将客户安全地连接到思科安全互联网网关 (SIG)

使用 Cisco Defense Orchestrator 管理 Umbrella

Umbrella 是思科基于云的安全互联网网关 (SIG) 平台，可针对基于互联网的威胁提供多个级别的防御。Umbrella 集成了安全的 Web 网关、防火墙、DNS 层安全和云访问安全代理 (CASB) 功能，以保护系统抵御威胁。通过利用 SIG 和 DNS 保护，ASA 设备将同时受到设备上的本地 DNS 检测策略和基于云的 DNS 检测策略的保护。通过提供多种检查和检测传入流量的方法，Umbrella 使 ASA 设备可与 FTD 下一代防火墙 (NGFW) 相媲美。

目前，CDO 仅支持 ASA 与 Umbrella 组织的集成。

使用 SASE 构建网桥

安全访问服务边缘 (SASE) 是一种前瞻性框架，其中网络和安全功能融合为单一集成服务，可在云边缘提供保护和性能。无论您身在何处，这种努力都可以安全可靠地整合服务，并且无论您的组织规模如何，都可以控制和管理您的网络。降低复杂性和灵活的管理意味着您的部署简单、可扩展且安全。

什么是 Umbrella 组织？

Umbrella 组织是与单个许可证密钥关联的具有不同用户角色的用户组；一个用户可以访问多个 Umbrella 组织。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。组织 ID 用于标识用于部署虚拟设备等组件的组织，有时支持人员可能会要求您提供组织 ID。

什么是 SIG 隧道？

安全互联网网关 (SIG) 隧道是发生在 ASA 和 Umbrella 之间的 SIG IPSec（互联网协议安全）隧道的实例，其中所有互联网绑定流量都转发到 Umbrella SIG 进行检查和过滤。此解决方案提供集中式安全管理，因此网络管理员不必单独管理每个分支机构的安全设置。

当您载入已配置隧道的 Umbrella 组织时，这些隧道将在 CDO 的站点间 VPN 页面中列出。要从 CDO UI 为您的 Umbrella 组织创建 SASE 隧道，请参阅为 Umbrella 配置 SASE 隧道。

注释 如果您载入 Umbrella 组织及其对等设备，则站点间 VPN 页面会将与该组织关联的隧道的所有设备合并为一个条目。要手动刷新“隧道”(Tunnels) 页面并读取从 Umbrella 控制面板所做的任何更改，请参阅读取 Umbrella 隧道配置。

CDO 如何与 Umbrella 通信？

您必须载入 Umbrella 组织以及与该组织关联的任何 ASA 设备。

当 ASA 设备与 Umbrella 云关联时，该连接需要站点间 VPN SIG 隧道来在设备和云之间创建安全连接。CDO 与 Umbrella 组织和 ASA 设备进行通信。这种双重通信方法使 CDO 能够即时检测配置更改或隧道更改，并立即提醒您 Umbrella、ASA 和隧道的更改越界、错误或运行状况不佳。

当您将 Umbrella 组织载入 CDO 时，您需要使用该组织的 API 密钥和密钥载入，这两个密钥对组织和与该组织关联的 ASA 设备都是唯一的。CDO 会通过 Umbrella API 与 Umbrella 云通信，使用用于载入组织的 API 密钥和密钥来请求和发送有关 ASA 设备的信息。此级别的通信不会影响 ASA 和 Umbrella 云之间的 SIG 隧道。

载入 Umbrella 组织后，“设备和服务”(Devices & Services) 页面会将检测到的与该组织关联的任何 ASA 设备显示为“对等体”，并注明设备是否已载入到CDO。如果对等设备尚未载入，您可以点击“载入设备”(Onboard Device) 直接从该页面载入。当与 Umbrella 组织关联的 ASA 设备载入 CDO 时，“设备和服务”(Devices & Services) 页面会显示关系，而“VPN 隧道”(VPN Tunnels) 页面会显示设备与组织之间的隧道。如果与组织关联的 ASA 设备未载入到 CDO，则与该设备关联的隧道会显示在 VPN 隧道中，您可以选择直接从此页面载入设备。

