



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

VMware Identity Manager

DECEMBER 2016 V3

**Table of Contents**

Overview ..... 2

Adding Google Apps to the VMware Identity Manager Catalog ..... 2

    Add Google Apps to the Catalog ..... 2

    Download the Service’s SAML-Signing Certificate ..... 2

Configuring Google Apps to Enable SAML for Authentication ..... 3

    Configure Google Apps ..... 3

Complete the Setup in the Service ..... 4

(Optional) Provisioning Users in Google from the Service ..... 4

    Configure a Google Service Account ..... 4

    Configure the Google Apps Provisioning Adapter ..... 5

    Provision Users in Google ..... 6

    Provision Groups in Google ..... 7

    Deprovision Groups in Google ..... 9

    Enable or Disable the Google Apps Provisioning Adapter ..... 9

Testing Single Sign-on Configuration ..... 9

    Test Single Sign-on with Provisioning Enabled ..... 9

    Test Single Sign-on without Provisioning ..... 10

Entitling Users to Google Apps ..... 11

## Overview

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

Google Apps is a suite of Google applications for businesses, such as email, Google Docs, and Google Calendar.

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

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

## Adding Google Apps to the VMware Identity Manager Catalog

To enable single sign-on to Google Apps from the service, you must configure Google Apps in the catalog and copy the SAML signing certificate of the service to Google Apps.

### Add Google Apps 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 **Google Apps** icon.

The Modify application page appears.

Google Apps is added to the catalog but is not configured. You complete the application configuration after you enable single sign-on in Google Apps.

### Download the Service's SAML-Signing Certificate

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

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



Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

**Sign-in page URL**   
URL for signing in to your system and Google Apps

**Sign-out page URL**   
URL for redirecting users to when they sign out

**Change password URL**   
URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

**Verification certificate** Replace certificate"/>  
The certificate file must contain the public key for Google to verify sign-in requests. ?

5. Click **SAVE CHANGES**.

## Complete the Setup in the Service

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, select the Google Apps icon.
3. In the Modify application page, click **Configuration**.
4. In the **Application Parameters** section, update the value of the **domainName** parameter with the domain name used in your Google account. For example, **example.com**.

This updates {domainName} wherever it appears.

Application Parameters

You can map these attributes to specific user profile values.

NAME	DESCRIPTION	DEFAULT VALUE	VALUE
<input type="text" value="domainName"/>	<input type="text" value="Google Apps Domain"/>	<input type="text"/>	<input type="text" value="example.com"/>

5. Click **Save**.

## (Optional) Provisioning Users in Google from the Service

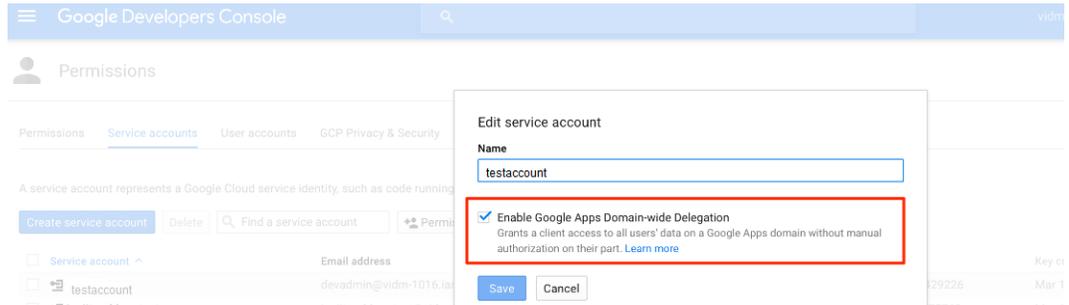
You can use the Google Apps provisioning adapter to automatically provision users in Google from the VMware Identity Manager service. If provisioning is enabled, whenever you entitle a user to Google Apps in the service, the user is also created in Google. You can also use the adapter to provision groups in Google.

### Configure a Google Service Account

Before you enable the Google Apps provisioning adapter in VMware Identity Manager, you must create a Google service account.

1. Create a Google service account and its credentials.  
 You will need your service account's client ID, email address, and private key file to enable provisioning.
2. After you create the Google service account, enable Google Apps domain-wide delegation.

