



MobileIron Access Cookbook

Access with ServiceNow and Okta

October 25, 2017



Contents

Overview	3
Prerequisites	3
Configuring ServiceNow and Okta with MobileIron Access	4
Configure the Okta environment	4
Configure the ServiceNow environment	7
Enabling Multi-Provider SSO Properties.....	7
Configure Multi-Provider SSO	9
Configure users for Multi-Provider SSO	10
Configure Access to create a Federated Pair	11
Configure the ServiceNow environment with Access	12
Configure the Okta environment with Access	12
Register Sentry to Access	13
Verification	13



Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as ServiceNow is federated with an identity provider such as Okta for authentication. Users authenticate to Okta as an identity provider and obtain a SAML token for accessing applications in a cloud environment, such as ServiceNow.

This guide serves as step-by-step configuration manual for users using Okta as an authentication provider with ServiceNow in a cloud environment.

Prerequisites

You must perform the following steps before you configure the service provider and identity provider with Access:

- Verify that you have the credentials for Okta admin account.
<http://developer.okta.com>
Note: After signing up, you will receive an activation link on the registered email. Save the activation URL. The URL might be similar to dev-931016-admin.oktapreview.com
- Verify that you have the metadata files for ServiceNow
For more information, see [Configure the ServiceNow environment](#)
- Verify that you have the metadata files for Okta.
For more information, see [Configure the Okta environment](#).
 - Perform the steps 1 to 10 in the [Configure the Okta environment](#) section.



Configuring ServiceNow and Okta with MobileIron Access

You must perform the following tasks to configure ServiceNow and Okta with MobileIron Access:

- [Configure the Okta environment](#)
- [Configure the ServiceNow environment](#)
- [Configure Access to create a Federated Pair](#)
- [Register Sentry to Access](#)
- [Configure the ServiceNow environment with Access](#)
- [Configure the Okta environment with Access](#)

[Configure the Okta environment](#)

1. Login to Okta with admin credentials using the sign-in URL received in the activation mail.
2. Select **Admin >Directory > People**.
3. Select **Add Person > Fill details > Save details**.
Note: The email id should be same as that of ServiceNow.
4. On the **Application** tab, click **Add Application**.
5. In the **Create a New Application Integration** window, select **SAML 2.0** radio button. Click **Create**.

The screenshot shows a dialog box titled "Create a New Application Integration". It has a blue header with a close button. The "Platform" dropdown menu is set to "Web". Under the "Sign on method" section, there are three radio buttons: "Secure Web Authentication (SWA)", "SAML 2.0", and "OpenID Connect". The "SAML 2.0" option is selected. Below each radio button is a short description. At the bottom right, there are two buttons: "Create" (highlighted in green) and "Cancel".

6. Under the **General Setting** tab, enter the **Application name** and click **Next**.
7. In SAML settings, enter the Audience URL, Name ID format, and Application username and click **Show Advanced Settings**.



GENERAL

Single sign on URL
 Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState
If no value is set, a blank RelayState is sent.

Name ID format

Application username

[Show Advanced Settings](#)

8. Enter the configuration values as shown in the below screen and click **Next**.

[Hide Advanced Settings](#)

Response

Assertion Signature

Signature Algorithm

Digest Algorithm

Assertion Encryption

Enable Single Logout Allow application to initiate Single Logout

Authentication context class

Honor Force Authentication

SAML Issuer ID



ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value	
IDPEmail	Unspecified	user.email	×
UPN	Unspecified	user.email	×

[Add Another](#)

9. Configure the feedback settings as below and click **Finish**.

1 General Settings

2 Configure SAML

3 Help Okta Support understand how 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

i The optional questions below assist Okta Support in understanding your app integration.

App type **i**

This is an internal app that we have created

[Previous](#) [Finish](#)

10. Click **Applications** and select the application that you created. Click **Sign On** and download the identity provider metadata.



← Back to Applications

Access-Successfactors

Active View Logs

General Sign On Import Assignments

Settings Edit

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

CREDENTIALS DETAILS

Application username format Okta username

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

11. Click **Directory > People > Add Person** and create a **User**.
12. On the **Applications** tab, select **Assign Applications**.
13. Select the **Application** and the **User** and click **Next**.
14. Click **Confirm Assignment**.

