



# Google Cloud Identity for Maximizer SSO

## Configuration Guide

---

Maximizer Inc.

# Table of Contents

- About This Guide ..... 3
  - Who Should Read This Guide ..... 3
  - Typographic Conventions ..... 3
- Overview..... 4
  - How Maximizer SSO Works with Google Cloud Identity..... 4
- Setting up SSO Using Google Cloud Identity ..... 5
  - Obtaining a Signing Certificate..... 5
  - Setting up Maximizer CRM as a Custom SAML Application ..... 5
  - Adding Google Cloud Identity as the IdP in Maximizer CRM ..... 6
  - Getting the Maximizer CRM ACS URL..... 9
  - Completing the Google Cloud Identity Configuration .....10
- Contacting Support..... 12
  - Phone .....12
  - Email.....12
  - Chat.....12



## About This Guide

The **Google Cloud Identity for Maximizer SSO Configuration Guide** provides instructions for configuring Google Cloud Identity as an Identity Provider (IdP) for logging on to Maximizer CRM using Google credentials. This guide assumes that you have familiarity with Google Cloud Identity.

## Who Should Read This Guide

The **Google Cloud Identity for Maximizer SSO Configuration Guide** is primarily intended for administrators tasked with setting up Maximizer CRM.

## Typographic Conventions

In the **Google Cloud Identity for Maximizer SSO Configuration Guide**, you might encounter the following conventions:

Convention	Explanation
<b>Note</b>	Information, supplementary in nature, which must be highlighted. Notes usually appear in a green box.
Text appearing in bold	The names of menu items.
<a href="#">Blue text</a>	A hyperlink to a section within this document or a Web site.

## Overview

Maximizer CRM permits Single Sign-On (SSO) login using Google Cloud Identity as an Identity Provider (IdP). When configured this way, SSO login validations are typically managed by Google Cloud Identity, thereby eliminating the need for separate, dedicated credentials to access Maximizer CRM resources.

Using Google Cloud Identity to implement SSO has the following benefits:

### Reduced Administration Efforts

With SSO, users do not require usernames or passwords to access Maximizer CRM. This translates to reduction in user & password management activities for Maximizer administrators.

### Reduced Login Time

Typically, a user needs 5 to 20 seconds to log in to an online application. SSO eliminates the efforts required for a manual login, thus increasing productivity.

### Increased Security

The password policies enforced across your organization are applicable when you use SSO. The one-time authentication tokens used to validate SSO attempts translate to added security for users having access to sensitive data.

## How Maximizer SSO Works with Google Cloud Identity

Maximizer CRM supports Single Sign-On by implementing federated authentication using Security Assertion Markup Language (SAML) 2.0. For this purpose, Google Cloud Identity functions as the Identity Provider (IdP). In order to validate user logins, Maximizer CRM communicates with Google Cloud Identity using SAML assertions via HTTP POST queries. For every login attempt, Maximizer CRM sends an authentication assertion to the IdP Login URL specified under System Options > Single Sign-On. Google Cloud Identity validates the SAML query, and if the validation is successful, sets the assertion in the HTTP POST query to True. Maximizer CRM receives the assertion, verifies it against its SSO configuration, and allows single sign-on.

When SSO is implemented this way, a user only logs in once to Google Cloud Identity. Thereafter, for all login attempts to Maximizer CRM, the user's Google Cloud Identity credentials are used.

### **i** Note:

This document assumes that you are familiar with Google Cloud Identity. Maximizer does not provide support for and is not responsible for changes to Google Cloud Identity. For information about using Google Cloud Identity, read the Google Cloud Identity documentation.

## Setting up SSO Using Google Cloud Identity

To use Google Cloud Identity as the IdP for enabling SSO, you must first configure Google Cloud Identity to recognize Maximizer CRM, and then, add Google Cloud Identity as an IdP within Maximizer CRM. As a last step, configure Google Cloud Identity to add Maximizer CRM as a Service Provider.

