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

VMware Identity Manager

OCTOBER 2015 V1

Table of Contents

Overview

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

ClearSlide is a sales communications application providing web-based services for the communication needs of sales teams.

When ClearSlide is configured in the VMware Identity Manager catalog, users can sign in to ClearSlide from their apps portal or if they sign in to their ClearSlide account directly, they are redirected to the VMware Identity Manager sign in page to enter their sign-in credentials.

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

Adding ClearSlide to VMware Identity Manager Catalog

To enable single sign-on to ClearSlide on the service, you must configure the app in the catalog and configure the identity provider information in ClearSlide.

Add ClearSlide 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 **ClearSlide** icon.

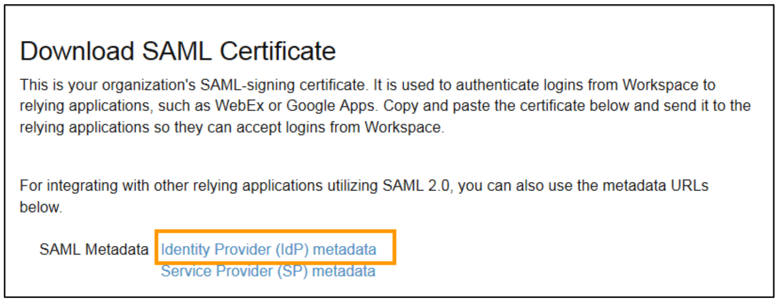
   The Modify application page appears.

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

Locate Identity Provider SAML Metadata

You must have the VMware Identity Provider identity provider metadata xml URL to configure ClearSlide.

1. In the Catalog > Settings tab, click **SAML Metadata**.
2. In the SAML Metadata section, click **Identity Provider (IdP) metadata** to display the metadata content. Save the URL. The URL is similar to this example. https://*myco.vmwareidentity.com*/SAAS/API/1.0/GET/metadata/idp.xml.



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.

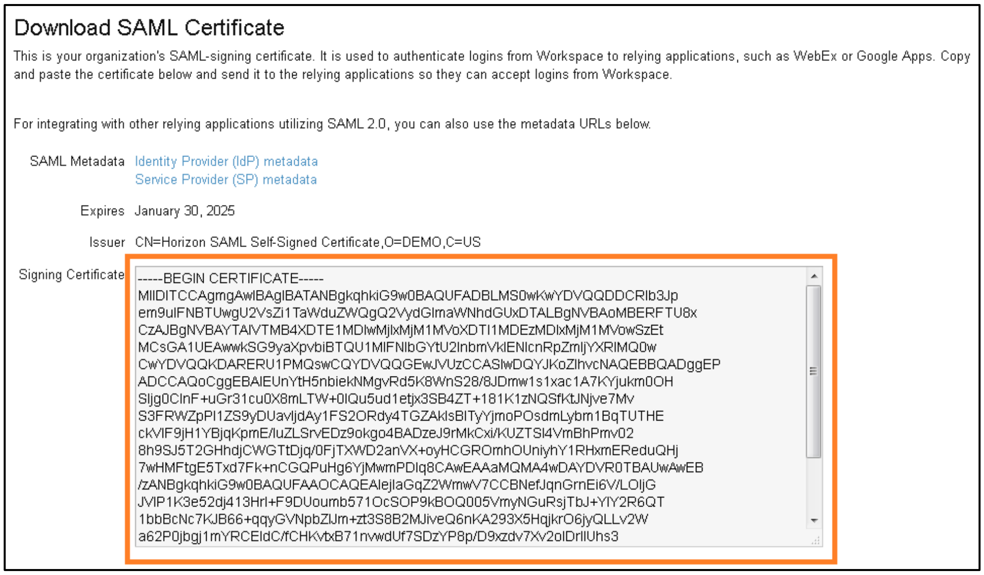
For integrating with other relying applications utilizing SAML 2.0, you can also use the metadata URLs below.

