Mail flow rules (transport rules) in Exchange Online

By AshaIyengar21

Archived: 2026-04-05 23:19:11 UTC

In cloud-based organizations, you can use Exchange mail flow rules (also known as transport rules) to identify and take action on messages that flow through your organization.

Mail flow rules are similar to the Inbox rules that are available in Outlook and Outlook on the web (formerly known as Outlook Web App). The main difference is that the mail flow rules take action on messages while they're in transit, and not after the message is delivered to the mailbox. Mail flow rules contain a richer set of conditions, exceptions, and actions, which provides you with the flexibility to implement many types of messaging policies.

This article explains the components of mail flow rules, and how they work.

For steps to create, copy, and manage mail flow rules, see Manage mail flow rules. For each rule, you have the option of enforcing it, testing it, or testing it and notifying the sender. For more information about the testing options, see Test mail flow rules in Exchange Online and Policy Tips (not available in the Built-in security add-on for on-premises mailboxes).

For summary and detail reports about messages that matched mail flow rules, see Use mail protection reports to view data about malware, spam, and rule detections.

A mail flow rule is made of conditions, exceptions, actions, and properties:

- **Conditions**: Identify the messages that you want to apply the actions to. Some conditions examine message header fields (for example, the To, From, or Cc fields). Other conditions examine message properties (for example, the message subject, body, attachments, message size, or message classification). Most conditions require you to specify a comparison operator (for example, equals, doesn't equal, or contains) and a value to match.

  For more information about mail flow rule conditions in Exchange Online, see Mail flow rule conditions and exceptions (predicates) in Exchange Online.

- **Exceptions**: Optionally, identify the messages that the actions shouldn't apply to. The same message identifiers that are available in conditions are also available in exceptions. Exceptions override conditions and prevent the rule actions from being applied to a message, even if the message matches all of the configured conditions.

- **Actions**: Specify what to do to messages that match the conditions in the rule, and that don't match any of the exceptions. There are many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers in the message body.

For more information about mail flow rule actions that are available in Exchange Online, see Mail flow rule actions in Exchange Online.

- **Properties**: Specify other rules settings that aren't conditions, exceptions, or actions, for example, when the rule should be applied, whether to enforce or test the rule, and the time period when the rule is active.

  For more information, see the Mail flow rule properties section in this article.

Note

If you create a rule without conditions and exceptions, the rule action is applied to all messages. This result can have unintended consequences. For example, if the rule action is to delete the message, removing the conditions and exceptions could cause the rule to delete all inbound and outbound messages for the entire organization.

The following table shows how multiple conditions, condition values, exceptions, and actions are handled in a rule:

Component	Logic	Comments
Multiple conditions	AND	A message must match all the conditions in the rule. If you need to match one condition or another, use separate rules for each condition. For example, if you want to add the same disclaimer to messages with attachments and messages that contain specific text, create one rule for each condition. In the EAC, you can easily copy a rule.
One condition with multiple values	OR	Some conditions allow you to specify more than one value. The message must match any one (not all) of the specified values. For example, if an email message has the subject "Stock price information", and the **The subject includes any of these words** condition is configured to match the words "Contoso" or "stock", the condition is satisfied because the subject contains at least one of the specified values.
Multiple exceptions	OR	If a message matches any one of the exceptions, the actions aren't applied to the message. The message doesn't have to match all the exceptions.

Component	Logic	Comments
Multiple actions	AND	Messages that match a rule's conditions get all the actions that are specified in the rule. For example, if the actions **Prepend the subject of the message with** and **Add recipients to the Bcc box** are selected, both actions are applied to the message. Keep in mind that some actions (for example, the **Delete the message without notifying anyone** action) prevent subsequent rules from being applied to a message. Other actions (for example, the **Forward the message** action) don't allow additional actions. You can also set an action on a rule so that when that rule is applied, subsequent rules aren't applied to the message.

The following table describes the rule properties that are available in mail flow rules:

Property name in the EAC	Parameter name in PowerShell	Description
Priority	*Priority*	Indicates the order in which the rules are applied to messages. The default priority is based on when the rule is created (older rules have a higher priority than newer rules, and higher priority rules are processed before lower priority rules). You can change the rule priority in the EAC by moving the rule up or down in the list of rules. In the PowerShell, you set the priority number (0 is the highest priority). For example, if you have one rule to reject messages that include a credit card number, and another one requiring approval, you'll want the reject rule to happen first, and other rules stopped from being applied. For more information, see Set the priority of a mail flow rule.
Severity	*SetAuditSeverity*	Sets the severity level of the incident report and the corresponding entry that's written to the message tracking log. Valid values are **DoNotAudit**, **Low**, **Medium**, and **High**.

