# 使用 Cisco Defense Orchestrator 管理 ASA

**首次发布日期:** 2021 年 3 月 10 日

**上次修改日期:** 2024 年 4 月 18 日

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# 目录

# 使用 Cisco Defense Orchestrator 管理 ASA



# 使用 Cisco Defense Orchestrator 管理 ASA

Cisco Defense Orchestrator (CDO) 是一种基于云的多设备管理器，可提供一种简单、一致且安全的方式来管理所有 ASA 设备上的安全策略。

本文档的目标是为 Cisco Defense Orchestrator (CDO) 的新客户提供可用于标准化对象和策略、升级受管设备以及管理 VPN 策略和监控远程工作人员的活动大纲。本文档假设如下：

- 您已开设 30 天试用账户，或者您已购买 CDO，并且思科已为您创建 CDO 租户。
- 您已为CDO中的用户角色用户设置了 新 CDO 租户的初始登录，第 3 页。
- 您的 ASA 已配置，您正在企业中使用它。
- 如果您希望 CDO 管理的 ASA 无法直接从互联网访问，则需要在网络中部署安全设备连接器 (SDC)。SDC 管理 CDO 和 ASA 之间的通信。有关详细信息，请参阅使用 CDO 的 VM 映像部署安全设备连接器，第 10 页或在您自己的虚拟机上部署安全设备连接器，第 14 页。

### 立即行动

#### 安全设备连接器

使用设备凭证将 CDO 连接到 ASA 时，最佳实践是在网络中下载并部署安全设备连接器 (SDC)，以管理 CDO 与 ASA 之间的通信。ASA 都可以使用设备凭证载入到 CDO。如果您不希望 SDC 管理 ASA 和 CDO 之间的通信，并且可以直接从互联网访问您的设备，则无需在网络中安装 SDC。可以使用云连接器将 ASA 载入 CDO。

通过为租户部署多个SDC，您可以通过CDO租户来管理更多设备，而不会出现性能下降。单个SDC可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。但是，出于规划部署的目的，我们预计一个 SDC 可支持大约 500 台设备。

查看 SDC：

1. 登录 CDO。

使用 Cisco Defense Orchestrator 管理 ASA

2. 从 CDO 菜单中选择**管理 (Admin)** > **安全连接器 (Secure Connectors)**。

### 载入设备

您可以批量载入 ASA或将 ASA 设备载入 CDO地将 ASA 载入 CDO。有关 CDO 支持的 ASA 软件和硬件的讨论，请参阅ASA 支持详情，第 35 页。

### 在租户上创建其他 CDO 用户

Cisco Defense Orchestrator (CDO) 中有多种用户角色：只读、仅编辑、仅部署、管理员和超级管理员。为每个租户上的每个用户配置用户角色。如果CDO用户可以访问多个租户，则他们可能具有相同的用户 ID，但在不同的租户中具有不同的角色。当接口或文档提及只读用户、管理员用户或超级管理员用户时，我们描述的是该用户对特定租户的权限级别。请参阅CDO中的用户角色，第61页，了解授予不同类型用户的权限。

创建租户时，系统会自动为您分配超级管理员用户。超级管理员能够在您的租户上创建其他用户。对于要连接到租户的新用户，他们需要拥有或创建一个使用与其在CDO中的用户记录相同的电子邮件地址的 Cisco Secure Sign-On 帐户。请参阅将用户帐户添加到 CDO，第 66 页，在 CDO 中创建用户记录。

### 策略编排

策略协调涉及查看对象和策略。请记住，使用ASA策略时，CDO将“访问组”称为“访问策略”。当您查找 ASA 访问策略时，您可以从 CDO 菜单栏策略 > ASA 访问策略进行导航。

### 解决网络对象问题

多年来，您的安全设备上可能有不再使用的对象，这些对象与其他对象重复，或者其值在设备之间不一致。通过修复这些对象问题开始您的协调任务。


按以下顺序处理对象问题。您在早期步骤中所做的工作可能会解决您在后续步骤中必须解决的许多问题：

1. 解决未使用的对象问题。未使用的对象 是设备中存在但未被其他对象、访问列表或 NAT 规则引用的对象。
2. 解决重复对象问题。重复对象 是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常是意外创建的，可用于类似的目的，并供不同的策略使用。解决重复对象问题后，CDO 会使用保留的对象名称来更新所有受影响的对象引用。
3. 解决不一致的对象问题。不一致对象 是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。这可能是一个安全问题。您可能有一条保护过时资源的规则。

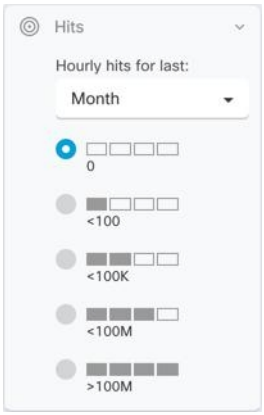
使用 Cisco Defense Orchestrator 管理 ASA

### 修复影子规则

现在，您已解决网络对象问题，请查看影子规则的网络策略并进行修复。影子规则，第 194 页**影子规则**在 ASA 访问策略页面上用半月形标记 ◑ 进行标记。访问策略中的规则在列表中进行配置，并从上到下一次评估一个。策略中的影子规则永远不会匹配，因为网络流量与策略中的影子规则上方的规则相匹配。如果存在永远不会命中的影子规则，请将其删除，或编辑 ASA 网络策略以使规则生效。

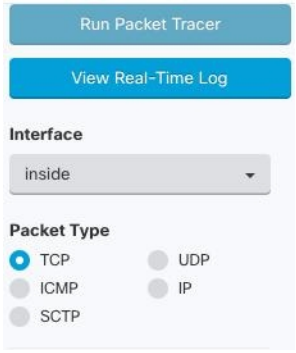
### 评估策略命中率

确定策略中的规则是否实际评估网络流量。CDO 每小时收集一次有关策略中规则的命中率数据。您的设备由 CDO 管理的时间越长，特定规则的命中率数据就越有意义。按您感兴趣的时间段内的命中计数过滤 ASA 访问策略，以查看其是否受到命中。如果不是，请考虑重写策略或将其删除。




### 策略故障排除

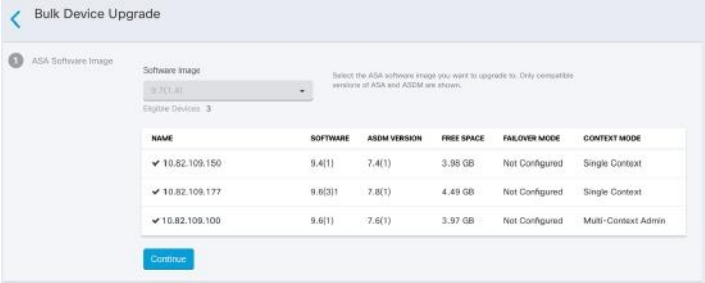
您可以使用 ASA 数据包跟踪器 通过策略测试合成数据包的路径，并确定规则是否无意中阻止或允许访问。




### 升级 ASA 和 ASDM

接下来，升级到最新版本的 ASA 和 ASDM。客户报告称，使用 CDO 升级其 ASA 可节省 75%-90% 的时间。

使用 Cisco Defense Orchestrator 管理 ASA




CDO 提供的向导让您能够在单情景或多情景模式下升级单个 ASA 或多个 ASA 上安装的 ASA 和 ASDM 映像。CDO 维护 ASA 和 ASDM 映像的数据库。

CDO 在后台执行必要的升级兼容性检查。该向导将指导您选择兼容的 ASA 和 ASDM 映像，安装这些映像并重新启动设备以完成升级。CDO 会验证您在 CDO 上选择的映像是否是复制到并安装在 ASA 上的映像，从而确保升级过程的安全。

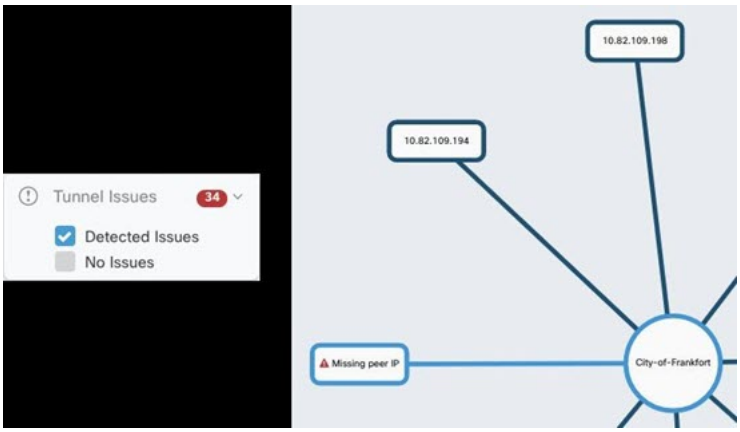
CDO 会定期查看其数据库并向其添加最新的 ASA 和 ASDM 映像。CDO 仅支持正式发布 (GA) 映像，不会将自定义映像添加到其数据库。如果您在列表中没有看到特定的 GA 映像，请通过**联系支持人员 (Contact Support)** 页面联系思科 TAC。我们将使用已建立的支持请求 SLA 处理请求，并上传缺少的 GA 映像。

查看在单个 ASA 上升级 ASA 和 ASDM 映像，第 147 页并继续使用您自己的存储库中的映像升级多个 ASA，第 145 页以了解有关升级 ASA 的更多信息。

### 监控和管理 VPN 连接

#### 查看站点间 VPN 问题

CDO 报告网络中 ASA 设备上存在的 VPN 问题。您可以通过两种方式查看您的环境，即显示 VPN 对等体列表的表或显示中心辐射型拓扑中的 VPN 连接的映射。使用过滤器边栏搜索需要注意的 VPN 隧道。




使用 CDO 评估您的 VPN 隧道：

- 检查站点间 VPN 隧道连接
- 查找缺少对等体的 VPN 隧道

使用 Cisco Defense Orchestrator 管理 ASA

- 查找存在加密密钥问题的 VPN 对等体
- 查找为隧道定义的不完整或配置错误的访问列表
- 查找隧道配置中的问题

### 板载非托管站点间 VPN 对等体

CDO 还标识非托管 VPN 对等体。识别这些设备后，请使用载入非托管站点间 VPN 对等体，第 232 页载入设备并使用 CDO 对其进行管理。

### ASA 远程访问 VPN 支持

CDO 允许创建远程访问虚拟专用网络 (RA VPN) 配置，以允许用户在通过 ASA 连接时安全地访问企业资源。当您的 ASA 载入 CDO 时，CDO 会识别已使用 ASDM 或思科安全管理器 (CSM) 配置的任何 RA VPN 设置，以便您可以使用 CDO 对其进行管理。

AnyConnect 是终端设备上通过 RA VPN 连接的唯一受支持客户端。

CDO 支持 ASA 设备上的 RA VPN 功能的以下方面：

- 基于 SSL 客户端的远程访问
- IPv4 和 IPv6 寻址
- 跨多台 ASA 设备共享 RA VPN 配置

有关详细信息，请参阅 为 ASA 配置远程访问虚拟专用网络，第 234 页。

### 监控设备配置同步

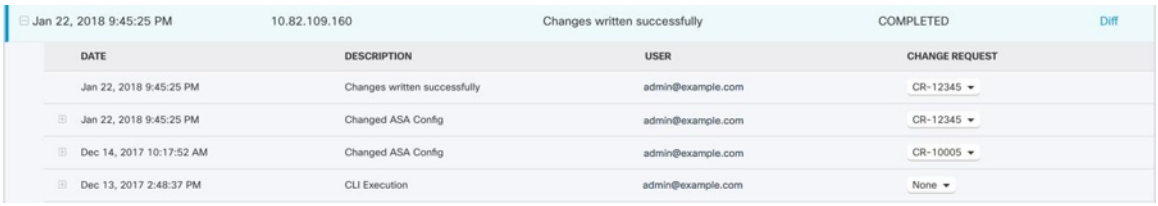
CDO 会定期将其数据库中存储的设备配置与 ASA 上安装的设备配置进行比较。您载入 CDO 的 ASA 仍可载入 ASA 仍可由设备的自适应安全设备管理器 (ASDM) 管理，因此 CDO 会确保其配置与设备上的配置相同，并会提醒您注意差异。有关“已同步”、“未同步”或“检测到冲突”设备状态的详细信息，请参阅冲突检测，第 323 页。

### 跟踪更改日志中的更改

您对设备配置所做的更改会记录在 中。变更日志，第 329 页更改日志显示的信息包括从 CDO 部署到设备的更改、从设备导入到CDO的更改、更改内容以及查看更改“差异”的功能、更改发生的时间以及执行者。

您还可以创建自定义标签，并将其应用到您所做的更改。更改请求管理，第 334 页在更改日志中，您可以按该自定义标签、日期范围、按特定用户或按更改类型过滤更改列表，以查找您要查找的内容。

使用 Cisco Defense Orchestrator 管理 ASA




### 恢复之前的配置

如果您对要“撤消”的ASA进行了更改，可以使用CDO将设备恢复为以前的配置。有关详细信息，请参阅 恢复 ASA 配置，第 99 页。

### 使用命令行接口和命令宏管理设备

CDO 是一种基于 Web 的管理产品，为您提供图形用户界面 (GUI) 和CDO 命令行界面 (CLI)，以便一次管理一个或多个设备。

ASA CLI 用户会喜欢我们的 CLI 工具的额外功能。以下是使用 CDO 的 CLI 工具而不是通过 SSH 会话连接到设备的一些原因：

- CDO知道命令所需的用户模式。您不需要提升或降低您的权限级别来执行命令，也不需要输入特定的命令上下文来执行命令。
- CDO保留了的命令历史记录需求链接，因此您可以通过从列表中选择命令来轻松地重新运行该命令。
- CLI 操作记录在更改日志中，因此您可以查看发送的命令和执行的操作。
- 命令可以在批量模式下运行，允许您同时将对象或策略部署到多个设备。
- CDO 用品 CLI 宏。CLI 宏是存储的即用命令，您可以按原样运行，或者可以完成并运行“填空”CLI 命令。您可以在一台设备上运行这些命令，也可以同时将命令发送到多个 ASA。
- CLI 为您提供完整的 ASA 配置文件。您可以查看它，或者如果您是高级用户，可以直接编辑它并保存更改，而不是发出 CLI 命令来更改它。

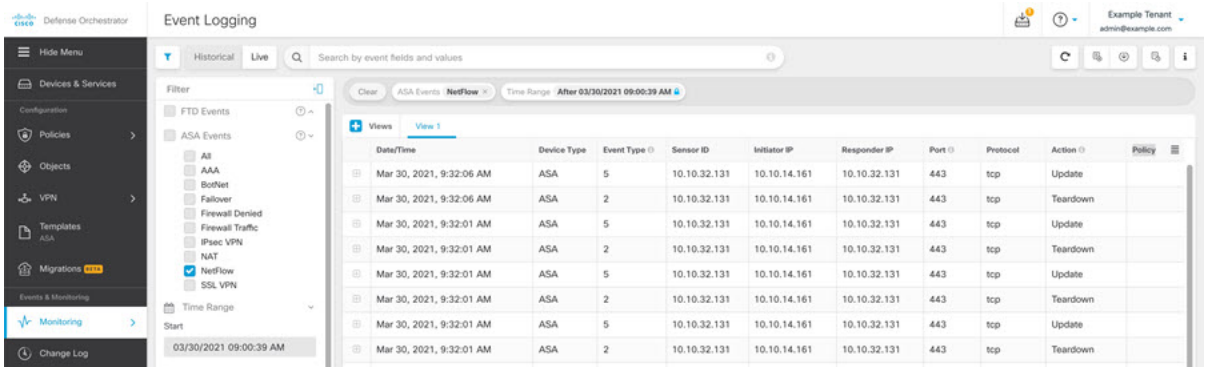
### 将 CDO 与 SecureX 集成

Cisco SecureX 平台思科 SecureX 结合了思科的集成安全产品组合以及客户基础设施的优势，旨在提供可统一可视性、实现自动化并增强网络、终端、云和应用安全性的一致体验。通过集成平台中的连接技术，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。您可以阅读有关以及如何操作的更多信息。SecureX和CDO，第 473 页将 CDO 添加到 SecureX，第 474 页

### 思科安全分析和日志记录

通过额外许可，思科安全分析和日志记录，第 341 页让您可以将系统日志事件和 Netflow 安全事件日志记录 (NSEL) 事件从 ASA 定向到 安全事件连接器，第 379 页 (SEC)，然后由 SEC 将其转发到思科云。进入云后，您可以在 CDO 的“事件日志记录”(Event Logging) 页面中查看这些事件。您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。

使用 Cisco Defense Orchestrator 管理 ASA




除了监控事件，您还可以从 CDO 启动 Secure Cloud Analytics 门户，以对记录的事件执行行为分析。

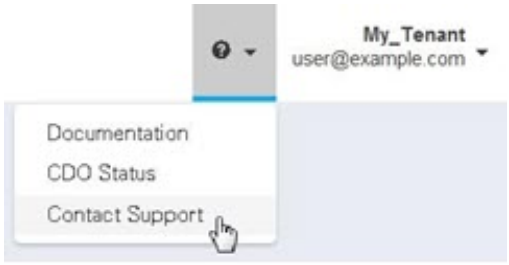
有关如何实施思科安全分析和日志记录的完整说明，请参阅为 ASA 设备实施安全日志记录分析 (SaaS)，第 350 页。

### 后续操作

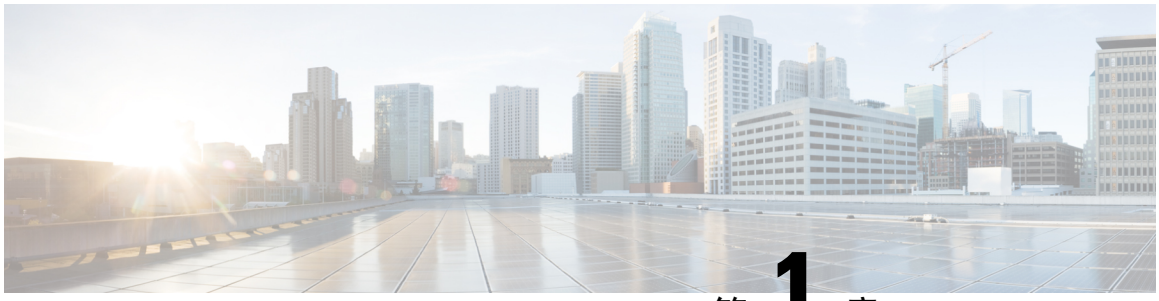
现在，您可以开始载入 ASA 并协调策略。

### 如果您需要帮助

您可以通过点击 CDO GUI 中的支持菜单联系思科威胁防御支持或阅读我们的产品文档。



使用 Cisco Defense Orchestrator 管理 ASA



第 1 章

# Cisco Defense Orchestrator 基础知识

( ) 通过清晰简洁的界面提供策略管理的独特视图。思科防御协调器CDO以下主题介绍了首次使用的基础知识。CDO

# 创建 CDO 租户

您可以调配新的 CDO 租户以载入和管理您的设备。如果您使用 本地防火墙管理中心 7.2 及更高版本，并希望将其与思科安全云集成，则还可以在集成工作流程中创建CDO租户。您可以联系思科客户团队将您的租户升级到许可的租户。

### 操作步骤

1. 转至https://www.defenseorchestrator.com/provision。
2. 选择要调配 CDO 租户的区域并点击**登录 (Sign Up)**。
3. 在 **Security Cloud Sign On** 页面上，提供您的凭据。
4. 如果您没有 安全云登录 帐户并想创建一个，请点击**立即注册 (Sign up now)**。
   a. 提供系统提示的信息，然后点击**注册 (Sign up)**。

      点击**注册 (Sign up)** 后，系统会向您提供的邮箱 ID 发送邮件，其中包含激活账户的链接。
   b. 点击邮件和 **Security Cloud Sign On** 页面上的**激活账户 (Activate account)**。
   c. 在您选择的设备上使用 Duo 配置多重身份验证，然后点击**通过 Duo 登录 (Log in with Duo)** 和**完成 (Finish)**。

**Note** 我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。

5. 为租户提供名称，然后点击**创建新帐户 (Create new account)**。
6. 在您选择的区域中创建了一个新的 CDO 租户；您还将收到有关正在创建的 CDO 租户的电子邮件，其中包含详细信息。如果您已与多个 CDO 租户关联，请在**选择租户 (Choose a tenant)** 页面上，选择您刚刚创建的租户以登录该租户。如果您是第一次创建新的 CDO 租户，则会直接登录到您的租户。

   有关首次登录 CDO 租户的信息，请参阅新 CDO 租户的初始登录。

   有关管理 CDO 租户和各种租户设置的信息，请参阅租户管理。

# 登录到 CDO

要登录 思科防御协调器 (CDO)，客户需要具有符合 SAML 2.0 标准的身份提供程序 (IdP)、多因素身份验证提供程序以及 在 CDO 中管理用户。

IdP 账户包含用户的凭证，IdP 根据这些凭证对用户进行身份验证。多因素身份验证提供了额外的身份安全层。CDO用户记录主要包含用户名、与其关联的CDO租户以及用户的角色。当用户登录时，CDO 会尝试将 IdP 的用户 ID 映射到 CDO 中租户的现有用户记录。当 CDO 找到匹配项时，用户已登录到该租户。

除非您的企业有自己的单点登录身份提供程序，否则身份提供程序是思科安全云登录。Cisco Security Cloud Sign On 使用 Duo 进行多因素身份验证。客户可以选择将 SAML 单点登录与 Cisco Defense Orchestrator 集成。

要登录 CDO，您必须首先在 Cisco Security Cloud Sign On 中创建一个账户，使用 Duo Security 来配置多因素身份验证 (MFA)，并让租户超级管理员创建 CDO 记录。

2019 年 10 月 14 日，CDO 将所有先前存在的租户转换为使用 Cisco Security Cloud Sign On 作为其身份提供程序和 Duo for MFA。

注释

- 如果您使用自己的单点登录身份提供程序登录 CDO，则转换到 Cisco Security Cloud Sign On 不会影响您。您可以继续使用自己的登录解决方案。
- 如果您正在免费试用 CDO，则此过渡确实会影响您。

如果您的 CDO 租户是在 2019 年 10 月 14 日或之后创建的，请参阅新 CDO 租户的初始登录，第 3 页。

如果您的 CDO 租户在 2019 年 10 月 14 日之前就已存在，请参阅迁移到 Cisco Security Cloud Sign On 身份提供程序，第 4 页。

# 新 CDO 租户的初始登录

### 准备工作

**安装 DUO Security**。我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。

**时间同步**。您要使用移动设备生成一次性密码。由于OTP是基于时间的，所以您的设备时钟与实时同步是非常重要的。请确保您的设备时钟自动或手动设置为正确的时间。

思科防御协调器 (CDO) 使用 Cisco Security Cloud Sign On 作为身份提供程序，并使用 Duo 进行多重身份验证 (MFA)。。如果您没有思科 安全云登录 账户，当您使用 https://www.defenseorchestrator.com/provision创建新的 CDO 租户时，调配流程涉及各种步骤，包括创建 安全云登录 账户和使用 Duo 配置 MFA。

MFA 为保护您的用户身份提供额外的一重保障。双因素身份验证（一种 MFA）需要两个部分或因素来确保登录CDO的用户身份真实。第一个因素是用户名和密码，第二个是按需生成的一次性密码 (OTP)。

重要事项 **如果您的 CDO 租户在 2019 年 10 月 14 日之前就已存在，**请使用 迁移到 Cisco Security Cloud Sign On 身份提供程序，第 4 页 登录说明，而不是本文。

### 后续操作？

请继续 创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 58 页。这是 4 步流程。您需要完成所有四个步骤。

# 登录失败故障排除

### 登录失败，因为您无意中登录到错误的 CDO 区域

请确保您登录的是适当的 CDO 区域。登录 https://sign-on.security.cisco.com 后，您可以选择要访问的区域。点击 **CDO** 磁贴访问 Defenseorchestrator.com 或点击 **CDO (EU)** 访问 Defenseorchestrator.eu。

# 迁移到 Cisco Security Cloud Sign On 身份提供程序

在 2019 年 10 月 14 日，思科防御协调器(CDO) 会将租户转换为 Cisco Security Cloud Sign On 作为身份提供程序，并使用 Duo 进行多因素身份验证 (MFA)。**要登录 CDO，必须先在 Cisco Secure Sign-On 中激活帐户，然后再使用 Duo 配置 MFA**。

CDO 需要 MFA，它为保护您的用户身份提供额外的一重保障。双因素身份验证（一种 MFA）需要两个部分或因素来确保登录CDO的用户身份真实。第一个因素是用户名和密码，第二个是按需生成的一次性密码 (OTP)。

注释

- 如果您使用自己的单点登录身份提供程序登录 CDO，则转换到 Cisco Security Cloud Sign On 和 Duo 不会影响您。您可以继续使用自己的登录解决方案。
- 如果您正在免费试用 CDO，则此过渡适用于您。
- **如果您的 CDO 租户是在 2019 年 10 月 14 日或之后创建的，**请参阅新 CDO 租户的初始登录，第 3 页，而不是本文。

### 准备工作

我们强烈建议在迁移之前执行以下步骤：

-  **安装 DUO Security**。我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。
- **时间同步**。您要使用移动设备生成一次性密码。由于 OTP 是基于时间的，所以您的设备时钟与实时同步是非常重要的。请确保您的设备时钟自动或手动设置为正确的时间。
- 创建新的思科 Secure Sign-On 账户并配置 Duo 多因素身份验证。这是 4 步流程。您需要完成所有四个步骤。

# 迁移后的登录失败故障排除

**由于用户名或密码不正确，CDO 登录失败**

**解决方法** 如果您尝试登录 CDO，并且知道您使用的是正确的用户名和密码，但登录失败，或者您尝试“忘记密码”无法恢复有效的密码，则您可能已尝试在未创建新 Cisco Security Cloud Sign On 帐户的情况下进行登录，则您需要按照创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 58 页中的说明注册新的 Cisco Security Cloud Sign On 帐户。

**登录到 Cisco Security Cloud Sign On 控制面板成功，但您无法启动 CDO**

**解决方法** 您可能使用与 CDO 租户不同的用户名创建了 Cisco Security Cloud Sign On 账户。请联系思科技术支持中心 (TAC)，以规范 CDO 和 Cisco Secure Sign-On 之间的用户信息。

**使用保存的书签登录失败**

**解决方法** 您可能正在尝试使用浏览器中保存的旧书签登录。书签可能指向 https://cdo.onelogin.com。https://cdo.onelogin.com/

**解决方法** 登录 https://sign-on.security.cisco.com。

- **解决方法** 如果您尚未创建 Cisco Secure Sign-On 账户，请创建一个账户。创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 58 页
- **解决方法** 如果您已创建新账户，请点击控制面板上与 思科防御协调器（美国）、思科防御协调器（欧盟）或 思科防御协调器（亚太地区）对应的 CDO 磁贴
- **解决方法** 将书签更新为指向 https://sign-on.security.cisco.com。https://sign-on.security.cisco.com/

# 启动 CDO 租户

**步骤 1** 在 Cisco Security Cloud Sign On 控制板上点击适当的 CDO 按钮。CDO 磁贴会将您导向 https://defenseorchestrator.com，而 CDO (EU) 磁贴会将您导向 https://defenseorchestrator.eu

**步骤 2** 请点击身份验证器徽标以选择 Duo Security 或 Google Authenticator， 如果您已设置这两个身份验证器。

- 如果您在现有租户上已有用户记录，则将登录该租户。
- 如果您在多个门户上已有用户记录，您将能够选择要连接的门户。

- 如果您在若干租户上已有用户记录，则将能够选择要连接的 CDO 租户。
- 如果您在现有租户上尚无用户记录，将能够了解有关 CDO 的详细信息或申请试用租户。

门户视图检索并显示来自多个租户的整合信息。有关详细信息，请参阅管理多租户门户, on page 49。

租户视图显示您拥有用户记录的多个租户。


# 管理租户的超级管理员

最佳做法是限制租户上的超级管理员数量。确定哪些用户应具有超级管理员权限，查看用户管理，并将其他用户的角色更改为“管理员”。在 CDO 中管理用户, on page 52

# 关于 CDO 许可证

CDO需要基本订用租户授权和设备许可证来管理设备。您可以根据所需的租户数量购买一个或多个基本订用，并根据设备型号和数量购买设备许可证。CDO换句话说，购买基本订用会为您提供一个租户，对于您选择使用的每台设备，您都需要单独的设备许可证。CDOCDO出于规划部署的目的，请注意，每个租户可以通过安全设备连接器 (SDC) 管理大约 500 台设备，并使用云连接器管理任意数量的设备。CDO有关详细信息，请参阅安全设备连接器 (SDC)。

要从 载入和管理设备，您需要根据要管理的设备购买基本订用和设备特定的期限订用。思科防御协调器

### 订用

思科防御协调器 订用是基于期限的：

- 基本 - 提供一年、三年和五年订用，并提供访问租户和载入充分许可设备的权利。CDO
- 设备许可证 - 为您选择管理的任何受支持设备提供一年、三年和五年的订用。例如，如果您购买了思科 Firepower 1010 设备的三年软件订用，则可以选择在三年内使用 CDO 来管理思科 Firepower 1010 设备。

有关CDO支持的思科安全设备的详细信息，请参阅 CDO 支持的软件和硬件。

**重要事项** 您不需要两个单独的设备许可证来管理高可用性设备对。CDO如果您有 Cisco Secure Firewall ASA (ASA) 高可用性对，则购买一个 ASA 设备许可证就足够了，因为 CDO 会将高可用性设备对视为一台设备。

**注释** 您无法通过思科智能许可门户管理许可。CDO

### 软件订用支持

基本订用包括在订用期限内有效的软件订用支持，并可免费访问软件更新、主要升级和思科技术支持中心 (TAC)。CDO虽然默认选择软件支持，但您也可以根据自己的要求利用解决方案支持。CDO

### 思科防御协调器 评估许可证

您可以从您的 SecureX 账户申请 30 天试用。思科防御协调器 有关详细信息，请参阅请求 CDO 租户。

## 云交付防火墙管理中心和威胁防御许可证

您无需购买单独的许可证即可在CDO中使用 云交付的防火墙管理中心；CDO租户的基本订用包括云交付的防火墙管理中心的成本。

### 云交付的防火墙管理中心 评估许可证

云交付的防火墙管理中心 提供 90 天的评估许可证，在此之后，威胁防御 服务将被阻止。

要了解如何在CDO租户上调配 云交付的防火墙管理中心，请参阅为CDO租户请求云交付的防火墙管理中心。

**注释** 云交付的防火墙管理中心不支持气隙网络中的设备的特定许可证预留 (SLR)。

### 云交付防火墙管理中心的威胁防御许可证

您需要为 云交付的防火墙管理中心 管理的每台 Secure Firewall Threat Defense 设备购买单独的许可证。有关详细信息，请参阅使用 *Cisco* 防御协调器中的云交付防火墙管理中心管理防火墙威胁防御中的许可证。

要了解 CDO 如何处理迁移到 云交付的防火墙管理中心 的设备的许可，请参阅将威胁防御从管理中心迁移到云。

# 安全设备连接器

安全设备连接器 (SDC) 是允许思科设备与 CDO通信的智能代理。使用设备凭证将无法通过互联网直接访问的设备载入到 CDO 时，您可以在网络中部署 SDC 来代理设备和 CDO之间的通信。或者，如果您愿意，可以使设备通过其外部接口从 CDO接收直接通信。自适应安全设备 (ASA)、Meraki MX、Secure Firewall Threat Defense 设备和 Firepower 管理中心 设备、通用 SSH 和 IOS 设备都可以使用 SDC 载入 CDO 。

SDC监控 CDO 需要在受管设备上执行的命令，以及需要发送到受管设备的消息。SDC 代表 CDO执行命令，代表受管设备向 CDO 发送消息，并将受管设备的应答返回给 CDO。

SDC 使用通过 HTTPS (TLS 1.2) 的 AES-128-GCM 签名和加密的安全通信消息与 CDO通信。载入的设备和服务的所有凭证都会直接从浏览器加密到 SDC ，并使用 AES-128-GCM 进行静态加密。只有 SDC 可以访问设备凭证。其他 CDO 服务均无权访问凭证。有关如何允许在 SDC 和 CDO 之间通信的信息，请参阅将 思科防御协调器 连接到托管设备 ， 第 9 页。

SDC 可以安装在设备上，作为虚拟机监控程序上的虚拟机，也可以安装在 AWS 或 Azure 等云环境中。您可以使用 SDC 提供的组合虚拟机和 CDO 映像来安装 SDC ，也可以创建自己的虚拟机并在其上安装 SDC。 SDC 虚拟设备包括 CentOS 或 Ubuntu 操作系统，并在 Docker 容器中运行。

每个 CDO 租户可以拥有无限数量的 SDC。这些 SDC 不会在租户之间共享，而是专用于单个租户。单个SDC可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。但是，出于规划部署的目的，预计一个 SDC 可支持大约 500 台设备。

为租户部署多个 SDC 还具有以下优势：

- 您可以使用 CDO 租户管理更多设备，而不会降低性能。
- 您可以将SDC部署到网络中的隔离网段，并且仍然使用相同的CDO租户管理该网段中的设备。如果没有多个 SDC，您将需要使用不同的 CDO 租户管理这些隔离网段中的设备。

部署第二个或后续 SDC 的程序与部署第一个 SDC的程序相同。租户上的初始 SDC 包含租户的名称和数字 1，并显示在 CDO 的**安全连接器 (Secure Connectors)** 选项卡**服务 (Services)** 页面上。每个额外的 SDC 都按顺序编号。请参阅使用 CDO 的 VM 映像部署安全设备连接器 ， 第 10 页和在您自己的虚拟机上部署安全设备连接器 ， 第 14 页

**相关信息：**

- 将 思科防御协调器 连接到托管设备
- 更新您的安全设备连接器 ， 第 26 页

• 删除安全设备连接器， 第 24 页

# 将 思科防御协调器 连接到托管设备

CDO 通过云连接器或安全设备连接器 (SDC) 连接到其管理的设备。

如果可以直接从互联网访问您的设备，则应使用云连接器连接到您的设备。如果可以将设备配置为，则允许从云区域中的 CDO IP 地址对端口 443 进行入站访问。

如果无法从互联网访问您的设备，您可以在网络中部署本地 SDC，以允许 CDO 与您的设备进行通信。如果您可以将设备配置为，则允许端口 443（或您为设备管理配置的任何端口）上的完全入站访问。

您的网络中需要有本地 SDC 才能载入：

- 无法从云访问的 ASA 设备。

所有其他设备和服务都不需要本地SDC。CDO将使用其“云连接器”进行连接。请参阅下一部分，了解入站访问必须允许的 IP 地址。

### 通过云连接器将设备连接到 CDO

通过云连接器将 CDO 直接连接到您的设备时，您应允许 EMEA、美国或 APJC 区域中的各种 IP 地址在端口 443（或您为设备管理配置的任何端口）上进行入站访问。

如果您是**欧洲、中东或非洲 (EMEA)** 地区的客户，并且您在 https://defenseorchestrator.eu/ 连接到 CDO，请允许从以下 IP 地址进行入站访问：

- 35.157.12.126
- 35.157.12.15

如果您是**美国**地区的客户，并且您通过 https://defenseorchestrator.com 连接到 CDO，请允许从以下 IP 地址进行入站访问：

- 52.34.234.2
- 52.36.70.147

如果您是**亚太地区-日本-中国 (APJC)** 地区的客户，并且您通过 https://www.apj.cdo.cisco.com/ 连接到 CDO，请允许来自以下 IP 地址的入站访问：

- 54.199.195.111
- 52.199.243.0

### 使用 SDC 将设备连接到 CDO

当通过 SDC 将 CDO 连接到您的设备时，您希望 CDO 管理的设备必须允许在端口 443（或您为设备管理配置的任何端口）上进行完全入站访问。这是使用管理访问控制规则配置的。

您还必须确保部署了 SDC 的虚拟机与受管设备的管理接口建立了网络连接。

### 将 ASA 连接到 SDC 的特殊注意事项

具体而言，对于 ASA，SDC 使用与 ASDM 相同的安全通信通道。

如果管理的 ASA 也配置为接受 AnyConnect VPN 客户端连接，则必须将 ASDM HTTP 服务器端口更改为 1024 或更高的值。请注意，此端口号与将 ASA 设备载入 CDO 时使用的端口号相同。

### 示例 ASA 命令

以下示例假定 ASA 外部接口名为“outside”，并且在 ASA 上配置了 AnyConnect 客户端，因此 ASDM HTTP 服务器正在侦听端口 8443。

要启用外部接口，请输入以下命令：

欧洲、中东和非洲地区：

**http 35.157.12.126 255.255.255.255 outside**

**http 35.157.12.15 255.255.255.255 outside**

美国：

**http 52.34.234.2 255.255.255.255 outside**

**http 52.36.70.147 255.255.255.255 outside**

亚太地区-日本-中国地区：

**http 54.199.195.111 255.255.255.255 outside**

**http 52.199.243.0 255.255.255.255 outside**

要启用 ASDM HTTP 服务器端口，在使用 AnyConnect VPN 客户端的情况下，请输入以下命令：

**http server enable 8443**

# 使用 CDO 的 VM 映像部署安全设备连接器

使用设备凭证将 CDO 连接到设备时，最佳做法是在网络中下载并部署 SDC，以管理 CDO 与设备之间的通信。通常，这些设备不是基于边界的，没有公共 IP 地址，或者具有通往外部接口的开放端口。自适应安全设备 (ASA)、FDM 管理 设备、Firepower 管理中心 (FMC) 以及 SSH 和 IOS 设备都可以使用 SDC 载入 CDO 。

SDC 监控 CDO 需要在受管设备上执行的命令，以及需要发送到受管设备的消息。SDC 代表 CDO执行命令，代表受管设备向 CDO 发送消息，并将受管设备的应答返回给 CDO。

单个 SDC 可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。但是，出于规划部署的目的，我们预计一个 SDC 可支持大约 500 台设备。有关详细信息，请参阅在单个 CDO 租户上使用多个 SDC，第 27 页。

此程序介绍如何使用 CDO 的 VM 映像在网络中安装 SDC。这是创建 SDC 的首选、最简单、最可靠的方法。如果需要使用您创建的 VM 创建 SDC，请执行 在您自己的虚拟机上部署安全设备连接器，第 14 页。

### 开始之前

在部署 SDC 之前，请查看以下前提条件：

- CDO 需要进行严格的证书检查，并且不支持安全设备连接器 (SDC) 和互联网之间的 Web/内容代理检查。如果使用代理服务器，请禁用对 SDC 和 CDO之间的流量的检测。
- SDC 必须在 TCP 端口 443 或您为设备管理配置的端口上具有对互联网的完全出站访问权限。CDO 管理的设备还必须允许来自此端口的入站流量。
- 查看将 思科防御协调器 连接到托管设备 以确保适当的网络访问。
- CDO 支持使用 vSphere Web 客户端或 ESXi Web 客户端安装其 SDC VM OVF 映像。
- CDO 不支持使用 vSphere 桌面客户端安装 SDC VM OVF 映像。
- ESXi 5.1 虚拟机监控程序。
- Cent OS 7 访客操作系统。
- 仅具有一个 SDC 的 VMware ESXi 主机的系统要求：
  - VMware ESXi 主机需要 2 个 CPU。
  - VMware ESXi 主机至少需要 2 GB 内存。
  - VMware ESXi 需要 64 GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。
- 具有 SDC 和租户的**单个**安全事件连接器 (SEC) 的 VM 的系统要求。（SEC 是关于 Cisco Defense Orchestrator 中安全分析和日志记录 (SaaS)中使用的组件）。

  添加到 VMware ESXi 主机的每个 SEC 都需要额外的 4 个 CPU 以及额外的 8 GB 内存。

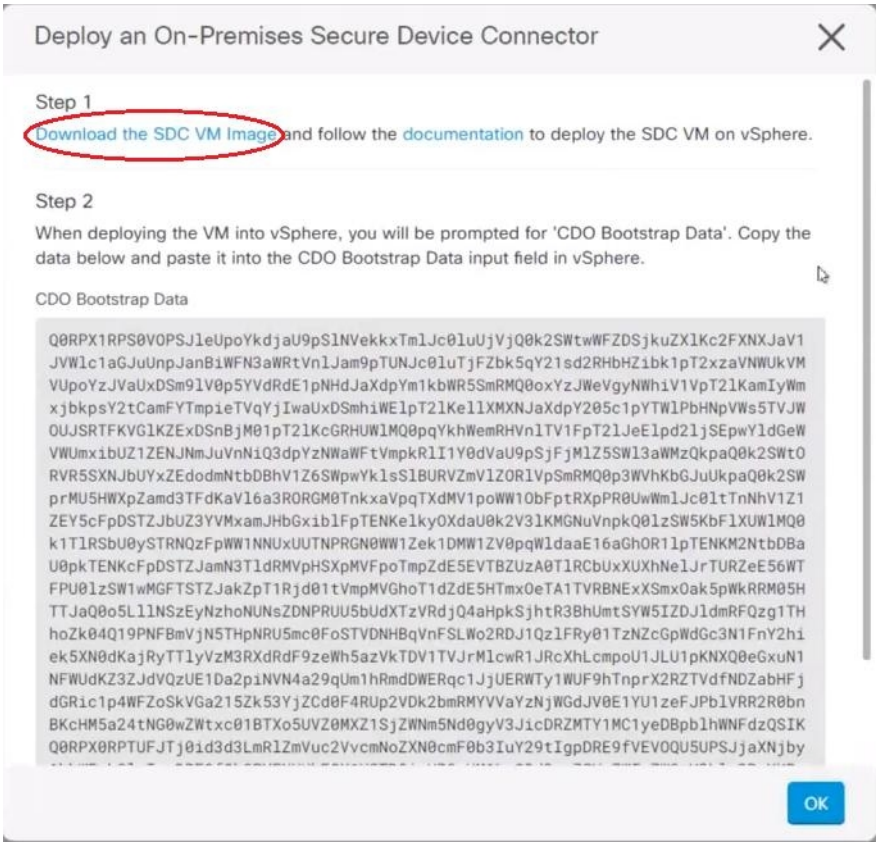
  因此，以下是对具有一个 SDC 和一个 SEC 的 VMware ESXi 主机的要求：
  - VMware ESXi 主机需要 6 个 CPU。
  - VMware ESXi 主机至少需要 10 GB 内存。
  - VMware ESXi 需要 64 GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。
- Docker 的 IP 必须与 SDC 的 IP 范围**和**设备 IP 范围位于不同的子网中。
- 在开始安装之前收集以下信息：
  - 要用于 SDC 的静态 IP 地址。
  - 您在安装过程中创建的 `root` 和 `cdo` 用户的密码。
  - 您的组织使用的 DNS 服务器的 IP 地址。
  - SDC 地址所在网络的网关 IP 地址。
  - 时间服务器的 FQDN 或 IP 地址。
- SDC 虚拟机配置为定期安装安全补丁，为此，需要打开端口 80 出站。

**步骤 1** 登录到要为其创建 SDC 的 CDO 租户。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 在**服务 (Services)** 页面上，选择**安全连接器 (Secure Connectors)** 选项卡，点击蓝色加号按钮，然后选择**安全设备连接器 (Secure Device Connector)**。

**步骤 4** 在步骤 1 中，点击**下载 SDC VM 映像 (Download the SDC VM image)**。这将在单独的选项卡中打开。




**步骤 5** 从 zip 文件中提取所有文件。它们看起来和下面有些相似：

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

**步骤 6** 使用 vSphere Web 客户端以管理员身份登录 VMware 服务器。

**注释** 请勿使用 ESXi Web 客户端。

**步骤 7** 按照提示从 OVF 模板部署安全设备连接器虚拟机。

**步骤 8** 设置完成后，打开 SDC VM。

**步骤 9** 打开新 SDC VM 的控制台。

**步骤 10** 使用用户名 **cdo** 登录。默认密码为 **adm123**。

**步骤 11** 在提示符后，键入 `sudo sdc-onboard setup`。

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

**步骤 12** 出现密码提示时，输入 `adm123`。

**步骤 13** 按照提示为用户 `root`创建新密码。输入 root 用户的密码。

**步骤 14** 按照提示为 **cdo** 用户创建新密码。输入 cdo 用户的密码。

**步骤 15** 当系统提示 **请选择要连接的 CDO 域** 时，请输入您的 Cisco Defense Orchestrator 域信息。

**步骤 16** 系统提示时，输入以下的 SDC 的域信息：

a) IP 地址/CIDR
b) 网关
c) DNS 服务器
d) NTP 服务器或 FQDN
e) Docker 网桥

如果 Docker 网桥不适用，请按 Enter 键。

**步骤 17** 当系统提示 **这些值是否正确时？（是/否）(Are these values correct? [y/n])**， 使用 **y确认您的输入**。

**步骤 18** 确认您的输入内容。

**步骤 19** 当系统提示 **您是否要设置 SDC 时？（是/否）(Would you like to setup the SDC now? [y/n])**，输入 `n`。

**步骤 20** VM 控制台会自动将您注销。

**步骤 21** 创建与 SDC 的 SSH 连接。以 **cdo** 身份登录并输入密码。

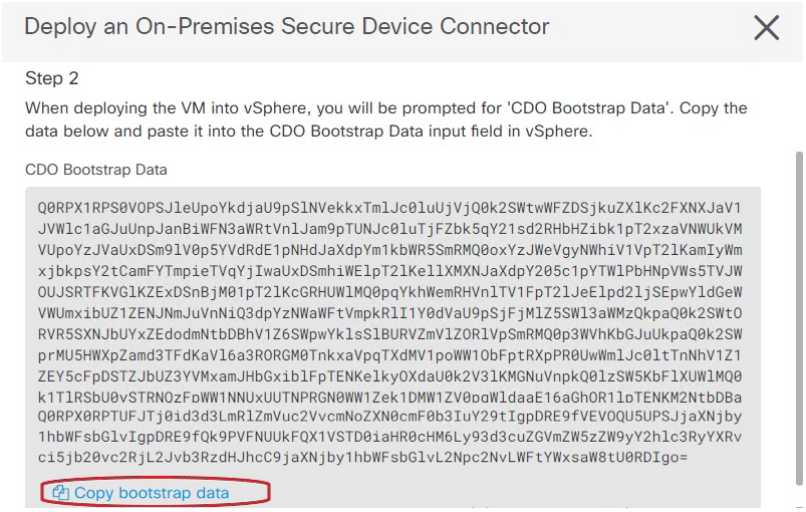
**步骤 22** 在提示符后，键入 `sudo sdc-onboard bootstrap`。

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

**步骤 23** 当系统提示输入 **[sudo] 密码**时，请输入您在步骤 14 中创建的 cdo 密码。

**步骤 24** 当系统提示**请从 CDO 的安全连接器页面复制引导程序数据 (Please copy the bootstrap data form the Secure Connector Page of CDO)** 时，请执行以下程序：

1. 登录至 CDO。
2. 在操作窗格中，点击**部署现场安全设备连接器 (Deploy an On-Premises Secure Device Connector)**。
3. 点击对话框第 2 步中的**复制引导程序数据 (Copy the bootstrap data)**，然后粘贴到 SSH 窗口中。




**步骤 25** 当系统提示 您是否想更新这些设置？（是/否）**(Do you want to update these setting? [y/n])**，输入 `n`。

**步骤 26** 返回“安全设备连接器”(Secure Device Connector) 页面。刷新屏幕，直到您看到新 SDC 的状态更改为**活动 (Active)**。

# 在您自己的虚拟机上部署安全设备连接器

使用设备凭证将 CDO 连接到设备时，最佳做法是在网络中下载并部署安全设备连接器 (SDC)，以管理 CDO 与设备之间的通信。通常，这些设备不是基于边界的，没有公共 IP 地址，或者具有通往外部接口的开放端口。自适应安全设备 (ASA)、FDM 管理 设备、Firepower 管理中心 (FMC) 设备均可使用设备凭证载入 CDO。

SDC 监控需要在受管设备上执行的命令，以及需要发送到受管设备的消息。SDC 代表 CDO 执行命令，代表受管设备向 CDO 发送消息，并将受管设备的应答返回给 CDO。

单个 SDC 可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。但是，出于规划部署的目的，我们预计一个 SDC 可支持大约 500 台设备。有关详细信息，请参阅在单个 CDO 租户上使用多个 SDC，第 27 页。

此程序介绍如何使用您自己的虚拟机映像在网络中安装 SDC。

**注释** 安装 SDC 的首选、最简单、最可靠的方法是下载 CDO 的 SDC OVA 映像并进行安装。对于说明，请参阅 使用 CDO 的 VM 映像部署安全设备连接器，第 10 页。

### 开始之前

- CDO 需要严格的证书检查，并且不支持 SDC 和互联网之间的 Web/内容代理。
- SDC 必须在 TCP 端口 443 上具有对互联网的完全出站访问权限。

- 关于网络指南，请查看将 思科防御协调器 连接到托管设备。
- 安装了 vCenter Web 客户端或 ESXi Web 客户端的 VMware ESXi 主机。

**注释** 我们不支持使用 vSphere 桌面客户端进行安装。

- ESXi 5.1 虚拟机监控程序。
- Cent OS 7 访客操作系统。
- 仅具有 SDC 的 VM 的系统要求：
  - VMware ESXi 主机需要 2 个 CPU。
  - VMware ESXi 主机至少需要 2 GB 内存。
  - VMware ESXi 需要 64 GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。此值假定您对分区使用逻辑卷管理 (LVM)，因此您可以根据需要扩展所需的磁盘空间。
- 具有 SDC 和租户的**单个**安全事件连接器 (SEC) 的 VM 的系统要求。（SEC 是关于 Cisco Defense Orchestrator 中安全分析和日志记录 (SaaS)中使用的组件）。

  添加到 VMware ESXi 主机的每个 SEC 都需要额外的 4 个 CPU 以及额外的 8 GB 内存。

  因此，以下是对具有一个 SDC 和一个 SEC 的 VMware ESXi 主机的要求：
  - VMware ESXi 主机需要 6 个 CPU。
  - VMware ESXi 主机至少需要 10 GB 内存。
  - VMware ESXi 需要 64 GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。
- 更新 VM 上的 CPU 和内存后，打开 VM 并确保“安全连接器”页面指示 SDC 处于“活动”状态。
- 执行此过程的用户应该能够轻松地在 Linux 环境中使用 vi 可视化编辑器编辑文件。
- 如果您在 CentOS 虚拟机上安装本地 SDC，我们建议您定期安装 Yum 安全补丁。根据您的 Yum 配置，要获取 Yum 更新，您可能需要在端口 80 和 443 上打开出站访问。您还需要配置 yum-cron 或 crontab 来安排更新。与您的安全运营团队合作，确定是否需要更改任何安全策略以允许您获取 Yum 更新。

**注释** **开始之前**：不要将程序中的命令复制并粘贴到终端窗口中，而应键入这些命令。某些命令包括“n-dash”，在剪切和粘贴过程中，这些命令可以作为 “m-dash” 应用，这可能会导致命令失败。

**步骤 1** 登录到要为其创建 SDC 的 CDO 租户。

**步骤 2** 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 在 **服务 (Services)** 页面上，选择 **安全连接器 (Secure Connectors)** 选项卡，点击蓝色加号按钮，然后选择 **安全设备连接器 (Secure Device Connector)**。

**步骤 4** 将窗口中步骤 2 中的引导程序数据复制到记事本。

**步骤 5** 安装 **CentOS 7 虚拟机**，至少为 SDC 分配以下 RAM 和磁盘空间：

- 8 GB RAM
- 10GB 磁盘空间

**步骤 6** 安装后，配置基本网络，例如指定 SDC 的 IP 地址、子网掩码和网关。

**步骤 7** 配置 DNS（域名服务器）服务器。

**步骤 8** 配置 NTP（网络时间协议）服务器。

**步骤 9** 在 CentOS 上安装 SSH 服务器，以便与 SDC 的 CLI 轻松交互。

**步骤 10** 运行 yum 更新，然后安装软件包： **open-vm-tools**、 **nettools** 和 **bind-utils**

```
[root@sdc-vm ~]# yum update -y
                [root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

**步骤 11** 安装 AWS CLI 软件包；请参阅https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html。

**注释** 请勿使用 **--user** 标志。

**步骤 12** 安装 Docker CE 软件包；请参阅https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce

**注释** 使用“使用存储库安装”方法。

**步骤 13** 启动 Docker 服务并使其在启动时启动：

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
    /usr/lib/systemd/system/docker.service.
```

**步骤 14** 创建两个用户：“cdo”和“sdc”。cdo 用户将是您登录以运行管理功能的用户（因此您无需直接使用 root 用户），sdc 用户将是运行 SDC docker 容器的用户。

```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

**步骤 15** 为 cdo 用户设置密码。

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

**步骤 16** 将 cdo 用户添加到“wheel”组，为其提供管理 (sudo) 权限。

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

**步骤 17** 安装 Docker 时，会创建一个用户组。根据 CentOS/Docker 的版本，它可能被称为 “docker” 或 “dockerroot”。检查 /etc/group 文件以查看创建的组，然后将 sdc 用户添加到此组。

```
[root@sdc-vm ~]# grep docker /etc/group
 docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

**步骤 18** 如果 /etc/docker/daemon.json 文件不存在，请创建该文件，并使用以下内容填充。创建后，重新启动 Docker 后台守护程序。

**注释** 确保在 "group" 项中输入的组名称与您在上一步中在 /etc/group 文件中找到的组匹配。

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
        {
           "live-restore": true,
           "group": "docker"
        }
        [root@sdc-vm ~]# systemctl restart docker
        [root@sdc-vm ~]#
```

**步骤 19** 如果您当前使用的是 vSphere 控制台会话，请切换到 SSH 并使用 “cdo” 用户登录。登录后，更改为 “sdc” 用户。当系统提示输入密码时，请输入 “cdo” 用户的密码。

```
[cdo@sdc-vm ~]$ sudo su sdc
              [sudo] password for cdo: <type password for cdo user>
              [sdc@sdc-vm ~]$
```

**步骤 20** 将目录更改为 **/usr/local/cdo**。

**步骤 21** 创建一个名为 `bootstrapdata` 的新文件，并将**部署现场安全设备连接器**向导的步骤 2 中的引导程序数据粘贴到此文件中。**保存**文件。您可以使用 `vi` 或 `nano` 创建该文件。

**步骤 22** 引导程序数据采用 base64 编码。对其进行解码并将其导出到名为 `extractedbootstrapdata` 的文件

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata > /usr/local/cdo/extractedbootstrapdata
             [sdc@sdc-vm ~]$
```

运行 cat 命令以查看解码后的数据。命令和解码后的数据应如下所示：

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
              CDO_TOKEN="<token string>"
              CDO_DOMAIN="www.defenseorchestrator.com"
              CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

**步骤 23** 运行以下命令，将解码的引导程序数据部分导出到环境变量。

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
             [sdc@sdc-vm ~]$
```

**步骤 24** 从 CDO 下载引导程序捆绑包。

```
[sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
              100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
```

```
[sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/tenant-name-SDC
```

**步骤 25** 解压缩 SDC tar 包，并运行 `bootstrap.sh` 文件以安装 SDC 软件包。

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
[2018-07-23 13:54:04] startup new container
Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458: Pulling from
ciscodefenseorchestrator/sdc_prod
08d48e6f1cff: Pull complete
ebbd10b629b1: Pull complete
d14d580ef2ed: Pull complete
45421d451ab8: Pull complete
<snipped - downloads>
no crontab for sdc
```

SDC 现在应在 CDO 中显示“活动”。

---

下一步做什么

- 
- 如果要安装安全事件连接器，请返回 在 SDC 虚拟机上安装安全事件连接器，第 380 页。
- 如果要在租户上安装**第二个或多个**安全事件连接器，请返回使用 CDO 映像安装 SEC。

# 在 Ubuntu 虚拟机上部署 安全设备连接器 和安全事件连接器

使用设备凭证将 CDO 连接到设备时，最佳做法是在网络中下载并部署 安全设备连接器 (SDC)，以管理 CDO 与设备之间的通信。通常，这些设备不是基于边界的，没有公共 IP 地址，或者具有通往外部接口的开放端口。自适应安全设备 (ASA)、FDM 管理 设备、Firepower 管理中心 (FMC) 设备均可使用设备凭证载入 CDO。

SDC 可监控必须在托管设备上执行的命令，以及必须发送到托管设备的消息。SDC 代表 CDO 执行命令，代表受管设备向 CDO 发送消息，并将受管设备的应答返回给 CDO。

安全事件连接器 (SEC) 将事件从 ASA 和 FTD 转发到思科云，以便您可以在“事件日志记录”页面中查看它们，并根据您的许可使用安全云分析进行调查。

部署 SDC后，添加 SEC 容器就成为了一项简单的任务。SEC 服务旨在从 ASA、Cisco IOS 和 FDM 管理 设备接收系统日志消息，并将其安全地发送到思科云。这使得 CDO 分析和思科 XDR 等事件服务能够轻松存储、扩充和分析日志消息。

您可以执行 CiscoDevNet 站点上提供的脚本，以便在 Linux Ubuntu 系统上安装 SDC 和 SEC。

开始之前

- CDO 需要严格的证书检查，并且不支持 SDC 和互联网之间的 Web/内容代理。
- SDC 必须在 TCP 端口 443 上具有对互联网的完全出站访问权限。
- 关于网络指南，请查看将 思科防御协调器 连接到托管设备。
- 安装了 vCenter Web 客户端或 ESXi Web 客户端的 VMware ESXi 主机。

注释 我们不支持使用 vSphere 桌面客户端进行安装。

- ESXi 5.1 虚拟机监控程序。
- 虚拟机上安装了 Ubuntu 操作系统 20.04 或更高版本。

  SDC：
  - CPU：双核
  - RAM：最低 2 GB

  SDC 和 SEC：
  - CPU：4 核
  - RAM：最低 8 GB

- 运行 SDC 的 Ubuntu 计算机必须能够访问 ASA 和 Cisco IOS 设备的管理接口。

**步骤 1** 登录到要为其创建 SDC 的 CDO 租户。

**步骤 2** 选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 在**服务 (Services)** 页面上，选择**安全连接器 (Secure Connectors)** 选项卡，点击 +，然后选择**安全设备连接器 (Secure Device Connector)**。

**步骤 4** 将窗口中步骤 2 中的引导程序数据复制到记事本。

**步骤 5** 打开 CiscoDevNet 以部署 SDC。

**步骤 6** 点击**代码 (Code)** 并复制 **HTTPS** 选项卡中的 URL。

**步骤 7** 在 Ubuntu 系统上，按 Ctrl+Alt+T 快速打开终端窗口。

**步骤 8** 在终端中，输入 **git** 并粘贴之前复制的 HTTPS URL。

```
[sdc@vm]:~$ git https://github.com/CiscoDevNet/cdo-deploy-sdc.git
Resolving deltas: 100% (22/22). done.
```

**步骤 9** 转到“cdo-deploy-sdc”目录。

```
[sdc@vm]:~$ cd cdo-deploy-sdc.
```

**步骤 10** 执行 **ls -la** 以查看文件和脚本。

- **delete_sdc.sh**：删除系统上先前安装的 SDC。
- **deploy_sdc.sh**：在您的系统上部署 SDC。
- **install_docker.sh**：在系统上部署建议的 Docker 版本。

**步骤 11** 运行脚本以安装 Docker。

```
[sdc@vm]:~/cdo-deploy-sdc$ ./install_docker.sh

Remove docker docker.io docker-compose docker-compose-v2 docker-doc podmand-docker {y/n] n
Active: active (running) since date time UTC; 32s ago
Adding the current user to the docker permmissions group
Done!
```

**步骤 12** 运行脚本以部署 SDC。

输入 **./deploy_sdc.sh** 并粘贴从 CDO UI 复制的引导程序数据。

```
[sdc@vm]:~/cdo-deploy-sdc$ ./deploy_sdc.sh <bootstap data>.

If the docker container is up and running, the status of the SDC should go to 'ACtive' in the CDO Event
 Connectors panel.
```

安全设备连接器 现在必须在 CDO 中显示“活动”。

---

### 下一步做什么

- 
- 转到 在 Ubuntu 虚拟机上部署安全事件连接器，第 389 页 以安装安全事件连接器。

# 使用 Terraform 将安全设备连接器部署到 vSphere

### 开始之前

此程序详细介绍了如何将适用于 vSphere 的 CDO SDC Terraform 模块与 CDO Terraform 提供程序结合使用，以将 SDC 部署到 vSphere。在尝试执行该任务程序之前，请确保查看以下前提条件：

- 您需要 vSphere 数据中心 7 及更高版本
- 您需要具有数据中心权限的管理员账户才能执行以下操作：
  - 创建虚拟机
  - 创建文件夹
  - 创建内容库
  - 将文件上传到内容库
- Terraform 知识

**步骤 1** 在 CDO 中创建仅 API 用户并复制 API 令牌。要了解如何创建仅 API 用户，请参阅创建仅 API 用户。

**步骤 2** 按照 CDO Terraform 提供程序中的说明在 Terraform 存储库中配置 CDO Terraform 提供程序。

**示例：**

```
terraform {
  required_providers {
    cdo = {
      source = "CiscoDevNet/cdo"
      version = "0.7.0"
    }
  }
}

provider "cdo" {
  base_url = “<the CDO URL you use to access CDO>”
  api_token = “<the API Token generated in step 1>”
}
```

**步骤 3** 编写 Terraform 代码，以便使用 CDO Terraform 提供程序来创建 `cdo_sdc` 资源。有关详细信息，请参阅 cdo-sdc 资源的 Terraform 注册表。

**示例：**

```
Resource “cdo_sdc” “my-sdc” {
  name = “my-sdc-in-vsphere”
}
```

此资源的 `bootstrap_data` 属性使用 CDO 引导程序数据的值来填充，并在下一步中提供给 `cdo_sdc` Terraform 模块。

**步骤 4** 使用 cdo_sdc Terraform 模块来编写 Terraform 代码，以便在 vSphere 中创建 SDC。

**示例：**

```
data "cdo_tenant" "current" {}

module "vsphere-cdo-sdc" {
  source               = "CiscoDevNet/cdo-sdc/vsphere"
  version              = "1.0.0"
  vsphere_username     = "<replace-with-username-with-admin-privileges>"
  vsphere_password     = "<super-secure-password>"
  vsphere_server       = "<replace-with-address-of-vsphere-server>"
  datacenter           = "<replace-with-datacenter-name>"
  resource_pool        = "<replace-with-resource-pool-name>"
  cdo_tenant_name      = data.cdo_tenant.current.human_readable_name
  datastore            = "<replace-with-name-of-datastore-to-deploy-vm-in>"
  network              = "<replace-with-name-of-network-to-deploy-vm-in>"
  host                 = "<replace-with-esxi-host-address>"
  allow_unverified_ssl = <boolean; set to true if your vsphere server does not have a valid SSL
certificate>
  ip_address          = "<sdc-vm-ip-address; must be in the subnet of the assigned network for the VM>"

  gateway              = "<replace-with-network-gateway-address>"
  cdo_user_password    = "<replace-with-password-for-cdo-user-in-sdc-vm>"
  root_user_password   = "<replace-with-password-for-root-user-in-sdc-vm>"
  cdo_bootstrap_data   = cdo_sdc.sdc-in-vsphere.bootstrap_data
}
```

请注意，创建的 VM 有两个用户，一个是 `root` 用户，另一个是名为 `cdo`的用户，而且 VM 的 IP 地址是静态配置的。为 `cdo_bootstrap_data` 属性指定在创建 `cdo_sdc` 资源时生成的 `bootstrap_data` 属性的值。

**步骤 5** 像往常一样，使用 `terraform plan` 和 `terraform apply` 来规划和应用 Terraform。

有关完整示例，请参阅 CiscoDevNet 中的 CDO 自动化存储库。

---

如果您的 SDC 处于载入状态，请使用远程控制台连接到 vSphere 虚拟机，以 CDO 用户身份登录，然后执行以下命令：

```
sudo su
/opt/cdo/configure.sh startup
```

**注释** CDO Terraform 模块在 Apache 2.0 许可证下作为开源软件发布。如果需要支持，您可以在 GitHub 上提交问题。

# 使用 Terraform 模块在 AWS VPC 上部署安全设备连接器

### 开始之前

在尝试在 AWS VPC 上部署 SDC 之前，请查看以下前提条件：

- CDO 需要严格的证书检查，并且不支持 SDC 和互联网之间的 Web/内容代理。如果使用代理服务器，请禁用对安全设备连接器 (SDC) 和 CDO 之间的流量进行检查。
- 查看将 思科防御协调器 连接到托管设备 以确保适当的网络访问。
- 您需要一个 AWS 账户、一个至少具有一个子网的 AWS VPC 和一个 AWS Route53 托管区域。
- 确保您有 CDO 引导程序数据、AWS VPC ID 及其子网 ID。
- 确保您部署 SDC 的私有子网连接了 NAT 网关。
- 在运行防火墙管理 HTTP 接口的端口上打开从防火墙到连接到 NAT 网关的弹性 IP 的流量。

---

**步骤 1** 在 Terraform 文件中添加以下代码行；请确保手动输入变量：

```
module "example-sdc" {
  source             = "git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"
  env                = "example-env-ci"
  instance_name      = "example-instance-name"
  instance_size      = "r5a.xlarge"
  cdo_bootstrap_data = "<replace-with-cdo-bootstrap-data>"
  vpc_id             = <replace-with-vpc-id>
  subnet_id          = <replace-with-private-subnet-id>
}
```

有关输入变量和说明的列表，请参阅安全设备连接器 Terraform 模块。

**步骤 2** 将 `instance_id` 注册为 Terraform 代码中的输出：

```
output "example_sdc_instance_id" {
  value = module. example-sdc.instance_id
}
```

您可以使用 `instance_id` 连接到 SDC 实例，以便使用 AWS 系统管理器会话管理器 (SSM) 进行故障排除。有关可用输出的列表，请参阅安全设备连接器 Terraform 模块中的输出。

### 下一步做什么

要对 SDC 进行任何故障排除，您需要使用 AWS SSM 连接到 SDC 实例。请参阅 AWS 系统管理器会话管理器，了解有关如何连接到实例的更多信息。请注意，出于安全原因，使用 SSH 连接到 SDC 实例的端口不会被公开。

**注释** CDO Terraform 模块在 Apache 2.0 许可证下作为开源软件发布。如果需要支持，您可以在 GitHub 上提交问题。

# 更改安全设备连接器的 IP 地址

### 开始之前

- 您必须是管理员才能执行此任务。
- SDC 必须在 TCP 端口 443 或您为设备管理配置的端口上具有对互联网的完全出站访问权限。

**注释** 更改 SDC 的 IP 地址后，您无需将任何设备重新载入 CDO。

**步骤 1** 创建与 SDC 的 SSH 连接或打开虚拟机的控制台，并以 CDO 用户身份登录。

**步骤 2** 如果您希望在更改 IP 地址之前查看 SDC VM 的网络接口配置信息，请使用 ifconfig 命令。

```
[cdo@localhost ~]$ ifconfig
```

**步骤 3** 要更改接口的 IP 地址，请键入 sudo sdc-onboard setup 命令。

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

**步骤 4** 出现提示时，请输入密码。

```
[sudo] password for cdo:
```

**步骤 5** 在提示符后键入 n 以重置 root 和 CDO 密码。

```
Would you like to reset the root and cdo passwords? (y/n):
```

**步骤 6** 在提示符后键入 y 以重新配置网络。

```
Would you like to re-configure the network? (y/n):
```

**步骤 7** 出现提示时，输入要分配给 SDC 的新 IP 地址和 SDC VM 的其他域信息：

a) IP 地址
b) 网关
c) DNS 服务器
d) NTP 服务器或 FQDN

如果 NTP 服务器或 FQDN 不适用，请按 Enter 键。

e) Docker 网桥

如果 Docker 网桥不适用，请按 Enter 键。

**步骤 8** 当系统提示输入值是否正确时，请使用 y 确认输入。

```
Are these values correct? (y/n):
```

**注释** 在键入 y 之前，请确保您的值准确无误，因为在此命令后，您与旧 IP 地址的 SSH 连接将丢失。

**步骤 9** 使用分配给 SDC 的新 IP 地址创建 SSH 连接并登录。

**步骤 10** 您可以运行连接状态测试命令，以确保 SDC 正常运行。

```
[cdo@localhost ~]$ sudo sdc-onboard status
```

所有检查都必须以绿色显示 [ OK ]。

**注释** 如果在 VM 的控制台中执行此程序，则在确认值正确后，连接状态测试将自动运行并显示状态。

**步骤 11** 您还可以通过 CDO 用户界面检查 SDC 的连接。要执行此操作，请打开 CDO 应用并导航至“工具和服务安全连接器”页面。 >

**步骤 12** 刷新页面并选择已更改 IP 地址的安全连接器。

**步骤 13** 在操作窗格中，点击请求检测信号。

您应该会看到已成功请求心跳消息，并且上次心跳应显示当前日期和时间。

**重要事项** 您所做的 IP 地址更改仅在格林威治标准时间上午 3:00 后反映在 SDC 的“详细信息”窗格中。

有关在 VM 上部署 SDC 的信息，请参阅。在您自己的虚拟机上部署安全设备连接器，第 14 页

# 删除安全设备连接器

**Warning** 此程序会删除您的安全设备连接器 (SDC)。这一操作不可逆。在执行此操作后，您将无法管理连接到该 SDC 的设备，直到安装新的 SDC 并重新连接设备。重新连接设备可能需要您为要重新连接的每个设备重新输入管理员凭证。

要从租户中删除 SDC，请遵循以下程序：

**步骤 1** 删除连接到您要删除的 SDC 的任何设备。您可以采用以下两种方式之一：

- 将某些设备移至不同的 SDC 或完全移出 SDC。有关详细信息，请参阅下文：
- 从 CDO 中删除连接到您要删除的 SDC 的任何设备。
  a. 请参阅CDO 使用同一 SDC 的设备，以便确定 SDC 使用的所有设备。
  b. 在**清单 (Inventory)** 页面中，选择您确定的所有设备。
  c. 在“设备操作”(Device Actions) 窗格中，点击**删除 (Remove)**，然后点击**确定 (OK)** 以确认您的操作。

**步骤 2** 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 在**服务 (Services)** 页面上，选择**安全连接器 (Secure Connectors)** 选项卡，点击蓝色加号按钮，然后选择**安全设备连接器 (Secure Device Connector)**。

**步骤 4** 在“安全连接器”(Secure Device Connector) 表中，选择要删除的 SDC。其设备计数现在应为零。

**步骤 5** 在“操作”(Actions) 窗格中，点击 **删除 (Remove)**。您会收到以下警告：

**Warning** 您即将删除 <sdc_name>。删除 SDC 的操作不可逆。删除 SDC 需要先创建并载入新的 SDC，然后才能载入或重新载入设备。

由于您当前有已载入的设备，因此删除 SDC 将要求您在设置新的 SDC 后重新连接这些设备并再次提供凭证。

- 如果您有任何问题或疑虑，请点击**取消 (Cancel)** 并联系 CDO 支持。
- 如果要继续，请输入 <sdc_name> 在下面的文本框中，然后点击**确定 (OK)**。

**步骤 6** 在确认对话框中，如果您想继续，请输入警告消息中所述的 SDC 名称。

**步骤 7** 点击**确定 (OK)** 以确认删除 SDC。

# 将 ASA 从一个 SDC 移至另一个 SDC

CDO 支持每个租户使用多个 SDC。在单个 CDO 租户上使用多个 SDC，第 27 页您可以使用以下程序将受管 ASA 从一个 SDC 移至另一个 SDC：

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备 (Devices)** 选项卡，然后点击 **ASA** 选项卡。

**步骤 3** 选择要移动到其他 SDC 的 ASA。

**步骤 4** 在**设备操作 (Device Actions)** 窗格中，点击**更新凭证 (Update Credentials)**。

**步骤 5** 点击 Secure Device Connector 按钮，然后选择要将设备移动到的 SDC。

**步骤 6** 输入用于登录设备的管理员用户名和密码，然后点击**更新 (Update)**。除非已更改，否则管理员用户名和密码与您用于载入 ASA 的凭证相同。您不必将这些更改部署到设备。

注释　如果所有 ASA 都使用相同的凭证，则可以将 ASA 从一个 SDC 批量移至另一个 SDC。如果 ASA 具有不同的凭证，则必须一次将其从一个 SDC 移至另一个 SDC。

# 重命名安全设备连接器

**步骤 1** 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 2** 选择要重命名的 SDC。

**步骤 3** 在详细信息窗格中，点击 SDC 名称旁边的编辑图标。

**步骤 4** 重命名 SDC。

此新名称将显示在 CDO 界面中出现 SDC 名称的任何位置，包括**清单 (Inventory)** 窗格的“安全设备连接器”(Secure Device Connectors) 过滤器。

# 指定默认的安全设备连接器。

许多由 CDO 管理的设备（尽管不是全部）通过 SDC 连接到 CDO。当您通过 SDC 载入连接到 CDO 的设备时，这些设备将与您的租户的默认 SDC 关联，除非您在载入期间另行指定。

您可以在“安全连接器”(Secure Connectors) 页面上指定默认选择的 SDC：

**步骤 1** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 2** 选择要作为默认值的 SDC。

**步骤 3** 在“操作”(Actions) 窗格中，点击**设为默认值 (Make Default)**。如果您没有看到“设为默认”操作，则该 SDC 已是默认 SDC。

# 更新您的安全设备连接器

使用此程序作为故障排除工具。通常，SDC 会自动更新，您不必使用此程序。但是，如果 VM 上的时间配置不正确，则 SDC 无法与 AWS 建立用于接收更新的连接。此程序将启动 SDC 更新，并应解决由于时间同步问题而导致的错误。

**步骤 1** 连接到 SDC。您可以使用 SSH 进行连接，也可以使用 VMware 虚拟机监控程序中的控制台视图。）

**步骤 2** 以 **cdo** 用户身份登录 SDC。

**步骤 3** 切换到 SDC 用户以更新 SDC Docker 容器：

```
[cdo@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

**步骤 4** 升级 SDC 工具包：

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeToolkit
                [sdc@sdc-vm ~]$
```

**步骤 5** 升级 SDC：

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeSDC
                [sdc@sdc-vm ~]$
```

# 在单个 CDO 租户上使用多个 SDC

通过为租户部署多个SDC，您可以管理更多设备，而不会出现性能下降。单个SDC可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。

您可以在租户上安装无限数量的 SDC。每个 SDC 可以管理一个网段。这些 SDC 会将这些网段中的设备连接到同一个 CDO 租户。如果没有多个 SDC，您将需要使用不同的 CDO 租户管理隔离网段中的设备。

部署第二个或后续 SDC 的程序与部署第一个 SDC 的程序相同。使用 CDO 的 VM 映像部署安全设备连接器，也可以在您自己的虚拟机上部署安全设备连接器。租户的初始SDC包含租户的名称和数字1。每个额外的 SDC 都按顺序编号。

# CDO 使用同一 SDC 的设备

请按照以下程序识别所有使用相同 SDC 连接到 CDO 的设备：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 如果已指定任何过滤条件，请点击“清单”(Inventory) 表顶部的**清除**按钮，以显示您使用 CDO管理的所有设备和服务。

**步骤 5** 点击过滤器按钮  以展开过滤器菜单。

**步骤 6** 在过滤器的“安全设备连接器”(Secure Device Connectors) 部分中，选中您感兴趣的SDC的名称。“清单”(Inventory) 表仅显示通过您在过滤器中选中的 SDC 连接到 CDO 的设备。

**步骤 7** （可选）检查过滤器菜单中的其他过滤器，以便进一步细化搜索。

**步骤 8** （可选）完成后，点击清单表顶部的 **清除** 按钮，以便显示您使用 CDO管理的所有设备和服务。

# SDC 中的开源和第三方许可证

==========

*** amqplib ***

**amqplib** 版权所有 **(c) 2013, 2014**

米歇尔·布里根**<mikeb@squaremobius.net>**

此软件包“**amqplib**”根据 **MIT** 许可证获得许可。可以在此目录中的文件 **LICENSE-MIT** 中找到副本，或从以下位置下载

http://opensource.org/licenses/MIT

==========

*** async ***

版权所有 **(c) 2010-2016 Caolan McMaho**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** bluebird ***

**MIT** 许可证 **(MIT)**

版权所有 **(c) 2013-2015 Petka Antonov**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

***cheerio ***

版权所有 **(c) 2012** 马特穆勒**<mattmuelle@gmail.com>**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** command-line-args ***

**MIT** 许可证 **(MIT)**

版权所有 **(c) 2015 Lloyd Brookes <75镑@gmail.com>**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** ip ***

此软件根据 **MIT** 许可证获得许可。

**Fedor Indutny, 2012** 版权所有。

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** json-buffer ***

版权所有 **(c) 2013 Dominic Tarr**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** json-stable-stringify ***

此软件在 **MIT** 许可证下发布：

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** json-stringify-safe ***

**ISC** 许可证

**版权所有 (c) Isaac Z. Schlueter 和贡献者**

特此授予出于任何目的使用、复制、修改和/或分发本软件的权限，前提是所有副本中均包含上述版权声明和本许可声明。

本软件按“原样”提供，作者否认与本软件相关的所有担保，包括对适销性和适用性的所有暗示担保。在任何情况下，作者均不对因使用、数据或利润损失而导致的任何特殊、直接、间接或后果性损害负责，无论是因合同、过失或其他原因造成的与本软件的使用或性能相关。

==========

*** lodash ***

版权所有 JS 基金会和其他贡献者 < https://js.foundation/ >https://js.foundation/

基于 **Underscore.js**，版权所有，

DocumentCloud 和 Investigative Reporters & Editors < >http://underscorejs.org/

该软件由许多个人自愿提供。有关确切的贡献历史记录，请参阅https://github.com/lodash/lodash中的修订历史记录

以下许可证适用于本软件的所有部分，但作为

记录如下：

====

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

====

通过 **CC0** 放弃示例代码的版权和相关权利。示例代码定义为文档中显示的所有源代码。

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

位于 node_modules 和 vendor 目录中的文件是此软件使用的外部维护的库，它们有自己的许可证；我们建议您阅读它们，因为它们的术语可能与上述术语不同。

==========

*** log4js ***

版权所有 **2015 Gareth Jones**（许多其他人的贡献）

根据 **Apache** 许可证 **2.0** 版本 **(**\“许可\”**)** 授权； 除非遵守本许可的规定，否则不得使用此文件。 您可以通过以下网址获取许可证副本：

http://www.apache.org/licenses/LICENSE-2.0

除非适用法律要求或达成书面协议， 根据许可证分发的软件均\“按原样\”分发， 且不附带任何明示或默示的保证或条件。 请参阅许可证，了解许可证中有关语言管理权限和限制的特定规定。

==========

*** mkdirp ***

版权所有 **2010 James Galliday (mail@substack.net)**

此项目是在 **MIT/X11** 许可证下发布的免费软件：

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** node-forge ***

新 **BSD** 许可证（**3** 个子句）

版权所有 **(c) 2010, Digital Bazaar, Inc.**

版权所有。

对源代码或二进制形式代码的重新发行和使用（包含或不含修改）需要符合下列条件：

***** 源代码的重新分发必须保留上述版权声明、本条件列表及以下免责声明。

***** 以二进制形式重新发行时，必须通过文档和/或在发行时一并提供的其它材料复制上述版权声明、此条件清单和下面的免责声明。

***** 未经事先明确书面许可，不得使用 **Digital Bazaar, Inc.** 及其参与者姓名宣传或推广本软件的衍生产品。

该软件由版权所有者和贡献者按“原样”提供，不承担任何明示或暗示的担保，包括但不限于用于特定用途的适销性和适用性的暗示担保。在任何情况下，**DIGITAL BAZAAR** 对于以任何方式使用该软件造成的任何直接、间接、意外、特殊、惩罚性或后果性损害（包括但不限于替代货物或服务的采购；用途丧失、数据丢失或利润损失；或业务中断），均不承担任何责任，无论导致前述损害的原因与责任推断如何，也无论是否因合同、严格责任或侵权（包括疏忽或其他原因）造成该等损害，即使已被告知发生此类损害的可能性。

==========

*** request ***

**Apache** 许可证

版本 **2.0**，**2004** 年 **1** 月

http://www.apache.org/licenses/

使用、复制和分发条款和条件

**1.** 定义。

“许可”是指本文档第 **1- 9** 节规定的使用、复制和分发的条款和条件。

“许可方”是指版权所有者或由版权所有者授权进行许可授予的实体。

“法律实体”是指实施实体以及所有其他控制该实体、由该实体控制或与该实体共同受控制的实体的联合整体。在此定义中，“控制”是指 **(i)** 通过合同或其他方式，有权直接或间接决定此类实体的方向或管理，或 **(ii)** 拥有此类实体百分之五十 **(50%)** 或以上已发行股份的所有权，或 **(iii)** 拥有此类实体的受益所有权。

“您”（或“您的”）是指行使此许可证所授权限的个人或法律实体。

“源”形式是指用于进行修改的首选形式，包括但不限于软件源代码、文档源和配置文件。

“目标”形式是指任何通过对源形式进行机械转换或翻译所获得的形式，包括但不限于经过编译的对象代码、生成的文档以及转换为其他媒体类型。

“作品”是指根据许可（如作品包含或随附的版权声明所示）提供的源形式或目标形式的著作（下面的附录中提供了一个示例）。

“衍生作品”是指任何基于作品创作（或从作品衍生而来）的，其编辑修订、注释、详细描述或其他修改等从整体上构成原创作品的源形式或目标形式的作品。根据此项许可，衍生作品不包括与作品及其衍生作品分离之作品，或仅与作品及其衍生作品的接口相链接（或以名称绑定）之作品。

“投稿”是指任何创作作品，包括作品的原始版本和对该作品或衍生作品所做的任何修改或增补，由版权所有者或经授权可代表版权所有者进行提交的个人或法律实体特意提交给许可方以纳入其作品中。在此定义中，“提交”是指发送给许可方或其代表的任何电子、口头或书面形式的通信，包括但不限于通过许可方管理的或代表许可方管理的邮件清单、源代码控制系统以及发布跟踪系统为讨论和改善作品而进行的通信，但不包括由版权所有者以书面形式明显标注或指定为“非投稿”的通信。“投稿者”是指许可方，以及许可方已收到其投稿并随后纳入作品中的任何个人或代表该个人的法律实体。

“贡献者”是指许可方以及代表许可方收到文稿并随后纳入作品的任何个人或法人实体。

**2.** 版权许可的授予。根据此项许可的条款和条件，每位投稿者特此授予您一项永久的、全球性的、非专有的、免费且无版权费的、不可撤销的版权许可，准许您对作品和衍生作品的源形式或目标形式进行复制、制备衍生作品、公开陈列、公开演示、授予分许可，以及分发。

**3.** 专利许可的授予。根据此项许可的条款和条件，每位投稿者特此授予您一项永久的、全球性的、非专有的、免费且无版权费的、不可撤销的（除非本节另有规定）专利许可，准许您制作、已经制作、使用、邀约销售、销售、进口和以其他方式转让作品，此类许可仅适用于投稿者可予许可的专利权利要求，并且如不授予许可，则单独使用其投稿或将其投稿与提交以供纳入其中的作品组合使用必定构成对前述要求的侵权。如果您对任何实体提起专利法律诉讼（包括交叉诉讼或反诉），主张作品或作品中所含投稿构成直接或共同专利侵权，则根据此项许可授予您的针对该作品的任何专利许可都将在提起上述诉讼之日起终止。

**4.** 再分发。您可以在任何介质中以源或对象形式复制和分发作品或其衍生作品的副本，无论是否进行修改，前提是您满足以下条件：

您必须向作品或衍生作品的任何其他接收者提供本许可证的副本；和

您必须在任何已修改的文件上放置醒目的通知，说明您更改了文件；和

您必须在您分发的任何衍生作品的源形式中保留作品的源形式的所有版权、专利、商标和归属声明，不包括与衍生作品任何部分无关的声明；和

如果作品包含“通知”文本文件作为其分发的一部分，则您分发的任何衍生作品必须包括该通知文件中包含的归属通知的可读副本，不包括不属于任何部分的通知衍生作品，至少在以下位置：作为衍生作品的一部分分发的通知文本文件；在源表单或文档中（如果与衍生作品一起提供）；或者，在衍生作品生成的显示中，如果以及通常出现此类第三方通知。声明文件的内容仅供参考，并不构成对许可的修改。您可在您分发的衍生作品中随同作品的声明文本或以附录形式添加自己的归属声明，前提是附加的归属声明不得构成对许可的修改。只要您对作品的使用、复制和分发符合此项许可规定的条件，您可以为自身所做的修改添加自己的版权声明并可就自身所修改内容或任何此类衍生作品作为整体的使用、复制或分发提供附加或不同的许可条款和条件。

**5.** 投稿的提交。除非您明确作出不同声明，否则您向许可方提交的旨在纳入作品中的任何投稿均受此项许可的条款和条件的约束，无任何附加条款或条件。尽管有上述规定，如您与许可方就该等投稿签订了任何单独许可协议，此项许可的条款不得取代或修改该单独许可协议的条款。

**6.** 商标。此项许可并未授予您使用许可方的商号、商标、服务标记或产品名称的权限，除非此类使用是合理和惯例性描述作品来源和复制声明文件内容之所必需。

**7.** 免责声明。除非适用法律要求或达成书面协议，否则许可方均“按原样”提供作品（且每位投稿者均“按原样”提供其投稿），不附带任何明示或默示的保证或条件，包括但不限于关于所有权、非侵权、适销性或适用性的保证或条件。您应全权负责确定使用或再分发作品的适当性，并且承担行使此项许可项下权限的所有风险。

**8.** 责任限制。在任何情况下，在任何法律理论下，无论是侵权（包括过失）、合同或其他理论，除非适用法律要求（例如故意和重大过失行为）或达成书面协议，否则对于您所遭受的损害，包括因此项许可或者因使用或无法使用作品而产生的任何性质的直接、间接、特殊、附带或后果性损害（包括但不限于商誉损失、停工、计算机失效或故障等损害，或任何及所有其他商业损害或损失），任何投稿者概不负责，即使投稿者已被告知发生此类损害的可能性，也是如此。

**9.**接受担保或附加责任。再分发作品或衍生作品时，您可以选择接受与此项许可一致的支持、担保、赔偿或其他责任义务和/或权利，并就此收取费用。但是，在接受上述义务时，您只可代表您自己并对此全权负责，不得代表任何其他投稿者，除非您同意，如因您接受任何此类担保或附加责任，致使此等投稿者承担任何责任或遭受任何索赔，您将对其作出赔偿、为其辩护并保护其免受损害。

条款和条件结束

==========

*** rimraf ***

**ISC** 许可证

版权所有 **(c) Isaac Z. Schlueter** 和贡献者

特此授予出于任何目的使用、复制、修改和/或分发本软件的权限，前提是所有副本中均包含上述版权声明和本许可声明。

本软件按“原样”提供，作者否认与本软件相关的所有担保，包括对适销性和适用性的所有暗示担保。在任何情况下，作者均不对因使用、数据或利润损失而导致的任何特殊、直接、间接或后果性损害负责，无论是因合同、过失或其他原因造成的与本软件的使用或性能相关。

==========

*** uuid ***

版权所有 **(c) 2010-2012 Robert Kieffer**

**MIT** 许可证 - http://opensource.org/licenses/mit-license.php

==========

***** 验证器 *****

版权所有 **(c) 2016 Chris O'Hara<cohara87@gmail.com>**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** 何时 ***

开源计划 **OSI - MIT** 许可证

http://www.opensource.org/licenses/mit-license.php

版权所有 **(c) 2011** 布赖恩·卡瓦利埃

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

# CDO 支持的软件和硬件

CDO 文档介绍其支持的软件和设备。它不会指出 CDO 不支持的软件和设备。如果我们未明确声明对软件版本或设备类型的支持，则表示不支持。

相关信息：

- ASA 支持详情，第 35 页
- CDO 中支持的浏览器，第 36 页

# ASA 支持详情

CDO 可以管理运行 ASA 8.4 及更高版本的所有平台（请参阅每个型号的 ASA 和 ASDM 兼容性），包括 ASAv 实例，但 CDO 不支持的 ASA 服务模块 (ASASM) 除外。

CDO 可以载入运行 ASA 8.3 的 ASA，但不能对其部署更改或以任何其他方式对其进行管理。支持为“只读”。

可能存在不支持所有 ASA 版本的 CDO 功能，例如从 9.12 之前的版本升级 ASA 和 ASDM 升级必备条件。在这些情况下，CDO 文档将列出所有版本例外情况以及该功能的必备条件。

CDO 不管理运行与 ASA 不同的操作系统的 ASA FirePOWER 模块。您必须使用 Firepower 管理中心或 ASDM 单独管理 ASA FirePOWER 模块。

**Note** EOL 代码和硬件可以继续与 CDO 配合使用，但我们无法保证 CDO 的所有功能都与 EOL 代码和硬件有关，因为它不是我们测试的一部分。CDO 不保证也不担保 EOL 软件和硬件的正确操作。例如，EOL ASA 版本 8.x、9.1 和 9.2 在管理平面上不支持 TLS 1.2，被视为管理 ASA 软件的不安全方式。

请遵循思科“建议版本”或“金牌”版本的版本下载页面。

有关 ASA、ASDM 和硬件兼容性的完整讨论，请参阅 Cisco Secure Firewall ASA 兼容性指南。

## 云设备支持详情

下表介绍了基于云的设备的软件和设备类型支持。阅读附属链接，了解有关下表中设备类型的载入和功能的详细信息：

| 设备类型 | 注意 |
|---|---|
| **Google 云平台** | Google 云平台 (GCP) 会通过 GCP 控制台接收任何更新。有关平台和可用服务的详细信息，请参阅 Google Cloud 文档。请参阅 |
| **Microsoft Azure** | Azure 通过 Azure 控制台接收任何更新。有关平台和可用服务的详细信息，请参阅 Azure 文档。 |

# CDO 中支持的浏览器

CDO 支持以下浏览器的最新版本：

- Google Chrome
- Mozilla Firefox

# CDO 平台维护时间表

### CDO 维护时间表

CDO 会每周更新其平台，提供新功能和质量改进。根据此计划，更新可在 3 小时内完成。

表 *1: CDO* 维护时间表

| 星期 | 时间<br>（**24** 小时制） |
|---|---|
| 星期四 | 09:00 UTC - 12:00 UTC |

在此维护期间，您仍然可以访问您的租户，并且如果您有 云交付的防火墙管理中心，也可以访问该平台。此外，您已载入CDO的设备将继续执行其安全策略。

注释 我们建议您在维护期间不要使用 CDO 来在其管理的设备上部署配置更改。

如果发生阻止 CDO 或 云交付的防火墙管理中心 进行通信的故障，则会尽快在所有受影响的租户上解决该故障，即使并非是在维护时间窗口之内。

### 云交付的防火墙管理中心维护时间表

在CDO更新云交付的防火墙管理中心环境前大约1周通知在租户上部署了云交付的防火墙管理中心的客户。通过邮件通知租户的超级管理员和管理员用户。CDO还会在其主页上显示一个横幅，通知所有用户即将发布的更新。

在分配给租户区域的维护日的 3 小时维护期内，对租户进行更新最多可能需要 1 小时。在更新租户时，您将无法访问云交付的防火墙管理中心环境，但仍可访问 CDO 的其余部分。

**表 2: 云交付的防火墙管理中心维护时间表**

| 星期 | 时间<br>（24 小时制） | 地区 |
|---|---|---|
| 星期三 | 04:00 UTC - 07:00 UTC | 欧洲、中东或非洲 (EMEA) |
| 星期三 | 17:00 UTC - 20:00 UTC | 亚太地区-日本 (APJ) |
| 星期四 | 09:00 UTC - 12:00 UTC | 美洲地区 |

# CDO 租户管理

Cisco Defense Orchestrator (CDO) 使您能够在“设置”页面上自定义租户和个人用户帐户的某些方面。在 CDO 菜单栏中，点击左侧导航面板中的**设置 (Settings)**。

## 常规设置

在右上角的“管理”下拉列表中，点击 **设置**。

请参阅以下有关常规 CDO 设置的主题：

- 用户设置, on page 38
- 对于**我的令牌**，请参阅API 令牌, on page 46
- 有关**租户设置**，请参阅：
  - 启用更改请求跟踪, on page 38

## 用户设置

选择所需的 CDO UI 显示语言。此选择仅影响进行此更改的用户。

## 我的令牌

有关详细信息，请参阅 API 令牌。

## 租户设置

### 启用更改请求跟踪

启用更改请求跟踪会影响租户的所有用户。要启用更改请求跟踪，请执行以下程序：

**步骤 1** 在右上角的“管理”下拉列表中，点击**设置 (Settings)**。

**步骤 2** 点击**常规 (General)**选项卡。

**步骤 3** 点击**更改请求跟踪 (Change Request Tracking)** 下的滑块。

确认后，您会在界面的左下角看到“更改请求”(Change Request) 工具栏，并在“更改日志”(Change Log) 中看到“更改请求”(Change Request) 下拉菜单。

### 阻止思科支持人员查看您的租户

思科支持将其用户与您的租户相关联，以解决支持请求或主动修复影响多个客户的问题。但是，如果您愿意，可以通过更改帐户设置来阻止思科支持人员访问您的租户。为此，请滑动“防止思科支持人员查看此租户”下的按钮，以显示绿色复选标记。

要防止思科支持人员查看您的租户，请执行以下程序：

**步骤 1** 在右上角的“管理”下拉列表中，点击 **设置**。

**步骤 2** 点击**常规**选项卡。

**步骤 3** 点击**阻止思科支持人员查看此租户 (Prevent Cisco support from viewing this tenant)** 下的滑块。

## 启用自动接受设备更改的选项

启用设备更改自动接受后， Defense Orchestrator 可以自动接受直接在设备上进行的任何更改。如果禁用或稍后禁用此选项，则需要先查看每个设备冲突，然后才能接受它。

要启用设备更改自动接受，请执行以下程序：

**步骤 1** 在右上角的“管理”下拉列表中，点击 **设置**。

**步骤 2** 点击**常规**选项卡。

**步骤 3** 点击**启用自动接受设备更改的选项 (Enable the option to auto-accept device changes)** 下的滑块。

## 默认冲突检测间隔

此时间间隔将确定CDO轮询已载入的设备以了解更改的频率。此选择会影响使用此租户管理的所有设备，并且可以随时更改。

**Note** 选择一个或多个设备后，可以通过**清单 (Inventory)** 页面中的**冲突检测 (Conflict Detection)** 选项覆盖此选择。

要配置此选项并选择新的冲突检测间隔，请执行以下程序：

**步骤 1** 在右上角的“管理”下拉列表中，点击 **设置**。

**步骤 2** 点击**常规设置 (General Settings)** 选项卡。

**步骤 3** 点击**默认冲突检测间隔 (Default Conflict Detection Interval)** 下拉菜单，然后选择一个时间值。

## 启用计划自动部署的选项

如果启用计划自动部署选项，您就可以计划在方便的未来日期和时间进行部署。启用后，您可以计划单次或定期自动部署。要计划自动部署，请参阅计划自动部署。

请注意，如果其本身的  有待处理的更改，则在CDO上对设备所做的更改不会自动部署到该设备。如果设备未处于**已同步 (Synced)** 状态（例如**检测到冲突 (Conflict Detected)** 或**未同步 (Not Synced)**），则不会执行计划部署。作业页面会列出计划部署失败的所有实例。

如果**启用计划自动部署的选项 (Enable the Option to Schedule Automatic Deployments)** 被关闭，则所有计划的部署都将被删除。

**Important** 如果使用CDO为一台设备创建多个计划部署，则新部署会覆盖现有部署。如果使用 API 创建多个计划部署，则**必须**首先删除现有部署，然后才能计划新的部署。

要启用该选项以计划自动部署，请执行以下程序：

**步骤 1** 在右上角的“管理”下拉列表中，点击 **设置**。

**步骤 2** 点击**常规设置 (General Settings)** 选项卡。

**步骤 3** 点击**启用计划自动部署的选项 (Enable the option to schedule automatic deployments)** 下的滑块。

### Web 分析

网络分析可根据页面点击量向思科提供匿名产品使用情况信息。这类信息包括查看的页面、在页面上花费的时间、浏览器版本、产品版本、设备主机名等。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。

默认启用网络分析。要禁用 Web 分析或在将来启用，请执行以下程序：

**步骤 1** 在右上角的“管理”下拉列表中，点击 **设置**。

**步骤 2** 点击**常规设置 (General Settings)** 选项卡。

**步骤 3** 点击**网络分析 (Web Analytics)** 下的滑块。

### 配置默认定期备份计划

要使设备之间的备份计划保持一致，请使用此设置配置您自己的默认定期备份计划。为特定设备安排备份时，可以使用默认设置或对其进行更改。更改默认定期备份计划不会更改任何现有的计划备份或定期备份计划。

**步骤 1** 在**频率 (Frequency)** 字段中，选择每日、每周或每月备份。

**步骤 2** 选择一天中要进行备份的时间（24 小时制）。请注意，以协调世界时 (UTC) 安排时间。

- 对于每周备份：选中要在星期几进行备份。
- 对于每月备份：点击**当月的天数 (Days of Month)** 字段，然后添加要计划备份的每月日期。注意：如果输入第 31 天，但一个月中没有 31 天，则不会进行备份。为计划的备份时间指定名称和说明。

**步骤 3** 点击**保存 (Save)**。

### 租户 ID

租户 ID 标识租户。如果您需要联系思科技术支持中心 (TAC)，此信息将非常有用。

### 租户名称

您的租户名称还标识您的租户。请注意，租户名称不是组织名称。如果您需要联系思科技术支持中心 (TAC)，此信息将非常有用。

# 租户通知设置

每当与租户关联CDO的设备遇到特定操作、设备证书即将到期或已过期，或者后台日志搜索开始、完成或失败时，都会生成通知。虽然这些通知适用于与您的租户关联的所有设备，但并非所有设备类型都支持所有可用的选项。例如，后台日志搜索仅适用于注册事件日志记录的租户。

在左侧的导航栏中，点击**设置 (Settings)** > **通知设置 (Notification Settings)**。

**Note** 您必须具有**超级管理员**用户角色才能更改这些设置。有关详细信息，请参阅CDO中的用户角色。

### 邮件用户

添加或修改从 CDO 租户接收警报的邮件。有关详细信息，请参阅启用邮件用户, on page 41。

### 服务集成

在您的消息传递应用上**启用传入 Webhook**，并直接将 CDO 通知接收到您的应用控制面板。有关详细信息，请参阅为 CDO 通知启用服务集成。

## 启用邮件用户

来自CDO的邮件通知会指明操作类型和受影响的设备。有关设备当前状态和操作内容的更多信息，我们建议您登录 CDO 并检查受影响设备的变更日志。

**警告** 如果要添加邮件收发器，请务必输入正确的邮箱。CDO不会检查与您的租户关联的已知用户的邮件地址。

### 添加邮件订用

#### 开始之前

您必须是**管理员**才能查看邮件订用列表，而必须是**超级管理员**才能添加、删除或编辑邮件订用。

**步骤 1** 登录 CDO 并导航至 **设置 (Settings)** > **通知设置 (Notification Settings)**。

**步骤 2** 点击页面右上角的 + 图标。

**步骤 3** 请在文本字段中输入有效的邮箱地址。

**步骤 4** 选中和取消选中要通知用户的事件和警报对应的复选框。

**步骤 5** 点击**保存**。在任何时候，点击**取消 (Cancel)** 可为租户创建新的邮件订用。

### 编辑邮件订用

#### 开始之前

您必须是**管理员**才能查看邮件订用列表，而必须是**超级管理员**才能添加、删除或编辑邮件订用。

**步骤 1** 登录 CDO 并导航至 **设置 (Settings)** > **通知设置 (Notification Settings)**。

**步骤 2** 找到要为邮件订用启用编辑的邮件地址。

**步骤 3** 点击**编辑**图标。

**步骤 4** 编辑以下属性：

- 电子邮件地址
- ...时发送警报设备工作流程
- ...时发送警报设备事件
- ...时发送警报后台日志搜索

**步骤 5** 点击**确定**。在任何时候，点击**取消 (Cancel)** 都会取消对邮件订用所做的任何更改。

### 删除邮件订用

使用以下程序可从邮件订用列表中删除邮件收发器：

#### 开始之前

您必须是**管理员**才能查看邮件订用列表，而必须是**超级管理员**才能添加、删除或编辑邮件订用。

**步骤 1** 登录 CDO 并导航至 **设置 (Settings)** > **通知设置 (Notification Settings)**。

**步骤 2** 找到要从租户的邮件订用中删除的用户。

**步骤 3** 点击要删除的用户的**删除**图标。

**步骤 4** 确认要从订用列表中删除用户。请注意，这不会以任何方式影响用户功能。

## 为 CDO 通知启用服务集成

启用服务集成，以便通过指定的消息传送应用或服务来转发CDO通知。您需要从消息传递应用生成 Webhook URL，并将 CDO 指向 CDO 的**通知设置 (Notification Settings)** 页面中的 Webhook 以接收通知。

CDO 本身支持 Cisco Webex 和 Slack 作为服务集成。发送到这些服务的邮件会经过专门的格式化，可用于通道和自动化机器人。

注释 您必须为每个 Webhook 选中要接收的通知的相应复选框。

## Webex Teams 的传入 Webhook

### 开始之前

CDO 通知显示在指定的工作空间中，或显示为私人邮件中的自动化机器人。有关 Webex Teams 如何处理 Webhook 的更多信息，请参阅面向开发人员的 Webex。

使用以下程序为 Webex Teams 允许传入 Webhook：

**步骤 1** 打开 Webex Teams 应用。

**步骤 2** 在窗口的左下角，点击应用图标。此操作将在您的首选浏览器中的新选项卡中打开思科 Webex 应用中心。

**步骤 3** 使用搜索栏查找传入 Webhook。

**步骤 4** 选择**连接 (Connect)**。此操作会在新选项卡中打开 OAuth 授权以允许应用。

**步骤 5** 选择**接受 (Accept)**。该选项卡会自动重定向到应用的配置页面。

**步骤 6** 进行以下配置：

- Webhook 名称 - 提供用于标识此应用提供的消息的名称。
- 选择空间 - 使用下拉菜单选择空间。空间必须已存在于 Webex 团队中。如果空间不存在，您可以在 Webex Teams 中创建新空间并刷新应用的配置页面以显示新空间。

**步骤 7** 选择**添加**。您选择的 Webex Space 将收到添加应用的通知。

**步骤 8** 复制 Webhook URL。

**步骤 9** 登录至 CDO。

**步骤 10** 在左侧的导航栏中，点击**设置 (Settings)** > **通知设置 (Notification Settings)**。

**步骤 11** 检查并确认检查的通知是否正确。如果不正确，强烈建议在连接到服务集成之前修改通知选择。

**步骤 12** 滚动到服务集成。

**步骤 13** 点击蓝色加号按钮。

**步骤 14** 输入 **Name**。此名称在 CDO 中显示为已配置的服务集成。它不会出现在转发到已配置服务的任何事件中。

**步骤 15** 展开下拉菜单并选择 Webex 作为服务类型。

**步骤 16** 粘贴从服务生成的 Webhook URL。

**步骤 17** 点击**确定**。

## Slack 的传入 Webhook

CDO 通知显示在指定渠道中，或显示为私人邮件中的自动机器人。有关 Slack 如何处理传入 Webhook 的详细信息，请参阅 Slack 应用。

使用以下程序允许 Slack 的传入 Webhook：

**步骤 1** 登录您的 Slack 帐户。

**步骤 2** 在左侧的面板中，滚动到底部并选择添加应用。

**步骤 3** 在应用目录中搜索传入 Webhook 并找到该应用。选择**添加**。

**步骤 4** 如果您不是 Slack 工作空间的管理员，则必须向组织的管理员发送请求，并等待应用添加到您的账户。选择请求配置。输入可选消息，然后选择提交请求。

**步骤 5** 为工作空间启用传入 Webhook 应用后，刷新 Slack 设置页面，然后选择将新 Webhook 添加到工作空间。

**步骤 6** 使用下拉菜单选择要在其中显示 CDO 通知的 Slack 通道。选择**授权 (Authorize)**。如果您在等待请求启用时离开此页面，只需登录 Slack 并在左上角选择工作空间名称即可。从下拉菜单中选择**自定义工作空间 (Customize Workspace)**，然后选择**配置应用 (Configure Apps)**。导航至管理自定义集成。 > 选择传入 Webhook 以打开应用的登录页面，然后从选项卡中选择配置。这将列出您的工作空间中启用了此应用的所有用户。您只能查看和编辑账户的配置。选择您的工作空间名称以编辑配置并继续。

**步骤 7** “Slack 设置”页面会将您重定向到应用的配置页面。找到并复制 Webhook URL。

**步骤 8** 登录至 CDO。

**步骤 9** 在左侧的导航栏中，点击**设置 (Settings)** > **通知设置 (Notification Settings)**。

**步骤 10** 检查并确认检查的通知是否正确。如果不正确，强烈建议在连接到服务集成之前修改通知选择。

**步骤 11** 滚动到服务集成。

**步骤 12** 点击蓝色加号按钮。

**步骤 13** 输入 **Name**。此名称在 CDO 中显示为已配置的服务集成。它不会出现在转发到已配置服务的任何事件中。

**步骤 14** 展开下拉菜单并选择 Slack 作为服务类型。

**步骤 15** 粘贴从服务生成的 Webhook URL。

**步骤 16** 点击“确定”。

## 自定义集成的传入 Webhook

### 开始之前

CDO 不会为自定义集成设置消息格式。如果您选择集成自定义服务或应用，CDO 会发送 JSON 消息。

有关如何启用传入 Webhook 和生成 Webhook URL 的信息，请参阅服务文档。获得 Webhook URL 后，请使用以下程序启用 Webhook：

**步骤 1** 从您选择的自定义服务或应用生成并复制 Webhook URL。

**步骤 2** 登录至 CDO。

**步骤 3** 在左侧的导航栏中，点击**设置 (Settings)** > **通知设置 (Notification Settings)**。

**步骤 4** 检查并确认检查的通知是否正确。如果不正确，强烈建议在连接到服务集成之前修改通知选择。

**步骤 5** 滚动到服务集成。

**步骤 6** 点击蓝色加号按钮。

**步骤 7** 输入 **Name**。此名称在 CDO 中显示为已配置的服务集成。它不会出现在转发到已配置服务的任何事件中。

**步骤 8** 展开下拉菜单并选择自定义作为服务类型。

**步骤 9** 粘贴从服务生成的 Webhook URL。

**步骤 10** 点击“确定”。

# 日志记录设置

查看每月事件日志记录限制以及限制重置前剩余的天数。请注意，存储的日志记录表示思科云接收的压缩事件数据。

点击“查看历史使用情况”可查看租户在过去 12 个月内收到的所有日志记录。

您还可以使用链接请求额外的存储空间。

# 将 SAML 单点登录与 Cisco Defense Orchestrator 集成

思科防御协调器 (CDO) 使用 Cisco Secure Sign-On 作为 SAML 单点登录身份提供商 (Idp)，并使用 Duo Security 进行多因素身份验证 (MFA)。这是 CDO 的首选身份验证方法。

但是，如果客户希望将自己的 SAML 单点登录 IdP 解决方案与 CDO 集成，只要他们的 IdP 支持 SAML 2.0 和身份提供程序启动的工作流程，就可以。

要将您自己的或第三方身份提供程序 (IdP) 与思科安全云登录集成，请参阅《思科安全云登录身份提供程序集成指南》。

如果您需要更多支持来将您自己的SAML解决方案与CDO集成，您必须联系支持人员并创建案例。

**Attention** 提交支持案例时，请确保为您的请求选择**手动选择技术 (Manually Select A Technology)**，然后选择**SecureX - 登录和管理 (SecureX - Sign-on and Administration)**，以便与正确的团队联系。

# 更新 SSO 证书

您的身份提供程序 (IdP) 通常与 SecureX SSO 集成。创建思科 TAC 支持案例并提供 metadata.xml 文件。https://www.cisco.com/c/en/us/support/index.html有关更多信息，请参阅《思科 SecureX 登录第三方身份提供程序集成指南》。

**注意** 当您提交支持案例时，请确保为您的请求选择手动选择技术，然后选择 SecureX - 登录和管理，以便联系正确的团队。

（仅限旧版）如果您的身份提供程序 (IdP) 直接与 CDO 集成，请向 CDO TAC 提交支持请求，并提供 metadata.xml 文件。CDO 客户如何通过 TAC 提交支持请求，第 535 页

# API 令牌

开发人员在进行 CDO REST API 调用时使用 CDO API 令牌。必须在 REST API 授权报头中插入 API 令牌，调用才能成功。API 令牌是“长期”访问令牌，不会过期；但是，您可以续订和撤销它们。

您可以从 CDO 中生成 API 令牌。这些令牌仅在生成后立即可见，并且只要“常规设置”页面处于打开状态。如果您在 CDO 中打开另一个页面并返回到**常规设置 (General Settings)** 页面，则该令牌不再可见，但很明显已发出令牌。

个人用户可以为特定租户创建自己的令牌。一个用户不能代表另一个用户生成令牌。令牌特定于账户-租户对，不能用于其他用户-租户组合。

## API 令牌格式和声明

API 令牌是 JSON Web 令牌 (JWT)。要了解有关 JWT 令牌格式的更多信息，请阅读 JSON Web 令牌简介。https://jwt.io/introduction/

CDO API 令牌提供以下一组声明：

- id - 用户/设备 uid
- parentId - 租户 uid
- ver - 公钥的版本（初始版本为 0，例如 cdo_jwt_sig_pub_key.0）
- 订用 - 订用（可选）安全服务交换
- client_id - " api-client "
- jti - 令牌 ID

## 令牌管理

### 生成 API 令牌

**步骤 1** 在左侧的导航栏中，点击**设置 (Settings)** > **常规设置 (General Settings)**。

**步骤 2** 在我的令牌中，点击生成 API 令牌。

**步骤 3** 根据企业维护敏感数据的最佳实践，将令牌保存在安全位置。

### 续订 API 令牌

API 令牌不会过期。但是，如果令牌丢失、遭到破坏或符合其企业的安全准则，用户可以选择更新其 API 令牌。

**步骤 1** 在左侧导航栏中，点击 **设置 (Settings)** > **常规设置 (General Settings)**。

**步骤 2** 在“我的令牌”(My Tokens) 中，点击**续约 (Renew)**。CDO 会生成新的令牌。

**步骤 3** 根据企业维护敏感数据的最佳实践，将新令牌保存在安全位置。

### 撤销 API 令牌

**步骤 1** 在左侧导航栏中，点击 **设置 (Settings)** > **常规设置 (General Settings)**。

**步骤 2** 在“我的令牌”(My Tokens) 中，点击**撤销 (Revoke)**。CDO 将撤销令牌。

# 身份提供程序账户与思科防御协调器用户记录之间的关系

要登录思科防御协调器 (CDO)，客户需要具有符合 SAML 2.0 标准的身份提供程序 (IdP)、多因素身份验证提供程序以及 CDO 中的用户记录。IdP 账户包含用户的凭证，IdP 根据这些凭证对用户进行身份验证。多因素身份验证提供了额外的身份安全层。CDO 用户记录主要包含用户名、与其关联的 CDO 租户以及用户的角色。当用户登录时，CDO 会尝试将 IdP 的用户 ID 映射到 CDO 中租户的现有用户记录。当 CDO 找到匹配项时，用户将登录到该租户。

除非您的企业有自己的单点登录身份提供程序，否则身份提供程序是思科安全云登录。Cisco Security Cloud Sign On 使用 Duo 进行多因素身份验证。客户可以选择将 SAML 单点登录与 Cisco Defense Orchestrator 集成。

## 登录工作流程

以下是 IdP 账户如何与 CDO 用户记录交互以登录 CDO 用户的简化说明：

**步骤 1** 用户通过登录到符合 SAML 2.0 标准的身份提供程序 (IdP)（例如 Cisco Security Cloud Sign On (https://sign-on.security.cisco.com)）来请求访问 CDO，以进行身份验证。

**步骤 2** IdP 发出用户真实可信的 SAML 断言，门户显示用户可以访问的应用，例如表示 https://defenseorchestrator.com 或 https://defenseorchestrator.eu 或 https://www.apj.cdo 的磁贴.cisco.com/。https://defenseorchestrator.com/ https://defenseorchestrator.eu/https://www.apj.cdo.cisco.com/

**步骤 3** CDO 验证 SAML 断言，提取用户名并尝试在其租户中查找与该用户名对应的用户记录。

- 如果用户在 CDO 上的单个租户上有用户记录，则 CDO 会向用户授予对租户的访问权限，并且用户的角色决定了他们可以执行的操作。
- 如果用户在多个租户上有用户记录，则CDO会向经过身份验证的用户显示可供他们选择的租户列表。用户选择一个租户并允许访问该租户。用户在该特定租户上的角色决定了他们可以执行的操作。
- 如果 CDO 没有将经过身份验证的用户映射到租户上的用户记录，则 CDO 会显示一个登录页面，让用户有机会了解有关 CDO 的更多信息或请求免费试用。

在 CDO 中创建用户记录不会在 IdP 中创建账户，在 IdP 中创建账户不会在 CDO 中创建用户记录。

同样，删除 IdP 上的账户并不意味着您已从 CDO 中删除用户记录；但是，如果没有 IdP 账户，则无法向 CDO 对用户进行身份验证。删除 CDO用户记录并不意味着您已删除 IdP 账户；但是，如果没有 CDO用户记录，经过身份验证的用户将无法访问 CDO 租户。

# 此架构的含义

### 使用 Cisco Security Cloud Sign On 的客户

对于使用 CDO 的 Cisco Security Cloud Sign On 身份提供程序的客户，超级管理员可以在 CDO 中创建用户记录，并且用户可以向 CDO 自行注册。如果两个用户名匹配，并且用户已正确进行身份验证，则用户可以登录 CDO。

如果超级管理员需要阻止用户访问 CDO，他们只需删除 CDO 用户的用户记录即可。Cisco Security Cloud Sign On 账户仍然存在，如果超级管理员想要恢复用户，他们可以使用与 Cisco Security Cloud Sign On 相同的用户名创建新的 CDO 用户记录。

如果客户遇到需要致电我们的技术支持中心 (TAC) 的 CDO 问题，客户可以为 TAC 工程师创建用户记录，以便他们可以调查租户并向客户报告信息和建议。

### 拥有自己的身份提供程序的客户

对于将 SAML 单点登录与 Cisco Defense Orchestrator 集成，他们可以控制身份提供程序账户和 CDO 租户。这些客户可以在 CDO 中创建和管理身份提供程序账户和用户记录。

如果他们需要阻止用户访问 CDO，他们可以删除 IdP 账户和/或 CDO 用户记录。

如果他们需要思科 TAC 的帮助，他们可以为其 TAC 工程师创建具有只读角色的身份提供程序账户和 CDO 用户记录。然后，TAC 工程师将能够访问客户的 CDO 租户，进行调查，并向客户报告信息和建议。

### 思科托管服务提供商

如果思科托管服务提供商 (MSP) 使用 CDO 的 Cisco Security Cloud Sign On IdP，则他们可以自行注册 Cisco Security Cloud Sign On，他们的客户可以在 CDO 中为其创建用户记录，以便 MSP 可以管理客户的租户。当然，客户可以在选择时完全控制删除 MSP 的记录。

### 相关主题

- 常规设置
- 在 CDO 中管理用户
- CDO中的用户角色

# 管理多租户门户

CDO 多租户门户视图检索并显示来自多个租户的所有设备的信息。此多租户门户显示设备状态、设备上运行的软件版本等。

**Note** 在多租户门户中，您可以跨多个区域添加租户，并查看这些租户管理的设备。您无法从多租户门户编辑任何租户或配置任何设备。

### 准备工作

多租户门户仅在您的租户上启用该功能时可用。要为租户启用多租户门户，请向思科 TAC 提交支持请求。解决支持请求并创建门户后，门户上具有“超级管理员”(Super Admin) 角色的用户就可以向其添加租户。

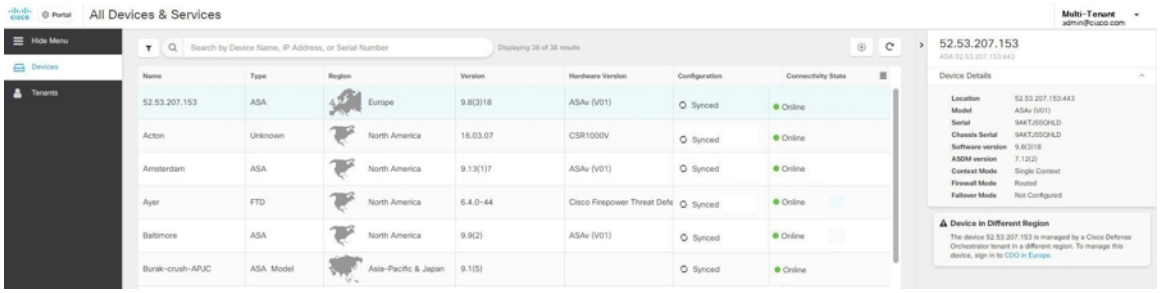
我们建议您从 Web 浏览器清除缓存和 Cookie，以避免可能发生的某些浏览器相关问题。

### 多租户门户

门户提供以下菜单：

- **设备：**
  - 显示驻留在添加到门户的租户中的所有设备。使用过滤器和搜索字段搜索要查看的设备。您可以点击设备以查看其状态、载入方法、防火墙模式、故障切换模式、软件版本等。
  - 该界面提供了一个列选择器，允许您选择或清除要在表中查看的设备属性。除“AnyConnect 远程访问 VPN”外，默认情况下会选择所有其他设备属性。如果您自定义表，CDO 会在您下次登录 CDO 时记住您的选择。
  - 您可以点击设备以在右侧查看其详细信息。
  - 您可以将 门户信息导出为逗号分隔值 (.csv) 文件。此信息可帮助您分析设备或将其发送给无权访问的人员。每次导出数据时，CDO 都会创建一个新的 .csv 文件，其中创建的文件会在名称中包含日期和时间。
  - 您只能从管理设备的 CDO 租户管理设备。多租户门户提供**管理设备 (Manage devices)** 链接，可将您定向到CDO租户页面。如果您在该租户上有账户，并且该租户与门户位于同一区域，您将在设备上看到此链接。如果您没有访问租户的权限，您将看不到管理设备链接。您可以联系组织中的超级管理员获取权限。

**Note** 如果管理设备的租户位于其他区域，您将在该区域看到用于登录 CDO 的链接。如果您无权访问该区域中的 CDO 或该区域中的租户，您将无法管理设备。




- 租户：
  - 显示添加到门户的租户。
  - 它允许超级管理员用户将租户添加到门户。
  - 您可以点击 查看 CDO 租户的主页。

## 将租户添加到多租户门户

具有超级管理员角色的用户可以向门户添加租户。您可以跨多个区域添加租户。例如，您可以将欧洲区域的租户添加到美国区域，反之亦然。

**Important** 我们建议您为租户创建仅 API 用户，并生成用于向 CDO 进行身份验证的 API 令牌。

**Note** 如果要将多个租户添加到门户，请从每个租户生成 API 令牌并将其粘贴到文本文件中。然后，您可以轻松地将租户逐个添加到门户，而无需每次都切换到租户以生成令牌。

**步骤 1** 在左侧的导航栏中，点击**设置 (Settings)** > **常规设置 (General Settings)** > **我的令牌 (My Tokens)**。

**步骤 2** 点击生成 API 令牌，然后复制它。

**步骤 3** 转到门户，然后点击租户选项卡。

**步骤 4** 点击右侧的添加租户按钮。

**步骤 5** 粘贴令牌，然后点击保存。

## 从多租户门户删除租户

**步骤 1** 转到门户，然后点击租户选项卡。

**步骤 2** 点击右侧显示的相应删除图标，删除所需的租户。

**步骤 3** 点击**删除 (Remove)**。关联的设备也会从门户中删除。

## 管理租户门户设置

Cisco Defense Orchestrator （ Defense Orchestrator ）使您能够在“设置”页面上自定义多租户门户和个人用户帐户的某些方面。点击左侧导航栏中的设置，访问**设置 (Settings)** 页面。

### 设置

#### 常规设置

网络分析可根据页面点击量向思科提供匿名产品使用情况信息。这类信息包括查看的页面、在页面上花费的时间、浏览器版本、产品版本、设备主机名等。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。

默认启用网络分析。要禁用 Web 分析或在将来启用，请执行以下程序：

1. 在 CDO 控制面板中，点击左侧导航栏中的**设置 (Settings)**。
2. 点击 **General Settings**。
3. 点击**网络分析 (Web Analytics)** 下的滑块。

#### 用户管理

您可以在**用户管理 (User Management)** 屏幕上查看与多租户门户关联的所有用户记录。您可以添加、编辑或删除用户帐户。有关详细信息，请参阅在 CDO 中管理用户。

### 切换租户

如果您有多个门户租户，则可以在不同的门户或租户之间切换，而无需注销 CDO。

**步骤 1** 在多租户门户上，点击右上角显示的租户菜单。

**步骤 2** 点击**切换租户 (Switch tenant)**。

**步骤 3** 选择要查看的门户或租户。

# 思科成功网络

思科成功网络是一项用户启用的云服务。启用思科成功网络时，设备与思科云之间会建立安全连接以传输使用情况信息和统计信息。数据流遥测提供一种机制，可从设备选择相关数据，并以结构化的格式将其传输至远程管理站，从而获得以下优势：

- 通知您在网络中可用来改进产品效果的未使用功能。
- 通知您适用于您产品的其他技术支持服务和监控。
- 帮助思科改善我们的产品。

设备将建立并始终维护该安全连接，使您能够注册思科成功网络。注册设备后，可以更改思科成功网络设置。

注释

- 对于 威胁防御可用性对，主用设备的选择会覆盖备用设备上的思科成功网络设置。
- CDO 不会管理思科成功网络设置。通过 防火墙设备管理器用户界面管理的设置和遥测信息。

### 启用或禁用思科成功网络

在初始系统设置期间，系统会提示您将设备注册到思科智能软件管理器。如果您选择使用90天的评估许可证，必须在评估期结束前注册设备。要注册该设备，请使用思科智能软件管理器（在“智能许可”页面上）注册该设备，或者通过输入注册密钥使用CDO进行注册。

注册设备时，您的虚拟帐户会向设备分配许可证。注册设备也会注册已启用的任何可选许可证。

您可以通过禁用思科成功网络随时关闭此连接，但只能通过 防火墙设备管理器 UI 禁用此选项。禁用上述功能将断开设备与云的连接。断开连接不会影响接收更新或运行智能许可功能，该功能将继续正常运行。有关详细信息，请参阅《Firepower 设备管理器配置指南》（6.4.0 版或更高版本）**系统管理**一章的“连接到思科成功网络”部分。

# 在 CDO 中管理用户

在CDO中创建或编辑用户记录之前，请阅读身份提供程序账户与思科防御协调器用户记录之间的关系以了解身份提供程序 (IdP) 账户与用户记录的交互方式。CDO 用户需要 CDO 记录和相应的 IdP 账户，这样他们才能通过身份验证并访问您的 CDO 租户。

除非您的企业有自己的 IdP，否则思科安全登录是所有 CDO 租户的身份提供程序。本文的其余部分假设您使用思科安全登录作为身份提供程序。

您可以在**用户管理 (User Management)** 屏幕上查看与您的租户关联的所有用户记录。这包括临时与您的账户关联以解决支持请求的任何思科支持工程师。

## 查看与您的租户关联的用户记录

从 CDO 导航栏中，点击**设置 (Settings)** > **用户管理 (User Management)**。

注释 要防止思科支持人员访问您的租户，请在“常规设置”页面中配置您的账户设置。常规设置，第 37 页

# 用户管理中的 Active Directory 组

对于大量用户的高周转率的租户，您可以将 CDO 映射到 Active Directory (AD) 组，而不是将个人用户添加到CDO，以便更轻松地管理用户列表和用户角色。任何用户更改（例如添加新用户或删除现有用户）现在都可以在 Active Directory 中完成，而不再需要在 CDO 中完成。

您必须具有超级管理员用户角色，才能从“用户管理”页面添加、编辑或删除 AD 组。有关详细信息，请参阅CDO中的用户角色。

### “Active Directory 组”选项卡

**设置 (Settings)** 页面的“用户管理”(User Management) 部分具有当前映射到 CDO 的 Active Directory 组的选项卡。最重要的是，此页面显示 AD 管理器中分配的 AD 组的角色。

AD 组中的用户不会在 Active Directory Groups 选项卡或 Users 选项卡中单独列出。

### “审核日志”选项卡

“设置”(Settings) 页面的“用户管理”(User Management) 部分有一个用于审核日志的选项卡。此新部分显示访问 CDO 租户的所有用户的最后登录时间，以及每个用户在上次登录时的角色。这包括显式用户登录和 AD 组登录。

### 多角色用户

作为 CDO 中 IAM 功能的扩展，用户现在可以拥有多个角色。

一个用户可以属于 AD 中的多个组，并且每个组都可以在 CDO 中定义为不同的 CDO 角色。用户在登录时获得的最终权限是用户所属的 CDO 中定义的所有 AD 组的角色的组合。例如，如果用户属于两个 AD 组，并且这两个组都以两个不同的角色（例如仅编辑和仅部署）添加到 CDO 中，则该用户将同时具有仅编辑和仅部署权限。这适用于任意数量的组和角色。

AD 组映射只需在 CDO 中定义一次，然后通过在不同组之间添加、删除或移动用户，即可在 AD 中实现对用户的访问和权限管理。

**注释** 如果用户既是单个用户又是同一租户上的 AD 组的一部分，则单个用户的用户角色将覆盖 AD 组的用户角色。

# 准备工作

在将 AD 组映射作为用户管理形式添加到 CDO 之前，您必须将 AD 与 SecureX 集成。如果您的 AD 身份提供程序 (IdP) 尚未集成，可向思科 TAC 提交支持案例，并请求使用以下信息进行自定义 AD IdP 集成：

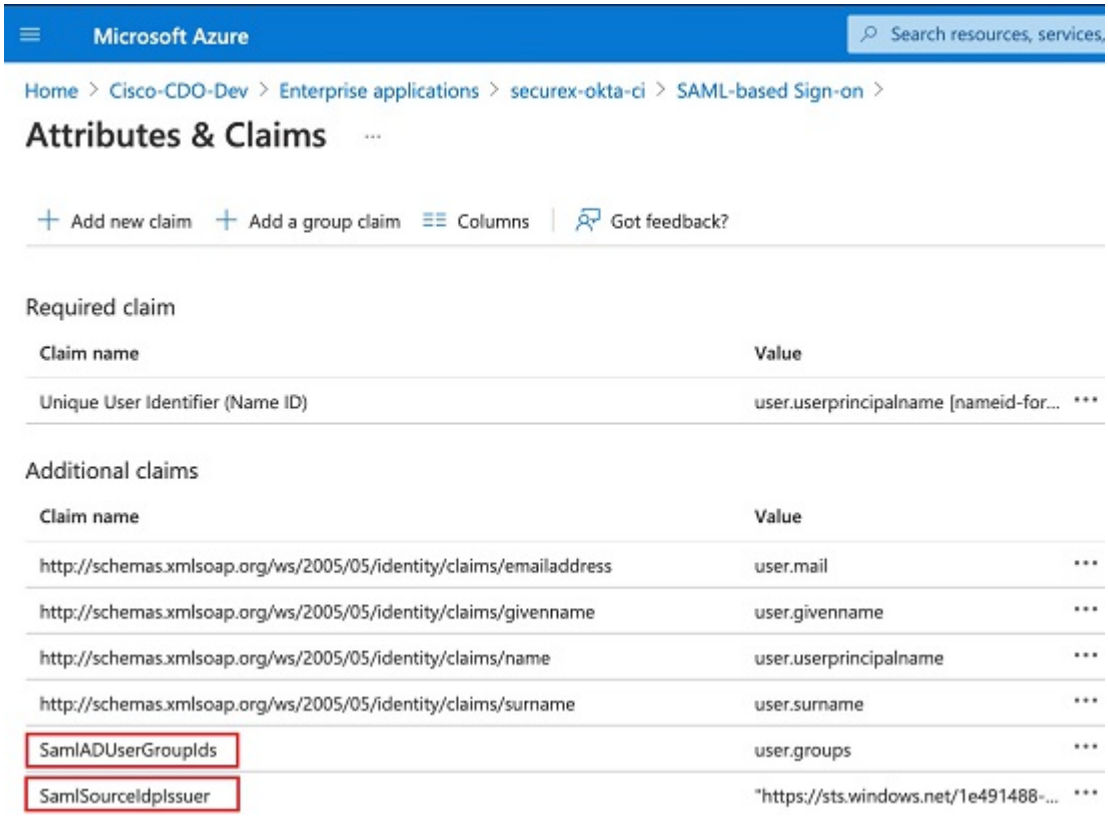
- 您的 CDO 租户名称和区域
- 定义自定义路由的域（例如：@cisco.com、@myenterprise.com）

- XML 格式的证书和联合元数据

AD 集成完成后，在 AD 中添加以下自定义 SAML 声明。要在 AD 集成完成后成功登录 CDO 租户，必须提供 SAML 声明和属性。请注意，这些值区分大小写：

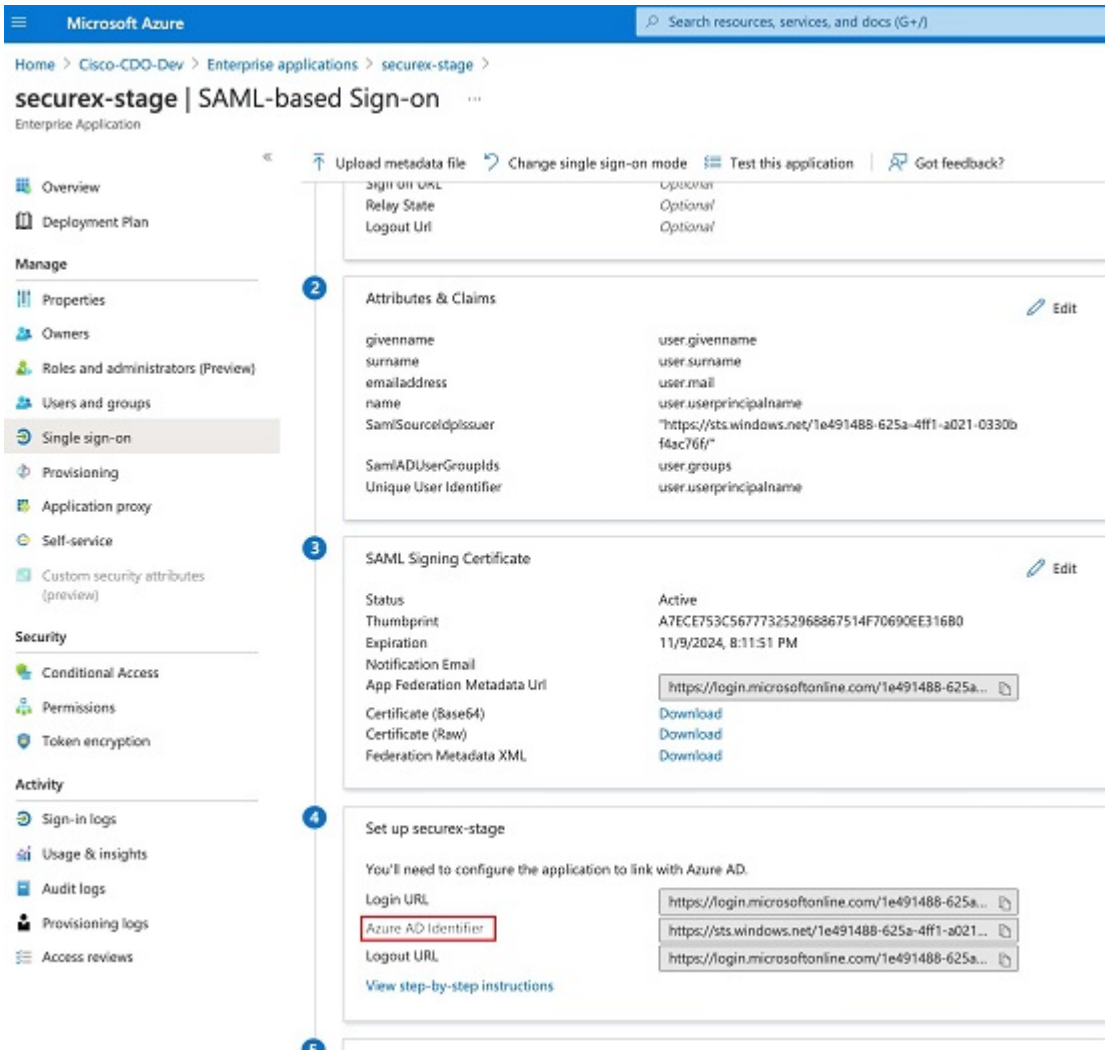
- SamlADUserGroupIds - 此属性描述用户在 AD 上的所有组关联。例如，在 Azure 中选择 + 添加组申领，如下面的屏幕截图所示：

**图 *1: Active Directory* 中定义的自定义声明**




- SamlSourceIdpIssuer - 此属性唯一标识 AD 实例。例如，在 Azure 中选择 + 添加组申领，然后滚动查找 Azure AD 标识符，如下面的屏幕截图所示：

图 2: 找到 *Azure Active Directory* 标识符




# 添加用于用户管理的 Active Directory 组

**步骤 1** 登录 CDO。

**步骤 2** 在右上角的“管理”下拉列表中，点击 **设置**。

**步骤 3** 点击 **用户管理** 选项卡。

**步骤 4** 选择表顶部的 Active Directory 组选项卡。

**步骤 5** 如果当前没有 AD 组，请点击添加 AD 组。如果有现有条目，请点击添加按钮。

**步骤 6** 输入以下信息：

- **组名称 (Group Name)** - 输入唯一的名称。此名称不必与 AD 中的组名称匹配。CDO 不支持此字段的特殊字符。

- 组标识符 - 从您的 AD 手动输入组标识符。组标识符的值应与自定义声明定义中的组标识符相同。它可以是与组的唯一标识对应的任何值，例如，my-f Favorite-group、12345 等。
- AD 颁发者 - 手动输入 AD 中的 AD 颁发者值。
- 角色 - 确定此 AD 组中包含的所有用户的角色。有关详细信息，请参阅用户角色。
- （可选）备注 - 添加适用于此 AD 组的任何备注。

**步骤 7** 点击**确定**。

# 编辑用于用户管理的 Active Directory 组

**开始之前**

请注意，在 CDO 中编辑 AD 组的用户管理仅允许修改 CDO 如何限制 AD 组。您无法在 CDO 中编辑 AD 组本身。必须使用 AD 编辑 AD 组中的用户列表。

**步骤 1** 登录 CDO。
**步骤 2** 在右上角的“管理”下拉列表中，点击 **设置**。
**步骤 3** 点击 **用户管理** 选项卡。
**步骤 4** 选择表顶部的 Active Directory 组选项卡。
**步骤 5** 确定要编辑的 AD 组，然后选择编辑图标。
**步骤 6** 修改以下值：

- **组名称 (Group Name)** - 输入唯一的名称。CDO 不支持此字段的特殊字符。
- 组标识符 - 从您的 AD 手动输入组标识符。组标识符的值应与自定义声明定义中的组标识符相同。它可以是与组的唯一标识对应的任何值，例如，my-f Favorite-group、12345 等。
- AD 颁发者 - 手动输入 AD 中的 AD 颁发者值。
- 角色 - 确定此 AD 组中包含的所有用户的角色。有关详细信息，请参阅用户角色。
- 备注 - 添加适用于此 AD 组的任何备注。

# 删除用于用户管理的 Active Directory 组

**步骤 1** 登录 CDO。
**步骤 2** 在右上角的“管理”下拉列表中，点击 **设置**。
**步骤 3** 点击 **用户管理** 选项卡。

**步骤 4** 选择表顶部的 Active Directory 组选项卡。

**步骤 5** 确定要删除的 AD 组。

**步骤 6** 选择删除图标。

**步骤 7** 点击确定以确认要删除 AD 组。

# 创建新的 CDO 用户

要创建新的 CDO 用户，需要执行这两项任务。它们不需要按顺序执行：

- 为新用户创建 Cisco Security Cloud Sign On 账户
- 使用您的 CDO 用户名创建 CDO 用户记录

完成这些任务后，用户可以新用户从思科安全登录控制面板打开 CDO。

# 为新用户创建 Cisco Security Cloud Sign On 账户

新用户可以随时自行创建 Cisco Security Cloud Sign On 账户。他们不需要知道他们将被分配到的租户的名称。

## 关于登录 CDO

思科防御协调器 (CDO) 使用 Cisco Security Sign On 作为身份提供程序，并使用 Duo 进行多重身份验证 (MFA)。**要登录 CDO，必须先在 Cisco Security Cloud Sign On 中创建账户，然后再使用 Duo 配置 MFA**。

CDO 需要 MFA，它为保护您的用户身份提供额外的一重保障。双因素身份验证（一种 MFA）需要两个部分或因素来确保登录CDO的用户身份真实。第一个因素是用户名和密码，第二个是按需生成的一次性密码 (OTP)。

**Important** **如果您的 CDO 租户在 2019 年 10 月 14 日之前就已存在**，请使用 迁移到 Cisco Security Cloud Sign On 身份提供程序, on page 4 登录说明，而不是本文。

## 登录前

**安装 DUO Security**。我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。

**时间同步**。您要使用移动设备生成一次性密码。由于OTP是基于时间的，所以您的设备时钟与实时同步是非常重要的。请确保您的设备时钟自动或手动设置为正确的时间。

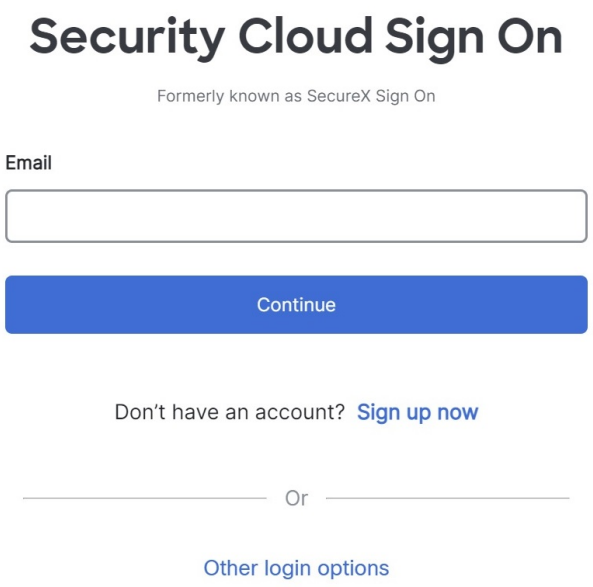
# 创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证

初始登录工作流程分为四步。您需要完成所有四个步骤。

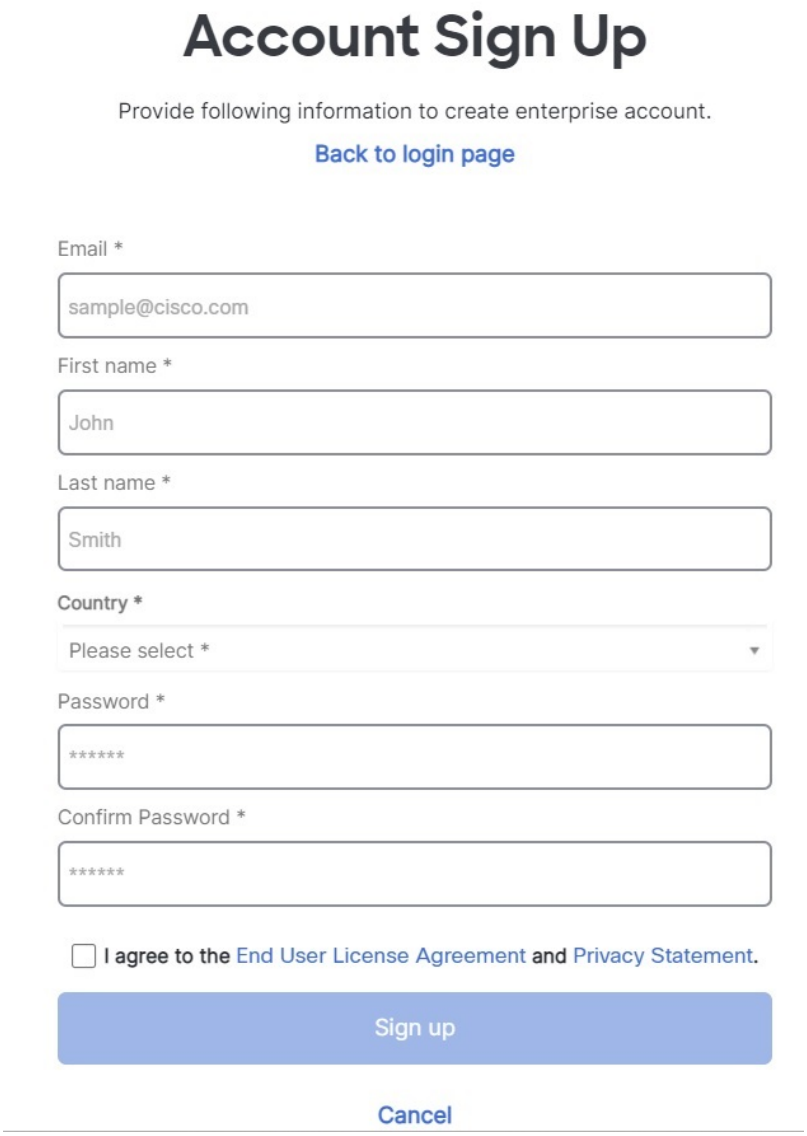
**步骤 1** 注册新的 Cisco 安全云登录 帐户。

**a.** 浏览到 https://sign-on.security.cisco.com。

**b.** 在“登录”(Sign In) 屏幕的底部，点击**立即注册 (Sign up now)**。




**c.** 填写“创建帐户”(Create Account) 对话框中的字段。




我们为您提供了以下提示：

- **电子邮件 (Email)** - 输入您最终将用于登录 CDO 的邮箱地址。
- **密码 (Password)** - 输入强密码。

**d.** 在您点击**创建帐户 (Create Account)** 之后。

Cisco 会将验证电子邮件发送到您注册的地址。打开电子邮件，然后点击**激活帐户 (Activate Account)**。

**步骤 2 使用 Duo 设置多因素身份验证**

我们建议在设置多因素身份验证时使用移动设备。

**a.** 在**设置多因素身份验证 (Set up multi-factor authentication)** 屏幕中，点击**配置因素 (Configure factor)**。

b. 点击**开始设置 (Start setup)**，按照提示选择移动设备，然后验证该移动设备与您的账户是否配对。

有关详细信息，请参阅 Duo 双因素身份验证指南：注册指南。如果您的设备上已经有 Duo 应用，您将收到此帐户的激活代码。Duo 支持一个设备上的多个帐户。

c. 在向导结束时，点击**继续登录**。

d. 通过双因素身份验证登录 Cisco 安全云登录 。

**步骤 3** （可选）**将 Google 身份验证器设置为附加身份验证器**

a. 选择要与 Google Authenticator 配对的移动设备，然后点击**下一步**。

b. 按照安装向导中的提示设置 Google Authenticator。

**步骤 4** **配置思科 安全云登录 的账户恢复选项**

a. 选择恢复电话号码以使用 SMS 重置帐户。

b. 选择安全图像。

c. 点击**创建帐户**。

# 使用您的 CDO 用户名创建 CDO 用户记录

只有具有“超级管理员”权限的 CDO 用户才能创建 CDO 用户记录。超级管理员应使用上述 **创建您的 CDO 用户名** 任务中指定的相同邮箱地址创建用户记录。

使用以下程序创建具有适当用户角色的用户记录：

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 导航栏中，点击**设置 (Settings)** > **用户管理 (User Management)**。

**步骤 3** 点击蓝色加号按钮 (  )，将新用户添加到租户。

**步骤 4** 提供用户的邮件地址。

**Note** 用户的邮箱地址必须与 Cisco Secure Log-On 账户的邮箱地址相对应。

**步骤 5** 从下拉菜单中选择用户的CDO中的用户角色。

**步骤 6** 点击**确定**。

# 新用户从思科安全登录控制面板打开 CDO

**步骤 1** 在 Cisco Secure Sign-On 控制板上点击适当的 **CDO** 磁贴。**CDO** 磁贴会将您导向 https://defenseorchestrator.com，而 **CDO (EU)** 磁贴会将您导向 https://defenseorchestrator.eu。

**步骤 2** 请点击身份验证器徽标以选择 Duo Security 或 Google Authenticator， 如果您已设置这两个身份验证器。

- 如果您在现有租户上已有用户记录，则将登录该租户。
- 如果您在多个门户上已有用户记录，您将能够选择要连接的门户。
- 如果您在若干租户上已有用户记录，则将能够选择要连接的 CDO 租户。
- 如果您在现有租户上尚无用户记录，将能够了解有关 CDO 的详细信息或申请试用租户。

门户视图检索并显示来自多个租户的整合信息。有关详细信息，请参阅管理多租户门户。

租户视图显示您拥有用户记录的多个租户。


# CDO中的用户角色

思科防御协调器 (CDO) 中有多种用户角色：只读、仅编辑、仅部署、管理员和超级管理员。为每个租户上的每个用户配置用户角色。如果 CDO 用户可以访问多个租户，则他们可能具有相同的用户 ID，但在不同的租户中具有不同的角色。用户可能在一个租户上具有只读角色，在另一个租户上具有超级管理员角色。当接口或文档提及只读用户、管理员用户或超级管理员用户时，我们描述的是该用户对特定租户的权限级别。

# 只读角色

分配了只读角色的用户会在每个页面上看到此蓝色横幅：

Read Only User. You cannot make configuration changes.

具有只读角色的用户可以执行以下操作：

- 查看 CDO 中的任何页面或任何设置。
- 搜索和过滤任何页面的内容。
- 比较设备配置，查看更改日志，并查看 VPN 映射。
- 查看有关任何页面上的任何设置或对象的每个警告。
- 生成、刷新和撤销自己的 API 令牌。请注意，如果只读用户撤销自己的令牌，则无法重新创建令牌。
- 通过我们的界面联系支持人员，并可以导出更改日志。

只读用户不能执行以下操作：

- 创建、更新、配置或删除任何页面上的任何内容。
- 载入设备。
- 逐步完成创建对象或策略等内容所需的任务，但无法保存。
- 创建 CDO 用户记录。
- 更改用户角色。
- 将访问规则附加或分离到策略。

# 仅编辑角色

具有“仅编辑”角色的用户可以执行以下操作：

- 编辑和保存设备配置，包括但不限于对象、策略、规则集、接口、VPN 等。
- 允许通过读取配置操作进行配置更改。
- 利用“变更请求管理”操作。

仅编辑用户不能执行以下操作：

- 将更改部署到一台设备或多台设备。
- 丢弃暂存的更改或通过 OOB 检测到的更改。
- 上传 AnyConnect 软件包，或配置这些设置。
- 为设备安排或手动启动映像升级。

- 计划或手动启动安全数据库升级。
- 在 Snort 2 和 Snort 3 版本之间手动切换。
- 创建模板。
- 更改现有的 OOB Change 设置。
- 编辑系统管理设置。
- 载入设备。
- 删除设备。
- 删除 VPN 会话或用户会话。
- 创建 CDO 用户记录。
- 更改用户角色。

# 仅部署角色

具有“仅部署”角色的用户可以执行以下操作：

- 将暂存更改部署到一台设备或多台设备。
- 恢复或恢复 ASA 设备的配置更改。
- 为设备安排或手动启动映像升级。
- 计划或手动启动安全数据库升级。
- 利用“变更请求管理”操作。

仅部署用户不能执行以下操作：

- 在 Snort 2 和 Snort 3 版本之间手动切换。
- 创建模板。
- 更改现有的 OOB Change 设置。
- 编辑系统管理设置。
- 载入设备。
- 删除设备。
- 删除 VPN 会话或用户会话。
- 创建、更新、配置或删除任何页面上的任何内容。
- 载入设备。
- 逐步完成创建对象或策略等内容所需的任务，但无法保存。

- 创建 CDO 用户记录。
- 更改用户角色。
- 将访问规则附加或分离到策略。

# VPN 会话管理器角色

“VPN 会话管理器”(Sessions Manager) 角色专为监控远程访问 VPN 连接而非站点间 VPN 连接的管理员而设计。

具有 VPN 会话管理器角色的用户可以执行以下操作：

- 查看 CDO 中的任何页面或任何设置。
- 搜索和过滤任何页面的内容。
- 比较设备配置，查看更改日志，并查看 RA VPN 映射。
- 查看有关任何页面上的任何设置或对象的每个警告。
- 生成、刷新和撤销自己的 API 令牌。请注意，如果 VPN 会话管理器用户撤销其自己的令牌，则无法重新创建该令牌。
- 通过我们的界面联系支持人员并导出更改日志。
- 终止现有的 RA VPN 会话。

VPN 会话管理器用户不能执行以下操作：

- 创建、更新、配置或删除任何页面上的任何内容。
- 载入设备。
- 逐步完成创建对象或策略等内容所需的任务，但无法保存。
- 创建 CDO 用户记录。
- 更改用户角色。
- 将访问规则附加或分离到策略。

# 管理角色

管理员用户对 CDO 的大多数方面具有完全访问权限。管理员用户可以执行以下操作：

- 在 CDO 中创建、读取、更新和删除任何对象或策略，并配置任何设置。
- 载入设备。
- 查看 CDO 中的任何页面或任何设置。
- 搜索和过滤任何页面的内容。

- 比较设备配置，查看更改日志，并查看 VPN 映射。
- 查看有关任何页面上的任何设置或对象的每个警告。
- 生成、刷新和撤销自己的 API 令牌。如果他们的令牌被撤销，他们可以通过我们的界面联系支持人员，并可以导出更改日志。

管理员用户不能执行以下操作：

- 创建 CDO 用户记录。
- 更改用户角色。

# 超级管理员角色

超级管理员用户可以完全访问 CDO 的所有方面。超级管理员可以执行以下操作：

- 更改用户角色。
- 创建用户记录。

**Note** 虽然超级管理员可以创建CDO用户记录，但该用户记录并不是用户登录租户所需的全部内容。用户还需要具有租户使用的身份提供程序的账户。除非您的企业有自己的单点登录身份提供程序，否则身份提供程序是思科安全云登录。用户可以自行注册 Cisco Security Cloud Sign On 账户；有关详细信息，请参阅新 CDO 租户的初始登录, on page 3。

- 在 CDO 中创建、读取、更新和删除任何对象或策略，并配置任何设置。
- 载入设备。
- 查看 CDO 中的任何页面或任何设置。
- 搜索和过滤任何页面的内容。
- 比较设备配置，查看更改日志，并查看 VPN 映射。
- 查看有关任何页面上的任何设置或对象的每个警告。
- 生成、刷新和撤销自己的 API 令牌。如果他们的令牌被撤销，他们可以
- 通过我们的界面联系支持人员，并可以导出更改日志。

# 更改用户角色的记录

用户记录是当前记录的用户角色。通过查看与您的租户关联的用户，您可以确定每个用户的记录。通过更改用户角色，您可以更改用户记录。用户的角色通过其在“用户管理”表中的角色进行标识。有关详细信息，请参阅在 CDO 中管理用户。

您必须是超级管理员才能更改用户记录。如果您的租户没有超级管理员，请联系CDO客户如何通过TAC 提交支持请求。

# 将用户帐户添加到 CDO

CDO 用户需要 CDO 记录和相应的 IdP 账户，以便他们可以进行身份验证并访问您的 CDO 租户。此程序会在 Cisco Security Cloud Sign On 中创建用户的 CDO 用户记录，而不是用户的账户。如果用户在 Cisco Security Cloud Sign On 中没有账户，则可以通过导航到 https://sign-on.security.cisco.com 并点击**登录 (Sign up)** 屏幕底部的“注册”来自行注册。

**Note** 您需要在 CDO 上具有超级管理员角色角色才能执行此任务。

## 创建用户记录

使用以下程序创建具有适当用户角色的用户记录：

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 导航栏中，点击**设置 (Settings)** > **用户管理 (User Management)**。

**步骤 3** 点击蓝色加号按钮 (+)，将新用户添加到租户。

**步骤 4** 提供用户的邮件地址。

**Note** 用户的邮箱地址必须与 Cisco Secure Log-On 账户的邮箱地址相对应。

**步骤 5** 从下拉菜单中选择用户的CDO中的用户角色。

**步骤 6** 点击 v。

**Note** 虽然超级管理员可以创建CDO用户记录，但该用户记录并不是用户登录租户所需的全部内容。用户还需要具有租户使用的身份提供程序的账户。除非您的企业有自己的单点登录身份提供程序，否则身份提供程序是思科安全登录。用户可以自行注册 Cisco Secure Sign-On 账户；有关详细信息，请参阅新 CDO 租户的初始登录, on page 3。

## 创建仅 API 用户

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 导航栏中，点击**设置 (Settings)** > **用户管理 (User Management)**。

**步骤 3** 点击蓝色加号按钮 (+)，将新用户添加到租户。

**步骤 4** 选择**仅 API 用户 (API Only User)** 复选框。

**步骤 5** 在用户名字段中，输入用户的名称，然后点击确定。

**重要事项** 用户名不能是邮件地址或包含“@”字符，因为“@yourtenant”后缀将自动附加到用户名。

**步骤 6** 从下拉菜单中选择用户的CDO中的用户角色。

**步骤 7** 点击**确定**。

**步骤 8** 点击 **用户管理** 选项卡。

**步骤 9** 在新的仅 API 用户的令牌列中，点击生成 API 令牌以获取 API 令牌。

# 编辑用户角色的用户记录

您需要具有超级管理员的角色才能执行此任务。如果超级管理员更改已登录的CDO用户的角色，则在其角色更改后，该用户将自动从其会话中注销。用户重新登录后，他们将承担新角色。

**Note** 您需要在 CDO 上具有超级管理员角色角色才能执行此任务。

**Caution** 更改用户记录的角色将删除与用户记录关联的 API 令牌（如果有）。API 令牌, on page 46用户角色更改后，用户必须生成新的 API 令牌。

## 编辑用户角色

**Note** 如果 CDO 用户已登录，并且超级管理员更改其角色，则该用户必须注销并重新登录，更改才会生效。

要编辑用户记录中定义的角色，请执行以下程序：

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 导航栏中，点击**设置 (Settings)** > **用户管理 (User Management)**。

**步骤 3** 点击用户行中的编辑图标。

**步骤 4** 从“角色”(Role) 下拉菜单中选择用户的新CDO中的用户角色。

**步骤 5** 如果用户记录显示有与用户关联的 API 令牌，则需要确认要更改用户的角色并删除 API 令牌。

**步骤 6** 点击 **v**。

**步骤 7** 如果 CDO 删除了 API 令牌，请联系用户，以便他们可以创建新的 API 令牌。

# 删除用户角色的用户记录

删除 CDO 中的用户记录会破坏用户记录与 Cisco Security Cloud Sign On 账户的映射，从而防止关联用户登录 CDO。删除用户记录时，也会删除与该用户记录关联的 API 令牌（如果有）。删除 CDO 中的用户记录不会删除 Cisco Security Cloud Sign On 中的用户 IdP 账户。

**Note** 您需要在 CDO 上具有超级管理员角色角色才能执行此任务。

## 删除用户记录

要删除用户记录中定义的角色，请参阅以下程序：

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 导航栏中，点击**设置 (Settings)** > **用户管理 (User Management)**。

**步骤 3** 点击要删除的用户所在行的垃圾桶图标。

**步骤 4** 点击**确定 (OK)**。

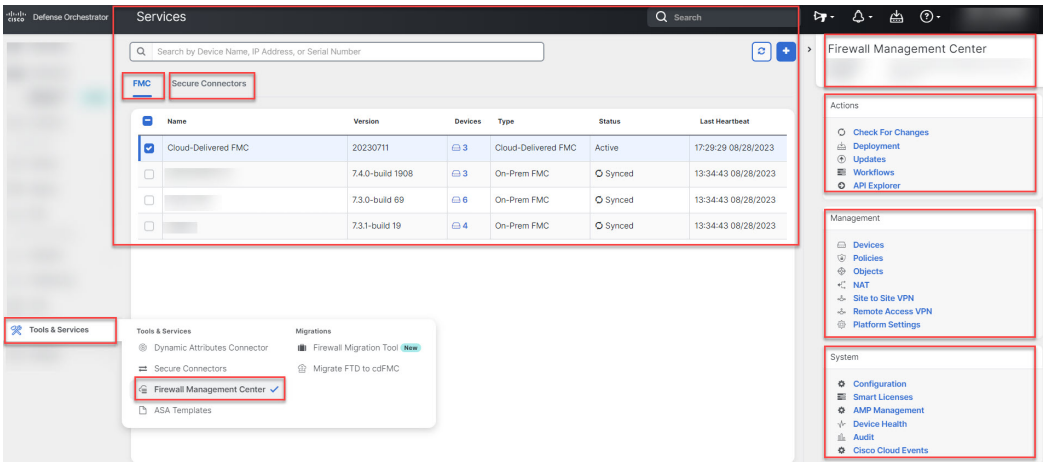
**步骤 5** 点击确定，确认要从租户中删除帐户。

# CDO 服务页面

**服务 (Services)** 页面显示 CDO 提供的服务列表。选择 **FMC** 选项卡，系统将列出与 云交付的防火墙管理中心 账户关联的 CDO 和所有已注册到 本地管理中心 的 CDO。由这些本地管理中心管理的设备在**清单 (Inventory)** 页面中列出。**服务** 页面还列出 **安全连接器** 选项卡下的安全连接器。

您可以点击 **FMC** 选项卡并通过点击蓝色加号图标 (+) 载入 本地管理中心，然后使用右侧窗格中的选项执行设备操作。您还可以查看设备信息，例如版本、管理中心管理的设备数量、设备类型以及设备的同步状态。点击受管设备图标会将您带到**清单 (Inventory)** 页面，其中将自动过滤并显示所选 本地管理中心 管理的设备。**服务** 页面还允许您一次选择多个 本地管理中心，以便一次性对一组管理中心执行操作。选择 云交付的防火墙管理中心 时，不能选择任何 本地管理中心。要添加新的安全连接器或对现有安全连接器执行操作，请选择**安全连接器 (Secure Connectors)** 选项卡，然后点击 +。

导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。




对于 云交付的防火墙管理中心，“服务”页面显示以下信息：

- 如果您的租户上没有部署 云交付的防火墙管理中心，请点击**启用云交付的 FMC (Enable Cloud-Delivered FMC)**。有关更多信息，请参阅为您的 CDO 租户启用云交付的防火墙管理中心。
- 上部署的设备数量。Secure Firewall Threat Defense云交付的防火墙管理中心
- 与页面之间的连接状态。CDO云交付的防火墙管理中心
- 的最后一次心跳。云交付的防火墙管理中心这表示上次将 云交付的防火墙管理中心 本身的状态及其管理的设备数量与此页面上的表同步。
- 所选对象的主机名。云交付的防火墙管理中心

选择**云交付的 FMC (Cloud-Delivered FMC)**，然后使用**操作 (Actions)**、**管理 (Management)** 或**设置 (Settings)** 窗格中的链接，打开 云交付的防火墙管理中心 用户界面以执行与点击的链接关联的配置任务。

**操作 (Actions)**：

- **检查更改 (Check For Changes)**：表中的设备计数和状态信息将使用上次此页面和 云交付的防火墙管理中心 同步时可用的信息进行更新。每 10 分钟进行一次同步。
- **部署 (Deployment)**：转到 云交付的防火墙管理中心上的设备配置部署页面。请参阅部署配置更改。
- **工作流程 (Workflows)**：转到**工作流程 (Workflows)** 页面，以监控 CDO 在与设备通信时运行的每个进程。请参阅工作流程页面。
- **API Explorer**：转到列出 云交付的防火墙管理中心 REST API 的页面。请参阅 Cisco Secure Firewall Management Center REST API。

**管理**：

- **设备 (Devices)**：将您带到 云交付的防火墙管理中心 门户上的 威胁防御 设备列表页面。请参阅配置设备。

- **策略 (Policies)**：转至 云交付的防火墙管理中心 门户上的策略页面来编辑系统提供的访问控制策略，并创建自定义访问控制策略。请参阅管理访问控制策略。
- **对象 (Objects)**：将您引导至 云交付的防火墙管理中心 门户上的策略页面，以管理可重用对象。请参阅对象管理。
- **NAT**：将您引导至 云交付的防火墙管理中心 门户上的策略页面，以在 威胁防御 设备上配置网络地址转换策略。请参阅管理 NAT 策略。
- **站点间 VPN (Site to Site VPN)**：将您引导至 云交付的防火墙管理中心 门户上的站点间 VPN 控制面板页面，以配置两个站点之间的站点间 VPN 策略。请参阅站点间 VPN。
- **远程访问 VPN (Remote Access VPN)**：将您引导至 云交付的防火墙管理中心 门户上的远程访问 VPN 控制面板页面，以配置远程访问 VPN 配置。请参阅远程访问 VPN。
- **平台设置 (Platform Settings)**：转至 云交付的防火墙管理中心 门户上的平台设置页面来配置您可能希望在多台设备之间共享其值的一系列无关功能。请参阅平台设置。

**系统：**

- **配置 (Configuration)**：将您引导至 云交付的防火墙管理中心 门户上的系统配置设置页面，以配置系统配置设置。请参阅系统配置。
- **智能许可证 (Smart Licenses)**：将您引导至 云交付的防火墙管理中心 门户上的智能许可证页面，以将许可证分配给设备。请参阅将许可证分配到设备。
- **AMP 管理 (AMP Management)**：将您带到 云交付的防火墙管理中心 门户上的 AMP 管理页面，该页面提供系统用于检测和阻止网络上的恶意软件的情报。请参阅恶意软件防护的云连接。
- **设备运行状况 (Device Health)**：转至 云交付的防火墙管理中心 门户上的运行状况监控页面，运行状况监控跟踪各种运行状况指标，以确保系统中的硬件和软件正常工作。请参阅关于运行状况监控。
- **审核 (Audit)**：将您引导至 云交付的防火墙管理中心 门户上的审核日志页面，以显示为每个用户与 Web 界面交互生成的审核记录。
- **思科云事件 (Cisco Cloud Events)**：将您引导至 CDO 门户上的配置思科云事件页面，将 [ 云交付的防火墙管理中心 配置为将事件直接发送到 SAL (SaaS)。请参阅将事件发送到 SAL (SaaS)。

打开 云交付的防火墙管理中心 页面后，点击蓝色问号按钮，然后选择 **页面级帮助** 以了解有关您所在页面的详细信息，以及您可以采取的进一步操作。

### 支持在不同的选项卡上打开 CDO 和 云交付的防火墙管理中心 应用

在 云交付的防火墙管理中心 中配置 威胁防御 设备或对象时，您可以在其他浏览器选项卡中打开相应的配置页面，以便在 CDO 和 云交付的防火墙管理中心 门户中同时工作，而无需注销。例如，您可以在 云交付的防火墙管理中心 上创建对象，同时监控从安全策略生成的 CDO 上的事件日志。

此功能适用于导航到 云交付的防火墙管理中心 门户的所有 CDO 链接。要在新选项卡中打开 云交付的防火墙管理中心 门户，请执行以下操作：

在 CDO 门户上，按住 **Ctrl** (Windows) 或 **Command** (Mac) 按钮，然后点击相应的链接。

注释 点击一下即可在同一选项卡中打开 云交付的防火墙管理中心 页面。

以下是在新选项卡中打开 云交付的防火墙管理中心 门户页面的一些示例：

- 选择**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 并选择 **云交付的 FMC (Cloud-Delivered FMC)**。

  在右侧窗格中，按住 **Ctrl** (Windows) 或 **Command** (Mac) 按钮，然后点击要访问的页面。

- 选择 **对象** > **其他 FTD 对象**。
- 点击CDO页面右上角的搜索图标，然后在显示的搜索字段中输入搜索字符串。

  在搜索结果中，按住 **Ctrl** (Windows) 或 **Command** (Mac) 按钮，然后点击箭头图标。

- 选择 **控制面板** > **快速操作**。

  按住 **Ctrl** (Windows) 或 **Command** (Mac) 按钮，然后点击 **管理 FTD 策略** 或 **管理 FTD 对象**。

注释 当您切换到新的 CDO 租户时，已在新选项卡中打开的相应 云交付的防火墙管理中心 门户将注销。

**相关主题**

- 使用思科防御协调器管理本地部署防火墙管理中心
- 载入本地防火墙管理中心
- 为您的 CDO 租户申请云交付的防火墙管理中心
- 安全设备连接器
- 安全事件连接器

# CDO 设备和服务管理

Cisco Defense Orchestrator (CDO) 提供在**清单 (Inventory)** 页面上查看、管理、过滤和评估已载入设备的功能。在**清单 (Inventory)** 页面中，您可以：

- 用于 CDO 管理的载入设备和服务。
- 查看受管设备和服务的配置状态和连接状态。
- 在单独的选项卡中查看已载入的设备和模板。请参阅CDO 清单信息，第 78 页。
- 评估各个设备和服务并采取措施。
- 查看设备和服务特定信息并解决问题。

- 查看由以下人员管理的威胁防御设备的设备运行状况：
  - 云交付的防火墙管理中心
  - 本地管理中心

  对于 云交付的防火墙管理中心 管理的威胁防御设备，您还可以查看集群中设备的节点状态。
- 按名称、类型、IP 地址、型号名称、序列号或标签搜索设备或模板。搜索不区分大小写。提供多个搜索词会调出至少与其中一个搜索词匹配的设备和服务。请参阅页面级搜索，第 80 页。
- 设备或模板过滤器可按设备类型、硬件和软件版本、Snort 版本、配置状态、连接状态、冲突检测以及保护设备连接器和标签进行过滤。请参阅过滤器。

# 在 CDO 中更改设备的 IP 地址

在使用 IP 地址将设备载入 Cisco Defense Orchestrator (CDO) 时，CDO 会将该 IP 地址存储在其数据库中，并使用该 IP 地址与设备通信。如果设备的 IP 地址发生更改，您可以更新 CDO 中存储的 IP 地址以匹配新地址。在 CDO 上更改设备的 IP 地址不会更改设备的配置。

要更改 CDO 用于与设备通信的 IP 地址，请执行以下程序：

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击设备类型选项卡。

您可以使用 过滤器 和 页面级搜索 功能查找所需的设备。

**步骤 4** 选择要更改其 IP 地址的设备。

**步骤 5** 在**设备详细信息 (Device Details)** 窗格上方，点击设备 IP 地址旁边的编辑按钮。


**步骤 6** 在字段中输入新的 IP 地址，然后点击蓝色的复选按钮。

设备本身不会发生更改，因此设备的配置状态将继续显示已同步。

**相关信息：**

- 在租户之间移动设备, on page 77
- 将设备批量重新连接到 CDO, on page 77

# 在 CDO 中更改设备的名称

所有设备、型号、模板和服务在载入或在CDO中创建时都会获得一个名称。您可以更改该名称，而无需更改设备本身的配置。

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击**设备 (Device)** 选项卡以找到设备。

**步骤 3** 选择要更改其名称的设备。

**步骤 4** 在**设备详细信息 (Device Details)** 窗格上方，点击设备名称旁边的编辑按钮。


**步骤 5** 在字段中输入新的名称，然后点击蓝色的复选按钮。

设备本身不会发生更改，因此设备的配置状态将继续显示已同步。

# 导出设备和服务列表

本文介绍如何将设备和服务列表导出为逗号分隔值 (.csv) 文件。转换为该格式后，您可以在电子表格应用（例如 Microsoft Excel）中打开该文件，以对列表中的项目进行排序和过滤。

导出按钮在设备和模板选项卡中可用。您还可以从所选设备类型选项卡下的设备导出详细信息。

在导出设备和服务列表之前，请查看过滤器窗格并确定清单表是否显示要导出的信息。清除所有过滤器以查看所有受管设备和服务，或过滤信息以显示所有设备和服务的子集。导出功能会导出您在清单表中看到的内容。

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击相应的设备类型选项卡以从该选项卡下的设备导出详细信息，或点击**全部 (All)** 以从所有设备导出详细信息。

您可以使用 过滤器 和 页面级搜索 功能查找所需的设备。

**步骤 4** 点击**将列表导出到 CSV (Export list to CSV)**：


**步骤 5** 如果出现提示，请保存 .csv 文件。

**步骤 6** 在电子表格应用中打开 .csv 文件，对结果进行排序和过滤。

# 导出设备配置

一次只能导出一个设备配置。使用以下程序将设备的配置导出到 JSON 文件：

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

您可以使用 过滤器 和 页面级搜索 功能查找所需的设备。

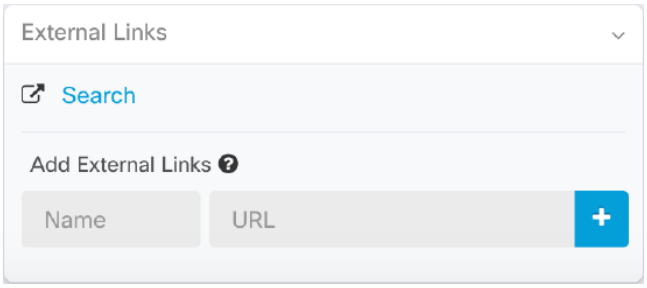
**步骤 4** 选择所需的设备以便将其突出显示。

**步骤 5** 在操作窗格中，选择导出配置。

**步骤 6** 选择确认以将配置另存为 JSON 文件。

# 设备的外部链接

您可以创建指向外部资源的超链接，并将其与您使用CDO管理的设备相关联。您可以使用此功能创建指向其中一个设备的本地管理器的便捷链接（适用于 ASA 的自适应安全设备管理器 (ASDM)）。您还可以使用它来链接到搜索引擎、文档资源、公司 Wiki 或您选择的任何其他 URL。您可以根据需要将任意数量的外部链路与设备关联。您还可以同时将同一链路与多个设备关联。




您创建的链路可以到达任何地方，但您公司的安全要求不会改变。例如，如果您通常需要通过本地部署或通过 VPN 连接来访问特定 URL，则这些要求仍然存在。如果您的公司阻止特定 URL，这些 URL 将继续被阻止。不受限制的 URL 将继续不受限制。

### 位置变量

我们已创建 {location} 变量，您可以将其合并到您的 URL 中。此变量将填充设备的 IP 地址。例如，

