VMware Identity Manager Integration with Salesforce

JAN 2019 V2

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

Salesforce is a customer relationship management (CRM) platform that provides cloud-based applications for sales, service, marketing, and more. 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 Salesforce to the catalog and configure SSO settings, users only need to enter their credentials one time in the Workspace ONE portal. Salesforce 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 Salesforce.

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

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

Configuring SSO Settings in Salesforce 2

You set up Salesforce 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 and SAML signing certificate associated with the VMware Identity Manager service. Salesforce requires both of these SAML components to set up VMware Identity Manager as its identity provider.

Note To ensure compatibility with the Salesforce authentication settings, copy and save the SAML metadata URL to a .txt file on your computer. Download the SAML signing certificate as a .cer file and save the file on your computer.

This chapter includes the following topics:

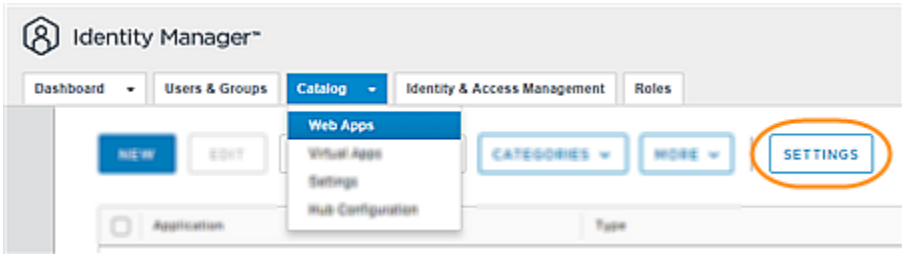
Obtain the VMware Identity Manager SAML Metadata

Salesforce 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.

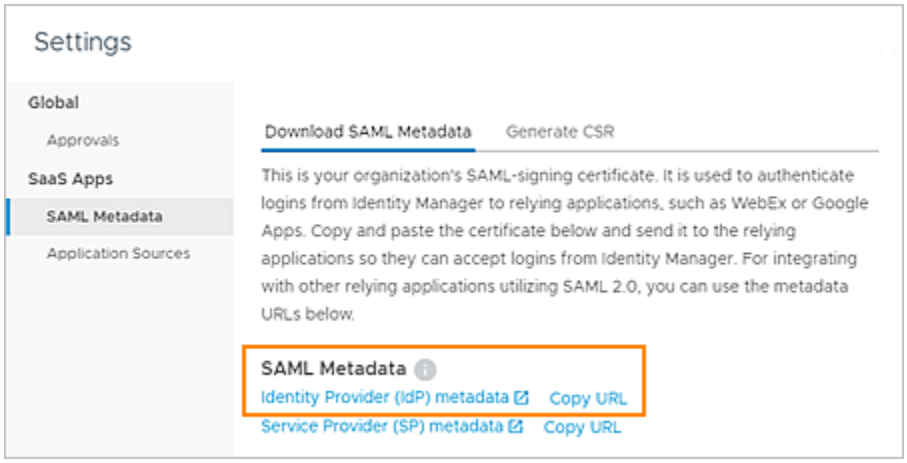


3 Click **Settings** and then select **SAML Metadata**.

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.

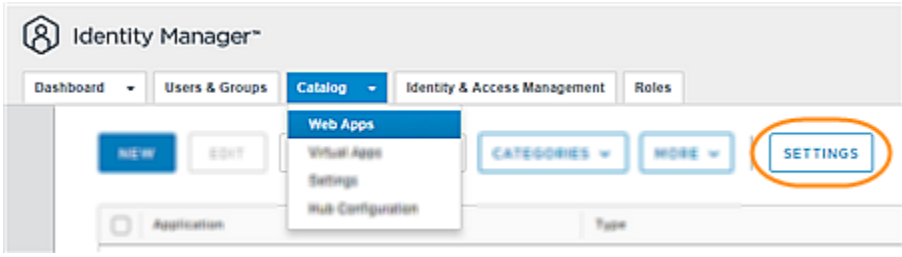
Obtain the VMware Identity Manager SAML Signing Certificate

Salesforce 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 Salesforce originate from the VMware Identity Manager service.

