mobileiron

Cookbook for Azure AD

Shruthy Devendra | December 30,2021 | r43

Configuring Azure AD

SAML provides single sign-on service for users accessing their services hosted in a cloud environment. Generally, a service provider such as G Suite is federated with an identity provider such as Azure AD for authentication. The user gets authenticated by Azure AD and obtains a SAML token for accessing applications in a cloud environment.

This document serves as step-by-step configuration manual for users using Azure AD as an authentication provider in a cloud environment.

Complete the following steps to configure Azure AD:

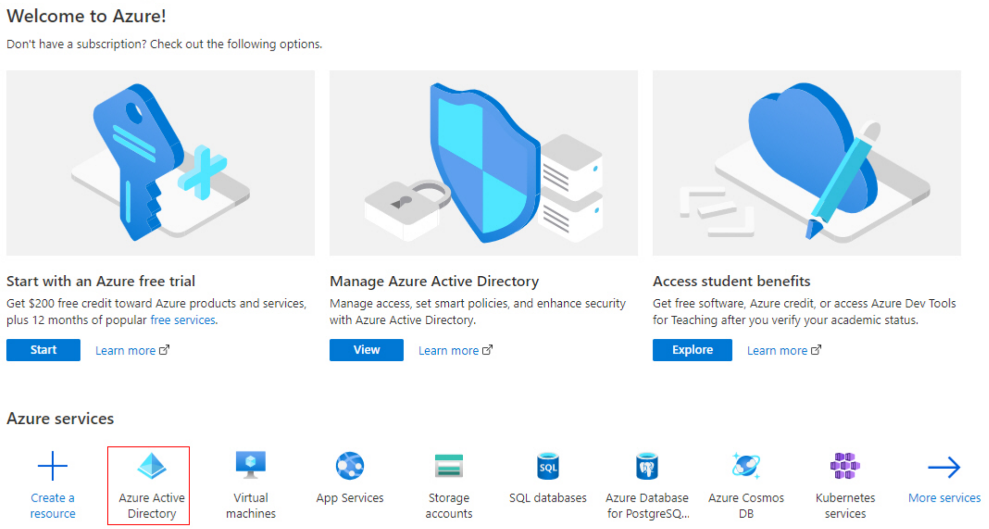
- **Fetching metadata files for Azure AD**
- **Configuring Azure AD**

Fetching Metadata files for Azure AD

- **Entity ID:** https://sts.windows.net
  Post SSO URL: https://login.microsoft.com/
  Redirect SSO Url: https://login.microsoft.com/

Configuring Azure AD

1. Login to Azure portal with admin credentials.
2. Under Azure Services, click **Azure Active Directory. The Overview page opens.**



Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

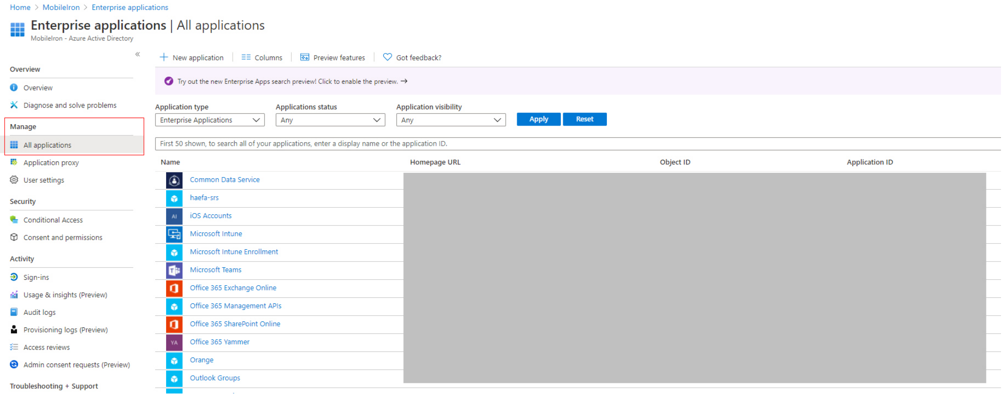
Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

