设置思科安全邮件威胁防御

安全邮件威胁防御设置包括以下内容：

1. 登录您的帐户，第 11 页
2. 指明您是否有 Cisco Secure Email Gateway (SEG)，第 12 页
3. 选择邮件来源、可视性和补救措施，第 12 页
4. 设置邮件来源，第 12 页
5. 查看您的策略设置，第 14 页
6. 导入 Microsoft 邮件域，第 14 页

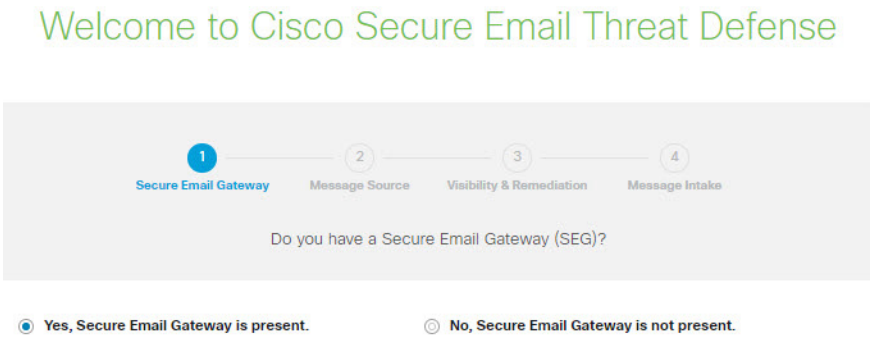
这些步骤将假定您符合**要求，第 9 页**。

登录您的帐户

1. 按照思科欢迎邮件中的说明来设置用户帐户。

   Secure Email Threat Defense 使用 Cisco Security Cloud 登录管理用户身份验证。有关 Cisco Security Cloud 登录的信息，请参阅 https://cisco.com/go/securesignon。如果您是 Cisco SecureX Threat Response、Cisco Secure Malware Analytics（以前称为 Cisco Threat Grid）或 Cisco Secure Endpoint（以前称为 AMP）的客户，请使用现有的凭证进行登录。如果您不是现有用户，则需要创建一个新的 Cisco Security Cloud 登录帐户。

2. 成功登录后，请接受“条款和条件”(Terms and Conditions)。
3. 您现在可以访问**欢迎使用 (Welcome to)思科安全邮件威胁防御** 页面。按照以下各部分中所述的安装向导执行操作。



指明您是否有 Cisco Secure Email Gateway (SEG)

无论您的邮件来源如何（在下一部分中选择），都必须指出存在 Cisco Secure Email Gateway (SEG) 以及哪个信头可用于在传入日志中识别该信头，以便 Secure Email Threat Defense 可以确定邮件的真正源发件人。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。

1. 通过选择“是”(Yes) 或“否”(No) 来指示是否存在 Cisco Secure Email Gateway (SEG)，然后点击**下一步 (Next)**。
2. 如果您回答“是”(Yes)，请输入您的 SEG 类型和信头。单击**下一步 (Next)**。

选择邮件来源、可视性和补救措施

1. 选择邮件来源：Microsoft O365 或网关。如果您在上一步中选择了无 SEG，则会假定 Microsoft O365 作为您的邮件来源。
2. 选择您的可视性和补救措施。

   可视性和补救模式定义了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。

     注意：如果您选择**读/写 (Read/Write)**，则在设置完成后，您需要在**策略设置，第 15 页**中打开“自动补救策略”(Automated Remediation Policy)。要将自动补救应用于所有内部邮件，请确保在“策略”(Policy) 页面上选中**对不在域列表中的域应用自动补救 (Apply auto-remediation to domains not in the domain list)** 框。

   无身份验证

   如果您使用思科 SEG 作为邮件来源，则会出现此选项。它仅提供可视性。您将无法对邮件进行补救。
3. 如果您选择了 Microsoft 365 身份验证，请连接到 Microsoft 365。
   a. 点击**下一步 (Next)** 以连接到 Microsoft 365。
   b. 根据提示登录您的 Microsoft 365 帐户。此帐户必须具有全局管理员权限；帐户不会被 Secure Email Threat Defense 存储或使用。有关为什么需要这些权限的信息，请参阅思科安全电子邮件威胁防御常见问题解答：为什么设置安全电子邮件威胁防御需要 Microsoft 365 全局管理员权限？。
   c. 点击**接受 (Accept)** 以接受 Secure Email Threat Defense 应用的权限。您将被重定向回 Secure Email Threat Defense 设置页面。
   d. 单击**下一步 (Next)**。

设置邮件来源

为所选的邮件来源完成相关步骤。

Microsoft O365 邮件来源

如果您选择 Microsoft O365 作为邮件来源，则必须将 Microsoft 365 配置为向 Secure Email Threat Defense 发送日志。要执行此操作，请添加日志规则。如果您有网关，请先在 Microsoft 365 中添加连接器，然后再添加日志规则。

1. **对于使用 Cisco Secure Email Gateway (SEG) 的用户**：在 Microsoft 365 中添加一个连接器。

   为了确保日志直接从 Microsoft 365 发送到 Secure Email Threat Defense，而无需通过 Cisco Secure Email Gateway，我们建议在 Microsoft 365 中添加出站连接器。在添加连接器后才能设置日志记录。

