



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

VMware Identity Manager

JULY 2016 V1

## Table of Contents

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

## Overview

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

Gerrit is a web-based team code collaboration tool. Software developers in a team can review each other's modifications on their source code using a Web browser and approve or reject those changes.

When Gerrit is configured in the VMware Identity Manager catalog, users can sign in to Gerrit from their VMware Identity Manager apps portal.

You must have an administrator account for the VMware Identity Manager service to configure Gerrit. You work with your Gerrit representative to configure VMware Identity Manager for single sign-on in the Gerrit server.

## Adding Gerrit to VMware Identity Manager Catalog

To enable single sign-on to Gerrit on the service, you must configure the app in the catalog.

### Add Gerrit 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 **Gerrit** icon.
4. Click **Configuration**. The Configuration page is preconfigured as follows.

FIELD	CONFIGURED VALUE
Launch URL	Automatically populated with your launch URL.
RelayState	
Proxy Count	
LoginRedirection URL	
Include Destination	Enabled
Sign Response	Enabled
Sign Assertion	
Include Cert	
Signature Algorithm	SHA1 with RSA
Digest Algorithm	SHA1

<b>Allow API Access</b>									
<b>Assertion Consumer Service *</b>	Automatically populated with the URL where the SAML is posted. <b>https://review.nicira.eng.{CompanyName}.com/Shibboleth.sso/SAML2/POST</b>								
<b>Name ID Format</b>	Unspecified (username)								
<b>Name ID Value</b>	Custom value <code>\${user.userName}</code>								
<b>Recipient Name *</b>	The SP' assertion consumer service URL populated as <b>https://review.nicira.eng.{CompanyName}.com/Shibboleth.sso/SAML2/POST</b>								
<b>Audience *</b>	The SP's unique identifier populated as <b>https://spgerrit.example.org/shibboleth</b>								
<b>Assertion Lifetime</b>	Populated with a value of 200 seconds.								
<b>Signing Certificate</b>									
<b>Application Parameters</b>	Set the CompanyName value. For example, if your Gerrit log in is <b>https://review.nicira.eng.act.com/</b> , then set the CompanyName value as <b>act.</b>								
<b>Attribute Mapping</b>	Map the <b>remoteUser</b> attribute to specific user profile values <table border="1" data-bbox="704 1045 1383 1138"> <thead> <tr> <th>NAME</th> <th>FORMAT</th> <th>NAME SPACE</th> <th>VALUE</th> </tr> </thead> <tbody> <tr> <td>remoteUser</td> <td>Unspecified</td> <td>--</td> <td><code>\${user.firstName}</code></td> </tr> </tbody> </table>	NAME	FORMAT	NAME SPACE	VALUE	remoteUser	Unspecified	--	<code>\${user.firstName}</code>
NAME	FORMAT	NAME SPACE	VALUE						
remoteUser	Unspecified	--	<code>\${user.firstName}</code>						

5. Click **Save**.

## Download SAML-Signing Certificate

If the SAML-signing certificate from the VMware Identity Manager service is required for the Gerrit configuration, you can retrieve the certificate from the Catalog > Settings tab.

1. In the **Catalog > Settings** tab, click **SAML Metadata**.

Copy and save the **Signing Certificate** text as 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-----
MIIDITCCAgmgAwIBAgIBATANBqkqhkiG9w0BAQUFAADBLMS0wkwYDVQDDCRib3Jp
em9uIFNBTFUwZ2VsZi1TaWduZWQgQ2YydGlnaWVhdGx0DzALBgNVBAoMBERFTU8x
CzAJBGNVBAVTAiVtMB4XDTE1MDIwMjM1MVoXDTE1MDEzMDEkMjM1MVoWszEz
MCsGA1UEAwkSG9yaXpviBTQU1MIFNlbG9yYU2lnbmVkdENicnRpZmlyYXRIMQ0w
CwYDVQKQDARERU1PMQswCQYDVQQGEwJVUzCCASwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAIEUnYb5nblekNMgyRd5K8WnS28/BJDrmw1s1xac1A7kYjukm0OH
Sljg0ClnF+uGr31cu0X8mLTW+0lQu5ud1etjx3SB4ZT+181K1zNQsftLInjve7Mv
S3FRWZpPl1ZS9yDUavjdAy1FS2ORdy4TGZAKsBITyYjmoPOsdmLybm1BqTUTHE
cKVF9H1YBjgkpmE/uzLSvEDz9okgo4BADzeJ9mKcXlKUZTSl4VmBhPrm02
8h9SJ5T2GHndjCWGTDJq0FjTXWD2anVX+oyHCGROmhOUUnyhY1RHxmEReduQHj
7wHMFtgE5Txd7Fk+nCGQPuHg6YjMwmPDIq8CAwEAAAMQMA4wDAYDVR0TBAAUwAwEB
/zANBqkqhkiG9w0BAQUFAAOCAQEAEjjaGqZ2WmmV7CCBNtJqnGrmEi6V/L0lJG
JMIP1K3e52dj413Hri+F9DUoumb571OcSOP9kBOQ005VmyNGuRsjTbJ+YIY2R6QT
1bbBcNc7KJB66+qqyGVNpbZUm+zt3S8B2MjiveQ6nKA293X5HqjkrO6jyQLLv2W
a62P0jbg1mYRCeIdC/CHKvxb71nwdUf7SDzYp8p/D9zdv7Xv2olDriUhs3
-----
```

## Setting up Identity Manager in Gerrit

Contact the Gerrit application support team to set up single sign-on with VMware Identity Manager.

## 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 on the Gerrit application.
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	<a href="#">Remove</a>
-------------------	-----------	------------------------

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

## Set up a User in Gerrit for Testing

Make sure the test user you set up in VMware Identity Manager can access Gerrit.

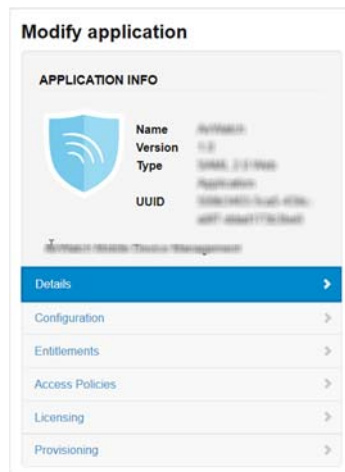
## Verify Test-User can Sign into Gerrit

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

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

## 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 external approval requirements, and entitle users and groups to the app.



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

**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** In some applications, licensing can be used to require users to request external approval before they can access the application. In addition, 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 approval information for the application.

## Entitle Users to Gerrit

You can activate single sign-on for all users.

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click Gerrit.
3. In the **Modify application** page, click **Entitlements**.
4. Click **+Add group entitlement**.
5. Select **ALL USERS** and change the DEPLOYMENT TYPE value to **Automatic**.



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

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