如何从 CDO 访问 Umbrella 云？

将 Umbrella 组织成功载入 CDO 后，您可以从 CDO UI 交叉启动到组织的控制面板或 Umbrella 隧道页面。

请参阅 交叉启动到 Umbrella 控制面板，第 6 页 和 交叉启动到 Umbrella 隧道页面，第 7 页 并从 CDO UI 访问 Umbrella 云。

前提条件

硬件和软件支持。

Umbrella 组织基于云，因此无版本。请注意，当您将 Umbrella 组织载入 CDO 时，您只能将该组织与 ASA 设备关联。

对于 Umbrella 集成，CDO 支持运行 9.1.2 及更高版本的 ASA 设备。有关 CDO 支持的 ASA 设备型号和软件的列表，请参阅云设备支持详情。

许可要求

要成功将 Umbrella 组织载入 CDO，您必须选择以下许可证包之一：

- Umbrella SIG Essentials
- SIG 优势

载入

要成功管理 Umbrella 账户，必须同时载入 载入 Umbrella 组织 和与其关联的 ASA 设备。载入 Umbrella 组织后，CDO 将读取与该组织关联的任何现有 ASA 隧道，并监控这些隧道以及您创建并与该组织关联的任何其他隧道的运行状况。在载入 Umbrella 组织之前，请查看一般设备要求和载入必备条件。

如果您在载入与其关联的任何 ASA 设备之前载入 Umbrella 组织，则可以从 **站点间 VPN** (Site-to-site VPN) 页面查看 ASA 对等体，并从“VPN”页面载入设备。

注释 如果为故障切换配置了 ASA 对，则必须 仅载入两个对等体中的主用设备。将主用和备用设备载入到 CDO 可能会为 Umbrella 中已配置的 SASE 隧道生成重复的隧道信息。

监控网络

CDO 提供总结安全策略的影响的报告，以及查看这些安全策略触发的显着事件的方法。CDO 还会记录您对设备所做的更改，并为您提供一种标记这些更改的方法，以便您可以将您在 CDO 中提交的工作与帮助请求或其他操作请求相关联。

变更日志

更改日志会持续捕获在 CDO 中进行的配置更改。此单一视图包括所有受支持设备和服务的更改。由于 Umbrella 是基于云的产品，因此会立即部署更改。

以下是更改日志的一些功能：

- 并排比较对设备配置所做的更改。
- 所有更改日志条目的纯英文标签。
- 记录设备的载入和删除。
- 检测在 CDO 之外发生的策略更改冲突。
- 回答事件调查或故障排除期间的人员、内容和时间。
- 可以将完整更改日志或仅一部分下载为 CSV 文件。

注释 请注意，当您创建、编辑或删除与 Umbrella 组织关联的 SASE 隧道时，系统会为该 Umbrella 组织以及与其关联的任何 ASA 设备显示请求和配置更改。

Umbrella 文档

- Umbrella 帮助
- Umbrella 和思科 ASA 配置
- 通过隧道连接到思科 Umbrella
- 思科 Umbrella API

载入 Umbrella 组织

Umbrella 许可证要求

要成功将 Umbrella 组织载入 CDO，您必须从 Umbrella 控制面板中选择以下许可证包之一：

- Umbrella SIG Essentials
- SIG 优势

要验证当前已启用的许可证，请登录 Umbrella 控制面板并导航至**管理员 (Admin)** > **许可 (Licensing)**。

生成 API 密钥和秘密

在将 Umbrella 组织载入 CDO 之前，请生成新的 API 密钥并 **同时** 检索 **API 密钥**和相应的**密钥**。

如果当前没有 API 密钥，请使用以下程序创建一个：

开始之前

来自 Umbrella 的管理 API 密钥用于以下 Umbrella 服务：

- 网络和域
- 网络隧道
- 用户和角色
- 目标列表
- 服务提供商

如果不允许 CDO 访问这些服务，则无法载入 Umbrella 组织。

步骤 1 访问思科 Umbrella 控制面板 (Cisco Umbrella dashboard) 并登录您的组织。

步骤 2 在 Umbrella 控制面板中，点击左侧导航窗格中的**管理员 (Admin)**，然后选择 **API 密钥 (API Keys)**。

步骤 3 点击**创建 API 密钥 (Create API Key)**。

如果您已有 API 密钥，但未保存密钥，请导航至**管理员 (Admin)** > **API 密钥 (API Keys)**屏幕，然后点击**刷新 (Refresh)** 以更新密钥和密钥。

