Umbrella 漫游安全

Umbrella 漫游安全模块要求订用思科 Umbrella 漫游服务（包含 Professional、Insights、Platform 或 MSP 软件包）。思科 Umbrella 漫游可在没有处于活动状态的 VPN 时提供 DNS 层安全，思科 Umbrella 订用将在线或离线添加智能代理和 IP 层实施功能。此外，思科 Umbrella 订用还将提供内容过滤、多重策略、稳健性报告、Active Directory 集成等更多功能。无论订用情况如何，都将使用相同的 Umbrella 漫游安全模块。

Umbrella 漫游模块配置文件 (OrgInfo.json) 会将各种部署与相对应的服务关联起来，并将自动启用相对应的保护功能。

可以通过 Umbrella 控制面板实时查看源自漫游安全模块的所有互联网活动。策略和报告中的精细度级别取决于 Umbrella 订用情况。

有关各个服务级别订用中包含哪些功能的详细对比，请参阅 https://umbrella.cisco.com/products/packages。

Umbrella 漫游客户端与 Umbrella 漫游安全模块不兼容

Umbrella 漫游安全模块与 Umbrella 漫游客户端不兼容。如果您要部署 Umbrella 漫游安全模块，在安装漫游安全模块过程中将检测任何现已安装的 Umbrella 漫游客户端并自动删除，以防止冲突。如果现已安装的 Umbrella 漫游客户端与某项 Umbrella 服务订用相关联，会将该项服务订用自动迁移至 Umbrella 漫游安全模块，除非 OrgInfo.json 文件与配置用于网络部署或预部署的 AnyConnect 安装程序处于 Umbrella 模块目录中的同一位置。您也可能希望在部署 Umbrella 漫游安全模块之前手动卸载 Umbrella 漫游客户端。

获得思科 Umbrella 帐户

Umbrella 控制面板 (http://dashboard.umbrella.com/) 是登录页面，您可在此获得用于要包括在您的部署中的 AnyConnect Umbrella 漫游安全模块的配置文件 (OrgInfo.json)。您还可以在此对漫游客户端活动的策略和报告进行管理。

从控制面板下载 OrgInfo 文件

OrgInfo.json 文件包含关于您的 Umbrella 控制面板实例的具体信息，可让漫游安全模块了解向哪里报告，以及需要实施哪些策略。

要为部署 AnyConnect Umbrella 漫游安全模块做好准备，请从 Umbrella 控制面板获取 OrgInfo.json 文件 (https://dashboard.umbrella.com)。

单击“身份 (Identities)”菜单结构中的**漫游计算机 (Roaming Computers)**，然后单击页面左上角的 + 符号。向下滚动到 AnyConnect Umbrella 漫游安全模块并单击**模块配置文件 (Module Profile)**。有关具体说明/部署步骤以及软件包和文件的具体信息，请参阅 AnyConnect 部署概述。

注释 在首次部署 OrgInfo.json 文件时，会将该文件复制到数据子目录 (/umbrella/data) 中，还会在该子目录中创建几个其他注册文件。因此，如果您需要部署替代 OrgInfo.json 文件，则必须删除该数据子目录。或者，您也可以卸载 Umbrella 漫游安全模块（这将删除该数据子目录），然后使用新 OrgInfo.json 文件重新安装。

安装和运行 Umbrella 漫游安全

在部署 AnyConnect 时，Umbrella 漫游安全模块是您可以引入以启用额外功能的众多可选模块之一。

注释 如果您与网络安全模块一起部署 Umbrella 漫游安全模块，必须进行配置，以排除网络安全和漫游的安全兼容性所需的主机例外和网络安全与 Umbrella 漫游安全模块兼容性所需的静态例外中引用的静态和主机例外。

对于 Windows 7 SP1 用户，我们建议您在安装和首次使用之前安装 Microsoft .NET framework 4.0。在启动时，Umbrella 服务将检查是否已安装了 .NET framework 4.0（或更高版本）。如果未检测到，则不会激活 Umbrella 漫游安全模块，并将显示一条消息。下载然后安装 .NET Framework，必须重新启动才能激活 Umbrella 漫游安全模块。

配置 OrgInfo.json 文件

OrgInfo.json 文件包含关于您的 Umbrella 服务订阅的具体信息，可让安全漫游模块了解向哪里报告，以及需要实施哪些策略。可以使用 CLI 或 GUI 从 ASA 或 ISE 来部署 OrgInfo.json 文件并启用 Umbrella 漫游安全模块。下面的步骤首先描述了如何从 ASA 启用，然后描述了如何从 ISE 启用：

ASA CLI

1. 将您从 Umbrella 控制面板 (https://dashboard.umbrella.com) 获得的 OrgInfo.json 上传到 ASA 文件系统。
2. 发布以下命令，针对您的配置根据需要调整组策略名称。

```
webvpn
 anyconnect profiles OrgInfo disk0:/OrgInfo.json

group-policy DfltGrpPolicy attribute
 webvpn
  anyconnect profiles value OrgInfo type umbrella
```

