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 4

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 Enhanced Filtering for Connectors 10

4.5 Set up the MailMarshal Entra Connector 11

About Trustwave **12**

About This Document

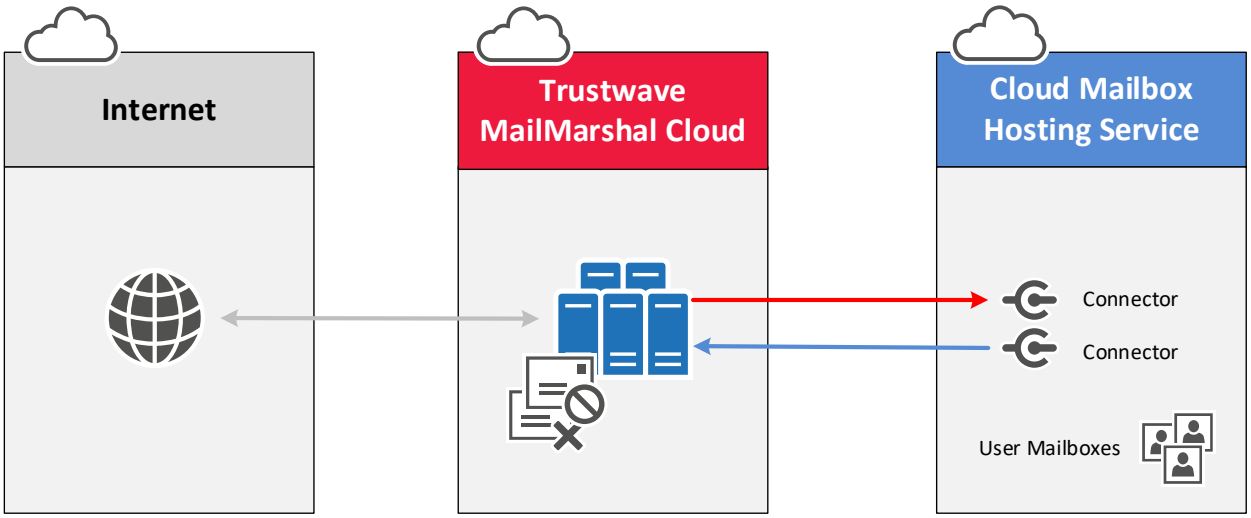
This document is for the use of email administrators who are using Trustwave MailMarshal Cloud to accept and filter messages from the Internet, and Microsoft Exchange Online to host user mailboxes.

The content has been updated in August 2024 with information about the Entra Connector and Enhanced Filtering.

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

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 MailMarshal Cloud Information 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.

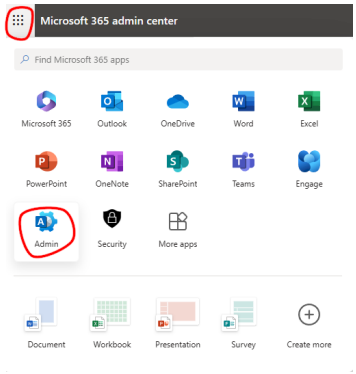
4 Configuring Exchange Online

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

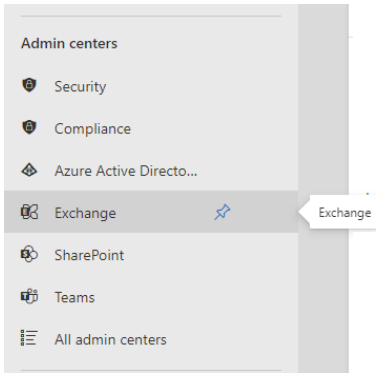
To complete this step, you must have an Office 365 Administrator credential with permission to create connectors. You may find that the validation process only works with a Microsoft browser.

To create a connector in Office 365:

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



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



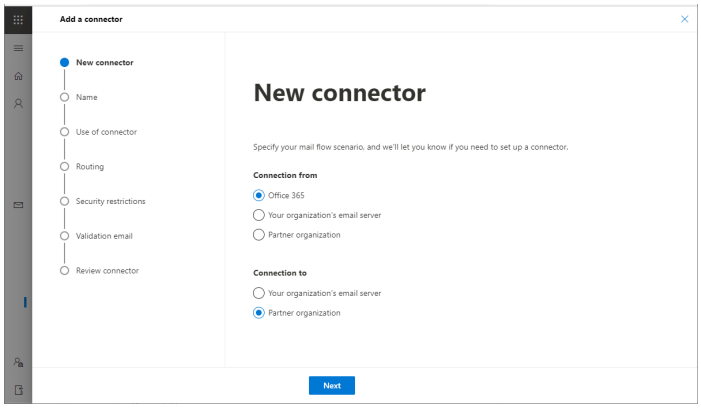
5. Next, expand **mail flow**, and then click **connectors**.