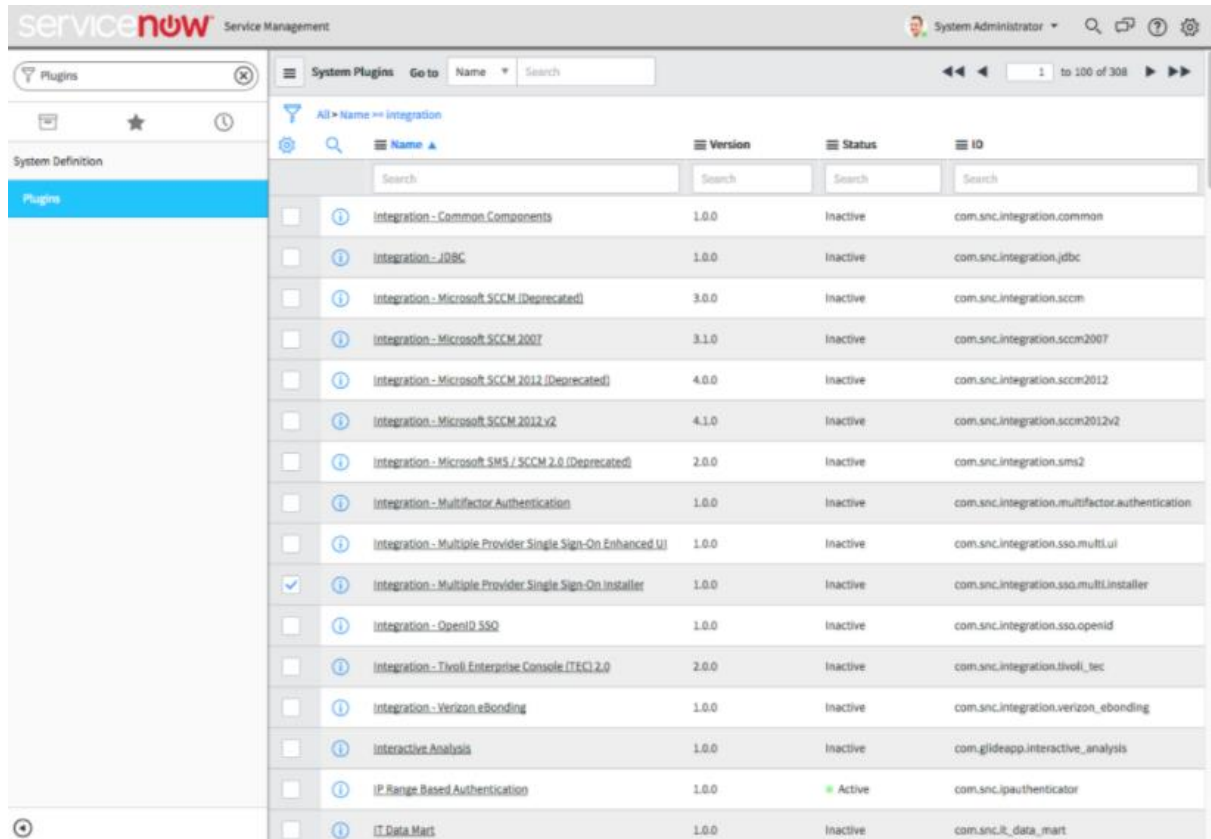
[Configure the ServiceNow environment](#)

You must configure ServiceNow with Access natively by performing the following tasks:

- [Enabling Multi-Provider SSO Properties](#)
- [Configure Multi-Provider SSO](#)
- [Configure users for Multi-Provider SSO](#)

