

MobileIron Access Cookbook Access with Salesforce and OneLogin

Jun 10, 2017



Contents

Overview	3
Prerequisites	3
Configuring Salesforce and OneLogin with MobileIron Access	4
Configure Access to create a Federated Pair	4
Configure the Onelogin environment	5
Configure the Salesforce environment	6
Configure Salesforce with Access	7
Configure OneLogin with Access	7
Register Sentry to Access	7



Overview

SAML provides single sign-on service for users accessing their services hosted in a cloud environment. Generally, a service provider such as Salesforce is federated with an identity provider such as OneLogin for authentication. The user gets authentication from OneLogin and obtains a SAML token for accessing applications in a cloud environment, such as Salesforce.

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

Prerequisites

- Ensure that you read about OneLogin online tips at <u>https://support.onelogin.com/hc/en-us/articles/201173414-Configuring-SAML-for-Salesforce</u>
- Verify that you have downloaded the Salesforce metadata file:
 - 1. Login to Salesforce tenant with admin credentials.
 - 2. Click Security Control > Single Sign-On Settings > Download Metadata.
 - 3. Click Save.
- Verify that you have downloaded the OneLogin metadata file:
 - 1. Login to OneLogin tenant with admin credentials.
 - 2. Click **MORE ACTIONS** > **SAML Metadata**.
 - 3. Click Save.



Configuring Salesforce and OneLogin with MobileIron Access

You must perform the following tasks to configure Salesforce and OneLogin with MobileIron Access:

- Configure Access to create a Federated Pair
- <u>Configure the OneLogin environment</u>
- <u>Configure the Salesforce environment</u>
- Configure Salesforce with Access
- Configure OneLogin with Access
- <u>Register Sentry to Access</u>

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. It creates a federated pair.

Procedure

- 1. In Access, click **Profiles** > **Get Started**.
- 2. Enter the Access host information and upload the ACCESS SSL Certificate. Use the default values for the other fields. Click **Save**.
- 3. Click Profiles > Federated Pairs > Add New Pair.
- 4. Select Salesforce as the Service Provider.
- 5. Enter the following details
 - Name
 - Description
 - Upload the SP Proxy Certificate
 - Upload the Salesforce metadata file that you downloaded from the Salesforce tenant.
 - (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.
- 7. Select **OneLogin** as the Identity Provider and click **Next**.
- 8. Upload the IdP Proxy certificate and the IdP metadata file that you downloaded.
- 9. Click Done.
- 10. Download the Access SP Metadata (Upload to IDP) and ACCESS IDP Metadata (Upload to SP) metadata files.
- 11. On the **Profile** tab, click **Publish** to publish the profile.



Task Result

The Federated Pair is created.

Configure the OneLogin environment

You must configure OneLogin to use with Salesforce with all the services. This means that there is no Access Sentry configuration yet.

Prerequisites

Verify that you have the admin credentials for OneLogin.

Procedure

- 1. Log in to OneLogin tenant portal with admin credentials.
- 2. Select **Apps** > **Add Apps**.
- 3. Under the **Find Applications** field, search for **Salesforce** and select the following option:



- 4. Click Save.
- 5. On the **Configuration** tab, enter the Salesforce login URL path. **Note**: Login to Salesforce to get the Organization ID. For example:

Info Configur	ation Parameters Rules SSO Access Provisioning Users Privileges
Application Details	Update Entitlements
	"Salesforce Login URL"
	https://login.salesforce.com?so=00D360000
	If you are using a single idP you should use https://login.salestorce.com/so=orgid is the consumer URL
	To find the Org ID navigate to Company Information-Company Profile. If you are using multiple IdPs you will find the Consumer URL in your SAML configuration screen as login URL. NOTE: Org ID is NOT required for sandbox accounts. Please verify your "Salesforce Login URL" in the Salesforce SSO settings. API Version
	To find the Org ID navigate to Company Information-Company Profile. If you are using multiple IdPs you will find the Consumer URL in your SAML configuration screen as login URL. NOT: Org ID is NOT required for sandbox accounts. Please verify your "Salesforce Login URL" in the Salesforce SSO settings. API Version Version 24
API Connection	To find the Org ID havigate to Company Information-Company Profile. If you are using multiple IdPs you will find the Consumer IRL in your SAML configuration screen as login URL. NOT required for sandbox accounts. Please verify your "Salesforce Login URL" in the Salesforce SSO settings. API Version Version 24
API Connection	To find the Org ID havigate to Company Information-Company Profile. If you are using multiple IdPs you will find the Consumer URL in your SAML configuration screen as login URL. NOT required for sandbox accounts. Please verify your "Salesforce Login URL" in the Salesforce SSO settings. API Version Varsion 24 O Disabled ENABLE
API Connection	To find the Org ID havigate to Company Information-Company Profile. If you are using multiple IdPs you will find the Consumer URL in your SAML configuration screen as login URL NOT required for sandbox accounts. Please verify your "Salesforce Login URL" in the Salesforce SSO settings. API Version Version 24 API Status O Disabled ENABLE Connect to Salesforce API over OAuth.

