VMware Identity Manager Integration with Uptime

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 Uptime with the VMware Identity Manager™ service to enable single sign-on access to Uptime.

Uptime is a monitoring service that checks on the availability and performance of your website at one-minute intervals from 30 different locations across 6 continents. 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 Uptime to the catalog and configure SSO settings, users only need to enter their credentials one time in the Workspace ONE portal. Uptime 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 Uptime.

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

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

Configuring SSO Settings in Uptime

2

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

Before configuring SSO settings, you must gather the SAML metadata and SAML signing certificate associated with the VMware Identity Manager service. Uptime requires both of these SAML components to set up the VMware Identity Manager service as its identity provider.

Note To ensure compatibility with the Uptime SSO settings, save the SAML metadata to a .xml file on your computer. Copy the contents of the SAML signing certificate to a .txt file saved on your computer.

This chapter includes the following topics:

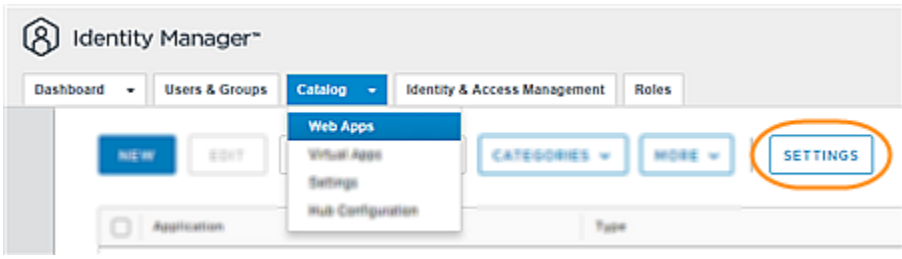
Obtain the VMware Identity Manager SAML Metadata

Uptime 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.

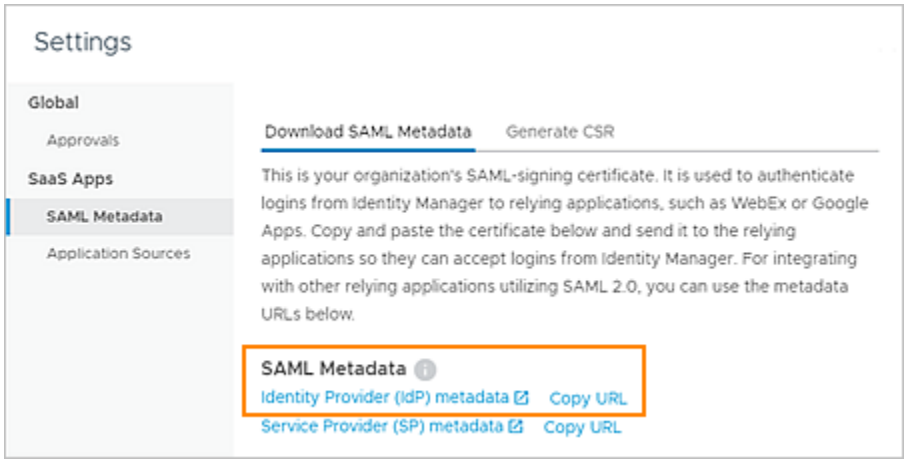


3 Click **Settings** and then select **SAML Metadata**.

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.

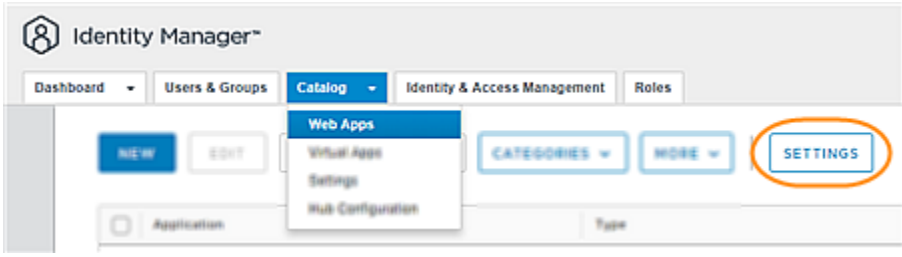
Obtain the VMware Identity Manager SAML Signing Certificate

Uptime requires the VMware Identity Manager SAML signing certificate for the SSO configuration. This self-signed certificate ensures that SAML requests, responses, and assertions sent to Uptime originate from the VMware Identity Manager service.

