



配置 本地防火墙管理中心 设备

本章涵盖以下部分：

- [读取、丢弃、检查和部署更改](#)，第 1 页
- [读取所有设备配置](#), on page 2
- [预览和部署所有设备的配置更改](#)，第 3 页
- [批量部署设备配置](#), on page 4
- [放弃更改](#), on page 5
- [设备上的带外更改](#), on page 5
- [同步 Defense Orchestrator 和设备之间的配置](#)，第 6 页
- [冲突检测](#), on page 6
- [自动接受设备的带外更改](#), on page 7
- [解决配置冲突](#), on page 8
- [安排设备更改轮询](#), on page 9

读取、丢弃、检查和部署更改

为了管理设备，CDO 必须在其本地数据库中存储自己的设备配置副本。当 CDO 从其管理的设备“读取”配置时，它会获取设备配置的副本并将其保存。CDO 首次和设备载入时读取并保存设备配置的副本。这些选项描述了出于不同目的而读取配置：

- 当设备的配置状态为“未同步”(Not Synced)时，可以使用**放弃更改 (Discard Changes)**。在“未同步”状态下，CDO 上的设备配置有待更改。此选项允许您撤消所有待处理的更改。待处理的更改将被删除，并且 CDO 会使用设备上存储的配置副本覆盖其配置副本。
- **检查更改**。如果设备的配置状态为“已同步”(Synced)，则此操作可用。点击“检查更改”(Checking for Changes)会指示 CDO 将其设备配置副本与设备上存储的配置副本进行比较。如果存在差异，CDO 会立即使用设备上存储的副本覆盖其设备配置副本。
- **审核冲突并接受而不审核**。如果您在设备上启用了**冲突检测 (Conflict Detection)**，CDO 会每 10 分钟检查一次设备上的配置更改。如果设备上存储的配置副本已更改，CDO 会通过显示“检测到冲突”配置状态来通知您。
 - **查看冲突**。点击查看冲突，您可以查看直接在设备上进行的更改，并接受或拒绝这些更改。

- **接受而不审核**。此操作会使用设备上存储的最新配置副本来覆盖设备配置的 CDO 副本。在执行覆盖操作之前，CDO 不会提示您确认配置的两个副本中的差异。

读取所有是一个批处理操作。您可以选择任何状态的多个设备，然后点击**读取全部 (Read All)**，以使用设备上存储的配置覆盖 CDO 上存储的所有设备的配置。

部署更改

当您更改设备的配置时，CDO 会将您所做的更改保存到自己的配置副本中。在将这些更改部署到设备之前，这些更改在 CDO 上“待处理”。当设备的配置发生更改但尚未部署到设备时，该设备将处于“未同步”配置状态。

待处理的配置更改对通过设备运行的网络流量没有影响。只有在 CDO 将更改部署到设备后，它们才会生效。当 CDO 将更改部署到设备的配置时，它只会覆盖已更改的配置元素。它不会覆盖设备上存储的整个配置文件。可以为单个设备或同时在多个设备上启动部署。

丢弃全部 (Discard All) 选项仅在您点击**预览并部署...(Preview and Deploy...)**。点击“预览并部署” (Preview and Deploy) 后，CDO 会向您显示 CDO 中待处理更改的预览。点击**丢弃全部 (Discard All)** 会从 CDO 中删除所有待处理的更改，并且不会将任何内容部署到所选设备。与上面的“放弃更改” (Discard Changes) 不同，删除待处理的更改是操作的结束。

读取所有设备配置

如果在 Cisco Defense Orchestrator (CDO) 之外对设备进行配置更改，则存储在 CDO 上的设备配置与其配置的本地副本将不再相同。您可能希望使用设备上存储的配置覆盖 CDO 的设备配置副本，以使配置再次相同。您可以使用**全部读取 (Read All)** 链接在多台设备上同时执行此任务。

