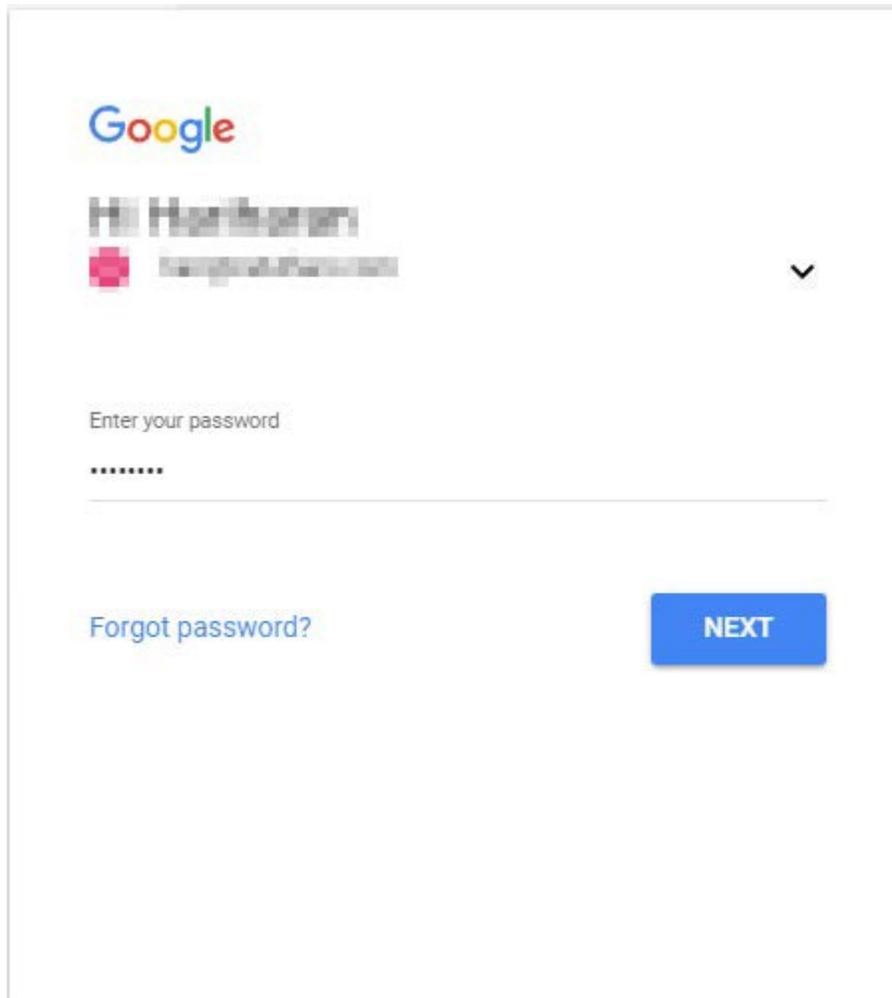
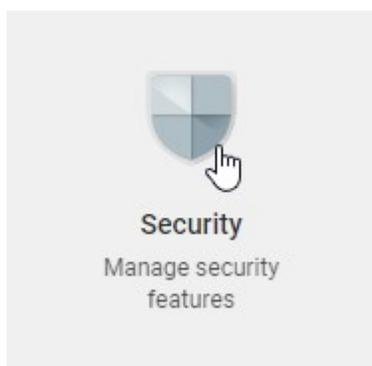


Configuring G Suite



1. Login to G Suite as an Admin user.



2. Click on **Security**.

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).

Advanced settings

Manage advanced security features such as authentication, and integrating G Suite with internal services.

3. Security window will open. Click on **Set up single sign-on (SSO)**.

1 Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. [?](#)

Sign-in page URL **2**

URL for signing in to your system and G Suite

Sign-out page URL **3**

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"/> **4**
The certificate file must contain the public key for Google to verify sign-in requests. [?](#)

5 Use a domain specific issuer [?](#)

4. Fill the fields with the following values:-

Field Name	Values
Setup SSO with third party IdP	Should be checked
Sign-in page URL	<a href="https://ug1.<customer domain>.com/saml/login">https://ug1.<customer domain>.com/saml/login
Sign-out page URL	<a href="https://ug1.<customer domain>.com/cgi/logout">https://ug1.<customer domain>.com/cgi/logout
Verification Certificate	IdP certificate needs to be uploaded
Use a domain specific issuer	Should be checked

1 Setup SSO with third party identity provider ?

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

Sign-in page URL **2**
URL for signing in to your system and G Suite

Sign-out page URL **3**
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 **4**
The certificate file must contain the public key for Google to verify sign-in requests. ?

5 Use a domain specific issuer ?

5. Fill the fields with the following values:

Field Name	Values
Setup SSO with third party IdP	Should be checked
Sign-in page URL	<a href="https://ug1.<customer domain>.com/saml/login">https://ug1.<customer domain>.com/saml/login
Sign-out page URL	<a href="https://ug1.<customer domain>.com/cgi/logout">https://ug1.<customer domain>.com/cgi/logout
Verification Certificate	IdP certificate needs to be uploaded
Use a domain specific issuer	Should be checked