺ R

View, filter, and search applica

The list of applications that are

Search: captive-

Name	↑↓	Obj
Captive-Auth...		efda

Red arrow points from 'Custom authentication extensions' to 'Captive-Auth...'.

Azure Enterprise 관리 센터 엔터프라이즈 앱 탐색

- Activity > Sign-in logs를 선택합니다.

Home > Enterprise applications | All applications > Captive-Auth-SAML

Captive-Auth-SAML | Sign-in logs

Enterprise Application

«

Download

Export data Settings

Troubleshoot

Refresh

Manage view

Got feedback?

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Want to switch back to the legacy signin logs experience? Click here to leave the preview.

Add filter

Show dates as: UTC

Date range: 10/7/2026 - 10/7/2026

Application contains

User sign-ins (interactive)

User sign-ins (non-interactive)

Service principal sign-ins

Managed identity sign-ins

Date ↓	Request ID	User principal name	Application	Status
2026-10-07T06:10:02Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:00Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:59Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:58Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:52Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:51Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:29Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted

Azure 엔터프라이즈 응용 프로그램 로그인 활동 로그

CLI

- FTD CLI에서 SAML 및 종속 포털 응답과 관련된 통계를 볼 수 있습니다.

<#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
```

문제 해결

종속 포털 디버그

- FTD에서 시스템 지원 captive-portal-debug 명령을 사용할 수 있습니다. 출력은 디버그를 활성화하는 방법을 보여주며 종속 포털 흐름을 이해하는 데 도움이 되도록 출력의 주요 세그먼트를 기록합니다.

<#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 portal

192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 didn't find active binding, initiating captive portal

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 is complete

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_MATCH

...

!---

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_LOGIN
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 app event changes: service, client, host, url
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_FORWARDING
...
!---

```

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 username
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 username
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 username
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 username
...

```

사용자 ID 덤프

- FTD에서 현재 사용자 ID 상태 데이터의 스냅샷을 만들려면 FTD CLI에서 system support firewall-engine-dump-user-identity-data 명령을 실행합니다.

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

```
Successfully commanded snort.
```

```
>
```

- Expert 모드 CLI에서 FTD 디바이스의 로컬 관리자 자격 증명으로 로그인하는 동안 /ngfw/var/sf/user_enforcement/user_identity.dump에서 덤프된 파일의 내용을 확인합니다

```
<#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:
```

```
-----
```

```
...
```

가능한 문제

종속 포털 알 수 없는 인증 기관

문제: 인증을 시도할 때 클라이언트 브라우저에서 알 수 없는 발급자 오류를 반환합니다.

가능한 원인: 클라이언트 브라우저 내에서 내부 인증 기관을 신뢰할 수 없습니다.

해결: 브라우저 내에서 CA를 신뢰할 수 있는지 확인합니다. 여기에 표시된 예에서는 내부 CA 인증서를 신뢰할 수 있음을 확인합니다.

종속 포털 "서버를 찾을 수 없음

문제: 클라이언트 브라우저가 종속 포털을 로드하려고 시도하면 기본 URL에 연결하려고 시도하는 동안 기본 URL에 대해 "Server Not Found"가 반환됩니다.

가능한 원인: DNS 연결 또는 DNS 잘못된 컨피그레이션입니다.

해결: 클라이언트에 A 레코드를 확인하도록 구성된 적절한 DNS 서버가 있는지 확인합니다. 서버에 FQDN에 매핑된 A 레코드가 있는지, 그리고 서버에 연결할 수 있으며 응답이 있는지 확인합니다.

관련 정보

- [활성 인증\(종속 포털\)을 위한 Microsoft Azure AD\(SAML\) 영역 만들기 - FMC Device Config Guide 10.x](#)
- [Azure Event Hub 설명서](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.