

보안 방화벽에서 제로 트러스트 원격 액세스 구축 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[필수 구성](#)

[일반 컨피그레이션](#)

[애플리케이션 그룹 구성](#)

[애플리케이션 그룹 1: 듀오를 IdP로 사용](#)

[응용 프로그램 그룹 2: Microsoft Enterprise ID\(Azure AD\)를 IdP로 사용](#)

[애플리케이션 구성](#)

[응용 프로그램 1: FMC 웹 UI 테스트\(응용 프로그램 그룹 1의 멤버\)](#)

[애플리케이션 2: CTB 웹 UI\(애플리케이션 그룹 2의 멤버\)](#)

[다음을 확인합니다.](#)

[모니터링](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 보안 방화벽에서 클라이언트리스 제로 트러스트 액세스 원격 액세스 구축을 구성하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- FMC(Firepower Management Center)
- 기본 ZTNA 지식
- SAML(Basic Security Assertion Markup Language) 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Firewall 버전 7.4.1
- FMC(Firepower Management Center) 버전 7.4.1
- Duo as IdP(Identity Provider)
- Microsoft Entra ID(이전, Azure AD)를 IdP로 사용

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

제로 트러스트 액세스 기능은 ZTNA(Zero Trust Network Access) 원칙을 기반으로 합니다. ZTNA는 암시적 신뢰를 없애는 제로 트러스트 보안 모델입니다. 모델은 사용자, 요청의 컨텍스트, 액세스 권한이 부여된 경우 위험을 분석한 후 최소 권한 액세스 권한을 부여합니다.

ZTNA의 현재 요구 사항 및 제한 사항은 다음과 같습니다.

- FMC 버전 7.4.0에서 관리되는 Secure Firewall 버전 7.4.0에서 지원됨(Firepower 4K Series)
- FMC 버전 7.4.1에서 관리되는 Secure Firewall 버전 7.4.1에서 지원됨(다른 모든 플랫폼)
- 웹 애플리케이션(HTTPS)만 지원됩니다. 암호 해독 제외가 필요한 시나리오는 지원되지 않습니다.
- SAML IdP만 지원합니다.
- 원격 액세스를 위해서는 공용 DNS 업데이트가 필요합니다.
- IPv6는 지원되지 않습니다. NAT66, NAT64 및 NAT46 시나리오는 지원되지 않습니다.
- 이 기능은 Snort 3이 활성화된 경우에만 위협 방어에서 사용할 수 있습니다.
- 보호된 웹 응용 프로그램의 모든 하이퍼링크에는 상대 경로가 있어야 합니다.
- 가상 호스트에서 실행되거나 내부 로드 밸런서 뒤에서 실행되는 보호된 웹 애플리케이션은 동일한 외부 및 내부 URL을 사용해야 합니다.
- 개별 모드 클러스터에서는 지원되지 않습니다.
- 엄격한 HTTP 호스트 헤더 검증이 활성화된 응용 프로그램에서는 지원되지 않습니다.
- 애플리케이션 서버가 여러 애플리케이션을 호스팅하고 TLS Client Hello의 SNI(Server Name Indication) 헤더를 기반으로 콘텐츠를 제공하는 경우, 제로 트러스트 애플리케이션 컨피그레이션의 외부 URL이 해당 특정 애플리케이션의 SNI와 일치해야 합니다.
- 라우팅 모드에서만 지원됨
- Smart License 필요(평가 모드에서 작동하지 않음)

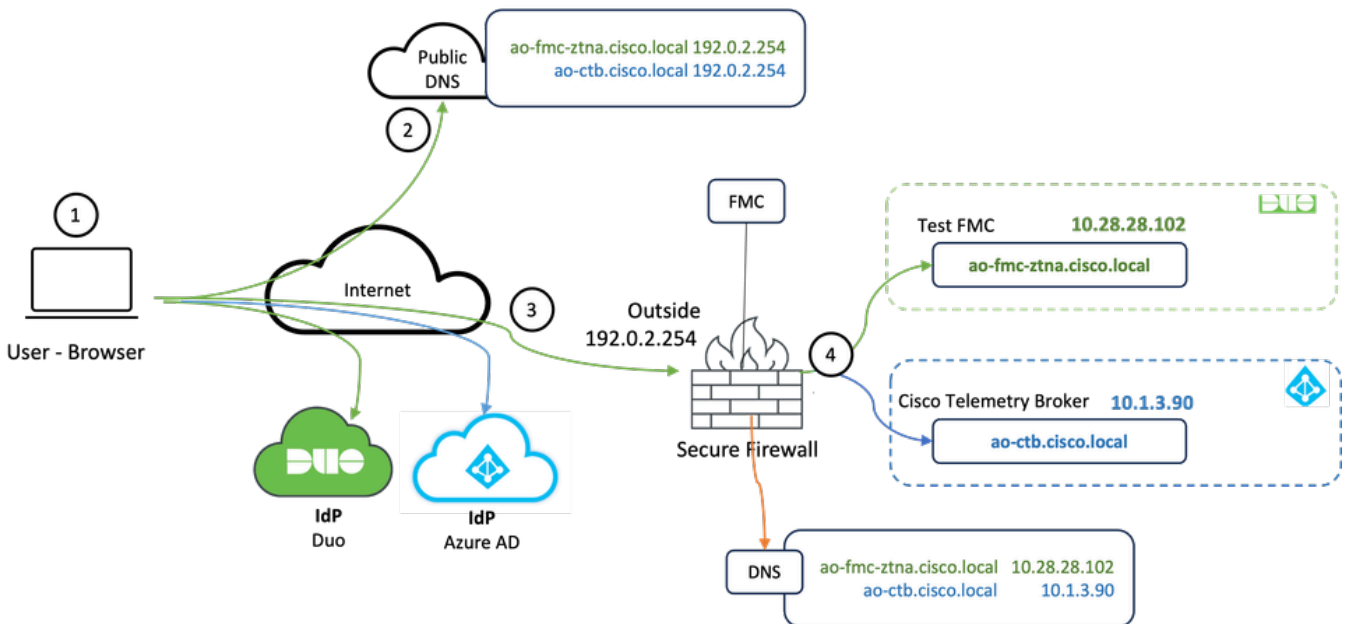
보안 방화벽의 Zero Trust Access에 대한 자세한 내용 및 내용은 [Cisco Secure Firewall Management Center Device Configuration Guide, 7.4](#)를 참조하십시오.

구성

이 문서에서는 ZTNA의 원격 액세스 구축을 중점적으로 다룹니다.

이 예제 시나리오에서는 원격 사용자가 보안 방화벽 뒤에서 호스팅되는 테스트 FMC 및 Cisco CTB(Telemetry Broker)의 웹 사용자 인터페이스(UI)에 액세스해야 합니다. 다음 다이어그램에 나와 있는 것처럼, 두 개의 서로 다른 IdP, 즉 Duo와 Microsoft Entra ID를 통해 이러한 애플리케이션에 액세스할 수 있습니다.

네트워크 다이어그램



토폴로지 다이어그램

1. 원격 사용자는 Secure Firewall 뒤에서 호스팅되는 애플리케이션에 액세스해야 합니다.
2. 각 애플리케이션에는 공용 DNS 서버에 DNS 항목이 있어야 합니다.
3. 이러한 애플리케이션 이름은 Secure Firewall Outside 인터페이스의 IP 주소로 확인해야 합니다.
4. 보안 방화벽은 애플리케이션의 실제 IP 주소를 확인하고 SAML 인증을 사용하여 각 애플리케이션에 대해 각 사용자를 인증합니다.