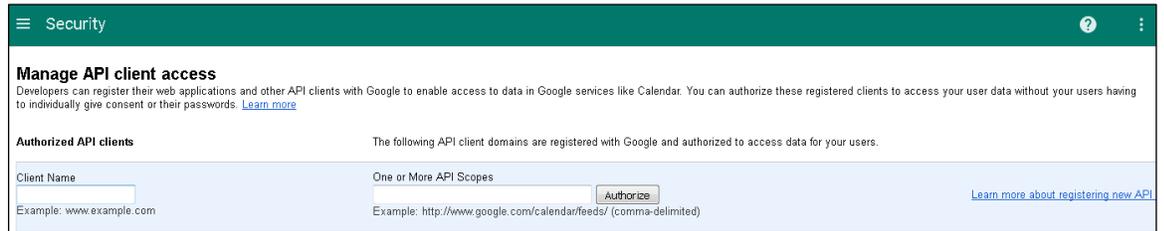
- a. In the API Manager **Credentials - Create credentials** page, click **Manage service accounts**.
- b. Click the  icon next to your service account and select **Edit**.
- c. Select the **Enable Google Apps Domain-wide Delegation** checkbox, and click **Save**.



3. Delegate Google Apps domain-wide authority to the service account from the **Security > Advanced Settings > Authentication > Manage API client access** page in the Google Admin console. See the [Google documentation](#) for more information.

When you delegate domain-wide authority to the service account, enter the following values for the **One or More API Scopes** field:

```
https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.user.alias.readonly,https://www.googleapis.com/auth/admin.directory.user.alias,https://www.googleapis.com/auth/admin.directory.user,https://www.googleapis.com/auth/admin.directory.group.readonly,https://www.googleapis.com/auth/admin.directory.group.member.readonly,https://www.googleapis.com/auth/admin.directory.group.member,https://www.googleapis.com/auth/admin.directory.group
```



## Configure the Google Apps Provisioning Adapter

Configure the Google Apps provisioning adapter to provision users and groups in Google from the VMware Identity Manager service.

If provisioning is enabled, whenever you entitle a user to Google Apps in the service, the user is also created in Google. You can also provision groups in Google.

1. Log in to the VMware Identity Manager administration console.
2. Click the **Catalog** tab.
3. Click **Google Apps**.
4. In the Modify application page, click **Provisioning**.
5. In the **Configuration** tab, configure the provisioning adapter.

OPTION	DESCRIPTION
<b>Enable Provisioning</b>	Select this option.

<b>Admin User Name</b>	Your Google Apps administrator user name. Do not include the domain name. For example: <b>admin</b>
<b>Service Account</b>	The client email of the service account. You can get the client email from the key file.
<b>Private Key</b>	Copy and paste the service account's private key.
<b>Domain Name</b>	Your company's domain name. For example: <b>example.com</b>
<b>Suspend On Deprovisioning</b>	Select this option if you want users to be suspended in Google when you remove their entitlement to Google Apps.

For example:

The screenshot shows the 'Provisioning' configuration interface. At the top, there are three tabs: 'Configuration', 'User Provisioning', and 'Group Provisioning'. The 'Configuration' tab is selected. Below the tabs, the 'Configure Adapter' section is visible. It contains several fields and checkboxes:

- Enable Provisioning:** A checked checkbox.
- Admin User Name\*:** A text input field containing 'admin'.
- Service Account\*:** A text input field containing 'test126120@developer.gserviceaccount.com'.
- Private Key\*:** A text input field with masked characters (dots).
- Domain Name\*:** A text input field containing 'example.com'.
- Suspend On Deprovisioning:** A checked checkbox.

At the bottom of the configuration area, there are two buttons: 'Test Connection' (green) and 'Save' (blue).

6. Click **Test Connection**.

If the connection is successful, a "Made a connection to Google service" message appears at the top of the page.

7. Click **Save**.

Provisioning is now enabled. To complete the user provisioning setup, specify the attributes with which to provision users in Google.

## Provision Users in Google

To provision users in Google, you configure the Google Apps provisioning adapter, enable provisioning, and specify the attributes with which to provision users in Google.

