

适用于 Android 设备的 Citrix Secure Access 客户端

适用于 Android 的 Citrix Secure Access 客户端提供了 NetScaler Gateway 提供的同类最佳的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。

注意：

- 从版本 23.12.1 开始，适用于 Android 的 Citrix SSO 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。
- 有关适用于 Android 的 Citrix Secure Access 的管理员特定说明，请参阅 [适用于 Android 设备的 Citrix Secure Access](#)。

如何在您的 Android 设备上使用 Citrix Secure Access

从您的 Play 商店安装 Citrix Secure Access。首次使用的用户必须在非 MDM 情况下通过添加服务器来创建与 NetScaler Gateway 的连接。对于后续使用，您可以连接到现有连接或添加连接，如果您的管理员在 MDM 部署中允许，您也可以编辑现有连接。您还可以查看日志并采取相应的操作。

注意：

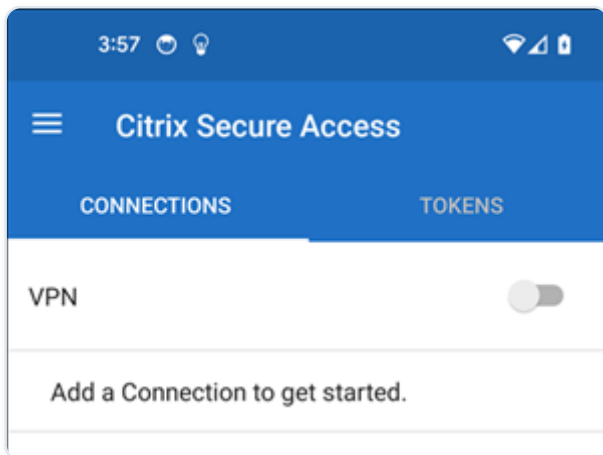
- 通过 MDM 部署的连接无法编辑。
- 系统可能会提示您授予 Citrix Secure Access 应用程序 [查询所有软件包](#) 的权限。一旦授予权限，Citrix Secure Access 应用程序将：
 - 从操作系统接收软件包安装通知。
 - 重启 Always On VPN。

当您首次连接到 VPN 配置文件时，系统会提示您提供同意（Google 政策要求）以收集有关已安装软件包的信息。如果您授予同意，VPN 连接将启动。如果您拒绝同意，VPN 连接将被中止。一旦授予同意，同意屏幕将不再出现。

添加连接

注意：此步骤仅在非 MDM 情况下需要。

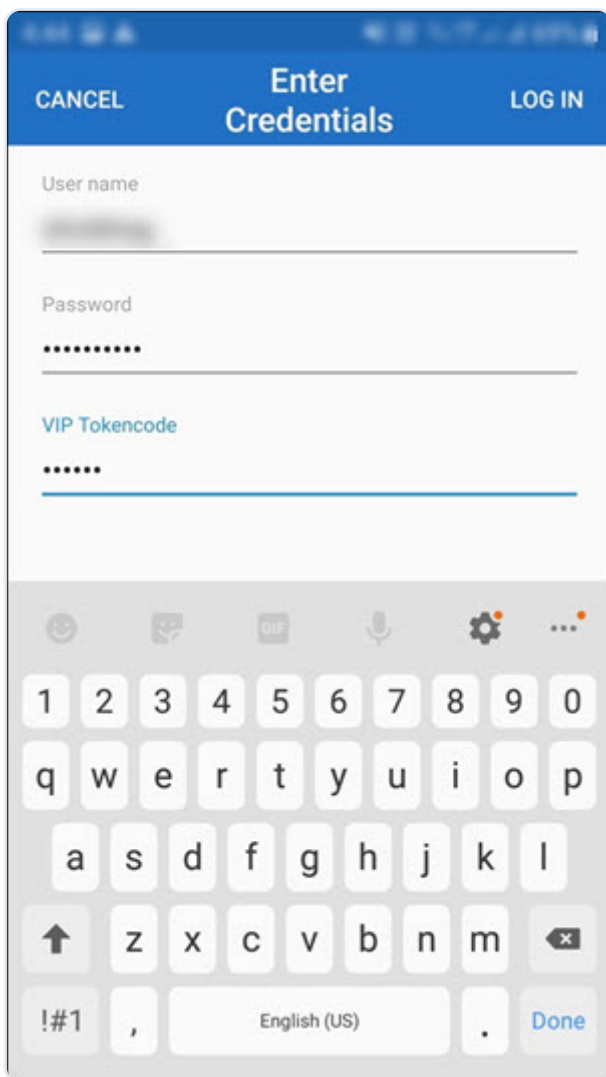
在您的 Android 设备上安装 Citrix Secure Access 并打开应用程序后，将出现以下屏幕。



1. 单击 + 添加连接。
2. 输入基本 URL（例如，[我的公司](#)）和 VPN 连接的名称。您可以选择输入用户名。
3. 单击 **保存**，然后根据需要单击 **保存并连接** 或 **仅保存**。

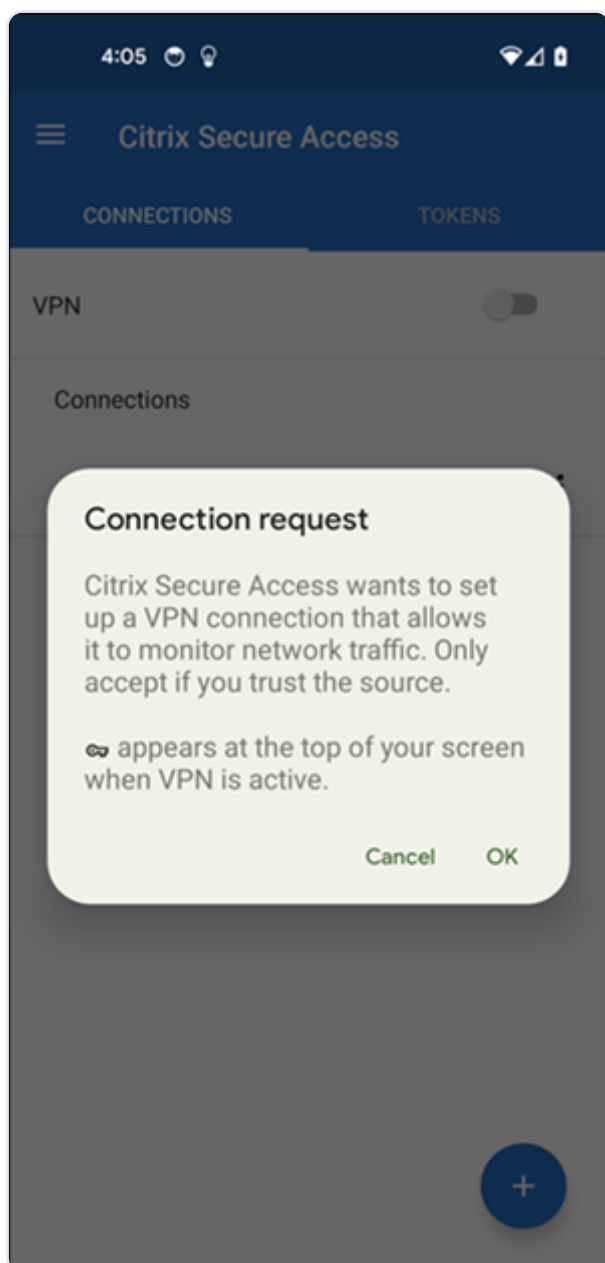
The screenshot shows a mobile application interface for adding a connection. The top bar is blue with the title 'Add Connection' and two buttons: 'CANCEL' and 'SAVE'. The 'SAVE' button is highlighted with a red box. Below the header, there are three input fields: 'Server', 'Description', and 'User Name'. At the bottom, there are three buttons: 'Save and Connect', 'Just Save', and 'Cancel'. The 'Save and Connect' and 'Just Save' buttons are grouped together and highlighted with a red box.

4. 为您的服务器提供身份验证凭据，然后在键盘上点击 **登录** 或 **完成**。

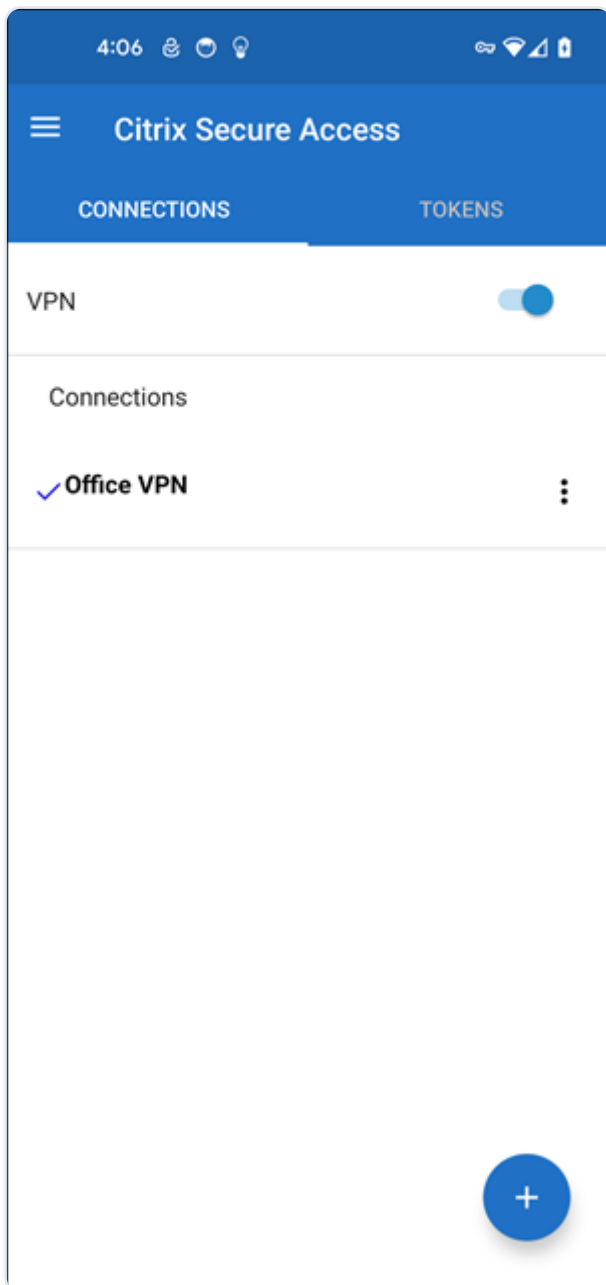


连接请求消息出现。点击 **确定**。

注意：此消息仅在 Citrix Secure Access 首次建立任何 VPN 连接时出现。如果用户首次允许连接，则在用户卸载并重新安装应用程序之前，此消息不会再次显示。



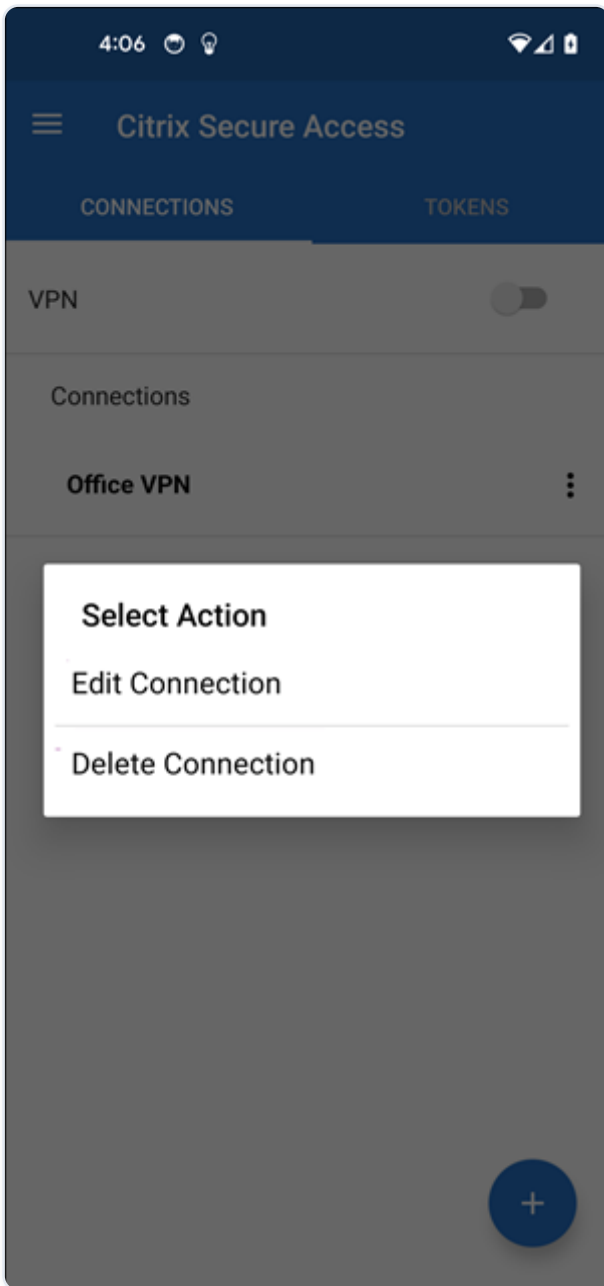
注意：要从 Citrix Secure Access 注销，请关闭 **VPN** 开关。



修改或删除现有连接

从 Citrix Secure Access 注销后，您可以编辑或删除连接。

点击并按住服务器名称，然后选择 **编辑连接** 或 **删除连接**。



VPN 连接失败后重新连接到 NetScaler Gateway - 预览

当 VPN 连接丢失时，适用于 Android 的 Citrix Secure Access 客户端会提示您重新向 NetScaler Gateway 进行身份验证。您的 Android 设备的 UI 和通知面板上会显示通知，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。

注意：

此功能为预览版。

重新使用 NetScaler Gateway 进行身份验证(/en-us/citrix-ssso/media/reconnect-to-gateway-android.png)

在 Android 17 及更高版本上允许本地网络访问权限

从 Citrix Secure Access for Android 26.08.1 版本开始，在 Android 17 及更高版本上安装、重新安装或更新应用程序的用户会收到提示，要求允许本地网络访问。如果拒绝访问，则在 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。

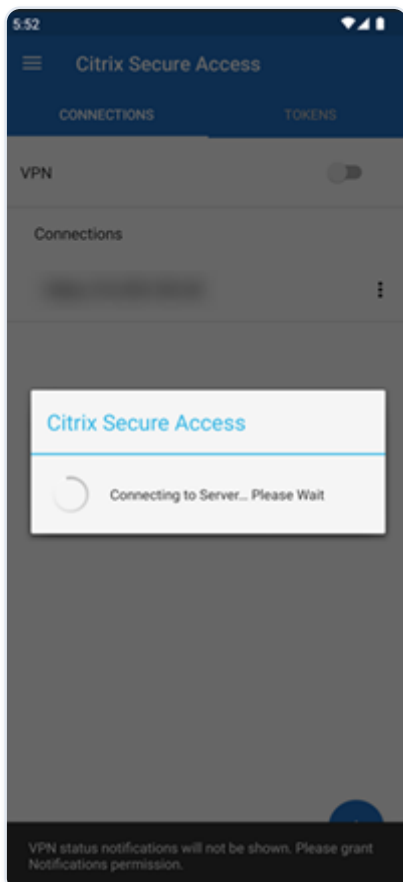
建议 MDM 管理员预先授予 Citrix Secure Access 应用程序此权限。

