Configuración del acceso a Firepower Management Center a través de la autenticación SSO con Okta

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Límites y Restricciones Configuration Steps Pasos de configuración en el proveedor de identidad (Okta) Pasos de configuración en FMC Verificación

Introducción

Este documento describe cómo configurar Firepower Management Center (FMC) para la autenticación mediante el inicio de sesión único (SSO) para el acceso a la gestión.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica del inicio de sesión único y SAML
- Comprensión de la configuración en el proveedor de identidad (iDP)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Firepower Management Center (FMC) versión 6.7.0
- Okta como proveedor de identidad

Nota: La información de este documento se creó a partir de dispositivos en un entorno de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier cambio de configuración.

Antecedentes

El inicio de sesión único (SSO) es una propiedad de gestión de identidades y acceso (IAM) que permite a los usuarios autenticarse de forma segura con varias aplicaciones y sitios web iniciando sesión una sola vez con un solo conjunto de credenciales (nombre de usuario y contraseña). Con SSO, la aplicación o el sitio web al que el usuario intenta acceder depende de un tercero de confianza para verificar que los usuarios son quienes dicen ser.

SAML (lenguaje de marcado de aserción de seguridad) es un marco basado en XML para intercambiar datos de autenticación y autorización entre dominios de seguridad. Crea un círculo de confianza entre el usuario, un proveedor de servicios (SP) y un proveedor de identidad (IdP) que permite al usuario iniciar sesión en una sola vez para varios servicios

Un proveedor de servicios (SP) es una entidad que recibe y acepta una afirmación de autenticación emitida por un proveedor de identidad (iDP). Como se describe en sus nombres, los proveedores de servicios proporcionan servicios mientras que los proveedores de identidad proporcionan la identidad de los usuarios (autenticación).



SSO SAML Workflow

Estos iDP son compatibles y se prueban para la autenticación:

- Okta
- OneLogin
- PingID
- Azure AD
- Otros (Cualquier iDP que se ajuste a SAML 2.0)

Nota: No se requiere nueva licencia. Esta función funciona tanto en modo de evaluación como de licencia.

Límites y Restricciones

Estas son limitaciones y restricciones conocidas para la autenticación SSO para el acceso FMC:

- SSO sólo se puede configurar para el dominio global
- Los FMC en el par HA requieren configuración individual
- Sólo los administradores locales/AD pueden configurar SSO en FMC (los usuarios administradores de SSO no podrán configurar/actualizar la configuración de SSO en FMC).

Configuration Steps

Pasos de configuración en el proveedor de identidad (Okta)

Paso 1. Inicie sesión en el portal de Okta. Navegue hasta **Aplicaciones > Aplicaciones**, como se muestra en esta imagen.



Paso 2. Como se muestra en esta imagen, haga clic en AddApplication.

Application:	S	
H Add Application	Assign Applications	
Q Search		

Paso 3. Como se muestra en esta imagen, haga clic en Create NewApp.

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

Paso 4. Elija la **Plataforma** como **Web**. Elija el **método Sign On** como **SAML 2.0**. Haga clic en **Crear**, como se muestra en esta imagen.

Platform	Web
Sign on method	 Secure Web Authentication (SWA) Uses credentials to sign in. This integration works with most apps.
	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.
	OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.

Paso 5. Proporcione un **nombre de aplicación**, **logotipo de aplicación (opcional),** y haga clic en **Siguiente**, como se muestra en esta imagen.



App name	FMC-Login	
App logo (optional) 🕜	cisco.	
	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 upscalin Landscape orientation Transparent background 	g
App visibility	Do not display application icon to users	
	Do not display application icon in the Okta Mo	bile app

Cancel

Next

Paso 6. Introduzca la configuración de SAML.

URL de inicio de sesión único: https://<fmc URL>/saml/acs

URI de público (ID de entidad SP): https://<fmc URL>/saml/metadatos

Estado de retransmisión predeterminado: /ui/login



Single sign on URL 👔	https:// <fmc url="">/saml/acs</fmc>	
	Use this for Recipient URL and	Destination URL
	Allow this app to request other	SSO URLs
Audience URI (SP Entity ID) 🔞	https:// <fmc url="">/saml/metadata</fmc>	1
Default RelayState 👔	/ui/login	
	If no value is set, a blank RelayState	e is sent
Name ID format 🔞	Unspecified	¥
Application username 🔞	Okta username	•
Update application username or	Create and update	Ŧ
		Show Advanced Setting
ATTRIBUTE STATEMENTS (OP	IONAL)	LEARN MOR
Name Nar	ne format (optional) Value	
l	Inspecified v	v

Paso 7. Vuelva a **Aplicaciones > Aplicaciones**, como se muestra en esta imagen.



Paso 8. Haga clic en el nombre de la aplicación que se creó.



Paso 9. Navegue hasta Asignaciones. Haga clic en Asignar.

Puede optar por asignar usuarios o grupos individuales al nombre de la aplicación creado.