After you configure the provisioning adapter and enable provisioning, specify the attributes.

A list of Google attributes is available. For the attributes that you want to use, specify the attribute mapping. You can either map the attributes to VMware Identity Manager user attributes or enter other values.

The following attributes are required for users provisioned to Google. These attributes have default values.

- User Name
- First Name
- Last Name

1. In the Google Apps Provisioning page, click the **User Provisioning** tab.
2. Select the attributes with which to provision users in Google by setting values for them.
  - a. Click the edit icon next to the attribute.
  - b. Select or type a value.

The expressions in the drop-down list are the ones listed in the Identity & Access Management > Setup > User Attributes page. If you want to add any expressions to the list, add them to the User Attributes page. You can also type in a value directly.

For some attributes, you can specify multiple values. Click the + icon at the top-right to add another value. For example, you can specify multiple phone numbers for the **Phones** attribute.

The screenshot shows a dialog box titled "Edit Mapped Values (Phones)". It contains a table of attribute mappings. The first row has "Number" set to "\$ (user.phone)", "Is Primary" checked, and "Type" set to "work". The second row has "Number" set to "1-877-486-9273", "Is Primary" unchecked, and "Type" set to "company\_main". Each row has a red "x" and a green "+" icon to its right. At the bottom right are "Cancel" and "Save" buttons.

- c. Click **Save**.
3. To delete an attribute mapping, click the delete icon next to the attribute.

Attributes without values are not used when users are provisioned in Google.

User provisioning is now configured. When you entitle a user to Google Apps in VMware Identity Manager, the user will also be created in Google, unless the user already exists in Google.

**NOTE:** When you entitle a user to Google Apps, if you set the deployment type to Automatic, the user is provisioned immediately. If you set the deployment type to User-Activated, the user is provisioned when the user adds Google Apps to the Launcher page in the Workspace ONE portal.

## Provision Groups in Google

You can provision groups in Google from the VMware Identity Manager service using the Google Apps provisioning adapter. You can select any of your VMware Identity Manager groups to provision, regardless of whether they are created locally or synced from your enterprise directory. The group is created in Google and the email addresses of the group members are added to it.

Groups in Google can be used as mailing lists. They can also be used to manage access to documents, sites, calendars, and so on.

After you provision a group in Google, you can manage it like any other Google group. For example, you can add or delete users.

Before provisioning groups in Google, ensure that you have configured the Google Apps provisioning adapter and enabled provisioning.

1. In the VMware Identity Manager administration console, click the **Catalog** tab.

2. Click **Google Apps**.
3. In the Modify application page, click **Provisioning**.
4. In the Provisioning page, click the **Group Provisioning** tab.
5. Click **Add Group to Provision**.
6. In the Add Group to Provision page that appears, enter the following information.

OPTION	DESCRIPTION
<b>Group Name</b>	Enter the name of the VMware Identity Manager group you want to provision in Google. You can start typing to search for a group.
<b>Group Owner Email</b>	Enter the email address of the owner of the group.
<b>Group Email</b>	<p>Enter an email address for the group in Google. The group will be created in Google with this email address. The email address must either be new or belong to an existing Google group. It must not belong to a user.</p> <p>If a group with this email address already exists in Google, members of the VMware Identity Manager group you selected are added to that group.</p> <p><b>NOTE:</b> Ensure that the domain of the email address matches the domain you specified in the Domain Name text box in the Configuration tab.</p>

For example:

Add Group to Provision

Group Name\*

Group Owner Email\*

Group Email\*

Cancel
Provision

7. Click **Provision**.

The group is provisioned in Google with the same name as the VMware Identity Manager group and with the email address you specified. The provisioning status is displayed in the Group Provisioning tab.

To verify that the group is provisioned in Google:

1. Log in to the Google Admin console.
2. Click the **Groups** icon.  
You may need to click **MORE CONTROLS** at the bottom of the page to see the **Groups** icon.
3. Select the new group to view details.

## Deprovision Groups in Google

You can deprovision groups that you provisioned in Google from the VMware Identity Manager service. Deprovisioning a group deletes the group in Google.

Before you deprovision a group, verify that the Google Apps provisioning adapter is enabled.

