# RingCentral for Google Workspace

## Admin Guide

RingCentral

# CONTENTS

# Introduction

## About RingCentral for Google Workspace

RingCentral for Google Workspace provides seamless integration between your Google Workspace and your RingCentral services. The key benefit of integrating Google Workspace with your RingCentral organization is to allow authentication and provisioning driven by your existing Google Workspace infrastructure.

Formerly G Suite, Google Workspace offers these features and benefits:

- Make decisions faster, face-to-face.
- Use shared calendars to see when others are available and schedule meetings with automatic email invites.
- Turn your meeting into a video conference from any camera-enabled computer, phone, or tablet with one click.
- Share your screen to review your work as a team and make decisions on the spot.
- Collaborate in real-time.
- Store and share files in the cloud.
- Quickly invite others to view, download, and collaborate on any file – no email attachment needed.
- File updates are automatically saved and stored in Drive, so everyone can always access the latest version.
- Archive email messages and on-the-record chats and control how long they are retained.
- Easily configure security settings from a centralized administration console, and call or email Google support for help 24/7.

## About this guide

This guide is designed for IT administrators to automatically provision Google Workspace users into RingCentral and integrate the Google Directory into RingCentral. It will also help administrators to set up a Google Single Sign-On in their RingCentral account.

# Getting started

## Setting up RingCentral as SAML 2.0 service provider (SP) in Google Workspace

1. Sign in to the Google Workspace Admin console.
2. Navigate to **Apps > Web and mobile apps.**
3. Click **Add App > Search for apps**.
4. Enter **RingCentral Office** in the search field, and click **Select**.
5. On the **Google Identity Provider details** page, click **Continue**.
6. In the **Service Provider Details** section, enter the following URLs into the **ACS URL**, **Entity ID,** and **Start URL** fields:

**For US:**

| | |
|---|---|
| ACS URL | https://sso.ringcentral.com/sp/ACS.saml2 |
| Entity ID | saml2:ringcentral:prod |
| Start URL | https://service.ringcentral.com/mobile/ssoLogin? |

**For UK:**

| | |
|---|---|
| ACS URL | https://ssoeuro.ringcentral.com/sp/ACS.saml2 |
| Entity ID | saml2:ringcentral:prodeuro |
| Start URL | https://service.ringcentral.co.uk/mobile/ssoLogin? |

**For EU:**

| | |
|---|---|
| ACS URL | https://ssoeuro.ringcentral.com/sp/ACS.saml2 |
| Entity ID | saml2:ringcentral:prodeuro |
| Start URL | https://service.ringcentral.eu/mobile/ssoLogin? |

Note: Your Service Provider Details depend on your region. Check the table below for the information for your region. For US clients, you don't need to change the Service Provider Details.

7. Leave **Signed Response** unchecked. Note: When the **Signed Response** checkbox is unchecked, only the assertion is signed. When the **Signed Response** checkbox is checked, the entire response is signed.
8. The default **Name ID** is the primary email.
   Note: Multi-value input is not supported. RingCentral Office requires the primary email for authentication. Contact RingCentral Office support if you require a different Name ID mapping. The

custom attributes for the user schema need to be created before setting up the RingCentral Office SAML application.

9. Click **Continue**.
10. Review the **Attribute Mapping** settings, and then click **Finish**.
    Note: The Attribute Mapping is already pre-populated; you may, however, update the location. Verify that you have the correct attributes set, such as the email (RingCentral email) and Primary email (Google email).
11. Click **Finish**.

### Enabling RingCentral SAML app in your Google account

1. Sign in to the Google Workspace Admin console.
2. Navigate to **Apps > Web and mobile apps.**
3. Select **RingCentral.**
4. Click **User access**.
5. Toggle **On for everyone**, and click **Save**.
   Note: Ensure that your RingCentral Office user account email IDs match those in your Google domain.

## Setting up Google Single Sign-On (SSO)

**Single Sign-On** on the Admin Portal allows employees to access all the company applications with one set of credentials. You can set up SSO for your company by yourself or contact support for assistance.

