使用云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense 设备

云交付的防火墙管理中心是一种软件即服务 (SaaS) 产品，可管理 Cisco Secure Firewall Threat Defense 并通过思科防御协调器 (CDO) 交付。云交付的防火墙管理中心提供了许多与本地 Cisco Secure Firewall Management Center 相同的功能。

云交付的防火墙管理中心与本 Cisco Secure Firewall Management Center 具有相同的外观和行为，并且它们都使用相同的 FMC API。

作为 SaaS 产品，思科防御协调器 (CDO) 运营团队负责云交付的防火墙管理中心软件的部署与维护。随着新功能的推出，CDO 运营团队会为您更新 CDO 租户的云交付的防火墙管理中心。

迁移向导可帮助您将 Cisco Secure Firewall Threat Defense 设备从本地 Cisco Secure Firewall Management Center 迁移到云交付的防火墙管理中心。设备必须安装威胁防御软件版本 7.0.3 或更高版本 7.0.x，或者安装版本 7.2 或更高版本才能进行迁移。不支持威胁防御 7.1 版本。

在 CDO 中使用熟悉的流程（例如使用设备序列号载入设备或使用包含注册密钥的 CLI 命令）来载入安全防火墙威胁防御设备。在载入设备后，将同时显示在 CDO 和云交付的防火墙管理中心中，但是，您可以在云交付的防火墙管理中心中配置设备。

CDO 可为其通过数据接口管理的威胁防御设备提供高可用性支持。运行 7.2 或更高版本软件的设备支持此功能。

您可以使用安全分析和日志记录 (SaaS) 或安全分析和日志记录（本地）分析已载入的威胁防御设备生成的系统日志事件。SaaS 版本会将事件存储在云端，您可以在 CDO 中查看事件。本地版本会将事件存储在本地安全网络分析设备中，而分析在本地安全防火墙管理中心完成。在这两种情况下，就像今天的本地 FMC 一样，您仍然可以直接从传感器将日志发送到您选择的日志收集器。

云交付的防火墙管理中心的许可证是按设备管理的许可证，而云交付的防火墙管理中心本身不需要许可证。现有的安全防火墙威胁防御设备会重复使用其现有的智能许可证，而新的安全防火墙威胁防御设备会为 FTD 上实施的每项功能调配新的智能许可证。

现有客户可以继续使用 CDO 来管理其他设备类型，例如 Cisco Secure Firewall ASA、Meraki、思科 IOS 设备、Cisco Secure Firewall Cloud Native、Umbrella 和 AWS 虚拟私有云。如果您使用 CDO 管理已配置为通过 Firepower 设备管理器进行本地管理的安全防火墙威胁防御设备，则也可以继续使用 CDO 对其进行管理。

要了解如何在租户上调配云交付的防火墙管理中心，请参阅为您的 CDO 租户请求 云交付的防火墙管理中心 ， 第 2 页。

为您的 CDO 租户请求 云交付的防火墙管理中心

如果要使用 云交付的防火墙管理中心 来管理 Cisco Secure Firewall Threat Defense 设备，您可以请求在租户上调配 云交付的防火墙管理中心。

Procedure

步骤 1 在 CDO 菜单栏中，点击**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 2 点击 **请求 FMC**。

步骤 3 点击**发送请求 (Send Request)** 以确认您的云交付的防火墙管理中心 请求。

在您确认后，请求会被发送到CDO团队以调配云交付的防火墙管理中心。在调配后，您将收到一封从 *cdo-alert@cisco.com* 发送到您注册电子邮箱的邮件。您还将在CDO通知面板和已配置传入Webhook的应用上收到**云交付的防火墙管理中心 就绪**通知。有关详细信息，请参阅通知设置。

然后，您可以将 威胁防御 设备载入 云交付的防火墙管理中心 并进行管理。

硬件和软件支持

云交付的防火墙管理中心 支持 Cisco Secure Firewall Threat Defense版本 7.0.3 和 7.0.x 版本 7.0.3 及更高版本以及版本 7.2 及更高版本，可安装在许多不同的 Firepower 硬件设备或虚拟机上。

云交付的防火墙管理中心 不支持任何版本的 Cisco Secure Firewall Threat Defense版本 7.1。

有关详细信息，请参阅 Firepower 威胁防御支持说明。

思科防御协调器平台维护计划

思科防御协调器维护计划

CDO 会每周更新其平台，提供新功能和质量改进。根据此计划，更新可在 3 小时内完成。

大多数情况下，更新会在星期四完成，但如有必要，也可以安排在星期五和星期日进行维护。

表 *1: CDO* 维护时间表

星期	时间 （24 小时制）
星期四	09:00 UTC - 12:00 UTC
星期五	09:00 UTC - 12:00 UTC
星期日	09:00 UTC - 12:00 UTC

在此维护期间，您仍然可以访问您的租户，并且如果您有 云交付的防火墙管理中心，也可以访问该平台。此外，您已载入CDO的设备将继续执行其安全策略。

注释 我们建议您在维护期间不要使用 CDO 来在其管理的设备上部署配置更改。

如果发生阻止 CDO 或 云交付的防火墙管理中心 进行通信的故障，则会尽快在所有受影响的租户上解决该故障，即使并非是在维护时间窗口之内。

云交付的防火墙管理中心维护时间表

在CDO更新云交付的防火墙管理中心环境前大约1周通知在租户上部署了云交付的防火墙管理中心的客户。通过邮件通知租户的超级管理员和管理员用户。CDO还会在其主页上显示一个横幅，通知所有用户即将发布的更新。

在分配给租户区域的维护日的 3 小时维护期内，对租户进行更新最多可能需要 1 小时。在更新租户时，您将无法访问云交付的防火墙管理中心环境，但仍可访问 CDO 的其余部分。

表 *2:* 云交付的防火墙管理中心维护时间表

星期	时间 （24 小时制）	地区
星期三	04:00 UTC - 07:00 UTC	欧洲、中东或非洲 (EMEA)
星期三	17:00 UTC - 20:00 UTC	亚太、日本、中国 (APJC)
星期四	09:00 UTC - 12:00 UTC	美国 (US)

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。