VMware Identity Manager Integration with ServiceNow

JUL 2019 V4

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

ServiceNow intelligently automates business tasks and workflows to integrate systems, people, and data across the enterprise. 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 ServiceNow to the catalog and configure SSO settings, users only need to enter their credentials one time in the Workspace ONE portal. ServiceNow 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 ServiceNow.

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

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

Configuring SSO Settings in ServiceNow

2

You set up ServiceNow 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. ServiceNow requires both of these SAML components to set up the VMware Identity Manager service as its identity provider.

Note To ensure compatibility with the ServiceNow authentication settings, save the URL of the SAML metadata to a .txt file on your computer. Copy and save the contents of the SAML signing certificate as a .pem file on your computer.

This chapter includes the following topics:

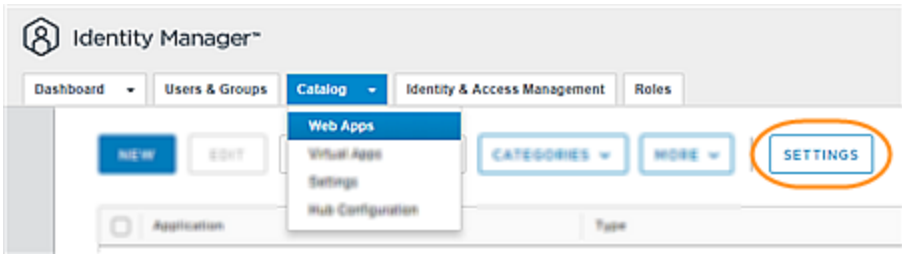
Obtain the VMware Identity Manager SAML Metadata

ServiceNow 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.

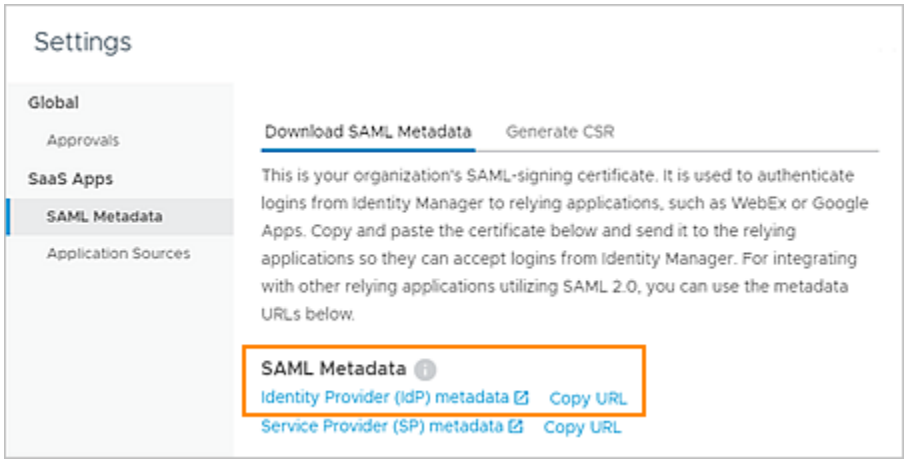


3 Click **Settings** and then select **SAML Metadata**.

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.

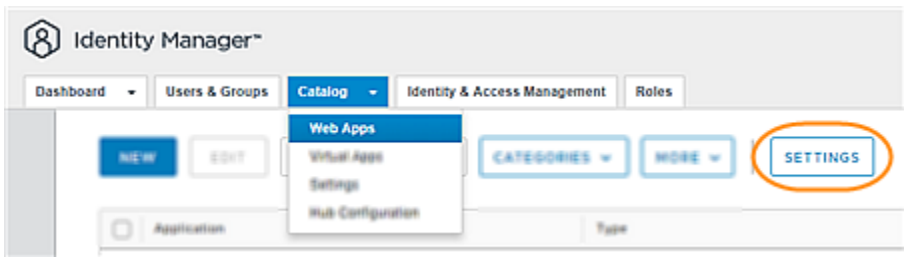
Obtain the VMware Identity Manager SAML Signing Certificate

ServiceNow 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 ServiceNow originate from the VMware Identity Manager service.

