与思科 SecureX 威胁响应集成

本章包含以下各节：

将邮件网关与思科 SecureX 威胁响应集成

思科 SecureX 是嵌入到每个思科安全产品中的安全平台。它采用云原生，无需部署新技术。思科 SecureX 提供的平台统一了可视性，实现了自动化，并增强了您在网络、终端、云和应用中的安全性，从而简化了威胁保护的要求。通过集成平台中的连接技术，思科 SecureX 提供了可衡量的洞察力、预期成果以及无与伦比的跨团队协作。思科 SecureX 通过连接您的安全基础设施来大幅提升您的能力。

将邮件网关与思科 SecureX 威胁响应集成包括以下部分：

您可以将邮件网关与思科 SecureX 威胁响应集成，并在思科 SecureX 威胁响应中执行下列操作：

- 查看和发送来自组织中多个邮件网关的邮件数据。
- 识别、调查和补救在邮件报告、发件人和目标关系中观察到的威胁，搜索多个邮件地址和主题行以及邮件跟踪。
- 阻止受侵害的用户或违反传出邮件策略的用户。
- 快速解决已识别的威胁，并针对已识别的威胁提供建议的操作。
- 记录威胁以保存调查结果，并启用其他设备之间的信息协作。
- 阻止恶意域，跟踪可疑观察结果，启动审批工作流程或创建 IT 故障单以更新邮件策略。

您可以通过以下 URL 来访问思科 SecureX 威胁响应：

https://securex.us.security.cisco.com/login

思科安全邮件网关包括高级威胁防护功能，可以更快地检测、阻止威胁并进行补救，防止数据丢失，并通过端到端加密在传输过程中保护重要信息。有关可通过 ESA 模块充实的可观察对象的更多信息，请转至https://securex.us.security.cisco.com/settings/modules/available并导航至与思科 SecureX 集成的模块，然后单击**了解更多**。

如何将邮件网关与思科 SecureX 威胁响应集成

表 *1:* 如何将邮件网关与思科 *SecureX* 威胁响应集成

	相应操作	更多信息
第 1 步	查看先决条件。	前提条件，第 3 页
第 2 步	[仅适用于使用经典许可模式的用户]。 **注释** 如果您使用的是智能许可模式，则可以跳过此步骤，因为邮件网关会自动启用思科云服务门户。 在邮件网关上启用思科云服务门户。	在邮件网关上启用思科云服务门户，第 4 页
第 3 步	在思科 SecureX 上，将您的邮件网关添加为设备，为其注册并生成注册令牌。	有关详细信息，请转至 https://securex.us.security.cisco.com/help/settings-devices
第 4 步	[仅适用于使用经典许可模式的用户]。 **注释** 如果您使用的是智能许可模式，则可以跳过此步骤，因为邮件网关会自动向思科云服务门户注册。 向思科云服务门户注册您的邮件网关。	在思科云服务门户注册邮件网关，第 4 页
第 5 步	确认注册是否成功。	确认注册是否成功，第 5 页
第 6 步	在邮件网关上启用思科 SecureX 威胁响应	在邮件网关上启用思科 SecureX 威胁响应，第 5 页

	相应操作	更多信息
第 7 步	在思科 SecureX 上添加思科安全邮件网关模块。	有关详细信息，请转至 https://securex.us.security.cisco.com/settings/modules/available，导航至要与思科 SecureX 集成的思科安全邮件网关模块，单击**添加新模块”(Add New Module)**，然后查看页面上的说明。

前提条件

注释 如果您已有思科威胁响应用户账号，则无需创建思科 SecureX 用户账号。您可以使用思科威胁响应用户账号凭证来登录思科 SecureX。

- 请确保在思科 SecureX 中创建一个具有管理员访问权限的用户账号。要创建新用户账号，请使用 URL https://securex.us.security.cisco.com/login转至**思科 SecureX 登录 (Cisco SecureX login)**页面，然后在登录页面中单击**创建 SecureX 登录帐户 (Create a SecureX Sign-on Account)**。如果您无法创建新用户账号，请联系思科 TAC 寻求帮助。
- [仅当没有使用代理服务器时。]确保为以下 FQDN 打开防火墙上的 HTTPS（入和出）443 端口，以便向思科 SecureX 威胁响应注册邮件网关：
  - api-sse.cisco.com（仅适用于 NAM 用户）
  - api.eu.sse.itd.cisco.com（仅适用于欧盟 (EU) 用户）
  - api.apj.sse.itd.cisco.com（仅适用于亚太、日本和中国用户）
  - est.sco.cisco.com（适用于亚太、日本和中国、欧盟和 NAM 用户）

