VMware Identity Manager Integration with Apteligent

JAN 2019 V1

VMware Identity Manager

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Getting Started

1

This documentation provides information about integrating Apteligent with the VMware Identity Manager™ service to enable single sign-on access to Apteligent.

Apteligent is a management solution for mobile apps that provides data-driven insights into application performance, user behavior, and business analytics. The VMware Identity Manager service is an identity provider that supports federated single sign-on (SSO) capabilities based on the Security Assertion Markup Language (SAML) protocol.

When you add Apteligent to the catalog and configure SSO settings, users only need to enter their credentials one time in the Workspace ONE portal. Apteligent trusts the VMware Identity Manager service to authenticate and authorize these users, and allows access to the application without requiring any additional sign-on information.

Note To complete the integration procedures, you must have administrator privileges for both the VMware Identity Manager console and Apteligent.

To integrate Apteligent with the VMware Identity Manager service, complete the following tasks:

- Configure SAML SSO settings in Apteligent.
- Add Apteligent to the catalog, and configure Apteligent SSO settings in the VMware Identity Manager console.
- Test and verify the SSO configuration.
- Provide users with SSO access to Apteligent.

Configuring SSO Settings in Apteligent

2

You set up Apteligent for SSO by defining VMware Identity Manager as the SAML identity provider for the application.

Before configuring SSO settings, you must gather the SAML metadata associated with the VMware Identity Manager service. Apteligent requires the SAML metadata to set up the VMware Identity Manager service as its identity provider.

Note To ensure compatibility with the Apteligent SSO settings, save the VMware Identity Manager SAML metadata as a .xml file on your computer.

This chapter includes the following topics:

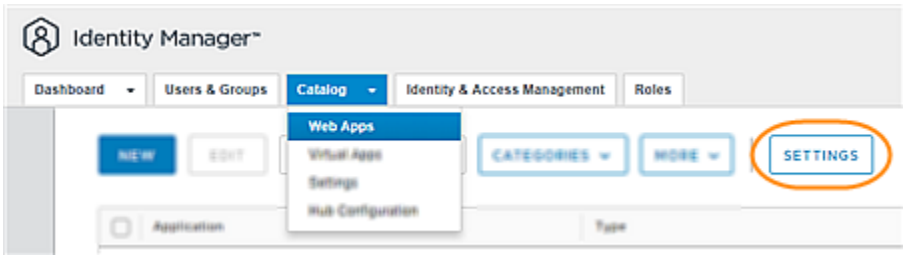
Obtain the VMware Identity Manager SAML Metadata

Apteligent requires the VMware Identity Manager SAML metadata for the SSO configuration. The SAML metadata describes the capabilities and requirements of the VMware Identity Manager service, and resides as an XML file on the VMware Identity Manager service domain.

Procedure

1 Log in to the VMware Identity Manager console.

2 Select the **Catalog > Web Apps** tab.

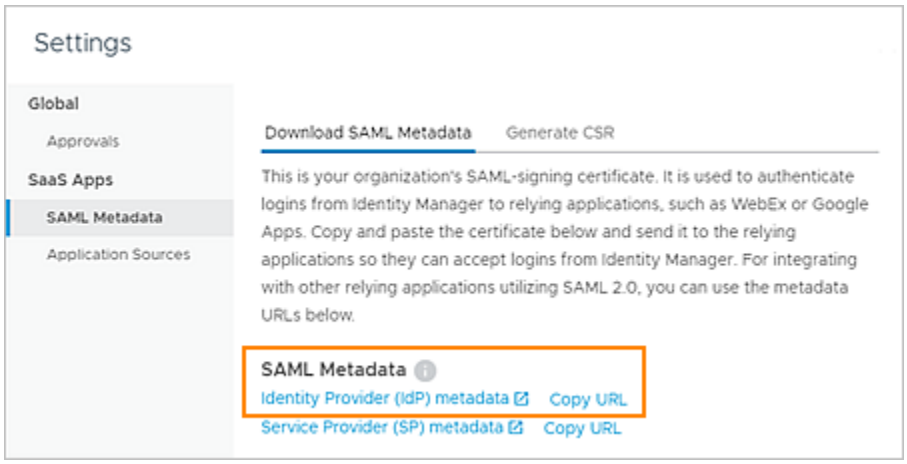


3 Click **Settings** and then select **SAML Metadata**.

4 In the SAML Metadata section, obtain and save the identity provider metadata XML or URL, as required by your application.

- Under the SAML Metadata section, click the **Identity Provider (IdP) metadata** link to open a new window displaying the contents of the SAML metadata .xml file. Save the contents to a .xml file on your computer.
- Under the SAML Metadata section, next to Identity Provider (IdP) metadata, click **Copy URL** to copy the metadata URL to the clipboard. Then save the URL to a .txt file on your computer.

The metadata URL resembles this example: **https://myco.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml**, where **myco.vmwareidentity.com** is replaced with your organization's domain name for the VMware Identity Manager service.



5 Close the Settings page.

Configure SAML SSO Settings in Apteligent

You configure SSO in Apteligent by defining the VMware Identity Manager service as the SAML-based identity provider for Apteligent.

Note The following procedure provides general guidelines for configuring SAML SSO settings in Apteligent. For the most up-to-date, detailed instructions, see the Apteligent documentation or consult with your Apteligent account representative.

Prerequisites

- Obtain the VMware Identity Manager SAML metadata.
- Obtain the Apteligent account login information from your account representative.

Procedure

1 Using the account login information that you obtained previously, log in to Apteligent.

2 Navigate to the **Account Management > Single Sign-On** page.

3 Upload the VMware Identity Manager SAML metadata that you obtained previously.

4 Note the **Identity Provider Name** displayed on the Single Sign-On page.

> **Note** You need the identity provider name to configure settings in the VMware Identity Manager console.

5 Accept the default values for all other settings.

What to do next

Configure SSO settings in the VMware Identity Manager console.

Configuring SSO Settings in the VMware Identity Manager Console

3

The SSO configuration in the VMware Identity Manager console consists of adding Apteligent to the catalog and configuring application settings.

Add Apteligent to the Catalog

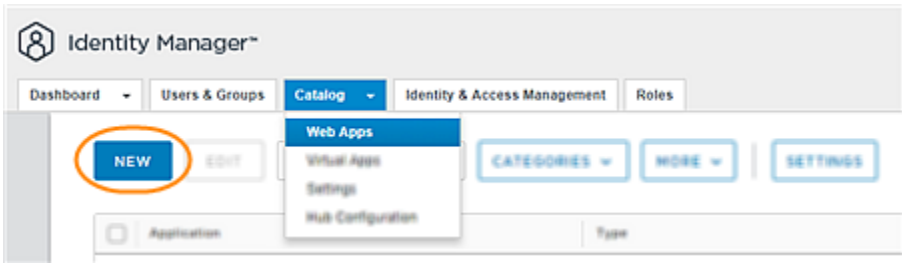
Adding Apteligent to the catalog makes the application available as a resource that users can access from the Workspace ONE portal. You enable SSO to Apteligent by configuring SAML settings in the VMware Identity Manager console.

Prerequisites

- Configure SSO settings in Apteligent and obtain the Identity Provider Name.
- Obtain the Apteligent account ID from your account representative.

Procedure

1. Log in to the VMware Identity Manager console.
2. Select the **Catalog > Web Apps** tab.

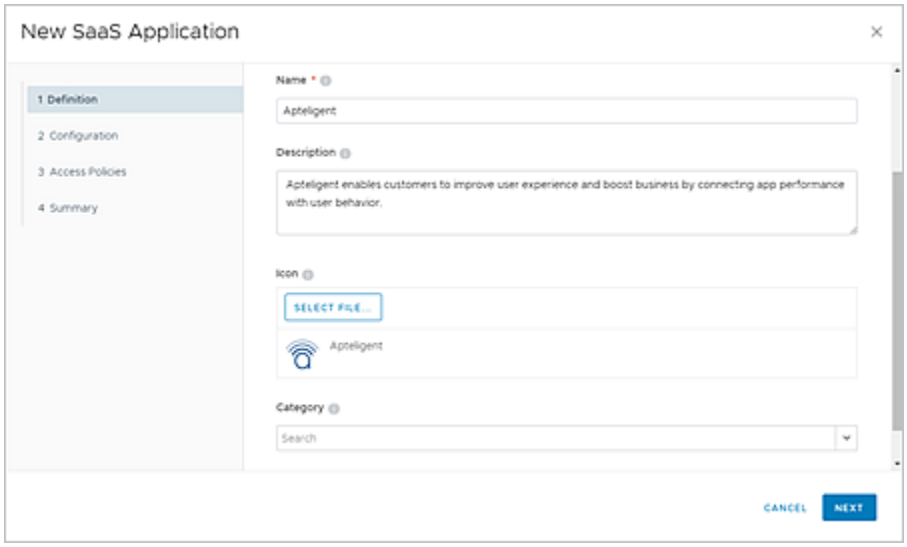


3. Click **New**.

   The New SaaS Application wizard appears.

