为 Cisco Secure Firewall Management Center 配置 Umbrella DNS 连接器

首次发布日期: 2023 年 2 月 8 日

上次修改日期: 2023 年 7 月 18 日

为 Cisco Secure Firewall Management Center 配置 Umbrella DNS 连接器

本文档介绍如何在 Cisco Secure Firewall Management Center 设置 Umbrella DNS 连接器。

Umbrella 连接器的优势

管理中心中的 Cisco Umbrella DNS 连接有助于将 DNS 查询重定向到 Cisco Umbrella。这使 Cisco Umbrella 可以根据域名验证请求是被允许还是被阻止，并对请求应用基于 DNS 的安全策略。如果使用 Cisco Umbrella，可以配置 Cisco Umbrella 连接，将 DNS 查询重定向到 Cisco Umbrella。

Umbrella 连接器是系统 DNS 检测的一部分。如果现有 DNS 检测策略映射决定根据 DNS 检测设置阻止或丢弃请求，则该请求不会转发至 Cisco Umbrella。因此，有两条保护防线：本地 DNS 检测策略和 Cisco Umbrella 基于云的策略。

将 DNS 查询请求重定向到 Cisco Umbrella 时，Umbrella 连接器会添加 EDNS （DNS 扩展机制） 记录。EDNS 记录包括设备标识符信息、 组织 ID 和客户端 IP 地址。基于云的策略可以使用 FQDN 信誉以及这些标准来控制访问。还可以选择使用 DNSCrypt 加密 DNS 请求，以确保用户名和内部 IP 地址的隐私性。

系统要求

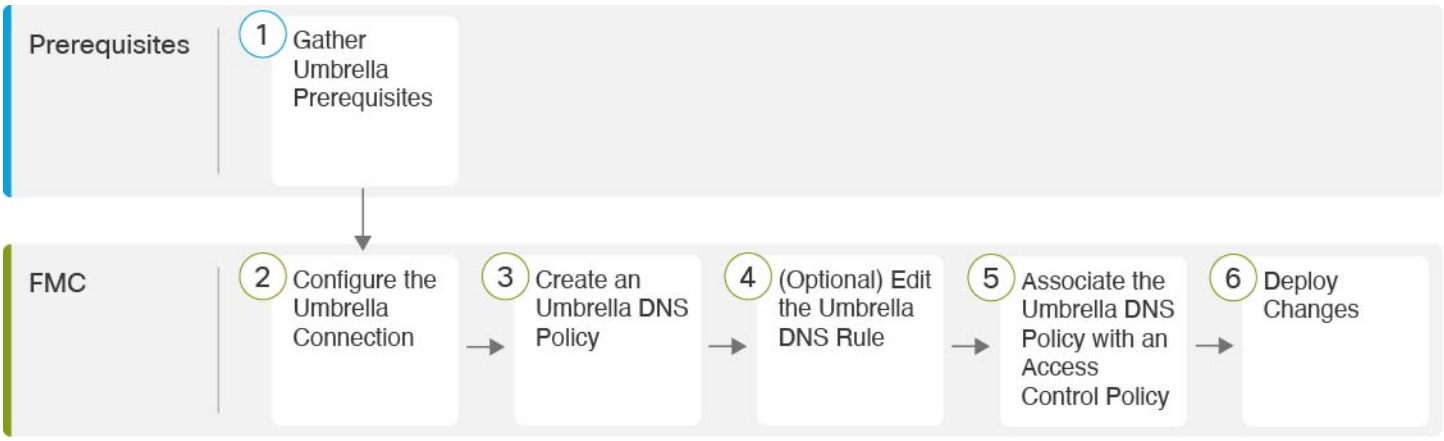
下表显示了此程序所需的产品：

表 *1:* 支持的平台最低版本

产品	版本
Firepower 威胁防御	6.6.0 +
Firewall Management Center	7.2+

配置 FMC Umbrella DNS 连接器

图 *1:* 端到端程序



1	前提条件	收集 Umbrella 前提条件， 第 2 页
2	FMC	配置 Umbrella 连接， 第 4 页
3	FMC	创建 Umbrella DNS 策略， 第 5 页
4	FMC	（可选）编辑 Umbrella DNS 规则， 第 5 页
5	FMC	将 Umbrella DNS 策略与访问控制策略相关联 ， 第 6 页
6	FMC	部署更改 ， 第 6 页