필수 구성

IdP(Identity Provider) 및 DNS(Domain Name Server)

- 응용 프로그램 또는 응용 프로그램 그룹은 Duo, Okta 또는 Azure AD와 같은 SAML IdP(Identity Provider)에서 구성해야 합니다. 이 예에서는 Duo 및 Microsoft Entra ID가 IdP로 사용됩니다.
- IdPs에서 생성된 인증서 및 메타데이터는 보안 방화벽에서 애플리케이션을 구성할 때 사용됨

니다

내부 및 외부 DNS 서버

- 외부 DNS 서버(원격 사용자가 사용)에는 애플리케이션의 FQDN 항목이 있어야 하며 보안 방화벽 외부 인터페이스 IP 주소로 확인해야 합니다
- 내부 DNS 서버(보안 방화벽에서 사용)에는 애플리케이션의 FQDN 항목이 있어야 하며 애플리케이션의 실제 IP 주소로 확인되어야 합니다

인증서

다음 인증서는 ZTNA 정책 컨피그레이션에 필요합니다.

- ID/프록시 인증서: 보안 방화벽에서 애플리케이션을 가장하는 데 사용됩니다. 여기서 Secure Firewall은 SAML SP(Service Provider)의 역할을 합니다. 이 인증서는 프라이빗 애플리케이션의 FQDN과 일치하는 와일드카드 또는 SAN(주체 대체 이름) 인증서여야 합니다(인증 전 단계의 모든 프라이빗 애플리케이션을 나타내는 공통 인증서).
- IdP 인증서: 인증에 사용되는 IdP는 정의된 각 애플리케이션 또는 애플리케이션 그룹에 대한 인증서를 제공합니다. 이 인증서는 보안 방화벽이 수신 SAML 어설션에 대한 IdP 서명을 확인할 수 있음(애플리케이션 그룹에 대해 정의된 경우 전체 애플리케이션 그룹에 대해 동일한 인증서가 사용됨)
- 애플리케이션 인증서: 원격 사용자로부터 애플리케이션으로 전송되는 암호화된 트래픽은 보안 방화벽에 의해 해독되어야 합니다. 따라서 각 애플리케이션의 인증서 체인과 개인 키를 보안 방화벽에 추가해야 합니다.

일반 컨피그레이션


새 Zero Trust 애플리케이션을 구성하려면 다음 단계를 수행합니다.

1. Policies(정책) > Access Control(액세스 제어) > Zero Trust Application(제로 트러스트 애플리케이션)으로 이동하고 Add Policy(정책 추가)를 클릭합니다.


2. 필수 필드를 완료합니다.

a) 일반: 정책의 이름 및 설명을 입력합니다.

b) 도메인 이름: DNS에 추가된 이름이며 애플리케이션이 액세스되는 위협 방어 게이트웨이 인터페이스로 확인되어야 합니다.

 참고: 도메인 이름은 애플리케이션 그룹의 모든 개인 애플리케이션에 대한 ACS URL을 생성하는 데 사용됩니다.

c) ID 인증서: 이 인증서는 인증 전 단계의 모든 개인 애플리케이션을 나타내는 공통 인증서입니다.

 참고: 이 인증서는 전용 애플리케이션의 FQDN과 일치하는 와일드카드 또는 SAN(주체 대체 이름) 인증서여야 합니다.

d) 보안 영역: 사설 애플리케이션이 규제되는 외부 또는/및 내부 영역을 선택합니다.

e) 전역 포트 풀: 이 풀의 고유 포트가 각 개인 애플리케이션에 할당됩니다.

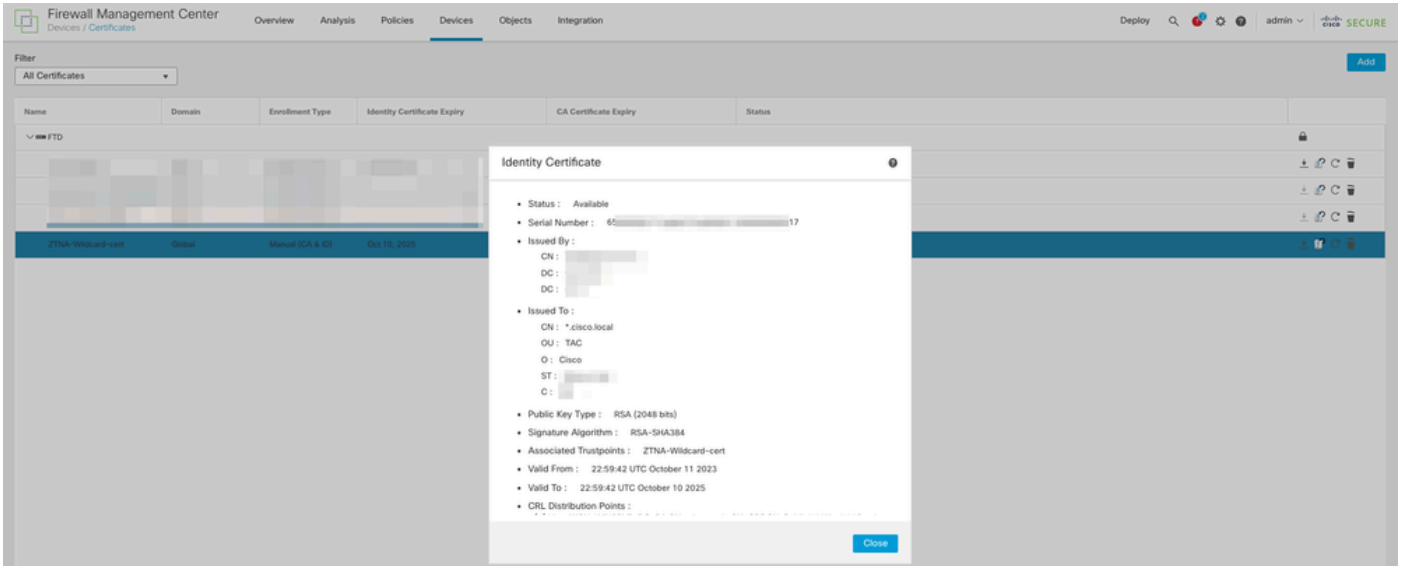
f) 보안 제어(선택 사항): 프라이빗 애플리케이션이 검사 대상인지 여부를 선택합니다.

이 샘플 컨피그레이션에서는 다음 정보를 입력했습니다.

The screenshot shows the 'Add a Zero Trust Application Policy' configuration page in the Firewall Management Center. The page is titled 'Add a Zero Trust Application Policy' and includes a 'Cancel' button and a 'Save' button. The configuration is divided into several sections:

- General:** Name* (ZTNA-TAC), Description.
- Domain Name:** Domain Name* (with a note: 'Ensure that the domain name is added to the DNS. The domain name resolves to the threat defense gateway interface from where the application is accessed. The domain name is used to generate the ACS URL for all private applications in an Application Group.')
- Identify Certificate:** Certificate* (ZTNA-Wildcard-cert, with a note: 'This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications.')
- Security Zones:** Security Zones* (Outside, with a note: 'This is the default setting for all private applications. It can be overridden at an Application or Application Group level.')
- Global Port Pool:** Port Range* (20000-22000, Range: (1024-65535), with a note: 'Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other configurations.')
- Security Controls (Optional):** Intrusion Policy (None), Variable Set (None), Malware and File Policy (None, with a note: 'These are default settings for all private applications. It can be overridden at an Application or Application Group level.')

이 경우에 사용되는 ID/프록시 인증서는 사설 애플리케이션의 FQDN과 일치시키기 위한 와일드카드 인증서입니다.



3. 정책을 저장합니다.

4. 신규 애플리케이션 그룹 및/또는 신규 애플리케이션을 생성합니다.

- 애플리케이션은 SAML 인증, 인터페이스 액세스, 침입 및 악성코드와 파일 정책을 사용하여 사설 웹 애플리케이션을 정의합니다.
- 애플리케이션 그룹을 사용하면 여러 애플리케이션을 그룹화하고 SAML 인증, 인터페이스 액세스 및 보안 제어 설정과 같은 공통 설정을 공유할 수 있습니다.