ASDM GUI

1. 导航到 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
2. 选择 **Add**。
3. 为简档命名。
4. 从 Profile Usage 下拉菜单中选择 Umbrella 安全漫游客户端类型。OrgInfo.json 文件将填充在 Profile Location 字段中。
5. 单击 **Upload**，然后浏览到您从控制面板下载的 OrgInfo.json 文件的位置。
6. 将其与 Group Policy 下拉菜单上的 DfltGrpPolicy 关联起来。请参阅启用其他 AnyConnect 模块以在组策略中指定新模块名称。

ISE

按照以下步骤操作，以从 ISE 启用：

1. 上传来自 Umbrella 控制面板 https://dashboard.umbrella.com 的 OrgInfo.json。
2. 重命名文件 OrgInfo.xml。
3. 按照配置 ISE 以部署 AnyConnect中的步骤操作。

云更新

Umbrella 漫游安全模块可从 Umbrella 云基础设施为所有已安装的 AnyConnect 模块提供自动更新。通过云更新，可自动从 Umbrella 云基础设施获得软件升级，且更新跟踪将取决于该软件升级，而非管理员的任何操作。

默认情况下，将禁用通过云更新进行自动更新。要为 Umbrella 漫游安全和 AnyConnect 的其余模块启用云更新，请登录到 Umbrella 控制面板。在**身份 (Identities) > 漫游计算机 (Roaming Computers) >** 设置图标（齿轮图标）下，选中**无论何时发布新版本，都自动更新 AnyConnect，包括 VPN 模块 (Automatically update AnyConnect, including VPN module, whenever new versions are released)**。更新将在 VPN 处于活动状态时进行。默认情况下，不会选择此选项。

需要考虑以下有关云更新的情况：

- 只会更新当前安装的软件模块。
- 不支持定制、本地化和任何其他部署类型。
- 更新仅在登录到桌面时才会进行，如果建立了 VPN，则不会进行更新。
- 当禁用更新时，最新软件功能和更新将不可用。
- 禁用云更新对其他更新机制或设置（例如网络部署、延迟更新等）没有影响。
- 云更新将忽略装有较新、未发布的版本（例如临时版本和修补版本）AnyConnect 的设备。

配置安全策略以及审核报告

您必须有思科 Umbrella 漫游帐户，才能接受保护、查看报告信息以及配置策略。请访问 https://docs.umbrella.com/product/umbrella/ 以了解深入说明，或请访问 https://support.umbrella.com 以了解更多信息。

在安装后，可在 90 分钟至 2 小时后在您的 Umbrella 控制面板中看到漫游计算机。导航到 https://dashboard.umbrella.com 进行身份验证，然后转到 **Identities > Roaming Computers**，将显示漫游客户端的列表（包括处于活动状态和非活动状态的漫游客户端），以及关于每个已安装客户端的详情。

最初将为您的漫游计算机应用包含基本安全筛选级别的默认策略。此默认策略可在控制面板的Policies 部分（或 Configuration > Policy for Cisco Umbrella accounts）中找到。

可在 Policies 部分下找到漫游客户端的报告。选中 Activity Search 报告以查看来自装有 Umbrella 漫游安全模块并已关闭 VPN 的计算机的 DNS 流量。

了解您将在终端上看到哪些 UI 变化

在 AnyConnect UI 中，Umbrella 漫游安全模块图块将提供当前状态。

状态	图标颜色	说明	情况
保留	橙色	检查连接状态。Umbrella 模块尚未确定保护状态。	此操作状态将在以下条件下发生： • 当首次激活该模块时。 • 当网络接口发生更改时（例如检测到新的网络适配器、现有适配器上的 IP 更改，或已建立或中断新 VPN 隧道）。
开放	黄色	您当前不受 *Umbrella* 保护。由于与 Umbrella 解析器的连接问题，因此本地 Umbrella 模块 DNS 保护处于不活动状态。至少有一个活动网络连接；但漫游客户端无法连接到任何活动连接上的 Umbrella 服务。 系统的 DNS 设置恢复为其原始设置（DHCP 或 Static）。	此操作状态将在以下条件下发生： • UDP 端口 443 或 UDP 端口 53 没有连接到 Umbrella 解析器 (208.67.222.222)。 • 未在本地网络上配置 Umbrella DNS VA。 • VPN 隧道可能暂时处于断开或建立状态。
受到保护	绿色	您受 *Umbrella* 保护。DNS 查询未加密。本地 Umbrella 模块 DNS 保护处于活动状态，并以未加密形式将 DNS 请求发送到 Umbrella 解析器。	当首次激活该模块或者网络接口发生更改时，可能会发生这种状态。
已加密	绿色	您受 *Umbrella* 保护。DNS 查询已加密。本地 Umbrella 模块 DNS 保护处于活动状态，并以加密形式将 DNS 请求发送到 Umbrella 解析器。	此操作状态将在以下条件下发生： • UDP 端口 443 连接到 Umbrella 解析器 (209.67.222.222)。 • TCP 端口 443 和 TCP 端口 53 连接到 Umbrella 解析器 (208.67.222.222)。

