

# 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

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

	III Office 365 Service @ 2 🔎									
	Onice 365 Security & Con	nphance				0	1	Q		
Le	Data loss prevention	~	Home >	Policy						
Б	. Records management	$\sim$								
uuc			Thre	eat policies						
A	Information governance	$\sim$								
			Template	ed policies						
0	Supervision	1 I.	R	Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates					
<del>@</del>	, Threat management	~	<b>Ľ</b> 6	Configuration analyzer	Identify issues in your current policy configuration to improve your security					
-	Darbhaard									
	Dashboard		Policies							
	Investigations		5	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.					
	Explorer							-		
	Campaigns		28	Anti-spam	Protect your organization's email from spam, including what actions to take it spam is detected			_		
			CL.	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected					
	Submissions		0	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams					
	User tags		ø	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps					
	Attack simulator							-		
	Review									
	Policy		Rules							
	Toncy	-	Θ	Tenant Allow/Block Lists	Manage allow or block entries for your organization.					
	Threat tracker		9	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from you	r users				
2	Mail flow	~	⊕:	Advanced delivery	Manage overrides for special system use cases.			0		
A	Data privacy	$\sim$	76	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP f	irst	¢	2		
~										

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

III Office 365 Security & Co	mpliance			٩	) ? 🔿
🚡 Data loss prevention	~	Home >	Policy		
Records management	~	Thre	eat policies		
A Information governance	~	Template			
Supervision		Ra	Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates	
🔬 Threat management	~	£6	Configuration analyzer	Identify issues in your current policy configuration to improve your security	
Dashboard		De l'alter			
Investigations		Policies	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.	
Explorer			Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected	
Campaigns		a	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected	
Submissions		0	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams	
User tags		ବ୍ତ	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps	
Review		Rules			
		Θ	Tenant Allow/Block Lists	Manage allow or block entries for your organization.	
Threat tracker		9	DKIM	Add DomainKeys Identified Mail (DKM) signatures to your domains so recipients know that email messages actually came from your us	215
🔀 Mail flow	~	<b>0</b> 1	Advanced delivery	Manage overrides for special system use cases.	0
🛆 Data privacy	$\sim$	76	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first	æ
<u></u>		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:

III Office 365 Security & Con	npliance				۲	?	(A)
🔓 Data loss prevention	~	Home > Policy > Anti-snam policies			$\uparrow$	$\downarrow$	×
Records management	~	Use this page to configure policies that are included in anti-spam protection. These p	olicies include connection	Connection filter policy (Default)			
	~	$+$ Create policy $\vee$ $\circlearrowright$ Refresh		Always on   Priority Lowest			
		Name Anti-spam inbound policy (Default)	Always on	Description			~
	~	Connection filter policy (Default)	<ul> <li>Always on</li> </ul>	Area L Security Policy Edit name and description			
		Anti-spam outbound policy (Default)	<ul> <li>Always on</li> </ul>	Connection filtering			~
				IP Allow list Configured			
				IP Block list Not configured			
				Safe list			
				File annual file and a			
				East connection inter poincy			
🞽 Mail flow	~						
	~						
				Close			

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

::: Office 365 Security & Co	mpliance			@ ? A
Data loss prevention	~	Home > Policy > Anti-spam policies		$\leftarrow$ ×
Records management	~	Use this page to configure policies that are included in anti-spam pro-	otection. These policies include connection	Connection filter policy (Default)
A Information governance	$\sim$	$+$ Create policy $\vee$ () Refresh		Always on   Priority Lowest
- Commission		Name	Status	
C Supervision		Anti-spam inbound policy (Default)	<ul> <li>Always on</li> </ul>	Always allow messages from the following IP addresses or address range:
⊕ Threat management	~	<ul> <li>Connection filter policy (Default)</li> </ul>	<ul> <li>Always on</li> </ul>	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 ×
Dashboard		Anti-spam outbound policy (Default)	<ul> <li>Always on</li> </ul>	52.11.209.211 ×
Investigations				
Explorer				Always block messages from the following IP addresses or address range:
Campaigns				
Submissions				V Turn on safe list
User tags				
Attack simulator				
Review				
Policy				
Threat tracker				
Mail flow	~			
🔒 Data privacy	~			
<u></u>				Save Cancel

Egress IP's list can be found here:

https://developers.cloudflare.com/email-security/deployment/inline/reference/egre ss-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: <u>https://docs.microsoft.com/en-us/powershell/module/exchange/enable-orga</u> <u>nizationcustomization</u> 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.



