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 (SDC)。

本章涵盖以下部分：

载入 威胁防御 设备

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

有多种方法可以载入 威胁防御 设备。我们建议使用注册密钥方法。

如果您在载入设备时遇到问题，请参阅对使用序列号载入 FDM 管理 设备进行故障排除或由于许可证不足而失败了解详细信息。

将 威胁防御 设备载入 云交付的防火墙管理中心

您可以将运行版本 7.2 及更高版本的 威胁防御 设备载入 云交付的防火墙管理中心。有关详细信息，请参阅将 FTD 载入云交付的防火墙管理中心。

通过序列号载入 威胁防御 设备

此程序是对运行受支持软件版本的 Firepower 1000、Firepower 2100 或 Secure Firewall 3100 系列物理设备进行载入的简化方法。要载入设备，您需要设备的机箱序列号或PCA序列号，并确保将设备添加到可以访问互联网的网络中。

您可以将新出厂的设备或已配置的设备载入 CDO。

有关详细信息，请参阅 使用设备的序列号载入 FDM 管理 设备, on page 19。

使用注册密钥载入 威胁防御 设备。

建议使用注册密钥来载入 威胁防御 设备。如果使用 DHCP 为您的设备分配 IP 地址，这将非常有用。如果该 IP 地址由于某种原因发生变化，则您的 威胁防御 设备将保持连接到 CDO（如果您已使用注册密钥载入设备）。

- 使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5, on page 11
- 使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+, on page 15

使用凭证载入 威胁防御 设备

您可以使用设备凭证和设备的外部、内部或管理接口的 IP 地址来载入 威胁防御 设备，具体取决于设备在网络中是如何配置的。要使用凭证载入设备，请参阅 使用用户名、密码和 IP 地址载入 FDM 管理 设备, on page 9。要使用接口地址来载入，请参阅本文后面的载入 威胁防御 设备。

CDO 需要通过 HTTPS 访问设备才能管理它。如何允许 HTTPS 访问设备要取决于您的设备在网络中是如何配置的，以及您是使用安全设备连接器还是云连接器来载入设备。

Note 如果您连接到 https://www.defenseorchestrator.eu 并且使用的软件版本 6.4，则必须使用此方法来载入 威胁防御 设备。您不能使用注册密钥方法。

使用设备凭证连接 CDO 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 和设备之间的通信。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。在使用凭证载入后，威胁防御 设备就可以使用 SDC 载入 CDO。

请注意，当使用 威胁防御 设备作为 VPN 连接的前端时，客户将无法使用外部接口来管理设备。

载入 威胁防御 集群

您可以在载入 CDO 之前载入已加入集群的 威胁防御 设备。集群允许您将多个防火墙 威胁防御 单元集合在一起，作为单个逻辑设备来提供全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

请参阅 载入集群的 设备, on page 32。

载入的 FDM 管理 设备配置和必备条件

FDM 管理 设备管理

您只能载入由 Firepower 设备管理器 (FDM) 管理的 威胁防御 设备。由 Firepower 管理中心 管理的 威胁防御 设备无法由 云交付的防火墙管理中心 管理。

如果设备未配置为本地管理，则必须在载入设备之前切换到本地管理。请参阅《适用于 Firepower 设备管理器的 配置指南》的 **在本地管理和远程管理之间切换**一章。

许可

设备**必须**至少安装一个许可证才能载入到 CDO，但在某些情况下可以应用智能许可证。

载入方法	Firepower 设备管理器 软件版本	90 天评估许可证是否允许？	在载入之前，设备是否可以先获得智能许可？	在载入之前，设备是否可以先在思科云服务中注册？
凭证（用户名和密码）	全部	是	是	是
注册密钥	6.4 或 6.5	是	不行。请取消注册智能许可证，然后载入设备。	不适用
注册密钥	6.6 或更高版本	是	是	不行。请从思科云服务取消注册设备，然后载入设备。
低接触调配	6.7 或更高版本	是	是	是
通过序列号载入设备	6.7 或更高版本	是	是	是

请参阅思科 FirePOWER 系统功能许可证。

设备编址

最佳实践是使用静态地址来载入 FDM 管理 设备。如果设备的 IP 地址由 DHCP 分配，则最好使用 DDNS（动态域名系统）在设备的新 IP 地址更改时自动使用设备的域名条目进行更新。

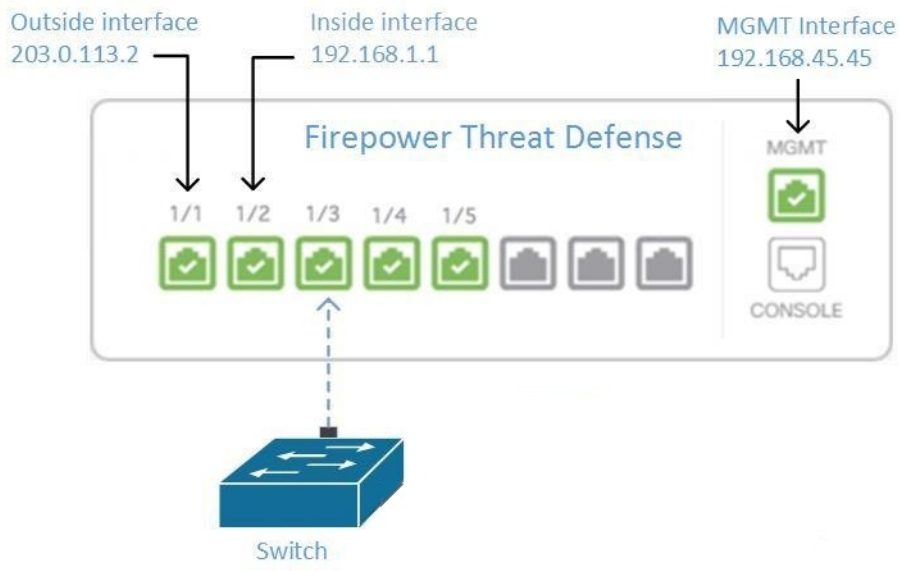
Note FDM 管理 设备本身不支持 DDNS；您必须配置自己的 DDNS。

Important 如果您的设备从 DHCP 服务器获取 IP 地址，并且您没有使用任何新 IP 地址更新 FDM 管理 设备域名条目的 DDNS 服务器，或者您的设备收到了新地址，您可以更改 CDO 为 维护的 IP 地址设备，然后再重新连接设备。更好的方法是使用注册密钥来载入设备。

从内部接口管理设备FDM 管理

如果为专用MGMT接口分配了在您的组织内不可路由的地址，则可能需要使用内部接口管理设备；例如，它可能只能从您的数据中心或实验中访问。FDM 管理

Figure 1: 接口地址



远程接入 VPN 要求

如果您使用 CDO 管理的设备将管理远程接入 VPN (RA VPN) 连接，则 CDO 必须使用内部接口管理设备。FDM 管理

后续操作：

继续，了解配置设备的程序。从内部接口管理设备FDM 管理FDM 管理

从内部接口管理设备FDM 管理

此配置方法：

- 假定设备尚未自行激活。FDM 管理CDO
- 将数据接口配置为内部接口。
- 配置内部接口以接收 MGMT 流量 (HTTPS)。
- 允许云连接器的地址到达设备的内部接口。

Before you begin

在以下主题中查看此配置的前提条件：

- 从内部接口管理设备FDM 管理
- 将 思科防御协调器 连接到托管设备

Procedure

步骤 1 登录Firepower 设备管理器。

步骤 2 在系统设置菜单中，点击管理访问。

步骤 3 点击数据接口选项卡，然后点击创建数据接口。

a. 在接口字段中，从接口列表中选择预先命名为“内部”的接口。

b. 在协议字段中，选择 HTTPS（如果尚未选择）。

c. 在允许的网络 (Allowed Networks) 字段中，选择代表将允许访问设备内部地址的组织内部网络的网络对象。FDM 管理SDC 或云连接器的 IP 地址应在允许访问设备内部地址的地址中。

在接口地址图中，SDC 的 IP 地址 192.168.1.10 应该能够到达 192.168.1.1。
managing-ftd-with-cisco-defense-orchestrator_chapter1.pdf#nameddest=unique_67 unique_67_Connect_42_ftd-interf-addrss

步骤 4 部署更改。您现在可以使用内部接口管理设备。

What to do next

如果您使用的是云连接器，该怎么办？

使用上述程序并添加以下步骤：

- 将外部接口 (203.0.113.2)“NAT”添加到内部接口 (192.168.1.1)。
- 在上述程序的步骤 3c 中，“允许的网络”是包含云连接器的公共 IP 地址的网络组对象。
- 添加创建访问控制规则的步骤，允许从云连接器的公共 IP 地址访问外部接口 (203.0.113.2)。

如果您是欧洲、中东或非洲 (EMEA) 的客户，并且连接到 ，则这些是云连接器的公共 IP 地址：
CDOhttps://defenseorchestrator.eu/

- 35.157.12.126
- 35.157.12.15

如果您是美国的客户，并且连接到，云连接器的这些公共 IP 地址：CDOhttps://defenseorchestrator.com/

- 52.34.234.2
- 52.36.70.147

如果您是**亚太地区-日本-中国 (AJPC)** 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

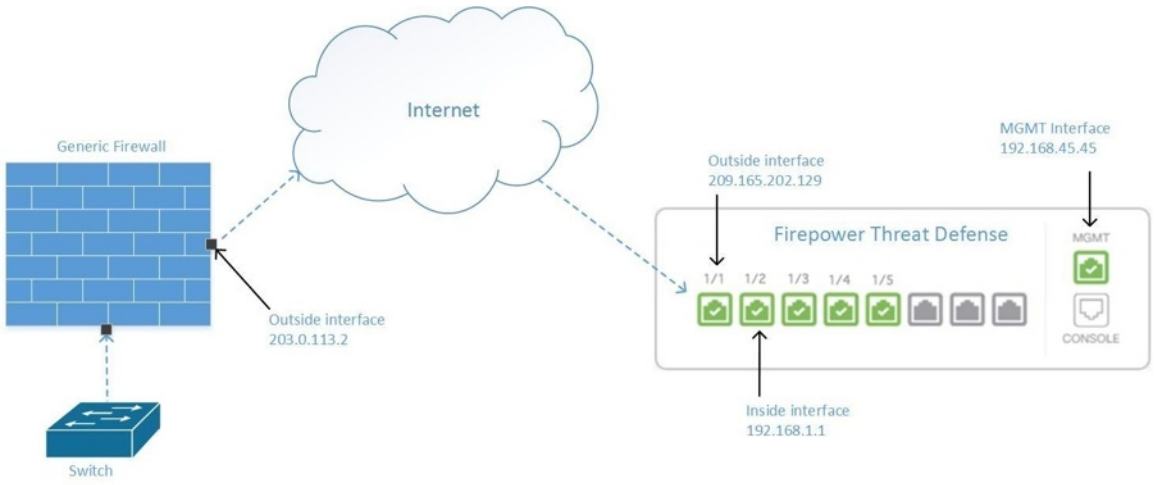
载入 FDM 管理 设备

推荐的自行激活设备的方法是使用注册令牌自行激活方法。FDM 管理CDO将内部接口配置为允许从云连接器对设备进行管理访问后，使用用户名和密码载入设备。FDM 管理FDM 管理有关详细信息，请参阅载入 威胁防御 设备。您将使用内部接口的 IP 地址进行连接。在上面的场景中，该地址是 192.168.1.1。

从外部接口管理设备FDM 管理

如果您有一个分配给分支机构的公共 IP 地址，并使用另一个位置的云连接器进行管理，则可能需要从外部接口管理设备。云交付的防火墙管理中心思科防御协调器

Figure 2: 外部接口上的设备管理



此配置并不意味着物理 MGMT 接口不再是设备的管理接口。如果您在设备所在的办公室，您将能够连接到 MGMT 接口的地址并直接管理设备。云交付的防火墙管理中心

远程接入 VPN 要求

如果您管理的设备将管理远程接入 VPN (RA VPN) 连接， 将无法使用外部接口管理设备。云交付的防火墙管理中心云交付的防火墙管理中心云交付的防火墙管理中心请参阅从内部接口管理设备。FDM 管理

后续操作：

继续，了解配置设备的程序。管理设备的外部接口FDM 管理云交付的防火墙管理中心

管理设备的外部接口FDM 管理

此配置方法：

1. 假定设备尚未自行激活。FDM 管理CDO
2. 将数据接口配置为外部接口。
3. 在外部接口上配置管理访问。
4. 允许云连接器的公共 IP 地址（通过防火墙进行 NAT 后）到达外部接口。

Before you begin

在以下主题中查看此配置的前提条件：

- 管理设备的外部接口FDM 管理
- 将 思科防御协调器 连接到托管设备

Procedure

步骤 1 登录Firepower 设备管理器。

步骤 2 在系统设置菜单中，点击管理访问。

步骤 3 点击数据接口选项卡，然后点击创建数据接口。

a. 在接口字段中，从接口列表中选择预先命名为“外部”的接口。

b. 在协议字段中，选择 HTTPS（如果尚未选择）。只需要 HTTPS 访问。CDO

c. 在允许的网络 (Allowed Networks) 字段中，创建一个主机网络对象，其中包含云连接器通过防火墙的 NAT 后面向公众的 IP 地址。

   在从外部接口进行设备管理的网络图中，云连接器的 IP 地址 10.10.10.55 将通过 NAT 转换为 203.0.113.2。managing-ftd-with-cisco-defense-orchestrator_chapter1.pdf#nameddest=unique_71 unique_71_Connect_42_ftd-mgmt-out-addrss对于允许的网络，您将创建一个值为 203.0.113.2 的主机网络对象。

步骤 4 在中创建访问控制策略，允许从SDC或云连接器的公共IP地址到设备外部接口的管理流量(HTTPS)。Firepower 设备管理器FDM 管理在此场景中，源地址为 203.0.113.2，源协议为 HTTPS；目的地址为 209.165.202.129，协议为 HTTPS。

步骤 5 部署更改。您现在可以使用外部接口管理设备。

What to do next

如果您使用的是云连接器，该怎么办？

该过程非常相似，但有两点不同：

- 在上述程序的步骤 3c 中，“允许的网络”是包含云连接器的公共 IP 地址的网络组对象。
  - 如果您是欧洲、中东或非洲(EMEA)的客户，并且连接到，则这些是云连接器的公共IP地址：CDOhttps://defenseorchestrator.eu/
    - 35.157.12.126
    - 35.157.12.15
  - 如果您是美国的客户，并且连接到，则这些是云连接器的公共 IP 地址：CDOhttps://defenseorchestrator.com/
    - 52.34.234.2
    - 52.36.70.147
  - 如果您是**亚太地区-日本-中国 (AJPC)** 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
- 在上述程序的第 4 步中，创建一个允许从云连接器的公共 IP 地址访问外部接口的访问控制规则。

注册令牌自行激活方法是将设备自行激活到的推荐方法。使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+, on page 15FDM 管理CDO将外部接口配置为允许从云连接器进行管理访问后，载入设备。FDM 管理您将使用外部接口的IP地址进行连接。在我们的场景中，该地址是209.165.202.129。

将 FDM 管理 设备载入 CDO

使用以下程序按照以下方法将 FDM 管理 载入 CDO。

使用用户名、密码和 IP 地址载入 FDM 管理 设备

按照此程序仅使用设备凭证和设备的管理 IP 地址载入 FDM 管理 设备。这是载入 FDM 管理 设备最简单的方法。但是，建议使用使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+将 FDM 管理 设备载入 CDO。

Before you begin

Important 在将 FDM 管理 设备载入 思科防御协调器 之前，请阅读载入 威胁防御 设备和 将 思科防御协调器 连接到托管设备。它们提供了载入设备所需的一般设备要求和载入必备条件。

- 使用凭证方法载入 FDM 管理 设备需要以下信息：
  - CDO 将用于连接到设备的设备凭证。
  - 用来管理设备的设备接口的 IP 地址。它可以是管理接口、内部接口或外部接口，具体取决于您的网络配置。
  - 设备必须由 Firepower 设备管理器 管理，并针对本地管理而配置，以便将其载入 CDO。无法由 Firepower 管理中心 管理。

Note 如果您连接到 https://www.defenseorchestrator.eu ，并且 FDM 管理 设备运行的是 6.4 版本的软件，则必须使用此方法。您只能载入运行 6.5 及更高版本软件的 FDM 管理 设备。