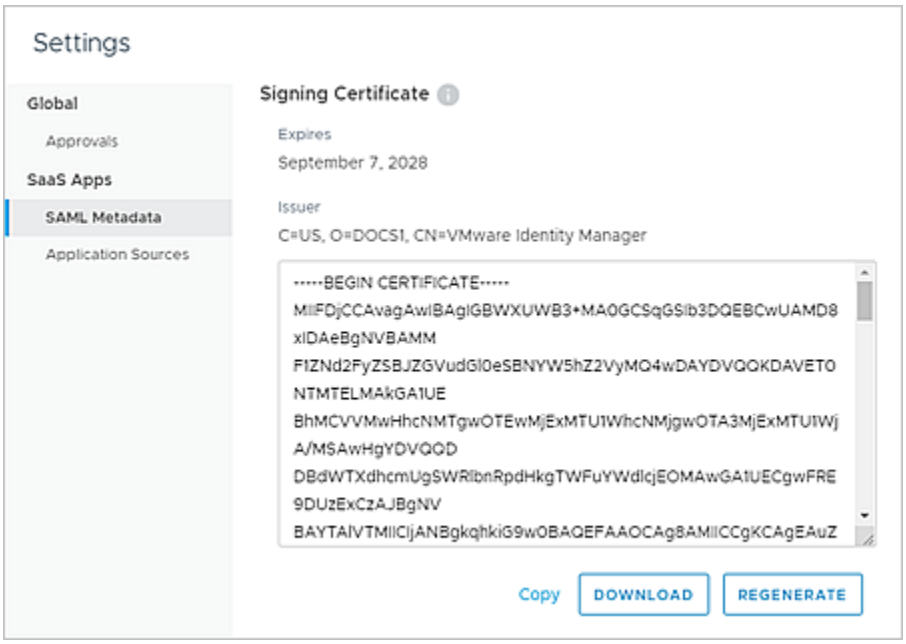
Procedure

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 Signing Certificate section, obtain and save the certificate in the format required by your application.

- To copy the certificate text to the clipboard, click **Copy**. Save the certificate text to a .txt or .pem file on your computer.

  Note If your application requires the certificate value to be a single-line item, remove the beginning and ending certificate brackets ("------BEGIN CERTIFICATE------" and "------END CERTIFICATE------) and all carriage returns from the certificate text.

- To download the certificate as a .cer file, click **Download**. Save the certificate file on your computer.