```
https://{location}
```

应连通 ASA 的 ASDM 。

**相关信息：**

- 编写设备说明, on page 77
- 导出设备和服务列表, on page 73

## 从您的设备创建外部链路

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择设备或型号。

您可以使用 过滤器 和 页面级搜索 功能查找所需的设备。

**步骤 5** 在右侧的详细信息窗格中，转到“外部链接”部分。

**步骤 6** 输入链接的名称。

**步骤 7** 在 URL 字段中输入链接的 URL。您需要指定完整的 URL，例如，对于思科，请输入 http://www.cisco.com。http://www.cisco.com/

**步骤 8** 点击 + 将链接与设备关联。

## 创建到 ASDM FDM 的外部链路

以下是直接从 CDO 打开 ASA 的自适应安全设备管理器 (ASDM) 和 FTD 的 Firepower 设备管理器 (FDM) 的便捷方法。

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

您可以使用 过滤器 和 页面级搜索 功能查找所需的设备。

**步骤 4** 选择设备或型号。

**步骤 5** 在右侧的详细信息窗格中，转到“外部链接”部分。

**步骤 6** 输入链路的名称，例如 ASDM FDM。

**步骤 7** 在 URL 字段中输入 https://{location}。{location} 变量将填充设备的 IP 地址。

**步骤 8** 点击 + 框。

## 为多个设备创建外部链路

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

您可以使用过滤器和页面级搜索功能来查找所需的设备。

**步骤 4** 请选择多个设备或型号。

**步骤 5** 在右侧的详细信息窗格中，转到“外部链接”部分。

**步骤 6** 输入链接的名称。

**步骤 7** 使用以下方法之一输入要访问的 URL：

- 输入

  ```
  https://{location}
  ```

  在 URL 字段中。{location} 变量将填充设备的 IP 地址。这会为您的设备创建指向 ASDM 的自动链接。

- 在 URL 字段中输入链接的 URL。您需要指定完整的 URL，例如，对于思科，请输入 http://www.cisco.com。http://www.cisco.com/

**步骤 8** 点击 + 将链接与设备关联。

## 编辑或删除外部链接

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

您可以使用 过滤器 和 页面级搜索 功能查找所需的设备。

**步骤 4** 选择设备或型号。

**步骤 5** 在右侧的详细信息窗格中，转到“外部链接”部分。

**步骤 6** 将鼠标悬停在链接名称上可显示编辑和删除图标。

**步骤 7** 点击相应的图标可编辑或删除外部链接，并确认您的操作。

## 编辑或删除多台设备的外部链接

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

您可以使用过滤器和页面级搜索功能来查找所需的设备。

**步骤 4** 请选择多个设备或型号。

**步骤 5** 在右侧的详细信息窗格中，转到“外部链接”部分。

**步骤 6** 将鼠标悬停在链接名称上可显示编辑和删除图标。

**步骤 7** 点击相应的图标可编辑或删除外部链接，并确认您的操作。

# 将设备批量重新连接到 CDO

CDO 允许管理员同时尝试将多个受管设备重新连接到 CDO。当设备 CDO 管理的 标记为“无法访问”时，CDO无法再检测到带外配置更改或管理设备。断开连接可能有许多不同的原因。尝试重新连接设备是恢复 CDO 对设备的管理的简单第一步。

**Note** 如果您要重新连接具有新证书的设备，CDO会自动审核并接受设备上的新证书，并继续与其重新连接。但是，如果您仅与一台设备重新连接，CDO会提示您手动查看并接受证书，以继续与其重新连接。

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击 **设备** 选项卡以找到设备。

**步骤 3** 点击设备类型选项卡。

使用过滤器查找连接状态为“无法访问”的设备。

**步骤 4** 从过滤结果中，选择要尝试重新连接的设备。

**步骤 5** 点击**重新连接 (Reconnect)** 。请注意，CDO 仅提供可应用于所有选定设备的操作的命令按钮。

**步骤 6** 查看**通知 (notifications)** 选项卡，了解批量设备重新连接操作的进度。如果您想了解有关批量设备重新连接作业中的操作是如何成功或失败的更多信息，请点击蓝色查看链接，您将被定向到 作业页面, on page 338。

**Tip** 如果由于设备的证书或凭证已更改而导致重新连接失败，则必须单独重新连接到这些设备，以添加新凭证并接受新证书。

# 在租户之间移动设备

在将设备载入 CDO 租户后，无法将设备从一个 CDO 租户迁移到另一个租户。如果要将设备移至新租户，您需要从旧租户中删除设备并将其重新载入新租户。

# 编写设备说明

使用此程序为设备创建单个纯文本注释文件。

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要为其创建备注的设备或型号。

**步骤 5** 在左侧的**管理 (Management)** 窗格中，点击**备注 (Notes)**。 Notes。

**步骤 6** 点击右侧的编辑器按钮，然后选择默认文本编辑器、Vim 或 Emacs 文本编辑器。

**步骤 7** 编辑“备注”(Notes) 页面。

**步骤 8** 点击**保存 (Save)**。
注释会被保存在选项卡中。

# CDO 清单信息

**清单 (Inventory)** 页面显示所有已载入的物理和虚拟设备以及从已激活设备创建的模板。该页面根据设备和模板的类型对其进行分类，并在专用于每种设备类型的相应选项卡中显示它们。您可以使用页面级搜索功能或应用过滤器在所选设备类型选项卡中查找设备。

您可以在此页面上查看以下详细信息：

- **设备 (Devices)** 选项卡显示载入 CDO 的所有实时设备。
- **模板 (Templates)** 显示从实时设备或导入到 CDO 的配置文件创建的所有模板设备。

# CDO 标签和过滤

标签用于对设备或对象进行分组。您可以在载入期间或在载入之后随时将标签应用于一台或多台设备。您可以在创建对象后对其应用标签。将标签应用于设备或对象后，即可按该标签过滤设备表或对象表的内容。

**注释** 应用于设备的标签不会扩展到其关联对象，应用于共享对象的标签不会扩展到其关联对象。

可以使用以下语法“group name:label”创建标签组。例如，Region: East 或 Region:West。如果您要创建这两个标签，则组标签将为区域，您可以在该组中选择 East 或 West。

## 将标签应用于设备和对象

要将标签应用于设备，请执行以下步骤：

**步骤 1** 要向设备添加标签，请点击左侧导航窗格中的**设备和服务 (Devices & Services)**。要向对象添加标签，请点击左侧导航窗格中的**对象 (Objects)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 在生成的表中选择一个或多个设备或型号。

**步骤 5** 在右侧的添加组和标签字段中，指定设备的标签。

**步骤 6** 点击蓝色 + 图标。

# 过滤器

您可以在**清单 (Inventory)** 和**对象 (Objects)** 页面上使用许多不同的过滤器来查找要查找的设备和对象。

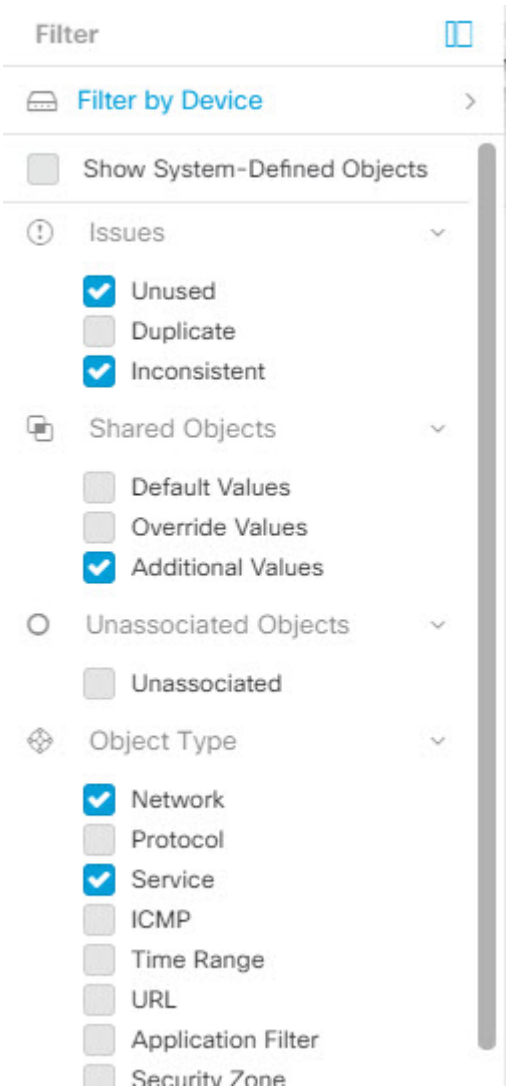
要过滤，请点击清单、策略和对象选项卡的左侧窗格中的 ：

清单过滤器允许您按设备类型、硬件和软件版本、Snort 版本、配置状态、连接状态、冲突检测以及保护设备连接器和标签进行过滤。您可以应用过滤器在所选设备类型选项卡中查找设备。您可以使用过滤器在所选设备类型选项卡中查找设备。

对象过滤器允许您按设备、问题类型、共享对象、未关联的对象和对象类型进行过滤。您可以在结果中包含或不包含系统对象。您还可以使用搜索字段在过滤器结果中搜索包含特定名称、IP 地址或端口号的对象。

过滤设备和对象时，您可以组合搜索词来创建多个潜在的搜索策略来查找相关结果。

在以下示例中，过滤器应用于“问题（已使用或不一致）AND 具有其他值的共享对象 AND 类型为网络 OR 服务的对象”。




# 使用 CDO 搜索功能

CDO 平台具有高效的搜索功能，可以轻松查找任何所需的内容。每个页面上的搜索栏都根据该页面的内容进行定制，而全局搜索则允许在整个租户中进行全面搜索。这可以节省时间和精力，因为您可以快速找到必要的信息。

## 页面级搜索

通过页面级搜索，您可以搜索“清单”(Inventory)、“策略”(Policies)、“对象”(Objects)、“VPN”、“更改日志”(Change Log) 和“作业”(Jobs) 页面上的特定项目。

- 在**清单 (Inventory)** 空间中，您只需在搜索栏中开始键入，就会显示符合搜索条件的设备。您可以键入设备的任何部分名称、IP 地址或物理设备的序列号来查找设备。

- 在**策略 (Policies)** 空间中，您可以按策略名称、策略中使用的组件或对象进行搜索。
- 您可以在**对象 (Objects)** 空间中通过键入对象名称的任何部分或部分 IP 地址、端口、或协议来查找对象。
- 在 **VPN** 空间中，您可以按 VPN 策略中使用的隧道名称、设备名称和 IP 地址进行搜索。
- 在**更改日志 (Change log)** 空间中，您可以根据事件、设备名称或操作搜索日志。

**步骤 1** 导航到界面顶部附近的搜索栏。

**步骤 2** 在搜索栏中键入搜索条件，系统将显示相应的结果。

# 全局搜索

通过全局搜索功能，您可以快速查找并导航至 管理的设备。CDO

所有搜索结果都基于您选择的索引选项。索引选项如下：

- 完整索引 - 要求调用完整索引过程。此过程会扫描系统中的所有设备和对象，并仅在调用索引后将其显示在搜索索引中。要调用完全索引，您必须具有管理权限。

  有关详细信息，请参阅启动完全索引，第 82 页。

- 增量索引 - 一种基于事件的索引过程，每次添加、修改或删除设备或对象时，搜索索引都会自动更新。

您在搜索字段中输入的信息不区分大小写。您可以使用以下实体执行全局搜索：

- 设备名称 - 支持部分设备名称、URL、IP 地址或范围。
- 对象类型 - 支持对象名称、对象说明和配置的值。
- 策略类型 - 支持策略名称、策略说明、规则名称和规则注释。

  在 CDO 中管理的云交付防火墙管理中心和本地 FMC 支持以下策略类型：

  - 访问控制策略
  - 预过滤器策略
  - 威胁防御 NAT 策略

键入搜索表达式时，界面开始显示搜索结果，您无需按 Enter 键即可执行搜索。

搜索结果将显示与您的搜索字符串匹配的所有设备和对象。如果搜索字符串与多个设备或对象匹配，则结果将显示在类别（设备、对象和 connected_fmc）下。

默认情况下，搜索结果中的第一个项目会突出显示，并且该项目的相关信息显示在右侧窗格中。您可以滚动浏览搜索结果，然后点击任何项目以查看相应的信息。您可以点击项目旁边的箭头图标以导航到相应的页面。

注释

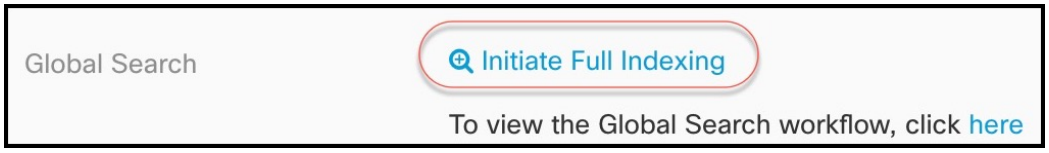
- 全局搜索不显示重复的搜索结果。对于对象，共享对象的 UID 用于导航到对象视图。
- 如果从 中删除设备，则会从全局搜索索引中删除所有关联对象。CDO
- 如果在启动完全索引之前从策略中删除对象并保留设备，则该对象将保留在全局搜索索引中，因为它与设备关联。

## 启动完全索引

**步骤 1** 使用具有管理员或超级管理员权限的帐户登录 CDO。

**步骤 2** 从菜单栏中，导航至 **设置 (Settings)** > **常规设置 (General Settings)**。

**步骤 3** 在全局搜索中，点击启动完整索引以触发索引。



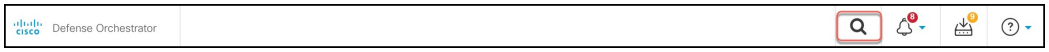

注释 启动完整索引会清除 CDO 租户的现有索引。

**步骤 4** 点击此处查看全局搜索工作流程。

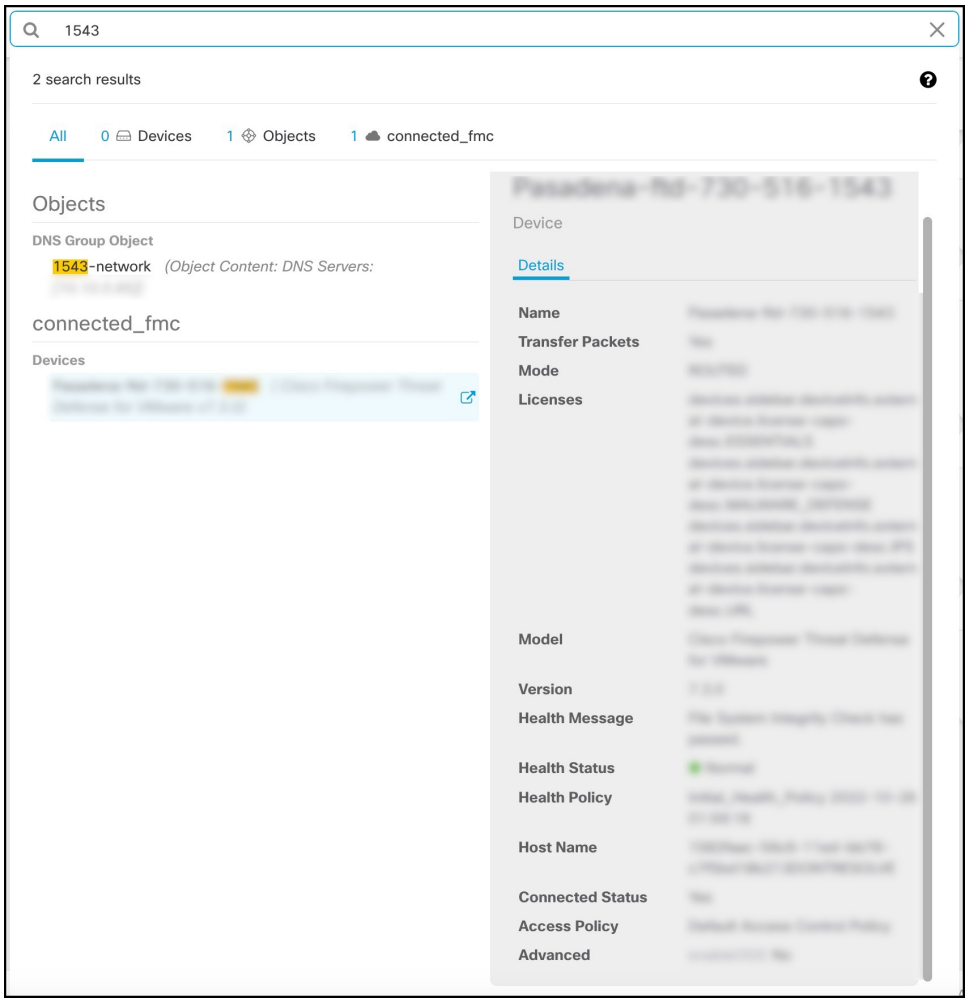
## 执行全局搜索

**步骤 1** 登录至 CDO。

**步骤 2** 点击CDO页面右上角的搜索图标，然后在显示的搜索字段中输入搜索字符串。




当您开始输入搜索字符串时，搜索结果会显示可能的项目列表。搜索结果显示在四个类别下：All、Devices、Objects 和 connected_fmc。右侧窗格显示所选搜索结果的信息。




**步骤 3** 从搜索结果中选择设备或对象，然后点击箭头图标从搜索结果导航到相应的设备和对象页面。从搜索结果中选择一个项目，然后点击箭头图标从搜索结果导航到相应的页面。

**注释** 在云交付的防火墙管理中心中选择设备的搜索结果，可以导航到CDO中的云交付的防火墙管理中心用户界面。

有关 云交付的防火墙管理中心 的信息，请参阅使用 Cisco 防御协调器中的云交付防火墙管理中心管理防火墙威胁防御。

**步骤 4** 点击 **X** 关闭搜索栏。

# CDO 命令行界面

CDO 为用户提供命令行界面 (CLI)，用于管理 ASA 设备。用户可以将命令发送到单个设备或同时发送到多个设备。

相关信息：

- 有关详细的 ASA CLI 文档，请参阅ASA 命令行接口文档, on page 95。

# 使用命令行接口

**步骤 1** 打开**清单 (Inventory)** 页面。

**步骤 2** 点击“清单”(Inventory) 表上方的**设备 (Devices)** 按钮。

**步骤 3** 使用设备选项卡和过滤器按钮查找要使用命令行界面 (CLI) 管理的设备。

**步骤 4** 选择设备。

**步骤 5** 在**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 6** 点击 **命令行接口 (Command Line Interface)**。

**步骤 7** 在命令窗格中输入一个或多个命令，然后点击发送。 设备对命令的响应显示在下面的“响应窗格”中。

**Note** 如果可以运行的命令有限制，则会在命令窗格上方列出这些限制。

**Related Topics**

在命令行接口中输入命令 ，第 84 页

# 在命令行接口中输入命令

可以在一行中输入单个命令，也可以在多行中依次输入多个命令，CDO将按顺序执行这些命令。以下示例发送创建三个网络对象和包含这些网络对象的网络对象组的一批命令。ASA


输入设备命令：CDO 在 的全局配置模式下执行命令。ASAASA

长命令：如果您输入一个很长的命令，CDO 会尝试将您的命令拆分为多个命令，以便可以针对 API 运行所有这些命令。如果CDO无法确定命令的正确分隔，它会提示您提示中断命令列表的位置。例如：

错误：CDO 尝试执行此命令中长度超过 600 个字符的部分。您可以通过在命令列表之间添加一个空行来向 CDO 提示适当的命令分隔点。

如果收到此错误：

**步骤 1** 点击 CLI 历史记录窗格中导致错误的命令。CDO 使用一长串命令填充命令框。

**步骤 2** 通过在相关命令组后面输入空行来编辑长命令列表。例如，在定义网络对象列表并将其添加到上述示例中的组后，添加一个空行。您可能希望在命令列表中的几个不同位置执行此操作。

**步骤 3** 点击**发送 (Send)**。

# 使用命令历史记录

发送 CLI 命令后，CDO 会在“命令行界面”(Command Line Interface) 页面的历史记录窗格中记录该命令。您可以重新运行历史记录窗格中保存的命令，或将这些命令用作模板：

**步骤 1** 在**清单 (Inventory)** 页面上，选择要配置的设备。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 点击 **>_命令行接口 (>_Command Line Interface)**。

**步骤 5** 点击时钟图标可展开历史记录窗格（如果尚未展开）。

**步骤 6** 在历史记录窗格中选择要修改或重新发送的命令。

**步骤 7** 按原样重新使用命令，或在命令窗格中对其进行编辑，然后点击发送。CDO 在响应窗格中显示命令的结果。

**Note** CDO 显示 Done!两种情况下响应窗格中的消息：

- 成功执行命令后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

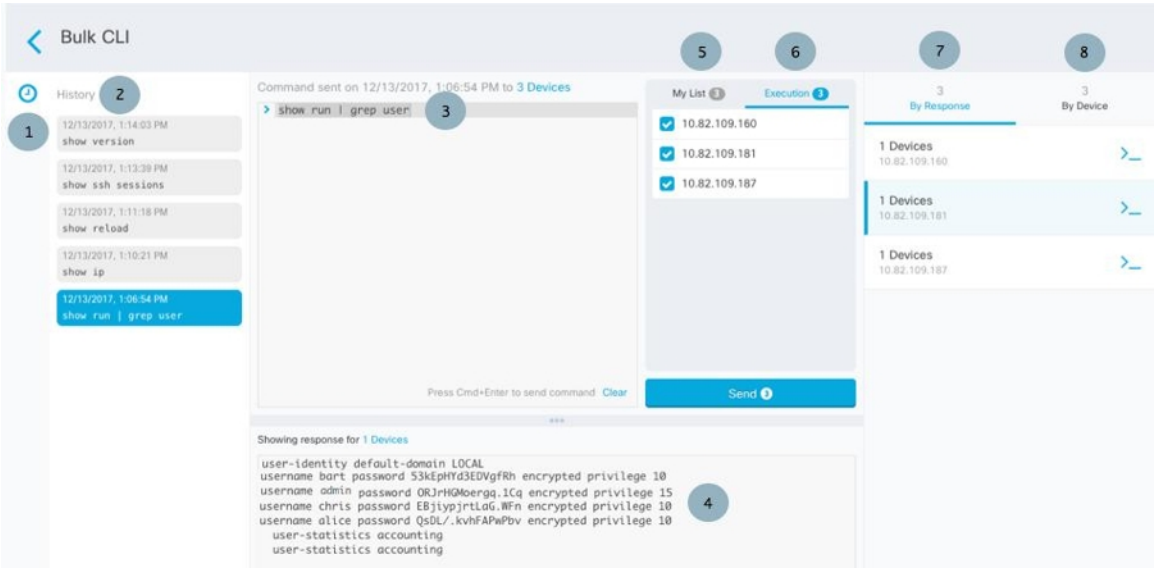
# 批量命令行接口

CDO 为用户提供使用命令行接口 (CLI) 管理 Secure Firewall ASA、FDM 管理 威胁防御、SSH 和 Cisco IOS 设备。用户可以将命令发送到单个设备或同时发送到多个同类设备。本节介绍一次向多台设备发送 CLI 命令。

**相关信息：**

- 有关详细的 ASA CLI 文档，请参阅ASA 命令行接口文档, on page 95。

# 批量 CLI 接口




**Note** CDO 显示 Done!两种情况下的消息：

- 成功执行命令且无错误后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

| 编号 | 说明 |
|---|---|
| 1 | 点击时钟可展开或折叠命令历史记录窗格。 |
| 2 | 命令历史记录。发送命令后，CDO 会在此历史记录窗格中记录该命令，以便您可以返回到该窗格，选择并再次运行该命令。 |
| 3 | 命令窗格。在此窗格的提示符后输入命令。 |
| 4 | 响应窗格。CDO 显示设备对命令的响应以及 CDO 消息。如果多个设备的响应相同，则响应窗格会显示消息“显示 X 台设备的响应”(Showing Responses for X devices)。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。<br>**Note** CDO 显示 Done!两种情况下的消息：<br>• 成功执行命令且无错误后。<br>• 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。 |

| 编号 | 说明 |
|---|---|
| 5 | **我的列表 (My List)** 选项卡显示您从**清单 (Inventory)** 表中选择的设备，并允许您包含或排除要向其发送命令的设备。 |
| 6 | 上图中突出显示的“执行”选项卡显示在历史记录窗格中选择的命令中的设备。在本例中，show run \|在历史记录窗格中选择了 grep 用户命令，执行选项卡显示它已发送到 10.82.109.160、10.82.109.181 和 10.82.10.9.187。 |
| 7 | 点击“By Response”（按响应）选项卡将显示命令生成的响应列表。相同的响应组合在一行中。当您在“按响应”选项卡中选择一行时，CDO 会在响应窗格中显示对该命令的响应。 |
| 8 | 点击“按设备”选项卡会显示每个设备的单独响应。点击列表中的其中一个设备，即可查看特定设备对命令的响应。 |

# 批量发送命令

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 选择相应的设备选项卡，然后使用过滤器按钮查找要使用命令行界面配置的设备。

**步骤 4** 选择设备。

**步骤 5** 在**设备操作 (Device Actions)** 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

**步骤 6** 您可以在“我的列表”字段中选中或取消选中要向其发送命令的设备。

**步骤 7** 在命令窗格中输入命令，然后点击发送。命令输出显示在响应窗格中，命令记录在更改日志中，命令CDO在批量 CLI 窗口的历史记录窗格中记录您的命令。

**Note** 命令将在已同步的选定ASA设备上成功执行，但在未同步的设备上可能会失败。如果任何选定的ASA设备未同步，则仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto、dir、write 和 copy。

# 使用批量命令历史记录

发送批量 CLI 命令后，CDO 会在“批量 CLI”页面历史记录页面中记录该命令。批量 CLI 接口, on page 86您可以重新运行历史记录窗格中保存的命令，也可以将这些命令用作模板。历史记录窗格中的命令与运行这些命令的原始设备相关联。

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以找到设备。

**步骤 3** 点击相应的设备类型选项卡，然后点击过滤器图标以查找要配置的设备。

**步骤 4** 选择设备。

**步骤 5** 点击 **命令行接口 (Command Line Interface)**。

**步骤 6** 在“历史记录”窗格中选择要修改或重新发送的命令。请注意，您选择的命令与特定设备相关联，而不一定是您在第一步中选择的设备。

**步骤 7** 查看我的列表选项卡，确保您要发送的命令将发送到您期望的设备。

**步骤 8** 在命令窗格中编辑命令，然后点击**发送 (Send)**。CDO 在响应窗格中显示命令的结果。

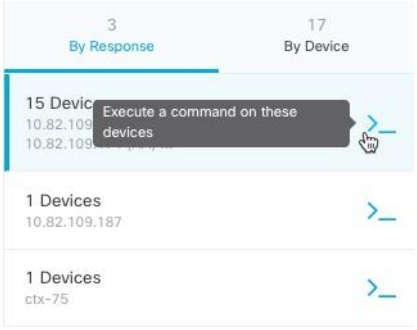
**Note** 命令将在已同步的选定 ASA 设备上成功执行，但在未同步的设备上可能会失败。如果任何选定的 ASA 设备未同步，则仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto、dir、write 和 copy。

# 使用批量命令过滤器

运行批量 CLI 命令后，您可以使用“按响应”过滤器和“按设备”过滤器继续配置设备。

## 按响应过滤器

运行批量命令后，CDO 会使用发送该命令的设备返回的响应列表填充“按响应”选项卡。具有相同响应的设备会合并到一行中。点击“按响应”(By Response) 选项卡中的行会在响应窗格中显示设备的响应。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。




要将命令发送到与命令响应关联的设备列表，请执行以下程序：

**步骤 1** 点击 By Response 选项卡中一行中的命令符号。

**步骤 2** 查看命令窗格中的命令，然后点击发送以重新发送命令，或点击清除以清除命令窗格并输入要发送到设备的新命令，然后点击发送。

**步骤 3** 查看从命令收到的响应。

**步骤 4** 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 write memory，然后点击 Send。这样会将运行配置保存至启动配置。

## 按设备过滤器

运行批量命令后，CDO 会使用已发送命令的设备列表填充“执行”选项卡和“按设备”选项卡。点击“按设备”(By Device) 选项卡中的行会显示每个设备的响应。

要在同一设备列表上运行命令，请执行以下程序：

**步骤 1** 点击**按设备 (By Device)** 选项卡。

**步骤 2** 点击 **>_在这些设备上执行命令**。

**步骤 3** 点击**清除 (Clear)** 以清除命令窗格并输入新命令。

**步骤 4** 在我的列表窗格中，通过选中或取消选中列表中的单个设备来指定要向其发送命令的设备列表。

**步骤 5** 点击**发送 (Send)**。命令的响应会显示在响应窗格中。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。

**步骤 6** 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入`write memory`，然后点击**发送 (Send)**。

# 命令行界面宏

CLI 宏是可以使用的完整形式的 CLI 命令，或者是可以在运行之前修改的 CLI 命令的模板。所有宏都可以在一个或多个 ASA 设备上同时运行。

使用类似模板的 CLI 宏可同时在多台设备上运行相同的命令。CLI 宏可促进设备配置和管理的一致性。使用完全格式的 CLI 宏获取有关设备的信息。您可以立即在 ASA 设备上使用不同的 CLI 宏。

您可以创建 CLI 宏来监控您经常执行的任务。有关详细信息，请参阅从新命令创建 CLI 宏。

CLI 宏是系统定义的或用户定义的。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。

**Note** 只有在设备载入 CDO 后，才能为设备创建宏。

以 ASA 为例，如果要查找其中一个 ASA 上的特定用户，可以运行以下命令：

```
show running-config | grep username
```

运行命令时，您要将 *username* 替换为要搜索的用户的用户名。要使用此命令来创建宏，请使用相同的命令并在用户名周围加上大括号。

```
> show running-config | grep {{username}}
```

您可以随意命名参数。您还可以使用此参数名称创建相同的宏：

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

参数名称可以是描述性的，并且必须使用字母数字字符和下划线。命令语法，在本例中为

```
show running-config | grep
```

命令的一部分，必须对要向其发送命令的设备使用正确的 CLI 语法。

# 从新命令创建 CLI 宏

**步骤 1** 在创建 CLI 宏之前，请在 CDO 的命令行界面中测试命令，以便确保命令语法正确并返回可靠的结果。

**Note**
- 有关详细的 ASA CLI 文档，请参阅ASA 命令行接口文档, on page 95。

**步骤 2** 在导航栏中，点击**清单 (Inventory)**。

**步骤 3** 点击 **设备 (Devices)**选项卡以找到设备。

**步骤 4** 点击相应的设备类型选项卡，然后选择在线和同步的设备。

**步骤 5** 点击 **>_Command Line Interface**。

**步骤 6** 点击 CLI 宏收藏夹星标 ★，以查看已经存在的宏。

**步骤 7** 点击加号按钮  。

**步骤 8** 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

**步骤 9** 在**命令 (Command)** 字段中输入完整命令。

**步骤 10** 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

**步骤 11** 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 CLI 宏。

# 从 CLI 历史记录或现有 CLI 宏创建 CLI 宏

在此程序中，您将从已运行的命令、另一个用户定义的宏或从系统定义的宏创建用户定义的宏。

**步骤 1** 在导航栏中，点击 **设备和服务**。

**注释** 如果要从CLI历史记录创建用户定义的宏，请选择运行命令的设备。CLI宏在同一账户上的设备之间共享，但不是 CLI 历史记录。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择在线和同步的设备。

**步骤 4** 点击 **>_命令行接口**。

**步骤 5** 查找要生成 CLI 宏的命令，然后选择该命令。使用以下方法之一：

- 点击时钟 可查看您在该设备上运行的命令。选择要转换为宏的命令，命令将显示在命令窗格中。
- 点击 CLI 宏收藏夹星标 ，以查看已经存在的宏。选择要更改的用户定义或系统定义的 CLI 宏。命令显示在命令窗格中。

**步骤 6** 使用 命令窗格中的 命令，点击 CLI 宏金色星标 。命令现在是新 CLI 宏的基础。

**步骤 7** 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

**步骤 8** 查看命令字段中的命令，并进行所需的更改。

**步骤 9** 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

**步骤 10** 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 CLI 宏。

# 运行 CLI 宏

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择一个或多个设备。

**步骤 4** 点击 **>_命令行接口**。

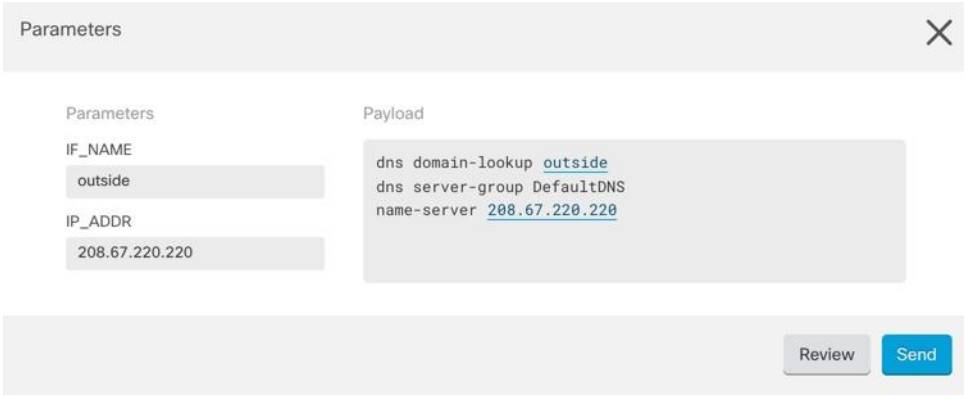
**步骤 5** 在命令面板中，点击星号 。

**步骤 6** 从命令面板中选择 CLI 宏。

**步骤 7** 使用以下两种方式之一运行宏：

- 如果宏没有要定义的参数，请点击**发送 (Send)**。命令的响应显示在响应窗格中。就行了。
- 如果宏包含参数，例如下面的配置 DNS 宏，请点击 **>_ 查看参数**。


**步骤 8** 在“参数”(Parameters) 窗格中，在“参数”(Parameters) 字段中填写参数的值。




**步骤 9** 点击 **Send**。在 CDO 成功发送命令并更新设备配置后，您会收到消息完成！

- 对于 ASA，将更新当前配置文件：

**步骤 10** 发送命令后，您可能会看到消息“某些命令可能已对运行配置进行了更改”(Some commands may have made changes to the running config) 以及两个链接。


- 点击**写入磁盘 (Write to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到设备的启动配置中。
- 点击**消除 (Dismiss)**，可关闭消息。

# 编辑 CLI 宏

您可以编辑用户定义的 CLI 宏，但不能编辑系统定义的宏。编辑 CLI 宏会更改所有 ASA 设备。宏并非特定于特定设备。

**步骤 1** 在导航栏中，点击 **设备和服务**。
**步骤 2** 点击**设备**选项卡。
**步骤 3** 点击适当的设备类型选项卡。
**步骤 4** 请选择您的设备。
**步骤 5** 点击 **命令行接口 (Command Line Interface)**。
**步骤 6** 选择要编辑的用户定义的宏。
**步骤 7** 点击宏标签中的编辑图标。
**步骤 8** 在编辑宏对话框中编辑 CLI 宏。
**步骤 9** 点击**保存 (Save)**。

有关如何运行 CLI 宏的说明，请参阅运行 CLI 宏。

# 删除 CLI 宏

您可以删除用户定义的 CLI 宏，但不能删除系统定义的宏。删除 CLI 宏会删除所有设备的宏。宏并非特定于特定设备。

**步骤 1** 在导航栏中，点击 **设备和服务**。
**步骤 2** 点击**设备**选项卡。
**步骤 3** 点击适当的设备类型选项卡。
**步骤 4** 请选择您的设备。
**步骤 5** 点击 >_**命令行接口 (Command Line Interface)**。
**步骤 6** 选择要删除的用户定义的 CLI 宏。
**步骤 7** 点击 CLI 宏标签中的垃圾桶图标 。
**步骤 8** 确认要删除 CLI 宏。

# 使用 CDO CLI 配置 ASA

您可以通过在 CDO 中提供的 CLI 界面中运行 CLI 命令来配置 ASA 设备。要使用该接口，请在**清单 (Inventory)** 菜单上选择设备，然后点击**命令行界面 (Command Line Interface)**。有关更多信息，请参阅使用 CDO 命令行接口。

### 添加新的日志记录服务器

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。

有关详细信息，请参阅您正在运行的 ASA 版本的《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中“日志记录”一章的“监控”部分。

### 配置 DNS 服务器

需要配置 DNS 服务器，以便 ASA 能够将主机名解析为 IP 地址。还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

有关详细信息，请参阅所运行 ASA 版本的《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中“配置 DNS 服务器”部分的“基本设置”一章。

### 添加静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。

有关详细信息，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中的“静态和默认路由”一章。

### 配置接口

您可以使用 CLI 命令配置管理和数据接口。有关详细信息，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》的“基本接口配置”一章。

# 使用 CDO 来比较 ASA 配置

使用此程序可比较两个 ASA 的配置。

**步骤 1** 在导航菜单中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备 (Devices)** 选项卡以查找 ASA 设备，或点击**模板 (Templates)** 选项卡以查找 ASA 型号设备。

**步骤 3** 点击 **ASA** 选项卡。

**步骤 4** 过滤要比较的设备的设备列表。

**步骤 5** 选择两个 ASA。它们的状态无关紧要。您正在比较 Defense Orchestrator 上存储的 ASA 配置。

**步骤 6** 在右侧的“设备操作”(Device Actions) 窗格中，点击 **比较 (Compare)**。

**步骤 7** 在比较配置对话框中，点击**下一步**和**上一步**可跳过配置文件中以蓝色突出显示的差异。

# ASA 批量 CLI 使用案例

以下情况是您对 ASA 设备使用 CDO 的批量 CLI 功能时可能遇到的工作流程。

## 显示 ASA 的运行配置中的所有用户，然后删除其中一个用户

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击 **ASA** 选项卡。

**步骤 4** 搜索并过滤要从中删除用户的设备的设备列表，然后选择这些设备。

**Note** 确保您选择的设备已同步。设备未同步时，仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto、dir、copy 和 write。

**步骤 5** 在详细信息窗格中点击 **>_命令行接口 (>_Command Line Interface)**。CDO 列出您在我的列表窗格中选择的设备。如果您决定将命令发送到更少的设备，请取消选中该列表中的设备。

**步骤 6** 在命令窗格中，输入 show run | grep user，然后点击 Send。 运行配置文件中包含字符串 user 的所有行都将显示在响应窗格中。系统将打开“执行”选项卡，显示执行命令的设备。

**步骤 7** 点击按响应选项卡并查看响应，以确定哪些设备具有要删除的用户。

**步骤 8** 点击我的列表选项卡，然后选择要从中删除用户的设备列表。

**步骤 9** 在命令窗格中，输入 no 形式的 user 命令以删除 user2，然后点击 Send。在本示例中，您将删除 user2：
no user user2 password reallyhardpassword privilege 10

**步骤 10** 在历史记录面板中查找 show run | 的实例。用于搜索用户名的 grep user 命令。选择该命令，查看“执行”列表中的设备列表，然后选择“发送”。您应该会看到用户名已从您指定的设备中删除。

**步骤 11** 如果您确信已从运行配置中删除了正确的用户，并且正确的用户仍保留在运行配置中：

**a.** 从历史记录窗格中选择 no user user2 password reallyhardpassword privilege 10 命令。

**b.** 点击 By Device 选项卡，然后点击 Execute a command on these devices。

**c.** 在命令窗格中，点击清除以清除命令窗格。

**d.** 输入命令 deploy memory，然后点击 Send。

# 查找所选 ASA 上的所有 SNMP 配置

此程序显示 ASA 运行配置中的所有 SNMP 配置条目。

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击 **ASA** 选项卡。

**步骤 4** 过滤并搜索要在其上分析运行配置中的 SNMP 配置的设备，然后选择这些设备。

**Note** 确保您选择的设备已同步。设备未同步时，仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto 和 dir。

**步骤 5** 在详细信息窗格中点击 **命令行接口 (Command Line Interface)**。您选择的设备位于我的列表窗格中。如果您决定将命令发送到更少的设备，请取消选中列表中的设备。

**步骤 6** 在命令窗格中，输入 show run | grep snmp，然后点击 Send。 运行配置文件中包含字符串 snmp 的所有行都将显示在响应窗格中。系统将打开“执行”选项卡，显示执行命令的设备。

**步骤 7** 查看响应窗格中的命令输出。

# ASA 命令行接口文档

CDO 完全支持 ASA 命令行界面。我们在 CDO 中提供类似终端的接口，供用户同时向单个设备和多个设备发送 ASA 命令。ASA 命令行接口文档涵盖的范围非常广泛。这里不是在 CDO 文档中重新创建部分内容，而是指向 Cisco.com 上的 ASA CLI 文档。

### ASA 命令行界面配置指南

从 ASA 9.1 版开始，《ASA CLI 配置指南》分为三本单独的指南：

- 《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》
- 《CLI 手册 2：思科 ASA 系列防火墙 CLI 配置指南》
- 《CLI 手册 3：思科 ASA 系列 VPN CLI 配置指南》

您可以通过以下方式访问 Cisco.com 上的 ASA CLI 配置指南：支持 (Support) > 按类别划分的产品 (Products by Category) > 安全 (Security) > 防火墙 (Firewalls) > ASA 5500 > 配置 (Configure) > 配置指南 (Configuration Guides)。

### ASA 命令行界面配置指南的几个特定部分

**过滤 show 和 more 命令输出**。您可以在《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》的过滤 show 和 more 命令输出下了解如何使用正则表达式过滤 show 命令输出。

### ASA 命令参考

《ASA 命令参考指南》按字母顺序列出了所有 ASA 命令及其选项。ASA 命令参考不是特定于版本的。它出版了四本书：

- 思科 ASA 系列命令参考，A - H 命令
- 思科 ASA 系列命令参考，I - R 命令
- 思科 ASA 系列命令参考，S 命令
- 思科 ASA 系列命令参考，适用于 ASASM 的 T - Z 命令和思科 IOS 命令

您可以通过以下方式访问 Cisco.com 上的《ASA 命令参考指南》：支持 (Support) > 按类别划分的产品 (Products by Category) > 安全 (Security) > 防火墙 (Firewalls) > ASA 5500 > 参考指南 (Reference Guides) > 命令参考 (Command References) > ASA 命令参考 (ASA Command References)。

# 导出 CDO CLI 命令结果

您可以将向独立设备或多个设备发出的CLI命令结果导出为逗号分隔值（.csv）文件，以便您可以随意过滤和排序其中的信息。您可以导出单个设备或多个设备的CLI结果。导出的信息包含以下内容：

- 设备
- 日期
- 用户
- 命令
- 输出

# 导出 CLI 命令结果

您可以将刚刚在命令窗口中执行的命令的结果导出到 .csv 文件：

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备，使其突出显示。

**步骤 5** 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 6** 在命令行界面窗格中，输入命令并点击**发送 (Send)** 以向设备发出命令。

**步骤 7** 在已输入命令的窗口右侧，点击导出图标。

**步骤 8** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

# 导出 CLI 宏的结果

您可以导出已在命令窗口中执行的宏的结果。使用以下程序可将在一台或多台设备上执行的 CLI 宏的结果导出到 .csv 文件：

**步骤 1** 打开 **设备和服务** 页面。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备，使其突出显示。

**步骤 5** 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 6** 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。

**步骤 7** 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

**步骤 8** 在已输入命令的窗口右侧，点击导出图标 。

**步骤 9** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

# 导出 CLI 命令历史记录

使用以下程序将一个或多个设备的 CLI 历史记录导出到 .csv 文件：

**步骤 1** 在导航窗格中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备，使其突出显示。

**步骤 5** 在设备的“设备操作”(Device Actions) 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 6** 如果历史记录窗格尚未展开，请点击时钟图标将其展开。

**步骤 7** 在已输入命令的窗口右侧，点击导出图标。

**步骤 8** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

**相关信息：**

- CDO 命令行界面, on page 83
- 从新命令创建 CLI 宏
- 删除 CLI 宏
- 编辑 CLI 宏
- 运行 CLI 宏
- ASA 批量 CLI 使用案例
- ASA 命令行接口文档
- 批量命令行接口

# 导出 CLI 宏列表

您只能导出已在命令窗口中执行的宏。使用以下程序将一个或多个设备的 CLI 宏导出到 .csv 文件：

**步骤 1** 在导航窗格中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备，使其突出显示。

**步骤 5** 在设备的“设备操作”(Device Actions) 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

**步骤 6** 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。

**步骤 7** 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

**步骤 8** 在已输入命令的窗口右侧，点击导出图标。

**步骤 9** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。

# 恢复 ASA 配置

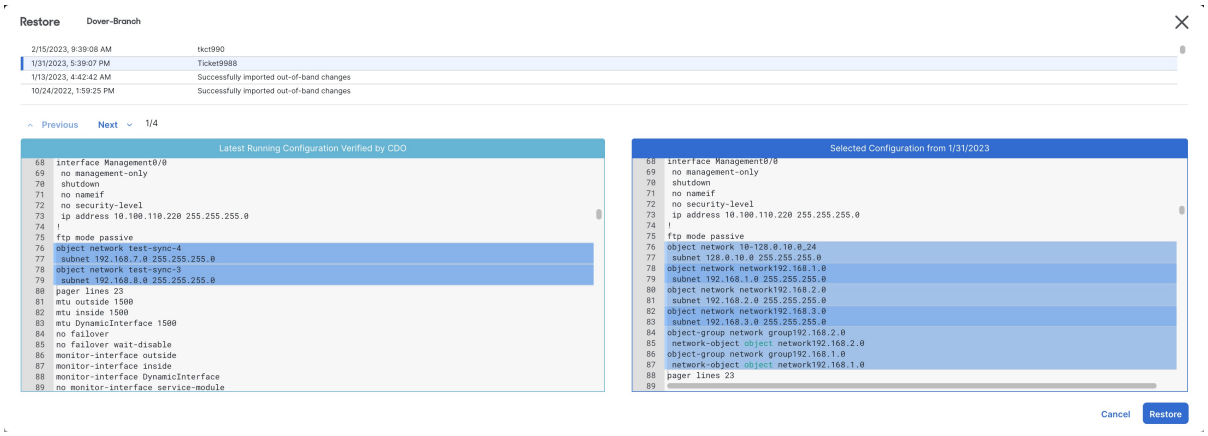
如果对的配置进行了更改，并且想要恢复该更改，则可以恢复过去的配置。ASAASA这是一种删除具有意外或意外结果的配置更改的便捷方法。

## 关于恢复 ASA 配置

在恢复配置之前，请查看以下说明：

- 会将您选择要恢复的配置与部署到 的最后一个已知配置进行比较，但不会将您选择要恢复的配置与已暂存但未部署到的配置进行比较。CDOASAASA如果您的上有任何未部署的更改，并且您恢复了过去的配置，则恢复过程将覆盖未部署的更改，您将丢失这些更改。ASA
- 在恢复过去的配置之前， 可以处于“已同步”或“未同步”状态，但如果设备处于“检测到冲突”状态，则必须先解决冲突，然后才能恢复过去的配置。ASA
- 恢复过去的配置会覆盖所有中间部署的配置更改。例如，从以下列表中的 1/31/2023 恢复配置会覆盖在 2/15/2023 所做的配置更改。
- 点击“Next”（下一步）和“Previous”（上一步）按钮将在配置文件中移动并突出显示配置文件更改
- 如果您最初对配置更改应用了更改请求标签，则该标签会显示在“恢复配置”列表中。

***Figure 3: ASA*** 恢复配置屏幕




## 配置更改保留多长时间？

您可以恢复使用时间不超过 1 年的配置。恢复在其更改日志中记录的配置更改。ASACDO每次向 写入或读取配置更改时，更改日志都会记录更改。存储 1 年的变更日志，并且对上一年内进行的备份数量没有限制。ASACDO

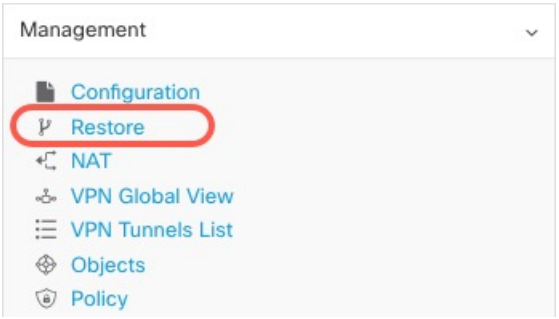
# 恢复 Secure Firewall ASA 配置

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

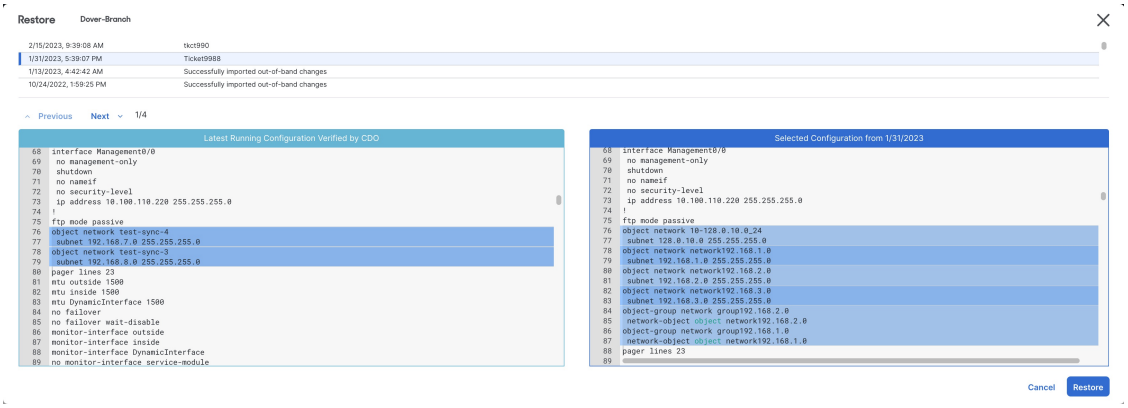
**步骤 2** 点击ASA选项卡。

**步骤 3** 选择您要恢复其配置的 ASA。

**步骤 4** 在**管理 (Management)** 窗格中，点击**恢复 (Restore)**。




**步骤 5** 在“恢复”(Restore) 页面中，选择要恢复的配置。




例如，在上图中，选择了 1/31/2023 的配置。

**步骤 6** 比较“由 CDO 验证的最新运行配置”和“自 < 日期 > 起的选定配置”，以确保您要恢复“自 < 日期 > 起的选定配置 > 窗口中显示的配置。使用“上一个”和“下一个”比较所有更改。

**步骤 7** 点击恢复，这将在 CDO 中暂存配置。在**清单 (Inventory)** 页面上，您会看到设备的配置状态现在为“未同步”(Not Synced)。

**步骤 8** 点击右侧窗格中的**部署更改...(Deploy Changes...)** 以部署更改并同步 ASA。

# 故障排除

如何恢复丢失但想要保留的更改？

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击 ASA 选项卡。

**步骤 4** 选择所需的设备。

**步骤 5** 点击右侧窗格中的更改日志。

**步骤 6** 查看更改日志中的更改。您可以根据这些记录重建丢失的配置。

# 管理 ASA 和 Cisco IOS 设备配置文件

某些类型的设备将其配置存储在单个文件中，例如 ASA 和 Cisco IOS 设备。对于这些设备，您可以在 Cisco Defense Orchestrator 上查看配置文件并在上面执行各种操作。

## 查看设备的配置文件

对于将整个配置存储在单个配置文件中的设备（例如 ASA、SSH 托管设备和运行Cisco IOS 的设备），您可以使用 CDO 查看配置文件。

注释 SSH 管理的设备和思科 IOS 设备具有只读配置。

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要查看其配置的设备或型号。

**步骤 5** 在右侧的 **管理 (Management)** 窗格中，点击**配置 (Configuration)**。
系统将显示完整的配置文件。

相关信息：

- 编辑完整的设备配置文件

## 编辑完整的设备配置文件

某些类型的设备将其配置存储在单个配置文件中，例如 ASA 。对于这些设备，您可以在 CDO 上查看设备配置文件，并根据设备对其执行各种操作。

目前，只能使用 CDO 直接编辑 ASA 配置文件。

**Caution** 此程序适用于熟悉设备配置文件语法的高级用户。此方法直接对 Defense Orchestrator 上存储的配置文件副本进行更改。

## 操作步骤

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击 **ASA** 选项卡。

**步骤 4** 选择要编辑其配置的设备。

**步骤 5** 在右侧的 **管理 (Management)** 窗格中，点击**配置 (Configuration)**。

**步骤 6** 在设备配置页面中，点击编辑。

**步骤 7** 点击右侧的编辑器按钮，然后选择**默认**文本编辑器、**Vim** 或 **Emacs** 文本编辑器。

**步骤 8** 编辑文件并保存更改。

**步骤 9** 返回到设备和服务页面，预览并部署更改。

# 对象

对象是可在一个或多个安全策略中使用的信息容器。使用对象可以轻松维护策略一致性。您可以创建单个对象，使用不同的策略，修改对象，然后将该更改传播到使用该对象的每个策略。如果没有对象，则需要单独修改需要进行相同更改的所有策略。

当您载入设备时， 会识别该设备使用的所有对象，保存它们，并在“对象”(Objects) 页面上列出它们。CDO在“对象”(Objects) 页面中，可以编辑现有对象并创建要在安全策略中使用的新对象。

CDO 将多台设备上使用的对象称为**共享对象**，并在**对象 (Objects)** 页面中使用此标记 进行标识。

有时，共享对象会产生一些“问题”，并且不再在多个策略或设备之间完美共享：

- **重复对象**是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常可用于类似的目的，并供不同的策略使用。重复的对象由此问题图标标识：
- **不一致对象**是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。不一致的对象由此问题图标标识：
- **未使用的对象**是设备配置中存在但未被其他对象、访问列表或NAT规则引用的对象。未使用的对象由此问题图标标识：

您还可以创建在规则或策略中立即使用的对象。您可以创建不与任何规则或策略关联的对象。

您可以通过导航至**对象**菜单或在网络策略的详细信息中查看对象来查看CDO管理的对象。

CDO 允许您从一个位置跨受支持的设备管理网络和服务对象。使用 ，您可以通过以下方式管理对象：CDO

- 根据各种条件搜索和对象过滤器。
- 查找设备上的重复、未使用和不一致的对象，并合并、删除或解决这些对象问题。
- 查找未关联的对象，如果未使用，请将其删除。
- 发现跨设备通用的共享对象。
- 在提交更改之前，评估对象更改对一组策略和设备的影响。
- 比较一组对象及其与不同策略和设备的关系。
- 捕获设备在载入后使用的对象。CDO

如果您在创建、编辑或读取已载入设备的对象时遇到问题，请参阅对思科防御协调器进行故障排除, on page 507以了解详细信息。

# 对象类型

下表介绍您可以为设备创建和使用 CDO 管理的对象。

***Table 3:*** 自适应安全设备 ***(ASA)*** 对象类型

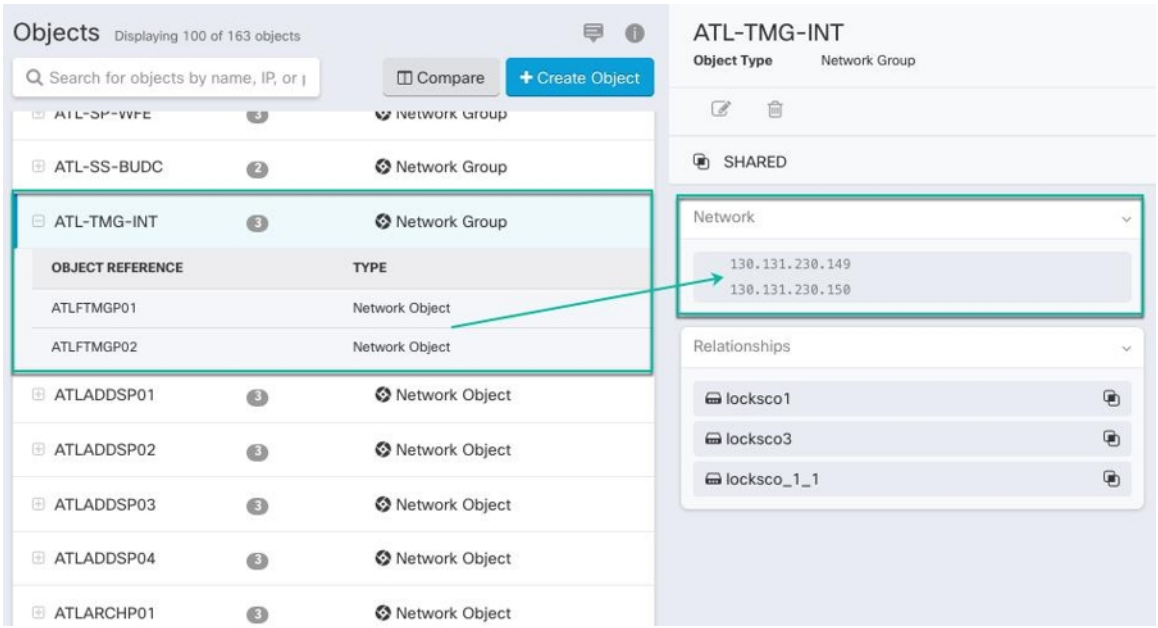
| 对象 | 说明 |
|---|---|
| 创建 IP 地址池 | 可以将地址池对象配置为根据单个 IPv4 或 IPv6 地址或 IP 地址范围进行匹配。 |
| 上传 RA AnyConnect 客户端配置文件 | AnyConnect客户端文件对象是文件对象，表示配置中使用的文件，通常适用于远程访问 VPN 策略。可以包含 AnyConnect 客户端配置文件和 AnyConnect 客户端映像文件。 |
| 网络对象 | 网络组和网络对象（统称为“网络对象”）定义主机或网络的地址。 |
| 服务对象 | 服务对象、服务组和端口组是包含被视为 TCP/IP 协议簇一部分的协议或端口的可重用组件。 |
| ASA 时间范围对象 | 时间范围对象定义了由起始时间、结束时间和可选循环条目组成的特定时间。可以将这些网络中的对象用于对特定功能或资产提供基于时间的访问。 |
| 信任点对象 | 通过信任点，您可以管理并跟踪 ASA 中的数字证书。 |

# 共享对象

Cisco Defense Orchestrator (CDO) 会调用多个设备上具有相同名称和相同内容的对象，即**共享对象**。共享对象由此图标标识

在**对象 (Objects)** 页面上。使用共享对象可以轻松维护策略，因为您可以在一个位置修改对象，并且该更改会影响使用该对象的所有其他策略。如果没有共享对象，则需要单独修改需要进行相同更改的所有策略。

查看共享对象时，CDO 会在对象表中显示该对象的内容。共享对象具有完全相同的内容。CDO 在详细信息窗格中显示对象元素的组合视图或“平面化”视图。请注意，在详细信息窗格中，网络元素被展平为一个简单的列表，而不是直接与命名对象关联。



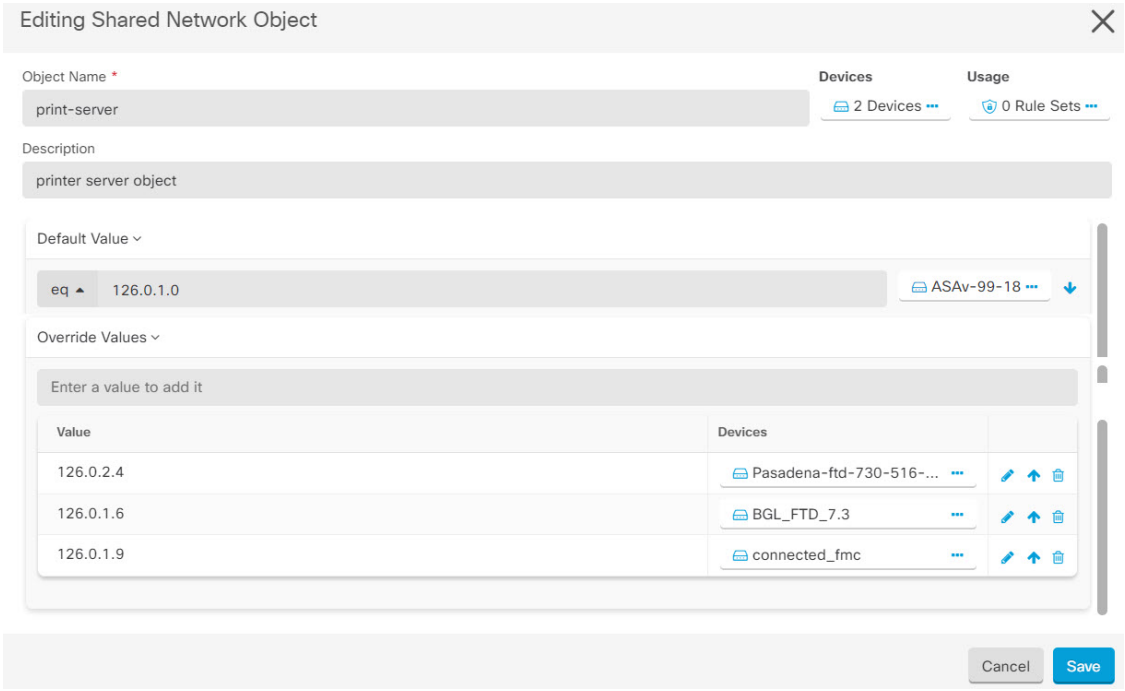

# 对象覆盖

对象覆盖允许您覆盖特定设备上共享网络对象的值。CDO 会使用您在配置覆盖时指定的设备的相应值。虽然对象位于两个或多个名称相同但值不同的设备上，但 CDO 不会将其识别为**不一致对象**，因为这些值是作为覆盖值添加的。

您可以创建其定义适用于大多数设备的对象，然后使用覆盖为需要不同定义的几个设备指定对象的修改。您还可以创建需要为所有设备覆盖的对象，但其使用使您能够为所有设备创建单个策略。对象覆盖允许您创建较小的一组在设备间使用的共享策略，而不会失去在各个设备需要时修改策略的能力。

例如，假设您的每个办公室都有一台打印机服务器，并且您创建了一个打印机服务器对象 `print-server`。您的 ACL 中有一条规则，用于拒绝打印机服务器访问互联网。打印机服务器对象有

一个您想在办公室之间更改的默认值。您可以使用对象覆盖来实现此目的，并在所有位置保持规则和“printer-server”对象的一致性，但它们的值可能不同。



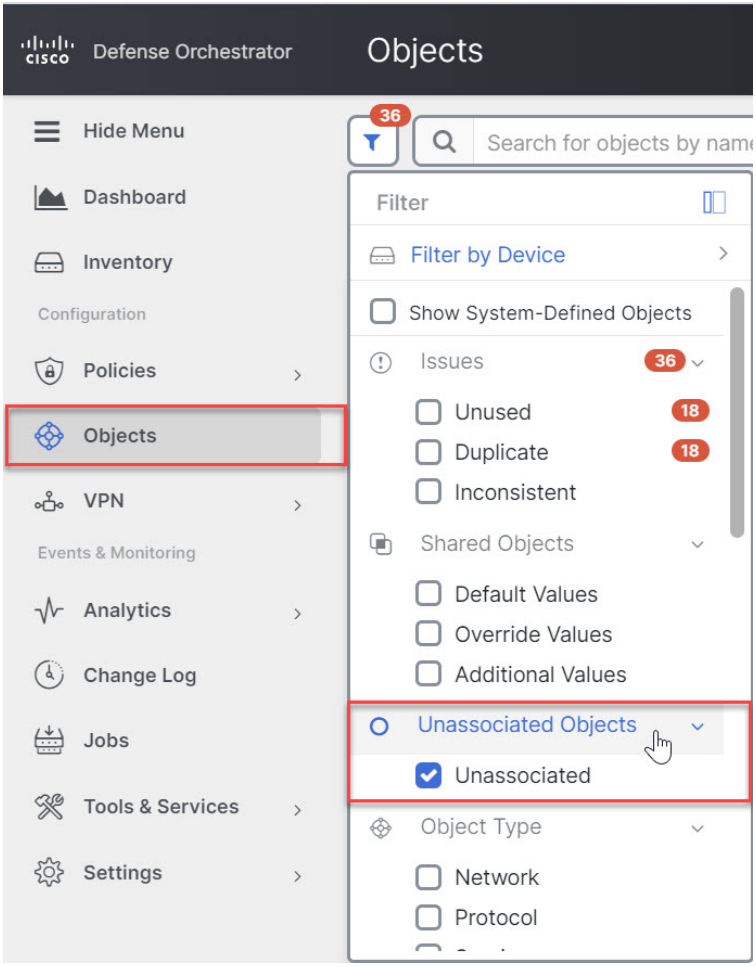

**Note** 如果存在不一致的对象，您可以将它们合并为一个具有覆盖的共享对象。有关详细信息，请参阅解决不一致的对象问题, on page 513。

# 未关联的对象

您可以创建对象以立即在规则或策略中使用。您还可以创建不与任何规则或策略关联的对象。当您在规则或策略中使用该未关联的对象时，CDO 会创建该对象的副本并使用该副本。原始未关联对象仍保留在可用对象列表中，直到被夜间维护作业删除或您将其删除。

未关联的对象作为副本保留在 CDO 中，以确保在意外删除与对象关联的规则或策略时不会丢失所有配置。

要查看未关联的对象，请点击对象选项卡的左侧窗格中的 ，然后选中**未关联 (Unassociated)** 复选框。




# 比较对象

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 过滤页面上的对象以查找要比较的对象。

**步骤 3** 点击**比较**按钮 Compare。

**步骤 4** 最多选择三个要比较的对象。

**步骤 5** 并排查看屏幕底部的对象。

- 点击“对象详细信息”(Object Details) 标题栏中的向上和向下箭头，可查看更多或更少的对象详细信息。
- 展开或折叠详细信息和关系框以查看更多或更少的信息。

**步骤 6** （可选）“关系”框显示对象的使用方式。它可能与设备或策略相关联。如果对象与设备关联，您可以点击设备名称，然后点击**查看配置**以查看设备的配置。CDO 显示设备的配置文件，并突出显示该对象的条目。

# 过滤器

您可以在**清单 (Inventory)** 和**对象 (Objects)** 页面上使用许多不同的过滤器来查找要查找的设备和对象。

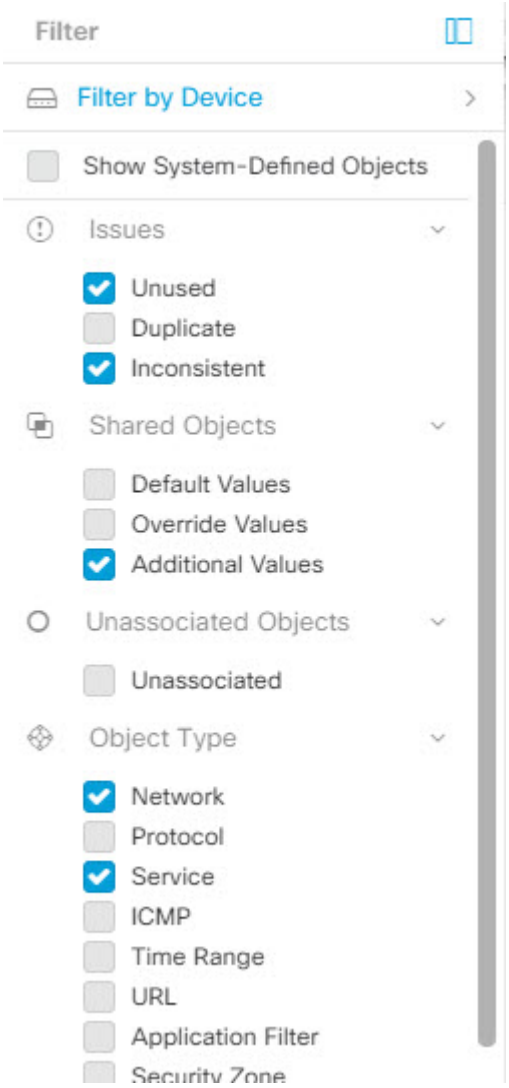
要过滤，请点击清单、策略和对象选项卡的左侧窗格中的 ：

清单过滤器允许您按设备类型、硬件和软件版本、Snort版本、配置状态、连接状态、冲突检测以及保护设备连接器和标签进行过滤。您可以应用过滤器在所选设备类型选项卡中查找设备。您可以使用过滤器在所选设备类型选项卡中查找设备。

对象过滤器允许您按设备、问题类型、共享对象、未关联的对象和对象类型进行过滤。您可以在结果中包含或不包含系统对象。您还可以使用搜索字段在过滤器结果中搜索包含特定名称、IP 地址或端口号的对象。

过滤设备和对象时，您可以组合搜索词来创建多个潜在的搜索策略来查找相关结果。

在以下示例中，过滤器应用于“问题（已使用或不一致）AND 具有其他值的共享对象 AND 类型为网络 OR 服务的对象”。




# 对象过滤器

要过滤，请点击“对象”(Objects) 选项卡的左侧窗格的 ：

- **所有对象 (All Objects)** - 此过滤器提供您在 CDO 中注册的所有设备中可用的所有对象。此过滤器可用于浏览所有对象，或作为搜索或进一步应用子过滤器的起点。
- **共享对象 (Shared Objects)** - 此快速过滤器显示 CDO 发现的在多台设备上共享的所有对象。
- **按设备排列的对象 (Objects By Device)** - 允许您选择特定设备，以便可以查看在所选设备上找到的对象。

**子过滤器 (Sub filters)** - 在每个主过滤器中，您可以应用子过滤器以进一步缩小选择范围。这些子过滤器基于对象类型 - 网络、服务、协议等。

此过滤器栏中的选定过滤器将返回与以下条件匹配的对象：

***** 位于两台设备之一上的对象。（点击**按设备过滤 (Filter by Device)** 以指定设备。）AND 是

*** 不一致** 对象 AND 是

*** 网络 (Network)** 对象 OR **服务 (Service)** 对象 AND

***** 包含**"组"** 在对象命名约定中

由于选中了**显示系统对象 (Show System Objects)**，因此结果将包括系统对象和用户定义的对象。

### 显示系统对象过滤器

某些设备随附常见服务的预定义对象。这些系统对象很方便，因为它们已经为您创建，您可以在规则和策略中使用它们。对象表中可以有许多系统对象。系统对象无法编辑或删除。

默认情况下，**显示系统对象**处于**关闭**状态。要在对象表中显示系统对象，请选中过滤器栏中的**显示系统对象 (Show System Objects)**。要隐藏对象表中的系统对象，请在过滤器栏中保持未选中状态。

如果隐藏系统对象，它们将不会包含在搜索和过滤结果中。如果显示系统对象，它们将包含在对象搜索和过滤结果中。

## 配置对象过滤器

您可以根据需要过滤任意数量的条件。过滤所依据的类别越多，预期的结果就越少。

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 点击页面顶部的过滤器图标 ，打开过滤器面板。取消选中任何已选中的过滤器，以确保不会无意中过滤掉任何对象。此外，查看搜索字段并删除可能已在搜索字段中输入的任何文本。

**步骤 3** 如果要将结果限制为在特定设备上找到的结果，请执行以下操作：

**a.** 点击**按设备过滤 (Filter By Device)**。

**b.** 搜索所有设备或点击设备选项卡以仅搜索特定类型的设备。

**c.** 选中要包含在过滤条件中的设备。

**d.** 点击**确定 (OK)**。

**步骤 4** 选中**显示系统对象 (Show System Objects)** 以在搜索结果中包含系统对象。取消选中**显示系统对象 (Show System Objects)** 可从搜索结果中排除系统对象。

**步骤 5** 选中要作为过滤依据的对象**问题**。如果选中多个问题，则选中的任何类别的对象都将包含在过滤器结果中。

**步骤 6** 如果要查看存在问题但被管理员忽略的对象，请选中**已忽略 (Ignored)** 的问题。

**步骤 7** 如果要过滤两台或多台设备之间共享的对象，请在**共享对象 (Shared Objects)** 中选中所需的过滤器。

- **默认值 (Default Values)**：过滤仅具有默认值的对象。
- **覆盖值 (Override Values)**：过滤具有覆盖值的对象。
- **其他值 (Additional Values)**：过滤具有其他值的对象。

**步骤 8** 如果要过滤不属于任何规则或策略的对象，请选中**未关联 (Unassociated)** 。

**步骤 9** 选中要作为过滤依据的**对象类型 (Object Types)**。

**步骤 10** 您还可以将对象名称、IP 地址或端口号添加到对象搜索字段，以在过滤结果中查找符合搜索条件的对象。

### 何时从过滤条件中排除设备

将设备添加到过滤条件时，结果会显示设备上的对象，但不会显示这些对象与其他设备的关系。例如，假设 ObjectA 在 ASA1 和 ASA2 之间共享。如果要过滤对象以查找 ASA1 上的共享对象，则会找到 ObjectA，但“关系”窗格只会显示该对象位于 ASA1 上。

要查看与对象相关的所有设备，请不要在搜索条件中指定设备。按其他条件过滤并添加搜索条件（如果您愿意）。选择CDO识别的对象，然后在“关系”窗格中进行查看。您将看到与对象相关的所有设备和策略。

## 忽略对象

解决具有未使用、重复或不一致问题对象的方法之一是忽略它们。您可以决定，尽管对象未使用、重复或不一致，但该状态存在正当理由，并且您选择不解决对象问题。解决未使用的对象问题, on page 512解决重复对象问题, on page 511解决不一致的对象问题, on page 513在未来的某个时候，您可能希望解析这些被忽略的对象。由于CDO在搜索对象问题时不显示已忽略的对象，因此您需要过滤已忽略对象的对象列表，然后对结果执行操作。

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 过滤和搜索被忽略的对象。对象过滤器, on page 108

**步骤 3** 在**对象 (Object)** 表中，选择要取消忽略的对象。一次可以取消忽略一个对象。

**步骤 4** 点击详细信息窗格中的取消忽略。

**步骤 5** 确认您的请求。现在，当您按问题过滤对象时，您应该会找到以前忽略的对象。

## 删除对象

可以删除单个对象或多个对象。

### 删除单个对象

**Caution** 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。此外，还会在**具有待处理更改的设备**页面中为每个启用了**发现和管理网络对象**的 本地管理中心 创建一个条目，您可以从中选择变更并将其部署到有这些对象的 本地管理中心。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

**步骤 1** 在左侧的 CDO 导航栏中，选择**对象 (Objects)**并选择一个选项。
**步骤 2** 使用对象过滤器和搜索字段找到要删除的对象，然后将其选中。
**步骤 3** 查看关系窗格。如果在策略或对象组中使用了对象，则在将其从该策略或组中删除之前，无法删除该对象。
**步骤 4** 点击“操作”(Actions) 窗格中，点击**编辑**图标 。
**步骤 5** 点击确定，确认要删除对象。
**步骤 6** 预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

## 删除一组未使用的对象

当您载入设备并开始解决对象问题时，您会发现许多未使用的对象。一次最多可以删除 50 个未使用的对象。

**步骤 1** 使用问题过滤器查找未使用的对象。您还可以使用设备过滤器通过选择无设备来查找未与设备关联的对象。过滤对象列表后，系统将显示对象复选框。
**步骤 2** 选中对象表标题中的全选复选框，以选择过滤器找到的显示在对象表中的所有对象；或者，选中要删除的各个对象的各个复选框。
**步骤 3** 点击“操作”(Actions) 窗格中，点击**编辑**图标 。
**步骤 4** 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

# 网络对象

**网络对象** 可以包含主机、网络 IP 地址、IP 地址范围、完全限定域名 (FQDN)或用 CIDR 符号表示的子网 。**网络组**是添加到组中的网络对象和其他单个地址或子网络的集合。网络对象和网络组用于访问规则、网络策略和 NAT 规则。您可以使用 CDO 创建、更新和删除网络对象和网络组。

***Table 4:*** 网络对象的允许值

| 设备类型 | **IPv4 / IPv6** | 单个地址 | 地址范围 | 域名名称 | 使用 **CIDR** 表示法的子网。 |
|---|---|---|---|---|---|
| ASA | IPv4 和 IPv6 | 是 | 是 | 是 | 是 |

***Table 5:*** 网络组允许的内容

| 设备类型 | **IP** 值 | 网络对象 | 网络组 |
|---|---|---|---|
| ASA | 是 | 是 | 是 |

### 跨产品重用网络对象

如果您的 思科防御协调器 租户具有 云交付的防火墙管理中心 和一个或多个已载入的 本地管理中心 到租户：

- 在创建 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象或组时，对象的副本也会被添加到在配置 云交付的防火墙管理中心 时使用的**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的对象列表中。
- 创建 Secure Firewall Threat Defense、 FDM 管理 威胁防御或 ASA 网络对象或组时，系统会在“**Devices with Pending Changes**”页面中为每个启用了“**Discover & Manage Network Objects**”的 本地防火墙管理中心 创建一个条目。从此列表中，您可以选择对象并将其部署到要 本地管理中心 在其上使用的对象，并丢弃不需要的对象。导航**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**，选择 本地管理中心，然后点击**对象 (Objects)** 以查看本地防火墙管理中心 用户界面中的对象并将其分配给策略。

对任一页面上的网络对象或组所做的更改适用于两个页面上的对象或组实例。从一个页面删除对象也会从另一个页面删除该对象的相应副本。

例外情况：

- 如果 云交付的防火墙管理中心 已存在同名的网络对象，则不会在 思科防御协调器 的**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上复制新的 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象
- 由本地 Cisco Secure Firewall Management Center 管理的载入 威胁防御 设备中的网络对象和组不会复制到**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，因此无法在 云交付的防火墙管理中心 中使用。

  请注意，对于已迁移到 云交付的防火墙管理中心 的本地 Cisco Secure Firewall Management Center 实例，如果在部署到 FTD 设备的策略中使用网络对象和组，它们将被复制到 CDO 对象页面。
- 新租户上会自动启用在 CDO 和 云交付的防火墙管理中心 之间共享网络对象，但现有租户必须另行请求。如果您的网络对象未与 云交付的防火墙管理中心 共享，请CDO 客户如何通过 TAC 提交支持请求 以在您的租户上启用这些功能。
- CDO 和 本地管理中心 之间的共享网络对象不会在 CDO 上自动启用，以便新的 本地管理中心 已载入 CDO。如果您的网络对象未与 本地管理中心 共享，请确保为**设置 (Settings)** 中的 本地管理中心 启用**发现和管理网络对象 (Discover & Manage Network Objects)** 切换按钮，或CDO 客户如何通过 TAC 提交支持请求 以在您的租户上启用这些功能。

### 查看网络对象

使用 CDO 创建的网络对象以及已载入的设备配置中的 CDO 识别的网络对象会显示在对象页面上。它们标有对象类型。这使您可以按对象类型进行过滤，以快速找到要查找的对象。

在“对象”(Objects) 页面上选择网络对象时，您可在“详细信息”(Details) 窗格中看到该对象的值。“关系”(Relationships) 窗格显示对象是否用于策略中，以及对象存储在什么设备上。

在点击网络组时，您会看到该组的内容。网络组是网络对象为其提供的所有值的综合体。

# 创建或编辑 ASA 网络对象和网络组

**ASA 网络对象**可以包含以 CIDR 表示法表示的主机名、IP 地址或子网地址。**网络组**是在访问规则、网络策略和 NAT 规则中使用的网络对象、网络组和 IP 地址的集合。您可以使用 CDO 来创建、读取、更新和删除网络对象和网络组。

***Table 6: ASA* 网络对象和组的允许值**

| 设备类型 | **IPv4 / IPv6** | 单个地址 | 地址范围 | 部分限定域名 **(PQDN)** | 使用 **CIDR** 表示法的子网。 |
|---|---|---|---|---|---|
| ASA | IPv4 / IPv6 | 是 | 是 | 是 | 是 |

**Note** 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。此外，还会在**具有待处理更改的设备**页面中为每个启用了**发现和管理网络对象**的本地管理中心创建一个条目，您可以从中选择对象并将其部署到需要这些对象的 本地管理中心。

**Caution** 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。此外，还会在**具有待处理更改的设备**页面中为每个启用了**发现和管理网络对象**的 本地管理中心 创建一个条目，您可以从中选择变更并将其部署到有这些对象的 本地管理中心。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

## 创建 ASA 网络对象

**网络对象** 可以包含主机、网络 IP 地址、IP 地址范围、完全限定域名 (FQDN)或用 CIDR 符号表示的子网 。网络对象用于访问规则、网络策略和 NAT 规则。您可以使用 CDO 创建、更新和删除网络对象和网络组。

**Note** 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。此外，还会在**具有待处理更改的设备**页面中为每个启用了**发现和管理网络对象**的本地管理中心创建一个条目，您可以从中选择对象并将其部署到需要这些对象的 本地管理中心。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击蓝色加号按钮  以创建新的对象。

**步骤 3** 点击 **ASA** > **网络 (Network)**。

**步骤 4** 输入对象名称。

**步骤 5** 选择**创建网络对象 (Create a network object)**。

**步骤 6** （可选）输入对象说明。

**步骤 7** 在**值 (Value)** 部分中，通过以下方式之一添加 IP 地址信息：

- 选择 **eq**，然后输入单个 IP 地址、使用 CIDR 表示法的子网地址或部分限定域名 (PQDN)。
- 选择**范围 (range)**，然后输入 IP 地址范围。输入范围内的起始地址和结束地址，以空格分隔。例如，10.1.1.1 10.1.1.255 或 2001:DB8:1::1 2001:DB8:1::3

**步骤 8** 点击**添加 (Add)**。

**Important** 新创建的网络对象不与任何 ASA 设备关联，因为它们不属于任何规则或策略。要查看这些对象，请在对象过滤器中选择**未关联**的对象类别。有关详细信息，请参阅对象过滤器。在设备的规则或策略中使用未关联的对象后，此类对象将与该设备关联。

## 创建 ASA 网络组

网络组可以包含 IP 地址值、网络对象和网络组。创建新的网络组时，可以按名称、IP 地址、IP 地址范围或 FQDN 搜索现有对象，并将其添加到网络组。如果对象不存在，您可以立即在同一接口中创建该对象并将其添加到网络组。网络组可以同时包含 IPv4 和 IPv6 地址。

**Note** 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。此外，还会在**具有待处理更改的设备**页面中为每个启用了**发现和管理网络对象**的本地管理中心创建一个条目，您可以从中选择对象并将其部署到需要这些对象的 本地管理中心。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击蓝色加号按钮  以创建新的对象。

**步骤 3** 点击 **ASA** > **网络 (Network)**。

**步骤 4** 输入 **对象名称**。

**步骤 5** 选择创建网络组。

**步骤 6** （可选）输入对象说明。

**步骤 7** 在**值 (Values)** 字段中输入值或对象名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。

**步骤 8** 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

**步骤 9** 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

**步骤 10** 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。
- 点击**添加值 (Add Value)** 可在不使用对象的情况下创建内联值。输入一个值，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

**Note** 您可以点击编辑图标来修改详细信息。点击“删除”按钮不会删除对象本身；相反，它会将其从网络组中删除。

**步骤 11** 添加所需的对象后，点击**添加 (Add)** 以创建新的网络组。

**步骤 12** 预览和部署所有设备的配置更改, on page 313。

## 编辑 ASA 网络对象

**Caution** 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。此外，还会在**具有待处理更改的设备**页面中为每个启用了**发现和管理网络对象**的 本地管理中心 创建一个条目，您可以从中选择变更并将其部署到有这些对象的 本地管理中心。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 使用对象过滤器和搜索字段找到要编辑的对象。

**步骤 3** 选择网络对象，然后点击**操作 (Actions)** 窗格中的编辑图标 。

**步骤 4** 以在上述过程中创建值的相同方式编辑对话框中的值。

**Note** 点击旁边的删除图标，从网络组中删除对象。

**步骤 5** 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

**步骤 6** 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

## 编辑 ASA 网络组

**Caution** 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。此外，还会在**具有待处理更改的设备**页面中为每个启用了**发现和管理网络对象**的 本地管理中心 创建一个条目，您可以从中选择变更并将其部署到有这些对象的 本地管理中心。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 使用对象过滤器和搜索字段找到您要编辑的网络组。

**步骤 3** 选择网络组，然后点击**操作 (Actions)** 窗格中的编辑图标 。

**步骤 4** 如果要更改已添加到网络组的对象或网络组，请执行以下步骤：

**a.** 点击对象名称或网络组旁边的编辑图标 可对其进行修改。

**b.** 点击复选标记以保存更改。

**Note** 您可以点击删除图标从网络组中删除该值。

**步骤 5** 如果要向此网络组添加新的网络对象或网络组，必须执行以下步骤：

**a.** 在值字段中，输入新值或现有网络对象的名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

**b.** 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

**c.** 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。
- 点击**添加值 (Add Value)** 可在不使用对象的情况下创建内联值。输入一个值，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

**步骤 6** 点击**保存 (Save)**。CDO 显示将受更改影响的策略。

**步骤 7** 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

**步骤 8** 预览和部署所有设备的配置更改, on page 313。

## 向共享网络组添加其他值

共享网络组中与其关联的所有设备上都存在的值被称为“默认值”。CDO 允许您向共享网络组添加“其他值”，并将这些值分配给与该共享网络组关联的某些设备。当CDO将更改部署到设备时，它会确定内容并将“默认值”推送到与共享网络组关联的所有设备，而“其他值”只会被推送到指定的设备。

例如，假设您的总部有四台 AD 主服务器，那么这些服务器应可从您的所有站点进行访问。因此，您创建了一个名为“Active-Directory”的对象组，以便将其用于所有站点。现在，您要为其中一个分支机构再添加两台 AD 服务器。为此，您可以通过将其详细信息添加为对象组“Active-Directory”上该分支机构的特定附加值来执行此操作。这两台服务器不参与确定对象“Active-Directory”是一致的还是共享的。因此，您可从所有站点访问四台 AD 主服务器，但分支机构（具有两台附加服务器）可以访问两台 AD 服务器和四台 AD 主服务器。

**Note** 如果存在不一致的共享网络组，则您可以将它们合并为具有其他值的单个共享网络组。有关详细信息，请参阅解决不一致的对象问题。

**Caution** 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。此外，还会在**具有待处理更改的设备**页面中为每个启用了**发现和管理网络对象**的 本地管理中心 创建一个条目，您可以从中选择变更并将其部署到有这些对象的 本地管理中心。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 使用对象过滤器和搜索字段找到您要编辑的共享网络组。

**步骤 3** 点击**操作 (Actions)** 窗格中的编辑图标 。

- **设备 (Devices)** 字段会显示共享网络组所在的设备。
- **使用情况 (Usage)** 字段会显示与共享网络组关联的规则集。
- **默认值 (Default Values)** 字段将指定默认网络对象及其与创建期间提供的共享网络组关联的值。在此字段旁边，您可以看到包含此默认值的设备数量，您可以点击查看其名称和设备类型。您还可以查看与此值关联的规则集。

**步骤 4** 在 其他值 (Additional Values) 字段中输入值或名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。

**步骤 5** 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

**步骤 6** 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

**步骤 7** 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。
- 点击添加值可在不使用对象的情况下创建内联值。输入一个值，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

**步骤 8** 在**设备 (Devices)** 列中，点击与新添加的对象关联的单元格，然后点击**添加设备 (Add Devices)**。

**步骤 9** 选择所需的设备，然后点击**确定 (OK)**。

**步骤 10** 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

**步骤 11** 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

**步骤 12** 预览和部署所有设备的配置更改, on page 313。

## 编辑共享网络组中的其他值

⚠

**Caution** 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。此外，还会在**具有待处理更改的设备**页面中为每个启用了**发现和管理网络对象**的 本地管理中心 创建一个条目，您可以从中选择变更并将其部署到有这些对象的 本地管理中心。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

**步骤 3** 点击 **操作** 窗格中的编辑图标 。

**步骤 4** 修改覆盖值：

- 点击编辑图标以修改值。
- 点击**设备 (Devices)** 列中的单元格以分配新设备。您可以选择已分配的设备，然后点击**删除覆盖 (Remove Overrides)** 以删除该设备上的覆盖。
- 点击**默认值 (Default Values)** 中的 箭头，将其设置为共享网络组的其他值。与共享网络组关联的所有设备都会自动分配到该共享网络组。
- 点击**覆盖值 (Override Values)** 中的 箭头，将其推送并设置为共享网络组的默认对象。
- 点击旁边的删除图标，从网络组中删除对象。

**步骤 5** 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

**步骤 6** 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

**步骤 7** 预览和部署所有设备的配置更改, on page 313。

### 删除网络对象和组

如果 云交付的防火墙管理中心 被部署在您的租户上：

从 或 **对象 (Objects) > ASA 对象 (ASA Objects)** 页面删除网络对象或组都会从 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面中删除复制的对象或组，反之亦然。

# 信任点对象

CDO 允许您将数字证书添加为信任点对象，然后将其安装在一个或多个托管 ASA 设备上。单个信任点对象是包含身份对（身份证书和颁发者的 CA 证书）、仅身份证书或仅 CA 证书的容器。

您可以在 ASA 设备配置多个信任点。支持的证书格式为 PKCS12、PEM 和 DER。

## 使用 PKCS12 添加身份证书对象

此程序通过上传证书文件或将现有证书文本粘贴到文本框中来创建内部证书身份或内部身份证书。您可以根据需要生成任意数量的身份证书。

您可以上传以 **PKCS12** 格式编码的文件。PKCS12 是将服务器证书、任何中间证书和私钥保存在一个加密文件中的单个文件。PKCS#12 或 PFX 文件将服务器证书、中间证书和私钥保存在一个加密文件中。输入**口令**值进行解密。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击  并选择 **ASA** > **信任点 (Trustpoints)**。

**步骤 3** 为证书输入一个**对象名称 (Object Name)**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

**步骤 4** 在**证书类型 (Certificate Type)** 步骤中，选择 **身份证书 (Identity Certificate)**。

**步骤 5** 在**导入类型 (Import Type)** 步骤中，选择**上传 (Upload)** 以上传证书文件。

**登记 (Enrollment)** 步骤设置为“终端”(Terminal)。

**步骤 6** 在**证书内容 (Certificate Contents)** 步骤中，输入 PKCS12 格式详细信息。

PKCS#12 或 PFX 文件将服务器证书、中间证书和私钥保存在一个加密文件中。输入**口令**值进行解密。

**步骤 7** 点击**继续**。

**步骤 8** 在**高级选项 (Advanced Options)** 步骤中，您可以配置以下内容：

在**吊销 (Revocation)** 选项卡中，您可以配置以下内容：

- **启用证书撤销列表 (CRL) (Enable Certificate Revocation Lists [CRL])** - 选中可启用 CRL 检查。

默认情况下会选中**使用来自证书的 CRL 分发点 (Use CRL distribution point from the certificate)** 复选框，以便获取来自证书的吊销列表分发 URL。

**缓存刷新时间（以分钟为单位）(Cache Refresh Time [in minutes])** - 输入缓存刷新之间间隔的分钟数。默认值为 60 分钟。范围为 1 至 1440 分钟。为了避免必须从 CA 重复检索同一 CRL，ASA 可以将检索的 CRL 存储在本地，我们称之为 CRL 缓存。CRL 缓存容量根据平台而异，并且是跨所有情景的累积容量。如果尝试缓存新检索的 CRL 会超出其存储限制，则 ASA 会删除最近最不常用的 CRL，直到更多空间可用为止。

- **启用在线证书状态协议 (OCSP) (Enable Online Certificate Status Protocol [OCSP])** - 选中可启用 OCSP 检查。

  **OCSP 服务器 URL (OCSP Server URL)** - 需要进行 OCSP 检查时，用以检查撤销的 OCSP 服务器的 URL。此 URL 必须以 **`http://`** 开头。

  **禁用 nonce 扩展 (Disable Nonce Extension)** - 选中此复选框，从而以加密方式将请求与响应绑定来避免重放攻击。此过程适用是由于通过将请求中的扩展与响应中的扩展进行匹配，从而确保其相同。如果您所使用的 OCSP 服务器发送的是不包含此匹配随机数扩展的预生成响应，请取消选中 **Disable nonce extension** 复选框。

  **评估优先级 (Evaluation Priority)** - 指定是首先在 CRL 还是 OSCP 中评估证书的吊销状态。

- **如果吊销信息无法访问，请考虑证书是否有效 (Consider the certificate valid if revocation information cannot be reached)** - 选中此复选框可在吊销信息无法访问时将证书视为有效证书。

  有关吊销检查的详细信息，请参阅思科 ASA 系列常规操作 ASDM 配置的“基本设置”一书 X.Y 文档中的“数字证书”一章。

点击**其他 (Others)** 选项卡：

- **使用 CA 证书验证 (Use CA Certificate for the Validation of)** - 指定可以由此 CA 验证的连接类型。
  - **IPSec 客户端 (IPSec Client)** - 验证远程 SSL 服务器提供的证书。
  - **SSL 客户端 (SSL Client)** - 验证传入 SSL 连接提供的证书。
  - **SSL 服务器 (SSL Server)** - 验证传入 IPSec 连接提供的证书。
- **将身份证书用于 (Use Identity Certificate for)** - 指定如何使用已注册的 ID 证书。
  - **SSL 和 IPSec (SSL & IPSec)** - 用于验证 SSL 和 IPSec 连接。
  - **代码签名者 (Code Signer)** - 代码签名者证书是其关联私钥用于创建数字签名的特殊证书。代码签名证书从 CA 获取，已签名代码本身可揭示证书来源。
- **其他选项：**
  - **在基本约束扩展中启用 CA 标志 (Enable CA flag in basic constraints extension)** - 如果需要此证书能够签署其他证书，则选中此选项。基本约束扩展标识证书主体是否为证书颁发机构 (CA)，这种情况下证书可用于签署其他证书。CA 标志是此扩展的一部分。证书中包含这些项目
  - **接受由该CA签发的证书 (Accept certificates issued by this CA)** - 选择此选项以指示 ASA 应从指定的 CA 接收证书。

- **忽略 IPsec 密钥使用 (Ignore IPSec Key Usage)** - 如果不希望在 IPsec 远程客户端证书的密钥使用和扩展密钥使用扩展中验证值，则选择此选项。您可以抑制对 IPsec 客户端证书的密钥用法检查。默认情况下不启用此选项。

**步骤 9** 点击 **Add**。

## 创建自签名身份证书对象

此程序介绍通过在向导中输入相应的证书字段值来为您的ASA生成自签名证书的步骤。您可以根据需要来生成任意数量的自签名证书。

要创建自签名身份证书对象，请执行以下步骤：

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击  并选择 **ASA** > **信任点 (Trustpoints)**。

**步骤 3** 为证书输入一个**对象名称 (Object Name)**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

**步骤 4** 在**身份证书** 步骤中，选择**身份证书 (Identity Certificate)**。

**步骤 5** 在**导入类型 (Import Type)** 步骤中，选择**新建 (New)** 以上传证书文件，然后点击**继续 (Continue)**。

**步骤 6** 在**注册 (Enrollment)** 步骤中，选择**自签名 (Self-Signed)**，然后点击**继续 (Continue)**。

系统将显示**证书内容 (Certificates Content)** 步骤。阅读根据证书内容生成自签名证书和 CSR 证书，了解正在生成的自签名证书中的 CN 和 SANS 内容。

**步骤 7** 在**证书内容 (Certificate Contents)** 步骤中，请配置以下内容：

- **国家/地区 (Country [C])** - 从下拉列表中选择国家/地区代码。
- **州或省 (ST) (State or Province [ST])** - 证书中包括的州或省。
- **地区或城市 (Locality or City) (L)** - 证书中包括的地区，例如城市名称。
- **组织 (O) (Organization [O])** - 要包含在证书中的组织或公司名称。
- **组织单位（部门）(Organizational Unit [Department]) (OU)** - 证书中包含的组织单位名称（例如部门名称）。
- **公用名 (CN)(Common Name [CN])** - 要包含在证书中的 X.500 公用名。它们可能是设备、网站或其他文本字符串的名称。通常需要有此元素，才能成功进行连接。例如，用于远程访问 VPN 的内部证书中必须包括 CN。
- **电子邮件地址 (Email Address) (EA)**- 与身份证书关联的邮件地址。
- **IP 地址 (IP Address)** - 网络中的 ASA IP 地址，采用由四部分组成的点分十进制表示法。
- **设备的 FQDN (Device's FQDN)** - 一个明确的域名，用于指示 DNS 树状层次结构中的节点位置。
- **包括设备的序列号 (Include Device's Serial Number)** - 如果要将 ASA 序列号添加到证书参数，则选中此复选框。

a) 点击**密钥 (Key)** 选项卡。

- 选择 **RSA** 或 **ECDSA** 密钥类型。
- **密钥大小 (Key Size)**：如果密钥对不存在，可定义所需的密钥大小（模数，以位为单位）。建议的 RSA 密钥大小为 1024，建议的 ECDSA 密钥大小为 348。模数越大，密钥越安全。但是，生成模数较大的密钥需要更长的时间（模数大于 512 位时需要一分钟或更长时间），而且交换时的处理时间也更长。
- 点击**继续**。

**步骤 8** 在**高级选项 (Advanced Options)** 步骤中，您可以配置以下内容：

在**吊销 (Revocation)** 选项卡中，您可以配置以下内容：

- **启用证书撤销列表 (CRL) (Enable Certificate Revocation Lists [CRL])** - 选中可启用 CRL 检查。

  默认情况下会选中**使用来自证书的 CRL 分发点 (Use CRL distribution point from the certificate)** 复选框，以便获取来自证书的吊销列表分发 URL。

  **缓存刷新时间（以分钟为单位）(Cache Refresh Time [in minutes])** - 输入缓存刷新之间间隔的分钟数。默认值为 60 分钟。范围为 1 至 1440 分钟。为了避免必须从 CA 重复检索同一 CRL，ASA 可以将检索的 CRL 存储在本地，我们称之为 CRL 缓存。CRL 缓存容量根据平台而异，并且是跨所有情景的累积容量。如果尝试缓存新检索的 CRL 会超出其存储限制，则 ASA 会删除最近最不常用的 CRL，直到更多空间可用为止。

- **启用在线证书状态协议 (OCSP) (Enable Online Certificate Status Protocol [OCSP])** - 选中可启用 OCSP 检查。

  **OCSP 服务器 URL (OCSP Server URL)** - 需要进行 OCSP 检查时，用以检查撤销的 OCSP 服务器的 URL。此 URL 必须以 **`http://`** 开头。

  **禁用 nonce 扩展 (Disable Nonce Extension)** - 选中此复选框，从而以加密方式将请求与响应绑定来避免重放攻击。此过程适用是由于通过将请求中的扩展与响应中的扩展进行匹配，从而确保其相同。如果您所使用的 OCSP 服务器发送的是不包含此匹配随机数扩展的预生成响应，请取消选中 **Disable nonce extension** 复选框。

  **评估优先级 (Evaluation Priority)** - 指定是首先在 CRL 还是 OSCP 中评估证书的吊销状态。

- **如果吊销信息无法访问，请考虑证书是否有效 (Consider the certificate valid if revocation information cannot be reached)** - 选中此复选框可在吊销信息无法访问时将证书视为有效证书。

  有关吊销检查的详细信息，请参阅思科 ASA 系列常规操作 ASDM 配置的“基本设置”一书X.Y 文档中的“数字证书”一章。

点击**其他 (Others)** 选项卡：

- **使用 CA 证书验证 (Use CA Certificate for the Validation of)** - 指定可以由此 CA 验证的连接类型。
  - **IPSec 客户端 (IPSec Client)** - 验证远程 SSL 服务器提供的证书。
  - **SSL 客户端 (SSL Client)** - 验证传入 SSL 连接提供的证书。
  - **SSL 服务器 (SSL Server)** - 验证传入 IPSec 连接提供的证书。
- **将身份证书用于 (Use Identity Certificate for)** - 指定如何使用已注册的 ID 证书。
  - **SSL 和 IPSec (SSL & IPSec)** - 用于验证 SSL 和 IPSec 连接。

- **代码签名者 (Code Signer)** - 代码签名者证书是其关联私钥用于创建数字签名的特殊证书。代码签名证书从 CA 获取，已签名代码本身可揭示证书来源。

- 其他选项：
  - **在基本约束扩展中启用 CA 标志 (Enable CA flag in basic constraints extension)** - 如果需要此证书能够签署其他证书，则选中此选项。基本约束扩展标识证书主体是否为证书颁发机构 (CA)，这种情况下证书可用于签署其他证书。CA 标志是此扩展的一部分。证书中包含这些项目
  - **接受由该CA签发的证书 (Accept certificates issued by this CA)** - 选择此选项以指示 ASA 应从指定的 CA 接收证书。
  - **忽略 IPsec 密钥使用 (Ignore IPSec Key Usage)** - 如果不希望在 IPsec 远程客户端证书的密钥使用和扩展密钥使用扩展中验证值，则选择此选项。您可以抑制对 IPsec 客户端证书的密钥用法检查。默认情况下不启用此选项。

**步骤 9** 点击 **Add**。

## 为证书签名请求 (CSR) 添加身份证书对象

证书颁发机构 (CA) 服务器信息和注册参数是生成证书签名请求 (CSR) 和从指定的CA获取身份证书所必需的。您需要选择 Rivest-Shamir-Adleman (RSA) 或椭圆曲线数字签名算法 (ECDSA) 密钥类型来生成请求。

通过提供标识信息并（可选）上传从 CA 获取的 CA 证书来创建信任点对象。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击  并选择 **ASA > 信任点 (Trustpoints)**。

**步骤 3** 为证书输入一个**对象名称 (Object Name)**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

**步骤 4** 在**身份证书** 步骤中，选择**身份证书 (Identity Certificate)**。

**步骤 5** 在**导入类型 (Import Type)** 步骤中，选择**新建 (New)** 以上传证书文件，然后点击**继续 (Continue)**。

**步骤 6** 在**注册 (Enrollment)** 步骤中，选择**手动 (Manual)**。

**步骤 7** （可选）您可以粘贴或上传从 CA 获取的 CA 证书。您可以将此字段留空。

**步骤 8** 点击“继续”(Continue)。

系统将显示“证书内容”(Certificates Content) 步骤。阅读根据证书内容生成自签名证书和 CSR 证书以了解正在生成的签名证书中的 CN 和 SANS 内容。

**步骤 9** 在**证书内容 (Certificate Contents)** 步骤中，请配置以下内容：

- **国家/地区 (Country [C])** - 从下拉列表中选择国家/地区代码。
- **州或省 (ST) (State or Province [ST])** - 证书中包括的州或省。
- **地区或城市 (Locality or City) (L)** - 证书中包括的地区，例如城市名称。

- **组织 (O) (Organization [O])** - 要包含在证书中的组织或公司名称。
- **组织单位（部门）(Organizational Unit [Department]) (OU)** - 证书中包含的组织单位名称（例如部门名称）。
- **公用名 (CN)(Common Name [CN])** - 要包含在证书中的 X.500 公用名。它们可能是设备、网站或其他文本字符串的名称。通常需要有此元素，才能成功进行连接。例如，用于远程访问 VPN 的内部证书中必须包括 CN。
- **电子邮件地址 (Email Address) (EA)**- 与身份证书关联的邮件地址。
- **IP 地址 (IP Address)** - 网络中的 ASA IP 地址，采用由四部分组成的点分十进制表示法。
- **使用者可选名称 (SAN) (Subject Alternative Name [SAN])** - 此字段也将作为“unstructuredName”作为证书使用者 DN 的一部分。如果证书用于多个域或 IP 地址，我们建议您使用此字段。
  - **使用设备主机名 (Use Device Host Name)**：使用设备的主机名。
  - **自定义：设备的 FQDN (Custom: Device's FQDN)** - 一个明确的域名，用于指示 DNS 树状层次结构中的节点位置。

    注释　　我们建议 CN 和 **自定义 FQDN** 中指定的值相同。

- **包括设备的序列号 (Custom: Device's FQDN)** - 如果要将 ASA 序列号添加到证书，则选中此复选框。CA 使用序列号对证书进行验证，或者之后将证书与特定设备相关联。如有疑问，请含序列号，因为这对调试用途非常有用。

a) 点击**密钥 (Key)** 选项卡。
   - 选择 **RSA** 或 **ECDSA** 密钥类型。
   - **密钥大小 (Key Size)**：如果密钥对不存在，可定义所需的密钥大小（模数，以位为单位）。建议的 RSA 密钥大小为 1024，建议的 ECDSA 密钥大小为 348。模数越大，密钥越安全。但是，生成模数较大的密钥需要更长的时间（模数大于 512 位时需要一分钟或更长时间），而且交换时的处理时间也更长。
   - 点击**继续**。

**步骤 10** 在**高级选项 (Advanced Options)** 步骤中，您可以配置以下内容：

在**吊销 (Revocation)** 选项卡中，您可以配置以下内容：

- **启用证书撤销列表 (CRL) (Enable Certificate Revocation Lists [CRL])** - 选中可启用 CRL 检查。

  默认情况下会选中**使用来自证书的 CRL 分发点 (Use CRL distribution point from the certificate)** 复选框，以便获取来自证书的吊销列表分发 URL。

  **缓存刷新时间（以分钟为单位）(Cache Refresh Time [in minutes])** - 输入缓存刷新之间间隔的分钟数。默认值为 60 分钟。范围为 1 至 1440 分钟。为了避免必须从 CA 重复检索同一 CRL，ASA 可以将检索的 CRL 存储在本地，我们称之为 CRL 缓存。CRL 缓存容量根据平台而异，并且是跨所有情景的累积容量。如果尝试缓存新检索的 CRL 会超出其存储限制，则 ASA 会删除最近最不常用的 CRL，直到更多空间可用为止。
- **启用在线证书状态协议 (OCSP) (Enable Online Certificate Status Protocol [OCSP])** - 选中可启用 OCSP 检查。

**OCSP 服务器 URL (OCSP Server URL)** - 需要进行 OCSP 检查时，用以检查撤销的 OCSP 服务器的 URL。此 URL 必须以 **http://** 开头。

**禁用 nonce 扩展 (Disable Nonce Extension)** - 选中此复选框，从而以加密方式将请求与响应绑定来避免重放攻击。此过程适用是由于通过将请求中的扩展与响应中的扩展进行匹配，从而确保其相同。如果您所使用的 OCSP 服务器发送的是不包含此匹配随机数扩展的预生成响应，请取消选中 **Disable nonce extension** 复选框。

**评估优先级 (Evaluation Priority)** - 指定是首先在 CRL 还是 OSCP 中评估证书的吊销状态。

- **如果吊销信息无法访问，请考虑证书是否有效 (Consider the certificate valid if revocation information cannot be reached)** - 选中此复选框可在吊销信息无法访问时将证书视为有效证书。

  有关吊销检查的详细信息，请参阅思科 ASA 系列常规操作 ASDM 配置的“基本设置”一书 X.Y 文档中的“数字证书”一章。

点击**其他 (Others)** 选项卡：

- **使用 CA 证书验证 (Use CA Certificate for the Validation of)** - 指定可以由此 CA 验证的连接类型。
  - **IPSec 客户端 (IPSec Client)** - 验证远程 SSL 服务器提供的证书。
  - **SSL 客户端 (SSL Client)** - 验证传入 SSL 连接提供的证书。
  - **SSL 服务器 (SSL Server)** - 验证传入 IPSec 连接提供的证书。
- **将身份证书用于 (Use Identity Certificate for)** - 指定如何使用已注册的 ID 证书。
  - **SSL 和 IPSec (SSL & IPSec)** - 用于验证 SSL 和 IPSec 连接。
  - **代码签名者 (Code Signer)** - 代码签名者证书是其关联私钥用于创建数字签名的特殊证书。代码签名证书从 CA 获取，已签名代码本身可揭示证书来源。
- **其他选项：**
  - **在基本约束扩展中启用 CA 标志 (Enable CA flag in basic constraints extension)** - 如果需要此证书能够签署其他证书，则选中此选项。基本约束扩展标识证书主体是否为证书颁发机构 (CA)，这种情况下证书可用于签署其他证书。CA 标志是此扩展的一部分。证书中包含这些项目
  - **接受由该CA签发的证书 (Accept certificates issued by this CA)** - 选择此选项以指示 ASA 应从指定的 CA 接收证书。
  - **忽略 IPsec 密钥使用 (Ignore IPSec Key Usage)** - 如果不希望在 IPsec 远程客户端证书的密钥使用和扩展密钥使用扩展中验证值，则选择此选项。您可以抑制对 IPsec 客户端证书的密钥用法检查。默认情况下不启用此选项。

**步骤 11** 点击**添加 (Add)**。

这将创建信任点证书对象。

# 添加受信任 CA 证书对象

受信任 CA 证书可从外部证书颁发机构获取，也可以使用自己的内部 CA 创建（例如通过 OpenSSL 工具生成证书）。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

---

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击  并选择 **ASA** > **信任点 (Trustpoints)**。

**步骤 3** 为证书输入一个**对象名称 (Object Name)**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

**步骤 4** 在**证书类型 (Certificate Type)** 步骤中，选择**受信任的 CA 证书 (Trusted CA Certificate)**。

**步骤 5** 在**证书内容 (Certificate Contents)** 步骤中，将证书内容粘贴到文本框中，或按照向导中的说明上传 CA 证书文件。

**步骤 6** 点击**继续**。向导前进到步骤 4。

证书必须遵循以下准则：

- 证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。
- 该证书必须为 PEM 或 DER 格式的 X509 证书。
- 您粘贴的证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。例如：

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

**步骤 7** 在**高级选项 (Advanced Options)** 步骤中，您可以配置以下内容：

在**吊销 (Revocation)** 选项卡中，您可以配置以下内容：

- **启用证书撤销列表 (CRL) (Enable Certificate Revocation Lists [CRL])** - 选中可启用 CRL 检查。

  默认情况下会选中**使用来自证书的 CRL 分发点 (Use CRL distribution point from the certificate)** 复选框，以便获取来自证书的吊销列表分发 URL。

  **缓存刷新时间（以分钟为单位）(Cache Refresh Time [in minutes])** - 输入缓存刷新之间间隔的分钟数。默认值为 60 分钟。范围为 1 至 1440 分钟。为了避免必须从 CA 重复检索同一 CRL，ASA 可以将检索的 CRL 存储在本地，我们称之为 CRL 缓存。CRL 缓存容量根据平台而异，并且是跨所有情景的累积容量。如果尝试缓存新检索的 CRL 会超出其存储限制，则 ASA 会删除最近最不常用的 CRL，直到更多空间可用为止。

- **启用在线证书状态协议 (OCSP) (Enable Online Certificate Status Protocol [OCSP])** - 选中可启用 OCSP 检查。

  **OCSP 服务器 URL (OCSP Server URL)** - 需要进行 OCSP 检查时，用以检查撤销的 OCSP 服务器的 URL。此 URL 必须以 **http://** 开头。

  **禁用 nonce 扩展 (Disable Nonce Extension)** - 选中此复选框，从而以加密方式将请求与响应绑定来避免重放攻击。此过程适用是由于通过将请求中的扩展与响应中的扩展进行匹配，从而确保其相同。如果您所使用的 OCSP 服务器发送的是不包含此匹配随机数扩展的预生成响应，请取消选中 **Disable nonce extension** 复选框。

  **评估优先级 (Evaluation Priority)** - 指定是首先在 CRL 还是 OSCP 中评估证书的吊销状态。

- **如果吊销信息无法访问，请考虑证书是否有效 (Consider the certificate valid if revocation information cannot be reached)** - 选中此复选框可在吊销信息无法访问时将证书视为有效证书。

  有关吊销检查的详细信息，请参阅思科 ASA 系列常规操作 ASDM 配置的“基本设置”一书 X.Y 文档中的“数字证书”一章。

点击**其他 (Others)** 选项卡：

- **使用 CA 证书验证 (Use CA Certificate for the Validation of)** - 指定可以由此 CA 验证的连接类型。
  - **IPSec 客户端 (IPSec Client)** - 验证远程 SSL 服务器提供的证书。
  - **SSL 客户端 (SSL Client)** - 验证传入 SSL 连接提供的证书。
  - **SSL 服务器 (SSL Server)** - 验证传入 IPSec 连接提供的证书。
- **其他选项：**
  - **在基本限制扩展中启用 CA 标志 (Enable CA flag in basic constraints extension)** - 如果要验证证书的主题是否为使用基本限制扩展的 CA，请选择此选项。
  - **接受由该CA签发的证书 (Accept certificates issued by this CA)** - 选择此选项以指示 ASA 应从指定的 CA 接收证书。
  - **接受由该CA 的从属 CA 签发的证书** - 选择此选项以指示 ASA 应从从属 CA 接收证书。
  - **忽略 IPsec 密钥使用 (Ignore IPSec Key Usage)** - 如果不希望在 IPsec 远程客户端证书的密钥使用和扩展密钥使用扩展中验证值，则选择此选项。您可以抑制对 IPsec 客户端证书的密钥用法检查。默认情况下不启用此选项。

**步骤 8** 点击**添加 (Add)**。

这将创建信任点证书对象。

## 根据证书内容生成自签名证书和 CSR 证书

您需要了解自签名证书和 CSR 证书中的 CN 和 SANS 概念。内容基于您在创建时指定的参数。您需要为 AnyConnect 客户端精确配置参数，以便连接到组织的预期 VPN 前端。

本节提供不同的使用案例和示例，让您了解基于所指定参数的自签名证书和 CSR 证书的内容。

### 使用案例 1：不同的 CN 和 FQDN 值

示例：

- 通用名称 (CN)：mywebsite.com
- FQDN：mysan.com

表 *7:* 示例：不同的 *CN* 和 *FQDN* 值

| | 公共名 | unstructuredName | SANS |
|---|---|---|---|
| 自签名 | mywebsite.com | mysan.com | mysan.com |
| CSR | mywebsite.com | mysan.com | - |

### 使用案例 2：FQDN 字段设置为“无”(None)

示例：

- 通用名称 (CN)：mywebsite.com
- FQDN：无

表 *8:* 示例：*FQDN* 字段设置为“无”*(None)*

| | 公共名 | SANS |
|---|---|---|
| 自签名 | 主机名 | - |
| CSR | mywebsite.com | - |

### 使用案例 3：无 FQDN（默认 FQDN）

示例：

- 通用名称 (CN)：mywebsite.com

表 *9:* 示例：无 *FQDN*（默认 *FQDN*）

| | 公共名 | unstructuredName | SANS |
|---|---|---|---|
| 自签名 | mywebsite.com | 主机名 | - |
| CSR | mywebsite.com | 主机名 | 主机名 |

### 使用案例 4：在 FQDN 中指定 IP 地址

示例：

- 通用名称 (CN)：mywebsite.com

- FQDN：4.5.6.7

表 *10:* 示例：在 *FQDN* 中指定 *IP* 地址

| | 公共名 | unstructuredName | SANS |
|---|---|---|---|
| 自签名 | mywebsite.com | 4.5.6.7 | - |
| CSR | mywebsite.com | 4.5.6.7 | 4.5.6.7 |

### 使用案例 5：指定 IP 地址

示例：

- IP 地址：4.5.6.7
- 通用名称 (CN)：mywebsite.com
- FQDN：fqdn.com

表 *11:* 示例：指定 *IP* 地址

| | 公共名 | 非结构化地址 | unstructuredName | SANS |
|---|---|---|---|---|
| 自签名 | mywebsite.com | 4.5.6.7 | fqdn.com | - |
| CSR | mywebsite.com | 4.5.6.7 | fqdn.com | fqdn.com |

### 使用案例 6：选中“序列号”(Serial Number) 复选框

示例：

- 序列号：9AQXMWOKDT9

表 *12:* 示例：选中“*IP* 序列号”*(IP Serial Number)* 复选框

| | serialNumber | SANS |
|---|---|---|
| 自签名 | 9AQXMWOKDT9 | - |
| CSR | 9AQXMWOKDT9 | fqdn.com |

### 使用案例 7：指定邮箱地址

示例：

- EA：abc@xyz.com

表 *13:* 示例：指定邮箱地址

| | unstructedName | emailAddress | SANS |
|---|---|---|---|
| 自签名 | 主机名 | abc@xyz.com | 主机名 |
| CSR | 主机名 | abc@xyz.com | - |

# RA VPN 对象

# 服务对象

### ASA 服务对象

ASA 服务对象、服务组和端口组是包含被视为 IP 协议簇一部分的协议或端口的可重用组件。在服务对象中，可以指定单个协议并将其分配给源端口、目的端口或同时分配给源端口和目的端口。服务组包含许多服务对象，并且可以包含多种协议。

端口组是一种 ASA 服务对象。端口组包含对服务类型（例如 TCP 或 UDP）和端口号或端口号范围进行配对的端口对象。然后，可以将安全策略中的对象用于定义流量匹配条件。例如，您可以在访问控制规则中使用它们来允许流量流向特定范围的 TCP 端口。

有关详细信息，请参阅创建和编辑 ASA 服务对象。

### 协议对象

协议对象是一种包含不太常用或传统协议的服务对象。协议对象由名称和协议编号来标识。CDO 可识别 ASA 和 Firepower（FDM 管理 设备）配置中的这些对象，并为其提供自己的“协议”过滤器，以便您可以轻松找到它们。

### ICMP 对象

互联网控制消息协议 (ICMP) 对象是专门用于 ICMP 和 IPv6-ICMP 消息的服务对象。当 ASA 和 Firepower 配置中的这些设备已载入时，CDO 会识别这些对象，并且 CDO 会为其提供自己的“ICMP”过滤器，以便您轻松找到这些对象。

使用 CDO，您可以从 ASA 配置中重命名或删除 ICMP 对象。您可以使用 CDO 在 Firepower 配置中创建、更新和删除 ICMP 和 ICMPv6 对象。

**Note** 对于 ICMPv6 协议，AWS 不支持选择特定参数。仅支持允许所有 ICMPv6 消息的规则。

相关信息：

- 删除对象, on page 110

# 创建和编辑 ASA 服务对象

在服务对象中，可以指定单个协议并将其分配给源端口、目标端口或同时分配给源端口和目标端口。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击**创建对象 (Create Object)** > **ASA** > **服务 (Service)**。

**步骤 3** 输入对象名称。

**步骤 4** 选择 **创建服务对象**

**步骤 5** 点击**服务类型 (Service Type)** 按钮，然后选择要为其创建对象的协议。

- **对于 TCP、UDP 和 TCP-UDP 服务类型**，请输入源端口和/或目的端口：
  - 源端口标识符允许您匹配源自特定编号端口的流量。在源端口标识符中，选择运算符：等于、范围、小于、大于或不等于，并提供适当的端口号或范围。
  - 目的端口标识符允许您匹配到达特定编号端口的流量。在目的端口标识符中，选择运算符：等于、范围、小于、大于或不等于，并提供适当的端口号或范围。
- **对于协议服务类型**，输入 介于 0 到 255 之间的协议编码，或已知名称，如 ip、tcp、udp、gre 等等。

**步骤 6** 点击**添加 (Add)**。

示例

- 识别传入 FTP 流量的服务对象是 TCP 服务类型和目的端口范围 21。
- 标识传出 DNS 和 DNS over TCP 流量的服务对象是具有 tcp-udb 服务类型且源端口为 53 的服务对象。

## 创建 ASA 服务组

服务组可以由代表一个或多个协议的一个或多个服务对象组成。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击**创建对象 (Create Object)** > **ASA** > **服务 (Service)**。

**步骤 3** 输入对象名称。

**步骤 4** 选择**创建服务组 (Create a service group)**。

**步骤 5** 通过点击**添加对象 (Add Object)**，选择一个对象，然后点击**选择 (Select)**，添加现有对象。重复此步骤以添加更多对象。

**步骤 6** 如果需要，请向服务组添加额外的单个服务类型值

- **对于 TCP、UDP 和 TCP-UDP 服务类型**，请输入源端口和/或目的端口：
  - 源端口标识符允许您匹配源自特定编号端口的流量。在源端口标识符中，选择运算符：等于、范围、小于、大于或不等于，并提供适当的端口号或范围。

- 目的端口标识符允许您匹配到达特定编号端口的流量。在目的端口标识符中，选择运算符：等于、范围、小于、大于或不等于，并提供适当的端口号或范围。

- **对于协议服务类型**，输入 介于 0 到 255 之间的协议编码，或已知名称，如 ip、tcp、udp、gre 等等。

**步骤 7** 要添加更多单个端口值，请点击**添加另一个值 (Add Another Value)** 并重复步骤 6。

**步骤 8** 将服务对象和服务值添加到服务组后，点击**添加 (Add)**。

### 编辑 ASA 服务对象或服务组

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。

**步骤 3** 在详细信息窗格中，点击编辑。

**步骤 4** 以在上述过程中创建值的相同方式编辑对话框中的值。

**步骤 5** 点击**保存 (Save)**。

**步骤 6** CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

# ASA 时间范围对象

### 什么是时间范围对象？

时间范围对象定义了由起始时间、结束时间和可选循环条目组成的特定时间。可以将这些网络中的对象用于对特定功能或资产提供基于时间的访问。例如，可以创建一条仅允许在工作时间内对特定服务器进行访问的访问规则。创建时间范围并不会限制对设备的访问。请注意，为这些对象配置的时间是设备的本地时间。

您可以向此对象添加绝对时间范围或循环时间范围。重复出现的范围被视为定期时间范围。

**Note** 如果为时间范围规定指定了绝对值和周期值，则只有在达到绝对起始时间后才开始评估周期值，而且在绝对结束时间到达后便不再对其进行评估。

## 创建 ASA 时间范围对象

使用以下程序为 ASA 设备创建时间范围对象：

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击蓝色加号按钮 以创建新的对象。

**步骤 3** 点击 **ASA** > **时间范围 (Time Range)**。

**步骤 4** 输入对象名称。

**步骤 5** 定义时间范围。

- 绝对时间范围 - 输入所需时间范围的开始时间和结束时间；您可以选择在几分钟、几小时、几天或几周内执行此对象。一个时间范围对象只能有一个绝对时间范围。
- 周期性时间范围 - 点击以添加将在一周内重复的周期性时间范围。  从下拉菜单中选择**频率 (Frequency)**、时间范围应在**星期几 (Days)**以及**开始 (Start)** 时间和**结束 (End)** 时间。一个时间范围对象可以有多个周期范围。

**Note** 时间范围对象的开始时间和结束时间是可选的。如果对象未建立开始时间，则时间范围会立即生效。如果对象未确定结束时间，则时间范围无限期。

**步骤 6** 点击**添加 (Add)** 以创建对象。

## 编辑 ASA 时间范围对象

使用以下程序编辑 ASA 设备的时间范围对象：

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。

**步骤 3** 在详细信息窗格中，点击编辑。 

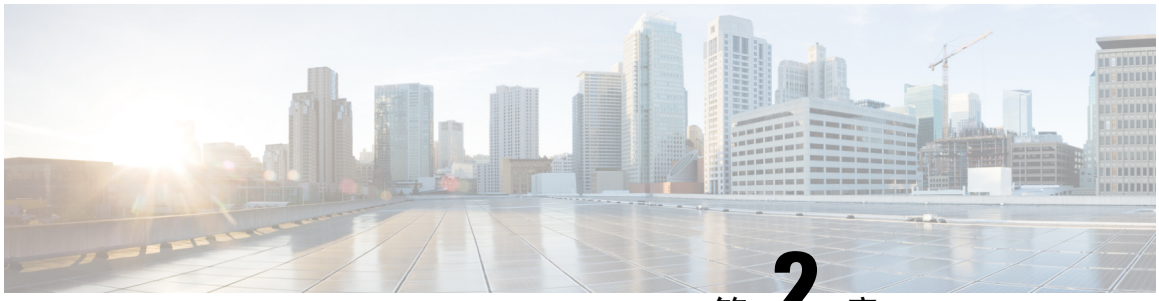
**步骤 4** 根据需要编辑设置，然后点击**保存 (Save)**。

**步骤 5** 如果对象当前由任何策略使用，则 CDO 会显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

**步骤 6** 如果对象被用于设备上的策略，请立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

相关信息：

- 删除对象
- 管理传统 ASA 访问策略



第 2 章

# 载入设备和服务

您可以将实时设备和模型设备载入 CDO。模型设备是您可以使用 CDO 查看和编辑的已上传配置文件。

大多数实时设备和服务都需要开放的 HTTPS 连接，以便安全设备连接器可以将 CDO 连接到设备或服务。

有关 SDC 及其状态的详细信息，请参阅安全设备连接器，第 8 页。

本章涵盖以下部分：



# 将 ASA 设备载入 CDO

使用此程序将单个实时 ASA 设备（而不是 ASA 型号）载入 CDO。如果要一次载入多个 ASA，请参阅批量载入 ASA。

### Before you begin

#### 设备必备条件

- 查看 将 思科防御协调器 连接到托管设备, on page 9。

- 设备必须至少运行版本 8.4+。

**Note** 在版本 9.3(2) 之前，TLS 1.2 不可用于 ASA 管理平面。在版本 9.3(2) 中，需要本地 SDC 才能加入 CDO。

- ASA 的运行配置文件必须小于 4.5 MB。要确认运行配置文件的大小，请参阅确认 ASA 运行配置大小。
- IP 寻址：每个 ASA、ASAv 或 ASA 安全情景必须具有唯一的 IP 地址，并且 SDC 必须在配置为接收管理流量的接口上与其连接。

### 证书必备条件

如果您的 ASA 设备没有兼容的证书，则载入设备可能会失败。确保满足以下要求：

- 设备使用 TLS 版本 1.0 或更高版本。
- 设备提供的证书未过期，并且其颁发日期是过去的日期（即，它已经有效，未计划在以后生效）。
- 证书必须是 SHA-256 证书。不接受 SHA1 证书。
- 以下条件之一成立：
  - 设备使用自签名证书，并且与授权用户信任的最新证书相同。
  - 设备使用受信任证书颁发机构 (CA) 签名的证书，并提供将所提供的枝叶证书链接到相关 CA 的证书链。

如果在载入过程中遇到证书错误，请参阅由于证书错误而无法载入 ASA, on page 477以了解详细信息。

### 开放式 SSL 密码必备条件

如果设备没有兼容的 SSL 密码套件，则设备无法成功与安全设备连接器 (SDC) 通信。使用以下任何密码套件：

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

如果您在 ASA 上使用的密码套件不在此列表中，则 SDC 不支持该密码套件，您需要更新 ASA 的密码套件。

---

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击蓝色加号按钮  以载入 ASA。

**步骤 3** 点击 **ASA** 磁贴。

**步骤 4** 在**查找设备**步骤中，执行以下操作：

**a.** 点击**安全设备连接器 (Secure Device Connector)** 按钮，然后选择网络中安装的安全设备连接器。如果您不想使用 SDC，CDO 可以使用云连接器连接到您的 ASA。您的选择取决于您如何 将 思科防御协调器 连接到托管设备。

**b.** 为设备命名。

**c.** 输入设备或服务的位置（IP 地址、FQDN 或 URL）。默认端口为 443。

**d.** 点击**下一步**。

**步骤 5** 在**凭证 (Credentials)** 步骤中，输入 CDO 将用于连接到设备的 ASA 管理员或类似的最高权限 ASA 用户的用户名和密码，然后点击 **下一步 (Next)**。

**步骤 6** （可选）在完成步骤中，输入设备的标签。您将能够按此标签过滤设备列表。有关详细信息，请参阅CDO 标签和过滤。

**步骤 7** 标记设备或服务后，您可以在**清单 (Inventory)** 列表中查看它。

**Note** 根据配置的大小和其他设备或服务的数量，可能需要一些时间来分析配置。

---

# 将 ASA 设备的高可用性对载入 CDO

载入属于高可用性对的 ASA 时，请使用 将 ASA 设备载入 CDO, on page 135 仅载入该对的主设备。

# 在多情景模式下载入 ASA

## 关于多情景模式

您可以将安装在物理设备上的单个ASA划分为多个逻辑设备（也被称为情景）。在多情景模式下配置的 ASA 中会使用三种配置：

- 安全情景 (Security Context)
- 管理情景
- 系统配置

## 关于安全情景

每个安全情景都可以作为独立设备，拥有自己的安全策略、接口和管理员。多安全情景类似于拥有多台独立设备。安全情景并非安装在私有云基础设施中的虚拟机映像意义上的虚拟 ASA。在硬件设备上安装的 ASA 上配置安全情景。每个情景都会在该设备的物理接口上进行配置。

有关多情景模式的详细信息，请参阅《ASA CLI 和 ASDM 配置指南》。

CDO 会将每个安全情景作为单独的 ASA 来载入，并将其作为单独的 ASA 来管理。

## 关于管理情景

管理情景就像一个安全情景，而不同之处在于，当用户登录到管理情景时，该用户将具有系统管理员权限并可访问系统和所有其他情景。管理情景在任何情况下都不受限制，可用作常规情景。但是，由于登录到管理情景会授予用户针对所有情景的管理员权限，因此可能需要将对管理情景的访问限定于适当的用户。

CDO 会将每个管理情景作为单独的 ASA 来载入，并将其作为单独的 ASA 来管理。在设备上升级 ASA 和 ASDM 软件时，CDO 也会使用管理员情景。

## 关于系统配置

系统管理员通过在系统配置（与单模式配置类似的启动配置）中配置每个情景配置位置、分配的接口以及其他情景运行参数，从而添加并管理情景。系统配置可标识ASA的基本设置。系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。

CDO 不会载入系统配置。

## 安全和管理情景的载入必备条件

载入安全和管理员情景的必备条件与载入任何其他ASA的必备条件相同。有关必备条件的列表，请参阅将 ASA 设备载入 CDO，第 135 页。

要了解哪些思科设备在多情景模式下支持 ASA，请参阅《*CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南*》中适用于您所运行的任何 ASA 软件版本的“多情景模式”一章。

对于作为单情景防火墙运行的ASA和多情景防火墙的管理情景，很多不同的端口号都可以用于ASDM和 CDO 访问。但对于安全情景，ASDM 和 CDO 访问端口会固定为端口 443。这是 ASA 的一项限制。

### 载入 ASA 安全和管理情景

载入安全情景或管理情景的方法与载入任何其他 ASA 的方法相同。有关载入说明，请参阅将 ASA 设备载入 CDO，第 135 页或批量载入 ASA，第 139 页。

### 升级安全情景

CDO将多情景ASA的每个安全和管理情景均视为单独的ASA，并且每个情景都会单独载入。但是，多情景 ASA 的所有安全和管理情景都会运行设备上安装的相同版本的 ASA 软件。

要升级 ASA 安全情景使用的 ASA 和 ASDM 版本，请载入管理情景并在该情景上执行升级。有关详细信息，请参阅在单个 ASA 上升级 ASA 和 ASDM 映像，第 147 页或批量 ASA 和 ASDM 升级，第 143 页 批量 ASA 和 ASDM 升级，第 143 页。

# 批量载入 ASA

Cisco Defense Orchestrator (CDO) 让您能够通过在 .csv 文件中提供所有 ASA 的必要信息来批量载入 ASA。在载入ASA时，您可以使用过滤器窗格来显示哪些载入尝试已加入队列、正在加载、已完成或已失败。

### Before you begin

- 查看 将 思科防御协调器 连接到托管设备, on page 9。
- 准备一个 .csv 文件，其中包含要载入的 ASA 的连接信息。在自己的行中添加有关一个 ASA 的信息。可以在行首使用 # 表示注释。
  - ASA 位置（IP 地址或 FQDN）
  - ASA 管理员用户名
  - ASA 管理员密码
  - （可选）CDO 的设备名称
  - 在 SDCName 字段中，指定网络中要用于将 CDO 连接到 ASA 的安全设备连接器 (SDC) 的名称。如果您不打算使用 SDC 将 ASA 连接到 CDO，也可以输入“无”。在载入设备时，如果在 SDCName 字段中指定“none”，则会使用云连接器来载入 ASA。云连接器允许您将设备连接到 CDO，而无需安装 SDC。您的选择取决于您如何将 思科防御协调器 连接到托管设备。
  - （可选）CDO 的设备标签
  - 要添加一个标签，请将标签名称添加到最后一个 CSV 字段。
  - 要向设备添加多个标签，请用引号将值引起来。例如，`alpha、beta、Gamma。`

- 要添加类别和选项标签，请使用冒号 (:) 分隔两个值。例如，`Rack:50`。

配置文件示例：

