将 FTD 载入 云交付的防火墙管理中心

阅读以下信息，了解载入的前提条件和程序。

载入概述

查看 云交付的防火墙管理中心 支持的型号和使用案例。

支持的设备

您可以字啊如以下设备型号：

- Firepower 1000 系列
- Firepower 2100 系列
- Secure Firewall 3100 系列
- Firepower 4100 系列
- Firepower 9300 系列
- ISA 3000
- 虚拟Secure Firewall Threat Defense

支持的使用案例

云交付的防火墙管理中心 目前支持以下设备的载入场景：

- 设备必须运行版本 7.0.3 或 7.2.0 以及更高版本。要查看所有支持的版本和产品兼容性，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》以了解详细信息。

- 配置为由 设备管理器 进行本地管理的设备。在载入之前，设备可能已登录，也可能未登录。对于尚未登录的设备，您可以通过通过低接触调配激活设备来载入设备。

注释 如果您将 FDM 管理 设备载入 云交付的防火墙管理中心，则无法再使用 设备管理器 来管理设备。

- 由 本地管理中心 管理的设备。

  如果您已有由 本地管理中心 管理的 威胁防御 设备，则可以迁移该设备以进行云管理。有关详细信息，请参阅将安全防火墙威胁防御迁移到云。

注释 将设备移动或迁移到 云交付的防火墙管理中心 时会发生以下情况：

- 如果您从 本地管理中心 或 Secure Firewall Threat Defense 设备管理器 中删除设备以载入 云交付的防火墙管理中心，则管理器的更改会擦除通过 本地管理中心 配置的任何策略。
- 如果将设备从 本地管理中心 **迁移**到 云交付的防火墙管理中心，则该设备将保留您之前配置的大多数策略。

如果您不知道您的设备是否已由备用管理器管理，请在设备的 CLI 中使用 `show managers` 命令。

载入方法

云交付的防火墙管理中心 支持以下载入方法：

- 使用 CLI 注册密钥载入设备 - 使用注册密钥载入设备。在设备上完成初始设置向导。
- 通过低接触调配激活设备 - 对**未**在设备上执行初始设备安装向导的新出厂设备进行载入。请注意，此方法仅支持 Firepower 1000、Firepower 2100 或 Secure Firewall 3100 设备。

注释 版本 7.0.3 不支持低接触调配。

- 通过序列号载入设备 - 载入已初始配置序列号的设备。请注意，此方法仅支持 Firepower 1000、Firepower 2100 或 Secure Firewall 3100 设备。

注释 版本 7.0.3 不支持使用序列号载入。

将设备载入 云交付的防火墙管理中心的前提条件

自行激活限制和要求

将设备载入 云交付的防火墙管理中心时，请注意以下限制：

- 设备 **必须** 运行 7.0.3 版本或 7.2 或更高版本。我们 **强烈** 建议使用 7.2 或更高版本。
- 您不需要本地或虚拟 SDC 来载入设备。
- 您可以按照 迁移 FTD 到云交付的防火墙管理中心 流程来迁移由 本地防火墙管理中心 管理的 HA 对。在迁移之前，确认两个对等体都处于正常状态。
- 只有配置为本地管理且由 设备管理器 管理的设备才能使用序列号和低接触调配方法自行激活。
- 如果设备由 本地管理中心管理，您可以将设备载入或迁移到 云交付的防火墙管理中心 。迁移会保留任何现有策略和对象，而自行激活设备会删除大多数策略和所有对象。有关详细信息，请参阅 将 FTD 迁移到云交付的防火墙管理中心 。
- 如果您的设备当前由 设备管理器管理，请在将设备载入之前取消注册所有智能许可证。即使您切换了设备管理，思科智能软件管理器仍将保留智能许可证。
- 如果您之前载入了由 设备管理器 管理的设备，并从 CDO 中删除了该设备，以便重新载入以进行云管理，则 **必须** 在删除设备后将 设备管理器 注册到 安全服务交换 云。请参阅《*Firepower* 和思科 *SecureX* 威胁响应集成指南》中的“访问安全服务交换”章节。