이 예에서는 두 개의 서로 다른 애플리케이션 그룹과 두 개의 서로 다른 애플리케이션이 구성됩니다. 하나는 Duo에서 애플리케이션을 인증하기 위한 것입니다(테스트 FMC 웹 UI). 다른 하나는 Microsoft Entra ID(CTB 웹 UI)에서 애플리케이션을 인증하기 위한 것입니다.

애플리케이션 그룹 구성

애플리케이션 그룹 1: 듀오를 IdP로 사용

a. 애플리케이션 그룹 이름을 입력하고 다음을 클릭하여 SAML SP(서비스 공급자) 메타데이터를 표시합니다.

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group

Name External_Duo

Edit

2 SAML Service Provider (SP) Metadata

The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.

Entity ID

https://[redacted]/External_Duo/saml/sp/metadata

Copy

Assertion Consumer Service (ACS) URL

https://[redacted]/External_Duo/+CSCOE+/saml/sp/acs?tgname=

Copy

Download SP Metadata

Next

3 SAML Identity Provider (IdP) Metadata

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

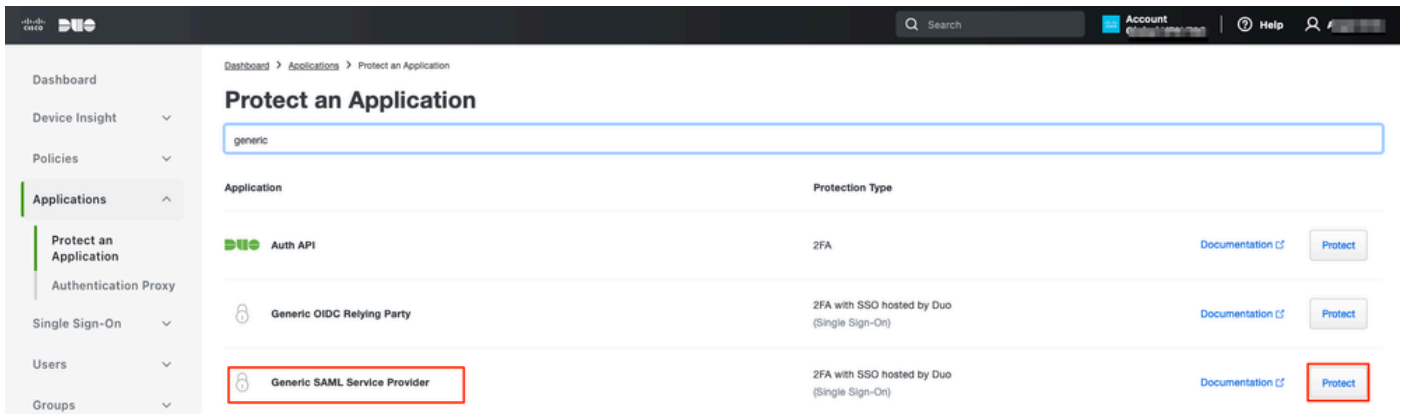
Finish

b. SAML SP 메타데이터가 표시되면 IdP로 이동하여 새 SAML SSO 애플리케이션을 구성합니다.

c. Duo에 로그인하여 Applications(애플리케이션) > Protect an Application(애플리케이션 보호)으로 이동합니다.

The screenshot shows the Duo Applications dashboard. The left sidebar contains navigation options: Dashboard, Device Insight, Policies, Applications (selected), Authentication Proxy, Single Sign-On, Users, Groups, and Endpoints. The main content area is titled 'Applications' and includes a sub-header 'Manage your update to the new Universal Prompt experience, all in one place.' Below this, there are two buttons: 'See My Progress' and 'Get More Information'. A summary section shows '11 All Applications' and '0 End of Support'. At the bottom right, there is an 'Export' button and a search bar. A red arrow points to a 'Protect an Application' button in the top right corner of the main content area.

d. Generic SAML Service Provider(일반 SAML 서비스 제공자)를 찾고 Protect(보호)를 클릭합니다.



e. Secure Firewall에서 컨피그레이션을 계속 진행해야 하므로 IdP에서 인증서 및 SAML 메타데이터를 다운로드합니다.

f. ZTNA 애플리케이션 그룹(단계 a에서 생성됨)에서 Entity ID 및 Assertion Consumer Service(ACS) URL을 입력합니다.

- Dashboard
- Device Insight
- Policies
- Applications**
- Protect an Application
- Authentication Proxy
- Single Sign-On
- Users
- Groups
- Endpoints
- 2FA Devices
- Administrators
- Trusted Endpoints
- Trust Monitor
- Reports
- Settings
- Billing

You're using the new Admin Panel menu and left-side navigation.

[Provide feedback](#)

[Temporarily switch to the old experience](#)

Generic SAML Service Provider - Single Sign-On 1

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<code>https://sso-.../metadata</code>	Copy
Single Sign-On URL	<code>https://sso-8.../sso</code>	Copy
Single Log-Out URL	<code>https://sso-i.../slo</code>	Copy
Metadata URL	<code>https://sso-8.../metadata</code>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<code>9E:5...5C</code>	Copy
SHA-256 Fingerprint	<code>?:85:...E9:52</code>	Copy

Downloads

Certificate	Download certificate	Expires: 01-19-2038
SAML Metadata	Download XML	

Service Provider

Metadata Discovery: None (manual input)

[Early Access](#)

Entity ID *

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

[+ Add an ACS URL](#)

g. 특정 요구 사항에 따라 애플리케이션을 편집하고 원하는 사용자만 애플리케이션에 액세스할 수 있도록 허용한 후 Save(저장)를 클릭합니다.

Type Generic SAML Service Provider - Single Sign-On

Name
 Duo Push users will see this when approving transactions.

Self-service portal Let users remove devices, add new devices, and reactivate Duo Mobile
 See [Self-Service Portal documentation](#)
 To allow Duo to notify users about self-service portal activity, select [Settings > Notifications](#)

Username normalization Username normalization for Single-Sign On applications is controlled by the enabled authentication source. Please visit your [authentication source](#) to modify this configuration.
 Controls if a username should be altered before trying to match them with a Duo user account.

Voice greeting
 Specify the message read to users who use phone callback, followed by authentication instructions. Maximum 512 characters.

Notes
 For internal use. Maximum 512 characters.

Administrative unit

Permitted groups Only allow authentication from users in certain groups

 When unchecked, all users can authenticate to this application.

Allowed Hostnames Since this application is using Frameless Duo Universal Prompt, configuring allowed hostnames is no longer supported.
 [Get more information](#)

h. FMC로 다시 이동하고 IdP에서 다운로드한 파일을 사용하여 애플리케이션 그룹에 SAML IdP 메타데이터를 추가합니다.

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group

Name External_Duo

Edit

2 SAML Service Provider (SP) Metadata

Entity ID https://[redacted]External_Duo/saml/sp/metadata
Assertion Consumer Service (ACS) URL https://[redacted]External_Duo/+CSCOE+/saml/sp/acs?tname=D...

Edit

3 SAML Identity Provider (IdP) Metadata

Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.

- Import IdP Metadata
- Manual Configuration
- Configure Later

Import IdP Metadata

Drag and drop your file here
[or select file](#)
External Applications ZTNA - IDP Metadata.xml

Entity ID*

https://sso-8[redacted] N

Single Sign-On URL*

https://sso-8[redacted] N

IdP Certificate

MIIDDTC[redacted]yDQYJKoZI
[redacted]
[redacted]
[redacted]

Next

Cancel

Finish

i. Next(다음)를 클릭하고 요구 사항에 따라 Re-Authentication Interval(재인증 간격) 및 Security Controls(보안 제어)를 구성합니다. 요약 컨피그레이션을 검토하고 Finish(마침)를 클릭합니다.