在 Android 13 及更高版本上接收或阻止通知

从 Citrix Secure Access for Android 23.12.1 版本开始，在 Android 13 及更高版本上安装、重新安装或更新应用程序的用户会收到提示，要求允许通知。如果拒绝通知，用户将不会收到来自 Citrix Secure Access 的 VPN 状态或推送通知。

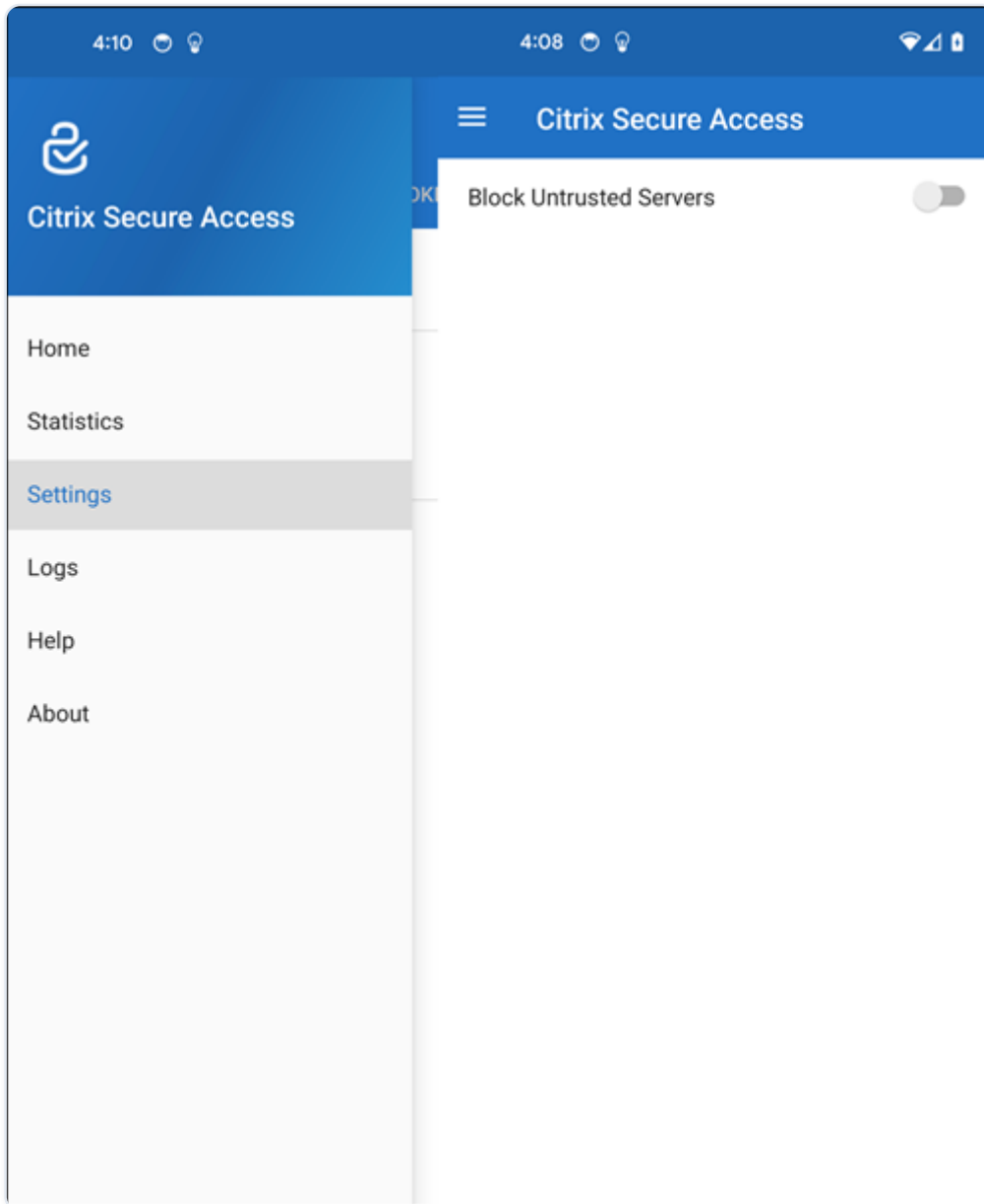
您可以导航到 Android 设备上的 **设置 > 通知** 来更改通知权限。

在以下示例中，VPN 状态通知已被禁用。



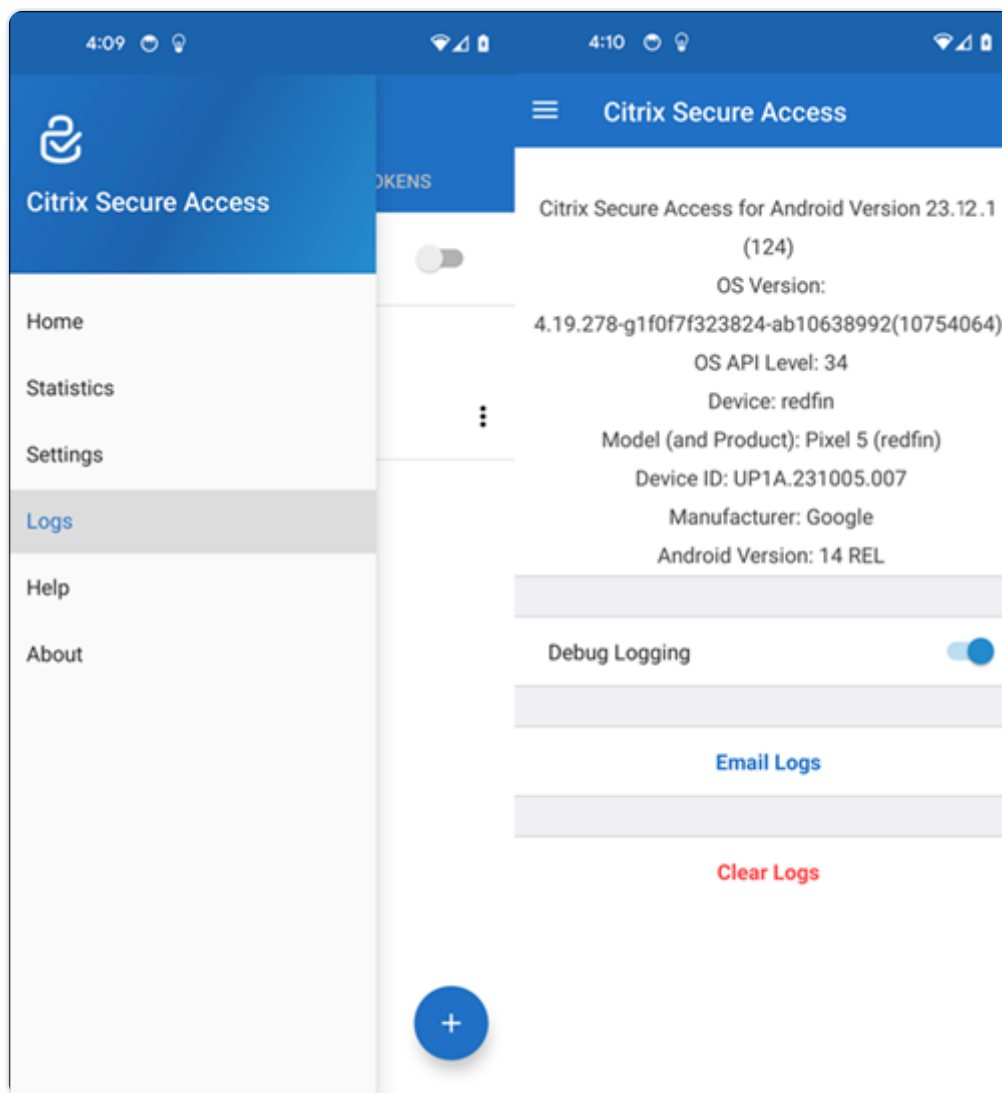
阻止不受信任的服务器

默认情况下，Citrix Secure Access 不连接到不受信任的服务器。不受信任的服务器是指使用自签名证书或没有网关的受信任根证书的服务器。要允许这些类型的连接，您可以将“阻止不受信任的服务器”开关设置为“关闭”。



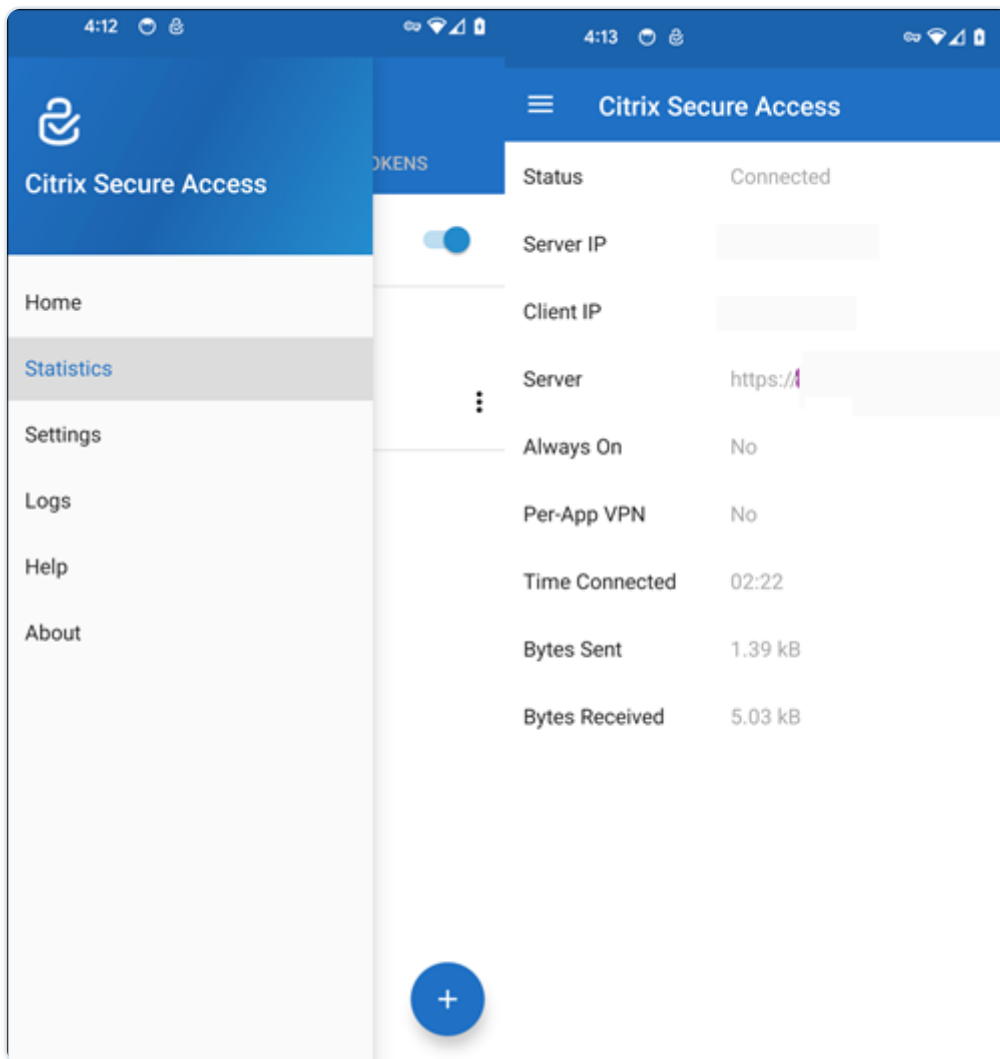
启用调试日志

捕获调试日志是故障排除或向 Citrix 支持报告问题的关键部分。点击“调试日志记录”开关“开启”以后用 Citrix Secure Access 的调试日志记录。您可以使用“电子邮件日志”链接在排查连接问题时发送日志。



查看统计信息

VPN 连接后，您可以查看连接统计信息。



密码令牌

您可以添加一个 6 位数字的密码令牌作为第二因素身份验证。此代码使用基于时间的单次密码协议生成 OTP 代码。

您可以手动添加密码令牌，也可以使用二维码扫描方法注册密码令牌。如果您选择手动输入令牌，则不会启用使用推送通知的第二因素身份验证。

注册密码令牌

1. 在台式机或笔记本电脑上，使用 Web 浏览器登录您组织的管理一次性 PIN 页面。
2. 单击 **添加设备**。
3. 输入设备的名称，然后单击 **Go**。

将生成一个二维码。

通过扫描浏览器上的二维码添加密码令牌

1. 导航到 **主页** 视图上的 **令牌** 选项卡。

2. 点击 **+**，然后点击 **扫描二维码**。
3. 将摄像头对准浏览器上的二维码。

Citrix Secure Access 会自动填充设备名称和密钥。

或者，您可以手动输入显示在二维码上方的密钥。

Citrix Secure Access 会验证二维码，然后向网关注册以接收推送通知。如果注册过程中没有错误，令牌将成功添加到令牌选项卡。

注意：

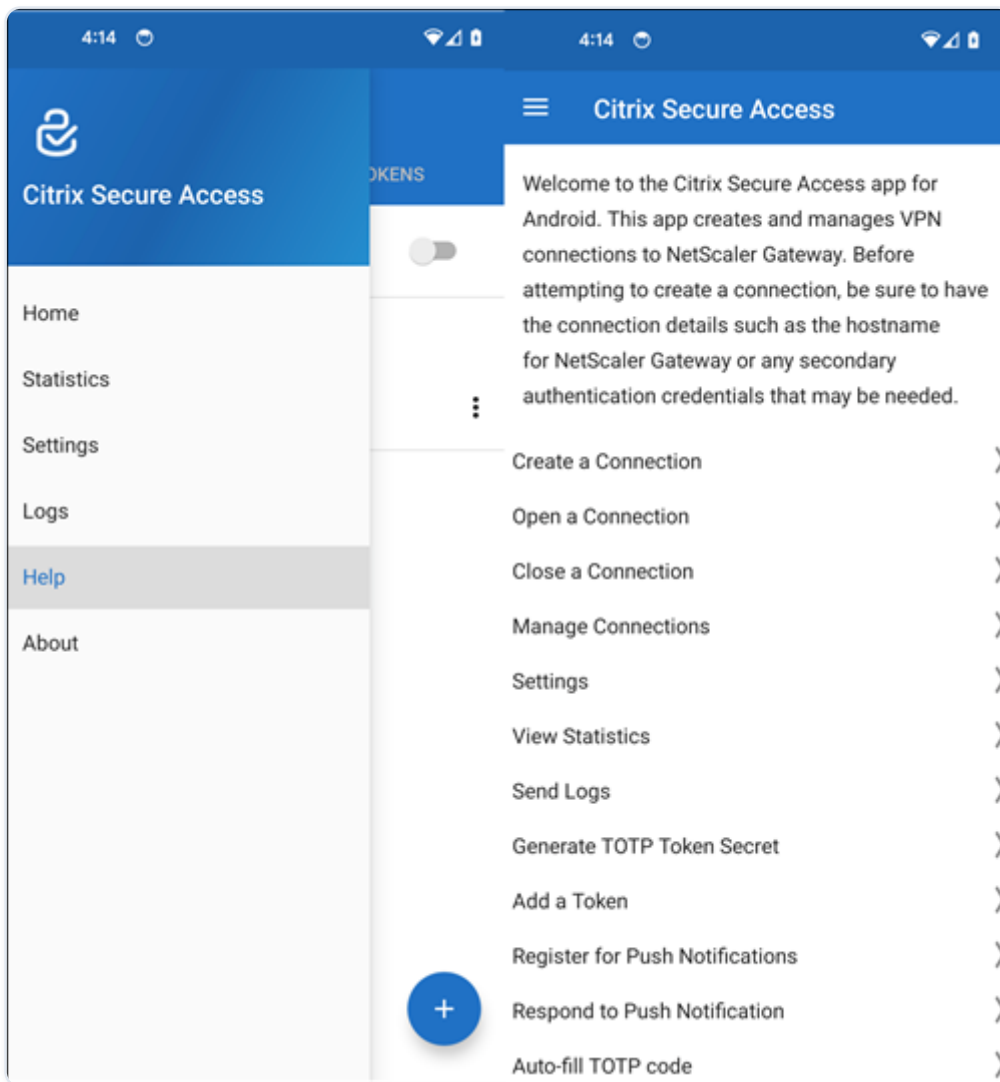
- 您必须允许 Citrix Secure Access 访问摄像头权限才能捕获二维码。
- 您必须在设备上启用设备 PIN/密码。