Procedure

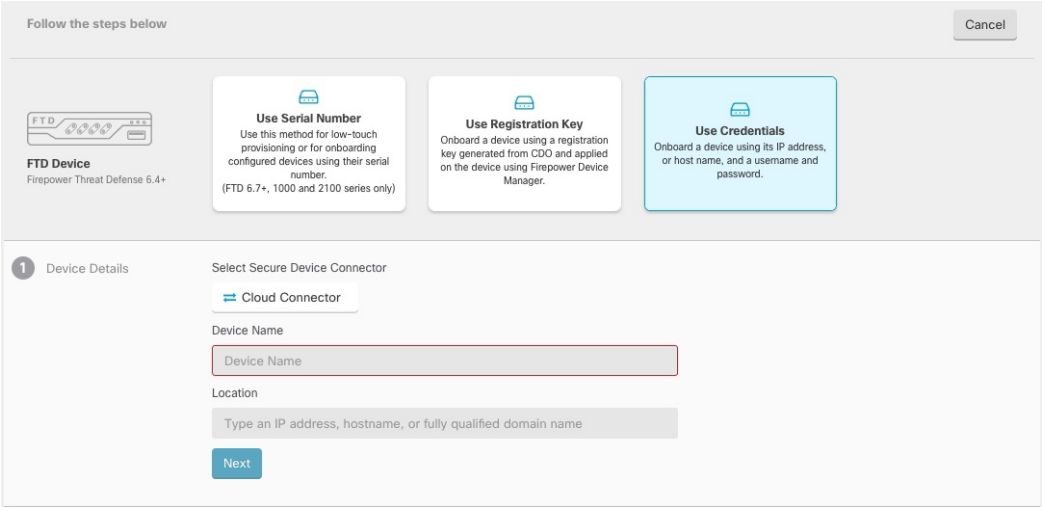
步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击 **清单 (Inventory)** ，然后点击蓝色加号按钮  以便**载入**设备。

步骤 3 点击 **FTD**。

Important 在尝试载入 FDM 管理 设备时，CDO 会提示您阅读并接受 Secure Firewall Threat Defense 最终用户许可协议 (EULA)，这是面向租户的一次性活动。接受 EULA 后，CDO 不会再次提示您接受 EULA，除非 EULA 发生更改。

步骤 4 在载入向导中，点击**使用凭证 (Use Credentials)**。



步骤 5 在设备详细信息步骤中：

- 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 (SDC)。如果您不想使用 SDC，CDO 可以使用云连接器连接到 FDM 管理 设备。您的选择取决于您如何将 CDO 连接到托管设备。
- 在**设备名称 (Device Name)** 字段中输入设备名称。它可以是设备的主机名或您选择的任何其他名称。
- 在**位置 (Location)** 字段中，输入设备的管理接口 IP 地址、主机名或设备的完全限定设备名称。默认端口为 443。

Important 如果您已有 SecureX 或思科威胁响应 (CTR) 账户，则需要合并 CDO 租户和 SecureX/CTR 账户，以便您的设备能够注册 SecureX。您的账户可以通过 SecureX 门户合并。有关说明，请参阅合并您的 CDO 和 SecureX 账户。在您的账户合并之前，您将无法在 SecureX 中查看设备的事件或受益于其他 SecureX 功能。

步骤 6 在**数据库更新**区域中，**立即执行安全更新并启用定期更新**默认启用。此选项立即触发安全更新并自动安排设备在每周一凌晨 2 点检查是否有额外更新。有关详细信息，请参阅更新 FTD 安全数据库和安排安全数据库更新。

禁用此选项不会影响您通过 FDM 配置的以前计划的任何更新。

点击**下一步 (Next)**。

步骤 7 输入设备管理员的用户名和密码，然后点击**下一步 (Next)**。

步骤 8 如果设备的 Firepower 设备管理器 上有待处理的更改，您将收到通知，您可以恢复更改或登录管理器并部署待处理的更改。如果 Firepower 设备管理器 上没有待处理的更改，您将不会看到提示。

步骤 9 （可选）添加设备的标签。有关详细信息，请参阅标签和标签组。

使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5

此程序介绍了如何使用注册码载入 FDM 管理 设备。此方法是将 FDM 管理 设备载入到 思科防御协调器 的推荐方法，如果使用 DHCP 为您的 FDM 管理 设备分配 IP 地址，则此方法非常有用。如果该 IP 地址由于任何原因发生变化，则您的 FDM 管理 设备仍会连接到 CDO。此外，您的 FDM 管理 设备可以在您的局域网上有一个地址，只要它可以访问外部网络，就可以使用此方法载入 CDO。

Warning 如果您已有 SecureX 或思科威胁响应 (CTR) 账户，则需要合并 CDO 租户和 SecureX/CTR 账户，以便您的设备能够注册 SecureX。在您的账户合并之前，您将无法在 SecureX 中查看设备的事件或受益于其他 SecureX 功能。我们强烈建议在 SecureX 中创建 CDO 模块之前合并您的账户。您的账户可以通过 SecureX 门户合并。有关说明，请参阅合并账户。

载入之前

- 对于运行版本 6.4 的客户，仅美国区域 (defenseorchestrator.com) 支持此载入方法。
- 对于运行版本 6.4 并连接到 EU 区域 (defenseorchestrator.eu) 的客户，他们必须使用使用用户名、密码和 IP 地址载入 FDM 管理 设备。
- 运行版本 6.5 或更高版本并连接到美国、欧盟或 APJC 区域 (apj.cdo.cisco.com) 的客户可以使用此载入方法。
- 查看 将 思科防御协调器 连接到托管设备 以了解将 CDO 连接到 FDM 管理 设备所需的网络要求。
- 请确保您的设备由 Firepower 设备管理器 管理，而不是由 Firepower 管理中心 管理。
- 运行版本 6.4 和 6.5 的设备在使用注册密钥载入之前，不得向思科智能软件管理器注册。您需要先取消注册这些 FDM 管理 设备的智能许可证，然后再将其载入 CDO。请参阅下面的“取消注册智能许可 防火墙设备管理器”。
- 设备可能正在使用 90 天的评估许可证。
- 登录 FDM 管理 设备并确保设备上没有等待处理的更改。
- 确保在您的 FDM 管理 设备上正确配置 DNS。
- 请确保在 FDM 管理 设备上正确配置时间服务。
- 请确保 FDM 管理 设备显示正确的日期和时间，否则载入将失败。

后续操作

执行以下两项操作之一：

- 从思科智能软件管理器取消注册您的 FDM 管理 设备（如果它已获得智能许可）。**您必须先从智能软件管理器取消注册该设备，然后再使用注册密钥将其载入 CDO**。请继续取消注册智能许可的 FDM 管理 设备, on page 12。

- 如果您的设备尚未获得智能许可，请继续使用注册密钥载入运行软件版本 6.4 或 6.5 的 FDM 管理 设备的程序, on page 13。

取消注册智能许可的 FDM 管理 设备

如果要载入的设备运行的是版本 6.4 或 6.5，并且已获得智能许可，则该设备可能已向思科智能软件管理器注册。**您必须先从智能软件管理器取消注册该设备，然后再使用注册密钥将其载入 CDO**。取消注销时，与设备关联的基本许可证和所有可选许可证将在您的虚拟帐户中释放。

注销设备后，该设备中的当前配置和策略将继续按原样运行，但无法进行或部署任何更改。

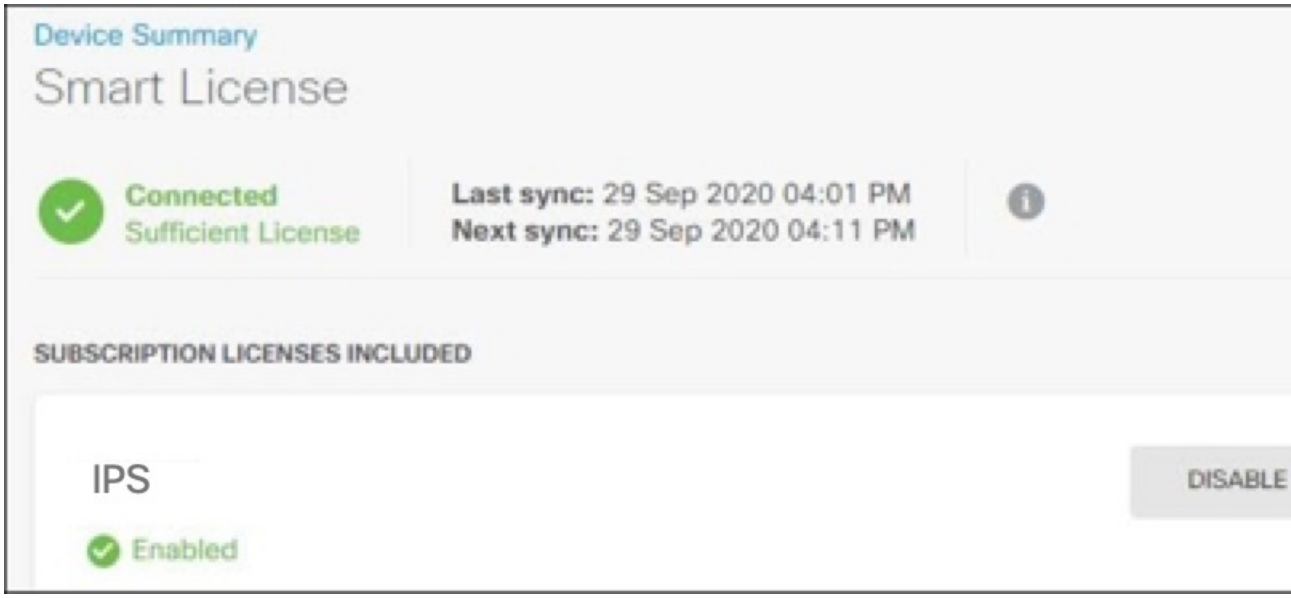
Procedure

步骤 1 使用 Firepower 设备管理器 登录设备。

步骤 2 点击上方选项卡中的设备图标。

步骤 3 点击**智能许可证 (Smart License)** 区域中的 **查看配置 (View Configuration)**。

步骤 4 点击**转到云服务 (Go to Cloud Services)** 齿轮菜单，然后选择**注销设备 (Unregister Device)**。



步骤 5 阅读警告并点击**取消注册 (Unregister)**，以取消注册该设备。

What to do next

如果您已取消注册以便将其载入 CDO，请继续使用注册密钥载入运行软件版本 6.4 或 6.5 的 FDM 管理 设备的程序, on page 13

使用注册密钥载入运行软件版本 6.4 或 6.5 的 FDM 管理 设备的程序

要使用注册密钥载入 FDM 管理，请遵循此程序：

Before you begin

查看先决条件，如 使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5, on page 11中所讨论。

Procedure

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击 **清单 (Inventory)**，然后点击蓝色加号按钮  以便**载入**设备。

步骤 3 点击 **FTD**。

Important 在尝试载入 FDM 管理 设备时，思科防御协调器 会提示您阅读并接受 Firepower 威胁防御最终用户许可协议 (EULA)，这是面向租户的一次性活动。接受本协议后，CDO 不会在后续的 FDM 管理 载入中再次提示您接受协议。如果 EULA 协议未来发生变化，则您必须在收到提示时再次接受它。

步骤 4 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用注册密钥 (Use Registration Key)**。

步骤 5 在**设备名称 (Device Name)** 字段中输入设备名称。它可以是设备的主机名或您选择的任何其他名称。

步骤 6 在**数据库更新 (Database Updates)** 区域中，**立即执行安全更新并启用定期更新 (Immediately perform security updates, and enable recurring updates)** 选项会被默认启用。此选项立即触发安全更新并自动安排设备在每周一凌晨 2 点检查是否有额外更新。有关详细信息，请参阅更新 FTD 安全数据库和安排安全数据库更新。

Note 禁用此选项不会影响您通过 Firepower 设备管理器 配置的以前计划的任何更新。

步骤 7 在**创建注册密钥 (Create Registration Key)** 区域中，CDO 将生成注册密钥。

Note 在生成密钥后，如果您在设备完全载入之前离开了载入屏幕，您将无法返回载入屏幕；但是，CDO 会在**清单 (Inventory)** 页面为该设备创建一个占位符。当您选择设备的占位符时，您将能够在位于右侧的操作窗格中看到该设备的密钥。

步骤 8 点击复制图标 以复制注册密钥。

Note 您可以跳过复制注册密钥的步骤，然后点击**下一步 (Next)** 完成设备的占位符输入，稍后注册设备。如果您尝试先创建设备后注册，或者您是在客户网络中安装价值证明 (POV) 设备的 Cisco 合作伙伴，则此选项很有用。

在**清单 (Inventory)** 页面中，您会看到设备现在处于连接状态“未提供”(Unprovisioned)。将**未调配 (Unprovisioned)** 下出现的注册密钥复制到 防火墙设备管理器，以完成载入过程。

步骤 9 在要载入到 CDO 的设备上登录 Firepower 设备管理器。

步骤 10 在**系统设置 (System Settings)**中，点击**云服务 (Cloud Services)**。

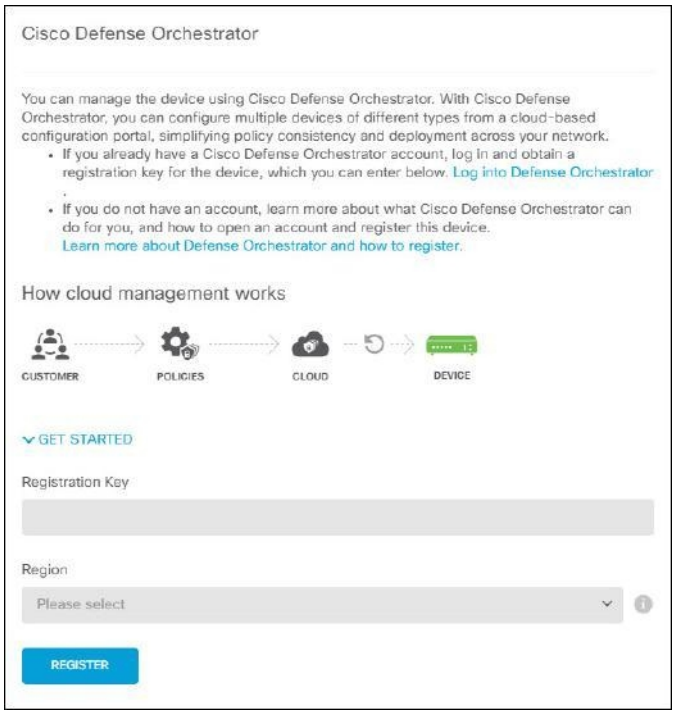
步骤 11 在 CDO 磁贴中，点击**开始 (Get Started)**。

步骤 12 在**区域 (Region)** 字段中，选择您的租户要分配到的 思科云区域：

- 如果您登录到 defenseorchestrator.com，请选择美国。
- 如果您登录到 defenseorchestrator.eu，请选择欧盟。
- 如果您登录到 apj.cdo.cisco.com，请选择亚太及日本地区。

Note 此步骤不适用于运行版本 6.4 的 FDM 管理 设备。

步骤 13 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。



步骤 14 点击**注册 (Register)**，然后**接受** Cisco 披露声明。

步骤 15 返回至 CDO。选择所有要应用于设备的许可证。

有关详细信息，请参阅 应用或更新智能许可证。您也可以点击**跳过 (Skip)** 以使用 90 天评估许可证继续载入。

步骤 16 返回 CDO，打开**清单 (Inventory)** 页面，观察设备状态从“未提供”(Unprovisioned) 到“正在定位”(Locating) 到“正在同步”(Syncing) 再到“已同步”(Synced) 的发展过程。

使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+

此程序介绍了如何使用注册码载入运行 6.6+ 版本的 FDM 管理 设备。此方法是将 FDM 管理 设备载入到 思科防御协调器 的推荐方法，如果使用 DHCP 为您的 FDM 托管设备分配 IP 地址，则此方法非常有用。如果该 IP 地址由于任何原因发生变化，则您的 FDM 管理 设备仍会连接到 CDO。此外，您的 FDM 管理 设备可以在您的局域网上有一个地址，只要它可以访问外部网络，就可以使用此方法载入 CDO。

Warning 如果您已有 SecureX 或思科威胁响应 (CTR) 账户，则需要合并 CDO 租户和 SecureX/CTR 账户，以便您的设备能够注册 SecureX。在您的账户合并之前，您将无法在 SecureX 中查看设备的事件或受益于其他 SecureX 功能。我们强烈建议在 SecureX 中创建 CDO 模块之前合并您的账户。您的账户可以通过 SecureX 门户合并。有关说明，请参阅合并账户。

如果要载入运行软件版本 6.4 或 6.5 的 FDM 管理 设备，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5。

载入之前

- 此载入方法目前适用于 6.6+ 版本以及连接到 defenseorchestrator.com、defenseorchestrator.eu 和 apj.cdo.cisco.com 的客户。
- 查看 将 思科防御协调器 连接到托管设备 以了解将 CDO 连接到 FDM 管理 设备所需的网络要求。
- 请确保您的设备由 Firepower 设备管理器 管理，而不是由 Firepower 管理中心 管理。
- 设备可以使用 90 天评估许可证，也可以使用智能许可。运行版本 6.6+ 的设备可以使用注册密钥载入到 CDO，而无需取消注册任何已安装的智能许可证。
- 设备不能已注册到 Cisco 云服务。在载入之前，请参阅下面的“从思科云服务取消注册 FDM 管理 设备”。
- 登录设备的 Firepower 设备管理器 UI 并确保设备上没有等待处理的更改。
- 确保在您的 FDM 管理 设备上正确配置 DNS。
- 请确保在 FDM 管理 设备上正确配置时间服务。
- 请确保 FDM 管理 设备显示正确的日期和时间，否则载入将失败。

