策略设置

设置（齿轮图标）> **策略 (Policy)** 页面上的设置确定 Cisco Secure Email Cloud Mailbox 将如何处理邮件。默认设置在您 **设置思科安全邮件威胁防御，第11页**时应用。要更改设置，请进行更改，然后点击**保存并应用(Save and Apply)**按钮。

表 1　　策略设置

设置	说明	选项	默认
消息源	定义邮件的来源。	■ **Microsoft O365** ■ **网关**（仅适用于传入邮件）	在设置思科安全邮件威胁防御时手动选择。
可视性和补救措施	定义可以应用的补救策略的类型。	■ **Microsoft 365 身份验证** - **读/写 (Read/Write)** - 允许查看和按需或自动补救（即，移动或删除可疑邮件）。将从 Microsoft 365 请求读/写权限。 - **读取 (Read)** - 仅允许显示，不允许补救措施。将从 Microsoft 365 请求只读权限。 如果选择**阅读(Read)**，则只需设置**附件分析 (Attachment Analysis)**和**邮件分析 (Message Analysis)**方向。将不会应用补救策略。 ■ **无身份验证** 仅允许可视性。	在设置思科安全邮件威胁防御时手动选择。 如果您更改 Microsoft 365 身份验证设置，则会被重定向以重置 Microsoft 365 权限。系统可能还会指示您设置日志记录；如果您已设置日志记录，则可以跳过此步骤。 **注意：**如果选择 **Microsoft 365 身份验证：读/写 (Microsoft 365 Authentication: Read/Write)**，则您还应验证**自动补救策略 (Automated Remediation Policy)** 设置。
Cisco Secure Email Gateway (SEG)	Cisco Secure Email Gateway(SEG)的存在会影响 Secure Email Threat Defense 识别发件人 IP 的方式。	■ 未选择任何内容（无 SEG） ■ **SEG 存在** - **使用思科 SEG 默认信头** (X-IronPort-RemoteIP). - **使用自定义 SEG 信头**。您必须添加要使用的信头。	在设置思科安全邮件威胁防御时手动选择。 有关详细信息，请参阅使用网关的策略设置，第 17 页。

表 1　　策略设置

设置	说明	选项	默认
邮件分析	要动态分析的邮件，包括： ■ 邮件方向 ■ Cisco Secure Malware Analytics 要分析的邮件附件的方向 ■ 垃圾邮件和灰色邮件分析	■ **邮件方向** – **传入** – **传出** – **内部** ■ **附件方向** – **传入** – **传出** – **内部** ■ **垃圾邮件和灰色邮件** – **开**或**关**	■ **邮件方向** – **全部**，Microsoft O365 邮件来源 – **传入**，网关邮件来源 ■ **附件方向** – **传入** ■ **垃圾邮件和灰色邮件** – 为 2023 年 5 月 9 日之后创建的所有账户**关闭**
自动补救策略	对发现的邮件采取的补救操作： ■ **威胁**（BEC、诈骗、网络钓鱼或恶意邮件） ■ **垃圾邮件** ■ **Graymail**	■ **不执行操作** ■ **移至隔离区** ■ **移至垃圾桶** ■ **移至垃圾邮件** **注意：**如果发件人地址属于Exchange 中的发件人允许列表，或者如果邮件已由 Microsoft 365 进行补救，则不会应用补救操作。	■ **自动补救策略**切换 – **关** ■ 威胁 – **移至隔离区** ■ 垃圾邮件 – **移至垃圾邮件** ■ 灰色邮件 – **无操作**
安全发件人：不使用垃圾邮件或灰色邮件判定来补救 Microsoft 安全发件人邮件。	如果选中此复选框，将不会对 Microsoft 在日志信头中标记为“安全发件人”且被 Secure Email Threat Defense 判定为垃圾邮件或灰色邮件的邮件进行补救。	**选中**或**取消选中**	**已取消选中**
导入的域 – 导入域以帮助确定邮件方向。域可以从自动补救策略中排除。			
应用自动补救	将自动补救应用于特定域。	**选中**或**取消选中**	**取消选中**。在打开**读/写**补救模式时，请选中这些复选框以将自动补救应用于特定域。
对不在上述域列表中的域应用自动补救	当域未明确列出时适用。例如，如果新域已被添加到您的 Microsoft 365 帐户但尚未导入。Secure Email Threat Defense	**选中**或**取消选中**	**取消选中**。当您打开**读/写**模式时，选中此复选框可确保将自动补救应用于所有内部邮件。

使用网关的策略设置

如果您有思科邮件安全设备或类似网关，请考虑使用以下策略设置。

表 2　　建议使用网关的策略设置

设置名称	推荐的选择
Cisco Secure Email Gateway (SEG)	**SEG 存在**，并指示信头
邮件分析	**传出**和**内部**
附件分析	**无**
补救措施	■ 威胁 - **移至隔离区** ■ 垃圾邮件 - **移至垃圾邮件**

务必指明存在安全邮件网关 (SEG)，以及哪个信头可用于在传入日志中识别该网关，以便 Secure Email Threat Defense 可以确定邮件的真实源发件人。如果没有此配置，则可能会出现所有邮件都来自 SEG 的情况，从而可能导致误报。

有关在思科安全邮件云网关（以前称为CES）或CiscoSecureEmailGateway（以前称为ESA）上验证或配置信头的信息，请参阅 https://docs.ces.cisco.com/docs/configuring-asyncos-message-filter-to-add-sender-ip-header-for-cloud-mailbox。

如果您使用 Microsoft 365 作为邮件来源，我们还建议绕过您的设备，以便将日志直接从 Microsoft 365 发送到 Secure Email Threat Defense。您可以通过在 Microsoft 365 中添加连接器来执行此操作，如设置思科安全邮件威胁防御，第 11 页中所述。

切换邮件来源

要更改邮件来源，请导航至**设置**（齿轮图标）> **策略 (Policy)** 页面。

1. 选择新邮件来源的单选按钮。
2. 系统将显示一条通知，指明您正在切换邮件来源。点击**继续 (Continue)**。
3. 系统将显示“切换邮件来源”对话框。您需要配置之前的邮件来源，以便停止向思科安全邮件威胁防御发送邮件。有关如何执行此操作的详细信息，请参阅删除 Secure Email Threat Defense 日志规则，第 55 页或将网关配置为停止发送邮件，第 56 页。
4. 选中表示您已停止发送先前来源的日志或邮件的复选框，然后点击**下一步 (Next)**。
5. 使用对话框中显示的邮件接收地址或日志地址来配置新邮件来源。设置邮件来源，第 12 页中详细介绍了设置每种邮件来源的步骤。

切换邮件来源

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。