To set up SSO using Google Cloud Identity, follow these high-level steps:

Step 1: [Obtain a signing certificate](#)

Step 2: [Set up Maximizer CRM as a custom SAML application within Google Cloud Identity](#)

Step 3: [Add Google Cloud Identity as the IdP in Maximizer CRM](#)

Step 4: [Get the Maximizer CRM ACS URL](#)

Step 5: [Complete the Google Cloud Identity Configuration](#)

### Obtaining a Signing Certificate

The signing certificate is used to generate the signature on a SAML request that Maximizer CRM sends to Google Cloud Identity. This signing certificate is required in scenarios where Maximizer CRM initiates a SAML login (also called as service provider-initiated login).

As an example, consider that a user accesses Maximizer CRM first, and then sends an authorization request to Google Cloud Identity. After Google authenticates the user's identity, the user is logged into Maximizer CRM. The request signing certificate is used to authenticate the handshake between Google Cloud Identity and Maximizer CRM.

- The signing certificate for Google Cloud Identity must satisfy the following conditions:
- The certificate must be created and signed with the supported signing algorithm (SHA-256)
- The certificate must be available as a Base64 encoded file

### Setting up Maximizer CRM as a Custom SAML Application

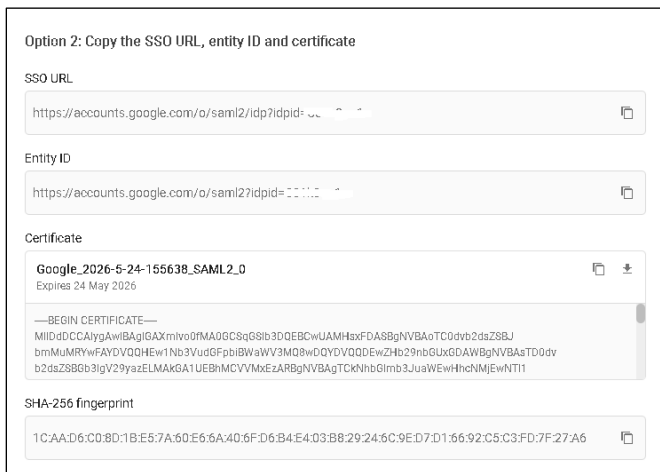
Google Cloud Identity comes with a catalog of pre-integrated applications that it recognizes as Service Providers. However, since Maximizer CRM is not a pre-integrated application, as a first step, you must set it up as a SAML application within Google Cloud Identity.

#### Note:

This procedure has been adapted from the Google documentation available at: <https://support.google.com/cloudidentity/answer/6087519?hl=enax>

To set up Maximizer as a custom application:

- 1 Log in to your Google Admin Console using an account with super administrator privileges.
- 2 From the home page, go to **Apps**, and then **Web and mobile apps**.
- 3 Click **Add App**, and then **Add custom SAML app**.
- 4 On the **App Details** page, enter a name for the app. For example, Maximizer CRM.
- 5 (*Optional*) Upload an icon if necessary. This icon will appear on the Web and mobile apps list, and in the app launcher. If you choose to not upload an icon, Google will create one with the first two letters of the app name.
- 6 Click **Continue**. The **Google Identity Provider details** page appears with the setup information that you need to provide to Maximizer CRM (the Service Provider).



Option 2: Copy the SSO URL, entity ID and certificate

**SSO URL**  
https://accounts.google.com/a/saml2/ldp?idpid=...

**Entity ID**  
https://accounts.google.com/a/saml2?idpid=...

**Certificate**  
Google\_2026-5-24-155638\_SAML2\_0  
Expires 24 May 2026  
-----BEGIN CERTIFICATE-----  
MIIDdDCCAlYgAwIBAgIGAXmivo0rMA0GCSqGSIb3DQEBCwUAMHxzFDA8BgNVBAoTC0dvb2daZSBJ  
bmMuMURyYwFAVDV0QHEw1Nb3VudGFpbWwaHV3M08wDQYDVQDDewZhb29nbGUxGDAWBgNVBAstD0dv  
b2daZSBJb3V2y9azELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkhnbGlmb3JuaWEwHhcNMjE1MjE1  
SHA-256 fingerprint  
1CAAD6:C08D:1BE5:7A:60:E6:5A:40:6F:D6:B4:E4:03:B8:29:24:6C:9E:D7:D1:66:92:C5:C3:FD:7F:27:A6

- 7 Copy the **SSO URL** and **Entity ID** to a text editor.
- 8 Either download the **Certificate** or copy the contents of the certificate that appear between **BEGIN CERTIFICATE** and **END CERTIFICATE**.
- 9 Keep this session active.

