



# 将 Cisco Secure Firewall Threat Defense 迁移到云

- [将 Secure Firewall Threat Defense 从 Cisco Secure Firewall Management Center 迁移到云](#)，第 1 页
- [迁移程序](#)，第 8 页
- [查看 威胁防御 迁移作业](#)，第 11 页
- [对 FTD 迁移到云进行故障排除](#)，第 15 页

## 将 Secure Firewall Threat Defense 从 Cisco Secure Firewall Management Center 迁移到云

思科防御协调器 允许具有 CDO 管理员权限的用户将 威胁防御 设备从 管理中心 迁移到云。

在威胁防御设备上启动迁移过程之前，与这些设备关联的 管理中心 必须已经被载入到 CDO。

在将 威胁防御 迁移到云时，CDO 会载入设备并将所有共享策略和关联对象、设备特定策略以及设备配置从 管理中心 导入至 CDO。



**注释** CDO 会处理 管理中心 迁移过程中识别的所有重复策略和对象名称。本文档的后续部分将详细介绍此行为。

事件和分析管理可以转移到 CDO 或保留在管理中心上。

在执行迁移后，您有 14 天的时间来评估更改。评估期允许您修改或更改特定操作，或者将这些设备的管理更改回管理中心。在评估期之后，您将无法恢复任何更改。

## 支持的软件

本节介绍迁移的最低软件要求：

- 管理中心: 7.2

- Secure Firewall Threat Defense:

- 7.0.3 或更高版本
- 7.2 或更高版本



---

注释 运行软件版本 7.1 的 威胁防御 上未提供此支持。

---

## 许可

- 当 威胁防御 被迁移到云后，与设备关联的所有功能许可证都将转移到 CDO，并从管理中心 释放到智能许可证池。设备会在向 CDO 注册期间收回设备特定的许可证。您无需再次在设备上申请许可证。
- 如果要将设备保留在 管理中心 中以进行分析，则不需要设备特定许可证。
- 确保您已使用智能许可证注册 云交付的防火墙管理中心。

## 支持的功能

### 处理共享策略和对象

在迁移过程开始时，首先导入与 威胁防御 设备关联的共享策略和关联对象，然后导入设备配置。

更改 威胁防御 设备上的管理器后，将以下共享策略导入 CDO:

- 访问控制
- IPS
- SSL
- 预过滤器
- NAT
- QoS
- 身份
- 平台设置
- Flex config
- 网络分析
- DNS
- 恶意软件和文件

- 运行状况
- 远程接入 VPN

如果 CDO 中的策略或对象与从 Cisco Secure Firewall Management Center 导入的策略或对象同名，则 CDO 会在成功更改管理后执行以下操作。

策略、对象	条件	操作
访问控制、SSL、IPS、预过滤器、NAT、QoS、身份、平台设置、网络分析、DNS、恶意软件和文件策略。	云交付的防火墙管理中心策略的名称与管理中心策略匹配。	使用云交付的防火墙管理中心策略而不是从管理中心导入的策略。
RA VPN 默认组策略 <b>DfltGrpPolicy</b>	管理中心中的默认组策略 <b>DfltGrpPolicy</b> 将被忽略。	改为使用现有的云交付的防火墙管理中心默认组策略 <b>DfltGrpPolicy</b> 。
网络、端口对象	云交付的防火墙管理中心中的网络和端口对象的名称和内容与管理中心中的匹配。	使用具有相同名称和内容的现有云交付的防火墙管理中心网络和端口对象，而不是从管理中心导入的对象。  如果对象具有相同的名称但内容不同，则会创建对象覆盖。请参阅 <a href="#">对象覆盖</a> 。
所有其他对象		使用现有云交付的防火墙管理中心对象，而不是从管理中心导入的对象。

与访问控制策略关联的任何系统日志警报对象都会被导入思科防御协调器。

### 高可用性对中的威胁防御迁移支持

您可以迁移高可用性对中的设备。主用和备用设备的设备管理会被更改并导入到 CDO 中。



**重要事项** 强烈建议在执行任何高级操作之前提交管理器更改，例如在正在迁移的设备上创建 HA 配置或中断 HA。

不支持在评估期间执行此类操作，否则可能会导致意外行为。

### 高可用性对中的管理中心迁移支持

您可以将威胁防御设备从配置了高可用性的管理中心迁移到云。

管理中心可以使用 SecureX 或凭证通过 SDC 方法载入。始终载入主用管理中心，而不是备用管理中心。



**注释** 如果您已载入独立管理中心，而稍后又将其配置为备用管理中心，请删除该备用管理中心并载入主用管理中心。

#### 要点回顾：

- **SecureX 载入方法**
  - 在 14 天评估期内，不支持高可用性中断。您可以在评估期后手动或自动提交更改后中断高可用性。
  - 在 14 天评估期内，支持高可用性切换。
- **使用 SDC 的凭证载入方法**
  - 在 14 天评估期内，不支持高可用性中断或高可用性切换。您可以在手动提交更改后执行这些操作，也可以在评估期后自动提交。
  - 在切换后，载入之前处于备用模式的新主用设备，然后在设备上启动迁移作业。

