Configurer l'accès à Firepower Management Center via l'authentification SSO avec Okta

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Limitations et restrictions Configuration Steps Étapes de configuration sur le fournisseur d'identité (Okta) Étapes de configuration sur FMC Vérification

Introduction

Ce document décrit comment configurer Firepower Management Center (FMC) pour l'authentification à l'aide de l'authentification unique (SSO) pour l'accès à la gestion.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base de l'authentification unique et de SAML
- Présentation de la configuration sur le fournisseur d'identité (iDP)

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco Firepower Management Center (FMC) version 6.7.0
- Okta en tant que fournisseur d'identité

Remarque : les informations de ce document ont été créées à partir de périphériques dans un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toute modification de configuration.

Informations générales

L'authentification unique (SSO) est une propriété de gestion des identités et des accès (IAM) qui permet aux utilisateurs de s'authentifier en toute sécurité avec plusieurs applications et sites Web en se connectant une seule fois avec un seul ensemble d'informations d'identification (nom d'utilisateur et mot de passe). Avec SSO, l'application ou le site Web auquel l'utilisateur tente d'accéder dépend d'un tiers de confiance pour vérifier que les utilisateurs sont ceux qu'ils disent être.

SAML (Security Assertion Markup Language) est un cadre XML permettant d'échanger des données d'authentification et d'autorisation entre des domaines de sécurité. Il crée un cercle de confiance entre l'utilisateur, un fournisseur de services (SP) et un fournisseur d'identité (IdP) qui permet à l'utilisateur de se connecter à une seule heure pour plusieurs services

Un fournisseur de services (SP) est une entité qui reçoit et accepte une assertion d'authentification émise par un fournisseur d'identité (iDP). Comme l'indiquent leurs noms, les fournisseurs de services fournissent des services tandis que les fournisseurs d'identité fournissent l'identité des utilisateurs (authentification).



SSO SAML Workflow

Ces iDP sont pris en charge et testés pour l'authentification :

- Okta
- OneLogin

- PingID
- Azure AD
- Autres (tout iDP conforme à SAML 2.0)

Remarque : Aucune nouvelle licence n'est requise. Cette fonctionnalité fonctionne en mode licence et évaluation.

Limitations et restrictions

Voici les limitations et restrictions connues pour l'authentification SSO pour l'accès FMC :

- SSO ne peut être configuré que pour le domaine global
- La paire FMC en HA nécessite une configuration individuelle
- Seuls les administrateurs locaux/AD peuvent configurer SSO sur FMC (les utilisateurs de l'administrateur SSO ne pourront pas configurer/mettre à jour les paramètres SSO sur FMC).

Configuration Steps

Étapes de configuration sur le fournisseur d'identité (Okta)

Étape 1. Connectez-vous au portail Okta. Accédez à **Applications > Applications**, comme illustré dans cette image.

okta	Get Started	Dashboard	Direc or	y Applications	Security	Workflow	Reports	Settings
🕖 Dashl	board			Applications				
Status								0
Usage - Las	st 30 Days							0

Étape 2. Comme le montre cette image, cliquez sur AddApplication.

Applications	6	
HAD Application	Assign Applications	
Q Search		

Étape 3. Comme le montre cette image, cliquez sur Create NewApp.

← Back to Applications		Create New App
CATEGORIES	O kearch	
Featured	C pedicit	
API Management 6	Featured Integrations	See all

Étape 4. Sélectionnez la **plate-forme** en tant que **Web**. Choisissez la **méthode Sign On** en tant que **SAML 2.0**. Cliquez sur **Créer**, comme illustré dans cette image.

	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. 	
at n		 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. 	
ic:		OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.	
		Create Cancel	

Étape 5. Indiquez un **nom d'application**, un **logo d'application (facultatif),** puis cliquez sur **Suivant**, comme indiqué dans cette image.



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

Cancel

Next

Étape 6. Entrez les paramètres SAML.

URL de connexion unique : https://<URL fmc>/saml/acs

URI d'audience (ID d'entité SP) : https://<URL fmc>/saml/métadonnées

État de relais par défaut : /ui/login



Single sign on one	9	https:// <fmc url="">/saml/acs</fmc>						
		Use this for Recipient U	Use this for Recipient URL and Destination URL					
		Allow this app to reque	st other SSO URLs					
Audience URI (SP Ent	ity ID) 🔞	https:// <fmc url="">/saml/n</fmc>	netadata					
Default RelayState		/ui/login						
		If no value is set, a blank Re	elayState is sent					
Name ID format 🔞		Unspecified	Ŧ					
Application username	• •	Okta username	•					
Update application us	ername on	Create and update	Ŧ					
			Sho	w Advanced Setting				
ATTRIBUTE STATEM		L)		LEARN MOR				
		~						
	Name for	mat (optional) Value						
Name								

Étape 7. Revenez à **Applications > Applications**, comme illustré dans cette image.



Étape 8. Cliquez sur le nom de l'application qui a été créé.



Étape 9. Accédez à Affectations. Cliquez sur Affecter.

Vous pouvez choisir d'affecter des utilisateurs ou des groupes individuels au nom d'application créé.

General	Sign On	Import Assignments		
Assign 🔻	🖌 Convert	t Assignments	Q Search	People *
FILTERS	Pe	erson	Туре	
People	-	Rohan Biswas robiswas@cisco.com	Individual	×

Étape 10. Accédez à **Connexion**. Cliquez sur **Afficher les instructions de configuration**. **Cliquez sur les métadonnées du fournisseur d'identité** pour afficher les métadonnées de l'iDP.