```
#Location,Username,Password,DeviceName,SDCName,DeviceLabel
192.168.3.2,admin,CDO123!,ASA3,sdc1,"HA-1,Rack:50"
192.168.4.2,admin,CDO123!,ASA4,sdc1,"HA-1,Rack:50"
ASA2.example.com,admin,CDO123!,ASA2,none,Rack:51
asav.virtual.io,admin,CDO123!,ASA-virtual,sdc3,Test
```

**Caution** CDO 不会验证 .csv 文件中的任何数据。您需要确保条目的准确性。

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击蓝色加号按钮 以载入 ASA。

**步骤 3** 在“载入”(Onboarding) 页面上，点击**多个 ASA (Multiple ASAs)** 磁贴。

**步骤 4** 点击**浏览 (Browse)** 以找到包含 ASA 条目的 .csv 文件。您指定的设备现在已在 ASA 批量载入表中排队准备载入。

**Caution** 在载入过程完成之前，请勿离开“ASA 批量载入”(ASA Bulk Onboarding) 页面。离开会停止载入过程。

**步骤 5** 点击**开始**。您将在“ASA 批量载入”(ASA Bulk Onboarding) 表的状态列中看到载入过程的进度。设备成功载入后，您会看到其状态更改为“完成”(Complete)。

### What to do next

如果您需要暂停批量载入并稍后恢复，请参阅暂停和恢复批量载入, on page 140

。

# 暂停和恢复批量载入

如果您需要暂停载入过程，请点击**暂停 (Pause)**。CDO 完成其已开始载入的任何设备的载入。要恢复批量载入过程，请点击**开始 (Start)**。CDO 将开始载入下一个排队的设备。

如果您点击**暂停 (Pause)** 并离开此页面，则需要返回到该页面并从头开始再次执行批量载入程序。但是，CDO 会识别其已载入的设备，将此次新的载入尝试中的设备标记为重复设备，并快速浏览列表以载入排队的设备。

# 创建和导入 ASA 模型

**步骤 1** 在导航栏中，点击 **设备和服务**。
**步骤 2** 点击**设备**选项卡。
**步骤 3** 点击 **ASA** 选项卡。
**步骤 4** 选择 ASA 设备，然后在左侧窗格的**管理**中，点击**配置**。
**步骤 5** 点击**下载**，将设备配置下载到本地计算机。

# 导入 ASA 配置

**注意**：载入的 ASA 运行配置文件必须小于 4.5 MB。在载入之前，请确认配置文件的大小。

**步骤 1** 在导航栏中，点击 **设备和服务**。
**步骤 2** 点击蓝色加号 (  ) 按钮以导入配置。
**步骤 3** 点击**导入配置以进行离线管理 (Import configuration for offline management)**。
**步骤 4** 选择 **ASA** 作为**设备类型 (Device Type)**。
**步骤 5** 点击**浏览 (Browse)** 并选择要上传的配置文件（文本格式）。
**步骤 6** 验证配置后，系统会提示您为设备或服务添加标签。有关详细信息，请参阅CDO 标签和过滤。
**步骤 7** 标记型号设备后，您可以在**设备和服务 (Devices & Services)** 列表中查看它。

**Note** 根据配置的大小和其他设备或服务的数量，可能需要一些时间来分析配置。

# 从CDO删除设备

使用以下程序可从 中删除设备：CDO

**步骤 1** 登录至 CDO。
**步骤 2** 导航至**清单 (Inventory)** 页面。
**步骤 3** 找到要删除的设备，然后选中设备行中的设备以将其选中。
**步骤 4** 在右侧的“设备操作”(Device Actions) 面板中，选择**删除 (Remove)**。
**步骤 5** 出现提示时，选择**确定 (OK)** 以确认删除所选设备。选择**取消 (Cancel)** 以使设备保持已载入状态。

# 导入设备的配置以进行离线管理

通过导入设备的配置以进行离线管理，您可以查看和优化设备的配置，而无需在网络中的实时设备上进行操作。CDO 还将这些上传的配置文件称为“模型”。

您可以将这些设备的配置导入到 CDO：

- 自适应安全设备 (ASA)。请参阅创建和导入 ASA 模型。
- Firepower 威胁防御 (FTD)。
- 像汇聚服务路由器 (ASR) 和集成服务路由器 (ISR) 的 Cisco IOS 设备。

# ASA 和 ASDM 升级必备条件

Cisco Defense Orchestrator (CDO) 提供的向导可帮助您升级单个 ASA、多个 ASA、主用-备用配置中的 ASA 以及在单情景或多情景模式下运行的 ASA 上安装的 ASA 和 ASDM 映像。

CDO 维护您可以升级到的 ASA 和 ASDM 映像存储库。当您从 CDO 的映像存储库中选择升级映像时，CDO 会在后台执行所有必要的升级步骤。该向导将指导您选择兼容的 ASA 软件和 ASDM 映像，安装这些映像并重新启动设备以完成升级。我们会验证您在CDO上选择的映像是否是复制到并安装在 ASA 上的映像，从而确保升级过程的安全。CDO 会定期查看其 ASA 二进制文件清单，并在最新的 ASA 和 ASDM 映像可用时将其添加到其存储库中。对于 ASA 具有互联网出站访问权限的客户，这是最佳选择。

CDO 的映像存储库仅包含正式发布 (GA) 映像。如果您在列表中没有看到特定的 GA 映像，请联系思科 TAC 或从**联系支持人员 (Contact Support)** 页面发送邮件支持。我们将使用已建立的支持请求 SLA 处理请求，并上传缺少的 GA 映像。

如果您的 ASA 没有互联网出站访问权限，您可以从 Cisco.com 下载所需的 ASA 和 ASDM 映像，将其存储在您自己的存储库中，为升级向导提供这些映像的自定义 URL，然后 CDO 执行升级使用这些图像。但是，在这种情况下，您需要确定要升级到的映像。CDO 不执行映像完整性检查或磁盘空间检查。您可以使用以下任何协议从存储库检索映像：FTP、TFTP、HTTP、HTTPS、SCP 和 SMB。

### 所有 ASA 的配置前提条件

- 需要在 ASA 上启用 DNS。
- 如果您使用 CDO 的映像存储库中的升级映像，ASA 应该能够访问互联网。
- 确保 ASA 和存储库 FQDN 之间是 HTTPS 连接。
- ASA 已成功载入 CDO。
- ASA 已同步到 CDO。
- ASA 在线。
- 对于自定义 URL 升级：

- 使用思科 ASA 升级指南确定与您的 ASA 兼容的 ASA 和 ASDM 版本。
- 将 ASA 和 ASDM 映像下载到映像存储库。
- 确保 ASA 有权访问您的映像存储库。
- 确保 ASA 上有足够的磁盘空间用于 ASA 和 ASDM 映像。
- 有关 URL 语法信息，请参阅使用您自己的映像升级 ASA 或 ASDM。

### Firepower 1000 和 Firepower 2100 系列设备的配置前提条件

- 必须为**设备**模式配置 Firepower 2100 系列设备的 FXOS 模式。有关详细信息，请参阅将 Firepower 2100 设置为设备或平台模式。
- 设备必须运行 ASA 版本 9.13(1) 或更高版本。
- 在升级 ASA 软件之前，必须先升级 FXOS 捆绑包。有关详细信息，请参阅 Firepower 2100 ASA 和 FXOS 兼容性。

### 运行 ASA 的 Firepower 4100 和 Firepower 9300 系列设备

CDO 不支持 Firepower 4100 或 Firepower 9300 系列设备的升级。您必须在 CDO 之外升级这些设备。

### 升级指南

- CDO 可以升级配置为主用/备用“故障转移”对的 ASA。CDO 无法升级主用/主用“集群”对中配置的 ASA。

### 软件和硬件必备条件

可从中升级的最低 ASA 和 ASDM 版本：

- ASA：ASA 9.1.2
- ASDM：没有最低版本要求。

支持的硬件版本

- 请参阅CDO 支持的软件和硬件。

# 批量 ASA 和 ASDM 升级

**步骤 1** 查看 ASA 和 ASDM 升级必备条件，了解升级要求以及有关升级 ASA 和 ASDM 映像的重要信息。

**Note** 如果要升级 ASA 1000 或 2000 系列设备，请务必阅读 ASA 和 ASDM 升级必备条件。

**步骤 2** （可选）在导航栏中，点击**设备和服务 (Devices & Services)**，创建更改请求管理以在更改日志中标识通过此操作升级的设备。

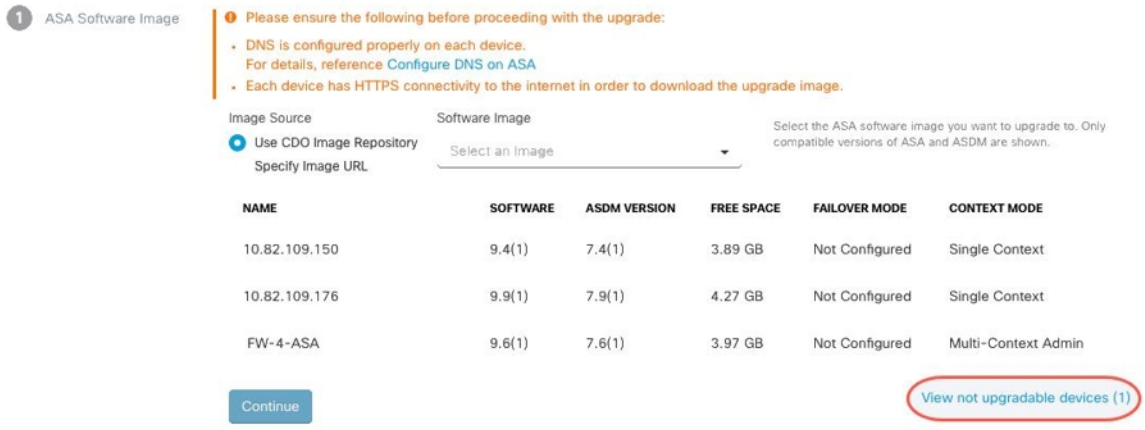
**步骤 3** 点击**设备**选项卡。

**步骤 4** 使用过滤器缩小可能要包含在批量升级中的设备列表。

**步骤 5** 从过滤后的设备列表中，选择要升级的设备。

**步骤 6** 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

**步骤 7** 在“批量设备升级”(Bulk Device Upgrade) 页面上，您会看到可升级的设备。如果您选择的任何设备不可升级，CDO 会为您提供一个链接，供您查看不可升级的设备。




**步骤 8** 在步骤 1 中，点击**使用 CDO 映像存储库 (Use CDO Image Repository)** 以选择要升级到的 ASA 软件映像，然后点击**继续 (Continue)**。

该列表指示您选择的多少个 ASA 可以升级到您选择的软件版本。在下面的示例中，所有设备都可以升级到版本 9.9(1.2)，两台设备可以升级到 9.8(2)，其中一台设备可以升级到 9.6(1)。


如果您选择的任何软件版本与您选择的任何设备不兼容，CDO 会向您发出警报。在下面的示例中，CDO 无法将 10.82.109.176 设备升级到其运行之前的版本。

| NAME | SOFTWARE | ASDM VERSION | FREE SPACE | FAILOVER MODE | CONTEXT MODE |
|---|---|---|---|---|---|
| ✔ 10.82.109.150 | 9.4(1) | 7.4(1) | 3.89 GB | Not Configured | Single Context |
| ✔ FW-4-ASA | 9.6(1) | 7.6(1) | 3.97 GB | Not Configured | Multi-Context Admin |
| ✖ 10.82.109.176 | 9.9(1) | 7.9(1) | 4.27 GB | Not Configured | Single Context |

**步骤 9** 在步骤 2 中，选择要升级到的 ASDM 映像。系统只会显示与您可以升级的 ASA 兼容的 ASDM 选项。

**步骤 10** 在步骤 3 中，确认您的选择，并决定是仅将映像下载到 ASA，还是复制映像、安装并重新启动设备。

**步骤 11** 准备就绪后，点击**执行升级 (Perform Upgrade)**。

**Note** 如果升级失败，CDO 会显示一条消息。升级失败的原因通常是阻止 ASA 和 ASDM 映像传输到 ASA 的网络问题。

**步骤 12** 或者，如果您希望 CDO 稍后执行升级，请选中计划升级复选框。点击该字段可选择未来的日期和时间。完成后，点击“计划升级”(Schedule Upgrade) 按钮。

**步骤 13** （对于多情景模式）在管理情景和安全情景启动后，您可能会看到安全情景显示消息“检测到新证书”(New certificate detected)。如果您看到该消息，请接受所有安全情景的证书。接受升级导致的任何其他更改。

**步骤 14** 查看作业页面，了解批量升级操作的进度。如果您想了解有关批量升级作业中操作成功与否的详细信息，请点击蓝色查看链接，系统会将您定向到作业页面。

**步骤 15** 如果您创建并激活了更改请求标签，请记住将其清除，以免无意中将其他配置更改与此事件关联。

# 使用您自己的存储库中的映像升级多个 ASA

**步骤 1** 查看 ASA 和 ASDM 升级必备条件 ，了解升级要求以及有关升级 ASA 和 ASDM 映像的重要信息。

**步骤 2** （可选）在**设备和服务 (Devices & Services)** 页面中，创建一个更改请求管理以在更改日志中标识通过此操作升级的设备。

**步骤 3** 点击**设备**选项卡。

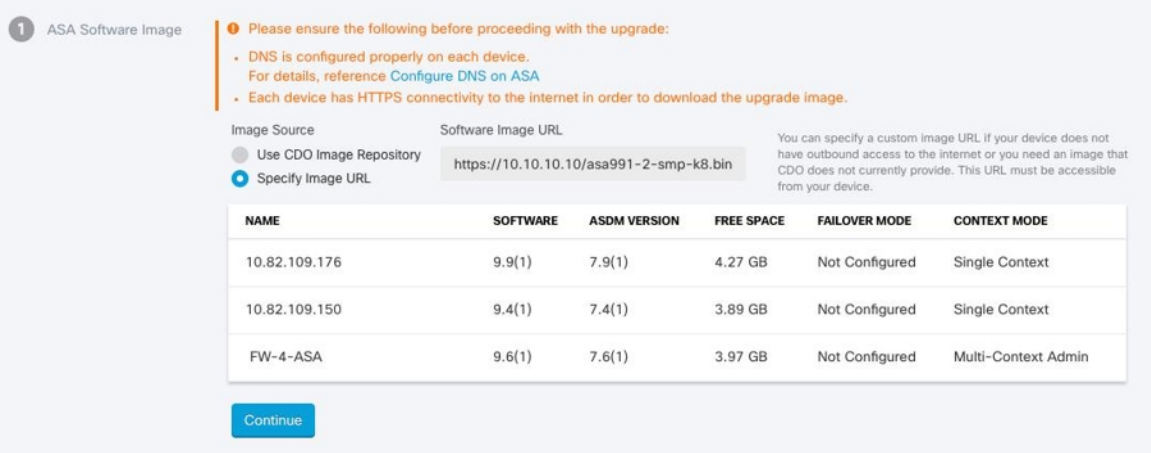
**步骤 4** 使用 过滤器, on page 79 来缩小可能要包含在批量升级中的设备列表。

**步骤 5** 从过滤后的设备列表中，选择要升级的设备。

**步骤 6** 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

**步骤 7** 在步骤 1 中，点击**指定映像 URL (Specify Image URL)**，在**软件映像 URL (Software Image URL)** 字段中输入要升级到的 ASA 映像的 URL， 然后点击**继续 (Continue)**。有关 URL 语法信息，请参阅使用您自己的映像升级 ASA 或 ASDM。

**Note** 下图显示了软件映像URL字段中的HTTPS URL。您可以使用以下任何协议从存储库检索映像：FTP、TFTP、HTTP、HTTPS、SCP 和 SMB。有关 URL 语法信息，请参阅使用您自己的映像升级 ASA 或 ASDM。




**步骤 8** 在步骤 2 中，点击**指定映像 URL (Specify Image URL)**，在**软件映像 URL (Software Image URL)** 字段中输入要升级到的 ASDM 映像的 URL， 然后点击**继续 (Continue)**。

**步骤 9** 在步骤 3 中，确认您的选择，并决定是仅将映像下载到 ASA，还是复制映像、安装并重新启动设备。

**步骤 10** 准备就绪后，点击**执行升级 (Perform Upgrade)**。

**Note** 如果升级失败，CDO 会显示一条消息。升级失败的原因通常是阻止 ASA 和 ASDM 映像传输到 ASA 的网络问题。

**步骤 11** 或者，如果您希望 CDO 稍后执行升级，请选中计划升级复选框。点击该字段可选择未来的日期和时间。完成后，点击“计划升级”(Schedule Upgrade) 按钮。

**步骤 12** （对于多情景模式）在管理情景和安全情景启动后，您可能会看到安全情景显示消息“检测到新证书”(New certificate detected)。如果您看到该消息，请接受所有安全情景的证书。接受升级导致的任何其他更改。

**步骤 13** 查看作业页面，了解批量升级操作的进度。如果您想了解有关批量升级作业中操作成功与否的详细信息，请点击蓝色查看链接，系统会将您定向到作业页面。

**步骤 14** 如果您创建并激活了更改请求标签，请记住将其清除，以免无意中将其他配置更改与此事件关联。

### What to do next

**升级说明**

- 您还可以通过打开设备和服务页面并查看表中的配置状态列来监控批量升级的进度。
- 您可以通过在设备和服务页面上选择该设备并点击升级按钮来查看批量升级中包含的单个设备的进度。CDO 会将您引导至该设备的“设备升级”页面。

# 在单个 ASA 上升级 ASA 和 ASDM 映像

按照此程序在单个 ASA 上升级 ASA 和 ASDM 映像。

**步骤 1** 查看 ASA 和 ASDM 升级必备条件，了解升级要求以及有关升级 ASA 和 ASDM 映像的重要信息。

**Note** 如果要升级 ASA 1000 或 2000 系列设备，请务必阅读 ASA 和 ASDM 升级必备条件。

**步骤 2** 在导航栏中，点击 **设备和服务**。

**步骤 3** 点击**设备**选项卡。

**步骤 4** （可选）创建更改请求管理，以便在更改日志中标识通过此操作升级的设备。

**步骤 5** 选择想要升级的设备。

**步骤 6** 在 **设备操作** 窗格中，点击 **升级**。

**步骤 7** 在设备升级页面上，按照向导提供的说明进行操作。

**a.** 在步骤 1 中，点击 **使用 CDO 映像存储库** 以选择要升级到的 ASA 软件映像，然后点击 **继续**。

**Note** 将 ASA 和 ASDM 升级到您自己的存储库中存储的映像时，请选择**指定映像 URL (Specify Image URL)**，然后在软件映像 URL 字段中输入 ASA 或 ASDM 映像的 URL。您可以使用以下任何协议从存储库检索映像：FTP、TFTP、HTTP、HTTPS、SCP 和 SMB。有关 URL 语法信息，请参阅使用您自己的映像升级 ASA 或 ASDM。

（可选）如果您希望 CDO 稍后执行升级，请选中计划升级复选框。点击该字段可选择未来的日期和时间。完成后，点击**计划升级 (Schedule Upgrade)**。

**b.** 在步骤 2 中，选择要升级到的 ASDM 映像。系统只会显示与您可以升级的 ASA 兼容的 ASDM 选项。

**c.** 在步骤 3 中，确认您的选择，并决定是仅将映像下载到 ASA，还是复制映像、安装并重新启动设备。

**步骤 8** 准备就绪后，点击**执行升级 (Perform Upgrade)**。

**步骤 9** （对于多情景模式）在管理情景和安全情景启动后，您可能会看到安全情景显示消息“检测到新证书”(New certificate detected)。如果您看到该消息，请接受所有安全情景的证书。接受升级导致的任何其他更改。想要观看演示？观看此程序的截屏视频！

### What to do next

升级说明

- 如果您选择了要升级到的映像，并且您改变了主意，请选中与该软件映像关联的**跳过升级 (Skip Upgrade)** 复选框。映像不会复制到设备，也不会使用映像升级设备。
- 在**执行升级**步骤中，如果您选择仅将映像复制到 ASA，则可以稍后返回到“设备升级”(Device Upgrade) 页面，然后点击“立即升级”(Upgrade Now) 以执行升级。复制任务完成后，您将在“设备和服务”(Devices & Services) 页面上看到该设备的消息“准备升级”(Ready to Upgrade)。

- 在复制映像、安装映像和重新启动设备的过程中，您无法对设备执行操作。正在安装映像然后重新启动的设备在“设备和服务”(Devices & Services) 页面中显示为“正在升级”(Upgrading)。
- 在升级过程中，您无法对设备执行操作；也就是说，安装映像并重新启动设备。
- 如果您选择仅将映像复制到设备，则可以在设备上执行操作。正在复制映像的设备在“设备和服务”页面中显示为“正在复制映像”。
- 升级具有自签名证书的设备可能会遇到问题；有关详细信息，请参阅新证书问题故障排除。

# 升级高可用性对中的 ASA 和 ASDM 映像

在主用/备用故障切换模式下升级 ASA 对之前，请查看以下前提条件。如果您需要有关如何配置 ASA 以及如何在故障切换模式下工作的详细信息，请参阅 ASA 文档中的故障切换以实现高可用性。

想要观看演示？观看此程序的截屏视频。

### 前提条件

- 查看 ASA 和 ASDM 升级必备条件，了解要求以及有关升级 ASA 和 ASDM 映像的重要信息。
- 在主用/备用故障切换模式下配置主（主用）和辅助（备用）ASA。
- 主 ASA 是主用/备用对中的主用设备。如果主 ASA 处于非活动状态，CDO 将不会执行升级。
- 主要和辅助 ASA 软件版本相同。

## 工作流程

CDO 升级主用/备用 ASA 对的过程如下：

**步骤 1** CDO 将 ASA 和 ASDM 映像下载到两个 ASA。

**Note** 用户可以选择下载 ASA 和 ASDM 映像，但不能立即升级。如果之前已下载 ASA 和 ASDM 映像，则 CDO 不会再次下载； CDO 继续执行下一步的升级工作流程。

**步骤 2** CDO 首先升级辅助 ASA。

**步骤 3** 升级完成且辅助 ASA 恢复为“备用就绪”状态后，CDO 将启动故障切换，以便辅助 ASA 成为主用 ASA。

**步骤 4** CDO 升级主 ASA，即当前的备用 ASA。

**步骤 5** 一旦主 ASA 恢复为“备用就绪”状态，CDO 将启动故障切换，以便主 ASA 成为主用 ASA。

**Warning** 升级具有自签名证书的设备可能会遇到问题；有关详细信息，请参阅新证书问题故障排除。

# 升级主用/备用对中的 ASA 和 ASDM 映像

**步骤 1** 登录 CDO。

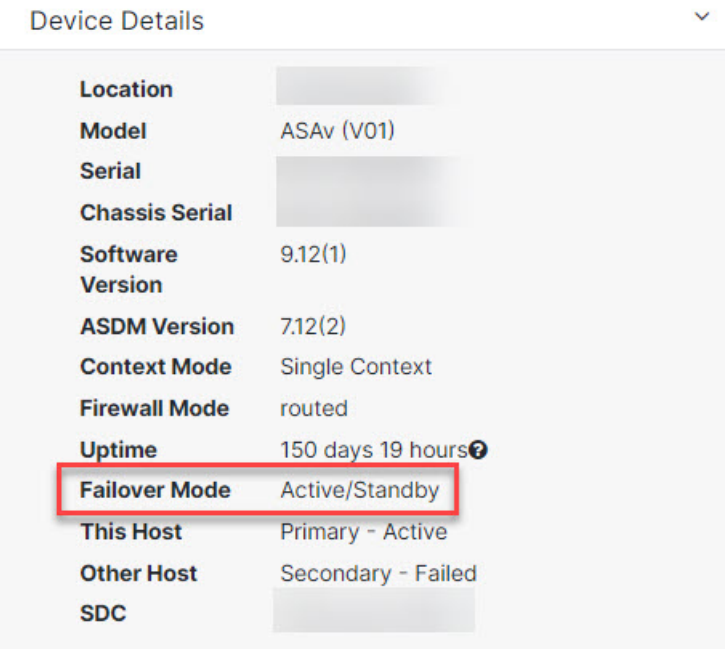
**步骤 2** 点击**清单 (Inventory)**。

**步骤 3** 点击**设备**选项卡。

**步骤 4** 选择想要升级的设备。

**步骤 5** 在 **设备操作** 窗格中，点击 **升级**。

请注意，设备的故障切换模式为“主用/备用”：




**步骤 6** 在设备升级页面上，按照向导提供的说明进行操作。

**Note** 将 ASA 和 ASDM 升级到您自己的存储库中存储的映像时，请选择**指定映像 URL (Specify Image URL)**，然后在软件映像 URL 字段中输入 ASA 或 ASDM 映像的 URL。您可以使用以下任何协议从存储库检索映像：FTP、TFTP、HTTP、HTTPS、SCP 和 SMB。有关 URL 语法信息，请参阅使用您自己的映像升级 ASA 或 ASDM。

# 使用您自己的映像升级 ASA 或 ASDM

使用新的 ASA 软件和 ASDM 映像升级 ASA 时，可以使用 Cisco Defense Orchestrator (CDO) 存储在其映像存储库中的映像，也可以使用存储在自己的映像存储库中的映像。如果您的ASA没有互联网出站访问权限，维护您自己的映像存储库是使用 CDO 升级 ASA 的最佳选择。

CDO 使用 ASA 的复制命令检索映像并将其复制到 ASA 的闪存驱动器 (disk0:/)。在指定映像 URL 字段中，您需要提供复制命令的 URL 部分。例如，如果整个复制命令是：

```
ciscoasa# copy ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin disk:/0
```

您将提供：

```
ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin
```

在指定映像 URL 字段中。

CDO 支持检索升级映像的 http、https、ftp、tftp、smb 和 scp 方法。

### URL 语法示例

以下是 ASA 复制命令的 URL 语法示例。对于这些 URL 示例，假设如下：

- **映像存储库地址**：10.10.10.10
- **访问映像存储库的用户名**：admin
- **密码**：adminpass
- **路径**：images/asa
- **映像文件名**：asa991-smp-k8.bin

**http**[**s**]**://** [[ *user* [ : *password* ] **@** ] *server* [ : *port* ] **/** [ *path* **/** ] *filename* ]

```
https://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin
HTTP[s] example without a username and password:
https://10.10.10.10:8080/images/asa/asa991-smp-k8.bin
```

ftp://[[**user**[:**password**]@]**server**[:*port*]/[**path**/]**filename**[;*type*=**xx**]] - *type*可以是这些关键字的其中一个：**ap**（ASCII 被动模式）、**an**（ASCII 正常模式）、**ip**（默认 - 二进制被动模式）、**in**（二进制正常模式）。

```
ftp://admin:adminpass@10.10.10.10:20/images/asa/asa991-smp-k8.bin
FTP example without a username and password:
ftp://10.10.10.10:20/images/asa/asa991-smp-k8.bin
```

**tftp://** [[ *user* [ : *password* ] **@** ] *server* [ : *port* ] **/** [ *path* **/** ] *filename* [ **;int=** *interface_name* ]]

```
tftp://admin:adminpass@10.10.10.10/images/asa/asa991-smp-k8.bin outside
TFTP example without a username and password:
tftp://10.10.10.10/images/asa/asa991-smp-k8.bin outside
```

**Note** 路径名不能包含空格。如果路径名有空格，则在 **tftp-server** 命令而不是 **复制 tftp** 命令中设置路径。**;int=** *interface* 选项会绕过路由查找并始终使用指定接口来访问 TFTP 服务器。

smb:/[[**path**/]***filename***] - 指示 UNIX 服务器本地文件系统。

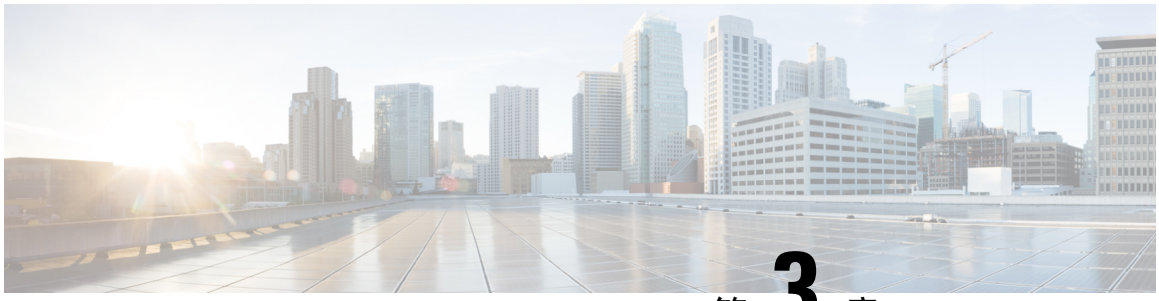
```
smb:/images/asa/asa991-smp-k8.bin
```

[[**user**[:*password*]@] **server**[/*path*]/**filename**[;*int*=**interface_*name*]]- ***;int=****interface*选项会绕过路由查找并始终使用指定接口来访问安全复制 (SCP) 服务器。

```
 scp://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
SCP example without a username and password:
scp://10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
```

思科 ASA 系列命令参考，A-H 命令指南中包含了 URL 语法的完整 copy 命令。

有关使用自定义 URL 升级 ASA 和 ASDM 映像的详细信息，请参阅 ASA 和 ASDM 升级必备条件。



第 3 章

# 配置 ASA 设备

本章涵盖以下部分：

# 更新 ASA 连接凭证

在载入 ASA 的过程中，您输入了 CDO 必须用于连接到设备的用户名和密码。如果这些凭证在设备上发生更改，请使用更新凭证设备操作在 CDO 上更新这些凭证。此功能允许您更新 CDO 上的凭证，而无需重新载入设备。切换到的用户名和密码组合必须已存在于该用户的 ASA 或身份验证、授权和审计 (AAA) 服务器上。此过程仅影响 Cisco Defense Orchestrator 数据库；使用更新凭证功能时，不会对 ASA 配置进行任何更改。

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备 (Devices)** 选项卡，然后点击 **ASA**。

**步骤 3** 选择要更新其连接凭证的 ASA。您可以一次更新一个或多个 ASA 上的凭证。

**步骤 4** 在**设备操作 (Device Actions)** 窗格中，点击**更新凭证 (Update Credentials)**。

**步骤 5** 选择用于将 ASA 连接到 CDO 的云连接器或安全设备连接器 (SDC)。

**步骤 6** 输入要用于连接到 ASA 的新用户名和密码。

**步骤 7** 凭证更改后，CDO 会同步设备。

注释 如果 CDO 无法同步设备，CDO 中的连接状态可能会显示“无效凭证”(Invalid Credentials)。如果是这种情况，您可能尝试使用无效的用户名和密码组合。请确保要使用的凭证已存储在 ASA 或 AAA 服务器上，然后重试。

# 将 ASA 从一个 SDC 移至另一个 SDC

CDO 支持每个租户使用多个 SDC。在单个 CDO 租户上使用多个 SDC，第 27 页您可以使用以下程序将受管 ASA 从一个 SDC 移至另一个 SDC：

**步骤 1** 在 CDO 菜单栏中，点击**清单 (Inventory)**。

**步骤 2** 选择要移动到其他 SDC 的 ASA。

**步骤 3** 在“设备操作”(Device Actions) 窗格中，点击**更新凭证 (Update Credentials)**。

**步骤 4** 点击 Secure Device Connector 按钮，然后选择要将设备移动到的 SDC。

**步骤 5** 输入用于载入 ASA 的管理员用户名和密码，然后点击更新。您不必将这些更改部署到设备。

# ASA 接口配置

Cisco Defense Orchestrator (CDO) 通过提供无需使用命令行界面的用户友好界面来简化 ASA 接口配置。您可以完全控制 ASA 的物理接口、子接口和 EtherChannel 的配置。此外，您还可以查看在基于路由的站点间 VPN 期间创建的虚拟隧道接口，但它们是只读的。您可以使用 CDO 来配置和编辑 ASA 设备上的数据接口或管理/诊断接口。

将电缆（以物理方式或虚拟方式）连接到接口接头时，您需要配置该接口。至少需要命名并启用该接口，流量才会通过该接口。如果该接口是网桥组的成员，则只用为接口命名。如果接口是桥接虚拟接口 (BVI)，则需要为 BVI 分配一个 IP 地址。如果要在特定端口上创建 VLAN 子接口（而非单一物理接口），通常要在该子接口（而不是物理接口）上配置 IP 地址。通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。

接口列表将显示可用的接口及其名称、地址和状态。您可以通过选择接口行并点击“操作”(Actions) 窗格中的**编辑 (Edit)** 来更改接口的状态（打开或关闭）或编辑接口。列表将基于您的配置显示接口特征。展开接口行以查看子接口或桥接组成员。

### 管理接口

可以通过连接至以下接口来管理 ASA：

- 任何直通流量接口
- 专用的管理插槽/端口接口（如果适用于所用的型号）

### 使用 MTU 设置

MTU 会指定设备可在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

### 虚拟隧道接口 (VTI) 的只读支持

在两台 ASA 设备之间配置基于路由的站点间 VPN 隧道会在设备之间创建虚拟隧道接口 (VTI)。已配置 VTI 隧道的设备可以载入 CDO，CDO 会在 **ASA 接口 (ASA Interfaces)** 页面上发现并列出这些隧道，但不支持对其进行管理

# 配置 ASA 物理接口

**步骤 1** 在 CDO 导航窗格，点击**清单 (Inventory)**。

**步骤 2** 点击 **ASA** 选项卡。

**步骤 3** 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

**步骤 4** 点击要配置的物理接口，然后点击 **Edit**。

系统将显示**编辑物理接口 (Editing Physical Interface)** 对话框。

**步骤 5** 在**逻辑名称 (Logical Name)** 字段中，输入接口名称。

**步骤 6** 继续执行以下程序之一：

- 如果要为物理接口分配 IPv4 地址，请为 ASA 物理接口配置 IPv4 地址。
- 为 ASA 物理接口配置 IPv6 地址，第 157 页 如果打算为该接口分配 IPv6 地址。
- 配置高级 ASA 物理接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了接口并且不想继续使用高级接口选项，请继续启用 ASA 物理接口。

## 为 ASA 物理接口配置 IPv4 地址

**步骤 1** 在**编辑物理接口 (Edit Physical Interface)** 对话框中，在 **IPv4 地址 (IPv4 Address)** 选项卡中配置以下内容：

- **类型 (Type)**：您可以为接口使用静态 IP 寻址或 DHCP。

  **静态 (Static)** - 如果希望分配固定的地址，请选择此选项。

  - **IP 地址和子网掩码 (IP Address and Subnet Mask)**：对于连接到接口的网络，键入接口的 IP 地址和子网掩码。

- **备用 IP 地址 (Standby IP Address)**：如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IP 地址。备用设备上的此接口使用备用地址。

  为每个接口设置一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。

**DHCP**：如果应从网络中的 DHCP 服务器获取地址，请选择此选项。

您可以选中**获取默认路由 (Obtain Default Route)** 复选框以便从 DHCP 服务器获取默认路由。您通常都要选中此选项。

**步骤 2** 完成后点击**保存 (Save)**，或者继续执行其中一个程序。

- 为 ASA 物理接口配置 IPv6 地址，第 157 页 如果打算为该接口分配 IPv6 地址。
- 配置高级 ASA 物理接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了接口并且不想继续使用高级接口选项，请继续启用 ASA 物理接口。

## 为 ASA 物理接口配置 IPv6 地址

**步骤 1** 在**编辑物理接口 (Editing Physical Interface)** 对话框中，点击 **IPv6 地址 (IPv6 Address)** 选项卡。

**步骤 2** 进行以下配置：

- **状态 (State)** - 在您未配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请点击**状态 (State)** 滑块将其启用。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  **注释** 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置**：

  选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

  虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

- **抑制 RA (Suppress RA)**：如果要抑制路由器通告，请选中此复选框。设备可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

  也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

  对于不希望设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

- **DAD 尝试 (DAD Attempts)**：接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD会验证新单播IPv6地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。
- **本地链路地址 (Link-Local Address)**：如果要仅将地址用作链路本地地址，请在链路本地地址字段中输入该地址。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

  **注释** 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用链路本地地址 (Standby Link-Local Address)**：如果接口连接高可用性设备，请配置此地址。输入此接口所连接的另一台设备上的接口本地链路地址。
- **静态地址/前缀 (Static Address/Prefix)**：如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。您可以添加另一个静态地址。
- **备用 IP 地址 (Standby IP Address)**： 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

**步骤 3** 完成后点击**保存 (Save)**，或者继续执行其中一个程序。

- 配置高级 ASA 物理接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了接口并且不想继续使用高级接口选项，请继续启用 ASA 物理接口。

## 配置高级 ASA 物理接口选项

高级接口选项的默认设置适用于大多数网络。只有在需要解决网络问题时，再配置它们。

以下步骤程序假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

此程序及其中的所有步骤都是可选的。

**步骤 1** 在**编辑物理接口 (Editing Physical Interface)** 对话框中，点击**高级 (Advanced)** 选项卡。

**步骤 2** 配置以下高级设置：

- **HA 监控 (HA Monitoring)**：启用后，可在当 HA 对决定是否在高可用性配置中故障转移到对等设备时考虑接口的运行状况。如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。
- **仅管理 (Management Only)**：启用后，可进行数据接口管理。

  仅管理接口不允许直通流量，所以将数据接口设置为**仅管理 (Management Only)** 接口的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

- **MTU**：默认 MTU 为 1500 字节。您可以指定 64 - 9198 之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。
- **复用和速度 (Mbps) (Duplex and Speed [Mbps])**：默认设置为该接口与线路另一端的接口协商最佳复用和速度，但如有必要，您可以强制实施特定的复用或速度。所列的选项仅为接口支持的设置。在网络模块上设置这些选项之前，请阅读接口配置限制。
  - **复用 (Duplex)** - 选择“自动”(Auto)、“半”(Half) 或“全”(Full)。当接口支持时，自动为默认值。
  - **速度 (Speed)** - 选择自动可使接口协商速度（默认值）或选取特定速度：10 Mbps、100 Mbps、1000 Mbps、10000 Mbps。此外，您还可以选择以下特殊选项：
- **DAD 尝试 (DAD Attempts)**：接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。
- **MAC 地址 (MAC Address)**：采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
- **备用 MAC 地址 (Standby MAC Address)**：用于高可用性。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

**步骤 3** 如果您保存了接口并且不想继续使用高级接口选项，请继续启用 ASA 物理接口。

**步骤 4** 点击**保存 (Save)**。

## 启用 ASA 物理接口

**步骤 1** 选择要启用的物理接口。

**步骤 2** 移动与接口逻辑名称关联的窗口右上角的**状态 (State)** 滑块。

**步骤 3** 预览和部署所有设备的配置更改所做的更改。

# 添加 ASA VLAN 子接口

通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或设备。

如果您将物理接口连接到交换机的中继端口，请创建子接口。为交换机中继端口上显示的每个VLAN创建子接口。如果您将物理接口连接到交换机的接入端口，创建子接口将没有意义。

- 配置 ASA VLAN 子接口

为 ASA 子接口配置 IPv4 地址，第 160 页
- 为 ASA 子接口配置 IPv6 地址，第 161 页
- 配置高级 ASA 子接口选项，第 162 页
- 启用子接口，第 163 页

## 配置 ASA VLAN 子接口

**步骤 1** 在 CDO 导航窗格，点击**清单 (Inventory)**。

**步骤 2** 点击 **ASA** 选项卡。

**步骤 3** 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

**步骤 4** 您可以使用以下方法之一来添加子接口：

- 选择 + > **子接口 (Subinterface)**
- 点击要配置的物理接口，然后在右侧的**操作 (Actions)** 窗格中，点击**新建子接口 (New Subinterface)**。

**步骤 5** 在 **VLAN ID** 字段中，输入介于 1 和 4094 之间的 VLAN ID。

某些 VLAN ID 可能是连接的交换机中的保留 VLAN ID，因此请查看交换机文档以了解详细信息。对于多情景模式，您只能在系统配置中设置 VLAN。

**步骤 6** 在**子接口 ID (Subinterface ID)** 字段中，输入子接口 ID（介于 1 到 4294967293 之间的整数）。

允许的子接口数因平台而异。此 ID 一旦设置便不可更改。

**步骤 7** 继续执行以下程序之一：

- 如果要向此接口分配 IPv4 地址，请为 ASA 子接口配置 IPv4 地址。
- 如果要向此接口分配 IPv6 地址，请为 ASA 子接口配置 IPv6 地址。
- 配置高级 ASA 子接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了子接口，并且不想继续使用高级子接口选项，请继续启用子接口。

## 为 ASA 子接口配置 IPv4 地址

**步骤 1** 在**创建子接口 (Creating Subinterface)** 对话框中，在 **IPv4 地址 (IPv4 Address)** 选项卡中配置以下内容：

- **类型 (Type)**：您可以为接口使用静态 IP 寻址或 DHCP。

  **静态 (Static)** - 如果希望分配固定的地址，请选择此选项。

- **IP 地址和子网掩码 (IP Address and Subnet Mask)**：对于连接到接口的网络，键入接口的 IP 地址和子网掩码。
- **备用 IP 地址 (Standby IP Address)**：如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IP 地址。备用设备上的此接口使用备用地址。

  为每个接口设置一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。

**DHCP**：如果应从网络中的 DHCP 服务器获取地址，请选择此选项。

您可以选中**获取默认路由 (Obtain Default Route)** 复选框以便从 DHCP 服务器获取默认路由。您通常都要选中此选项。

**步骤 2** 完成后点击**保存 (Save)**，或者继续执行其中一个程序。

- 如果要向此接口分配 IPv6 地址，请为 ASA 子接口配置 IPv6 地址。
- 配置高级 ASA 子接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了子接口，并且不想继续使用高级子接口选项，请继续启用 ASA 物理接口。

## 为 ASA 子接口配置 IPv6 地址

**步骤 1** 在**创建子接口 (Creating Subinterface)** 对话框中，点击**IPv6 地址 (IPv6 Address)** 选项卡。

**步骤 2** 进行以下配置：

- **状态 (State)** - 在您未配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请点击**状态 (State)** 滑块将其启用。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  **注释** 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置**：

  选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

  虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

- **抑制 RA (Suppress RA)**：如果要抑制路由器通告，请选中此复选框。设备可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

- **DAD 尝试** - 接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。
- **本地链路地址 (Link-Local Address)**：如果要仅将地址用作链路本地地址，请在链路本地地址字段中输入该地址。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

  注释　链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用链路本地地址 (Standby Link-Local Address)**：如果接口连接高可用性设备，请配置此地址。输入此接口所连接的另一台设备上的接口本地链路地址。
- **静态地址/前缀 (Static Address/Prefix)**：如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。您可以添加另一个静态地址。
- **备用 IP 地址 (Standby IP Address)**：如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

**步骤 3** 完成后点击**保存 (Save)**，或者继续执行其中一个程序。

- 配置高级 ASA 子接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了子接口，并且不想继续使用高级子接口选项，请继续启用子接口。

## 配置高级 ASA 子接口选项

高级接口选项的默认设置适用于大多数网络。只有在需要解决网络问题时，再配置它们。

以下步骤程序假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

此程序及其中的所有步骤都是可选的。

**步骤 1** 在**创建子接口 (Creating Subinterface)** 对话框中，点击**高级 (Advanced)** 选项卡。

**步骤 2** 配置以下高级设置：

- **HA 监控 (HA Monitoring)**：启用后，可在当 HA 对决定是否在高可用性配置中故障转移到对等设备时考虑接口的运行状况。如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。

- **仅管理 (Management Only)**：启用后，可进行数据接口管理。

  仅管理接口不允许直通流量，所以将数据接口设置为**仅管理 (Management Only)** 接口的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

- **MTU**：默认 MTU 为 1500 字节。您可以指定 64 - 9198 之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。

- **DAD 尝试 (DAD Attempts)**：接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

- **MAC 地址 (MAC Address)**：采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。

- **备用 MAC 地址 (Standby MAC Address)**：用于高可用性。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

**步骤 3** 如果您保存了接口并且不想继续使用高级接口选项，请继续启用子接口。

**步骤 4** 点击**保存 (Save)**。

## 启用子接口

**步骤 1** 选择要启用的子接口。

**步骤 2** 移动与接口逻辑名称关联的窗口右上角的**状态 (State)** 滑块。

**步骤 3** 查看和部署所做的更改。

## 删除 ASA 子接口

使用以下程序从 ASA 中删除子接口。

**步骤 1** 在 CDO 导航窗格，点击**清单 (Inventory)**。

**步骤 2** 点击 **ASA** 选项卡。

**步骤 3** 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

**步骤 4** 在**接口 (Interfaces)** 页面上，展开与要删除的子接口链接的物理接口，然后选择该特定子接口。

**步骤 5** 在右侧的**操作 (Actions)** 窗格中，点击**删除 (Remove)**。

**步骤 6** 确认要删除 EtherChannel 接口，然后点击**删除 (Delete)**。

步骤 7 预览和部署所有设备的配置更改所做的更改。

# 关于 ASA EtherChannel 接口

802.3ad EtherChannel 是逻辑接口（称为端口通道接口），该接口由一组单独的以太网链路（通道组）组成，以便可以提高单个网络的带宽。配置接口相关功能时，可以像使用物理接口一样来使用端口通道接口。

最多可以配置 48 个 Etherchannel，具体取决于型号支持的接口数量。

### 链路汇聚控制协议

链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

有关 ASA EtherChannel 接口的详细信息，请参阅《ASDM 手册 1：思科 ASA 系列常规操作 ASDM 配置指南 X, Y》的 **EtherChannel 和冗余接口**一章。

## 配置 ASA EtherChannel

使用此程序将新的 EtherChannel 接口添加到 ASA。

### 开始之前

要在 ASA 接口上配置 EtherChannel，必须满足以下前提条件：

- 通道组中的所有接口都必须具有相同的介质类型和容量，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 3100 除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。
- 如果已为物理接口配置了名称，则不能将该物理接口添加到通道组。您必须先删除该名称。
- 不能添加另一个 EtherChannel 接口组的接口部分、交换机端口接口和具有子接口的接口。

**步骤 1** 在 CDO 导航窗格，点击**清单 (Inventory)**。

**步骤 2** 点击 **ASA** 选项卡。

**步骤 3** 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

**步骤 4** 选择  > **EtherChannel 接口 (EtherChannel Interface)**。

**步骤 5** 在**逻辑名称 (Logical Name)** 字段中，提供 EtherChannel 接口的名称。

**步骤 6** 在**冗余 ID (Redundant ID)** 字段中，请输入一个介于 1 和 8 之间的整数。

**步骤 7** 点击**链路汇聚控制协议 (Link Aggregation Control Protocol)** 的下拉按钮，然后选择以下两个选项之一：

- **Active (活动)** - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- **开 (On)** - EtherChannel 始终开启，并且不使用 LACP。**开启**的 EtherChannel 只能与另一个**开启**的 EtherChannel 建立连接。

**步骤 8** 搜索并选择要作为成员包含在 EtherChannel 中的接口。您**必须**包含至少一个接口。

警告 如果将 EtherChannel 接口添加为成员，并且该接口已配置了 IP 地址，则 CDO 会删除该成员的 IP 地址。

**步骤 9** 选择 **IPv4**、**IPv6** 或**高级 (Advanced)** 选项卡以配置子接口的 IP 地址。

- 如果要为 ASA EtherChannel 接口分配 IPv4 地址，请为 ASA 物理接口配置 IPv4 地址。
- 如果要为 ASA EtherChannel 接口分配 IPv6 地址，请为 ASA 物理接口配置 IPv6 地址。
- 配置高级 ASA 物理接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

**步骤 10** 移动窗口右上角的**状态 (State)** 滑块以启用 EtherChannel 接口。

**步骤 11** 点击**保存 (Save)**。

**步骤 12** 预览和部署所有设备的配置更改所做的更改。

### 编辑 ASA EtherChannel

使用此程序可编辑 ASA 上的现有 EtherChannel。

**步骤 1** 在 CDO 导航窗格，点击**清单 (Inventory)**。

**步骤 2** 点击 **ASA** 选项卡。

**步骤 3** 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

**步骤 4** 在**接口 (Interfaces)** 页面上，选择要编辑的 EtherChannel 接口。

**步骤 5** 在位于右侧的**操作 (Actions)** 窗格中，点击**编辑 (Edit)**。

**步骤 6** 修改所需的值，然后点击**保存 (Save)**。

**步骤 7** 预览和部署所有设备的配置更改所做的更改。

### 移除 ASA EtherChannel 接口

使用以下程序从 ASA 中删除 EtherChannel 接口。

**步骤 1** 在 CDO 导航窗格，点击**清单 (Inventory)**。

**步骤 2** 点击 **ASA** 选项卡。

**步骤 3** 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

**步骤 4** 在**接口 (Interfaces)** 页面上，选择要删除的 EtherChannel 接口。

**步骤 5** 在右侧的**操作 (Actions)** 窗格中，点击**删除 (Remove)**。

**步骤 6** 确认要删除 EtherChannel 接口，然后点击**删除 (Delete)**。

**步骤 7** 预览和部署所有设备的配置更改所做的更改。

# ASA 系统设置策略

### ASA 系统设置策略简介

使用系统设置策略来管理ASA设备的操作和功能。此策略包括基本配置，例如域名服务、启用安全复制服务器、消息日志记录以及允许 VPN 流量而不检查 ACL。通过设置策略，您可以确保正确配置设备以维护安全的网络环境。

在配置ASA设备时，请务必注意，您可以选择使用共享系统设置策略管理多个设备的设置，也可以单独编辑任何单个设备的设置。

### 共享系统设置策略

共享系统设置策略适用于网络中的多个ASA设备。通过它可以同时配置多个受管设备，从而在部署中提供一致性并精简管理工作。对共享策略的参数所做的任何更改都会影响使用该策略的其他 ASA 设备。

选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。请参阅创建 ASA 共享系统设置策略，第 166 页。

您还可以修改特定于单个 ASA 设备的设备特定系统设置，以覆盖共享系统设置策略值。选择**清单 (Inventory)** > **ASA 设备 (ASA device)** > **管理 (Management)** > **设置 (Settings)**。请参阅配置或修改设备特定系统设置，第 173 页。

# 创建 ASA 共享系统设置策略

使用此部分为 ASA 设备创建新的共享系统设置策略。

**步骤 1** 选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。

**步骤 2** 请点击  。

**步骤 3** 在**名称 (Name)** 字段中，输入策略的名称并点击**保存 (Save)**。

**步骤 4** 在编辑 ASA 共享系统设置页面中，配置所需的参数：

- 配置基本 DNS 设置，第 167 页

- 配置 HTTP 设置，第 168 页
- 使用 NTP 服务器设置日期和时间，第 168 页
- 配置 SSH 访问，第 169 页
- 配置系统日志记录，第 170 页
- 启用 Sysopt 设置，第 172 页


注释

- 相应参数上的橙色点 ( ) 会突出显示未保存的更改。
- 被拒绝的符号 ( ) 突出显示了使用设备中现有本地值的参数。

## 配置基本 DNS 设置

需要配置 DNS 服务器，以便 ASA 能够将主机名解析为 IP 地址。还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

**步骤 1** 在编辑 ASA 系统设置页面中，点击左侧窗格中的 **DNS**。

**步骤 2** 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

**重要事项** 如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

**步骤 3** 在 **DNS** 部分中，点击 以配置服务器。

- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)**：指定 DNS 服务器的 IP 地址。
- **接口名称 (Interface Name)**：指定应启用 DNS 查找的接口。

注释 确保此处指定的接口名称在与此共享系统设置策略相关联的 ASA 设备上相同。

**步骤 4** 点击**保存 (Save)**。

**步骤 5** 在**域名 (Domain name)** 字段中，指定 ASA 的域名。

ASA 会将域名作为后缀追加到不受限定的名称。例如，如果您将域名设置为“example.com”并通过不受限定的名称“jupiter”来指定系统日志服务器，则 ASA 会将名称限定为“jupiter.example.com”。

**步骤 6** 在 **DNS 查找 (DNS Lookup)** 部分中，点击 并指定接口名称。

如果不在接口上启用 DNS 查找，则 ASA 将不会与该接口上的 DNS 服务器通信。确保在将用于访问 DNS 服务器的所有接口上启用 DNS 查找。

注释　　要删除配置的接口，您可以点击**操作 (Actions)** 下的删除图标。

**步骤 7** 点击**保存 (Save)**。

## 配置 HTTP 设置

要访问 ASA 接口以进行管理访问，您必须指定允许使用 HTTP 访问 ASA 的所有主机/网络的地址。如果您配置 HTTP 重定向以将 HTTP 连接自动重定向至 HTTPS，则必须启用允许 HTTP 的访问规则；否则，该接口无法侦听 HTTP 端口。

**步骤 1** 在编辑 ASA 系统设置页面中，点击左侧窗格中的 **HTTP**。

**步骤 2** 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

重要事项　　如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

**步骤 3** 选中 **启用 HTTP 服务器** 复选框以启用 HTTP 服务器。

**步骤 4** 在**端口号 (Port Number)** 字段中，设置端口号。port 确定接口从其重定向 HTTP 连接的端口。

警告　　如果更改设备上的 HTTP 端口，则可能会导致其与 CDO 的连接出现一些问题。如果您计划更改与设备网络连接相关的任何设置，请务必记住这一点。

**步骤 5** 点击  添加 HTTP 信息。

- **接口 (Interface)**：确保此处指定的接口名称在与此共享系统设置策略相关联的 ASA 设备上相同。
- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)**：指定可以使用 HTTP 访问 ASA 的所有主机/网络的地址。
- **网络掩码 (Netmask)**：指定网络子网掩码。

注释　　要删除主机，您可以点击**操作 (Actions)** 下的删除图标。

**步骤 6** 点击**保存 (Save)**。

## 使用 NTP 服务器设置日期和时间

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，例如验证 CRL，其包括精确时间戳。可配置多个 NTP 服务器。ASA 选择层级最低的服务器，作为衡量数据可靠性的方式。

NTP 服务器生成的时间将覆盖手动设置的任何时间。

ASA 支持 NTPv4。

**步骤 1** 在编辑 ASA 系统设置页面中，点击左侧窗格中的 **NTP**。

**步骤 2** 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

**重要事项** 如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

**步骤 3** 点击  以添加 NTP 服务器详细信息。

- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)**：指定 NTP 服务器的 IP 地址。

  不能输入服务器的主机名；ASA 不支持 NTP 服务器的 DNS 查找。
- **密钥 ID (Key Id)**：输入一个介于 1 和 4294967295 之间的数字。

  该设置指定此身份验证密钥的密钥ID，可供您使用身份验证与NTP服务器进行通信。NTP服务器数据包必须也使用此密钥 ID。
- **接口名称 (Interface Name)**：指定接口名称。确保此处指定的接口名称在与此共享系统设置策略相关联的ASA设备上相同。

  NTP 使用一种算法确定最准确的服务器，然后与该服务器同步。如果多台服务器准确度相似，则使用首选服务器。但是，如果某台服务器的准确度明显高于首选服务器，则 ASA 将使用这台更准确的服务器。
- **首选 (Prefer)**：（可选）选中**首选 (Preferred)** 复选框，将该服务器设置为首选服务器。

**注释** 要删除 NTP 服务器，您可以点击**操作 (Actions)** 下的删除图标。

**步骤 4** 点击**保存 (Save)**。

## 配置 SSH 访问

您可以在 ASA 上启用安全复制 (SCP) 服务器。只有经允许使用 SSH 访问 ASA 的客户端才能建立安全复制连接。

**步骤 1** 在编辑 ASA 设置策略页面中，点击左侧窗格中的 **SSH**。

**步骤 2** 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

**重要事项** 如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

**步骤 3** 启用**启用 Scopy SSH (Enable Scopy SSH)**（安全复制 SSH）。

**步骤 4** 在**超时时间 (Timeout in Minutes)** 字段中，将超时值设置为 1 到 60 分钟。默认值为 5 分钟。在大多数情况下，默认持续时间都太短，应增加为直到完成所有前期测试和故障排除所需的时间。

**步骤 5** 点击  并配置以下各项：

- **接口 (Interface)**：指定接口名称。确保此处指定的接口名称在与此共享系统设置策略相关联的 ASA 设备上相同。
- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)**：指定可以使用 SSH 访问 ASA 的所有主机/网络的地址。
- **网络掩码 (Netmask)**：指定网络子网掩码。

注释　要删除 SSH 详细信息，您可以点击**操作 (Actions)** 下的删除图标。

**步骤 6** 点击**保存 (Save)**。

## 配置系统日志记录

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。思科设备可以将其日志消息发送到 UNIX 样式的系统日志服务。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

### 安全级别

下表列出系统日志消息严重性级别。

**表 *14:* 系统日志消息严重级别**

| 级别号 | 安全等级 | 说明 |
|---|---|---|
| 0 | 应急 | 系统不可用 |
| 1 | 警报 | 需要立即采取措施。 |
| 2 | 严重 | 严重情况。 |
| 3 | 错误 | 错误情况。 |
| 4 | 警告 | 警告情况。 |
| 5 | 通知 | 正常但重大的情况。 |
| 6 | 信息性 | 消息仅供参考。 |
| 7 | 调试 | 消息仅供调试。<br>调试问题时，仅临时记录此级别的日志。此日志级别可能会生成太多消息，从而影响系统性能。 |

注释 ASA 不会生成严重性级别为零（紧急）的系统日志消息。

**步骤 1** 在编辑 ASA 系统设置页面中，点击左侧窗格中的**系统日志 (Syslog)**。

**步骤 2** 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

**重要事项** 如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

**步骤 3** 进行以下配置：

- **日志记录已启用 (Logging Enabled)**：启用安全日志记录。
- **时间戳已启用 (Timestamp Enabled)**：启用后可在系统日志消息中包含日期和时间。
- **允许主机关闭 (Permit host down)**：（可选）禁用在 TCP 连接的系统日志服务器关闭时阻止新连接的功能。
- **缓冲区大小 (Buffer Size)**：指定内部日志缓冲区的大小。允许的范围为 4096 到 1048576 字节。
- **已缓冲的日志记录级别 (Buffered Logging Level)**：指定应将哪些系统日志记录消息发送到充当临时存储位置的内部日志缓冲区。
- **控制台日志记录级别 (Console Logging Level)**：指定应将哪些系统日志消息发送到控制台端口。
- **陷阱日志记录级别 (Trap Logging Level)**：指定应将哪些系统日志消息发送到系统日志服务器。

**步骤 4** 点击  以添加系统日志服务器详细信息。

- **接口名称 (Interface Name)**：指定系统日志服务器所在接口的名称。确保此处指定的接口名称在与此共享系统设置策略相关联的 ASA 设备上相同。
- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)** - 指定系统日志服务器的 IP 地址。
- **协议 (Protocol)**：选择 ASA 应该用于将系统日志消息发送到系统日志服务器的协议（**TCP** 或 **UDP**）。
  - **端口 (Port)**：指定系统日志服务器为获取系统日志消息所侦听的端口。允许的 TCP 端口范围为 1 至 65535，UDP 端口范围为 1025 至 65535。
  - **思科 EMBLEM 格式的日志消息（仅限 UDP）(Log messages in Cisco EMBLEM format [UDP only])**：仅为带有 UDP 的系统日志服务器启用 EMBLEM 格式日志记录。
  - **使用 SSL 启用安全系统日志？(Enable secure syslog using SSL?)**：指定与远程日志记录主机的连接应仅对 TCP 使用 SSL/TLS。
- **引用身份 (Reference Identity)**：指定引用身份类型，以便根据先前配置的引用身份对象对证书进行 RFC 6125 引用身份检查。有关引用标识对象的详细信息，请参阅配置引用身份。

注释　　要删除系统日志服务器，您可以点击**操作 (Actions)** 下的删除图标。

**步骤 5** 点击**保存 (Save)**。

## 启用 Sysopt 设置

与传出接口绑定的加密映射 ACL 将允许或拒绝 IPSec 数据包通过 VPN 隧道。IPsec 对从 IPSec 隧道到达的数据包进行身份验证和解密，并使其按照与隧道关联的 ACL 接受评估。

ACL 定义要保护的 IP 流量。例如，您可以创建 ACL 以保护两个子网或两台主机之间的所有 IP 流量。

**步骤 1** 在编辑 ASA 系统设置页面中，点击左侧窗格中的 **Sysopt**。

**步骤 2** 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

重要事项　　如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

**步骤 3** 启用**允许 VPN 流量绕行接口访问列表 (Allow VPN traffic to bypass interface access lists)** 会绕过 ACL 检查。

**步骤 4** 点击**保存 (Save)**。

## 从“共享系统设置”(Shared System Settings) 页面分配策略

在配置共享系统设置策略后，分配已载入的ASA设备并将设置部署到设备，以使更改生效。对策略所做的任何更改都会影响与该策略关联的设备。

您还可以从设备特定设置页面分配策略。

注释　　您只能将 ASA 设备关联到一个共享系统设置策略。

**步骤 1** 选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。

**步骤 2** 选择共享策略，然后点击**编辑 (Edit)**。

**步骤 3** 点击策略名称旁边显示的过滤器以分配设备。

**步骤 4** 选择要与所选策略关联的 ASA 设备，然后点击**确定 (OK)**。

注释　　选中已与所选策略关联的设备的复选框。

如果您看到红色图标 ，则表示将共享系统设置策略应用于您的设备时发生错误。要解决问题，请点击**ASA 系统设置 (ASA System Settings)** 页面上的策略，然后在**检测到的错误 (Error Detected)** 窗格中点击**设备工作流程 (Device Workflows)** 以获取更多信息。

**步骤 5** 部署使用 CDO GUI 进行的配置更改所做的更改。

# 配置或修改设备特定系统设置

设备特定系统设置是 ASA 设备特定的现有值，可使用 CDO 进行修改。您可以使用所需参数的现有设备特定值来覆盖共享系统设置策略值。

本主题介绍如何配置已载入的 ASA 设备的系统设置。

**步骤 1** 在左侧窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击 **ASA** 选项卡。

**步骤 3** 选择您想要的 ASA 设备，然后在右侧的**管理 (Management)** 窗格中点击**设置 (Settings)**。

您将看到所选 ASA 设备的设备特定系统设置。

**注释** 如果为所选设备分配了共享系统设置策略，**父策略**将提供打开该策略的链接。您还可以从设备特定的设置页面分配策略。选择要与所选策略关联的 ASA 设备，然后点击**确定 (OK)**

**步骤 4** 配置或修改所需的系统设置值，然后点击**保存 (Save)**。

**注释** 共享和设备特定系统设置的字段说明会保持不变。您可以点击下面的相应链接了解更多信息。

- 配置基本 DNS 设置， 第 167 页
- 配置 HTTP 设置， 第 168 页
- 使用 NTP 服务器设置日期和时间， 第 168 页
- 配置 SSH 访问， 第 169 页
- 配置系统日志记录， 第 170 页
- 启用 Sysopt 设置， 第 172 页

您可以点击**返回清单 (Return to Inventory)** 以导航至清单页面。

**步骤 5** 完成更改后点击**保存 (Save)**。

**注释** 相应参数上的橙色点 (  ) 会突出显示未保存的更改。

## 从设备特定设置页面分配策略

您还可以从已载入的 ASA 设备的设备特定设置页面分配策略。

**步骤 1** 在左侧窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击 **ASA** 选项卡。

**步骤 3** 选择您想要的 ASA 设备，然后在右侧的**管理 (Management)** 窗格中点击**设置 (Settings)**。

您将看到所选 ASA 设备的设备特定设置。

注释 如果为所选设备分配了共享系统设置策略，**父策略**将提供打开该策略的链接。选择要与所选策略关联的 ASA 设备，然后点击**确定 (OK)**

**步骤 4** 点击**父策略 (Parent Policy)** 按钮以分配共享系统设置策略。

**步骤 5** 选择策略，然后点击**应用 (Apply)**。

**步骤 6** 部署使用 CDO GUI 进行的配置更改所做的更改。

# 将 ASA 设备自动分配到共享系统设置策略

在载入新的 ASA 设备或检查更改或处理现有设备的带外更改时，CDO 会验证是否：

- 设备特定设置与预先存在的共享系统设置策略相匹配。如果匹配，设备将被分配到共享系统设置策略。
- 已载入设备的设备特定本地设置彼此匹配。如果是这样，则会自动创建一个新的共享系统设置策略，并将具有相同本地设置的设备分配给该共享策略。

注释 无论它是由用户还是系统创建的，您都可以重命名共享设置策略。

# 过滤 ASA 共享系统设置策略

如果您在ASA系统设置页面上搜索特定的共享系统设置策略，则可以使用基于问题和使用情况的过滤器来缩小搜索范围并更轻松地查找所需内容。

选择**策略 (Policies)**> **ASA 系统设置 (ASA System Settings)** > 。

- 问题：
  - **检测到的问题 (Issue Detected)**：仅显示在向其应用设备时存在问题的策略。
  - **无问题 (No issue)**：仅显示已成功应用于设备的策略。
- 用法：
  - **使用中 (In Use)**：显示已分配给设备的策略。
  - **未使用 (Unused)**：显示尚未分配给任何设备的策略。

# 将设备从共享系统设置策略取消关联

如果共享系统设置策略中不再需要ASA设备，则可以轻松地将其取消关联。在以下情况下，设备将从策略中分离：

- 对特定于设备的设置进行了更改，其中共享策略上的相应设置未配置为保留设备中的现有值。
- 设备从共享系统设置策略中手动分离。
- 共享系统设置策略已从 CDO 中删除。但是，这样不会删除设备。请参阅 删除共享设置策略，第 175 页。

**步骤 1** 选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。

**步骤 2** 选择共享策略，然后点击**编辑 (Edit)**。

**步骤 3** 点击策略名称旁边显示的过滤器以分离设备。

**步骤 4** 取消选中要从所选共享系统设置策略中分离的设备，然后点击**确定 (OK)**。

**注释** 更改会自动保存，无需任何手动部署。

# 删除共享设置策略

如果要删除某些共享设置策略，您可以选择其中一个或多个策略并将其删除。但务必注意，只有在尚未将其应用或提交到任何设备的情况下，才能将其删除。

### 开始之前

确保设备已与要删除的共享设置策略取消关联。有关详细信息，请参阅将设备从共享系统设置策略取消关联。

**步骤 1** 选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。

**步骤 2** 选择共享策略，然后点击**删除 (Delete)**。

**步骤 3** 点击**确定 (OK)** 以确认操作。

**注释** 如果从 CDO 中删除 ASA，则设备特定的设置和配置也将被删除，并且设备引用将从共享设置策略中删除。

# ASA 路由

路由协议使用指标来评估传播数据包的最佳路径。指标是一种测量标准，例如供路由算法用于确定目标的最佳路径的路径带宽。为帮助执行确定路径的过程，路由算法会初始化和维护其中包含路由信息的路由表。路由信息根据所使用的路由算法而异。

路由算法使用各种信息来填充路由表。目标或下一跳关联告知路由器，可以通过将数据包发送到特定路由器（表示通往最终目标的下一跳）来以最优路径到达特定目标。当路由器收到传入数据包时，会检查目标地址并尝试将此地址与下一跳关联。

路由表还包含其他信息，例如有关路径可取性的数据。路由器通过比较指标来确定最佳路由，而这些指标根据所使用的路由算法的设计而异。

路由器互相进行通信，并通过传输各种消息来维护其路由表。路由更新消息是通常由路由表的全部或部分内容组成的消息。通过分析来自所有其他路由器的路由更新，路由器可以构建详细的网络拓扑图。链路状态通告（路由器之间发送的另一种消息）用于告知其他路由器发送方链路的状态。链路信息可用于构建完整网络拓扑图，以使路由器能够确定通向网络目标的最佳路径。

# 关于 ASA 静态路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。通常，您必须配置至少一个静态路由：所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

有关 ASA 如何路由的概念和 CLI 命令的一般信息，请参阅以下文档：

- ASDM 手册 1：《思科 ASA 系列通用操作 ASDM 配置指南 X,Y 版》的静态和默认路由一章。
- CLI 手册 1：《思科 ASA 系列通用操作 CLI 配置指南 X,Y 版》的静态和默认路由一章。

### 默认路由

最简单的方法是配置一个默认静态路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关IP地址进行标识，ASA将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

应始终定义一个默认路由。

### Static Route

在以下情况下，您可能希望使用静态路由：

- 您的网络使用不受支持的路由器发现协议。
- 网络规模较小，并且可以轻松管理静态路由。
- 不希望流量或 CPU 开销与路由协议相关联。

- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与 ASA 连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。

### 静态路由跟踪

使用静态路由的一个问题是，缺乏用于确定路由处于开启还是关闭状态的内在机制。即使下一跳网关变得不可用，这些路由依然保留在路由表中。只有当ASA上的关联接口发生故障时，才会从路由表中删除静态路由。

静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。例如，您可以定义一条到 ISP 网关的默认路由和一条到辅助 ISP的备用默认路由，以防主 ISP 不可用。

ASA 通过将静态路由与 ASA 使用 ICMP 回应请求监控的目标网络上的监控目标主机相关联来实施静态路由跟踪。如果在指定时间内没有收到回应回复，则主机将被视为关闭，并且会从路由表中删除关联路由。使用具有较高指标的未跟踪备用路由替代已删除的路由。

选择监控目标时，您需要确保它能够响应 ICMP 回应请求。该目标可以是您选择的任何网络对象，但是应考虑使用以下对象：

- ISP 网关（用于支持双 ISP）地址。
- 下一跳网关地址（如果您关注网关的可用性）。
- 目标网络上的服务器，例如 ASA 需要与之进行通信的系统日志服务器。
- 目标网络上的持久网络对象。

## 配置 ASA 静态路由

静态路由用于定义为特定目标网络发送流量的位置。

本节介绍将静态路由添加到 ASA 设备的步骤。

**步骤 1** 在左侧窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击 **ASA** 选项卡。

**步骤 3** 选择要配置静态路由的设备。

**步骤 4** 在左侧的**管理 (Management)** 窗格中，点击**路由 (Routing)**。

**步骤 5** 点击  以添加静态路由。

**步骤 6** 您可以输入路由的**说明**。

**步骤 7** 选择路由是用于 **IPv4** 还是 **IPv6** 地址。

**步骤 8** 配置路由属性：

- **接口 (Interface)**：选择要通过其发送流量的接口。通过此接口需能够访问网关地址。

您可以使用 **Null0** 路由转发不必要或不需要的流量，从而丢弃该流量。静态 Null0 路由具有良好的性能配置文件。您还可以使用静态 null0 路由防止产生路由环路。

ASA CLI 接受 Null0 或 null0 字符串。

- **网关 IP (Gateway IP)**：（不适用于 **Null0** 路由）选择标识网关 IP 地址的主机网络对象至目标网络。流量将发送至此地址。
- **度量 (Metric)**：路由的管理距离，该值介于 1 和 254 之间。静态路由的默认值为 1。如果接口和网关之间还有其他路由器，请输入跳数作为管理距离。

  管理距离是用于比较路由的参数。数字越小，为该路由指定的优先级越高。连接的路由（直连到设备接口的网络）始终优先于静态路由。
- **目标 IP (Destination IP)**：选择标识目标网络的网络对象，该目标网络包含在此路由中使用网关的主机。
- **目标掩码 (Destination Mask)**（仅适用于 IPv4 寻址）：输入目的 IP 的子网掩码。
- **跟踪 (Tracking)**（仅适用于 IPv4 寻址）：输入路由跟踪进程的唯一标识符。

**步骤 9** 点击**保存 (Save)**。

**步骤 10** 部署使用 CDO GUI 进行的配置更改您所做的更改，或等待并一次部署多个更改。

## 编辑 ASA 静态路由

您可以编辑与 ASA 设备关联的静态路由参数。

**注释** 但是，在修改静态路由时不能选择其他 IP 版本。或者，您可以根据自己的要求创建新的静态路由。

**步骤 1** 选择要编辑静态路由的 ASA 设备。

**步骤 2** 在左侧的**管理 (Management)** 窗格中，点击**路由 (Routing)**。

**步骤 3** 在路由列表页面中，选择要修改的路由，然后在右侧的**操作 (Actions)** 窗格中，点击**编辑 (Edit)**。

**步骤 4** 修改所需的值，然后点击**保存 (Save)**。有关路由参数的信息，请参阅配置 ASA 静态路由，第 177 页。

**步骤 5** 部署使用 CDO GUI 进行的配置更改您所做的更改，或等待并一次部署多个更改。

## 删除静态路由

### 开始之前

删除静态路由可能会影响与设备的本地 SDC 或 CDO 的连接。确保为任何连接丢失制定了适当的灾难恢复程序。

**步骤 1** 选择要删除的 ASA 设备。

**步骤 2** 在左侧的**管理 (Management)** 窗格中，点击**路由 (Routing)**。

**步骤 3** 在路由列表页面中，选择要修改的路由，然后在右侧的**操作 (Actions)** 窗格中，点击**删除 (Delete)**。

**步骤 4** 点击“确定”(OK) 确认更改。

**步骤 5** 部署使用 CDO GUI 进行的配置更改您所做的更改，或等待并一次部署多个更改。

# 安全策略管理

安全策略检查网络流量，最终目标是允许流量到达其预定目的地，或者在识别出安全威胁时丢弃该流量。您可以使用 CDO 在许多不同类型的设备上配置安全策略。

- ASA 策略（扩展访问列表），第 189 页
- 网络地址转换，第 196 页

# 管理传统 ASA 访问策略

本部分提供有关传统网络策略页面的信息，该页面显示 Cisco Defense Orchestrator (CDO) 管理的所有设备正在使用的所有网络策略的列表。导航策略 ASA 策略以到达网络策略页面。 >

网络策略是网络规则的集合。每个网络规则根据源和目标 IP 地址、IP 协议、端口号、EtherType 等特征允许或阻止网络流量到达网络目标。

当 CDO 创建网络策略时，它会将其与 ASA 接口关联，并在策略中创建一个默认规则。与接口关联的网络策略是 ASA 所称的“访问组”。策略名称相当于 ASA 中的访问控制列表 (ACL) 名称。CDO 创建的默认规则以及您添加到此网络策略的后续规则在 ASA 中称为访问控制条目 (ACE)。访问控制条目 (ACE)，第 189 页

**相关信息：**

- 在传统视图中创建 ASA 网络策略
- 编辑 ASA 网络策略
- 复制 ASA 网络策略
- 比较 ASA 网络策略
- 删除 ASA 网络策略
- 搜索和过滤 ASA 网络策略和规则
- 共享 ASA 网络策略
- 访问控制条目 (ACE)

# 在传统视图中创建 ASA 网络策略

使用此程序创建 ASA 网络策略：

**步骤 1** 选择策略 ASA 策略。 >
**步骤 2** 点击**创建策略**。
**步骤 3** 点击设备过滤器以搜索您将在其上保存策略的设备。
**步骤 4** 输入策略的名称。请注意，一台设备上不能有两个具有相同名称的网络策略。
**步骤 5** 选择要应用此策略的接口。
**步骤 6** 指定策略是用于出站流量还是入站流量。请注意，同一设备上的同一接口不能有两个策略。
**步骤 7** 点击**保存 (Save)**。CDO 为该策略创建网络策略和单个“permit IP any any”规则。
**步骤 8** 根据需要编辑策略。编辑 ASA 网络策略, on page 180
**步骤 9** 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

# 编辑 ASA 网络策略

Defense Orchestrator 允许您从“策略详细信息”页面编辑网络策略和策略规则。您可以通过以下方式编辑 ASA 策略：

- 重命名策略
- 将规则添加到策略
- 在策略中移动规则
- 在策略之间移动规则
- 在策略中停用规则
- 记录规则活动
- 定义策略的时间范围

## 重命名策略

**步骤 1** 选择策略 ASA 策略。 >
**步骤 2** 选择要重命名的网络策略。
**步骤 3** 点击详细信息窗格中的重命名图标 。
**步骤 4** 编辑策略名称，然后点击蓝色复选框以保存更改。

## 将规则添加到策略

**步骤 1** 选择策略 > ASA 策略。

**步骤 2** 选择要编辑的网络策略。

**步骤 3** 点击**编辑策略 (Edit Policy)**。

**步骤 4** 在详细信息窗格中，点击编辑工具工具栏中的 ，将规则添加到网络策略。新规则将添加到策略中突出显示的规则上方。规则按规则列表中的位置确定优先级，从 1 到“最后”。

**Note** 默认情况下，为新规则分配“允许”操作。

**步骤 5** 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

**步骤 6** 查看策略详细信息窗格中的设备字段。如果超过了最佳条目数，您将收到一条警告，例如“ACE count exceeded, 500 max entries, 1000 found”，具体取决于安装 ASA 的 ASA 硬件型号。

**步骤 7** 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

## 在策略中移动规则

**步骤 1** 选择策略 > ASA 策略。

**步骤 2** 选择网络策略。

**步骤 3** 在详细信息窗格中，点击编辑策略。

**步骤 4** 在规则表中选择一条规则，点击“编辑工具”栏中的“剪切”。

**步骤 5** 选择要在刚剪切的规则之前放置的规则。规则按规则列表中的位置确定优先级。数值越大，优先级越高。

**步骤 6** 点击粘贴。

**步骤 7** 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

**步骤 8** 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

## 在策略之间移动规则

您可以复制一个策略中的规则并将其粘贴到另一个策略中。

**步骤 1** 选择策略 ASA 策略。 >

**步骤 2** 选择包含要复制的规则的网络策略。

**步骤 3** 在详细信息窗格中，点击编辑策略。

**步骤 4** 在规则表中选择一条规则，点击“编辑工具”栏中的复制。

**步骤 5** 选择策略 > ASA 策略。

**步骤 6** 选择要将规则复制到的网络策略。

**步骤 7** 在详细信息窗格中，点击编辑策略。

**步骤 8** 选择要放在刚刚复制的规则之后的规则。规则按规则列表中的位置确定优先级。数值越大，优先级越高。

**步骤 9** 点击粘贴。

**步骤 10** 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

**步骤 11** 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

## 在策略中停用规则

默认情况下，规则处于活动状态。您可以停用策略中的单个规则。

**步骤 1** 选择策略 > ASA 策略。

**步骤 2** 选择包含要停用的规则的网络策略。

**步骤 3** 在详细信息窗格中，点击编辑策略。

**步骤 4** 选择要停用的规则。

**步骤 5** 关闭 Active 设置。 


**步骤 6** 点击**保存 (Save)**。

**步骤 7** 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

**步骤 8** 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

## 记录规则活动

默认情况下，不记录网络策略规则产生的活动。您可以为单个规则激活日志记录。

**步骤 1** 选择策略 ASA 策略。 >

**步骤 2** 选择包含要激活的规则的网络策略。

**步骤 3** 在详细信息窗格中，点击**编辑策略 (Edit Policy)**。

**步骤 4** 选择要记录活动的规则。

**步骤 5** 点击滑块以激活日志记录。 

**步骤 6** 点击**编辑 (Edit)**。

**步骤 7** 选择从该规则收集活动的日志记录级别和频率。下表列出系统日志消息严重性级别。

| 严重性级别 | 说明 |
|---|---|
| 应急 | 系统不可用。 |
| 警报 | 需要立即采取措施。 |
| 严重 | 严重情况。 |

| 严重性级别 | 说明 |
| --- | --- |
| 错误 | 错误情况。 |
| 警告 | 警告情况。 |
| 通知 | 正常但重大的情况。 |
| 信息性 | 消息仅供参考。 |
| 调试 | 消息仅供调试。 |
| **Note** | ASA 不会生成严重性级别为零（紧急）的系统日志消息。 |

**步骤 8** 您还可以更改日志记录间隔。日志记录间隔显示在该间隔内日志被命中的次数。日志记录间隔以秒为单位定义，范围为从 1 到 600。默认值为 300。此值也用作从用于收集丢弃统计信息的缓存中删除非活动的流的超时值。

**步骤 9** 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

**步骤 10** 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

## 定义策略的时间范围

基于时间的ASA网络策略允许基于一天中的时间访问网络和资源。时间由时间范围对象定义。时间范围对象具有开始时间和结束时间，也可以定义为周期性事件。

如果已在 ASA 上定义时间范围对象，则可以将其与网络策略相关联。如果 ASA 上尚不存在时间范围对象，则必须使用 Defense Orchestrator 中的 CLI 工具创建它们，或直接在 ASA 上创建它们。

请按照以下程序为网络策略添加时间范围：

**步骤 1** 选择策略 ASA 策略。 >

**步骤 2** 选择要编辑的网络策略。

**步骤 3** 点击**编辑策略 (Edit Policy)**。

**步骤 4** 在网络策略框中，点击滑块以启用时间范围。

**步骤 5** 创建时间范围对象或从下拉列表中选择现有时间范围对象。

**步骤 6** 点击**保存 (Save)**。

**步骤 7** 返回到设备和服务页面，然后选择您刚刚对其进行策略编辑的设备。您应该会看到设备现在处于“未同步”(Not synced) 状态。

**步骤 8** 点击预览并部署...

**步骤 9** 在设备同步框中，查看将创建策略的命令和策略中的规则。

**步骤 10** 如果您对建议的更改感到满意，请点击将更改应用到设备。

**步骤 11** 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

# 复制 ASA 网络策略

使用此程序可将网络策略从一个 ASA 复制到另一个 ASA。

**步骤 1** 选择策略 ASA 策略。 >

**步骤 2** 搜索并过滤要复制的策略。

**步骤 3** 在要复制的网络策略所在的行中，点击复制图标。

**步骤 4** 将策略添加到设备：

- 对于分配给单个接口的网络策略：在将策略添加到设备对话框中，选择要将策略复制到的设备、接口和流量方向。如果要将全局访问策略复制到另一台设备
- 对于全局策略：在将策略添加到设备对话框中，选择要向其复制策略的设备，然后选中创建为全局策略。您会看到无法为策略选择接口或方向。全局策略始终分配给设备上的所有接口，并始终评估入站流量。

**步骤 5** 点击**保存 (Save)**。

**步骤 6** 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

# 比较 ASA 网络策略

**步骤 1** 在导航窗格中，选择**策略 (Policies) > ASA 策略 (ASA Policies)**。

**步骤 2** 点击查看器右上角的**比较 (Compare)**。

**步骤 3** 最多选择两个要比较的策略。

**步骤 4** 点击查看器底部的**查看比较 (View Comparison)**。这将打开比较查看器。完成后，点击**完成 (Done)**，然后点击**完成比较 (Done Comparing)**。

# 删除 ASA 网络策略

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击 **设备** 选项卡，找到您的设备。

**步骤 3** 点击 ASA 选项卡，搜索要从中删除策略的 ASA 并将其选中。

**步骤 4** 在管理窗格中，点击配置。

**步骤 5** 点击**编辑**。

**步骤 6** 在设备配置中，查找网络策略和规则。

网络策略在 ASA 配置文件中称为访问组，格式如下：

access-group < policy name > < direction of traffic > interface < interface name >

以下是访问组条目的示例：

```
access-group abc-75-1-out interface interface-1
```

网络规则在 ASA 配置文件中称为访问列表，格式如下：

```
access-list <policy name> extended permit ip any any
```

以下是访问列表条目的示例：

```
access-list abc-75-1-out extended permit ip any any
```

**步骤 7** 突出显示并删除包含网络策略的行和包含网络规则的行。

**步骤 8** **保存**更改。

**步骤 9** 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

# 搜索和过滤 ASA 网络策略和规则

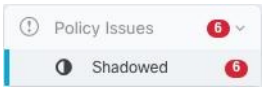
使用搜索栏在网络策略的名称和策略内的规则中搜索名称、关键字或短语。搜索不区分大小写。

### 过滤

使用过滤器边栏查找网络策略问题、共享策略以及特定设备上的策略。过滤不是相加的，每个过滤器设置相互独立。

### 政策问题

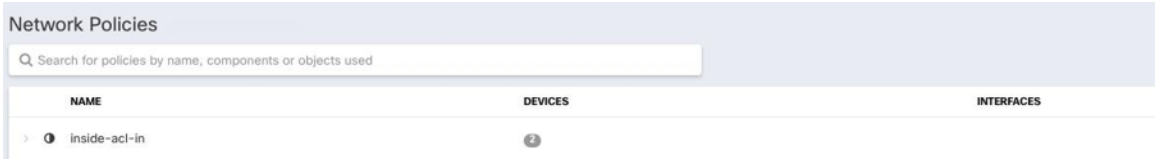
CDO 识别包含影子规则的网络策略。“策略问题”(Policy Issues) 过滤器中会指示包含影子规则的策略数量：




CDO 在网络策略页面上使用影子标记标记包含这些规则的影子规则和网络策略。◑点击已阴影 (Shadowed) 以查看包含阴影规则的所有策略。有关详细信息，请参阅影子规则。

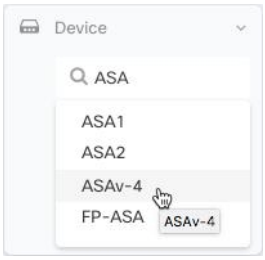
### 共享策略

共享策略是在多台设备上找到的策略。对共享策略所做的更改会影响找到该策略的所有设备。在下面的示例中，inside-acl-in 策略由两台设备共享。有关详细信息，请参阅共享 ASA 网络策略。



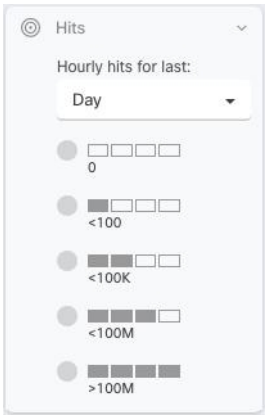
### 设备

通过展开设备过滤器，在搜索设备字段中输入名称或 IP 地址，然后选择在结果中找到的设备，按设备过滤网络策略列表。




### 点击数

使用此过滤器可查找在指定时间段内已触发多次的策略。




## 查找命中数为零的所有网络策略

如果您的网络策略没有任何命中，则可以对其进行编辑以使其更有效，也可以直接将其删除。

**步骤 1** 导航**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

**步骤 2** 在过滤器窗格中，点击全部显示以清除任何现有过滤器。

**步骤 3** 展开 Hits 过滤器。

**步骤 4** 选择一个时间段

**步骤 5** 选择 0 个匹配项。

## 查找设备上命中数为零的所有网络策略

**步骤 1** 导航**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

**步骤 2** 在过滤器窗格中，点击全部显示以清除任何现有过滤器。

**步骤 3** 展开设备过滤器，然后选择要过滤的设备。
**步骤 4** 展开 Hits 过滤器。
**步骤 5** 选择一个时间段
**步骤 6** 选择 0 个匹配项。

## 了解网络策略中的规则被命中的频率

**步骤 1** 导航**策略 (Policies)** > **ASA 策略 (ASA Policies)**。
**步骤 2** 在过滤器窗格中，点击全部显示以清除任何现有过滤器。
**步骤 3** 选择一台设备上使用的网络策略。
**步骤 4** 查看规则表的“命中”列，了解网络策略中每条规则的命中频率。
**步骤 5** 如果网络策略中的规则过多，无法一目了然地查看结果，请展开“命中”(Hits) 过滤器。
**步骤 6** 选择一个时间段
**步骤 7** 选择不同的命中过滤器，查看不同的规则所属的类别。

## 了解共享网络策略的命中频率

针对各个设备计算网络策略命中数。如果不指定过滤器中的设备，您将无法查看在两台或更多设备上共享的单个网络策略的命中率：

**步骤 1** 导航**策略** > **ASA 访问策略**。
**步骤 2** 在策略表上方，点击**清除**以清除任何现有过滤器
**步骤 3** 展开共享策略过滤器，然后点击**共享**。
**步骤 4** 选择共享网络策略。
**步骤 5** 在该策略的详细信息窗格中，记下使用该网络策略的设备，然后返回到网络策略表。
**步骤 6** 在搜索字段中输入共享策略名称。
**步骤 7** 展开设备过滤器，并按使用共享策略的设备之一进行过滤。
**步骤 8** 展开 Hits 过滤器
**步骤 9** 选择一个时间段
**步骤 10** 选择不同的命中过滤器以确定其所属的类别。

## 按命中率过滤网络策略

**步骤 1** 导航策略 ASA 访问策略。 >
**步骤 2** 在策略表上方，点击**清除 (Clear)** 以清除任何现有过滤器。

**步骤 3** 展开 Hits 过滤器。

**步骤 4** 选择时间段。

**步骤 5** 选择不同的命中率类别。CDO 显示以您指定的速率命中的策略。如果存在与命中率条件匹配的共享网络策略，则 CDO 会为使用该共享策略的每个设备显示一行。

# 共享 ASA 网络策略

Cisco Defense Orchestrator (CDO) 可查找多个 ASA 使用的相同网络策略，并在网络策略页面上进行标识。如果您有共享网络策略，则可以对其进行一次更改，并将更改分发到共享该策略的其他设备。这可以使各种设备的网络策略保持一致。

## 共享网络策略属性

网络策略表标识使用网络策略的设备数量。任何表明它被多个设备使用的网络策略都是共享策略。查找共享网络策略：

**步骤 1** 导航**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

**步骤 2** 在过滤器窗格中，点击**全部显示 (Show All)** 以从页面中清除任何过去的过滤或搜索条件。

**步骤 3** 在过滤器栏中，展开共享策略并选择共享。

**步骤 4** 在搜索栏中输入关键字以进一步细化搜索。

**步骤 5** 从网络策略表中选择共享网络策略。

**Note** 过滤器和搜索条件不能组合使用，一次只能使用一个。例如，如果按“共享策略”进行过滤，则会看到所有共享策略。如果将设备名称添加到搜索中，无论策略是否共享，您都会看到该设备名称使用的所有网络策略。

## 编辑共享网络策略

**步骤 1** 查找要编辑的共享策略。共享 ASA 网络策略, on page 188

**步骤 2** 选择共享策略。CDO 标识 CDO 管理的哪些设备使用该网络策略。

**步骤 3** 在详细信息窗格中，点击**编辑策略 (Edit Policy)**。

**步骤 4** 编辑策略中的一个或多个规则。

**步骤 5** 点击**保存 (Save)**。

**步骤 6** **确认**将受更改影响的设备。

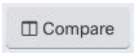
**步骤 7** 打开设备和服务页面，并注意设备不再同步。

**步骤 8** 点击**手动部署更改... (Deploy Changes Manually...)**，然后按照显示的说明使用您的更改更新 ASA 上保存的配置。

## 比较共享网络策略

比较共享网络策略的目的是找到略有差异的策略并重新调整它们。如果您有几个几乎相同的策略，则可能它们已经不同，它们实际上应该是相同的。重新调整网络策略后，CDO 会将这些策略识别为共享策略，当您更改策略时，您将能够使用该策略将更改分发到其他设备。

**步骤 1** 查找要比较的共享策略。共享 ASA 网络策略, on page 188

**步骤 2** 点击**比较 (Compare)** 

。

**步骤 3** 选择要比较的两个网络策略，然后点击查看比较。

**步骤 4** 记下差异，然后点击完成比较。

**步骤 5** 如果要更改其中一个策略以使其与另一个策略保持一致，请从网络策略表中选择该策略，然后点击详细信息窗格中的编辑策略进行编辑。

# ASA 策略（扩展访问列表）

Cisco Defense Orchestrator (CDO) 为用户提供在所有设备上保持网络和应用安全策略一致的能力。借助此独特功能，可以轻松地同时跨多台设备更改策略。

## 访问控制条目 (ACE)

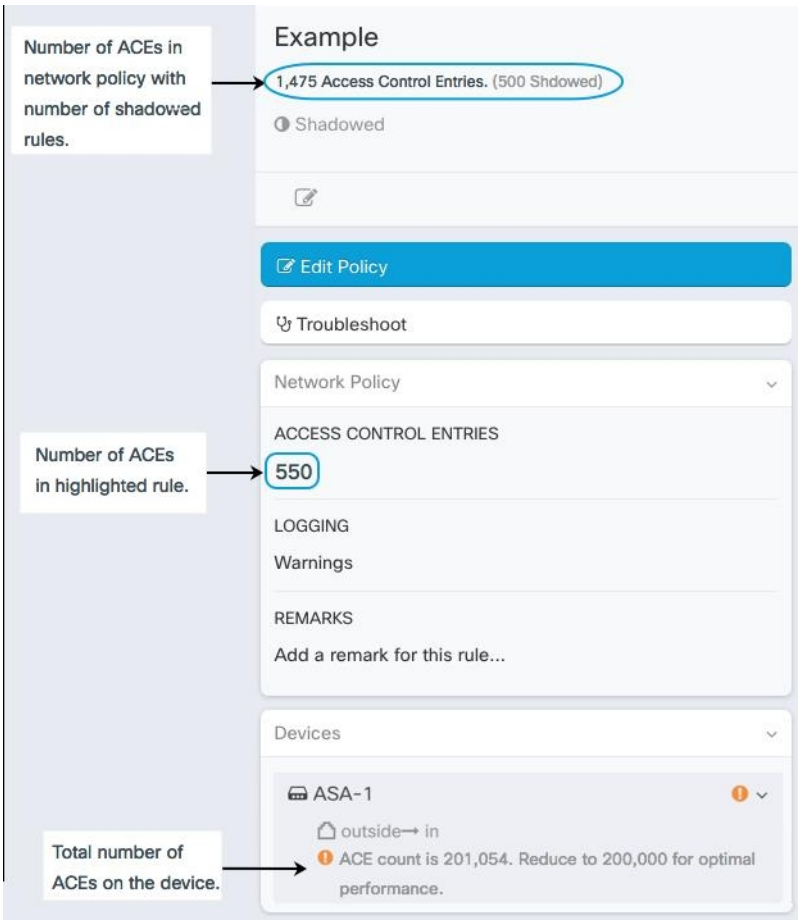
从您可以看到和看不到的方面考虑访问控制条目。

下面是您可以看到的内容。就 CDO 的用户界面而言，添加到网络策略的规则是 ASA 上的访问控制条目。该规则定义允许源地址和目的地址之间或一组地址和另一组地址之间的网络流量。

下面是您无法看到的内容。ASA 会扩展您创建的网络规则，以考虑网络规则隐含的每个可能的源 IP 地址和目标 IP 地址组合。例如，如果有一个规则，其中一个网络对象中的三个 IP 地址被拒绝访问另一个对象中的三个 IP 地址，则 ASA 会在内存中存储 9 个可能的访问控制条目。

ASA 可以处理的 ACE 数量没有硬编码限制，但当 ACE 数量过多时，ASA 性能会下降。请参阅表 4。有关特定 ASA 设备预期的最大 ACE 条目数，请参阅此自适应安全设备常见问题中的“思科 ASA 型号的最大访问控制条目数”。https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-appliance-asa-software/qa_c67-731962.html

CDO 维护从所有网络策略派生的 ACE 总数，并在 ACE 计数超过设备上预期的最大 ACE 限制时通知您。以下是 CDO 提供的信息：




### 减少设备上的 ACE 数量

以下是减少超过预期 ACE 最大数量的设备上的 ACE 数量的一些方法：

- 查找具有部分阴影和完全阴影规则的策略。影子规则，第 194 页如果合适，请删除这些规则。
- 过滤网络策略以查找设备上命中率为零的策略或查找命中率为零的规则。查找设备上命中数为零的所有网络策略，第 186 页了解网络策略中的规则被命中的频率，第 187 页删除命中数为零的策略或规则（如果合适）。
- 查找设备上超过预期访问控制条目数的所有网络策略，并查看这些策略。搜索和过滤 ASA 网络策略和规则，第 185 页考虑这些策略的源和目标寻址是否需要与您最初计划的一样广泛。

# 配置 ASA 全局访问策略

全局访问策略是应用于 ASA 上所有接口的网络策略。这些策略仅适用于入站网络流量。如果要将一组规则统一应用于所有 ASA 接口，请创建全局访问策略。

只能在 ASA 上配置一个全局访问策略。与任何其他策略一样，全局访问策略可以分配多个规则。

ASA 全局访问策略在特定接口的网络策略之后处理，在所有流量的隐式拒绝规则之前处理。以下是 ASA 上的规则处理顺序：

1. 接口访问规则。
2. 对于网桥组成员接口，网桥虚拟接口 (BVI) 访问规则。
3. 全局访问规则。
4. 隐式拒绝。

### 配置 ASA 全局访问策略的限制

CDO 允许您为 ASA 创建和编辑全局访问策略。但是，如果您的 ASA 在将其载入 CDO 时具有全局访问策略，则会受到以下限制：

- 您将能够编辑策略，但无法创建新策略，因为每台设备只允许一个全局访问策略。
- 如果 ASA 上的全局访问策略包含 CDO 不支持的规则，您将无法编辑该策略。
- 您只能使用 CLI 接口或通过编辑设备配置文件来删除策略。

# 创建全球访问策略

**步骤 1** 点击**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

**步骤 2** 在过滤器面板中，过滤策略列表以查找要向其添加全局策略的设备。

**步骤 3** 在“网络策略”表的“接口”列中，确保没有标记为“全局”的策略。

**步骤 4** 点击**创建策略**。

**步骤 5** 点击设备按钮，然后选择要向其添加全局策略的 ASA。点击**选择**。

**步骤 6** 为策略指定名称，然后选中**创建为全局策略**。您会看到无法为策略选择接口或方向。全局策略始终分配给设备上的所有接口，并始终评估入站流量。

**步骤 7** 点击**保存 (Save)**。

**步骤 8** 使用 编辑 ASA 网络策略 将规则添加到新策略。

# 编辑全局访问策略

请牢记上述配置限制，使用“编辑 ASA 网络策略”(Edit an ASA Network Policy) 编辑全局访问策略。
编辑 ASA 网络策略, on page 180

**Note** 如果您发现由于 Edit Policy 按钮已停用而无法编辑全局策略，则可能是因为该策略是在 ASA 上创建的，并且包含具有 CDO 不支持的对象的规则。这些规则在全局访问策略表中不可见。在这种情况下，您需要使用 CDO 的 CLI 工具编辑配置文件，方法是使用 CDO 编辑 ASA 的配置文件，或直接在 ASA 上编辑全局策略。

### 将全局访问策略复制到另一台设备

使用 Copy an ASA Network Policy 将全局访问策略从一台设备复制到另一台设备，或将全局访问策略从一台设备复制到另一台设备上的单个接口。复制 ASA 网络策略, on page 184

### 删除全球访问策略

您无法使用 CDO 的用户界面删除全局访问策略。要删除全局访问策略，您需要使用 CDO 的 CLI 工具在命令行中删除全局访问策略，方法是使用 CDO 编辑 ASA 的配置文件，或直接在 ASA 上编辑全局策略。

# 命中率

CDO 使您能够在安全且可扩展的策略协调之上评估策略规则的结果，提供简单的可视化，以实现更准确的策略分析，并立即可操作地转向根本原因，所有这些都在云的单个窗格中。命中率功能使您能够：

- 消除过时和不匹配的策略规则，提高安全状态。
- 通过即时识别瓶颈以及确保实施正确有效的优先级来优化防火墙性能（例如，大多数触发的策略规则的优先级更高）。
- 在配置的数据保留期（1 年）内维护命中率信息的历史记录，即使在设备或策略规则重置时也是如此。
- 根据可操作的信息，加强对可疑的影子规则和未使用的规则的验证。消除对更新或删除的疑问。
- 在整个策略的上下文中可视化策略规则的使用情况，利用预定义的时间间隔（日、周、月、年）和实际命中的规模（零、> 100、> 100k 等）来评估对通过网络的数据包的影响。

# 查看 ASA 策略的命中率

**步骤 1** 从 CDO 菜单栏中选择策略 ASA 访问策略。 >

**步骤 2** 点击过滤器图标并将其固定为打开状态。

**步骤 3** 在命中 (Hits) 区域中，点击各种命中计数过滤器，以显示哪些策略的命中频率高于或低于其他策略。

# 导出网络策略规则

您可以将每个访问组或加密映射的内容导出到 .csv 文件。This.csv 显示每个访问控制列表 (ACL) 以及 CDO 具有的每个 ACL 的数据。

**步骤 1** 在导航窗格中，点击**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

**步骤 2** （可选）使用搜索和过滤 ASA 网络策略和规则过滤结果。

**步骤 3** 从结果中选择网络策略。

**步骤 4** 点击**导出到 CSV (Export to CSV)** 

。

**步骤 5** CDO 会将您在屏幕上看到的规则导出至 .csv 文件。

# 将 ASA 策略更改应用于设备

当您在 Cisco Defense Orchestrator (CDO) 中修改安全策略时，更改会暂存到受影响的设备或服务。这会导致配置不同步。您可以通过在当前未同步的任何设备或服务上点击部署到设备...来查看并应用策略更改。

## 通过脚本部署到设备

完成 ASA 设备策略配置更改后，需要查看更改并将其应用于设备。

**步骤 1** 导航到设备选项卡，然后点击设备选项卡。

**步骤 2** 点击相应的设备类型选项卡，然后从表中选择修改的设备。配置状态应显示未同步，表示它具有尚未应用于设备的更改。

**步骤 3** 点击右侧栏中的同步，生成将应用于设备的命令，以使其与 CDO 配置处于同步状态。

**步骤 4** 出现提示时，点击下载命令 (Download Commands) 在本地下载命令的副本。这些命令将包含在文本文件中，可以在应用之前进行查看。如果需要，还将生成命令以恢复更改。

**步骤 5** 在 CDO 之外，使用标准协议登录设备，并应用下载的命令。

**步骤 6** 输入所有命令后，返回到 CDO 并再次在设备选项卡上选择修改的设备。

**步骤 7** 点击刷新以确认与 CDO 同步。

如果执行了部分命令或在带外执行了其他命令，则CDO通过打开一个显示差异的窗口来指示差异，并通过提供名为“检测到冲突”的更新状态来提醒用户。

# ASA 策略中的安全组标记

如果您载入的 ASA 在其访问控制规则中使用安全组对象组（以下称为“SGT 组”）中的安全组标记，则思科 Defense Orchestrator 允许您编辑使用这些 SGT 组的规则并管理策略有这些规则。但是，您无法使用 CDO GUI 创建或编辑 SGT 组。要创建或编辑 SGT 组，您需要使用 ASA 的自适应安全设备管理器 (ASDM) 或 CDO 中提供的命令行接口。

在 CDO 的对象页面中，当阅读 SGT 组的详细信息时，您会看到这些对象被标识为系统提供的不可编辑的对象。

CDO 管理员可以对包含 SGT 组的 ACL 和 ASA 策略执行以下任务：

- CDO 管理员可以编辑 ACL 的所有方面，但源和目标安全组除外。
- 将包含 SGT 组的策略从一个 ASA 复制到另一个 ASA。

有关使用命令行接口配置思科 TrustSec 的详细说明，请参阅适用于您的 ASA 版本的《ASA CLI 手册 2：思科 ASA 系列防火墙 CLI 配置指南》的“ASA 和思科 TrustSec”一章。

# 影子规则

具有影子规则的网络策略是指策略中至少有一个规则永远不会触发，因为它前面的规则会阻止数据包被影子规则评估。

例如，请考虑“示例”网络策略中的这些网络对象和网络规则：

```
object network 02-50
range 10.10.10.2 10.10.10.50
object network 02-100
range 10.10.10.2 10.10.10.100
```

```
access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

**此规则不会评估任何流量，**

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

**因为之前的规则**

```
access-list example extended deny ip any4 object 02-50
```

**拒绝任何 ipv4 地址访问 10.10.10.2 - 10.10.10.50 范围内的任何地址。**

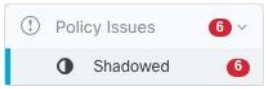
# 查找具有影子规则的网络策略

要查找包含影子规则的网络策略，请使用网络策略过滤器：

**步骤 1** 在导航窗格中，点击**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

**步骤 2** 点击 ASA 访问策略表顶部的过滤器图标。

**步骤 3** 在“策略问题”(Policy Issues) 过滤器中，选中已阴影 (Shadowed) 以查看具有阴影规则的所有策略。




# 解决影子规则的问题

以下是 CDO 显示上述“示例”网络策略中所述规则的方式：

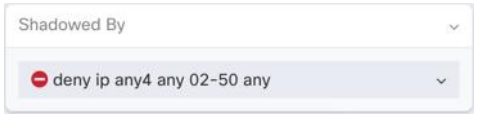

第 1 行的规则标有影子警告标志，因为它会影响策略中的另一条规则。⚠第 2 行的规则被标记为被策略中的另一条规则覆盖。◑第 2 行规则的操作显示为灰色，因为它完全被策略中的另一个规则所掩盖。CDO 能够告诉您策略中的哪条规则会影响第 2 行中的规则。

第 3 行的规则只能在某些时候触发。这是部分阴影规则。任何 IPv4 地址尝试到达 10.10.10.2-10.10.10.50 范围内的 IP 地址的网络流量都不会被评估，因为它已被第一条规则拒绝。但是，任何尝试访问 10.10.10.51-10.10.10.100 范围内的地址的 IPv4 地址都将通过最后一条规则进行评估，并被允许。

**Caution** CDO 不会将影子警告标志应用于部分影子规则。⚠

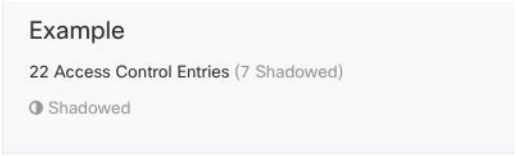
**步骤 1** 选择策略中的影子规则。在上面的示例中，这意味着点击第 2 行。

**步骤 2** 在规则详细信息窗格中，查找Shadowed By 区域。在本示例中，第 2 行中的规则的阴影部分区域显示它被第 1 行中的规则阴影：




**步骤 3** 查看 shadow 规则。是否太宽泛？查看 shadow ed 规则。您真的需要它吗？编辑 shadow 规则或删除 shadow ed 规则。

**Note** 通过删除影子规则，可以减少 ASA 上的访问控制条目 (ACE) 数量。这为创建其他 ACE 的规则释放了空间。CDO 计算从网络策略中的所有规则派生的 ACE 数量，并在网络策略详细信息窗格的顶部显示该总数。如果网络策略中的任何规则被映射，它也会列出该编号。




CDO还显示从网络策略中的单个规则派生的ACE数量，并在网络策略详细信息窗格中显示该信息。以下是该列表的示例：


**步骤 4** 通过查看网络策略详细信息窗格的设备区域，确定哪些设备使用该策略。

**步骤 5** 打开设备和服务页面，然后将更改部署回受策略更改影响的设备。

# 网络地址转换

IP 网络中的每台计算机和设备都分配了标识主机的唯一 IP 地址。因为缺乏公用 IPv4 地址，所以这些 IP 地址中的大多数都是专用地址，在专用公司网络以外的任何地方都不可路由。RFC 1918 定义可以在内部使用但不应通告的专用 IP 地址：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 至 172.31.255.255
- 192.168.0.0 到 192.168.255.255

网络地址转换 (NAT) 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。NAT 以此方式保存公用地址，因为它可配置为至少仅将整个网络的一个公用地址向外界通告。

NAT 的其他功能包括：

- 安全-隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案-使用 NAT 时不会出现重叠 IP 地址。
- 灵活性-可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

您可以使用 Cisco Defense Orchestrator 为许多不同的使用案例创建 NAT 规则。使用 NAT 规则向导或以下主题创建不同的 NAT 规则：

# NAT 规则的处理顺序

网络对象 NAT 和两次 NAT 规则存储在划分为三部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

***Table 15: NAT* 规则表**

| 表部分 | 规则类型 | 部分中的规则顺序 |
|---|---|---|
| 第 1 部分 | 两次 NAT (ASA)<br>手动 NAT (FTD) | 系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保具体规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，两次 NAT 规则会添加到第 1 部分。 |
| 第 2 部分 | 网络对象 NAT (ASA)<br>自动 NAT (FTD) | 如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则：<br>**1.** 静态规则。<br>**2.** 动态规则。<br>**在每个规则类型中，遵循以下排序准则：**<br>**1.** 实际IP地址数量â€”从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。<br>**2.** 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。<br>**3.** 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，先评估对象“Arlington”，然后再评估对象“Detroit”。 |
| 第 3 部分 | 两次 NAT (ASA)<br>手动 NAT (FTD) | 如果仍未找到匹配项，则按照在配置中出现的顺序，应用第三部分规则的第一个匹配项。此部分应当包含最通用的规则。还必须确保此部分的特定规则位于通用规则之前，否则会应用通用规则。 |

例如，对于第二部分规则，在网络对象中定义以下 IP 地址：

- 192.168.1.0/24（静态）
- 192.168.1.0/24（动态）

- 10.1.1.0/24（静态）
- 192.168.1.1/32（静态）
- 172.16.1.0/24（动态）（对象 Drtroit）
- 172.16.1.0/24（动态）（对象 Arlington）

结果排序可能是：

- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 Arlington）
- 172.16.1.0/24（动态）（对象 Drtroit）
- 192.168.1.0/24（动态）

# 网络地址转换向导

网络地址转换 (NAT) 向导可帮助您在设备上为以下类型的访问创建 NAT 规则：

- 为内部用户启用互联网访问。您可以使用此 NAT 规则允许内部网络上的用户访问互联网。
- 向互联网公开内部服务器。您可以使用此 NAT 规则允许网络外部的人员访问内部 Web 或邮件服务器。

### “为内部用户启用互联网访问”的前提条件

在创建 NAT 规则之前，请收集以下信息：

- 最接近用户的接口；这通常称为“内部”接口。
- 离您的互联网连接最近的接口；这通常称为“外部”接口。
- 如果您只想允许特定用户访问互联网，则需要这些用户的子网地址。

### “将内部服务器暴露给互联网”的必备条件

在创建 NAT 规则之前，请收集以下信息：

- 最接近用户的接口；这通常称为“内部”接口。
- 离您的互联网连接最近的接口；这通常称为“外部”接口。
- 要转换为面向互联网的 IP 地址的网络内服务器的 IP 地址。
- 您希望服务器使用的公共 IP 地址。

### 后续操作

请参阅使用 NAT 向导创建 NAT 规则, on page 199。

# 使用 NAT 向导创建 NAT 规则

### Before you begin

有关使用 NAT 向导创建 NAT 规则所需的必备条件，请参阅网络地址转换向导, on page 198。

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 使用过滤器和页面级搜索字段查找要为其创建 NAT 规则的设备。

**步骤 5** 在详细信息面板的**管理 (Management)** 区域中，点击 **NAT** NAT。

**步骤 6** 点击 > NAT 向导。 

**步骤 7** 回答 NAT 向导问题并按照屏幕上的说明进行操作。

- NAT向导创建规则。网络对象,onpage111从下拉菜单中选择现有对象，或使用创建按钮创建新对象。 + Create...
- 在保存 NAT 规则之前，需要将所有 IP 地址定义为网络对象。

**步骤 8** 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

# NAT 常见使用案例

### 两次 NAT 和手动 NAT

以下是使用“网络对象 NAT”（也称为“自动 NAT”）可以实现的一些常见任务：

- 启用内部网络上的服务器以使用公共 IP 地址访问互联网， 第 200 页
- 使内部网络上的用户能够使用外部接口的公共 IP 地址访问互联网， 第 201 页
- 使内部网络上的服务器在公共 IP 地址的特定端口上可用， 第 202 页
- 将专用 IP 地址范围转换为公用 IP 地址范围， 第 206 页

### 网络对象 NAT 和自动 NAT

以下是使用“两次 NAT”（也称为“手动 NAT”）可以实现的常见任务：

- 防止在遍历外部接口时转换某个范围的 IP 地址， 第 207 页

# 启用内部网络上的服务器以使用公共 IP 地址访问互联网

### 使用案例

当您的服务器具有需要从互联网访问的私有 IP 地址，并且您有足够的公共 IP 地址将一个公共 IP 地址转换为私有 IP 地址时，请使用此 NAT 策略。如果您的公共 IP 地址数量有限，请参阅使内部网络上的服务器在公共 IP 地址的特定端口上可用（该解决方案可能更合适）。

### 战略

您的服务器具有静态专用 IP 地址，网络外部的用户必须能够访问您的服务器。创建将静态私有 IP 地址转换为静态公共 IP 地址的网络对象 NAT 规则。之后，创建允许来自该公共 IP 地址的流量到达专用 IP 地址的访问策略。最后，将这些更改部署到您的设备。

### Before you begin

在开始之前，请创建两个网络对象。将一个对象命名为 servername _inside，将另一个对象命名为 _outside。servername _inside 网络对象应包含服务器的专用 IP 地址。servername _outside 网络对象应包含服务器的公共 IP 地址。有关说明，请参阅网络对象。

