



CONFIGURATION GUIDE

Single Sign On for MailMarshal Cloud with Azure Active Directory

Table of Contents

About This Document	1
1 Gather Required Data from MailMarshal Cloud	2
2 Create the Application in Azure	2
3 Complete Configuration in MailMarshal Cloud for the SQM	3
3.1 Deploy SSO for the SQM.....	5
4 Complete Configuration in MailMarshal Cloud for the Console	5
4.1 Deploy SSO for the Console	6
About LevelBlue	7

About This Document

This document describes the steps required to configure SAML Single Sign On (SSO) to the 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.
- The MailMarshal Cloud provisioning team 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**).

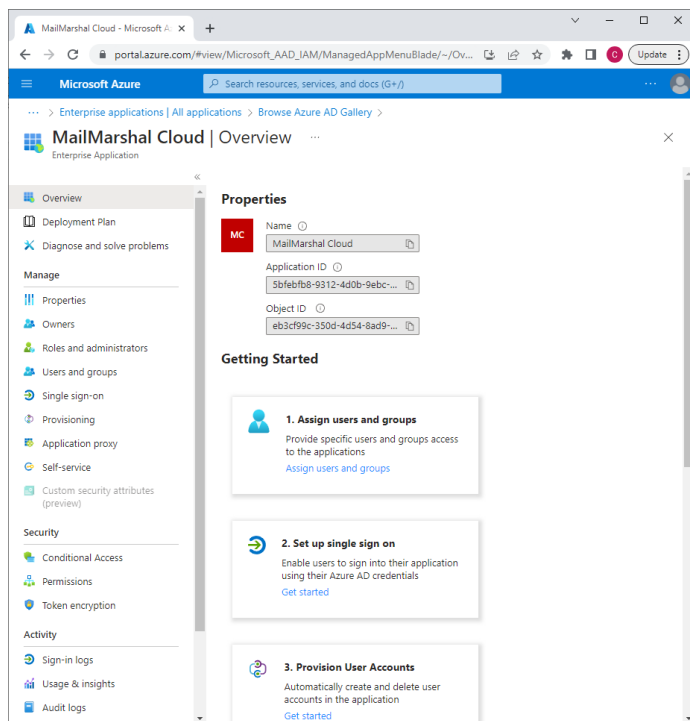


Note: If you do not see one or both of these options, SSO is not enabled for you. Contact your reseller.

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.

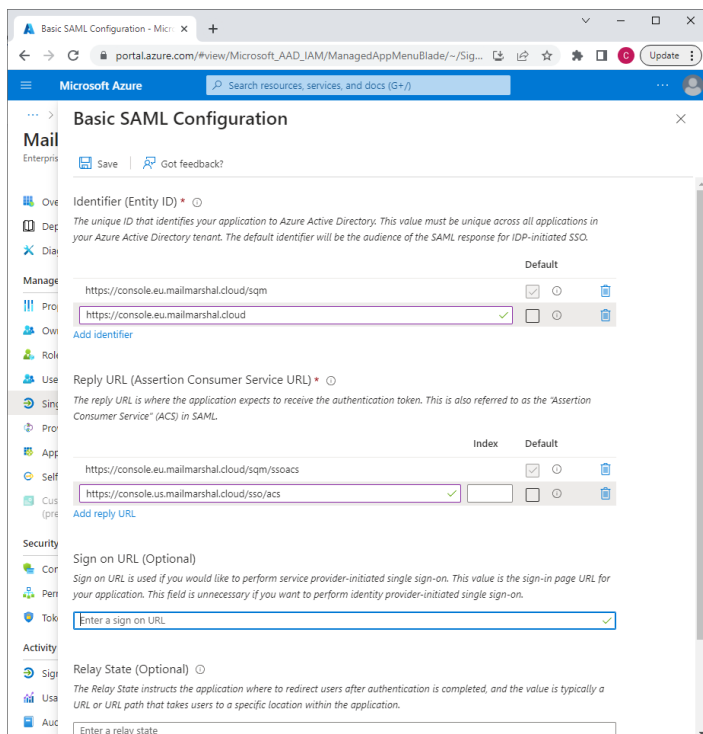
2 Create the Application in Azure

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**.



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 ACS URL if you want to use the same provider for the Console and SQM, as in the screenshot. You can also use separate providers.



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.