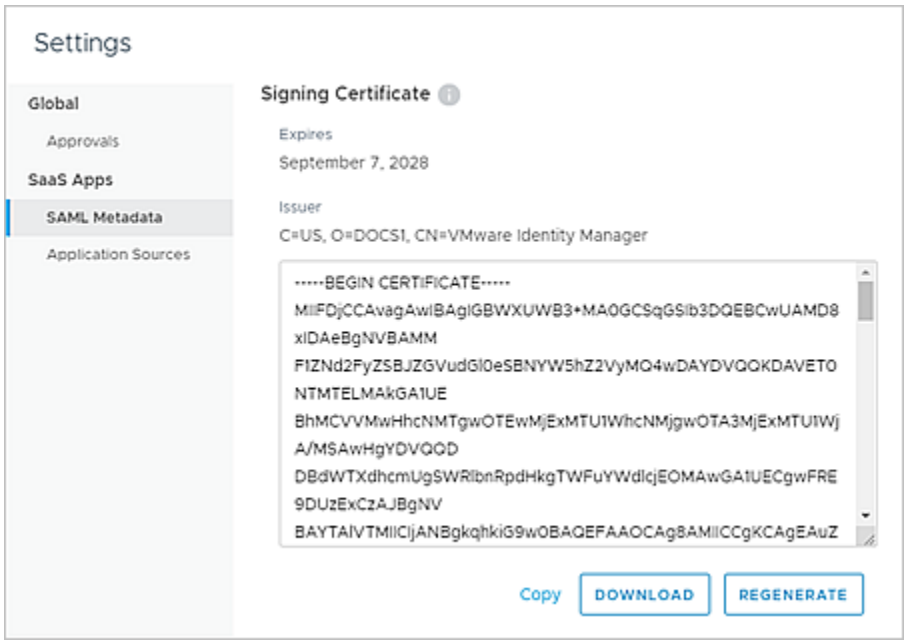
Procedure

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 ServiceNow

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

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

If you create a SAML 2.0 configuration using Multi-Provider SSO, make sure that the Signing/Encryption Key Alias set in the Encryption and Signing tab is **saml2sp**.

Prerequisites

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

Procedure

1. In ServiceNow, log in as an administrator and navigate to **SAML2 Single Sign-on > Certificate**.
2. Click **New**.
3. In the Name text box, enter **SAML 2.0**.

   Note If the name is not SAML 2.0, ServiceNow fails to recognize the SAML signing certificate.
4. In the Format text box, enter `PEM`.
5. In the PEM Certificate text box, paste the text from the SAML signing certificate file that you saved previously. Make sure that you include text from -----BEGIN CERTIFICATE---- through ---------END CERTIFICATE-----.
6. Click **Submit**.
7. Navigate to **SAML2 Single Sign-on > Properties**.
8. On the SAML 2.0 Single Sign-on page, configure settings as required by your organization.

   For the example URLs in the following table, replace the placeholder text with the appropriate domain names defined by your organization.

   - Replace `myco.vmwareidentity.com` with your organization's domain name for the VMware Identity Manager service.
   - Replace `company` with your organization's domain name for ServiceNow.

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

Setting	Description
Enable External Authentication	Select **Yes**.
The Identity Provider URL which will issue the SAML2 security token with user info	This value is 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`
The base URL to the Identity Provider's AuthnRequest service….	Enter the VMware Identity Manager login URL in this format: `https://myco.vmwareidentity.com/SAAS/API/1.0/POST/sso`
The base URL to the Identity Provider's SingleLogoutRequest service…	Enter the VMware Identity Manager logout URL in this format: `https://myco.vmwareidentity.com/SAAS/API/1.0/GET/logout`
When SAML 2.0 single sign-on fails because the session is not authenticated, or if this is the first login, redirect to this URL	Enter the VMware Identity Manager login URL in this format: `https://myco.vmwareidentity.com/SAAS/API/1.0/POST/sso`

Setting	Description
URL to redirect users after logout, typically back to the portal that enabled the SSO	Enter the VMware Identity Manager logout URL in this format: `https://myco.vmwareidentity.com/logout`
The URL to the Service-now instance homepage	Enter the ServiceNow instance URL in this format: `https://company.service-now.com/navpage.do`
The entity identification, or the issuer	Enter the ServiceNow entity identification URL in this format: `https://company.service-now.com`
The audience uri that accepts SAML2 token	Enter the same URL as the ServiceNow entity identification URL: `https://company.service-now.com`

9 Click **Save**.

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 ServiceNow to the catalog and configuring application settings.