---

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要为其创建 NAT 规则的设备。

**步骤 5** 点击右侧**管理 (Management)** 窗格中的 **NAT**。

**步骤 6** 点击 > 网络对象 NAT。 

**步骤 7** 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

**步骤 8** 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

**步骤 9** 在第 3 部分“数据包”中，执行以下操作：

**a.** 展开 Original Address 菜单，点击 Choose，然后选择 servername_inside 对象。

**b.** 展开 Translated Address 菜单，点击 Choose，然后选择 servername_outside 对象。

**步骤 10** 跳过第 4 节“高级”。

**步骤 11** 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

**步骤 12** 点击**保存 (Save)**。

**步骤 13** 对于ASA，部署网络策略规则，或者对于FDM管理设备，部署访问控制策略规则，以允许流量从*servername*_inside流向 *servername*_outside。

**步骤 14** 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

---

### ASA 的已保存配置文件中的条目

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

**Note** 这不适用于设备。FDM 管理

**通过此程序创建的对象：**

```
object network servername_outside
host 209.165.1.29
object network servername_inside
host 10.1.2.29
```

**此程序创建的 *NAT* 规则：**

```
object network servername_inside
 nat (inside,outside) static servername_outside
```

# 使内部网络上的用户能够使用外部接口的公共 IP 地址访问互联网

**使用案例**

通过共享外部接口的公共地址，允许专用网络中的用户和计算机连接到互联网。

**战略**

创建端口地址转换 (PAT) 规则，允许专用网络上的所有用户共享设备的外部接口公共 IP 地址。

将私有地址映射到公有地址和端口号后，设备会记录该映射。当收到发往该公共 IP 地址和端口的传入流量时，设备会将其发送回请求它的私有 IP 地址。

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要为其创建 NAT 规则的设备。

**步骤 5** 点击右侧**管理 (Management)** 窗格中的 **NAT**。

**步骤 6** 点击网络对象 NAT。 

**步骤 7** 在第 1 部分中，**键入**选择**动态 (Dynamic)**。点击**继续 (Continue)**。

**步骤 8** 在部分 2 中，为源接口选择 any，为目标接口选择 outside。点击**继续 (Continue)**。

**步骤 9** 在第 3 部分“数据包”中，执行以下操作：

**a.** 展开 Original Address 菜单，点击 Choose 并根据您的网络配置选择 any-ipv4 或 any-ipv6 对象。

**b.** 展开 Translated Address 菜单，然后从可用列表中选择 interface。接口指示使用外部接口的公共地址。

**步骤 10** 对于 FDM 托管设备，在第 5 部分**名称 (Name)**中，为 NAT 规则指定一个名称。

**步骤 11** 点击**保存 (Save)**。

**步骤 12** 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

### ASA 的已保存配置文件中的条目

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

**Note** 这不适用于设备。FDM 管理

**通过此程序创建的对象：**

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

**此程序创建的 *NAT* 规则：**

```
object network any_network
nat (any,outside) dynamic interface
```

# 使内部网络上的服务器在公共 IP 地址的特定端口上可用

### 使用案例

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

### 前提条件

在开始之前，请创建三个单独的网络对象，分别用于 FTP、HTTP 和 SMTP 服务器。出于以下程序的考虑，我们将这些对象称为 ftp-server-object、http-server-object 和 smtp-server-object。有关说明，请参阅创建或编辑 ASA 网络对象和网络组。

## 到 FTP 服务器的 NAT 传入 FTP 流量

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要为其创建 NAT 规则的设备。

**步骤 5** 点击右侧**管理 (Management)** 窗格中的 **NAT**。

**步骤 6** 点击 > 网络对象 NAT。 

**步骤 7** 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

**步骤 8** 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

**步骤 9** 在第 3 部分“数据包”中，执行以下操作：

- 展开 Original Address 菜单，点击 **Choose**，然后选择 **ftp-server-object**。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。

- 选中使用端口转换 **(Use Port Translation)**。
- 选择 **tcp**、**ftp, ftp**。


**步骤 10** 跳过第 4 节“高级”。

**步骤 11** 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

**步骤 12** 点击**保存 (Save)**。新规则在 NAT 表的NAT 规则的处理顺序中创建。

**步骤 13** 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

### ASA 的已保存配置文件中的条目

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

**Note** 这不适用于FDM 管理设备。

### 此程序创建的对象

```
object network ftp-object
host 10.1.2.27
```

### 此程序创建的 *NAT* 规则

```
object network ftp-object
nat (inside,outside) static interface service tcp ftp ftp
```

## 流向 HTTP 服务器的 NAT 传入 HTTP 流量

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

### Before you begin

在开始之前，为 http 服务器创建网络对象。在本程序中，我们将调用对象 **http-object**。有关说明，请参阅创建或编辑 ASA 网络对象和网络组。

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要为其创建 NAT 规则的设备。

**步骤 5** 点击右侧**管理 (Management)** 窗格中的 **NAT**。

**步骤 6** 点击 > 网络对象 NAT。

**步骤 7** 在第 1 部分中，键入选择**静态 (Static)**。点击**继续 (Continue)**。

**步骤 8** 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

**步骤 9** 在第 3 部分“数据包”中，执行以下操作：

- 展开 Original Address 菜单，点击 **Choose**，然后选择 **http** 对象。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。
- 选中**使用端口转换 (Use Port Translation)**。
- 选择 **tcp**、**http**、http。


**步骤 10** 跳过第 4 节“高级”。

**步骤 11** 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

**步骤 12** 点击**保存 (Save)**。新规则在 NAT 表的NAT 规则的处理顺序中创建。

**步骤 13** 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

**ASA 的已保存配置文件中的条目**

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

**Note** 这不适用于FDM 管理设备。

**此程序创建的对象**

```
object network http-object
host 10.1.2.28
```

**此程序创建的 *NAT* 规则**

```
object network http-object
nat (inside,outside) static interface service tcp www www
```

## 到 SMTP 服务器的 NAT 传入 SMTP 流量

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

### Before you begin

在开始之前，为 SMTP 服务器创建网络对象。在本程序中，我们将调用对象 **smtp-object**。有关说明，请参阅创建或编辑 ASA 网络对象和网络组。

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要为其创建 NAT 规则的设备。

**步骤 5** 点击右侧**管理 (Management)** 窗格中的 **NAT**。

**步骤 6** 点击 > 网络对象 NAT。 

**步骤 7** 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

**步骤 8** 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

**步骤 9** 在第 3 部分“数据包”中，执行以下操作：

- 展开 Original Address 菜单，点击 **Choose**，然后选择 smtp-server-object。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。
- 选中**使用端口转换 (Use Port Translation)**。
- 选择 **tcp**、**smtp**、**smtp**。


**步骤 10** 跳过第 4 节“高级”。

**步骤 11** 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

**步骤 12** 点击**保存 (Save)**。新规则在 NAT 表的NAT 规则的处理顺序中创建。

**步骤 13** 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

### ASA 的已保存配置文件中的条目

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

**Note** 这不适用于FDM 管理设备。

#### 此程序创建的对象

```
object network smtp-object
host 10.1.2.29
```

#### 此程序创建的 *NAT* 规则

```
object network smtp-object
nat (inside,outside) static interface service tcp smtp smtp
```

# 将专用 IP 地址范围转换为公用 IP 地址范围

### 使用案例

如果您有一组特定设备类型或用户类型，需要将其 IP 地址转换为特定范围，以便接收设备（事务另一端的设备）允许流量传入。

## 将内部地址池转换为外部地址池

### Before you begin

为要转换的私有 IP 地址池创建网络对象，并为要将这些私有 IP 地址转换为的公有地址池创建网络对象。

对于ASA，“原始地址”池（要转换的私有IP地址池）可以是具有地址范围的网络对象、定义子网的网络对象或包含所有地址的网络组池中。对于 FTD，“原始地址”池可以是定义包含池中所有地址的子网或网络组的网络对象。

**Note** 对于 ASA，定义“转换后的地址”池的网络组不能是定义子网的网络对象。

创建这些地址池时，请使用 Create or Edit ASA Network Objects and Network Groups use Create or Edit a Firepower Network Object or Network Groups 了解相关说明。创建或编辑 ASA 网络对象和网络组, on page 113

出于以下程序的考虑，我们将私有地址池命名为 inside_pool，将公共地址池命名为 outside_pool。

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要为其创建 NAT 规则的设备。

**步骤 5** 点击右侧**管理 (Management)** 窗格中的 **NAT**。

**步骤 6** 点击  > **网络对象 NAT (Network Object NAT)**。

**步骤 7** 在第 1 部分**类型 (Type)** 中，选择**动态 (Dynamic)**，然后点击**继续 (Continue)**。

**步骤 8** 在第 2 部分**接口 (Interfaces)** 中，为源接口选择**内部**内部，为目标接口选择**外部**。点击**继续 (Continue)**。

**步骤 9** 在部分 3 数据包中，执行以下任务：

- 对于 Original Address，请点击**选择 (Choose)**，然后选择您在上述前提条件部分中创建的 **inside_pool** 网络对象（或网络组）。

- 对于 Translated Address，点击**选择 (Choose)**，然后选择您在上述前提条件部分中创建的 **outside_pool** 网络对象（或网络组）。

**步骤 10** 跳过第 4 节“高级”。

**步骤 11** 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

**步骤 12** 点击**保存 (Save)**。

**步骤 13** 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

### ASA 的已保存配置文件中的条目

这些是执行这些程序后将显示在 ASA 的已保存配置文件中的条目。

**Note** 这不适用于设备。FDM 管理

### 通过此程序创建的对象

```
object network outside_pool
    range 209.165.1.1 209.165.1.255
object network inside_pool
    range 10.1.1.1 10.1.1.255
```

### 此程序创建的 *NAT* 规则

```
object network inside_pool
nat (inside,outside) dynamic outside_pool
```

# 防止在遍历外部接口时转换某个范围的 IP 地址

### 使用案例

使用此两次 NAT 使用案例启用站点间 VPN。

### 策略

您将 IP 地址池转换为自身，以便网络上一个位置的 IP 地址到达另一个位置时保持不变。

## 创建两次 NAT 规则

### Before you begin

创建定义要转换为自身的 IP 地址池的网络对象或网络组。对于 ASA，地址范围可以通过使用 IP 地址范围的网络对象、定义子网的网络对象或包含该范围内所有地址的网络组对象来定义。

创建网络对象或网络组时，请使用创建或编辑 ASA 网络对象和网络组获取说明。

在以下程序中，我们将调用网络对象或网络组，即站点间 PC 池。

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要为其创建 NAT 规则的设备。

**步骤 5** 点击右侧**管理 (Management)** 窗格中的 **NAT**。

**步骤 6** 点击  > **两次 NAT (Twice NAT)**。。

**步骤 7** 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

**步骤 8** 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

**步骤 9** 在第 3 部分**数据包**中，进行以下更改：

- 展开原始地址菜单，点击**Choose**，然后选择您在先决条件部分中创建的站点到站点 PC 池对象。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择您在前提条件部分中创建的 Site-to-Site-PC-Pool 对象。

**步骤 10** 跳过第 4 节“高级”。

**步骤 11** 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

**步骤 12** 点击**保存 (Save)**。

**步骤 13** 为 ASA 创建一个加密映射。有关创建加密映射的详细信息，请参阅《CLI 手册 3：思科 ASA 系列 VPN CLI 配置指南》并查看 LAN 到 LAN IPsec VPN 一章。

**步骤 14** 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

#### ASA 的已保存配置文件中的条目

这些是执行这些程序后将显示在 ASA 的已保存配置文件中的条目。

**Note** 这不适用于设备。FDM 管理

#### 通过此程序创建的对象

```
object network Site-to-Site-PC-Pool
range 10.10.2.0 10.10.2.255
```

#### 此程序创建的 *NAT* 规则

```
nat (inside,outside) source static Site-to-Site-PC-Pool Site-to-Site-PC-Pool
```

# 在 CDO 中管理虚拟专用网络管理

虚拟专用网络 (VPN) 连接在使用公共网络（如互联网）的终端之间建立安全隧道。

本节适用于自适应安全设备 (ASA) 设备上的远程访问和站点间 VPN。它还介绍了用于在 ASA FTD 上构建和远程访问 VPN 连接的 SSL 标准。

CDO 支持以下几种类型的 VPN 配置：



# 站点间虚拟专用网络简介

站点间VPN隧道可连接不同地理位置的网络。您可以在托管设备之间以及托管设备与其他符合所有相关标准的思科或第三方对等体之间创建站点间的IPsec连接。这些对等体可以采用内部和外部IPv4和IPv6地址的任意组合。站点间隧道使用 Internet Protocol Security (IPsec) 协议套件或网络密钥交换版本 2 (IKEv2) 构建。建立 VPN 连接之后，本地网关后台的主机可通过安全 VPN 隧道连接至远程网关后台的主机。

### VPN 拓扑

要创建一个新的站点间VPN拓扑，至少必须为其指定一个唯一名称，指定拓扑类型，选择用于IPsec IKEv1 和/或 IKEv2 的 IKE 版本。配置完毕后，可以将拓扑部署到 ASA。

### IPsec 和 IKE 协议

在 CDO 中，站点间 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议配置的。策略和建议是定义站点到站点 VPN 的特性的参数集，例如用于在 IPsec 隧道中保护流量安全的安全协议和算法。可能需要多种策略类型来定义可以分配给 VPN 拓扑的完整配置映像。

### 身份验证 VPN 隧道

要对VPN连接进行身份验证，请在每个设备上拓扑中配置预共享密钥。预共享密钥允许在两个对等体之间共享安全密钥，该共享密钥在 IKE 身份验证阶段使用。

### VPN 加密域

有两种方法可以定义 VPN 的加密域：路由型或策略型流量选择器。

- **策略型**：加密域设置为允许任何流量进入 IPSec 隧道。IPSec 本地和远程流量选择器会被设为 0.0.0.0。这意味着无论源/目标子网如何，路由到 IPSec 隧道的任何流量都会被加密。ASA 支持具有加密映射的策略型 VPN。
- **路由型**：加密域设置为仅加密源和目标的特定 IP 范围。它会创建一个虚拟 IPsec 接口，并且会加密和解密进入该接口的任何流量。ASA 通过使用虚拟隧道接口 (VTI) 来支持路由型 VPN。

### 关于外联网设备

您可以将非思科或非托管思科设备作为具有静态或动态IP地址的“外联网”设备添加到VPN拓扑。

- 非思科设备：不能使用 CDO 来创建配置以及将配置部署到非思科设备。
- 非托管思科设备：并非由贵公司管理的思科设备，例如，由您公司内的其他部门管理的网络中的分支，或者与服务提供商或合作伙伴的网络的连接。

相关信息：

- ASA 站点间 VPN 配置, on page 210
- 监控 ASA 站点间虚拟专用网络

# ASA 站点间 VPN 配置

Cisco Defense Orchestrator (CDO) 支持自适应安全设备 (ASA) 设备上的站点间 VPN 功能：

- 支持 IPsec IKEv1 和 IKEv2 协议。
- 用于身份验证的自动或手动预共享密钥。
- IPv4 和 IPv6。支持内部和外部的所有组合。
- IPsec IKEv2 站点间 VPN 拓扑提供符合安全认证的配置设置。
- 静态和动态接口。
- 支持作为终端的外联网设备的静态或动态 IP 地址。

### 配置与动态寻址对等体的站点间 VPN 连接

如果其中一个对等体的 VPN 接口 IP 地址未知或接口从 DHCP 服务器获取其地址，CDO 允许您在对等体之间创建站点间 VPN 连接。预共享密钥、IKE 设置和 IPsec 配置与另一个对等体匹配的任何动态对等体都可以建立站点间 VPN 连接。

假设有两个对等体 A 和 B。静态对等体是其 VPN 接口为固定 IP 地址的设备，而动态对等体是其 VPN 接口为未知 IP 地址或具有临时 IP 地址的设备。

以下使用案例介绍了与动态寻址对等体建立安全站点间 VPN 连接的不同场景：

- A 是静态对等体，而 B 是动态对等体，反之亦然。
- A 是静态对等体，而 B 是具有来自 DHCP 服务器的已解析 IP 地址的动态对等体，反之亦然。
- A 是动态对等体，而 B 是具有静态或动态 IP 地址的外联网设备。
- A 是具有来自 DHCP 服务器的已解析 IP 地址的动态对等体，而 B 是具有静态或动态 IP 地址的外联网设备。

注释 如果使用自适应安全设备管理器 (ASDM) 等本地管理器更改了接口的 IP 地址，则 CDO 中该对等体的**配置状态 (Configuration Status)** 会显示“检测到冲突”(Conflict Detected)。当您解决“检测到冲突”状态时，其他对等体的**配置状态 (Configuration Status)** 会变成“未同步”(Not Synced) 状态。您必须将 CDO 配置部署到处于“未同步”(Not Synced) 状态的设备。

通常，连接必须由动态对等体发起，因为另一个对等体不知道动态对等体的 IP 地址。当远程对等体尝试建立连接时，另一个对等体会使用预共享密钥、IKE 设置和 IPsec 配置来验证连接。

由于只有在远程对等体发起连接之后才会建立VPN连接，因此在连接建立之前，系统会丢弃与允许流量通过 VPN 隧道的访问控制规则匹配的出站流量。这可确保数据不会在未采取适当加密和 VPN 保护措施的情况下离开您的网络。

注释 在以下情况下，无法配置站点间 VPN 连接：

如果设备有多个动态对等体连接。

- 考虑三台设备 A、B 和 C。
- 配置 A（静态对等体）和 B（动态对等体）之间的站点间 VPN 连接。
- 通过创建外联网设备来配置 A 和 C（动态对等体）之间的 VPN 连接。将 A 的静态 VPN 接口 IP 地址分配给外联网设备，并与 C 建立连接。

### 站点间 VPN 指南和限制

- CDO 不支持使用 crypto-acl 来设计 S2S VPN 需要关注的流量。它仅支持受保护的网络。
- 只要使用的是 IKE 端口 500/4500，或者有一些 PAT 转换处于活动状态，则无法在同一端口上配置站点间 VPN，因为无法在这些端口上启动服务。
- 不支持传输模式，仅支持隧道模式。IPsec 隧道模式对整个原始 IP 数据报进行加密，使其成为新 IP 数据包中的负载。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPsec。
- 对于此版本，仅支持包含一个或多个 VPN 隧道的 PTP 拓扑。点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。

### Virtual Tunnel Interface 准则

- VTI 只有在 IPsec 模式下才可配置。不支持在 ASA 上终止 GRE 隧道。
- 可以将动态或静态路由用于使用这种隧道接口的流量。
- VTI 的 MTU 将根据底层物理接口自动设置。但是，如果在启用 VTI 后更改物理接口 MTU，则您必须禁用并重新启用 VTI 才能使用新的 MTU 设置。
- 如果必须应用网络地址转换，则将 IKE 和 ESP 数据包封装在 UDP 报头中。
- 无论隧道中的数据流量如何，IKE 和 IPsec 安全关联都将不断重新生成密钥。这可确保 VTI 隧道始终处于活动状态。
- 隧道组名称必须与对等体作为其 IKEv1 或 IKEv2 身份发送的内容相符。
- 对于 LAN 间隧道组中的 IKEv1，仅当隧道身份验证方法为数字证书和/或对等体配置为使用积极模式时，才能使用非 IP 地址的名称。

- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地址不同，VTI 和加密映射配置就可以在同一个物理接口上共存。
- 默认情况下，通过 VTI 的所有流量都经过加密。
- 默认情况下，VTI 接口的安全级别为 0。
- 可以在 VTI 接口上应用访问列表来控制通过 VTI 的流量。
- 仅 VTI 上支持 BGP。
- 如果 ASA 终结 IOS IKEv2 VTI 客户端，请禁用 IOS 上的配置交换请求，因为 ASA 无法为由 IOS VTI 客户端发起的 L2L 会话检索 mode-CFG 属性。
- 不支持 IPv6。

**相关信息：**

- 创建 ASA 站点间 VPN 隧道， 第 214 页
- VPN 中使用的加密和散列算法
- 从 NAT 豁免远程访问流量， 第 264 页

## VPN 中使用的加密和散列算法

由于VPN隧道通常流经公共网络（最可能是互联网），因此您需要对连接进行加密以保护流量。可以使用 IKE 策略和 IPsec 提议定义要应用的加密和其他安全技术。

如果您的设备许可证允许应用较强的加密，则有大量的加密和散列算法以及Diffie-Hellman组供您选择。然而，通常情况下，应用于隧道的加密越强，系统性能越差。您要在安全性和性能之间实现平衡，在提供充分保护的同时不牺牲效率。

我们无法就选择哪些选项提供具体指导。如果您在大型公司或其他组织执行运营，可能已有需要满足的指定标准。如果没有，请花些时间研究各个选项。

下面的主题介绍了几个可用选项：

### 决定使用哪个加密算法

在决定用于 IKE 策略或 IPsec 提议的加密算法时，您的选择仅限于 VPN 中的设备所支持的算法。

对于 IKEv2，您可以配置多个加密算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

对于 IPsec 提议，该算法用于封装安全协议 (ESP)，该协议提供身份验证、加密和防重放服务。ESP 为 IP 协议类型 50。在 IKEv1 IPsec 提议中，算法名称以 ESP 为前缀。

如果设备许可证符合强加密要求，可以从以下加密算法中选择。如果不符合强加密要求，则只能选择 DES。

- AES-GCM -（仅限 IKEv2。）Galois/Counter 模式中的高级加密标准是提供机密性和数据源身份验证的分组加密操作模式，并且提供比 AES 更高的安全性。AES-GCM 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。

GCM 是支持 NSA Suite B 所需的 AES 模式。NSA Suite B 是一套加密算法，设备必须支持这套算法才能满足密码强度的联邦标准。

- AES-GMAC -（仅限 IKEv2 IPsec 提议。）高级加密标准 Galois 消息身份验证代码是仅提供数据源身份验证的分组加密操作模式。它是 AES-GCM 的一个变体，允许在不加密数据的情况下进行数据身份验证。AES-GMAC 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。
- AES - 高级加密标准是一种对称密码算法，提供比 DES 更高的安全性，在计算上比 3DES 更高效。AES 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。
- DES - 数据加密标准，使用 56 位密钥进行加密，是一种对称密钥块算法。如果您的许可证账户不符合导出控制要求，这将是您唯一的选择。此算法比 3DES 快且使用的系统资源更少，但安全性也较低。如果不需要很强的数据保密性，并且系统资源或速度存在问题，请选择 DES。
- 3DES - 三重 DES，使用 56 位密钥加密三次，比 DES 更加安全，因其使用不同密钥对每个数据块处理三次。不过，此算法比 DES 使用的系统资源更多且速度更慢。
- NULL - 空加密算法提供不加密的身份验证。这通常仅用于测试目的。

### 决定使用哪些散列算法

在 IKE 策略中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，散列算法分成两个选项，一个用于完整性算法，一个用于伪随机函数 (PRF)。

在 IPsec 提议中，散列算法由封装安全协议 (ESP) 用于身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀，并且还有 -HMAC 后缀（代表“散列方法身份验证代码”）。

对于 IKEv2，您可以配置多个散列算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

您可以选择以下散列算法：

- SHA （安全散列算法）- 生成 160 位摘要的标准 SHA (SHA-1)。SHA 抗暴力攻击的能力高于 MD5。但是，它也比 MD5 占用更多资源。对于需要最高级别安全性的实施，请使用 SHA 散列算法。
- 以下 SHA-2 选项更加安全，可用于 IKEv2 配置。如果要实施 NSA Suite B 加密规范，请选择以下选项之一。
  - SHA-256 - 指定具有 256 位摘要的安全散列算法 SHA-2。
  - SHA-384 - 指定具有 384 位摘要的安全散列算法 SHA-2。
  - SHA-512 - 指定具有 512 位摘要的安全散列算法 SHA-2。
- MD5（消息摘要 5）- 生成 128 位的摘要。MD5 能使用更少的处理时间实现比 SHA 更快的整体性能，但 MD5 被认为安全性低于 SHA。

- 空或无（NULL、ESP-NONE）-（仅限 IPsec 提议。）空散列算法；这通常仅用于测试目的。但是，如果选择 AES-GCM/GMAC 选项之一作为加密算法，则应选择空完整性算法。即使选择非空选项，这些加密标准也会忽略完整性散列。

#### 决定要使用的 Diffie-Hellman 模数组

您可以使用以下 Diffie-Hellman 密钥导出算法生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数更大则安全性越高，但需要更多的处理时间。两个对等体上必须具有一个匹配的模数组。

如果选择 AES 加密，要支持 AES 所需的大型密钥长度，应使用 Diffie-Hellman (DH) 组 5 或更高组。IKEv1 策略不支持下面列出的所有组。

要实施 NSA Suite B 加密规范，请使用 IKEv2 并选择椭圆曲线 Diffie-Hellman (ECDH) 的一个选项：19、20 或 21。使用 2048 位模数的椭圆曲线选项和组较少遭受 Logjam 等攻击。

对于 IKEv2，您可以配置多个组。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

- 2 - Diffie-Hellman 组 2：1024 位模幂算法 (MODP) 组。此选项不再是一种良好的保护措施。
- 5 - Diffie-Hellman 组 5：1536 位 MODP 组。曾经被认为可以良好地保护 128 位密钥，如今却不再是一种良好的保护措施。
- 14 - Diffie-Hellman 组 14：2048 位模幂算法 (MODP) 组。被认为可以良好地保护 192 位密钥。
- 19 - Diffie-Hellman 组 19：美国国家标准与技术研究所 (NIST) 256 位椭圆曲线取素数 (ECP) 组。
- 20 - Diffie-Hellman 组 20： NIST 384 位 ECP 组。
- 21 - Diffie-Hellman 组 21： NIST 521 位 ECP 组。
- 24 - Diffie-Hellman 组 24：带 256 位素数阶子组的 2048 位 MODP 组。我们不再建议采用此选项。

#### 确定使用哪种身份验证方法

您可以使用以下方法对站点间 VPN 连接中的对等体进行身份验证。

#### 预共享密钥

预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。这些密钥由 IKE 在身份验证阶段使用。对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。对于 IKEv2，您可以在每个对等体上配置唯一密钥。

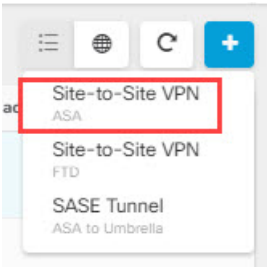
与证书相比，预共享密钥的扩展性相对逊色。如果需要配置大量的站点间VPN连接，请使用证书而非预共享密钥。

## 创建 ASA 站点间 VPN 隧道

使用以下程序在两个 ASA 或具有外联网设备的 ASA 之间创建站点间 VPN 隧道：

**步骤 1** 在导航窗格中，选择 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

**步骤 2** 点击右上角的蓝色加号  ，然后点击**站点间 VPN (Site-to-Site VPN)** 和 ASA 标签。




**步骤 3** 在**配置名称 (Configuration Name)** 字段中，输入您创建的站点间 VPN 配置的名称。

**步骤 4** 选择以下选项之一，以便创建新的**策略型**或**路由型**站点间 VPN。

**步骤 5** 在**对等设备 (Peer Devices)** 部分中，执行以下操作：

a) **对等体 1 (Peer 1)**：选择 ASA 设备，然后点击**选择 (Select)**。

b) **对等体 2 (Peer 2)**：选择其他 ASA 设备，然后点击**选择 (Select)**。

**外联网 (Extranet)**：如果要在对等体 2 中选择外联网设备，请点击外联网滑块将其启用。

选择**静态 (Static)**，并指定 IP 地址，或为使用 DHCP 分配 IP 的外联网设备选择**动态 (Dynamic)**。**IP 地址 (IP Address)** 显示静态接口的 IP 地址或为动态接口**分配的 DHCP (DHCP Assigned)**。

c) 为终端设备选择 **VPN 访问接口** 。

d) （适用于路由型 VPN）选择控制 LAN 子网的 **LAN 接口**。您可以选择多个接口。

连接到所选 LAN 接口的网络将被添加到路由策略访问列表中。匹配路由策略访问列表的流量将由 VPN 隧道进行加密/解密。

e) 点击**添加网络 (Add Network)**，为参与的设备添加**受保护的网络 (Protected Networks)**。受保护的网络被定义为受此 VPN 终端保护的网络。

f) （可选且适用于策略型）选择 **NAT 免除 (NAT Exempt)** 以便从本地 VPN 访问接口的 NAT 策略中免除 VPN 流量。必须为单个对等体手动配置。如果不想将 NAT 规则应用于本地网络，请选择托管本地网络的接口。此选项仅在本地网络驻留在单个路由接口（而非网桥组成员）后时有用。如果本地网络位于多个路由接口或一个或多个网桥组成员之后，则必须手动创建 NAT 豁免规则。有关手动创建所需规则的信息，请参阅从 NAT 豁免 ASA 站点间 VPN 流量。

g) 点击**下一步**。

**步骤 6** （适用于路由型）在**隧道详细信息 (Tunnel Details)** 中，一旦在上一步中配置了对等设备，就会自动填充 **VTI 地址 (VTI Address)** 字段。如有必要，您可以手动输入要用作新 VTI 的 IP 地址。

**步骤 7** 在 **IKE 设置 (IKE Settings)** 部分中，选择要在互联网密钥交换 (IKE) 协商期间使用的 IKE 版本，并指定隐私配置：有关 IKE 策略的详细信息，请参阅关于全局 IKE 策略。

根据用户所做的配置，CDO 会建议 IKE 设置。您可以继续使用建议的 IKE 配置设置，也可以定义新的配置设置。

**注释** IKE 策略对设备是全局的，并应用于与其关联的所有 VPN 隧道。因此，添加或删除策略会影响此设备参与的所有 VPN 隧道。

a) 根据需要选择一个或两个 IKE 版本。

默认情况下，**IKEV 版本 2** 处于启用状态。

注释 不允许对路由型 VPN 启用两个 IKE 版本。

b) 点击**添加 IKEv2 策略 (Add IKEv2 Policy)**，然后选择 IKEv2 策略

注释 点击 **创建新的 IKEv2 策略** 以创建新的 IKEv2 策略。有关创建新 IKEv2 策略的详细信息，请参阅管理 IKEv2 策略。要删除现有 IKEv2 策略，请将鼠标悬停在所选策略上，然后点击 x 图标。

c) 输入参与设备的**预共享密钥**。预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。IKE在身份验证阶段使用这些密钥。

(IKEv2) **对等体 1 预共享密钥、对等体 2 预共享密钥**：对于 IKEv2，您可以在每个对等体上配置唯一的密钥。输入**预共享密钥 (Pre-shared Key)**。您可以点击显示按钮，并为对等体输入适当的预共享。该密钥可以有 1 至 127 个字母数字字符。下表介绍了两个对等体的预共享密钥的用途。

| | 本地预共享密钥 | 远程对等预共享密钥 |
|---|---|---|
| **对等体 1** | 对等体 1 预共享密钥 | 对等体 2 预共享密钥 |
| **对等体 2** | 对等体 2 预共享密钥 | 对等体 1 预共享密钥 |

d) 点击 **IKE 版本 1** 以启用它。

e) 点击**添加 IKEv1 策略 (Add IKEv1 Policy)**，然后选择 IKEv1 策略。点击 **创建新的 IKEv1 策略** 以创建新的 IKEv1 策略。有关创建新 IKEv1 策略的详细信息，请参阅 管理 IKEv1 策略。要删除现有 IKEv1 策略，请将鼠标悬停在所选策略上，然后点击 x 图标。

f) (IKEv1) **预共享密钥**：对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。该密钥可以有 1 至 127 个字母数字字符。在此场景中，对等体 1 和对等体 2 使用相同的预共享密钥加密和解密数据。

g) 点击**下一步**。

**步骤 8** 在 **IPSec 设置 (IPSec Settings)** 部分，根据用户所做的配置，CDO 会建议 IKEv2 提议。您可以继续使用建议的 IKE 配置设置，也可以定义新的配置设置。有关 IPSec 设置的详细信息，请参阅配置 IPsec 提议。

a) 点击**+ IKEv2 提议 (+ IKEv2 Proposals)** 以选择 IPSec 配置。相应的 IKEV 提议是否可用，具体取决于在 **IKE 设置** 步骤中所做的选择。要删除现有的 IKEv2 提议，请将鼠标悬停在所选提议上，然后点击 x 图标。

注释 点击**创建新的 IKEv2 提议 (Create New IKEv2 Proposals)** 以创建新的 IKEv2 提议。有关创建新 IKEv2 策略的详细信息，请参阅关于 IPSec 提议。

b) 选择**适用于完全向前保密的 Diffie-Hellman 组 (Diffie-Hellman Group for Perfect Forward Secrecy)**。有关详细信息，请参阅VPN 中使用的加密和散列算法，第 212 页

c) 点击**下一步**。

**步骤 9** 在**完成**部分中，请阅读配置，并在您对配置满意时继续操作，然后点击**提交 (Submit)**。

---

您将被定向到“VPN 隧道” (VPN Tunnels)页面，该页面显示新配置的站点间 VPN 隧道。这些更改已暂存，并且必须手动部署。系统会创建路由策略，以便通过 VTI 隧道在设备之间自动路由 VTI 流

量。要查看此策略，请从**清单 (Inventory)** 页面中选择设备，然后选择**配置 (Configuration)** > **差异 (Diff)**。

请参阅部署使用 CDO GUI 进行的配置更改部分，在与新隧道关联的设备上部署站点间 VPN 配置。

## 删除 CDO 站点间 VPN 隧道

**步骤 1** 在导航栏上，选择 **VPN**> **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

**步骤 2** 选择要删除的所需站点间 VPN 隧道。

**步骤 3** 在**操作 (Actions)** 窗格中，点击**删除 (Delete)**。

所选站点间 VPN 隧道将被删除。

## 使站点间 VPN 流量豁免 NAT

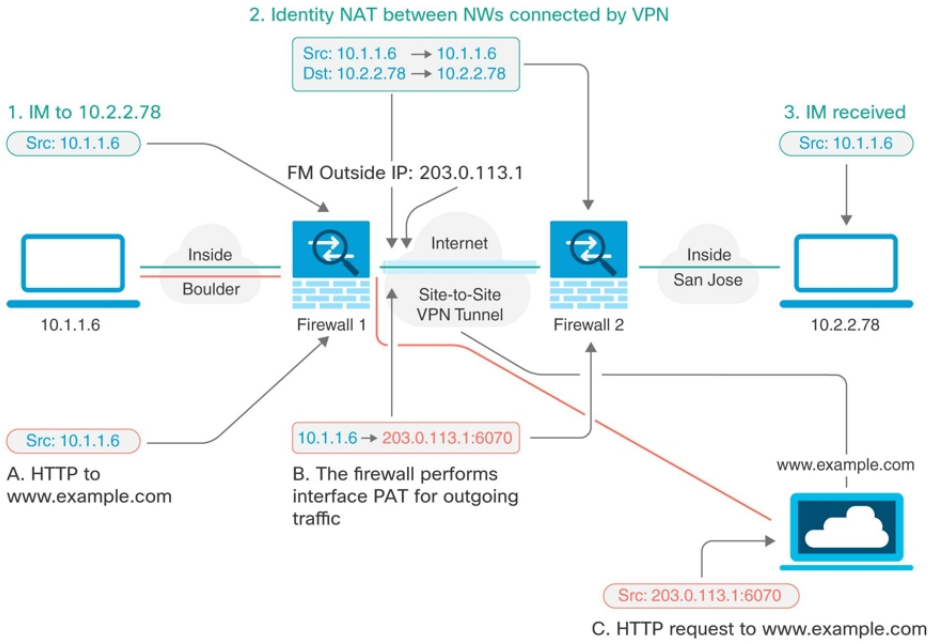
当您在某个接口上定义了站点间 VPN 连接并且还对该接口实施了 NAT 规则时，可以选择使该 VPN 上的流量豁免 NAT 规则。如果 VPN 连接的远端可以处理您的内部地址，则可能要执行此操作。

创建 VPN 连接时，可以选择 **NAT 豁免**选项自动创建 NAT 豁免规则。不过，此操作仅在通过单个路由接口（而非网桥组成员）连接本地受保护网络时才奏效。相反，如果该连接中的本地网络位于两个或多个路由接口之后或者一个或多个网桥组成员之后，则需要手动配置 NAT 豁免规则。

要使 VPN 流量豁免 NAT 规则，需要为目的是远程网络时的本地流量创建身份手动 NAT 规则。然后，将NAT应用于目的是其他网络（例如互联网）时的流量。如果本地网络有多个接口，请为每个接口分别创建规则。也可以考虑以下建议：

- 如果连接中有多个本地网络，请创建一个网络对象组用于容纳定义这些网络的对象。
- 如果 VPN 中同时包括 IPv4 和 IPv6 网络，请为其各创建一个单独的身份 NAT 规则。

下例显示连接博尔德办公室和圣荷西办公室的站点间隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口端口地址转换 (PAT) 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中的 10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 将地址转换为其相同的地址。




以下示例说明 Firewall1（博尔德办公室）的配置。该示例假定内部接口是网桥组，因此需要为每个成员接口编写规则。如果有一个或多个路由内部接口，其过程相同。

**Note** 此示例假定只包括 IPv4 网络。如果该 VPN 还包括 IPv6 网络，请为 IPv6 创建并行规则。请注意，由于无法实施 IPv6 接口 PAT，因此需要使用唯一 IPv6 地址创建主机对象用于 PAT。

**步骤 1** 创建对象来定义各种网络。

**a.** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

**b.** 点击蓝色加号按钮  以创建新的对象。

**c.** 点击 **ASA** > **网络**。

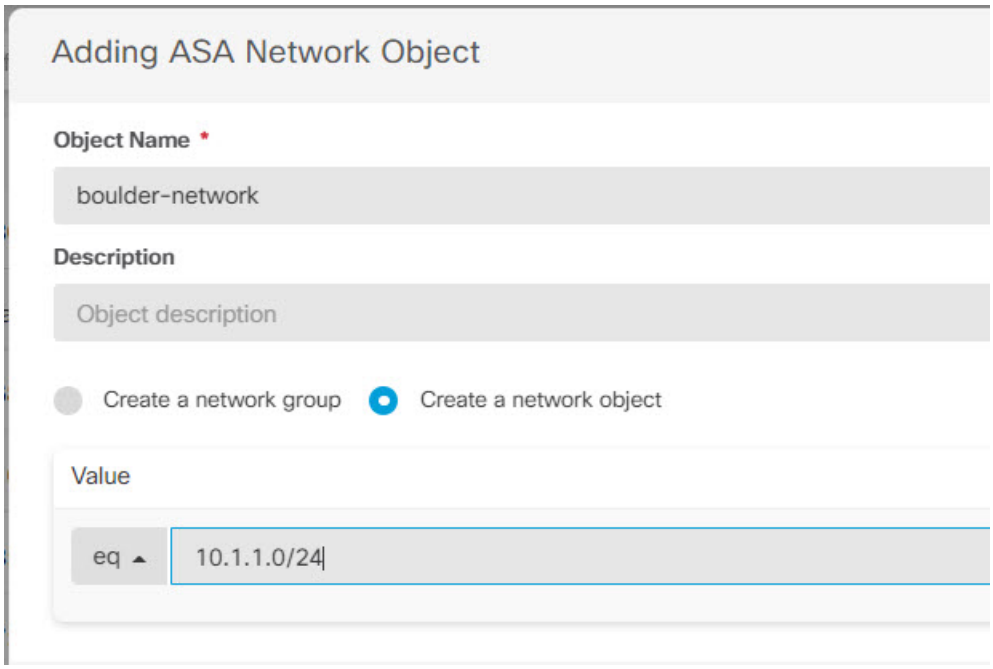
**d.** 找到博尔德办公室内部网络。

**e.** 输入对象名称（例如，boulder-network）。

**f.** 选择 **创建网络对象**。

**g.** 在“值”部分：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址或子网地址。
- 选择 **范围** 并输入 IP 地址范围。例如，输入网络地址 10.1.1.0/24。




**h.** 点击**添加 (Add)**。

**i.** 点击蓝色加号按钮  以创建新的对象。

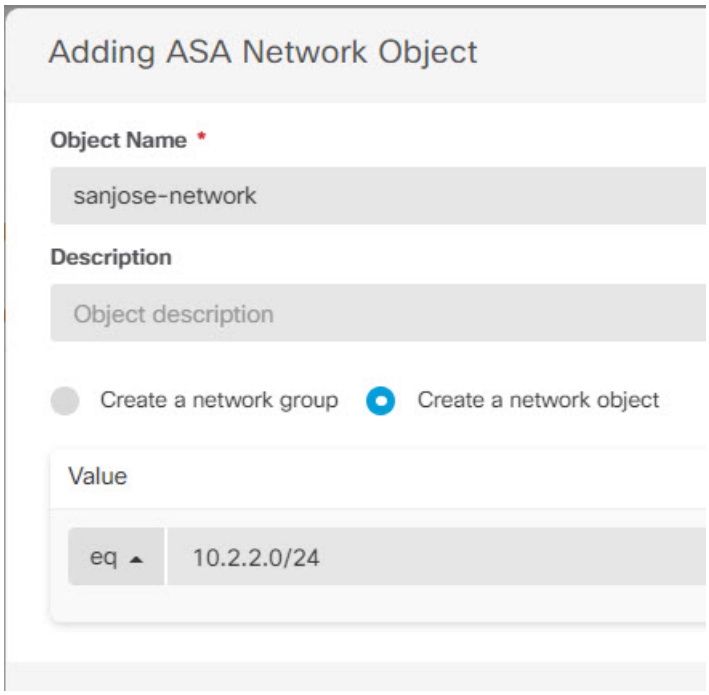
**j.** 定义内部圣荷西办公室网络。

**k.** 输入对象名称（例如，san-jose）。

**l.** 选择 **创建网络对象**。

**m.** 在“值”部分：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址或子网地址。
- 选择 **范围** 并输入 IP 地址范围。例如，输入网络地址 10.1.1.0/24。




**n.** 点击**添加 (Add)**。

**步骤 2** 在 Firewall1（博尔德办公室）上，为博尔德办公室网络配置经过 VPN 连接到圣荷西办公室时的手动身份 NAT。

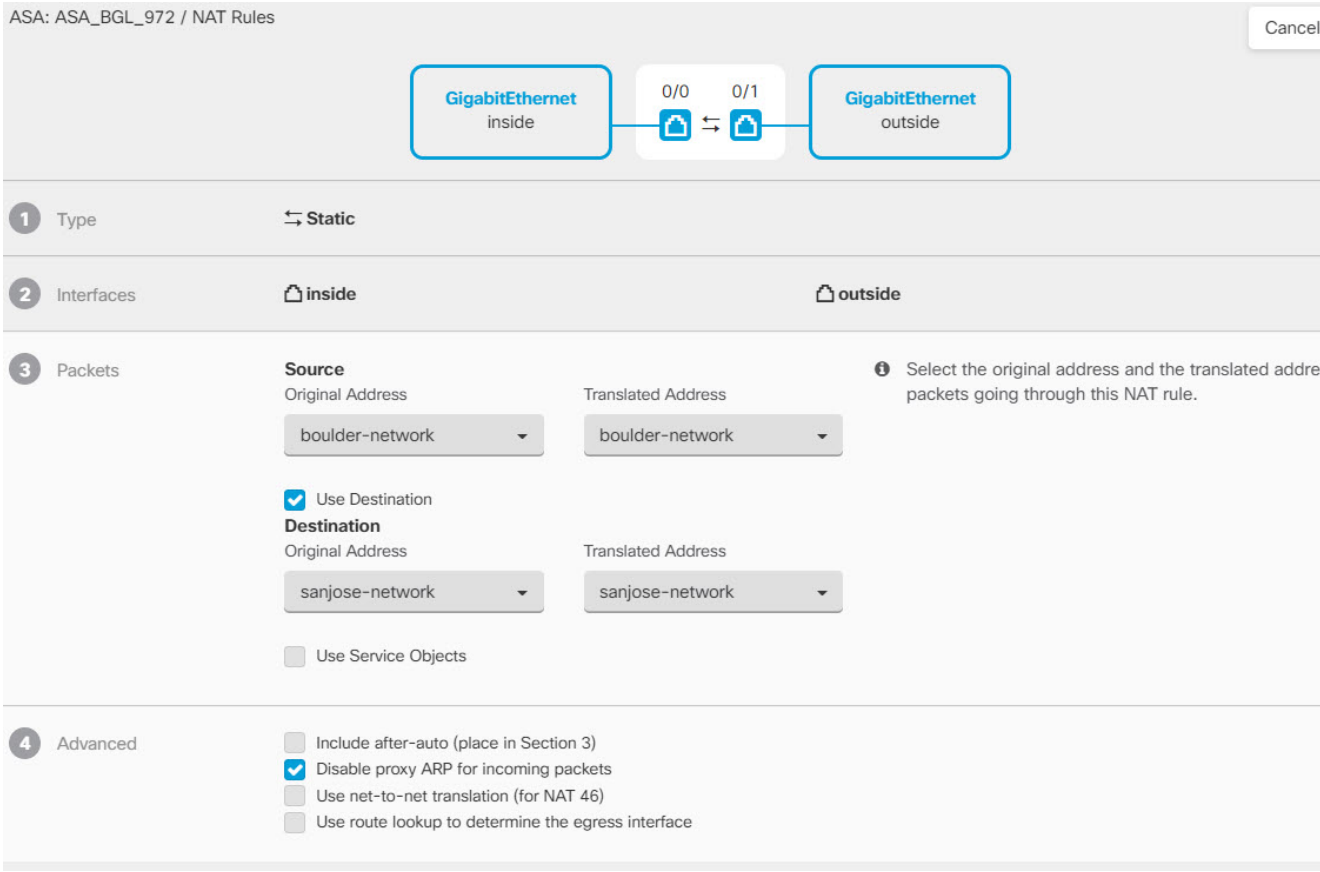
**a.** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**b.** 使用过滤器查找要为其创建 NAT 规则的设备。

**c.** 在详细信息面板的管理区域中，点击 **NAT** NAT。

**d.** 点击 + > **两次 NAT**。

- 在第 1 部分中，选择**静态 (Static)**。点击**继续**。
- 在部分 2 中，选择**源接口 (Source Interface)** = **inside** 和**目标接口 (Destination Interface)** = **outside**。点击**继续**。
- 在第 3 部分中，选择**原始源地址 (Source Original Address)** = 'boulder-network' 和 **转换后的源地址 (Source Translated Address)** = 'boulder-network'。
- 选择 **使用目的**。
- 选择**原始目标地址 (Destination Original Address)** = 'sanjose-network' 和**转换后的源地址 (Source Translated Address)** = 'sanjose-network'。**注意：**由于您不需要转换目的地址，因此需要通过为原始目的地址和转换后的目的地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。此规则为源和目标配置身份 NAT。




- 选择为传入数据包禁用代理 **ARP (Disable proxy ARP for incoming packets)**。
- 点击保存 **(Save)**。
- 重复此过程，为每个其他内部接口创建相应规则。

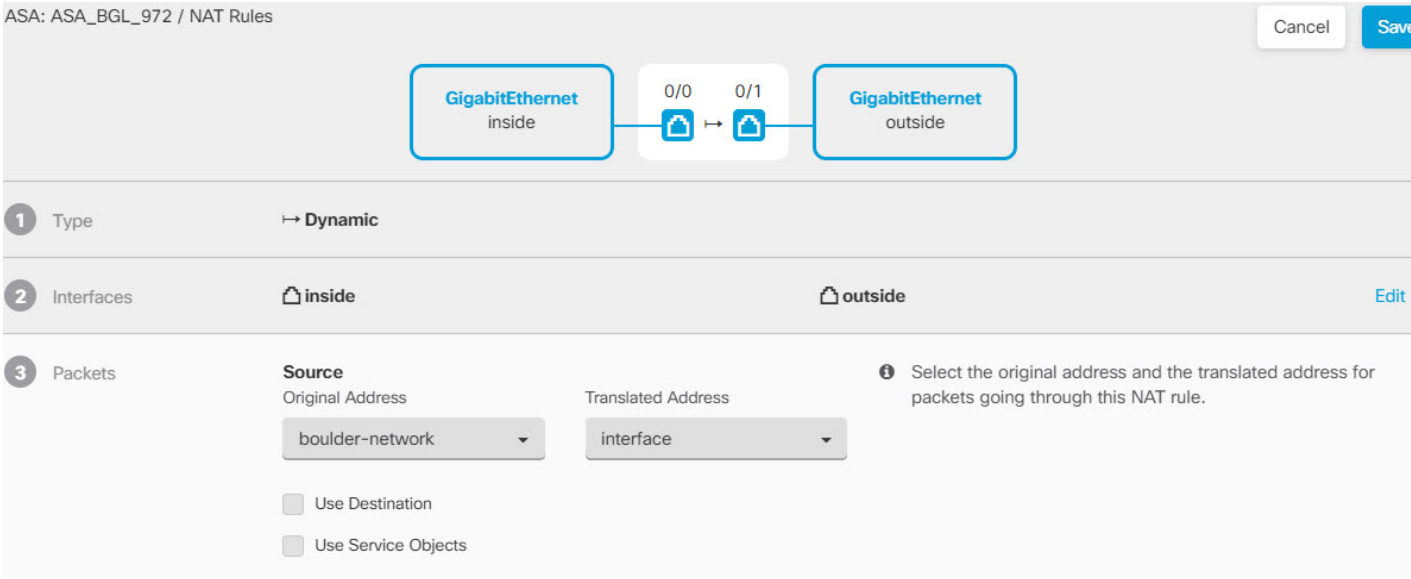
**步骤 3** 在 Firewall1（博尔德办公室）上，为内部博尔德办公室网络配置接入互联网时的手动动态接口 PAT。**注意：**内部接口可能已经配置了将所有 IPv4 流量包括在内的动态接口 PAT 规则，因为初始配置过程中会默认创建这些规则。不过，为完整起见，此处仍显示了这些配置。完成这些步骤之前，请检查是否已经存在将内部接口和网络包括在内的规则，如有则跳过此步骤。

**a.** 点击 + > **两次 NAT**。

**b.** 在第 1 部分中，选择**动态 (Dynamic)**。点击**继续**。

**c.** 在部分 2 中，选择**源接口 (Source Interface)** = **inside** 和**目标接口 (Destination Interface)** = **outside**。点击**继续**。

**d.** 在第 3 部分中，选择**原始源地址 (Source Original Address)** = 'boulder-network' 和**转换后的源地址 (Source Translated Address)** = 'interface'。




e. 点击**保存 (Save)**。

f. 重复此过程，为每个其他内部接口创建相应规则。

**步骤 4** 将配置更改部署到 CDO。有关详细信息，请参阅部署使用 CDO GUI 进行的配置更改, on page 316。

**步骤 5** 如果您也管理着 Firewall2（圣荷西办公室），您可以为该设备配置类似的规则。

- 当目标是 boulder-network 时，手动身份 NAT 规则将用于 'sanjose-network'。为 Firewall2 内部和外部网络创建新的接口对象。
- 当目标是“任何”时，手动动态接口 PAT 规则将用于 'sanjose-network'。

## 关于全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”(Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的编辑，来启用、禁用和创建策略。

以下主题介绍如何为每个 IKE 策略版本配置 IPsec 提议：

- 管理 IKEv1 策略
- 管理 IKEv2 策略

## 管理 IKEv1 策略

### 关于 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

**Related Topics**

创建 IKEv1 策略，第 223 页

## 创建 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。您还可以点击对象列表中所示的**创建新 IKE 策略 (Create New IKEv1 Policy)** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

---

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

**步骤 2** 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择**FDM** > **IKEv1 策略 (IKEv1 Policy)** 以创建新的 IKEv1 策略。
- 在对象页面中，选择要编辑的 IKEv1 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

**步骤 3** 输入**对象名称**，最多 128 个字符。

**步骤 4** 配置 IKEv1 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。

- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅“决定使用哪种加密算法”。
- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的解释，请看“决定要使用的 Diffie-Hellman 模数组”。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。
- **身份验证 (Authentication)** - 在两个对等体之间使用的身份验证方法。关于更多信息，请参阅 确定使用哪种身份验证方法。
  - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
  - **证书 (Certificate)** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签证书。
- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组。

**步骤 5** 点击 **Add**。

## 管理 IKEv2 策略

### 关于 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

**Related Topics**

创建 IKEv2 策略 ， 第 224 页

## 创建 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。您还可以点击对象列表中所示的 **创建新的 IKE 策略** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

**步骤 2** 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FDM** > **IKEv2 策略 (IKEv2 Policy)** 以创建新的 IKEv2 策略。
- 在对象页面中，选择要编辑的 IKEv2 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

**步骤 3** 输入**对象名称 (object name)**，最多 128 个字符。

**步骤 4** 配置 IKEv2 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密 (Encryption)** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要求选择完整性散列，而混合模式禁止选择单独的完整性散列。) 系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定决定使用哪个加密算法。
- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的解释，请参阅决定要使用的 Diffie-Hellman 模数组。
- **完整性散列 (Integrity Hash)** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅 决定使用哪些散列算法。
- **伪随机函数 (PRF) 散列 (Pseudo-Random Function [PRF] Hash)** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

**步骤 5** 点击 **Add**。

# 关于 IPSec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

**Note** 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议：

- 管理 IKEv1 IPsec 提议对象
- 管理 IKEv2 IPsec 提议对象

## 管理 IKEv1 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前， Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

**Note** 我们建议对 IPsec 隧道使用加密和身份验证。

### Related Topics

创建 IKEv1 IPsec 提议对象 ， 第 226 页

### 创建 *IKEv1 IPsec* 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前， Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

**Note** 我们建议对 IPsec 隧道使用加密和身份验证。

有几个预定义的 IKEv1 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑站点间 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IKEv1 提议 (Create New IKEv1 Proposal)** 链接来创建 IKEv1 IPsec 提议对象。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

**步骤 2** 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FDM > IKEv1 IPsec 提议 (IKEv1 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的 IPsec 方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

**步骤 3** 为新对象输入**对象名称**。

**步骤 4** 选择 IKEv1 IPsec 提议对象的运行模式。

- **隧道**模式会封装整个 IP 数据包。IPSec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPSec。
- **传输**模式只封装 IP 数据包的上层协议。IPSec 报头被插入到 IP 报头和上层协议报头（例如 TCP）之间。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。通常只有在保护第 2 层或第 3 层隧道协议（例如 GRE、L2TP 和 DLSW）时，才会使用传输模式。

**步骤 5** 选择**加密 (Encryption)**提议的（封装安全协议加密）算法。有关选项的说明，请参阅 决定使用哪个加密算法。

**步骤 6** 选择要用于身份验证的 **ESP 散列 (ESP Hash)** 或完整性算法。有关选项的说明，请参阅决定使用哪些散列算法。

**步骤 7** 点击 **Add**。

## 管理 IKEv2 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

**Related Topics**

创建或编辑 IKEv2 IPsec 提议对象 ， 第 228 页

创建或编辑 *IKEv2 IPsec* 提议对象

有几个预定义的IKEv2 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所示的创建新 IPsec 提议链接来创建 IKEv2 IPsec 提议对象。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

**步骤 2** 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FDM** > **IKEv2 IPsec 提议 (IKEv2 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的 IPsec 方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

**步骤 3** 为新对象输入**对象名称**。

**步骤 4** 配置 IKEv2 IPsec 方案对象：

- **加密 (Encryption)** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定决定使用哪个加密算法.
- **完整性散列 (Integrity Hash)** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法。

**步骤 5** 点击**添加 (Add)**。

## 监控 ASA 站点间虚拟专用网络

通过 CDO，您可以监控已载入的 ASA 设备上的现有站点间 VPN 配置。它不允许您修改或删除站点间配置。

### 检查站点间 VPN 隧道连接

使用 Check Connectivity 按钮触发对隧道的实时连接检查，以确定隧道当前处于活动状态还是空闲状态。搜索和过滤器站点间 VPN 隧道, on page 231除非您点击“按需连接检查”按钮，否则将每小时检查一次所有已载入设备上可用的所有隧道。

**Note**

- CDO 在 ASA FTD 上运行此连接检查命令，以确定隧道处于活动状态还是空闲状态：

```
show vpn-sessiondb l2l sort ipaddress
```

- 建模 ASA 设备将始终显示为空闲。

要从 VPN 页面检查隧道连接，请执行以下操作：

**步骤 1** 在主导航栏中，点击 VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)。

**步骤 2** 搜索并过滤站点间 VPN 隧道的隧道列表，然后选择该列表。搜索和过滤器站点间 VPN 隧道, on page 231

**步骤 3** 在右侧的操作窗格中，点击检查连接。

## 确定 VPN 问题

CDO 可以识别 ASA FTD 上的 VPN 问题。（此功能尚不适用于 AWS VPC 站点间 VPN 隧道。）本文将介绍以下内容：

- 查找缺少对等体的 VPN 隧道
- 查找存在加密密钥问题的 VPN 对等体
- 查找为隧道定义的不完整或配置错误的访问列表
- 查找隧道配置中的问题

解决隧道配置问题, on page 230

### 查找缺少对等体的 *VPN* 隧道

“缺少 IP 对等体”情况在 ASA 设备上比设备上更可能发生。FDM 管理

**步骤 1** 在 CDO 导航窗格中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

**步骤 2** 选择**表视图 (Table View)**。

**步骤 3** 通过点击过滤器图标 打开过滤器面板。

**步骤 4** 检查检测到的问题。

**步骤 5** 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。系统将列出一个对等体名称。CDO 报告另一个对等体名称为“[缺少对等体 IP.]”。

### 查找存在加密密钥问题的 *VPN* 对等体

使用此方法查找存在加密密钥问题的 VPN 对等体，例如：

- IKEv1 或 IKEv2 密钥无效、缺失或不匹配
- 过时或低加密隧道

**步骤 1** 在 CDO 导航栏中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

**步骤 2** 选择**表视图 (Table View)**。

**步骤 3** 通过点击过滤器图标 打开过滤器面板。

**步骤 4** 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。⚠对等体信息将显示两个对等体。

**步骤 5** 点击其中一台设备的**查看对等体 (View Peers)**。

**步骤 6** 双击图表视图中报告问题的设备。

**步骤 7** 点击底部隧道详细信息面板中的**密钥交换 (Key Exchange)**。您将能够查看两台设备并从该点诊断关键问题。

---

查找为隧道定义的不完整或配置错误的访问列表

“不完整或配置错误的访问列表”条件只能出现在 ASA 设备上。

---

**步骤 1** 在 CDO 导航栏中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

**步骤 2** 选择**表视图 (Table View)**。

**步骤 3** 通过点击过滤器图标 打开过滤器面板。

**步骤 4** 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。⚠对等体信息显示两个对等体。

**步骤 5** 点击其中一台设备的查看对等体。

**步骤 6** 双击图表视图中报告问题的设备。

**步骤 7** 点击底部隧道详细信息面板中的隧道详细信息。您将看到消息“网络策略：不完整”

---

查找隧道配置中的问题

在以下情况下可能会发生隧道配置错误：

- 当站点间 VPN 接口的 IP 地址更改时，“对等 IP 地址值已更改”。
- 当 VPN 隧道的 IKE 值与另一个 VPN 隧道不匹配时，系统将显示“IKE 值不匹配”消息。

---

**步骤 1** 在 CDO 导航栏中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

**步骤 2** 选择**表视图 (Table View)**。

**步骤 3** 通过点击过滤器图标 打开过滤器面板。

**步骤 4** 在**隧道问题 (Tunnel Issues)** 中，点击**检测到的问题 (Detected Issues)** 以查看 VPN 配置报告错误。您可以查看配置报告问题。⚠

**步骤 5** 选择 VPN 配置报告问题。

**步骤 6** 在右侧的“对等体”窗格中，会显示存在问题的对等体的图标。⚠将鼠标悬停在图标上可查看问题和解决方案。⚠

下一步：解决隧道配置问题。解决隧道配置问题, on page 230

---

解决隧道配置问题

此程序尝试解决以下隧道配置问题：

- 当站点间 VPN 接口的 IP 地址更改时，“对等 IP 地址值已更改”。

- 当 VPN 隧道的 IKE 值与另一个 VPN 隧道不匹配时，系统将显示“IKE 值不匹配”消息。

有关详细信息，请参阅查找隧道配置中的问题。

---

**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择与报告问题的 VPN 配置关联的设备。

**步骤 4** 接受设备更改。解决“检测到冲突”状态，第 326 页

**步骤 5** 在 CDO 导航窗格中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

**步骤 6** 选择报告此问题的 VPN 配置。

**步骤 7** 点击**操作 (Actions)** 窗格中的**编辑** 图标 。

**步骤 8** 在每个步骤中点击**下一步**，直到您在步骤 4 中点击**完成**按钮。

**步骤 9** 预览和部署所有设备的配置更改，第 313 页。

---

### 搜索和过滤器站点间 VPN 隧道

将过滤器边栏 与搜索字段结合使用，可重点搜索 VPN 隧道图中显示的 VPN 隧道。

---

**步骤 1** 在主导航栏中，导航至 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

**步骤 2** 点击过滤器图标 可打开过滤器窗格。

**步骤 3** 使用以下过滤器细化搜索：

- **按设备过滤 (Filter by Device)** - 点击**按设备过滤 (Filter by Device)**，选择设备类型选项卡，然后选中要通过过滤查找的设备。
- **隧道问题 (Tunnel Issues)** - 我们是否检测到隧道的任一端存在问题。存在问题的设备的一些示例可能包括（但不限于）：缺少关联的接口或对等体 IP 地址或访问列表、IKEv1 提议不匹配等。（检测隧道问题尚不适用于 AWS VPC VPN 隧道。）
- **设备/服务 (Devices/Services)** - 按设备类型过滤。
- **状态 (Status)** - 隧道状态可以是活动或空闲。
  - **活动 (Active)** - 存在网络数据包通过 VPN 隧道的开放会话，或者已成功建立会话且尚未超时的会话。活动可以帮助指示隧道处于活动状态和相关性。
  - **空闲 (Idle)** - CDO 无法发现此隧道的开放会话，隧道可能未在使用或此隧道存在问题。
- **已载入 (Onboarded)** - 设备可以由 CDO 管理，也可以不由 CDO 管理（非托管）。
  - **托管 (Managed)** - 按 CDO 管理的设备过滤。
  - **非托管 (Unmanaged)** - 按 CDO 不管理的设备进行过滤。

- **设备类型 (Device Types)** - 隧道的任一端是实时（已连接设备）还是模型设备。

**步骤 4** 您还可以通过在搜索栏中输入设备名称或 IP 地址来搜索过滤结果。搜索不区分大小写。

### 载入非托管站点间 VPN 对等体

在载入其中一个对等设备时，CDO 将发现站点间 VPN 隧道。如果第二个对等设备不由 CDO 管理，则您可以过滤 VPN 隧道列表以查找非受管设备并将其载入：

**步骤 1** 在主导航栏中，选择 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

**步骤 2** 选择**表视图 (Table View)**。

**步骤 3** 通过点击 打开过滤器面板。

**步骤 4** 点击**非托管 (Unmanaged)**。

**步骤 5** 从表中的结果中选择一个隧道。

**步骤 6** 在右侧的**对等体 (Peers)** 窗格中，点击**载入设备 (Onboard Device)**，然后按照屏幕上的说明进行操作。

相关信息：

- 载入设备和服务, on page 135
- 将 ASA 设备载入 CDO, on page 135

### 查看站点间 VPN 隧道的 IKE 对象详细信息

您可以查看所选隧道的对等体/设备上配置的 IKE 对象的详细信息。这些详细信息根据 IKE 策略对象的优先级显示在层次结构中的树结构中。

**Note** 外联网设备不显示 IKE 对象详细信息。

**步骤 1** 在左侧 CDO 导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

**步骤 2** 在 VPN Tunnels 页面中，点击连接对等体的 VPN 隧道的名称。

**步骤 3** 在右侧的“关系”下，展开要查看其详细信息的对象。

### 查看上次成功建立站点间 VPN 隧道的日期

**步骤 1** 查看 IPsec 站点间虚拟专用网络隧道信息。查看站点间 VPN 隧道信息, on page 233

**步骤 2** 点击 Tunnel Details 窗格。

**步骤 3** 查看上次查看的活动字段。

## 查看站点间 VPN 隧道信息

站点间 VPN 表视图是载入 CDO 的所有设备上可用的所有站点间 VPN 隧道的完整列表。隧道在此列表中仅存在一次。点击表中列出的隧道会在右侧栏中提供一个选项，以直接导航到隧道的对等体以进行进一步调查。

如果 CDO 不管理隧道的两端，您可以点击载入非托管站点间 VPN 对等体 以打开主载入页面并载入非托管对等设备。在 CDO 管理隧道两端的情况下，对等体 2 列包含受管设备的名称。但是，对于 AWS VPC，对等体 2 列包含 VPN 网关的 IP 地址。

要在表视图中查看站点间 VPN 连接，请执行以下操作：

**步骤 1** 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

**步骤 2** 点击**表格视图 (Table view)**  按钮。

**步骤 3** 使用搜索和过滤器站点间 VPN 隧道 以查找特定隧道，或放大全局视图图形以查找要查找的 VPN 网关及其对等体。

站点间 *VPN* 全局视图

**步骤 1** 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

**步骤 2** 点击**全局视图 (Global view)** 按钮。

**步骤 3** 使用搜索和过滤器站点间 VPN 隧道 以查找特定隧道，或放大全局视图图形以查找要查找的 VPN 网关及其对等体。

**步骤 4** 选择全局视图中表示的对等体之一。

**步骤 5** 点击**查看详细信息**。

**步骤 6** 点击 VPN 隧道的另一端，CDO 将显示该连接的隧道详细信息、NAT 信息和密钥交换信息：

- 隧道详细信息 - 显示有关隧道的名称和连接信息。点击刷新图标可更新隧道的连接信息。
- 特定于 AWS 连接的隧道详细信息 - AWS 站点到站点连接的隧道详细信息与其他连接略有不同。对于从 AWS VPC 到 VPN 网关的每个连接，AWS 会创建两个 VPN 隧道。这用于高可用性。
  - 隧道的名称代表您的 VPN 网关所连接的 VPC 的名称。隧道中指定的 IP 地址是您的 VPN 网关获知的 VPC 的 IP 地址。
  - 如果 CDO 连接状态显示为“活动”，则 AWS 隧道状态为“运行”。如果 CDO 连接状态为“非活动”，则 AWS 隧道状态为“关闭”。
- NAT 信息 - 显示正在使用的 NAT 规则类型、原始和转换后的数据包信息，并提供指向 NAT 表的链接以查看该隧道的 NAT 规则。（尚不可用于 AWS VPC 站点间 VPN。）

- 密钥交换 - 显示隧道和密钥交换问题正在使用的加密密钥。（尚不可用于 AWS VPC 站点间 VPN。）

站点间 *VPN* 隧道 *(Site-to-Site VPN Tunnels)* 窗格

Tunnels 窗格显示与特定 VPN 网关关联的所有隧道的列表。对于 VPN 网关和 AWS VPC 之间的站点间 VPN 连接，隧道窗格显示从 VPN 网关到 VPC 的所有隧道。由于您的 VPN 网关和 AWS VPC 之间的每个站点间 VPN 连接都有两个隧道，因此您会看到通常用于其他设备的隧道数量的两倍。

**VPN 网关详细信息**

显示连接到 VPN 网关的对等体的数量以及 VPN 网关的 IP 地址。这仅在“VPN 隧道”(VPN Tunnels) 页面中可见。

**查看对等体**

选择站点间VPN对等体后，对等体窗格将列出该对中的两台设备，并允许您点击其中一台设备的**查看对等体 (View Peer)**。通过点击**查看对等体 (View Peer)**，您可以看到与该设备关联的任何其他站点到站点对等体。这在“表”视图和“全局”视图中可见。

# 远程访问虚拟专用网络

远程访问虚拟专用网络 (RA VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

RA VPN 配置包括以下组件：

- 连接配置文件：您可以创建远程访问 VPN 连接配置文件，允许用户在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。连接配置文件由身份源和组策略组成。

**相关信息：**

- 为 ASA 配置远程访问虚拟专用网络, on page 234

## 为 ASA 配置远程访问虚拟专用网络

ASA 通过跨 TCP/IP 网络（如互联网）创建被用户视为专用连接的安全连接来创建远程访问虚拟专用网络 (VPN)。它可以创建单一用户到 LAN 连接和 LAN 到 LAN 连接。

这种安全连接被称为隧道，ASA 使用隧道协议来协商安全参数，创建并管理隧道，封装数据包，通过隧道收发数据包，然后再对它们解除封装。ASA 相当于一个双向隧道终端：可以接收普通数据包，封装它们，再将它们发送到隧道的另一端，在那里系统将对数据包解除封装并将其发送到最终目标。它也可以接收已封装的数据包，解除数据包封装，然后将它们发送到最终目标。

CDO 提供直观的用户界面，用于配置新的远程访问虚拟专用网络。它还允许您快速轻松地为 CDO 中载入的多个自适应安全设备 (ASA) 配置远程访问 VPN 连接。

CDO 允许您从头开始在 ASA 设备上配置远程访问 VPN 配置。它还允许您管理已使用其他 ASA 管理工具（例如自适应安全防御管理器 [ASDM] 或思科安全管理器 [CSM]）配置的远程访问 VPN 设置。当您载入已具有远程访问 VPN 设置的 ASA 设备时，CDO 会自动创建“默认远程访问 VPN 配置”并将ASA设备与此配置相关联。此默认配置可以包含设备上定义的所有连接配置文件对象。如果要了解读入 CDO 的 RAVPN 属性，请参阅管理和部署预先存在的 ASA 远程访问 VPN 配置部分。否则，您可以开始执行“ASA 的端到端远程访问 VPN 配置过程”部分中所述的步骤。

**相关信息：**

- ASA 的端到端远程访问 VPN 配置过程
  - 为 ASA 配置身份源
    - 创建 ASA Active Directory 领域对象
    - 创建 ASA RADIUS 服务器对象或组
  - 创建 ASA 远程访问 VPN 组策略, on page 241
  - 创建 ASA 远程访问 VPN 配置, on page 247
  - 配置 ASA 远程访问 VPN 连接配置文件, on page 251
- 管理和部署预先存在的 ASA 远程访问 VPN 配置
- 创建 IP 地址池
- 从 NAT 豁免远程访问流量, on page 264
- 验证 ASA 的远程访问 VPN 配置
- 查看 ASA 的远程访问 VPN 配置详细信息

## ASA 的端到端远程访问 VPN 配置过程

本节提供在载入到 CDO 的 ASA 设备上配置远程访问 VPN 的端到端程序。

要为客户端启用远程访问 VPN，需要配置多个单独的项目。以下程序介绍了端到端流程。

---

**步骤 1** 配置用于对远程用户进行身份验证的身份源。有关详细信息，请参阅为 ASA 配置身份源。

您可以使用以下来源对尝试使用远程访问 VPN 连接到您的网络的用户进行身份验证。此外，可以使用客户端证书进行身份验证，可单独使用，也可与身份源配合使用。

- Active Directory 身份领域：作为主要身份验证源。在 Active Directory AD 服务器中定义用户账户。请参阅“配置 AD 身份领域”。请参阅创建 ASA Active Directory 领域对象。
- RADIUS 服务器组：充当主要或辅助身份验证源，并用于授权和记账。请参阅创建 ASA RADIUS 服务器对象或组。
- 本地身份源（本地用户数据库）：作为主要或回退源。您可以直接在设备上定义用户，不使用外部服务器。如果您使用本地数据库作为回退源，请确保您定义与外部服务器中描述的相同用户名/密码。注意：只能从自

适应安全设备管理器 (ASDM) 直接在 ASA 设备上创建用户帐户。请参阅《思科 ASA 系列防火墙 ASDM 配置指南，X.Y》的“访问控制对象”一章中的“配置本地用户组”部分。

**步骤 2** （可选）创建 ASA 远程访问 VPN 组策略, on page 241。组策略定义用户相关的属性。可以配置组策略，根据组成员身份提供差异化的资源访问权限。或者，可以对所有连接使用默认策略。

**步骤 3** 创建 ASA 远程访问 VPN 配置, on page 247。

**步骤 4** 配置 ASA 远程访问 VPN 连接配置文件, on page 251。

**步骤 5** （可选）从 NAT 豁免远程访问流量, on page 264。

**步骤 6** 将配置更改从 CDO 部署到 ASA。

**Important** 如果使用本地管理器（如自适应安全设备管理器 (ASDM)）更改远程访问 VPN 配置，CDO 中该设备的**配置状态 (Configuration Status)** 将显示“检测到冲突”(Conflict Detected)。请参阅 设备上的带外更改。您可以解决此 ASA 上的配置冲突。解决配置冲突, on page 325

### What to do next

**后续步骤**

将远程访问 VPN 配置下载到 ASA 设备后，用户可以使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备从远程位置连接到您的网络。您可以从租户中所有已载入的 ASA 远程访问 VPN 前端监控实时 AnyConnect 远程访问 VPN 会话。请参阅监控远程访问虚拟专用网络会话。

## 为 *ASA* 配置身份源

身份源（例如 Microsoft Active Directory (AD) 领域和 RADIUS 服务器）是为组织内的人员定义用户账户的 AAA 服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程访问 VPN 连接或到 CDO 的访问进行身份验证。

点击**对象 (Objects) > ASA 对象 (ASA Objects)**，然后点击 (  )> **身份源**以创建源。后期配置需要使用身份源的服务时，可以使用这些对象。您可以应用适当的过滤器来搜索现有源并对其进行管理。

### 确定目录基准标识名

配置目录属性时，需要为用户和组指定公共基准标识名 (DN)。基准在您的目录服务器中定义，并且会因网络而不同。您必须输入正确的基准，身份策略才能正常使用。如果基准错误，则系统无法确定用户名或组名，进而导致基于身份的策略无法使用。

**Note** 要获得正确的基准，请咨询目录服务器的管理员。

对于 Active Directory，您可以用域管理员的身份登录 Active Directory 服务器，并按照如下所示在命令提示符后输入 **dsquery** 命令来确定正确的基准：

**用户搜索库**

输入具有已知用户名（部分或完整）的 **dsquery user** 命令，以确定基准标识名。例如，以下命令使用部分名称“John*”返回以“John.”开头的所有用户的信息。

**C:\Users\Administrator>dsquery user -name "John*"**

**"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"**

基准 DN 为“DC=csc-lab,DC=example,DC=com”。

**组搜索基准**

输入具有已知组名称的 **dsquery group** 命令，以确定基准标识名。例如，以下命令使用组名称 Employees 返回标识名：

**C:\>dsquery group -name "Employees"**

**"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"**

组基准 DN 为“DC=csc-lab,DC=example,DC=com”。

此外，您还可以使用 ADSI Edit 程序浏览 Active Directory 结构 (**Start** > **Run** > **adsiedit.msc**)。在 ADSI Edit 中，右键点击任意对象，例如组织单位 (OU)、组或用户，然后选择**属性 (Properties)** 查看标识名。然后，可以复制 DC 值的字符串作为基准。

要验证您是否获得了正确的基准，请执行以下操作：

**步骤 1** 点击目录属性中的“测试连接”(Test Connection) 按钮验证连接。解决所有问题后，保存目录属性。

**步骤 2** 提交对设备的更改。

**步骤 3** 创建访问规则，选择**用户**选项卡，并尝试从目录添加已知的用户和组名称。在您键入内容时，系统会自动填充建议，以匹配包含该目录的领域中的用户和组。如果这些建议显示在一个下拉列表中，则说明系统可以成功查询目录。如果您没有看到建议，而且确定您键入的字符串应显示在用户或组名称中，则需要更正相应的搜索基准。

### What to do next

有关详细信息，请参阅创建 ASA Active Directory 领域对象。

## RADIUS 服务器和组

您可以使用 RADIUS 服务器对管理用户进行身份验证和授权。配置要使用 RADIUS 服务器的功能时，您应选择 RADIUS 组而不是单个服务器。RADIUS 组所含 RADIUS 服务器是彼此副本的集合。如果一个组具有多个服务器，这些服务器可构成备份服务器链，在其中一台服务器不可用时提供冗余。但即使只有一台服务器，也必须创建包含一个成员的组，以配置功能的 RADIUS 支持。

您可以将此源用于以下目的：

- 远程访问 VPN 用作身份验证、授权和记账的身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，作为被动身份源来从远程访问 VPN 登录收集用户身份信息。

有关详细信息，请参阅创建 ASA RADIUS 服务器对象或组。

## 创建 ASA Active Directory 领域对象

当您创建或编辑身份源对象（例如 AD 领域对象）时，CDO 通过 SDC 将配置请求发送到 ASA 设备。然后，ASA 与配置的 AD 领域通信。

使用以下程序创建对象：

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击创建对象 () RA VPN 对象（ASA 和 FDM）身份源。  >

**步骤 3** 为对象输入**对象名称 (Object Name)**。

**步骤 4** 选择 **ASA** 作为**设备类型 (Device Type)**。

**步骤 5** 在向导的第一部分中，选择 Active Directory 领域作为身份源类型。点击**继续 (Continue)**。

**步骤 6** 配置基本领域属性。

- **目录用户名、目录密码 (Directory Username, Directory Password)** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

  **注释** 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=administrator,cn=users,dc=example,dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准区别名称 (Base Distinguished Name)** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如，cn=users,dc=example,dc=com。

**步骤 7** 配置目录服务器属性。

- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。
- Encryption - 要使用加密连接下载用户和组信息，请选择 LDAPS 以使用 SSL 保护 ASA 与 LDAP 服务器之间的通信。它需要基于 SSL 的 LDAP。使用端口 636。

  系统默认为**无**，也就是说以明文形式下载用户和组信息。

**步骤 8** （可选）使用测试按钮验证配置。

**步骤 9** （可选）点击添加其他配置，将多个 Active Directory (AD) 服务器添加到 AD 领域。AD 服务器需要彼此复制并支持相同的 AD 域。因此，与该 AD 领域关联的所有 AD 服务器的基本领域属性（例如目录名称、目录密码和基本可分辨名称）必须相同。

**步骤 10** 点击 **Add**。

## 编辑 ASA Active Directory 领域对象

请注意，在编辑身份源对象时，不能更改身份源类型。您必须创建具有正确类型的新对象。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 使用对象过滤器和搜索字段找到要编辑的对象。

**步骤 3** 选择要编辑的对象。

**步骤 4** 点击**操作 (Actions)** 窗格中的编辑图标 。

**步骤 5** 以在上述过程中创建值的相同方式编辑对话框中的值。展开下面列出的配置栏，以编辑或测试主机名/IP 地址或加密信息。

**步骤 6** 点击**保存 (Save)**。

**步骤 7** CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

**步骤 8** 立即将配置更改从 CDO 部署到 ASA您所做的更改，或等待并一次部署多个更改。

创建 ASA RADIUS 服务器对象或组

在创建或编辑 RADIUS 服务器对象或一组 RADIUS 服务器对象等身份源对象时，CDO 会通过 SDC 将配置请求发送到 ASA 设备。

创建 ASA RADIUS 服务器对象

RADIUS 服务器提供 AAA（身份验证、授权和记账）服务。

使用以下程序创建对象：

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击**创建对象 (Create Object)** ( )**> RA VPN 对象 (ASA & FDM) (RA VPN Objects [ASA & FDM])** > **身份源 (Identity Source)**。

**步骤 3** 为对象输入**对象名称 (Object name)**。

**步骤 4** 选择 **ASA** 作为**设备类型 (Device Type)**。

**步骤 5** 选择 RADIUS 服务器作为身份源类型。点击**继续 (Continue)**。

**步骤 6** 使用以下属性编辑身份源配置：

- **服务器名称或 IP 地址 (Server Name or IP Address)** - 服务器的完全限定主机名 (FQDN) 或 IP 地址。
- **身份验证端口 (Authentication Port)**（可选）- 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **超时 (Timeout)** - 系统将请求发送至下一服务器之前等待服务器响应的时长，此为 1-300 秒之间的数值。默认值为 10 秒。
- 输入**服务器密钥 (Server Secret Key)**（可选）- 用于加密 ASA 设备和 RADIUS 服务器之间数据的共享密钥。该密钥是一个区分大小写的字母数字字符串，最多 64 个字符，且不含空格。密钥必须以字母数字字符或下划线开头，它可以包含特殊字符：$ & - _ . + @。字符串必须匹配 RADIUS 服务器上配置的字符串。如果不配置密钥，则不加密连接。

**步骤 7** 点击**添加 (Add)**。

**步骤 8** 立即将配置更改从 CDO 部署到 ASA您所做的更改，或等待并一次部署多个更改。

---

创建 ASA RADIUS 服务器组

RADIUS 服务器组中包含一个或多个 RADIUS 服务器对象。组中的服务器必须是彼此的备份。这些服务器构成备份服务器链，因此，如果第一台服务器不可用，系统可以尝试列表中的下一个服务器。

使用以下程序创建对象组：

---

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击创建对象 () RA VPN 对象（ASA 和 FDM）身份源。 

**步骤 3** 为对象输入**对象名称 (Object name)**。

**步骤 4** 选择 **ASA** 作为**设备类型 (Device Type)**。

**步骤 5** 选择 RADIUS 服务器组作为身份源类型。 点击**继续 (Continue)**。

**步骤 6** 使用以下属性编辑身份源配置：

- **断路时间 (Dead Time)** - 只有当所有服务器均发生故障时，才会重新激活故障服务器。断路时间是指最后一台服务器发生故障后，在重新激活所有服务器之前所等待的时间。
- **最大失败尝试次数 (Maximum Failed Attempts)** - 尝试组中下一个服务器之前发送到 RADIUS 服务器的失败请求（即，未收到响应的请求）数。超过最大失败尝试次数时，系统会将服务器标记为故障。对于给定功能，如果您使用本地数据库配置回退方法，并且组中的所有服务器都无法响应，则会将该组视为无法响应，并将尝试回退方法。该服务器组会在断路时间内保持标记为无响应，以确保该时段内其他 AAA 请求不会尝试联系该服务器组，而是立即使用回退方法。
- **动态授权/端口 (Dynamic Authorization/Port)**（可选）- 如果为此 RADIUS 服务器组启用 RADIUS 动态授权或授权更改 (CoA) 服务，该组会注册 CoA 通知并侦听指定的端口，以便使 CoA 策略从 Cisco Identity Services Engine (ISE) 进行更新。仅当您在远程访问 VPN 中结合 ISE 使用此服务器组时，才能启用动态授权。

**步骤 7** 从下拉菜单中选择支持 RADIUS 服务器的 AD 领域。如果尚未创建 AD 领域，请从下拉菜单中点击创建。

**步骤 8** 点击 RADIUS 服务器添加按钮，添加现有的 RADIUS 服务器对象。  或者，您可以从此窗口创建新的 RADIUS 服务器对象。

**Note** 优先级添加这些对象，因为列表中的第一个服务器将被使用，直到它停止响应。然后，ASA 默认使用列表中的下一个服务器。

**步骤 9** 立即将配置更改从 CDO 部署到 ASA您所做的更改，或等待并一次部署多个更改。

---

编辑 ASA Radius 服务器对象或组

使用以下程序编辑 Radius 服务器对象或 Radius 服务器组：

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 使用对象过滤器和搜索字段找到要编辑的对象。

**步骤 3** 选择要编辑的对象。

**步骤 4** 点击**操作 (Actions)** 窗格中的编辑图标 。

**步骤 5** 以在上述过程中创建值的相同方式编辑对话框中的值。要编辑或测试主机名/IP 地址或加密信息，请展开配置栏。

**步骤 6** 点击**保存 (Save)**。

**步骤 7** CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

**步骤 8** 立即将配置更改从 CDO 部署到 ASA您所做的更改，或等待并一次部署多个更改。

## 创建 *ASA* 远程访问 *VPN* 组策略

组策略是一组面向用户的远程访问 VPN 的属性/值对。连接配置文件使用组策略在建立隧道后设置用户连接的条款。通过组策略可将整组属性应用于用户或用户组，而不必为每个用户单独指定每个属性。

系统包含名为“DfltGrpPolicy”的默认组策略。您可以创建其他组策略，以提供您所需的服务。

**注释** 不能将不一致的组策略对象添加到远程访问 VPN 配置。在将组策略添加到远程访问 VPN 配置之前，请解决所有不一致问题。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击“加号” 按钮。

**步骤 3** 点击 **RA VPN 对象（ASA 和 FDM）(RA VPN Objects [ASA & FDM]) > RA VPN 组策略 (RA VPN Group Policy)**。

**步骤 4** 输入组策略的名称。此名称最多可包含 64 个字符，允许使用空格。

**步骤 5** 在**设备类型 (Device Type)** 下拉列表中，选择 **ASA**。

**步骤 6** 执行以下任一操作：

- 点击所需的选项卡并配置页面上的属性：
  - ASA 远程访问 VPN 组策略属性
  - AnyConnect 客户端配置文件， 第 242 页
  - 会话设置属性， 第 243 页
  - 地址分配属性， 第 243 页
  - 分割隧道属性， 第 244 页
  - AnyConnect 属性， 第 245 页

- 流量过滤器属性，第 246 页
- Windows 浏览器代理属性，第 247 页

**步骤 7** 点击**保存 (Save)** 以保存组策略。

---

ASA 远程访问 VPN 组策略属性

本节介绍与 ASA 远程访问 VPN 组策略关联的属性。

### 常规属性

组策略的常规属性定义组名称和一些其他基本设置。

- **DNS 服务器**：输入连接到 VPN 时用于域名解析的 DNS 服务器的 IP 地址。可以使用逗号分隔地址。
- **横幅**：登录时向用户显示的横幅文本或欢迎消息。默认无横幅。最多 496 字符。AnyConnect 客户端支持部分 HTML。为确保向远程用户正确地显示横幅，请使用 <BR> 标记表示换行。
- **默认域 (Default Domain)**：远程访问 VPN 中用户的默认域名。例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。

### AnyConnect 客户端配置文件

运行软件版本 6.7 或更高版本的 FTD 支持此功能。

Cisco AnyConnect VPN 客户端通过各种内置模块提供增强的安全性。这些模块提供网络安全，终端流量的网络可视性和网络外漫游保护等服务。每个客户端模块都包含一个客户端配置文件，其中包含根据您的要求的一组自定义配置。

当 VPN 用户下载 VPN AnyConnect 客户端软件时，您可以选择要下载到客户端的 AnyConnect VPN 配置文件对象和 AnyConnect 模块。

1. 选择或创建 AnyConnect VPN 配置文件对象。请参阅上传 RA AnyConnect 客户端配置文件, on page 267。除 DART 和“登录前启动”模块外，必须选择 AnyConnect VPN 配置文件对象。
2. 点击**添加Any 链接客户端模块 (Add Any Connect Client Module)**。

   以下 AnyConnect 模块是可选的，您可以将这些模块配置为在 VPN AnyConnect 客户端软件时下载：

   - **AMP 启用程序 (AMP Enabler)** - 为终端部署高级恶意软件防护 (AMP) 。
   - **DART** - 捕获系统日志和其他诊断信息的快照并在桌面上创建 .zip 文件，因此您可以便利地将故障排除信息发送到思科 TAC。
   - **反馈 (Feedback)** - 提供有关客户已启用和使用的功能和模块的信息。
   - **ISE 终端安全评估 (ISE Posture)** - 使用 OPSWAT v3 库执行终端安全评估检查，评估终端的合规性。

- **网络访问管理器 (Network Access Manager)** - 为有线和无线网络访问提供 802.1X（第 2 层）和设备身份验证。
- **网络可视性 (Network Visibility)** - 可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。
- **登录前启动 (Start Before Login)** - 通过在 Windows 登录对话框出现之前启动 AnyConnect，强制用户在登录到 Windows 之前通过 VPN 连接而连接到企业基础设施。
- **Umbrella 漫游安全 (Umbrella Roaming Security)** - 在没有处于活动状态的 VPN 时提供 DNS 层安全。
- **网络安全 (Web Security)** - 根据定义的安全策略分析网页的元素，允许可接受的内容，并阻止恶意或不可接受的内容。

3. 在**客户端模块 (Client Module)** 列表中选择 **AnyConnect 模块 (AnyConnect module)**。
4. 在**配置文件 (Profile)** 列表中，选择或创建包含 AnyConnect 客户端配置文件的配置文件对象。
5. 选择**启用模块下载 (Enable Module Download)** 以下载客户端模块以及配置文件。如果未选择，则终端只能下载客户端配置文件。

### 会话设置属性

组政策会话设置控制用户可以连接到 VPN 的时长和可以创建的独立连接的数量。

- **最长连接时间 (Maximum Connection Time)**：在不注销和重新连接的情况下，用户可持续连接到 VPN 的最大时间长度（以分钟为单位），范围为 1 到 4473924 或留空。默认值为无限（留空），但空闲超时仍适用。
- **连接时间警报间隔 (Connection Time Alert Interval)**：如果您指定了最大连接时间，则警报间隔定义，在达到最长时间之前，向用户显示即将自动断开连接警告的时间。用户可以选择结束连接并重新连接，以重新启动计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **空闲时间 (Idle Time)**：VPN 连接在自动关闭之前可以闲置的时间长度（以分钟为单位），范围为 1 到 35791394。如果在此时间段内此连接上无通信活动，则系统会终止连接。默认值为 30 分钟。
- **空闲时间警报间隔 (Idle Time Alert Interval)**：在达到空闲时间之前，向用户显示因闲置会话而即将自动断开连接的警报的时间。任何活动都会重置计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **每个用户的同时登录数 (Simultaneous Login Per User)**：允许用户执行的最多同时登录数。默认值为 3。可以指定 1 到 2147483647 个连接。允许许多同时连接可能会危害安全性并影响性能。

### 地址分配属性

组策略的地址分配属性定义组的 IP 地址池。此处定义的地址池将覆盖使用此组的任何连接配置文件中定义的池。如果您希望使用连接配置文件中定义的池，请将这些设置留空。

- **IPv4 地址池 (IPv4 Address Pool)、IPv6 地址池 (IPv6 Address Pool)**：这些选项定义远程终端的地址池。根据客户端用于建立 VPN 连接的 IP 版本，从这些池为客户端分配地址。选择 IP 地址池，定义要支持的每个 IP 类型的子网。如果您不想支持该 IP 版本，则可以空着列表。例如，可以将 IPv4 池定义为 10.100.10.0/24。地址池不能与外部接口的 IP 地址位于同一子网。创建新的创建IP地址池。可以指定包含最多六个地址池的列表，用于本地地址分配。地址池的指定顺序非常重要。系统按照地址池出现的顺序分配这些地址池中的地址。**注意**：可为同一个组策略同时配置 IPv4 和 IPv6 地址池。如果在同一个组策略中配置了两个版本的 IP 地址，则配置了 IPv4 的客户端将获得 IPv4 地址，配置了 IPv6 的客户端将获得 IPv6 地址，而同时配置了 IPv4 和 IPv6 地址的客户端将获得 IPv4 和 IPv6 地址。
- **DHCP 范围 (DHCP Scope)**：如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个池。作用域允许您选择DHCP服务器中定义的部分地址池，用于此特定组。如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。要指定作用域，请输入包含网络号主机地址的网络对象。例如，要告诉 DHCP 服务器使用 192.168.5.0/24 子网池中的地址，请输入指定 192.168.5.0 为主机地址的网络对象。DHCP 仅可用于 IPv4 寻址。

### 分割隧道属性

组策略的分割隧道属性定义系统如何处理用于内部网络的流量和流向外部的流量。分割隧道引导一些网络流量通过 VPN 隧道（加密），将剩下的网络流量引导至 VPN 隧道外部（未加密或以明文形式）。

典型地，在远程访问 VPN 中，您可能希望 VPN 用户通过您的设备访问互联网。但是，您可以允许 VPN 用户在连接到远程访问 VPN 时访问外部网络。这种技术有时候称为分割隧道或发夹方法。拆分隧道不仅允许 VPN 通过安全隧道连接到远程网络，而且允许连接到 VPN 隧道外的网络。拆分隧道可减少 FTD 设备上的网络负载，并增加外部接口上的带宽。

### 准备工作

为 IPv4 网络创建一个分割隧道策略并为 IPv6 网络创建另一个分割隧道策略，则指定的访问列表同时用于两种协议。因此，访问列表应同时包含 IPv4 和 IPv6 流量的访问控制项 (ACE)。

当 ASA 设备载入 CDO 时，它会读取与该设备关联的扩展 ACL。有关详细信息，请参阅组策略 。如果要创建新的 ACL，请参阅 ASA 策略（扩展访问列表）以进行创建。

**Note** 确保在要创建的 ACL 中将用于分割隧道的网络指定为源网络。

- **IPv4 分割隧道 (IPv4 Split Tunneling)、IPv6 分割隧道 (IPv6 Split Tunneling)**：可以根据流量是使用 IPv4 寻址还是 IPv6 寻址来指定不同的选项，但每个流量的选项都相同。如果想要启用分割隧道，指定其中一个要求您选择网络对象的选项。
  - **允许所有流量通过隧道 (Allow all traffic over tunnel)**：不分割隧道。一旦用户建立远程访问VPN连接，用户的所有流量都会通过受保护隧道。这是默认值。这也被视为最安全的选项。

- **允许指定的流量通过隧道**：选择定义源网络的扩展访问列表。任何来自这些源的流量都会通过受保护隧道。客户端会将前往其他目标的流量路由至隧道外部（例如，本地 Wi-Fi 或网络连接）。
- **排除以下指定网络**：选择定义源网络的网络对象。客户端将来自这些源的任何流量路由到隧道外部的连接。来自任何其他来源的流量通过隧道。
- **网络列表**：选择可以同时具有 IPv4 和 IPv6 网络的扩展 ACL 网络。

- **分割 DNS**：您可以配置系统通过安全连接发送某些 DNS 请求，同时允许客户端将其他 DNS 请求发送到客户端上配置的 DNS 服务器。您可以配置以下 DNS 行为：
  - **根据分割隧道策略发送 DNS 请求 (Send DNS Request as per split tunnel policy)**：使用此选项时，系统将按照与定义分割隧道选项相同的方式处理DNS请求。如果启用分割隧道，则会根据目标地址发送 DNS 请求。如果未启用分割隧道，所有 DNS 请求都会通过受保护的连接。
  - **始终通过隧道发送 DNS 请求 (Always send DNS requests over tunnel)**：如果启用了分割隧道，但想要通过受保护连接将所有 DNS 请求发送到为该组定义的 DNS 服务器上，则可选择此选项。
  - **仅通过隧道发送指定的域 (Send only specified domains over tunnel)**：如果想要让受保护的 DNS 服务器仅解析特定域的地址，则可选择此选项。然后，指定这些域，用逗号分隔域名。例如，example.com, example1.com。如果想要让内部 DNS 服务器解析内部域的名称，同时让外部 DNS 服务器处理所有其他互联网流量，请使用此选项。

### AnyConnect 属性

组策略的 AnyConnect 属性定义 AnyConnect 客户端用于远程访问 VPN 连接的某些 SSL 和连接设置。

- **SSL 设置**
  - **启用数据报传输层安全 (DTLS) (Enable Datagram Transport Layer Security [DTLS])**：是否允许 AnyConnect 客户端使用两个同步隧道：SSL 隧道和 DTLS 隧道。使用 DTLS 可避免某些 SSL 连接带来的延迟和带宽问题，并可改进对数据包延迟敏感的实时应用的性能。如果不启用 DTLS，AnyConnect 客户端用户在建立 SSL VPN 连接时仅与 SSL 隧道连接。
  - **DTLS 压缩 (DTLS Compression)**：是否使用 LZS 为此组压缩数据报传输层安全 (DTLS) 连接。默认情况下会禁用 DTLS 压缩。
  - **SSL 压缩 (SSL Compression)**：是否启用数据压缩，如启用，则设置要使用的数据压缩方法：**Deflate** 或 **LZS**。默认情况下会**禁用** SSL 压缩。数据压缩加快了传输速率，但也增加了每个用户会话的内存需求和 CPU 使用率。因此，SSL 压缩会降低设备的整体吞吐量。
  - **SSL 重新生成密钥方法 (SSL Rekey Method)**、**SSL 重新生成密钥间隔 (SSL Rekey Interval)**：客户端能够为VPN连接重新生成密钥，重新协商加密密钥和初始化向量，从而提高连接的安全性。选择**无**可禁用重新生成密钥。要启用重新生成密钥，请选择 **新隧道 (New Tunnel)** 来创建新的隧道。（ **现有隧道 (Existing Tunnel)** 选项导致的操作与 **新隧道 (New Tunnel)** 的相同。）如果启用重新生成密钥，还需设置重新生成密钥间隔，默认间隔为 4 分钟。可以将间隔设置为 4 到 10080 分钟（1 周）。

- 连接设置
  - **忽略 DF（不分片）位 (Ignore the DF [Don't Fragment] bit)**：是否忽略需要分片的数据包内的“不分片” (DF) 位。选择此选项会允许强制将已设置 DF 位的数据包分片，从而使这些数据包能够通过隧道。
  - **客户端绕行协议**：允许您配置安全网关管理 IPv4 流量（安全网关仅允许 IPv6 流量时）或管理 IPv6 流量（安全网关仅允许 IPv4 流量时）的方式。

    当 AnyConnect 客户端建立与头端的 VPN 连接时，头端可以为客户端分配 IPv4 和/或 IPv6 地址。如果头端对 AnyConnect 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置 Client Bypass Protocol 以丢弃头端尚未分配 IP 地址（默认、已禁用、未检查）的网络流量，或允许该流量绕过头端并从客户端以未加密或“明文形式”发送（已启用、已检查）。

    例如，假设安全网关只将一个 IPv4 地址分配给 AnyConnect 连接，且终端为双协议栈。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。
  - **MTU**：思科 AnyConnect VPN 客户端为 SSL VPN 连接建立的最大传输单位 (MTU) 大小。默认值为 1406 字节。范围为 576 至 1462 字节。
    - **AnyConnect 和 VPN 网关之间的保持连接消息**：是否在对等体之间交换保持连接消息，以证明它们可用于在隧道中发送和接收数据。保持连接消息以设置的时间间隔传输。默认间隔为 20 秒，有效范围为 15 到 600 秒。
    - **网关端 DPD 间隔、客户端 DPD 间隔**：启用失效对等体检测 (DPD)，确保 VPN 网关或 VPN 客户端快速检测对等体不再响应的时间。您可以单独启用网关或客户端 DPD。发送 DPD 消息的默认间隔为 30 秒。时间间隔可以是 5 到 3600 秒。

### 流量过滤器属性

组策略的流量过滤器属性定义您想要对分配到该组的用户设置的限制。您可以使用这些属性（而非创建策略规则）根据主机或子网地址和协议或 VLAN 来限制远程访问 VPN 用户仅可访问特定资源。默认情况下，远程访问 VPN 用户不会受到组策略的限制，可以访问受保护网络上的任何目标。

- **访问列表过滤器 (Access List Filter)**：使用扩展的访问控制列表 (ACL) 限制访问权限。选择 Smart CLI 扩展 ACL 对象。扩展 ACL 允许您基于源地址、目的地址和协议（例如 IP 或 TCP）进行过滤。ACL 评估遵循自上而下、“先匹配的规则先应用”原则，因此，请确保特定规则放在一般规则之前。ACL 末尾不包含隐式“deny any”语句，因此如果您想要拒绝对几个子网的访问，同时允许其他访问，请确保在 ACL 末尾加上“permit any”规则。由于您无法在编辑扩展的 ACL Smart CLI 对象时创建网络对象，因此您应在编辑组策略之前创建 ACL。否则，您可能需要先创建对象，然后再返回来创建网络对象，最后创建您需要的所有访问控制条目。要创建 ACL，登录 FDM，请转至**设备 (Device)** > **高级配置 (Advanced Configuration)** > **智能 CLI (Smart CLI)** > **对象 (Objects)**，创建对象，并选择**扩展访问列表 (Extended Access List)** 作为对象类型。
- **限制 VPN 到 VLAN (Restrict VPN to VLAN)**：也称为“VLAN 映射”，此属性指定该组策略应用到的会话的出口 VLAN 接口。系统将该组中的所有流量都转发到所选 VLAN。使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。确保您指定了在设备子接口上定义的 VLAN 编号。值的范围为 1 到 4094。

### Windows 浏览器代理属性

组策略的 Windows 浏览器代理属性确定用户浏览器上定义的代理是否运行以及如何运行。

可以为 **VPN 会话期间浏览器代理**选择以下值之一：

- **终端设置无变化 (No change in endpoint settings)**：允许用户配置（或不配置）浏览器代理或 HTTP，并在已配置的情况下使用代理。
- **禁用浏览器代理 (Disable browser proxy)**：不使用为浏览器定义的代理（如有）。浏览器连接不会通过该代理。
- **自动检测设置 (Auto detect settings)**：在客户端设备的浏览器中启用自动代理服务器检测。
- **使用自定义设置 (Use custom settings)**：定义所有客户端设备应对 HTTP 流量使用的代理。配置以下设置：
  - **代理服务器 IP 或主机名 (Proxy Server IP or Hostname)、端口 (Port)**：代理服务器的 IP 地址或主机名，以及代理服务器用于代理连接的端口。主机和端口总共不能超过 100 个字符。
  - **浏览器例外列表 (Browser Proxy Exemption List)**：与例外列表中的主机/端口的连接不通过代理。添加不应使用代理的所有目标的主机/端口值。例如，www.example.com 端口 80。点击**添加代理例外 (Add proxy exemption)** 以将项目添加到列表。点击垃圾桶图标可删除项目。整个代理例外列表（包括所有地址和端口）不能超过 255 个字符。

## 创建 *ASA* 远程访问 *VPN* 配置

CDO 允许您将一个或多个自适应安全设备 (ASA) 设备添加到远程访问 VPN 配置向导，并配置与设备关联的 VPN 接口、访问控制和 NAT 豁免设置。因此，每个远程访问 VPN 配置都可以在与远程访问 VPN 配置关联的多个 ASA 设备之间共享连接配置文件和组策略。此外，您可以通过创建连接配置文件和组策略来增强配置。

您可以载入已配置远程访问 VPN 设置的 ASA 设备，也可以载入没有远程访问 VPN 设置的新设备。请参阅将 ASA 设备载入 CDO，第 135 页。当您载入已具有远程访问 VPN 设置的 ASA 设备时，CDO 会自动创建“默认远程访问 VPN 配置”并将 ASA 设备与此配置相关联。此外，此默认配置可以包含设备上定义的所有连接配置文件对象。有关详细信息，请参阅管理和部署预先存在的 ASA 远程访问 VPN 配置。CDO 允许您删除默认配置。

**重要事项**

- 不允许在同一远程访问 VPN 配置中添加 ASA 和 FTD。
- 一台 ASA 设备不能有多个远程访问 VPN 配置。

### 开始之前

在将 ASA 设备添加到远程访问 VPN 配置之前，ASA 设备必须满足以下前提条件：

- 许可证要求。

  必须启用设备才能使用出口控制功能。

要查看 ASA 设备的许可证摘要，请在 ASA 命令行界面中执行 show license summary 命令。要使用 CDO ASA CLI 界面，请参阅CDO 命令行界面。

- 许可证摘要中启用的出口控制功能示例：

注册：状态：已注册智能账户：Cisco SVS temp-request access license@cisco.com 出口控制功能：ALLOWED http://licensing@cisco.com

```
Last Renewal Attempt: None

Next Renewal Attempt: Jun 08 2021 09:46:22 UTC
```

要创建或编辑 VPN 配置，“导出控制功能”属性必须处于“允许”状态。

如果该属性处于“不允许”(Not Allowed) 状态，CDO 将在创建或修改 VPN 配置时显示错误信息（“无法为不符合出口标准的设备配置远程访问 VPN。”[remote access VPN cannot be configured for devices which are not export compliant.]），并且不允许在设备上配置远程访问 VPN。

- 设备身份证书。

  对客户端与 ASA 设备之间的连接进行身份验证需要使用证书。在开始 VPN 配置之前，请确保身份证书已存在于 ASA 设备上。

  要确定设备上是否存在证书，请在 ASA 命令行界面中执行 show crypto CA Certificates 命令。要使用 CDO ASA CLI 界面，请参阅CDO 命令行界面。

  如果身份证书不存在或者您想要注册新证书，请使用 CDO 在 ASA 上安装它们。请参阅 ASA 证书管理。

  中介绍了数字证书在远程访问 VPN 环境中的使用。远程访问 VPN 基于证书的身份验证，第 263 页

- 外部接口。

  必须已在 ASA 设备上配置外部接口。您需要使用 ASDM 或 ASA CLI 来配置接口。 要了解如何使用 ASDM 配置接口，请参阅《思科 ASA 系列常规操作 CLI 配置指南 X.Y》的“接口”一书。

- 下载 AnyConnect 软件包并将其上传到远程服务器。稍后，使用远程访问 VPN 向导或 ASA 文件管理向导将 AnyConnect 软件包从服务器上传到 ASA。有关说明，请参阅管理 ASA 设备上的 AnyConnect 软件包。

- 没有待处理的配置部署。

- 如果使用本地数据库进行身份验证，请使用 ASDM 或 ASA CLI 将用户账户添加到本地数据库。

  要使用 ASDM 添加用户帐户，请参阅《思科 ASA 系列 VPN CLI 配置指南，X.Y》的“AAA 服务器和本地数据库”一书中的“将用户帐户添加到本地数据库”部分。

  要使用 ASA CLI 添加用户账户，请执行 username password priv_level] 命令。**username[] password [] privilege [**

- ASA 更改会同步到 CDO。

  1. 在左侧的 CDO 导航栏中，点击**清单 (Inventory)** 并搜索一个或多个要同步的 ASA 设备。
  2. 选择一个或多个设备，然后点击检查更改。CDO 与一个或多个 FTD 设备通信以同步更改。

- 远程访问 VPN 配置组策略对象一致。
  - 确保解决所有不一致的组策略对象，因为它们无法添加到远程访问VPN配置中。解决问题或从“对象”(Objects) 页面删除不一致的组策略对象。有关详细信息，请参阅解决重复对象问题和解决不一致的对象问题。

---

**步骤 1** 将 ASA 设备载入 CDO，第 135 页。

**步骤 2** 在左侧的 CDO 导航栏中，点击 VPN ASA/FDM 远程访问 VPN 配置。 >

**步骤 3** 点击蓝色加号  按钮以创建远程访问 VPN 配置。

**步骤 4** 输入远程访问 VPN 配置的名称。

**步骤 5** 点击蓝色加号 (  ) 按钮将 ASA 设备添加到配置。

您可以添加设备详细信息并配置与设备关联的网络流量相关权限。

1. 提供以下设备详细信息：
   - 设备：选择要添加的ASA设备，然后点击选择。重要提示：不允许在同一远程访问VPN配置中添加ASA和FTD。
   - **设备身份证书 (Certificate of Device Identity)**：选择用于建立设备身份的内部证书。在 AnyConnect 客户端与设备进行连接时确定客户端的设备身份。客户端必须接受此证书才能完成安全的 VPN 连接。
   - **外部接口 (Outside Interface)**：选择用户在进行远程访问 VPN 连接时连接的接口。请选择您使用此连接配置文件支持的设备与最终用户之间的任何接口，虽然这通常是外部（面向互联网的）接口。

     **注意** 您无法为不符合导出要求的设备创建或修改远程访问 VPN 配置。您必须在启用出口控制功能的情况下许可 ASA 设备，然后重试。

2. 点击继续以配置流量权限。
   - **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)**：默认情况下，已解密流量要经过访问控制策略的检查。启用此选项可绕过解密流量选项，绕过访问控制策略检查，但从AAA服务器下载的VPN筛选ACL和授权 ACL 仍会应用于 VPN 流量。

     请注意，如果选择此选项，系统会配置 sysopt connection permit-vpn 命令，此为全局设置。这也会影响站点间 VPN 连接的行为。

     如果不选择此选项，外部用户可能会骗取远程访问 VPN 地址池中的 IP 地址，从而获取访问您网络的权限。这种情况可能会发生，因为您创建的访问控制规则需要允许地址池访问内部资源。如果您使用访问控制规则，请考虑使用用户说明来控制访问，而不是只使用源 IP 地址。

     选择此选项的弊端在于，VPN 流量将不会被检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映VPN连接。
   - **NAT 豁免 (NAT Exempt)**：NAT 豁免将豁免转换地址，并允许已转换的主机和远程主机发起与受保护主机的连接。配置 NAT 免除，使进出远程访问 VPN 终端的流量免于执行 NAT 转换。请参阅从 NAT 豁免远程访问流量，第 264 页。

3. 点击**确定 (OK)**。

“检测到的 AnyConnect 软件包”显示设备上已有的 AnyConnect 软件包。

有两个选项可用于从远程访问 VPN 向导将 AnyConnect 软件包上传到 ASA：

- （选项 1）：从 CDO 的存储库中选择一个软件包。ASA 必须能够访问互联网。
- （选项 2）：指定预加载 AnyConnect 软件包的 ftp/http/https/scp/smb/tftp URL 位置。

有关说明，请参阅管理 ASA 设备上的 AnyConnect 软件包。

**注释** 注意：如果要替换现有软件包，请参阅管理 ASA 设备上的 AnyConnect 软件包。

**步骤 6** 点击**确定 (OK)**。

ASA VPN 配置已创建。

---

修改 ASA 远程访问 VPN 配置

您可以修改现有远程访问 VPN 配置的名称和设备详细信息。

---

**步骤 1** 选择要修改的配置，然后在操作下点击编辑。

- 如果需要，请修改名称。
- 点击蓝色加号按钮  以添加新设备。
- 点击以在 ASA 设备上执行以下操作。 
  - 点击**编辑 (Edit)** 以修改现有的远程访问 VPN 配置。
  - 点击**删除 (Remove)**，从远程访问 VPN 配置中删除 ASA 设备。除组策略外，与该设备关联的所有连接配置文件和远程访问 VPN 设置都将被删除。您可以从对象页面中明确删除组策略。

    **Note** 如果 ASA 是唯一使用该配置的设备，则无法删除。或者，您可以删除远程访问 VPN 配置。

**步骤 2** 将配置更改从 CDO 部署到 ASA。

---

### What to do next

您还可以通过键入配置或设备的名称来搜索远程访问 VPN 配置。

**相关信息：**

- 配置 ASA 远程访问 VPN 连接配置文件, on page 251。

# 配置 *ASA* 远程访问 *VPN* 连接配置文件

远程访问 VPN 连接配置文件定义了一些特征，这些特征允许外部用户使用 AnyConnect 客户端与系统创建 VPN 连接。每个配置文件都定义了用于用户身份验证的 AAA 服务器和证书、分配用户 IP 地址的地址池，以及定义各种面向用户的属性的组策略。

如果需要为不同的用户组提供不同的服务，或者有不同的身份验证源，您可以在远程访问 VPN 配置中创建多个配置文件。例如，如果您的组织与使用不同身份验证服务器的组织合并，您可以为使用这些身份验证服务器的新组创建配置文件。

远程访问 VPN 连接配置文件让您的用户可在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。

### 开始之前

创建 ASA 远程访问 VPN 配置，第 247 页。

---

**步骤 1** 在 CDO 导航窗格中，点击**VPN** > **ASA/FDM 远程访问 VPN 配置 (ASA/FDM Remote Access VPN Configuration)**。您可以点击 VPN 配置以查看当前已配置多少连接配置文件和组策略的摘要信息。

**注释** 要了解分配给设备的组策略，请在操作中点击组策略。分配给连接配置文件的组策略会自动添加到列表中，并且无法删除。

如果您需要的组策略尚不存在，请点击  并从列表中进行选择。您可以创建其他组策略，以提供您所需的服务。请参阅创建 ASA 远程访问 VPN 组策略，第 241 页。

**步骤 2** 点击连接配置文件，然后在右侧边栏中的操作下点击添加连接配置文件。

**步骤 3** 配置基本连接属性。

- **连接配置文件名称 (Connection Profile Name)**：此连接的名称，最多 50 个字符，不能含空格。例如，MainOffice。

  **注释** 您在此输入的名称将是用户在 AnyConnect 客户端的连接列表中看到的名称。选择一个对您的用户来说有意义的名称。

- **组别名、组 URL (Group Alias, Group URL)**：别名包含特定连接配置文件的备用名称或 URL。在连接到 ASA 设备时，VPN 用户可以在连接列表中的 AnyConnect 客户端中选择别名。连接配置文件名称会自动添加为组别名。您还可以配置组 URL 列表，在发起远程访问 VPN 连接时您的终端可以从该列表中进行选择。如果用户使用组 URL 进行连接，系统将自动使用与 URL 匹配的连接配置文件。此 URL 供尚未安装 AnyConnect 客户端的客户使用。按需要添加组别名和 URL。在设备上定义的所有连接配置文件中，这些别名和 URL 必须是唯一的。组 URL 必须以 **https://** 开头。

- 例如，您可能有别名承包商和组 URLhttps://ravpn.example.com/contractor。安装 AnyConnect 客户端后，用户只需在连接的 AnyConnect VPN 下拉列表中选择组别名。

**步骤 4** 配置主身份源和辅助身份源（可选）。这些选项确定设备如何对远程用户进行身份验证，以启用远程访问 VPN 连接。最简单的方法是仅使用 AAA，然后选择 AD 领域或使用 LocalIdentitySource。根据**身份验证类型**，您可以使用以下方法：

- **仅 AAA (AAA Only)**：根据用户名和密码对用户进行身份验证和授权。有关详细信息，请参阅为连接配置文件配置 AAA ，第 252 页。
- **仅客户端证书 (Client Certificate Only)**：根据客户端设备身份证书进行用户身份验证。有关详细信息，请参阅为连接配置文件配置证书身份验证。
- **AAA 和 ClientCertificate (AAA and ClientCertificate)**：同时使用用户名/密码和客户端设备身份证书。

**步骤 5** 配置客户端的地址池。地址池定义了远程客户端在建立 VPN 连接时，系统可以分配给它们的 IP 地址。有关详细信息，请参阅配置客户端地址池分配。

**步骤 6** 点击**继续 (Continue)**。

**步骤 7** 从列表中选择要用于此配置文件的**组策略**，然后点击**选择 (Select)**。

组策略在建立隧道后设置用户连接的条款。系统包含名为“DfltGrpPolicy”的默认组策略。您可以创建其他组策略，以提供您所需的服务。请参阅创建 ASA 远程访问 VPN 组策略，第 241 页。

**步骤 8** 点击**继续 (Continue)**。

**步骤 9** 审核摘要。首先，验证摘要是否正确。您可以查看最终用户初步安装 AnyConnect 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击  将这些说明复制到剪贴板，然后分发给您的用户。

**步骤 10** 点击**完成 (Done)**。

**步骤 11** 执行适用于 ASA 的端到端远程访问 VPN 配置过程的步骤 5。ASA 的端到端远程访问 VPN 配置过程，第 235 页

---

为连接配置文件配置 AAA

身份验证、授权和记账(AAA)服务器使用用户名和密码来确认是否允许用户访问远程访问VPN。如果使用 RADIUS 服务器，则可以区分已验证用户的授权级别，从而提供对受保护资源的差异化访问权限。还可以使用 RADIUS 记账服务来跟踪使用情况。

在配置AAA时，您必须配置主身份源。辅助源和备用源是可选的。如果想要实施双重身份验证，请使用辅助源，例如，RSA 令牌或 DUO。

### 主身份源选项

- **用户身份验证的主身份源 (Primary Identity Source for User Authentication)**：身份验证提供了一种识别用户的方法，这种方法通常先请用户输入有效用户名和有效密码，然后再授予访问权限。用于对远程用户进行身份验证的主身份源。必须在此源或可选的回退源中定义最终用户，才能完成 VPN 连接。选择以下一个选项：
  - Active Directory (AD) 身份领域。
  - RADIUS 服务器组。
  - LocalIdentitySource（本地用户数据库）：您可以直接在设备上定义用户，而不使用外部服务器。

    您可以点击身份源创建新的身份源。为 ASA 配置身份源, on page 236

- **回退本地身份源 (Fallback Local Identity Source)**：如果主要源是一个外部服务器，您可以选择LocalIdentitySource作为回退源，以防主服务器不可用。如果使用本地数据库作为回退源，请确保您定义的本地用户名/密码与外部服务器中的定义的用户名/密码相同。
- **删除选项 (Strip options)**：领域是管理域。启用以下选项将允许仅基于用户名进行身份验证。您可以启用这些选项的任意组合。但是，如果服务器无法分析分隔符，则必须选中这两个复选框。
  - **从用户名删除身份源服务器 (Strip Identity Source Server from Username)**：在将用户名传递到AAA服务器之前，是否要从用户名删除身份源名称。例如，如果选择此选项且用户输入域\用户名作为用户名，则该域将从用户名中删除，并发送到AAA服务器进行身份验证。默认情况下，此选项处于取消选中状态。
  - **从用户名删除组 (Strip Group from Username)**：在将用户名传递到 AAA 服务器之前，是否要从用户名删除组名称。此选项适用于 username@domain 格式中给定的名称；此选项会剥离域和 @ 符号。默认情况下，此选项处于取消选中状态。

辅助身份源

- **用于用户授权的辅助身份源 (Secondary Identity Source for User Authorization)**：可选的第二个身份源。如果用户成功使用主要源进行身份验证，则系统会提示其使用辅助源进行身份验证。可以选择 AD 领域、RADIUS 服务器组或本地身份源。
- **高级 (Advanced) 选项**：点击**高级 (Advanced)** 链接并配置以下选项：
  - **辅助源的备用本地身份源 (Fallback Local Identity Source for Secondary)**：如果辅助源为外部服务器，您可以选择LocalIdentitySource作为备用源，以防辅助服务器不可用。如果使用本地数据库作为备用源，请确保您定义的本地用户名/密码与辅助外部服务器中定义的用户名/密码相同。
  - **使用主要用户名进行辅助登录 (Use Primary Username for Secondary Login)**：默认情况下，使用辅助身份源时，系统将提示输入辅助源的用户名和密码。如果选择此选项，系统将仅提示您输入辅助密码，并使用与主身份源相同的用户名来进行辅助源身份验证。如果您在主身份源和辅助身份源中配置了相同的用户名，请选择此选项。
    - **会话服务器用户名 (Username for Session Server)**：身份验证成功后，用户名将显示在事件和统计控制面板中，用于确定基于用户或组的 SSL 解密和访问控制规则之间的匹配关系，并用于记账。由于使用了两个身份验证源，因此您需要告诉系统是使用主用户名还是辅助用户名作为用户身份。默认情况下，使用主用户名。
    - **密码类型 (Password Type)**：如何获取辅助服务器的密码。默认值为**提示**，这表明系统将提示用户输入密码。选择**主身份源密码**，自动使用用户在主服务器中进行身份验证时输入的密码。选择**公用密码**，为每个用户使用相同的密码，然后在**公用密码**字段中输入该密码。
  - **授权服务器 (Authorization Server)**：已配置为授权远程访问 VPN 用户的 RADIUS 服务器组。身份验证完成后，授权将控制对每个经过身份验证的用户都可用的服务和命令。授权通过组合一组描述用户被授权执行的操作、其实际功能和限制的属性来工作。如果您不使用授权，则单独的身份验证将为所有经过身份验证的用户提供相同的访问权限。

请注意，如果系统从 RADIUS 服务器获取的授权属性与组策略中定义的属性重叠，则 RADIUS 属性将覆盖组策略属性。

您可以点击创建 RADIUS 服务器组来创建新的服务器组。创建 ASA RADIUS 服务器对象或组, on page 239

- **记账服务器 (Accounting Server)**：（可选。）用于为远程访问 VPN 会话记账的 RADIUS 服务器组。记账会跟踪用户正在访问的服务以及他们正在使用的网络资源数量。ASA 设备向 RADIUS 服务器报告用户活动。记账信息包括每个会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。然后，您可分析该数据，以进行网络管理、客户端计费或审核。您可以单独使用记账功能，也可以将其与身份验证和授权功能配合使用。

  您可以点击创建 RADIUS 服务器组来创建新的服务器组。创建 ASA RADIUS 服务器对象或组, on page 239

### 为连接配置文件配置证书身份验证

**Note** 此部分不适用于仅作为 AAA 的身份验证类型。

可以使用客户端设备安装的证书对远程访问 VPN 连接进行身份验证。

使用客户端证书时，仍可以配置辅助身份源、备用源，以及授权和记账服务器。这些是 AAA 选项；有关详细信息，请参阅配置 ASA 远程访问 VPN 连接配置文件, on page 251。

以下是证书特定的属性。您可以为主身份源和辅助身份源单独配置这些属性。配置辅助源为可选操作。

- **从证书中获取的用户名 (Username from Certificate)**：选择以下选项之一：
  - **映射特定字段 (Map Specific Field)**：按照**主要字段 (Primary Field)** 和**辅助字段 (Secondary Field)** 的顺序使用证书元素。默认值为 CN（公用名）和 OU（组织单位）。选择适用于您的组织的选项。这些字段组合在一起用于提供用户名，此名称用于事件和控制面板中，并出于匹配的目的，在 SSL 解密和访问控制规则中使用。
  - **使用完整 DN（可分辨名称）作为用户名 (Use entire DN [distinguished name] as username)**：系统自动从 DN 字段派生出用户名。
- 高级选项（不适用于作为仅客户端证书的身份验证类型）：点击高级链接并配置以下选项：
  - **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)**：在提示用户进行身份验证时，是否在用户名字段填写检索到的用户名。
  - **在登录窗口隐藏用户名 (Hide username in login window)**：如果选择**预填充 (Prefill)** 选项，则可以隐藏用户名，这意味着用户无法编辑密码提示中的用户名。

### 配置客户端地址池分配

系统必须可以通过某种方法向连接到远程访问 VPN 的终端提供 IP 地址。AAA 服务器、DHCP 服务器、组策略中配置的 IP 地址池，或连接配置文件中配置的 IP 地址池可以提供这些地址。系统会按照以上顺序尝试使用这些资源，并在获取一个可用地址后停止尝试，然后将此地址分配给客户端。因此，您可以配置多个选项，以便在并发连接数异常多的情况下，可保障系统能获取地址。

使用下列一个或多个方法配置连接配置文件的地址池。

- IPv4 地址池和 IPv4 地址池：首先，创建最多六个指定子网的网络对象。可以为 IPv4 和 IPv6 单独配置池。然后，在组策略或者连接配置文件的 **IPv4 地址池 (IPv4 Address Pool)** 和 **IPv6 地址池 (IPv6 Address Pool)** 选项中，选择这些对象。无需同时配置 IPv4 和 IPv6，配置您想要支持的寻址方案即可。也不需要同时在组策略和连接配置文件中配置池。组策略会覆盖连接配置文件的设置，因此如果您在组策略中配置了池，则请将连接配置文件中的选项留空。请注意，系统按照您列出的顺序使用地址池。要创建新的 IPv4 地址池或新的 IPv6 地址池，请参阅创建 IP 地址池。
- **DHCP 服务器 (DHCP Servers)**：首先，使用一个或多个 IPv4 地址范围为远程访问 VPN 配置 DHCP 服务器（您无法使用 DHCP 配置 IPv6 池）。然后，使用 DHCP 服务器的 IP 地址创建主机网络对象。随后，便可以在连接配置文件的 **DHCP 服务器 (DHCP Servers)**属性中选择此对象。可以配置多个 DHCP 服务器。如果 DHCP 服务器有多个地址池，则可以在与连接配置文件关联的创建 ASA 远程访问 VPN 组策略中使用 **DHCP 作用域 (DHCP Scope)** 属性，选择要使用的池。使用池的网络地址创建主机网络对象。例如，如果 DHCP 池包含 192.168.15.0/24 和 192.168.16.0/24，将 DHCP 范围设置为 192.168.16.0 可确保从 192.168.16.0/24 子网中选择地址。

**相关信息：**

ASA 的端到端远程访问 VPN 配置过程

## 管理 *ASA* 设备上的 *AnyConnect* 软件包

您可以执行以下步骤之一，使用远程访问 VPN 向导上传 AnyConnect 软件包：

- 从 CDO 存储库上传软件包。
- 使用 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP 协议从服务器上传数据包。

### 从 CDO 存储库上传 AnyConnect 软件包

远程访问 VPN 配置向导显示 CDO 存储库中每个操作系统的 AnyConnect 软件包，您可以从中选择并上传到设备。确保设备可以访问互联网并进行正确的 DNS 配置。

**注释** 如果所需的软件包在显示的列表中不可用，或者设备无法访问互联网，则可以使用预加载 AnyConnect 软件包的服务器上传软件包。

**步骤 1** 点击与操作系统对应的字段，然后选择 AnyConnect 软件包。

**步骤 2** 点击  以上传软件包。如果校验和不匹配，则 AnyConnect 软件包上传失败。您可以查看设备的工作流程选项卡，了解有关故障的更多详细信息。

从服务器将 AnyConnect 软件包上传到 ASA

将 AnyConnect 客户端软件包下载到您的计算机，并将其上传到可从 ASA 访问的远程服务器。稍后，使用 RA VPN 向导或 ASA 文件管理向导将 AnyConnect 软件包从该服务器上传到 ASA。必须在设备上为使用域名的 URL 正确配置 DNS。

ASA RA VPN 向导支持使用 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP 协议上传数据包。

用于上传文件的受支持协议的语法：

| 协议 | 语法 | 示例 |
|---|---|---|
| HTTP | http://[[path/]filename] | http://www.geonames.org/data-sources.html |
| HTTPS | https://[[path/]filename] | https://docs.aws.amazon.com/amazov/tagging.html |
| TFTP | tftp://[[path/]filename] | tftp://10.10.16.6/ftd/components.html |
| FTP | ftp://[user[:password]@]server[:port]/[path/]filename] | [illegible] |
| 中小企业 | smb://[[path/]filename] | smb://10.10.32.145//sambashare/hello.txt |
| SCP | scp://[[user[:password]@]server[/path]/filename] | scp://root:cisco123@10.10.10.166//root/events_send.py |

**Before you begin**

请确保为所需的操作系统下载“AnyConnect 前端部署软件包”。始终下载最新的 AnyConnect 版本，以确保获得最新的功能、漏洞修复和安全补丁。请定期更新设备上的软件包。

**Important** 如果您选择使用 ASA 文件管理向导上传软件包，请不要在下载后修改软件包的名称。

**Note** 您可以为以下每个操作系统 (OS) 上传一个 AnyConnect 软件包：Windows、Mac 和 Linux。无法为特定操作系统类型上传多个版本。

**步骤 1** 从 https://software.cisco.com/download/home/283000185 下载 AnyConnect 软件包。

- 确保您接受 EULA 并具有 K9（加密映像）权限。
- 为您的操作系统选择“AnyConnect 前端部署软件包”。软件包名称类似于“anyconnect-win-4.7.04056-webdeploy-k9.pkg”。有适用于 Windows、macOS 和 Linux 的单独前端软件包。

**步骤 2** 将 AnyConnect 软件包上传到远程服务器。确保存在来自 ASA 设备和服务器的网络路由。

ASA RA VPN 向导支持上传数据包 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP 协议。

**Important** 如果要将 AnyConnect 软件包上传到 HTTPS 服务器，请确保执行以下步骤：

- 在 ASA 设备上上传该服务器的受信任 CA 证书。
- 在 HTTPS 服务器上安装受信任的 CA 证书。

**步骤 3** 远程服务器的 URL 必须是不提示进行身份验证的直接链接。如果 URL 已进行预身份验证，则可以通过指定 RA VPN 向导的 URL 来下载文件。

**步骤 4** 如果远程服务器 IP 地址经过 NAT，则必须提供远程服务器位置的 NAT 公共 IP 地址。

---

将新的 AnyConnect 软件包上传到 ASA

您可以使用 RA VPN 向导或 ASA 文件管理向导将 AnyConnect 软件包上传到 ASA。

使用以下程序将新的 AnyConnect 软件包从 HTTP 或 HTTPS 服务器上传到 ASA 设备：

---

**步骤 1** 在**检测到的 AnyConnect 软件包 (AnyConnect Package Detected)** 中，您可以为 Windows、Mac 和 Linux 终端上传单独的软件包。

**步骤 2** 在相应的平台字段中，指定预上传与 Windows、Mac 和 Linux 兼容的 AnyConnect 软件包的服务器路径。服务器路径示例：'http://<ip_address> :port_number/<folder_name> /anyconnect-win-4.8.01090-webdeploy-k9.pkg', 'https:// :port_number/ /anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'。

**步骤 3** 点击 以上传软件包。CDO 验证路径是否可访问，以及指定的文件名是否有效。验证成功后，系统将显示 AnyConnect 软件包的名称。当您将更多 ASA 设备添加到 RA VPN 配置时，您可以将 AnyConnect 软件包上传到这些设备。

**步骤 4** 点击**确定 (OK)**。AnyConnect 软件包已添加到 RA VPN 配置中。

**步骤 5** 从第 5 步开始创建 ASA 远程访问 VPN 配置。

---

### What to do next

要完成 VPN 连接，您的用户必须在他们的工作站上安装 AnyConnect 客户端软件。有关详细信息，请参阅用户如何在 ASA 上安装 AnyConnect 客户端软件 。

使用文件管理向导上传 AnyConnect 软件包

使用文件管理向导将 AnyConnect 软件包从 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP 服务器上传到单个或多个 ASA 设备。当您想要将 AnyConnect 软件包同时推送到多个 ASA 设备时，批量上传会派上用场。有关详细信息，请参阅 ASA 文件管理。

**Important** 如果您选择使用 ASA 文件管理向导上传软件包，请不要在下载后修改软件包的名称。

上传完成后，打开 ASA RA VPN 配置向导，您会注意到软件包已自动检测到。如果您为一个操作系统版本上传多个软件包，向导会在下拉列表中列出这些软件包，以便您从中选择一个。然后，您可以创建 RA VPN 配置并将其部署到设备。

## 替换现有的 AnyConnect 软件包

如果设备上已存在 AnyConnect 软件包，您可以在 RA VPN 向导中看到它们。您可以在下拉列表中查看操作系统的所有可用 AnyConnect 软件包。您可以从列表中选择现有软件包并将其替换为新软件包，但不能向列表中添加新软件包。

**Note** 如果要将现有软件包替换为新软件包，请确保已将新的 AnyConnect 软件包上传到 ASA 可以访问的网络上的服务器。

**步骤 1** 在左侧的 CDO 导航栏中，点击 VPN ASA/FDM Remote Access VPN。 >

**步骤 2** 选择要修改的 RA VPN 配置，然后在操作下点击编辑。

**步骤 3** 在“检测到的 AnyConnect 软件包”中，点击现有 AnyConnect 软件包旁边的图标。如果操作系统有多个版本的 AnyConnect 软件包，请从列表中选择要替换的软件包，然后点击编辑。现有软件包将从相应字段中消失。

**步骤 4** 指定预加载新 AnyConnect 软件包的服务器路径，然后点击 上传软件包。

**步骤 5** 点击**确定 (OK)**。新的 AnyConnect 软件包已添加到 RA VPN 配置中。

**步骤 6** 从步骤 6 开始继续创建 ASA 远程访问 VPN 配置, on page 247。

## 删除 AnyConnect 软件包

**步骤 1** 在左侧的 CDO 导航栏中，点击 VPN ASA/FDM Remote Access VPN。 >

**步骤 2** 选择要修改的 RA VPN 配置，然后在操作下点击编辑。

**步骤 3** 在“检测到的 AnyConnect 软件包”中，点击要删除的 AnyConnect 软件包旁边的图标。如果某个操作系统有多个版本的 AnyConnect 软件包，请从列表中选择要删除的软件包。现有软件包将从相应字段中消失。

**Note** 点击取消以停止删除操作并保留现有软件包，

**步骤 4** 点击**确定 (OK)**。设备的配置状态处于“未同步”状态。

**Note** 如果要在此阶段撤消删除操作，请转到**清单 (Inventory)** 页面，然后点击**放弃更改 (Discard Changes)** 以保留现有的 AnyConnect 软件包。

**步骤 5** 将配置更改从 CDO 部署到 ASA。

## 管理和部署预先存在的 ASA 远程访问 VPN 配置

当您载入已具有 RA VPN 设置的 ASDM 托管 ASA 设备时，它会发现并显示现有的远程访问 VPN 配置。CDO 会自动创建“默认 RA VPN 配置”，并将 ASA 设备与此配置相关联。有些 RA VPN 配置在 CDO 中无法读取或不受支持，但可以在 CDO 命令行界面中进行配置。

**Note** 本节未涵盖 CDO 中支持或不支持的每个配置。相反，它仅介绍最常用的内容。

要从已载入的 ASA 查看 RA VPN 配置，请执行以下步骤：

**步骤 1** 在 CDO 界面上，导航至 VPN ASA/FDM 远程访问 VPN 配置。 >

**步骤 2** 点击与载入的 ASA 设备对应的 RA VPN 配置。CDO 会自动创建“Default_RA_VPN_Configuration”并将 ASA 设备与此配置关联。您可以删除默认配置。在 CDO 中读取的 ASA RA VPN 配置分类如下：

- 设备设置
- 连接配置文件
- 组策略

设备设置

与载入的 ASA 设备关联的 RA VPN 配置显示在 Default_RA_VPN_Configuration 中。您需要点击此配置以查看与该配置关联的 ASA 设备的名称（在右侧的设备窗格中）。您还可以通过点击编辑按钮查看 ASA 设备中的 AnyConnect 软件包。

连接配置文件

CDO 支持并读取 ASA 设备的“AnyConnect 客户端 VPN 访问”中定义的连接配置文件。它不支持“无客户端 SSL VPN 访问”配置。

要查看连接配置文件属性，请执行以下步骤：

**步骤 1** 展开 **Default_RA_VPN_Configuration**。

**步骤 2** 点击所需的连接配置文件之一，然后点击**编辑**。

所有基本和高级 ASA RA VPN 属性都可以在 CDO RA VPN 配置页面的**连接配置文件名称和详细信息**中看到。

**Note** 您可以删除默认配置（选择默认的 RA VPN 配置，然后在右侧的**操作**窗格中点击**删除**）。

主身份源

- CDO 将 Connection Aliases 和 Group URLs 属性读取为 Group Alias 和 Group URL。

**Note**

- 系统不会读取配置了 SAML、多个证书和 AAA 以及多个证书的连接配置文件。
- 不支持具有接口和服务器组的身份验证服务器组。

- CDO 支持在主身份源中使用“AAA”、“AAA 和证书”和“仅证书”身份验证方法配置的 AnyConnect 连接配置文件。
- AAA 服务器组在 CDO 中被读取为主身份源中用户身份验证的主身份源（您可以通过选择 AAA 或 AAA 和客户端证书作为身份验证类型来查看此属性）。
  - 如果 AAA 服务器组配置的内容不是 LOCAL，则 CDO 会在主身份源下的“回退本地身份源”字段中读取并显示此属性。（您可以通过选择AAA作为身份验证类型来查看此属性）。

    要了解有关 CDO 中读取的服务器组属性的详细信息，请参阅 AAA 服务器组。

### 辅助身份源

辅助身份源显示 ASA 设备的辅助身份验证属性。要查看这些属性，请选择 AAA 或 AAA 和客户端证书作为身份验证类型，然后点击查看辅助身份源。

- 用户身份验证的辅助身份源显示辅助身份验证服务器组属性。
  - 如果服务器组配置的内容不是 LOCAL，则 CDO 会在“辅助身份源”下的“备用本地身份源”字段中读取并显示此属性。
- CDO 不支持 Attribute Server 和 Interface-Specific Authorization Server Groups 属性。

要了解有关 CDO 中读取的服务器组属性的详细信息，请参阅 AAA 服务器组。

### 授权服务器

- 授权服务器显示授权服务器组属性。
- CDO 不支持具有接口和服务器组的授权服务器组。

要了解有关 CDO 中读取的 RADIUS 服务器组属性的详细信息，请参阅 RADIUS 服务器组。

### 审计服务器

记帐服务器显示记帐服务器组属性。要了解有关 CDO 中读取的服务器组属性的详细信息，请参阅 RADIUS 服务器组。

客户端地址池分配

CDO 会将**客户端地址分配属性**（**DHCP 服务器**、**客户端地址池**和**客户端 IPv6 地址池**）作为对象进行读取。（您可以在客户端地址池分配中查看这些属性）。DHCP服务器详细信息以文字形式读取。

**Note** CDO 不支持在特定接口上分配 IP 地址池。但是，可以在 ASA 命令行界面 (CLI) 中看到这些属性。

*AAA* 服务器组

CDO 将 LDAP 服务器组及其关联的 LDAP 服务器表示为 Active Directory 领域对象。对于 Active Directory (AD)，领域就等于 Active Directory 域。请注意，CDO 会读取已经存在的 AD 领域对象的 AD 密码。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 应用 Active Directory 领域过滤器以查看此对象。

**步骤 3** 选择所需的 Active Directory 领域对象，然后点击编辑以查看其详细信息。

**What to do next**

可以看到 AD 领域包含关联的 AD 服务器及其配置。如果 AD 领域有多个 Active Directory (AD) 服务器，则 AD 服务器需要彼此重复，并支持相同的 AD 域。因此，与该 AD 领域关联的所有 AD 服务器的基本领域属性（例如目录名称、目录密码和基本可分辨名称）必须相同。如果这些属性不同，CDO 会在 Active Directory 领域对象中显示警告消息。您必须更正这些属性，使它们在所有 AD 服务器之间保持一致。如果继续而不解决此警告，CDO 将使用其中一个 AD 服务器属性并将其应用于该领域对象中的其他服务器。

*RADIUS* 服务器组

ASA 设备的 AAA RADIUS 服务器组属性在 CDO 中作为 RADIUS 服务器组对象读取。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 应用 RADIUS 服务器组过滤器以查看此对象。

**步骤 3** 选择所需的对象，然后点击编辑以查看其详细信息。

- 在 ASA 中启用动态授权在 CDO 中读取为动态授权（仅适用于 RA VPN）。
- 重新激活模式下的耗尽选项在 CDO 中读取，因此与耗尽时间关联的死区时间值在 CDO 中读取。但是，不会在 CDO 中读取 Timed 属性。
- CDO 不支持记账模式、定时、启用临时记账更新、启用临时记账更新和仅使用授权模式。

*RADIUS* 服务器

当 CDO 从 ASA 读取 Radius 服务器时，它会创建一个 Radius 服务器对象，该对象将名称指定为“Radius 服务器组名称或 IP 地址”。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 应用 RADIUS 服务器过滤器以查看此对象。

**步骤 3** 选择所需的对象，然后点击编辑以查看其详细信息。

组策略

在**组策略 (Group Policy)** 部分中，点击下拉列表以查看与设备关联的组策略。

**Attention** CDO 将使用隧道协议配置的组策略读取为 **SSL VPN 客户端**。

CDO 读取 ASA 中配置的大多数组策略属性。该信息显示在 RA VPN 组策略向导中的选项卡中。要查看从 ASA 设备读取的组策略的详细信息，您需要执行以下操作：

