

CONFIGURATION GUIDE

Single Sign On for MailMarshal Cloud with Google G Suite

Table of Contents

About This Document	1
1 Gather Required Data from MailMarshal Cloud	2
2 Create the Application in Google SAML Apps	2
3 Turn On SSO to the SAML App	5
4 Complete Configuration in MailMarshal Cloud for the SQM	5
5 Complete Configuration in MailMarshal Cloud for the Console	7
6 Deploy SSO	8
About Trustwave	9

About This Document

This document describes the steps required to configure SAML Single Sign On (SSO) to the Trustwave MailMarshal Cloud Spam Quarantine Management site, using Google SAML as the Identity Provider.

You can use the same Google identity provider for both SQM and the Console, by adding the appropriate values in the Google Admin Console.

This document assumes that:

- You have administrator access to the Google Admin Console for a managed domain.
- Your reseller has enabled your access to Single Sign On for SQM.

1 Gather Required Data from MailMarshal Cloud

- 1. Log in to the MailMarshal Cloud Console. Navigate to **Configuration > Security Configuration** and expand **Single Sign On**.
- 2. Select an option (SQM Identity Providers or Console Identity Provider).



Note: If you do not see one or both of these options, SSO is not enabled for you. Contact your reseller.

- 3. At the top of the list, click Add.
- 4. Note the Entity Provider and ACS URL. You will enter these items in the Google Console.
 - Carefully copy the values. The path parts differ for SQM and the Console.

2 Create the Application in Google SAML Apps

- 1. Sign in to the Google Admin Console using an administrator account.
- 2. From the Admin console Home page, go to Apps and then SAML Apps.



Tip: To see Apps on the Home page, you might have to click **More controls** at the bottom.

3. Click the plus (+) icon in the bottom corner.



4. At the bottom of the window, click Setup my own custom app.

5. The Google IDP Information window opens and the Single Sign-On URL and the Entity ID URL fields automatically populate.

Step 2 of 5 Google IdP Inform	mation	×
Choose from either option config for the service prov	n to setup Google as your identity provider. Please add details in the SSO vider. Learn more	
Option 1		
SSO URL	https://accounts.google.com/o/saml2/idp?idpid=A2Bc4193v	
Entity ID	https://accounts.google.com/o/saml2?idpid=A2Bc4193	
Certificate	Google_2022-8-24-1078_SAML2.0	
o chinouto	Expires Aug 24, 2022	
	± DOWNLOAD	
	OR	
Option 2		
IDP metadata	± DOWNLOAD	
PREVIOUS	CANCEL NEX	r

- 6. Copy the Entity ID and the Single Sign-On URL field values and download the X.509 Certificate. You will enter these items in MailMarshal Cloud.
- 7. In the Basic Application Information window, add the application name MailMarshal Cloud and a description.
- 8. Optionally you can upload a PNG or GIF file to serve as an icon. The file size should be 256 pixels square.
- 9. In the Service Provider Details window, add the following settings.
 - ACS URL: The ACS URL you copied from MailMarshal Cloud
 - Entity ID: The Entity ID you copied from MailMarshal Cloud
 - Start URL: The Entity ID you copied from MailMarshal Cloud



Note: Thes values depends on the regional instance of MailMarshal Cloud and the service (Console or SQM)

The image below shows an example of detail entry for the US regional instance of MailMarshal Cloud:

Please provide service D are mandatory.	provider details to configure s	SSO for you	r Custom App. Th	ie ACS url ai	nd Entity
ACS URL *	https://console.us.mailn	narshal.clou	ud/sqm/ssoacs		
Entity ID *	https://console.us.mailn	narshal.clou	ıd/sqm 🔤		
Start URL	https://console.us.mailr	marshal.clou	ud/sqm		
Signed Response					
lame ID	Basic Information	~	Primary Email		v
Name ID Format	UNSPECIFIED	v			

- 10. Click Next.
- 11. Add a minimum of three attribute mappings. For each one, click **Add new mapping**, enter the name, and select the profile field. These mappings allow the user name and email address information to be provided to MailMarshal Cloud.
 - a. FirstName (Basic Information): First Name
 - b. LastName (Basic Information): Last Name
 - c. PrimaryEmail (Basic Information): Primary Email

Attribute Mapping						
Provide mappings between serv	rice provider attributes to availabl	le user pr	ofile fields.			
FirstName	Basic Information	Ŧ	First Name	Ŧ		
LastName	Basic Information	Ŧ	Last Name	Ŧ		
PrimaryEmail	Basic Information	Ŧ	Primary Email	Ŧ		
ADD NEW MAPPING						
					DISCARD	SAVE



Tip: If you use the secondary email address field, you can map this attribute as **Alias.**

12. Click Finish.

3 Turn On SSO to the SAML App

- 1. From the Google Admin console Home page, go to Apps and then SAML Apps.
- 2. Select your new SAML app.
 - a. At the top of the gray box, click **More Settings**, and choose **On for some organizations** to change the setting only for some users. Select one or more users to test.