## 不支持的功能

在以下情况下，将 FTD 迁移到云 屏幕不允许将设备迁移到云：

- 集群的设备部分。
- 向 管理中心 注册的仅用于分析的设备。

以下配置不会作为迁移的一部分从 管理中心 导入到 CDO：

- 自定义构件、应用检测器、关联、SNMP 和邮件警报、扫描程序、组、动态访问策略、自定义 AMP 配置、用户、域、计划的部署任务、ISE 配置、计划的 GeoDB 更新、威胁智能导向器配置、动态分析连接。
- ISE 内部证书对象不会作为迁移的一部分导入。您必须从 ISE 导出新的系统证书或某个证书及其关联的专用密钥并将其导入 CDO。

### Cisco Secure Firewall 推荐规则

将 威胁防御 迁移到云会导入与入侵策略关联的 Cisco Secure Firewall IPS 建议的规则。但是，当执行刷新计划程序时，云交付的防火墙管理中心 不会在迁移后自动更新这些规则。请参阅[思科自动推荐的规则](#)。

### 自定义网络分析

如果设备与自定义网络分析策略相关联，则必须在迁移前从本地中删除对该策略的所有引用。

1. 登录本地 管理中心。

2. 选择策略 (Policies) > 访问控制 (Access Control)。
3. 点击要取消关联自定义 NAP 的访问控制策略上的编辑图标，然后点击高级 (Advanced) 选项卡。
4. 在网络分析和入侵策略 (Network Analysis and Intrusion Policies) 区域中，点击编辑图标。
5. 在默认网络分析策略 (Default Network Analysis Policy) 列表中，选择系统提供的策略。
6. 点击确定 (OK)。
7. 点击保存 (Save) 以保存更改，然后点击部署 (Deploy) 将更改下载到设备。

在迁移后，您可以在 CDO 中手动创建网络分析策略。

## VPN 配置的迁移准则和限制

在使用 VPN 配置迁移设备时，请记住以下几点：

### 远程访问 VPN 策略的迁移支持

作为迁移的一部分，CDO 会导入远程访问 VPN 策略的所有设置。

在迁移过程中，CDO 会导入远程访问 VPN 策略的所有设置，但以下设置除外：

- 不导入对象覆盖。

如果在地址池对象中使用了覆盖，则必须在迁移后使用 CDO 将其手动添加到导入的对象。请参阅[对象覆盖](#)。

- 不导入本地用户。

如果身份验证服务器配置为用于用户身份验证的本地数据库，则关联的本地领域对象将被导入 CDO。但是，您必须在迁移后使用 CDO 将本地用户手动添加到导入的本地领域对象。请参阅[创建领域和领域目录](#)。

- VPN 负载均衡配置不会迁移。
- 不导入具有域配置的 RA VPN 认证登记。

您可以在迁移后执行以下操作：

1. 在 CDO 中，点击清单 (Inventory) > FTD。
2. 选择迁移的 FTD，然后在右侧的设备管理 (Device Management) 中，点击设备概述 (Device Overview)。
3. 选择设备 (Devices) > 证书 (Certificates)。

执行下列操作之一：

- 如果在错误状态下导入证书，请点击刷新证书状态 (Refresh certificate status) 图标以将证书状态与设备同步。证书状态会变为绿色。
- 如果未导入证书，则必须手动添加在管理中心中配置的 RA VPN 策略中定义的证书。

## 用户角色

迁移后，管理中心的用户角色不再适用于 CDO。您执行任务的授权基于您在 CDO 中的用户角色。

CDO 用户角色	说明
CDO 管理员	超级管理员和管理员用户可以访问产品中的所有内容。此用户可以创建、读取、修改和删除策略和对象，并将其部署到设备。
CDO 仅部署	仅部署用户可以查看所有策略和对象。将暂存更改部署到一个或多个设备。
CDO 仅编辑	“仅编辑”用户可以修改并保存策略和对象，但不能将其部署到设备。
CDO 只读	“只读”用户可以查看所有策略和对象，但不能将其部署到设备。