手动添加密码令牌

1. 导航到“主页”视图上的“令牌”选项卡。
2. 点击 **+**，然后点击“手动输入”。
3. 输入设备名称和密钥，与浏览器上生成的密码令牌中显示的一致。

帮助主题

有关如何使用 Citrix Secure Access 的更多信息，请参阅“[帮助](#)”。



使用在 Intune 环境中配置的 Citrix Secure Access 连接到您的公司网络

注意：

有关适用于 Android 的 Citrix Secure Access 的管理员特定说明，请参阅[适用于 Android 设备的 Citrix Secure Access](#)。

本主题介绍了如何使用在 Microsoft Intune Android Enterprise 环境中配置的 Citrix Secure Access 客户端连接到公司网络。

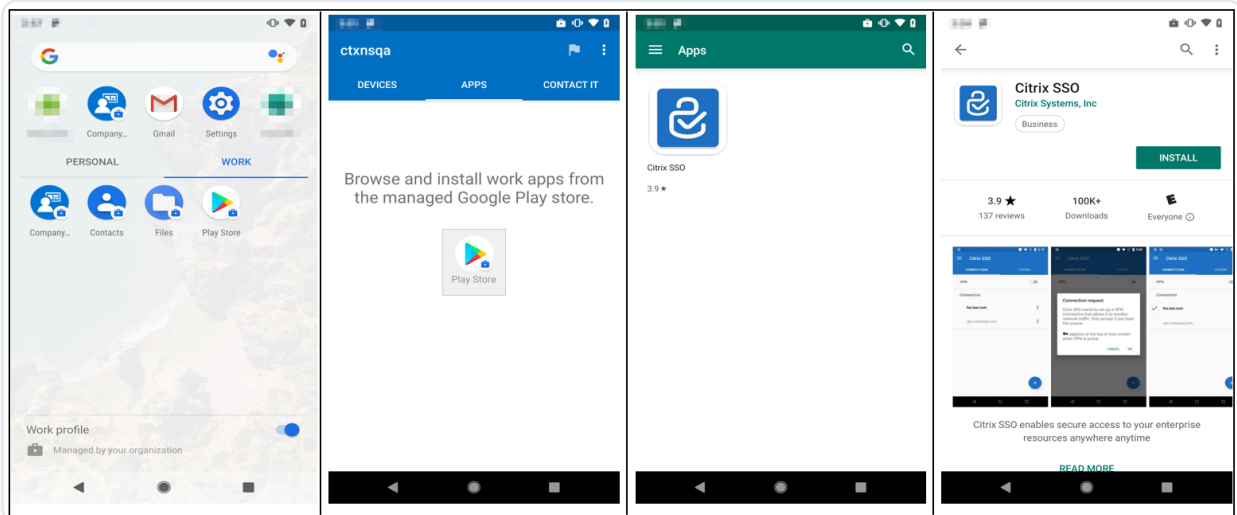
假设：

- 您已使用 Intune 公司门户应用在 Intune 中注册设备。

- 已在设备上为用户设置工作配置文件。

1. 从工作配置文件中打开设备上的 **Intune 公司门户** 应用。
2. 单击三点菜单以打开应用的设置并滚动到屏幕底部。单击 **SYNC** 以与 Intune 服务器同步，然后导航到主应用屏幕。
3. 单击 **APPS** 选项卡，然后单击 **Managed Google Play Store** 链接。

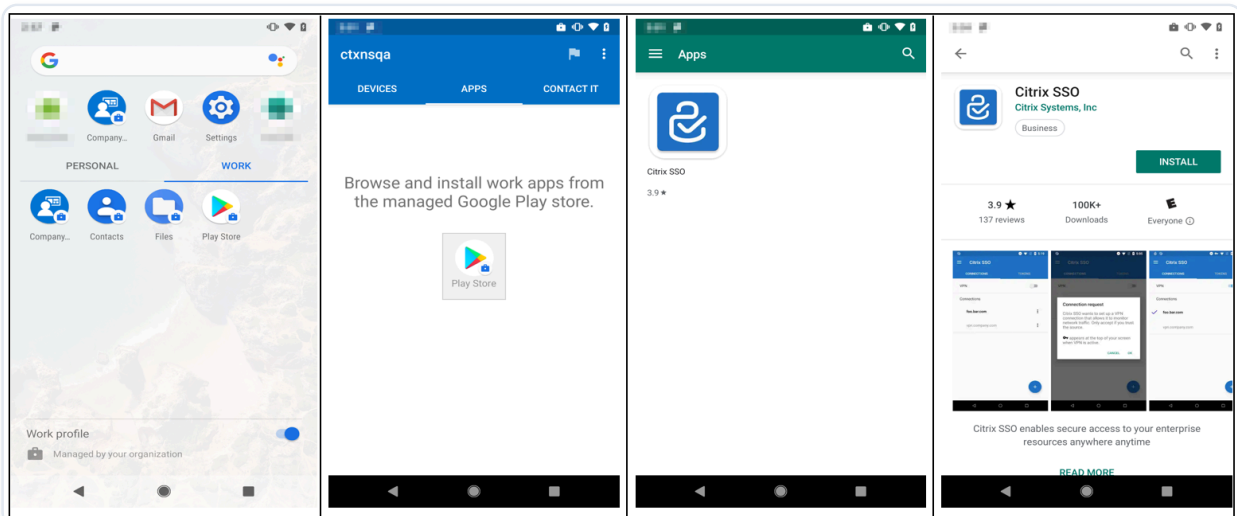
将显示用户的已批准应用列表。



4. 单击 **思杰安全访问**。

Citrix Secure Access 客户端将显示在 Managed Google Play 商店中。

5. 单击 **INSTALL**。
6. 返回工作配置文件应用列表。Citrix Secure Access 已添加到已安装应用列表。
7. 单击工作配置文件应用列表中的 Citrix Secure Access 图标以将其打开。



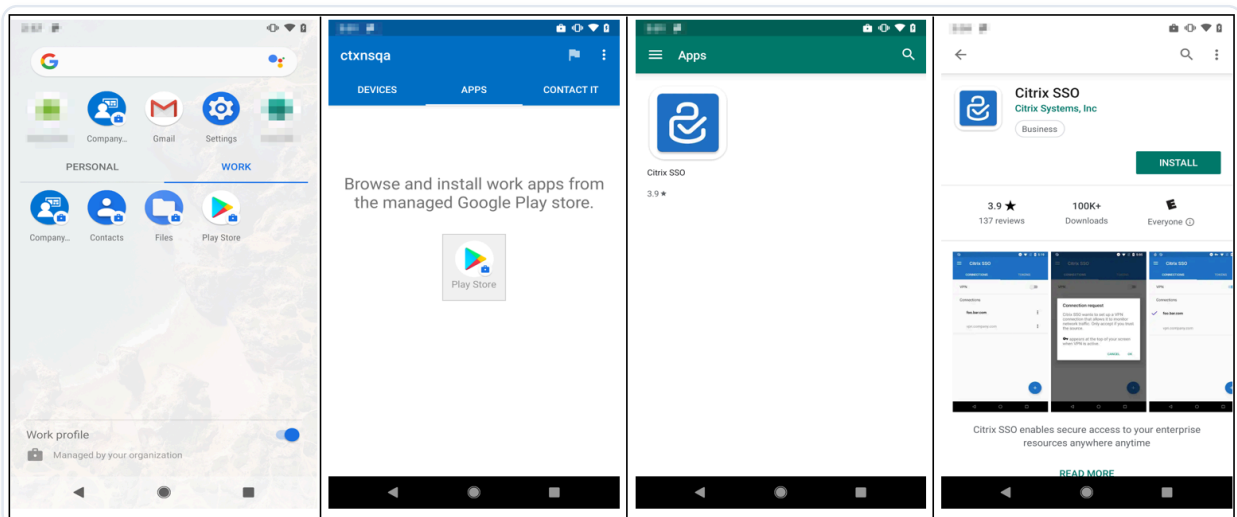
Citrix Secure Access 打开。系统会提示您允许或拒绝与公司内部网络安全通信的权限。

8. 点击**允许**以授予权限。如果您选择**不允许**，Citrix Secure Access 将关闭，并且您无法使用 Citrix Secure Access 客户端。

注意：

系统可能会提示您允许或拒绝**管理和拨打电话的权限**（如果尚未通过 Intune 授予）。点击**允许**以授予权限。您可以拒绝此权限，但如果 NetScaler Gateway 上的设备身份验证需要 Intune NAC 检查，则在您授予此权限之前，您无法连接到公司的内部网络。

9. **我的公司 VPN**（或您在 Intune 的 Citrix Secure Access 配置中选择的名称）列在**连接**选项卡的“托管连接”部分。点击此连接，系统会提示您输入凭据以通过 NetScaler Gateway 进行身份验证。
10. 提供用于通过 NetScaler Gateway 进行身份验证的凭据，然后点击**登录**。



如果 NetScaler Gateway 上配置了客户端证书身份验证，系统可能会提示您选择证书。您可以提供对证书的访问权限。

11. Android 系统会提示您允许**连接请求**以设置 VPN 隧道。点击**确定**以授予 Citrix Secure Access 权限，以便与您的公司内部网络建立安全连接。

****注意：****此提示仅在您首次与 NetScaler Gateway 建立安全连接时显示。在设备上卸载并重新安装 Citrix Secure Access 之前，后续连接尝试不会显示此提示。

您已连接到公司的内部网络。设备状态栏中会出现一个钥匙图标，通知您 VPN 连接处于活动状态。Citrix Secure Access 客户端的 VPN 服务通知图标也会出现在状态栏上。连接开关的状态变为已连接，并且 VPN 配置文件名称旁边会出现一个勾选标记图标。

适用于 iOS 设备的 Citrix Secure Access 客户端

适用于 iOS 的 Citrix Secure Access 客户端提供了由 NetScaler Gateway 提供的业界最佳的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 应用程序在 iOS 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 配置文件和按应用程序 VPN 配置文件。

重要提示：

- 从版本 23.11.1 开始，适用于 iOS 的 Citrix SSO 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。
- 有关适用于 iOS 的 Citrix Secure Access 的管理员专用说明，请参阅[适用于 iOS 的 Citrix SSO](#) 和[适用于 macOS 的 Citrix Secure Access](#)。

在 Citrix Secure Access 应用程序中导入和安装证书

iOS 上的 Citrix Secure Access 支持使用 NetScaler Gateway 进行客户端证书身份验证。证书可以通过以下方式交付到 Citrix Secure Access：

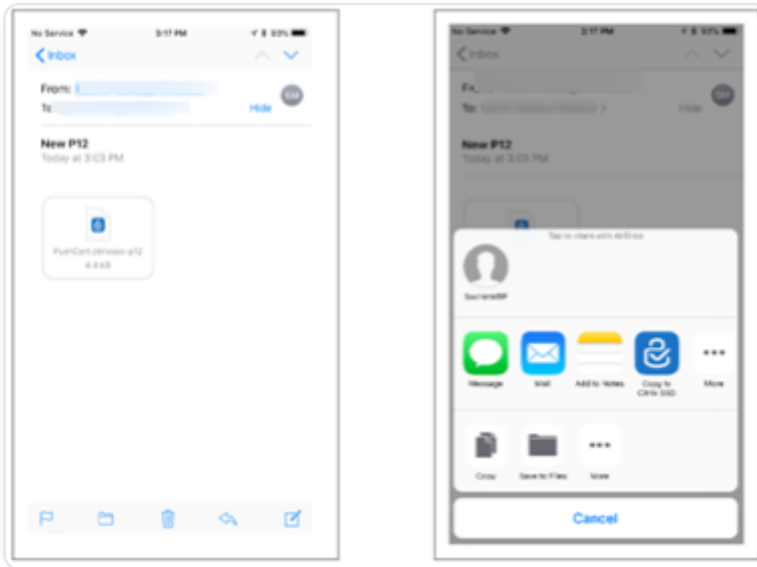
- **MDM 服务器** - MDM 客户的首选方法。证书直接在 MDM 管理的 VPN 配置文件上配置。当设备注册到 MDM 服务器时，VPN 配置文件和证书都会推送到已注册的设备。请遵循 MDM 供应商特定的文档来了解此方法。
- **电子邮件** - 非 MDM 客户的唯一方法。管理员将包含用户证书身份（证书和私钥）的电子邮件作为 PKCS#12 文件附件发送给用户。用户必须在其 iOS 设备上配置电子邮件帐户才能接收带附件的电子邮件。然后将该文件导入到 iOS 上的 Citrix Secure Access 中。

注意：

文件名扩展名 `.pfx` 和 `.p12` 被 iOS 系统占用，不能被 Citrix Secure Access 等第三方应用程序占用。因此，管理员必须将用户证书的扩展名/MIME 类型从标准 `.pfx` 或 `.p12` 分别更改为 `.citrixsso-pfx` 或 `.citrixsso-p12`。

1. 打开包含用户证书身份（证书和私钥）并以 PKCS#12 文件形式附加的电子邮件。

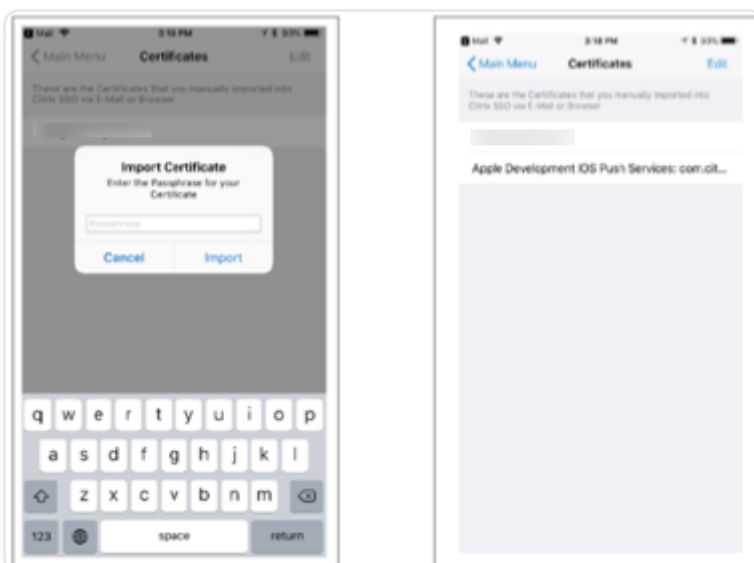
- 点击附件以显示系统 **OpenIn** 菜单。
- 点击 **复制到 Citrix SSO**。



