

Integrate With Google Apps

OpenAM can serve as the identity provider when you use [Google Apps for Business](#).

- [Install & Configure OpenAM](#)
- [Create a Hosted Identity Provider](#)
- [Configure Google Apps for Single Sign-On](#)
- [Enable Access to the Google Apps API](#)

Install & Configure OpenAM

1. See the latest draft of the [OpenAM Installation Guide](#) for instructions.
2. Configure a certificate for the Signing Key in the OpenAM key store.
The key store is under the OpenAM configuration directory, for example `$HOME/openam/openam/keystore.jks`.
3. Set up a identity repository for your users.
Your users must have the same user IDs in OpenAM and in Google Apps.

Create a Hosted Identity Provider

1. In the OpenAM console Common Tasks page, click Create Hosted Identity Provider.
2. Accept the default values, and provide a name for your New Circle of Trust before clicking configure.

Create a SAMLv2 Identity Provider on this Server Configure Cancel

This page allows you to configure this instance of OpenAM server as an Identity Provider (IDP). You can provide a Name for the provider, Circle of Trust (COT), its metadata of the provider and optionally Signing Certificate. A COT is a group of IDPs and Service Providers (SPs) that trust each other and in effect represents the confines within which all federation communications are performed. Metadata represents the configuration necessary to execute federation protocols (eg SAMLv2) as well as the mechanism to communicate this configuration to other entities (eg SPs) in a COT. We shall generate the metadata if you do not have one. You are required to pick a realm for this provider if there are more than one realm in the system. Otherwise, this provider will be configured under the root realm.

* Indicates required field

Do you have metadata for this provider?: Yes No ?

metadata

* Name: ?

Signing Key: Please note "test" is a selfsigned certificate setup at installation for testing purposes. It is recommended you obtain a certificate from a Certificate Authority for production deployments. ?

Circle of Trust

Choose from existing circles of trust listed or provide one to be created in which to include this IDP. A COT is a group of IDPs and SPs that trust each other and provides the confines within which all SAMLv2 communications are performed.

* New Circle of Trust:

Attribute Mapping

3. On the "What would you like to do next?" page, click configure Google Apps.

Configure Google Apps for Single Sign-On

1. Add the domain name you registered with Google Apps in the Configure the Remote SP list.

Configure Google Apps for Single Sign-On Create Cancel

You must provide Identity Provider and remote Service Provider information before the metadata can be configured. OpenAM acts as the Identity Provider, and Google Apps acts as the Service Provider. SAMLv2 is the single sign-on protocol for creating a circle of trust at the Identity Provider.

* Indicates required field

* Circle of Trust: GoogleAppsCOT

* Identity Provider: http://openam.example.com:8080/openam

Configure the Remote SP

* Domain Name: Current Values Remove

New Value Add

This is the primary domain you have registered at Google Apps. Example: domain.com

2. Click Create.

- On the "Google Apps Single Sign-On Configuration" page, download a copy of the Verification Certificate.

Google Apps Single Sign-On Configuration Finish

You must supply the following information to Google Apps when you configure Google Apps Single Sign-On. Save these URLs and Verification Certificate information before proceeding to Google Apps Single Sign-On setup.

URLs

Sign-in Page URL:
URL for signing in to OpenAM 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 OpenAM

Verification Certificate

Verification Certificate:

```
-----BEGIN CERTIFICATE-----
MIICQDCCAAkCBEdNB0swDQYJKoZIhvcNAQEEBQAwZzELMAkGA1UEBhMCVVMxZzARBgNVBAgTCkNh
bGImb3JuaWEzFDASBgNVBAQTC1NhbWVhbnRlENsYXJhMQwwCgYDVQQKEwN0dW4xZDA0BgNVBAAsTB09w
ZW50U08xDTALBgNVBAMTBHRlc3QwHhcNMDE1MTkxOTM5WzYxOTM5WjBnMQswCQYDVQQGEwJVUzE
tMBEGA1UECBMkQ2FsaWZvcm5pYTEUMBIGA1UEBxMLU2FudGEgQ2xhcmExDDAKBgNVBAoTA1N1bjE
QMA4GA1UECzMHT3BibINTZENNAsGA1UEAxMEdGVzdDCBnzANBgkqhkiG9w0BAQEFAAOBQAwgYkC
gYEArsQcU75GB2AikhbGS5piiLkmJzqEsp64DxbMJ+xDrye0EN/q1U5Qf+RkDsaN/gkAvV1cuX
EgTL6RlaFFPcUX7QxDhZBhsYF9pbwIMz4A4su9hnxhURebGEmxKW9qJNYJs0Vos+gjkUEWj
mVgHTs1+mq5QYTA7E6Zyl8CAWEAAATANBgkqhkiG9w0BAQFAAOBgQ3PwUJQzPKTPTTY9upbF
XlrAKMwIF2OW4yGWWVlcwNSZJmTJ8ARvVYOMEVnbsT4Ofu2/PeYoAdIDAcy/F2Zuj8XJpuQRSE
6PQqBuDEHjImOQJ0r/r8mO1ZCHRhPz5zYRjRRC9eCbjx9VrFax0JDC/FwWigmrW0Y0Q=====
END CERTIFICATE-----
```

[Click here to download](#)

Copy this text to a text file, and upload the new text file to the Google Apps Verification Certificate.

Enable Access to the Google Apps API

- Follow the instructions at the bottom of the "Google Apps Single Sign-On Configuration" page.