Tutorial: Azure Active Directory single sign-on (SSO) integration with G Suite

09/23/2019 • 10 minutes to read • +14

In this article

In this tutorial, you'll learn how to integrate G Suite with Azure Active Directory (Azure AD). When you integrate G Suite with Azure AD, you can:

- Control in Azure AD who has access to G Suite.
- Enable your users to be automatically signed-in to G Suite with their Azure AD accounts.
- Manage your accounts in one central location - the Azure portal.

To learn more about SaaS app integration with Azure AD, see What is application access and single sign-on with Azure Active Directory.

Prerequisites

To get started, you need the following items:

- An Azure AD subscription.
- G Suite single sign-on (SSO) enabled subscription.
- A Google Apps subscription or Google Cloud Platform subscription.

ⓘ Note

To test the steps in this tutorial, we do not recommend using a production environment. This document was created using the new user Single-Sign-on experience. If you are still using the old one, the setup will look different. You can enable the new experience in the Single Sign-on settings of G-Suite application. Go to **Azure AD, Enterprise applications**, select **G Suite**, select **Single Sign-on** and then click on **Try out our new experience**.

To test the steps in this tutorial, you should follow these recommendations:

- Do not use your production environment, unless it is necessary.
- If you don't have a subscription, you can get a free account.

Frequently Asked Questions

1. **Q: Does this integration support Google Cloud Platform SSO integration with Azure AD?**

   A: Yes. Google Cloud Platform and Google Apps share the same authentication platform. So to do the GCP integration you need to configure the SSO with Google Apps.

2. **Q: Are Chromebooks and other Chrome devices compatible with Azure AD single sign-on?**

   A: Yes, users are able to sign into their Chromebook devices using their Azure AD credentials. See this G Suite support article for information on why users may get prompted for credentials twice.

3. **Q: If I enable single sign-on, will users be able to use their Azure AD credentials to sign into any Google product, such as Google Classroom, GMail, Google Drive, YouTube, and so on?**

   A: Yes, depending on which G Suite you choose to enable or disable for your organization.

4. **Q: Can I enable single sign-on for only a subset of my G Suite users?**

   A: No, turning on single sign-on immediately requires all your G Suite users to authenticate with their Azure AD credentials. Because G Suite doesn't support having multiple identity providers, the identity provider for your G Suite environment can either be Azure AD or Google -- but not both at the same time.

5. **Q: If a user is signed in through Windows, are they automatically authenticate to G Suite without getting prompted for a password?**

A: There are two options for enabling this scenario. First, users could sign into Windows 10 devices via Azure Active Directory Join. Alternatively, users could sign into Windows devices that are domain-joined to an on-premises Active Directory that has been enabled for single sign-on to Azure AD via an Active Directory Federation Services (AD FS) deployment. Both options require you to perform the steps in the following tutorial to enable single sign-on between Azure AD and G Suite.

6. **Q: What should I do when I get an "invalid email" error message?**

   A: For this setup, the email attribute is required for the users to be able to sign-in. This attribute cannot be set manually.

   The email attribute is autopopulated for any user with a valid Exchange license. If user is not email-enabled, this error will be received as the application needs to get this attribute to give access.

   You can go to portal.office.com with an Admin account, then click in the Admin center, billing, subscriptions, select your Office 365 Subscription and then click on assign to users, select the users you want to check their subscription and in the right pane, click on edit licenses.

   Once the O365 license is assigned, it may take some minutes to be applied. After that, the user.mail attribute will be autopopulated and the issue should be resolved.

Scenario description

In this tutorial, you configure and test Azure AD SSO in a test environment.

- G Suite supports **SP** initiated SSO
- G Suite supports **Automated** user provisioning

Adding G Suite from the gallery

To configure the integration of G Suite into Azure AD, you need to add G Suite from the gallery to your list of managed SaaS apps.

1. Sign in to the Azure portal using either a work or school account, or a personal Microsoft account.
2. On the left navigation pane, select the **Azure Active Directory** service.
3. Navigate to **Enterprise Applications** and then select **All Applications**.
4. To add new application, select **New application**.

5. In the **Add from the gallery** section, type **G Suite** in the search box.
6. Select **G Suite** from results panel and then add the app. Wait a few seconds while the app is added to your tenant.