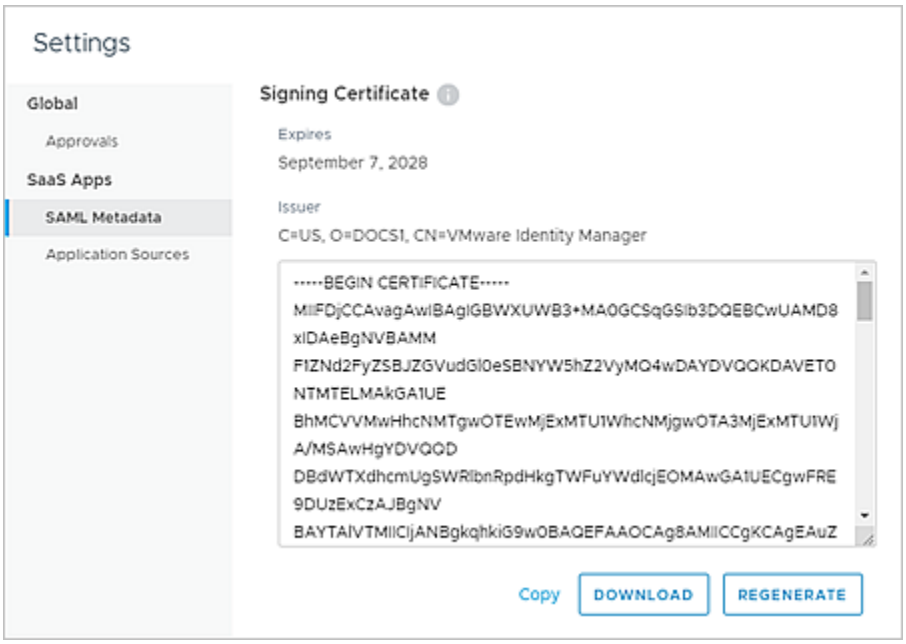
Procedure

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 Salesforce

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

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

Prerequisites

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

Procedure

1. In Salesforce, log in as an administrator and navigate to the **Setup > Settings > Identity > Single Sign-On Settings** page.
2. At the top of the Federated Single Sign-On Using SAML section, click **Edit**. Select **SAML Enabled** and then click **Save**.
3. In the SAML Single Sign-On Settings section, click **New**.
4. 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
Name	Enter the name that refers to the VMware Identity Manager service.
Issuer	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.
Identity Provider Certificate	The signing certificate that establishes the VMware Identity Manager service as the identity provider. Upload the SAML signing certificate .cer file that you downloaded previously.
SAML Identity Type	Select **Assertion contains User's Salesforce.com username**.
SAML Identity Location	Select **Identity is the NameIdentifier element of the Subject statement**.
API Name	The unique name used by the API and managed packages to refer to the VMware Identity Manager service. Use only alphanumeric characters and underscores for the name; the first character must be a letter. The name cannot contain two consecutive underscores or end in an underscore.
Entity ID	Enter this URL: `https://saml.salesforce.com`

Setting	Description
Identity Provider Login URL	Enter the VMware Identity Manager login URL in this format: **`https://myco.vmwareidentity.com/SAAS/API/1.0/POST/sso`**, where **`myco.vmwareidentity.com`** is replaced with your organization's domain name for the VMware Identity Manager service.
Single Logout Enabled	Select this option if you want to log users out of their VMware Identity Manager session after they log out of Salesforce. For **Identity Provider Single Logout URL**, enter the logout URL in this format: **`https://myco.vmwareidentity.com/SAAS/auth/logout`**, where **`myco.vmwareidentity.com`** is replaced with your organization's domain name for the VMware Identity Manager service.

5 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 Salesforce to the catalog and configuring application settings.

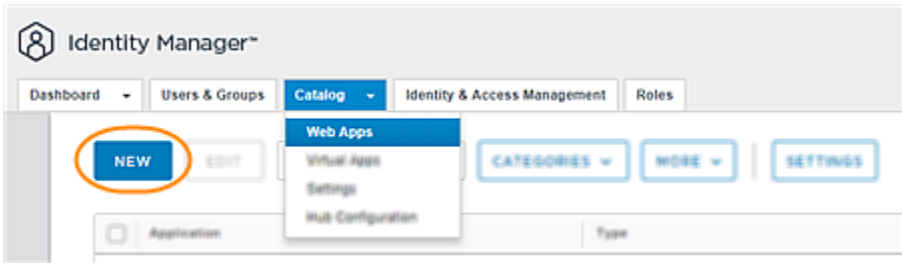
Add Salesforce to the Catalog

Adding Salesforce to the catalog makes the application available as a resource that users can access from the Workspace ONE portal. You enable SSO to Salesforce 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.