有关 CDO 如何管理设备配置的两个副本的详细信息，请参阅[读取](#)、[丢弃](#)、[检查](#)和[部署更改](#)。

以下是三种配置状态，其中点击**全部读取 (Read All)** 将使用设备的配置副本覆盖 CDO 的设备配置副本。

- **检测到冲突 (Conflict Detected)** - 如果启用冲突检测，CDO 将每 10 分钟轮询一次其管理的设备，以了解对其配置所做的更改。如果 CDO 发现设备上的配置已更改，则 CDO 会显示设备的“检测到冲突” (Conflict detected) 配置状态。
- **已同步 (Synced)** - 如果设备处于同步状态，并且您点击**全部读取 (Read All)**，CDO 会立即检查设备以确定是否直接对其配置进行了任何更改。点击**读取全部 (Read All)** 后，CDO 会确认您是否打算覆盖其设备配置副本，然后 CDO 会执行覆盖。
- **未同步 (Not Synced)** - 如果设备处于未同步状态，并且您点击**全部读取 (Read All)**，则 CDO 会警告您使用 CDO 对设备的配置进行了待处理的更改，并且继续执行读取操作将删除这些更改，然后覆盖 CDO 的配置副本以及设备上的配置。此读取所有功能，例如[放弃更改](#)。

步骤 1 从导航栏中，点击**清单 (Inventory)**。

步骤 2 点击设备 (**Devices**) 选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 （可选）创建[更改请求标签](#)以便在更改日志中轻松识别此批量操作的结果。

步骤 5 选择要保存 CDO 配置的设备。请注意，CDO 仅提供可应用于所有选定设备的操作的命令按钮。

步骤 6 点击[全部读取 \(Read All\)](#)。

步骤 7 如果您选择的任何设备的 CDO 上有配置更改，CDO 会发出警告，并询问您是否要继续执行批量读取配置操作。点击[全部读取 \(Read All\)](#) 以继续。

步骤 8 查看通知选项卡以了解“全部读取” (Read All) 配置操作的进度。

步骤 9 如果您创建并激活了更改请求标签，请记住将其清除，以免无意中将其其他配置更改与此事件关联。

相关信息

- [读取、丢弃、检查和部署更改](#)
- [放弃更改](#)

预览和部署所有设备的配置更改

当您对租户上的设备进行了配置更改，但您尚未部署该更改时，CDO 会通过部署图标上显示一个橙色点来通知您




。受这些更改影响的设备在设备和服务 (**Services**) 页面中显示“未同步” (Not Synced) 状态。通过点击[部署 \(Deploy\)](#)，您可以查看哪些设备具有待处理的更改，并将更改部署到这些设备。

此部署方法适用于所有受支持的设备。


您可以将此部署方法用于单个配置更改，也可以等待并一次部署多个更改。

SUMMARY STEPS

1. 在屏幕的右上角，点击[部署 \(Deploy\)](#) 图标 。
2. 选择要部署更改的设备。如果设备有黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在黄色警告三角形上，了解无法将更改部署到该设备的原因。
3. 选择设备后，您可以在右侧面板中将其展开并预览其特定更改。
4. （可选）如果要查看有关待处理更改的更多信息，请点击[查看详细更改日志 \(View Detailed Changelog\)](#) 链接以打开与该更改关联的更改日志。点击[部署 \(Deploy\)](#) 图标可返回具有待处理更改的设备 (**Devices with Pending Changes**) 页面。
5. （可选）[创建更改请求](#) 以跟踪更改，而无需离开具有待处理更改的设备 (**Devices with Pending Changes**) 页面。
6. 点击[立即部署 \(Deploy Now\)](#)，立即将更改部署到您选择的设备。您将在“作业” (Jobs) 托盘的“活动作业” (Active jobs) 指示器中看到进度。
7. （可选）部署完成后，点击 CDO 导航栏中的[作业 \(Jobs\)](#)。您将看到最近的“部署更改” (Deploy Changes) 作业，其中显示了部署的结果。

- 如果您创建了更改请求标签，并且没有其他配置更改与之关联，请将其清除。

DETAILED STEPS


- 在屏幕的右上角，点击部署 (Deploy) 图标 。
- 选择要部署更改的设备。如果设备有黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在黄色警告三角形上，了解无法将更改部署到该设备的原因。
- 选择设备后，您可以在右侧面板中将其展开并预览其特定更改。
- (可选) 如果要查看有关待处理更改的更多信息，请点击查看详细更改日志 (View Detailed Changelog) 链接以打开与该更改关联的更改日志。点击部署 (Deploy) 图标可返回具有待处理更改的设备 (Devices with Pending Changes) 页面。
- (可选) 创建更改请求以跟踪更改，而无需离开具有待处理更改的设备 (Devices with Pending Changes) 页面。
- 点击立即部署 (Deploy Now)，立即将更改部署到您选择的设备。您将在“作业” (Jobs) 托盘的“活动作业” (Active jobs) 指示器中看到进度。
- (可选) 部署完成后，点击 CDO 导航栏中的作业 (Jobs)。您将看到最近的“部署更改” (Deploy Changes) 作业，其中显示了部署的结果。
- 如果您创建了更改请求标签，并且没有其他配置更改与之关联，请将其清除。