5 Close the Settings page.

Configure SAML SSO Settings in Uptime

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

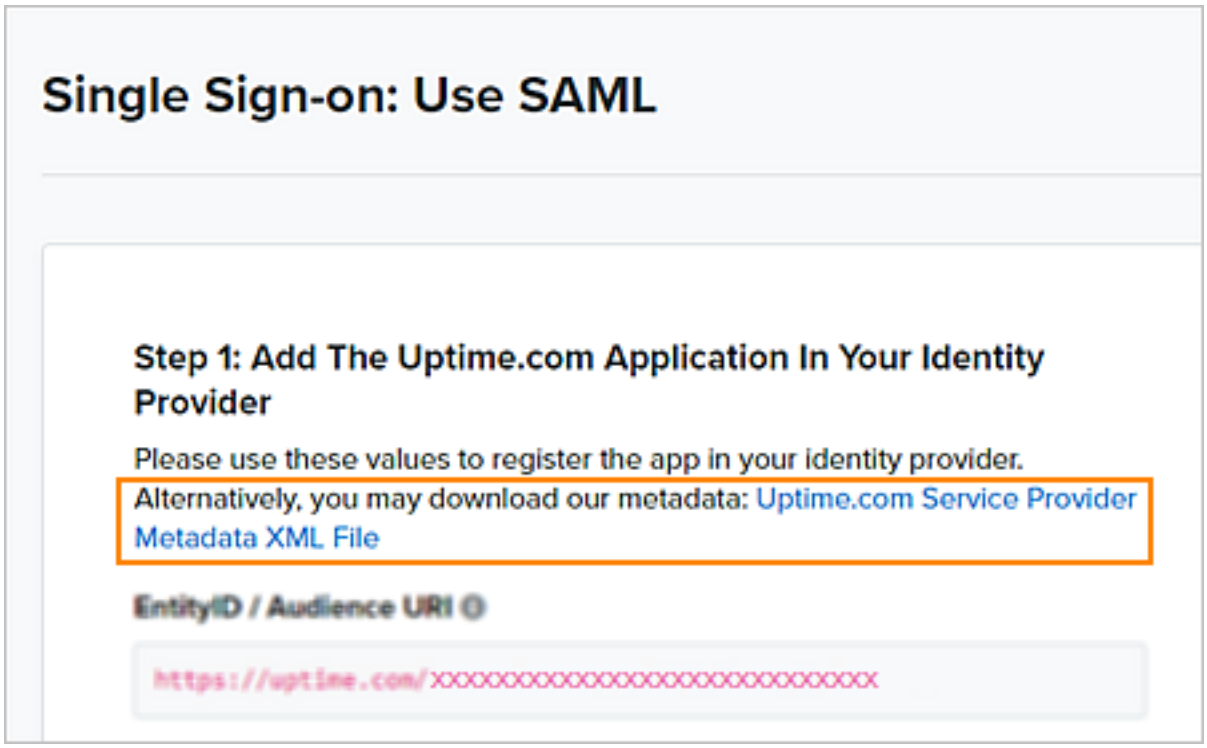
Note The following procedure provides general guidelines for configuring SAML SSO settings in Uptime. For the most up-to-date, detailed instructions, see the Uptime documentation or consult with your Uptime account representative.

Prerequisites

- Obtain the VMware Identity Manager SAML metadata.
- Obtain the VMware Identity Manager SAML signing certificate.