## 管理威胁防御事件和分析

事件和分析管理可以保留在管理中心中，也可以转移到 CDO，其中设备必须配置为将事件发送到 CDO。在启动迁移过程时，您可以选择必须将设备事件发送到哪个管理器进行分析。

如果选择发送到管理中心进行分析，则 CDO 将成为所选设备的管理器，但会在管理中心上以仅分析模式保留这些设备的副本。设备会继续向管理中心发送事件，而 CDO 会管理配置更改。

如果选择发送到 CDO 进行分析，则 CDO 将成为所选设备的管理员，并会从管理中心中删除这些设备。CDO 会管理配置更改以及事件和分析管理。您必须配置威胁防御设备以将事件发送到思科云。您可以使用安全服务交换或安全事件连接器 (SEC) 将事件从设备发送到云中的 Cisco Secure 分析和日志记录 (SAL)。

## 启用通知设置

您可以订用电子邮件通知，以便在将威胁防御设备迁移到 CDO 时，当与您的租户关联的设备遇到特定操作时从 CDO 接收通知。

如果启用，则 CDO 会在将 FTD 迁移到云作业期间接收以下状态的通知：

- **失败 (Failed)**：迁移作业失败时。
- **已开始 (Started)**：启动迁移作业时。
- **成功 (Succeeded)**：迁移作业成功完成时。
- **提交待定 (Commit Pending)**：在提交管理器更改时。

要启用通知设置，请参阅[通知设置](#)。

## 通过云交付的防火墙管理中心验证威胁防御连接

本节提供用于确定威胁防御与云交付的防火墙管理中心的连接的命令。

### 检查设备上的互联网连接

执行 **ping system** *<any OpenDNS server address>* 命令以检查设备是否可以访问互联网。

1. 通过控制台端口或使用 SSH 连接至设备的 CLI。
2. 使用“管理员”(Admin) 用户名和密码登录。
3. 输入 **ping system** *<OpenDNS IPAddress>*。

```
ping system 208.67.222.222
PING 208.67.222.222 (208.67.222.222) 56(84) bytes of data.
64 bytes from 208.67.222.222: icmp_seq=1 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=2 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=3 ttl=48 time=22.8 ms
64 bytes from 208.67.222.222: icmp_seq=4 ttl=48 time=22.6 ms
^C
--- 208.67.222.222 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 22.588/22.841/22.995/0.223 ms
```

上面的示例显示了设备可以使用 OpenDNS 服务器 IP 地址连接到互联网。此外，传输的数据包数与接收的数据包数相同，表明设备上的互联网连接可用。这就表明设备可以访问互联网。



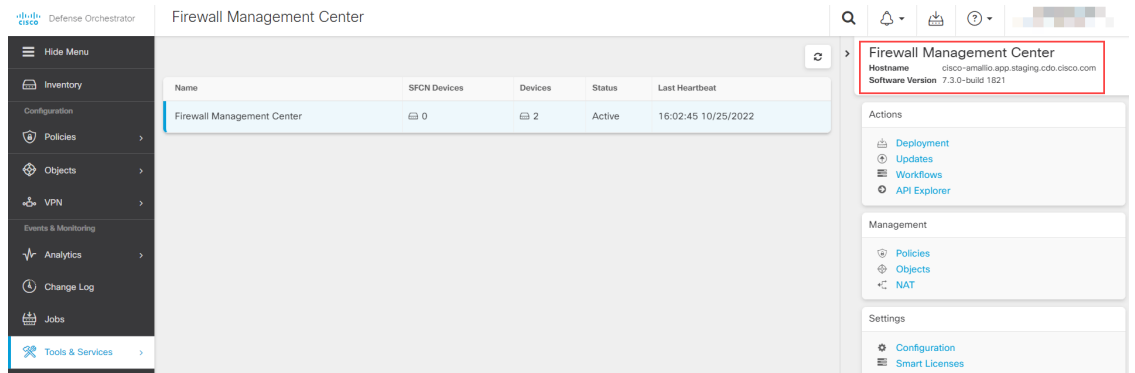
---

**注释** 如果结果不匹配，请手动检查互联网连接。

---

### 检查与云交付的防火墙管理中心的设备连接

1. 获取云交付的防火墙管理中心的主机名。
  1. 从 CDO 导航窗格中，点击工具和服务 (Tools & Services) > 防火墙管理中心 (Firewall Management Center)。
  2. 点击防火墙管理中心 (Firewall Management Center) 可在右侧窗格中查看详细信息。
  3. 在主机名 (Hostname) 字段中，仅复制以下图例中显示的主机名。