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1	Application Group	Name	External_Duo	Edit
2	SAML Service Provider (SP) Metadata	Entity ID	https://[redacted] External_Duo/saml/sp/metadata	Edit
		Assertion Consumer Service (ACS) URL	https://[redacted] External_Duo/+CSCOE+/saml/sp/acs?tname=D...	
3	SAML Identity Provider (IdP) Metadata	Entity ID	https://ssc [redacted]	Edit
		Single Sign-On URL	https://ssc [redacted]	
		IdP Certificate	External_Duo-1697063490514	
4	Re-Authentication Interval	Timeout Interval	1440 minutes	Edit
5	Security Zones and Security Controls	Security Zones	Inherited: (Outside)	Edit
		Intrusion Policy	Inherited: (None)	
		Variable Set	Inherited: (None)	
		Malware and File Policy	Inherited: (None)	

Cancel

Finish

응용 프로그램 그룹 2: Microsoft Enterprise ID(Azure AD)를 IdP로 사용

a. 애플리케이션 그룹 이름을 입력하고 다음을 클릭하여 SAML SP(서비스 공급자) 메타데이터를 표시합니다.

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- 1 Application Group** Edit
Name **Azure_apps**
- 2 SAML Service Provider (SP) Metadata**
The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.
Entity ID
 Copy
Assertion Consumer Service (ACS) URL
 Copy
Download SP Metadata Next
- 3 SAML Identity Provider (IdP) Metadata**
- 4 Re-Authentication Interval**
- 5 Security Zones and Security Controls**

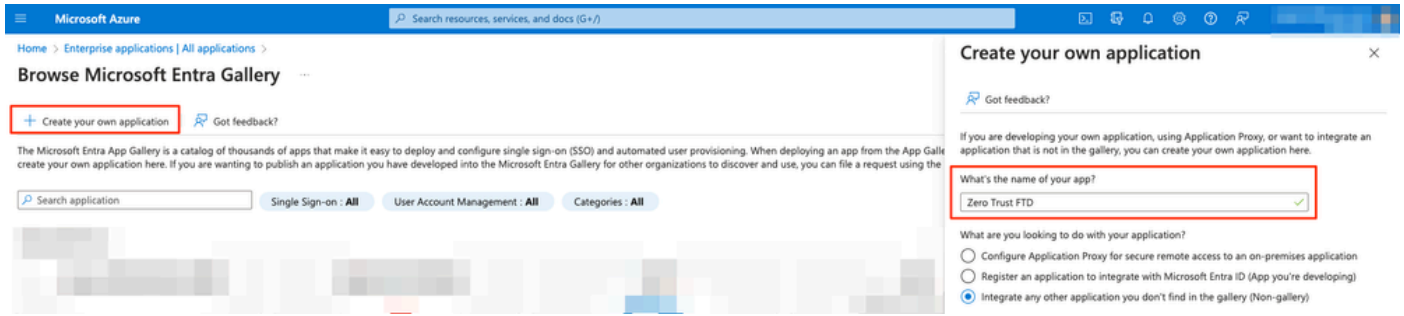
Cancel Finish

b. SAML SP 메타데이터가 표시되면 IdP로 이동하여 새 SAML SSO 애플리케이션을 구성합니다.

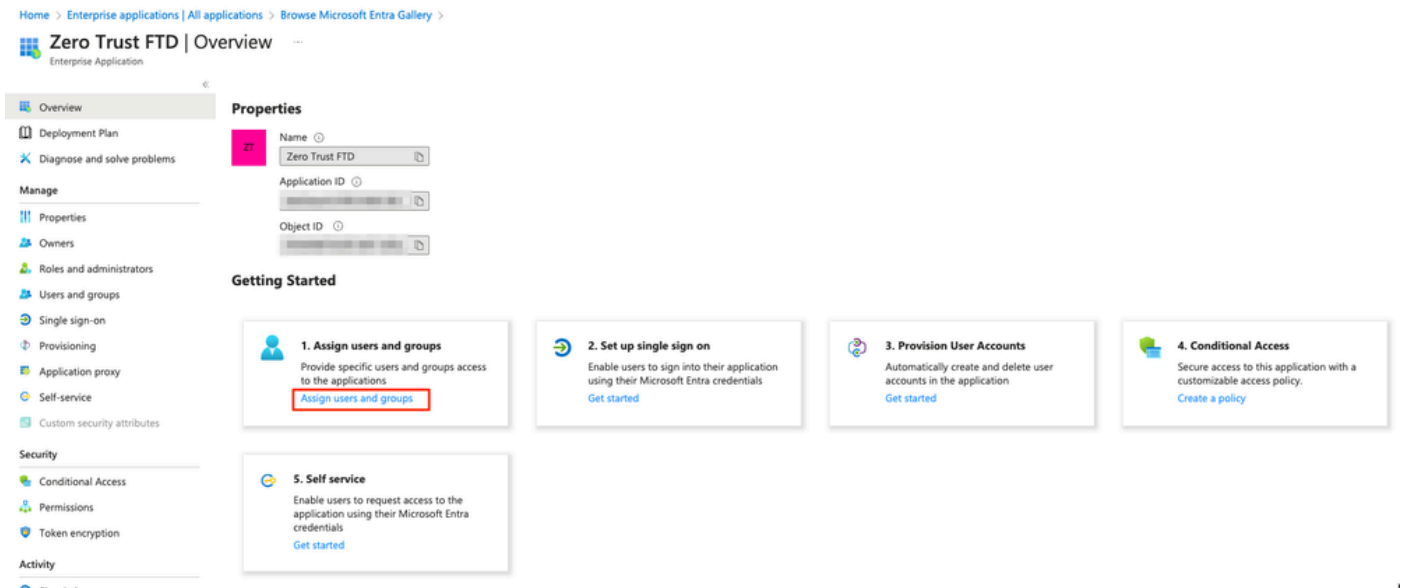
c. Microsoft Azure에 로그인하고 Enterprise Applications(엔터프라이즈 애플리케이션) > New Application(새 애플리케이션)으로 이동합니다.

The screenshot shows the Microsoft Azure portal interface for Enterprise Applications. The breadcrumb navigation is 'Home > Enterprise applications'. The main heading is 'Enterprise applications | All applications'. On the left sidebar, 'All applications' is highlighted. The main content area shows a '+ New application' button (highlighted with a red box), 'Refresh', 'Download (Export)', 'Preview info', 'Columns', 'Preview features', and 'Got feedback?' options. Below this is a search bar and filter options: 'Application type == Enterprise Applications' and 'Application ID starts with'. A table header is visible with columns: Name, Object ID, Application ID, Homepage URL, and Created on. The table indicates '77 applications found'.

d. Create your own application(자체 애플리케이션 생성) > Enter the name of application(애플리케이션 이름 입력) > Create(생성)를 클릭합니다.



e. 애플리케이션을 열고 Assign users and groups(사용자 및 그룹 할당)를 클릭하여 애플리케이션에 액세스할 수 있는 사용자 및/또는 그룹을 정의합니다.



f. Add user/group(사용자/그룹 추가) > Select the required users/groups(필요한 사용자/그룹 선택) > Assign(할당)을 클릭합니다. 올바른 사용자/그룹을 할당했으면 Single sign-on을 클릭합니다.

Zero Trust FTD | Users and groups

Overview
Deployment Plan
Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on

1 Add user/group Edit assignment Remove Update credentials Columns Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & gro...

	Display Name	Object Type
<input type="checkbox"/>	AO Angel	
<input type="checkbox"/>	FG Fernando	

g. Single sign-on 섹션에서 SAML을 클릭합니다.

