

AirWatch SAML Integration

Setting Up SAML 2.0 Integration with a Service Provider and an Identity Provider for AirWatch

Note: This document contains instructions on other software vendors' solutions, and was last updated for accuracy June 2017. Please contact the specific vendor if you have questions about the accuracy of the integration steps in this document.

© 2017 VMware, Inc. All rights reserved.

This document, as well as the software described in it, is furnished under license. The information in this manual may only be used in accordance with the terms of the license. This document should not be reproduced, stored or transmitted in any form, except as permitted by the license or by the express permission of AirWatch, LLC.

All other marks and names mentioned herein may be trademarks or trade names of their respective companies.

Contents

Introduction to the SAML Integration Guide.....	3
In This Guide	3
Before You Begin	4
Requirements.....	4
Recommended Reading.....	4
Getting Started.....	4
Configuring SAML	6
Overview	6
SAML Authentication without LDAP Integration	6
SAML Authentication with LDAP Integration.....	13
Authenticating Using SAML.....	19
Overview	19
Logging into the Console as an Administrator.....	19
Enrolling a Device as an End User	20
Appendix A — Explaining Binding Types	22
Overview	22
Request and Response Flows.....	22
Selecting a Binding Type	23
Appendix B — SAML Flow Diagrams	24
Overview	24
Appendix C — Locating a Group ID	27
Appendix D — Specifying a Post-Authentication Landing Page.....	27
Appendix E — Sample XML.....	27
Appendix F — Testing and Troubleshooting	28
Overview	28
Verifying the Service Provider and the IdP are Connected	28
AirWatch Errors.....	28
PingFederate Errors	31
SiteMinder Errors.....	33

Introduction to the SAML Integration Guide

The Single-Sign-On (SSO) architecture and federated authentication help provide higher levels of security and reduce the number of IDs and passwords users need to remember. As a result, AirWatch never sees a user's password because it is shared only between the user's device and their Identity Provider (IdP).

Security Assertion Markup Language (SAML) version 2.0 is a cross-domain, XML-based protocol that enables user-level authentication using an SSO ID across web applications. SAML leverages an IdP server to manage user identities, attributes, and entitlements and ultimately grant access to enterprise applications and information with a single user ID and password. The user's position in the organization can determine their level of access to enterprise applications and information.

AirWatch supports Active Directory (AD), Lotus Domino, Novell e-Directory, or any other directory service that uses Lightweight Directory Access Protocol (LDAP) integration for user groups and user attributes for SAML-authenticated users. AirWatch administrators have the option of authenticating device users with SAML 2.0 instead of authenticating directly with their directory service. Administrators also have the ability to define whether attribute mapping or directory services retrieves and synchronizes user information from the SAML response. This allows granular control by enabling administrators to disable directory services integration at lower Organization Group (OG) levels while maintaining directory services at higher OG levels.

IdPs generally do not support all Request and Response binding types. AirWatch provides support for all of the most current Request and Response binding types in both directions to give administrators the flexibility to integrate with all IdPs.

SAML authentication is available during enrollment or as an option for accessing the Self-Service Portal (SSP). When AirWatch enables SAML authentication, and after the user enters their AirWatch Group ID, the user is redirected to the SSO user interface for authentication.

In This Guide

- [Before You Begin](#) – This section covers topics and prerequisites you should familiarize yourself with so you can get the most out of using this guide.
- [Configuring SAML](#) – This section details configuring SAML with or without LDAP integration.
- [Authenticating Using SAML](#) – This section explains how to enable end-user enrollment and Self Service Portal authentication.
- [Appendix A – Explaining Binding Types](#) – This section provides more detail about the binding types that AirWatch supports.
- [Appendix B – SAML Flow Diagrams](#) – This section illustrates the various requests and response binding types AirWatch supports.
- [Appendix C – Locating a Group ID](#) – This section gives brief instructions on how to find an AirWatch Group ID for an Organization Group.
- [Appendix D – Sample XML](#) – This section gives an example of XML code.
- [Appendix E – Testing and Troubleshooting](#) – This section lists various issues and errors you may encounter and proposed resolutions for each.

Before You Begin

This section covers topics and prerequisites you should familiarize yourself with so you can get the most out of using this guide.

Requirements

Before performing this installation, ensure the IdP's metadata is available to you. Your IdP should have provided it to you. You will need to import your IdP's metadata in [Acquiring and Importing the IdP's Metadata into the AirWatch Admin Console](#). Know the AirWatch GroupID that is used for SAML. For information on how to locate your GroupID, see [Appendix C —Locating a GroupID](#).

End-users utilizing SAML authentication are considered Directory users even if you select to integrate SAML without LDAP. SAML authentication does not work if you only enable **Basic** user enrollment. To ensure SAML integration is successful, navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment**, select the **Directory** checkbox under **Authentication Mode(s)**, and then click **Save**.

Recommended Reading

- [AirWatch Configuring ADFS for SAML Integration](#) – This guide includes detailed instructions on how to configure ADFS for SAML integration with AirWatch.

Getting Started

IdP Considerations

There are several different SAML IdP software options available. AirWatch leverages SAML functionality by adhering to the defined SAML 2.0 standard protocols. Accordingly, the directions in this document make certain assumptions about the SAML IdP while interfacing with the AirWatch SAML functionality.

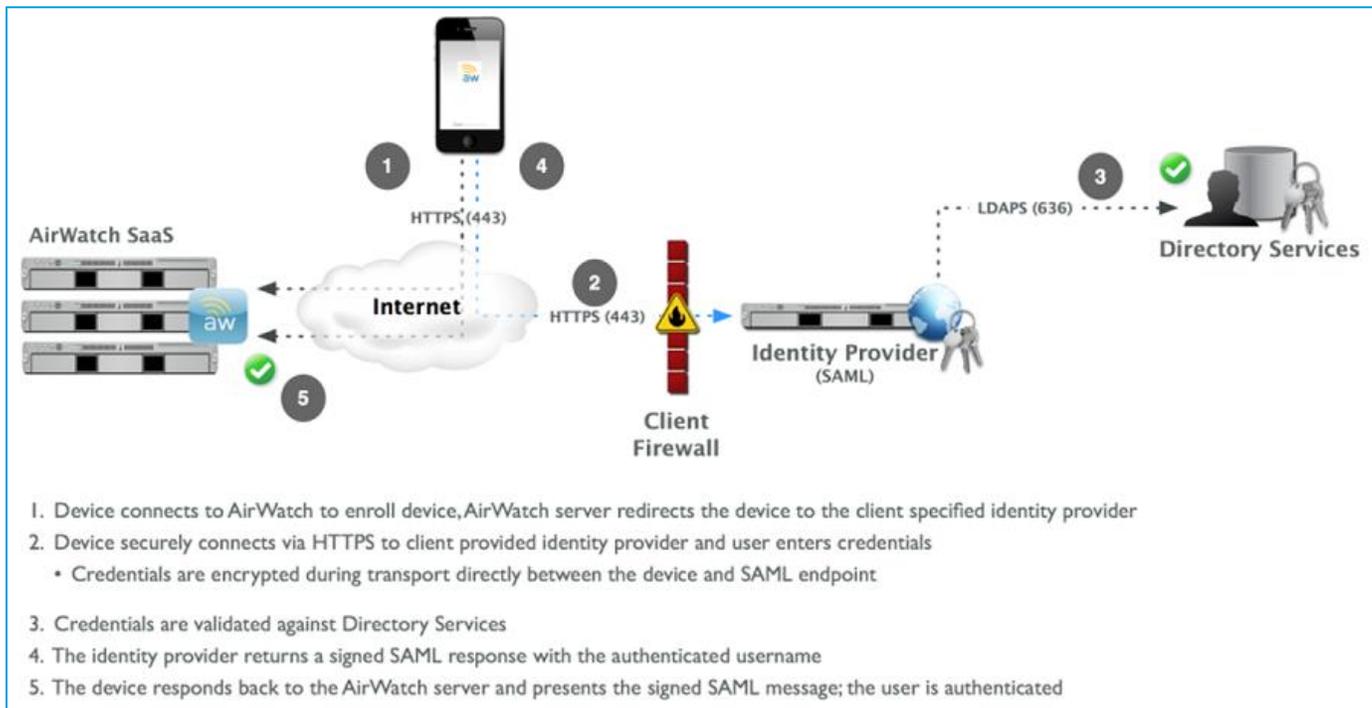
- If the IdP software requires additional setup outside of the standard protocol information provided by AirWatch, it may be necessary to perform some manual configuration with the IdP.
- Not all IdPs load and export settings the same way. Consult the IdP's documentation and/or support for recommendations.
- Not all IdPs are able to provide support for all Request and Response binding types or combinations of these binding types in both directions. Consult the IdP's documentation and/or support to verify the binding type you intend to select in the AirWatch Admin Console is supported by the IdP.

High-Level Overview

To use SAML for authentication you need to set up a trust between the Service Provider (AirWatch) and the IdP. Below is a high-level overview of this procedure.

- Enable SAML authentication.
 - Using SAML authentication with an LDAP directory service (e.g., AD) for only SAML authentication while relying on LDAP directory services for user enrollment.
 - Using SAML authentication without an LDAP directory service for SAML authentication and user enrollment.
- Configure the Service Provider (AirWatch) to authenticate with the IdP.
 - Acquiring and importing the IdP's metadata into the AirWatch Admin Console.
 - Selecting the Service Provider and IdP binding types.
 - Verifying the certificates being used by the IdP and Service Provider.
 - Testing and saving the Service Provider's SAML configuration.
- Create a trust between the Service Provider (AirWatch) and IdP.
 - Exporting the Service Provider's metadata from the AirWatch Admin Console into XML file format for the IdP.
 - Importing the Service Provider's metadata into the IdP.
- Login to the Console as an Administrator.
- Enroll devices using SAML.

SAML SaaS Process Flow



Configuring SAML

Overview

You can use SAML for authentication while retaining the role of your LDAP directory service for looking up user information needed for device enrollment. On the other hand, you can also eliminate the need for a direct AirWatch connection to your LDAP directory service and allow SAML to authenticate and enroll devices.

- **SAML Authentication without LDAP Integration** –This approach allows for federated authentication with the ability to accept SAML mappings from your corporate IdP.
- **SAML Authentication with LDAP Integration** –This approach allows for AirWatch to sync additional attributes and User Group membership for your corporate users that are authenticated against your corporate IdP.

