Trustwave®

CONFIGURATION GUIDE

Single Sign On for MailMarshal Cloud with Microsoft Active Directory

Table of Contents

About This Document

This document describes the steps required to configure SAML Single Sign On (SSO) to the Trustwave MaiMarshal Cloud Spam Quarantine Management site and/or Customer Console, using Microsoft AD FS as the Identity Provider. You can use the same AD FS identity provider for both SQM and the Console, by adding the appropriate values in the AD FS Relying Party setup.

This document assumes that:

- Your reseller has enabled your access to Single Sign On for these services.
- You have configured Microsoft AD FS and have administrator access.
  - For help with configuring AD FS, see Microsoft resources such as the Windows Server 2016 and 2012 R2 AD FS Deployment Guide.

1 Set Up the Relying Party Trust in AD FS

To set up AD FS, first create a Relying Party Trust and then add Claim Rules to define the information that is returned on a successful authentication.

1.1 Gather Required Data from MailMarshal Cloud

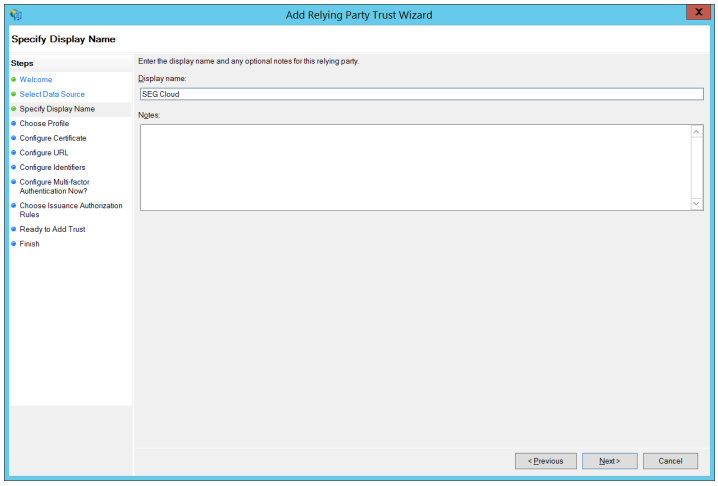
1. Log in to the MailMarshal Cloud Console. Navigate to **Configuration > Security Configuration** and expand **Single Sign On**.
2. Select an option (**SQM Identity Providers** or **Console Identity Provider**).

Note: If you do not see one or both of these options, SSO is not enabled for you. Contact Trustwave or 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 AD FS.
   - Carefully copy the values. The path parts differ for SQM and the Console.

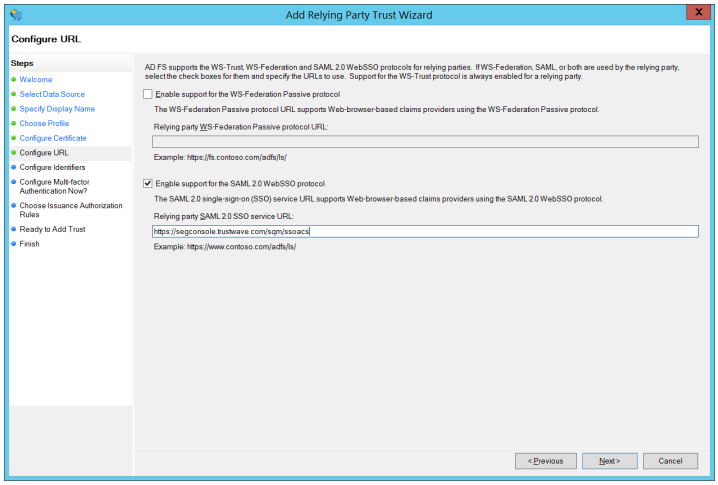
1.2 Create the Relying Party Trust

1. Log on to the AD server and open AD FS Management.
2. Expand the menu tree item **Trust Relationships**, and then select **Relying Party Trusts**.
3. From the Actions pane, click **Add Relying Party Trust**.
4. Click **Start** to start the wizard. After completing each step below, click **Next**.
5. On the **Select Data Source** page, select **Enter data manually**.
6. On the **Specify Display Name** page, enter the name `MailMarshal Cloud`.