2	SEG Cloud OFF for everyone	ON for everyone OFF for everyone ON for some organizations
Service Provider Details Set up basic service provider	(SP) details like the ACS URL, entity id and more	
Attribute Mapping Configure additional parame token	ters that need to be sent to the service provider along with the authentication	

- 3. Ensure that the domain for your Google service matches a domain in your MailMarshal Cloud account.
- 4 Complete Configuration in MailMarshal Cloud for the SQM
- Log in to the MailMarshal Cloud Console. Navigate to Configuration > Security Configuration > Single Sign On > SQM Identity Providers.



Note: If you do not see this option, SSO is not enabled for you. Contact Trustwave or your reseller.

- 2. At the top of the list, click Add.
- 3. Enter a name such as Google SAML.
- 4. Enter the Entity ID and SSO URL that you noted from the Google Admin Console.
- 5. Check the box **Partner Certificate**, and then import the certificate that you saved from the Google Console.

Trustwave MailMarshal Cloud US × +				~	-		(
\leftrightarrow \rightarrow C \bullet console.us.mailmarshal	.cloud/security-configuration/sqm-identity-provide	er 🖻	☆	* 0	0	Update	D
Trustwave < * sqn	1 Identity Provider			Save	Cancel	? Help	
Trustwave Managed Admin * Servi	ce Provider Settings						
Overview 👻 🗌	Force User Interaction Send Requested User Name						
	Entity ID						
	https://console.us.mailmarshal.cloud/sqm						
	https://console.us.mailmarshal.cloud/sqm/ssoa						
Audit History Notifications (3) Ident	ity Provider Settings						
	Name						
	Entity ID						
	SSO URL						
	Use Partner Certificate Import Certificate						

- 6. To set the default Identity Provider, on the SQM Identity Providers page, select the provider and then click **Set Default**.
- 7. To set a provider for an individual domain:
 - From the domain list (Configuration > System Configuration > Domains), edit the domain.
 - Select an Identity Provider from the menu, and then click Save.

Trustwave MailMarshal Cloud US 🗙	+		~	-		×
\leftrightarrow \rightarrow C $($ console.us.mailm	narshal.cloud/config/domains	12 ☆	* 0	C (Update	
Trustwave < 🛛 🛪	Domain		Save	Cance	· ? ·	lelp
Trustwave Managed Admin -	General Delivery					
Overview	Incoming and Outgoing Costs					
Dashboard	Specify the incoming and outgoing costs for the domain	for use in billing reports (these	figures are n	ot used	to	
🕒 Reports	charge for services).					
Management	Incoming Cost Per MB	Outgoing Cost Per MB				
Messages						
Email Policy						
Policy Elements	Single Sing On					
 Audit History 		co.u				
A Notifications 3	The identity provider to use for this domain for accessing	SQM.				
	Identity Provider					
Configuration	Default 🗸					
system Configuration	Default					
Security Configuration	Azure AD Domain specific tyourcation citian Addresses					
SQM Configuration	Override the default email addresses used for notification	s sent by this service.				
Support	Administrator Email Address	Server Email Address				
? Help						
Documentation						
	Executive Names List					
	Names or email addresses which correspond to the execu	tives of this domain. This inform	nation is use	d in frau	d	
	detection.					

Copyright © Trustwave Holdings, Inc. All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. 6

8. Test the configuration by logging in to SQM as a valid user. If the user is not in in the MailMarshal Cloud SQM users list, they will be added to the list. All email aliases from the configured attributes will be added for the user.

5 Complete Configuration in MailMarshal Cloud for the Console

Log in to the MailMarshal Cloud Console. Navigate to Configuration > Security Configuration > Single Sign On > Console Identity Provider.



Note: If you do not see this option, SSO is not enabled for you. Contact Trustwave or your reseller.

- 2. At the top of the list, click Add.
- 3. Enter a name such as Google SAML.
- 4. Enter the Entity ID and SSO URL that you noted from the Google Console.
- 5. Check the box **Partner Certificate**, and then import the certificate that you saved from the Google Console.



6. To enable use of this provider immediately select **Enable**.



Caution: Double-check all settings before enabling SSO for the Console. Enabling SSO will immediately disable the plain username and password login. Ensure that

you have enabled at least one user for SSO on the provider side. Console users must be created explicitly in MailMarshal Cloud (for security, self-provisioning is not supported for the Console).

Before logging out of the session where you enable SSO, test access from another workstation using the permitted user details.

If you cannot log in after enabling SSO, contact your reseller for assistance. Reseller Support logins can always access the Console.

- 7. For other available options, see Help for the page.
- 8. Click Save.

6 Deploy SSO

When you are ready to deploy SSO:

- 1. From the Google Admin console Home page, go to Apps and then SAML Apps.
- 2. Select the MailMarshal Cloud SAML app.
 - At the top of the gray box, click **More Settings**, and turn SAML on for all the users you want to authenticate with SSO.



Caution: The number of users that can be created and authenticated in MailMarshal Cloud SQM is limited to the licensed user count in MailMarshal Cloud.

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.