Procedure

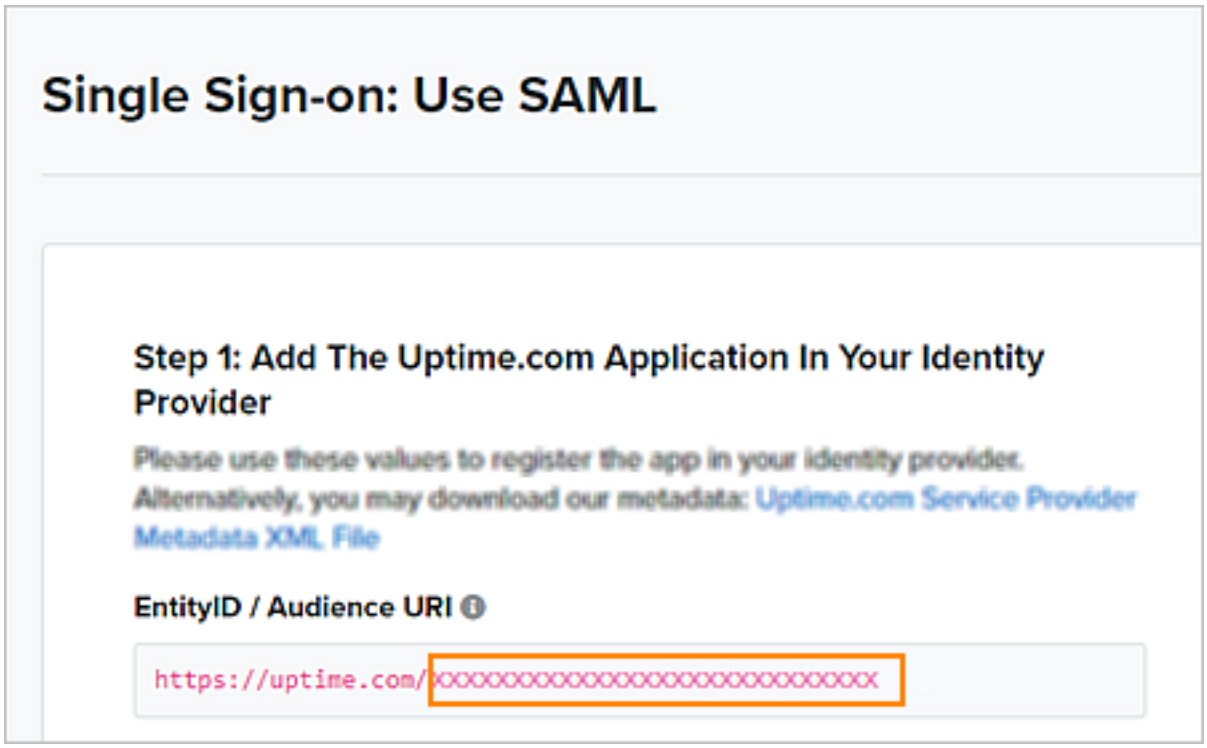
1. In Uptime, log in as an administrator and navigate to **Settings > SSO**.
2. Under **Step 1** on the Single Sign-on: Use SAML page, click the **Uptime.com Service Provider Metadata XML File** link.



This link opens a window displaying the contents of the Uptime SAML metadata .xml file, which uniquely describes Uptime as the service provider. Save the metadata contents to a .xml file on your computer.

Note You need the service provider metadata to configure settings later in the VMware Identity Manager console.

3 Under **EntityID/Audience URI**, note the value that appears at the end of the URL. This value is the Uptime account ID. Copy and save the account ID to a .txt file on your computer.



For example, if the URL is **`https://uptime.com/{accountID}`**, copy and save the **`{accountID}`** value.

Note You need the Uptime account ID to configure settings later in the VMware Identity Manager console.

4 Under **Step 2** on the Single Sign-on: Use SAML page, configure the required settings relevant to the VMware Identity Manager service.

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

Setting	Description
Identity Provider's EntityID	The metadata URL that establishes the VMware Identity Manager service as the identity provider. Enter the SAML metadata URL that you saved previously, using this format: **`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.
SSO Target URL	Enter the VMware Identity Manager login URL in this format: **`https://myco.vmwareidentity.com/SAAS/auth/federation/sso`**, where **`myco.vmwareidentity.com`** is replaced with your organization's domain name for the VMware Identity Manager service.
Identity Provider's Certificate	The signing certificate that establishes the VMware Identity Manager service as the identity provider. Paste in the contents of the SAML signing certificate that you copied previously.

5 Click **Save 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 Uptime to the catalog and configuring application settings.

Add Uptime to the Catalog

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

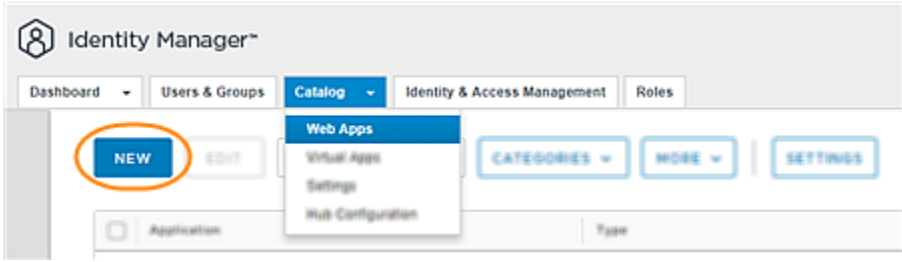
Prerequisites

Configure SSO settings in Uptime, and obtain the Uptime service provider metadata and the Uptime account ID.