Configure and test Azure AD single sign-on for G Suite

Configure and test Azure AD SSO with G Suite using a test user called **B.Simon**. For SSO to work, you need to establish a link relationship between an Azure AD user and the related user in G Suite.

To configure and test Azure AD SSO with G Suite, complete the following building blocks:

1. **Configure Azure AD SSO** - to enable your users to use this feature.
   a. **Create an Azure AD test user** - to test Azure AD single sign-on with B.Simon.
   b. **Assign the Azure AD test user** - to enable B.Simon to use Azure AD single sign-on.
2. **Configure G Suite SSO** - to configure the single sign-on settings on application side.
   a. **Create G Suite test user** - to have a counterpart of B.Simon in G Suite that is linked to the Azure AD representation of user.
3. **Test SSO** - to verify whether the configuration works.

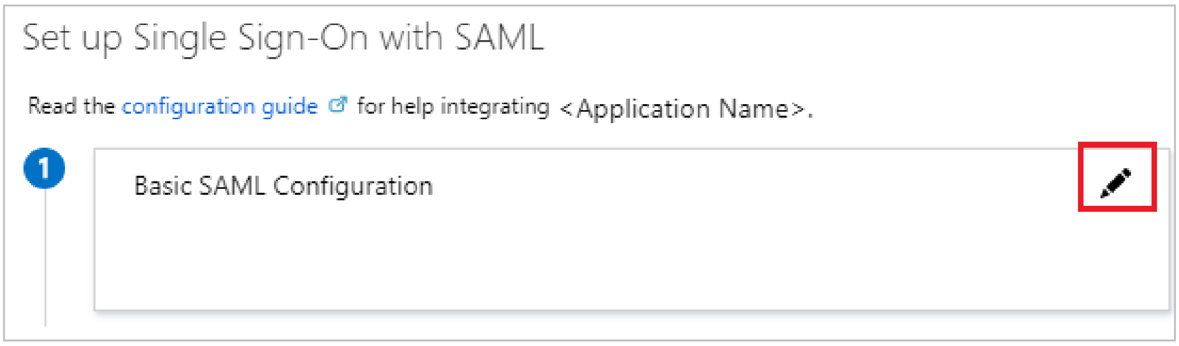
Configure Azure AD SSO

Follow these steps to enable Azure AD SSO in the Azure portal.

1. In the Azure portal, on the **G Suite** application integration page, find the **Manage** section and select **single sign-on**.

2. On the **Select a single sign-on method** page, select **SAML**.

3. On the **Set up single sign-on with SAML** page, click the edit/pen icon for **Basic SAML Configuration** to edit the settings.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating <Application Name>.

1 Basic SAML Configuration

4. On the **Basic SAML Configuration** section, if you want to configure for the **Gmail** perform the following steps:

   a. In the **Sign-on URL** textbox, type a URL using the following pattern: `https://www.google.com/a/<yourdomain.com>/ServiceLogin?continue=https://mail.google.com`

   b. In the **Identifier** textbox, type a URL using the following pattern:

   `google.com/a/<yourdomain.com>`

   `google.com`

   `https://google.com`

   `https://google.com/a/<yourdomain.com>`

5. On the **Basic SAML Configuration** section, if you want to configure for the **Google Cloud Platform** perform the following steps:

   a. In the **Sign-on URL** textbox, type a URL using the following pattern: `https://www.google.com/a/<yourdomain.com>/ServiceLogin?continue=https://console.cloud.google.com`

   b. In the **Identifier** textbox, type a URL using the following pattern:

   `google.com/a/<yourdomain.com>`

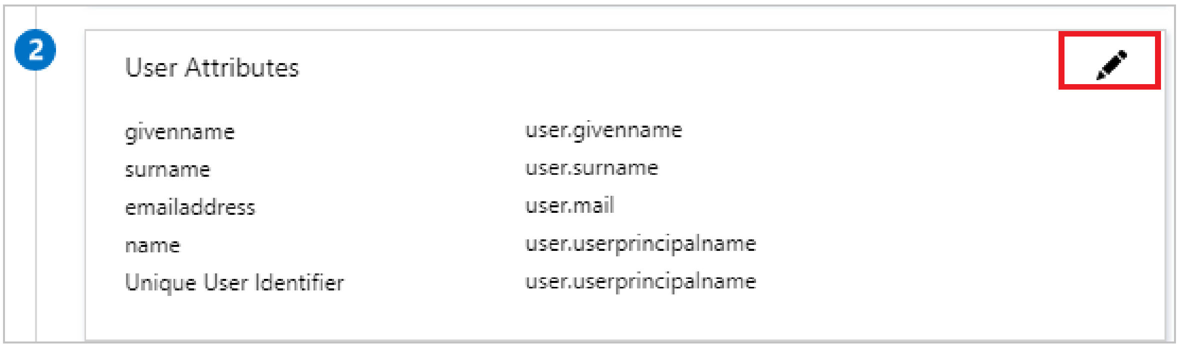
   `google.com`

   `https://google.com`

   `https://google.com/a/<yourdomain.com>`

> ⓘ Note
>
> These values are not real. Update these values with the actual Sign-On URL and Identifier. G Suite doesn't provide Entity ID/Identifier value on Single Sign On configuration so when you uncheck the **domain specific issuer** option the Identifier value will be `google.com`. If you check the **domain specific issuer** option it will be `google.com/a/<yourdomainname.com>`. To check/uncheck the **domain specific issuer** option you need to go to the **Configure G Suite SSO** section which is explained later in the tutorial. For more information contact G Suite Client support team.

6. Your G Suite application expects the SAML assertions in a specific format, which requires you to add custom attribute mappings to your SAML token attributes configuration. The following screenshot shows an example for this. The default value of **Unique User Identifier** is **user.userprincipalname** but G Suite expects this to be mapped with the user's email address. For that you can use **user.mail** attribute from the list or use the appropriate attribute value based on your organization configuration.



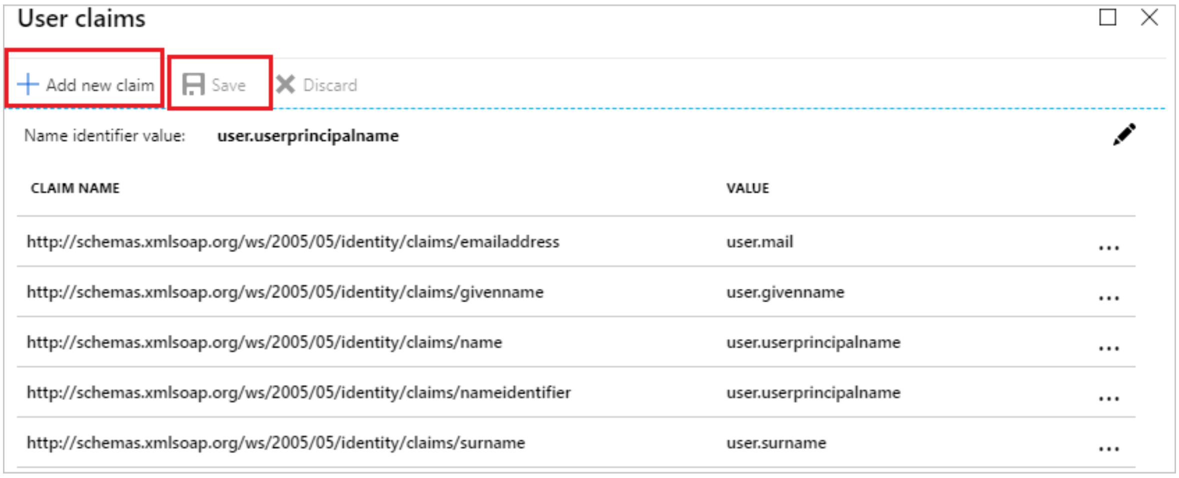
User Attributes

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

7. In the **User Claims** section on the **User Attributes** dialog, edit the claims by using **Edit icon** or add the claims by using **Add new claim** to configure SAML token attribute as shown in the image above and perform the following steps:

Name	Source Attribute
Unique User Identifier	User.mail

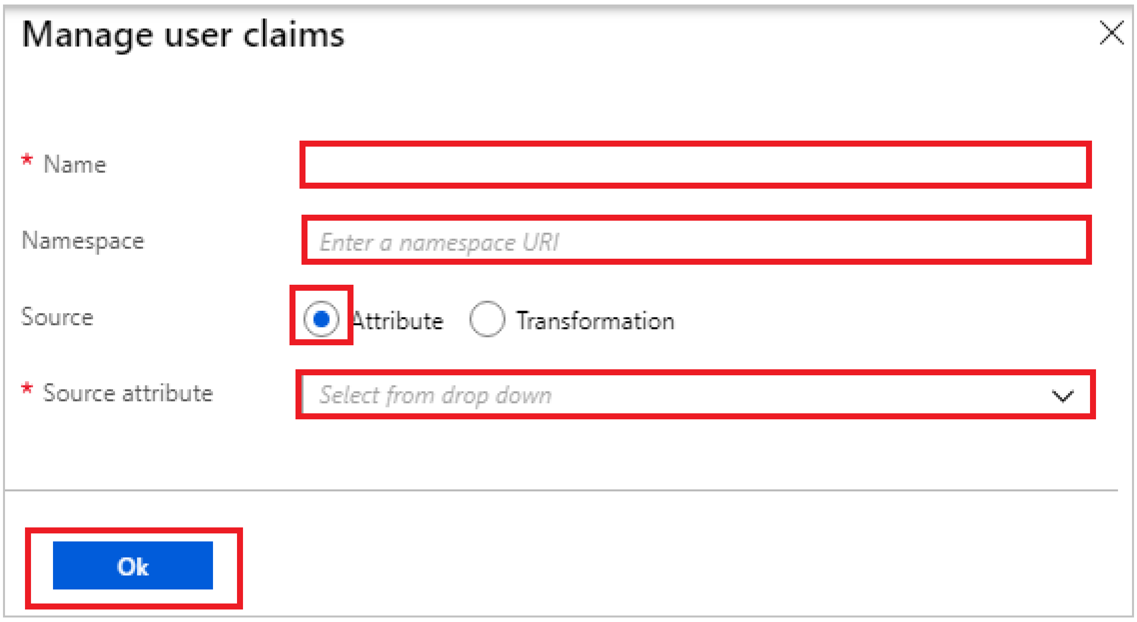
a. Click **Add new claim** to open the **Manage user claims** dialog.



User claims

Name identifier value: user.userprincipalname

CLAIM NAME	VALUE
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname



Manage user claims

* Name

Namespace: Enter a namespace URI

Source: ● Attribute ○ Transformation

* Source attribute: Select from drop down

b. In the **Name** textbox, type the attribute name shown for that row.

c. Leave the **Namespace** blank.

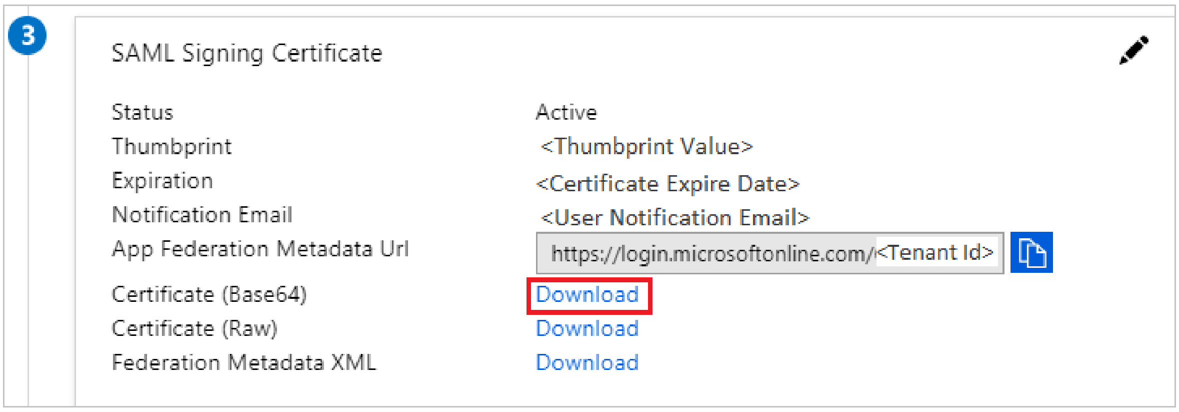
d. Select Source as **Attribute**.

e. From the **Source attribute** list, type the attribute value shown for that row.

f. Click **Ok**

g. Click **Save**.

