Configuring Single Sign-on from the VMware Identity Manager Service to AirWatch Applications

VMware Identity Manager

AUGUST 2015 V1

vmware®

Table of Contents

Overview

This document provides information about configuring single sign-on from the VMware Identity Manager service to AirWatch applications.

You can integrate the AirWatch Self Service Portal and AirWatch Content Locker Web applications with the service. This enables you to manage them like any other application in the catalog, entitle users to them, and provide single sign-on access to them.

AirWatch Content Locker allows you to manage document distribution and mobile access to corporate documents through a Web-based console. The AirWatch Self Service Portal enables end users to view and manage their enrolled devices.

To integrate the applications with the VMware Identity Manager service, you add each application to the VMware Identity Manager catalog and enable SAML authentication in AirWatch to allow users logged in to the service to have single sign-on access to the AirWatch applications.

You must have an administrator account for the VMware Identity Manager service as well as an administrator account for the application you are adding.

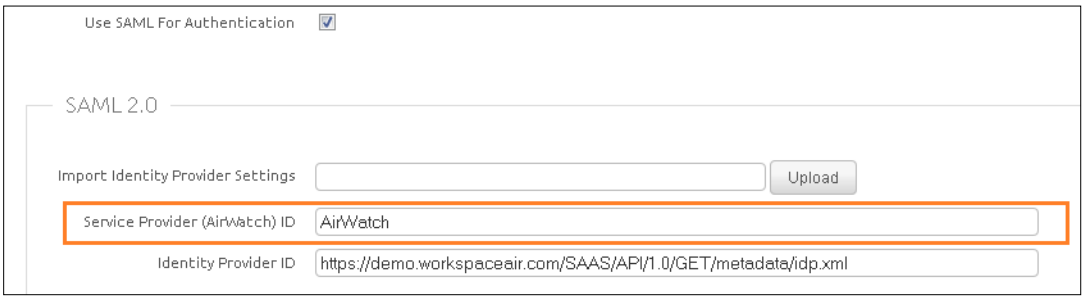
Add AirWatch Applications to the VMware Identity Manager Catalog

Add the AirWatch Self Service Portal application, the AirWatch Content Locker application, or both, to the VMware Identity Manager catalog.

Obtain AirWatch Group ID and Service Provider ID Information for VMware Identity Manager

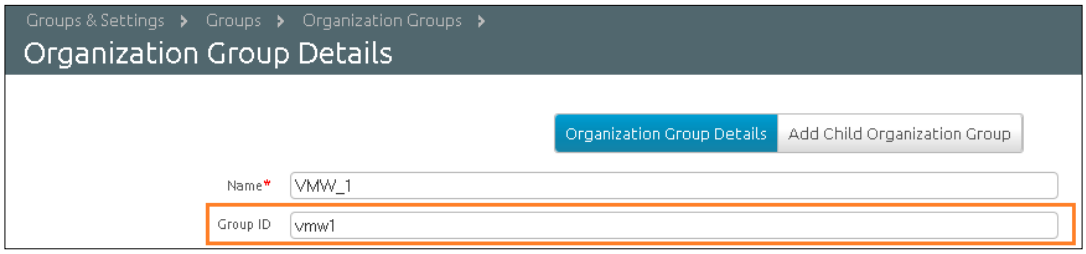
Before you can add the applications to the catalog, you obtain the AirWatch service provider ID and group ID, and disable **Use SAML For Authentication** on the AirWatch server.

1. Log in to the AirWatch console.
2. Navigate to the **Accounts > Administrators > Administrators Settings > Directory Services** page.
3. Select the **Use SAML for Authentication** checkbox to display the SAML 2.0 information.
4. Make a note of the value of the **Service Provider (Airwatch) ID** field, if it is set.