提示 将设备自行激活到 云交付的防火墙管理中心 会删除通过上一个管理器配置的任何策略和大多数对象。如果您的设备当前由 本地管理中心管理，则可以迁移设备并保留您的策略和对象。有关详细信息，请参阅 将 FTD 迁移到云交付的防火墙管理中心 。

网络要求

在载入设备之前，请确保以下端口具有外部和出站访问权限。确认允许设备上的以下端口。如果通信端口被防火墙阻止，则激活设备可能会失败。

注释 您无法在 CDO UI 中配置这些端口。您必须通过设备的 SSH 来启用这些端口。

表 *1:* 设备端口要求

端口	协议/功能	详细信息
443/tcp	HTTPS	发送和接收来自互联网的数据。
443	HTTPS	与 AMP 云（公共或私有）通信

端口	协议/功能	详细信息
8305/tcp	设备通信	在同一部署中的设备之间安全地进行通信。

管理和数据接口

确保您的设备已正确配置管理或数据接口。

要在设备上配置管理或数据接口，请参阅使用 CLI 完成 Secure Firewall Threat Defense 设备初始配置。

使用 CLI 注册密钥载入设备

使用以下程序通过 CLI 注册密钥为 云交付的防火墙管理中心 载入设备。

注释 如果您的设备当前由 本地管理中心管理，则载入设备将失败。您可以从 本地管理中心 删除设备并作为没有策略或对象的全新设备载入，也可以迁移设备并保留现有策略和对象。有关详细信息，请参阅将 FTD 迁移到云交付防火墙管理中心。

重要事项 您可以使用 Cisco Secure Firewall 机箱管理器或 FXOS CLI 来创建 CDO 托管的独立逻辑 威胁防御 设备。

开始之前

在载入设备之前，请务必完成以下任务：

- 已为您的租户启用 云交付的防火墙管理中心。
- 确认设备的 CLI 配置已成功完成。有关详细信息，请参阅 使用 CLI 完成 Secure Firewall Threat Defense 设备初始配置。
- 在载入设备之前，请查看前提条件和限制。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的“将设备载入云交付的防火墙管理中心的前提条件”。
- 可以将设备配置为使用 Secure Firewall 设备管理器 进行本地管理或使用 Cisco Secure Firewall Management Center 进行远程管理。
- 设备必须运行版本 7.0.3 或 7.2.0 以及更高版本。

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。

步骤 3 点击 **FTD** 磁贴。

步骤 4 在 **管理模式**下，确保选择 **FTD** 。

警告 在**管理模式 (Management Mode)** 下选择 **FTD**，您将无法使用之前的管理平台来管理设备。除接口配置外，所有现有策略配置都会被重置。载入设备后，您必须重新配置策略。

如果您希望设备从 Secure Firewall 设备管理器 保持管理，请选择 **FDM** 并参阅 使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+ 以了解详细信息。

步骤 5 选择**使用 CLI 注册密钥 (Use CLI Registration Key)** 作为载入方法。

步骤 6 在 **设备名称** 字段中输入设备名称，然后点击 **下一步**。

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许可证。点击**下一步**。

步骤 10 CDO 使用注册密钥生成命令。使用 SSH 连接到您要载入的设备。以“admin”或具有同等管理员权限的用户身份登录，并将整个注册密钥按原样粘贴到设备的 CLI 中。

注意：对于 Firepower 1000、Firepower 2100、ISA 3000 和 threat defense virtual 设备，打开与设备的 SSH 连接并以 `admin` 登录。复制整个注册命令，并在提示符后将其粘贴到设备的 CLI 界面中。在 CLI 中，输入 **Y** 完成注册。如果您的设备以前由 设备管理器管理，请输入 **是 (Yes)** 以确认提交。

步骤 11 在 CDO 载入向导中点击 **下一步 (Next)** 。

步骤 12 （可选）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。标签会在设备载入 CDO后应用到设备。

下一步做什么

在设备同步后，从**清单 (Inventory)** 页面中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《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的访问控制概述。
- 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。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的思科安全分析和日志记录。