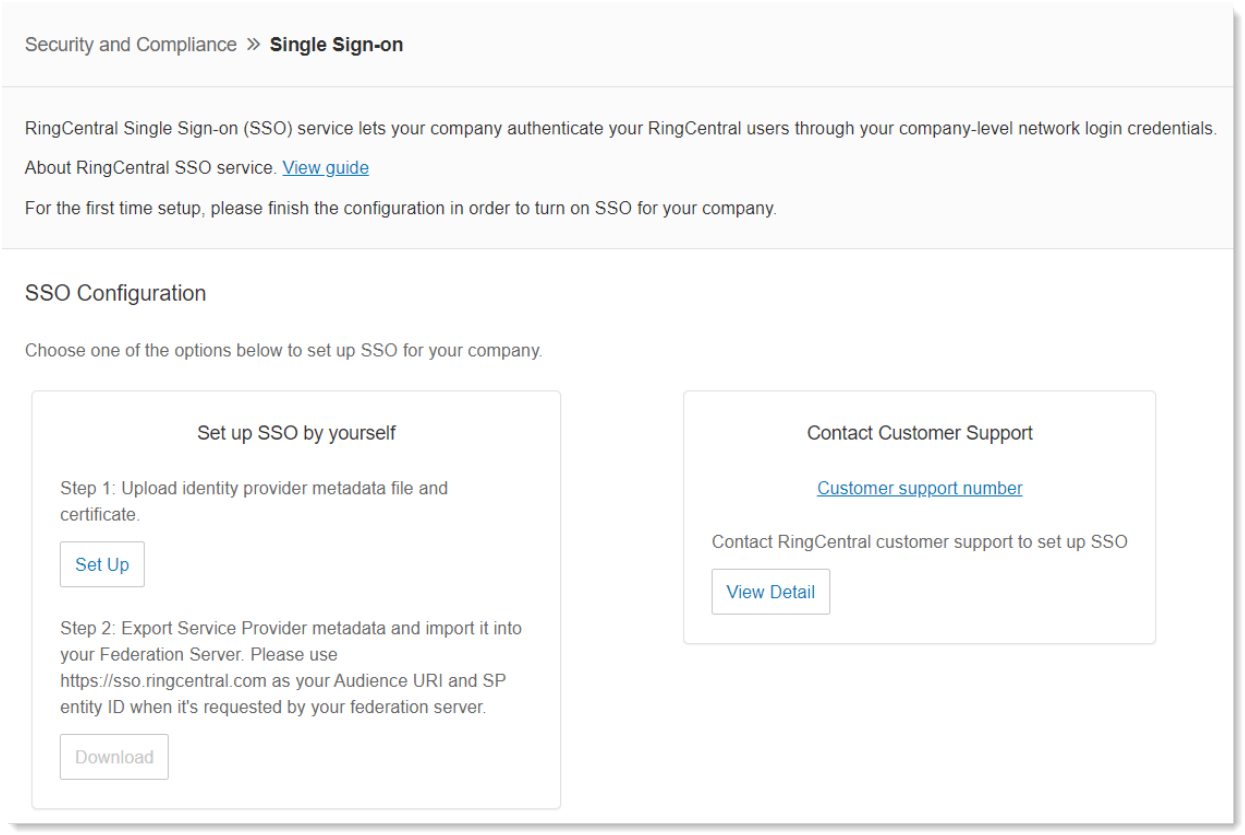
The Google Single Sign-on feature allows you to sign in to your RingCentral account using your Google Workspace sign in credentials. Administrators of companies who use Google Single Sign-On can set up this feature in their RingCentral account.

### Setting up Google as a SAML identity provider (IdP)

1. Sign in to the Google Workspace Admin console.
2. Navigate to **Security > Set up single sign-on (SSO) for SAML applications**.
3. Click **Download Metadata** to download the Google IdP metadata.
4. Set up SSO in the Admin Portal. If you still don't have the SSO settings in your RingCentral account, contact RingCentral Customer Support.