后续操作：

执行以下操作之一：

- 如果运行版本 6.6+ 的 FDM 管理 设备已注册到思科云服务，则需要先取消注册设备，然后再载入。请继续从思科云服务取消注册 FDM 管理 设备, on page 16。
- 如果您的设备未注册到思科云服务，请继续 使用注册密钥载入运行软件版本 6.6+ 的 FDM 管理设备的程序, on page 17。

从思科云服务取消注册 FDM 管理 设备

以下程序是如何从思科云服务取消注册设备的程序。在使用注册密钥载入和 FDM 管理 设备以 CDO 之前，请使用此方法。

Note 如果您载入运行 7.0 或更高版本的虚拟 FDM 管理 设备，将虚拟 FDM 管理 设备注册到 CDO 会自动将性能分层智能许可选项重置为 **变量**，这是默认级别。在载入后，您 **必须** 通过 Firepower 设备管理器 UI 手动重新选择与设备关联的许可证匹配的层。

使用此程序检查并确保它未注册到思科云服务：

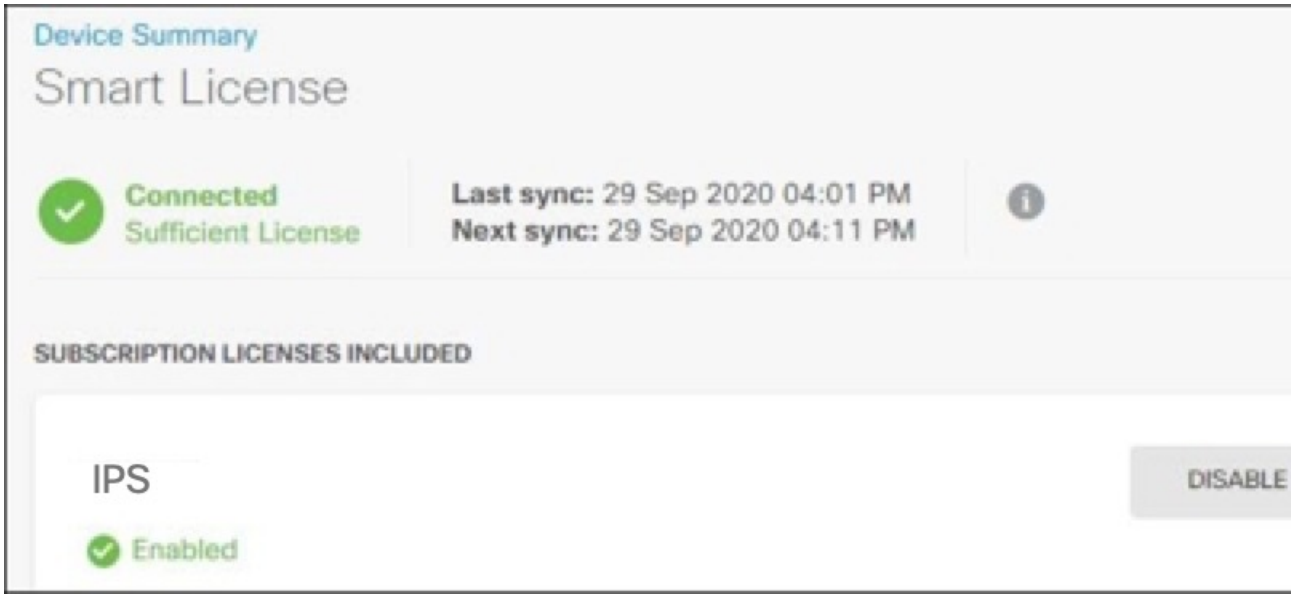
Procedure

步骤 1 使用 Firepower 设备管理器 登录设备。

步骤 2 点击上方选项卡中的设备图标。

步骤 3 展开**系统设置 (System Settings)** 菜单，然后点击**云服务 (Cloud Services)**。

步骤 4 在**云服务 (Cloud Services)** 页面中，点击齿轮菜单，然后选择**取消注册云服务 (Unregister Cloud Services)**。



步骤 5 阅读警告并点击**取消注册 (Unregister)**，以取消注册该设备。

What to do next

如果您尝试载入运行 6.6 或更高版本的 FDM 管理 设备，请继续使用注册密钥载入运行软件版本 6.6+ 的 FDM 管理 设备的程序, on page 17。

使用注册密钥载入运行软件版本 6.6+ 的 FDM 管理 设备的程序

要使用注册密钥载入 FDM 管理 设备，请遵循此程序：

Procedure

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击 **清单 (Inventory)**，然后点击蓝色加号按钮  以便**载入**设备。

步骤 3 点击 **FTD**。

Important 在尝试载入 FDM 管理 设备时，思科防御协调器 会提示您阅读并接受最终用户许可协议 (EULA)，这是租户中的一次性活动。接受本协议后，CDO 不会在后续的载入中再次提示您接受协议。如果 EULA 协议未来发生变化，则您必须在收到提示时再次接受它。

步骤 4 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用注册密钥 (Use Registration Key)**。

步骤 5 在**设备名称 (Device Name)** 字段中输入设备名称。它可以是设备的主机名或您选择的任何其他名称。

步骤 6 在**数据库更新 (Database Updates)** 区域中，**立即执行安全更新并启用定期更新 (Immediately perform security updates, and enable recurring updates)** 会被默认启用。此选项立即触发安全更新并自动安排设备在每周一凌晨 2 点检查是否有额外更新。有关详细信息，请参阅更新 FTD 安全数据库和安排安全数据库更新。

Note 禁用此选项不会影响您通过 Firepower 设备管理器 配置的以前计划的任何更新。

步骤 7 在**创建注册密钥**步骤中，CDO 将生成注册密钥。

Note 在生成密钥后，如果您在设备完全载入之前离开了载入屏幕，您将无法返回载入屏幕；但是，CDO 会在**清单 (Inventory)** 页面为该设备创建一个占位符。当您选择设备的占位符时，您将能够在该页面上看到该设备的密钥。

步骤 8 点击复制图标 以复制注册密钥。

Note 您可以跳过复制注册密钥的步骤，然后点击**下一步 (Next)** 完成设备的占位符输入，稍后注册设备。如果您尝试先创建设备后注册，或者您是在客户网络中安装价值证明 (POV) 设备的 Cisco 合作伙伴，则此选项很有用。

在**清单 (Inventory)** 页面，您会看到设备现在处于连接状态“未提供”。将**未调配 (Unprovisioned)** 下出现的注册密钥复制到 防火墙设备管理器，以完成 载入过程。

步骤 9 登录到您要载入的设备的 Firepower 设备管理器。

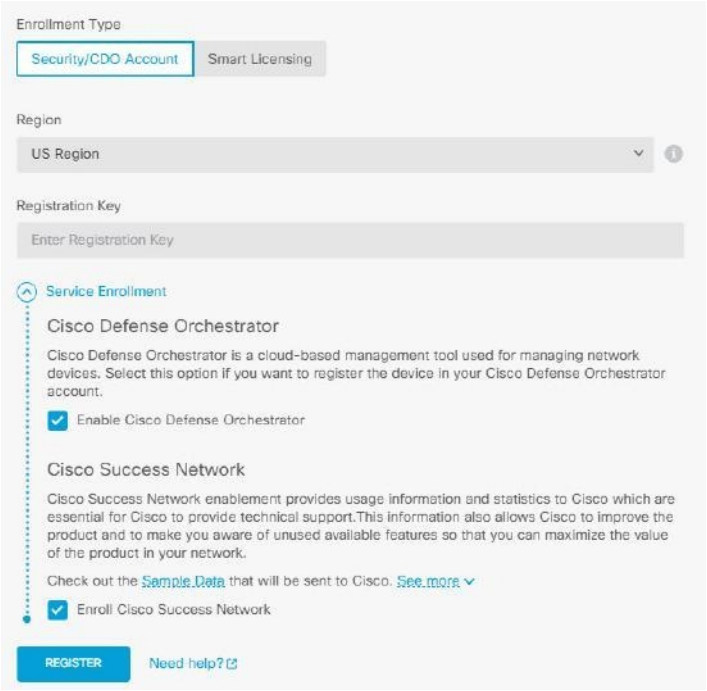
步骤 10 在 **系统设置**下，点击 **云服务**。

步骤 11 在**区域 (Region)** 字段中，选择您的租户要分配到的 思科云区域：

- 如果您登录到 defenseorchestrator.com，请选择美国。
- 如果您登录到 defenseorchestrator.eu，请选择欧盟。
- 如果您登录到 apj.cdo.cisco.com，请选择亚太及日本地区。

步骤 12 在**注册类型 (Enrollment Type)** 区域中，点击**安全账户 (Security Account)**。

Note 对于运行版本 6.6 的设备，请注意，CDO 的“租户”(Tenancy) 选项卡标题为 **安全账户 (Security Account)**，您必须在 Firepower 设备管理器 中手动启用 CDO。



步骤 13 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。

步骤 14 对于在“服务注册”(Service Enrollment) 区域运行版本 6.7 或更高版本的设备，请选中**启用 Cisco Defense Orchestrator (Enable Cisco Defense Orchestrator)**。

步骤 15 查看有关思科成功网络注册的信息。如果您不想参与，请取消选中**注册思科成功网络 (Enroll Cisco Success Network)** 复选框。

步骤 16 点击**注册 (Register)**，然后点击**接受 (Accept)** 以接受思科披露声明。Firepower 设备管理器 会将注册请求发送至 CDO。

步骤 17 返回到 CDO，在**创建注册密钥 (Create Registration Key)** 区域中，点击**下一步 (Next)**。

步骤 18 选择所有要应用于设备的许可证。点击**下一步**。

步骤 19 返回 CDO，打开**清单 (Inventory)** 页面，观察设备状态从“未提供”(Unprovisioned) 到“正在定位”(Locating) 到“正在同步”(Syncing) 再到“已同步”(Synced) 的发展过程。

使用设备的序列号载入 FDM 管理 设备

此程序是设置 FDM 管理 设备并将其载入到 思科防御协调器 的简化方法。您只需要设备的机箱序列号或 PCA 序列号。在载入设备时，您可以申请智能许可证或使用 90 天评估许可证。

在执行使用低接触调配载入 FDM 管理 设备的工作流程和必备条件之前，请确保通读使用案例以了解概念。

Important 这些载入 FDM 管理 设备的方法仅适用于运行版本 6.7 或更高版本的设备。

使用案例

- 使用设备的序列号载入 FDM 管理 设备, on page 19：载入被添加到网络并从互联网访问的新出厂 FDM 管理 设备。在设备上未完成初始安装向导。
- 使用设备的序列号载入已配置的 FDM 管理 设备, on page 25：载入已配置的 FDM 管理 设备或已添加到网络并从互联网访问的已升级设备。在设备上完成初始设置向导。

Important 如果要使用此方法载入在设备支持的较旧软件版本上运行的设备，则需要在该设备上执行软件的全新安装（重新映像），而不是升级。

相关信息：

- 术语和定义
- 使用序列号对 FDM 托管设备载入进行故障排除

使用低接触调配载入 FDM 管理 设备的工作流程和必备条件

低接触调配功能允许自动调配和配置新出厂的 Firepower 1000、Firepower 2100 或 Secure Firewall 3100 系列设备，从而消除将设备载入到 CDO 所涉及的大多数手动任务。低接触调配适用于远程办公室或员工不太熟悉网络设备的其他位置。

要使用低接触调配流程，您必须将设备载入 CDO，将其连接到可以访问互联网的网络，然后打开设备电源。有关详细信息，请参阅 使用设备的序列号载入已配置的 FDM 管理 设备, on page 25。

Note 您可以在将设备载入 CDO 之前或之后启动设备。**我们建议您先将设备载入 CDO，然后再启动设备，再将其连接到分支机构网络**。当您在 CDO 中载入设备时，该设备将与思科云中的 CDO 租户关联，并且 CDO 会自动同步设备。

您还可以使用此程序载入从外部供应商处购买的设备，或者载入已由其他区域中的其他云租户管理的设备。但是，如果设备已注册到外部供应商的云租户或其他区域的云租户，则 CDO 不会载入设备，但会显示 “设备序列号已申领 *(Device serial number already claimed)*” 错误消息。在这种情况

下，CDO 管理员必须从其先前的云租户中取消注册设备的序列号，然后在自己的租户中申领 CDO 设备。请参阅故障排除一章中的已申领设备序列号。

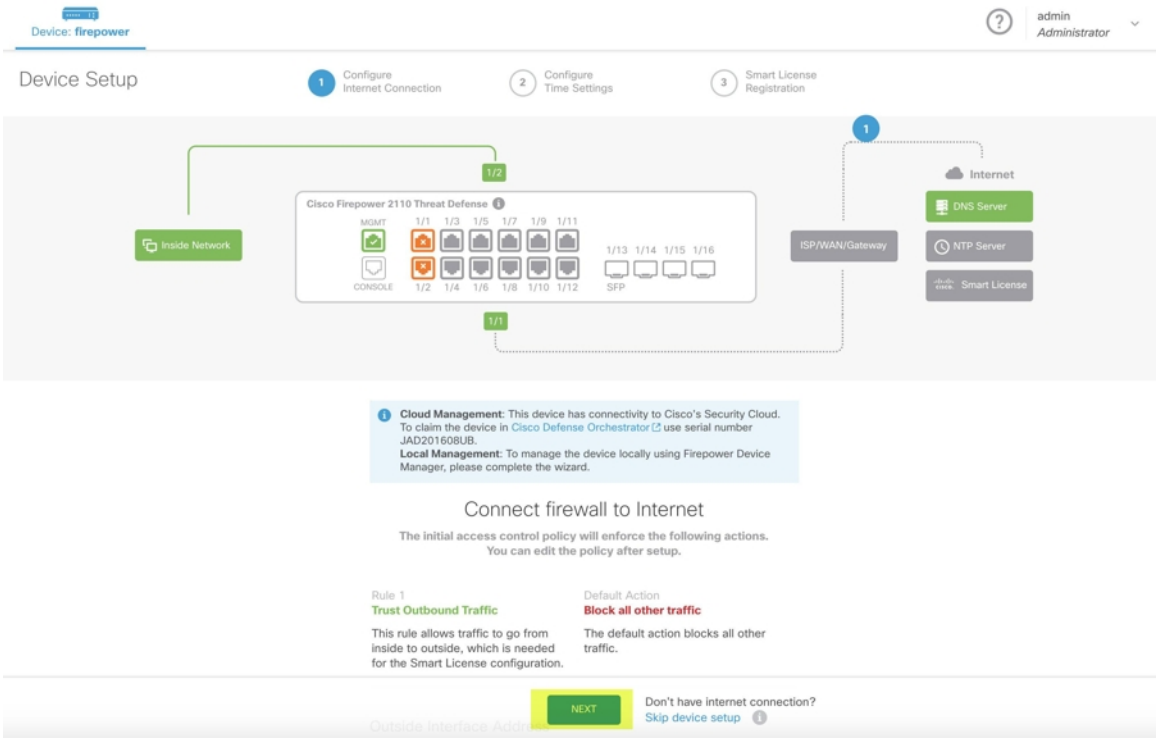
设备**连接 (Connectivity)** 状态更改为“在线”(Online)， **配置 (Configuration)** 状态更改为“已同步”(Synced)。FDM 管理 设备已被载入 CDO。

您可以看到硬件后面板上的状态 LED (Firepower 1010)、SYS LED (Firepower 2100) 或 S LED (Secure Firewall 3100) 呈绿色闪烁。连接到云时，设备 LED 会继续闪烁绿色。如果设备无法连接到思科云或在连接后失去连接，您可以看到状态 LED (Firepower 1010)、SYS LED (Firepower 2100) 或 M LED (Secure Firewall 3100) 交替闪烁绿色和琥珀色。

请参阅此视频：使用低接触调配安装思科 Firepower 防火墙视频，以便了解 LED 指示灯。

Important 如果您已登录 FDM 管理 设备控制台、SSH 或 Firepower Threat Defense，您将在首次登录时更改设备的密码。您仍然可以使用低接触调配流程来使用 CDO 载入设备。登录 Firepower Threat Defense 后，请勿完成配置外部接口的设备安装向导步骤。如果完成此步骤，则设备将从云中注销，并且您无法使用低接触调配。

当您登录 Firepower Threat Defense 时，您将在控制面板上看到以下屏幕。



无需在 Firepower Threat Defense UI 上继续操作，转至序列号载入向导并载入设备。在这里，您必须选择**默认密码已更改 (Default Password Changed)**，因为设备密码已更改。

前提条件

软件和硬件要求

FDM 管理 设备必须运行支持序列号载入的软件。使用下表作为指南：

Table 1: 硬件和软件支持

支持低接触调配的防火墙型号	支持的防火墙软件版本	软件包
Firepower 1000 系列设备型号：1010、1120、1140、1150	6.7 或更高版本	SF-F1K-TDx.x-K9
Firepower 2100 系列设备型号：2110、2120、2130、2140	6.7 或更高版本	SF-F2K-TDx.x-K9
Secure Firewall 3100 系列设备型号：3110、3120、3130、3140	7.1 或更高版本	SF-F3K-TDx.x-K9

