使用 Cisco Defense Orchestrator 管理 本地防火墙管理中心

- 使用 Cisco Defense Orchestrator 管理 本地防火墙管理中心， 第 i 页

使用 Cisco Defense Orchestrator 管理 本地防火墙管理中心

关于本地防火墙管理中心

本地管理中心 支持仅限于载入、查看器托管设备、查看 对象以及交叉启动到 6.4 或更高版本设备的本地管理中心。其他功能即将推出。对于此时可能不支持的功能，您必须使用控制台。CDO本地管理中心请参阅您的系统所运行版本的《Cisco Secure Firewall Management Center 配置指南》，了解有关 本地管理中心 提供的功能的更多信息。

本地管理中心 是具有图形化用户界面的集中管理控制台，可用于执行管理、分析和报告任务。它是一种管理控制台，与 ASDM 和 FDM 类似，但不完全相同。有关支持的设备和软件版本的列表，请参阅 CDO 提供的软件和硬件支持。本地管理中心CDOCDO 支持的软件和硬件

版本支持

CDO 支持 6.4 及更高版本。本地管理中心 可以管理较旧的设备，通常有几个主要版本。例如，运行 6.6.0 版本的设备可以管理版本 6.4.0 设备。如果 管理的设备运行的版本低于 6.4，则该设备可能会显示在“资产”页面中，但无法部署到 或从中修改其策略。本地管理中心CDO您必须从 UI 进行更改和部署。本地管理中心

注释 如果受管设备已禁用或无法访问，则可能会在“资产”页面中显示该设备，但无法成功发送请求或查看设备信息。CDO

CDO 如何与 FMC 通信

CDO 充当 REST API 客户端，将请求发送到，然后使用其指定的客户端将请求传送到其受管设备。本地管理中心本地管理中心由于设备不允许使用相同的登录凭证进行多次登录，因此我们建议在 上

使用 Cisco Defense Orchestrator 管理 本地防火墙管理中心

创建一个专门用于具有管理员级别权限的通信的新用户。本地管理中心CDO必须以 提供的管理员或具有系统和设备权限的自定义用户角色的身份复制此新用户。CDOCDO如果没有管理员登录，将无法成功使用 REST API 命令修改或创建策略、规则或对象。CDO

载入或删除 本地管理中心

您可以随时自行激活或删除 。本地管理中心及其注册的设备必须至少运行版本 6.4 才能读取。本地管理中心CDO要载入 本地管理中心 及其已注册的设备，请参阅载入 FMC 以了解详细信息。在 本地管理中心 载入后，从**清单 (Inventory)** 页面中选择 本地管理中心 并点击**管理设备 (Manage Devices)** 会交叉启动所选 本地管理中心 Web UI 作为新选项卡。

从租户中删除 也会删除向该租户注册的设备。本地管理中心CDO本地管理中心有关详细信息，请参阅从 CDO 中删除 FMC。从 CDO 中删除 本地防火墙管理中心如果在自行激活后遇到“凭证无效”状态，您可以重新连接设备。本地管理中心有关详细信息，请参阅对无效凭证进行故障排除。对无效凭证进行故障排除

注释 运行 Firepower 6.6 的设备不支持重新连接功能。如果您必须重新连接设备，我们建议删除并重新载入设备。本地管理中心

本地管理中心 高可用性对

不支持设备的高可用性 (HA) 功能。CDO本地管理中心如果为高可用性配置了一对 本地管理中心 设备，则该对在**清单 (Inventory)** 页面中会列为单个设备。

由 本地管理中心 管理的设备

载入 后，注册到该 的所有设备也会被读入。本地管理中心CDO本地管理中心CDO在资产页面中，您可以查看设备信息，例如名称、IP 地址、设备类型、软件版本和状态。

您还可以使用**清单 (Inventory)** 中右侧窗格的**设备操作 (Device Actions)**、**监控 (Monitoring)**、**设备管理 (Device Management)** 和**策略 (Policies)** 面板中的相关选项执行操作。如果选择当前由 FMC 管理的设备并点击这些选项，会自动启动管理设备的控制台。CDO本地管理中心使用过滤器图标进一步组织“资产”页面。在这里，您可以选择查看所有由载入的本地管理中心托管的设备，以及其他支持的设备类型。此外，您可以展开或折叠集群中的设备，并单独或作为一个组选择它们以执行操作。

设备运行状况状态

CDO 会在**清单 (Inventory)** 页面中显示威胁防御设备的运行状况，例如**正常 (Normal)**、**错误 (Error)**、**警告 (Warning)** 和**已禁用 (Disabled)**；您可以点击设备的状态以导航到与 本地管理中心 用户界面中的设备对应的**运行状况监控 (Health Monitoring)** 页面。

注释 CDO 会每隔 10 分钟自动更新一次设备运行状况；但是，您可以通过选择设备并点击**检查更改 (Check for Changes)** 来手动执行此操作。

使用 Cisco Defense Orchestrator 管理 本地防火墙管理中心

安全策略管理

安全策略检查网络流量，最终目标是允许流量到达其预定目的地，或者在识别出安全威胁时丢弃该流量。您可以使用 CDO 在许多不同类型的设备上配置安全策略。

对象

载入时，从受管设备导入对象。本地管理中心CDOCDO本地管理中心导入到后，对象为只读。CDO虽然对象是只读的，但允许您将对象的副本应用于租户上不受管理的其他设备。本地管理中心CDO本地管理中心副本与原始对象取消关联，因此您可以编辑副本，而无需更改从 导入的对象的值。对象可在您管理的支持该对象类型的任何设备上使用。本地管理中心本地管理中心

本地管理中心 支持以下对象类型：

- 网络对象
- 网络组对象

对象问题

不识别 上的重复、不一致或未使用的对象。CDO本地管理中心您将无法根据这些问题状态过滤对象。

事件功能

搜索和过滤特定事件的历史和实时事件表的方式与在CDO中搜索和过滤其他信息时的方式相同。有关详细信息，请参阅《Firepower 管理中心和思科安全分析与日志记录 (SaaS) 集成指南》。

思科安全分析和日志记录

思科安全分析和日志记录允许您从所有设备捕获连接、入侵、文件、恶意软件和安全情报事件，并在 CDO 中的一个位置进行查看。

事件存储在思科云中，可从CDO中的“事件日志记录”页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。**日志记录和故障排除**软件包为您提供这些功能。

使用**防火墙分析和监控**软件包，系统可以将安全云分析动态实体建模应用于您的事件，并使用行为建模分析生成安全云分析观察结果和警报。如果您获取**全部网络分析和监控** 软件包，则系统会对设备事件和网络流量应用动态实体建模，并生成观察结果和警报。您可以使用思科单点登录从CDO交叉启动为您调配的安全云分析门户。

使用 **Cisco Defense Orchestrator** 管理 本地防火墙管理中心

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。