

# 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

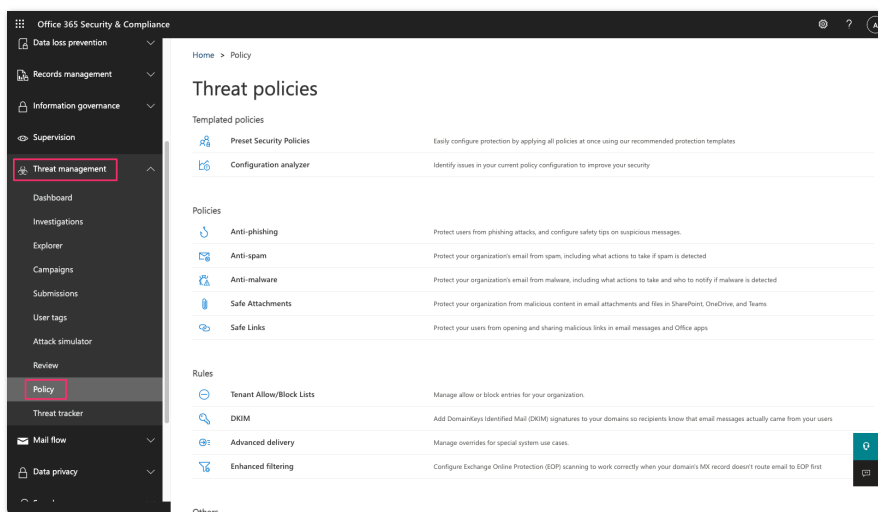


## Configuration Steps

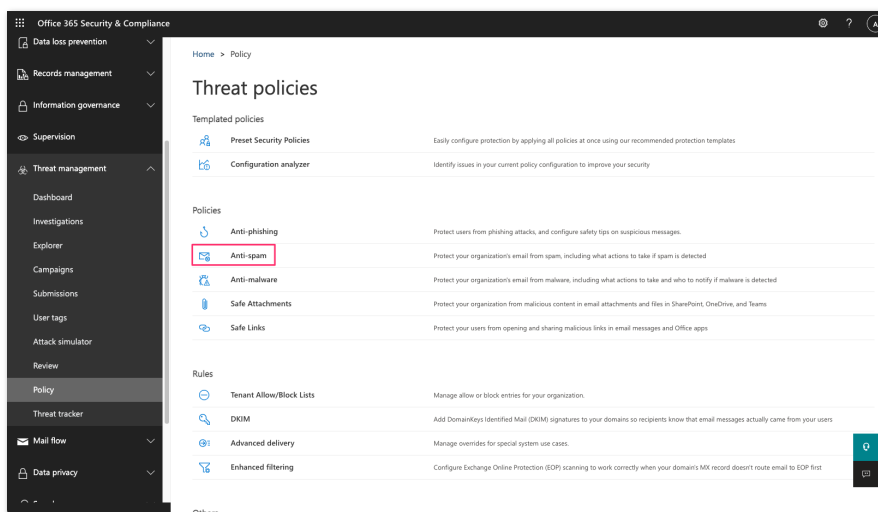
- Step 1: Add Area 1 IP addresses to Allow List
- Step 2: Execute O365 Enable-OrganizationCustomization (if required)
- Step 3: Enhanced Filtering Configuration
- Step 4: Configure Area 1 Quarantine Policies
- Step 5: Update your domain MX Records

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

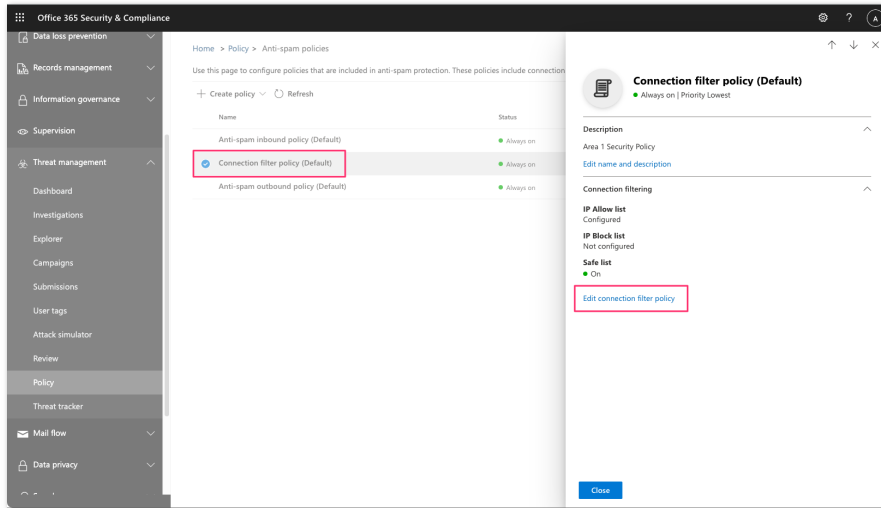
1. From the Microsoft Security admin center (<https://protection.office.com/homepage>), under the Threat management section, select the Policy settings (<https://protection.office.com/threatpolicy>):



