CLOUDFLARE
AREA 1 SECURITY

POV Guide for Microsoft Exchange

Bcc Mode

Cloudflare Area 1 Overview

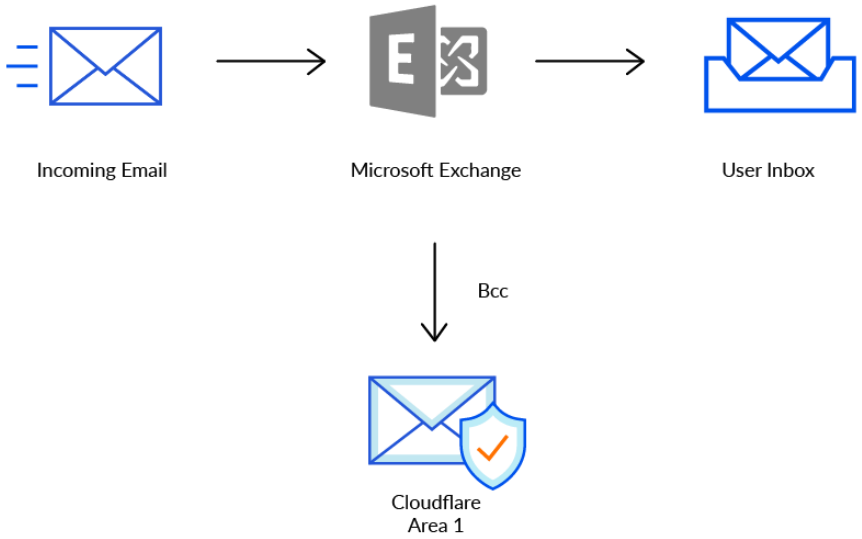
Phishing is the root cause of upwards of 90% of security breaches that lead to financial loss and brand damage. Cloudflare Area 1 is a cloud-native service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors and comprehensive attack analytics, Area 1 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.

POV Configuration

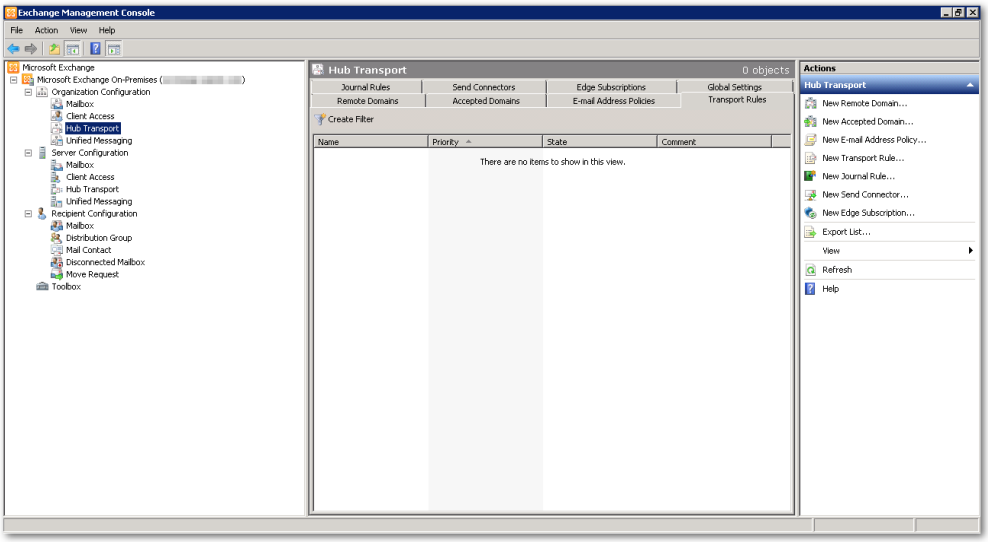
For customers using Microsoft Exchange, doing a Bcc POV with Area 1 for detecting phishing emails is quick and easy to setup as detailed below.

