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
- 将配置更改从防御协调器部署到 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
- 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？

请参阅解析新证书

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，请参阅网络策略管理。

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）然后重新连接设备（请参阅将设备批量重新连接到 CDO）。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。

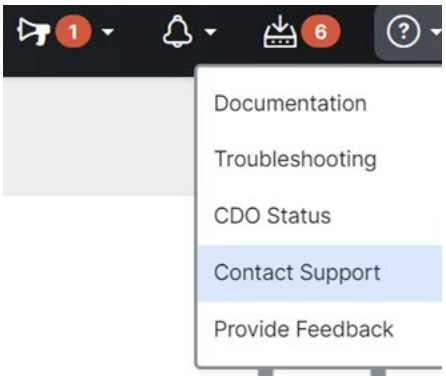
- CDO 客户如何通过 TAC 提交支持请求。
- CDO 试用客户如何向 TAC 提交支持请求。CDO 试用客户如何向 TAC 提交支持请求，第 11 页

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：

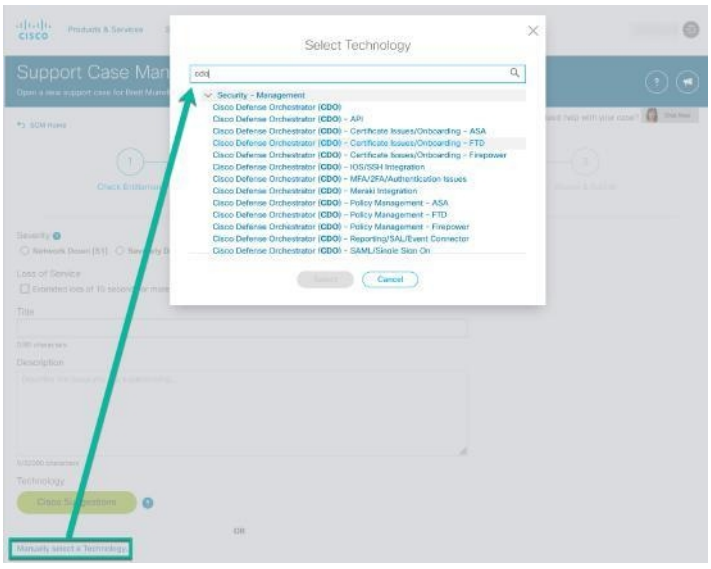
- **产品名称 (PID) (Product Name [PID])** - 如果您没有此编号，请参阅思科防御协调器产品手册。
- **产品说明 (Product Description)** - 这是 PID 的说明。
- **站点名称 (Site Name)** - 输入站点名称。如果您是为某个客户创建案例的思科合作伙伴，请输入该客户的姓名。
- **服务合同 (Service Contract)** - 输入服务合同号。
  - **重要提示：**为了使您的案例与您的 Cisco.com 账户相关联，您需要将您的合同编号与您的 Cisco.com 配置文件相关联。使用此程序将您的合同编号关联到您的 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)**。



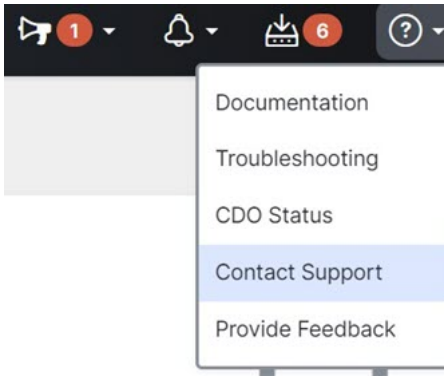
步骤 13 完成服务请求的其余部分，然后点击**提交 (Submit)**。

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。