

OneLogin for Google Apps

www.onelogin.com | twitter.com/onelogin

OneLogin, Inc. | 150 Spear Street, Suite 1400, San Francisco, CA 94105

855.426.7227



1. Signup for OneLogin
2. Adding Google Apps to OneLogin
3. Setting up Single Sign-on
4. Mapping Google Apps to Users
5. Rule Provisioning
6. POP3 / IMAP Passwords
7. Direct Linking to Mail, Docs, Calendars, and Sites
8. Adding Your Directory

1. SIGN UP FOR ONELOGIN

OneLogin is the smart and simple way to eliminate passwords and automate user management for Google Apps!

1.1 If you don't already have OneLogin, start by navigating to the OneLogin homepage and proceed to the OneLogin free trial at <http://www.onelogin.com/partners/app-partners/google-apps>. At this point, you should be re-directed back into your account and have selected a password. Once you're within your OneLogin account, let's get started on setting up Google Apps.

2. ADDING GOOGLE APPS TO ONELOGIN

2.1 To add Google Apps to your OneLogin account, start at your dashboard portal and proceed to **Apps > Add Apps** and search for 'Google Apps'. Select the connector that just says 'Google Apps', and when you're in the configuration page, ensure that the connector is set to 'SAML 2.0. Afterwards', select **Save** to add Google Apps to your account.

3. SETTING UP SINGLE SIGN-ON

NOTE: Google Apps usernames are the name part of the email address for the users. Do not provide SAML access to your Google Apps account for other users than those on your domain. If you invite a user from another domain into your OneLogin account, you might accidentally give that user access to Google Apps.

3.1 Upon adding Google Apps to your account, you will be immediately brought into the app **Info** page. Instead, select the **Configuration** tab adjacent to it. Here you'll start under the **Application Details** section by inputting your organization's custom OneLogin domain under **Domain**.

3.2 After, enter the administrative credentials for your Google Apps account, with the username under **API Email**, and password under **API Password**. Completed, your page will resemble the example below and when you're done, select **Save** to confirm your settings.

← Google Apps MORE ACTIONS ▾ SAVE

Info **Configuration** Parameters Rules SSO Access Provisioning Users Setup

Application Details

Domain

 Your main company domain, e.g. mycompany.com

API Email

API Password

[Generate password](#) [Toggle visibility](#)

3.3 Proceed now to the **Parameters** tab. First you'll want to ensure that **Credentials** are set to 'Configured by admin', and that User Attribute fields are set to the value mappings specified in left column. When your page resembles the example below, select **Save** to confirm your configuration.

Here's a quick list of the required mappings you'll be needing within the User Fields section:

Aliases

-No Default-

Email

-Email name part-

First Name

First Name

Groups

-No Value-

Is Admin

False

Last Name

Last Name

Organization

-No Value-

Password

SSO Password

← Google Apps MORE ACTIONS SAVE

Info Configuration **Parameters** Rules SSO Access Provisioning Users Setup

Credentials are

☒ Configured by admin
☐ Configured by admins and shared by all users

Google Apps Field	Value
Aliases	- No default -
Email	Email name part
Firstname	First Name
Groups	- No value -
Is Admin	False
Lastname	Last Name
Organization	- No value -
Password	SSO password

3.4 Next, navigate over to the SSO page. Here you'll be begin by copying the **SAML 2.0 Endpoint**, and then proceed to 'View Details' under the associated X.509 Certificate to view that certificate's page. Select the **X.509 PEM** format, and then **Download** to acquire the certificate. The certificate and both URL's will be placed within the Google Apps dashboard to confirm the SAML SSO connection.

← Google Apps MORE ACTIONS SAVE

Info Configuration Parameters Rules **SSO** Access Provisioning Users Setup

Assumed Sign-In ☐ Allow assumed users to sign into this app

When enabled, admins who assume users can sign into this app with their identity. This setting can only be changed by the account owner. Note that the account owner can also completely disable the assume feature under Account -> Settings.

Single Sign On

Sign on method
SAML2.0

X.509 Certificate

[Change](#) | [View Details](#)

Issuer URL

SAML 2.0 Endpoint (HTTP)

SLO Endpoint (HTTP)

3.5 With the SAML configuration completed for the OneLogin end of the setup, let's proceed over to the Google Apps admin dashboard. Starting at the administrator dashboard, navigate to **Security > Advanced Settings > Set up single sign-on (SSO)**.

