Okta Cookbook

This cookbook is to configure Okta for passive authentication in SAML protocol. **Note**: WS-Fed for Office 365 and Okta pair is not supported.

Prerequisites

• Ensure that you download the deployment guide for Okta with Office 365: https://support.okta.com/help/Documentation/Knowledge_Article/Office365-Deployment-Guide

Complete the following steps to configure Okta:

Step 1: Creating an application and download the metadata for Okta Step 2: Configuring Okta in MobileIron Access Step 3: Updating the IDP configuration

Step 1: Creating an application and downloading the metadata file for Okta

Note: If you have already created an application, skip to Step 12 in the following procedure.

Procedure

- 1. Login to Okta with admin credentials.
- 2. Click Applications > Add Application > Create New App.

Okto Get Started Cett Started Add Applications Add Apply Okta Verified Add	Classic UI V Q Search people, apps							Help and Sup	port Sign out
- Back to Applications	Okta Get Started Dashboard	Directory Applic	cations Security				Upgrade		My Apps 🔿
Add Application	- Back to Applications								
Q Search for an application All A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Can't find an app? &frankly &frankly Add Create New App Apps you created (6) → I00000t Add INTEGRATION PROPERTIES I01domains.com Add Supports SAML I01domains.com Add	Add Application								
Q search for an application AI A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Can't find an app? & frankly Create New App Add Apps you created (6) → 10000ft Okta Verified Add INTEGRATION PROPERTIES 101domains.com Supports SAML Add									
Can't find an app? &frankly &frankly Add Create New App Apps you created (6) → Image: Constant of the second of t	Q Search for an application		A	И А В С О	EFG	ніјкі	LMNOP	QRSTU	VWXYZ
Create New App Apps you created (6) → Integration PROPERTies Any Integration Properties Supports SAML	Can't find an app?	&frankly	&frankly						Add
Apps you created (6) → Integration PROPERTies Integration PROPERTies Add Any Integration Properties Integration Properties Supports SAML Okta Verified Add	Create New App		Okta verified 🗸	SAML					
INTEGRATION PROPERTIES Any Supports SAML Supports SAML Supports Revisions	Apps you created (6) \rightarrow		10000ft						0 st st
INTEGRATION PROPERTIES Any ID/demails ID/dem		•	Okta Vertfied						Add
Any Woodmains.com Okto Verfied Add	INTEGRATION PROPERTIES		101domaine com						
Supports SAML	Any	[]]] domaloj	Okta Verified						Add
Supports Providencing	Supports SAML								
Supports Provisioning Okti Connector by Aquera Learn More	Supports Provisioning	•	10kft Connector b	y Aquera					Learn More

3. Select SAML 2.0 and click Create.

Create a New Application Integration		×
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.	
	Create Cancel	

4. On the **General Settings** tab, enter the **App name** for the application and click **Next**.

1 General Settings	2 Configure SAML	3 Feedback
1 General Settings		
App name		
App logo (optional) 💿	Ø	
	Upload Logo	Browse.
App visibility	Do not display application icon to users Do not display application icon in the Okta Mobile app	5
Cancel		Next

5. On the **Configure SAML** tab, enter the configuration values.

1 General Settings		2 Configure S	AML		3 Feedback
SAML Settings					
					What does this form do?
GENERAL					This form generates the XML needed for the app's SAML request.
Single sign on URL 👔					Where do I find the info this form need
	Vse th	is for Recipient URL and Destinati	on URL		The app you're trying to integrate with
	Allow	this app to request other SSO URI	_s		should have its own documentation on using SAML You'll need to find that doc
					and it should outline what information yo
Audience URI (SP Entity ID) 🔞					need to specify in this form.
Default RelayState 🕘					Okta Certificate
	lf no value	is set, a blank RelayState is sent			Import the Okta certificate to your Identit Provider if required.
Name ID format 👔	Unspecif	ied 🔹			且 Download Okta Certificate
Application username 💿	Okta use	rname 👻			
Update application username on	Create a	nd update 🔻			
			Show Advanced Sett	ings	

SAML Settings	Values
Single sign on URL	Extract the single sign on URL from the SP metadata file. Select the check box for Use this for Recipient URL and destination URL .
Audience URI (SP Entity ID)	Enter the above single sign on URL.
Default RelayState	Enter the above single sign on URL. If no value is set, a blank relay is sent.
Name ID format	Persistent
Application username	Okta username