Email Flow During POV

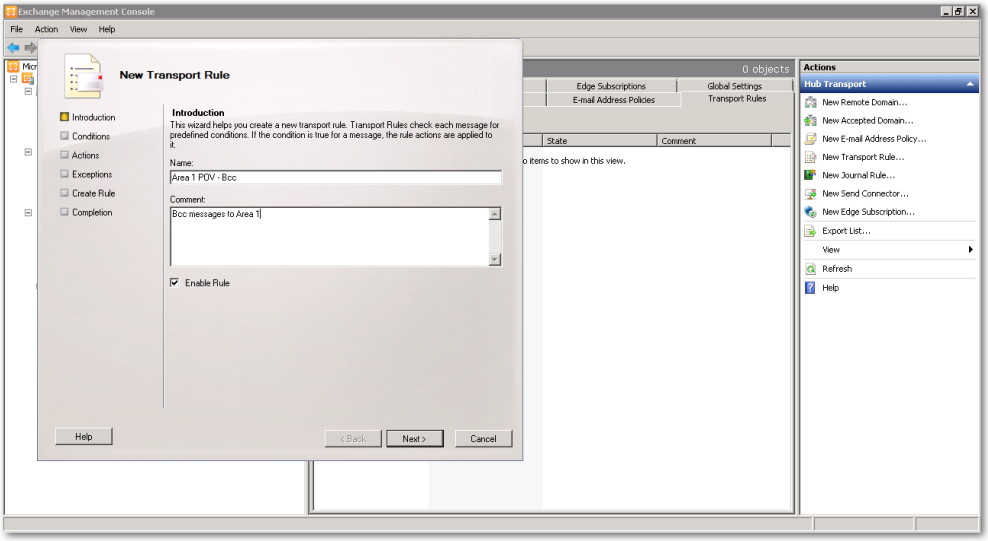


Configure Inbound Rule to Bcc to Area 1

To configure the rule to Bcc the inbound messages to Area 1, Access the Exchange Management Console, select the **Hub Transport** option under the **Organization Configuration**. Select **New Transport Rule…** on the right **Actions** pane to start the configuration of the **Transport Rule**.

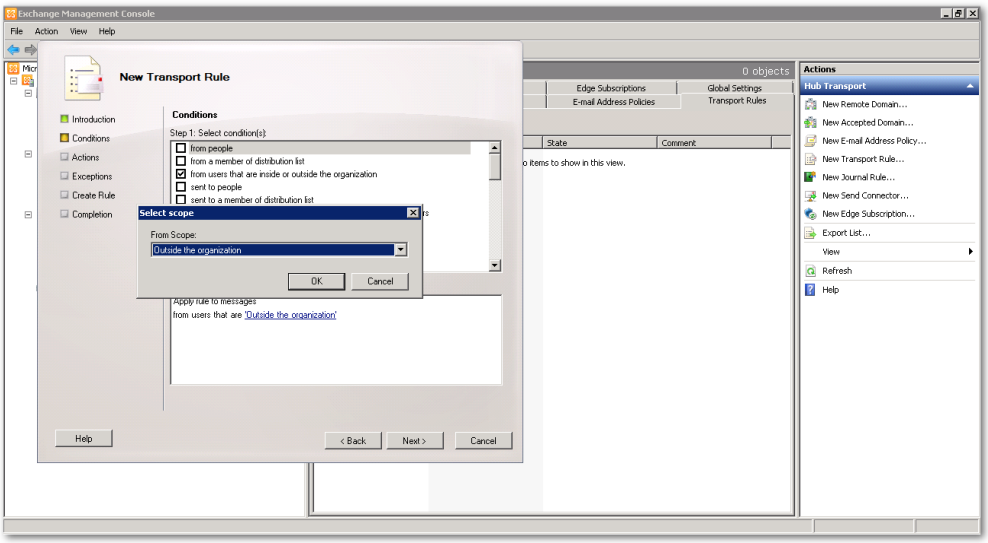

Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Microsoft Exchange On-Premises (
)
Organization Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Mailbox
Distribution Group
Mail Contact
Disconnected Mailbox
Move Request
Toolbox
Hub Transport
0 objects
Journal Rules
Send Connectors
Edge Subscriptions
Global Settings
Remote Domains
Accepted Domains
E-mail Address Policies
Transport Rules
Create Filter
Name
Priority
State
Comment
There are no items to show in this view.
Actions
Hub Transport
New Remote Domain...
New Accepted Domain...
New E-mail Address Policy...
New Transport Rule...
New Journal Rule...
New Send Connector...
New Edge Subscription...
Export List...
View
Refresh
Help

In the **New Transport Rule** configuration panel, give the transport rule a name and a description.

