# Configurazione dell'accesso a Firepower Management Center tramite autenticazione SSO con Okta

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Limitazioni e restrizioni Procedura di configurazione Procedura di configurazione nel provider di identità (Okta) Procedura di configurazione in FMC Verifica

### Introduzione

In questo documento viene descritto come configurare Firepower Management Center (FMC) per l'autenticazione tramite Single Sign-On (SSO) per l'accesso di gestione.

### Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Single Sign-On e SAML
- Informazioni sulla configurazione del provider di identità (iDP)

### Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Cisco Firepower Management Center (FMC) versione 6.7.0
- Okta come provider di identità

**Nota:** le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali modifiche alla configurazione.

# Premesse

Single Sign-On (SSO) è una proprietà di gestione delle identità e degli accessi (IAM) che consente agli utenti di autenticarsi in modo sicuro con più applicazioni e siti Web eseguendo l'accesso una sola volta con un solo insieme di credenziali (nome utente e password). Con SSO, l'applicazione o il sito Web a cui l'utente sta tentando di accedere si basa su una terza parte attendibile per verificare che gli utenti siano chi dicono di essere.

SAML (Security Assertion Markup Language) è un framework basato su XML per lo scambio di dati di autenticazione e autorizzazione tra domini di sicurezza. Crea un cerchio di fiducia tra l'utente, un provider di servizi (SP) e un provider di identità (IdP) che consente all'utente di accedere una sola volta a più servizi

Un provider di servizi (SP) è un'entità che riceve e accetta un'asserzione di autenticazione emessa da un provider di identità (iDP). Come descritto dai rispettivi nomi, i provider di servizi forniscono i servizi mentre i provider di identità forniscono l'identità degli utenti (autenticazione).



#### SSO SAML Workflow

Questi iDP sono supportati e testati per l'autenticazione:

- OneLogin
- IDping
- Azure AD
- Altri (qualsiasi iDP conforme a SAML 2.0)

**Nota:** nessuna nuova licenza richiesta. Questa funzione funziona sia in modalità di valutazione che in modalità con licenza.

#### Limitazioni e restrizioni

Si tratta di limitazioni e restrizioni note per l'autenticazione SSO per l'accesso FMC:

- SSO può essere configurato solo per il dominio globale
- I FMC in coppia HA richiedono una configurazione individuale
- Solo gli amministratori locali/AD possono configurare SSO su FMC (gli utenti amministratori SSO non potranno configurare/aggiornare le impostazioni SSO su FMC).

### Procedura di configurazione

#### Procedura di configurazione nel provider di identità (Okta)

Passaggio 1. Accedere al portale Okta. Passare a **Applicazioni > Applicazioni**, come mostrato in questa immagine.

okta	Get Started	Dashboard	Direct	ory	Applications	Security	Workflow	Reports	Settings
🕖 Dash	board				Applications				
Status									0
Usage - La	st 30 Days								0

Passaggio 2. Come mostrato nell'immagine, fare clic su AddApplication.

Applications	5	
Add Application	Assign Applications	
Q Search		

Passaggio 3. Come mostrato in questa immagine, fare clic su Create NewApp (Crea nuova app).

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

Passaggio 4. Scegliere **Piattaforma** come **Web**. Scegliere il **metodo Sign On** come **SAML 2.0**. Fare clic su **Create** (Crea), come mostrato nell'immagine.

	Create a New Application Integration	n	×
n	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>	
F at		<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>	
CI		OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.	
		Create Cancel	

Passaggio 5. Fornire un **nome di app**, **il logo dell'app (facoltativo)** e fare clic su **Avanti**, come mostrato nell'immagine.



App name	FMC-Login	
App logo (optional) 🔞		
	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 upso</li> <li>Landscape orientation</li> <li>Transparent background</li> </ul>	aling
App visibility	Do not display application icon to users	
	Do not display application icon in the Okta	Mobile app

Cancel

Next

Passaggio 6. Inserire le impostazioni SAML.

