NetScaler Gateway 客户端

Machine translated content

Disclaimer

Contents

NetScaler Gateway VPN 客户端和支持的功能

February 1, 2024

> 重要提示：
>
> - 适用于 iOS/Android 的 Citrix SSO 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。
> - 旧版 VPN 客户端是使用 Apple 的专用 VPN API 构建的，这些 API 现已过时。适用于 macOS/iOS 的 Citrix Secure Access 客户端中的 VPN 支持是使用 Apple 的公共网络扩展框架重写的。不再支持适用于 iOS 和 macOS 的 NetScaler Gateway 插件和 VPN。适用于 iOS/macOS 的 Citrix Secure Access 是推荐使用的 VPN 客户端。
> - 即将发布的版本之一将提供针对 Android 设备的 nFactor 身份验证支持的正式发布。

下表列出了每个 VPN 客户端支持的一些常用功能。

功能	适用于 Windows 的 Citrix Secure Access	适用于 Linux 的 Citrix Secure Access	适用于 macOS 的 Citrix Secure Access	适用于 iOS 的 Citrix Secure Access	适用于 Android 的 Citrix Secure Access
始终开启（用户模式）	是的（11.1 及更高版本）	否	否	否	是的（通过 MDM） Android 7.0+
PAC 文件	是（12.0 及更高版本）	否	是	是	否
客户端代理支持	是	是	否	否	是。请参阅注释 *1*
Intranet 应用程序的最大限制	512	128	无限制	无限制	无限制
内联网 IP (IIP) 支持	是	是	是	是	是
拆分通道打开	是	是	是	是	是
拆分通道反向	是	是	是	是	是。请参阅注释 *5*
Split DNS REMOTE	否	是	是	是	是。参见注释 *6*
拆分 DNS BOTH	是	否	是	是	是。参见注释 *6*

功能	适用于 Windows 的 Citrix Secure Access	适用于 Linux 的 Citrix Secure Access	适用于 macOS 的 Citrix Secure Access	适用于 iOS 的 Citrix Secure Access	适用于 Android 的 Citrix Secure Access
基于 FQDN 的拆分通道	是-仅开（13.0 及更高版本）	否	是	是	是。请参阅注释 *5*
客户端空闲超时	是	是	是	否	否
端点分析	是	是	是	否	否
设备证书（经典）	是	否	是	否	否
nFactor 身份验证	是（12.1 及更高版本）	否	是	是	是。请参阅注释 *3*
EPA (nFactor)	是（12.1 及更高版本）	否	是	否	否
设备证书 (nFactor)	是（12.1 及更高版本）	否	是	否	否
推送通知	是（12.1 及更高版本）	否	否	是	是
OTP 令牌自动填充支持。请参阅注释 *2*	否	否	否	是	是
DTLS 支持。请参阅注释 *4*	是（13.0 及更高版本）	否	是	是	否
HTTPOnly 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	否	始终启用	始终启用	否

注意：

1. 支持在适用于 Android 10 及更高版本的网关配置中的 VPN 虚拟服务器的客户端配置中设置代理。仅支持具有 IP 地址和端口的基本 HTTP 代理配置。
2. 只有通过 QR 代码扫描的令牌才有资格自动填充。nFactor 身份验证流程不支持自动填充。
3. 默认情况下，Android 设备的 nFactor 身份验证支持处于预览状态，该功能处于禁用状态。要启用此功能，请联系 NetScaler 支持人员。客户必须向支持团队提供其 NetScaler Gateway 的 FQDN，以便为 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. 默认情况下，Android 设备的基于 FQDN 的拆分通道支持和反向拆分通道处于预览状态，并且该功能处于

> 禁用状态。要启用此功能，请联系 NetScaler 支持人员。客户必须向支持团队提供 NetScaler Gateway 的 FQDN，以便在 Android 设备上启用该功能。
> 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。其余的查询将在本地解析。适用于 Android 的 Citrix Secure Access 还支持分割 DNS 本地模式。

参考

最终用户帮助文档

适用于 **macOS/iOS** 的 **Citrix Secure Access**

February 1, 2024

旧版 VPN 客户端是使用 Apple 的专用 VPN API 构建的，这些 API 现已过时。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开始重写的。

> 注意
>
> - 适用于 iOS 的 Citrix SSO 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。
> - 适用于 macOS 的 Citrix Secure Access 在 10.15 (Catalina)、11.x (Big Sur) 和 12.x (Monterey) 中受支持。它支持配备 Intel 芯片和 M1 芯片的设备。
> - 硬件无法升级到前面提到的版本之一（macOS 10.15 和 macOS 11.0）的用户可以访问 App Store 上最新的兼容版本，但旧版本没有进一步的更新。
> - 如果 macOS 用户在 App Store 应用程序和 TestFlight 预览版之间切换，或者相反，则用户必须通过执行以下步骤重新创建连接配置文件：
>
>   1. Click the hamburger menu and then click **Configuration**.
>   2. Delete the profile from the list and add the same profile again.

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 6 位数的代码，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) 协议来生成类似于 Google Authenticator 和 Microsoft Authenticator 等服务的 OTP 代码。在对给定 Active Directory 用户进行 NetScaler Gateway 身份验证时，系统会提示用户输入两个密第二个因素是用户从 Google 或 Microsoft Authenticator 等注册的第三方服务复制到桌面浏览器中的六位数代码不断变化。用户必须首先在 NetScaler 设备上注册 T-OTP。有关注册步骤，请参阅

https://support.citrix.com/article/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 密码来添加 OTP 功能。一旦添加了 OTP 令牌，就会显示在用户界面的“密码令牌”部分中。

为了改善体验，添加 OTP 会提示用户自动创建 VPN 配置文件。用户可以利用此 VPN 配置文件直接从他们的 iOS 设备连接到 VPN。

适用于 macOS/iOS 的 Citrix Secure Access 客户端可用于扫描 QR 码，同时注册本地 OTP 支持。
NetScaler Gateway 推送通知功能仅适用于 macOS/iOS 的 Citrix Secure Access 用户可用。

- 推送通知： NetScaler Gateway 在您注册的移动设备上发送推送通知，以实现简化的双重身份验证体验。与其启动适用于 macOS/iOS 的 Citrix Secure Access Client 来在 NetScaler 登录页面上提供第二要素 OTP，不如通过提供注册设备的设备 PIN/Touch ID/Face ID 来验证自己的身份。

注册设备接收推送通知后，您还可以使用适用于 macOS/iOS 的 Citrix Secure Access 使用该设备获得原生 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 支持推送通知，设备也会注册推送通知。

发行说明

February 1, 2024

> 重要提示：
>
> Citrix SSO for iOS 现已重命名为 Citrix Secure Access。我们正在更新文档中的用户界面屏幕截图，以反映此名称的更改。此外，您可能会注意到在此过渡期内，iOS 文档中使用了 Citrix SSO 参考资料。

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。发行说明包括以下一个或多个部分：

新增功能：当前版本中提供的新增功能和增强功能。

已修复的问题：当前版本中修复的问题。

已知问题：当前版本中存在的问题及其解决方法（如果适用）。

> 关于 **EPA** 客户端的重要注意事项：
>
> - macOS 10.13、10.14、10.15、11.x、12.x 和 13.x 版本支持 EPA 客户端。
> - NetScaler 版本 12.1、13.0、13.1 和 14.1 支持 EPA 客户端。

V23.12.2（2023 年 12 月 20 日）

新增功能

此版本解决了提高整体性能和稳定性的问题。

V23.12.1（2023 年 12 月 6 日）

新增功能

- EPA 库已更新至 23.11.1.5（OPSWAT OESIS 库 V 4.3.3318.0）。

  [CSACLIENTS-8516]
- 此版本解决了其他问题，以提高整体性能和稳定性。

V23.11.2 (2023 年 11 月 1 日)

新增功能

EPA 库已更新至 23.11.1.1（OPSWAT OESIS 库 V 4.3.3279.0）。

[CSACLIENTS-8515]

V23.11.1（2023 年 10 月 27 日）

新增功能

- Citrix SSO for iOS 现已重命名为 Citrix Secure Access。我们正在更新文档中的用户界面屏幕截图，以反映此名称的更改。
- EPA 库已更新至 23.10.1.1（OPSWAT OESIS 库 V 4.3.3246.0）。
- 此版本解决了以下问题：
  - Citrix Secure Private Access 环境的连接问题。
  - 提高整体性能和稳定性的其他问题。

V23.10.2（2023 年 10 月 17 日）

此版本解决了 IPv6 登录问题。

V23.10.1（2023 年 10 月 9 日）

新增功能

- EPA 库已更新至 23.9.1.2（OPSWAT OESIS 库 V4.3.3221.0）。
- 支持本地局域网接入

  适用于 macOS 的 Citrix Secure Access/Citrix SSO for iOS 现在支持 NetScaler Gateway 的本地局域网访问功能。您可以配置本地 LAN 访问，这样一旦建立 VPN 连接，便允许或禁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，请参阅以下主题：

  - NetScaler Gateway 管理配置
  - 最终用户配置-macOS
  - 最终用户配置-iOS

V23.09.1（2023 年 9 月 7 日）

> 重要提示：
>
> 如果您使用的是最新的 Apple 操作系统版本，例如 macOS 14/iOS 17 及更高版本，那么我们建议您升级到 Citrix Secure Access 客户端/Citrix SSO 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 库已更新至 1.3.9.9（OPSWAT OESIS v4.3.3160）。

  [CSACLIENTS-6547]

- 用户界面上的安全连接见解

  在 Citrix Secure Access 客户端用户界面的“连接”屏幕上，您可以查看安全连接的详细信息。详细信息包括 IP 地址、FQDN、目标端口和连接时长。有关更多信息，请参阅安全连接见解。

  [SPA-2364]

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

  现在，当 VPN 连接中断时，适用于 macOS 的 Citrix Secure Access 客户端和 Citrix SSO for iOS 会提示您重新通过 NetScaler Gateway 进行身份验证。用户界面上会通知您，表明与 NetScaler Gateway 的连接已断开，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 macOS 重新连接到 NetScaler Gateway
  - VPN 连接失败后，从 iOS 重新连接到 NetScaler Gateway。

  [CSACLIENTS-6071]

V23.08.1 (2023 年 8 月 24 日)

新增功能

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

23.7.6 适用于 macOS 的 EPA 客户端（2023 年 8 月 10 日）

此版本解决了有助于改进整体性能和稳定性的问题。

V23.07.1 (2023 年 7 月 17 日)

新增功能

- 共享日志文件的各种选项

  Citrix SSO for iOS 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。

  有关更多信息，请参阅 发送日志。

  [CSACLIENTS-3834]

- “日志”页面的增强功能

  适用于 macOS 的 Citrix Secure Access 的“日志”页面通过以下选项进行了增强：

  - 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。

  有关更多信息，请参阅 发送日志。

  [SPA-2365]

已修复的问题

连接到 VPN 时，如果系统提示您选择证书进行身份验证，则身份验证登录屏幕将显示在 Citrix Secure Access 客户端的主页后面。

[CSACLIENTS-455]

V23.06.1 (2023 年 6 月 7 日)

新增功能

- 导航栏上的“帮助”菜单

  现在，Citrix Secure Access 客户端的导航栏中添加了“帮助”菜单。“帮助”菜单中的选项（打开日志、导出日志、电子邮件日志和清除日志）可用于调试日志。

  “帮助”菜单下引入了“电子邮件日志”选项。它可用于通过电子邮件共享日志。有关更多信息，请参阅 发送日志。

  [SPA-2361]

已修复的问题

在某些情况下，适用于 macOS 的 Citrix Secure Access 和 Citrix SSO for iOS 上的 DNS 短名解析会失败。

[NSHELP-34568]

已知问题

在某些情况下，反向分割通道中排除的路由会通过通道传输。

[CGOP-24575]

V23.05.2 (2023 年 5 月 11 日)

已修复的问题

升级后，Citrix SSO for iOS 客户端设备无法建立每个应用程序的 VPN 连接。

[NSHELP-35224]

V23.05.1 (2023 年 5 月 4 日)

新增功能

- EPA 图书馆更新到 1.3.9.3，OPSWAT 图书馆更新到 4.3.2987。
- 支持向 **Citrix Analytics** 发送事件

  适用于 macOS 的 Citrix Secure Access 现在支持向 Citrix Analytics 服务发送会话创建、会话终止和应用程序连接等事件。然后，这些事件将记录在 Secure Private Access 服务控制板中。

  [SPA-2197]

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”字段无法以特定区域的格式显示时间。

  [CGOP-23587]

V23.04.1 (2023 年 4 月 4 日)

新增功能

- EPA 库更新到 1.3.9.1，OPSWAT 库更新到 4.3.2923。

V22.12.2 (2023 年 2 月 27 日)

新增功能

- EPA 库已更新至 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改进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

- 转移登录不适用于使用本地网关的非 nFactor 身份验证。

  [CGOP-22729]

适用于 macOS 的 22.11.3 EPA 插件 (28-Nov-2022)

已修复的问题

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

  [CGOP-22722]

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，其中可以为允许的 IP 地址列表创建模式集。

  [CGOP-22095]

已修复的问题

- 有时，NetScaler Gateway 版本 13.0 或 13.1 中的空代理设置会导致 Citrix SSO 创建不正确的代理设置。

  [NSHELP-31970]
- 有时，在网络中断或设备从睡眠模式中唤醒后，VPN 客户端无法重新连接。

  [NSHELP-32483]
- 有时，使用 IPv6 文字作为目标时，网关连接会失败。

  [NSHELP-32876]

22.10.1 适用于 macOS 的 EPA 插件 (27-Oct-2022)

新增功能

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

  [CGOP-22098]
- 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

  [CGOP-21751]

V22.06.1 (2022 年 9 月 20 日)

新增功能

- EPA 库已更新至 4.3.2523.0 (1.3.7.5)

已修复的问题

- 使用 EPA 扫描的 nFactor 身份验证在 macOS 客户端上不起作用。

  [NSHELP-32182-macOS]

- 在 macOS 的 Secure Access Agent 主页上，根据所选主题（浅色或深色），汉堡菜单的左侧和顶部会出现额外的白色或黑色填充。

  [CGOP-19353-macOS]

- 登录 VPN 时，如果配置了设备证书，WebView 窗口会在首次尝试时最小化。

  [CGOP-19354-macOS]

- 在 NetScaler 设备上启用 GSLB 时，Endpoint Analysis 不适用于 macOS 客户端上的 Citrix Secure Access 应用程序。

  [CGOP-21634-macOS]

- 如果配置的应用程序名称中有空格而您尝试访问该应用程序，则 macOS 客户端上不会显示“启用增强安全”弹出窗口。

  [ACS-2632-macOS]

- 当设备上没有相应的客户端证书时，使用可选客户端证书的 nFactor 身份验证会失败。

  [NSHELP-32127-iOS]

- 在使用 Chrome 的 Mac 设备上，VPN 扩展程序在访问两个 FQDN 时崩溃。

  [NSHELP-32144]

- 从网关接收到错误的位置值时，Citrix Secure Access 崩溃。如果管理员定义响应程序策略以重定向到另一台主机，则可能会发生这种情况。

  [NSHELP-32312]

- 如果出现严重延迟或拥塞，则与 Citrix Secure Access 建立的通道之外的资源的直接连接可能会失败。

  [NSHELP-31598]

V3.2.4.9 - 适用于 macOS 的 EPA 插件 (01-Aug-2022)

已修复的问题

- Citrix Endpoint Analysis 插件不处理来自 Google Chrome 浏览器 104 版的专用网络访问预检请求。

  [CGOP-20709]

- 适用于 macOS 的 Citrix Endpoint Analysis 插件不支持 GSLB。

  [CGOP-21543]

已知问题

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

  [CGOP-21751]

V22.03.1 (14-Jun-2022)

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，当分割通道设置为“拆分”或“两者”时，只有指定的域及其子域不会通过通道传输。如果指定的域名是 A.B.C，则除了 A.B.C 和 *.A.B.C. 之外，还会匹配 B.C.

  [CGOP-21657]

- 不使用 PAC 文件的 HTTP/HTTPS 代理设置已损坏。

  [CGOP-21660]

V22.02.3 (24-Mar-2022)

新增功能

- 适用于 macOS 的 Citrix Secure Access 会解析来自客户端的每个 TCP 数据连接上的服务节点的 FQDN，用于云工作区连接。解析每个 TCP 数据连接上的服务节点的 FQDN 不适用于本地网关连接。

  [ACS-1068]

已修复的问题

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

  [NSHELP-31004]

- 当服务器在客户端之前即建立连接后立即发送数据时，Citrix Secure Access 应用程序会破坏某些协议。

  [NSHELP-29374]

- 如果用户在未完成身份验证的情况下关闭了适用于 macOS 的 Citrix Secure Access 客户端的身份验证窗口，则在应用程序重新启动之前，后续尝试连接到服务器会失败。

  [ACS-2415]

- 适用于 macOS 的 Citrix Secure Access 客户端现已与 OPSWAT 库版本 4.3.2367.0 捆绑在一起

  [NSHELP-30802]

- 适用于 macOS 的 Citrix Secure Access 运行身份验证后 EPA 检查所需的时间比预期的要长。

  [NSHELP-29118]

已知问题

- 在已经连接的 Citrix Secure Private Access 服务区域变得无法访问一分钟后，适用于 macOS 的 Citrix Secure Access 应用程序注销。但是，这不会影响本地网关连接。

  [ACS-2715]

V22.02.2 (15-Feb-2022)

已修复的问题

- 当用户尝试从适用于 macOS 的 Citrix Secure Access 访问未订阅的 Web 应用程序时，会显示多个弹出窗口。

  [ACS-2406]

V22.01.1 (08-Feb-2022)

已修复的问题

- 使用 Citrix SSO for iOS 设备的 PerApp VPN 连接无法在 443 以外的端口上连接到 NetScaler Gateway。

  [NSHELP-30653]

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。

  [ACS-1092]

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。

  [CGOP-20388]
- 如果由于客户端和 ADC 之间存在代理，服务器证书只有公用名称的 IP 地址，Citrix SSO 将无法建立 VPN 连接。

  [CGOP-20390]
- 在 macOS 上，用于检查防病毒软件的上一次完整系统扫描的 EPA 扫描失败。

  [NSHELP-29571]
- 有时，Citrix SSO 应用程序在处理大型 DNS 数据包时会崩溃。

  [NSHELP-29133]

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。

  [NSHELP-28942]
- 网络中断后，Citrix SSO 无法重新建立 VPN 连接。

  [CGOP-19988]

V1.3.13 (05-Nov-2021)

已修复的问题

- 筛选托管 VPN 与非托管 VPN 的会话时可能会出现故障。建立会话的初始请求缺少 User-Agent 标头中的“ManagedVpn”信息。

  [CGOP-19561]

V1.3.12 (21-Oct-2021)

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将失败。

  [NSHELP-28551]

- Citrix SSO 应用程序在接收通知时会间歇性崩溃。

  [CGOP-19363]

- 当调用“isFeatureEnabled”参数来检查功能标志时，VPN 扩展可能会崩溃。

  [CGOP-19360]

- 如果 DTLS 协议的有效负载为空，网关 VPN 扩展就会崩溃。

  [CGOP-19361]

- 当设备从睡眠模式唤醒并连接 VPN 时，SSO 应用程序会间歇性地崩溃。

  [CGOP-19362]

V1.3.11 (17-Sep-2021)

已修复的问题

- 对于使用 Citrix SSO 的 macOS 设备，EPA 扫描防火墙检查失败。

  [CGOP-19271]

- 配置旧版身份验证或 Intune 网络访问合规性 (NAC) 后，Citrix SSO 在 iOS 12 设备中崩溃。

  [CGOP-19261]

V1.3.10 (31-Aug-2021)

新增功能

- Citrix SSO for macOS 现在与 OPSWAT 库版本 4.3.1977.0 捆绑在一起。

  [NSHELP-28467]

V1.3.9 (13-Aug-2021)

已修复的问题

- 在安装了 HTTP 代理软件的某些系统上，NetScaler Gateway IP 地址在内部显示为 127.0.0.1，因此无法建立通道。

  [CGOP-18538]

- 设置“阻止不受信任的服务器”在支持 Citrix SSO for iOS 的非英语本地化的系统上不起作用。

  [CGOP-18539]

- Citrix SSO 无法连接到 DNS 名称与服务器证书中的公用名称不匹配的系统。Citrix SSO 现在会检查主题的备用名称，并正确连接。

  [NSHELP-28348]

V1.3.8 (07-Jul-2021)

新增功能

- Citrix SSO for macOS 仅与版本 10.15（卡塔利娜）及更高版本兼容。

  [CGOP-12555]