通过低接触调配激活设备

只有 Firepower 1000、Firepower 2100 和 Secure Firewall 3100 设备可以使用低接触调配方法来载入。

开始之前

在载入之前，确认已完成以下操作：

- 已为您的租户启用 云交付的防火墙管理中心。
- 设备是全新安装的，但从未通过设备 CLI 或 设备管理器 登录。
- 设备正在运行 7.2 或更高版本。版本 7.0.3 不支持低接触调配。

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。

步骤 3 点击 **FTD** 磁贴。

步骤 4 在 **管理模式**下，确保选择 **FTD** 。

警告 在**管理模式 (Management Mode)** 下选择 **FTD**，您将无法使用之前的管理平台来管理设备。除接口配置外，所有现有策略配置都会被重置。载入设备后，您必须重新配置策略。

如果您希望设备从 Secure Firewall 设备管理器 保持管理，请选择 **FDM** 并参阅 使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+ 以了解详细信息。

步骤 5 输入 **设备序列号** 和 **设备名称**。选择**下一步**。

步骤 6 密码重设选择**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)** 选项。

如果您的设备之前已注册管理器或 仍 注册到管理器，请参阅 通过序列号载入设备，第 7 页。

步骤 7 点击**下一步 (Next)**。

步骤 8 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 9 选择要应用于设备的所有许可证。点击**下一步**。

下一步做什么

在设备同步后，从**清单 (Inventory)** 页面中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《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的访问控制概述。

- 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。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的思科安全分析和日志记录。

通过序列号载入设备

只有 Firepower 1000、Firepower 2100 和 Secure Firewall 3100 设备可以使用序列号载入方法来载入。

开始之前

请确保在载入之前完成以下操作：

- 已为您的租户启用 云交付的防火墙管理中心。
- 确认设备的 CLI 配置已成功完成。有关详细信息，请参阅 使用 CLI 完成 Secure Firewall Threat Defense 设备初始配置。
- 在载入设备之前，请查看前提条件和限制。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的“将设备载入云交付的防火墙管理中心的前提条件”。
- 取消注册设备在载入之前可能已启用的任何现有智能许可证。
- 确认设备已被配置为本地管理并且当前由 Secure Firewall 设备管理器 管理。
- 设备正在运行 7.2 或更高版本。版本 7.0.3 不支持使用序列号载入。

过程

步骤 1 在 Secure Firewall 设备管理器 UI 中，请转至 **系统设置 (System Settings)** > **云服务 (Cloud Services)**，然后选 **通过 Cisco 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)**。

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。

步骤 4 点击 **FTD** 磁贴。

步骤 5 在 **管理模式**下，确保选择 **FTD** 。

在**管理模式**下选择**FTD**，您将无法使用之前的管理平台来管理设备。除接口配置外，所有现有策略配置都会被重置。载入设备后，您必须重新配置策略。

步骤 6 输入 **设备序列号** 和 **设备名称**。点击**下一步 (Next)**。

步骤 7 密码重设选择**否，此设备已登录并为管理器配置 (No, this device has been logged into and configured for a manager)**。这意味着该设备已被注册至 设备管理器，并且默认密码已作为该配置的一部分进行了更改。

如果您的设备是全新的，并且从未配置过管理器，请参阅 通过低接触调配激活设备，第 6 页。

步骤 8 点击**下一步 (Next)**。

步骤 9 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 10 选择要应用于设备的所有许可证。点击**下一步**。

下一步做什么

在设备同步后，从**清单 (Inventory)** 页面中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《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的访问控制概述。
- 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。有关详细信息，请参阅《使用思科防御协调器中的云交付防火墙管理中心来管理防火墙威胁防御》中的思科安全分析和日志记录。

载入与 AWS VPC 关联的 威胁防御 设备

使用以下程序载入并初步调配与要由 云交付的防火墙管理中心 管理的 AWS VPC 关联的 威胁防御 设备的防火墙。

开始之前

在载入之前，确认满足以下前提条件：

- 您必须启用 云交付的防火墙管理中心 功能并将其与您的租户关联。
- AWS VPC 必须已被载入 CDO。有关更多信息，请参阅载入 AWS VPC。

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。

步骤 3 选择 **FTD** 磁贴。

步骤 4 在 **管理模式**下，确保选择 **FTD** 。

步骤 5 选择**使用 AWS VPC (Use AWS VPC)** 作为载入方法。如果没有已载入的 AWS VPC，您可以点击此步骤中提供的链接并载入虚拟环境。

