

MobileIron Access Cookbook Access with SuccessFactors and Okta

Revised: 03 January 2017



Contents

Overview	3
Prerequisites	3
Configure the Okta environment	4
Configuring SuccessFactors and Okta with MobileIron Access	7
Register Sentry to Access	7
Configure Access to create a Federated Pair	7
Configure the Okta environment with MobileIron Access	8
Configure the SuccessFactors environment with MobileIron Access	9
Verification	11



Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as SuccessFactors is federated with an identity provider such as Okta for authentication. The user gets authenticated by Okta and obtains a token for accessing applications in a cloud environment, such as SuccessFactors. This guide serves as step-by-step configuration manual for users using Okta as an authentication provider with SuccessFactors in a cloud environment.

Disclaimer:

This cookbook is informational to help with the setup flow and actual screenshots. The steps might vary in your deployment scenario due to changes in SP/IdP versions.

Prerequisites

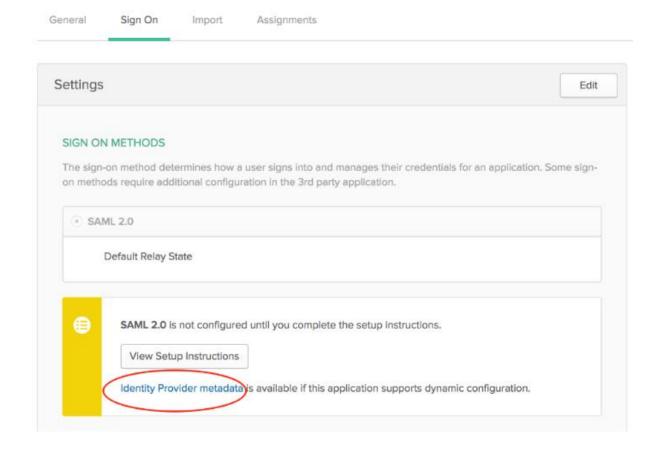
- Ensure that you have a working setup of native federation for SuccessFactors and Okta in your environment.
- Verify that you have the metadata files for Successfactors and Okta.
- Okta (IDP) Metadata Files

Download the metadata files for Okta (IdP)

Perform the steps 1 to 10 in the

• Configure the Okta environment section.





• SuccessFactors (SP) Metadata Files

Download the metadata files for SuccessFactors (SP)

- > Tenant ID:
 - https://salesdemo4.successfactors.com/login?company=<your_company>
- **EntityID**: <a href="https://www.successfactors.com/<your_company">https://www.successfactors.com/<your_company
- Assertion Consumer Service URL:
 <a href="https://salesdemo4.successfactors.com/saml2/SAMLAssertionConsumer?<your_company">https://salesdemo4.successfactors.com/saml2/SAMLAssertionConsumer?<your_company

Configure the Okta environment

Configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

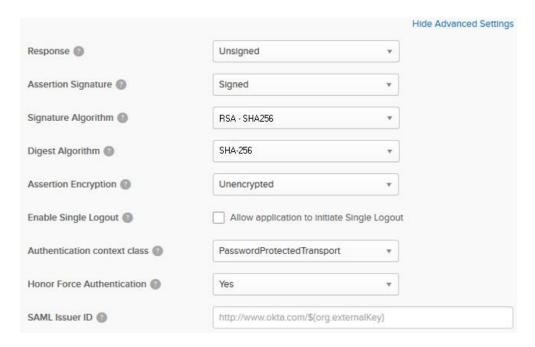
Procedure

- 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.

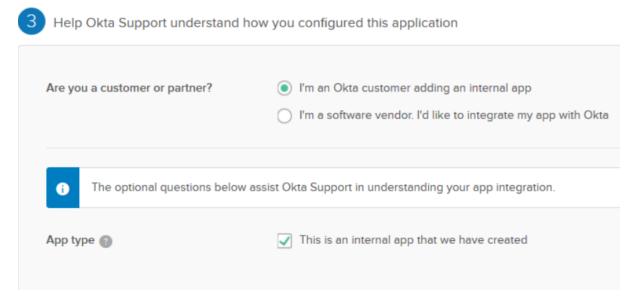
Note: The email id should be same as that of SuccessFactors.