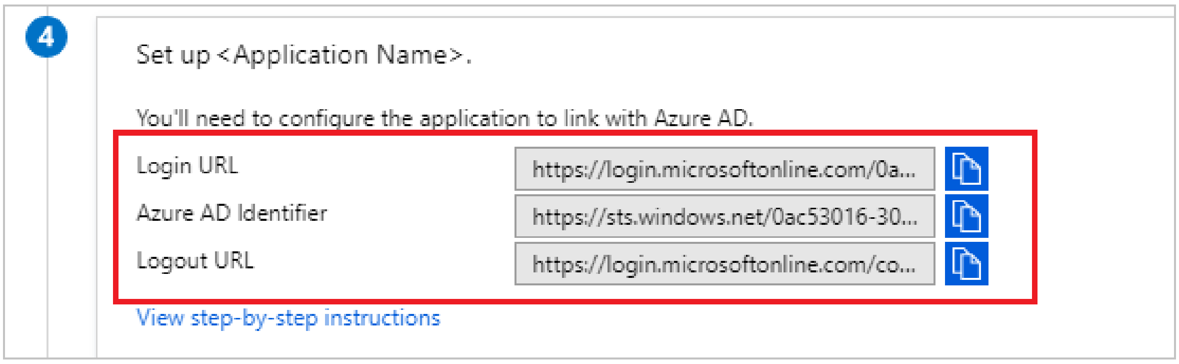
8. On the **Set up single sign-on with SAML** page, in the **SAML Signing Certificate** section, find **Certificate (Base64)** and select **Download** to download the certificate and save it on your computer.



SAML Signing Certificate

Status	Active
Thumbprint	<Thumbprint Value>
Expiration	<Certificate Expire Date>
Notification Email	<User Notification Email>
App Federation Metadata Url	https://login.microsoftonline.com/<Tenant Id>
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

9. On the **Set up G Suite** section, copy the appropriate URL(s) based on your requirement.



Set up <Application Name>.

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/0a...
Azure AD Identifier	https://sts.windows.net/0ac53016-30...
Logout URL	https://login.microsoftonline.com/co...

View step-by-step instructions

Create an Azure AD test user

In this section, you'll create a test user in the Azure portal called B.Simon.

1. From the left pane in the Azure portal, select **Azure Active Directory**, select **Users**, and then select **All users**.
2. Select **New user** at the top of the screen.
3. In the **User** properties, follow these steps:
   a. In the **Name** field, enter `B.Simon`.
   b. In the **User name** field, enter the username@companydomain.extension. For example, `B.Simon@contoso.com`.
   c. Select the **Show password** check box, and then write down the value that's displayed in the **Password** box.
   d. Click **Create**.

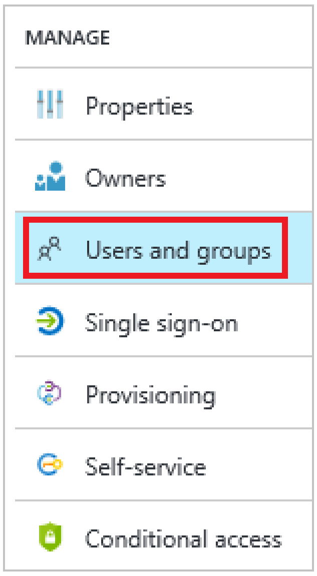
Assign the Azure AD test user

In this section, you'll enable B.Simon to use Azure single sign-on by granting access to G Suite.

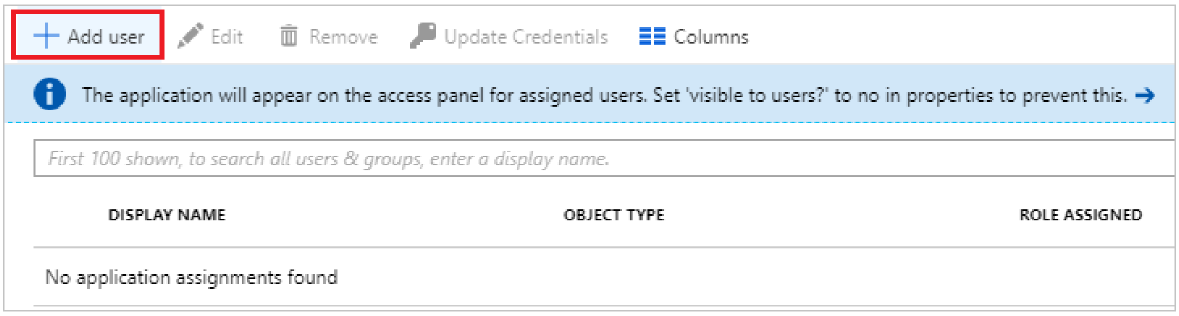
1. In the Azure portal, select **Enterprise Applications**, and then select **All applications**.