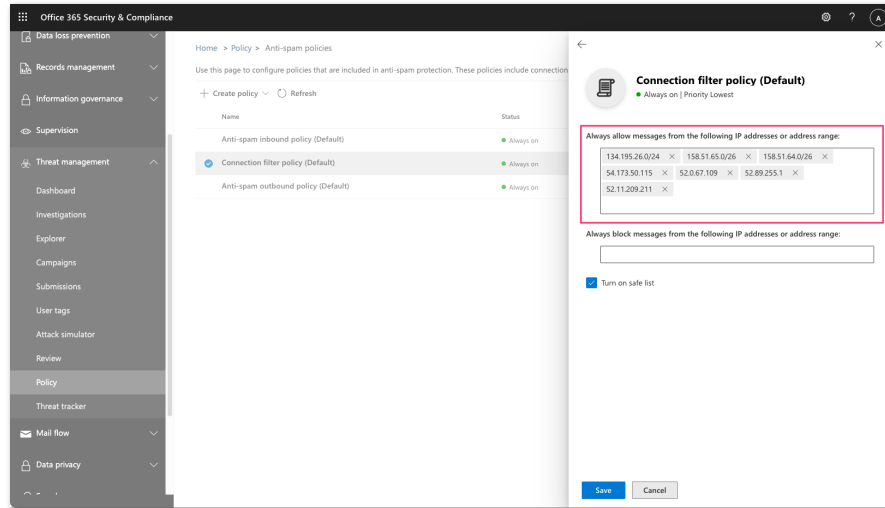
2. On the right configuration pane, select the Anti-spam option (<https://protection.office.com/antispam>):



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:



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



Egress IP's list can be found here:

<https://developers.cloudflare.com/email-security/deployment/inline/reference/egress-ips/>

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)

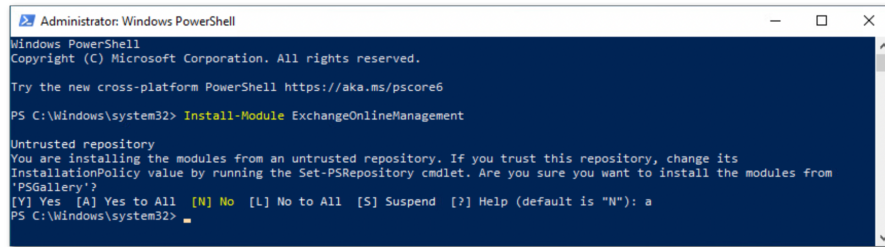
The following steps are only required if you have not previously customized your O365 instance. In the previous step, if you received the message to run this cmdlet, you will need to execute it in order to proceed with the configuration.

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.



```
Administrator: Windows PowerShell
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>
```

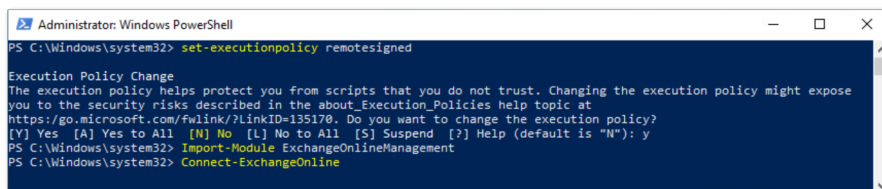
2. Execute the following commands to execute the policy change and connect to the O365 instance:

> **set-executionpolicy remotesigned**

> Enter **Y** or **A**, to confirm the change

> **Import-Module ExchangeOnlineManagement**

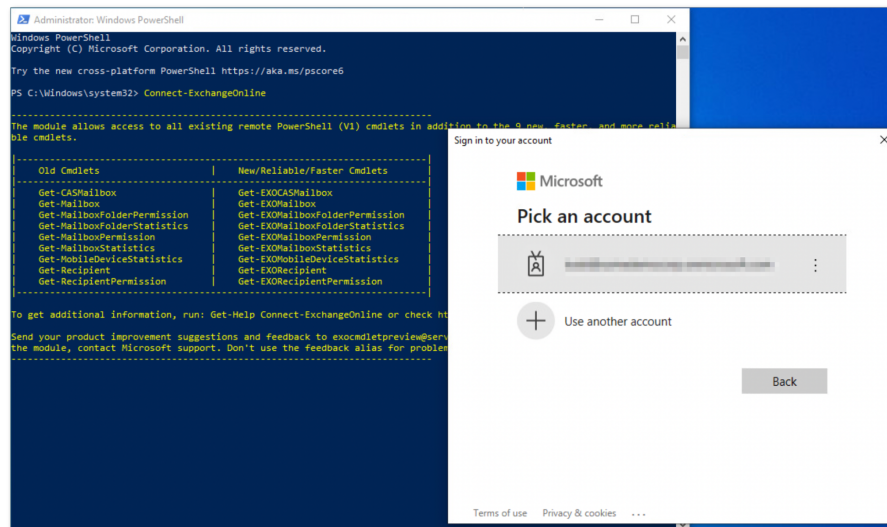
> Execute **Connect-ExchangeOnline**, to authenticate against your O365 instance