- 从 Citrix SSO for macOS 版本 1.3.8 开始，EPA 库嵌入在应用程序中，不会从 NetScaler Gateway 服务器下载。当前的嵌入式 EPA 库版本为 1.3.5.1。

  [NSHELP-26838]

为 **iOS** 用户设置 **Citrix Secure Access**

February 1, 2024

> 重要提示：
>
> - Citrix SSO for iOS 现已重命名为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。在此过渡期间，您可能会注意到文档中使用的 Citrix SSO 参考资料。
> - 无法在 iOS 12 及更高版本上使用 VPN。要继续使用 VPN，请使用 Citrix Secure Access。

有关适用于 iOS 的 Citrix Secure Access 支持的一些常用功能的列表，请参见 NetScaler Gateway VPN 客户端和支持功能。

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（前身为 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 的详细信息，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 macOS/iOS 上将 Citrix Secure Access 客户端与不带 MDM 的 NetScaler Gateway VPN 一起使用，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** 托管的 **VPN** 配置文件

以下部分介绍了以 Citrix Endpoint Management（前身为 XenMobile）为例，为 Citrix Secure Access 客户端（macOS/iOS）配置全设备和每个应用程序 VPN 配置文件的分步说明。其他 MDM 解决方案在使用 Citrix Secure Access (macOS/iOS) 时可以使用本文档作为参考。

> 注意：
>
> 本部分说明基本的设备范围和 PerApp VPN 配置文件的配置步骤。您也可以按照 Citrix Endpoint Management（前身为 XenMobile）文档或 Apple 的 MDM VPN 有效负载配置来配置按需代理、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。根据 NetScaler 中定义的 VPN 策略（例如全通道、拆分通道、反向拆分通道），将来自所有应用程序和服务的流量通道传输到 NetScaler Gateway。

在 Citrix Endpoint Management 上配置设备级 VPN　执行以下步骤在 Citrix Endpoint Management 上配置设备级别的 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，然后在 连接类型 中选择 自定义 **SSL**。

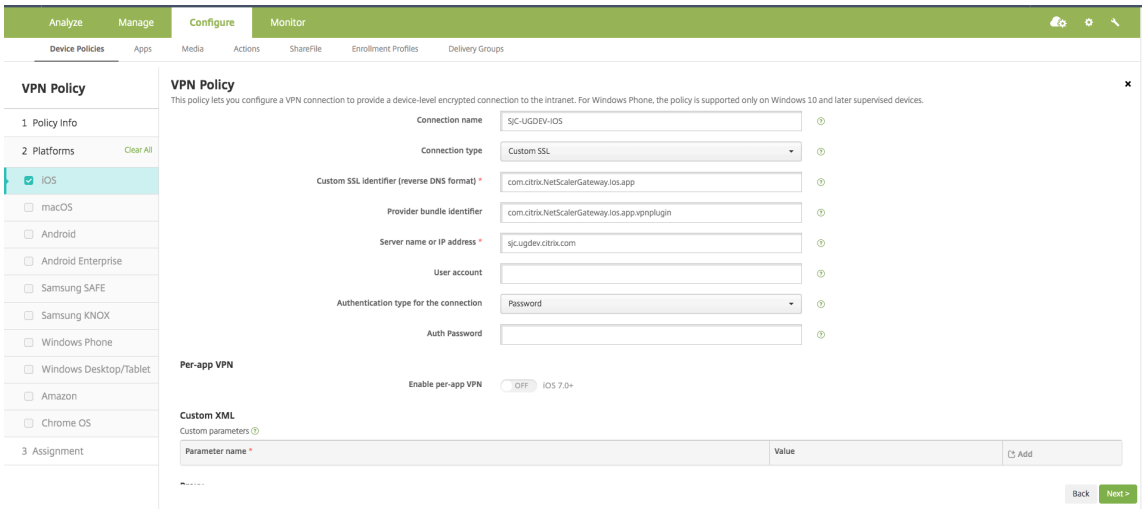
   在 MDM VPN 有效负载中，连接名称对应于 **UserDefinedName** 密钥，**VPN** 类型密钥 必须设置为 **VPN**。
5. 在自定义 **SSL** 标识符（反向 **DNS** 格式）中，输入 **com.citrix.NetScalerGateway.ios.app**。这是 iOS 上 Citrix Secure Access 的捆绑标识符。

   在 MDM VPN 有效负载中，自定义 SSL 标识符对应于 **VPNSubType** 密钥。
6. 在提供商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包标识符。

   在 MDM VPN 有效负载中，提供程序捆绑包标识符与 **ProviderBundleIdentifier** 密钥相对应。
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。这些字段的配置可以在 Citrix Endpoint Management（以前称为 XenMobile）文档中找到。

8. 单击下一步。



9. 单击“保存”。

PerApp VPN 配置文件

PerApp VPN 配置文件用于为特定应用程序设置 VPN。仅来自特定应用程序的流量会通过通道传输到 NetScaler Gateway。P er-**App VPN** 有效负载 支持设备级 VPN 的所有密钥以及其他一些密钥。

在 **Citrix Endpoint Management** 上配置每应用程序级别的 **VPN**　要配置 PerApp VPN，请执行以下步骤：

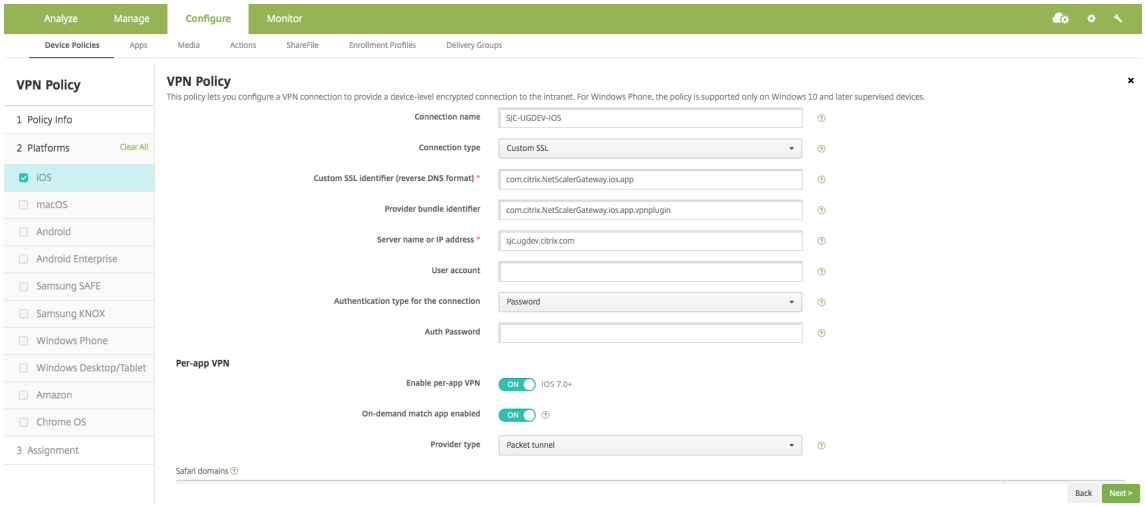
1. 在 Citrix Endpoint Management 上完成设备级别的 VPN 配置。
2. 在“每应用程序 **VPN**”部分中打开“启用 每应用程序 VPN”开关。
3. 如果启动 匹配应用程序时必须自动启动 Citrix Secure Access (macOS/iOS)，请打开“启用按需匹配应用程序”开关。对于大多数每应用程序案例，建议使用此

   在 MDM VPN 有效负载中，此字段对应于键 **OnDemandMatchAppEnabled**。
4. 在 提供商类型中，选择 数据包通道。

   在 MDM VPN 有效负载中，此字段对应于密钥提 供程序类型。
5. Safari 域名配置是可选的。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。如果要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。这些字段的配置可以在 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，您必须按照本指南创建
应用程序清单策略和凭据提供程序策略- https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/。

在 **PerApp VPN** 中配置拆分通道

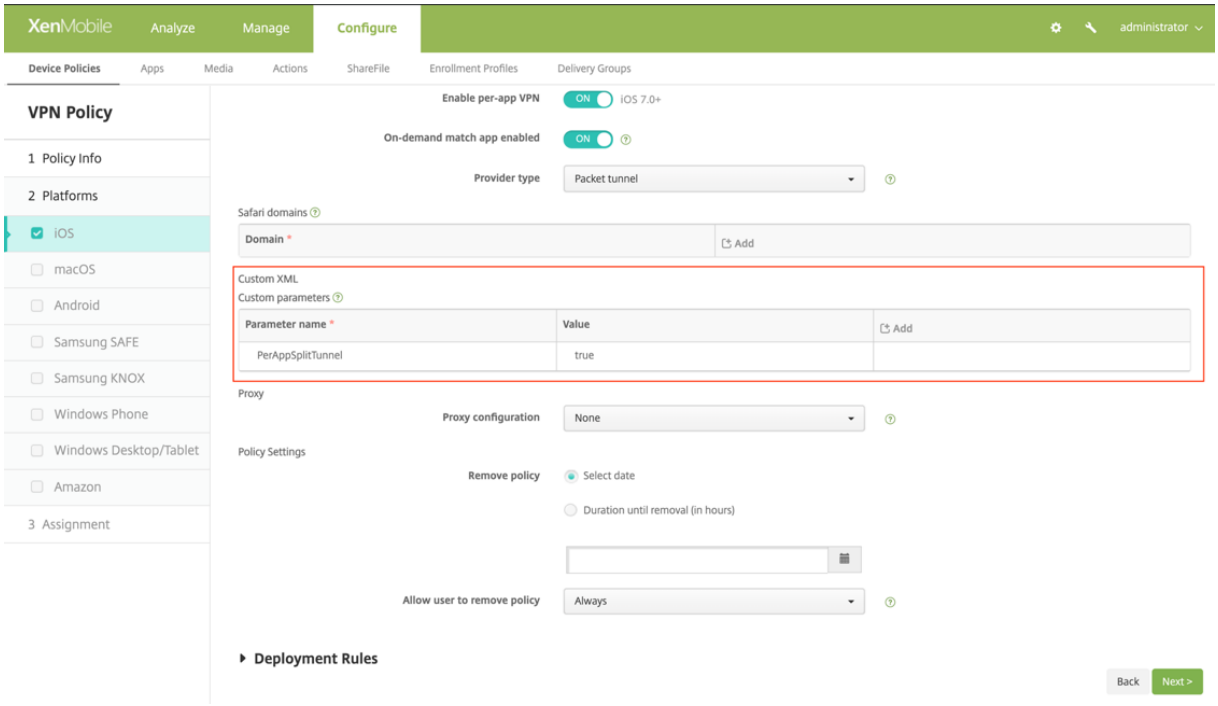
MDM 客户可以在 Per-App VPN 中为 Citrix Secure Access (macOS/iOS) 配置拆分通道。必须将以下键/值对添加到在 MDM 服务器上创建的 VPN 配置文件的供应商配置部分。

```
-  Key = "PerAppSplitTunnel"
-  Value = "true or 1 or yes"
<!--NeedCopy-->
```

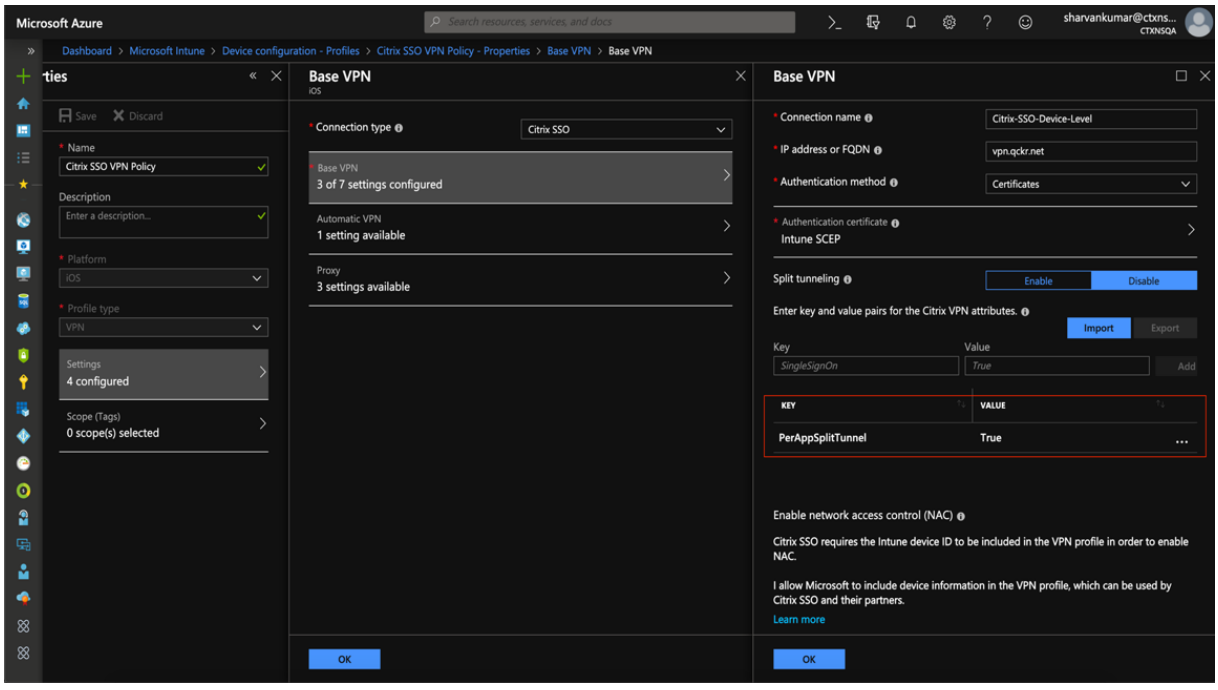
键区分大小写，必须完全匹配，而值不区分大小写。

> 注意：
>
> 用于配置供应商配置的用户界面在 MDM 供应商中不是标准的。请与 MDM 供应商联系，在 MDM 用户控制台上查找供应商配置部分。

以下是 Citrix Endpoint Management 中配置（特定于供应商的设置）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** 配置式

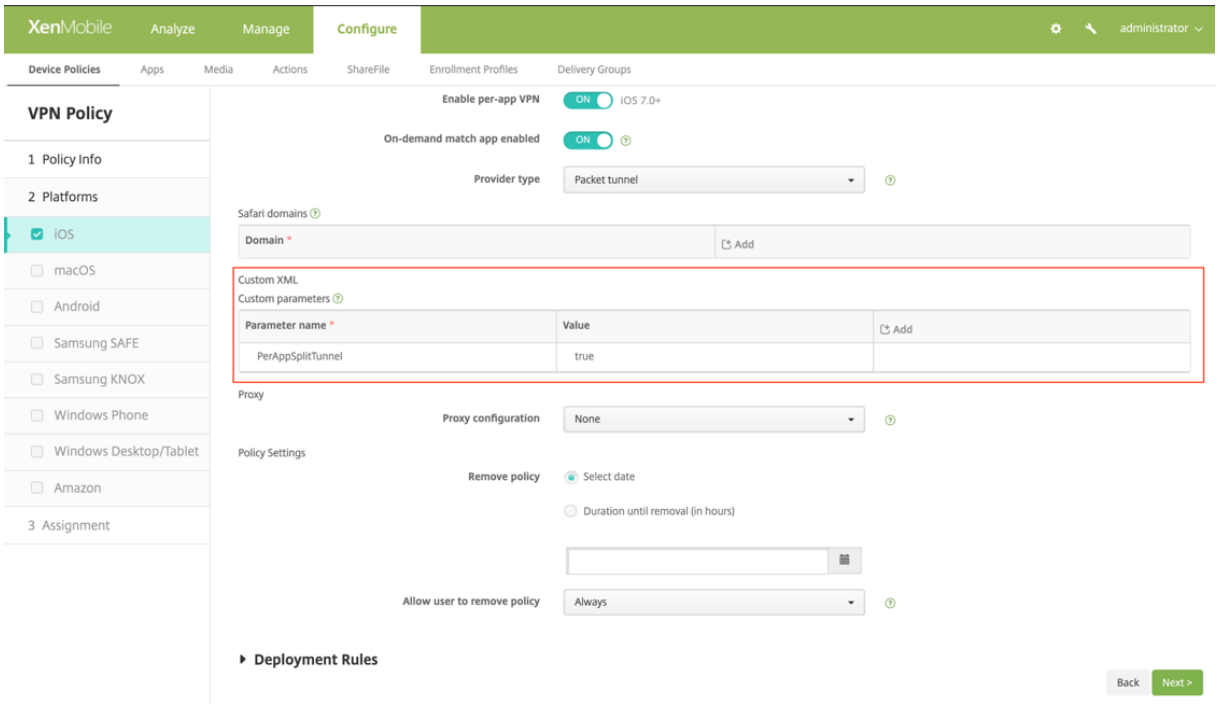
MDM 客户可以阻止用户在 Citrix Secure Access (macOS/iOS) 中手动创建 VPN 配置文件。为此，必须将以下键/值对添加到在 MDM 服务器上创建的 VPN 配置文件的供应商配置部分。


```
1  -  Key = "disableUserProfiles"
2  -  Value = "true or 1 or yes"
3  <!--NeedCopy-->
```

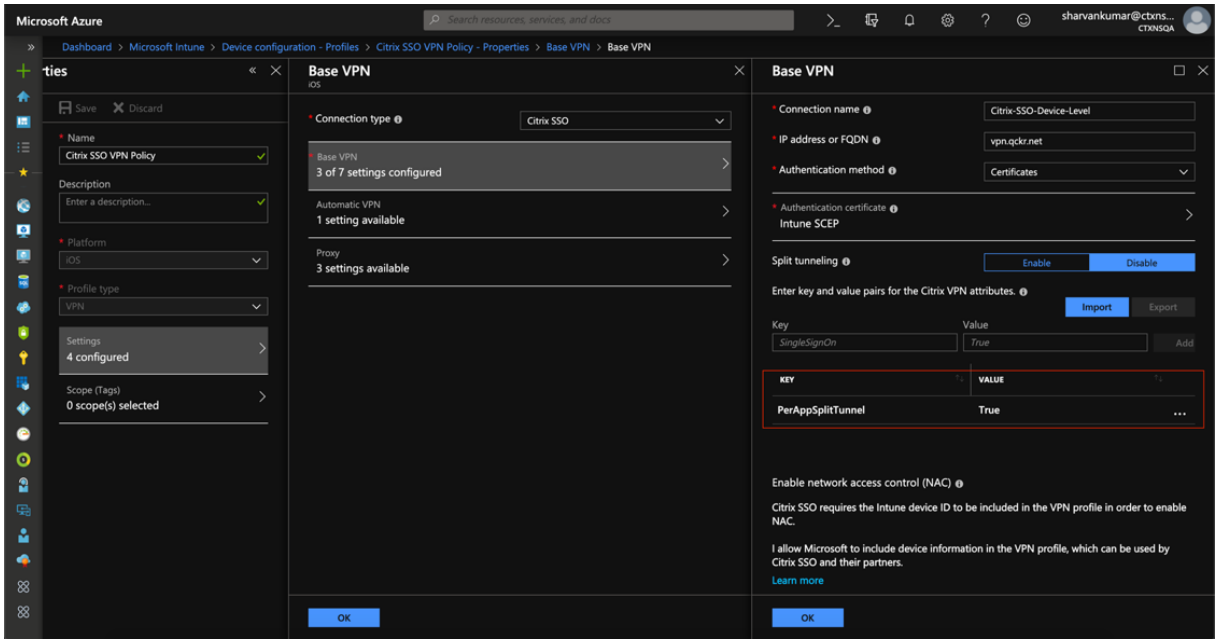
键区分大小写，必须完全匹配，而值不区分大小写。

> 注意：
>
> 用于配置供应商配置的用户界面在 MDM 供应商中不是标准的。请与 MDM 供应商联系，在 MDM 用户控制台上查找供应商配置部分。

以下是 Citrix Endpoint Management 中配置（特定于供应商的设置）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 客户端的推荐的 DNS 设置如下：

- 如果拆分通道设置为关，则拆分 **DNS > REMOTE**。
- 如果拆分通道设置为开，则拆分 **DNS > BOTH**。在这种情况下，管理员必须为 Intranet 域添加 DNS 后缀。属于 DNS 后缀的 FQDN 的 DNS 查询将通过通道传输到 NetScaler 设备，其余查询将转到本地路由器。

> 注意：
>
> - 建议将 **DNS** 截断修复 标志始终打 开。有关更多详细信息，请参阅https://support.citrix.com/article/CTX200243。
> - 当拆分通道设置为 开 并将拆分 DNS 设置为 **REMOTE** 时，在连接 VPN 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。

