CLOUDFLARE
AREA 1 SECURITY

# Email Security for Microsoft Office 365

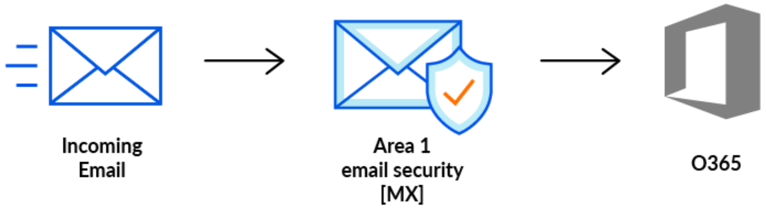
Deployment and Configuration Guide - Cloudflare Area 1 as MX Record

## Cloudflare Area 1 Overview

Phishing is the root cause of upwards of 90% of security breaches that lead to financial loss and brand damage. Cloudflare Area 1 is a cloud-native service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors and comprehensive attack analytics, Area 1 cloud email security proactively identifies phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of a phishing attack cycle. Using flexible enforcement platforms, Area 1 allows customers to take preemptive action against these targeted phishing attacks across all vectors - email, web and network; either at the edge or in the cloud.

# Email Flow

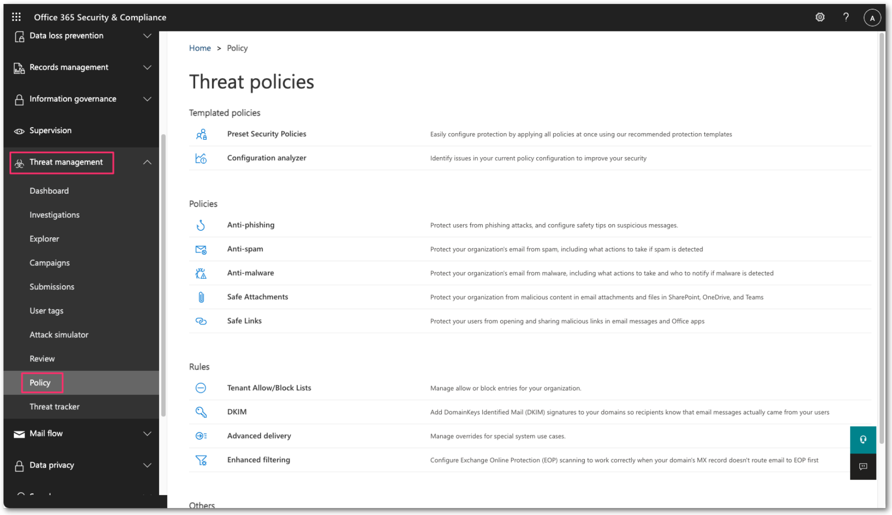


## Configuration Steps

- Step 1: Add Area 1 IP addresses to Allow List
- Step 2: Execute O365 Enable-OrganizationCustomization (if required)
- Step 3: Enhanced Filtering Configuration
- Step 4: Configure Area 1 Quarantine Policies
- Step 5: Update your domain MX Records

# Step 1: Add Area 1 IP addresses to Allow List

1. From the Microsoft Security admin center (https://protection.office.com/homepage), under the Threat management section, select the Policy settings (https://protection.office.com/threatpolicy):



Threat policies

Templated policies

| | |
|---|---|
| Preset Security Policies | Easily configure protection by applying all policies at once using our recommended protection templates |
| Configuration analyzer | Identify issues in your current policy configuration to improve your security |

Policies

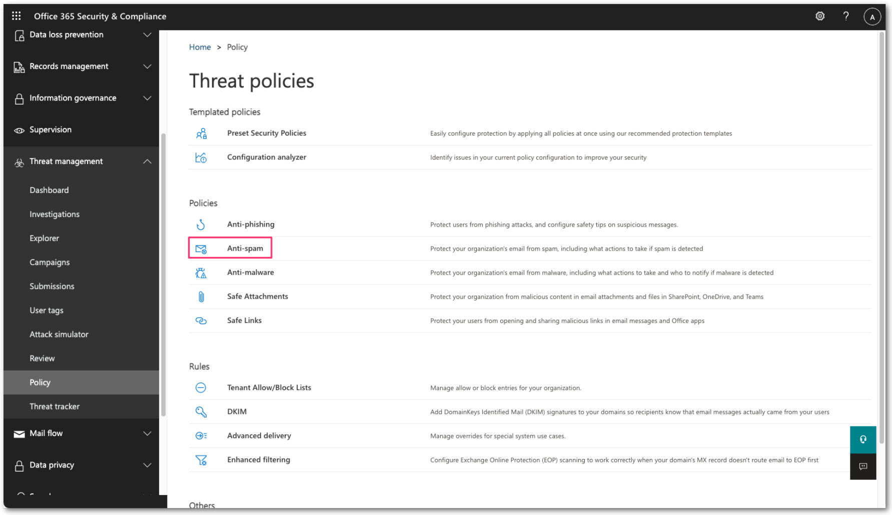
| | |
|---|---|
| Anti-phishing | Protect users from phishing attacks, and configure safety tips on suspicious messages. |
| Anti-spam | Protect your organization's email from spam, including what actions to take if spam is detected |
| Anti-malware | Protect your organization's email from malware, including what actions to take and who to notify if malware is detected |
| Safe Attachments | Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams |
| Safe Links | Protect your users from opening and sharing malicious links in email messages and Office apps |

Rules

| | |
|---|---|
| Tenant Allow/Block Lists | Manage allow or block entries for your organization. |
| DKIM | Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users |
| Advanced delivery | Manage overrides for special system use cases. |
| Enhanced filtering | Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first |

Others

2. On the right configuration pane, select the Anti-spam option (https://protection.office.com/antispam):



Threat policies

Templated policies

| | |
|---|---|
| Preset Security Policies | Easily configure protection by applying all policies at once using our recommended protection templates |
| Configuration analyzer | Identify issues in your current policy configuration to improve your security |

Policies

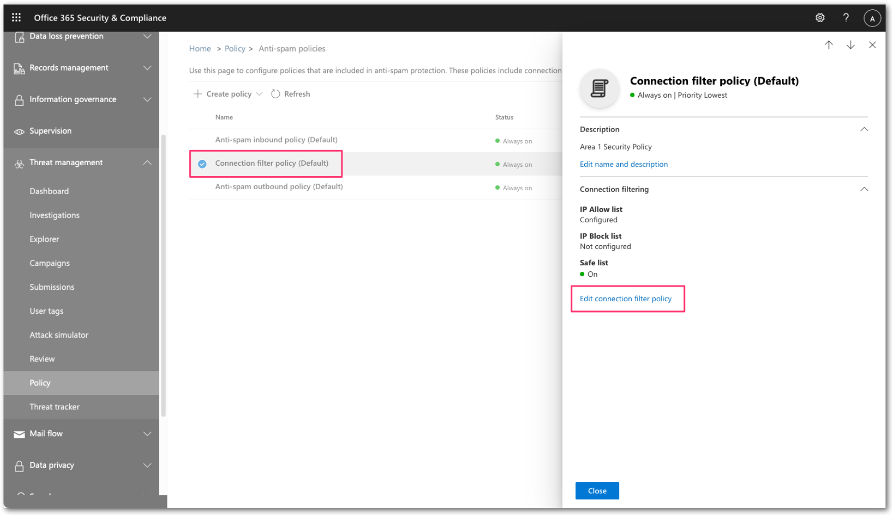
| | |
|---|---|
| Anti-phishing | Protect users from phishing attacks, and configure safety tips on suspicious messages. |
| Anti-spam | Protect your organization's email from spam, including what actions to take if spam is detected |
| Anti-malware | Protect your organization's email from malware, including what actions to take and who to notify if malware is detected |
| Safe Attachments | Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams |
| Safe Links | Protect your users from opening and sharing malicious links in email messages and Office apps |

Rules

| | |
|---|---|
| Tenant Allow/Block Lists | Manage allow or block entries for your organization. |
| DKIM | Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users |
| Advanced delivery | Manage overrides for special system use cases. |
| Enhanced filtering | Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first |

Others

3. Click the Connection filter policy (Default) to edit the policy, then select the Edit connection filter policy in the drawer window to access the edit dialog:



Use this page to configure policies that are included in anti-spam protection. These policies include connection

| Name | Status |
|---|---|
| Anti-spam inbound policy (Default) | ● Always on |
| Connection filter policy (Default) | ● Always on |
| Anti-spam outbound policy (Default) | ● Always on |