Property name in the EAC	Parameter name in PowerShell	Description
Mode	*Mode*	You can specify whether you want the rule to start processing messages immediately, or whether you want to test rules without affecting the delivery of the message, with or without Policy Tips. Policy Tips present a brief note in Outlook or Outlook on the web that provides information about possible policy violations to the person that's creating the message. For more information about the modes, see Test mail flow rules in Exchange Online.
Activate this rule on the following date **Deactivate this rule on the following date**	*ActivationDate* *ExpiryDate*	Specifies the date range when the rule is active.
On checkbox selected or not selected	New rules:*Enabled* parameter on the **New-TransportRule** cmdlet. Existing rules: Use the **Enable-TransportRule** or **Disable-TransportRule** cmdlets. The value is displayed in the **State** property of the rule.	You can create a disabled rule and enable it when you're ready to test it. Or, you can disable a rule without deleting it to preserve the settings.
Defer the message if rule processing doesn't complete	*RuleErrorAction*	You can specify how the message should be handled if the rule processing can't be completed. By default, the rule will be ignored, but you can choose to resubmit the message for processing.
Match sender address in message	*SenderAddressLocation*	If the rule uses conditions or exceptions that examine the sender's email address, you can look for the value in the message header, the message envelope, or both.

Property name in the EAC	Parameter name in PowerShell	Description
Stop processing more rules	*StopRuleProcessing*	This element is an action for the rule, but it looks like a property in the EAC. You can choose to stop applying additional rules to a message after a rule processes a message.
Comments	*Comments*	You can enter descriptive comments about the rule.

All messages (except NDRs) that flow through your organization are evaluated against the enabled mail flow rules in your organization. Rules are processed in the order listed on the **Mail flow** > **Rules** page in EAC, or based on the corresponding *Priority* parameter value in the PowerShell.

Each rule also offers the option of stopping to processing more rules when the rule is matched. This setting is important for messages that match the conditions in multiple mail flow rules (which rule do you want applied to the message? All? Just one?).

There are several types of messages that pass through an organization. The following table shows which messages types can be processed by mail flow rules:

Type of message	Can a rule be applied?
Regular messages: Messages that contain a single rich text format (RTF), HTML, or plain text message body, or a multipart or alternative set of message bodies.	Yes
Message Encryption: Messages encrypted by Message Encryption in Microsoft 365 or Office 365. For more information, see Encryption.	Rules can always access envelope headers and process messages based on conditions that inspect those headers. For a rule to inspect or modify the contents of an encrypted message, you need to verify that transport decryption is enabled. You can also create a rule that automatically decrypts encrypted messages. For more information, see Define rules to encrypt email messages.
S/MIME encrypted messages	Rules can only access envelope headers and process messages based on conditions that inspect those headers. Rules with conditions that require inspection of the message's content, or actions that modify the message's

Type of message	Can a rule be applied?
	content can't be processed.
RMS protected messages: Messages that had an Active Directory Rights Management Services (AD RMS) or Azure Rights Management (RMS) policy applied.	Rules can always access envelope headers and process messages based on conditions that inspect those headers. For a rule to inspect or modify the contents of an RMS-protected message, you need to verify that transport decryption is enabled by setting the `TransportDecryptionSetting` to Mandatory or Optional using the Set-IRMConfiguration cmdlet.
Clear-signed messages: Messages that have been signed but not encrypted.	Yes
Anonymous messages: Messages sent by anonymous senders.	Yes
Read reports: Reports that are generated in response to read receipt requests by senders. Read reports have a message class of `IPM.Note*.MdnRead` or `IPM.Note*.MdnNotRead`.	Yes

System-generated messages don't get processed by your organization's mail flow rules (or transport rules). Some of the messages that aren't processed by mail flow rules are:

- Non-Delivery report (NDR) generated by Exchange. The NDRs created by non-Exchange service won't be detected as NDR by Exchange Mail flow rules, and the corresponding Mail flow rules conditions/exceptions won't be matched.
- Messages sent to the arbitration mailbox (like approval request notification).
- Journal report.

- The **Version** or **RuleVersion** property value for a rule isn't important in Exchange Online.
- After you create or modify a mail flow rule, it can take up to 30 minutes for the new or updated rule to be applied to messages.
- You can create a transport rule to bypass email protection filtering and allow mail to flow without delay from internal senders such as scanners, faxes, and other trusted sources that send attachments that are known to be safe. Don't bypass filtering for all internal messages; in this situation, a compromised account could send malicious content.
- History and changes to mail flow rules aren't maintained; so, you can't revert mail flow rules back to previous states.

Source: https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules