邮件规则

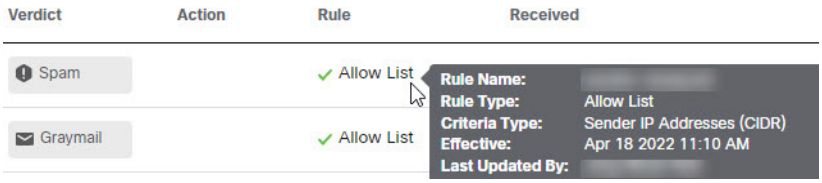
邮件规则允许您指定不应补救或扫描的某些类型的邮件。您可以创建：

- “允许列表”规则
- “判定覆盖”规则
- “绕过分析”规则

注意：“允许列表”和“判定覆盖”规则不适用于无身份验证模式下的企业。

从**设置 (Settings) > 邮件规则 (Message Rules)** 页面创建和管理邮件规则。

“绕过分析”规则优先于“允许列表”和“判定覆盖”规则。如果邮件受规则影响，则会在“邮件”(Messages) 页面的“邮件规则”(Message Rules) 列中指明。将光标悬停在“邮件规则”(Message Rules) 列中的项目上即可查看应用的规则。



注意：规则不会自动应用于子域。域会完全按照规则中的指示进行匹配。

允许列表规则

“允许列表”规则让您能够阻止对来自特定发件人邮件地址、发件人域或发件人 IP 地址的垃圾邮件和灰色邮件进行补救。系统仍会分析邮件，但不会应用自动补救。例如，如果 Secure Email Threat Defense 确定来自某个发件人的项目是垃圾邮件，但您希望将这些项目保留在用户收件箱中，则可以创建“允许列表”规则来覆盖对此类邮件进行补救的任何策略。“允许列表”规则是策略的例外情况。与“允许列表”规则匹配的邮件仍会显示在“影响”(Impact) 报告中。

“允许列表”规则：

- 应用于灰色邮件和/或垃圾邮件。
- 指定允许的发件人邮件地址、发件人域或发件人 IP 地址（IPv4 或 CIDR 块）。
- 每个规则最多可以包含 50 个条件。也就是说，可以包含 50 个邮件地址、域或地址。

活动规则的数量限制为 20。规则可以停用，但不能删除。

判定覆盖规则

“判定覆盖”规则允许您覆盖与规则指定的条件匹配的垃圾邮件和灰色邮件判定。邮件会被标记为“中性”判定，并且不会进行补救。判定被覆盖的邮件不会显示在“影响”(Impact) 报告中。

“判定覆盖”规则：

- 应用于灰色邮件和/或垃圾邮件。
- 指定允许的发件人邮件地址、发件人域或发件人 IP 地址（IPv4 或 CIDR 块）。
- 每个规则最多可以包含 50 个条件。也就是说，可以包含 50 个邮件地址、域或 IP 地址。

活动规则的数量限制为 20。规则可以停用，但不能删除。

绕过分析规则

“绕过分析”规则让您能绕过对网络钓鱼测试或安全邮箱邮件的分析。符合规则条件的邮件将绕过所有引擎分析，因此您可以在不受引擎干扰的情况下处理安全测试。Secure Email Threat Defense 不会打开或扫描附件和链接。

“网络钓鱼测试”规则：

- 应用于来自指定发件人邮件地址、发件人域或 IP 地址的所有传入邮件（IPv4 或 CIDR 块）；邮件不会被分析。
- 每个规则最多可以包含 50 个条件。

“安全邮箱”规则：

- 应用于指定收件人邮件地址的传入邮件；邮件不会被分析。

  注意：如果指定的收件人是邮件的唯一收件人，则会应用“安全邮箱”规则。如果其他收件人被复制或作为密件抄送（密件抄送），则邮件不会绕过分析引擎。

- 每个规则最多可以包含 50 个条件。

活动“绕过分析”规则的数量限制为 20。规则可以停用，但不能删除。

添加邮件规则

添加邮件规则的步骤会因规则类别而异。

添加新的允许列表或判定覆盖规则

完成以下步骤以创建新规则：

1. 选择**设置**（齿轮图标）> **邮件规则 (Message Rules)**。
2. 选择要创建的规则类别：**允许列表 (Allow List)** 或**判定覆盖 (Verdict Override)**。
3. 点击 **Add New Rule** 按钮。
4. 创建规则名称。每个规则必须有唯一名称。
5. 选择条件类型。您可以选择发件人邮件、发件人域、发件人 IP 地址 (IPv4) 或发件人 IP 地址 (CIDR)。
6. 输入允许的项目，以逗号分隔。

7. 根据要允许的判定，选择“垃圾邮件”(Spam)和/或“灰色邮件”(Graymail)。
8. 点击**提交 (Submit)** 完成创建此规则。

您的规则会被添加到列表中。更改最多可能需要 20 分钟即可生效。

添加新的绕过分析规则

完成以下步骤以创建新规则：

1. 选择**设置**（齿轮图标）> **邮件规则 (Message Rules)**。
2. 选择**绕过分析 (Bypass Analysis)**。
3. 点击 **Add New Rule** 按钮。
4. 创建规则名称。每个规则必须有唯一名称。
5. 选择要创建的规则类型：**网络钓鱼测试 (Phish Test)** 或**安全邮箱 (Security Mailbox)**。
6. 对于网络钓鱼测试规则，请选择条件类型：发件人邮件地址、发件人域、发件人 IP 地址 (IPv4) 或 IP 地址 (CIDR)。然后，输入您的项目，以逗号分隔。

   对于安全邮箱规则，请输入收件人邮件地址，以逗号分隔。
7. 点击**提交 (Submit)** 完成创建此规则。

您的规则会被添加到列表中。更改最多可能需要 20 分钟即可生效。

编辑规则

请注意，只能编辑已启用的规则。要编辑规则，请执行以下操作：

1. 选择**设置**（齿轮图标）> **邮件规则 (Message Rules)**。
2. 选择要编辑的规则类型。
3. 在“操作”(Actions) 列下，点击要编辑的规则旁边的铅笔图标。
4. 进行所需的更改，然后点击**保存更改 (Save Changes)**。

您的规则已更新。更改最多可能需要 20 分钟即可生效。

启用或禁用规则

要启用或禁用现有规则，请执行以下操作：

1. 选择**设置**（齿轮图标）> **邮件规则 (Message Rules)**。
2. 选择要启用或禁用的规则类型。
3. 在“操作”(Actions) 列下，点击要更改其状态的规则旁边的启用或禁用图标。

规则的状态已更新。更改最多可能需要 20 分钟即可生效。

Microsoft 允许列表和安全发件人

Secure Email Threat Defense 遵循添加到 Microsoft 365 垃圾邮件和灰色邮件中的垃圾邮件过滤器允许列表中的发件人和域。恶意或网络钓鱼判定不遵循 MS 允许列表。有关详细信息，请参阅思科安全邮件威胁防御常见问题解答：思科安全邮件威胁防御和 Microsoft 365。

如果您的组织允许个人用户在其邮箱中配置允许列表，并且邮件恰好属于用户的允许列表，则 Secure Email Threat Defense 不总是遵循 Microsoft 允许列表。如果要让 Secure Email Threat Defense 遵循这些设置，请在“策略”(Policy) 页面上选中**不补救包含垃圾邮件或灰色邮件判定的Microsoft安全发件人邮件(DonotremediateMicrosoftSafeSendermessages withSpamorGraymailverdicts)**复选框。垃圾邮件和灰色邮件判定会遵循安全发件人标志，但恶意和网络钓鱼判定不会遵循安全发件人标志。也就是说，带有垃圾邮件或灰色邮件判定的安全发件人邮件将不会进行补救。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。