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

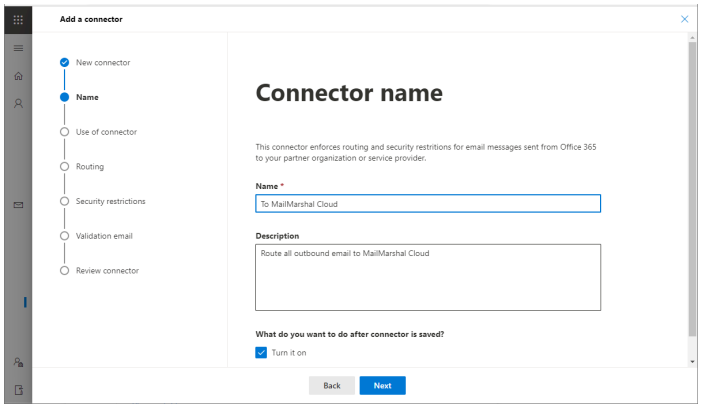
1. To start the Connector wizard, click **Add a connector**.
2. On the first screen, choose a connector as follows:

Connection from
Office 365
Connection to
Partner Organization

Click **Next**.

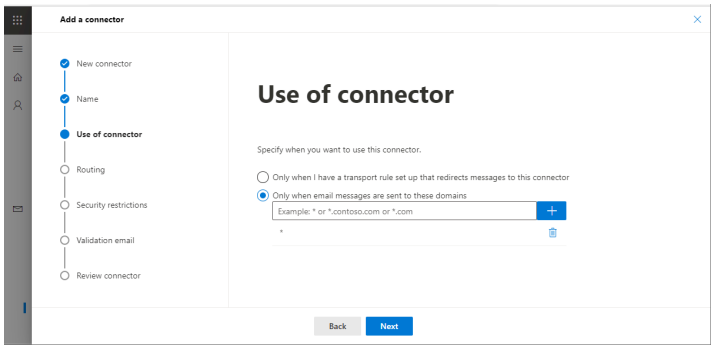


3. On the next screen, give the connector a name and a detailed description. If you want to enable this routing immediately, check the box **Turn it on**. Click **Next**.



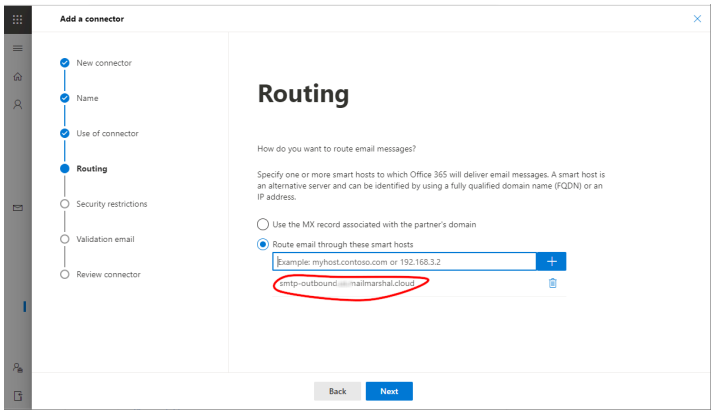
4. On the following screen (Use of connector), select *Only when email messages are sent to these domains.*

   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*.

6. 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.

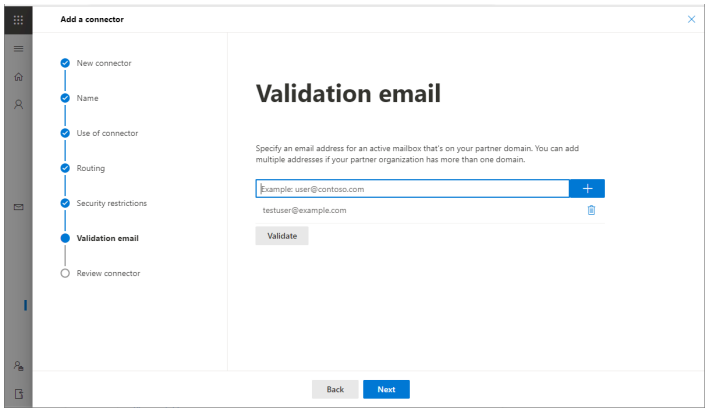


7. On the following screen (Security restrictions), the *Always use Transport Layer Security* box should be selected.

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.