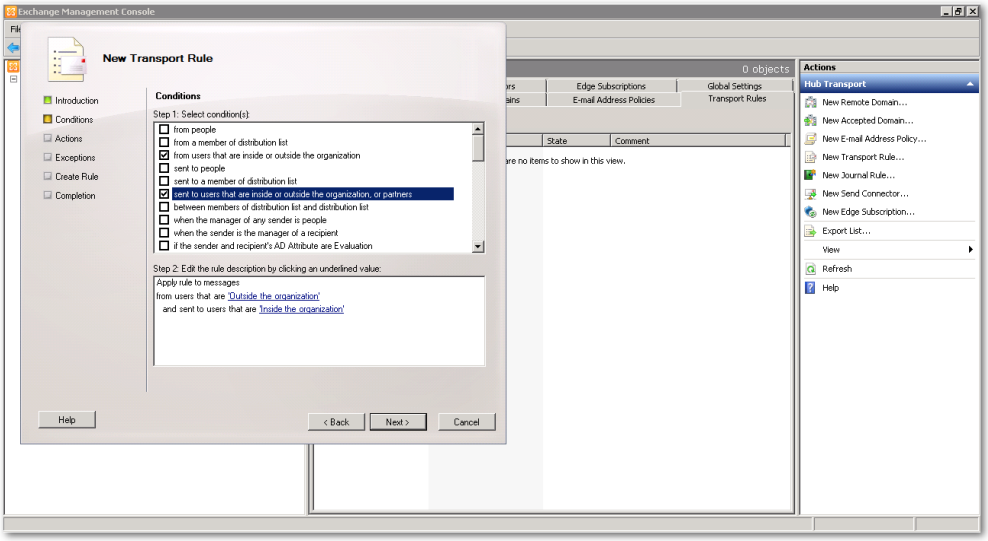


Click **Next** to move to the **Conditions** configuration panel

In the **Condition** configuration panel, select **from users that are inside or outside the organization** option and in the dropdown, select **Outside the organization**.

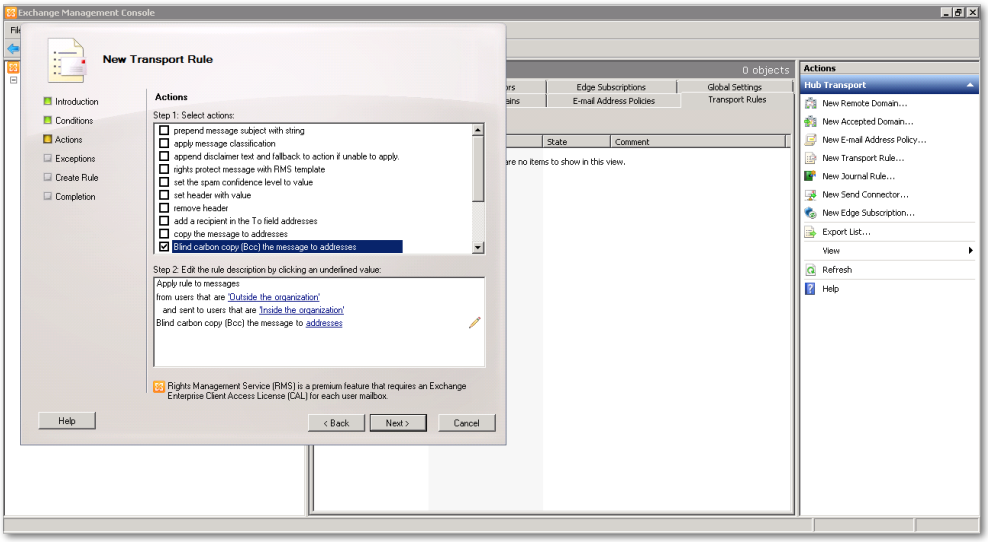


Add a second condition to the transport rule, select **sent to users that are inside or outside the organization, or partners** option. We want to keep the default value of **Inside the organization**.