**Connection filter policy (Default)**

● Always on | Priority Lowest

Description

Area 1 Security Policy

Edit name and description

Connection filtering

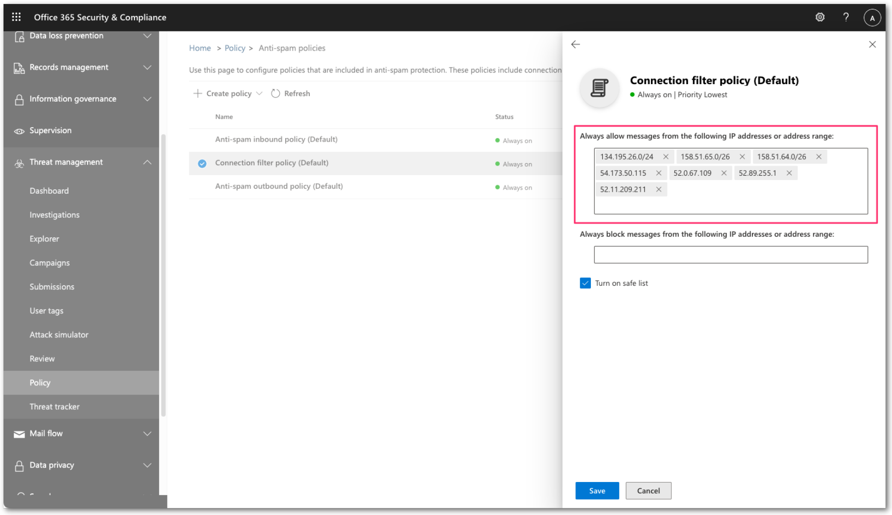
**IP Allow list**
Configured

**IP Block list**
Not configured

**Safe list**
● On

Edit connection filter policy

4. In the Always allow messages from the following IP addresses or address range section, add the following IP addresses and CIDR blocks.



Use this page to configure policies that are included in anti-spam protection. These policies include connection

| Name | Status |
|---|---|
| Anti-spam inbound policy (Default) | Always on |
| Connection filter policy (Default) | Always on |
| Anti-spam outbound policy (Default) | Always on |

**Connection filter policy (Default)**
Always on | Priority Lowest

Always allow messages from the following IP addresses or address range:
134.195.26.0/24 158.51.65.0/26 158.51.64.0/26 54.173.50.115 52.0.67.109 52.89.255.1 52.11.209.211

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

☑ Turn on safe list

- 52.11.209.211
- 52.89.255.11
- 52.0.67.109
- 54.173.50.115
- 158.51.64.0/26
- 158.51.65.0/26
- 134.195.26.0/24

If you are a European customer, you will need to add the additional IPs of our European datacenter to the exception list:

- 52.58.35.43
- 35.157.195.63

5. Once added, click **save** to save the configuration changes.

**Note:** Depending on your O365 configuration, you may receive a warning indicating that you need to run the **Enable-OrganizationCustomization** cmdlet before you create or modify objects in your Exchange Online organization.  Please follow the next step to enable this cmdlet.

Reference: https://docs.microsoft.com/en-us/powershell/module/exchange/enable-organizationcustomization for details on how to execute this cmdlet.

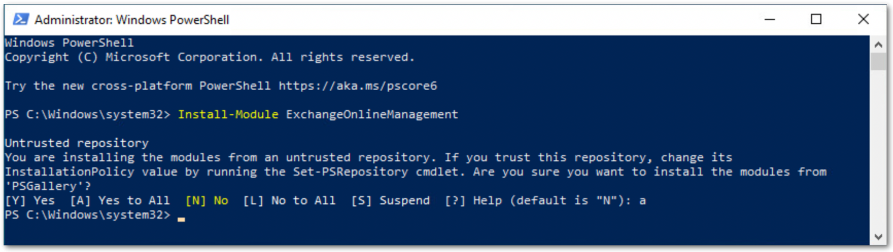
## Step 2: Execute Enable-OrganizationCustomization (if required)

The following steps are only required if you have not previously customized your O365 instance. In the previous step, if you received the message to run this cmdlet, you will need to execute it in order to proceed with the configuration.

1. Run PowerShell as administrator, execute the following command

   > **Install-Module ExchangeOnlineManagement**
   > Enter **Y** or **A** to allow the installation of the untrusted module.

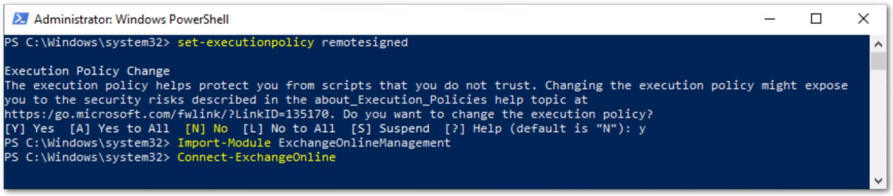
   Note: This module is a Microsoft module.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Install-Module ExchangeOnlineManagement

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): a
PS C:\Windows\system32> _
```

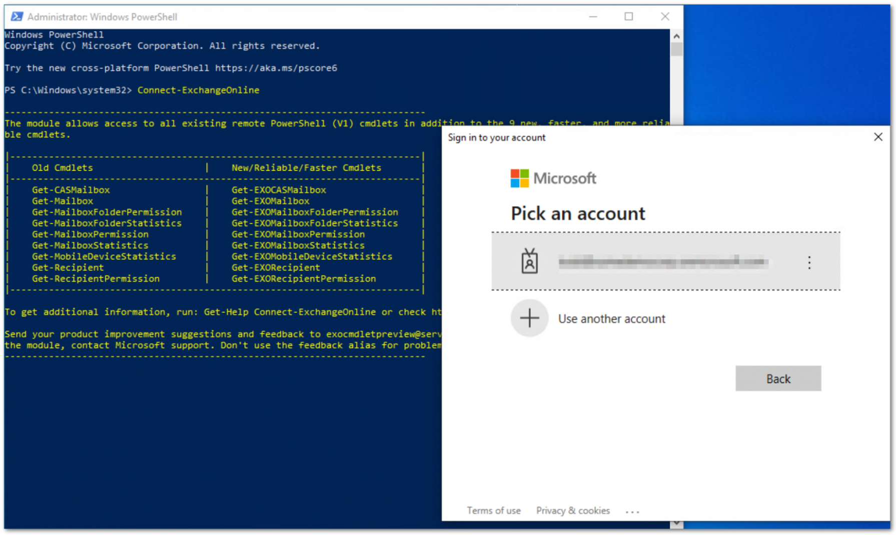
2. Execute the following commands to execute the policy change and connect to the O365 instance:

   > **set-executionpolicy remotesigned**
   > Enter **Y** or **A**, to confirm the change
   > **Import-Module ExchangeOnlineManagement**
   > Execute **Connect-ExchangeOnline**, to authenticate against your O365 instance



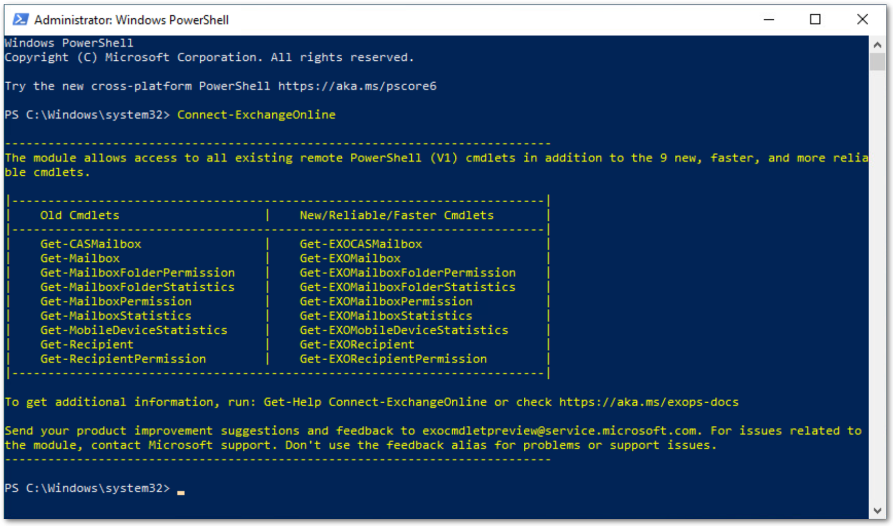
```
PS C:\Windows\system32> set-executionpolicy remotesigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
PS C:\Windows\system32> Import-Module ExchangeOnlineManagement
PS C:\Windows\system32> Connect-ExchangeOnline
```

3. The **Connect-ExchangeOnline** cmdlet will prompt you to login. Please login using an O365 administrator account:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Connect-ExchangeOnline

----------------------------------------------------------------------------
The module allows access to all existing remote PowerShell (V1) cmdlets in addition to the 9 new, faster, and more relia
ble cmdlets.

|--------------------------------------------------------------------------|
|    Old Cmdlets                    |    New/Reliable/Faster Cmdlets       |
|--------------------------------------------------------------------------|
|    Get-CASMailbox                 |    Get-EXOCASMailbox                 |
|    Get-Mailbox                    |    Get-EXOMailbox                    |
|    Get-MailboxFolderPermission    |    Get-EXOMailboxFolderPermission    |
|    Get-MailboxFolderStatistics    |    Get-EXOMailboxFolderStatistics    |
|    Get-MailboxPermission          |    Get-EXOMailboxPermission          |
|    Get-MailboxStatistics          |    Get-EXOMailboxStatistics          |
|    Get-MobileDeviceStatistics     |    Get-EXOMobileDeviceStatistics     |
|    Get-Recipient                  |    Get-EXORecipient                  |
|    Get-RecipientPermission        |    Get-EXORecipientPermission        |
|--------------------------------------------------------------------------|

To get additional information, run: Get-Help Connect-ExchangeOnline or check ht

Send your product improvement suggestions and feedback to exocmdletpreview@serv
the module, contact Microsoft support. Don't use the feedback alias for problem
----------------------------------------------------------------------------
```