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

Paso 10. Navegue hasta **Iniciar sesión**. Haga clic en **Ver instrucciones de configuración**. **Haga clic en los metadatos del proveedor de identidad** para ver los metadatos del iDP.

eneral Sign On Import Assignments	
Settings	Edit
SIGN ON METHODS	
SIGN ON METHODS The sign-on method determines how a user signs into and m on methods require additional configuration in the 3rd party a	nages their credentials for an application. Some sign- pplication.
SIGN ON METHODS The sign-on method determines how a user signs into and m on methods require additional configuration in the 3rd party a Application username is determined by the user profile mapp	nages their credentials for an application. Some sign- pplication. ng. Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into and m on methods require additional configuration in the 3rd party a Application username is determined by the user profile mapp	nages their credentials for an application. Some sign- pplication. ng. Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into and m 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 ui/login	nages their credentials for an application. Some sign- pplication. ng. Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into and m 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 ui/login	nages their credentials for an application. Some sign- pplication. ng. Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into and m 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 ui/login SAML 2.0 is not configured until you complete the	nages their credentials for an application. Some sign- pplication. ng. Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into and m 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 ui/login SAML 2.0 is not configured until you complete th View Setup Instructions	nages their credentials for an application. Some sign- pplication. ng. Configure profile mapping

Guarde el archivo como un archivo .xml que se utilizará en el FMC.



Pasos de configuración en FMC

Paso 1. Inicie sesión en el FMC con privilegios Admin. Navegue hasta Sistema >Usuarios.

Overview Analysi	s Policies	Devices	Objects	AMP	Intelligence	e								_							Dec oy	System
												Configuration	Users	Dor	mains	Integration	Updates	Licenses	• 1	Logging •	Health •	Mon

Paso 2. Haga clic en Inicio de sesión único, como se muestra en esta imagen.

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

Paso 3. Active la opción Inicio de sesión único (Desactivado de forma predeterminada).

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

Paso 4. Haga clic en Configurar SSO para iniciar la configuración SSO en FMC.



Paso 5. Seleccione el proveedor SAML de FMC. Haga clic en Next (Siguiente).

Para el propósito de esta demostración, se utiliza Okta.

Salart the SAMI provider to authenticate SSO users for the EMC:	
Okta	
OneLogin	
O Azure	
O Other	
tep 1 of 3	Next

Paso 6. Puede elegir **Configuración manual** e introducir los datos iDP manualmente. Haga clic en **Siguiente**, como



También puede elegir **Cargar archivo XML** y cargar el archivo XML recuperado en el <u>Paso 10</u> de Configuración de Okta.

SSO manu	the FMC to work with your Okta ally, or upload the XML metada al Configuration	a IdP by selecting one of the ta file.	following two options: Fill out	required fields for your
Uploa	id XML File			_
	Drag and drop an XML fi	le here, or click to upload an	XML file containing your SSO	credentials.

Una vez que se carga el archivo, el FMC muestra los metadatos. Haga clic en **Next**, como se muestra en esta imagen.

Configure Okta Metadata O
Configure the FMC to work with your Okta IdP by selecting one of the following two options: Fill out required fields for you SSO manually, or upload the XML metadata file. Manual Configuration Upload XML File
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 MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1U!
Step 2 of 3 Back Next

Paso 7. Verifique los metadatos. Haga clic en Guardar, como se muestra en esta imagen.

Verify Okta Metadata	۰×
Test the Okta metadata by clicking the Test Configuration button on the System / Users / Single Sign- you save.) Identity Provider Single Sign-On URL https://cisco-robiswas.okta.com/app/ciscoorg842643_fmclogin_1/exkjmr3gbDQjCYNin4x6/sso/saml	Dn page after
Identity Provider Issuer http://www.okta.com/exkjmr3gbDQjCYNin4x6 X.509 Certificate MUDrDCCApSqAwJBAqIGAXMtNBBiMA0GCSqGSIb3DQEBCwJAMIGWMQcwCQYDVQQGEwJVJzETMBEGA1UEC	AwKO2EcaW7v
Step 3 of 3	* Save

Paso 8. Configure la Asignación de Función/Función de Usuario Predeterminada en Configuración Avanzada.

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	

Paso 9. Para probar la configuración, haga clic en **Test Configuration**, como se muestra en esta imagen.



Si la prueba se realiza correctamente, debería ver la página mostrada en esta imagen, en una nueva pestaña del navegador.

# Clisco Firepower Management X 🕑 https://fmov.example.com/sam X +	
← → C ■ fmcv.example.com/sami/acs	
	Success
	Success You can close this tab and save your SSO configuration.

Paso 10. Haga clic en Aplicar para guardar la configuración.

Configuration Details	/
Identity Provider Sir	ngle Sign-On URL
https://cisco-rob	iswas.okta.com/app/ciscoorg842643_
Identity Provider Iss	Juer
http://www.okta	.com/exkjmr3gbDQjCYNin4x6
X.509 Certificate	
MIIDrDCCApSgA	wIBAgIGAXMtNBBjMA0GCSqGSIb3DQ
Advanced Configu	ration (Role Mapping)

SSO debe estar habilitado correctamente.

ingle	Sign-On (SSO) Configuration 🛛 🗨 🗨
Configur	ation Details 🖌
Identity https:/	Provider Single Sign-On URL /cisco-robiswas.okta.com/app/ciscoorg842643_
Identity	Provider Issuer
http://	www.okta.com/exkjmr3gbDQjCYNin4x6
X.509 C	ertificate
MIIDrD	CCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ

Verificación

Navegue hasta la URL de FMC desde su navegador: https://<fmc URL>. Haga clic en Inicio de

S.		
	cisco	1
W. in	Firepower	
R	Management	
	Center	
		100
	Username	
	Password	
P	Single Sign-On	
	Log In	5
		1

Se le redirigirá a la página de inicio de sesión de iDP (Okta). Proporcione sus credenciales de SSO. Haga clic en **Iniciar sesión**.

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

Si se realiza correctamente, debería poder iniciar sesión y ver la página predeterminada de FMC.

En FMC, navegue hasta **System > Users** para ver el usuario SSO agregado a la base de datos.

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