Enabling Multi-Provider SSO Properties

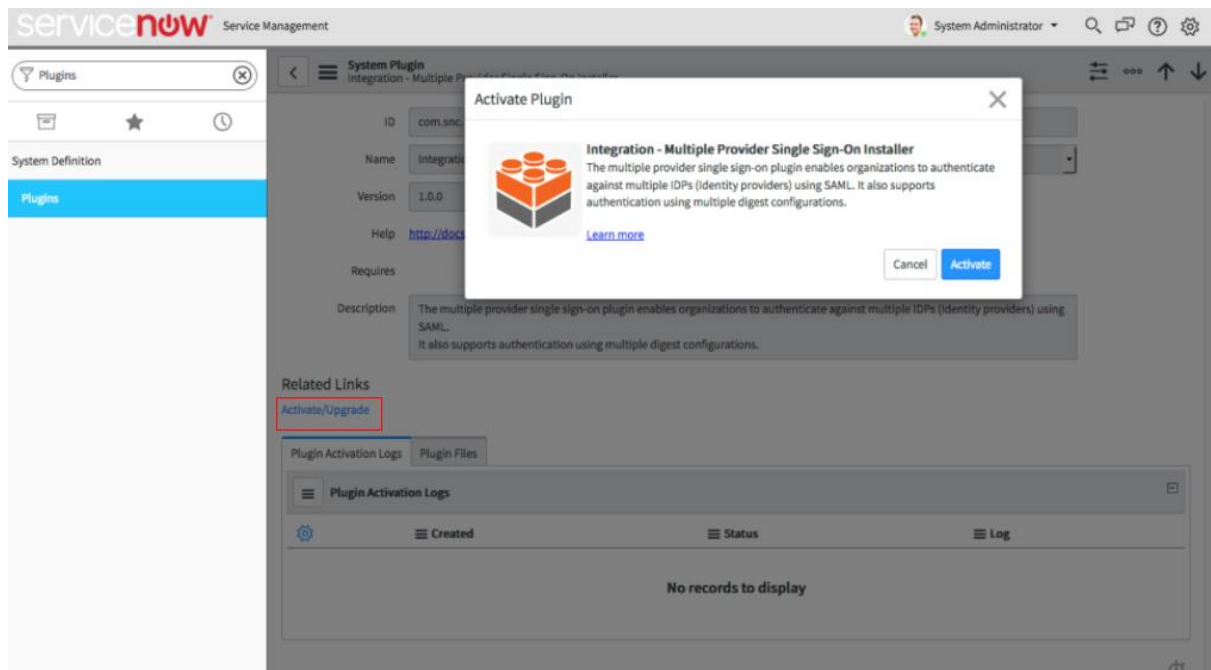
1. Login to ServiceNow with admin credentials.
2. Type **Plugins** in the filter navigator > click **Plugins**.
3. Search for **Integration** in the **Search** box.
4. Select **Integration – Multiple Provider Single Sign-On Installer**.



The screenshot shows the ServiceNow System Plugins interface. The left sidebar contains 'System Definition' and 'Plugins'. The main area displays a table of plugins with columns for Name, Version, Status, and ID. The 'Integration - Multiple Provider Single Sign-On Installer' plugin is selected, indicated by a checkmark in the first column.

	Name	Version	Status	ID
<input type="checkbox"/>	Integration - Common Components	1.0.0	Inactive	com.snc.integration.common
<input type="checkbox"/>	Integration - JDBC	1.0.0	Inactive	com.snc.integration.jdbc
<input type="checkbox"/>	Integration - Microsoft SCCM (Deprecated)	3.0.0	Inactive	com.snc.integration.sccm
<input type="checkbox"/>	Integration - Microsoft SCCM 2007	3.1.0	Inactive	com.snc.integration.sccm2007
<input type="checkbox"/>	Integration - Microsoft SCCM 2012 (Deprecated)	4.0.0	Inactive	com.snc.integration.sccm2012
<input type="checkbox"/>	Integration - Microsoft SCCM 2012 v2	4.1.0	Inactive	com.snc.integration.sccm2012v2
<input type="checkbox"/>	Integration - Microsoft SMS / SCCM 2.0 (Deprecated)	2.0.0	Inactive	com.snc.integration.sms2
<input type="checkbox"/>	Integration - Multifactor Authentication	1.0.0	Inactive	com.snc.integration.mulfactor.authentication
<input type="checkbox"/>	Integration - Multiple Provider Single Sign-On Enhanced UI	1.0.0	Inactive	com.snc.integration.sso.multi.ui
<input checked="" type="checkbox"/>	Integration - Multiple Provider Single Sign-On Installer	1.0.0	Inactive	com.snc.integration.sso.multi.installer
<input type="checkbox"/>	Integration - OpenID SSO	1.0.0	Inactive	com.snc.integration.sso.openid
<input type="checkbox"/>	Integration - Thwoli Enterprise Console (TECI) 2.0	2.0.0	Inactive	com.snc.integration.thwoli_tec
<input type="checkbox"/>	Integration - Verizon eBonding	1.0.0	Inactive	com.snc.integration.verizon_ebonding
<input type="checkbox"/>	Interactive Analysis	1.0.0	Inactive	com.glideapp.interactive_analysis
<input type="checkbox"/>	IP Range Based Authentication	1.0.0	Active	com.snc.ipauthenticator
<input type="checkbox"/>	IT Data Mart	1.0.0	Inactive	com.snc.it_data_mart