This chapter includes the following topics:

- Add ServiceNow to the Catalog

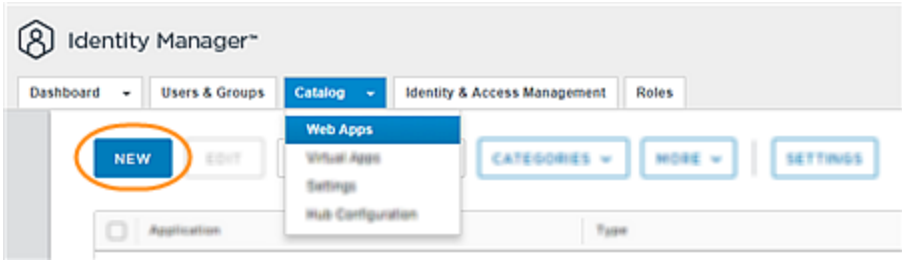
Add ServiceNow to the Catalog

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

Procedure

1 Log in to the VMware Identity Manager console.

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

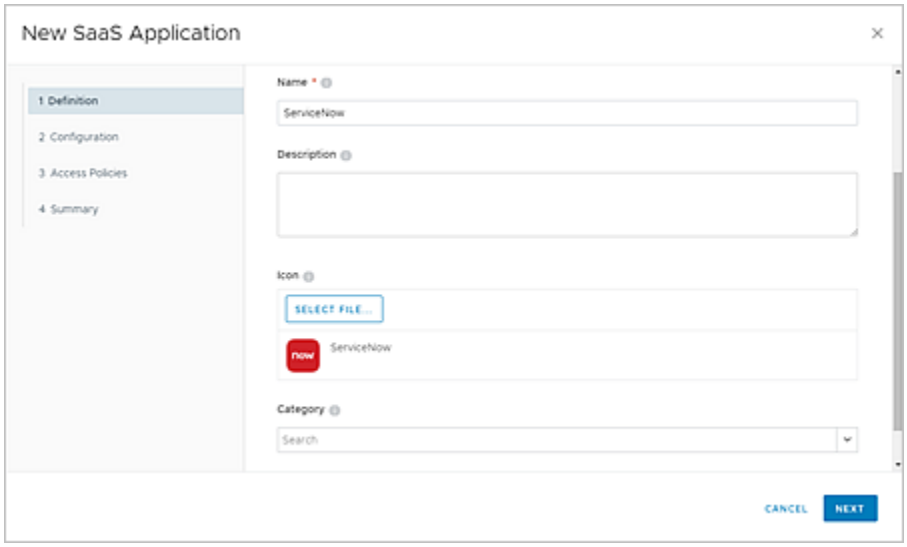


3 Click **New**.

The New SaaS Application wizard appears.

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

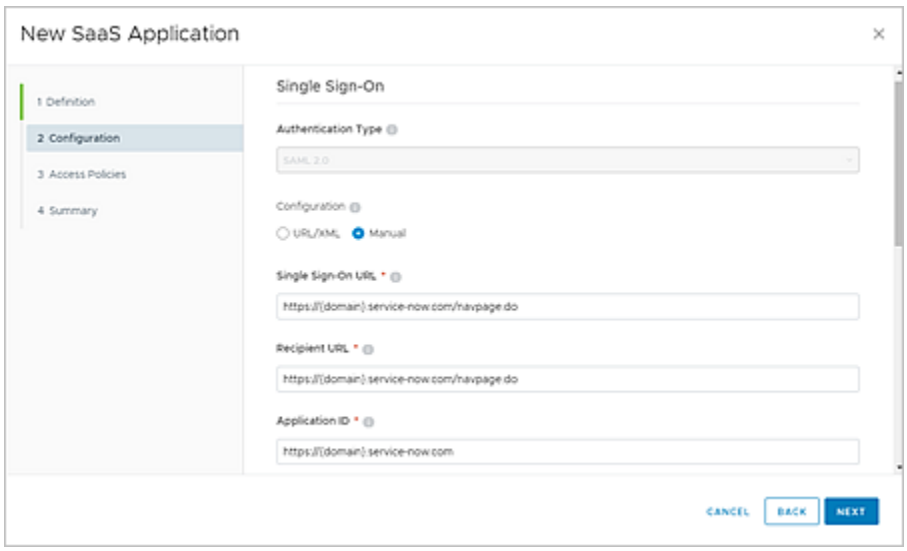
The Definition page displays the ServiceNow name and description. If you want, use the **Category** setting to display ServiceNow under a specific category in the Workspace ONE portal.