2. In the applications list, select **G Suite**.

3. In the app's overview page, find the **Manage** section and select **Users and groups**.



4. Select **Add user**, then select **Users and groups** in the **Add Assignment** dialog.



The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
No application assignments found		

5. In the **Users and groups** dialog, select **B.Simon** from the Users list, then click the **Select** button at the bottom of the screen.

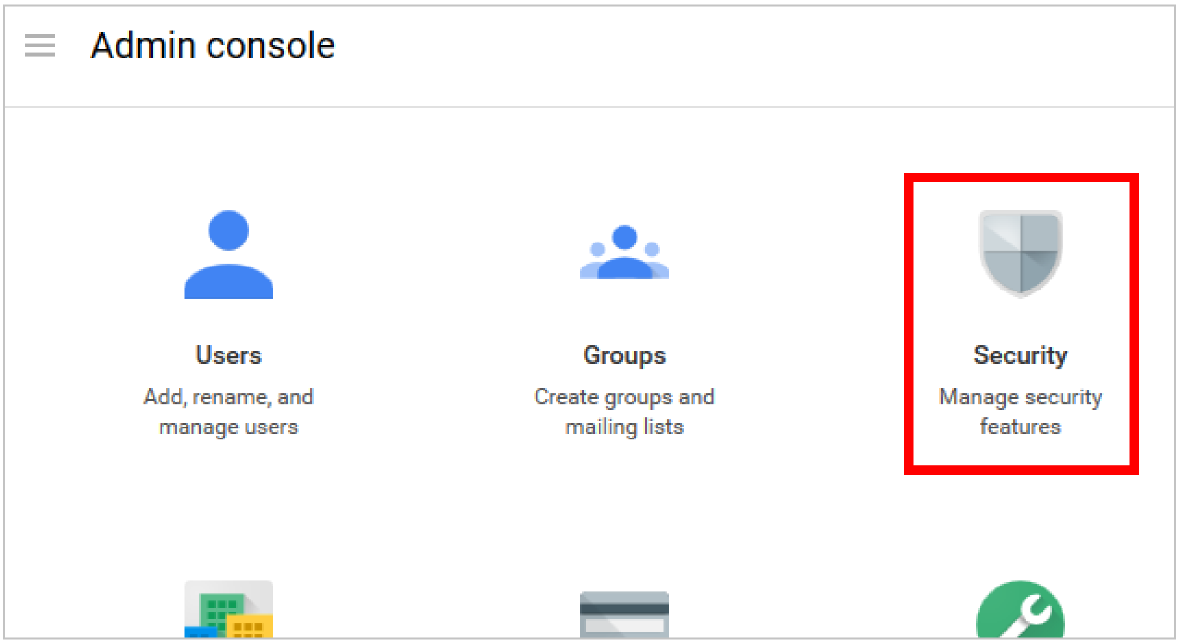
6. If you're expecting any role value in the SAML assertion, in the **Select Role** dialog, select the appropriate role for the user from the list and then click the **Select** button at the bottom of the screen.