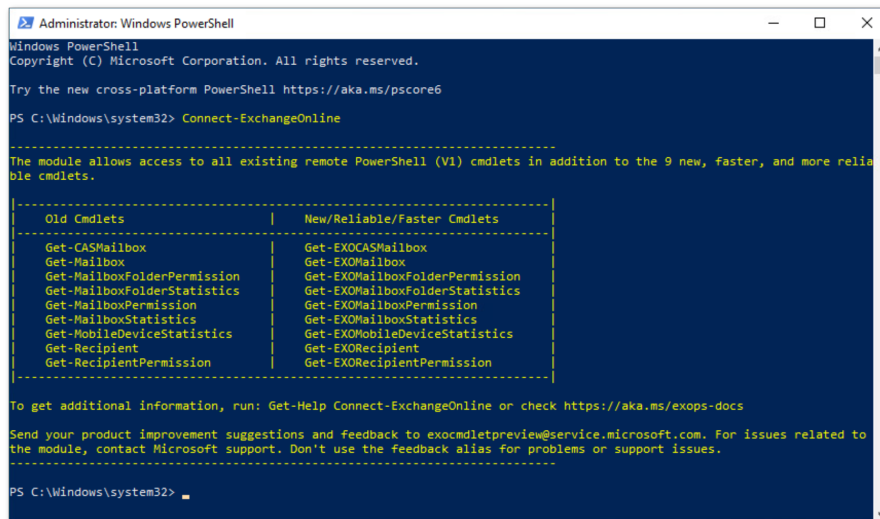
```
Administrator: Windows PowerShell
PS C:\Windows\system32> set-executionpolicy remotesigned

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:



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





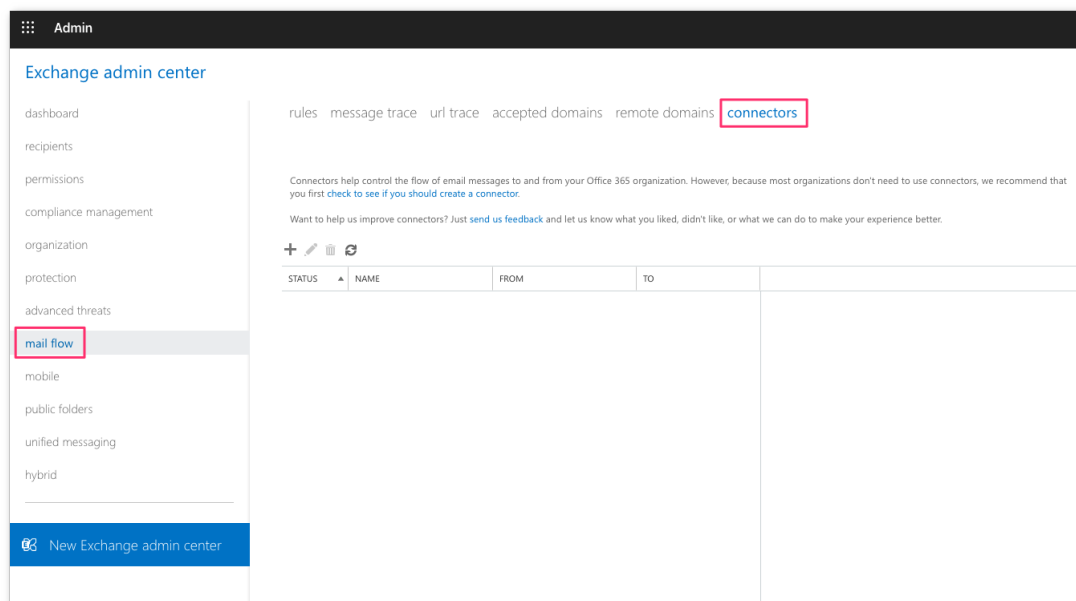


## Step 3: Enhanced Filtering Configuration

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



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**

New Connector

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

### 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](#)

Next Cancel

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

Next Cancel

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.

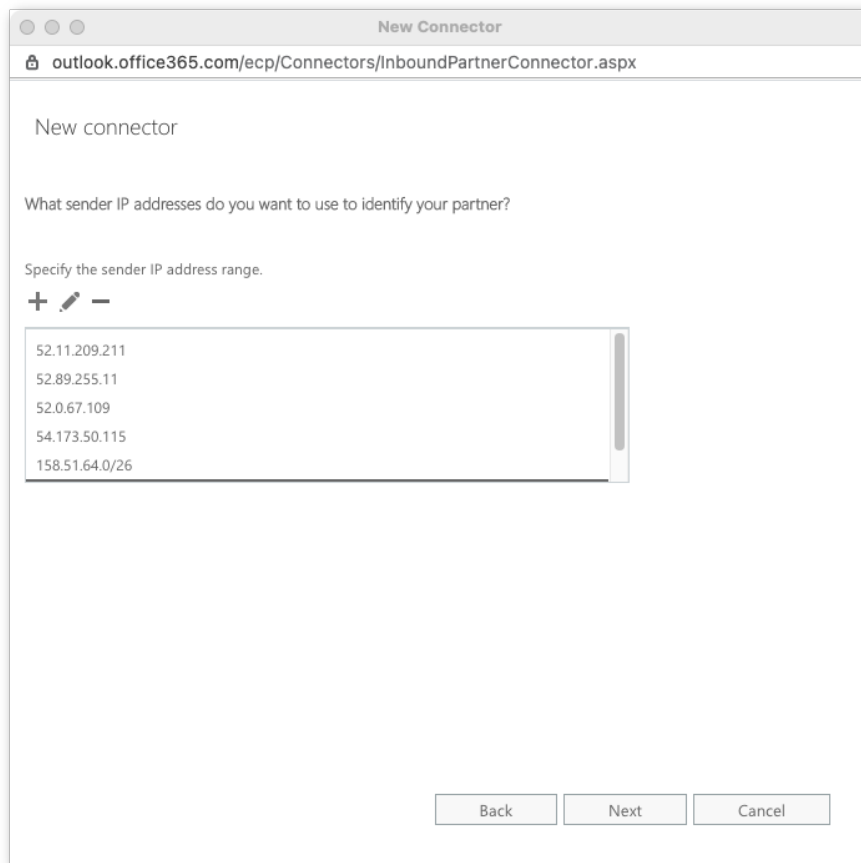
Back Next Cancel

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:

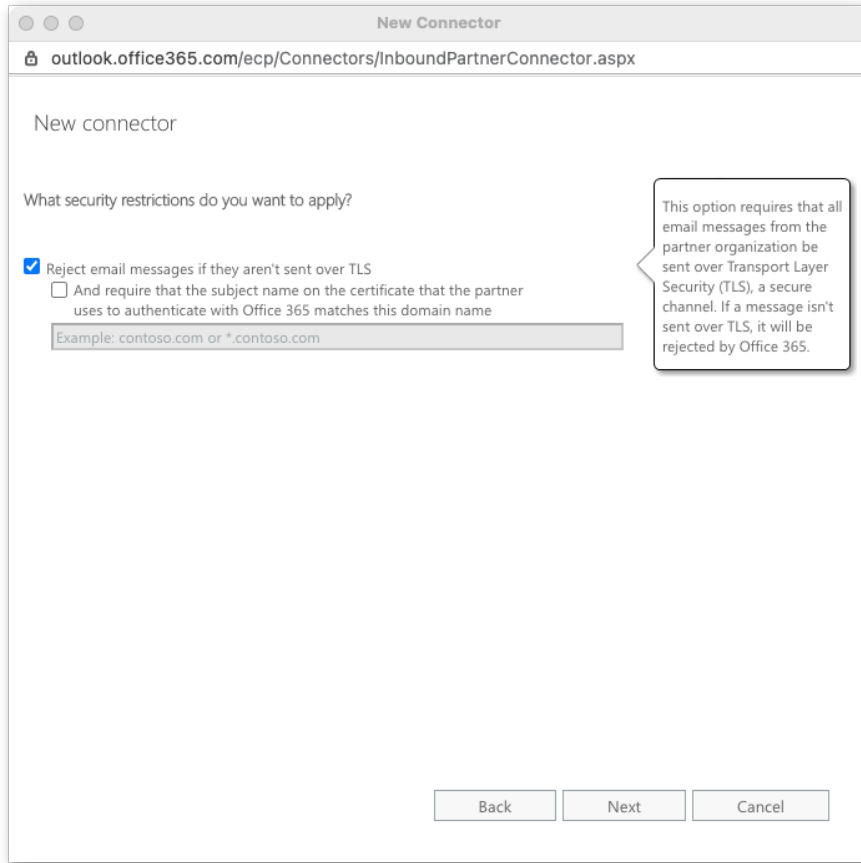
Egress IP's list can be found here:

<https://developers.cloudflare.com/email-security/deployment/inline/reference/egress-ips/>