3.67 Here we'll be installing the information from OneLogin's Google Apps configuration page to confirm the SAML connection between the two. Start by selecting **Enable Single Sign-on** and then proceed to upload the x.509 certificate under **Verification certificate**. Afterwards, fill out the rest of the form with the information on the left and when you've finished, select **Save changes** to confirm the setting configuration.

With the information from OneLogin's Google Apps configuration page, fill in the following fields like so:

Sign-in page URL

<Your SAML HTTP Endpoint>

Sign-out page URL

<https://app.onelogin.com/client/apps>

Change password URL

<https://app.onelogin.com/password>

Security ? ⚙

Set up single sign-on (SSO)

To set up SSO, please provide the information below. [SSO Reference](#)

☒ **Enable Single Sign-on**

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

Sign-out page URL *
 URL to redirect users to when they sign out

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

Verification certificate *
 A certificate file has been uploaded. [Replace certificate](#)

The certificate file must contain the public key for Google to verify sign-in requests. [Learn more](#)

☐ **Use a domain specific issuer**

This must be checked if your domain uses an IDP Aggregator to handle SAML requests. If enabled, the issuer value sent in the SAML request will be **google.com/a/tryonelogin.com** instead of simply **google.com**. [Learn more](#)

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16)
 For ranges, use a dash. Example: (64.233.167-204.99/32)
 All network masks must end with a CIDR. [Learn more](#)

With the config, OneLogin and Google Apps should be successfully connected via SAML!

4. MAPPING GOOGLE APPS TO USERS

With SAML successfully enabled and single sign-on properly configured, let's allocate Google Apps to a group of users.

Roles are the key component of OneLogin that grant users access to an application. In many cases, Roles are linked to a security group in the corporate directory and members of that group are then granted access to apps in OneLogin.

4.1 Proceed to **Users > Roles > New Role** and give your role a name and associate it with Google Apps. For simplicity I will use a Role named "Google Apps" and the Security Group named "Google Apps" in Active Directory.

← Google Apps

MORE ACTIONS ▾

SAVE

Applications

Users

Select Applications for this Role

Blue Jeans Network

Google Apps

Nexgate

Small Improvements

Bonusly

Google Apps

Office 365

SpringCM

4.2 Now with the Role established, let's generate a custom mapping that will assign the the Role of Google Apps to everyone within the Group of Google Apps. Proceed to **Users > Mappings** and, seeing as we have no mappings that includes Google Apps, go ahead and select **New Mapping**.

4.3 In the **Custom Mapping** page, you can name a mapping and give it actions, and a condition to execute that action; here we're making a simple group for Google Apps, a Role we've generated to give a group of users Google Apps based on their active directory grouping. When you've created your mapping, select **Save** to proceed.

← Google Apps Mapping

CANCEL

SAVE

Conditions			+
MemberOf ▾	equals ▾	Syncplicity	-
Actions			+
Set role ▾	Google Apps ▾		-

4.4 Note how when the **Condition** = Memberof > Contains > Google Apps, **Perform these actions** = Set role > Google Apps, it's saying that 'Anytime a user is a member of the group Google Apps, set their role to 'Google Apps'. Mappings are flexible, so tailor them to your personal user situations.

4.5 You can always check what users are going to be affected by your mapping by selecting **More Actions > Preview All Mapped Users** or **Preview All Mapped Users**.

4.6 Once you're back in the Mappings page, select **Reapply All Mappings** to confirm and refresh the mapped entitlements to all users.

At this point, you and your users should have full access to Google Apps and be able to log in to their accounts via single sign-on!

5. RULE PROVISIONING

5.1 Google Apps can be provisioned to users via mappings discussed previously, but can also be provisioned through **Rules** within the connector itself. Proceed to the **Apps > Company Apps > Google Apps > Configuration**, and under the **API Connection** section, input your Google Apps administrative username and password under **Admin Email**, and **Admin Password**, respectively. When you've established the connection by selecting **Connect**, select **Save** to confirm your settings.

5.2 Proceed to the **Provisioning** tab within the Google Apps connector page and begin by selecting **Enable provisioning for Google Apps**. You may also configure which provisioning actions require administrator approval to execute, while deselecting an action will allow it to execute automatically. Settings for defining what occurs in Google Apps when a **User is Deleted** from OneLogin are also found here.