在上图中，突出显示的文本是要复制的 FMC 的主机名 (*cdo-acc10.app.us.cdo.cisco.com*)。

2. 通过控制台端口或使用 SSH 连接至设备的 CLI。
3. 输入 **ping system** *<hostname of the FMC>*。

```
ping system cdo-acc10.app.us.cdo.cisco.com
PING cdo-acc10.app.us.cdo.cisco.com (54.187.125.161) 56(84) bytes of data.
^C
--- cdo-acc10.app.us.cdo.cisco.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 64ms
```

在上面的示例中，主机名会使用 IP 地址来解析，表示连接成功。忽略响应中显示的“100% 丢包” (100% packet loss) 消息。



**注释** 如果无法连接到主机，您可以使用 **configure network dns** *<address>* 在 CLI 中纠正 DNS 配置。

## 迁移程序

### 开始之前

在开始此过程之前，请确保满足以下前提条件：

- 已调配的 CDO 租户。
- CDO 已使用智能许可证进行注册。
- 管理中心 已被载入到 CDO。载入 管理中心 还会载入注册到 管理中心 的所有 威胁防御 设备。请参阅[载入 FMC](#)。





**注释** 在管理中心中创建具有管理员角色的新用户或具有用于载入的“设备”和“系统”权限的自定义用户角色。



**注意** 如果您将本地管理中心载入 CDO 并同时使用相同的用户名登录本地管理中心，则载入会失败。


- 威胁防御设备必须同步，并且没有待处理的更改。如果 CDO 识别出该设备上有待处理的更改，则该设备上的迁移作业将失败。
- 管理中心应允许出站 HTTP/HTTPS 将配置上传到 Amazon S3。
- CDO 会从管理中心导入访问控制策略中使用的系统日志 (Syslog) 警报对象。如果 CDO 已包含名称相同但类型不同的警报对象 (SNMP、邮件)，则会在配置导入期间重复使用该对象。  
用户必须检查系统日志对象名称是否与 CDO 中的现有 SNMP 或邮件警报对象匹配。如果名称匹配，则您必须在本地管理中心中重命名系统日志对象，然后才能开始迁移过程。
- 如果您尝试将包含已修改的系统定义的 FlexConfig 文本对象的防火墙从本地管理中心迁移到云交付的防火墙管理中心，则修改后的系统定义的 FlexConfig 文本对象的值不会迁移到云交付的防火墙管理中心，并且部署将失败。

为避免这种情况，请在开始迁移之前执行以下任务：

- 在迁移之前，将修改后的系统定义的 FlexConfig 文本对象值从本地管理中心复制到云交付的防火墙管理中心。
- 在验证预定义的 FlexConfig 文本对象后，启动从本地管理中心到云交付的防火墙管理中心的迁移。

## 过程

**步骤 1** 在左侧的导航栏中，点击工具和服务 (Tools & Services) > 迁移 (Migrations) > 将 FTD 迁移到云。

**步骤 2** 点击  图标启动威胁防御迁移流程。

**注释** 一次只能启动一个迁移作业。

**步骤 3** 在选择本地 FMC (Select OnPrem FMC) 步骤中，执行以下操作：

1. 如果尚未完成，可以点击载入 FMC (Onboard an FMC) 链接以载入本地管理中心。请参阅[载入 FMC](#)。
2. 从可用列表中选择管理中心并点击下一步 (Next)。

在选择设备 (Select Devices) 步骤中，您将看到所选管理中心管理的威胁防御设备。

上次同步时间 (**Last Synced time**) 字段指明自设备配置同步到 管理中心 以来经过的时间。您可以点击立即从本地 **FMC 同步 (Sync from OnPrem FMC Now)** 以获取最新的设备更改。

**步骤 4** 在选择设备 (**Select Devices**) 步骤中，执行以下操作：

a) 选择要迁移的设备。

**Migrate FTD to Cloud**  
Migrate FTD Manager from Firewall Management Center to CDO

**1** Select OnPrem FMC      **OnPrem FMC: FMC\_OnPrem**

**2** Select Devices      Select FTD devices to migrate to cloud from OnPrem FMC to CDO and specify an action in bulk or per device.