状态	图标颜色	说明	情况
受保护的网络	绿色	您所在的网络受 *Umbrella* 保护。由于使用 Umbrella 解析器保护当前终端网络保护，因此本地 Umbrella 模块 DNS 保护处于不活动状态。漫游客户端已将 DNS 设置重新恢复为通过 DHCP 设置或静态设置的内容。连接未加密。	此操作状态将在以下条件下发生： • 使用与当前终端相同的 Umbrella 帐户注册该终端的网络出口 IP 地址。 • 使用的解析器是 Umbrella 云解析器（208.67.222.222、208.67.220.220）。 • 通过 Umbrella 控制面板配置的策略 (Disable Behind Protected Networks) 规定，在受保护的网络上时应该禁用 Umbrella 模块。 注释 对于所有思科 Umbrella 漫游软件包客户，此状态不可能发生，因为没有网络级保护。
在虚拟设备后台	绿色	您受 *Umbrella* 虚拟设备保护。由于将 Umbrella 虚拟设备配置为内部 DNS 解析器，因此本地 Umbrella 模块 DNS 保护处于不活动状态。客户端漫游禁用自己，并将 DNS 设置重新恢复为通过 DHCP 设置或静态设置的内容。连接未加密。	当终端配置的 DNS 地址（通过 DHCP 或静态）为 Umbrella VA 地址时，将发生此操作状态。
Umbrella 受信任网络状态	灰色	在访问受信任网络时被禁用。由于将当前终端网络配置为 Umbrella 受信任网络，因此本地 Umbrella 模块 DNS 保护处于不活动状态。	此操作状态将在以下条件下发生： • 使用魔力域名配置了 Umbrella 控制面板。 • 在本地 DNS 解析器上配置了相对应的魔力域名或记录。

状态	图标颜色	说明	情况
VPN 受信任网络状态	灰色	在访问受信任网络时被禁用。由于将当前终端网络配置为 AnyConnect VPN 受信任网络，因此本地 Umbrella 模块 DNS 保护处于不活动状态。	此操作状态将在以下条件下发生： • AnyConnect VPN 模块报告受信任网络检测的状态为受信任。 • AnyConnect VPN 隧道在全隧道模式下未连接或未建立。 • 通过 Umbrella 控制面板配置的策略规定，在 AnyConnect VPN 受信任网络上时应该禁用 Umbrella 模块。 **注释** 对于所有漫游软件包客户而言，此设置为 true，并且管理员无法更改。
由于 VPN 状态而被禁用	灰色	当 *VPN* 处于活动状态时被禁用。由于终端当前已建立处于活动状态的 AnyConnect VPN 隧道，因此本地 Umbrella 模块 DNS 保护处于不活动状态。	此操作状态将在以下条件下发生： • AnyConnect VPN 模块报告受信任网络检测状态为不受信任。 • 在全隧道模式下建立 AnyConnect VPN 隧道。 • 通过 Umbrella 控制面板配置的策略规定，在建立 AnyConnect VPN 隧道时应该禁用 Umbrella 模块。 **注释** 对于所有漫游软件包客户而言，此设置为 true，并且管理员无法更改。
无 OrgInfo.json 状态	红色	您当前不受 *Umbrella* 保护。缺少配置文件。由于终端当前已建立处于活动状态的 AnyConnect VPN 隧道，因此本地 Umbrella 模块 DNS 保护处于不活动状态。	当 OrgInfo.json 文件未部署到以下适当目录中时，将发生此操作状态： Windows：%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella macOS：opt/cisco/anyconnect/umbrella
代理不可用状态	红色	您当前不受 *Umbrella* 保护。服务不可用。由于 Umbrella 代理没有运行，因此本地 Umbrella 模块 DNS 保护处于不活动状态。	当 Umbrella 代理服务当前没有运行时（由于崩溃或手动服务停止），将发生此操作状态。

状态	图标颜色	说明	情况
缺少 .NET 依赖性状态（仅限 Windows）	红色	您当前不受 *Umbrella* 保护。未安装 Microsoft 4.0 NET 框架。由于 Umbrella 代理没有运行，因此本地 Umbrella 模块 DNS 保护处于不活动状态。缺少 .NET 运行时框架。	当 Umbrella 代理服务由于缺少 .NET 4.0 运行时而没有运行时，将发生此操作状态。

AnyConnect UI 还将在 Umbrella 漫游安全模块中显示统计数据和消息历史记录。

对诊断进行解读

您应运行 DART 报告，以诊断任何思科 Umbrella 漫游安全模块问题。有关 Umbrella 的问题和故障排除详情，请参阅 docs.umbrella.com。