# Oktaを使用したSSO認証によるFirepower Management Center(FMC)アクセスの設定

# 内容

概要 <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>背景説明</u> <u>制限と制限</u> <u>設定手順</u> <u>アイデンティティプロバイダー(Okta)の設定手順</u> <u>FMCの設定手順</u> <u>確認</u>

# 概要

このドキュメントでは、管理アクセスにシングルサインオン(SSO)を使用して認証するように Firepower Management Center(FMC)を設定する方法について説明します。

# 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- •シングルサインオンとSAMLの基礎知識
- •アイデンティティプロバイダー(iDP)の設定について

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Firepower Management Center(FMC)/ $\mathcal{N} = \mathcal{V}6.7.0$
- IDプロバイダーとしてokta

**注:このド**キュメントの情報は、特定のラボ環境のデバイスから作成されたものです。この ドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動して います。ネットワークが稼働中の場合は、設定変更による潜在的な影響について理解してお いてください。

# 背景説明

シングルサインオン(SSO)は、IDおよびアクセス管理(IAM)のプロパティで、1つのクレデンシャ ル(ユーザ名とパスワード)を使用して1回だけログインするだけで、複数のアプリケーションや Webサイトで安全に認証できます。 SSOを使用すると、ユーザがアクセスしようとしているアプ リケーションまたはWebサイトは、信頼できるサードパーティに依存して、ユーザが自分が言っ ているユーザであることを確認します。

SAML(Security Assertion Markup Language)は、セキュリティドメイン間で認証および許可デー タを交換するためのXMLベースのフレームワークです。ユーザ、サービスプロバイダー(SP)、ア イデンティティプロバイダー(IdP)の間に信頼の輪が作成され、ユーザは複数のサービスに対して 一度にサインインできます

サービスプロバイダー(SP)は、アイデンティティプロバイダー(iDP)によって発行された認証アサ ーションを受信して受け入れるエンティティです。 名前に記載されているように、サービスプロ バイダーはサービスを提供し、アイデンティティプロバイダーはユーザのアイデンティティを提 供します(認証)。



#### SSO SAML Workflow

次のiDPがサポートされ、認証がテストされています。

- 岡田
- OneLogin
- PingID

• Azure AD

その他(SAML 2.0に準拠するiDP)

**注:新しい**ライセンス要件はありません。この機能は、ライセンス供与モードと評価モード で動作します。

#### 制限と制限

FMCアクセスのSSO認証に関する既知の制限と制限は次のとおりです。

- •SSOはグローバルドメインに対してのみ設定できます
- •HAペアのFMCでは個別の設定が必要
- ローカル/AD管理者のみがFMCでSSOを設定できます(SSO管理者ユーザはFMCでSSO設定 を設定/更新できません)。

# 設定手順

### アイデンティティプロバイダー(Okta)の設定手順

ステップ1:Oktaポータルにログインします。次の図に示すように、[**Applications**] > [**Applications**]に移動します。

okta	Get Started	Dashboard	Direc o	vry	Applications	Security	Workflow	Reports	Settings
💋 Dash	board				Applications				
Status									۲
Usage - La	st 30 Days								۲

ステップ2:次の図に示すように、[AddApplication]をクリックします。

Application	S	
H Add Application	Assign Applications	]
Q Search		

ステップ3 : 次の図に示すように、[Create NewApp]をクリ**ックします**。

Back to Applications     Add Application		Create New App
CATEGORIES	O kearch	
Featured	Q pearun.	
API Management 6	Featured Integrations	See all

ステップ4:[Platform]を[**Web**]として選択**します**。Sign Onメソッド**をSAML 2.0**と選択し**ます。次** の図に示すように[Create]をクリックします。

Platform	Web 💌
Sign on method	<ul> <li>Secure Web Authentication (SWA)</li> <li>Uses credentials to sign in. This integration works with most apps.</li> </ul>
	<ul> <li>SAML 2.0</li> <li>Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.</li> </ul>
	OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.