5. Click **Activate/Upgrade** and click **Activate** to complete the activation.



The screenshot shows the 'Activate Plugin' dialog box for the 'Integration - Multiple Provider Single Sign-On Installer' plugin. The dialog includes a description of the plugin and an 'Activate' button. In the background, the 'Activate/Upgrade' link in the 'Related Links' section is highlighted with a red box.

Activate Plugin

Integration - Multiple Provider Single Sign-On Installer
The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (identity providers) using SAML. It also supports authentication using multiple digest configurations.
[Learn more](#)

Cancel Activate

Related Links
Activate/Upgrade

Plugin Activation Logs Plugin Files

Plugin Activation Logs

Created	Status	Log
No records to display		



4. Click **Generate Metadata** and save it to xml file.

Configure users for Multi-Provider SSO

Prerequisites

Verify that you have enabled and configured Multi-Provider SSO.

Procedure

1. Login to ServiceNow with admin credentials.
2. Type **Multi** in the search filter and select **Identity Providers**. Right-click **IdP record** and copy the `sys_id`.

The screenshot shows the ServiceNow Identity Providers list. The search filter is set to 'mult'. A context menu is open over the 'https://pingone.com' record, with 'Copy sys_id' selected. The table below shows the details of the Identity Providers.

Name	Active	External logout redirect	Single Sign-On Script	Default	Auto Redirect IdP
Digested Token	true	external_logout_complete.do	MultiSSO_DigestedToken	false	false
https://pingone.com	true	external_logout_complete.do	MultiSSO_SAML2_Update1	true	false
SAML2_Update1	false	external_logout_complete.do	MultiSSO_SAML2_Update1	false	false

3. Type **Users** in the search filter. Select **Users** > **New** > right-click on the top bar next to **User** > **Configure** > **Form Layout** and select **SSO Source** in **Available** list and move it to the **Selected** list. Click **Save**.

The screenshot shows the 'Configuring User form' page in ServiceNow. The 'Available' list contains various fields, and 'SSO Source' has been moved to the 'Selected' list. The 'Form view and section' section shows the 'User' section selected. The 'Create new field' section is also visible.

Available	Selected
Building [+]	Permissions needs reset
City	Locked out
Class	Active
Company [+]	Web service access only
Cost center [+]	Internal integration User
Country code	{ split }
Created	Email
Created by	Language
Default perspective [+]	Notification
Department [+]	Calendar integration
Domain [+]	Time zone
Domain Path	Date format
Employee number	Business phone
Failed login attempts	Mobile phone
Gender	Photo
Home phone	{ end_split }
	SSO Source



4. Click **New** and enter the **User ID** and **Email** of the User.
5. Paste the sys_id in the **SSO Source** field and click **Update**.

6. Click **Test Connection** > Enter **Username** and **Password** > **Sign On**.
The test connection should be successful.
7. Click **Activate** to activate the rule. The Activate button is available after the connection is tested.
8. Enable **Auto Redirect IdP** at the bottom of the page.