The topics that follow discuss each scenario. Choose which scenario is best for your configuration and skip the other section.

SAML Authentication without LDAP Integration

This configuration allows you to securely authenticate users and retrieve user attributes from your LDAP directory service without requiring the AirWatch Cloud Connector (ACC) to facilitate communication to your corporate backend systems.

To enable SAML authentication without LDAP Integration, navigate to **Directory Services** in the AirWatch Admin Console and override the use of the LDAP directory service (e.g., AD) so that SAML provides device authentication and enrollment. To do this, complete the following steps.

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.
2. Select the **Directory Type** drop-down in **LDAP** and select **None**.

Note: If you want to disable the LDAP directory service (e.g., AD) for enrollment at a particular Organization Group (OG) and below, go to the highest OG level you want to disable and then select 'None' from **Directory Type**. That OG and all OGs below it (child) now use SAML for enrollment.

System / Enterprise Integration / Directory Services

Server User

Current Setting Inherit Override

LDAP

Directory Type * None

Server * YOUR.ADSERVER.URL

Encryption Type * None SSL Start TLS

Port * 10

Protocol Version * 3

Use Service Account Credentials Enabled Disabled

Bind Authentication Type * Anonymous Basic Digest Kerberos NTLM GSS-NEGOTIATE

Bind Username awsso\svcLDAPdev

Clear Bind Password

Bind Password

Domain Server

awsso airwatch.sso

+ Add Domain

ADVANCED

Use Azure AD for Identity Services

Use SAML For Authentication Enabled Disabled

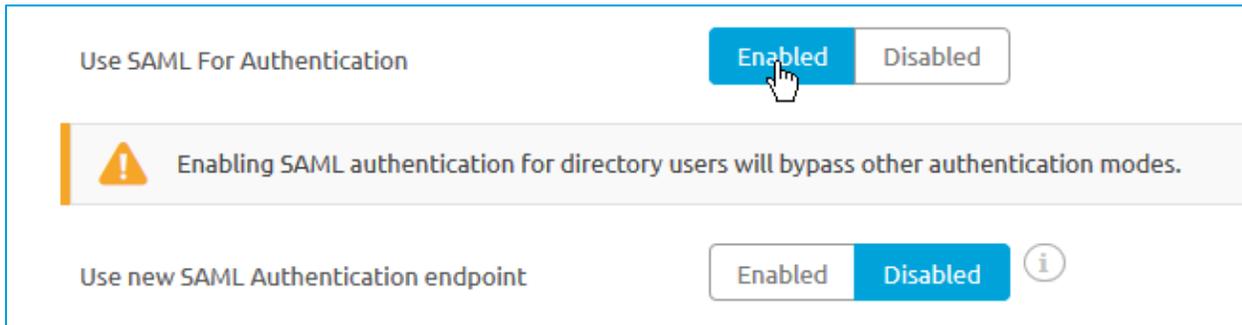
Child Permission Inherit Override Inherit or Override

Save Launch Setup Wizard

By selecting 'None' in Directory Type, the LDAP directory service (e.g., Lotus Domino) no longer performs enrollment. Your LDAP directory service only provides the IdP with information about the end-user so the user can enroll their device.

3. Select the **Use SAML For Authentication** option. An enable SAML authentication message appears.

Note: By selecting the option above, the IdP performs authentication, rather than by your LDAP service (e.g., Novell e-Directory). The screen above demonstrates using the IdP for enrollment and SAML for authentication.



Label	Definition
Use SAML for Authentication	Enable this option to use SAML to authenticate devices. This option displays all the dropdowns, fields, and radio buttons on the following page for configuring SAML to authenticate devices.
Use new SAML Authentication endpoint	<p>A new SAML authentication endpoint has been created for end-user authentication (device enrollment and login to SSP), to replace the dedicated enrollment and SSP endpoints. While you may choose to keep your existing settings, AirWatch recommends updating your SAML settings to take advantage of the new endpoint.</p> <p>If you would like to make use of the new endpoint, please enable the Use new SAML Authentication endpoint field, save the page, and then use the Export Service Provider Settings button below to export the new metadata file and upload it to your IdP. Doing so will establish trust between the new endpoint and your IdP.</p>

Configuring the Service Provider to Authenticate with the IdP

Now that you have selected SAML as the authentication method, you need to configure AirWatch to use SAML to communicate with your IdP by making selections using the **Directory Services** page.

SAML 2.0

Import Identity Provider Settings

 To load the imported settings, click save. Any changes made to the form will be lost.

Service Provider (AirWatch) ID

Identity Provider ID

 Enabling SAML authentication for directory users will bypass other authentication modes.

Request

Request Binding Type Redirect POST Artifact

Identity Provider Single Sign-On Url

NameID Format*

Authentication Request Security*

Response

Response Binding Type Redirect POST Artifact

Sp Assertion Url

Authentication Response Security*

Certificate

Identity Provider Certificate

Service Provider (AirWatch) Certificate

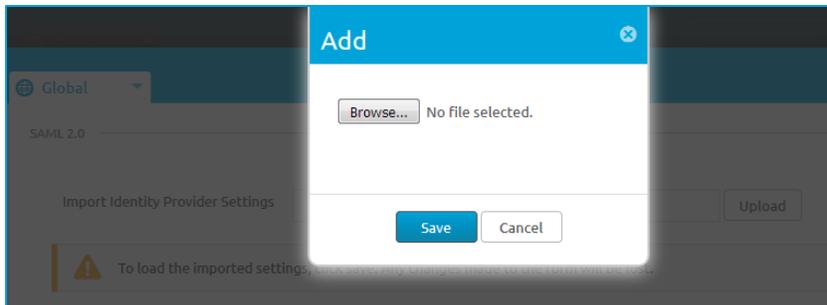
Label	Definition
SAML 2.0	
Import Identity Provider Settings	Select the Upload button to import the SAML metadata (identity certificate) obtained from the IdP. This is in XML format.
Service Provider (AirWatch) ID	Enter the Uniform Resource Identifier (URI) with which AirWatch identifies itself to the identity provider. This string must match the ID that has been established as trusted by the identity provider.
Identity Provider ID	Enter the URI that the identity provider uses to identify itself. AirWatch checks authentication responses to verify that the identity matches the ID provided here.

REQUEST	
Request Binding Type	Select one of the Request Binding Types for the request. The options include Redirect, POST, and Artifact .
Identity Provider Single Sign On Url	Enter the IdP's URL that the Service Provider (AirWatch) uses to send requests.
NameID Format	Select from the drop-down the format the IdP uses to send a NameID for an authenticated user. You can select Unspecified, Transient Identifier, Persistent Identifier, Entity Identifier, Email Address, X509 Subject Name, Kerberos, or Windows Domain Qualified Name . This selection is not required (Unspecified) since the Service Provider (AirWatch) obtains the username from the FriendlyName UID required attribute.
Authentication Request Security	Select from the dropdown whether or not the Service Provider (AirWatch) signs the authentication requests. You can select None, Sign Authentication Requests (SHA1), and Sign Authentication Requests (SHA256) .
RESPONSE	
Response Binding Type	Select one of the Response Binding Types for the response. The options include Redirect, POST, and Artifact .
Sp Assertion Url	This value specifies the AirWatch URL that is configured by the identity provider to direct its authentication responses. Assertions regarding the authenticated user are included in success responses from the IdP.
Authentication Response Security	This value specifies whether the IdP signs the response. You can select between None, Validate Response Signatures, and Validate Assertions Signatures . Consider selecting Validate Response Signatures for a more secure authentication.
CERTIFICATE	
Identity Provider Certificate	Click Upload to install the IdP's certificate on the AirWatch server. Select Clear or Change to upload a new certificate that replaces the existing one.
Service Provider (AirWatch) Certificate	Click Upload to install the service provider's (AirWatch) certificate on the AirWatch server. Select Clear or Change to upload a new certificate that replaces the existing one.
Export Service Provider Settings (button)	Select this button to export the metadata file for uploading to your IdP. Doing so will establish trust between the new SAML endpoint (for enrollment and SSP login) and your IdP.

Acquiring and Importing the IdP's Metadata into the AirWatch Admin Console

First, you need to acquire the metadata your IdP sent you, and then import it into the AirWatch Admin Console.

1. In the **Import Identity Provider Settings** field, located in the **SAML 2.0** subsection, select the **Upload** button. The **Add** dialog box appears.



2. Select **Browse...** to navigate to the metadata XML file exported from your IdP and provided to you. The IdP file you upload is SAML metadata used as a descriptor for the IdP side of the communications. This file is in XML format and contains information such as, entityId, optional certificate, URLs it listens on, formats it accepts, etc.
3. Select **Save**. The metadata in the XML file automatically populates fields on an internal form. The user cannot view this form. The information is retained for when you click Export Service Provider Settings to export SAML metadata for the IdP in XML format, which you will do later in this guide. For more information, see [Exporting the Service Provider's Metadata from the AirWatch Admin Console](#).

Selecting the Service Provider and IdP Binding Types

Next, you need to select the proper binding type protocol so the Service Provider (AirWatch) and your IdP use the correct matching protocol. The protocol you choose can be any combination of the three supported by AirWatch. The following is an example of a **Request Redirect** along with a **Response POST**.

If you do not know which binding type protocol is best to use for your environment, ask your IdP before continuing in order to ensure a seamless installation. You can find additional information about the various binding types both AirWatch and your IdP support in [Appendix A —Explaining Binding Types](#).

REQUEST	
Request Binding Type	<input checked="" type="radio"/> Redirect <input type="radio"/> POST <input type="radio"/> Artifact
Identity Provider Single Sign On Url	https://[redacted]/SAML2/Redirect/SSO
NameID Format *	Email Address
Authentication Request Security *	Sign Authentication Requests (SHA256)

RESPONSE	
Response Binding Type	<input type="radio"/> Redirect <input checked="" type="radio"/> POST <input type="radio"/> Artifact
Sp Assertion Url	~/SAML/AssertionService.ashx?binding=HttpPost
Authentication Response Security *	Validate response signatures

Verifying the Certificates Being Used by the IdP and Service Provider

You can view and verify the IdP and Service Provider (AirWatch) certificates.

- Select the **Change** button if you want your IdP to use a different certificate.
- Select the **Clear** button to delete the current IdP certificate.
- Select the **Upload** button to upload a new certificate from the Service Provider.