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 ServiceNow 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	Populated with the SAML profile.
Configuration	Select **Manual**.

Setting	Description
Single Sign-On URL	Also known as the Assertion Consumer Services URL. The VMware Identity Manager service sends SAML assertions to this URL during the SSO process. Accept the default value of `https://{domain}.service-now.com/navpage.do`, or enter the URL provided by your ServiceNow account administrator. If you accept the default value, replace `{domain}` with your organization's domain name for the ServiceNow tenant.
Recipient URL	Describes the valid domain for receiving SAML assertions. 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 of `https://{domain}.service-now.com`, or enter the URL provided by your ServiceNow account administrator. If you accept the default value, replace `{domain}` with your organization's domain name for the ServiceNow tenant.
Username Format	Specifies the SAML subject format for the processing of SAML assertions. Accept the default value of **Email Address**.
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 of **${user.email}**.
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 single sign-on credentials. Leave this setting blank if your application service provider already has a workflow for redirecting users.
Application Parameters	Correspond to your ServiceNow account profile. To integrate ServiceNow with the VMware Identity Manager service, you must configure the **domain** parameter. For Value, enter your organization's domain name for the ServiceNow tenant.
Advanced Properties	Expand the Advanced Properties section, and configure required settings as follows. 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**: ServiceNow does not require any custom attribute mappings for the SSO setup. You can leave the Custom Attribute Mapping table blank.
Open in VMware Browser	Set to **Yes** if you want to open ServiceNow 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 ServiceNow application appears in the Workspace ONE portal.

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

The VMware Identity Manager service includes a default policy that is automatically assigned to the ServiceNow 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 ServiceNow. 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 ServiceNow, 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 ServiceNow 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

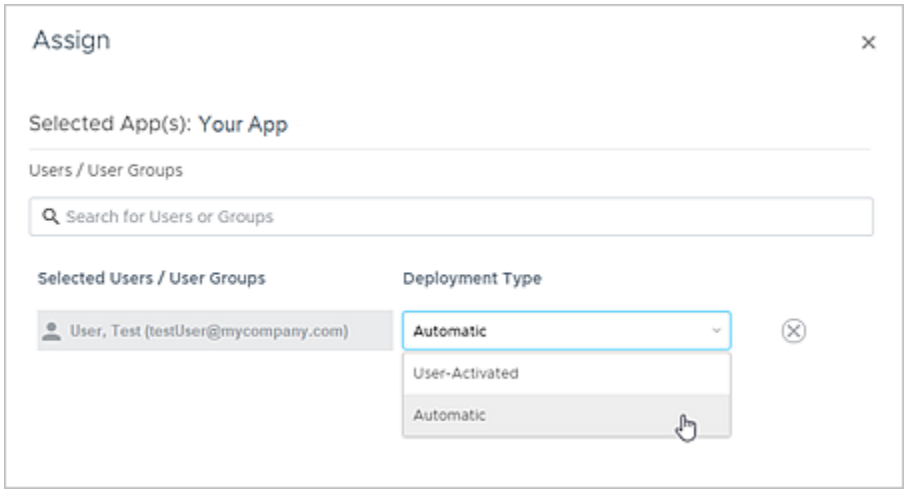
To set up a test user in the VMware Identity Manager console, you assign ServiceNow as a resource to that user. This assignment allows the test user to access ServiceNow from the Workspace ONE portal and test SSO capabilities.

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 and has a valid email address.

   Ensure that the user information matches the test user information in ServiceNow.
3. Select the **Catalog > Web Apps** tab.
4. Select the check box next to ServiceNow 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 ServiceNow.

7 Click **Save**.

What to do next

Set up the test user in ServiceNow.

Set Up the Test User In ServiceNow

To set up the test user in ServiceNow, 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 ServiceNow. For the most up-to-date, detailed instructions, see the ServiceNow documentation or consult with your ServiceNow account representative.