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

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



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

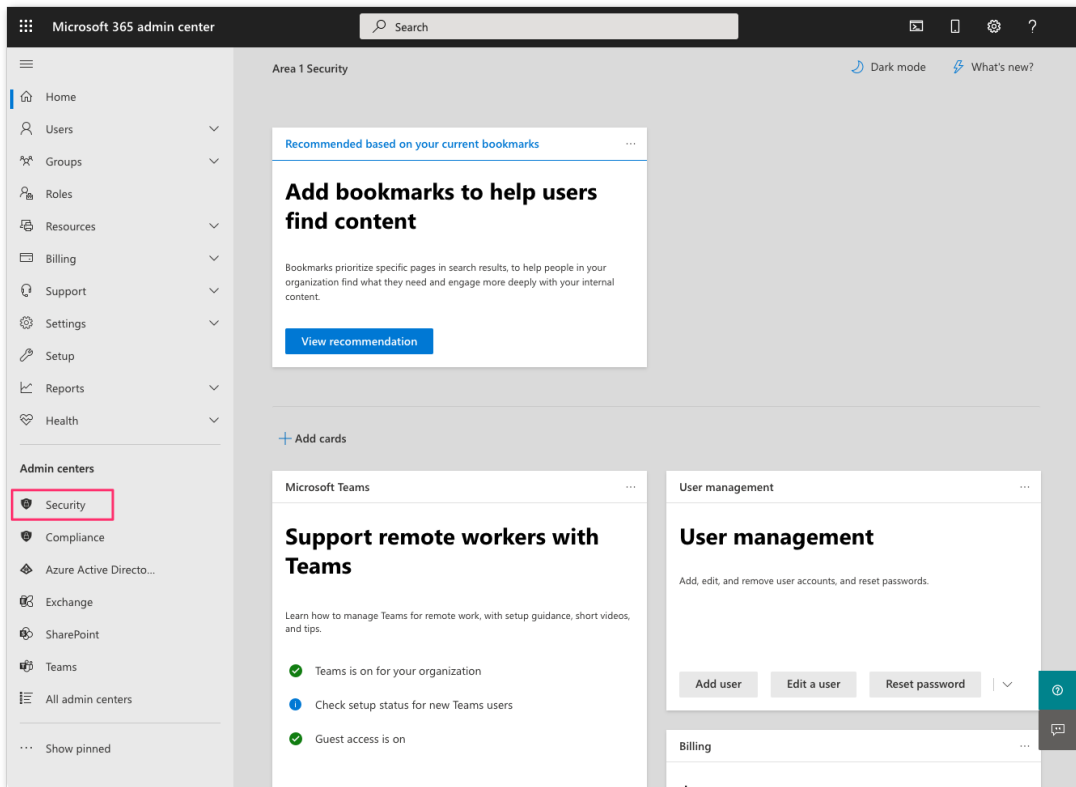
7. Confirm the connector configuration and click the **Save** button to save the configuration:

The screenshot shows a web browser window titled "New Connector" with the URL "outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx". The page content includes:

- 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).

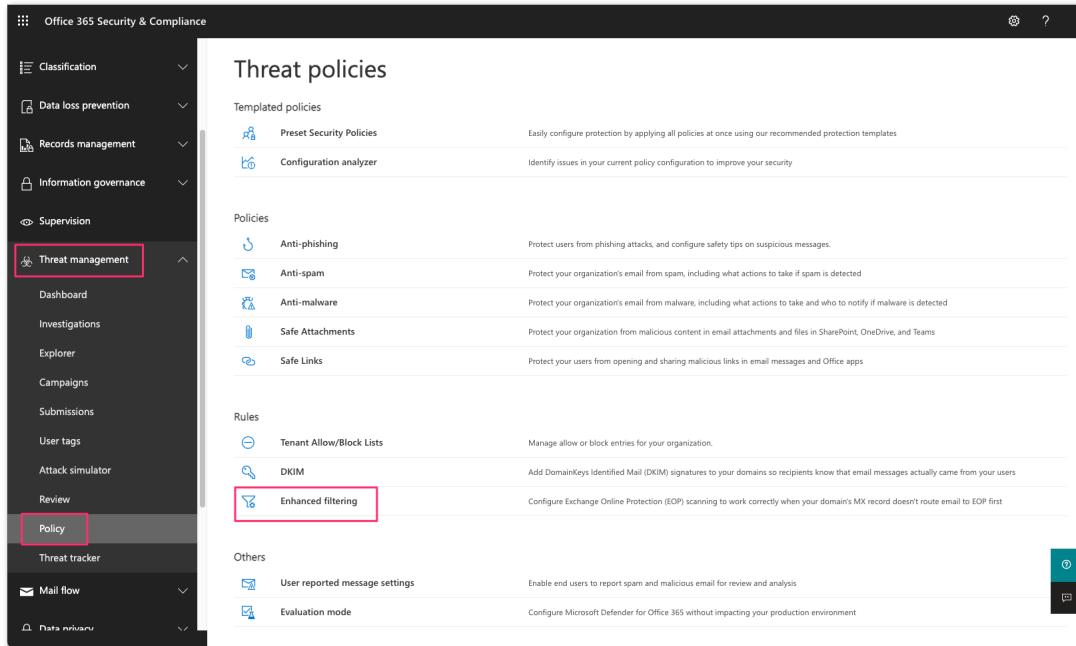
At the bottom right, there are three buttons: "Back", "Save", and "Cancel". The "Save" button is highlighted with a light blue background.

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>):



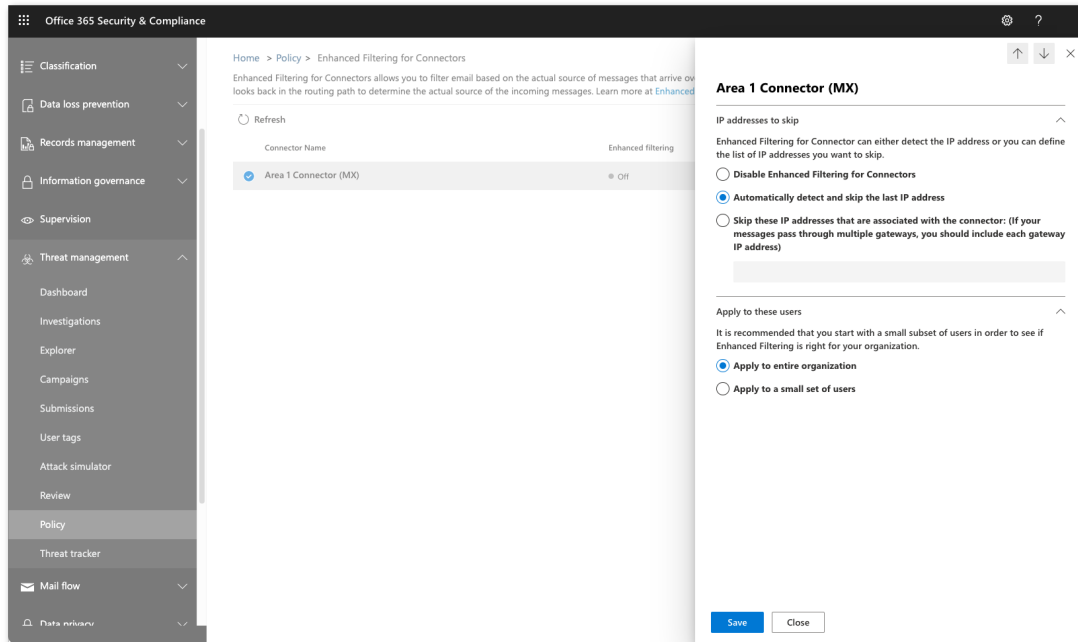


1. In the **Security Admin** console (<https://protection.office.com/homepage>), navigate to the **Threat Management** section and select the **Policy** option, then select the **Enhanced filtering** option:



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



- 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** [X]

DOMAIN: examplecorporation.com

CONFIGURED AS:  MX Records  Hops 1

FORWARDING TO: examplecorporation-com.mail.protection.outlook.com

IP RESTRICTIONS

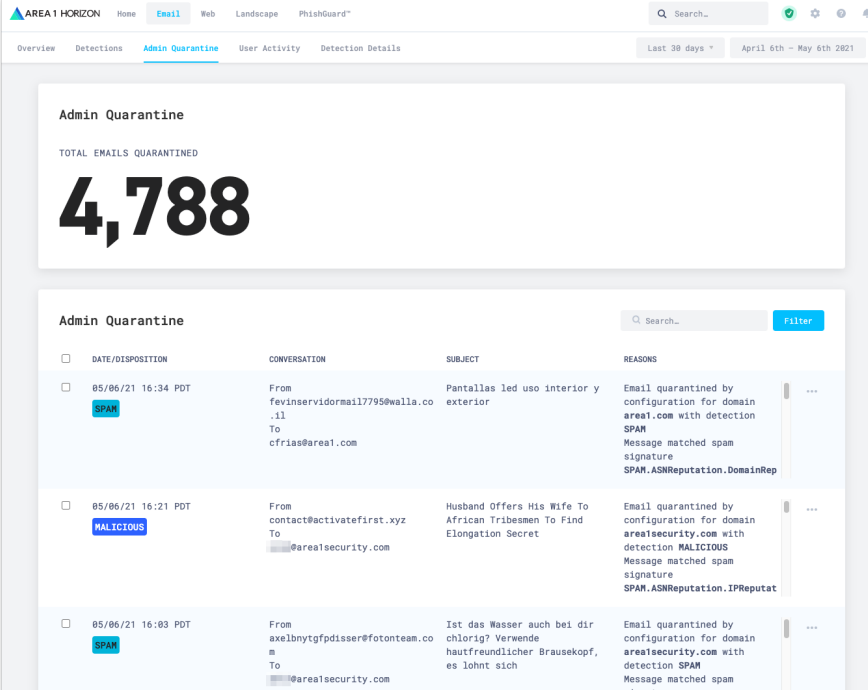
OUTBOUND TLS:  Forward all messages over TLS (REQUIRED FOR GMAIL)  Forward all messages using opportunistic TLS

QUARANTINE POLICY:  Malicious  Spam  Bulk  Suspicious  Spoof

[Update Domain]

## 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

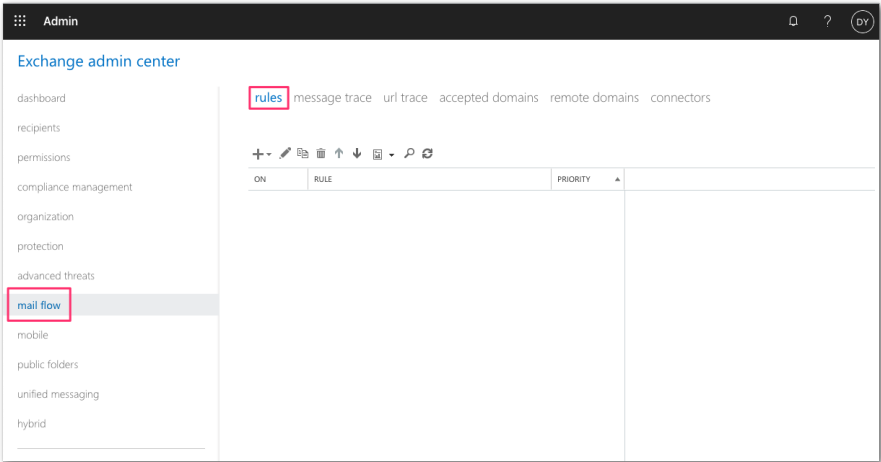
DATE/DISPOSITION	CONVERSATION	SUBJECT	REASONS	
<input type="checkbox"/> 05/06/21 16:34 PDT SPAM	From fevinservidormail17795@walla.co To cfrlas@area1.com	Pantallas led uso interior y exterior	Email quarantined by configuration for domain area1.com with detection SPAM Message matched spam signature SPAM, ASNReputation.DomainRep	...