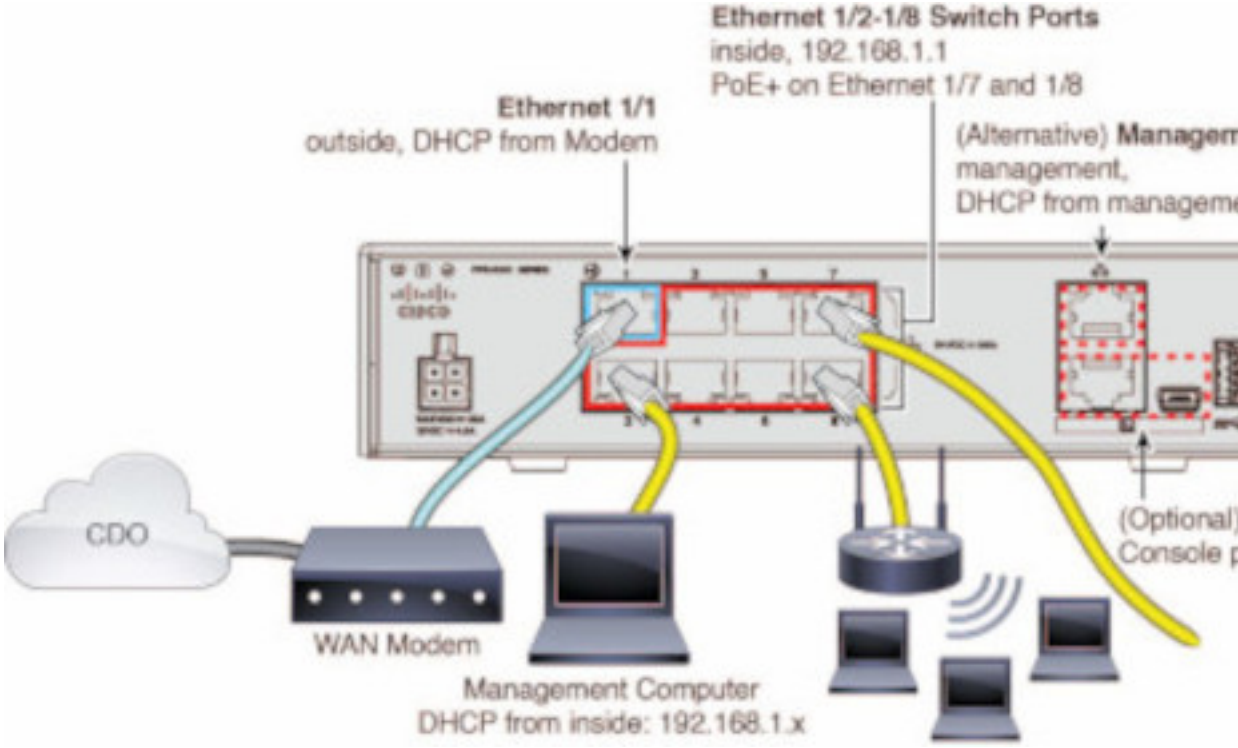
确认管理平台运行的是正确的版本。

Table 2: 支持 ***FTD*** 管理器版本

管理器	支持的版本
Firepower 设备管理器	7.0 或更高版本
本地防火墙管理中心	7.2 或更高版本
云交付的防火墙管理中心	不适用

硬件安装的配置前提条件

- **分支机构的网络无法使用 192.168.1.0/24 地址空间**。以太网 1/1（外部）上的网络无法使用 192.168.1.0/24 地址空间。运行 FDM 6.7 的 1000 和 2100 系列设备上的以太网 1/2“内部”接口的默认 IP 地址为 192.168.1.1，如果它在该子网上，则可能与 WAN 调制解调器分配的 DHCP 地址冲突。
  - **内部** - 以太网 1/2，IP 地址 192.168.1.1
  - **外部** - 以太网 1/1、来自 DHCP 的 IP 地址或在设置过程中指定的地址



如果无法更改外部接口设置，请使用 Firepower 设备管理器 更改以太网 1/2“内部”接口设置上的子网，以避免冲突。例如，您可以更改为以下子网设置：

- IP 地址：192.168.95.1
- DHCP 服务器范围：192.168.95.5-192.168.95.254

要了解配置物理接口的步骤，请参阅 《思科防火墙设备管理器配置指南》。在“接口”一章中，请参阅“配置物理接口”部分。

- 威胁防御 设备必须已安装并连接到思科云。
- 设备的外部或管理接口必须连接到提供 DHCP 寻址的网络。通常，设备在外部或管理接口上有一个默认的 DHCP 客户端。

Note 如果管理接口连接到具有 DHCP 服务器的网络，则它优先于 Linux 堆栈发起的流量的外部接口。

- 需要访问您的外部或管理接口才能访问以下 安全服务交换 域以便使用串行载入方法。
  - 美国地区
    - api-sse.cisco.com
    - est.sco.cisco.com（跨地域通用）

- mx*.sse.itd.cisco.com（目前仅 mx01.sse.itd.cisco.com）
- dex.sse.itd.cisco.com（客户成功案例）
- eventing-ingest.sse.itd.cisco.com （CTR 和 CDO）
- registration.us.sse.itd.cisco.com（允许设备注册到思科区域云）

- 欧盟地区
  - api.eu.sse.itd.cisco.com
  - est.sco.cisco.com（跨地域通用）
  - mx*.eu.sse.itd.cisco.com（目前仅 mx01.eu.sse.itd.cisco.com）
  - dex.eu.sse.itd.cisco.com（客户成功案例）
  - eventing-ingest.eu.sse.itd.cisco.com（CTR 和 CDO）
  - registration.eu.sse.itd.cisco.com（允许设备注册到思科区域云）

- 亚太地区
  - api.apj.sse.itd.cisco.com
  - est.sco.cisco.com（跨地域通用）
  - mx*.apj.sse.itd.cisco.com（目前仅 mx01.apj.sse.itd.cisco.com）
  - dex.apj.sse.itd.cisco.com（客户成功案例）
  - eventing-ingest.apj.sse.itd.cisco.com（CTR 和 CDO）
  - http://registration.apj.sse.itd.cisco.com（允许设备注册到思科区域云）
    http://registration.apj.sse.itd.cisco.com/

- 设备的外部接口必须具有对思科 Umbrella DNS 的 DNS 访问权限。

在 CDO 中申领设备之前

在 CDO 中申领设备之前，请确保您拥有以下信息：

- 威胁防御 设备的机箱序列号或PCA编号。您可以在硬件机箱的底部或装运设备的包装箱上找到此信息。在下面的示例图片中，您可以看到Firepower 1010机箱底部的序列号“*******X0R9”。

- 设备的默认密码。
- 从思科智能软件管理器生成以用于其他功能的智能许可证。但是，您可以使用90天评估许可证来完成设备载入，然后再申请智能许可证。

通过低接触调配载入*FDM* 管理设备

Caution 在 思科防御协调器 中载入设备时，我们建议您不要使用 Firepower 设备管理器 来执行设备简易设置。这会导致 CDO 出现临时错误。

Before you begin

如果您载入设备并打算使用 本地管理中心 对其进行管理，则 本地管理中心 **必须**运行 7.4 及更高版本。较早的版本不支持低接触调配。

Procedure

步骤 1 如果要载入从外部供应商处购买的设备，则必须先重新映像设备。有关更多信息，请参阅《思科 FXOS 故障排除指南》中的“重新映像程序”一章。

步骤 2 登录 CDO。

步骤 3 在导航窗格中，点击 **清单 (Inventory)**，然后点击蓝色加号按钮 以便**载入**设备。

步骤 4 点击 **FTD** 磁贴。

Important 在尝试载入设备时，CDO 会提示您阅读并接受最终用户许可协议 (EULA)，这是租户中的一次性活动。接受本协议后，CDO 不会在后续的载入中再次提示您接受协议。如果 EULA 协议未来发生变化，则您必须在收到提示时再次接受它。

步骤 5 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用序列号 (Use Serial Number)**。

步骤 6 在**选择 FMC** 步骤中，使用下拉菜单选择已被载入 CDO 的 本地管理中心。点击**下一步**。

本地管理中心 必须运行 7.4 或更高版本。如果您没有载入的 本地管理中心，请点击“+ 载入本地 FMC”(+Onboard On-Prem FMC) 以查看载入向导。

步骤 7 在**连接 (Connection)** 步骤中，输入设备的序列号和设备名称。点击**下一步**。

步骤 8 对于低接触调配，设备必须是全新的或已重新映像。对于**密码重置 (Password Reset)**，确保选择**是，此新设备从未登录或配置管理器 (Yes, this new device has never been logged into or configured for a manager)**。输入设备的新密码并确认新密码，，然后点击**下一步 (Next)**。

步骤 9 对于**策略分配 (Policy Assignment)**，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果没有自定义策略，CDO 会自动选择默认访问控制策略。点击**下一步**。

步骤 10 选择所有要应用于设备的许可证。点击**下一步**。

步骤 11 （可选）为设备添加标签。CDO 会在设备成功载入后应用这些标签。

What to do next

CDO 会开始申领设备，您将在右侧看到**正在申领 (Claiming)** 消息。CDO 会持续轮询一小时，以确定设备是否在线并已注册到云。注册到云后，CDO 将开始初始调配并成功载入设备。当设备上的 LED 状态呈绿色闪烁时，可以确认设备注册。如果设备在连接后无法连接到思科云或失去连接，您可以看到状态 LED (Firepower 1000) 或 SYS LED (Firepower 2100) 交替闪烁绿色和琥珀色。

如果设备在前一小时内仍未注册到云，则会发生超时，现在 CDO 会每隔 10 分钟定期轮询一次，以确定设备状态并保持**正在申领 (Claiming)** 状态。当设备打开并连接到云时，您无需等待 10 分钟即可了解其载入状态。您可以随时点击**检查状态 (Check Status)** 链接查看状态。CDO 会开始初始调配并成功载入设备。

Important 假设您已完成设备安装向导（请参阅 使用设备的序列号载入已配置的 FDM 管理 设备），设备已从云中取消注册，在这种情况下，CDO 仍处于**正在申领 (Claiming)** 状态。您需要从 Firepower 设备管理器 完成手动注册，才能将其添加到 CDO。（在 Firepower 设备管理器 中，转至**系统设置 (System Settings)** > **云服务 (Cloud Services)**，然后选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)** 选项并点击**注册 (Register)**）。然后，点击**检查状态 (Check Status)**。

使用设备的序列号载入已配置的 FDM 管理 设备

此程序适用于已配置为进行管理的设备。由于设备安装向导是在已配置的FDM管理 设备上完成的，因此设备将从云中取消注册，并且您无法使用低接触调配过程将此类设备载入 CDO。

如果您的设备是全新的，并且从未进行过管理或配置，您可以通过低接触调配来载入设备。有关详细信息，请参阅 通过低接触调配载入FDM 管理设备, on page 24。

Note 当设备未连接到思科云时，您可以看到状态 LED（Firepower 1000）、SYS LED（Firepower 2100）或 M LED（Secure Firewall 3100）交替闪烁绿色和琥珀色。

您可能已完成设备安装向导以执行以下任务：

- 设备必须运行版本 6.7 或更高版本。
- 在设备的管理接口上配置静态 IP 地址。如果接口无法获取必要的动态 IP 地址，或者 DHCP 服务器不提供网关路由，则需要配置静态 IP 地址。
- 使用 PPPoE 获取地址并配置外部接口。
- 使用 Firepower 设备管理器 或 Firepower 管理中心 来管理运行 6.7 或更高版本的设备。

Important 您可以将 Secure Firewall Threat Defense 设备的管理器从 Firepower 设备管理器 切换为 Firepower 管理中心，也可以切换为其他方式。对于设备运行的版本，执行《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》的“系统管理”一章的**在本地管理和远程管理之间切换**部分中介绍的步骤。

如果要载入设备，请执行以下操作：

Procedure

步骤 1 有关载入的前提条件，请查看此处的使用低接触调配载入 FDM 管理 设备的工作流程和必备条件。

步骤 2 在 Firepower 设备管理器 UI 中，请转至 **系统设置** > **云服务** ，然后选 **通过 Cisco 防御协调器自动注册租用** 选项并点击 **注册**。

步骤 3 登录 CDO。

步骤 4 在导航窗格中，点击 **清单 (Inventory)** ，然后点击蓝色加号按钮 以便**载入**设备。

步骤 5 点击 **FTD 磁贴**。

步骤 6 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用序列号 (Use Serial Number)**。

步骤 7 在**选择 FMC** 步骤中，使用下拉菜单选择已被载入 CDO 的 本地管理中心。点击**下一步**。

本地管理中心 必须运行 7.4 或更高版本。如果您没有载入的 本地管理中心，请点击“+ 载入本地 FMC”(+Onboard On-Prem FMC) 以查看载入向导。

步骤 8 在**连接 (Connection)** 步骤中，输入设备的序列号和设备名称。点击**下一步**。

步骤 9 如果设备**并非**全新的，并且已配置为进行管理，请选择**是，此新设备从未登录或为管理器配置 (Yes, this new device has never been logged into or configured for a manager)** 以进行**密码重置**。点击**下一步**。

步骤 10 对于**策略分配 (Policy Assignment)**，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果没有自定义策略，CDO 会自动选择默认访问控制策略。点击**下一步**。

步骤 11 选择所有要应用于设备的许可证。点击**下一步**。

CDO 将设备**连接 (Connectivity)** 状态更改为“在线”(Online)，并将**配置 (Configuration)** 状态更改为“已同步”(Synced) 状态。FDM 管理 设备已被载入 CDO。您可以看到硬件后面板上的状态 LED (Firepower 1000)、SYS LED (Firepower 2100) 或 M LED 呈绿色闪烁。当设备连接到思科云时，设备 LED 会继续闪烁绿色。如果设备无法连接到思科云或在连接后失去连接，您可以看到相同的状态 LED 交替闪烁绿色和琥珀色。

相关信息：

- 术语和定义

载入 FDM 管理 高可用性对

要将 Secure Firewall Threat Defense HA 对载入 CDO，必须单独载入该对中的每台设备。一对设备中的两个对等设备均已被载入后，CDO 会自动将其合并为**清单 (Inventory)** 页面中的单个条目。使用设备登录凭证或注册密钥载入设备。我们建议使用相同的方法载入**两台**设备。另请注意，如果您首先载入处于备用模式的设备，则CDO会禁用从该设备进行部署或读取的功能。您只能读取或部署到 HA 对中的主用设备。

注释 CDO 强烈建议使用注册密钥来载入设备。对于运行特定版本的 FTD 设备，使用注册密钥载入略有不同。有关详细信息，请参阅载入运行版本 6.4 或版本 6.5 的 FDM 管理 HA 对，第 28 页和载入运行版本 6.6 或版本 6.7 及更高版本的 FDM 管理 HA 对，第 29 页。

在将 FTD HA 对载入 CDO 之前，请查看以下内容：

- 您的 HA 对会在载入到 CDO 之前形成。
- 两台设备均处于正常状态。该对可以是主/主用和辅助/备用模式，**或** 主/备用和辅助/主用模式。运行状况不佳的设备将无法成功同步到 CDO。
- 您的 HA 对由 Firepower 设备管理器 管理，而不是由 Firepower 管理中心 管理。
- 您的云连接器连接到 CDO，https://www.defenseorchestrator.com。

使用注册密钥载入 FDM 管理高可用性对

在使用注册密钥载入 FDM 管理高可用性 (HA) 对之前，请注意以下前提条件：

- 仅美国区域 (defenseorchestrator.com) 支持使用注册密钥载入 6.4 版本的设备。要连接到欧盟区域 (defenseorchestrator.eu)，则必须使用用户名、密码和 IP 地址载入其 HA 对。
- 运行版本 6.5 或更高版本并连接到美国、欧盟或 APJC 的客户可以使用此载入方法。

- 运行版本 6.4 和 6.5 的设备在使用注册密钥载入之前，不得向思科智能软件管理器注册。您需要先取消注册这些 FDM 管理 设备的智能许可证，然后再将其载入 CDO。有关详细信息，请参阅取消注册智能许可的 FDM 管理 设备, on page 12。

载入运行版本 *6.4* 或版本 *6.5* 的 *FDM* 管理 *HA* 对

要载入运行软件版本 6.4 或 6.5 的 FDM 管理 HA 对，您必须一次载入一个设备。载入的设备是主设备还是辅助设备并不重要。

Note 如果使用注册密钥载入 HA 对的任一台设备，则必须以相同的方法载入另一台对等设备。

使用以下步骤来载入运行版本 6.4 或 6.5 的 HA 对：

Procedure

步骤 1 载入对等设备。请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5以载入对中的第一台设备。

步骤 2 在导航窗格中，点击**清单 (Inventory)**。

步骤 3 点击 **设备** 选项卡，找到您的设备。

步骤 4 点击 **FTD** 选项卡。设备同步后，请选择设备，使其突出显示。在**设备详细信息 (Device Details)** 正下方的操作窗格中，点击**载入设备 (Onboard Device)**。

