

MobileIron Access Cookbook Access with SuccessFactors and Microsoft ADFS

Revised: 03 January 2018



Contents

Overview	3
Prerequisites	3
Configuring SuccessFactors and Microsoft ADFS with MobileIron Access	4
Register Sentry to Access	4
Configure Access to create a Federated Pair	4
Configure the ADFS environment with MobileIron Access	5
Configure the SuccessFactors environment with MobileIron Access	8
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 Microsoft ADFS for authentication. The user gets authenticated by ADFS 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 ADFS 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

Verify that you have the following components in your environment:

- ADFS version 3.0
- Ensure that you have a working setup of native federation for SuccessFactors and ADFS in your environment.
- <u>ADFS (IDP) Metadata Files</u> Download the ADFS metadata files for ADFS (IdP)
 - Download ADFS metadata file from <u>https://<ADFS Server</u> <u>FQDN>/FederationMetadata/2007-06/FederationMetadata.xml</u>

<u>SuccessFactors (SP) Metadata Files</u>

You must get the information for metadata files for SuccessFactors (SP) from Single Sign-On Settings.

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



Configuring SuccessFactors and Microsoft ADFS with MobileIron Access

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

- Register Sentry to Access
- Configure Access to create a Federated Pair
- Configure the ADFS environment with MobileIron Access
- <u>Configure the SuccessFactors environment with MobileIron Access</u>

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

- 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

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

Prerequisites

Verify that you have the credentials for MobileIron Access.



Procedure

- 1. In Access, click **Profile** > **Get Started**.
- Enter the Access host information and upload the ACCESS SSL Certificate. The other fields retain their default values. Click Save.
 Netry Derform stores 1 and 2 analysis a profile is not prosted.
- Note: Perform steps 1 and 2 only if a profile is not created.
- 3. Click **Profile** > **Federated Pairs** > **Add New Pair.**
- 4. Select 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.
 - Upload or Add the service provider metadata.
 If you select Add, enter the Entity ID and Assertion Consumer Service URL. See <u>Prerequisites</u>.
 - (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 Microsoft as the identity provider.
- 7. Select the Access Signing Certificate or use the Advanced Options to create a new self-signed Access Signing Certificate.
- Select Upload Metadata, Add Metadata, or Metadata URL to provide the IdP metadata details that you saved. See <u>Prerequisites</u>. See <u>https://support.mobileiron.com/docs/curent/accs</u> for more information. Click Done.
- 9. Download the Access SP Metadata (Upload to IDP) and ACCESS IDP Metadata (Upload to SP) metadata files.
- 10. Click **Publish** to publish the profile.

Configure the ADFS environment with MobileIron Access

You must configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

Procedure

- 1. Use Remote Desktop services to log into an ADFS machine with Admin credentials.
- 2. Click Start > Administrative tools > ADFS Management > Expand Trust Relationships.
- 3. Click **Relying Party Trust.** Right-click and select **Add Relying Party Trust** and follow the prompts.



. = .			dc01.misentry.com	
	AD FS			-
le Action View Window Help				
۱ 🔁 🖬 🖬				
D FS	Relying Party Trusts			Actions
Service Trust Relationships Claims Provider Trusts Relying Party Trusts Relying Party Trusts Attribute Stores Authentication Policies	Display Name Device Registration Service 0365eaml	Enabled Ty Yes W Yes W	pi Ukoffan 15 auf JSNE, / WS-Federation STratt / SNE, / WS-Federation STratt / SNE, / WS-Federation Umr federation Knonet/Dolve	Relying Party Trusts Add Relying Party Trust Add Non-Claims-Aware Relying Party Tr View New Window from Hare
		\$ 2	Add Relying Party Trust Wizard	ici Befreih
		Welcome		Help
				O265raml
		Wilcom Steet Dis Source Grange National from Advectant from Advectant from Advectant from Advectant Advectant	Instruction Instruction Instruction Instruction	Update from Falancian Mandata En Claim Bulan Disable Progreties Claimes Delate Help

4. Click Start and select Import data about the relying party from a file. Click Next.

Microsoft Hemote Desktop Window Help		6 6 4 5 6 6 6 7 + 8 -	🕄 🛜 🖬 🔝 🛄 U.S. Wed 3:45 PM mgamez Q
		dc01.misentry.com	
		AD FS	- 6
the action view window nep			- 6
AD 55			Later.
Construction Provides Andrementation Provides Andrementation Provides Andrementation Provides	Dead 10 Yee 10 Yee 10 Select Data Source 10 Select Data Source 10 Select Data Source 10 Source Source 10 Soure S	And Selection matches about the intervention of the intervent	Action: Relying Party Trust: Add Non-Charan Charae Relying Party Trust Ven New Workser from Here Image: Annotation of the State

5. Click **Browse** and select the service provider proxy metadata file that you downloaded and click **Next**.

Note: The filename for the proxy metadata file name ends with *UploadTo-Microsoft ADFS-IdP.xml*.



