通過Okta的SSO身份驗證配置Firepower管理中心 訪問

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>限制和限制</u> <u>配置步驟</u> <u>身份提供程式(Okta)上的配置步驟</u> <u>FMC的配置步驟</u> <u>驗證</u>

簡介

本文檔介紹如何配置Firepower管理中心(FMC)以使用單一登入(SSO)進行身份驗證,以便進行管理 訪問。

必要條件

需求

思科建議您瞭解以下主題:

- 對單點登入和SAML的基本瞭解
- •瞭解身份提供程式(iDP)上的配置

採用元件

本檔案中的資訊是根據以下軟體版本:

- •思科Firepower管理中心(FMC)版本6.7.0
- Okta作為身份提供程式

注意:本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清 除(預設)的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何組態變更的潛在影響 。

背景資訊

單點登入(SSO)是身份和訪問管理(IAM)的一項屬性,使使用者只需使用一組憑證(使用者名稱和密

碼)登入一次,即可通過多個應用程式和網站進行安全身份驗證。 使用SSO時,使用者嘗試訪問的 應用程式或網站依賴於可信的第三方來驗證使用者是否擁有其聲稱的身份。

SAML(Security Assertion Markup Language)是一個基於XML的框架,用於在安全域之間交換驗證 和授權資料。它在使用者、服務提供商(SP)和身份提供者(IdP)之間建立一個信任圈,允許使用者一 次性登入多個服務

服務提供程式(SP)是接收並接受身份提供程式(iDP)發出的身份驗證斷言的實體。 正如其名稱所描述 的,服務提供商提供服務,而身份提供商提供使用者的身份(身份驗證)。





這些iDP受支援並進行身份驗證測試:

- 奧克塔
- OneLogin
- PingID
- Azure AD
- 其他(符合SAML 2.0的任何iDP)

注意:無新許可證要求。此功能在許可模式和評估模式下均可用。

限制和限制

以下是用於FMC訪問的SSO身份驗證的已知限制和限制:

- •只能為全域性域配置SSO
- HA配對中的FMC需要單獨配置
- •只有本地/AD管理員才能在FMC上配置SSO(SSO管理員使用者將無法在FMC上配置/更新 SSO設定)。

配置步驟

身份提供程式(Okta)上的配置步驟

步驟1.登入Okta門戶。導覽至Applications > Applications,如下圖所示。

okta	Get Started	Dashboard	Direc o	тy	Applications	Security	Workflow	Reports	Settings
💋 Dash	board				Applications				
Status									٥
Usage - La	st 30 Days								٢

步驟2.如本圖所示,按一下AddApplication。

Applications	S	
HAD Application	Assign Applications	
Q Search		

步驟3.如本圖所示,按一下Create NewApp。

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

步驟4.選擇Platform作為Web。選擇Sign On method 作為 SAML 2.0。按一下Create,如下圖所示

o

	Create a New Application Integratio	A no	<
	Platform	Web	
	Sign on method	 Secure Web Authentication (SWA) Uses credentials to sign in. This integration works with most apps. 	
t		 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. 	
1		OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.	
		Create Cancel	

步驟5.提供App 名稱、App**徽標(可選),**然後按一下Next,如下圖所示。



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 up: 	scaling
	 Landscape orientation Transparent background 	
App visibility	Do not display application icon to users	
	Do not display application icon in the Ok	ta Mobile app

Cancel

Next

步驟6.輸入SAML設定。

單點登入URL:https://<fmc URL>/saml/acs

受眾URI(SP實體ID): https://<fmc URL>/saml/metadata

預設中繼狀態:/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>	https:// <fmc url="">/saml/metadata</fmc>				
Default RelayState 👔	/ui/login					
	If no value is set, a blank RelayState is se	nt				
Name ID format 🔞	Unspecified	¥				
Application username 👔	Okta username	v				
Update application username or	Create and update	•				
		Show Advanced Setting				
ATTRIBUTE STATEMENTS (OP)	IONAL)	I FARN MOR				
		LEARNMON				
Name Nar	e format (optional) Value					
L	nspecified v	•				

步驟7.導覽至Applications > Applications,如下圖所示。



步驟8.按一下建立的應用程式名稱。

Add Application Add Application More • Q bearch STATUS ACTIVE INACTIVE 0	Application:	S		
Q Search STATUS ACTIVE 1 INACTIVE 0	👯 Add Application	時 Assigr	Applications	More *
STATUS FMC-Login	Q [\$earch	_		
ACTIVE 1 INACTIVE 0	STATUS		alada	FMC-Login
INACTIVE 0	ACTIVE		cisco.	
	INACTIVE	0		

步驟9.定位至分配。按一下Assign。

您可以選擇將單個使用者或組分配給建立的應用程式名稱。

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

步驟10.導覽至**Sign On**。按一下**檢視安裝說明。按一下Identity Provider metadata**檢視iDP的後設資 料。

CISCO FIVIC-LOGIN	gs
eneral Sign On Import Assignments	
Settings	Edit
SIGN ON METHODS The sign-on method determines how a user signs into a on methods require additional configuration in the 3rd p	nd manages their credentials for an application. Some sign- arty application.
SIGN ON METHODS The sign-on method determines how a user signs into a on methods require additional configuration in the 3rd p Application username is determined by the user profile to SAML 2.0	nd manages their credentials for an application. Some sign- arty application. mapping. Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into a on methods require additional configuration in the 3rd p Application username is determined by the user profile r SAML 2.0 Default Relay State ul/login	nd manages their credentials for an application. Some sign- arty application. mapping. Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into a on methods require additional configuration in the 3rd p Application username is determined by the user profile i SAML 2.0 Default Relay State ui/login SAML 2.0 is not configured until you comple View Setup Instructions	nd manages their credentials for an application. Some sign- arty application. mapping. Configure profile mapping ete the setup instructions.