1. On the left navigation pane, navigate to **Enterprise applications** > **All Applications**.



Home > MobileIron > Enterprise applications
Enterprise applications | All applications
MobileIron - Azure Active Directory
«
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Consent and permissions
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
Access reviews
Admin consent requests (Preview)
Troubleshooting + Support
New application
Columns
Preview features
Got feedback?
Apply
Reset

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application type: Enterprise Applications

Applications status: Any

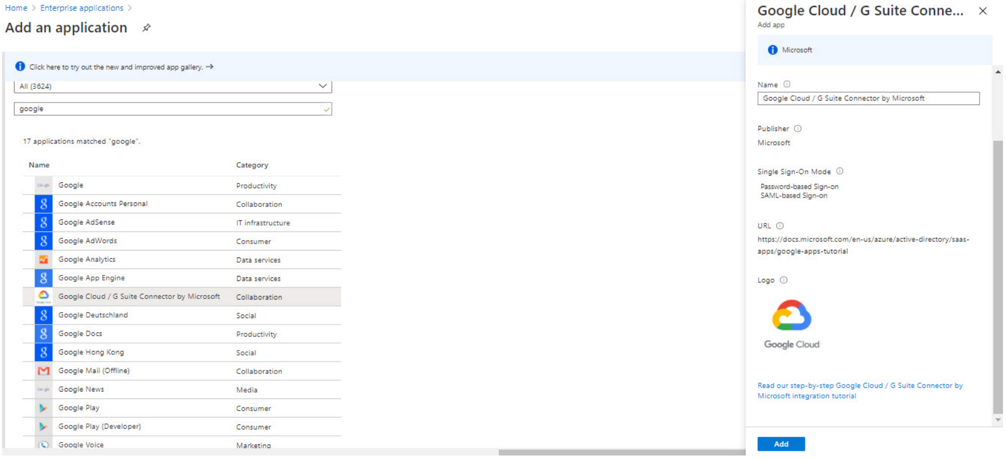
Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID	Application ID
Common Data Service	[redacted]	[redacted]	[redacted]
haefa-srs	[redacted]	[redacted]	[redacted]
iOS Accounts	[redacted]	[redacted]	[redacted]
Microsoft Intune	[redacted]	[redacted]	[redacted]
Microsoft Intune Enrollment	[redacted]	[redacted]	[redacted]
Microsoft Teams	[redacted]	[redacted]	[redacted]
Office 365 Exchange Online	[redacted]	[redacted]	[redacted]
Office 365 Management APIs	[redacted]	[redacted]	[redacted]
Office 365 SharePoint Online	[redacted]	[redacted]	[redacted]
Office 365 Yammer	[redacted]	[redacted]	[redacted]
Orange	[redacted]	[redacted]	[redacted]
Outlook Groups	[redacted]	[redacted]	[redacted]

1. Click **New application**.

2. Under Add from the gallery, type Google.
3. In the results panel, select **Google Cloud / G Suite Connector by Microsoft** and click **Add**.


Home > Enterprise applications >
Add an application
Click here to try out the new and improved app gallery. →
Google Cloud / G Suite Conne...
Add app
Microsoft
Add

All (3624)

google

17 applications matched "google".