Opping Party Trust Enabled Type More Regulation Service Type More Regulation More methods More Regulation			dc01	.misentry.com		
Deploy Name Deploy Na	elving Party Trusts				_	
Device Registration Service Device Registration Service Device Registration Service Device Registration Service OSSSeard Yes WSTutt / SAML / WSTederation ummed materity com OSSSeard Yes WSTutt / SAML / WSTederation ummed materity com OSSSeard Yes WSTutt / SAML / WSTederation ummed materity com View WSTutt / SAML / WSTederation ummed materity com Select Data Source Select Rotes Source Select Rotes Source Select Rotes Source Select Rotes Source Immed data adout the relying paty published online or on a local network. Once Issuers Select Rotes Source Immed data adout the relying paty published online or on a local network. Once Issuers Select Rotes Tools Immed data adout the relying paty published online or on a local network. Oscience Select Rotes Tool Tool Issuers Rote Rote Rote Rote Rotes Tool Tool Issuers Once Issuers Rote Rote Rote Rote Rote Rote Rote Rote	Deelay Name	Feeblad	Tune	Identifier		
Yes WSTust / SMUL / WSFederation untedevation.MicrosoftOnities	Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	umms-drsmisentry.com		
Add Relying Party Trust Wizard Add Relying Party Trust Wizard Select Data Source Select Data Source Select an option that this wizard wil use to obtain data about this relying party. Videone Solect Data Source Solect Data Source Portion Source Solect Data Source So	O365saml	Yes	WS-Trust / SAML / WS-Federation	um federation MicrosoftOnline		
< Previous Next > Cancel	0365eeml	Yes Select Data Source Sepa Select Data Source Sepa Select Data Source	WS-Trust / SAML / WS-Federation Add Relyin Ce	um federation: Microsoft/Online g Party Trust Wizard d will use to obtain data about this rely g party published online or on a local rencessary data and certificates from ter or a local network. Ness (host name or URL): or https://www.contoso.com/app g party from a file necessary data and certificates from date to a file. Exercised on the file and certificates from date to a file. Exercised on the file and certificates from date to a file. Exercised on the file and certificates from cectors: Exercised on the file and certificates from the necessary data about this rel party manually input the necessary data about this rel	ing party: hetwork a relying party organization m a trusted source. The Prevey Measded sort lying party organization.	x In that publishes In that has Interd will not Browse_
				< Prev	nious Next >	Cancel
				crite	THOM >	

- 6. Enter the **Display Name** and click **Next**. All other fields are set to defaults. Click **Add Rule**.
- 7. At the end, select **Open Edit Claim rules dialog for relying party trust**.
- 8. Select RSA-SHA01 or RSA-SHA256 for encrypted algorithm.
- 9. In the Claim Rule Template drop-down, select Send LDAP Attributes as Claims and click Next.
- 10. Configure the **Claim rules** as follows:

	Edit f	Rule - Rule1	x	
You ca which issued	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.			
Claim r	ule name:			
Rule1				
Rule te	emplate: Send LDAP Attributes as Claims			
Attribu	te store:			
Active	Directory	v		
Маррія	ng of LDAP attributes to outgoing claim type	\$.		
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)		
•	SAM-Account-Name V	Given Name	~	
*	~ ~		\mathbf{v}	

11. Add another rule and select the option Transform an Incoming Claim. Click Next.



12. Enter a name for the rule. The incoming type is Given Name and Outgoing Type is Name ID. The outgoing name ID format must be **Unspecified**.

Edit Rule - Rule2					
You can configure this rule to also map an incoming claim outgoing claim type and whe	map an incoming claim type to an out value to an outgoing claim value. Spec ther the claim value should be mapped	tgoing claim type. As an option, you can sify the incoming claim type to map to the d to a new claim value.			
Claim rule name:					
Rule2					
Rule template: Transform an	Incoming Claim				
Incoming claim type:	Given Name	¥			
Incoming name ID format:	Unspecified	V			
Outgoing claim type:	Name ID	¥			
Outgoing name ID format:	Unspecified	¥			
Pass through all claim values					
 Replace an incoming claim 	m value with a different outgoing claim	i value			
Incoming claim value:					
Outgoing claim value:		Browse			
 Replace incoming e-mail 	suffix claims with a new e-mail suffix				
New e-mail suffix:					
	Example: fabrikam.com				

