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

VMware Identity Manager

NOVEMBER 2015 V1

vmware

Table of Contents

Overview

This document provides information about configuring SAML-based single sign-on from the VMware Identity Manager service to ScreenSteps.

ScreenSteps is an application that enables you to create visual user documentation, including articles, how-to-guides, and manuals.

You add ScreenSteps to the VMware Identity Manager catalog and enable SAML authentication in ScreenSteps to allow users logged into the service to have single sign-on access to ScreenSteps.

You must have an administrator account for the VMware Identity Manager service, as well as an administrator account for ScreenSteps.

Adding ScreenSteps to VMware Identity Manager Catalog

To enable single sign-on to ScreenSetps on the service, you must configure the application in the catalog and copy the SAML-signing certificate to ScreenSteps.

Add ScreenSteps 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 **ScreenSteps** icon.

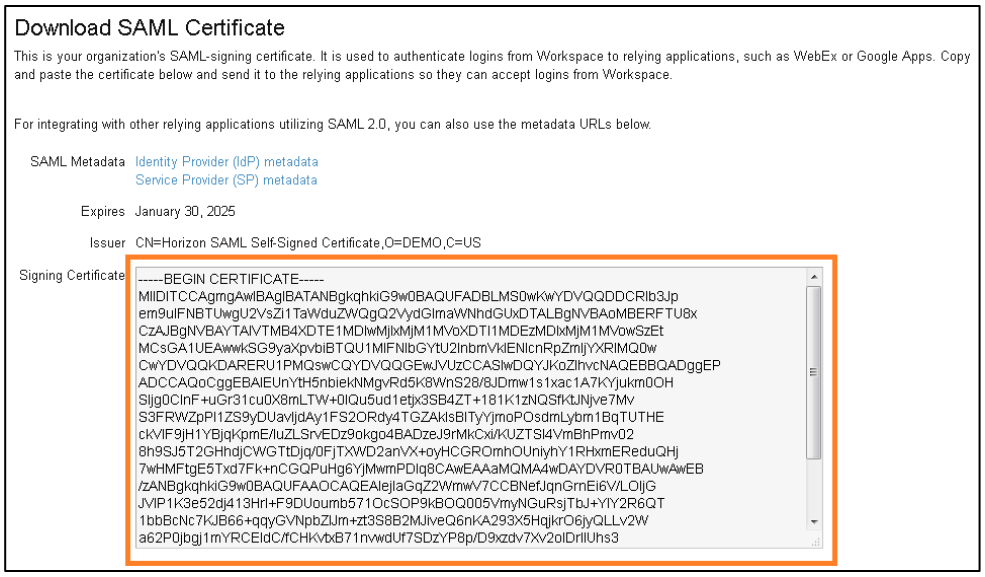
   The Modify application page appears.

   ScreenSteps is added to the catalog but is not configured. You complete the application setup in the catalog after you configure single sign-on in ScreenSteps.

Download SAML-Signing Certificate

You must have the SAML-signing certificate from the VMware Identity Manager service for the ScreenSteps configuration.

1. In the **Catalog > Settings** tab, click **SAML Metadata**.
2. Copy and save the **Signing Certificate** text to a text file on your computer. Make sure that you include text from -----BEGIN CERTIFICATE---- through ---------END CERTIFICATE-----.

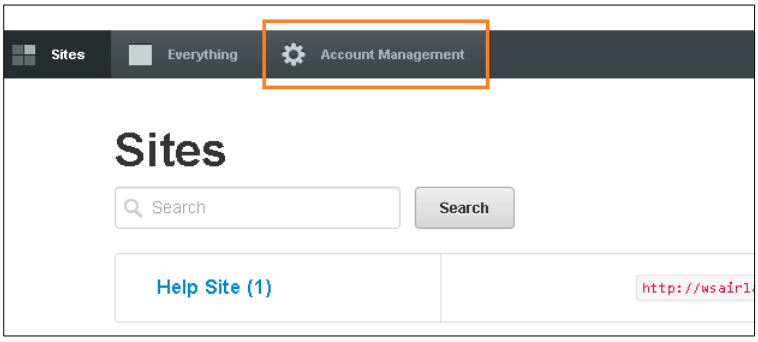


Setting up ScreenSteps

To configure ScreenSteps for single sign-on from the service, you set up single-sign on in ScreenSteps and upload the VMware Identity Manager SAML-signing certificate.