下一步做什么


批量部署设备配置


如果您对多个设备进行了更改（例如通过编辑共享对象），则可以一次将这些更改应用到所有受影响的设备：

- 在导航窗格中，点击 设备和服务。
- 点击设备选项卡。
- 点击适当的设备类型选项卡。
- 选择已在 CDO 上进行配置更改的所有设备。这些设备应显示“未同步” (Not Synced) 状态。
- 使用以下方法之一部署更改：

- 点击屏幕右上角的部署 (Deploy) 按钮 。这使您有机会在部署之前查看所选设备上的待处理更改。点击立即部署 (Deploy Now) 以部署更改。

Note 如果在有待处理更改的设备 (Devices with Pending Changes) 屏幕上看到某个设备旁边显示黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在警告三角形上，了解有关无法将更改部署到该设备的信息。

- 点击详细信息窗格中的**全部部署 (Deploy All)** 。查看所有警告，然后点击**确定 (OK)**。批量部署会立即开始，无需审核更改。

步骤 6 (可选) 点击导航栏中的“作业” (Jobs) 图标  以查看批量部署的结果。

放弃更改

如果要“撤消”使用 CDO 对设备配置所做的所有未部署的配置更改，请点击**放弃更改 (Discard Changes)**。在点击**放弃更改 (Discard Changes)** 时，CDO 会使用设备上存储的配置完全覆盖设备配置的本地副本。

点击**放弃更改 (Discard Changes)** 时，设备的配置状态为**未同步 (Not Synced)**。在放弃更改后，CDO 上的配置副本将与设备上的配置副本相同，CDO 中的配置状态将恢复为“已同步” (Synced)。

要放弃或“撤消”设备的所有未部署的配置更改，请执行以下操作：

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择您已对其进行配置更改的设备。

步骤 5 点击右侧未同步窗格中的**放弃更改 (Discard Changes)**。

- 对于 FDM 管理设备，CDO 会警告您“CDO 上的待处理更改将被丢弃，此设备的 CDO 配置将替换为设备上当前运行的配置” (Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device)。点击**继续 (Continue)** 以放弃更改。
- 对于 Meraki 设备 - CDO 会立即删除更改。
- 对于 AWS 设备 - CDO 会显示您要删除的内容。点击**接受 (Accept)** 或**取消 (Cancel)**。

设备上的带外更改

带外更改是指在不使用 CDO 的情况下直接在设备上进行的更改。可以使用设备的命令行界面通过 SSH 连接进行这些更改，也可以使用本地管理器（例如适用于 ASA 的自适应安全设备管理器 (ASDM) 或适用于 FDM 管理设备的 FDM）进行这些更改。带外更改会导致 CDO 上存储的设备配置与设备本身上存储的配置之间发生冲突。

检测设备上的带外更改

如果为 ASA、FDM 管理 设备或 Cisco IOS 设备启用了冲突检测，CDO 会每 10 分钟检查一次设备，以搜索在 CDO 之外直接对设备配置进行的任何新更改。

如果 CDO 发现未存储在 CDO 上的设备配置更改，则会将该设备的配置状态更改为“检测到冲突”状态。

当 Defense Orchestrator 检测到冲突时，可能出现以下两种情况：

- 直接对设备进行的配置更改尚未保存到 CDO 的数据库中。
- 对于 FDM 管理 设备，FDM 管理 设备上可能存在尚未部署的“待处理”配置更改。

同步 Defense Orchestrator 和设备之间的配置

关于配置冲突

在“设备和服务”页面上，您可能会看到设备或服务状态为“已同步”(Synced)、“未同步”(Not Synced)或“检测到冲突”(Conflict Detected)。