CERTIFICATE

Identity Provider Certificate Certificate Uploaded

Type Cert

Issued to CN=ipfedel.airwatchportal.com

Issued by CN=ipfedel.airwatchportal.com

Valid From 9/29/2011

Valid To 9/29/2031

Thumbprint 288F7119D2A182C7048D83F28A23A8C38471102F

Service Provider (AirWatch) Certificate

Creating a Trust between the Service Provider and IdP

Now that you have loaded the IdP metadata into the Service Provider's (AirWatch) Admin Console and configured the Service Provider's portion of the configuration, you need to export the Service Provider's metadata so the IdP can import it into their system. This completes the trust between the IdP and Service Provider, which allows SAML to authenticate device users.

Exporting the Service Provider's Metadata from the AirWatch Admin Console

Export, save, and view the Service Provider's metadata.

1. Select the **Export Service Provider Settings** button at the bottom of the screen. A series of dialog boxes appear.
2. Click **Save** and store the XML file to a location that is easy to find (e.g., Desktop). To view an example of the XML, see [Appendix E – Sample XML](#).

Importing the Service Provider's Metadata into the IdP

For the IdP to work properly with the Service Provider (AirWatch), the IdP needs to import the Service Provider's metadata. This is similar to the procedure you completed earlier in this document in which you imported the IdP's metadata into the Service Provider's Admin Console. The procedure will vary among the different IdPs, but the basic steps should be similar to the following.

1. Contact your IdP to find out the exact procedure for sending them the Service Provider metadata XML file.
2. Send your IdP the Service Provider metadata XML file that you exported from the AirWatch Admin Console.

- After you receive confirmation that your IdP imported the Service Provider metadata XML file, proceed to the next section to test.
- Click the **User** tab. The user **Attributes** and **Mapping Values** display.

System / Enterprise Integration / Directory Services

Server
User

Current Setting Inherit Override

Domain Base DN*

awsso DC=airwatch,DC=sso +

User Object Class * i

person

User Search Filter * i

(&(objectCategory=person)(sAMAccountName={EnrollmentUser})

ADVANCED

Enable Custom Attributes
Enabled
Disabled

Attribute	Mapping Value
Object Identifier	objectGUID ✎ ↻
Username	sAMAccountName ✎ ↻
Member Of	memberOf ✎ ↻
Full Name	fullName ✎ ↻
Display Name	displayName ✎ ↻
First Name	givenName ✎ ↻
Middle Name	middleName ✎ ↻
Last Name	sn ✎ ↻

- Click to edit or to sync each **Mapping Value**.
- Click **Save**. SAML now performs authentication and enrollment.

Label	Definition
Attributes	Required field change: Username mapping value of sAMAccountName may need to be changed to uid depending on your IdP.

SAML Authentication with LDAP Integration

This approach allows for Federated Authentication with the ability to accept SAML mappings from your corporate IdP. To enable SAML and integrate authentication with your LDAP directory service (e.g., AD), navigate to **Directory Services** in the AirWatch Admin Console and override the sole use of your LDAP directory service by selecting SAML. This enables SAML for authentication and uses your LDAP directory service (e.g., AD) connection for user enrollment.

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services** and select the **Server** tab.
2. Verify the correct **LDAP** directory services (e.g., AD) is selected. If not, select the correct LDAP directory services you want to integrate with SAML.

System / Enterprise Integration / Directory Services

Server
User
Group

Current Setting Inherit Override

LDAP

Directory Type * (i)

Server * (i)

Encryption Type * (i)
None
SSL
Start TLS

Port * (i)

Protocol Version * (i)

Use Service Account Credentials (i)
Enabled
Disabled

Bind Authentication Type * (i)
Anonymous
Basic
Digest
Kerberos
NTLM
GSS-NEGOTIATE

Bind Username (i)

Clear Bind Password (i)

Bind Password (i)

Domain

Add Domain

Server

Use Azure AD for Identity Services

Use SAML For Authentication (i)
Enabled
Disabled

Child Permission Inherit Override Inherit or Override

Save
Test Connection
Launch Setup Wizard

Label	Definition
Directory Type	Select the type of directory service your organization uses. You can select Active Directory , Lotus Domino , or Novell e-Directory , Other LDAP , or None .
Server	Enter the address of your domain controller.
Encryption Type	Select the type of encryption to use for directory services communication. You can select None , SSL , or Start TLS .
Port	Enter the TCP port used to communicate with the domain controller. The default for unencrypted LDAP directory service communication is port 389. Only SaaS environments allow SSL encrypted traffic using port 636. To view a KnowledgeBase article that lists the most up-to-date AirWatch SaaS data center IP ranges, refer to https://support.air-watch.com/articles/115001662168 .
Verify SSL Certificate	Select the checkbox to receive SSL errors when the Encryption Type is None .

Protocol Version	Select the version of the LDAP directory service (e.g., AD) protocol that is in use. You can select 1 , 2 , or 3 . Active Directory (AD) uses LDAP versions 2 or 3. If you are unsure of which Protocol Version to select, try the commonly used value of 3. You will know if your selection is not correct when you click Test Connection .
Use Service Account Credentials	Use the credentials from the App pool of the server on which EIS or MAG is installed for authenticating with the domain controller. Enabling this option hides the Bind Username and Bind Password fields.
Bind Authentication Type	Select the type of bind authentication to enable the AirWatch server to communicate with the domain controller. You can select Anonymous , Basic , Digest , Kerberos , NTLM , or GSS-NEGOTIATE . If you are unsure of which Bind Authentication Type to use, try the commonly used GSS-NEGOTIATE . You will know if your selection is not correct when you click Test Connection .
Bind Username and Bind Password	Enter the credentials used to authenticate with the domain controller. This account allows read-access permission on your LDAP directory service (e.g., AD) and binds the connection when authenticating the users.
Clear Bind Password	Select the checkbox to clear the bind password from the domain controller database.
Domain/Server	Enter the default domain and server name for any directory-based user accounts. You can add additional domains by selecting the Add Domain option. In this case, AirWatch will automatically change the Port setting to 3268 for global catalog. You may choose to change this to 3269 for SSL encrypted traffic, or override it completely by entering a separate port.

3. You may optionally select and expand the **Advanced** section.

▼ ADVANCED

Search Subdomains Enabled Disabled ⓘ

Connection Timeout * ⓘ

Request timeout * ⓘ

Search without base DN Enabled Disabled ⓘ

Use Recursive OID at Enrollment Enabled Disabled ⓘ

Use Recursive OID For Group Sync Enabled Disabled ⓘ

Object Identifier Data Type * Binary String ⓘ

Sort Control Enabled Disabled ⓘ

Label	Definition
Search Subdomains	Select to enable subdomain searching to find nested users. Leaving this setting Disabled can make searches faster and avoid potential network issues, but users and groups located in subdomains under the base DN will not be identified.
Connection Timeout	Enter the LDAP connection timeout value (in seconds).
Request Timeout	Enter the LDAP query request timeout value (in seconds).

Search without base DN	Enable this option when using a global catalog and do not want to require a base DN to search for users and groups.
Use Recursive OID at Enrollment	Enable this option to task the server to verify user group membership at the time of enrollment. Since this feature executes by the system at the time you enroll, your performance may decrease with some directories.
Use Recursive OID For Group Sync	Enable this option to task the server to verify user group membership at the time of Group synchronization.
Object Identifier Data Type	Select the unique identifier that will never change for a user or group. The options available are Binary and String. Typically, the Object Identifier is in Binary format.
Sort Control	Option to enable sorting. Leaving this option disabled can make searches faster and avoid sync timeouts.

4. Click the **User** tab. The user **Attributes** and **Mapping Values** display.

System / Enterprise Integration / Directory Services

Server **User** Group

Current Setting Inherit Override

Domain ACMECORP Base DN* DC=airwatch,DC=sso +

User Object Class * user ⓘ

User Search Filter * (&(objectCategory=person)(sAMAccountName={EnrollmentUser}) ⓘ

ADVANCED

Auto Merge Enabled Disabled

Automatically Set Disabled Users To Inactive Enabled Disabled

Value For Disabled Status 2 Flag Bit Match ⓘ

Enable Custom Attributes Enabled Disabled

Attribute	Mapping Value
Object Identifier	objectGUID
Username	sAMAccountName
Member Of	memberOf

5. Select the **Advanced** drop-down to display additional settings as shown in the table below.

Label	Definition
User Object Class	Enter the appropriate Object Class. In most cases, the value to enter in this field is user .
User Search Filter	Enter the search parameter used to associate user accounts with Active Directory (AD) accounts. The recommended format is "<LDAPUserIdentifier>={EnrollmentUser}" where <LDAPUserIdentifier> is the parameter used on the directory services server to identify the specific user. <ul style="list-style-type: none"> For AD servers, use "sAMAccountName={EnrollmentUser}" For LDAP servers, use "CN={EnrollmentUser}" or "UID={EnrollmentUser}"

Auto Merge	Enable to allow user group updates from your LDAP directory service (e.g., AD) to merge automatically with the associated users and groups in AirWatch.
Automatically Set Disabled Users to Inactive	Select Enable to deactivate the associated user in AirWatch if that user becomes disabled in your LDAP directory service (e.g., Novell e-Directory).
Value for Disabled Status	<p>This value determines the type of Lightweight Directory Access Protocol (LDAP) attribute used to represent a user's status.</p> <p>Select Flag Bit Match if a bitwise flag (which is the default for Active Directory) designates the user status. With "Flag Bit Match" selected, directory services will consider the user to be disabled if any bits from the property match the entered numeric value. This field will only be visible when the field Automatically Set Disabled Users to Inactive is checked.</p> <p>If you select this option, then AirWatch administrators set as inactive in your directory service will not be able to log into the AirWatch Admin Console. In addition, enrolled devices assigned to users who are set to inactive in your directory service will automatically be unenrolled.</p>
Enable Custom Attributes	Select to enable custom attributes and mapping values and to display fields at the bottom of the screen that allow you to define each custom attribute that can be mapped to Active Directory entities.
Attributes	Required field change: Username mapping value of sAMAccountName may need to be changed to uid depending on your IdP.