5.3 When you've configured your settings, select **Refresh Entitlements** (which should be done whenever settings are changed) and then select **Save** to confirm your configuration.

← Google Apps MORE ACTIONS SAVE

Info Configuration Parameters Rules SSO Access **Provisioning** Users Setup

Workflow

☒ Enable provisioning for Google Apps

Require admin approval before this action is performed in Google apps

☒ Create user ☒ Delete user ☒ Update user

When users are deleted in OneLogin, perform this action in Google apps

Delete

Entitlements [Refresh Entitlements](#)

5.4 Proceed now to the **Rules** tab. Here we'll create the mapping that associates various attributes within Google Apps to a user or group of users. Select **New Rule** to bring up the **New Mapping** pane. Here, the example below shows a user with the name of 'Josh Ames' being mapped to the Role of Administrator within Google Apps.

New Mapping

Name Administrator - Josh

Conditions

DistinguishedName equals Josh Ames

Actions

Set Is Admin

☒ Is Admin

CANCEL SHOW AFFECTED USERS SAVE

5.5 Note how when the **Conditions** = DistinguishedName > equals > Josh Ames, **Perform these actions** = Set Roles > Administrator, it's saying that 'If provisioning encounters a User named Josh Ames, assign him into the Google Apps Role of 'Administrator'. Be aware that each application has a different set of available mappings based upon the application's features and functionality.

5.6 As always, you can select **Show Affected Users** to see which users will be affected by your configuration before you commit to any mappings. And as always, be sure to **Refresh Entitlements** in the **Provisioning** tab whenever you change any settings.

6. POP3/IMAP PASSWORDS

Once you enable SAML in Google Apps, users can no longer change the password their POP3/IMAP mail client uses to retrieve mail.

6.1 Make sure you enter your administrator email and password when setting up the app, as this is required for users to set their mail client password via the dashboard. This is done by editing the Google Apps login and then selecting **Change Password**.

Please note:

- The provisioning API must be enabled for your Google Apps account.
- The credentials used for changing passwords must be that of a Google Apps account Super Admin.
- You must login to Google Apps as this user to accept the user agreement.

7. DIRECT LINKING TO MAIL, DOCS, CALENDARS, AND SITES

7.1 You can use regular bookmarks to jump directly to Mail, Docs, Calendar and Sites. See <https://onelogin.zendesk.com/hc/en-us/articles/201174234-Quick-navigation-in-Google-Apps-with-bookmarks> for more information on how to get that up and running.

8. ADDING YOUR DIRECTORY

OneLogin easily integrates with all major user and corporate directories, and linking them to your account is incredibly easy.

6.1 Start by going to **Users > Directories** to select the directory you wish to integrate and then select it.

Select a Directory Type

CANCEL

Directories allow you to sync users with an external user store, such as Active Directory or Google Apps as well as authenticate users using the password in that user store. You can configure multiple directories, for example one for employees and one for contractors. Or you can simply use OneLogin as your directory.

 Active Directory Install OneLogin's Active Directory Connector, which synchronizes users in real-time and enables authentication against AD. All communication is done over outbound SSL and does not require firewall changes.	 Google Apps Users are periodically synchronized during the day and users are authenticated against Google Apps using their Google password.	 LDAP via SSL Authenticate users against any LDAP server using LDAP or LDAP/SSL. Synchronize users from LDAP into OneLogin.
 LDAP via Connector Install OneLogin's LDAP Connector, which synchronizes users in near real-time and enables authentication against LDAP. All communication is done over outbound SSL and does not require firewall changes.	 Workday Use Workday as your system of record for employees. Users are periodically imported into OneLogin.	 Workday Custom Reports - Beta Use Workday as your system of record for employees. Users are periodically imported into OneLogin via Workday's Custom Reports.

6.2 Each directory has its own workflow and such things are detailed elsewhere. Here are some links to helpful articles detailing how to configure your directory:

Active Directory:

<https://onelogin.zendesk.com/hc/en-us/articles/202361690-Directory-Active-Directory>

LDAP via Connector:

<https://onelogin.zendesk.com/hc/en-us/articles/202361700-Directory-LDAP>

Google Apps:

<https://onelogin.zendesk.com/hc/en-us/articles/202361710-Directory-Google-Apps>

Questions?

Send us an email at support@onelogin.com