已知问题

问题描述：为包含 PerApp VPN 或按需 VPN 配置中的 “.local” 域的 FQDN 地址进行通道传输。Apple 的网络扩展框架存在一个错误，它阻止了域部分（例如 http://wwww.abc.local）中包含 .local 的 FQDN 地址通过系统的 TUN 接口进行通道传输。取而代之的是，FQDN 地址的流量通过客户端设备的物理接口发送。仅在 PerApp VPN 或按需 VPN 配置中观察到此问题，而在系统范围的 VPN 配置中不会出现此问题。Citrix 已向 Apple 提交了一份雷达错误报告，Apple 指出，根据 RFC-6762: https://tools.ietf.org/html/rfc6762，local 是一个多播 DNS (mDNS) 查询，因此不是错误。但是，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。

解决办法：为解决方法之类的地址分配 non .local 域名。

限制

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

将用户证书身份作为电子邮件附件发送给 iOS 用户

February 1, 2024

> 重要提示：
>
> 适用于 iOS 的 Citrix SSO 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

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，可以通过以下方式之一将证书交付给 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。有关此方法，请遵循 MDM 供应商特定的文档。
- 电子邮件 - 仅适用于非 MDM 客户的方法。在这种方法中，管理员向用户发送一封电子邮件，其中包含作为 PCKS #12 文件附加的用户证书身份（证书和私钥）。用户需要在 iOS 设备上配置其电子邮件帐户才能接收带有附件的电子邮件。然后可以将该文件导入到 iOS 上的 Citrix Secure Access。以下部分介绍了此方法的配置步骤。

必备条件

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

配置步骤

1. 重命名用户证书的扩展名 /MIME 类型。

   最常用于用户证书的文件扩展名为“.pfx”、“.p12”等。与.pdf、.doc 等格式不同，这些文件扩展名对于 iOS 平台来说是非标准的。“.pfx”和“.p12”均由 iOS 系统申领，Citrix Secure Access 等第三方应用程序无法申领。因此，Citrix Secure Access 定义了一种名为“.citrixsso-pfx”和“.citrixso-p12”的新扩展/MIME 类型。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，管理员可以在命令提示符或终端上运行以下命令。

Windows 10

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.
   citrixsso-pfx
<!--NeedCopy-->
```

macOS

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-
   pfx
<!--NeedCopy-->
```

2. 将文件作为电子邮件附件发送。

   具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 **iOS** 用户的 **Citrix SSO** 应用程序设置代理 **PAC** 文件或为 **macOS** 用户的 **Citrix Secure Access** 客户端设置代理 **PAC** 文件

February 1, 2024

> 重要提示：
>
> 适用于 iOS 的 Citrix SSO 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

适用于 iOS 的 Citrix Secure 应用程序或适用于 macOS 的 Citrix Secure Access 客户端在 VPN 通道建立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

有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 是 172.16.111.43，PAC 文件的名称是 proxy.pac。

如果实际代理服务器的 IP 地址是正在监听端口 8080 的 172.16.43.83，那么 proxy.pac 的示例如下：

```
function FindProxyForURL(url, host)
{
```


return “PROXY 172.16.43.83:8080”；
}

代理 PAC URL 是 http://172.16.111.43/proxy.pac。假设文件托管在端口 HTTP 端口 80 上。

有关更多详细信息，请参阅 https://support.citrix.com/article/CTX224235 或 NetScaler Gateway 的出站代理支持的代理自动配置。

注意：

- 如果“拆分通道”已打开，则确保内部网应用程序列表中包含承载 PAC 文件的服务器的 IP 地址，以便可以通过 VPN 访问该文件。
- 从 Citrix Secure Access (macOS/iOS) 登录后，浏览器开始使用代理 PAC 文件中的规则。如果像上一个示例一样只提供了一个代理规则，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**

February 1, 2024

> 重要提示：
>
> 适用于 iOS 的 Citrix SSO 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

适用于 macOS 的 Citrix Secure Access 客户端提供了 NetScaler Gateway 提供的一流应用程序访问和数据保护解决方案。现在，您可以随时随地安全地访问业务关键应用程序、虚拟桌面和企业数据。
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 的网络扩展在运行 macOS 10.11+ 的设备上可用。

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 PerApp 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的列表，请参阅 NetScaler Gateway VPN 客户端和支持的功能。

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。它支持称为网络访问控制 (NAC) 的功能，使用该功能，MDM 管理员可以在连接到 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 XenMobile 和 NetScaler Gateway 等 MDM 服务器。有关 NAC 的详细信息，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，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** 托管 **VPN** 配置文件

以下部分介绍了使用 Citrix Endpoint Management（以前称为 XenMobile）为示例为 Citrix Secure Access 配置设备范围和 PerApp VPN 配置文件的分步说明。其他 MDM 解决方案在使用 Citrix Secure Access 时可以使用本文档作为参考。

> 注意：
>
> 本部分说明基本的设备范围和 PerApp VPN 配置文件的配置步骤。您也可以按照 Citrix Endpoint Management（前身为 XenMobile）文档或 Apple 的 MDM VPN 有效负载配置来配置按需代理、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。根据 NetScaler 中定义的 VPN 策略（例如全通道、拆分通道、反向拆分通道），将来自所有应用程序和服务的流量通道传输到 NetScaler Gateway。

在 Citrix Endpoint Management 上配置设备级 VPN 执行以下步骤来配置设备级别的 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. 在左侧策略平台窗格中选择 **macOS** 。在右窗格中选择 **VPN** 策略。
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 macOS 的 策略详细信息 页面上，键入有效的连接名称，然后在 连接类型 中选择 自定义 **SSL**。

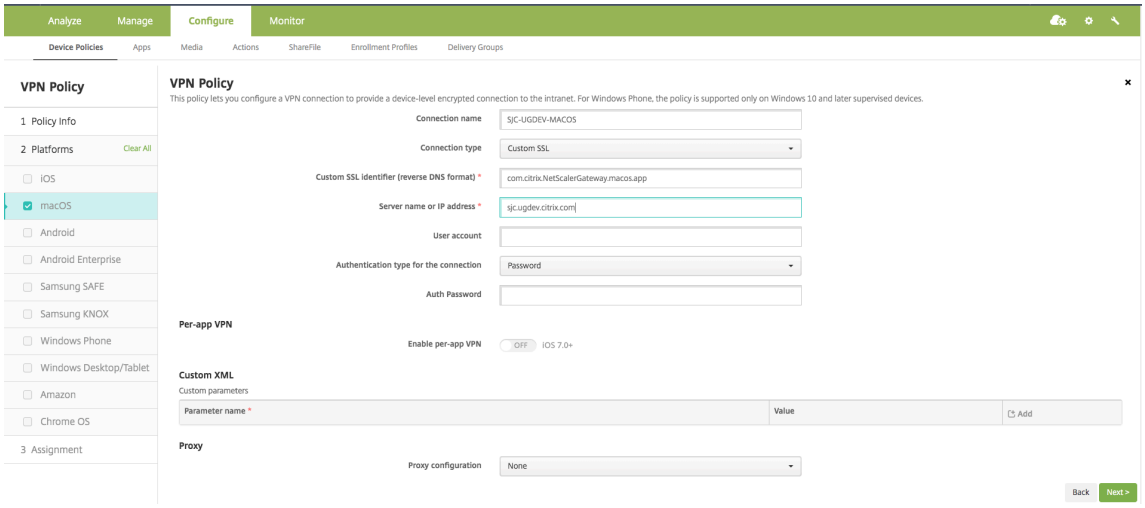
   在 MDM VPN 有效负载中，连接名称对应于 **UserDefinedName** 密钥，**VPN** 类型密钥 必须设置为 **VPN**。
5. 在自定义 **SSL** 标识符（反向 **DNS** 格式）中，输入 **com.citrix.NetScalerGateway.macos.app**。这是 macOS 上 Citrix Secure Access 的捆绑包标识符。

   在 MDM VPN 有效负载中，自定义 SSL 标识符对应于 **VPNSubType** 密钥。
6. 在提供商捆绑包标识符 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标识符。

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

   配置页面中的其余字段是可选的。这些字段的配置可以在 Citrix Endpoint Management 文档中找到。

8. 单击下一步。



9. 单击“保存”。

PerApp VPN 配置文件

PerApp VPN 配置文件用于为特定应用程序设置 VPN。仅来自特定应用程序的流量会通过通道传输到 NetScaler Gateway。P **er-App VPN** 有效载荷支持设备范围 **VPN** 的所有 密钥以及其他一些密钥。

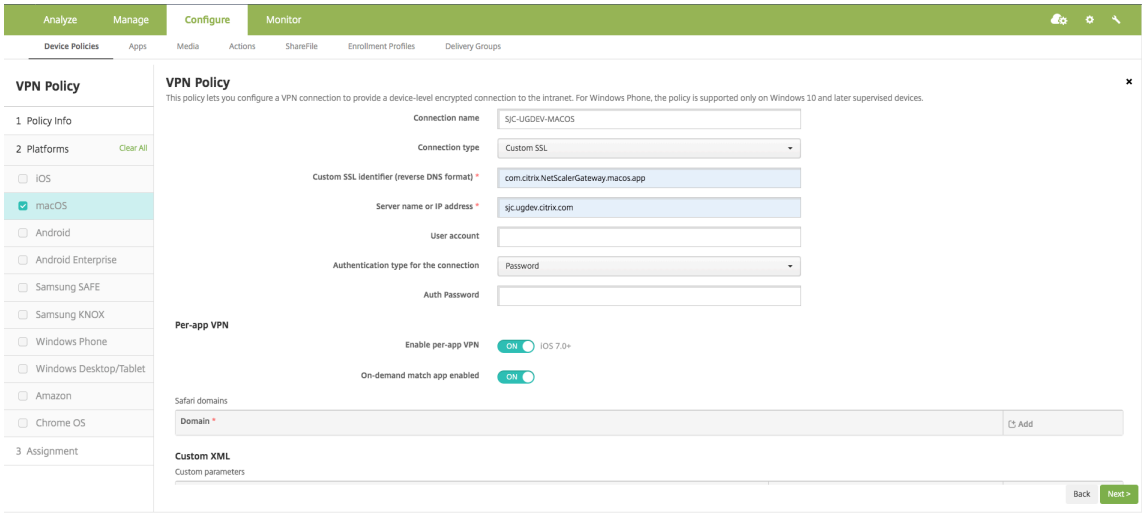
在 **Citrix Endpoint Management** 上配置每应用程序级别的 **VPN**　执行以下步骤在 Citrix Endpoint Management 上配置 PerApp VPN：

1. 在 Citrix Endpoint Management 上完成设备级别的 VPN 配置。
2. 打开“每应用程序 **VPN**”部分中的“启用每应用程序 **VPN**”开关。
3. 如果在启动 匹配应用程序时必须自动启动 **Citrix Secure Access**，请打开“按需匹配应用程序已启用”开关。对于大多数每应用程序案例，建议使用此

   在 MDM VPN 有效负载中，此字段对应于键 **OnDemandMatchAppEnabled**。
4. Safari 域名配置是可选的。配置 Safari 域后，当用户启动 Safari 并导航到与“域”字段中的 URL 相匹配的 URL 时，Citrix Secure Access 会自动启动。如果要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。这些字段的配置可以在 Citrix Endpoint Management（以前称为 XenMobile）文档中找到。



5. 单击下一步。
6. 单击“保存”。

   要将 VPN 配置文件与设备上的特定应用程序关联，您必须按照本指南创建应用程序清单策略和凭据提供程序策略- https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/

在 **PerApp VPN** 中配置拆分通道

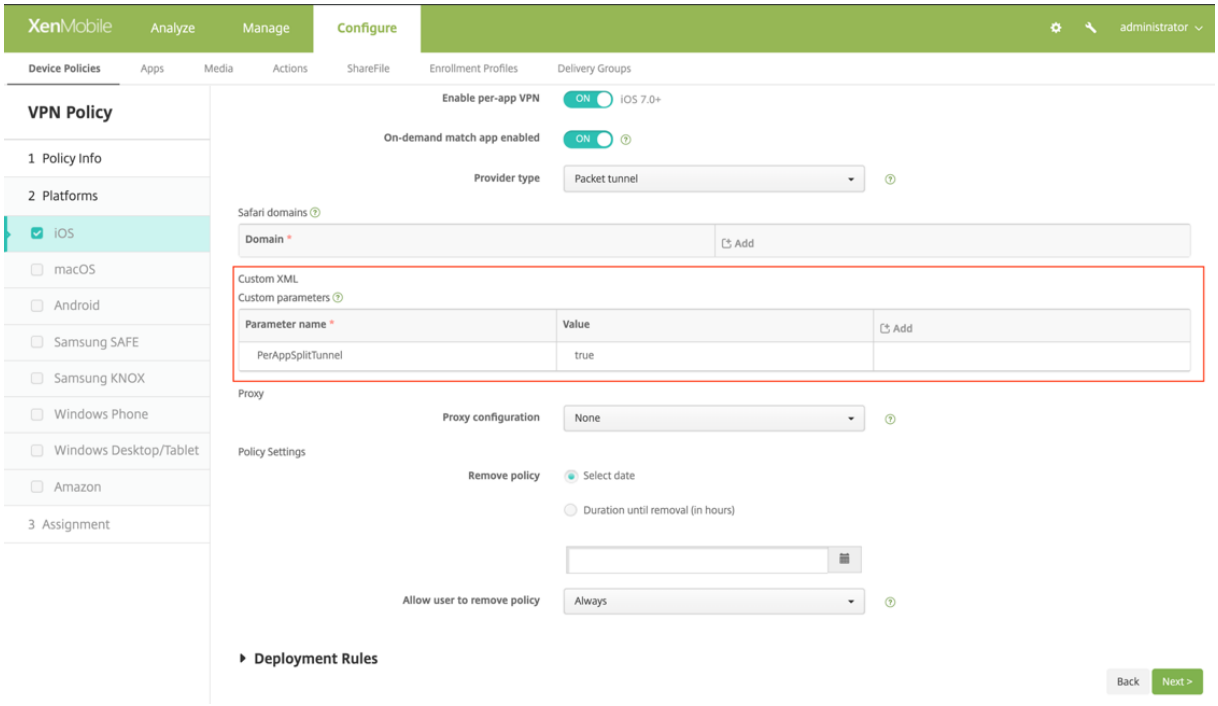
MDM 客户可以在 PerApp VPN 中为 Citrix Secure Access 配置拆分通道。必须将以下键/值对添加到在 MDM 服务器上创建的 VPN 配置文件的供应商配置部分。

```
1  -  Key = "PerAppSplitTunnel"
2  -  Value = "true or 1 or yes"
```

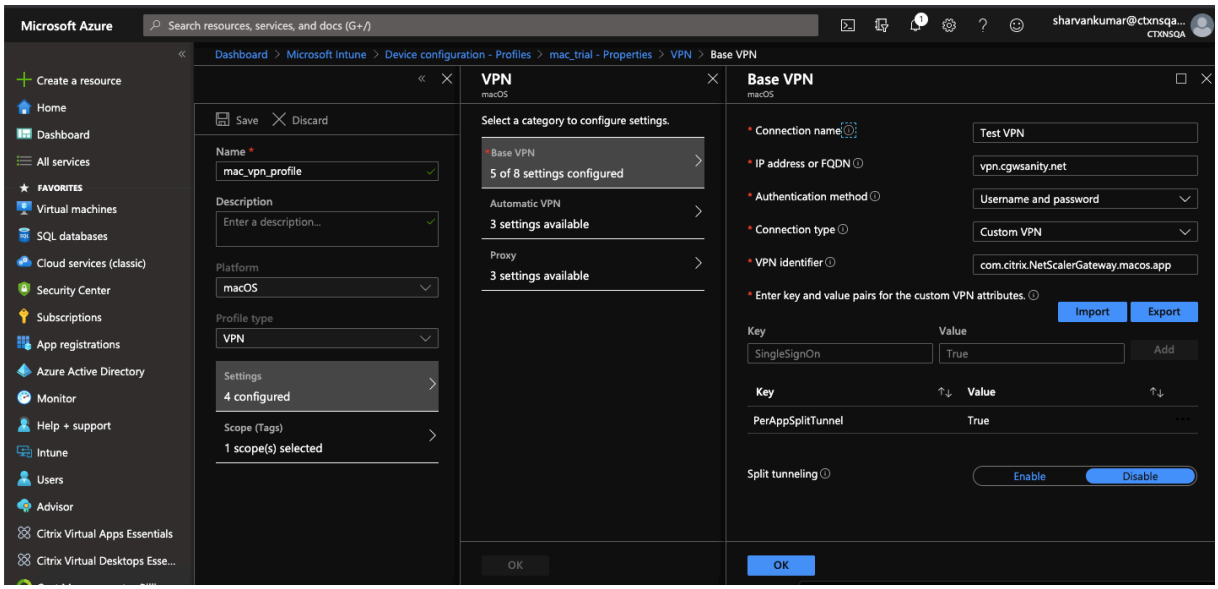
键区分大小写，必须完全匹配，而值不区分大小写。

> 注意：
>
> 用于配置供应商配置的用户界面在 MDM 供应商中不是标准的。请与 MDM 供应商联系，在 MDM 用户控制台上查找供应商配置部分。

以下是 Citrix Endpoint Management 中配置（特定于供应商的设置）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** 配置式

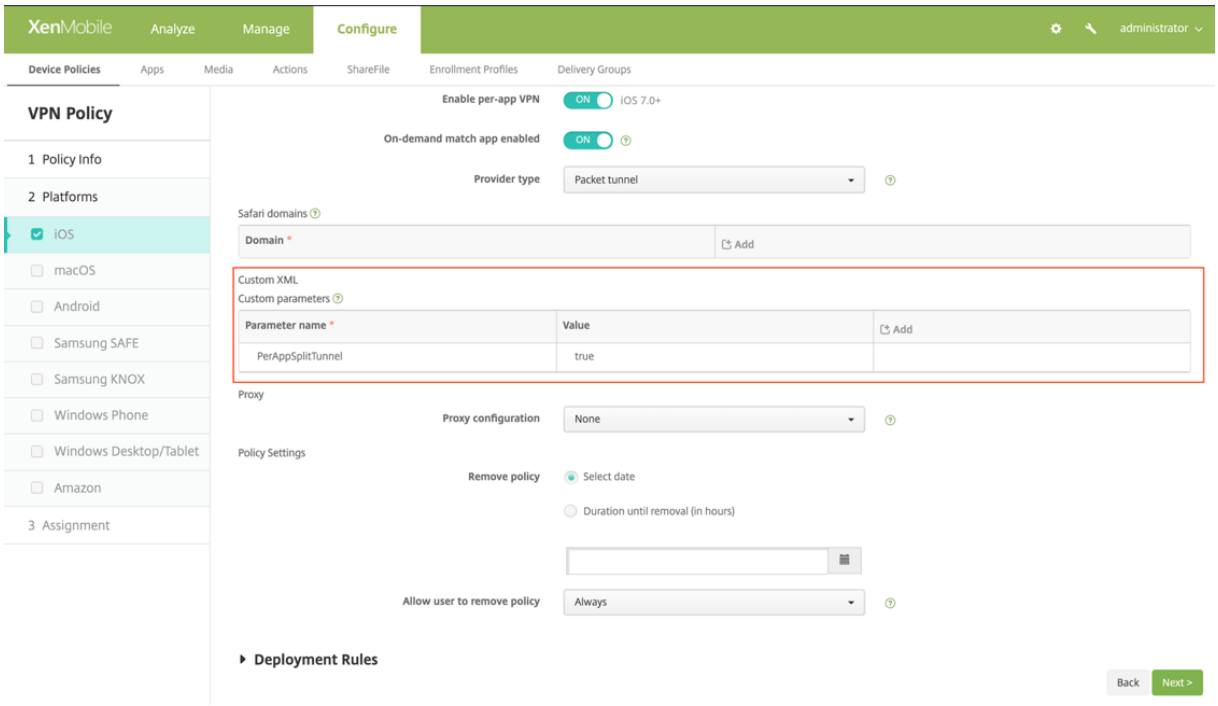
MDM 客户可以阻止用户从 Citrix Secure Access 中手动创建 VPN 配置文件。为此，必须将以下键/值对添加到在 MDM 服务器上创建的 VPN 配置文件的供应商配置部分。