收集 Umbrella 前提条件

开始之前

- 在 https://umbrella.cisco.com 建立 Cisco Umbrella 账户，然后在 http://login.umbrella.com 上登录 Umbrella。
- 将 CA 证书从 Cisco Umbrella 服务器导入管理中心。在 Cisco Umbrella 中，选择**部署 (Deployments)** > **配置 (Configuration)** > **根证书 (Root Certificate)**，然后下载证书。

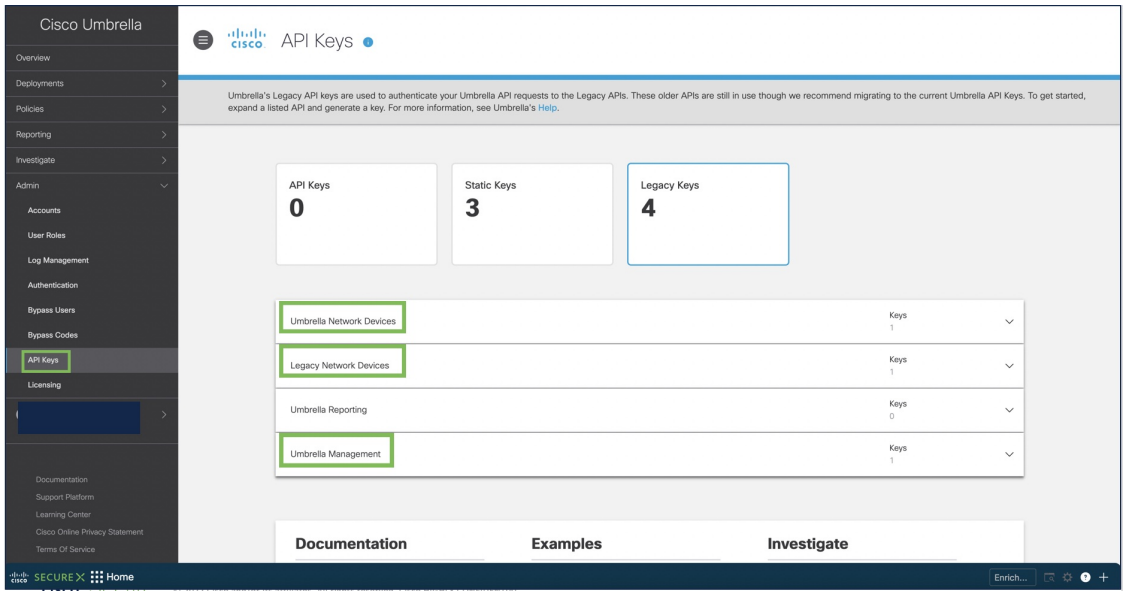
必须导入根证书，才能与 Cisco Umbrella 注册服务器建立 HTTPS 连接。证书需要受信任才能进行 SSL 服务器验证，这是管理中心中的非默认选项。复制并粘贴管理中心中设备的证书（**设备 (Device) > 证书 (Certificates)**）。

- 在设备上安装证书。
- 从 Umbrella 获取以下数据：
  - 组织 ID
  - 网络设备密钥
  - 网络设备密钥
  - 旧版网络设备令牌
- 确保管理中心已连接到互联网。
- 确保已在管理中心中启用具有出口控制功能选项的基础许可证。
- 确保将 DNS 服务器配置为解析 api.opendns.com。
- 确保管理中心可以解析 management.api.umbrella.com 以进行策略配置。
- 将威胁防御路由配置到 api.opendns.com。

过程

步骤 1 在 Umbrella 控制面板中，选择**管理员 (Admin)** > **API 密钥 (API Keys)** > **旧密钥 (Legacy Keys)**。

图 *2:* 用于集成的 ***Umbrella*** 密钥



步骤 2 从以下 URL 获取**组织 ID**：`dashboard.umbrella.com/o/[Organization ID]/#/admin/apikeys`