1. In the VMware Identity Manager administration console, click the **Catalog** tab.
2. Click **Google Apps**.
3. In the Modify application page, click **Provisioning**, then click the **Group Provisioning** tab.
4. In the table, select the check box next to the group you want to deprovision and click **Deprovision**.

The group is deleted in Google. It is also removed from the Group Provisioning page.

## Enable or Disable the Google Apps Provisioning Adapter

If the Google Apps provisioning adapter is enabled, whenever you entitle a user to Google Apps, the user is also created in Google. You can disable the provisioning adapter if you do not want to provision users to Google.

1. In the administration console, click the **Catalog** tab.
2. Click **Google Apps**.
3. In the Modify application page, click **Provisioning**.
4. In the Provisioning page, click the **Configuration** tab, if it is not selected.
5. Select the **Enable Provisioning** check box to enable the adapter or deselect the check box to disable the adapter.
6. 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. You can test in two ways, with provisioning enabled in the VMware Identity Manager service and without provisioning.

### Test Single Sign-on with Provisioning Enabled

To test your single sign-on configuration with provisioning enabled in the VMware Identity Manager service, you use the Google Apps provisioning adapter.

Ensure that you have a user ID and email address for testing.

1. Log in to the VMware Identity Manager administration console.
2. In the **Users & Groups** page, click **Users** and verify that the user you are testing is in the list of users.
3. Enable provisioning if you have not yet done so. See the *Provisioning Users in Google from the Service* section for information.
4. Click the **Catalog** tab, then click **Google Apps**.
5. In the Modify application page, click **Entitlements**.
6. Click **+Add user entitlement**.

7. 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

8. Click **Save**, then click **Done**.
9. In the top-right corner of the page, click your user name and select **Logout**.
10. Log in to the Workspace ONE portal as the test user.
11. Click the Google Apps icon in the Launcher page.

You should now have single sign-on access to Google Apps.

## Test Single Sign-on without Provisioning

To test your single sign-on configuration without provisioning enabled in the VMware Identity Manager service, you configure user entitlement in the service and add the user to Google Apps.

Ensure that you have a user ID and email address for testing.

### Set up User in VMware Identity Manager for Testing

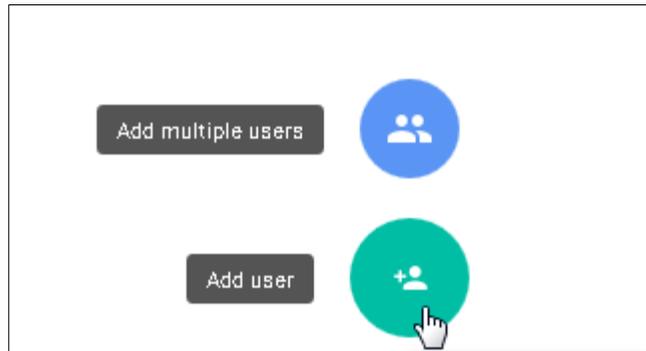
1. Log in to the VMware Identity Manager administration console.
2. In the **Users & Groups** page, click **Users** and verify that the user you are testing is in the list of users.
3. In the **Catalog** page, click the **Google Apps** application.
4. In the Modify application page, click **Entitlements**.
5. Click **+Add user entitlement**.
6. Select the test user and change the **DEPLOYMENT** 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**.

### Set up User in Google Apps for Testing

1. Log in to the Google Admin console at <https://admin.google.com> as administrator.
2. Click **Users**.
3. Point to the green + sign at the bottom-right of the page and click **Add user**.



4. In the **Create a new user** dialog box, enter the first name, last name, and email address of the test user. Ensure that the information matches the test user information in the VMware Identity Manager service.
5. Click **CREATE** to create the new user.

## Verify Test User Can Sign in to Google Apps from VMware Identity Manager

1. Log in to the Workspace ONE portal as the test user.
2. Click the Google Apps icon on the Launcher page.  
You should now have single sign-on access to Google Apps.

## Entitling Users to Google Apps

You can activate single sign-on for all users. Before you do so, either ensure that all the users are added to Google Apps or enable provisioning.

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Google Apps**.
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](http://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.