



与思科 SecureX 或思科威胁响应 集成

本章包含以下主题：

[将设备与思科 SecureX 或思科威胁响应 集成 ， 第 1 页](#)

- [将设备与思科 SecureX 或思科威胁响应 集成 ， 第 1 页](#)

将设备与思科 SecureX 或思科威胁响应 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。

思科 思科威胁响应 是一个威胁事件响应协调中心，支持多个思科安全产品之间的集成并实现自动化。作为思科集成安全架构的一个关键支柱，威胁响应加速了关键的安全运营功能：检测、调查和补救。

设备与思科 SecureX 或思科威胁响应 的集成包括以下 部分：

- [如何将设备与思科 SecureX 或思科威胁响应 集成 ， 第 2 页](#)
- [使用思科 SecureX 功能区执行威胁分析](#)

您可以将设备与思科 SecureX 或思科威胁响应 集成，并在思科 SecureX 或思科威胁响应 中执行下列操作：

- 查看和发送来自组织中多个设备的邮件数据。
- 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：

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

思科安全管理设备 (SMA) 可以将多个思科邮件安全设备的管理及报告功能集中到一起。有关可通过 SMA 电子邮件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，然后点击 [了解更多](#)。

如何将设备与思科 SecureX 或思科威胁响应 集成

表 1: 如何将设备与思科 SecureX 或思科威胁响应 集成

	相应操作	更多信息
第 1 步	查看前提条件。	前提条件
第 2 步	在您的安全管理设备上，启用思科 SecureX 或思科威胁响应 集成。	在您的安全管理设备上，启用思科 SecureX 集成，第 3 页
第 3 步	在思科 SecureX 上，将设备作为设备进行添加、注册并生成注册令牌。	有关详细信息，请转到 https://securex.us.security.cisco.com/help/settings-devices 。
第 4 步	在您的安全管理设备上，完成思科 SecureX 或思科威胁响应 注册。	在您的安全管理设备上使用 Cisco SecureX 或 Cisco Threat Response 注册，第 3 页
第 5 步	确认注册是否成功。	确认注册是否成功
第 6 步	在思科 SecureX 上，添加 SMA 邮件 模块。	有关详细信息，请转至 https://securex.us.security.cisco.com/settings/modules/available ，然后导航至与思科 SecureX 集成的模块，点击 添加新模块 ，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 **Cisco SecureX 登录** 页面，然后在登录页面中点击 **创建 SecureX 登录账户**。如果您无法创建新用户账号，请联系思科 TAC 寻求帮助。

- [仅当不使用代理服务器时] 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 或思科威胁响应 注册设备：
 - 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 [防火墙信息](#)。

在您的安全管理设备上，启用思科 SecureX 集成。

步骤 1 登录到设备。

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

步骤 3 点击编辑全局设置 (Edit Global Settings)。

步骤 4 选中启用复选框。

步骤 5 提交并确认更改。

步骤 6 等待几分钟，然后检查设备上是否出现了注册 (Register) 按钮。



注释 在集群配置中，只能在计算机模式下向思科 SecureX 或思科威胁响应 注册已登录的设备。如果您已在单机模式下向思科 SecureX 或思科威胁响应 注册设备，请确保手动取消该设备的注册，然后您才能将其加入集群。



注释 要使用 CLI 启用该集成，请使用 `threatresponseconfig` 命令。

下一步做什么

在思科 SecureX 或思科威胁响应 中注册设备。有关详细信息，请转至 <https://securex.us.security.cisco.com/settings/modules/available>，然后导航至与思科 SecureX 集成的模块，点击开始，然后查看页面上的说明。

在您的安全管理设备上使用 Cisco SecureX 或 Cisco Threat Response 注册

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，然后点击注册 (**Register**)。



注释 要使用 CLI 来注册思科 SecureX 或思科威胁响应，请使用 `cloudserviceconfig` 命令。

下一步做什么

[确认注册是否成功](#)

向思科云服务门户重新注册

您可以根据以下任一场景向思科云服务门户重新注册本地思科安全邮件和 Web 管理器：

- 如果在自动向思科云服务门户注册思科安全邮件和 Web 管理器时无法查看或管理添加到思科云服务门户的设备（思科安全邮件和 Web 管理器）。
- 如果在向思科云服务门户自动注册思科安全邮件和 Web 管理器时，智能账户和思科云服务帐户未关联。

您还可以在 CLI 中使用 `cloudserviceconfig > reregister` 子命令向思科云服务门户重新注册思科安全邮件和 Web 管理器。

开始之前

确保您已满足以下前提条件：

- 已在思科安全邮件和 Web 管理器上启用智能软件许可。
- 向思科智能软件管理器注册思科安全邮件和 Web 管理器。

步骤 1 转到思科安全邮件和 Web 管理器上的网络 (Networks) > 云服务设置 (Cloud Service Settings) 页面。

步骤 2 点击重新注册 (**Reregister**)。

注释 点击重新注册后，您可以根据需要选择是要执行第 3 步还是第 4 步，还是同时执行第 2 步中的任务。

步骤 3 [可选] 如果您的思科安全邮件和 Web 管理器自动注册了不正确的思科安全服务器，请选择适当的思科安全服务器将设备连接到思科云服务门户。

步骤 4 [可选] 如果思科安全邮件和 Web 管理器已使用不正确的智能帐户自动注册，则输入从思科云服务门户获取的注册令牌。

步骤 5 点击提交 (**Submit**)，只有当您在第 4 步中未输入注册令牌时才会显示“确认重新注册” (Confirm reregistration) 对话框。