- Review and edit the **Mapping Values** for the listed **Attributes**, if necessary. These columns show the mapping between AirWatch user attributes (left) and your LDAP directory service attributes (right). By default, these attributes are values most commonly used in LDAP directory services. You should update these mapping values to reflect the values used by your LDAP directory service (e.g., Lotus Domino).
- Click  to enable or  to disable each **Mapping Value**.
 In some instances, global catalogs are used to manage multiple domains or LDAP directory service (e.g., AD) forests. If you experience delays when searching for or authenticating users, this may be due to a complex directory structure. For better performance, you can integrate directly with the global catalog to query multiple forests using one LDAP directory service endpoint. To do this, configure the following settings.
Encryption Type = None
Port = 3268
 Verify that your firewall allows for this traffic on port 3268.
- Select **Sync Attributes** to sync manually the attributes mapped in this screen to the user records in AirWatch.

Note: This automatically occurs each time a user is modified in your LDAP directory service (e.g., Novell e-Directory).

9. Click the **Group** tab. The group **Attributes** and **Mapping Values** display.

System / Enterprise Integration / Directory Services

Server
User
Group

Current Setting Inherit Override

Domain Base DN*

ACMECORP +

Group Object Class * (i)

Organizational Unit Object Class * (i)

▼ ADVANCED

Group Search Filter

Auto Sync Default Automatically add/remove users in User Groups based on membership in LDAP/AD

Auto Merge Default Automatically apply sync changes without administrative approval

Maximum Allowable Changes

Attribute	Mapping Value
Object Identifier	<input type="text" value="objectGUID"/> ✎ ↻
Name	<input type="text" value="name"/> ✎ ↻
Member	<input type="text" value="member"/> ✎ ↻
Common Name	<input type="text" value="cn"/> ✎ ↻
Member Of	<input type="text" value="memberOf"/> ✎ ↻
Distinguished Name	<input type="text" value="distinguishedName"/> ✎ ↻

10. Select **Show Advanced** to display additional settings as shown in the table below.

Label	Definition
Group Object Class	Enter the appropriate Object Class. In most cases, the value to enter in this field is group .
Organizational Unit Object Class	Enter the appropriate Organizational User Object Class.
Group Search Filter	Enter the search parameter used to associate user groups with your LDAP directory service (e.g., AD) accounts.
Auto Sync Default	Select this checkbox to automatically add or remove users in AirWatch configured user groups based on their membership in your LDAP directory service (e.g., Novell e-Directory).
Auto Merge Default	Select this checkbox to apply sync changes automatically without administrative approval.
Maximum Allowable Changes	Enter the maximum number of allowable group membership changes to be merged into AirWatch.

11. Review and edit the **Mapping Values** for the listed **Attributes**, if necessary. These columns show the mapping between AirWatch user attributes (left) and your LDAP directory service (e.g., AD) attributes (right). By default, these attributes are values most commonly used in LDAP directory services. You should update these mapping values to reflect the values used by your LDAP directory service.

12. Click  to enable or  to disable each **Mapping Value**.

In some instances, global catalogs are used to manage multiple domains or LDAP directory service (e.g., AD) forests. If you experience delays when searching for or authenticating users, this may be due to a complex directory structure. To increase performance, you can integrate directly with the global catalog to query multiple forests using one LDAP directory service endpoint. To do this, configure the following settings.

Encryption Type = None

Port = 3268

Verify that your firewall allows for this traffic on port 3268.

13. Click **Save**. SAML now performs the authentication while your LDAP directory service performs the enrollment.

Once these steps are complete, a trust between the Service Provider (AirWatch) and IdP is established, allowing SAML to authenticate the device users.

Authenticating Using SAML

Overview

Now that SAML is configured and working properly, you are ready to log in as an administrator to the AirWatch Management Console. Additional steps are required to enable end-user enrollment and Self Service Portal authentication. See [Enrolling a Device as an End User](#) below.

End-users utilizing SAML authentication are considered Directory users even if you select to integrate SAML without LDAP. SAML authentication does not work if you only enable Basic user enrollment. To ensure SAML integration is successful, navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment**, select the **Directory** checkbox under **Authentication Mode(s)**, and then click Save.

Logging into the Console as an Administrator

If you are an administrator of a group of user devices and you want to access the AirWatch Admin Console using SAML, you need to add a **?GID** and the SAML GroupID to the query string at the end of the URL that was provided to you.

This query string tells AirWatch to look up the OG you belong to and determines the proper SAML settings to use, thus making your admin login experience seamless by directing you to the correct OG in the AirWatch Admin Console. The following is an example of a typical URL with the additional **?GID** query string.

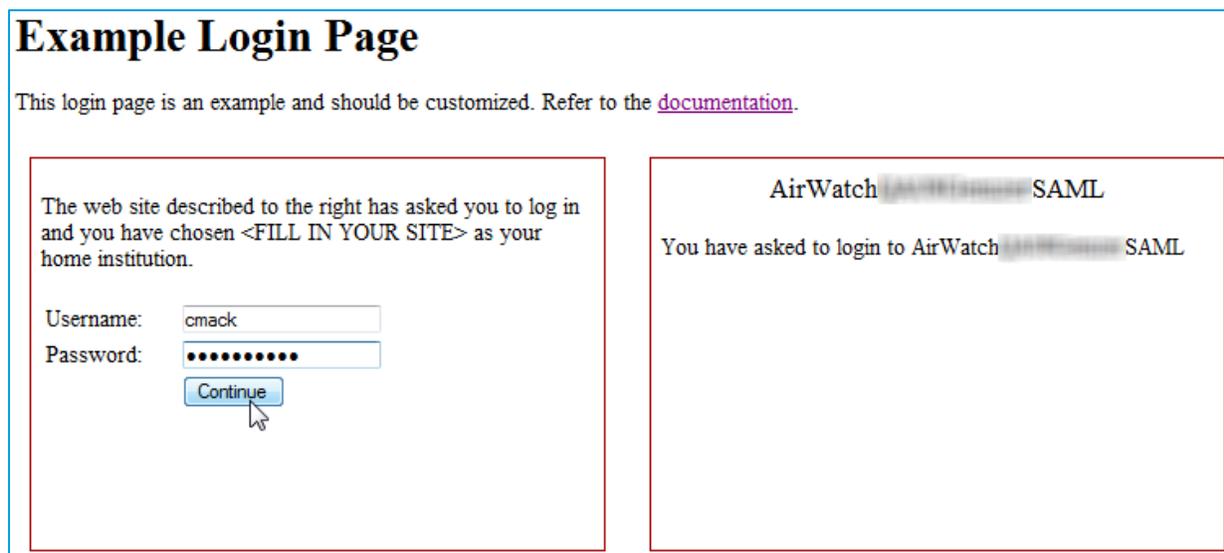
1. Locate the GroupID your company uses for SAML IdP authentication. For information on how to locate your GroupID, see [Appendix C —Locating a GroupID](#).
2. Enter in your browser the **AirWatch URL** provided to you followed by **?GID** plus your **GroupID**. The syntax is: <https://consoleURL/AirWatch/Login?GID=abc123>.

where *consoleURL* is the URL of your AirWatch server and *abc123* is your GroupID.

For example, <https://mdm.ACME.com/AirWatch/Login?GID=ACMEsaml>

You are directed to your IdP's login page.

The look of a SAML IdP login page differs between providers. For example:



3. Enter your corporate **Username** and **Password** credentials and then continue/accept.
4. Once authenticated by your IdP, you are redirected to the AirWatch management portal.

Enrolling a Device as an End User

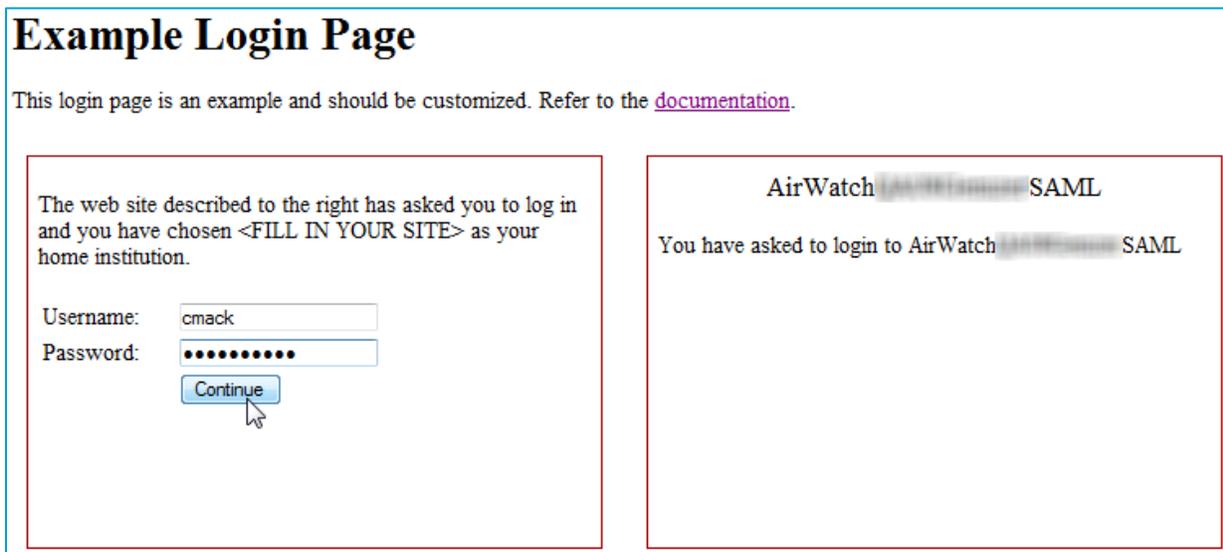
Before you can enroll an iOS, Android, or Windows Phone 8 device, you (or end-users) need the following.

- **Credentials** –This username and password allow you to access your AirWatch environment. Credentials might be the same as your network LDAP directory service password or may be uniquely defined in the AirWatch Admin Console.
- **Directory Authentication Mode enabled** - End-users utilizing SAML authentication are considered Directory users even if you select to integrate SAML without LDAP. SAML authentication does not work if you only enable **Basic** user enrollment. To ensure SAML integration is successful, navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment**, select the **Directory** checkbox under **Authentication Mode(s)**, and then click **Save**.

Enrollment Steps

1. **Enrollment URL** –This URL is unique to your organization's enrollment environment and advances you directly to the enrollment screen. For example, <https://mdm.acme.com/enroll>.
2. **Group ID** –This Group ID associates your device with your corporate role and is defined in the AirWatch Admin Console. For information on how to locate your GroupID, see [Appendix C —Locating a GroupID](#).
3. **SAML Logon Page** –Users are redirected to your SAML IdP's logon page.