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FTD 网络对象 (FTD Network Objects)**。

**步骤 2** **RA VPN 组策略**的过滤器。

**步骤 3** 选择与该设备关联的组策略，然后点击**编辑 (Edit)**。

**What to do next**

**Note** CDO 不支持 ASA 设备的分割隧道中定义的标准访问控制列表 (ACL)。它支持扩展访问控制列表 (ACL) 并将其作为 ACL 读取到 ASA 策略中。有关详细信息，请参阅ASA 远程访问 VPN 组策略属性。要查看策略，可以在导航栏上点击**策略 (Policies)** > **ASA 访问策略 (ASA Access Policies)**。

要选择扩展 ACL，请执行以下操作：

- 点击**拆分隧道 (Split Tunneling)** 选项卡。
- 根据 ASA 中的流量是使用 IPv4 还是 IPv6 地址，从相应的下拉列表中选择“允许指定的流量通过隧道”(Allow specified traffic over tunnel) 或“排除下面指定的网络”(Exclude networks specified below)。选择从 ASA 导入的扩展 ACL。

## 创建 IP 地址池

您可以为 ASA 配置 IPv4 和 IPv6 IP 地址池，以将其分配给使用 VPN 连接远程连接到您的网络的客户端。地址池的指定顺序非常重要。如果为连接配置文件或组策略配置了多个地址池，则ASA将按您向 ASA 添加地址池的顺序使用地址池。

要定义 IPv4 地址池，请提供 IP 地址范围。IPv4 地址池的一个示例是 10.10.147.100 - 10.10.147.177。

定义 IPv6 地址池时，需要提供起始地址范围、地址前缀和地址池可配置的地址数量。IPv6 地址池的一个示例是 2001:DB8:1::1。

如果从非本地子网分配地址，我们建议添加位于子网边界的地址池，从而可更轻松地添加这些网络的路由。

执行以下操作以创建 IP 地址池：

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

**步骤 2** 点击蓝色加号按钮  ，然后选择 **ASA** > **地址池 (Address Pool)**。

**步骤 3** 在**创建 IP 地址池 (Create IP Address Pool)** 对话框中输入以下信息：

- **对象名称 (Object Name)**：输入地址池的名称。最多可包含 64 个字符
- **IPv4 地址池 (IPv4 address pool)**：选择此单选按钮可配置 IPv4 地址池。
  - **IPv4 地址范围 (IPv4 Address Range)**：输入每个配置的池中可用的第一个 IP 地址和最后一个 IP 地址。例如，10.10.147.100 - 10.10.147.177。
  - **掩码 (Mask)**：标识此 IP 地址池所属的子网。
- **IPv6 地址池 (IPv6 address pool)**：选择此单选按钮可配置 IPv6 地址池。
  - **IPv6 地址**：输入配置的池中可用的第一个 IP 地址和前缀长度（以位为单位）。 <address>/<prefix> 格式。例如，2001:DB8:1::1/3。
  - **地址数量 (Number of Addresses)**：标识地址池中从开始 IP 地址开始的 IPv6 地址的数量。

**步骤 4** 点击**保存 (Save)**。

## 远程访问 VPN 基于证书的身份验证

在以下情况下，远程访问 VPN 使用数字证书对安全网关和 AnyConnect 客户端（终端）进行身份验证：

**重要事项** CDO 处理 VPN 头端 (ASA ) 上的数字证书安装。它不处理 AnyConnect 客户端设备上的证书安装。您的组织的管理员必须处理此问题。

- 识别和认证 VPN 前端设备 (ASA )：

当 AnyConnect 客户端请求 VPN 连接时，VPN 头端需要身份证书来识别和认证自己。使用 CDO，您必须在设备上安装身份证书。请参阅使用 PKCS12 或证书和密钥安装身份证书。不强制要求在 AnyConnect 客户端上安装颁发机构的 CA 证书。

从 CDO 创建远程访问 VPN 配置时，将注册的身份证书分配给设备的外部接口，并将配置下载到设备。身份证书在设备的外部接口上完全可操作。

当 AnyConnect 客户端尝试连接到 VPN 时，设备通过向 AnyConnect 客户端提供其身份证书来对自身进行身份验证。AnyConnect 客户端使用其受信任的 CA 证书验证此身份证书，并信任该证书，从而信任设备。如果 CA 证书未安装在 AnyConnect 客户端上，则用户必须在系统提示时手动信任设备。

- 识别和认证 AnyConnect 客户端：

**注释** 当您在 RA VPN 配置的连接配置文件中使用“仅客户端证书”或“AAA 和客户端证书”作为身份验证方法时，这适用。它不适用于“仅 AAA”。

设备受信任后，AnyConnect 客户端需要对自身进行身份验证才能完成 VPN 连接。您必须在 AnyConnect 客户端上安装身份证书，并使用 CDO 在设备上安装受信任的 CA 证书。这些证书必须由同一证书颁发机构颁发。请参阅在 ASA 中安装受信任的 CA 证书。

AnyConnect 客户端提供其身份证书，设备使用其受信任的 CA 证书验证此证书并建立 VPN 连接。

## 从 NAT 豁免远程访问流量

配置 NAT 免除，使进出远程访问 VPN 终端的流量免于执行 NAT 转换。如果不豁免 VPN 流量执行 NAT，请确保外部和内部接口的现有 NAT 规则不适用于 RA VPN 地址池。NAT 豁免规则是给定源/目标接口和网络组合的手动静态身份 NAT 规则，但它们不会反映在 NAT 策略中，它们是隐藏起来的。如果启用 NAT 豁免，还必须进行以下配置。

- **内部接口**：选择远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
- **内部网络**：选择代表远程用户将访问的内部网络的网络对象。网络列表必须包含与您支持的地址池相同的 IP 类型。

### 开始之前

创建与该设备的连接配置文件和组策略中使用的本地 IP 地址池的配置相匹配的 ASA 网络对象。配置 NAT 规则时，必须将这些网络对象分配为目的地址和转换后的地址。请参阅创建 ASA 网络对象，第 113 页。

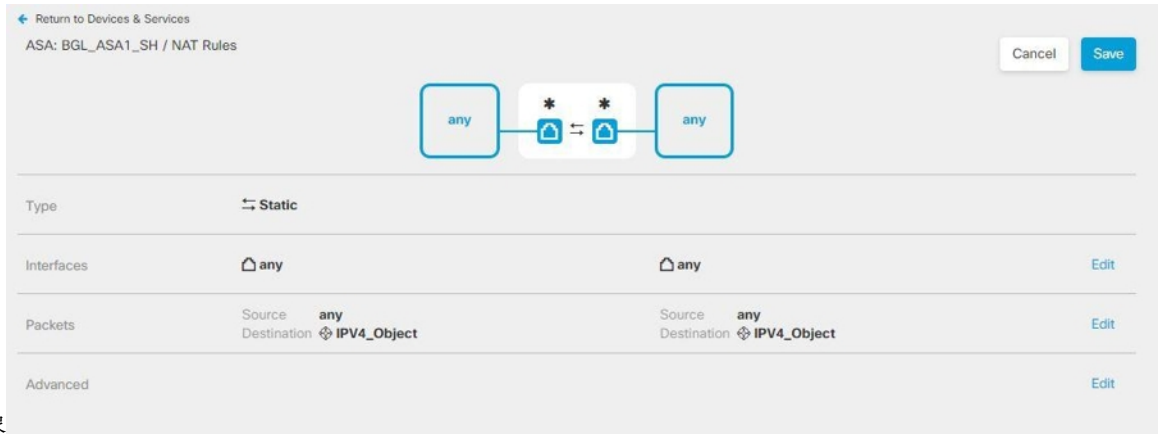
**步骤 1** 在 CDO 导航栏中，点击**清单 (Inventory)**。

**步骤 2** 使用**清单 (Inventory)** 过滤器和搜索字段查找要为其创建 NAT 规则的 ASA 设备。

**步骤 3** 在详细信息面板的**管理 (Management)** 区域中，点击 **NAT** NAT。

**步骤 4** 点击 + > **两次 NAT (Twice NAT)**。

1. 在第 1 部分中，选择**静态 (Static)**。点击**继续**。
2. 在第 2 部分中，选择**源接口 (Source Interface)** = 'any' 以及**目标接口 (Destination Interface)** = 'any'。点击**继续 (Continue)**。
3. 在第 3 部分中，选择**源接口地址 (Source Original Address)** = 'any' 以及**源转换地址 (Source Translated Address)** = 'any'。
4. 选择**使用目标 (Use Destination)**。
   1. **目标原始地址 (Destination Original Address)** 和**源转换地址 (Source Translated Address)**：点击下拉列表中的**选择 (Choose)**，然后选择与本地 IP 地址池的配置匹配的网络对象。在下面的示例中，“IPV4_Object”是与 ASA (BGL_ASA1_SH) 设备的连接配置文件和组策略设置中使用的 IPv4 地址池对象具有相同配置的网络对象




   2. 选择**为传入数据包禁用代理 ARP (Disable proxy ARP for incoming packets)**。
   3. 点击**保存 (Save)**。
   4. 重复此过程（从步骤 4 开始），为与 IP 地址池等效的每个其他网络对象创建等效规则。

**步骤 5** 将配置更改从 CDO 部署到 ASA。

## 用户如何在 ASA 上安装 AnyConnect 客户端软件

要完成 VPN 连接，您的用户必须安装 AnyConnect 客户端软件。可以使用现有的软件分发方法直接安装该软件。或者，可以让用户直接从 ASA 设备安装 AnyConnect 客户端。

**Note** 用户必须对其工作站具有管理员权限才能安装软件。

如果您决定让用户一开始从 ASA 设备安装软件，请告知用户执行以下步骤。

**Note** Android 和 iOS 用户应从相应的应用商店下载 AnyConnect。

**步骤 1** 使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。您在配置远程访问 VPN 时确定此接口。系统提示用户登录。

**步骤 2** 登录到网站。用户使用为远程访问 VPN 配置的目录服务器进行身份验证。登录成功后可继续操作。如果登录成功，系统将确定用户是否已具有所需的 AnyConnect 客户端版本。如果用户的计算机上没有 AnyConnect 客户端，或者客户端的版本较低，系统将自动开始安装 AnyConnect 软件。安装后，AnyConnect 会完成远程访问 VPN 连接。

## 修改 ASA 远程访问 VPN 配置

当 ASA 设备载入 CDO 时，它会发现并显示来自载入的 ASA 设备的原有远程访问 VPN 配置。有关详细信息，请参阅管理和部署预先存在的 ASA 远程访问 VPN 配置，第 259 页。

您可以修改这些配置并将新配置下载到设备。

- 修改 ASA 远程访问 VPN 配置
- 修改 ASA 连接配置文件

### 修改远程访问 *VPN* 配置

**步骤 1** 在左侧的 CDO 导航栏中，点击 VPN > 远程访问 VPN 配置。

**步骤 2** 如果要在 VPN 配置中添加或删除组策略，请点击与载入的 ASA 设备关联的 VPN 配置。在左侧的操作窗格中，点击组策略。

a) 点击蓝色 + 图标并配置选择，然后点击选择。

b) 点击“保存”(Save)。您还可以创建 ASA 远程访问 VPN 组策略。

**步骤 3** 点击 VPN 配置，然后在左侧的操作窗格中，点击编辑。

向导将列出与配置关联的 ASA 设备。

a) 您可以按照与创建时相同的方式修改以下详细信息：

- 更改远程访问 VPN 配置的名称。
- 点击显示设备详细信息的行中显示的三个点，然后点击编辑。

有关详细信息，请参阅创建 ASA 远程访问 VPN 配置，第 247 页

**步骤 4** 点击**确定**。

**步骤 5** 预览和部署所有设备的配置更改，第 313 页

修改 *ASA* 连接配置文件

**步骤 1** 在左侧的 CDO 导航栏中，点击 VPN > 远程访问 VPN 配置。

**步骤 2** 展开与载入的 ASA 设备关联的 VPN 配置，并选择连接配置文件。

**步骤 3** 在左侧的**操作 (Actions)** 窗格中，点击**编辑 (Edit)**。

**步骤 4** 以与创建时相同的方式编辑值，然后点击完成。

有关详细信息，请参阅配置 ASA 远程访问 VPN 连接配置文件 ，第 251 页

**步骤 5** 预览和部署所有设备的配置更改 ，第 313 页

### 上传 RA AnyConnect 客户端配置文件

远程访问 VPN AnyConnect 客户端配置文件是存储在文件中的一组配置参数。这些不同的 AnyConnect 客户端配置文件包含核心客户端 VPN 功能和可选客户端模块网络访问管理器、AMP 启动器、ISE 终端安全评估、网络可视性、客户体验反馈、Umbrella 漫游安全和网络安全的配置设置。

CDO 允许将这些配置文件作为对象上传，以便稍后在组策略中使用。

- **AnyConnect VPN 配置文件 (AnyConnect VPN Profile)** - AnyConnect 客户端配置文件随 AnyConnect 客户端软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及最终用户是否可以更改 AnyConnect 客户端首选项和高级设置中的选项。CDO 支持 XML 文件格式。
- **AMP 启用程序服务配置文件 (AMP Enabler Service Profile)** - 该配置文件用于 AnyConnect AMP 启用程序。当远程访问 VPN 用户连接到 VPN 时，AMP 启动器和此配置文件会从 FDM 管理 设备推送到终端。CDO 支持 XML 和 ASP 文件格式。
- **反馈配置文件 (Feedback Profile)** - 您可以添加客户体验反馈配置文件并选择此类型，以接收有关客户已启用和使用的功能和模块的信息。CDO 支持 FSP 文件格式。
- **ISE 终端安全评估配置文件 (ISE Posture Profile)** - 如果要为 AnyConnect ISE 终端安全评估模块添加配置文件，请选择此选项。CDO 支持 XML 和 ISP 文件格式。
- **网络访问管理器服务配置文件 (Network Access Manager Service Profile)** - 使用网络访问管理器配置文件编辑器配置和添加 NAM 配置文件。CDO 支持 XML 和 NSP 文件格式。
- **网络可视性服务配置文件 (Network Access Manager Service Profile)** - AnyConnect 网络可视性模块的配置文件。您可以使用 NVM 配置文件编辑器创建配置文件。CDO 支持 XML 和 NVMSP 文件格式。
- **Umbrella 漫游安全配置文件 (Umbrella Roaming Security Profile)** - 如果部署 Umbrella 漫游安全模块，则必须选择此文件类型。CDO 支持 XML 和 JSON 文件格式。
- **网络安全服务配置文件 (Web Security Service Profile)** - 在为网络安全模块添加配置文件时选择此文件类型。CDO 支持 XML、WSO 和 WSP 文件格式。

**Before you begin**

使用适当的基于GUI AnyConnect配置文件编辑器创建所需的配置文件。您可以从思科软件下载中心的 AnyConnect 安全移动客户端类别下载配置文件编辑器，并安装 AnyConnect“配置文件编辑器 - Windows/独立安装程序 (MSI)”(Profile Editor - Windows / Standalone installer [MSI])。配置文件编辑器安装程序包含独立版本的配置文件编辑器。此安装文件仅适用于 Windows，文件名为 anyconnect-profileeditor-win-<version>-k9.msi，其中 <version> 指 AnyConnect 版本。例如，anyconnect-profileeditor-win-4.3.04027-k9.msi。您还必须在安装配置文件编辑器之前安装 Java JRE 1.6（或更高版本）。

除 Umbrella 漫游安全配置文件编辑器外，此软件包包含创建模块所需的所有配置文件编辑器。有关详细信息，请参阅相应版本的《思科 AnyConnect 安全移动客户端管理员指南》中的 *AnyConnect* 配置文件编辑器一章。从 Umbrella 控制面板单独下载 Umbrella 漫游安全配置文件。有关详细信息，请参阅《思科 Umbrella 用户指南》中“Umbrella 漫游安全”一章的“从 Umbrella 控制面板下载 AnyConnect 漫游安全配置文件”部分。

**步骤 1** 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

**步骤 2** 点击“加号”  按钮。

**步骤 3** 点击 **RA VPN 对象（ASA 和 FDM）(RA VPN Objects [ASA & FDM]) > AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

**步骤 4** 在**对象名称 (Object Name)** 字段中输入 AnyConnect 客户端配置文件名称。

**步骤 5** 点击**浏览 (Browse)** 并选择使用配置文件编辑器创建的文件。

**步骤 6** 点击**打开**上传配置文件。

**步骤 7** 点击**添加 (Add)** 以添加对象。

**相关信息：**

- 将客户端模块与 RA VPN 组策略窗口中的 AnyConnect VPN 配置文件关联。请参阅创建 ASA 远程访问 VPN 组策略 。

**Note** 所有 ASA 版本和运行软件版本 6.7 或更高版本的 FDM 都支持客户端模块关联。

## 验证 ASA 的远程访问 VPN 配置

在配置远程访问 VPN 并将该配置部署到设备后，请确认是否可以进行远程连接。

**步骤 1** 在外部网络中，使用 AnyConnect 客户端建立 VPN 连接。使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。如有必要，安装客户端软件并完成连接。请参阅用户如何在 ASA 上安装 AnyConnect 客户端软件 。如果配置了组 URL，也可尝试这些 URL。

**步骤 2** 在**清单 (Inventory)** 页面中，选择要验证的设备（FTD 或 ASA），然后点击**设备操作 (Device Actions)** 下的**命令行接口 (Command Line Interface)**。

**步骤 3** 使用 **show vpn-sessiondb** 命令可查看有关当前 VPN 会话的摘要信息。

**步骤 4** 统计信息应显示您的活动 AnyConnect 客户端会话以及有关累积会话、峰值并发会话数量和非活动会话的信息。以下是该命令的输出示例。

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client          :      1 :         49 :           3 :        0
  SSL/TLS/DTLS             :      1 :         49 :           3 :        0
Clientless VPN             :      0 :          1 :           1
  Browser                  :      0 :          1 :           1
--------------------------------------------------------------------------------


  Total Active and Inactive    :      1            Total Cumulative :     50
  Device Total VPN Capacity    :  10000
  Device Load                  :     0%
  --------------------------------------------------------------------------------

  --------------------------------------------------------------------------------
  Tunnels Summary
  --------------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ------------------------------------------------
  Clientless                 :      0 :          1 :               1
  AnyConnect-Parent          :      1 :         49 :               3
  SSL-Tunnel                 :      1 :         46 :               3
  DTLS-Tunnel                :      1 :         46 :               3
  --------------------------------------------------------------------------------
  Totals                     :      3 :        142
  --------------------------------------------------------------------------------

  --------------------------------------------------------------------------------
  IPv6 Usage Summary
  --------------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ------------------------------------------------
  AnyConnect SSL/TLS/DTLS    :        :           :
    Tunneled IPv6            :      1 :         20 :           2
  --------------------------------------------------------------------------------
```

**步骤 5** 使用 **show vpn-sessiondb anyconnect** 命令可查看有关当前 AnyConnect VPN 会话的详细信息。详细信息包括使用的加密方式、传输和接收的字节数及其他统计信息。如果使用 VPN 连接，随着您重新发出命令，您应可看到传输/接收的字节数会变化。

**步骤 6** 使用 **show vpn-sessiondb anyconnect** 命令可查看有关当前 AnyConnect VPN 会话的详细信息。详细信息包括使用的加密方式、传输和接收的字节数及其他统计信息。如果使用VPN连接，随着您重新发出命令，您应可看到传输/接收的字节数会变化。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

### 查看 ASA 的远程访问 VPN 配置详细信息

**步骤 1** 在左侧的 CDO 导航栏中，点击 **VPN** > **ASA/FDM 远程访问 VPN 配置**。

**步骤 2** 点击现有的 VPN 配置对象。该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

- 展开 RA VPN 配置以查看与其关联的所有连接配置文件。
  - 点击添加 + 按钮可添加新的连接配置文件。
  - 点击查看按钮 ( )，打开连接配置文件和连接说明的摘要。在操作下，您可以点击编辑以修改更改。
- 您可以点击“操作”下的以下选项之一来执行其他任务：
  - 点击组策略以分配/添加组策略。
  - 点击不再需要的配置对象或连接配置文件，然后点击删除进行删除。

## 监控远程访问虚拟专用网络会话

远程访问虚拟专用网络 (RA VPN) 为远程用户（如移动用户或远程工作者）提供安全连接。监控这些连接可以让连接和用户会话性能的重要指标变得一目了然。Cisco Defense Orchestrator (CDO) RA VPN 监控功能使您能够快速确定远程访问 VPN 问题是否存在及其存在的位置。然后，您可以应用这些知识并使用网络管理工具来减少或消除网络和用户问题。您还可以根据需要断开远程访问 VPN 会话。

“远程访问虚拟专用监控”(Remote Access Virtual Private Monitoring) 页面提供以下信息：

- 长达一年的活动会话和历史会话列表。
- 显示直观的图形视觉效果，让 CDO 管理的所有活动 VPN 前端变得一目了然。

- 实时会话屏幕会显示 CDO 租户中最常用的操作系统和 VPN 连接配置文件。它还会显示平均会话持续时间以及上传和下载的数据。
- 过滤功能可根据设备类型、设备名称、会话长度以及传输和接收的数据量等条件来缩小搜索范围。

相关信息：

- 监控实时 AnyConnect RA VPN 会话, on page 271
- 监控历史 AnyConnect RA VPN 会话, on page 272
- 搜索和过滤 RA VPN 会话
- 自定义 RA VPN 监控视图
- 将 RA VPN 会话导出至 CSV 文件
- 断开用户的所有活动 RA VPN 会话

## 监控实时 AnyConnect RA VPN 会话

您可以监控设备上活动 AnyConnect RA VPN 会话的实时数据。这些数据每 10 分钟会自动刷新一次。如果要随时检索最新的会话列表，请点击屏幕右上角显示的重新加载图标 。

### 开始之前

- 将 RA VPN 前端载入 CDO。
- 确保要监控实时数据的设备的连接状态在**清单 (Inventory)** 页面上为“在线”(Online)。

**步骤 1** 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

或者，您可以点击 CDO 主页上的**查看活动远程访问 VPN 会话 (View Active Remote Access VPN Sessions)**，或导航至 **VPN** > **远程访问 VPN (Remote Access VPN)**并点击屏幕右上角的 图标。

**步骤 2** 点击 **RA VPN**。

**步骤 3** 点击**实时 (Live)**。

您可以搜索和过滤 RA VPN 会话以根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。

注释 **数据 TX** 和**数据 RX** 信息不适用于 FTD。

### 查看实时数据

实时数据以控制面板和表格形式显示。

### 面板视图

您必须点击屏幕右上角的**显示图表视图**图标才能查看控制面板。

控制面板提供 CDO 管理的所有活动 VPN 头端的概览视图。

- **明细（所有设备）**：显示实时会话总数。它还显示了一个分为四个弧长的饼形图。它说明会话数最多的前三台设备的 VPN 会话百分比。剩余的弧长表示其他设备的总和。
- 显示 CDO 租户中最常用的操作系统和 VPN 连接配置文件。
- 显示平均会话持续时间以及上传和下载的数据。
- **按国家/地区排列的活动会话 (Active Sessions by Country)**：显示连接到 RA VPN 前端的用户的位置的交互式热度地图。
  - 用户已连接的国家/地区以逐渐变深的蓝色显示，具体取决于从该国家/地区建立的会话的相对比例 - 蓝色越深表示从该国家/地区建立的会话越多。
  - 地图底部的图例提供了一个比例，表示某个国家/地区的会话数与其所用蓝色阴影之间的相关性。
  - 将鼠标指针悬停在地图上，可查看国家/地区名称以及从该国家/地区建立的活动用户会话总数。
  - 将鼠标指针悬停在表格上，可在地图上看到国家/地区的位置和活动用户会话总数。

### 表格视图

点击屏幕右上角的**显示表格视图**图标，以表格格式查看数据。

表格形式提供当前连接的 VPN 用户的完整列表。

- “位置”列通过对公共 IP 地址进行地理定位来显示连接到 VPN 头端的所有用户的位置。点击一行可查看用户详细信息。点击左侧窗格中的位置链接时，用户的位置会显示在 Google 地图上。

**重要事项** CDO 对实时数据应用标准过滤器，并在控制面板上显示这些数据。仅当显示表格数据时，才能应用新过滤器，因为可视化控制面板视图中不支持自定义过滤器。点击**清除**以删除已应用的所有过滤器。您无法删除标准过滤器。

您可以使用搜索和过滤 RA VPN 会话功能根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。请注意，一次最多可以显示 10,000 个结果。

状态列中带有活动标签的绿点表示活动 VPN 用户的会话。

## 监控历史 AnyConnect RA VPN 会话

您可以监控过去三个月内记录的 AnyConnect RA VPN 会话的历史数据。

开始之前

- 将 RA VPN 前端载入 CDO。

步骤 1 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

或者，您可以点击 CDO 主页上的**查看活动远程访问 VPN 会话 (View Active Remote Access VPN Sessions)**，或导航至 **VPN** > **远程访问 VPN (Remote Access VPN)** 并点击右上角的 图标。

步骤 2 点击 **RA VPN**。

步骤 3 点击**历史 (Historical)**。

CDO 会显示过去三个月内记录的 RA VPN 会话的历史数据。

您可以使用搜索和过滤 RA VPN 会话功能根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。

**数据 TX** 和**数据 RX** 信息不适用于 FTD。

查看历史数据

历史数据以控制面板和表格形式显示。

### 面板视图

您必须点击屏幕右上角的“显示图表视图”图标才能查看控制面板。您将看到控制面板视图和表格视图。

控制面板提供 CDO 管理的所有活动 VPN 头端的概览视图。它会提供一个条形图，以便显示过去 24 小时、7 天和 30 天内为所有设备记录的 VPN 会话。您可以从下拉列表中选择持续时间。您可以将鼠标悬停在各个条形上，以查看当天的日期和会话总数。

### 表格视图

您必须点击屏幕右上角显示的“显示表格视图”图标，才能仅查看表格视图。此表格提供了过去三个月内连接的 VPN 用户的完整列表。

“位置”列通过对公共 IP 地址进行地理定位来显示连接到 VPN 头端的所有用户的位置。点击一行可查看用户详细信息。点击左侧窗格中的位置链接时，用户的位置会显示在 Google 地图上。

**重要事项** CDO 对历史数据应用标准过滤器，并将其显示在控制面板上。您只能在显示表格数据时应用新过滤器，因为自定义过滤器不支持控制面板。清除新应用的过滤器会重新启动控制面板（在屏幕上，点击清除可删除手动应用的过滤器）。您无法删除标准过滤器。

您可以使用搜索和过滤 RA VPN 会话功能根据会话日期和时间范围、会话长度以及上传和下载数据范围等条件来缩小搜索范围。请注意，一次最多可以显示 10,000 个结果。

状态列中带有活动标签的绿点表示活动 VPN 用户的会话。

## 搜索和过滤 RA VPN 会话

### 搜索

使用搜索栏功能查找 RA VPN 会话。开始在搜索栏中键入设备名称、IP 地址或序列号，系统将显示符合搜索条件的 RA VPN 会话。搜索不区分大小写。

### 过滤

使用过滤器边栏可根据会话时间范围、会话长度以及上传和下载数据范围等条件查找RA VPN会话。过滤功能可用于实时视图和历史视图。

- **按设备过滤 (Filter by Devices)**：从**所有类型 (All Types)** 选项卡中选择一个或所有设备以查看所选设备的会话。该窗口还会根据设备的类型来对它们进行分类，并在相应的选项卡下显示它们。
- **会话时间范围 (Sessions Time Range)**（仅适用于历史数据）：查看指定日期和时间范围内的历史会话。请注意，您可以查看过去三个月内记录的数据。
- **会话长度 (Sessions Length)**：根据指定会话的持续时间长度查看会话。设置时间单位（小时、分钟或秒），并通过移动滑块指定最小和最大持续时间。您还可以在提供的字段中指定长度。
- **上传 (TX) (Upload [TX])**：根据上传或传输到安全网络的指定数据量查看会话。设置单位（GB、MB 或 KB），并通过相应地移动滑块来选择范围。您还可以在可用字段中指定值。
- **下载 (RX) (Download [RX])**：根据从安全网络下载或接收的指定数据量查看会话。设置单位（GB、MB 或 KB），并通过相应地移动滑块来选择范围。您还可以在可用字段中指定值。

## 自定义 RA VPN 监控视图

您可以在实时和历史模式下修改 RA VPN 监控视图，以仅包含适用于所需视图的列标题。点击列右侧的列过滤器图标  ，然后选择或取消选择所需的列。

CDO 会在您下次登录 CDO 时记住您的选择。

## 将 RA VPN 会话导出至 CSV 文件

您可以将一个或多个设备的 RA VPN 会话导出至以逗号来分隔值的 (.csv) 文件。您可以在电子表格应用（例如 Microsoft Excel）中打开 .csv 文件，对列表中的项目进行排序和过滤。这些信息可帮助您分析 RA VPN 会话。每次导出会话时，CDO 都会创建一个新的 .csv 文件，其中创建的文件会在名称中包含日期和时间。

CDO 最多可以将 100,000 个活动会话导出至 CSV 文件。如果来自所有设备的会话总数超过最大限制，则可以使用**按设备查看 (View By Device)** 过滤器并为各个设备生成报告。

---

**步骤 1** 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控 (Remote Access VPN Monitoring)**。

**步骤 2** 在**按设备查看 (View By Devices)** 区域中，选择以下选项之一：

- **所有设备 (All Devices)**，可从其下面列出的所有设备导出活动会话。
- 点击要导出其会话的设备。

**步骤 3** 点击右上角的 图标。CDO 会将您在屏幕上看到的规则导出至 .csv 文件。

**步骤 4** 在电子表格应用中打开 .csv 文件，对结果进行排序和过滤。

### 断开 ASA 用户的活动 RA VPN 会话

您可以在 ASA 设备上终止所有用户的所有活动 RA VPN 会话。您可以在实时和历史模式下执行此任务。

CDO 会提供“VPN 会话管理器”用户角色，以允许用户查看和终止 VPN 会话。有关详细信息，请参阅CDO中的用户角色。

**步骤 1** 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

**步骤 2** 在**按设备查看 (View By Devices)** 区域中，点击要结束该设备上所有活动会话的 ASA 设备。

**步骤 3** 点击右上角显示的 Terminate All Sessions。

**步骤 4** 点击 Yes, Terminate All Sessions（是，终止所有会话）以确认您的选择。

### 断开用户的所有活动 *RA VPN* 会话

当您断开用户连接时，CDO 将终止该 ASA 设备上的所有活动 RA VPN 会话。您可以在实时和历史模式下执行此任务。

**步骤 1** 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

**步骤 2** 搜索要断开其会话的用户。您可以在**搜索 (Search)** 栏中键入搜索条件。

**步骤 3** 点击活动会话，然后在右侧的**操作 (Actions)** 窗格中，点击**终止此用户的所有 RA VPN 会话 (Terminate all RA VPN sessions for this user )** 链接。

# ASA 模板

模板使用户能够构建设备/服务配置，以便他们可以将该配置应用于已组合在一起的其他配置。这些模板提供了一个进行更改的位置，以便影响组合在一起的许多实施者。

# ASA 模板参数

创建新模板时，您可能希望根据特定设备对其进行建模。CDO 提供根据模板建模所依据的设备配置中的选定文本字段设置模板参数的功能。可以从现有参数创建、设置参数，并在模板参数视图中搜索参数。

**Note** 如果您选择导入 ASA 模板的配置，则该配置必须采用 JSON 格式。

## 创建新参数

**步骤 1** 载入现有设备后，导航至 CDO 顶部的“模板”选项卡。
**步骤 2** 选择新建模板或管理模板。
**步骤 3** 选择所需的配置以创建参数。
**步骤 4** 通过在屏幕顶部的名称字段中键入来命名模板。
**步骤 5** 选择要向其添加参数的所需文本字段。
**步骤 6** 为参数提供说明、添加值和任何必要的注释。
**步骤 7** 点击名称 (Name) 字段旁边的保存 (Save) 以保存参数。
**步骤 8** 然后，您可以通过点击查看模板来查看模板。

您现在有一个已保存的参数，该参数将应用于未来使用此模板载入的所有设备。

# 创建新的 ASA、ISR 或 ASR 模板

### 基本配置

从已知的 ASA、ISR 或 ASR 基本配置开始。选择所需的配置以开始模板的参数化。参数化涉及选择配置文件中的字段或属性，并标识将在配置文件实例化时选择的值列表。

**Note** 如果您选择导入 ASA 模板的配置，则该配置必须采用 JSON 格式。

### 添加参数

选择基本配置后，即可开始参数化过程。从配置编辑器中，选择所需的参数化字段。请注意，所选字符串括在双括号中。在左侧窗格中，可以重命名参数、添加说明以及添加多个值。选择“允许自定义值”(Allow Custom Value) 可在实例化时设置自定义值。否则，只能选择已识别的值。

参数化完成后，确定模板的名称，然后点击保存。

在此处了解有关参数化的更多信息。 ASA 模板参数, on page 276

### 审核

保存模板后，点击审核以进入审核流程。在查看时，可以按原样导出模板，包括参数化值。请注意，这不一定是有效的配置，但提供了一种方法来查看存储在CDO中的模板。如果需要，也可以通过点击编辑来编辑模板。Diff 按钮可以演示保存的模板和最新编辑之间的差异。

# 从模板生成 ASA 配置

### 从模板创建配置

选择从模板配置按钮，开始从模板生成自定义配置的过程。列出可用模板，选择所选模板，然后点击选择模板。

在大多数情况下，模板将包含必须在导出时设置的参数化值，以提供自定义配置。在左侧窗格中，根据需要选择此配置的每个参数和值。请注意，这些值在编辑器中进行了演示。这些是将在导出时替换参数的值。设置所有参数值后，点击导出按钮以导出配置并下载。如果模板不包含参数化值，请点击导出按钮按原样导出配置。

# 管理 ASA 模板

通过管理模板视图，您可以查看所有现有模板以及对其进行编辑和删除。可以在编辑模板时修改参数化和值配置。只需将鼠标悬停在现有模板上，然后选择编辑即可进行更改。

### 编辑模板

进入编辑视图后：

- 通过双击或突出显示编辑器中的文本来添加参数。
- 通过在说明文本框中键入来说明参数。然后点击**添加值 (Add Value)**。
- 提供值并添加注释。点击**添加 (Add)**。
- 完成后，点击**保存**。
- 现在，您可以通过点击**查看模板 (Review Template)** 来查看模板。
  - 您可以通过点击**差异 (Diff)** 来比较文件。
  - 要导出模板，请点击**导出 (Export)**。

# API 令牌

开发人员在进行 CDO REST API 调用时使用 CDO API 令牌。必须在 REST API 授权报头中插入 API 令牌，调用才能成功。API 令牌是“长期”访问令牌，不会过期；但是，您可以续订和撤销它们。

您可以从 CDO 中生成 API 令牌。这些令牌仅在生成后立即可见，并且只要“常规设置”页面处于打开状态。如果您在CDO中打开另一个页面并返回到“常规设置”页面，则该令牌不再可见，但很明显已发出令牌。

个人用户可以为特定租户创建自己的令牌。一个用户不能代表另一个用户生成令牌。令牌特定于账户-租户对，不能用于其他用户-租户组合。

### API 令牌格式和声明

API 令牌是 JSON Web 令牌 (JWT)。要了解有关 JWT 令牌格式的更多信息，请阅读 JSON Web 令牌简介。https://jwt.io/introduction/

CDO API 令牌提供以下一组声明：

- id - 用户/设备 uid
- parentId - 租户 uid
- ver - 公钥的版本（初始版本为 0，例如 cdo_jwt_sig_pub_key.0）
- 订用 - 订用（可选）安全服务交换
- client_id - " api-client "
- jti - 令牌 ID

# 将 ASA 配置迁移到 FDM 管理 设备模板

**Attention** Firepower 设备管理器 (FDM) 支持和功能仅应要求提供。如果您的租户上尚未启用 防火墙设备管理器 支持，则无法管理或部署到 FDM 管理 设备。向支持团队发送请求以启用此平台。通过 TAC 打开提交支持请求, on page 535

思科防御协调器 可帮助您将 ASA 迁移到 FDM 管理 设备。CDO 提供了一个向导来帮助您将 ASA 的运行配置的这些元素迁移到 FDM 管理 模板：

- 访问控制规则 (ACL)
- 接口
- 网络地址转换 (NAT) 规则
- 网络对象和网络组对象
- 路由
- 服务对象和服务组对象
- 站点间 VPN

将 ASA 运行配置的这些元素迁移到 FDM 管理 模板后，即可将 FDM 模板应用于由 CDO 管理的新 FDM 管理 设备。FDM 管理 设备采用模板中定义的配置，因此，FDM 管理 设备现在配置了 ASA 运行配置的某些方面。

使用此过程不会迁移 ASA 运行配置的其他元素。这些其他元素在 FDM 管理 设备模板中由空值表示。将模板应用于 FDM 管理 设备时，我们会应用迁移到新 FDM 管理 设备的值并忽略空值。无论新 FDM 管理 设备具有哪些其他默认值，它都会保留。我们未迁移的 ASA 运行配置的其他元素将需要在迁移过程之外在 FDM 管理 设备上重新创建。

有关使用 CDO 将 ASA 迁移到 FDM 管理 设备的过程的完整说明，请参阅使用思科防御协调器将 ASA 迁移到 FDM 托管设备。

# 管理 ASA 证书

数字证书为设备和个人用户的身份验证提供数字标识。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或IP地址。数字证书还包括用户或设备的公钥副本。有关数字证书的详细信息，请参阅思科 ASA 系列常规操作 ASDM 配置的“基本设置”一书 X.Y 文档中的“数字证书”一章。

证书颁发机构 (CA) 是指“签署”证书以确认其真实性，从而确保设备或用户的身份的可信颁发机构。CA 还颁发身份证书。

- **身份证书 (Identity Certificate)** - 内部身份证书是用于特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。CA 会颁发身份证书，这是特定系统或主机的证书。
- **受信任 CA 证书 (Trusted CA Certificate)** - 受信任 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。受信任 CA 证书是自签名证书，也称为根证书。

远程访问 VPN 使用数字证书对安全网关和 AnyConnect 客户端（终端）进行身份验证，以建立安全的 VPN 连接。有关详细信息，请参阅远程访问 VPN 基于证书的身份验证。

### 证书安装指南

请阅读以下有关在 ASA 上安装证书的准则：

- 证书可以同时安装在单个或多个 ASA 设备上。
- 一次只能安装一个证书。
- 证书只能安装在实时 ASA 设备上，而不能安装在模态设备上。

# ASA 证书安装

您必须将数字证书作为信任点对象上传，并将其安装在 CDO 管理的 ASA 设备上。信任点对象，第 119 页

注释 确保 ASA 设备没有带外更改，并且已部署所有暂存更改。

下面列出了 CDO 支持的数字证书和格式：

- 可以使用以下方法安装身份证书：
  - PKCS12 文件导入。
  - 自签名证书
  - 证书签名请求 (CSR) 导入。
- 可以使用 PEM 或 DER 格式安装受信任 CA 证书。

观看演示如何使用 CDO 在 ASA 上安装证书的截屏视频。https://www.youtube.com/watch?v=9ihOs_AmQ8s它还显示修改、导出和删除已安装证书的步骤。

### 支持的证书格式

- PKCS12：PKCS#12、P12 或 PFX 格式是一种二进制格式，用于在一个可加密文件中存储服务器证书、任何中间证书和私钥。PFX 文件通常具有 .pfx 和 .p12 等扩展名。
- PEM：PEM（原为“隐私增强邮件”）文件包含 ASCII（或 Base64）编码数据，证书文件可以是 .pem、.crt、.cer 或 .key 格式。它们是 Base64 编码的 ASCII 文件，包含“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”语句。
- DER：DER（可分辨编码规则）格式只是证书的二进制形式，而不是 ASCII PEM 格式。它的文件扩展名有时为 .der，但文件扩展名通常为 .cer，因此区分 DER.cer 文件和 PEM.cer 文件的唯一方法是在文本编辑器中打开该文件，然后查找 BEGIN/END 语句。与 PEM 不同，DER 编码文件不包含纯文本语句，例如 -----BEGIN CERTIFICATE-----。

### 信任点屏幕

将 ASA 设备载入 CDO 后，在设备和服务选项卡上，选择 ASA 设备，然后在左侧的管理窗格中点击信任点。

在“信任点”选项卡中，您将看到设备上已安装的证书。

- “已安装”状态表示已在设备上成功安装相应的证书。
- “未知”状态表示相应的证书不包含任何信息。您需要将其删除并使用正确的详细信息重新上传。CDO 发现所有未知证书都是受信任的 CA 证书。
- 点击显示“已安装”的行，在右侧窗格中查看证书详细信息。点击“更多”可查看所选证书的其他详细信息。
- 已安装的身份证书可以 PKCS12 或 PEM 格式导出，并导入到其他 ASA 设备中。请参阅“导出身份证书”。
- 只能修改已安装证书的高级设置。

- 点击编辑以修改高级设置。
- 进行更改后，点击发送以安装更新的证书。

# 使用 PKCS12 安装身份证书

您可以选择为 PKCS12 格式创建的现有信任点对象，并将其安装在 ASA 设备上。您还可以从安装向导创建新的信任点对象，并在 ASA 设备上安装证书。

### 开始之前

- 阅读证书安装指南。证书安装指南，第 279 页
- ASA 必须处于“已同步”状态和“在线”状态。

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 要在单个 ASA 设备上安装身份证书，请执行以下操作：

a) 点击**设备**选项卡。
b) 点击 ASA 选项卡并选择 ASA 设备。
c) 在左侧的**管理 (Management)** 窗格中，点击**信任点 (Trustpoints)**。
d) 点击 **Install**。

**注释** 您还可以在多个 ASA 设备上安装证书。选择多个 ASA 设备，然后在右侧的设备操作中，点击安装证书。

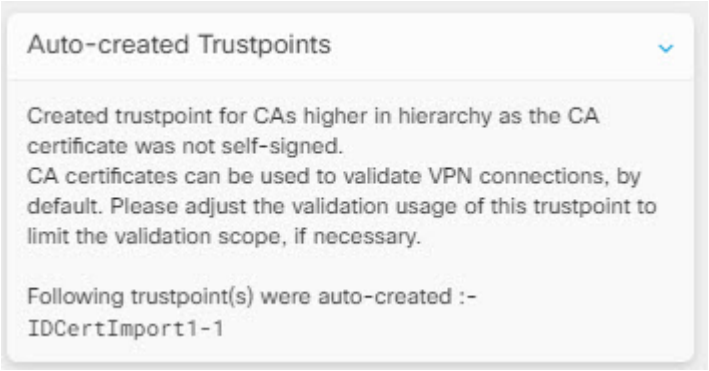
**步骤 3** 从选择要安装的信任点证书中，点击以下选项之一：

- 创建以添加新的信任点对象。有关更多信息，请参阅使用 PKCS12 添加身份证书对象。
- **选择**以选择 PKCS 类型的认证登记对象。

**步骤 4** 点击**发送 (Send)**。

这将在 ASA 设备上安装证书

注释　如果要导入已安装中间 CA 的 PKCS12 证书，ASA 会自动在设备上为尚未安装的每个中间 CA 证书创建并安装信任点对象。当您点击身份证书时，您会在右侧窗格中看到一条消息，如以下示例所示。




# 使用自签注册安装证书

您可以选择为自签名证书创建的现有信任点对象，并将其安装在ASA设备上。您还可以从安装向导创建新的信任点对象，并在 ASA 设备上安装证书。

### 开始之前

- 阅读证书安装指南。证书安装指南，第 279 页
- ASA 必须处于“已同步”状态和“在线”状态。

**步骤 1**　在导航栏中，点击 **设备和服务**。

**步骤 2**　要在单个 ASA 设备上安装身份证书，请执行以下操作：

a) 点击**设备**选项卡。
b) 点击 ASA 选项卡并选择 ASA 设备。
c) 在左侧的**管理 (Management)** 窗格中，点击**信任点 (Trustpoints)**。
d) 点击 **Install**。

注释　您还可以在多个 ASA 设备上安装签名证书。选择多个 ASA 设备，然后在右侧的设备操作中，点击安装证书。

**步骤 3**　从选择要安装的信任点证书中，点击以下选项之一：

- 创建以添加新的信任点对象。有关更多信息，请参阅使用 PKCS12 添加身份证书对象。
- **选择**选择自签名类型的认证登记对象。

**步骤 4**　点击**发送 (Send)**。

对于自签名注册类型的信任点，颁发者常用名状态将始终显示 ASA 设备，因为受管设备会充当自己的 CA，而不需要 CA 证书来生成自己的身份证书。

# 管理证书签名请求 (CSR)

您必须首先生成 CSR 请求，然后由受信任的证书颁发机构 (CA) 签署此请求。然后，您可以在 ASA 设备上安装由 CA 颁发的签名身份证书。

- 阅读证书安装指南。证书安装指南，第 279 页
- ASA 必须处于“已同步”状态和“在线”状态。

下图描述了在 ASA 中生成 CSR 和安装已认证的证书的工作流程：

# 生成 CSR 请求

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击 ASA 选项卡并选择 ASA 设备。

**步骤 4** 要在单个 ASA 设备上安装身份证书，请执行以下操作：

**步骤 5** 点击 **Install**。

**步骤 6** 从选择要安装的信任点证书中，点击以下选项之一：

- 创建以添加新的信任点 CSR 对象。有关详细信息，请参阅为证书签名请求 (CSR) 添加身份证书对象，第 123 页。
- 选择以选择已创建的 CSR 请求信任点。

**步骤 7** 点击**发送 (Send)**。

这会生成未签名的证书签名请求 (CSR)。

**步骤 8** 点击复制图标 copy_icon.png 以复制 CSR 详细信息。您还可以下载“.csr”文件格式的 CSR 请求。

**步骤 9** 点击**确定 (OK)**。

**步骤 10** 提交证书签名请求 (CSR) 到证书颁发机构，以便签署证书。

# 安装证书颁发机构颁发的签名身份证书

CA 颁发签名证书后，将其安装在 ASA 设备上

**步骤 1** 在“信任点”屏幕中，点击状态为“等待签名证书安装”的 CSR 请求，然后在右侧的“操作”窗格中，点击安装认证 ID 证书。

**步骤 2** 上传从 CA 收到的签名证书。您可以拖放文件或将其内容粘贴到提供的字段中。根据您选择的信任点生成信任点命令。

**步骤 3** 点击**发送 (Send)**。

这会将签名的身份证书安装到 ASA 设备。安装证书会立即将更改部署到设备。

**注释** 您还可以在多个 ASA 设备上安装证书。选择多个 ASA 设备，然后在右侧的设备操作中，点击安装证书。

# 在 ASA 中安装受信任 CA 证书

开始之前

- 阅读证书安装指南。证书安装指南，第 279 页
- ASA 必须处于“已同步”状态和“在线”状态。

**步骤 1** 在导航菜单中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击 ASA 选项卡并选择 ASA 设备。

**步骤 4** 要在单个 ASA 设备上安装身份证书，请执行以下操作：

a) 选择 ASA 设备，然后在右侧的**管理 (Managemento** 窗格中，点击**信任点 (Trustpoints)**。

b) 点击 **Install**。

注释 您还可以在多个 ASA 设备上安装证书。选择多个 ASA 设备，然后在右侧的设备操作中，点击安装证书。

**步骤 5** 从选择要安装的信任点证书中，点击以下选项之一：

- 创建以添加新的信任点对象。有关详细信息，请参阅添加受信任 CA 证书对象，第 126 页。
- **选择**选择一个受信任证书颁发机构对象。

**步骤 6** 点击**发送 (Send)**。

这会在 ASA 设备上安装受信任的 CA 文件。

# 导出身份证书

您可以 PKCS12 或 PEM 格式导出和导入密钥对，以及与某个信任点关联的已颁发证书。此格式对于在其他 ASA 上手动复制信任点配置来说非常有用。

**SUMMARY STEPS**

1. 在导航菜单中，点击**设备和服务 (Devices & Services)**。
2. 点击**设备**选项卡。
3. 点击 **ASA**。
4. 选择 ASA 设备，然后在右侧的 **Management** 中点击 **Trustpoints**。
5. 点击身份证书以导出证书配置。或者，您可以通过在搜索字段中输入证书名称来搜索证书。
6. 在右侧的**操作**窗格中，点击**导出证书**。
7. 通过点击 **PKCS12 格式 (PKCS12 Format)** 或 **PEM 格式 (PEM Format)** 来选择证书格式。
8. 输入用于加密要导出的 PKCS12 文件的加密密码。

9. 确认加密密码。
10. 点击**导出 (Export)** 以导出证书配置。

**DETAILED STEPS**

| | 命令或操作 | 目的 |
|---|---|---|
| **步骤 1** | 在导航菜单中，点击**设备和服务 (Devices & Services)**。 | |
| **步骤 2** | 点击**设备**选项卡。 | |
| **步骤 3** | 点击 **ASA**。 | |
| **步骤 4** | 选择 ASA 设备，然后在右侧的 **Management** 中点击 **Trustpoints**。 | |
| **步骤 5** | 点击身份证书以导出证书配置。或者，您可以通过在搜索字段中输入证书名称来搜索证书。 | |
| **步骤 6** | 在右侧的**操作**窗格中，点击**导出证书**。 | |
| **步骤 7** | 通过点击 **PKCS12 格式 (PKCS12 Format)** 或 **PEM 格式 (PEM Format)** 来选择证书格式。 | |
| **步骤 8** | 输入用于加密要导出的 PKCS12 文件的加密密码。 | |
| **步骤 9** | 确认加密密码。 | |
| **步骤 10** | 点击**导出 (Export)** 以导出证书配置。 | 系统将显示一个信息对话框，通知您证书配置文件已成功导出到指定的位置。 |

# 编辑已安装的证书

您只能修改已安装证书的高级选项。

**步骤 1** 在导航菜单中，点击**设备和服务 (Devices & Services)**。
**步骤 2** 点击**设备**选项卡。
**步骤 3** 点击 **ASA** 选项卡。
**步骤 4** 选择 ASA 设备，然后在右侧的 **Management** 中点击 **Trustpoints**。
**步骤 5** 点击要修改的证书，然后在右侧的**操作**窗格中，点击**编辑**。
**步骤 6** 修改所需的参数并点击**保存**。

# 从 ASA 删除现有证书

您可以逐个删除证书。在删除证书后，无法将其恢复。

**步骤 1** 在导航菜单中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 选择 ASA 设备，然后在右侧的“管理”中，点击“信任点”。

**步骤 3** 点击要删除的证书，然后在右侧的操作窗格中，点击删除。

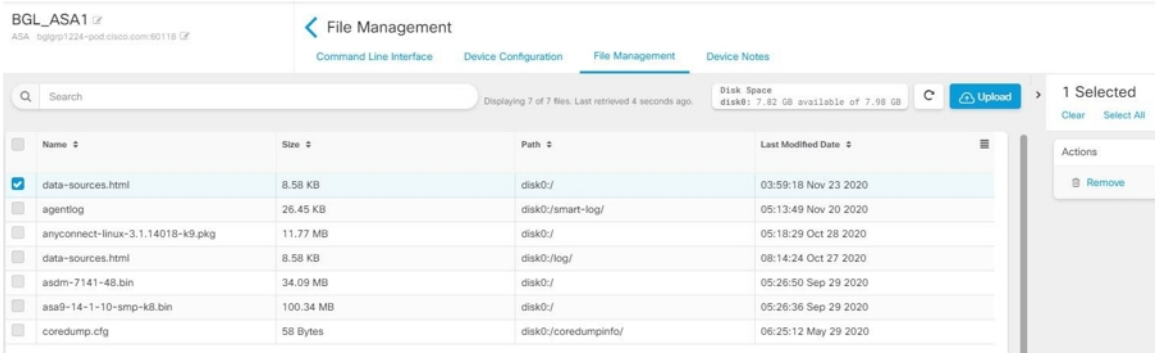
**步骤 4** 点击确定以删除所选证书。

# ASA 文件管理

CDO 提供文件管理工具来帮助您执行基本的文件管理任务，例如查看、上传或删除 ASA 设备的闪存 (disk0) 空间中的文件。

**Note** 您无法管理 disk1 上的文件。

File Management 屏幕列出了设备闪存（disk0）上的所有文件。成功上传文件后，您可以点击刷新图标查看文件。默认情况下，此屏幕每 10 分钟自动刷新一次。磁盘空间字段显示 disk0 目录上的磁盘空间量。




您可以将 AnyConnect 映像上传到单个或多个 ASA 设备。成功上传后，AnyConnect 映像将与所选 ASA 设备上的 RA VPN 配置相关联。这有助于您将新发布的 AnyConnect 软件包同时上传到多个 ASA 设备。

### 将文件上传到闪存系统

CDO 仅支持从远程服务器上传基于 URL 的文件。支持的文件上传协议包括 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP。您可以将任何文件（例如 AnyConnect 软件映像、DAP.xml、data.xml）和主机扫描映像文件上传到单个或多个 ASA 设备。

**Note** 如果远程服务器的 URL 路径无效或可能出现任何问题，CDO 不会将文件上传到选定的 ASA 设备。您可以导航至设备工作流程以了解更多详细信息。

假设设备配置为高可用性，CDO 首先将文件上传到备用设备，并且只有在成功上传后，才会将文件上传到主用设备。在文件删除过程中应用相同的行为。

用于上传文件的受支持协议的语法：

| 协议 | 语法 | 示例 |
|---|---|---|
| HTTP | http://[[path/]filename] | http://www.geonames.org/data-sources.html |
| HTTPS | https://[[path/]filename] | https://docs.aws.amazon.com/amazov/tagging.html |
| TFTP | tftp://[[path/]filename] | tftp://10.10.16.6/ftd/components.html |
| FTP | ftp://[[user[:password]@]server[:port]/[path/]filename] | [illegible] |
| 中小企业 | smb://[[path/]filename] | smb://10.10.32.145//sambashare/hello.txt |
| SCP | scp://[[user[:password]@]server[/path]/filename] | scp://rootcisco123@10.10.166//root/events_send.py |

### 准备工作

- 确保可从 ASA 设备访问远程服务器。
- 确保文件已上传到远程服务器。
- 确保存在从 ASA 设备到该服务器的网络路由。
- 如果在 URL 中使用 FQDN，请确保已配置 DNS。
- 远程服务器的 URL 必须是不提示进行身份验证的直接链接。
- 如果远程服务器 IP 地址经过 NAT，则必须提供远程服务器位置的 NAT 公共 IP 地址。

**Note** 如果将文件上传到在故障切换中配置为对等体的 ASA，则 CDO 不会为故障切换对中的另一个对等体确认新文件，并且设备状态更改为“未同步”。您必须手动将更改部署到两台设备，以便 CDO 识别两台设备中的文件。

# 将文件上传到单个 ASA 设备

使用此程序将文件上传到单个 ASA 设备。

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击 ASA 选项卡并选择 ASA 设备。

**步骤 4** 在右侧的**管理 (Management)** 窗格中点击**文件管理 (File Management)**。您可以查看 ASA 设备上的可用磁盘空间和文件。

**步骤 5** 点击右边的**上传 (Upload )** 按钮。

**步骤 6** 在 **URL 链接**中，指定预上传文件的服务器路径。**Destination Path** 字段显示正在上传到 **disk0** 目录的文件的名称。如果要将文件上传到 disk0 中的特定目录，请在此字段中指定其名称。例如，如果要将 dap.xml 文件上传到“DAPFiles”目录，请在字段中指定“**disk0:**/DAPFiles/dap.xml”。

**Note** 您可以通过在 CDO ASA CLI 接口中执行 **dir** 命令来查看 disk0 文件夹中的目录。

**步骤 7** 如果指定的服务器路径指向 AnyConnect 文件，则**将文件与 RA VPN 配置关联**复选框处于启用状态。 注意：仅对遵循正确命名约定的 AnyConnect 文件名（即“anyconnect-win-xxx.pkg”、“anyconnect-linux-xxx.pkg”或“anyconnect-mac-xxx”）启用此复选框。 pkg' 格式。选中此复选框后，CDO 会在成功上传后将 AnyConnect 文件关联到所选 ASA 设备上的 RA VPN 配置。

**步骤 8** 点击**上传**。CDO 将文件上传到设备。

**步骤 9** 如果您已在步骤 5 中选择将 AnyConnect 软件包与 RA VPN 配置相关联，请将配置更改从 CDO 部署到 ASA。

### What to do next

您不必在设备上部署配置更改。

# 将文件上传到多个 ASA 设备

使用此程序将文件同时上传到多个 ASA 设备。

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击 **ASA** 选项卡并选择多个 ASA 设备以执行批量上传。

**步骤 4** 在右侧的**设备操作 (Device Actions)** 窗格中，点击**上传文件 (Upload File)**。注意：如果 ASA 设备在线，系统将显示**上传文件**链接。

**步骤 5** 在 **URL 链接**中，指定预上传文件的服务器路径。**Destination Path** 字段显示正在上传到 **disk0** 目录的文件的名称。如果要将文件上传到 disk0 中的特定目录，请在此字段中指定其名称。例如，如果要将 dap.xml 文件上传到“DAPFiles”目录，请在字段中指定“**disk0:**/DAPFiles/dap.xml”。

**Note** 您可以通过在 CDO ASA CLI 接口中执行 **dir** 命令来查看 disk0 文件夹中的目录。

**步骤 6** 如果指定的服务器路径指向 AnyConnect 文件，则**将文件与 RA VPN 配置关联**复选框处于启用状态。

**Note** 仅对遵循正确命名约定的 AnyConnect 文件名（即“anyconnect-win-xxx.pkg”、“anyconnect-linux-xxx.pkg”或“anyconnect-mac-xxx.pkg”）启用此复选框。格式。选中此复选框后，CDO 会在成功上传后将 AnyConnect 文件关联到所选 ASA 设备上的 RA VPN 配置。

**步骤 7** 点击**上传**。

**步骤 8** 如果您已在步骤 4 中选择将 AnyConnect 软件包与 RA VPN 配置关联，请将配置更改从 CDO 部署到 ASA。

### What to do next

您可以查看在各个设备上上传文件的进度。选择 ASA 设备，然后在右侧的**管理 (Management)** 窗格中点击**文件管理 (File Management)**。如果文件上传正在进行，请等待操作完成。

您不必在设备上部署配置更改。

# 从 ASA 中删除文件

不允许删除与 RA VPN 配置关联的 AnyConnect 文件。您必须取消 AnyConnect 文件与相应的 RA VPN 配置的关联，然后从文件管理工具中删除该文件。

**Note** 如果将文件上传到在故障切换中配置为对等体的 ASA，则 CDO 不会为故障切换对中的另一个对等体确认新文件，并且设备状态更改为**未同步**。您必须手动将更改部署到**两台**设备，以便 CDO 识别两台设备中的文件。

删除操作会从闪存中永久删除所选文件。删除文件时，系统会显示一条消息，要求确认。使用以下程序从所选 ASA 设备中删除文件：

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击 **ASA** 选项卡并选择 ASA 设备。

**步骤 4** 在右侧的**管理 (Management)** 窗格中点击**文件管理 (File Management)**。

**步骤 5** 选择要删除的文件，然后在右侧的**操作**下，点击**删除**。最多可以选择 25 个文件。如果 CDO 无法删除某些文件，您可以查看设备**工作流程**以确定已删除和保留的文件。

**步骤 6** 如果您已选择删除 AnyConnect 软件包，请将配置更改从 CDO 部署到 ASA。

# 管理 ASA 高可用性

## 在主用-主用故障切换模式下对 ASA 所做的配置更改

当 Cisco Defense Orchestrator (CDO) 使用 CDO 上的暂存配置更改 ASA 的运行配置时，或者当它使用 ASA 上存储的配置更改 CDO 上的配置时，它会尝试仅更改配置文件的相关行（如果该方面存在）的配置可以通过 CDO GUI 进行管理。如果无法使用 CDO GUI 进行所需的配置更改，CDO 会尝试覆盖整个配置文件以进行更改。

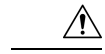
以下是两个示例：

- 您可以使用 CDO GUI 创建或更改网络对象。如果 CDO 需要将该更改部署到 ASA 的配置中，则会在发生更改时覆盖 ASA 上正在运行的配置文件的相关行。

- 您无法使用 CDO GUI 创建新的 ASA 用户。如果使用 ASA 的 ASDM 或 CLI 将新用户添加到 ASA，当该带外更改被接受且 CDO 更新存储的配置文件时，CDO 会尝试覆盖在 CDO 上暂存的 ASA 的整个配置文件。

在主用-主用故障切换模式下配置 ASA 时，不遵循这些规则。当 CDO 管理在主用-主用故障切换模式下配置的 ASA 时，CDO 无法始终将所有配置更改从自身部署到 ASA 或将所有配置更改从 ASA 读取到自身中。以下是这种情况的两种情况：

- 在 CDO 中对 ASA 的配置文件所做的更改（CDO 在 CDO GUI 中不支持）无法部署到 ASA。此外，对 CDO 不支持的配置文件所做的更改，以及对 CDO 支持的配置文件所做的更改，都无法部署到ASA。在这两种情况下，您都会收到错误消息：“CDO 目前不支持在故障切换模式下替换设备的完整配置。请点击“取消”并手动将更改应用到设备。”与CDO界面中的消息一起，您会看到已禁用的替换配置按钮。
- CDO 不会拒绝对在主用-主用故障切换模式下配置的 ASA 所做的带外更改。如果对 ASA 的运行配置进行带外更改，则 ASA 会在“设备和服务”(Devices & Services) 页面上标记为“检测到冲突”(Conflict Detected)。如果您查看冲突并尝试拒绝，CDO 会阻止该操作。您收到消息“CDO 不支持拒绝此设备的带外更改。此设备正在运行不受支持的软件版本，或者是主用/主用故障切换对的成员。请点击“继续”以接受带外更改。”



**Caution** 如果您发现自己必须接受来自 ASA 的带外更改，则在 CDO 上暂存但尚未部署到 ASA 的任何配置更改都将被覆盖并丢失。

当 CDO GUI 支持这些更改时，CDO 支持在故障切换模式下对 ASA 进行的配置更改。

**相关信息：**

# 在 ASA 上配置 DNS

使用此程序在每个 ASA 上配置域名服务器 (DNS)。

### 前提条件

- ASA 必须能够访问互联网。
- 在开始安装之前收集这些信息：
  - 可以访问 DNS 服务器的 ASA 接口的名称；例如，inside、outside 或 dmz。
  - 您的组织使用的 DNS 服务器的 IP 地址。如果您不维护自己的 DNS 服务器，可以使用思科 Umbrella。思科 Umbrella 的 IP 地址为 208.67.220.220。

## 操作步骤

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。
**步骤 2** 点击**设备 (Devices)** 选项卡。
**步骤 3** 点击 **ASA** 选项卡，然后选择要配置 DNS 的所有 ASA。
**步骤 4** 在右侧的操作窗格中，选择**命令行接口 (Command Line Interface)**。
**步骤 5** 点击 CLI 宏收藏夹星标。
**步骤 6** 在宏面板中选择配置 DNS 宏。
**步骤 7** 选择 > 视图参数，然后在参数列中填写以下参数的值：

- IF_Name - 可以访问 DNS 服务器的 ASA 接口的名称。
- IP_ADDR - 您的组织使用的 DNS 服务器的 IP 地址。

**步骤 8** 点击**发送到设备 (Send to devices)**。

# CDO 命令行界面

CDO 为用户提供命令行界面 (CLI)，用于管理 ASA 设备。用户可以将命令发送到单个设备或同时发送到多个设备。

**相关信息：**

- 有关详细的 ASA CLI 文档，请参阅ASA 命令行接口文档, on page 95。

## 使用命令行接口

**步骤 1** 打开**清单 (Inventory)** 页面。
**步骤 2** 点击“清单”(Inventory) 表上方的**设备 (Devices)** 按钮。
**步骤 3** 使用设备选项卡和过滤器按钮查找要使用命令行界面 (CLI) 管理的设备。
**步骤 4** 选择设备。
**步骤 5** 在**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。
**步骤 6** 点击 **命令行接口 (Command Line Interface)**。
**步骤 7** 在命令窗格中输入一个或多个命令，然后点击发送。 设备对命令的响应显示在下面的“响应窗格”中。

**Note** 如果可以运行的命令有限制，则会在命令窗格上方列出这些限制。

**Related Topics**

在命令行接口中输入命令，第 84 页

# 在命令行接口中输入命令

可以在一行中输入单个命令，也可以在多行中依次输入多个命令，CDO将按顺序执行这些命令。以下示例发送创建三个网络对象和包含这些网络对象的网络对象组的一批命令。ASA


输入设备命令：CDO 在 的全局配置模式下执行命令。ASAASA

长命令：如果您输入一个很长的命令，CDO 会尝试将您的命令拆分为多个命令，以便可以针对 API 运行所有这些命令。如果CDO无法确定命令的正确分隔，它会提示您提示中断命令列表的位置。例如：

错误：CDO 尝试执行此命令中长度超过 600 个字符的部分。您可以通过在命令列表之间添加一个空行来向 CDO 提示适当的命令分隔点。

如果收到此错误：

**步骤 1** 点击 CLI 历史记录窗格中导致错误的命令。CDO 使用一长串命令填充命令框。

**步骤 2** 通过在相关命令组后面输入空行来编辑长命令列表。例如，在定义网络对象列表并将其添加到上述示例中的组后，添加一个空行。您可能希望在命令列表中的几个不同位置执行此操作。

**步骤 3** 点击**发送 (Send)**。

# 使用命令历史记录

发送 CLI 命令后，CDO 会在“命令行界面”(Command Line Interface) 页面的历史记录窗格中记录该命令。您可以重新运行历史记录窗格中保存的命令，或将这些命令用作模板：

**步骤 1** 在**清单 (Inventory)** 页面上，选择要配置的设备。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 点击 **>_命令行接口 (>_Command Line Interface)**。

**步骤 5** 点击时钟图标可展开历史记录窗格（如果尚未展开）。

**步骤 6** 在历史记录窗格中选择要修改或重新发送的命令。

**步骤 7** 按原样重新使用命令，或在命令窗格中对其进行编辑，然后点击发送。CDO 在响应窗格中显示命令的结果。

**Note** CDO 显示 Done!两种情况下响应窗格中的消息：

- 成功执行命令后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

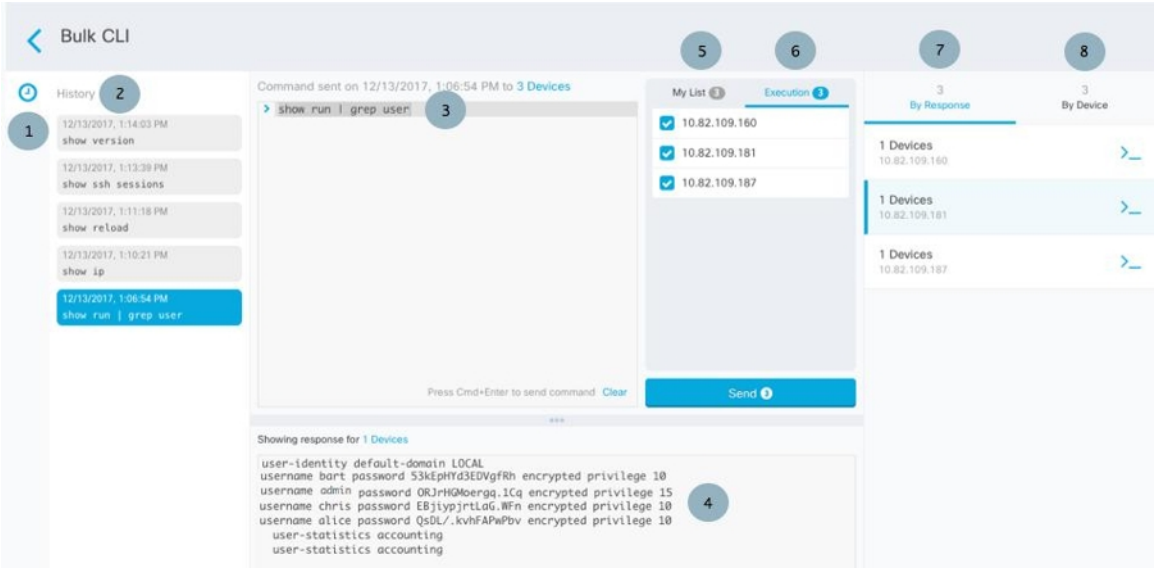
# 批量命令行接口

CDO 为用户提供使用命令行接口 (CLI) 管理 Secure Firewall ASA、FDM 管理 威胁防御、SSH 和 Cisco IOS 设备。用户可以将命令发送到单个设备或同时发送到多个同类设备。本节介绍一次向多台设备发送 CLI 命令。

**相关信息：**

- 有关详细的 ASA CLI 文档，请参阅ASA 命令行接口文档, on page 95。

## 批量 CLI 接口



**Note** CDO 显示 Done!两种情况下的消息：

- 成功执行命令且无错误后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的show命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

| 编号 | 说明 |
|---|---|
| 1 | 点击时钟可展开或折叠命令历史记录窗格。 |
| 2 | 命令历史记录。发送命令后，CDO 会在此历史记录窗格中记录该命令，以便您可以返回到该窗格，选择并再次运行该命令。 |
| 3 | 命令窗格。在此窗格的提示符后输入命令。 |
| 4 | 响应窗格。CDO 显示设备对命令的响应以及 CDO 消息。如果多个设备的响应相同，则响应窗格会显示消息“显示 X 台设备的响应”(Showing Responses for X devices)。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。<br>**Note** CDO 显示 Done!两种情况下的消息：<br>• 成功执行命令且无错误后。<br>• 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的show命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。 |
| 5 | **我的列表 (My List)** 选项卡显示您从**清单 (Inventory)** 表中选择的设备，并允许您包含或排除要向其发送命令的设备。 |
| 6 | 上图中突出显示的“执行”选项卡显示在历史记录窗格中选择的命令中的设备。在本例中，show run \|在历史记录窗格中选择了 grep 用户命令，执行选项卡显示它已发送到 10.82.109.160、10.82.109.181 和 10.82.10.9.187。 |
| 7 | 点击“By Response”（按响应）选项卡将显示命令生成的响应列表。相同的响应组合在一行中。当您在“按响应”选项卡中选择一行时，CDO 会在响应窗格中显示对该命令的响应。 |
| 8 | 点击“按设备”选项卡会显示每个设备的单独响应。点击列表中的其中一个设备，即可查看特定设备对命令的响应。 |

# 批量发送命令

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 选择相应的设备选项卡，然后使用过滤器按钮查找要使用命令行界面配置的设备。

**步骤 4** 选择设备。

**步骤 5** 在**设备操作 (Device Actions)** 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

**步骤 6** 您可以在“我的列表”字段中选中或取消选中要向其发送命令的设备。

**步骤 7** 在命令窗格中输入命令，然后点击发送。命令输出显示在响应窗格中，命令记录在更改日志中，命令CDO在批量CLI 窗口的历史记录窗格中记录您的命令。

**Note** 命令将在已同步的选定ASA 设备上成功执行，但在未同步的设备上可能会失败。如果任何选定的ASA 设备未同步，则仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto、dir、write 和 copy。

# 使用批量命令历史记录

发送批量 CLI 命令后，CDO 会在“批量 CLI”页面历史记录页面中记录该命令。批量 CLI 接口, on page 86您可以重新运行历史记录窗格中保存的命令，也可以将这些命令用作模板。历史记录窗格中的命令与运行这些命令的原始设备相关联。

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以找到设备。

**步骤 3** 点击相应的设备类型选项卡，然后点击过滤器图标以查找要配置的设备。

**步骤 4** 选择设备。

**步骤 5** 点击 **命令行接口 (Command Line Interface)**。

**步骤 6** 在“历史记录”窗格中选择要修改或重新发送的命令。请注意，您选择的命令与特定设备相关联，而不一定是您在第一步中选择的设备。

**步骤 7** 查看我的列表选项卡，确保您要发送的命令将发送到您期望的设备。

**步骤 8** 在命令窗格中编辑命令，然后点击**发送 (Send)**。CDO 在响应窗格中显示命令的结果。

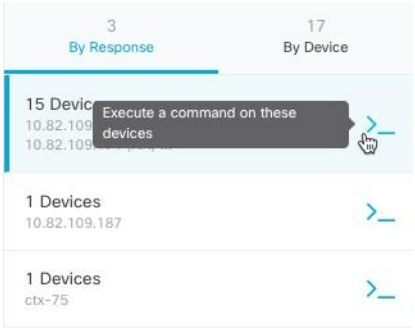
**Note** 命令将在已同步的选定ASA 设备上成功执行，但在未同步的设备上可能会失败。如果任何选定的ASA 设备未同步，则仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto、dir、write 和 copy。

# 使用批量命令过滤器

运行批量 CLI 命令后，您可以使用“按响应”过滤器和“按设备”过滤器继续配置设备。

## 按响应过滤器

运行批量命令后，CDO 会使用发送该命令的设备返回的响应列表填充“按响应”选项卡。具有相同响应的设备会合并到一行中。点击“按响应”(By Response) 选项卡中的行会在响应窗格中显示设备的响应。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。




要将命令发送到与命令响应关联的设备列表，请执行以下程序：

**步骤 1** 点击 By Response 选项卡中一行中的命令符号。

**步骤 2** 查看命令窗格中的命令，然后点击发送以重新发送命令，或点击清除以清除命令窗格并输入要发送到设备的新命令，然后点击发送。

**步骤 3** 查看从命令收到的响应。

**步骤 4** 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 write memory，然后点击 Send。这样会将运行配置保存至启动配置。

## 按设备过滤器

运行批量命令后，CDO 会使用已发送命令的设备列表填充“执行”选项卡和“按设备”选项卡。点击“按设备”(By Device) 选项卡中的行会显示每个设备的响应。

要在同一设备列表上运行命令，请执行以下程序：

**步骤 1** 点击**按设备 (By Device)** 选项卡。

**步骤 2** 点击 **>_在这些设备上执行命令**。

**步骤 3** 点击**清除 (Clear)** 以清除命令窗格并输入新命令。

**步骤 4** 在我的列表窗格中，通过选中或取消选中列表中的单个设备来指定要向其发送命令的设备列表。

**步骤 5** 点击**发送 (Send)**。命令的响应会显示在响应窗格中。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。

**步骤 6** 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入`write memory`，然后点击**发送 (Send)**。

# 命令行界面宏

CLI 宏是可以使用的完整形式的 CLI 命令，或者是可以在运行之前修改的 CLI 命令的模板。所有宏都可以在一个或多个 ASA 设备上同时运行。

使用类似模板的 CLI 宏可同时在多台设备上运行相同的命令。CLI 宏可促进设备配置和管理的一致性。使用完全格式的 CLI 宏获取有关设备的信息。您可以立即在 ASA 设备上使用不同的 CLI 宏。

您可以创建 CLI 宏来监控您经常执行的任务。有关详细信息，请参阅从新命令创建 CLI 宏。

CLI 宏是系统定义的或用户定义的。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。

**Note** 只有在设备载入 CDO 后，才能为设备创建宏。

以 ASA 为例，如果要查找其中一个 ASA 上的特定用户，可以运行以下命令：

```
show running-config | grep username
```

运行命令时，您要将 *username* 替换为要搜索的用户的用户名。要使用此命令来创建宏，请使用相同的命令并在用户名周围加上大括号。

```
> show running-config | grep {{username}}
```

您可以随意命名参数。您还可以使用此参数名称创建相同的宏：

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

参数名称可以是描述性的，并且必须使用字母数字字符和下划线。命令语法，在本例中为

```
show running-config | grep
```

命令的一部分，必须对要向其发送命令的设备使用正确的 CLI 语法。

# 从新命令创建 CLI 宏

**步骤 1** 在创建 CLI 宏之前，请在 CDO 的命令行界面中测试命令，以便确保命令语法正确并返回可靠的结果。

**Note**
- 有关详细的 ASA CLI 文档，请参阅ASA 命令行接口文档, on page 95。

**步骤 2** 在导航栏中，点击**清单 (Inventory)**。

**步骤 3** 点击 **设备 (Devices)**选项卡以找到设备。

**步骤 4** 点击相应的设备类型选项卡，然后选择在线和同步的设备。

**步骤 5** 点击 **>_Command Line Interface**。

**步骤 6** 点击 CLI 宏收藏夹星标 ，以查看已经存在的宏。

**步骤 7** 点击加号按钮 。

**步骤 8** 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

**步骤 9** 在**命令 (Command)** 字段中输入完整命令。

**步骤 10** 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

**步骤 11** 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 CLI 宏。

# 从 CLI 历史记录或现有 CLI 宏创建 CLI 宏

在此程序中，您将从已运行的命令、另一个用户定义的宏或从系统定义的宏创建用户定义的宏。

**步骤 1** 在导航栏中，点击 **设备和服务**。

**注释** 如果要从CLI历史记录创建用户定义的宏，请选择运行命令的设备。CLI宏在同一账户上的设备之间共享，但不是 CLI 历史记录。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择在线和同步的设备。

**步骤 4** 点击 **>_命令行接口**。

**步骤 5** 查找要生成 CLI 宏的命令，然后选择该命令。使用以下方法之一：

- 点击时钟 可查看您在该设备上运行的命令。选择要转换为宏的命令，命令将显示在命令窗格中。
- 点击 CLI 宏收藏夹星标 ，以查看已经存在的宏。选择要更改的用户定义或系统定义的 CLI 宏。命令显示在命令窗格中。

**步骤 6** 使用 命令窗格中的 命令，点击 CLI 宏金色星标 。命令现在是新 CLI 宏的基础。

**步骤 7** 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

**步骤 8** 查看命令字段中的命令，并进行所需的更改。

**步骤 9** 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

**步骤 10** 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 CLI 宏。

# 运行 CLI 宏

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择一个或多个设备。

**步骤 4** 点击 **>_命令行接口**。

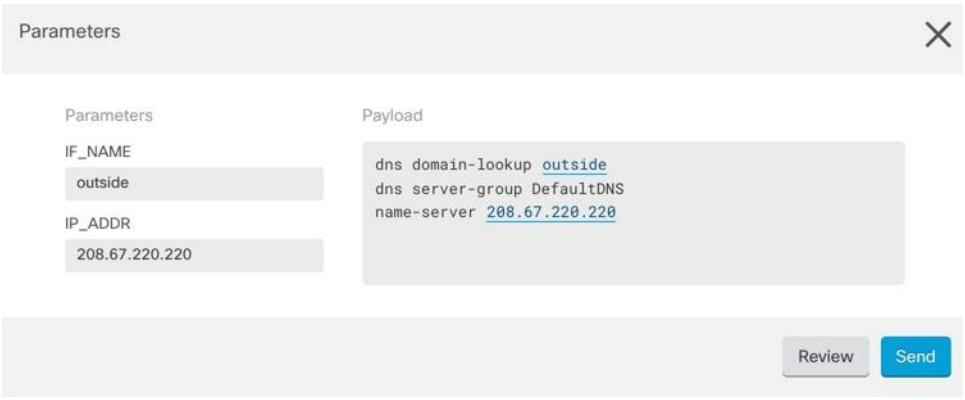
**步骤 5** 在命令面板中，点击星号 ★。

**步骤 6** 从命令面板中选择 CLI 宏。

**步骤 7** 使用以下两种方式之一运行宏：

- 如果宏没有要定义的参数，请点击**发送 (Send)**。命令的响应显示在响应窗格中。就行了。
- 如果宏包含参数，例如下面的配置 DNS 宏，请点击 **>_ 查看参数**。


**步骤 8** 在“参数”(Parameters) 窗格中，在“参数”(Parameters) 字段中填写参数的值。




**步骤 9** 点击 **Send**。在 CDO 成功发送命令并更新设备配置后，您会收到消息完成！

- 对于 ASA，将更新当前配置文件：

**步骤 10** 发送命令后，您可能会看到消息“某些命令可能已对运行配置进行了更改”(Some commands may have made changes to the running config) 以及两个链接。


- 点击**写入磁盘 (Write to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到设备的启动配置中。

- 点击**消除 (Dismiss)**，可关闭消息。

# 编辑 CLI 宏

您可以编辑用户定义的 CLI 宏，但不能编辑系统定义的宏。编辑 CLI 宏会更改所有 ASA 设备。宏并非特定于特定设备。

**步骤 1** 在导航栏中，点击 **设备和服务**。
**步骤 2** 点击**设备**选项卡。
**步骤 3** 点击适当的设备类型选项卡。
**步骤 4** 请选择您的设备。
**步骤 5** 点击 **命令行接口 (Command Line Interface)**。
**步骤 6** 选择要编辑的用户定义的宏。
**步骤 7** 点击宏标签中的编辑图标。
**步骤 8** 在编辑宏对话框中编辑 CLI 宏。
**步骤 9** 点击**保存 (Save)**。

有关如何运行 CLI 宏的说明，请参阅运行 CLI 宏。

# 删除 CLI 宏

您可以删除用户定义的 CLI 宏，但不能删除系统定义的宏。删除 CLI 宏会删除所有设备的宏。宏并非特定于特定设备。

**步骤 1** 在导航栏中，点击 **设备和服务**。
**步骤 2** 点击**设备**选项卡。
**步骤 3** 点击适当的设备类型选项卡。
**步骤 4** 请选择您的设备。
**步骤 5** 点击 >_**命令行接口 (Command Line Interface)**。
**步骤 6** 选择要删除的用户定义的 CLI 宏。
**步骤 7** 点击 CLI 宏标签中的垃圾桶图标 。
**步骤 8** 确认要删除 CLI 宏。

# 使用 CDO CLI 配置 ASA

您可以通过在 CDO 中提供的 CLI 界面中运行 CLI 命令来配置 ASA 设备。要使用该接口，请在**清单 (Inventory)** 菜单上选择设备，然后点击**命令行界面 (Command Line Interface)**。有关更多信息，请参阅使用 CDO 命令行接口。

### 添加新的日志记录服务器

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。

有关详细信息，请参阅您正在运行的 ASA 版本的《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中“日志记录”一章的“监控”部分。

### 配置 DNS 服务器

需要配置 DNS 服务器，以便 ASA 能够将主机名解析为 IP 地址。还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

有关详细信息，请参阅所运行 ASA 版本的《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中“配置 DNS 服务器”部分的“基本设置”一章。

### 添加静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。

有关详细信息，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中的“静态和默认路由”一章。

### 配置接口

您可以使用 CLI 命令配置管理和数据接口。有关详细信息，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》的“基本接口配置”一章。

# 使用 CDO 来比较 ASA 配置

使用此程序可比较两个 ASA 的配置。

**步骤 1** 在导航菜单中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备 (Devices)** 选项卡以查找 ASA 设备，或点击**模板 (Templates)** 选项卡以查找 ASA 型号设备。

**步骤 3** 点击 **ASA** 选项卡。

**步骤 4** 过滤要比较的设备的设备列表。

**步骤 5** 选择两个 ASA。它们的状态无关紧要。您正在比较 Defense Orchestrator 上存储的 ASA 配置。

**步骤 6** 在右侧的“设备操作”(Device Actions) 窗格中，点击 **比较 (Compare)**。

**步骤 7** 在比较配置对话框中，点击**下一步**和**上一步**可跳过配置文件中以蓝色突出显示的差异。

# ASA 批量 CLI 使用案例

以下情况是您对 ASA 设备使用 CDO 的批量 CLI 功能时可能遇到的工作流程。

## 显示 ASA 的运行配置中的所有用户，然后删除其中一个用户

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击 **ASA** 选项卡。

**步骤 4** 搜索并过滤要从中删除用户的设备的设备列表，然后选择这些设备。

**Note** 确保您选择的设备已同步。设备未同步时，仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto、dir、copy 和 write。

**步骤 5** 在详细信息窗格中点击**>_命令行接口 (>_Command Line Interface)**。CDO 列出您在我的列表窗格中选择的设备。如果您决定将命令发送到更少的设备，请取消选中该列表中的设备。

**步骤 6** 在命令窗格中，输入 show run | grep user，然后点击 Send。 运行配置文件中包含字符串 user 的所有行都将显示在响应窗格中。系统将打开“执行”选项卡，显示执行命令的设备。

**步骤 7** 点击按响应选项卡并查看响应，以确定哪些设备具有要删除的用户。

**步骤 8** 点击我的列表选项卡，然后选择要从中删除用户的设备列表。

**步骤 9** 在命令窗格中，输入 no 形式的 user 命令以删除 user2，然后点击 Send。在本示例中，您将删除 user2：
no user user2 password reallyhardpassword privilege 10

**步骤 10** 在历史记录面板中查找 show run | 的实例。用于搜索用户名的 grep user 命令。选择该命令，查看“执行”列表中的设备列表，然后选择“发送”。您应该会看到用户名已从您指定的设备中删除。

**步骤 11** 如果您确信已从运行配置中删除了正确的用户，并且正确的用户仍保留在运行配置中：

**a.** 从历史记录窗格中选择 no user user2 password reallyhardpassword privilege 10 命令。

**b.** 点击 By Device 选项卡，然后点击 Execute a command on these devices。

**c.** 在命令窗格中，点击清除以清除命令窗格。

**d.** 输入命令 deploy memory，然后点击 Send。

## 查找所选 ASA 上的所有 SNMP 配置

此程序显示 ASA 运行配置中的所有 SNMP 配置条目。

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击 **ASA** 选项卡。

**步骤 4** 过滤并搜索要在其上分析运行配置中的 SNMP 配置的设备，然后选择这些设备。

**Note** 确保您选择的设备已同步。设备未同步时，仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto 和 dir。

**步骤 5** 在详细信息窗格中点击 **命令行接口 (Command Line Interface)**。您选择的设备位于我的列表窗格中。如果您决定将命令发送到更少的设备，请取消选中列表中的设备。

**步骤 6** 在命令窗格中，输入 show run | grep snmp，然后点击 Send。 运行配置文件中包含字符串 snmp 的所有行都将显示在响应窗格中。系统将打开“执行”选项卡，显示执行命令的设备。

**步骤 7** 查看响应窗格中的命令输出。

# ASA 命令行接口文档

CDO 完全支持 ASA 命令行界面。我们在 CDO 中提供类似终端的接口，供用户同时向单个设备和多个设备发送 ASA 命令。ASA 命令行接口文档涵盖的范围非常广泛。这里不是在 CDO 文档中重新创建部分内容，而是指向 Cisco.com 上的 ASA CLI 文档。

### ASA 命令行界面配置指南

从 ASA 9.1 版开始，《ASA CLI 配置指南》分为三本单独的指南：

- 《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》
- 《CLI 手册 2：思科 ASA 系列防火墙 CLI 配置指南》
- 《CLI 手册 3：思科 ASA 系列 VPN CLI 配置指南》

您可以通过以下方式访问 Cisco.com 上的 ASA CLI 配置指南：支持 (Support) > 按类别划分的产品 (Products by Category) > 安全 (Security) > 防火墙 (Firewalls) > ASA 5500 > 配置 (Configure) > 配置指南 (Configuration Guides)。

### ASA 命令行界面配置指南的几个特定部分

**过滤 show 和 more 命令输出**。您可以在《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》的过滤 show 和 more 命令输出下了解如何使用正则表达式过滤 show 命令输出。

### ASA 命令参考

《ASA 命令参考指南》按字母顺序列出了所有 ASA 命令及其选项。ASA 命令参考不是特定于版本的。它出版了四本书：

- 思科 ASA 系列命令参考，A - H 命令
- 思科 ASA 系列命令参考，I - R 命令
- 思科 ASA 系列命令参考，S 命令
- 思科 ASA 系列命令参考，适用于 ASASM 的 T - Z 命令和思科 IOS 命令

您可以通过以下方式访问 Cisco.com 上的《ASA 命令参考指南》：支持 (Support) > 按类别划分的产品 (Products by Category) > 安全 (Security) > 防火墙 (Firewalls) > ASA 5500 > 参考指南 (Reference Guides) > 命令参考 (Command References) > ASA 命令参考 (ASA Command References)。

# 导出 CDO CLI 命令结果

您可以将向独立设备或多个设备发出的CLI命令结果导出为逗号分隔值（.csv）文件，以便您可以随意过滤和排序其中的信息。您可以导出单个设备或多个设备的CLI结果。导出的信息包含以下内容：

- 设备
- 日期
- 用户
- 命令
- 输出

## 导出 CLI 命令结果

您可以将刚刚在命令窗口中执行的命令的结果导出到 .csv 文件：

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备，使其突出显示。

**步骤 5** 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 6** 在命令行界面窗格中，输入命令并点击**发送 (Send)** 以向设备发出命令。

**步骤 7** 在已输入命令的窗口右侧，点击导出图标。

**步骤 8** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

# 导出 CLI 宏的结果

您可以导出已在命令窗口中执行的宏的结果。使用以下程序可将在一台或多台设备上执行的 CLI 宏的结果导出到 .csv 文件：

**步骤 1** 打开 **设备和服务** 页面。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备，使其突出显示。

**步骤 5** 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 6** 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。

**步骤 7** 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

**步骤 8** 在已输入命令的窗口右侧，点击导出图标 。

**步骤 9** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

# 导出 CLI 命令历史记录

使用以下程序将一个或多个设备的 CLI 历史记录导出到 .csv 文件：

**步骤 1** 在导航窗格中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备，使其突出显示。

**步骤 5** 在设备的“设备操作”(Device Actions) 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 6** 如果历史记录窗格尚未展开，请点击时钟图标将其展开。

**步骤 7** 在已输入命令的窗口右侧，点击导出图标。

**步骤 8** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

**相关信息：**

- CDO 命令行界面, on page 83
- 从新命令创建 CLI 宏
- 删除 CLI 宏

- 编辑 CLI 宏
- 运行 CLI 宏
- ASA 批量 CLI 使用案例
- ASA 命令行接口文档
- 批量命令行接口

# 导出 CLI 宏列表

您只能导出已在命令窗口中执行的宏。使用以下程序将一个或多个设备的 CLI 宏导出到 .csv 文件：

**步骤 1** 在导航窗格中，点击 **设备和服务**。
**步骤 2** 点击**设备**选项卡。
**步骤 3** 点击适当的设备类型选项卡。
**步骤 4** 选择一个或多个设备，使其突出显示。
**步骤 5** 在设备的“设备操作”(Device Actions) 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。
**步骤 6** 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。
**步骤 7** 点击要导出的宏命令。填写任何适当的参数，然后点击发送。
**步骤 8** 在已输入命令的窗口右侧，点击导出图标。
**步骤 9** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。

# 恢复 ASA 配置

如果对的配置进行了更改，并且想要恢复该更改，则可以恢复过去的配置。ASAASA这是一种删除具有意外或意外结果的配置更改的便捷方法。

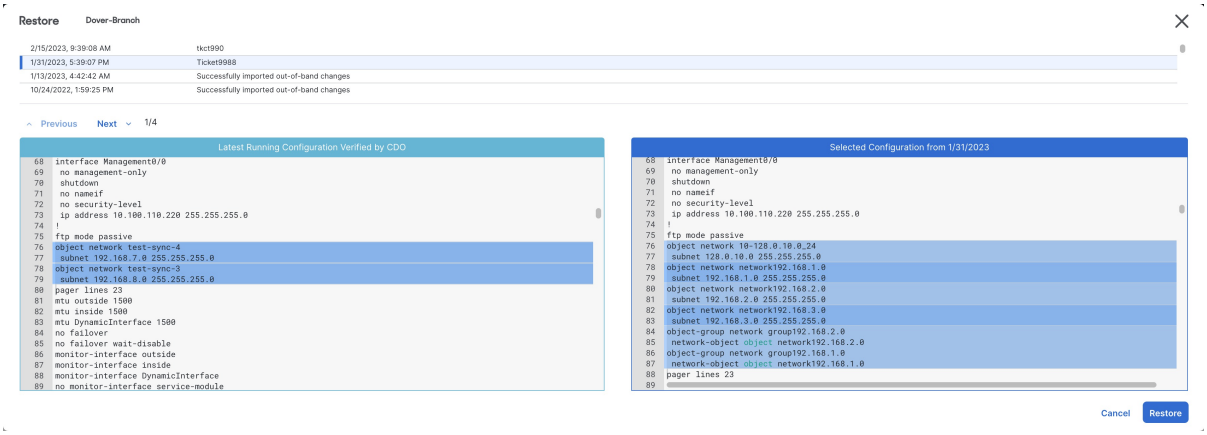
### 关于恢复 ASA 配置

在恢复配置之前，请查看以下说明：

- 会将您选择要恢复的配置与部署到 的最后一个已知配置进行比较，但不会将您选择要恢复的配置与已暂存但未部署到的配置进行比较。CDOASAASA如果您的上有任何未部署的更改，并且您恢复了过去的配置，则恢复过程将覆盖未部署的更改，您将丢失这些更改。ASA
- 在恢复过去的配置之前， 可以处于“已同步”或“未同步”状态，但如果设备处于“检测到冲突”状态，则必须先解决冲突，然后才能恢复过去的配置。ASA
- 恢复过去的配置会覆盖所有中间部署的配置更改。例如，从以下列表中的 1/31/2023 恢复配置会覆盖在 2/15/2023 所做的配置更改。

- 点击“Next”（下一步）和“Previous”（上一步）按钮将在配置文件中移动并突出显示配置文件更改
- 如果您最初对配置更改应用了更改请求标签，则该标签会显示在“恢复配置”列表中。

***Figure 4: ASA*** 恢复配置屏幕




### 配置更改保留多长时间？

您可以恢复使用时间不超过 1 年的配置。恢复在其更改日志中记录的配置更改。ASACDO每次向 写入或读取配置更改时，更改日志都会记录更改。存储 1 年的变更日志，并且对上一年内进行的备份数量没有限制。ASACDO

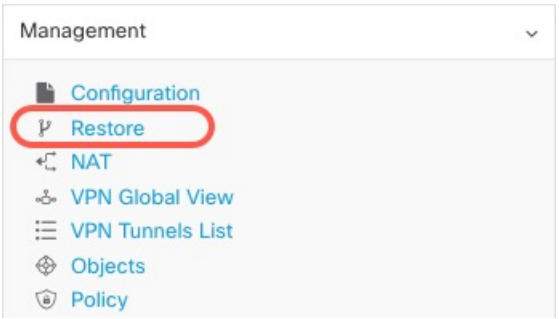
# 恢复 Secure Firewall ASA 配置

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

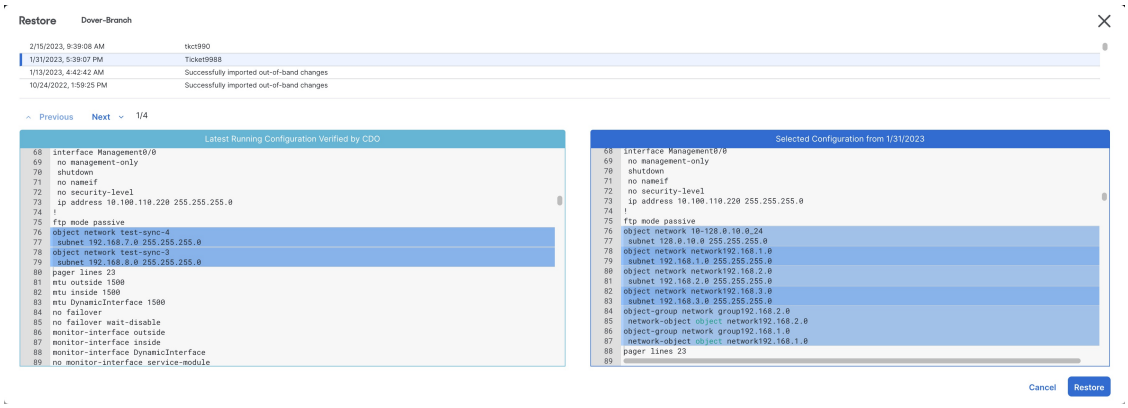
**步骤 2** 点击ASA选项卡。

**步骤 3** 选择您要恢复其配置的 ASA。

**步骤 4** 在**管理 (Management)** 窗格中，点击**恢复 (Restore)**。




**步骤 5** 在“恢复”(Restore) 页面中，选择要恢复的配置。




例如，在上图中，选择了 1/31/2023 的配置。

**步骤 6** 比较“由 CDO 验证的最新运行配置”和“自 < 日期 > 起的选定配置”，以确保您要恢复“自 < 日期 > 起的选定配置 > 窗口中显示的配置。使用“上一个”和“下一个”比较所有更改。

**步骤 7** 点击恢复，这将在 CDO 中暂存配置。在**清单 (Inventory)** 页面上，您会看到设备的配置状态现在为“未同步”(Not Synced)。

**步骤 8** 点击右侧窗格中的**部署更改...(Deploy Changes...)** 以部署更改并同步 ASA。

## 故障排除

如何恢复丢失但想要保留的更改？

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击 ASA 选项卡。

**步骤 4** 选择所需的设备。

**步骤 5** 点击右侧窗格中的更改日志。

**步骤 6** 查看更改日志中的更改。您可以根据这些记录重建丢失的配置。

# 管理 ASA 和 Cisco IOS 设备配置文件

某些类型的设备将其配置存储在单个文件中，例如 ASA 和 Cisco IOS 设备。对于这些设备，您可以在 Cisco Defense Orchestrator 上查看配置文件并在上面执行各种操作。

## 查看设备的配置文件

对于将整个配置存储在单个配置文件中的设备（例如 ASA、SSH 托管设备和运行Cisco IOS 的设备），您可以使用 CDO 查看配置文件。

注释 SSH 管理的设备和思科 IOS 设备具有只读配置。

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要查看其配置的设备或型号。

**步骤 5** 在右侧的 **管理 (Management)** 窗格中，点击**配置 (Configuration)**。
系统将显示完整的配置文件。

**相关信息：**

- 编辑完整的设备配置文件

# 编辑完整的设备配置文件

某些类型的设备将其配置存储在单个配置文件中，例如 ASA 。对于这些设备，您可以在 CDO 上查看设备配置文件，并根据设备对其执行各种操作。

目前，只能使用 CDO 直接编辑 ASA 配置文件。

**Caution** 此程序适用于熟悉设备配置文件语法的高级用户。此方法直接对 Defense Orchestrator 上存储的配置文件副本进行更改。

## 操作步骤

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击 **ASA** 选项卡。

**步骤 4** 选择要编辑其配置的设备。

**步骤 5** 在右侧的 **管理 (Management)** 窗格中，点击**配置 (Configuration)**。

**步骤 6** 在设备配置页面中，点击编辑。

**步骤 7** 点击右侧的编辑器按钮，然后选择**默认**文本编辑器、**Vim** 或 **Emacs** 文本编辑器。

**步骤 8** 编辑文件并保存更改。

**步骤 9** 返回到设备和服务页面，预览并部署更改。

# 读取、丢弃、检查和部署更改

为了管理设备，CDO必须在其本地数据库中存储自己的设备配置副本。当CDO从其管理的设备“读取”配置时，它会获取设备配置的副本并将其保存。CDO首次在设备载入时读取并保存设备配置的副本。这些选项描述了出于不同目的而读取配置：

- 当设备的配置状态为“未同步”(Not Synced)时，可以使用**放弃更改 (Discard Changes)**。在“未同步”状态下，CDO上的设备配置有待更改。此选项允许您撤消所有待处理的更改。待处理的更改将被删除，并且 CDO 会使用设备上存储的配置副本覆盖其配置副本。
- **检查更改**。如果设备的配置状态为“已同步”(Synced)，则此操作可用。点击“检查更改”(Checking for Changes) 会指示 CDO 将其设备配置副本与设备上存储的配置副本进行比较。如果存在差异，CDO 会立即使用设备上存储的副本覆盖其设备配置副本。
- **审核冲突**并**接受而不审核**。。如果您在设备上启用了冲突检测 (Conflict Detection)，CDO 会每10分钟检查一次设备上的配置更改。如果设备上存储的配置副本已更改，CDO会通过显示“检测到冲突“配置状态来通知您。
  - **查看冲突**。点击查看冲突，您可以查看直接在设备上进行的更改，并接受或拒绝这些更改。
  - **接受而不审核**。此操作会使用设备上存储的最新配置副本来覆盖设备配置的CDO副本。在执行覆盖操作之前，CDO 不会提示您确认配置的两个副本中的差异。

**读取所有**是一个批处理操作。您可以选择任何状态的多个设备，然后点击**读取全部 (Read All)**，以使用设备上存储的配置覆盖 CDO 上存储的所有设备的配置。

### 部署更改

当您更改设备的配置时，CDO会将您所做的更改保存到自己的配置副本中。在将这些更改部署到设备之前，这些更改在CDO上“待处理”。当设备的配置发生更改但尚未部署到设备时，该设备将处于“未同步”配置状态。

待处理的配置更改对通过设备运行的网络流量没有影响。只有在CDO将更改部署到设备后，它们才会生效。当CDO将更改部署到设备的配置时，它只会覆盖已更改的配置元素。它不会覆盖设备上存储的整个配置文件。可以为单个设备或同时在多个设备上启动部署。

注释 您可以安排部署或定期部署。有关详细信息，请参阅计划自动部署，第 319 页。

**丢弃全部 (Discard All)** 选项仅在您点击**预览并部署...(Preview and Deploy...)**。点击“预览并部署”(Preview and Deploy) 后，CDO 会向您显示 CDO 中待处理更改的预览。点击**丢弃全部 (Discard All)** 会从 CDO 中删除所有待处理的更改，并且不会将任何内容部署到所选设备。与上面的“放弃更改”(Discard Changes) 不同，删除待处理的更改是操作的结束。

# 读取所有设备配置

如果在 Cisco Defense Orchestrator (CDO) 之外对设备进行配置更改，则存储在 CDO 上的设备配置与其配置的本地副本将不再相同。您可能希望使用设备上存储的配置覆盖CDO的设备配置副本，以使配置再次相同。您可以使用**全部读取 (Read All)** 链接在多台设备上同时执行此任务。

有关 CDO 如何管理设备配置的两个副本的详细信息，请参阅读取、丢弃、检查和部署更改。

以下是三种配置状态，其中点击**全部读取 (Read All)** 将使用设备的配置副本覆盖 CDO 的设备配置副本。

- **检测到冲突 (Conflict Detected)** - 如果启用冲突检测，CDO 将每 10 分钟轮询一次其管理的设备，以了解对其配置所做的更改。如果 CDO 发现设备上的配置已更改，则 CDO 会显示设备的“检测到冲突”(Conflict detected) 配置状态。
- **已同步 (Synced)** - 如果设备处于同步状态，并且您点击**全部读取 (Read All)**，CDO 会立即检查设备以确定是否直接对其配置进行了任何更改。点击**读取全部 (Read All)** 后，CDO 会确认您是否打算覆盖其设备配置副本，然后 CDO 会执行覆盖。
- **未同步 (Not Synced)** - 如果设备处于未同步状态，并且您点击**全部读取 (Read All)**，则 CDO 会警告您使用CDO对设备的配置进行了待处理的更改，并且继续执行读取操作将删除这些更改，然后覆盖CDO 的配置副本以及设备上的配置。此读取所有功能，例如放弃更改。

---

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** （可选）创建更改请求管理以便在更改日志中轻松识别此批量操作的结果。

**步骤 5** 选择要保存 CDO 配置的设备。请注意，CDO 仅提供可应用于所有选定设备的操作的命令按钮。

**步骤 6** 点击**全部读取 (Read All)**。

**步骤 7** 如果您选择的任何设备的 CDO 上有配置更改，CDO 会发出警告，并询问您是否要继续执行批量读取配置操作。点击**全部读取 (Read All)** 以继续。

**步骤 8** 查看作业页面以了解“全部读取”(Read All) 配置操作的进度。如果您想了解有关批量操作中各个操作是如何成功或失败的更多信息，请点击蓝色查看链接，您将被定向到作业页面 页面。

**步骤 9** 如果您创建并激活了更改请求标签，请记住将其清除，以免无意中将其他配置更改与此事件关联。

---

**相关信息**

- 读取、丢弃、检查和部署更改
- 放弃更改
- 检查配置更改

# 将 ASA 的配置更改读取到 CDO

**为什么 Cisco Defense Orchestrator 会“读取”ASA 配置？**

为了管理 ASA，CDO 必须拥有自己存储的 ASA 运行配置文件副本。CDO 首次读取并保存设备配置文件的副本是在设备载入时。随后，当 CDO 从 ASA 读取配置时，您将选择**检查更改 (Check for Changes)**、**接受而不审核 (Accept without Review)** 或**读取配置 (Read Configuration)**。有关详细信息，请参阅读取、丢弃、检查和部署更改。

在以下情况下，CDO 还需要读取 ASA 配置：

- 将配置更改部署到 ASA 失败，并且设备状态未列出或**未同步 (Not Synced)**。
- 载入设备失败，设备状态为“未配置”。
- 您已在 CDO 之外对设备配置进行了更改，但尚未轮询或检测到这些更改。设备状态为“已同步”或“已检测到冲突”。

在这些情况下，CDO 需要存储在设备上的最后一个已知配置的副本。

## 读取 ASA 上的配置更改

当系统提示读取 ASA 上的配置更改时：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择 CDO 最近未能载入的设备或 CDO 未能将更改部署到的设备。

**步骤 5** 点击右侧“已同步”窗格中的**读取配置**。此选项会覆盖当前保存到 CDO 的配置。

# 预览和部署所有设备的配置更改

当您对租户上的设备进行了配置更改，但您尚未部署该更改时，CDO 会通过在部署图标上显示一个橙色点来通知您

。受这些更改影响的设备在设备和**服务 (Services)** 页面中显示“未同步”(Not Synced) 状态。通过点击**部署 (Deploy)**，您可以查看哪些设备具有待处理的更改，并将更改部署到这些设备。

注释 对于您创建和更改的每个新 FDM 或 FTD 网络对象或组，CDO 会在此页面中为 CDO 管理的所有 本地管理中心 创建一个条目。

此部署方法适用于所有受支持的设备。

您可以将此部署方法用于单个配置更改，也可以等待并一次部署多个更改。

**步骤 1** 在屏幕的右上角，点击**部署 (Deploy)** 图标 。

**步骤 2** 选择要部署更改的设备。如果设备有黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在黄色警告三角形上，了解无法将更改部署到该设备的原因。

**步骤 3** （可选）如果要查看有关待处理更改的更多信息，请点击**查看详细更改日志 (View Detailed Changelog)** 链接以打开与该更改关联的更改日志。点击**部署 (Deploy)** 图标可返回**具有待处理更改的设备 (Devices with Pending Changes)** 页面。

**步骤 4** （可选）更改请求管理以跟踪更改，而无需离开**具有待处理更改的设备 (Devices with Pending Changes)** 页面。

**步骤 5** 点击**立即部署 (Deploy Now)**，立即将更改部署到您选择的设备。您将在“作业”(Jobs) 托盘的“活动作业”(Active jobs) 指示器中看到进度。

**步骤 6** （可选）部署完成后，点击 CDO 导航栏中的**作业 (Jobs)**。您将看到最近的“部署更改”(Deploy Changes) 作业，其中显示了部署的结果。

**步骤 7** 如果您创建了更改请求标签，并且没有其他配置更改与之关联，请将其清除。

### 下一步做什么

- 已计划的自动部署
- 将配置更改从 CDO 部署到 ASA，第 314 页
- 部署到 ASA 后的更改日志条目，第 331 页

# 将配置更改从 CDO 部署到 ASA

### 为什么 CDO 会将更改部署到 ASA?

当您使用 Cisco Defense Orchestrator (CDO) 管理和更改设备配置时，CDO 会将您所做的更改保存到自己的配置文件副本中。在“部署”到设备之前，这些更改将被视为已在CDO上“暂存”。暂存配置更改对通过设备运行的网络流量没有影响。只有在CDO将更改“部署”到设备后，它们才会影响通过设备运行的流量。当CDO将更改部署到设备的配置时，它只会覆盖已更改的配置元素。它不会覆盖设备上存储的整个配置文件。

ASA 有一个“运行”的配置文件（有时称为“运行配置”）和一个“启动”配置文件（有时称为“启动配置”）。对通过ASA的流量会强制执行运行配置文件中存储的配置。对运行配置进行更改

并对这些更改产生的行为感到满意后，您可以将其部署到启动配置。如果ASA重新启动，它会使用启动配置作为其配置起点。重新启动ASA后，您对运行配置所做的任何未保存到启动配置的更改都将丢失。

在将更改从 CDO 部署到 ASA 时，这些更改会被写入运行配置文件。在对这些更改产生的行为感到满意后，您就可以将这些更改部署到启动配置文件。

部署可以为单个设备或同时在多个设备上启动。您可以为单个设备安排单独的部署或定期部署。

### 某些更改会被直接部署到 ASA

如果您在 CDO 上使用 CDO 命令行界面 命令行界面宏接口来对 ASA 进行更改，则这些更改不会被“暂存”在 CDO 上。它们会被直接部署到 ASA 的运行配置中。在以这种方式进行更改时，您的设备会与 CDO 保持“同步”。

# 关于部署配置更改

本部分假定您使用 CDO 的 GUI 或编辑“设备配置”页面，而不是使用 CDO 的 CLI 界面或 CLI 宏界面对 ASA 配置文件进行更改。

更新 ASA 配置的过程分为两步。

**步骤 1** 使用以下方法之一对 CDO 进行更改：

- CDO GUI
- “设备配置”页面上的设备配置

**步骤 2** 进行更改后，返回到**清单 (Inventory)** 页面，然后选择**预览并部署... (Preview and Deploy...)**以预览并部署更改到设备。

### 下一步做什么

当 CDO 使用暂存在 CDO 上的运行配置更新 ASA 的运行配置时，或者当它使用存储在 ASA 上的运行配置更改CDO上的配置时，它会尝试仅更改配置文件的相关行，前提是配置的该方面可以由CDO GUI 管理。如果无法使用 CDO GUI 进行所需的配置更改，CDO 会尝试覆盖整个配置文件以进行更改。

以下是两个示例：

- 您可以使用 CDO GUI 创建或更改网络对象。如果 CDO 需要将该更改部署到 ASA 的配置，则会在发生更改时覆盖 ASA 上正在运行的配置文件的相关行。
- 您**无法**使用 CDO GUI 创建新的本地 ASA 用户，但可以通过编辑“设备配置”(Device Configuration) 页面上的ASA配置来创建本地用户。如果您在“设备配置”页面上添加用户，并将该更改部署到 ASA，CDO 将通过覆盖整个运行配置文件来尝试将该更改保存到 ASA 的运行配置文件。

# 部署使用 CDO GUI 进行的配置更改

**步骤 1** 在使用 CDO GUI 进行配置更改并保存更改后，该更改将保存在 ASA 的运行配置文件的 CDO 存储版本中。

**步骤 2** 返回**清单 (Inventory)** 页面上的设备。

**步骤 3** 点击设备选项卡。您应该会看到设备现在处于“未同步”(Not synced) 状态。

**步骤 4** 使用以下方法之一部署更改：

- 点击屏幕右上角的**部署 (Deploy)** 图标  。这使您有机会在部署之前查看对设备进行的更改。检查您所做更改的设备，展开设备以查看更改，点击**立即部署 (Deploy Now)** 以部署更改。

  **注释** 如果在“有待处理更改的设备”(Devices with Pending Changes) 屏幕上看到设备旁边显示黄色警告三角形，则无法部署更改。将鼠标悬停在警告三角形上，了解无法将更改部署到设备的原因。

- 在未同步窗格中，点击**预览并部署... (Preview and Deploy...)**。

  1. 查看将更改 ASA 配置文件的命令。
  2. 如果您对命令感到满意，请选择“配置恢复首选项”(Configuration Recovery Preference)。

     **注释** 如果您选择“告诉我，我将手动恢复配置”(Let me know and I will restore the configuration manually)，请在继续之前点击**查看手动同步说明 (View Manual Synchronization Instructions)**。

  3. 点击**将更改应用到设备 (Apply Changes to Device)**。
  4. 点击成功消息中的**确定 (OK)**。

# 计划自动部署

您还可以配置租户，通过计划自动部署来将部署安排到具有待定更改的单个设备或所有设备。

# 使用 CDO 的 CLI 界面部署配置更改

**步骤 1** 在导航窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择要更改其配置的设备。

**步骤 5** 在**操作 (Actions)** 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

**步骤 6** 如果命令行界面表中有任何命令，请点击清除以将其删除。

**步骤 7** 在命令行界面表的顶部框中，在命令提示符下输入命令。您可以运行单个命令，也可以通过在其自己的行中输入每个命令或输入配置文件的一部分作为命令来运行批处理中的多个命令。以下是您可以在命令行界面表中输入的一些命令示例：

创建网络对象“albany”的单个命令

```
object network albany
host 209.165.30.2
```

多个命令一起发送：

```
object network albany
host 209.165.30.2
object network boston
host 209.165.40.2
object network cambridge
host 209.165.50.2
```

作为命令输入的运行配置文件的一部分：