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



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

Administrator: Windows PowerShell		- 🗆 ×	
Windows PowerShell Copyright (C) Microsoft Corporation.	All rights reserved.	<u>^</u>	
Try the new cross-platform PowerShel	- 1 https://aka.ms/pscore6		
PS C:\Windows\system32> Connect-Exch	angeOnline		
The module allows access to all exis ble cmdlets.	ting remote PowerShell (V1) cmdlets in a	ddition to the 9 new, faster, and more celia Sign in to your account	;
Old Cmdlets	New/Reliable/Faster Cmdlets	Microsoft	
Get-CASMailbox Get-Mailbox	Get-EXOCASMailbox Get-EXOMailbox		
Get-MailboxFolderPermission Get-MailboxFolderStatistics	Get-EXOMailboxFolderPermission Get-EXOMailboxFolderStatistics	Pick an account	
Get-MailboxPermission	Get-EXOMailboxPermission		
Get-MobileDeviceStatistics	Get-EXOMobileDeviceStatistics	<b>岗</b>	i inte
Get-RecipientPermission	Get-EXORecipientPermission		
Sand your product improvement sugger	tions and feedback to evocad stonewier	+ Use another account	
the module, contact Microsoft suppor	t. Don't use the feedback alias for prob	len	
			Deat
			васк
		Terms of use Privacy & cookies	
		· · · · · · · · · · · · · · · · · · ·	

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

C:\Wi	indows\system32> Connect-Excha	angeOnline			
e modu	ule allows access to all exist	ting remote PowerShell (V1) cmdlets ir	 addition to the 9 new, faster, a	nd more	re
e cmdl	lets.				
01d	d Cmdlets	New/Reliable/Faster Cmdlets			
Get	-CASMailbox	Get-EXOCASMailbox			
Get	-Mailbox	Get-EXOMailbox			
Get	-MailboxFolderPermission	Get-EXOMailboxFolderPermission			
Get	t-MailboxFolderStatistics	Get-EXOMailboxFolderStatistics			
Get	t-MailboxPermission	Get-EXOMailboxPermission			
Get	t-MailboxStatistics	Get-EXOMailboxStatistics			
Get	t-MobileDeviceStatistics	Get-EXOMobileDeviceStatistics			
C-+	-Recipient	Get-EXORecipient			
uet		Get-EXOPerinientPermission			

- 4. You can verify that the OrganizationCustomization is enabled by running the command:
  - > Get-OrganizationConfig | FL isDehydrated



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



# 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

::: Admin				
Exchange admin center				
dashboard	rules message trace url trace	accepted domains rem	note domains <b>conn</b>	ectors
recipients				
permissions	Connectors help control the flow of email mess you first check to see if you should create a cor	ages to and from your Office 365 on	organization. However, becau	se most organizations don't need to use connectors, we recommend that
compliance management	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.
organization	+ / 🖻 😂			
protection	STATUS 🔺 NAME	FROM	то	
advanced threats				
mail flow				
mobile				
public folders				
unified messaging				
hybrid				
🕅 New Exchange admin center				

- 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

entire and a state of the s	/ecp/Connectors/ConnectorSelection.aspx?ActivityCorrelationID=
Select your mail flow	scenario
Specify your mail flow scenario Learn more	and we'll let you know if you need to set up a connector.
From: Partner organization	v
To: Office 365	
Creating a connector is options want to enhance security for th or service provider and Office : each applying to different part enhancing email security	for this mail flow scenario. Create a connector only if you email messages sent between your partner organization 55. You can create multiple connectors for this scenario, er organizations or service providers. Learn more about
	Next Cancel