7. In the **Add Assignment** dialog, click the **Assign** button.

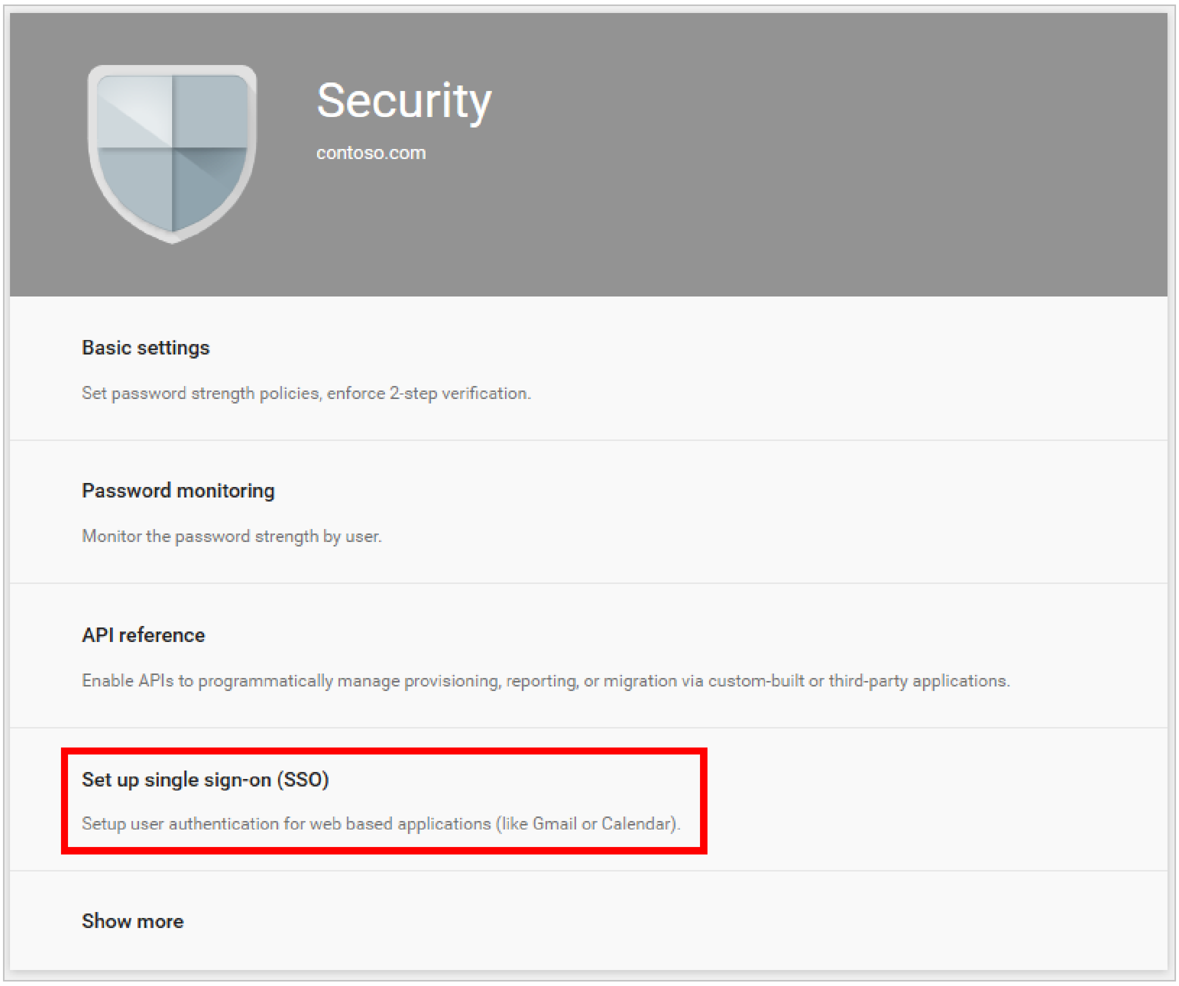
Configure G Suite SSO

1. Open a new tab in your browser, and sign into the G Suite Admin Console using your administrator account.

2. Click **Security**. If you don't see the link, it may be hidden under the **More Controls** menu at the bottom of the screen.


Admin console
Users
Add, rename, and manage users
Groups
Create groups and mailing lists
Security
Manage security features

3. On the **Security** page, click **Set up single sign-on (SSO).**



Security

contoso.com

Basic settings

Set password strength policies, enforce 2-step verification.

Password monitoring

Monitor the password strength by user.