Configure ScreenSteps

1. Log in to ScreenSteps as administrator.
2. Click the **Admin** link.
3. Click the **Account Management** tab.

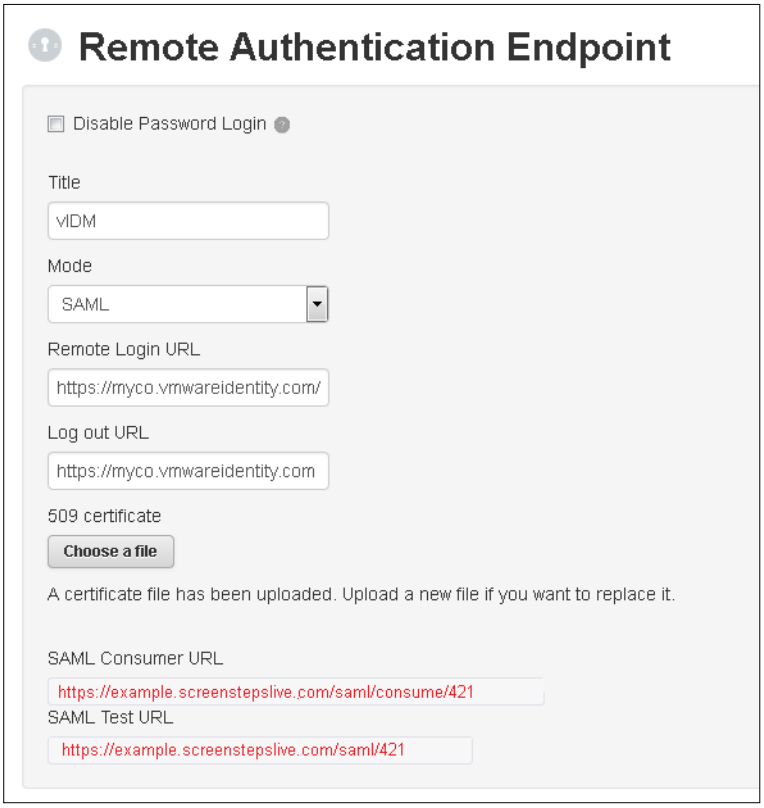


4. Click **Remote Authentication** in the left pane.
5. In the Remote Authentication Endpoint page, enter the following information.

OPTION	VALUE
Disable Password Login	Select the checkbox.
Title	Name of the authentication endpoint. For example, **VMware Identity Manager**.
Mode	Select **SAML**.
Remote Login URL	Enter the VMware Identity Manager single sign-on URL in the following format:

	https://*myco.vmwareidentity.com*/SAAS/auth/federation/sso Replace *myco.vmwareidentity.com* with your company's VMware Identity Manager service domain name.
Log out URL	Enter your VMware Identity Manager logout URL. If you want the logout URL to return users to the VMware Identity Manager service, enter your logout URL in the following format: **https://*myco.vmwareidentity.com***
509 certificate	Click **Choose a file** and upload the SAML-signing certificate you copied from the VMware Identity Manager administration console.