```
interface GigabitEthernet0/5
 nameif guest
 security-level 0
 no ip address
```

**注释** CDO 不要求您在 EXEC 模式、特权 EXEC 模式和全局配置模式之间切换。它会解释您在适当的上下文中输入的命令。

**步骤 8** 输入命令后，点击发送。在 CDO 成功部署对 ASA 的运行配置文件的更改后，您会收到消息“完成！”(Done!)。

**步骤 9** 发送命令后，您可能会看到消息“某些命令可能已对运行配置进行了更改”(Some commands may have made changes to the running config) 以及两个链接。

- 点击**部署到磁盘 (Deploy to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到 ASA 的启动配置中。
- 点击**消除 (Dismiss)**，可关闭消息。

# 通过编辑设备配置部署配置更改

⚠

**注意** 此程序适用于熟悉 ASA 配置文件语法的高级用户。此方法直接更改存储在 CDO 上的运行配置文件。

**步骤 1** 在导航窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择要更改其配置的设备。

**步骤 5** 点击操作窗格中的查看配置。

**步骤 6** 点击**编辑**。

**步骤 7** 对运行配置进行更改并保存。

**步骤 8** 返回**清单 (Inventory)** 页面。在未同步窗格中，点击**预览并部署... (Preview and Deploy...)**。

**步骤 9** 在设备同步窗格中，查看更改。

**步骤 10** 根据更改的类型，点击替换配置或将更改应用到设备。

# 在多个设备上部署共享对象的配置更改

对两台或多台设备共享的策略或对象进行更改时，请使用此程序。您可以在许多设备上更改通用策略。

**步骤 1** 打开并编辑包含要编辑的共享对象的策略页面或对象页面。

**步骤 2** 查看共享设备列表，并确认要对提及的所有设备进行更改。

**步骤 3** 点击 **Confirm**。

**步骤 4** 点击**保存 (Save)**。

**步骤 5** 点击**部署**图标 并预览和部署所有设备的配置更改。

# 批量部署设备配置

如果您对多个设备进行了更改（例如通过编辑共享对象），则可以一次将这些更改应用到所有受影响的设备：

**步骤 1** 在导航窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择已在 CDO 上进行配置更改的所有设备。这些设备应显示“未同步”(Not Synced) 状态。

**步骤 5** 使用以下方法之一部署更改：

- 点击屏幕右上角的 按钮可查看**有待处理更改的设备 (Devices with Pending Changes)** 窗口。这使您有机会在部署之前查看所选设备上的待处理更改。点击**立即部署 (Deploy Now)** 以部署更改。

  **Note** 如果在**有待处理更改的设备 (Devices with Pending Changes)** 屏幕上看到某个设备旁边显示黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在警告三角形上，了解有关无法将更改部署到该设备的信息。

- 点击详细信息窗格中的**全部部署 (Deploy All)** 。查看所有警告，然后点击**确定 (OK)**。批量部署会立即开始，无需审核更改。

**步骤 6** （可选）点击导航栏中的“作业”(Jobs) 图标  以查看批量部署的结果。

**相关信息：**

- 计划自动部署, on page 319

# 已计划的自动部署

通过使用CDO，您可以对其管理的一个或多个设备进行配置更改，然后安排在您方便的时间将更改部署到这些设备。

只有您在“设置”(Settings) 页面的**租户设置 (Tenant Settings)** 选项卡中 启用计划自动部署的选项, on page 39 才能安排部署。一旦启用此选项，您就可以创建、编辑或删除计划部署。计划的部署会在设置的日期和时间部署在 CDO 上保存的所有暂存更改。您还可以在“作业”(Jobs) 页面中查看和删除计划部署。

如果直接对设备进行了尚未读取、丢弃、检查和部署更改到CDO的更改，则将跳过计划的部署，直到该冲突得以解决。“作业”(Jobs) 页面将列出计划部署失败的所有实例。如果**启用计划自动部署的选项 (Enable the Option to Schedule Automatic Deployments)** 被关闭，则所有计划的部署都将被删除。

**Caution** 如果您为多台设备安排新的部署，并且其中一些设备已安排了部署，则新的安排部署将覆盖现有的安排部署。

**Note** 当您创建计划部署时，将按照本地时间来创建计划，而不是设备的时区。计划的部署不会自动调整夏令时。

## 计划自动部署

部署计划可以是单个事件或周期性事件。您可能会发现定期自动部署是一种将定期部署与维护窗口对齐的便捷方式。请按照以下程序为单个设备安排一次性或周期性部署：

**Note** 如果为已安排现有部署的设备安排部署，新的安排部署将覆盖现有部署。

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备。

**步骤 5** 在设备详细信息窗格中，找到计划的部署选项卡，然后点击**计划 (Schedule)**。

**步骤 6** 选择应进行部署的时间。

- 对于一次性部署，请点击**一旦开启 (Once on)** 选项以从日历中选择日期和时间。
- 对于周期性部署，请点击**每次 (Every)** 选项。您可以选择每天或每周一次部署。选择部署的**日期 (Day)** 和**时间 (Time)**。

**步骤 7** 点击**保存 (Save)**。

# 编辑计划部署

请按照以下程序编辑计划部署：

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备。

**步骤 5** 在**设备详细信息 (Device Details)** 窗格中，找到计划的部署选项卡，然后点击**编辑 (Edit)**。

**步骤 6** 编辑计划部署的重复周期、日期或时间。

**步骤 7** 点击**保存 (Save)**。

# 删除计划部署

请按照以下程序删除计划部署：

**Note** 如果为多台设备安排部署，然后更改或删除某些设备的安排，则其余设备的原始安排部署将保留。

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Services)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择一个或多个设备。

**步骤 5** 在**设备详细信息 (Device Details)** 窗格中，找到计划的部署选项卡，然后点击**删除 (Delete)** 。

### What to do next

- 读取、丢弃、检查和部署更改
- 读取所有设备配置, on page 312
- 将配置更改从 CDO 部署到 ASA, on page 314
- 预览和部署所有设备的配置更改, on page 313

# 检查配置更改

**检查更改**以确定设备的配置是否已直接在设备上更改，并且它不再与CDO上存储的配置副本相同。当设备处于“已同步”(Synced) 状态时，您将看到此选项。

要检查更改，请执行以下操作：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择您怀疑其配置可能已直接在设备上更改的设备。

**步骤 5** 点击右侧“已同步”(Synced) 窗格中的**检查更改 (Check for Changes)**。

**步骤 6** 以下行为因设备而有细微差别：

- 对于 设备，如果设备的配置发生变化，您将收到以下消息：

  从设备读取策略。如果设备上有活动的部署，则将在完成后开始读取。

  - 点击 **OK** 继续操作。设备上的配置将覆盖 CDO 上存储的配置。
  - 点击**取消 (Cancel)** 以取消操作。

- 对于 ASA 设备：

**a.** 比较呈现给您的两种配置。点击**继续**。标记为**最后已知的设备配置 (Last Known Device Configuration)** 的配置是存储在 CDO 上的配置。标记为 **在设备上找到 (Found on Device)** 的配置是保存在 ASA上的配置。

**b.** 选择以下选项中的一种：

1. **拒绝**带外更改以保留“最后已知的设备配置”(Last Known Device Configuration)。
2. **接受**带外更改，以使用设备上找到的配置来覆盖 CDO 中存储的设备配置。

**c.** 点击**继续**。

# 放弃更改

如果要“撤消”使用 CDO 对设备配置所做的所有未部署的配置更改，请点击**放弃更改 (Discard Changes)**。在点击**放弃更改 (Discard Changes)** 时，CDO 会使用设备上存储的配置完全覆盖设备配置的本地副本。

点击**放弃更改 (Discard Changes)** 时，设备的配置状态为**未同步 (Not Synced)**。在放弃更改后，CDO 上的配置副本将与设备上的配置副本相同，CDO 中的配置状态将恢复为“已同步”(Synced)。

要放弃或“撤消”设备的所有未部署的配置更改，请执行以下操作：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备 (Devices)** 选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择您已对其进行配置更改的设备。

**步骤 5** 点击右侧**未同步 (Not Synced)** 窗格中的**放弃更改 (Discard Changes)**。

- 对于 FDM 管理 设备，CDO 会警告您“CDO 上的待处理更改将被丢弃，此设备的 CDO 配置将替换为设备上当前运行的配置”(Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device)。点击**继续 (Continue)** 以放弃更改。
- 对于 Meraki 设备 - CDO 会立即删除更改。
- 对于 AWS 设备 - CDO 会显示您要删除的内容。点击**接受 (Accept)** 或**取消 (Cancel)**。

# 设备上的带外更改

带外更改是指在不使用 CDO 的情况下直接在设备上进行的更改。这些更改可以通过 SSH 连接使用设备的命令行界面，或使用本地管理器（如适用于 ASA 的自适应安全设备管理器 (ASDM)、适用于 FDM 管理 管理设备的 FDM 或 本地防火墙管理中心 用户界面上的 本地防火墙管理中心）来进行。带外更改会导致 CDO 上存储的设备配置与设备本身上存储的配置之间发生冲突。

### 检测设备上的带外更改

如果为 ASA、FDM 管理 设备、Cisco IOS 设备或 本地防火墙管理中心 启用了冲突检测，则 CDO 会每 10 分钟检查一次设备，以搜索在 CDO 之外直接对设备配置进行的任何新更改。

如果 CDO 发现未存储在 CDO 上的设备配置更改，则会将该设备的**配置状态**更改为“检测到冲突”状态。

当 Defense Orchestrator 检测到冲突时，可能出现以下两种情况：

- 直接对设备进行的配置更改尚未保存到 CDO 的数据库中。
- 对于 FDM 管理 设备，FDM 管理 设备上可能存在尚未部署的“待处理”配置更改。
- 对于 本地防火墙管理中心，可能会对 CDO 外部的对象进行更改，而这些更改会等待与 CDO 同步，或者在 CDO 中进行的更改等待部署到 本地防火墙管理中心。

# 同步 Defense Orchestrator 和设备之间的配置

### 关于配置冲突

在**清单 (Inventory)** 页面上，您可能会看到设备或服务的状态为“已同步”(Synced)、“未同步”(Not Synced) 或“检测到冲突”(Conflict Detected)。要了解使用 CDO 管理的 本地防火墙管理中心 的状态，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

- 如果设备为**已同步 (Synced)**， Cisco Defense Orchestrator (CDO) 上的配置与设备本地存储的配置相同。
- 如果设备为**未同步 (Not Synced)**，CDO 中存储的配置已更改，现在存储在设备上的配置有所不同。将您的更改从 CDO 部署到设备会更改设备上的配置以匹配 CDO 的版本。
- 在 CDO 之外对设备进行的更改称为**带外更改**。进行带外更改时，如果为设备启用了冲突检测，您会看到设备状态更改为“检测到冲突”(Conflict Detected)。接受带外更改会更改 CDO 上的配置以匹配设备上的配置。

# 冲突检测

启用冲突检测后， Cisco Defense Orchestrator (CDO) 将按默认间隔轮询设备，以确定是否在 CDO 之外对设备配置进行了更改。如果 CDO 检测到已进行更改，则会将设备的配置状态更改为**检测到冲突 (Conflict Detected)**。在 CDO 之外对设备进行的更改称为“带外”更改。

对于由 CDO 管理的 本地防火墙管理中心 ，如果存在已暂存的更改且设备处于**未同步 (Not Synced)** 状态，则 CDO 会停止轮询设备以检查更改。当在 CDO 外部进行的更改等待与 CDO 同步，而在 CDO 中进行的更改等待部署到 本地管理中心 时，CDO 会声明 本地管理中心 处于**检测到冲突 (Conflict Detected)** 状态。

启用此选项后，您可以配置每台设备检测冲突或 OOB 更改的频率。有关详细信息，请参阅安排设备更改轮询, on page 326。

# 启用冲突检测

启用冲突检测会提醒您在 Defense Orchestrator 之外对设备进行更改。

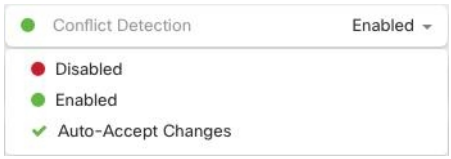
**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 选择适当的设备类型选项卡。

**步骤 4** 选择要启用冲突检测的设备。

**步骤 5** 在设备表右侧的冲突检测框中，从列表中选择已启用。




# 自动接受设备的带外更改

您可以通过启用自动接受更改，将 Cisco Defense Orchestrator (CDO) 配置为自动接受直接对受管设备所做的任何更改。不使用 CDO 直接对设备进行的更改称为带外更改。带外更改会在 CDO 上存储的设备配置与设备本身上存储的配置之间产生冲突。

自动接受更改功能是对冲突检测的增强。如果您在设备上启用了自动接受更改，CDO 会每 10 分钟检查一次更改，以确定是否对设备的配置进行了任何带外更改。如果配置发生更改，CDO 会自动更新其本地版本的设备配置，而不会提示您。

如果对 CDO 进行的配置更改尚未部署到设备，则 CDO **不**会自动接受配置更改。按照屏幕上的提示确定下一步操作。

要使用自动接受更改，请先启用租户，以在**清单 (Inventory)** 页面中显示自动接受选项；然后，您可以为单个设备启用自动接受更改。

如果您希望 CDO 检测带外更改，但为您提供手动接受或拒绝更改的选项，请改为启用 冲突检测, on page 323。

# 配置自动接受更改

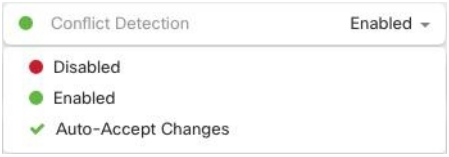
**步骤 1** 使用具有管理员或超级管理员权限的帐户登录 CDO。

**步骤 2** 从 CDO 菜单中，导航至 **设置 (Settings)** > **常规设置 (General Settings)**。

**步骤 3** 在租户设置区域中，点击切换按钮以启用“自动接受设备更改的选项”。这将使“自动接受更改”菜单选项显示在**清单 (Inventory)** 页面的“冲突检测”菜单中。

**步骤 4** 打开**清单 (Inventory)** 页面，然后选择要自动接受带外更改的设备。

**步骤 5** 在“冲突检测”(Conflict Detection) 菜单中，选择下拉菜单中的“自动接受更改”(Auto-Accept Changes)。




# 为租户上的所有设备禁用自动接受更改

**步骤 1** 使用具有管理员或超级管理员权限的帐户登录 CDO。

**步骤 2** 从 CDO 菜单中，导航至 **设置 (Settings)** > **常规设置 (General Settings)**

**步骤 3** 在“租户设置”区域中，通过将切换开关向左滑动来禁用“启用自动接受设备更改的选项”，使其显示灰色 X。这将禁用“冲突检测”菜单中的“自动接受更改”选项，并为以下项禁用此功能：租户上的每台设备。

**Note** 禁用“自动接受”将要求您查看每个设备冲突，然后才能将其接受到CDO中。这包括之前配置为自动接受更改的设备。

# 解决配置冲突

本节提供有关解决设备上发生的配置冲突的信息。

## 解决“未同步”状态

使用以下程序解决配置状态为“未同步”的设备：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**Note** 对于 本地防火墙管理中心，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 并选择处于**未同步 (Not Synced)** 状态的 FMC，然后从步骤 5 继续操作。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择报告为“未同步”的设备。

**步骤 5** 在右侧的未同步面板中，选择以下任一选项：

- **预览并部署...** - 如果要将配置更改从 CDO 推送到设备，请预览并部署您现在所做的更改，或者等待并一次部署多个更改。预览和部署所有设备的配置更改, on page 313

- 放弃更改 - 如果您不想将配置更改从 CDO 推送到设备，或者您想要“撤消”您开始在 CDO 上进行的配置更改。此选项使用设备上存储的运行配置覆盖 CDO 中存储的配置。

# 解决“检测到冲突”状态

CDO 允许您在每个实时设备上启用或禁用冲突检测。如果 冲突检测, on page 323 已启用，并且在未使用 CDO 的情况下对设备的配置进行了更改，则设备的配置状态将显示为**检测到冲突 (Conflict Detected)**。

要解决“检测到冲突”(Conflict Detected) 状态，请执行以下程序：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**Note** 对于 本地防火墙管理中心，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 并选择处于**检测到冲突 (Conflict Detected)** 状态的 FMC，然后从步骤 4 继续操作。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择报告冲突的设备，然后点击右侧详细信息窗格中的**查看冲突 (Review Conflict)**。

**步骤 5** 在**设备同步 (Device Sync)** 页面中，通过查看突出显示的差异来比较两种配置。

- 标记为“最后一次设备配置”(Last Known Device Configuration) 的面板是存储在 CDO 上的设备配置。
- 标记为“在设备上找到”(Found on Device) 的面板是存储在运行 ASA 配置中的配置。

**步骤 6** 通过选择以下选项之一来解决冲突：

- **接受设备更改 (Accept Device changes)**：这将使用设备的运行配置覆盖 CDO **上存储的配置** 和任何待处理的更改。

  **Note** 由于 CDO 不支持在命令行界面之外部署对Cisco IOS 设备的更改，因此在解决冲突时，您对Cisco IOS 设备的唯一选择是选择**接受而不查看 (Accept Without Review)**。

- **拒绝设备更改 (Reject Device Changes)**：这将使用存储在 CDO 上的配置覆盖设备上存储的配置。

**Note** 所有配置更改（拒绝或接受）都记录在更改日志中。

# 安排设备更改轮询

如果已启用 冲突检测, on page 323 或从“设置”(Settings) 页面 **启用自动接受设备更改的选项 (Enable the option to auto-accept device changes)**，则 CDO 将按默认间隔轮询设备，以确定是否在 CDO 之

外对设备配置进行了更改。您可以自定义CDO轮询每台设备更改的频率。这些更改可以应用于多个设备。

如果没有为设备配置选择，则会自动为“租户默认”配置间隔。

**Note** 从**设备和服务 (Devices & Services)** 页面自定义每台设备的间隔会覆盖从**常规设置 (General Settings)** 页面选择作为默认冲突检测间隔 的轮询间隔。

从**设备和服务 (Devices & Services)** 页面启用**冲突检测 (Conflict Detection)** 或从“设置”(Settings) 页面选择**启用该选项以自动接受设备更改 (Enable the option to auto-accept device changes)** 后，请使用以下程序来安排您希望 CDO 轮询设备的频率：

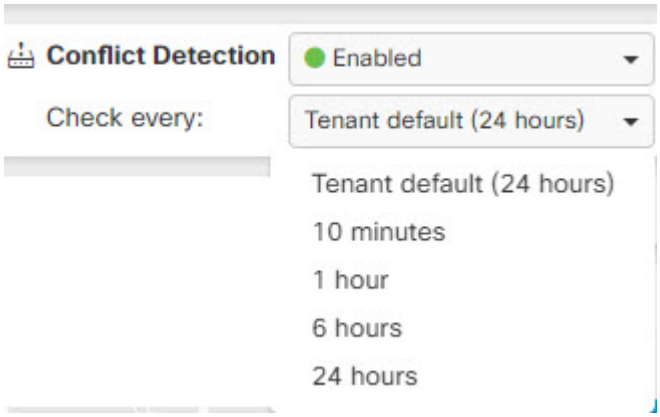
**步骤 1** 在导航栏中，点击 **设备和服务**。

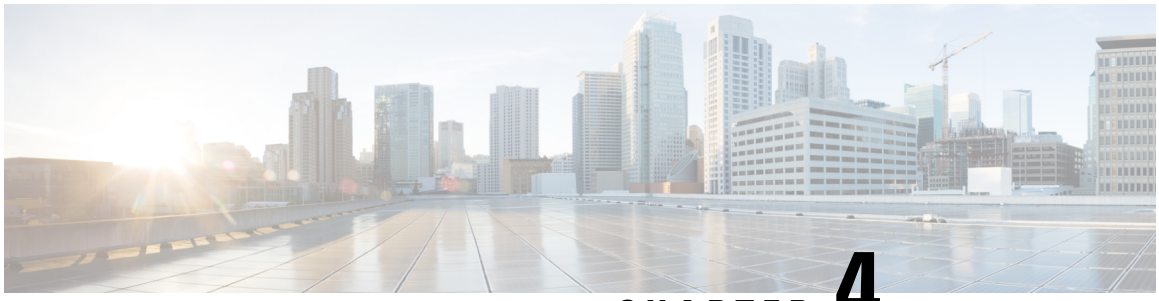
**步骤 2** 点击 **设备** 选项卡，找到您的设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择要启用冲突检测的设备。

**步骤 5** 在与**冲突检测 (Conflict Detection)** 相同的区域中，点击**检查间隔 (Check every)** 下拉菜单，然后选择所需的轮询间隔：





CHAPTER 4

# 监控和报告

CDO 的监控和报告功能可帮助您深入了解现有策略的影响以及由此产生的安全状况。



# 变更日志

### 关于更改日志

更改日志 会持续捕获在 CDO 中进行的配置更改。此单一视图包括所有受支持设备和服务的更改。以下是更改日志的一些功能：

- 并排比较对设备配置所做的更改。
- 所有更改日志条目的纯英文标签。
- 记录设备的载入和删除。
- 检测在 CDO 之外发生的策略更改冲突。
- 回答事件调查或故障排除期间的人员、内容和时间。
- 可以将完整更改日志或仅一部分下载为 CSV 文件。

### 更改日志容量

CDO 会将更改日志中的信息保留一年。超过一年的信息将被删除。

CDO 在其数据库中存储的更改日志信息与导出更改日志时看到的信息之间存在差异。有关详细信息，请参阅将更改日志导出到 CSV 文件, on page 333。

### “更改日志”(Change Log) 页面上的更改日志条目

更改日志条目反映对单个设备配置的更改、在设备上执行的操作，或者是否在CDO之外对设备进行了更改。

- 对于包含配置更改的更改日志条目，您可以通过点击行中的任意位置来展开更改。
- 对于在 CDO 之外进行的被检测为冲突的带外更改，**系统用户**将被报告为最后一个用户。
- 在CDO上的设备配置与设备上的配置同步后，或从CDO中删除设备时，CDO会关闭更改日志条目。将配置从设备“读取”到 CDO 或通过将配置从 CDO 部署到设备后，配置会同步。
- CDO在关闭现有条目后立即创建新的更改日志条目。其他配置更改将添加到打开的更改日志条目中。
- 显示针对设备的读取、部署和删除操作的事件。这些操作会关闭设备的更改日志。
- 一旦 CDO 与设备上的配置同步（通过读取或部署），或者当 CDO 不再管理设备时，更改日志就会关闭。
- 如果在 CDO 之外对设备进行了更改，则会在更改日志中写入“检测到冲突”的条目。

### 活动和已完成的更改日志条目

更改日志的状态为 **活动**或**已完成**。当您使用 CDO 更改设备的配置时，这些更改会记录在**活动**更改日志条目中。将配置从设备读取到CDO、将更改从CDO部署到设备、从CDO删除设备或运行更新运行配置文件的 CLI 命令都会完成活动更改日志，并为未来的更改创建新的更改日志。

下图显示的是 ASA 中的**活动**更改日志条目。请注意左侧时间戳旁边的空心圆圈。


### 在更改日志中查找条目

更改日志事件可搜索和过滤。使用搜索栏查找与关键字匹配的事件。使用过滤器 以查找符合您指定的所有条件的条目。您还可以通过过滤更改日志并将关键字添加到搜索字段来组合操作，以在过滤后的结果中查找条目。

# ASA 更改日志详细信息

有关 ASA 更改日志条目的说明，请参阅以下文章：



# 部署到 ASA 后的更改日志条目

以下是对更改日志条目的说明。条目左上角带有复选标记的绿色圆圈表示更改日志已完成。更改日志会按从新到旧的顺序显示条目，并对条目内的更改进行排序。

如果点击更改日志条目行中的蓝色查看更改日志差异 链接，则会在运行配置文件的上下文中并排对比显示更改。

请参阅下面对不同更改的说明。


| 图中的数字 | 说明 |
|---|---|
| 1 | 这是 admin@example.com 在 2018 年 9 月 11 日上午 10:03:59 所做的更改。<br>**1.** 添加了“HR_network”对象。<br>**2.** 将初始网络地址 (10.10.11.0) 和子网掩码 (255.255.255.0) 添加到了 HR_network 对象。<br>**3.** 在“engineering_access”网络策略中添加了一条规则，拒绝“engineering”网络中的地“HR_network” |
| 2 | 运行配置文件的校验和已由 ASA 重新计算并更改。旧值已被删除，而新值已被添加。 |

| 图中的数字 | 说明 |
| --- | --- |
| 3 | ASA 会将对象移至运行配置文件中的其他位置，而不是 Defense Orchestrator 放置该对象的位<br>**Note** 您不会始终看到这种条目。 |
| 4 | 上次更新运行配置文件的记录。旧时间戳被删除，新时间戳被添加。此更改由 ASA 进行。 |
| 5 | 这些是由防御协调器送到 ASA 进行配置更改的命令。 |

# 从 ASA 读取更改后的更改日志条目

当 Cisco Defense Orchestrator (CDO) 在其管理的 ASA 上检测到更改时，它会打开一个更改日志条目并记录检测到配置冲突的时间。当 CDO 检测到冲突时，您可以看到以下更改日志条目：


如果您接受更改，或查看并接受更改，则该更改将添加到更改日志条目中，并且该条目已完成。


此条目显示检测到的冲突 (Conflict Detected) 更改以及阻止工程网络中的地址到达 HR_network 的规则的删除。更改日志条目还显示带有消息“已成功导入带外更改”的更改。如果管理员已选择拒绝带外更改，则更改日志将显示消息“已成功拒绝设备上的带外更改”以及被拒绝的内容。带外更改是指在不使用 CDO 的情况下直接在 ASA 设备上进行的更改。

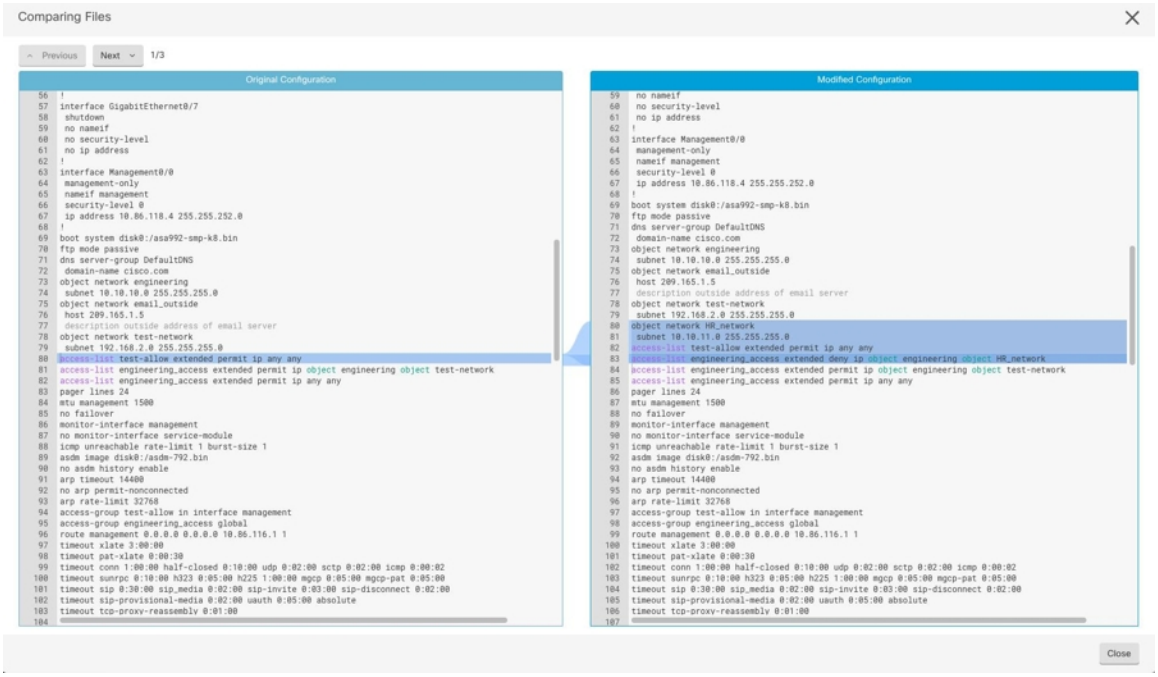
### 相关主题

- 变更日志, on page 329
- 部署到 ASA 后的更改日志条目, on page 331
- 查看更改日志差异, on page 333
- 读取、丢弃、检查和部署更改

# 查看更改日志差异

点击更改日志中的蓝色“差异”(Diff)链接，可以并排比较设备的运行配置文件中的更改。您会看到两个版本的差异。

在下图中，“原始配置”(Original Configuration) 是更改写入之前的运行配置文件，“修改后的配置”(Modified Configuration) 列显示更改写入 ASA 后的运行配置文件。在这种情况下，原始配置列会突出显示运行配置文件中实际未更改的行，但会在修改后的配置列中提供参考点。按照从左到右列的行，您会看到添加了 HR_network 对象和访问规则，以防止“工程”网络中的地址访问“HR_network”网络中的地址。点击**上一个 (Previous)** 和**下一个 (Next)** 按钮浏览文件中的更改。




**相关主题**

- 变更日志, on page 329

# 将更改日志导出到 CSV 文件

您可以将 CDO 更改日志的全部或子集导出到逗号分隔值 (.csv) 文件，以便您可以随意过滤和排序其中的信息。

要将更改日志导出到 .csv 文件，请执行以下程序：

**步骤 1** 在导航窗格中，点击 **更改日志**。

**步骤 2** 通过执行以下操作之一查找要导出的更改：

- 使用过滤器 字段和搜索字段准确查找要导出的内容。例如，按设备过滤以仅查看所选设备的更改。
- 清除更改日志中的所有过滤器和搜索条件。这允许您导出整个更改日志。

**Note** 请记住，CDO 会存储 1 年的更改日志数据。最好是过滤更改日志内容并将结果下载到 .csv 文件，而不是下载长达一年的更改日志历史记录。

**步骤 3** 点击更改日志右上角的蓝色导出按钮  。

**步骤 4** 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。

# CDO 中的更改日志容量与导出的更改日志大小之间的差异

您从 CDO 的更改日志页面导出的信息与 CDO 存储在其数据库中的更改日志信息不同。

对于每个更改日志，CDO 会存储设备配置的两个副本，即“开始”配置和“结束”配置（如果更改日志已关闭）；或“当前”配置（如果是打开的更改日志）。这允许 CDO 并排显示配置差异。此外，CDO 会跟踪并存储每个步骤的“更改事件”，包括进行更改的用户名、更改时间以及其他详细信息。

但是，导出更改日志时，导出的内容不包括配置的两个完整副本。它仅包括“更改事件”，这使得导出文件比 CDO 存储的更改日志小得多。

CDO 最多可存储 1 年的更改日志信息，其中包括配置的两个副本。

# 更改请求管理

变更请求管理 允许您将在第三方故障单系统中打开的变更请求及其业务理由与变更日志中的事件相关联。使用更改请求管理在 CDO 中创建更改请求，使用唯一名称进行标识，输入更改说明，并将更改请求与更改日志事件相关联。您可以稍后在更改日志中搜索更改请求名称。

**Note** 您可能还会在 CDO 中看到对变更请求跟踪的引用。变更请求跟踪和变更请求管理指的是相同的功能。

# 启用更改请求管理

启用更改请求跟踪会影响租户的所有用户。要启用更改请求跟踪，请执行以下程序：

**步骤 1** 从用户菜单中，选择“设置”(Settings)。

**步骤 2** 从用户菜单中，点击常规设置。

**步骤 3** 点击“更改请求跟踪”下的滑块。

确认后，您会在 Defense Orchestrator 界面的左下角看到 Change Request 工具栏，并在 Change Log 中看到 Change Request 下拉菜单。

# 创建更改请求

**步骤 1** 在任何 CDO 页面中，点击页面左下角的更改请求工具栏中的蓝色 + 按钮。

**步骤 2** 为更改请求指定名称和说明。让变更请求名称反映您的组织想要实施的变更请求标识符。使用说明字段描述更改的目的。

**Note** 更改请求的名称一旦创建便无法更改。

**步骤 3** 保存更改请求。

**Note** CDO 保存更改请求并将所有新更改与该更改请求名称关联，直到您禁用更改请求或清除更改请求工具栏中的更改请求信息。

# 将更改请求与更改日志事件关联

**步骤 1** 在导航窗格中，点击**更改日志 (Change Log)**。

**步骤 2** 展开更改日志以显示要与更改请求关联的事件。

**步骤 3** 在“更改请求”列中，点击事件的下拉菜单。请注意，最新的更改请求列在更改请求列表的顶部。

**步骤 4** 点击更改请求的名称，然后点击选择。

# 使用更改请求搜索更改日志事件

**步骤 1** 在导航窗格中，点击**更改日志 (Change Log)**。

**步骤 2** 在更改日志搜索字段中，输入更改请求的确切名称，以便查找与该更改请求关联的更改日志事件。CDO 突出显示具有完全匹配项的更改日志事件。

# 搜索更改请求

**步骤 1** 点击更改请求工具栏中的更改请求菜单。

**步骤 2** 开始键入您要搜索的更改请求名称或关键字。您将开始在更改请求列表的名称字段和说明字段中看到部分匹配的结果。

# 过滤器更改请求

过滤器托盘中有一个“更改请求”过滤器，可用于查找更改日志事件。

**步骤 1** 在“更改日志”页面左侧的过滤器托盘中，找到“更改请求”区域。

**步骤 2** 展开过滤器并开始在搜索字段中键入更改请求的名称。部分匹配开始显示在搜索字段下方。

**步骤 3** 选择更改请求名称，选中相应的复选框，然后在“更改日志”表中显示匹配项。CDO 突出显示具有完全匹配项的更改日志事件。

# 清除更改请求工具栏

清除更改请求工具栏可防止更改日志事件与现有更改请求自动关联。

**步骤 1** 选择更改请求工具栏中的更改请求菜单。

**步骤 2** 点击**清除**。更改请求菜单更改为“无”。

# 清除与更改日志事件关联的更改请求

**步骤 1** 在导航窗格中，点击 **更改日志**。

**步骤 2** 展开更改日志以显示要与更改请求取消关联的事件。

**步骤 3** 在“更改请求”列中，点击事件的下拉菜单。

**步骤 4** 点击**清除**。

# 删除更改请求

删除更改请求时，是将其从更改请求列表中删除，而不是从更改日志中删除。

**步骤 1** 点击更改请求工具栏中的更改请求菜单。

**步骤 2** 点击更改请求名称。

**步骤 3** 点击该行中的删除图标。

**步骤 4** 点击绿色复选标记以确认您要删除更改请求。

# 禁用更改请求管理

禁用更改请求管理会影响您账户的所有用户。要禁用变更请求管理，请执行以下程序：

**步骤 1** 从用户名菜单中，选择设置。

**步骤 2** 滑动更改请求跟踪下的按钮以显示灰色 X。

# 使用案例

这些使用案例假定您之前已按照上述说明启用了变更请求管理。

### 跟踪为解决外部系统中维护的故障单所做的防火墙更改

在此使用案例中，用户正在更改防火墙以解决在外部系统中维护的故障单。用户希望将这些防火墙更改导致的更改日志事件与更改请求相关联。请按照以下程序创建更改请求，并将更改日志事件与其关联。

1. 创建更改请求, on page 335。使用外部系统中的故障单名称或编号作为更改请求的名称。使用说明字段添加更改理由或其他相关信息。
2. 确保新的更改请求在更改请求工具栏中可见。
3. 进行防火墙更改。
4. 在导航窗格中，点击更改日志并查找与新更改请求关联的更改日志事件。
5. 清除更改请求工具栏, on page 336 完成后。

### 更改防火墙后手动更新单个更改日志事件

在此使用案例中，用户进行了防火墙更改以解决在外部系统中维护的故障单，但忘记使用更改请求管理功能将更改请求与更改日志事件相关联。用户希望返回更改日志，以使用故障单编号更新更改日志事件。请按照以下程序将更改请求与更改日志事件相关联。

1. 创建更改请求, on page 335。使用外部系统中的故障单名称或编号作为更改请求的名称。使用说明字段添加更改理由或其他相关信息。
2. 在导航窗格中，点击更改日志并搜索与防火墙更改关联的更改日志事件。
3. 将更改请求与更改日志事件关联, on page 335。
4. 完成后，清除更改请求工具栏。

### 搜索与更改请求关联的更改日志事件

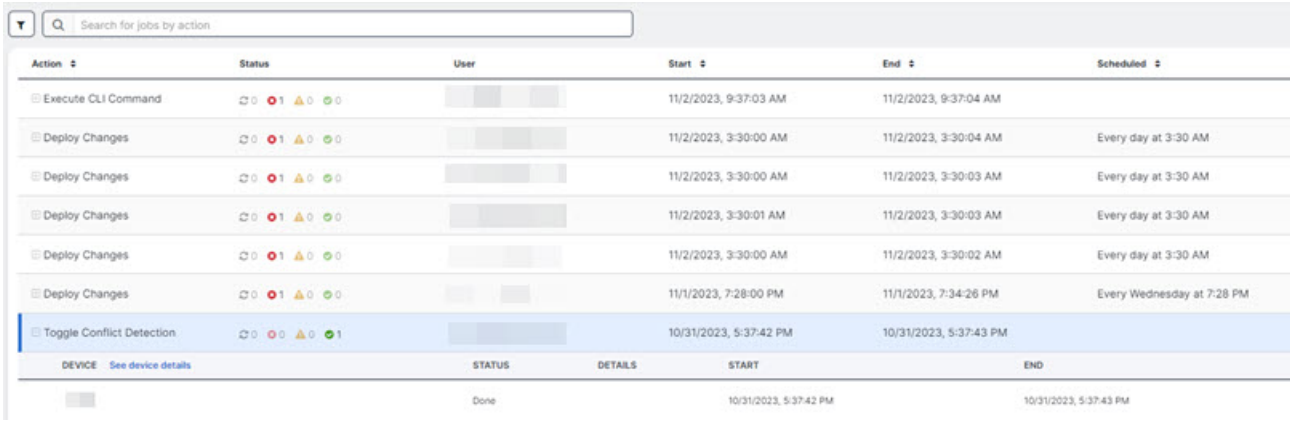
在此使用案例中，用户希望了解由于解决外部系统中维护的故障单而导致的更改日志中记录了哪些更改日志事件。请按照以下程序搜索与更改请求关联的更改日志事件：

1. 在导航窗格中，点击**更改日志 (Change Log)**。
2. 使用以下方法之一搜索与更改请求关联的更改日志事件。
   - 在更改日志搜索字段中，输入更改请求的确切名称，以便查找与该更改请求关联的更改日志事件。CDO 突出显示具有完全匹配项的更改日志事件。
   - 过滤器更改请求, on page 336 查找更改日志事件。
3. 查看每个更改日志，查找显示相关更改请求的突出显示的更改日志事件。

# 作业页面

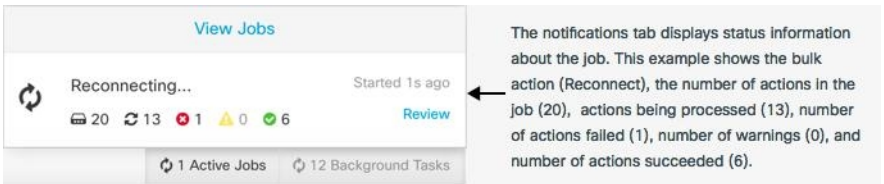
“作业”(Jobs)会页面显示有关批量操作状态的信息。批量操作可能是重新连接多个设备、从多个设备读取配置或同时升级多个设备。作业表中用颜色标记的行表示成功或失败的各个操作。

表中的一行代表一个批量操作。例如，该批量操作可能是尝试重新连接20台设备。展开“作业”(Jobs)页面中的一行，将显示受批量操作影响的每个设备的结果。




您可以通过两种不同的方式访问“作业”(Jobs) 页面：

- 在当通知选项卡有新作业中，点击通知行中的**查看 (Review)** 链接。您将被重定向到“作业”(Jobs)页面，并查看该通知所代表的特定作业。




- 从 CDO 的菜单中，选择**作业 (Jobs)**。此表显示了在 CDO 中执行的批量操作的完整列表。

### 搜索和过滤

进入“作业”(Jobs) 页面后，您可以按操作类型、执行这些操作的用户以及操作状态进行过滤和搜索。

## 重新启动导致操作失败的批量操作

查看“作业”(Jobs) 页面时，如果发现批量操作中的一个或多个操作失败，则可以在进行任何必要的更正后重新运行批量操作。CDO将仅对失败的操作重新运行作业。要重新运行批量操作，请执行以下操作：

**步骤 1** 选择作业页面中指示失败操作的行。

**步骤 2** 点击“作业”(Job) 行上的重新启动 **重试**图标。

## 取消批量操作

现在，您可以取消在多台设备上执行的任何活动批量操作。例如，假设您已尝试重新连接四台受管设备，其中三台设备已成功重新连接，但第四台设备既未成功重新连接，也无法重新连接。

要取消批量操作，请执行以下操作：

**步骤 1** 在 CDO 导航菜单上，点击作业。

**步骤 2** 找到仍在运行的批量操作，然后点击作业行右侧的取消链接。

如果批量操作的任何部分成功，这些操作将不会被撤销。任何仍在运行的操作都将被取消。

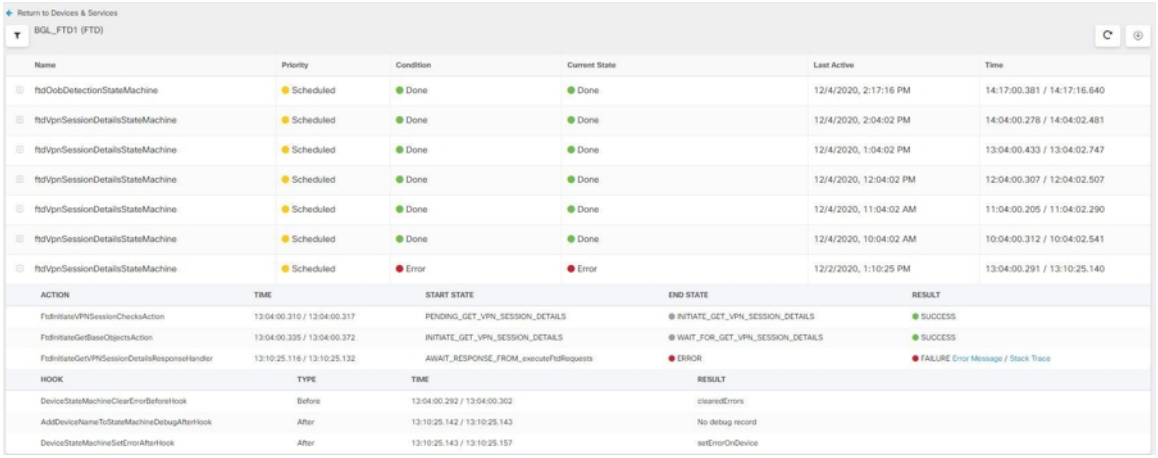
# 工作流程页面

通过“工作流程”(Workflow) 页面，您可以监控 CDO 在与设备、安全设备连接器 (SDC) 或安全事件连接器 (SEC) 通信时以及在对设备应用规则集更改时运行的每个进程。CDO 会在工作流程表中为每个步骤创建一个条目，并在此页面上显示其结果。该条目只会包含与 CDO 执行的操作相关的信息，而不是与其交互的设备相关的信息。

当 CDO 无法在设备上执行任务时，它会报告错误，您可以导航至“工作流程”(Workflows) 页面查看发生错误的步骤以了解更多详细信息。

您可以访问此页面来确定错误并进行故障排除，或者在 TAC 坚持时与他们共享信息。

要导航至“工作流程”(Workflows) 页面，请在**清单 (Inventory)** 页面上点击**设备 (Devices)** 选项卡。点击相应的设备类型选项卡，以便查找设备并选择所需的设备。在右侧窗格的**设备和操作 (Devices and Actions)** 中，点击**工作流程 (Workflows)**。下图显示了“工作流程”(Workflow) 页面，其中包含“工作流程”(Workflow) 表中的条目。

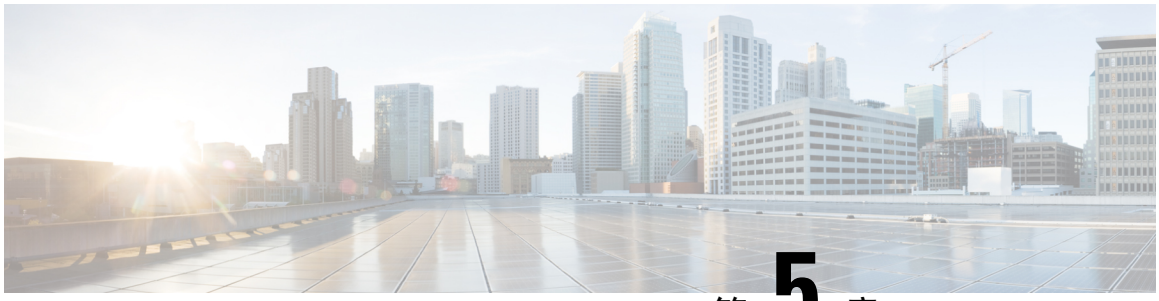



### 下载工作流程信息

您可以将完整的工作流程信息下载到 JSON 文件，并在 TAC 团队要求进行进一步分析时提供。要下载这些信息，您可以选择设备并导航至其工作流程页面，然后点击右上角显示的导出按钮 。

### 生成堆栈跟踪

如果您遇到无法解决的错误，TAC 可能会要求您提供堆栈跟踪的副本。要收集错误的堆栈跟踪，请点击**堆栈跟踪 (Stack Trace)** 链接，然后点击**复制堆栈跟踪 (Copy Stacktrace)**，以便将屏幕上显示的堆栈复制到剪贴板。



第 5 章

# 思科安全分析和日志记录

# 关于 Cisco Defense Orchestrator 中安全分析和日志记录 (SaaS)

思科安全分析和日志记录 (SAL) 允许您从所有 ASA 设备捕获连接、入侵、文件、恶意软件和安全情报事件，以及从 Secure Firewall Threat Defense 捕获所有系统日志事件和 Netflow 安全事件日志记录 (NSEL) 事件并在 Cisco Defense Orchestrator (CDO) 中的一个位置进行查看。事件存储在思科云中，可从 CDO 中的**事件日志记录 (Event Logging)**页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。

通过额外许可，在捕获这些事件后，您可以从CDO交叉启动为您调配的安全云分析门户。安全云分析是一种软件即服务 (SaaS) 解决方案，通过对事件和网络流数据执行行为分析来跟踪网络状态。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

**术语说明**：在本文档中，当思科安全分析和日志记录与安全云分析门户（软件即服务产品）配合使用时，您会看到此集成称为思科安全分析和日志记录 (SaaS) 或 SAL (SaaS) 。

# CDO 中的事件类型

过滤安全日志分析 (SaaS) 记录的 ASA 和 Secure Firewall Threat Defense 事件时，可以从 CDO 支持的 ASA 和 FTD 事件类型列表中进行选择。从 CDO 菜单中，导航到**分析 (Analytics)** > **事件日志记录 (Event Logging)**，然后点击过滤器图标以选择事件。这些事件类型代表系统日志 ID 组。下表显示了包含在哪种事件类型中的系统日志 ID。如果要了解有关特定系统日志 ID 的更多信息，可以在思科 ASA 系列系统日志消息或 Cisco Secure Firewall Threat Defense 系统日志消息指南中进行搜索。

某些系统日志事件将具有附加属性“EventName”。您可以通过过滤“属性:值”对来过滤事件表，查找使用 EventName 属性的事件。请参阅系统日志事件的 EventName 属性。

某些系统日志事件将具有附加属性“EventGroup”和“EventGroupDefinition”。您将能够通过过滤“属性:值”对来过滤事件表，查找使用这些附加属性的事件。请参阅某些系统日志消息的 EventGroup 和 EventGroupDefinition 属性。

NetFlow 事件不同于系统日志事件。**NetFlow** 过滤器搜索生成 NSEL 记录的所有 NetFlow 事件 ID。这些 NetFlow 事件 ID 在《思科 ASA NetFlow 实施指南》中进行了定义。

下表介绍了 CDO 支持的事件类型，并列出了与这些事件类型对应的系统日志或NetFlow事件编号：

| 过滤器名称 | 说明 | 相应的系统日志事件或 NetFlow 事件 |
| --- | --- | --- |
| AAA | 这些是系统在配置 AAA 的情况下，在认证、授权或用尽网络资源的尝试失败或无效时生成的事件。 | 109001-109035<br>113001-113027 |
| 僵尸网络 | 当用户尝试访问可能包含受恶意软件感染的主机（可能是僵尸网络）的恶意网络时，或者当系统检测到流向或来自动态过滤器阻止列表中的域或 IP 地址的流量时，系统会记录这些事件。 | 338001-338310 |
| 故障切换 | 当系统在发生故障切换时检测到有状态和无状态故障切换配置中的错误或辅助防火墙设备中的错误时，将记录这些事件。 | 101001-101005、102001、103001-103007、104001-104004、105001-105048<br>210001-210022<br>311001-311004<br>709001-709007 |
| 防火墙被拒绝 | 当防火墙系统出于各种原因拒绝网络数据包流量时，会生成这些事件，从安全策略导致的数据包丢弃到由于系统收到具有相同源 IP 和目的 IP 的数据包而导致的丢弃，这可能意味着对网络的攻击。<br>防火墙拒绝事件可能包含在 NetFlow 中，并且可能使用 NetFlow 事件 ID 和系统日志 ID 进行报告。 | 106001, 106007, 106012, 106013, 106015, 106016, 106017, 106020, 106021, 106022, 106023, 106025, 106027 |

| 过滤器名称 | 说明 | 相应的系统日志事件或 NetFlow 事件 |
| --- | --- | --- |
| 防火墙流量 | 这些是根据网络中的各种连接尝试、用户身份、时间戳、终止的会话等记录的事件。<br>防火墙流量事件可能包含在 NetFlow 中，并且可能使用 NetFlow 事件 ID 和系统日志 ID 进行报告。 | 106001-106100, 108001-108007, 110002-110003<br>201002-201013、209003-209005、215001<br>302002-302304、302022-302027、303002-303005、313001-313008、317001-317006、324000-324301、337001-337009<br>400001-400050, 401001-401005, 406001-406003, 407001-407003, 408001-408003, 415001-415020, 416001, 418001-418002, 419001-419003, 424001-424002, 431001-431002, 450001<br>500001-500005、508001-508002<br>607001-607003、608001-608005、609001-609002、616001<br>703001-703003、726001 |
| IPSec VPN | 当 IPsec 安全关联中发生不匹配或系统在其接收的 IPsec 数据包中检测到错误时，这些事件会记录在 IPsec VPN 配置的防火墙中。 | 402001-402148、602102-602305、702304-702307 |
| NAT | 当创建或删除 NAT 条目时，以及当 NAT 池中的所有地址都用尽并耗尽时，这些事件会记录在 NAT 配置的防火墙中。 | 201002-201013、202001-202011、305005-305012 |
| SSL VPN | 当创建或终止 WebVPN 会话、用户访问错误和用户活动时，这些事件会记录在 SSL VPN 配置的防火墙中。 | 716001-716060、722001-722053、723001-723014、724001-724004、725001-725015 |
| NetFlow | 当网络数据包进出接口时，这些事件记录在 IP 网络流量、时间戳、用户身份和传输的数据量周围。 | 0, 1, 2, 3, 5 |

| 过滤器名称 | 说明 | 相应的系统日志事件或 NetFlow 事件 |
| --- | --- | --- |
| 连接 | 您可以在用户生成通过系统传递的流量时生成连接事件。启用访问规则连接日志记录以生成这些事件。还可启用安全情报策略和 SSL 解密规则日志记录，以生成连接事件。<br><br>连接事件包含关于检测到的会话的数据。任何单个连接事件的可用信息都取决于多种因素，但通常包括：<br><br>• 基本连接属性：时间戳、源和目标 IP 地址、入口和出口区域，处理连接的设备等。<br><br>• 系统发现或推断的其他连接属性：应用、请求的 URL 或与连接关联的用户等。<br><br>• 有关连接记录原因的元数据：哪个配置处理流量，连接是被允许还是被阻止，以及有关已加密和已解密连接的详细信息等。 | 430002, 430003 |
| 入侵 | 系统检查网络上传输的数据包是否存在可能影响主机及其数据的可用性、完整性和机密性的恶意活动。如果系统识别出潜在的入侵，会生成入侵事件；入侵事件是有关攻击源和攻击目标的日期、时间、攻击程序类型以及情境信息的记录。无论调用访问控制规则的日志记录配置如何，系统均会生成设为阻止或提醒的入侵规则的入侵事件。 | 430001 |

| 过滤器名称 | 说明 | 相应的系统日志事件或 NetFlow 事件 |
| --- | --- | --- |
| 文件 | 文件事件表示系统基于文件策略在网络流量中检测到或者被阻止的文件。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。<br>无论调用访问控制规则采用何种日志记录配置，在系统生成文件事件时，都会记录相关连接的终止。 | 430004 |
| 恶意软件 | 作为整体访问控制配置的一部分，系统可在网络流量内检测恶意软件。适用于 Firepower 的 AMP 可以生成恶意软件事件，其中包含生成事件的处置，有关检测该恶意软件的方式、位置和时间的情境数据。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。<br>文件的处置可能发生变化，例如，从安全变为恶意软件或从恶意软件变为安全。如果适用于 Firepower 的 AMP 向 AMP 云查询文件，且云决定在查询一周内更改处置，系统即会生成追溯性恶意软件事件。 | 430005 |
| 安全情报 | 安全情报事件是由安全情报策略为该策略阻止或监控的每个连接生成的一种连接事件。所有安全情报事件都有一个由系统填充的“安全情报类别”字段。<br>对于各事件，都有一个相应的“常规”连接事件。由于评估安全智能策略后才会评估许多其他安全策略（包括访问控制），所以当安全智能阻止连接时，所生成事件不含系统从后续评估中收集的信息（如用户身份）。 | 430002, 430003 |

# 关于 ASA 的安全分析和日志记录 (SAL SaaS)

通过安全分析和日志记录 (SaaS)，您可以从 ASA 捕获所有系统日志事件和 Netflow 安全事件日志记录 (NSEL)，并在 Cisco Defense Orchestrator (CDO) 中的一个位置进行查看。

事件存储在思科云中，可从CDO中的“事件日志记录”页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。**日志记录和故障排除**软件包为您提供这些功能。

使用**日志记录分析和检测**包（以前称为**防火墙分析和日志记录**包），系统可以将安全云分析动态实体建模应用于FTD事件，并使用行为建模分析生成安全云分析观察结果和警报。如果您获取**全部网络分析和监控**软件包，则系统会对 FTD 事件和网络流量应用动态实体建模，并生成观察结果和警报。您可以使用思科单点登录从 CDO 交叉启动为您调配的安全云分析门户。

### 如何在 CDO 事件查看器中显示 ASA 事件

在 ASA 上启用日志记录且网络流量与访问控制规则条件匹配时，会生成系统日志事件和 NSEL 事件。将事件存储在思科云中后，您可以在 CDO 中查看它们。

您可以安装多个安全事件连接器 (SEC)，并将任何设备上的规则生成的事件发送到任何 SEC，就像它是系统日志服务器一样。然后，SEC 将事件转发到思科云。请勿将相同的事件转发到您的所有 SEC。您将复制发送到思科云的事件，并不必要地提高每日采集速率。

### 如何通过安全事件连接器将系统日志和 NSEL 事件从 ASA 发送到思科云

使用基本**日志记录和故障排除**许可证，ASA 事件通过以下方式到达思科云：

1. 您使用用户名和密码将 ASA 载入 CDO。
2. 将 ASA 配置为将系统日志和 NSEL 事件作为系统日志服务器转发到任何一个 SEC，并在设备上启用日志记录。
3. SEC 将事件转发到存储事件的思科云。
4. CDO 根据您设置的过滤器在其事件查看器中显示来自思科云的事件。

使用 **日志记录分析和检测** 或 **全部网络分析和监控** 许可证时，还会发生以下情况：

1. 思科安全云分析将分析应用到存储在思科云中的 ASA 系统日志事件。
2. 生成的观察结果和警报可从与您的 CDO 门户关联的安全云分析门户访问。
3. 在 CDO 门户中，您可以交叉启动 Secure Cloud Analytics 门户，以查看这些观察结果和警报。

### 解决方案中使用的组件

**安全设备连接器 (SDC)** - SDC 会将 CDO 连接到您的 ASA。ASA 的登录凭证被存储在 SDC 上。有关详细信息，请参阅安全设备连接器, on page 8。

**安全事件连接器 (SEC)** - SEC 是一种可从 ASA 接收事件并将其转发到思科云的应用。进入思科云后，您可以在CDO的“事件日志记录”(Event Logging) 页面上查看事件，或使用“安全云分析”进

行分析。根据您的环境，SEC 安装在安全设备连接器（如果有）上；或在您的网络中维护的 CDO 连接器虚拟机上。有关详细信息，请参阅安全事件连接器, on page 379。

**自适应安全设备 (asa)** - ASA 在一台设备以及带附加模块的集成服务中提供高级状态防火墙和 VPN 集中器功能。ASA 包括许多高级功能，例如多安全情景（类似于虚拟化防火墙）、集群（将多个防火墙组合成一个防火墙）、透明（第 2 层）防火墙或路由（第 3 层）防火墙操作、高级检测引擎、IPsec VPN、SSL VPN 和无客户端 SSL VPN 支持以及许多其他功能。

**安全云分析**可将动态实体建模应用于 ASA 事件，并根据此信息生成检测。这提供了对从网络收集的遥测数据的更深入分析，使您能够识别趋势并检查网络流量中的异常行为。如果您拥有**日志记录分析和检测**或**全面的网络分析和监控**许可证，则可以使用此服务。

### 许可

要配置此解决方案，您需要以下账户和许可证：

- **思科防御协调器**。您必须有 CDO 租户。
- **安全设备连接器**。安全设备连接器没有单独的许可证。
- **安全事件连接器**。安全事件连接器没有单独的许可证。
- **安全日志记录分析 (SaaS)**。请参阅 安全分析和日志记录许可证表格。
- **自适应安全设备 (ASA)**。基本许可证或更高版本。

### 安全分析和日志记录许可

要实施安全分析和日志记录 (SaaS)，您需要购买以下许可证之一：

| 许可证名称 | 提供的功能 | 可用许可证持续时间 | 功能前提条件 |
|---|---|---|---|
| 日志记录故障排除 | • 在 CDO 中以实时源和历史视图的形式查看 ASA 事件和事件详细信息 | • 1 年<br>• 3 年<br>• 提高 | • 首席数据官<br>• 运行软件版本 9.6 或更高版本的本地 ASA 部署。<br>• 部署一个或多个 SEC 以将 ASA 事件传递到思科云。 |

| 许可证名称 | 提供的功能 | 可用许可证持续时间 | 功能前提条件 |
| --- | --- | --- | --- |
| 日志记录分析和检测（以前称为 防火墙分析和监控） | 日志记录和故障排除 功能，以及：<br>• 对事件应用动态实体建模和行为分析。<br>• 根据事件数据在 Secure Cloud Analytics 中打开警报，从 CDO 事件查看器交叉启动。 | • 1 年<br>• 3 年<br>• 提高 | • 首席数据官<br>• 运行 9.6 或更高版本软件的本地 ASA 部署<br>• 部署一个或多个 SEC 以将 ASA 事件传递到思科云。<br>• 新调配的或现有的 Cisco Secure Cloud Analytics 门户。 |
| 全面的网络分析和监控 | 日志记录分析和检测，以及：<br>• 将动态实体建模和行为分析应用于 ASA 事件、本地网络流量和基于云的网络流量<br>• 基于 ASA 事件数据、思科安全云分析传感器收集的本地网络流量数据以及从 CDO 交叉启动传递到思科安全云分析的基于云的网络流量的组合，在思科安全云分析中打开警报事件查看器。 | • 1 年<br>• 3 年<br>• 提高 | • 首席数据官<br>• 运行 9.6 或更高版本软件的本地 ASA 部署<br>• 部署一个或多个 SEC 以将事件传递到思科云。<br>• 部署至少一个 Cisco Secure Cloud Analytics 传感器版本 4.1 或更高版本，以将网络流量数据传递到云，或者将 Cisco Secure Cloud Analytics 与基于云的部署集成，以将网络流量数据传递到 Cisco Secure Cloud Analytics。<br>• 新调配的或现有的 Cisco Secure Cloud Analytics 门户。 |

### 数据计划

您需要购买一个数据计划，以反映思科云每天从注册的ASA接收的事件数量。这称为“每日注入速率”。您可以使用日志记录量估算器工具来估算您的每日注入速率，并且随着该速率的变化，您可以更新数据计划。

数据计划有 1 年、3 年或 5 年期限，每日增量为 1 GB。有关数据计划的信息，请参阅《安全日志分析 (SaaS) 订购指南 》。

**Note** 如果您有安全分析和日志记录许可证和数据计划，则在以后获取不同的许可证，这不需要您获取不同的数据计划。如果您的网络流量吞吐量发生变化，并且您获得了不同的数据计划，则不需要您获得不同的安全分析和日志记录许可证。

### 30 天免费试用

您可以通过登录 CDO 并导航到**监控 (Monitoring)** > **事件日志记录 (Event Logging)** 选项卡来申请 30 天无风险试用。完成 30 天试用后，您可以按照 安全日志分析 (SaaS) 订购指南中的说明，从思科商务工作空间 (CCW) 订购所需的事件数据量，以继续使用该服务。

### 下一步

转至为 ASA 设备实施安全日志记录分析 (SaaS)

# 为 ASA 设备实施安全日志记录分析 (SaaS)

### 准备工作

- 查看关于 ASA 的安全分析和日志记录 (SAL SaaS)，以了解：
  - 如何将事件发送到思科云
  - 应用解决方案
  - 您需要的许可证
  - 您需要的数据计划
- 您已联系托管服务提供商或 CDO 销售代表创建 CDO 租户。
- 查看 安全设备连接器，第 8 页。使用 SDC 将 CDO 连接到 ASA 被视为“最佳实践”，但这不是必需的。
- 如果您选择在网络中部署 SDC，可以使用以下方法之一进行安装：
  - 使用使用 CDO 的 VM 映像部署安全设备连接器，以使用 CDO 准备的 VM 映像安装 SDC。这是部署 SDC 的首选且最简单的方法。

- 使用在您自己的虚拟机上部署安全设备连接器。

- 您安装安全事件连接器，并且可以将任何 ASA 中的事件发送到载入到您的租户的任何 SEC。
- 您已为账户的用户 创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证 。

### 实施思科安全分析和日志记录 (SaaS) 以及通过安全事件连接器将事件发送到思科云的工作流程

1. 请务必查看上面的“开始之前”，确保您的环境配置正确。
2. 将 ASA 设备载入 CDO， 第 135 页 用户名和密码。
3. 使用命令行接口将 ASA 系统日志事件发送到思科云。
4. 使用 CDO 宏为 ASA 设备配置 NSEL。
5. 确认事件显示在 CDO 中。从导航栏中，选择**监控 (Monitoring) > 事件日志记录 (Event Logging)**。点击“实时”(Live) 选项卡以查看实时事件。
6. 如果您有**防火墙分析和监控**或**全面网络分析和监控**许可证，请继续下一部分**使用 Cisco Secure Cloud Analytics 分析事件**。

### 使用 Cisco Secure Cloud Analytics 分析事件

如果您有**防火墙分析和监控**或**全面网络分析和监控**许可证，除上述步骤外还应执行以下操作：

1. 调配思科安全云分析门户， 第 401 页。
2. 如果您购买了**全面网络分析和监控**许可证，请将一个或多个安全云分析传感器部署到您的内部网络。请参阅用于全面网络分析和报告的思科安全云分析传感器部署， 第 402 页。
3. 邀请用户创建与其思科单点登录凭证相关联的安全云分析用户账户。请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报， 第 403 页。
4. 从 CDO 到 Secure Cloud Analytics 的交叉启动，以监控 FTD 事件生成的安全云分析警报。请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报， 第 403 页。

### 通过从 CDO 交叉启动查看 Cisco Secure Cloud Analytics 警报

使用**防火墙分析和监控**或**全面网络分析和监控**许可证，您可以从 CDO 交叉启动安全云分析，以查看 FTD 事件生成的警报。

有关详细信息，请参阅以下文章：

- 登录到 CDO
- 从 CDO 查看 Cisco Secure Cloud Analytics 警报， 第 403 页
- 思科安全云分析和动态实体建模
- 使用基于防火墙事件的警报

### 安全事件连接器问题故障排除

使用这些故障排除主题收集有关状态和日志记录的信息

- 安全事件连接器载入故障排除
- 事件日志记录故障排除日志文件
- 使用运行状况检查了解安全事件连接器的状态

### 工作流程

使用安全和分析日志记录事件排除网络问题介绍了如何使用思科安全分析和日志记录生成的事件来确定用户无法访问网络资源的原因。

另请参阅使用基于防火墙事件的警报。

# 使用 CDO 宏将 ASA 系统日志事件发送到思科云

您可以使用使用命令行接口将 ASA 系统日志事件发送到思科云中描述的所有命令来创建一个 CDO 宏，并在同一批次的所有 ASA 上运行该宏，从而配置所有 ASA 将事件发送到思科云。

通过 CDO 的宏工具，您可以组合 CLI 命令列表，将命令语法的元素转换为参数，然后保存命令列表，以便可以多次使用。宏也可以一次在多台设备上运行。

使用经过验证的宏可提高设备之间的配置一致性，并防止使用命令行界面时可能发生的语法错误。

在进一步阅读之前，请查看这些主题，以便了解使用宏的机制。本文仅介绍汇编最终宏。

- 命令行界面宏
- 从新命令创建 CLI 宏
- 运行 CLI 宏
- 编辑 CLI 宏
- 删除 CLI 宏

## 创建 ASA 安全分析和日志记录 (SaaS) 宏

您将在以下过程中看到两种类型的格式：ASA CLI 命令和宏格式。编写 ASA CLI 命令遵循 ASA 语法约定。创建 CLI 宏中介绍了宏约定。 从新命令创建 CLI 宏, on page 90

在开始之前，请在单独的窗口中打开 Send ASA Syslog Events to the Cisco Cloud，并与此程序同时阅读，以便在创建宏时阅读命令说明。使用命令行接口将 ASA 系统日志事件发送到思科云, on page 355

**Note** 如果 ASA 上已存在日志记录配置，则从 CDO 运行宏不会先清除所有现有的日志记录配置。相反，CDO 宏中定义的设置将合并到可能已经存在的任何设置中。

**步骤 1** 打开纯文本编辑器，并根据以下说明和选项创建要转换为宏的命令列表。CDO 将按照在宏中写入的顺序执行命令。某些命令会将值转换为 {{parameters}}，以便在运行宏时填写。

**步骤 2** **配置 ASA 将消息发送到 SEC，就像它是系统日志 服务器一样。**

使用 logging host 命令将 SEC 指定为您向其发送消息的系统日志服务器。您可以将事件发送到您已载入到租户的任何一个 SEC。

logging host 命令指定要向其发送事件的 TCP 或 UDP 端口。要确定应该使用哪个端口，请参阅查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口。

interface_name SEC_IP_address **logging host** {**tcp/port** | **udp/port**}

根据您用于向 SEC 发送系统日志事件的协议，将此命令转换为两个不同的宏之一：

logging host {{interface_name}} {{SEC_ip_address}} tcp/{{port_number}}

logging host {{interface_name}} {{SEC_ip_address}} udp/{{port)_number}}

（可选）如果使用 TCP，可以将此命令添加到宏命令列表中。它不需要任何参数。

**logging permit-hostdown**

**步骤 3** **指定应将哪些系统日志消息发送到系统日志服务器。**

使用 logging trap 命令指定应将哪些系统日志消息发送到系统日志服务器：

**logging trap** {*severity_level* | *message_list*}

如果要按严重性级别定义发送到 SEC 的事件，请将命令转换为以下宏：

logging trap {{severity_level}}

如果您只想将属于邮件列表的事件发送到 SEC，请将命令转换为以下宏：

日志记录陷阱 {{message_list_name}}

如果在上一步中选择了 logging trap message_list 命令，则需要在消息列表中定义系统日志。打开创建自定义事件列表，以便在创建宏时阅读命令说明。创建自定义事件列表, on page 358使用以下命令启动：

**logging list***name* {**level***level* [**class***message_class*] | **message***start_id* [*-end_id*] }

并将其分解为以下变体：

日志记录列表 {{message_list_name}} 级别 {{security_level}}

logging list {{message_list_name}} level {{security_level}} class {{message_class}}

日志记录列表 {{message_list_name}} 消息 {{syslog_range_or_number}}

在最后一个变体中，消息参数 {{syslog_range_or_number}} 可以输入为单个系统日志 ID 106023 或范围 302013-302018。在任意数量的行中使用一个或多个命令变体来创建邮件列表。请记住，在单个宏中，具有相同名称的所有参数都将使用您输入的相同值。CDO 不会运行参数为空的宏。

**Important** 在宏中，logging list 命令必须位于 logging trap 命令之前。首先定义列表，然后 logging trap 命令可以使用它。请参阅下面的示例宏。

**步骤 4** （可选）添加系统日志时间戳。 如果要向 ASA 上发出系统日志消息的消息添加日期和时间，请添加此命令。时间戳值显示在系统日志时间戳 (SyslogTimestamp) 字段中。将此命令添加到命令列表中，它将不需要任何参数：

**logging timestamp**

**Note** 从版本 9.10(1) 开始，ASA 提供了在事件系统日志中根据 RFC 5424 启用时间戳的选项。当启用此选项时，系统日志消息的所有时间戳将按照 RFC 5424 格式显示时间。以下是 RFC 5424 格式的输出示例：

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
src interface :src IP/src port to dest IP/dest port
```

。

**步骤 5** （可选）**在非 EMBLEM 格式的系统日志 消息中包括设备 ID**。打开 Include the Device ID in Non-EMBLEM Format Syslog Messages，以便您可以在创建宏时阅读命令说明。在非 EMBLEM 格式系统日志消息中包含设备 ID, on page 360这是您的宏所基于的 CLI 命令：

**logging device-id** {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string***text*}

并将其分解为以下变体：

**logging device-id cluster-id**

**logging device-id context-name**

**logging device-id  hostname**

logging device-id ipaddress {{interface_name}} system

logging device-id string {{text_16_char_or_less}}

**步骤 6** 启用日志记录。将此命令按原样添加到宏。它没有任何参数：

**logging enable**

**步骤 7** 不要将写入内存添加到宏的最后一行。 请改为添加 **show running-config logging** 命令，以查看您输入的日志记录命令的结果，然后再将其提交到 ASA 的启动配置。

**show running-config logging**

**步骤 8** 在确定已进行配置更改后，您可以为 write memory 命令创建单独的宏，或使用 CDO 的批量命令行接口功能向使用宏配置的所有设备发出该命令。批量 CLI 接口, on page 86

**write memory**

**步骤 9** （可选）对访问控制规则“允许”事件启用日志记录。 将 ASA 系统日志事件发送到思科云程序中所述的此步骤，但未包含在此宏中。使用命令行接口将 ASA 系统日志事件发送到思科云, on page 355它在 CDO GUI 中执行。

**步骤 10** 保存宏。

---

### Example

以下是组合成单个宏的命令列表示例：

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
```

```
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```

**Note** 有多个 logging list 命令可用于添加不同的特定系统日志 ID 或范围。{{syslog_range_or_number_X}} 参数需要数字或其他一些区分符，否则在填写宏时，它们的值将全部相同。另请记住，如果不是所有参数都指定了值，CDO 将不会运行宏，因此仅包含要执行的宏中的命令。我们希望所有系统日志 ID 都包含在同一个列表中，以便每行中的 event_list_name 保持不变。

#### What to do next

运行宏

创建并保存 ASA 安全分析和日志记录宏后，运行宏将 ASA 系统日志事件发送到思科云。

# 使用命令行接口将 ASA 系统日志事件发送到思科云

此程序介绍如何将 ASA 系统日志事件转发到安全事件连接器 (SEC)，然后启用日志记录。这些程序仅说明了完成该工作流程所需执行的操作。有关在ASA上配置日志记录的所有方式的更广泛讨论，请参阅《ASDM1：思科 ASA 系列常规操作 ASDM 配置指南》或《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中的“监控”一章。

### 支持的 ASA 命令的限制

CDO 尚未支持以下系统日志命令或消息格式：

- 系统日志的 EMBLEM 格式
- 保护系统日志

# ASA 的 CDO 命令行界面

对于此程序中的所有任务，您将使用 ASA 的 CDO 的命令行界面。要打开命令行界面页面，请执行以下操作：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择要为其启用日志记录的 ASA。

**步骤 4** 在右侧“设备操作”(Device Actions) 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 5** 点击 **命令行接口 (Command Line Interface)**。现在，您可以在提示符后输入如下所述的命令。

输入每个命令后，您将点击“发送”。由于 CDO 的 CLI 接口是与 ASA 的直接连接，因此该命令会立即写入设备的运行配置。要将更改写入 ASA 的启动配置，还需要发出 `write memory` 命令。

# 将 ASA 系统日志事件转发到安全事件连接器

要将 ASA 系统日志事件转发到您已自行激活的安全事件连接器 (SEC) 之一，然后启用日志记录，您需要在以下程序中完成这些任务。

**步骤 1** 配置 ASA 以便将消息发送到 SEC，就像它是系统日志服务器一样。

**步骤 2** 决定要发送到 SEC 的所有日志的严重性级别或系统日志事件列表。

**步骤 3** 启用日志记录。

**步骤 4** 保存对 ASA 的启动配置所做的更改。

# 使用 CLI 将 ASA 系统日志事件发送到思科云

**步骤 1** **配置 ASA 以便将消息发送到 SEC，就像它是系统日志服务器一样**

将系统日志事件从 ASA 发送到思科云时，您可以将其作为外部系统日志服务器转发到 SEC，然后 SEC 会将消息转发到思科云。

要将系统日志消息发送到 SEC，请执行以下步骤：

**a.** 将 ASA 配置为使用 TCP 或 UDP 将消息发送到 SEC，就像它是系统日志服务器一样。SEC 可以使用 IPv4 或 IPv6 地址。您将向 TCP 或 UDP 端口发送事件。要确定应该使用哪个端口，请参阅查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口。

以下是 **logging host** 命令语法的示例：

**logging host** *interface_name SEC_IP_address* [ [ **tcp/port** ] | [ **udp/port** ] ]

示例：

```
 > logging host mgmt 192.168.1.5 tcp/10125
> logging host mgmt 192.168.1.5 udp/10025
> logging host mgmt 2002::1:1 tcp/10125
> logging host mgmt 2002::1:1 udp/10025
```

- **interface_name** 参数指定将消息发送到系统日志服务器的 ASA 接口。“最佳实践”是通过已用于与 SDC 通信的同一 ASA 接口将系统日志消息发送到 SDC。
- **SEC_IP_address** 参数应包含安装了 SEC 的虚拟机的 IP 地址。

- **tcp/port** 或 **udp/port** 关键字-参数对指定应使用 TCP 协议和相关端口或 UDP 协议和相关端口发送系统日志消息。可以将 ASA 配置为使用 UDP 或 TCP（但不同时使用两者）将数据发送到系统日志服务器。如果未指定协议，则默认协议为 UDP。

  如果指定 TCP，则在系统日志服务器发生故障时 ASA 会发现此情况，作为安全防御措施，将会阻止通过 ASA 的新连接。要允许新连接而不考虑与 TCP 系统日志服务器的连接，请参阅步骤 b。如果指定 UDP，则无论系统日志服务器是否正常运行，ASA 都将继续允许新连接。有效的端口值

  **Note** 如果要将 ASA 消息发送到两个单独的系统日志服务器，可以使用另一个系统日志服务器的相应接口、IP 地址、协议和端口运行第二个 logging host 命令。

**b.** （可选）如果通过 TCP 向 SEC 发送事件，并且 SEC 已关闭或 ASA 上的日志队列已满，则会阻止新连接。备份系统日志服务器，且日志队列不再已满后，将再次允许新连接。要允许新连接而不考虑与 TCP 系统日志服务器的连接，请使用以下命令禁用该功能以在连接 TCP 的系统日志服务器关闭时阻止新连接：

**logging permit-hostdown**

示例：

```
> logging permit-hostdown
```

**步骤 2** 通过以下命令指定应将哪些系统日志消息发送到系统日志服务器：

**logging trap** { severity_level | message_list }

示例：

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

可以指定严重性级别号（1 至 7）或名称。例如，如果将严重性级别设置为 3，则 ASA 会发送严重性级别为 3、2 和 1 的系统日志消息。

message_list 参数将替换为自定义事件列表的名称（如果已创建）。指定自定义事件列表时，仅将该列表中的系统日志消息发送到安全事件连接器。在上面的示例中，asa_syslogs_to_cloud 是事件列表的名称。

使用 message_list 可以通过严格定义将哪些系统日志消息发送到思科云来节省资金。

请参阅创建自定义事件列表以创建 message_list。有关数据注入和存储成本的详细信息，请参阅数据存储计划。

**步骤 3** （可选）添加系统日志时间戳

使用 logging timestamp 命令将在 ASA 上发出的系统日志消息的日期和时间添加到消息中。时间戳值显示在**系统日志时间戳 (SyslogTimestamp)** 字段中。

**示例：**

```
> logging timestamp
```

**Note** 从版本 9.10(1) 开始，ASA 提供了在事件系统日志中根据 RFC 5424 启用时间戳的选项。当启用此选项时，系统日志消息的所有时间戳将按照 RFC 5424 格式显示时间。以下是 RFC 5424 格式的输出示例：

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from src
interface :src IP/src port to dest IP/dest port.
```

**步骤 4** （可选）在非 **EMBLEM** 格式的系统日志消息中包括设备 **ID**

设备 ID 是可插入到系统日志消息中的标识符，可帮助您轻松区分从特定 ASA 发送的所有系统日志消息。有关说明，请参阅在非 EMBLEM 格式系统日志消息中包含设备 ID。

**步骤 5** （可选）对访问控制规则“允许”事件启用日志记录

当访问控制规则拒绝访问资源时，系统会自动记录该事件。如果您还想记录访问控制规则允许访问资源时生成的事件，则需要打开访问控制规则的日志记录并配置严重性类型。有关如何为单个网络访问控制规则打开日志记录的说明，请参阅记录规则活动。

**Note** 启用访问控制规则“允许”事件的日志记录将使用您购买的更多数据计划，因为它基于您的每日事件采集速率。

**步骤 6** 启用日志记录

在命令提示符下，键入 logging enable。在 ASA 上，为整个设备启用日志记录，而不是为单个规则启用日志记录。

示例：

```
> logging enable
```

**Note** 目前，CDO 不支持启用安全日志记录。

**步骤 7** 保存对启动配置所做的更改

在命令提示符下，键入 write memory。在 ASA 上，为整个设备启用日志记录，而不是为单个规则启用日志记录。

示例：

```
> write memory
```

---

相关信息：

- 在 SDC 虚拟机上安装安全事件连接器, on page 380
- 使用 CDO 映像安装 SEC

# 创建自定义事件列表

使用以下方法之一将 ASA 系统日志事件发送到思科云时，创建自定义事件列表：

- 使用命令行接口将 ASA 系统日志事件发送到思科云
- 使用 CDO 宏将 ASA 系统日志事件发送到思科云

您可以根据以下三个条件创建事件列表（也称为 message_list）：

- 事件类
- 严重性
- 消息 ID

要创建将发送到特定日志记录目标（例如，系统日志服务器或安全事件连接器）的自定义事件列表，请执行以下步骤：

**步骤 1** 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

**步骤 2** 点击相应的选项卡，然后选择要将其系统日志消息包含在自定义事件列表中的 ASA。

**步骤 3** 在**设备操作 (Device Actions)** 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

**步骤 4** 使用此命令语法向 ASA 发出 **logging list** 命令：

**logging list** *name* { **level** *level* [ **class** *message_class* ] | **message** *start_id* [ *-end_id* ] }

*name* 参数指定列表的名称。**level** *level* 关键字/参数对指定严重性级别。**class** *message_class* 关键字/参数对指定特定消息类。**message** *start_id* [*-end_id*] 关键字-参数对指定单个系统日志消息编号或编号范围。

**Note** 请勿使用严重性级别的名称作为系统日志消息列表的名称。禁止的名称包括 emergencies、alert、critical、error、warning、notification、informational 和 debugging。同样，请勿在事件列表名称的开头使用这些单词的前三个字符。例如，请勿使用以字符“err”开头的事件列表名称。

- **根据严重性将系统日志消息添加到事件列表**。例如，如果将严重性级别设置为 3，则 ASA 会发送严重性级别为 3、2 和 1 的系统日志消息。

  示例：

  ```
  > logging list asa_syslogs_to_cloud level 3
  ```

- **根据其他条件将系统日志消息添加到事件列表：**

  输入与上一步中相同的命令，指定现有消息列表的名称和其他条件。为要添加到列表的每个条件输入新命令。例如，可以将在列表中包含系统日志消息的条件指定如下：

  - 日志消息 ID 属于范围 302013 至 302018。
  - 所有系统日志消息都具有 critical 或更高的严重性级别（emergency、alert 或 critical）。
  - 所有 HA 类系统日志消息都具有 warning 或更高的严重性级别（emergency、alert、critical、error 或 warning）。

    示例：

    ```
    > logging list asa_syslogs_to_cloud message 302013-302018
    > logging list asa_syslogs_to_cloud level critical
    > logging list asa_syslogs_to_cloud level warning class ha
    ```

    **Note** 如果系统日志消息满足以下任何条件，则会将其记录。如果系统日志消息满足其中多个条件，则该消息仅记录一次。

**步骤 5** 保存对启动配置所做的更改

在命令提示符下，键入 write memory。

示例：

```
> write memory
```

# 在非 EMBLEM 格式系统日志消息中包含设备 ID

您可以将 ASA 配置为在非 EMBLEM 格式系统日志中包括设备 ID。只能为系统日志指定一种类型的设备 ID。以下程序引用此程序：

- 使用命令行接口将 ASA 系统日志事件发送到思科云
- 使用 CDO 宏将 ASA 系统日志事件发送到思科云

此设备标识符将反映在“事件日志记录”(Event Logging) 页面上显示的系统日志事件的“传感器 ID”(SensorID) 字段中。

**步骤 1** 选择要为其系统日志信息分配设备 ID 的 ASA。

**步骤 2** 在“设备操作”(Device Actions) 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

**步骤 3** 使用此命令语法向设备发出 logging device-id 命令。

**logging device-id** {**cluster-id** | **context-name** | **hostname** | **ipaddress***interface_name* [**system**] | **string***text*}

示例：

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

**context-name** 关键字指示应用作设备 ID 的当前情景的名称（仅适用于多情景模式）。如果在多情景模式下为管理情景启用日志记录设备 ID，则源于系统执行空间中的消息使用设备 ID **system**，源于管理情景中的消息使用管理情景的名称作为设备 ID。

**Note** 在 ASA 集群中，始终使用所选接口的主设备 IP 地址。

**cluster-id** 关键字指定集群中单个 ASA 设备的启动配置中的唯一名称作为设备 ID。

**hostname** 关键字指定应用作设备 ID 的 ASA 的主机名。

**ipaddress** *interface_name* 关键字/参数对指定应将指定为 *interface_name* 的接口 IP 地址用作设备 ID。如果使用 **ipaddress** 关键字，则无论从哪个接口发送系统日志消息，设备 ID 都会成为指定的 ASA 接口 IP 地址。在集群环境中，**system** 关键字指示设备 ID 成为接口上的系统 IP 地址。此关键字为从设备发送的所有系统日志消息提供单个一致的设备 ID。

**string** *text* 关键字/参数对指定应将 text 字符串用作设备 ID。字符串可以包含多达 16 个字符。

不能使用空格或以下任何字符：

- &（与号）
- ‘（单引号）
- "（双引号）

- <（小于）
- >（大于）
- ?（问号）

**步骤 4** 保存对启动配置所做的更改

在命令提示符下，键入 write memory。

示例：

```
> write memory
```

# ASA 设备的 NetFlow 安全事件日志记录 (NSEL)

来自 ASA 的基本系统日志消息缺少安全云分析用于确定 ASA 报告的事件是否表明存在威胁所需的许多数据。Netflow 安全事件日志记录 (NSEL) 为安全云分析提供该数据。

“流定义为通过网络设备传递的具有一些常见属性的单向数据包序列。这些收集的流将导出到外部设备，即 NetFlow 收集器。网络流具有高度的粒度；例如，流记录包括 IP 地址、数据包和字节计数、时间戳、服务类型 (ToS)、应用端口、输入和输出接口等详细信息。“[1]

Cisco ASA 支持 NetFlow 版本 9 服务。NSEL 的 ASA 和实施提供 IP 状态流跟踪方法，该方法仅导出那些表示流中重大事件的记录。在状态流跟踪中，跟踪的流将经历一系列状态更改。

本文档介绍使用 CDO 宏为您的 ASA 配置 NetFlow 的直接方法。《思科 ASA NetFlow 实施指南》提供了有关在 ASA 上配置 NetFlow 的极其详细的讨论，您可能会发现它是与此内容配套的宝贵资源。

### 后续操作

转至使用 CDO 宏为 ASA 设备配置 NSEL。

### 相关文章

- 使用 CDO 宏为 ASA 设备配置 NSEL
- 从 ASA 删除 NetFlow 安全事件日志记录 (NSEL) 配置
- 确定 ASA 全局策略的名称

1. ("Cisco Systems NetFlow 服务导出版本 9." 互联网工程任务组，网络工作组，征求意见：3954，2004 年 10 月，B. Claise，Ed.https://www.ietf.org/rfc/rfc3954.txt）

# 使用 CDO 宏为 ASA 设备配置 NSEL

ASA 使用 Netflow 安全事件日志记录 (NSEL) 报告详细的连接事件数据。您可以将 Cisco Secure Cloud Analytics 应用于此连接事件数据，其中包括双向流统计信息。此程序介绍如何在 ASA 设备上配置 NSEL 并将这些 NSEL 事件发送到流收集器。在这种情况下，流收集器是安全事件连接器 (SEC)。

此过程引用此宏，**配置 NSEL**：

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
     match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
     class {{flow_export_class_name}}
          flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}
```

以下是Configure NSEL 宏的示例，其中填写了所有默认值、类映射的通用名称以及添加到global_policy的类映射。完成这些过程后，您的宏将如下所示：

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
     match any
policy-map global_policy
     class flow_export_class_map
          flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map
```

### 准备工作

收集以下信息：

- 如果您以前从未使用过 CDO 宏，请阅读以下主题：
  - 命令行界面宏, on page 89
    - 编辑 CLI 宏, on page 92
    - 运行 CLI 宏, on page 91
- 从 ASA 接收数据的 SEC 的 IPv4 地址
- ASA 上用于将数据发送到 SEC 的接口
- 用于转发 NetFlow 事件的 UDP 端口号请参阅查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口, on page 461。
- 确定 ASA 全局策略的名称, on page 368

### 工作流程

按照此工作流程使用 CDO 宏为 ASA 设备配置 NSEL。您需要执行以下每个步骤：

1. 打开配置 NSEL 宏 , on page 363。
2. 定义 NSEL 消息的目的地及其发送到 SEC 的间隔, on page 363。
3. 创建定义将发送到 SEC 的 NSEL 事件的类映射, on page 364。
4. 为 NSEL 事件定义策略映射, on page 365。
5. 禁用冗余系统日志消息, on page 366。
6. 查看并发送宏, on page 367。

### 后续操作

通过转至 打开配置 NSEL 宏 , on page 363开始上述工作流程。

## 打开配置 NSEL 宏

### Before you begin

这是较长工作流程的第一部分，在开始之前请参阅使用 CDO 宏为 ASA 设备配置 NSEL, on page 361。

**步骤 1** 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。
**步骤 2** 点击相应的设备类型选项卡，然后选择要配置 NetFlow 安全事件日志记录 (NSEL) 的 ASA。
**步骤 3** 在**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。
**步骤 4** 点击宏星标  以显示可用宏的列表。
**步骤 5** 从宏列表中，选择**配置 NSEL (Configuring NSEL)**。
**步骤 6** 在“宏”(Macro) 框下，点击**查看参数 (View Parameters)**。

### What to do next

请继续定义 NSEL 消息的目的地及其发送到 SEC 的间隔, on page 363。

## 定义 NSEL 消息的目的地及其发送到 SEC 的间隔

NSEL 消息可以发送到您已载入到租户的任何一个 SEC。这些说明引用了宏的这一部分：

流导出目的地 {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

### Before you begin

这是更大工作流程的一部分。在开始之前，请参阅使用 CDO 宏为 ASA 设备配置 NSEL, on page 361。

步骤 1 **flow-export destination** 命令定义将 NetFlow 数据包发送到的收集器。在这种情况下，您会将它们发送到 SEC。填写以下参数的字段：

- **{{interface}}** - 输入发送 NetFlow 事件的 ASA 上的接口的名称。
- **{{SEC_IPv4_address}}** - 输入 SEC 的 IPv4 地址。SEC 用作流收集器。
- **{{SEC_NetFlow_port}}** - 输入 SEC 上向其发送 NetFlow 数据包的 UDP 端口号。

步骤 2 **flow-export template timeout-rate** 指定将模板记录发送到所有已配置的输出目标的时间间隔。

- **{{timeout_rate_in_mins}}** - 输入重新发送模板之前的分钟数。**我们建议使用 60 分钟的值**。SEC 不处理模板。较大的数字会减少到 SEC 的流量。

步骤 3 **flow-export delay flow-create** 命令将流创建事件的发送延迟指定的秒数。此值与建议的活动超时值匹配，并减少从 ASA 导出的流事件数。在该速率下，NSEL 事件将在连接关闭时或在创建连接后的 55 秒内首次出现在 CDO 中，以较早者为准。如果未配置此命令，则不会延迟，并会在创建流后立即导出流创建事件。

- **{{delay_flow_create_rate_in_secs}}** - 输入发送流创建事件之间的延迟秒数。**我们建议使用 55 秒的值**。

步骤 4 **flow-export active refresh-interval** 命令定义从 ASA 发送长生存期流状态更新的频率。有效值为 1 到 60 分钟。在“流更新间隔”(Flow Update Interval) 字段中，将 **flow-export active refresh-interval** 配置为至少比 **flow-export delay flow-create** 间隔多 5 秒可防止流更新事件出现在流创建事件之前。

- **{{refresh_interval_in_mins}}** - **我们建议使用 1 分钟的值**。有效值为 1 到 60 分钟。

### What to do next

请继续创建定义将发送到 SEC 的 NSEL 事件的类映射, on page 364。

## 创建定义将发送到 SEC 的 NSEL 事件的类映射

宏中的以下命令将所有 NSEL 事件分组到一个类中，然后将该类导出到安全事件连接器 (SEC)。这些说明引用了宏的这一部分：

class {{flow_export_class_name}}

匹配 {{add_this_traffic_to_class_map}}

### Before you begin

这是更大工作流程的一部分。在开始之前，请参阅使用 CDO 宏为 ASA 设备配置 NSEL, on page 361。

步骤 1 **class-map** 命令命名用于标识将导出到 SEC 的 NSEL 流量的类映射。

- **{{flow-export-class-name}}**-输入类映射的名称。其中，名称最多可包含 40 个字符。名称“class-default”和任何以“_internal”或“_default”开头的名称均已保留。所有类型的类映射都使用同一命名空间，因此无法重复使用已被另一类型的类映射使用的名称。

**步骤 2** 标识将与您的类映射关联（匹配）的流量。为 **{{add_this_traffic_to_class_map}} 的值选择以下选项之一：**

- 在 **{{add_this_traffic_to_class_map}}** 字段中输入 **any**。这将监控 NSEL 流量的所有流量类型。**我们建议使用值“any”**。
- 在 **{{add_this_traffic_to_class_map}}** 字段中输入 **access-list *name-of-access-list*** 。这会将所有与您创建的访问列表关联的流量相关联。有关详细信息，请参阅《思科 ASA NetFlow 实施指南》中的通过模块化策略框架配置流导出操作。

### What to do next

请继续为 NSEL 事件定义策略映射, on page 365。

## 为 NSEL 事件定义策略映射

该任务会将NetFlow导出操作分配给您在上一个任务中创建的类，然后将该类分配给新的策略映射。这些说明引用了宏的这一部分：

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

### Before you begin

这是更大工作流程的一部分。在开始之前，请参阅使用 CDO 宏为 ASA 设备配置 NSEL, on page 361。

**步骤 1** **policy-map** 命令可创建策略映射。在下一个任务中，您可以将此策略映射与全局策略关联。

- **{{global_policy_map_name}}** - 输入策略映射的名称。**我们建议使用防火墙现有全局策略的名称（如有）**。全局策略的默认名称为 **global_policy**。请参阅确定 ASA 全局策略的名称。如果您根据《思科 ASA NetFlow 实施指南》中的通过模块化策略框架配置流导出操作来创建新的策略映射并全局应用，则其余检测策略将被停用。

**步骤 2** **class** 命令会继承您在 创建定义将发送到 SEC 的 NSEL 事件的类映射, on page 364 中创建的类映射的名称。

**步骤 3** **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} 命令可定义应将哪些事件类型发送到流收集器（在本例中为 SEC）。

- **{{event-type}}** - event_type 关键字是过滤的受支持事件的名称。**我们建议使用值"all"**。
- **{{SEC_IPv4_address}}** - 这是 SEC 的 IPv4 地址。其值继承自您在 定义 NSEL 消息的目的地及其发送到 SEC 的间隔, on page 363 中输入的值。

### What to do next

请继续禁用冗余系统日志消息, on page 366。

## 禁用冗余系统日志消息

这些说明引用了宏的这一部分。您不需要修改命令。

logging flow-export-syslogs disable

启用 NetFlow 以导出流信息会使列出在下列表格中的系统日志消息冗余。出于性能考虑，建议您禁用冗余系统日志消息，因为相同的信息会通过 NetFlow 导出。

**Note** 当 NSEL 和系统日志消息均已启用时，不能保证两种日志记录类型之间的时间排序。

| 系统日志消息 | 说明 | NSEL 事件 ID | NSEL 扩展事件 ID |
|---|---|---|---|
| 106100 | 每当遇到访问控制规则 (ACL) 时生成。 | 1—已创建流（如果 ACL 允许流）。<br>3—流被拒绝（如果 ACL 拒绝流）。 | 0—如果 ACL 允许流。<br>1001—流被入口 ACL 拒绝。<br>1002—流被出口 ACL 拒绝。 |
| 106015 | TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。 | 3—流被拒绝。 | 1004—TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。 |
| 106023 | 当通过**访问组**命令连接到接口的 ACL 拒绝流时。 | 3—流被拒绝。 | 1001—流被入口 ACL 拒绝。<br>1002—流被出口 ACL 拒绝。 |
| 302013、302015、302017、302020 | TCP、UDP、GRE 和 ICMP 连接创建。 | 1—已创建流。 | 0—忽略。 |
| 302014、302016、302018、302021 | TCP、UDP、GRE 和 ICMP 连接断开。 | 2—已删除流。 | 0—忽略。<br>> 2000—流已断开。 |
| 313001 | 发送到设备的 ICMP 数据包被拒绝。 | 3—流被拒绝。 | 1003—由于配置，已拒绝传入流。 |
| 313008 | 发送到设备的 ICMP v6 数据包被拒绝。 | 3—流被拒绝。 | 1003—由于配置，已拒绝传入流。 |
| 710003 | 尝试连接到设备接口被拒绝。 | 3—流被拒绝。 | 1003—由于配置，已拒绝传入流。 |

如果您不想禁用冗余系统日志消息，可以编辑此宏并仅从中删除此行：

**logging flow-export-syslogs disable**

您可以稍后按照禁用和重新启用 NetFlow 相关系统日志消息中的程序启用或禁用各个系统日志消息。

## 查看并发送宏

**Before you begin**

这是更大工作流程的一部分。在开始之前，请参阅使用 CDO 宏为 ASA 设备配置 NSEL, on page 361。

**步骤 1** 填写宏的字段后，点击 **查看 (Review)** 以查看命令，然后再将其发送到 ASA。

**步骤 2** 如果您对命令的响应感到满意，请点击**发送 (Send)**。

**步骤 3** 在发送命令后，您可能会看到消息“某些命令可能对运行配置进行了更改”(Some commands may have made changes to the running config) 以及两个链接。


- 点击**写入磁盘 (Write to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到设备的启动配置中。
- 点击**消除 (Dismiss)** 关闭消息。

您已完成使用 CDO 宏为 ASA 设备配置 NSEL, on page 361中所述的工作流程。

# 从 ASA 删除 NetFlow 安全事件日志记录 (NSEL) 配置

此程序介绍如何删除 ASA 上的 NetFlow 安全事件日志记录 (NSEL) 配置，该配置将安全事件连接器 (SEC) 指定为 NSEL 流收集器。此程序与使用 CDO 宏为 ASA 设备配置 NSEL 中所述的宏相反。

此过程引用此宏 **DELETE NSEL**：

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

## 打开 DELETE-NSEL 宏

**步骤 1** 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

**步骤 2** 点击相应的设备类型选项卡，然后选择要删除 NetFlow 安全事件日志记录 (NSEL) 配置的 ASA。

**步骤 3** 在**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 4** 点击宏星标  以显示可用宏的列表。

**步骤 5** 在宏列表中，选择 **DELETE-NSEL**。

**步骤 6** 在“宏”(Macro) 框下，点击**查看参数 (View Parameters)**。

## 在宏中输入值以完成无命令

ASA CLI 使用命令的“no”形式将其删除。填写宏中的字段以填写命令的“no”形式：

**步骤 1** policy-map {{flow_export_policy_name}}

- {{flow_export_policy_name}} - 输入策略映射名称的值。

**步骤 2** no class {{flow_export_class_name}}

- {{flow_export_class_name}} - 输入类映射名称的值。

**步骤 3** no class-map {{flow_export_class_name}}

- {{flow_export_class_name}} - 类映射名称的值继承自上述步骤。

**步骤 4** no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}

- **{{interface}}** - 输入发送 NetFlow 事件的 ASA 上的接口的名称。
- **{{IPv4_address}}**-输入 SEC 的 IPv4 地址。SEC 用作流收集器。
- **{{NetFlow_port}}**-输入 SEC 上向其发送 NetFlow 数据包的 UDP 端口号。

**步骤 5** no flow-export template timeout-rate {{timeout_rate_in_mins}}

- **{{timeout_rate_in_mins}}**-输入流导出模板超时速率。

**步骤 6** no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

- **{{delay_flow_create_rate_in_secs}}**-输入流导出延迟流创建速率。

**步骤 7** no flow-export active refresh-interval {{refresh_interval_in_mins}}

- **{{refresh_interval_in_mins}}**-输入流导出活动刷新间隔。

# 确定 ASA 全局策略的名称

要确定 ASA 的全局策略的名称，请遵循以下程序：

**步骤 1** 在 **清单 (Inventory)** 页面中，选择要为其查找全局策略名称的设备。

**步骤 2** 在“设备操作”(Device Actions) 窗格中，选择 **>_Command Reference**。

**步骤 3** 在命令行界面窗口中，在提示符后键入：

**show running-config service-policy**

在下面的示例输出中，global_policy 是全局策略的名称。

示例：

> **show running-config service-policy**

**service-policy global_policy global**

# NSEL 数据流故障排除

使用 CDO 宏为 ASA 设备配置 NSEL 后，请使用以下程序验证 NSEL 事件是否从 ASA 发送到思科云以及思科云是否正在接收这些事件。

请注意，一旦 ASA 被配置为将 NSEL 事件发送到安全事件连接器 (SEC)，然后再发送到思科云，数据不会立即流动。假设 ASA 上生成了与 NSEL 相关的流量，第一个 NSEL 数据包可能需要几分钟才能到达。

**Note** 此工作流程向您展示如何直接使用“flow-export counters”命令和“capture”命令对 NSEL 数据流进行故障排除。有关这些命令用法的更详细讨论，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中的“数据包捕获”和《思科 ASA NetFlow 实施指南》中的“监控 NSEL”。

执行这些任务：

- 验证 NetFlow 数据包是否正在发送到 SEC
- 验证思科云是否正在接收 NetFlow 数据包

## 验证 NSEL 事件是否正在发送到 SEC

使用以下两个命令之一验证是否正在向 SEC 发送 NSEL 数据包：

- flow-export counters
- 捕获

### 使用 "flow-export counters" 命令检查正在发送的流导出数据包和 NSEL 错误

- 请确保您已将 ASA 配置为向 SEC 发送 NSEL 事件。请参阅使用 CDO 宏为 ASA 设备配置 NSEL。
- SEC IP 地址是 NSEL 事件的流收集器地址。如果您已将多个 SEC 载入租户，请确保使用正确的 IP 地址。

- 查找用于转发 NetFlow 事件的 UDP 端口号。请参阅查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口。
- 我们推荐的发送 NSEL 事件的接口是 ASA 上的管理接口；您的接口可能有所不同。

使用 CDO 中的命令行界面将这些命令发送到您为 NSEL 配置的 ASA。批量命令行接口, on page 85

---

**步骤 1** 在导航窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备选项卡，然后选择您配置的 ASA 将 NSEL 事件发送到 SEC。

**步骤 4** 在右侧**设备操作(Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 5** 通过运行 clear flow-export counters 命令重置流导出计数器。这会将清除导出流计数器重置为零，以便您可以轻松判断是否有新事件传入。

示例：

```
> clear flow-export counters
Done!
```

**步骤 6** 运行 show flow-export counters 命令以查看 NSEL 数据包的目的地、发送的数据包数量和任何错误：

示例：

```
>show flow-export counters
目的地： management 209.165.200.225 10425
统计信息：
发送的数据包数 25000
错误：
block allocation errors 0
invalid interface 0
template send failure 0
no route to collector 0
source port allocation 0
```

在上面的输出中，目的行显示从其发送 NSEL 事件的 ASA 上的接口、SEC 的 IP 地址和 SEC 的端口 10425。它还显示发送的数据包 25000。

如果没有错误且正在发送数据包，请跳至下面的验证思科云是否已接收 NetFlow 数据包。验证思科云是否正在接收 NetFlow 数据包, on page 372

---

错误说明：

- **block allocation errors** - 如果收到块分配错误，则 ASA 未将内存分配给流导出器。
  - 恢复操作：致电 思科 Technical Assistance Center (TAC)。

- 接口无效 - 表示您正在尝试将 NSEL 事件发送到 SEC，但您为流导出定义的接口未配置为执行此操作。
  - 恢复操作：查看您在配置 NSEL 时选择的接口。我们建议使用管理接口，您的接口可能与此不同。
- 模板发送失败 - 未正确解析您必须定义的 NSEL 模板。
  - 恢复操作：联系 Defense Orchestrator 支持。联系思科威胁防御支持, on page 534
- **no route to collector** - 表示没有从 ASA 到 SEC 的网络路由。
  - 恢复操作：
    - 确保配置 NSEL 时用于 SEC 的 IP 地址是正确的。
    - 确保 SEC 的状态为“活动”，并且最近已发送心跳。请参阅SDC 无法接通, on page 489。
    - 确保安全设备连接器的状态为活动，并且最近发送了心跳。
- **source port allocation** - 可能表示您的 ASA 上的端口存在问题。

## 使用“capture”命令捕获从 ASA 发送到 SEC 的 NSEL 数据包

- 请确保您已将 ASA 配置为向 SEC 发送 NSEL 事件。请参阅使用 CDO 宏为 ASA 设备配置 NSEL。
- SEC IP 地址是 NSEL 事件的流收集器地址。如果您已将多个 SEC 载入租户，请确保使用正确的 IP 地址。
- 查找用于转发 NetFlow 事件的 UDP 端口号。请参阅查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口。
- 我们推荐的发送 NSEL 事件的接口是 ASA 上的管理接口；您的接口可能有所不同。

使用 CDO 中的命令行界面将这些命令发送到您为 NSEL 配置的 ASA。CDO 命令行界面 ，第 83 页

---

**步骤 1** 在导航窗格中，点击**清单 (Inventory)**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择您配置的 ASA 将 NSEL 事件发送到 SEC。

**步骤 4** 在右侧**设备操作(Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

**步骤 5** 在命令窗口中，运行以下 **capture** 命令：

>**capture***capture_name***interface***interface_name* **match udp any host** *IP_of_SEC***eq***NetFlow_port*

位置

- *capture_name* 是数据包捕获的名称。
- *interface_name* 是 NSEL 数据包离开 ASA 的接口的名称。

- *IP_of_SEC* 是 SEC VM 的 IP 地址。
- *NetFlow_port* 是 NSEL 事件发送到的端口。

这将启动数据包捕获。

**步骤 6** 运行 **show capture** 命令以查看捕获的数据包：

**> show capture***capture_name*

其中，*capture_name* 是您在上一步中定义的数据包捕获的名称。

以下是显示捕获时间、发送数据包的IP地址、IP地址以及数据包发送到的端口的输出示例。在本例中，192.168.25.4 是 SEC 的 IP 地址，端口 10425 是 SEC 上接收 NSEL 事件的端口。

6 个数据包被捕获

```
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: udp 476
2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: udp 248
3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: udp 1436
4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: udp 1276
5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: udp 112
6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: udp 196
```

**步骤 7** 运行 **capture stop** 命令以手动停止数据包捕获：

**> capture** *capture_name***stop**

其中，*capture_name* 是您在上一步中定义的数据包捕获的名称。

## 验证思科云是否正在接收 NetFlow 数据包

**准备工作**

验证是否正在从 ASA 发送 NSEL 事件。

## 检查实时 NSEL 事件

检查实时事件和历史事件。

此程序将过滤思科云在过去一小时内收到的 NSEL 事件。

**步骤 1** 从 CDO 菜单中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**实时 (Live)** 选项卡。

**步骤 3** 固定打开事件过滤器。

**步骤 4** 在“ASA 事件”(ASA Events) 部分中，确保选中 NetFlow。

**步骤 5** 在传感器 ID 字段中，输入配置为发送 NSEL 事件的 ASA 的 IP 地址。

**步骤 6** 在过滤器的底部，确保选中“包括 NetFlow 事件”。

## 检查历史 NSEL 事件

此程序将过滤思科云在您指定的时间范围内收到的 NSEL 事件。

**步骤 1** 从 CDO 菜单中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**历史 (Historical)** 选项卡。

**步骤 3** 固定打开事件过滤器。

**步骤 4** 在“ASA 事件”(ASA Events) 部分中，确保选中 NetFlow。

**步骤 5** 将开始时间设置得足够远，以检查 CDO 是否收到过 NSEL 事件。

**步骤 6** 在传感器 ID 字段中，输入配置为发送 NSEL 事件的 ASA 的 IP 地址。

**步骤 7** 在过滤器的底部，确保选中“包括 NetFlow 事件”。

# 已解析的 ASA 系统日志事件

解析的系统日志事件包含比其他系统日志事件更多的事件属性，并允许您搜索任何特定的解析字段。SEC 会将您指定的所有 ASA 事件转发到思科云，但仅解析下表中的系统日志消息。所有已解析的系统日志事件均显示为斜体，以帮助您识别事件类型。

有关系统日志的详细说明，请参阅思科 ASA 系列系统日志消息。

| 系统日志 ID | 系统日志类别 | 系统日志消息的用途 |
|---|---|---|
| 106015 | 防火墙 | 表示非 TCP 拒绝状态 |
| 106023 | 防火墙 | ACL 拒绝了真实 IP 数据包。即便您没有为 ACL 启用 **log** 选项，也会显示此消息。 |
| 106100 | 访问列表/用户会话 | 数据包被 ACL 允许或拒绝。 |
| 113019 | 用户身份验证 | 关键 AnyConnect |
| 302013、302015、302017、302020 | 用户会话 | TCP、UDP、GRE 和 ICMP 连接创建的连接开始和结束系统日志。 |
| 302014、302016、302018、302021 | 用户会话 | TCP、UDP、GRE 和 ICMP 连接创建的连接开始和结束系统日志。 |
| 302020 - 302021 | 用户会话 | ICMP 会话建立和断开。 |

| 系统日志 ID | 系统日志类别 | 系统日志消息的用途 |
|---|---|---|
| 305006 | 用户会话/NAT 和 PAT | NAT 连接失败 |
| 305011-305014 | 用户会话/NAT 和 PAT | NAT Build/Teardown 相关 |
| 313001、313008 | IP 堆栈 | 表示拒绝与设备的连接。 |
| 414004 | System | 关键 AnyConnect |
| 609001 - 609002 | 防火墙 | 网络状态容器时为连接到区域的主机 **ip-address** 而保留或移除的。 |
| 710002、710004 710005 | 用户会话 | 连接 box 失败 |
| 710003 | 用户会话 | 表示拒绝与设备的连接。 |
| 746012、746013 | 用户会话 | 关键 AnyConnect |

相关信息：

- 使用命令行接口将 ASA 系统日志事件发送到思科云
- 在事件日志记录页面中搜索和过滤事件

# 为云交付的防火墙管理中心托管设备实施 SAL (SaaS)

要部署此集成，您必须使用系统日志或直接连接在 SAL (SaaS) 中设置事件数据存储。

- 使用系统日志将 云交付的防火墙管理中心 托管事件发送到 SAL (SaaS)，第 375 页
- 使用直接连接将 云交付的防火墙管理中心 托管的时间日志发送到 SAL (SaaS)，第 377 页

# SAL (SaaS) 集成的要求、准则和限制

| 类型 | 说明 |
|---|---|
| Cisco Secure Firewall Threat Defense | • CDO 管理的独立威胁防御设备，版本 7.2 及更高版本。<br>• 要使用系统日志发送事件，您必须有威胁防御 6.4 或更高版本。<br>• 要直接发送事件，您必须有威胁防御 7.2 或更高版本。<br>• 必须部署防火墙系统并成功生成事件。 |

| 类型 | 说明 |
| --- | --- |
| 区域云 | • 确定要向其发送事件的区域云。<br>• 无法在不同的区域云之间查看或移动事件。<br>• 如果您使用直接连接将事件发送到云以与思科 SecureX 或思科 SecureX 威胁响应集成，则必须使用相同的云区域来进行此集成。<br>• 如果直接发送事件，则在 CDO 中指定的区域云必须与 CDO 租户的区域相匹配。 |
| 数据计划 | • 您必须购买一个数据计划，以反映思科云每天从威胁防御设备接收的事件数量。这称为每日注入速率。<br>• 使用日志记录量估算器工具来估算您的数据存储要求。 |
| 帐户 | 当您购买此集成的许可证时，系统会为您提供一个 CDO 租户账户来支持集成。 |

# 使用系统日志将云交付的防火墙管理中心托管事件发送到 SAL (SaaS)

本步骤提供了有关从 CDO 托管的设备发送安全事件（连接、安全情报、入侵、文件和恶意软件事件）的系统日志消息的配置信息。

### 开始之前

- 配置策略以生成安全事件，并验证您希望看到的事件显示在**分析 (Analysis)** 菜单下的适用表中。
- 收集与系统日志服务器 IP 地址，端口和协议（UDP 或 TCP）相关的信息。
- 确保您的设备可以访问系统日志服务器。

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 菜单中，点击 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 以打开**服务 (Services)** 页面。

**步骤 3** 点击并选择**云托管 FMC (Cloud-Delivered FMC)**，然后点击**配置 (Configuration)**。

**步骤 4** 为威胁防御设备配置系统日志设置：

a) 点击**设备 (Devices)** > **平台设置 (Platform Settings)** 并编辑与您的威胁防御设备关联的平台设置策略。

b) 在左侧导航窗格中，点击**系统日志 (Syslog)** 并配置系统日志设置，如下所示：

| 点击此 UI 元素... | 要执行以下操作： |
|---|---|
| 日志记录设置 | 启用日志记录，制定FTP服务器设置，以及闪存用法。 |
| 日志记录目标 | 启用向特定目标的记录日志，并指定按邮件严重性级别、事件类别或自定义事件列表进行过滤。 |
| 邮件设置 | 指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。 |
| 事件列表 | 定义包括事件类、严重性级别和事件ID的自定义事件列表。 |
| 速率限制 | 指定发送到所有配置的目标的邮件数量，并定义要为其分配速率限制的邮件严重性级别。 |
| 系统日志设置 | 指定日志记录设施，启用时间戳包含，并启用其他设置以将服务器设置为一个系统日志目标。 |
| 系统日志服务器 | 为指定为日志记录目标的系统日志服务器指定 IP 地址、使用的协议、格式和安全区域。 |

c) 点击**保存**。

**步骤 5** 配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录）：

a) 点击**策略 (Policies)** > **访问控制 (Access Control)**，然后编辑与威胁防御设备关联的访问控制策略。

b) 点击**更多 (More)**，然后选择**日志记录 (Logging)**。配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录），如下所示：

| 点击此 UI 元素... | 要执行以下操作： |
|---|---|
| 使用特定系统日志警报发送 | 从现有的预定义警报列表中选择一个系统日志警报，或者通过指定名称、日志主机、端口、设施和严重程度来添加一个警报。 |
| 使用在设备上部署的FTD平台设置策略中配置的系统日志设置 | 通过在**平台设置 (Platform Settings)** 中配置系统日志配置并重新使用访问控制策略中的设置来统一系统日志配置。所选的严重性适用于所有连接和入侵事件。默认严重性为**警报 (ALERT)**。 |
| 发送 IPS 事件的系统日志消息 | 作为系统日志消息发送事件。除非覆盖，否则将使用默认的系统日志设置。 |
| 发送文件和恶意软件事件的系统日志消息 | 作为系统日志消息发送文件和恶意软件事件。除非覆盖，否则将使用默认的系统日志设置。 |

c) 点击**保存**。

**步骤 6** 为访问控制策略启用安全情报事件日志记录：

a) 在同一访问控制策略中，点击 **安全情报** 选项卡。
b) 点击**日志记录 (Logging)** 并使用以下条件启用安全智能日志记录：
   - 按域名 - 点击 **DNS 策略 (DNS Policy)** 下拉列表旁边的日志记录。
   - 按 IP 地址 - 点击 **网络**旁边的日志记录。
   - 按 URL - 点击 **URL**旁边的日志记录。
c) 点击**保存 (Save)**。

**步骤 7** 为访问控制策略中的每个规则启用系统日志记录：
a) 在同一访问控制策略中，点击 **规则** 选项卡。
b) 点击要编辑的规则。
c) 点击规则中的**日志记录 (Logging)** 选项卡。
d) 选中**连接开始时的日志 (Log at beginning of connection)** 和**连接结束时的日志 (Log at end of connection)** 复选框。
e) 如果要记录文件事件，请选中**日志文件 (Log Files)** 复选框。
f) 选中**系统日志服务器 (Syslog Server)** 复选框。
g) 验证规则是**在访问控制日志记录中使用默认系统日志配置 (ng default syslog configuration in Access Control Logging)**。
h) 点击**保存**。
i) 对策略中的每个规则重复步骤 7.a 至 7.h。

### 下一步做什么

如果您已完成所有必要的更改，请将更改部署到托管设备。

# 使用直接连接将 云交付的防火墙管理中心 托管的时间日志发送到 SAL (SaaS)

配置 云交付的防火墙管理中心 以便直接向 SAL (SaaS) 发送事件。按照此程序在云交付的防火墙管理中心中启用思科云事件全局设置。必要时，您可以排除单个 FTD 设备向 SAL (SaaS) 发送事件日志。有关详细信息，请参阅启用或禁用威胁防御设备以使用直接连接将事件日志发送到 SAL (SaaS)，第 378 页。

### 开始之前

- 将设备载入云交付的防火墙管理中心，将许可证分配给这些设备，然后将这些设备配置为直接将事件发送到 SAL (SaaS)。
- 通过编辑规则并选择**在连接开始时记录 (Log at Beginning of Connection)** 和**在连接结束时记录 (Log at End of Connection)** 选项来启用基于每个规则的连接日志记录。

**步骤 1** 登录 CDO。

**步骤 2** 在 CDO 菜单中，点击 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

**步骤 3** 点击**云交付的 FMC (Cloud-Delivered FMC)**，然后在右侧的**系统 (System)** 窗格中，点击**思科云事件 (Cisco Cloud Events)**。

**步骤 4** 在**配置思科云事件 (Configure Cisco Cloud Events)** 构件中，执行以下操作：

1. 点击**将事件发送到云 (Send Events to the Cisco Cloud)** 切换按钮以启用整体配置。
2. 选中**将入侵事件发送到云 (Send Intrusion Events to the cloud)** 复选框以将入侵事件发送到云。
3. 选中**将文件和恶意软件事件发送到云 (Send File and Malware Events to the cloud)** 复选框，将文件和恶意软件事件发送到云。
4. 选择一个选项以便将连接事件发送到云：
   - 点击**无 (None)** 单选按钮可不将连接事件发送到云。
   - 点击**安全事件 (Security Events)** 单选按钮，仅将安全情报事件发送到云。
   - 点击**全部 (All)** 单选按钮，将所有连接事件发送到云。
5. 点击**保存 (Save)**。

# 启用或禁用威胁防御设备以使用直接连接将事件日志发送到 SAL (SaaS)

启用或禁用 云交付的防火墙管理中心 管理的 FTD 设备，以将事件直接发送到 SAL (SaaS)。通过此设备级控制，您可以选择性地排除特定 FTD 设备向思科云发送事件日志，以减少流量或维护 SAL 和本地事件日志存储的组合。

**注释**

- 要启用或禁用从 FTD 设备向思科云发送事件，请在云交付的防火墙管理中心中启用思科云事件全局设置。有关启用思科云事件全局设置的详细信息，请参阅使用直接连接将 云交付的防火墙管理中心 托管的时间日志发送到 SAL (SaaS)，第 377 页。

  在云交付的防火墙管理中心中启用思科云事件全局设置时，默认情况下会为所有 FTD 设备启用将事件发送到思科云。

- FTD 7.4.1 或更高版本支持启用或禁用 FTD 设备向云发送事件日志的选项。

开始之前

- 将设备载入 云交付的防火墙管理中心，将许可证分配给这些设备，然后将这些设备配置为直接将事件发送到 SAL (SaaS)。
- 通过编辑规则并选择**在连接开始时记录 (Log at Beginning of Connection)** 和**在连接结束时记录 (Log at End of Connection)** 选项来启用基于每个规则的连接日志记录。

**步骤 1** 登录 CDO。
**步骤 2** 在 CDO 菜单中，点击**清单 (Inventory)**。
**步骤 3** 点击**设备 (Devices)** 选项卡以找到设备。
**步骤 4** 点击 **FTD** 选项卡。
**步骤 5** 从清单列表中选择要编辑其配置的 FTD 设备。
**步骤 6** 在**设备管理 (Device Management)** 窗格中，点击**云事件 (Cloud Events)**。
**步骤 7** 点击**将事件发送到云 (Send Events to the Cisco Cloud)** 切换按钮以启用或禁用配置。
**步骤 8** 点击**保存 (Save)**。

# 安全事件连接器

安全事件连接器 (SEC) 是安全分析和日志记录 SaaS 解决方案的一个组件。它接收来自 ASA 和 FDM 管理 设备的事件，并将其转发到思科云。 CDO 在“事件日志记录”(Event Logging) 页面上显示事件，以便管理员可以在该页面或使用 Cisco Secure Cloud Analytics 进行分析。

SEC 安装在您的网络中部署的安全设备连接器上，安装在您的网络中部署的自己的CDO连接器虚拟机上，或安装在 AWS 虚拟私有云 (VPC) 上。

### 安全事件连接器 ID

与思科 Technical Assistance Center (TAC) 或其他 CDO 支持人员合作时，您可能会需要 SEC 的 ID。该 ID 可在 CDO 的“安全连接器”(Secure Connectors) 页面上找到。要查找 SEC ID，请执行以下操作：

1. 从左侧 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。
2. 点击您要标识的 SEC。
3. SEC ID 是“详细信息”(Details) 窗格中“租户 ID”(Tenant ID) 上方列出的 ID。

相关信息：

- 关于 ASA 的安全分析和日志记录 (SAL SaaS)
- 在 SDC 虚拟机上安装安全事件连接器，第 380 页
- 使用 VM 映像安装 SEC

- 使用 VM 映像安装 SEC
- 使用 Terraform 模块在 AWS VPC 上安装安全事件连接器，第 398 页
- 删除安全事件连接器
- 取消调配思科安全分析和日志记录 (SaaS)

# 安装安全事件连接器

安全事件连接器 (SEC) 可以安装在有或没有 SDC 的租户上。

您可以在与安全设备连接器相同的虚拟机上安装一个 SEC（如果有）；或者，您可以在网络中维护的 SEC 自己的 CDO 连接器虚拟机上安装 SEC。

请参阅以下介绍各种安装情况的主题：

- 使用 VM 映像安装 SEC，第 390 页
- 使用 CDO 映像安装 SEC，第 383 页
- 使用 Terraform 模块在 AWS VPC 上安装安全事件连接器，第 398 页

# 在 SDC 虚拟机上安装安全事件连接器

安全事件连接器 (SEC) 从 ASA 和 FDM 管理 设备接收事件，并将其转发到思科云。CDO 在“事件日志记录”(Event Logging) 页面上显示事件，以便管理员可以在该页面或使用思科安全云分析进行分析。

您可以在与安全设备连接器相同的虚拟机上安装一个 SEC（如果有）；或者，您可以在网络中维护的 SEC 自己的 CDO 连接器虚拟机上安装 SEC。

本文介绍如何在与 SDC 相同的虚拟机上安装 SEC。如果要安装更多 SEC，请参阅 使用 CDO 映像安装 SEC，第 383 页 或 使用 VM 映像安装 SEC，第 390 页。

### 开始之前

- 购买思科安全和分析日志记录、**日志记录和故障排除**许可证。或者，如果您想先注销思科安全和分析，请登录 CDO，然后在主导航栏上，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)** 并点击**请求试用 (Request Trial)**。您还可以购买 **日志记录 分析和检测 (Logging Analytics and Detection)** 以及 **全面网络分析和监控 (Total Network Analytics and Monitoring)** 许可证，以将安全云分析应用于事件。
- 确保您的 SDC 已安装。如果需要安装 SDC，请执行以下程序之一：
  - 使用 CDO 的 VM 映像部署安全设备连接器
  - 在您自己的虚拟机上部署安全设备连接器

注释 如果您在自己的虚拟机上安装了本地 SDC，则需要进行您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置才能允许事件到达它。

- 确保 SDC 与 CDO 通信：
  1. 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。
  2. 在安装 SEC 之前，请确保 SDC 的最后一次心跳不超过 10 分钟，并且 SDC 的状态为活动。
- 系统要求 - 为运行 SDC 的虚拟机分配额外的 CPU 和内存：
  - CPU：分配**额外** 4 个 CPU 以容纳 SEC，使 CPU 总数达到 6 个。
  - 内存：为 SEC 分配**额外** 8 GB 内存，使内存总量达到 10 GB。

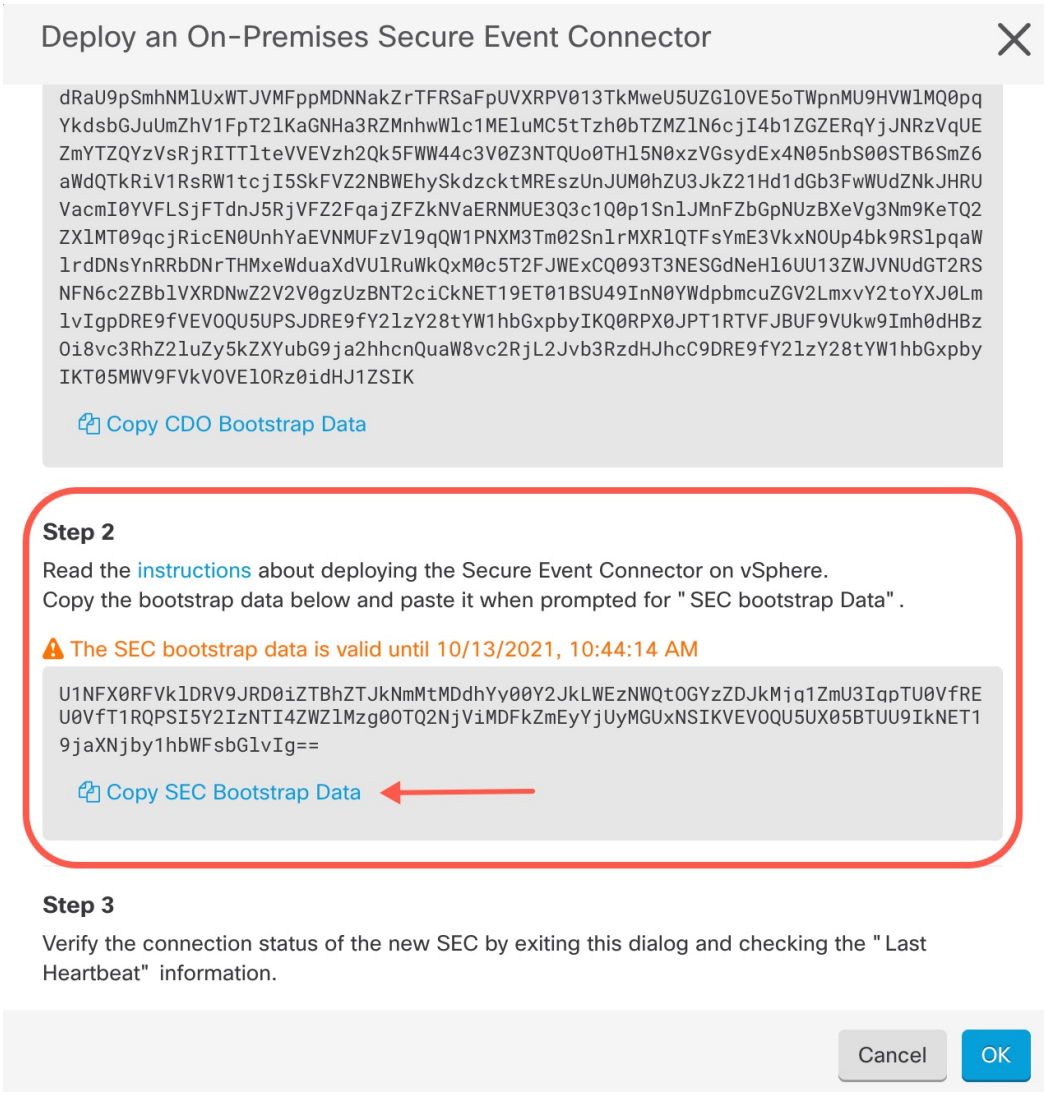
    更新 VM 上的 CPU 和内存以适应 SEC 后，打开 VM 并确保“安全连接器”页面指示 SDC 处于“活动”状态。

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 点击蓝色加号按钮，然后点击**安全事件连接器 (Secure Event Connector)**。

**步骤 4** 跳过向导的步骤 1，转至步骤 2。在向导的步骤 2 中，点击复制 **SEC 引导程序数据 (Copy SEC Bootstrap Data)**的链接。




**步骤 5** 打开终端窗口并以“cdo”用户身份登录 SDC。

**步骤 6** 登录后，切换到“sdc”用户。当系统提示输入密码时，请输入“cdo”用户的密码。以下是这些命令的示例：

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

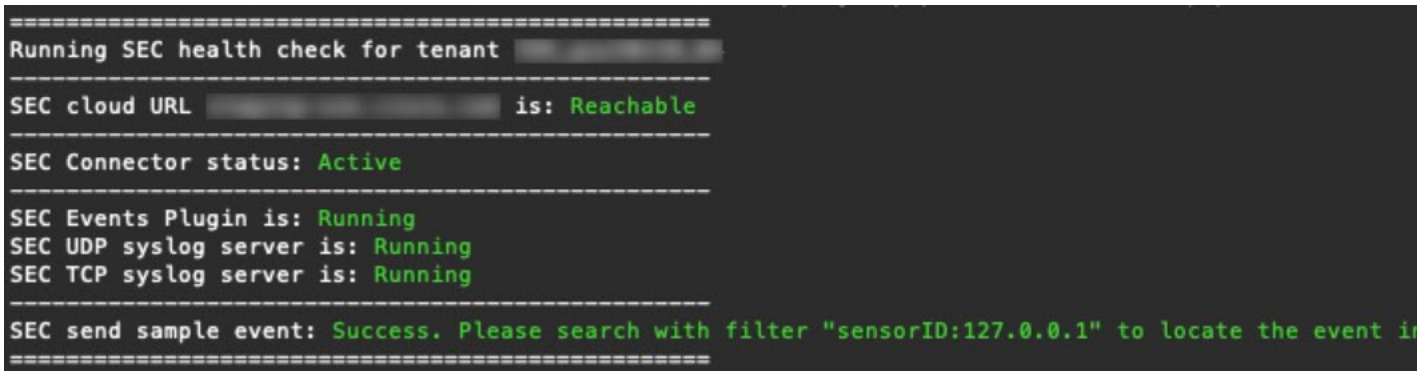
**步骤 7** 在提示符后，运行 **sec.sh setup** 脚本：

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

**步骤 8** 在提示符的末尾，粘贴您在步骤 4 中复制的引导程序数据，然后按 **Enter**键。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

载入 SEC 后，sec.sh 将运行脚本来检查 SEC 的运行状况。如果所有运行状况检查均为“绿色”，则运行状况检查会向事件日志发送示例事件。示例事件在事件日志中显示为名为“sec-health-check”的策略。




如果您收到注册失败或 SEC 载入失败的消息，请转至安全事件连接器载入故障排除。

**步骤 9** 确定运行 SDC 和 SEC 的虚拟机是否需要额外配置：

- 如果您在自己的虚拟机上安装了 SDC，请继续 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 395 页。
- 如果您使用 CDO 映像安装了 SDC，请继续执行“下一步”。

---

**下一步做什么**

退回至 为 ASA 设备实施安全日志记录分析 (SaaS)，第 350 页 。

**相关信息：**

- 对安全设备连接器进行故障排除，第 488 页
- 安全事件连接器故障排除
- 安全事件连接器载入故障排除
- 安全事件连接器注册失败故障排除，第 499 页

# 使用 CDO 映像安装 SEC

安全事件连接器 (SEC) 将事件从 ASA 和 FTD 转发到思科云，以便您可以在“事件日志记录”页面中查看它们，并根据您的许可使用安全云分析进行调查。

您可以在租户上安装多个安全事件连接器 (SEC)，并将事件从您的 ASA 和 FDM 托管的设备定向到您安装的任何 SEC。拥有多个 SEC 可让您将 SEC 安装在不同的位置，并将事件发送到思科云的工作分发给他们。

安装 SEC 的过程分为两部分：

1. 使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器 ，第 384 页 您安装的每个 SEC 都需要一个 CDO 连接器。CDO 连接器不同于安全设备连接器 (SDC)。
2. 在 CDO 连接器虚拟机上安装安全事件连接器 ，第 396 页。

注释 如果要通过创建自己的 VM 来创建 CDO 连接器，请参阅您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置。

**后续操作：**

继续执行 使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器 ，第 384 页

# 使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器

**开始之前**

- 购买思科安全和分析日志记录、**日志记录和故障排除**许可证，您还可以购买**日志记录分析和检测**以及**全面网络分析和监控**许可证，以便将安全云分析应用于事件。

  如果愿意，您还可以登录 CDO，然后在主导航栏中选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)** 并点击**请求试用 (Request Trial)**，以便申请获取试用版的安全分析和日志记录。
- CDO 需要进行严格的证书检查，并且不支持 CDO 连接器和互联网之间的 Web/内容代理检查。如果使用代理服务器，请禁用对 CDO 连接器和 CDO 之间的流量进行检查。
- **此进程中安装的 CDO 连接器必须在 TCP 端口 443 上具有对互联网的完全出站访问权限。**
- **查看** 将 思科防御协调器 连接到托管设备 ，**以便确保 CDO 连接器能够正确访问网络。**
- CDO 支持使用 vSphere Web 客户端或 ESXi Web 客户端来安装其 CDO 连接器 VM OVF 映像。
- CDO 不支持使用 VM vSphere 桌面客户端来安装 CDO 连接器 VM OVF 映像。
- ESXi 5.1 虚拟机监控程序。
- 仅用于托管 CDO 连接器和 SEC 的 VM 的系统要求：
  - VMware ESXi 主机需要 4 个 vCPU。
  - VMware ESXi 主机至少需要 8GB 内存。
  - VMware ESXi 需要 64GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。
- 在开始安装之前收集以下信息：
  - 要用于 CDO 连接器虚拟机的静态 IP 地址。
  - 您在安装过程中创建的 **root** 和 **cdo** 用户的密码。
  - 您的组织使用的 DNS 服务器的 IP 地址。
  - SDC 地址所在网络的网关 IP 地址。

- 时间服务器的 FQDN 或 IP 地址。
- CDO 连接器虚拟机被配置为定期安装安全补丁，为此需要打开出站端口 80。

**步骤 1** 登录到要为其创建 CDO 连接器的 CDO 租户。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 点击蓝色加号按钮，然后点击**安全事件连接器 (Secure Event Connector)**。


**步骤 4** 在步骤 1 中，点击**下载 CDO 连接器虚拟机映像 (Download the CDO Connector VM image)**。这是您在上面安装 SEC 的特殊映像。始终下载 CDO 连接器虚拟机，以确保使用的是最新映像。


**步骤 5** 从 zip 文件中提取所有文件。它们看起来和下面有些相似：

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

**步骤 6** 使用 vSphere Web 客户端以管理员身份登录 VMware 服务器。

**注释** 请勿使用 VM vSphere 桌面客户端。

**步骤 7** 按照相关提示从 OVF 模板部署本地 CDO 连接器虚拟机。（您将需要 .ovf、.mf 和 .vdk 文件才能部署模板。）

**步骤 8** 在设置完成后，打开虚拟机电源。

**步骤 9** 打开新 CDO 连接器虚拟机的控制台。

**步骤 10** 以 **cdo** 用户的身份登录。默认密码为 `adm123`。

**步骤 11** 在提示符处键入 `sudo sdc-onboard setup`

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

**步骤 12** 出现提示时，输入 cdo 用户的默认密码：`adm123`。

**步骤 13** 按照提示为 **root** 用户创建一个新密码。

**步骤 14** 按照提示为 **cdo** 用户创建一个新密码。

**步骤 15** 按照提示输入 Cisco Defense Orchestrator 的域信息。

**步骤 16** 输入您要用于 CDO 连接器虚拟机的静态 IP 地址。

**步骤 17** 输入要在上面安装 CDO 连接器虚拟机的网络的网关 IP 地址。

**步骤 18** 输入 CDO 连接器的 NTP 服务器地址或 FQDN。

**步骤 19** 出现提示时，输入 Docker 网桥的信息，如果不适用，则可将其留空，然后按 <Enter>。

**步骤 20** 确认您的输入内容。

**步骤 21** 当系统提示“您想立即设置 SDC 吗？”(Would you like to setup the SDC now?) 时输入 **n**。

**步骤 22** 以 **cdo** 用户身份登录，以便创建与 CDO 连接器的 SSH 连接。

**步骤 23** 在提示符处键入 **sudo sdc-onboard bootstrap**

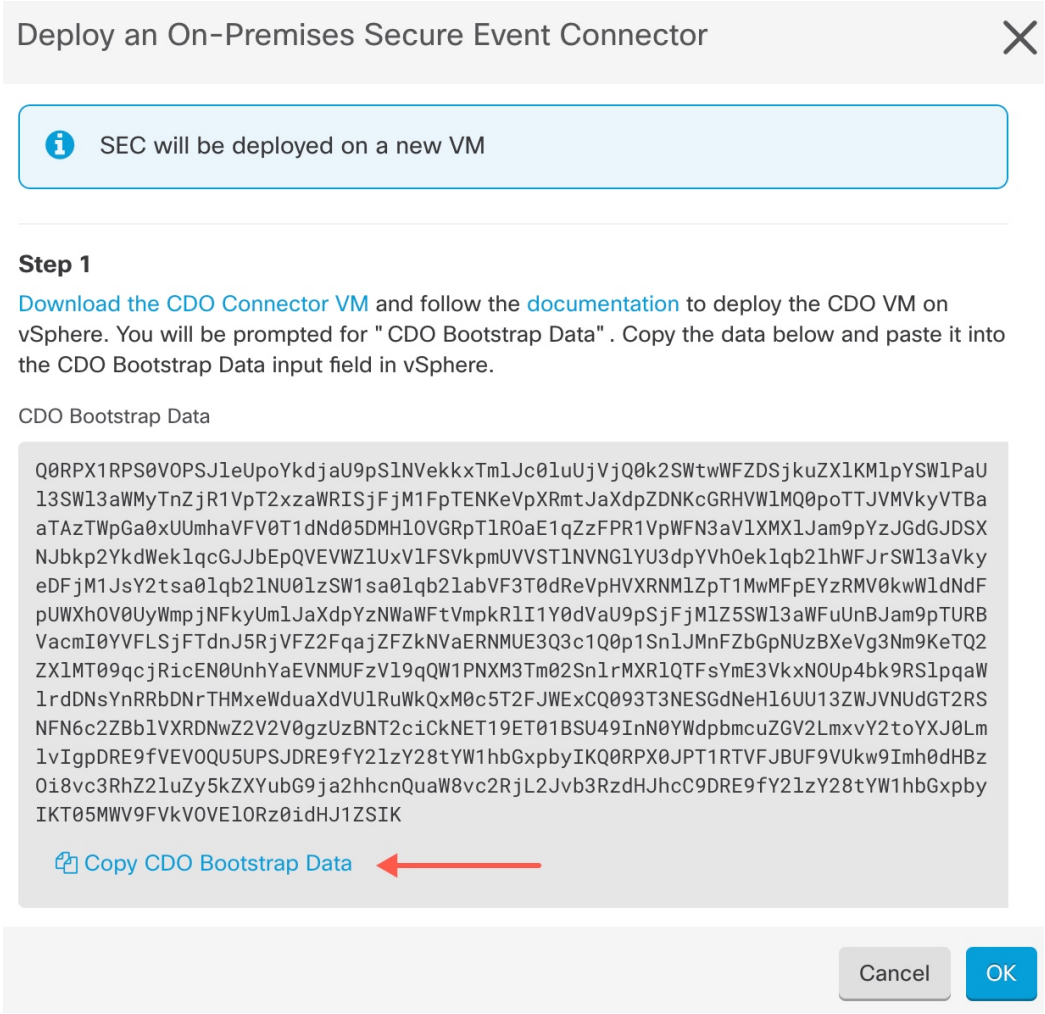
```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

**步骤 24** 在出现提示时，请输入 cdo 用户的密码。

**步骤 25** 在出现提示时，返回 CDO 并复制 CDO 引导程序数据，然后将其粘贴到 SSH 会话中。要复制 CDO 引导程序数据，请执行以下操作：

1. 登录 CDO。
2. 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。
3. 选择您开始载入的安全事件连接器。状态应显示为“正在载入”(Onboarding)。
4. 在“操作”(Actions) 窗格中，点击**部署本地安全事件连接器 (Deploy an On-Premises Secure Event Connector)**。

5. 复制对话框步骤 1 中的 CDO 引导程序数据。




**步骤 26** 当系统提示**您是否要更新这些设置时？(Would you like to update these settings?)** 输入 **n**。

**步骤 27** 返回 CDO 中的“部署本地安全事件连接器对话框”(Deploy an On-Premises Secure Event Connector)，然后点击**确定 (OK)**。在“安全连接器”(Secure Connectors) 页面上，您会看到安全事件连接器处于黄色的正在载入状态。

### 下一步做什么

请继续在 CDO 连接器虚拟机上安装安全事件连接器，第 387 页。

## 在 CDO 连接器虚拟机上安装安全事件连接器

### 开始之前

您应该已安装 CDO 连接器虚拟机，如使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器，第 384 页中所述。

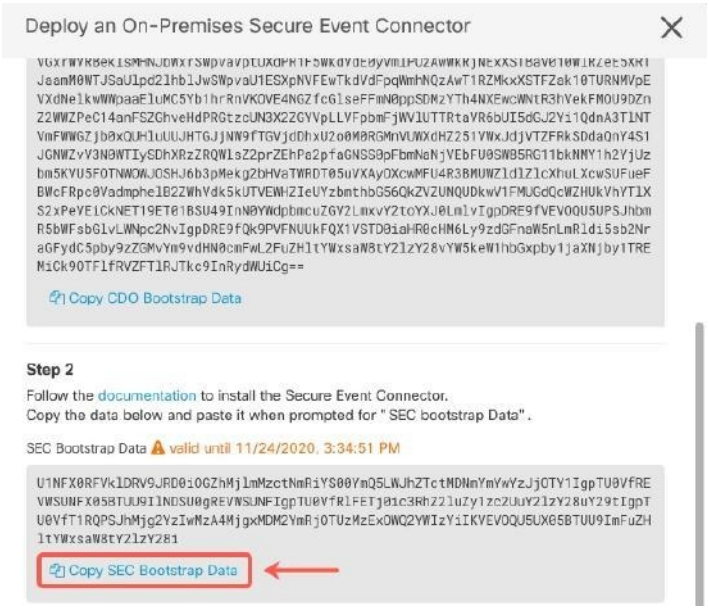
**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 选择您在上面载入的CDO连接器。在“安全连接器”(Secure Connectors)表中，它将被称为“安全事件连接器”，并且应仍处于“正在载入”状态。

**步骤 4** 点击右侧“操作”(Actions) 窗格中的**部署现场安全事件连接器 (Deploy an On-Premises Secure Event Connector)**。

**步骤 5** 在向导的**步骤 2** 中，点击**复制 SEC 引导程序数据 (Copy SEC bootstrap data)** 的链接。




**步骤 6** 创建与 CDO 连接器的 SSH 连接，并以 **cdo** 用户身份登录。

**步骤 7** 登录后，切换到 **sdc** 用户。当系统提示输入密码时，请输入“cdo”用户的密码。以下是这些命令的示例：

```
[cdo@sdc-vm ~]$ sudo su sdc
 [sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

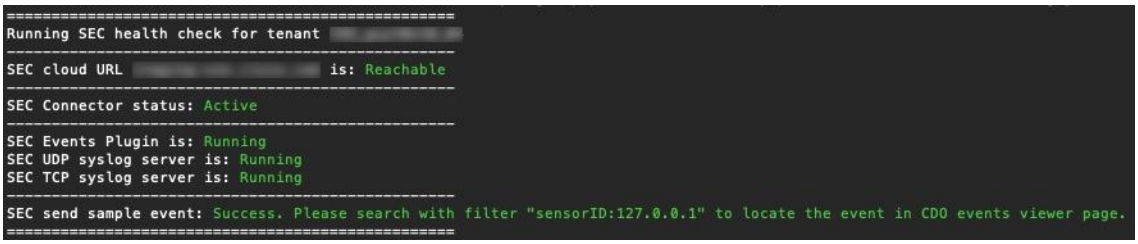
**步骤 8** 在提示符后，运行 sec.sh 安装脚本：

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

**步骤 9** 在提示符的末尾，粘贴您在步骤 4 中复制的引导程序数据，然后按 **Enter**键。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

载入 SEC 后，sec.sh 将运行脚本来检查 SEC 的运行状况。如果所有运行状况检查均为“绿色”，则运行状况检查会向事件日志发送示例事件。示例事件在事件日志中显示为名为“sec-health-check”的策略。




如果您收到注册失败或 SEC 载入失败的消息，请转至安全事件连接器载入故障排除， 第 496 页。

如果您收到成功消息，请返回 CDO 并点击**完成部署现场安全事件连接器 (Done on the Deploy an ON-Premise Secure Event Connector)** 对话框。

**步骤 10** 继续“下一步做什么。"

### 下一步做什么

退回至 为 ASA 设备实施安全日志记录分析 (SaaS)， 第 350 页 。

相关信息：

- 对安全设备连接器进行故障排除， 第 488 页
- 安全事件连接器故障排除， 第 496 页
- 安全事件连接器载入故障排除， 第 496 页

# 在 Ubuntu 虚拟机上部署安全事件连接器

### 开始之前

您应该已按照 在 Ubuntu 虚拟机上部署 安全设备连接器 和安全事件连接器， 第 18 页 中的说明在 Ubuntu VM 上安装了 安全设备连接器。

**步骤 1** 登录 CDO。

**步骤 2** 选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 在**服务 (Services)** 页面上，选择**安全连接器 (Secure Connectors)** 选项卡，点击  ，然后选择**安全事件连接器 (Secure Event Connector)**。

**步骤 4** 将窗口中步骤 2 中的 SEC 引导程序数据复制到记事本。

**步骤 5** 执行以下命令：

```
[sdc@vm]:~$sudo su sdc
sdc@vm:/home/user$ cd /usr/local/cdo/toolkit
```

出现提示时，请输入您复制的 SEC 引导程序数据。

```
sdc@vm:~/toolkit$ ./sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
Successfully on-boarded SEC
```

安全事件连接器可能需要几分钟才能在 CDO 中变为“活动”状态。

# 使用 VM 映像安装 SEC

安全事件连接器 (SEC) 将事件从 ASA 和 FTD 转发到思科云，以便您可以在“事件日志记录”页面中查看它们，并根据您的许可使用安全云分析进行调查。

您可以在租户上安装多个安全事件连接器 (SEC)，并将事件从您的 ASA 和 FDM 托管的 设备定向到您安装的任何 SEC。拥有多个 SEC 可让您在不同区域安装 SEC，并将事件发送到思科云的工作分发给他们。

使用您自己的 VM 映像安装多个 SEC 的过程分为三部分。您必须执行以下每个步骤：

1. 使用 VM 映像安装 CDO 连接器以支持 SEC， 第 390 页
2. 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置， 第 395 页
3. 在 CDO 连接器虚拟机上安装安全事件连接器

**注释** 将 CDO VM 映像用于 CDO 连接器是安装 CDO 连接器的最简单、最准确和首选的方法。如果要使用该方法，请参阅使用 CDO 映像安装 SEC， 第 383 页。

**后续操作：**

请继续使用 VM 映像安装 CDO 连接器以支持 SEC， 第 390 页

## 使用 VM 映像安装 CDO 连接器以支持 SEC

CDO 连接器 VM 是安装 SEC 的虚拟机。CDO 连接器仅用于为思科安全分析和日志记录 (SaaS) 客户提供 SEC 支持。

这是安装和配置安全事件连接器 (SEC) 所需完成的三个步骤中的第一步。完成此程序后，您需要完成以下程序：

- 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置， 第 395 页
- 在 CDO 连接器虚拟机上安装安全事件连接器

**开始之前**

- 购买思科安全和分析日志记录、**日志记录和故障排除**许可证，您还可以购买**日志记录分析和检测**以及**全面网络分析和监控**许可证，以将安全云分析应用于事件。

如果愿意，您还可以登录 CDO，然后在主导航栏中选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)** 并点击**请求试用 (Request Trial)**，以便申请获取试用版的安全分析和日志记录。

- CDO 需要严格的证书检查，并且不支持 CDO 连接器和互联网之间的 Web/内容代理。
- **CDO 连接器必须在 TCP 端口 443 上具有对互联网的完全出站访问权限。**
- **查看** 将 思科防御协调器 连接到托管设备**以确保对 CDO 连接器进行适当的网络访问。**
- 安装了 vCenter Web 客户端或 ESXi Web 客户端的 VMware ESXi 主机。

**注释** 我们不支持使用 vSphere 桌面客户端进行安装。

- ESXi 5.1 虚拟机监控程序。
- Cent OS 7 访客操作系统。
- 仅托管 CDO 连接器和 SEC 的 VM 的系统要求：
  - CPU：分配 4 个 CPU 以容纳 SEC。
  - 内存：为 SEC 分配 8 GB 内存。
  - 磁盘空间：64 GB
- 执行此过程的用户应该能够轻松地在 Linux 环境中使用 **vi** 可视化编辑器编辑文件。
- 如果您在 CentOS 虚拟机上安装 CDO 连接器，我们建议您定期安装 Yum 安全补丁。根据您的 Yum 配置，要获取 Yum 更新，您可能需要在端口 80 和 443 上打开出站访问。您还需要配置 yum-cron 或 crontab 来安排更新。与您的安全运营团队合作，确定是否需要更改任何安全策略以允许您获取 Yum 更新。
- 在开始安装之前收集以下信息：
  - 要用于 CDO 连接器的静态 IP 地址。
  - 您在安装过程中创建的 **root** 和 **cdo** 用户的密码。
  - 您的组织使用的 DNS 服务器的 IP 地址。
  - CDO 连接器地址所在网络的网关 IP 地址。
  - 时间服务器的 FQDN 或 IP 地址。
- CDO 连接器虚拟机被配置为定期安装安全补丁，为此需要打开出站端口 80。
- **开始之前：**不要将本程序中的命令复制并粘贴到终端窗口中，而应键入这些命令。某些命令包括“n-dash”，在剪切和粘贴过程中，这些命令可以作为“m-dash”应用，这可能会导致命令失败。

**步骤 1** 在安全设备连接器页面中，点击蓝色加号按钮  ，然后点击安全事件连接器。

**步骤 2** 使用提供的链接，复制“部署现场安全事件连接器”(Deploy an On-Premises Secure Event Connector) 窗口的步骤 2 中的 SEC 引导程序数据。

**步骤 3** 安装 CentOS 7 虚拟机 (http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso)，其内存、CPU 和磁盘空间至少应符合此程序的要求。

**步骤 4** 安装后，配置基本网络，例如指定 CDO 连接器的 IP 地址、子网掩码和网关。

**步骤 5** 配置 DNS（域名服务器）服务器。

**步骤 6** 配置 NTP（网络时间协议）服务器。

**步骤 7** 在 CentOS 上安装 SSH 服务器，以便与 CDO 连接器的 CLI 轻松交互。

**步骤 8** 运行 yum 更新，然后安装软件包： **open-vm-tools**、 **nettools** 和 **bind-utils**

```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

**步骤 9** 安装 **AWS CLI 软件包** (https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html)

**注释** 请勿使用 `--user` 标志。

**步骤 10** 安装 **Docker CE 软件包** (https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce)

**注释** 使用“使用存储库安装”方法。

**步骤 11** 启动 Docker 服务并使其在启动时启动：

```
[root@sdc-vm ~]# systemctl start docker
 [root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
/usr/lib/systemd/system/docker.service.
```

**步骤 12** 创建两个用户： **cdo** 和 **sdc**。cdo 用户将是您登录以运行管理功能的用户（因此您无需直接使用 root 用户），sdc 用户将是运行 CDO 连接器 docker 容器的用户。

```
[root@sdc-vm ~]# useradd cdo
 [root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

**步骤 13** 配置 sdc 用户以使用 crontab：

```
[root@sdc-vm ~]# touch /etc/cron.allow
[root@sdc-vm ~]# echo "sdc" >> /etc/cron.allow
```

**步骤 14** 为 cdo 用户设置密码。

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

**步骤 15** 将 cdo 用户添加到“wheel”组，为其提供管理 (sudo) 权限。

```
[root@sdc-vm ~]# usermod -aG wheel cdo
 [root@sdc-vm ~]#
```

**步骤 16** 安装 Docker 时，会创建一个用户组。根据 CentOS/Docker 的版本，它可能被称为“docker”或“dockerroot”。检查 /etc/group 文件以查看创建的组，然后将 sdc 用户添加到此组。

```
 [root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

**步骤 17** 如果 `/etc/docker/daemon.json` 文件不存在，请创建该文件，并使用以下内容填充。创建后，重新启动 Docker 后台守护程序。

**注释** 确保在 "组" 项中输入的组名称与步骤 16匹配。

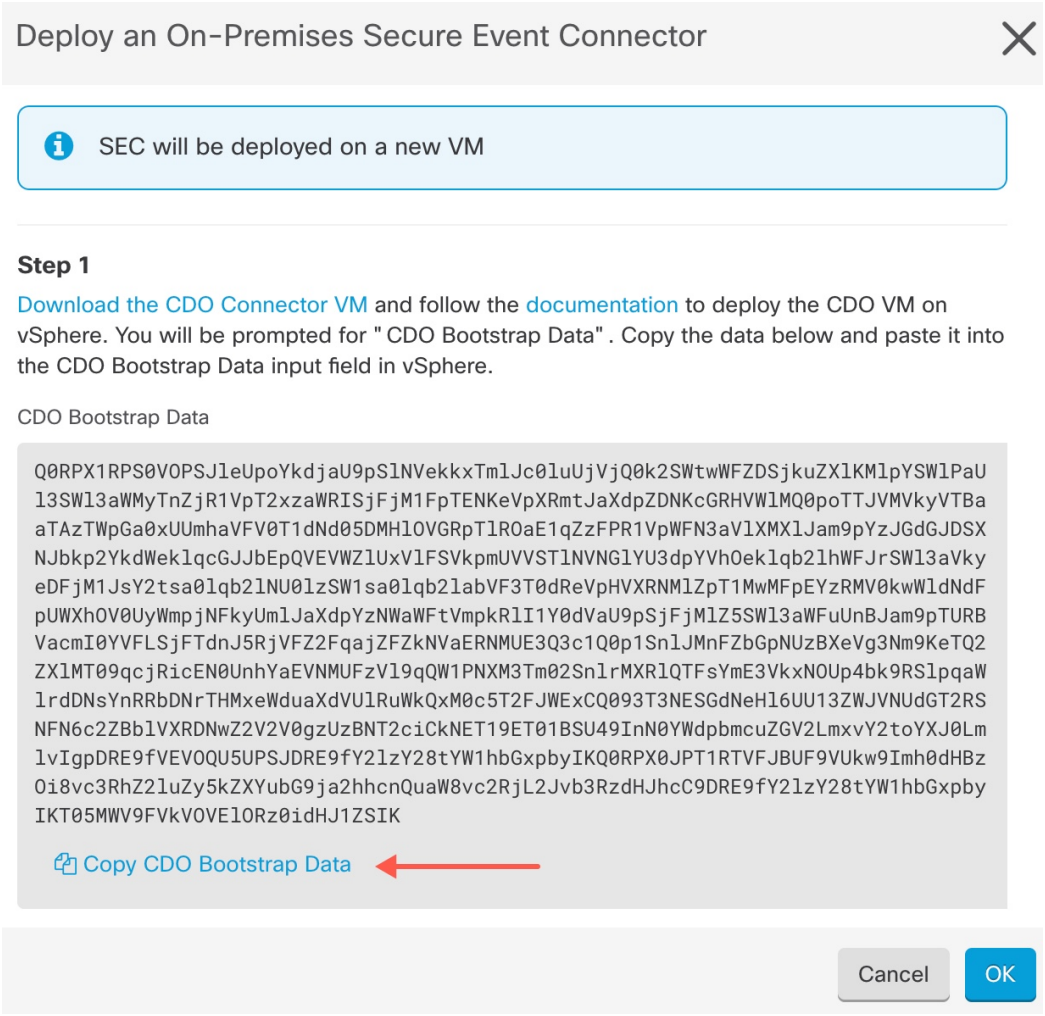
```
 [root@sdc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

**步骤 18** 如果您当前使用的是 vSphere 控制台会话，请切换到 SSH 并以 **cdo** 用户身份登录。登录后，更改为 **sdc** 用户。当系统提示输入密码时，请输入 **cdo** 用户的密码。

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

**步骤 19** 将目录更改为 **/usr/local/cdo**。

**步骤 20** 创建一个名为 **bootstrapdata** 的新文件，并将部署向导步骤 1 中的引导程序数据粘贴到此文件中。**保存**文件。您可以使用 **vi** 或 **nano** 创建该文件。




**步骤 21** 引导程序数据采用 base64 编码。对其进行解码并将其导出到名为 **extractedbootstrapdata** 的文件

```
 [sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata > /usr/local/cdo/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

运行 cat 命令以查看解码后的数据。命令和解码后的数据应如下所示：

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
CDO_TOKEN="<token string>"
CDO_DOMAIN="www.defenseorchestrator.com"
CDO_TENANT="<tenant-name>"
<CDO_URL>/sdc/bootstrap/CDO_acm="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

**步骤 22** 运行以下命令，将解码的引导程序数据部分导出到环境变量。

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > secenv && source secenv
[sdc@sdc-vm ~]$
```

**步骤 23** 从 CDO 下载引导程序捆绑包。

```
[sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL" -o $CDO_TENANT.tar.gz

100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/CDO_<tenant_name>
```

**步骤 24** 解压缩 CDO 连接器 tarball，并运行 bootstrap_sec_only.sh 文件以安装 CDO 连接器软件包。

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/cdo/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/cdo/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

### 下一步做什么

请继续 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 395 页。

## 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置

如果您在自己的 CentOS 7 虚拟机上安装了 CDO 连接器，则需要执行以下附加配置程序**之一**，以允许事件到达 SEC。

- 在 CentOS 7 虚拟机上禁用 firewalld 服务。这与思科提供的 SDC VM 的配置相匹配。
- 允许 firewalld 服务运行并添加防火墙规则以允许事件流量到达 SEC，第 396 页。这是一种允许入站事件流量的更精细的方法。

### 准备工作：

这是安装和配置 SEC 所需完成的三个步骤中的第二步。如果尚未完成这些配置，请完成使用 VM 映像安装 CDO 连接器以支持 SEC，第 390 页。

完成此处所述的其中一项其他配置更改后，请完成在 CDO 连接器虚拟机上安装安全事件连接器

### 在 CentOS 7 虚拟机上禁用 firewalld 服务

1. 以“cdo”用户身份登录 SDC VM 的 CLI。

2. 停止 firewalld 服务，然后确保该服务在 VM 后续重新启动时保持禁用。如果系统提示，请输入 **cdo** 用户的密码：

```
[cdo@SDC-VM ~]$ sudo systemctl stop firewalld
cdo@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. 重新启动 Docker 服务，以便将 Docker 特定条目重新插入本地防火墙：

```
[cdo@SDC-VM ~]$ sudo systemctl restart docker
```

4. 继续在 CDO 连接器虚拟机上安装安全事件连接器。

#### 允许 firewalld 服务运行并添加防火墙规则以允许事件流量到达 SEC

1. 以“cdo”用户身份登录 SDC VM 的 CLI。
2. 添加本地防火墙规则，以便允许从配置的 TCP、UDP 或 NSEL 端口到 SEC 的传入流量。有关 SEC 使用的端口，请参阅查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口。如果系统提示，请输入 **cdo** 用户的密码。以下是命令的示例。您可能需要指定不同的端口值。

```
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10425/udp
```

3. 重新启动 firewalld 服务，以便让新的本地防火墙规则始终保持激活：

```
[cdo@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. 继续在 CDO 连接器虚拟机上安装安全事件连接器。

## 在 CDO 连接器虚拟机上安装安全事件连接器

### 开始之前

这是安装和配置安全事件连接器 (SEC) 所需完成的三个步骤中的第三步。如果尚未完成，请先完成以下两项任务，然后再继续执行此程序：

- 使用 VM 映像安装 CDO 连接器以支持 SEC，第 390 页
- 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 395 页

---

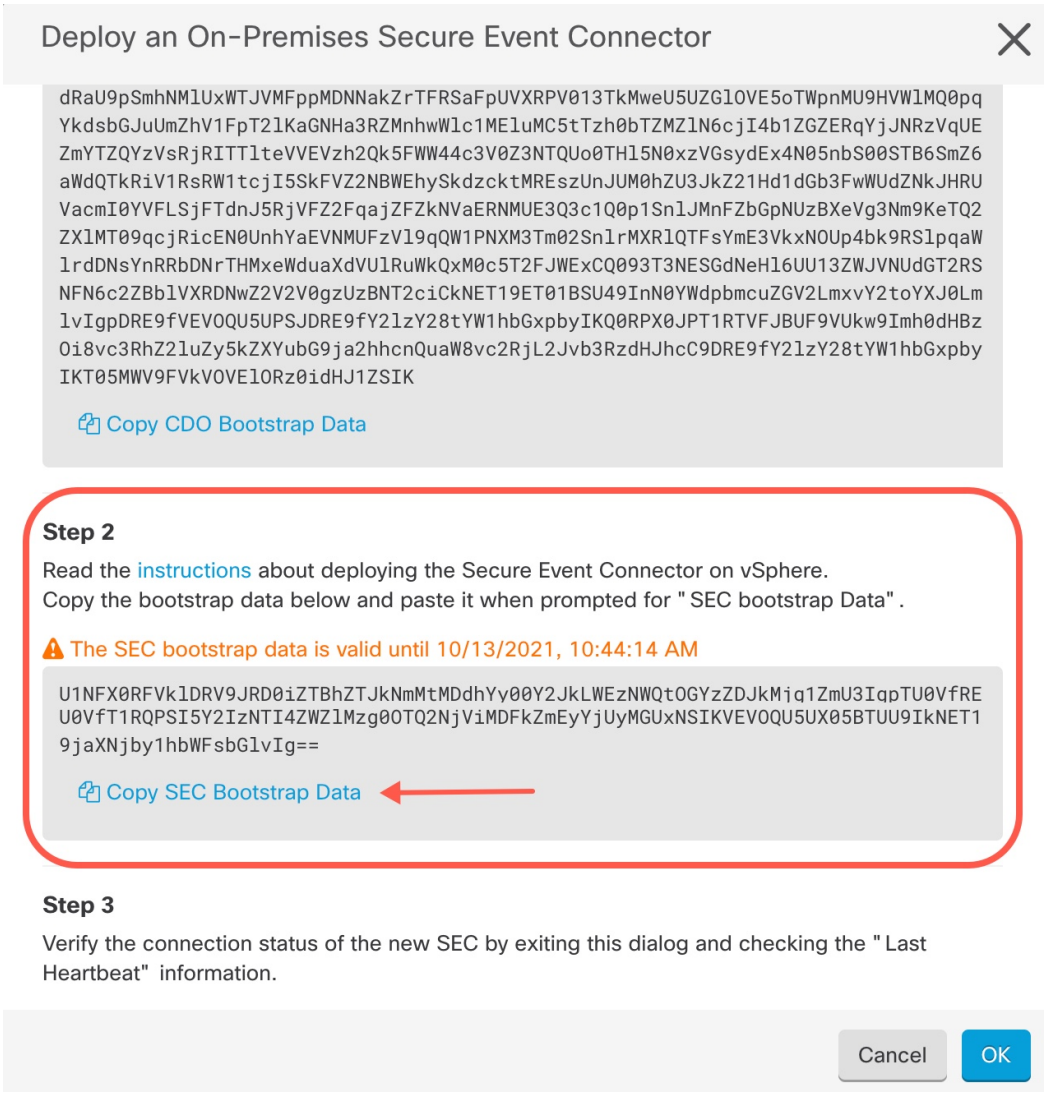
**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 选择您使用上述必备条件中的程序安装的CDO连接器。在“安全连接器”(Secure Connectors) 表中，它将被称为“安全事件连接器”(Secure Event Connector)。

**步骤 4** 点击右侧“操作”窗格中的 **部署现场安全事件连接器** 。

**步骤 5** 在向导的 **步骤 2** 中，点击**复制 SEC 引导程序数据 (Copy SEC Bootstrap Data)** 的链接。




**步骤 6** 使用 SSH 连接到安全连接器并以 **cdo** 用户身份登录。

**步骤 7** 登录后，切换到 **sdc** 用户。当系统提示输入密码时，请输入“cdo”用户的密码。以下是这些命令的示例：

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

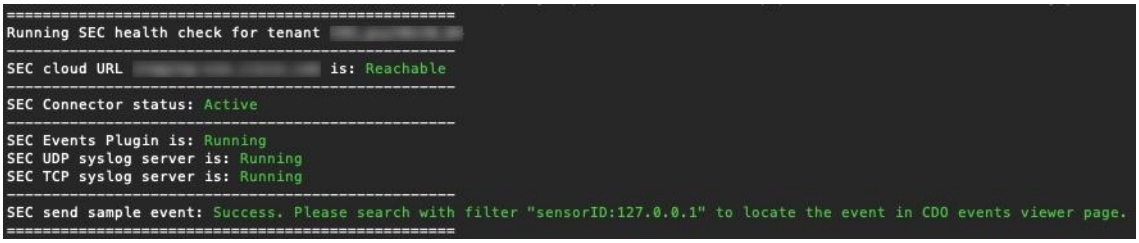
**步骤 8** 在提示符后，运行 sec.sh 安装脚本：

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

**步骤 9** 在提示符的末尾，粘贴您在步骤 4 中复制的引导程序数据，然后按 **Enter**键。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

载入 SEC 后，sec.sh 将运行脚本来检查 SEC 的运行状况。如果所有运行状况检查均为“绿色”，则运行状况检查会向事件日志发送示例事件。示例事件在事件日志中显示为名为“sec-health-check”的策略。




如果您收到注册失败或 SEC 载入失败的消息，请转至安全事件连接器故障排除。

如果您收到成功消息，请点击**部署现场安全事件连接器 (Deploy an ON-Premise Secure Event Connector)** 对话框中的**完成 (Done)**。您已在虚拟机映像上安装 SEC。

**步骤 10** 继续执行 “**下一步操作**”。

---

**下一步做什么**

返回此程序以继续实施 SAL SaaS： 为 ASA 设备实施安全日志记录分析 (SaaS)，第 350 页 。

**相关信息：**

- 对安全设备连接器进行故障排除，第 488 页
- 安全事件连接器故障排除
- 安全事件连接器载入故障排除
- 安全事件连接器注册失败故障排除

# 使用 Terraform 模块在 AWS VPC 上安装安全事件连接器

**开始之前**

- 要执行此任务，您必须在 CDO 租户上启用 SAL。本部分假定您已拥有 SAL 许可证。如果还没有，请购买思科安全和分析日志记录、日志记录和故障排除许可证。
- 确保您已安装新的 SEC。要创建新的 SEC，请参阅在 SDC 虚拟机上安装安全事件连接器，第 380 页。
- 在安装 SEC 时，请确保记下 CDO 引导程序数据和 SEC 引导程序数据。

---

**步骤 1** 转到 Terraform 注册表中的安全事件连接器 Terraform 模块，然后按照说明将 SEC Terraform 模块添加到 Terraform 代码。

**步骤 2** 应用 Terraform 代码。

**步骤 3** 确保打印 `instance_id` 和 `sec_fqdn` 输出，因为稍后在程序中会用到它们。

**注释** 要对 SEC 进行故障排除，您必须使用 AWS 系统管理器会话管理器 (SSM) 来连接到 SEC 实例。请参阅 AWS 系统管理器会话管理器文档，了解有关使用 SSM 连接到实例的更多信息。

出于安全原因，使用 SSH 连接到 SDC 实例的端口不会被公开。

**步骤 4** 要启用从 ASA 向 SEC 发送日志的功能，请使用步骤 3 的输出来运行以下命令，以获取您创建的 SEC 的证书链并删除枝叶证书：

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 < /dev/null
| awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++}; out="/tmp/cert_chain.pem";
 if(a > 1) print >>out}'
```

