Okta를 사용한 SSO 인증을 통해 Firepower Management Center 액세스 구성

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>배경 정보</u> <u>제한 사항 및 제한 사항</u> <u>구성 단계</u> ID 제공자(OKTA)의 구성 단계 FMC의 구성 단계 다음을 확인합니다.

소개

이 문서에서는 관리 액세스를 위해 SSO(Single Sign-On)를 사용하여 인증하도록 FMC(Firepower Management Center)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Single Sign-On 및 SAML에 대한 기본적인 이해
- iDP(Identity Provider)의 컨피그레이션 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco FMC(Firepower Management Center) 버전 6.7.0
- ID 공급자로 확인

참고: 이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 컨 피그레이션 변경의 잠재적 영향을 이해해야 합니다.

배경 정보

증명(사용자 이름 및 비밀번호)으로 한 번만 로그인하면 여러 애플리케이션 및 웹 사이트를 통해 안 전하게 인증할 수 있습니다. SSO를 사용하면 사용자가 액세스하려는 애플리케이션 또는 웹 사이트 는 신뢰할 수 있는 서드파티에 의존하여 사용자가 자신이 누구인지 확인합니다.

SAML(Security Assertion Markup Language)은 보안 도메인 간에 인증 및 권한 부여 데이터를 교환 하기 위한 XML 기반 프레임워크입니다.사용자, SP(서비스 제공자) 및 사용자가 여러 서비스에 대 해 한 번에 로그인할 수 있도록 하는 IdP(Identity Provider) 간에 신뢰 원을 생성합니다

SP(서비스 제공자)는 iDP(Identity Provider)에서 발급한 인증 어설션을 수신하고 수락하는 엔티티 입니다. 서비스 공급자는 이름에 따라 서비스를 제공하는 반면 ID 제공자는 사용자의 ID(인증)를 제 공합니다.



SSO SAML Workflow

이러한 iDP는 지원되며 인증을 위해 테스트됩니다.

- 옥타
- OneLogin
- PingID
- Azure AD
- 기타(SAML 2.0을 준수하는 모든 iDP)

참고: 새 라이센스 요구 사항이 없습니다.이 기능은 라이센스와 평가 모드에서 작동합니다.

제한 사항 및 제한 사항

다음은 FMC 액세스를 위한 SSO 인증의 알려진 제한 사항 및 제한 사항입니다.

- SSO는 전역 도메인에 대해서만 구성할 수 있습니다.
- HA 쌍의 FMC에는 개별 컨피그레이션이 필요합니다.
- 로컬/AD 관리자만 FMC에서 SSO를 구성할 수 있습니다(SSO 관리자 사용자는 FMC에서 SSO 설정을 구성/업데이트할 수 없음).

구성 단계

ID 제공자(OKTA)의 구성 단계

1단계. Okta 포털에 로그인합니다.이 이미지에 표시된 대로 **Applications(애플리케이션**) > Applications(애플리케이션)로 이동합니다.

okta	Get Started	Dashboard	Direc	ory	Applications	Security	Workflow	Reports	Settings
🕖 Dash	board				Applications				
Status									۲
Usage - La	st 30 Days								0

2단계. 이 이미지에 표시된 대로 Add(추가)Application(애플리케이션)을 클릭합니다.

Application:	S	
HAD Application	Assign Applications	
Q Search		

3단계. 이 이미지에 표시된 대로 Create NewApp를 클릭합니다.

← Back to Applications		Create New App
CATEGORIES	O Search	
Featured	Q pedicini	
API Management 6	Featured Integrations	See all

4단계. **플랫폼**을 **웹**으로 **선택합니다**.로그인 **방법**을 SAML 2.0으로 선택합니다. 이 이미지에 표시된 대로 생성을 누릅니다.

	Create a New Application Integratio	n	×	
en:	Platform	Web		
	Sign on method	Secure Web Authentication (SWA) Uses credentials to sign in. This integration works with most apps.		. 40
at an		 SAML 2.0 Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it. 		or
lci		OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.		r
		Create Cancel		

5단계. 앱 이름, 앱 로고(선택 사항)를 입력하고 이 이미지에 표시된 대로 다음을 클릭합니다.



App name	FMC-Login	
App logo (optional) 🔞	cisco.	
	cisco.png	Browse
	Upload Logo	
	Requirements	
	 Must be PNG, JPG or GIF Less than 1MB 	
	For Best Results, use a PNG image with	
	 Minimum 420px by 120px to prevent u Landscape orientation Transparent background 	pscaling
App visibility	Do not display application icon to users	4
	_	

Cancel

Next

6단계. SAML 설정을 입력합니다.