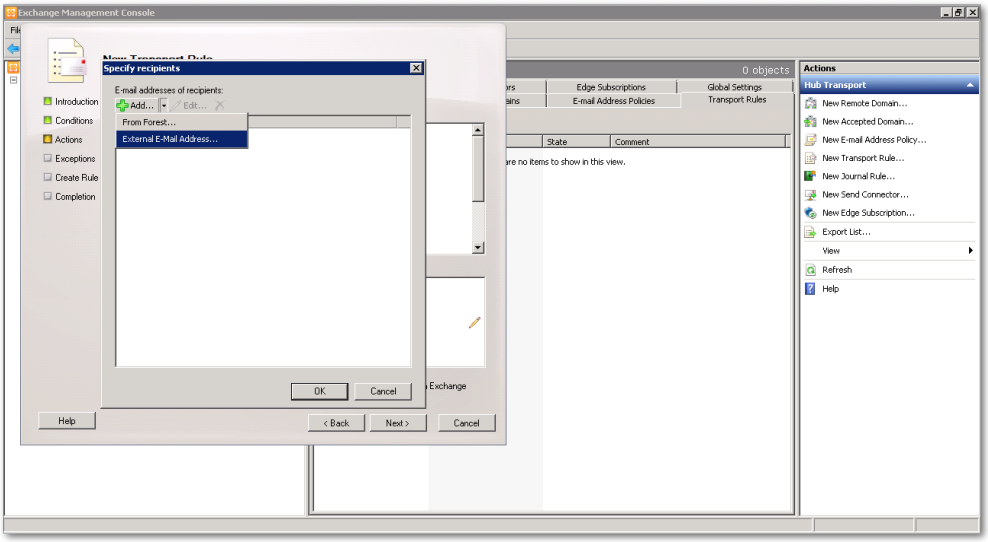


Click **Next** to move to the **Action** configuration panel

In the **Action** configuration panel, select **Blink carbon copy (Bcc) the message to addresses** option and click on the **address** variable to edit the address to Bcc.

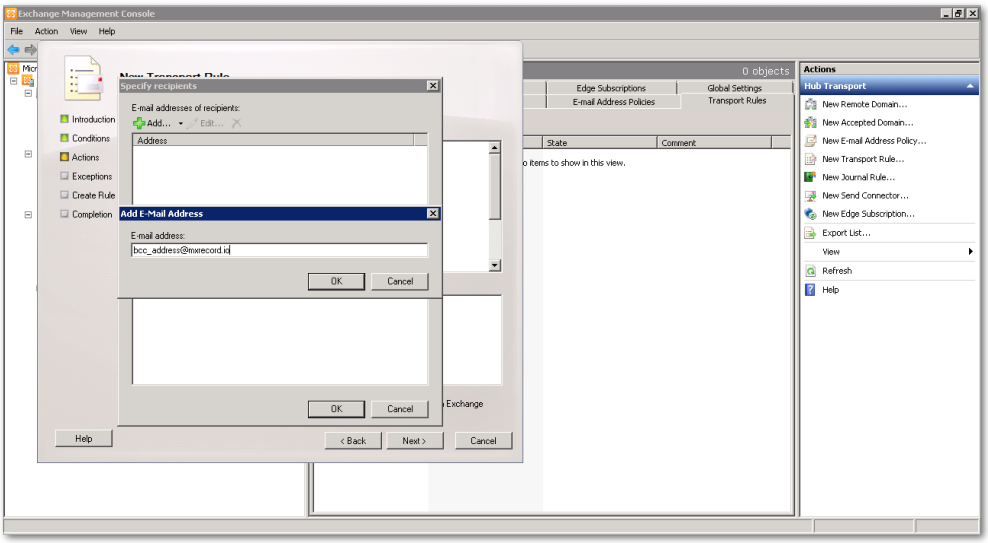


In the **Specify Recipient** dialog, click the down arrow icon on the right of the **Add...** button and select **External E-Mail Address...**

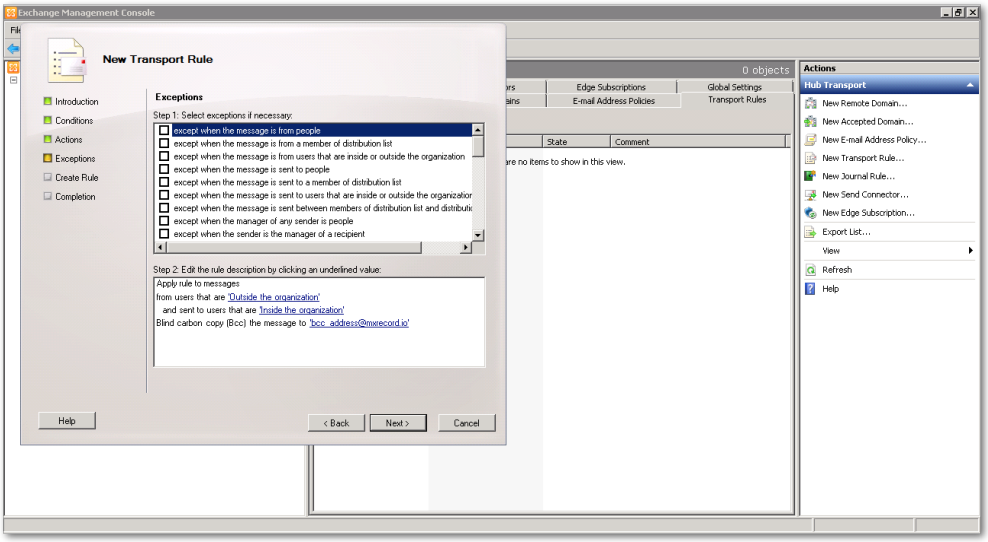


Enter the Bcc address provided by Area 1. This address is specific to your account.