2. 在 Citrix Secure Access 中安装证书。

应用程序现已启动，并显示证书密码短语提示。输入正确的证书密码短语以将其安装到应用程序的钥匙串中，然后点击 **导入**。

验证成功后，证书将被导入。



3. 将基于证书的身份验证与 VPN 结合使用。

- 要使用证书进行 VPN 身份验证，您必须首先在 Citrix Secure Access 上创建 VPN 配置或配置文件。
 - 导航到“VPN 连接”视图，然后点击“添加 VPN 配置”。
 - 在 VPN 配置文件的配置视图中，您可以在“证书”部分选择导入的证书。

添加 VPN 配置或配置文件(/en-us/citrix-sso/media/sso-ios-certificate1.png)

- 点击“保存”以导入证书。

证书导入成功(/en-us/citrix-sso/media/sso-ios-certificate2.png)

4. 管理证书。

要管理导入到 Citrix Secure Access 的证书，请导航到“主菜单”中的“证书”选项卡。

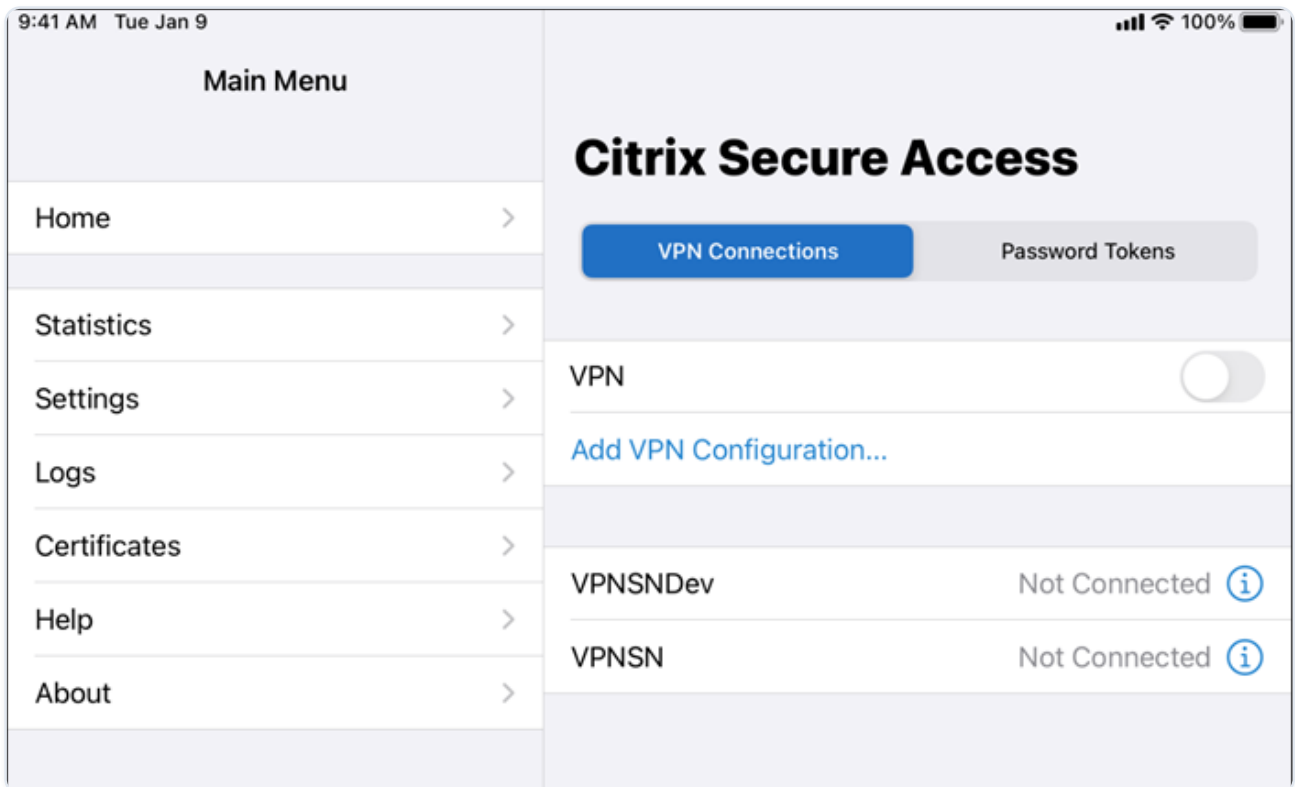
如何从您的 iOS 设备使用 Citrix Secure Access

从 App Store 安装 Citrix Secure Access 应用程序。安装应用程序后，首次使用时，您必须通过添加服务器来创建与 NetScaler Gateway 的连接。后续使用时，您可以连接到现有连接或添加新连接，也可以编辑现有连接。您还可以查看日志并采取相应的操作。

对于 MDM 客户，您的管理员可能已预配置 VPN 连接，这些连接在您注册设备时会自动显示。您可以通过选择连接并打开 VPN 开关来直接启动连接。这些 VPN 连接用户不可编辑。

添加连接

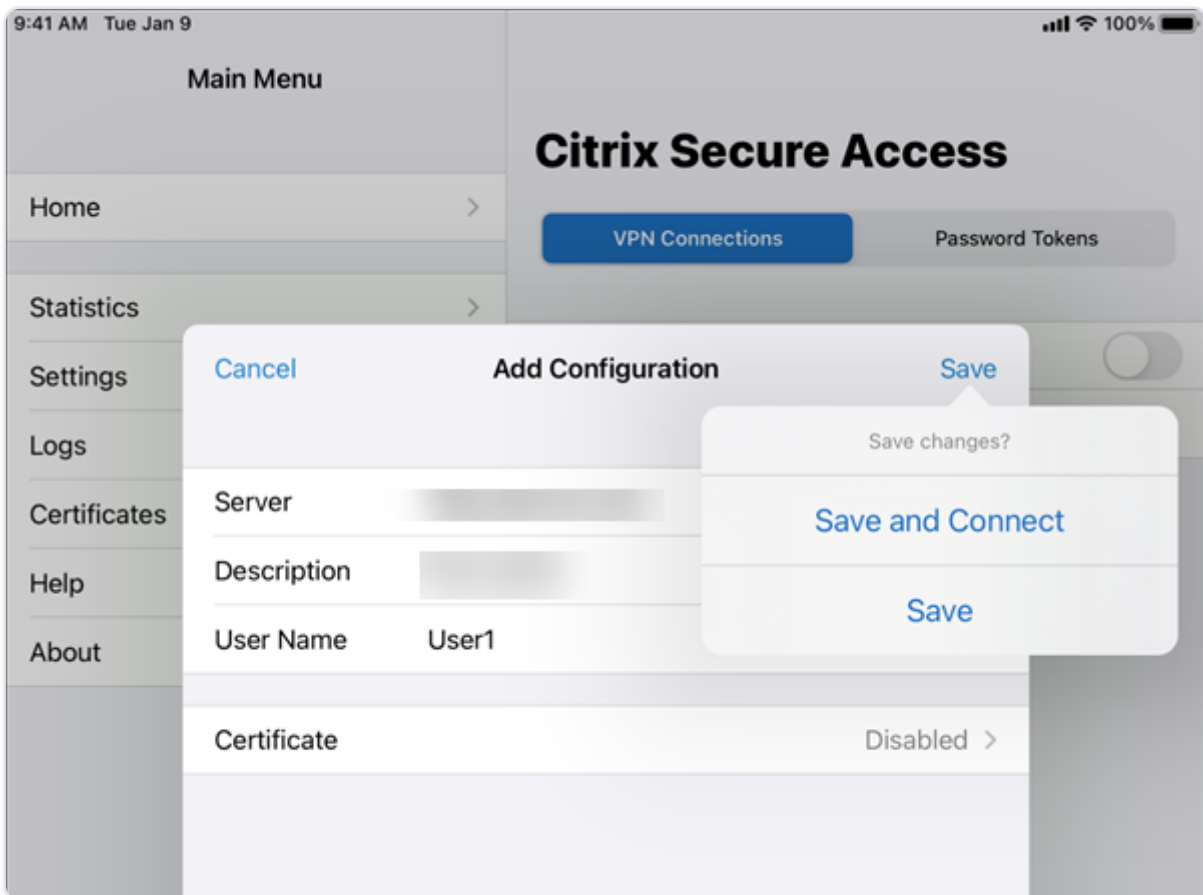
安装 Citrix Secure Access 并打开应用程序后，将显示以下屏幕。



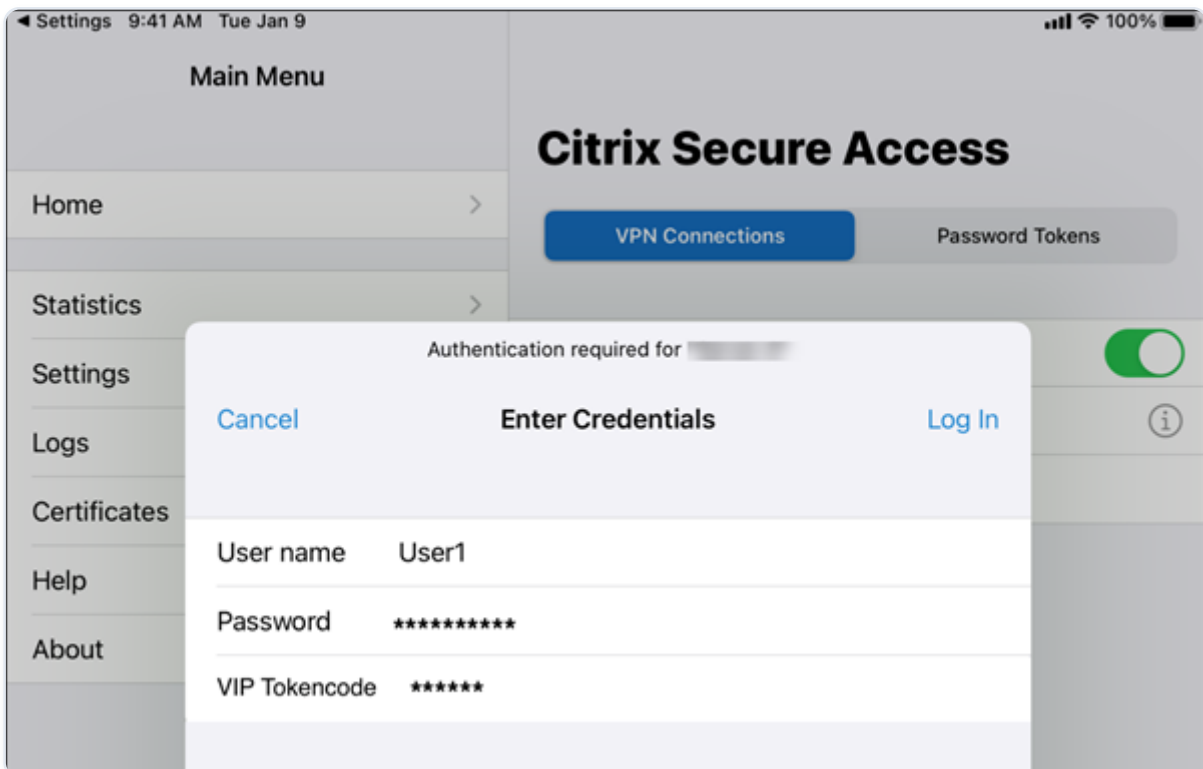
1. 点击 **添加 VPN 配置** 以添加新连接。
2. 输入服务器详细信息。

您还可以选择添加用户名。

3. 点击 **保存**，然后根据需要点击 **保存并连接** 或 **保存**。



4. 为您的服务器提供身份验证凭据，然后点击 **登录**。



注意：要从 Citrix Secure Access 注销，请关闭 VPN。

在 VPN 连接失败后重新连接到 NetScaler Gateway

当 VPN 连接丢失时，适用于 iOS 的 Citrix Secure Access 应用程序会提示您使用 NetScaler Gateway 重新进行身份验证。您会在 UI 上收到通知，告知您与 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。

删除现有连接

点击连接旁边的图标，然后点击“删除配置”。

删除现有连接(/en-us/citrix-sso/media/sso-ios-delete.png)

断开连接

将 VPN 开关切换到“关”，然后点击“断开连接”。

断开连接(/en-us/citrix-sso/media/sso-ios-disconnect.png)

查看统计信息

当 VPN 连接时，您可以查看连接统计信息。

查看统计信息(/en-us/citrix-sso/media/sso-ios-stats.png)

阻止不受信任的服务器

默认情况下，Citrix SSO 不会连接到不受信任的服务器（使用自签名证书或网关没有受信任根证书的服务器）。要允许此类连接，您可以将“阻止不受信任的服务器”开关关闭。

阻止不受信任的服务器(/en-us/citrix-sso/media/sso-ios-block.png)

本地 LAN 访问

适用于 iOS 的 Citrix SSO 23.10.1 支持本地 LAN 访问功能，您可以在 VPN 连接建立后决定是否要访问客户端设备上的本地 LAN 资源。您只有在管理员已在 NetScaler Gateway 上配置了本地 LAN 访问设置的情况下才能使用此功能。

在 Citrix Secure Access UI 上配置本地 LAN 访问：

1. 导航到主菜单并单击“设置”。
2. 启用“允许本地 LAN 访问”。

您可以在“统计信息”页面上验证本地 LAN 访问的状态。

发送日志

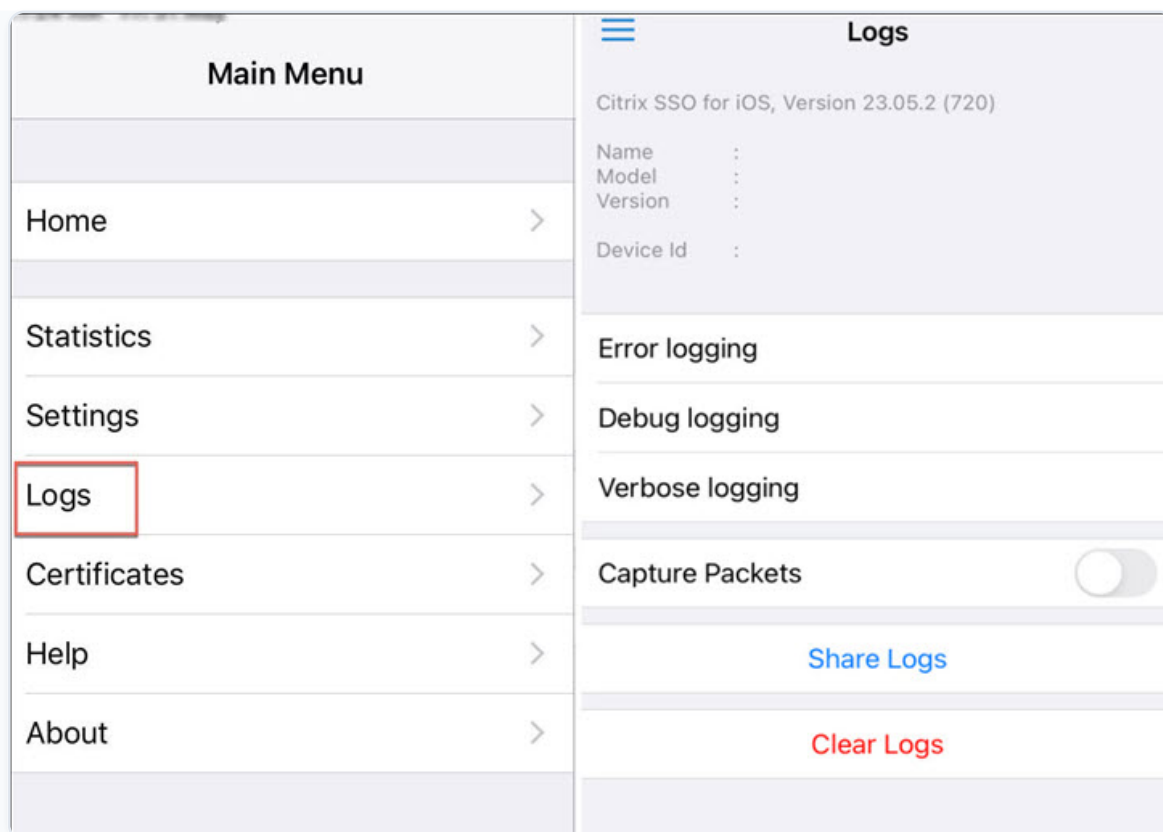
捕获调试日志是故障排除或向 Citrix 支持报告问题的关键部分。

以下是捕获和共享调试日志的步骤：

1. 将“调试日志记录”开关设置为“开”。
2. 使用电子邮件、聊天、保存到文件等选项共享日志。

注意：

- 要生成一组新日志，请首先使用“清除日志”删除旧日志。
- 从版本 23.07.1 开始，“电子邮件日志”选项已替换为“共享日志”选项。“共享日志”提供了多种共享压缩日志文件的选项。

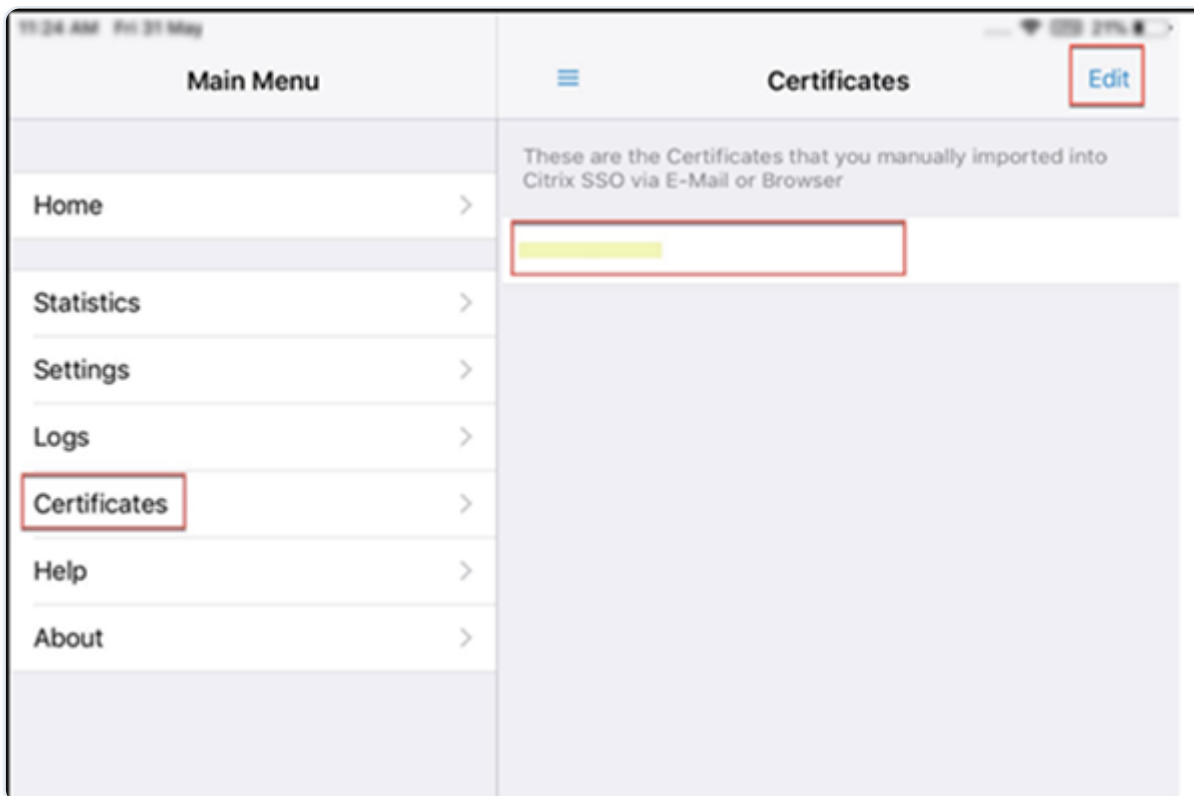


查看客户端证书

您可以查看导入到 Citrix Secure Access 中的客户端证书。导入的证书显示在“证书”部分。您可以通过以下任一方式删除证书。

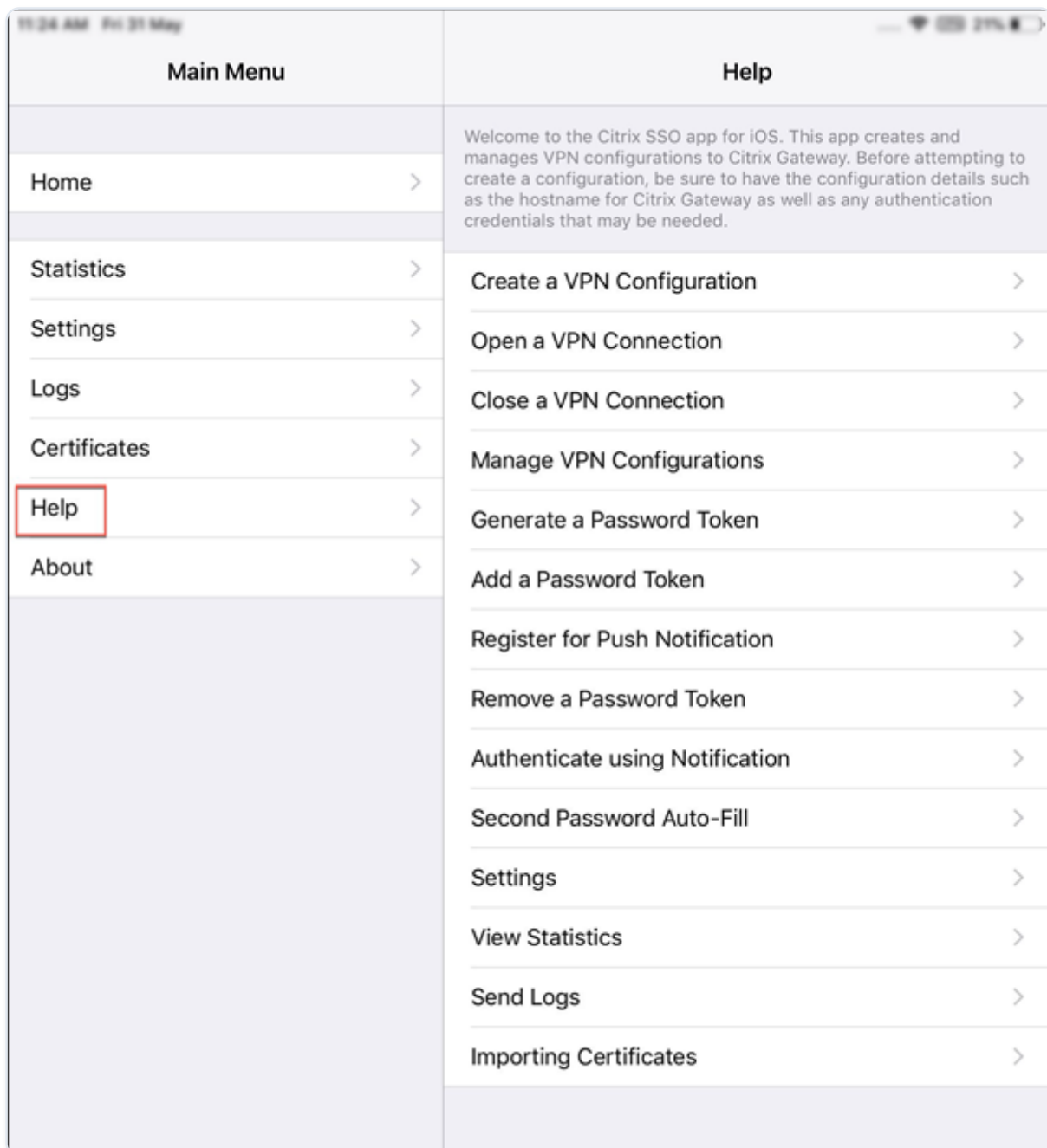
- 在证书单元格上，从右向左滑动以显示“删除”按钮。然后点击“删除”。

- 点击“编辑”以显示“删除”按钮，然后点击“删除”。



帮助主题

有关各种项目的帮助，请参阅“帮助”。



macOS 设备版 Citrix Secure Access 客户端

Citrix Secure Access 应用程序提供 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 应用程序是使用 Apple 的网络扩展框架构建的下一代 NetScaler Gateway VPN 客户端。它取代了 App Store 上的旧版 Citrix VPN 客户端。

Citrix Secure Access 应用程序在 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 配置文件和按应用程序 VPN 配置文件。

重要提示：

- Citrix Secure Access 应用程序支持零信任网络访问。除了 NetScaler Gateway URL，您还可以连接到 Workspace URL。
- 有关适用于 macOS 的 Citrix Secure Access 的管理员特定说明，请参阅 [适用于 iOS 的 Citrix SSO](#) 和 [适用于 macOS 的 Citrix Secure Access](#)。

安装适用于 macOS 的 Citrix Secure Access 客户端

从适用于 macOS 的 Citrix Secure Access 客户端 25.06.1.1 版本开始，您可以使用 [适用于 macOS 的 Citrix Secure Access](#) 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 等管理工具安装。以前，用户只能从 App Store 安装适用于 macOS 的 Citrix Secure Access 客户端。

使用 .pkg 文件在 macOS 上安装 Citrix Secure Access 应用程序

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 电脑运行的是 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。

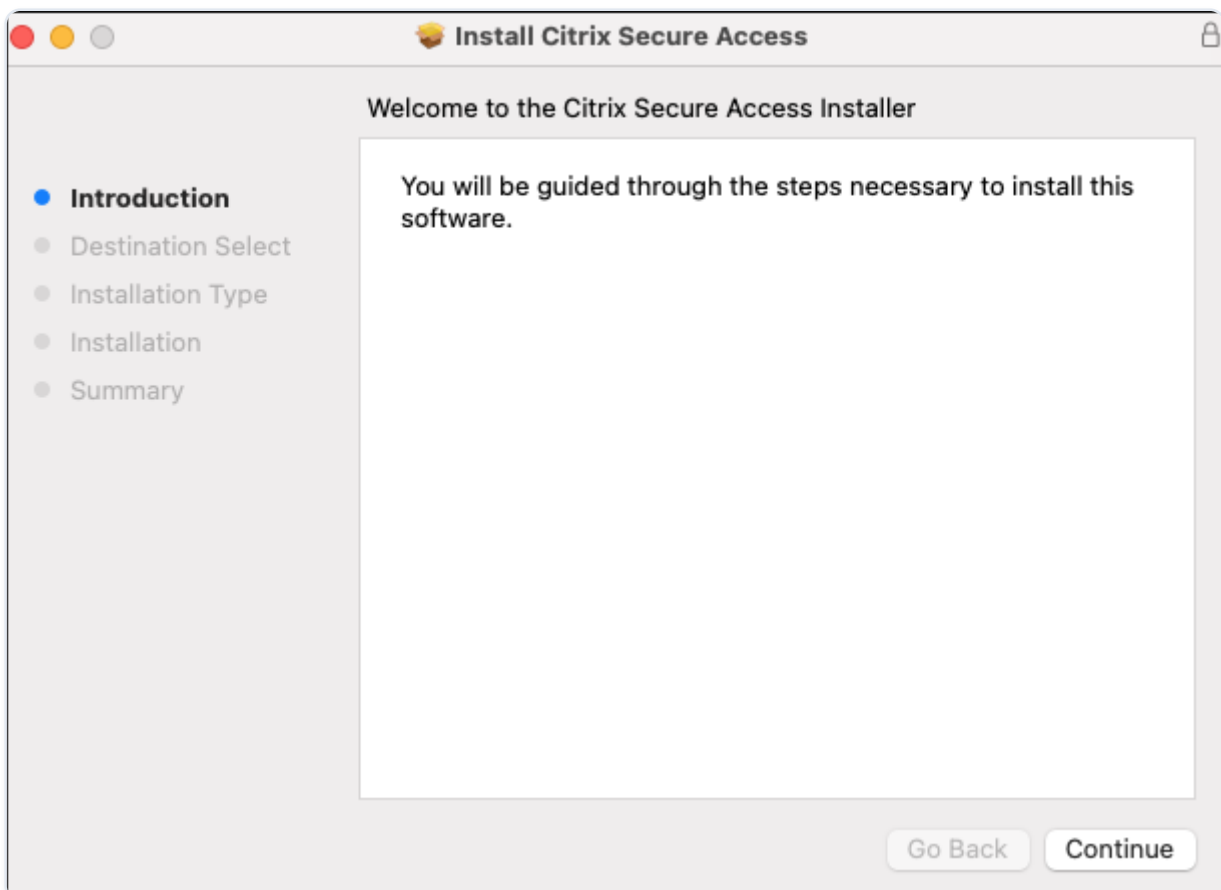
- 如果 Citrix Secure Access 应用程序当前正在运行，请退出该应用程序。
- 删除任何以前安装的 App Store 版本的 Citrix Secure Access 应用程序。

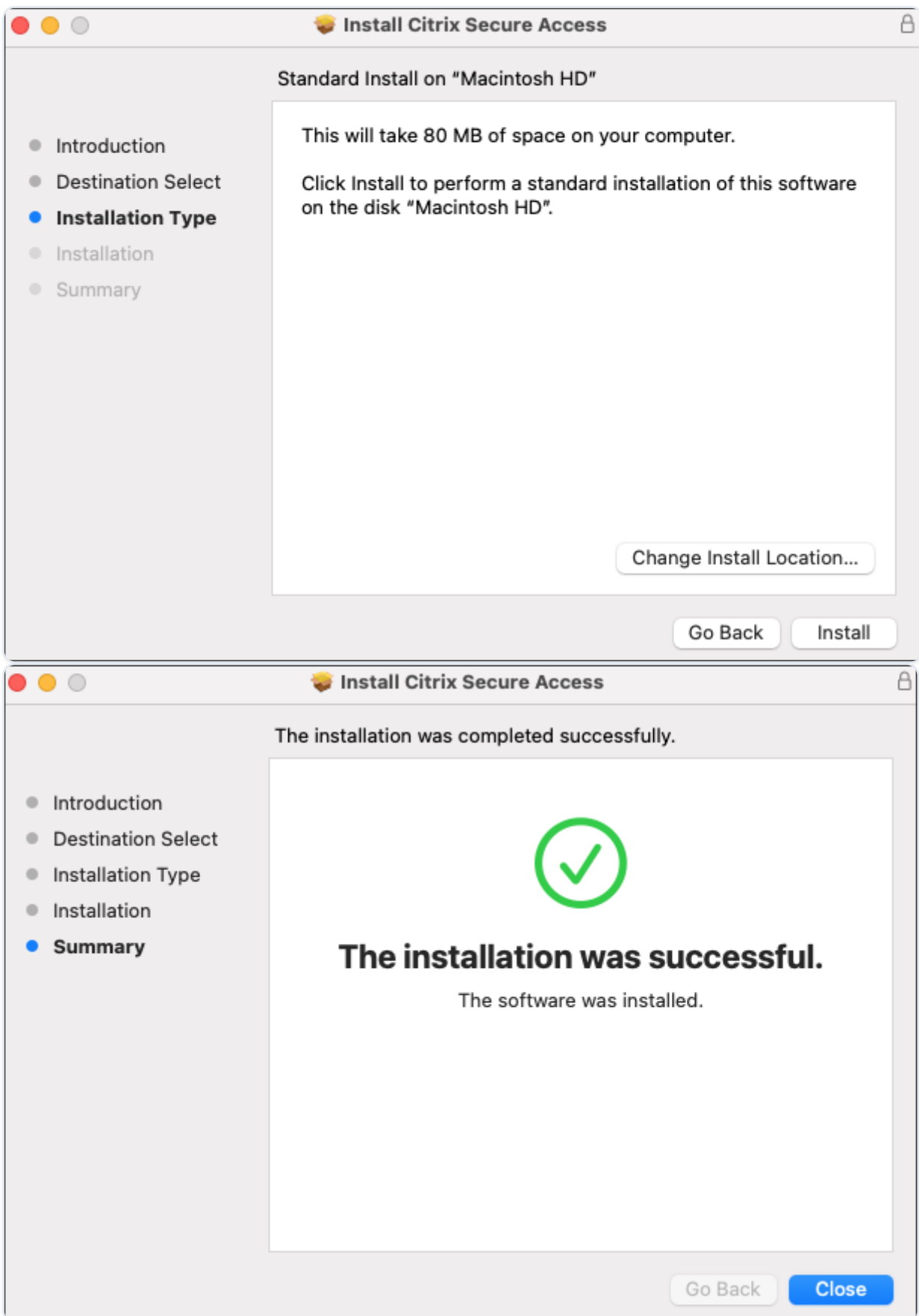
如何在 macOS 上安装 Citrix Secure Access 应用程序

重要提示：

- Citrix Secure Access 应用程序的 `.pkg` 文件使用标识符为 "com.citrix.NSG.macos.app.vpnplugin" 的系统扩展程序进行 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 系统扩展程序无法从 **登录钥匙串** 访问证书。
- 如果同一证书同时安装在 **系统钥匙串** 和 **登录钥匙串** 中，请从 **登录钥匙串** 中删除该证书及其密钥。

1. 从 [适用于 macOS 的 Citrix Secure Access](#) 下载 `.pkg` 文件。
2. 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。

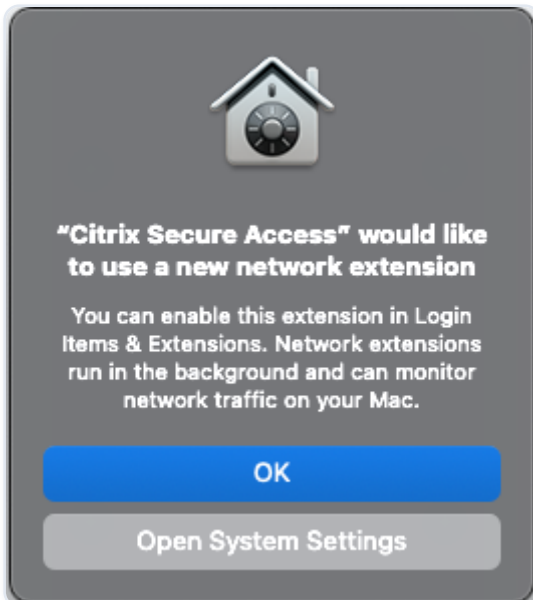




首次设置

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：

1. 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。
2. 首次启动时，系统会提示您授予安装系统扩展程序的权限。在系统提示中单击 **确定**。



如果系统提示未出现，请前往**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。

隐私与安全性(/en-us/citrix-sso/media/macos-privacy-and-security.png)

- 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。

网络扩展(/en-us/citrix-sso/media/macos-network-extensions.png)

随 Citrix Secure Access 应用程序自动安装 Endpoint Analysis™ 插件的支持

从版本 25.11.1.1 开始，Citrix Secure Access 应用程序包含 Endpoint Analysis (EPA) 插件的自动安装。EPA 插件现在默认与所有安装和更新捆绑在一起，无需单独安装，并简化了设置过程。此功能不适用于应用程序的 App Store 版本。

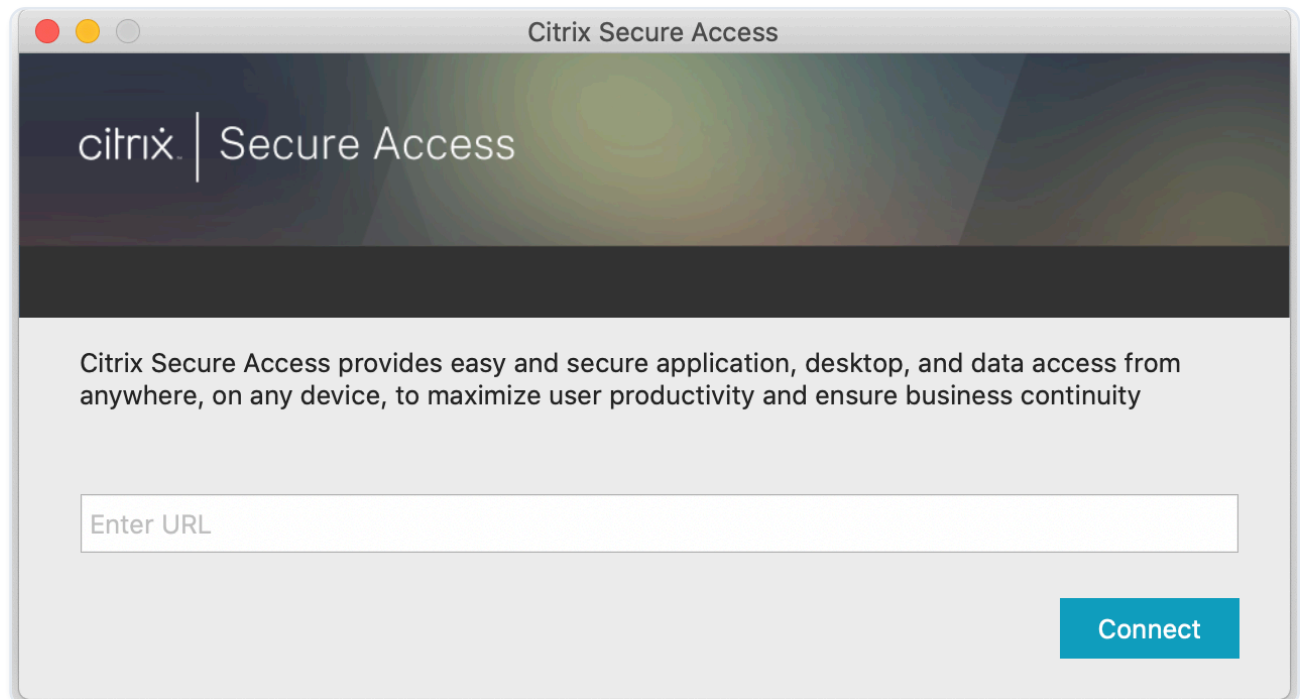
以前，用户必须在 Citrix Secure Access 应用程序登录期间手动下载并安装 EPA 插件。

如何在macOS设备上使用Citrix Secure Access应用程序

首次使用的用户必须通过添加服务器来创建与NetScaler Gateway的连接。现有用户可以连接到现有连接或添加新连接，也可以编辑现有连接。您还可以查看日志并采取相应的操作。

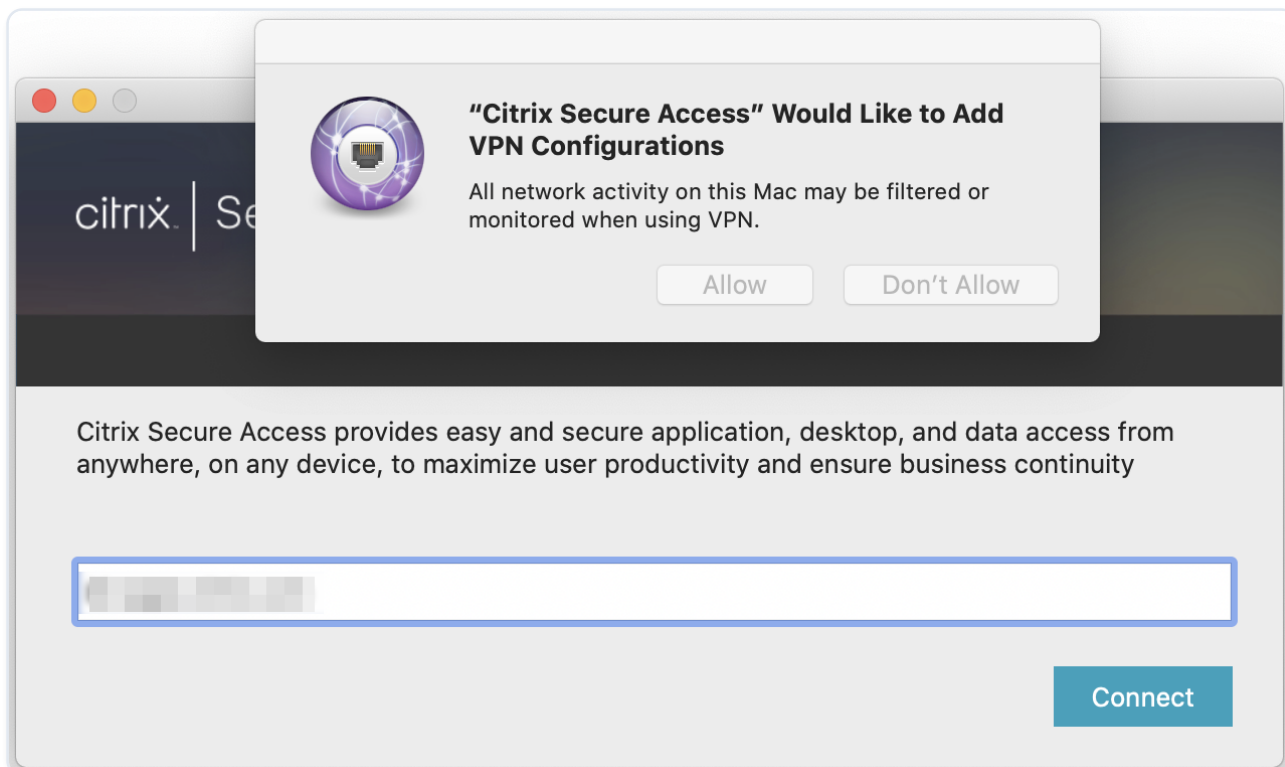
首次用户体验

首次安装并打开Citrix Secure Access应用程序后，将显示以下屏幕。

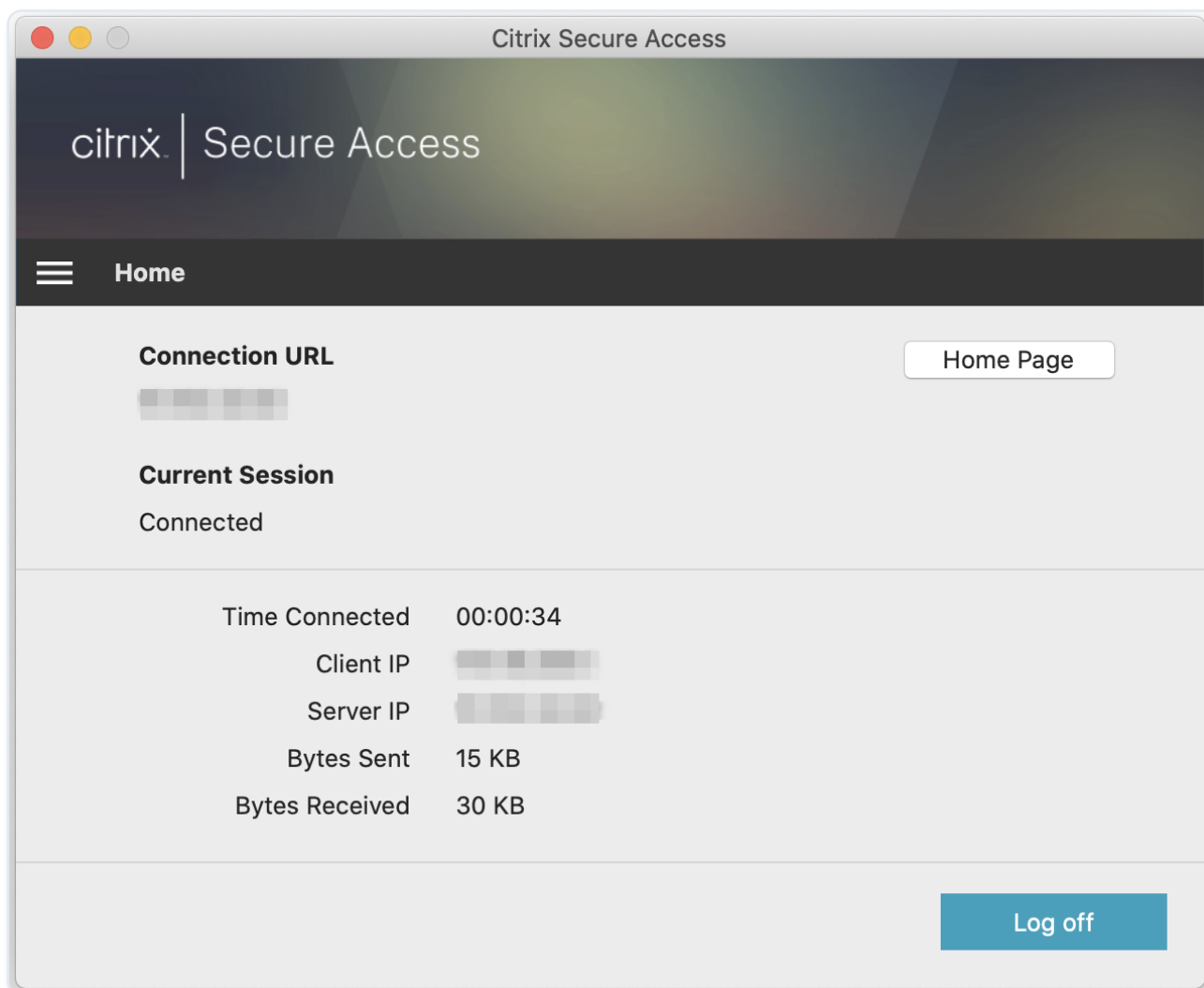


输入NetScaler Gateway基本URL或Citrix Workspace URL，然后单击**连接**。

将出现一个弹出消息。单击**允许**以后用添加连接。此消息仅在首次出现。对于后续的新连接，此消息不会出现。



注意：要从Citrix Secure Access注销，建议您首先在应用程序中单击**注销**，然后从Dock退出应用程序。请勿使用Dock中的**退出**选项。