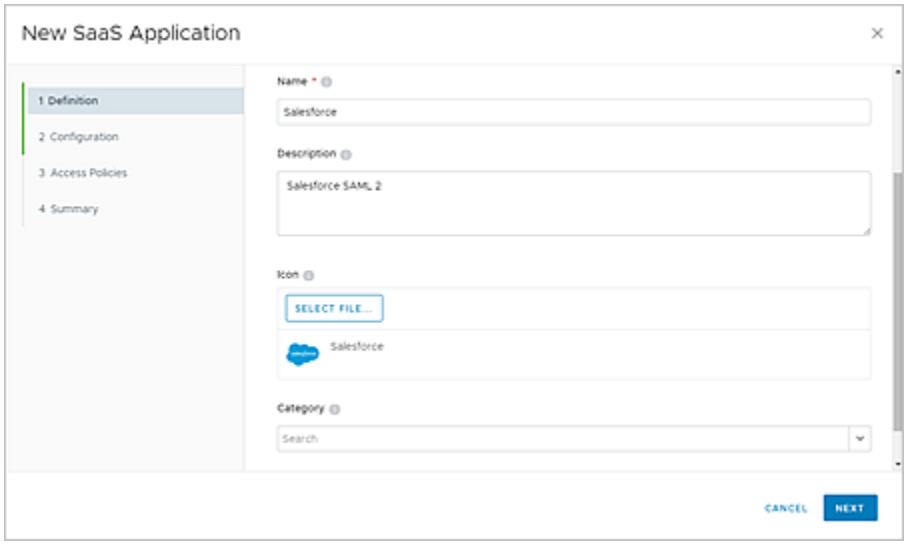


3 Click **New**.

The New SaaS Application wizard appears.

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

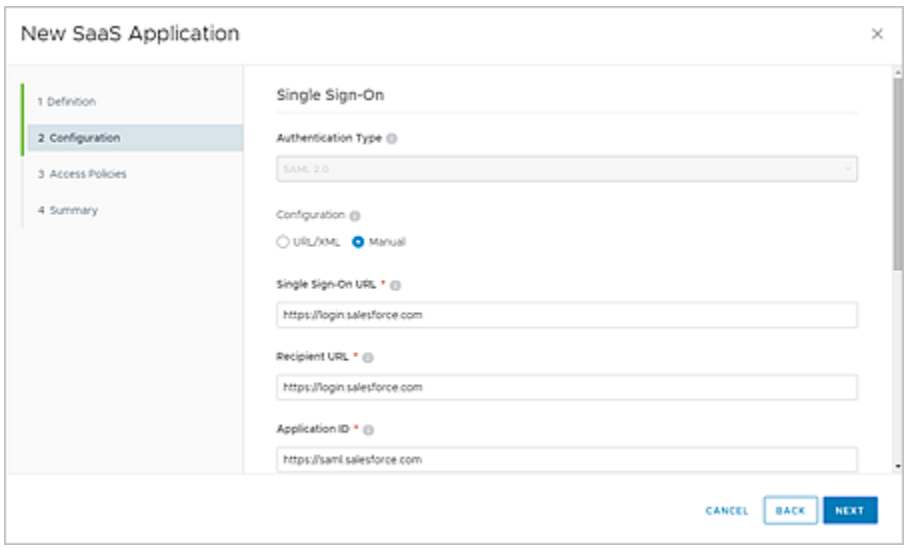
The Definition page displays the Salesforce name and description. If you want, use the **Category** setting to display Salesforce under a specific category in the Workspace ONE portal.



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 Salesforce 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**.
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, or enter the URL provided by your Salesforce account administrator.

Setting	Description
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, or enter the URL provided by your Salesforce account administrator.
Username Format	Specifies the SAML subject format for the processing of SAML assertions. Accept the default format of **Email Address**, or select the format provided by your Salesforce account administrator.
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}**, or enter the value provided by your Salesforce account administrator.
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.
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**: Salesforce 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 the VMware Identity Manager service to open Salesforce 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 Salesforce application appears in the Workspace ONE portal.

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

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

This chapter includes the following topics:

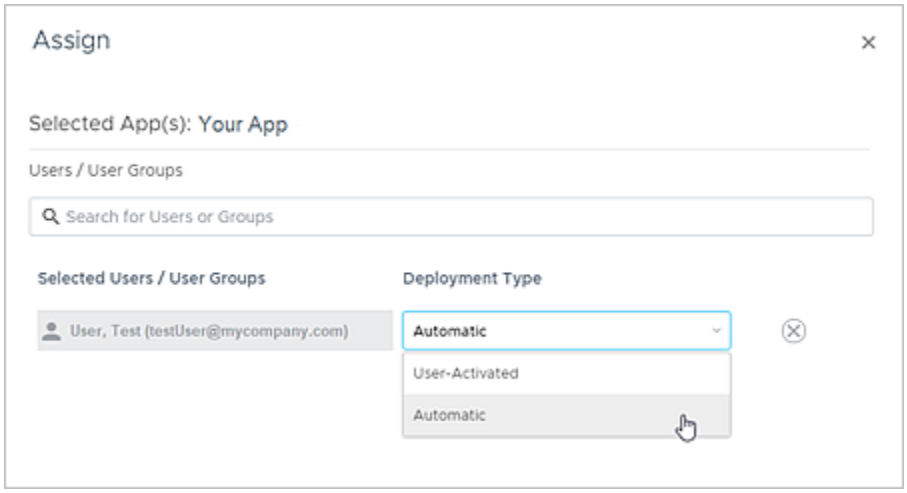
Set Up a Test User in the VMware Identity Manager Console

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

7 Click **Save**.

What to do next

Set up the test user in Salesforce.