复制URL中显示的数字，并将其粘贴到管理中心Umbrella连接详细信息页面的**组织ID (Organization ID)** 字段中。

步骤 3 点击 **Umbrella 网络设备 (Umbrella Network Devices)**。

a) 如果**密钥 (Key)** 和**密钥 (Secret)**不可用或未知，请点击**刷新 (Refresh)** 以生成密钥和密钥对。
b) 复制密钥并将其粘贴到 管理中心 Umbrella 连接详细信息页面的**网络设备密钥 (Network Device Key)** 字段中。
c) 复制密钥并将其粘贴到 管理中心 Umbrella 连接详细信息页面的**网络设备密钥 (Network Device Secret)**。

步骤 4 点击**旧版网络设备 (Legacy Network Devices)**。

a) 如果**密钥 (Key)** 不可用或未知，请点击**刷新 (Refresh)** 以生成密钥。
b) 复制密钥并将其粘贴到管理中心Umbrella连接详细信息页面的**旧版网络设备令牌 (Legacy Network Device Token)** 字段中。

配置 Umbrella 连接

过程

步骤 1 在 管理中心 中，选择**集成 (Integration)** > **其他集成 (Other Integrations)** > **云服务 (Cloud Services)** > **Cisco Umbrella 连接 (Cisco Umbrella Connection)**。

步骤 2 获取以下详细信息并将其添加到**常规 (General)** 设置中：

- **组织 ID (Organization ID)** - 在 Cisco Umbrella 上标识您的组织的唯一编号。每个 Umbrella 组织都是一个单独的Umbrella实例，并且有自己的控制面板。组织通过其名称和组织ID（组织ID）进行标识。
- **网络设备密钥 (Network Device Key)** - 从 Cisco Umbrella 获取 Umbrella 策略的密钥。
- **网络设备密钥 (Network Device Secret)** - 从 Cisco Umbrella 获取 Umbrella 策略的密钥。
- **传统网络设备令牌 (Legacy Network Device Token)** - 通过 Cisco Umbrella 控制面板颁发 Umbrella 传统网络设备 API 令牌。Umbrella 需要 API 令牌才能注册网络设备。

步骤 3 在**高级 (Advanced)** 下，配置以下可选设置：

- **DNSCrypt 公共密钥 (DNSCrypt Public Key)** - DNSCrypt 会对终端和 DNS 服务器之间的 DNS 查询进行身份验证和加密。 要启用 DNScrypt，您可以为证书验证配置 DNScrypt 公共密钥。密钥是一个 32 字节的十六进制值，预配置为 B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79，即公共密钥的 Umbrella 任意播服务器。
- **管理密钥 (Management Key)** - 从 Umbrella 云获取 VPN 策略的数据中心详细信息的密钥。

- **管理秘密 (Management Secret)** - 用于从 Umbrella 云获取 VPN 数据中心的秘密。

步骤 4 点击**测试连接 (Test Connection)** - 测试是否可从 管理中心 访问 Cisco Umbrella Cloud。在提供所需的组织 ID 和网络设备详细信息时，您会创建 Umbrella 连接。

步骤 5 添加信息后，点击**保存 (Save)** 以保存连接详细信息。

创建 Umbrella DNS 策略

过程

步骤 1 在 管理中心 中，选择**策略 (Policies)** > **DNS**。系统将显示所有现有的 DNS 策略。

步骤 2 点击**添加 DNS 策略 (Add DNS Policy)** > **Umbrella DNS 策略 (Umbrella DNS Policy)**。

步骤 3 输入策略的名称和说明，然后点击**保存 (Save)**。

（可选）编辑 Umbrella DNS 规则

如果您需要对此程序中所述的设置进行任何更改，请编辑“Umbrella DNS 规则”(Umbrella DNS Rule)。

过程

步骤 1 导航至**策略 (Policies)** > **访问控制 (Access Control)** > **DNS**。

步骤 2 点击要配置的 DNS 策略上的 **编辑**（ ） 图标。

步骤 3 导航到正确的规则，然后再次点击 **编辑**（ ） 图标以编辑规则。

a) **Umbrella 标签**必须与 Umbrella 中配置的内容相匹配。

b) **绕过域 (Bypass Domain)** 指定哪些域应该绕过 Cisco Umbrella 而直接进入 DNS 服务器。

c) **DNSCrypt** 用于加密设备和 Cisco Umbrella 之间的连接。创建新规则时，**DNSCrypt** 的默认设置为 **YES**。

d) 如果 Umbrella 服务器未响应，则**空闲超时 (Idle Timeout)** 会调整将您从 Umbrella 服务器中删除的时间。 在创建新规则时，**空闲超时 (Idle Timeout)** 的默认设置为 00:02:00