6. Click Show Advanced Settings.

		Hide Advanced Settings
Response 💿	Signed	
Assertion Signature 💿	Signed	
Signature Algorithm 💿	RSA-SHA256	
Digest Algorithm 💿	SHA256	
Assertion Encryption	Unencrypted •	
Enable Single Logout 💿	Allow application to initiate Single Logo	but
Authentication context class 📀	PasswordProtectedTransport -	
Honor Force Authentication 💿	Yes 💌	
SAML Issuer ID 💿	http://www.okta.com/\${org.externalKey}	

Settings	Values
Response	Unsigned
Assertion Signature	Signed
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
Enable Single Logout	Deselect the check box for Allow application to
	initiate Single Logout
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/\$(org.externalKey)

(Optional) Add the screen, ATTRIBUTE STATEMENTS.

- user.email for IDPEmail
- UPN
 - 7. Configure the **Feedback Settings** and click **Finish**.
 - Are you a customer partner: Select I'm an Okta customer adding an internal app.
 - Select the This is an internal app that we have created check box.

Create SAML Integration

1 General Settings	2 Configure SAML	3 Feedback
3 Help Okta Support understand ho	v you configured this application	
Are you a customer or partner?	I'm an Okta customer adding an internal app I'm a software vendor. I'd like to integrate my app with Okta	Why are you asking me this? This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate It.
Previous		Finish

8. Click **Directory** >**People** > **Add Person**. The **Add Person** screen displays. Create a new user.

User type 🔘	User v
First name	
Last name	
Username	
Primary email	
Secondary email (optional)	
Groups (optional)	You haven't added any groups
Password 💿	Set by user 👻
	Send user activation email now 🔘

- 9. On the Applications tab, click Assign Application.10. Select the Application and the User that you have created and click Next.

Б Д	ssign Applic	cations							
1	Assign Apps to Pe	ople 2	Confirm Assignment	5					
	ancei								Next
A	pplications 1				<u>الم</u>	eople 1			
Se	arch				Q	Search by person	1.		
	Application & Labe		*	Sign-on		Person & Username	^	Status	
	٥			SAML 2.0	۲	tu4 acc		Active	
	acc	ess sp		SAML 2.0		admin admin		Active	

11. Click **Confirm Assignments**.

Ssign Applications	
1 Assign Apps to People 2 Confirm Assignments	
Review your assignments before confirming	
	Assignment Summary
Contre Contre Contre Assignments	Applications (1)
	• abhi

12. Click **Applications**. Select the application you created.

13. Click **Sign On** tab.

14. Click **Identity Provider metadata** to download the metadata file for Okta. General Sign On Mobile Import Assignme

ettings	Ed
SIGN OI	N METHODS
The sign on meth	on method determines how a user signs into and manages their credentials for an application. Some sign ods require additional configuration in the 3rd party application.
Applicati	on username is determined by the user profile mapping. Configure profile mapping
. SA	ML 2.0
	Default Relay State
A	SAML 2.0 is not configured until you complete the setup instructions.
	View Setup Instructions

Step 2: Configuring Okta in MobileIron Access

You must create the federated pair in MobileIron Access.

Procedure

- 1. Login to MobileIron Access administrative portal with admin credentials.
- 2. Click **Profile** > **Federation**.

	Profile / Federation									
M								① Changes have been made. You must republish the profile.	View Changes	Publish
	Federation Hide Description Configure a trust between the Service Provider(SP), Identity Provider(IDP) and Access Control for Cloud Service. Important: Ensure that you have federation(Single Sign on) setup between the SP and IDP before proceeding. Review the critical errors and warnings below. The issues may cause the federation to stop working									
¢	Add Pair 🖂									
	✓ Delegated IDP									
	How to configure Access as Delegated	IdP.								/
	IDP NAME	POLICY	CREATED	ON		ACTION 8				
	You dont have any pairs yet. Let's fix that!	Click on Add Pair above								
	\checkmark Federated Pairs									
	How to upload my Access metadata to	my IDP or SP.								
	SP	IDP	NAME	POLICY	CERT \$ SO	CREATED ON	ACTION S			
•	Custom SAML Service Provider	okta	custom	ZSO-Policy	Yes	2020/02/17 3:09 PM	🖹 🥢 :			
\odot	Access SP Metadata (Upload to IDP) Vi Access IDP Metadata (Upload to SP) Vi	ew Download Copy URL ew Download Copy URL								