URL Single Sign-On: https://<URL fmc>/saml/acs

URI gruppo di destinatari (ID entità SP): https://<URL fmc>/saml/metadata

RelayState predefinito: /ui/login



Single sign on URL 👔	https:// <fmc url="">/saml/acs</fmc>	
	Use this for Recipient URL and Dest	ination URL
	Allow this app to request other SSO	URLs
Audience URI (SP Entity ID) 💿	https:// <fmc url="">/saml/metadata</fmc>	
Default RelayState 🔞	/ui/login	
	If no value is set, a blank RelayState is se	ent
Name ID format 🔞	Unspecified	Y
Application username 🔞	Okta username	v
Update application username on	Create and update	¥
		Show Advanced Setting
ATTRIBUTE STATEMENTS (OPT	ONAL)	LEARN MOR
Name Nam	e format (optional) Value	
U	specified v	v

Passaggio 7. Tornare a **Applicazioni > Applicazioni**, come mostrato in questa immagine.



Passaggio 8. Fare clic sul nome dell'app creata.

Applications	5		
# Add Application	時 Assign	Applications	More 🔻
Q  \$earch	_		
STATUS		alada cisco	FMC-Login
ACTIVE			
INACTIVE	0		

Passaggio 9. Passare ad Assegnazioni. Fare clic su Assegna.

Èpossibile scegliere di assegnare singoli utenti o gruppi al nome dell'app creata.

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

Passaggio 10. Passare a Sign On. Fare clic su Visualizza istruzioni di installazione. Fare clic sui metadati del provider di identità per visualizzare i metadati dell'iDP.

FMC-Login	
eneral Sign On Import Assignments	
Settings	Edit
SIGN ON METHODS	
SIGN ON METHODS The sign-on method determines how a user signs into and man on methods require additional configuration in the 3rd party app	ges their credentials for an application. Some sign- ication.
SIGN ON METHODS The sign-on method determines how a user signs into and man on methods require additional configuration in the 3rd party app Application username is determined by the user profile mapping	ges their credentials for an application. Some sign- ication. . Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into and man on methods require additional configuration in the 3rd party app Application username is determined by the user profile mapping SAML 2.0	ges their credentials for an application. Some sign- ication. . <b>Configure profile mapping</b>
SIGN ON METHODS The sign-on method determines how a user signs into and man on methods require additional configuration in the 3rd party app Application username is determined by the user profile mapping SAML 2.0 Default Relay State ui/login	ges their credentials for an application. Some sign- ication. . <b>Configure profile mapping</b>
SIGN ON METHODS The sign-on method determines how a user signs into and man on methods require additional configuration in the 3rd party app Application username is determined by the user profile mapping SAML 2.0 Default Relay State ui/login	ges their credentials for an application. Some sign- ication. . <b>Configure profile mapping</b>
SIGN ON METHODS The sign-on method determines how a user signs into and man on methods require additional configuration in the 3rd party app Application username is determined by the user profile mapping SAML 2.0 Default Relay State ui/login SAML 2.0 is not configured until you complete the	ges their credentials for an application. Some signication. Configure profile mapping
SIGN ON METHODS The sign-on method determines how a user signs into and man on methods require additional configuration in the 3rd party app Application username is determined by the user profile mapping SAML 2.0 Default Relay State ui/login SAML 2.0 is not configured until you complete the View Setup Instructions	ges their credentials for an application. Some signication. Configure profile mapping

Salvare il file come file xml da utilizzare nel CCP.



### Procedura di configurazione in FMC

Passaggio 1. Accedere al CCP con privilegi di amministratore. Passare a Sistema > Utenti.

Overview	Analysis Policies	Devices	Objects	AMP	Intelli	lligence														Dep oy	System
											Configura	tion	Users	Domains	Integration	Update	as -	Licenses •	Logging •	Health •	Monit

Passaggio 2. Fare clic su Single Sign-On, come illustrato nell'immagine.

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

Passaggio 3. Abilitare l'opzione Single Sign-On (disabilitata per impostazione predefinita).

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

Passaggio 4. Fare clic su Configura SSO per avviare la configurazione dell'SSO in FMC.



Passaggio 5. Selezionare il provider SAML FMC. Fare clic su Next (Avanti).

Ai fini della presente dimostrazione, viene utilizzato Okta.

alact the CAMI provider to a	with anticate CEO upper for the DMC.	
<ul> <li>Okta</li> </ul>	sumenucate 550 users for the PMC:	
OneLogin		
<ul> <li>Azure</li> </ul>		
O PingID		
Other		
n 1 of 3		Net
p 1 of 3		Next

Passaggio 6. È possibile scegliere **Configurazione manuale** e immettere i dati iDP manualmente. Fare clic su **Avanti**, come



Èinoltre possibile scegliere **Carica file XML** e caricare il file XML recuperato nel <u>passo 10</u> della configurazione Okta.