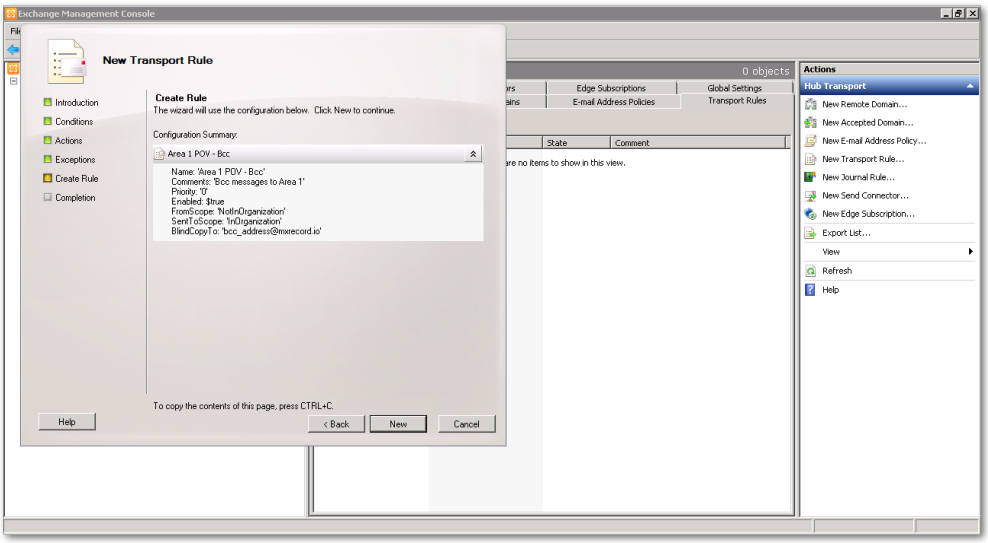
Click **OK** on both dialogs to confirm the addition of the Bcc address. This will return you to the main configuration page of the transport rule.



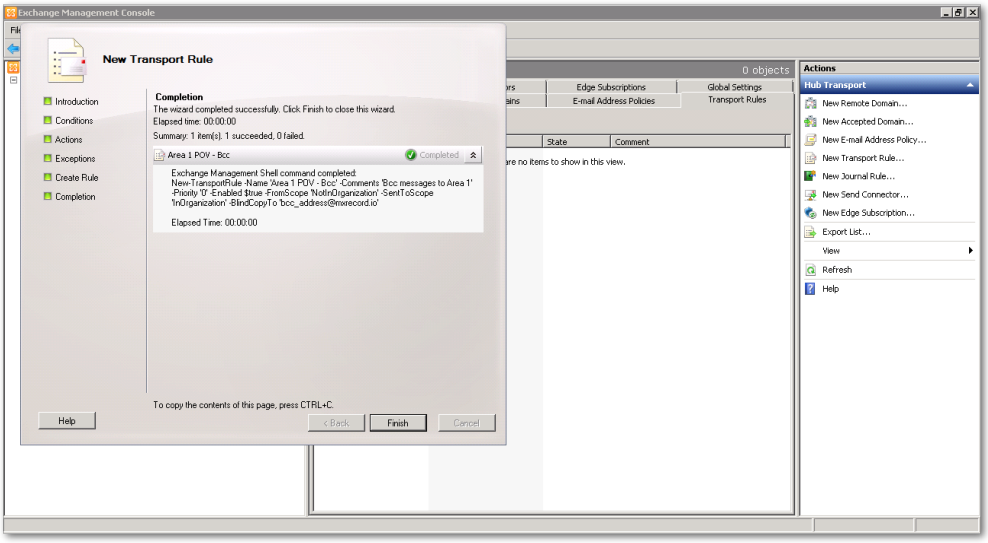
Once back to the main configuration panel, click on **Next** to move to the **Exception** configuration panel.



No exception will be configured. Click **Next** to move to the transport rule verification panel.



Click the **New** button on the verification panel to create the transport rule



Click **Finish** to close the transport rule configuration panel. This will return you to the Exchange Management Console.

Note: If you have multiple rules, you may need to re-order the Bcc rule to the right location in your rule sequence so you can appropriately send the Bcc messages to Area 1. Generally, the Area 1 Bcc rule will be at the top of the ruleset. The configured conditions of the Area 1 Bcc rule will only trigger for inbound messages.

Email Processing & Reports

In the Bcc mode, all emails are put through automated phishing detections by Area 1. Emails that trigger phishing detections are logged for reporting via product portal, email and Slack. Emails that don't trigger any detections are deleted.