步骤 4 要创建新的 API 密钥和密钥，请点击 + 按钮。

步骤 5 输入**名称**并将以下范围添加到 API 密钥：

- 部署。
- 策略。

步骤 6 点击**生成密钥 (Generate Key)**。

步骤 7 复制 API 密钥和相应的密钥。我们建议暂时将信息粘贴到备注或 .txt 中，直到您准备使用它。

Umbrella 组织 ID

您必须使用 Umrbrella 组织的查找组织 ID，并将其与登录凭证一起使用，才能将组织成功载入 CDO：

步骤 1 访问 Cisco Umbrella 控制面板并登录您的组织/

步骤 2 页面 URL 将包含数字标识符。例如，https://dashboard.umbrella.com/o/**123456**/#/overview 的组织 ID 是 **123456**。

步骤 3 从 URL 复制组织 ID。我们建议暂时将信息粘贴到备注中，直到您准备使用它。

载入 Umbrella 组织

使用以下程序将 Umbrella 组织载入 CDO：

开始之前

在载入此环境之前，请阅读Umbrella 许可证要求，第 4 页。

步骤 1 在 Umbrella 控制面板中，找到Umbrella 组织 ID，第 5 页和生成 API 密钥和秘密，第 4 页。在此过程中，请准备好这些项目。

步骤 2 登录至 CDO。

步骤 3 在导航栏中，点击**清单 (Inventory)**。

步骤 4 点击蓝色加号按钮以开始载入设备。

步骤 5 点击 Umbrella 组织。

步骤 6 输入您从 Umbrella 控制面板生成的 Umbrella 网络设备的 **API 密钥**和对应的**密钥**，以及 Umbrella 控制面板 URL 中的**组织 ID**。

步骤 7 点击**下一步**。

步骤 8 （可选）为设备添加唯一**标签**。您可以稍后按此标签过滤设备列表。

步骤 9 点击**转至清单 (Go to Inventory)**。

将 Umbrella 组织重新连接到 CDO

警告 如果存储的凭证无效，则CDO无法向Umbrella组织成功部署或读取配置更改，但CDO可以从与该组织关联的任何ASA设备成功部署或读取更改。更新和验证凭证后，这可能会导致问题。我们建议在部署任何配置更改之前更新组织凭证。

如果 Umbrella 组织的 API 密钥和密钥已刷新或已超时，则必须手动将 Umbrella 组织重新连接到 CDO。使用以下程序重新连接：

步骤 1 前往 Umbrella 控制面板。在左侧导航窗格中点击**管理 (Admin)**，然后选择现有的 Umbrella 管理 **API 密钥**。

步骤 2 点击**刷新**。确认要刷新 API 密钥和密钥。

步骤 3 复制 API 密钥和相应的密钥。

步骤 4 登录至 CDO。

步骤 5 导航至**清单 (Inventory)** 页面。

步骤 6 使用 过滤器或搜索栏查找 Umbrella 组织。

步骤 7 在**设备操作 (Device Actions)** 窗格中，点击**重新连接 (Reconnect)**。CDO 确认存储的 API 密钥和密钥不再有效。

步骤 8 将 API 密钥和密钥粘贴到相应的弹出窗口中。

步骤 9 点击**继续 (Continue)**。

步骤 10 CDO确认新密钥和密钥有效后，点击**关闭**。

交叉启动到 Umbrella 控制面板

一旦 ASA 设备和 Umbrella 组织被成功载入 CDO，您就可以从 CDO UI 交叉启动到组织的控制面板。

使用以下程序来交叉启动设备的 Umbrella 控制面板：

步骤 1 登录 CDO。

步骤 2 点击**设备和服务 (Devices & Services)**。

步骤 3 查找或过滤 Umbrella 组织。

步骤 4 点击管理窗格中的**管理 Umbrella 组织 (Manage Umbrella Organization)** 。CDO 在您的浏览器中启动了一个新选项卡，该选项卡将打开与所选组织关联的 Umbrella 控制面板。