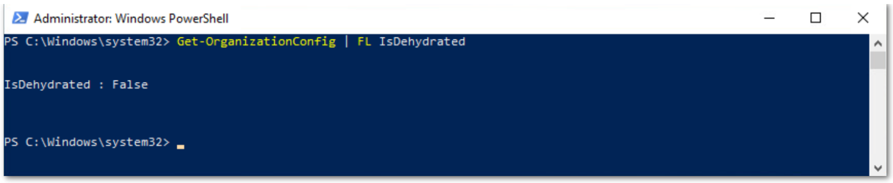
Once authenticated, you will be returned to the PowerShell prompt:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Connect-ExchangeOnline

----------------------------------------------------------------------------
The module allows access to all existing remote PowerShell (V1) cmdlets in addition to the 9 new, faster, and more relia
ble cmdlets.

|--------------------------------------------------------------------------|
|    Old Cmdlets                    |    New/Reliable/Faster Cmdlets       |
|--------------------------------------------------------------------------|
|    Get-CASMailbox                 |    Get-EXOCASMailbox                 |
|    Get-Mailbox                    |    Get-EXOMailbox                    |
|    Get-MailboxFolderPermission    |    Get-EXOMailboxFolderPermission    |
|    Get-MailboxFolderStatistics    |    Get-EXOMailboxFolderStatistics    |
|    Get-MailboxPermission          |    Get-EXOMailboxPermission          |
|    Get-MailboxStatistics          |    Get-EXOMailboxStatistics          |
|    Get-MobileDeviceStatistics     |    Get-EXOMobileDeviceStatistics     |
|    Get-Recipient                  |    Get-EXORecipient                  |
|    Get-RecipientPermission        |    Get-EXORecipientPermission        |
|--------------------------------------------------------------------------|

To get additional information, run: Get-Help Connect-ExchangeOnline or check https://aka.ms/exops-docs

Send your product improvement suggestions and feedback to exocmdletpreview@service.microsoft.com. For issues related to
the module, contact Microsoft support. Don't use the feedback alias for problems or support issues.
----------------------------------------------------------------------------

PS C:\Windows\system32> _
```

4. You can verify that the OrganizationCustomization is enabled by running the command:

   > **Get-OrganizationConfig | FL isDehydrated**

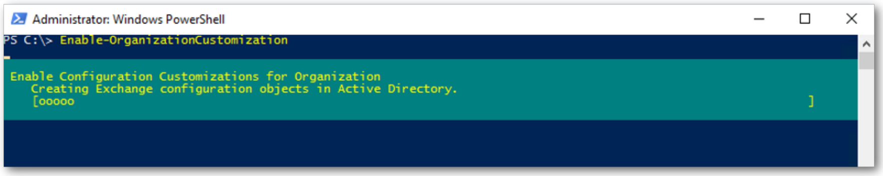


```
PS C:\Windows\system32> Get-OrganizationConfig | FL IsDehydrated

IsDehydrated : False

PS C:\Windows\system32> _
```

   If the result is **false** OrganizationCustomization is already enabled, no further actions are required.

5. If the result is **true**, then you will need to run the following command to enable the OrganizationCustomization:

   > **Enable-OrganizationCustomization**



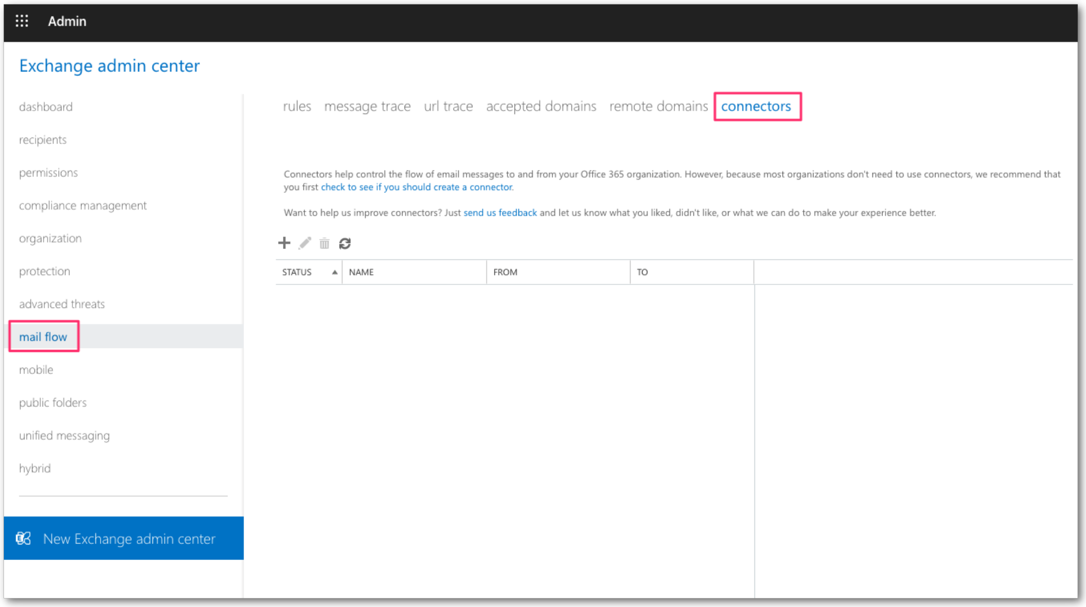
```
PS C:\> Enable-OrganizationCustomization