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

000	New Connector
a outlook.office365.cor	/ecp/Connectors/InboundPartnerConnector.aspx
New connector	
This connector enforces routing partner organization or service	and security restrictions for email messages sent from your rovider to Office 365.
Name:	
Area T Connector (MX)	
Description:	
Area 1 Connector (MX)	Optionally include a description for this connector.
What do you want to do after o 🖌 Turn it on	nnector is saved?
	Next Cancel

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



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/egre ss-ips/

outlook.office365.co	m/ecp/Connectors/InboundPartnerCo	onnector.aspx	
New connector			
/hat sender IP addresses do	you want to use to identify your partner?		
osify the conder ID address	F38.6.6		
	range.		
52.11.209.211			
52.0.67.109			
54.173.50.115			
158.51.64.0/26			
	Deek	Next	Cancel

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

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



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

000	New Connector
outlook.office365.com	/ecp/Connectors/InboundPartnerConnector.aspx
New Connector	
Confirm your settings	re the settings you want to configure
before saving, make sure these a	ne are settings you want to configure.
Mail flow scenario	
From: Partner organization	
IO. Office 565	
Name	
Area 1 Connector (MX)	
Description	
Area 1 Connector (MX)	
Status	
Turn it on after saving	
How to identify your partne	er 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 en	crypted using Transport Layer Security (TLS).
	Back Save Cancel
	Dack Save Califer

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 (<u>https://admin.microsoft.com</u>) and select the **Security admin** console (<u>https://protection.office.com/homepage</u>):



 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:

III Office 365 Security & Co	ompliance			i i	₿ ?
E Classification	~	Thr	eat policies		
Data loss prevention	~	Templat	ed policies		
Records management	~	Ra	Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates	
Information governance	$\sim$	Łô	Configuration analyzer	Identify issues in your current policy configuration to improve your security	
		Policies			
() Threat management		১	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.	
		2	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected	
Dashboard		K.	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected	
Investigations		0	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams	
Explorer		ନ୍ତ	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps	
Campaigns					
Submissions		Rules			
User tags		Θ	Tenant Allow/Block Lists	Manage allow or block entries for your organization.	
Attack simulator		9	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your user	s
Review		76	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first	
Policy					
Threat tracker		Others			0
📉 Mail flow	$\sim$	5	User reported message settings	Enable end users to report spam and malicious email for review and analysis	
Ω. Data privacy	~		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



• 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.



### 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.



### 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

III Admin					Q	? (DY
Exchange admin center						
dashboard	rules m	nessage trace url trace accepted domains	remote doma	ains connectors		
recipients						
permissions	+- 🖉 🛙					
compliance management	ON	RULE	PRIORITY A			
organization						
protection						
advanced threats						
mail flow						
mobile						
public folders						
unified messaging						
hybrid						

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

specify words o	or phrases	:
SUSPICIOUS		
	OK	Cancel

**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...  $\rightarrow$  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/referenc e/egress-ips/ • In the **Do the following...** section, select **Redirect the message to ...** → hosted quarantine.

ne	w rule			
	Name:			
	Quarantine Area 1 Suspicious Messages			
	*Apply this rule if			
×	A message header matches	'X-Area1Security-Disposit	on' header matche	s <u>'SUSPICIOUS'</u>
	and			
×	Sender's IP address is in the range	'134.195.26.0/24' or '158.5 '52.11.209.211' or '52.89.2	1.65.0/26' or '158.5 55.11' or '52.0.67.1	i <u>1.64.0/26' or</u> )9' or '54.173.50.115'
	add condition			
	*Do the following			
	Deliver the message to the hosted quarantine			
	add action			
	Evcent if			
	add execution			
	add exception			
	Properties of this rule:			
	Audit this rule with severity level:			
	Not specified 👻			
	Chanse a mode for this rule:			
	Enforce			
	○ Test with Policy Tips			
	O Test without Policy Tips			
	Activate this rule on the following date:			
	Mon 7/12/2021 V 1:00 PM V			
	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:			
B R	ghts Management Services (RMS) is a premium feature that requires an Enterprise Client . earn more	Access License (CAL) or a RM	S Online license for	each user mailbox.
			-	
			Save	Cancel

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.