ステップ5 : 次の図に示すように、[**App name**]、[**App logo**](オ**プション)を指定**し、[**Next**]をクリッ クします。



App name	FMC-Login					
App logo (optional) 🕜	cisco.					
	cisco.png	Browse				
	Upload Logo					
	Requirements					
	<ul> <li>Must be PNG, JPG or GIF</li> <li>Less than 1MB</li> </ul>					
	For Best Results, use a PNG image with					
	<ul> <li>Minimum 420px by 120px to prevent up</li> <li>Landscape orientation</li> <li>Transparent background</li> </ul>	oscaling				
App visibility	Do not display application icon to users					
	Do not display application icon in the O	kta Mobile app				

Cancel

Next

ステップ6:[SAML Settings]を入力します。

シングルサインオンURL:https://<fmc URL>/saml/acs

対象者URI (SPエンティティID): https://<fmc URL>/saml/metadata

既定のリレー状態:/ui/login



Single sign on URL 🔞	https:// <f< th=""><th>MC URL&gt;/saml/acs</th><th></th><th></th></f<>	MC URL>/saml/acs		
	Vse th	is for Recipient URL	and Destination UR	L
	Allow t	this app to request o	ther SSO URLs	
Audience URI (SP Entity ID) 🥼	https:// <f< td=""><td>MC URL&gt;/saml/meta</td><td>data</td><td></td></f<>	MC URL>/saml/meta	data	
Default RelayState 👔	/ui/login			
	If no value	is set, a blank Relay	itate is sent	
Name ID format 💿	Unspecifi	ied	Ŧ	
Application username 🔞	Okta use	rname	•	
Update application username	on Create ar	nd update	•	
			Sho	ow Advanced Setting
ATTRIBUTE STATEMENTS (C	PTIONAL)			LEARN MOR
Name N	lame format (optional)	Value		
	Unspecified +			-
		·		

ステップ7:次の図に示すように、[Applications] > [Applications]に戻ります。



ステップ8:作成されたアプリ名をクリックします。

Add Application     Assign Applications     More •     Q  search     STATUS     ACTIVE     INACTIVE     0	Applications		
Q  şearch STATUS ACTIVE INACTIVE 0	H Add Application	Assign Applications	More 🔻
STATUS FMC-Login	Q [Search		
ACTIVE 0	STATUS	alada	FMC-Login
INACTIVE 0	ACTIVE	- Cisco.	
	INACTIVE	0	

ステップ9:「割当」にナビゲートします。[割り当て]をクリックします。

作成したアプリ名に個々のユーザーまたはグループを割り当てることができます。

General	Sign On	Import Assignments			
Assign 👻		Assignments	Q Search	People *	
FILTERS	Pe	erson	Туре		
People	<b>.</b>	Rohan Biswas robiswas@cisco.com	Individual	×	
Groups					-

### ステップ10:[サインオ**ン]に移動します**。「設定手順の表**示」をクリック**しま**す。「アイデンティ ティプロバイダ」メタデータ**をクリックすると、iDPのメタデータが表示されます。

CISCO. Active  View Logs eneral Sign On Import Assignments	
Settings	Edit
0.011.011.000	
The sign-on method determines how a user signs into and manages on methods require additional configuration in the 3rd party applicat Application username is determined by the user profile mapping. <b>Co</b>	their credentials for an application. Some sign- ion. nfigure profile mapping
The sign-on method determines how a user signs into and manages on methods require additional configuration in the 3rd party applicat Application username is determined by the user profile mapping. Co SAML 2.0 Default Relay State ui/login	their credentials for an application. Some sign- lon. nfigure profile mapping

FMCで使用する.xmlフ**ァイル**としてファイルを保存します。



# FMCの設定手順

ステップ1:管理者権限でFMCにログインします。[System] > [Users]に移動します。

Overview Analysis Policies Devices Objects AMP Intelligence Objects AMP Intelligence System
Configuration Users Domains Integration Updates Licenses Logging + Health + Mont

ステップ2:次の図に示すように、[Single Sign-On]をクリックします。

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

ステップ3:シングル**サインオ**プションを有効にする(デフォルトでは無効)。

ntication	Single Sign-On		
		Single Sign-On (SSO) Configuratio	3
		This feature is currently disabled.	