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

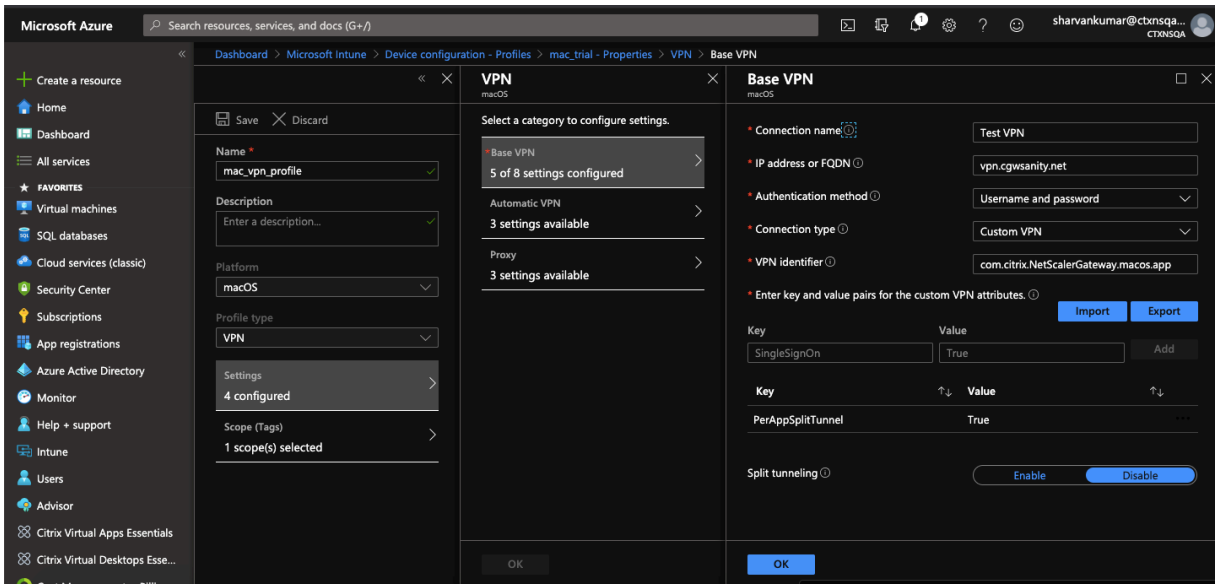

键区分大小写，必须完全匹配，而值不区分大小写。

> 注意：
>
> 用于配置供应商配置的用户界面在 MDM 供应商中不是标准的。请与 MDM 供应商联系，在 MDM 用户控制台上查找供应商配置部分。

以下是 Citrix Endpoint Management 中配置（特定于供应商的设置）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 的建议使用 DNS 设置如下：

- 如果拆分通道设置为关，则拆分 **DNS > REMOTE**。
- 如果拆分通道设置为开，则拆分 **DNS > BOTH**。在这种情况下，管理员必须为 Intranet 域添加 DNS 后缀。属于 DNS 后缀的 FQDN 的 DNS 查询将通过通道传输到 NetScaler 设备，其余查询将转到本地路由器。

> 注意：
>
> - 建议将 **DNS** 截断修复 标志始终打 开。有关更多详细信息，请参阅https://support.citrix.com/article/CTX200243。
> - 当拆分通道设置为 开 并将拆分 DNS 设置为 **REMOTE** 时，在连接 VPN 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，请参阅最新的 EPA 库。

1. 在 **OPSWAT v4** 支持的扫描列表部分中，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

以下是当前的已知问题。

- 如果将用户置于隔离组中，EPA 登录将失败。
- 不显示强制超时警告消息。
- 如果拆分通道处于开启状态且未配置任何内联网应用程序，则 Citrix Secure Access 允许登录。

限制

以下是目前的限制。

- 以下 EPA 扫描可能会失败，因为沙箱导致对安全访问的访问受到限制。
  - 硬盘加密“类型”和“路径”
  - Web 浏览器“默认”和“正在运行”
  - 修补程序管理“缺少补丁”
  - 在 EPA 期间终止进程操作
- 不支持基于端口/协议的拆分通道。
- 确保密钥链中没有两个具有相同名称和过期日期的证书，因为这会导致客户端只显示其中一个证书，而不是同时显示两个证书。

故障排除

如果在 Citrix Secure Access 的身份验证窗口中向最终用户显示下载 **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，以便允许使用 `com.citrix.agmacepa://`。

nFactor 支持 macOS/iOS 上的 Citrix Secure Access 客户端

February 1, 2024

> 重要提示：
>
> 适用于 iOS 的 Citrix SSO 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

多重 (nFactor) 身份验证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按任意顺序进行配置。

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，将使用 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来呈现身份验证 GUI。
- 经典—经典协议是在网关的 VPN 虚拟服务器上配置经典身份验证策略时使用的默认回退协议。如果 nFactor 对于特定的身份验证方法（例如 NAC）失败，则经典协议是后备协议。
- **Citrix** 身份平台—Citrix 身份平台协议用于对 CloudGateway 或 Citrix Gateway 服务进行身份验证，需要在 Citrix Cloud 注册 MDM。

下表总结了每种协议支持的各种身份验证方法。

身份验证方法	nFactor	经典	Citrix IdP
客户端证书	受支持	受支持	不支持
LDAP	受支持	受支持	不支持
本地	受支持	受支持	不支持
RADIUS	受支持	不支持	不支持
SAML	受支持	不支持	不支持
OAuth	受支持	不支持	不支持

身份验证方法	nFactor	经典	Citrix IdP
TACACS	受支持	不支持	不支持
WebAuth	受支持	不支持	不支持
谈判	受支持	不支持	不支持
EPA	受支持	受支持	不支持
NAC	不支持	受支持	不支持
StoreFront	不支持	不支持	不支持
ADAL	不支持	不支持	不支持
DS-AUTH	不支持	不支持	受支持

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：
>
> 要在 macOS/iOS 上将 nFactor 协议与 Citrix Secure Access 客户端一起使用，推荐的 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）要求客户端发送签名的设备标识符，作为 NetScaler Gateway 身份验证的一部分。签名的设备标识符是一个可旋转的私有密钥，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 配置文件上启用 NAC，则 macOS/iOS 上的 Citrix Secure Access 客户端会自动回退到经典身份验证协议。
- 您无法使用适用于 macOS 的 Intune 配置 NAC 检查，因为与 iOS 不同，Intune 没有提供为 macOS 启用 NAC 的选项。

解决常见的 **Citrix Secure Access for macOS/iOS** 问题

February 1, 2024

> 重要提示：
>
> 适用于 iOS 的 Citrix SSO 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

DNS 解析问题

- 如果设备进入睡眠状态或长时间处于非活动状态，则 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阻止了 DNS 流量。请参阅 https://support.citrix.com/article/CTX232237 以解决此问题。
- 始终从浏览器检查 DNS 解析。使用终端 `nslookup` 命令进行的 DNS 查询可能不准确。如果必须使用命 `nslookup` 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

- 网守被认为是防病毒软件。如果有扫描检查“任何防病毒软件”（MAC-ANTIVIR_0_0），即使用户没有安装其他供应商的任何防病毒软件，扫描也始终会通过。

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 `clientsecurityLog` 将 VPN 参数设置为 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”应用程序。“软件更新”的版本必须类似于 `"MAC-PATCH_100011_100076_VERSION_==_3.0[COMMENT: Software Update]"`
- 始终使 NetScaler 上的 EPA 库保持最新状态。最新的库可以在以下位置找到 https://www.citrix.com/downloads/citrix-gateway/epa-libraries/epa-libraries-for-netscaler-gateway.html

nFactor 问题

- Citrix Secure Access 打开 **Citrix SSO** 身份验证窗口，用于 nFactor 身份验证。它类似于浏览器。如果此页面上有错误，可以通过在 Web 浏览器上尝试进行身份验证来进行交叉验证。
- 如果启用 nFactor 后传输登录失败，则将门户主题更改为“RFWeBUI”。
- 如果收到错误消息“无法建立与 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“无法访问网关”，则网关服务器证书已过期或服务器证书已绑定启用 SNI。Citrix Secure Access 尚不支持 SNI。在未启用 SNI 的情况下绑定服务器证书。该错误还可能是由于在 MDM VPN 配置文件中配置的证书固定以及 NetScaler Gateway 提供的证书与固定的证书不匹配所致。
- 尝试连接到网关时，如果 **Citrix SSO** 身份验证窗口 打开但为空白，则检查 ECC 曲线 (ALL) 是否绑定到默认密码组。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。

常见问题解答

February 1, 2024

> 重要提示：
>
> 适用于 iOS 的 Citrix SSO 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

本节介绍有关适用于 macOS/iOS 的 Citrix Secure Access 的常见问题解答。

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 iOS 版 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，这些应用程序现已过时。应用商店中不再提供对 Citrix VPN 的支持。

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。支持 SSL VPN 的网络
扩展可在运行 iOS 9+ 和 macOS 10.11+ 的设备上使用。

适用于 **macOS/iOS** 的 **Citrix Secure Access** 客户端兼容哪些版本的 **NetScaler**?
NetScaler 版本 10.5 及更高版本支持适用于 macOS/iOS 的 Citrix Secure Access 客户端中的 VPN 功能。TOTP 在 NetScaler 版本 12.0 及更高版本上可用。NetScaler 上的推送通知尚未公开宣布。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运作?
之前通过电子邮件或浏览器分发证书以在 VPN 中执行客户证书身份验证的客户在使用适用于 macOS/iOS 的 Citrix Secure Access Client 时必须注意这一更改。对于不使用 MDM 服务器分发用户证书的非 MDM 客户来说尤其如此。

什么是网络访问控制 **(NAC)**？如何使用适用于 **iOS** 的 **Citrix Secure Access** 和 **NetScaler Gateway** 配置 **NAC**?
Microsoft Intune 和 Citrix Endpoint Management（前身为 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。使用 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。管理员可以在身份验证时在适用于 iOS 的 Citrix Secure Access 中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，必须在 NetScaler Gateway 和 MDM 服务器上启用它。

- 要在 NetScaler 上启用 NAC，请参阅 配置 NetScaler Gateway 虚拟服务器的网络访问控制设备检查以进行单因素登录。
- 如果 MDM 供应商是 Intune，请参阅 与 Intune 的网络访问控制 (NAC) 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 客户端支持的最低版本为 1.1.6 及更高版本。

适用于 **Android** 的 **Citrix Secure Access**

February 1, 2024

适用于 Android 的 Citrix Secure Access（以前称为 Citrix SSO）提供了 NetScaler Gateway 提供的一流应用程序访问和数据保护解决方案。现在，您可以随时随地安全地访问业务关键应用程序、虚拟桌面和企业数据。

> 重要提示：
>
> Citrix SSO for Android 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

发行说明

February 1, 2024

> 重要提示：
>
> - Citrix SSO for Android 现已重命名为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。在此过渡期间，您可能会注意到文档中使用的 Citrix SSO 参考资料。
> - 基于 FQDN 的分割通道和 nFactor 身份验证支持目前处于预览阶段。
> - 2020 年 6 月之后，Android 6.x 及更低版本将不支持 Citrix Secure Access。

Citrix Secure Access 发行说明描述了服务版本中的新功能、现有功能的增强、已修复的问题和已知问题。发行说明包括以下一个或多个部分：

新增功能：当前版本中提供的新增功能和增强功能。

已修复的问题：当前版本中修复的问题。

已知问题：当前版本中存在的问题及其解决方法（如果适用）。

V23.12.2（2023 年 12 月 15 日）

> 注意：
>
> 适用于 Android 的 Citrix Secure Access 版本 23.12.2 包括针对 CSACLIENTS-8799 的修复，并取代了 23.12.1 版。

[CSACLIENTS-8799]

新增功能

- **Citrix SSO for Android** 更名为 **Citrix Secure Access**

  Citrix SSO for Android 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

  [CSACLIENTS-6337]

- 在 **Android 13** 及以上设备上接收或屏蔽通知

  在 Android 13 设备上安装或重新安装 Citrix Secure Access 客户端时，现在会提示最终用户提供从 Citrix Secure Access 客户端接收通知的权限。如果最终用户拒绝许可，他们将不会在其 Android 设备上收到任何 VPN 状态或来自 Citrix Secure Access 客户端的推送通知。建议 MDM 管理员在其解决方案中向 Citrix Secure Access（软件包 ID：`com.citrix.CitrixVPN`）授予通知权限。

  最终用户可以导航到 Android 设备上的设置 **>** 通知，以更改
  Citrix Secure Access 客户端的通知权限。有关详细信息，请参阅如何在 Android 设备上使用 Citrix Secure Access。

  [CSACLIENTS-8252]

- 支持在始终可用的 **VPN** 模式下转移登录

  适用于 Android 的 Citrix Secure Access 现在支持“始终可用的 VPN”模式下的“转移登录”功能。有关如何配置转移登录的详细信息，请参阅配置转移登录页面。

  [CSACLIENTS-8305]

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。

[CSACLIENTS-8799]

V23.10.2（2023 年 12 月 19 日）

新增功能

> 备注：
>
> - Citrix SSO for Android 版本 23.10.2 包括针对 CSACLIENTS-8314 的修复，并取代了 23.10.1 版。
> - Citrix SSO for Android 23.10.1 适用于 Android 14。

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

  现在，当 VPN 连接中断时，Citrix SSO for Android 会提示您使用 NetScaler Gateway 重新进行身份验证。您会在 Citrix SSO 界面和 Android 设备的通知面板上收到通知，表明与 NetScaler Gateway 的连接已断开，必须重新进行身份验证才能恢复连接。此功能在预览版中提供。

  有关更多信息，请参阅 VPN 连接失败后重新连接到 NetScaler Gateway。

已修复的问题

在某些始终可用的 VPN 场景中重新启动 VPN 服务时，Citrix SSO 会间歇性地崩溃。

[CSACLIENTS-8314]

V23.8.1 (2023 年 8 月 31 日)

新增功能

- 自动重启始终可用的 **VPN**

  当允许列表或阻止列表中的应用安装在工作资料或设备资料中时，Citrix SSO 应用会自动重启始终可用的 VPN。来自此应用程序的流量会自动通过 VPN 连接进行通道传输，无需重新启动工作配置文件或重启设备。要启用始终可用的 VPN 的自动重启，最终用户必须向 Citrix SSO 应用授予查询所有包的同意。有关更多信息，请参阅自动重启始终可用的 VPN。

  [CSACLIENTS-6158]

- 在托管 **VPN** 配置文件中启用调试日志记录

  MDM 管理员现在可以在 Endpoint Management 控制台的托管 VPN 配置文件中将调试日志作为自定义参数启用。要启用调试日志记录，必须将 `EnableDebugLogging` 的值设置为 True。如果任何托管 VPN 配置启用了调试日志记录，则调试日志记录功能将在解析配置后生效。有关更多详细信息，请参阅 Intune 配置的自定义参数。

  [CSACLIENTS-3746]

已修复的问题

- 有时，Citrix SSO 应用程序可能无法通过通道将流量传输到某些资源。当分割通道设置为 OFF 并且某些无法访问的域或 IP 地址被黑洞访问时，就会出现此问题。

[NSHELP-35555]

V22.11.1（2022 年 11 月 30 日）

新增功能

- **Citrix Secure Access** 已更新为针对 **Android 12.1**（**API** 级别 **32**）

  Citrix Secure Access 现已更新为针对 Android 12.1（API 级别 32）。对于每个应用程序的 VPN，如果在设置 VPN 通道后安装了每个应用程序 VPN 软件包列表中的一个软件包，则 VPN 服务可能不会自动重启。这是由于 Android 11 中引入的应用程序可见性限制所致。有关详细信息，请参阅 https://developer.android.com/training/package-visibility。

  [CGOP-21409]

V22.10.1（2022 年 10 月 21 日）

新增功能

- 应用程序版本号的显示更新为 YY.MM.point-release 格式，其中 YY 表示 2 位数年份，MM 表示 2 位数月份，积分发行量为 1+，具体取决于一个月内的版本号。
- 对于 Android 客户端，Google Analytics/Crashlytics 从欧盟地区收集数据已禁用。

已修复的问题

- 在“添加连接”和“编辑连接”屏幕中因输入无效而出现的错误消息未本地化。

  [CGOP-22060]

V2.5.3 (2022 年 5 月 5 日)

新增功能

- Citrix SSO 已更新为 Android 11 目标 SDK (API 30)

  Citrix SSO 应用程序现已更新为 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 https://support.citrix.com/article/CTX331615。

  [CGOP-19774]

已修复的问题

- 有时，Citrix SSO 可能不会在网络更改后使用备用 DNS 服务器进行主机名解析。

  [NSHELP-29378]

V2.5.2（2021 年 10 月 21 日）

已修复的问题

- 有时，Citrix SSO 在处理 NAC 检查中的不合规错误时会崩溃。

  [CGOP-19198]

V2.5.1 (2021 年 8 月 12 日)

已修复的问题

- 当 CNAME 链长度超过 6 个跃点时，Citrix SSO 应用程序无法解析主机。

  [CGOP-18475]
- 当 NetScaler Gateway 仅需要 NAC 检查身份验证时，Citrix SSO 会显示身份验证提示。

  [CGOP-18348]
- Citrix SSO 在处理异常大的 ICMP 数据包时可能会崩溃。

  [CGOP-18286]
- 在某些 Android 8.0 设备上添加 VPN 配置文件时，Citrix SSO 可能会崩溃。

  [CGOP-17607]
- 当您重新启动为“始终开启”配置的 VPN 时，Citrix SSO 可能会崩溃。

  [CGOP-17580]
- 在 nFactor 身份验证流程中处理 SSL 错误时，Citrix SSO 可能会崩溃。

  [CGOP-17577]

V2.5.0（2021 年 6 月 8 日）

新增功能

- 支持基于 **FQDN** 的拆分通道

Citrix SSO for Android 现在支持基于 FQDN 的拆分通道。

[CGOP-12079]

已修复的问题

- Citrix SSO 预览版 2.5.0 无法连接到 NetScaler Gateway 版本 12.1 及更早版本 (110)。

  [CGOP-17735]
- 重新启动 SSO 应用程序后，不会应用“DisableUserProfiles”设置。

  [CGOP-17454]

V2.4.16 (31-Mar-2021)

已修复的问题

- 如果某些设备未启用安全浏览，则 nFactor 身份验证将中止。

  [CGOP-17514]

V2.4.15 (17-Mar-2021)

已修复的问题

- 有时，NetScaler Gateway 设备上发生会话超时时时，Citrix SSO 不会重新连接始终可用的 VPN。

  [CGOP-16800]

V2.4.14 (23-Feb-2021)

已修复的问题

- 当将带有仅证书身份验证的 Always-On VPN 与 nFactor 身份验证一起使用时，Citrix SSO 需要用户交互。

  [CGOP-16805]
- 有时，Citrix SSO 可能会在 VPN 服务重启或过渡期间崩溃。

  [CGOP-16766]

V2.4.13 (04-Feb-2021)

已修复的问题

- 在某些情况下，Citrix SSO 登录请求会在 NetScaler Gateway 响应之前超时。

  [CGOP-16759]

V2.4.12 (2021 年 1 月 15 日)

此版本解决了有助于改进整体性能和稳定性的各种问题。

V2.4.11 (08-Jan-2021)

- 经典身份验证失败，因为 Citrix SSO 向 NetScaler Gateway 发送 HTTP 标头（X-Citrix-Gateway），该标头仅在 nFactor 身份验证中使用。

  [CGOP-16449]

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。

  [CGOP-16219]

- 执行经典身份验证时，Citrix SSO 可能会崩溃。

  [CGOP-16012]

- 旋转设备时，Citrix SSO 应用程序的方向不会更改。

  [CGOP-639]

V2.4.9 (20-Nov-2020)

已修复的问题

- 当用户单击设备上的 TOTP 令牌值时，Citrix SSO 应用程序崩溃。

  [CGOP-15886]

V2.4.8 (04-Nov-2020)

已修复的问题

- 在网关上的会话超时后断开 VPN 连接时，Citrix SSO 可能会崩溃。

  [CGOP-15592]

V2.4.7 (12-Oct-2020)

此版本解决了有助于改进整体性能和稳定性的各种问题。

V2.4.6 (28-Sep-2020)

此版本解决了有助于改进整体性能和稳定性的各种问题。

V2.4.5 (16-Sep-2020)

新增功能

- 新的 NetScaler 徽标已推出。

  [CGOP-15327]

V2.4.4 (10-Sep-2020)

已修复的问题

- 有时，Citrix SSO 在重新连接 VPN 会话时会崩溃。

  [CGOP-15215]

V2.4.3

已知问题

- 当 Android 设备受到资源限制时，Citrix SSO 无法建立与 NetScaler Gateway 的 VPN 会话。

  [NSHELP-24647]

V2.4.2

已修复的问题

- 加载先前保存的损坏令牌数据时，Citrix SSO 应用程序崩溃。通过此修复，令牌列表中损坏的令牌值将显示为“令牌数据已损坏”。删除损坏的令牌，然后再次添加。

  [CGOP-14546]