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



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



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



Configuring SuccessFactors and Okta with MobileIron Access

You must perform the following tasks to accomplish the configuration between SuccessFactors and Okta:

- Register Sentry to Access
- 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. Click **OK**.
- 6. **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.

- Configure Access to create a Federated Pair
- Configure the Okta environment with MobileIron Access
- Configure the SuccessFactors environment with MobileIron Access

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

- 7. **Clish** Sentry. In the configuration mode, execute the following command for registration.
 - (config)#accs registration https:/<FQDN of Access server><Admin Username of Access
- 8. Enter the **Tenant password** and complete the registration.
- 9. In Access, click the Sentry tab.
- 10. Select the appropriate Sentry instance, then click **Action** > **Assign**.
- 11. Click **OK**.
- 12. **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.

Configure Access to create a Federated Pair

You must configure Access to select your service provider and the identity provider to create a federated pair.

Procedure

- 1. In Access, click **Profile** > **Get Started**.
- 2. Enter the Access host information and upload the ACCESS SSL Certificate. The other fields retain their default values. Click **Save**.
- 3. Click Profile > Federated Pairs > Add New Pair.
- 4. Select **SAP SuccessFactors** as the service provider.
- 5. Enter the following details:
 - Name
 - Description
 - Select the **Access Signing Certificate** or use the **Advanced Options** to create a new Access Signing Certificate.
 - Enter the Entity ID, and Assertion Consumer Service URL for SuccessFactors. See Prerequisites.
 - (Optional): Select **Use Tunnel Certificates for SSO** for users to be authenticated automatically. This leverages the user's authentication in the MobileIron Tunnel VPN. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/curent/accs.
- 6. Click **Next** and select **Okta** as the identity provider.



- 7. Select the **Access Signing Certificate** or use the **Advanced Options** to create and upload a new self-signed Access Signing Certificate.
- 8. **Add** the IdP metadata or **Upload** the IdP metadata file that you downloaded in <u>Prerequisites</u>.
- 9. Click **Done**.
- 10. Download the Access SP Metadata (Upload to IDP) and ACCESS IDP Metadata (Upload to SP) metadata files.
- 11. Click **Publish** to publish the profile.

Configure the Okta environment with MobileIron Access

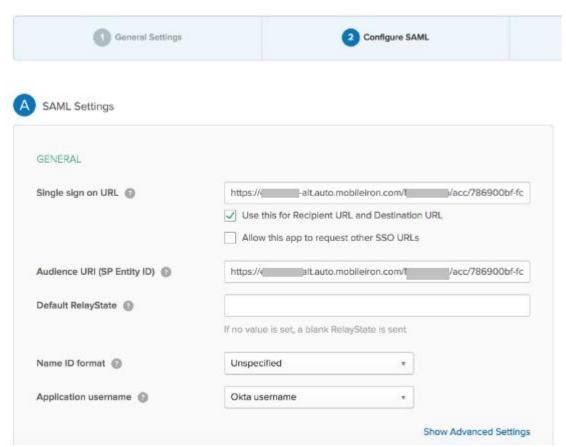
Procedure

1. Login to Okta with admin credentials.

Click **Application** and select the application that you created in the

- 2. Configure the Okta environment section.
- 3. On the General tab, click Edit SAML Settings and click Next.
- 4. Extract the service provider entity ID from SP proxy metadata file and configure the settings as shown below:

Edit SAML Integration





Configure the SuccessFactors environment with MobileIron Access

Procedure

1. Login to SAP SuccessFactors instance and click **Single Sign-On (SSO)** settings. Extract the **SAML Issuer**, **Certificate**, **Global Logout Service URL (Logout Request destination)**, **Single Sign On** redirect service location from the metadata file that you downloaded in the Step 10 of **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