3. Click Add Pair > Federated Pair. The Choose Service Provider window appears.

	← Back to list				
	Add Cancel Federated Pair	Choose Service Provide	er		
9	Choose Service Provider	box	cisco Webex	CONCUP.	Dropbox Business
L.	2 Configure Service Provider				
	3 Choose Identity Provider				
¢	4 Configure Identity Provider	by facebook	G Suite	Using SAML	Office 365 Using WS-Federation
		SAP SuccessFactors ♡	salesforce	servicenow	‡‡+++++++++++++++++++++++++++++++++++
		Custom SAML Service Provider	Custom WS-Federation Service Provider		
$\mathbf{\Omega}$					

4. Select the appropriate service provider from the catalog and click **Next** to configure the desired service provider.

5. Click **Next** to select the **Okta** as the identity provider and configure the identity provider.

	← Back to list							
M	Add Cancel	Microsoft Office 365(SAM	L)					
ą	Pair	Conditional access control for Microsoft Office 385 applications like OneDrive, Outlook app and the ecosystem of applications that access Microsoft Office 385 (SAML 2.0)						
9	Choose Service Provider	Choose Identity Provid	er					
Ŀ	Configure Service Provider							
C	3 Choose Identity Provider	G Suite	Microsoft	Microsoft Azure Active Directory	okta			
¢	4 Configure Identity Provider		Active Directory Federation Services		United			
		onelogin	Ping Identity	S SECUREAUTH	Provider			
0		- Back						
-								

- 6. Select the Access Signing Certificate from the drop-down list or click Advanced Options to generate a signing certificate.
- 7. Enter the Identity Provider Federation Metadata.
 - 1. **Upload Metadata**: Click **Choose File** to upload the metadata file that you downloaded in Step 1 from Okta portal.
 - 2. Add Metadata: Extract the Entity ID URL and the Base64 Encoded Certificate from the metadata file downloaded in Step 1.
 - Enter the same URL for the Entity ID, POST SSO URL, and Redirect SSO URL.
 - Enter the **Base64 Encoded Certificate for Signing**.

▼ <md:entitydescriptor [entityid="http://www.okta.com/exkhgpzuvSrPwfsng0h7" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" }<br="">▼<md:idpssodescriptor protocolsupportenumeration="urn:oasis:names:tc:SAML:2.0:protocol" wantuthnrequestssigned="false"></md:idpssodescriptor></md:entitydescriptor>
<pre>w<mo:keydescriptor use="`signing`"></mo:keydescriptor></pre>
<pre>%<ds:keyinto_xmins:ds="http: 09="" 2000="" www.w3.org="" xmidsig#"=""></ds:keyinto_xmins:ds="http:></pre>
▼ <ds:x549ub1a></ds:x549ub1a>
V <s:xs09certificate></s:xs09certificate>
MIIDpDCCAoygAwIBAgIGAVyqFbL8MA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZYYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCmRldi03MTIxODQxHDAaBgkqhkiG9w0BCQEW DWluZm9Ab2t0YS5jb20wHhcNMTcwNjE1MDQ0ODI3WhcNMjcwNjE1MDQ0OTI3WjCBkjELMAkGA1UE
BhMCvVMxEzARBgNVBAgMCkNhbG1mb3JuaWExFjAUBgNVBAcMDVNhb1BGcmFuY21zY28xDTALBgNV_BAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRMwEQYDVQQDDApkZXYtNZEyMTg0MRwwGgYJ
KoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA hWjlowHSnPhyndzsPUsV5vYyvmsMhJGBop9PDOIXHOqvjuQS/2pbQIrfZV+RQANZmEWVBaCTnDQU
s001o+CDqD6iH/7/IWm+psHWlMbvD66akvMuN2iRgukGJzWk8yg90FP5MsVbtbtK0QCvv/6ccai3 rl8PW9/+/bRvFDkEUSCjORYAcYvsmZeO++38eHz7i/SV+etnq5Fvvh5cM/2x3n46gsEEBWWfxjLq
Q5aRKhBxqF36SO16nOhDvX3QjXJCP6F40/9tK3GoHe5PkI0dAhggHaogyS71PPIJsDu7MsCzZ3xx ARmvCZOHYPBKvHM/RUv7/FolCsRG0M5Gvh1VowIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA5I0mh
vBNzZbS7PiNFrqrkbXcblBysXeMBYCClE1pDcnLE3zfXTTk3LoHPhSTNOAkOG5h422IZKT4rGXyO hQw8dhLC3vkluOoZq6YR/vHoL3uMcBqP0MC21MukCT0fY/siQ4nPYVY4I9G4uaW6bfBFaF0KBZBO
4W3gxfnidEDwGtiUBaG6vHs6/XBCglhN8kOog4hC32P5jsgMvbMPncCfEhVDzD6H/t9A0Xdny9Tx nrMJrNm29TuhTDGeFBBI5JRfWul1/lMHIIDz606AI57857bVilZvVR4eqcRoRu81esRAP8DvWrFs
qBjKGBaxjJQ7Jls1EXyv8KMQXmN75VGp
▼ <md:nameidformat></md:nameidformat>
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
<md:singlesignonservice binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" location="https://dev-</td></tr><tr><td>712184.oktapreview.com/app/mobdev712184_gsuiteokta_1/exkhgpzuw5rPwfsng0h7/sso/saml"></md:singlesignonservice>
<md:singlesignonservice binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" location="https://dev-</td></tr><tr><td>712184.oktapreview.com/app/mobdev712184_gsuiteokta_1/exkhgpzuw5rPwfsng0h7/sso/saml"></md:singlesignonservice>