1 device(s) selected      Multi-Device Action      Retain on OnPrem FMC for Analytics

Name	Domain	Action
FMC_OnPrem_192.168.0.31	Global	Retain on OnPrem FMC for Analytics
FMC_OnPrem_192.168.0.32	Global	Retain on OnPrem FMC for Analytics

Displaying 2 of 2 results

**Migrate FTD to Cloud**

注释

- 无法选择在不支持的版本上运行的设备。
- 只在管理中心注册分析的设备或具有待部署的更改的设备不符合迁移的条件。
- CDO 仅允许选择高可用性对中的主用设备。在成功更改主用设备的管理器后，CDO 会自动更改备用设备的管理器，并在设备上保留高可用性配置。

b) 在多设备操作 (**Multi-Device Action**) 列表中，您可以选择要应用于所有设备的通用操作。

c) 在提交操作 (**Commit Action**) 列中，您可以为所选设备选择以下操作之一：

- **保留在本地 FMC 以进行分析 (Retain on OnPrem FMC for Analytics)**：在迁移过程完成后，所选 威胁防御 设备的分析管理将保留在 管理中心 上。
- **从本地 FMC 删除 FTD (Delete FTD from OnPrem FMC)**：迁移过程完成后，所选设备将从 管理中心 中删除，并可供 CDO 用于处理分析。您必须配置设备，以便将事件发送至 CDO 进行管理分析。一旦将设备从 管理中心 中删除，它们就无法撤销。

注释      除非自动或手动提交更改，否则不会从 管理中心 中删除设备。

注释      此处指定的操作将在 14 天评估期后自动提交，或在手动提交更改后提交。

**步骤 5** 点击将 FTD 迁移到云 (Migrate FTD to Cloud)。


**步骤 6** 点击查看迁移到云的进度 (View Migration to Cloud Progress) 以查看作业的进度。

### 下一步做什么

您可以查看迁移作业的整体和个别状态，并在作业成功完成时生成报告。请参阅[查看威胁防御迁移作业，第 11 页](#)。

## 查看 威胁防御 迁移作业

您可以查看从 CDO 启动的所有迁移作业的状态。您可以展开作业以查看与 管理中心 关联的各个设备的状态。

如果您已启用通知设置设备工作流程的警报，请点击通知图标  以查看迁移期间发生的警报。如果您已订用从 CDO 接收邮件通知，您也会收到邮件通知。

迁移作业成功后，您有 14 天的时间使用 CDO 来评估您的设备。在此期间，您可以修改或更改特定操作，或者将这些设备的管理更改回 管理中心。

如果您确信迁移更改，我们建议手动提交设备。评估期到期后，CDO 会自动提交更改，而您无需执行进一步操作。提交操作会将更改应用于设备。请参阅[手动提交管理器变更，第 14 页](#)。

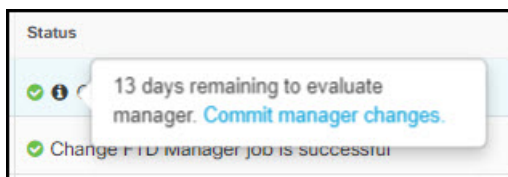
提交更改后，您将无法撤销在窗口中指定的操作。



**重要事项** 在评估期内，可以进行更改并使用 CDO 将其部署到使用的设备。如果您选择将设备管理恢复为 管理中心，则在恢复其管理器后，在评估期间进行的 CDO 特定更改将不会在设备上保留。在恢复设备管理器后，您必须将更改从本地 管理中心 部署到设备。

- **名称 (Name):** 表示作业名称，显示作业启动时的 管理中心 名称以及日期和时间。
- **FTD 数量 (Number of FTDs):** 这显示正在迁移到云的设备总数。
- **状态 (Status):** 显示作业的状态。展开作业以查看各个设备的状态。

作业成功完成后，**状态 (Status)** 列中会显示 **FTD 迁移作业成功 (FTD Migration job is successful)** 消息。您可以点击工具提示以查看评估管理器的剩余天数。



您可以点击[手动提交管理器变更](#)，在 14 天评估期结束之前手动提交更改。

- **上次更新 (Last Update):** 仅当设备发生更改时，才会更新日期和时间。

### • 操作 (Actions):

- **工作流程 (Workflows):** 提供一个链接，可将您定向到用于监控作业的工作流程页面。请参阅[工作流程页面](#)。
- **下载报告 (Download Report):** 允许您生成并下载成功完成的每个作业的报告。请参阅[生成威胁防御迁移报告](#)，第 14 页。
- **提交管理器更改 (Commit Manager Changes):** 允许您在评估期结束之前将更改手动应用到设备。请参阅[手动提交管理器变更](#)，第 14 页。
- **删除迁移作业 (Remove Migration Job):** 允许您删除已完成的作业。此链接仅适用于已完成的作业。

在成功迁移后，CDO 会将配置部署到设备。如果系统在要部署的更改中发现错误或警告，则会在 **验证消息 (Validation Messages)** 窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。如果部署失败，请参阅《[Firepower 管理中心配置指南 X.Y](#)》中的 [部署配置更改最佳实践部分](#)。