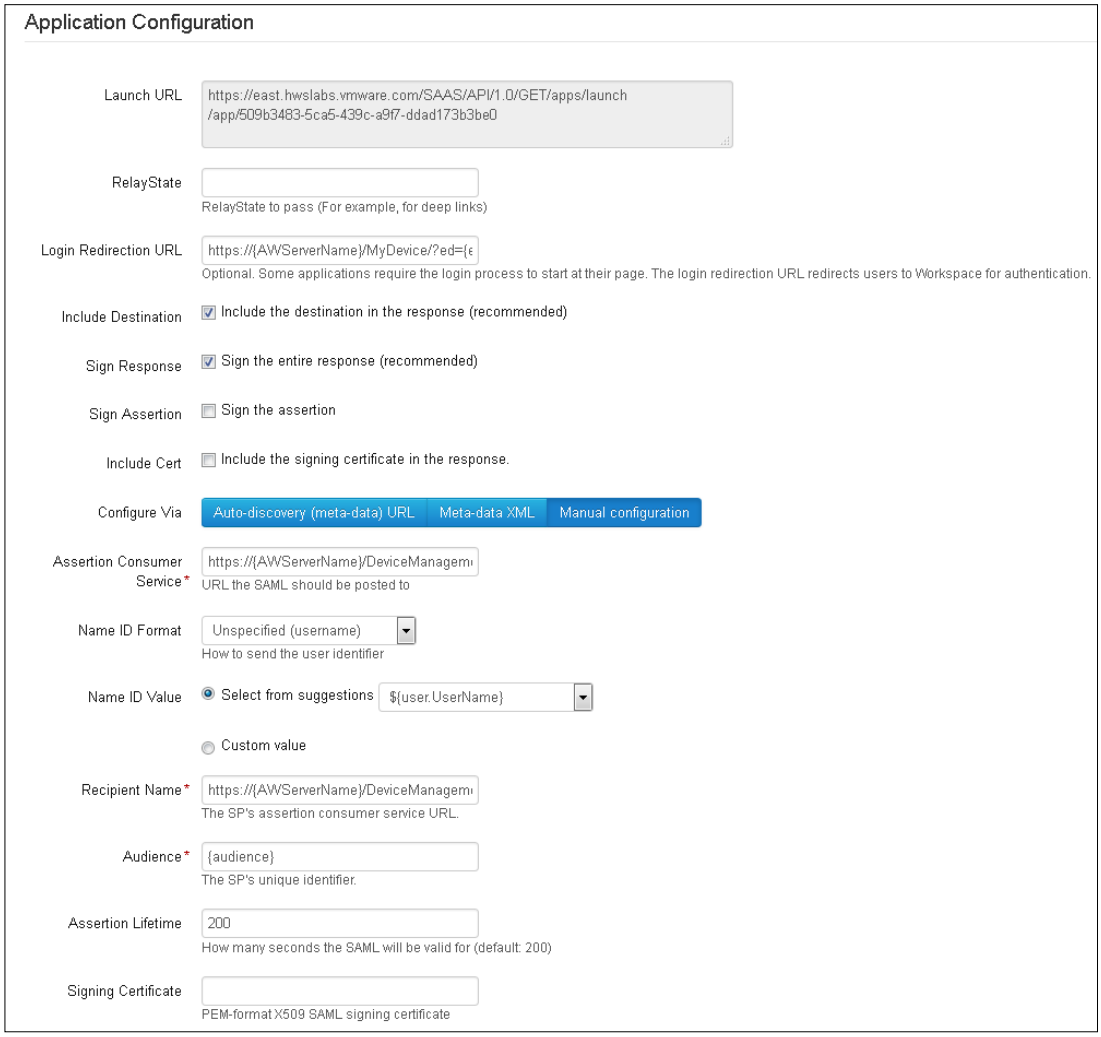
5. Deselect the **Use SAML for Authentication** checkbox.
6. Navigate to the **Groups & Settings > Groups > Organization Groups > Organization Group Details** page.