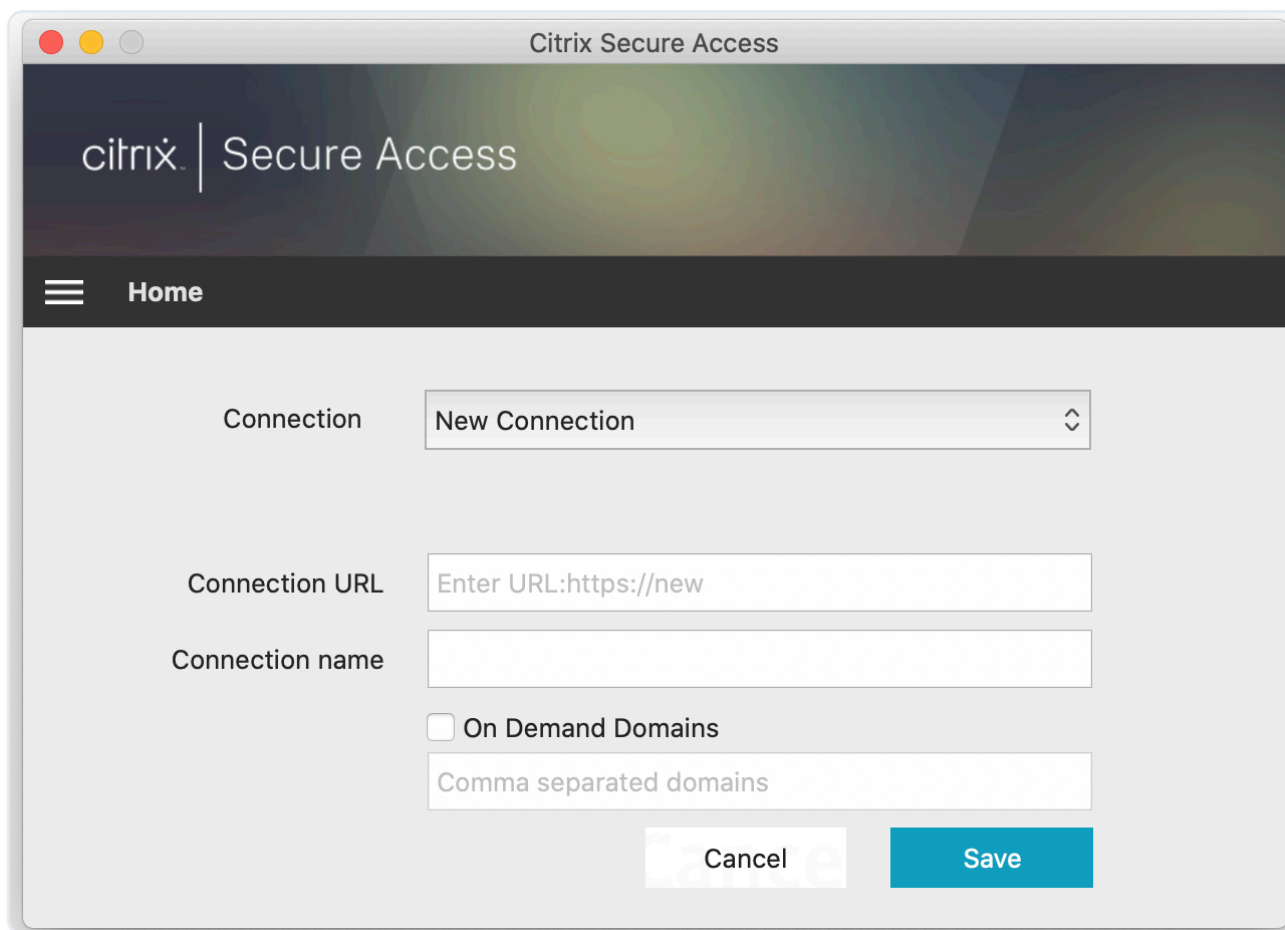


连接到NetScaler Gateway

添加第一个连接后，对于后续连接，您可以连接到现有的NetScaler Gateway或Citrix Workspace，或者添加一个连接。

添加连接

输入基本URL（例如，[我的公司 <https://gateway.mycompany.com>](https://gateway.mycompany.com)）和VPN连接的名称。

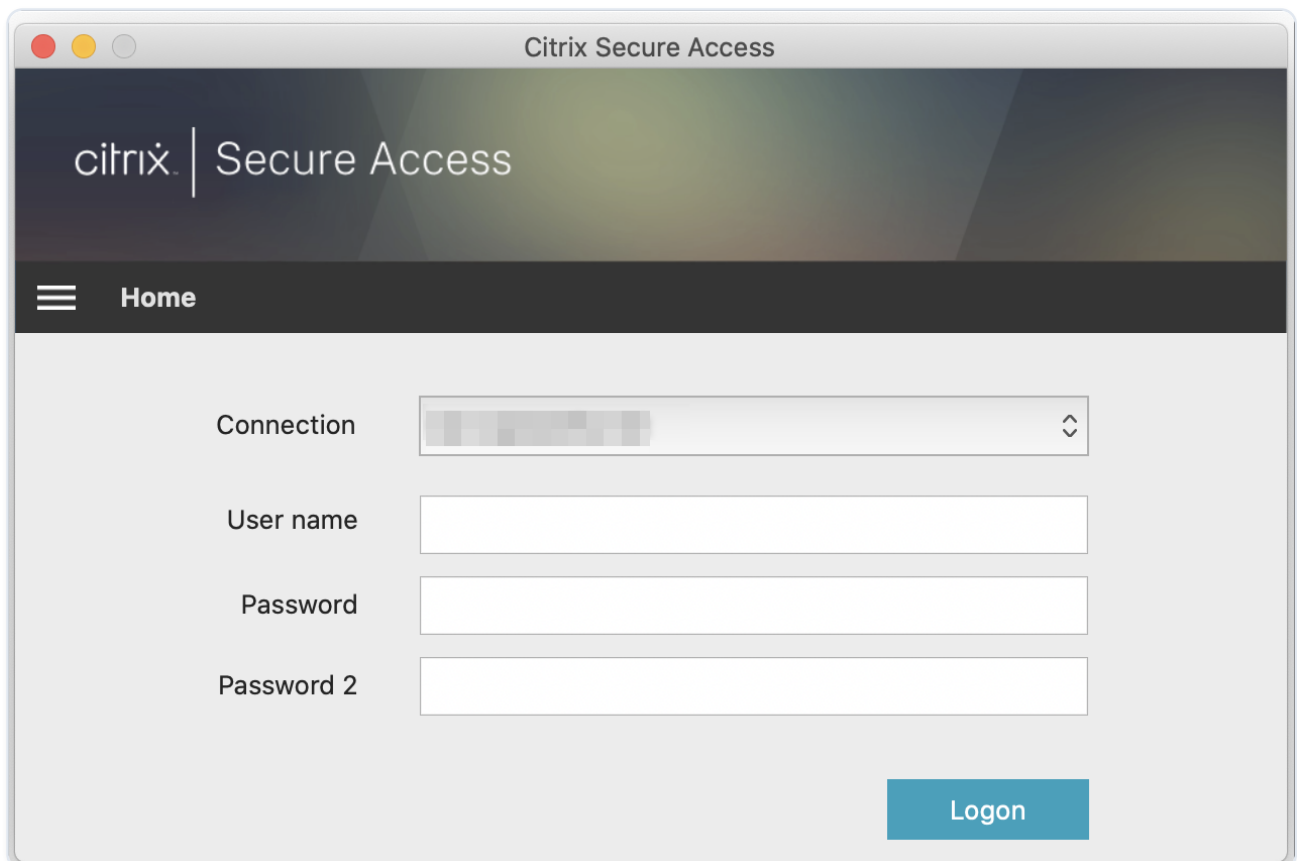


The image shows a macOS-style window titled "Citrix Secure Access". The window has a dark header bar with the Citrix logo and the text "Secure Access". Below the header is a dark navigation bar with a hamburger menu icon and the word "Home". The main content area is light gray and contains the following fields and controls:

- Connection:** A dropdown menu currently showing "New Connection".
- Connection URL:** A text input field with placeholder text "Enter URL:https://new".
- Connection name:** An empty text input field.
- On Demand Domains:** A checkbox that is currently unchecked, followed by the text "On Demand Domains".
- Comma separated domains:** A text input field with placeholder text "Comma separated domains".
- Buttons:** At the bottom right, there are two buttons: a light gray "Cancel" button and a blue "Save" button.

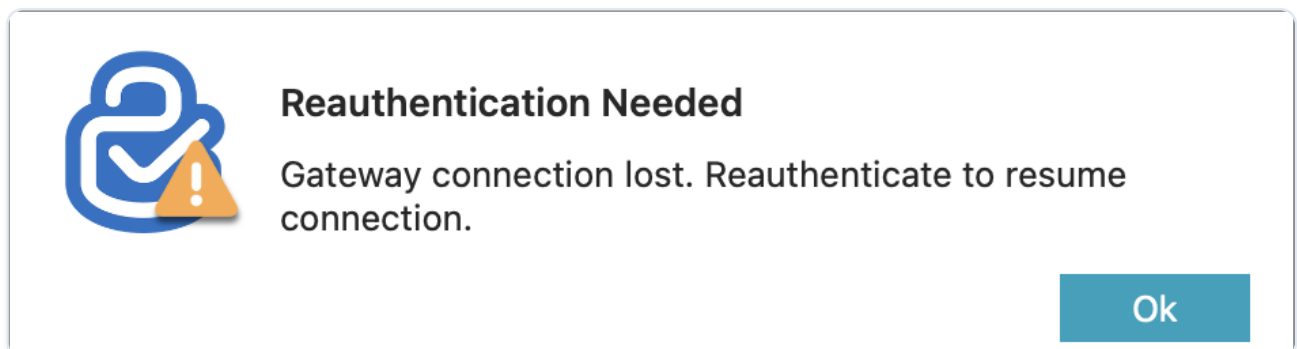
连接到现有 NetScaler Gateway

选择一个现有连接，提供服务器的身份验证凭据，然后选择 **登录**。

A screenshot of the Citrix Secure Access login window. The window has a title bar with three colored buttons (red, yellow, grey) and the text "Citrix Secure Access". The main area has a dark header with the "citrix | Secure Access" logo. Below the header is a dark bar with a hamburger menu icon and the word "Home". The main content area is light grey and contains four input fields: "Connection" (a dropdown menu), "User name" (a text box), "Password" (a text box), and "Password 2" (a text box). A blue "Logon" button is located at the bottom right of the form.

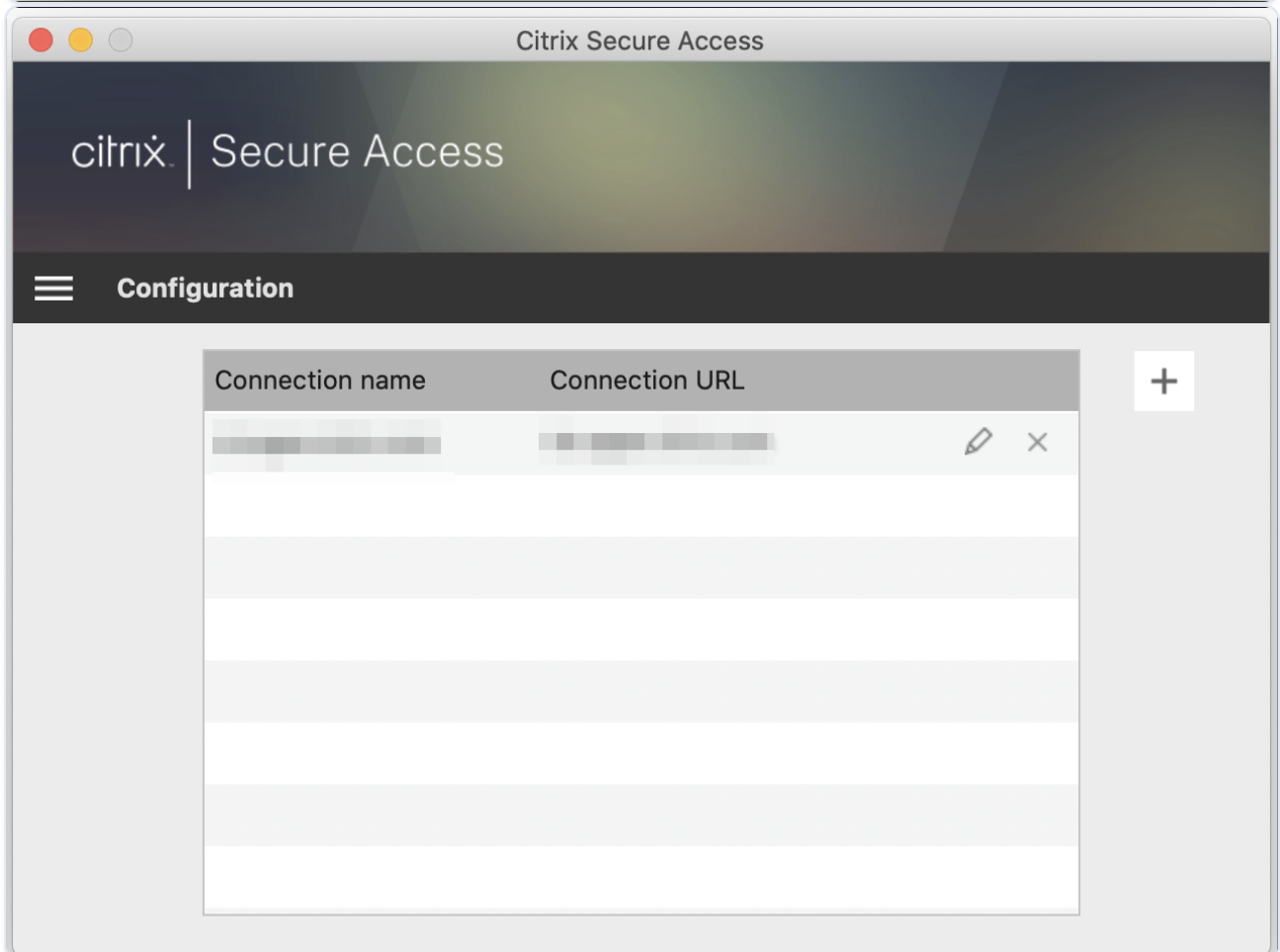
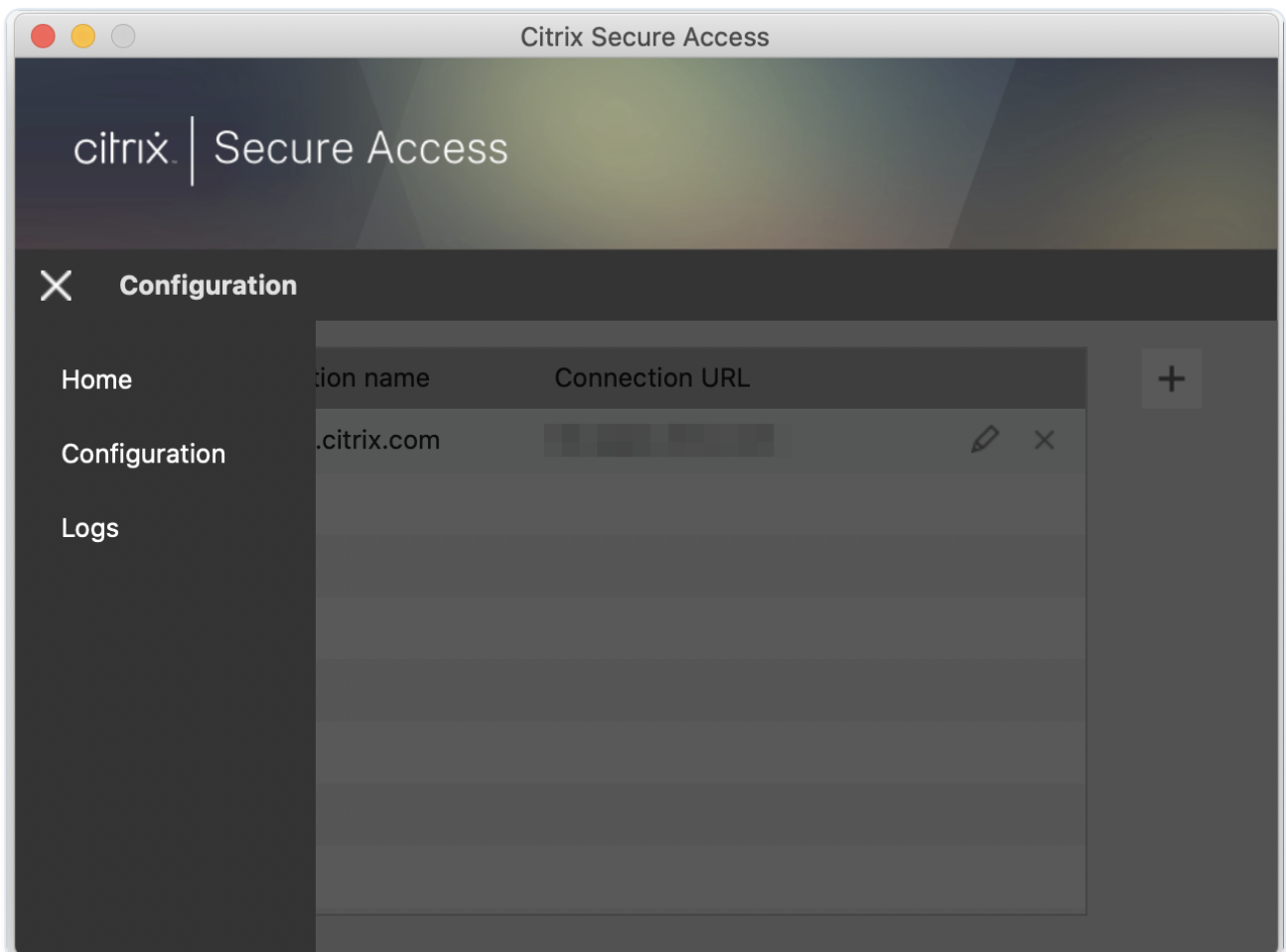
VPN 连接失败后重新连接到 NetScaler Gateway

