➢ Trustwave[®]

CONFIGURATION GUIDE

Using MailMarshal Cloud with Exchange Online

Table of Contents

| About This Document | 1 |
|----------------------------------------------------------------------------|----|
| 1 Trustwave MailMarshal Cloud for Anti-Malware with Exchange Online | 2 |
| 2 Networking and DNS Setup | 2 |
| 3 Provisioning Trustwave MailMarshal Cloud | 3 |
| 4 Configuring Exchange Online | 4 |
| 4.1 Set up a connector to send outgoing messages through MailMarshal Cloud | 5 |
| 4.2 Set up a connector to accept incoming messages from MailMarshal Cloud | 7 |
| 4.3 Set up Connection Filter Exclusions | 8 |
| 4.4 Set up the SEG Connector Agent for Azure AD | 10 |
| About Trustwave | 13 |

About This Document

This document is for the use of email administrators who are using Trustwave MailMarshal Cloud to accept and filter messages from the Internet, and a cloud based solution to host user mailboxes.

This document provides specific instructions for configuration with Microsoft Exchange Online.



Note: Microsoft frequently re-organizes the management interfaces. Exact steps may differ, but the concepts are the same.

The same ideas can be used to configure other cloud-based mailbox hosting solutions. (For Google G Suite, see the separate document with detailed instructions.)

1 Trustwave MailMarshal Cloud for Anti-Malware with Exchange Online

In this scenario, the organization hosts user mailboxes on a cloud-based service such as Microsoft Exchange Online. The organization uses the Trustwave MailMarshal Cloud service to provide filtering of spam and malware, and other policy controls for both inbound and outbound messages.



2 Networking and DNS Setup

- 1. Configure MX records for all your local domains to point to the Trustwave MailMarshal Cloud environment.
- 2. Add the MailMarshal Cloud server to your SPF record as an include. Also include the Office365 SPF record.



Note: The settings depend on the regional instance of MailMarshal Cloud configured for your customer account when provisioned. For details of the configuration data required, see the details for your instance (US, Australia, or EU linked from the <u>MailMarshal Cloud Information</u> page.

In most cases MX records are updated when you are ready to direct email into the new environment (after all other configuration is complete).

3 Provisioning Trustwave MailMarshal Cloud

Trustwave Provisioning or Managed Security Services must configure MailMarshal Cloud to accept and deliver email for your domains.

- 1. MailMarshal Cloud will deliver email incoming for your managed domains to the cloud hosting environment. Provide the delivery details to Trustwave.
 - For Exchange Online, use the "MX endpoint" of your Exchange Online environment (such as yourexampledomain-com.mail.protection.outlook.com).
- 2. MailMarshal Cloud will accept email relaying (messages sent to other domains "from" your managed domains) based on the configured inbound delivery addresses. For Exchange Online, to ensure that the relaying addresses are up to date, Trustwave will also configure relaying based on the SPF records published by the service.



Tip: The default domain in Exchange Online must be a domain configured in MailMarshal Cloud.

4 Configuring Exchange Online

You will set up two connectors to route email between MailMarshal Cloud and Exchange Online.

To complete this step, you must have an Office 365 Administrator credential with permission to create connectors. You may find that the validation process only works with a Microsoft browser.

To create a connector in Office 365:

1. From the Office site, open the app menu and click Admin (If you do not see Admin, click All apps).



2. From the Admin left menu, click Exchange to go to the Exchange Admin Center.



3. Next, expand mail flow, and then click connectors.

4.1 Set up a connector to send outgoing messages through MailMarshal Cloud

- 1. To start the Connector wizard, click Add a connector.
- 2. On the first screen, choose a connector as follows:

Connection from Office 365 Connection to Partner Organization

Click Next.

| Add a connector | |
|-------------------------|--------------------------------------------------------------------------------------------|
| New connector | |
| O Name | New connector |
| O Use of connector | Specify your mail flow scenario, and we'll let you know if you need to set up a connector. |
| O Routing | Connection from |
| O Security restrictions | Office 365 Your organization's email server |
| Validation email | Partner organization |
| Review connector | Connection to |
| | Vour organization's email server Partner organization |
| | |
| | Next |

