



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

VMware Identity Manager

NOVEMBER 2015 V1

Table of Contents

- Overview 1
- Adding Freshservice to VMware Identity Manager Catalog 1
 - Add Freshservice to the Catalog 1
 - Download SAML-Signing Certificate and Obtain the SHA1 Certificate Fingerprint 2
- Setting up Freshservice 3
 - Configure Freshservice..... 3
- Testing Single Sign-on Configuration 4
 - Set up User in VMware Identity Manager for Testing..... 4
 - Set up User in Freshservice for Testing 4
 - Verify Test-User can Sign into Freshservice 5
- Completing the Configuration in the Catalog 5
- Entitle Users to Freshservice 6

Overview

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

Freshservice provides cloud-based IT service desk software.

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

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

Adding Freshservice to VMware Identity Manager Catalog

To enable single sign-on to Freshservice on the service, you must configure the application in the catalog and copy the VMware Identity Manager SAML-signing certificate's SHA1 fingerprint to Freshservice.

Add Freshservice 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 **Freshservice** icon.
The Modify application page appears.
4. Select **Configuration** in the left pane.
5. In the **Application Parameters** section, set the value of the **subdomain** parameter to the name used in your Freshservice account. For example, if the Freshservice URL is `https://myco.freshservice.com`, set the value to **myco**.

For example:

Application Parameters			
You can map these attributes to specific user profile values.			
NAME	DESCRIPTION	DEFAULT VALUE	VALUE
subdomain	Your organization's Freshdesk su		myco

6. Click **Save**.

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

Application Configuration

Launch URL:

RelayState:
RelayState: to pass (for example, for deep links)

Proxy Count:
Proxy Count

Login Redirection URL:
Optional. Some applications require the login process to start at their page. The login redirection URL redirects users to Identity Manager for authentication.

Include Destination: Include the destination in the response (recommended)

Sign Response: Sign the entire response (recommended)

Sign Assertion: Sign the assertion

Include Cert: Include the signing certificate in the response.

Allow API Access: Allow API access to this application.

Configure Via:

Assertion Consumer Service:
URL the SAML should be posted to

Name ID Format:
How to send the user identifier

Name ID Value: Selection suggestions Custom value:

Recipient Name:
The SP's assertion consumer service URL.

Audience:
The SP's unique identifier.

Assertion Lifetime:
How many seconds the SAML will be valid for (default: 300)

Signing Certificate:
PEM-format X.509 SAML signing certificate

Application Parameters

You can map these attributes to specific user profile values.

ATTRIBUTE	EXPRESSION	DEFAULT VALUE	VALUE
subdomain	Your organization's Freshdesk sub		myco

Attribute Mapping

You can map these attributes to specific user profile values.

ATTRIBUTE	FORMAT	EXPRESSION	VALUE	Actions
<input type="text"/>	Basic	<input type="text"/>	Expression as { } or Value	<input type="button" value="Delete"/>

Download SAML-Signing Certificate and Obtain the SHA1 Certificate Fingerprint

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

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

Download SAML Certificate

This is your organization's SAML-signing certificate. It is used to authenticate logins from Workspace to relying applications, such as WebEx or Google Apps. Copy and paste the certificate below and send it to the relying applications so they can accept logins from Workspace.

For integrating with other relying applications utilizing SAML 2.0, you can also use the metadata URLs below.

SAML Metadata [Identity Provider \(IdP\) metadata](#)
[Service Provider \(SP\) metadata](#)