Name	Category
Google	Productivity
Google Accounts Personal	Collaboration
Google AdSense	IT infrastructure
Google AdWords	Consumer
Google Analytics	Data services
Google App Engine	Data services
Google Cloud / G Suite Connector by Microsoft	Collaboration
Google Deutschland	Social
Google Docs	Productivity
Google Hong Kong	Social
Google Mail (Offline)	Collaboration
Google News	Media
Google Play	Consumer
Google Play (Developer)	Consumer
Google Voice	Marketing

Name: Google Cloud / G Suite Connector by Microsoft

Publisher: Microsoft

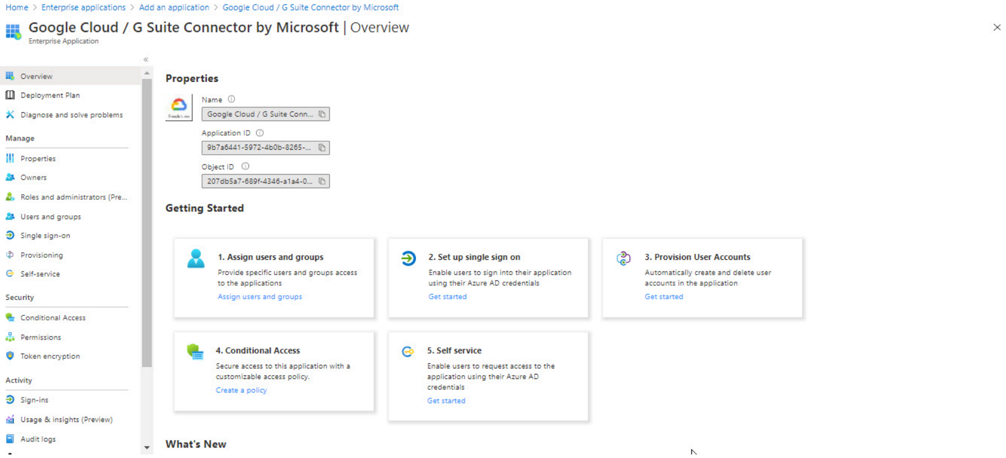
Single Sign-On Mode: Password-based Sign-on
SAML-based Sign-on

URL: https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/google-apps-tutorial

Logo: Google Cloud

Read our step-by-step Google Cloud / G Suite Connector by Microsoft integration tutorial

4. On the Google Cloud application integration page, click **Set up single sign-on**.


Home > Enterprise applications > Add an application > Google Cloud / G Suite Connector by Microsoft
Google Cloud / G Suite Connector by Microsoft | Overview
Enterprise Application
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators (Pre...
Users and groups
Single sign-on
Provisioning
Self-service
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-ins
Usage & insights (Preview)
Audit logs

Properties

Name: Google Cloud / G Suite Conn...

Application ID: 9b7a6441-5972-4b0b-8265-...

Object ID: 207db5a7-689f-4346-a1a4-0...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

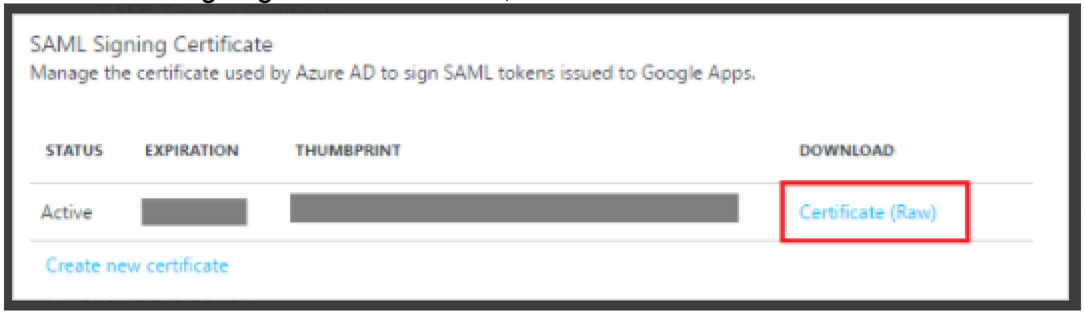
5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

What's New

1. On the Single sign-on dialog, select mode as **SAML** to enable single sign-on.

2. On the **Google Apps Domain and URLs** section, enter the following details:

3. On the **SAML Signing Certificate** section, click **Certificate** and then save the certificate on your computer. Click **Save**.