步骤 6 从下拉菜单选择**可用性区域**。选择云 威胁防御 所在的区域，而不是本地计算机所在的区域。

步骤 7 通过以下任一选项来选择管理接口子网：

- **使用现有子网 (Use existing subnets)** - 展开下拉菜单并为管理接口、内部接口和外部接口子网选择适当的子网。
- **创建新子网 (Create new subnets)** - 添加一组子网接口，供设备在载入后使用。作为载入程序的一部分，CDO 会自动创建这些子网并将其应用于 AWS VPC。

请注意，诊断接口将使用与管理接口相同的接口。

步骤 8 点击**选择 (Select)** 以分配子网。点击**下一步**。

步骤 9 在 **设备名称** 字段中输入设备名称，然后点击 **下一步**。

步骤 10 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 11 选择您要应用于设备的**订用许可证 (Subscription Licenses)**。您必须至少拥有为虚拟 威胁防御 设备选择的 URL 许可证。

下一步做什么

设备可能需要几分钟才能显示在CDO的**清单 (Inventory)** 页面中，因为在 CDO 成功部署云形成、初始化设备连接并与虚拟设备和 AWS VPC 环境建立通信之前，设备无法同步。

如有必要，您可以在载入后通过 云交付的防火墙管理中心 UI 来修改虚拟 威胁防御 设备性能层选择。

从云交付的防火墙管理中心删除设备

虽然设备已注册到 云交付的防火墙管理中心，但 CDO 仍会管理设备注册。您必须从 CDO 控制面板中删除设备才能从云交付的防火墙管理中心中删除设备。

注释 CDO 不会同步与 AWS VPC 环境关联的设备的删除。您必须从 AWS VPC UI 中直接删除设备目录。有关详细信息，请参阅 AWS 文档。

过程

步骤 1 登录 CDO 并点击**清单 (Inventory)**。

步骤 2 使用过滤器或搜索栏找到要删除的设备。选择它以突出显示设备行。

步骤 3 在右侧的设备操作窗格中，点击**删除 (Remove)**。

步骤 4 出现提示时，选择**确定 (OK)** 以确认删除所选设备。点击**取消 (Cancel)** 以使设备保持已载入状态。

故障排除

使用以下场景对任何载入问题进行故障排除。

使用 CLI 注册密钥将设备载入 云交付的防火墙管理中心进行故障排除

错误：载入后设备仍处于待处理设置状态

当设备注册失败时，设备的连接状态显示为**待设置 (Pending Setup)**。在右侧的面板中，CDO 会显示一条**注册失败 (Registration Failed)** 消息以及一个**重试载入 (Retry Onboarding)** 按钮，以允许您立即重新尝试载入设备。

如果您在将其载入 CDO 后的 3 分钟内未在设备 CLI 中执行 `configuration manager` 命令，则设备的注册尝试会到期并导致注册失败。使用以下程序解决此问题：

过程

步骤 1 登录 CDO 并导航至**清单 (Inventory)** 页面。找到注册失败的设备。

步骤 2 在右侧的面板中，找到**注册失败 (Registration Failed)** 窗口。在设备的 CLI 注册密钥旁边，点击**复制 (Copy)**。此操作会将 CLI 密钥复制到本地剪贴板。

步骤 3 打开到设备的 SSH 连接并以管理员身份登录。

步骤 4 将 CLI 注册密钥粘贴到设备的 CLI 界面中。在 CLI 中，输入 **Y** 完成注册。如果您的设备以前由 设备管理器管理，请输入 **是 (Yes)** 以确认提交。

对使用序列号将设备载入 云交付的防火墙管理中心 进行故障排除

设备离线或无法访问

如果设备在载入过程中或在载入后的任何时候无法访问，CDO 会显示**无法访问 (Unreachable)** 连接状态。在设备能够连接之前，设备将无法完全载入CDO。这可能是以下情况所致：