7. Make a note of the value of the Group ID field.



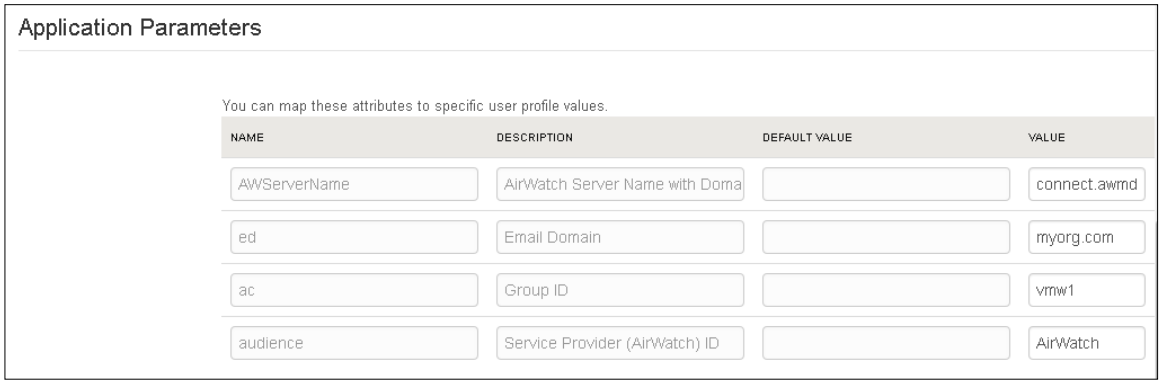
Add AirWatch Applications to the Catalog

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Add Application > ...from the cloud application catalog**.
3. Click the icon for the application you want to add: the AirWatch icon (for the Self Service Portal) or the Content Locker icon.
4. In the Modify application page, click **Configuration**.
5. In the **Application Configuration** section, accept the default values for all fields. For example:

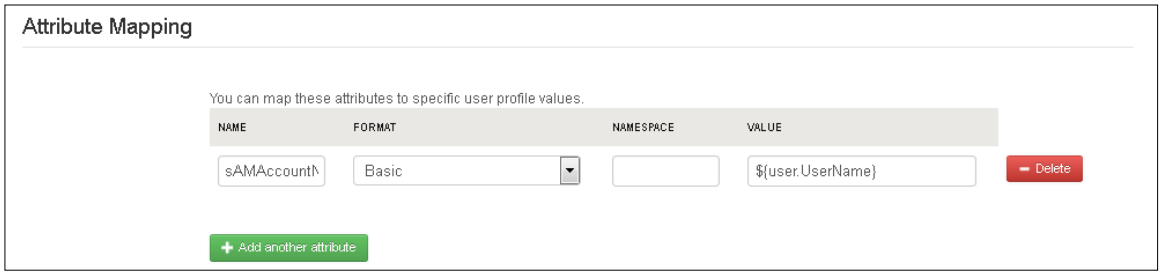


6. In the **Application Parameters** section, enter the following values.

FIELD	DESCRIPTION
AWServerName	Enter the AirWatch server name and domain. For example, **connect.awmdm.com**.
ed	Enter the email domain that has been set for the organization in AirWatch. For example, **myorg.com**. When an email domain is set, users can specify the email domain instead of the Group ID while logging in. If an email domain has not been set for the organization in AirWatch, enter any value. If the **ed** field has a valid value, it is used to determine the AirWatch Group ID, otherwise the value of the **ac** field is used.
ac	Enter the AirWatch Group ID that you obtained. For example, **vmw1**.
audience	Enter the AirWatch Service Provider ID that you obtained. For example, **AirWatch**. If the Service Provider ID field was not set, enter a unique name.



7. In the **Attribute Mapping** section, ensure that at least one attribute is mapped to a specific user profile value.



8. Click **Save**.
9. Click **Entitlement** and entitle the application to the appropriate users and groups.
10. Repeat these steps to add the other AirWatch application to the VMware Identity Manager catalog, if necessary.

The AirWatch applications are now in the VMware Identity Manager catalog.