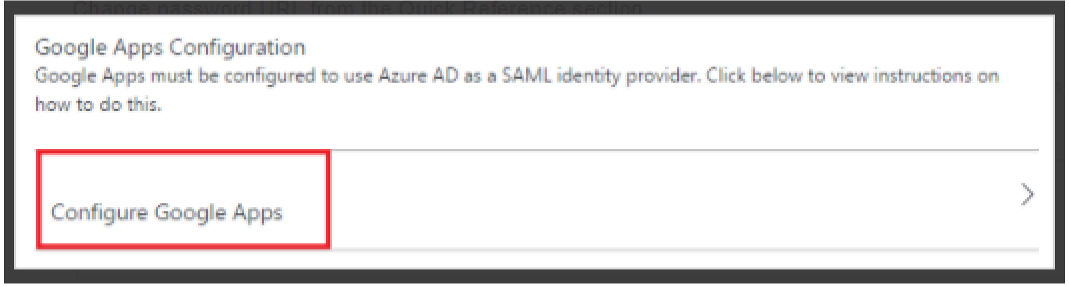
SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to Google Apps.

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active	[redacted]	[redacted]	Certificate (Raw)

Create new certificate

4. On the **Google Apps Configuration** section, click **Configure Google Apps** to open Configure sign-on window.
   Copy the **Sign-Out URL**, **SAML Single Sign-On Service URL** and **Change password URL** from the Quick Reference section.



Google Apps Configuration

Google Apps must be configured to use Azure AD as a SAML identity provider. Click below to view instructions on how to do this.

Configuring Access to create a Federated Pair

You must configure Access to create a federated pair.

Prerequisites

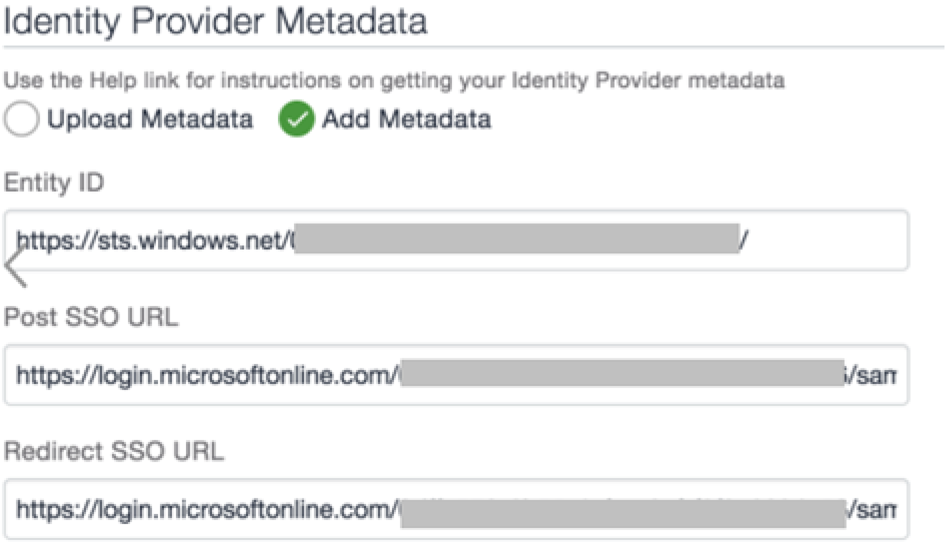
Verify that you have configured G Suite and Azure AD. See Prerequisites.