### Setting up SSO in the Admin Portal

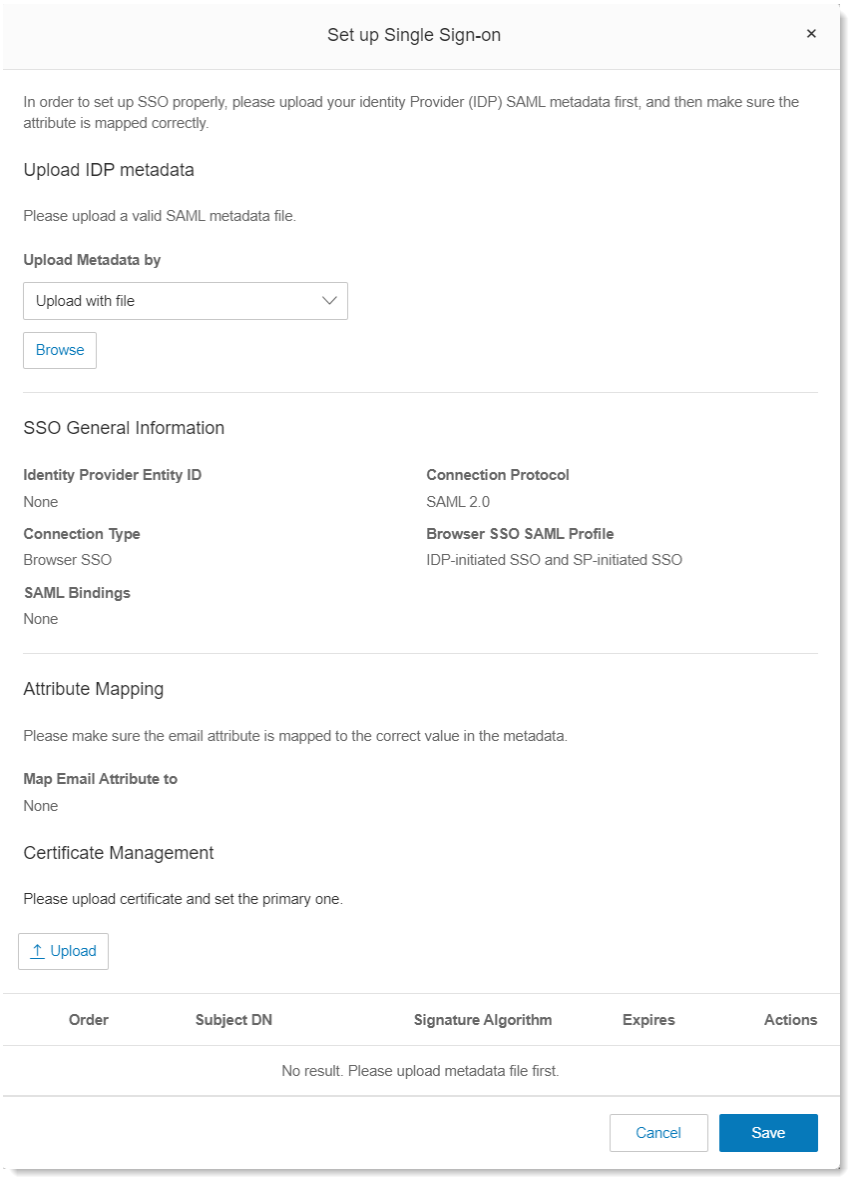
1. Sign in to the Admin Portal.
2. Click **More > Security and Compliance > Single Sign-on**.
3. Under **SSO Configuration**, select either set up SSO by yourself or contact customer support.




## Set up SSO by yourself

Note: If the IDP (Identity provider) entity ID is used by another account or multiple accounts, you will not be able to set up SSO yourself; you will need to contact RingCentral Support for manual configuration.