V2.4.1

已修复的问题

- 2020 年 6 月之后，Android 6.x 及更低版本不支持 Citrix SSO 应用程序。

  [CGOP-13853]

V2.3.19

此版本解决了有助于改进整体性能和稳定性的各种问题。

V2.3.18

新增功能

- 适用于 Android 10 设备的 Android Citrix SSO 应用程序现在支持代理配置。

  [CGOP-12007]

V2.3.17

此版本解决了有助于改进整体性能和稳定性的各种问题。

V2.3.16

此版本解决了有助于改进整体性能和稳定性的各种问题。

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。

  [CGOP-12538]
- 适用于 Android 的 Citrix SSO 应用程序 10 现在可以从系统设置中检测始终可用的 VPN。

  [CGOP-12656]

已修复的问题

- 如果仅定义了 MDM VPN 配置文件，则在断开与 VPN 的连接时，Citrix SSO 应用程序会崩溃。

  [CGOP-13825]

V2.3.14

新增功能

- Citrix SSO 应用程序现在可以代表 Citrix Workspace 应用程序对本机应用程序单点登录执行用户身份验证。

  [CGOP-12083]
- 如果在 VPN 通道设置之后安装了每个应用程序 VPN 软件包列表中的一个软件包，则 VPN 服务将重新启动。

  [CGOP-11262]

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。

  [CGOP-12488]
- NetScaler Gateway IP 地址现在只能解析一次。之前，NetScaler Gateway IP 地址已被多次解析，有时会导致连接失败。

  [CGOP-12101]

已知问题

- 应用程序用户界面中的 Always-On VPN 状态并不总是正确更新。

  [NSHELP-21709]

V2.3.13

已修复的问题

- NetScaler Gateway IP 地址现在只能解析一次。

  之前，NetScaler Gateway IP 地址已被多次解析，有时会导致连接失败。

  [CGOP-12101]

已知问题

- 应用程序用户界面中的 Always-On VPN 状态并不总是正确更新。

  [NSHELP-21709]

V2.3.12

已修复的问题

- 保存 VPN 配置文件时，Citrix SSO 可能会崩溃。

  [CGOP-12137]

V2.3.11

已修复的问题

- 保存 VPN 配置文件时，Citrix SSO 可能会崩溃。

  [CGOP-12137]

- 当新的 VPN 配置文件或对现有配置文件的更新导致 disableUserProfile 值发生更改时，disableUserProfile 设置不会正确反映在用户界面中。

  [CGOP-11899]

- Citrix SSO for Android 不会在设备所有者 (DO) 模式下处理 VPN 配置文件。

  [CGOP-11981]

- 当只有 IPv6 的本地 DNS 服务器时，不会建立 VPN 连接。

  [CGOP-12053]

V2.3.10

已修复的问题

- 在设备上空闲一段时间后，VPN 连接丢失。

  [CGOP-11381]

V2.3.8

新增功能

- 在 **Intune Android Enterprise** 环境中设置 **Citrix SSO** 应用

  现在，您可以在 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 SSO 应用程序。

  [CGOP-635]

- 支持通过 **Android Enterprise** 配置 **VPN** 配置文件

  现在支持通过 Android Enterprise 配置 VPN 配置文件。

  [CGOP-631]

已修复的问题

- 如果您保存已保存的令牌然后尝试将其打开，令牌名称中会出现乱码字符。

  [CGOP-11696]

- 如果 NetScaler Gateway 上未配置 DNS 搜索域，Citrix SSO 应用程序将无法建立 VPN 会话。

  [CGOP-11259]

V2.3.6

新增功能

- 对 **Citrix SSO** 的始终在机支持

  Citrix SSO 的始终开启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 通道来实现的。

  [CGOP-10015]

- 如果 **Athena** 令牌到期导致注销，则会显示重新登录的通知

  如果满足以下条件，则会显示一条提示用户重新登录 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
  - 由于雅典娜令牌到期，用户已退出 Citrix Workspace 应用程序

  [CGOP-10016]

- 使用 **NetScaler Gateway** 完成推送通知服务的注册

  现在，您可以使用 NetScaler Gateway 设备注册推送通知服务。之前，注册是在客户端设备上完成的。

  [CGOP-10542]

已修复的问题

有时，当扫描新令牌时，Citrix SSO 会崩溃。例如，当删除现有令牌并使用相同的令牌名称扫描另一个令牌时，Citrix SSO 会崩溃。

[CGOP-10818]

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，包括针对 Android Enterprise 环境的“BlockUntrustedServers”、“DefaultProfileName”和“DisableUserProfiles”设置。

  [CGOP-10033]

- 增强的推送通知支持

  在为 NetScaler Gateway 配置类型为“OTP”的推送通知时，在用户选择“允许”以响应请求用户同意允许身份验证继续进行的推送通知时，系统不会询问 PIN/ 指纹。

  [CGOP-9843]

- **Firebase** 分析支持

  添加了对基本 Firebase 分析的支持，以提供有关 Citrix SSO 应用程序的使用情况信息。该增强功能适用于粗略的地理位置，屏幕使用情况，正在使用的不同版本的 Android 等。

  [CGOP-7523]

- 支持基于 **Android** 托管配置的 **VPN** 配置文件配置

  可以使用诸如 Citrix Endpoint Management 之类的 EMM/UEM 供应商在 Android Enterprise 环境中配置 Citrix SSO 应用程序。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，以实现简化的双重身份验证体验。

  [CGOP-9592]

已修复的问题

- “添加连接”屏幕下的“服务器”字段中允许使用非 URL 字符。

  [CGOP-588]

在 MDM 环境中设置 Citrix Secure Access

February 1, 2024

> 重要提示：
>
> Citrix SSO for Android 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

要在 MDM 环境中设置 Citrix Secure Access 协议，请参阅配置适用于 Android 的 Citrix Secure Access 协议。

> 备注：
>
> - 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 为 Android Enterprise 配置 VPN 配置文件。
> - 对于使用 Citrix Secure Access 23.12.1 及更高版本的 Android 13 以上的用户，建议 MDM 管理员在其解决方案中向 Citrix Secure Access（软件包 ID：`com.citrix.CitrixVPN`）授予通知权限。

在 **Intune Android Enterprise** 环境中设置 **Citrix Secure Access**

February 1, 2024

> 重要提示：
>
> Citrix SSO for Android 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

该主题详细介绍了如何通过 Microsoft Intune 部署和配置 Citrix Secure Access。本文档假定 Intune 已针对 Android Enterprise 支持进行了配置，并且设备注册已经完成。

必备条件

- Intune 已针对 Android Enterprise 支持进行了配置
- 设备注册已完成

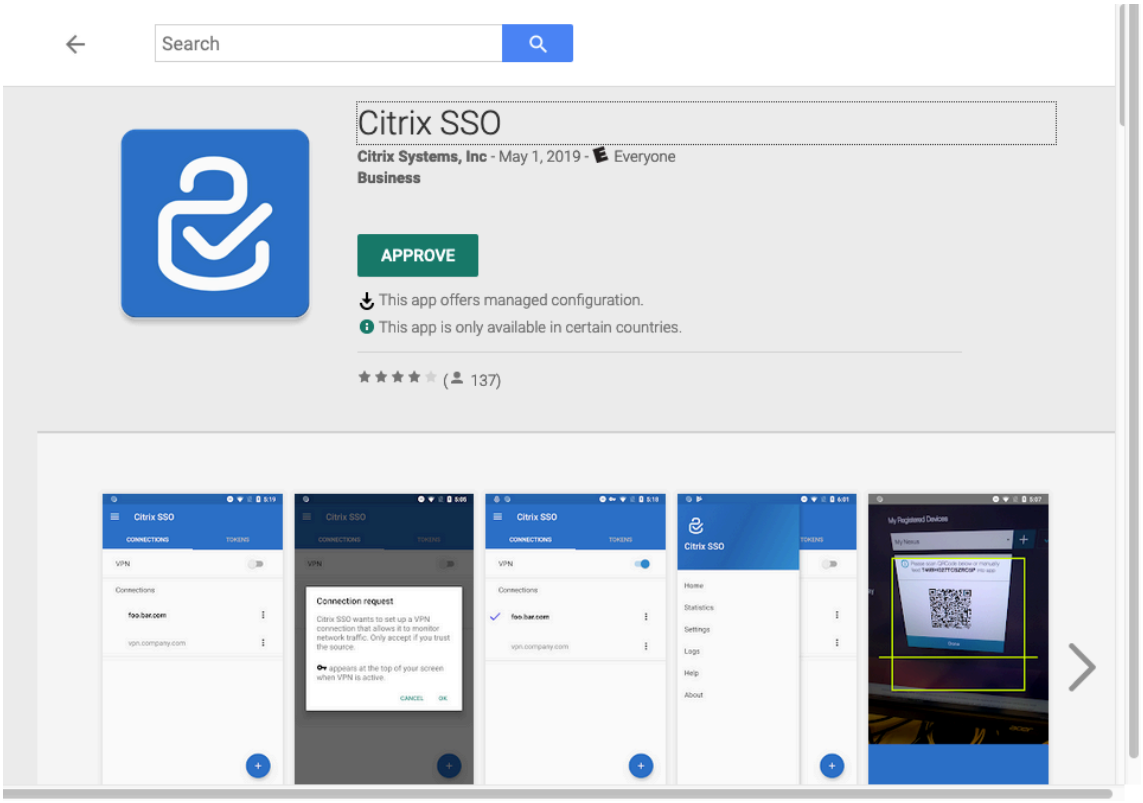
在 **Intune Android Enterprise** 环境中设置 **Citrix Secure Access**

- 将 Citrix Secure Access 添加为托管应用程序
- 为 Citrix Secure Access 配置托管应用程序策略

将 **Citrix Secure Access** 添加为托管应用程序

1. 登录到您的 Azure 门户。
2. 单击左侧导航刀片上的 **Intune** 。
3. 在 Microsoft Intune Blade 中单击 客户端应用程 序，然后单击客户端应用程序 Blade 中的应用程序。
4. 单击右上角菜单选项中的 **+** 添加链接。将显示添加应用程序配置 Blade。
5. 为应用类型选择 托管 **Google Play** 。

   如果您已配置 Android Enterprise，这将添加“管理 Google Play”搜索和批准 Blade。
6. 搜索 Citrix Secure Access，然后从应用程序列表中将其选中。



注意：如果 Citrix Secure Access 未出现在列表中，则表示该应用程序在您所在的国家/地区不可用。

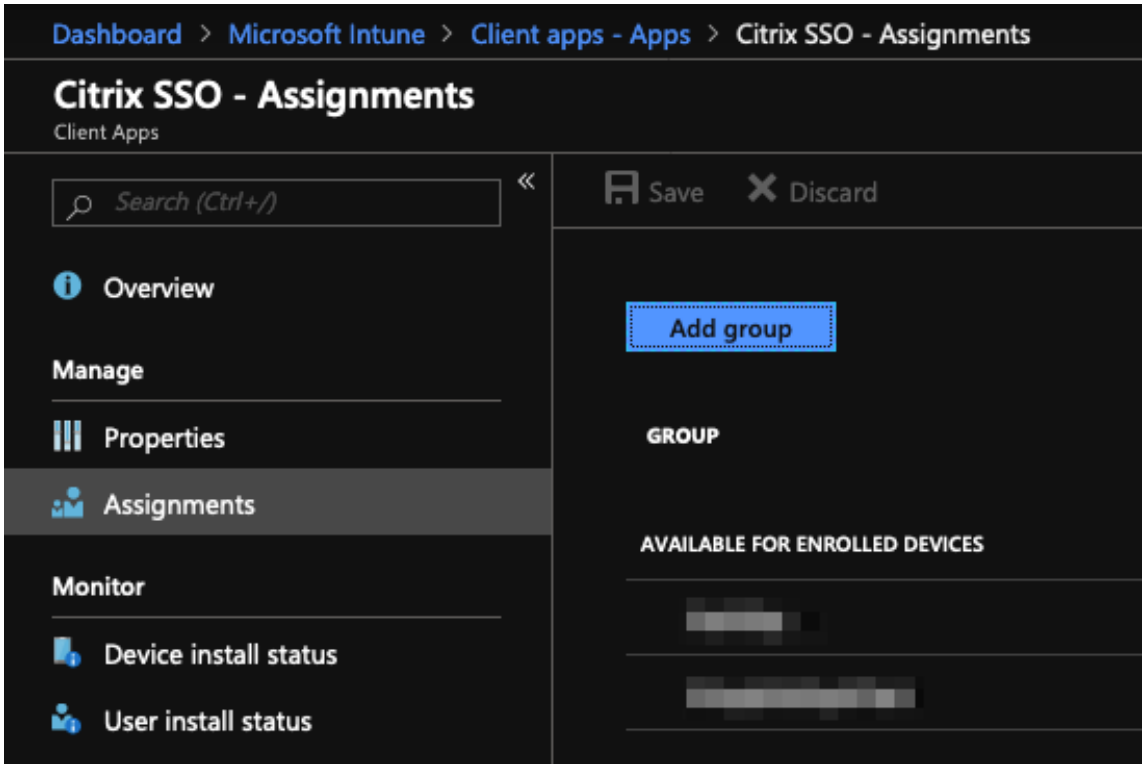
7. 单击“批准”以批准通过 Google Play 托管应用商店部署 Citrix Secure Access。

   列出了 Citrix Secure Access 所需的权限。

8. 单击 批准 以批准应用程序进行部署。
9. 单击“同步”以将此选择内容与 Intune 同步。

   Citrix Secure Access 已添加到客户端应用程序列表中。如果添加了许多应用程序，则可能需要搜索 Citrix Secure Access。

10. 单击 **Citrix Secure Access** 应用程序打开应用程序详细信息窗口。
11. 单击详细信息刀片中的“分配”。此时将显示 **Citrix Secure Access -** 分配刀片。



12. 单击“添加组”，分配要授予安装 Citrix Secure Access 权限的用户组，然后单击“保存”。
13. 关闭 Citrix Secure Access 详细信息刀片。

Citrix Secure Access 已添加并启用，可以部署到您的用户。

为 **Citrix Secure Access** 配置托管应用程序策略

添加 Citrix Secure Access 后，您必须为 Citrix Secure Access 创建托管配置策略，以便可以将 VPN 配置文件部署到设备上的 Citrix Secure Access。

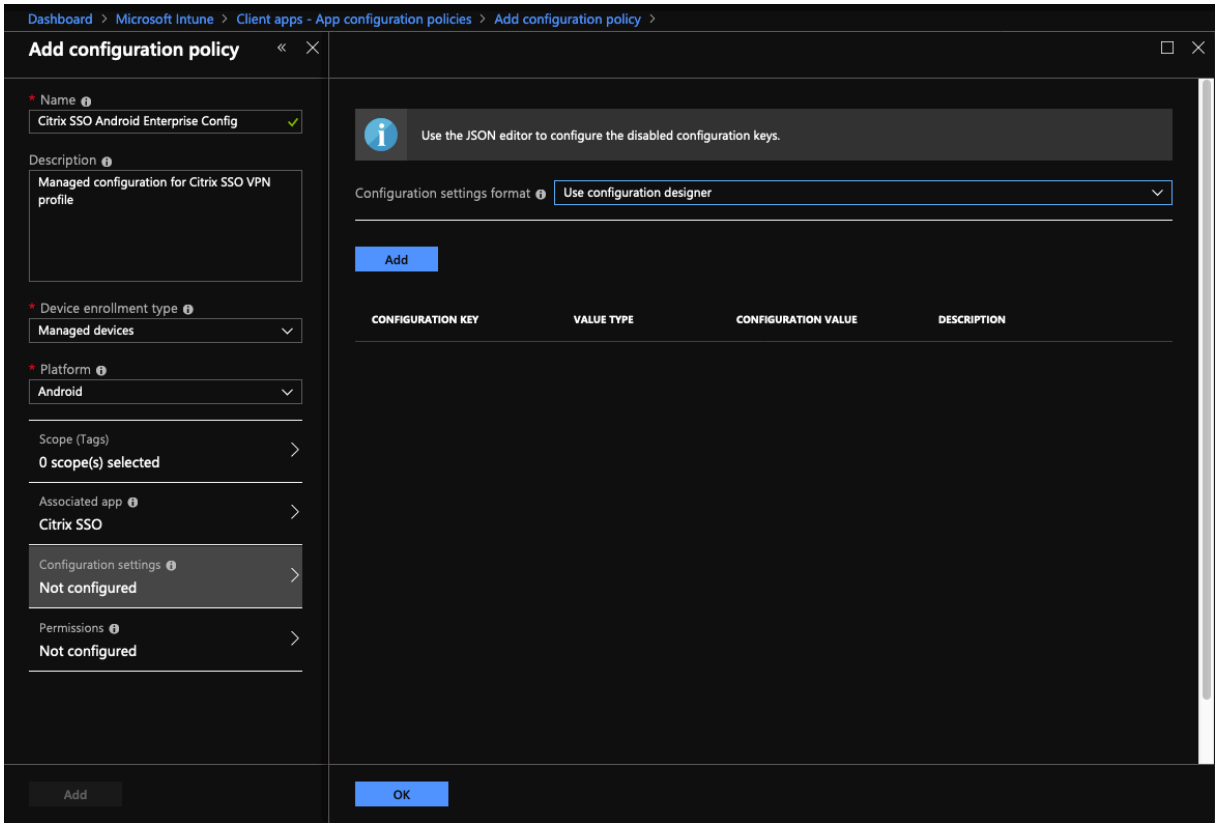
1. 在 Azure 门户中打开 **Intune** 刀片。
2. 从 Intune 刀片打开 客户端应用 刀片式服务器。
3. 从客户端应用 程序 **Blade** 中选择应用程序配置策 略项，然后单击 添加 以打开 添加配置策略 Blade。
4. 输入策略的名称并为其添加说明。
5. 在设 备注册类型中，选择 托管设备。
6. 在 平台中，选择 **Android**。

   这将为关联的应用程序添加另一个配置选项。
7. 单击关联应用程序，然后选择 **Citrix Secure Access** 应用程序。

   如果您有很多应用程序，您可能必须搜索它。

8. 单击确定。添加配置策略 Blade 中添加了配置设置选项。
9. 单击 配置 设置。

   此时将显示用于配置 Citrix Secure Access 的刀片。
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。