[Configure Access to create a Federated Pair](#)

You must configure Access to select your service provider and the identity provider. You can apply the configuration settings for the service provider and the identity provider to create a federated pair.

Procedure

1. Log in to **Access**.
2. Click **Profile** > **Get Started**.
3. Enter Access host information and upload the **ACCESS SSL certificate**. The other fields retain the default values. Click **Save**. For more information on Access SSL certificates, see *Certificates* in the *MobileIron Access Guide*.
4. Click **Profile** > **Federated Pairs** > **Add New Pair**.
5. Select **ServiceNow** as the service provider.
6. Enter the following details:
 - a. Enter a **Name** for the federated pair.
 - b. Enter an appropriate **Description**.



- c. Select or upload a new **Access Signing Certificate**.
 - d. Upload the metadata details for **ServiceNow**. See [Prerequisites](#).
 - e. (Optional) Select *Use Tunnel Certificates for SSO* to configure Cert SSO on MobileIron Core. See *Appendix* in the *MobileIron Access Guide* at <https://support.mobileiron.com/docs/current/accs/> .
7. Click **Next**.
 8. Select **Okta** as the Identity provider. Click **Next**.
 9. Select or upload the **Access Signing certificate**.
 10. Upload the **IdP metadata file**. Click **Done**.
 11. On the **Profile** tab, click **Publish** to publish the profile.
 12. Download the **ACCESS SP Metadata and upload to IDP** from the federated pair page.
 13. Download the **ACCESS IDP Metadata and upload to SP** from the federated pair page.

Task Result

The Federated Pair is created.

[Configure the ServiceNow environment with Access](#)

You must configure ServiceNow with Access to upload the metadata file that you downloaded when configuring the Federated Pair with Access.

Prerequisites

Verify that you have the “**Access IDP Metadata and Upload to SP**” XML that you downloaded in **Step 13** in the [Configure Access to create a Federated Pair](#) section.

Procedure

1. Login to ServiceNow with admin credentials.
2. Type Multi in the Search filter and select Identity Providers > New > SAML > Import IdP Metadata using “**Access IdP Metadata and Upload to SP**” XML downloaded at **Step 13** in the Configure Access to create a Federated Pair section.
3. Click **Test Connection** and enter the **username** and **password**.
4. Click **Sign On**. The Test Connection must be successful.
5. Click **Activate** which is available after you test the connection.
6. Select **Set As Auto Redirect IdP** option to enable Auto Redirect IdP.

[Configure the Okta environment with Access](#)

You must configure Okta with Access to upload the metadata file that you downloaded when configuring the Federated Pair with Access.

Prerequisites

Extract the entity ID from “**Access SP Metadata and Upload to IdP**” XML that you downloaded at **Step 12** in the [Configure Access to create a Federated Pair](#) section.



Procedure

1. Login to Okta with admin credentials.
2. Click **Applications** > **ServiceNow** that was added earlier.
3. Click **General** > **Edit SAML Settings** > **Next**.
4. Enter the **Entity ID URL** to **Single Sign On URL** and **Audience URL**.
5. Click **Show Advanced Settings**
 - Modify response to Unsigned.
 - Signature Algorithm to SHA 1.
6. Click **Next** > **Finish**.

[Register Sentry to Access](#)

You must register Sentry to Access to fetch the latest configuration from Access.

Prerequisite

Verify that you have registered Sentry earlier. If so, then do not perform this step.

Procedure

1. **Clish** Sentry. In the configuration mode, execute the following command for registration.
(config)#accs registration https://<FQDN of Access server><Admin Username of Access Server>
2. Enter the **Tenant password** and complete the registration.
3. In **Access**, click the **Sentry** tab.
4. Select the appropriate Sentry instance, then click **Action** > **Assign**.
5. Enter the tenant password.
6. Click **OK**.
7. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

(config)# accs config-fetch update

Note: All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

Verification

Login to ServiceNow and enter the custom domain details. You are redirected to Okta login page for authentication.

When you provide the credentials for Okta, you must be redirected to ServiceNow home page.



Copyright © 2016 - 2017 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.