  有关详细信息，请参阅 防火墙资讯。
- [对于在邮件网关上注册了智能许可的用户] 确保已将您的智能帐户（在思科智能软件管理器门户中创建）与思科安全服务交换相关联。有关详情，请参阅以下文档：
  - [适用于 NAM 用户] https://admin.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html
  - [适用于欧盟 (EU) 用户] https://admin.eu.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html
  - [适用于亚太、日本和中国用户] https://admin.apj.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html

在邮件网关上启用思科云服务门户

过程

步骤 1 登录您的邮件网关。

步骤 2 选择**网络 (Networks)** > **云服务设置 (Cloud Service Settings)**。

步骤 3 单击**启用 (Enable)**。

步骤 4 选中**启用思科云服务 (Enable Cisco Cloud Services)** 复选框。

步骤 5 选择所需的思科安全服务器，以便将您的邮件网关连接到思科云服务门户。

步骤 6 提交并确认更改。

步骤 7 等待几分钟，然后检查“云服务设置”(Cloud Services Settings) 页面上是否出现了**注册 (Register)** 按钮。

在集群配置中，您只能在计算机模式下向思科云服务门户注册所登录的邮件网关。如果您已在单机模式下向思科云服务门户注册邮件网关，请确保在将其加入集群之前手动取消注册该邮件网关。

注释 要使用 CLI 启用思科云服务门户，请使用 `cloudserviceconfig` 命令。

下一步做什么

向思科云服务门户注册您的邮件网关。有关详细信息，请转至https://securex.us.security.cisco.com/settings/modules/available，导航至与思科 SecureX 集成的模块，单击**添加新模块 (Add New Module)**，然后查看页面上的说明。

在思科云服务门户注册邮件网关

过程

步骤 1 前往**网络 (Networks)** > **云服务设置 (Cloud Service Settings)**。

步骤 2 在“云服务设置”(Cloud Services Settings) 中输入注册令牌，然后单击**注册 (Register)**。

注释 要使用 CLI 向或思科云服务门户注册您的邮件网关，请使用 `cloudserviceconfig` 命令。

下一步做什么

确认注册是否成功，第 5 页

确认注册是否成功

- 在安全服务交换上，通过查看安全服务交换中的状态来确认注册是否成功。
- 在思科 SecureX 上，导航至**设备 (Devices)** 页面并查看已向安全服务交换注册的 ESA。

注释 如果要切换到其他思科 SecureX 威胁响应服务器（例如，“Europe - api.eu.sse.itd.cisco.com”），则必须先从思科 SecureX 威胁响应中注销您的邮件网关，然后按照如何将邮件网关与思科 SecureX 威胁响应集成，第 2 页中的步骤执行操作。

在将邮件网关与思科SecureX威胁响应集成后，无需将思科安全管理器邮件和网络网关与思科SecureX威胁响应集成。

在安全服务交换上成功注册邮件网关后，请在思科 SecureX 上添加 ESA 邮件模块。有关详细信息，请转至https://securex.us.security.cisco.com/settings/modules/available，导航至与思科 SecureX 集成的模块，单击**添加新模块 (Add New Module)**，然后查看页面上的说明。

在邮件网关上启用思科 SecureX 威胁响应

过程

步骤 1 登录您的邮件网关。

步骤 2 选择**网络 (Networks)** > **云服务设置 (Cloud Service Settings)**。

步骤 3 选中 SecureX 下的**启用 (Enable)** 复选框。

步骤 4 提交并确认更改。

使用思科 SecureX 功能区执行威胁分析

注释 在从思科安全邮件网关 13.5.1 或更早版本升级时，**案例集**将成为思科 SecureX 功能区的一部分。

思科 SecureX 支持分布式功能集，可统一可视性、实现自动化、加速事件响应工作流程并改善威胁搜索。这些分布式功能以思科 SecureX 功能区中的应用程序（应用）和工具的形式呈现。

本主题包含以下部分：

- 访问思科 SecureX 功能区， 第 6 页
- 使用思科 SecureX 功能区和透视菜单将可观察对象添加到案例集中以进行威胁分析， 第 7 页

您会在页面的底部窗格中找到思科 SecureX 功能区，当您在环境中的控制面板和其他安全产品之间移动时，它会始终显示。思科 SecureX 功能区包含以下图标和元素：

- 展开/折叠功能区
- 主页
- 案例集应用
- 事件应用
- Orbital 应用
- 增强搜索框
- 查找可观察对象
- 设置

有关思科 SecureX 功能区的详细信息，请参阅 https://securex.us.security.cisco.com/help/ribbon。

访问思科 SecureX 功能区

开始之前

确保您满足前提条件， 第 3 页中提到的所有前提条件。

注释 假设您已为思科安全邮件网关13.5.1或更早版本配置了**案例集**。您需要在思科 SecureX API 客户端中创建具有其他范围的新**客户端 ID**和**客户端密钥**，如以下程序所述。

