



# Using VMware Horizon Workspace™ to Enable SSO in VMware vCloud Director® 5.1

March 2013

© 2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at <http://www.vmware.com/download/patents.html>.

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.

VMware, Inc.  
3401 Hillview Ave  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

## Contents

1. Overview .....	5
2. Requirements for SSO in VMware vCloud Director .....	5
3. Configuring vCloud Director .....	7
3.1 Exporting XML Metadata from vCloud Director .....	9
4. Configuring Horizon Workspace for vCloud Director SSO .....	10
5. Other Considerations .....	11
5.1 Groups .....	11
5.2 Previous LDAP Users .....	11
5.3 API Access .....	11
5.4 Known Issues .....	11



## 1. Overview

VMware Horizon Workspace™ can be used to enable single sign-on (SSO) in VMware vCloud Director 5.1. vCloud Director® provides methods to authenticate end users via LDAP and federation to external authentication sources.

This document provides information and procedures for configuring vCloud Director to allow for account federation from VMware Horizon Workspace. This information is also applicable for third-party Identity Providers.

## 2. Requirements for SSO in VMware vCloud Director

The SAML process and the people using it have formal roles and responsibilities:

- Service Provider – An entity that receives the SAML message from an Identity Provider (vCloud Director).
- Identity Provider – An entity that authenticates an user (Horizon Workspace).