13. Click Apply and OK.

Configure the SuccessFactors environment with MobileIron Access

Procedure

- 1. Login to SAP SuccessFactors instance and click **Single Sign-On (SSO)** settings.
- 2. 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.Configure Access to create a Federated Pair.

art.auto. .com/Mobile	Iron/acc/786900bf-fcf8-4488-bb8d-815080e667e5/idp">
<md:keydescriptor <="" http:="" th="" use="signing
<ds:KeyInfo xmlns:ds="><th>> /www.w3.org/2000/09/xmldsig#"></th></md:keydescriptor>	> /www.w3.org/2000/09/xmldsig#">
<ds:x509certificate3< th=""><th>MIIDazCCAlOgAwIBAgIFAIngxCEwDQYJKoZIhvcNAQELBQAwdzEUMBIGA1UEAwwLU21nbm1uZ0N1c</th></ds:x509certificate3<>	MIIDazCCAlOgAwIBAgIFAIngxCEwDQYJKoZIhvcNAQELBQAwdzEUMBIGA1UEAwwLU21nbm1uZ0N1c
QxEDAOBgNVBAsMB1N1cF CkNhbG1mb3JuaWExCzAJ JuZBN1ccQxEDAOBoNVBA	BvcnQxEzARBgNVBAoMCk1vYm1sZUlyb24xFjAU8gNVBAcMDU1vdW58VW1u1FZpZXcxEzARBgNVBAg BgNVBAYTAIVTM84XDTE3MDkyMDE@NDAxM1oXDTQ3MDkxMzE@NDAxM1owdzEUMBIGA1UEAwwLU21bb MB1N1-HBucoDvE-ABBcNVBAcMCk1vW1e21Ub24xEfAIB6NVBAcMD11vUFZpZVcxEzA
BgNVBAgMCkNhbG1mb3Ju 7rXF12N+Kz27Bd26frt5	aWExCZAJBgNVBAYTALVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQBAMIIBCgKCAQEArsgB5R9c9oK9s jmaiRk:B5j/C5o2HDXWOaPm+zZvE1cdjo1e5JVaOS+C/mzSckB19m+9QJf37H1+xht/
IHhw4E0mt1Z1Baf+YTv8 VjYkI5RirMFQWdnI9Cyd	VYyhiQA2noAgSMK/hdlibkMejlW/YNUk4HgZls5EBEt8NMB0J20cohKQVqgn/21NBqCIMr/ @NZfzy9KgCBG9xElbzdoEGK9rAZQy/cAiwv3ySxqSxjxDsywb4f3hLW6TRI+RzO6Dk0q60nsDg/
HQ@r/ 9RCvXjRSUyxcIHE61hne	0+b5cfvoHlnmIDt3IQ95keL1EpuLwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAgAxmWzDhNHK8tbA
v3Hu9khL5EXsnKceprze +TIg09m087BMai/t1315	<pre>6hzVB7D0PY3p9hqzC7luz1M3vM3BfLirGh2BEBq31FPj2MlLC+ibLDA1LrBtFEAKBrwL AoZzdCBaGddNr1RApTblwj1+5JRdJ1DlGKYXkWlxhfw 20k4z70cjanianianianianianianianianianianianiania</pre>
+6SyX77Lzzc/HgrpN4y- 	<pre>robuezenujngzj:5a90+bonzepishnvaskkm/ykzazownokueze52017H0skokk+lone01AwLueiy 7T043oyR8KrXdmifznQXbqhUvQLSuEcVe142reteLLt14GdX1UBh/410</pre>
<md:nameidformat>urn:oasis:nam <md:nameidformat>urn:oasis:nam</md:nameidformat></md:nameidformat>	<pre>wes:tc:SAML:1.1:nameid-format:emailAddress wes:tc:SAML:1.1:nameid-format:unspecified</pre>
<md:singlesignonservice bindin<br="">alt.auto.mobileiron.com/</md:singlesignonservice>	<pre>c="urn:oasis:names:tc:SAML_2.0:bindings:HTTP-POST" Location="https:/// /acc/786900bf-fcf8-4488-bb8d-815080e667e5/idp"/></pre>
<pre><md:singlesignonservice auto.mobileirp<="" bindin="" pre=""></md:singlesignonservice></pre>	g="urn:oasis:names:tc:SAML 2.0:bindings:HTTP-Redirect" Location=" <u>https://</u> n.com/acc/78690@bf-fcf8-4488-bb8d-8150800667e5/idp"/>
<pre> md:EntityDescriptor></pre>	
 urn:oasis:nam <md:nameidformat>urn:oasis:nam <md:singlesignonservice bindin<br="">alt.auto.mobileiron.com/ <md:singlesignonservice bindin<br="">auto.mobileiro md:EntityDescriptor></md:singlesignonservice></md:singlesignonservice></md:nameidformat>	<pre>es:tc:SAML:1.1:nameid-format:emailAddress es:tc:SAML:1.1:nameid-format:unspecified o="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POSI" Location="https:// /acc/786900bf-fcf8-4488-bb8d-815080e667e5/idp"/> g="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https:// n.com/ facc/7869005bf-fcf8-4488-bb8d-815080e667e5/idp"/></pre>