#### 重要事项

在 14 天的评估期内，您无法从 CDO 中删除设备或本地 FMC。执行以下操作之一，然后删除设备或本地 FMC:

- 执行与要删除的本地 FMC 或设备关联的[删除迁移作业](#)。
- 选择将管理器恢复至本地 FMC (**Revert Manager to OnPrem FMC**)并[手动提交管理器变更](#)。

### 为身份策略配置领域序列

如果设备包含具有领域或 ISE 配置的身份策略，请将设备配置为 CDO 的代理以便与身份源通信。如果 CDO 无法连接到身份领域，则身份策略将不起作用。

需要额外配置的设备的状态 (**Status**) 列中会显示工具提示。

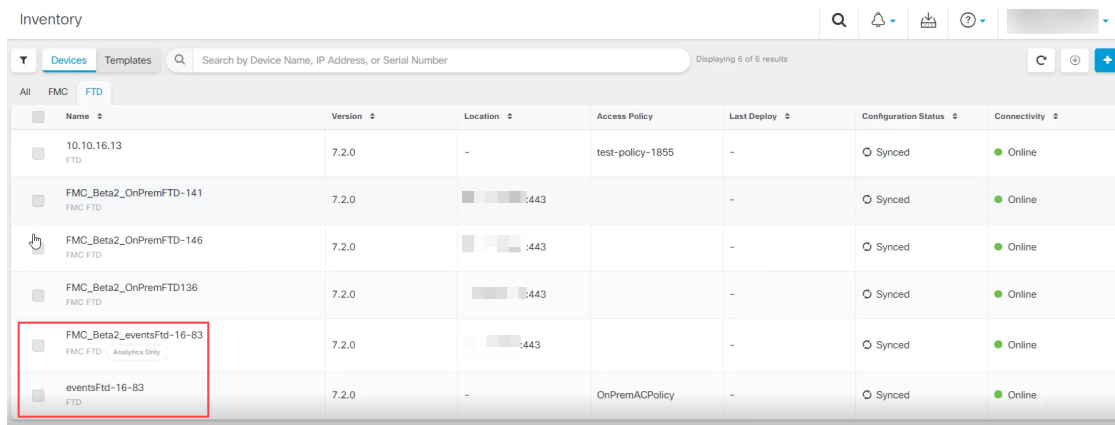


1. 点击工具提示图标，然后点击[了解更多 \(Learn more\)](#)。
2. 在配置代理 (**Configure Proxy**) 窗口中，点击[配置我的领域 \(Configure my realms\)](#)。

