Zero Trust 访问模块

Zero Trust 访问

当您在 Cisco Secure Client 磁贴中看到“已注册 Zero Trust 访问”(Enrolled in Zero Trust Access) 时，就表明 Zero Trust 访问模块已启用并正在运行。此访问涉及了解、了解和控制网络上的人员和内容。通过明确了解用户，可根据用户的角色或职能以及这些角色所拥有的网络权限授予适当的访问权限。除 AnyConnect VPN 之外，它还为整个网络提供更精细的控制和安全的用户体验。虽然 VPN 信任通过网络控制的任何人或任何事物，但 Zero Trust 访问方法是不信任任何具有访问权限的用户或设备，直到得到证实。没有人会自动得到信任；并且经过验证后，只能提供和重新验证有限的访问权限。它将 Zero Trust 模型扩展到网络之外，并通过隐藏互联网应用来减少受攻击面。

目前，Zero Trust 访问模块仅支持思科安全访问服务。有关其他详细信息，请参阅安全访问文档。它涵盖配置专用资源以允许 Zero Trust 连接、设置访问规则以确定可以使用这些连接访问资源的人员、流量控制等。

启动并运行 Zero Trust 访问

要使用预部署进行安装，请下载适用于 Windows 的 **cisco-secure-client-win-版本-zta-k9.msi**。对于 macOS 预部署，下载 **cisco-secure-client-macos-版本-predeploy-k9.dmg**，Zero Trust 模块将成为其可选组件的一部分。

要使用 webdeploy 进行安装，请下载适用于 Windows 的 **cisco-secure-client-win-版本-webdeploy-k9.pkg**。ASA 配置的模块名称为 zta。要为 macOS 安装 webdeploy，请下载 **cisco-secure-client-macos-版本-webdeploy-k9.pkg**

在 Windows 上，Duo Desktop 也将打包在此模块安装程序中并自动安装，即使它是未与 Cisco Secure Client 集成的独立应用。但是，在 macOS 上，Duo Desktop 需要单独安装，在 macOS 11（及更高版本）上通过 MDM 部署 Zero Trust 访问时，Duo Desktop 有自己的其他设置要求。有关这些额外的 Duo 设置要求，请参阅《适用于 macOS 11+ 用户的 Duo 设备运行状况应用证书部署指南》。有关任何其他 Duo 详细信息，请参阅 Duo Desktop 文档。

安装软件后，系统会提示用户使用 Zero Trust 访问模块登录服务，以获取客户端证书和必要的服务 URL。Cisco Secure 访问注册涉及用户身份验证部分，并且这些注册在重新启动后仍然存在。注册存储在全局/计算机上下文中，但与本地用户相关联，并在每个本地用户的基础上应用。

开始之前

- Windows 10 和 11（支持 TPM 的设备）以及 macOS 11、12、13 和 14（支持 TPM 的设备）支持 Zero Trust 访问模块。
- Windows 设备必须在包含可信平台模块 2.0 版的系统上运行。macOS 设备必须在包含 Secure Enclave 的系统上运行，例如配备 Apple T1 芯片的带 Touch Bar 的 MacBook Pro（016 和 2017）、配备 Apple T2 安全芯片的基于 Intel 的 Mac 计算机或配备 Apple 芯片的 Mac 计算机。
- 如果要使用 Zero Trust 访问模块，则必须安装 Windows WebView2，并且必须进行带外部署。
- 如果您在 macOS 11 或更高版本上预部署 Zero Trust 访问，请参阅macOS 11（及更高版本）上的其他 Duo Desktop 要求以了解其他要求。
- 您必须具有符合以下条件的 AnyConnect VPN 和 Zero Trust 访问版本才能正常运行：AnyConnect VPN 需要 5.1.1.38，Zero Trust 访问需要 5.1.1.4867。
- 为获得最佳性能，您应使用动态分割排除隧道从隧道中排除以 zpc.sse.cisco.com 为目标的流量。有关配置步骤，请参阅配置动态拆分排除隧道。如果通过隧道解析该域不会生成具有最佳地理位置的 IP 地址，则还应为分割排除配置分割 DNS，以便仅在隧道外部尝试解析其名称。有关分割排除隧道配置，请参阅拆分 DNS。

当前限制：

- macOS 上没有 Duo Desktop 日志的 DART 收集。
- 不支持服务器首先发送流量的隧道应用（例如： MySQL）。
- 当多个用户同时登录到一个终端时，Zero Trust 访问功能将被禁用。
- 支持不依赖于 ICMP 或 DNS SRV 发现的任何客户端 TCP 或 UDP 应用，但存在以下限制：
  - 所有 TCP 连接或 UDP 流都必须由客户端应用发起。
  - 不支持服务器上需要唯一客户端 IP 地址的任何协议，例如 SMBv1。（SMBv3 按预期工作。）

步骤 1 要开始使用 Zero Trust 访问，需要注册。在 Cisco Secure Client 的 Zero Trust 访问磁贴中点击**注册 (Enroll)** 。

步骤 2 输入您的工作电子邮件地址。

步骤 3 如果在 SSO/SAML 登录中自动选择了所需的组织，请输入用于身份验证的邮箱地址和密码。如果您属于多个组织，请从下拉菜单中选择相应的组织。
当身份验证过程完成或继续注册时，系统将显示 Zero Trust 访问磁贴。Zero Trust 访问模块安装到一个通用的 Cisco Secure Client 文件夹：

- Windows: C:\Program Files (x86)\Cisco\Cisco Secure Client\ZTA
- macOS: /opt/cisco/secureclient/zta

注释 为了在注册过程中获得最高安全性，强烈建议您利用已建立的基于MFA的身份验证，并使用生物识别身份进行用户身份验证。

下一步做什么

有关 DART 日志文件的位置，请参阅对 Zero Trust 访问模块进行故障排除 ， 第 5 页 。

有关这些程序，请参阅如何取消注册 ， 第 3 页或如何卸载 ， 第 3 页。

有关互操作性要求和预期流程，请参阅Zero Trust 访问模块的操作详细信息 ， 第 4 页。

启动资源访问

注册完成后，Zero Trust访问磁贴会显示其处于活动状态。然后，您可以开始访问管理员根据访问规则定义为可用的内部应用。任何资源访问问题都显示在“Zero Trust访问模块”磁贴中。您可以点击**详细信息**，了解有关影响安全资源访问的内容的其他信息。

如何取消注册

如果要从 Zero Trust 访问服务注销，请点击 Zero Trust 访问模块中的**高级 (Advanced)** 选项卡，然后点击**取消注册 (Unenroll)**。它会注销您的帐户，删除客户端证书，并从您的服务中删除任何关联的配置。

如何卸载

在 macOS 中，使用 UI 安装程序或命令行卸载 AnyConnect VPN 或仅使用 Zero Trust 访问模块。在 Windows 中，使用“添加/删除程序”卸载 AnyConnect VPN 或仅使用 Zero Trust 访问模块。卸载 Zero Trust 访问不会卸载 Duo Desktop。

配置 Zero Trust 访问

注册后，Zero Trust 访问模块会执行配置同步，以获取相应文件夹中的初始 json 配置。之后，它会定期检查以确保文件夹中包含最新的 json 文件。检查返回的内容将确定 Zero Trust 访问是否不需要更改配置，或者是否需要下载新配置。根据需要，您还可以选择 Zero Trust 访问模块中的**配置 (Configuration)** 选项卡，然后点击**立即同步 (Sync Now)** 以从 SSE 控制面板提取最新的 json 文件。系统将显示上次配置同步的日期。

所有其他配置都通过云中的 Cisco Secure 访问来完成。

Zero Trust 访问模块的操作详细信息

要排除的域

为了与 VPN 和 Umbrella SWG 实现适当的互操作性，应从 VPN 隧道和 SWG 代理中排除以下域（以及基础子域/主机）：

- ztna.sse.cisco.com（注册）
- acme.sse.cisco.com（证书）
- devices.api.umbrella.com（配置同步）
- zpc.sse.cisco.com（代理）
- sseposture-routing-commercial.k8s.5c10.org（终端安全评估）
- sseposture-routing-commercial.posture.duosecurity.com（终端安全评估）

保存配置文件的路径

配置文件存储在全局目录中，但按本地用户进行跟踪。本地注册文件保存在以下位置：

Windows— C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments

macOS— /opt/cisco/secureclient/zta/enrollments

可以在此处找到缓存的配置文件：

Windows—C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments\cached_configs

macOS—/opt/cisco/secureclient/zta/enrollments/cached_configs

与其他安全客户端模块的互操作性

Zero Trust 访问拦截的任何流量将不可用于 Umbrella 代理或 VPN 隧道。拦截的第一个流量是 Zero Trust 访问，其次是 Umbrella DNS/SWG，然后是 VPN。同样，Network Visibility Module 报告不会报告已被Zero Trust访问拦截的单个网络流。它只会向 Zero Trust 访问代理报告网络流量，其中包含 Zero Trust 访问拦截的加密应用流。

证书详细信息

证书的有效期为五周，续约尝试在到期前两周开始。续约时，系统会生成新的密钥。如果未执行自动续约，则用户必须遵循重新注册流程。使用 Windows 上的 TPM 和 macOS 上的系统密钥链在平台的系统证书存储区中生成密钥。取消注册或卸载时，将删除证书/密钥。

对 Zero Trust 访问模块进行故障排除

Zero Trust 访问遇到的任何错误都会显示在“Zero Trust 访问”(Zero Trust Access) 磁贴上或安全客户端 UI 的“消息历史记录”(Message History) 选项卡中。

您可能会遇到以下任何情况：

- 身份验证要求
- 需要启用和打开的防火墙
- 拒绝访问的权限错误
- 由于中断或移动到新位置而无法访问的应用

DART 会收集用于对 Cisco Secure Client 安装和进行故障排除的数据。您必须安装诊断和报告工具 (DART) 并以管理员身份运行该工具。默认情况下，客户端的所有必要日志都存储在 DARTBundle.zip 中，并保存到本地桌面。您还可以通过创建自定义捆绑包来指定要包含在捆绑包中的文件以及存储文件的位置。默认情况下，数据收集基于美国区域格式 (MM/DD/YY)。

注释 增强了 DART 以收集 Duo Desktop 日志。在 Windows 上，Duo 使用 PowerShell 脚本收集日志。由于默认情况下会阻止 PowerShell 脚本执行，因此只有在以管理员权限启动时，DART 才能收集 Duo 日志。在初始 5.1 版本中，DART 不会在 macOS 上收集 Duo Desktop 日志。它将为 Windows 收集相关数据。

当 Cisco Secure Client 在 Windows 设备上运行时，DART 会启动。对于 macOS 设备，请选择**应用 (Applications) > Cisco > Cisco DART**。然后点击齿轮图标和**诊断 (Diagnostics)**。

要增强日志记录并获得更多可视性以进行故障排除，您可以使用 logconfig.json 文件来启用 Zero Trust 访问的跟踪日志记录。

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。