CONFIGURATION GUIDE

Single Sign On for MailMarshal Cloud with Azure Active Directory

Table of Contents

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 and/or the Customer Console, using Azure Active Directory as the Identity Provider.

This document assumes that:

- You have completed initial configuration of Azure AD
- You have permission to add a “non-gallery” application to Azure Enterprise Applications.
- Trustwave or your reseller has enabled your access to Single Sign On for SQM.

1 Gather Required Data from MailMarshal Cloud

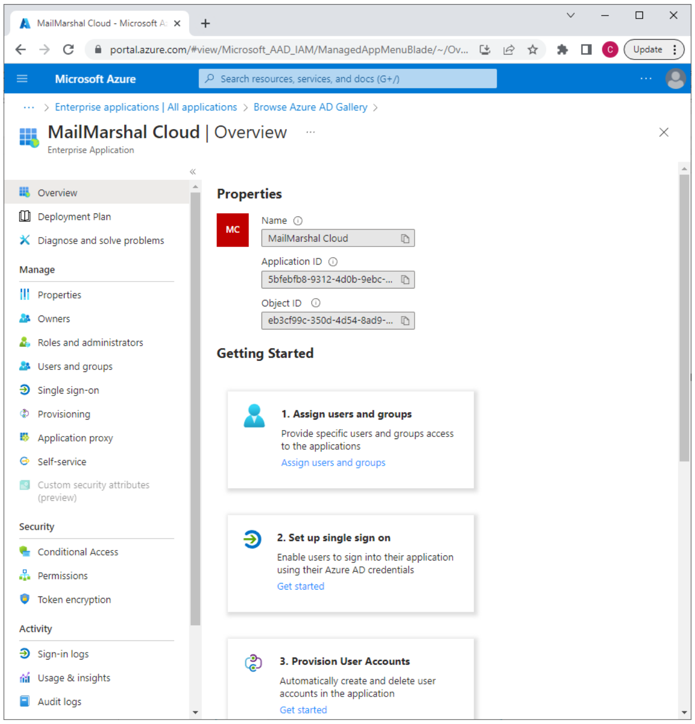
1. Log in to the MailMarshal Cloud Console. Navigate to **Configuration > Security Configuration** and expand **Single Sign On**.
2. Select an option (**SQM Identity Providers** or **Console Identity Provider**).

> **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 Azure portal.
   - Carefully copy the values. The path parts differ for SQM and the Console.

2 Create the Application in Azure

1. Log on to Azure and navigate to **Azure Active Directory > Enterprise applications**.
2. Click **New application**, and then click **Create your own application.** Enter the name **MailMarshal Cloud** and then click **Create.**



MailMarshal Cloud - Microsoft A
portal.azure.com/#view/Microsoft_AAD_IAM/ManagedAppMenuBlade/~/Ov...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
... > Enterprise applications | All applications > Browse Azure AD Gallery >
MailMarshal Cloud | Overview
Enterprise Application
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes (preview)
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-in logs
Usage & insights
Audit logs
MC

Properties

Name: MailMarshal Cloud

Application ID: 5bfebfb8-9312-4d0b-9ebc-...

Object ID: eb3cf99c-350d-4d54-8ad9-...

Getting Started

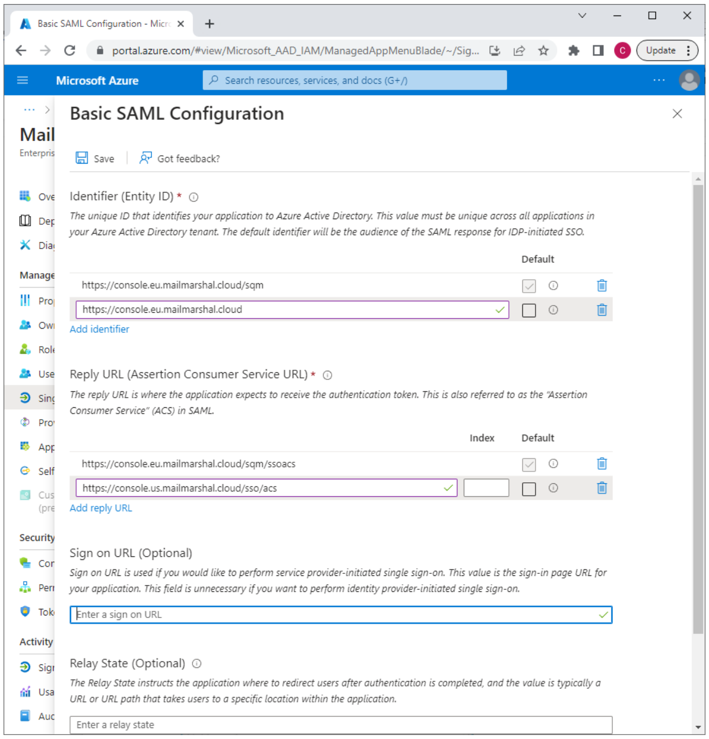
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

3. Click **Set up single sign on.**
4. **On the Method page select SAML**
5. Edit the Basic SAML Configuration. Enter the Entity ID and the ACS URL that you copied from MailMarshal Cloud.