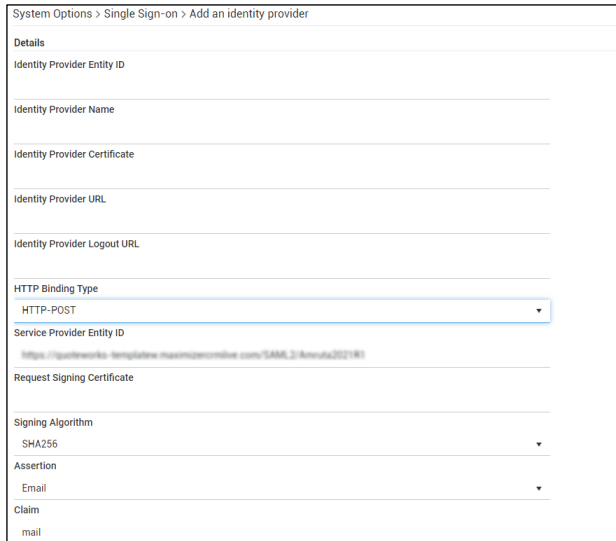
## Adding Google Cloud Identity as the IdP in Maximizer CRM

As a next step, add the IdP details to the Maximizer CRM SSO setup.

To do that:

- 1 In a separate tab or window, log on to Maximizer CRM.
- 2 Click the cog icon (⚙️) in the left pane.
- 3 Go to **Administration > Settings**.
- 4 Click **Single Sign-on**.

- Click **Add Identity Provider**. The **Add an Identity Provider** screen appears.



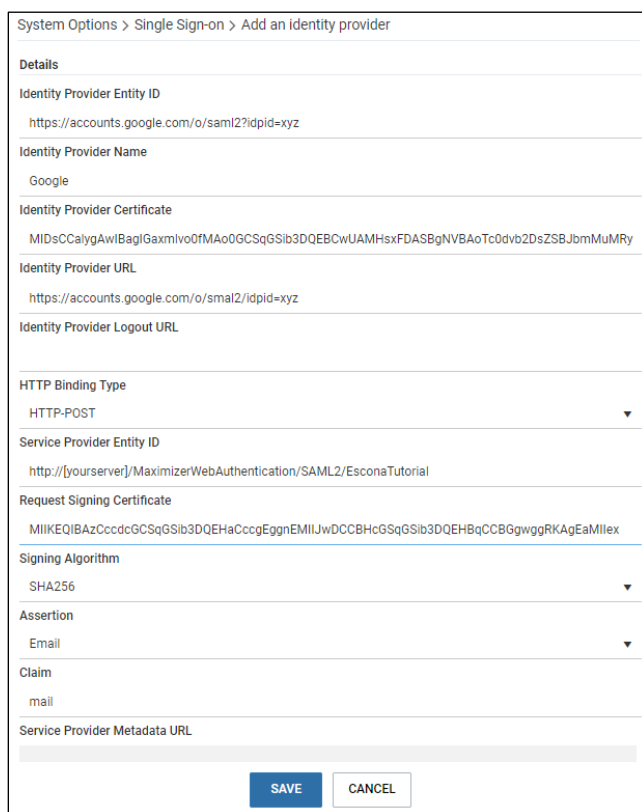
- Provide the following details:

Field	Description
Identity Provider Entity ID	Enter the value as it appears under <b>Entity ID</b> .
Identity Provider Name	Type a name for the IdP. For example, Google Cloud for Maximizer.
Identity Provider Certificate	Paste the contents as they appear in the <b>Certificate</b> box.
Identity Provider URL	Type the value as it appears in the <b>SSO URL</b> box.
Identity Provider Logout URL	Leave this field blank.
HTTP Binding Type	Ensure that HTTP-POST is selected.
Service Provider Entity ID	This field is auto-populated.