SAML Metadata Identity Provider (IdP) metadata
Service Provider (SP) metadata

Download SAML-Signing Certificate

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

3. In the **Catalog > Settings** tab, click **SAML Metadata**.
4. 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-----
MIIDITCCAgmgAwIBAgIBATANBgkqhkiG9w0BAQUFADBLMS0wKwYDVQQDDCRIb3Jp
em9uIFNBTUwgU2VsZi1TaWduZWQgQ2VydGlmaWNhdGUxDTALBgNVBAoMBERFTU8x
CzAJBgNVBAYTAlVTMB4XDTE1MDIwMjIxMjM1MVoXDTI1MDEzMDIxMjM1MVowSzEt
MCsGA1UEAwwkSG9yaXpvbiBTQU1MIFNlbGYtU2lnbmVkIENlcnRpZmljYXRlMQ0w
CwYDVQQKDARERU1PMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAIEUnYtH5nbiekNMgvRd5K8WnS28/8JDmw1s1xac1A7KYjukm0OH
SIjg0CInF+uGr31cu0X8mLTW+0IQu5ud1etjx3SB4ZT+181K1zNQSfKtJNjve7Mv
S3FRWZpPI1ZS9yDUavIjdAy1FS2ORdy4TGZAkIsBITyYjmoPOsdmLybm1BqTUTHE
cKVIF9jH1YBjqKpmE/luZLSrvEDz9okgo4BADzeJ9rMkCxi/KUZTSI4VmBhPmv02
8h9SJ5T2GHhdjCWGTtDjq/0FjTXWD2anVX+oyHCGROmhOUniyhY1RHxmEReduQHj
7wHMFtgE5Txd7Fk+nCGQPuHg6YjMwmPDIq8CAwEAAaMQMA4wDAYDVR0TBAUwAwEB
/zANBgkqhkiG9w0BAQUFAAOCAQEAlejlaGqZ2WmwV7CCBNefJqnGrnEi6V/LOIjG
JVIP1K3e52dj413HrI+F9DUoumb571OcSOP9kBOQ005VmyNGuRsjTbJ+YlY2R6QT
1bbBcNc7KJB66+qqyGVNpbZlJm+zt3S8B2MJiveQ6nKA293X5HqjkrO6jyQLLv2W
a62P0jbgj1mYRCEIdC/fCHKvtxB71nvwdUf7SDzYP8p/D9xzdv7Xv2oIDrIlUhs3
```

Setting up ClearSlide

To set up ClearSlide for single sign-on from the service, you enter the VMware Identity Manager identity provider metadata URL, provide the identity manager single sign-on information, and add the x.509 signing certificate to ClearSlide.

Configure ClearSlide

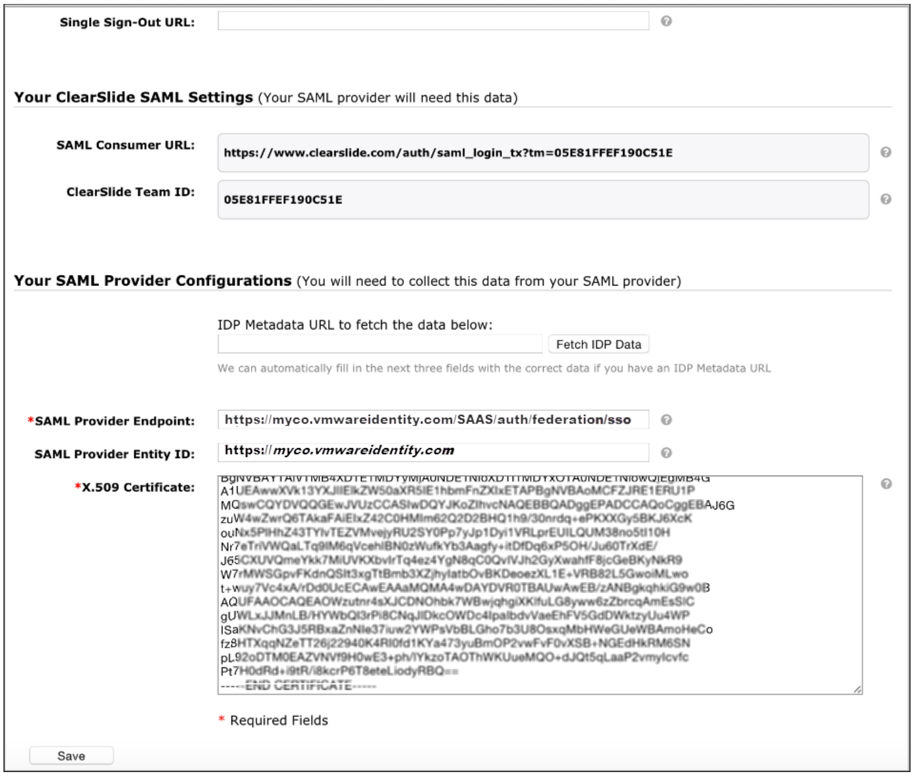
1. Log in to the ClearSlide admin console as the admin user.
2. On the admin console page, click **My Account**.
3. In the navigation pane on the right, click **Single Sign-on Settings**.
4. In the **SAML Provider Configurations** section, enter values for the following fields.

FIELD	DESCRIPTION
IDP Metadata …	This is the metadata.xml URL that identifies VMware Identity Manager as the identity provider. Enter your VMware Identity Manager identity provider metadata URL that you saved previously. Enter as https://*myco.vmwareidentity.com*/SAAS/API/1.0/GET/metadata/idp.xml Replace *myco.vmwareidentity.com* with your company's VMware Identity Manager service domain name.

SAML Provider Endpoint	Enter the VMware Identity Manager login URL in the format https://*myco.vmwareidentity.com*/SAAS/auth/federation/sso Replace *myco.vmwareidentity.com* with your company's VMware Identity Manager service domain name.
SAML Provider Entity ID	Enter your VMware Identity Manager unique name as https://*myco.vmwareidentity.com*
X.509 Certificate	Upload the SAML signing certificate file that you saved to your computer.

5. Copy and save the **SAML Consumer URL** and the **ClearSlide Team ID** information that is on this page. You configure this inforamtion in VMware Identity Manager.

6. Click **Save**.



Single Sign-Out URL:

Your ClearSlide SAML Settings (Your SAML provider will need this data)

SAML Consumer URL: https://www.clearslide.com/auth/saml_login_tx?tm=05E81FFEF190C51E

ClearSlide Team ID: 05E81FFEF190C51E

Your SAML Provider Configurations (You will need to collect this data from your SAML provider)

IDP Metadata URL to fetch the data below:

We can automatically fill in the next three fields with the correct data if you have an IDP Metadata URL

*SAML Provider Endpoint: https://myco.vmwareidentity.com/SAAS/auth/federation/sso

SAML Provider Entity ID: https://*myco.vmwareidentity.com*

*X.509 Certificate:

```
BgNVBAYTAlVTMB4XDTE1MDYyMjA0NDE1NloXDTI1MDYxOTA0NDE1NlowQjEgMB4G
A1UEAwwXVk13YXJlIElkZW50aXR5IE1hbmFnZXIxETAPBgNVBAoMCFZJRE1ERU1P
MQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ6G
zuW4wZwrQ6TAkaFAiElxZ42C0HMlm62Q2D2BHQ1h9/30nrdq+ePKXXGy5BKJ6XcK
ouNx5PlHhZ43TYlvTEZVMvejyRU2SY0Pp7yJp1Dyi1VRLprEUILQUM38no5tl10H
Nr7eTriVWQaLTq9lM6qVcehlBN0zWufkYb3Aagfy+itDfDq6xP5OH/Ju60TrXdE/
J65CXUVQmeYkk7MiUVKXbvlrTq4ez4YgN8qC0QvIVJh2GyXwahfF8jcGeBKyNkR9
W7rMWSGpvFKdnQSlt3xgTtBmb3XZjhylatbOvBKDeoezXL1E+VRB82L5GwoiMLwo
t+wuy7Vc4xA/rDd0UcECAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQUFAAOCAQEAOWzutnr4sXJCDNOhbk7WBwjqhgiXKlfuLG8yww6zZbrcqAmEsSlC
gUWLxJJMnLB/HYWbQl3rPi8CNqJlDkcOWDc4lpalbdvVaeEhFV5GdDWktzyUu4WP
lSaKNvChG3J5RBxaZnNle37iuw2YWPsVbBLGho7b3U8OsxqMbHWeGUeWBAmoHeCo
fz8HTXqqNZeTT26j22940K4Rl0fd1KYa473yuBmOP2vwFvF0vXSB+NGEdHkRM6SN
pL92oDTM0EAZVNVf9H0wE3+ph/lYkzoTAOThWKUueMQO+dJQt5qLaaP2vmylcvfc
Pt7H0dRd+i9tR/i8kcrP6T8eteLiodyRBQ==
-----END CERTIFICATE-----
```

* Required Fields

Complete the Setup and Review the Application Configuration Page

In the Catalog > ClearSlide >Application Configuration page, configure the ClearSlide information and verify that the required fields are configured correctly.

1. Log in to the VMware Identity Manager administration console.
2. In the Catalog page, click the **ClearSlide** icon.
3. Click **Configuration** and configure the following fields.

FIELD	DESCRIPTION
Relay State	Enter the SAML Consumer URL that you saved from the ClearSlide single sign on page. This is the same as the custom login URL.
Applications Parameters section	In the **NAME** field, enter **teamID**. Add a description, ClearSlide teamID. In the **VALUE** field, enter the **team ID number** you saved from the ClearSlide single sign on page.

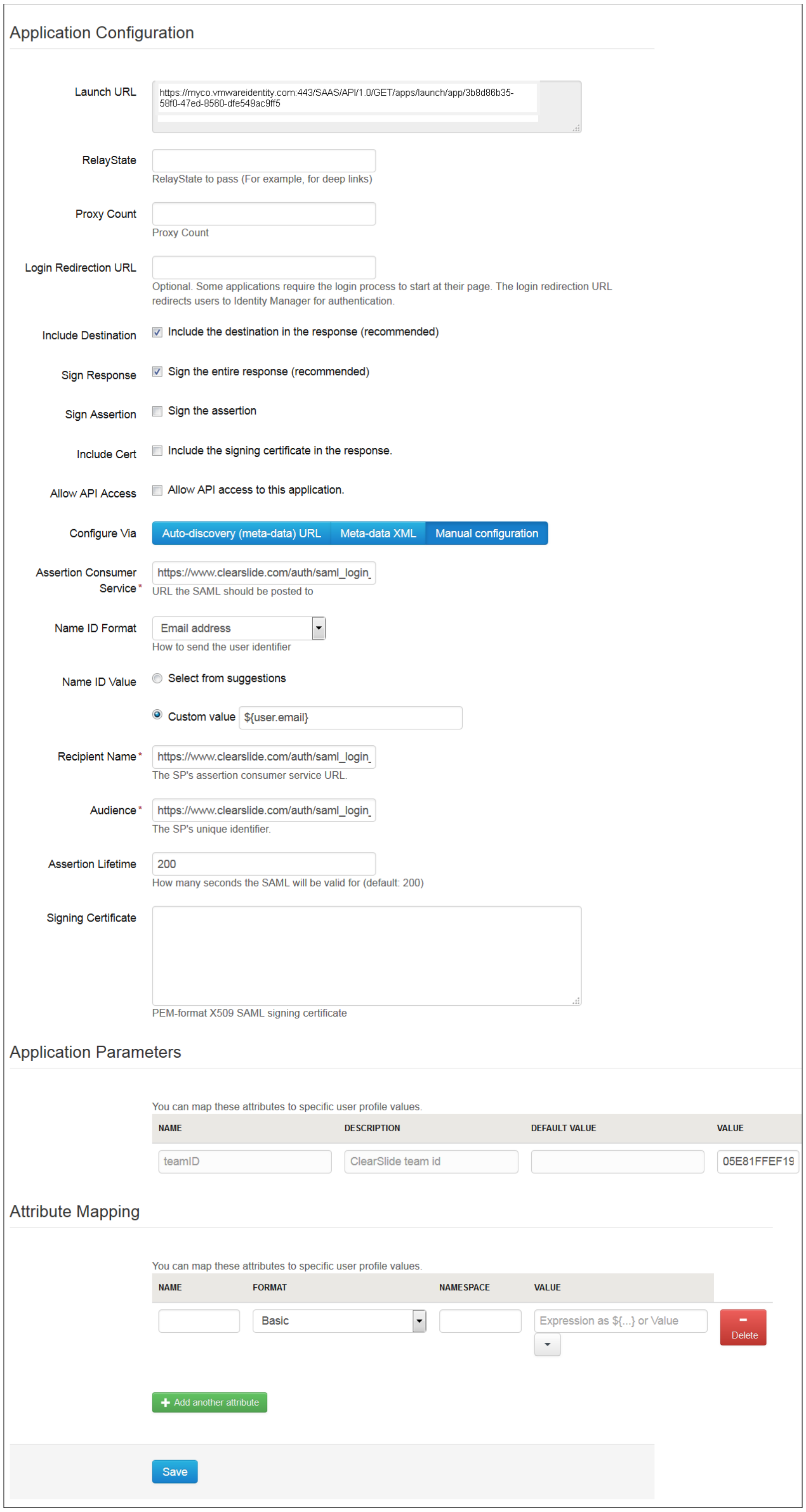