- You can enter more than one Entity ID and ACL URL if you want to use the same provider for the Console and SQM, as in the screenshot. You can also use separate providers.



Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://console.eu.mailmarshal.cloud/sqm	☑
https://console.eu.mailmarshal.cloud	□

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://console.eu.mailmarshal.cloud/sqm/ssoacs		☑
https://console.us.mailmarshal.cloud/sso/acs		□

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

6. Save the SAML configuration and close the pane.
7. Download the **Certificate (Base64),** and copy the **Login URL** and **Azure AD Identifier**. These values will be unique to your organization.
8. In the Enterprise Applications list, select MailMarshal Cloud, and then click **Assign Users and Groups**.
9. For testing purposes, select at least one user and assign the User role to this user.

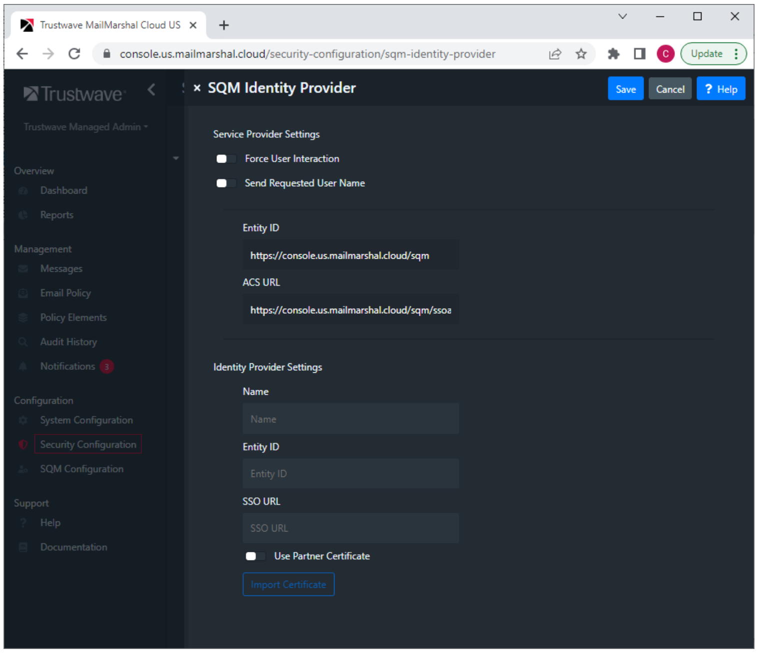
Tip: Azure uses the User Principal Name (`user@domain`) as the user Name by default. If you want to use the personal full name as the user Full Name, in Azure edit Single Sign On for the MailMarshal Cloud application, expand the list of User Attributes, remove the Name attribute, and save the configuration. MailMarshal Cloud will use the GivenName and Surname to construct the Full Name.

3 Complete Configuration in MailMarshal Cloud for the SQM

1. 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 your reseller.

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



× SQM Identity Provider

Service Provider Settings

Force User Interaction

Send Requested User Name

Entity ID
https://console.us.mailmarshal.cloud/sqm

ACS URL
https://console.us.mailmarshal.cloud/sqm/ssoa

Identity Provider Settings

Name
Name

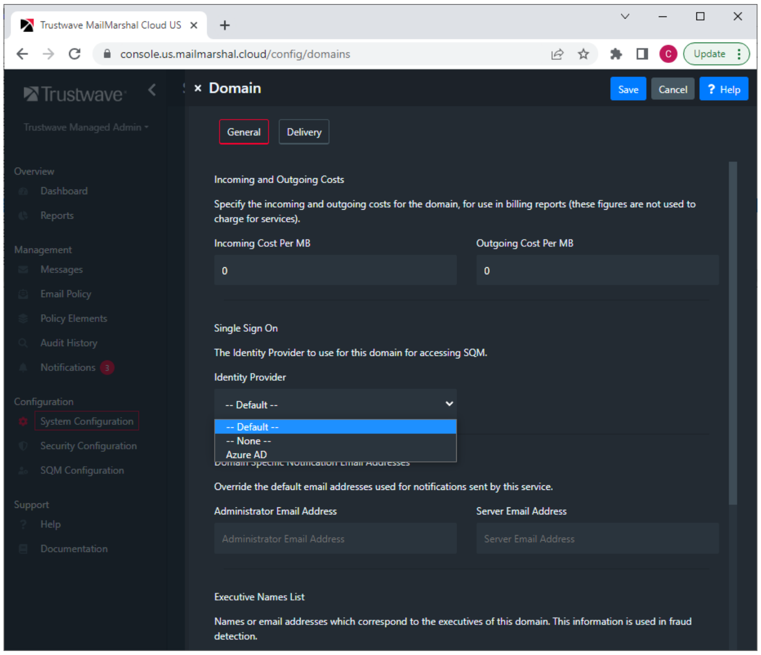
Entity ID
Entity ID

SSO URL
SSO URL

Use Partner 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**.