步骤 6 点击“确认重新注册” (Confirm reregistration) 对话框中的提交 (**Submit**)，以便允许思科云服务使用从思科云服务门户自动生成的令牌以及智能帐户信息，从而向思科云服务门户重新注册思科安全邮件和 Web 管理器。

确认注册是否成功

- 在安全服务交换，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，导航到本地设备页面 (<https://xdr.us.security.cisco.com/administration/on-premise-appliances>)，查看已向安全服务交换 注册的 SMA 。



注释

如果要切换到其他 Cisco SecureX or Cisco Threat Response 服务器（例如，“Europe - api.eu.sse.itd.cisco.com”），则必须先从 Cisco SecureX or Cisco Threat Response 中注销您的设备，然后按照 [如何将设备与思科 SecureX 或思科威胁响应 集成，第 2 页](#) 中的步骤执行操作。

将设备与 Cisco SecureX or Cisco Threat Response 集成后，您无需将邮件安全设备与 Cisco SecureX or Cisco Threat Response 集成，因为邮件和 Web 报告功能本身就是集中式的。

在安全服务交换上成功注册设备后，请在 Cisco SecureX 上添加 SMA 邮件模块。有关详细信息，请转至 <https://securex.us.security.cisco.com/settings/modules/available>，然后导航至与思科 SecureX 集成的模块，并点击添加新模块，然后查看页面上的说明。

在内容安全网关上启用思科 SecureX 或威胁响应

步骤 1 登录到设备。

步骤 2 依次选择网络 > 云服务设置。

步骤 3 点击启用 (Enable)。

步骤 4 选中启用云服务 (Enable Cloud Service) 复选框。

步骤 5 选择思科 SecureX 服务器。

步骤 6 提交并确认更改。

在内容安全网关上启用思科云服务门户

步骤 1 登录您的邮件网关。

步骤 2 依次选择网络 > 云服务设置。

步骤 3 点击启用 (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。等待几分钟，然后检查内容安全网关上是否出现了“注册” (Register) 按钮。

下一步做什么

使用思科 SecureX 功能区执行威胁分析



注释 在从安全管理设备 13.6.1 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](#)
- [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](#)

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](#)中提到的所有前提条件。



注释 假设您已为安全管理设备 13.6.1 或更早版本配置了**案例集**，则需要在思科 SecureX API 客户端中使用其他范围来创建**客户端 ID**和**客户端密钥**，如下程序所述。

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。

步骤 1 登录设备的新 Web 界面。有关详细信息，请参阅[访问 Web 界面](#)。

步骤 2 点击思科 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 在设备的要使用 **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**) 对话框中选择所需的思科 SecureX 服务器。

步骤 6 点击身份验证 (**Authentication**)。

注释 如果要编辑客户端 ID、客户端密码和思科 SecureX 服务器，请右键点击思科 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](#)

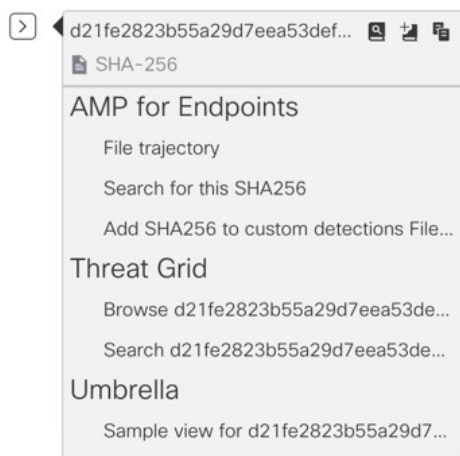
使用思科 SecureX 功能区和透视菜单将可观察对象添加到案例集中以进行威胁分析

开始之前



确保获取客户端 ID 和客户端密码，以访问设备上的思科 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](#)。

步骤 1 登录设备的新 Web 界面。有关详细信息，请参阅[访问 Web 界面](#)。


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




请执行以下操作：

- 点击  按钮可将一个可观察对象添加到活动案例。
- 点击  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（例如面向终端的高级恶意软件防护）进行调查，以便进行威胁分析。


步骤 3 将鼠标悬停在  图标上，然后点击  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）点击  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：

- 点击思科 SecureX 功能区中的增强 (Enrichment)  搜索框，然后搜索可观察对象。

- 点击思科 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

开始之前

在思科威胁响应中，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

在对思科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 服务器注册思科安全邮件和 Web 管理器。有关详细信息，请参阅在思科内容安全设备上启用思科 SecureX 或 Cisco Threat Response 集成，以及在思科内容安全设备上注册 SecureX 或 Cisco Threat Response。
- 将您的安全电子邮件和 Web 管理器模块添加到 Cisco SecureX，并在 Cisco 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 Cisco SecureX 集成的安全邮件和网页管理器模块，点击添加新模块，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，请参阅思科安全邮件网关用户指南中“补救邮箱中的邮件”一章。

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）并点击调查 (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 点击思科邮件 ID 或邮件消息 ID 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“透视菜单”主题，网址为 <https://visibility.amp.cisco.com/help/investigate>。

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。