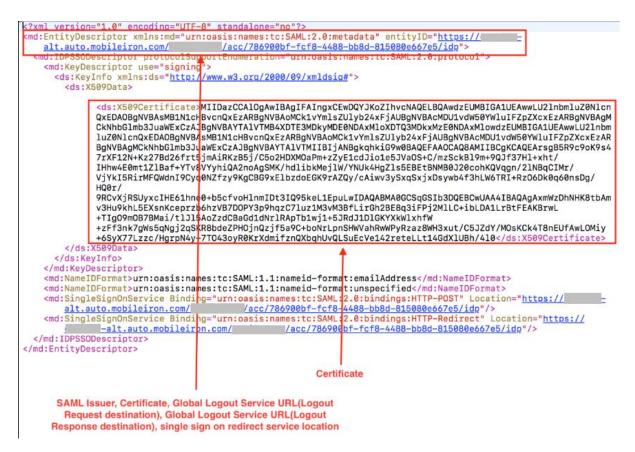
- 13. **Clish** Sentry. In the configuration mode, execute the following command for registration.
 - (config)#accs registration https:/<FQDN of Access server><Admin Username of Access Server>
- 14. Enter the Tenant password and complete the registration.
- 15. In Access, click the Sentry tab.
- 16. Select the appropriate Sentry instance, then click Action > Assign.
- 17. Click OK.
- 18. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

(config)# accs config-fetch update

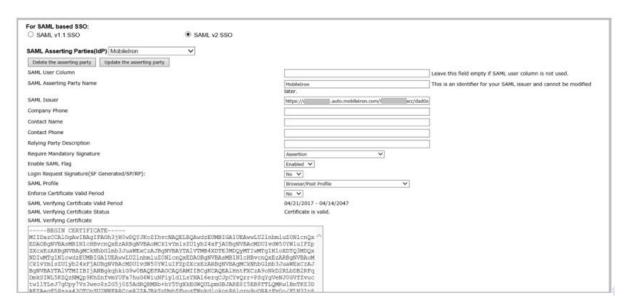
Note: All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

2. Configure Access to create a Federated Pair.





3. Configure SSO settings as shown below on the Success Factors portal.





SAML v2 : SP-initiated logout			
Support SP-initiated Global Logout	Yes 🗸		
SP sign LogoutRequest	No 🗸		
SP validate LogoutResponse	No 🗸		
Global Logout Service URL (LogoutRequest destination)	https://	alt.auto.mobileiron.com/	/acc/dad0e42;
SAML V2 : IDP-initiated Global Logout SP validate LogoutRequest signature SP sign LogoutResponse	Yes ✔ Yes ✔		
Global Logout Service URL (LogoutResponse destination	https://	alt.auto.mobileiron.com/	/acc/dad0e42a
D : 1// /D D: 1 // / /	lo Y		
SAML v2: NameID Setting Require sp must encrypt all NameID elements NameID Format unspecifi	ied 🗸		
SAML v2 : SP-initiated login Enable sp initiated login (AuthnRequest) Default issuer single sign on redirect service location (to be provided by	Yes ✓ ✓ idp) https://	auto.mobileiron.com/I	acc/dad0e42a
Send request as Company-Wide issuer	No 🗸		

Verification

SuccessFactors Mobile App follows Activation process for the user to activate the profile. There are three kinds of Activation process. These processes do not support SAML SSO flow.

- 1. Activation Code
- 2. QR Code



Profile Activation

Help

Activation

Please activate your profile by selecting one of the activation methods below:

Use Activation Code

Scan QR Code

Try Demo

3. Email based Activation

- Download the SuccessFactors mobile application on the device.
- From safari on iOS and chrome on Android, Access the URL mentioned in step 2 in the email.

It prompts to open the link in Mobile App on iOS. Click Ok. On Android, everything is seamless. This starts the SAML SSO flow.



Copyright © 2016 - 2018 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.