Zero Trust FTD | Single sign-on

Overview
Deployment Plan
Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy

Select a single sign-on method [Help me decide](#)

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).

- Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
- Password-based**
Password storage and replay using a web browser extension or mobile app.

h. 메타데이터 파일 업로드를 클릭하고 서비스 공급자(보안 방화벽)에서 다운로드한 XML 파일을 선택하거나 ZTNA 애플리케이션 그룹(단계 a에서 생성됨)에서 엔티티 ID 및 어설션 소비자 서비스 (ACS) URL을 수동으로 입력합니다.

참고: 보안 방화벽에서 컨피그레이션을 계속 진행하려면 페더레이션 메타데이터 XML을 다운로드하거나 인증서를 개별적으로 다운로드하고(기본 64) IdP(로그인 및 로그아웃 URL 및 Microsoft Entra 식별자)에서 SAML 메타데이터를 복사해야 합니다.

Zero Trust FTD | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs
 - Provisioning logs
 - Access reviews
- Troubleshooting + Support
 - New support request

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Zero Trust FTD.

- Basic SAML Configuration** Edit

Identifier (Entity ID)	https://[redacted]/Azure_apps/saml/sp/metadata
Reply URL (Assertion Consumer Service URL)	https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tgname=DefaultZeroTrustGroup
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims** Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates**

Token signing certificate Edit	Active
Status	Active
Thumbprint	[redacted]
Expiration	[redacted]
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download
Verification certificates (optional) Edit	
Required	No
Active	0
Expired	0
- Set up Zero Trust FTD**

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://[redacted]
Microsoft Entra Identifier	https://[redacted]
Logout URL	https://[redacted]

i. FMC로 다시 이동하여 IdP에서 다운로드한 메타데이터 파일을 사용하여 SAML IdP 메타데이터를 애플리케이션 그룹 2로 가져오거나 필요한 데이터를 수동으로 입력합니다.

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group

Name Azure_apps

Edit

2 SAML Service Provider (SP) Metadata

Entity ID https://[redacted]/Azure_apps/saml/sp/metadata
Assertion Consumer Service (ACS) URL https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=Def...

Edit

3 SAML Identity Provider (IdP) Metadata

Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.

Import IdP Metadata

Manual Configuration

Configure Later

Import IdP Metadata

Drag and drop your file here
or select file
Zero Trust FTD.xml

Entity ID*

https://[redacted]

Single Sign-On URL*

https://[redacted]

IdP Certificate

MIIc8DCCAdigAwIBAgIQdtt7Lwlj7aRGm1m212dU/DANBqkqhkiG9w0B

[redacted certificate content]

Next

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

Finish

j. Next(다음)를 클릭하고 요구 사항에 따라 Re-Authentication Interval(재인증 간격) 및 Security Controls(보안 제어)를 구성합니다. 요약 컨피그레이션을 검토하고 Finish(마침)를 클릭합니다.

Add Application Group
? ✕

An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1	Application Group		Edit
	Name	Azure_apps	
2	SAML Service Provider (SP) Metadata		Edit
	Entity ID	https://[redacted]/Azure_apps/saml/sp/metadata	
	Assertion Consumer Service (ACS) URL	https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=Def...	
3	SAML Identity Provider (IdP) Metadata		Edit
	Entity ID	https://[redacted]	
	Single Sign-On URL	https://[redacted]	
	IdP Certificate	[redacted]	
4	Re-Authentication Interval		Edit
	Timeout Interval	1440 minutes	
5	Security Zones and Security Controls		Edit
	Security Zones	Inherited: (Outside)	
	Intrusion Policy	Inherited: (None)	
	Variable Set	Inherited: (None)	
	Malware and File Policy	Inherited: (None)	

Cancel
Finish

애플리케이션 구성

애플리케이션 그룹이 생성되었으므로 애플리케이션 추가를 클릭하여 원격으로 보호 및 액세스할 애플리케이션을 정의합니다.

1. 애플리케이션 설정을 입력합니다.

a) 애플리케이션 이름: 구성된 애플리케이션의 식별자.

b) 외부 URL: 공용/외부 DNS 레코드에 있는 애플리케이션의 게시된 URL. 사용자가 애플리케이션에 원격으로 액세스하기 위해 사용하는 URL입니다.

c) 애플리케이션 URL: 애플리케이션의 실제 FQDN 또는 네트워크 IP. 보안 방화벽에서 애플리케이션에 연결하기 위해 사용하는 URL입니다.

참고: 기본적으로 외부 URL은 애플리케이션 URL로 사용됩니다. 다른 애플리케이션 URL을 지정하려면 이 확인란의 선택을 취소합니다.

(d) 애플리케이션 인증서: 액세스할 애플리케이션의 인증서 체인 및 개인 키(FMC 홈 페이지 > Objects > Object Management > PKI > Internal certs에서 추가)

e) IPv4 NAT 소스(선택 사항): 원격 사용자의 소스 IP 주소는 패킷을 애플리케이션에 전달하기 전에 선택한 주소로 변환됩니다(IPv4 주소를 갖는 호스트 및 범위 유형 네트워크 객체/객체 그룹만 지원됨). 이는 애플리케이션이 Secure Firewall을 통해 원격 사용자에게 다시 경로를 제공하도록 구성할 수 있습니다

f) 응용 프로그램 그룹(선택 사항): 이 응용 프로그램을 기존 응용 프로그램 그룹에 추가하여 구성된 설정을 사용하려면 선택합니다.

이 예에서 ZTNA를 사용하여 액세스할 수 있는 애플리케이션은 테스트 FMC 웹 UI 및 Secure Firewall 뒤에 있는 CTB의 웹 UI입니다.

애플리케이션의 인증서는 Objects(개체) > Object Management(개체 관리) > PKI > Internal certs(내부 인증서)에서 추가해야 합니다.

Add Known Internal Certificate



Name:

ao-fmc-ztna.cisco.local

Certificate Data or, choose a file:

Browse..

```
-----BEGIN CERTIFICATE-----  
[Redacted Certificate Data]  
T  
G  
AY
```

Key or, choose a file:

Browse..

```
-----BEGIN RSA PRIVATE KEY-----  
[Redacted Private Key Data]
```

Encrypted, and the password is: [Password Field]

Cancel

Save

참고: ZTNA로 액세스할 각 애플리케이션에 대한 모든 인증서를 추가해야 합니다.

인증서가 내부 인증서로 추가되었으면 나머지 설정을 계속 구성합니다.

이 예에 대해 구성된 애플리케이션 설정은 다음과 같습니다.

응용 프로그램 1: FMC 웹 UI 테스트(응용 프로그램 그룹 1의 멤버)

Add Application ? ×

Enabled

- Application Settings**
 - Application Name*
 - External URL* ?
 - Application URL (FQDN or Network IP)*
 - Use External URL as Application URL
By default, External URL is used as Application URL. Uncheck the checkbox to specify a different URL. For e.g., https://10.72.34.57:8443
 - Application Certificate* ?
 × ▼ +
 - IPv4 NAT Source ?
 ▼ +
 - Application Group
 × ▼
- SAML Service Provider (SP) Metadata
- SAML Identity Provider (IdP) Metadata
- Re-Authentication Interval
- Security Zones and Security Controls

Next

Cancel Finish

응용 프로그램이 응용 프로그램 그룹 1에 추가되었으므로 이 응용 프로그램에 대해 나머지 설정이 상속됩니다. 보안 영역 및 보안 제어를 다른 설정으로 재정의할 수 있습니다.

구성된 애플리케이션을 검토하고 Finish(마침)를 클릭합니다.