您可以使用  按钮从右侧拖动位于页面底部窗格的思科 SecureX 功能区。

过程

步骤 1 登录邮件网关的新 Web 界面。有关详细信息，请参阅 访问基于 Web 的图形用户界面 (GUI)。

步骤 2 单击思科 SecureX 功能区。

步骤 3 在 **SecureX API 客户端**中创建**客户端 ID** 及**客户端密钥**。有关生成 API 客户端凭证的详细信息，请参阅创建 API 客户端。

在创建客户端 ID 和客户端密码时，请确保选择以下范围：

- casebook

- enrich:read
- global-intel:read
- inspect:read
- integration:read
- profile
- private-intel
- response
- registry/user/ribbon
- telemetry:write
- users:read
- orbital（如果您有访问权限）

步骤 4 在您的邮件网关的**要使用 SecureX 功能区，请登录 (Login to use SecureX Ribbon)** 对话框中输入在步骤 3 中获取的客户端 ID 和客户端密码。

步骤 5 在**要使用 SecureX 功能区，请登录 (Login to use SecureX Ribbon)** 话框中选择所需的思科 SecureX 服务器。

步骤 6 单击**身份验证 (Authentication)**。

注释 如果要编辑客户端 ID、客户端密码和思科 SecureX 服务器，请右键单击思科 SecureX 功能区并添加详细信息。

下一步做什么

使用思科 SecureX 功能区和透视菜单将可观察对象添加到案例集中以进行威胁分析，第 7 页

使用思科 SecureX 功能区和透视菜单将可观察对象添加到案例集中以进行威胁分析

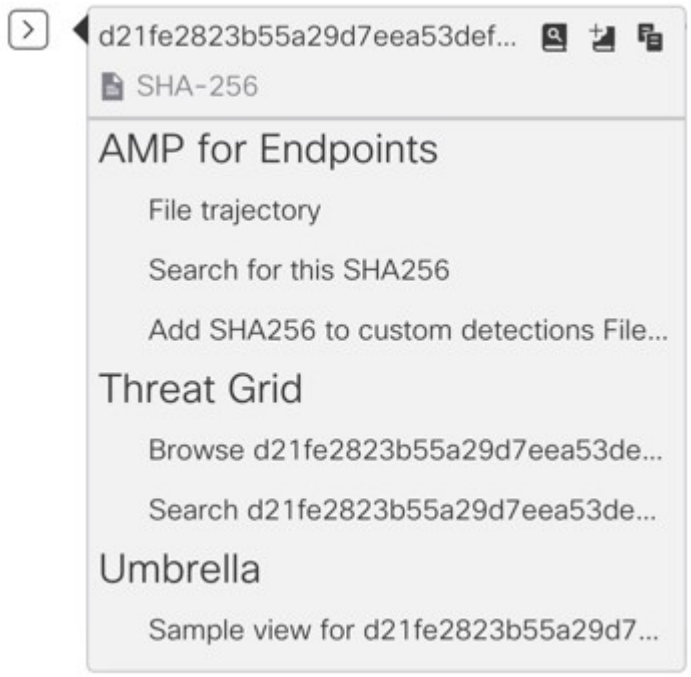
开始之前

确保获取客户端 ID 和客户端密码，以访问邮件网关上的思科 SecureX 功能区和数据透视菜单小组件。有关详细信息，请参阅 访问思科 SecureX 功能区，第 6 页。

过程

步骤 1 登录邮件网关的新 Web 界面。有关详细信息，请参阅 访问基于 Web 的图形用户界面 (GUI)。

步骤 2 导航至**邮件报告 (Email Reporting)** 页面，单击所需可观察对象（例如，bit.ly）旁边的透视菜单按钮。



请执行以下操作：

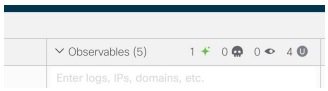
- 单击 按钮可将一个可观察对象添加到活动案例。
- 单击 按钮将可观察对象添加到新案例。

注释 使用透视菜单 按钮将可观察对象绕过门户上注册的其他设备（例如面向终端的 AMP）进行调查，以便进行威胁分析。

步骤 3 将鼠标悬停在 图标上，然后单击 按钮打开**案例集**。检查可观察对象是否已添加到新案例或现有案例。

步骤 4 （可选）单击 按钮可向**案例集**添加标题、说明或备注。

注释 您可以通过两种不同的方式搜索可观察对象以进行威胁分析：

- 单击思科 SecureX 功能区中的**增强 (Enrichment)**  搜索框，然后搜索可观察对象。
- 单击思科 SecureX 功能区内的**案例集**图标，然后在搜索  字段中搜索可观察对象。