3. On the next screen, give the connector a name and a detailed description. If you want to enable this routing immediately, check the box **Turn it on**. Click **Next**.

| | Add a connector | |
|---|-----------------------|--------------------------------------------------------------------------------------------------|
| = | New connector | |
| | Name | Connector name |
| | O Use of connector | This connector enforces routing and security restritions for email messages sent from Office 365 |
| | O Routing | to your partner organization or service provider. |
| | Security restrictions | To MailMarshal Cloud |
| | Validation email | Description Route all outbound email to MailMarchal Cloud |
| | Review connector | |
| | | What do you want to do after connector is saved? |
| | | V Turn it on |
| ß | | Back Next |

4. On the following screen (Use of connector), select *Only when email messages are sent to these domains.*

| | Add a connector | × |
|---|-------------------------------------------|---------------------------------------------------------------------------------------------|
| = | New connector | |
| R | Name | Use of connector |
| | Use of connector | Specify when you want to use this connector. |
| | C Routing | Only when I have a transport rule set up that redirects messages to this connector |
| 9 | Security restrictions | Only when email messages are sent to these domains Example: * or *.contoso.com or *.com |
| | Validation email | · 💼 |
| | Review connector | |
| | | Back Next |

In the field, enter * and then click + to add the entry. Click Next.

- 5. On the next screen (Routing), select Route email through these smart hosts.
- Enter the externally resolvable hostname of the Trustwave MailMarshal Cloud server, then click + to add the entry. For details of the name required, see the connection details for your instance (US, Australia, or EU) linked from the MailMarshal Cloud Information page.

| | Add a connector | | × |
|------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| = | New connector | | |
| 6 | Name | Routing | |
| × | Use of connector | 5 | |
| | Routing | How do you want to route email messages? Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an all-emails are not and can be identified builtion a fully multified domain agree (EDDM) or an | |
| | O Security restrictions | all rationauro server and can be identified by daming a rainy qualified domain name (r-Qohy or an IP address. | |
| | Validation email | Route email through these smart hosts | |
| | C Review connector | psample myhost contos com or 192166.3.2 + | |
| | | | |
| <i>R</i> e | | | |
| G | | Back Next | |

- 7. On the following screen (Security restrictions), the *Always use Transport Layer Security* box should be selected.
- 8. Ensure that your connector validates. You will need to add a deliverable email address where a message can be sent for validation. Because this connector is used for all outbound messages, you can enter any address outside your managed domains.



Tip: The default domain in Exchange Online will be used as the domain of the From address. Be sure that this domain is one of your domains configured in MailMarshal Cloud. If it is not, the validation email will be rejected with the message 550 Cannot determine unique tenancy.

If your Exchange Online environment includes domains that are not configured in MailMarshal Cloud, you must configure a Transport Rule to limit the messages sent through this connector.

| Add a connector | | |
|-------------------------------------------|----------------------------------------------------------|----------------------------------|
| New connector | | |
| Name | Validation email | |
| Use of connector | Specify an email address for an active mailbox that's on | your partner domain. You can add |
| Routing | multiple addresses if your partner organization has more | e than one domain. |
| Security restrictions | Example: user@contoso.com testuser@example.com | ÷ |
| Validation email | Validate | |
| Review connector | | |
| | | |
| | | |
| | Back Next | |

9. Save the connector.

4.2 Set up a connector to accept incoming messages from MailMarshal Cloud



Note: When you set up a connector as described in this section, Exchange Online will ONLY accept incoming SMTP messages that are sent from the MailMarshal Cloud servers at the IP addresses you specify. Messages from any other source will be refused.

This connector is required to ensure that malware or spam cannot bypass MailMarshal Cloud. You should only enable the connect AFTER you have updated MX records and confirmed email is flowing through MailMarshal Cloud to Exchange Online.

The steps to accept incoming messages are similar to those for outgoing messages.