將檔案另存為.xml檔案,以便在FMC上使用。



FMC的配置步驟

步驟1.使用管理員許可權登錄FMC。導航至系統>使用者。

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

步驟2.按一下Single Sign-On,如下圖所示。

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

步驟3. **啟用**單一登入選項(預設為停用)。



步驟4.按一下配置SSO開始在FMC上配置SSO。

Single Sign-On (SSO) Configuration					
The FMC supports Security Assertion Marka 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				

步驟5.選擇FMC SAML提供程式。按「Next」(下一步)。

在本演示中,使用Okta。

for the DIC.
for the PMC:

步驟6.您可以選擇**手動配置**,然後手動輸入iDP資料。按一下**Next**,作為



您還可以選擇**上傳XML檔案**,並上傳在<u>Okta配置</u>的步驟10中檢索的XML檔案。

Configure the	e FMC to work wil	h your Okta IdP I (ML metadata file	by selecting one	of the following tw	o options: Fill out	required fields fo	or your
Manual	Configuration	CPIL metadata me					
Opload	XML File						
	Drag and dro	p an XML file her	e, or click to upl	oad an XML file cor	ntaining your SSO	credentials.	
top 2 of 3						Back	Next

一旦上傳檔案,FMC將顯示後設資料。按一下「Next」,如下圖所示。

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 MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1UI
Step 2 of 3 Back Next

步驟7.**驗**證後設資料。按一下「**Save**」,如下圖所示。

Verify Okta Metadata	۰×
Test the Okta metadata by clicking the Test Configuration button on the System / Users / Single you save.) Identity Provider Single Sign-On URL https://cisco-robiswas.okta.com/app/ciscoorg842643_fmclogin_1/exkjmr3gbDQjCYNin4x6/sso/saml Identity Provider Issuer	Sign-On page after
http://www.okta.com/exkjmr3gbDQjCYNin4x6	
X.509 Certificate MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG	A1UECAwKQ2FsaWZv
Step 3 of 3	Back Save

步驟8.在**高級配置**下配置角色對映/預設使用者角色。

	Configuration 🔍
Configuration Details 🖌	
Identity Provider Single Sign-C https://cisco-robiswas.ok	On URL ta.com/app/ciscoorg842643_
Identity Provider Issuer http://www.okta.com/exk	kjmr3gbDQjCYNin4x6
X.509 Certificate MIIDrDCCApSgAwIBAgIG	AXMtNBBjMA0GCSqGSIb3DQ
 Advanced Configuration (Ro 	le Mapping)
Default User Role	Administrator
Group Member Attribute	
Access Admin	
Administrator	
Discovery Admin	
Discovery Admin External Database User	
Discovery Admin External Database User Intrusion Admin	
Discovery Admin External Database User Intrusion Admin Maintenance User	
Discovery Admin External Database User Intrusion Admin Maintenance User Network Admin	
Discovery Admin External Database User Intrusion Admin Maintenance User Network Admin Security Analyst	
Discovery Admin External Database User Intrusion Admin Maintenance User Network Admin Security Analyst Security Analyst (Read Only)	
Discovery Admin External Database User Intrusion Admin Maintenance User Network Admin Security Analyst Security Analyst (Read Only)	

步驟9.若要測試組態,請按一下**Test Configuration**,如下圖所示。



如果測試成功,您應該會看到此圖中所示的頁面,位於瀏覽器上的新頁籤上。



步驟10.按一下Apply 以儲存組態。

Configuration Details	/
Identity Provider Sin	gle Sign-On URL
https://cisco-rob	swas.okta.com/app/ciscoorg842643_
Identity Provider Iss	uer
http://www.okta	.com/exkjmr3gbDQjCYNin4x6
X.509 Certificate	
MIIDrDCCApSgAv	vIBAgIGAXMtNBBjMA0GCSqGSIb3DQ
Advanced Configu	ration (Role Mapping)

應成功啟用SSO。

Configuration Details 🖌 Identity Provider Single Sign-On URL	
Identity Provider Single Sign-On URL	
https://cisco-robiswas.okta.com/app/ciscoorg84264	3_
Identity Provider Issuer	
http://www.okta.com/exkjmr3gbDQjCYNin4x6	
X.509 Certificate	
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3D	Q

驗證

1		
	cisco	
14	Firepower	A Real
1	Management	
	Center	
		a sur
	Username	
2	Password	
P	Single Sign-On	
	Log In	1
1		

系統會將您重新導向至iDP(Okta)登入頁面。提供您的SSO憑據。按一下**登入**。

Connecting	to	cisco.
------------	----	--------

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

Login

	okta	
	Ciam In	
Username	Sign In	
Username robiswas@	Sign In cisco.com	
Username robiswas@ Password	Sign In	
Username robiswas@ Password ••••••	Sign In cisco.com	
Username robiswas@ Password ••••••	sign In cisco.com	

如果成功,您應該能夠登入並檢視FMC預設頁面。

在FMC上,導航到System > Users,檢視新增到資料庫的SSO使用者。

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