Enable Configuration Customizations for Organization
   Creating Exchange configuration objects in Active Directory.
   [ooooo                                                            ]
```

## Step 3: Enhanced Filtering Configuration

To configure the Enhanced Filtering function, this will allow O365 to properly identify the original connecting IP before the message was received by Area 1 to help with the SPF analysis.

You will first need to create an inbound connector.

1. From the Microsoft **Exchange admin center**, select the **mail flow** configuration pane and navigate to the **connectors** section of the configuration



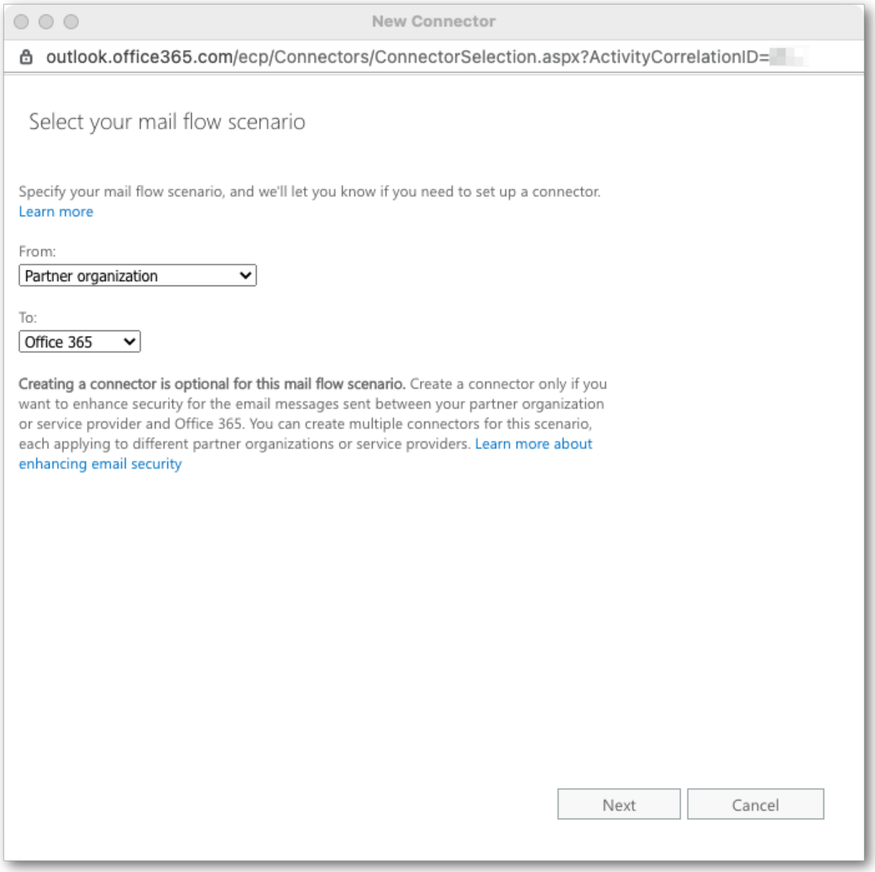
Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first check to see if you should create a connector.

Want to help us improve connectors? Just send us feedback and let us know what you liked, didn't like, or what we can do to make your experience better.

| STATUS ▲ | NAME | FROM | TO |
|---|---|---|---|

2. Click the **+** icon to configure a new connector. This will open a dialog to configure the new connector. In the **Select your mail flow scenario** panel, select:

    - In the "From" dropdown, select **Partner organization**
    - In the "To" dropdown, select **Office 365**



outlook.office365.com/ecp/Connectors/ConnectorSelection.aspx?ActivityCorrelationID=[redacted]

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.
Learn more

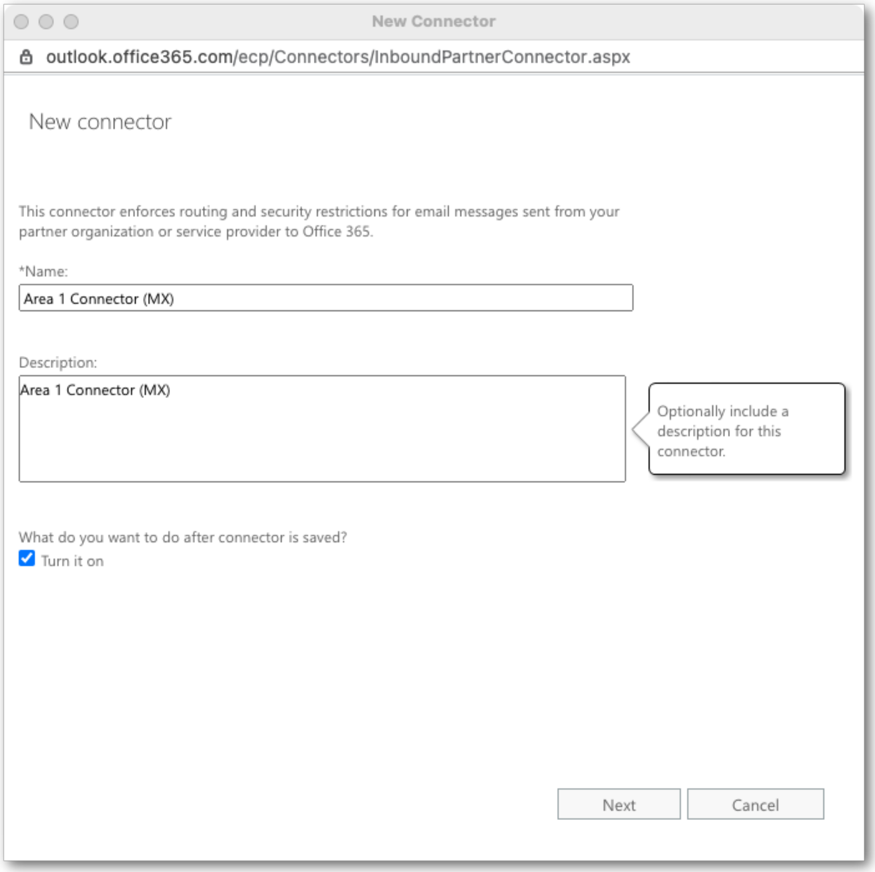
From:
Partner organization

To:
Office 365

**Creating a connector is optional for this mail flow scenario.** Create a connector only if you want to enhance security for the email messages sent between your partner organization or service provider and Office 365. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. Learn more about enhancing email security

Click the **Next** button to continue the configuration.

3. Provide a **Name** and a **Description** for the new connector. Leave the **Turn it on** checkbox enabled.



New Connector
outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx

New connector

This connector enforces routing and security restrictions for email messages sent from your partner organization or service provider to Office 365.

*Name: Area 1 Connector (MX)

Description: Area 1 Connector (MX)

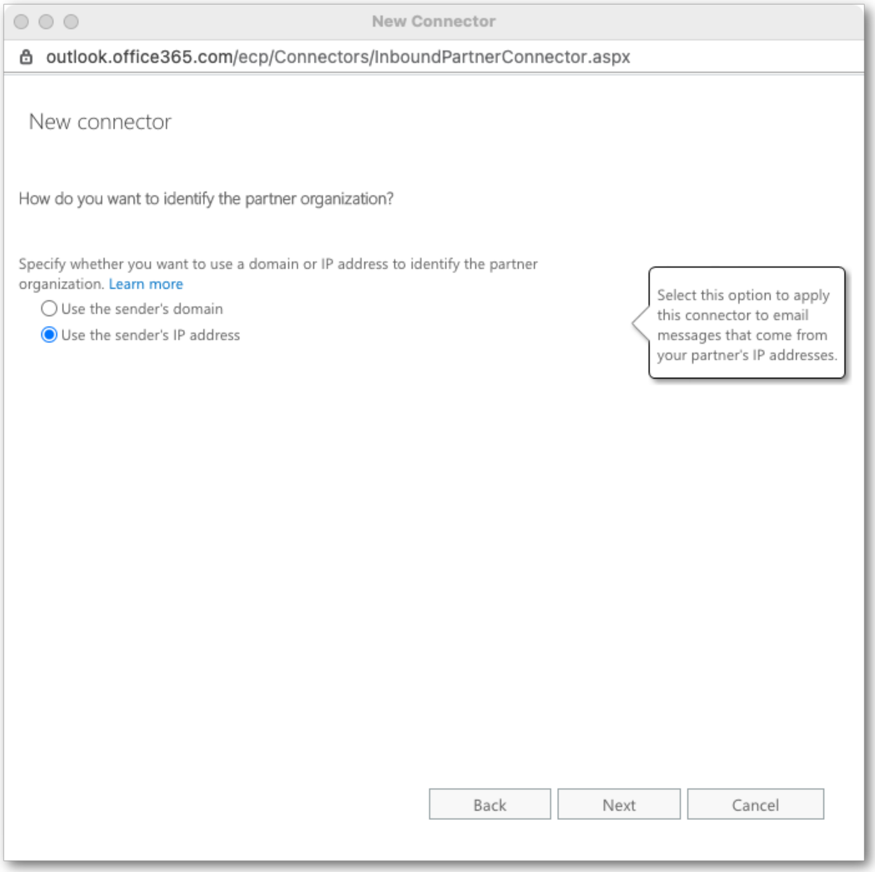
Optionally include a description for this connector.

What do you want to do after connector is saved?

☑ Turn it on

Click the **Next** button to continue the configuration.

4. In the **How do you want to identify the partner organization?** configuration panel, select **Use the sender’s IP address**:



New Connector
outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx

New connector

How do you want to identify the partner organization?

Specify whether you want to use a domain or IP address to identify the partner organization. Learn more

○ Use the sender's domain

● Use the sender's IP address

Select this option to apply this connector to email messages that come from your partner's IP addresses.

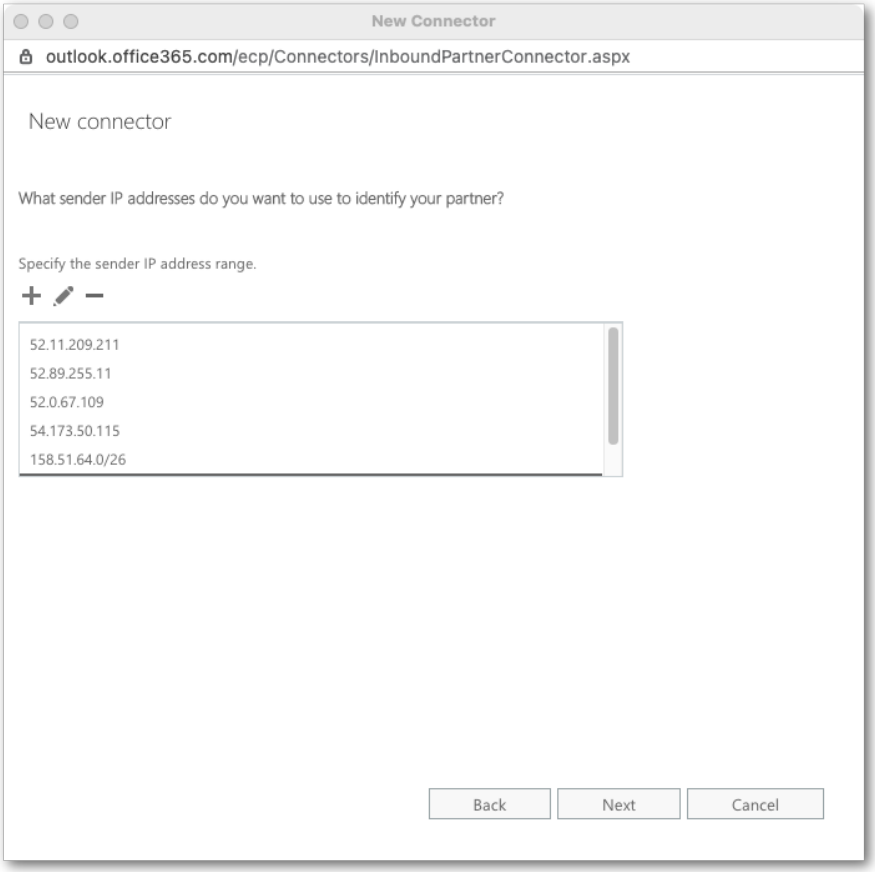
Click the **Next** button to continue the configuration.

5. In the **What sender IP addresses do you want to use to identify your partner?** configuration panel add the following IP addresses and CIDR blocks:

   - 52.11.209.211