Add Application ? ×

Enabled

1 Application Settings Edit

Application Name	FMC
External URL	https://ao-fmc-ztna.cisco.local
Application URL	https://ao-fmc-ztna.cisco.local
IPv4 NAT Source	-
Application Certificate	ao-fmc-ztna.cisco.local
Application Group	External_Duo

2 SAML Service Provider (SP) Metadata

Configurations are derived from Application Group 'External_Duo'

3 SAML Identity Provider (IdP) Metadata

Configurations are derived from Application Group 'External_Duo'

4 Re-Authentication Interval

Configurations are derived from Application Group 'External_Duo'

5 Security Zones and Security Controls Edit

Security Zones	Inherited: (Outside)
Intrusion Policy	Inherited: (None)
Variable Set	Inherited: (None)
Malware and File Policy	Inherited: (None)

Cancel Finish

애플리케이션 2: CTB 웹 UI(애플리케이션 그룹 2의 멤버)

이 응용 프로그램에 대한 구성 요약은 다음과 같습니다.

Enabled

1 Application Settings Edit

Application Name: CTB
 External URL: https://ao-ctb.cisco.local
 Application URL: https://ao-ctb.cisco.local
 IPv4 NAT Source: ZTNA_NAT_CTB
 Application Certificate: ao-ctb.cisco.local
 Application Group: Azure_apps

2 SAML Service Provider (SP) Metadata
 Configurations are derived from Application Group 'Azure_apps'


3 SAML Identity Provider (IdP) Metadata
 Configurations are derived from Application Group 'Azure_apps'

4 Re-Authentication Interval
 Configurations are derived from Application Group 'Azure_apps'

5 Security Zones and Security Controls Edit

Security Zones: Inherited: (Outside)
 Intrusion Policy: Inherited: (None)
 Variable Set: Inherited: (None)
 Malware and File Policy: Inherited: (None)

Cancel Finish

 참고: 이 애플리케이션의 경우 네트워크 객체 "ZTNA_NAT_CTB"가 IPv4 NAT 소스로 구성되었습니다. 이 구성에서는 패킷을 애플리케이션에 전달하기 전에 원격 사용자의 소스 IP 주소가 구성된 객체 내의 IP 주소로 변환됩니다. 이는 애플리케이션(CTB) 기본 경로가 보안 방화벽이 아닌 게이트웨이를 가리키므로 반환 트래픽이 원격 사용자에게 전송되지 않기 때문에 구성되었습니다. 이 NAT 컨피그레이션을 통해서서브넷 ZTNA_NAT_CTB가 보안 방화벽을 통해 연결할 수 있도록 애플리케이션에 고정 경로가 구성되었습니다.

애플리케이션이 구성되면 해당 애플리케이션 그룹 아래에 표시됩니다.

ZTNA-TAC Targeted: 1 device
 Groups: 3 Applications:

Applications Settings

Bulk Actions Add Application Group Add Application

Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled
<input checked="" type="checkbox"/> Azure_apps (1 Application)			https://sts.v...	Outside (Inherited)	None (Inherited)	None (Inherited)	
<input checked="" type="checkbox"/> CTB	https://ao-ctb.cisco.local	https://ao-ctb.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True
<input checked="" type="checkbox"/> External_Duo (1 Application)			https://sso-...	Outside (Inherited)	None (Inherited)	None (Inherited)	
<input checked="" type="checkbox"/> FMC	https://ao-fmc-ztna.cisco.local	https://ao-fmc-ztna.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True


마지막으로, 변경 사항을 저장하고 컨피그레이션을 구축합니다.

다음을 확인합니다.

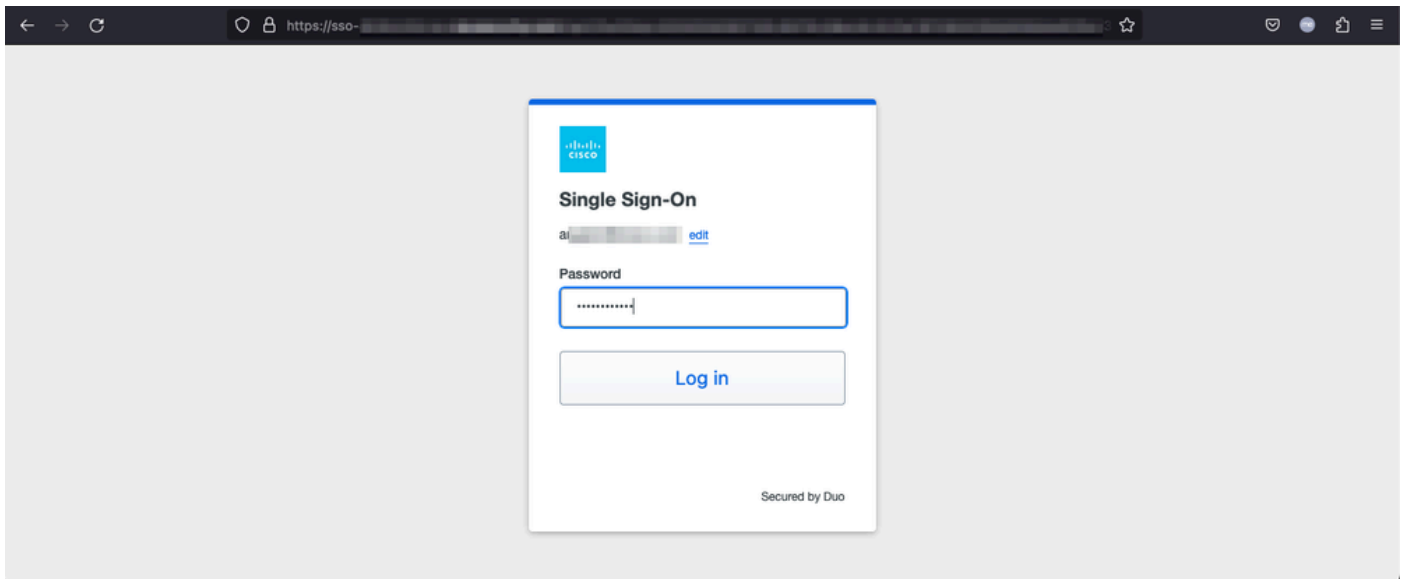
컨피그레이션이 실행되면 원격 사용자가 외부 URL을 통해 애플리케이션에 연결할 수 있으며, 해당 IdP에서 허용하면 애플리케이션에 액세스할 수 있습니다.

애플리케이션 1

1. 사용자가 웹 브라우저를 열고 애플리케이션 1의 외부 URL로 이동합니다. 이 경우 외부 URL은 <https://ao-fmc-ztna.cisco.local/>입니다.

 참고: 외부 URL 이름은 구성된 보안 방화벽 인터페이스의 IP 주소로 확인되어야 합니다. 이 예에서는 외부 인터페이스 IP 주소(192.0.2.254)로 확인됩니다

2. 새 액세스이므로 사용자는 애플리케이션에 대해 구성된 IdP 로그인 포털로 리디렉션됩니다.

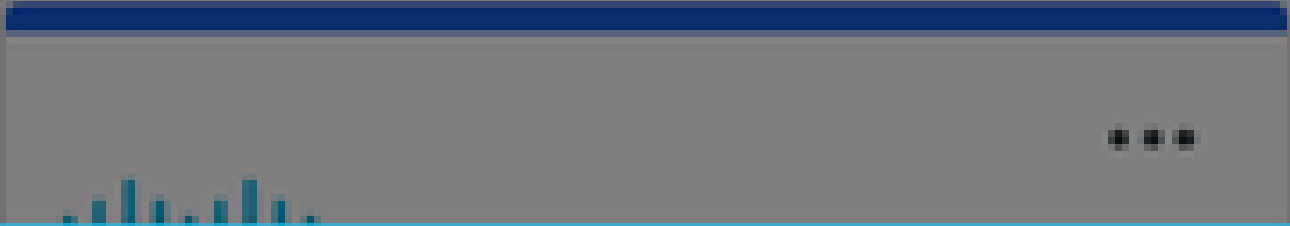


3. 사용자에게 MFA 푸시를 보냅니다(IdP에 구성된 MFA 방법에 따라 다름).



Accounts

Add



Are you logging in to **External Applications ZTNA?**

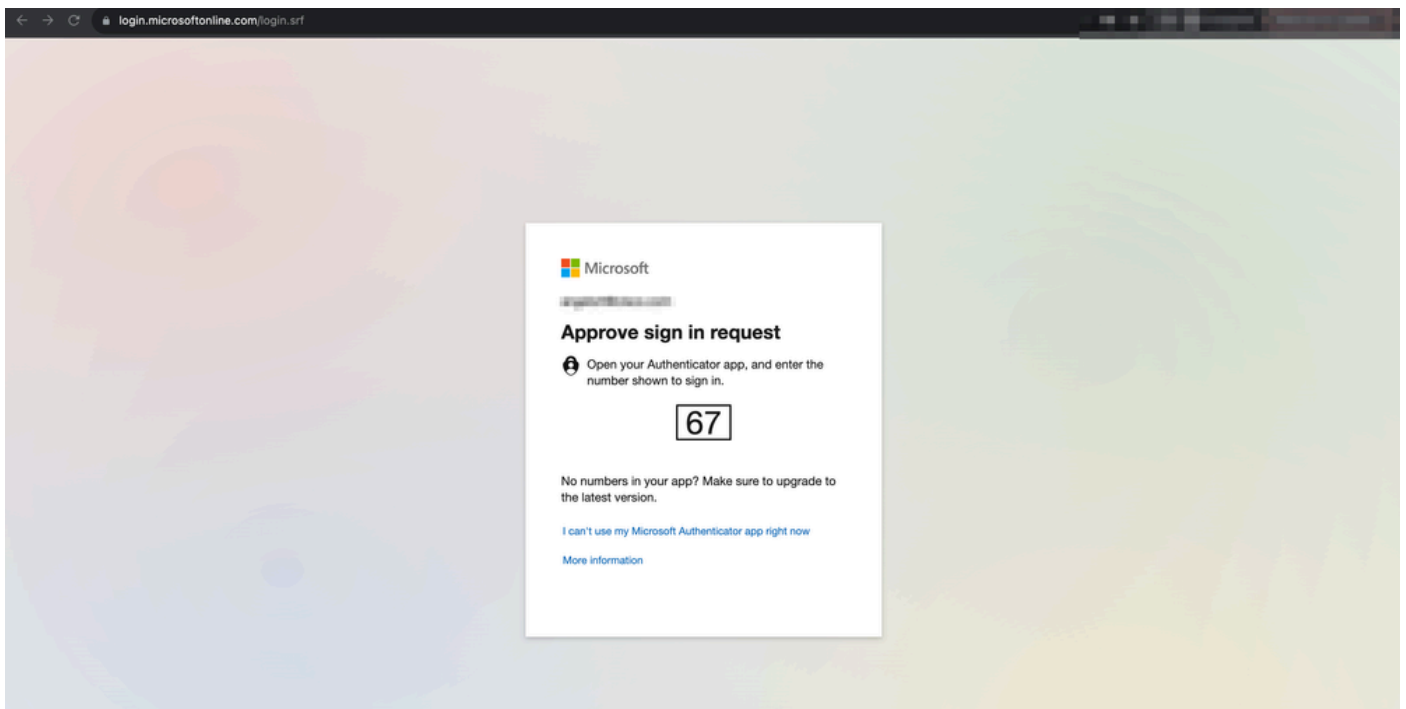
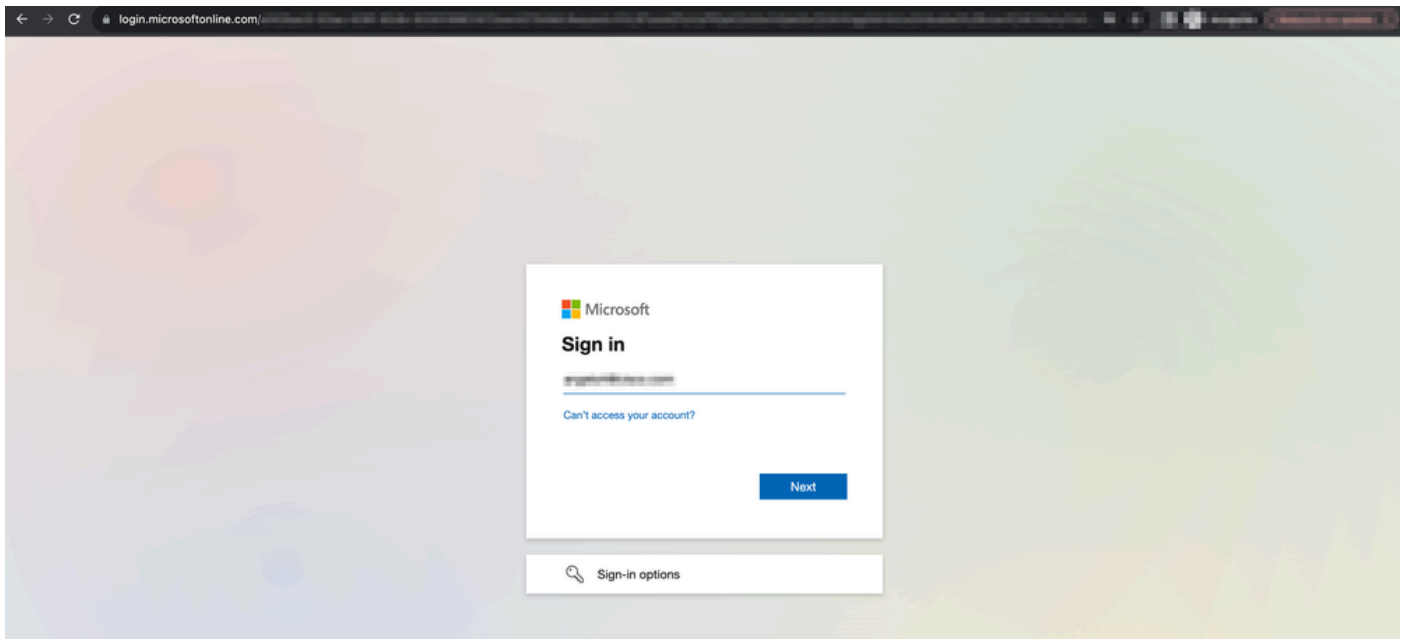
 Global VPN TAC

 [Redacted]

 1:13 p.m.

 [Redacted]

2. 새 액세스이므로 사용자는 애플리케이션에 대해 구성된 IdP 로그인 포털로 리디렉션됩니다.

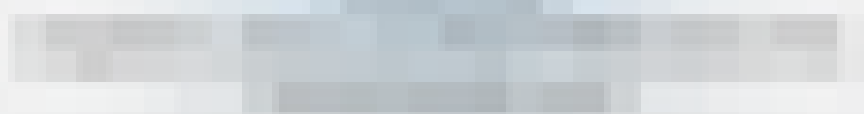


3. 사용자에게 MFA 푸시를 보냅니다(IdP에 구성된 MFA 방법에 따라 다름).

4:24



Are you trying to sign in?



Enter the number shown to sign in.

Enter number

No, it's not me

Yes

컨피그레이션에서 문제가 발생한 시점을 표시하여 사용자의 문제 해결 프로세스를 용이하게 하도록 설계되었습니다

- 진단을 통해 전반적인 분석(정상 여부 확인)을 제공하며 문제를 해결하기 위해 분석할 수 있는 자세한 로그를 수집합니다.

애플리케이션별 진단을 사용하여 다음을 탐지합니다.