从CDO删除设备

使用以下程序可从 中删除设备：CDO

步骤 1 登录至 CDO。

步骤 2 导航至**清单 (Inventory)** 页面。

步骤 3 找到要删除的设备，然后选中设备行中的设备以将其选中。

步骤 4 在右侧的“设备操作”(Device Actions) 面板中，选择**删除 (Remove)**。

步骤 5 出现提示时，选择**确定 (OK)** 以确认删除所选设备。选择**取消 (Cancel)** 以使设备保持已载入状态。

配置 Cisco Umbrella 组织

读取 Umbrella 隧道配置

在 Umbrella 组织载入到 CDO 后，您可以手动强制 CDO 从 Umbrella 请求和更新隧道配置。这包括添加、删除或修改的隧道。

警告 如果在 Umbrella 组织凭证被视为无效的情况下从 CDO 中删除隧道，或者在您载入组织后发生了变化，则 CDO 只能将隧道配置部署到与该组织关联的 ASA 设备。更新凭证后，CDO 会读取 Umbrella 配置并重新填充已删除的任何隧道。由于隧道存在于 Umbrella 组织中，但不存在于任何 ASA 设备中，因此会出现同步问题，并且 ASA 设备可能不会显示为组织的对等体。

步骤 1 登录 CDO。

步骤 2 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

步骤 3 点击 **ASA** 选项卡。

步骤 4 选择 Umbrella 组织，使其突出显示。

步骤 5 在 **操作** 窗格中，选择 **读取隧道**。

交叉启动到 Umbrella 隧道页面

在将 ASA 设备和 Umbrella 组织成功载入 CDO 后，您可以从 CDO UI 交叉启动隧道的 Umbrellas 控制面板。

使用以下程序交叉启动设备的 Umbrella 隧道页面：

步骤 1 登录 CDO。

步骤 2 导航到 VPN 窗口。选择**站点间 VPN (Site-to-Site VPN)**。

步骤 3 选择所需的隧道，使其突出显示。

步骤 4 在“操作”(Actions) 窗格中，点击**管理 Umbrella 中的隧道 (Manage Tunnel in Umbrella)**。CDO 在浏览器中启动一个新选项卡，打开“隧道”(Tunnels) 概述页面。

为 Umbrella 配置 SASE 隧道

使用以下程序为 Umbrella 组织创建一个 SASE 隧道：

开始之前

请注意，您要为其创建隧道的 Umbrella 组织和 ASA 设备**必须**已经载入 CDO。

如果与您刚部署的隧道关联的 ASA 或 Umbrella 组织处于不正常状态，则 CDO 可能无法成功部署隧道。如果您遇到任何问题，请联系思科 TAC。

步骤 1 登录 CDO。

步骤 2 导航到 **VPN** 窗口。选择**站点间 VPN (Site-to-Site VPN)**。

步骤 3 点击蓝色加号按钮，然后选择**创建 SASE 隧道 (Create SASE Tunnel)**。

步骤 4 输入 Umbrella 对等体信息：

- **选择 Umbrella (Select Umbrella)** - 选择您所选的 **Umbrella** 组织。
- **数据中心 (Datacenter)** - 选择前端数据中心。我们建议选择在地理位置上靠近与 Umbrella 组织关联的 ASA 的数据中心。

步骤 5 输入 ASA 对等体信息：

- **选择 ASA 设备 (Select ASA Device)** - 从下拉列表中选择与 Umbrella 组织关联的 ASA 设备，然后点击**选择 (Select)**。
- **公共接口 (Public Facing Interface)** - 选择静态且可公开路由的 IPv4 地址。所用的地址不应被用于 NAT。
- **LAN 地址 (LAN Address)** - 选择控制 LAN 子网的 LAN 接口。您必须至少为 LAN 选择一个接口。
- **虚拟隧道接口 (Virtual Tunnel Interface)** - 在选择 Umbrella 组织和 ASA 对等设备后，系统会自动填充此字段。如有必要，您可以手动输入要用作新 VTI 的 IP 地址。