**步骤 5** 将 `/tmp/cert_chain.pem` 的内容复制到剪贴板。

**步骤 6** 使用以下命令记录 SEC 的 IP 地址：

```
nslookup <FQDN>
```

**步骤 7** 登录 CDO 并开始添加新的信任点对象。有关详细信息，请参阅添加受信任 CA 证书对象。在点击**添加 (Add)**，请确保取消选中**其他选项 (Other Options)** 中的**在基本限制扩展中启用 CA 标志 (Enable CA flag in basic constraints extension)** 复选框。

**步骤 8** 点击**添加 (Add)**，复制 CDO 生成的 CLI 命令在**安装证书 (Install Certificate)** 页面中，然后点击**取消 (Cancel)**。

**步骤 9** 在`注册终端 (enrollment terminal)` 下方，在文本剪贴板中添加 `no ca-check`。

**步骤 10** 通过 SSH 连接到 ASA 设备或使用 CDO 中的 ASA CLI 选项并执行以下命令：

```
DataCenterFW-1> en
Password: *****************
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

### 下一步做什么

您可以使用 AWS SSM 来检查 SEC 是否正在接收数据包：

您现在应该会看到类似于以下内容的日志：

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
 plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

# 取消调配思科安全分析和日志记录 (SaaS)

如果允许思科安全分析和日志记录 (SaaS) 付费许可证失效，则您有 90 天的宽限期。如果您在此宽限期内续订付费许可证，则服务不会发生中断。

否则，如果您允许 90 天的宽限期，系统将清除所有的客户数据。您无法再从“事件日志记录”(Event Logging) 页面查看 ASA 或 FTD 事件，也无法将动态实体建模行为分析应用于您的 ASA 或 FTD 事件和网络流数据。

# 删除安全事件连接器

**警告**：此程序会从安全设备连接器中删除安全事件连接器。这样做会阻止您使用安全日志分析(SaaS)。这一操作不可逆。如果您有任何问题或疑虑，请在执行此操作之前联系思科威胁防御支持。

从安全设备连接器中删除安全事件连接器的过程可分为两步：

1. 从 CDO 中删除 SEC。
2. 从 SDC 中删除 SEC 文件。

**下一步**：继续从 CDO 中删除 SEC

# 从 CDO 中删除 SEC

### 开始之前

请参阅删除安全事件连接器， 第 400 页。

**步骤 1** 登录 CDO。

**步骤 2** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 3** 选择设备类型为**安全事件连接器 (Secure Event Connector)** 的行。

**警告**：要小心。请勿选择您的安全设备连接器。

**步骤 4** 在“操作”(Actions) 窗格中，点击**删除 (Remove)**。

**步骤 5** 点击**确定 (OK)** 以确认您删除安全事件连接器的意图。

### 下一步做什么

请继续从 SDC 中删除 SEC 文件， 第 400 页。

# 从 SDC 中删除 SEC 文件

这是从 SDC 中删除安全事件连接器程序的第二部分。开始前，请参阅删除安全事件连接器， 第 400 页 。

**步骤 1** 打开虚拟机监控程序并启动 SDC 的控制台会话。

**步骤 2** 切换到 SDC 用户。

```
[cdo@tenant toolkit]$sudo su sdc
```

**步骤 3** 在提示符后键入以下命令之一：

- 如果您仅管理自己的租户：

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
```

- 如果您管理多个租户，请将 CDO_ 添加到租户名称的开头。例如：

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
```

**步骤 4** 确认您打算删除 SEC 文件。

# 调配思科安全云分析门户

**所需许可证： 日志记录分析和检测 或 全面网络分析和监控**

如果您购买了**日志记录分析和检测**或**全局网络分析和监控**许可证，则在部署和配置安全事件连接器 (SEC) 后，必须将安全云分析门户与 CDO 门户关联，以查看安全云分析警报。购买许可证时，如果您有安全云分析门户，则可以提供安全云分析门户名称，并立即将其链接到您的 CDO 门户。

否则，您可以从 CDO UI 请求新的安全云分析门户。首次访问安全云分析警报时，系统会将您引导至请求安全云分析门户的页面。向请求此门户的用户授予门户中的管理员权限。

**步骤 1** 从 CDO 菜单中，选择 **分析 (Analytics)** > **安全云分析 (Secure Cloud Analytics)** 以在新窗口中打开安全云分析 UI。

**步骤 2** 点击**开始免费试用 (Start Free Trial)** 以调配安全云分析门户并将其与您的 CDO 门户关联。

**Note** 请求门户后，调配可能需要几个小时。

在继续下一步之前，请确保您的门户已调配。

1. 从 CDO 菜单中，选择 **分析 (Analytics)** > **安全云分析 (Secure Cloud Analytics)** 以在新窗口中打开安全云分析 UI。
2. 您有以下选择：
   - 如果您请求了安全云分析门户，并且系统指出它仍在调配门户，请稍后再尝试访问警报。
   - 如果已调配安全云分析门户，请输入您的**用户名**和**密码**，然后点击**登录 (Sign in)**。

**Note** 管理员用户可以邀请其他用户在安全云分析门户中创建账户。有关详细信息，请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 403。

### What to do next

- 如果您购买了**日志记录分析和检测**许可证，则配置已完成。如果要从安全云分析门户 UI 查看 CDO 集成状态或传感器运行状况，请参阅在安全云分析中查看传感器运行状况和 CDO 集成状

态, on page 402了解更多信息。如果要使用安全云分析门户中的警报，请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 403和使用基于防火墙事件的警报以了解详细信息。

- 如果您购买了**全面网络分析和监控**许可证，请将一个或多个安全云分析传感器部署到您的内部网络，以将网络流数据传递到云。如果要监控基于云的网络流数据，请将基于云的部署配置为将流数据传递到安全云分析。有关详细信息，请参阅用于全面网络分析和报告的思科安全云分析传感器部署, on page 402。

# 在安全云分析中查看传感器运行状况和 CDO 集成状态

**传感器状态**

**所需许可证： 日志记录分析和检测 或 全面网络分析和监控**

在思科安全云分析 Web UI 中，您可以从“传感器列表”(Sensor List) 页面查看 CDO 集成状态和已配置的传感器。CDO 集成是只读连接事件传感器。Stelathwatch 云在主菜单中提供传感器的整体运行状况：

- 绿色云图标 ( ) - 已与所有传感器和 CDO（如果已配置）建立连接
- 黄色云图标 ( ) - 已与某些传感器或 CDO（如果已配置）建立连接，但一个或多个传感器未正确配置
- 红色云图标 ( ) - 与所有已配置的传感器和 CDO（如果已配置）的连接丢失

每个传感器或 CDO 集成，绿色图标表示连接已建立，红色图标表示连接丢失。

**步骤 1** 1. 在安全云分析门户 UI 中，选择设置 ( ) > **传感器 (Sensors)**。

**步骤 2** 选择**传感器列表 (Sensor List)**。

# 用于全面网络分析和报告的思科安全云分析传感器部署

**安全云分析传感器概述和部署**

**所需许可证：全面网络分析和监控**

如果您获得了**全面网络分析和监控**许可证，则在调配安全云分析门户后，您可以：

- 在本地网络中部署和配置安全云分析传感器，以将网络流数据传递到云进行分析。
- 配置基于云的部署，以将网络流日志数据传递到安全云分析进行分析。

网络边界的防火墙收集有关内部网络和外部网络之间流量的信息，而安全云分析传感器收集有关内部网络流量的信息。

**Note** FDM 管理Secure Firewall Threat Defense 设备可以配置为传递 NetFlow 数据。部署传感器时，请勿将其配置为从您还配置为将事件信息传递到 CDO 的任何 FDM 管理Secure Firewall Threat Defense 设备传递 NetFlow 数据。

有关传感器部署说明和建议，请参阅《安全云分析传感器安装指南》。

有关基于云的部署配置说明和建议，请参阅《安全云分析公共云监控指南》。

**Note** 您还可以查看安全云分析门户 UI 中的说明，以配置传感器和基于云的部署。

有关安全云分析的详细信息，请参阅《安全云分析免费试用指南》。

### 后续步骤

- 继续执行从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 403。

# 从 CDO 查看 Cisco Secure Cloud Analytics 警报

**所需许可证： 日志记录分析和检测 或 全面网络分析和监控**

虽然您可以在“事件日志记录”(Events logging) 页面上查看防火墙事件，但无法从 CDO 门户 UI 中查看 Cisco Secure Cloud Analytics 警报。您可以使用“安全分析”(Security Analytics) 菜单选项从 CDO 交叉启动安全云分析门户，并查看从防火墙事件数据（如果启用了**全面网络分析和监控 (Total Network Analytics and Monitoring)**，则从网络流数据）生成的警报。“安全分析”(Security Analytics) 菜单选项会显示一个标记，其中包含处于打开的工作流程状态的安全云分析警报的数量（如果有一个或多个）。

如果您使用安全分析和日志记录许可证生成安全云分析警报，并且已调配新的安全云分析门户，请登录 CDO，然后使用 Cisco Security Cloud Sign On 来启动安全云分析。您还可以通过其 URL 直接访问安全云分析门户。

有关详细信息，请参阅 Cisco Security Cloud Sign On。

# 邀请用户加入您的安全云分析门户

请求安全云分析门户调配的初始用户在安全云分析门户中具有管理员权限。该用户可以通过邮件邀请其他用户加入门户。如果这些用户没有 Cisco Security Cloud Sign On 凭证，可以使用邀请邮件中的链接创建这些凭证。然后，用户可以在从 CDO 到 Secure Cloud Analytics 的交叉启动期间使用 Cisco Security Cloud Sign On 凭证登录。

要通过邮件邀请其他用户访问 Secure Cloud Analytics 门户，请执行以下操作：

**步骤 1** 以管理员身份登录 Secure Cloud Analytics 门户。

**步骤 2** 选择 Settings Account Management User Management。 > >

**步骤 3** 输入**邮件**地址。

**步骤 4** 点击**邀请 (Invite)**。

# 从 CDO 交叉启动到 Cisco Secure Cloud Analytics

要从 CDO 查看安全警报，请执行以下操作：

**步骤 1** 登录到 CDO 门户。

**步骤 2** 从 CDO 菜单中，选择 **分析 (Analytics)** > **安全云分析 (Secure Cloud Analytics)**。

**步骤 3** 在 Cisco Secure Cloud Analytics 界面中，选择**监控 (Monitor)** > **警报 (Alerts)**。

# 思科安全云分析和动态实体建模

**所需许可证 (Required License)： 日志记录分析和检测 (Logging Analytics and Detection)** 或**全面网络分析和监控 (Total Network Analytics and Monitoring)**

安全云分析是一种软件即服务 (SaaS) 解决方案，可用于监控您的本地和基于云的网络部署。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

## 动态实体建模

动态实体建模可通过对防火墙事件和网络流数据执行行为分析来跟踪网络状态。在 Cisco Secure Cloud Analytics 环境中，实体是指可以随时间推移进行跟踪的对象，例如网络上的主机或终端。动态实体建模根据实体传输的流量及其在网络上执行的活动，收集实体的相关信息。与**日志记录分析和检测**许可证集成的 Cisco Secure Cloud Analytics 可以从防火墙事件和其他流量信息中进行提取，以便确定实体通常传输的流量类型。如果您购买了**全面网络分析和监控**许可证，则 Cisco Secure Cloud Analytics 还可以在对实体流量进行建模时纳入 NetFlow 和其他流量信息。Cisco Secure Cloud Analytics 会随着时间的推移更新这些模型，因为实体会继续发送流量，并且可能会发送不同的流量，从而保持每个实体的最新模型。根据这些信息，Cisco Secure Cloud Analytics 可以识别：

- 实体的角色，即实体通常执行的操作的描述符。例如，如果实体发送通常与邮件服务器关联的流量，Cisco Secure Cloud Analytics 会为该实体分配邮件服务器角色。角色/实体关系可以是多对一，因为实体可以履行多种角色。

- 对实体的观察结果，即有关实体在网络上的行为的事实，例如与外部 IP 地址建立的心跳连接或与另一个实体建立的远程访问会话。如果与 CDO 集成，则可以从防火墙事件中获取这些事实。如果您还购买了**全面的网络分析和监控**许可证，则系统还可以从 NetFlow 获取事实，并从防火墙事件和 NetFlow 中生成观察结果。观察结果本身并不具有超出其所代表的事实的意义。一个典型的客户可能有数千个观察结果和若干个警报。

### 警报和分析

Cisco Secure Cloud Analytics 会根据角色、观察结果和其他威胁情报的组合生成警报，这些警报是可操作项目，代表系统标识的可能的恶意行为。请注意，一个警报可能代表多个观察结果。如果防火墙记录了与同一连接和实体相关的多个连接事件，则可能只会生成一个警报。

例如，新的内部设备观察结果本身并不构成可能的恶意行为。但是，随着时间的推移，如果实体传输的流量与域控制器一致，则系统会向该实体分配域控制器角色。如果实体随后使用异常端口与之前未建立连接的外部服务器建立了连接，并且传输了大量的数据，则系统将记录新的大型连接（外部）观察结果和异常域控制器观察结果。如果该外部服务器被识别为一个 Talos 监视列表，则所有这些信息的组合将导致 Cisco Secure Cloud Analytics 生成此实体行为的警报，从而提示您采取进一步措施来研究和补救恶意行为。

在 Cisco Secure Cloud Analytics Web 门户 UI 中打开警报时，您可以查看导致系统生成该警报的支持性观察结果。您还可以从这些观察结果中查看有关所涉实体的其他背景信息，包括它们传输的流量以及外部威胁情报（如果可用）。您还可以查看实体涉及的其他观察结果和警报，然后确定此行为是否与其他潜在恶意行为相关。

请注意，在 Cisco Secure Cloud Analytics 中查看和关闭警报时，无法允许或阻止来自 Cisco Secure Cloud Analytics UI 的流量。如果在主动模式下部署设备，则必须更新防火墙访问控制规则以允许或阻止流量；如果在被动模式下部署防火墙，则必须更新防火墙访问控制规则。

# 使用基于防火墙事件的警报

**所需许可证： 日志记录分析和检测 或 全面网络分析和监控**

### 警报工作流程

警报的工作流程基于其状态。当系统生成警报时，其默认状态为“待处理”，并且未分配任何用户。当您查看警报总结时，默认情况下会显示所有待处理警报，因为这些是最需要关注的。

注意：如果您拥有**全面网络分析和监控**许可证，则警报可以基于从 NetFlow 生成的观察结果、从防火墙事件生成的观察结果或来自两个数据源的观察结果。

查看警报总结时，可以分配和标记警报，以及将其状态更新为初始分类。您可以使用过滤器和搜索功能查找特定警报，也可以显示不同状态的警报或具有不同标记或负责人的警报。您可以将警报的状态设置为“已暂停”，在这种情况下，警报要等暂停期过后才会重新显示在待处理警报列表中。您也可以移除警报的“已暂停”状态，使其再次显示为待处理警报。查看警报时，您可以将其分配给您自己或系统中的其他用户。用户可以搜索分配给其用户名的所有警报。

在警报摘要中，您可以查看警报详细信息页面。此页面允许您查看有关生成此警报的支持性观察结果的其他背景信息，以及有关此警报中涉及的实体的其他背景信息。这些信息可帮助您查明实际问题，以便进一步研究网络上的问题，并且有可能解决恶意行为。

当您在 CDO 中的 Stealthwatch 云 web 门户 UI 和网络中进行研究时，可以进行备注，描述您对警报的发现。这有助于为您的研究创建记录，供您将来参考。

完成分析后，您可以将状态更新为“已关闭”，使其不再默认显示为待处理警报。如果情况发生变化，您还可以在将来重新打开已关闭的警报。

下面介绍有关如何调查给定警报的一般准则和建议。Stealthwatch 云会在记录警报时提供附加背景信息，因此，您可以使用此信息帮助指导调查工作。

这些步骤既不全面，也非包罗万象。它们仅提供一个总体框架来帮助您开始调查警报。

通常，查看警报时可以采取以下步骤：

1. 对待处理警报进行分类, on page 406
2. 暂停警报以供以后分析, on page 407
3. 更新警报以进行进一步调查, on page 407
4. 查看警报并开始调查, on page 408
5. 检查实体和用户, on page 409
6. 使用安全云分析补救问题, on page 410
7. 更新并关闭警报, on page 410

# 对待处理警报进行分类

对待处理警报进行分类，特别是如果要调查多个待处理警报：

- 有关从 CDO 交叉启动和查看警报的详细信息，请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报。

询问以下问题：

- 您是否将此警报类型配置为高优先级？
- 您是否为受影响的子网设置了高灵敏度？
- 这是网络上新实体的异常行为吗？
- 实体的正常角色是什么，此警报中的行为与该角色的匹配度如何？
- 这是否是此实体正常行为的异常偏离？
- 如果用户参与其中，这是用户的预期行为还是异常行为？
- 受保护数据或敏感数据是否有被泄露的风险？
- 如果允许此行为继续下去，会对网络产生多严重的影响？

- 如果与外部实体有通信，这些实体过去是否与您网络上的其他实体建立了连接？

如果这是高优先级警报，请考虑将该实体与互联网隔离，或以其他方式关闭其连接，然后再继续调查。

# 暂停警报以供以后分析

当警报的优先级较低（与其他警报相比）时，可将其暂停。例如，如果您的组织将邮件服务器重新定位为 FTP 服务器，并且系统生成紧急配置文件警报（表明一个实体的当前流量匹配了它以前没有匹配的行为概要文件），您可以暂停此警报（因为这是预期行为），并在以后重新访问它。已暂停的警报不会与待处理警报一起显示；您必须专门过滤才能查看这些暂停的警报。

暂停警报：

**步骤 1** 点击**关闭警报 (Close Alert)**。

**步骤 2** 在暂停此警报窗格中，从下拉列表中选择暂停时段。

**步骤 3** 点击**保存 (Save)**。

### What to do next

当您准备好查看这些警报时，可以取消暂停该警报。这会将状态设置为“未处理”(Open)，并在其他“未处理”的警报旁边显示该警报。

取消暂停已暂停的警报：

- 从暂停的警报中，点击**取消暂停警报 (Unsnooze Alert)**。

# 更新警报以进行进一步调查

打开警报详细信息：

**步骤 1** 选择**监控 (Monitor)** > **警报 (Alerts)**。

**步骤 2** 点击警报类型名称。

### What to do next

根据您的初始分类和优先级，分配警报并标记：

1. 从**被分派人 (Assignee)** 下拉列表中选择用户以分配警报，以便用户可以开始调查。
2. 从下拉列表中选择一个或多个**标签**，以将标签添加到警报，以便更好地对警报进行分类以供将来识别，并尝试在警报中建立长期模式。

3. 输入为此警报添加注释 **(Comment on this alert)**，然后点击注释 **(Comment)** 以根据需要留下注释，以跟踪您的初始发现，并协助分配到警报的人员。警报同时跟踪系统注释和用户注释。

# 查看警报并开始调查

如果您正在查看已分配的警报，请查看警报详细信息以了解 Stealthwatch 云生成警报的原因。查看支持性观察结果，了解这些观察结果对源实体的意义。

请注意，如果警报是基于防火墙事件生成的，则系统不会注意到您的防火墙部署是此警报的来源。

查看此源实体的所有支持性观察结果，以了解其一般行为和模式，并查看此活动是否可能影响着某个长期趋势：

## SUMMARY STEPS

1. 在观察结果控制面板上，点击观察结果类型旁边的箭头图标 (➔)，以查看该类型的所有已记录观察结果。
2. 点击网络的所有观察结果 **(All Observations for Network)** 旁边的箭头图标 (➔)，查看此警报的源实体的所有已记录观察结果。

## DETAILED STEPS

**步骤 1** 在观察结果控制面板上，点击观察结果类型旁边的箭头图标 (➔)，以查看该类型的所有已记录观察结果。

**步骤 2** 点击网络的所有观察结果 **(All Observations for Network)** 旁边的箭头图标 (➔)，查看此警报的源实体的所有已记录观察结果。

如果要对这些观察结果执行其他分析，请下载逗号分隔值文件中的支持观察结果：

- 在警报详细信息的支持观察结果窗格中，点击 **CSV**。

从观察结果，确定源实体行为是否指示恶意行为。如果源实体与多个外部实体建立了连接，请确定外部实体是否以某种方式相关，例如它们是否都具有相似的地理位置信息，或者它们的 IP 地址是否来自同一子网。

从源实体 IP 地址或主机名称查看有关源实体的其他背景信息，包括它可能涉及的其他警报和观察结果、有关设备本身的信息以及它传输的会话流量类型：

- 从 IP 地址或主机名下拉列表中选择警报 **(Alerts)**，以查看与该实体相关的所有警报。
- 从 IP 地址或主机名下拉列表中选择观察结果 **(Observations)**，以查看与实体相关的所有观察结果。
- 从 IP 地址或主机名下拉列表中选择设备 **(Device)**，以查看有关设备的信息。
- 从 IP 地址或主机名下拉列表中选择会话流量 **(Session Traffic)**，以查看与此实体相关的会话流量。
- 从 IP 地址或主机名下拉列表中选择复制 **(Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的源实体始终位于您的网络内部。将此与防火墙事件中的发起方 IP 进行对比，后者指示发起连接的实体，并且可能位于您的网络内部或外部。

从观察结果中，检查有关其他外部实体的信息。检查地理位置信息，确定是否有任何地理位置数据或 Umbrella 数据标识恶意实体。查看这些实体生成的流量。检查 Talos、AbuseIPDB 或 Google 是否有关于这些实体的任何信息。查找多天的 IP 地址，并查看外部实体与您网络上的实体建立的其他类型的连接。如有必要，请找到这些内部实体，并确定是否有任何证据表明存在攻击活动或意外行为。

查看与源实体建立了连接的外部实体 IP 地址或主机名称的背景信息：

- 从 IP 地址或主机名下拉列表中选择 **IP 流量 (IP Traffic)**，以查看此实体的最近流量信息。
- 从 IP 地址或主机名下拉列表中选择**会话流量 (Session Traffic)**，以查看此实体的最近会话流量信息。
- 从 IP 地址或主机名下拉列表中选择 **AbuseIPDB**，以查看有关 AbuseIPDB 网页实体的信息。
- 从 IP 地址或主机名下拉列表中选择**思科 Umbrella (Cisco Umbrella)**，可在 Cisco Umbrella 网站上查看有关此实体的信息。
- 从 IP 地址或主机名下拉列表中选择 **Google 搜索 (Google Search)**，以在 Google 上搜索此 IP 地址。
- 从 IP 地址或主机名下拉列表中选择 **Talos 智能 (Talos Intelligence)**，以查看有关 Talos 网页的信息。
- 从 IP 地址或主机名下拉列表中选择**将 IP 添加到监视列表 (Add IP to watchlist)**，以将此实体添加到监视列表。
- 从 IP 地址或主机名下拉列表中选择**查找多天的 IP (Find IP on multiple days)**，以搜索此实体上个月的流量。
- 从 IP 地址或主机名下拉列表中选择**复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的连接实体始终位于您的网络外部。将此与防火墙事件中的响应方 IP 进行对比，后者指示响应连接请求的实体，并且可能位于您的网络的内部或外部。

就您的发现进行备注。

- 在警报详细信息中，输入**对此警报的注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

# 检查实体和用户

在 Stealthwatch 云门户 UI 中查看警报后，您可以直接对源实体、可能与此警报相关的任何用户以及其他相关实体执行其他检查。

- 确定源实体在网络上的物理位置或云中的位置，并直接访问它。找到此实体的日志文件。如果它是网络上的物理实体，请访问设备以查看日志信息，并查看是否有任何信息表明是什么导致了此行为。如果它是虚拟实体或存储在云中，请访问日志并搜索与此实体相关的条目。检查日志，了解有关未经授权的登录、未经批准的配置更改等活动的更多信息。

- 检查实体。确定您能否识别实体本身上的恶意软件或漏洞。查看是否发生了一些恶意更改，包括设备是否发生了物理更改，例如插入了未经组织批准的 U 盘。
- 确定所涉及的用户来自您的网络内部还是外部。如果可能，询问他们当时在做什么。如果询问未果，请确定他们是否应该具有访问权限，以及是否发生了导致此行为的情况，例如，离职员工在离开公司之前将文件上传到外部服务器。

就您的发现进行备注：

- 在警报详细信息中，输入**对此警报的注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

# 使用安全云分析补救问题

如果恶意行为导致生成警报，请修复恶意行为。例如：

- 如果恶意实体或用户尝试从网络外部进行登录，请更新防火墙规则和防火墙配置，防止该实体或用户访问您的网络。
- 如果实体尝试访问未经授权或恶意的域，请检查受影响的实体，以确定是否为恶意软件导致的原因。如果存在恶意DNS重定向，请确定网络上的其他实体是否受到影响，或是否是僵尸网络的一部分。如果用户有意这样做，请确定是否存在合法原因，例如测试防火墙设置。更新防火墙规则和防火墙配置，以防止进一步访问该域。
- 如果实体表现出与历史实体模型行为不同的行为，请确定是否有意更改行为。如果不是故意的，请检查网络上的其他授权用户是否应对更改负责。更新防火墙规则和防火墙配置，以解决涉及与网络外部实体的连接的意外行为。
- 如果发现漏洞或漏洞攻击，请更新或修补受影响的实体以消除漏洞，或更新防火墙配置以防止未经授权的访问。确定网络上的其他实体是否可能受到类似影响，并向这些实体应用相同的更新或补丁。如果漏洞或漏洞攻击当前没有修补程序，请联系相应的供应商告知他们。
- 如果发现恶意软件，请隔离实体并删除恶意软件。查看防火墙文件和恶意软件事件，以确定网络上的其他实体是否存在风险，更新实体以防止此恶意软件传播。使用有关此恶意软件或导致此恶意软件的实体的信息更新安全情报。更新您的防火墙访问控制以及文件和恶意软件规则，以防止此恶意软件将来感染您的网络。根据需要向供应商发出警报。
- 如果恶意行为导致数据泄露，请确定发送到未授权源的数据的性质。对于未经授权的数据泄露，请遵循组织协议进行操作。更新您的防火墙配置，以防止此来源未来的数据泄露尝试。

# 更新并关闭警报

根据您的调查结果添加其他标签：

**步骤 1** 在 Cisco Secure Cloud Analytics 门户 UI 中，选择**监控 (Monitor)** > **警报 (Alerts)**。

**步骤 2** 从下拉列表中选择一个或多个**标签**。

添加描述调查结果的最终注释，以及所采取的任何补救步骤：

- 在警报的详细信息中，输入**为此警报添加注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

关闭警报，然后将其标记为有用或无用：

1. 在警报的详细信息中，点击**关闭警报 (Close Alert)**。
2. 如果警报有用，请选择**是 (Yes)**；如果警报无用，请点击**否 (No)**。请注意，这并不一定意味着该警报是由恶意行为导致的，而只是表示它对您的组织有所帮助。
3. 点击**保存 (Save)**。

### What to do next

#### 重新打开已关闭的警报

如果您发现与已关闭警报相关的其他信息，或者想要添加与该警报相关的更多备注，则可以将其重新打开，并将状态更改为“待处理”。然后，您可以根据需要对警报进行更改，并在其他调查完成后再次将其关闭。

重新打开已关闭的警报：

- 在已关闭警报的详细信息中，点击**重新打开警报 (Reopen Alert)**。

# 修改警报优先级

**所需许可证 (Required License)： 日志记录分析和检测 (Logging Analytics and Detection)** 或**全面网络分析和监控 (Total Network Analytics and Monitoring)**

警报类型具有默认优先级，这会影响系统对生成此类警报的敏感程度。根据思科情报和其他因素，警报的优先级默认为低或正常。根据您的网络环境，您可能希望重新确定警报类型的优先级，以强调您关注的某些警报。您可以将任何风险通告类型配置为低、正常或高优先级。

- 选择**监控 (Monitor)** > **警报 (Alerts)**。
- 点击设置下拉图标 ()，然后选择警报类型和优先级。
- 点击警报类型旁边的编辑图标 ()，然后选择低、中或高以更改优先级。

# 查看实时事件

实时事件页面显示与您输入的在事件日志记录页面中搜索和过滤事件匹配的最新 500 个事件。如果“实时事件”页面最多显示 500 个事件，并且有更多事件传入，则 CDO 会显示最新的实时事件，并将最早的实时事件传输到“历史事件”页面，使实时事件总数保持为 500。执行该传输大约需要一分钟。如果未添加过滤条件，您将看到配置为记录事件的规则生成的所有最新实时 500 事件。

事件的时间戳以查看事件的 CDO 管理员的本地时间显示。

更改过滤条件（无论是正在播放还是已暂停的实时事件）会清除事件屏幕并重新启动收集过程。

要在 CDO 事件查看器中查看实时事件，请执行以下操作：

**步骤 1** 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**实时 (Live)** 选项卡。

### What to do next

通过阅读了解如何播放和暂停事件。

相关信息：

- 播放/暂停实时事件, on page 412
- 查看历史事件, on page 413
- 自定义事件视图, on page 413

# 播放/暂停实时事件

您可以在实时事件传入时“播放”  或“暂停”  。如果实时事件正在“播放”，则 CDO 将按接收顺序来显示与事件查看器中指定的过滤条件匹配的事件。如果事件已暂停，则在您重新开始播放实时事件之前，CDO 不会更新“实时事件”(Live events) 页面。当您重新开始播放事件时，CDO 会从您重新开始播放事件的位置开始在“实时”(Live) 页面中填充事件。它不会回填您遗漏的内容。

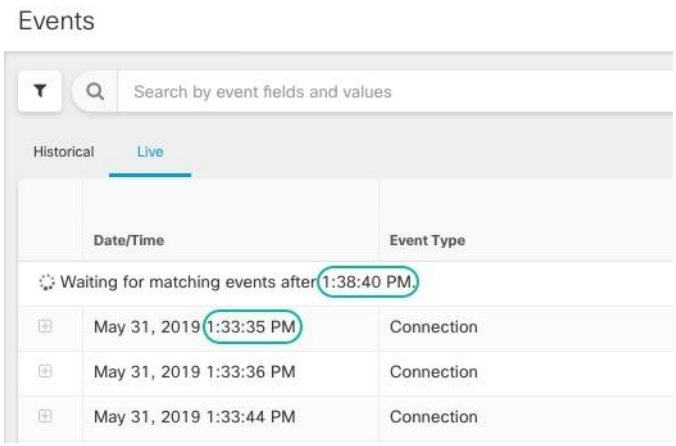
要查看 CDO 收到的所有事件（无论您已播放还是暂停），请点击“历史”(Historical) 选项卡。

### 自动暂停实时事件

在连续显示事件约 5 分钟后，CDO 会警告您即将暂停实时事件流。届时，您可以点击该链接以继续流传输其他 5 分钟的实时事件，或者允许流停止。在准备就绪后，您可以重新启动实时事件流。

### 接收和报告事件

在实时事件查看器中，安全事件连接器 (SEC) 接收事件和 CDO 发布事件之间可能会存在一点延迟。您可以在“实时”(Live) 页面上查看差距。事件的时间戳是 SEC 收到的时间。




# 查看历史事件

实时事件页面会显示与您输入的在事件日志记录页面中搜索和过滤事件匹配的 500 个最新事件。超出最近的 500 个事件将被传输到历史事件表。执行该传输大约需要一分钟。然后，您可以过滤已存储的所有事件，以便找到要查找的事件。

要查看历史事件，请执行以下操作：

**步骤 1** 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**历史 (Historical)** 选项卡。默认情况下，当您打开历史事件表时，过滤器会被设置为显示最近一小时内收集的事件。

事件属性与 Firepower 设备管理器 (FDM) 或自适应安全设备管理器 (ASDM) 报告的属性基本相同。

- 有关 Firepower 威胁防御事件属性的详尽说明，请参阅思科 FTD 系统日志消息。
- 有关 ASA 事件属性的详尽说明，请参阅思科 ASA 系列系统日志消息。

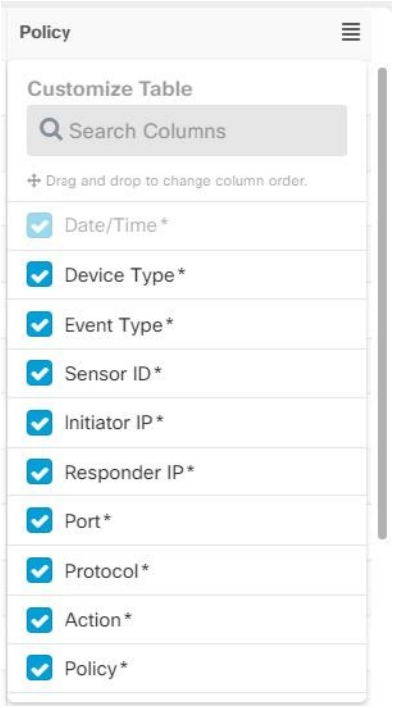
# 自定义事件视图

当您离开此页面并稍后返回时，系统会自动保存对“事件日志记录”(Event Logging) 页面所做的任何更改。

**Note** 实时和历史事件视图具有相同的配置。自定义事件视图时，这些更改将同时应用于实时和历史视图。

### 列

您可以修改实时事件和历史事件的事件视图，以仅包含适用于所需视图的列标题。点击列右侧的列过滤器图标 ，然后选择或取消选择所需的列：




默认情况下，事件表中提供带星号的列，但您可以随时将其删除。使用搜索栏手动搜索可能要包括的其他列的关键字。

### 订单

您可以对“事件”视图的列重新排序。点击列右侧的列过滤器图标 可展开所选列的列表，并手动将列拖放到所需的顺序，其中下拉菜单中列表顶部的列位于左侧- 事件视图中的大多数列。

**相关信息：**

- 在事件日志记录页面中搜索和过滤事件
- 安全分析和日志记录中的事件属性

# 在事件日志记录页面上显示和隐藏列

事件日志记录页面显示从配置的 ASA 和 FDM 管理 设备发送到思科云的 ASA 和 FTD 系统日志事件以及 ASA NetFlow 安全事件日志记录 (NSEL) 事件。

您可以通过对表使用显示/隐藏构件来显示或隐藏“事件日志记录”页面上的列：

**步骤 1** 从 CDO 导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 滚动到表格的最右侧，然后点击**显示/隐藏列 (Show/Hide Columns)** 按钮 ≣。

**步骤 3** 选中要查看的列，并取消选中要隐藏的列。

**步骤 4** 将鼠标悬停在“显示/隐藏列”(Show/Hide Columns) 下拉菜单中的列名称上，然后抓住灰色十字，重新排列列顺序。

登录到租户的其他用户将看到您选择显示的相同列，直到列再次显示或隐藏。

下表介绍了列标题：

| 列标题 | 说明 |
| --- | --- |
| 日期/时间 | 设备生成事件的时间。时间以计算机的本地时间显示。 |
| 设备类型 | ASA（自适应安全设备）<br>FTD（Firepower 威胁防御） |

| 列标题 | 说明 |
| --- | --- |
| 事件类型 | 此组合列可以包含以下任何内容：<br>• **FTD 事件类型**<br>• 连接 - 显示访问控制规则中的连接事件。<br>• 文件 - 显示访问控制规则中文件策略报告的事件。<br>• 入侵 - 显示访问控制规则中入侵策略报告的事件。<br>• 恶意软件 - 显示访问控制规则中的恶意软件策略报告的事件。<br>• ASA **事件类型** - 这些事件类型表示系统日志或 NetFlow 事件组。有关哪个系统日志 ID 或哪个 NetFlow ID 包含在哪个组中的详细信息，请参阅 ASA 事件类型。<br>• 解析的事件 - 解析的系统日志事件包含比其他系统日志事件更多的事件属性，并且 CDO 能够更快地返回基于这些属性的搜索结果。解析的事件不是过滤类别；但是，解析的事件 ID 以 斜体显示在“事件类型”(Event Types) 列中。不以斜体显示的事件 ID 不会被解析。<br>• ASA NetFlow 事件 ID：此处会显示 ASA 的所有 Netflow (NSEL) 事件 。 |
| 传感器 ID (Sensor ID) | 传感器 ID 是将事件发送到安全事件连接器的 IP 地址。这通常是 Firepower 威胁防御或 ASA 上的管理接口。 |
| 发起方 IP | 这是网络流量源的 IP 地址。发起方地址字段的值对应于事件详细信息中发起方 IP 字段的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。 |
| 响应方 IP | 这是流数据包的目的 IP 地址。“目的地址”(Destination address) 字段的值对应于事件详细信息中 ResponderIP 字段中的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。 |

| 列标题 | 说明 |
| --- | --- |
| Port | 会话**响应方**使用的端口或 ICMP 代码。目标端口的值对应于事件详细信息中的**ResponderPort**值。 |
| 协议 | 它代表事件中的协议。 |
| 操作 | 指定规则定义的安全操作。输入的值必须与要查找的内容完全匹配；但是，大小写无关紧要。为连接、文件、入侵、恶意软件、系统日志和 NetFlow 事件类型输入不同的值：<br>• 对于连接事件类型，过滤器在 AC_RuleAction 属性中搜索匹配项。这些值可以是“允许”(Allow)、“阻止”(Block)、“信任”(Trust)。<br>• 对于文件事件类型，过滤器在 FileAction 属性中搜索匹配项。这些值可以是“允许”、“阻止”、“信任”。<br>• 对于入侵事件类型，过滤器在 InLineResult 属性中搜索匹配项。这些值可以是 “已允许”(Allowed)、“已阻止”(Blocked)、“已信任”(Trusted)。<br>• 对于恶意软件事件类型，过滤器会在 FileAction 属性中搜索匹配项。这些值可以是“云查找超时”(Cloud Lookup Timeout)。<br>• 对于系统日志和 NetFlow 事件类型，过滤器在操作属性中搜索匹配项。 |
| 策略 | 触发事件的策略的名称。ASA 和 FDM 管理 设备的名称将有所不同。 |

**相关信息：**

在事件日志记录页面中搜索和过滤事件, on page 450

# 可自定义的事件过滤器

如果您是安全日志记录分析 (SaaS) 客户，则可以创建并保存您经常使用的自定义过滤器。

过滤器的元素会在您配置时保存到过滤器选项卡中。每当您返回“事件日志记录”(Event Logging) 页面时，这些搜索都可供使用。租户的其他CDO用户将无法使用它们。如果您管理多个租户，它们将无法在其他租户上使用。

**Note** 请注意，在过滤器选项卡中操作时，如果修改任何过滤器条件，这些更改将自动保存到自定义过滤器选项卡。

**步骤 1** 从主菜单中选择**分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 清除任何值的搜索字段。

**步骤 3** 在事件表上方，点击蓝色加号按钮以添加视图选项卡。过滤器视图被标记为“视图 1”(View 1)、“视图 2”(View 2)、“视图 3”(View 3) 等，直到您为其指定名称。


**步骤 4** 选择一个视图选项卡。

**步骤 5** 打开过滤器栏，然后在自定义过滤器中选择所需的过滤器属性。请参阅在事件日志记录页面中搜索和过滤事件, on page 450。请记住，自定义过滤器中仅保存过滤器属性。

**步骤 6** 自定义要在事件日志记录表中显示的列。有关显示和隐藏列的讨论，请参阅在事件日志记录页面上显示和隐藏列, on page 414。

**步骤 7** 双击带有“视图 X”(View X) 标签的过滤器选项卡并将其重命名。

**步骤 8** （可选）现在您已创建自定义过滤器，您可以通过向“搜索”(Search) 字段添加搜索条件来微调“事件日志记录”(Event Logging) 页面上显示的结果，而无需更改自定义过滤器。请参阅在事件日志记录页面中搜索和过滤事件, on page 450。

# 安全分析和日志记录中的事件属性

### 事件属性说明

CDO 使用的事件属性说明与 Firepower Device Manager (FDM) 和自适应安全设备管理器 (ASDM) 报告的内容基本相同。

- 有关自适应安全设备 (ASA) 事件属性的完整说明，请参阅思科 ASA 系列系统日志消息。

某些 ASA 系统日志事件经过“解析”，其他事件具有其他属性，您可以在使用“属性:值”对过滤事件日志记录表的内容时使用这些属性。有关系统日志事件的其他重要属性，请参阅以下附加主题：

- 已解析的 ASA 系统日志事件
- 某些系统日志消息的 EventGroup 和 EventGroupDefinition 属性
- 系统日志事件的 EventName 属性
- 系统日志事件中的时间属性

# 某些系统日志消息的 EventGroup 和 EventGroupDefinition 属性

某些系统日志事件将具有附加属性“EventGroup”和“EventGroupDefinition”。您将能够通过过滤“属性:值”对来过滤事件表，查找使用这些附加属性的事件。例如，您可以通过在事件日志记录表的搜索字段中输入 `apfw:415*` 来过滤应用防火墙事件。

**系统日志消息类和关联的消息 ID 号**

| 事件组 | EventGroupDefinition | 系统日志消息 ID 号（前 3 数字） |
|---|---|---|
| aaa/auth | 用户身份验证 | 109、113 |
| acl/session | 访问列表/用户会话 | 106 |
| apfw | 应用防火墙 | 415 |
| bridge | 透明防火墙 | 110、220 |
| ca | PKI 证书颁发机构 | 717 |
| citrix | Citrix Client | 723 |
| clst | 集群 | 747 |
| cmgr | 卡管理 | 323 |
| config | 命令界面 | 111、112、208、308 |
| csd | 安全桌面 | 724 |
| cts | Cisco TrustSec | 776 |
| dap | 动态访问策略 | 734 |
| eap, eapoudp | 用于网络准入控制的 EAP 或 EAPoUDP | 333、334 |
| eigrp | EIGRP 路由 | 336 |
| 电子邮件 | 邮件代理 | 719 |
| ipaa/envmon | 环境监控 | 735 |
| ha | 故障转移 | 101、102、103、104、105、210、311、709 |
| idfw | 基于身份认证的防火墙 | 746 |
| ids | 入侵检测系统 | 733 |
| ids/ips | 入侵检测系统/入侵保护系统 | 400 |
| ikev2 | IKEv2 工具包 | 750、751、752 |
| ip | IP 堆栈 | 209、215、313、317、408 |
| ipaa | IP 地址分配 | 735 |

| 事件组 | EventGroupDefinition | 系统日志消息 ID 号（前 3 数字） |
|---|---|---|
| ips | 入侵保护系统 | 401、420 |
| ipv6 | IPv6 | 325 |
| l4tm | 阻止列表、允许列表、灰名单 | 338 |
| 许可证 | 许可 | 444 |
| mdm-proxy | MDM 代理 | 802 |
| nac | 网络准入控制 | 731、732 |
| vpn/nap | IKE 和 IPsec/网络接入点 | 713 |
| np | 网络处理器 | 319 |
| ospf | OSPF 路由 | 318、409、503、613 |
| passwd | 密码加密 | 742 |
| pp | 电话代理 | 337 |
| rip | RIP 路由 | 107、312 |
| rm | 资源管理器 | 321 |
| sch | Smart Call Home | 120 |
| session | 用户会话 | 106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710 |
| 会话/natpat | 用户会话/NAT 和 PAT | 305 |
| snmp | SNMP | 212 |
| ssafe | ScanSafe | 775 |
| ssl/np ssl | SSL 协议栈/NP SSL | 725 |
| svc | SSL VPN 客户端 | 722 |
| sys | System | 199、211、214、216、306、307、315、414、604、605，606、610、612、614、615、701、711、741 |
| tre | 事务规则引擎 | 780 |
| ucime | UC-IME | 339 |
| 标记交换 | 服务标记交换 | 779 |
| td | 威胁检测 | 733 |

| 事件组 | EventGroupDefinition | 系统日志消息 ID 号（前 3 数字） |
|---|---|---|
| vm | VLAN 映射 | 730 |
| vpdn | PPTP 和 L2TP 会话 | 213、403、603 |
| vpn | IKE 和 IPsec | 316、320、402、404、501、602、702、713、714、715 |
| vpnc | VPN 客户端 | 611 |
| vpnfo | VPN 故障转移 | 720 |
| vpnlb | VPN 负载均衡 | 718 |
| vxlan | VXLAN | 778 |
| webfo | WebVPN 故障转移 | 721 |
| webvpn | WebVPN 和 AnyConnect 客户端 | 716 |
| 会话/natpat | 用户会话/NAT 和 PAT | 305 |

# 系统日志事件的 EventName 属性

某些系统日志事件将具有附加属性“EventName”。您将能够通过过滤“属性:值”对来过滤事件表，查找使用 EventName 属性的事件。例如，您可以通过在事件日志记录表的搜索字段中输入 **EventName:"Denied IP Packet"** 来过滤“被拒绝的 IP 数据包”的事件。

### 系统日志事件 ID 和事件名称表

- AAA 系统日志事件 ID 和事件名称
- 僵尸网络系统日志事件 ID 和事件名称
- 故障切换系统日志事件 ID 和事件名称
- 防火墙拒绝系统日志事件 ID 和事件名称
- 防火墙流量系统日志事件 ID 和事件名称
- 基于身份的防火墙系统日志事件 ID 和事件名称
- IPSec 系统日志事件 ID 和事件名称
- NAT 系统日志事件 ID 和事件名称
- SSL VPN 系统日志事件 ID 和事件名称

### AAA 系统日志事件 ID 和事件名称

| EventID | EventName |
|---|---|
| 109001 | AAA 开始 |

| EventID | EventName |
|---|---|
| 109002 | AAA 失败 |
| 109003 | AAA 服务器发生故障 |
| 109005 | 身份验证成功 |
| 109006 | 身份验证失败 |
| 109007 | 授权成功 |
| 109008 | 授权失败 |
| 109010 | AAA 待处理 |
| 109011 | AAA 会话已启动 |
| 109012 | AAA 会话已结束 |
| 109013 | AAA |
| 109014 | AAA 失败 |
| 109016 | 未找到 AAA ACL |
| 109017 | AAA 限制到达 |
| 109018 | AAA ACL 空 |
| 109019 | AAA ACL 错误 |
| 109020 | AAA ACL 错误 |
| 109021 | AAA 错误 |
| 109022 | AAA HTTP 限制已达到 |
| 109023 | 需要 AAA 身份验证 |
| 109024 | 授权失败 |
| 109025 | 授权失败 |
| 109026 | AAA 错误 |
| 109027 | AAA 服务器错误 |
| 109028 | AAA 绕行 |
| 109029 | AAA ACL 错误 |
| 109030 | AAA ACL 错误 |

| EventID | EventName |
|---|---|
| 109031 | 身份验证失败 |
| 109032 | AAA ACL 错误 |
| 109033 | 身份验证失败 |
| 109034 | 身份验证失败 |
| 109035 | AAA 限制到达 |
| 113001 | AAA 会话限制范围 |
| 113003 | AAA 已覆盖 |
| 113004 | AAA 成功 |
| 113005 | 授权被拒绝 |
| 113006 | AAA 用户已锁定 |
| 113007 | AAA 用户已解锁 |
| 113008 | AAA 成功 |
| 113009 | AAA 已检索 |
| 113010 | AAA 挑战已收到 |
| 113011 | AAA 已检索 |
| 113012 | 身份验证成功 |
| 113013 | AAA 错误 |
| 113014 | AAA 错误 |
| 113015 | 身份验证已被拒绝 |
| 113016 | AAA 已被拒绝 |
| 113017 | AAA 已被拒绝 |
| 113018 | AAA ACL 错误 |
| 113019 | AAA 已断开 |
| 113020 | AAA 错误 |
| 113021 | AAA 日志记录失败 |
| 113022 | AAA 失败 |

| EventID | EventName |
|---|---|
| 113023 | AAA 已重新激活 |
| 113024 | AAA 客户端证书 |
| 113025 | AAA 认证失败 |
| 113026 | AAA 错误 |
| 113027 | AAA 错误 |

僵尸网络系统日志事件 ID 和事件名称

| EventID | EventName |
|---|---|
| 338001 | 僵尸网络源阻止列表 |
| 338002 | 僵尸网络目标阻止列表 |
| 338003 | 僵尸网络源阻止列表 |
| 338004 | 僵尸网络目标阻止列表 |
| 338101 | 僵尸网络源允许列表 |
| 338102 | 僵尸网络目标允许列表 |
| 338202 | 僵尸网络目的地（灰色） |
| 338203 | 僵尸网络源灰色 |
| 338204 | 僵尸网络目标灰色 |
| 338301 | 僵尸网络 DNS 已拦截 |
| 338302 | 僵尸网络 DNS |
| 338303 | 僵尸网络 DNS |
| 338304 | 僵尸网络下载成功 |
| 338305 | 僵尸网络下载失败 |
| 338306 | 僵尸网络身份验证失败 |
| 338307 | 僵尸网络解密失败 |
| 338308 | 僵尸网络客户端 |
| 338309 | 僵尸网络客户端 |
| 338310 | 僵尸网络动态过滤器失败 |

故障切换系统日志事件 ID 和事件名称

| EventID | EventName |
|---|---|
| 101001 | 故障切换电缆 OK |
| 101002 | 故障切换电缆 BAD |
| 101003 | 故障切换电缆未连接 |
| 101004 | 故障切换电缆未连接 |
| 101005 | 故障切换电缆读取错误 |
| 102001 | 故障转移电源失败 |
| 103001 | 故障转移伙伴无响应 |
| 103002 | 故障转移配对接口 OK |
| 103003 | 故障转移伙伴接口 BAD |
| 103004 | 故障转移伙伴报告失败 |
| 103005 | 故障转移伙伴报告自身失败 |
| 103006 | 故障转移版本不兼容 |
| 103007 | 故障转移版本差异 |
| 104001 | 故障转移角色切换 |
| 104002 | 故障转移角色切换 |
| 104003 | 故障转移设备发生故障 |
| 104004 | 故障转移单元 OK |
| 106100 | 允许/被 ACL 拒绝 |
| 210001 | 状态故障转移错误 |
| 210002 | 状态故障转移错误 |
| 210003 | 状态故障转移错误 |
| 210005 | 状态故障转移错误 |
| 210006 | 状态故障转移错误 |
| 210007 | 状态故障转移错误 |
| 210008 | 状态故障转移错误 |

| EventID | EventName |
|---|---|
| 210010 | 状态故障转移错误 |
| 210020 | 状态故障转移错误 |
| 210021 | 状态故障转移错误 |
| 210022 | 状态故障转移错误 |
| 311001 | 状态故障转移更新 |
| 311002 | 状态故障转移更新 |
| 311003 | 状态故障转移更新 |
| 311004 | 状态故障转移更新 |
| 418001 | 被拒绝的向管理发送的数据包 |
| 709001 | 故障转移复制错误 |
| 709002 | 故障转移复制错误 |
| 709003 | 故障转移复制开始 |
| 709004 | 故障转移复制完成 |
| 709005 | 故障转移接收复制开始 |
| 709006 | 故障转移接收复制完成 |
| 709007 | 故障转移复制失败 |
| 710003 | 被拒绝的访问设备 |

防火墙拒绝系统日志事件 ID 和事件名称

| EventID | EventName |
|---|---|
| 106001 | 被安全策略拒绝 |
| 106002 | 出站拒绝 |
| 106006 | 被安全策略拒绝 |
| 106007 | 被拒绝的入站 UDP |
| 106008 | 被安全策略拒绝 |
| 106010 | 被安全策略拒绝 |
| 106011 | 被拒绝的入站 |

| EventID | EventName |
|---|---|
| 106012 | 由于 IP 选项错误而被拒绝 |
| 106013 | 对 PAT IP 的 ping 操作丢弃 |
| 106014 | 被拒绝的入站 ICMP |
| 106015 | 被安全策略拒绝 |
| 106016 | 被拒绝的 IP 欺骗 |
| 106017 | 由于着陆攻击而被拒绝 |
| 106018 | 被拒绝的出站 ICMP |
| 106020 | 被拒绝的 IP 数据包 |
| 106021 | 被拒绝的 TCP |
| 106022 | 被拒的绝欺骗数据包 |
| 106023 | 被拒绝的 IP 数据包 |
| 106025 | 被丢弃的数据包未能检测情景 |
| 106026 | 被丢弃的数据包未能检测情景 |
| 106027 | 被丢弃的数据包未能检测情景 |
| 106100 | 允许/被 ACL 拒绝 |
| 418001 | 被拒绝的向管理发送的数据包 |
| 710003 | 被拒绝的访问设备 |

防火墙流量系统日志事件 **ID** 和事件名称

| EventID | EventName |
|---|---|
| 108001 | 检查 SMTP |
| 108002 | 检查 SMTP |
| 108003 | 检查 ESMTP 已丢弃 |
| 108004 | 检查 ESMTP |
| 108005 | 检查 ESMTP |
| 108006 | 检查 ESMTP 违规 |
| 108007 | 检查 ESMTP |

| EventID | EventName |
|---|---|
| 110002 | 找不到路由器 |
| 110003 | 未能找到下一跳 |
| 209003 | 分段限制范围 |
| 209004 | 分段长度无效 |
| 209005 | 分段 IP 丢弃 |
| 302003 | H245 连接开始 |
| 302004 | H323 连接开始 |
| 302009 | 重新启动 TCP |
| 302010 | 连接使用情况 |
| 302012 | H225 CALL SIGNAL CONN |
| 302013 | 内置 TCP |
| 302014 | 拆解 TCP |
| 302015 | 内置 UDP |
| 302016 | 拆解 UDP |
| 302017 | 内置 GRE |
| 302018 | 拆解 GRE |
| 302019 | H323 失败 |
| 302020 | 内置 ICMP |
| 302021 | 拆解 ICMP |
| 302022 | 内置 TCP 末节 |
| 302023 | 拆解 TCP 末节 |
| 302024 | 内置 UDP 末节 |
| 302025 | 拆解 UDP 末节 |
| 302026 | 内置 ICMP 末节 |
| 302027 | 拆解 ICMP 末节 |
| 302033 | 连接 H323 |

| EventID | EventName |
|---|---|
| 302034 | H323 连接失败 |
| 302035 | 内置 SCTP |
| 302036 | 拆解 SCTP |
| 303002 | FTP 文件下载/上传 |
| 303003 | 检查 FTP 已丢弃 |
| 303004 | 检查 FTP 已丢弃 |
| 303005 | 检查 FTP 重置 |
| 313001 | ICMP 已拒绝 |
| 313004 | ICMP 丢弃 |
| 313005 | ICMP 错误消息丢弃 |
| 313008 | ICMP ipv6 已拒绝 |
| 324000 | GTP 数据包丢弃 |
| 324001 | GTP 数据包错误 |
| 324002 | 内存错误 |
| 324003 | GTP 数据包丢弃 |
| 324004 | 不支持 GTP 版本 |
| 324005 | GTP 隧道失败 |
| 324006 | GTP 隧道失败 |
| 324007 | GTP 隧道失败 |
| 337001 | 电话代理 SRTP 失败 |
| 337002 | 电话代理 SRTP 失败 |
| 337003 | 电话代理 SRTP 身份验证失败 |
| 337004 | 电话代理 SRTP 身份验证失败 |
| 337005 | 电话代理 SRTP 无媒体会话 |
| 337006 | 电话代理 TFTP 无法创建文件 |
| 337007 | 电话代理 TFTP 无法查找文件 |

| EventID | EventName |
|---|---|
| 337008 | 电话代理呼叫失败 |
| 337009 | 电话代理无法创建电话条目 |
| 400000 | IPS IP 选项 - 错误选项列表 |
| 400001 | IPS IP 选项 - 记录数据包路由 |
| 400002 | IPS IP 选项 - 时间戳 |
| 400003 | IPS IP 选项 - 安全 |
| 400004 | IPS IP 选项 - 松散源路由 |
| 400005 | IPS IP 选项 - SATNET ID |
| 400006 | IPS IP 选项 - 严格源路由 |
| 400007 | IPS IP 分段攻击 |
| 400008 | IPS IP 不可能的数据包 |
| 400009 | IPS IP 分段重叠 |
| 400010 | IPS ICMP 回应应答 |
| 400011 | IPS ICMP 主机不可达 |
| 400012 | IPS ICMP 源抑制 |
| 400013 | IPS ICMP 重定向 |
| 400014 | IPS ICMP 回应请求 |
| 400015 | 数据报的 IPS ICMP 超时 |
| 400017 | IPS ICMP 时间戳请求 |
| 400018 | IPS ICMP 时间戳应答 |
| 400019 | IPS ICMP 信息请求 |
| 400020 | IPS ICMP 信息应答 |
| 400021 | IPS ICMP 地址掩码请求 |
| 400022 | IPS ICMP 地址掩码应答 |
| 400023 | IPS 分段的 ICMP 流量 |
| 400024 | IPS 大 ICMP 流量 |

| EventID | EventName |
|---|---|
| 400025 | 死亡之 IPS Ping 攻击 |
| 400026 | IPS TCP NULL 标志 |
| 400027 | IPS TCP SYN+FIN 标志 |
| 400028 | 仅 IPS TCP FIN 标志 |
| 400029 | 指定了不正确的 IPS FTP 地址 |
| 400030 | 指定了不正确的 IPS FTP 端口 |
| 400031 | IPS UDP 炸弹攻击 |
| 400032 | IPS UDP Snork 攻击 |
| 400033 | IPS UDP Chargen DoS 攻击 |
| 400034 | IPS DNS HINFO 请求 |
| 400035 | IPS DNS 区域传输 |
| 400036 | 来自高端口的 IPS DNS 区域传输 |
| 400037 | 所有记录的 IPS DNS 请求 |
| 400038 | IPS RPC 端口注册 |
| 400039 | IPS RPC 端口取消注册 |
| 400040 | IPS RPC 转储 |
| 400041 | IPS 通过代理发送的 RPC 请求 |
| 400042 | IPS YP 服务器端口映射请求 |
| 400043 | IPS YP 绑定端口映射请求 |
| 400044 | IPS YP 密码端口映射请求 |
| 400045 | IPS YP 更新端口映射请求 |
| 400046 | IPS YP 传输端口映射请求 |
| 400047 | IPS 装载端口映射请求 |
| 400048 | IPS 远程执行端口映射请求 |
| 400049 | IPS 远程执行尝试 |
| 400050 | IPS Statd 缓冲区溢出 |

| EventID | EventName |
|---|---|
| 406001 | 检查 FTP 已丢弃 |
| 406002 | 检查 FTP 已丢弃 |
| 407001 | 主机限制到达 |
| 407002 | 初期限制已到达 |
| 407003 | 既定限制已到达 |
| 415001 | 检查 Http 信头字段计数 |
| 415002 | 检查 Http 信头字段长度 |
| 415003 | 检查 Http 正文长度 |
| 415004 | 检查 Http 内容类型 |
| 415005 | 检查 Http URL 长度 |
| 415006 | 检查 Http URL 匹配 |
| 415007 | 检查 Http 正文匹配 |
| 415008 | 检查 Http 信头匹配 |
| 415009 | 检查 Http 方法匹配 |
| 415010 | 检查传输编码匹配 |
| 415011 | 检查 Http 协议违规 |
| 415012 | 检查 Http 内容类型 |
| 415013 | 检查 Http 格式错误 |
| 415014 | 检查 Http MIME 类型 |
| 415015 | 检查 Http Transfer-encoding |
| 415016 | 检查 Http 未应答 |
| 415017 | 检查 Http 参数匹配 |
| 415018 | 检查 Http 信头长度 |
| 415019 | 检查 Http 状态已匹配 |
| 415020 | 检查 Http non-ASCII |
| 416001 | 检查 SNMP 已丢弃 |

| EventID | EventName |
|---|---|
| 419001 | 已丢弃的数据包 |
| 419002 | 重复 TCP SYN |
| 419003 | 数据包已修改 |
| 424001 | 被拒绝的数据包 |
| 424002 | 已丢弃的数据包 |
| 431001 | 已丢弃的 RTP |
| 431002 | 已丢弃的 RTCP |
| 500001 | 检查 ActiveX |
| 500002 | 检查 Java |
| 500003 | 检查 TCP 信头 |
| 500004 | 检查 TCP 信头 |
| 500005 | 检查连接已终止 |
| 508001 | 检查 DCERPC 已丢弃 |
| 508002 | 检查 DCERPC 已丢弃 |
| 509001 | 已阻止 No Forward Cmd |
| 607001 | 检查 SIP |
| 607002 | 检查 SIP |
| 607003 | 检查 SIP |
| 608001 | 检查 Skinny |
| 608002 | 检查 Skinny 已丢弃 |
| 608003 | 检查 Skinny 已丢弃 |
| 608004 | 检查 Skinny 已丢弃 |
| 608005 | 检查 Skinny 已丢弃 |
| 609001 | 内置本地主机 |
| 609002 | 拆解本地主机 |
| 703001 | H225 不支持的版本 |

| EventID | EventName |
|---|---|
| 703002 | H225 连接 |
| 726001 | 检查即时消息 |

基于身份的防火墙系统日志事件 ID 和事件名称

| EventID | EventName |
|---|---|
| 746001 | 导入已开始 |
| 746002 | 导入完成 |
| 746003 | 导入失败 |
| 746004 | 超出用户组限制 |
| 746005 | AD 代理关闭 |
| 746006 | AD 代理不同步 |
| 746007 | Netbios 响应失败 |
| 746008 | Netbios 已启动 |
| 746009 | Netbios 已停止 |
| 746010 | 导入用户失败 |
| 746011 | 超出用户限制 |
| 746012 | 用户 IP 添加 |
| 746013 | 用户 IP 删除 |
| 746014 | FQDN 过时 |
| 746015 | FQDN 已解析 |
| 746016 | DNS 查找失败 |
| 746017 | 导入用户已颁发 |
| 746018 | 导入用户已完成 |
| 746019 | 更新 AD 代理失败 |

IPSec 系统日志事件 ID 和事件名称

| EventID | EventName |
|---|---|
| 402114 | 收到无效的 SPI |

| EventID | EventName |
|---|---|
| 402115 | 收到意外的协议 |
| 402116 | 数据包与身份不匹配 |
| 402117 | 收到的非 IPSEC 数据包 |
| 402118 | 无效的分段偏移量 |
| 402119 | 防重放检查失败 |
| 402120 | 身份验证失败 |
| 402121 | 数据包已丢弃 |
| 426101 | cLACP 端口捆绑包 |
| 426102 | cLACP 端口备用 |
| 426103 | 已将 cLACP 端口从备用端口移至捆绑包 |
| 426104 | cLACP 非捆绑端口 |
| 602103 | 路径 MTU 已更新 |
| 602104 | 路径 MTU 已超出 |
| 602303 | 新 SA 已创建 |
| 602304 | SA 已删除 |
| 702305 | SA 到期 - 序列滚动 |
| 702307 | SA 到期 - 数据滚动 |

**NAT 系统日志事件 ID 和事件名称**

| EventID | EventName |
|---|---|
| 201002 | 超出主机的最大连接数 |
| 201003 | 已超出初期限制 |
| 201004 | 已超出 UDP 连接限制 |
| 201005 | FTP 连接失败 |
| 201006 | RCMD 连接失败 |
| 201008 | 不允许新建连接 |
| 201009 | 超出连接限制 |
| 201010 | 已超出初期连接限制 |
| 201011 | 已超出连接限制 |
| 201012 | 已超出每个客户端的初期连接限制 |

| EventID | EventName |
|---|---|
| 201013 | 已超出每个客户端连接限制 |
| 202001 | 全局 NAT 已耗尽 |
| 202005 | 初期连接错误 |
| 202011 | 超出连接限制 |
| 305005 | 未找到 NAT 组 |
| 305006 | 转换已失败 |
| 305007 | 连接已断开 |
| 305008 | NAT 分配问题 |
| 305009 | NAT 已创建 |
| 305010 | NAT 拆解 |
| 305011 | PAT 已创建 |
| 305012 | PAT 拆解 |
| 305013 | 连接已被拒绝 |

**SSL VPN 系统日志事件 ID 和事件名称**

| EventID | EventName |
|---|---|
| 716001 | WebVPN 会话已启动 |
| 716002 | WebVPN 会话已终止 |
| 716003 | WebVPN 用户 URL 访问 |
| 716004 | WebVPN 用户 URL 访问被拒绝 |
| 716005 | WebVPN ACL 错误 |
| 716006 | WebVPN 用户已禁用 |
| 716007 | WebVPN 无法创建 |
| 716008 | WebVPN 调试 |
| 716009 | WebVPN ACL 错误 |
| 716010 | WebVPN 用户接入网络 |
| 716011 | WebVPN 用户访问 |
| 716012 | WebVPN 用户目录访问 |
| 716013 | WebVPN 用户文件访问 |
| 716014 | WebVPN 用户文件访问 |

| EventID | EventName |
|---|---|
| 716015 | WebVPN 用户文件访问 |
| 716016 | WebVPN 用户文件访问 |
| 716017 | WebVPN 用户文件访问 |
| 716018 | WebVPN 用户文件访问 |
| 716019 | WebVPN 用户文件访问 |
| 716020 | WebVPN 用户文件访问 |
| 716021 | WebVPN 用户访问文件被拒绝 |
| 716022 | WebVPN 无法连接代理 |
| 716023 | WebVPN 会话限制已到达 |
| 716024 | WebVPN 用户访问错误 |
| 716025 | WebVPN 用户访问错误 |
| 716026 | WebVPN 用户访问错误 |
| 716027 | WebVPN 用户访问错误 |
| 716028 | WebVPN 用户访问错误 |
| 716029 | WebVPN 用户访问错误 |
| 716030 | WebVPN 用户访问错误 |
| 716031 | WebVPN 用户访问错误 |
| 716032 | WebVPN 用户访问错误 |
| 716033 | WebVPN 用户访问错误 |
| 716034 | WebVPN 用户访问错误 |
| 716035 | WebVPN 用户访问错误 |
| 716036 | WebVPN 用户登录成功 |
| 716037 | WebVPN 用户登录失败 |
| 716038 | WebVPN 用户身份验证成功 |
| 716039 | WebVPN 用户身份验证被拒绝 |
| 716040 | WebVPN 用户日志记录被拒绝 |
| 716041 | WebVPN ACL 命中计数 |
| 716042 | WebVPN ACL 命中 |
| 716043 | WebVPN 端口转发 |

| EventID | EventName |
|---|---|
| 716044 | WebVPN 错误参数 |
| 716045 | WebVPN 参数无效 |
| 716046 | WebVPN 连接已终止 |
| 716047 | WebVPN ACL 使用情况 |
| 716048 | WebVPN 内存问题 |
| 716049 | WebVPN 空 SVC ACL |
| 716050 | WebVPN ACL 错误 |
| 716051 | WebVPN ACL 错误 |
| 716052 | WebVPN 会话已终止 |
| 716053 | WebVPN SSO 服务器已添加 |
| 716054 | WebVPN SSO 服务器已删除 |
| 716055 | WebVPN 身份验证成功 |
| 716056 | WebVPN 身份验证失败 |
| 716057 | WebVPN 会话已终止 |
| 716058 | WebVPN 会话已丢失 |
| 716059 | WebVPN 会话已恢复 |
| 716060 | WebVPN 会话已终止 |
| 722001 | WebVPN SVC 连接请求错误 |
| 722002 | WebVPN SVC 连接请求错误 |
| 722003 | WebVPN SVC 连接请求错误 |
| 722004 | WebVPN SVC 连接请求错误 |
| 722005 | WebVPN SVC 连接更新问题 |
| 722006 | WebVPN SVC 地址无效 |
| 722007 | WebVPN SVC 消息 |
| 722008 | WebVPN SVC 消息 |
| 722009 | WebVPN SVC 消息 |
| 722010 | WebVPN SVC 消息 |
| 722011 | WebVPN SVC 消息 |
| 722012 | WebVPN SVC 消息 |

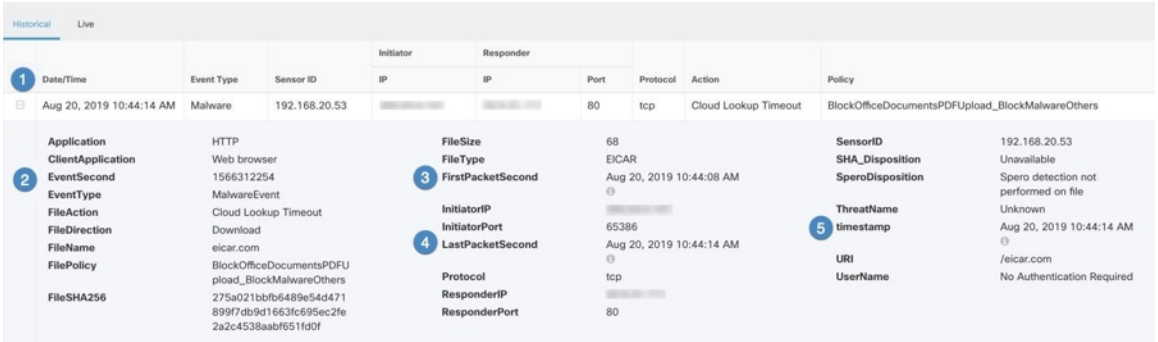
| EventID | EventName |
|---|---|
| 722013 | WebVPN SVC 消息 |
| 722014 | WebVPN SVC 消息 |
| 722015 | WebVPN SVC 无效帧 |
| 722016 | WebVPN SVC 无效帧 |
| 722017 | WebVPN SVC 无效帧 |
| 722018 | WebVPN SVC 无效帧 |
| 722019 | WebVPN SVC 数据不足 |
| 722020 | WebVPN SVC 无地址 |
| 722021 | WebVPN 内存问题 |
| 722022 | WebVPN SVC 连接已建立 |
| 722023 | WebVPN SVC 连接已终止 |
| 722024 | WebVPN 压缩已启用 |
| 722025 | WebVPN 压缩已禁用 |
| 722026 | WebVPN 压缩重置 |
| 722027 | WebVPN 解压重置 |
| 722028 | WebVPN 连接已关闭 |
| 722029 | WebVPN SVC 会话已终止 |
| 722030 | WebVPN SVC 会话已终止 |
| 722031 | WebVPN SVC 会话已终止 |
| 722032 | WebVPN SVC 连接替换 |
| 722033 | WebVPN SVC 连接已建立 |
| 722034 | WebVPN SVC 新连接 |
| 722035 | WebVPN 收到大数据包 |
| 722036 | WebVPN 传输大型数据包 |
| 722037 | WebVPN SVC 连接已关闭 |
| 722038 | WebVPN SVC 会话已终止 |
| 722039 | WebVPN SVC 无效 ACL |
| 722040 | WebVPN SVC 无效 ACL |
| 722041 | WebVPN SVC IPv6 不可用 |

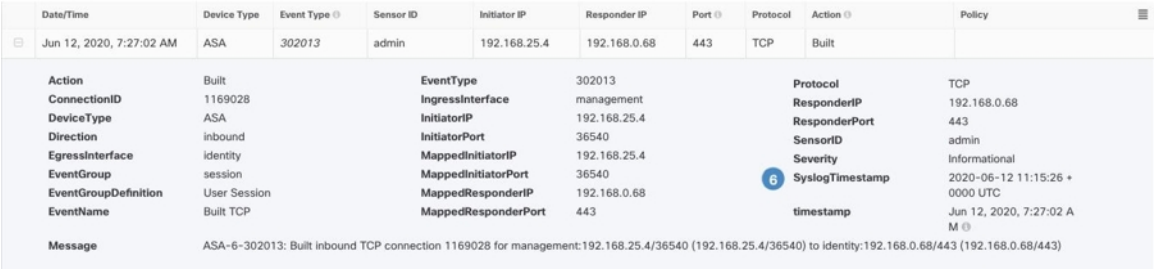
| EventID | EventName |
|---|---|
| 722042 | WebVPN 无效协议 |
| 722043 | WebVPN DTLS 已禁用 |
| 722044 | WebVPN 无法请求地址 |
| 722045 | WebVPN 连接已终止 |
| 722046 | WebVPN 会话已终止 |
| 722047 | WebVPN 隧道已终止 |
| 722048 | WebVPN 隧道已终止 |
| 722049 | WebVPN 会话已终止 |
| 722050 | WebVPN 会话已终止 |
| 722051 | 分配的 WebVPN 地址 |
| 722053 | WebVPN 未知客户端 |
| 723001 | WebVPN Citrix 连接开启 |
| 723002 | WebVPN Citrix 连接关闭 |
| 723003 | WebVPN Citrix 无内存问题 |
| 723004 | WebVPN Citrix 不良流量控制 |
| 723005 | WebVPN Citrix 无信道 |
| 723006 | WebVPN Citrix SOCKS 错误 |
| 723007 | WebVPN Citrix 连接列表已损坏 |
| 723008 | WebVPN Citrix 无效 SOCKS |
| 723009 | WebVPN Citrix 无效连接 |
| 723010 | WebVPN Citrix 无效连接 |
| 723011 | WebVPN citrix 不良 SOCKS |
| 723012 | WebVPN Citrix 不良 SOCKS |
| 723013 | WebVPN Citrix 无效连接 |
| 723014 | WebVPN Citrix 连接到服务器 |
| 724001 | 不允许使用 WebVPN 会话 |
| 724002 | WebVPN 会话已终止 |
| 724003 | WebVPN CSD |
| 724004 | WebVPN CSD |
| 725001 | SSL 握手已开始 |

| EventID | EventName |
|---|---|
| 725002 | SSL 握手已完成 |
| 725003 | SSL 客户端会话恢复 |
| 725004 | SSL 客户端请求身份验证 |
| 725005 | SSL 服务器请求认证 |
| 725006 | SSL 握手已失败 |
| 725007 | SSL 会话已终止 |
| 725008 | SSL 客户端密码 |
| 725009 | SSL 服务器密码 |
| 725010 | SSL 密码 |
| 725011 | SSL 设备选择密码 |
| 725012 | SSL 设备选择密码 |
| 725013 | SSL 服务器选择密码 |
| 725014 | SSL LIB 错误 |
| 725015 | SSL 客户端证书已失败 |

# 系统日志事件中的时间属性

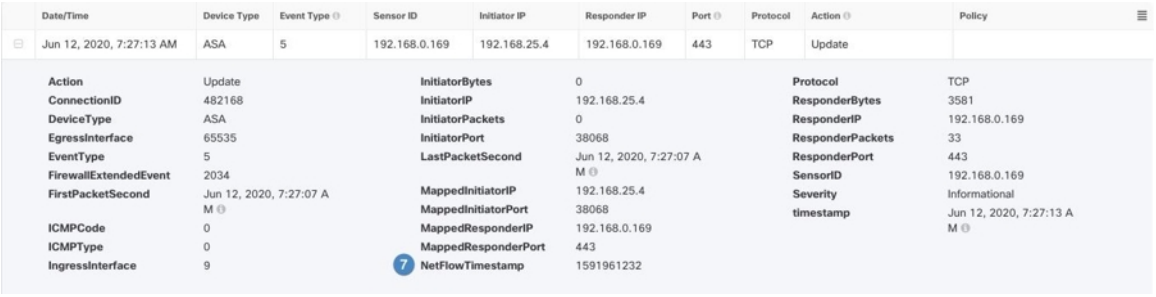
了解“事件日志记录”(Event Logging) 页面中不同时间戳的用途将有助于您过滤并查找感兴趣的事件。





| Date/Time | Device Type | Event Type | Sensor ID | Initiator IP | Responder IP | Port | Protocol | Action | Policy |
|---|---|---|---|---|---|---|---|---|---|
| Jun 12, 2020, 7:27:02 AM | ASA | 302013 | admin | 192.168.25.4 | 192.168.0.68 | 443 | TCP | Built | |

| | | | | | |
|---|---|---|---|---|---|
| Action | Built | EventType | 302013 | Protocol | TCP |
| ConnectionID | 1169028 | IngressInterface | management | ResponderIP | 192.168.0.68 |
| DeviceType | ASA | InitiatorIP | 192.168.25.4 | ResponderPort | 443 |
| Direction | inbound | InitiatorPort | 36540 | SensorID | admin |
| EgressInterface | identity | MappedInitiatorIP | 192.168.25.4 | Severity | Informational |
| EventGroup | session | MappedInitiatorPort | 36540 | 6 SyslogTimestamp | 2020-06-12 11:15:26 + 0000 UTC |
| EventGroupDefinition | User Session | MappedResponderIP | 192.168.0.68 | | |
| EventName | Built TCP | MappedResponderPort | 443 | timestamp | Jun 12, 2020, 7:27:02 A M |
| Message | ASA-6-302013: Built inbound TCP connection 1169028 for management:192.168.25.4/36540 (192.168.25.4/36540) to identity:192.168.0.68/443 (192.168.0.68/443) | | | | |



| Date/Time | Device Type | Event Type | Sensor ID | Initiator IP | Responder IP | Port | Protocol | Action | Policy |
|---|---|---|---|---|---|---|---|---|---|
| Jun 12, 2020, 7:27:13 AM | ASA | 5 | 192.168.0.169 | 192.168.25.4 | 192.168.0.169 | 443 | TCP | Update | |

| | | | | | |
|---|---|---|---|---|---|
| Action | Update | InitiatorBytes | 0 | Protocol | TCP |
| ConnectionID | 482168 | InitiatorIP | 192.168.25.4 | ResponderBytes | 3581 |
| DeviceType | ASA | InitiatorPackets | 0 | ResponderIP | 192.168.0.169 |
| EgressInterface | 65535 | InitiatorPort | 38068 | ResponderPackets | 33 |
| EventType | 5 | LastPacketSecond | Jun 12, 2020, 7:27:07 A M | ResponderPort | 443 |
| FirewallExtendedEvent | 2034 | | | SensorID | 192.168.0.169 |
| FirstPacketSecond | Jun 12, 2020, 7:27:07 A M | MappedInitiatorIP | 192.168.25.4 | Severity | Informational |
| | | MappedInitiatorPort | 38068 | timestamp | Jun 12, 2020, 7:27:13 A M |
| ICMPCode | 0 | MappedResponderIP | 192.168.0.169 | | |
| ICMPType | 0 | MappedResponderPort | 443 | | |
| IngressInterface | 9 | 7 NetFlowTimestamp | 1591961232 | | |

| 数字 | 编号 | 说明 |
|---|---|---|
| 1 | 日期/时间 | 安全事件连接器 (SEC) 处理事件的时间。这可能与防火墙检查该流量的时间有所不同。与时间戳相同的值。 |
| 2 | EventSecond | 等于 LastPacketSecond。 |
| 3 | FirstPacketSecond | 连接打开的时间。防火墙会在此时检查数据包。<br>FirstPacketSecond 的值通过从 LastPacketSecond 中减去 ConnectionDuration 来计算得出。<br>对于在连接开始时记录的连接事件，FirstPacketSecond、LastPacketSecond 和 EventSecond 的值均相同。 |
| 4 | LastPacketSecond | 连接被关闭的时间。对于在连接结束时记录的连接事件，LastPacketSecond 和 EventSecond 将相等。 |
| 5 | timestamp | 安全事件连接器 (SEC) 处理事件的时间。这可能与防火墙检查该流量的时间有所不同。与日期/时间相同的值。 |

| 数字 | 编号 | 说明 |
| --- | --- | --- |
| 6 | 系统日志时间戳 | 如果使用“日志记录时间戳”，则表示系统日志的发起时间。如果系统日志中没有此信息，则会反映 SEC 收到事件的时间。 |
| 7 | NetflowTimeStamp | ASA 完成收集足够的流记录/事件以填充 NetFlow 数据包，然后将其发送到流收集器的时间。 |

# 思科安全云分析和动态实体建模

**所需许可证 (Required License)：日志记录分析和检测 (Logging Analytics and Detection)** 或**全面网络分析和监控 (Total Network Analytics and Monitoring)**

安全云分析是一种软件即服务 (SaaS) 解决方案，可用于监控您的本地和基于云的网络部署。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

## 动态实体建模

动态实体建模可通过对防火墙事件和网络流数据执行行为分析来跟踪网络状态。在 Cisco Secure Cloud Analytics 环境中，实体是指可以随时间推移进行跟踪的对象，例如网络上的主机或终端。动态实体建模根据实体传输的流量及其在网络上执行的活动，收集实体的相关信息。与**日志记录分析和检测**许可证集成的 Cisco Secure Cloud Analytics 可以从防火墙事件和其他流量信息中进行提取，以便确定实体通常传输的流量类型。如果您购买了**全面网络分析和监控**许可证，则 Cisco Secure Cloud Analytics 还可以在对实体流量进行建模时纳入 NetFlow 和其他流量信息。Cisco Secure Cloud Analytics 会随着时间的推移更新这些模型，因为实体会继续发送流量，并且可能会发送不同的流量，从而保持每个实体的最新模型。根据这些信息，Cisco Secure Cloud Analytics 可以识别：

- 实体的角色，即实体通常执行的操作的描述符。例如，如果实体发送通常与邮件服务器关联的流量，Cisco Secure Cloud Analytics 会为该实体分配邮件服务器角色。角色/实体关系可以是多对一，因为实体可以履行多种角色。
- 对实体的观察结果，即有关实体在网络上的行为的事实，例如与外部 IP 地址建立的心跳连接或与另一个实体建立的远程访问会话。如果与 CDO 集成，则可以从防火墙事件中获取这些事实。如果您还购买了**全面的网络分析和监控**许可证，则系统还可以从 NetFlow 获取事实，并从防火墙事件和 NetFlow 中生成观察结果。观察结果本身并不具有超出其所代表的事实的意义。一个典型的客户可能有数千个观察结果和若干个警报。

### 警报和分析

Cisco Secure Cloud Analytics 会根据角色、观察结果和其他威胁情报的组合生成警报，这些警报是可操作项目，代表系统标识的可能的恶意行为。请注意，一个警报可能代表多个观察结果。如果防火墙记录了与同一连接和实体相关的多个连接事件，则可能只会生成一个警报。

例如，新的内部设备观察结果本身并不构成可能的恶意行为。但是，随着时间的推移，如果实体传输的流量与域控制器一致，则系统会向该实体分配域控制器角色。如果实体随后使用异常端口与之前未建立连接的外部服务器建立了连接，并且传输了大量的数据，则系统将记录新的大型连接（外部）观察结果和异常域控制器观察结果。如果该外部服务器被识别为一个 Talos 监视列表，则所有这些信息的组合将导致 Cisco Secure Cloud Analytics 生成此实体行为的警报，从而提示您采取进一步措施来研究和补救恶意行为。

在 Cisco Secure Cloud Analytics Web 门户 UI 中打开警报时，您可以查看导致系统生成该警报的支持性观察结果。您还可以从这些观察结果中查看有关所涉实体的其他背景信息，包括它们传输的流量以及外部威胁情报（如果可用）。您还可以查看实体涉及的其他观察结果和警报，然后确定此行为是否与其他潜在恶意行为相关。

请注意，在 Cisco Secure Cloud Analytics 中查看和关闭警报时，无法允许或阻止来自 Cisco Secure Cloud Analytics UI 的流量。如果在主动模式下部署设备，则必须更新防火墙访问控制规则以允许或阻止流量；如果在被动模式下部署防火墙，则必须更新防火墙访问控制规则。

# 使用基于防火墙事件的警报

**所需许可证： 日志记录分析和检测 或 全面网络分析和监控**

### 警报工作流程

警报的工作流程基于其状态。当系统生成警报时，其默认状态为“待处理”，并且未分配任何用户。当您查看警报总结时，默认情况下会显示所有待处理警报，因为这些是最需要关注的。

注意：如果您拥有**全面网络分析和监控**许可证，则警报可以基于从 NetFlow 生成的观察结果、从防火墙事件生成的观察结果或来自两个数据源的观察结果。

查看警报总结时，可以分配和标记警报，以及将其状态更新为初始分类。您可以使用过滤器和搜索功能查找特定警报，也可以显示不同状态的警报或具有不同标记或负责人的警报。您可以将警报的状态设置为“已暂停”，在这种情况下，警报要等暂停期过后才会重新显示在待处理警报列表中。您也可以移除警报的“已暂停”状态，使其再次显示为待处理警报。查看警报时，您可以将其分配给您自己或系统中的其他用户。用户可以搜索分配给其用户名的所有警报。

在警报摘要中，您可以查看警报详细信息页面。此页面允许您查看有关生成此警报的支持性观察结果的其他背景信息，以及有关此警报中涉及的实体的其他背景信息。这些信息可帮助您查明实际问题，以便进一步研究网络上的问题，并且有可能解决恶意行为。

当您在 CDO 中的 Stealthwatch 云 web 门户 UI 和网络中进行研究时，可以进行备注，描述您对警报的发现。这有助于为您的研究创建记录，供您将来参考。

完成分析后，您可以将状态更新为“已关闭”，使其不再默认显示为待处理警报。如果情况发生变化，您还可以在将来重新打开已关闭的警报。

下面介绍有关如何调查给定警报的一般准则和建议。Stealthwatch 云会在记录警报时提供附加背景信息，因此，您可以使用此信息帮助指导调查工作。

这些步骤既不全面，也非包罗万象。它们仅提供一个总体框架来帮助您开始调查警报。

通常，查看警报时可以采取以下步骤：

1. 对待处理警报进行分类, on page 406
2. 暂停警报以供以后分析, on page 407
3. 更新警报以进行进一步调查, on page 407
4. 查看警报并开始调查, on page 408
5. 检查实体和用户, on page 409
6. 使用安全云分析补救问题, on page 410
7. 更新并关闭警报, on page 410

## 对待处理警报进行分类

对待处理警报进行分类，特别是如果要调查多个待处理警报：

- 有关从 CDO 交叉启动和查看警报的详细信息，请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报。

询问以下问题：

- 您是否将此警报类型配置为高优先级？
- 您是否为受影响的子网设置了高灵敏度？
- 这是网络上新实体的异常行为吗？
- 实体的正常角色是什么，此警报中的行为与该角色的匹配度如何？
- 这是否是此实体正常行为的异常偏离？
- 如果用户参与其中，这是用户的预期行为还是异常行为？
- 受保护数据或敏感数据是否有被泄露的风险？
- 如果允许此行为继续下去，会对网络产生多严重的影响？
- 如果与外部实体有通信，这些实体过去是否与您网络上的其他实体建立了连接？

如果这是高优先级警报，请考虑将该实体与互联网隔离，或以其他方式关闭其连接，然后再继续调查。

## 暂停警报以供以后分析

当警报的优先级较低（与其他警报相比）时，可将其暂停。例如，如果您的组织将邮件服务器重新定位为 FTP 服务器，并且系统生成紧急配置文件警报（表明一个实体的当前流量匹配了它以前没有

匹配的行为概要文件），您可以暂停此警报（因为这是预期行为），并在以后重新访问它。已暂停的警报不会与待处理警报一起显示；您必须专门过滤才能查看这些暂停的警报。

暂停警报：

**步骤 1** 点击**关闭警报 (Close Alert)**。

**步骤 2** 在暂停此警报窗格中，从下拉列表中选择暂停时段。

**步骤 3** 点击**保存 (Save)**。

#### What to do next

当您准备好查看这些警报时，可以取消暂停该警报。这会将状态设置为“未处理”(Open)，并在其他“未处理”的警报旁边显示该警报。

取消暂停已暂停的警报：

- 从暂停的警报中，点击**取消暂停警报 (Unsnooze Alert)**。

## 更新警报以进行进一步调查

打开警报详细信息：

**步骤 1** 选择**监控 (Monitor)** > **警报 (Alerts)**。

**步骤 2** 点击警报类型名称。

#### What to do next

根据您的初始分类和优先级，分配警报并标记：

1. 从**被分派人 (Assignee)** 下拉列表中选择用户以分配警报，以便用户可以开始调查。
2. 从下拉列表中选择一个或多个**标签**，以将标签添加到警报，以便更好地对警报进行分类以供将来识别，并尝试在警报中建立长期模式。
3. 输入**为此警报添加注释 (Comment on this alert)**，然后点击**注释 (Comment)** 以根据需要留下注释，以跟踪您的初始发现，并协助分配到警报的人员。警报同时跟踪系统注释和用户注释。

## 查看警报并开始调查

如果您正在查看已分配的警报，请查看警报详细信息以了解 Stealthwatch 云生成警报的原因。查看支持性观察结果，了解这些观察结果对源实体的意义。

请注意，如果警报是基于防火墙事件生成的，则系统不会注意到您的防火墙部署是此警报的来源。

查看此源实体的所有支持性观察结果，以了解其一般行为和模式，并查看此活动是否可能影响着某个长期趋势：

**SUMMARY STEPS**

1. 在观察结果控制面板上，点击观察结果类型旁边的箭头图标(➔)，以查看该类型的所有已记录观察结果。
2. 点击**网络的所有观察结果 (All Observations for Network)** 旁边的箭头图标 (➔)，查看此警报的源实体的所有已记录观察结果。

**DETAILED STEPS**

**步骤 1** 在观察结果控制面板上，点击观察结果类型旁边的箭头图标 (➔)，以查看该类型的所有已记录观察结果。

**步骤 2** 点击**网络的所有观察结果 (All Observations for Network)** 旁边的箭头图标 (➔)，查看此警报的源实体的所有已记录观察结果。

如果要对这些观察结果执行其他分析，请下载逗号分隔值文件中的支持观察结果：

- 在警报详细信息的支持观察结果窗格中，点击 **CSV**。

从观察结果，确定源实体行为是否指示恶意行为。如果源实体与多个外部实体建立了连接，请确定外部实体是否以某种方式相关，例如它们是否都具有相似的地理位置信息，或者它们的 IP 地址是否来自同一子网。

从源实体 IP 地址或主机名称查看有关源实体的其他背景信息，包括它可能涉及的其他警报和观察结果、有关设备本身的信息以及它传输的会话流量类型：

- 从 IP 地址或主机名下拉列表中选择**警报 (Alerts)**，以查看与该实体相关的所有警报。
- 从 IP 地址或主机名下拉列表中选择**观察结果 (Observations)**，以查看与实体相关的所有观察结果。
- 从 IP 地址或主机名下拉列表中选择**设备 (Device)**，以查看有关设备的信息。
- 从 IP 地址或主机名下拉列表中选择**会话流量 (Session Traffic)**，以查看与此实体相关的会话流量。
- 从 IP 地址或主机名下拉列表中选择**复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的源实体始终位于您的网络内部。将此与防火墙事件中的发起方 IP 进行对比，后者指示发起连接的实体，并且可能位于您的网络内部或外部。

从观察结果中，检查有关其他外部实体的信息。检查地理位置信息，确定是否有任何地理位置数据或 Umbrella 数据标识恶意实体。查看这些实体生成的流量。检查 Talos、AbuseIPDB 或 Google 是否有关于这些实体的任何信息。查找多天的 IP 地址，并查看外部实体与您网络上的实体建立的其他类型的连接。如有必要，请找到这些内部实体，并确定是否有任何证据表明存在攻击活动或意外行为。

查看与源实体建立了连接的外部实体 IP 地址或主机名称的背景信息：

- 从 IP 地址或主机名下拉列表中选择 **IP 流量 (IP Traffic)**，以查看此实体的最近流量信息。
- 从 IP 地址或主机名下拉列表中选择**会话流量 (Session Traffic)**，以查看此实体的最近会话流量信息。
- 从 IP 地址或主机名下拉列表中选择 **AbuseIPDB**，以查看有关 AbuseIPDB 网页实体的信息。
- 从 IP 地址或主机名下拉列表中选择**思科 Umbrella (Cisco Umbrella)**，可在 Cisco Umbrella 网站上查看有关此实体的信息。
- 从 IP 地址或主机名下拉列表中选择 **Google 搜索 (Google Search)**，以在 Google 上搜索此 IP 地址。
- 从 IP 地址或主机名下拉列表中选择 **Talos 智能 (Talos Intelligence)**，以查看有关 Talos 网页的信息。
- 从 IP 地址或主机名下拉列表中选择**将 IP 添加到监视列表 (Add IP to watchlist)**，以将此实体添加到监视列表。
- 从 IP 地址或主机名下拉列表中选择**查找多天的 IP (Find IP on multiple days)**，以搜索此实体上个月的流量。
- 从 IP 地址或主机名下拉列表中选择**复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的连接实体始终位于您的网络外部。将此与防火墙事件中的响应方 IP 进行对比，后者指示响应连接请求的实体，并且可能位于您的网络的内部或外部。

就您的发现进行备注。

- 在警报详细信息中，输入**对此警报的注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

## 检查实体和用户

在 Stealthwatch 云门户 UI 中查看警报后，您可以直接对源实体、可能与此警报相关的任何用户以及其他相关实体执行其他检查。

- 确定源实体在网络上的物理位置或云中的位置，并直接访问它。找到此实体的日志文件。如果它是网络上的物理实体，请访问设备以查看日志信息，并查看是否有任何信息表明是什么导致了此行为。如果它是虚拟实体或存储在云中，请访问日志并搜索与此实体相关的条目。检查日志，了解有关未经授权的登录、未经批准的配置更改等活动的更多信息。
- 检查实体。确定您能否识别实体本身上的恶意软件或漏洞。查看是否发生了一些恶意更改，包括设备是否发生了物理更改，例如插入了未经组织批准的 U 盘。
- 确定所涉及的用户来自您的网络内部还是外部。如果可能，询问他们当时在做什么。如果询问未果，请确定他们是否应该具有访问权限，以及是否发生了导致此行为的情况，例如，离职员工在离开公司之前将文件上传到外部服务器。

就您的发现进行备注：

- 在警报详细信息中，输入**对此警报的注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

## 更新并关闭警报

根据您的调查结果添加其他标签：

**步骤 1** 在 Cisco Secure Cloud Analytics 门户 UI 中，选择**监控 (Monitor)** > **警报 (Alerts)**。

**步骤 2** 从下拉列表中选择一个或多个**标签**。

添加描述调查结果的最终注释，以及所采取的任何补救步骤：

- 在警报的详细信息中，输入**为此警报添加注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

关闭警报，然后将其标记为有用或无用：

1. 在警报的详细信息中，点击**关闭警报 (Close Alert)**。
2. 如果警报有用，请选择**是 (Yes)**；如果警报无用，请点击**否 (No)**。请注意，这并不一定意味着该警报是由恶意行为导致的，而只是表示它对您的组织有所帮助。
3. 点击**保存 (Save)**。

### What to do next

#### 重新打开已关闭的警报

如果您发现与已关闭警报相关的其他信息，或者想要添加与该警报相关的更多备注，则可以将其重新打开，并将状态更改为“待处理”。然后，您可以根据需要对警报进行更改，并在其他调查完成后再次将其关闭。

重新打开已关闭的警报：

- 在已关闭警报的详细信息中，点击**重新打开警报 (Reopen Alert)**。

# 修改警报优先级

**所需许可证 (Required License)： 日志记录分析和检测 (Logging Analytics and Detection)** 或**全面网络分析和监控 (Total Network Analytics and Monitoring)**

警报类型具有默认优先级，这会影响系统对生成此类警报的敏感程度。根据思科情报和其他因素，警报的优先级默认为低或正常。根据您的网络环境，您可能希望重新确定警报类型的优先级，以强调您关注的某些警报。您可以将任何风险通告类型配置为低、正常或高优先级。

- 选择**监控 (Monitor)** > **警报 (Alerts)**。
- 点击设置下拉图标 ()，然后选择警报类型和优先级。
- 点击警报类型旁边的编辑图标 ()，然后选择低、中或高以更改优先级。

# 在事件日志记录页面中搜索和过滤事件

搜索和过滤特定事件的历史和实时事件表的方式与在CDO中搜索和过滤其他信息时的方式相同。当您添加过滤条件时，CDO 就会开始限制其在“事件”(Events) 页面上显示的内容。您还可以在搜索字段中输入搜索条件，以便查找具有特定值的事件。如果结合使用过滤和搜索机制，搜索会尝试在过滤事件后从显示的结果中查找您输入的值。

以下是执行搜索事件日志的选项：

- 在事件日志记录页面中搜索事件， 第 457 页
- 在后台搜索历史事件， 第 457 页

过滤实时事件的方式与过滤历史事件的方式相同，但不能按时间过滤实时事件。

了解这些过滤方法：

- 过滤实时或历史事件， 第 450 页
- 仅过滤 NetFlow 事件， 第 452 页
- 过滤 ASA 或 FDM 管理 设备系统日志事件，但不过滤 ASA NetFlow 事件， 第 452 页
- 组合过滤器元素， 第 452 页

## 过滤实时或历史事件

此程序介绍了如何使用事件过滤查看“事件日志记录”(Event Logging) 页面中的事件子集。如果您发现自己重复使用某些过滤条件，则可以创建自定义过滤器并保存。有关详细信息，请参阅可自定义的事件过滤器。

**步骤 1** 在导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**

**步骤 2** 点击“历史”(Historical) 或“实时”(Live) 选项卡。

**步骤 3** 点击过滤器按钮 。点击固定图标 可固定打开过滤列。

**步骤 4** 点击没有已保存过滤器元素的视图选项卡。


**步骤 5** 选择要作为过滤条件的事件详细信息：

- **FTD 事件**
  - 连接 - 显示访问控制规则中的连接事件。
  - 文件 - 显示访问控制规则中文件策略报告的事件。
  - 入侵 - 显示访问控制规则中入侵策略报告的事件。

- 恶意软件 - 显示访问控制规则中的恶意软件策略报告的事件。

- **ASA 事件 (ASA Events)** - 这些事件类型表示系统日志或 NetFlow 事件组。

  有关事件的详细信息，请参阅 CDO 中的事件类型 。

  - 解析的事件 - 已解析的 ASA 系统日志事件包含比其他系统日志事件更多的事件属性，并且 CDO 能够根据这些属性更快地返回搜索结果。解析的事件不是过滤类别；但是，解析的事件ID以斜体显示在“事件类型”列中。不以斜体显示的事件 ID 不会被解析。

- **时间范围 (Time Range)** - 点击开始或结束时间字段以选择要显示的时间段的开始和结束时间。时间戳以计算机的本地时间显示。

- **操作 (Action)** - 指定规则定义的安全操作。输入的值必须与要查找的内容完全匹配；但是，大小写无关紧要。为连接、文件、入侵、恶意软件、系统日志和 NetFlow 事件类型输入不同的值：

  - 对于连接事件类型，过滤器在 AC_RuleAction 属性中搜索匹配项。这些值可以是“允许”(Allow)、“阻止”(Block)、“信任”(Trust)。
  - 对于文件事件类型，过滤器在 FileAction 属性中搜索匹配项。这些值可以是“允许”、“阻止”、“信任”。
  - 对于入侵事件类型，过滤器在 InLineResult 属性中搜索匹配项。这些值可以是“已允许”(Allowed)、“已阻止”(Blocked)、“已信任”(Trusted)。
  - 对于恶意软件事件类型，过滤器会在 FileAction 属性中搜索匹配项。这些值可以是“云查找超时”(Cloud Lookup Timeout)。
  - 对于系统日志和 NetFlow 事件类型，过滤器在操作属性中搜索匹配项。

- **传感器 ID (Sensor ID)** - 传感器 ID 是将事件发送到安全事件连接器的管理 IP 地址。

  对于 FDM 管理 设备，传感器 ID 通常是设备管理接口的 IP 地址。

- **IP 地址**

  - **发起方 (Initiator)** - 这是网络流量源的 IP 地址。发起方地址字段的值对应于事件详细信息中发起方 IP 字段的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。
  - **响应方 (Responder)** - 这是流数据包的目的 IP 地址。“目的地址”(Destination address) 字段的值对应于事件详细信息中 ResponderIP 字段中的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。

- **端口**

  - **发起方 (Initiator)** - 会话发起方使用的端口或 ICMP 类型。源端口的值对应于事件详细信息中的发起方端口的值。（添加范围 - 起始端口和结束端口之间的空格或发起方和响应方）
  - **响应方 (Reponder)** - 会话响应方使用的端口或 ICMP 代码。目标端口的值对应于事件详细信息中的 ResponderPort 值。

- **NetFlow** - ASA 设备的 NetFlow 安全事件日志记录 (NSEL) 事件不同于系统日志事件。NetFlow 过滤器搜索生成 NSEL 记录的所有 NetFlow 事件 ID。这些“NetFlow 事件 ID”在《思科 ASA NetFlow 实施指南》中进行了定义。

**步骤 6** （可选）点击查看选项卡，将过滤器另存为自定义过滤器。

# 仅过滤 NetFlow 事件

此程序仅查找 ASA NetFlow 事件：

**步骤 1** 从 CDO 菜单栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击过滤器图标 并将过滤器固定为打开状态。

**步骤 3** 检查 **Netflow** ASA 事件过滤器。

**步骤 4** 清除所有其他 ASA 事件过滤器。

事件日志记录表中仅显示 ASA NetFlow 事件。

# 过滤 ASA 或 FDM 管理 设备系统日志事件，但不过滤 ASA NetFlow 事件

此过程仅查找系统日志事件：

**步骤 1** 从 CDO 菜单栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击过滤器图标 并将过滤器固定为打开状态。

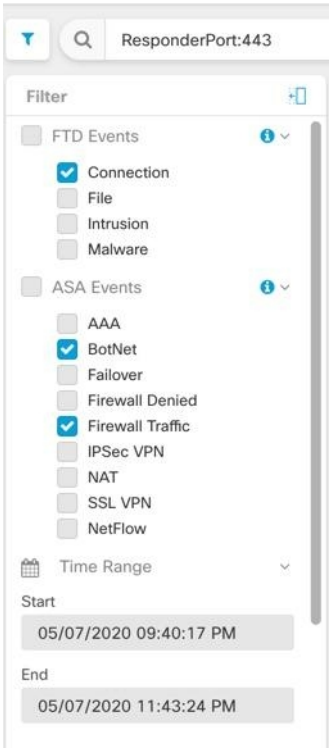
**步骤 3** 滚动到过滤器栏的底部，并确保**取消选中包括 NetFlow 事件 (Include NetFlow Events)** 过滤器。

**步骤 4** 向上滚动到 ASA 事件过滤器树，并确保 **取消选中 NetFlow** 框。

**步骤 5** 选择 ASA 其余部分或 FTD 过滤条件。

# 组合过滤器元素

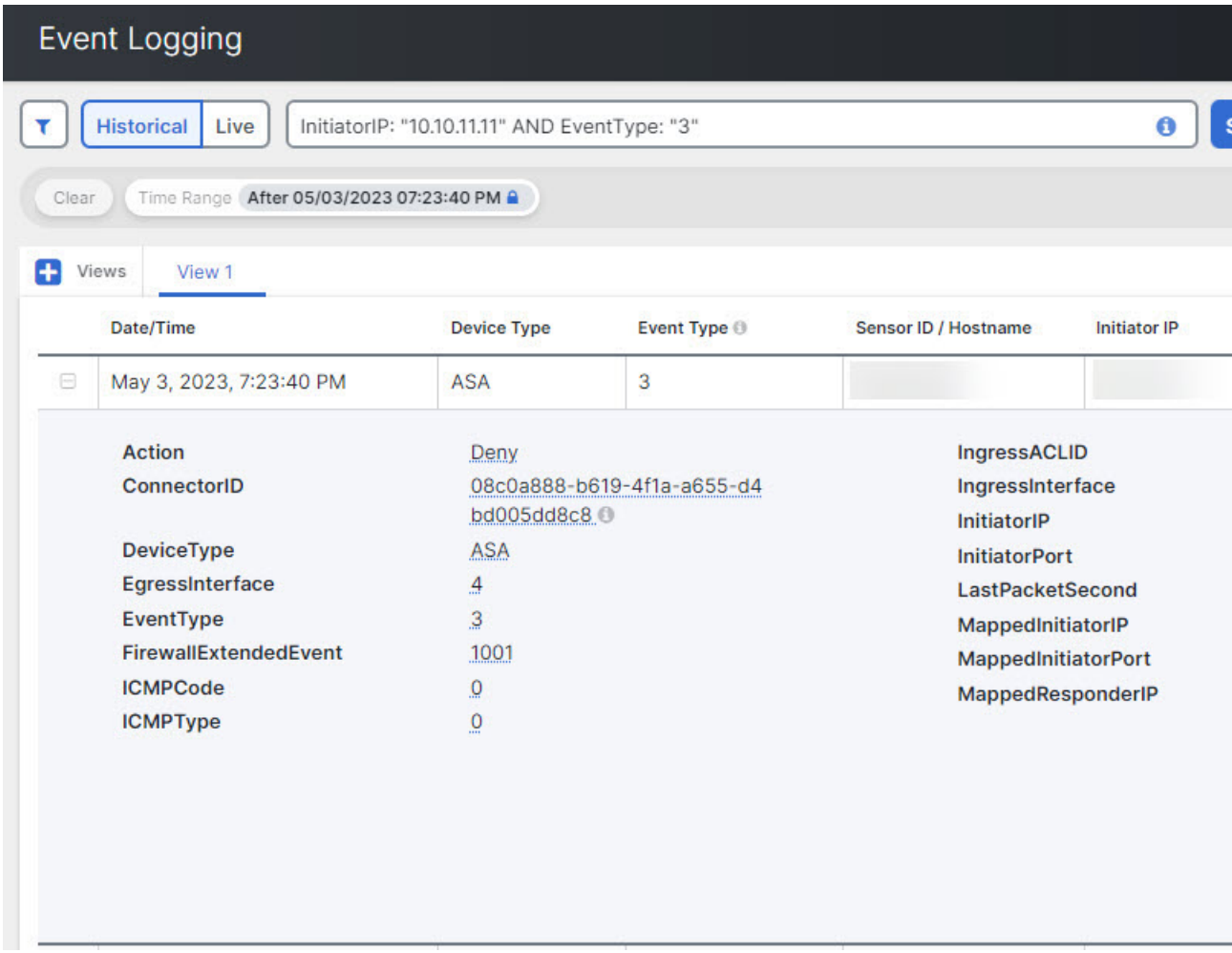
过滤事件通常遵循 CDO 中的标准过滤规则：过滤类别为“AND-ed”，类别中的值“OR-ed”。您还可以将过滤器与您自己的搜索条件配合使用。对于事件过滤器；但是，设备事件过滤器也是“OR-ed”。例如，如果在过滤器中选择了这些值：




使用此过滤器时，CDO 将显示 威胁防御 设备连接事件**或** ASA 僵尸网络**或**防火墙流量事件，**以及**时间范围内两个时间之间发生的事件，**并且**还包含响应器端口 443 的事件。您可以按时间范围内的历史事件进行过滤。实时事件页面会始终显示最新事件。

### 搜索特定属性：值对

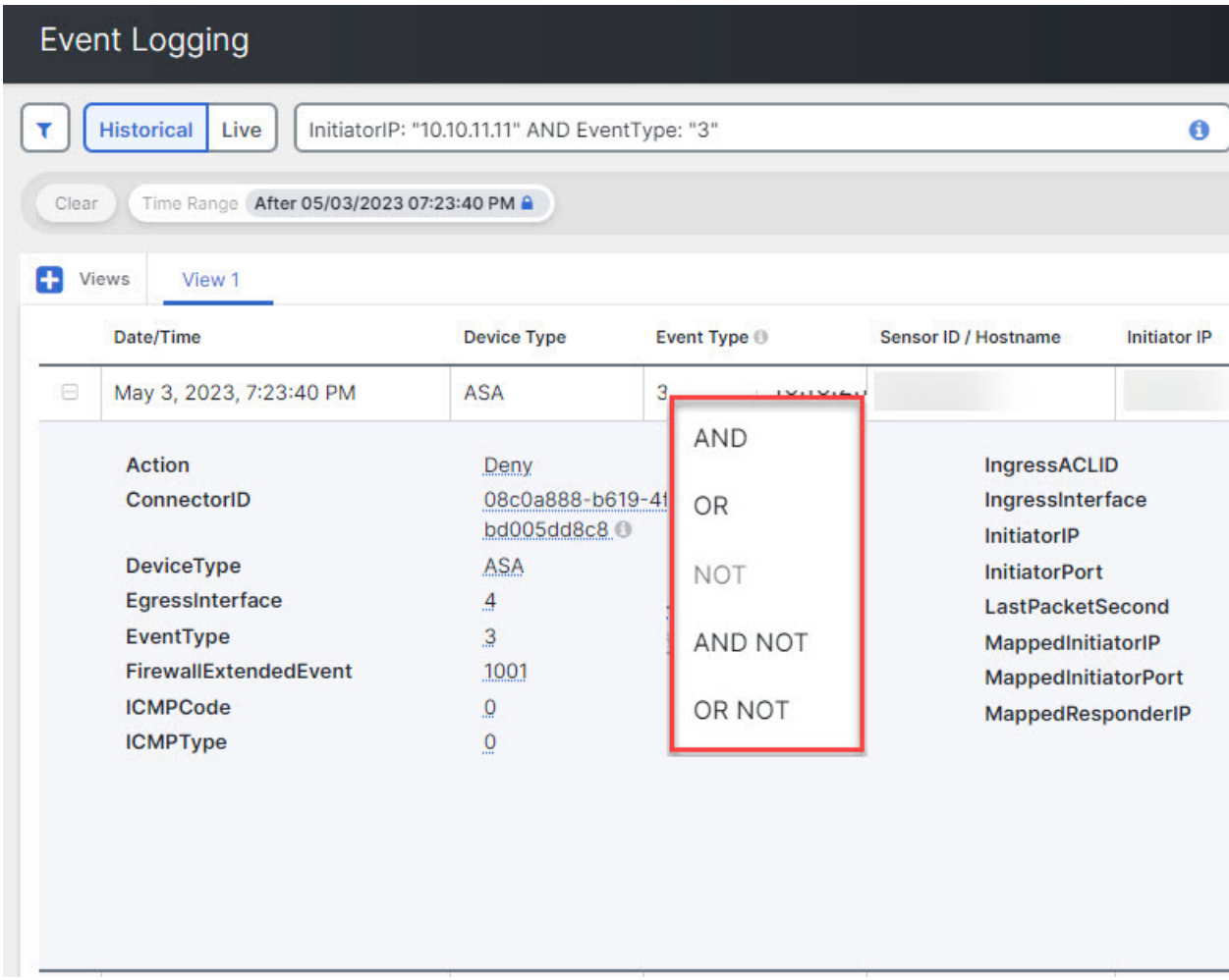
您可以通过在搜索字段中输入事件属性和值来搜索实时或历史事件。执行此操作的最简单方法是在“事件日志记录”(Event Logging) 表中点击要搜索的属性，然后 CDO 会在“搜索”(Search) 字段中输入该属性。在滚动鼠标时，您可以点击的事件会显示为蓝色。以下为输出示例：




在本示例中，通过滚动“InitiatorIP”值 10.10.11.11 并点击它即可开始搜索。发起方 IP 及其值已被添加到搜索字符串中。接下来，滚动并点击事件类型 3，然后将其添加到搜索字符串中，并且 CDO 添加了 AND。因此，此搜索的结果将是从 10.10.11.11 和 3 种事件类型发起的事件列表。

请注意上面示例中值3旁边的放大镜。如果将鼠标悬停在放大镜上，您还可以选择AND、OR、AND NOT 和 OR NOT 运算符来匹配要添加到搜索中的值。

在下面的示例中，选择的是“OR”。此搜索的结果将是从 10.10.11.11 或 106023 种事件类型发起的事件列表。请注意，如果搜索字段为空，并且您右键点击表中的值，则只有NOT可用，因为没有其他值。




只要滚动鼠标指针并将其突出显示为蓝色，您就可以将该值添加到搜索字符串中。

### AND、OR、NOT、AND NOT 和 OR NOT 过滤器运算符

以下是在搜索字符串中使用的“AND”、“OR”、“NOT”、“AND NOT”和“OR NOT”的行为：

**和**

在过滤器字符串中使用 AND 运算符可以查找包含所有属性的事件。AND 运算符不能位于搜索字符串的开头。

例如，下面的搜索字符串将搜索包含 TCP 协议、源自发起方 IP 地址 10.10.10.43 且从发起方端口 59614 发送的事件。正常情况下，每增加一个 AND 语句，符合条件的事件数量就会越来越少。

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

**或**

在过滤器字符串中使用OR运算符可以查找包含任何属性的事件。OR运算符不能位于搜索字符串的开头。

例如，下面的搜索字符串将在事件查看器中显示事件，这些事件包括 TCP 协议、源自发起方 IP 地址 10.10.10.43 或从发起方端口 59614 发送的事件。正常情况下，每增加一个 OR 语句，符合条件的事件数量就会越来越多。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

### 不

仅在搜索字符串的开头使用此选项，以便排除具有某些属性的事件。例如，此搜索字符串将从结果中排除任何具有 InitiatorIP 192.168.25.3 的事件。

```
NOT InitiatorIP: "192.168.25.3"
```

### AND NOT

在过滤器字符串中使用 AND NOT 运算符可以排除包含某些属性的事件。AND NOT 不能用于搜索字符串的开头。

例如，此过滤器字符串将显示发起方 IP 为 192.168.25.3 的事件，但不会显示响应方 IP 地址为 10.10.10.1 的事件。

```
InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

您还可以组合使用 NOT 和 AND NOT，从而排除多个属性。例如，此过滤器字符串将排除具有 InitiatorIP 192.168.25.3 的事件以及具有 ResponderIP 10.10.10.1 的事件

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

### OR NOT

使用 OR NOT 运算符可包含排除了某些元素的搜索结果。OR NOT 运算符不能用于搜索字符串的开头。

例如，此搜索字符串将查找协议为 TCP 或发起方 IP 为 10.10.10.43 的事件，或者非发起方端口 59614 的事件。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

您也可以这样考虑：搜索 (Protocol: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614")。

### 通配符搜索

使用星号 (*) 表示属性值字段中的 **attribute:value** 搜索可在事件中查找结果。例如，此过滤器字符串，

```
URL:*feedback*
```

将在事件的 URL 属性字段中查找包含字符串 **feedback** 的字符串。

### 相关信息：

- 在事件日志记录页面上显示和隐藏列
- 安全分析和日志记录中的事件属性

# 在后台搜索历史事件

通过CDO，您可以定义搜索条件，并根据任何已定义的搜索条件来搜索事件日志。通过使用后台搜索功能，您还可以在后台执行事件日志搜索，并在后台搜索完成后查看搜索结果。

根据您配置的订用警报和服务集成，当后台搜索完成后，您会收到通知。

您可以直接从“后台搜索”页面查看、下载或删除搜索结果。您还可以安排对一次性事件进行后台搜索，或安排周期性安排。导航至“通知设置”(Notification Settings) 页面以查看或修改订用选项。

# 在事件日志记录页面中搜索事件

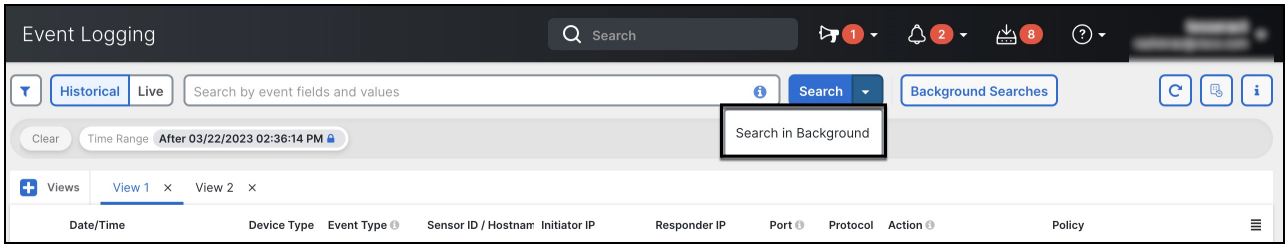
使用搜索和后台搜索功能查看“事件日志记录”(Event Logging) 页面中记录的所有事件。请注意，只能对历史事件执行后台搜索。

**步骤 1** 在导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**历史 (Historical)** 或**实时 (Live)** 选项卡。

**步骤 3** 导航至搜索栏，键入搜索表达式，然后输入 **搜索 (Search)** 按钮以执行搜索。您可以使用绝对时间范围或相对时间范围来缩小或扩大搜索范围。

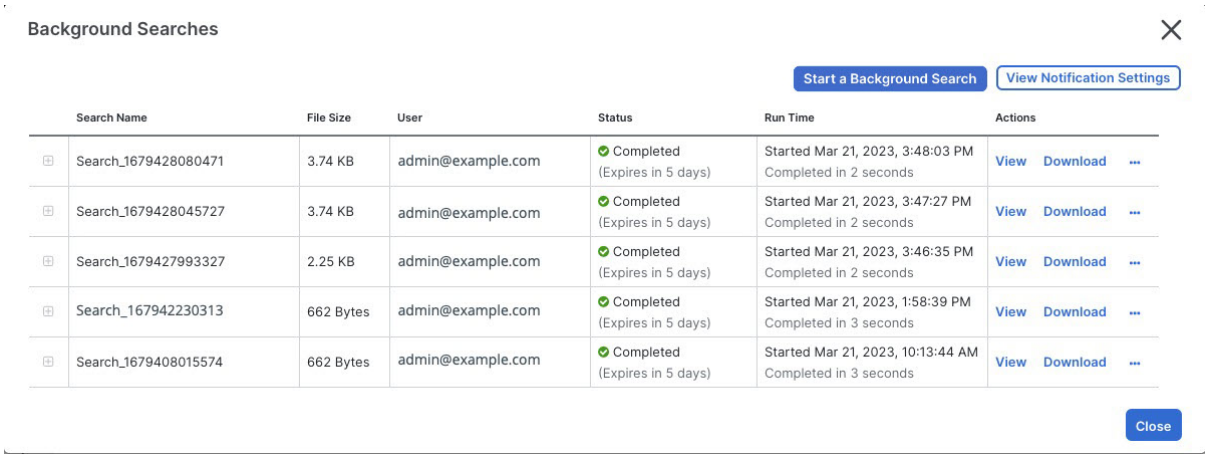
或者，从搜索下拉列表中选择在后台搜索，以便在离开搜索页面时在后台执行搜索。当搜索结果准备就绪时，您会收到通知。




如果点击**搜索 (Search)** 按钮，结果将直接显示在事件日志记录视图中。选择任何特定搜索结果后，搜索条件会显示在搜索栏中，以便于参考。

如果您选择在后台执行搜索，搜索操作会加入队列，并在搜索完成后通知您。您可以在后台执行多个搜索查询。

**步骤 4** 点击“背景搜索”按钮以查看“背景搜索”页面。




“后台搜索”页面显示搜索结果列表。您可以选择查看、下载或删除搜索结果。您还可以导航至“通知设置”页面以查看或修改订用选项。选择**开始后台搜索 (Start a Background Search)** 按钮可从此页面启动搜索。

### 下一步做什么

如果需要重复查询，您可以将任何后台搜索转换为计划后台搜索。有关详细信息，请参阅在事件查看器中计划后台搜索，第 458 页。

# 在事件查看器中计划后台搜索

在事件查看器页面的后台计划定期查询。只能为历史事件安排搜索。您可以随时修改或取消预定搜索。您还可以将现有查询修改为周期性搜索。

**注释** 您可以选择获取有关已开始、已完成或已失败的搜索的警报。

只能为**历史**事件安排后台搜索。使用以下步骤创建计划的后台搜索：

**步骤 1** 在导航栏中，选择**分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**历史 (Historical)** 开关将其选中。您只能为历史事件安排后台搜索。

**步骤 3** 在搜索栏中，键入要搜索的搜索表达式。点击**搜索 (Search)** 下拉按钮，然后选择**在后台搜索 (Search in background)**。

**步骤 4** （可选）重命名搜索。

**步骤 5** 默认情况下，**立即搜索 (Search Now)** 复选框处于选中状态。如果已选中，将在保存时开始搜索；如果取消选中，则后台查询仅作为未来搜索运行。

**步骤 6** 检查**设置定期计划 (Setup recurring schedule)** 并配置以下设置：

- **搜索最近日志 (Search Logs for the Last)** - 要搜索多长时间以前的日志。
- **频率 (Frequency)** - 您希望进行预定搜索的频率。

**步骤 7** 确认窗口底部的计划搜索条件。选择**计划并立即搜索 (Schedule and Search Now)**。或者，如果您没有选择立即开始搜索，则该按钮显示为**计划搜索 (Schedule Search)**

### 下一步做什么

计划后台搜索的结果最多可查看 7 天，然后 CDO 会自动将其删除。

# 下载后台搜索

搜索结果和计划查询会在 CDO 自动删除之前存储 7 天。下载对历史事件执行的后台搜索的 CSV 副本。

**步骤 1** 在导航窗格中，转到**分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**后台搜索 (Background Searches)** > **操作 (Actions)** > **下载 (Download)**。

**步骤 3** 找到您的搜索内容。计划的搜索存储在**查询 (Queries)** 选项卡下。

**步骤 4** 点击 **Download**。.CSV 文件会自动下载到本地驱动器上的默认存储位置。

# 数据存储计划

您需要购买反映思科云每天从您载入的 ASA 和 FDM 托管 设备接收的事件数量的数据存储计划。这称为“每日注入速率”。数据计划有整数 GB/天和 1 年、3 年或 5 年期限。确定注入速率的最佳方法是在购买之前参加安全日志分析 (SaaS) 的免费试用。这将为您提供对事件数量的一个很好的估计。

客户自动获得 90 天的滚动数据存储。这意味着最近 90 天的事件存储在思科云中，第 91 天将被删除。

客户可以升级到超过默认90天的额外事件保留，或通过更改订单对现有订用添加额外的每日量（GB/天），并且只需按比例为剩余的订用期限计费。

有关数据计划的所有详细信息，请参阅《安全日志分析 (SaaS) 订购指南》。

**Note** 如果您拥有安全分析和日志记录许可证和数据计划，然后在之后获得了不同的安全分析和日志记录许可证，则无需获得不同的数据计划。如果您的网络流量吞吐量发生变化，并且您获得了不同的数据计划，则不需要您获得不同的安全分析和日志记录许可证。

### 我的配额会统计哪些数据？

发送到安全事件连接器的所有事件都在安全日志分析 (SaaS) 云中累积，并根据您的数据分配进行计数。

过滤您在事件查看器中看到的内容并不会减少安全日志分析 (SaaS) 云中存储的事件数量，而是会减少您可以在事件查看器中看到的事件数量。

您的事件在安全日志分析 (SaaS) 云中存储 90 天；之后，它们将被清除。

**我们的存储配额很快用尽，我们该怎么办？**

以下是解决该问题的两种方法：

- 请求更多存储空间。https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html您可能低估了您的需求。
- 减少记录事件的规则数量。您可以从 SSL 策略规则、安全情报规则、访问控制规则以及入侵策略以及文件和恶意软件策略中记录事件。检查您正在记录的内容。您是否需要记录尽可能多的规则和策略的事件？

# 延长事件存储持续时间并增加事件存储容量

安全分析和日志记录客户在购买任何这些许可证时都会收到 90 天的事件存储。许可，第 348 页

- **日志记录故障排除**
- **日志记录分析和检测**
- **全面的网络分析和监控**

您可以选择在首次购买许可证时或在许可证有效期内的任何时间将许可证升级为具有 1 年、2 年或 3 年的滚动事件存储。

首次购买安全分析和日志记录许可证时，系统会询问您是否要升级存储容量。如果您回答“是”，系统会在您购买的 PID 列表中添加一个额外的产品标识符 (PID)。

如果您在许可期限中间决定扩展滚动事件存储或增加事件云存储量，您可以：

**步骤 1** 在思科商务工作空间上登录您的账户。

**步骤 2** 选择您的 Cisco Defense Orchestrator PID。

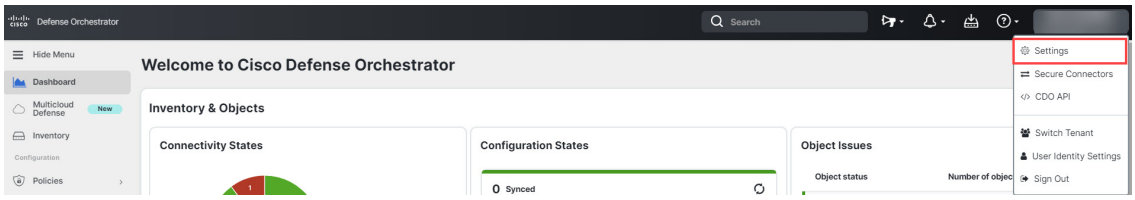
**步骤 3** 按照提示升级存储容量的长度或容量。

增加的成本将根据现有许可证的剩余期限按比例分配。有关详细说明，请参阅《安全日志分析 (SaaS) 订购指南》。

# 查看安全分析和日志记录数据计划的使用情况

要查看每月的日志记录限制、已使用的存储量以及使用期何时重置为零，请执行以下操作：

**步骤 1** 点击租户，选择**设置 (Settings)**。




**步骤 2** 点击**日志记录设置 (Logging Settings)**。

**步骤 3** 您还可以点击**查看历史使用情况 (View Historical Usage)**，查看最近 12 个月的存储使用情况。

# 查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口

安全日志分析 (SaaS) 允许您将事件从您的 ASA 或 FDM 管理 设备发送到安全事件连接器 (SEC) 上的某些 UDP、TCP 或 NSEL 端口。然后，SEC 会将这些事件转发到思科云。

如果这些端口尚未被占用，SEC 会将其用于接收事件，而安全日志分析 (SaaS) 文档会建议您在配置功能时使用这些端口。

- TCP：10125
- UDP：10025
- NSEL：10425

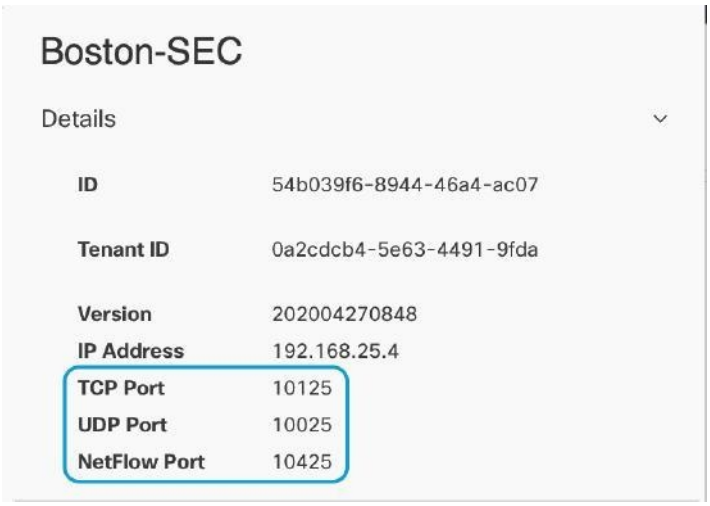
如果这些端口已被占用，则在配置安全日志记录分析 (SaaS) 之前，请查看 SEC 设备详细信息，以确定其实际用于接收事件的端口。

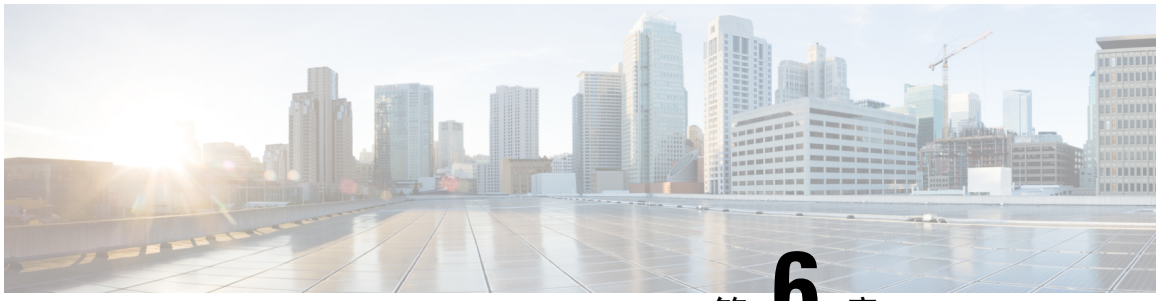
要查找 SEC 使用的端口号，请执行以下操作：

**步骤 1** 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 2** 在“安全连接器”(Secure Connectors) 页面中，选择要向其发送事件的 SEC。

**步骤 3** 在“详细信息”(Details) 窗格中，您将看到应向其发送事件的 TCP、UDP 和 NetFlow (NSEL) 端口。


Boston-SEC
Details
ID
54b039f6-8944-46a4-ac07
Tenant ID
0a2cdcb4-5e63-4491-9fda
Version
202004270848
IP Address
192.168.25.4
TCP Port
10125
UDP Port
10025
NetFlow Port
10425



第 6 章

# 将客户安全地连接到思科安全互联网网关 (SIG)



## 使用 Cisco Defense Orchestrator 管理 Umbrella

Umbrella 是思科基于云的安全互联网网关 (SIG) 平台，可针对基于互联网的威胁提供多个级别的防御。Umbrella 集成了安全的 Web 网关、防火墙、DNS 层安全和云访问安全代理 (CASB) 功能，以保护系统抵御威胁。通过利用 SIG 和 DNS 保护，ASA 设备将同时受到设备上的本地 DNS 检测策略和基于云的 DNS 检测策略的保护。通过提供多种检查和检测传入流量的方法，Umbrella 使 ASA 设备可与 FTD 下一代防火墙 (NGFW) 相媲美。

目前，CDO 仅支持 ASA 与 Umbrella 组织的集成。

### 使用 SASE 构建网桥

安全访问服务边缘 (SASE) 是一种前瞻性框架，其中网络和安全功能融合为单一集成服务，可在云边缘提供保护和性能。无论您身在何处，这种努力都可以安全可靠地整合服务，并且无论您的组织规模如何，都可以控制和管理您的网络。降低复杂性和灵活的管理意味着您的部署简单、可扩展且安全。

### 什么是 Umbrella 组织？

Umbrella 组织是与单个许可证密钥关联的具有不同用户角色的用户组；一个用户可以访问多个 Umbrella 组织。每个 Umbrella 组织都是一个单独的 Umbrella 实例，并且有自己的控制面板。组织通过其名称和组织 ID（组织 ID）进行标识。组织 ID 用于标识用于部署虚拟设备等组件的组织，有时支持人员可能会要求您提供组织 ID。

### 什么是 SIG 隧道？

安全互联网网关 (SIG) 隧道是发生在 ASA 和 Umbrella 之间的 SIG IPSec（互联网协议安全）隧道的实例，其中所有互联网绑定流量都转发到 Umbrella SIG 进行检查和过滤。此解决方案提供集中式安全管理，因此网络管理员不必单独管理每个分支机构的安全设置。

当您载入已配置隧道的 Umbrella 组织时，这些隧道将在 CDO 的站点间 VPN 页面中列出。要从 CDO UI 为您的 Umbrella 组织创建 SASE 隧道，请参阅为 Umbrella 配置 SASE 隧道。

注释 如果您载入 Umbrella 组织及其对等设备，则站点间 VPN 页面会将与该组织关联的隧道的所有设备合并为一个条目。要手动刷新“隧道”(Tunnels) 页面并读取从 Umbrella 控制面板所做的任何更改，请参阅读取 Umbrella 隧道配置。

### CDO 如何与 Umbrella 通信？

您必须载入 Umbrella 组织以及与该组织关联的任何 ASA 设备。

当 ASA 设备与 Umbrella 云关联时，该连接需要站点间 VPN SIG 隧道来在设备和云之间创建安全连接。CDO 与 Umbrella 组织和 ASA 设备进行通信。这种双重通信方法使 CDO 能够即时检测配置更改或隧道更改，并立即提醒您 Umbrella、ASA 和隧道的更改越界、错误或运行状况不佳。

当您将 Umbrella 组织载入 CDO 时，您需要使用该组织的 API 密钥和密钥载入，这两个密钥对组织和与该组织关联的 ASA 设备都是唯一的。CDO 会通过 Umbrella API 与 Umbrella 云通信，使用用于载入组织的 API 密钥和密钥来请求和发送有关 ASA 设备的信息。此级别的通信不会影响 ASA 和 Umbrella 云之间的 SIG 隧道。

载入 Umbrella 组织后，“设备和服务”(Devices & Services) 页面会将检测到的与该组织关联的任何 ASA 设备显示为“对等体”，并注明设备是否已载入到CDO。如果对等设备尚未载入，您可以点击“载入设备”(Onboard Device) 直接从该页面载入。当与 Umbrella 组织关联的 ASA 设备载入 CDO 时，“设备和服务”(Devices & Services) 页面会显示关系，而“VPN 隧道”(VPN Tunnels) 页面会显示设备与组织之间的隧道。如果与组织关联的 ASA 设备未载入到 CDO，则与该设备关联的隧道会显示在 VPN 隧道中，您可以选择直接从此页面载入设备。

### 如何从 CDO 访问 Umbrella 云？

将 Umbrella 组织成功载入 CDO 后，您可以从 CDO UI 交叉启动到组织的控制面板或 Umbrella 隧道页面。

请参阅 交叉启动到 Umbrella 控制面板， 第 468 页 和 交叉启动到 Umbrella 隧道页面， 第 469 页 并从 CDO UI 访问 Umbrella 云。

### 前提条件

#### 硬件和软件支持。

Umbrella 组织基于云，因此无版本。请注意，当您将 Umbrella 组织载入 CDO 时，您只能将该组织与 ASA 设备关联。

对于 Umbrella 集成，CDO 支持运行 9.1.2 及更高版本的 ASA 设备。有关 CDO 支持的 ASA 设备型号和软件的列表，请参阅云设备支持详情， 第 36 页。

#### 许可要求

要成功将 Umbrella 组织载入 CDO，您必须选择以下许可证包之一：

- Umbrella SIG Essentials
- SIG 优势

### 载入

要成功管理 Umbrella 账户，必须同时载入 载入 Umbrella 组织 和与其关联的 将 ASA 设备载入 CDO。载入 Umbrella 组织后，CDO 将读取与该组织关联的任何现有 ASA 隧道，并监控这些隧道以及您创建并与该组织关联的任何其他隧道的运行状况。在载入 Umbrella 组织之前，请查看一般设备要求和载入必备条件。

如果您在载入与其关联的任何 ASA 设备之前载入 Umbrella 组织，则可以从 **站点间 VPN** (Site-to-site VPN) 页面查看 ASA 对等体，并从“VPN”页面载入设备。

**注释** 如果为故障切换配置了 ASA 对，则必须 仅载入两个对等体中的主用设备。将主用和备用设备载入到 CDO 可能会为 Umbrella 中已配置的 SASE 隧道生成重复的隧道信息。

### 监控网络

CDO 提供总结安全策略的影响的报告，以及查看这些安全策略触发的显着事件的方法。CDO 还会记录您对设备所做的更改，并为您提供一种标记这些更改的方法，以便您可以将您在 CDO 中提交的工作与帮助请求或其他操作请求相关联。

### 变更日志

变更日志会持续捕获在 CDO 中进行的配置更改。此单一视图包括所有受支持设备和服务的更改。由于 Umbrella 是基于云的产品，因此会立即部署更改。

以下是更改日志的一些功能：

- 并排比较对设备配置所做的更改。
- 所有更改日志条目的纯英文标签。
- 记录设备的载入和删除。
- 检测在 CDO 之外发生的策略更改冲突。
- 回答事件调查或故障排除期间的人员、内容和时间。
- 可以将完整更改日志或仅一部分下载为 CSV 文件。

**注释** 请注意，当您创建、编辑或删除与 Umbrella 组织关联的 SASE 隧道时，系统会为该 Umbrella 组织以及与其关联的任何 ASA 设备显示请求和配置更改。

**Umbrella 文档**

- Umbrella 帮助
- Umbrella 和思科 ASA 配置
- 通过隧道连接到思科 Umbrella
- 思科 Umbrella API

# 载入 Umbrella 组织

## Umbrella 许可证要求

要成功将 Umbrella 组织载入 CDO，您必须从 Umbrella 控制面板中选择以下许可证包之一：

- Umbrella SIG Essentials
- SIG 优势

要验证当前已启用的许可证，请登录 Umbrella 控制面板并导航至**管理员 (Admin)** > **许可 (Licensing)**。

## 生成 API 密钥和秘密

在将 Umbrella 组织载入 CDO 之前，请生成新的 API 密钥并 **同时** 检索 **API 密钥**和相应的**密钥**。

如果当前没有 API 密钥，请使用以下程序创建一个：

**开始之前**

来自 Umbrella 的管理 API 密钥用于以下 Umbrella 服务：

- 网络和域
- 网络隧道
- 用户和角色
- 目标列表
- 服务提供商

如果不允许 CDO 访问这些服务，则无法载入 Umbrella 组织。

---

**步骤 1** 访问思科 Umbrella 控制面板 (Cisco Umbrella dashboard) 并登录您的组织。

**步骤 2** 在 Umbrella 控制面板中，点击左侧导航窗格中的**管理员 (Admin)**，然后选择 **API 密钥 (API Keys)**。

**步骤 3** 点击**创建 API 密钥 (Create API Key)**。

如果您已有 API 密钥，但未保存密钥，请导航至**管理员 (Admin)** > **API 密钥 (API Keys)**屏幕，然后点击**刷新 (Refresh)** 以更新密钥和密钥。