3. Metadata URL: In the Okta admin portal, on the Applications > Sign On tab, click Identity Provider Metadata. This file opens in a new tab and the URL of this page forms the Metadata URL for Okta.

For example: <u>https://dev-</u> 712184.oktapreview.com/app/exkpstisjbzZN6o0h7/sso/saml/metadata

- 8. Enter the Identity Provider Settings.
 - 1. Select the ECP backend Type from the drop-down list.
 - WS-Trust 1.3
 - WS_Trust 2005
 - SAML 2.0
 - 2. Enter the Federated Domain: <domain_name>
- 9. Enter the Active Logon Settings: Original IDP Active Logon URL: <u>https://<okta>.oktapreview.com/app/office365/exkc1nvw91H9nuyFX0h7/sso/w</u> <u>sfed/active</u>
- 10. Click Done.
- 11. On **Profile** > **Federation**, download the following files:
 - Access SP Metadata (Upload to IDP)
 - Access IDP Metadata (Upload to SP)

Federated Pairs

8P	ID P	NAME	POLICY	CERT 880	CREATED ON	ACTION 8			
Custom SAML Service Provider	okta	custom	ZSO-Policy	Yes	2020/02/17 3:09 PM	ľ	Ø	÷	
Access SP Metadata (Upload to IDP) Vie Access IDP Metadata (Upload to SP) Vie	w Download Copy URL w Download Copy URL								

Step 3: Updating the IDP configuration

You must configure the IDP settings with the SP proxy settings to build a trust relationship.

Prerequisites

Extract the Entity ID from the Access SP Metadata (Upload to IDP) downloaded after creating the federated pair.

Procedure

- 1. Login to Okta administrative portal with admin credentials.
- 2. On the **Application** tab, select the application that you created.
- 3. On the **General tab** > **SAML Settings**. Click **Edit**.
- 4. On General Settings tab, click Next.
- 5. Enter the following details extracted from the Access SP Metadata (Upload to IDP):

- Single sign on URL: Entity ID of the Access SP Metadata (Upload to IDP)
- Audience URI: Same as Single sign on URL
- Name ID Format: Persistent
- Application username: Okta username
- 6. Click **Next** > **Finish**.

Related Topics

The following topics are available in the MobileIron Access Guide. See <u>Access Product</u> <u>Documentation</u>.

- See "Zero Sign-on with MobileIron Access" in the *MobileIron Access Guide*.
- See "Configuring LDAP in MobileIron Cloud for session revocation" and "Configuring LDAP in MobileIron Core for session revocation" in the <u>MobileIron</u> <u>Access Guide</u>.