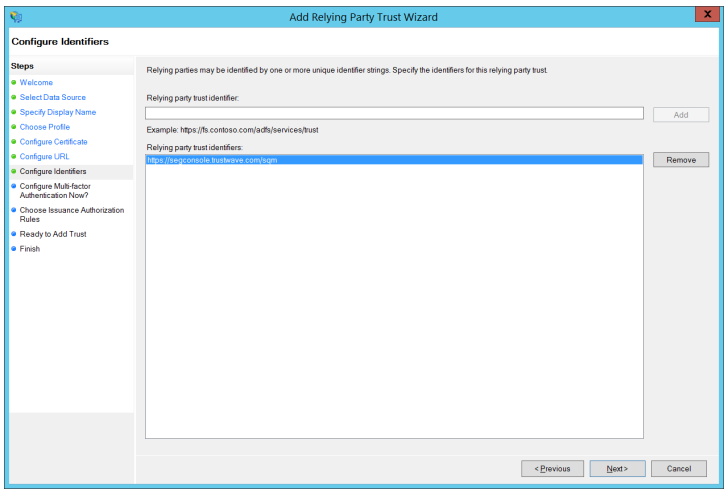


7. On the **Choose Profile** page, choose **AD FS profile** (default selection).
8. On the **Configure Certificate** page, do not enter any information.

9. On the **Configure URL** page, select **Enable Support for the SAML 2.0 WebSSO protocol**. Enter the ACS URL (the examples below use the US Region SQM URL)



10. On the **Configure Identifiers** page, enter the Entity Provider URL and then click **Add**.

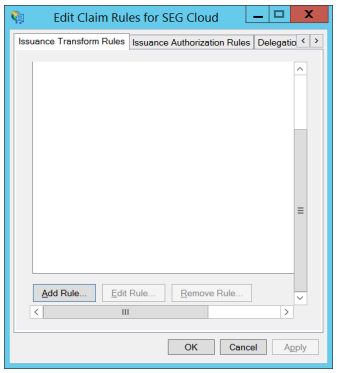


11. On the **Configure Multi-factor authentication Now** page, do not enter any information. You can modify the MFA settings later if required.
12. On the **Choose Issuance Authorization Rules** page, choose to Permit all users. You can modify the permissions later if required.
13. On the **Ready to Add Trust** page, review the settings and then click Next.
14. On the **Finish** page, make sure **Open the Edit Claim Rules** is selected, and then click **Close**.

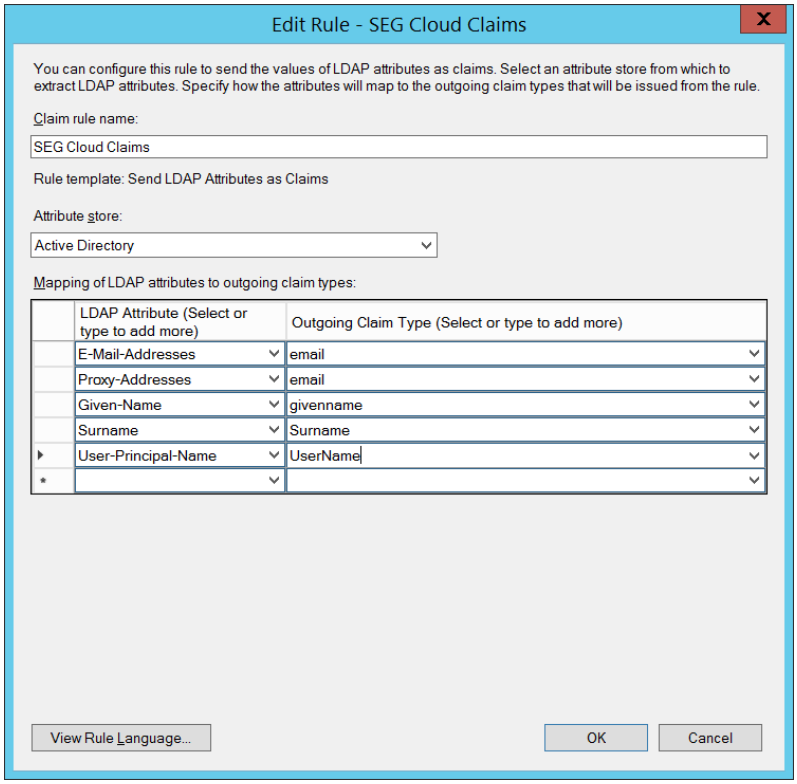
1.3 Add Claim Rules

1. If you are not continuing from the Relying Party Trust wizard, from the FS Management Relying Party Trusts list right-click the MailMarshal Cloud trust item and click Edit Claim Rules.

2. On the Edit Claim Rules window, click **Add Rule**. (If necessary, scroll to the bottom of the pane to see this button.)



3. On the Choose Rule Type page, accept the default **Send LDAP Attributes as Claims**, and then click **Next**.
4. On the Configure Claim Rule page:
    - Give the rule a descriptive name such as MailMarshal Cloud.
    - Select the Attribute Store (normally Active Directory).
    - Select LDAP attributes and claim names as shown and explained below.



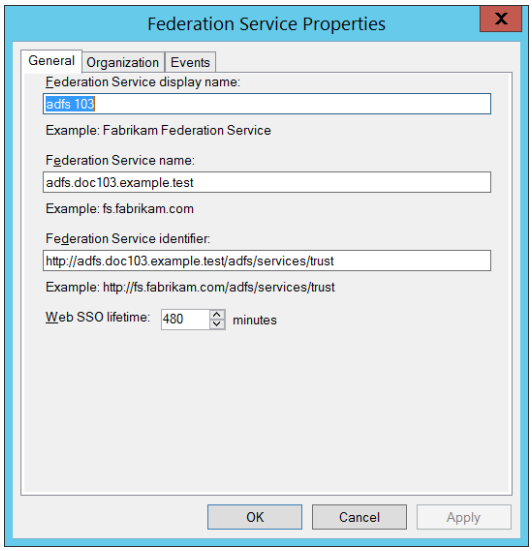
LDAP Attribute	Outgoing Claim Type	Comments
E-Mail-Addresses	email	The list of email addresses from AD
Proxy-Addresses	email	The list of email aliases for the user (this attribute is populated by Exchange Server when integrated with AD). This information is only used by SQM.
Given-Name	givenname	The user's given name, used to construct the text full name shown in MailMarshal Cloud
Surname	surname	The user's surname, used to construct the text full name shown in MailMarshal Cloud
User-Principal-Name	UserName	The user's logon and primary email address

Note: If you store email addresses in more locations, you can add more LDAP attributes for SQM by using the claim type **email**.

1.4 Gather Information

Copy the information that you will need to enter in MailMarshal Cloud to configure the Identity Provider. The required items are the SSO URL, Entity ID, and Partner Certificate.