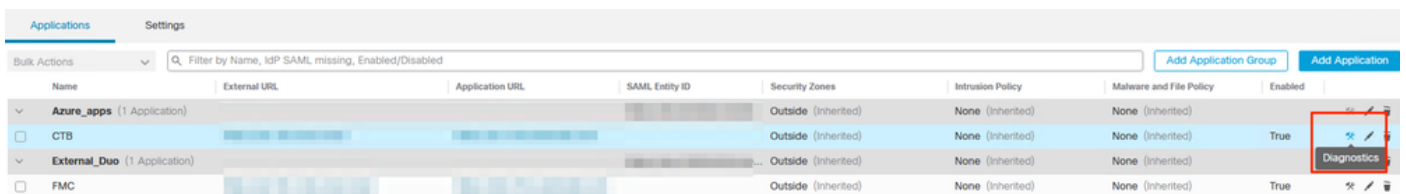
- DNS 관련 문제
- 잘못된 컨피그레이션(예: 소켓 열리지 않음, 분류 규칙, NAT 규칙)
- 제로 트러스트 액세스 정책의 문제
- 인터페이스 관련 문제(예: 인터페이스가 구성되지 않았거나 인터페이스가 다운됨)


검색할 일반 진단:

- 강력한 암호 라이선스가 활성화되지 않은 경우
- 애플리케이션 인증서가 유효하지 않은 경우
- 인증 방법이 기본 터널 그룹에서 SAML로 초기화되지 않은 경우
- HA 및 클러스터 대량 동기화 문제
- 토큰 또는 암호 해독 관련 문제를 진단하기 위해 snort 카운터에서 통찰력을 얻습니다.
- 소스 변환의 PAT 폴 소모 문제

진단을 실행하려면

- 각 ZTNA 애플리케이션에 대해 표시되는 진단 아이콘으로 이동합니다.



Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled	
Azure_apps (1 Application)				Outside (Inherited)	None (Inherited)	None (Inherited)		
<input type="checkbox"/> CTB				Outside (Inherited)	None (Inherited)	None (Inherited)	True	
External_Duo (1 Application)				Outside (Inherited)	None (Inherited)	None (Inherited)		
<input type="checkbox"/> FMC				Outside (Inherited)	None (Inherited)	None (Inherited)	True	

- 장치를 선택하고 실행을 클릭합니다.

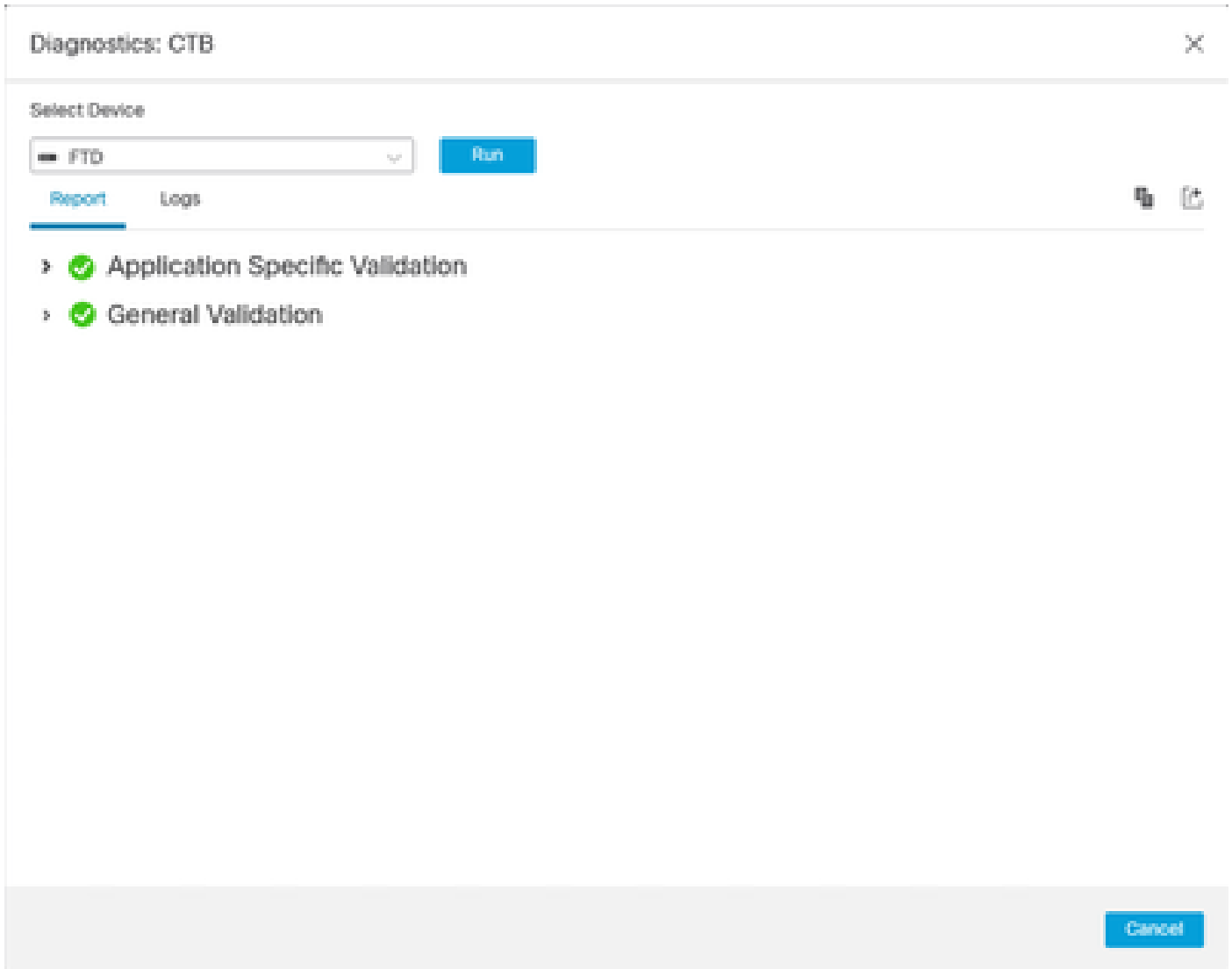
Select Device

Select...
FTD

Run

Cancel

3. 보고서의 결과를 조회합니다.



FTD CLI에서는 show 및 clear 명령을 사용하여 제로 트러스트 컨피그레이션을 보고 통계와 세션 정보를 표시할 수 있습니다.

```
<#root>
```

```
firepower# show running-config zero-trust
```

```
application      Show application configuration information
application-group Show application group configuration
|                Output modifiers
<cr>
```

```
firepower# show zero-trust
```

```
sessions  Show zero-trust sessions
statistics Show zero-trust statistics
```

```
firepower# show zero-trust sessions
```

```
application      show zero-trust sessions for application
application-group show zero-trust sessions for application group
count            show zero-trust sessions count
user            show zero-trust sessions for user
detail          show detailed info for the session
|              Output modifiers
<cr>
```

```
firepower# clear zero-trust
```

```
sessions  Clear all zero-trust sessions
statistics Clear all zero-trust statistics
```

```
firepower# clear zero-trust sessions
```

```
application Clear zero-trust sessions for application
user        Clear zero-trust sessions for user
<cr>
```

제로 트러스트 및 webvpn 모듈 디버그를 활성화하려면 Lina 프롬프트에서 다음 명령을 사용합니다

- firepower# 디버그 제로 트러스트 255
- firepower 번호 디버그 webvpn 요청 255
- firepower 번호 디버그 webvpn 응답 255
- firepower 번호 디버그 webvpn saml 255

관련 정보

- 추가 지원이 필요한 경우 TAC(Technical Assistance Center)에 문의하십시오. 유효한 지원 계약이 필요합니다. [Cisco Worldwide Support Contacts](#).
- [여기서](#) Cisco VPN Community를 방문할 수도 [있습니다](#).

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.