**步骤 4** 要创建新的 API 密钥和密钥，请点击 + 按钮。

**步骤 5** 输入**名称**并将以下范围添加到 API 密钥：

- 部署。
- 策略。

**步骤 6** 点击**生成密钥 (Generate Key)**。

**步骤 7** 复制 API 密钥和相应的密钥。我们建议暂时将信息粘贴到备注或 .txt 中，直到您准备使用它。

# Umbrella 组织 ID

您必须使用 Umrbrella 组织的查找组织 ID，并将其与登录凭证一起使用，才能将组织成功载入 CDO：

**步骤 1** 访问 Cisco Umbrella 控制面板并登录您的组织/

**步骤 2** 页面 URL 将包含数字标识符。例如，https://dashboard.umbrella.com/o/**123456**/#/overview 的组织 ID 是 **123456**。

**步骤 3** 从 URL 复制组织 ID。我们建议暂时将信息粘贴到备注中，直到您准备使用它。

# 载入 Umbrella 组织

使用以下程序将 Umbrella 组织载入 CDO：

### 开始之前

在载入此环境之前，请阅读Umbrella 许可证要求，第 466 页。

**步骤 1** 在 Umbrella 控制面板中，找到Umbrella 组织 ID，第 467 页和生成 API 密钥和秘密，第 466 页。在此过程中，请准备好这些项目。

**步骤 2** 登录至 CDO。

**步骤 3** 在导航栏中，点击**清单 (Inventory)**。

**步骤 4** 点击蓝色加号按钮以开始载入设备。

**步骤 5** 点击 Umbrella 组织。

**步骤 6** 输入您从 Umbrella 控制面板生成的 Umbrella 网络设备的 **API 密钥**和对应的**密钥**，以及 Umbrella 控制面板 URL 中的**组织 ID**。

**步骤 7** 点击**下一步**。

**步骤 8** （可选）为设备添加唯一**标签**。您可以稍后按此标签过滤设备列表。

**步骤 9** 点击**转至清单 (Go to Inventory)**。

# 将 Umbrella 组织重新连接到 CDO

**警告** 如果存储的凭证无效，则CDO无法向Umbrella组织成功部署或读取配置更改，但CDO可以从与该组织关联的任何ASA设备成功部署或读取更改。更新和验证凭证后，这可能会导致问题。我们建议在部署任何配置更改之前更新组织凭证。

如果 Umbrella 组织的 API 密钥和密钥已刷新或已超时，则必须手动将 Umbrella 组织重新连接到 CDO。使用以下程序重新连接：

**步骤 1** 前往 Umbrella 控制面板。在左侧导航窗格中点击**管理 (Admin)**，然后选择现有的 Umbrella 管理 **API 密钥**。

**步骤 2** 点击**刷新**。确认要刷新 API 密钥和密钥。

**步骤 3** 复制 API 密钥和相应的密钥。

**步骤 4** 登录至 CDO。

**步骤 5** 导航至**清单 (Inventory)** 页面。

**步骤 6** 使用 过滤器或搜索栏查找 Umbrella 组织。

**步骤 7** 在**设备操作 (Device Actions)** 窗格中，点击**重新连接 (Reconnect)**。CDO 确认存储的 API 密钥和密钥不再有效。

**步骤 8** 将 API 密钥和密钥粘贴到相应的弹出窗口中。

**步骤 9** 点击**继续 (Continue)**。

**步骤 10** CDO确认新密钥和密钥有效后，点击**关闭**。

# 交叉启动到 Umbrella 控制面板

一旦 ASA 设备和 Umbrella 组织被成功载入 CDO，您就可以从 CDO UI 交叉启动到组织的控制面板。

使用以下程序来交叉启动设备的 Umbrella 控制面板：

**步骤 1** 登录 CDO。

**步骤 2** 点击**设备和服务 (Devices & Services)**。

**步骤 3** 查找或过滤器 Umbrella 组织。

**步骤 4** 点击管理窗格中的**管理 Umbrella 组织 (Manage Umbrella Organization)** 。CDO 在您的浏览器中启动了一个新选项卡，该选项卡将打开与所选组织关联的 Umbrella 控制面板。

## 从CDO删除设备

使用以下程序可从 中删除设备：CDO

**步骤 1** 登录至 CDO。

**步骤 2** 导航至**清单 (Inventory)** 页面。

**步骤 3** 找到要删除的设备，然后选中设备行中的设备以将其选中。

**步骤 4** 在右侧的“设备操作”(Device Actions) 面板中，选择**删除 (Remove)**。

**步骤 5** 出现提示时，选择**确定 (OK)** 以确认删除所选设备。选择**取消 (Cancel)** 以使设备保持已载入状态。

# 配置 Cisco Umbrella 组织

## 读取 Umbrella 隧道配置

在 Umbrella 组织载入到 CDO 后，您可以手动强制 CDO 从 Umbrella 请求和更新隧道配置。这包括添加、删除或修改的隧道。

**警告** 如果在 Umbrella 组织凭证被视为无效的情况下从 CDO 中删除隧道，或者在您载入组织后发生了变化，则 CDO 只能将隧道配置部署到与该组织关联的 ASA 设备。更新凭证后，CDO 会读取 Umbrella 配置并重新填充已删除的任何隧道。由于隧道存在于 Umbrella 组织中，但不存在于任何 ASA 设备中，因此会出现同步问题，并且 ASA 设备可能不会显示为组织的对等体。

**步骤 1** 登录 CDO。

**步骤 2** 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

**步骤 3** 点击 **ASA** 选项卡。

**步骤 4** 选择 Umbrella 组织，使其突出显示。

**步骤 5** 在 **操作** 窗格中，选择 **读取隧道**。

## 交叉启动到 Umbrella 隧道页面

在将 ASA 设备和 Umbrella 组织成功载入 CDO 后，您可以从 CDO UI 交叉启动隧道的 Umbrellas 控制面板。

使用以下程序交叉启动设备的 Umbrella 隧道页面：

**步骤 1** 登录 CDO。

**步骤 2** 导航到 VPN 窗口。选择**站点间 VPN (Site-to-Site VPN)**。

**步骤 3** 选择所需的隧道，使其突出显示。

**步骤 4** 在“操作”(Actions) 窗格中，点击**管理 Umbrella 中的隧道 (Manage Tunnel in Umbrella)**。CDO 在浏览器中启动一个新选项卡，打开“隧道”(Tunnels) 概述页面。

# 为 Umbrella 配置 SASE 隧道

使用以下程序为 Umbrella 组织创建一个 SASE 隧道：

### 开始之前

请注意，您要为其创建隧道的 Umbrella 组织和 ASA 设备**必须**已经载入 CDO。

如果与您刚部署的隧道关联的 ASA 或 Umbrella 组织处于不正常状态，则 CDO 可能无法成功部署隧道。如果您遇到任何问题，请联系思科 TAC。

**步骤 1** 登录 CDO。

**步骤 2** 导航到 **VPN** 窗口。选择**站点间 VPN (Site-to-Site VPN)**。

**步骤 3** 点击蓝色加号按钮，然后选择**创建 SASE 隧道 (Create SASE Tunnel)**。

**步骤 4** 输入 Umbrella 对等体信息：

- **选择 Umbrella (Select Umbrella)** - 选择您所选的 **Umbrella** 组织。
- **数据中心 (Datacenter)** - 选择前端数据中心。我们建议选择在地理位置上靠近与 Umbrella 组织关联的 ASA 的数据中心。

**步骤 5** 输入 ASA 对等体信息：

- **选择 ASA 设备 (Select ASA Device)** - 从下拉列表中选择与 Umbrella 组织关联的 ASA 设备，然后点击**选择 (Select)**。
- **公共接口 (Public Facing Interface)** - 选择静态且可公开路由的 IPv4 地址。所用的地址不应被用于 NAT。
- **LAN 地址 (LAN Address)** - 选择控制 LAN 子网的 LAN 接口。您必须至少为 LAN 选择一个接口。
- **虚拟隧道接口 (Virtual Tunnel Interface)** - 在选择 Umbrella 组织和 ASA 对等设备后，系统会自动填充此字段。如有必要，您可以手动输入要用作新 VTI 的 IP 地址。

**步骤 6** 在选择 Umbrella 组织和 ASA 对等设备后，系统会自动填写**密码**。**确认密码 (Confirm Passphrase)** 也会被自动填写。如有必要，您可以手动输入这些字段。

**步骤 7** （可选）弹出窗口底部的**立即部署对 ASA 的更改 (Deploy changes to ASA immediately)** 会被默认启用。如果启用，SASE 隧道配置会立即部署到在隧道配置中选择的 ASA 对等体。如果要暂存更改并稍后部署，请手动将该选项切换为禁用。

**步骤 8** 点击**部署 (Deploy)**。或者，点击**部署并创建另一个 (Deploy and Create Another)**，以便同时部署此 SASE 隧道并创建另一个隧道。部署后，隧道将显示在“VPN 隧道”(VPN Tunnels) 页面中。如果您选择**部署并创建另一个 SASE 隧道 (Deploy and Create Another SASE tunnel)**，CDO 会同时保存 Umbrella 组织选择和**将更改立即部署到 ASA (Deploy changes to ASA immediately)** 切换设置，并自动将这些选择应用到下一个隧道配置。您可以在部署之前手动更改这些选择。

# 编辑 SASE 隧道

使用以下程序修改现有 SASE 隧道：

**步骤 1** 登录 CDO。

**步骤 2** 导航到 **VPN** 窗口。选择**站点间 VPN (Site-to-Site VPN)**。

**步骤 3** 选择要修改的隧道。

**步骤 4** 在“操作”(Actions) 窗格中，选择**编辑 (Edit)**。

**步骤 5** 编辑 SASE 隧道的以下字段：

- **名称** - 更改 CDO 和 Umbrella 控制面板中显示的 SASE 隧道的名称。
- **Umbrella 对等体的数据中心** - 从下拉菜单中选择新的前端数据中心。
- **ASA 对等体的公共接口** - 从下拉菜单中选择新的 IPv4 地址。
- **ASA 对等体的 LAN 接口** - 从下拉菜单中选择一个或多个新的 LAN 接口。
- **ASA 虚拟隧道接口 (VTI) 地址** - 手动编辑 VTI。
- **密码** - 手动修改隧道的密码。
- **确认密码** - 手动修改此条目以匹配密码并确认新值。

**步骤 6** （可选）弹出窗口底部的**立即部署对 ASA 的更改 (Deploy changes to ASA immediately)** 会被默认启用。如果启用，SASE 隧道配置会立即部署到在隧道配置中选择的 ASA 对等体。如果要暂存更改并稍后部署，请手动将该选项切换为禁用。如果您选择暂存更改并稍后部署，则**清单 (Inventory)** 页面中的 ASA 对等体状态显示为`待部署 (Deploy Pending)`。

**步骤 7** 选择**保存更新**。

# 从 Umbrella 中删除 SASE 隧道

使用以下程序通过 CDO UI 删除 SASE 隧道：

### 开始之前

要删除 SASE 隧道，与其关联的 ASA 在 CDO 中必须处于同步状态。如果设备运行状况不佳，则无法删除隧道。

请注意，如果从 CDO 中删除 SASE 隧道，则会从 ASA 设备和与其关联的 Umbrella 组织中删除该隧道。

**警告** 如果在 Umbrella 组织凭证被视为无效的情况下从 CDO 中删除隧道，或者在您载入组织后发生了变化，则 CDO 只能将隧道配置部署到与该组织关联的 ASA 设备。更新凭证后，CDO 会读取 Umbrella 配置并重新填充已删除的任何隧道。由于隧道存在于 Umbrella 组织中，但不存在于任何 ASA 设备中，因此会出现同步问题，并且ASA 设备可能不会显示为组织的对等体。我们建议在删除与组织关联的任何隧道之前确认 Umbrella 凭证。

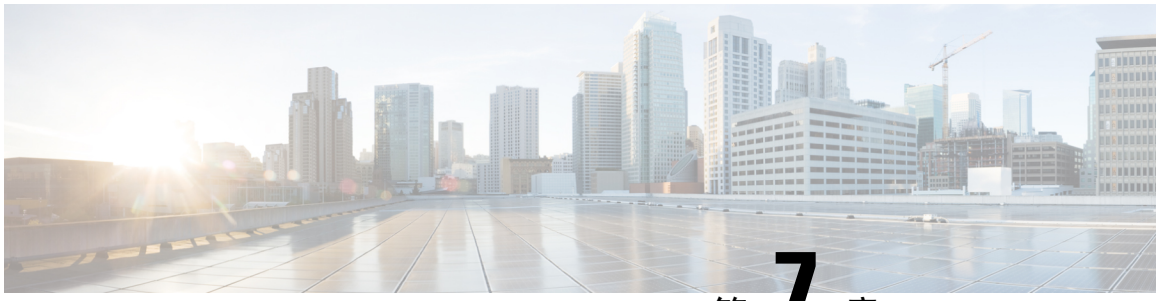
**步骤 1** 登录 CDO。

**步骤 2** 导航到 **VPN** 窗口。选择**站点间 VPN (Site-to-Site VPN)**。

**步骤 3** 选择要从 CDO 中删除的隧道。

**步骤 4** 在“操作”(Actions) 窗格中，点击**删除 (Delete)**。

**步骤 5** 确认要删除隧道，然后点击**确定 (OK)**。



第 7 章

# 将 CDO 与 Cisco Security Cloud Sign On 集成



## SecureX和CDO

思科 SecureX 平台结合了思科的集成安全产品组合以及客户基础设施的优势，旨在提供可统一可视性、实现自动化并增强网络、终端、云和应用安全性的一致体验。通过集成平台中的连接技术，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。有关 SecureX 是什么以及此平台提供的功能的更多信息，请参阅关于 SecureX。

允许 SecureX 访问您的 CDO 租户会生成设备事件摘要，包括设备总数以及出现错误的设备、存在冲突的设备以及当前可能不同步的设备。事件摘要还提供了第二个窗口，用于记录当前应用的策略以及与这些策略关联的对象。策略按设备类型定义，对象通过对象类型标识。

将 CDO 模块添加到 SecureX 控制面板需要多个步骤。有关详细信息，请参阅将 CDO 添加到 SecureX。

**Warning** 如果您尚未合并 CDO 和 SecureX 账户，则可能无法查看所有已载入设备的事件。我们强烈建议在 SecureX 中创建 CDO 模块之前合并您的账户。有关详细信息，请参阅合并您的 CDO 和 SecureX 或思科 XDR 租户账户。

**相关信息：**

- 关于 SecureX
- 合并您的 CDO 和 SecureX 或思科 XDR 租户账户
- 将 CDO 添加到 SecureX

## 合并您的 CDO 和 SecureX 或思科 XDR 租户账户

如果您的 Secure Firewall Threat Defense 或 本地防火墙管理中心 与 CDO 或思科安全分析和日志记录 (SaaS) 以及 SecureX 或思科 XDR 配合使用，则必须将 CDO 租户账户与设备关联的 SecureX 或思科 XDR 租户账户关联。

请注意何时启动此过程。此合并过程可能需要较长时间。

有关说明，请参阅合并账户。

**Note** 如果您在多个区域云上有账户，则必须为每个区域云单独合并账户。

# 将 CDO 添加到 SecureX

允许 SecureX 访问您注册的设备，并将 CDO 模块添加到 SecureX 控制面板，以查看您的设备策略和对象的摘要以及安全产品组合中的其他思科平台。

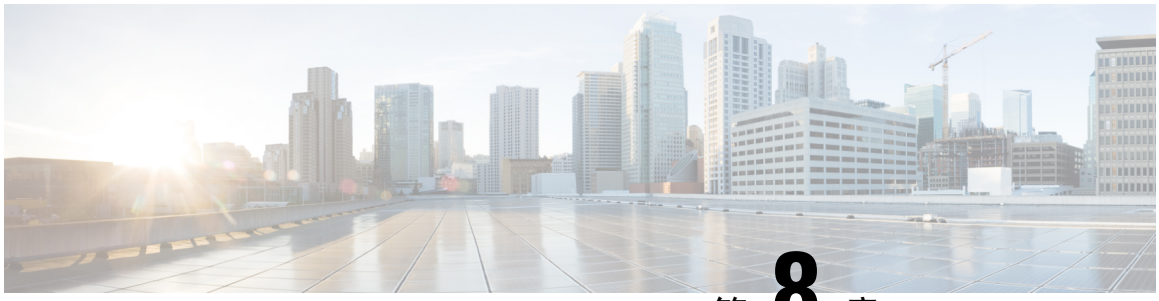
**Note** 请注意何时启动此过程。将 CDO 合并到 SecureX 可能需要较长时间。

### 准备工作

在 CDO 中连接 SecureX 之前，我们强烈建议执行以下操作：

- 您必须至少是 SecureX 账户的管理员。
- 您的 CDO 租户必须具有超级管理员用户角色。
- 合并您的租户账户，以促进租户通信。安全服务交换有关详细信息，请参阅合并您的 CDO 和 SecureX 或思科 XDR 租户账户。
- 将 CDO 租户与 安全服务交换 合并后，请确保注销 CDO 租户并重新登录。
- 如果您已经这样做，请将 Cisco Secure Sign-On 配置为 SAML 单点登录身份提供程序 (Idp)，并使用 Duo Security 进行多因素身份验证 (MFA)。CDO 和 SecureX 均使用此身份验证方法。有关详细信息，请参阅将 SAML 单点登录与 Cisco Defense Orchestrator 集成。

**Note** **注意：**如果您有多个租户，则必须在 SecureX 中为每个租户创建一个模块。每个租户都需要唯一的 API 令牌进行授权。



第 8 章

# Terraform



## 关于 Terraform

CDO 客户可以使用 CDO Terraform 提供程序和 CDO Terraform 模块，使用可重复且受版本控制的代码来快速设置租户。CDO Terraform 提供程序允许用户执行以下操作：

- **管理**用户
- 在云交付的防火墙管理中心、Cisco Secure ASA 设备和 iOS 设备上**载入** Cisco Secure Firewall Threat Defense
- 在 vSphere 和 AWS 上**载入**安全设备连接器
- 在 AWS 上**载入**安全事件连接器

有关详细信息，请参阅以下页面：

- CDO Terraform 提供程序页面
- vSphere 模块页面上的 CDO SDC
- AWS 模块页面上的 CDO SDC
- AWS 模块页面上的 CDO SEC
- 完成 Devnet 学习实验
- 使用 Cisco Defense Orchestrator Terraform 提供程序实现安全基础设施管理自动化 - 学习实验
- GitHub 上的 CDO 自动化示例

### 支持

CDO Terraform 提供程序和模块在 Apache 2.0 许可证下作为开源软件发布。如果需要支持，请在以下存储库中的 GitHub 上提交问题：

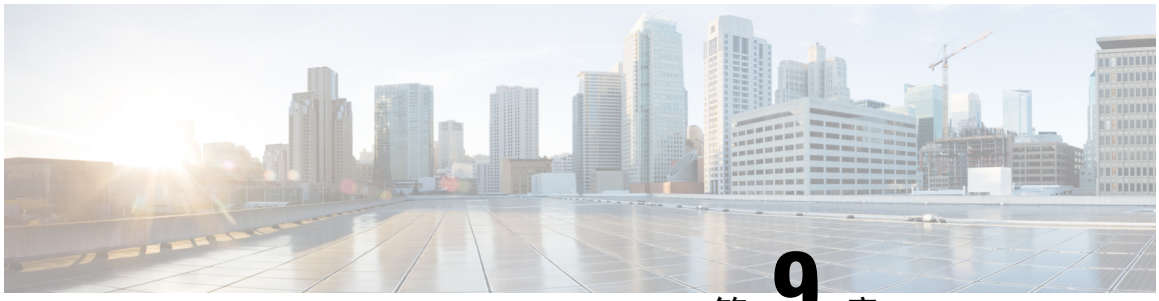
| 模块 | 存储库 (Repository) |
| --- | --- |
| CDO Terraform 提供程序 | https://github.com/ciscodevnet/terraform-provider-cdo |
| CDO SDC 模块 (vSphere) | https://github.com/CiscoDevNet/terraform-vsphere-cdo-sdc |
| CDO SDC 模块 (AWS) | https://github.com/CiscoDevNet/terraform-aws-cdo-sdc |
| CDO SEC 模块 (AWS) | https://github.com/CiscoDevNet/terraform-aws-cdo-sec |

### 对存储库的贡献

CDO 团队欢迎对上述存储库做出贡献。如果您希望为改进提供程序和模块做出贡献，请在这些 GitHub 存储库上创建请求。

### 相关主题

- 使用 Terraform 将 SDC 部署到 vSphere
- 使用 Terraform 将 SDC 部署到 AWS VPC
- 使用 Terraform 将 SEC 部署到 AWS VPC



第 9 章

# 故障排除

本章涵盖以下部分：



# Secure Firewall ASA 设备故障排除

## 重新启动后，ASA 无法重新连接到 CDO

如果 CDO 和您的 ASA 在 ASA 重新启动后不连接，可能是因为 ASA 已回退到使用 CDO 的安全设备连接器 (SDC) 不支持的 OpenSSL 密码套件。此故障排除主题针对该案例进行测试，并提供补救步骤。

### 现象

- ASA 重新启动，CDO 和 ASA 无法重新连接。CDO 显示消息“重新连接失败”。
- 尝试载入 ASA 时，CDO 显示消息：无法检索以下项的证书：<ASA_IP_Address> 。

## 由于证书错误而无法载入 ASA

**环境**：ASA 配置了客户端证书身份验证。

**解决方案**：禁用客户端证书身份验证。

**详细信息**：ASA 支持基于凭证的身份验证以及客户端证书身份验证。CDO 无法连接到使用客户端证书身份验证的 ASA。在将 ASA 载入 CDO 之前，请使用以下程序来确保其未启用客户端证书身份验证：

**步骤 1** 打开终端窗口并使用 SSH 连接到 ASA。

**步骤 2** 进入全局配置 模式。

**步骤 3** 在 hostname (config)# 提示符处输入以下命令：

```
no ssl certificate-authentication interface interface-name port 443
```

接口名称是 CDO 连接到的接口的名称。

## 确定 ASA 使用的 OpenSSL 密码套件

使用此程序可识别 ASA 使用的 OpenSSL 密码套件。如果命令输出中指定的密码套件不在支持的密码套件列表中，则 SDC 不支持该密码套件，您需要在 ASA 上更新密码套件。CDO 的安全设备连接器支持的密码套件, on page 478

**步骤 1** 在可以访问 SDC 的计算机上打开控制台窗口。

**步骤 2** 使用 SSH 连接到 SDC。您可以以常规用户（例如 CDO 或 SDC）或您创建的其他用户身份登录。您无需以 root 用户身份登录。

**Tip** 要查找 SDC IP 地址，请执行以下操作：

a. 打开 CDO。

b. 从用户菜单中，选择“安全设备连接器”(Secure Device Connectors)。

c. 点击表中显示的 SDC。SDC 的 IP 地址显示在设备的详细信息窗格中。

**步骤 3** 在命令提示符后输入：openssl s_client -showcerts -connect ASA_IP_Address :443

**步骤 4** 在命令输出中查找这些行。

```
New, TLSV1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
            Protocol: TLSv1.2
            Cipher: DES-CB3-SHA
```

在本示例中，ASA 使用的密码套件是 DES-CB3-SHA。

## CDO 的安全设备连接器支持的密码套件

CDO 的安全设备连接器使用仅接受最新和最安全密码的 node.js。因此，CDO 的 SDC 仅支持以下密码列表：

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

如果您在 ASA 上使用的密码套件不在此列表中，则 SDC 不支持该密码套件，您需要更新 ASA 的密码套件。

## 更新 ASA 的密码套件

**要更新 ASA 上的 TLS 密码套件，请执行以下操作：**

**步骤 1** 使用 SSH 连接到 ASA。

**步骤 2** 连接到 ASA 后，将权限提升到全局配置模式。您的提示符应如下所示：asaname(config)#

**步骤 3** 在提示符后，输入与此类似的命令：

```
ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256
 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA256
DHE-RSA-AES256-SHA256"
```

**Note** 此命令配置 ASA 支持的密码套件包含在引号之间和单词 custom 之后。在此命令中，指定的密码套件以 `ECDHE-RSA-AES128-GCM-SHA256` 开头，以 `DHE-RSA-AES256-SHA256`结尾。当您在 ASA 上输入 命令时，请删除您知道 ASA 不支持的任何密码套件。

**步骤 4** 提交命令后，在提示符后输入 write memory 以保存本地配置。例如：`asaname(config)#write memory`

# 使用 CLI 命令对 ASA 进行故障排除

本节讨论您可能希望用于对 ASA 进行故障排除和测试基本连接的一些重要命令。请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》，了解其他故障排除场景和 CLI 命令。在“系统管理”部分，导航至“测试和故障排除”一章。

您可以使用每个 ASA 设备可用的 CDO CLI 界面来执行这些命令。请参阅CDO 命令行界面，了解如何在 CDO 中使用 CLI 界面。

### NAT 策略设置

确定 NAT 设置的一些重要命令如下：

- 要确定 NAT 策略统计信息，请使用 show nat。
- 要确定 NAT 池，包括已分配的地址和端口，及其分配次数，请使用 **show nat pool**。

有关与 NAT 相关的更多命令，请参阅《CLI 手册 2：思科 ASA 系列防火墙 CLI 配置指南》，并导航至“网络地址转换 (NAT)”一章。

### 测试基本连接：Ping 通地址

您可以使用 ping 命令对 ASA 设备执行 ping 操作<IP address>命令。了解有关

### 显示路由表

使用 **show route** 命令来查看路由表中的条目。

**ciscoasa# show route**

ASA 路由表的输出示例：

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - 静态 InterVRF
Gateway of last resort is 192.168.0.254 to network 0.0.0.0
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, management
C 10.0.0.0 255.0.0.0 is directly connected, outside
L 10.10.10.1 255.255.255.255 is directly connected, Outside
C 192.168.0.0 255.255.255.0 is directly connected, management
L 192.168.0.118 255.255.255.255 is directly connected, management
```

### 监控交换机端口

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

- **show arp**

显示动态、静态和代理 ARP 条目。动态 ARP 条目包括 ARP 条目时限（秒）。

ARP 条目输出示例：

```
management 10.10.32.129 0050.568a.977b 0
management 10.10.32.136 0050.568a.5387 21
LANFAIL 20.20.21.1 0050.568a.4d70 96
outsi 10.10.16.6 0050.568a.e6d3 3881
outsi 10.10.16.1 0050.568a.977b 5551
```

# ASA 远程访问 VPN 故障排除

本节讨论在 ASA 设备上配置远程访问 VPN 时可能出现的一些故障排除问题。

### “RA VPN 监控”页面上缺少信息

如果未为 Webvpn 启用外部接口，则可能会出现此问题。

**解决方法：**

1. 在导航窗格中，点击 **设备和服务**。
2. 点击**设备 (Devices)** 选项卡，然后点击 **ASA** 选项卡。
3. 选择存在问题的 RA VPN 头端 ASA 设备。
4. 在右侧的 **管理 (Management)** 窗格中，点击**配置 (Configuration)**。
5. 点击“编辑”并搜索“webvpn”。
6. 按 Enter 键并添加 enable interface_name。这里，interface_name 是用户在进行远程访问 VPN 连接时所连接的外部接口的名称。请选择您使用此连接配置文件支持的设备与最终用户之间的任何接口，虽然这通常是外部（面向互联网的）接口。

   例如：

   ```
   webvpn
   enable outside
   ```
7. 点击**保存 (Save)**。
8. 预览配置并将其部署到设备。预览和部署所有设备的配置更改，第 313 页

# 无法将 ASA 添加到现有 RA VPN 配置

-

开始之前

- 

**SUMMARY STEPS**

**1.**

**DETAILED STEPS**

| | 命令或操作 | 目的 |
|---|---|---|
| 步骤 1 | 示例： | |

示例

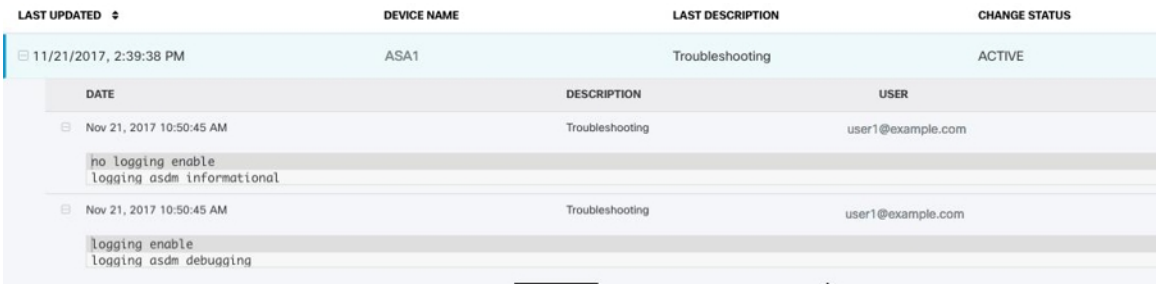
下一步做什么

- 

# ASA 实时日志记录

使用实时日志记录显示最近 20 秒记录的数据或最后 10 KB 的记录数据，以先达到的限制为准。当 CDO 检索实时数据时，它会查看 ASDM 上的现有日志记录配置，将其更改为请求调试级别的数据，然后将日志记录配置返回到您的配置。日志记录 CDO 显示反映您在 ASDM 中设置的任何日志记录过滤器。

您可以通过查看更改日志来查看 CDO 发送的用于执行日志记录的命令。以下是更改日志条目的示例。第一个条目（位于底部）表示 CDO 使用 logging enable 命令“打开”日志记录，并将 ASDM 日志记录级别更改为调试。第二个条目（位于顶部）显示日志记录配置已恢复到之前的状态。已使用 no logging enable 命令“关闭”日志记录，并且 ASDM 日志记录级别已恢复为 informational。




## 查看 ASA 实时日志

**步骤 1** 在 **设备和服务** 页面上，点击 **设备** 选项卡。

**步骤 2** 点击相应的设备类型选项卡，然后选择要查看其实时数据的设备。

**步骤 3** 点击**故障排除 (Troubleshoot)** Troubleshoot 。

**步骤 4** （可选）在点击查看实时日志之前，您可以在左侧窗格中定义过滤器，以优化日志记录搜索的结果。

**步骤 5** 点击查看实时日志。CDO 根据您的过滤条件检索实时日志记录数据并显示该数据。

**步骤 6** 查看额外的 20 秒记录的数据或最后 10 KB 的记录数据。再次点击查看实时日志。

# ASA 数据包跟踪器

数据包跟踪器允许您将合成数据包发送到网络中，并评估现有路由配置、NAT 规则和策略配置如何影响该数据包。使用此工具可对以下类型的问题进行故障排除：

- 用户报告他们无法访问他们应该能够访问的资源。
- 用户报告他们可以访问他们不应该能够访问的资源。
- 测试策略以确定其是否按预期工作。

数据包跟踪器可用于物理或虚拟的实时在线 ASA 设备。Packet Tracer 在 设备类型上不起作用。数据包跟踪器根据 ASA 上保存的配置评估数据包。数据包跟踪器不会评估 CDO 上的暂存更改。

我们认为最佳做法是在处于同步状态的ASA上运行数据包跟踪器。虽然如果设备未同步，数据包跟踪器将运行，但您可能会遇到一些意外结果。例如，如果您在CDO上删除了暂存配置中的规则，并且在数据包跟踪期间在 ASA 上触发了同一规则，则 CDO 将无法显示数据包与该规则的交互结果。

### 使用 ASA Packet Tracer 进行故障排除

当数据包跟踪器通过 ASA 的路由配置、NAT 规则和安全策略发送数据包时，它会在每个步骤显示数据包的状态。如果策略允许该数据包，则会显示绿色复选标记。如果数据包被拒绝并丢弃，CDO 会显示一个红色的 X。

数据包跟踪器还会显示数据包跟踪结果的实时日志。在下面的示例中，您可以看到规则拒绝 tcp 数据包的位置。


## 对 ASA 设备安全策略进行故障排除

**步骤 1** 在设备和服务页面中，选择您的 ASA，然后点击操作窗格中的故障排除。 Troubleshoot

**步骤 2** 在 Values 窗格中，选择要通过 ASA 虚拟发送的接口和数据包类型。

**步骤 3** （可选）如果要跟踪将安全组标签值嵌入第 2 层 CMD 报头 (Trustse) 的数据包，请选中 SGT 编号，然后输入安全组标签编号 0-65535。

**步骤 4** 指定源和目标。如果使用思科 Trustsec，可以指定 IPv4 或 IPv6 地址、完全限定域名 (FQDN) 或安全组名称或标记。对于源地址，您还可以指定 Domain\username 格式的用户名。

**步骤 5** 指定其他协议特征：

- ICMP - 输入 ICMP 类型、ICMP 代码 (0-255)，并且可以选择键入 ICMP 标识符。
- TCP/UDP/SCTP - 通过从列表中选择源和目标端口或在端口组合框中输入值来输入它们。
- IP - 输入协议编号 0-255。

**步骤 6** 点击运行 **Packet Tracer (Run Packet Tracer)**。

**步骤 7** 继续分析 Packet Tracer 结果。分析 Packet Tracer 结果, on page 485

## 对访问规则进行故障排除

**步骤 1** 选择**策略 (Policies)** > **网络策略 (Network Policies)** > 。

**步骤 2** 选择与您的 ASA 关联的策略。

**步骤 3** 在网络策略中选择要进行故障排除的规则，然后点击详细信息窗格中的**故障排除** Troubleshoot 。请注意，在故障排除页面的“值”面板中，许多字段已预填充了您选择的规则的属性。

**步骤 4** 在其余必填字段中输入信息。完成所有必填字段后，“运行 Packet Tracer”按钮变为活动状态。

**步骤 5** 点击运行 **Packet Tracer (Run Packet Tracer)**。

**步骤 6** 继续分析 Packet Tracer 结果。分析 Packet Tracer 结果, on page 485

## 对 NAT 规则进行故障排除

**步骤 1** 在**设备和服务** 页面中，选择您的 ASA，然后点击操作窗格中的**查看 NAT 规则** View NAT Rules 。

**步骤 2** 从NAT规则表中选择要进行故障排除的规则，然后点击详细信息窗格中的**故障排除** Troubleshoot 。请注意，在“故障排除”(Troubleshoot) 页面的“值”(values) 面板中，许多字段都预填充了您选择的规则的属性。

**步骤 3** 在其余必填字段中输入信息。完成所有必填字段后，Run Packet Tracer 将变为活动状态。

**步骤 4** 点击运行 **Packet Tracer (Run Packet Tracer)**。

**步骤 5** 继续分析 Packet Tracer 结果。分析 Packet Tracer 结果, on page 485

## 对两次 NAT 规则进行故障排除

**步骤 1** 在设备和服务页面中，选择您的 ASA，然后点击操作窗格中的查看 NAT 规则。 View NAT Rules

**步骤 2** 从 NAT 规则表中选择要进行故障排除的规则，然后点击详细信息窗格中的故障排除。 Troubleshoot 对于双向 Twice NAT 规则，这将打开一个下拉列表，您可以在其中选择对源数据包转换或目标数据包转换进行故障排除。

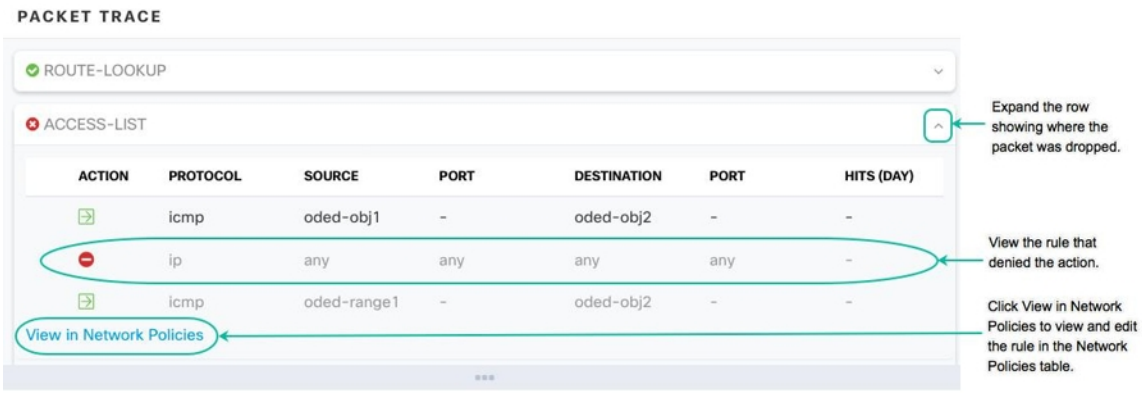
**步骤 3** 在其余必填字段中输入信息。完成所有必填字段后，Run Packet Tracer 将变为活动状态。

**步骤 4** 点击**运行 Packet Tracer (Run Packet Tracer)**。

## 分析 Packet Tracer 结果

无论数据包被丢弃还是被允许，您都可以通过展开数据包跟踪表中的一行并读取与该操作相关的规则或日志记录信息来了解原因。在下面的示例中，数据包跟踪器识别了一个访问列表策略，该策略包含一条拒绝来自任何源并发往任何目的地的 IP 数据包的规则。如果这不是您想要的操作，您可以点击**在网络策略中查看**链接并立即编辑该规则。编辑规则后，请务必将该配置更改部署到 ASA，然后重新运行数据包跟踪器，以确保获得预期的访问结果。

除数据包跟踪器结果外，CDO 还会显示来自 ASA 的ASA 实时日志记录。




# 思科 ASA 公告 cisco-sa-20180129-asa1

思科产品安全事件响应团队 (PSIRT) 发布了安全公告 cisco-sa-20180129-asa1，其中描述了严重性为 ASA 和 Firepower 的安全漏洞。 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1有关受影响的 ASA 和 Firepower 硬件、软件和配置的完整说明，请阅读整个 PSIRT 团队公告。https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

如果您确定您的 ASA 受到公告的影响，您可以使用 CDO 将您的 ASA 升级到补丁版本。使用此过程：

**步骤 1** 在每个受影响的 ASA 上配置 DNS 服务器。在 ASA 上配置 DNS, on page 291

**步骤 2** 返回到公告，确定您需要的软件补丁。https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

**步骤 3** 有关介绍如何使用 CDO 将 ASA 升级到 ASA 公告中列出的固定版本的主题，请参阅在单个 ASA 上升级 ASA 和 ASDM 映像, on page 147。从升级必备条件开始，然后阅读有关升级单个 ASA、在主用-备用配置中升级 ASA 或批量升级 ASA 的信息。ASA 和 ASDM 升级必备条件, on page 142

为方便起见，以下是思科报告的安全公告的摘要：

2018 年 2 月 5 日更新：经过进一步调查，思科已确定受此漏洞影响的其他攻击媒介和功能。此外，还发现原始修复不完整，因此现在可以使用新的修复代码版本。有关详细信息，请参阅固定软件部分。思科自适应安全设备 (ASA) 软件的 XML 解析器中存在允许未经身份验证的远程攻击者重新加载受影响系统或远程执行代码的漏洞。由于内存不足，ASA 也可能停止处理传入的虚拟专用网络 (VPN) 身份验证请求。该漏洞是由处理恶意 XML 负载时分配和释放内存的问题引起的。攻击者可以通过将特制的 XML 数据包发送到受影响系统上的易受攻击的接口来利用此漏洞。通过利用该漏洞，攻击者可执行任意代码并获得系统的完全控制，导致受影响设备重新加载或停止处理传入的 VPN 身份验证请求。要受到攻击，ASA 必须在接口上启用安全套接字层 (SSL) 服务或 IKEv2 远程访问 VPN 服务。漏洞被利用的风险还取决于接口对攻击者的可访问性。有关易受攻击的 ASA 功能的完整列表，请参阅易受攻击的产品部分中的表格。思科已发布解决此漏洞的软件更新。目前还没有解决受此漏洞影响的所有功能的变通方法。此公告位于以下链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

# 确认 ASA 运行配置大小

要确认运行配置文件的大小，请执行以下程序：

**步骤 1** 通过以下方式之一访问 ASA 的命令行界面：

- 打开终端窗口并使用 SSH 登录 ASA。将您的权限提升到“特权 EXEC”模式，以便您看到带有 `hostname#` 的提示符。
- 如果您已成功载入 ASA，请打开**清单 (Inventory)** 页面，选择要连接的设备，然后点击“设备操作”(Device Actions) 窗格中的 **>_ 命令行接口 (>_ Command Line Interface)** 按钮。

**步骤 2** 在提示符后键入 `copy running-config flash`

**步骤 3** 当系统提示输入源文件名时，请勿输入任何内容并按 <Enter>

**步骤 4** 当提示输入目标文件名时，请输入输出文件的名称。在 ASA 复制您指定的文件的运行配置后，它会返回到特权 EXEC 提示符。

**步骤 5** 在提示符后键入 `show flash`。

**步骤 6** 查看长度列。如果文件超过 4718592 字节，则大于 4.5 MB。

以下是一组命令和输出示例：

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time------ path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

# 影响安全设备连接器的容器权限升级漏洞：cisco-sa-20190215-runc

思科产品安全事件响应团队 (PSIRT) 发布了安全公告 cisco-sa-20190215-runc，其中描述了 Docker 中的一个高严重性漏洞。阅读整个 PSIRT 团队公告，了解漏洞的完整说明。https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190215-runc

此漏洞会影响所有 CDO 客户：

- 使用 CDO 云部署的安全设备连接器 (SDC) 的客户无需执行任何操作，因为 CDO 运营团队已执行补救步骤。
- 使用本地部署的 SDC 的客户需要升级其 SDC 主机才能使用最新的 Docker 版本。他们可以按照以下说明执行此操作：

## 更新 CDO 标准 SDC 主机

如果您使用 CDO 映像部署了 SDC，请使用以下说明。 使用 CDO 的 VM 映像部署安全设备连接器，第 10 页

**步骤 1** 使用 SSH 或虚拟机监控程序控制台连接到 SDC 主机。

**步骤 2** 运行以下命令检查 Docker 服务的版本：

```
docker version
```

**步骤 3** 如果您运行的是最新的虚拟机 (VM)，您应该会看到如下输出：

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

您可能会在这里看到旧版本。

**步骤 4** 运行以下命令以更新 Docker 并重新启动服务：

```
> sudo yum update docker-ce
> sudo service docker restart
```

**注释** 当 Docker 服务重新启动时，CDO 和您的设备之间会出现短暂的连接中断。

**步骤 5** 再次运行 docker version 命令。您应该会看到以下输出：

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

**步骤 6** 大功告成。您现在已升级到 Docker 的最新版本并安装了补丁。

## 更新自定义 SDC 主机

如果您已创建自己的 SDC 主机，则需要按照说明根据 Docker 的安装方式进行更新。如果您使用的是 CentOS、yum 和 Docker-ce（社区版），则前面的程序将起作用。

如果您已安装 Docker-ee（企业版）或使用其他方法安装 Docker，则 Docker 的固定版本可能不同。您可以查看 Docker 页面以确定要安装的正确版本：Docker 安全更新和容器安全最佳实践。
https://blog.docker.com/2019/02/docker-security-update-cve-2018-5736-and-container-security-best-practices/

## 缺陷跟踪

思科将继续评估此漏洞，并将在获得更多信息时更新公告。公告被标记为最终版本后，您可以参考相关的思科漏洞了解更多详细信息：

CSCvo33929-CVE-2019-5736: runc container breakout

# 大型 ASA 运行配置文件

### CDO 中的行为

您可能会看到 ASA 无法载入、CDO 未显示 ASA 运行配置文件中定义的所有配置或 CDO 无法写入更改日志等行为。

### 可能的原因

ASA 的运行配置文件对于 CDO 而言可能“过大”。

当您将 ASA 载入 CDO 时，CDO 会在其数据库中存储 ASA 的运行配置文件的副本。通常，如果该运行配置文件过大（4.5 MB 或更大），或者包含的行过多（大约 22,000 行），或者单个访问组的访问列表条目过多，则 CDO 将无法可预测地管理该设备。

要确认运行配置文件的大小，请参阅确认 ASA 运行配置大小。

### 解决方法或解决方案

请联系您的思科客户团队寻求帮助，以在不中断安全策略的情况下安全地减小配置文件的大小。

# 对安全设备连接器进行故障排除

使用这些主题对现场安全设备连接器 (SDC) 进行故障排除。

如果这些场景都不符合您的情况，CDO 客户如何通过 TAC 提交支持请求。

# SDC 无法接通

如果 SDC 未能连续响应来自 CDO 的两个心跳请求，则该 SDC 处于“无法访问”状态。如果您的 SDC 无法访问，您的租户将无法与您已载入的任何设备通信。

CDO 表示无法通过以下方式访问 SDC：

- 您会看到消息“某些安全设备连接器 (SDC) 无法访问。您将无法与与这些 SDC 关联的设备进行通信。”在 CDO 主页上。
- “服务”(Services) 页面中的 SDC 状态为“无法访问”(Unreachable)。

首先，尝试将 SDC 重新连接到租户以解决此问题：

1. 检查 SDC 虚拟机是否正在运行，并且可以访问您所在地区的 CDO IP 地址。请参阅将 思科防御协调器 连接到托管设备，第 9 页。
2. 尝试通过手动请求心跳来重新连接 CDO 和 SDC。如果 SDC 响应心跳请求，它将返回“活动”状态。要手动请求心跳，请执行以下操作：
   1. 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。
   2. 点击无法访问的 SDC。
   3. 在“操作”(Actions) 窗格中，点击**请求检测信号 (Request Heartbeat)**。
   4. 点击**重新连接 (Reconnect)**。
3. 如果在手动尝试将 SDC 重新连接到租户后，SDC 未返回到主用状态，请按照中的说明进行操作。部署后，SDC 状态在 CDO 上未变为活动状态，第 489 页

   。

# 部署后，SDC 状态在 CDO 上未变为活动状态

如果 CDO 在部署后约 10 分钟内未指示您的 SDC 处于活动状态，请使用您在部署 SDC 时创建的 cdo 用户和密码，通过 SSH 连接到 SDC VM。

---

**步骤 1** 查看 /opt/cdo/configure.log。它会显示您为 SDC 输入的配置设置，以及这些设置是否已成功应用。如果设置过程中出现任何故障，或者值输入不正确，请再次运行 sdc-onboard 设置：

a) 在 [cdo@localhost cdo]$ 提示符后，输入 sudo sdc-onboard setup。
b) 输入 `cdo` 用户的密码。
c) 按照提示操作。设置脚本将指导您完成在设置向导中执行的所有配置步骤，并为您提供更改输入的值的机会。

**步骤 2** 如果在查看日志并运行 sudo sdc-onboard setup 后，CDO 仍不指示 SDC 处于活动状态，请联系 CDO 支持。联系思科威胁防御支持, on page 534

---

# 更改后的 SDC IP 地址未反映在 CDO 中

如果您更改了 SDC 的 IP 地址，则在格林威治标准时间上午 3:00 之前，它不会反映在 CDO 中。

# 排除设备与 SDC 的连接故障

使用此工具可测试从CDO通过安全设备连接器(SDC)到您的设备的连接。如果您的设备未能载入，或者您想在载入之前确定 CDO 是否可以访问您的设备，则可能需要测试此连接。

**步骤 1** 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 2** 选择 SDC。

**步骤 3** 在右侧的**故障排除 (Troubleshooting)** 窗格中，点击**设备连接 (Device Connectivity)**。

**步骤 4** 输入您尝试进行故障排除或尝试连接的设备的有效 IP 地址或 FQDN 和端口号，然后点击**开始 (Go)**。CDO 执行以下验证：

a) **DNS 解析 (DNS Resolution)** - 如果您提供 FQDN 而不是 IP 地址，这将验证 SDC 可以解析域名并获取 IP 地址。

b) **连接测试 (Connection Test)** - 验证设备是否可访问。

c) **TLS 支持 (TLS Support)** - 检测设备和 SDC 支持的 TLS 版本和密码。

- **不支持的密码 (Unsupported Cipher)** - 如果没有设备和 SDC 都支持的 TLS 版本，则 CDO 还会测试设备（而不是 SDC）支持的 TLS 版本和密码。

d) “SSL 证书”(SSL Certificate) - 故障排除提供证书信息。

**步骤 5** 如果在载入或连接设备方面仍有问题，请联系思科威胁防御支持。

# 与 SDC 间歇性连接或无连接

本节中讨论的解决方案仅适用于本地安全设备连接器 (SDC)。

症状：与 SDC 的连接断断续续或无连接。

诊断：如果磁盘空间几乎已满（80% 以上），可能会出现此问题。

执行以下步骤以检查磁盘空间使用情况。

1. 打开 Secure Device Connector (SDC) VM 的控制台。
2. 使用用户名 **cdo** 登录。
3. 输入初始登录时创建的密码。
4. 首先，通过键入 df -h 确认没有可用磁盘空间，以检查可用磁盘空间量。

   您可以确认磁盘空间已被 Docker 占用。正常磁盘使用量应低于 2 GB。
5. 要查看 Docker 文件夹的磁盘使用情况，

执行 sudo du -h /var/lib/docker | sort -h.

您可以看到 Docker 文件夹的磁盘空间使用情况。

### 操作步骤

如果 Docker 文件夹的磁盘空间使用量快要满了，请在 Docker 配置文件中定义以下内容：

- 最大大小：在当前文件达到最大大小后强制执行日志轮换。
- 最大文件：在达到最大限制时删除多余的轮换日志文件。

请执行以下操作：

1. 执行 sudo vi /etc/docker/daemon.json。
2. 将以下行插入文件。

```
{
"log-driver": "json-file",
"log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. 按 ESC，然后键入 :wq!写入更改并关闭文件。

注释 您可以执行 sudo cat /etc/docker/daemon.json 来验证对文件所做的更改。

4. 执行 sudo systemctl restart docker 以重新启动 docker 文件。

   更改需要几分钟才能生效。您可以执行 sudo du -h /var/lib/docker | sort -h 以查看 docker 文件夹的更新磁盘使用情况。

5. 执行 df -h 以验证可用磁盘大小是否已增加。
6. 在 SDC 状态从“无法连通”(Unreachable) 变成“活动”(Active) 之前，您必须从 CDO 转到**服务 (Services)**页面中的“安全连接器”(Secure Connectors) 选项卡，然后从“操作”(Actions) 菜单中点击请求**重新连接 (Request Reconnect)**。

# 影响安全设备连接器的容器权限升级漏洞：cisco-sa-20190215-runc

思科产品安全事件响应团队 (PSIRT) 发布了安全公告 **cisco-sa-20190215-runc**，其中描述了 Docker 中的一个高严重性漏洞。阅读整个 PSIRT 团队公告，了解漏洞的完整说明。https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190215-runc

此漏洞会影响所有 CDO 客户：

- 使用 CDO 云部署的安全设备连接器 (SDC) 的客户无需执行任何操作，因为 CDO 运营团队已执行补救步骤。

- 使用本地部署的 SDC 的客户需要升级其 SDC 主机才能使用最新的 Docker 版本。他们可以按照以下说明执行此操作：
  - 更新 CDO 标准 SDC 主机，第 487 页
  - 更新自定义 SDC 主机，第 488 页
  - 缺陷跟踪，第 488 页

# 更新 CDO 标准 SDC 主机

如果您使用 CDO 映像部署了 SDC，请使用以下说明。使用 CDO 的 VM 映像部署安全设备连接器，第 10 页

**步骤 1** 使用 SSH 或虚拟机监控程序控制台连接到 SDC 主机。

**步骤 2** 运行以下命令检查 Docker 服务的版本：

```
docker version
```

**步骤 3** 如果您运行的是最新的虚拟机 (VM)，您应该会看到如下输出：

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

您可能会在这里看到旧版本。

**步骤 4** 运行以下命令以更新 Docker 并重新启动服务：

```
> sudo yum update docker-ce
> sudo service docker restart
```

**注释** 当 Docker 服务重新启动时，CDO 和您的设备之间会出现短暂的连接中断。

**步骤 5** 再次运行 docker version 命令。您应该会看到以下输出：

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

**步骤 6** 大功告成。您现在已升级到 Docker 的最新版本并安装了补丁。

## 更新自定义 SDC 主机

如果您已创建自己的 SDC 主机，则需要按照说明根据 Docker 的安装方式进行更新。如果您使用的是 CentOS、yum 和 Docker-ce（社区版），则前面的程序将起作用。

如果您已安装 Docker-ee（企业版）或使用其他方法安装 Docker，则 Docker 的固定版本可能不同。您可以查看 Docker 页面以确定要安装的正确版本：Docker 安全更新和容器安全最佳实践。
https://blog.docker.com/2019/02/docker-security-update-cve-2018-5736-and-container-security-best-practices/

## 缺陷跟踪

思科将继续评估此漏洞，并将在获得更多信息时更新公告。公告被标记为最终版本后，您可以参考相关的思科漏洞了解更多详细信息：

CSCvo33929-CVE-2019-5736: runc container breakout

# 无效系统时间

Cisco Defense Orchestrator (CDO) 正在采用一种与安全设备连接器 (SDC) 进行通信的新方式。为此，CDO 必须在 2024 年 2 月 1 日之前将您现有的 SDC 迁移到新的通信方式。

**注释** 如果您的 SDC 在 2024 年 2 月 1 日之前未迁移，则 CDO 将无法再通过 SDC 与您的设备通信。

CDO 的运营团队尝试迁移您的 SDC 但未成功，因为您的 SDC 系统时间比 AWS 系统时间早或晚 15 分钟。

请按照以下步骤来更正系统时间问题。解决此问题后，我们将能够继续进行迁移。

**步骤 1** 通过 VM 终端或通过 SSH 连接登录到 SDC VM。

**步骤 2** 在提示符后，输入 `sudo sdc-onboard setup` 并进行身份验证。

**步骤 3** 现在，您将像第一次设置 SDC 一样回答 SDC 设置问题。重新输入与之前相同的所有密码和网络信息，但要特别注意 NTP 服务器地址：

a) 使用用于设置 SDC 的相同密码重置 root 和 cdo 用户密码。
b) 当系统提示时，输入 **y** 以重新配置网络。
c) 输入您之前输入的 IP 地址/CIDR 值。
d) 像以前一样输入网络网关的值。
e) 像以前一样输入 DNS 服务器的值。
f) 当系统提示您输入 NTP 服务器时，请务必提供有效的 NTP 服务器地址，例如 `time.aws.com`。
g) 查看您提供的值，如果正确，请输入 **y** 。

**步骤 4** 通过在提示符后输入 `date`，验证您的时间服务器是否可访问并与您的 SDC 同步。系统将显示 UTC 日期和时间，您可以将其与 SDC 时间进行比较。

### 下一步做什么

完成这些步骤后或遇到任何错误时，请联系思科技术支持中心 (TAC)。在成功完成这些步骤后，CDO 运营团队即可完成向新通信方法的 SDC 迁移。

# SDC 版本低于 202311****

Cisco Defense Orchestrator (CDO) 正在采用一种与安全设备连接器 (SDC) 进行通信的新方式。为此，CDO 必须在 2024 年 2 月 1 日之前将您现有的 SDC 迁移到新的通信方式。

**注释** 如果您的 SDC 在 2024 年 2 月 1 日之前未迁移，则 CDO 将无法再通过 SDC 与您的设备通信。

CDO 的运营团队尝试迁移您的 SDC 但未成功，因为您的租户运行的版本低于 202311****。

通过从 CDO 菜单栏**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)** 导航，“安全连接器”(Secure Connectors) 页面上会列出 SDC 的当前版本。选择 SDC 后，可在屏幕右侧的**详细信息 (Details)** 窗格中找到其版本号。

请按照以下步骤升级 SDC 版本。问题一旦解决，CDO 操作人员将能够再次运行迁移过程。

**步骤 1** 登录到 SDC VM 并进行身份验证。

**步骤 2** 在提示符后，输入 `sudo su - sdc` 并进行身份验证。

**步骤 3** 在提示符处输入 `crontab -r`。

如果收到消息 `no crontab for sdc`，则可以将其忽略并移至下一步。

**步骤 4** 在提示符处输入 `./toolkit/toolkit.sh upgrade`。CDO 将确定您是否需要升级并对工具包进行升级。确保控制台中未报告任何错误。

**步骤 5** 验证 SDC 的新版本：

a) 登录 CDO。

b) 通过 CDO 菜单栏**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)** 导航到“安全连接器”(Secure Connectors) 页面。

c) 选择您的 SDC，然后点击**操作 (Actions)** 窗格中的**请求检测信号 (Request Heartbeat)**。

d) 验证 SDC 版本是否为 202311**** 或更高版本。

### 下一步做什么

完成这些步骤后或遇到任何错误时，请联系思科技术支持中心 (TAC)。成功完成这些步骤后，CDO 运营团队可以再次运行迁移过程。

# AWS 服务器的证书或连接错误

Cisco Defense Orchestrator (CDO) 正在采用一种与安全设备连接器 (SDC) 进行通信的新方式。为此，CDO 必须在 2024 年 2 月 1 日之前将您现有的 SDC 迁移到新的通信方式。

注释 如果您的 SDC 在 2024 年 2 月 1 日之前未迁移，则 CDO 将无法再通过 SDC 与您的设备通信。

CDO 的运营团队尝试迁移您的 SDC，但未成功，因为他们遇到了连接问题。

请按照以下步骤纠正连接问题。解决此问题后，我们将能够继续进行迁移。

**步骤 1** 创建允许在端口 443 上连接到您所在区域的域的防火墙规则：

- 美国地区的生产租户：
  - cognito-identity.us-west-2.amazonaws.com
  - cognito-idp.us-west-2.amazonaws.com
  - sns.us-west-2.amazonaws.com
  - sqs.us-west-2.amazonaws.com
- 欧盟地区的生产租户：
  - cognito-identity.eu-central-1.amazonaws.com
  - cognito-idp.eu-central-1.amazonaws.com
  - sns.eu-central-1.amazonaws.com
  - sqs.eu-central-1.amazonaws.com
- 亚太地区的生产租户：
  - cognito-identity.ap-northeast-1.amazonaws.com
  - cognito-idp.ap-northeast-1.amazonaws.com
  - sqs.ap-northeast-1.amazonaws.com
  - sns.ap-northeast-1.amazonaws.com

**步骤 2** 您可以使用以下命令之一确定需要添加到防火墙“允许列表”(allow list) 的 IP 地址的完整列表。

注释 以下命令适用于已安装 **jq** 的用户。IP 地址将显示在一个列表中。

- 美国地区的生产租户：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select( (.service ==
"AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- 欧盟地区的生产租户：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select( (.service == "AMAZON" ) and .region == "eu-central-1") | .ip_prefix'
```

- 亚太地区的生产租户：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select( (.service == "AMAZON" ) and .region == "ap-northeast-1") | .ip_prefix'
```

注释 如果您没有安装 **jq**，则可以使用此命令的简化版本：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

### 下一步做什么

完成这些步骤后或遇到任何错误时，请联系思科技术支持中心 (TAC)。在成功完成这些步骤后，CDO 运营团队即可完成向新通信方法的 SDC 迁移。

# 安全事件连接器故障排除

如果这些场景都不符合您的情况，CDO 客户如何通过 TAC 提交支持请求。

# 安全事件连接器载入故障排除

这些故障排除主题介绍了与安全事件连接器 (SEC) 载入失败相关的许多不同症状。

### SEC 载入失败

**症状**：SEC 载入失败。

**修复**：删除 SEC 并重新载入。

如果收到此错误：

1. 从虚拟机容器中删除安全事件连接器及其文件。
2. 更新您的安全设备连接器，第 26 页。通常，SDC 会自动更新，您不必使用此程序，但此程序在故障排除的情况下非常有用。
3. 在 SDC 虚拟机上安装安全事件连接器，第 380 页。

提示 激活 SEC 时，请始终使用复制链接复制引导程序数据。

注释 如果此程序无法解决问题，请事件日志记录故障排除日志文件并联系您的托管服务提供商或思科技术支持中心。

### 未提供 SEC Bootstrap 数据

**消息**：错误，无法引导程序安全事件连接器，不提供引导程序数据，正在退出。(ERROR cannot bootstrap Secure Event Connector, bootstrap data not provided, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
provided, exiting.
```

**诊断**：系统提示时，Boostrap 数据未输入到设置脚本中。

**修复**：在载入时，如果提示输入引导程序数据，提供在 CDO UI 中生成的 SEC 引导程序数据。

### 引导程序配置文件不存在

**消息**：错误，无法为租户引导安全事件连接器：<tenant_name>，引导程序配置文件（“/usr/local/cdo/es_bootstrapdata”）不存在，正在退出。(ERROR Cannot bootstrap Secure Event Connector for tenant: <tenant_name>, bootstrap config file ("/usr/local/cdo/es_bootstrapdata") does not exist, exiting.)

**诊断**：SEC 引导程序数据文件（“/usr/local/cdo/es_bootstrapdata”）不存在。

**修复**：将 CDO UI 中生成的 SEC 引导程序数据放到文件 **/usr/local/cdo/es_bootstrapdata** 中，然后再次尝试载入。

1. 重复载入程序。
2. 复制引导程序日期。
3. 以“sdc”用户身份登录 SEC VM。
4. 将 CDO UI 中生成的 SEC 引导程序数据放到文件 **/usr/local/cdo/es_bootstrapdata** 中，然后再次尝试载入。

### 解码引导程序数据失败

**消息**：错误无法为租户引导安全事件连接器：<tenant_name>，未能解码 SEC Boostrap 数据，正在退出。(ERROR cannot bootstrap Secure Event Connector for tenant: <tenant_name>, faile to decode SEC boostrap data, exiting.)

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 failed to decode SEC bootstrap data, exiting.
```

**诊断**：解码引导程序数据失败

**修复**：重新生成 SEC 引导程序数据，然后再次尝试载入。

### 引导程序数据没有载入 SEC 所需的信息

**消息：**

- 错误，无法为租户引导安全事件连接器容器，安全服务交换 FQDN 未设置，正在退出。
- 错误，无法为租户引导安全事件连接器容器，安全服务交换 OTP 未设置，正在退出。

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 安全服务交换
 FQDN not set, exiting.
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 安全服务交换
 FQDN not set, exiting.
```

**诊断：**引导程序数据没有载入 SEC 所需的信息

**修复：**重新生成 bootstrapdata，然后再次尝试载入。

### 当前正在运行的工具包 Cron

**消息：**错误，SEC 工具包已在运行，正在退出。(ERROR SEC toolkit already running, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
 [2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

**诊断：** 工具包 cron 当前正在运行。

**修复：**再次重试载入命令。

### 没有足够的 CPU 和内存

**消息：**错误，无法设置安全事件连接器，需要至少 4 个 CPU 和 8 GB 内存，正在退出。(ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8 GB ram required, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8
GB ram required, exiting.
```

**诊断：**没有足够的 CPU 和内存。

**修复：**确保至少为虚拟机上的 SEC 调配了 4 个 CPU 和 8 GB RAM，然后再次尝试载入。

### SEC 已在运行

**消息：**错误安全事件连接器已在运行，在载入新的安全事件连接器并退出之前执行“cleanup”。

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup' before
 onboarding a new Secure Event Connector, exiting.
```

**诊断：**SEC 已在运行。

**修复：**在载入新的 SEC 之前运行 SEC 清理命令。

### SEC 域无法访问

**消息：**

- 未能连接到 api-sse.cisco.com:443；连接被拒绝 (Failed connect to api-sse.cisco.com:443; Connection refused)
- 错误，无法设置安全事件连接器，无法访问域 api-sse.cisco.com，正在退出。(ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com unreachable, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com
 unreachable, exiting.
```

**诊断**：SEC 域不可达

**修复**：确保本地 SDC 具有互联网连接，然后再次尝试载入。

#### 载入 SEC 命令成功且未出错，但 SEC docker 容器未启动

**症状**：载入 SEC 命令成功且未出错，但 SEC docker 容器未启动

**诊断**：载入 SEC 命令成功且未出错，但 SEC docker 容器未启动

**修复**：

1. 以“sdc”用户身份登录 SEC。
2. 检查 SEC docker 容器启动日志中是否存在任何错误 (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/startup.log)。
3. 如果是，请运行 SEC 清理命令，然后再次尝试载入。

#### 联系 CDO 支持人员

如果这些场景都不符合您的情况，CDO 客户如何通过 TAC 提交支持请求。

# 安全事件连接器注册失败故障排除

**症状**：向云事件服务注册思科安全事件连接器失败。

**诊断**：这些是 SEC 无法注册到事件云服务的最常见原因。

- **SEC 无法从 SEC 访问 Eventing 云服务**

  修复：确保可在端口 443 上访问互联网，并且 DNS 配置正确。

- **由于 SEC bootstrapdata 中的一次性密码无效或过期，注册失败**

  修复：

---

**步骤 1** 以“sdc”用户身份登录 SDC。

**步骤 2** 查看连接器日志：( /usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log ) 以检查注册状态。

如果注册因令牌无效而失败，您将在日志文件中看到类似于以下内容的错误消息。

**context:(*contextImpl).handleFailed] registration - CE2001：注册失败 - 因无效令牌，注册设备失败。请使用新的有效令牌重试。- 失败"**

**步骤 3** 在 SDC VM 上运行 SEC 清理命令步骤，从“安全连接器”(Secure Connectors) 页面删除 SEC。

**步骤 4** 生成新的 SEC 引导程序数据，然后重试 SEC 激活步骤。

# 使用安全和分析日志记录事件排除网络问题

以下是使用事件查看器排除网络问题的基本框架。

此场景假设您的网络运营团队收到报告，指出用户无法访问网络上的资源。根据报告问题的用户及其位置，网络运营团队可以合理地了解哪个防火墙控制其对资源的访问。

**Note** 此场景还假设 FDM 管理 设备是管理网络流量的防火墙。安全分析和日志记录不会从其他设备类型收集日志记录信息。

**步骤 1** 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**历史 (Historical)** 选项卡。

**步骤 3** 按**时间范围 (Time Range)** 开始过滤事件。默认情况下，“历史”(Historical) 选项卡显示最近一小时的事件。如果这是正确的时间范围，请输入当前日期和时间作为**结束**时间。如果该时间范围不正确，请输入包含所报告问题时间的开始和结束时间。

**步骤 4** 在**传感器 ID (Sensor ID)** 字段中输入您怀疑控制用户访问的防火墙的 IP 地址。如果可能是多个防火墙，请使用搜索栏中的 **attribute:value** 对过滤事件。输入两个条目并将其与 OR 语句组合在一起。例如：`SensorID:192.168.10.2 OR SensorID:192.168.20.2`。

**步骤 5** 在事件过滤器栏中的**源 IP (Source IP)** 字段中输入用户的 IP 地址。

**步骤 6** 如果用户无法访问资源，请尝试在**目标 IP (Destination IP)** 字段中输入该资源的 IP 地址。

**步骤 7** 展开结果中的事件并查看其详细信息。以下是一些需要查看的详细信息：

- **AC_RuleAction** - 触发规则时采取的操作（允许、信任、阻止）。
- **FirewallPolicy** - 触发事件的规则所在的策略。
- **FirewallRule** - 触发事件的关联规则的名称。如果值为“默认操作”(Default Action)，则触发事件的是策略的默认操作，而不是策略中的某个规则。
- **UserName** - 与发起方 IP 地址关联的用户。发起方 IP 地址与源 IP 地址相同。

**步骤 8** 如果规则操作阻止访问，请查看 FirewallRule 和 FirewallPolicy 字段，以确定策略中阻止访问的规则。

# NSEL 数据流故障排除

使用 CDO 宏为 ASA 设备配置 NSEL 后，请使用以下程序验证 NSEL 事件是否从 ASA 发送到思科云以及思科云是否正在接收这些事件。

请注意，一旦 ASA 被配置为将 NSEL 事件发送到安全事件连接器 (SEC)，然后再发送到思科云，数据不会立即流动。假设 ASA 上生成了与 NSEL 相关的流量，第一个 NSEL 数据包可能需要几分钟才能到达。

**Note** 此工作流程向您展示如何直接使用“flow-export counters”命令和“capture”命令对 NSEL 数据流进行故障排除。有关这些命令用法的更详细讨论，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中的“数据包捕获”和《思科 ASA NetFlow 实施指南》中的“监控 NSEL”。

执行这些任务：

- 验证 NetFlow 数据包是否正在发送到 SEC
- 验证思科云是否正在接收 NetFlow 数据包

# 事件日志记录故障排除日志文件

安全事件连接器 (SEC) troubleshoot.sh 收集所有事件流传输器日志，并将其压缩到单个 .tar.gz 文件中。

使用以下程序创建 comparessed.tar.gz 文件并解压缩该文件：

1. 运行故障排除脚本，第 501 页。
2. 解压缩 sec_troubleshoot.tar.gz 文件，第 502 页。

## 运行故障排除脚本

安全事件连接器 (SEC) troubleshoot.sh 收集所有事件流传输器日志，并将其压缩到单个 .tar.gz 文件中。请按照以下程序运行 Troubleshooting.sh 脚本：

**步骤 1** 打开 VM 虚拟机监控程序并启动安全设备连接器 (SDC) 的控制台会话。

**步骤 2** 登录并切换到 **root** 用户：

```
[cdo@localhost ~]$sudo su root
```

**Note** 您也可以切换到 sdc 用户，但作为根用户，您还将收到 IP 表信息。IP 表信息显示防火墙正在设备上运行，并且所有防火墙路由。如果防火墙阻止安全事件连接器 TCP 或 UDP 端口，事件将不会显示在事件日志记录表中。IP 表将帮助您确定是否属于这种情况。

**步骤 3** 在提示符后，运行故障排除脚本并指定租户名称。以下是命令语法：

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

以下为输出示例：

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

在命令输出中，您会看到 sec_troubleshoot 文件存储在 SDC 上的 **/tmp/troubleshoot** 目录中。文件名遵循约定 **sec_troubleshoot-*timestamp*.tar.gz.**

**步骤 4** 要检索文件，请以 CDO 用户身份登录并使用 SCP 或 SFTP 下载文件。

以下为输出示例：

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

### What to do next

请继续解压缩 sec_troubleshoot.tar.gz 文件, on page 502。

## 解压缩 sec_troubleshoot.tar.gz 文件

安全事件连接器 (SEC) 运行故障排除脚本 脚本收集所有事件流传输器日志，并将其压缩到一个 sec_troubleshoot.tar.gz 文件中。按照此程序解压缩 sec_troubleshoot.tar.gz 文件。

1. 打开 VM 虚拟机监控程序并启动安全设备连接器 (SDC) 的控制台会话。
2. 登录并切换到 **root** 用户：

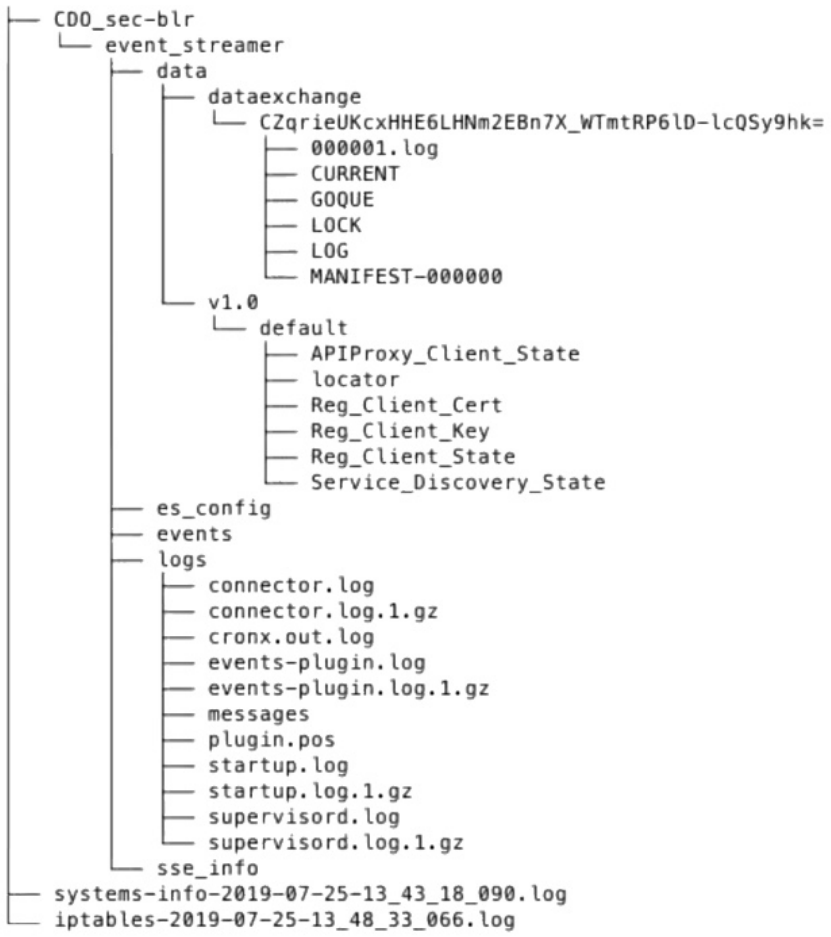
   ```
   [cdo@localhost ~]$sudo su root
   ```

**Note** 您也可以切换到 **sdc** 用户，但作为根用户，您还将收到 IP 表信息。IP 表信息显示防火墙正在设备上运行，并且所有防火墙路由。如果防火墙阻止安全事件连接器 TCP 或 UDP 端口，事件将不会显示在事件日志记录表中。IP 表将帮助您确定是否属于这种情况。

3. 在提示符后，键入以下命令：

   ```
   [root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
   ```

日志文件存储在以租户命名的目录中。这些是存储在 sec_troubelshoot-timestamp.tar.gz 文件中的日志类型。如果您以 root 用户身份收集所有日志文件，则包括 iptables 文件。




# 生成 SEC 引导程序数据失败。

症状：在 CDO 中生成 SEC 引导程序数据时，“引导程序生成”步骤失败并显示错误：“获取引导程序数据时出错。请重试。"

修复：再次重试引导程序数据生成。如果仍然失败，请联系 CDO 支持。CDO 客户如何通过 TAC 提交支持请求, on page 535

# 载入后，CDO 安全连接器页面中的 SEC 状态为“非活动”

症状：由于以下原因之一，CDO 安全连接器页面中的安全事件连接器状态显示为“非活动”：

- 心跳失败
- 连接器注册失败

**修复：**

- 心跳失败：请求 SEC 心跳并刷新“安全连接器”页面，以查看状态是否更改为“活动”，如果未更改，请检查安全设备连接器注册是否失败。

- **连接器注册失败**：请参阅问题 安全事件连接器注册失败故障排除。

# SEC 处于“在线”状态，但 CDO 事件日志记录页面中没有事件

症状：安全事件连接器在 CDO 安全连接器页面中显示“活动”，但在 CDO 事件查看器中看不到事件。

解决方案或解决方法：

---

**步骤 1** 以“sdc”用户身份登录到本地 SDC 的虚拟机。在提示符后，键入 **sudo su - sdc**。

**步骤 2** 执行以下检查：

- 查看 SEC 连接器日志 ( /usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log ) 并确保 SEC 注册已成功。如未成功，请参阅问题“安全事件连接器注册失败故障排除”。
- 检查 SEC 事件日志 ( /usr/local/cdo/data/<tenantDir> /event_streamer/logs/events-plugin.log）并确保事件正在处理。否则，请CDO 客户如何通过 TAC 提交支持请求。
- 登录到 SEC docker 容器并执行命令“supervisorctl -c /opt/cssp/data/conf/supervisord.conf”，并确保输出如下所示，并且所有进程都处于 RUNNING 状态。否则，请CDO 客户如何通过 TAC 提交支持请求。

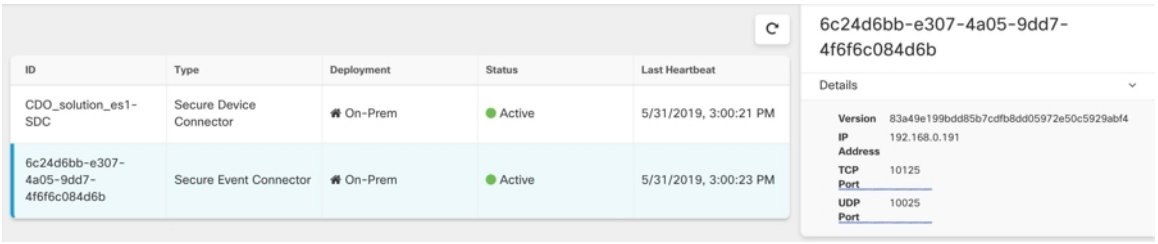
**estreamer-connector RUNNING pid 36, uptime 5:25:17**

**estreamer-cron RUNNING pid 39, uptime 5:25:17**

**estreamer-plugin RUNNING pid 37, uptime 5:25:17**

**estreamer-rsyslog RUNNING pid 38, uptime 5:25:17**

- 确保本地 SDC 上的防火墙规则未阻止“安全连接器”(Secure Connectors) 页面上为 SEC 显示的 UDP 和 TCP 端口。要确定需要打开的端口，请参阅查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口。




- 如果您使用自己的 CentOS 7 虚拟机手动设置了 SDC，并将防火墙配置为阻止传入请求，则可以执行以下命令来取消阻止 UDP 和 TCP 端口：

**firewall-cmd --zone=public --add-port=<udp_port> /udp --permanent**

**firewall-cmd --zone=public --add-port=<tcp_port> /tcp --permanent**

**firewall-cmd --reload**

- 使用您选择的 Linux 网络工具，检查是否在这些端口上接收数据包。如果未收到，请重新检查 FTD 日志记录配置。

如果上述修复方法均无效，请向 CDO 支持人员提交支持请求。 CDO 客户如何通过 TAC 提交支持请求, on page 535。

# SEC 清理命令

安全事件连接器 (SEC) 清理命令可从安全设备连接器 (SDC) 虚拟机中删除 SEC 容器及其关联的文件。您可以在 安全事件连接器注册失败故障排除, on page 499 或载入失败的情况下运行此命令。

运行命令：

### Before you begin

要执行此任务，您需要知道租户的名称。要查找租户名称，请在CDO中打开用户菜单，然后点击**设置 (Settings)**。向下滚动页面以找到您的**租户名称 (Tenant Name)**。

**步骤 1** 以 `sdc` 用户身份登录 SDC。在提示符后，键入 `sudo su - sdc`。

**步骤 2** 连接到 `/usr/local/cdo/toolkit` 目录。

**步骤 3** 运行 `sec.sh remove`*`tenant_name`* 并确认您打算删除 SEC。

示例：

```
 [sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

### What to do next

如果此命令无法删除 SEC，请继续执行 SEC 清理命令失败, on page 505：

# SEC 清理命令失败

如果 SEC 清理命令, on page 505 失败，请使用此程序。

**消息**：找不到 SEC，正在退出。

**症状**：清理 SEC 命令无法清理现有 SEC。

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42] SEC
 not found, exiting.
```

**修复**： 当清理命令失败时，手动清理安全事件连接器。

删除已在运行的 SEC docker 容器：

**步骤 1** 以“sdc”用户身份登录 SDC。在提示符后，键入 `sudo su - sdc`。

**步骤 2** 运行 **docker ps** 命令以查找 SEC 容器的名称。SEC 名称的格式为“es_ *name*”。

**步骤 3** 运行 **docker stop** 命令以停止 SEC 容器。

**步骤 4** 运行 **rm** 命令以删除 SEC 容器。

**例如：**

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

# 使用运行状况检查了解安全事件连接器的状态

安全事件连接器 (SEC) 运行状况检查脚本提供有关 SEC 状态的信息。

请按照以下程序运行运行状况检查：

**步骤 1** 打开 VM 监控程序并启动安全设备连接器 (SDC) 的控制台会话。

**步骤 2** 以“cdo”用户身份登录 SDC。

**步骤 3** 切换到“sdc”用户：

```
[cdo@tenant]$sudo su sdc
```

**步骤 4** 在提示符后，运行 healthcheck.sh 脚本并指定租户名称：

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

例如：

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

脚本的输出提供以下信息：

```
================================================
Running SEC health check for tenant [redacted]
------------------------------------------------
SEC cloud URL [redacted] is: Reachable
------------------------------------------------
SEC Connector status: Active
------------------------------------------------
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
------------------------------------------------
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
================================================
```

运行状况检查输出的值：

- **SEC 云 URL**：显示 CDO 云 URL 以及 SEC 是否可以访问 CDO。
- **SEC 连接器**：如果 SEC 连接器已正确载入并启动，则会显示“正在运行”(Running)。
- **SEC UDP 系统日志服务器**：如果 UDP 系统日志服务器已准备好发送 UDP 事件，则显示“正在运行”。
- **SEC TCP 系统日志服务器**：如果 TCP 系统日志服务器已准备好发送 TCP 事件，将显示“正在运行”。
- **SEC 连接器状态**：如果 SEC 正在运行并已载入到 CDO，则会显示为“活动”(Active)。

- **SEC 发送示例事件**：如果在运行状况检查结束时，所有状态检查均为“绿色”，则该工具会发送示例事件。（如果有任何进程“关闭”，则工具会跳过发送测试事件。）示例事件在事件日志中显示为名为“sec-health-check” 的策略。

# 对思科防御协调器进行故障排除

## 登录失败故障排除

**登录失败，因为您无意中登录到错误的 CDO 区域**

请确保您登录的是适当的 CDO 区域。登录 https://sign-on.security.cisco.com 后，您可以选择要访问的区域。点击 **CDO** 磁贴访问 Defenseorchestrator.com 或点击 **CDO (EU)** 访问 Defenseorchestrator.eu。

## 迁移后的登录失败故障排除

**由于用户名或密码不正确，CDO 登录失败**

**解决方法** 如果您尝试登录 CDO，并且知道您使用的是正确的用户名和密码，但登录失败，或者您尝试“忘记密码”无法恢复有效的密码，则您可能已尝试在未创建新 Cisco Security Cloud Sign On 帐户的情况下进行登录，则您需要按照创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 58 页中的说明注册新的 Cisco Security Cloud Sign On 帐户。

**登录到 Cisco Security Cloud Sign On 控制面板成功，但您无法启动 CDO**

**解决方法** 您可能使用与 CDO 租户不同的用户名创建了 Cisco Security Cloud Sign On 账户。请联系思科技术支持中心 (TAC)，以规范 CDO 和 Cisco Secure Sign-On 之间的用户信息。

**使用保存的书签登录失败**

**解决方法** 您可能正在尝试使用浏览器中保存的旧书签登录。书签可能指向 https://cdo.onelogin.com。https://cdo.onelogin.com/

**解决方法** 登录 https://sign-on.security.cisco.com。

- **解决方法** 如果您尚未创建 Cisco Secure Sign-On 账户，请创建一个账户。创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 58 页
- **解决方法** 如果您已创建新账户，请点击控制面板上与 思科防御协调器（美国）、思科防御协调器（欧盟）或 思科防御协调器（亚太地区）对应的 CDO 磁贴
- **解决方法** 将书签更新为指向 https://sign-on.security.cisco.com。https://sign-on.security.cisco.com/

# 访问和证书故障排除

## 使用 CDO 排除用户访问故障

考虑用户被拒绝访问他们应该有权访问的资源的情况。以下是您可以用来诊断和补救该问题的方法。

**步骤 1** 用户通知您的安全团队其对资源的访问已被阻止。确定通常如何访问该资源。它的 IP 地址是什么？您是否在特定端口上访问它？使用哪种协议向资源发送信息？

**步骤 2** 在**设备和服务 (Devices & Services)** 页面上，点击**设备 (Devices)** 选项卡。

**步骤 3** 点击 FTD 选项卡，选择 ASA 并运行数据包跟踪器。有关详细说明，请参阅 ASA 数据包跟踪器。

**步骤 4** 检查数据包跟踪表，了解可能已拒绝访问资源的规则。

**步骤 5** 确定拒绝访问的规则后，在CDO中创建一个更改请求标签并启用它。请参阅更改请求管理, on page 334。这将帮助您在更改日志中识别您为允许访问资源所做的更改。

**步骤 6** 从 CDO 编辑规则以更正行为。您的 ASA 现在与 CDO 不同步。

**步骤 7** 从设备和服务页面将更改部署到 ASA。CDO 通过保存在 ASA 上的配置来跟踪数据包，而不是在 CDO 上暂存的配置。请注意，您还会将在 CDO 上暂存的任何其他配置更改部署到 ASA。

**步骤 8** 重新运行数据包跟踪器，以确定策略更改是否提供所需的结果。确认您的用户现在有权访问资源。

**步骤 9** 假设您的用户现在具有访问权限，请清除CDO中的更改请求标签。这可以防止不相关的活动与此修复程序关联。

**Note** 如果您所做的更改不能解决问题或产生了一些新问题，并且您想要恢复到以前的配置，则可以恢复ASA配置。请参阅恢复 ASA 配置。

## 解析检测到的新指纹状态

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择处于检测到**新指纹状态**的设备。

**步骤 5** 点击检测到的新指纹窗格中的**查看指纹**。

**步骤 6** 当系统提示您查看并接受指纹时：

**a.** 点击**下载指纹**并进行查看。

**b.** 如果您对指纹满意，请点击**接受**。如果不是，请点击**取消**。

**步骤 7** 解决新的指纹问题后，设备的连接状态可能会显示为**在线**，而配置状态可能会显示“未同步”或“检测到冲突”。回顾解决配置冲突 以查看和解决 CDO 与设备之间的配置差异。

# 使用安全和分析日志记录事件排除网络问题

以下是使用事件查看器排除网络问题的基本框架。

此场景假设您的网络运营团队收到报告，指出用户无法访问网络上的资源。根据报告问题的用户及其位置，网络运营团队可以合理地了解哪个防火墙控制其对资源的访问。

**Note** 此场景还假设 FDM 管理 设备是管理网络流量的防火墙。安全分析和日志记录不会从其他设备类型收集日志记录信息。

**步骤 1** 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**历史 (Historical)** 选项卡。

**步骤 3** 按**时间范围 (Time Range)** 开始过滤事件。默认情况下，“历史”(Historical) 选项卡显示最近一小时的事件。如果这是正确的时间范围，请输入当前日期和时间作为**结束**时间。如果该时间范围不正确，请输入包含所报告问题时间的开始和结束时间。

**步骤 4** 在**传感器 ID (Sensor ID)** 字段中输入您怀疑控制用户访问的防火墙的 IP 地址。如果可能是多个防火墙，请使用搜索栏中的 **attribute:value** 对过滤事件。输入两个条目并将其与 OR 语句组合在一起。例如：`SensorID:192.168.10.2 OR SensorID:192.168.20.2`。

**步骤 5** 在事件过滤器栏中的**源 IP (Source IP)** 字段中输入用户的 IP 地址。

**步骤 6** 如果用户无法访问资源，请尝试在**目标 IP (Destination IP)** 字段中输入该资源的 IP 地址。

**步骤 7** 展开结果中的事件并查看其详细信息。以下是一些需要查看的详细信息：

- **AC_RuleAction** - 触发规则时采取的操作（允许、信任、阻止）。
- **FirewallPolicy** - 触发事件的规则所在的策略。
- **FirewallRule** - 触发事件的关联规则的名称。如果值为“默认操作”(Default Action)，则触发事件的是策略的默认操作，而不是策略中的某个规则。
- **UserName** - 与发起方 IP 地址关联的用户。发起方 IP 地址与源 IP 地址相同。

**步骤 8** 如果规则操作阻止访问，请查看 FirewallRule 和 FirewallPolicy 字段，以确定策略中阻止访问的规则。

# SSL 解密问题故障排除

### 处理解密重签名适用于浏览器而非应用的 Web 站点（SSL 或证书颁发机构锁定）

智能手机和其他设备的某些应用使用 SSL（或证书颁发机构）锁定技术。SSL 锁定技术将原始服务器证书的散列值嵌入到应用本身内部。因此，当应用收到来自 Firepower Threat Defense设备的重签证书时，散列验证会失败并中止连接。

主要表现是，用户使用站点应用无法连接到网站，但可以使用网络浏览器连接，即使在应用无法正常工作的同一台设备上使用浏览器也可以连接。例如，用户不能使用 Facebook iOS 或 Android 应用，但可以通过 https://www.facebook.com 转至 Safari 或 Chrome，进行成功连接。

由于 SSL 锁定专用于避免中间人攻击，因此此问题无法解决。必须从以下选项中选择一项：

**更多详细信息**

如果站点在浏览器中可用，但不能在同一设备的应用中使用，几乎可以肯定这是一个 SSL 锁定实例。但是，如果您想要更深入地挖掘，除了浏览器测试之外，还可以使用连接事件确定 SSL 锁定。

应用可能会通过两种方式处理散列验证失败：

- 第 1 组应用，例如 Facebook，从服务器收到 SH、CERT、SHD 消息后立即发送 SSL 警告消息。警告通常是一个表示 SSL 锁定的“Unknown CA (48)” 警告。紧接着警告消息发送 TCP 重置。在事件详细信息中，您应看到以下现象：
  - SSL 流标志包括 ALERT_SEEN。
  - SSL 流标志不包括 APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE。
- 第 2 组应用，例如 Dropbox，不会发送任何警告。而是，等到完成握手后发送 TCP 重置。在事件中，您应看到以下现象：
  - SSL 流标志不包括 ALERT_SEEN、APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED。

# 迁移后的登录失败故障排除

**由于用户名或密码不正确，CDO 登录失败**

**解决方法** 如果您尝试登录 CDO，并且知道您使用的是正确的用户名和密码，但登录失败，或者您尝试“忘记密码”无法恢复有效的密码，则您可能已尝试在未创建新 Cisco Security Cloud Sign On 帐户的情况下进行登录，则您需要按照创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 58 页中的说明注册新的 Cisco Security Cloud Sign On 帐户。

**登录到 Cisco Security Cloud Sign On 控制面板成功，但您无法启动 CDO**

**解决方法** 您可能使用与 CDO 租户不同的用户名创建了 Cisco Security Cloud Sign On 账户。请联系思科技术支持中心 (TAC)，以规范 CDO 和 Cisco Secure Sign-On 之间的用户信息。

**使用保存的书签登录失败**

**解决方法** 您可能正在尝试使用浏览器中保存的旧书签登录。书签可能指向 https://cdo.onelogin.com。https://cdo.onelogin.com/

**解决方法** 登录 https://sign-on.security.cisco.com。

- **解决方法** 如果您尚未创建 Cisco Secure Sign-On 账户，请创建一个账户。创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 58 页
- **解决方法** 如果您已创建新账户，请点击控制面板上与 思科防御协调器（美国）、思科防御协调器（欧盟）或 思科防御协调器（亚太地区）对应的 CDO 磁贴
- **解决方法** 将书签更新为指向 https://sign-on.security.cisco.com。https://sign-on.security.cisco.com/

# 对象故障排除

## 解决重复对象问题

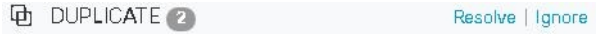
重复对象 是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常是意外创建的，可用于类似的目的，并供不同的策略使用。解决重复对象问题后，CDO 会使用保留的对象名称来更新所有受影响的对象引用。

要解决重复对象问题，请执行以下操作：

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 然后对象过滤器对象以查找重复的对象问题。

**步骤 3** 选择其中一个结果。在对象详细信息面板中，您将看到“重复”(DUPLICATE) 字段以及受影响的重复项数：




**步骤 4** 点击**解决**。CDO 会显示要比较的重复对象。

**步骤 5** 选择两个要比较的对象。

**步骤 6** 您现在有以下选项：

- 如果要将其中一个对象替换为另一个对象，请点击要保留的对象的**选择 (Pick)**，点击**解决 (Resolve)** 以查看将受到影响的设备和网络策略，如果对更改满意，请点击**确认 (Confirm)**。CDO 会保留您选择替换的对象，同时删除重复项。
- 如果列表中有要忽略的对象，请点击**忽略 (Ignore)**。如果您忽略某个对象，它就会从 CDO 显示的重复对象列表中删除。
- 如果要保留对象，但又不希望 CDO 在搜索重复对象时找到该对象，请点击**全部忽略 (Ignore All)**。

**步骤 7** 一旦解决重复对象问题，请预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

## 解决未使用的对象问题

未使用的对象 是设备配置中存在但未被其他对象、访问列表或 NAT 规则引用的对象。

**相关信息：**

- 导出设备和服务列表，第 73 页

- 将设备批量重新连接到 CDO ， 第 77 页

## 解决未使用的对象问题

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 然后对象过滤器对象以查找未使用的对象问题。

**步骤 3** 选择一个或多个未使用的对象。

**步骤 4** 您现在有以下选项：

- 在操作窗格中，点击**删除 (Remove)** 以从 CDO 中删除未使用的对象。
- 在问题窗格中，点击**忽略 (Ignore)**。如果您忽略某个对象，CDO 将停止在未使用的对象的结果中显示该对象。

**步骤 5** 如果您删除了未使用的对象、 预览和部署所有设备的配置更改, on page 313 您现在所做的更改，或者等待并一次部署多个更改。

**Note** 要批量解决未使用的对象问题，请参阅批量解决对象问题。

## 批量删除未使用的对象

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 然后对象过滤器对象以查找未使用的对象问题。

**步骤 3** 选择要删除的未使用对象：

- 点击对象表头行中的复选框，以便选择页面上的所有对象。
- 在对象表中选择单个未使用的对象。

**步骤 4** 在“操作”(Actions) 窗格中，点击**删除 (Remove)** 以删除在 CDO 中选定的所有未使用的对象。一次可以删除 99 个对象。

**步骤 5** 点击**确定 (OK)** 以确认您要删除未使用的对象。

**步骤 6** 您有两种选择来部署这些更改：

- 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。
- 打开**清单 (Inventory)** 页面并查找受更改影响的设备。选择受更改影响的所有设备，然后在管理窗格中点击**全部部署**。阅读警告并采取适当的措施。

# 解决不一致的对象问题

不一致对象  是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。

**注意**：要批量解决不一致的对象问题，请参阅批量解决对象问题。

您可以对不一致的对象执行以下操作：

- **忽略**：CDO 忽略对象之间的不一致并保留其值。对象将不再列在不一致类别下。
- **合并**：CDO 将所有选定对象及其值合并到一个对象组中。
- **重命名**：CDO 允许您重命名其中一个不一致的对象并为其指定新名称。
- **将共享网络对象转换为覆盖**：CDO 允许您将不一致的共享对象（有或没有覆盖）合并为一个具有覆盖的共享对象。不一致对象中最常见的默认值设置为新形成的对象中的默认值。

**Note** 如果有多个通用默认值，则选择其中一个作为默认值。其余默认值和覆盖值设置为该对象的覆盖。

- **将共享网络组转换为其他值**： - CDO 允许您将不一致的共享网络组合并为具有其他值的单个共享网络组。此功能的条件是，要转换的不一致网络组必须至少有一个具有相同值的通用对象。与此条件匹配的所有默认值都将成为默认值，其余对象将作为新形成的网络组的其他值进行分配。

  例如，请考虑两个不一致的共享网络组。第一个网络组“shared_network_group”由“object_1”（192.0.2.x）和“object_2”（192.0.2.y）组成。它还包含附加值“object_3”(192.0.2.a)。第二个网络组“shared_network_group”由“object_1”(192.0.2.x) 和附加值“object_4”(192.0.2.b) 组成。将共享网络组转换为其他值时，新形成的组“shared_network_group”包含默认值“object_1”(192.0.2.x) 和“object_3”(192.0.2.y)”。 2.a) 和 'object_4' (192.0.2.b) 作为附加值。

**Note** 当您创建新的网络对象时，CDO 会自动将其值作为覆盖分配给具有相同名称的现有共享网络对象。这也适用于将新设备载入 CDO 的情况。

仅当满足以下条件时才会进行自动分配：

1. 必须将新网络对象分配给设备。
2. 租户中只能存在一个具有相同名称和类型的共享对象。
3. 共享对象必须已包含覆盖。

要解决不一致的对象问题，请执行以下操作：

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 然后对象过滤器对象以查找不一致的对象问题。

**步骤 3** 选择不一致的对象。在对象详细信息面板中，您将看到包含受影响对象数量的不一致字段：

**步骤 4** 点击**解决**。CDO 显示不一致的对象以供比较。

**步骤 5** 您现在有以下选项：

- **全部忽略**：
  a. 比较显示的对象，然后在其中一个对象上点击**忽略 (Ignore)**。或者，要忽略所有对象，请点击**全部忽略 (Ignore All)**。
  b. 点击**确定 (OK)**以进行确认。
- **通过合并对象来解决**：
  a. 点击**通过合并 X 对象来解决 (Resolve by Merging X Objects)**。
  b. 点击**确认 (Confirm)**。
- **重命名**：
  a. 点击**重命名**。
  b. 保存对受影响的网络策略和设备所做的更改，然后点击**确认 (Confirm)**。
- **转换为覆盖（对于不一致的共享对象）**：将共享对象与覆盖进行比较时，比较面板仅显示**不一致的值 (Inconsistent Values)** 字段中的默认值。
  a. 点击**转换为覆盖 (Convert to Overrides)**。所有不一致的对象都将转换为具有覆盖的单个共享对象。
  b. 点击**确认 (Confirm)**。您可以点击**编辑共享对象 (Edit Shared Object)** 以查看新创建的对象的详细信息。您可以使用向上和向下箭头在默认值和覆盖之间移动值。
- **转换为其他值（对于不一致的网络组）**：
  a. 点击**转换为其他值 (Convert to Additional Values)**。所有不一致的对象都将转换为具有其他值的单个共享对象。
  b. 保存对受影响的网络策略和设备所做的更改，然后点击**确认 (Confirm)**。

**步骤 6** 解决不一致问题后，请立即预览和部署所有设备的配置更改所做的更改，或者等待并立即部署多个更改。

## 批量解决对象问题

解决具有解决未使用的对象问题、解决重复对象问题或解决不一致的对象问题, on page 513 问题的对象的方法之一是忽略它们。您可以选择并忽略多个对象，即使对象表现出多个问题也是如此。例如，如果对象既不一致又未使用，则一次只能忽略一种问题类型。

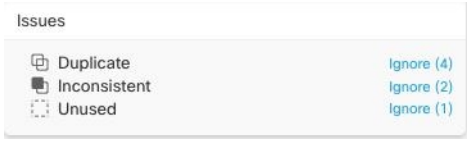
**Important** 如果该对象稍后与其他问题类型关联，则您提交的忽略操作仅影响您当时选择的问题。例如，如果您忽略某个对象，因为它是重复的，并且该对象后来被标记为不一致，则将其忽略为重复对象并不意味着它将作为不一致的对象被忽略。

要批量忽略问题，请执行以下程序：

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 要缩小搜索范围，您可以对象过滤器对象问题。

**步骤 3** 在对象表中，选择要忽略的所有适用对象。“问题”窗格按问题类型对对象进行分组。




**步骤 4** 点击**忽略 (Ignore)** 可按类型忽略问题。您必须单独**忽略**每种问题。

**步骤 5** 点击**确定 (OK)** 以确认要忽略这些对象。

# 设备连接状态

您可以查看 CDO 租户中载入的设备的连接状态。本主题可帮助您了解各种连接状态。在**清单 (Inventory)** 页面上，**连接 (Connectivity)** 列显示设备连接状态。

当设备连接状态为“在线”时，表示设备已通电并连接到CDO。当设备由于各种原因遇到问题时，通常会出现下表中所述的其他状态。下表提供了从此类问题中恢复的方法。可能有多个问题导致连接失败。当您尝试重新连接时，CDO 会提示您先解决所有这些问题，然后再执行重新连接。

| 设备连接状态 | 可能的原因 | 解决方法 |
|---|---|---|
| 在线 | 设备已通电并连接到 CDO。 | 不适用 |
| 离线 | 设备已关闭或丢失网络连接。 | 检查设备是否处于离线状态。 |
| 许可证不足 | 设备没有足够的许可证。 | 许可证不足故障排除, on page 516 |
| 凭证无效 | CDO 用于连接到设备的用户名和密码组合不正确。 | 对无效凭证进行故障排除, on page 516 |

| 设备连接状态 | 可能的原因 | 解决方法 |
| --- | --- | --- |
| 载入 | 设备载入已启动，但尚未完成。 | 检查设备的连接并确保完成设备注册。 |
| 检测到新证书 | 设备上的证书已更改。如果设备使用自签名证书，则可能是由于设备重新启动而导致的。 | 新证书问题故障排除, on page 517 |
| 载入错误 | 在载入设备时，CDO 可能已失去与设备的连接。 | 对载入错误进行故障排除, on page 525 |

# 许可证不足故障排除

如果设备连接状态显示“许可证不足”(Insufficient License)，请执行以下操作：

- 等待一段时间，直到设备获得许可证。通常，思科智能软件管理器需要一些时间才能将新许可证应用于设备。
- 如果设备状态未更改，请从 CDO 注销并重新签名，以刷新 CDO 门户，以解决许可证服务器和设备之间的任何网络通信故障。
- 如果门户刷新未更改设备状态，请执行以下操作：

**步骤 1** 从思科智能软件管理器生成新的令牌并进行复制。您可以观看生成智能许可视频了解详细信息。

**步骤 2** 在 CDO 导航栏中，点击**设备和服务 (Devices & Services)** 页面。

**步骤 3** 点击**设备**选项卡。

**步骤 4** 点击相应的设备类型选项卡，然后选择状态为**许可证不足**的设备。

**步骤 5** 在**设备详细信息 (Device Details)** 窗格中，点击**许可证不足 (Insufficient Licenses)**中出现的**管理许可证 (Manage Licenses)**。此时将出现**管理许可证 (Manage Licenses)** 窗口。

**步骤 6** 在**激活 (Activate)** 字段中，粘贴新的令牌，然后点击**注册设备 (Register Device)**。

将令牌成功应用于设备后，其连接状态将变为**在线 (Online)**。

# 对无效凭证进行故障排除

执行以下操作以解决由于凭证无效而导致设备断开连接的问题：

**步骤 1** 打开**清单 (Inventory)** 页面。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择具有**无效凭证 (Invalid Credentials)** 状态的设备。

**步骤 4** 在**设备详细信息 (Device Details)** 窗格中，点击**无效凭证 (Invalid Credentials)** 中显示的 **重新连接 (Reconnect)**。CDO 尝试与您的设备重新连接。

**步骤 5** 出现提示时，输入设备的用户名和密码。

**步骤 6** 点击**继续**。

**步骤 7** 设备在线并准备好使用后，点击**关闭 (Close)**。

**步骤 8** 可能是因为 CDO 尝试使用错误的凭证连接到设备，因此直接在设备上更改了 CDO 用于连接到设备的用户名和密码组合。您现在可能会看到设备处于“在线”(Online) 状态，但配置状态为“检测到冲突”(Conflict Detected)。使用解决配置冲突 以查看和解决 CDO 与设备之间的配置差异。

# 新证书问题故障排除

### CDO 对证书的使用

CDO 在连接到设备时检查证书的有效性。具体而言，CDO 要求：

1. 设备使用 TLS 版本 1.0 或更高版本。
2. 设备提供的证书未过期，并且其颁发日期是过去的日期（即，它已经有效，未计划在以后生效）。
3. 证书必须是 SHA-256 证书。不接受 SHA-1 证书。
4. 以下条件之一成立：
   - 设备使用自签名证书，并且与授权用户信任的最新证书相同。
   - 设备使用受信任证书颁发机构 (CA) 签名的证书，并提供将所提供的枝叶证书链接到相关 CA 的证书链。

以下是 CDO 使用与浏览器不同的证书的方式：

- 如果是自签名证书，则 CDO 会覆盖域名检查，而不会在设备载入或重新连接期间检查证书是否与授权用户信任的证书完全匹配。
- CDO 尚不支持内部 CA。目前无法检查由内部 CA 签名的证书。

  可以按设备禁用 ASA 设备的证书检查。当 CDO 无法信任 ASA 的证书时，您可以选择禁用该设备的证书检查。如果您已尝试禁用设备的证书检查，但仍无法将其载入，则可能是您为设备指定的 IP 地址和端口不正确或无法访问。无法全局禁用证书检查，也无法对具有受支持证书的设备禁用证书检查。无法禁用非 ASA 设备的证书检查。

  当您禁用设备的证书检查时，CDO 仍将使用 TLS 连接到设备，但不会验证用于建立连接的证书。这意味着被动的中间人攻击者将无法窃听连接，但主动的中间人可以通过提供具有无效证书的 CDO 来拦截连接。

### 确定证书问题

CDO 可能无法载入设备的原因有很多种。当 UI 显示消息“CDO 无法使用提供的证书连接到设备”时，表示证书存在问题。当UI不显示此消息时，问题更有可能与连接问题（设备无法访问）或其他网络错误有关。

要确定 CDO 拒绝给定证书的原因，您可以在 SDC 主机或可访问相关设备的其他主机上使用 openssl 命令行工具。使用以下命令创建显示设备提供的证书的文件：

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

此命令将启动交互式会话，因此您需要在几秒钟后使用 Ctrl-c 退出。

您现在应该有一个包含如下输出的文件：

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
```

```
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

在此输出中要注意的第一件事是最后一行，您可以在其中看到**验证返回代码 (Verify return code)**。如果存在证书问题，返回代码将为非零值，并且会有错误说明。

**展开此证书错误代码列表，查看常见错误及其补救方法**

0 X509_V_OK 操作成功。

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT 无法找到不受信任证书的颁发者证书。

3 X509_V_ERR_UNABLE_TO_GET_CRL 无法找到证书的 CRL。

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE 无法解密证书签名。这意味着无法确定实际签名值，而不是与预期值不匹配。这仅对 RSA 密钥有意义。

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE 无法解密 CRL 签名。这意味着无法确定实际签名值，而不是与预期值不匹配。未使用。

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY 无法读取证书 SubjectPublicKeyInfo 中的公钥。

7 X509_V_ERR_CERT_SIGNATURE_FAILURE 证书签名无效。

8 X509_V_ERR_CRL_SIGNATURE_FAILURE 证书签名无效。

9 X509_V_ERR_CERT_NOT_YET_VALID 证书无效：notBefore 日期晚于当前时间。有关详细信息，请参阅下面的验证返回代码：9（证书尚未生效）。

10 X509_V_ERR_CERT_HAS_EXPIRED The certificate has expired;也就是说，notAfter 日期早于当前时间。有关详细信息，请参阅下面的验证返回代码：10（证书已过期）。

11 X509_V_ERR_CRL_NOT_YET_VALID CRL 尚未生效。

12 X509_V_ERR_CRL_HAS_EXPIRED CRL 已过期。

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD 证书 notBefore 字段包含无效时间。

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD 证书 notAfter 字段包含无效时间。

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD CRL lastUpdate 字段包含无效时间。

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD CRL nextUpdate 字段包含无效时间。

17 X509_V_ERR_OUT_OF_MEM 尝试分配内存时发生错误。这绝不应该发生。

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT 通过的证书是自签名证书，在受信任证书列表中找不到相同的证书。

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN 可以使用不受信任的证书建立证书链，但无法在本地找到根证书。

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 无法找到本地查找的证书的颁发者证书。这通常意味着受信任证书列表不完整。

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE 无法验证签名，因为该链仅包含一个证书，并且它不是自签名证书。有关详细信息，请参阅下面的“验证返回代码：21（无法验证第一个证书）”。验证返回代码：21（无法验证下面的第一个证书）以了解详细信息。

22 X509_V_ERR_CERT_CHAIN_TOO_LONG 证书链长度大于提供的最大深度。未使用。

23 X509_V_ERR_CERT_REVOKED 证书已被撤销。

24 X509_V_ERR_INVALID_CA CA 证书无效。它不是 CA 或其扩展名与提供的用途不一致。

25 X509_V_ERR_PATH_LENGTH_EXCEEDED BasicConstraints 路径长度参数已被超过。

26 X509_V_ERR_INVALID_PURPOSE 提供的证书不能用于指定的目的。

27 X509_V_ERR_CERT_UNTRUSTED 根 CA 未标记为用于指定用途的受信任。

28 X509_V_ERR_CERT_REJECTED 根 CA 被标记为拒绝指定用途。

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH 当前候选颁发者证书被拒绝，因为其使用者名称与当前证书的颁发者名称不匹配。仅在设置了 -issuer_checks 选项时显示。

30 X509_V_ERR_AKID_SKID_MISMATCH 当前候选颁发者证书被拒绝，因为其使用者密钥标识符存在且与当前证书的颁发机构密钥标识符不匹配。仅在设置了 -issuer_checks 选项时显示。

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH 当前候选颁发者证书被拒绝，因为其颁发者名称和序列号存在，并且与当前证书的颁发机构密钥标识符不匹配。仅在设置了 -issuer_checks 选项时显示。

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN 当前候选颁发者证书被拒绝，因为其 keyUsage 扩展不允许证书签名。

50 X509_V_ERR_APPLICATION_VERIFICATION 应用特定错误。未使用。

### 检测到新证书

如果升级具有自签名证书的设备，并且在升级过程后生成了新证书，则CDO可能会生成“检测到新证书”(New Certificate Detected) 消息作为**配置状态 (Configuration Status)** 和**连接 (Connectivity)** 状

态。您必须手动确认并解决此问题，然后才能继续从CDO对其进行管理。证书同步且设备处于正常状态后，即可管理设备。

**Note** 当您同时将多个托管设备将设备批量重新连接到 CDO连接到 CDO 时，CDO 会自动审核并接受设备上的新证书，并继续与其重新连接。

使用以下程序解析新证书：

1. 导航到**设备和服务 (Device & Services)** 页面。
2. 使用过滤器显示**检测到新证书 (New Certificate Detected)** 连接或配置状态的设备，然后选择所需的设备。
3. 在右侧窗格中，点击**查看证书 (Review Certificate)**。CDO 允许您下载证书以供审核并接受新证书。
4. 在设备同步窗口中，点击**接受 (Accept)**，或在重新连接到设备窗口中，点击**继续 (Continue)**。

   CDO 会自动将设备与新的自签名证书同步。您可能需要手动刷新**设备和服务 (Devices & Services)** 页面，才能在设备同步后查看设备。

### 证书错误代码

#### 验证返回代码：0（正常），但 CDO 返回证书错误

CDO 获得证书后，它会尝试通过对“https://”进行 GET 调用来连接到设备的 URL。<device_ip>：<port> "。如果这不起作用，CDO 将显示证书错误。如果您发现证书有效（openssl 返回 0 ok），则问题可能是其他服务正在侦听您尝试连接的端口。只能使用命令：

```
curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

确定您是否确实在与 ASA 通信，并检查 HTTPS 服务器是否在 ASA 上的正确端口上运行：

```
 # show asp table socket
Protocol         Socket         State         Local Address              Foreign Address
SSL              00019b98        LISTEN        192.168.1.5:443             0.0.0.0:*
SSL              00029e18        LISTEN        192.168.2.5:443             0.0.0.0:*
TCP              00032208        LISTEN        192.168.1.5:22              0.0.0.0:*
```

#### 验证返回代码：9（证书尚未生效）

此错误意味着所提供证书的颁发日期是未来，因此客户端不会将其视为有效。这可能是由于证书构建不良导致的，或者在自签名证书的情况下，可能是由于设备生成证书时时间错误。

您应该会在错误中看到一行，包括证书的 notBefore 日期：

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

通过此错误，您可以确定证书何时生效。

**补救**

证书的 notBefore 日期需要是过去的日期。您可以使用更早的 notBefore 日期重新颁发证书。当客户端或颁发设备上的时间设置不正确时，也会出现此问题。

**验证返回代码：10（证书已过期）**

此错误意味着所提供的至少一个证书已过期。您应该会在错误中看到一行，包括证书的notBefore日期：

```
 error 10 at 0 depth lookup:certificate has expired
```

到期日期位于证书正文中。

**补救**

如果证书确实已过期，则唯一的补救方法是获取另一个证书。如果证书仍将到期，但openssl声称它已过期，请检查计算机上的时间和日期。例如，如果某个证书设置为在2020年到期，但您的计算机上的日期是 2021 年，则您的计算机会将该证书视为已过期。

**验证返回代码：21（无法验证第一个证书）**

此错误表示证书链存在问题，并且openssl无法验证设备提供的证书是否应受信任。我们来看看上面示例中的证书链，了解证书链的工作原理：

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

证书链是服务器提供的证书列表，从服务器自己的证书开始，然后包括将服务器的证书与证书颁发机构的顶级证书链接的更高级别的中间证书。每个证书都会列出其使用者（以“s:”开头的行及其颁发者）（以“i”开头的行）。

使用者是证书所标识的实体。它包括组织名称，有时还包括为其颁发证书的实体的通用名称。

颁发者是颁发证书的实体。它还包括一个组织字段，有时还包括一个通用名称。

如果服务器具有由受信任证书颁发机构直接颁发的证书，则无需在其证书链中包含任何其他证书。它将显示一个如下所示的证书：

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

鉴于此证书，openssl 将验证 ***.example.com** 的 ExampleCo 证书是否由受信任的颁发机构证书正确签名，该证书存在于 openssl 的内置信任存储区中。验证后，openssl 将成功连接到设备。

但是，大多数服务器没有直接由受信任 CA 签名的证书。相反，与第一个示例一样，服务器的证书由一个或多个中间设备签名，而最高级别的中间设备具有由受信任 CA 签名的证书。默认情况下，OpenSSL 不信任这些中间 CA，并且只有在获得以受信任 CA 结尾的完整证书链时才能对其进行验证。

由中间机构签署证书的服务器必须提供将其链接到受信任 CA 的所有证书，包括所有中间证书。如果它们不提供整个链，则 openssl 的输出将如下所示：

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
```

```
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

此输出显示服务器仅提供一个证书，并且提供的证书是由中间机构而不是受信任的根签名的。输出还显示特征验证错误。

**补救**

此问题是由设备提供的证书配置错误引起的。解决此问题的唯一方法是将正确的证书链加载到设备上，以便 CDO 或任何其他程序可以安全地连接到设备，以便为连接的客户端提供完整的证书链。

要将中间 CA 添加到信任点，请访问以下链接之一（具体取决于您的情况 - 是否在 ASA 上生成了 CSR）：

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

## 检测到新证书

如果升级具有自签名证书的设备，并且在升级过程后生成了新证书，则CDO可能会生成“检测到新证书”(New Certificate Detected) 消息作为**配置状态 (Configuration Status)** 和**连接 (Connectivity)** 状态。您必须手动确认并解决此问题，然后才能继续从CDO对其进行管理。证书同步且设备处于正常状态后，即可管理设备。

**注释** 当您选择将设备批量重新连接到 CDO 同时将多个托管设备连接到CDO时，CDO 会自动审核并接受设备上的新证书，并继续与其重新连接。

使用以下程序解析新证书：

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 使用过滤器显示**检测到新证书 (New Certificate Detected)** 连接或配置状态的设备，然后选择所需的设备。

**步骤 5** 在右侧窗格中，点击**查看证书 (Review Certificate)**。CDO 允许您下载证书以供审核并接受新证书。

**步骤 6** 在设备同步窗口中，点击**接受 (Accept)**，或在重新连接到设备窗口中，点击**继续 (Continue)**。

CDO 会自动将设备与新的自签名证书同步。您可能需要手动刷新**设备和服务 (Devices & Services)** 页面，才能在设备同步后查看设备。

# 对载入错误进行故障排除

出现设备载入错误的原因有很多。

可以采取以下操作：

**步骤 1** 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

**步骤 2** 点击相应的设备类型选项卡，然后选择遇到此错误的设备。在某些情况下，您会在右侧看到错误说明。执行说明中提到的必要操作。

或

**步骤 3** 从 CDO 中删除设备实例，然后尝试重新载入设备。

# 解决“检测到冲突”状态

CDO 允许您在每个实时设备上启用或禁用冲突检测。如果 冲突检测, on page 323 已启用，并且在未使用 CDO 的情况下对设备的配置进行了更改，则设备的配置状态将显示为**检测到冲突 (Conflict Detected)**。

要解决“检测到冲突”(Conflict Detected) 状态，请执行以下程序：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**Note** 对于 本地防火墙管理中心，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 并选择处于**检测到冲突 (Conflict Detected)** 状态的 FMC，然后从步骤 4 继续操作。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择报告冲突的设备，然后点击右侧详细信息窗格中的**查看冲突 (Review Conflict)**。

**步骤 5** 在**设备同步 (Device Sync)** 页面中，通过查看突出显示的差异来比较两种配置。

- 标记为“最后一次设备配置”(Last Known Device Configuration) 的面板是存储在 CDO 上的设备配置。
- 标记为“在设备上找到”(Found on Device) 的面板是存储在运行 ASA 配置中的配置。

**步骤 6** 通过选择以下选项之一来解决冲突：

- **接受设备更改 (Accept Device changes)**：这将使用设备的运行配置覆盖 CDO **上存储的配置** 和任何待处理的更改。

  **Note** 由于 CDO 不支持在命令行界面之外部署对Cisco IOS 设备的更改，因此在解决冲突时，您对Cisco IOS 设备的唯一选择是选择**接受而不查看 (Accept Without Review)**。

- **拒绝设备更改 (Reject Device Changes)**：这将使用存储在 CDO 上的配置覆盖设备上存储的配置。

**Note** 所有配置更改（拒绝或接受）都记录在更改日志中。

# 解决“未同步”状态

使用以下程序解决配置状态为“未同步”的设备：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**Note** 对于 本地防火墙管理中心，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 并选择处于**未同步 (Not Synced)** 状态的 FMC，然后从步骤 5 继续操作。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择报告为“未同步”的设备。

**步骤 5** 在右侧的未同步面板中，选择以下任一选项：

- **预览并部署...** - 如果要将配置更改从 CDO 推送到设备，请预览并部署您现在所做的更改，或者等待并一次部署多个更改。预览和部署所有设备的配置更改, on page 313
- 放弃更改 - 如果您不想将配置更改从 CDO 推送到设备，或者您想要“撤消”您开始在 CDO 上进行的配置更改。此选项使用设备上存储的运行配置覆盖 CDO 中存储的配置。

第 10 章

# 常见问题和支持

本章包含以下各节：



# 思科 Defense Orchestrator

**什么是 Cisco Defense Orchestrator**?

Cisco Defense Orchestrator (CDO) 是一种基于云的多设备管理器，允许网络管理员跨各种安全设备创建和维护一致的安全策略。

您可以使用 CDO 管理以下设备：

- Cisco Secure Firewall ASA
- Cisco 安全防火墙威胁防御
- 思科资安防护伞
- Meraki
- 思科 IOS 设备
- Amazon Web 服务 (AWS) 实例
- 使用 SSH 连接管理的设备

CDO 管理员可以通过一个界面监控和维护所有这些设备类型。

# 有关将设备载入到思科 Defense Orchestrator 的常见问题解答

## 关于 CDO 载入的常见问题Secure Firewall ASA

### 如何使用凭证载入？ASA

您可以一次载入一个或批量载入 ASA 设备。载入属于高可用性对的 ASA 时，请使用载入 ASA 设备 (Onboard an ASA Device) 仅载入该对的主设备。载入安全情景或管理情景的方法与载入任何其他 ASA 的方法相同。

### 如何一次载入多个设备？ASA

您可以使用 CSV 文件创建一个 ASA 列表，CDO 将载入列表中的所有 ASA。有关如何批量载入 ASA 的说明，请参阅批量载入 ASA。

### 载入 后应该怎么做？ASA

有关入门，请参阅使用思科防御协调器管理 ASA。

## 关于将 FDM 管理的设备载入的常见问题 CDO

### 如何载入 FDM 管理的设备？

有多种方法可以载入 FDM 管理的设备。我们建议使用注册密钥方法。请参阅载入 FDM 管理的设备以开始使用。

## 关于将安全防火墙威胁防御载入的常见问题 云交付的防火墙管理中心

### 如何载入 Cisco Secure Firewall Threat Defense？

您可以使用 CLI 注册密钥、通过低接触调配或使用序列号载入 FTD 设备。

### 在注册 Cisco Secure Firewall Threat Defense 后应该怎么做？

在设备同步后，导航至“工具和服务”(Tools & Services)>“防火墙管理中心”(Firewall Management Center)，然后从“操作”(Actions)、“管理”(Management) 或“设置”(Settings) 窗格中选择一个操作，以开始在云交付的防火墙管理中心中配置威胁防御设备。请参阅云交付的防火墙管理中心应用页面以开始。

### 如何对 Cisco Secure Firewall Threat Defense 进行故障排除？

请参阅对载入 Cisco Secure Firewall Threat Defense 进行故障排除。

# 关于本地 Cisco Secure Firewall Management Center 的常见问题

### 如何载入本地管理中心？

您可以将本地管理中心载入 CDO。载入本地管理中心也会将注册到本地管理中心的所有设备载入。CDO 不支持创建或修改与本地管理中心或注册到本地管理中心的设备关联的对象或策略。您必须在本地管理中心 UI 中进行这些更改。请参阅载入本地管理中心以开始使用。

# 有关将 Meraki 设备载入的常见问题解答 CDO

### 如何载入 Meraki 设备？

MX 设备既可由 CDO 管理，也可由 Meraki 控制面板管理。CDO 将配置更改部署到 Meraki 控制面板，后者又将配置安全地部署到设备。请参阅载入 Meraki MX 设备以开始使用。

# 有关载入 SSH 设备的常见问题解答 CDO

### 如何载入 SSH 设备？

您可以使用 SSH 设备上存储的高权限用户的用户名和密码，通过安全设备连接器 (SDC) 载入设备。请参阅载入 SSH 设备以开始使用。

### 如何删除设备？

您可以从清单页面中删除设备。

# 关于载入 IOS 设备的常见问题解答 CDO

### 如何载入思科 IOS 设备？

您可以使用安全设备连接器 (SDC) 载入运行思科 IOS（互联网操作系统）的实时思科设备。请参阅载入思科 IOS 设备以开始使用。

### 如何删除设备？

您可以从“清单”(Inventory) 页面删除设备。

# 设备类型

### 什么是自适应安全设备 (ASA)？

思科 ASA 在一台设备以及带附加模块的集成服务中提供高级状态防火墙和 VPN 集中器功能。ASA 包括许多高级功能，例如多安全情景（类似于虚拟化防火墙）、集群（将多个防火墙组合成一个防火墙）、透明（第 2 层）防火墙或路由（第 3 层）防火墙操作、高级检测引擎、IPsec VPN、SSL VPN 和无客户端 SSL VPN 支持以及许多其他功能。ASA 可以安装在虚拟机或受支持的硬件上。

### 什么是 ASA 型号？

ASA 型号是已载入 CDO 的 ASA 设备的运行配置文件的副本。您可以使用 ASA 模型分析 ASA 设备的配置，而无需载入设备。

### 设备何时同步？

当 CDO 上的配置和设备本地存储的配置相同时。

### 何时设备未同步？

如果 CDO 中存储的配置已更改，现在存储在设备上的配置有所不同。

### 设备何时处于“检测到冲突”状态？

设备上的配置在 CDO 外部（带外）更改，现在与 CDO 上存储的配置不同。

### 什么是带外更改？

在对 CDO 外部设备进行了更改时。使用 CLI 命令或使用设备上的管理器（例如 ASDM 或 FDM）直接在设备上进行更改。带外更改会导致 CDO 报告设备的“检测到冲突”状态。

### 将更改部署到设备意味着什么？

将设备载入 CDO 后，CDO 会维护其配置的副本。当您对 CDO 进行更改时，CDO 会对其设备配置的副本进行更改。当您将该更改“部署”回设备时，CDO 会将您所做的更改复制到设备的配置副本。请参阅以下主题：

- 预览和部署所有设备的配置更改, on page 313
- 将配置更改从 CDO 部署到 ASA

### 当前支持哪些 ASA 命令？

所有命令。点击设备操作下的**命令行界面**链接以使用 ASA CLI。

### 设备管理是否有任何规模限制？

CDO 的云架构使其能够扩展到数千台设备。

### CDO 会管理思科集成多业务和汇聚多业务路由器吗？

CDO 允许您为 ISR 和 ASR 创建模型设备并导入其配置。然后，您可以根据导入的配置创建模板，并将配置导出为可部署到新的或现有的 ISR 和 ASR 设备的标准化配置，以实现一致的安全性。

### CDO 能否管理 SMA？

否，CDO 当前不管理 SMA。

# 安全

### CDO 安全吗？

CDO 通过以下功能为客户数据提供端到端安全：

- 新 CDO 租户的初始登录, on page 3
- API 和数据库操作的身份验证调用
- 传输中和静态数据隔离
- 角色分离

CDO 需要对用户进行多因素身份验证才能连接到其云门户。多因素身份验证是保护客户身份所需的重要功能。

传输中和静态的所有数据均已加密。来自客户端和 CDO 设备的通信使用 SSL 进行加密，并且所有客户-租户数据量都已加密。

CDO 的多租户架构可隔离租户数据并加密数据库与应用服务器之间的流量。当用户进行身份验证以获得对 CDO 的访问权限时，他们会收到一个令牌。此令牌用于从密钥管理服务获取密钥，该密钥用于加密到数据库的流量。

CDO 快速为客户创造价值，同时确保客户凭证的安全。这是通过在云或客户自己的网络（路线图）中部署“安全数据连接器”来实现的，该网络控制所有入站和出站流量，以确保凭证数据不会离开客户场所。

### 第一次登录 CDO 时收到错误“无法验证您的 OTP”

检查您的桌面或移动设备时钟是否与世界时间服务器同步。时钟不同步的时间少于或超过一分钟可能会导致生成不正确的 OTP。

### 我的设备是否直接连接到思科 Defense Orchestrator 云平台？

是。使用 CDO SDC 执行安全连接，该 CDO SDC 用作设备和 CDO 平台之间的代理。CDO 架构在设计时考虑到了安全性，可以完全分离到设备的数据来回传输。

### 如何连接没有公共 IP 地址的设备？

您可以利用 CDO 安全设备连接器 (SDC)，该连接器可部署在您的网络内，无需打开任何外部端口。安全设备连接器, on page 8部署 SDC 后，您可以使用内部（非互联网路由）IP 地址载入设备。

### SDC 是否需要任何额外费用或许可证？

否。

### 如何检查隧道状态？状态选项

CDO 每小时自动执行一次隧道连接检查，但可以通过选择隧道并请求检查连接来执行临时 VPN 隧道连接检查。处理结果可能需要几秒钟。

### 是否可以根据设备名称及其对等体之一的 IP 地址搜索隧道？

是。使用名称和对等体 IP 地址上的可用过滤器和搜索功能，搜索并转至特定 VPN 隧道的详细信息。

# 故障排除

### 在从 CDO 到受管设备执行设备配置的完整部署时，我收到一条警告“无法将更改部署到设备”。我该怎么做才能解决这个问题？

如果在将完整配置（在 CDO 支持的命令之外执行的更改）部署到设备时发生错误，请点击“检查更改”以从设备提取最新的可用配置。这可能会解决问题，您将能够继续对 CDO 进行更改并进行部署。如果问题仍然存在，请从“联系支持”页面联系思科 TAC。

### 在解决带外问题（在 CDO 外部执行的更改；直接对设备进行更改）时，将 CDO 中的配置与设备的配置进行比较，CDO 会显示我未添加或修改的其他元数据。为什么会出现这种情况？

随着 CDO 扩展其功能，将从设备的配置中收集其他信息，以丰富和维护所有所需的数据，以便更好地进行策略和设备管理分析。这些不是在受管设备上发生的更改，而是已经存在的信息。通过检查设备中的更改并查看发生的更改，可以轻松解决检测到的冲突状态。

### 为什么 CDO 会拒绝我的证书？

请参阅新证书问题故障排除

# 低接触调配中使用的术语和定义

- **已申领 (Claimed)** - 用于在 CDO 中载入序列号的情景。如果设备的序列号已载入 CDO 租户，则该设备为“已申领”。
- **暂留 (Parked)** - 用于在 CDO 中载入序列号的情景。如果设备已连接到思科云，并且 CDO 租户未申领其序列号，则该设备为“暂留”。

- **初始调配 (Initial provisioning)** - 用于初始 FTD 设置的情景。在此阶段期间，设备会接受 EULA，创建新密码，配置管理 IP 地址，设置 FQDN，设置 DNS 服务器，并选择使用 FDM 在本地管理设备。
- **低接触调配 (Low-touch provisioning)** - 将 FTD 从工厂运送到客户现场（通常是分支机构），现场的员工将 FTD 连接到其网络，然后设备与思科云联系。此时，如果设备的序列号已被“申领”，则设备会被载入 CDO 租户，否则 FTD 会在思科云中“暂留”，直到 CDO 租户申领。
- **序列号载入 (Serial number onboarding)** - 这是使用已配置（安装和设置）的序列号载入 FTD 的过程。

# 策略优化

### 当两个或多个访问列表（在同一访问组内）相互重叠时，如何识别情况？

Cisco Defense Orchestrator 网络策略管理 (NPM) 能够识别并提醒用户，如果在规则集中，某个顺序更高的规则正在重影其他规则。用户可以在所有网络策略之间导航，也可以过滤以识别所有影子问题。有关详细信息，请参阅管理传统 ASA 访问策略。

**Note** CDO 仅支持完全镜像的规则。

# 连接

### 安全设备连接器已更改 IP 地址，但这未反映在 CDO 中。如何反映更改？

要在 CDO 中获取和更新新的安全设备连接器 (SDC)，您需要使用以下命令重新启动容器：

```
 Stop Docker deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$ ./cdo/toolkit/toolkit.sh restartSDC
 <tenant-name>
```

### 如果 CDO 用于管理我的设备（ FTD 或 ASA）的 IP 地址发生更改，会发生什么情况？

如果设备的 IP 地址因任何原因发生更改，无论是静态 IP 地址更改还是 DHCP 导致的 IP 地址更改，您都可以更改 CDO 用于连接到设备的 IP 地址（请参阅在 CDO 中更改设备的 IP 地址, on page 72）然后重新连接设备（请参阅将设备批量重新连接到 CDO, on page 77）。重新连接设备时，系统会要求您输入设备的新 IP 地址，并重新输入身份验证凭证。

### 将 ASA 连接到 CDO 需要什么网络？

- 已为 ASA 启用并启用 ASDM 映像。
- 对 52.25.109.29、52.34.234.2、52.36.70.147 的公共接口访问

- ASA 的 HTTPS 端口必须设置为 443 或 1024 或更高的值。例如，不能将其设置为端口 636。
- 如果管理的 ASA 也配置为接受 AnyConnect VPN 客户端连接，则必须将 ASA HTTPS 服务器端口更改为 1024 或更高的值。

# 关于数据接口

您可以使用专用的管理接口或常规数据接口与设备通信。如果想要从外部接口远程管理 FTD，或者您没有单独的管理网络，则在数据接口上进行CDO访问非常有用。CDO支持从数据接口远程管理的 FTD 上的高可用性。

从数据接口进行 FTD 管理访问具有以下限制：

- 只能在一个物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 FTD 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用CDO启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。

# CDO 如何处理个人信息

要了解 Cisco Defense Orchestrator 如何处理您的个人身份信息，请参阅《思科防御协调器隐私数据表》。

# 联系思科威胁防御支持

本章涵盖以下部分：

## 导出工作流程

我们强烈建议在提交支持请求之前导出遇到问题的设备的工作流程。此附加信息可帮助支持团队快速识别并纠正任何故障排除工作。

使用以下程序导出工作流程：

**步骤 1** 在导航栏中，点击**设备和服务 (Devices & Service)**。

**步骤 2** 点击 **设备** 选项卡，找到您的设备。

**步骤 3** 点击相应的设备类型选项卡，然后选择需要进行故障排除的设备。

使用过滤器或搜索栏查找需要进行故障排除的设备。选择设备以便将其突出显示。

**步骤 4** 在设备操作窗格中，选择工作流程。

**步骤 5** 点击页面右上角、事件表上方的**导出 (Export)** 按钮。该文件在本地自动保存为 .json 文件。将此附加到您使用 TAC 打开的任何邮件或故障单。

# 通过 TAC 打开提交支持请求

使用 30 天试用版或许可 CDO 账户的客户可以向思科技术支持中心 (TAC) 提交支持请求。

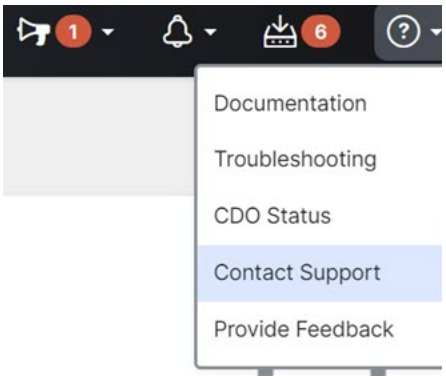
- CDO 客户如何通过 TAC 提交支持请求。
- CDO 试用客户如何向 TAC 提交支持请求。CDO 试用客户如何向 TAC 提交支持请求，第 537 页

## CDO 客户如何通过 TAC 提交支持请求

本节介绍使用许可 CDO 租户的客户如何向思科技术支持中心 (TAC) 提交支持请求。

**步骤 1** 登录 CDO。

**步骤 2** 点击租户名称旁边的帮助按钮，然后选择**联系支持 (Contact Support)**。




**步骤 3** 点击**支持请求管理器 (Support Case Manager)**。

**步骤 4** 点击**打开新案例 (Open New Case)** 按钮。

**步骤 5** 点击**创建支持案例 (Open Case)**。

**步骤 6** 选择**产品和服务 (Products and Services)**，然后点击**提交支持案例 (Open Case)**。

**步骤 7** 选择**请求类型 (Request Type)**。

**步骤 8** 展开**按服务协议查找产品 (Find Product by Service Agreement)** 行。

**步骤 9** 填写所有字段。许多字段是显而易见的。这是一些额外信息：

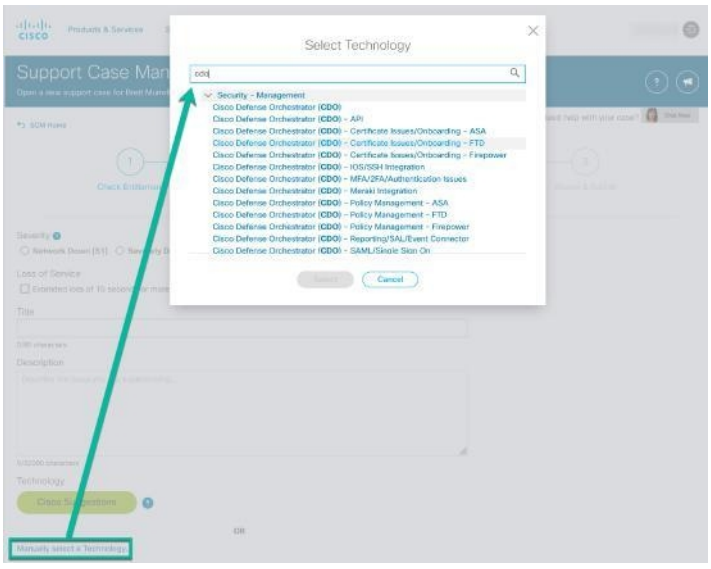
- **产品名称 (PID) (Product Name [PID])** - 如果您没有此编号，请参阅思科防御协调器产品手册。
- **产品说明 (Product Description)** - 这是 PID 的说明。
- **站点名称 (Site Name)** - 输入站点名称。如果您是为某个客户创建案例的思科合作伙伴，请输入该客户的姓名。
- **服务合同 (Service Contract)** - 输入服务合同号。
  - **重要提示：**为了使您的案例与您的 Cisco.com 账户相关联，您需要将您的合同编号与您的 Cisco.com 配置文件相关联。使用此程序将您的合同编号关联到您的 Cisco.com 配置文件。
    a. 打开至思科配置文件管理器 (Cisco Profile Manager)。
    b. 点击**访问管理 (Access Management)** 选项卡。
    c. 点击**添加访问 (Add Access)**。
    d. 选择 **TAC 和 RMA 支持请求提交、软件下载、支持工具和 Cisco.com** 上的授权内容，点击**跳转 (Go)**。
    e. 在提供的空白处输入服务合同编号，然后点击**提交 (Submit)**。您将通过邮件收到服务合同关联已完成的通知。完成服务合同关联最多可能需要 6 小时。

**Important** 重要提示：如果您无法访问以下任何链接，请联系您的思科授权合作伙伴或经销商、您的思科客户代表或您公司中负责管理思科服务协议信息的人员。

**步骤 10** 点击**下一步**。

**步骤 11** 在**描述问题 (Describe Problem)** 屏幕中，向下滚动到**手动选择技术 (Manually select a Technology)**，点击该技术，然后在搜索字段中键入 **CDO**。

**步骤 12** 选择最符合您的请求的类别，然后点击**选择 (Select)**。



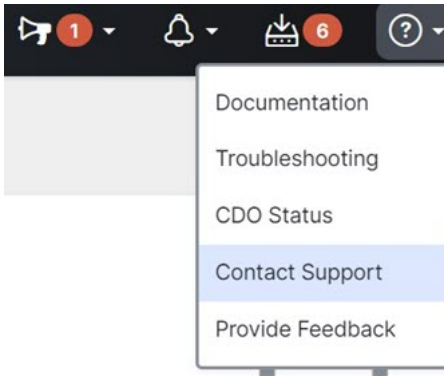
**步骤 13** 完成服务请求的其余部分，然后点击**提交 (Submit)**。

## CDO 试用客户如何向 TAC 提交支持请求

本节介绍使用 CDO 租户免费试用的客户如何向思科技术支持中心 (TAC) 提交支持请求。

**步骤 1** 登录 CDO。

**步骤 2** 点击租户和账户名称旁边的帮助按钮，然后选择**联系支持 (Contact Support)**。




**步骤 3** 在下方输入问题或请求字段中，指定您面临的问题或请求，然后点击提交。

您的请求以及技术信息将发送给支持团队，技术支持工程师将回复您的查询。

# CDO 服务状态页面

CDO 维护着一个面向客户的服务状态页面，该页面显示 CDO 服务是否已启动以及它可能遇到的任何服务中断。您可以使用每日、每周或每月图表查看正常运行时间信息。

您可以通过点击 CDO 中任何页面上的帮助菜单中的 CDO 状态来访问 CDO 状态页面。

在状态页面上，您可以点击订用更新，以便在 CDO 服务关闭时收到通知。

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。