- 1. To start the Connector wizard, click the plus symbol +.
- 2. On the first screen, choose a connector as follows (note the direction):

Connection from Partner Organization Connection to Office 365

- 3. Give the connector a name and verbose description.
- 4. On the screen Authenticating sent email, select By verifying that the sender domain matches one of the following domains.
 - Enter * (to signify all domains), and then click + to add the entry.
- 5. On the Security restrictions screen, keep the entry *Reject email messages if they aren't sent over TLS*. Do not require a subject name on the certificate.
- 6. Select Reject email messages if they aren't sent from within this IP address range

• Type or paste each required range and then click + to add it. For details of the ranges required, see the connection details for your instance (US, Australia, or EU) linked from the MailMarshal Cloud Information page.

| Add a connector | |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| New connector | |
| Name | Security restrictions |
| Authenticating sent email | What security restrictions do you want to apply? |
| Security restrictions | Reject email messages if they aren't sent over TLS |
| Review connector | And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name |
| | Example: contoso.com or *.contoso.com |
| | Reject email messages if they aren't sent from within this IP address range Example: 10.5.3.2 or 10.3.1.5/24 |
| | |
| | |
| | |
| | |

7. Repeat until you have added all required ranges for your instance.



Note: Some instances use ranges with CIDR /22. Because Exchange Online only allows ranges with /24 or higher, in this case you must enter four ranges to cover the required addresses.

8. Save the connector.

4.3 Set up Connection Filter Exclusions

Exchange Online includes a "connection filtering" function that limits the number of messages received from each IP address. You must exclude MailMarshal Cloud from this filtering to ensure that all incoming messages can be delivered.

To set up exclusions:

1. From the Office site, open the app menu and click **Security** (*If you do not see Security, click* **All** *apps*).

2. Navigate to Policies & Rules > Threat policies > Anti-spam policies. Edit the Connection filter policy (default).

| | Microsoft 365 Defender | | ۵ | 20 \$ |
|------------|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------|
| = | | | | |
| ŵ | Home | Policies & rules > Threat policies > Anti-spam policies | | |
| 0 | Incidents & alerts | | | |
| 3 | Actions & submissions $\qquad \qquad \lor$ | Please go to the quarantine policy page to configure end-user spam notification as we will remove the configuration from the Anti-s December 2021. Learn more about quarantine policy | pam policy | by |
| ⊉ | Secure score | Use this page to configure policies that are included in anti-spam protection. These policies include connection filterin filtering, and outbound spam filtering. Learn more | ng, spam | |
| ð | Trials | + Create policy \checkmark \circlearrowright Refresh 1 of 3 selected \bigcirc Search | | - ~ |
| | Email & collaboration | Name Status Priority Type | | |
| Ξ | Review | Anti-spam inbound policy (Def • Always on Lowest | | |
| D a | Exchange message trace | Connection filter policy (Default) • Always on Lowest | | |
| <u>B</u> | Attack simulation training | Anti-spam outbound policy (De • Always on Lowest | | |
| <u></u> | Policies & rules | | | |
| Ł | Reports | | | |
| R | Audit | | | |
| S | Health | | | Ţ. |
| Q | Permissions & roles | | | |

- 3. On the edit pane, in the Always Allow list, add the IP address ranges for MailMarshal Cloud, as in the connector setup.
- 4. Click Save.



Note: Be sure to enter the correct IP ranges to allow inbound for your instance (US, Australia, or EU) linked from the <u>MailMarshal Cloud Information</u> page.

The filtering information may appear as below:



| 20.01.201.30/08 | 10 | 52 H85.84.52/28 × | 52 NEL34 Ng/28 × | |
|----------------------------|--------------|-------------------------|-------------------|---|
| 51,111,241,310,310,210 | \mathbb{R} | 511.1465.2551.2000/08 × | 52,145,15,150,000 | 1 |
| 571, 1686, 1923, 1986, 209 | 1 | 201-40 HER 1/76/201 | 30.40105.00/08 | × |
| ALIN SEAL ST | 40.0 | N 57250 × 364070 | 15.230 × | |
| 20.40102010 | | 04/03/04 × 30 | × #0,012002.0014 | |
| 21141 112.2111.31 | 10 | 204 (3.200.0/54 × | | |

Always block messages from the following IP addresses or address range:



4.4 Set up the MailMarshal Connector Agent for Azure AD

The Connector Agent is an optional module of MailMarshal Cloud that allows you to retrieve information about local user groups and email addresses from your Active Directory server or LDAP server, for use in MailMarshal Cloud policy.

