Message Rules

Message rules allow you to specify that some types of messages should not be remediated or scanned. You can create:

- Allow List rules
- Verdict Override rules
- Bypass Analysis rules

Note: Allow List and Verdict Override rules are not available for businesses in No Authentication mode.

Create and manage your message rules from the **Administration** > **Message Rules** page.

Bypass Analysis rules take precedence over Allow List and Verdict Override rules. If a message is affected by a rule, it is indicated in the Message Rules column of the Messages page. Hover your cursor over the item in the Rule column to see which rule was applied.

Note: Rules do not automatically apply to sub-domains. Domains are matched exactly as indicated in a rule.

Allow List Rules

Allow List rules allow you to prevent remediation of Threat, Spam, and/or Graymail messages from specific sender email addresses, sender domains, or sender IP addresses. Messages will still be analyzed but auto-remediation will not be applied. For example, if Secure Email Threat Defense determines items from a certain sender are Spam, but you want to keep the items in user Inboxes, you can create an Allow List rule to override any policy that would remediate such messages. An Allow List rule acts an exception to your overall policy settings. Messages that match an Allow List rule still appear on the Impact report.

Allow List rules:

- Apply to Threats, Spam, and/or Graymail.
- Specify allowed sender email addresses, sender domains, or sender IP addresses (IPv4 or CIDR block).
- Can have up to 50 criteria per rule. That is, 50 email addresses, domains, or addresses.

There is a limit of 20 active rules. Rules can be deactivated or deleted.

Verdict Override Rules

Verdict Override rules allow you to override Threat, Spam, and/or Graymail verdicts that match the criteria specified by the rule. Messages are marked with a Neutral verdict and are not remediated. Messages where the verdict was overridden do not appear on the Impact report.

Verdict Override rules:

- Apply to Threats, Spam, and/or Graymail.
- Specify allowed sender email addresses, sender domains, or sender IP addresses (IPv4 or CIDR block).
- Can have up to 50 criteria per rule. That is, 50 email addresses, domains, or IP addresses.

There is a limit of 20 active rules. Rules can be deactivated or deleted.

Bypass Analysis Rules

Bypass Analysis rules allow you to bypass analysis for Phish Test or Security Mailbox messages that match the criteria. Messages that meet the rule criteria will bypass all engine analysis so you can process your security tests without engines interfering. Attachments and links are not opened or scanned by Secure Email Threat Defense.

Note: If a Bypass Analysis rule is created for testing, the rule should be reconsidered after an appropriate period of time to prevent vulnerabilities.

Phish Test rules:

- Apply to all incoming messages from the specified sender email addresses, sender domains, or IP addresses (IPv4 or CIDR block); messages will not be analyzed.

  Note: We recommend only using sender IP addresses/CIDR criteria to bypass specific sender infrastructure; IP addresses are not as easily spoofed as sender email addresses or domains.

- Can have up to 50 criteria per rule.

Security Mailbox rules:

- Apply to incoming messages for the specified recipient email addresse(s); messages will not be analyzed.

  Note: Security Mailbox rules are applied if the specified recipient is the only recipient of the message. If other recipients are copied or included as a BCC (blind carbon copy), the message will not bypass the analysis engines.

- Can have up to 50 criteria per rule.

There is a limit of 20 active Bypass Analysis rules. Rules can be deactivated or deleted.

Advisory on Creating and Using Bypass Rules

Note the following important caveats when creating and using Bypass Rules.

- A Bypass Rule bypasses all scanning and protections for messages that match the rule conditions. Do not use Bypass Rules for any use-cases other than customer employee security awareness training (Phish Test) or for end-mailbox-user reporting to an organization's Security Mailbox. These are the only supported scenarios for Bypass Rules. For all other scenarios only Verdict Override or Allow Rules are supported.
- It is strongly advised to use only the dedicated Sender IP Addresses/CIDR blocks provided by your Phish Test vendor as the basis of Bypass Rules.
- Be aware if your Phish Test vendor is unable to provide dedicated Sender IP Addresses/CIDR blocks; the usage of Sender Domain or Email Address in a Bypass Rule opens you up to bypassing potentially spoofed messages.
- Do not use Sender Domain or Email Address in a Bypass Rule unless you have separately validated that sender email authentication is strongly enforced by your organization's upstream edge email controls, and the specified Sender Domain or Sender Email Address exactly matches the final Return-Path header on all messages intended to match the Bypass Rule.