4. Enter Apteligent in the Search text box or click **or browse from catalog**, and select Apteligent from the results.

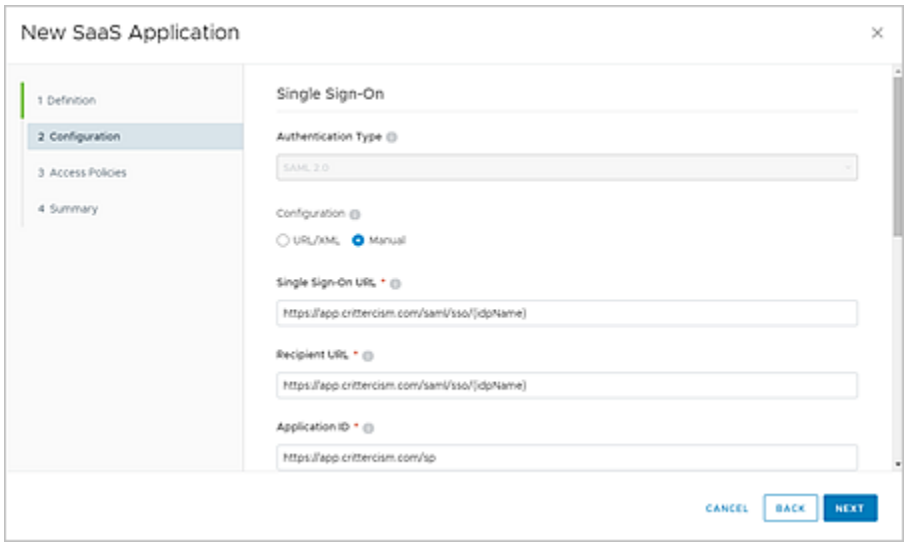
   The Definition page displays the Apteligent name and description. If you want, use the **Category** setting to display Apteligent under a specific category in the Workspace ONE portal.



5 To proceed to the SSO setup, click **Next**.

6 On the Single Sign-On page, configure settings as required by your organization.

Some settings are populated with default values relevant to the Apteligent application. To learn more about a setting, click the information icon next to the setting.



Note For any setting not listed in the following table, accept the default value.

Setting	Description
Authentication Type	Automatically populated with the SAML profile.
Configuration	Select **Manual**.

Setting	Description
Single Sign-On URL	Also known as the Assertion Consumer Services URL. Accept the default value, or enter the URL provided by your Apteligent account representative. If you accept the default value of `https://app.crittercism.com/saml/sso/{idpName}`, replace `{idpName}` with the Identity Provider Name that you obtained when configuring SSO settings in Apteligent.
Recipient URL	Enter the same URL as for **Single Sign-On URL**.
Application ID	Uniquely identifies the application service provider tenant, to ensure that the VMware Identity Manager service sends SAML assertions to the correct tenant. Accept the default value, or enter the URL provided by your Apteligent account representative.
Username Format	If your application service provider requires a specific SAML subject format for the processing of SAML assertions, select the format from the list. Otherwise, select **Unspecified**.
Username Value	Ensures that the VMware Identity Manager service sends SAML assertions with subject statements that the application service provider recognizes. Accept the default value, or enter the value required by provided by your Apteligent account representative.
Relay State URL	Enter the URL of the custom landing page that you want the VMware Identity Manager service to redirect users to after they enter their SSO credentials. Leave this option blank if your application service provider already has a workflow for redirecting users.
Application Parameters	Correspond to your Apteligent account profile. Configure the following parameters. ■ **accountID**: For Value, enter the Apteligent account ID that you obtained previously from your account representative. ■ **idpName**: For Value, enter the Identity Provider Name that you obtained when configuring SSO settings in Apteligent.
Advanced Settings	Expand the Advanced Settings section, and configure the required settings. If a setting does not appear in the following list, accept the default value. ■ **Sign Response**: Set to **Yes** to sign the SAML response sent to the application service provider. ■ **Sign Assertion**: Set to **Yes** to sign the SAML assertion contained within the SAML response. ■ **Custom Attribute Mapping**: Populated with the attributes **User.FirstName**, **User.LastName**, **email**, **autoAssign**, **accountIDs**. Accept all the default formats, namespaces, and values.
Open in VMware Browser	Set to **Yes** to open Apteligent in the VMware Browser, which provides a secure alternative to the native Web browser.
Show in User Portal	Set to **Yes** to ensure that the Apteligent application appears in the Workspace ONE portal.