   - 52.89.255.11
   - 52.0.67.109
   - 54.173.50.115
   - 158.51.64.0/26
   - 158.51.65.0/26
   - 134.195.26.0/24

   If you are a European customer, you will need to add the additional IPs of our European datacenter to the exception list:

   - 52.58.35.43
   - 35.157.195.63



New Connector
outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx
New connector

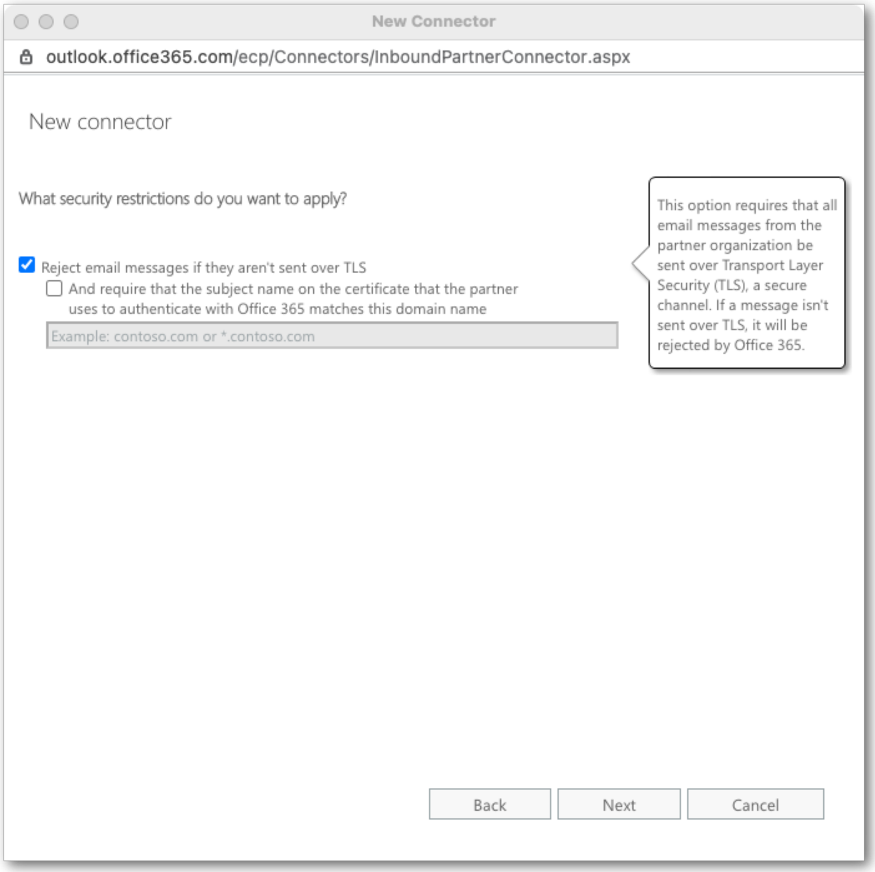
What sender IP addresses do you want to use to identify your partner?

Specify the sender IP address range.

52.11.209.211
52.89.255.11
52.0.67.109
54.173.50.115
158.51.64.0/26

Click the **Next** button to continue the configuration.

6. Keep the default TLS requirements (requiring TLS):



New Connector
outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx

New connector

What security restrictions do you want to apply?

☑ Reject email messages if they aren't sent over TLS

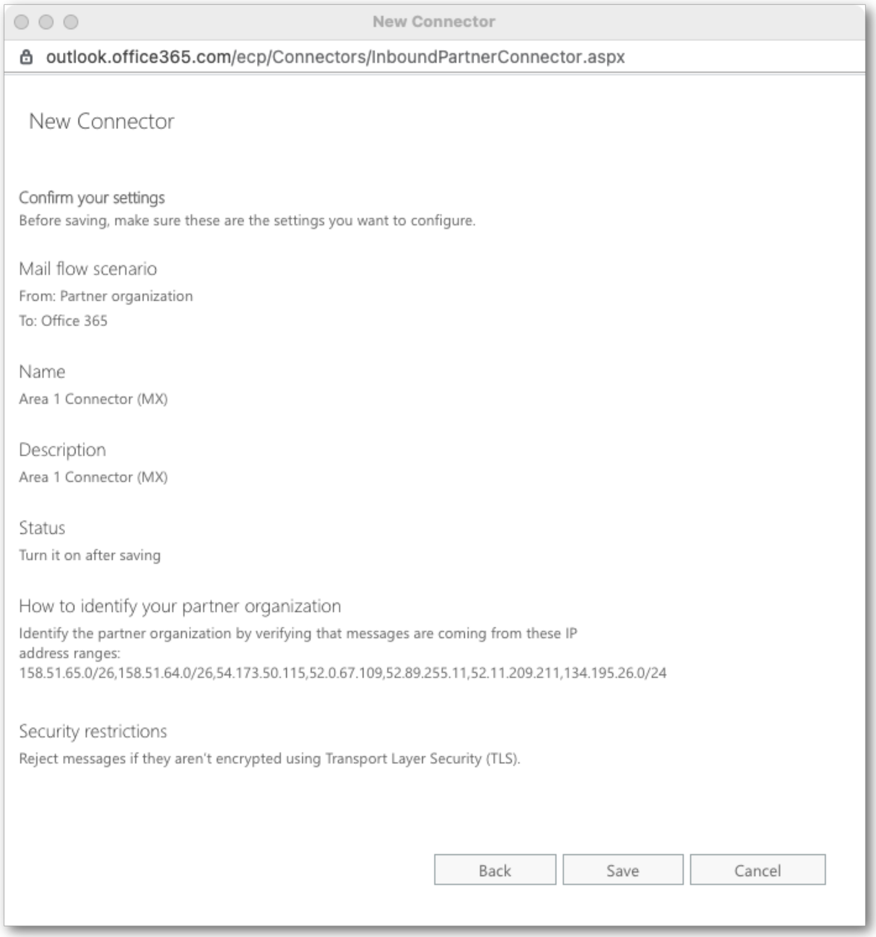
□ And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name

Example: contoso.com or *.contoso.com

This option requires that all email messages from the partner organization be sent over Transport Layer Security (TLS), a secure channel. If a message isn't sent over TLS, it will be rejected by Office 365.

Click the **Next** button to continue the configuration.

7. Confirm the connector configuration and click the **Save** button to save the configuration:



New Connector
outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx

New Connector

Confirm your settings

Before saving, make sure these are the settings you want to configure.

Mail flow scenario

From: Partner organization
To: Office 365

Name

Area 1 Connector (MX)

Description

Area 1 Connector (MX)

Status

Turn it on after saving

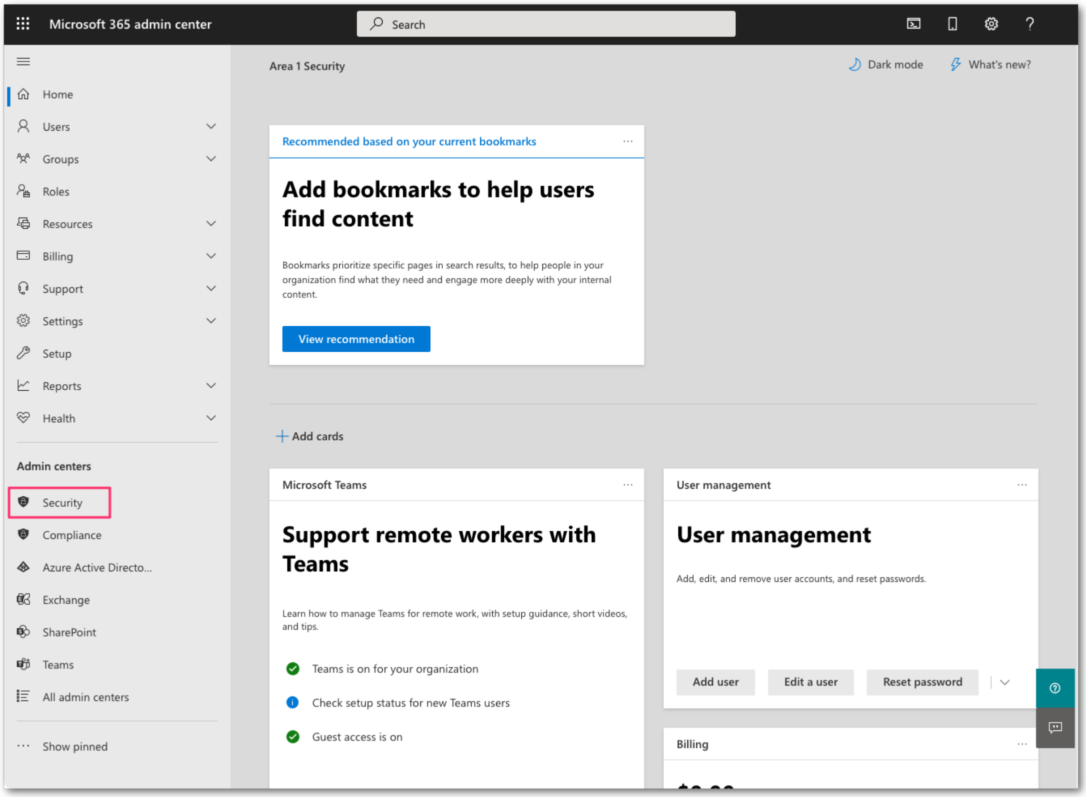
How to identify your partner organization

Identify the partner organization by verifying that messages are coming from these IP address ranges:
158.51.65.0/26,158.51.64.0/26,54.173.50.115,52.0.67.109,52.89.255.11,52.11.209.211,134.195.26.0/24

Security restrictions

Reject messages if they aren't encrypted using Transport Layer Security (TLS).

Now that the Inbound connector has been configured, you will need to enable the enhanced filtering configuration of the connector. Exit the **Exchange Admin** console and return to the main O365 Administration Console (https://admin.microsoft.com) and select the **Security admin** console (https://protection.office.com/homepage):



Add bookmarks to help users find content

Bookmarks prioritize specific pages in search results, to help people in your organization find what they need and engage more deeply with your internal content.

Support remote workers with Teams

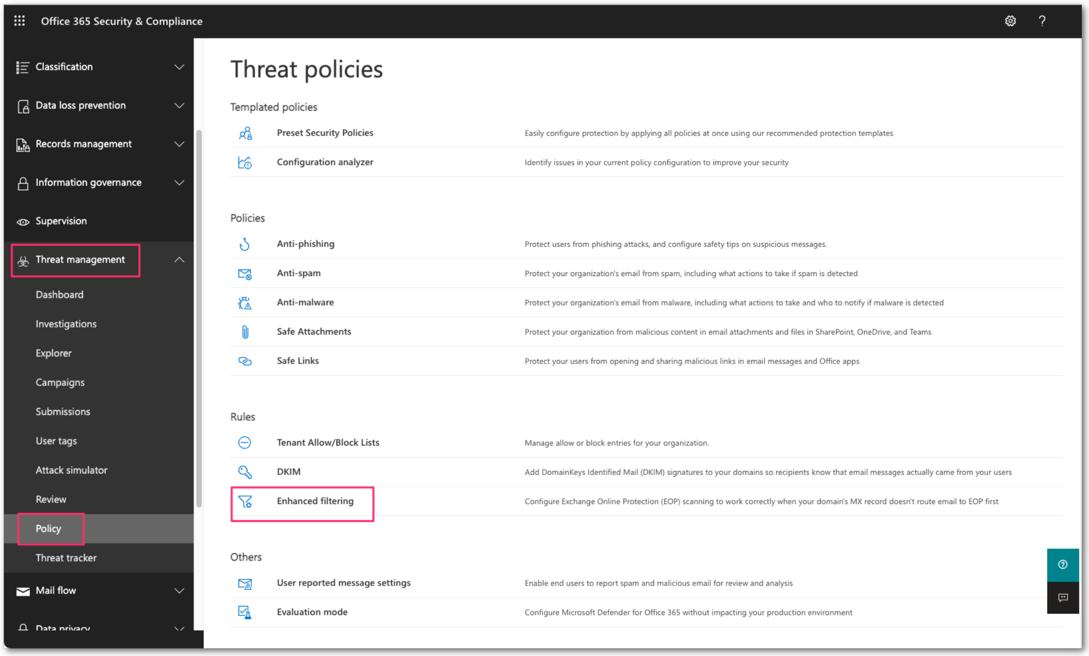
Learn how to manage Teams for remote work, with setup guidance, short videos, and tips.

- Teams is on for your organization
- Check setup status for new Teams users
- Guest access is on

User management

Add, edit, and remove user accounts, and reset passwords.

1. In the **Security Admin** console (https://protection.office.com/homepage), navigate to the **Threat Management** section and select the **Policy** option, then select the **Enhanced filtering** option:



Threat policies

Templated policies

| | |
|---|---|