要添加代理序列，请参阅《[Firepower 管理中心设备配置指南, 7.2](#)》中的创建代理序列部分。

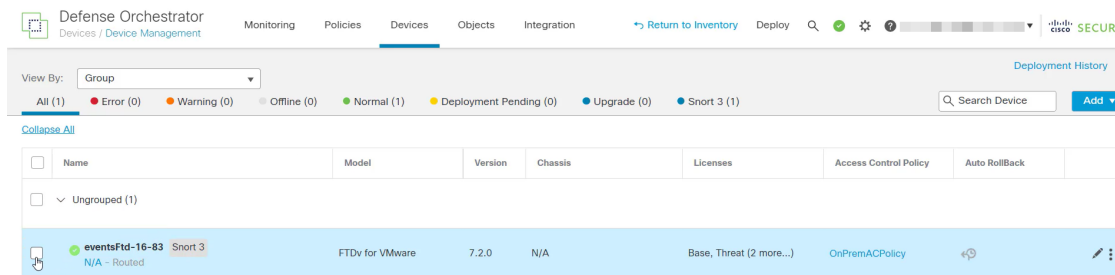
### 分析仅威胁防御设备示例

CDO 会创建同一个设备的两个实例，而该设备会被配置为保留在管理中心上进行分析。



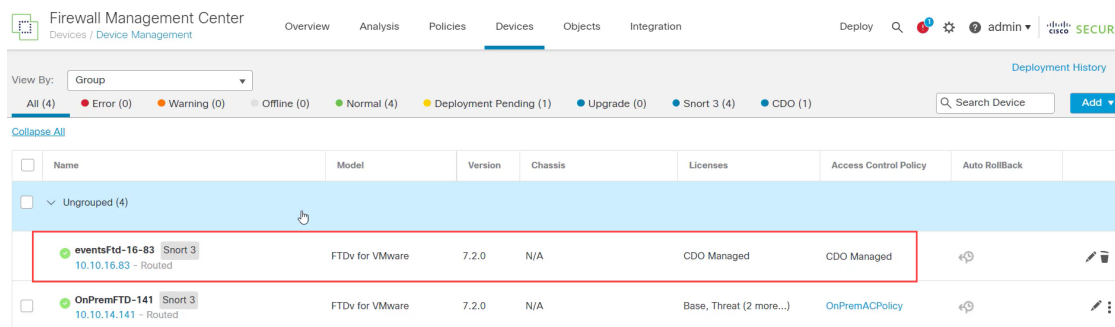
带有 **FMC FTD** 和仅分析 (**Analytics Only**) 标签的设备实例显示由管理中心处理分析。带有 **FTD** 标签的设备实例表示由 CDO 管理其配置。

您可以使用 CDO 来管理设备的配置。要查看云交付的防火墙管理中心中的设备，请执行以下操作：  
选择带有 **FTD** 标签的设备，然后在右侧的**管理 (Management)** 窗格中，点击**设备摘要 (Device Summary)**。



您可以在管理中心中查看设备中的事件。要查看事件，请执行以下操作：

1. 选择具有 **FMC FTD** 和仅分析 (**Analytics Only**) 标签的设备，然后点击右侧的**管理设备 (Manage Devices)** 链接。
2. 登录本地管理中心。
3. 点击**设备 (Device)** > **设备管理 (Device Management)**。




您无法选择此设备，因为 CDO 会管理配置。管理中心 会显示此设备的 **CDO 托管** 标签。

要查看管理中心中的实时事件，请点击 **分析 (Analysis) > 事件 (Events)**。

## 生成威胁防御迁移报告

在迁移作业成功后，您可以生成并下载 PDF 格式的报告，以分析从 CDO 管理中心导入的每个参数的值。该报告提供与作业关联的每个设备的详细信息。详细信息包括有关设备、共享策略值、对象、路由详细信息、接口、网络设置等的信息。

在迁移作业页面上，点击已完成作业的操作 (**Actions**) 列下的 ，然后点击 **下载报告 (Download Report)**。

## 手动提交管理器变更

如果您确信所做的更改正确无误，我们建议您手动提交管理器更改，而无需等待 CDO 自动提交更改。该窗口显示要恢复到作为设备管理器的管理中心或更改操作并将更改提交到 CDO 的剩余天数。在评估期间，您可以在确认更改之前更改所选威胁防御设备的指定操作。

更改一旦提交，您就无法撤销窗口中指定的操作。



**注释** 在以下情况时，提交管理器更改操作将被禁用：

- 已超出 14 天的评估期。
- 威胁防御 设备已被恢复或删除，在这种情况下，无法执行进一步操作。

### 过程

**步骤 1** 在迁移作业页面上，点击已完成作业的操作 (**Actions**) 列下的 。

**步骤 2** 点击 **提交管理器更改 (Commit Manager Changes)**。仅当作业成功完成时，此链接才可用。

**步骤 3** 如果要更改为设备指定的操作，请选择设备，然后在操作 (**Actions**) 列表中选择操作：

- **保留本地 FMC 以进行分析 (Retain on OnPrem FMC for Analytics)**：在提交更改后，所选威胁防御设备的分析管理将保留在管理中心。
- **从本地 FMC 删除 FTD (Delete FTD from OnPrem FMC)**：在提交更改后，所选设备将从管理中心删除，并可供 CDO 用于处理分析。您必须配置威胁防御，以便将事件发送至 CDO 进行管理分析。一旦将威胁防御从 管理中心 中删除，它们就无法撤销。
- **将管理器恢复为本地 FMC (Revert Manager to OnPrem FMC)**：在提交更改后，设备管理将从 CDO 返回到 管理中心。

- 注释
- 在提交此操作后，您无法再次将设备的管理更改为 CDO。  
**解决方法：**您必须从管理中心中删除设备并将其载入。然后，您可以在 CDO 中更改设备的管理。
  - 在提交此操作后，设备不会在管理中心中显示“过期”(Out-of-Date)状态。  
**解决方法：**在本地管理中心上部署对设备的更改。