Active View Logs eneral Sign On Import Assignments	
ettings	Edit
SIGN ON METHODS The sign-on method determines how a user signs into and ma on methods require additional configuration in the 3rd party a Application username is determined by the user profile mapp	inages their credentials for an application. Some sign- pplication. ing. Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into and ma on methods require additional configuration in the 3rd party a Application username is determined by the user profile mapp SAML 2.0 Default Relay State ul/login	inages their credentials for an application. Some sign- pplication. ing. Configure profile mapping

Enregistrez le fichier en tant que fichier .xml à utiliser sur le FMC.



Étapes de configuration sur FMC

Étape 1. Connectez-vous au FMC avec les privilèges Admin. Accédez à Système > Utilisateurs.

Overview Analysis Policies Devices Obj	jects AMP	Intelligence										Dep oy S	ystem
					Configuration	Users	Domains	Integration	Updates	Licenses •	Logging •	Health •	Monit

Étape 2. Cliquez sur **Connexion unique**, comme illustré dans cette image.

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

Étape 3. Activez l'option Connexion unique (Désactivée par défaut).



Étape 4. Cliquez sur **Configurer SSO** pour commencer la configuration SSO sur FMC.



Étape 5. Sélectionnez le fournisseur SAML FMC. Cliquez sur Next (Suivant).

Aux fins de cette démonstration, Okta est utilisé.

Select the SAMI provider to authenticate SSO users for	or the EMC+	
 Okta 	a die reio.	
OneLogin		
 Azure 		
O PingID		
Other		
he 1 4 2		
ep 1 of 3		Next

Étape 6. Vous pouvez choisir **Configuration manuelle** et saisir les données iDP manuellement. Cliquez sur **Suivant**, comme



Vous pouvez également choisir **Télécharger le fichier XML** et télécharger le fichier XML récupéré à l'<u>étape 10</u> de Configuration Okta.

Configure the FMC to SSO manually, or up	o work with your Okta IdP t bload the XML metadata file	by selecting one of the fo	llowing two options: Fill o	out required fields for your
Manual Configu Upload XML File	e			
Dra	ag and drop an XML file her	e, or click to upload an X	ML file containing your SS	SO credentials.

Une fois le fichier téléchargé, le FMC affiche les métadonnées. Cliquez sur **Suivant**, comme illustré dans cette image.

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 yo SSO manually, or upload the XML metadata file. Manual Configuration Upload XML File	ur
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 Ne	xt

Étape 7. Vérifiez les métadonnées. Cliquez sur Enregistrer, comme illustré dans cette image.

Verify Okta Metadata	٥×		
Test the Okta metadata by clicking the Test Configuration button on the System / Users / Single Sign-On page af 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			
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1	UECAwKQ2FsaWZv		
Step 3 of 3	Back Save		

Étape 8. Configurez le rôle Mappage de rôle/Rôle utilisateur par défaut sous Configuration avancée.

Single Sign-On (SSO) (Configuration 🔍
Configuration Details / Identity Provider Single Sign-O https://cisco-robiswas.okd Identity Provider Issuer http://www.okta.com/exk X.509 Certificate MIIDrDCCApSgAwIBAgIG	On URL ta.com/app/ciscoorg842643_ cjmr3gbDQjCYNin4x6 AXMtNBBjMA0GCSqGSIb3DQ
 Advanced Configuration (Ro 	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	

Étape 9. Afin de tester la configuration, cliquez sur **Test Configuration**, comme indiqué dans cette image.



Si le test est réussi, vous devriez voir la page affichée dans cette image, sur un nouvel onglet du navigateur.

🗱 Cisco Firepower Management I X 💿 https://tmcv.example.com/sam X +	
← → ○ ■ fmcv.example.com/sami/acs	
	Success
	You can close this tab and save your SSO configuration.

Étape 10. Cliquez sur Apply pour enregistrer la configuration.

Configuration Details	/
Identity Provider Sing	le Sign-On URL
https://cisco-robis	was.okta.com/app/ciscoorg842643_
Identity Provider Issu	er
http://www.okta.c	om/exkjmr3gbDQjCYNin4x6
X.509 Certificate	
MIIDrDCCApSgAw	IBAgIGAXMtNBBjMA0GCSqGSIb3DQ
Advanced Configura	ition (Role Mapping)

SSO doit être activé avec succès.

Single S	ign-On (SSO) Configuration 🛛 🔍
Configura	tion Details 🖌
Identity i https://	rovider Single Sign-On URL cisco-robiswas.okta.com/app/ciscoorg842643_
Identity F	Provider Issuer
http://v	ww.okta.com/exkjmr3gbDQjCYNin4x6
X.509 Ce	rtificate
MIIDrD	CCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ

Vérification

Accédez à l'URL FMC à partir de votre navigateur : https://<URL fmc>. Cliquez sur Connexion

1		line.
	cisco	/
11-14	Firepower	A STATE
112	Management	
	Center	***
1		18
	Username	
	Password	
P	Single Sign-On	
	Log In	
		K

Vous serez redirigé vers la page de connexion iDP (Okta). Fournissez vos informations d'identification SSO. Cliquez sur **Connexion**.

Si	gn-in with your cisco-org-842643 account to access FMC- Login	
	okta	
	Sign In Username	1
	robiswas@cisco.com	
	Password	
	••••••	
L	Remember me	1
	Sign In	
	Need help signing in?	

Si vous réussissez, vous devriez pouvoir vous connecter et voir la page par défaut de FMC.

Sur FMC, accédez à **System > Users** pour voir l'utilisateur SSO ajouté à la base de données.

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