- 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，或者存在阻止网络的外部 DNS。
- 如果您的设备与欧洲地区 (https://defenseorchestrator.eu/) 相关联，则您可能需要启用 PPPoE 身份验证。对于其他域，请查看域要求。
- 设备可能被防火墙阻止，或者错误地阻止了用于连接的端口。查看设备 网络要求，第 3 页 并确认已启用正确的传出端口。

错误：序列号已被申领

设备是从外部供应商处购买的

如果设备是从外部供应商处购买的，并且由于**序列号已申领 (Serial Number Already Claimed)** 错误而无法载入，则该设备可能仍与供应商的租户相关联。使用以下步骤来申领设备及其序列号：

1. 从 CDO 租户中删除设备。
2. 在设备上安装 FXOS 映像。有关详细信息，请参阅《Firepower 1000/21000 和 Cisco Secure Firewall 3100 Firepower 威胁防御的 FXOS 故障排除指南》南的“重新映像程序”一章。
3. 将笔记本电脑连接到设备的控制台端口。
4. 连接到 FXOS CLI 并以**管理员**身份登录。
5. 在 FXOS CLI 中，通过 `firepower # connect local-mgmt` 命令连接到 **local-mgmt**。
6. 执行 `firepower(local-mgmt) # cloud deregister` 命令，以便从云租户取消注册设备。
7. 一旦设备成功取消注册，CLI 接口会返回成功消息。消息示例：

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

注释 如果设备从未注册到其他 CDO 租户，则上面的消息会指出 `RESULT=success MESSAGE=DEVICE_NOT_FOUND`。

8. 使用序列号将设备载入 CDO 租户。有关详细信息，请参阅 通过序列号载入设备，第 7 页。

设备被其他区域的 CDO 租户申领

该设备之前可能已由其他区域中的另一个 CDO 实例管理，并仍注册到该租户。

如果您**确实**有权访问设备当前注册到的租户，请使用以下程序：

1. 从错误的 CDO 租户中删除设备。
2. 登录设备的 设备管理器 UI。
3. 导航至**系统设置 (System Settings)** > **云服务 (Cloud Services)**。
4. 点击**云服务 (Cloud Services)**，然后从下拉列表中选择**取消注册云服务 (Unregister Cloud Services)**。
5. 确认操作，然后点击**取消注册 (Unregister)**。此操作会生成警告，指明设备已从 CDO 中删除。这是预期行为。
6. 登录到正确区域的 CDO 租户并载入设备。有关详细信息，请参阅 通过序列号载入设备，第 7 页。
7. 导航至**系统设置 (System Settings)** > **云服务 (Cloud Services)**。

8. 点击**云服务 (Cloud Services)**，然后从下拉列表中选择**取消注册云服务 (Unregister Cloud Services)**。
9. 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)**并点击**注册 (Register)**。设备会映射到属于新区域的新租户，而 CDO 会载入设备。

如果您**无权**访问租户，请使用以下程序：

1. 从控制台端口连接到 FXOS CLI 并以**管理员**身份登录。有关如何登录 FXOS CLI 的信息，请参阅访问 FXOS CLI。
2. 在 FXOS CLI 中，通过 `firepower # connect local-mgmt` 命令连接到 **local-mgmt**。
3. 执行 `firepower(local-mgmt) # cloud deregister` 命令，以便从云租户取消注册设备。
4. 一旦设备成功取消注册，CLI 接口会返回成功消息。消息示例：

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

注释 如果设备从未注册到其他 CDO 租户，则上面的消息会指出 `RESULT=success MESSAGE=DEVICE_NOT_FOUND`。

5. 在正确域中的 CDO 租户中，载入设备。有关详细信息，请参阅 通过序列号载入设备，第 7 页。
6. 在设备的 设备管理器 中，导航至**系统设置 (System Settings)** > **云服务 (Cloud Services)**。
7. 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)**并点击**注册 (Register)**。设备会映射到属于新区域的新租户，而 CDO 会载入设备。