Expires: January 30, 2025

Issuer: CN=Horizon SAML Self-Signed Certificate,O=DEMO,C=US

Signing Certificate

```
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIBATANBgkqhkiG9w0BAQUFADBLS0wkwYDVQQDDCRlb3Jp
em9uIFNBTSUwZ2V5Zi1TaWduZWQgQ2VydGlnaWNhdGUxDTALBgNVBAoMBERFU8x
CzAJBgNVBAYTAiVUM0TE1MDWwMjM1MVoXDTI1MDEzMDkxMjM1MVoXDTI1MDEz
MCsGA1UEAwkxSG9yaXpvbiBTQU1MIFNlbG9yYU2InbmlkEiENicRzRmJlYXRIMQDw
CwYDVQQKIDARERU1PMQswCQYDVQQGEwJVUzCCASwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAIEUnYtH5niekNMgvRd5k8WnS28/8JDrmw1s1xac1A7KYJukm0OH
Sjg0CinF+uGr31cu0X8mLTW+0lQu5ud1etjx3SB4ZT+181K1zNQSFkLNjve7Mv
S3FRWZpP11ZS9yDUavjdzAy1FS2ORdy4TGZAksBITyYjmoPOsdmLybm1EqTUTHE
ckVIF9jH1YBjgKpmE/uzLSrVEdz9kgod4BADzeJsrMkCxi/KUzTS4VrBhPmv02
8h9SJ5T2GhhdjCWGTIDjg/0FJTjXWD2anVx+oyHCGROmnhOUnyhY1RHxmeReduQHj
7wHMFtgE5Tx07Fk+nCGQPuHg6YjMwmPDlq8CAwEAAAMQMA4wDAYDR0TBAUwAwEB
/ANBgkqhkiG9w0BAQUFAAOCAQEAEIjJaGqZ2Wmwv7CCBNefJqnGmEi6V/LOjG
JVIP1K3e52dj413Hrl+F9DUoumb571OcSOP9kBOQ005VmyNGUrsjTbj+Y1Y2R6QT
1bbBcNc7k4JB66+qqyGVNpbZUm+zt3S8B2MjveQ6nkA293x5HqjkrO6jyQLLV2V
a62P0bjg1mYRCEldC/CHkVbB71nwwdUf7SDzyP8p/D9xzdV7Xv2oIDrliUhs3
-----END CERTIFICATE-----
```

- Obtain the SHA1 certificate fingerprint from the certificate file by running the following command in the Command Prompt window:

openssl x509 -noout -fingerprint -in SAMLcertificateFileName

Setting up Freshservice

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

Configure Freshservice

- Log in to the Freshservice administrative console as administrator.
- Click the **Admin** tab.
- In the **Customer Portal** section, click **Security**.
- On the Security page, slide the button to turn on **Single Sign On**.
- Select the **SAML SSO** option.
- Enter the following values.

Field	Value
SAML Login URL	Enter your VMware Identity Manager login URL in the format https://myco.vmwareidentity.com/SAAS/auth/federation/sso . Replace <i>myco.vmwareidentity.com</i> with your company's VMware Identity Manager service domain name.
Logout URL	Enter your VMware Identity Manager logout URL in the format https://myco.vmwareidentity.com/SAAS/auth/logout . Replace <i>myco.vmwareidentity.com</i> with your company's VMware Identity Manager service domain name.
Security Certificate Fingerprint	Copy and paste the SHA1 certificate fingerprint from the certificate file you downloaded.

For example:

Security

ON **Single Sign On (SSO)**

SAML SSO

SAML is an XML standard used for communicating identities between two web applications. You can use it to let large teams access your support portal easily using Single Sign On.

SAML Login URL
Freshdesk will redirect users to this URL to login. You can get this from your SAML Identity Provider.

Logout URL
Optional logout URL to which users will be sent to when they logout of freshdesk.

Security Certificate Fingerprint
Fingerprint (SHA1) of the SAML certificate provided by your SAML Provider. This will be used for encryption / validation

Simple SSO

Single Sign On allows you to use your own application or a centralized Server (like MS Active Directory) to authenticate agents and customers so that they can access Freshdesk without entering a separate username and password.

7. Click **Save**.

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 **Freshservice**.
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:

Add User Entitlement ✕

| [or browse...](#)

User, Demo (demo)	Automatic ▼	Remove
-------------------	-------------	------------------------

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 Freshservice for Testing

1. Sign in to the Freshservice site as administrator.

2. Click the **ADMIN** tab.
3. Under **User Management**, click **Agents**.
4. Click **New Agent**, enter the user's information, and click **Save**.

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

Verify Test-User can Sign into Freshservice

1. Sign in to the user portal as the test user.
2. Click the **Freshservice** icon on the My Apps page.
You should now have single sign-on access to Freshservice.

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 Freshservice

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

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



	GROUP NAME	DEPLOYMENT TYPE
<input checked="" type="checkbox"/>	ALL USERS	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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.