단일 로그인 URL: https://<fmc URL>/saml/acs

대상 그룹 URI(SP 엔티티 ID): https://<fmc URL>/saml/metadata

기본 릴레이 상태: /ui/login



Single sign on URL 👔	https:// <f< th=""><th>MC URL>/saml/acs</th><th></th><th></th></f<>	MC URL>/saml/acs		
	✓ Use the second se	nis for Recipient URL	and Destination L	IRL
	Allow	this app to request o	other SSO URLs	
Audience URI (SP Entity ID) 🥼	https://<	FMC URL>/saml/meta	adata	
Default RelayState 👔	/ui/login			
	If no value	is set, a blank Relay	State is sent	
Name ID format 💿	Unspecif	fied	•	
Application username 👔	Okta use	ername	Ŧ	
Update application username	on Create a	nd update	Ŧ	
			s	how Advanced Setting
ATTRIBUTE STATEMENTS (O	PTIONAL)			LEARN MOR
Name N	ame format (optional)	Value		
	Unspecified +			•

7단계. 이 이미지에 표시된 대로 **애플리케이션 > 애플리케이션**으로 돌아갑니다.



8단계. 생성된 앱 이름을 클릭합니다.

Add Application Assign Applications More • Q bearch STATUS ACTIVE INACTIVE	Applications	ŝ		
Q Search STATUS ACTIVE INACTIVE	HAD Application	ilija Assign	Applications	More 🔻
STATUS FMC-Login	Q Search	_		
ACTIVE 0	STATUS		alada	FMC-Login
INACTIVE 0	ACTIVE	1	cisco.	
	INACTIVE	0		

9단계. 지정으로 **이동합니다**.Assign(할당)을 **클릭합니다**.

생성된 앱 이름에 개별 사용자 또는 그룹을 할당하도록 선택할 수 있습니다.

General Sig	gn On Import	Assignments		
Assign 🗸	Convert Assignments		Q Search	People *
FILTERS	Person		Туре	
People	Rohan Biswas robiswas@cise	co.com	Individual	×

10단계. **로그인**으로 **이동합니다**.[설정 지침 **보기]를 클릭합니다. ID 공급자 메타데이터를 클릭하여** iDP의 메타데이터를 봅니다.

FMC-Login	ogs
eneral Sign On Import Assignments	
Settings	Edit
SIGN ON METHODS	
The sign-on method determines how a user signs into on methods require additional configuration in the 3rd Application username is determined by the user profile	and manages their credentials for an application. Some sign- party application.
The sign-on method determines how a user signs into on methods require additional configuration in the 3rd Application username is determined by the user profile SAML 2.0	and manages their credentials for an application. Some sign- party application. mapping. Configure profile mapping
The sign-on method determines how a user signs into on methods require additional configuration in the 3rd Application username is determined by the user profile SAML 2.0 Default Relay State ui/login	and manages their credentials for an application. Some sign- party application. mapping. Configure profile mapping
The sign-on method determines how a user signs into on methods require additional configuration in the 3rd Application username is determined by the user profile SAML 2.0 Default Relay State ui/login SAML 2.0 is not configured until you comp View Setup Instructions	and manages their credentials for an application. Some sign- party application. • mapping. Configure profile mapping

파일을 FMC에서 사용할 **.xml** 파일로 저장합니다.



FMC의 구성 단계

1단계. 관리자 권한으로 FMC에 로그인합니다.System(**시스템) > Users(사용자)로 이동합니다**.

Overview Analysis Policies Devices Objects AMP Intelligence Objects AMP Intelligence Objects AMP Intelligence Objects Licenses Logging + Heattin + Monte

2단계. 이 이미지에 표시된 대로 Single Sign-On을 클릭합니다.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	
							_
Users	User Role	es Exte	ernal Autho	entication	Sing	le Sign-On	

3단계. Single Sign-On 옵션을 활성화합니다(기본적으로 비활성화됨).

e Sign-On		
	Single Sign-On (SSO) Configuration	
	This feature is currently disabled.	

4단계. Configure SSO(**SSO 구성)를** 클릭하여 FMC에서 SSO 컨피그레이션을 시작합니다.

Single Sign-On (SSO) Configura	ation
The FMC supports Security Assertion Marke authentication. This allows you to provide access to your FMC dashboard. Show More	up Language (SAML) for single sign-on (SSO)
No SSO configuration created.	Configure SSO

5단계. FMC SAML Provider를 선택합니다.Next(다음)를 클릭합니다.

이 데모에서는 Okta가 사용됩니다.

Calact the CAMI provider to suthentic	ata CCO unarr far tha EMC:	
 Okta 	ate 550 users for the PMC:	
OneLogin		
O PingID		
O Other		
ten 1 of 3		Nevt

6단계. Manual Configuration(**수동 컨피그레이션)을** 선택하고 iDP 데이터를 수동으로 입력할 수 있 습니다.다음**을** 클릭합니다.