Add Message Rules

The steps for adding message rules differ slightly depending on the category of rule.

Add a New Allow List or Verdict Override Rule

Complete the following steps to create a new rule:

1. Select **Administration** > **Message Rules**.
2. Select the category of rule you want to create: **Allow List** or **Verdict Override**.
3. Click the **Add New Rule** button.
4. Create a rule name. Each rule must have a unique name.
5. Select a criteria type. You can select Sender Email, Sender Domain, Sender IP Addresses (IPv4), or Sender IP Addresses (CIDR).
6. Enter the items you want to allow or override, separated by commas.
7. Select Spam, Graymail, and/or Threats, depending on which verdicts you want to allow.
8. Click **Submit** to finish creating the rule.

Your rule is added to the list. It may take up to 20 minutes for the change to take effect.

Add a New Bypass Analysis Rule

Complete the following steps to create a new rule:

1. Select **Administration** > **Message Rules**.
2. Select **Bypass Analysis**.
3. Click the **Add New Rule** button.
4. Create a rule name. Each rule must have a unique name.
5. Select which rule type you want to create: **Phish Test** or **Security Mailbox**.
6. For a Phish Test rule, select a criteria type: Sender Email Addresses, Sender Domains, Sender IP Addresses (IPv4), or IP Addresses (CIDR). Then, enter your items, separated by commas.

   For a Security Mailbox rule, enter your recipient email addresse(s), separated by commas.
7. Click **Submit** to finish creating the rule.

Your rule is added to the list. It may take up to 20 minutes for the change to take effect.

Note: If a Bypass Analysis rule is created for testing, the rule should be reconsidered after an appropriate period of time to prevent vulnerabilities. See for important caveats to keep in mind when creating and using Bypass Rules.

Edit a Rule

Note that only enabled rules can be edited. To edit a rule:

1. Select **Administration** > **Message Rules**.
2. Select the type of rule you want to edit.
3. Under the Actions column, click the pencil icon next to the rule you want to edit.
4. Make your desired changes, then click **Save Changes**.

Your rule is updated. It may take up to 20 minutes for the change to take effect.

Enable or Disable a Rule

To enable or disable an existing rule:

1. Select **Administration** > **Message Rules**.
2. Select the type of rule you want to enable or disable.
3. Under the Actions column, click the enable or disable icon next to the rule you want to change the status of.

The status of your rule is updated. It may take up to 20 minutes for the change to take effect.

Delete a Rule

To delete a rule:

1. Select **Administration** > **Message Rules**.
2. Select the type of rule you want to delete.
3. Under the Actions column, click the delete icon next to the rule you want to delete.

Your rule is deleted.

Microsoft Allow Lists and Safe Senders

Secure Email Threat Defense honors senders and domains added to your spam filter allow lists in Microsoft 365 for Spam and Graymail messages. MS Allow lists are not honored for Threat verdicts (BEC, Scam, Malicious, Phishing); these items will be remediated according to your policy settings. For more information, see Cisco Secure Email Threat Defense FAQ: Secure Email Threat Defense and Microsoft 365.

Microsoft Allow lists are not always honored by Secure Email Threat Defense if your organization allows individual users to configure allow lists in their mailbox and a message happens to fall in a user's allow list. If you want Secure Email Threat Defense to honor these settings, select the **Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts** check box on the Policy page. Safe Sender flags are respected for Spam and Graymail verdicts, but are not respected for Malicious and Phishing verdicts. That is, Safe Sender messages with Spam or Graymail verdicts will not be remediated.