Procedure

1. Log in to **Access**.
2. Click **Profile** > **Get Started**.
3. Enter the Access host information, and upload the **ACCESS SSL certificate** in p12 format. All the other fields are set to default. Click **Save**.
4. On the **Federated Pairs** tab, click **Add New Pair** and select **G Suite** as the service provider.
5. Enter the following details:
   - Name

- Description
- Upload the Access Signing Certificate or click **Advanced Options** to create a new certificate.
- Click **Add Metadata** and enter the entity ID and Assertion consumer Service URL:
  Entity ID: https://docs.google.com/a/<domain_name>
  Assertion Consumer Service URL: https://www.google.com/a/domain_name/acs
- (Optional) Select *Use Tunnel Certificates for SSO* to configure Cert SSO on MobileIron Core. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/current/accs/

6. Click **Next**.
7. Select **Azure AD** as the Identity provider. Click **Next**.
8. Select the **Access Signing Certificate** or click **Advanced options** to create a new certificate.
9. Upload the IdP metadata file that you downloaded. See Prerequisites. Click **Done**.



Identity Provider Metadata

Use the Help link for instructions on getting your Identity Provider metadata

○ Upload Metadata ✓ Add Metadata

Entity ID

https://sts.windows.net/[redacted]/

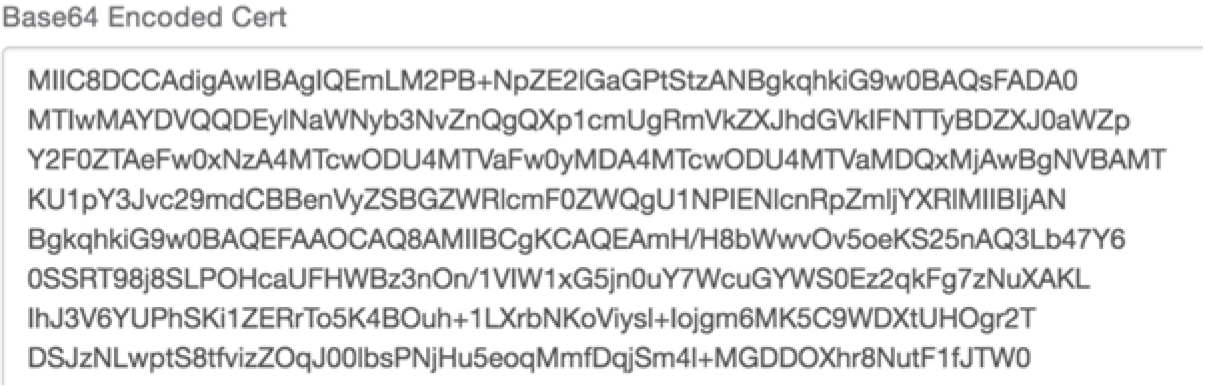
Post SSO URL

https://login.microsoftonline.com/[redacted]/san

Redirect SSO URL

https://login.microsoftonline.com/[redacted]/san

For the Base64 Encoded cert, extract the certificate downloaded from the SAML Signing Certificate in Azure portal. Run the following commands in a terminal:



Base64 Encoded Cert

```
MIIC8DCCAdigAwIBAgIQEmLM2PB+NpZE2lGaGPtStzANBgkqhkiG9w0BAQsFADA0
MTIwMAYDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZp
Y2F0ZTAeFw0xNzA4MTcwODU4MTVaFw0yMDA4MTcwODU4MTVaMDQxMjAwBgNVBAMT
KU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmH/H8bWwvOv5oeKS25nAQ3Lb47Y6
0SSRT98j8SLPOHcaUFHWBz3nOn/1VIW1xG5jn0uY7WcuGYWS0Ez2qkFg7zNuXAKL
IhJ3V6YUPhSKi1ZERrTo5K4BOuh+1LXrbNKoViysl+Iojgm6MK5C9WDXtUHOgr2T
DSJzNLwptS8tfvizZOqJ00lbsPNjHu5eoqMmfDqjSm4l+MGDDOXhr8NutF1fJTW0
```

10. Download the **ACCESS SP Metadata (Upload to IDP)** and the **ACCESS IDP Metadata (Upload to SP)** files from the federated pair page.
11. On the **Profile** tab, click **Publish** to publish the profile.