4. The following required fields are pre-populated. Do not change these.

FIELD	DESCRIPTION
Assertion Consumer Service	This is the URL that the SAML should be posted to. **https://www.clearslide.com/auth/saml_login_tx?tm={teamID}**
Recipient Name	This is the same as the Assertion Consumer Service URL.
Audience	This is the same as the Assertion Consumer Service URL

Do not deselect any of the checked boxes.

5. Click **Save**.

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



Application Configuration

Launch URL: https://myco.vmwareidentity.com:443/SAAS/API/1.0/GET/apps/launch/app/3b8d86b35-58f0-47ed-8560-dfe549ac9ff5

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: Auto-discovery (meta-data) URL | Meta-data XML | [✓ Manual configuration]

Assertion Consumer Service*: https://www.clearslide.com/auth/saml_login
URL the SAML should be posted to

Name ID Format: Email address
How to send the user identifier

Name ID Value: ○ Select from suggestions

● Custom value ${user.email}

Recipient Name*: https://www.clearslide.com/auth/saml_login
The SP's assertion consumer service URL.

Audience*: https://www.clearslide.com/auth/saml_login
The SP's unique identifier.

Assertion Lifetime: 200
How many seconds the SAML will be valid for (default: 200)

Signing Certificate:
PEM-format X509 SAML signing certificate

Application Parameters

You can map these attributes to specific user profile values.

NAME	DESCRIPTION	DEFAULT VALUE	VALUE
teamID	ClearSlide team id		05E81FFEF19

Attribute Mapping

You can map these attributes to specific user profile values.

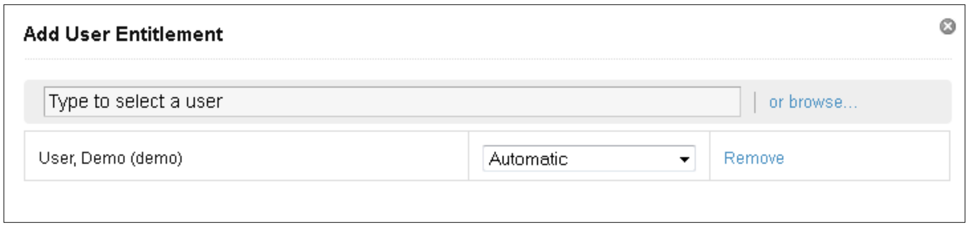
NAME	FORMAT	NAMESPACE	VALUE	
	Basic		Expression as ${...} or Value	Delete

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 a 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 **ClearSlide** 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

