

CONFIGURATION GUIDE

Single Sign On for MailMarshal Cloud with Microsoft Active Directory

Table of Contents

About This Document	1
1 Set Up the Relying Party Trust in AD FS	2
1.1 Gather Required Data from MailMarshal Cloud	2
1.2 Create the Relying Party Trust	2
1.3 Add Claim Rules	3
1.4 Gather Information	5
2 Complete Configuration in MailMarshal Cloud for the SQM	6
3 Complete Configuration in MailMarshal Cloud for the Console	8
About Trustwave1	0

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 <u>Windows Server 2016</u> 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.

\$ 0	Add Relying Party Trust Wizard	X
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	SEG Cloud	
Specify Display Name	Neter	
Choose Profile		
 Configure Certificate 		Ĥ
 Configure URL 		
Configure Identifiers		
 Configure Multi-factor Authentication Now? 		
 Choose Issuance Authorization Rules 		~
Ready to Add Trust		
 Finish 		
		_
	< <u>Previous</u> <u>Next</u> > Cancel	

- 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)

\$ 2	Add Relying Party Trust Wizard
Configure URL	
Steps 9 Wicknom 9 Secket Otale Source 9 Speechy Display Name 9 Concess Publie 9 Condigue Collections 9 Condigue Lotter 9	AD ES sugados Be WS Trust WS Frederation and SAME 20 WebSSD protocols for valveg parties. IIWS Frederation, SAME, or both see sured by the IRIE to use. Suggester the WS-Trust protocols always enabled for a relying party. C Incluing sugards the WS-Frederation Passive protocol. Relying party (S Frederation Passive)) (Relying Party (S Frede
	< <u>P</u> revious <u>N</u> ext> Cancel

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

Ŵ.	Add Relying Party Trust Wizard	
Configure Identifiers		
Steps	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust	
Welcome		
Select Data Source	Relying party trust identifier:	
Specify Display Name		Add
Choose Profile	Example: https://fs.contoso.com/adfs/services/trust	
Configure Certificate	Polying party trust identificar	
Configure URL	https://seaconsole.trustwave.com/sam	Remove
Configure Identifiers		
Configure Multi-factor Authentication Now?		
Choose Issuance Authorization Rules		
Ready to Add Trust		
• Finsh		
	< Previous Next>	Cancel

- 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.

		E	dit Rule - SEG Cloud Claims				
You extra	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.						
<u>C</u> lain	n rule name:						
SEG	Cloud Claims						
Rule	template: Send LDAP Attribut	es as	Claims				
A 44-11-							
Attrib	oute <u>s</u> tore:						
Activ	ve Directory		¥				
<u>M</u> ap	ping of LDAP attributes to outg	going	claim types:				
	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)				
	E-Mail-Addresses	~	email 🗸				
	Proxy-Addresses	~	email 🗸 🗸				
	Given-Name	~	givenname 🗸 🗸				
	Surname	~	Surname 🗸				
▶	User-Principal-Name	~	UserName 🗸 🗸				
*		~	×				
Vi	ew Rule <u>L</u> anguage		OK Cancel				

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. 4

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**.

Federation Service Properties
General Organization Events Federation Service display name:
adfs 103
Example: Fabrikam Federation Service
F <u>e</u> deration Service name:
adfs.doc103.example.test
Example: fs.fabrikam.com
Federation Service identifier:
http://adfs.doc103.example.test/adfs/services/trust
Example: http://fs.fabrikam.com/adfs/services/trust
Web SSO lifetime: 480 🖍 minutes
OK Cancel Apply

- 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**.

1 0			AD FS			_ D X
File Action View Window	Help					- 8
🗢 🔶 🙇 📰 📓 💷						
AD FS	Certificates		_	_		Actions
Endpoints	Subject	Issuer	Effective D	Expiration	Status Pr	Certificates -
Certificates	Service communications	Chicada da 103 ana	7/2/2010	7/2/2010		Add Token-Signing Certificate
Claim Descriptions	Token desception	CIN-add. doc ros exa	7/3/2010	7/3/2015		Add Token-Decrypting Certificate
Trust Relationships	FalcN+ADFS Encryption	CN+ADES Encryptio	7/3/2018	7/3/2019	P	Set Service Communications Certificate
Claims Provider Trusts	Token-signing					View
Attribute Stores	E CN+ADFS Signing - a	CN+ADFS Signing	7/3/2018	7/3/2019	P	New Window from Horo
Authentication Policies						
						G Kefresh
						Help
						CN=ADFS Signing - adfs.doc103.ex
						View Certificate
						Set as Primary
						Help
						a nop
	1					

- 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.

Trustwave MailMarshal Cloud US 🗙 🕂	ł			~	-		×
\leftrightarrow \rightarrow C \bullet console.us.mailmarsh	nal.cloud/security-configuration/sqm-identity-provider	Ê	☆	* 0	C	Update	:
rustwave < ∶× sc	M Identity Provider			Save	Cance	?	lelp
Trustwave Managed Admin * Se	rvice Provider Settings						
▼ □	Force User Interaction						
Dashboard	Send Requested User Name						
	Entity ID						
	https://console.us.mailmarshal.cloud/som						
	ACSTIR						
	https://console.us.mailmarshal.cloud/sqm/ssoa						
A Notifications 📵 Id	entity Provider Settings						
	Name						
	Entity ID						
	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.

Trustwave MailMarshal Cloud US 🗙	+		`	/	-		×
← → C 🔒 console.us.mailm	arshal.cloud/config/domains	Ê	☆ 🗯		0	Update	2
Trustwave < : ×	Domain		Si	ive	Cance	?	Help
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 (t	here figures	are n	oturad	to	
Reports	charge for services).	tor use in bining reports (e	neae ngurea		otuscu		
Management	Incoming Cost Per MB	Outgoing Cost Per MB					
Messages							
Email Policy							
Policy Elements	Single Sign On						
 Audit History 		504					
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						
SQM Configuration	Override the default email addresses used for notification	c cent by this cenvice					
Support	Administrator Empil Address	Source Empil Address					
? Help		Server Email Address					
Documentation							
	Executive Names List						
	Names or email addresses which correspond to the execu	tives of this domain. This i	nformation	is used	d in frau	ıd	
	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. 7

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

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.



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. 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.