Configure to SSO manua Manua	he FMC to work with your Okta IdP by selecting one of the following two options: Fill out required fields for y illy, or upload the XML metadata file. I Configuration I XML File	our
	Drag and drop an XML file here, or click to upload an XML file containing your SSO credentials.	

Una volta caricato il file, il FMC visualizza i metadati. Fare clic su **Avanti**, come mostrato nell'immagine.

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/exkimr3gbDQiCYNin4x6/sso/saml
Identity Provider Issuer http://www.okta.com/exkjmr3gbDQjCYNin4x6
X.509 Certificate MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1UI
Step 2 of 3 Back Next

Passaggio 7. Verificare i metadati. Fare clic su Save (Salva), come mostrato nell'immagine.

Verify Okta Metadata		• ×
Test the Okta metadata by clicking the <b>Test Configuration</b> button on the <b>System / Users / Single</b> you save.) Identity Provider Single Sign-On URL	e Sign-On p	age after
https://cisco-robiswas.okta.com/app/ciscoorg842643_fmclogin_1/exkjmr3gbDQjCYNin4x6/sso/saml		
Identity Provider Issuer		
http://www.okta.com/exkjmr3gbDQjCYNin4x6		
X.509 Certificate		
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBE	GA1UECAwk	(Q2FsaWZv
Step 3 of 3	Back	Save

Passaggio 8. Configurare il mapping ruoli/ruolo utente predefinito in Configurazione avanzata.

Single Sign-On (SSO)	
Configuration Details / Identity Provider Single Sign- https://cisco-robiswas.ok Identity Provider Issuer http://www.okta.com/ext X.509 Certificate MIIDrDCCApSgAwIBAgIG	On URL tta.com/app/ciscoorg842643_ kjmr3gbDQjCYNin4x6 GAXMtNBBjMA0GCSqGSIb3DQ
<ul> <li>Advanced Configuration (Ro</li> </ul>	ole Mapping)
Default User Role	Administrator
Access Admin	
Administrator	
Administrator Discovery Admin	
Administrator Discovery Admin External Database User	
Administrator Discovery Admin External Database User Intrusion Admin	
Administrator Discovery Admin External Database User Intrusion Admin Maintenance User	
Administrator Discovery Admin External Database User Intrusion Admin Maintenance User Network Admin	
Administrator Discovery Admin External Database User Intrusion Admin Maintenance User Network Admin Security Analyst	
Administrator Discovery Admin External Database User Intrusion Admin Maintenance User Network Admin Security Analyst Security Analyst (Read Only)	
Administrator Discovery Admin External Database User Intrusion Admin Maintenance User Network Admin Security Analyst Security Analyst (Read Only)	

Passaggio 9. Per verificare la configurazione, fare clic su **Test della configurazione**, come mostrato nell'immagine.



Se il test ha esito positivo, la pagina visualizzata in questa immagine dovrebbe essere una nuova scheda del browser.

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

Passaggio 10. Fare clic su Apply (Applica) per salvare la configurazione.

Configuration Details	/
Identity Provider Sing	gle Sign-On URL
https://cisco-robis	swas.okta.com/app/ciscoorg842643_
Identity Provider Issu	ier
http://www.okta.	com/exkjmr3gbDQjCYNin4x6
X.509 Certificate	
MIIDrDCCApSgAw	IBAgIGAXMtNBBjMA0GCSqGSIb3DQ
Advanced Configure	ation (Belo Manning)

L'SSO deve essere abilitato correttamente.

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

# Verifica

Accedere all'URL FMC dal browser: https://<URL fmc>. Fare clic su Single Sign-On.

cisco	
Firepower	
Management	1
Center	靛
	and the second
Username	
Password	
Single Sign-On	
Log In	/
	X

Verrai reindirizzato alla pagina di accesso iDP (Okta). Fornire le credenziali SSO. Fare clic su Accedi.

Sig	connecting to cisco- gn-in with your cisco-org-842643 account to access FMC- Login	
	okta	
	Sign In Username robiswas@cisco.com	
	Password	
	Sign In Need help signing in?	

Se l'operazione ha esito positivo, sarà possibile accedere e visualizzare la pagina predefinita del CCP.

In FMC, passare a **Sistema > Utenti** per visualizzare l'utente SSO aggiunto al database.

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