Incoming and Outgoing Costs

Specify the incoming and outgoing costs for the domain, for use in billing reports (these figures are not used to charge for services).

Incoming Cost Per MB: 0

Outgoing Cost Per MB: 0

Single Sign On

The Identity Provider to use for this domain for accessing SQM.

Identity Provider: -- Default --

-- Default --
-- None --
Azure AD

Domain Specific Notification Email Addresses

Override the default email addresses used for notifications sent by this service.

Administrator Email Address: Administrator Email Address

Server Email Address: Server Email Address

Executive Names List

Names or email addresses which correspond to the executives of this domain. This information is used in fraud detection.

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 (assuming self-provisioning is enabled). All email aliases from the configured attributes will be added for the user.

3.1 Deploy SSO for the SQM

When you are ready to deploy SSO for SQM:

1. In Azure navigate to **Enterprise Applications > MailMarshal Cloud > Users and Groups**.
2. Assign the User role for all the users and groups you want to have access to the SQM.

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.

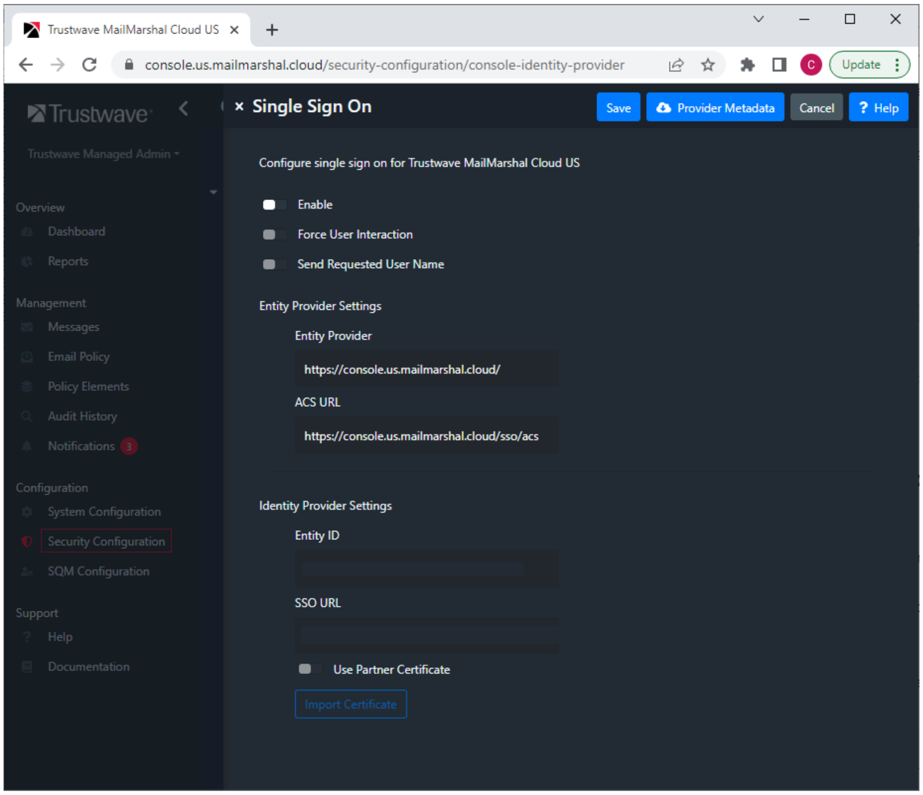
4 Complete Configuration in MailMarshal Cloud for the Console

1. 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 your reseller.

2. At the top of the list, click **Add.**
3. Enter a name such as `Azure AD`.

4. Enter the **Entity ID** and **SSO URL** that you noted from Azure AD.
5. Check the box **Partner Certificate**, and then import the certificate that you saved from Azure AD.



Configure single sign on for Trustwave MailMarshal Cloud US

- Enable
- Force User Interaction
- Send Requested User Name

Entity Provider Settings

Entity Provider

https://console.us.mailmarshal.cloud/

ACS URL

https://console.us.mailmarshal.cloud/sso/acs

Identity Provider Settings

Entity ID

SSO URL

Use Partner Certificate

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.

Click **Save**.

4.1 Deploy SSO for the Console

When you are ready to deploy SSO for the Console:

1. In Azure navigate to **Enterprise Applications > MailMarshal Cloud > Users and Groups**.
2. Assign the User role for all the users and groups you want to have access to the Console.

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.