步骤 5 输入已载入的对等设备的 **HA 对等体设备名称**。点击**下一步**。

步骤 6 如果您为第一台设备提供了智能许可证，CDO 会重新填充该许可证，以便您可以使用它来载入此当前设备。点击**下一步**。

Note 如果您取消注册设备的智能许可证以载入 FDM 管理 设备，您可以在此处重新应用智能许可证。

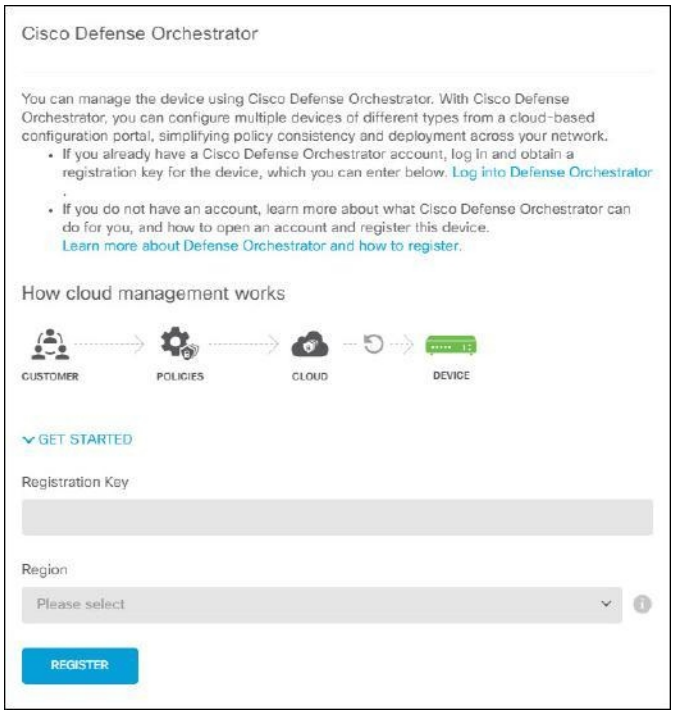
步骤 7 CDO 会自动为您准备载入的设备生成该注册密钥。点击**复制**图标 以复制注册密钥。

步骤 8 登录到您要载入的设备的 Firepower 设备管理器 UI。

步骤 9 在**系统设置 (System Settings)**中，点击**云服务 (Cloud Services)**。

步骤 10 在 CDO 磁贴中，点击**开始 (Get Started)**。

步骤 11 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。



步骤 12 在**区域 (Region)** 字段中，选择您的租户要分配到的 思科云区域：

- 如果您登录到 defenseorchestrator.com，请选择美国。
- 如果您登录到 defenseorchestrator.eu，请选择欧盟。
- 如果您登录到 apj.cdo.cisco.com，请选择亚太及日本地区。

Note 此步骤不适用于在版本 6.4 上运行的 FDM 管理 设备。

步骤 13 点击**注册 (Register)**，然后**接受** Cisco 披露声明。

步骤 14 返回到 CDO，然后在**创建注册密钥 (Create Registration Key)** 区域中，点击**下一步 (Next)**。

步骤 15 点击**转至清单 (Go to Inventory)**。CDO 会自动载入设备并将其合并为一个条目。与您载入的第一个对等设备类似，设备状态会从“未调配”(Unprovisioned) 依次变为“正在查找”(Locating)、“正在同步”(Syncing)、“已同步”(Synced)。

载入运行版本 *6.6* 或版本 *6.7* 及更高版本的 *FDM* 管理 *HA* 对

要载入运行版本 6.6 或 6.7 的 FDM 管理 HA 对，必须一次载入一个设备。载入的设备是主设备还是辅助设备并不重要。

Note 如果使用注册密钥载入 HA 对的任一台设备，则必须以相同的方法载入另一台对等设备。

使用以下步骤载入运行版本 6.6 或 6.7 的 HA 对：

Procedure

步骤 1 载入对等设备。有关详细信息，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+。

步骤 2 在导航窗格中，点击**清单 (Inventory)**。

步骤 3 点击 **设备** 选项卡，找到您的设备。

步骤 4 点击 **FTD** 选项卡。设备同步后，请选择设备，使其突出显示。在**设备详细信息 (Device Details)** 正下方的操作窗格中，点击**载入设备 (Onboard Device)**。

步骤 5 输入已被载入的对等设备的 HA 对等设备名称。点击**下一步**。

步骤 6 如果您为第一台设备提供了智能许可证，CDO 会重新填充该许可证，以便您可以使用它来载入此当前设备。点击**下一步**。

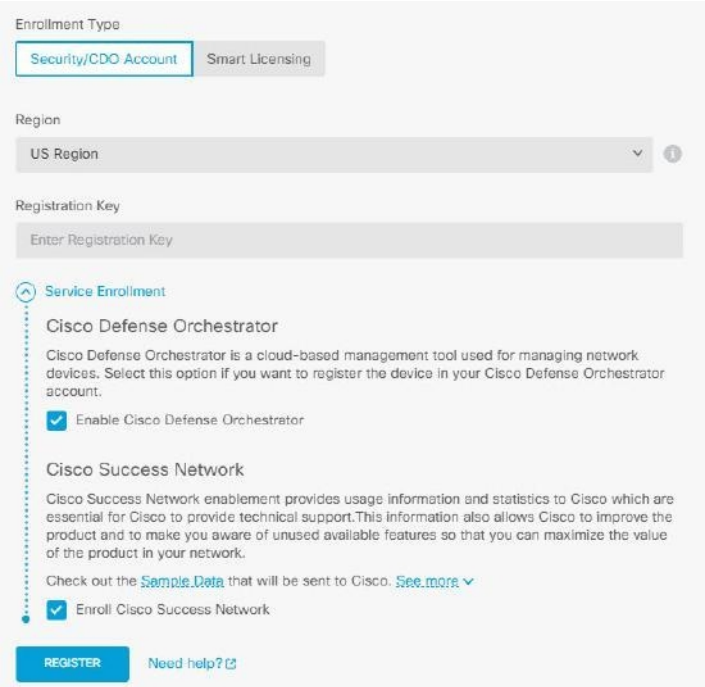
步骤 7 CDO 会自动为您准备载入的设备生成该注册密钥。点击复制图标 以复制注册密钥。

步骤 8 在要载入到 CDO 的设备上登录 Firepower 设备管理器。

步骤 9 在**系统设置 (System Settings)** 下，点击**云服务 (Cloud Services)**。

步骤 10 在**注册类型 (Enrollment Type)** 区域中，点击**安全/CDO 账户 (Security/CDO Account)**。

Note 对于运行版本 6.6 的设备，请注意，CDO 的“租户”(Tenancy) 选项卡标题为 **安全账户 (Security Account)**，您必须在 Firepower 设备管理器 UI 中手动启用 CDO。



步骤 11 在**区域 (Region)** 字段中，选择您的租户要分配到的 思科云区域：

- 如果您登录到 defenseorchestrator.com，请选择美国。
- 如果您登录到 defenseorchestrator.eu，请选择欧盟。
- 如果您登录到 apj.cdo.cisco.com，请选择亚太及日本地区。

步骤 12 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。

步骤 13 对于在“服务注册”(Service Enrollment) 区域运行版本 6.7 或更高版本的设备，请选中**启用思科防御协调器 (Enable Cisco Defense Orchestrator)**。

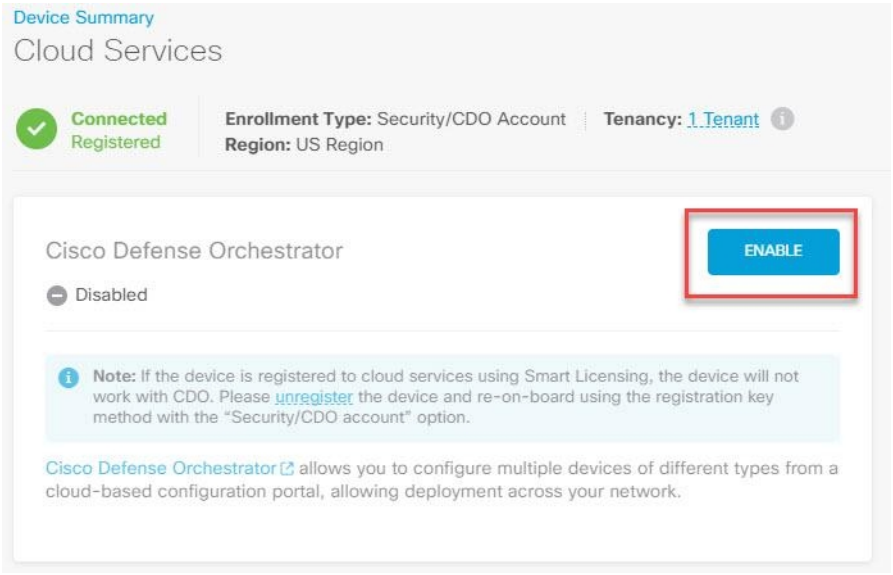
步骤 14 查看有关思科成功网络注册的信息。如果您不想参与，请取消选中**注册思科成功网络 (Enroll Cisco Success Network)** 复选框。

步骤 15 点击**注册 (Register)**，然后**接受** Cisco 披露声明。FDM 将注册请求发送到 CDO。

步骤 16 返回到 CDO，在**创建注册密钥 (Create Registration Key)** 区域中，点击**下一步 (Next)**。

步骤 17 在**智能许可证 (Smart License)** 区域中，您可以将智能许可证应用于 FDM 管理 设备，然后点击**下一步 (Next)**，也可以点击**跳过 (Next)** 以使用 90 天评估许可证继续载入，或者如果设备已获得智能许可。有关详细信息，请参阅 更新 FTD 设备的现有智能许可证。

Note 如果您的设备运行的是版本 6.6，则需要手动启用与 CDO 的通信。在设备的 FDM 管理 UI 中，导航至 **系统设置 (System Settings)** > **云服务 (Cloud Services)** ，然后在**思科防御协调器 (Cisco Defense Orchestrator)** 磁贴中点击**启用 (Enable)**。



步骤 18 返回到 CDO，点击**转至清单 (Go to Inventory)**。CDO 会自动载入设备并将其合并为一个条目。与您载入的第一个对等设备类似，设备状态会从“未调配”(Unprovisioned) 依次变为“正在查找”(Locating)、“正在同步”(Syncing)、“已同步”(Synced)。

载入 FDM 管理 高可用性对

注释 无论您使用什么方法来载入 HA 对的第一台设备，都必须以相同的方法载入另一台对等设备。

要载入在 CDO 外部创建的 FDM 管理 HA 对，请执行以下程序：

过程

步骤 1 载入 HA 对中的一个对等设备。使用设备的使用用户名、密码和 IP 地址载入 FDM 管理 设备、使用注册密钥载入运行软件版本 6.6+ 的 FDM 管理 设备的程序或使用设备的序列号载入已配置的 FDM 管理 设备来载入设备。

步骤 2 在设备同步后，在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择设备。在**设备详细信息 (Device Details)** 正下方的操作窗格中，点击**载入设备 (Onboard Device)**。

步骤 5 在弹出窗口中，输入 HA 对等体的设备名称和位置。

步骤 6 点击**载入设备 (Onboard Device)**。两台设备成功同步到 CDO 后，HA 对在**清单 (Inventory)** 页面中显示为单个实体。

载入 FTD 集群

-

载入集群的 设备

按照以下程序载入已加入集群的 威胁防御 设备：

开始之前

以下设备支持集群：

- Secure Firewall 3100 设备
- Firepower 4100 设备
- Firepower 9300 设备
- FTDv 设备（AWS、Azure、VMware、KVM、GCP）

请注意集群设备的以下限制：

- 设备必须至少运行 6.4 版本。
- 设备必须由物理或虚拟 Firepower 管理中心 管理。
- Firepower 4100 和 Firepower 9300 设备都必须通过设备的机箱管理器进行集群。
- Secure Firewall 3100 设备、KVM 和 VMware 环境必须通过 UI 进行集群。
- Azure、AWS 和 GCP 环境集群必须通过各自的环境创建并载入 Cisco Secure Firewall Management Center。

过程

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击 **清单 (Inventory)** ，然后点击蓝色加号按钮  以便**载入**设备。

步骤 3 点击 **FTD**。

步骤 4 在 **管理模式**下，确保选择 **FTD** 。

通过选择 **FTD**，您将保留 作为管理平台。如果选择 **FDM**，这会将管理器从 切换到本地管理器，例如 防火墙设备管理器 或 云交付的防火墙管理中心。请注意，交换管理器会重置除接口配置以外的所有现有策略配置，并且您必须在载入设备后重新配置策略。

步骤 5 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用 CLI 注册密钥 (Use Registration Key)**。

步骤 6 在**设备名称 (Device Name)** 字段中输入设备名称。它可以是设备的主机名或您选择的任何其他名称。

步骤 7 在策略分配步骤中，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

步骤 8 指定要载入的设备是物理设备还是虚拟设备。如果要载入虚拟设备，则必须从下拉菜单中选择设备的性能级别。

步骤 9 选择要应用于设备的基础版许可证。点击**下一步**。

步骤 10 CDO 使用注册密钥生成命令。将整个注册密钥按原样粘贴到设备的 CLI 中。

步骤 11 设备开始载入。作为可选步骤，您可以向设备添加标签，以帮助对“清单”(Inventory) 页面进行排序和过滤。输入标签，然后选择蓝色加号按钮。。

下一步做什么

设备同步后，CDO 会自动检测到设备已加入集群。在这里，请从“清单”(Inventory) 页面选择您刚刚载入的设备，然后选择位于右侧的“管理”(Management) 窗格下列出的任何选项。我们强烈建议您执行以下操作：

- 如果还没有创建，请创建自定义访问控制策略，以自定义环境的安全性。有关详细信息，请参阅FDM 管理 访问控制策略。
- 启用思科安全分析和日志记录 (SAL) 以在 CDO 控制面板中查看事件， **或**将设备注册到 Cisco Secure Firewall Management Center 以进行安全分析。

应用或更新智能许可证

将新的智能许可证应用于 FDM 管理 设备

执行以下程序之一，以智能许可 Firepower 威胁防御 (FTD) 设备：

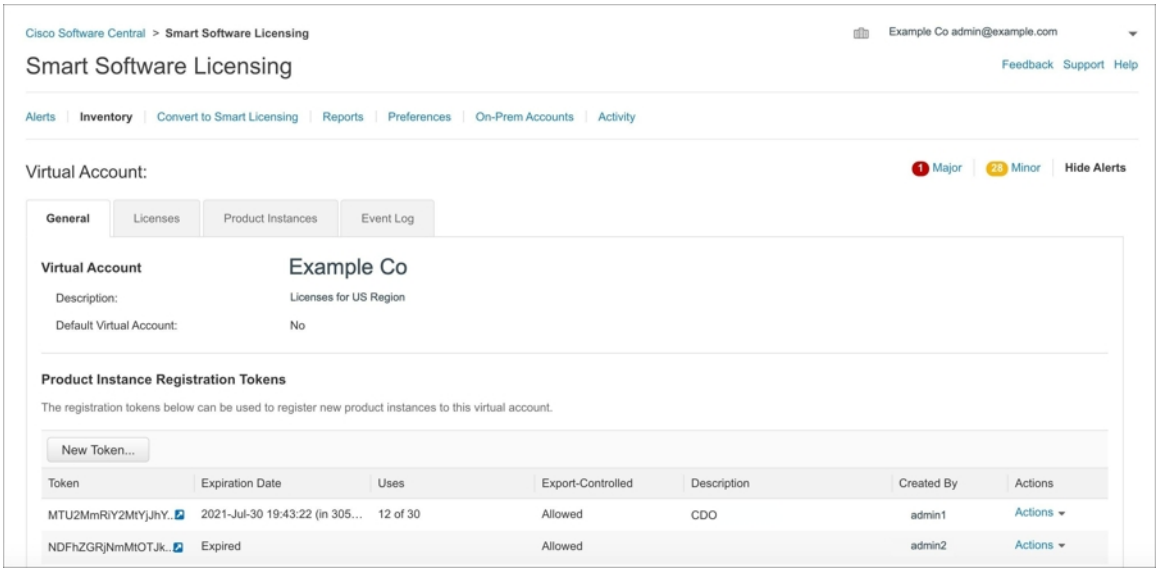
- 使用注册密钥载入 FDM 管理 设备时为设备提供智能许可证。
- 在使用注册密钥或管理员凭证载入设备后，为 FDM 管理 设备授予智能许可证。

