安装 Citrix Secure Access 应用程序

安装适用于 Windows 的 Citrix Secure Access 客户端

- 有关安装适用于 Windows 的 Citrix Secure Access 客户端的详细信息，请参阅安装适用于 Windows 的 Citrix Secure Access 客户端。
- 有关如何使用适用于 Windows 的 Citrix Secure Access 客户端的详细信息，请参阅如何使用适用于 Windows 的 Citrix Secure Access 客户端。

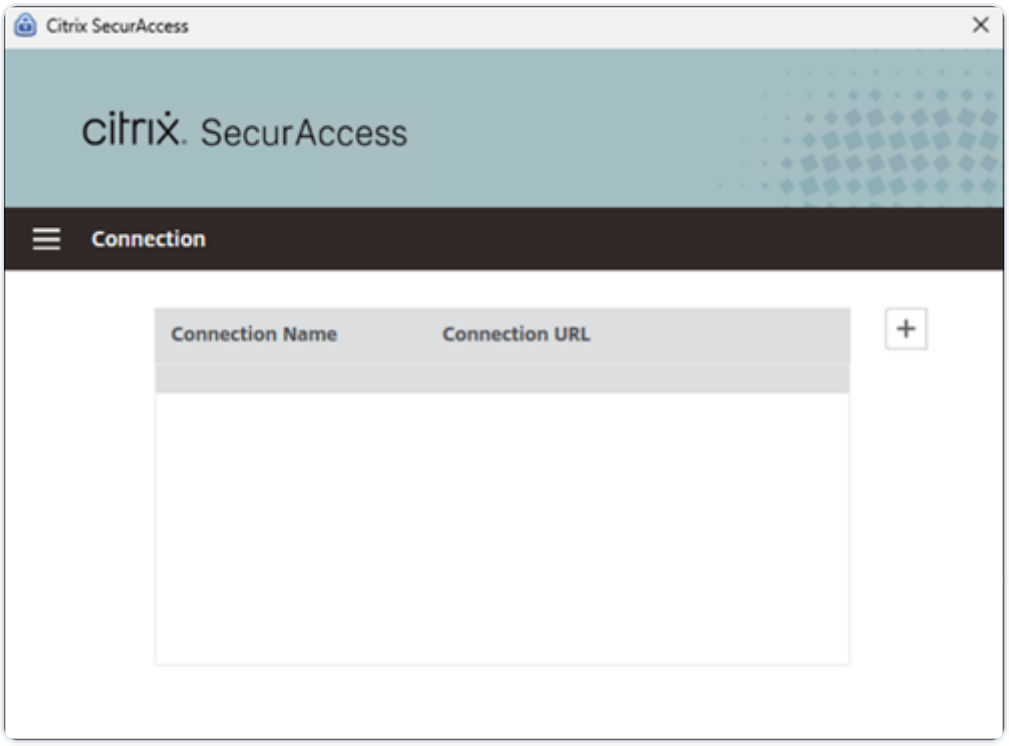
Citrix Secure Access 客户端的 ARM64 支持

从 25.7.1.11 版本开始，Citrix Secure Access 应用程序支持 ARM64 Windows 设备。安装程序会自动检测系统架构并安装相应的 ARM64 版本。这允许 ARM64 Windows 设备上的用户访问 NetScaler Gateway 和 Citrix SecurAccess ZTNA。以前，Citrix Secure Access 客户端与 ARM64 Windows 设备不兼容。

如何连接到 Citrix Secure Access 客户端

最终用户必须执行以下步骤才能在其计算机上启动 Citrix Secure Access 客户端：

1. 在客户端设备上启动 Citrix Secure Access 客户端。
2. 在 Citrix Secure Access 客户端的 **URL** 字段中输入客户管理员提供的 Workspace URL，然后单击**连接**。这是一次性活动，URL 会保存以供后续使用。



3. 系统会根据 Citrix Cloud 中配置的身份验证方法提示用户进行身份验证。

成功通过身份验证后，用户可以访问配置的私有应用程序。

> **注意：**
>
> 如果管理员已配置 SSO，则最终用户无需连接到 Citrix Secure Access，因为他们会自动登录。

安装适用于 macOS 的 Citrix Secure Access 客户端

- 有关安装适用于 macOS 的 Citrix Secure Access 客户端的详细信息，请参阅安装适用于 macOS 的 Citrix Secure Access 客户端。
- 有关如何使用适用于 macOS 的 Citrix Secure Access 的详细信息，请参阅如何从 macOS 设备使用 Citrix Secure Access 应用程序。

> **注意：**
>
> - 适用于 macOS 的 Citrix Secure Access 客户端可用于 macOS 10.15 (Catalina) 及更高版本。

- 预览版本可在 TestFlight 应用程序中获取。
- 如果您在 App Store 应用程序和 TestFlight 预览应用程序之间切换，则必须重新创建要与 Citrix Secure Access 应用程序一起使用的配置文件。例如，如果您一直使用 `blr.abc.company.com` 的连接配置文件，请删除 VPN 配置文件，然后再次创建相同的配置文件。

安装适用于 iOS 的 Citrix Secure Access 客户端

1. 从 App Store 下载适用于 iOS 的 Citrix Secure Access 应用程序。
2. 下载完成后，单击**打开**。

有关如何使用适用于 iOS 的 Citrix Secure Access 的详细信息，请参阅如何从 iOS 设备使用 Citrix Secure Access。

注意：

适用于 iOS 的 Citrix Secure Access 客户端支持使用 NetScaler Gateway 进行客户端证书身份验证。有关详细信息，请参阅在 Citrix Secure Access 应用程序中导入和安装证书。

安装适用于 Linux 的 Citrix Secure Access 客户端

- 有关在 Linux 上安装 Citrix Secure Access 客户端的详细信息，请参阅安装 Citrix Secure Access 客户端。
- 有关如何在 Linux 上使用 Citrix Secure Access 的详细信息，请参阅 适用于 Linux 的 Citrix Secure Access 客户端。

安装适用于 Android 的 Citrix Secure Access 客户端

从 Google Play 商店 下载适用于 Android 的 Citrix Secure Access 应用程序。

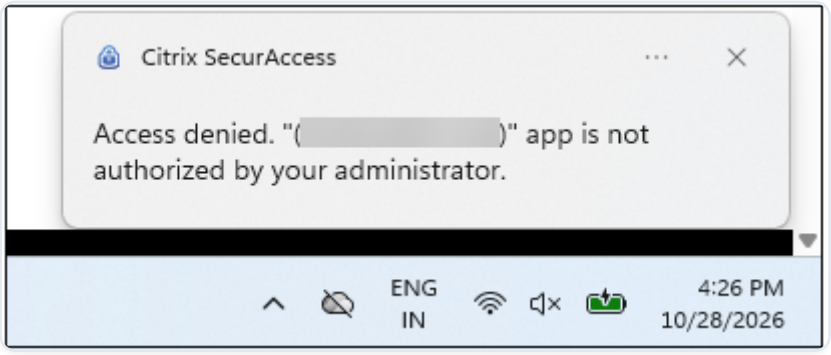
有关如何在 Android 上使用 Citrix Secure Access 的详细信息，请参阅 如何从 Android 设备使用 Citrix Secure Access。

用户通知消息

在以下情况下会显示弹出通知消息：

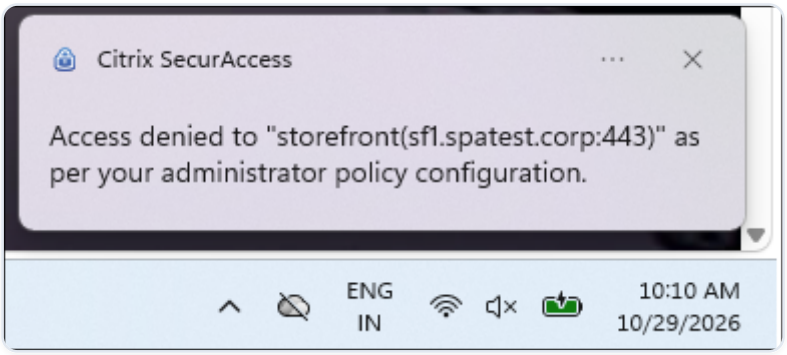
- 管理员未授权用户使用该应用程序。

  原因： 为访问的目标 IP 地址或 FQDN 配置的应用程序未订阅给登录用户。



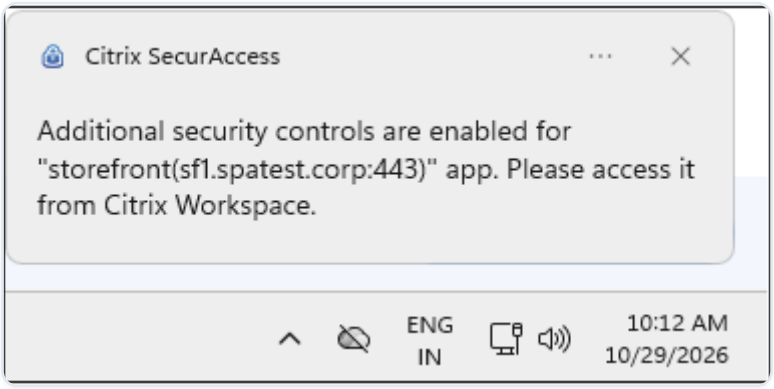
- 访问策略评估结果为拒绝访问。

  原因： 访问目标 IP 地址或 FQDN 被拒绝，因为绑定到应用程序的策略对登录用户评估为“拒绝访问”。



- 已为应用程序启用增强安全控制。

  原因： 已为访问的目标应用程序启用增强安全控制。可以使用 Citrix Workspace™ 应用程序启动该应用程序。



系统要求

Citrix Secure Access 客户端作为桌面应用程序支持以下操作系统和 Web 浏览器。

支持的操作系统	支持的版本	支持的浏览器	支持的部署
Windows 操作系统	Windows 操作系统 10 和 Windows 操作系统 11	Google Chrome 30 或更高版本；Mozilla Firefox 24 或更高版本；Edge Chromium	NetScaler 网关 和 Citrix SecurAccess ZTNA
Windows 服务器	Windows Server 2016、Windows Server 1709、Windows Server 1803 和 Windows Server 2019		
macOS	14.x (Sonoma) 和 15.x (Sequoia)	Safari 7.1-18.1；Google Chrome 30 或更高版本；Mozilla Firefox 30 或更高版本	NetScaler 网关 和 Citrix SecurAccess ZTNA
Ubuntu (乌班图)	22.04 和 24.04	Mozilla Firefox 44 及更高版本；Google Chrome 50 及更高版本	NetScaler Gateway 和 Citrix SecurAccess 零信任网络访问
	eLux® 和 IGEL OS		

注意：

- 目前，适用于 Ubuntu 的 Citrix Secure Access 客户端和 Citrix EPA 客户端仅支持默认的 GNOME 显示管理器。
- 适用于 Linux 的 Citrix Secure Access 客户端 24.11.4 及更高版本支持 eLux OS。

Citrix Secure Access 客户端作为移动应用程序支持以下操作系统。

VPN 应用	支持的版本	支持的部署
iOS	iOS 16、17 和 18	NetScaler Gateway 和 Citrix SecurAccess 零信任网络访问
安卓	安卓 13、14、15、16 和 17	NetScaler 网关

注意：

如果您使用的是最新的 Apple 操作系统版本，例如 macOS 26 (Tahoe)/iOS 26 及更高版本，我们建议您升级到 Citrix Secure Access 客户端版本 25.08.1.1/25.08.1 或更高版本。

Citrix SecurAccess ZTNA 的兼容性矩阵

平台	支持的客户端版本	服务部署	本地部署	混合部署
视窗	24.6.1.17 及更高版本	是	是	是
macOS	24.06.2 及更高版本	是	是	是
iOS	25.08.1 及更高版本	是	否	是
安卓	25.11.1 及更高版本	是	否	是
Linux 系统	24.10.1 及更高版本	是	是	是

支持的功能

重要提示：

- 适用于 iOS/Android 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。
- 旧版 VPN 客户端是使用 Apple 已弃用的私有 VPN API 构建的。macOS/iOS 版 Citrix Secure Access 客户端中的 VPN 支持已使用 Apple 的公共 Network Extension 框架重写。NetScaler Gateway 插件以及适用于 iOS 和 macOS 的 VPN 不再受支持。建议使用适用于 iOS/macOS 的 Citrix Secure Access 作为 VPN 客户端。
- 适用于 Android 设备的 nFactor 身份验证支持的普遍可用性将在即将发布的版本之一中提供。

Citrix Secure Access 客户端支持 NetScaler Gateway 和 Citrix SecurAccess ZTNA 部署。

- NetScaler Gateway 中支持的 Citrix Secure Access 客户端功能
- Citrix SecurAccess ZTNA 中支持的 Citrix Secure Access 客户端功能

NetScaler Gateway 中支持的 Citrix Secure Access 客户端功能

下表列出了 NetScaler Gateway 中每个 VPN 客户端支持的一些常用功能。

功能	适用于 WINDOWS 的思杰安全访问	适用于 MACOS 的 CITRIX SECURE ACCESS	适用于 IOS 的 CITRIX SECURE ACCESS	适用于 LINUX 的思杰安全访问	适用于 ANDROID 的 思杰安全访问
始终开启（用户模式）	是（11.1 及更高版本）	否	否	否	是（通过 MDM）

功能	适用于 WINDOWS 的思杰安全访问	适用于 MACOS 的 CITRIX SECURE ACCESS	适用于 IOS 的 CITRIX SECURE ACCESS	适用于 LINUX 的思杰安全访问	适用于 ANDROID 的 思杰安全访问
PAC 文件	是（12.0 及更高版本）	是	是	否	否
客户端代理支持	是	否	否	否	是。*请参阅注释 1*
内网应用程序的最大限制	512	无限制	无限制	128	无限制
内网 IP (IIP) 地址支持	是	是	是	是	是
拆分隧道开启	是	是	是	是	是
拆分隧道反向	是	是	是	是	是。*请参阅注释 5*
拆分 DNS 远程	是	是	是	是	是。*请参阅注释 6*
拆分 DNS 两者	是	是	是	是。*请参阅注释 8*	是。*请参阅注释 6*
基于 FQDN 的拆分隧道	是 - 仅限开启 (13.0 及更高版本)	是	是	是	是。*请参阅注释 5*
客户端空闲超时	是	是	否	否	否
端点分析	是	是	否	是	否
设备证书（经典）	是	是	否	否	否

功能	适用于 WINDOWS 的思杰安全访问	适用于 MACOS 的 CITRIX SECURE ACCESS	适用于 IOS 的 CITRIX SECURE ACCESS	适用于 LINUX 的思杰安全访问	适用于 ANDROID 的 思杰安全访问
nFactor 身份验证	是 (12.1 及更高版本)	是	是	是	是。*请参阅注释 3*
EPA (nFactor)	是 (12.1 及更高版本)	是	否	是	否
设备证书 (nFactor)	是 (12.1 及更高版本)	是	否	否	否
推送通知	是 (12.1 及更高版本)	否	是	否	是
OTP 令牌自动填充支持。*请参阅注释 2*	否	否	是	否	是
支持 TLS 1.3	是	是。*请参阅注释 7*	是。*请参阅注释 7*	是	是
支持 DTLS。*请参阅注释 5*	是（13.0 及更高版本）	是	是	否	否
HTTPOnly 类型的 Cookie	是	是	是	是	是
全局服务器负载平衡 (GSLB)	是	是	是	是	是
本地 LAN 访问	是	是。*请参阅注释 7*	是。*请参阅注释 7*	否	否

注意：

1. 支持在网关配置中 VPN 虚拟服务器的客户端配置中设置适用于 Android 10 及更高版本的代理。仅支持使用 IP 地址和端口的基本 HTTP 代理配置。
2. 只有通过二维码扫描的令牌才符合自动填充的条件。nFactor 身份验证流程不支持自动填充。
3. 适用于 Android 设备的 nFactor 身份验证支持处于预览阶段，默认情况下禁用此功能。请联系 NetScaler 支持部门以启用此功能。客户必须向支持团队提供其 NetScaler Gateway 的 FQDN，才能为 Android 设备启用 nFactor 身份验证。
4. 有关详细信息，请参阅使用 SSL VPN 虚拟服务器配置 DTLS VPN 虚拟服务器。
5. 适用于 Android 设备的基于 FQDN 的拆分隧道支持和反向拆分隧道处于预览阶段，默认情况下禁用此功能。请联系 NetScaler 支持部门以启用此功能。客户必须向支持团队提供其 NetScaler Gateway 的 FQDN，才能为 Android 设备启用此功能。
6. 对于“拆分 DNS BOTH”模式，必须在网关上配置 DNS 后缀，并且只有以这些后缀结尾的 DNS A 记录查询才会发送到网关。其余查询在本地解析。适用于 Android 的 Citrix Secure Access 还支持“拆分 DNS LOCAL”模式。
7. 在适用于 macOS 和 iOS 的 Citrix Secure Access 客户端中，TLS 1.3 和本地 LAN 访问默认处于禁用状态。如果需要，请联系Citrix 支持。
8. 在适用于 Linux 的 Citrix Secure Access 客户端中，“拆分 DNS BOTH”模式的功能与“拆分 DNS LOCAL”模式相同。

在 Citrix SecurAccess ZTNA 中支持的 Citrix Secure Access 客户端功能

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
始终开启（计算机 + 用	是	否	否	是	否	否	否	否	是。*请参阅注释 1*	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
户隧道）													
始终开启（仅限用户	是	否	否	是	否	否	否	否	是	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
隧道）													
始终在线服务（仅限机	是	否	否	是	否	否	否	否	是。*请参阅注释 1*	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
器隧道）													
客户端空闲超时	是	是	是	是	是	否	否	是	是	是	否	否	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
SSO 到 Citrix Workspace™ 应	否	否	否	是	是	否	否	否	否	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
用程序													
数据报传输层安全 (D	是	是	否	否	否	否	否	否	是	是	是	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
TLS)													
EPAv2 或设备姿态服务	是	是。*请参阅注释 4*	是	是	是。*请参阅注释 4*	否	否	是	是。*请参阅注释 3*	是。*请参阅注释 3* 和 4	否	否	是。*请参阅注释 3*

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
排除域 DNS	是	是	否	是	是	是	否	否	是。*请参阅注释 7*	是。*请参阅注释 7*	是。*请参阅注释 7*	否	否
强制超时	是	是	是	是	是	是	是	是	是	是	是	是	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
全局服务器负载平衡 (GSLB)	是	是	是	否	否	否	否	否	是	是	是	是	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
HttpOnly 会话饼干	是	是	是	否	否	否	否	否	是	是	是	是	是
内网 IP 地	是	是	是	是。*请参*	是。*请参*	是。*请参*	是。*请参*	是。*请参*	是	是	是	是。*请参*	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
址和服务器发起连接 (SIC)				*阅注释 5*	*阅注释 5*	*阅注释 5*	*阅注释 9*	*阅注释 5*				*阅注释 9*	

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
本地 LAN 访问	是	是	否	否	否	否	否	否	是	是	是	否	否
nFactor 认证	是	是	是	是	是	是	是	是	是	是	是	是。*请参阅*	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
												注 11	
设备证书认证	是	是	否	是。*请参阅注释 2*	是。*请参阅注释 2*	否	否	否	是	是	否	否	否
会话	是	是	是	是	是	是	是	是	是	是	是	是	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
超时													
智能欺骗 IP 地址	是	否	否	是	否	否	是	否	是	否	否	是	否
分流隧	否	否	否	否	否	否	否	否	否	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
道关闭													
分流隧道开启（基于主	是	是	是	是	是	是	是	是	是	是	是	是	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
机名）													
拆分隧道开启（基于IP	是	是	是	是	是	是	是	是	是	是	是	是	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
地址）													
反向拆分隧道（基于主	否	否	否	否	否	否	否	否	否	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
机名）													
反向拆分隧道（基于 IP	否	否	否	否	否	否	否	否	否	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
地址）													
支持 UDP 和 TCPD	是	是。*请参阅注释 8*	是	是	是。*请参阅注释 8*	是。*请参阅注释 8*	是。*请参阅注释 10*	是	是	是。*请参阅注释 8*	是。*请参阅注释 8*	是。*请参阅注释 10*	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
NS 的欺骗性 IP 地址													
使用 PR	是	否	否	是	否	否	否	否	是	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
T令牌进行SSO													
使用Windo	是	否	否	是	否	否	否	否	是	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
wsHello 进行 SSO													
TCP 分	是	否	是	是	否	否	否	是	是	否	否	否	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
割DNS支持													
传输层安全性 (T	是	是。*请参阅注*	是	是	是。*请参阅注*	是。*请参阅注*	是	是	是	是。*请参阅注*	是。*请参阅注*	是	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
LS) 1.3		*释 6*			*释 6*	*释 6*				*释 6*	*释 6*		
通过网关设备配置服	否	否	否	否	否	否	否	否	否	否	否	否	否

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
务 (GACS) 升级插件													
可观	是	是	是	是	是	否	否	是	是	是	否	否	是

功能	CITRIX SECURE ACCESS ZTNA - 本地部署 (WINDOWS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (MACOS)	CITRIX SECURE ACCESS ZTNA - 本地部署 (LINUX)	适用于 WINDOWS 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (MACOS)	CITRIX SECURE ACCESS ZTNA 服务 (IOS)	适用于 ANDROID 的 CITRIX SECURE ACCESS ZTNA 服务	CITRIX SECURE ACCESS ZTNA 服务 (LINUX)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (WINDOWS)	CITRIX SECURE ACCESS ZTNA 混合 (MACOS)	CITRIX SECURE ACCESS ZTNA 混合 (IOS)	CITRIX SECURE ACCESS ZTNA 混合模式客户端 (ANDROID)	CITRIX SECURE ACCESS ZTNA 混合 (LINUX)
测性													

注意：

1. Citrix SecurAccess ZTNA 2502 版及更高版本的混合部署支持始终开启（机器和用户隧道）和始终开启服务（仅机器隧道）模式。
2. 在 Citrix SecurAccess ZTNA 服务中，不支持使用第三方颁发的证书进行设备证书身份验证。
3. Citrix SecurAccess ZTNA 2502 版及更高版本的混合部署支持设备状态服务。

4. 适用于 macOS 的设备状态服务需要独立的 EPA 客户端。
5. Citrix SecurAccess ZTNA 服务不支持 UDP。因此，来自服务器的 VoIP、SCCM 和 GPO 推送在 Citrix SecurAccess ZTNA 服务中不起作用。
6. 对于 macOS 和 iOS 平台，TLS 1.3 位于功能标志之后，默认禁用。请联系 Citrix 支持 以启用此功能。
7. Citrix SecurAccess ZTNA 2502 版及更高版本的混合部署支持排除域 DNS 功能。
8. 适用于 macOS/iOS 的 Citrix SecurAccess ZTNA 中 TCP DNS 的欺骗 IP 地址支持位于功能标志之后。请联系 Citrix 支持 以启用此功能。
9. Android 设备中的 TCP/UDP 连接不支持 SIC。
10. 支持 UDP DNS 的欺骗 IP 地址，但不支持 TCP DNS。
11. 如果本地 NetScaler Gateway 也使用网络访问控制 (NAC) 检查用于 Intune 或 CEM，则不支持 nFactor 身份验证。

客户端管理

Citrix Secure Access™ 客户端可以使用诸如 Microsoft Endpoint Configuration Manager、以前称为 System Center Configuration Manager (SCCM) 以及 Citrix Global App Configuration service (GACS) 之类的解决方案进行管理。

通过适用于 Windows 的 Citrix Workspace 应用程序单点登录 Citrix Secure Access

通过适用于 Mac 的 Citrix Workspace 应用程序单点登录 Citrix Secure Access - 预览

通过适用于 Windows 的 Citrix Workspace™ 应用程序单点登录 Citrix Secure Access

Citrix Workspace 应用程序为 Citrix Secure Access 提供统一的客户端管理体验。当用户登录 Citrix Workspace 应用程序时，他们会自动登录 Citrix Secure Access，并且可以无缝访问 TCP/UDP 应用程序，无需手动配置和登录多个客户端应用程序。

工作原理：

Citrix Workspace 应用程序可安装、自动更新并单点登录 (SSO) 到 Citrix Secure Access 客户端。最终用户无需手动干预即可自动登录 Citrix Secure Access，并在 SSO 成功后收到通知。

此功能可节省时间，因为最终用户只需登录一个应用程序，从而提供统一的用户体验。此外，最终用户与 Citrix Secure Access 之间无需交互。

先决条件：

最终用户必须使用 适用于 Windows 的 Citrix Workspace 应用程序 2405 或更高版本。

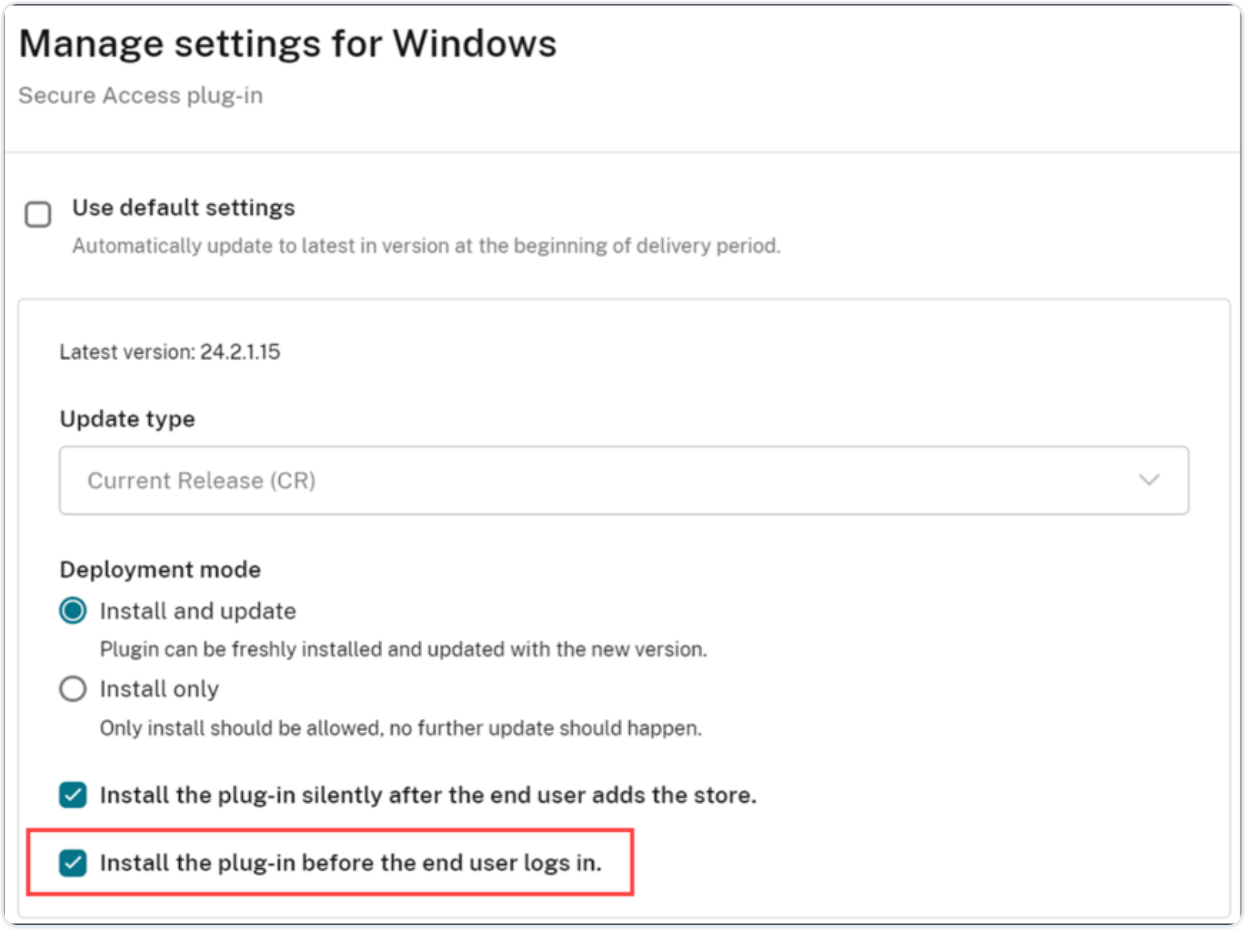
配置：

管理员必须在 Citrix Cloud™ 上配置 Global App Configuration Service (GACS) 设置，以启用 Citrix Workspace 应用程序的安装、自动更新和单点登录 (SSO) 到 Citrix Secure Access 客户端。

通过 Citrix Workspace 应用程序启用 Citrix Secure Access 的安装和自动更新：

1. 登录 Citrix Cloud。

2. 单击汉堡菜单并导航到 **Workspace Configuration（工作区配置）> App Configuration（应用程序配置）**。
3. 选择 **Updates and Plug-ins（更新和插件）** 部分并导航到 **Secure Access Plug-in（安全访问插件）**。
4. 启用 **Windows** 复选框。此步骤将安装适用于 Windows 的 Citrix Secure Access 并自动更新到最新版本。
5. 单击 **Edit（编辑）** 以配置 Windows 插件设置。
6. 在 **Manage settings for Windows（管理 Windows 设置）** 页面上，启用 **Install the plug-in before the end-user logs in（在最终用户登录前安装插件）** 选项。
7. 单击 **Save draft（保存草稿）**。
8. 在出现的确认窗口中，单击 **Yes（是）**。

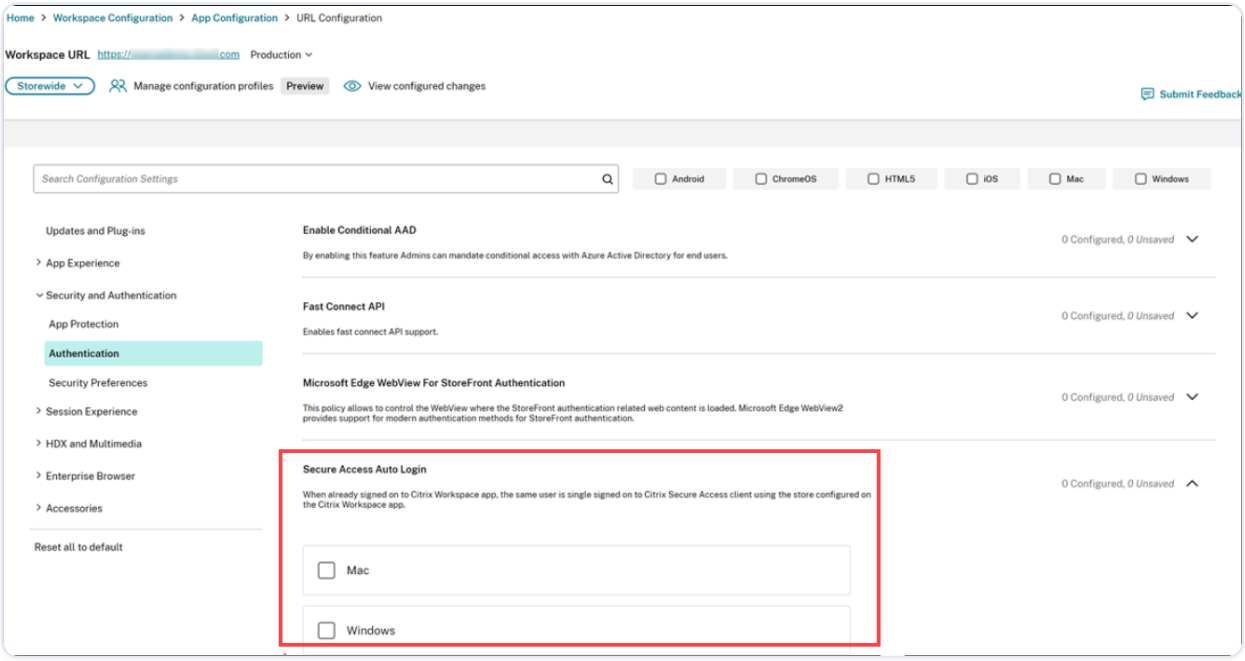


注意：

Citrix Secure Access 客户端的自动更新通过 Beta 渠道进行。要订阅 Beta 渠道，请参阅 Installing Citrix Workspace app Beta program。

通过 Citrix Workspace 应用程序启用 Citrix Secure Access 的 SSO

1. 登录到 Citrix Cloud。
2. 单击汉堡菜单并导航到 **Workspace Configuration（工作区配置）> App Configuration（应用程序配置）**。
3. 导航到 **Security and Authentication（安全和身份验证）> Authentication（身份验证）**。
4. 在 **Secure Access Auto Login（安全访问自动登录）** 部分中，启用 **Windows** 复选框。



有关 GACS 的更多信息，请参阅 (/zh-cn/citrix-workspace-app/citrix-workspace-app.html#configure-citrix-workspace-app-using-global-app-configuration-service)。

限制：

- 从 Citrix Workspace 应用程序到 Citrix Secure Access 的 SSO 登录仅在单个主域上受支持。不支持在多个域上进行 SSO。
- Citrix Workspace 应用程序不记录 Citrix Secure Access 客户端事件（成功登录或失败）。

通过注册表启用 Citrix Workspace 应用程序到 Citrix Secure Access 的 SSO

通过 Citrix Workspace 应用程序启用 Citrix Secure Access SSO 所用的注册表详细信息如下：

- Citrix Workspace 应用程序版本 - **Citrix Workspace 22.10.5.14(2210.5) 或更高版本**
- Citrix Secure Access 版本 - **22.10.1.9 或更高版本**
- Citrix 安全访问 Windows 注册表 - **EnableCWASSO**

SSO 功能默认处于禁用状态。要启用此功能，请在最终用户计算机上添加以下注册表。

- 注册表名称 - EnableCWASSO
- 注册表路径 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- 注册表类型 - REG_DWORD
- 注册表值 - 1

> **重要：**
>
> 有时，最终用户设备可能需要重新启动，才能成功与 Citrix Workspace 应用程序建立单点登录。

通过适用于 Mac 的 Citrix Workspace 应用程序单点登录到 Citrix Secure Access - 预览

从适用于 macOS 的 Citrix Secure Access 24.03.1 开始，登录到 Citrix Workspace 应用程序可以将最终用户单点登录 (SSO) 到 Citrix Secure Access 客户端，建立用户隧道，并无缝提供对 TCP/UDP 应用程序的访问。如果最终用户已连接到 Citrix Workspace 应用程序，适用于 macOS 的 Citrix Secure Access 将自动启动，最终用户可以使用单点登录无缝登录。

当最终用户从 Citrix Workspace 应用程序注销时，Citrix Secure Access 会自动注销，无需用户干预。此功能可节省时间，因为最终用户只需登录一个应用程序，从而提供统一的体验。

先决条件：

1. 最终用户必须使用 适用于 Mac 的 Citrix Workspace 应用程序](https://docs.citrix.com/zh-cn/citrix-workspace-app-for-mac) 或更高版本。有关适用于 Mac 的 Citrix Workspace 应用程序安装的详细信息，请参阅 适用于 Mac 的 Citrix Workspace 应用程序。
2. 最终用户必须使用 适用于 macOS 的 Citrix Secure Access 24.03.1)) 或更高版本。
3. 要通过 MDM 启用此功能，管理员必须使用以下设置：
    - `<key>EnableSecureAccessAutoLogin</key><true/>`

注意事项：

- 如果最终用户在此功能启用之前已登录 Citrix Workspace 应用程序，他们必须重新登录，以便 Citrix Workspace 应用程序可以触发 SSO 到 Citrix Secure Access 客户端。

- 当 Citrix Workspace 应用程序因超时或手动用户注销等原因而注销时，Citrix Secure Access 也会注销，并且用户会话断开连接（仅当 Citrix Secure Access 是通过 Citrix Workspace 应用程序自动启动时）。
- 从 Citrix Workspace 应用程序到 Citrix Secure Access 的 SSO 登录仅在单个主域上受支持。不支持跨多个域的 SSO。
- 如果您在单点登录到 Citrix Secure Access 后将 Citrix Workspace 应用程序连接切换到不同的 URL，系统会提示您选择 Citrix Workspace 应用程序连接 URL。

使用客户端应用管理进行客户端版本控制

您可以使用客户端应用管理，自动更新和管理 SecurAccess ZTNA 服务的最终用户所使用的 Citrix Secure Access 客户端版本。有关详细信息，请参阅 Citrix Secure Access - 客户端应用管理。

支持的客户端

下表列出了支持客户端应用管理的平台和相应的版本：

平台	版本
Windows 操作系统	25.11.1.12

功能管理

Citrix Secure Access 客户端提供对预览功能的访问，并允许通过 Citrix 管理的功能标志动态管理生产中的功能。要请求预览功能，客户必须联系 Citrix 支持。Citrix 团队将从后端为客户的网关 URL 启用和管理该功能。

适用于 Windows 的 Citrix Secure Access 客户端的功能管理

为确保适用于 Windows 的 Citrix Secure Access 客户端中预览功能（功能标志下的功能）的最佳性能，您必须启用流向 `features.netscalergateway.net` 的流量，并将客户端升级到版本 24.8.1.19 或更高版本。

如果无法立即升级，请使用预览功能的注册表设置，直到最终用户更新其客户端版本。有关注册表的详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

> **注意：**
>
> 除非防火墙或代理正在阻止出站流量，否则无需配置即可为功能管理启用流量。在这种情况下，您必须根据策略要求允许流量流向特定的 URL 或 IP 地址。

Citrix Secure Access™ 适用于 视窗

重要提示：

从适用于 Windows 的 Citrix Secure Access 客户端 25.2.1.18 版本开始，您可以确保与从 `C:\Windows` 或 `C:\Program Files` 以外的目录执行 DLL 注入的第三方软件兼容。将第三方软件配置为排除 nsload.exe 进程。或者，使用注入 DLL 的签名者名称配置 `ExternalTrustedSigners` 注册表。有关详细信息，请参阅由于第三方软件导致的登录失败。

适用于 Windows 的 Citrix Secure Access 客户端使您能够使用 NetScaler® Gateway 和 SecurAccess ZTNA 远程访问公司数据和应用程序。

适用于 Windows 的 Citrix Secure Access 客户端现已独立发布，并与所有 NetScaler 版本兼容。我们建议您使用最新版本的 Citrix Secure Access 客户端，因为它包含最新的修复和增强功能。

注意：

- 我们建议您使用适用于 Windows 的 Citrix Secure Access 客户端 24.6.1.18 或更高版本。
- 适用于 Windows 的 Citrix Secure Access 23.5.1.3 及更高版本解决了 CTX561480 中描述的安全漏洞。我们不支持低于 23.5.1.3 版本的适用于 Windows 的 Citrix Secure Access。

发行说明

重要提示：

从适用于 Windows 的 Citrix Secure Access 客户端版本 25.2.1.18 开始，您可以确保与从 `C:\Windows` 或 `C:\Program Files` 以外的目录执行 DLL 注入的第三方软件兼容。配置第三方软件以排除 nsload.exe 进程。或者，使用注入的 DLL 的签名者名称配置 `ExternalTrustedSigners` 注册表。有关详细信息，请参阅由于第三方软件导致登录失败。

> 适用于 Windows 的 Citrix Secure Access 客户端现已独立发布，并与所有 NetScaler 版本兼容。我们建议您使用最新版本的 Citrix Secure Access 客户端，因为它包含最新的修复和增强功能。

Citrix Secure Access 客户端版本遵循 YY.MM.Release.Build 格式。

发行说明描述了新功能、现有功能的增强以及已修复的问题。

新增功能： 当前版本中提供的新功能和增强功能。

已修复的问题： 当前版本中已修复的问题。

有关支持功能的详细信息，请参阅NetScaler Gateway 产品文档。

> **注意：**
>
> 适用于 Windows 的 Citrix Secure Access 客户端版本 26.6.1.20 或更高版本解决了 CTX696734 中描述的安全漏洞。我们建议您使用适用于 Windows 的 Citrix Secure Access 客户端版本 26.6.1.20。

26.7.1.3 (Aug 14, 2026)

已修复的问题

- Citrix Secure Access 在 Windows 10 Enterprise LTSC 2019 操作系统上安装失败。
- 当 NetScaler Gateway 明确配置为压缩 VPN 隧道内的流量时，Citrix Secure Access 客户端会断开连接。
- 在 Always On 部署中启用位置检测时，用户在连接到公司网络时可能会失去对本地网络的访问权限。
- 当同时配置了手动代理和自动代理时，VPN 注销可能无法恢复原始的自动代理设置。
- 升级到版本 26.6.1.20 后，Citrix Secure Access 客户端无法在 ARM64 设备上连接。

26.6.1.20 (Jul 14, 2026)

新增功能

- **支持多个 Entra 配置文件**

  当 Windows 设备注册到多个 Microsoft Entra 租户（包括主 Entra Join 或 Workplace Join）时，Citrix Secure Access WebView 身份验证会自动选择与配置的 Workspace 身份验证关联的 Entra 帐户，从而实现无缝登录体验。

已修复的问题

- 当 Citrix Secure Access 通过客户端应用程序管理进行管理时，系统重启后它不会自动更新到配置的版本。
- 当配置了大量内部网应用程序并在客户端计算机上应用了 ProxyOverride 时，内部站点的访问可能会失败。
- 在 Windows 11 上，由于代理 URL 解析限制，Citrix Secure Access 无法使用配置的自动代理 URL 建立 VPN 连接。
- 当在最终用户计算机上配置了基于主机名的应用程序，并且该计算机的网络适配器使用 0.0.0.0 子网掩码时，可能会发生 Citrix Secure Access 连接失败。
- 当 NetScaler 上强制要求基于客户端证书的身份验证时，使用硬件智能卡读卡器（CNG 支持的证书）的 Windows 11 用户可能无法通过 Citrix Secure Access 进行身份验证。
- SecurAccess ZTNA 诊断日志可能会被 TCP DNS 连接事件淹没。
- 在机器隧道设置中启用位置检测时，如果用户从内部网切换到互联网，Citrix Secure Access 客户端将无法自动重新连接。
- 当您在 SecurAccess ZTNA 中同时配置内部网 IP 地址和位置检测时，内部网应用程序访问可能会失败。
- 如果只配置了机器隧道且 Citrix Secure Access 在 DNE 模式下运行，则对内部站点的访问可能会失败。
- 当 Always-On VPN 配置文件下的 ClientControl 配置设置为 DENY 时，即使 VPN 隧道已建立，Citrix Secure Access 客户端 UI 仍会显示“注销”按钮，允许用户手动断开连接。

26.4.1.8 (May 06, 2026)

新增功能

- **用于故障排除的集成数据包捕获工具**

  适用于 Windows 的 Citrix Secure Access VPN 客户端现在包含一个集成的网络数据包捕获工具，可帮助排查连接问题。

  在 Citrix Secure Access 用户界面中，您可以：

  - 启动实时数据包捕获
  - 停止实时数据包捕获
  - 查看活动数据包捕获的状态

  捕获的文件会自动保存到 Citrix Secure Access 安装文件夹下的 `logs\captures\` 目录中。自动文件轮换用于帮助限制磁盘使用。

  当为 Citrix 支持收集日志时，数据包捕获文件也会自动包含在诊断日志包中。

  要启用此功能，管理员必须配置以下注册表：

  - **注册表路径：** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`
  - **注册表类型：** `REG_DWORD`
  - **注册表名称：** `EnableNetworkTroubleshooting`
  - **注册表值：** `1` (已启用)

  > **注意：**
  >
  > Citrix Secure Access 安装程序包含数据包捕获实用程序以及所有必需的依赖项，因此无需单独安装。此功能支持增强型 Citrix Secure Access UI。有关详细信息，请参阅 25.11.1.12)。

  > 有关详细信息，请参阅用于故障排除的集成数据包捕获工具。

- **用于访问 TCP 和 UDP 应用程序的自定义工作区域支持**

  自定义工作区域支持允许组织通过品牌化的、组织拥有的域（例如，workspace.company.com）而不是默认的 *.cloud.com 域，为用户提供对 TCP 和 UDP 应用程序的访问。管理员可以将自

定义域配置为通过 Citrix SecurAccess ZTNA 访问的应用程序的身份验证和访问端点。最终用户受益于无缝的品牌体验，而组织则对访问和安全性拥有更大的控制权。

有关详细信息，请参阅配置自定义域。

- **Citrix Secure Access 中的服务器名称指示支持**

  Citrix Secure Access 通过在它发起的每个 TLS 连接中包含 SNI 标头来支持服务器名称指示 (SNI)。这可以在每次 TLS 握手期间实现准确的服务器识别。

  > **注意：**
  >
  > 在网关位于 GSLB 配置后的始终在线严格模式 (AlwaysOn = 2) 部署中，Citrix Secure Access 可能不会始终连接到相同的已解析 IP 地址，因为存在 SNI 驱动的路由行为。这可能导致间歇性身份验证失败。为获得无缝体验，请确保网关的所有 GSLB 解析的 IP 地址都包含在始终在线允许列表中，以便在 IP 地址更改时保持连接一致。有关更多详细信息，请参阅始终在线。

- **支持在 Citrix Secure Access 升级期间遵守 SkipDNE 更改**

  当启用 SkipDNE 标志时，Citrix Secure Access 现在在升级和降级期间都为仅限 WFP 的配置提供全面支持。

  要启用此行为，管理员必须配置以下注册表：

  - **注册表路径 (REG_PATH)：** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`
  - **注册表类型 (REG_TYPE)：** `REG_DWORD`
  - **注册表名称 (REG_NAME)：** `SkipDNE`
  - **注册表值 (REG_VALUE)：** `1` (已启用)

- **设备姿态更改时对应用程序访问的实时控制**

  当设备姿态在活动 VPN 会话期间发生更改时，适用于 Windows 的 Citrix Secure Access 客户端现在会强制执行实时应用程序访问更新。

  当设备姿态服务检测到端点安全姿态发生变化时，Citrix Secure Access 会自动刷新其配置，确定受影响的应用程序，通过倒计时器通知用户，然后优雅地撤销对被拒绝应用程序的访问，或者如果所有应用程序都被拒绝，则断开会话。

要启用连续设备姿态，请遵循以下注册表设置：

- **注册表路径 (REG_PATH)：** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`
- **注册表类型：** `REG_DWORD`
- **注册表名称：** `EnableContinousPosture`
- **注册表值：** `1` (已启用)

> **注意：**
>
> 推荐的 EPA 版本：26.3.1.10

- **使用客户端应用程序管理服务对 SecurAccess ZTNA 混合部署进行客户端版本控制**

  Citrix Secure Access 现在通过全局应用程序配置服务 (GACS) 集成支持 SecurAccess ZTNA 混合部署的版本控制。

  有关详细信息，请参阅 Citrix Secure Access。

- **在 Always On VPN 模式下支持用户注销和网关切换**

  Citrix Secure Access 应用程序中具有客户端控制配置的 Always On VPN 模式现在支持用户注销，同时保持机器隧道处于活动状态，以实现不间断的设备连接。注销用户隧道后，用户可以再次登录以建立新的用户隧道，并且如果需要，可以切换网关（SecurAccess ZTNA 或本地）以连接到不同的端点。

  要启用此功能，管理员必须配置以下注册表项：

  - **注册表路径：** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`
  - **注册表类型：** `DWORD`
  - **注册表名称：** `ClientControl`
  - **注册表值：** `1`

  > **注意：**

> 如果机器隧道和用户隧道连接到不同的网关（例如，机器隧道连接到端点 A，用户隧道连接到端点 B），请确保当 DNS 查询通过机器隧道路由时，可以通过端点 A 访问端点 B。此外，请确保将端点 B 从端点 A 的隧道范围和应用程序访问列表中排除，以防止路由冲突并允许用户隧道成功建立。

已修复的问题

- 在 Wi-Fi 切换期间，例如从 Wi-Fi A 切换到 Wi-Fi B，Citrix Secure Access UI 仍处于“不可访问”状态，尽管对应用程序访问没有影响。此 UI 故障仅适用于增强型 Citrix Secure Access UI。
- 在非 Edge WebView 模式（也称为 IE WebView 模式）下运行的 Citrix Secure Access 在将 NetScaler 升级到版本 13.1.62.x 或 14.1.66.x 后，无法通过网关进行身份验证，并抛出 JavaScript 错误。在 Edge WebView 模式下运行 Citrix Secure Access 时未观察到此问题。
- 在全局服务器负载平衡 (GSLB) 设置中，如果 NetScaler 上启用了 HttpOnly cookie、CSP 标头和 HSTS 功能，则从浏览器建立 Citrix Secure Access 客户端会话可能会失败。
- 当满足以下两个条件时，IPv6 环回流量会被阻止，并且依赖 IPv6 环回的应用程序可能会失败或出现意外行为：
  - 拆分隧道设置为“关闭”
  - Citrix Secure Access 在 WFP 模式下连接，且 IPv6 已禁用（默认行为）
- 当 Citrix Secure Access 配置为在 Windows 筛选平台 (WFP) 模式下运行时，Windows 防火墙入站规则不适用于隧道流量。
- 在 Always-On 机器隧道部署中，Citrix Secure Access 客户端在会话超时或重新身份验证期间出现瞬时网络中断后，可能无法重新建立隧道。这种情况尤其发生在睡眠模式期间或之后，或者连接恢复时。
- 当 NetScaler 上配置了内网 IP 地址且 Citrix 虚拟适配器被禁用或未安装时，VPN 流量会被丢弃。
- 在 Windows 筛选平台 (WFP) 模式下，Citrix Secure Access 会阻止第三方签名 DLL 注入到 Citrix Secure Access 应用程序中，即使签名者已列在 ExternalTrustedSigner 注册表中。要解决此问题，请参阅 Windows 版 Citrix Secure Access 客户端故障排除。

- Citrix Secure Access 清理实用程序可能无法删除 Citrix 虚拟网络适配器，从而在端点上留下残留适配器。这个残留适配器可能会阻止新版 Citrix Secure Access 的自动安装，需要对受影响的设备进行手动干预。此问题已在清理实用程序版本 25.11.1.1 中修复。
- 如果 VPN 会话持续数天，可能会出现隧道中断，具体取决于网络流量的容量和类型。
- 在工作组计算机上，Citrix 虚拟适配器上的防火墙配置文件可能被错误地归类为公共配置文件，而非预期的域配置文件。
- 如果本地网络子网与内网应用程序子网重叠且未配置内网 IP 地址 (IIP)，则通过 Citrix Secure Access 访问应用程序可能会失败。
- 安装 Citrix Secure Access 会启用 TLS 1.1，即使系统之前已禁用它。
- 当欺骗性 IP 范围与内网 IP 范围重叠时，DNS 解析可能会间歇性失败。
- 通过 NetScaler 将 Citrix Secure Access 从版本 25.11.1.12 升级到更高版本时，会提示管理员批准，导致非管理员用户升级失败。

26.3.1.5 (Mar 26, 2026)

已修复的问题

- 当在 Always On 部署中启用隐藏 UI 功能时，用户手动退出 Citrix Secure Access 后，它不会自动重新启动。

  有关隐藏 UI 功能的信息，请参阅 25.11.1.12 发行说明) 中的**增强型 Always On 模式用户体验**。

- 使用 MSI 安装程序安装 Citrix Secure Access 客户端时，可能会出现“文件正在使用”警告，从而中止安装过程。此问题仅在 Citrix Secure Access 上启用增强型 UI (EnableWebModuleUI 注册表) 时才会出现。
- 当使用 Citrix Secure Access 不支持的智能卡支持的密钥存储提供程序进行身份验证时，移除智能卡可能不会触发用户隧道注销。

  通过此修复，添加了一个新的字符串注册表项 (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\smartCardProviders)，允许管理员通过分号分隔的列表配置其他智能卡提供程序。

- 当 Citrix Secure Access 配置为在 Windows 筛选平台 (WFP) 模式下通过机器隧道进行 Always On 部署操作，并且启用了严格模式时，外部（互联网）访问将变为不可用。

26.1.1.9 (Feb 10, 2026)

新增功能

- **混合数据路径的无缝网关更新**

  Citrix Secure Access 应用程序支持在 SecurAccess ZTNA 配置中添加或删除网关，而不会中断活动的客户端会话。有关混合数据路径的更多信息，请参阅 适用于 SecurAccess ZTNA 服务的混合数据路径。

- **Always On VPN 模式的用户隧道回退**

  Citrix Secure Access 客户端现在包含 Always On VPN 模式的回退机制。如果机器隧道无法建立，并且启用了 `UserTunnelFallbackEnabled` 注册表项，Citrix Secure Access 客户端将自动尝试形成用户隧道。 有关更多信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

  要启用此功能，管理员必须配置以下注册表项：

  - **注册表路径：** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - **注册表类型：** REG_DWORD
  - **注册表名称：** UserTunnelFallbackEnabled
  - **注册表值：** 1（已启用）

已修复的问题

- 即使配置了 DisableWebViewForAutoLogon 注册表项，Citrix Secure Access 也会在单点登录流程中向最终用户显示设备状态屏幕。

- 用户通过网关连接时，可能会遇到 Avaya 注册失败或登录延迟的问题。

- 在极少数情况下，当应用程序流量碎片化时，用户可能无法访问 Citrix Secure Access 的内部应用程序。

- 在极少数情况下，当 Citrix Secure Access 应用程序配置为“始终开启”严格模式时，如果浏览器与插件之间的通信失败，用户可能会遇到登录延迟或登录错误。

- 当 Citrix Secure Access 应用程序配置为“始终开启”严格模式且启用了客户端控制时，用户可能无法切换到其他网关 URL。
- 由于欺骗范围和 VPN 适配器网络之间存在内部 IP 映射重叠，可能会间歇性发生 DNS 解析失败。
- Citrix Secure Access 应用程序在 SecurAccess ZTNA 混合部署中频繁登录或注销序列期间可能会间歇性崩溃。

25.11.1.12 (Dec 08, 2025)

新增功能

- **具有通知中心和集成 WebView 的增强型用户界面**

  Citrix Secure Access 客户端现在具有增强型 UI，引入了用于简化警报的**通知中心**和用于直接在其计算机上改进客户端处理的集成 WebView。

  要启用新 UI，管理员必须配置以下注册表项：

  - **注册表路径：** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - **注册表类型：** DWORD
  - **注册表名称：** EnableWebModuleUI
  - **注册表值：** 1

- **Citrix Secure Access 客户端中的强制门户支持**

  Citrix Secure Access 应用程序现在将强制门户登录直接集成到应用程序中。用户无需切换应用程序即可完成强制门户的身份验证。此功能是新 UI 的一部分。要启用新 UI，管理员必须配置 `EnableWebModuleUI` 注册表。有关详细信息，请参阅NetScaler Gateway Windows VPN 客户端注册表项。

- **通过反 DLL 保护增强安全性**

  反 DLL 保护有助于保护 Citrix Secure Access 客户端免受未经授权的动态链接库 (DLL) 或不受信任模块的侵害。如果注入了此类不受信任的模块，Citrix Secure Access 客户端会检测到这些干预并阻止模块加载。此外，如果在 Citrix Secure Access 启动期间检测到任何不受信任或恶意 DLL，它会生成通知并终止应用程序启动。

  要启用反 DLL 注入安全增强功能，管理员必须配置以下注册表项：

- **注册表路径 (REG_PATH)：** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- **注册表类型 (REG_TYPE)：** DWORD
- **注册表名称 (REG_NAME)：** EnableAntiDllProtection
- **注册表值 (REG_VALUE)：** 1

- **Citrix Secure Access 客户端中的无缝登录体验**
  - **隐藏登录/注销脚本执行**

    在 Citrix Secure Access 隧道建立或终止期间执行登录或注销脚本时，命令提示符不再闪烁。

    要启用此行为，管理员必须配置以下注册表项：

    - **注册表路径 (REG_PATH)：** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
    - **注册表类型 (REG_TYPE)：** DWORD
    - **注册表名称 (REG_NAME):** HideLoginLogoutScriptsPrompt
    - **注册表值 (REG_VALUE):** 1
  - **增强的始终开启模式用户体验**

    Citrix Secure Access 客户端在始终开启模式下运行时，现在会完全隐藏设备状态或身份验证屏幕。此功能是新 UI 的一部分，通过 `EnableWebModuleUI` 注册表启用。

    除了 `EnableWebModuleUI` 注册表之外，管理员还必须配置以下注册表项才能启用此行为：

    - **注册表路径 (REG_PATH):** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
    - **注册表类型 (REG_TYPE):** DWORD
    - **注册表名称 (REG_NAME):** DisableWebViewForAutoLogon
    - **注册表值 (REG_VALUE):** 1

- **Citrix SecurAccess ZTNA 仅使用计算机隧道的始终开启模式**

  Citrix Secure Access 客户端现在支持 Citrix SecurAccess ZTNA 部署的“仅计算机隧道”配置。

  要启用仅计算机隧道配置，管理员必须配置以下注册表：

- **注册表路径 (REG_PATH):** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- **注册表类型 (REG_TYPE):** DWORD
- **注册表名称：** AlwaysOnService
- **注册表值：** 1

有关详细信息，请参阅 Windows 登录前的 Always On。

- **使用客户端应用程序管理进行客户端版本控制**

  您现在可以使用客户端应用程序管理，自动更新和管理 SecurAccess ZTNA 服务的最终用户的 Citrix Secure Access 客户端版本。

  先决条件：

  - 管理员必须在 Citrix Secure Access 客户端中创建以下注册表项：
    - **注册表路径：** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
    - **注册表类型：** DWORD
    - **注册表名称：** EnableAdminConfigFetch
    - **注册表值：** 1
  - 确保为 Citrix Secure Access 启用了与以下端点的连接：
    - `<https://gacs-discovery.cloud.com>`
    - `<https://gacs-config.cloud.com>`
    - `<https://downloadplugins.citrix.com>`
  - 验证您是否拥有 Citrix Cloud 帐户。如果没有，您可以从 `<https://onboarding.cloud.com/>` 创建一个帐户。有关详细信息，请参阅 注册 Citrix Cloud。

  配置客户端应用程序管理以进行 Citrix Secure Access 客户端的版本控制：

  a. 登录 Citrix Cloud 门户并导航到 **客户端应用程序管理 > Citrix Secure Access**。
  b. 从已配置的商店 URL 列表中，选择要配置设置的商店。
  c. 导航到 **所有设置 > Citrix Secure Access 版本**。
  d. 在 **Citrix Secure Access 版本** 屏幕中，从所需平台旁边的下拉菜单中选择 **已启用**。
  e. 在 **管理 Windows 设置** 屏幕中，启用以下选项：

- **更新通道：**
  - **发布：** 选择此选项以控制生产版本的客户端版本。
  - **Beta：** 选择此选项以控制预览版本的客户端版本。
- **选择更新方式：**
  - **更新到最新版本：** 选择此选项可将所有最终用户的客户端版本更新到最新版本。如果您启用 **Beta** 通道，则只有最新版本可用。
  - **更新到特定版本：** 选择此选项可将所有最终用户的客户端版本更新到特定版本。启用后，从 **版本** 下拉列表中选择所需的客户端版本，该列表显示三个最新的客户端版本。

f. 单击 **保存草稿 > 是 > 保存** 以保存您的设置。

g. 点击 **查看未保存的设置** 以查看未保存的设置。

h. 查看更改并点击 **发布草稿 > 发布** 以发布您的设置。

> **注意：**
>
> 设置会立即更新到 Citrix Secure Access 客户端。

> **相关主题：**

- Citrix Secure Access - 客户端应用管理
- NetScaler Gateway Windows VPN 客户端注册表项
- 客户端管理

已修复的问题

- 如果用户名或密码包含 UTF-8 编码字符，则使用 Edge WebView 自动登录 Citrix Secure Access 客户端会失败。
- 当 Citrix Secure Access 客户端在“始终开启”严格模式下运行时，用户连接到 NetScaler Gateway 可能会遇到延迟。
- 由于日志和错误报告未优化，管理员在排查 Web 代理自动发现 (WPAD) 问题时面临挑战。

- 当 Citrix Secure Access 客户端启用了分流隧道，并且基于文件的代理 PAC 被配置为通过 VPN 隧道的系统代理时，互联网访问失败。默认情况下，此功能处于禁用状态。

  要启用此功能，管理员必须配置以下 Windows 注册表：

  - **注册表路径：** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - **注册表类型：** REG_DWORD
  - **注册表值：** 1
  - **注册表名称：** DisableWpadProxyPacUsage

- 极少数情况下，当会话超时与计算机从睡眠状态恢复同时发生时，处于“始终开启”模式的 Citrix Secure Access 客户端无法重新建立 VPN 连接。

- 启用机器隧道后，登录屏幕可能会短暂显示不正确的“已连接”消息，而此时隧道仍在建立中。

- 当启用了具有上下文访问权限的机器隧道时，Active Directory 用户可能无法登录 Citrix Secure Access 客户端。

- Citrix Secure Access 客户端从 25.2.1.x 或更早版本升级到 25.7.1.x 或更高版本时，在 Windows 10 版本 1709 之前的较旧 Windows 操作系统上会失败。

- 当启用“始终开启”服务模式时，Citrix Secure Access 图标间歇性地无法显示在 Windows 凭据屏幕上。

- Citrix Secure Access 客户端会阻止对本地 DNS 服务器的 Ping 操作。

- 在极少数情况下，Citrix Secure Access 客户端可能会因 DNS 处理不当而崩溃。

25.9.1.5 (Sep 30, 2025)

> **重要更新：**
>
> - Citrix Secure Access 25.9.1.5 版取代了 25.9.1.4 版，现已正式发布。

已修复的问题

- 如果使用非标准 DNS 端口（53 以外），则与 DNS 服务器和网关 IP 地址的连接可能会失败。

- 在 Citrix SecurAccess ZTNA 混合部署中，Citrix Monitor 会使用默认值覆盖管理员配置的更新频率。
- 在 Citrix SecurAccess ZTNA 混合部署中，Citrix Monitor 显示不正确的即时跳数详细信息。
- 即使在 VPN 虚拟服务器上启用了**智能卡移除时注销**设置，Citrix Secure Access 客户端在智能卡移除时也不会注销。
- 在 Citrix SecurAccess ZTNA 部署中捕获诊断日志时，Citrix Secure Access 客户端可能会崩溃。
- 如果使用非标准端口（443 以外的端口），连接到 NetScaler Gateway 虚拟服务器可能会失败。当 Citrix Secure Access 客户端在 Microsoft Edge WebView 模式下运行时，会出现此问题。
- 升级到版本 25.5.1.15 后，Citrix Secure Access 客户端无法启动。此问题是由于依赖的第三方库初始化失败导致的。
- 在 SecurAccess ZTNA 模式下运行时，Citrix Secure Access 客户端在登录期间会间歇性崩溃。
- 将 Citrix Secure Access 客户端升级到版本 25.5.1.15 或更高版本后，系统会反复提示用户输入域凭据。当 Windows 域加入因 DNS 解析错误而失败时，会出现此问题。
- 在 WFP 模式下连接时，Citrix Secure Access 客户端在隧道传输 TCP DNS 流量时会间歇性崩溃。
- Citrix Secure Access 客户端因区分大小写的路径验证而无法启动。

25.7.1.11 (Aug 13, 2025)

新增功能

- **Citrix Secure Access 客户端支持 ARM64**

  Citrix Secure Access 应用程序现在支持 ARM64 Windows 设备。安装程序会自动检测系统架构并安装相应的 ARM64 版本。这使得 ARM64 Windows 设备上的用户能够访问 NetScaler Gateway 和 Citrix SecurAccess ZTNA。

- **Citrix SecurAccess ZTNA 中应用程序的增强型 DNS 后缀处理**

增强型 DNS 后缀处理现在可确保只有与配置的后缀匹配的应用程序域才能通过 Citrix SecurAccess ZTNA 安全地进行隧道传输，从而允许其他域直接访问互联网。

已修复的问题

- 当设备上启用基于 Windows Hello 的身份验证时，用户可能会在 Citrix Secure Access 客户端中遇到间歇性自动登录失败。用户必须手动启动 Citrix Secure Access 客户端才能建立与 NetScaler Gateway 的连接。

- 当最终用户设备上激活 IPv6 DNS 服务器时，Citrix Secure Access 客户端会间歇性地无法启动登录脚本。

- Citrix Secure Access 客户端用户在访问内部网应用程序时可能会遇到长达 30 秒的连接延迟。此问题在一段时间不活动或休眠后发生。

- Citrix Secure Access 客户端在 Windows 11 24H2 版本计算机上以“始终开启”或“始终开启服务”模式运行时，可能无法自动登录。

  要解决此问题，管理员必须创建以下注册表项：

  - **注册表路径：** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - **REG_TYPE:** DWORD
  - **REG_NAME:** EnableCsaAutoLaunch
  - **REG_VALUE:** 1

- 当设备从待机状态恢复时，Citrix Secure Access 客户端可能无法建立 VPN 连接。当 Hyper-V 虚拟交换机用作最终用户设备上的主要外部接口时，会发生此问题。

- 当 Citrix Secure Access 客户端在 WFP 模式下运行时，EPA 定期扫描失败。

- 即使 VPN 连接处于活动状态，用户也可能由于 DNS 解析失败而无法访问内部网应用程序。发生此故障是因为 Citrix Secure Access 客户端强制执行 `nsapimgr -ys enable_vpn_dnstruncate_fix=1` 设置，即使在 NetScaler Gateway 上禁用该设置也是如此。

- 在 WFP 模式下连接时，通过隧道进行的 TCP 连接下载吞吐量低于 DNE 模式。

- 即使最终用户计算机已连接到公司网络，**状态**菜单仍错误地显示 VPN 已连接。当 Citrix Secure Access 客户端在启用位置检测的 Always On 服务模式下运行时，会出现此问题。

- 当使用脚本 PAC 文件配置代理服务器时，Citrix Secure Access 客户端无法在 Windows 11 计算机上登录。
- Citrix Secure Access 客户端用户遇到间歇性登录失败。当启用 Always On 严格模式时，此问题会在 GSLB 部署中发生。
- 当启用 Microsoft Edge WebView 且 NetScaler Gateway 上配置了除“singleauth.xml”之外的登录方案时，Citrix Secure Access 客户端中的自动登录可能会失败。
- Citrix Secure Access 客户端版本 24.11.1.17 及更高版本中，经典身份验证的自动登录失败，因为默认的 Microsoft Edge WebView 不支持经典身份验证。

  通过此修复，Citrix Secure Access 客户端允许将默认 WebView 恢复为支持经典身份验证的 Internet Explorer WebView。有关详细信息，请参阅Citrix Secure Access 客户端版本 24.11.1.17 及更高版本中的自动登录失败。
- Citrix Secure Access 客户端用户可能会因 DNS 解析错误而导致内网应用程序访问失败。当满足以下两个条件时，会出现此问题：
  - Citrix Secure Access 客户端中启用了本地 LAN 访问。
  - DNS 服务器的 IP 地址在 LAN 子网内。
- 当隧道处于活动状态时，Citrix Secure Access 客户端会间歇性崩溃。

25.5.1.15 (Jun 17, 2025)

已修复的问题

- 如果 DNS 服务器也用于其他功能，例如动态主机配置协议 (DHCP) 或流量监控，用户在访问应用程序时可能会遇到中断。
- Citrix Secure Access 客户端与 NetScaler Gateway 之间的 TLS 握手可能会失败，导致 VPN 断开连接。当 NetScaler Gateway 上的客户端证书配置设置为 **可选** 且客户端计算机没有用户证书时，会出现此问题。
- 尽管在 Citrix Secure Access 客户端的“**配置**”菜单中禁用了“**自动打开主页**”复选框，Citrix Secure Access 客户端仍会在 Windows Hello 登录时自动启动。
- 用户无法访问内部网和互联网资源，只有与虚拟服务器或 NetScaler Gateway 的连接保持不变。当满足以下两个条件时，会出现此问题：

  - 用户的设备已连接到内部网。
  - Citrix Secure Access 客户端在启用 WFP 模式的 Always On 严格模式下运行。

- 在分配的 IIP 地址的动态 DNS (DDNS) 注册期间，Citrix Secure Access 客户端会间歇性崩溃。
- 当启用反向拆分隧道时，Citrix Secure Access 客户端中会发生间歇性 DNS 故障。有关更多信息，请参阅未配置域的反向拆分隧道。

25.4.1.9 (May 08, 2025)

新增功能

- **支持多工作区 URL**

  Citrix Secure Access 客户端现在支持 SecurAccess ZTNA 服务部署的多工作区 URL 功能。

已修复的问题

- 如果 LDAP 身份验证的用户名或密码包含特殊字符，则自动登录 Citrix Secure Access 客户端可能会失败。
- 当使用默认登录架构配置高级身份验证，并且登录按钮 ID 设置为“Logon”时，使用 Edge WebView 自动登录 Citrix Secure Access 客户端会失败。
- 当最终用户的设备在“始终开启”严格模式下运行时（即“始终开启”设置为 2），Citrix Secure Access 客户端的自动登录可能会失败。

  在 `AlwaysOnAllowlist` 中包含环回地址 `127.0.0.1; loopback` 以在“始终开启”严格模式下启用自动登录。
- 当 EPA 客户端以独立模式安装和运行时，设备证书扫描可能会失败。
- 启用设备状态服务后，用户每次使用 Citrix Secure Access 客户端连接到 Citrix Workspace™ URL 时，都可能会被提示运行 EPA 客户端。
- 在配置 EnableAutoUpdate 注册表以启用自动更新功能后，Citrix Secure Access 客户端的自动更新可能无法在不重启系统的情况下运行。

25.2.1.18 (Apr 09, 2025)

新增功能

- **支持基于 Windows Hello 登录的单点登录**

  当最终用户的设备上启用了基于 Windows Hello 的登录时，Citrix Secure Access 客户端现在在“始终开启”模式下支持单点登录，无论是在 Citrix SecurAccess ZTNA 部署还是 NetScaler Gateway 部署中。

- **支持在 SecurAccess ZTNA 中通过 UDP 进行基于主机名的应用程序访问**

  Citrix Secure Access 客户端现在支持在 SecurAccess ZTNA 模式下运行时，通过机器级隧道通过 UDP 进行基于主机名的应用程序访问。

- **支持在启用 DTLS 的情况下进行基于主机名的应用程序访问**

  Citrix Secure Access 客户端现在支持对基于 TCP 和 UDP 的 DNS 请求进行 IP 地址欺骗，从而在 NetScaler Gateway 中配置 DTLS 时启用基于主机名的应用程序访问。

- **EPA 客户端中增强的插件升级行为**

  当在最终用户设备上检测到更高版本的 EPA 客户端时，EPA 客户端现在会阻止降级到较低版本的提示。此功能适用于 NetScaler Gateway 中 **Windows EPA 插件升级** 配置（**始终**、**基本** 或 **从不**）的任何情况。此增强功能可确保最终用户设备始终运行最新版本的 EPA 客户端，从而维护安全性和稳定性。

已修复的问题

- 在本地部署中，当启用双因素身份验证时，Citrix Secure Access 客户端可能无法建立 VPN 连接。

- 在本地部署中，基于主机名的访问的 DNS 解析可能会在响应发送到 NetScaler Gateway 进行解析的 DNS 查询时返回单个 IP 地址。即使 DNS 可以解析为多个 IP 地址，也会出现此问题。

- 当 Citrix Secure Access 客户端上启用机器级隧道时，如果使用非标准端口（443 以外的端口），则与 NetScaler Gateway 虚拟服务器的连接可能会失败。

- 当 Citrix Secure Access 客户端尝试连接到内部网 IP 地址时，DNS 解析可能会失败。如果未在 NetScaler Gateway 虚拟适配器上配置 DNS 服务器，则会出现此问题。

- 当有多个会话可供传输时，处于计算机隧道模式的 Citrix Secure Access 客户端可能无法将登录传输到另一个会话。
- 当启用本地安全机构时，自动登录 Citrix Secure Access 客户端可能会失败。
- 启用 Always On 严格模式时，用户隧道建立会延迟。
- 如果最终用户计算机上的默认语言设置包含非英文字符（例如 å 或 ø），则 EPA 客户端的 nglauncher 可能会崩溃，并且设备状态检查可能会失败。
- 如果达到隧道连接限制，即使实际连接数较低，最终用户在使用数小时后也可能无法访问内部网应用程序。

25.1.1.27 (Mar 21, 2025)

> **重要更新：**
>
> - Citrix Secure Access 25.1.1.27 版取代了 25.1.1.11 版，现已正式发布。
> - 从 Citrix Secure Access 25.1.1.27 版开始，Windows 筛选平台 (WFP) 默认启用。

已修复的问题

- 当设备从待机状态恢复时，通过 Citrix Secure Access 客户端进行的互联网和内网访问在“始终开启”模式下（使用机器级隧道时）可能会失败。
- 在 SecurAccess ZTNA 模式下，当多个主机名解析到同一个 IP 地址时，Citrix Secure Access 客户端可能无法建立与 UDP 应用程序的连接。
- 当会话因不活动而终止后，Citrix Secure Access 客户端不会自动重新建立 VPN 连接。当在“始终开启”模式下的 Citrix SecurAccess ZTNA 中配置了 **Server Idle Session Timeout** 时，会出现此问题。
- 当 EPA 客户端以独立模式安装和运行时，设备证书扫描可能会失败。
- 如果配置了基于客户端证书的身份验证，Citrix Secure Access 客户端中的“**Windows 登录前始终开启 VPN**”配置可能无法建立 VPN 连接。

- 即使已安装正确版本的 Citrix EPA，最终用户也会被提示下载插件。此问题在以下情况下发生：
  - HttpOnly cookie 已启用。
  - **windowsEPAPluginUpgrade** 参数设置为 **Always**。

24.11.1.17 (Dec 19, 2024)

> **重要更新：**

> 从 Citrix Secure Access 版本 24.11.1.17 开始，Microsoft Edge WebView 默认启用。要禁用 Microsoft Edge WebView，请联系 Citrix 支持。有关详细信息，请参阅 Windows Citrix Secure Access 的 Microsoft Edge WebView 支持。

新增功能

- **支持 SecurAccess ZTNA 中的上下文访问功能**

  Citrix Secure Access 客户端支持上下文访问功能，该功能使管理员能够根据网络位置、地理位置和设备状态等用户上下文动态实施 ZTNA 策略。管理员可以使用 `EnableContextualAccess` 注册表或联系 Citrix 支持 启用此功能。有关详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

- **Citrix Secure Access 客户端安装程序包含在 VDA 元安装程序中**

  Citrix Secure Access 客户端安装程序现已集成到 Citrix Virtual Apps and Desktops 7 2411 中的 VDA 元安装程序中。此增强功能允许管理员将 Citrix Secure Access 客户端 for Windows 作为 VDA 安装过程的一部分进行安装。有关详细信息，请参阅 安装 VDA 文档。

- **增强的 Windows 上次更新扫描以支持按类别扫描**

  Windows 上次更新扫描输出包括按类别列出的**安全更新**、**关键更新**、**定义更新**和**更新汇总**。以前，Windows 上次更新扫描仅包含通用更新。有关详细信息，请参阅 Windows 上次更新扫描。

- **增强了多会话 VDA 的故障排除功能**

  Citrix Secure Access 客户端现在支持在多会话 VDA 环境中为每个用户发送通知。对于管理员，多会话 VDA 的事件可在 DaaS Monitor 中查看。

- **支持基于 Windows Hello 登录的自动登录**

当最终用户的设备上启用基于 Windows Hello 的登录时，Citrix Secure Access 客户端现在支持自动启动和登录。

- **Citrix Secure Access 客户端的自动更新支持**

  Citrix Secure Access 客户端现在可以自动将 Windows 客户端更新到最新的可用版本。此功能默认不启用。管理员可以启用此功能，并使用注册表 `EnableAutoUpdate` 和 `IsAutoUpdateControlledViaAdmin` 选择哪些计算机必须自动获取早期访问版本或生产版本的更新。有关详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

  > **注意：**
  >
  > 由于自动更新功能是在 Citrix Secure Access 客户端 Windows 版本 24.11.1.17 中引入的，管理员可以在后续版本中使用此功能。

已修复的问题

- 登录 Citrix Secure Access 客户端 for Windows 时，Microsoft Edge WebView 可能无法加载。即使已安装，也可能会出现错误消息“您的计算机未安装 Microsoft Edge 运行时”。

- Windows 11 计算机上的 Citrix Secure Access 客户端无法与 NetScaler Gateway 建立 DTLS 连接。

24.10.1.5 (Nov 08, 2024)

已修复的问题

- 在 SecurAccess ZTNA 模式下，当设备从待机状态恢复时，基于主机名的应用程序访问可能会失败。

- 当设备从待机状态恢复时，适用于 Windows 的 Citrix Secure Access 客户端有时可能需要 60 多秒才能激活并连接。

- 当启用服务器名称指示 (SNI) 时，适用于 Windows 的 Citrix Secure Access 客户端无法与 NetScaler Gateway 建立 VPN 连接。

- 当 NetScaler Gateway 上启用会话票证参数时，由于 SSL 重新协商失败，用户无法建立 VPN 连接。

- 如果在上次注销过程中发生网络故障，用户无法建立 VPN 连接。
- Citrix Secure Access 客户端的 `nsRmSac.exe` 清理实用程序需要在最终用户设备上进行手动干预才能运行。有关详细信息，请参阅 完全跳过 DNE 安装。
- 注销 VPN 后，如果计算机上的某个网络适配器使用环回地址作为 DNS 服务器，则 localhost 通信可能会失败。因此，当用户尝试通过浏览器重新登录 VPN 时，即使已安装 EPA 插件，也可能会提示他们再次下载 EPA 插件（如果 EPA 配置为身份验证因素）。
- 当用户使用适用于 Windows 的 Citrix Secure Access 客户端登录到 NetScaler® Gateway 虚拟服务器时，自定义重定向可能会失败。

24.8.1.19 (Oct 10, 2024)

> **重要更新：**
>
> Citrix Secure Access 24.8.1.19 版取代了 24.8.1.15 版，现已正式发布。

新增功能

- **SecurAccess ZTNA 支持云托管多会话 VDI**

  Citrix Secure Access 客户端现在支持使用 SecurAccess ZTNA，以实现从云托管多会话 VDI 对企业资源的零信任访问。管理员可以使用 `EnableMultiSessionFlow` 注册表启用此功能。对于已加入域的计算机，请同时使用 `EnableMultiSessionFlow` 和 `AlwaysOnService` 注册表。有关详细信息，请参阅NetScaler Gateway Windows VPN 客户端注册表项。

- **针对活动的 SecurAccess ZTNA 应用程序的持续设备态势评估**

  在设备态势服务中启用**定期扫描**设置后，EPA 客户端会每 30 分钟扫描一次设备。如果检测到态势状态降级，它会通知用户并通过 Citrix Secure Access 客户端断开活动的 SecurAccess ZTNA 连接。有关详细信息，请参阅设备的定期扫描。

- **支持 Citrix Secure Access 排除 DNS 流量**

  您现在可以排除 DNS 流量不被 Citrix Secure Access 客户端拦截。有关详细信息，请参阅从客户端拦截中排除特定域流量。

- **SecurAccess ZTNA 的 Always On 位置检测支持**

适用于 Windows 的 Citrix Secure Access 支持 SecurAccess ZTNA 服务的位置检测功能。如果用户计算机不在公司网络中，它会将其连接到 VPN 会话；如果计算机在公司网络中，它会断开用户的 VPN 会话。您必须使用 locationDetection 注册表并在 SecurAccess ZTNA 管理 UI 控制台上配置 DNS 后缀才能启用位置检测功能。

有关使用注册表的更多信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

有关配置 DNS 后缀的更多信息，请参阅 用于将 FQDN 解析为 IP 地址的 DNS 后缀。

- **对 Azure Entra ID 的自动登录支持**

  Citrix Secure Access 支持使用主刷新令牌 (PRT) 机制为 NetScaler Gateway 和 SecurAccess ZTNA 提供 Azure AD 联接计算机和混合 Azure AD 联接计算机的自动登录功能。有关详细信息，请参阅 适用于 Windows Azure AD 联接计算机的 Citrix Secure Access 自动登录。

- **支持分类和排查枚举失败**

  Citrix Secure Access 现在支持在 SecurAccess ZTNA 部署中使用 Citrix Monitor 或 Citrix Director 分类和排查枚举失败。有关详细信息，请参阅 SecurAccess ZTNA 与 Director 集成（预览版）。

- **增强的 Windows 上次更新扫描**

  Windows 上次更新扫描现在会检查通过 Windows 自动升级服务安装的 Windows 更新，以及通过 BigFix、Intune 和其他第三方工具安装的更新。有关详细信息，请参阅 高级端点分析扫描。

- **支持基于 TCP 的 DNS 请求的分裂 DNS**

  Citrix Secure Access 支持基于 TCP 的 DNS 请求的分裂 DNS，与基于 UDP 的 DNS 请求相同。管理员可以使用 `EnableTCPDNS` 注册表启用此功能。有关详细信息，请参阅 会话策略 和 NetScaler Gateway Windows VPN 客户端注册表项。

- **增强的客户端证书身份验证**

  在客户端证书身份验证期间，Citrix Secure Access 会根据 NetScaler Gateway 上配置的 CA 证书自动选择客户端证书。有关详细信息，请参阅 配置客户端证书身份验证。

- **支持本地部署的 Citrix SecurAccess ZTNA™**

  Citrix Secure Access 现在支持本地部署的 Citrix SecurAccess ZTNA。有关详细信息，请参阅 Citrix Secure Access 客户端。

已修复的问题

- 如果由于网络无法访问导致身份验证失败，Citrix Secure Access 客户端不会在 Windows 凭据提供程序屏幕上显示正确的错误消息。
- Citrix Secure Access 客户端 UI 无法显示使用 NetScaler Gateway RfWebUI 门户主题配置的自定义消息。
- 如果应用于 Citrix 虚拟适配器（连接到 Citrix Secure Access）的 DNS 后缀在 15 个字符后被截断，则 DNS 流量将被丢弃。发生此问题的原因是 NetScaler Gateway 将 DNS 后缀视为 NetBIOS 名称。
- 当用户通过 VPN 隧道访问多个应用程序时，Citrix Secure Access 客户端会产生高 DNS 流量。

24.6.1.18 (Jul 24, 2024)

> **重要更新：**
>
> Citrix Secure Access 版本 24.6.1.18 取代了 24.6.1.17，现已正式发布。

新增功能

- **EPA 扫描以检查 Citrix Workspace 应用程序版本**

  Citrix Secure Access 支持新的 EPA 扫描“CWA Version”，用于验证 Windows 计算机上的 Citrix Workspace 版本。有关支持的 EPA 扫描的详细信息，请参阅 Expression strings。

- **通过 Citrix Workspace 应用程序自动单点登录到 Citrix Secure Access**

  Citrix Workspace 应用程序为 Citrix Secure Access 提供了统一的客户端管理体验。当用户登录到 Citrix Workspace 应用程序时，他们会自动登录到 Citrix Secure Access，并且可以无缝访问 TCP/UDP 应用程序，无需手动配置和登录多个客户端应用程序。有关详细信息，请参阅 Automatic single sign-on to Citrix Secure Access through Citrix Workspace app for Windows - Preview。

- **SecurAccess ZTNA 中的隧道排除支持**

  Citrix Secure Access 现在可以通过使用注册表排除某些应用程序流量不进行隧道传输，`ExcludeDomainsFromTunnel`。

如果 `example.com` 是托管多个应用程序的内网域，并且您想排除特定应用程序（例如 `sshhost.example.com`、`rdphost.example.com`、`*.ftphost.example.com`），则可以使用此注册表。

有关详细信息，请参阅NetScaler Gateway Windows VPN 客户端注册表项。

- **基于 TCP 的 DNS 请求的 IP 地址欺骗**

  Citrix Secure Access 在以下场景中支持基于 TCP 的 DNS 请求的 IP 地址欺骗：

  - 在 NetScaler Gateway 上配置了基于 FQDN 的隧道规则。
  - FQDN 与 Citrix SecurAccess ZTNA 部署中的 DNS 后缀匹配。

- **与第三方安全 Web 网关的互操作性增强**

  Citrix Secure Access 的 User-Agent 字符串已更新，以增强与第三方安全 Web 网关的互操作性。

- **支持本地部署的 Citrix SecurAccess ZTNA**

  Citrix Secure Access 现在支持本地部署的 Citrix SecurAccess ZTNA。

- **增强的 EPA 扫描加密**

  EPA 扫描的安全加密通过椭圆曲线 Diffie-Hellman (ECDH) 密钥得到增强。

- **用于签名创建的哈希密钥**

  管理员现在可以使用 SHA-384 哈希密钥为设备证书身份验证创建签名。

- **POP 故障期间的无缝连接**

  在 SecurAccess ZTNA 部署中，当与当前 POP 的连接失败时，VPN 用户会自动重新连接到不同的接入点 (POP)，无需手动干预。

- **增强的诊断功能**

  Citrix Secure Access 诊断功能已增强，增加了更多字段，有助于排查 TCP/UDP 应用程序的访问问题。

已修复的问题

- 如果禁用 Windows Management Instrumentation Command-line (WMIC) 功能，Windows 11 设备上的 DNS 解析将失败。
- 如果在 NetScaler Gateway 上配置了反向拆分隧道和内网 IP 地址，Citrix Secure Access 会阻止 IPv6 流量通过环回接口路由。

  ,
- 如果内部网应用程序的 IP 地址范围配置了通配符子网掩码，Citrix Secure Access 会崩溃。
- 升级后，如果 NetScaler Gateway 上配置了反向拆分隧道和内部网 IP 地址，用户将无法连接到 Microsoft 应用程序。
- 当 Citrix Secure Access 客户端配置了 WFP 时，在活动会话期间或发生多次登录和注销时，VPN 连接会丢失。
- 当客户端计算机上的应用程序发送 `A` 和 `AAAA` 记录类型 DNS 查询时，DNS 解析会延迟。
- 在 Citrix SecurAccess ZTNA 部署中，Kerberos 身份验证失败。
- 在 Windows 筛选平台 (WFP) 模式下，Citrix Secure Access UI 上“安全应用程序”连接选项卡中，正在访问的内部网资源的应用程序名称显示为 **N/A**。
- 在 Citrix SecurAccess ZTNA 部署中，如果配置了 Always On，Citrix Secure Access 客户端无法从机器级隧道切换到用户级隧道。

24.4.1.7 (Apr 30, 2024)

已修复的问题

当 Microsoft Edge WebView 模式下的自动登录失败时，最终用户无法登录 Citrix Secure Access。

当客户端应用程序发送 AAAA 记录类型 DNS 查询时，某些后端资源的 DNS 解析失败。

,

如果客户端运行数小时，Citrix Secure Access 可能无法在 WFP 驱动程序模式下建立新连接。

, ,

尽管语言设置为英语，Citrix Secure Access 仍以其他语言显示设备证书失败的 EPA 扫描错误消息。

如果在 WFP 模式下配置了 Always On VPN，则在长时间的 VPN 会话后，Internet 和 Intranet 连接可能会丢失。

配置“filetime”参数时，EPA 扫描失败。

在 EPA 扫描期间，文件的 MD5 校验和配置失败。

Windows 凭据管理器屏幕显示 Citrix Secure Access 图标，即使 VPN 未处于 Always On VPN 模式。

Citrix Secure Access 日志以相反的顺序显示 IP 地址。例如，如果 Microsoft Edge 浏览器连接到 NetScaler (IP: 192.20.4.5:24)，则日志消息显示为：

```
"Application msedge.exe has opened a connection to 5.4.20.192:24 |Making a connection to 5.4.20.192:24 by msedge.exe |"
```

升级后，当用户单击 Citrix Secure Access GUI 上的“**主页**”按钮时，主页 URL 无法在默认浏览器中启动。

如果设备证书由中间 CA 而非根 CA 签名，则在 Citrix SecurAccess ZTNA 部署中设备证书检查将失败。

24.2.1.15 (Mar 04, 2024)

新增功能

- **支持 SNI**

  在 Citrix SecurAccess ZTNA 部署中，Citrix Secure Access 客户端现在支持所有预身份验证请求上的服务器名称指示 (SNI) 扩展。

- **支持 TLS 1.3**

  Citrix Secure Access 客户端现在支持 TLS 1.3 协议。TLS 1.3 支持以下平台：

  - Windows 11 及更高版本
  - Windows Server 2022 及更高版本

  有关如何在 NetScaler 上配置 TLS 1.3 的详细信息，请参阅支持 TLS 1.3 协议。

- **支持 HTTP 标头中的 Windows 操作系统详细信息**

  Citrix Secure Access 客户端现在将 Windows 操作系统详细信息作为 HTTP 标头 (user-agent) 字符串的一部分包含在内。

已修复的问题

- 如果客户端网络适配器上启用了 IPv6，DNS 解析会间歇性失败。
- 如果同时使用自动登录尝试登录，用户可能无法登录 Citrix Secure Access 客户端。
- 在非英语客户端计算机上启用 Smart App Control 时，Citrix Secure Access 安装失败。

  ,
- 如果 Citrix Secure Access 客户端配置了 WFP 驱动程序，用户将无法通过 VPN 访问某些应用程序。此问题是由于防火墙策略修改导致的。

  ,
- 在 EPA 扫描期间会弹出一个对话框。但是，当用户单击“确定”后，EPA 扫描会正常工作。当在 Citrix Secure Access 客户端 UI 上选择瑞典语（**配置 > 语言**）时，会出现此问题。
- 在 Always On VPN 模式下，当在 NetScaler Gateway 上配置了用户证书身份验证时，机器级隧道无法传输会话。
- 当 Citrix Secure Access 客户端上启用了 Windows 筛选平台 (WFP) 驱动程序时，对内部网资源的访问会间歇性失败。
- 当用户单击“主页”按钮时，Citrix Secure Access 客户端 UI 页面会间歇性冻结。
- 如果满足以下条件，非管理员用户无法连接到完整的 VPN 隧道：
  - EPA 在 nFactor 流程中配置为一个因素。
  - Edge WebView 已启用。
  - Citrix EPA 客户端的控制升级设置在 NetScaler Gateway 上设置为“**始终**”，并且客户端设备和 NetScaler 之间的 Citrix EPA 客户端版本不匹配。
- 如果客户端计算机的系统证书存储中只包含一个设备证书，则 EPA 设备证书扫描会失败。
- 连接到 Citrix SecurAccess ZTNA 服务时，Citrix Secure Access 客户端的登录页面会间歇性地显示为空白。

- 如果使用 Windows Server 2019 或更高版本，最终用户可能无法通过 VPN 将客户端计算机连接到域。
- 启用 Citrix Device Posture 服务后，Citrix Secure Access 客户端 UI 的“**连接**”下拉列表中会出现不需要的条目。
- 如果在 Citrix Secure Access 客户端上启用了单点登录功能，最终用户将无法访问内部网资源。
- Citrix Secure Access 可能会因内存损坏而崩溃。

23.10.1.7 (29-Nov-2023)

新增功能

- **配置用于服务器发起的连接的私有端口范围**

  您现在可以为服务器发起的连接配置一个私有端口范围，从 49152 到 64535。配置私有端口可避免在使用端口在 Citrix Secure Access 客户端和客户端计算机上的第三方应用程序之间创建套接字时可能出现的冲突。您可以通过使用“SicBeginPort”Windows VPN 注册表来配置私有端口。或者，您可以通过在 NetScaler 上使用 VPN 插件自定义 JSON 文件来配置私有端口范围。

  有关详细信息，请参阅配置服务器发起的连接 和NetScaler Gateway Windows VPN 客户端注册表项。

- **Kerberos 身份验证支持无缝自动登录**

  Citrix Secure Access 客户端现在使用 Kerberos 身份验证方法进行自动登录。作为此支持的一部分，引入了一个 VPN 客户端注册表项“EnableKerberosAuth”。作为先决条件，管理员必须在 NetScaler 和其客户端计算机上配置 Kerberos 身份验证。最终用户必须在其计算机上安装 Microsoft Edge WebView 才能启用 Kerberos 身份验证方法。有关详细信息，请参阅使用 Kerberos 身份验证自动登录。

- **自动分配欺骗 IP 地址范围**

  如果管理员配置的欺骗 IP 地址范围与基于 IP 的应用程序或最终用户的网络之间存在冲突，Citrix Secure Access 客户端现在可以检测并应用新的欺骗 IP 地址范围。

- **Microsoft 通知**

  Citrix Secure Access 客户端通知现在以 Microsoft 通知形式显示在您的 Windows 计算机的通知面板上。

- **改进的日志收集**

  Verbose 日志级别现在用作默认调试日志记录级别，以增强日志收集和故障排除。有关日志记录的详细信息，请参阅使用 Citrix Secure Access 客户端 UI 配置日志记录。

已修复的问题

如果 Always On 服务的计算机隧道未能检测到客户端设备位置，Citrix Secure Access 客户端将保持“正在连接”状态。

当 Citrix Secure Access 客户端中启用了 Microsoft Edge WebView 时，传输登录功能无法正常工作。

在 Always On 服务模式下，如果基于设备证书的经典身份验证策略绑定到 VPN 虚拟服务器，Citrix Secure Access 客户端无法与 NetScaler Gateway 建立计算机级隧道。

当用户连接到 VPN 时，传入和传出 Webex 呼叫失败。当 Citrix Secure Access 客户端上启用了 Windows 筛选平台 (WFP) 驱动程序而不是确定性网络增强器 (DNE) 驱动程序时，会出现此问题。

如果满足以下条件，Citrix Secure Access 客户端会崩溃：

- 当 SAML 策略绑定到 VPN 虚拟服务器时，连接会切换。
- 启用了 Internet Explorer WebView 支持。

在自动登录期间，Citrix Secure Access 客户端 UI 会显示“连接”按钮。如果使用 UserCert 身份验证方法连接到 VPN，则会出现此问题。

如果配置了机器级隧道，本地 LAN 访问功能将无法与 Citrix Secure Access 客户端配合使用。

在此版本中，本地 LAN 访问功能可以与机器级隧道配置一起设置。为此，在使用机器隧道模式时，必须将本地 LAN 访问参数配置为 FORCED。有关更多详细信息，请参阅 根据 ADC 配置对最终用户强制执行本地 LAN 访问。

当客户端计算机多次从睡眠模式唤醒时，Citrix Secure Access 客户端无法与内网应用程序建立 VPN 连接。

23.8.1.11 (19-Oct-2023)

已修复的问题

如果在 NetScaler Gateway 上配置了正向代理支持，则 epaPackage.exe 文件可能无法下载。

对于对 C 盘访问受限的非管理员用户，Citrix EPA 客户端安装失败。

23.8.1.5 (09-Aug-2023)

已修复的问题

当通过 Citrix SecurAccess ZTNA 服务连接时，应用程序的 Kerberos SSO 失败。

使用 Citrix SecurAccess ZTNA 服务访问应用程序会间歇性失败。当 Citrix Secure Access 客户端共享了 TCP 或 UDP 流量的不正确目标 IP 地址时，会出现此问题。

由于 DNS 缓存问题，Citrix Secure Access 客户端会间歇性地无法启动应用程序。

Citrix Secure Access 客户端无法将 DNS 后缀应用于 Citrix Virtual Adapter。当 Citrix Virtual Adapter 无法通过 Active Directory 进行身份验证时，会出现此问题。

如果满足以下条件，Citrix Secure Access 客户端会崩溃：

- NetScaler Gateway 虚拟服务器包含客户端证书作为 nFactor 身份验证的一个因素。
- Microsoft Edge WebView 支持已启用。

连接到 VPN 后，在应用 Microsoft KB5028166 后，您可能无法访问后端资源。

当门户自定义项超出允许的限制时，Citrix Secure Access 客户端会间歇性地无法从 NetScaler Gateway 下载配置。

已知问题

传输登录功能无法与 Citrix Secure Access 客户端配合使用。当 Microsoft Edge WebView 启用时，会出现此问题。

解决方法：使用 Web 浏览器登录以传输会话。

23.7.1.1 (2023 年 7 月 14 日)

已修复的问题

在某些情况下，升级到版本 23.x.x.x 后，流量无法通过 VPN 隧道，导致在 NetScaler 上配置了内网 IP 范围时 VPN 访问被阻止。当交叉配置文件防火墙规则未应用于 VPN 应用程序时，会发生这种情况。

23.5.1.3 (2023 年 6 月 2 日)

已修复的问题

当在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client` 下使用“useNewLogger”注册表启用改进的日志收集时，Always On 服务会崩溃。

23.4.1.5 (2023 年 4 月 14 日)

新增功能

- **对 Microsoft Edge WebView 的支持**

  Windows 版 Citrix Secure Access 客户端上的 Microsoft Edge WebView 支持可提供增强的最终用户体验。此功能默认禁用。有关详细信息，请参阅 Windows 版 Citrix Secure Access 的 Microsoft Edge WebView 支持。

- **添加 DNS 后缀以将 FQDN 解析为 IP 地址**

  管理员现在可以在操作系统级别为应用程序添加后缀。这有助于 Citrix Secure Access 客户端在名称解析期间解析非完全限定域名。

  管理员还可以使用 IP 地址（IP CIDR/IP 范围）配置应用程序，以便最终用户可以使用相应的 FQDN 访问应用程序。有关详细信息，请参阅DNS 后缀以将 FQDN 解析为 IP 地址。

- **改进的日志收集**

  Windows Secure Access 客户端的日志记录功能现已改进，可用于日志收集和调试。日志记录功能进行了以下更改。

  - 允许用户将最大日志文件大小更改为小于 600 MB 的值。
  - 允许用户将日志文件数量更新为小于 5。
  - 将新日志记录功能的日志级别增加到三个。

  通过这些更改，管理员和最终用户可以从当前会话和过去会话中收集日志。以前，日志收集仅限于当前会话。有关详细信息，请参阅改进的 Windows 客户端日志收集。

  > **注意：**

> 要启用调试日志记录，请从**选择日志级别**下拉列表中选择**日志记录 > 详细**。在 Citrix Secure Access 客户端 for Windows 23.4.1.5 版本之前，可以通过**配置 > 启用调试日志记录**复选框启用调试日志记录。

- **支持将事件发送到 Citrix Analytics 服务**

  Citrix Secure Access 客户端（适用于 Windows）现在支持将会话创建、会话终止和应用程序连接等事件发送到 Citrix Analytics 服务。这些事件随后会记录在 Citrix SecurAccess ZTNA 仪表板中。

已修复的问题

- 对于 Unicode 用户，Citrix Secure Access 客户端与 Citrix Workspace 应用程序到云端点的单点登录身份验证失败。
- 当在 Citrix SecurAccess ZTNA 中配置基于主机名的应用程序以及 DNS 后缀时，对资源的访问失败。
- 由于网关虚拟服务器可达性问题，Always-On VPN 连接在启动时间歇性失败。
- 当 Citrix Secure Access 客户端上的拆分隧道设置为“关闭”时，无法访问与欺骗性 IP 地址范围重叠的内部网资源。
- Citrix Secure Access 客户端无法加载身份验证架构，导致在 Citrix SecurAccess ZTNA 服务中登录失败。

23.1.1.11 (20-Feb-2023)

此版本解决了有助于提高 Citrix SecurAccess ZTNA 服务整体性能和稳定性的问题。

23.1.1.8 (2023 年 2 月 8 日)

已修复的问题

- 由于 Citrix Secure Access 未能优先处理 IPv4 数据包而非 IPv6 数据包，导致 DNS 解析失败。
- 当 Citrix Secure Access 客户端在 Windows 筛选平台 (WFP) 模式下运行时，将捕获操作系统筛选规则。

- 当 Citrix Secure Access 客户端在 Citrix Deterministic Network Enhancer (DNE) 模式下运行时，基于 IP 的内网应用程序会使用欺骗性 IP 地址。
- 使用 Windows 筛选平台 (WFP) 驱动程序时，有时在 VPN 重新连接后内网访问不起作用。
- 在 Windows 10 和 Windows 11 企业版多会话桌面上，用于操作系统版本检查的端点分析 (EPA) 扫描失败。
- Windows 客户端默认支持 64 KB 的配置文件大小，这限制了用户在配置文件中添加更多条目。可以通过在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client 中设置 `ConfigSize` 注册表值来增加此大小。`ConfigSize` 注册表项类型为 `REG_DWORD`，键数据为 `<Bytes size>`。如果配置文件大小大于默认值 (64 KB)，则每增加 64 KB，ConfigSize 注册表值必须设置为 5 x 64 KB（转换为字节后）。例如，如果您要额外添加 64 KB，则必须将注册表值设置为 64 x 1024 x 5 = 327680。同样，如果您要添加 128 KB，则必须将注册表值设置为 64 x 1024 x (5+5) = 655360。
- 在 VPN 注销时，SearchList 注册表中的 DNS 后缀列表条目会以一个或多个逗号分隔的倒序重写。
- 当 NetScaler 设备完成防病毒 EPA 扫描时，代理身份验证失败。
- 如果 Citrix Secure Access 相关的注册表值超过 1500 个字符，则日志收集器无法收集错误日志。

22.10.1.9 (2022年11月8日)

新增功能

- **GSLB 中连接代理类型站点持久性的 EPA 支持**

  现在，当从浏览器启动扫描时，Windows EPA 扫描支持 GSLB 中连接代理类型站点持久性。以前，Windows 的 EPA 扫描不支持浏览器启动的 EPA 扫描的连接代理持久性类型。

- **Workspace URL 的无缝单点登录（仅限云）**

  如果用户已通过 Citrix Workspace 应用程序登录，Citrix Secure Access 客户端现在支持 Workspace URL 的单点登录（仅限云）。有关更多详细信息，请参阅通过 Citrix Workspace 应用程序登录的用户对 Workspace URL 的单点登录支持。

- **通过 Citrix Workspace 应用程序管理 Citrix Secure Access 客户端和/或 EPA 插件版本（仅限云）**

  Citrix Workspace 应用程序现在能够通过全局应用程序配置服务下载并安装最新版本的 Citrix Secure Access 和/或 EPA 插件。有关更多详细信息，请参阅全局应用程序配置服务。

- **调试日志控制增强**

  Citrix Secure Access 客户端的调试日志控制现在独立于 NetScaler Gateway，并且可以从插件 UI 为机器隧道和用户隧道启用或禁用。

- **支持专用网络访问预检请求**

  适用于 Windows 的 Citrix Secure Access 客户端现在支持 Chrome 浏览器在从公共网站访问专用网络资源时发出的专用网络访问预检请求。

已修复的问题

- Citrix Secure Access 客户端 21.7.1.1 及更高版本无法为没有管理权限的用户升级到更高版本。

  这仅适用于从 NetScaler 设备执行 Citrix Secure Access 客户端升级的情况。

- 由于间歇性 EPA 故障，用户无法登录 VPN。

- 有时，处于仅机器隧道模式的 Citrix Secure Access 客户端在机器从睡眠模式唤醒后不会自动建立机器隧道。

- 在“始终开启”服务模式下，即使只配置了计算机隧道，用户隧道也会尝试启动。

- 如果 Microsoft Edge 是默认浏览器，Citrix Secure Access UI 上的“主页”链接将不起作用。

- 自定义 EPA 失败日志消息未在 NetScaler Gateway 门户上显示，而是显示“内部错误”消息。

- 当用户在 Windows 版 Citrix Secure Access 屏幕上单击“主页”选项卡时，页面会显示“连接被拒绝”错误。

- 在某些客户端计算机上，Citrix Secure Access 客户端无法检测到代理设置，这会导致登录失败。

已知问题

- 基于 Windows Update 检查的 EPA 扫描在 Windows 11 22H2 版本上不起作用。

22.6.1.5 (2022 年 6 月 17 日)

新增功能

- **登录和注销脚本配置**

  当 Citrix Secure Access 客户端连接到 Citrix SecurAccess ZTNA 云服务时，它会从以下注册表访问登录和注销脚本配置。

  注册表路径：**HKEY_LOCAL_MACHINE>SOFTWARE>Citrix > Secure Access Client**

  注册表值：

  - SecureAccessLogInScript type REG_SZ - 登录脚本路径
  - SecureAccessLogOutScript type REG_SZ - 注销脚本路径

- **使用 Windows 筛选平台 (WFP) 的 Windows Citrix Secure Access 客户端**

  WFP 是一组 API 和系统服务，提供用于创建网络筛选应用程序的平台。WFP 旨在取代以前的数据包筛选技术，即与 DNE 驱动程序一起使用的网络驱动程序接口规范 (NDIS) 筛选器。有关详细信息，请参阅 使用 Windows 筛选平台的 Windows Citrix Secure Access 客户端。

- **基于 FQDN 的反向拆分隧道支持**

  WFP 驱动程序现在支持基于 FQDN 的反向拆分隧道。DNE 驱动程序不支持此功能。有关反向拆分隧道的更多详细信息，请参阅 拆分隧道选项。

已修复的问题

- 有时，当用户在 Always On 服务模式下登录 Windows 计算机时，Windows 自动登录不起作用。计算机隧道不会转换为用户隧道，并且 VPN 插件 UI 中会显示“**正在连接**”消息。

- 在 VPN 注销时，SearchList (Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client) 注册表中的 DNS 后缀列表条目会以逗号分隔的倒序重写。

- 即使 NetScaler 内网应用程序配置从基于 FQDN 更改为基于 IP 的应用程序，仍会使用欺骗性 IP 地址。

- 网关插件成功建立 VPN 隧道后，网关主页不会立即显示。

  通过此修复，引入了以下注册表值。

  \HKLM\Software\Citrix\Secure Access Client\SecureChannelResetTimeoutSeconds

  类型: DWORD

  默认情况下，此注册表值未设置或未添加。当“SecureChannelResetTimeoutSeconds”的值为 0 或未添加时，处理延迟的修复不起作用，这是默认行为。管理员必须在客户端上设置此注册表以启用修复（即在网关插件成功建立 VPN 隧道后立即显示主页）。

- 如果注册表值大于 2000 字节，则 AlwaysOnAllow 列表注册表无法按预期工作。

- 如果已连接的 Citrix SecurAccess ZTNA 服务区域变得不可达，适用于 Windows 的 Citrix Secure Access 客户端不会将新的 TCP 连接隧道传输到后端 TCP 服务器。但是，这不影响本地网关连接。

22.3.1.5 (2022 年 3 月 24 日)

已修复的问题

- Windows EPA 插件名称已恢复为 NetScaler Gateway EPA 插件。

已知问题

- 如果已连接的 Citrix SecurAccess ZTNA 服务区域变得不可访问，适用于 Windows 的 Citrix Secure Access 客户端不会将新的 TCP 连接隧道传输到后端 TCP 服务器。但是，这不影响本地网关连接。

22.3.1.4 (2022 年 3 月 10 日)

新增功能

- **根据 ADC 配置对最终用户强制执行本地 LAN 访问**

  管理员可以限制最终用户在其客户端计算机上禁用本地 LAN 访问选项。现有本地 LAN 访问参数值中添加了一个新选项“FORCED”。当本地 LAN 访问值设置为“FORCED”时，客户端计算机上的最终用户始终启用本地 LAN 访问。最终用户无法使用 Citrix Secure Access 客户端 UI 禁用本

地 LAN 设置。如果管理员希望为最终用户提供启用或禁用本地 LAN 访问的选项，则必须将本地 LAN 访问参数重新配置为“ON”。

要使用 GUI 启用 **FORCED** 选项：

a. 导航到 **NetScaler Gateway > 全局设置 > 更改全局设置**。
b. 单击“**客户端体验**”选项卡，然后单击“**高级设置**”。
c. 在“**本地 LAN 访问**”中，选择“**FORCED**”。

要使用 CLI 启用 **FORCED** 选项，请运行以下命令：

```
set vpn parameter -localLanAccess FORCED
```

- **EPA 操作系统扫描支持 Windows Server 2019 和 2022**

  EPA 操作系统扫描现在支持 Windows Server 2019 和 2022。

  您可以使用 GUI 选择新的服务器。

  a. 导航到 **NetScaler Gateway > 策略 > 预身份验证**。
  b. 创建新的预身份验证策略或编辑现有策略。
  c. 单击 **OPSWAT EPA 编辑器** 链接。
  d. 在**表达式编辑器**中，选择 **Windows > Windows Update**，然后单击 **+** 图标。
  e. 在 **OS 名称**中，根据您的要求选择服务器。

  您可以升级到 OPSWAT 版本 4.3.2744.0，以便在 EPA 操作系统扫描中使用 Windows Server 2019 和 2022。

- **缺少安全补丁的 EPA 扫描新分类类型**

  以下新的分类类型已添加到 EPA 扫描中，用于检测缺少的安全补丁。如果客户端缺少以下任何安全补丁，EPA 扫描将失败。

  ◦ 应用程序
  ◦ 连接器
  ◦ 关键更新
  ◦ 定义更新
  ◦ 开发人员工具包

- 功能包
- 指导
- 安全更新
- 服务包
- 工具
- 更新汇总
- 更新

您可以使用 GUI 配置分类类型。

a. 导航到 **NetScaler Gateway > 策略 > 预身份验证**。
b. 创建新的预身份验证策略或编辑现有策略。
c. 单击 ((OPSWAT EPA Editor)) 链接。
d. 在表达式编辑器中，选择 **Windows > Windows Update**。
e. 在 **不应缺少以下 Windows 更新分类类型的修补程序** 中，选择缺少安全修补程序的分类类型
f. 单击 **确定**。

您可以升级到 OPSWAT 版本 4.3.2744.0 以使用这些选项。

- 有关 Windows 服务器更新服务分类 GUID 的详细信息，请参阅 `<https://docs.microsoft.com/zh-cn/previous-versions/windows/desktop/ff357803(v=vs.85)>`
- 有关 Microsoft 软件更新术语的说明，请参阅 `<https://docs.microsoft.com/zh-cn/troubleshoot/windows-client/deployment/standard-terminology-software-updates>`

此前，EPA 对 Windows 客户端上缺失安全补丁的扫描是根据严重性级别（严重、重要、中等和低）进行的。

- **支持 EPA 扫描的多个设备证书**

在 Always on VPN 配置中，如果配置了多个设备证书，则会尝试使用有效期最长的证书进行 VPN 连接。如果此证书成功通过 EPA 扫描，则建立 VPN 连接。如果此证书在扫描过程中失败，则使用下一个证书。此过程将持续到所有证书都尝试完毕。

此前，如果配置了多个有效证书，并且其中一个证书的 EPA 扫描失败，则不会尝试对其他证书进行扫描。

已修复的问题

- 如果在配置 VPN 虚拟服务器时，SSL 配置文件中的 clientCert 参数设置为“Optional”，则会多次提示用户选择智能卡。
- 用户在将“networkAccessOnVPNFailure”始终开启配置文件参数从“fullAccess”更改为“onlyToGateway`”后，无法连接到 NetScaler Gateway 设备。
- 配置“始终开启”时，由于 aoservice.exe 文件中的版本号不正确 (1.1.1.1)，用户隧道会失败。
- 在长时间的 VPN 会话期间，对内部和外部资源的 DNS 解析停止工作。
- Windows VPN 客户端不遵守来自服务器的“SSL close notify”警报，并在同一连接上发送传输登录请求。
- 针对“==”和“!=”运算符的注册表 EPA 检查对某些注册表项失败。

22.2.1.103 (2022 年 2 月 17 日)

已修复的问题

- 升级到 Chrome 98 或 Edge 98 浏览器版本后，用户无法启动 EPA 插件或 VPN 插件。要解决此问题，请执行以下操作：
  a. 对于 VPN 插件升级，最终用户必须首次使用 VPN 客户端连接才能在其计算机上获取修复。在随后的登录尝试中，用户可以选择浏览器或插件进行连接。
  b. 对于仅限 EPA 的用例，最终用户将没有 VPN 客户端连接到网关。在这种情况下，请执行以下操作：
     a. 使用浏览器连接到网关。 a. 等待下载页面出现并下载 nsepa_setup.exe。 b. 下载后，关闭浏览器并安装 nsepa_setup.exe 文件。 c. 重新启动客户端。

21.12.1.4 (2021 年 12 月 17 日)

新增功能

- **品牌重塑更改**

  适用于 Windows 的 NetScaler Gateway 插件已更名为 Citrix Secure Access 客户端。

- **支持 TCP/HTTP(S) 私有应用程序**

Citrix Secure Access 客户端现在通过 Citrix Workspace Secure Access 服务支持远程用户的 TCP/HTTP(S) 私有应用程序。

- **新增语言支持**

  适用于 NetScaler Gateway 的 Windows VPN 和 EPA 插件现在支持以下语言：

  - 韩语
  - 俄语
  - 中文（繁体）

- **Citrix Secure Access 提供对 Windows 11 的支持**

  Citrix Secure Access 客户端现已支持 Windows 11。

- **当用户从同一台计算机登录且已配置 Always on 时自动传输登录**

  当配置了 Always on 且用户从同一台计算机登录时，现在无需任何用户干预即可进行自动登录传输。以前，当客户端（用户）在系统重启或网络连接问题等情况下需要重新登录时，会弹出一个消息。用户必须确认传输登录。通过此增强功能，弹窗已被禁用。

- **从 NetScaler 提供的子网掩码派生 Citrix 虚拟适配器默认网关 IP 地址**

  Citrix 虚拟适配器默认网关 IP 地址现在从 NetScaler 提供的子网掩码派生。

已修复的问题

- 有时，在分流隧道开启模式下建立 VPN 隧道后，用户会失去互联网访问权限。Citrix 虚拟适配器错误的默认路由导致了此网络问题。

- 当分流隧道设置为“反向”时，内网域名的 DNS 解析失败。

21.9.100.1 (2021 年 12 月 30 日)

新增功能

- **Citrix Secure Access 提供对 Windows 11 的支持**

  Citrix Secure Access 客户端现在支持 Windows 11。

已修复的问题

- 有时，在分流模式下建立 VPN 隧道后，用户会失去互联网访问权限。Citrix 虚拟适配器错误的默认路由导致此网络问题。
- 当分流设置为“反向”时，内网域的 DNS 解析失败。

21.9.1.2 (2021 年 10 月 4 日)

已修复的问题

- 有时，在断开 VPN 连接后，DNS 解析器无法解析主机名，因为 DNS 后缀在 VPN 断开连接期间被删除。
- 有时，当设置了客户端空闲超时时，用户会在几秒钟内从 NetScaler Gateway 注销。
- Windows 插件在身份验证期间可能会崩溃。
- 在 Always On 服务模式下，用户登录到 Windows 计算机后，Windows 版 VPN 插件无法自动建立用户隧道。
- 隧道建立后，Windows 插件会使用默认网关地址添加路由，而不是使用之前的网关 IP 地址添加 DNS 服务器路由。

V21.7.1.1 (27-Aug-2021)

新增功能

- **新的 MAC 地址扫描**

  增加了对更新的 MAC 地址扫描的支持。

- **EPA 扫描以检查 Windows 操作系统及其内部版本**

  增加了 EPA 扫描以检查 Windows 操作系统及其内部版本。

- **EPA 扫描以检查特定值是否存在**

  注册表 EPA 扫描中的新方法现在可以检查特定值是否存在。

已修复的问题

- 如果在登录期间因网络错误而出现 JavaScript 错误，则后续登录尝试将因相同的 JavaScript 错误而失败。
- EPA 扫描无法检查 McAfee 防病毒软件的上次更新时间。
- 有时，用户在建立 VPN 隧道后会失去互联网访问权限。
- 在 nFactor 身份验证期间，可能会显示 VPN 插件的脚本错误。
- 如果发生网络中断，在网络中断之前开始的 UDP 流量流在长达 5 分钟内不会中断。
- 如果 DNS 注册花费的时间比预期长，您可能会遇到 VPN 隧道启动延迟的情况。

V21.3.1.2 (2021 年 3 月 31 日)

新增功能

- **升级了 EPA 库**

  EPA 库已升级，以支持 EPA 扫描中使用的软件应用程序的最新版本。

- **NetScaler Gateway 虚拟适配器兼容性**

  NetScaler Gateway 虚拟适配器现在与 Hyper-V 和 Microsoft Wi-Fi Direct 虚拟适配器（与打印机配合使用）兼容。

已修复的问题

- Windows VPN 网关插件会阻止通过 VPN 隧道使用“CTRL + P”和“CTRL + O”。
- 当为计算机名请求 `"nslookup"` 操作时，适用于 Windows 的 NetScaler Gateway 插件仅使用在 Active Directory 中注册的 Intranet IP 地址进行响应。
- 如果拆分 DNS 设置为“本地”或“两者”，则 IIP 注册和注销会间歇性失败。
- 如果配置了 Always On，则自动登录到 Windows VPN 网关插件会失败。
- Windows VPN 网关插件未能丢弃 IPv6 DNS 数据包，导致 DNS 解析出现问题。

- 即使由于 Internet Explorer 代理例外列表的浏览器限制导致列表溢出，Windows VPN 网关插件仍会维护现有的代理例外列表。
- 在 Always On 模式下，当 VPN 客户端注销时，Windows VPN 网关插件未能恢复代理设置。
- 如果满足以下条件，适用于 Windows 的 VPN 插件在登录 Windows 后不会建立隧道：
  - NetScaler Gateway 设备配置了 Always On 功能。
  - 设备配置为基于证书的身份验证，且双因素身份验证“关闭”。

预览版功能

预览版功能可在非生产或有限生产环境中使用，并为客户提供分享反馈的机会。我们不接受针对预览版功能的支援案例，但欢迎提供改进反馈。我们可能会根据反馈的严重性、关键性和重要性采取行动。

以下功能目前处于预览阶段：

适用于 Windows Citrix Secure Access 的微软 Edge WebView 支持

> **注意：**
>
> 从适用于 Windows 的 Citrix Secure Access 客户端版本 24.11.1.17 开始，Microsoft Edge WebView 默认启用。

Windows 客户端的日志收集改进

适用于 Windows 安全访问客户端的日志记录功能通过改进的日志收集和调试得到了增强。新的日志文件以“csa_”为前缀。

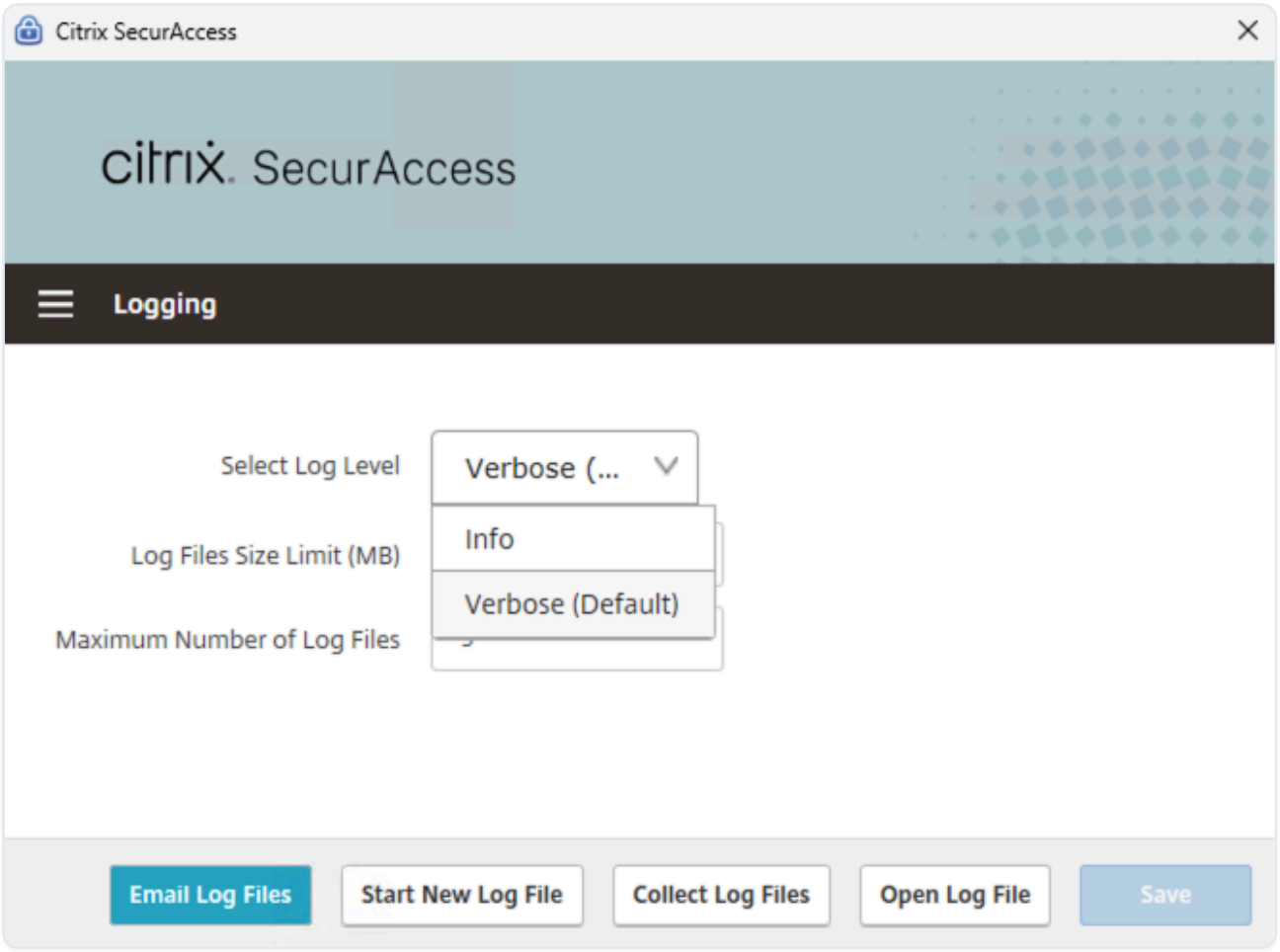
从适用于 Windows 23.10.1.7 的 Citrix Secure Access 客户端开始，默认日志级别设置为“详细”，以增强日志收集和故障排除功能。

通过这些更改，管理员和最终用户可以收集当前会话和过去会话的日志。以前，日志收集仅限于当前会话。

使用 Citrix Secure Access™ 客户端 UI 配置日志记录

1. 安装适用于 Windows 的 Secure Access 客户端。

2. 从菜单中单击“**日志记录**”。所有与日志相关的配置都可以在“日志记录”屏幕中完成。



- **选择日志级别：**

  启用新的日志记录机制后，可以使用以下三个日志级别。

  - 错误：仅记录应用程序报告的异常或故障。
  - 信息：此级别包括信息性消息和与程序执行相关的事件。它还包括错误和异常。
  - 详细（默认）：此级别包括错误和信息日志级别报告的所有日志消息以及可能有助于故障排除的其他消息。

- **日志文件大小限制：**（必填）输入每个日志文件的大小。最大值为 600 MB。
- **最大日志文件数：**（必填）输入要添加用于日志收集的文件数。最大值为 5。
- **发送日志文件** – 将日志文件发送到注册的电子邮件 ID。
- **启动新日志文件** – 选择此选项时，将创建一个新的日志文件。
- **收集日志文件** – 单击可创建包含应用程序所有日志文件的 zip 文件。此 zip 文件将保存到客户端的桌面。
- **打开日志文件** – 选择此选项时，将打开最新的 `csa_nssslvpn*.txt` 文件。

改进的 Citrix Secure Access 诊断适用于 Windows 客户端

从适用于 Windows 的 Citrix Secure Access 客户端版本 24.6.1.18 开始，Citrix Secure Access 诊断功能得到增强，以包含其他字段，用于排查 TCP/UDP 应用程序的访问问题。

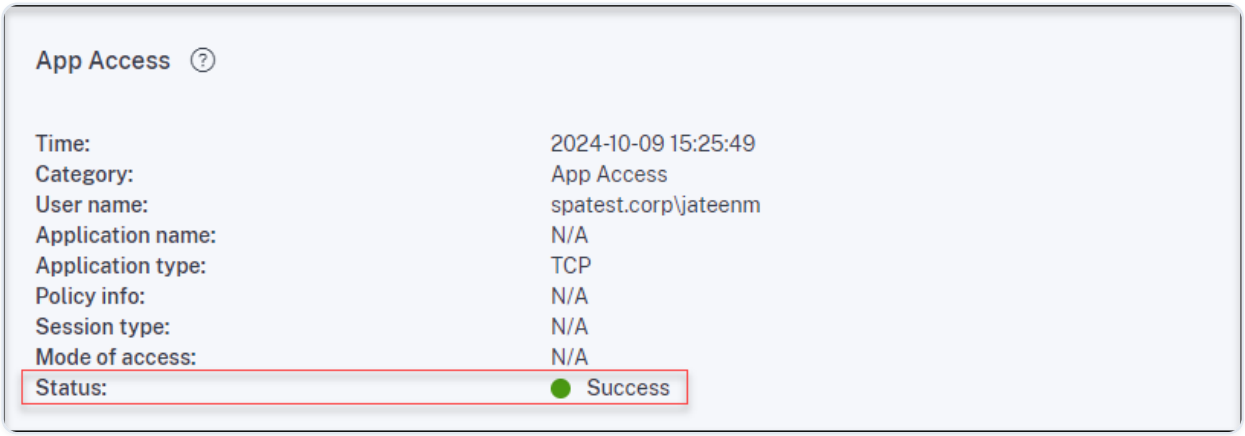
- **描述：** 当从适用于 Windows 的 Citrix Secure Access 客户端访问 TCP/UDP 应用程序失败时，目标 IP、源端口和目标端口包含在 **App Access** 日志的“**描述**”字段中。



- **DNS 故障：** 基于 TCP 的 DNS 故障和基于 UDP 的 DNS 故障在 **App Access** 日志中明确报告。

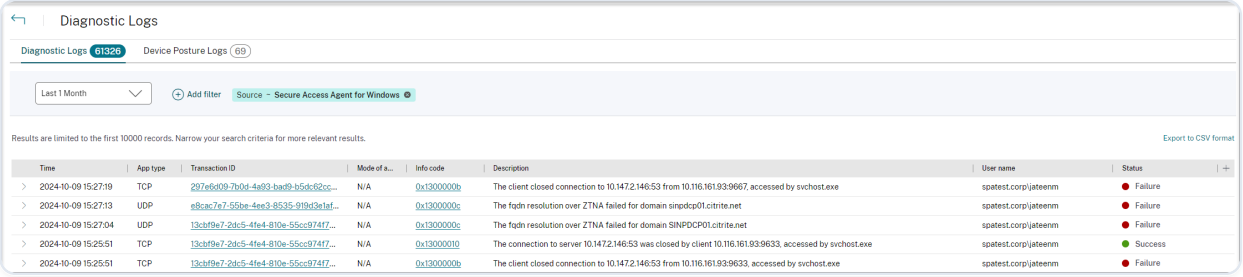


- **应用程序名称详细信息：** 适用于 Windows 的 Citrix Secure Access 客户端中的 **App Access** 日志包含应用程序名称以及访问失败或成功状态。此字段允许管理员了解哪些应用程序正在访问 TCP/UDP 工作流，以及它们是否正在使用不同的端口组合。



除了 **App Access** 日志之外，CAS (Citrix Access Security) **诊断日志** 也通过以下方式得到增强：

- **CAS 诊断日志概述：** CAS **诊断日志** 概述包括对适用于 Windows 的 Citrix Secure Access 客户端中失败内容和失败原因的描述。
- **WPAD DNS 故障：** 默认情况下，Windows 版 Citrix Secure Access 客户端的 **WPAD DNS** 故障会在 CAS **诊断日志**中报告。管理员必须在 Windows 版 Citrix Secure Access 客户端中配置 `DisableWpadDnsCasReporting` 注册表，以防止 CAS **诊断日志**因 WPAD DNS 故障而过载。



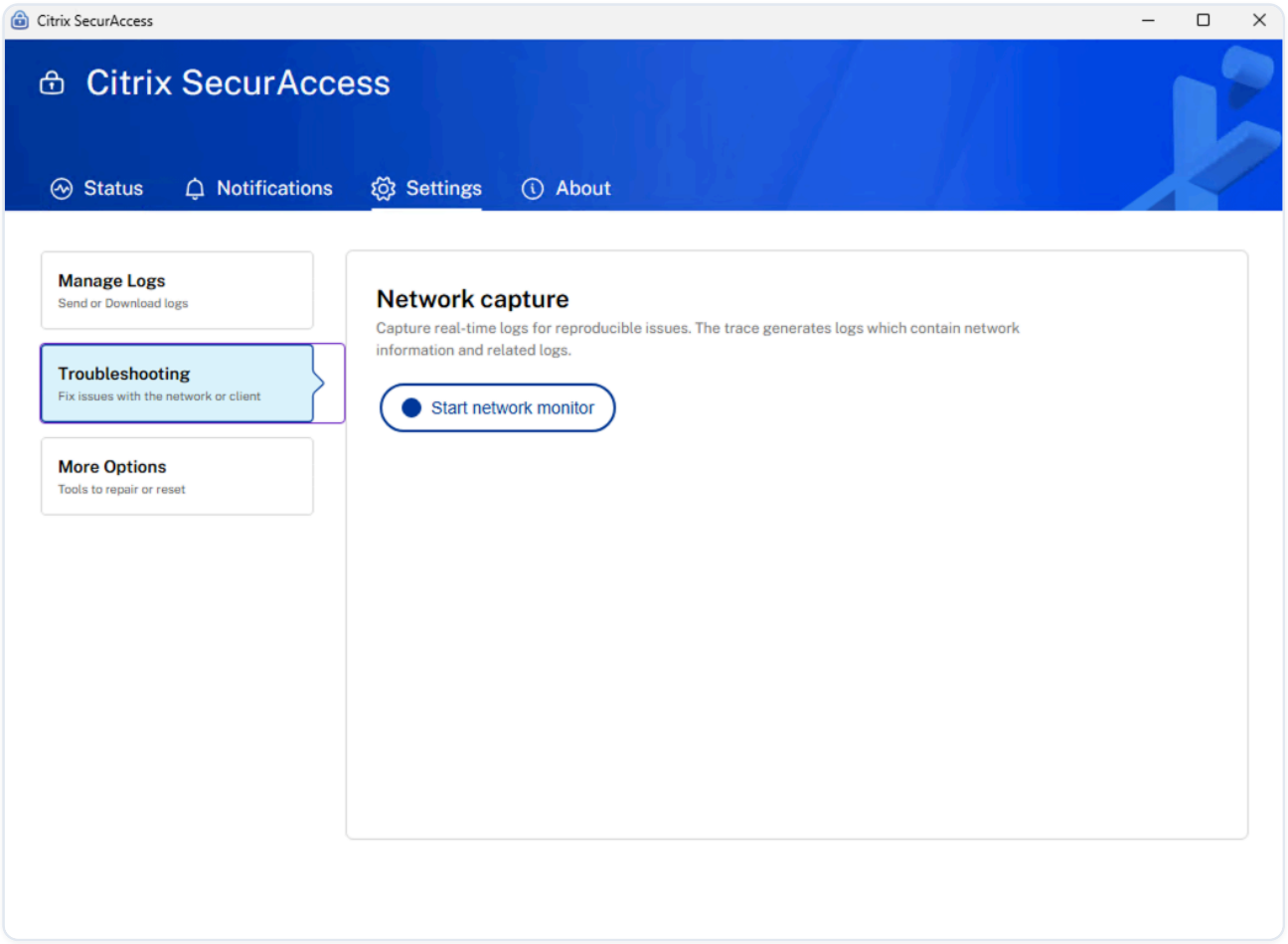
用于 Citrix Secure Access 的集成式数据包捕获工具，用于连接故障排除

适用于 Windows 的 Citrix Secure Access VPN 客户端包含一个集成的网络数据包捕获工具，可帮助排查连接问题。捕获的文件会自动保存到 Citrix Secure Access 安装文件夹下的 `logs\captures\` 目录中。自动文件轮换有助于限制磁盘使用。当为 Citrix 支持收集日志时，数据包捕获文件也会自动包含在诊断日志包中。

> **注意：**
>
> - 网络数据包捕获工具仅在新版 WebModule UI 中可用。
> - Citrix Secure Access 安装程序包含数据包捕获实用程序和所需的 WinDivert 内核驱动程序依赖项。无需单独安装。

启动数据包捕获

1. 打开 **Citrix Secure Access** 应用程序。
2. 单击“**设置**”选项卡。
3. 在左侧面板中，选择“**故障排除**”。
4. 在右侧窗格中，转到“**网络捕获**”部分。
5. 单击“**启动网络监视器**”以开始捕获网络流量。



捕获开始后，状态将变为“**正在捕获...**”，并且“**停止**”按钮将变为可用。

停止数据包捕获

1. 在 Citrix Secure Access 应用程序中，导航到“**设置**”>“**故障排除**”。
2. 当捕获处于活动状态时，**网络捕获**面板会显示**正在捕获...**，并带有红色指示器。
3. 单击**停止**按钮以结束捕获。

停止数据包捕获(/en-us/citrix-secure-access/media/stop-a-packet-capture.png)

捕获停止后：下载或重新启动

捕获停止后，状态将变为**捕获完成**（绿色指示器）。

然后，您可以选择以下选项之一：

- **下载**：将捕获文件保存到本地计算机。
- **重新启动**：立即开始新的数据包捕获会话。

信息横幅会显示捕获文件的完整保存路径。例如：

`C:\Program Files\Citrix\Secure Access Client\logs\captures\csatrace_20260407_092046.pcap`

可以在 Wireshark 等数据包分析工具中打开 `.pcap` 文件以进行进一步调查，或与 Citrix 支持部门共享。

Citrix Secure Access™ 自动登录到已加入 Windows Azure AD 的计算机

自动登录到 NetScaler Gateway 虚拟服务器

Citrix Secure Access 客户端可以使用 PRT 对 NetScaler Gateway 虚拟服务器执行 SSO，并自动将用户连接到 `AlwaysOnURL` 注册表中提到的 NetScaler Gateway URL。有关详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

管理员必须配置以下内容才能使用 PRT 启用对 NetScaler Gateway 虚拟服务器的 SSO：

- 必须将 Microsoft Entra ID 配置为 SAML IdP。
- 必须将 NetScaler Gateway 配置为 SAML SP。
- Citrix Secure Access 客户端必须配置为“始终开启”或“始终开启服务”模式。

要配置 Citrix Secure Access 客户端以使用 PRT 执行 SSO，您必须完成以下步骤：

1. 将 Windows 计算机加入 Azure Entra ID。管理员必须访问以下 URL 并加入 Windows 计算机：

   URL。
2. 将 NetScaler Gateway 配置为 SAML SP，将 Microsoft Entra ID 配置为 SAML IdP。有关详细信息，请参阅 将 Microsoft Entra ID 配置为 SAML IdP，将 NetScaler 配置为 SAML SP。
3. 将 Citrix Secure Access 客户端配置为“始终开启”和“始终开启服务”模式。有关详细信息，请参阅 Windows 登录前的始终开启 VPN（正式名称为始终开启服务） 和 始终开启。

用户必须首次使用其凭据登录。在随后的系统重启期间，Citrix Secure Access 客户端会使用 PRT 自动将用户连接到 NetScaler Gateway 虚拟服务器。

自动登录到 SecurAccess ZTNA 服务

Citrix Secure Access 客户端可以使用 PRT 对 SecurAccess ZTNA 服务执行 SSO。当客户端配置为“始终开启”或“始终开启服务”模式时，此功能有效。

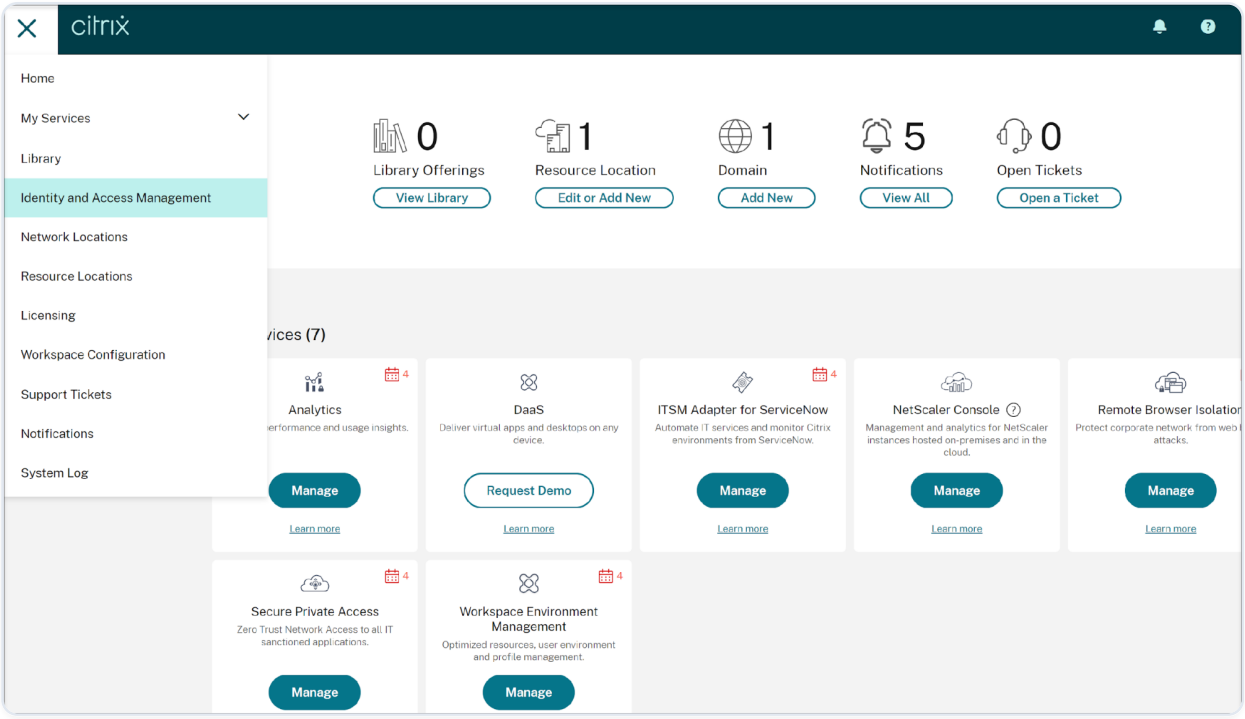
要配置 Citrix Secure Access 客户端以使用 PRT 执行 SSO，您必须完成以下步骤：

1. 将 Windows 计算机加入 Azure Entra ID。管理员必须访问以下 URL 并加入 Windows 计算机：

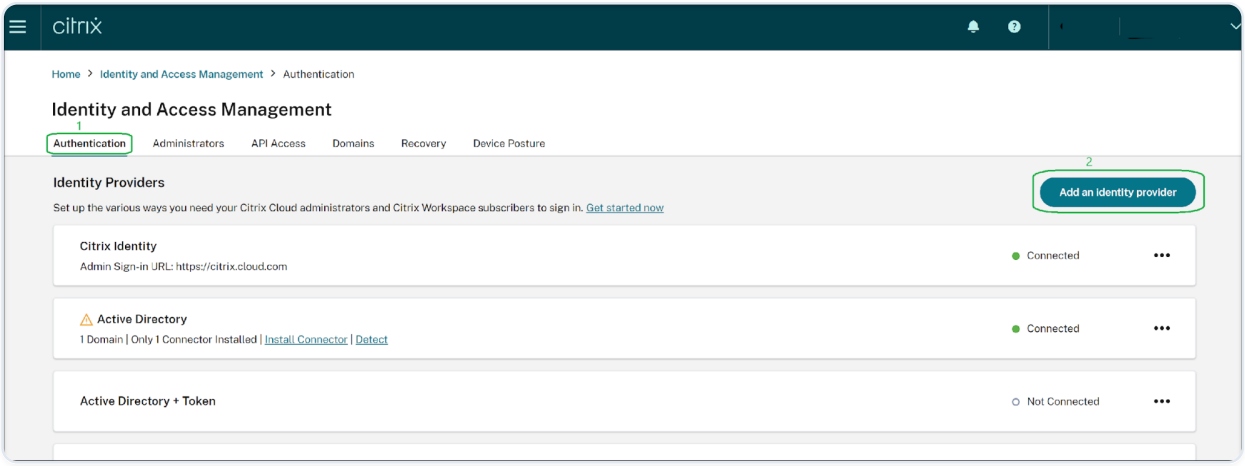
   URL。

2. 登录到 Citrix Cloud™ 帐户。

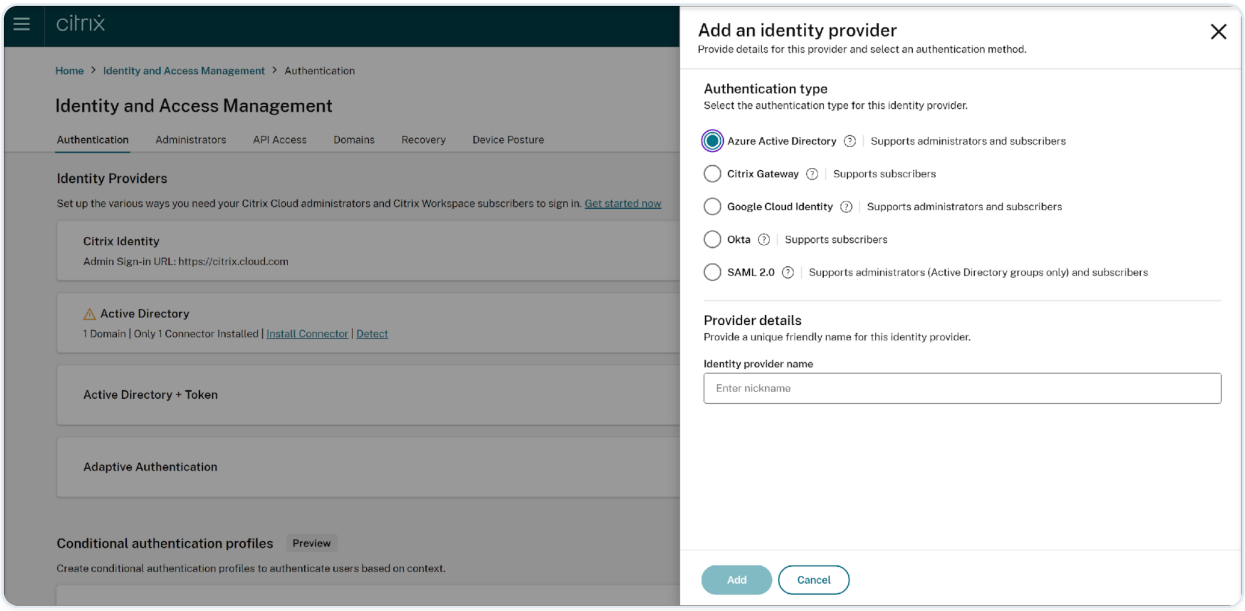
3. 单击汉堡图标并导航到 **身份和访问管理**。



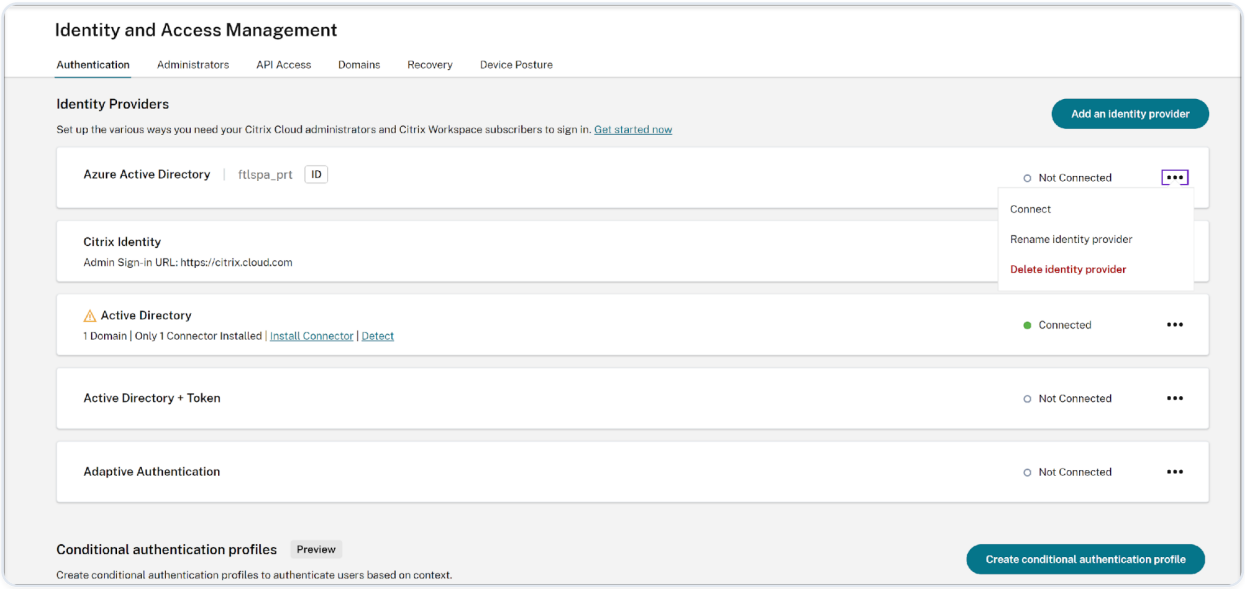
4. 在 **身份和访问管理** 屏幕上，单击 **身份验证** 选项卡，然后单击 **添加身份提供程序** 按钮。



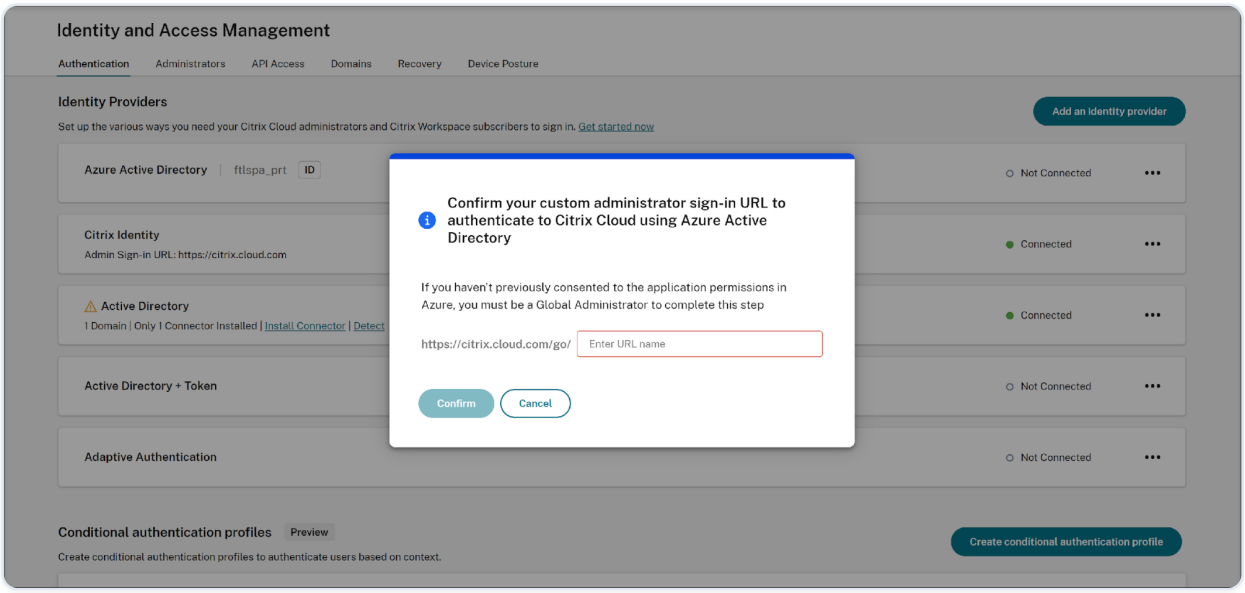
5. 选择身份验证类型为 **Azure Active Directory**，在 **身份提供程序名称** 文本框中为身份提供程序提供一个名称，然后单击 **添加** 按钮。



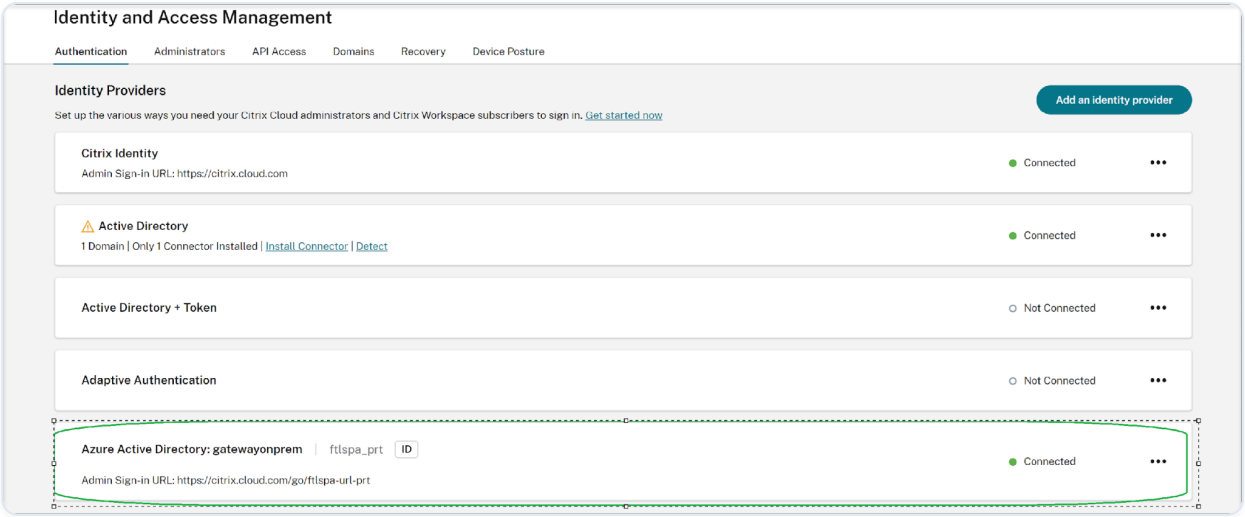
6. **Azure Active Directory** 显示在身份提供程序列表中，如下所示。单击 **连接**。



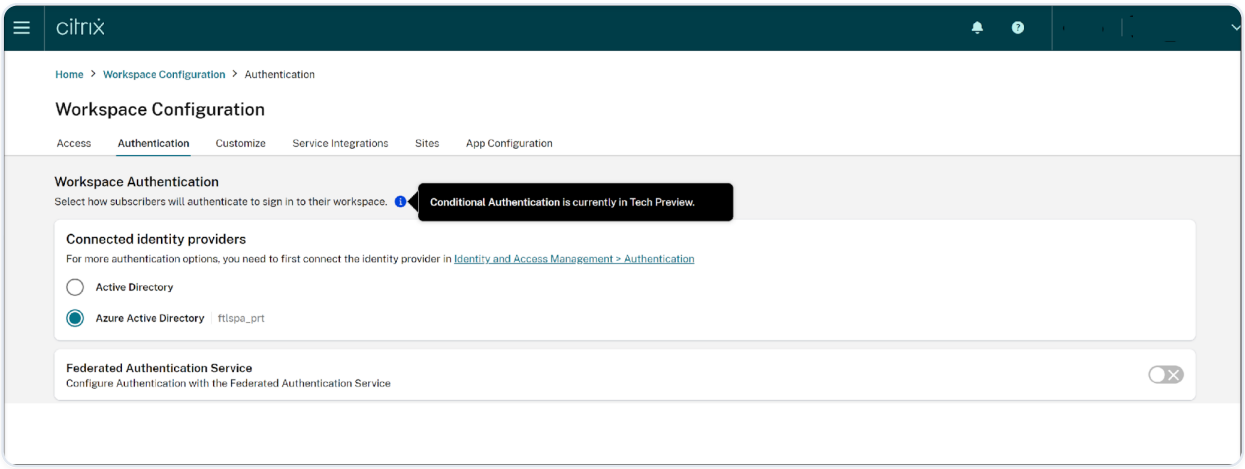
7. 在连接屏幕上，输入 URL 名称，然后单击 **确认** 按钮。



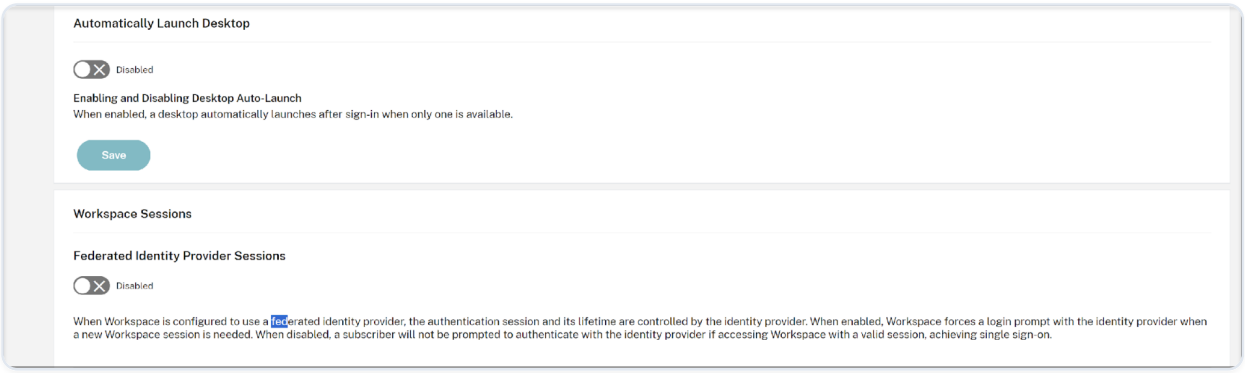
8. 管理员将被重定向到 Microsoft 登录页面。使用 Azure Entra ID 用户帐户登录。登录成功后，Azure Active Directory 将显示为已连接。



9. 返回到**工作区配置**，点击**身份验证**选项卡，然后选择**Azure Active Directory**。



10. 导航到**工作区配置** -> **自定义** -> **首选项**，并取消选中**联合身份提供程序会话**下方的复选框，以禁用联合身份验证服务。



用户必须首次使用其凭据登录。在随后的系统重启期间，Citrix Secure Access 客户端会自动使用 PRT 将用户连接到 SecurAccess ZTNA。

适用于 Windows Citrix Secure Access 的 Microsoft Edge WebView 支持功能

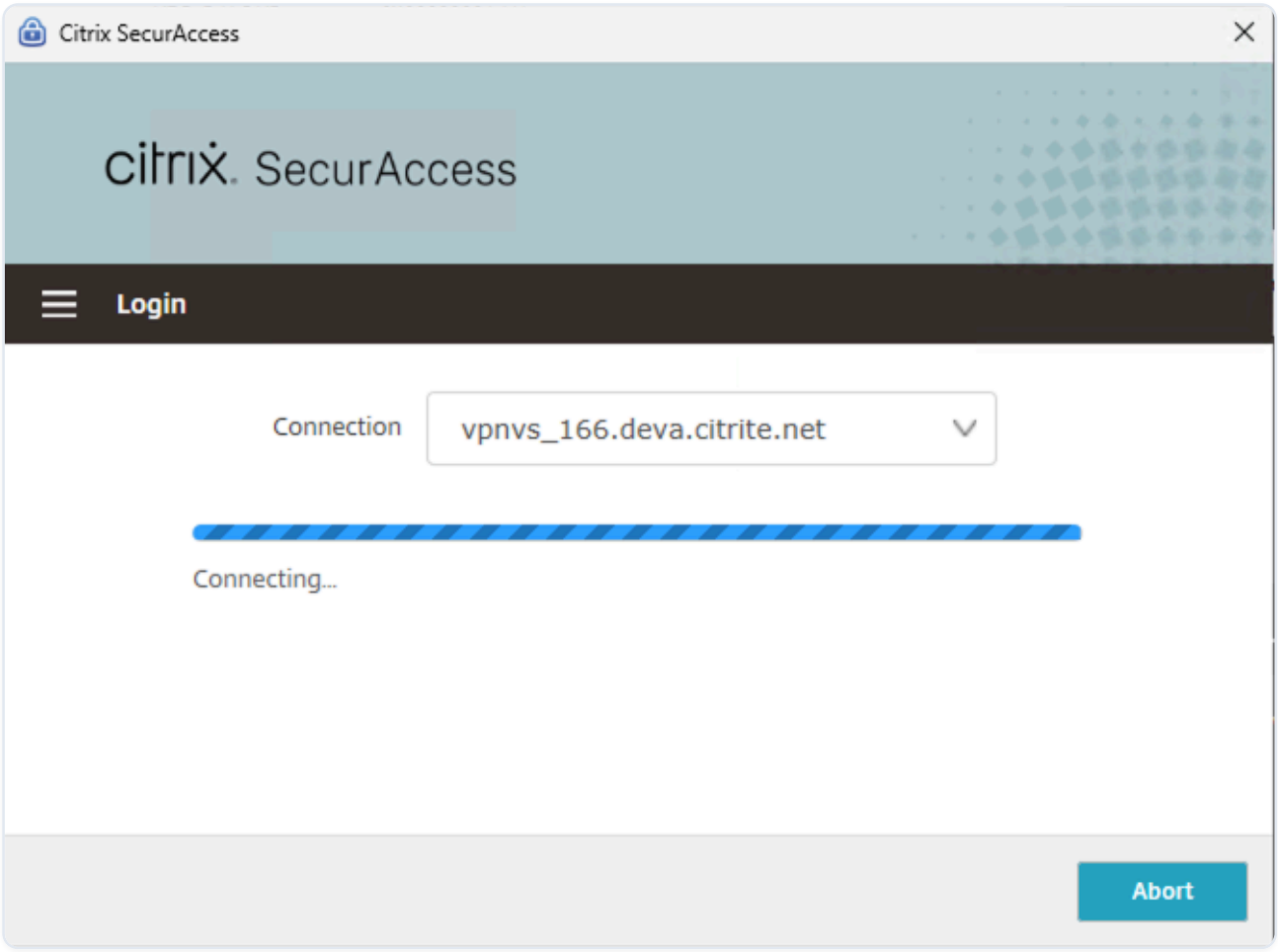
重要提示：

- 从适用于 Windows 的 Citrix Secure Access 客户端版本 24.11.1.17 开始，Microsoft Edge WebView 默认启用。
- 从 January 29, 2025 起，Citrix 将更改在适用于 Windows 的 Citrix Secure Access 客户端中启用预览功能的方法。为确保适用于 Windows 的 Citrix Secure Access 客户端中预览功能（功能标志下的功能）的最佳性能，您必须启用流向 `features.netscalergateway.net` 的流量，并将客户端升级到版本 24.8.1.19 或更高版本。有关更多信息，请参阅适用于 Windows 的 Citrix Secure Access 客户端的功能管理。

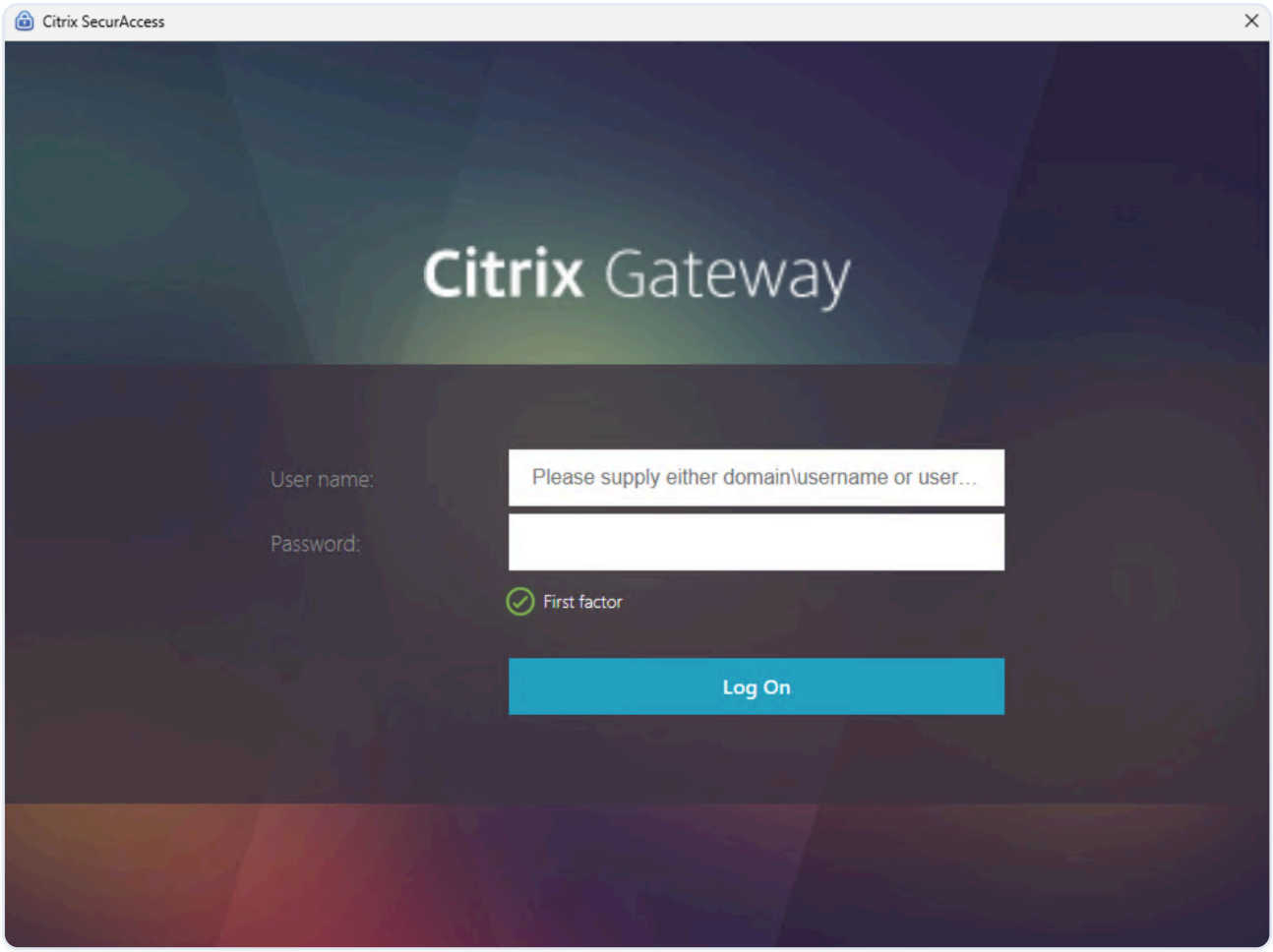
Microsoft Edge WebView 现在是 Microsoft 推荐的 WebView，因为 Internet Explorer WebView 已弃用。我们建议您使用 Citrix Secure Access 客户端 23.8.1.5 或更高版本来利用 Microsoft Edge WebView 的功能。

最终用户更改

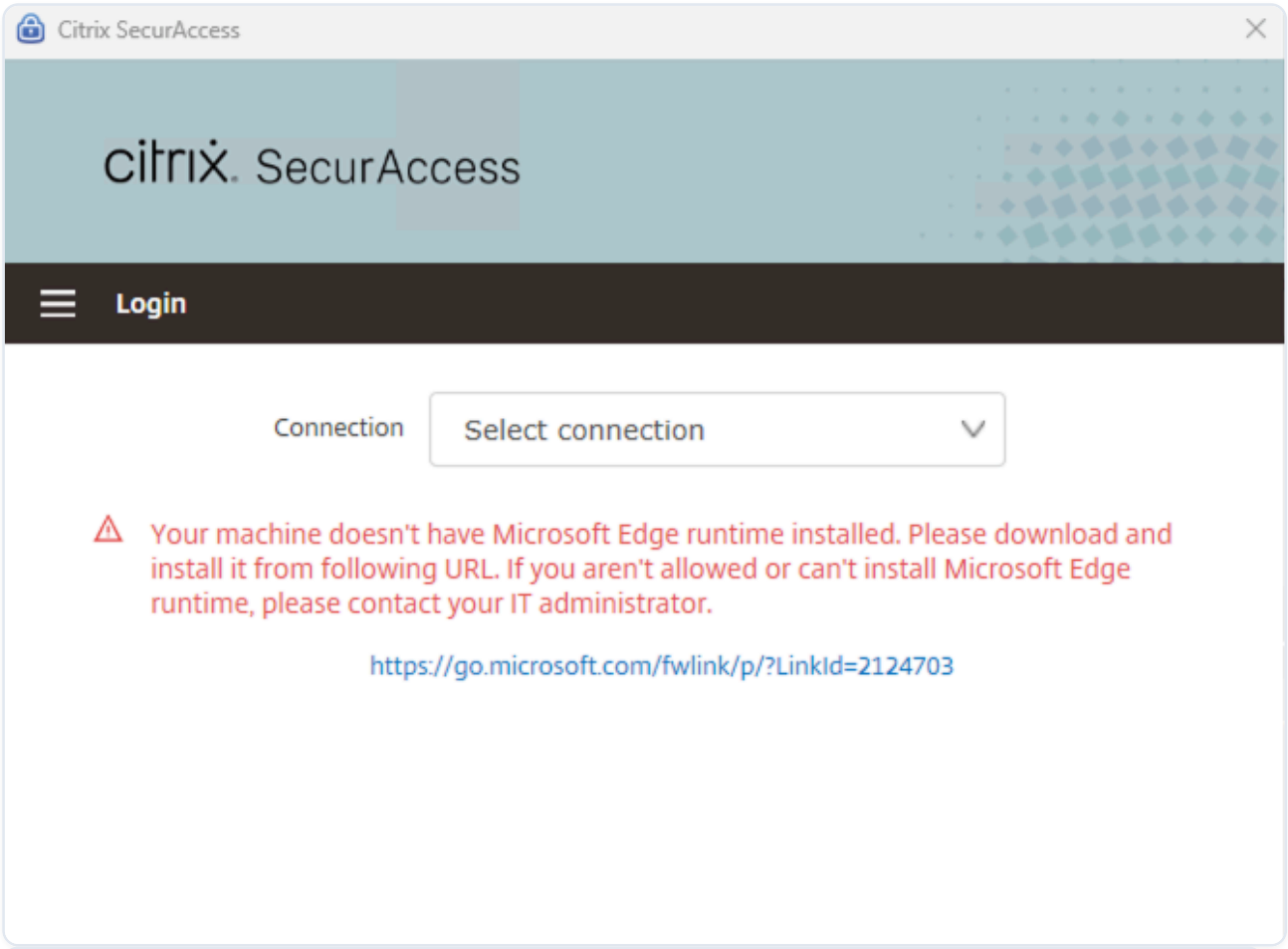
Citrix Secure Access 客户端 UI 的身份验证屏幕显示如下。

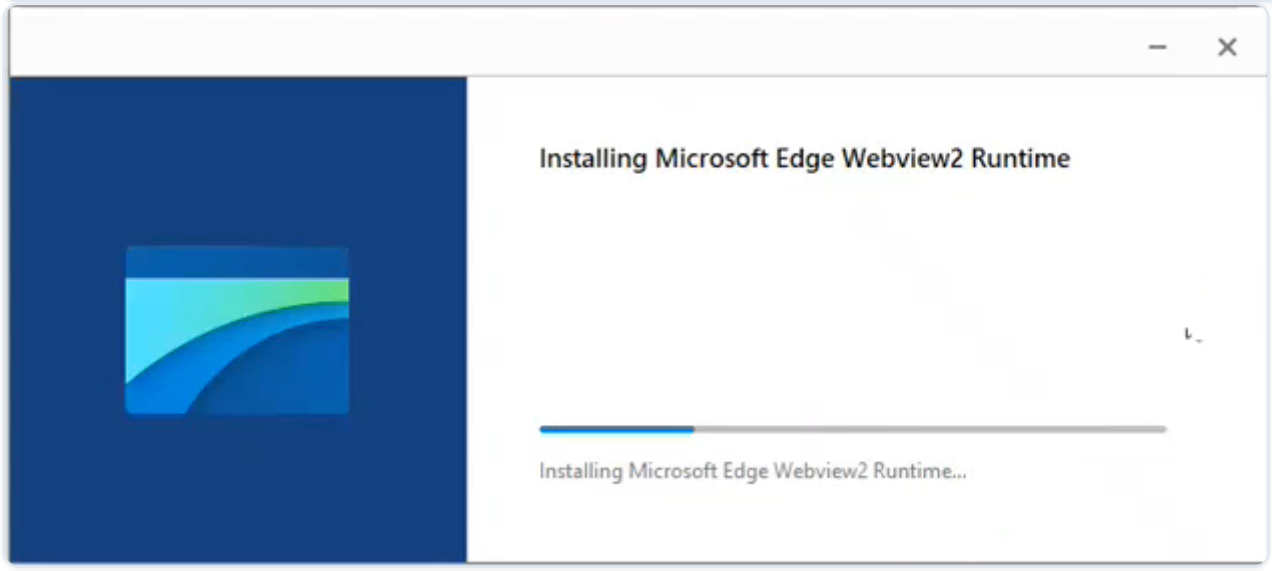


最终用户选择 URL 后，Citrix Secure Access 客户端会打开一个新窗口，提示他们使用凭据登录到 NetScaler Gateway。



如果 Windows 客户端计算机未安装 Microsoft Edge WebView 运行时，Citrix Secure Access 客户端 UI 上会提供一个链接，供最终用户下载并安装 Microsoft Edge WebView 运行时。最终用户在连接到 VPN 时可以无缝下载并安装 Edge WebView 运行时，并且在此过程中身份验证不会中断。





注意：

- Microsoft Edge WebView 功能不影响任何管理员特定的配置。

- 我们建议您在使用 Citrix Secure Access 上的 Edge WebView 时启用 HttpOnly cookie 功能。这在 nfactor 流程中将 EPA 用作因素时，可以缩短 NetScaler Gateway 的登录持续时间。

故障排除

- 如果此功能出现任何问题，请联系 Citrix 支持。
- 您可以通过 mailto:citrixgatewaybetafeedback@cloud.com 提交有关 Edge WebView 功能的反馈。

在 NetScaler Gateway 上升级适用于 Windows 的 Citrix Secure Access 客户端和 EPA 客户端

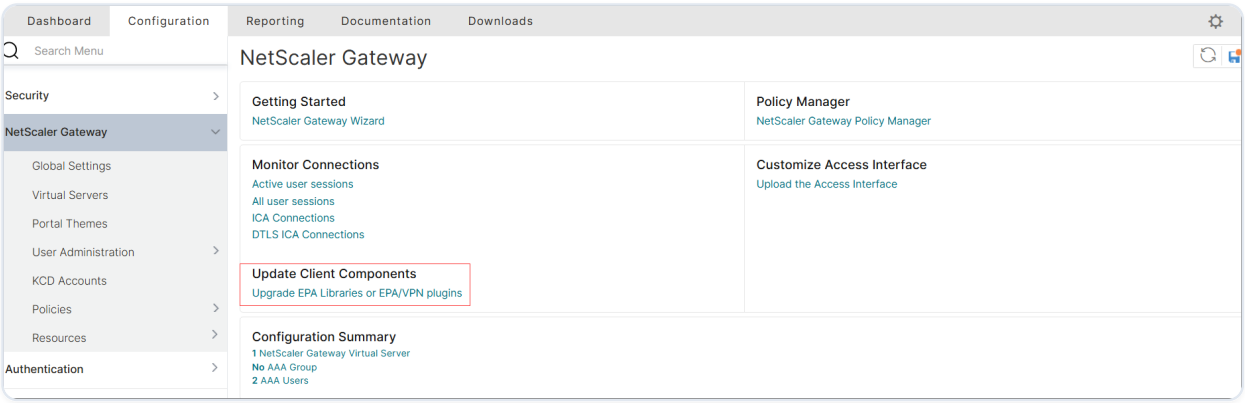
重要提示：

- 您可以在 NetScaler Gateway 上升级适用于 Windows 的 Citrix Secure Access 客户端和 EPA 客户端，以确保您的设备检查最新的防火墙和防病毒软件。
- 升级适用于 Windows 的 Citrix Secure Access 客户端和 EPA 客户端，无需仅仅为了客户端更新而升级 NetScaler Gateway。
- 从版本 13.0-76.31 及更高版本开始，可以通过 NetScaler Gateway UI 方便地升级适用于 Windows 的 Citrix Secure Access 客户端和 EPA 客户端。
- 在高可用性设置中，必须在主节点和辅助节点上都升级适用于 Windows 的 Citrix Secure Access™ 客户端和 EPA 客户端。
- 升级前，请确保已将升级文件（tar.zip 格式）上传到本地计算机或 NetScaler Gateway。
- 即使您不使用 EPA，我们也建议您同时更新 VPN 和 EPA 插件二进制文件，以防您以后选择使用 EPA 功能。

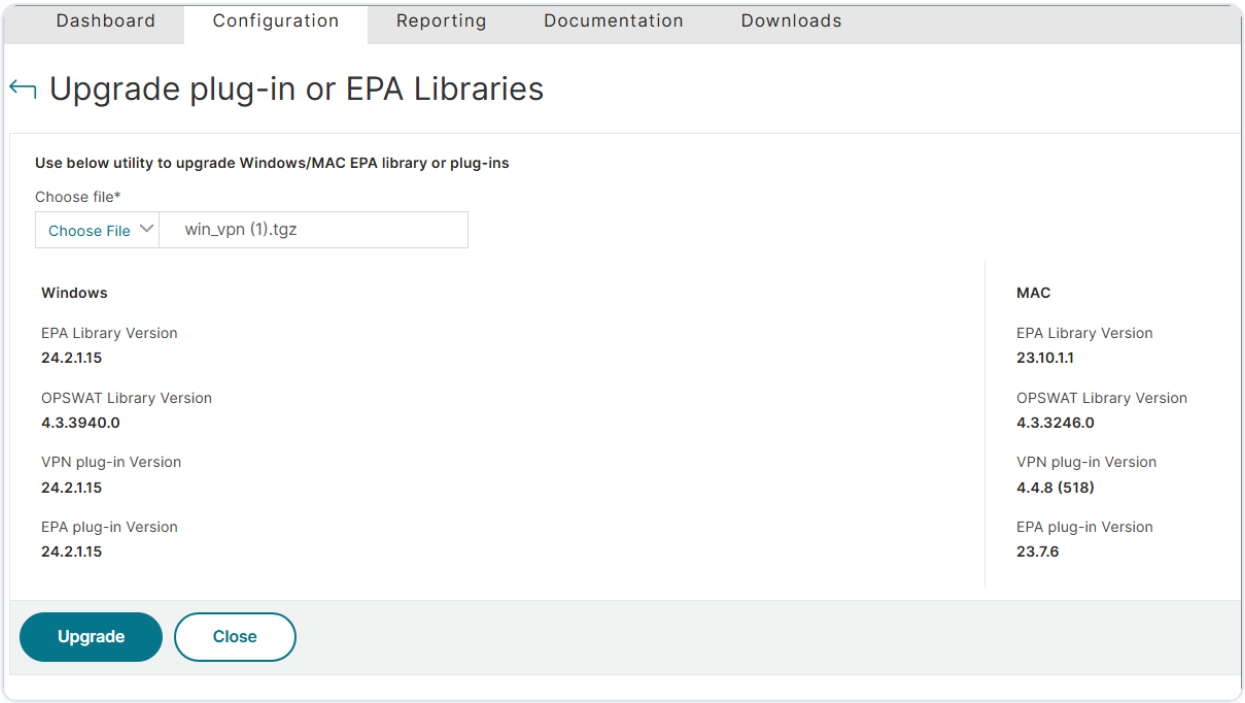
使用 NetScaler Gateway GUI 升级客户端

在 NetScaler Gateway GUI 上执行以下步骤来升级客户端：

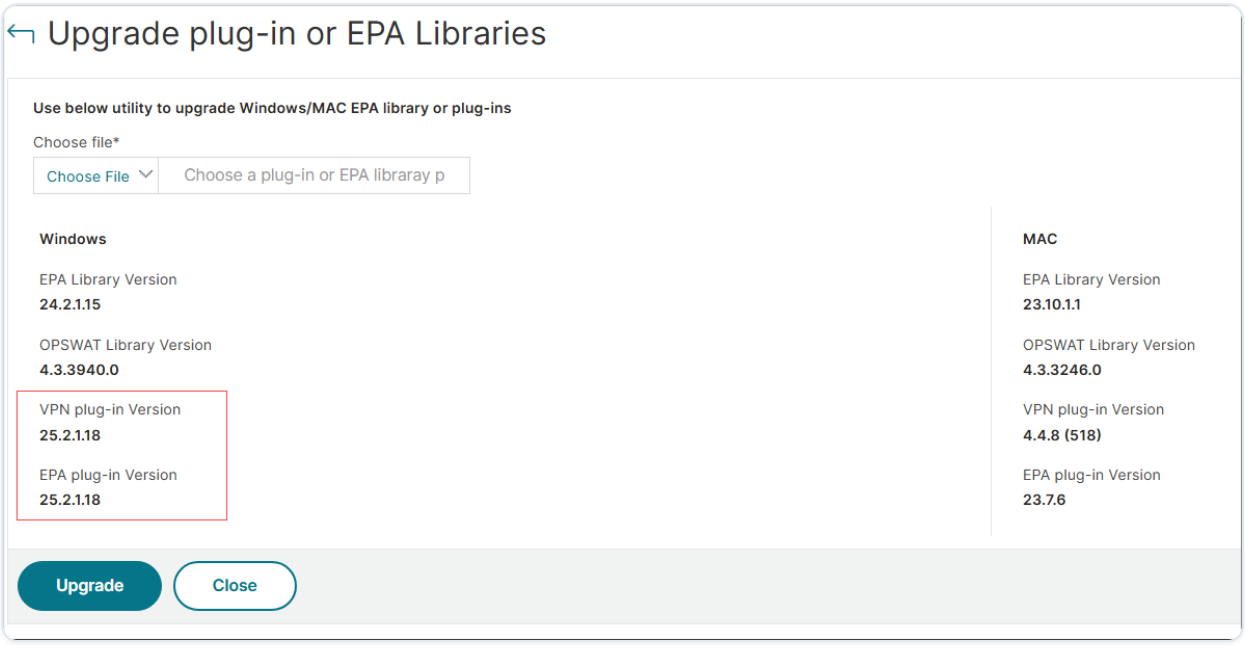
1. 导航到 **NetScaler Gateway** > **更新客户端组件**。
2. 在 **更新客户端组件** 下，单击 **升级 EPA/客户端组件** 链接。



3. 在 **选择文件** 中，选择升级文件的来源（本地或 NetScaler Gateway）。
4. 导航到文件以选择文件，然后单击 **升级**。



5. 升级完成后，单击**升级 EPA/客户端组件**链接并验证升级是否成功。



使用 NetScaler® 文件系统升级客户端

执行以下步骤以升级客户端：

1. 下载适用于 Windows 的最新版本 Citrix Secure Access 客户端和 EPA 客户端。
2. 使用安全文件传输协议 (SFTP) 或安全复制协议 (SCP) 应用程序（例如 winscp）打开 NetScaler 文件系统。
3. 要升级 Citrix Secure Access 客户端：

   a. 选择文件 `/var/netscaler/gui/vpns/scripts/vista`。

   b. 将 `AGEE_setup.exe` 文件替换为下载的客户端文件。

   c. 转到 `/netscaler/ns_gui/vpn/`。

   d. 打开 `pluginlist.xml` 文件。

   e. 将当前版本替换为最新版本，并将插件类型设置为“WIN-VPN”。请参阅下图以供参考：

```
![Set plug-in type](https://docs.citrix.com/content/dam/citrix/us/en/
citrix-secure-access/media/upgrade-win-vpn.png)



>**Note:**

>
```

> >Ensure to set the upgrade type to “Always” on the XML file.

f. 复制更新的 XML 文件并将其替换到 `/var/netscaler/gui/vpn/ directory` 中。

4. 要升级 EPA 客户端：

   a. 导航到 `/var/netscaler/gui/epa/scripts/win/`。

   b. 将 `nsepa_setup.exe` 文件替换为下载的客户端文件。

   c. 转到 `/netscaler/ns_gui/vpn/`。

   d. 打开 `pluginlist.xml` 文件。

   e. 将当前版本替换为最新版本，并根据您的要求将插件类型设置为“WIN-EPA”或“WIN-EPA64”。请参考下图：

> ![Set plug-in type for EPA](https://docs.citrix.com/content/dam/citrix/us/en/citrix-secure-access/media/upgrade-win-epa.png)

   f. 复制更新的 XML 文件，并将其替换到 `/var/netscaler/gui/vpn/` 目录中。

非配置域的反向拆分隧道

从适用于 Windows 版本 25.5.1.15 的 Citrix Secure Access 客户端开始，启用反向拆分隧道时，非配置域的 DNS 解析将远程执行，无论 **Split DNS** 设置如何。以前，非配置域的 DNS 解析在反向拆分隧道下按以下方式工作：

- 当 **Split DNS** 设置为 **BOTH** 时，非配置域将同时在本地和远程解析，导致冗余和歧义。
- 当 **Split DNS** 设置为 **LOCAL** 时，非配置域将在本地解析，增加了 DNS 泄漏和意外路由的风险。

DNS 解析矩阵

下表总结了启用反向拆分隧道时，不同 **Split DNS** 设置下的 DNS 解析行为。

SPLIT DNS 设置	主机名已配置	DNS 后缀已配置	域未配置
本地	本地	远程	远程
远程	远程	远程	远程

SPLIT DNS 设置	主机名已配置	DNS 后缀已配置	域未配置
两者	两者	远程	远程

示例：

以下是 Citrix Secure Access™ 客户端中的示例分流隧道配置：

```
{
    "Version": 1,
    "Username": "xyz",
    "Tunnel": {
        "Split-Tunnel": "ON",
        "Split-DNS": "BOTH",
        "Tunnel-Rules": [
            {
                "Protocol": "ANY",
                "Type": "Hostname",
                "Hostnames": [
                    "login.microsoftonline.com"
                ]
            },
            {
                "Protocol": "ANY",
                "Type": "Hostname",
                "Hostnames": [
```

```
                "*.spatest.corp"
            ]
        },
        {
            "Protocol": "ANY",
            "Type": "IPV4",
            "Start": "10.102.76.14",
            "Stop": "10.102.76.14"
        }
    ],
    "FQDN-SpoofedIP": {
        "IPv4": "172.16.0.0",
        "IPv4-Prefix": 16
    },
    "DNS-Truncate-Fix": true,
    "DNS-Suffix-List": [
        "cgwsanity.net"
    ]
},
"AlwaysON": {
    "Network-Access": true,
    "Client-Control": true
```

```
    },
    "EPA": {
    },
    "Proxy": {
    },
    "Client-Config": {
        "Local-Lan-Access": true,
        "Restart-NLA": true,
        "Allow-Logging": true,
        "Forced-Timeout": 0,
        "Forced-Timeout-Warning": 0,
        "Client-Idle-Timeout": 0
    },
    "Client-Cleanup": {
    },
    "Supported-Mux-Versions": "1,2"
}
```

对于上述分流隧道配置，DNS 解析按以下表格所示执行：

实体	配置	分流 DNS 设置	DNS 解析
`login.microsoftonline.com`	主机名 `login.microsoftonline.com` 配置在 `Tunnel-Rules`	两者	本地+远程
		本地	本地

实体	配置	分流 DNS 设置	DNS 解析
`*.spatest.corp`	主机名 `*.spatest.corp` 配置在 `Tunnel-Rules`	两者	本地+远程
		本地	本地
`dc.cgwsanity.net`	DNS 后缀 `cgwsanity.net` 已在 `Tunnel-Rules` 中配置	两者	远程
		本地	远程
`citrite.net`	域名或主机名未在 `Tunnel-Rules` 中配置	两者	远程
		本地	远程
`sf1.spatest.corp`	域或主机名未在 `Tunnel-Rules` 中配置	两者	远程
		本地	远程

恢复旧版拆分 DNS 行为

要恢复旧版拆分 DNS 行为（即在启用反向拆分隧道时，未配置的域在本地和远程均可解析），请配置以下注册表：

注册表名称： DisableReverseTunChangeSplitDnsBehavior

注册表类型： REG_DWORD

注册表值： 1

注册表路径： Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client

> **注意：**
>
> 仅当旧版行为对于兼容性或操作原因至关重要时，才使用此注册表。

针对 Windows 版 Citrix Secure Access 客户端故障进行故障排除

Citrix Secure Access 客户端 24.11.1.17 及更高版本中的自动登录失败

当 Microsoft Edge WebView 启用时，Citrix Secure Access 客户端中的经典身份验证自动登录失败。以前，24.11.1.17 之前的版本使用 Internet Explorer WebView 支持经典和高级身份验证的自动登录。

由于 Microsoft 弃用 Internet Explorer，Citrix Secure Access 客户端 24.11.1.17 及更高版本默认使用 Microsoft Edge WebView，它不支持经典身份验证。我们建议迁移到高级 (nFactor) 身份验证。如果您必须继续使用经典身份验证，请禁用 Microsoft Edge WebView，直到迁移完成。

下表总结了不同 Citrix Secure Access 客户端版本中不同身份验证模式和 WebView 组件的兼容性矩阵：

CITRIX SECURE ACCESS 客户端版本	默认 WEBVIEW	身份验证模式	自动登录支持	需要变通办法
24.11.1.17 及更低版本	Internet Explorer 网页视图	经典	支持	不需要
24.11.1.17 及以下	Internet Explorer 网页视图	高级 (nFactor)	支持	不需要
24.11.1.17 及以上	Microsoft Edge 网页视图	高级 (nFactor)	支持	不需要
24.11.1.17 及以上	Microsoft Edge 网页视图	经典	不支持	• 选项 1：联系 Citrix 支持 • 选项 2：配置注册表

解决自动登录失败

要在 Citrix Secure Access 客户端版本 24.11.1.17 及更高版本中启用经典身份验证的自动登录，必须使用以下方法之一将 Citrix Secure Access 客户端中的默认 WebView 恢复为 Internet Explorer WebView。

选项 1：联系 Citrix 支持

联系 Citrix 支持 以禁用客户环境的 Microsoft Edge WebView。

选项 2：配置注册表

要将默认 WebView 恢复为 Internet Explorer WebView，请应用以下注册表配置：

注册表名称： EnableEdgeWebView

注册表路径： HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client

注册表类型： REG_DWORD

注册表值： 0

第三方软件导致的登录失败

如果第三方软件从 `C:\\Windows` 或 `C:\\Program Files` 以外的目录执行动态链接库 (DLL) 注入，您可能会在 Citrix Secure Access 客户端中遇到登录失败。

要解决登录失败问题，请验证 `C:\Program Files\Citrix\Secure Access Client\logs\csa_nsverctl.txt` 处的日志文件。日志中出现“No External Signature matched”表示问题出在第三方软件。以下是失败日志的示例：

```
2025-05-27 14:15:24.398 | 17020 | DEBUG | D | NONE | Signer cert name to verify file: = ABC signername INC |

2025-05-27 14:15:24.398 | 17020 | ERROR | S | NONE | Verify file: No External Signature matched |
```

解决登录失败问题

由第三方软件导致的登录失败可以通过以下方法之一解决：

选项 1：排除 nsload.exe 进程

配置第三方软件以排除 nsload.exe 进程。此配置可确保与从 `C:\Windows` 或 `C:\Program Files` 以外的目录执行 DLL 注入的第三方软件实现最佳兼容性。

选项 2：配置注册表

从适用于 Windows 的 Citrix Secure Access 客户端版本 25.2.1.18 开始，如果需要 DLL 注入，您可以应用以下注册表配置：

注册表名称： ExternalTrustedSigners

注册表路径： HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client

注册表类型： REG_MULTI_SZ

注册表值： 正在注入的 DLL 的签名者名称

您可以从 `C:\Program Files\Citrix\Secure Access Client\logs\csa_nsverctl.txt` 处的日志文件中获取签名者名称。在以下示例日志中，“ABC signername INC”是要在 `ExternalTrustedSigners` 注册表中配置的签名者名称。

```
2025-05-27 14:15:24.398 | 17020 |   DEBUG | D | NONE | Signer cert name to
verify file: = ABC signername INC  |

2025-05-27 14:15:24.398 | 17020 |   ERROR | S | NONE | Verify file: No
External Signature matched |
```

适用于 macOS/iOS 的 Citrix Secure Access

旧版 VPN 客户端是使用 Apple 已弃用的私有 VPN API 构建的。适用于 macOS 和 iOS 的 Citrix Secure Access 中的 VPN 支持是使用 Apple 的公共网络扩展框架从头重写的。

注意

- 适用于 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新我们的文档和 UI 屏幕截图以反映此名称更改。
- 适用于 macOS 的 Citrix Secure Access 支持 12.x (Monterey)、13.x (Ventura)、14.x (Sonoma) 和 15.x (Sequoia)。它支持配备 Intel 芯片和 Apple 芯片的设备。
- 硬件无法升级到前面提到的版本（macOS 10.15 和 macOS 11.0）的用户可以在 App Store 上获取最后一个兼容版本，但旧版本将不再获得更新。
- 如果 macOS 用户在 App Store 应用和 TestFlight 预览版本之间切换，反之亦然，则用户必须通过执行以下步骤重新创建连接配置文件：

  a. 单击汉堡菜单，然后单击**配置**。

  b. 从列表中删除配置文件，然后再次添加相同的配置文件。

适用于 macOS/iOS 的 Citrix Secure Access 客户端的主要功能

- **密码令牌：** 密码令牌是一个 6 位代码，它是 VIP、OKTA 等辅助密码服务的替代方案。此代码使用基于时间的一次性密码 (T-OTP) 协议生成 OTP 代码，类似于 Google Authenticator 和 Microsoft Authenticator 等服务。在对给定 Active Directory 用户进行 NetScaler Gateway 身份验证期间，系统会提示用户输入两个密码。第二个因素是一个不断变化的六位代码，用户从 Google 或 Microsoft Authenticator 等注册的第三方服务复制到桌面浏览器中。用户必须首先在 NetScaler 设备上注册 T-OTP。有关注册步骤，请参阅 CTX228454。在应用程序上，用户可以通过扫描 NetScaler 上生成的 QR 码或手动输入 TOTP 密钥来添加 OTP 功能。添加后，OTP 令牌会显示在用户界面上的“密码令牌”部分。

为了改善体验，添加 OTP 会自动提示用户创建 VPN 配置文件。用户可以利用此 VPN 配置文件直接从其 iOS 设备连接到 VPN。

适用于 macOS/iOS 的 Citrix Secure Access 客户端可用于在注册原生 OTP 支持时扫描 QR 码。NetScaler Gateway 推送通知功能仅适用于适用于 macOS/iOS 的 Citrix Secure Access 用户。

- **推送通知：** NetScaler Gateway 会向您注册的移动设备发送推送通知，以简化双因素身份验证体验。您无需启动适用于 macOS/iOS 的 Citrix Secure Access 客户端在 NetScaler 登录页面上提供第二个因素 OTP，而是可以通过为注册设备提供设备 PIN/触控 ID/面容 ID 来验证您的身份。

注册设备以接收推送通知后，您还可以使用该设备通过适用于 macOS/iOS 的 Citrix Secure Access 获得原生 OTP 支持。推送通知的注册对用户是透明的。当用户注册 TOTP 时，如果 NetScaler 支持，该设备也会注册推送通知。

macOS 客户端的发行说明

发行说明描述了服务版本中提供的新功能、现有功能的增强、已修复的问题和已知问题。发行说明包含以下一个或多个部分：

新增功能：当前版本中提供的新功能和增强功能。

已修复的问题：当前版本中已修复的问题。

已知问题：当前版本中存在的问题及其适用的解决方法。

> **重要信息：**

- EPA 客户端支持 macOS 10.13、10.14、10.15、11.x、12.x、13.x、14.x 和 15.x 版本。
- EPA 客户端支持 NetScaler 12.1、13.0、13.1 和 14.1 版本。
- 适用于 macOS/iOS 24.06.1 及更高版本的 Citrix Secure Access 解决了 CVE-2024-3661 中描述的 TunnelVision 漏洞。

V25.11.3 (Oct 05, 2026)

> **重要提示：**

此版本仅在 App Store 中提供。

新增功能

此版本解决了问题，以提高整体性能、安全性和稳定性。

V26.09.1.1 (Sep 24, 2026)

新增功能

- 此版本引入了对 macOS 27 的零日支持，并包含性能和稳定性修复。
- EPA 库已更新到 26.8.1.0 (OPSWAT OESIS 库版本 4.3.5914.0)。

V26.08.1.1 (Aug 24, 2026)

> **重要提示：**

> 此版本仅在 Citrix 下载 页面上提供。

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。
- EPA 库已更新到 26.7.1.0 (OPSWAT OESIS 库版本 4.3.5733.0)。

V26.06.1.1 (Jul 14, 2026)

> **重要提示：**

> 此版本仅在 Citrix 下载 页面上提供。

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。
- EPA 库已更新到 26.5.1.0 (OPSWAT OESIS 库版本 4.3.5495.0)。

已修复的问题

- 当 Citrix Secure Access 连接且启用了上下文路由时，可能会出现 SSH 终止和直接流量访问问题。

- 用户在切换网络时可能会遇到重新建立连接失败的问题。

V26.04.1.1 (Apr 28, 2026)

> **重要提示：**

> 26.04.1.1 版本可在 Citrix 下载 页面获取。

新增功能

- **用于访问应用程序的自定义工作区域**

  Citrix Secure Access 客户端现在支持自定义工作区域。此功能允许组织通过品牌化的、组织拥有的域（例如，`workspace.company.com`）而不是默认的 `*.cloud.com` 域，为用户提供对 SaaS 和私有 Web 应用程序的访问。管理员可以将自定义域配置为通过 Chrome Enterprise Premium 和 Citrix SecurAccess ZTNA 交付的基于浏览器的应用程序的身份验证和访问端点。最终用户受益于无缝的品牌体验，而组织则对访问和安全性拥有更大的控制权。

- 此版本解决了问题，以提高整体性能和稳定性。

已修复的问题

- 当 `enable_vpn_dnstruncate_fix` 配置参数设置为 0 时，Mac 设备会从 Citrix Secure Access 客户端断开连接，从而导致 VPN 稳定性和用户连接问题。

- EPA 库已更新到 26.3.1.0 (OPSWAT OESIS 库版本 4.3.5186.0)。

V25.11.2 (Apr 08, 2026)

> **重要提示：**

> 此版本仅在 App Store 中提供。

新增功能

此版本解决了问题，以提高整体性能、安全性及稳定性。

V26.01.1.1 (Feb 09, 2026)

新增功能

- **自动更新功能支持**

  适用于 macOS 的 Citrix Secure Access 应用程序现在可以通过自动更新功能将客户端自动更新到最新可用版本，该功能提供以下功能：

  - 定期检查更新。
  - 在自动通知用户后更新应用程序。

  此功能默认未启用。要启用自动更新支持，请联系 Citrix 支持。 有关详细信息，请参阅 macOS 自动更新支持。

  > **注意：**
  >
  > 由于自动更新功能是在 26.01.1.1 版本中引入的，因此管理员可以在后续版本中使用此功能。

- EPA 库已更新到 26.1.1.0 版本（OPSWAT OESIS 库版本 4.3.4910.0）。

V25.11.1 (Dec 10, 2025)

> **重要提示：**
>
> 25.11.1 版本已在 App Store 中提供。

新增功能

- EPA 库已更新到 25.10.1.0 版本（OPSWAT OESIS 库版本 4.3.4523.0）。

已修复的问题

- Citrix Secure Access 客户端由于 DNS 处理不正确而间歇性崩溃。
- 如果 DNS 响应包含 CNAME 记录，用户可能无法通过 Citrix Secure Access 应用程序访问内部网应用程序。要为 Citrix Secure Access 客户端启用 CNAME 记录处理，请联系Citrix 支持。

已知问题

- 在 macOS 26 设备上，Citrix Secure Access 应用程序在首次安装后可能会反复提示文件系统权限。提示可能在建立 VPN 连接或执行 EPA 检查等操作期间出现。此行为是由于 macOS 问题引起的，并非由 Citrix Secure Access 应用程序造成。

V25.11.1.1（Dec 05, 2025）

> **重要提示：**

> 25.11.1.1 版本可在 Citrix 下载 页面获取。

新增功能

- **EPA 客户端插件与 Citrix Secure Access 应用程序集成**

  macOS Citrix Secure Access 应用程序（以 .pkg 文件形式分发）现在包含 EPA 客户端插件。这意味着当用户安装应用程序时，该插件会自动安装。

- **增强的客户端证书身份验证**

  在客户端证书身份验证期间，Citrix Secure Access 会根据 NetScaler Gateway 上配置的 CA 证书自动选择客户端证书。有关详细信息，请参阅配置客户端证书身份验证。

- EPA 库已更新至 25.10.1.0（OPSWAT OESIS 库版本 4.3.4523.0）。

已修复问题

- Citrix Secure Access 客户端由于 DNS 处理不当而间歇性崩溃。

- 如果 DNS 响应包含 CNAME 记录，用户可能无法通过 Citrix Secure Access 应用程序访问内部网应用程序。要为 Citrix Secure Access 客户端启用 CNAME 记录处理，请联系 Citrix 支持。

已知问题

- 在 macOS 26 设备上，Citrix Secure Access 应用程序在首次安装后可能会反复提示文件系统权限。提示可能在建立 VPN 连接或执行 EPA 检查等操作期间出现。此行为是由于 macOS 问题引起的，并非由 Citrix Secure Access 应用程序造成。

V25.08.1.2 (Oct 23, 2025)

> **重要提示：**

> 版本 25.08.1.2 可在 Citrix 下载 页面获取。

新增功能

- **Citrix Secure Access 客户端支持 PureAuth 应用程序**

  Citrix Secure Access 客户端现在支持在配置为身份验证时在 macOS 设备上启动 PureAuth 应用程序。

V25.08.2 (Oct 22, 2025)

> **重要提示：**

> 版本 25.08.2 已在 App Store 中提供。

新增功能

- **Citrix Secure Access 客户端支持 PureAuth 应用程序**

  Citrix Secure Access 客户端现在支持在配置身份验证后在 macOS 设备上启动 PureAuth 应用程序。

V25.08.1.1 和 V25.08.1 (Sep 17, 2025)

> **重要提示：**

> - 如果您使用的是最新的 Apple OS 版本（例如 macOS 26 (Tahoe) 及更高版本），建议您升级到 Citrix Secure Access 客户端版本 25.08.1.1/25.08.1 或更高版本。有关 NetScaler Gateway 客户端软件要求的更多信息，请参阅系统要求。
> - 版本 25.08.1.1 可在 Citrix Downloads 页面中获取，版本 25.08.1 可在 App Store 中获取。

新增功能

- **将 TCP DNS 查询路由到特定于应用程序的资源位置**

  现在，特定主机名的 TCP DNS 查询可以直接路由到相应应用程序中配置的资源位置。此路由通过确保 DNS 查询到达最相关的资源位置来提高应用程序性能。以前，所有 TCP DNS 查询默认路由到地理位置最近的资源位置，而不管应用程序的实际位置。

- **Citrix Secure Access 客户端的 SNI 支持**

  Citrix Secure Access 客户端现在将服务器名称指示 (SNI) 字段作为 TLS 握手的一部分发送。此功能默认启用。要禁用 SNI 支持，请联系 Citrix 支持。

- **Citrix Secure Access 客户端上的 Okta Verify 应用程序支持**

  Citrix Secure Access 客户端现在支持在配置用于身份验证时在 macOS 设备上启动 Okta Verify 应用程序。

- EPA 库已更新至 25.08.1.0 (OPSWAT OESIS 库版本 4.3.4253.0)。

V25.07.1 (Aug 12, 2025)

> **重要提示：**

> 此版本仅在 App Store 中提供。

新增功能

- **支持多工作区 URL**

  适用于 macOS 的 Citrix Secure Access 客户端现在支持多工作区 URL，允许管理员在 Citrix Cloud 环境中配置多个访问点。此功能对于必须为不同用户组（例如人力资源、IT、承包商或供应商）提供不同访问 URL 的企业非常有用。有关详细信息，请参阅 配置工作区 URL。

- EPA 库已更新到 25.07.1.0 (OPSWAT OESIS 库版本 4.3.4141.0)。

V25.07.1.1 (Aug 12, 2025)

> **重要提示：**

> 此版本仅在 Citrix 下载 页面提供。

新增功能

- **支持多工作区 URL**

  Citrix Secure Access 客户端现在支持多工作区 URL，允许管理员在 Citrix Cloud 环境中配置多个访问点。此功能对于必须为不同用户组（例如人力资源、IT、承包商或供应商）提供不同访问 URL 的企业非常有用。有关详细信息，请参阅配置工作区 URL。

- EPA 库已更新到 25.07.1.0 (OPSWAT OESIS 库版本 4.3.4141.0)。

V25.06.1.2 (Jul 16, 2025)

> **重要提示：**

> 此版本仅在 Citrix 下载 页面提供。

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.06.2 (Jul 10, 2025)

> **重要提示：**

> 此版本仅在 App Store 中提供。

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.06.1.1 (Jul 09, 2025)

> **重要提示：**

> 此版本适用于 macOS 版 Citrix Secure Access 客户端，并且仅在 Citrix 下载 页面提供。

新增功能

- **支持 macOS 版 Citrix Secure Access 客户端**

  您现在可以从 Citrix 下载 页面提供的软件包 (`.pkg`) 文件或从 App Store 下载并安装该应用程序。`.pkg` 文件可以手动安装，也可以使用 Jamf 和 Intune 等管理工具进行安装。

  先决条件

  在安装 Citrix Secure Access 应用程序的 `.pkg` 文件之前，请确保满足以下先决条件：

  - Mac 电脑运行 macOS 13.0 或更高版本。
  - 用户在 Mac 电脑上拥有管理员权限。在受管机器上，管理员必须确保已启用应用程序安装权限，并且已激活标识符为 "com.citrix.NSG.macos.app.vpnplugin" 的系统扩展。
  - 如果 Citrix Secure Access 应用程序当前正在运行，请退出该应用程序。
  - 删除之前安装的任何 App Store 版本的 Citrix Secure Access 应用程序。

  如何在 macOS 上安装 Citrix Secure Access 应用程序：

  > **重要**
  >
  > Citrix Secure Access 应用程序的 `.pkg` 文件使用标识符为 "com.citrix.NSG.macos.app.vpnplugin" 的系统扩展进行 VPN 连接。对于客户端证书身份验证，证书必须安装在 **系统钥匙串** 中，因为 macOS 系统扩展无法访问 **登录钥匙串** 中的证书。

  a. 从 Citrix 下载 下载 `.pkg` 文件。
  b. 使用管理工具（Jamf 或 Intune）或手动安装应用程序。要手动安装应用程序，请双击 `.pkg` 文件并按照屏幕上的说明进行操作。

  首次设置：

  安装 Citrix Secure Access 应用程序后，请按照以下说明从 macOS 设备使用 Citrix Secure Access 应用程序：

  a. 打开 **应用程序** 文件夹，然后双击 Citrix Secure Access 应用程序图标以启动它。
  b. 首次启动时，系统会提示安装系统扩展的权限。在系统提示中单击 **确定**。

如果系统提示未出现，请转到 **系统设置** 以启用标识符为 "com.citrix.NSG.macos.app.vpnplugin" 的系统扩展的安装。

- 对于 macOS 14.x，**系统设置** 选项位于 **隐私与安全性** 选项卡下。
- 对于 macOS 15.x 及更高版本，**系统设置**选项位于**登录项与扩展** -> **网络扩展**下。

V25.06.1 (Jul 09, 2025)

> **重要提示：**

> 此版本仅在 App Store 中提供。

- EPA 库已更新到 25.06.1.0 (OPSWAT OESIS 库版本 4.3.4025.0)。
- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.03.4 (May 14, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.03.3 (May 12, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.03.2 (May 08, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.03.1 (Apr 10, 2025)

新增功能

- **SecurAccess ZTNA 服务的混合数据路径支持**

Citrix Secure Access 客户端现在支持 SecurAccess ZTNA 服务中的混合数据路径，该服务同时使用本地和云基础架构来提供对应用程序的安全访问。您可以配置应用程序以通过 Cloud Connector 或本地 NetScaler Gateway 进行路由。有关详细信息，请参阅SecurAccess ZTNA 服务的混合数据路径。

- EPA 库已更新到 25.03.1.0 (OPSWAT OESIS 库版本 4.3.3980.0)。
- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.02.1 (Mar 14, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

已修复的问题

- 如果在登录期间使用的 WebView 中的 User-Agent 字符串不包含正确的标识符，Citrix Secure Access 客户端可能无法与第三方安全 Web 网关配合使用。

V25.01.2 (Feb 18, 2025)

新增功能

- 此版本解决了部分安全相关问题，并提升了应用程序的整体性能。

V25.01.1 (Jan 16, 2025)

新增功能

- **来自 SecurAccess ZTNA 的服务器发起连接支持**

  适用于 macOS 的 Citrix Secure Access 客户端现在支持来自 Citrix SecurAccess ZTNA 的服务器发起连接。此功能允许用户配置策略，使应用程序能够打开到端点的 TCP 连接。有关详细信息，请参阅 支持服务器到客户端的连接 - 预览。

- EPA 库已更新至 25.01.13.16 (OPSWAT OESIS 库版本 4.3.3910.0)。

已修复问题

- 在运行 macOS 15.2 及更高版本的设备上，Citrix Secure Access 客户端可能无法完成配置的 OPSWAT 扫描。

V24.11.1 (Nov 25, 2024)

新增功能

- **在 Citrix Director 中监控 TCP 应用程序会话活动**

  适用于 macOS 的 Citrix Secure Access 客户端现在将 TCP 应用程序会话活动发送到 Citrix Director，用于 Citrix SecurAccess ZTNA 的云部署和本地部署。

- **在 Citrix Director 中监控会话活动事件**

  适用于 macOS 的 Citrix Secure Access 客户端现在将汇总的会话活动事件（例如成功的应用程序启动、应用程序启动失败和 DNS 失败）发送到 Citrix Director，用于 Citrix SecurAccess ZTNA 的云部署和本地部署。

- **支持 SecurAccess ZTNA 中的上下文访问功能**

  Citrix Secure Access 客户端支持上下文访问功能，该功能使管理员能够根据用户上下文（例如网络位置、地理位置和设备状态）动态实施 ZTNA 策略。有关详细信息，请参阅基于上下文的应用程序路由和资源位置选择。

- EPA 库已更新到 24.11.1.0 (OPSWAT OESIS 库版本 4.3.3820.0)。

V24.10.1 (Oct 17, 2024)

新增功能

- **支持 Citrix Secure Access 客户端排除 DNS 流量**

  您现在可以配置 Citrix Secure Access 客户端以排除 DNS 流量不被拦截。有关详细信息，请参阅从客户端拦截中排除特定域流量。

- EPA 库已更新到 24.09.1.0 版本（OPSWAT OESIS 库版本 4.3.3750.0）。

- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.09.1 (Sep 16, 2024)

> **重要提示：**

> 如果您使用的是最新的 Apple OS 版本（例如 macOS 15 及更高版本），建议您升级到 Citrix Secure Access 客户端版本 24.09.1 或更高版本。有关 NetScaler Gateway 客户端软件要求的更多信息，请参阅Citrix Secure Access 客户端系统要求。

新增功能

- **SecurAccess ZTNA 的系统通知支持**

  Citrix Secure Access 客户端现在支持本地部署 SecurAccess ZTNA 的系统通知。

- EPA 库已更新到 24.08.1.0 版本（OPSWAT OESIS 库版本 4.3.3709.0）。
- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.08.1 (Aug 14, 2024)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.07.1 (Jul 15, 2024)

新增功能

- EPA 库已更新到 24.06.1.0 (OPSWAT OESIS 库版本 4.3.3612.0)。
- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.06.2 (Jun 27, 2024)

新增功能

此版本解决了 IPv6 登录问题。

V24.06.1 (Jun 24, 2024)

新增功能

- 此版本解决了 CVE-2024-3661 中描述的 TunnelVision 漏洞。
- 此版本解决了一些问题，以提高整体性能和稳定性。
- EPA 库已更新到 24.05.2.0 (OPSWAT OESIS 库版本 4.3.3586.0)。

- **EPA 扫描以检查 Citrix Workspace™ 应用程序版本**

  Citrix Secure Access 支持新的 EPA 扫描 `CWA Version`，用于验证 macOS 计算机上的 Citrix Workspace 版本。有关支持的 EPA 扫描的详细信息，请参阅表达式字符串。

- **与第三方安全 Web 网关的互操作性增强**

  Citrix Secure Access 的 User-Agent 字符串已更新，以增强与第三方安全 Web 网关的互操作性。

已修复的问题

- 如果启用了具有反向拆分隧道的每应用 VPN，Citrix Secure Access 将无法绕过排除应用程序的 VPN 隧道。

适用于 macOS 的 24.6.1 EPA 客户端 (Jun 18, 2024)

新增功能

- **EPA 扫描以检查 Citrix Workspace 应用程序版本**

  Citrix EPA 客户端支持一项新的扫描“CWA 版本”，用于验证 macOS 计算机上的 Citrix Workspace 版本。有关支持的 EPA 扫描的详细信息，请参阅表达式字符串。

V24.04.1 (Apr 18, 2024)

新增功能

- EPA 库已更新到 24.04.1.0 版本 (OPSWAT OESIS 库版本 4.3.3503.0)。
- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.03.1 (Mar 14, 2024)

新增功能

- EPA 库已更新到 24.03.1.0 版本 (OPSWAT OESIS 库版本 4.3.3460.0)。
- **通过 Citrix Workspace 应用程序自动单点登录 (SSO) 到 Citrix Secure Access - 预览版**

适用于 macOS 的 Citrix Secure Access 现在支持在登录 Citrix Workspace 应用程序时自动单点登录 (SSO) 到 Citrix Secure Access。请确保您使用适用于 macOS 的 Citrix Secure Access 24.03.1 和适用于 Mac 的 Citrix Workspace 应用程序 2402 及更高版本，以利用此功能。此功能仅在云商店中受支持，不支持本地商店。

  - 有关管理员和最终用户说明，请参阅通过适用于 Mac 的 Citrix Workspace 应用程序自动单点登录到 Citrix Secure Access - 预览版。
  - 有关最终用户说明，请参阅通过 Citrix Workspace 应用程序自动单点登录到 Citrix Secure Access。

- **整体性能和稳定性改进**

  Citrix Secure Access 客户端通过以下功能得到增强，以提高整体性能和稳定性：

  - 改进了与 IPv6 网关的 VPN 连接弹性。

V24.02.1 (Feb 15, 2024)

新增功能

- **支持 Mac 客户端上的 EPA 扫描运算符**

  适用于 macOS 的 Citrix Secure Access 客户端现在支持 EPA 编辑器上的所有运算符 `<`、`>`、`>=`、`<=`、`==` 和 `!=`。此外，**Mac OS** 选项作为单独的选项在 EPA 编辑器中提供（**Mac > Mac OS**）。您可以使用这些运算符对 macOS 设备执行产品版本扫描。

  有关详细信息，请参阅高级端点分析扫描 中的“**注意**”部分。

- EPA 库已更新至 24.1.2.1 (OPSWAT OESIS 库版本 4.3.3405.0)。

- 此版本解决了一些问题，以提高整体性能和稳定性。

适用于 macOS 的 24.1.5 EPA 客户端 (Feb 12, 2024)

新增功能

- **EPA 支持配备 Apple 芯片处理器的 Mac 设备**

  Citrix EPA 客户端现在支持使用 Apple 芯片处理器的 Mac 设备。Mac 设备不再需要安装 Rosetta 即可运行 Citrix EPA 客户端。

- **Mac 客户端对 EPA 扫描运算符的支持**

适用于 Mac 的 Citrix EPA 客户端现在支持 EPA 表达式中的运算符 (`<`、`>`、`>=` 和 `<=`)。管理员可以配置 EPA 扫描以允许各种 OS 版本。

例如，要允许从 12.4 到 13.0（不包括 12.8）的 OS 版本，管理员可以配置表达式 `version >= 12.4 && version <= 13.0 && version != 12.8`。这意味着 macOS 版本必须在 12.4 到 13.0 之间，但不能是 12.8。

有关详细信息，请参阅高级端点分析扫描。

V23.12.2 (20 Dec 2023)

新增功能

此版本解决了问题，以提高整体性能和稳定性。

V23.12.1 (06 Dec 2023)

新增功能

- EPA 库已更新到 23.11.1.5 (OPSWAT OESIS 库版本 4.3.3318.0)。
- 此版本解决了其他问题，以提高整体性能和稳定性。

V23.11.2 (01 Nov 2023)

新增功能

EPA 库已更新到 23.11.1.1 (OPSWAT OESIS 库版本 4.3.3279.0)。

V23.11.1 (27 Oct 2023)

新增功能

- EPA 库已更新到 23.10.1.1 (OPSWAT OESIS 库版本 4.3.3246.0)。
- 此版本解决了以下问题：
  - 与 Citrix SecurAccess ZTNA™ 环境的连接问题。
  - 其他问题，以提高整体性能和稳定性。

V23.10.2 (17 Oct 2023)

此版本解决了 IPv6 登录问题。

V23.10.1 (09 Oct 2023)

新增功能

- EPA 库已更新到 23.9.1.2 (OPSWAT OESIS 库版本 4.3.3221.0)。
- **支持本地 LAN 访问**

  适用于 macOS 的 Citrix Secure Access 现在支持 NetScaler Gateway 的本地 LAN 访问功能。您可以配置本地 LAN 访问，以便在建立 VPN 连接后，允许或阻止最终用户访问其客户端设备上的本地 LAN 资源。有关详细信息，请参阅：

  - NetScaler Gateway 管理员配置
  - 最终用户配置 - macOS

V23.09.1 (07 Sep 2023)

> **重要提示：**

> 如果您使用的是最新的 Apple OS 版本（例如 macOS 14 及更高版本），建议您升级到 Citrix Secure Access 客户端版本 23.09.1 或更高版本。有关 NetScaler Gateway 客户端软件要求的更多信息，请参阅 Citrix Secure Access 客户端系统要求。

新增功能

- EPA 库已更新到 1.3.9.9 (OPSWAT OESIS v4.3.3160)。
- **UI 上的安全连接洞察**

  在 Citrix Secure Access 客户端 UI 的“连接”屏幕上，您可以查看安全连接详细信息。详细信息包括 IP 地址、FQDN、目标端口和连接持续时间。有关详细信息，请参阅 安全连接洞察。

- **VPN 连接失败后使用 NetScaler Gateway 重新进行身份验证**

  macOS 版 Citrix Secure Access 客户端现在会在 VPN 连接丢失时提示您使用 NetScaler Gateway 重新进行身份验证。UI 上会通知您，指示与 NetScaler Gateway 的连接已丢失，并且您必须重新进行身份验证才能恢复连接。有关详细信息，请参阅 在 VPN 连接失败后从 macOS 重新连接到 NetScaler Gateway。

V23.08.1 (24 Aug 2023)

新增功能

- 此版本解决了有助于提高整体性能和稳定性的问题。
- EPA 库已更新到 1.3.9.9 (OPSWAT OESIS v4.3.3122)。

23.7.6 macOS 版 EPA 客户端 (10 Aug 2023)

此版本解决了有助于提高整体性能和稳定性的问题。

V23.07.1 (17 Jul 2023)

新增功能

- **日志页面增强功能**

  macOS 版 Citrix Secure Access 的“日志”页面已通过以下选项得到增强：

  - 最大日志文件数：指定要为日志收集添加的最大日志文件数。
  - 电子邮件日志：通过电子邮件发送日志。

  有关详细信息，请参阅 发送日志。

已修复问题

连接到 VPN 时，如果系统提示您选择用于身份验证的证书，则身份验证登录屏幕会出现在 Citrix Secure Access 客户端主页的后面。

V23.06.1 (07 Jun 2023)

新增功能

- **导航栏上的“帮助”菜单**

  Citrix Secure Access 客户端的导航栏中现已添加“帮助”菜单。“帮助”菜单中的选项（“打开日志”、“导出日志”、“通过电子邮件发送日志”和“清除日志”）可用于调试日志。

  “帮助”菜单下新增了“通过电子邮件发送日志”选项。此选项可用于通过电子邮件共享日志。有关详细信息，请参阅发送日志。

已修复问题

在某些情况下，Citrix Secure Access for macOS 上的 DNS 短名称解析会失败。

已知问题

在某些情况下，反向分流中排除的路由会被隧道化。

V23.05.2 (11 May 2023)

已修复的问题

升级后，适用于 iOS 客户端设备的 Citrix SSO 无法建立按应用 VPN 连接。

V23.05.1 (04 May 2023)

新增功能

- EPA 库已更新至 1.3.9.3，OPSWAT 库已更新至 4.3.2987。
- **支持将事件发送到 Citrix Analytics**

  适用于 macOS 的 Citrix Secure Access 现在支持将事件（例如会话创建、会话终止和应用程序连接）发送到 Citrix Analytics 服务。然后，这些事件将记录在 SecurAccess ZTNA 服务仪表板中。

已修复的问题

- 当用户连接到 Citrix Secure Access 或 Citrix SSO 时，“连接持续时间”字段无法以区域特定格式显示时间。

V23.04.1 (04 Apr 2023)

新增功能

- EPA 库已更新到 1.3.9.1，OPSWAT 库已更新到 4.3.2923。

V22.12.2 (2023 年 2 月 27 日)

新增功能

- EPA 库已更新到 1.3.8.9 (OPSWAT OESIS v4.3.2892.0)。

V22.12.1 (2022 年 12 月 7 日)

此版本解决了有助于提高整体性能和稳定性的问题。

V22.11.1 (2022 年 11 月 29 日)

已修复的问题

- 对于使用本地网关的非 nFactor 身份验证，传输登录不起作用。

适用于 macOS 的 22.11.3 EPA 插件 (2022 年 11 月 28 日)

已修复的问题

- 在 NetScaler 上启用 GSLB 时，适用于 macOS 的 Citrix EPA 插件会崩溃。

V22.10.1 (2022 年 11 月 17 日)

新增功能

- Citrix Endpoint Analysis 插件现在支持新的 MAC 地址验证表达式，可以为允许的 IP 地址列表创建模式集。

已修复的问题

- 有时，NetScaler Gateway 13.0 或 13.1 版本中的空代理设置会导致 Citrix SSO 创建不正确的代理设置。
- 有时，VPN 客户端在网络中断后或设备从睡眠模式唤醒后无法重新连接。
- 有时，当使用 IPv6 字面量作为目标时，网关连接会失败。

适用于 macOS 的 22.10.1 EPA 插件 (2022 年 10 月 27 日)

新增功能

- Citrix Endpoint Analysis 插件现在支持新的 MAC 地址验证表达式，可以为允许的 IP 地址列表创建模式集。
- Citrix Endpoint Analysis 插件在处理来自 Google Chrome 的专用网络访问预检请求时，会发送重复的同意警报。

V22.06.1 (2022 年 9 月 20 日)

新增功能

- EPA 库已更新到 4.3.2523.0 (1.3.7.5)

已修复问题

- 带有 EPA 扫描的 nFactor 身份验证在 macOS 客户端上不起作用。
- 在 macOS 的 Secure Access Agent 主页上，汉堡菜单的左侧和顶部会出现额外的白色或黑色填充，具体取决于所选主题（浅色或深色）。
- 如果配置了设备证书，首次尝试登录 VPN 时，WebView 窗口会最小化。
- 当 NetScaler 设备上启用 GSLB 时，macOS 客户端上的 Citrix Secure Access 应用程序的端点分析不起作用。
- 如果配置的应用程序名称中包含空格，并且您尝试访问该应用程序，则“增强安全性已启用”弹出窗口不会显示在 macOS 客户端上。
- 在使用 Chrome 浏览器的 Mac 设备上，访问两个 FQDN 时 VPN 扩展程序崩溃。
- 当从网关收到不正确的位置值时，Citrix Secure Access 会崩溃。如果管理员定义了响应程序策略以重定向到另一个主机，则可能会发生这种情况。
- 如果存在显著延迟或拥塞，则直接连接到 Citrix Secure Access 建立的隧道外部的资源可能会失败。

V3.2.4.9 - 适用于 macOS 的 EPA 插件 (2022 年 8 月 1 日)

已修复的问题

- Citrix Endpoint Analysis 插件无法处理来自 Google Chrome 浏览器版本 104 的专用网络访问预检请求。
- 适用于 macOS 的 Citrix Endpoint Analysis 插件不支持 GSLB。

已知问题

- 从 Google Chrome 浏览器版本 104 启动时，适用于 macOS 的 Citrix Endpoint Analysis 插件会显示重复的同意对话框。用户必须接受这两个提示。

V22.03.1 (2022 年 6 月 14 日)

新增功能

- EPA 库已更新至 4.3.2393.0。

已修复的问题

- 搜索列表中添加了一个额外的 DNS 域。这是因为，当拆分隧道设置为“拆分”或“两者”时，只有指定的域及其子域才不会被隧道化。如果指定的域是 A.B.C，那么除了 A.B.C 和 *.A.B.C 之外，B.C 也会被匹配。

- 不使用 PAC 文件的 HTTP/HTTPS 代理设置已损坏。

V22.02.3 (2022 年 3 月 24 日)

新增功能

- Citrix Secure Access for macOS 会在客户端的每个 TCP 数据连接上解析云工作区连接的服务节点 FQDN。在每个 TCP 数据连接上解析服务节点的 FQDN 不适用于本地网关连接。

已修复的问题

- 有时，Citrix Secure Access for macOS 会因为某些使用端口 53 的非 DNS 协议（例如 STUN）的问题而断开连接。

- 当服务器在连接建立后立即在客户端之前发送数据时，Citrix Secure Access 应用程序会导致某些协议中断。

- 如果用户关闭了 macOS 版 Citrix Secure Access 客户端的身份验证窗口而未完成身份验证，则后续连接服务器的尝试将失败，直到应用程序重新启动。

- macOS 版 Citrix Secure Access 客户端现在捆绑了 OPSWAT 库版本 4.3.2367.0。

- macOS 版 Citrix Secure Access 运行身份验证后 EPA 检查所需时间比预期长。

已知问题

- 在已连接的 Citrix SecurAccess ZTNA 服务区域变得不可达一分钟后，macOS 版 Citrix Secure Access 应用程序会注销。但是，这不影响本地网关连接。

V22.02.2 (15-Feb-2022)

已修复的问题

- 当用户尝试通过 macOS 版 Citrix Secure Access 访问未订阅的 Web 应用程序时，会显示多个弹出窗口。

V1.4.1 (28-Jan-2022)

新增功能

- 适用于 macOS 的 Citrix SSO 应用程序现已更名为 Citrix Secure Access。

已修复的问题

- 如果身份验证服务器在同一 Web 视图会话中多次请求客户端证书，则客户端证书身份验证将失败。
- 如果服务器证书的通用名称仅包含 IP 地址（因为客户端和 ADC 之间存在代理），则 Citrix SSO 无法建立 VPN 连接。
- 用于检查防病毒软件上次完整系统扫描的 EPA 扫描在 macOS 上失败。
- 有时，Citrix SSO 应用程序在处理大型 DNS 数据包时会崩溃。

V1.4.0 (17-Nov-2021)

已修复的问题

- 有时，当服务器证书受信任时，服务器验证代码会失败。因此，最终用户无法访问网关。
- 网络中断后，Citrix SSO 无法重新建立 VPN 连接。

V1.3.13 (2021 年 11 月 5 日)

已修复的问题

- 在筛选托管 VPN 与非托管 VPN 的会话时，您可能会遇到故障。建立会话的初始请求在 User-Agent 标头中缺少“ManagedVpn”信息。

V1.3.12 (2021 年 10 月 21 日)

已修复的问题

- 如果 macOS 钥匙串中没有客户端证书，则 Citrix SSO for macOS 的客户端证书身份验证会失败。
- Citrix SSO 应用程序在接收通知时会间歇性崩溃。
- VPN 扩展程序在调用 "isFeatureEnabled" 参数以检查功能标志时可能会崩溃。
- 如果 DTLS 协议具有空负载，网关 VPN 扩展程序会崩溃。
- 当设备从睡眠模式唤醒且 VPN 已连接时，SSO 应用程序会间歇性崩溃。

V1.3.11 (17-Sep-2021)

已修复的问题

- 对于使用 Citrix SSO 的 macOS 设备，防火墙检查的 EPA 扫描失败。
- 当配置了旧版身份验证或 Intune 网络访问合规性 (NAC) 时，Citrix SSO 在 iOS 12 设备中崩溃。

V1.3.10 (31-Aug-2021)

新增功能

- 适用于 macOS 的 Citrix SSO 现在捆绑了 OPSWAT 库版本 4.3.1977.0。

V1.3.9 (2021年8月13日)

已修复的问题

- 在某些安装了 HTTP 代理软件的系统上，NetScaler Gateway IP 地址在内部显示为 127.0.0.1，从而阻止了隧道建立。
- Citrix SSO 无法连接到 DNS 名称与服务器证书中的通用名称不匹配的系统。Citrix SSO 现在会检查主题备用名称，并正确连接。

V1.3.8 (2021年7月7日)

新增功能

- 适用于 macOS 的 Citrix SSO 仅兼容 10.15 (Catalina) 及更高版本。
- 从适用于 macOS 的 Citrix SSO 1.3.8 版开始，EPA 库嵌入在应用程序中，而不是从 NetScaler Gateway 服务器下载。当前嵌入式 EPA 库版本为 1.3.5.1。

iOS 客户端发行说明

发行说明描述了服务版本中可用的新功能、现有功能的增强、已修复的问题和已知问题。发行说明包含以下一个或多个部分：

新增功能：当前版本中可用的新功能和增强功能。

已修复的问题：当前版本中已修复的问题。

已知问题：当前版本中存在的问题及其适用的解决方法。

> **重要信息：**
>
> - 适用于 macOS/iOS 的 Citrix Secure Access 24.06.1 及更高版本解决了 CVE-2024-3661 中描述的 TunnelVision 漏洞。

V26.09.1 (Oct 05, 2026)

新增功能

- 此版本解决了问题，以提高整体性能、安全性和稳定性。

V26.08.1 (Sep 02, 2026)

新增功能

- 此版本解决了问题，以提高整体性能、安全性和稳定性。

V26.06.1 (Jul 22, 2026)

已修复的问题

- 用户在切换网络时可能会遇到连接重新建立失败的情况。

V26.05.2 (Jul 01, 2026)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V26.05.1 (Jun 30, 2026)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V26.04.1 (Apr 28, 2026)

新增功能

- **用于访问应用程序的自定义工作区域**

  Citrix Secure Access 客户端现在支持自定义工作区域。此功能允许组织通过品牌化的、组织拥有的域（例如 workspace.company.com）而不是默认的 `*.cloud.com` 域，为用户提供对 SaaS 和私有 Web 应用程序的访问。管理员可以将自定义域配置为通过 Citrix SecurAccess ZTNA 交付的基于浏览器的应用程序的身份验证和访问端点。最终用户受益于无缝的品牌体验，而组织则对访问和安全性拥有更大的控制权。

- 此版本解决了一些问题，以提高整体性能和稳定性。

V26.03.1 (Mar 24, 2026)

新增功能

- **适用于 iOS 版 Citrix Secure Access 的单点登录 (SSO) 支持**

  适用于 iOS 26.03.1 及更高版本的 Citrix Secure Access 支持单点登录 (SSO)。当用户登录到 Citrix Workspace 应用程序，然后在 Citrix Secure Access 应用程序中启动连接时，他们会自动登录，无需重新输入凭据。这使得可以无缝访问 SecurAccess ZTNA URL，并提供统一的体验。

  要启用此功能，请联系 Citrix 支持。

  有关详细信息，请参阅 通过适用于 iOS 的 Citrix Workspace 应用程序自动单点登录到 Citrix Secure Access。

- 适用于 iOS 的 Citrix Secure Access 应用程序现在支持 DNS 后缀。要启用此功能，请联系 Citrix 支持。

已修复的问题

- 设备唤醒后，用户可能会遇到数据包丢失，直到 DTLS 连接重新建立。

V25.11.1 (Dec 10, 2025)

新增功能

- **支持多工作区 URL**

  适用于 iOS 的 Citrix Secure Access 客户端现在支持多工作区 URL，允许管理员在 Citrix Cloud 环境中配置多个访问点。此功能对于必须为不同用户组（例如人力资源、IT、承包商或供应商）提供不同访问 URL 的企业非常有用。有关详细信息，请参阅 配置工作区 URL。

- **在 Citrix Director 中监控会话活动事件**

  适用于 iOS 的 Citrix Secure Access 客户端现在将汇总的会话活动事件（例如成功的应用程序启动、应用程序启动失败和 DNS 失败）发送到 Citrix Director，用于 Citrix SecurAccess ZTNA 的云部署和本地部署。

V25.08.1 (Sep 18, 2025)

重要提示：

如果您使用的是最新的 Apple OS 版本（例如 iOS 26 及更高版本），我们建议您升级到 Citrix Secure Access 客户端版本 25.08.1 或更高版本。有关 NetScaler Gateway 客户端软件要求的更多信息，请参阅系统要求。

新增功能

- **支持 Citrix SecurAccess ZTNA**

  适用于 iOS 的 Citrix Secure Access 客户端现在支持 Citrix SecurAccess ZTNA 部署。这使管理员能够强制执行 ZTNA 策略，确保用户可以从 iOS 设备安全地访问企业应用程序和 Web 资源。有关更多信息，请参阅适用于移动设备的 Citrix SecurAccess ZTNA。

- **将 TCP DNS 查询路由到特定于应用程序的资源位置**

  特定主机名的 TCP DNS 查询现在可以直接路由到相应应用程序中配置的资源位置。此路由通过确保 DNS 查询到达最相关的资源位置来提高应用程序性能。以前，所有 TCP DNS 查询默认路由到地理位置上最近的资源位置，而不管应用程序的实际位置如何。

- **Citrix Secure Access 客户端的 SNI 支持**

  Citrix Secure Access 客户端现在在 TLS 握手过程中发送服务器名称指示 (SNI) 字段。此功能默认启用。要禁用 SNI 支持，请联系 Citrix Support。

V25.07.1 (Aug 12, 2025)

新增功能

- **丢弃 QUIC 握手数据包**

  适用于 iOS 的 Citrix Secure Access 客户端现在会丢弃快速 UDP 互联网连接 (QUIC) 握手数据包，从而实现更快地切换到 TCP 连接建立。要启用此功能，请联系 Citrix Support。

V25.06.2 (Jul 11, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.06.1 (Jul 09, 2025)

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.03.4 (Jun 02, 2025)

已修复的问题

- 在适用于 iOS 的 Citrix Secure Access 客户端中启用按应用 VPN 时，外部应用程序可能加载缓慢或无法加载。

- 当满足以下两个条件时，iOS 设备用户可能会被提示转移其登录信息：

  - 已为用户分配内网 IP 地址 (IIP)。
  - 在网络转换期间（例如在 Wi-Fi 和移动数据之间切换时），之前的会话仍保持活动状态。

  请联系 Citrix 支持 以启用自动转移登录功能，这可以消除会话转移期间手动提示的需要。

V25.03.3 (May 12, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.03.2 (May 08, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.03.1 (Apr 10, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.02.1 (Mar 14, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.01.1 (Jan 16, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

已修复的问题

- 在运行 macOS 15.2 及更高版本的设备上，Citrix Secure Access 客户端可能无法完成配置的 OPSWAT 扫描。

V24.11.1 (Nov 25, 2024)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.10.1 (Oct 17, 2024)

新增功能

- **支持 Citrix Secure Access 客户端排除 DNS 流量**

  您现在可以配置 Citrix Secure Access 客户端以排除 DNS 流量不被拦截。有关详细信息，请参阅从客户端拦截中排除特定域流量。

- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.09.1 (Sep 16, 2024)

> **重要提示：**

> 如果您使用的是最新的 Apple 操作系统版本（例如 iOS 18 及更高版本），建议您升级到 Citrix Secure Access 客户端版本 24.09.1 或更高版本。有关 NetScaler Gateway 客户端软件要求的更多信息，请参阅Citrix Secure Access 客户端系统要求。

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.08.1 (Aug 14, 2024)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.07.1 (Jul 15, 2024)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.06.2 (Jun 27, 2024)

新增功能

此版本解决了 IPv6 登录问题。

V24.06.1 (Jun 24, 2024)

新增功能

- 此版本解决了 CVE-2024-3661 中描述的 TunnelVision 漏洞。
- 此版本解决了一些问题，以提高整体性能和稳定性。
- **与第三方安全 Web 网关的互操作性增强**

  Citrix Secure Access 的 User-Agent 字符串已更新，以增强与第三方安全 Web 网关的互操作性。

已修复的问题

- 如果启用了带反向拆分隧道的每应用 VPN，Citrix Secure Access 将无法绕过排除应用的 VPN 隧道。

V24.04.1 (Apr 18, 2024)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.03.1 (Mar 14, 2024)

新增功能

- **整体性能和稳定性改进**

  Citrix Secure Access 客户端通过以下功能得到增强，以提高整体性能和稳定性：

  - 增加了可通过 VPN 隧道传输的并发连接数。
  - 改进了与 IPv6 网关的 VPN 连接弹性。

V24.02.1 (Feb 15, 2024)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V23.12.2 (20 Dec 2023)

新增功能

此版本解决了问题，以提高整体性能和稳定性。

V23.12.1 (06 Dec 2023)

新增功能

- 此版本解决了其他问题，以提高整体性能和稳定性。

V23.11.1 (27 Oct 2023)

新增功能

- 适用于 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档中的 UI 屏幕截图以反映此名称更改。
- 此版本解决了以下问题：

  - 与 Citrix SecurAccess ZTNA™ 环境的连接问题。
  - 其他问题，以提高整体性能和稳定性。

V23.10.2 (17 Oct 2023)

此版本解决了 IPv6 登录问题。

V23.10.1 (09 Oct 2023)

新增功能

- **支持本地 LAN 访问**

  适用于 iOS 的 Citrix SSO 现在支持 NetScaler Gateway 的本地 LAN 访问功能。您可以配置本地 LAN 访问，以便在建立 VPN 连接后，允许或阻止最终用户访问其客户端设备上的本地 LAN 资源。有关详细信息，请参阅以下内容：

  - NetScaler Gateway 管理员配置
  - 最终用户配置 - iOS

V23.09.1 (07 Sep 2023)

> **重要提示：**
>
> 如果您使用的是最新的 Apple OS 版本（例如 iOS 17 及更高版本），建议您升级到 Citrix SSO 23.09.1 或更高版本。有关 NetScaler Gateway 客户端软件要求的更多信息，请参阅 Citrix Secure Access 客户端系统要求。

新增功能

- **UI 上的安全连接洞察**

  在 Citrix Secure Access 客户端 UI 的“连接”屏幕上，您可以查看安全连接详细信息。详细信息包括 IP 地址、FQDN、目标端口和连接持续时间。有关详细信息，请参阅安全连接洞察。

- **VPN 连接失败后使用 NetScaler Gateway 重新进行身份验证**

  当 VPN 连接丢失时，适用于 iOS 的 Citrix SSO 现在会提示您使用 NetScaler Gateway 重新进行身份验证。UI 上会通知您与 NetScaler Gateway 的连接已丢失，并且您必须重新进行身份验证才能恢复连接。有关详细信息，请参阅VPN 连接失败后从 iOS 重新连接到 NetScaler Gateway。

V23.07.1 (17 Jul 2023)

新增功能

- **共享日志文件的各种选项**

适用于 iOS 的 Citrix SSO 中的“电子邮件日志”选项现已替换为“共享日志”选项。现在可以通过电子邮件、聊天、保存到文件等选项共享压缩的日志文件。

有关详细信息，请参阅发送日志。

V23.06.1 (07 Jun 2023)

新增功能

- **导航栏上的“帮助”菜单**

  Citrix Secure Access 客户端的导航栏中新增了“帮助”菜单。“帮助”菜单中的选项（打开日志、导出日志、通过电子邮件发送日志和清除日志）可用于调试日志。

  “帮助”菜单下新增了“通过电子邮件发送日志”选项。此选项可用于通过电子邮件共享日志。有关详细信息，请参阅发送日志。

已修复的问题

在某些情况下，Citrix SSO for iOS 上的 DNS 短名称解析失败。

已知问题

在某些情况下，反向拆分隧道中的排除路由会被隧道化。

V23.05.2 (11 May 2023)

已修复的问题

升级后，适用于 iOS 客户端设备的 Citrix SSO 无法建立按应用程序 VPN 连接。

V23.05.1 (04 May 2023)

新增功能

- **支持将事件发送到 Citrix Analytics**

  适用于 macOS 的 Citrix Secure Access 现在支持将事件（例如会话创建、会话终止和应用程序连接）发送到 Citrix Analytics 服务。然后，这些事件将记录在 SecurAccess ZTNA 服务控制板中。

已修复的问题

- 当用户连接到 Citrix Secure Access 或 Citrix SSO 时，“连接持续时间”字段无法以区域特定格式显示时间。

V22.12.1 (2022 年 12 月 7 日)

此版本解决了有助于提高整体性能和稳定性的问题。

V22.11.1 (2022 年 11 月 29 日)

已修复的问题

- 传输登录不适用于使用本地网关的非 nFactor 身份验证。

V22.10.1 (2022 年 11 月 17 日)

新增功能

- Citrix Endpoint Analysis 插件现在支持新的 MAC 地址验证表达式，可以在其中为允许的 IP 地址列表创建模式集。

已修复的问题

- 有时，NetScaler Gateway 13.0 或 13.1 版本中的空代理设置会导致 Citrix SSO 创建不正确的代理设置。
- 有时，VPN 客户端在网络中断或设备从睡眠模式唤醒后无法重新连接。
- 有时，当使用 IPv6 字面量作为目标时，网关连接会失败。

V22.06.1 (2022 年 9 月 20 日)

已修复的问题

- 当设备上没有合适的客户端证书时，带有可选客户端证书的 nFactor 身份验证会失败。
- 当从网关接收到不正确的位置值时，Citrix Secure Access 会崩溃。如果管理员定义了响应器策略以重定向到另一个主机，则可能会发生这种情况。

- 如果存在显著延迟或拥塞，则直接连接到 Citrix Secure Access 建立的隧道外部的资源可能会失败。

V22.03.1 (14-Jun-2022)

已修复问题

- 搜索列表中添加了一个额外的 DNS 域。这是因为，当拆分隧道设置为“拆分”或“两者”时，只有指定的域及其子域才不会被隧道化。如果指定的域是 A.B.C，则除了 A.B.C 和 *.A.B.C 之外，B.C 也会被匹配。

- 不使用 PAC 文件的 HTTP/HTTPS 代理设置已损坏。

V22.02.3 (24-Mar-2022)

已修复问题

- 当服务器在客户端之前发送数据时（连接建立后立即），Citrix Secure Access 应用程序会破坏某些协议。

V22.01.1 (2022 年 2 月 8 日)

已修复的问题

- 适用于 iOS 设备的 Citrix SSO 的每应用 VPN 连接无法连接到 443 以外端口上的 NetScaler Gateway。

已修复的问题

- 如果在同一 Web 视图会话中，身份验证服务器多次请求客户端证书，则客户端证书身份验证会失败。

- 如果服务器证书的通用名仅包含 IP 地址，并且客户端与 ADC 之间存在代理，则 Citrix SSO 无法建立 VPN 连接。

- 用于检查防病毒软件上次完整系统扫描的 EPA 扫描在 macOS 上失败。

- 有时，Citrix SSO 应用程序在处理大型 DNS 数据包时会崩溃。

V1.4.0 (2021 年 11 月 17 日)

已修复问题

- 有时，当服务器证书受信任时，服务器验证代码会失败。因此，最终用户无法访问网关。
- 网络中断后，Citrix SSO 无法重新建立 VPN 连接。

V1.3.13 (05-Nov-2021)

已修复问题

- 在筛选托管 VPN 与非托管 VPN 的会话时，您可能会遇到故障。建立会话的初始请求在 User-Agent 标头中缺少“ManagedVpn”信息。

V1.3.12 (21-Oct-2021)

已修复问题

- Citrix SSO 应用程序在接收通知时会间歇性崩溃。
- 当调用“isFeatureEnabled”参数以检查功能标志时，VPN 扩展可能会崩溃。
- 如果 DTLS 协议的有效负载为空，网关 VPN 扩展会崩溃。
- 当设备从睡眠模式唤醒且 VPN 已连接时，SSO 应用程序会间歇性崩溃。

V1.3.11 (2021 年 9 月 17 日)

已修复的问题

- 在配置了旧版身份验证或 Intune 网络访问合规性 (NAC) 的 iOS 12 设备中，Citrix SSO 会崩溃。

V1.3.9 (2021 年 8 月 13 日)

已修复的问题

- 在安装了 HTTP 代理软件的某些系统中，NetScaler Gateway IP 地址在内部显示为 127.0.0.1，从而阻止了隧道建立。

- “阻止不受信任的服务器”设置在支持 Citrix SSO for iOS 非英语本地化的系统上不起作用。
- Citrix SSO 无法连接到 DNS 名称与服务器证书中的通用名称不匹配的系统。Citrix SSO 现在会检查主题备用名称，并正确连接。

为 iOS 用户设置 Citrix Secure Access™

> **重要提示：**
>
> - 适用于 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。在此过渡期间，您可能会在文档中看到 Citrix SSO 的引用。
> - VPN 无法在 iOS 12 及更高版本上使用。要继续使用 VPN，请使用 Citrix Secure Access。

> 有关 Citrix Secure Access for iOS 支持的一些常用功能列表，请参阅 NetScaler Gateway 中支持的 Citrix Secure Access 客户端功能。

与 MDM 产品的兼容性

Citrix Secure Access (macOS/iOS) 与大多数 MDM 提供商兼容，例如 Citrix Endpoint Management（以前称为 XenMobile）、Microsoft Intune 等。

Citrix Secure Access (macOS/iOS) 还支持一项名为网络访问控制 (NAC) 的功能。有关 NAC 的更多信息，请参阅 为单因素登录配置 NetScaler Gateway 虚拟服务器的网络访问控制设备检查。借助 NAC，MDM 管理员可以在连接到 NetScaler 设备之前强制执行最终用户设备的合规性。Citrix Secure Access (macOS/iOS) 上的 NAC 需要 MDM 服务器（例如 Citrix Endpoint Management 或 Intune）和 NetScaler。

> **注意：**
>
> 要在没有 MDM 的情况下将 Citrix Secure Access 客户端与 NetScaler Gateway VPN 配合使用，您必须添加 VPN 配置。您可以从 Citrix Secure Access (macOS/iOS) 主页在 iOS 上添加 VPN 配置。

为 Citrix Secure Access 客户端 (macOS/iOS) 配置 MDM 管理的 VPN 配置文件

以下部分介绍了为 Citrix Secure Access 客户端 (macOS/iOS) 配置设备范围和按应用程序 VPN 配置文件的分步说明，其中以 Citrix Endpoint Management（以前称为 XenMobile）为例。其他 MDM 解决方案在与 Citrix Secure Access (macOS/iOS) 配合使用时，可以将本文档作为参考。

> **注意：**
>
> 本节解释了基本设备范围和按应用程序 VPN 配置文件的配置步骤。您还可以通过遵循 Citrix Endpoint Management™（以前称为 XenMobile）文档或 Apple 的 MDM VPN 有效负载配置来配置按需和代理。

设备级 VPN 配置文件

设备级 VPN 配置文件用于设置系统范围的 VPN。来自所有应用程序和服务的流量会根据 NetScaler 中定义的 VPN 策略（例如，完全隧道、拆分隧道、反向拆分隧道）通过隧道传输到 NetScaler Gateway。

在 Citrix Endpoint Management 上配置设备级 VPN

执行以下步骤以在 Citrix Endpoint Management 上配置设备级 VPN。

1. 在 Citrix Endpoint Management MDM 控制台上，导航到“**配置**”>“**设备策略**”>“**添加新策略**”。
2. 在左侧的“策略平台”窗格中选择 **iOS**。在右侧窗格中选择 **VPN**。
3. 在“**策略信息**”页面上，输入有效的策略名称和描述，然后单击“**下一步**”。
4. 在适用于 iOS 的“**VPN 策略**”页面上，键入有效的连接名称，并在“**连接类型**”中选择“**自定义 SSL**”。

   在 MDM VPN 有效负载中，连接名称对应于 **UserDefinedName** 密钥，并且 **VPN Type Key** 必须设置为 **VPN**。
5. 在“**自定义 SSL 标识符（反向 DNS 格式）**”中，输入 **com.citrix.NetScalerGateway.ios.app**。这是适用于 iOS 的 Citrix Secure Access 的捆绑包标识符。

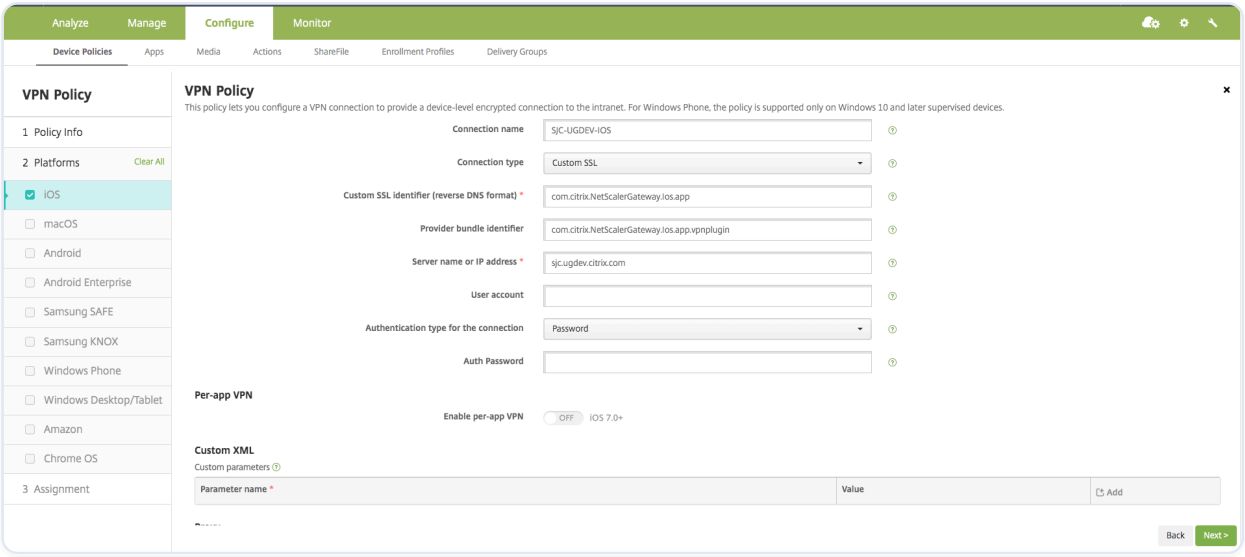
   在 MDM VPN 有效负载中，自定义 SSL 标识符对应于 **VPNSubType** 密钥。
6. 在“**提供程序捆绑包标识符**”中，输入 **com.citrix.NetScalerGateway.ios.app.vpnplugin**。这是 Citrix Secure Access iOS 应用程序二进制文件中包含的网络扩展的捆绑包标识符。

   在 MDM VPN 有效负载中，提供程序捆绑包标识符对应于 **ProviderBundleIdentifier** 密钥。

7. 在“**服务器名称或 IP 地址**”中，输入与此 Citrix Endpoint Management 实例关联的 NetScaler 的 IP 地址或 FQDN（完全限定域名）。

   配置页面中的其余字段是可选的。这些字段的配置可在 Citrix Endpoint Management（以前称为 XenMobile®）文档中找到。

8. 单击“**下一步**”。



9. 单击 **保存**。

每应用 VPN 配置文件

每应用 VPN 配置文件用于为特定应用程序设置 VPN。只有来自特定应用程序的流量才会通过隧道传输到 NetScaler Gateway。**每应用 VPN 有效负载** 支持设备范围 VPN 的所有密钥以及其他一些密钥。

在 Citrix Endpoint Management 上配置每应用级别 VPN

执行以下步骤以配置每应用 VPN：

1. 在 Citrix Endpoint Management 上完成设备级别 VPN 配置。
2. 在“每应用 VPN”部分中，将“**启用每应用 VPN**”开关设置为“开”。
3. 如果 Citrix Secure Access (macOS/iOS) 必须在启动匹配应用程序时自动启动，请将“**按需匹配应用程序已启用**”开关设置为“开”。这适用于大多数每应用场景。

   在 MDM VPN 有效负载中，此字段对应于密钥 **OnDemandMatchAppEnabled**。

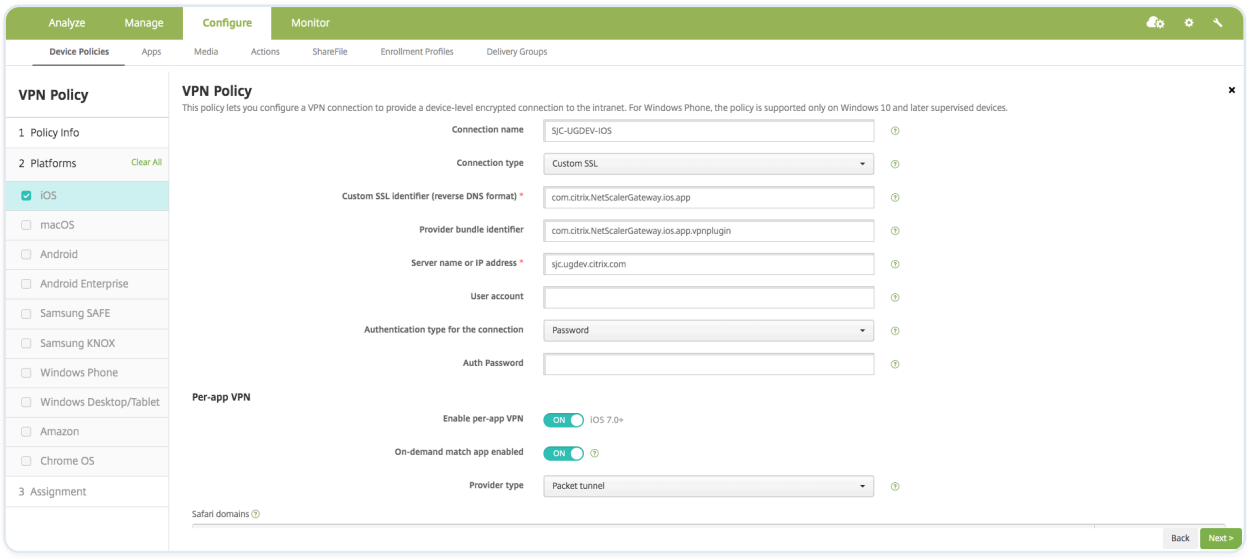
4. 在“**提供程序类型**”中，选择“**数据包隧道**”。

   在 MDM VPN 有效负载中，此字段对应于密钥 **Provider Type**。

5. Safari 域配置是可选的。配置 Safari 域后，当用户启动 Safari 并导航到与“**域**”字段中的 URL 匹配的 URL 时，Citrix Secure Access (macOS/iOS) 会自动启动。如果您想限制特定应用程序的 VPN，则不建议这样做。

   在 MDM VPN 有效负载中，此字段对应于密钥 **SafariDomains**。

   配置页面中的其余字段是可选的。这些字段的配置可在 Citrix Endpoint Management（以前称为 XenMobile）文档中找到。



6. 单击 **下一步**。
7. 单击 **保存**。

要将此 VPN 配置文件与设备上的特定应用程序关联，您必须创建一个 应用程序清单策略和凭据提供程序策略。

在每应用 VPN 中配置拆分隧道

MDM 客户可以在 Citrix Secure Access (macOS/iOS) 的每应用 VPN 中配置拆分隧道。必须将以下键/值对添加到在 MDM 服务器上创建的 VPN 配置文件的供应商配置部分。

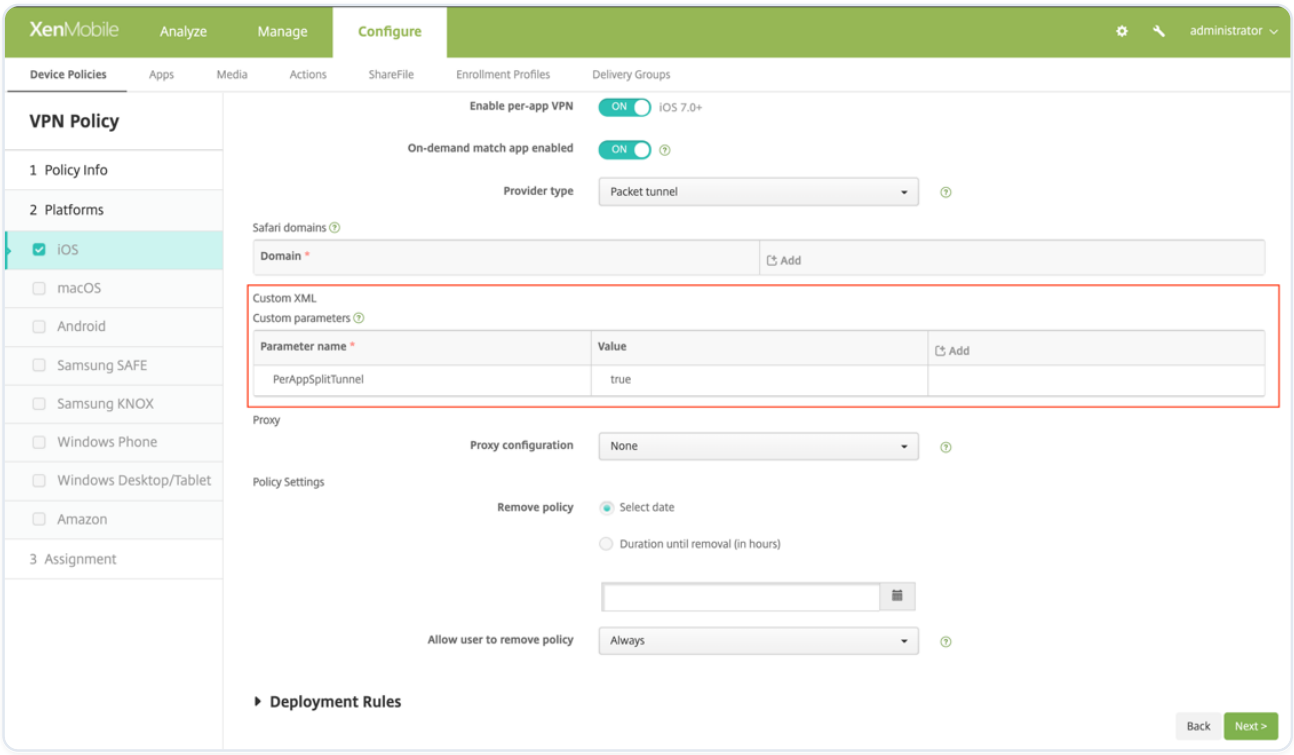
```
-  Key = "PerAppSplitTunnel"

-  Value = "true or 1 or yes"
```

键区分大小写且必须完全匹配，而值不区分大小写。

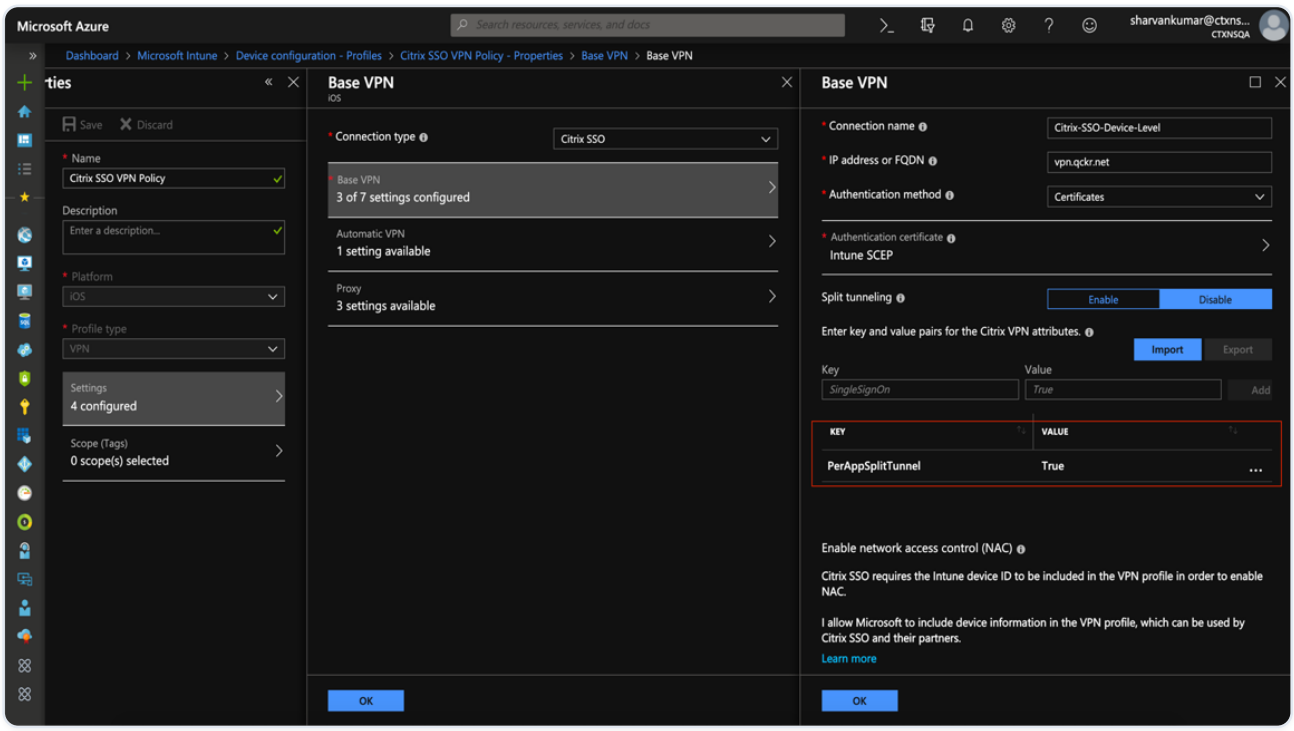
> **注意：**

> 配置供应商配置的用户界面在不同的 MDM 供应商之间不尽相同。请联系 MDM 供应商，以在您的 MDM 用户控制台中找到供应商配置部分。

> 以下是 Citrix Endpoint Management 中配置（供应商特定设置）的示例屏幕截图。



以下是 Microsoft Intune 中配置（供应商特定设置）的示例屏幕截图。



禁用用户创建的 VPN 配置文件

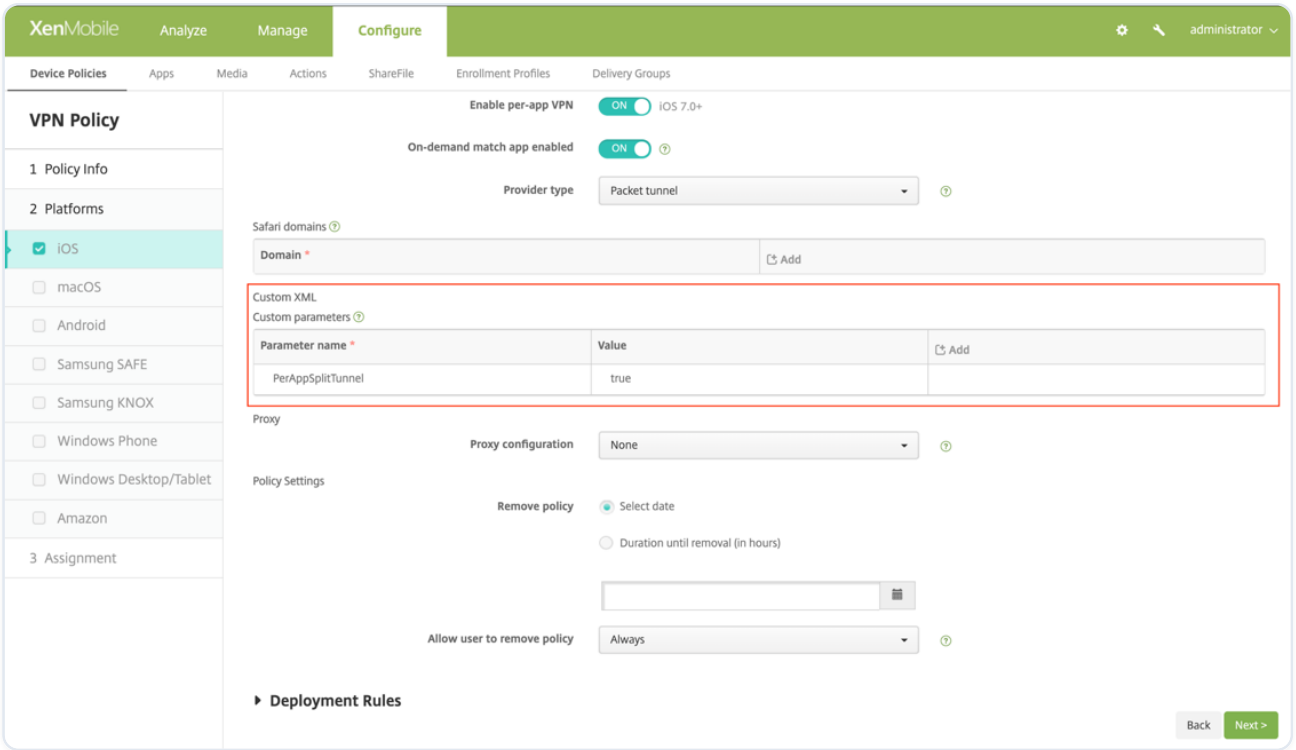
MDM 客户可以阻止用户在 Citrix Secure Access (macOS/iOS) 中手动创建 VPN 配置文件。为此，必须将以下键/值对添加到在 MDM 服务器上创建的 VPN 配置文件的供应商配置部分。

```
-  Key = "disableUserProfiles"

-  Value = "true or 1 or yes"
```

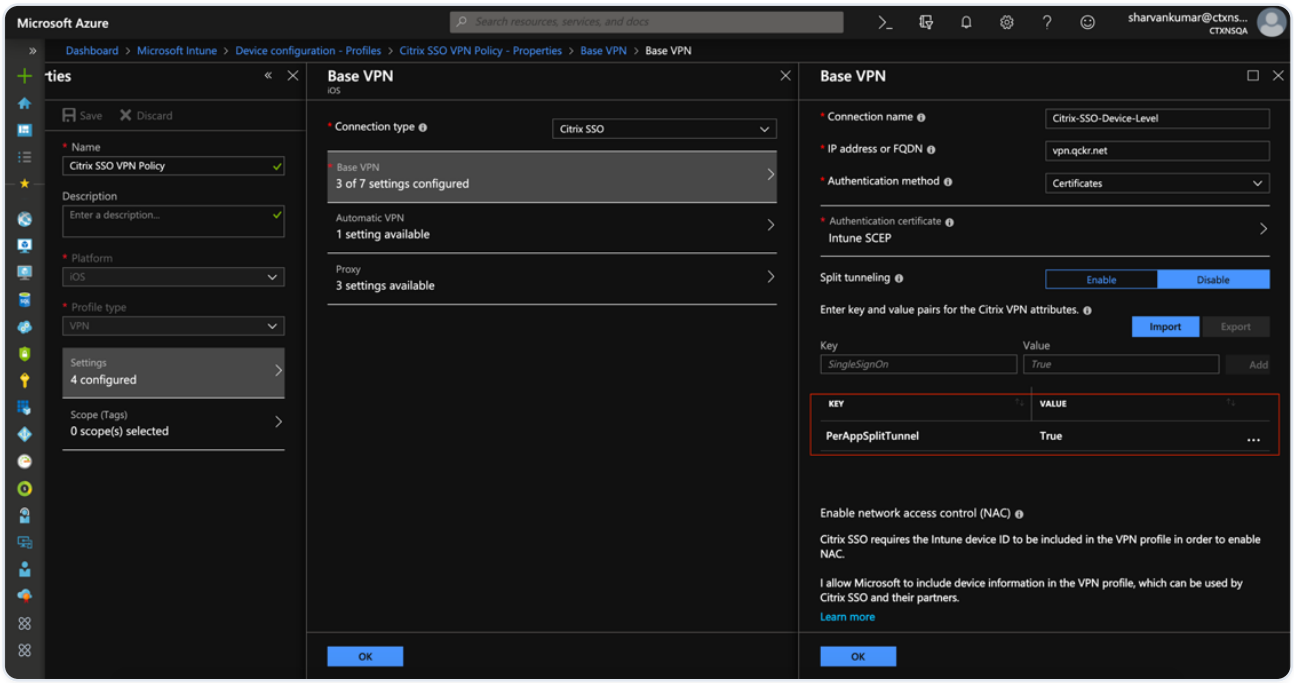
键区分大小写且必须精确匹配，而值不区分大小写。

> **注意：**
>
> 配置供应商配置的用户界面在所有 MDM 供应商中不统一。请联系 MDM 供应商，以在您的 MDM 用户控制台中找到供应商配置部分。

以下是 Citrix Endpoint Management 中配置（供应商特定设置）的示例屏幕截图。



以下是 Microsoft Intune 中配置（供应商特定设置）的示例屏幕截图。



DNS 处理

Citrix Secure Access 客户端的推荐 DNS 设置如下：

- 如果拆分隧道设置为**关闭**，则为**拆分 DNS > 远程**。
- 如果拆分隧道设置为**开启**，则为**拆分 DNS > 两者**。在这种情况下，管理员必须为内网域添加 DNS 后缀。属于 DNS 后缀的 FQDN 的 DNS 查询将通过隧道传输到 NetScaler 设备，其余查询将发送到本地路由器。

> **注意：**
>
> - 建议**DNS 截断修复**标志始终处于**开启**状态。有关详细信息，请参阅 CTX200243。
> - 当拆分隧道设置为**开启**且拆分 DNS 设置为**远程**时，VPN 连接后可能会出现解析 DNS 查询的问题。这与网络扩展框架未拦截所有 DNS 查询有关。

已知问题

问题描述：在每应用 VPN 或按需 VPN 配置中，包含 `".local"` 域的 FQDN 地址的隧道传输。Apple 的网络扩展框架中存在一个错误，该错误阻止了域名部分包含 `.local` 的 FQDN 地址（例如 `<http://wwww.abc.local>`）通过系统的 TUN 接口进行隧道传输。相反，FQDN 地址的流量会通过客户端设备的物理接口发送。此问题仅在每应用 VPN 或按需 VPN 配置中观察到，在系统范围的 VPN 配置中未发现。Citrix 已向 Apple 提交了一份雷达错误报告，Apple 指出，根据 RFC-6762。有关更多详细信息，请参阅 RFC-6762，local 是一个多播 DNS (mDNS) 查询，因此不

是一个错误。然而，Apple 尚未关闭该错误，目前尚不清楚该问题是否会在未来的 iOS 版本中得到解决。

解决方法：作为解决方法，为此类地址分配一个 `non .local` 域名。

限制

- iOS 不支持端点分析 (EPA)。
- 不支持基于端口/协议的拆分隧道。

通过适用于 Mac 的 Citrix Workspace 应用程序自动单点登录 Citrix Secure Access

从适用于 macOS 的 Citrix Secure Access 24.03.1 开始，登录 Citrix Workspace 应用程序可以单点登录 (SSO) 最终用户到 Citrix Secure Access 客户端，建立用户隧道，并无缝提供对 TCP/UDP 应用程序的访问。如果最终用户连接到 Citrix Workspace 应用程序，适用于 macOS 的 Citrix Secure Access 将自动启动，最终用户可以使用单点登录无缝登录。

当最终用户从 Citrix Workspace 应用程序注销时，Citrix Secure Access 会自动注销，无需用户干预。此功能节省了时间，因为最终用户只需登录一个应用程序，从而提供统一的体验。

目前，此功能默认处于禁用状态。

先决条件

1. 最终用户必须使用 Citrix Workspace 应用程序 2402 或更高版本。有关适用于 Mac 的 Citrix Workspace 应用程序安装的详细信息，请参阅 适用于 Mac 的 Citrix Workspace 应用程序。
2. 最终用户必须使用 适用于 macOS 的 Citrix Secure Access 24.03.1 或更高版本。
3. 要通过 MDM 启用此功能，管理员必须使用以下设置：
    - `<key>EnableSecureAccessAutoLogin</key><true/>`

注意事项

- 如果最终用户在此功能启用之前已登录 Citrix Workspace 应用程序，他们必须重新登录，以便 Citrix Workspace 应用程序可以触发对 Citrix Secure Access 客户端的 SSO。
- 当由于超时或手动用户注销等原因从 Citrix Workspace 应用程序注销时，Citrix Secure Access 也会注销，并且用户会话会断开连接（这仅在 Citrix Secure Access 是通过 Citrix Workspace 应用程序自动启动的情况下）。

- 从 Citrix Workspace 应用程序到 Citrix Secure Access 的 SSO 登录仅支持单个主域。不支持在多个域上进行 SSO。
- 如果您通过此功能单点登录到 Citrix Secure Access 后，将 Citrix Workspace 应用程序连接切换到不同的 URL，系统会提示您选择 Citrix Workspace 应用程序连接 URL。

通过适用于 iOS 的 Citrix Workspace 应用程序自动单点登录 Citrix Secure Access

从适用于 iOS 的 Citrix Secure Access 26.03.1 开始，登录 Citrix Workspace 应用程序可以将最终用户单点登录 (SSO) 到 Citrix Secure Access 客户端，建立用户隧道，并无缝提供对 TCP/UDP 应用程序的访问。如果最终用户已连接到 Citrix Workspace 应用程序，则在登录适用于 iOS 的 Citrix Secure Access 上的相同 URL 时，无需提供凭据。

与 Citrix Workspace 应用程序建立活动连接的最终用户可以无缝登录适用于 iOS 的 Citrix Secure Access 应用程序中的相同 URL，而无需提示输入凭据。此功能节省了时间并提供了统一的体验，因为最终用户只需登录一个应用程序。

要启用此功能，请联系 Citrix 支持。

> **注意：**
>
> 从 Citrix Workspace 应用程序注销不会触发从 Citrix Secure Access 应用程序注销。

将用户证书身份作为电子邮件附件发送给 iOS 用户

> **重要提示：**
>
> 适用于 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。

> iOS 上的 Citrix Secure Access 支持使用 NetScaler Gateway 进行客户端证书身份验证。在 iOS 上，证书可以通过以下方式之一交付给 Citrix Secure Access：

- MDM 服务器 - 这是 MDM 客户的首选方法。证书直接在 MDM 管理的 VPN 配置文件上配置。然后，当设备注册到 MDM 服务器时，VPN 配置文件和证书都会推送到已注册的设备。请遵循 MDM 供应商特定的文档来了解此方法。

- 电子邮件 - 非 MDM 客户的唯一方法。在此方法中，管理员将包含用户证书身份（证书和私钥）的电子邮件作为 PCKS#12 文件附件发送给用户。用户需要在其 iOS 设备上配置电子邮件帐户才能接收带附件的电子邮件。然后，该文件可以导入到 iOS 上的 Citrix Secure Access 中。以下部分解释了此方法的配置步骤。

先决条件

- 用户证书 - 具有 .pfx 或 .p12 扩展名的 PKCS#12 身份文件，用于给定用户。此文件包含证书和私钥。
- 在 iOS 设备上配置的电子邮件帐户。
- 在 iOS 设备上安装了 Citrix Secure Access。

配置步骤

1. 重命名用户证书的扩展名/MIME 类型。

   用户证书最常用的文件扩展名是“.pfx”、“.p12”等。这些文件扩展名对于 iOS 平台来说是非标准的，不像 .pdf、.doc 等格式。“.pfx”和“.p12”都被 iOS 系统占用，不能被 Citrix Secure Access 等第三方应用程序占用。因此，Citrix Secure Access 定义了新的扩展名/MIME 类型，称为“.citrixsso-pfx”和“.citrixsso-p12”。管理员必须将用户证书的扩展名/MIME 类型分别从标准的“.pfx”或“.p12”更改为“.citrixsso-pfx”或“.citrixsso-p12” 。要重命名扩展名，管理员可以在命令提示符或终端上运行以下命令。

   视窗 10

   ```
   cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>

   rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-
   pfx
   ```

   macOS

   ```
   cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>

   mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-pfx
   ```

2. 将文件作为电子邮件附件发送。

   带有新扩展名的用户证书文件可以作为电子邮件附件发送给用户。

   收到电子邮件后，用户必须在 Citrix Secure Access 中安装证书。

为适用于 iOS 用户的 Citrix SSO 应用程序或适用于 macOS 用户的 Citrix Secure Access™ 客户端设置代理 PAC 文件

> **重要提示：**
>
> 适用于 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。

适用于 iOS 的 Citrix Secure 应用程序或适用于 macOS 的 Citrix Secure Access 客户端在建立 VPN 隧道后支持自动代理配置（代理 PAC 文件）。管理员可以使用代理 PAC 文件，允许客户端的所有 HTTP 流量通过代理，包括解析主机名。

如何设置代理 PAC 文件

准备一台可以托管代理文件的内部计算机。例如，假设计算机的 IP 为 172.16.111.43，PAC 文件的名称为 proxy.pac。

如果实际代理服务器的 IP 地址为 172.16.43.83 且正在侦听端口 8080，则 proxy.pac 的示例如下：function FindProxyForURL(url, host) { return "PROXY 172.16.43.83:8080"; }

代理 PAC URL 为 `<http://172.16.111.43/proxy.pac>`。假设文件托管在 HTTP 端口 80 上。

有关更多详细信息，请参阅 CTX224235 或 Proxy Auto Configuration for Outbound Proxy support for NetScaler Gateway。

注意：

- 如果分流隧道处于开启状态，请确保托管 PAC 文件的服务器的 IP 地址包含在内网应用程序列表中，以便可以通过 VPN 访问它。
- 从 Citrix Secure Access (macOS/iOS) 登录后，浏览器将开始使用代理 PAC 文件中的规则。如果只提供一个代理规则（如上例所示），则所有 HTTP 或 HTTPS 流量都将路由到内部代理服务器。

为 macOS 用户设置 Citrix Secure Access

> **重要提示：**

> 适用于 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。

> 适用于 macOS 的 Citrix Secure Access 客户端提供了 NetScaler Gateway 提供的同类最佳应用程序访问和数据保护解决方案。您现在可以随时随地安全地访问业务关键型应用程序、虚拟桌面和公司数据。 Citrix Secure Access 是 NetScaler Gateway 的下一代 VPN 客户端，用于从 macOS 设备创建和管理 VPN 连接。Citrix Secure Access 是使用 Apple 的网络扩展 (NE) 框架构建的。Apple 的 NE 框架是一个现代库，其中包含可用于自定义和扩展 macOS 核心网络功能的 API。支持 SSL VPN 的网络扩展可在运行 macOS 10.11+ 的设备上使用。

Citrix Secure Access 在 macOS 上提供完整的移动设备管理 (MDM) 支持。借助 MDM 服务器，管理员现在可以远程配置和管理设备级 VPN 配置文件和每应用 VPN 配置文件。 适用于 macOS 的 Citrix Secure Access 可以从 Mac App Store 安装。

有关适用于 macOS 的 Citrix Secure Access 客户端支持的一些常用功能列表，请参阅NetScaler Gateway 中支持的 Citrix Secure Access 客户端功能。

与 MDM 产品的兼容性

适用于 macOS 的 Citrix Secure Access 与大多数 MDM 提供商兼容，例如 Citrix XenMobile、Microsoft Intune 等。它支持一项称为网络访问控制 (NAC) 的功能，MDM 管理员可以使用该功能在连接到 NetScaler Gateway 之前强制执行最终用户设备合规性。Citrix Secure Access 上的 NAC 需要 MDM 服务器（例如 XenMobile）和 NetScaler Gateway。有关 NAC 的更多信息，请参阅为单因素登录配置 NetScaler Gateway 虚拟服务器的网络访问控制设备检查。

> **注意：**

> 要在没有 MDM 的情况下将 Citrix Secure Access 与 NetScaler Gateway VPN 结合使用，您必须添加 VPN 配置。您可以从 Citrix Secure Access 配置页面在 macOS 上添加 VPN 配置。

为 Citrix Secure Access 配置 MDM 管理的 VPN 配置文件

以下部分介绍了使用 Citrix Endpoint Management™（以前称为 XenMobile）作为示例，为 Citrix Secure Access 配置设备范围和每应用 VPN 配置文件的分步说明。其他 MDM 解决方案在与 Citrix Secure Access 配合使用时可以参考本文档。

> **注意：**

> 本节介绍了基本设备范围和每应用 VPN 配置文件的配置步骤。您还可以通过遵循 Citrix Endpoint Management（以前称为 XenMobile）文档或 Apple 的MDM VPN 有效负载配置来配置按需连接和代理。

设备级 VPN 配置文件

设备级 VPN 配置文件用于设置系统范围的 VPN。来自所有应用程序和服务的流量都根据 NetScaler 中定义的 VPN 策略（例如，全隧道、拆分隧道、反向拆分隧道）通过隧道传输到 NetScaler Gateway。

在 Citrix Endpoint Management 上配置设备级 VPN

执行以下步骤配置设备级 VPN。

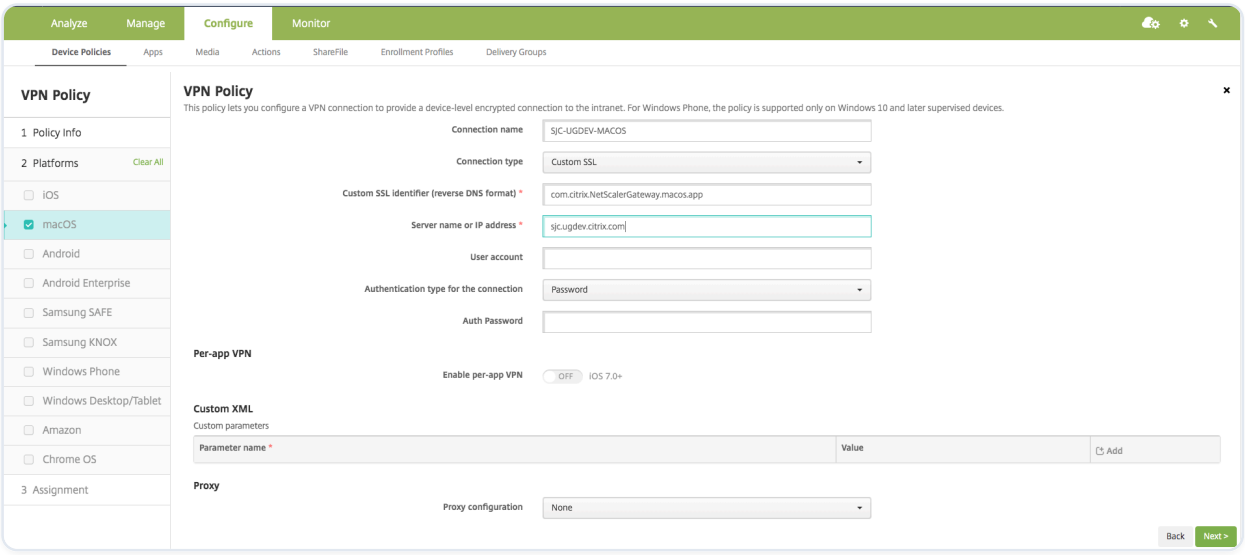
1. 在 Citrix Endpoint Management MDM 控制台上，导航到 **配置** > **设备策略** > **添加新策略**。
2. 在左侧的“策略平台”窗格中选择 **macOS**。在右侧窗格中选择 **VPN Policy**。
3. 在 **Policy Info** 页面上，输入有效的策略名称和描述，然后单击 **Next**。
4. 在 macOS 的 **Policy detail** 页面上，键入有效的连接名称，并在 **Connection Type** 中选择 **Custom SSL**。

   在 MDM VPN 有效负载中，连接名称对应于 **UserDefinedName** 键，并且 **VPN Type Key** 必须设置为 **VPN**。
5. 在 **Custom SSL identifier (reverse DNS format)** 中，输入 **com.citrix.NetScalerGateway.macos.app**。这是 macOS 上 Citrix Secure Access 的捆绑包标识符。

   在 MDM VPN 有效负载中，自定义 SSL 标识符对应于 **VPNSubType** 键。
6. 在 **Provider bundle identifier** 中输入 **com.citrix.NetScalerGateway.macos.app.vpnplugin**。这是 Citrix Secure Access 客户端二进制文件中包含的网络扩展的捆绑包标识符。

   在 MDM VPN 有效负载中，提供程序捆绑包标识符对应于 **ProviderBundleIdentifier** 键。
7. 在 **Server name or IP address** 中，输入与此 Citrix Endpoint Management 实例关联的 NetScaler 的 IP 地址或 FQDN。

   配置页面中的其余字段是可选的。这些字段的配置可在 Citrix Endpoint Management 文档中找到。
8. 单击 **Next**。



9. 单击**保存**。

每应用 VPN 配置文件

每应用 VPN 配置文件用于为特定应用程序设置 VPN。只有来自特定应用程序的流量会通过隧道传输到 NetScaler Gateway。**每应用 VPN 有效负载支持设备范围 VPN 的所有**密钥以及其他一些密钥。

在 Citrix Endpoint Management 上配置每应用级别 VPN

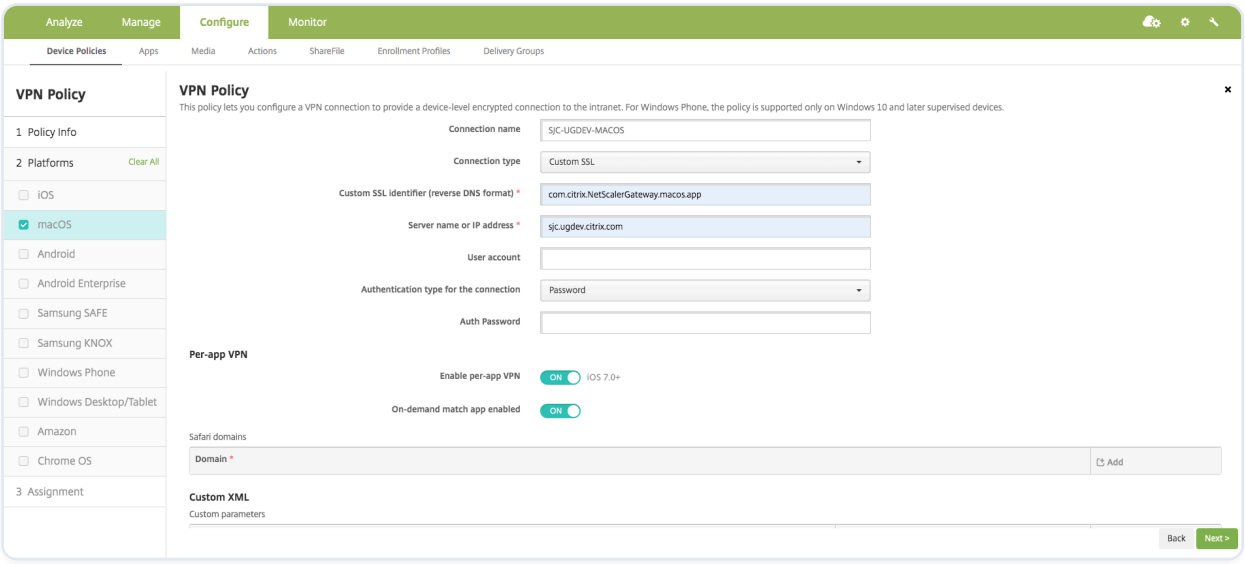
执行以下步骤以在 Citrix Endpoint Management 上配置每应用 VPN：

1. 完成 Citrix Endpoint Management 上的设备级别 VPN 配置。
2. 在**每应用 VPN**部分中，将**启用每应用 VPN**开关设置为“开”。
3. 如果 Citrix Secure Access 必须在启动匹配应用程序时自动启动，请将**按需匹配应用程序启用**开关设置为“开”。这适用于大多数每应用场景。

   在 MDM VPN 有效负载中，此字段对应于密钥 **OnDemandMatchAppEnabled**。
4. Safari 域配置是可选的。配置 Safari 域后，当用户启动 Safari 并导航到与**域**字段中的 URL 匹配的 URL 时，Citrix Secure Access 会自动启动。如果您想限制特定应用程序的 VPN，则不建议这样做。

   在 MDM VPN 有效负载中，此字段对应于密钥 **SafariDomains**。

   配置页面中的其余字段是可选的。这些字段的配置可在 Citrix Endpoint Management（以前称为 XenMobile®）文档中找到。



5. 单击**下一步**。
6. 点击“**保存**”。

   要将 VPN 配置文件与设备上的特定应用程序关联，您必须创建应用程序清单策略和凭据提供程序策略。

在每应用 VPN 中配置拆分隧道

MDM 客户可以在 Citrix Secure Access 的每应用 VPN 中配置拆分隧道。必须将以下键/值对添加到在 MDM 服务器上创建的 VPN 配置文件的供应商配置部分。

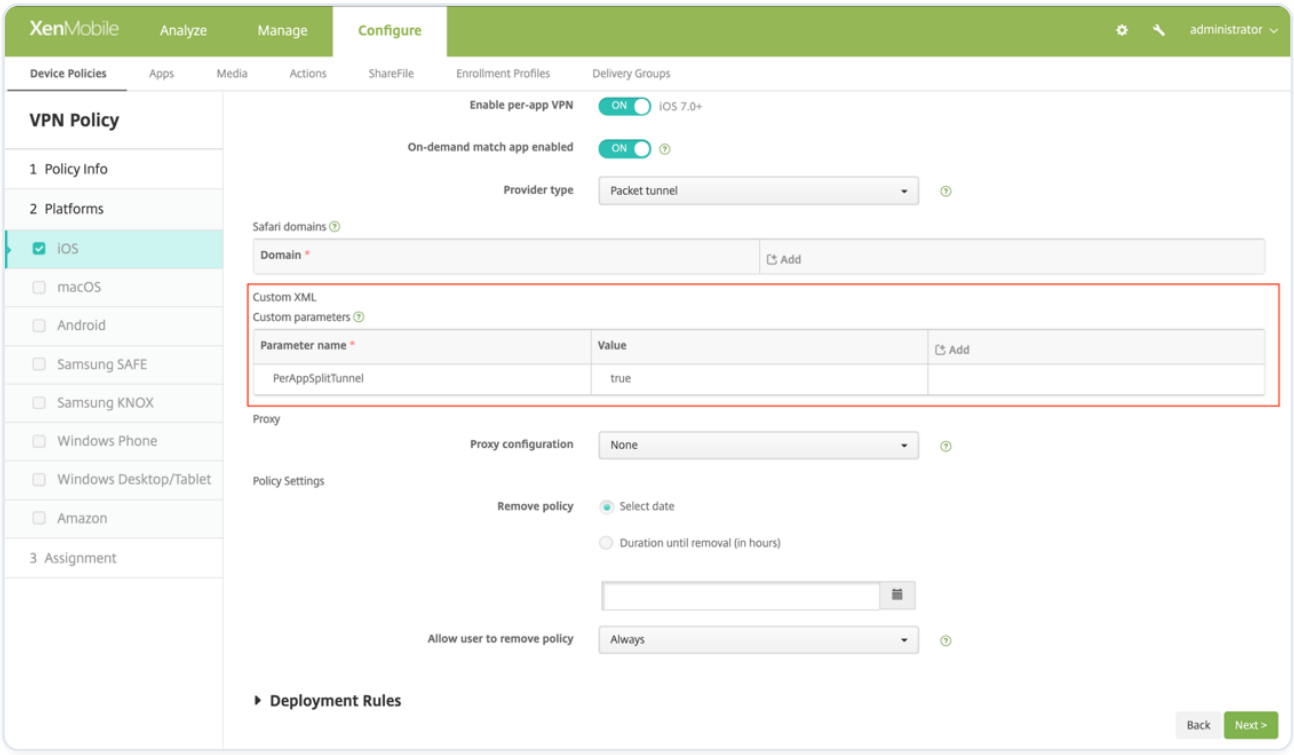
```
-  Key = "PerAppSplitTunnel"

-  Value = "true or 1 or yes"
```

键区分大小写且必须完全匹配，而值不区分大小写。

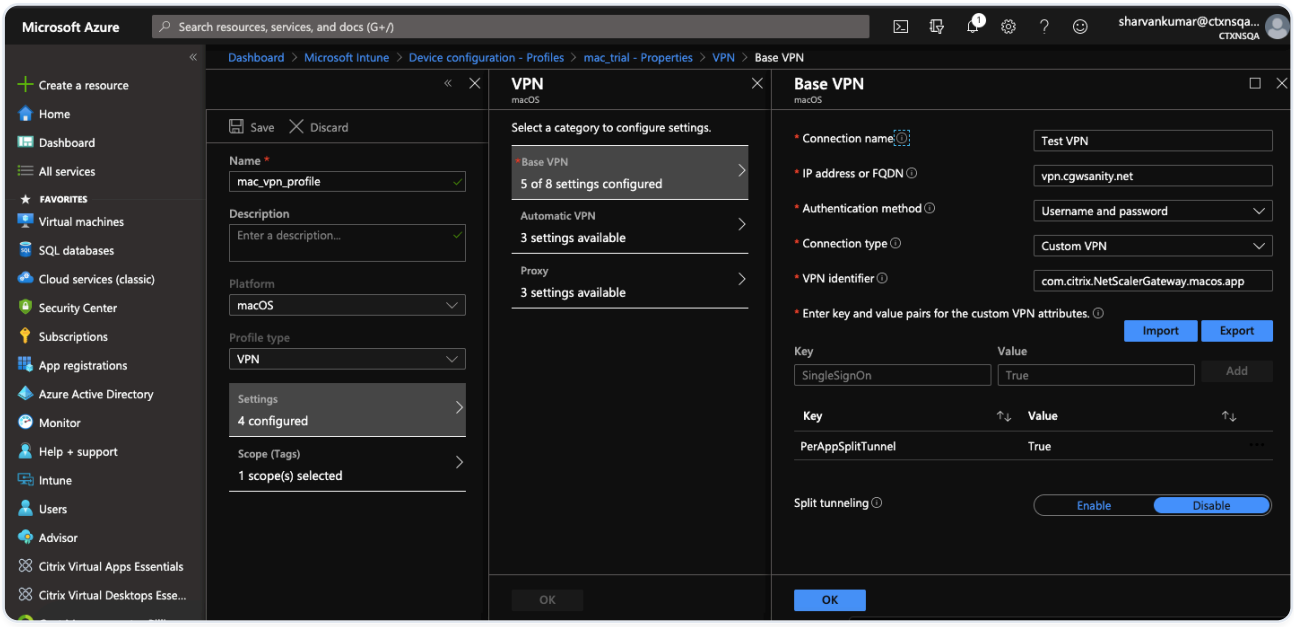
> **注意：**

> 配置供应商配置的用户界面在不同的 MDM 供应商之间不尽相同。请联系 MDM 供应商，以在您的 MDM 用户控制台中找到供应商配置部分。

> 以下是 Citrix Endpoint Management 中配置（供应商特定设置）的示例屏幕截图。



以下是 Microsoft Intune 中配置（供应商特定设置）的示例屏幕截图。



禁用用户创建的 VPN 配置文件

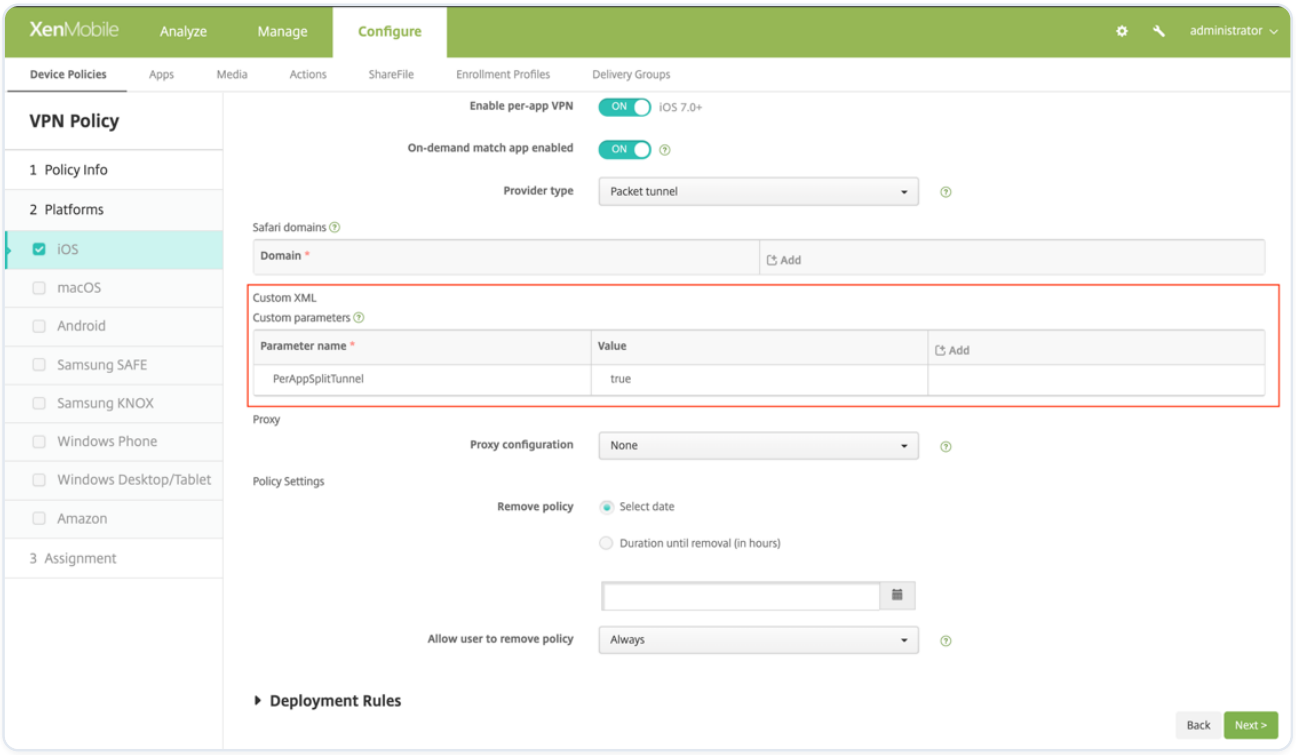
MDM 客户可以阻止用户在 Citrix Secure Access 中手动创建 VPN 配置文件。为此，必须将以下键/值对添加到在 MDM 服务器上创建的 VPN 配置文件的供应商配置部分。

```
-  Key = "disableUserProfiles"

-  Value = "true or 1 or yes"
```

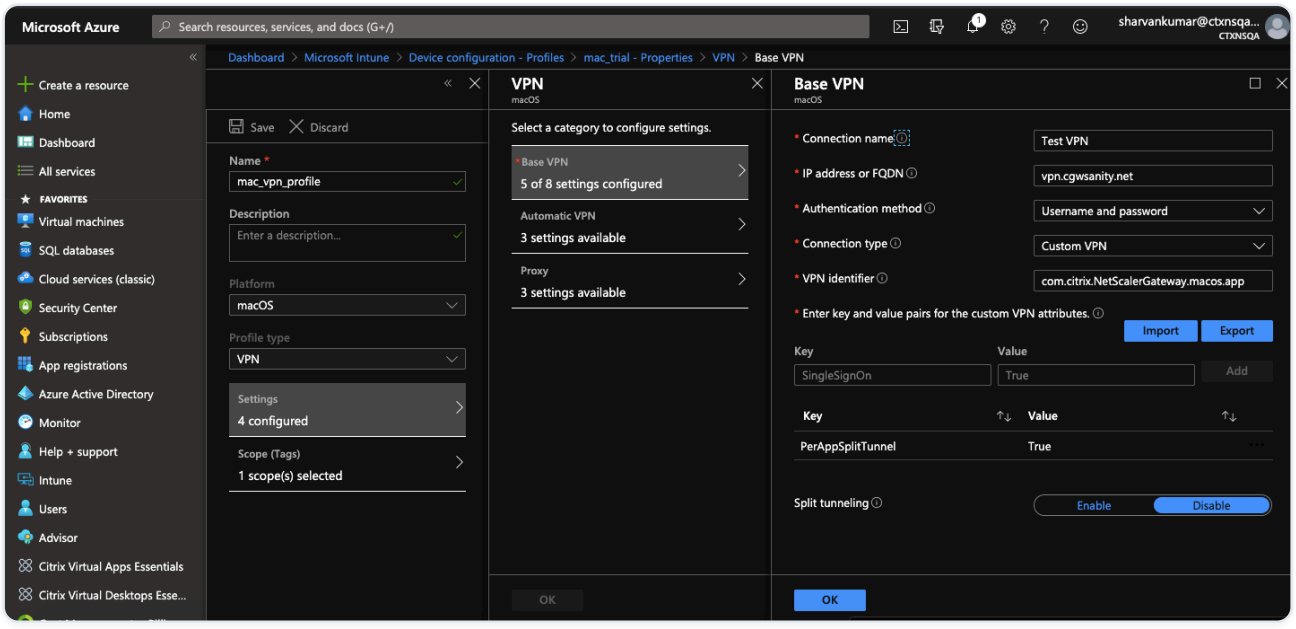
键区分大小写且必须完全匹配，而值不区分大小写。

> **注意：**
>
> MDM 供应商配置的用户界面在不同 MDM 供应商之间不尽相同。请联系 MDM 供应商，以在您的 MDM 用户控制台中找到供应商配置部分。

以下是 Citrix Endpoint Management 中配置（供应商特定设置）的示例屏幕截图。



以下是 Microsoft Intune 中配置（供应商特定设置）的示例屏幕截图。



DNS 处理

Citrix Secure Access 的推荐 DNS 设置如下：

- 如果分流隧道设置为 **OFF**，则为 **拆分 DNS > 远程**。
- 如果分流隧道设置为 **ON**，则为 **拆分 DNS > 两者**。在这种情况下，管理员必须为内网域添加 DNS 后缀。属于 DNS 后缀的 FQDN 的 DNS 查询将通过隧道传输到 NetScaler 设备，其余查询将发送到本地路由器。

> **注意：**
>
> - 建议始终将 **DNS 截断修复** 标志设置为 **ON**。有关更多详细信息，请参阅 CTX200243。
> - 当分流隧道设置为 **ON** 且拆分 DNS 设置为 **远程** 时，VPN 连接后解析 DNS 查询可能会出现问题。这与网络扩展框架未拦截所有 DNS 查询有关。

支持的 EPA 扫描

有关支持的扫描的完整列表，请参阅 最新 EPA 库。

1. 在 **OPSWAT v4 支持的扫描矩阵** 部分中，单击 **MAC OS 特定** 列下的 **支持的应用程序列表**。
2. 在 Excel 文件中，单击“**经典 EPA 扫描**”选项卡以查看详细信息。

已知问题

以下是当前已知问题。

- 如果用户被置于隔离组中，EPA 登录将失败。
- 未显示强制超时警告消息。
- 如果分流隧道处于开启状态且未配置任何内网应用程序，Citrix Secure Access 允许登录。

限制

以下是当前限制。

- 由于沙盒限制了对 Secure Access 的访问，以下 EPA 扫描可能会失败。
  - 硬盘加密“类型”和“路径”
  - Web 浏览器“默认”和“正在运行”
  - 补丁管理“缺失补丁”

    - EPA 期间的终止进程操作

- 不支持基于端口/协议的分流隧道。
- 确保密钥链中没有两个名称和过期日期相同的证书，因为这会导致客户端只显示其中一个证书而不是两个。

故障排除

如果最终用户在 Citrix Secure Access 的身份验证窗口中看到 **下载 EPA 插件** 按钮，则表示 NetScaler 设备上的内容安全策略正在阻止调用 URL `com.citrix.agmacepa://`。管理员必须修改内容安全策略，以允许 `com.citrix.agmacepa://`。

macOS/iOS 上 Citrix Secure Access 客户端的 nFactor 支持

> **重要提示：**

> 适用于 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。

> 多重身份验证 (nFactor) 要求用户提供多个身份证明才能获得访问权限，从而增强了应用程序的安全性。管理员可以配置不同的身份验证因素，包括客户端证书、LDAP、RADIUS、OAuth、SAML 等。这些身份验证因素可以根据组织的需要以任何顺序配置。

macOS/iOS 上的 Citrix Secure Access 客户端支持以下身份验证协议：

- **nFactor** – 当身份验证虚拟服务器绑定到网关上的 VPN 虚拟服务器时，使用 nFactor 协议。由于身份验证因素的顺序是动态的，因此客户端使用在应用程序上下文中呈现的浏览器实例 (WebView) 来显示身份验证 GUI。
- **经典** – 如果在网关上的 VPN 虚拟服务器上配置了经典身份验证策略，则经典协议是默认的回退协议。如果需要 NAC 检查，客户端也会将经典协议用于 nFactor 身份验证。
- **Citrix 身份平台** – Citrix 身份平台协议用于向 CloudGateway 或 Citrix Gateway 服务进行身份验证，并且需要通过 Citrix Cloud 进行 MDM 注册。

下表总结了每个协议支持的各种身份验证方法。

身份验证方法	NFACTOR	经典	CITRIX 身份提供商
客户端证书	支持	支持	不支持

身份验证方法	NFACTOR	经典	CITRIX 身份提供商
LDAP	支持	支持	不支持

注意：

*nFactor 身份验证与网络访问控制 (NAC) 检查在以下条件下运行：

- 当 nFactor 身份验证策略包含 NAC 检查时，适用于 iOS 的 Citrix Secure Access 客户端将使用经典身份验证协议，而不是基于 WebView 的身份验证。
- 不支持需要通过 WebView 收集凭据的身份验证策略。相反，适用于 iOS 的 Citrix Secure Access 客户端会显示一个旧版对话框来收集用户凭据。
- 对于 Intune NAC 检查，请确保所有必需的身份验证因素（例如一个或两个密码）都在一个步骤中收集。配置登录架构策略，以便在初始身份验证提示期间提示并收集所有必要的因素。

nFactor 配置

有关配置 nFactor 的详细信息，请参阅 配置 nFactor 身份验证。

重要提示：

要在 macOS/iOS 上将 nFactor 协议与 Citrix Secure Access 客户端配合使用，建议的 NetScaler Gateway 本地版本为 12.1.50.xx 及更高版本。

限制

- 移动设备特定的身份验证策略（例如 NAC（网络访问控制））要求客户端在与 NetScaler Gateway 身份验证时发送签名的设备标识符。签名的设备标识符是一个可旋转的密钥，用于唯一标识在 MDM 环境中注册的移动设备。此密钥嵌入在由 MDM 服务器管理的 VPN 配置文件中。可能无法将此密钥注入 WebView 上下文。如果在 MDM VPN 配置文件中启用了 NAC，则适用于 iOS 的 Citrix Secure Access 客户端会自动回退到经典身份验证协议。
- 您无法为 macOS 配置 Intune 的 NAC 检查，因为 Intune 不提供为 macOS 启用 NAC 的选项，这与 iOS 不同。

macOS 和 iOS 客户端的日志收集

macOS 客户端的日志收集

适用于 macOS 的 Citrix Secure Access 客户端为最终用户提供了多种选项，包括检查客户端日志并与开发团队共享。这些选项允许最终用户执行以下操作：

- 查看和检查实时日志
- 将日志通过电子邮件发送给开发团队
- 压缩日志并与开发团队共享
- 清除以前存储的日志

日志收集支持多个会话，不限于当前会话。

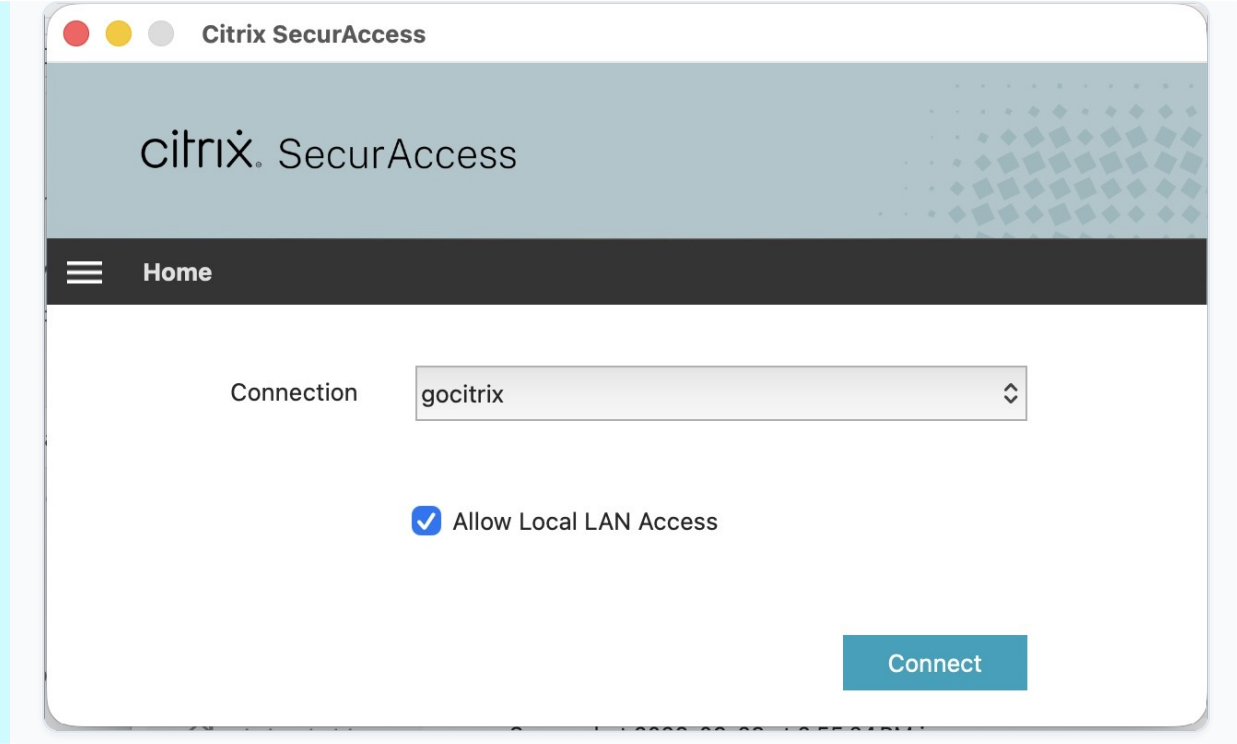
对于 macOS 客户端，由于应用程序和 VPN 扩展是独立运行的，因此日志以两种类型的文件收集：

- **nsgControllerApp.log：** 收集 Citrix Secure Access 应用程序工作流的所有日志。
- **nsg_vpnextension_process-pid_Date-time_file_number.log：** 收集网络扩展的所有日志。新文件时，`file_number` 增加 1。

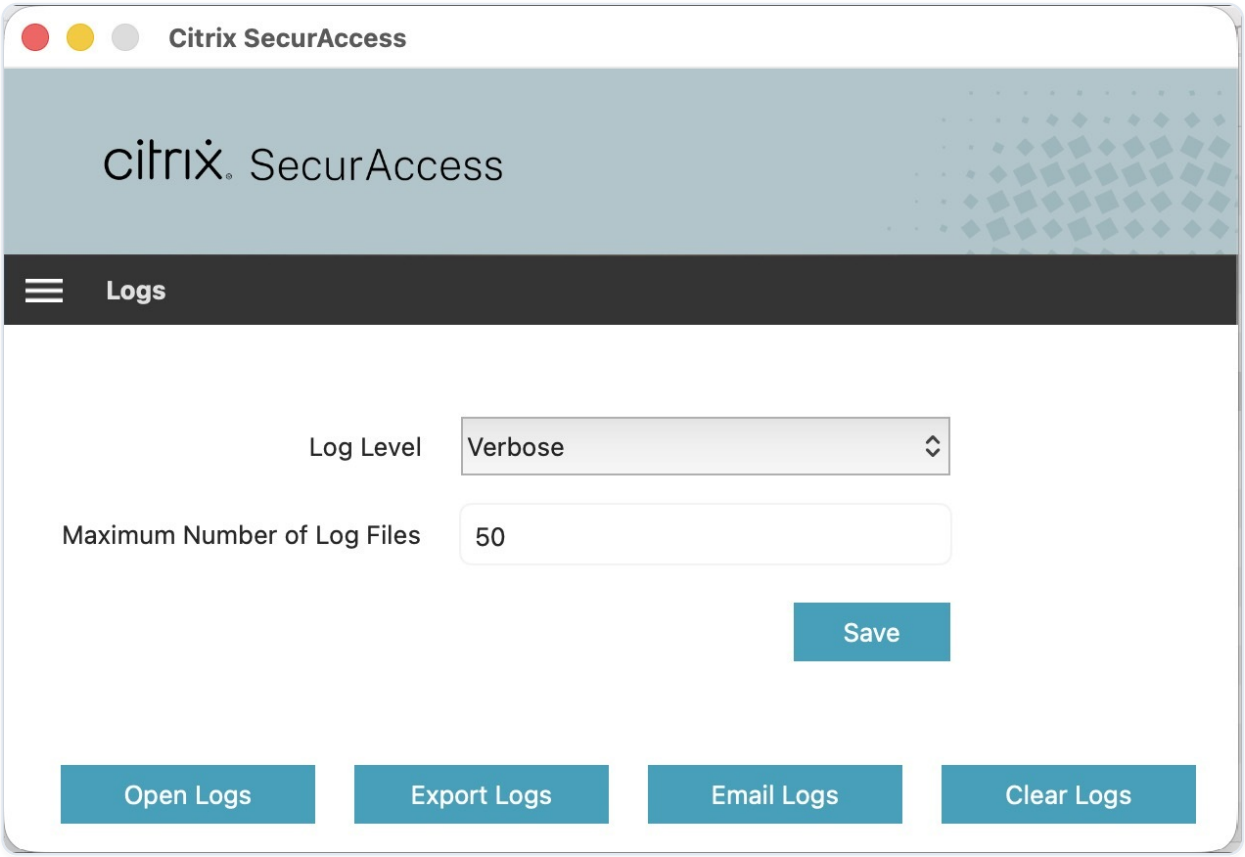
使用 GUI 配置日志记录

1. 单击“**主页**”屏幕上的汉堡图标，然后选择“**日志**”菜单以访问日志屏幕。

> **注意：**
>
> 只有当用户添加至少一个配置或服务器 URL 后，汉堡图标才可用。



2. 所有与日志相关的配置都可以在“**日志**”屏幕中完成。



- **日志级别：** 以下三个日志级别可供选择：
  - **错误**：仅记录应用程序报告的异常或故障。
  - **调试消息**：此级别包括调试消息和与程序执行相关的事件。

    - **详细**：此级别包括由“**错误**”和“**信息**”日志级别报告的所有日志消息以及可能有助于故障排除的其他消息。

- **最大日志文件数：** 输入要添加用于日志收集的文件数。此选项是强制性的。
- **打开日志：** 选择此选项后，最新的应用程序和扩展日志文件将在控制台中打开。
- **通过电子邮件发送日志：** 使用邮件应用程序将日志文件通过电子邮件发送到注册的电子邮件 ID。将打开一封新邮件，其中包含一个附件 `ta.gz` 文件。
- **导出日志：** 选择此选项后，所有已创建的日志文件都将压缩并保存到当前用户的 `Downloads` 文件夹中。zip 文件名类似于 `citrixsso-20251127-120843-logs.tar.gz` 。
- **清除日志：** 选择此选项后，除最新的 `nsgControllerApp.log` 文件外，所有已创建的日志文件都将被清除。

iOS 客户端的日志收集

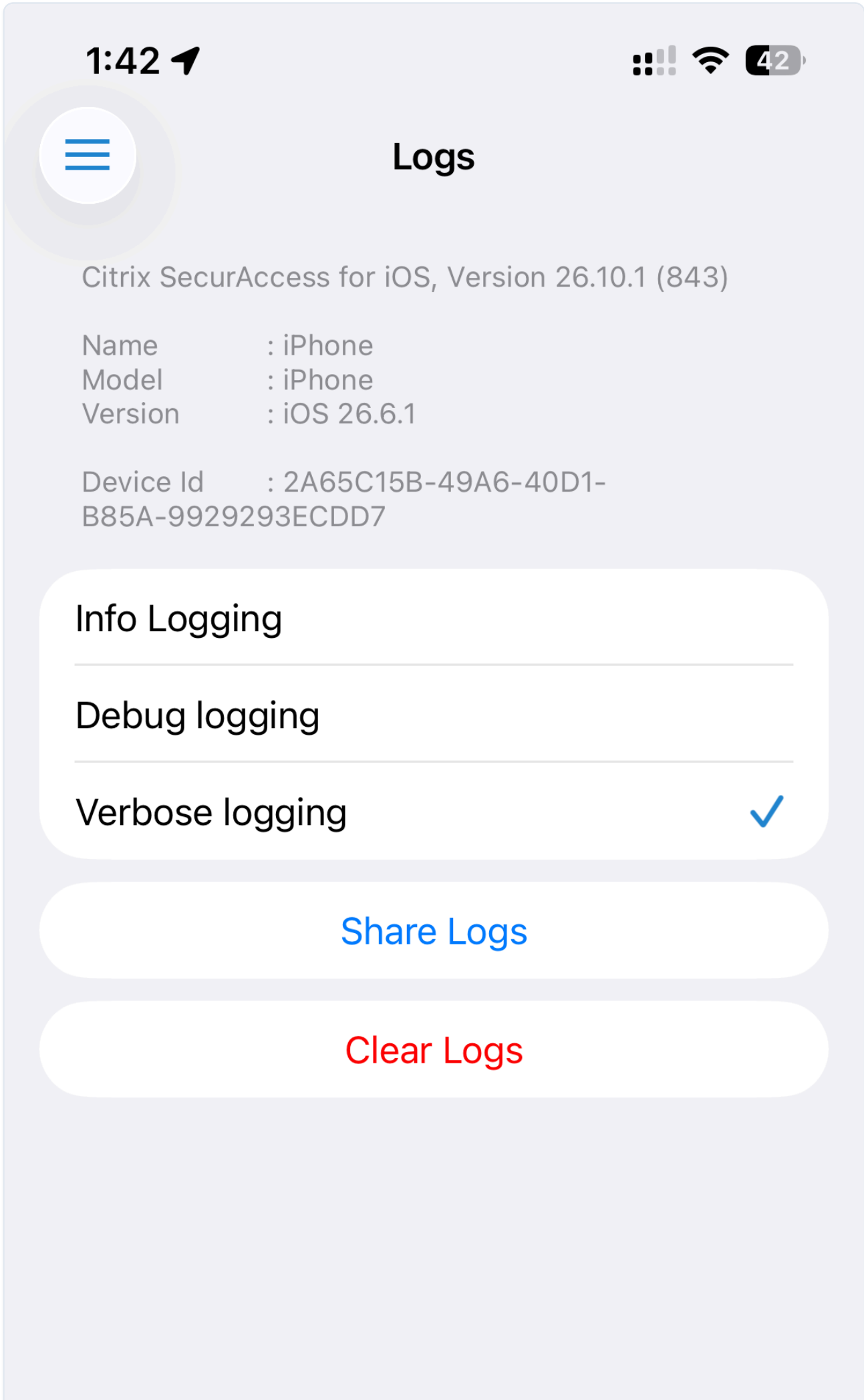
适用于 iOS 的 Citrix Secure Access 客户端为最终用户提供了不同的日志记录选项，例如：

- 共享日志
- 清除日志

对于 iOS 客户端，`Log` 文件夹包含应用程序和扩展的单独日志：

- **nsgControllerApp.log：** 收集 Citrix Secure Access 应用程序工作流的所有日志。
- **nsg_vpnextension_process-pid_Date-time_file_number.log：** 收集网络扩展的所有日志。新文件时 file_number 增加 1。

点击汉堡图标并选择“**日志**”以查看可用选项。

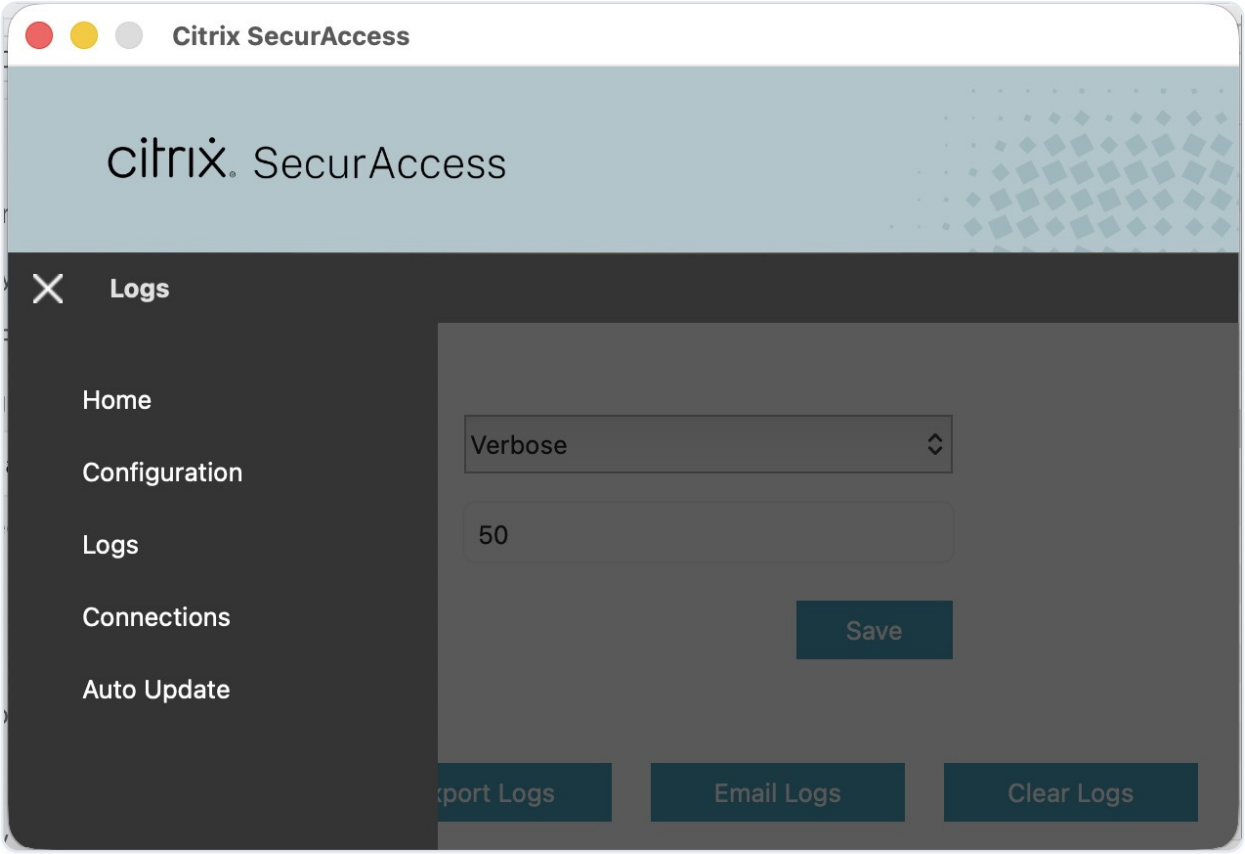

1:42
42
Logs
Citrix SecurAccess for iOS, Version 26.10.1 (843)
Name : iPhone
Model : iPhone
Version : iOS 26.6.1
Device Id : 2A65C15B-49A6-40D1-B85A-9929293ECDD7
Info Logging
Debug logging
Verbose logging
Share Logs
Clear Logs

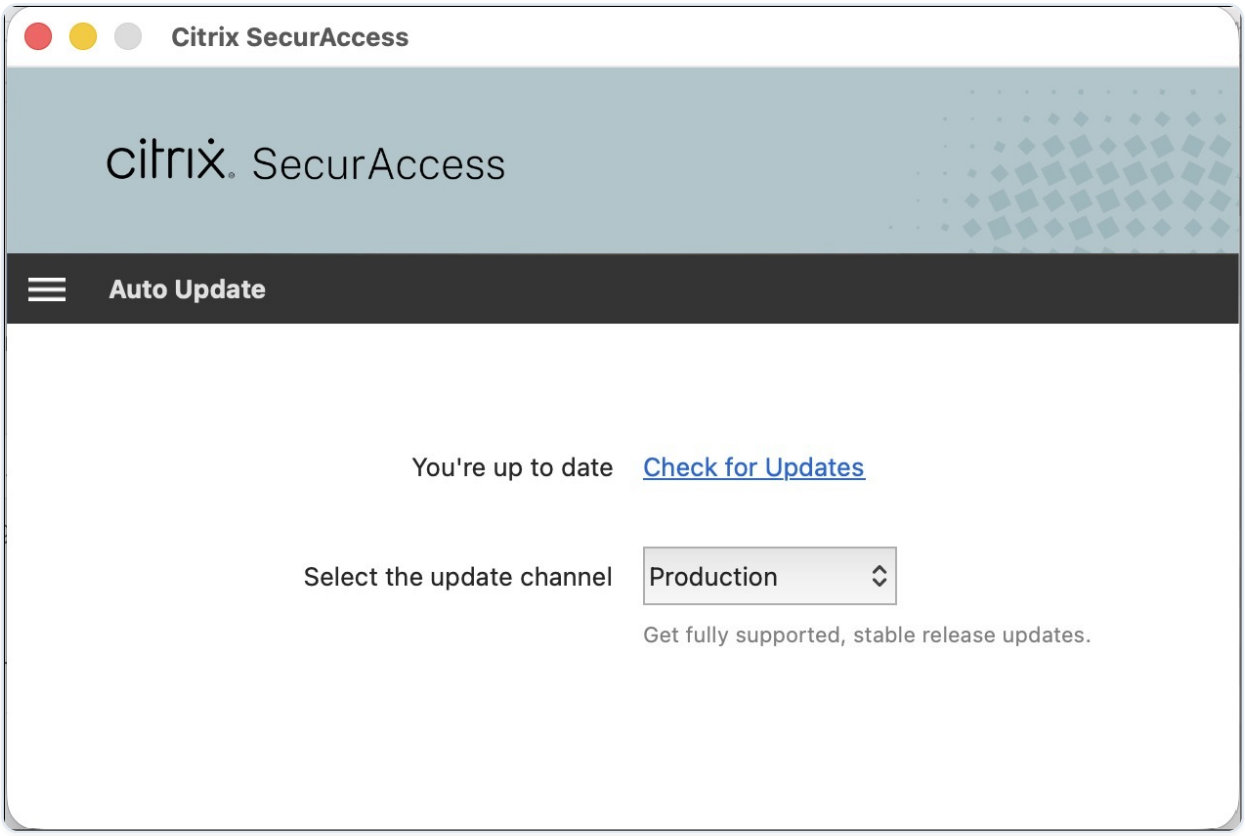
- **选择日志级别：** 以下三个日志级别可供选择：
  - **错误日志记录**：仅记录应用程序报告的异常或故障。
  - **调试日志记录**：此级别包括调试消息和与程序执行相关的事件。
  - **详细日志记录**：此级别包括由“**错误**”和“**信息**”日志级别报告的所有日志消息以及其他可能有助于故障排除的消息。
- **共享日志：** 点击此菜单时，设备会打开多个共享日志的选项，例如 AirDrop 和邮件。除了此选项，日志 zip 文件还可以保存到 `Files` 或复制。如果选择“**邮件**”选项，日志 zip 文件将作为附件添加到新邮件中并可以发送。
- **清除日志：** 点击此菜单时，现有日志文件将被清除。

macOS 自动更新支持

从版本 26.01.1.1 开始，适用于 macOS 的 Citrix Secure Access 应用程序包含自动更新功能，该功能提供以下功能：

- 定期检查是否有可用更新。
- 通知用户后自动更新应用程序。

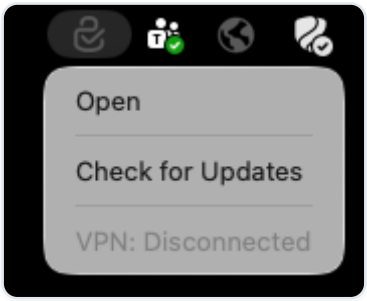




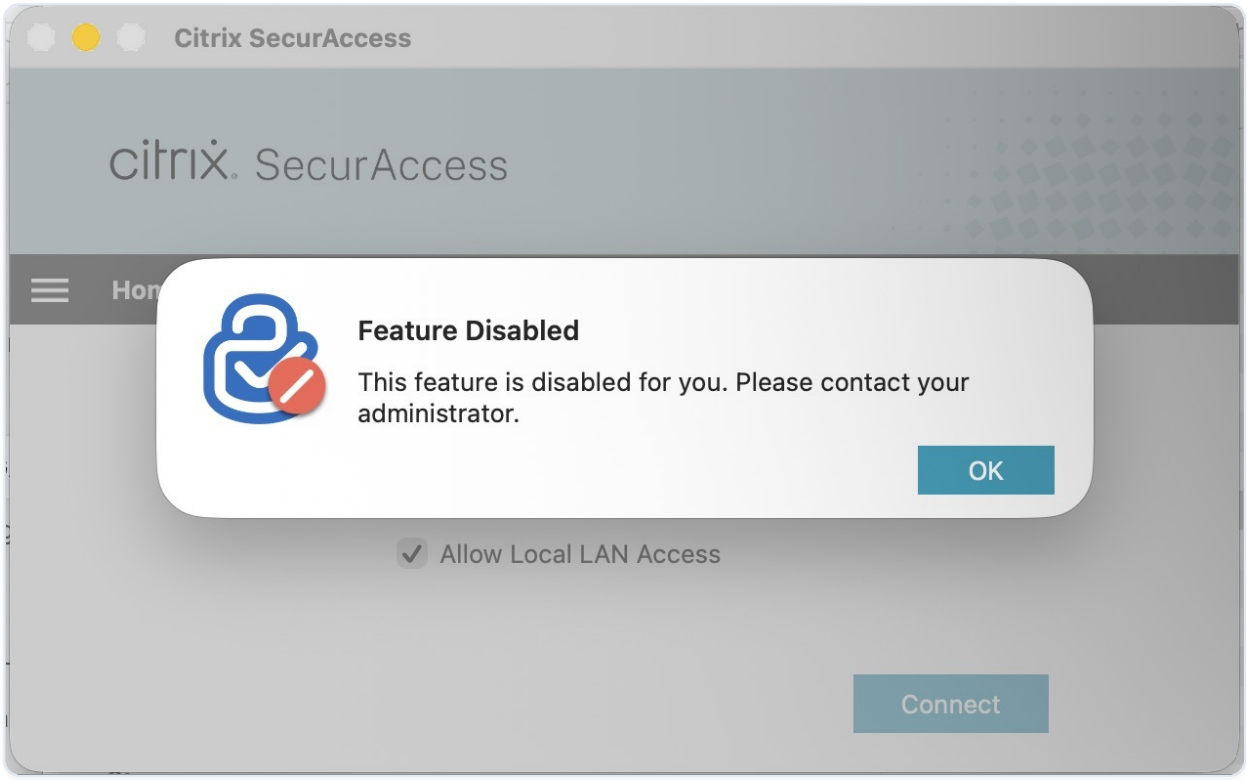
> **注意：**
>
> 自动更新功能仅在生产渠道中可用。

最终用户选项

- 最终用户还可以通过菜单栏中的“**检查更新**”选项手动检查更新并安装更新。



- 汉堡菜单中的“**自动更新**”选项对最终用户禁用。当最终用户单击该选项时，将显示消息“**功能已禁用**”。



解决 macOS/iOS 版 Citrix Secure Access 的常见问题

> **重要提示：**

> 适用于 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。

DNS 解析问题

- 如果设备进入睡眠状态或长时间不活动，VPN 可能需要大约 30-60 秒才能恢复。在此期间，用户可能会看到一些 DNS 请求失败。DNS 请求会在短时间后自动解决。 如果 DNS 查询无法解析，则可能是高级授权策略正在阻止 DNS 流量。请参阅 CTX232237 以解决此问题。
- 始终从浏览器检查 DNS 解析。从终端使用 `nslookup` 命令进行的 DNS 查询可能不准确。如果必须使用 `nslookup` 命令，则必须在命令中包含客户端 IP 地址。例如，`nslookup website_name 172.16.255.1.`.

EPA 问题

- Gatekeeper 被视为防病毒软件。如果存在检查“任何防病毒软件”(MAC-ANTIVIR_0_0) 的扫描，即使用户未安装任何其他供应商的防病毒软件，扫描也始终通过。

注意：

- 启用客户端安全日志记录以获取 EPA 的调试日志。您可以通过将 VPN 参数 `clientsecurityLog` 设置为 ON 来启用客户端安全日志记录。
- Apple 内置的补丁管理软件是“软件更新”。它对应于设备上的“App Store”应用。“软件更新”的版本必须类似于 `"MAC-PATCH_100011_100076_VERSION_==_3.0[COMMENT: Software Update]"`
- 始终保持 NetScaler 上的 EPA 库为最新。最新的库可在 EPA 库 找到。

nFactor 问题

- Citrix Secure Access 会打开 **Citrix SSO 身份验证**窗口进行 nFactor 身份验证。它类似于浏览器。如果此页面上出现错误，可以通过在 Web 浏览器上尝试身份验证来交叉验证。
- 如果启用 nFactor 时传输登录失败，请将门户主题更改为“RFWebUI”。
- 如果您收到错误“无法建立到 NetScaler Gateway 的安全连接，因为证书链不包含任何必需的证书。请联系您的管理员”或“网关不可达”，则可能是网关服务器证书已过期，或者服务器证书绑定时启用了 SNI。Citrix Secure Access 尚不支持 SNI。请在绑定服务器证书时禁用 SNI。此错误也可能是由于 MDM VPN 配置文件中配置了证书锁定，并且 NetScaler Gateway 提供的证书与锁定的证书不匹配。
- 尝试连接到网关时，如果**Citrix SSO 身份验证窗口**打开但为空白，请检查 ECC 曲线 (ALL) 是否已绑定到默认密码组。ECC 曲线 (ALL) 必须绑定到默认密码组。

网络访问控制 (NAC) 检查

NAC 身份验证策略仅在经典身份验证中受支持。它不作为 nFactor 身份验证的一部分受支持。

常见问题

> **重要提示：**
>
> 适用于 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。

> 本节介绍了适用于 macOS/iOS 的 Citrix Secure Access 的常见问题。

适用于 macOS/iOS 的 Citrix Secure Access 客户端与 VPN 应用程序有何不同？ 适用于 macOS 的 Citrix Secure Access 客户端和适用于 iOS 的 Citrix Secure Access 客户端（以前称为适用于 iOS 的 Citrix SSO）是 NetScaler 的下一代 SSL VPN 客户端。该应用程序使用 Apple 的网络扩展框架在 iOS 和 macOS 设备上创建和管理 VPN 连接。Citrix VPN 是使用 Apple 私有 VPN API 的旧版 VPN 客户端，这些 API 现已弃用。App Store 不再支持 Citrix VPN。

什么是 NE？ Apple 的网络扩展 (NE) 框架是一个现代库，其中包含可用于自定义和扩展 iOS 和 macOS 核心网络功能的 API。网络 扩展（支持 SSL VPN）可在运行 iOS 9+ 和 macOS 10.11+ 的设备上使用。

适用于 macOS/iOS 的 Citrix Secure Access 客户端与哪些版本的 NetScaler 兼容？ 适用于 macOS/iOS 的 Citrix Secure Access 客户端中的 VPN 功能在 NetScaler 10.5 及更高版本上受支持。TOTP 在 NetScaler 12.0 及更高版本上可用。NetScaler 上的推送通知尚未公开发布。该应用程序需要 iOS 9+ 和 macOS 10.11+ 版本。

非 MDM 客户的基于证书的身份验证如何工作？ 以前通过电子邮件或浏览器分发证书以在 VPN 中执行客户端证书身份验证的客户在使用适用于 macOS/iOS 的 Citrix Secure Access 客户端时必须注意此更改。这主要适用于不使用 MDM 服务器分发用户证书的非 MDM 客户。

什么是网络访问控制 (NAC)？如何为 iOS 和 NetScaler Gateway 配置 Citrix Secure Access 的 NAC？ Microsoft Intune 和 Citrix Endpoint Management™（以前称为 XenMobile）MDM 客户可以利用适用于 iOS 的 Citrix Secure Access 中的网络访问控制 (NAC) 功能。借助 NAC，管理员可以通过为由 MDM 服务器管理的移动设备添加额外的身份验证层来保护其企业内部网络。管理员可以在适用于 iOS 的 Citrix Secure Access 中进行身份验证时强制执行设备合规性检查。

要将 NAC 与适用于 iOS 的 Citrix Secure Access 结合使用，您必须在 NetScaler Gateway 和 MDM 服务器上启用它。

- 要在 NetScaler 上启用 NAC，请参阅 为单因素登录配置 NetScaler Gateway 虚拟服务器的网络访问控制设备检查。
- 如果 MDM 供应商是 Intune，请参阅 Microsoft Learn Challenge 页面中的“网络访问控制 (NAC) 与 Intune 集成”。
- 如果 MDM 供应商是 Citrix Endpoint Management（以前称为 XenMobile），请参阅 网络访问控制。

> **注意：**
>
> 适用于 macOS/iOS 的 Citrix Secure Access 客户端的最低支持版本为 1.1.6 及更高版本。

适用于 Linux 的 Citrix Secure Access 客户端

适用于 Linux 的 Citrix Secure Access 客户端是一款 VPN 客户端软件，使用户能够远程访问公司数据和应用程序。Citrix Secure Access 客户端可保护应用程序免受未经授权的访问、应用程序级威胁和基于浏览器的攻击。

Citrix 端点分析 (EPA) 客户端是一款客户端软件，可在通过 NetScaler Gateway 授予对公司数据的访问权限之前检查端点条件。Citrix EPA 客户端和 Citrix Secure Access 客户端彼此独立。

> **注意：**
>
> 即使您不使用 EPA，我们也建议您同时更新 EPA 和 VPN 插件二进制文件，以防您以后选择使用 EPA 功能。

支持的 Linux 版本

Citrix Secure Access 客户端和 Citrix EPA 客户端与 Ubuntu 22.04 和 24.04 版本以及 eLux 和 IGEL OS 兼容。有关支持的浏览器的更多信息，请参阅系统要求。

> **注意事项：**
>
> - 我们建议您使用适用于 Linux 的 Citrix Secure Access 客户端版本 24.8.5 或更高版本。
> - 适用于 Linux 的 Citrix Secure Access 客户端版本 24.11.4 及更高版本支持 eLux OS。
> - 对于 Ubuntu 22 及更高版本，要与 Citrix Secure Access 客户端和 Citrix EPA 客户端配合使用，请在 VPN 虚拟服务器上启用 TLS 1.3。如果仅启用了 TLS 1.2，则在 CLI 上将 SSL 参数 `denySSLReneg` 设置为 `NONSECURE`。
> - 从 Citrix Secure Access 客户端版本 25.8.1 开始，对 Ubuntu 20.04 的支持已弃用。

- NetScaler Gateway 上的“**Linux 插件升级**”和“**EPA Linux 升级**”设置与适用于 Linux 的 Citrix Secure Access 客户端一起使用时不支持“**基本**”选项。有关详细信息，请参阅用户如何使用 Citrix Secure Access 客户端连接和创建虚拟服务器。
- 对于 eLux 和 IGEL OS，以下是 NetScaler Gateway 中的推荐配置：
  - **全局配置：** 将“**Linux 插件升级**”设置为“**从不**”。有关详细信息，请参阅用户如何使用 Citrix Secure Access 客户端连接。
  - **会话配置文件：** 将 **Linux 插件升级** 设置为“**从不**”。有关详细信息，请参阅 配置 Citrix Secure Access 客户端的会话配置文件。
  - **会话配置文件：** 将 **Linux 插件升级** 设置为“**从不**”。有关详细信息，请参阅 配置 Citrix Secure Access 客户端的会话配置文件。
  - **虚拟服务器：** 将 **EPA 插件升级** 设置为“**从不**”。有关详细信息，请参阅 创建虚拟服务器。
- 对于使用经典身份验证的部署，NetScaler Gateway 会话配置文件中的 **Linux 插件升级** 设置不受支持。有关详细信息，请参阅 配置 Citrix Secure Access 客户端的会话配置文件。

支持的功能

适用于 Ubuntu 的 Citrix Secure Access 客户端支持以下功能：

- 拆分隧道和反向拆分隧道
- 隧道传输 TCP、UDP 和 ICMP 应用程序
- 通过内网 IP (IIP) 发起的服务器连接
- 拆分 DNS 远程
- 客户端代理
- 经典 EPA 扫描
- 高级身份验证 (nFactor)，包括高级 EPA 扫描
- 仅限 HTTP 的 Cookie
- 全局服务器负载平衡 (GSLB)

Citrix Secure Access 客户端的网络配置

适用于 Linux 的 Citrix Secure Access 客户端使用管理员必须注意的特定网络配置：

- 防火墙标记：`0xc5a00001` 和 `0xc5a00002`
- 自定义路由表：ID `221`，名称为 `csa`

> **重要提示：**
>
> 如果这些防火墙标记和路由表 ID 在其他应用程序中使用，则可能会与 Citrix Secure Access 客户端发生冲突。

在 NetScaler Gateway 上升级 Ubuntu 客户端

您可以从 下载 页面下载适用于 Ubuntu 的 Citrix Secure Access 客户端和 Citrix EPA 客户端。

Citrix Secure Access 客户端和 Citrix EPA 客户端分别命名为“nsgclient18_64.deb”和“nsepa18.deb”。这些客户端与 Ubuntu 20.04 兼容。

支持 Ubuntu 22.04 和 24.04 的 Citrix Secure Access 客户端和 Citrix EPA 客户端分别命名为“nsginstaller64.deb”和“nsepa.deb”。

例如，如果您想将 Citrix Secure Access 客户端从 1.0.0.x 版本升级到 23.6.1 版本：

1. 使用 shell 提示符替换位置 `/var/netscaler/gui/vpn/scripts/linux/` 处的“nsgclient18_64.deb”和“nsginstaller64.deb”文件。
2. 使用 shell 提示符替换位置 `/var/netscaler/gui/epa/scripts/linux/` 处的“nsepa18.deb”和“nsepa.deb”文件。
3. 打开 `/var/netscaler/gui/vpn/scripts/linux/clientversions.xml` 文件。

```
a.  For the Citrix EPA client, replace the current version (1.0.0.x) in
the following XML tags with the latest version (23.6.1). If the XML
tags do not exist, add them to the XML file. For example,



replace



`<component pkgname="nsepa18" currentversion="1.0.0.x"
minversion="1.0.0.x" ostype="ubuntu64" minkernelversion="0"
maxkernelversion="100" updatetype="compatible" action="/epa/scripts/
```

linux/nsepa18.deb" />`

with

`<component pkgname="nsepa18" currentversion="23.6.1" minversion="23.6.1" ostype="ubuntu64" minkernelversion="0" maxkernelversion="100" updatetype="compatible" action="/epa/scripts/linux/nsepa18.deb" />`

and replace

`<component pkgname="nsepa22" currentversion="1.0.0.x" minversion="1.0.0.x" ostype="ubuntu64" minkernelversion="0" maxkernelversion="100" updatetype="compatible" action="/epa/scripts/linux/nsepa.deb" />`

with

`<component pkgname="nsepa22" currentversion="23.6.1" minversion="23.6.1" ostype="ubuntu64" minkernelversion="0" maxkernelversion="100" updatetype="compatible" action="/epa/scripts/linux/nsepa.deb" />`

b. For the Citrix Secure Access client, replace the current version (1.0.0.x) in the following XML tags with the latest version (23.6.1). If the XML tags do not exist, add them to the XML file. For example,

replace

```
`<component pkgname="nsgclient18" currentversion="1.0.0.x"
minversion="1.0.0.x" ostype="ubuntu64" minkernelversion="3.0"
maxkernelversion="5.16" updatetype="compatible" action="/vpn/scripts/
linux/nsgclient18_64.deb" />`


to


`<component pkgname="nsgclient18" currentversion="23.6.1"
minversion="23.6.1" ostype="ubuntu64" minkernelversion="3.0"
maxkernelversion="5.16" updatetype="compatible" action="/vpn/scripts/
linux/nsgclient18_64.deb" />`


and


`<component pkgname="nsgclient22" currentversion="1.0.0.x"
minversion="1.0.0.x" ostype="ubuntu64" minkernelversion="3.0"
maxkernelversion="5.20" updatetype="compatible" action="/vpn/scripts/
linux/nsginstaller64.deb" />`


to


`<component pkgname="nsgclient22" currentversion="23.6.1"
minversion="23.6.1" ostype="ubuntu64" minkernelversion="3.0"
maxkernelversion="5.20" updatetype="compatible" action="/vpn/scripts/
linux/nsginstaller64.deb" />`
```

4. 在 NetScaler shell 提示符下，运行以下命令：

```
rm -rf /netscaler/ns_gui

ln -s /var/netscaler/gui /netscaler/ns_gui
```

5. 在 NetScaler CLI 上，运行以下命令：

```
set vpn parameter -clientversions all

flush cache contentgroup loginstaticobjects
```

参考资料

- Ubuntu 支持的端点分析扫描。
- 最终用户帮助文档。
- 最终用户帮助文档。

发行说明

适用于 Linux 的 Citrix Secure Access 客户端和 Citrix 端点分析 (EPA) 客户端现在独立发布，并与所有 NetScaler 版本兼容。Citrix Secure Access 客户端版本遵循 YY.MM Release.Build 格式。

发行说明描述了新功能、对现有功能的增强、已修复的问题和已知问题。

新增功能：当前版本中可用的新功能和增强功能。

已修复的问题：当前版本中已修复的问题。

已知问题：当前版本中存在的问题以及适用的解决方法。

有关支持功能的详细信息，请参阅 支持的功能。

25.8.2 (Sep 15, 2025)

重要更新：

- Citrix Secure Access 25.8.2 版本取代了 25.8.1 版本，现已正式发布。

新增功能

- **超时设置支持**

  适用于 Linux 的 Citrix Secure Access 客户端现在支持在 NetScaler Gateway 和 Citrix SecurAccess ZTNA 部署中配置的超时设置。有关详细信息，请参阅 配置超时设置 和 用户会话超时。

- **支持多工作区 URL**

  适用于 Linux 的 Citrix Secure Access 客户端现在支持多工作区 URL。此功能对于必须为不同用户组（例如人力资源、IT、承包商或供应商）提供不同访问 URL 的企业非常有用。有关更多信息，请参阅配置工作区 URL。

已修复的问题

- 如果在 NetScaler Gateway 中配置了经典身份验证，用户将无法登录 Citrix Secure Access 客户端。

25.5.3 (May 19, 2025)

> **重要更新：**
>
> - Citrix Secure Access 25.5.3 版本取代了 25.5.1 版本，现已正式发布。

新增功能

- **PoP 故障期间的无缝连接**

  在 Citrix SecurAccess ZTNA 部署中，如果 Citrix Secure Access 客户端用户与当前接入点 (PoP) 的连接丢失，他们将自动重新连接到备用接入点 (PoP)。此故障转移是无缝发生的，无需任何用户操作。

- **Citrix Secure Access 客户端和 Citrix EPA 客户端支持 Ubuntu 24.04**

  Citrix Secure Access 和 Citrix EPA 客户端现在与 Ubuntu 24.04 兼容。

- **支持 Microsoft Entra ID 条件访问身份验证**

Citrix Secure Access 客户端支持使用 Microsoft Edge 浏览器进行 Microsoft Entra ID 条件访问身份验证。

执行以下步骤，将 Citrix Secure Access 客户端配置为使用 Microsoft Edge 浏览器进行 Microsoft Entra ID 身份验证：

先决条件：

最终用户的设备上必须安装 Microsoft Edge 浏览器。

> **注意：**
>
> 仅当身份验证的 **Entra ID with conditional access** 设置为 **Allow only registered devices** 时，才必须进行以下配置更改。

a. 使用管理员权限打开文件 `/opt/Citrix/NSGClient/globalConfiguration.json`。
b. 将 `enable_edge_browser_auth` 的值更改为 `true`。
c. 要使 `globalConfiguration.json` 中的更改生效，请重新启动 Citrix Secure Access 客户端。
d. 关闭 Microsoft Edge 浏览器的所有窗口。

已知问题

- 如果未安装 EPA 客户端，通过 NetScaler 将 Citrix Secure Access 客户端从版本 25.5.3 自动升级到更高版本可能会失败，并导致“签名错误”。

  解决方法： 直接从 Citrix 下载 页面下载并安装 Citrix Secure Access 客户端版本 25.8.1 或更高版本。

25.2.2 (Feb 24, 2025)

新增功能

- **支持在 Citrix SecurAccess ZTNA 中实现持久且一致的连接**

  Citrix Secure Access 客户端支持连接器粘性以及客户端 IP 地址粘性，以确保在 Citrix SecurAccess ZTNA 部署中需要会话连续性的应用程序能够获得持久且一致的连接。有关详细信息，请参阅 维护一致的连接。

- **在 Citrix SecurAccess ZTNA 和 NetScaler Gateway 部署中支持拆分 DNS**

  Citrix Secure Access 客户端支持在 Citrix SecurAccess ZTNA 和 NetScaler Gateway 本地部署中拆分 DNS。

- **支持来自 Citrix SecurAccess ZTNA 的服务器发起的连接**

  适用于 Linux 的 Citrix Secure Access 客户端现在支持来自 Citrix SecurAccess ZTNA 的服务器发起的连接。此功能使管理员能够创建应用程序，允许服务器向远程端点发起 TCP 连接。有关详细信息，请参阅 支持服务器到客户端的连接。

- **支持在 Citrix SecurAccess ZTNA 部署中进行故障排除**

  Citrix Secure Access 客户端现在支持通过使用 Citrix Monitor 或 Citrix Director 在 Citrix SecurAccess ZTNA 部署中进行故障排除。

24.11.4 (Dec 03, 2024)

新增功能

- **与第三方安全 Web 网关的互操作性增强**

  Citrix Secure Access 用户代理字符串已更新，以增强与第三方安全 Web 网关的互操作性。

- **支持分类和排查枚举失败**

  Citrix Secure Access 现在支持在 SecurAccess ZTNA 部署中使用 Citrix Monitor 或 Citrix Director 对枚举失败进行分类和故障排除。有关详细信息，请参阅 SecurAccess ZTNA 与 Director 集成（预览版）。

- **基于 TCP 的 DNS 请求的 IP 地址欺骗**

  Citrix Secure Access 在以下场景中支持基于 TCP 的 DNS 请求的 IP 地址欺骗：

  - 在 NetScaler Gateway 上配置了基于 FQDN 的隧道规则。
  - FQDN 与 Citrix SecurAccess ZTNA 部署中应用程序配置的 DNS 后缀或主机名匹配。

24.10.1 (Oct 07, 2024)

新增功能

- **支持基于 FQDN 的隧道**

适用于 Linux 的 Citrix Secure Access 客户端支持在 SecurAccess ZTNA 和 NetScaler Gateway 本地部署中针对 TCP 和 UDP 应用程序的基于 FQDN 的隧道。有关详细信息，请参阅在会话配置文件中配置连接设置。

> **注意：**
>
> - 基于 FQDN 的隧道支持拆分隧道 **ON** 和拆分隧道 **OFF** 设置，但不支持拆分隧道 **REVERSE** 设置。
> - DNS 解析仅支持拆分 DNS **远程** 设置，并通过隧道执行，无论 NetScaler® Gateway 的拆分 DNS 设置如何。

已修复的问题

- 即使在用户从 Citrix Secure Access 客户端注销后，客户端会话也可能在 NetScaler Gateway 和服务节点上保持活动状态。

24.8.5 (Sep 02, 2024)

新增功能

- **支持 SecurAccess ZTNA 部署**

  适用于 Linux 的 Citrix Secure Access 支持在 Citrix SecurAccess ZTNA 的本地和云部署中基于 IP 地址的 TCP/UDP 应用程序。

  > **注意：**
  >
  > 基于 IP 地址的 TCP/UDP 应用程序支持 Ubuntu 18.04、Ubuntu 20.04。Ubuntu 22.04 不支持它们。

- **支持 nFactor 身份验证**

  适用于 Linux 的 Citrix Secure Access 现在直接通过 VPN 客户端支持 nFactor 身份验证。当用户登录适用于 Linux 的 Citrix Secure Access 时，将出现一个 Web 视图窗口，提示他们根据管

理员配置的 nFactor 流程进行身份验证。有关 nFactor 身份验证的详细信息，请参阅 nFactor 身份验证。

已修复的问题

- 如果 NetScaler Gateway 上配置的 EPA 表达式长度超过 1024 个字符，则 EPA 扫描将失败。
- 在 Citrix Secure Access 客户端 UI 中，当达到 NetScaler Gateway 会话的最大限制时，“选择要传输的会话”部分无法显示传输登录会话列表。

23.10.3 (2023 年 10 月 16 日)

已修复的问题

对于法国用户，适用于 Linux 的 Citrix Secure Access UI 的“连接”页面以 KB 和 MB 显示数据传输速率，而不是 Ko 和 Mo。

23.9.1 (2023 年 9 月 8 日)

新增功能

此版本解决了有助于提高整体性能和稳定性的问题。

23.6.2 (20-Jun-2023)

新增功能

- **Citrix Secure Access 客户端和 Citrix EPA 客户端支持 Ubuntu 22.04**

  Ubuntu 22.04 是 Ubuntu 的最新长期支持版本。Citrix Secure Access 和 Citrix EPA 客户端与 Ubuntu 22.04 兼容。有关详细信息，请参阅客户端软件要求。

- **Citrix Secure Access 和 Citrix EPA 客户端支持 GSLB**

  适用于 Ubuntu 的 Citrix Secure Access 客户端和 Citrix EPA 客户端支持 NetScaler Gateway 上的全局服务器负载平衡 (GSLB) 功能。通过为 NetScaler Gateway 配置 GSLB，管理员可以确保企业网络（内部网资源）始终可供来自任何地理位置的最终用户使用。GSLB 还可以解决灾难情况或网络中断，在这种情况下，一个数据中心的用户可以重定向到另一个数据中心。有关详细信息，请参阅支持 NetScaler Gateway 上的主动-主动 GSLB 部署。

- **Citrix Secure Access 和 Citrix EPA 客户端支持 HTTPOnly**

  Citrix Secure Access 和 Citrix EPA 客户端支持身份验证 Cookie 上的 HTTPOnly 标志。NetScaler Gateway 管理员在 Web 应用程序生成的身份验证 Cookie 上配置 HTTPOnly 功能。此功能有助于防止因跨站点脚本攻击而导致的 Cookie 窃取。有关详细信息，请参阅在身份验证 Cookie 上强制执行 HttpOnly 标志。

支持带条件访问的 Microsoft Entra ID 身份验证

从适用于 Linux 版本 25.5.1 的 Citrix Secure Access 客户端开始，Microsoft Edge 浏览器支持带条件访问的 Microsoft Entra ID 身份验证。

执行以下步骤，将 Citrix Secure Access™ 客户端配置为使用 Microsoft Edge 浏览器进行 Microsoft Entra ID 身份验证：

先决条件：

最终用户的设备上必须安装 Microsoft Edge 浏览器。

> **注意：**

> 仅当身份验证的 **Entra ID with conditional access** 设置为 **Allow only registered devices** 时，才需要进行以下配置更改。

1. 使用管理员权限打开文件 `/opt/Citrix/NSGClient/globalConfiguration.json`。
2. 将 `enable_edge_browser_auth` 的值更改为 `true`。
3. 要使 `globalConfiguration.json` 中的更改生效，请重新启动 Citrix Secure Access 客户端。
4. 关闭 Microsoft Edge 浏览器的所有窗口。

思杰安全访问 Android 版

适用于 Android 的 Citrix Secure Access（以前称为 Citrix SSO）提供 NetScaler Gateway 提供的业界最佳应用程序访问和数据保护解决方案。您现在可以随时随地安全地访问业务关键型应用程序、虚拟桌面和公司数据。

重要提示：

- 适用于 Android 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。
- 适用于 Android 的 Citrix Secure Access 客户端可在基于 ChromeOS 构建的 Android 子系统内运行。如果从 Play 商店安装为 Android 应用程序，它可与 ChromeOS 配合使用，并可隧道传输 Android 子系统内的任何应用程序。

发行说明

重要提示：

- 适用于 Android 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。在此过渡期间，您可能会在文档中看到 Citrix SSO 的引用。
- 基于 FQDN 的拆分隧道和 nFactor 身份验证支持目前处于预览阶段。
- Citrix Secure Access 在 2025 年 5 月之后将不再支持 Android 11 及更低版本。

Citrix Secure Access 发行说明描述了服务版本中可用的新功能、现有功能的增强、已修复的问题和已知问题。发行说明包含以下一个或多个部分：

新增功能：当前版本中可用的新功能和增强功能。

已修复的问题：当前版本中已修复的问题。

已知问题：当前版本中存在的问题及其适用的解决方法。

V26.08.1 (Sep 08, 2026)

新增功能

- **已移除对 Android 12 及更早版本的支持**

  Citrix Secure Access 应用程序不再支持 Android 12 及更早版本。

- **支持 Android 16/17 SDK 要求**

  Citrix Secure Access 应用程序现在支持 Android 16/17 SDK 要求。

- **允许在 Android 17 及更高版本上访问本地网络**

  当用户在 Android 17 及更高版本上安装、重新安装或更新 Citrix Secure Access 应用程序时，系统会提示他们允许访问本地网络。如果拒绝访问，则 VPN 会话开始时，某些本地网络服务（例如 Wi-Fi 打印机）可能不可用。

  建议 MDM 管理员预先授予 Citrix Secure Access 应用程序此权限。 有关详细信息，请参阅如何从 Android 设备使用 Citrix Secure Access。

V26.06.1 (Jun 23, 2026)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V26.04.1 (Apr 28, 2026)

新增功能

- **Citrix Secure Access 与适用于 Android 的 Citrix Workspace 应用程序之间的单点登录**

  从适用于 Android 的 Citrix Secure Access 26.04.1 版开始，支持与 Citrix Workspace 应用程序 (CWA) 进行单点登录 (SSO)。如果用户已登录 Citrix Workspace 应用程序，则在登录适用于 Android 的 Citrix Secure Access 中的相同 URL 时，无需再次输入凭据，反之亦然。

  此外，如果用户从 Citrix Secure Access 应用程序注销，则用户也会从 Citrix Workspace 应用程序注销，反之亦然。此行为可实现对 TCP/UDP 应用程序的无缝访问，并提供统一的 SecurAccess ZTNA 体验。此注销同步默认启用。要禁用此功能，请联系 Citrix 支持。有关详细信息，请参阅通过适用于 Android 的 Citrix Workspace 应用程序单点登录 Citrix Secure Access。

V26.01.1 (Feb 02, 2026)

已修复问题

- 将内网 IP 分配给设备的始终开启 VPN 可能会间歇性地进入持续重新连接循环。
- Citrix Secure Access 应用程序在应用程序重启后不会记住上次使用的选项卡。
- Citrix Secure Access 应用程序在处理分段 UDP 流量时可能会崩溃。
- 如果 NetScaler Gateway 上的 VPN 会话配置文件中的主页设置为 `none`，Citrix Secure Access 应用程序将无法建立 VPN 会话。

V25.11.1 (Dec 08, 2025)

新增功能

- **支持强制超时通知**

  如果在 NetScaler Gateway 上配置，Citrix Secure Access 应用程序现在会显示强制超时警告通知。有关详细信息，请参阅配置超时设置。

- **支持 Android 15 SDK 要求**

  Citrix Secure Access 应用程序现在支持 Android 15 SDK 要求。对于运行 Android 15 及更高版本的设备，已移除对 TLS 1.0 和 TLS 1.1 的支持。

- **支持 SecurAccess ZTNA**

  适用于 Android 的 Citrix Secure Access 客户端现在支持 SecurAccess ZTNA 部署。它为 TCP/UDP 应用程序提供基本隧道。如果通过客户端会话不允许访问任何 TCP/UDP 应用程序，则在为 Citrix Secure Access 应用程序启用通知权限的情况下，应用程序会通知您。

  在 Citrix Secure Access 应用程序中添加连接时，必须使用 StoreFront 基本 URL。有关添加连接的更多信息，请参阅如何从 Android 设备使用 Citrix Secure Access。

  相关主题

  - Citrix SecurAccess ZTNA 中支持的 Citrix Secure Access 客户端功能
  - 适用于移动设备的 Citrix SecurAccess ZTNA

V25.07.1 (Oct 14, 2025)

新增功能

- **已移除对 Android 11 及更早版本的支持**

  Citrix Secure Access 应用程序不再支持 Android 11 及更早版本。

- **使用 Google Play 应用签名增强签名验证**

  Citrix Secure Access 客户端应用程序现在使用 Google Play 应用签名来增强签名验证。

V25.03.3 (Jun 30, 2025)

已修复的问题

- 升级到版本 25.03.1 后，Citrix Secure Access 客户端可能无法重新建立 Always On VPN 连接，并显示错误消息“Always-On VPN 不支持交互式用户身份验证”。

V25.03.2 (Jun 13, 2025)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V25.03.1 (May 28, 2025)

新增功能

- **支持定期监控 Always On VPN 模式**

  现在增加了对 Always On VPN 模式的定期监控支持，以确保如果 Citrix Secure Access 客户端因 Google Play 服务更新而终止，它将自动重新启动。

已修复的问题

- 在始终开启 VPN 模式下，如果网关名称使用循环 DNS 负载平衡方法解析为多个 IP 地址，Citrix Secure Access 应用程序可能会反复尝试重新连接到 VPN。

V25.02.1 (Mar 19, 2025)

已修复的问题

- 如果 DNS 响应包含 CNAME 记录，用户可能无法通过 Citrix Secure Access 应用程序使用 FQDN 访问内部网应用程序。
- 在始终开启 VPN 模式下，当设备进入空闲或省电模式时，Citrix Secure Access 客户端可能无法在无需手动干预的情况下重新启动 VPN 会话。

V24.11.1 (Dec 02, 2024)

新增功能

- **支持 Android 14 SDK 要求**

  Citrix Secure Access 应用程序现在支持 Android 14 SDK 要求。

- **支持按应用程序语言设置**

  Citrix Secure Access 应用程序现在支持按应用程序语言系统设置。

已修复问题

- 即使启用了 Always On VPN，Citrix Secure Access 应用程序也可能会显示传输登录提示。

V24.10.1 (Oct 10, 2024)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

已修复问题

- 推送通知可能无法在适用于 Android 的 Citrix Secure Access 客户端上运行。
- 在会话空闲超时后，Always On 功能可能无法重新启动 NetScaler Gateway 会话。

V24.08.2 (Sep 26, 2024)

新增功能

- 此版本解决了一些问题，以提高整体性能和稳定性。

V24.08.1 (Sep 09, 2024)

新增功能

- **与第三方安全 Web 网关的互操作性增强**

  Citrix Secure Access 的 User-Agent 字符串已更新，以增强与第三方安全 Web 网关的互操作性。有关详细信息，请参阅定义客户端。

- **Citrix Secure Access Android 应用程序中的增强安全功能**

  当登录身份验证期间显示敏感信息时，用户设备中的第三方应用程序无法截取 Citrix Secure Access 应用程序的屏幕截图。

已修复的问题

- Citrix Secure Access 应用程序显示不适用于 SAML 身份验证的证书。

V24.04.1 (May 03, 2024)

- **Always On VPN 配置文件的增强功能**

  Citrix Secure Access 现在支持 VPN 配置文件中的 `Always On VPN'（可选）属性。此属性决定 VPN 配置文件是否为 Always On VPN 配置文件。当此属性设置为 True 时，表示该 VPN 配置文件是 Always On VPN 配置文件。

  > **注意：**
  >
  > 此属性只能在主 VPN 配置文件上设置。不能为附加 VPN 配置文件设置此属性。
  >
  > 在以下情况下，始终开启的 VPN 隧道会重新建立：

  - MDM 配置文件更新
  - Android 设备重启

- 在网络连接失败期间重新连接到不同的 NetScaler Gateway
- 当 Android 设备处于省电模式时，在 NetScaler Gateway 会话过期后重新连接。当设备退出省电模式时，连接会重新建立。

有关详细信息，请参阅以下文章：

- 使用配置设计器进行 VPN 配置
- 为 Android Enterprise 配置 VPN 配置文件
- 为 Android 配置 Citrix SSO 协议

V23.12.2 (2023 年 12 月 15 日)

> **注意：**
>
> 适用于 Android 的 Citrix Secure Access 23.12.2 版包含 CSACLIENTS-8799 的修复程序，并取代了 23.12.1 版。

新增功能

- **思杰 Android 单点登录更名为思杰安全访问**

  Citrix SSO for Android 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。

- **在 Android 13+ 设备上接收或阻止通知**

  在 Android 13 设备上安装或重新安装 Citrix Secure Access 客户端时，最终用户现在会收到提示，要求授予接收来自 Citrix Secure Access 客户端通知的权限。如果最终用户拒绝该权限，他们将不会在其 Android 设备上收到来自 Citrix Secure Access 客户端的任何 VPN 状态或推送通知。建议 MDM 管理员在其解决方案中向 Citrix Secure Access（程序包 ID: `com.citrix.CitrixVPN`）授予通知权限。

  最终用户可以在 Android 设备上导航到**设置 > 通知**以更改 Citrix Secure Access 客户端的通知权限。 有关详细信息，请参阅如何从您的 Android 设备使用 Citrix Secure Access。

- **在 Always On VPN 模式下支持传输登录**

适用于 Android 的 Citrix Secure Access 现在支持 Always On VPN 模式下的传输登录功能。有关如何配置传输登录的详细信息，请参阅配置传输登录页面。

已修复的问题

- 当用户在 Android 13+ 设备上复制基于时间的 OTP (TOTP) 令牌时，Citrix Secure Access 会崩溃。

V23.10.2 (2023年12月19日)

新增功能

> **注意：**
>
> - 适用于 Android 的 Citrix SSO 23.10.2 版包含 CSACLIENTS-8314 的修复，并取代了 23.10.1 版。
> - 适用于 Android 的 Citrix SSO 23.10.1 可与 Android 14 配合使用。

- **VPN 连接失败后使用 NetScaler Gateway 重新进行身份验证 - 预览**

  当 VPN 连接丢失时，适用于 Android 的 Citrix SSO 现在会提示您使用 NetScaler Gateway 重新进行身份验证。Citrix SSO UI 和 Android 设备的通知面板会通知您，NetScaler Gateway 的连接已丢失，您必须重新进行身份验证才能恢复连接。此功能处于预览阶段。

  有关详细信息，请参阅VPN 连接失败后重新连接到 NetScaler Gateway。

已修复的问题

在某些 Always On VPN 场景中重新启动 VPN 服务时，Citrix SSO 会间歇性崩溃。

V23.8.1 (2023年8月31日)

新增功能

- **Always On VPN 自动重启**

  当属于允许列表或阻止列表的应用程序安装在工作配置文件或设备配置文件中时，Citrix SSO 应用程序会自动重新启动 Always On VPN。来自此应用程序的流量会自动通过 VPN 连接进行隧道

传输，而无需重新启动工作配置文件或重新启动设备。要启用 Always On VPN 的自动重新启动，最终用户必须授予 Citrix SSO 应用程序 查询所有软件包 权限。有关详细信息，请参阅 Always On VPN 自动重启。

- **在托管 VPN 配置文件中启用调试日志记录**

  MDM 管理员现在可以将调试日志记录作为自定义参数在 Endpoint Management 控制台的托管 VPN 配置文件中启用。要启用调试日志记录，`EnableDebugLogging` 的值必须设置为 True。如果任何托管 VPN 配置启用了调试日志记录，则在解析配置时，调试日志记录功能将生效。有关更多详细信息，请参阅 Intune 配置的自定义参数。

已修复的问题

- 有时，Citrix SSO 应用程序可能无法将流量隧道传输到某些资源。当分流隧道设置为 OFF 且某些无法访问的域或 IP 地址被黑洞化时，会出现此问题。

V22.11.1 (30-Nov-2022)

新增功能

- **Citrix Secure Access 已更新以支持 Android 12.1（API 级别 32）**

  Citrix Secure Access 现已更新以支持 Android 12.1（API 级别 32）。对于按应用程序 VPN，如果在 VPN 隧道设置后安装了按应用程序 VPN 包列表中的某个包，VPN 服务可能不会自动重新启动。这是由于 Android 11 中引入的应用程序可见性限制。有关详细信息，请参阅 包可见性。

V22.10.1 (21-Oct-2022)

新增功能

- 应用程序版本号的显示已更新为 YY.MM.point-release 格式，其中 YY 是两位数的年份，MM 是两位数的月份，point-release 是根据一个月内的发布编号而定的 1+。
- 针对 Android 客户端，已禁用从欧盟地区收集 Google Analytics/Crashlytics 数据。

已修复问题

- 在“添加连接”和“编辑连接”屏幕中，无效输入出现的错误消息未本地化。

V2.5.3 (2022 年 5 月 5 日)

新增功能

- Citrix SSO 已更新到 Android 11 目标 SDK (API 30)

  Citrix SSO 应用程序现已更新到 Android 11 目标 SDK (API 30)。此更改要求 NetScaler Gateway 使用 Microsoft Intune NAC v2 API 进行设备合规性检查。有关详细信息，请参阅知识库文章 CTX331615。

已修复问题

- 有时，Citrix SSO 在网络更改后可能不会使用备用 DNS 服务器进行主机名解析。

V2.5.2 (2021 年 10 月 21 日)

已修复问题

- 有时，Citrix SSO 在 NAC 检查中处理不合规错误时会崩溃。

V2.5.1 (2021 年 8 月 12 日)

已修复的问题

- 当 CNAME 链长度超过 6 跳时，Citrix SSO 应用程序无法解析主机。
- 当 NetScaler Gateway 仅要求 NAC 检查身份验证时，Citrix SSO 会显示身份验证提示。
- Citrix SSO 在处理异常大的 ICMP 数据包时可能会崩溃。
- 在某些 Android 8.0 设备上添加 VPN 配置文件时，Citrix SSO 可能会崩溃。
- 当您重新启动配置为“始终开启”的 VPN 时，Citrix SSO 可能会崩溃。
- Citrix SSO 在 nFactor 身份验证流程中处理 SSL 错误时可能会崩溃。

V2.5.0 (2021 年 6 月 8 日)

新增功能

- **支持基于 FQDN 的拆分隧道**

适用于 Android 的 Citrix SSO 现在支持基于 FQDN 的拆分隧道。

已修复的问题

- Citrix SSO 预览版 2.5.0 无法连接 (110) 到 NetScaler Gateway 12.1 及更早版本。
- SSO 应用程序重启后，未应用“DisableUserProfiles”设置。

V2.4.16 (2021 年 3 月 31 日)

已修复的问题

- 如果在某些设备上未启用安全浏览，则 nFactor 身份验证将中止。

V2.4.15 (2021 年 3 月 17 日)

已修复问题

- 有时，当 NetScaler Gateway 设备上发生会话超时时，Citrix SSO 不会重新连接 Always On VPN。

V2.4.14 (2021 年 2 月 23 日)

已修复问题

- 当 Always-On VPN 与仅证书身份验证和 nFactor 身份验证一起使用时，Citrix SSO 需要用户交互。
- 有时，Citrix SSO 可能会在 VPN 服务重启或转换期间崩溃。

V2.4.13 (2021 年 2 月 4 日)

已修复问题

- 在某些情况下，Citrix SSO 登录请求在 NetScaler Gateway 响应之前超时。

V2.4.12 (2021 年 1 月 15 日)

此版本解决了各种问题，有助于提高整体性能和稳定性。

V2.4.11 (08-Jan-2021)

- 经典身份验证失败，因为 Citrix SSO 向 NetScaler Gateway 发送了一个 HTTP 标头 (X-Citrix-Gateway)，该标头仅用于 nFactor 身份验证。

V2.4.10 (09-Dec-2020)

已修复的问题

- 有时，Android 设备的经典身份验证可能会失败。
- 执行经典身份验证时，Citrix SSO 可能会崩溃。
- 旋转设备时，Citrix SSO 应用程序的方向不会改变。

V2.4.9 (20-Nov-2020)

已修复的问题

- 当用户点击设备上的 TOTP 令牌值时，Citrix SSO 应用程序会崩溃。

V2.4.8 (04-Nov-2020)

已修复的问题

- 在网关上会话超时后断开 VPN 连接时，Citrix SSO 可能会崩溃。

V2.4.7 (12-Oct-2020)

此版本解决了各种问题，有助于提高整体性能和稳定性。

V2.4.6 (28-Sep-2020)

此版本解决了各种问题，有助于提高整体性能和稳定性。

V2.4.5 (16-Sep-2020)

新增功能

- 引入了新的 NetScaler® 徽标。

V2.4.4 (10-Sep-2020)

已修复的问题

- 有时，在重新连接 VPN 会话时，Citrix SSO 会崩溃。

V2.4.3

已知问题

- 当 Android 设备资源受限时，Citrix SSO 无法与 NetScaler Gateway 建立 VPN 会话。

V2.4.2

已修复的问题

- 加载以前保存的损坏令牌数据时，Citrix SSO 应用程序崩溃。通过此修复，令牌列表中损坏令牌的令牌值显示为“令牌数据已损坏”。删除损坏的令牌并重新添加。

V2.4.1

已修复的问题

- 自 2020 年 6 月起，Citrix SSO 应用程序不再支持 Android 6.x 及更低版本。

V2.3.19

此版本解决了各种问题，有助于提高整体性能和稳定性。

V2.3.18

新增功能

- Android Citrix SSO 应用程序现在支持 Android 10 设备的代理配置。

V2.3.17

此版本解决了各种问题，有助于提高整体性能和稳定性。

V2.3.16

此版本解决了各种问题，有助于提高整体性能和稳定性。

V2.3.15

新增功能

- Citrix SSO 应用程序现在支持托管 VPN 配置文件的 NetScaler Gateway 证书固定。
- 适用于 Android 10 的 Citrix SSO 应用程序现在可以从系统设置中检测“始终开启 VPN”。

已修复的问题

- 如果只定义了 MDM VPN 配置文件，Citrix SSO 应用程序在断开 VPN 连接时会崩溃。

V2.3.14

新增功能

- Citrix SSO 应用程序现在可以代表 Citrix Workspace 应用程序执行用户身份验证，以实现本机应用程序单点登录。
- 如果在 VPN 隧道设置后安装了按应用程序 VPN 包列表中的某个包，VPN 服务会重新启动。

已修复的问题

- Citrix SSO 现在可以正确处理最终的 VPN 会话建立消息。
- NetScaler Gateway IP 地址现在只解析一次。以前，NetScaler Gateway IP 地址会解析多次，有时会导致连接失败。

已知问题

- 始终开启的 VPN 状态在应用程序用户界面中并非总是正确更新。

V2.3.13

已修复问题

- NetScaler Gateway IP 地址现在只解析一次。

此前，NetScaler Gateway IP 地址会多次解析，有时会导致连接失败。

已知问题

- Always-On VPN 状态在应用程序用户界面中并非总是正确更新。

V2.3.12

已修复问题

- 保存 VPN 配置文件时，Citrix SSO 可能会崩溃。

V2.3.11

已修复问题

- Citrix SSO 在保存 VPN 配置文件时可能会崩溃。
- 当新的 VPN 配置文件或现有配置文件的更新导致 disableUserProfile 值发生变化时，disableUserProfile 设置不会在用户界面中正确反映。
- 适用于 Android 的 Citrix SSO 在设备所有者 (DO) 模式下不处理 VPN 配置文件。
- 当只有 IPv6 本地 DNS 服务器时，VPN 连接无法建立。

V2.3.10

已修复问题

- 设备闲置一段时间后，VPN 连接丢失。

V2.3.8

新增功能

- **在 Intune Android Enterprise 环境中设置 Citrix SSO 应用程序**

  您现在可以在 Intune Android Enterprise 环境中设置 Citrix SSO 应用程序。有关详细信息，请参阅 在 Intune Android Enterprise 环境中设置 Citrix Secure Access。

- **通过 Android Enterprise 预配 VPN 配置文件的支持**

  现在支持通过 Android Enterprise 预配 VPN 配置文件。

已修复的问题

- 如果您保存了一个已保存的令牌，然后尝试打开它，令牌名称中会出现乱码字符。
- 如果在 NetScaler Gateway 上未配置 DNS 搜索域，Citrix SSO 应用程序将无法建立 VPN 会话。

V2.3.6

新增功能

- **Citrix SSO 的 Always On 支持**

  Citrix SSO 的 Always On 功能可确保用户始终连接到企业网络。这种持久的 VPN 连接是通过自动建立 VPN 隧道来实现的。

- **如果 Athena 令牌过期导致注销，则会显示重新登录通知**

  如果满足以下条件，则会显示提示用户重新登录 Citrix Workspace 的通知。

  - 在 Citrix Workspace 预配的 VPN 配置文件中启用了“始终开启”功能
  - Athena 身份验证用于 SSO
  - 由于 Athena 令牌过期，用户已从 Citrix Workspace 应用程序注销

- **使用 NetScaler Gateway 完成推送通知服务的注册**

  您现在可以使用 NetScaler Gateway 设备注册推送通知服务。以前，注册是在客户端设备上完成的。

已修复的问题

有时，当扫描新令牌时，Citrix SSO 会崩溃。例如，当删除现有令牌并扫描具有相同令牌名称的另一个令牌时，Citrix SSO 会崩溃。

V2.3.1

新增功能

- **托管配置已更新，以包含更多用户设置**

  托管配置已更新，以包含适用于 Android Enterprise 环境的“BlockUntrustedServers”、“DefaultProfileName”和“DisableUserProfiles”设置。

- **增强的推送通知支持**

  在将 NetScaler Gateway 配置为类型为“OTP”的推送通知后，当用户在响应请求用户同意进行身份验证的推送通知时选择“允许”后，将不再要求输入 PIN/指纹。

- **Firebase 分析支持**

  已添加对基本 Firebase Analytics 的支持，以提供有关 Citrix SSO 应用程序的使用信息。此增强功能适用于粗略地理位置、屏幕使用情况、正在使用的不同 Android 版本等。

- **支持基于 Android 托管配置的 VPN 配置文件配置**

  Citrix SSO 应用程序可以在 Android Enterprise 环境中通过 EMM/UEM 供应商（如 Citrix Endpoint Management）进行配置。CEM 中的 Android Enterprise 托管配置向导可用于将托管 VPN 配置部署到 Citrix SSO 应用程序。有关如何使用托管配置配置 Citrix SSO 应用程序的信息，请参阅 VPN 设备策略。

V2.2.9

新增功能

- **推送通知支持**

  NetScaler Gateway 会在您注册的移动设备上发送推送通知，以简化双因素身份验证体验。

已修复的问题

- 在“添加连接”屏幕下的服务器字段中允许非URL字符。

在 MDM 环境中设置 Citrix Citrix Secure Access

要在 MDM 环境中设置 Citrix Secure Access，请参阅 配置适用于 Android 的 Citrix Secure Access 协议。

注意：

- 在非 MDM 环境中，用户手动创建 VPN 配置文件。
- 您还可以为 Citrix Secure Access 创建 Android Enterprise 托管配置。有关详细信息，请参阅 配置适用于 Android Enterprise 的 VPN 配置文件。
- 对于使用 Citrix Secure Access 23.12.1 及更高版本的 Android 13+ 用户，建议 MDM 管理员在其解决方案中向 Citrix Secure Access（包 ID：`com.citrix.CitrixVPN`）授予通知权限。

在 Intune Android Enterprise 环境中配置和部署 Citrix Secure Access

重要提示：

适用于 Android 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。

本主题介绍了通过 Microsoft Intune 部署和配置 Citrix Secure Access 的详细信息。本文档假定 Intune 已配置为支持 Android Enterprise，并且设备注册已完成。

先决条件

- Intune 已配置为支持 Android Enterprise
- 设备注册已完成

在 Intune Android Enterprise 环境中配置和部署 Citrix Secure Access

- 将 Citrix Secure Access 添加为托管应用
- 为 Citrix Secure Access 配置托管应用策略

将 Citrix Secure Access 添加为托管应用

1. 登录到您的 Azure 门户。
2. 在左侧导航边栏中单击 **Intune**。
3. 在 Microsoft Intune 边栏中单击 **客户端应用**，然后在客户端应用边栏中单击“应用”。

4. 在右上角菜单选项中单击 **+添加链接**。“添加应用配置”边栏随即显示。
5. 选择 **Managed Google Play** 作为应用类型。

   如果您已配置 Android Enterprise，这会添加 Managed Google Play 搜索和批准面板。
6. 搜索 Citrix Secure Access 并从应用列表中选择它。

   选择安全访问(/en-us/citrix-secure-access/media/sso-for-intune1.png)

   注意： 如果 Citrix Secure Access 未出现在列表中，则表示该应用在您所在的国家/地区不可用。
7. 单击 **APPROVE** 以通过 Managed Google Play 商店批准部署 Citrix Secure Access。

   Citrix Secure Access 所需的权限已列出。
8. 单击 **APPROVE** 以批准部署该应用。
9. 单击 **Sync** 以将此选择与 Intune 同步。

   Citrix Secure Access 已添加到客户端应用列表。如果添加了许多应用，您可能需要搜索 Citrix Secure Access。
10. 单击 **Citrix Secure Access** 应用以打开应用详细信息面板。
11. 在详细信息面板中单击 **Assignments**。**Citrix Secure Access - Assignments** 面板随即出现。

    选择 Secure Access 分配(/en-us/citrix-secure-access/media/sso-for-intune3.png)
12. 单击 **Add group** 以分配您要授予安装 Citrix Secure Access 权限的用户组，然后单击 **Save**。
13. 关闭 Citrix Secure Access 详细信息面板。

Citrix Secure Access 已添加并启用，可部署给您的用户。

配置 Citrix Secure Access 的托管应用策略

添加 Citrix Secure Access 后，您必须为 Citrix Secure Access 创建一个托管配置策略，以便将 VPN 配置文件部署到设备上的 Citrix Secure Access。

1. 在 Azure 门户中打开 **Intune** 边栏选项卡。
2. 从 Intune 边栏选项卡中打开 **Client Apps** 边栏选项卡。
3. 从 Client apps 边栏选项卡中选择 **App configuration policies** 项，然后单击 **Add** 以打开 **Add configuration policy** 边栏选项卡。
4. 输入策略名称并添加描述。
5. 在 **设备注册类型** 中，选择 **托管设备**。

6. 在 **Platform** 中，选择 **Android**。

   这会为关联的应用添加另一个配置选项。

7. 单击 **Associated app** 并选择 **Citrix Secure Access** 应用。

   如果您有许多应用，可能需要搜索它。

8. 单击 **OK**。Add configuration policy 边栏选项卡中会添加一个配置设置选项。

9. 单击 **配置** 设置。

   出现一个用于配置 Citrix Secure Access 的边栏选项卡。

10. 在 **配置设置** 中，选择 **使用配置设计器** 或 **输入 JSON 数据** 来配置 Citrix Secure Access。

    为 Intune 设置 Citrix 安全访问(/en-us/citrix-secure-access/media/sso-for-intune4.png)

> **注意：**
>
> 对于简单的 VPN 配置，建议使用配置设计器。

使用配置设计器进行 VPN 配置

1. 在 **配置设置** 中，选择 **使用配置设计器** 并单击 **添加**。

   系统将显示一个键值输入屏幕，用于配置 Citrix Secure Access 支持的各种属性。您至少必须配置 **服务器地址** 和 **VPN 配置文件名称** 属性。您可以将鼠标悬停在 **说明** 部分上，以获取有关每个属性的更多信息。

2. 例如，选择 **VPN 配置文件名称** 和 **服务器地址(*)** 属性，然后单击 **确定**。

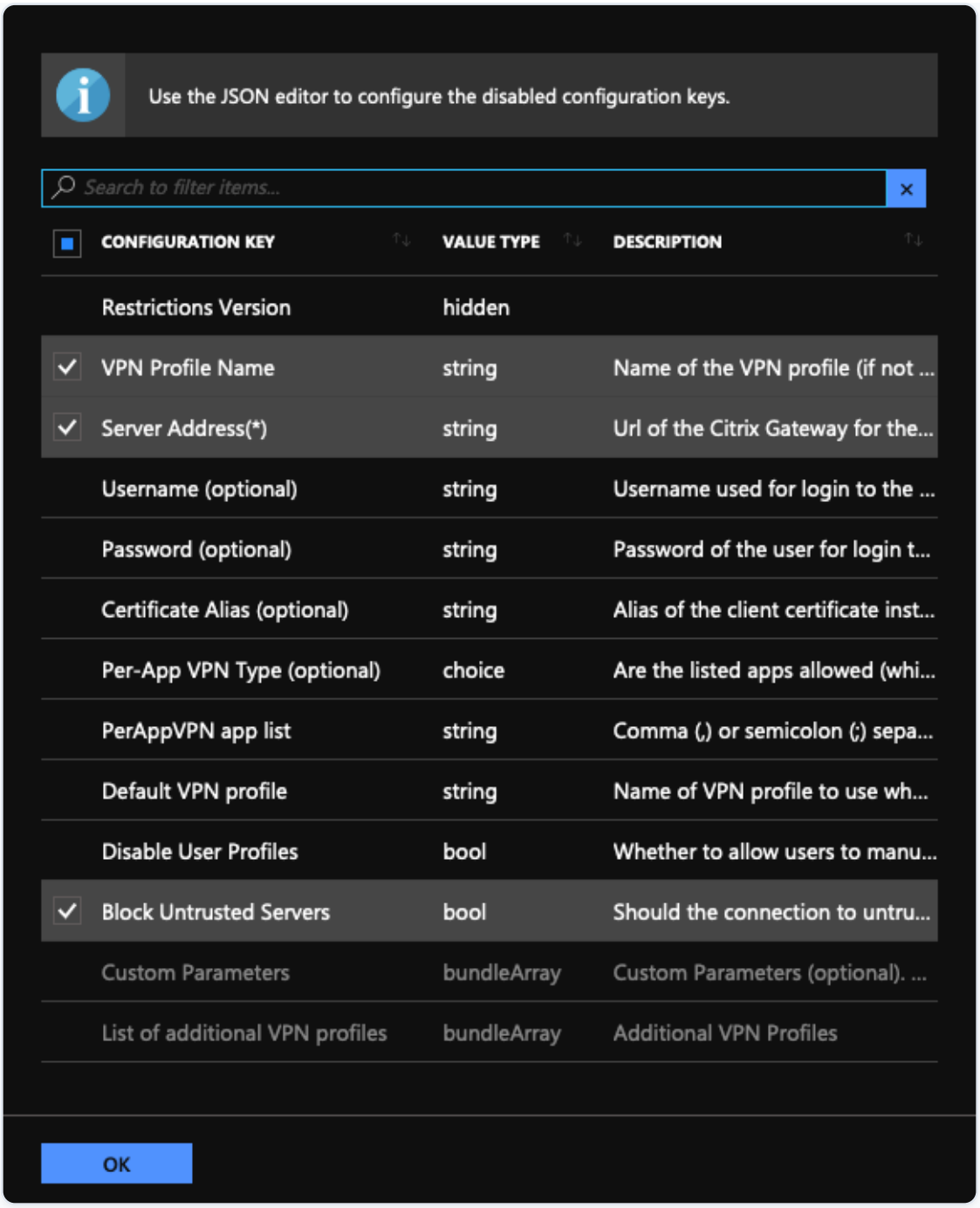
   这会将属性添加到配置设计器中。您可以配置以下属性。

   - **VPN 配置文件名称**。键入 VPN 配置文件的名称。如果您要创建多个 VPN 配置文件，请为每个配置文件使用唯一的名称。如果您未提供名称，则在“服务器地址”字段中输入的地址将用作 VPN 配置文件名称。
   - **服务器地址(*)**。键入您的 NetScaler Gateway 基本 FQDN。如果您的 NetScaler Gateway 端口不是 443，请同时键入您的端口。使用 URL 格式。例如，`https://vpn.mycompany.com:8443`。
   - **用户名（可选）**。输入最终用户用于向 NetScaler Gateway 进行身份验证的用户名。如果网关配置为使用此字段，则可以使用 Intune 配置值令牌 {{userprincipalname}}（请参阅配置值

令牌）。如果您未提供用户名，则用户在连接到 NetScaler Gateway 时会收到提供用户名的提示。

- **密码（可选）**。输入最终用户用于向 NetScaler Gateway 进行身份验证的密码。如果您未提供密码，则用户在连接到 NetScaler Gateway 时会收到提供密码的提示。
- **证书别名（可选）**。在 Android KeyStore 中提供一个证书别名，用于客户端证书身份验证。如果您使用基于证书的身份验证，则此证书将预先为用户选择。
- **网关证书固定（可选）**。描述用于 NetScaler Gateway 的证书固定的 JSON 对象。示例值：`{"hash-alg" : "sha256", "pinset" : ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="]}`。有关详细信息，请参阅 使用 Android Citrix Secure Access 进行 NetScaler Gateway 证书固定。
- **按应用 VPN 类型（可选）**。如果您正在使用按应用 VPN 来限制哪些应用使用此 VPN，则可以配置此设置。
  - 如果选择**允许**，则 PerAppVPN 应用列表中列出的应用包名称的网络流量将通过 VPN 路由。所有其他应用的流量将路由到 VPN 外部。
  - 如果选择**不允许**，则 PerAppVPN 应用列表中列出的应用包名称的网络流量将路由到 VPN 外部。所有其他应用的流量将通过 VPN 路由。默认值为允许。
- **PerAppVPN 应用列表**。根据按应用 VPN 类型的不同值，允许或不允许其流量通过 VPN 的应用列表。列出以逗号或分号分隔的应用包名称。应用包名称区分大小写，并且必须与它们在 Google Play 商店中显示的名称完全一致。此列表是可选的。要预配设备范围的 VPN，请将此列表留空。
- **默认 VPN 配置文件**。为 Citrix Secure Access 配置 Always On VPN 时使用的 VPN 配置文件名称。如果此字段为空，则主配置文件用于连接。如果只配置了一个配置文件，则将其标记为默认 VPN 配置文件。
- **Always On VPN（可选）**：当设置为 True 时，表示 VPN 配置文件是 Always On VPN 配置文件。此属性只能为主 VPN 配置文件设置。不能为其他 VPN 配置文件设置。默认情况下，此属性设置为 False。

> **注意：**
>
> 从 Citrix Secure Access for Android 24.04.1 版本开始提供 `Always On VPN (optional)` 属性。



注意：

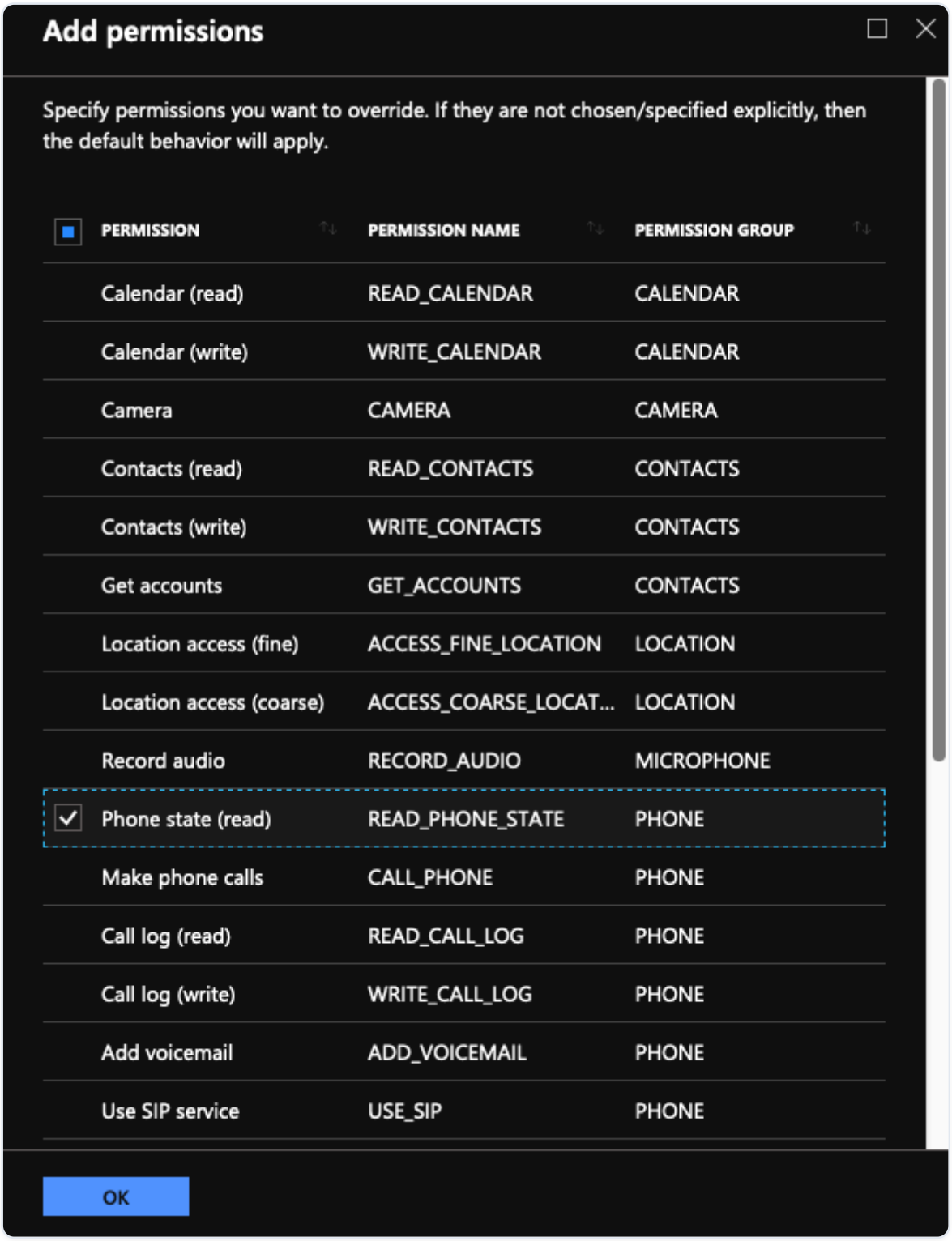
- 要在 Intune 中将 Citrix Secure Access 设置为 Always On VPN 应用，请使用自定义 VPN 提供程序，并将 `com.citrix.CitrixVPN` 作为应用包名称。
- Citrix Secure Access 的 Always On VPN 仅支持基于证书的客户端身份验证。
- 管理员必须在 NetScaler Gateway 上的**SSL 配置文件**或**SSL 属性**中选择**客户端身份验证**并将**客户端证书**设置为**强制**，Citrix Secure Access 才能按预期工作。

- **禁用用户配置文件**
  - 如果将此值设置为 true，则用户无法在其设备上添加新的 VPN 配置文件。
  - 如果您将此值设置为 false，用户可以在其设备上添加自己的 VPN。

  默认值为 false。
- **阻止不受信任的服务器**
  - 当为 NetScaler Gateway 使用自签名证书，或者颁发 NetScaler Gateway 证书的 CA 的根证书不在系统 CA 列表中时，请将此值设置为 false。
  - 将此值设置为 true 以启用 Android 操作系统验证 NetScaler Gateway 证书。如果验证失败，则不允许连接。

  默认值为 true。

3. 对于 **服务器地址(*)** 属性，输入您的 VPN 网关基本 URL（例如，`https://vpn.mycompany.com`）。
4. 对于 **VPN 配置文件名称**，输入一个在 Citrix Secure Access 客户端主屏幕中对最终用户可见的名称（例如，“我的公司 VPN”）。
5. 您可以根据 NetScaler Gateway 部署的需要添加和配置其他属性。完成配置后，单击 **确定**。
6. 单击 **权限** 部分。您可以授予 Citrix Secure Access 所需的以下权限：
   - 如果您正在使用 Intune NAC 检查，Citrix Secure Access 要求您授予 **电话状态（读取）** 权限。单击 **添加** 按钮以打开权限面板。目前，Intune 会显示一个适用于所有应用程序的大量权限列表。
   - 如果您正在使用 Intune NAC 检查，请选择 **电话状态（读取）** 权限并单击 **确定**。这会将其添加到应用程序的权限列表中。选择 **提示** 或 **自动授予**，以便 Intune NAC 检查可以工作，然后单击 **确定**。



- 建议您自动授予 Citrix Secure Access 通知权限。

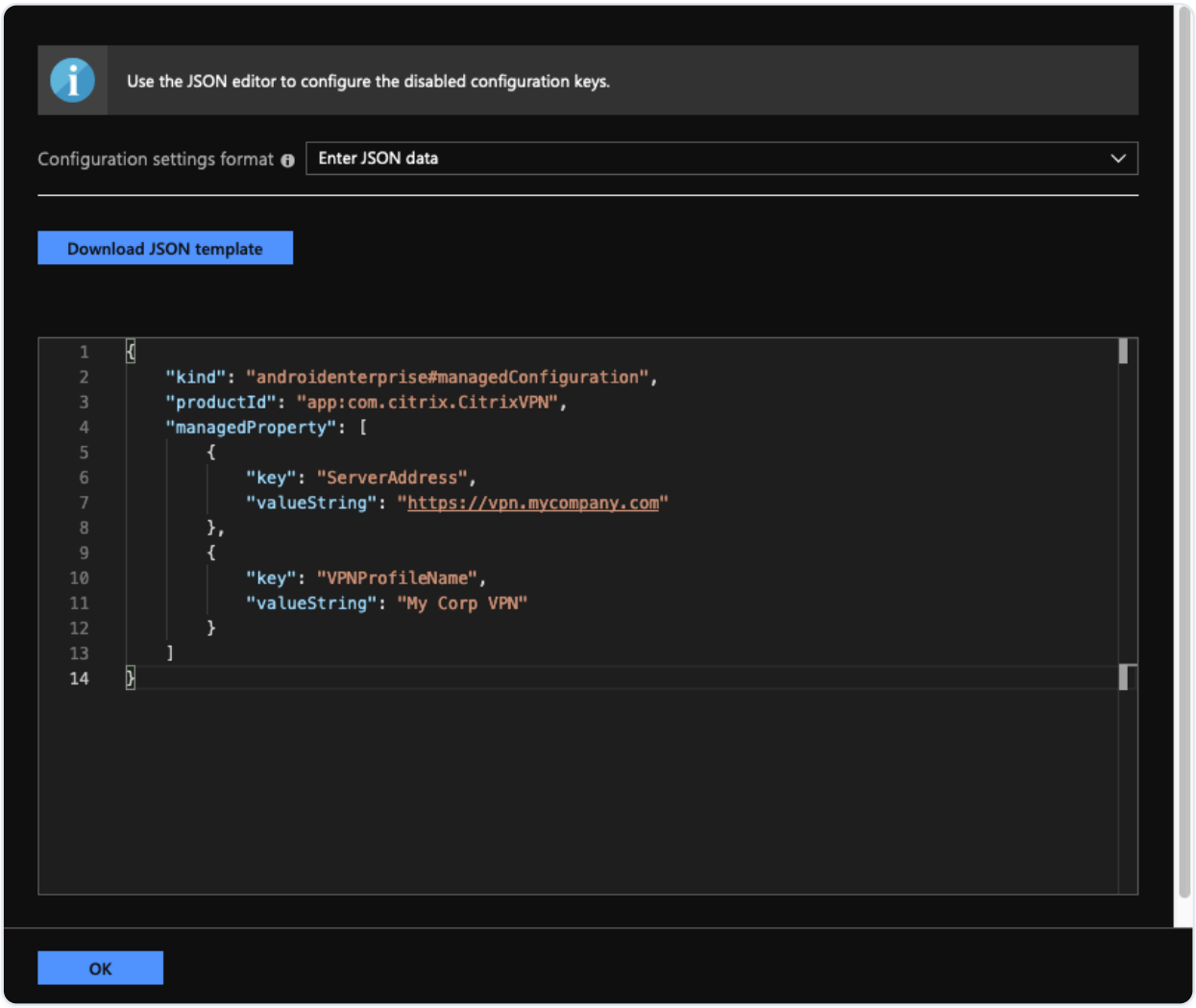
> **注意：**
>
> 对于使用 Citrix Secure Access 23.12.1 及更高版本的 Android 13+ 用户，建议 MDM 管理员在其解决方案中授予 Citrix Secure Access（包 ID: `com.citrix.CitrixVPN`）通知权限。

7. 单击“应用配置策略”边栏底部的“**添加**”以保存 Citrix Secure Access 的托管配置。
8. 单击“应用配置策略”边栏中的“**分配**”以打开“**分配**”边栏。
9. 选择您希望交付和应用此 Citrix Secure Access 配置的用户组。

通过输入 JSON 数据进行 VPN 配置

1. 在“**配置设置**”中，选择“**输入 JSON 数据**”以配置 Citrix Secure Access。
2. 使用“下载 JSON 模板”按钮下载一个模板，该模板允许为 Citrix Secure Access 提供更详细/复杂的配置。此模板是一组 JSON 键值对，用于配置 Citrix Secure Access 可识别的所有可能属性。

   有关可配置的所有可用属性列表，请参阅在 Citrix Secure Access 应用程序中配置 VPN 配置文件的可用属性。
3. 创建 JSON 配置文件后，将其内容复制并粘贴到编辑区域。例如，以下是之前使用配置设计器选项创建的基本配置的 JSON 模板。



这完成了在 Microsoft Intune Android Enterprise 环境中配置和部署 Citrix Secure Access 的 VPN 配置文件的过程。

重要提示：

用于基于客户端证书身份验证的证书是使用 Intune SCEP 配置文件部署的。此证书的别名必须在 Citrix Secure Access 托管配置的“**证书别名**”属性中进行配置。

在 Citrix Secure Access 中配置 VPN 配置文件的可用属性

配置键	JSON 字段名称	值类型	描述
VPN 配置文件名称	VPNProfileName	文本	VPN 配置文件的名称（如果未设置，则默认为服务器地址）。
服务器地址(*)	ServerAddress	URL	用于连接的 NetScaler Gateway 的基本 URL（`https://host[:port]`）。这是一个必填字段。
`Username`（可选）	用户名	文本	用于通过 NetScaler Gateway 进行身份验证的用户名（可选）。
密码 (可选)	密码	文本	用于通过 NetScaler Gateway 进行身份验证的用户的密码 (可选)。
证书别名 (可选)	ClientCertAlias	文本	安装在 Android 凭据存储中用于基于证书的客户端身份验证的客户端证书的别名 (可选)。在使用 NetScaler Gateway 上的基于证书的身份

配置键	JSON 字段名称	值类型	描述
			验证时，**证书别名**是必填字段。
网关证书固定 (可选)	ServerCertificatePins	JSON 文本	描述用于 NetScaler Gateway 的证书固定的嵌入式 JSON 对象。示例值：`{"hash-alg" : "sha256", "pinset" : ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="]}`。使用 JSON 配置器时，请务必转义此嵌入式 JSON 数据。
按应用 VPN 类型 (可选)	PerAppVPN_Allow_Disallow_Setting	枚举 (允许, 拒绝)	列出的应用程序是允许（允许列表）还是不允许（阻止列表）使用 VPN 隧道。如果设置为 **允许**，则只有列出的应用程序（在 PerAppVPN 应用程序列表属性中）才允许通过 VPN 隧道传输。如果设置为 **不允许**，则除列出的应用程序外，所有应用程序都允许通过 VPN 隧道传输。如果没有列出任何应用程序，则所有应用程序都允许通过 VPN 隧道传输。
PerAppVPN 应用程序列表	PerAppName_Appnames	文本	用于按应用程序 VPN 的应用程序包名称列

配置键	JSON 字段名称	值类型	描述
			表，以逗号 (,) 或分号 (;) 分隔。包名称必须与它们在 Google Play 商店应用程序列表页面 URL 中显示的名称相同。包名称区分大小写。
默认 VPN 配置文件	DefaultProfileName	文本	当系统启动 VPN 服务时要使用的 VPN 配置文件名称。此设置用于在设备上配置 Always On VPN 时识别要使用的 VPN 配置文件。
Always On VPN（可选）	IsAlwaysOnVpn	布尔值	确定 VPN 配置文件是否为 Always On VPN 配置文件。当设置为 True 时，表示 VPN 配置文件是 Always On VPN 配置文件。此属性只能在主 VPN 配置文件上设置。不能为附加 VPN 配置文件设置此属性。默认值为 False。
			此属性从 Citrix Secure Access for Android 24.04.1 版本开始可用。
禁用用户配置文件	DisableUserProfiles	布尔值	用于允许或不允许最终用户手动创建 VPN 配置文件的属性。将此值设置为 **true** 可禁用用户创建 VPN 配置文件。默认值为 **false**。

配置键	JSON 字段名称	值类型	描述
阻止不受信任的服务器	BlockUntrustedServers	布尔值	用于确定是否阻止连接到不受信任的网关（例如，使用自签名证书或颁发 CA 不受 Android 操作系统信任）的属性。默认值为 true（阻止连接到不受信任的网关）。
自定义参数（可选）	CustomParameters	列表	Citrix Secure Access 支持的自定义参数（可选）列表。有关详细信息，请参阅 自定义参数。请查看 **NetScaler Gateway 产品文档**以了解可用选项。
其他 VPN 配置文件列表	bundle_profiles	列表	其他 VPN 配置文件的列表。支持每个配置文件的大多数先前提及的值。有关详细信息，请参阅VPN 配置文件列表中每个 VPN 支持的属性。

自定义参数

每个自定义参数都必须使用以下键值名称进行定义。

键	值类型	值
ParameterName	文本	自定义参数的名称。
ParameterValue	文本	自定义参数的值。

Intune 配置的自定义参数

参数名称	描述	值
UserAgent	Citrix Secure Access 在与 NetScaler Gateway 通信时，会将此参数值附加到用户代理 HTTP 标头，以便在 NetScaler Gateway 上执行额外的检查。	指定需要附加到用户代理 HTTP 标头的文本。该文本必须符合 HTTP 用户代理规范。
EnableDebugLogging	在 Citrix Secure Access 上启用调试日志记录，以帮助排查 Always On VPN 情况下的 VPN 连接问题。您可以在任何一个托管 VPN 配置中启用它。调试日志记录在处理托管配置时生效。	**True**：启用调试日志记录。默认值：**False**。
DisableLogoutFromStoreOnExplicitDisconnect	控制当最终用户从应用程序 UI 显式断开 VPN 会话时从商店注销。仅适用于 Citrix SecurAccess ZTNA 部署。	**True**：禁用从 SecurAccess ZTNA 商店注销，并保持 SecurAccess ZTNA 会话完整，仅断开 Citrix Secure Access 应用程序会话。默认值：**False**。

有关自定义参数的更多信息，请参阅为 Citrix Secure Access 创建 Android Enterprise 托管配置。

VPN 配置文件列表中每个 VPN 支持的属性

使用 JSON 模板配置多个 VPN 配置文件时，每个 VPN 配置文件都支持以下属性。

配置密钥	JSON 字段名称	值类型
VPN 配置文件名称	bundle_VPNProfileName	文本
服务器地址(*)	bundle_ServerAddress	URL
用户名	bundle_Username	文本
密码	bundle_Password	文本
客户端证书别名	bundle_ClientCertAlias	文本

配置密钥	JSON 字段名称	值类型
网关证书锁定	bundle_ServerCertificatePins	文本
每应用VPN类型	bundle_PerAppVPN_Allow_Disallow_Setting	枚举（允许，禁止）
每应用VPN应用列表	bundle_PerAppVPN_Appnames	文本
自定义参数	bundle_CustomParameters	列表

将 Citrix Secure Access 设置为 Intune 中的 Always On VPN 提供程序

在 Android VPN 子系统中缺少按需 VPN 支持的情况下，Always On VPN 可用作替代方案，以提供无缝 VPN 连接选项以及 Citrix Secure Access 的客户端证书身份验证。VPN 在操作系统启动时或工作配置文件开启时启动。

要将 Citrix Secure Access 设置为 Intune 中的 Always On VPN 应用程序，您必须使用以下设置。

- 选择要使用的正确托管配置类型（个人拥有带工作配置文件或完全托管、专用和公司拥有的工作配置文件）。
- 创建设备配置配置文件，选择“**设备限制**”，然后转到“**连接**”部分。选择启用 Always On VPN 设置。
- 选择 **Citrix Secure Access** 作为 VPN 客户端。如果 Citrix Secure Access 不可用作选项，您可以选择“**自定义**”作为 VPN 客户端，并在“包 ID”字段中输入 **com.citrix.CitrixVPN**（“包 ID”字段区分大小写）。
- 其他选项保持不变。建议不要启用锁定模式。启用后，如果 VPN 不可用，设备可能会完全失去网络连接。
- 除了这些设置之外，您还可以在“**应用程序配置策略**”页面中设置“**每应用 VPN 类型**”和“**每应用 VPN 应用程序列表**”，以启用 Android 的每应用 VPN，如前几节所述。

> **注意：**
>
> Citrix Secure Access 中的 Always On VPN 仅支持客户端证书身份验证。

参考

有关在 Intune 中设置连接选项的更多详细信息，请参阅以下主题。

- 完全托管的专用公司拥有设备
- 个人拥有设备

Always On VPN 的自动重启

从 Citrix SSO for Android 23.8.1 开始，当属于允许列表或阻止列表的应用程序安装到工作资料或设备资料中时，Citrix Secure Access 会自动重启始终开启的 VPN。新安装应用程序的流量将自动通过 VPN 连接进行隧道传输，而无需重启工作资料或设备。

要启用始终开启的 VPN 的自动重启，最终用户必须授予 Citrix Secure Access 查询所有软件包 的同意。一旦授予同意，Citrix Secure Access 将：

- 接收来自操作系统的软件包安装通知。
- 重启始终开启的 VPN。

当最终用户首次连接到每应用 VPN 配置文件时，系统会提示用户提供同意（Google 政策要求）以收集已安装软件包的信息。如果最终用户授予同意，则 VPN 连接将启动。如果用户拒绝同意，则 VPN 连接将中止。一旦授予同意，同意屏幕将不再出现。有关最终用户说明的详细信息，请参阅 如何从 Android 设备使用 Citrix Secure Access。

限制

由于 Android 11 中引入的 软件包可见性限制，Android 11 及更高版本设备上的 Android Enterprise 环境中每应用 VPN 存在以下限制：

- 如果在 VPN 会话启动后，将属于允许/拒绝列表的应用程序部署到设备，则最终用户必须重启 VPN 会话，应用程序才能通过 VPN 会话路由其流量。
- 如果通过始终开启的 VPN 会话使用每应用 VPN，则在设备上安装新应用程序后，最终用户必须重启工作资料或设备，以便应用程序的流量通过 VPN 会话路由。

> **注意：**
>
> 如果您使用的是 Citrix SSO for Android 23.8.1 或更高版本，则这些限制不适用。有关更多详细信息，请参阅 始终开启的 VPN 的自动重启。

适用于 Android 的 Citrix Secure Access 和 Citrix Workspace 应用程序之间的单点登录

从适用于 Android 的 Citrix Secure Access 26.04.1 版开始，支持与 Citrix Workspace 应用程序 (CWA) 的单点登录 (SSO)。如果用户已登录 Citrix Workspace 应用程序，则在登录适用于 Android 的 Citrix Secure Access 中的相同 URL 时，无需再次输入凭据，反之亦然。

此外，如果用户从 Citrix Secure Access 应用程序注销，则用户也会从 Citrix Workspace 应用程序注销，反之亦然。此行为可实现对 TCP/UDP 应用程序的无缝访问，并提供统一的 SecurAccess ZTNA 体验。此注销同步默认启用。要禁用此功能，请联系 Citrix 支持。

使用 MDM 提供商在适用于 Android 的 Citrix Secure Access 应用程序中配置 VPN 配置文件的客户，还可以通过将自定义参数 `DisableLogoutFromStoreOnExplicitDisconnect` 添加到托管应用程序配置来禁用此功能。有关此参数的详细信息，请参阅 Intune 配置的自定义参数。

以前，SecurAccess ZTNA 服务的用户需要进行两次身份验证，一次是在 Android Citrix Workspace 应用程序中访问 SaaS 和已发布的应用程序，另一次是在 Android Citrix Secure Access 应用程序中访问 TCP/UDP 应用程序。

适用于 Android 的 Citrix Secure Access 的 NetScaler Gateway 证书锁定

> **重要提示：**
>
> 适用于 Android 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档和 UI 屏幕截图以反映此名称更改。
>
> 证书锁定有助于防止中间人攻击。Citrix Secure Access 仅支持 Android Enterprise 模式和旧版设备管理员模式下托管 VPN 配置的证书锁定。不支持最终用户添加的 VPN 配置文件。

使用 Android Citrix Secure Access 配置 NetScaler Gateway 证书锁定

有关 Citrix Secure Access 托管配置（以前称为应用程序限制）中证书锁定的详细信息，请参阅证书和身份验证。

定义了一个新的键值对，用于承载锁定的 NetScaler Gateway 证书哈希，如下所示。

```
Key: ServerCertificatePins

Value: {

  "hash-alg": "sha256",

  "pinset": [


"cert1_base64_encoded_SHA-256_hash_of_the_X509_SubjectPublicKeyInfo(SPKI)"
,

    "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",

    "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="

    ...

  ]

}
```

在托管配置中指定证书锁定详细信息的键是 **ServerCertificatePins**。该值是一个 JSON 有效负载，其中包含锁定的 NetScaler Gateway 证书的 base64 编码 SHA-256 哈希以及所使用的哈希算法。锁定的证书可以是操作系统验证的信任链中的任何证书。在此情况下，它是 Android。

证书锁定仅在操作系统在 TLS 握手期间验证证书链后进行。证书的 Pin 值通过对证书的主题公钥信息 (SPKI) 进行哈希计算得出。JSON 有效负载中必须指定这两个字段（“**hash-alg**”和“**pinset**”）。

“**hash-alg**”指定用于计算 SPKI 哈希的哈希算法。 “**pinset**”指定包含 NetScaler Gateway 证书 SPKI 数据的 base64 编码 SHA-256 哈希的 JSON 数组。 证书 Pin 至少必须指定一个值。可以指定更多 Pin 值以允许证书轮换或过期。

您可以使用以下 openssl 命令计算域（例如 gw.yourdomain.com）的 Pin 值。

```
openssl s_client -servername gw.yourdomain.com -connect
gw.yourdomain.com:443 | openssl x509 -pubkey -noout | openssl pkey -pubin
-outform der | openssl dgst -sha256 -binary | openssl enc -base64
```

该命令显示网关提供的叶证书的 base64 编码 SHA-256 哈希。链中的任何证书都可以用于证书锁定。例如，如果企业使用自己的中间 CA 为多个网关生成证书，则可以使用与中间签名证书对应的

Pin。如果没有任何 Pin 与已验证证书链中的证书匹配，则 TLS 握手将中止，并且无法继续连接到网关。

注意：

In device administrator mode, certificate pinning is supported only with Citrix Endpoint Management™ and Microsoft Endpoint Management solutions. Certificate pinning must be configured in the custom parameters used in the legacy VPN profile (not managed configuration) with the custom parameter ServerCertificatePins with the same JSON payload for pinning.

数据治理

Citrix Secure Access 将应用程序事件和指标发送到遥测分析平台 (TAP) 服务器。TAP 是一个 Citrix 专有的服务器平台，用于收集和存储事件和指标，以改进产品。

注意事项：

- Citrix Secure Access 发送的遥测数据仅发送到 TAP，不发送给任何第三方供应商。此外，Citrix Secure Access 不会与 TAP 共享用户的任何个人信息。
- 要阻止遥测数据发送到 TAP，请联系 Citrix 支持。
- 在 Windows 客户端上安装 Citrix Secure Access 后，文件将添加到 Windows 防火墙允许列表中。Citrix Secure Access 收集产品配置和使用数据以改善客户端体验。

数据收集

TAP 根据以下类别收集和存储从 Citrix Secure Access 发送的遥测数据：

- **地理位置：** 国家、大陆以及较大国家/地区的州。
- **客户端版本和客户端类型：** Windows、Linux
- **访问的 VPN URL：** 访问的 URL、MAC 地址模式。

每当启用或禁用以下功能时，TAP 都会收集元数据和遥测日志：

- Edge 网页视图
- 已加入域的计算机
- WFP
- 微软 Intune
- 始终开启
- 始终开启服务
- 分流隧道
- DNS / 分流 DNS

- 内网 IP 地址
- 本地 LAN 访问
- SSO
- GSLB
- 仅限 HTTP 的 Cookie
- NetScaler Gateway 和 SecurAccess ZTNA 部署
- DNS 截断修复