错误：申领错误

如果在载入设备时输入错误的序列号，CDO 会生成**申领错误 (Claim Error)** 状态。

注释 确认设备已在 CDO 内正确的区域中申领。

使用以下方法解决此问题：

过程

步骤 1 登录 CDO 并导航至**清单 (Inventory)** 页面。找到存在错误的设备。

步骤 2 选择设备，使其突出显示，然后从 CDO **删除**设备。

步骤 3 确认以下内容：

- 设备处于在线状态并且可以访问互联网。

- 设备尚未注册到您的 CDO 实例或由其他区域的 CDO 租户申领。

步骤 4 找到设备的序列号。可以使用以下一种方法：

- 对于 1000、2100 和 3100 系列型号，请找到实际设备上的序列号。
- 打开与设备的 SSH 连接并发出 `show serial-number` 命令。
- 如果设备当前是 FDM 管理，请登录 设备管理器 UI 并在**云服务 (Cloud Services)** 页面上找到序列号。

步骤 5 在 CDO 中，使用正确的序列号载入设备。有关详细信息，请参阅通过序列号载入设备，第 7 页。

错误：申领失败

如果您在尝试载入设备后看到**错误：无法申领 (Error: Failed to Claim)** 连接状态或错误消息，则可能是以下原因造成的：

- 安全服务交换 平台可能存在会导致无连接的临时问题。
- CDO 服务器可能已关闭。

请按照以下步骤解决此问题：

过程

步骤 1 登录 CDO 并导航至**清单 (Inventory)** 页面。找到注册失败的设备。

步骤 2 选择设备，使其突出显示，然后从 CDO 租户**删除**设备。

步骤 3 等待至少 10 分钟，然后再尝试将设备载入 CDO 租户。有关详细信息，请参阅通过低接触调配激活设备，第 6 页。

下一步做什么

如果您仍无法申领设备，请查看设备的工作流程，以确认是否存在错误消息。如果有，请导出工作流程并创建支持案例以进一步解决问题。

错误：临时错误

设备密码尚未更改

如果您在配置设备以进行远程管理时未更改设备的默认密码，并且在将设备载入CDO时选择了**否，此设备已登录并配置为管理器 (No, this device has been logged into and configured for a manager)** 选项，则设备将在**清单 (Inventory)** 页面中生成**未调配 (UnProvisioned)** 连接状态。

使用以下程序解决此问题：

1. 登录 CDO 并导航至**清单 (Inventory)** 页面。
2. 找到并选择连接状态为**未调配 (UnProvisioned)** 的设备，使其突出显示。
3. 在右侧窗格中，找到**更改密码 (Change Password)** 窗口。
4. 点击**更改密码 (Change Password)**，然后输入设备的新密码。这样就会覆盖默认密码。

设备可能需要几分钟才能载入并完全同步到 CDO。

设备密码已被更改

如果您在配置设备以进行远程管理时**确实**更改了设备的默认密码，并选择了**此设备是否为从未登录或配置过的新设备？(Is this a new device that has never been logged into or configured before?)** 选项将设备载入 CDO 时，CDO 会在**清单 (Invenotry)** 页面中生成**未调配 (UnProvisioned)** 连接状态。

使用以下程序解决此问题：

1. 登录 CDO 并导航至**清单 (Inventory)** 页面。
2. 找到并选择连接状态为**未调配 (UnProvisioned)** 的设备，使其突出显示。
3. 在右侧窗格中，找到**确认并继续 (Confirm and Proceed)** 窗口。
4. 点击**确认并继续 (Confirm and Proceed)**。此操作会忽略载入向导中提供的密码，并恢复设备的默认密码。然后 CDO 会继续载入设备。

其他临时错误场景

无论设备的默认密码配置如何，设备在载入过程中仍可能处于**未调配 (UnProvisioned)** 连接状态。如果您确认在载入向导中选择的密码对于设备的状态是准确的，请考虑使用以下选项来解决问题：

- 选择设备以便将其突出显示。在屏幕右侧窗格的窗口中，点击**重试 (Retry)** 以强制 CDO 使用现有临时参数重新载入设备。
- 从**清单 (Inventory)** 页面删除设备，然后尝试重新载入设备。
- 在设备的 设备管理器 中，导航至**系统设置 (System Settings)** > **云服务 (Cloud Services)**。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)** 并点击**注册 (Register)**。