<input type="checkbox"/> 05/06/21 16:21 PDT MALICIOUS	From contact@activatefirst.xyz To @area1security.com	Husband Offers His Wife To African Tribesmen To Find Elongation Secret	Email quarantined by configuration for domain area1security.com with detection MALICIOUS Message matched spam signature SPAM, ASNReputation.IPReputat	...
<input type="checkbox"/> 05/06/21 16:03 PDT SPAM	From axelbnytgpdisser@fotonteam.co To @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 Message matched spam signature	...

*Optional - Quarantining using the Microsoft Hosted Quarantine:*

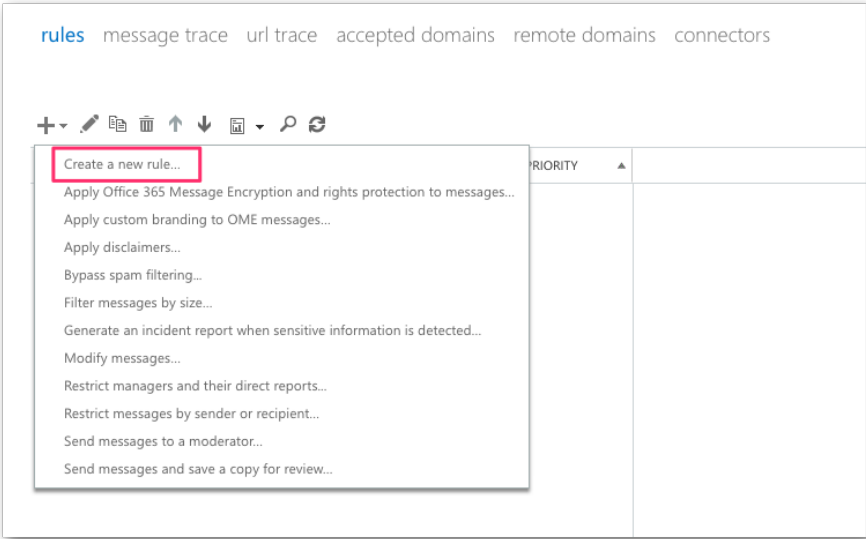
As previously noted, malicious and spam detections are automatically quarantined in Area 1's quarantine (this behavior cannot be modified). However, for the suspicious and spoof dispositions, you may prefer to apply a different behavior, where these messages can be quarantined into the Microsoft Hosted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



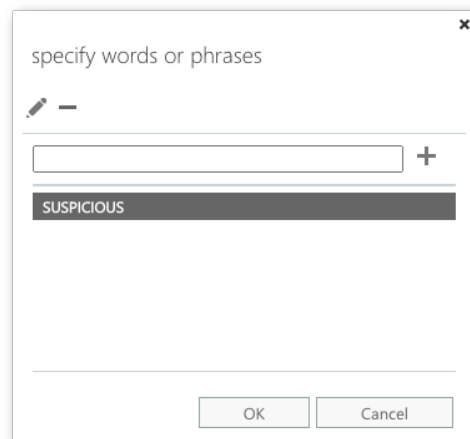
3. In the new rule dialog, click the **More options...** link at the bottom of the dialog box to get the advanced version of the rule creator. Set the following conditions and actions:

- 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**



**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**.

Egress IP's list can be found here:

<https://developers.cloudflare.com/email-security/deployment/inline/reference/egress-ips/>

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

new rule

Name:

\*Apply this rule if...

A message header matches...

and

Sender's IP address is in the range...

\*Do the following...

Except if...

Properties of this rule:

Audit this rule with severity level:

Choose a mode for this rule:

Enforce  
 Test with Policy Tips  
 Test without Policy Tips

Activate this rule on the following date:

Deactivate this rule on the following date:

Stop processing more rules

Defer the message if rule processing doesn't complete

Match sender address in message:

Comments:

[i](#) 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.