Configure AirWatch to Enable SAML for Authentication

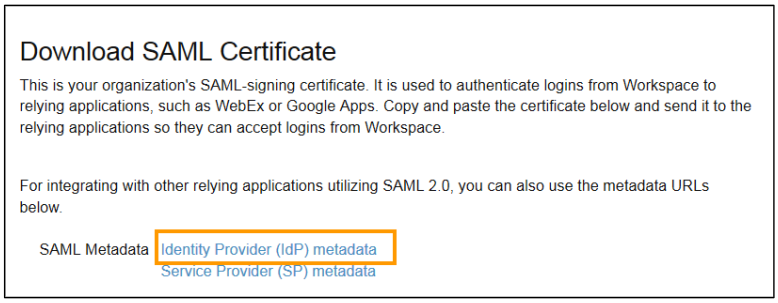
In the AirWatch console, enable SAML for authentication. This allows single sign-on from the VMware Identity Manager service to all the AirWatch applications that are added to the VMware Identity Manager catalog.

Before you enable SAML, ensure that the applications have been added to the VMware Identity Manager catalog.

Locate Identity Provider SAML Metadata

You must have the VMware Identity Provider identity provider metadata xml URL to configure AirWatch. From the VMware Identity Manager administration console, save a copy of the identity provider SAML metadata **idp.xml** file.

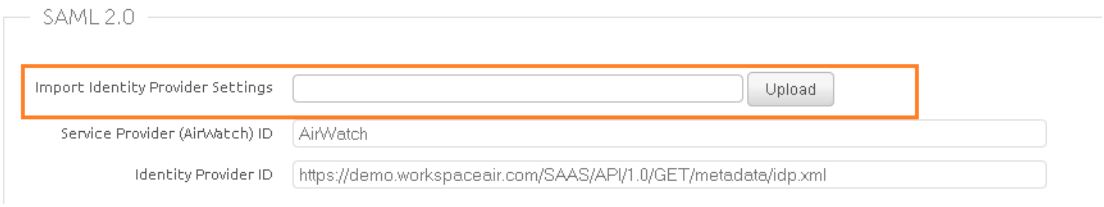
1. In the service's administration console Catalog tab, click **Settings > SAML Metadata**.
2. In the SAML Metadata section, click **Identity Provider (IdP) metadata** to display the metadata content. Save the URL. The URL is similar to this example. https://myco.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml.



3. Save the file.

Setting up AirWatch

1. Log in to the AirWatch console.
2. Navigate to the **Accounts > Administrators > Administrators Settings > Directory Services** page.
3. Select the **Use SAML For Authentication** check box.
4. Click **OK**.
5. In the SAML 2.0 section, in the **Import Identity Provider Settings** field, click **Upload** and upload the VMware Identity Manager **idp.xml** file that you saved.



6. Click **Save**.

   The remaining fields are automatically filled with information from the **idp.xml** file.

7. Verify that the settings on the page match the following.

FIELD	DESCRIPTION
Service Provider (AirWatch) ID	The AirWatch Service Provider ID. This value must match the value of the **Application Parameters - audience** field in the VMware Identity Manager service. For example: **AirWatch**.
REQUEST section	
Request Binding Type	**Redirect**
Identity Provider Single Sign On URL	The VMware Identity Manager URL that AirWatch uses to send requests. Prepopulated as **https://*yourtenant*.workspaceair.com/SAAS/auth/federation/sso**.
NameID Format	**Unspecified**
Authentication Request Security	**None**
RESPONSE section	
Response Binding Type	**POST**
Sp Assertion Url	AirWatch URL that is configured by VMware Identity Manager to direct its authentication responses, entered as **~/SAML/AssertionService.ashx?binding=HttpPost**
Authentication Response Security	**Validate response signatures**

8. Click **Test Connection** to verify that you can establish a connection with the VMware Identity Manager service.
9. Click **Save**.
10. Close the Settings page.
11. Navigate to the **Apps > Catalog > General** page.
12. In the **Require Authentication** field, select **Disabled**.
13. Click **Save**.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com