   在 Microsoft 365 Exchange 管理中心，使用**添加连接器 (Add a connector)**向导中的以下设置来创建新的连接器：

   - **连接自 (Connection from)**：Office 365
   - **连接至 (Connection to)**：合作伙伴组织
   - **连接器名称 (Connector name)**：出站到思科安全邮件威胁防御（选中**将其打开 (Turn it on)** 复选框）
   - **使用连接器**：仅当邮件被发送到这些域时（为北美环境添加 **mail.cmd.cisco.com**，为欧洲环境添加 **mail.eu.cmd.cisco.com**）
   - **路由 (Routing)**：使用与合作伙伴的域关联的 MX 记录
   - **安全限制 (Security restrictions)**：始终使用传输层安全 (TLS) 来保护连接（推荐）；由受信任的证书颁发机构 (CA) 颁发
   - **验证邮件 (Validation email)**：Secure Email Threat Defense 设置页面中的日志地址

     注意：如果您的O365租户已使用Exchange传输规则配置了条件邮件路由，以便将出站邮件路由到现有连接器，则连接器验证可能会失败。虽然日志邮件具有系统特权，并且不受传输规则的影响，但连接器验证测试邮件没有特权，并且会受传输规则的影响。

     要解决此验证问题，请找到已有的传输规则，并为思科安全邮件威胁防御日志地址添加例外项。等待该更改生效，然后重新测试新的连接器验证。

2. 配置要向 Secure Email Threat Defense 发送日志的 Microsoft 365。要执行此操作，请添加日志规则。

   a. 从 Secure Email Threat Defense 设置页面复制您的日志地址。如果您稍后需要重复此过程，还可以在“管理”(Administration) 页面上找到您的日志地址。

   b. 转至 Microsoft Purview 合规性门户：https://compliance.microsoft.com/homepage。

   c. 导航至**解决方案 (Solutions)** > **数据生命周期管理 (Data lifecycle management)** > **Exchange（传统）(Exchange [legacy])** > **日志规则 (Journal rules)**。

   d. 如果尚未执行此操作，请将 Exchange 收件人添加到**将无法送达的日记报告发送至 (Send undeliverable journal reports to)** 字段中，然后点击**保存 (Save)**。使用的邮箱地址不会被记录；请勿使用要让 Secure Email Threat Defense 分析的地址。如果没有要用于此目的的收件人，则需要创建一个收件人。

   e. 返回**日志规则 (Journal rules)** 页面。点击 **+** 按钮创建新的日志规则。

   f. 将日志地址从 Secure Email Threat Defense 设置页面粘贴到**将日志报告发送至 (Send journal reports to)** 字段。

   g. 在**日志规则名称 (Journal rule name)** 字段中，输入 **Cisco Secure Email Threat Defense**。

   h. 在**从其发送或接收的日志邮件 (Journal messages sent or received from)** 下，选择**每个人 (Everyone)**。

   i. 在**要记录的邮件类型 (Type of message to journal)** 下，选择**所有邮件 (All messages)**。

   j. 单击**下一步 (Next)**。

   k. 查看您的选择，然后点击**提交 (Submit)** 以完成规则创建。

3. 返回 Secure Email Threat Defense 设置页面。点击**查看策略 (Review Policy)**。

网关邮件来源

如果您选择网关作为邮件来源，请启用思科安全邮件云网关的威胁防御连接器，以便将邮件发送到思科安全邮件威胁防御。

1. 从 Secure Email Threat Defense 设置页面复制邮件接收地址。如果您稍后需要重复此过程，则可以在“管理”(Administration) 页面上找到您的邮件接收地址。
2. 从安全邮件云网关用户界面中，选择**安全服务 (Security Services)** > **威胁防御连接器 (Threat Defense Connector)**。
3. 选中**启用威胁防御连接器 (Enable Threat Defense Connector)** 复选框。
4. 输入您在步骤 1 中从思科安全邮件威胁防御中复制的邮件接收地址。
5. 点击**提交 (Submit)** 以确认更改。
6. 返回 Secure Email Threat Defense 设置页面。点击**查看策略 (Review Policy)**。

查看您的策略设置

有关策略设置的信息，请参阅**策略设置，第 15 页**。如果您已选择 **Microsoft O365 身份验证：读取/写入 (Microsoft O365 Authentication:Read/Write)**模式，则应立即验证您的**自动补救(AutomatedRemediation)**设置。要将自动补救应用于所有内部邮件，请确保选中**对不在域列表中的域应用自动补救(Apply auto-remediation to domains not in the domain list)**。一旦导入域，您就可以打开**自动补救策略 (Automated Remediation Policy)** 开关。

导入 Microsoft 邮件域

Secure Email Threat Defense 从 Microsoft 365 租户导入具有邮件功能的域。导入您的域，以便对特定域应用自动补救。根据您是否选中了**对不在域列表中的域应用自动补救 (Apply auto-remediation to domains not in the domain list)** 框，Secure Email Threat Defense 会对新导入的域进行不同的处理：

- 如果选中了**对不在域列表中的域应用自动补救(Apply auto-remediation to domains not in the domain list)**，则自动补救将应用于导入的任何新域。
- 如果未选中**对不在域列表中的域应用自动补救(Apply auto-remediation to domains not in the domain list)**，则则自动补救不会应用于导入的任何新域。

默认情况下不会选中**对不在域列表中的域应用自动补救 (Apply auto-remediation to domains not in the domain list)**。

手动导入

要手动导入 Microsoft 365 邮件域（建议在首次设置 Secure Email Threat Defense 时使用）：

1. 导航至**设置**（齿轮图标）> **策略 (Policy)**。
2. 点击**更新导入的域 (Update Imported Domains)** 按钮，将您的域导入 Secure Email Threat Defense 中。
3. 使用每个域旁边的复选框来调整该域的自动补救设置。
4. 我们还建议选中**对不在域列表中的域应用自动补救(Apply auto-remediation to domains not in the domain list)**，以确保将自动补救应用于所有内部邮件以及以后自动导入的任何域。
5. 点击**保存并应用**。

自动导入

域每 24 小时会自动导入一次，以确保列表保持最新。

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。