使用Okta通过SSO身份验证配置Firepower管理中 心访问

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> <u>限制和限制</u> <u>配置步骤</u> <u>身份提供程序(OKTA)上的配置步骤</u> <u>FMC上的配置步骤</u> <u>验证</u>

简介

本文档介绍如何配置Firepower管理中心(FMC)以使用单点登录(SSO)进行身份验证以进行管理访问。

先决条件

要求

Cisco 建议您了解以下主题:

- 对单点登录和SAML的基本了解
- •了解身份提供程序(iDP)上的配置

使用的组件

本文档中的信息基于以下软件版本:

- •思科Firepower管理中心(FMC)版本6.7.0
- 确定身份提供者

注意:本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采 用原始(默认)配置。如果您的网络处于活动状态,请确保您了解任何配置更改的潜在影响。

背景信息

单点登录(SSO)是身份和访问管理(IAM)的一个属性,通过仅使用一组凭证(用户名和密码)登录一次,用户就可以安全地使用多个应用和网站进行身份验证。 使用SSO时,用户尝试访问的应用或网

站依靠受信任的第三方来验证用户是否是他们所说的用户。

SAML(安全断言标记语言)是一个基于XML的框架,用于在安全域之间交换身份验证和授权数据 。它在用户、服务提供商(SP)和身份提供商(IdP)之间创建信任圈,允许用户一次登录多个服务

服务提供商(SP)是接收并接受由身份提供商(iDP)发出的身份验证断言的实体。 如其名称所述,服务 提供商提供服务,而身份提供商提供用户身份(身份验证)。





这些iDP受支持,并经过身份验证测试:

- 奥克塔
- OneLogin
- PingID
- Azure AD
- 其他(任何符合SAML 2.0的iDP)

注意:无新许可证要求。此功能在许可和评估模式下工作。

以下是FMC访问的SSO身份验证的已知限制和限制:

- •SSO只能配置为全局域
- HA对中的FMC需要单独配置
- •只有本地/AD管理员可以在FMC上配置SSO(SSO管理员用户将无法在FMC上配置/更新SSO设置)。

配置步骤

身份提供程序(OKTA)上的配置步骤

步骤1.登录Okta门户。导航至**应用程序>**应用程序,如下图所示。

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

步骤2.如此图所示,单击AddApplication(添加应用)。

Application:	S	
H Add Application	Assign Applications	
Q. Search		

步骤3.如此图所示,单击"创建**新应用"**。

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

步骤4.将平台**选**为Web。选择Sign On方法作为SAML 2.0。单击Create,如此图所示。

l	Create a New Application Integratio	n	×	
'n	Platform	Web		
	Sign on method	 Secure Web Authentication (SWA) Uses credentials to sign in. This integration works with most apps. 		. 40
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. 		or
ici		OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.		r
		Create Cancel		

步骤5.提供应**用名称**、应**用徽标(可选),然**后单击**下**一步,如下图所示。



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 upscaling Landscape orientation Transparent background
	Do not display application icon to users
App visibility	

Cancel

Next

步骤6.输入SAML Settings。

单点登录URL:https://<fmc URL>/saml/acs

受众URI(SP实体ID): https://<fmc URL>/saml/metadata

默认中继状态:/ui/login



single sign on one)	https:// <fmc url="">/saml/</fmc>	acs	
		Use this for Recipient	URL and Destination URL	
		Allow this app to requ	est other SSO URLs	
Audience URI (SP Entit	ty ID) 🔞	https:// <fmc url="">/saml/</fmc>	metadata	
Default RelayState 👩		/ui/login		
		If no value is set, a blank R	elayState is sent	
Name ID format 🔞		Unspecified	Ŧ	
Application username	0	Okta username	•	
Jpdate application use	ername on	Create and update	Ŧ	
			Show Ac	Ivanced Setting
ATTRIBUTE STATEME		Ð		LEARN MOR
Jamo	Name for	met (antional) Malue		Lo un mon
vanie	Name for	mat (optional) Value		
	Unspe	cified v		Ŧ

步骤7.导航回Applications>Applications,如下图所示。



步骤8.单击创建的应用名称。

4dd Application	Salary Assign Applications	More 🔻	
Q \$earch			
STATUS	abab	FMC-Login	
ACTIVE	cisco		
INACTIVE	0		•

步骤9.定位至"**分配**"。单击"Assign"。

您可以选择将单个用户或组分配给创建的应用名称。

General	Sign On	Import Assignments		
Assign 👻		Assignments	Q Search	People *
FILTERS	Pe	rson	Туре	
People	1	Rohan Biswas robiswas@cisco.com	Individual	/ ×
Groups				

步骤10.导航至**登录**。单击"查**看设置说明"**。单**击"身份提供程序"元**数据以查看iDP的元数据。

eneral Sign On Import Assignments	gs
Settings	Edit
The sign-on method determines how a user signs into an on methods require additional configuration in the 3rd pa	nd manages their credentials for an application. Some sign- arty application.
The sign-on method determines how a user signs into an on methods require additional configuration in the 3rd pa Application username is determined by the user profile m SAML 2.0	nd manages their credentials for an application. Some signarty application. An appling. Configure profile mapping
The sign-on method determines how a user signs into an on methods require additional configuration in the 3rd pa Application username is determined by the user profile n SAML 2.0 Default Relay State ul/login	nd manages their credentials for an application. Some sign- arty application. napping. Configure profile mapping
The sign-on method determines how a user signs into an on methods require additional configuration in the 3rd pa Application username is determined by the user profile n Image: SAML 2.0 Image: Default Relay State Image: SAML 2.0 Image: SAML 2.0	ad manages their credentials for an application. Some signarity application. happing. Configure profile mapping

将文件另存为要在FMC上使用的.xml文件。



FMC上的配置步骤

步骤1.使用管理员权限登录FMC。导航至系统>用户。

Overview Analysis Policies Devices Objects AMP Intelligence						0	Dep oy	System
Configuratio	Users	Domains	Integration	Updates	Licenses •	Logging •	Health	• Mon

步骤2.单击Single Sign-On(单点登录),如下图所示。

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

步骤3.**启**用Single Sign-On选项(默认为禁用)。



步骤4.单击"配置SSO"以开始FMC上的SSO配置。



步骤5.选择FMC SAML提供程序。单击 Next。

本演示使用Okta。

Select the SAML provider to authentic Okta	ate SSO users for the FMC:	
OneLogin		
Azure		
O PingID		
Other		
ten 1 of 3		Novt

步骤6.您可以选择手**动配置**并手动输入iDP数据。单击Next,如



您还可以选择上载XML文件并上载在Okta配置步骤10<u>中检索</u>的XML文件。

gare		
Configure the SSO manual Manual	FMC to work with your Okta IdP by selecting one of the following two options: Fill out required fy, or upload the XML metadata file. Configuration XML File	fields for your
	Drag and drop an XML file here, or click to upload an XML file containing your SSO credentia	ls.
tep 2 of 3	Bac	k Next

上传文件后,FMC将显示元数据。单击Next,如下图所示。

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 your 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 MIIDrDCCApSgAwIBAgIGAXMtNBBiMA0GCSgGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1UI
Step 2 of 3 Back Next

步骤7.**检验**元数据。单击**Save**,如此图所示。

Verify Okta Metadata	۰×
Test the Okta metadata by clicking the Test Configuration button on the System / Users / Single Sign-On page a you save.) Identity Provider Single Sign-On URL https://cisco-robiswas.okta.com/app/ciscoorg842643_fmclogin_1/exkjmr3gbDQjCYNin4x6/sso/saml	fter
Identity Provider Issuer http://www.okta.com/exkjmr3gbDQjCYNin4x6 X.509 Certificate MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2Fs	a₩Zv
Step 3 of 3 Back	šave

步骤8.在Advanced Configuration下**配置Role Mapping/Default User Role**。

Single Sign-On (SSO) C	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 (Rol	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					
Threat Intelligence Director (TID) User					

步骤9.要测试配置,请单击**测试配置**,如本图所示。



如果测试成功,您应在浏览器的新选项卡上看到此图像中显示的页面。



步骤10.单击"应用"保存配置。

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

SSO应该已成功启用。

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

验证

从浏览器导航至FMC URL:https://<fmc URL>。单击Single Sign-On。

j.	luilu isco
Fire	ower
Mana	gement 🛛
Ce	enter
Username	
Password	
Sing	le Sign-On
	Log In

您将被重定向到iDP(Okta)登录页。提供您的SSO凭证。单击"**Sign in(登录)**"。

Connecting to	
---------------	--

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

Login

okta	
Cian In	
Sign In Jsername	
Sign In Jsername robiswas@cisco.com	
Sign In Jsername robiswas@cisco.com Password	
Sign In Jsername robiswas@cisco.com Password ••••••	
Sign In Jsername robiswas@cisco.com Password •••••••	

如果成功,您应该能够登录并查看FMC默认页面。

在FMC上,导航至**System > Users**,查看已添加到数据库的SSO用户。

Users User Roles E	sternal Authentication	Single Sign-On						
							0	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