**步骤 4** 点击**提交 (Commit)** 会立即执行指定的操作，而无需进一步确认。

**步骤 5** 在迁移作业屏幕上，您可以展开作业以查看指定操作的进度。


---

## 删除迁移作业

您可以删除迁移作业，结果取决于删除时间

- 在 14 天的评估期内：停止迁移，并将与迁移作业关联的设备的配置恢复为原始状态。
- 提交迁移更改后：从迁移作业列表中删除记录。

### 过程

**步骤 1** 在迁移作业页面上，点击**操作 (Actions)** 列下的 ，然后点击**删除迁移作业 (Remove Migration Job)**。

**步骤 2** 点击**删除 (Delete)** 以确认操作。

---

## 对 FTD 迁移到云进行故障排除

本节提供对将 FTD 迁移到云时可能发生的特定错误进行故障排除的信息。

在 **FMC** 响应中找到 **HTTP 状态代码 201**（已创建）

CDO 会在设备级别显示此错误。

**问题：**

安全设备连接器 (SDC) 版本不兼容。

Number of FTDs	Status
1 devices	❌ Change FTD Manager job failed
IP ADDRESS	STATUS
10.10.90.32	❌ Device Connectivity with CDO failed. (HTTP status code 201 (Created) found in FMC response.)

### 解决方法：

确保将 SDC 升级到“202205191350”或更高版本。

1. 导航至管理 (**Admin**) > 安全连接器 (**Secure Connectors**)。
2. 点击 SDC，在右侧的详细信息 (**Details**) 窗格中查看现有 SDC 版本。
3. [更新安全设备连接器](#)。

### 设备与 CDO 的连接失败

Name	Number of FTDs	Status	Last Updated	Actions
1771Fmc_change-management_2022-02-28-104213	2 devices	❌ Change FTD Manager job failed	Feb 28, 2022, 4:14:12 PM	...
DEVICE NAME	IP ADDRESS	STATUS	LAST UPDATED	
1771Fmc_10.10.16.84	10.10.16.84	❌ Device Connectivity with CDO failed	Feb 28, 2022, 4:12:53 PM	

设备由于以下原因之一而无法访问 CDO：

- 设备布线不正确。
- 您的网络可能要求提供设备的静态 IP 地址。
- 您的网络使用自定义 DNS，或者客户网络上存在外部 DNS 屏蔽。
- 需要进行 PPPoE 身份验证。
- 设备位于代理后面。

### 解决方法：

- 检查布线和网络连接。
- 确保您的防火墙未阻止任何流量。
- [通过云交付的防火墙管理中心验证威胁防御连接](#)。

### 未能将 CDO 配置为配置管理器

当 CDO 由于网络丢失而无法与设备通信时，它无法使用云提供的防火墙管理中心来执行 `configure manager` 命令。



Name	Number of FTDs	Status	Last Updated	Actions
1771Fmc_change-management_2022-03-04-055700	2 devices	Change FTD Manager job is in progress	Mar 4, 2022, 11:33:07 AM	...
DEVICE NAME	IP ADDRESS	STATUS	LAST UPDATED	
1771Fmc_10.10.16.86	10.10.16.86	Syncing	Mar 4, 2022, 11:29:03 AM	
1771Fmc_10.10.16.84	10.10.16.84	Failed to configure CDO as Configuration Manager	Mar 4, 2022, 11:28:16 AM	

**解决方法:**

1. 检查布线和网络连接。
2. 确保您的防火墙未阻止任何流量。
3. 确保 FTD 具有互联网连接，并且 DNS 地址已被解析为 IP 地址。请参阅[通过云交付的防火墙管理中心验证威胁防御连接](#)，第 7 页。
4. 在新的变更管理器作业中，重新尝试从 CDO 迁移此 FTD。

**变更管理器已存在或正在成为源管理器**

只有当上一个作业完成时，才能为本地管理中心创建 FTD 迁移作业。

如果上一个作业正在进行中，在创建新作业时会发生此错误。

**Migrate FTD to Cloud**  
Change FTD Manager from Firewall Management Center to CDO

**1** Select OnPrem FMC      **OnPrem FMC: fmc-beta2-18-3**

---

**2** Select Devices      **change ftd management already exists or in progress for source manager fmc-beta2-18-3**

Select FTD devices to migrate to cloud from OnPrem FMC to CDO and specify an action in bulk or per device.

1 device(s) selected      Multi-Device Action: Retain on OnPrem FMC for Analytics

Name	Domain	Action
fmc-beta2-18-3_10.10.16.20	Global	Retain on OnPrem FMC for Analytics
<input checked="" type="checkbox"/> fmc-beta2-18-3_10.10.16.25	Global	Retain on OnPrem FMC for Analytics
fmc-beta2-18-3_10.10.16.9	Global	Retain on OnPrem FMC for Analytics

Displaying 3 of 3 results

**Migrate FTD to Cloud**

---

**3** Finish

**解决方法:**

1. 导航到迁移表，以查看特定源本地管理中心是否正在进行其他作业。
2. 等待当前迁移作业完成。

3. 启动下一个迁移作业。

## 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。