7 Click **Next** to assign access policies to Apteligent.

The VMware Identity Manager service includes a default policy that is automatically assigned to the Apteligent application when you add the application to the catalog. The default policy controls access to the service as a whole and allows access to all network ranges, from all device types, for all users. The policy has a session timeout of eight hours and uses password authentication as the authentication method.

If you do not want to use the default access policy, select another policy from the menu to define how users can access Apteligent. The menu displays all the available access policies on the Identity & Access Management > Policies page. For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to Apteligent, using which authentication methods, and for how long until reauthentication is required. For more information, see the VMware Identity Manager documentation at https://docs.vmware.com/en/VMware-Identity-Manager/index.html.

8 To proceed to the summary of configuration settings, click **Next**. Then click **Save**.

Testing the SSO Configuration

4

Before deploying Apteligent across your organization, test and verify the SSO configuration with a few test users.

This chapter includes the following topics:

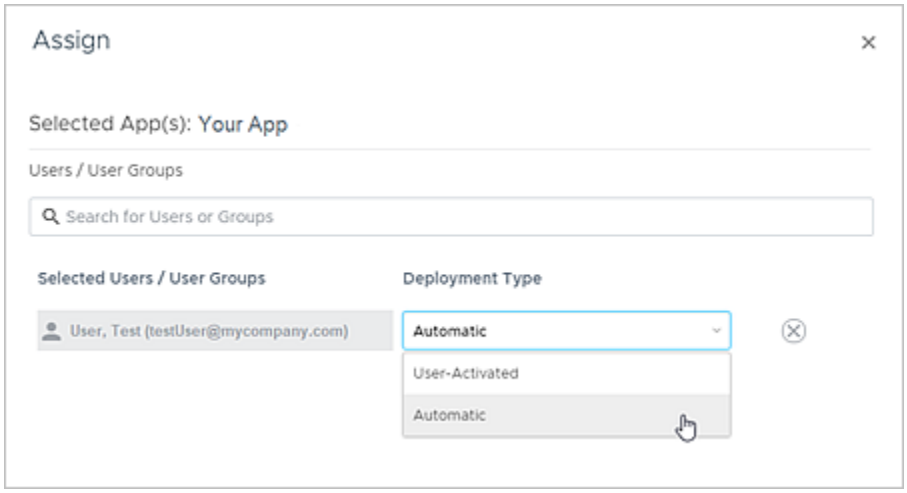
Set Up a Test User in the VMware Identity Manager Console

To set up a test user in the VMware Identity Manager console, you assign Apteligent as a resource to that user. This assignment allows the test user to access Apteligent from the Workspace ONE portal and test SSO capabilities.

Procedure

1. Log in to the VMware Identity Manager console.
2. Select the **Users & Groups** tab, and verify that a test user appears in the list of available users.
3. Select the **Catalog > Web Apps** tab.
4. Select the check box next to Apteligent in the application list. Then click **Assign**.

5 Select the test user by entering the user name in the **Search for Users or Groups** text box and selecting from the results.



6 Under Deployment Type, select **Automatic** to grant the test user immediate access to Apteligent.

7 Click **Save**.

What to do next

Set up the test user in Apteligent.

Set Up the Test User In Apteligent

Make sure the test user you set up in the VMware Identity Manager console is configured with the same user profile in Apteligent.

What to do next

Verify that the test user can sign in to Apteligent from the Workspace ONE portal.

Verify SSO for the Test User

You verify the integration of Apteligent with the VMware Identity Manager service by verifying that the test user can access the application through SSO.