如果您仍无法申领设备，请查看设备的工作流程，以确认是否存在错误消息。如果有，请导出工作流程并创建支持案例以进一步解决问题。

关于设备管理

使用 管理中心 来管理您的设备。

管理接口

设置设备时，指定您要连接到的 IP 地址。管理和事件流量都在初始注册时转到此地址。

注释 在某些情况下，设备可能会在其他管理接口上建立初始连接；后续连接应使用具有指定 IP 地址的管理接口。

如果设备具有单独的仅事件接口，则托管设备会在网络允许的情况下将后续事件流量发送到仅事件接口。此外，某些托管设备型号包括一个额外的管理接口，您可以为仅事件流量配置该接口。

注释 请注意，如果您配置用于管理的数据接口，则不能使用单独的管理接口和事件接口。

如果事件网络关闭，则事件流量将恢复到托管设备上的常规管理接口。

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。对于 Amazon Web 服务上的 FTDv，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。

设备管理接口上的网络路由

管理接口（包括事件专用接口）仅支持通过静态路由到达远程网络。在设置托管设备时，设置进程将为您指定的网关 IP 地址创建一个默认路由。不能删除此路由；只能修改网关地址。

注释 如果配置用于管理的数据接口而不是使用专用管理接口，则流量将通过背板路由以使用数据路由表。本节中的信息不适用。

如果要访问远程网络，建议为每个管理接口使用至少一个静态路由。我们建议将每个接口放在单独的网络中，以避免潜在的路由问题，包括从其他设备到设备的路由问题。如果同一网络上的接口没有遇到问题，请务必正确配置静态路由。例如，management0 和 management1 位于同一网络上，但 FTD 管理接口和事件接口则位于不同的网络上。网关是 192.168.45.1。如果您希望 management1 连接到位于 10.6.6.1/24 的管理的仅事件接口，则可以通过 management1 使用相同的网关 192.168.45.1 来创建 10.6.6.0/24 的静态路由。到达 10.6.6.0/24 的流量会在到达默认路由之前到达此路由，因此按照预期会使用管理。

登录 威胁防御 设备上的命令行界面

您可以在 威胁防御 设备上直接登录命令行界面。

注释 当用户连续三次尝试通过 SSH 登录 CLI 失败时，系统会终止 SSH 连接。

开始之前

使用默认 **admin** 用户进行初始登录，完成初始安装过程。创建可以使用 **configure user add** 命令登录 CLI 的其他用户账户。

过程

步骤 1 通过控制台端口或使用 SSH连接至 威胁防御 CLI。

可以通过SSH连接到威胁防御设备的管理接口。如果您为SSH连接打开某个数据接口，您也可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。请参阅配置安全外壳，以允许与特定数据接口建立 SSH 连接。

对于物理设备，您可以直接连接到设备上的控制台端口。使用设备随附的控制台电缆将您的 PC 连接到使用终端仿真器的控制台，终端仿真器的设置为 9600 波特率、8 个数据位、无奇偶校验、1 个停止位、无流量控制。有关控制台电缆的详细信息，请参阅设备的硬件指南。

在控制台端口上访问的初始 CLI 因设备类型而异。

- ISA 3000 和 threat defense virtual - 控制台端口上的 CLI 是常规 威胁防御 CLI。
- 其他型号-控制台端口上的 CLI 是 FXOS。您可以使用 **connect ftd** 命令进入 威胁防御 CLI。仅将 FXOS CLI 用于机箱级配置和故障排除。使用 威胁防御 CLI 进行基本配置、监控和正常的系统故障排除。有关 FXOS 命令的信息，请参阅 FXOS 文档。

步骤 2 使用 **admin** 用户名和密码登录。

步骤 3 在 CLI 提示符 (>) 处，使用命令行访问级别所允许的任何命令。

步骤 4 （可选）访问诊断 CLI：

system support diagnostic-cli

使用此 CLI 可进行高级故障排除。此CLI包括额外 **show** 和其他命令。

此 CLI 有两种子模式：用户 EXEC 和特权 EXEC 模式。在特权 EXEC 模式中，有更多命令可用。要进入特权 EXEC 模式，请输入 **enable** 命令；在收到提示时按 Enter 键，无需输入密码。

示例：

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

要返回到常规 CLI，请键入 **Ctrl+a**, **d**。

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。