| Preset Security Policies | Easily configure protection by applying all policies at once using our recommended protection templates |
| Configuration analyzer | Identify issues in your current policy configuration to improve your security |

Policies

| | |
|---|---|
| Anti-phishing | Protect users from phishing attacks, and configure safety tips on suspicious messages. |
| Anti-spam | Protect your organization's email from spam, including what actions to take if spam is detected |
| Anti-malware | Protect your organization's email from malware, including what actions to take and who to notify if malware is detected |
| Safe Attachments | Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams |
| Safe Links | Protect your users from opening and sharing malicious links in email messages and Office apps |

Rules

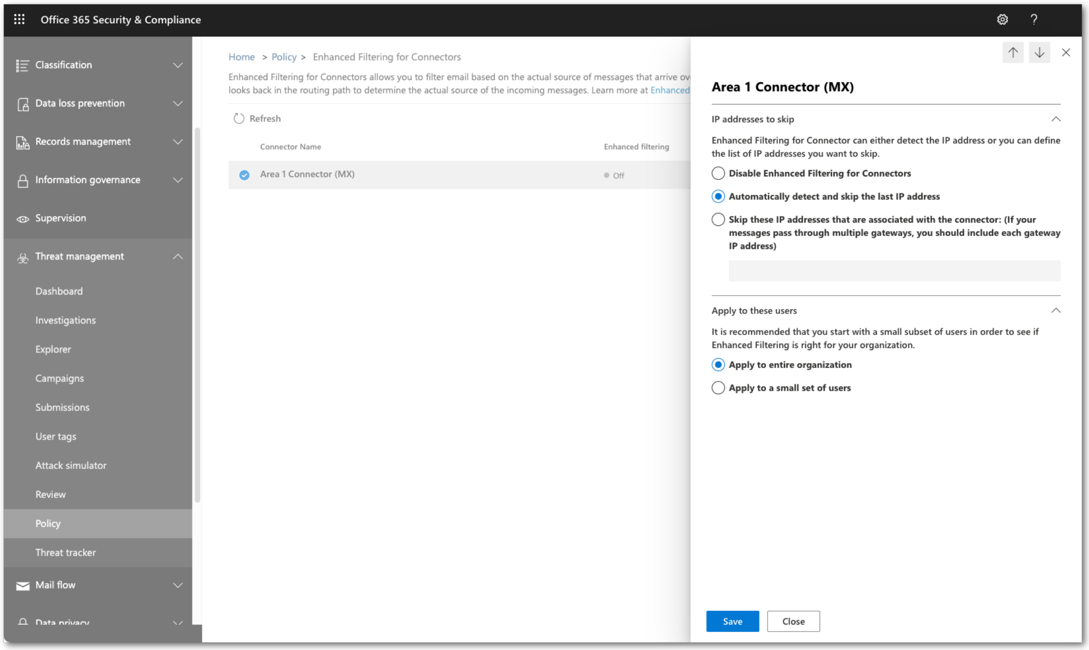
| | |
|---|---|
| Tenant Allow/Block Lists | Manage allow or block entries for your organization. |
| DKIM | Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users |
| Enhanced filtering | Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first |

Others

| | |
|---|---|
| User reported message settings | Enable end users to report spam and malicious email for review and analysis |
| Evaluation mode | Configure Microsoft Defender for Office 365 without impacting your production environment |

2. In the **Enhanced Filtering for Connectors** configuration panel, you will find the connector that was previously configured. Double click the connector to edit its configuration parameters.

    - Select **Automatically detect and skip the last IP address** option
    - Select **Apply to entire organization** option



Home > Policy > Enhanced Filtering for Connectors

Enhanced Filtering for Connectors allows you to filter email based on the actual source of messages that arrive ov
looks back in the routing path to determine the actual source of the incoming messages. Learn more at Enhanced

| Connector Name | Enhanced filtering |
|---|---|
| Area 1 Connector (MX) | Off |

**Area 1 Connector (MX)**

IP addresses to skip

Enhanced Filtering for Connector can either detect the IP address or you can define the list of IP addresses you want to skip.

○ Disable Enhanced Filtering for Connectors
● Automatically detect and skip the last IP address
○ Skip these IP addresses that are associated with the connector: (If your messages pass through multiple gateways, you should include each gateway IP address)

Apply to these users

It is recommended that you start with a small subset of users in order to see if Enhanced Filtering is right for your organization.

● Apply to entire organization
○ Apply to a small set of users

    - Click the **Save** button to activate the enhanced configuration

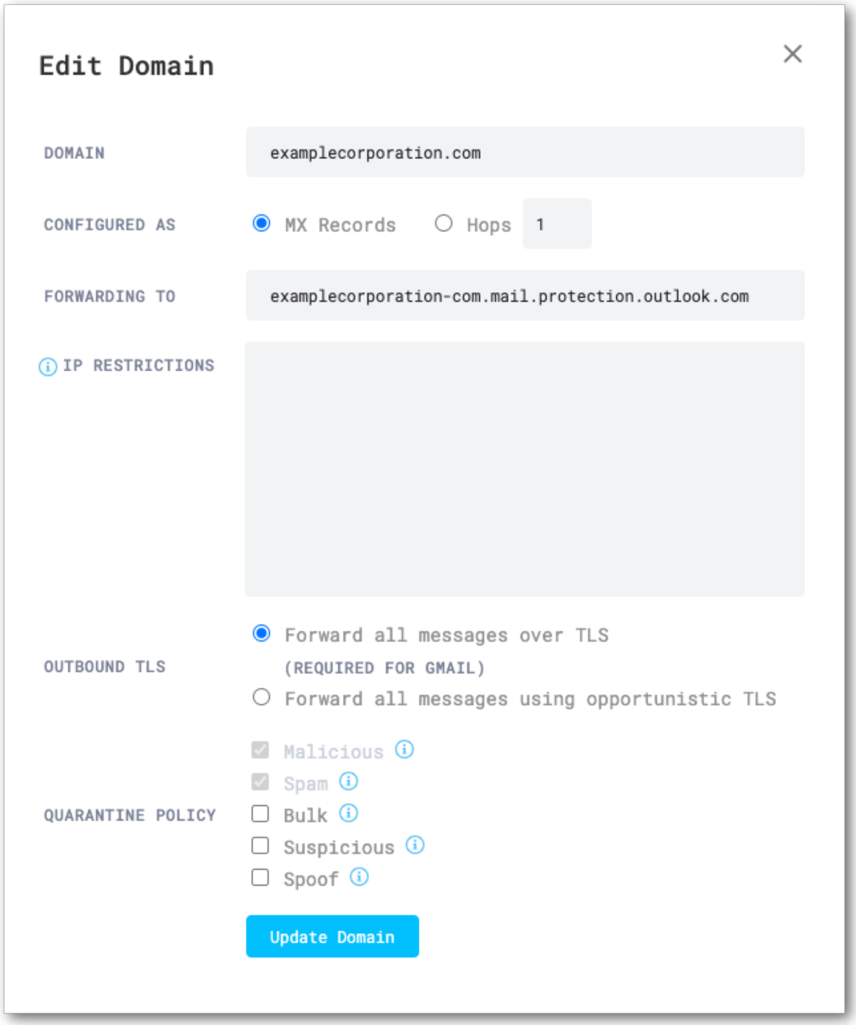
## Step 4: Configure Area 1 Quarantine Policies

*Selecting the disposition that you want to quarantine:*

- Quarantining messages is a per domain configuration. To modify which domains will have their message quarantines.  Access the domain configuration located under **Settings** > **Domains** and select the **...** icon on the right of the domain you'd like to modify.

  **Note:** When Area 1 is deployed as the MX record and protecting Office 365, Malicious and Spam detections will automatically be quarantined. This behavior cannot be modified.

- If you'd like  to quarantine additional dispositions, simply select the desired dispositions.

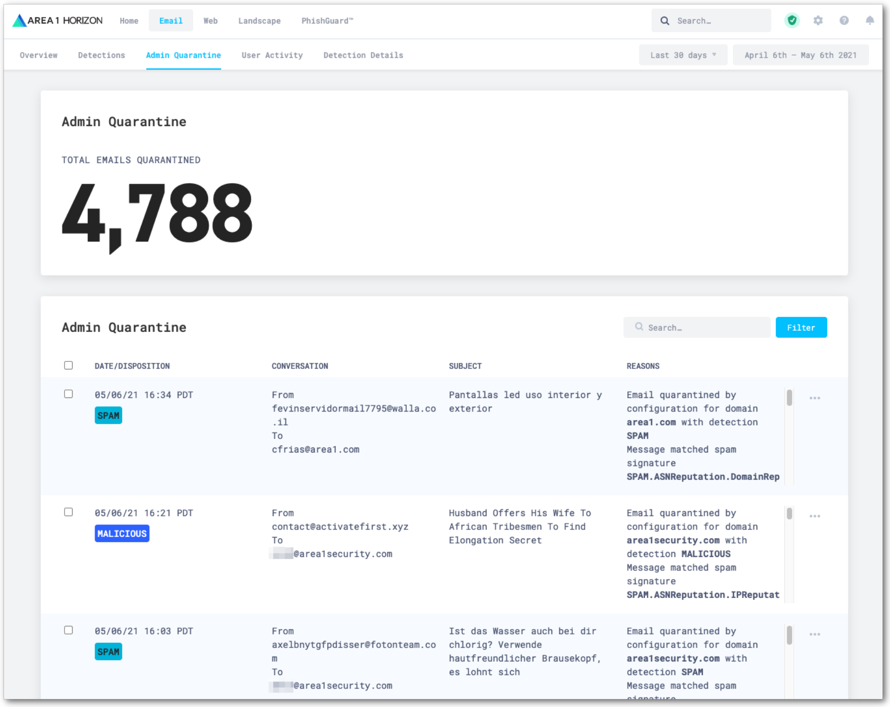


**Edit Domain**

| | |
|---|---|
| DOMAIN | examplecorporation.com |
| CONFIGURED AS | ● MX Records ○ Hops 1 |
| FORWARDING TO | examplecorporation-com.mail.protection.outlook.com |
| ⓘ IP RESTRICTIONS | |
| OUTBOUND TLS | ● Forward all messages over TLS (REQUIRED FOR GMAIL)<br>○ Forward all messages using opportunistic TLS |
| QUARANTINE POLICY | ☑ Malicious ⓘ<br>☑ Spam ⓘ<br>□ Bulk ⓘ<br>□ Suspicious ⓘ<br>□ Spoof ⓘ |

*Managing the Admin Quarantine:*

- To manage the quarantine, navigate to the Admin quarantine console, located under **Email** > **Admin Quarantine**.
- By clicking the **...** icon on the right of the messages, you'll be able to preview, download, or release the quarantined message.



Admin Quarantine

TOTAL EMAILS QUARANTINED

4,788

Admin Quarantine

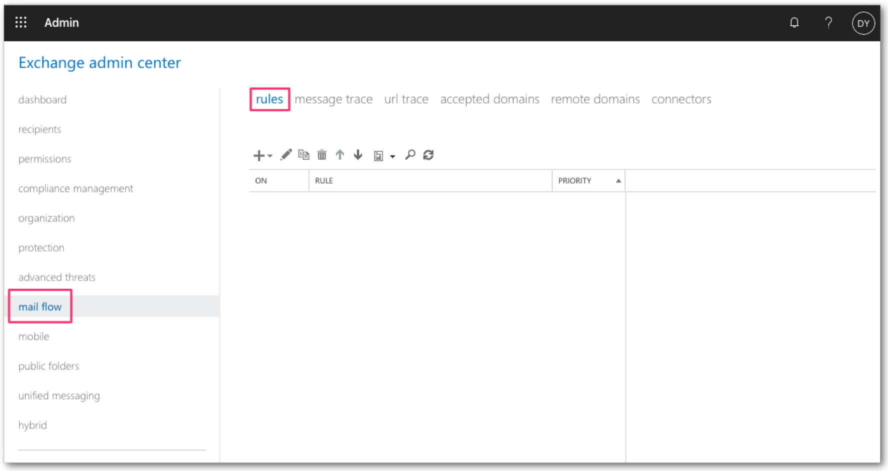
| □ | DATE/DISPOSITION | CONVERSATION | SUBJECT | REASONS |
|---|---|---|---|---|
| □ | 05/06/21 16:34 PDT<br>SPAM | From<br>fevinservidormail7795@walla.co.il<br>To<br>cfrias@area1.com | Pantallas led uso interior y exterior | Email quarantined by configuration for domain **area1.com** with detection **SPAM**<br>Message matched spam signature **SPAM.ASNReputation.DomainRep** |
| □ | 05/06/21 16:21 PDT<br>MALICIOUS | From<br>contact@activatefirst.xyz<br>To<br>[redacted]@area1security.com | Husband Offers His Wife To African Tribesmen To Find Elongation Secret | Email quarantined by configuration for domain **area1security.com** with detection **MALICIOUS**<br>Message matched spam signature **SPAM.ASNReputation.IPReputat** |
| □ | 05/06/21 16:03 PDT<br>SPAM | From<br>axelbnytgfpdisser@fotonteam.com<br>To<br>[redacted]@area1security.com | Ist das Wasser auch bei dir chlorig? Verwende hautfreundlicher Brausekopf, es lohnt sich | Email quarantined by configuration for domain **area1security.com** with detection **SPAM**<br>Message matched spam |

*Optional - Quarantining using the Microsoft Hosted Quarantine:*

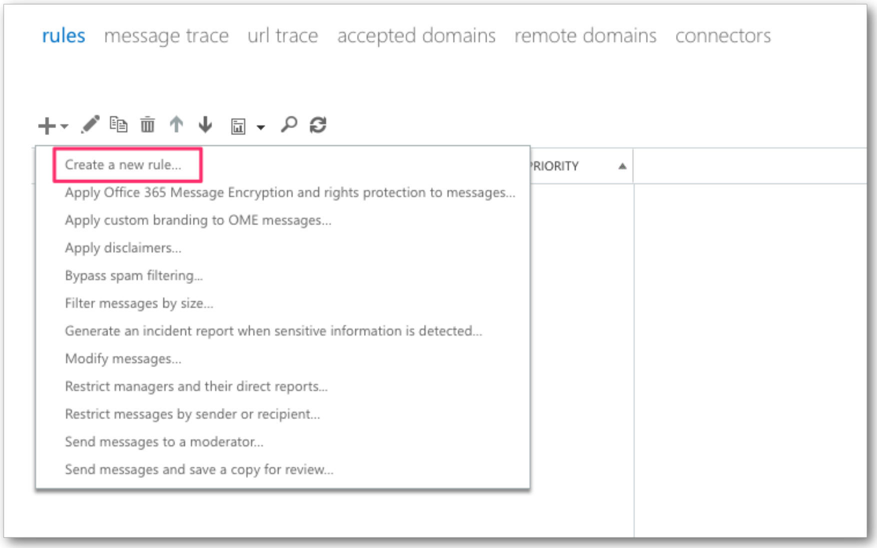
As previously noted, malicious and spam detections are automatically quarantined in Area 1's quarantine (this behavior cannot be modified). However, for the suspicious and spoof dispositions, you may prefer to apply a different behavior, where these messages can be quarantined into the Microsoft Hosted Quarantine or sent to the user's junk folder.

For this alternate behavior, you will need to configure a **transport rule** in Office 365:

1. From the **Exchange administrator** console, select the **rules** configuration in the **mail flow** configuration pane



2. Click the **+** button and select create a new rule


rules
message trace
url trace
accepted domains
remote domains
connectors
Create a new rule...
Apply Office 365 Message Encryption and rights protection to messages...
Apply custom branding to OME messages...
Apply disclaimers...
Bypass spam filtering...
Filter messages by size...
Generate an incident report when sensitive information is detected...
Modify messages...
Restrict managers and their direct reports...
Restrict messages by sender or recipient...
Send messages to a moderator...
Send messages and save a copy for review...
PRIORITY

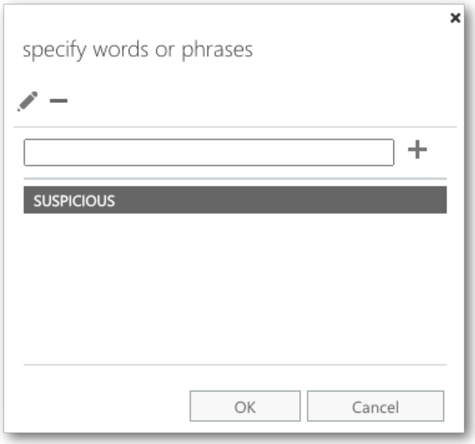