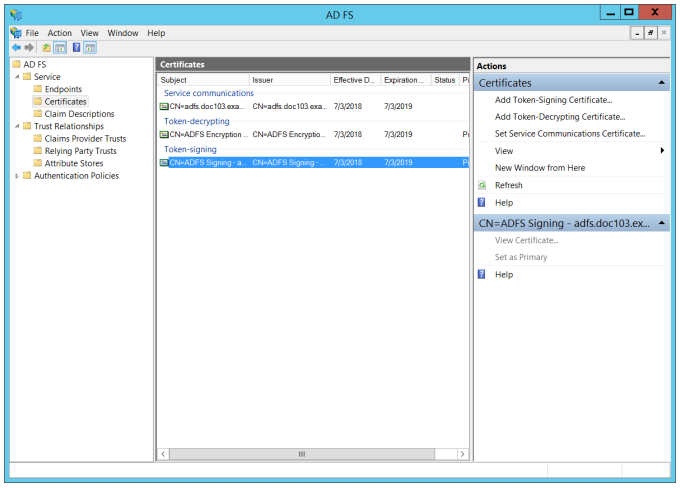
- In AD FS Management, click the menu tree item **Service**, and then from the Actions pane click **Edit Federation Service Properties**.



5. **SSO URL:** From the Federation Service Properties, copy the **Federation Service Name**. The SSO URL uses this value and looks like: `https://[federation service name]/adfs/ls` (without brackets)
6. **Entity ID:** From the Federation Service Properties, copy the value of the **Federation Service Identifier** field.

Note: Copy the value exactly including the Protocol part (this may be `http://` even if the SSO URL uses HTTPS). Typically the value is `http://[federation service name]/adfs/services/trust`

7. In AD FS Management, expand the menu tree item **Service**, and then click **Certificates**.
8. In the Certificates pane, right-click the certificate under **Token-signing** and then click **View Certificate**.



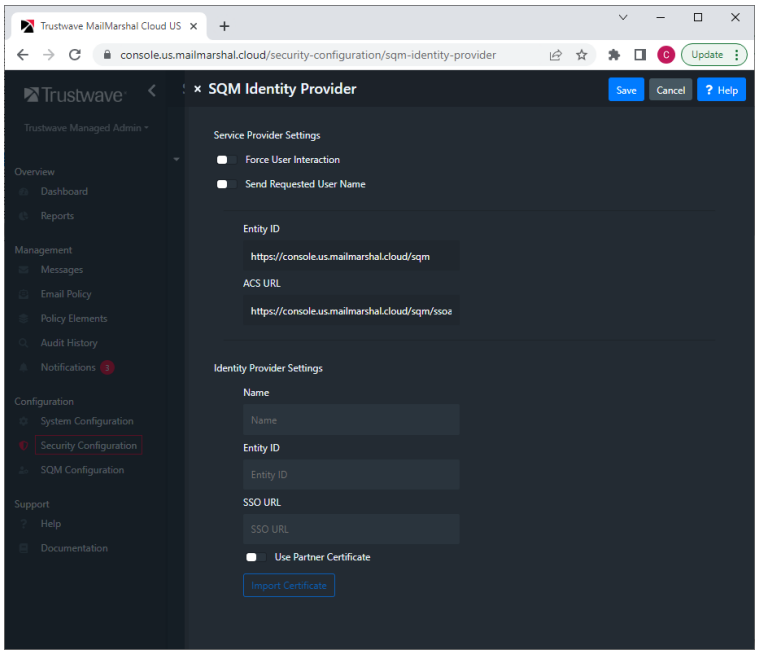
9. On the certificate window, click the Details tab and then click **Copy to File**. Complete the wizard to save the certificate as a DER encoded file.