Note FDM 管理 设备可能使用的是 90 天评估许可证，也可能是未注册的许可证。

在使用注册密钥载入时为 FDM 管理设备提供智能许可

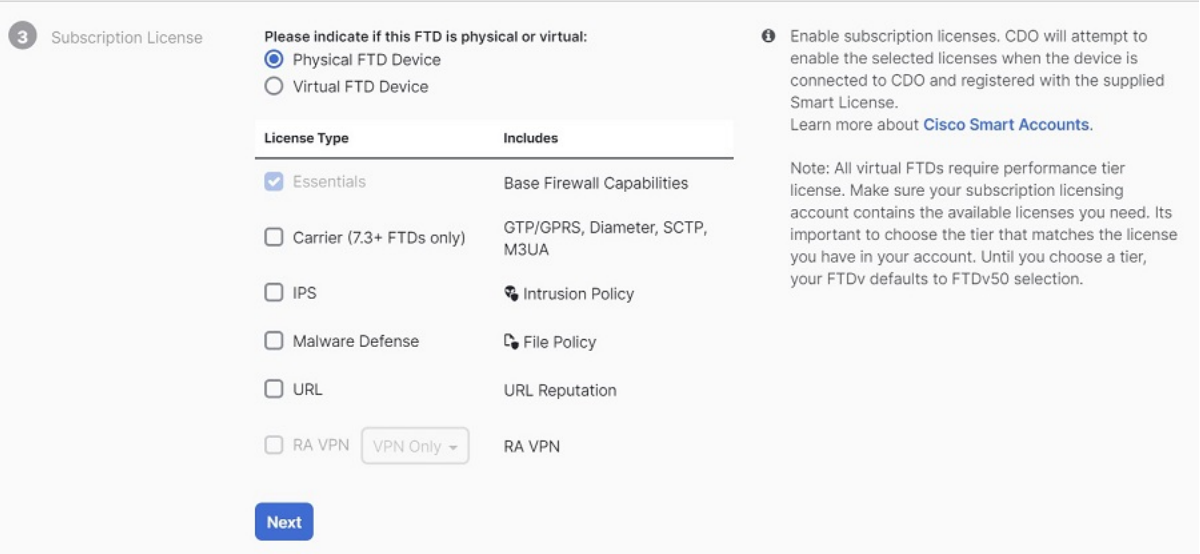
Procedure

步骤 1 登录思科智能软件管理器并生成新的智能许可证密钥。https://software.cisco.com/software/csws/ws/platform/home?locale=en_US#SmartLicensing-Inventory复制新生成的密钥。您可以观看生成智能许可视频了解详细信息。



步骤 2 使用注册密钥开始载入 FDM 管理设备。有关详细信息，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+或使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5。

步骤 3 在自行激活向导的第 4 步中，在此处的智能许可证框中，将智能许可证粘贴到激活字段中，然后点击下一步。

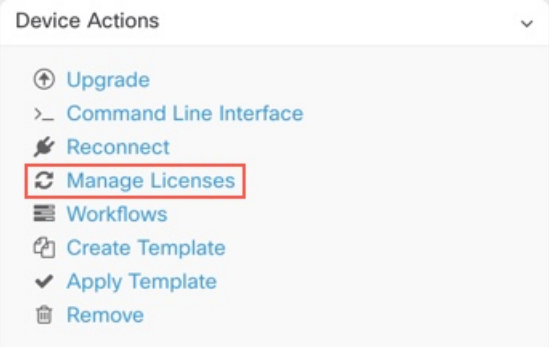


步骤 4 点击**转到清单页面 (Go to Inventory page)**。

步骤 5 点击 FTD 选项卡，查看自行激活过程的进度。设备开始同步并应用智能许可证。

您应该会看到设备现在处于在线连接状态。如果设备未处于在线连接状态，请查看右侧的设备操作窗格，然后点击管理许可证刷新许可证以更新连接状态。 >

步骤 6 将智能许可证成功应用于设备后，点击管理许可证。FDM 管理设备状态显示“已连接，许可证充足”。您可以启用或禁用可选许可证。有关详细信息，请参阅设备智能许可类型。FDM管理 设备许可类型



使用注册密钥或凭据载入设备后，为 FDM 管理设备授予智能许可证

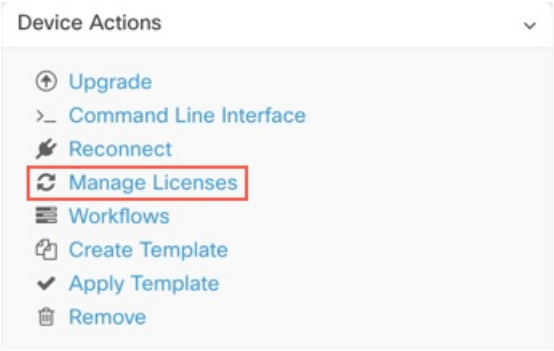
Procedure

步骤 1 在导航窗格中，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 **FTD** 选项卡，然后选择要许可的设备。

步骤 4 在右侧的设备操作窗格中，点击管理许可证。



步骤 5 按照屏幕说明输入从思科智能软件管理器生成的智能许可证。

步骤 6 将新的许可证密钥粘贴到框中，然后点击**注册设备 (Register Device)**。与设备同步后，连接状态变为“在线”。成功将智能许可证应用到 FDM 管理设备后，设备状态将显示“**已连接，许可证足够 (Connected, Sufficient License)**”。您可以启用或禁用可选许可证。有关详细信息，请参阅设备智能许可类型。FDM 管理 设备许可类型

更新 FTD 设备的现有智能许可证

您可以将新的智能许可证应用于智能许可的 FTD 设备。根据您选择的设备载入方法，选择适当的程序：

更改应用于使用注册密钥载入的 FDM 管理设备的智能许可证

Procedure

步骤 1 从 思科防御协调器 中删除相应的 FDM 管理设备。

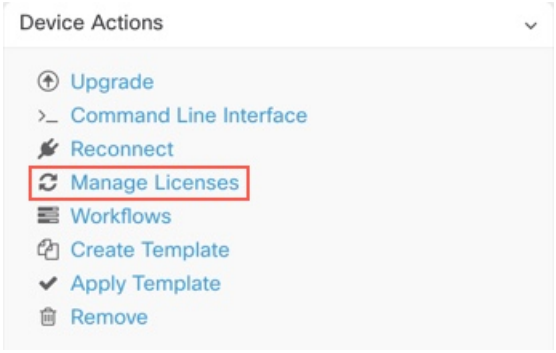
步骤 2 登录到该设备的 Firepower 设备管理器 并注销智能许可证。有关详细信息，请参阅取消注册智能许可的 FDM 管理 设备。

步骤 3 在 CDO 中，使用注册密钥再次载入 FDM 管理设备。有关详细信息，请参阅使用注册密钥载入 FDM 托管设备。使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+, on page 15

步骤 4 点击**设备 (Devices)** 选项卡以找到设备。

步骤 5 点击选项卡。

步骤 6 在载入过程中或通过查看右侧的**设备操作 (Device Actions)** 窗格并点击**管理许可证 (Manage Licenses)** 来应用新的智能许可证。



更改应用于使用其凭证载入的 FDM 管理 设备的智能许可证

Procedure

步骤 1 登录到该设备的 Firepower 设备管理器 并注销智能许可证。有关详细信息，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+。

步骤 2 将新的智能许可证应用于 Firepower 设备管理器 中的 FDM 管理 设备。

a. 点击**智能许可证 (Smart License)** 区域中的 **查看配置 (View Configuration)**。

b. 点击**立即注册 (Register Now)**，并按照屏幕上的说明执行操作。

步骤 3 在 CDO 中的**清单 (Inventory)** 页面上，点击**设备 (Devices)** 选项卡。

步骤 4 点击 **FTD** 设备。检查 FDM 管理 设备配置是否有更改，以便 CDO 可以复制 FDM 管理 设备的已部署配置并将其保存到 CDO 数据库。有关详细信息，请参阅读取、丢弃、检查和部署配置更改。

对 FDM 管理设备的 DHCP 寻址的 CDO 支持

如果我的 FDM 管理设备使用的 IP 地址发生更改会怎样？

Cisco Defense Orchestrator (CDO) 有许多自适应安全设备 (ASA) 和 FDM 管理设备客户，这些客户会使用其服务提供商使用 DHCP 提供的 IP 地址载入设备。

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，然后重新连接设备。

该字段表达了对由 CDO 管理的分支机构部署 FDM 管理设备的情况的担忧，FDM 管理设备的外部接口上需要静态 IP，在某些 SE 看来，当 FDM 管理设备具有为外部接口配置的 DHCP 地址。

但是，这种情况不会影响拥有通往远程分支机构防火墙的 VPN 隧道的客户，并且我们知道，绝大多数客户都拥有从分支机构到数据中心的站点到站点隧道。在使用站点间 VPN 从设备连接到中心站点的情况下，外部接口上的 DHCP 不是问题，因为 CDO（和任何管理平台）可以通过其内部静态寻址

的接口（如已配置）连接到 FW。这是建议的做法，我们的 CDO 客户有许多（+1000）设备都采用此部署模式。

此外，通过 DHCP 发布接口 IP 地址这一事实并不妨碍客户使用该 IP 来管理设备。同样，这并非最佳选择，但在 CDO 中必须定期更改 IP 地址的体验并未被视为对客户的障碍。这种情况并非 CDO 独有，任何使用外部接口（包括 ASDM、FDM 或 SSH）的管理器都存在这种情况。

FDM 管理 设备许可类型

智能许可证类型

下表介绍了 FDM 管理 设备可用的许可证。

购买 FDM 管理 设备会自动附带基本许可证。其他所有许可证均是可选的。

许可证	持续时间	授予的功能
许可证（自动包含）	永久	订用期限的许可证中未包括的所有功能。 您还必须还指定是否在使用此令牌注册的产品上允许出口控制功能。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。
	基于期限	**入侵检测和防御 (Intrusion detection and prevention)** - 入侵策略用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。 **文件控制 (File control)** - 文件策略用于检测和选择性地阻止用户上传（发送）或下载（接收）特定类型的文件。通过面向 Firepower 的 AMP（需要恶意软件许可证），您可以检查和阻止包含恶意软件的文件。必须拥有许可证才可使用任何类型的文件策略。 **安全情报过滤 (Security Intelligence filtering)** - 将选定流量丢弃后，通过访问控制规则对流量进行分析。动态源可用于根据最新情报立即丢弃连接。

许可证	持续时间	授予的功能
恶意软件	基于期限	检查恶意软件的文件策略，将思科高级恶意软件保护 (AMP) 与适用于 Firepower 的 AMP（基于网络的高级恶意软件保护）和思科 Threat Grid 结合使用。 文件策略可以检测和阻止通过网络传输的文件中的恶意软件。
URL 许可证	基于期限	基于类别和信誉的 URL 过滤。 您可以对单个 URL 执行 URL 过滤，而不使用此许可证。
	基于期限或永久，取决于许可证类型	远程接入 VPN 配置。您的基础版许可证必须允许出口控制功能，以便配置远程接入 RA VPN。在注册设备时，您需要选择是否满足出口要求。 Firepower 设备管理器可以使用任何有效的 AnyConnect 许可证。可用功能不因许可证类型不同而不同。如果尚未购买，请参阅《远程访问 VPN 的许可要求》。 此外，请参阅《思科 AnyConnect 订购指南》 http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。

虚拟 FDM 管理设备分层许可证

7.0 版引入了基于吞吐量要求和 RA VPN 会话限制的虚拟 FDM 管理设备性能分层智能许可支持。当虚拟 FDM 管理设备获得其中一个可用性能许可证的许可时，会出现两种情况：RA VPN 的会话限制由安装的虚拟 FDM 管理设备平台授权层确定，并通过速率限制器实施。

CDO 目前不完全支持分层智能许可；请参阅以下限制：

- 您无法通过 CDO 来修改分层许可证。您必须在 Firepower 设备管理器 UI 中进行更改。
- 如果注册由 云交付的防火墙管理中心 管理的虚拟 FDM 管理设备，则分层许可证选择会自动重置为**可变**，这是默认级别。
- 如果上载运行 7.0 或更高版本的虚拟 FDM 管理设备，并在上载过程中选择了**非**默认许可证的许可证，则分层许可证选择会自动重置为默认层级**可变**。

我们强烈建议您在载入设备后选择虚拟 FDM 管理设备许可证级别，以避免上述问题。有关详细信息，请参阅管理智能许可证。

查看设备的智能许可证

Procedure

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 **FTD** 选项卡。

步骤 4 选择 FDM 管理设备以查看其当前许可证状态。

步骤 5 在右侧的设备操作窗格中，点击管理许可证。**管理许可证 (Manage Licenses)** 屏幕提供以下信息：

- **只能许可证代理状态 (Smart License Agent status)**：显示您使用的是 90 天评估许可证，还是已注册到思科智能软件管理器。. 智能许可证代理状态可能如下：
  - **“已连接”(Connected)**、**“足够的许可证”(Sufficient Licenses)** - 设备已成功联系许可证颁发机构并向其注册，该机构已向设备授予许可证授权。设备现在处于合规状态。
  - **不合规 (Out-of-Compliance)** - 设备没有可用的许可证授权。许可功能可继续工作。但您可以购买或释放其他授权，以便变为合规状态。
  - **授权已过期 (Authorization Expired)** - 设备已连续 90 天或更长时间未与许可颁发机构通信。许可功能可继续工作。在此状态下，智能许可证代理将重试其授权申请。如果重试成功，代理会进入“不合规”(Out-of-Compliance) 或“已授权”(Authorized) 状态，并开始新的授权周期。尝试手动同步设备。
- **许可证注册 (License Registration)**：允许您将智能许可证应用于已载入的 FDM 管理设备。注册后，您可以查看与思科智能软件管理器的连接状态，以及各类许可证的状态。
- **许可证状态 (License Status)**：显示可用于您的 FDM 管理设备的可选许可证的状态。您可以启用许可证以便使用该许可证控制的功能。

启用或禁用可选许可证

您可以在使用 90 天评估许可证或完整许可证的 FDM 管理设备上启用（注册）可选许可证。只有启用许可证后，才能使用该许可证控制的功能。

如果您不想再使用某个可选期限许可证包含的功能，可以禁用（解除）该许可证。禁用许可证会在思科智能软件管理器账户中将其释放，以便可将其应用到其他设备。

在评估模式下，您还可以启用可选许可证的评估版本并执行所有操作。在该模式下，只有注册设备，许可证才会注册到思科智能软件管理器。

Note 您无法在评估模式下启用许可证。

Before you begin

在禁用许可证之前，请确保它不在使用中。重写或删除需要该许可证的任何策略。

对于在高可用性配置中运行的设备，只需在主用设备上上启用或禁用许可证。当备用设备请求（或释放）必要许可证时，更改会在下一次部署配置时反映在备用设备上。启用许可证时，必须确保思科智能软件管理器账户具有足够的许可证，否则可能会造成一台设备合规，而另一台设备不合规。

要启用或禁用可选许可证，请执行以下程序：

Procedure

步骤 1 在**清单 (Inventory)**页面中，选择所需的 FDM 管理设备，然后点击**设备操作 (Device Actions)** 窗格中的**管理许可证 (Manage Licenses)**，系统将显示**管理许可证 (Manage Licenses)** 屏幕。

步骤 2 根据需要，点击每个可选许可证的滑块控件。一旦启用，许可证的状态显示为“正常”(OK)。

- **已启用 (Enabled)**：将许可证注册到您的思科智能软件管理器帐户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **已禁用 (Disabled)**：取消许可证向思科智能软件管理器帐户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。

步骤 3 点击 **Save** 保存所做的更改。

可选许可证过期或被禁用的影响

如果可选许可证过期，您可以继续使用需要该许可证的功能。但是，该许可证将被标记为不合规，您需要购买许可证并将其添加到您的账户，才能使该许可证恢复合规状态。

如果禁用了某个可选许可证，系统将做出如下反应：

- **恶意软件许可证 (Malware license)**：系统会停止查询 AMP 云，还会停止确认从 AMP 云发送的追溯性事件。如果现有访问控制策略包括的文件策略会应用恶意软件检测，则无法重新部署现有访问控制策略。请注意，在禁用恶意软件许可证后的很短时间内，系统可以使用现有缓存文件处置情况。在时间窗过期后，系统将向这些文件分配不可用的处置情况。
- ：系统将不再应用入侵或文件控制策略。对于安全情报策略，系统不再应用策略并停止下载情报源更新。您无法重新部署需要该许可证的现有策略。
- **URL**：带有 URL 类别条件的访问控制规则会立即停止过滤 URL，且系统不会再下载对 URL 数据的更新。如果现有访问控制策略包括的规则带有基于类别和信誉的URL条件，则不能重新部署现有的访问控制策略。

- ：您不能编辑远程访问 VPN 配置，但可以将其删除。用户仍可使用 RA VPN 配置进行连接。但是，如果您更改设备注册，致使系统不再符合导出规定，则远程访问 VPN 配置会立即停止，且所有远程用户都无法通过 VPN 进行连接。

创建和导入 防火墙设备管理器 模型

思科防御协调器 提供将 CDO 租户上 FDM 管理设备的完整配置导出为 JSON 文件格式的功能。然后，您可以将此文件作为一个防火墙设备管理器模型导入到另一个租户，并将其应用于该租户上的新设备。当您想要在您管理的不同租户上使用 FDM 管理设备的配置时，此功能非常有用。

Note 如果 FDM 管理设备包含规则集，则在导出配置时，与规则集关联的共享规则将被修改为本地规则。稍后，当模型导入到另一个租户并应用于 FDM 管理设备时，您将在设备中看到本地规则。

导出 FDM 管理设备配置

如果您的 FDM 管理设备具有以下配置，则导出配置功能不可用：

- 高可用性
- Snort 3 已启用

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

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

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择一个 FDM 管理设备，然后在右侧窗格的**设备操作 (Device Actions)** 中，点击**导出配置 (Export Configuration)**。