> 注意：
>
> 对于简单的 VPN 配置，建议使用配置设计器。

使用配置设计器配置 **VPN**

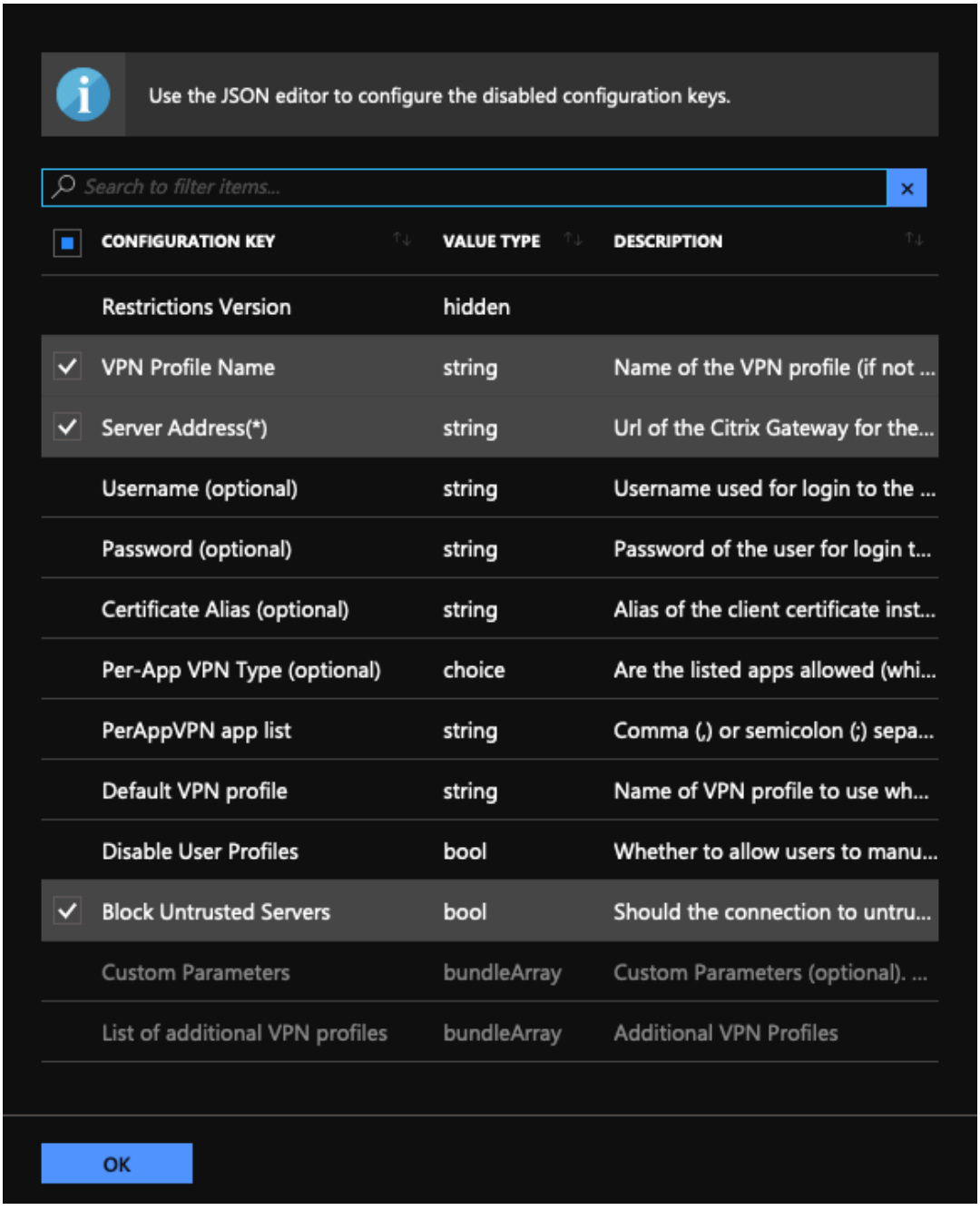
1. 在 配置设置中，选择 使用配置设计器，然后单击 添加。

   您将看到一个键值输入屏幕，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。如果不提供名称，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 NetScaler Gateway 端口不是 443，请键入您的端口。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 Intune 配置值令牌，则可以 为此字段使用 Intune 配置值令牌（请参阅配置值令牌）。如果不提供用户名，则系统会在用户连接到 NetScaler Gateway 时提示他们提供用户名。
- 密码（可选）。输入最终用户用于向 NetScaler Gateway 进行身份验证的密码。如果不提供密码，则系统会在用户连接到 NetScaler Gateway 时提示他们提供密码。
- 证书别名（可选）。在 Android KeyStore 中提供用于客户端证书身份验证的证书别名。如果您使用的是基于证书的身份验证，则会为用户预先选择此证书。
- 网关证书 **Pin**(可选)。JSON 对象，描述用于 NetScaler Gateway 的证书引脚。示例值：`{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`。有关详细信息，请参阅使用 Android Citrix Secure Access 固定 NetScaler Gateway 证书。
- 每个应用程序的 **VPN** 类型（可选）。如果您使用每应用程序 VPN 来限制哪些应用程序使用此 VPN，则可以配置此设置。
  - 如果选择 允许，PerAppVPN 应用程序列表中列出的应用程序包名称的网络流量将通过 VPN 路由。所有其他应用程序的网络流量都会在 VPN 外部进行路由。
  - 如果选择 不允许，PerAppVPN 应用程序列表中列出的应用程序包名称的网络流量将路由到 VPN 之外。所有其他应用程序的网络流量都通过 VPN 路由。默认设置为允许。
- **PerAppVPN** 应用程序列表。VPN 上允许或禁止其流量的应用程序列表，具体取决于 PerApp VPN 类型的值。列出以逗号或分号分隔的应用程序包的名称。应用程序包名称区分大小写，并且必须以与 Google Play 应用商店中完全一致的显示方式显示在此列表中。此列表是可选的。将此列表保留为空，以便预配设备范围的 VPN。
- 默认 **VPN** 配置文件。为 Citrix Secure Access 配置了始终可用的 VPN 时使用的 VPN 配置文件名称。如果此字段为空，则使用主配置文件进行连接。如果只配置了一个配置文件，则会将其标记为默认 VPN 配置文件。



> 注意：
>
> - 要在 Intune 中将 Citrix Secure Access 设置为始终可用的 VPN 应用程序，请使用 VPN 提供程序作为自定义名称，使用 `com.citrix.CitrixVPN` 作为应用程序包名称。
> - Citrix Secure Access 的始终可用的 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证书设置为必填项，Citrix Secure Access 才能按预期运行。

- 禁用用户配置文件

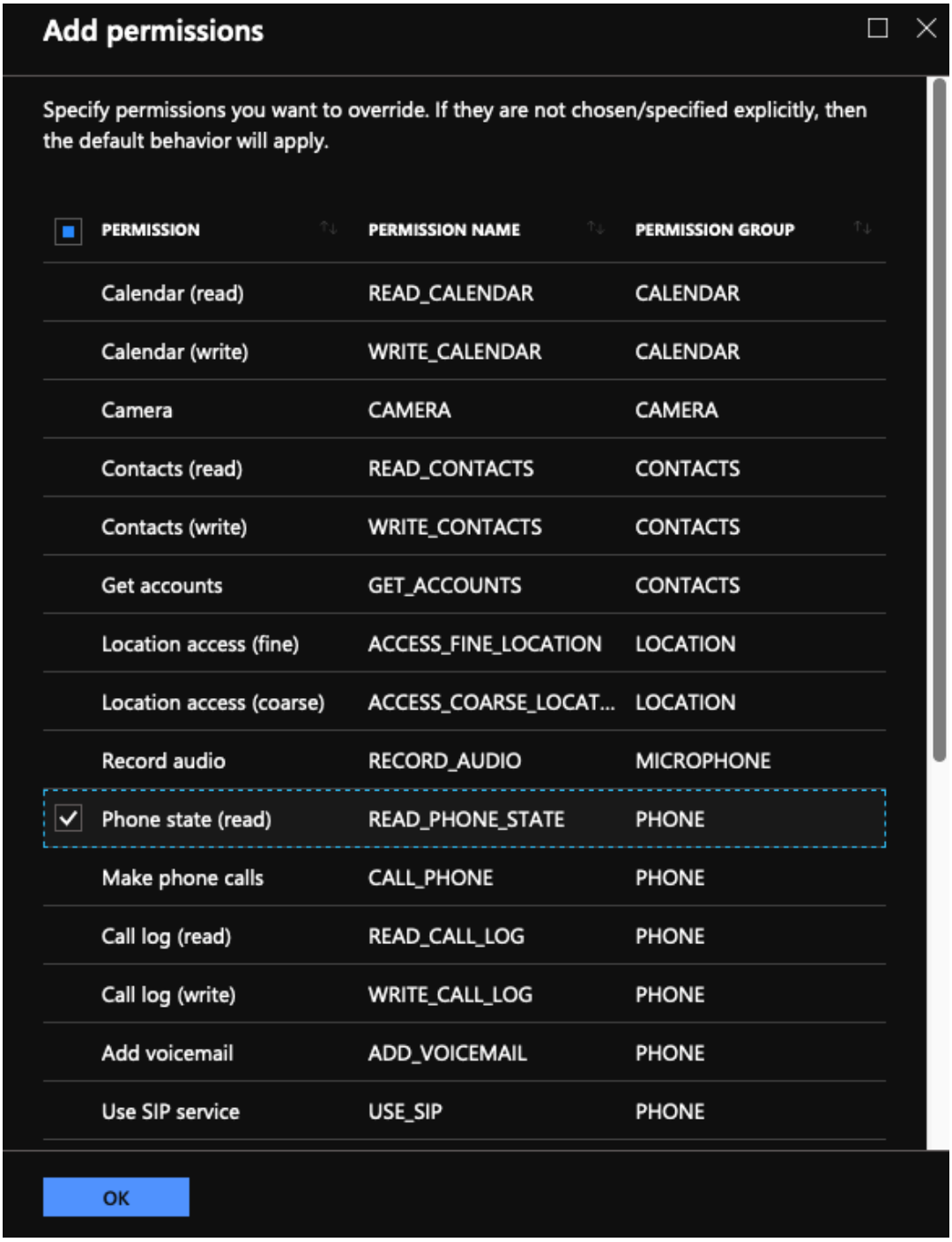
- 如果将此值设置为 true，用户将无法在其设备上添加新的 VPN 配置文件。
- 如果将此值设置为 false，则用户可以在其设备上添加自己的 VPN。

默认值为 false。

- 阻止不可信的服务器
  - 在为 NetScaler Gateway 使用自签名证书或颁发 NetScaler Gateway 证书的 CA 的根证书不在系统 CA 列表中时，将此值设置为 false。
  - 将此值设置为 true 可启用 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. 在“服务器地址 **(*)**”属性中，输入您的 VPN 网关基本 URL（例如，`https://vpn.mycompany.com`）。
4. 在 **VPN** 配置文件名称中，输入最终用户可以在 Citrix Secure Access 客户端主屏幕中看到的名称（例如，我的公司 VPN）。
5. 您可以根据需要为 NetScaler Gateway 部署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：
   - 如果您使用的是 Intune NAC 检查，Citrix Secure Access 要求您授予电话状态（读取）权限。单击 添加 按钮打开权限刀片。目前，Intune 显示了可供所有应用程序使用的重要权限列表。
   - 如果您使用的是 Intune NAC 检查，请选择 电话状态（读取）权限，然后单击 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 检查可以正常工作，然后单击“确定”。



- 建议您自动向 Citrix Secure Access 授予通知权限。

> 注意：
>
> 对于使用 Citrix Secure Access 23.12.1 及更高版本的 Android 13 以上的用户，建议 MDM 管理员在其解决方案中向 Citrix Secure Access（软件包 ID：`com.citrix.CitrixVPN`）授予通知权限。

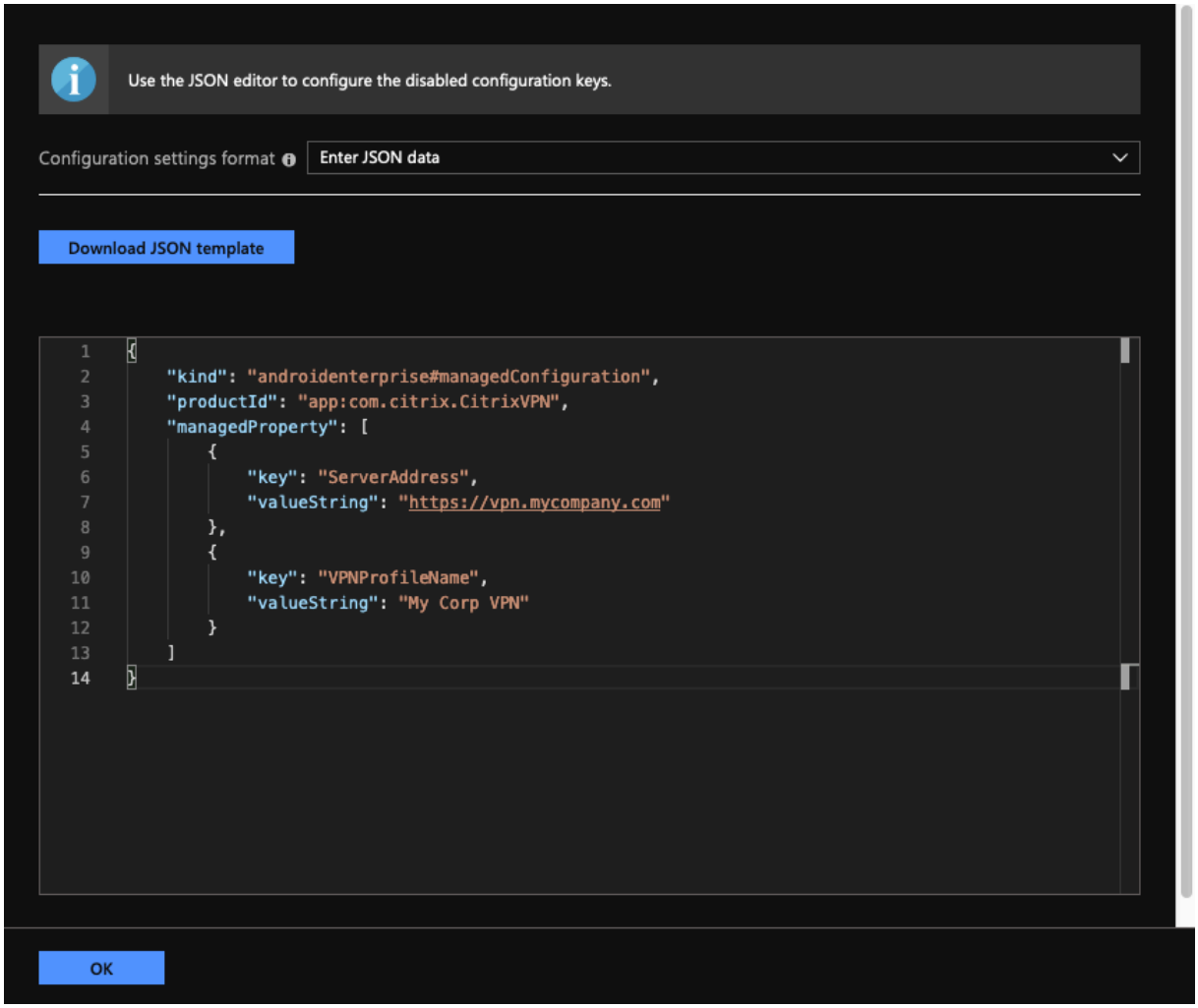
7. 单击“应用程序配置策略”边栏底部的“添加”，保存 Citrix Secure Access 的托管配置。

8. 单击应用程序配置策略 **Blade** 中的分配以打开任务 **Blade**。
9. 选择要为其交付和应用此 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** 数据用于配置 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/更复杂的配置。此模板是一组 JSON 键值对，用于配置 Citrix Secure Access 可以理解的所有可能属性。

   有关可以配置的所有可用属性的列表，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中。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。



这样就完成了在 Microsoft Intune Android Enterprise 环境中为 Citrix Secure Access 配置和部署 VPN 配置文件的过程。

> 重要：
>
> 用于基于客户端证书的身份验证的证书是使用 Intune SCEP 配置文件部署的。必须在 Citrix Secure Access 托管配置的证书别名属性中配置此证书的别名。

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	说明
VPN 配置文件名称	VPNProfileName	文本	VPN 配置文件的名称（如果未设置默认为服务器地址）。
服务器地址 (*)	ServerAddress	URL	用于连接的 NetScaler Gateway 的基本 URL (`https://host[:port]`)。此字段为必填字段。
`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	使用 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 凭据存储中的客户端证书的别名，用于基于证书的客户端身份验证（可选）。在 NetScaler Gateway 上使用基于证书的身份验证时，证书别名是必填字段。

配置键	JSON 字段名称	值类型	说明
网关证书固定（可选）	ServerCertificatePins	JSON 文本	描述用于 NetScaler Gateway 的证书引脚的嵌入式 JSON 对象。示例值：`{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`。使用 JSON 配置器时，请务必避开这些嵌入式 JSON 数据。
PerApp VPN 类型（可选）	PerAppVPN_Allow_Disallow_Setting	Enum (Allow, Disallow)	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 通道。如果设置为允许，则只允许列出的应用程序（在 PerAppVPN 应用程序列表属性中）通过 VPN 建立通道。如果设置为“不允许”，则允许除列出的应用程序以外的所有应用程序通过 VPN 建立通道。如果未列出任何应用程序，则允许所有应用程序通过 VPN 进行通道传输。
PerAppVPN 应用程序列表	PerAppName_Appnames	文本	以逗号 (,) 或分号 (;) 分隔的 PerApp VPN 的应用程序包名称列表。软件包名称必须与 Google Play 应用商店应用列表页面 URL 中显示的相同。包名区分大小写。
默认 VPN 配置文件	DefaultProfileName	文本	系统启动 VPN 服务时使用的 VPN 配置文件的名称。此设置用于识别在设备上配置始终可用的 VPN 时要使用的 VPN 配置文件。

配置键	JSON 字段名称	值类型	说明
禁用用户配置文件	DisableUserProfiles	布尔值	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** 可禁止用户创建 VPN 配置文件。默认值为 **false**。
阻止不可信的服务器	BlockUntrustedServers	布尔值	用于确定是否阻止与不可信网关的连接（例如，使用自签名证书或在颁发 CA 时不受 Android 操作系统信任）？默认值为 true（阻止与不可信网关的连接）。
自定义参数（可选）	CustomParameters	列表	Citrix Secure Access 支持的自定义参数列表（可选）。有关详细信息，请参阅自定义参数。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 配置文件列表。支持前面提到的每个配置文件的大多数值。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　必须使用以下键值名称定义每个自定义参数。

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	说明	值
UserAgent	与 NetScaler Gateway 通信时，Citrix Secure Access 会将此参数值附加到用户代理 HTTP 标头，以便对 NetScaler Gateway 进行额外检查。	指定需要附加到用户代理 HTTP 标头的文本。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，以帮助在始终可用的 VPN 的情况下解决 VPN 连接问题。您可以在任何一种托管 VPN 配置中将其启用。调试日志记录在处理托管配置后生效。	**True**：启用调试日志记录。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。

配置键	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
网关证书固定	bundle_ServerCertificatePins	文本
PerApp VPN 类型	bundle_PerAppVPN_Allow_Disallow_Setting	Enum (Allow, Disallow)
PerAppVPN 应用程序列表	bundle_PerAppVPN_Appnames	文本
自定义参数	bundle_CustomParameters	列表

在 **Intune** 中将 **Citrix Secure Access** 设置为始终可用的 **VPN** 提供程序

在 Android VPN 子系统不支持按需 VPN 的情况下，可以使用始终可用的 VPN 作为替代方案，提供无缝 VPN 连接选项以及通过 Citrix Secure Access 进行客户证书身份验证。VPN 在启动或工作配置文件开启时由操作系统启动。

要在 Intune 中将 Citrix Secure Access 设置为始终可用的 VPN 应用程序，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）。

- 创建设备配置文件并选择 设备限制，然后转到 连接 部分。为“始终可用的 VPN”设置选择启用。
- 选择 **Citrix Secure Access** 作为 VPN 客户端。如果 Citrix Secure Access 选项不可用，则可以选择“自定义”作为 VPN 客户端，然后在“软件包 ID”字段中输入 **com.citrix.CitrixVPN**（“软件包 ID”字段区分大小写）
- 保留其他选项原样。建议不要启用锁定模式。启用后，如果 VPN 不可用，设备可能会失去完整的网络连接。
- 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 **PerAppVPN** 类型和 **PerAppVPN** 应用程序列表，以启用适用于 Android 的 PerAppVPN，如前面部分所述。

> 注意：
>
> 只有 Citrix Secure Access 中的客户证书身份验证才支持始终可用的 VPN。

引用

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。

- 完全托管的企业专用设备
- 个人拥有的设备

自动重启始终可用的 **VPN**

从 Citrix SSO for Android 23.8.1 开始，当允许列表或阻止列表中的应用安装在工作配置文件或设备配置文件中时，Citrix Secure Access 会自动重启始终可用的 VPN。来自新安装应用程序的流量将自动通过 VPN 连接进行通道传输，无需重启工作配置文件或重启设备。

要启用始终可用的 VPN 的自动重启，最终用户必须向 Citrix Secure Access 授予查询所有包的同意。获得同意后，Citrix Secure Access：

- 接收来自操作系统的软件包安装通知。
- 重新启动始终可用的 VPN。

当最终用户首次连接到每个应用程序的 VPN 配置文件时，系统会提示用户提供同意（Google 策略要求）以收集已安装软件包的信息。如果最终用户表示同意，则会启动 VPN 连接。如果用户拒绝同意，VPN 连接将中止。同意后，同意屏幕不会重新出现。有关最终用户说明的详细信息，请参阅如何在 Android 设备上使用 Citrix Secure Access。

限制

下面是 Android 11+ 设备上的 Android Enterprise 环境中每个应用程序 VPN 的限制，这是由于 Android 11 中引入的包可见性限制所致：

- 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上，则最终用户必须重新启动 VPN 会话，该应用程序才能通过 VPN 会话路由其流量。
- 如果通过始终可用的 VPN 会话使用每应用程序 VPN，则在设备上安装新应用程序后，最终用户必须重新启动工作配置文件或重新启动设备才能通过 VPN 会话路由应用程序的流量。

> 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，请参阅自动重启始终可用的 VPN。

使用适用于 **Android** 的 **Citrix Secure Access** 固定的 **NetScaler Gateway** 证书

February 1, 2024

> 重要提示：
>
> Citrix SSO for Android 现在称为 Citrix Secure Access。我们正在更新文档和用户界面屏幕截图，以反映此名称的更改。

证书固定有助于防止中间人攻击。Citrix Secure Access 仅在 Android Enterprise 模式和传统设备管理员模式下支持对托管 VPN 配置进行证书锁定。最终用户添加的 VPN 配置文件不支持此功能。