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.

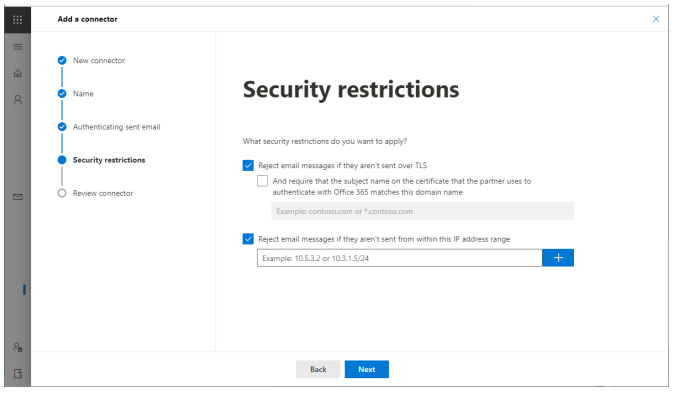
This connector is required to ensure that malware or spam cannot bypass MailMarshal Cloud. You should only enable the connect AFTER you have updated MX records and confirmed email is flowing through MailMarshal Cloud to Exchange Online.

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

10. To start the Connector wizard, click **Add a connector**.
11. On the first screen, choose a connector as follows **(note the direction):**

    Connection from
    Partner Organization
    Connection to
    Office 365

12. Give the connector a name and verbose description.
13. 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.
14. 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.**
15. 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.



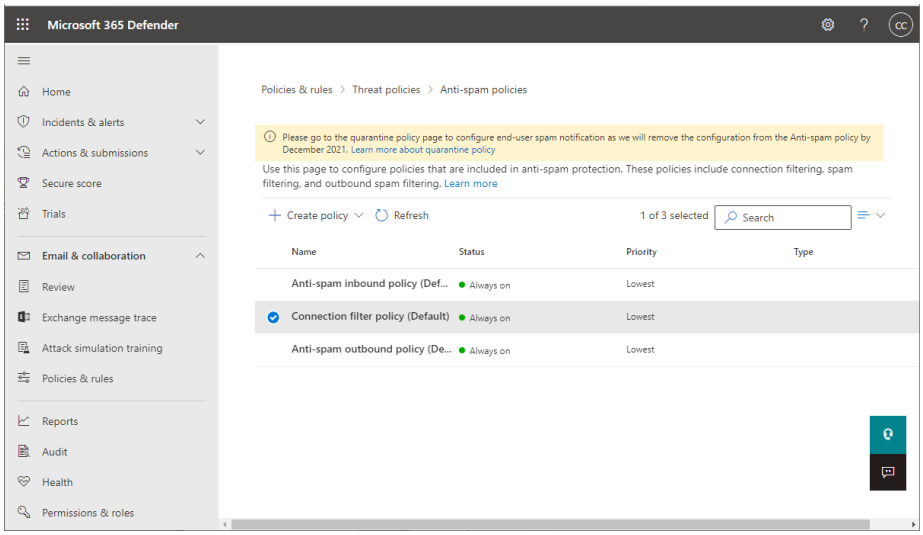
16. Repeat until you have added all required ranges for your instance.
17. Save the connector.

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 under Admin Centers, 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).**

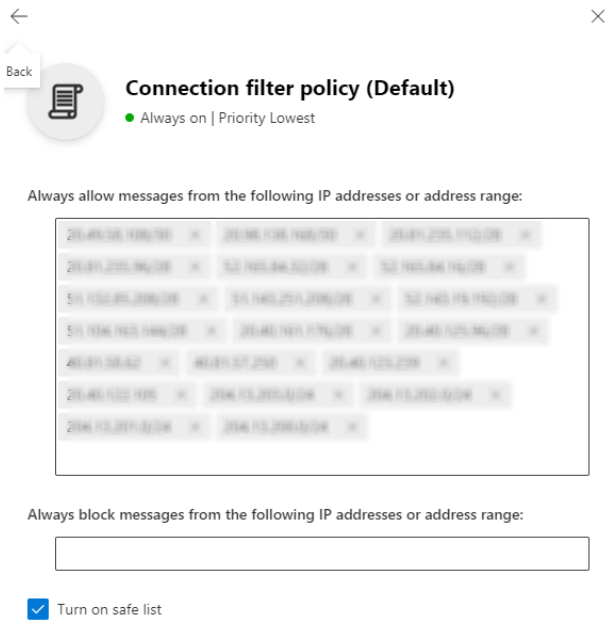


3. On the edit pane, in the Always Allow list, add the IP address ranges for MailMarshal Cloud, as in the connector setup.