The look of a SAML IdP login page differs between providers. For example:



4. **Credentials** –This username and password allow you to access your AirWatch environment. These credentials may be the same as your network LDAP directory service password or may be uniquely defined in the AirWatch Admin Console.
5. **MDM Installation Prompts** – Follow the remaining prompts to complete enrollment. At this time, you might be notified if your user account is not allowed or blocked because your account is blacklisted and not approved for enrollment.

Appendix A — Explaining Binding Types

Overview

The SAML screen allows you to choose the Request and Response binding types. The binding type is a protocol that specifies a selected set of bindings in sufficient detail. This ensures that all SAML software that conforms to the standard is able to interoperate when using standard messaging or communication binding type protocols.

AirWatch supports combinations of SAML Request and Response binding types that Identity Providers (IdPs) might require. Each of these binding types is bi-directional (request or response).

- Redirect
- Post
- Artifact

Request and Response Flows

Since each binding type can be a Request or Response, and you can combine any one of the Requests with any one of the Responses, the list below explains each binding type.

For flowcharts of the Redirect, Post, and Artifact binding types see [Appendix —SAML Flow Diagrams](#).

Request Binding Types

- Redirect:** The Service Provider (AirWatch) sends an HTTP 302 redirect to the user as a URL for authentication that contains a SAML request. The user's browser redirects to the IdP and prompts to log in.
- POST:** The Service Provider (AirWatch) sends an HTTP 200 message to the user that contains a form for authentication. The user's browser sends the form and SAML request to the IdP and prompts to log into the IdP.
- Artifact:** The user connects to the Service Provider (AirWatch) and then AirWatch sends a redirect to the user for authentication via SAML. The user's browser redirects to the IdP and prompts to log in. IdP requests the Service Provider to send an Artifact Resolution Service (token) directly to the IdP. The Service Provider returns the token to the IdP.

Response Binding Types

- Redirect:** The IdP packages a token identifier for authentication used by the Service Provider (AirWatch) and sends it to the user's browser. The user's browser delivers the token to the Service Provider to authenticate the user.
- POST:** The IdP packages the user's information and sends it to the user with a redirect to the Service Provider (AirWatch). The user redirects to the Service Provider and automatically authenticates with their credentials in its payload from the IdP.
- Artifact:** The IdP packages the user's information and sends it to the user with a redirect to the Service Provider (AirWatch). The user redirects to Service Provider and automatically authenticates with their credentials in its payload from the IdP. The Service Provider uses the token it received from the user's browser to communicate directly with the IdP. The IdP packages the user's information needed for authentication and sends it directly to the Service Provider.

Selecting a Binding Type

The table below shows the various Request and Responses for each SAML binding type. You can use any Request with any Response, although some IdPs do not support some of the binding types.

	Response —Redirect	Response —Post	Response —Artifact
Request —Redirect	Atypical	✓	✓
Request —Post	Atypical	✓	✓
Request —Artifact	Atypical	Atypical	Atypical

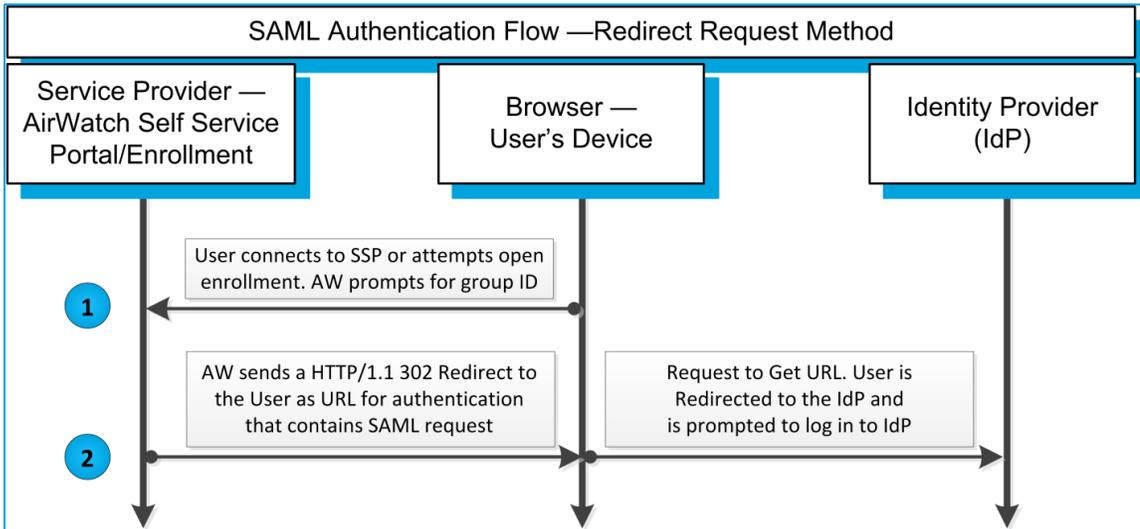
Most IdPs do not support all binding types. Make sure you check with the Identity Provider that you chose to make sure they support the Request and Response binding type you selected in the AirWatch Admin Console. If you choose a binding type your IdP does not support then SAML will not work properly.

Appendix B — SAML Flow Diagrams

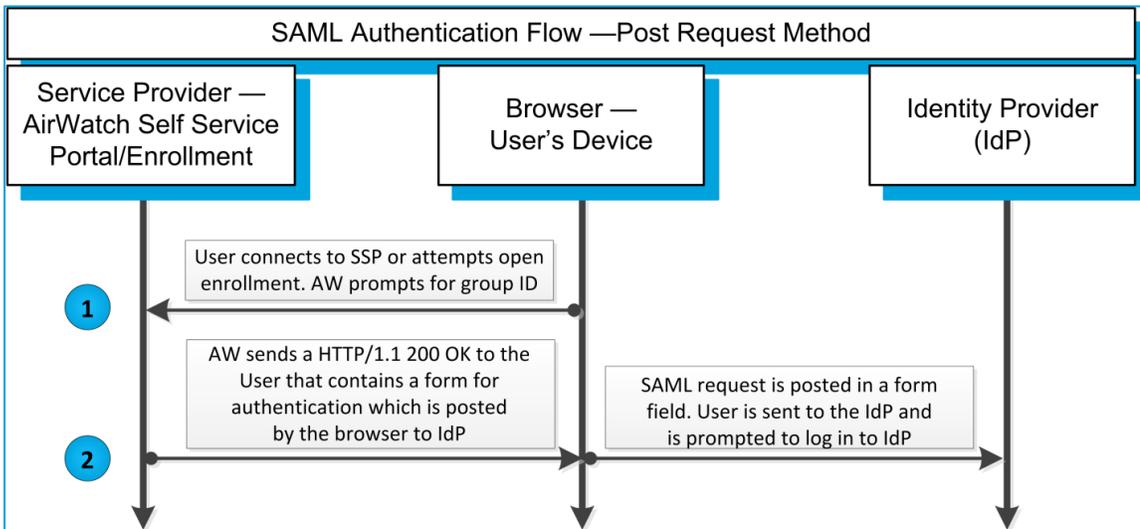
Overview

AirWatch supports any combination of SAML Request and Response binding types required by your IdP. The following are SAML flow diagrams for each Request and Response binding types.