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

For SAML based SSO:			
O SAML v1.1 SSO	SAML v2 SSO		
SAML Asserting Parties(IdP)	~		
Delete the asserting party Update the assertin	g party		
SAML User Column			Leave this field empty if SAML user column is not used.
SAML Asserting Party Name		MobileIron	This is an identifier for your SAML issuer and cannot be modified
		later.	
SAML Issuer		https:// a/t.auto.mobileiron.com/* acc/dad0e	
Company Phone]
Contact Name]
Contact Phone			1
Relying Party Description			1
Require Mandatory Signature		Assertion	
Enable SAML Flag		Enabled V	
Login Request Signature(SF Generated/SP/RP):		No V	
SAML Profile		Browser/Post Profile 🗸 🗸	
Enforce Certificate Valid Period		No 🗸	
SAML Verifying Certificate Valid Period		04/21/2017 - 04/14/2047	
SAML Verifying Certificate Status		Certificate is valid.	
SAML Verifying Certificate			
BEGIN CENTIFICATE MIII Das CCALO (April Hägi (FANG) 3 jiló Vorgy (7K EEAOBANYBANBEINI CHBVCngx) 25 KABANYB XXCHEZARBANYBAB(CHMBIGA) LUBANKUZI LIN CCLI VINI BOTI (JOŻA KAF / MORNINACHOU LO BANYBANYTAL VTMI IBJ (ANFILICAN) 40 KAF DIAK JILK JAKG (2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKG (2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAK JILK JAKE 2010) 9 KAF (AN JOHNACHOU LO DIAKE	D2ThvcNAQELBQAwdrEUMBIGAIUEAvwLU2 comckivimisEUJyb2ArFjAUEBgVVBAcMDU AufbynVBATHJVTMB4XDFSJDCybTyMFJAME IIIEGDYSTAUTHUTMB4XDFSJDCybTyMFJAME IIIEGDYSTAUTHUTMB4XDFSJDCybTyMFJAME SFYNIIIFSJDCXCE2AFBBJVDASMEINICHTVCA9 SFWDib5DXCE2AFBBJVDAGCAGLHmtFVCA9 SFWDib5DXSTXEXCEAFBJVDGJCymCFF35E55 SFWDib5DXSTXEXCEAFBJVDGJCAFBJS25E55 SFWDib5DXSTXEXCEAFBJVDGJCAFBJS25E55 SFWDib5DXSTXEXCEAFBJVDGJCAFBJS25E55	InbeluSONIcnQX IndBSONILIFEp QXESARBQNVBACM InbJuyBECKAJ ootki2ELDEBZERq QVVeNJOVFEvuc TIQGMULIENTKI3D Zarboic/TIJALe	



SAML v2 : SP-initiated logout	
Support SP-initiated Global Logout	Yes V
SP sign LogoutRequest	No 🗸
SP validate LogoutResponse	No 🗸
Global Logout Service URL (LogoutRequest destination)	https:// -alt.auto.mobileiron.com/ /acc/dad0e42a

SAML V2 : IDP-initiated Global Logout			
SP validate LogoutRequest signature	Yes 🗸		
SP sign LogoutResponse	Yes 🗸		
Global Logout Service URL (LogoutResponse destination)	https://	-alt.auto.mobileiron.com/	/acc/dad0e42a

SAML v2: Login Response with Http artifact binding

Artifact Resolution Service Location (supplied by idp):	
Require ArtifactResolve Signature (sp to idp) Require ArtifactResponse Signature (idp to sp)	

SAML v2: NameID Setting

Require sp must encrypt all NameID elements	No 💙
NameID Format	unspecified V

SAML v2 : SP-initiated login

Enable sp initiated login (AuthnRequest)	Yes 🗸		
Default issuer	\checkmark		
single sign on redirect service location (to be provided by idp)	https://c	·alt.auto.mobileiron.com/	/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 models. The following models do not support SAML SSO flow.

- 1. Activation Code
- 2. QR Code

Profile	Activation	Help
Acti	vation	
Please activate your p the activation method	profile by selecting s below:	g one of
Use Acti	vation Code	
Scan	QR Code	
Try	Demo	

- 3. Email based Activation: This model must be used to use Access with the SuccessFactors mobile application.
 - 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.
 Note: The Access Sentry URL must be added in the Safari domain configuration for Tunnel profile.

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.