3. In the new rule dialog, click the **More options…** link at the bottom of the dialog box to get the advanced version of the rule creator. Set the following conditions and actions:

    - Name: **Quarantine Area 1 Suspicious Messages**
    - Configure the first condition, select **A message header … → includes any of these words**:

        Enter text: **X-Area1Security-Disposition**

        Enter words:

        **SUSPICIOUS**



specify words or phrases

SUSPICIOUS

**Note:** If you also want to quarantine the spoof detections, add the string SPOOF to the list of words.

- Click the **add** condition button to add a second condition.

  In the new condition, select **The sender...** → **IP address is in any of these ranges or exactly matches**.

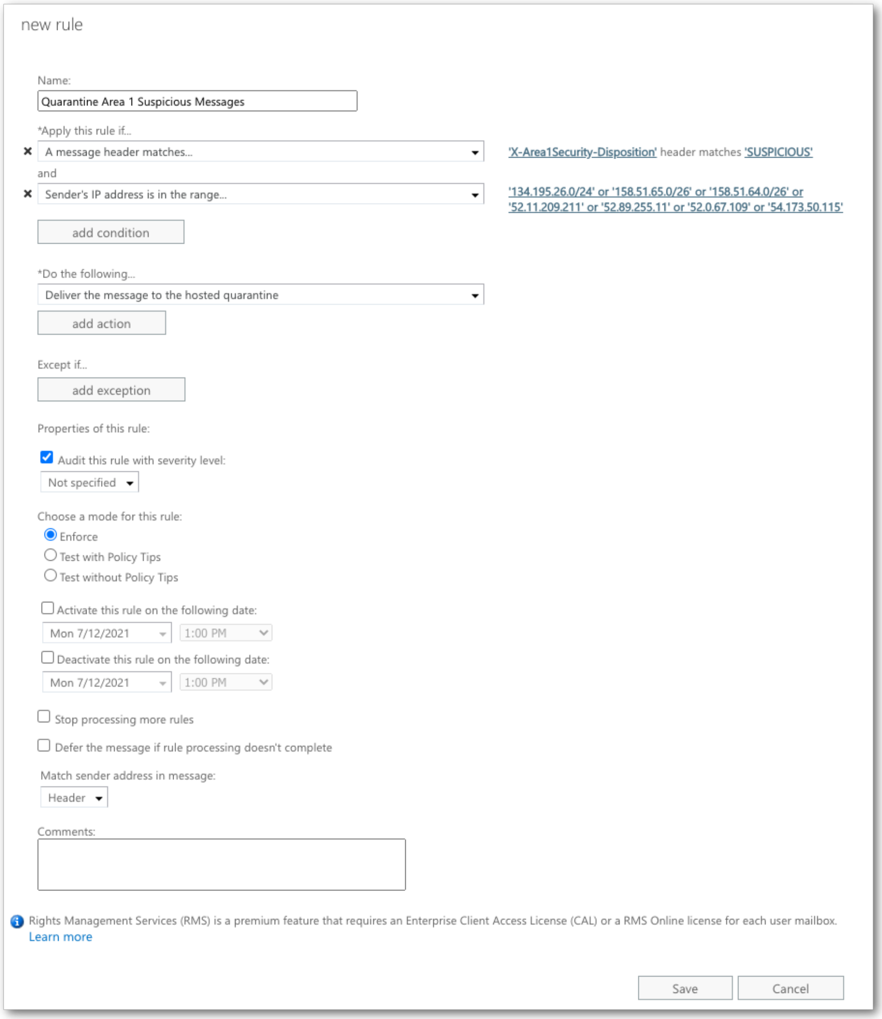
  If you are a US customer, enter the following four (6) IP addresses:

  - 52.11.209.211
  - 52.89.255.11
  - 52.0.67.109
  - 54.173.50.115
  - 158.51.64.0/26
  - 158.51.65.0/26
  - 134.195.26.0/24

  If you are a European customer, you will need to add the additional IPs of our European datacenter to the list:

  - 52.58.35.43
  - 35.157.195.63

- In the **Do the following…** section, select **Redirect the message to …** → **hosted quarantine**.



new rule

Name: Quarantine Area 1 Suspicious Messages

*Apply this rule if…

A message header matches… 'X-Area1Security-Disposition' header matches 'SUSPICIOUS'

and

Sender's IP address is in the range… '134.195.26.0/24' or '158.51.65.0/26' or '158.51.64.0/26' or '52.11.209.211' or '52.89.255.11' or '52.0.67.109' or '54.173.50.115'

*Do the following…

Deliver the message to the hosted quarantine

Except if…

Properties of this rule:

☑ Audit this rule with severity level: Not specified

Choose a mode for this rule:

● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date: Mon 7/12/2021 1:00 PM

□ Deactivate this rule on the following date: Mon 7/12/2021 1:00 PM

□ Stop processing more rules

□ Defer the message if rule processing doesn't complete

Match sender address in message: Header

Comments:

Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. Learn more

**Note:** If you prefer to send the message to the Junk folder, In the **Do the following…** section, select **Modify the message properties …** → **set the spam confidence level (SCL)**

Select the SCL value that will send the message to the junk folder, this behavior is dependent on the configured spam filter policies (spam and bulk actions).

- Click **Save** to save the new rule.

## Step 5: Update your domain MX records

Instructions to update your MX records will depend on the DNS provider you are using. You will want to update and replace your existing MX record with the Area 1 hosts.

Updated your domain MX records using Area 1:

| MX Priority | Host |
|---|---|
| 10 | mailstream-east.mxrecord.io |
| 10 | mailstream-west.mxrecord.io |
| 20 | mailstream-central.mxrecord.mx |

When configuring the Area 1 MX records, it’s important to configure both hosts with the same MX priority, this will allow mail flows to load balance between the hosts.

Once the MX change has been updated, the DNS updates may take up to 36 hours to fully propagate around the Internet. Some of the faster DNS providers will start to update records within minutes. DNS will reach the major DNS servers in about an hour.