Set Up the Test User In Salesforce

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

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

Prerequisites

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

Procedure

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

2 On the **All Users** page, click **New User**.

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

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

Setting	Description
Last name	Last name of the test user.
Alias	Last name of the test user.
Email	Email address of the test user.
Username	Email address of the test user.
Nickname	Can be set to any value for the test user.
Role	Can be set to any value for the test user.
User License	Can be set to any value for the test user.
Profile	Can be set to any value for the test user.
Email Encoding	Can be set to any value for the test user.
Time Zone	Can be set to any value for the test user.
Locale	Can be set to any value for the test user.
Language	Can be set to any value for the test user.

4 Click **Save**.

What to do next

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

Verify SSO for the Test User

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

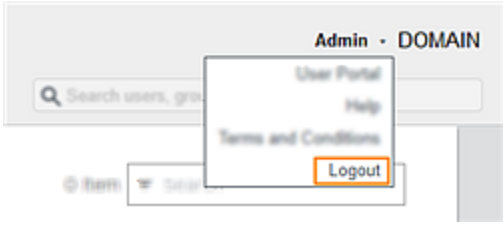
Prerequisites

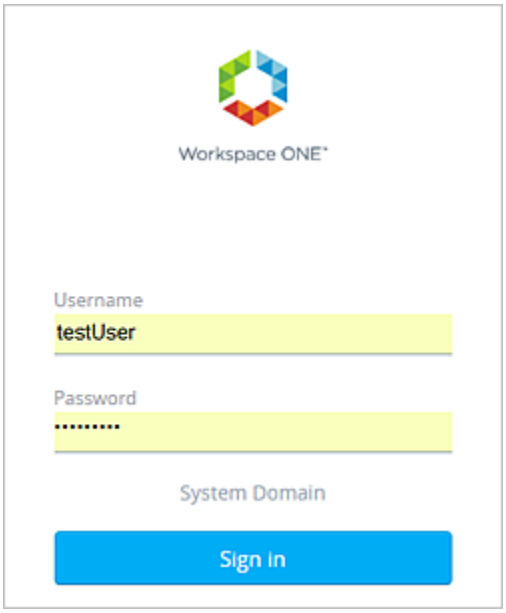
- Set up the test user in the VMware Identity Manager console.
- Set up the test user in Salesforce.

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 Salesforce by clicking the application icon in the catalog.

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

Assign the Application to Users

5

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

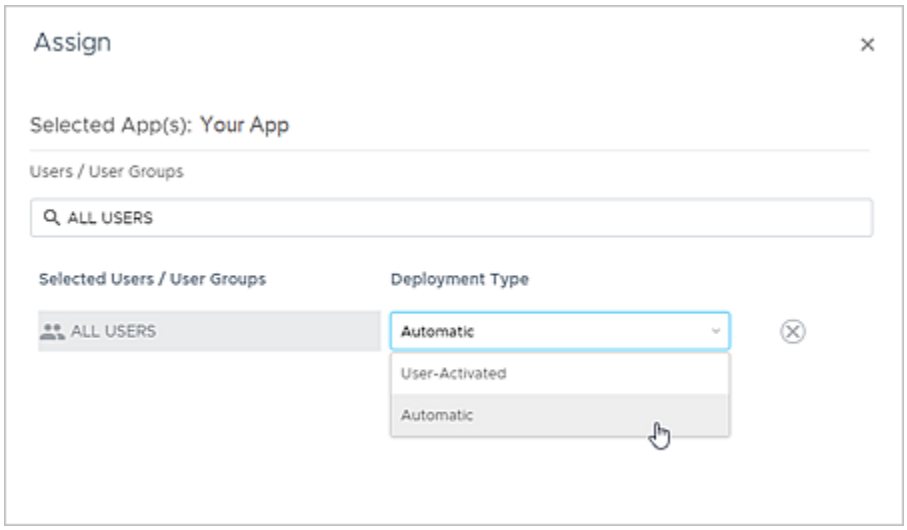
Procedure

1 Log in to the VMware Identity Manager console.

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

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

6 Click **Save**.

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