Type to select a user | 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**.

Add the User to ClearSlide for Testing

1. Log in to the ClearSlide admin console as the admin user.
2. In the header on the admin console page, click **My Account**.
3. In the navigation pane on the right, click **Group Based Permissions > Manage User Accounts**.
4. In the page that opens, click **Invite New User**.
5. Enter the first name, last name and email address of the test user you entitled to ClearSlide in the service.
6. Click **Invite**.

   An email is sent to the test user's email address with an activation link.
7. Retrieve the email and click on the activation link.
8. On the ClearSlide page set up a password and enter a mobile number.
9. Click **Active User** to activate the account.

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

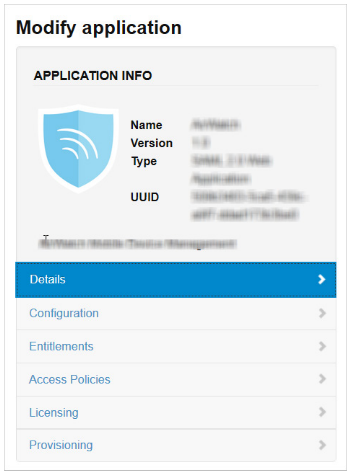
Verify Test-User can Sign in to ClearSlide

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

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

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 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 can access 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

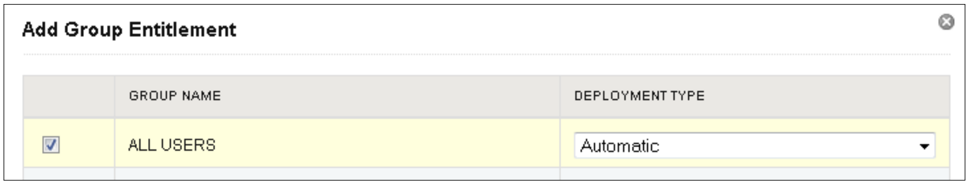
Provisioning provides automatic application user-management from a single location. Provisioning adapters allow the Web application to retrieve specific information from VMware Identity Manager, as required. The provisioning adapters that can be selected are either Google Apps, Mozy, or Vchs. If you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

Entitle Users to ClearSlide

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

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



Add Group Entitlement

	GROUP NAME	DEPLOYMENT TYPE
☑	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