For example:

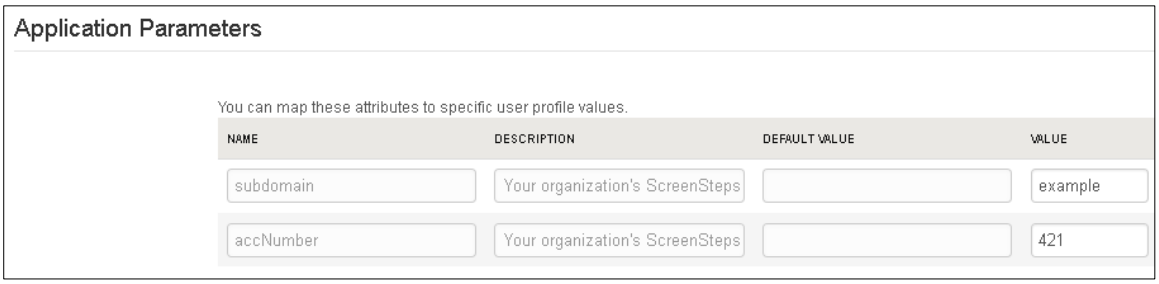


6. Click **Save**.
7. Make a note of the value of **the SAML Consumer URL** field. You need this information to complete the application configuration in the VMware Identity Manager administration console.

Complete the Setup in the Service

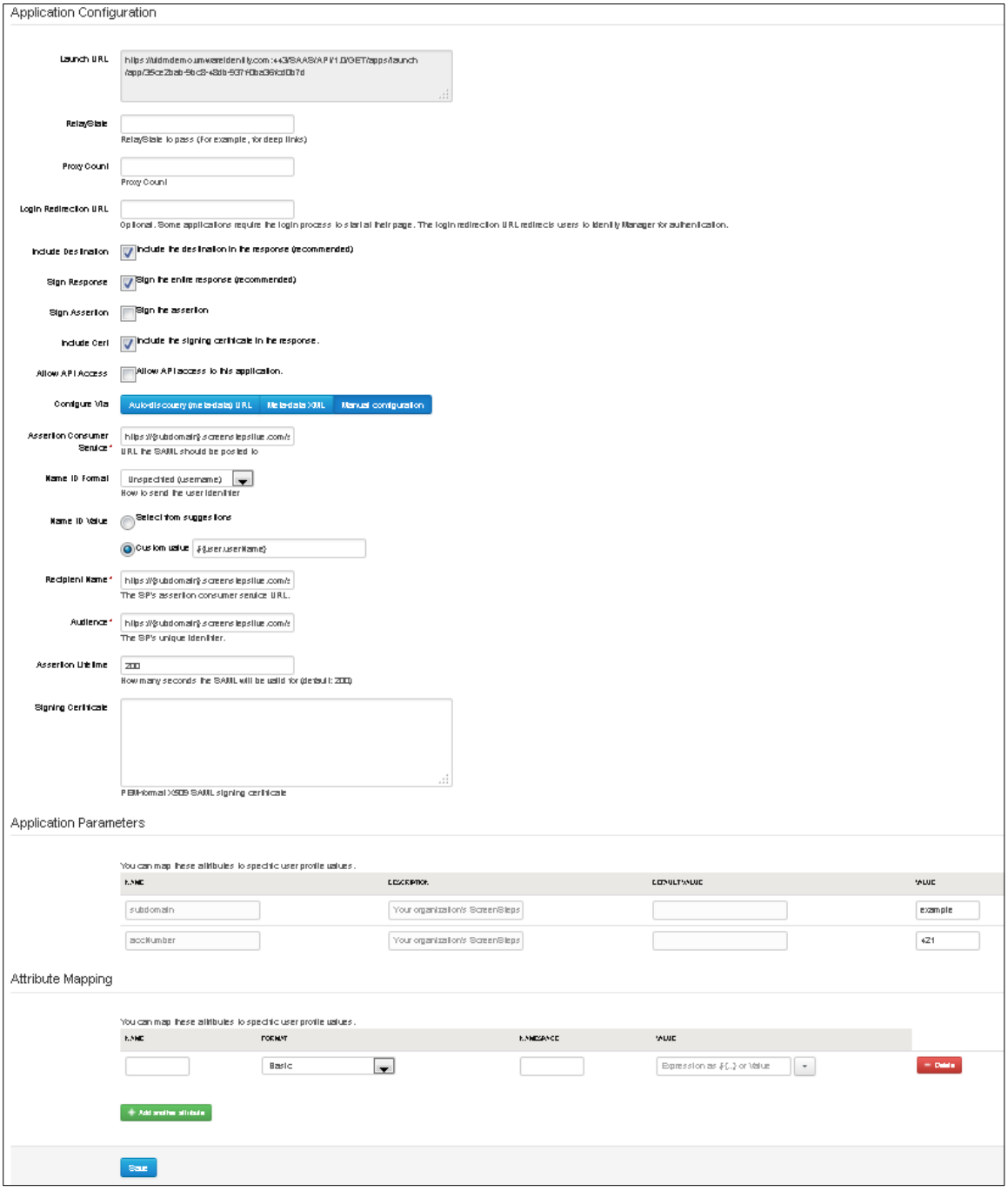
1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, select the ScreenSteps icon.
3. In the Modify application page, click **Configuration**.
4. In the **Application Parameters** section, set the value of the **subdomain** and **accNumber** parameters based on the SAML Consumer URL from ScreenSteps. For example, if the SAML Consumer URL is