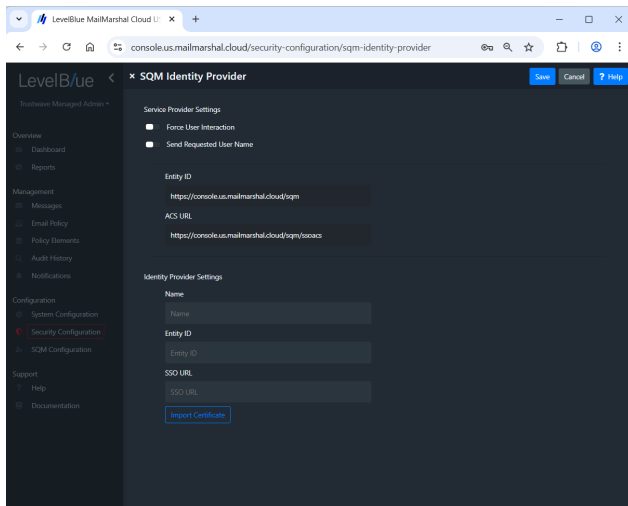
3 Complete Configuration in MailMarshal Cloud for the SQM

1. Log in to the MailMarshal Cloud Console. Navigate to **Configuration > Security Configuration > Single Sign On > SQM Identity Providers**.

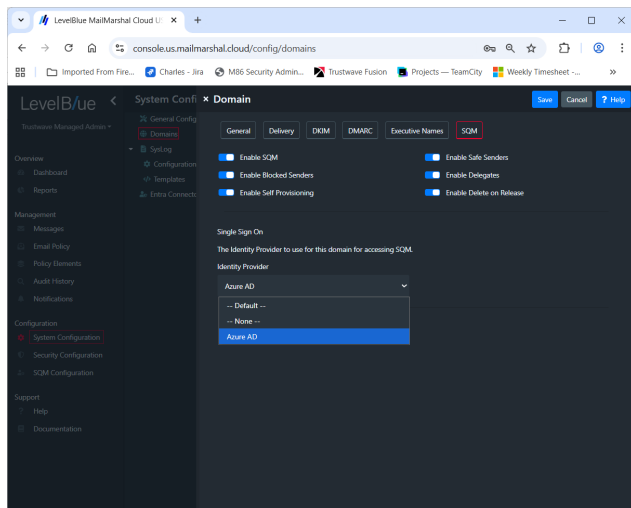


Note: If you do not see this option, SSO is not enabled for you. Contact your reseller.

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.



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**.



8. Test the configuration by logging in to SQM as a valid user. If the user is not 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.

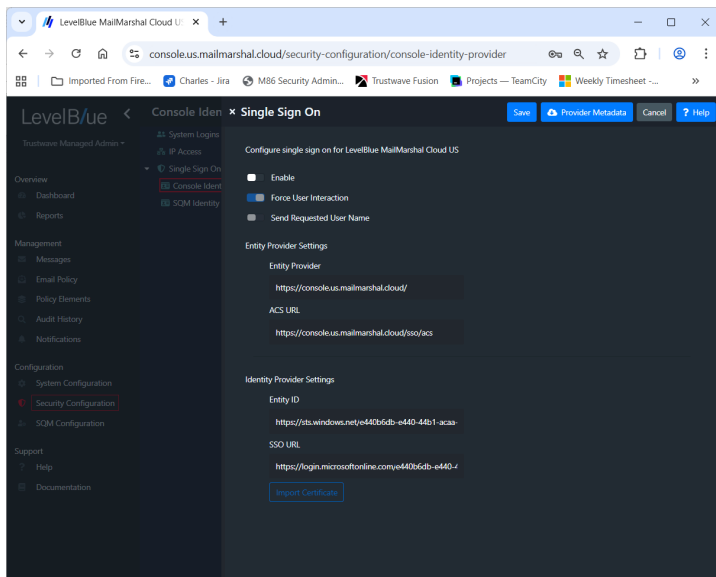
4 Complete Configuration in MailMarshal Cloud for the Console

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.



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 LevelBlue

LevelBlue reduces risk and builds lasting resilience so organizations can innovate and advance their mission with confidence. As the world's most analyst-recognized and largest pure-play managed security services provider, LevelBlue elevates client outcomes that matter: stronger defense, faster response, and sustained business continuity. LevelBlue combines AI-powered security operations, advanced threat intelligence, and elite human expertise to provide the most comprehensive portfolio of strategic advisory, managed security, offensive security, and incident response services.