步骤 6 在选择 Umbrella 组织和 ASA 对等设备后，系统会自动填写**密码**。**确认密码 (Confirm Passphrase)** 也会被自动填写。如有必要，您可以手动输入这些字段。

步骤 7 （可选）弹出窗口底部的**立即部署对 ASA 的更改 (Deploy changes to ASA immediately)** 会被默认启用。如果启用，SASE 隧道配置会立即部署到在隧道配置中选择的 ASA 对等体。如果要暂存更改并稍后部署，请手动将该选项切换为禁用。

步骤 8 点击**部署 (Deploy)**。或者，点击**部署并创建另一个 (Deploy and Create Another)**，以便同时部署此 SASE 隧道并创建另一个隧道。部署后，隧道将显示在“VPN 隧道”(VPN Tunnels) 页面中。如果您选择**部署并创建另一个 SASE 隧道 (Deploy and Create Another SASE tunnel)**，CDO 会同时保存 Umbrella 组织选择和**将更改立即部署到 ASA (Deploy changes to ASA immediately)** 切换设置，并自动将这些选择应用到下一个隧道配置。您可以在部署之前手动更改这些选择。

编辑 SASE 隧道

使用以下程序修改现有 SASE 隧道：

步骤 1 登录 CDO。

步骤 2 导航到 **VPN** 窗口。选择**站点间 VPN (Site-to-Site VPN)**。

步骤 3 选择要修改的隧道。

步骤 4 在“操作”(Actions) 窗格中，选择**编辑 (Edit)**。

步骤 5 编辑 SASE 隧道的以下字段：

- **名称** - 更改 CDO 和 Umbrella 控制面板中显示的 SASE 隧道的名称。
- **Umbrella 对等体的数据中心** - 从下拉菜单中选择新的前端数据中心。
- **ASA 对等体的公共接口** - 从下拉菜单中选择新的 IPv4 地址。
- **ASA 对等体的 LAN 接口** - 从下拉菜单中选择一个或多个新的 LAN 接口。
- **ASA 虚拟隧道接口 (VTI) 地址** - 手动编辑 VTI。
- **密码** - 手动修改隧道的密码。
- **确认密码** - 手动修改此条目以匹配密码并确认新值。

步骤 6 （可选）弹出窗口底部的**立即部署对 ASA 的更改 (Deploy changes to ASA immediately)** 会被默认启用。如果启用，SASE 隧道配置会立即部署到在隧道配置中选择的 ASA 对等体。如果要暂存更改并稍后部署，请手动将该选项切换为禁用。如果您选择暂存更改并稍后部署，则**清单 (Inventory)** 页面中的 ASA 对等体状态显示为待部署 (Deploy Pending)。

步骤 7 选择**保存更新**。

从 Umbrella 中删除 SASE 隧道

使用以下程序通过 CDO UI 删除 SASE 隧道：

开始之前

要删除 SASE 隧道，与其关联的 ASA 在 CDO 中必须处于同步状态。如果设备运行状况不佳，则无法删除隧道。

请注意，如果从 CDO 中删除 SASE 隧道，则会从 ASA 设备和与其关联的 Umbrella 组织中删除该隧道。

警告 如果在 Umbrella 组织凭证被视为无效的情况下从 CDO 中删除隧道，或者在您载入组织后发生了变化，则 CDO 只能将隧道配置部署到与该组织关联的 ASA 设备。更新凭证后，CDO 会读取 Umbrella 配置并重新填充已删除的任何隧道。由于隧道存在于 Umbrella 组织中，但不存在于任何 ASA 设备中，因此会出现同步问题，并且ASA 设备可能不会显示为组织的对等体。我们建议在删除与组织关联的任何隧道之前确认 Umbrella 凭证。

步骤 1 登录 CDO。

步骤 2 导航到 **VPN** 窗口。选择**站点间 VPN (Site-to-Site VPN)**。

步骤 3 选择要从 CDO 中删除的隧道。

步骤 4 在“操作”(Actions) 窗格中，点击**删除 (Delete)**。

步骤 5 确认要删除隧道，然后点击**确定 (OK)**。

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。