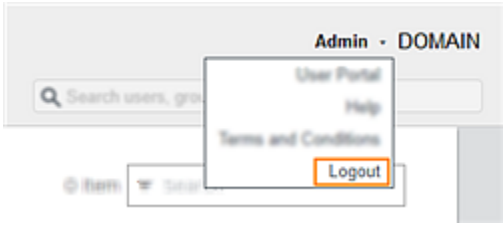
Prerequisites

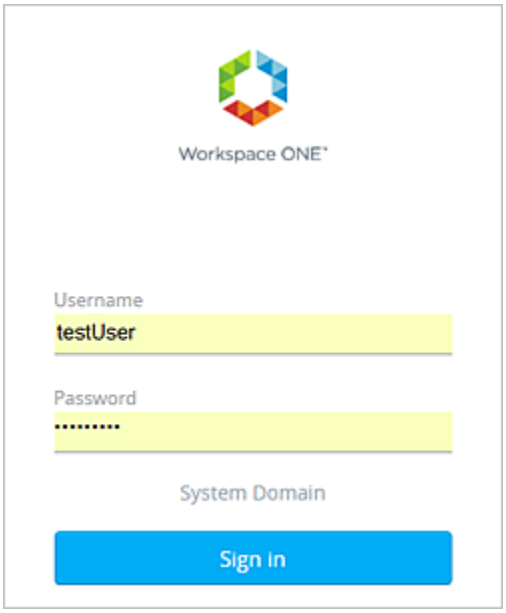
- Set up the test user in the VMware Identity Manager console.
- Set up the test user in Apteligent.

Procedure

1 Have the test user log in to the Workspace ONE portal.

Note Alternatively, you can perform the verification procedure yourself using the test user's credentials. First, log out as the administrator from the VMware Identity Manager console. Click your user name in the top-right corner of the console, and select **Logout**. Then log in to the Workspace ONE portal with the test user's credentials.





2 Have the test user run Apteligent by clicking the application icon in the catalog.

If SSO has been configured successfully, the test user can now access Apteligent without being prompted to enter credentials again.

Assign the Application to Users

5

After you verify the SAML SSO configuration, you can deploy Apteligent across your organization by assigning the application as a resource to users and groups in your organization.

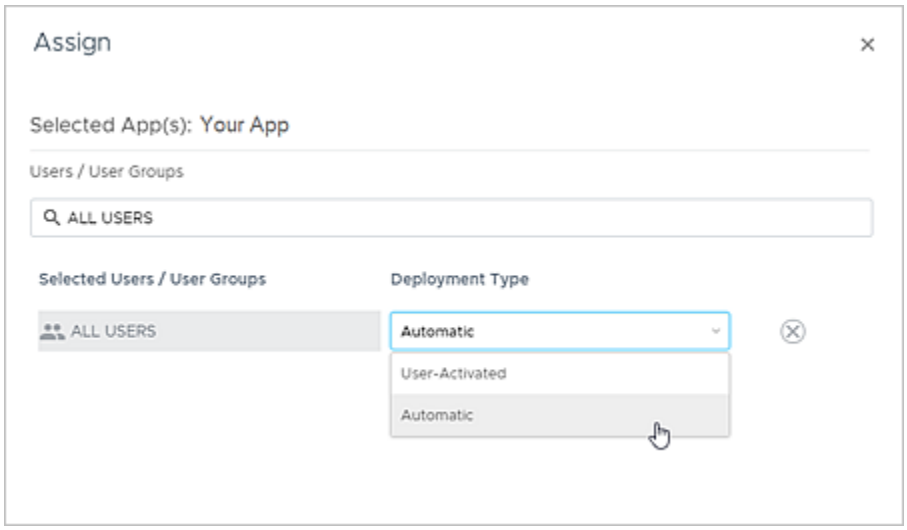
Procedure

1 Log in to the VMware Identity Manager console.

2 Select the **Catalog > Web Apps** tab.

3 Select the check box next to Apteligent in the application list. Then click **Assign**.

4 Select users and groups by entering the name in the text box and selecting from the results. To select all users in your organization, enter **ALL USERS** in the text box.



5 Under Deployment Type, select an option.

- Select **Automatic** if you want the selected users or groups to have immediate access to Apteligent.
- Select **User-Activated** if you plan to set up an approval flow for access to Apteligent. In an approval flow, users must request access to Apteligent and the request must be approved before they can use the application.

6 Click **Save**.

Apteligent now appears on the catalog page of the Workspace ONE portal for the selected users.