또한 Upload **XML file(XML 파일 업로드)을** 선택하고 <u>Step 10 of Okta Configuration(</u>확인 컨피그레 이션<u>10단계</u>에서 검색된 XML 파일을 업로드할 수 있습니다.

Configure the SSO manual	e FMC to work with your Ol y, or upload the XML meta	kta IdP by selecting one of data file.	the following two options:	Fill out required fields for your
 Manual Upload 	Configuration XML File			
	Drag and drop an XML	file here, or click to uploa	d an XML file containing yo	our SSO credentials.

파일이 업로드되면 FMC에서 메타데이터를 표시합니다.이 이미지에 표시된 대로 Next를 클릭합니 다.

Configure Okta Metadata	•×
Configure the FMC to work with your Okta IdP by selecting one of the following two options: Fill out required fields for y SSO manually, or upload the XML metadata file. Manual Configuration Upload XML File	our
Drag and drop an XML file here, or click to upload an XML file containing your SSO credentials.	
File metadata.xml	
Identity Provider Single Sign-On URL https://cisco-robiswas.okta.com/app/ciscoorg842643_fmclogin_1/exkjmr3gbDQjCYNin4x6/sso/saml	
Identity Provider Issuer http://www.okta.com/exkjmr3gbDQjCYNin4x6	
X.509 Certificate MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1UI	
Step 2 of 3 Back	lext

7단계. 메타데이터를 확인합니다.이 이미지에 표시된 대로 Save를 클릭합니다.

Verify Okta Metadata	• ×				
Test the Okta metadata by clicking the Test Configuration button on the System / Users / Single Sign-On page you save.) Identity Provider Single Sign-On URL https://cisco-robiswas.okta.com/app/ciscoorg842643_fmclogin_1/exkjmr3gbDQjCYNin4x6/sso/saml					
Identity Provider Issuer http://www.okta.com/exkjmr3gbDQjCYNin4x6					
X.509 Certificate MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2	2FsaWZv				
Step 3 of 3 Back	Save				

8단계. Advanced Configuration(고급 컨피그레이션) 아래**에 Role Mapping/Default User Role(역할 매핑/기본 사용자 역할)을 구성합니다**.

Single Sign-On (SSO) (Configuration 🔍					
Configuration Details / Identity Provider Single Sign-On URL https://cisco-robiswas.okta.com/app/ciscoorg842643_ Identity Provider Issuer http://www.okta.com/exkjmr3gbDQjCYNin4x6 X.509 Certificate MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ						
 Advanced Configuration (Ro 	le Mapping)					
Default User Role	Administrator 🗸					
Access Admin						
Administrator						
Discovery Admin						
External Database User						
Intrusion Admin						
Maintenance User						
Network Admin						
Security Analyst						
Security Analyst (Read Only)						
Security Approver						

9단계. 구성을 테스트하려면 이 이미지에 표시된 대로 Test Configuration(컨피그레이션 테스트)을 클릭합니다.



테스트가 성공하면 이 이미지에 표시된 페이지가 브라우저의 새 탭에 표시됩니다.



10단계. Apply(**적용**)를 클릭하여 컨피그레이션을 저장합니다.

Configuration Details	/
Identity Provider Single	Sign-On URL
https://cisco-robisw	vas.okta.com/app/ciscoorg842643_
Identity Provider Issue	r
http://www.okta.co	m/exkjmr3gbDQjCYNin4x6
X.509 Certificate	
MIIDrDCCApSgAwI	BAgIGAXMtNBBjMA0GCSqGSIb3DQ
Advanced Conformation	ine (Dele Maneire)

SSO를 사용하도록 설정해야 합니다.



다음을 확인합니다.

브라우저에서 FMC URL로 이동합니다. https://<fmc URL>.Single Sign-On을 클릭합니다.

1		
T	cisco	7
11-14	Firepower	No. of Contraction of
TP.	Management	
	Center	穀
1		
	Username	
	Password	2
P	Single Sign-On	
K	Log In	5
1		X

····· iDP(Okta) 로그인 페이지로 리디렉션됩니다.SSO 자격 증명을 제공합니다.Sign **in(로그인)을 클릭 합니다**.

Connecting to	CISCO.	
---------------	--------	--

Sign-in with your cisco-org-842643 account to access FMC-

Login

OKCO	L
Sign In	
Username	
rabiouse@eleca.com	
robiswas@cisco.com	
Password	
Password	
Password Remember me	

성공하면 로그인하고 FMC 기본 페이지를 볼 수 있습니다.

FMC에서 System > Users로 이동하여 데이터베이스에 추가된 SSO 사용자를 확인합니다.

Users	User Roles	External Authentication	Single Sign-On						
						Create Use			
							Filter		
Username			Real Name	Roles	Authentication Method	Password Lifetime		Enabled	Actions
admin				Administrator	Internal	Unlimited			Ø
robiswas@	cisco.com			Administrator	External (SSO)				0