ステップ4:[**Configure SSO**]をクリック**し、**FMCのSSO設定を開始します。

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

ステップ5:[FMC SAML Provider]を選択します。[next] をクリックします。

このデモンストレーションの目的は**お田**です。

Select FMC SAML Provider	•×
Okta     OneLogin     PingID     Other	
Step 1 of 3	Next

ステップ6:[**Manual Configuration**]を選択し**、iDPデー**タを手動で入力できます。[次へ]**をクリ**ック します。



「XMLファイルのアップロー**ド」を選択**し、Okta構成のステップ10で取得したXMLファイルを<u>ア</u> <u>ップロードする</u>こともできます。

Configure t SSO manu Manu	the FMC to work with your Okta IdP by selecting one of the following two options: Fill out required field ally, or upload the XML metadata file.	is for your
	Drag and drop an XML file here, or click to upload an XML file containing your SSO credentials.	

ファイルがアップロードされると、FMCにメタデータが表示されます。次の図に示すように [Next]をクリックします。

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 N	ext

## ステップ7:メタデ**ータを**確認します。次の図に示**すように**[Save]をクリックします。

Verify Okta Metadata	۰×
Test the Okta metadata by clicking the <b>Test Configuration</b> button on the <b>System / Users / Single Sign-On</b> page you save.) Identity Provider Single Sign-On URL https://cisco-robiswas.okta.com/app/ciscoorg842643_fmclogin_1/exkjmr3gbDQjCYNin4x6/sso/saml	after
Identity Provider Issuer http://www.okta.com/exkjmr3gbDQjCYNin4x6 X.509 Certificate MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2F	sa₩Zv
Step 3 of 3 Back	Save

ステップ8:[Advanced Configuration]の下で**[Role Mapping/Default User Role]**を設定**します**。

Single Sign-On (SSO) (	Configuration 🔍
Configuration Details / Identity Provider Single Sign-O https://cisco-robiswas.ok/ Identity Provider Issuer http://www.okta.com/exk X.509 Certificate MIIDrDCCApSgAwIBAgIG	On URL ta.com/app/ciscoorg842643_ cjmr3gbDQjCYNin4x6 AXMtNBBjMA0GCSqGSIb3DQ
<ul> <li>Advanced Configuration (Ro</li> </ul>	le Mapping)
Default User Role	Administrator 🗸
Group Member Attribute	
Access Admin	
Administrator	
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	

ステップ9:設定をテストするには、次の図に示すように[**Test Configuration**]をクリックします。



テストが成功した場合は、ブラウザの新しいタブに、次の図に示すページが表示されます。



ステップ10:[Apply]をクリックし、設定を保存します。

Configuration Details	s /
Identity Provider Si	ngle Sign-On URL
https://cisco-rob	oiswas.okta.com/app/ciscoorg842643_
Identity Provider Is	suer
http://www.okta	.com/exkjmr3gbDQjCYNin4x6
X.509 Certificate	
MIIDrDCCApSgA	wIBAgIGAXMtNBBjMA0GCSqGSIb3DQ
Advanced Config	uration (Bole Manping)

SSOを正常に有効にする必要があります。



# 確認

ブラウザからFMC URL https://<fmc URL>に移動します。[シングル**サインオン]をクリックします** 

al al al a	
cisco	
Firepower	A A A A A A A A A A A A A A A A A A A
Management	
Center	1
Username	
Password	
Single Sign-On	· L

o

iDP(Okta)ログインページにリダイレクトされます。SSOクレデンシャルを入力します。[サイン イン]を**クリックします**。

Connecting	to	-11	india.	
00111001119				

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

Login

okta	
Sign In	
Jsername	
robiswas@cisco.com	
robiswas@cisco.com Password	
robiswas@cisco.com Password	
robiswas@cisco.com Password  Remember me	

成功した場合は、ログインしてFMCのデフォルトページを表示できます。

FMCで、[システム(**System)] > [ユーザ(Users)]に移動**し、データベースに追加されたSSOユーザ を確認します。

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