导入 FDM 管理 设备配置

Procedure

步骤 1 在**清单 (Inventory)** 页面中，点击蓝色加号 (+) 按钮以导入配置。

步骤 2 点击**导入 (Import)** 以便导入配置进行离线管理。

步骤 3 选择设备类型作为 FTD。

步骤 4 点击**浏览 (Browse)** 并选择要上传的配置文件（JSON 格式）。

步骤 5 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，请参阅标签和标签组。

步骤 6 标记型号设备后，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。

从CDO删除设备

使用以下程序可从 中删除设备：CDO

过程

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。

请注意，必须同时删除 HA 对中的两台设备。FDM 管理点击 HA 对名称，而不是单个对等体。FDM 管理

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)。
- Firepower 威胁防御 (FTD)。请参阅创建和导入 FTD 模型。
- 像汇聚服务路由器 (ASR) 和集成服务路由器 (ISR) 的 Cisco IOS 设备。

备份 FDM 管理 设备

您可以使用 备份设备的系统配置，以便可以将设备恢复到以前的状态。思科防御协调器FDM管理备份仅包括配置，而不是系统软件。如果需要完全重新映像设备，您需要重新安装软件，然后才能上传备份和恢复配置。CDO 会保存设备的最近 5 次备份。进行新的备份时，会删除最早的备份，以便存储最新的备份。

Note 备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。

在备份期间将锁定配置数据库。在备份期间不能更改配置，但可以查看策略、控制面板等。在恢复期间，系统完全不可用。

要使设备之间的备份计划一致，您可以配置自己的默认备份计划。为特定设备安排备份时，可以使用自己的默认设置或进行更改。您可以安排定期备份，频率从每天到每月一次，并且可以执行按需备份。您还可以下载备份，然后使用设备管理器进行恢复。威胁防御

使用 CDO 备份和恢复 FDM 管理 设备的要求和最佳实践

- 可以备份运行 6.5 及更高版本软件的设备。CDOFDM 管理
- 设备必须使用注册密钥自行激活。FDM 管理CDO
- 仅当两台设备的型号相同且运行相同版本的软件（包括内部版本号，而不仅仅是相同的发布版）时，才可将备份恢复到替换设备上。例如，运行软件版本 6.6.0-90 的设备的备份只能恢复到运行 6.6.0-90 的设备。FDM 管理FDM 管理请勿使用备份和恢复过程在设备之间复制配置。备份文件包含唯一标识设备的信息，所以不能按此方式进行共享。
- 要在 CDO 中使用 Secure Firewall Threat Defense 备份功能，威胁防御 需要根据您的租户区域访问这些 CDO URL 之一。
  - edge.us.cdo.cisco.com
  - edge.eu.cdo.cisco.com
  - edge.apj.cdo.cisco.com
- 确保端口 443 具有 HTTPS 协议的外部和出站访问权限。如果端口被防火墙阻止，备份和恢复过程可能会失败。

最佳实践

您要备份的设备应处于已同步状态。 会从 设备备份设备的配置，而不是从中备份设备的配置。CDOCDOCDO因此，如果设备处于“未同步”状态，则不会备份上的更改。CDO如果设备处于“检测到冲突”状态，系统将备份这些更改。

相关信息：

- 为所有 FDM 管理的设备配置默认定期备份计划
- 为单个设备配置定期备份计划FDM 管理
- 按需备份设备FDM 管理
- 下载设备备份
- 编辑备份
- 将备份恢复到设备FDM 管理, on page 48

按需备份设备FDM 管理

此程序介绍如何备份设备，以便在需要时可以将其恢复。FDM 管理

准备工作

在备份设备之前，请查看这些要求和最佳实践。备份 FDM 管理 设备, on page 43FDM 管理

操作步骤

Procedure

步骤 1 （可选）为备份创建更改请求。

步骤 2 在导航栏中，点击**清单 (Inventory)**。

步骤 3 点击**设备**选项卡。

步骤 4 点击 **FTD** 选项卡，然后选择要备份的设备。

步骤 5 在右侧的设备操作窗格中，点击管理备份。

步骤 6 单击**立即备份 (Backup Now)**。设备进入“备份配置”状态。

在备份完成后，思科防御协调器 会显示备份开始前的设备配置状态。您还可以打开更改日志页面，查找描述为“备份已成功完成”(Backup completed successfully) 的最新更改日志记录。

如果在步骤 1 中创建了更改请求，则您还可以按该值进行过滤以查找更改日志条目。

步骤 7 如果在步骤 1 中创建了更改请求，请清除更改请求值，以免在无意中将更多更改与更改请求关联。

为单个设备配置定期备份计划FDM 管理

准备工作

在备份设备之前，请查看这些要求和最佳实践。备份 FDM 管理 设备, on page 43FDM 管理

操作步骤

Procedure

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 **FTD** 选项卡，然后选择要备份的设备。

步骤 4 在右侧的设备操作窗格中，点击管理备份。

步骤 5 在**设备备份 (Device Backups)** 页面中，点击**设置定期备份 (Set Recurring Backup)** 或点击定期备份字段中的计划。CDO 显示租户上所有 FDM 管理设备的默认备份计划。有关详细信息，请参阅为所有 FDM 托管设备配置默认定期备份计划。

步骤 6 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) 来安排时间。

步骤 7 在频率 (Frequency) 字段中，选择每日、每周或每月备份。

- 每日备份 (Daily backups)：为计划的备份时间指定名称和说明。
- 每周备份 (Weekly backups)：选中要在星期几进行备份。为计划的备份时间指定名称和说明。
- 每月备份 (Monthly backups)：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 8 点击**保存 (Save)**。请注意，在“设备备份”(Device Backup) 页面上，定期备份字段将替换为您设置的备份计划，并反映您的本地时间。

下载设备备份

此程序介绍如何下载包含设备备份的 .tar 文件。FDM 管理

Procedure

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 FTD 选项卡和要下载其备份的设备。

步骤 4 在右侧的操作窗格中，点击管理备份。

步骤 5 选择要下载的备份，然后在其行中点击生成下载链接 (Generate Download Link) 按钮。按钮更改为“下载备份映像”。

步骤 6 该按钮现在显示为“下载备份映像”。执行以下操作之一：

- 如果您使用的设备也可以访问要恢复的设备的防火墙设备管理器，请点击**下载备份映像 (Download Backup Image)** 按钮并保存下载的文件。使用您会记住的名称保存它。
- 如果您不在可以访问要恢复的设备的 FDM 的设备上：

  a. 右键点击 Download Backup Image（下载备份映像）按钮，然后复制链接地址。

  Important 点击“生成下载链接”(Generate Download Link) 按钮 15 分钟后，链接地址将到期。

  b. 在也将访问要将映像恢复到的 Secure Firewall Threat Defense 的 防火墙设备管理器 设备上打开浏览器。

c. 在浏览器地址栏中输入下载链接，并将备份文件下载到该设备。使用您会记住的名称保存它。

编辑备份

此程序允许您编辑成功下载设备的名称或说明。FDM 管理

Procedure

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 **FTD** 选项卡，然后选择要编辑的设备。

步骤 4 在右侧的操作窗格中，点击管理备份。

步骤 5 选择要编辑的备份及其所在的行，点击编辑图标。

步骤 6 更改备份的名称或说明。您可以在“设备备份”页面中查看新信息。

删除备份

CDO 会保存为设备所进行的最后 5 次备份。进行新的备份时，会删除最早的备份，以便存储最新的备份。删除现有备份可帮助您管理保留和删除的备份。

Procedure

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 **FTD** 选项卡，然后选择要删除的设备。

步骤 4 在右侧的操作窗格中，点击管理备份。

步骤 5 选择要删除的备份及其所在的行，点击垃圾箱图标 。

步骤 6 点击**确定 (OK)** 以进行确认。

管理设备备份

可以在“设备备份”(Device Backups) 页面中查看您使用 思科防御协调器 的 FDM 管理设备的备份：

Procedure

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 **FTD** 选项卡。

步骤 4 点击过滤器图标并选中设备/服务下的 FDM，以仅查看设备表中的 FDM 管理设备。

步骤 5 选择所需的设备。

步骤 6 在**设备操作 (Device Actions)** 窗格中，点击**管理备份 (Manage Backups)**。您最多将看到该设备的 5 个最新备份。

What to do next

如果要恢复备份，请参阅将备份恢复到设备FDM 管理, on page 48。

将备份恢复到设备FDM 管理

在恢复受管设备的备份之前，请查看此信息。FDM 管理威胁防御

- 在将备份恢复到设备之前，请查看这些要求和最佳实践。备份 FDM 管理 设备, on page 43FDM 管理 威胁防御
- 如果设备中没有要恢复的备份副本，必须先**上传**该备份，才能进行恢复。
- 在恢复期间，系统完全不可用。恢复备份后，设备会重新启动。
- 此程序假定您已准备好将设备备份到 设备。
- 当设备属于高可用性对的一部分时，您无法恢复备份。您必须首先从“设备”(Device)>“高可用性”(High Availability) 页面中断高可用性，然后才能恢复备份。如果备份包括高可用性配置，设备将重新加入高可用性组。不要在两台设备上恢复相同备份，因为这两台设备都会变成活动状态。相反，您要在想要首先恢复活动状态的设备上恢复备份，然后在另一台设备上恢复等效备份。

Note 备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。

Procedure

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 **FTD** 选项卡，然后选择要恢复的设备。

步骤 4 在右侧的设备操作窗格中，点击管理备份。

步骤 5 选择您要恢复的备份。在相应行中，点击生成下载链接 (Generate Download Link) 按钮。

Note 点击“生成下载链接”(Generate Download Link) 按钮 15 分钟后，链接地址将到期。

步骤 6 该按钮现在显示为“下载备份映像”。执行以下操作之一：

- 如果您使用的设备也可以访问要恢复的设备的防火墙设备管理器，请点击**下载备份映像 (Download Backup Image)** 按钮并保存下载的文件。使用您会记住的名称保存它。
- 如果您不在可以访问要恢复的设备的 防火墙设备管理器 的设备上：
  a. 右键点击 Download Backup Image（下载备份映像）按钮，然后复制链接地址。
  b. 在也将访问要将映像恢复到的 防火墙设备管理器 的设备上打开浏览器。
  c. 在浏览器地址栏中输入下载链接，并将备份文件下载到该设备。使用您会记住的名称保存它。

步骤 7 登录您要恢复的设备的 防火墙设备管理器。

步骤 8 打开 6.5 或更高版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》。导航至“系统管理”一章，然后搜索恢复备份。按照这些说明恢复您刚下载到设备的映像。FDM 管理

Tip 您需要将映像上传到 防火墙设备管理器 才能恢复映像。

步骤 9 按照 防火墙设备管理器 中的提示操作。恢复开始时，浏览器会断开与 防火墙设备管理器 的连接。恢复完成后，设备将重新启动。

相关信息：

- 备份 FDM 管理 设备
- 按需备份设备FDM 管理
- 为单个设备配置定期备份计划FDM 管理
- 下载设备备份
- 编辑备份

FDM 软件升级路径

升级 FDM 版本

如果您使用 CDO 升级您的 FDM 管理 防火墙，CDO 会确定您可以升级到哪个版本，您将不需要本主题。如果您维护自己的 FDM 映像存储库并使用自己的映像升级 FDM 托管的设备，则本主题将介绍可用的升级路径。

您可以将 FDM 托管的设备直接从一个主要版本或维护版本升级到另一个版本；例如，版本 6.4.0 > 6.5.0 或版本 6.4.0 > 7.0.1。您不需要运行任何特定级别的补丁。

如果无法直接升级，则升级路径必须包括中间版本，例如版本 6.4.0 > 7.0.0 > 7.1.0。

Table 3: 主要版本的升级路径

目标版本	可以升级到目标版本的最旧版本
7.3.x	7.0.0
7.2.x	6.6.0
7.1.x	6.5.0
7.0.x	6.4.0
6.7.x	6.4.0
6.6.x	6.4.0
6.5.0	6.4.0

修补 FDM 托管的设备

您无法直接从一个版本的修补程序升级到另一个版本的修补程序，例如从版本 6.4.0.1 > 6.5.0.1。您必须先升级到主要版本，然后再修补该版本。例如，您必须从版本 6.4.0.1 升级 > 6.5.0 > 6.5.0.1。

Firepower 热补丁

CDO 不支持修补程序更新或安装。如果有适用于您的设备型号或软件版本的热补丁，我们强烈建议使用已配置的管理器控制面板或 UI。在设备上安装热补丁后，CDO 会检测到带外配置更改。

删除 FDM 升级

您不能使用 CDO 删除或降级任何版本类型，无论是主版本、维护版本还是补丁。

从 Secure Firewall Threat Defense 版本 6.7.0 开始，您可以使用 Firepower 设备管理器或 FTD CLI 将成功升级的设备恢复到上次主要或维护升级之前的状态（也称为快照）。修补后恢复必然也会删除修补程序。恢复后，您必须重新应用在**升级**和恢复之间所做的任何配置更改。**请注意，要将主要或维护升级恢复到 FDM 版本 6.5.0 至 6.6.x，必须重新映像**。有关更多信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中的“系统许可”一章。

删除 FDM 补丁

您无法使用 CDO 或 FDM 删除 FDM 补丁。要删除修补程序，必须重新映像到主版本或维护版本。

Snort 升级

Snort 是产品的主要检测引擎，为了您的方便，它已打包到 Secure Firewall Threat Defense 软件中。版本 6.7 引入了可随时升级或恢复的软件包更新。虽然可以自由切换 Snort 版本，但 Snort 2.0 中的某些

入侵规则未在 Snort 3.0 中提供，反之亦然。我们强烈建议阅读《适用于版本 6.7.0 的 Firepower 设备管理器配置指南》中的差异，以了解详细信息。

要继续升级 FDM 管理 设备以使用 Snort 3 或从 CDO UI 从 Snort 3 恢复到 Snort 2，请分别参阅 升级到 Snort 3.0 和从 Snort 3.0 恢复 FDM 管理 设备。

其他升级限制

2100 系列设备

仅当运行设备模式时，CDO 才能升级 Firepower 2100 系列设备。

- Firepower 威胁防御设备始终处于设备模式。

下一步做什么

有关这些命令的更详细讨论，请参阅《思科 Firepower 2100 入门指南》。https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp2100/firepower-2100-gsg/asa-platform.html

4100 和 9300 系列设备

CDO 不支持 4100 或 9300 系列设备的升级。您必须在 CDO 之外升级这些设备。

相关信息：

- FDM 管理 设备升级前提条件
- 升级单个 FTD 设备
- 批量 FDM 管理 设备升级
- 升级 FDM 管理 高可用性对

FDM 管理 设备升级前提条件

思科防御协调器 (CDO) 提供了一个向导，可帮助您升级单个设备或 HA 对上安装的 防火墙设备管理器 (FDM) 映像。

该向导将指导您选择兼容的映像，安装这些映像，然后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您的 FDM 管理 设备上的映像，从而确保升级过程的安全。我们强烈建议您要升级的 FDM 管理 设备具有对互联网的出站访问权限。

如果您的FDM 管理 设备没有互联网出站访问权限，您可以从Cisco.com下载所需的映像，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使用这些映像执行升级。但是，在这种情况下，您需要确定要升级到的映像。CDO 不会执行映像完整性检查或磁盘空间检查。

配置必备条件

- 需要在 FDM 管理 设备上启用 DNS。有关详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中**系统管理**一章的“配置 DNS”部分。
- 如果您使用 CDO 的映像存储库中的升级映像， FDM 管理 设备应该能够访问互联网。
- FDM 管理 设备已被成功载入 CDO。
- FDM 管理 设备无法访问。
- FDM 管理 设备已同步。
  - 如果您更新的设备在CDO中有待处理的更改，并且您不接受更改，则在升级完成后，待处理的更改将会丢失。最佳实践是在升级之前部署所有待处理的更改。
  - 如果您在 防火墙设备管理器 中暂存了更改，并且设备未同步，则 CDO 中的升级将在资格检查时失败。

运行 FTD 的 4100 和 9300 系列

CDO 不支持 4100 或 9300 系列设备的升级。您必须在 CDO 外部升级这些设备。

软件和硬件要求

CDO 云管理平台。软件更新随时间推移而发布，通常不依赖于硬件。有关支持的硬件类型的信息，请参阅 CDO 支持的软件和硬件。

运行防火墙设备管理器软件的设备具有推荐的升级路径，以实现最佳性能。有关详细信息，请参阅 FDM 软件升级路径。

升级说明

您无法在设备升级时将更改部署到设备。

相关信息：

- FDM 软件升级路径
- 升级单个 FTD 设备
- 批量 FDM 管理 设备升级
- 升级 FDM 管理 高可用性对

升级单个 FTD 设备

准备工作

在升级之前，请务必仔细阅读 FDM 管理 设备升级前提条件、FDM 软件升级路径以及 CDO 支持的软件和硬件。本文档介绍了在升级到所需的 Firepower 软件版本之前应了解的所有要求和警告。