https://example.screenstepslive.com/saml/consume/421, then you would set **subdomain** to **example** and **accNumber** to **421**.



5. Click **Save**.

   Verify that the Application Configuration page is similar to this example.



Testing Single Sign-on Configuration

Test your single sign-on configuration with a small number of users before deploying the application across your organization.

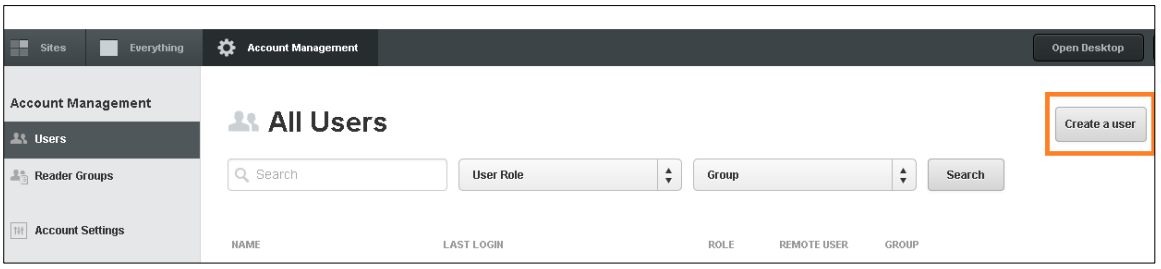
Set up User in VMware Identity Manager for Testing

1. Log in to the VMware Identity Manager administration console.
2. In the **Users & Groups** page, click **Users** and ensure that the user you are testing is in the list of users.
3. In the **Catalog** page, click **ScreenSteps**.
4. Click **Entitlements**.
5. Click +**Add user entitlement**.
6. Select the test user and change the **DEPLOYMENT** field value for the user to **Automatic**. For example:

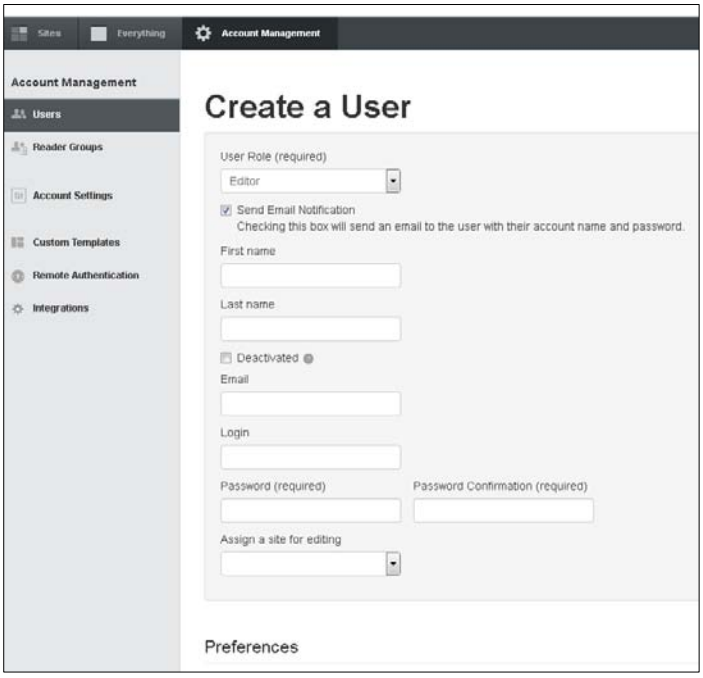
7. Click **Save**, then click **Done**.
8. In the top-right corner of the page, click your user name and select **Logout**.