Field	Description
Request Signing Certificate	The <a href="#">signing certificate</a> available as a Base64 encoded file. Copy the contents of the certificate in this text box.
Signing Algorithm	Ensure that SHA-256 is selected.
Assertion	Ensure that this field is set to <b>Email</b> .
Claim	Ensure that this field is set to <b>Mail</b> .
Service Provider Metadata URL	This field will be initially blank. After you save the settings on this screen, and open this screen again, Service Provider Metadata URL will be populated.

7 Ensure that the **Add an Identity Provider** screen looks like this:



System Options > Single Sign-on > Add an identity provider

**Details**

Identity Provider Entity ID  
https://accounts.google.com/o/saml2?idpid=xyz

Identity Provider Name  
Google

Identity Provider Certificate  
MIDScCalygAwIBAgIGaxmlvo0fMAo0GCSqGSIb3DQEBCwUAMHsxFDASBgNVBAoTc0dvb2DsZSBJbmMuMFRy

Identity Provider URL  
https://accounts.google.com/o/smal2/idpid=xyz

Identity Provider Logout URL

HTTP Binding Type  
HTTP-POST

Service Provider Entity ID  
http://[yourserver]/MaximizerWebAuthentication/SAML2/EsconaTutorial

Request Signing Certificate  
MIIKEQIBAzCccdcGCSqGSIb3DQEHaCccgEggnEMIJwDCCBHCgGSqGSIb3DQEHBqCCBGgwgwRKAgaEaMllex

Signing Algorithm  
SHA256

Assertion  
Email

Claim  
mail

Service Provider Metadata URL

**SAVE** **CANCEL**

8 Click **Save**.

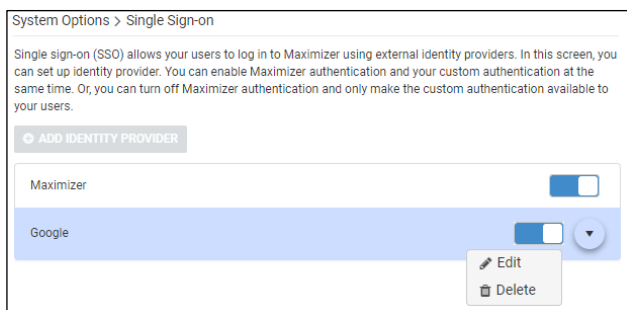
Google Cloud Identity appears in the IdP list, which is available on the **Single Sign-on** screen.

## Getting the Maximizer CRM ACS URL

Google requires the Assertion Consumer Service (ACS) URL of Maximizer CRM to identify it as a Service Provider. Google will use this URL to send a response in event of successful or unsuccessful verification of login attempts.

To get the ACS URL:

- 1 Add Google Cloud Identity as the IdP to Maximizer CRM.
- 2 In the IdP list, locate **Google**.
- 3 Click the drop-down arrow next to it, and then click **Edit**.



- 4 Copy **Service Provider Metadata URL** by using the copy button and save it as a text file.



- 5 Open the Service Provider Metadata URL in a separate tab.
- 6 Locate a line that looks like this:

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://mysite.test.com/MaximizerWebAuthentication/SAML2
/Return/TestSAML2" index="1"/>
```

- 7 Save this code to a simple text file.

This URL functions as the ACS URL in Google.

### **i** Note:

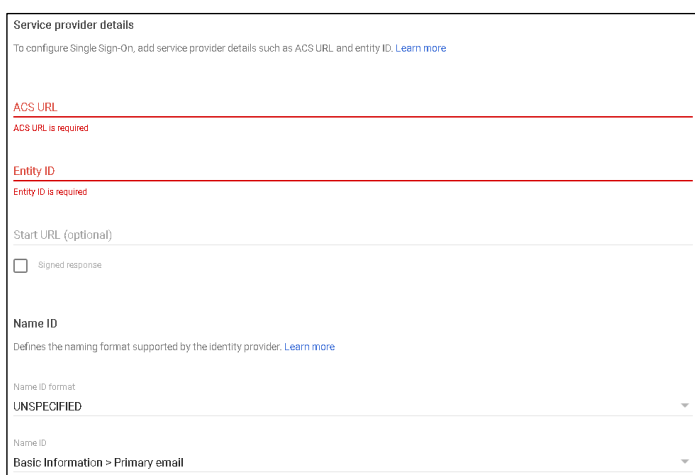
This URL must always be reachable by Google, and must have a [valid signing certificate](#).

## Completing the Google Cloud Identity Configuration

As a last step, add the Assertion Consumer Service (ACS) URL of Maximizer CRM to Google Cloud Identity. Once this is done, SSO is enabled in Maximizer CRM using Google Cloud Identity as the IdP.

To complete the configuration:

- 1 Go back to the Google Admin Console session that you kept active [while configuring Maximizer CRM as a custom application](#).
- 2 Click **Continue** on the **Google Identity Provider details** page. The **Service Provider Details** page appears.



**Service provider details**

To configure Single Sign-On, add service provider details such as ACS URL and entity ID. [Learn more](#)

**ACS URL**  
ACS URL is required

**Entity ID**  
Entity ID is required

Start URL (optional)

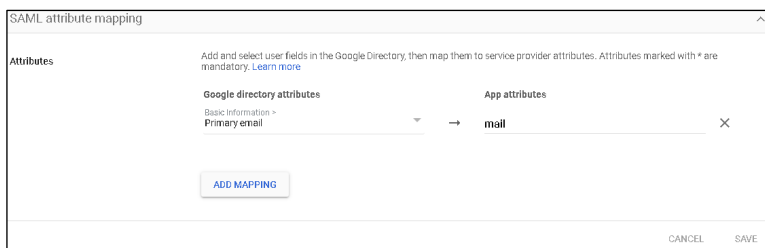
Signed response

**Name ID**  
Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format  
UNSPECIFIED

Name ID  
Basic Information > Primary email

- 3 Copy the Service Provider Metadata URL to the ACS URL text box.
- 4 Copy the Service Provider Entity ID to the Entity ID text box.
- 5 Click Continue. The Attribute mapping page appears.
- 6 Click **ADD MAPPING** and map Primary email from the Google directory attributes column to mail in the App attributes column.



**SAML attribute mapping**

Add and select user fields in the Google Directory, then map them to service provider attributes. Attributes marked with \* are mandatory. [Learn more](#)

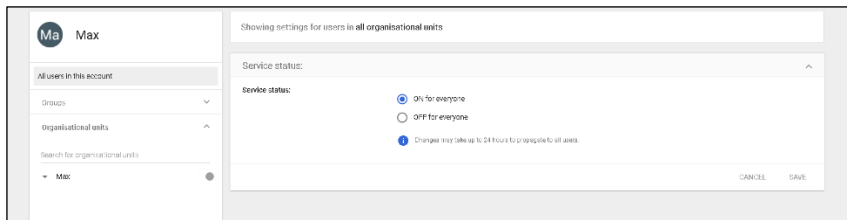
Google directory attributes	App attributes
Basic Information > Primary email	mail

**ADD MAPPING**

CANCEL SAVE

- 7 Click **SAVE**.

- 8 Expand **User Access**. The **Service Status** page appears.



- 9 Set the service status to one of the following:

- ON for everyone
- OFF for everyone

Google credentials can now be used to log on to Maximizer, provided that the email addresses of Maximizer users in your database match the primary email addresses of users in Google Cloud Identity.



## Contacting Support

If you have problems with or questions about Maximizer CRM or Maximizer CRM Live, contact the Maximizer Support team. In order to do that, you can use one of the following channels:

### Phone

- **North America:** 1-866-275-1254 (Monday through Friday, 5:00 AM to 7:30 PM, PST; Sunday 11:00 AM to 7:30 PM, PST)
- **Europe, Middle East, Africa:** +44 13 4476 6904 (Monday through Friday, 9.00 AM to 5.30 PM, GMT)
- **Australia & New Zealand:** + 61 2 9957 2011 (Monday through Friday, 5:00 AM to 7:30 PM, PST; Sunday 11:00 AM to 7:30 PM, PST)

### Email

Write to the support team at [support@maximizer.com](mailto:support@maximizer.com)

### Chat

The chat window can be accessed from within Maximizer CRM. Go to **Help Center > Support Chat**.