API reference

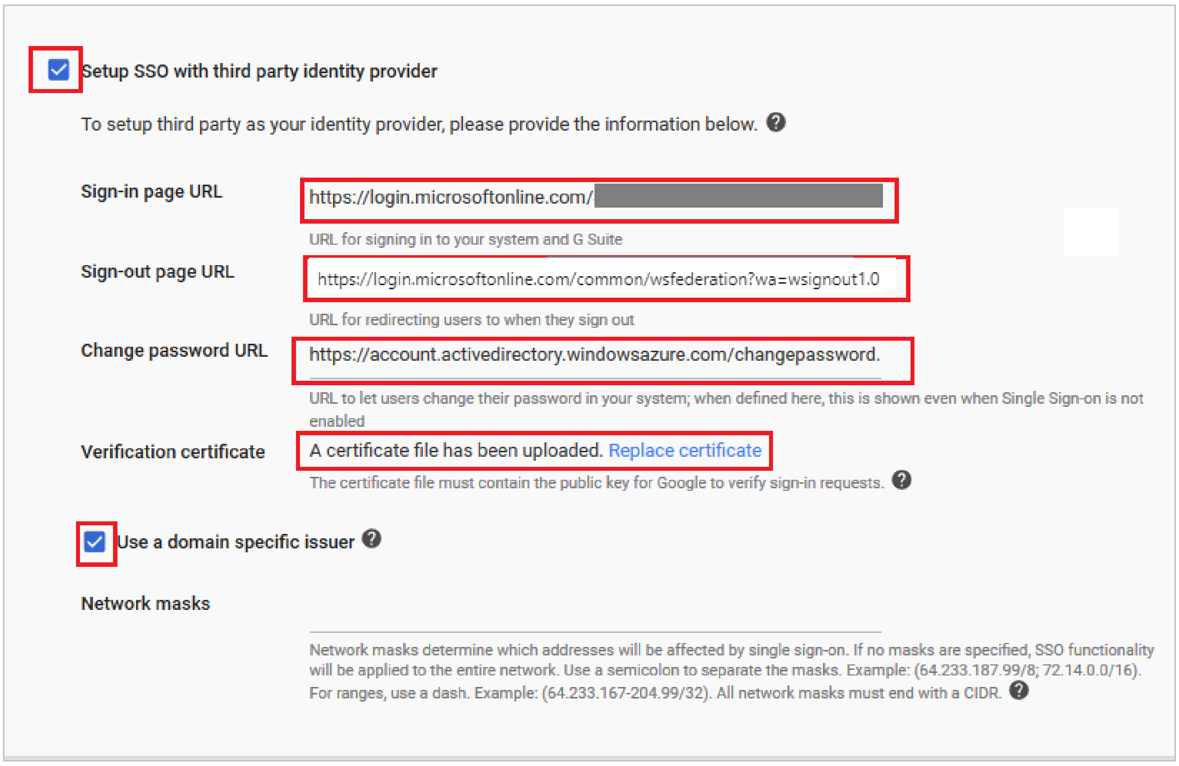
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

Show more

4. Perform the following configuration changes:



☑ Setup SSO with third party identity provider

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

Sign-in page URL: https://login.microsoftonline.com/[redacted]

URL for signing in to your system and G Suite

Sign-out page URL: https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0

URL for redirecting users to when they sign out

Change password URL: https://account.activedirectory.windowsazure.com/changepassword.

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: A certificate file has been uploaded. Replace certificate

The certificate file must contain the public key for Google to verify sign-in requests.

☑ Use a domain specific issuer

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.

a. Select **Setup SSO with third-party identity provider**.

b. In the **Sign-in page URL** field in G Suite, paste the value of **Login URL** which you have copied from Azure portal.

c. In the **Sign-out page URL** field in G Suite, paste the value of **Logout URL** which you have copied from Azure portal.

d. In the **Change password URL** field in G Suite, paste the value of **Change password URL** which you have copied from Azure portal.

e. In G Suite, for the **Verification certificate**, upload the certificate that you have downloaded from Azure portal.

f. Check/Uncheck the **Use a domain specific issuer** option as per the note mentioned in the above **Basic SAML Configuration** section in the Azure AD.

g. Click **Save Changes**.

Create G Suite test user

The objective of this section is to create a user in G Suite called B.Simon. After the user has manually been created in G Suite, the user will now be able to sign in using their Office 365 login credentials.

G Suite also supports automatic user provisioning. To configure automatic user provisioning, you must first configure G Suite for automatic user provisioning.

> ⓘ Note
>
> Make sure that your user already exists in G Suite if provisioning in Azure AD has not been turned on before testing Single Sign-on.

> ⓘ Note
>
> If you need to create a user manually, contact the **Google support team**.

Test SSO

In this section, you test your Azure AD single sign-on configuration using the Access Panel.

When you click the G Suite tile in the Access Panel, you should be automatically signed in to the G Suite for which you set up SSO. For more information about the Access Panel, see Introduction to the Access Panel.

Additional resources

- List of Tutorials on How to Integrate SaaS Apps with Azure Active Directory
- What is application access and single sign-on with Azure Active Directory?
- What is conditional access in Azure Active Directory?
- Configure User Provisioning
- Try G Suite with Azure AD

Is this page helpful?

👍 Yes 👎 No