使用 思科防御协调器 存储库中的映像升级单个 FDM 管理 设备

按照以下程序使用存储在 CDO 存储库中的软件映像升级独立 FDM 管理 设备

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择想要升级的设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 6 在步骤 1 中，点击**使用 CDO 映像存储库 (Use CDO Image Repository)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。

步骤 7 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，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)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，CDO 不会部署或检查设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

步骤 9 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 10 查看通知选项卡，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 11 升级系统数据库。您必须在 防火墙设备管理器 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

使用您自己的存储库中的映像升级单个设备FDM 管理

按照以下程序升级使用 URL 协议的独立设备以查找软件映像：FDM 管理

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择想要升级的设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 6 在步骤 1 中，点击**指定映像 URL (Specify Image URL)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。

步骤 7 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，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)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，思科防御协调器 不会部署或检查设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

步骤 9 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 10 查看通知选项卡，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 11 升级系统数据库。您必须在 防火墙设备管理器 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

监控升级过程

您可以通过在“资产”页面上选择该设备并点击升级按钮来查看单个设备的进度。CDO会将您引导至该设备的“设备升级”页面。

只要升级失败，CDO 就会显示一条消息。CDO 不会自动重新启动升级过程。

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，请参阅检测到新证书

批量 FDM 管理 设备升级

准备工作

在升级之前，请务必仔细阅读 FDM 管理 设备升级前提条件、FDM 软件升级路径以及 CDO 支持的软件和硬件。本文档介绍在升级到所需的 Firepower 软件版本之前应了解的所有要求和警告。

Note 仅当设备都升级到同一软件版本时，才能批量升级 FDM 管理 设备。

使用 思科防御协调器 存储库中的映像升级批量 FDM 管理 设备

按照以下程序使用存储在 CDO 存储库中的软件映像升级多个 FDM 管理 设备：

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 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 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 9 在步骤 1 中，点击**使用 CDO 映像存储库 (Use CDO Image Repository)** 以选择要升级到的软件映像。系统只会显示与您可以升级的设备兼容的选项。点击**继续 (Continue)**。

步骤 10 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，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)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果您在升级开始后取消升级，CDO不会部署或轮询设备中的更改。取消升级后，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

步骤 12 查看通知选项卡，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 13 升级系统数据库。您必须在防火墙设备管理器中执行此步骤。有关设备运行的版本，请参阅《适用于 Firepower 设备管理器的 Cisco Firepower Threat Defense 配置指南》中的**更新系统数据库**。

使用您自己的存储库中的映像升级批量 FDM 管理 设备

按照以下程序使用 URL 协议升级多个 FDM 管理 设备以查找软件映像：

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 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，思科防御协调器 会为您提供一个链接，供您查看不可升级的设备。

步骤 8 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 9 在步骤 1 中，点击**指定映像 URL (Specify Image URL)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。

步骤 10 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，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)**。在**资产**页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的**中止升级**。如果在升级开始后取消升级，CDO不会部署或轮询设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科TAC。

步骤 12 查看通知选项卡，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 13 升级系统数据库。您必须在 防火墙设备管理器 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

监控批量升级过程

您可以通过在**资产**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。您还可以通过点击导航窗格中的**作业**并展开批量操作来查看进度详细信息。

只要升级失败，CDO 就会显示一条消息。CDO 不会自动重新启动升级过程。

升级 FDM 管理 高可用性对

在不中断流量的情况下升级 HA 对；备用设备在升级辅助设备时继续处理流量检测。

升级 HA 对时，CDO 会执行资格检查并在开始升级之前复制或识别映像位置。高可用性对中的辅助设备首先升级，即使它当前是主用设备；如果辅助设备是主用设备，则配对的设备会自动切换升级过程的角色。辅助设备成功升级后，设备会切换角色，然后新的备用设备会升级。升级完成后，设备会自动配置，因此主用设备处于活动状态，辅助设备处于备用状态。

我们不建议在升级过程中部署到 HA 对。

准备工作

- 在升级之前，将所有待处理的更改部署到主用设备。
- 确保在升级期间没有正在运行的任务。
- 高可用性对中的两台设备都运行正常。
- 确认您已准备好升级；您无法在 CDO 中回滚到以前的版本。
- 仔细阅读 FDM 管理 设备升级前提条件、FDM 软件升级路径以及 CDO 支持的软件和硬件以查看在升级过程中可能出现的任何要求和警告。

使用 思科防御协调器 存储库中的映像升级 FDM 管理 HA 对

按照以下程序使用存储在 CDO 存储库中的软件映像升级 FDM 管理 HA 对：

Procedure

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 **FTD** 选项卡。

步骤 4 选择要升级的 HA 对。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 6 在步骤 1 中，点击**使用 CDO 映像存储库 (Use CDO Image Repository)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。

步骤 7 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，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)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，CDO不会从设备部署或轮询更改，并且设备不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科TAC。

步骤 9 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 10 查看通知选项卡，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 11 升级系统数据库。您必须在 FDM 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

使用您自己的存储库中的映像升级 HA 对FDM 管理

按照以下程序使用 URL 协议升级 HA 对以查找软件映像：FDM 管理

Procedure

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 **FTD** 选项卡。

步骤 4 选择要升级的 HA 对。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 6 在步骤 1 中，点击**指定映像 URL (Specify Image URL)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。

步骤 7 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，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)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，思科防御协调器 不会从设备部署或轮询更改，并且设备不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

步骤 9 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 10 查看通知选项卡，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 11 升级系统数据库。您必须在 防火墙设备管理器 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

监控升级过程

您可以通过在**清单 (Inventory)** 页面上选择该设备并点击升级按钮来查看单个设备的进度。思科防御协调器 会带您前往该设备的**设备升级 (Device Upgrade)** 页面。

升级期间，系统在更新系统库时挂起HA，其中包括自动部署，而且在整个升级过程中可能都不会处于正常运行状态。这是预期行为。在此过程的最后部分中，设备可用于SSH连接，因此，如果在应用升级后不久登录，则可能会看见挂起状态的HA。如果系统在升级过程中遇到问题，并且HA对似乎已暂停，请从主用设备的 防火墙设备管理器 控制台手动恢复 HA。

Note 如果升级在任何时候失败，CDO 会显示一条消息。CDO 不会自动重新启动升级过程。

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，请参阅检测到新证书。

升级到 Snort 3.0

Snort 3 是使用开源入侵防御系统 (IPS) 的最新 snort 引擎或强大的预处理器，适用于 Firepower 版本 6.7 及更高版本。Snort 引擎使用一系列规则来帮助定义恶意网络活动，并使用这些规则查找与其匹配的数据包，并为用户生成警报，理想情况下用作数据包嗅探器、数据包记录器或更传统的 aa独立网络 IPS。

使用 Snort 3，您现在可以创建自定义入侵策略；每个运行 Snort 3 的 FDM 管理 设备都有一组从思科 Talos 情报组 (Talos) 预定义的入侵策略。Snort 3 可以更改这些默认策略，但我们强烈建议在基本策略的基础上进行构建，以获得更强大的策略。

您无法使用 Snort 2 创建自定义策略。

从 Snort 2 切换到 Snort 3

您可以自由切换 Snort 版本，虽然 Snort 2.0 中的某些入侵规则未在 Snort 3.0 中提供，反之亦然。如果对现有规则更改了规则操作，则在从 Snort 3 切换到 Snort 2 或再次切换回 Snort 3 时，不会保留该更改。您对两个版本中现有规则的规则操作更改都将被保留。请注意，Snort 3 与 Snort 2 中的规则之间的映射可以是一对一或一对多的，因此系统将尽可能保留更改。

如果您选择从 Snort 2 升级到 Snort 3，请注意，升级 Snort 引擎相当于系统升级。我们强烈建议在维护窗口期间进行升级，以最大限度地减少网络流量监控的中断。有关切换snort版本将如何影响规则处理流量的方式，请参阅《*Firepower* 设备管理器配置指南》中的管理入侵策略 (Snort3) 。

Tip 您可以在**清单 (Inventory)** 页面上按 Snort 版本进行过滤，所选设备的详细信息窗口将显示设备上运行的当前版本。

Snort 3 限制

许可证要求

要允许 Snort 引擎处理流量以进行入侵和恶意软件分析，必须为 FDM 管理 设备启用 **许可证**。要通过 防火墙设备管理器 启用此许可证，请登录 防火墙设备管理器 UI 并导航至 **设备 (Device)** > **视图配置 (View Configuration)** > **启用/禁用 (Enable/Disable)**，然后启用 许可证。

硬件支持

以下设备支持 Snort 3：

- FTD 1000 系列
- FTD 2100 系列
- FTD 4100 系列
- FTD 虚拟与 AWS
- FTD 虚拟与 Azure
- 具备 FTD 的 ASA 5500-X 系列

软件支持

设备**必须**至少运行 防火墙设备管理器 版本 6.7。思科防御协调器 支持运行版本 6.7 及更高版本的设备的 Snort 3 功能。

对于 FTD 1000 和 2000 系列，请参阅 FXOS 捆绑支持，了解有关 FXOS 补丁支持的详细信息。

配置限制

如果您的设备具有以下配置，CDO 不支持升级到 Snort 3：

- 设备未运行至少版本 6.7。
- 如果设备有待处理的更改。在升级之前部署任何更改。
- 如果设备当前正在升级。在设备同步之前，请勿尝试升级或部署到设备。
- 如果设备配置了虚拟路由器。

Note 如果升级或恢复 Snort 版本，系统会自动部署以实施 Snort 2 入侵策略和 Snort 3 入侵策略之间的更改。

规则集和 Snort 3

请注意，Snort 3 目前没有完整的功能支持。CDO 规则集在 Snort 3 设备上不支持。如果您同时将设备升级到 防火墙设备管理器 6.7 或更高版本，并从 Snort 2 升级到 Snort 3，则在升级之前配置的任何规则集都将被分解，其中的规则将另存为单独的规则。

有关为 Snort 3 配置的设备的完整规则集支持列表，请参阅规则集。

同时升级设备和入侵防御引擎

CDO 允许您将设备升级到版本 6.7 和 Snort 3。使用以下程序升级 FTD 系统：

Procedure

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 **FTD** 选项卡，然后选择要升级的设备。

步骤 4 在右侧的**设备操作 (Devices Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 5 将升级切换开关设置为 FTD 系统升级。

步骤 6 （可选）如果您希望 CDO 稍后执行升级，请选中**计划升级 (Schedule Upgrade)** 复选框。点击该字段以选择未来的日期和时间。

步骤 7 在步骤 1 中，选择升级方法。使用 CDO 映像存储库和您自己的存储库中的映像：

- **使用 CDO 映像存储库 (Use CDO Image Repository)** - 点击此选项可选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。
- 指定映像 URL - 点击此选项可选择当前存储在您自己的存储库中的软件映像，然后点击继续。系统只会显示与您可以升级的设备兼容的选项。

步骤 8 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，还是复制映像、安装并重新启动设备。

步骤 9 选中升级到 Snort 3 引擎。

步骤 10 准备就绪后，点击**执行升级 (Perform Upgrade)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，CDO不会部署或检查设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科TAC。

升级入侵防御引擎

对于已运行版本 6.7 和 Snort 2 的设备，请使用以下程序将 Snort 引擎更新为版本 3：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

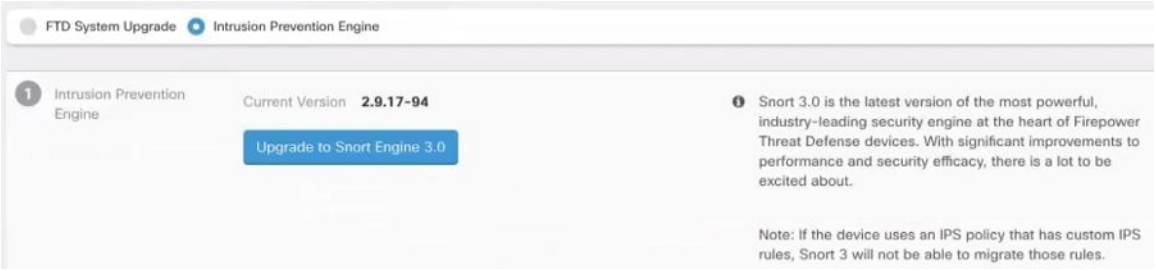
步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要升级的设备。

步骤 4 在右侧的**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 5 将升级切换开关设置为入侵防御引擎。

步骤 6 点击 **升级到 Snort Engine 3.0 (Upgrade to Snort Engine 3.0)**。



步骤 7 在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

监控升级过程

警告 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，CDO 不会部署或检查设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

您可以通过在“资产”页面上选择该设备并点击升级按钮来查看单个设备的进度。CDO 会将您引导至该设备的“设备升级”页面。

只要升级失败，CDO 就会显示一条消息。CDO 不会自动重新启动升级过程。

警告 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，请参阅检测到新证书

从 Snort 3.0 恢复 FDM 管理 设备

Snort 3.0 中可能不存在 Snort 2.0 中的某些入侵规则。如果降级到 2.0，您创建的所有自定义入侵策略都将转换为自定义策略中使用的基本策略。尽可能保留“覆盖”规则操作。如果多个自定义策略使用相同的基本策略，则系统将保留大多数访问控制策略中使用的自定义策略“覆盖”操作，而其他自定义策略的“覆盖”操作将丢失。现在，使用这些“重复”策略的访问控制规则将使用根据最常用自定义策略创建的基本策略。所有自定义策略都将被删除。

在您选择从 Snort 3.0 恢复之前，请阅读《 *Firepower* 设备管理器配置指南》中的管理入侵策略 (Snort2)，同时了解切换 Snort 引擎版本将如何影响您当前的规则和策略。

Note 恢复为版本 2 不会卸载 Firepower 软件版本。

从 Snort 3.0 恢复

如果更改 Snort 版本，系统将执行自动部署以实施更改。请注意，您只能将单个设备从 Snort 3.0 恢复到版本 2。

使用以下程序恢复入侵防御引擎：

Procedure

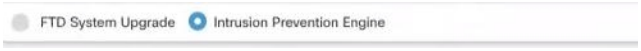
步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

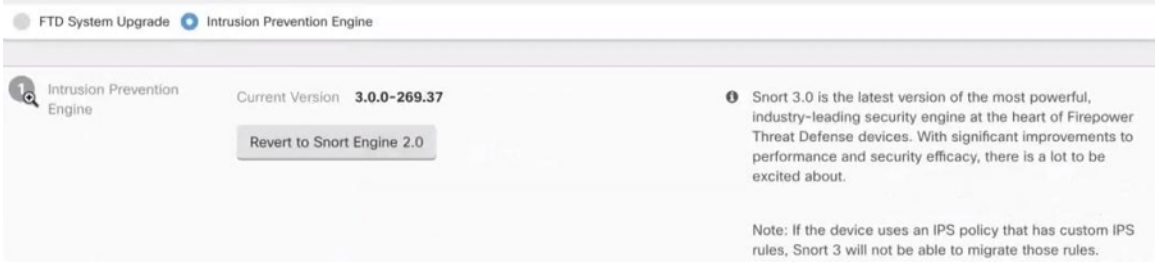
步骤 3 点击 **FTD** 选项卡，然后点击要恢复的设备。

步骤 4 在右侧的**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 5 将升级切换开关设置为**入侵防御引擎**。



步骤 6 在步骤 1 中，确认要从 Snort 版本 3 恢复，然后点击**恢复到 Snort 引擎 2**。



步骤 7 在**资产**页面中，正在升级的设备具有“正在进行升级”配置状态。

安排安全数据库更新

使用以下程序创建一个计划的任务，以检查和更新 FTD 设备的安全数据库：

Procedure

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 **FTD** 选项卡，然后选择所需的 FTD 设备。

步骤 4 在操作窗格中，找到**安全数据库更新 (Security Database Updates)** 部分，然后点击添加 **+** 按钮。

Note 如果所选设备已存在计划任务，请点击编辑图标创建新任务。创建新任务将覆盖现有任务。

步骤 5 使用以下内容配置计划任务：

- **频率 (Frequency)** - 选择每天、每周或每月进行更新。
- **时间 (Time)** - 选择每天的某个时间。请注意，显示的时间为 UTC。
- **选择天数 (Select Days)** - 选择您希望在一周内的哪一天进行更新。

步骤 6 点击**保存 (Save)**。

步骤 7 设备的配置状态将更改为“正在更新数据库”(Updating Databases)。

编辑计划安全数据库更新

使用以下程序编辑现有的计划任务，以检查和更新 FTD 设备的安全数据库

Procedure

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 **FTD** 选项卡，然后选择所需的 FTD 设备。

步骤 4 在“操作”(Actions) 窗格中，找到**数据库更新 (Database Updates)** 部分，然后点击编辑图标。

步骤 5 使用以下命令编辑计划任务：

- **频率 (Frequency)** - 选择每天、每周或每月进行更新。
- **时间 (Time)** - 选择每天的某个时间。请注意，显示的时间为 UTC。
- **选择天数 (Select Days)** - 选择您希望在一周内的哪一天进行更新。

步骤 6 点击**保存 (Save)**。

步骤 7 设备的配置状态将更改为“正在更新数据库”(Updating Databases)。

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。