To set up vCloud Director for SSO you need to acquire metadata from your SAML Identity Provider. Usually, this is in the form of an XML document such as the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor cacheDuration="P29DT12H44M3.840S"
entityID="https://domain.com/idp.xml" validUntil="2013-04-11T21:44:51.059Z"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
<md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
</md:KeyDescriptor>
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="domain.com" ResponseLocation="domain.com"/>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</md:NameIDFormat>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="domain.com"/>
</md:IDPSSODescriptor>
<md:AdditionalMetadataLocation
namespace="urn:oasis:names:tc:SAML:2.0:metadata">domain.com</md:AdditionalMetadataLoca
tion>
</md:EntityDescriptor>
```

This XML metadata file includes several certificates and the information required to allow vCloud Director to communicate with the SSO solution and validate and trust the SSO solution responses.

The Identity provider must provide values for the following case-sensitive fields in the response:

- UserName
- EmailAddress
- FullName
- Groups

Only UserName is required, but it is recommended that all fields be returned with appropriate information to allow for ease of management and administration of the users and their rights.

### 3. Configuring vCloud Director

Use the following procedure to configure vCloud Director for SSO.

#### To enable the use of a SAML Identity provider in vCloud Director 5.1

1. After logging in as an organization administrator or system administrator go to the organization Administration page, click **Federation**, and select **Use SAML Identity Provider**.

##### Identity Provider

Use SAML Identity Provider

Your identity provider is used to authenticate users in this organization. Enter the SAML v2.0 metadata service's X.509 certificate. The metadata can be provided by pasting the metadata XML in the field provided below.

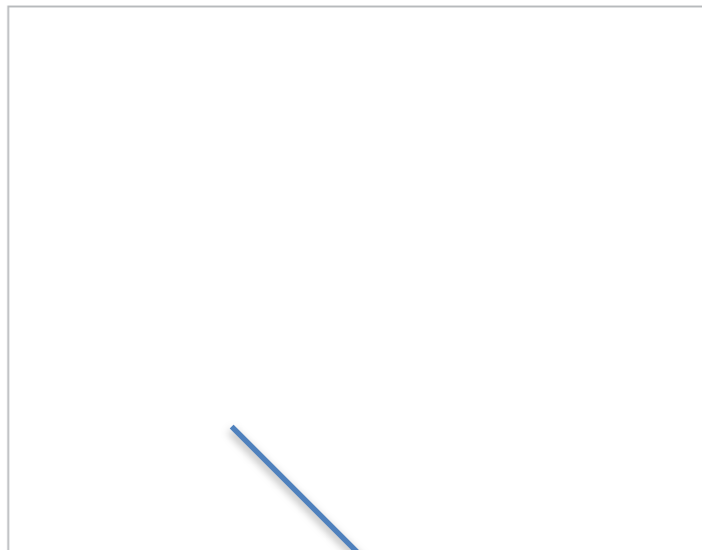
2. The XML metadata file from your SAML/SSO provider should be downloaded to the machine these actions are running from. In the case of Horizon Workspace the metadata can be found here:

<https://<hostname>/SAAS/API/1.0/GET/metadata/idp.xml>

Use the upload function to upload the XML file. (Do not paste the file into the text area as special characters might cause problems.)

Your identity provider is used to authenticate users in this organization. Enter the SAML v2.0 metadata service's X.509 certificate. The metadata can be provided by pasting the metadata XML in the field provided below.

Metadata XML:



You can upload a local file containing the metadata XML by clicking Browse to select a file.

3. Close the **Organization** tab, or log out and back into the UI, to make the Groups and Import from SAML options available from the UI. Then, import users into vCloud Director.

Import Users

Source: SAML

Enter user names to import:

User names must be in the name identifier format supported by the SAML identity provider configured for this organization. Use a new line for each user name.

Assign role: Organization Administrator

OK Cancel



Because SAML users and groups cannot be found using a search, users have to be added one per line for each role. Alternatively, access to the organization can be granted through the use of groups.



After importing users or groups the configuration of SSO for vCloud Director is complete.

### 3.1 Exporting XML Metadata from vCloud Director

Export a file similar to the file imported from the SAML provider so that the SAML provider can trust and validate requests coming from vCloud Director. This file and related certificates are controlled from the Federation page where we imported the SAML XML file.

#### To export XML metadata from vCloud Director

Click **Regenerate** to create a new certificate that is valid for one year.

##### Certificate

Certificate Expiration: 02/24/2014 11:19 AM

This certificate is used to sign federation messages and is valid

A warning about changing the certificate is displayed. If you have already set up a SAML provider relationship, changing this certificate breaks that relationship until the SAML provider replaces the current information with the new certificate.

After the certificate is generated you can download it from the following link:

<https://<domain>.<tld>/cloud/org/<OrganizationName>/saml/metadata/alias/vcd>

Save the certificate as an XML file, and provide it to your SAML provider when you configure Horizon Workspace for vCloud Director SSO.

## 4. Configuring Horizon Workspace for vCloud Director SSO

Log in to the administrator interface for Horizon Workspace and create a new application, then configure the following items for the newly created application.

### To configure Horizon Workspace for vCloud Director SSO

1. Configure the Login Redirection URL to be the organization URL in vCloud Director. This is required for vCloud Director to work properly because the authentication sequence must start with vCloud Director, not Horizon Workspace.
2. Select **Include the Destination in the response**.
3. Select the **Sign the entire response**.
4. Select **Sign the assertion**.
5. Deselect the **Include Cert** checkbox.
6. Select the **configure via Meta-data XML** option. Then upload the certificate (copy/paste) the certificate into the text box.
7. Click **Populate Attribute Mapping**.
8. Configure the attribute mapping to match your deployment of Horizon Workspace.

#### Attribute Mapping

You can map these attributes to specific user profile values.

Name	Format	Namespace	Value	
EmailAddress	Basic		\${user.Email}	Delete
UserName	Basic		\${user.UserName}	Delete
FullName	Basic		\${user.LastName}	Delete

## 5. Other Considerations

Also consider the following when configuring SSO.

### 5.1 Groups

Depending on the deployment source of truth for authentication, if the user can see the application in Horizon Workspace, it can be assumed to be granted access to vCloud Director. If that is the case, you can avoid having to manage two lists of users by hardcoding a group name. To do this set an attribute in Horizon Workspace of `Groups = TrustedUsers` (or similar name), and in vCloud Director add a group by that name (SAML is case sensitive). This allows any user that authenticates to Horizon Workspace and is presented with this application access to the vCloud Director instance, regardless of whether an account was prepopulated.

In Horizon Workspace, the attribute mapping looks like the following.

Groups	Basic	enabledusers	Delete
--------	-------	--------------	--------

[Add another attribute](#)

### 5.2 Previous LDAP Users

If you are migrating from LDAP to SAML you probably have some LDAP users in your vCloud installation. These users may even be owners of vApps or catalog items. If your SAML provider uses the same `UserName` as LDAP, vCloud Director will display errors about SAML failing to authenticate the user. To resolve this the LDAP user has to be removed from vCloud Director before the SAML user can be created. A solution for some LDAP users might be to disable and remove the user, transfer the ownership of the objects to a different user, create the SAML user, and change the ownership back to the new SAML account.

### 5.3 API Access

When using SAML Identity Providers and API access follow the instructions in the “Create a Login Session Using a SAML:Identity Provider” section of the *vCloud API Programming Guide* ([http://pubs.vmware.com/vcd-51/topic/com.vmware.vcloud.api.doc\\_51/GUID-335CFC35-7AD8-40E5-91BE-53971937A2BB.html?resultof=%22%73%61%6d%6c%22%20](http://pubs.vmware.com/vcd-51/topic/com.vmware.vcloud.api.doc_51/GUID-335CFC35-7AD8-40E5-91BE-53971937A2BB.html?resultof=%22%73%61%6d%6c%22%20)).

Another option is to use a LDAP user or local user to access the API, PowerCLI, or other means.

### 5.4 Known Issues

vCloud Director does not handle a logout event properly in a SAML installation. If a user ends up in a infinite loop between Horizon Workspace and vCloud Director, have the user close the browser (clearing the session cookies) and re-login. This problem presents itself mostly when a user has access to multiple organizations and attempts to change between those organizations without logging out of organization 1 and then logging into organization 2 through Horizon Workspace.