有关思科 SecureX 功能区的详细信息，请参阅 https://securex.us.security.cisco.com/help/ribbon。

对思科 SecureX 威胁响应中的邮件执行补救操作

在思科 SecureX 威胁响应中，您现在便可对邮件网关处理的邮件进行调查并采取以下补救操作：

- 删除
- 转发
- 转发并删除

开始之前

在对思科 SecureX 威胁响应中的邮件执行补救操作之前，请确保满足以下前提条件：

- 启用并向思科 SecureX 服务器注册了您的邮件网关。有关详细信息，请参阅 如何将邮件网关与思科 SecureX 威胁响应集成，第 2 页。
- 向思科 SecureX 添加了邮件网关模块，并在思科 SecureX 中指定了补救转发地址。有关详细信息，请转至https://securex.us.security.cisco.com/settings/modules/available，导航至要与思科 SecureX 集成的思科安全邮件网关模块，单击“添加新模块”(Add New Module)，然后查看页面上的说明。
- 在邮件网关的“系统管理”(System Administration) > “帐户设置”(Account Settings) 页面中启用并配置了补救配置文件。有关详细信息，请参阅 补救邮箱中的邮件。

过程

步骤 1 使用用户凭证登录思科 SecureX。

步骤 2 通过在调查面板中输入所需的 IOC（例如，URL、邮件消息 ID 等）并单击**调查 (Investigate)**，以便执行威胁分析调查。有关详细信息，请参阅“帮助”部分的“调查”主题，网址为 https://visibility.amp.cisco.com/help/investigate。

步骤 3 根据调查结果，使用相应的**思科邮件 ID** 或**邮件 MessageID** 来选择所需的邮件。有关详细信息，请参阅“帮助”部分的“调查”主题，网址为 https://visibility.amp.cisco.com/help/investigate。

步骤 4 单击思科邮件 ID 或邮件 MessageID 旁边的透视菜单  按钮，然后选择所需的补救操作（例如，“转发 (Forward)”）。有关详细信息，请参阅“帮助”部分的“调查”主题，网址为 https://visibility.amp.cisco.com/help/investigate

使用思科成功网络改善邮件网关的用户体验

概述

您可以使用思科成功网络 (CSN) 功能，以便将邮件网关和功能使用情况等详细信息发送给思科。这些详细信息供思科用于识别邮件网关版本以及您的邮件网关上已激活但尚未启用的功能。

将您的邮件网关和功能使用情况等详细信息发送给思科可帮助组织：

- 通过对收集的遥测数据执行分析并使用数字活动向用户提供建议，从而提高产品在用户网络中的有效性。
- 通过邮件网关改善用户体验。

下表显示了发送到思科的邮件网关和功能使用情况等详细信息的示例数据：

统计信息	示例数据
邮件网关详细信息	
UID	4215XXXXXXXXXXXXXXXX-XXXXXXXXXXXX
型号	C100V
sIVAN	邮件网关（适用于智能许可证）或 null（适用于经典许可证）
部署	集群/独立。
userAccountID	输入 SLPIID（智能许可证中）或 VLNID（经典许可证中）。
版本	1X.X.X-XXX
安装日期	1582535814000（自纪元以来的毫秒数）
功能信息	
名称	邮件网关功能
启用	支持
状态 (Status)	合规
过期日期	1831591683（自纪元以来的秒数）

统计信息	示例数据
功能 ID	a4deXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

相关主题

- 在邮件网关上启用 CSN，第 11 页
- 在邮件网关上禁用 CSN，第 11 页

在邮件网关上启用 CSN

开始之前

确保启用邮件网关并向思科云服务门户注册。有关详细信息，请参阅如何将邮件网关与思科 SecureX 威胁响应集成，第 2 页。

过程

步骤 1 转到**安全服务 (Security Services)** > **云服务设置 (Cloud Service Settings)**。
步骤 2 单击**编辑全局设置**。
步骤 3 选中**启用**思科成功网络下方的复选框。
步骤 4 提交并确认更改。

在邮件网关上禁用 CSN

过程

步骤 1 转到**安全服务 (Security Services)** > **云服务设置 (Cloud Service Settings)**。
步骤 2 单击**编辑全局设置**。
步骤 3 取消选中思科成功网络下的**启用 (Enable)** 复选框。
步骤 4 提交并确认更改。