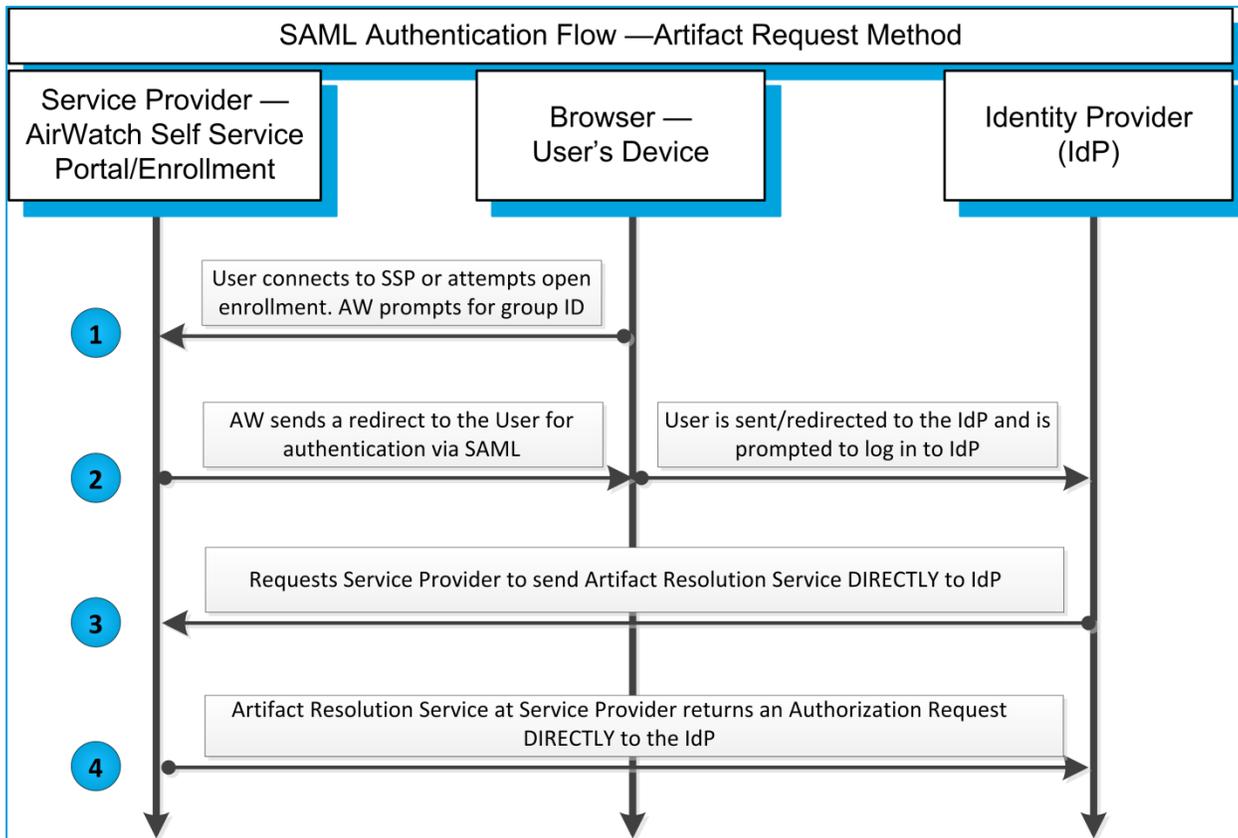
Request for Redirect



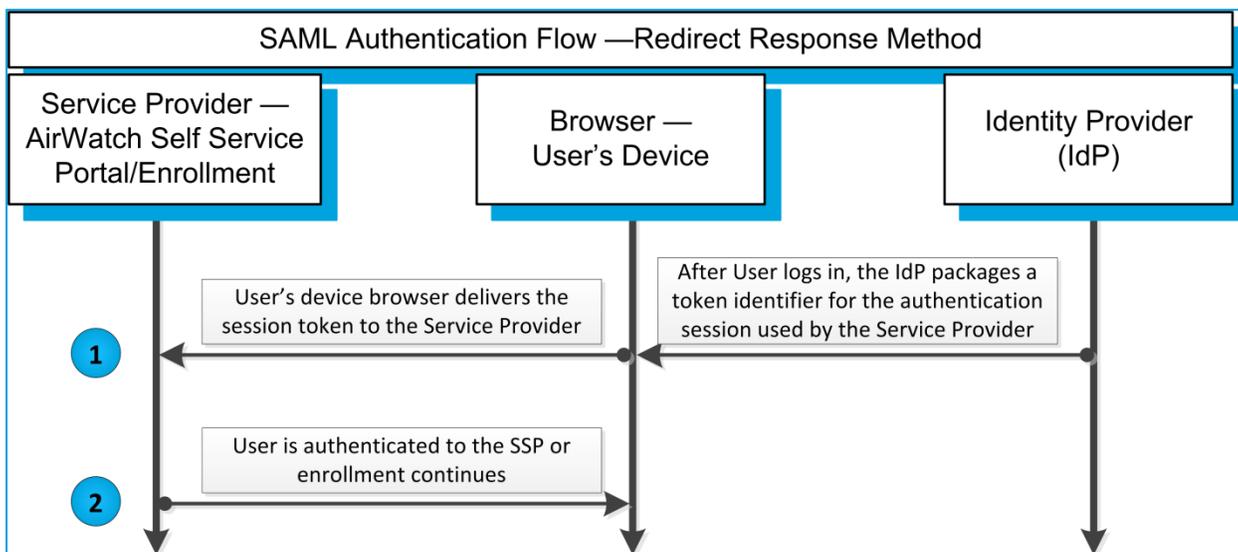
Request for Post



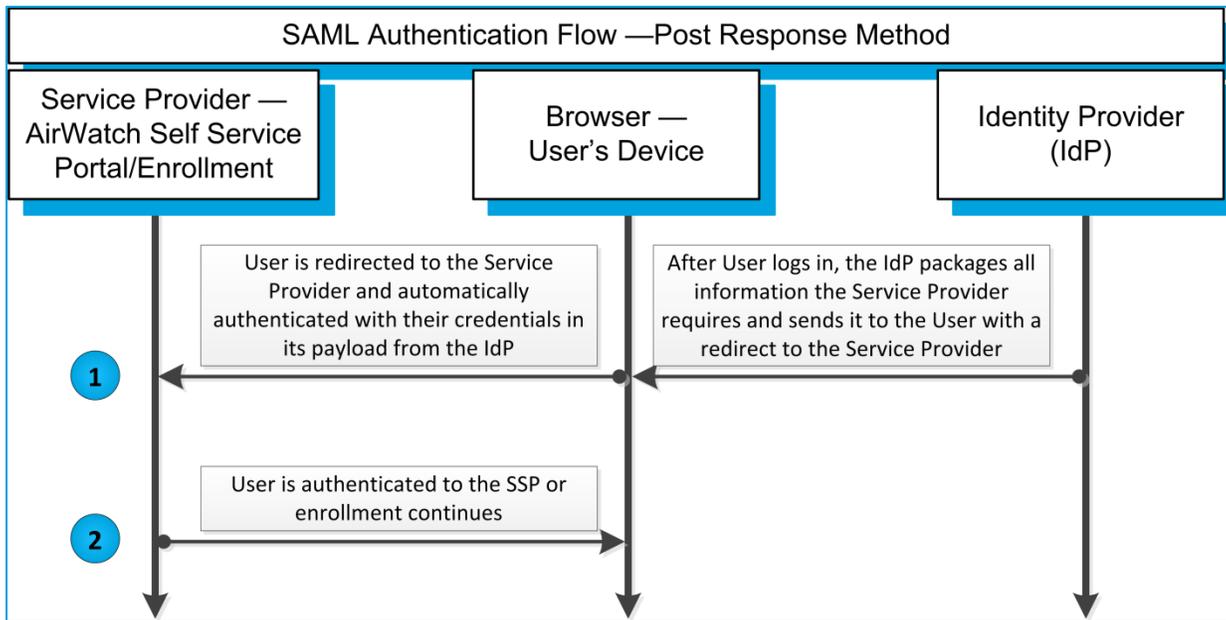
Request for Artifact



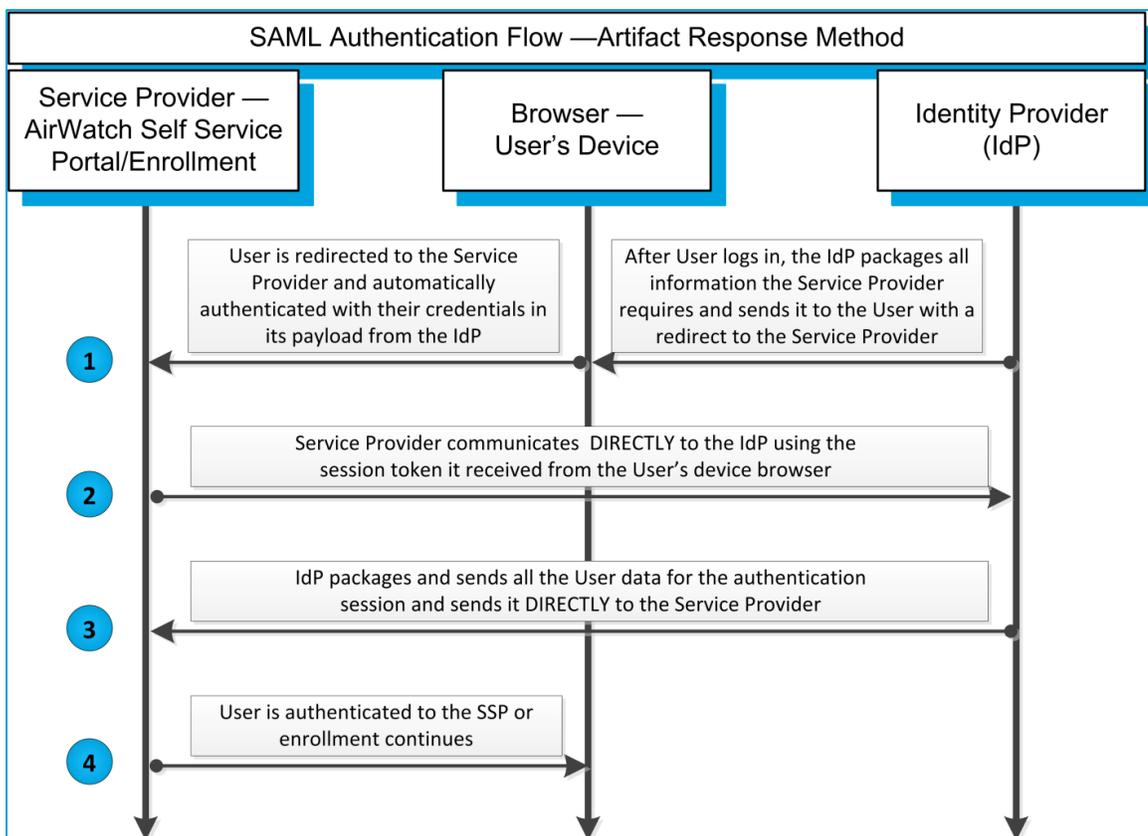
Response for Redirect



Response for Post



Response for Artifact



Appendix C — Locating a Group ID

In order to login to your IdP, you need your AirWatch GroupID that is configured for SAML. You can find the GroupID by performing the following steps.

1. Navigate to Groups & Settings > Groups > Organization Groups > Organization Group Details. It opens to the default Organization Group Details tab.
2. Locate the **GroupID** and make note of it for future use.
3. Add the **GroupID** to the end of the SAML URL. For example, <https://ACME.com/AirWatch/Login?GID=gsaml>

Appendix D — Specifying a Post-Authentication Landing Page

You may customize the authentication URL you forward to users so that when they complete the authentication process, they are automatically taken to a page of your choosing. Appending “&ReturnURL” (minus the quotes) to the URL used for SAML authentication will take users to the URL specified.

For example, <https://environmentURL/mydevice/?ac=GroupID&ReturnURL=%2MyDevice%2fContent> will take users to the **My Content** page of the **Self Service Portal** after they have authenticated via SAML.

Appendix E — Sample XML

Sample of the Service Provider’s (AirWatch) XML.

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ID="..." entityID="AirWatch">
  <- <md:SPSSODescriptor ID="..." VantAssertionsSigned="false" AuthnRequestsSigned="false">
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:ArtifactResolutionService isDefault="false" index="1" Location="..." /IdentityService/SAML/ArtifactResolver.ashx"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
      <md:ArtifactResolutionService isDefault="false" index="2" Location="..." /MyDevice/SAML/ArtifactResolver.ashx"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
      <md:ArtifactResolutionService isDefault="false" index="3" Location="..." /DeviceManagement/SAML/ArtifactResolver.ashx"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
      <md:ArtifactResolutionService isDefault="false" index="4" Location="..." /SAML/ArtifactResolver.ashx" Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
      <md:ArtifactResolutionService isDefault="false" index="5" Location="..." /Catalog/SAML/ArtifactResolver.ashx"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:entity</md:NameIDFormat>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
      <md:AssertionConsumerService isDefault="false" index="1" Location="..." /IdentityService/SAML/AssertionService.ashx?binding=HttpRedirect"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
      <md:AssertionConsumerService isDefault="false" index="2" Location="..." /IdentityService/SAML/AssertionService.ashx?binding=HttpPost"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <md:AssertionConsumerService isDefault="false" index="3" Location="..." /IdentityService/SAML/AssertionService.ashx?binding=HttpArtifact"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>
      <md:AssertionConsumerService isDefault="false" index="4" Location="..." /MyDevice/SAML/AssertionService.ashx?binding=HttpRedirect"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
      <md:AssertionConsumerService isDefault="false" index="5" Location="..." /MyDevice/SAML/AssertionService.ashx?binding=HttpPost"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <md:AssertionConsumerService isDefault="false" index="6" Location="..." /MyDevice/SAML/AssertionService.ashx?binding=HttpArtifact"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>
      <md:AssertionConsumerService isDefault="false" index="7" Location="..." /DeviceManagement/SAML/AssertionService.ashx?binding=HttpRedirect"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
      <md:AssertionConsumerService isDefault="false" index="8" Location="..." /DeviceManagement/SAML/AssertionService.ashx?binding=HttpPost"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <md:AssertionConsumerService isDefault="false" index="9" Location="..." /DeviceManagement/SAML/AssertionService.ashx?binding=HttpArtifact"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>
      <md:AssertionConsumerService isDefault="false" index="10" Location="..." /SAML/AssertionService.ashx?binding=HttpRedirect"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
      <md:AssertionConsumerService isDefault="false" index="11" Location="..." /SAML/AssertionService.ashx?binding=HttpPost"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <md:AssertionConsumerService isDefault="false" index="12" Location="..." /SAML/AssertionService.ashx?binding=HttpArtifact"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>
      <md:AssertionConsumerService isDefault="false" index="13" Location="..." /Catalog/SAML/AssertionService.ashx?binding=HttpRedirect"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
      <md:AssertionConsumerService isDefault="false" index="14" Location="..." /Catalog/SAML/AssertionService.ashx?binding=HttpPost"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <md:AssertionConsumerService isDefault="false" index="15" Location="..." /Catalog/SAML/AssertionService.ashx?binding=HttpArtifact"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>
    </md:SPSSODescriptor>
  </md:EntityDescriptor>
```

Appendix F – Testing and Troubleshooting

Overview

Use these testing and troubleshooting techniques to verify the connection between the Service Provider (AirWatch) and the IdP. These are some of the troubleshooting problems you might encounter along with solutions to resolve the problem. This section will expand as additional troubleshooting information becomes available.

Verifying the Service Provider and the IdP are Connected

1. Navigate to your enrollment URL (e.g., <https://<AirWatchEnrollment>/enroll>). An **AirWatch Enrollment** window appears.
2. Enter your Organization Group ID in the **Group ID** field. If the Service Provider and IdP make the proper connection, you are immediately redirected to your company Single Sign On (SSO) login page. If you do not see the SSO login page, continue to the next step.
3. Go to the SAML configuration page in the AirWatch Admin Console and verify the settings have not been changed or differ from what you would expect. If not, continue.
4. Verify the certificate date is valid. If not, request a new certificate.
5. Verify the **Request** binding type is set correctly. If not, set it to the correct binding type.
6. Verify the **Response** binding type is set correctly. If not, set it to the correct response type.

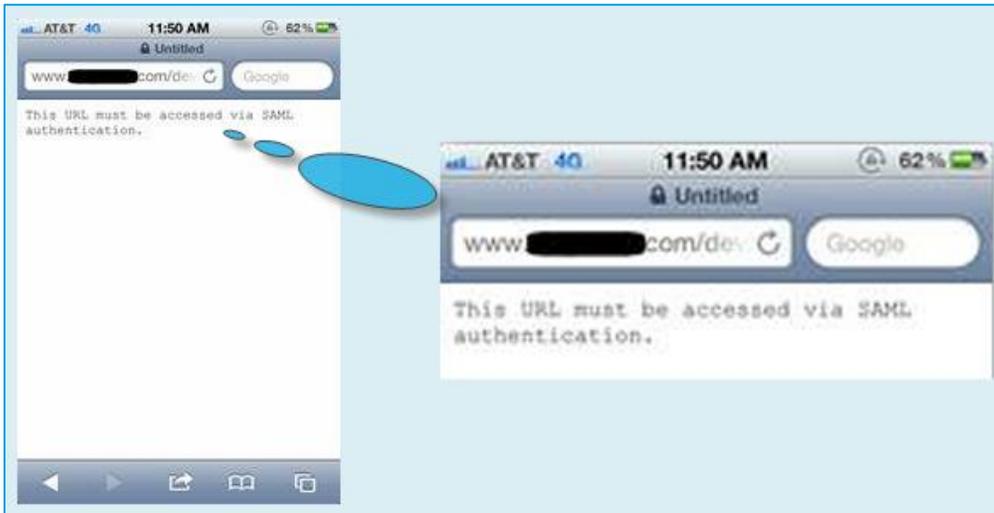
AirWatch supports all binding types in both directions (i.e., Request and Response). IdPs generally do not support all types in both directions. For that reason, you must match the correct Request and Response binding types in the AirWatch Admin Console to the binding type supported by the IdP. If not, the user is not redirected to the IdP's login page. If you need more information, consult your IdP's documentation and/or their technical support to verify the binding types they support.

AirWatch Errors

You may encounter the following common errors while troubleshooting SAML.

- [This URL must be accessed via SAML authentication](#)
- [SAML authentication has timed out; please try your request again](#)
- [The SAML response is missing form variable RelayState, required by SAML protocol](#)
- [Value cannot be null. Parameter name: key](#)
- [When using SAML with iOS devices, the user sees a welcome message but never gets redirected to the IDP.](#)

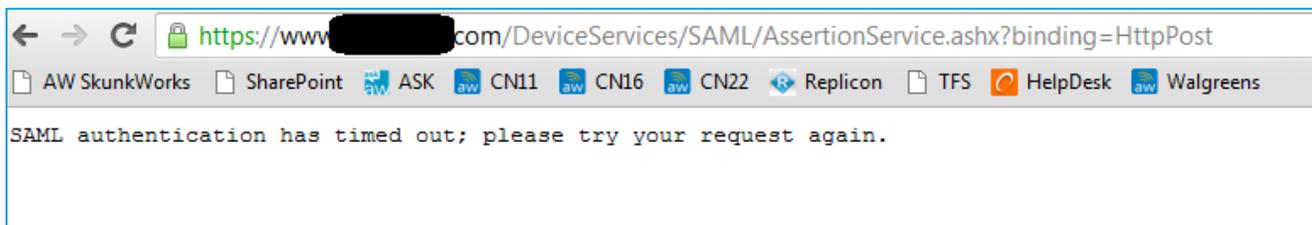
This URL must be accessed via SAML authentication



Problem: Verbose Logs Error. The device displays "This URL must be accessed via SAML authentication."
AW.Console.Web.Mobile.DeviceManagement.SAML.AssertionService Authentication response does not contain a "UID" attribute.

Resolution: Adding the UID field sends it to the device.

SAML authentication has timed out; please try your request again.



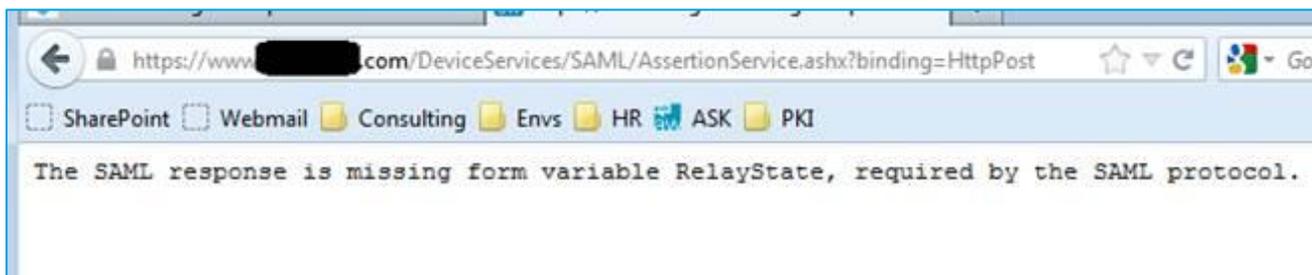
Problem: The “SAML authentication has timed out” error occurs when the AssertionService received a RelayState, but it does not have a matching entry stored locally in memory.

The AssertionService thinks that surely the IdP is sending the value it received, and surely it is coming back to the right place, so the RelayState record must have timed-out of the cache. This assumes the IdP correctly echoes the RelayState it received and it did not timeout, which can happen when the AssertionService is located in a different application server than the one where the process started.

Resolution #1: The AssertionService might be in DeviceServices, whereas the enrollment might be initiated in DeviceManagement. Update the URLs in the IdP.

Resolution #2: Any URL used that contains an attribute such as: ?SPID or ?PartnerSpId=AirWatch is most likely for an IdP initiation SAML integration. AirWatch does not support this type of URL. Check the URL and update it with one that AirWatch supports.

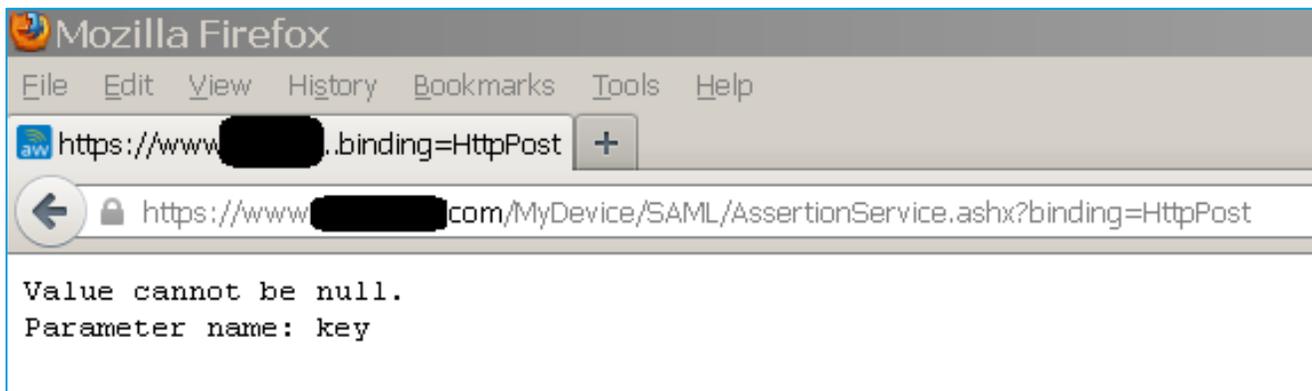
The SAML response is missing form variable RelayState, required by SAML protocol



Problem: The URL is for IdP initiated SSO, which AirWatch does not support.

Resolution: Any URL that contains an attribute such as, ?SPID or ?PartnerSpId=AirWatch is most likely for an IdP initiation SAML integration. AirWatch only supports Service Provider (i.e., the process starts with AirWatch) initiated SSO and then AirWatch redirects the browser to the IdP for authentication. Change the URL to a Service Provider (SP) initiated URL.

Value cannot be null. Parameter name: key



Problem: The “Value cannot be null. Parameter name: key” is a generic error.

Resolution: Most likely, you have an older version of AirWatch installed (e.g., AirWatch 5.17). AirWatch has made many enhancements to later versions that provide more details that would help you determine the problem and resolve it. Since this is a generic error and later versions of AirWatch provide more details needed for troubleshooting, upgrade to the latest version of AirWatch.

When using SAML with iOS devices, the user sees a welcome message but never gets redirected to the IDP

Problem: When enrolling an iOS devices with SAML enabled, if you have “Display Welcome Message” enabled in the AirWatch Admin Console then the user gets directed to the welcome message and never gets redirected to the IDP.

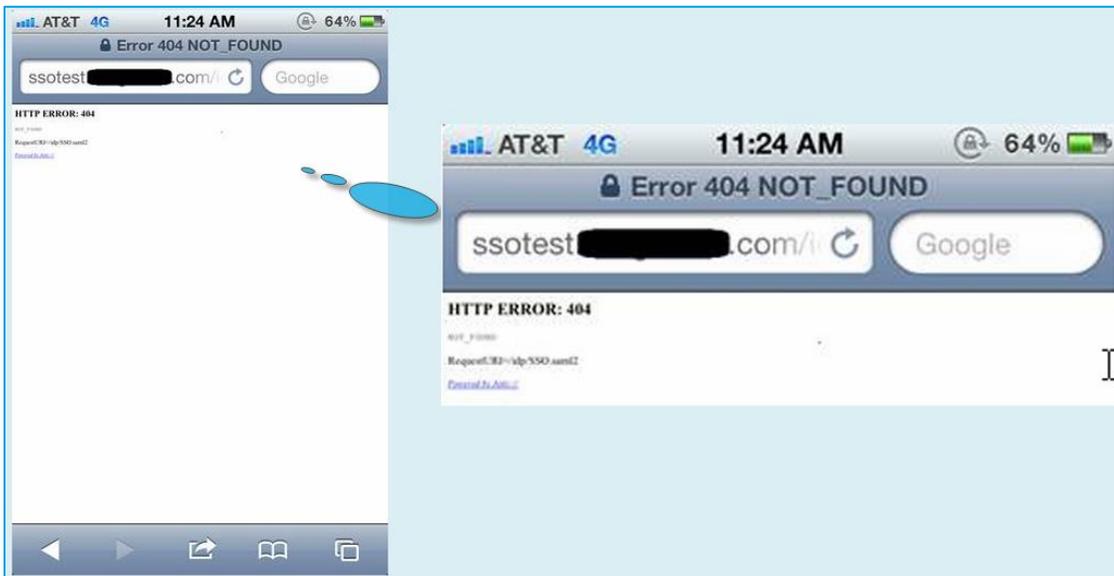
Resolution: Disable Display Welcome Message in the AirWatch Admin Console by navigating to Groups & Settings > All Settings > Devices & Users > General > Enrollment > Optional Prompt.

PingFederate Errors

You may encounter the following PingFederate errors while troubleshooting SAML:

- [HTTP Error 404](#)
- [User does not have access to the system, because of domain type mismatch \(Domain Type: ‘:Employee’\)](#)

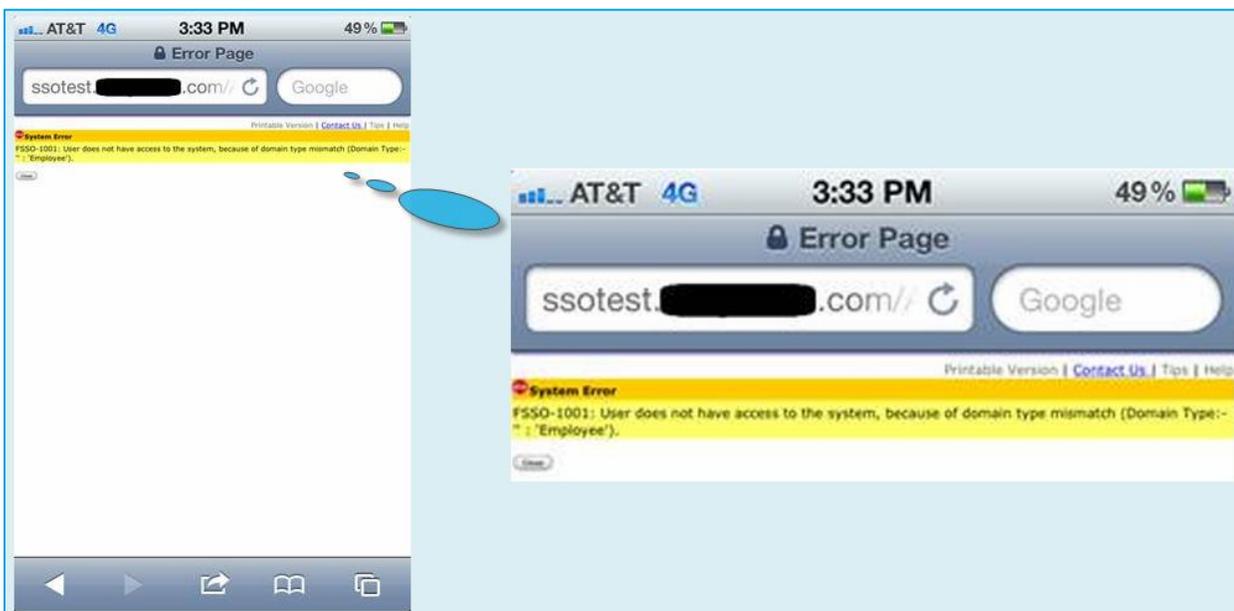
HTTP Error 404



Problem: The device is receiving a HTTP ERROR: 404. The SAML endpoint is not operational.

Resolution: Contact your IdP provider to inquire about the problem and make them aware it is not operational.

User does not have access to the system, because of domain type mismatch (Domain Type:- “:Employee”)



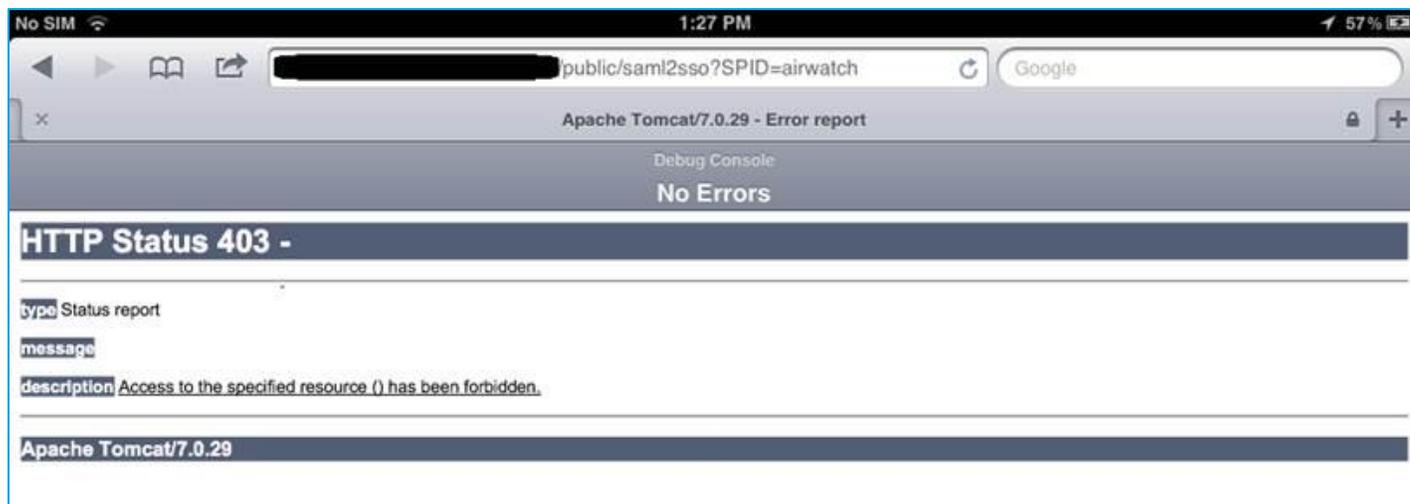
Problem: User received a permission error from the system. In this scenario, the user who attempted to authenticate was a **Contractor**, but only **Employees** can authenticate.

Resolution: Contact your AirWatch system administrator who can provide the **Contractor** with the necessary credentials needed to authenticate.

SiteMinder Errors

This covers the following SiteMinder errors you might encounter while troubleshooting SAML.

HTTP Status 403 – Access to the specified resource () has been forbidden



Problem: The URL is for IdP initiated SSO, which AirWatch does not support.

Resolution: Any URL that contains an attribute such as ?SPID or ?PartnerSpId=AirWatch is most likely for an IdP initiation SAML integration. AirWatch only supports Service Provider (i.e., the process starts with AirWatch) initiated SSO and then AirWatch redirects the browser to the IdP for authentication. You might be using a junction to redirect to the SSO page, which is probably not included in the imported IdP metadata. Ask the IdP resource what the junction site is, and add it into the SSO URL.

The sole intent of this document is to provide AirWatch customers with initial guidance to technical issues. The suggestions given herein are provided as a courtesy and are not intended to replace specific personalized advice provided by the reader's network administrators, computer security personnel, or other technical experts and consultants. References in this document whitepaper to any specific service provider, manufacturer, company, product, service, or software do not constitute an endorsement or recommendation by AirWatch. Under no circumstances shall AirWatch be liable to you or any other person for any damages, including without limitation, any direct, indirect, incidental, special or consequential damages, expenses, costs, profits, lost savings or earnings, lost or corrupted data, or other liability arising out of or related in any way to information, guidance, or suggestions provided in this document.