Prerequisites

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

Procedure

1 In ServiceNow, log in as an administrator and navigate to the **User Administration > Users** page.

2 Click **New**.

3 Configure the following required settings. Ensure that the information entered matches the test user information in the VMware Identity Manager console.

Setting	Description
UserID	User ID address for the test user. Must be the same user as created in the VMware Identity Manager console.
First name	First name of the test user.
Last name	Last name of the test user.
Email	Email address of the test user. The email address must match the email address of the test users in the VMware Identity Manager console.

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

What to do next

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

Verify SSO for the Test User

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

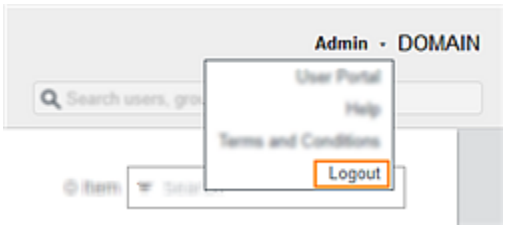
Prerequisites

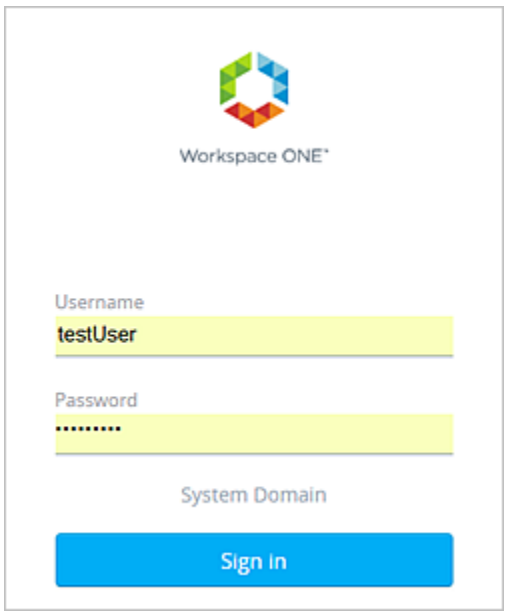
- Set up the test user in the VMware Identity Manager console.
- Set up the test user in ServiceNow.

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 ServiceNow by clicking the application icon in the catalog.

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

Assign the Application to Users

5

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

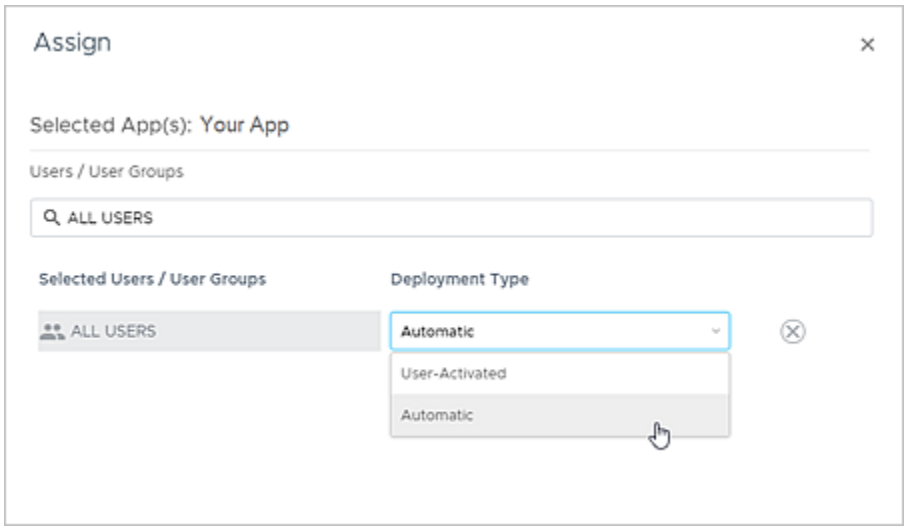
Procedure

1 Log in to the VMware Identity Manager console.

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

3 Select the check box next to ServiceNow 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 ServiceNow.
- Select **User-Activated** if you plan to set up an approval flow for access to ServiceNow. In an approval flow, users must request access to ServiceNow and the request must be approved before they can use the application.

6 Click **Save**.

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