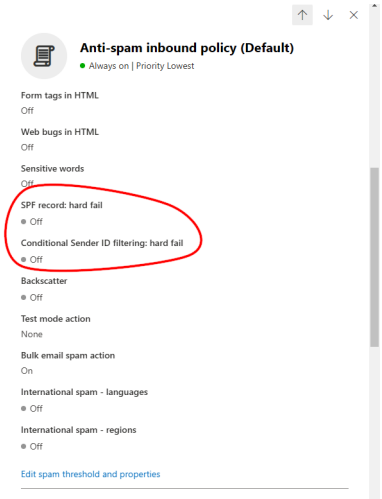
4. Click **Save**.

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

The filtering information may appear as below:



5. Return to **Anti-spam policies**. Edit the **Anti-spam inbound policy (default)**.
6. Scroll down to see the status of the following items. *These items must be set to **Off**. Validation of these policies is performed by MailMarshal Cloud. Results from Exchange Online will not be valid and can cause over-blocking of legitimate messages.*
   a. SPF Record: hard fail
   b. Conditional Sender ID filtering: hard fail



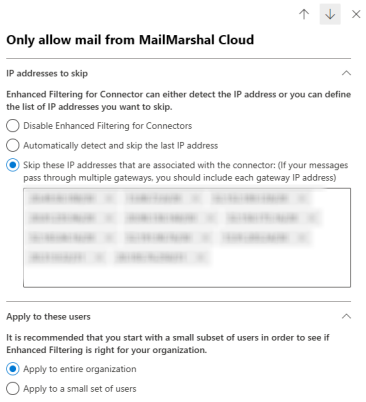
7. If either of the above items is set to **On**, scroll further and click the link Edit spam threshold and properties. Set each of the above items to **Off**, and click **Save**.

4.4 Set up Enhanced Filtering for Connectors

Exchange Online provides the ability to filter based on the source IP address of a message. This optional feature can provide an additional layer of security against spoofed or malicious messages. For this feature to be useful with MailMarshal Cloud, you must configure it to skip IP addresses associated with MailMarshal Cloud.

To set up exclusions:

1. From the Office site, open the app menu and under Admin Centers, click **Security** *(If you do not see Security, click **All apps**).*
2. Navigate to **Email & Collaboration > Policies & Rules > Threat policies > Enhanced Filtering.**
3. On the Enhanced Filtering for Connectors page, select the connector that you set up to accept incoming messages from MailMarshal Cloud.
4. On the fly-out menu, select “Skip these IP addresses”.
   a. Enter each required range for your instance of MailMarshal Cloud. For details of the ranges required, see the connection details for your instance (US, Australia, or EU) linked from the MailMarshal Cloud Information page.
      i. Type or paste each required range and then press **Enter** to add it.
   b. If you are planning to use the Sandbox feature in MailMarshal Cloud, also enter the following ranges associated with the Sandbox service:
      ```
      13.91.203.24/30
      52.191.90.76/30
      20.31.9.32/31
      20.105.76.250/31
      ```
5. Choose to test with a subset of users, or keep the default setting “Apply to entire organization”



6. Click **Save**.

4.5 Set up the MailMarshal Entra Connector

The Entra Connector is a feature of MailMarshal Cloud that allows you to retrieve user groups and the associate email addresses from Microsoft Entra ID (Azure AD).

Group membership is synchronized hourly.

You can use the imported groups in MailMarshal user matching by adding them to MailMarshal groups.

To use the Entra Connector:

7. Register an application in Microsoft Entra Admin Center. See MailMarshal Cloud Knowledgebase article 21218.
8. Enter the details of the Connector in the MailMarshal Console (System Configuration > Entra Connector Properties).
9. Select groups to import in the MailMarshal Console (Policy Elements > User Groups, Import Entra Groups).
10. Add the groups to local MailMarshal groups as required, and use these groups in policy user matching.

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 Fusion® 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.