VIDEAS

Quick Find / Search	Company Information Mobileiron			Hulp for this Page
Lightning Experience	The organization's profile is below.			
Salesforce1 Quick Start	Organization Detail	User Licenses (10+)	Parmission Set Licenses (S. Fasture Licenses (12) Usage-based Entitier	reenta (BETA) IO
Force com Home	Organization Name	Mobileiron	Phone	
	Primary Contact	Hashmath Rehman	Fax	
Administer	Division		Default Locale	English (United States)
Manage Users Manage Apps	Address	US	Default Language	English
Manage Territories	Fiscal Year Starts In	January	Default Time Zone	(GMT-08:00) Pacific Standard Time (America/Los_Angeles)
Company Profile	Allow Support to Activate Multiple Currencies		Currency Locale	English (United States) - USD
Company Information	Newsletter	×	Used Data Space	282 KB (6%) [View]
Fiscal Year	Admin Newsletter	1	Used File Space	19 KB (0%) [View]
Business Hours Holidays	Hide Notices About System Maintenance		API Requests, Last 24 Hours	0 (15,000 max)
Language Settings	Hide Notices About System Downtime		Streaming API Events, Last 24 Hours	0 (10,000 max)
Security Controls Domain Management			Restricted Logins, Current Month Salesforce.com Organization ID	0 (0 max) 00D36000000Kyi

- 6. Click Save.
- 7. On the **Parameters** tab, verify that the **Credentials** are as follows and click **Save**.
 - Select **Configured by admin**.
 - Enter **Email** in the User ID field.
- 8. On the **SSO** tab, under the **SAML Signature Algorithm** field select **SHA-1** from the drop-down menu and click **Save**.
- 9. Expand **MORE ACTIONS** and select **SAML Metadata** to download the metadata file. Click **Save**.
- 10. Create a new user and assign the Salesforce application.
 - a Select User > All Users > New.
 - **b** Create a **Test User** and click SAVE USER.

onelogin	USERS APPS DEVICES	ACTIVITY SETTINGS		VPGRADE NOW ?
	← New User		CANCEL SAVE USE	R
		User Info		
		Active		
	•	First Name *	ane	
		Email testone@mitest.com	Lestone	

c On the **Applications** tab > **Roles**, click + to expand the Applications list.

- **d** Select Salesforce as the application from the drop-down menu.
- e Click **Continue** and then click **Save**.
- 11. Set the password for new user.

Go to Users > All Users > User account > Change Password.

Configure the Salesforce environment

You must configure Salesforce to use OneLogin natively with all the services. This means that there is no Access Sentry configuration yet.

1. Login to the Salesforce Tenant with admin credentials.



- 2. Click Security Control > Single Sign-On Settings > Download Metadata.
- 3. Click New from Metadata file, and upload the SAML Metadata file.
- 4. Verify the Entity ID: <u>https://saml.salesforce.com</u> and SP Initiated Request Binding: HTTP POST.
- 5. Click **Manage User > User > New User** to create a new user.
- 6. Enter details in the General Information section, click Save.
- 7. Click **Domain Management > My Domains > Edit**, under the **Authentication Configuration** section. Select the **Authentication Service**.
- 8. Click Save.

Note: Access the tenant either from Desktop Browser or from Salesforce App. You must be able to access the service successfully.

Configure Salesforce with Access

- 1. Login to Salesforce with admin credentials.
- Click Security Controls > Single Sign-On > New from Metadata File and upload the IDP Metadata(Upload to SP) file that you downloaded when configuring Access.
- 3. Upload the metadata file and click **Save**.
- 4. Edit the **Single Sign-On settings**, and enter the Entity ID as follows: **https://saml.salesforce.com.**
- Click Domain Management > MyDomain >Edit Authentication Configuration settings and select IDP-Proxy(Sentry) instead of OneLogin.
- 6. Click Save.

Configure OneLogin with Access

- 1. Log in to OneLogin Tenant portal with admin credentials.
- 2. Click **Salesforce**.
- 3. On the **Configuration** tab, enter the **Salesforce Login URL** that is extracted from the *Upload to IdP metadata file*.
- 4. Click Save.

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 for the profile.
- 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.

Task Result

Single-sign-on service is now configured using SAML with Salesforce as the service provider and OneLogin as the identity provider. This configuration lets you fetch the latest configuration from Access.

You must verify SSO access to Salesforce at this point. The Access reports display the results for traffic flow. The display might be delayed by fifteen minutes.

- Open your Salesforce domain in a browser and log in as a user existing in both OneLogin and Salesforce domains. The browser must be redirected to the OneLogin page.
- Enter the user credentials. The browser must be redirected to Salesforce and you must have access to Salesforce.



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.