- 如果设备为已同步 (Synced)，Cisco Defense Orchestrator (CDO) 上的配置与设备本地存储的配置相同。
- 如果设备为未同步 (Not Synced)，CDO 中存储的配置已更改，现在存储在设备上的配置有所不同。将您的更改从 CDO 部署到设备会更改设备上的配置以匹配 CDO 的版本。
- 在 CDO 之外对设备进行的更改称为带外更改。进行带外更改时，如果为设备启用了冲突检测，您会看到设备状态更改为“检测到冲突”(Conflict Detected)。接受带外更改会更改 CDO 上的配置以匹配设备上的配置。

冲突检测

启用冲突检测后，Cisco Defense Orchestrator (CDO) 将按默认间隔轮询设备，以确定是否在 CDO 之外对设备配置进行了更改。如果 CDO 检测到已进行更改，则会将设备的配置状态更改为检测到冲突 (Conflict Detected)。在 CDO 之外对设备进行的更改称为“带外”更改。

启用此选项后，您可以配置每台设备检测冲突或 OOB 更改的频率。有关详细信息，请参阅[安排设备更改轮询, on page 9](#)。

启用冲突检测

启用冲突检测会提醒您在 Defense Orchestrator 之外对设备进行更改。

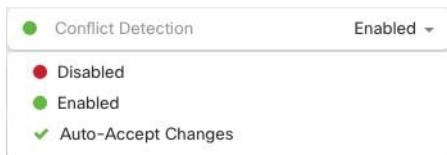
步骤 1 从导航栏中，点击清单 (Inventory)。

步骤 2 点击设备选项卡。

步骤 3 选择适当的设备类型选项卡。

步骤 4 选择要启用冲突检测的设备。

步骤 5 在设备表右侧的冲突检测框中，从列表中选择已启用。



自动接受设备的带外更改

您可以通过启用自动接受更改，将 Cisco Defense Orchestrator (CDO) 配置为自动接受直接对受管设备所做的任何更改。不使用 CDO 直接对设备进行的更改称为带外更改。带外更改会在 CDO 上存储的设备配置与设备本身上存储的配置之间产生冲突。

自动接受更改功能是对冲突检测的增强。如果您在设备上启用了自动接受更改，CDO 会每 10 分钟检查一次更改，以确定是否对设备的配置进行了任何带外更改。如果配置发生更改，CDO 会自动更新其本地版本的设备配置，而不会提示您。

如果对 CDO 进行的配置更改尚未部署到设备，则 CDO 不会自动接受配置更改。按照屏幕上的提示确定下一步操作。

要使用自动接受更改，请先启用租户，以在清单 (**Inventory**) 菜单中显示自动接受选项；然后，您可以为单个设备启用自动接受更改。

如果您希望 CDO 检测带外更改，但为您提供手动接受或拒绝更改的选项，请改为启用 [冲突检测](#), on [page 6](#)。

配置自动接受更改

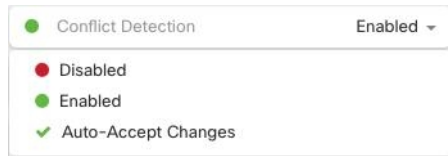
步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **设置 (Settings) > 常规设置 (General Settings)**。

步骤 3 在租户设置区域中，点击切换按钮以启用“自动接受设备更改的选项”。这将使“自动接受更改”菜单选项显示在“资产”页面的“冲突检测”菜单中。

步骤 4 打开“资产”页面，然后选择要自动接受带外更改的设备。

步骤 5 在“冲突检测” (Conflict Detection) 菜单中，选择下拉菜单中的“自动接受更改” (Auto-Accept Changes)。



为租户上的所有设备禁用自动接受更改

步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **设置 (Settings) > 常规设置 (General Settings)**

步骤 3 在“租户设置”区域中，通过将切换开关向左滑动来禁用“启用自动接受设备更改的选项”，使其显示灰色 X。这将禁用“冲突检测”菜单中的“自动接受更改”选项，并为以下项禁用此功能：租户上的每台设备。