使用 **Android Citrix Secure Access** 配置 **NetScaler Gateway** 证书固定

有关在 Citrix Secure Access 的托管配置（以前称为应用程序限制）中锁定证书的详细信息，请参阅证书和身份验证。

定义了一个新的键值对来承载固定的 NetScaler Gateway 证书哈希值，如下所示。

```
Key: ServerCertificatePins
Value: {

  "hash-alg": "sha256",
  "pinset": [
    "cert1_base64_encoded_SHA-256_hash_of_the_X509_SubjectPublicKeyInfo
       (SPKI)",
    "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
    "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="
    ...
  ]
 }

<!--NeedCopy-->
```


在托管配置中指定证书固定详细信息的密钥是 **ServerCertificatePins**。该值是一个 JSON 有效负载，其中包含固定的 NetScaler Gateway 证书的 base64 编码的 SHA-256 哈希值以及使用的哈希算法。固定的证书可以是操作系统验证的信任链中的任何证书。在这种情况下，它是 Android 系统。

只有在操作系统在 TLS 握手期间验证了证书链之后，才会进行证书固定。证书的 PIN 码是通过对证书的主题公钥信息 (SPKI) 进行哈希处理来计算的。必须在 JSON 负载中指定两个字段（“**hash-alg”和“pinset”**）。

“**hash-alg**”指定用于计算 SPKI 哈希的哈希算法。
“针脚集”指定包含 NetScaler Gateway 证书的 SPKI 数据的 base64 编码的 SHA-256 哈希值的 JSON 数组。
必须为证书 PIN 指定至少一个值。可以指定更多的引脚值以允许证书轮换或到期。

您可以使用以下 openssl 命令来计算域（例如 gw.yourdomain.com）的引脚值。

```
1 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
2 <!--NeedCopy-->
```

该命令显示网关提供的叶证书的 base64 编码的 SHA-256 哈希值。链中的任何证书都可以用于固定证书。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。如果所有引脚都不与经过验证的证书链中的证书匹配，则 TLS 握手将中止，并且不会继续连接到网关。

> 注意：
>
> 在设备管理员模式下，仅 Citrix Endpoint Management 和 Microsoft 端点管理解决方案支持证书固定。必须在旧版 VPN 配置文件（非托管配置）中使用的自定义参数中配置证书固定，并使用自定义参数 ServerCertificatePins 具有相同的 JSON 有效负载进行固定。

适用于 **Windows** 的 **Citrix Secure Access** 发行说明

February 1, 2024

适用于 Windows 的 Citrix Secure Access 客户端现已独立发布，与所有 NetScaler 版本兼容。Citrix Secure Access 客户端版本采用 YY.MM Release.Build 格式。

发行说明描述了新增功能、现有功能的增强功能以及已修复的问题。

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：当前版本中修复的问题。

有关受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 23.7.1.1 及更高版本包含的修复程序。https:

> //support.citrix.com/article/CTX564833
>
> - Citrix Secure Access 客户端（以前称为 Windows 版 NetScaler Gateway 插件）构建 21.9.1.2 及更高版本包含的修复程序 https://support.citrix.com/article/CTX341455。

23.10.1.7（2023 年 11 月 29 日）

新增功能

- 为服务器启动的连接配置专用端口范围

  现在，您可以为服务器启动的连接配置从 49152 到 64535 的专用端口。配置专用端口可以避免在使用端口在 Citrix Secure Access 客户端与客户端上的第三方应用程序之间创建套接字时可能出现的冲突。您可以使用 SicBeginPort Windows VPN 注册表配置专用端口。或者，您可以使用 NetScaler 上的 VPN 插件自定义 JSON 文件配置专用端口范围。

  有关更多信息，请参阅配置服务器启动的连接和 NetScaler Gateway Windows VPN 客户端注册表项。

  [NSHELP-36627]

- **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。作为这项支持的一部分，引入了 VPN 客户端注册表项 “EnableKerberosAuth”。作为必备条件，管理员必须在 NetScaler 及其客户端上配置 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。有关更多信息，请参阅使用 Kerberos 身份验证自动登录。

  [CSACLIENTS-3128]

- 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。

  [CSACLIENTS-6132]

- **Microsoft** 通知

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

  [CSACLIENTS-6136]

- 改进了日志收集

  Verbose 日志级别现在用作默认的调试日志记录级别，用于增强日志收集和故障排除。有关日志记录的更多信息，请参阅使用客户端用户界面配置日志记录。

  [CSACLIENTS-8151]

已修复的问题

如果 AlwaysOn 服务的计算机通道无法检测到客户端设备的位置，则 Citrix Secure Access 客户端仍处于“连接”状态。

[CSACLIENTS-1174]

在 Citrix Secure Access 客户端中启用 Microsoft Edge WebView 时，转移登录功能将失效。

[CSACLIENTS-6655]

在 AlwaysOn 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，则 Citrix Secure Access 客户端无法与 NetScaler Gateway 建立计算机级通道。

[NSHELP-33766]

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

[NSHELP-34651]

如果满足以下条件，Citrix Secure Access 客户端就会崩溃：

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

[NSHELP-35366]

Citrix Secure Access 客户端用户界面在自动登录期间显示“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。

[NSHELP-36134]

如果配置了计算机级通道，则本地 LAN 访问功能无法与 Citrix Secure Access 客户端一起使用。

在此版本中，可以使用计算机级通道配置来设置本地局域网访问功能。为此，在使用计算机通道模式时，必须将本地局域网访问参数配置为 FORCED。有关更多详细信息，请参阅根据 ADC 配置强制最终用户访问本地局域网。

[NSHELP-36214]

当客户端多次从睡眠模式中醒来时，Citrix Secure Access 客户端无法与 Intranet 应用程序建立 VPN 连接。

[NSHELP-36221]

23.8.1.11（**2023** 年 **10** 月 **19** 日）

已修复的问题

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

[CSACLIENTS-6917]

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

[NSHELP-36590]

23.8.1.5 (2023 年 8 月 9 日)

已修复的问题

通过 Citrix Secure Private Access Private Access 服务连接时，应用程序的 Kerberos SSO 会失败。

[CSACLIENTS-912]

使用 Citrix Secure Private Access Private Access 服务的应用程序访问会间歇性失败。当 Citrix Secure Access 客户端共享错误的 TCP 或 UDP 流量的目标 IP 地址时，就会出现此问题。

[CSACLIENTS-1151，CSACLIENTS-6326]

由于 DNS 缓存问题，Citrix Secure Access 客户端无法间歇性地启动应用程序。

[CSACLIENTS-1170]

Citrix Secure Access 客户端无法将 DNS 后缀应用于 Citrix 虚拟适配器。当 Citrix 虚拟适配器无法通过 Active Directory 进行身份验证时，就会出现此问题。

[NSHELP-33817]

如果满足以下条件，Citrix Secure Access 客户端就会崩溃：

- 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。

[CSACLIENTS-6171]

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

[NSHELP-35909]

当门户自定义超过允许的限制时，Citrix Secure Access 客户端间歇性地无法从 NetScaler Gateway 下载配置。

[NSHELP-35971]

已知问题

转移登录功能无法与 Citrix Secure Access 客户端配合使用。启用 Microsoft Edge WebView 时会出现此问题。

解决办法：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，升级到发行版 23.x.x.x 后，流量无法通过 VPN 通道，从而导致 NetScaler 上配置内联网 IP 范围时 VPN 访问被阻止。当跨配置文件防火墙规则未应用于 VPN 应用程序时，就会发生这种情况。

[NSHELP-35766]

23.5.1.3 (2023 年 6 月 2 日)

已修复的问题

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

[CGOP-24462]

23.4.1.5 (14-Apr-2023)

新增功能

- **Microsoft Edge WebView** 支持

  适用于 Windows 的 Citrix Secure Access 客户端上的 Microsoft Edge WebView 支持引入了增强的最终用户体验。默认情况下，此功能处于禁用状态。有关详细信息，请参阅 Microsoft Edge WebView 对 Windows Citrix Secure Access 的支持。

  [CGOP-22245]

- 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 客户端在域名解析期间解析不完全合格的域名。

  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，请参阅用于将 FQDN 解析为 IP 地址的 DNS 后缀。

  [ACS-2490]

- 改进了日志收集

  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。对日志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。

- 使用户能够将日志文件数更新到小于 5。
- 将新日志功能的日志级别增加到三级。

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，日志的收集仅限于当前会话。有关详细信息，请参阅 改进了 Windows 客户端的日志收集。

> 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”。在适用于 Windows 23.4.1.5 的 Citrix Secure Access 客户端发布之前，可以使用“配置”>“启用调试日志记录”复选框启用调试日志记录。

[CGOP-23537]

- 支持向 **Citrix Analytics** 服务发送事件

  适用于 Windows 的 Citrix Secure Access 客户端现在支持向 Citrix Analytics 服务发送会话创建、会话终止和应用程序连接等事件。然后，这些事件将记录在 Citrix Secure Private Access 控制面板中。

  [SPA-2197]

已修复的问题

- 对于 Unicode 用户，使用 Citrix Workspace 应用程序进行云端点的 Citrix Secure Access 客户端单点登录身份验证失败。

  [CGOP-22334]

- 在 Citrix Secure Private Access 中配置基于主机名的应用程序以及 DNS 后缀时，对资源的访问将失败。

  [SPA-4430]

- 由于网关虚拟服务器的可访问性问题，Always-On VPN 连接在启动时间歇性失败。

  [NSHELP-33500]

- 在 Citrix Secure Access 客户端上将拆分通道设置为“关”时，无法访问与欺诈 IP 地址范围重叠的 Intranet 资源。

  [NSHELP-34334]

- Citrix Secure Access 客户端无法加载身份验证架构，导致 Citrix Secure Private Access 服务登录失败。

  [SPAHELP-98]

23.1.1.11 (20-Feb-2023)

此版本解决了有助于提高 Citrix Secure Private Access 服务的整体性能和稳定性的问题。

23.1.1.8 (08-Feb-2023)

已修复的问题

- DNS 解析失败是因为 Citrix Secure Access 未能将 IPv4 数据包优先于 IPv6 数据包。

  [NSHELP-33617]

- 操作系统筛选规则是在 Citrix Secure Access 客户端在 Windows 筛选平台 (WFP) 模式下运行时捕获的。

  [NSHELP-33715]

- 当 Citrix Secure Access 客户端在 Citrix Deterministic Network Enhancer (DNE) 模式下运行时，欺诈 IP 地址用于基于 IP 的内联网应用程序。

  [NSHELP-33722]

- 使用 Windows 筛选平台 (WFP) 驱动程序时，有时在重新连接 VPN 后无法访问内联网。

  [NSHELP-32978]

- 在 Windows 10 和 Windows 11 Enterprise 多会话桌面上，端点分析 (EPA) 扫描操作系统版本检查失败。

  [NSHELP-33534]

- 默认情况下，Windows 客户端支持 64 KB 配置文件大小，这限制了用户在配置文件中添加更多条目。此大小可以通过在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client 中设置 `ConfigSize` 注册表值来增加。`ConfigSize` 注册表项类型为 `REG_DWORD`，注册表项数据为 <`Bytes size`>。如果配置文件大小大于默认值 (64 KB)，则每增加 64 KB，就必须将 ConfigSize 注册表值设置为 5 x 64 KB（转换为字节后）。例如，如果您要额外增加 64 KB，则必须将注册表值设置为 64 x 1024 x 5 = 327680。同样，如果您要增加 128 KB，则必须将注册表值设置为 64 x 1024 x (5+5) = 655360。

  [SPA-2865]

- VPN 注销时，SearchList 注册表中的 DNS 后缀列表条目将以相反的顺序重写，由一个或多个逗号分隔。

  [NSHELP-33671]

- 当 NetScaler 设备完成 EPA 防病毒扫描时，代理身份验证失败。

  [NSHELP-30876]

- 如果与 Citrix Secure Access 相关的注册表值大于 1500 个字符，日志收集器将无法收集错误日志。

  [NSHELP-33457]

22.10.1.9 (08-Nov-2022)

新增功能

- **EPA** 支持 **GSLB** 中的连接代理类型站点持久性

Windows EPA 扫描现在支持从浏览器启动扫描时在 GSLB 中保留连接代理类型的站点。以前，适用于 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。

[CGOP-21545]

- **Workspace URL** 的无缝单点登录（仅限云端）

  如果用户已经通过 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（仅限云端）。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。

  [ACS-2427]

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

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

  [ACS-2426]

- 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，可以从插件 UI 中为计算机和用户通道启用或禁用它。

  [NSHELP-31968]

- 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。

  [CGOP-20544]

已修复的问题

- 对于没有管理权限的用户，Citrix Secure Access 客户端（版本 21.7.1.1 及更高版本）无法升级到更高版本。

  这仅在通过 NetScaler 设备完成 Citrix Secure Access 客户端升级时适用。有关详细信息，请参阅 Citrix Secure Access 客户端上的升级/降级问题。

  [NSHELP-32793]

- 由于 EPA 间歇性故障，用户无法登录 VPN。

  [NSHELP-32138]

- 有时，处于仅限计算机通道模式的 Citrix Secure Access 客户端在计算机从睡眠模式中唤醒后不会自动建立计算机通道。

  [NSHELP-30110]

- 在 Always on 服务模式下，即使只配置了计算机通道，用户通道也会尝试启动。

  [NSHELP-31467]

- 如果 Microsoft Edge 是默认浏览器，则 Citrix Secure Access 用户界面上的主页链接将不起作用。

  [NSHELP-31894]

- NetScaler Gateway 门户上不显示自定义 EPA 故障日志消息，而是显示“内部错误”消息。

  [NSHELP-31434]

- 当用户单击适用于 Windows 的 Citrix Secure Access 屏幕上的“主页”选项卡时，该页面会显示连接被拒绝的错误。

  [NSHELP-32510]

- 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。

  [SPAHELP-73]

已知问题

- Windows Update 基于支票的 EPA 扫描不适用于 Windows 11 22H2 版本。有关详细信息，请参阅 Windows11 22H2 的 EPA 检查失败。

  [NSHELP-33068]

22.6.1.5 (17-June-2022)

新增功能

- 登录和注销脚本配置

  当 Citrix Secure Access 客户端连接到 Citrix Secure Access 云服务时，Citrix Secure Private Access 客户端将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 类型 REG_SZ - 登录脚本的路径
  - SecureAccessLogOutScript 类型 REG_SZ - 注销脚本的路径

  [ACS-2776]

- 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，为创建网络过滤应用程序提供了一个平台。WFP 旨在取代以前的包过滤技术，即与 DNE 驱动程序一起使用的网络驱动程序接口规范 (NDIS) 过滤器。有关详细信息，请参阅使用 Windows 筛选平台的 Windows Citrix Secure Access 客户端。

[CGOP-19787]

- 基于 **FQDN** 的反向拆分通道支持

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

  [CGOP-16849]

已修复的问题

- 有时，当用户以“始终开启”服务模式登录到 Windows 计算机时，Windows 自动登录不起作用。计算机通道不会转换为用户通道，VPN 插件 UI 中会显示消息“正在连接”。

  [NSHELP-31357]

- VPN 注销时，SearchList (Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client) 注册表中的 DNS 后缀列表条目将以相反的顺序重写，并用一个或多个逗号分隔。

  [NSHELP-31346]

- 即使在 NetScaler 内联网应用程序配置从基于 FQDN 的应用程序更改为基于 IP 的应用程序之后，也会使用欺骗 IP 地址。

  [NSHELP-31236]

- 网关插件成功建立 VPN 通道后，不会立即显示网关主页。

  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，不设置或添加此注册表值。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才能启用此修复（即在网关插件成功建立 VPN 通道后立即显示主页）。

  [NSHELP-30189]

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

  [NSHELP-31836]

- 如果无法访问已经连接的 Citrix Secure Private Access 服务区域，则适用于 Windows 的 Citrix Secure Private Access 客户端不会通过通道将新的 TCP 连接通过通道连接到后端 TCP 服务器。但是，这不会影响本地网关连接。

  [ACS-2714]

22.3.1.5 (24-Mar-2022)

已修复的问题

- Windows EPA 插件名称将恢复为 NetScaler Gateway EPA 插件。

  [CGOP-21061]

已知问题

- 如果无法访问已经连接的 Citrix Secure Private Access 服务区域，则适用于 Windows 的 Citrix Secure Private Access 客户端不会通过通道将新的 TCP 连接通过通道连接到后端 TCP 服务器。但是，这不会影响本地网关连接。

  [ACS-2714]

22.3.1.4 (10-Mar-2022)

新增功能

- 根据 **ADC** 配置对最终用户实施本地 **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局域网访问选项。一个新选项“强制”将添加到现有的“本地局域网访问”参数值中。当本地局域网访问值设置为 FORCED 时，客户端计算机上始终为最终用户启用本地局域网访问。最终用户无法使用 Citrix Secure Access 客户端用户界面禁用本地局域网设置。如果管理员想要为最终用户提供启用或禁用本地局域网访问的选项，则他们必须将本地局域网访问参数重新配置为“开”。

  要使用 GUI 启用 **FORCED** 选项，请执行以下操作：

  1. 导航到 **NetScaler Gateway >** 全局设置 **>** 更改全局设置。
  2. 单击“客户端体验”选项卡，然后单击“高级设置”。
  3. 在 本地局域网访问中，选择 强制。

  要使用 CLI 启用 **FORCED** 选项，请运行以下命令：

  ```
  set vpn parameter -localLanAccess FORCED
  <!--NeedCopy-->
  ```

  [CGOP-19935]

- 在 **EPA** 操作系统扫描中支持 **Windows** 服务器 **2019** 和 **2022**

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

  您可以使用 GUI 选择新服务器。

  1. 导航到 **NetScaler Gateway >** 策略 **>** 预身份验证。

2. 创建新的预身份验证策略或编辑现有策略。
3. 单击 **OPSWAT EPA** 编辑器 链接。
4. 在 表达式编辑器中，选择“窗口”**>** “**Windows** 更新”，然后单击“**+**”图标。
5. 在 操作系统名称中，根据需要选择服务器。

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。

[CGOP-20061]

- 缺失安全补丁的新 **EPA** 扫描分类类型

以下新的分类类型将添加到 EPA 扫描中以查找缺失的安全补丁程序。如果客户端缺少以下任何安全修补程序，则 EPA 扫描将失败。

- 应用程序
- 连接器
- CriticalUpdates
- DefinitionUpdates
- DeveloperKits
- FeaturePacks
- 指导
- SecurityUpdates
- ServicePacks
- 工具
- UpdateRollups
- 更新

您可以使用 GUI 配置分类类型。

1. 导航到 **NetScaler Gateway >** 策略 **>** 预身份验证。
2. 创建新的预身份验证策略或编辑现有策略。
3. 单击 ((OPSWAT EPA Editor)) 链接。
4. 在表达式编辑器中，选择“窗口”**>** “**Windows** 更新”。
5. 在 不应该缺少以下 **Windows** 更新分类类型的修补程序中，为缺失的安全修补程序选择分类类型
6. 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/en-us/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/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates

早些时候，EPA 扫描缺失的安全补丁程序是在严重级别上进行的：Windows 客户端上的“严重”、“重要”、“中”和“低”。

[CGOP-19465]

- 支持用于 **EPA** 扫描的多个设备证书

  在始终可用的 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用于 VPN 连接。如果此证书允许 EPA 成功扫描，则会建立 VPN 连接。如果此证书在扫描过程中失败，则使用下一个证书。此过程将一直持续到尝试所有证书为止。

  以前，如果配置了多个有效证书，如果一个证书的 EPA 扫描失败，则不会尝试对其他证书进行扫描。

  [CGOP-19782]

已修复的问题

- 如果在配置 VPN 虚拟服务器时在 SSL 配置文件中将 clientCert 参数设置为“可选”，则系统会多次提示用户选择智能卡。

  [NSHELP-30070]

- 将“networkAccessOnVPNFailure”始终开启配置文件参数从“fullAccess”更改为“onlyToGateway”后，用户无法连接到 NetScaler Gateway 设备。

  [NSHELP-30236]

- 如果配置了“始终打开”，则由于 aoservice.exe 文件中的版本号 (1.1.1.1) 不正确，用户通道将失败。

  [NSHELP-30662]

- 对内部和外部资源的 DNS 解析在长时间的 VPN 会话中停止工作。

  [NSHELP-30458]

- Windows VPN 客户端不接受来自服务器的“SSL 关闭通知”警报，而是在同一连接上发送转移登录请求。

  [NSHELP-29675]

- 注册局 EPA 检查“==”和“!=”运算符对某些注册表项失败。

  [NSHELP-29582]

22.2.1.103 (17-Feb-2022)