Set up User in ScreenSteps for Testing

1. Log in to the ScreenSteps site as administrator.
2. Click the **Admin** link.
3. Click the **Account Management** tab.
4. In the Users page, click **Create a User**.



5. Select a user role and enter the user information.



6. Click **Create User**.

Next, verify that the test user can sign in to the My Apps portal.

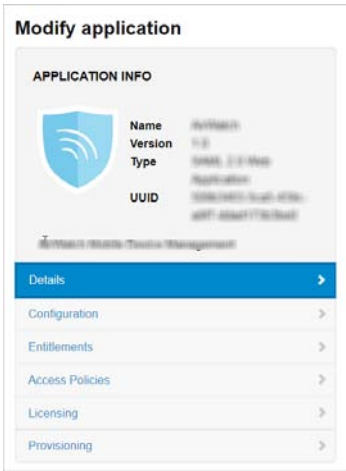
Verify Test-User can Sign into ScreenSteps

1. Sign in to the user portal as the test user.
2. Click the **ScreenSteps** icon on the My Apps page.

   You should now have single sign-on access to ScreenSteps.

Completing the Configuration in the Catalog

In addition to configuring the Web application for single sign-on to the service, you can configure additional settings to add an access policy, set up app licensing requirements, and entitle users and groups to the application.



Entitlements After you configure a Web application, you can add group entitlements and entitle individual users to the Web application.

Access Policies The VMware Identity Manager service includes a default policy that is automatically assigned to the Web app when you add the app to the Catalog. If you do not want to use the default access policy, create a new access policy and in the Access Policies link, select the access policy to use for this Web application.

For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity Manager documentation at http://pubs.vmware.com.

Licensing Licensing can be used to require users to request license approval before they can access the application. You can add additional information, including pricing, license type, cost per license and the number of licenses. You can run the Resource Usage report to see the licensing information for the application.

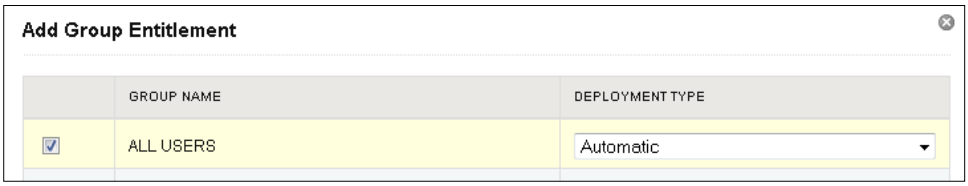
Provisioning Provisioning provides automatic application user-management from a single location. Provisioning adapters allow the Web application to retrieve specific information from VMware Identity Manager, as required. The provisioning adapters that can be selected are either Google Apps, Mozy, or Vchs. If you configure these applications, you can select the appropriate provisioning adapter.

Entitle Users to ScreenSteps

You can activate single sign-on for all users. Before you do so, ensure that all the user accounts are provisioned in ScreenSteps.

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **ScreenSteps**.

3. In the **Modify application** page, click **Entitlements**.
4. Click +**Add group entitlement**.
5. Select **ALL USERS** and change the **DEPLOYMENT TYPE** field value to **Automatic**.



6. Click **Save,** then click **Done**.

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