Note 禁用“自动接受”将要求您查看每个设备冲突，然后才能将其接受到 CDO 中。这包括之前配置为自动接受更改的设备。

解决配置冲突

本节提供有关解决设备上发生的配置冲突的信息。

解决“未同步”状态

使用以下程序解决配置状态为“未同步”的设备：

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

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

步骤 3 点击设备类型选项卡。

步骤 4 选择报告为“未同步”的设备。

步骤 5 在右侧的未同步面板中，选择以下任一选项：

- **预览并部署...** - 如果要将配置更改从 CDO 推送到设备，请预览并部署您现在所做的更改，或者等待并一次部署多个更改。[预览和部署所有设备的配置更改, on page 3](#)
- **放弃更改** - 如果您不想将配置更改从 CDO 推送到设备，或者您想要“撤销”您开始在 CDO 上进行的配置更改。此选项使用设备上存储的运行配置覆盖 CDO 中存储的配置。

解决“检测到冲突”状态

CDO 允许您在每个实时设备上启用或禁用冲突检测。如果 [冲突检测, on page 6](#) 已启用, 并且在未使用 CDO 的情况下对设备的配置进行了更改, 则设备的配置状态将显示为**检测到冲突 (Conflict Detected)**。

要解决“检测到冲突” (Conflict Detected) 状态, 请执行以下程序:

步骤 1 在导航栏中, 点击 **设备和服务**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择报告冲突的设备, 然后点击右侧详细信息窗格中的**查看冲突 (Review Conflict)**。

步骤 5 在**设备同步 (Device Sync)** 页面中, 通过查看突出显示的差异来比较两种配置。

- 标记为“最后一次设备配置” (Last Known Device Configuration) 的面板是存储在 CDO 上的设备配置。
- 标记为“在设备上找到” (Found on Device) 的面板是存储在运行 ASA 配置中的配置。

步骤 6 通过选择以下选项之一来解决冲突:

- **接受设备更改 (Accept Device changes)**: 这将使用设备的运行配置覆盖 CDO 上存储的配置 和任何待处理的更改。

Note 由于 CDO 不支持在命令行界面之外部署对 Cisco IOS 设备的更改, 因此在解决冲突时, 您对 Cisco IOS 设备的唯一选择是选择**接受而不查看 (Accept Without Review)**。

- **拒绝设备更改 (Reject Device Changes)**: 这将使用存储在 CDO 上的配置覆盖设备上存储的配置。

Note 所有配置更改 (拒绝或接受) 都记录在更改日志中。

安排设备更改轮询

如果已启用 [冲突检测, on page 6](#) 或从“设置” (Settings) 页面 **启用自动接受设备更改的选项 (Enable the option to auto-accept device changes)**, 则 CDO 将按默认间隔轮询设备, 以确定是否在 CDO 之外对设备配置进行了更改。您可以自定义 CDO 轮询每台设备更改的频率。这些更改可以应用于多个设备。

如果没有为设备配置选择, 则会自动为“租户默认”配置间隔。



Note 从**设备和服务 (Devices & Services)** 页面自定义每台设备的间隔会覆盖从**常规设置 (General Settings)** 页面选择作为**默认冲突检测间隔 (Default Conflict Detection Interval)** 的轮询间隔。

从设备和服务 (**Devices & Services**) 页面启用冲突检测 (**Conflict Detection**) 或从“设置” (**Settings**) 页面选择启用该选项以自动接受设备更改 (**Enable the option to auto-accept device changes**) 后，请使用以下程序来安排您希望 CDO 轮询设备的频率：

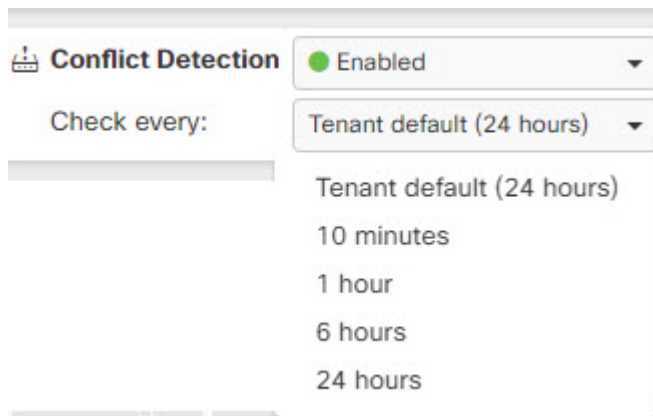
步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要启用冲突检测的设备。

步骤 5 在与冲突检测 (**Conflict Detection**) 相同的区域中，点击**检查间隔 (Check every)** 下拉菜单，然后选择所需的轮询间隔：



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。