空闲超时 (Idle Timeout) 的格式为 (hh:mm:ss)。

将 Umbrella DNS 策略与访问控制策略相关联

过程

步骤 1 导航至**策略 (Policies)** > **访问控制 (Access Control)**，然后选择要编辑的访问策略。

步骤 2 选择**安全智能 (Security Intelligence)**。

步骤 3 在 **Umbrella DNS 策略 (Umbrella DNS Policy)** 下，选择要用于“Umbrella DNS 策略”(Umbrella DNS Policy) 的策略。

步骤 4 选择**保存 (Save)** 以保存所有更改。

部署更改

过程

步骤 1 在 管理中心 菜单栏中，点击**部署 (Deploy)**，然后选择**部署 (Deployment)**。

步骤 2 识别并选择要部署配置更改的设备。

- 搜索 - 在搜索框中搜索设备名称、类型、域、组或状态。
- 展开 - 点击 **展开箭头** （ ） 以查看要部署的设备特定的配置更改。

  选中设备复选框后，该设备下列出的设备的所有更改都会推送到部署中。但是，您可以使用**策略选择**（ ）选择部署个别策略或配置，而保留其余的更改不予部署。

  （可选）使用**显示或隐藏策略**（ ）可选择性地查看或隐藏关联的未修改策略。

步骤 3 （可选）点击**估计 (Estimate)** 以获取粗略估计的部署持续时间。

步骤 4 点击 **部署**。

步骤 5 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

- 部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

验证部署

过程

步骤 1 在部署完成后，请在 管理中心 中验证部署。

步骤 2 选择**部署 (Deploy)**，然后点击**部署历史 (Deployment History)** 图标。

步骤 3 选择与 Umbrella 连接器关联的作业。

步骤 4 选择**脚本详细信息** （）图标。

此时将生成以下命令行界面脚本：

示例：

```
FMC >> strong-encryption-disable
FMC >> umbrella-global
FMC >> token umbrella_token
10.0.0.0 >> [info] : Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
FMC >> local-domain-bypass “test.com"
FMC >> timeout edns hh:mm:ss
FMC >> exit
FMC >> policy-map type inspect dns preset_dns_map
FMC >> parameters
FMC >> umbrella tag “Default Policy”
FMC >> dnscrypt
```

部署问题故障排除

- 旧版网络设备令牌未配置，第 7 页
- 出口管制功能未启用，第 8 页

旧版网络设备令牌未配置

错误：无法配置 Umbrella 全局，因为旧版网络设备令牌为空。

- **可能的原因** Umbrella 连接详细信息未添加到**集成 (Integration)** 选项卡。按照配置 Umbrella 连接，第 4 页来配置**集成 (Integration)** 选项卡中的详细信息。
- **可能的原因** 管理中心 未连接到互联网。如果没有互联网连接，则管理中心无法连接到 Umbrella 云。
- **可能的原因** 已添加 Umbrella 连接详细信息，但信息不正确。按照配置 Umbrella 连接，第 4 页输入正确的信息并测试连接，以确保 Umbrella 已连接。

出口管制功能未启用

您可以启用（注册）或禁用（解除）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。

另外，在评估模式下运行时，还可启用这些许可证的评估版本。在评估模式下，只有注册设备，许可证才会注册到思科智能软件管理器。但是，您不能在评估模式下启用远程访问 RA VPN 或运营商许可证。

开始之前

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。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。

过程

步骤 1 点击菜单中的设备名称，然后点击“智能许可证”(Smart License) 摘要中的**查看配置 (View Configuration)**。

步骤 2 根据需要，点击每个可选许可证的**启用/禁用**控件。

- **启用** - 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。
- **禁用** - 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 如果启用 **RA VPN** 许可证，请选择您账户中可用的许可证类型。

您可以使用以下任意许可证：**Plus**、**Apex** 或**仅 VPN**。如果您有 **Plus 和 Apex** 许可证，并想同时使用它们，则可以两个都选择。

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。