Procedure

1 Log in to the VMware Identity Manager console.

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

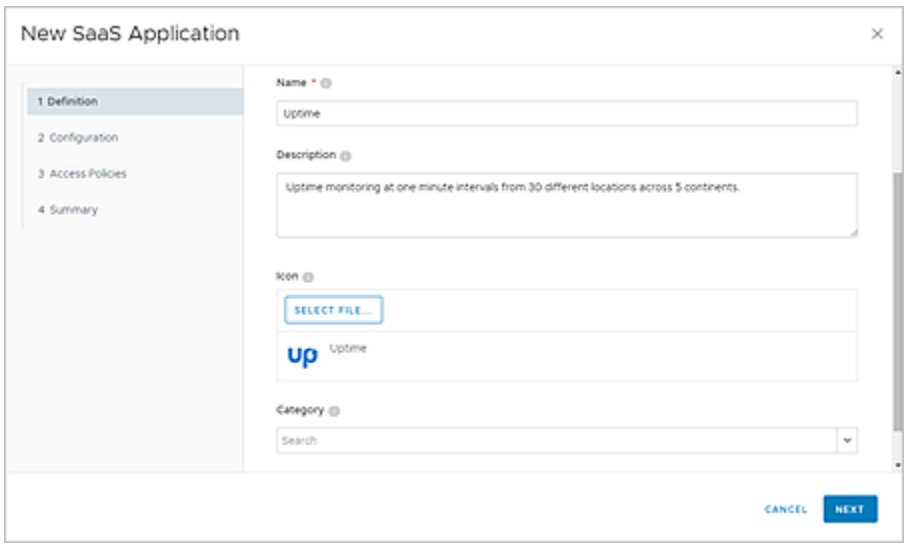


3 Click **New**.

The New SaaS Application wizard appears.

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

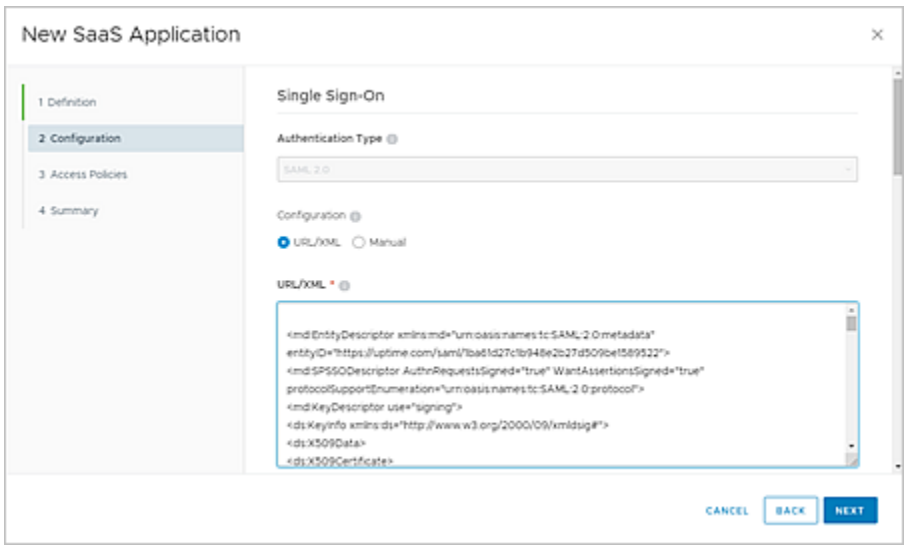
The Definition page displays the Uptime name and description. If you want, use the **Category** setting to display Uptime under a specific category in the Workspace ONE portal.