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。要修复此问题，请执行以下步骤：

  1. 对于 VPN 插件升级，最终用户必须首次使用 VPN 客户端进行连接，才能在其计算机上进行修复。在随后的登录尝试中，用户可以选择要连接的浏览器或插件。

2. 对于仅适用于 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。
   b) 等待下载页面出现并下载 nsepa_setup.exe。
   c) 下载完成后，关闭浏览器并安装 nsepa_setup.exe 文件。
   d) 重新启动客户端。

[NSHELP-30641]

21.12.1.4 (2021 年 12 月 17 日)

新增功能

- 品牌重塑变更

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

  [ACS-2044]

- 支持 **TCP/HTTP (S)** 专用应用程序

  Citrix Secure Access 客户端现在支持通过 Citrix Workspace Secure Access 服务为远程用户提供的 TCP/HTTP(S) 专用应用程序。

  [ACS-870]

- 其他语言支持

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

  - 韩语
  - 俄语
  - 繁体中文

  [CGOP-17721]

- **Windows 11** 支持 **Citrix Secure Access**

  Windows 11 现在支持 Citrix Secure Access 客户端。

  [CGOP-18923]

- 当用户从同一台计算机登录并且配置了 **Always on** 时，自动转移登录

  现在，当配置了 Always on 且用户从同一台计算机登录时，无需任何用户干预即可实现自动登录传输。以前，当客户端（用户）在系统重启或网络连接问题等情况下必须重新登录时，会出现弹出消息。用户必须确认转移登录。通过此增强功能，弹出窗口将被禁用。

  [CGOP-14616]

- 从 **NetScaler** 提供的网络掩码中获取 **Citrix** 虚拟适配器默认网关 **IP** 地址

  Citrix 虚拟适配器默认网关 IP 地址现在来自 NetScaler 提供的网络掩码。

  [CGOP-18487]

已修复的问题

- 有时，在拆分通道开启模式下建立 VPN 通道后，用户将无法访问 Internet。Citrix 虚拟适配器的错误默认路由会导致此网络问题。

  [NSHELP-26779]

- 当拆分通道设置为“反向”时，Intranet 域的 DNS 解析将失败。

  [NSHELP-29371]

21.9.100.1 (2021 年 12 月 30 日)

新增功能

- **Windows 11** 支持 **Citrix Secure Access**

  Windows 11 现在支持 Citrix Secure Access 客户端。

  [CGOP-18923]

已修复的问题

- 有时，在拆分通道开启模式下建立 VPN 通道后，用户将无法访问 Internet。Citrix 虚拟适配器的错误默认路由会导致此网络问题。

  [NSHELP-26779]

- 当拆分通道设置为“反向”时，Intranet 域的 DNS 解析将失败。

  [NSHELP-29371]

21.9.1.2 (2021 年 10 月 4 日)

已修复的问题

- 有时，断开 VPN 连接后，DNS 解析器无法解析主机名，因为在 VPN 断开连接期间会删除 DNS 后缀。

  [NSHELP-28848]

- 有时，设置客户端空闲超时后，用户会在几秒钟内注销 NetScaler Gateway。

  [NSHELP-28404]

- Windows 插件可能会在身份验证期间崩溃。

  [NSHELP-28394]

- 在“始终开机”服务模式下，Windows 的 VPN 插件无法在用户登录到 Windows 计算机后自动建立用户通道。

  [NSHELP-27944]

- 通道建立后，Windows 插件将添加具有默认网关地址的路由，而不是使用先前的网关 IP 地址添加 DNS 服务器路由。

  [NSHELP-27850]

V21.7.1.1 (27-Aug-2021)

新增功能

- 新的 **MAC** 地址扫描

  添加了对较新 MAC 地址扫描的支持。

  [CGOP-16842]

- **EPA** 扫描以检查 **Windows** 操作系统及其构建版本

  添加了 EPA 扫描以检查 Windows 操作系统及其构建版本。

  [CGOP-15770]

- **EPA** 扫描以检查是否存在特定值

  注册表 EPA 扫描中的一种新方法现在可以检查是否存在特定值。

  [CGOP-10123]

已修复的问题

- 如果由于网络错误而在登录过程中出现 JavaScript 错误，则随后的登录尝试将失败并出现相同的 JavaScript 错误。

  [NSHELP-27912]

- 对于 McAfee 防病毒软件的上次更新时间检查，EPA 扫描失败。

  [NSHELP-26973]

- 有时，在建立 VPN 通道后，用户会失去互联网访问权限。

  [NSHELP-26779]

- 在 nFactor 身份验证期间，可能会显示 VPN 插件的脚本错误。

  [NSHELP-26775]

- 如果发生网络中断，则在网络中断之前开始的 UDP 流量最多不会下降 5 分钟。

  [NSHELP-26577]

- 如果 DNS 注册所花费的时间比预期的长，您可能会遇到 VPN 通道启动延迟的情况。

  [NSHELP-26066]

V21.3.1.2 (31-Mar-2021)

新增功能

- 升级后的 **EPA** 库

  EPA 库已升级，以支持 EPA 扫描中使用的最新版本的软件应用程序。

  [NSHELP-26274]

- **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 直接虚拟适配器（用于打印机）兼容。

  [NSHELP-26366]

已修复的问题

- Windows VPN 网关插件阻止在 VPN 通道上使用“CTRL+P”和“CTRL + O”。

  [NSHELP-26602]

- 当请求对计算机名称执行操作时，适用于 Windows 的 NetScaler Gateway 插件仅使用在 Active Directory 中注册的 Intranet IP 地址进 `"nslookup"` 行响应。

  [NSHELP-26563]

- 如果拆分 DNS 设置为“本地”或“两者兼而有之”，则 IIP 注册和注销会间歇性失败。

  [NSHELP-26483]

- 如果配置了“始终开启”，则自动登录 Windows VPN 网关插件将失败。

  [NSHELP-26297]

- Windows VPN 网关插件无法丢弃 IPv6 DNS 数据包，从而导致 DNS 解析出现问题。

  [NSHELP-25684]

- Windows VPN 网关插件会保留现有的代理例外列表，即使由于 Internet Explorer 代理例外列表上的浏览器限制而溢出列表也是如此。

  [NSHELP-25578]

- 在始终开启模式下注销 VPN 客户端时，Windows VPN 网关插件无法还原代理设置。

  [NSHELP-25537]

- 如果满足以下条件，则 Windows 的 VPN 插件在登录到 Windows 后不会建立通道：

  - NetScaler Gateway 设备已配置为“始终开启”功能。
  - 设备配置为基于证书的身份验证，双因素身份验证“关闭”。

  [NSHELP-23584]

Microsoft Edge WebView 支持 Windows Citrix Secure Access - 预览版

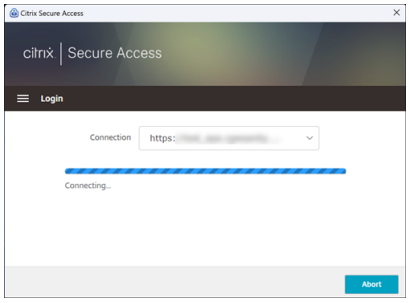
February 1, 2024

Microsoft Edge WebView 现在是 Microsoft 推荐的 WebView，因为 Internet Explorer WebView 已过时。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。

目前，默认情况下，Microsoft Edge WebView 处于禁用状态。您可以使用 https://podio.com/webforms/28291989/2245437 注册预览版。

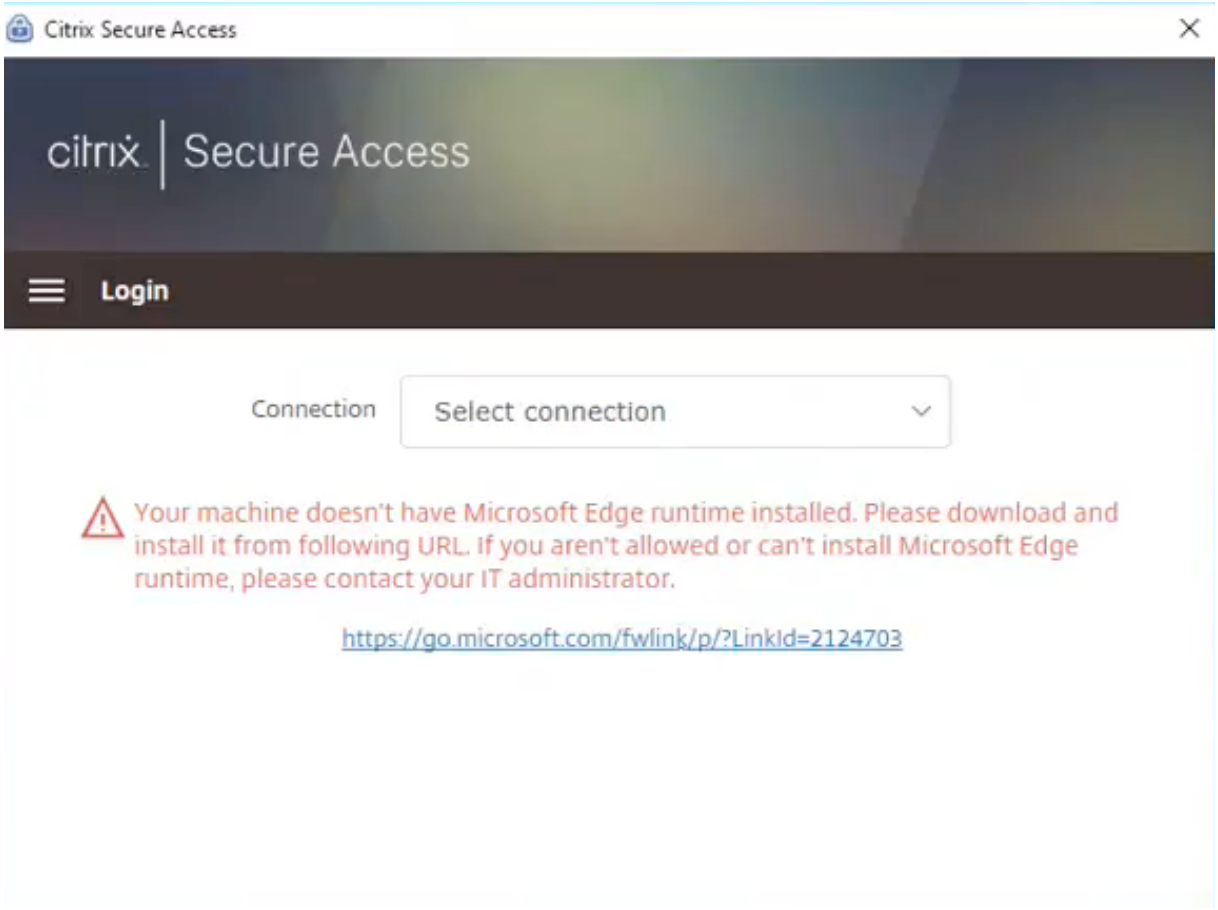
对最终用户的更改

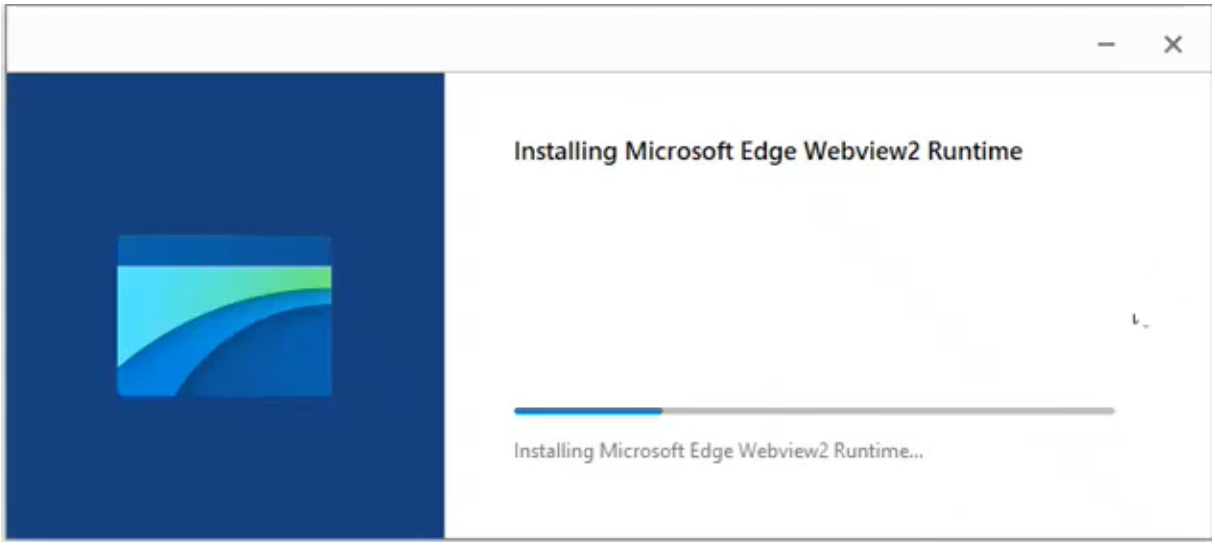
Citrix Secure Access 客户端 UI 的身份验证屏幕如下所示。



最终用户选择 URL 后，Citrix Secure Access 客户端会打开一个新窗口，提示他们使用自己的证书登录 NetScaler Gateway。

如果 Windows 客户端未安装 Microsoft Edge WebView 运行环境，则会在 Citrix Secure Access 客户端用户界面上为最终用户提供下载和安装 Microsoft Edge WebView 运行时的链接。当连接到 VPN 时，最终用户可以无缝下载和安装 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 功能不会影响任何管理员专用的配置。

故障排除

- 如果您在使用此功能时遇到任何问题，请联系 Citrix 支持部门。
- 您可以通过 citrixgatewaybetafeedback@cloud.com 提交有关 Edge WebView 功能的反馈。

改进了 **Windows** 客户端的日志收集

February 1, 2024

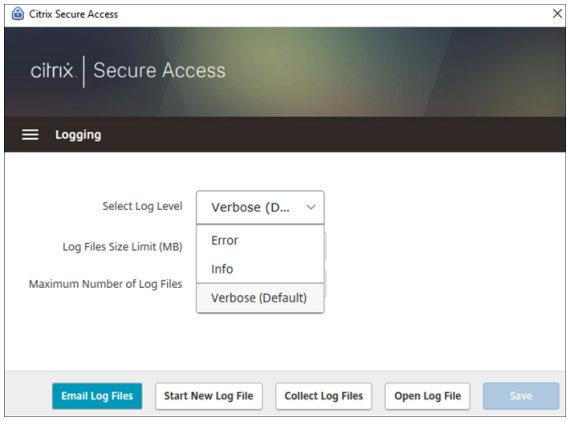
通过改进日志收集和调试，Windows Secure Access 客户端的日志记录功能得到了增强。新的日志文件以“csa_”为前缀。

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

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，日志的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“记录”。与日志相关的所有配置都可以在日志屏幕中完成。



- 选择日志级别：

  启用新的日志记录机制后，以下三个日志级别可用。

  - 错误：仅记录应用程序报告的异常或故障。
  - 信息：此级别包括与程序执行相关的信息消息和事件。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：（必选）输入每个日志文件的日志文件大小。最大值为 600 MB。
- 最大日志文件数：（必选）输入要为日志收集添加的文件数。最大值为 5。
- 电子邮件日志文件—通过电子邮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 -单击创建包含应用程序中所有日志文件的 zip 文件。此 zip 文件保存在客户端的桌面上。
- 打开日志文件 - 选择此选项时，最新的 `csa_nssslvpn*.txt` 文件将打开。

适用于 **Linux** 的 **Citrix Secure Access** 客户端

February 1, 2024

适用于 Linux 的 Citrix Secure Access 客户端是一款由 NetScaler Gateway 管理的 VPN 客户端软件，通过该软件，用户可以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 End Point Analysis (EPA) 客户端是一款由 NetScaler Gateway 管理的客户端软件。在授予通过 NetScaler Gateway 访问公司数据的权限之前，它会检查端点条件。Citrix EPA 客户端和 Citrix Secure Access 客户端相互独立。

> 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，以备日后选择使用 EPA 功能。

支持的 **Linux** 版本

Citrix Secure Access 客户端和 Citrix EPA 客户端兼容 Ubuntu 18.04、Ubuntu 20.04 和 Ubuntu 22.04 版本。有关支持的浏览器的更多信息，请参阅客户端软件要求。

> 注意：
>
> 要让 Ubuntu 22.04 与 Citrix Secure Access 客户端和 Citrix EPA 客户端配合使用，请在 NetScaler CLI 上将 SSL 参数 denySSLReneg 设置为 NONSECURE。

支持的功能

适用于 Ubuntu 的 Citrix Secure Access 客户端支持以下功能：

- 分割通道和反向分割通道
- 为 TCP、UDP 和 ICMP 应用程序建立通道
- 服务器通过内联网 IP (IIP) 发起的连接
- Split DNS remote
- 客户端代理
- 经典的 EPA 扫描
- 高级身份验证 (nFactor) 包括高级 EPA 扫描（仅限来自浏览器）
- HTTPOnly cookie
- 全局服务器负载平衡 (GSLB)

> 注意：
>
> 适用于 Ubuntu 的 Citrix Secure Access 客户端不支持 Split DNS BOTH。

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 客户端分别被命名为“nsgclient18_64.deb”和“nsepa18.deb”。这些客户端与 Ubuntu 18.04 和 20.04 兼容。

支持 Ubuntu 22.04 的 Citrix Secure Access 客户端和 Citrix EPA 客户端分别被命名为“nsginstaller64.deb”和“nsepa.deb”。

例如，如果您想升级到最新版本的 Citrix Secure Access 客户端，从 1.0.0.x 版本升级到版本 23.6.1，例如：

1. 使用 shell 提示符替换位置 /var/netscaler/gui/vpn/scripts/linux/ 的文件“nsg-client18_64.deb”和“nsginstaller64.deb”。
2. 使用 shell 提示符替换位置 /var/netscaler/gui/epa/scripts/linux/ 的文件“nsepa18.deb”和“nsepa.deb”。
3. 打开文件 /var/netscaler/gui/vpn/scripts/linux/clientversions.xml。

   a) 对于 Citrix EPA 客户端，将以下 XML 标签中的当前版本 (1.0.0.x) 替换为最新版本 (23.6.1)。如果 XML 标记不存在，请将其添加到 XML 文件中。例如，

   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"/>
   ```

   带

   ```
   <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"/>
   ```

   并替换

   ```
   <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"/>
   ```

   带

   ```
   <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) 对于 Citrix Secure Access 客户端，将以下 XML 标签中的当前版本 (1.0.0.x) 替换为最新版本 (23.6.1)。如果 XML 标记不存在，请将其添加到 XML 文件中。例如，

   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"/>
   ```


更改为

```
<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"/>
```

和

```
<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"/>
```

更改为

```
<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
```

引用

- NetScaler Gateway VPN 客户端和支持的功能
- Ubuntu 支持的端点分析扫描
- 最终用户帮助文档

适用于 **Linux** 的 **Citrix Secure Access** 发行说明

February 1, 2024

适用于 Linux 的 Citrix Secure Access 客户端和 Citrix End Point Analysis (EPA) 客户端现已独立发布，与所有 NetScaler 版本兼容。Citrix Secure Access 客户端版本采用 YY.MM Release.Build 格式。

发行说明描述了新增功能、对现有功能的增强、已修复的问题和已知问题。

新增功能：当前版本中提供的新功能和增强功能。

已修复的问题：当前版本中修复的问题。

已知问题：当前版本中存在的问题及其解决方法（如果适用）。

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

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 用户界面的“连接”页面分别以 KB 和 MB 为单位显示数据传输速率，而不是 Ko 和 Mo。

[NSOSLX-177]

23.9.1 (2023 年 9 月 8 日)

新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

[CGOP-25231]

23.6.2（2023 年 6 月 20 日）

新增功能

- **Ubuntu 22.04** 支持 **Citrix Secure Access** 客户端和 **Citrix EPA** 客户端

  Ubuntu 22.04 是 Ubuntu 最新的长期支持版本。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。

  [CGOP-24312]

- **GSLB** 支持 **Citrix Secure Access** 和 **Citrix EPA** 客户端

  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（内联网资源）始终可供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被重定向到另一个数据中心。有关更多信息，请参阅在 NetScaler Gateway 上支持主动-主动 GSLB 部署。

  [CGOP-23506]

- **HTTPOnly** 支持 **Citrix Secure Access** 和 **Citrix EPA** 客户端

  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。此功能有助于防止由于跨站脚本而导致的 cookie 被盗。有关更多信息，请参阅在身份验证 cookie 上强制使用 HttpOnly 标志。

  [CGOP-23517]