You can use the Connector Agent with Azure AD.



Tip: For full instructions about how to download, install, and configure the Connector Agent, refer to the MailMarshal Cloud Customer Guide.

- If you have a workstation or server available on premises that is a domain member, you can install and configure the Connector Agent in the same way as for a premises AD installation. Refer to the MailMarshal Cloud Customer Guide.
- You can also use the Connector Agent to synchronize information from Azure AD using LDAPS.

To use the Connector Agent with Azure AD LDAPS:

1. Configure Secure LDAP (LDAPS) in Azure AD Domain Services. See the Microsoft documentation for this task.

2. Once secure LDAP access to your managed domain over the internet is successfully enabled, the Azure AD Domain Services management site shows the external IP address that can be used to access your directory over LDAPS in the field **EXTERNAL IP ADDRESS FOR LDAPS ACCESS**.

| domain services PREVIEW | | |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------|---|
| ENABLE DOMAIN SERVICES FOR THIS DIRECTORY | YES NO | 0 |
| Users will not be able to login to the o | domain using their credentials until you enable password synchronization. | |
| DNS DOMAIN NAME OF DOMAIN SERVICES | contoso100.com | 0 |
| CONNECT DOMAIN SERVICES TO THIS VIRTUAL NETWORK | MyPreviewVnet Subnet-1(10.0.0/23) Central US subscrip v | ß |
| IP ADDRESS | 10.0.0.5; 10.0.0.4 | Ø |
| SECURE LDAP (LDAPS) | Configure certificate | 0 |
| SECURE LDAP CERTIFICATE | Thumbprint: 74FD5D7FED958DD9506A303E9690734A83F28040 Certificate expires: Tue, 18 Apr 2017 16:34:16 GMT | 0 |
| ENABLE SECURE LDAP ACCESS OVER THE INTERNET | YES NO | Ø |
| EXTERNAL IP ADDRESS FOR LDAPS ACCESS | 52.165.38.113 | 0 |

3. Install the Connector Agent on any computer that has Internet access (HTTPS access to MailMarshal Cloud, and port 636 for LDAPS access to the Azure LDAPS IP address).

4. Create a new connector, and specify a LDAP directory of type "Microsoft Active Directory".

| New Connector Wizard | × |
|--------------------------------------------------------------------------------------------------------------------------|---|
| Connector Type Connector Agent can import user groups and distribution lists from a variety of directory services. | |
| What type of network directory do you want to connect to? | |
| O Microsoft Active Directory | |
| C LDAP Directory | |
| Microsoft Active Directory | |
| C Load user list from text file | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| < <u>B</u> ack <u>N</u> ext > Cancel Help | |

5. Enter the Azure LDAPS IP address. Specify port 636 and select **Connect using SSL**. Enter logon credentials.

| New Connector Wizard | × |
|------------------------------------------------------------------------------------------------------------------------|---|
| LDAP Server and Logon Connector Agent will use the following settings to connect and log on to your LDAP server. | |
| Enter the server name and port details for this connector: | |
| Server <u>N</u> ame: 52.16538.113 <u>B</u> rowse | |
| Server Port: 636 | |
| Connect using <u>S</u> SL | |
| Version: 2 | |
| | |
| Iver Name: | |
| Decenverd | |
| Password: | |
| Domain: | |
| Use Windows Integrated Security (NTLM) | |
| | |
| | |
| < <u>B</u> ack Next > Cancel Help | |

- 6. Click Next. The Agent tests the connection.
- 7. When the connection is successfully tested, continue the Wizard as described in the MailMarshal Cloud Customer Guide.
- 8. When the connector has been successfully created, you can proceed to select groups for synchronization.

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.