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

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

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	Populated with the SAML profile.
Configuration	To configure the SSO settings automatically based on the Uptime service provider metadata, select **URL/XML**.
URL/XML	In the text box, paste the contents of the Uptime service provider metadata .xml file that you saved previously when you configured settings in Uptime. The VMware Identity Manager service automatically configures the SSO settings for Uptime based on the service provider metadata.

Setting	Description
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 setting blank if your application service provider already has a workflow for redirecting users.
Application Parameters	Correspond to your Uptime account profile. To integrate Uptime with the VMware Identity Manager service, you must configure the **accountID** parameter. For Value, enter the Uptime account ID that you saved previously when you configured settings in Uptime.
Advanced Properties	Expand the Advanced Properties 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 Uptime. ■ **Sign Assertion**: Set to **Yes** to sign the SAML assertion contained within the SAML response. ■ **Custom Attribute Mapping**: Populated with the attributes **FirstName**, **UserName**, **Email**, **LastName**. Accept all the default formats and values.
Open in VMware Browser	Set to **Yes** if you want to open Uptime 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 Uptime application appears in the Workspace ONE portal.

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

The VMware Identity Manager service includes a default policy that is automatically assigned to the Uptime 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 Uptime. 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 Uptime, 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 Uptime across your organization, test and verify the SSO configuration with a few test users.

This chapter includes the following topics:

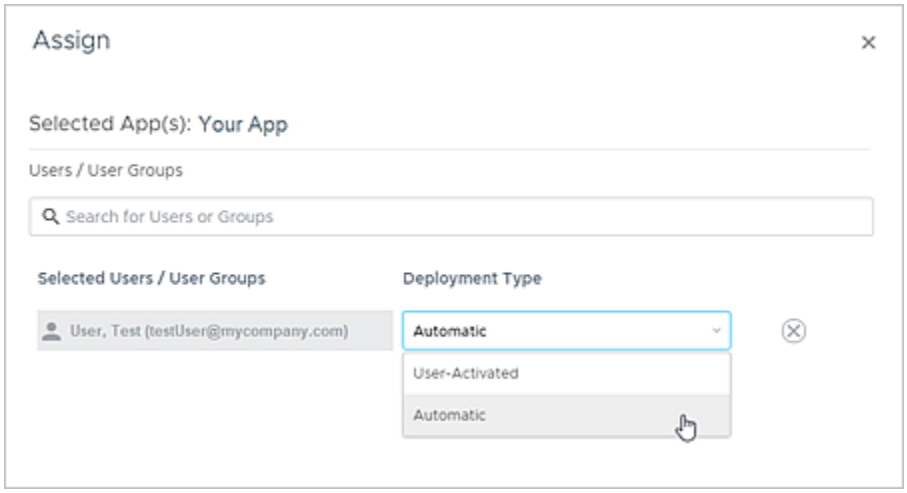
Set Up a Test User in the VMware Identity Manager Console

To set up a test user in the VMware Identity Manager console, you assign Uptime as a resource to that user. This assignment allows the test user to access Uptime 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 Uptime 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 Uptime.

7 Click **Save**.

What to do next

Set up the test user in Uptime.

Set Up the Test User In Uptime

To set up the test user in Uptime, create a user whose profile matches that of the test user you set up earlier in the VMware Identity Manager console.

Note The following procedure provides general guidelines for setting up a user in Uptime. For the most up-to-date, detailed instructions, see the Uptime documentation or consult with your Uptime account representative.

Prerequisites

Set up a test user in the VMware Identity Manager console.

Procedure

1 In Uptime, log in as an administrator and navigate to the **Settings > Users** page.

2 Click **New User**.

3 On the Add Account User page, configure the following settings. Ensure that the information entered matches the test user information in the VMware Identity Manager console.

Setting	Description
First Name	First name of the test user.
Last Name	Last name of the test user.