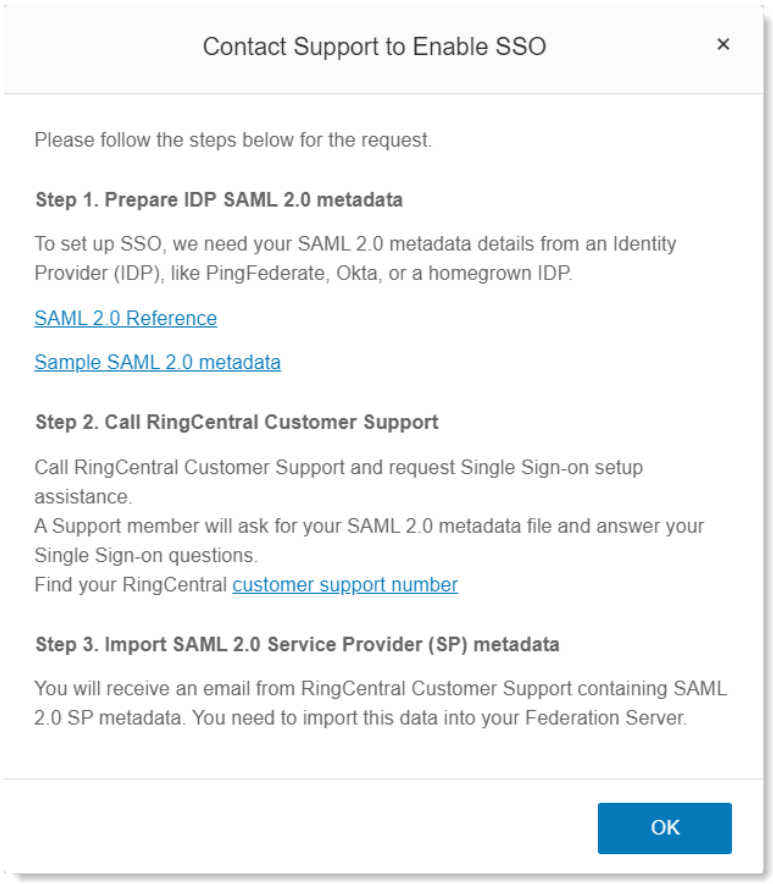
1. Click **Set Up** under **Upload identity provider metadata file and certificate**.
2. Under **Upload IDP metadata**, click the dropdown and select either **Upload with file** or **URL**.
    - *Upload with a file*: Click **Browse**, select a file, and click **Open**.
    - *URL*: Paste the URL and click **Import**.




1. Select email attributes you want to use within your metadata from the dropdown list under **Map Email Attribute**. If the email attribute is not recognized, enter the attribute's name by clicking **Custom** in the dropdown.
2. Under **Certificate Management**, click **Upload** to upload the certificate and set the primary one.
3. Click **Save**.
4. Download the Service Provider metadata and import it into your IdP server to complete the configuration on your IdP side.
5. Tick **Enable SSO Service checkbox**, then click **Save**.

### Contact Customer Support

1. Click **View Detail** under **Contact Customer Support**. The **Contact Support to Enable SSO** window will appear with instructions.




2. Prepare IDP SAML 2.0 metadata. RingCentral will need your SAML 2.0 metadata details from an Identity Provider (IDP). Export the SAML 2.0 metadata details from an Identity Provider (IDP), like PingFederate, Okta, or a homegrown IDP. Click on the links for guidance.
3. Contact RingCentral Customer Support and request Single Sign-On setup assistance. The Support staff will ask for the exported SAML 2.0 metadata file and answer your Single Sign-On questions.
4. Import SAML 2.0 Service Provider (SP) metadata. You will receive an email from RingCentral Customer Support containing SAML 2.0 SP metadata. You must import this data into your Federation Server.
5. Enable SSO Integration.

## Verifying your Google SSO

### IdP-initiated

1. Sign in to the Google Workspace Admin console.

2. Navigate to **Apps > Web and mobile apps.**
3. Select **RingCentral** on the list of SAML apps.
4. Click **Test SAML login** at top-left.
5. Log in via SSO.

### SP-initiated

Sign in to the Admin Portal using SSO. You will be automatically redirected to the Google sign-in page. After your sign-in credentials are authenticated, you will be logged in to the Admin Portal.

# Activating Auto User Provisioning

## Enabling Google Cloud Directory in RingCentral

Google Cloud Directory lets you automatically provision users from the Google Workspace user directory into RingCentral. If you are a Google Workspace customer, you can select this option to import and synchronize Google Workspace users into RingCentral.

You will need to contact RingCentral Customer Support to enable this feature in your RingCentral account.

1. Sign in to the Admin Portal.
2. Go to **Admin Portal > More > Account Settings > Directory Integration.**
3. Select **Google Cloud Directory** as your Directory Provider.
4. Click **Enable Google Cloud Directory**.
5. Click **Confirm**.