2 Complete Configuration in MailMarshal Cloud for the SQM

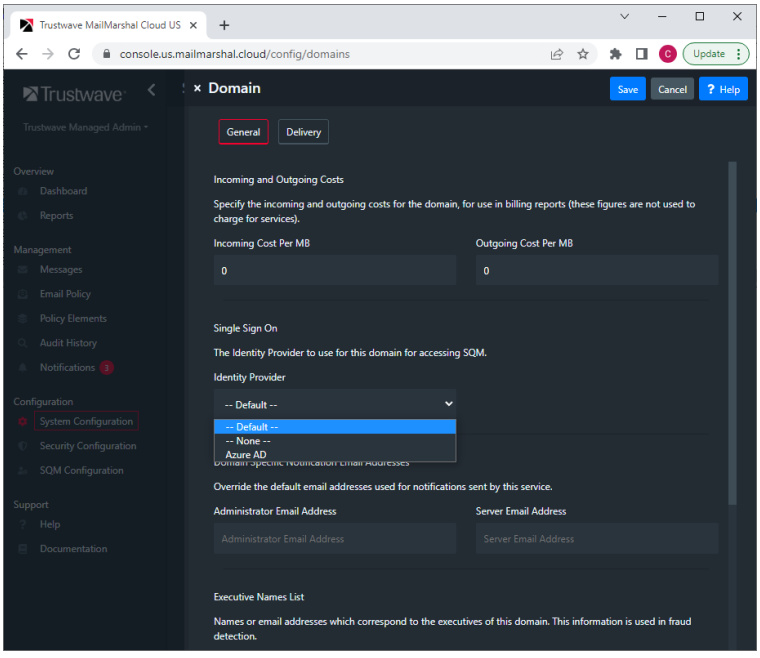
1. Log in to the MailMarshal Cloud Console. Navigate to **Configuration > Security Configuration > Single Sign On > SQM Identity Providers**.

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

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



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 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.

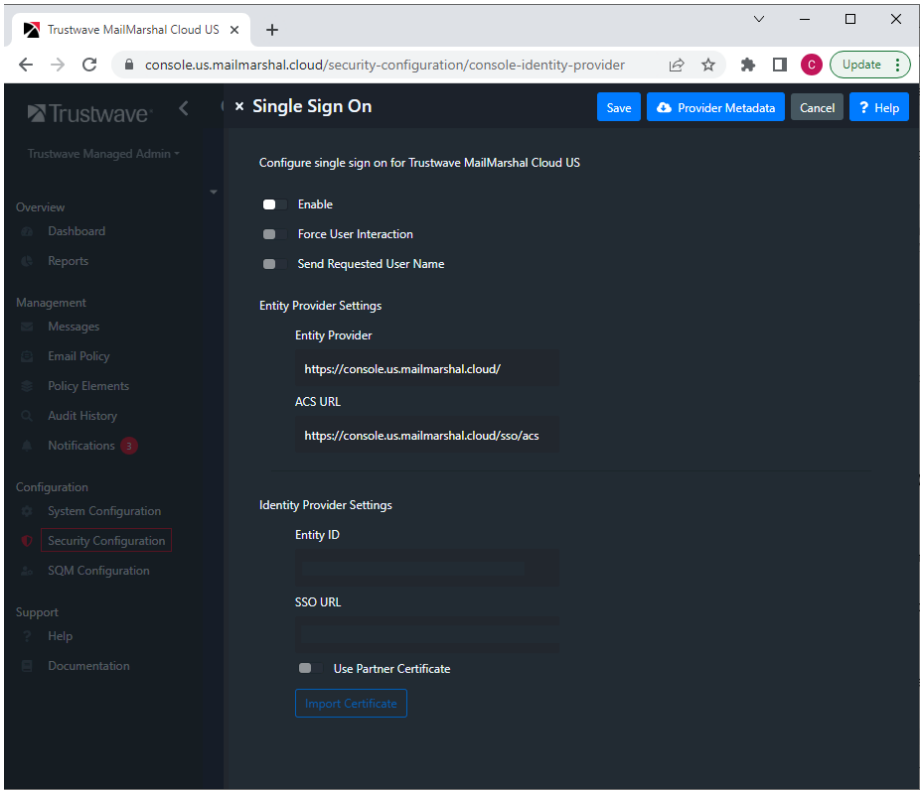
Caution: The number of users that can be created and authenticated in MailMarshal Cloud SQM is limited to the licensed user count in MailMarshal Cloud.

3 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 Trustwave or your reseller.

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



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**.

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.