Setting	Description
Email Address	Email address of the test user.
Password	Password used by the test user to log in to Uptime.
Timezone	Can be set to any value for the test user.
Access Level	Can be set to any value for the test user.

4 Accept the default values for all other settings, and click **Save**.

What to do next

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

Verify SSO for the Test User

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

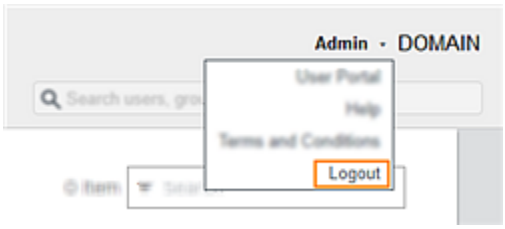
Prerequisites

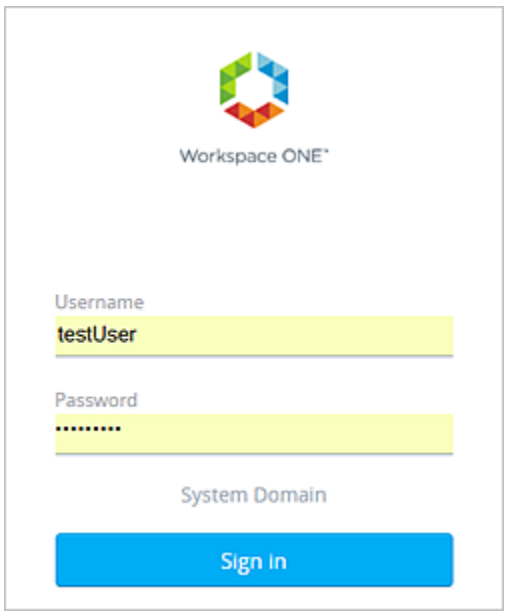
- Set up the test user in the VMware Identity Manager console.
- Set up the test user in Uptime.

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 Uptime by clicking the application icon in the catalog.

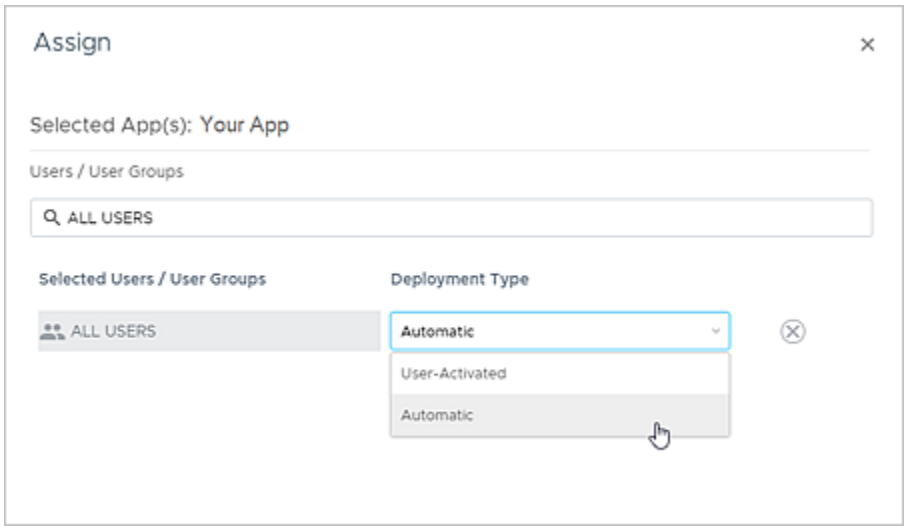
If SSO has been configured successfully, the test user can now access Uptime without being prompted to enter credentials again.

5 Assign the Application to Users

After you verify the SAML SSO configuration, you can deploy Uptime 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 Uptime 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 Uptime.
   - Select **User-Activated** if you plan to set up an approval flow for access to Uptime. In an approval flow, users must request access to Uptime and the request must be approved before they can use the application.
6. Click **Save**.

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