Note: You will get an error message when duplicate email addresses are found in your account. The error message contains a link that you can click to download the list of duplicate emails. You will need to make sure that all email addresses are unique to enable Google Cloud Directory. To edit a user's email address, click the Users tab and select the user's name that you want to update.

## Setting up Auto User Provisioning in RingCentral Google Workspace

1. Sign in to the Google Workspace Admin console.
2. Navigate to **Apps > Web and mobile apps.**
3. Select **RingCentral** on the list of SAML apps.
4. Under **Autoprovisioning,** click Configure Autoprovisioning.
5. Click **Authorize**.
6. Enter your RingCentral sign in credentials to verify authorization.
7. Map RingCentral user attributes to the Cloud Directory attributes, and click **Next**.
   Note: You can set up custom address attributes after if you haven't mapped it out.

8. Click **Continue**.
9. Select the groups you want to include in the Autoprovisioning. (Optional)
10. Click **Continue**.
11. Set up your **Deprovisioning** settings.
12. Click **Finish**.

Note: Changes may take up to 24 hours to propagate to all users.

If users exceed the admin authorized account seat limit, users will not be assigned. An error prompt will be shown in Google Workspace until the admin adds more users to the RingCentral account.

The users auto-created in RingCentral will be capped by the number of seats/users purchased in RingCentral. Attempting to auto-provision more users into RingCentral than the number of seats/users purchased will be flagged as an error in the Google Workspace provisioning dashboard.

Admin must purchase the appropriate number of seats/users in RingCentral to match the estimated number of provisioned users from Google Workspace.

# Managing Attribute Mapping

## Adding user custom address attributes

1. Sign in to the Google Workspace Admin console.
2. Navigate to **Directory > Users**.
3. Click **More**, then select **Manage custom attributes**.
4. Click **Add Custom Attribute** at the top-right.
5. Add the custom attributes equivalent to:
    - Street1
    - Country1
    - State1
    - ZipCode1
    - City1
    - Type1

    Note: You can name them differently as long as they can be identified and not conflict with other existing attribute names. The type and scope of the attributes are the same: "Text" type, "Visible to Org", and "Single Value".

## Editing custom address attributes for each user

1. Sign in to the Google Workspace Admin console.

2. Navigate to **Directory > Users**.
3. Select the user you want to edit the attributes.
4. Select **User information** to open the User detail settings.
5. Map the new custom attributes under **Street Custom Fields**.
   Note: Use ISO 3166-1 "alpha-2" for country. We use "US" for the country name component in the following example. (e.g., The United States and Sweden are "US" and "SE," respectively.)
   Please make sure that the "state" name should be either a standard "state name" (such as California) or "state code" (such as CA). The type of address should be "work" in "Type1".
6. Click **Save**.

# Disabling or deleting Google Cloud Directory

## Disabling Google Cloud Directory in Admin Portal

1. Sign in to the Admin Portal.
2. Go to **Admin Portal > More > Account Settings > Directory Integration.**
3. Select **None** as your Directory Provider.
4. Click **Confirm**.

## Deactivating autoprovisioning to RingCentral in Google

1. Sign in to the Google Workspace Admin console.
2. Navigate to **Apps > Web and mobile apps**.
3. Select **RingCentral** on the list of SAML apps.
4. Click **Autoprovisioning**, and slide the toggle off.
5. Alternatively, you can click the **Autoprovisioning** section to open the settings page, then click **Status > Turn off**.

## Removing autoprovisioning to RingCentral in Google

1. Sign in to the Google Workspace Admin console.
2. Navigate to **Apps > Web and mobile apps**.
3. Select **RingCentral** on the list of SAML apps.
4. Click the **Autoprovisioning** section to open the settings page.
5. In the **Delete configuration**, click **Delete**.
6. Click **Delete** to deactivate autoprovisioning and remove all the configuration information.
   Note: Existing users on RingCentral Office will not be deprovisioned.

# Appendix

## Google > RingCentral custom attribute mapping

The following list is the set of custom address attributes needed from Google into RingCentral:

| GOOGLE DIRECTORY | TO > RINGCENTRAL |
|---|---|
| Street | Street |
| Country | Country |
| State | State |
| City | Locality |
| ZipCode | Zip |
| Type | Department |