从版本 23.09.1 开始，当 VPN 连接丢失时，适用于 macOS 的 Citrix Secure Access 客户端会提示您重新向 NetScaler Gateway 进行身份验证。Citrix Secure Access 客户端 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。

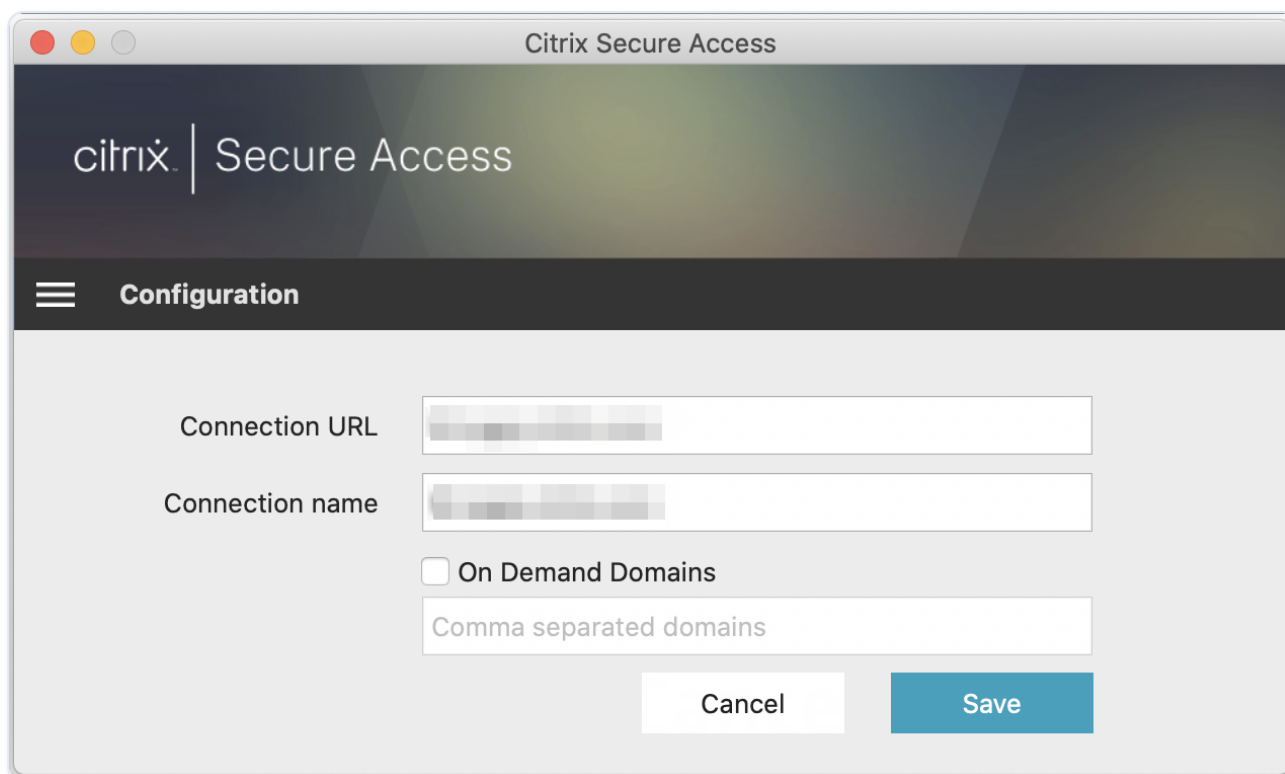


修改现有连接

您可以修改或删除现有连接。



根据需要修改连接详细信息。



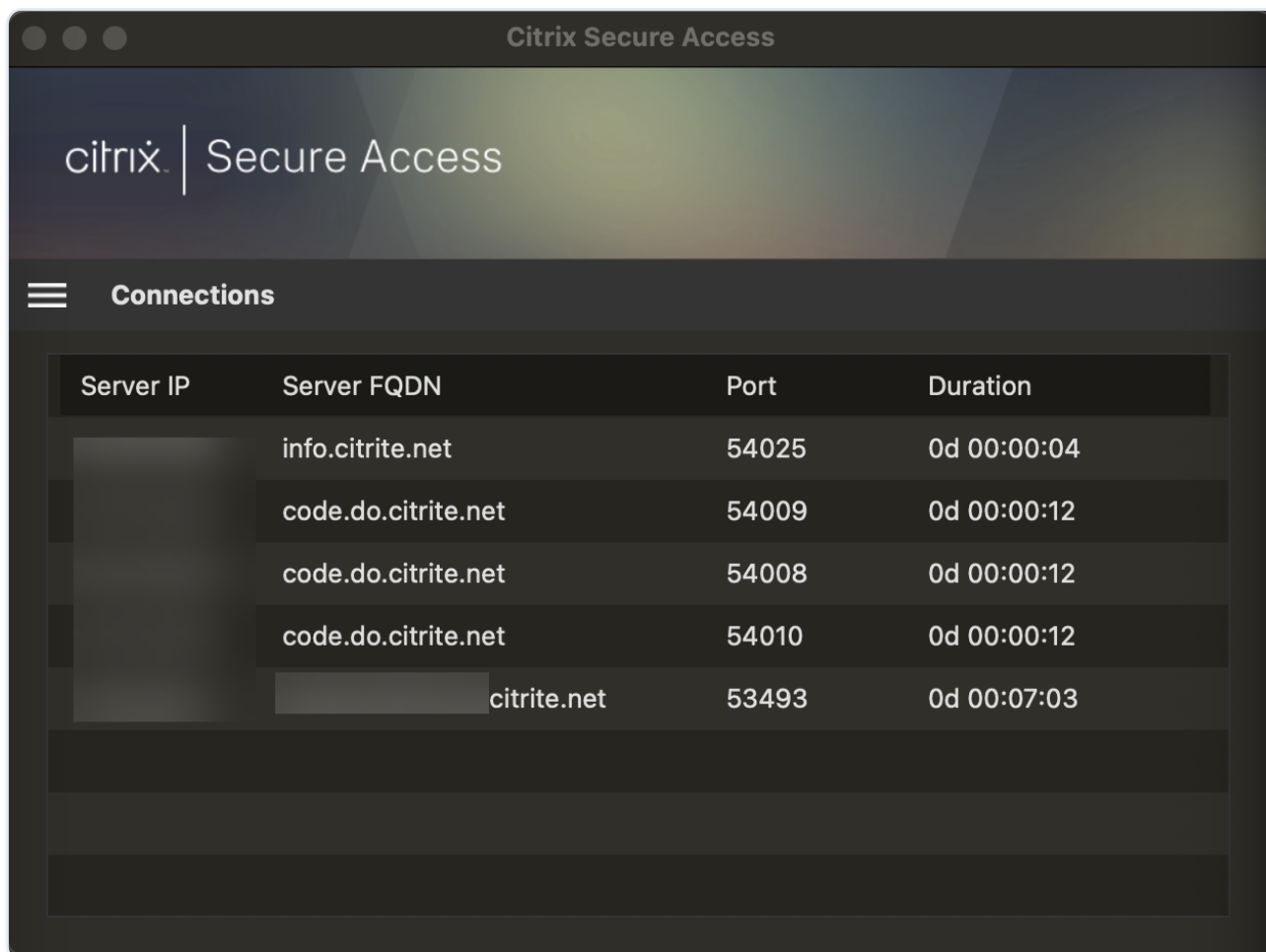
The image shows a macOS-style window titled "Citrix Secure Access". The window has a dark header bar with the Citrix logo and the text "Secure Access". Below the header is a dark bar with a hamburger menu icon and the word "Configuration". The main area is light gray and contains the following fields:

- Connection URL**: A text input field with a blurred value.
- Connection name**: A text input field with a blurred value.
- ☐ **On Demand Domains**: A checkbox that is currently unchecked.
- Comma separated domains**: A text input field with a blurred value.

At the bottom right of the window are two buttons: a white "Cancel" button and a blue "Save" button.

安全连接洞察

从版本 23.09.1 开始，您可以查看安全连接详细信息，其中包括 IP 地址、FQDN、目标端口和连接持续时间。要查看这些详细信息，请单击 UI 上的汉堡菜单并导航到 **连接**。



The screenshot shows the Citrix Secure Access interface with a table titled 'Connections'. The table has four columns: 'Server IP', 'Server FQDN', 'Port', and 'Duration'. There are five rows of data. The first four rows have a redacted 'Server IP' column, while the fifth row shows a specific IP address. The 'Server FQDN' column contains various Citrix-related domains, and the 'Duration' column shows connection times in days, hours, and minutes.

Server IP	Server FQDN	Port	Duration
	info.citrite.net	54025	0d 00:00:04
	code.do.citrite.net	54009	0d 00:00:12
	code.do.citrite.net	54008	0d 00:00:12
	code.do.citrite.net	54010	0d 00:00:12
10.10.10.10	citrite.net	53493	0d 00:07:03

本地 LAN 访问

适用于 macOS 23.10.1 的 Citrix Secure Access 客户端支持本地 LAN 访问功能，通过该功能，您可以在建立 VPN 连接后决定是否要访问客户端计算机上的本地 LAN 资源。只有当您的管理员在 NetScaler Gateway 上配置了本地 LAN 访问设置时，您才能使用此功能。

要在 Citrix Secure Access 客户端 UI 上启用本地 LAN 访问，请导航到主页并启用**允许本地 LAN 访问**复选框。

建立连接后，您可以在同一页面上验证本地 LAN 访问的状态。

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

重要提示：

此功能默认禁用。要使用此功能，请联系您的管理员。

从适用于 macOS 24.03.1 的 Citrix Secure Access 开始，登录 Citrix Workspace 应用程序可以使最终用户单点登录 (SSO) 到 Citrix Secure Access，建立用户隧道，并无缝提供对 TCP/UDP 应用程序的访问。如果您已连接到 Citrix Workspace 应用程序，则可以自动启动适用于 macOS 的 Citrix Secure Access，并且您可以使用单点登录无缝登录。

当您登录 Citrix Workspace 应用程序时，Citrix Secure Access 客户端会自动启动，并且您将单点登录到客户端。当您从 Citrix Workspace 应用程序注销时，Citrix Secure Access 会自动将您从应用程序中注销，无需您手动干预。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。

注意：

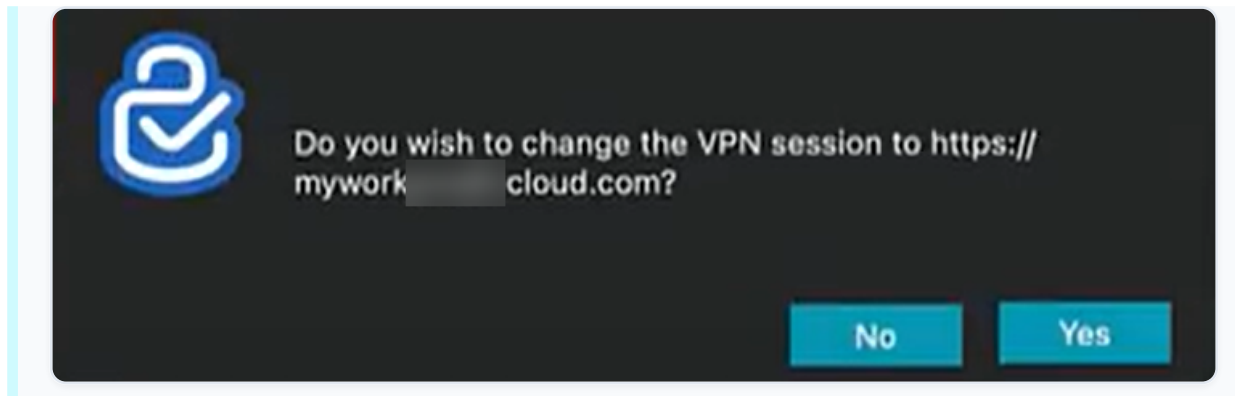
要使此功能正常工作，通过 Citrix Workspace 应用程序和 Citrix Secure Access 客户端访问的主 URL 必须相同。

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 Mac 版 Citrix Workspace 应用程序安装的详细信息，请参阅 [Mac 版 Citrix Workspace 应用程序](#)。
2. 最终用户必须使用 [适用于 macOS 24.03.1 的 Citrix Secure Access](#) 或更高版本。

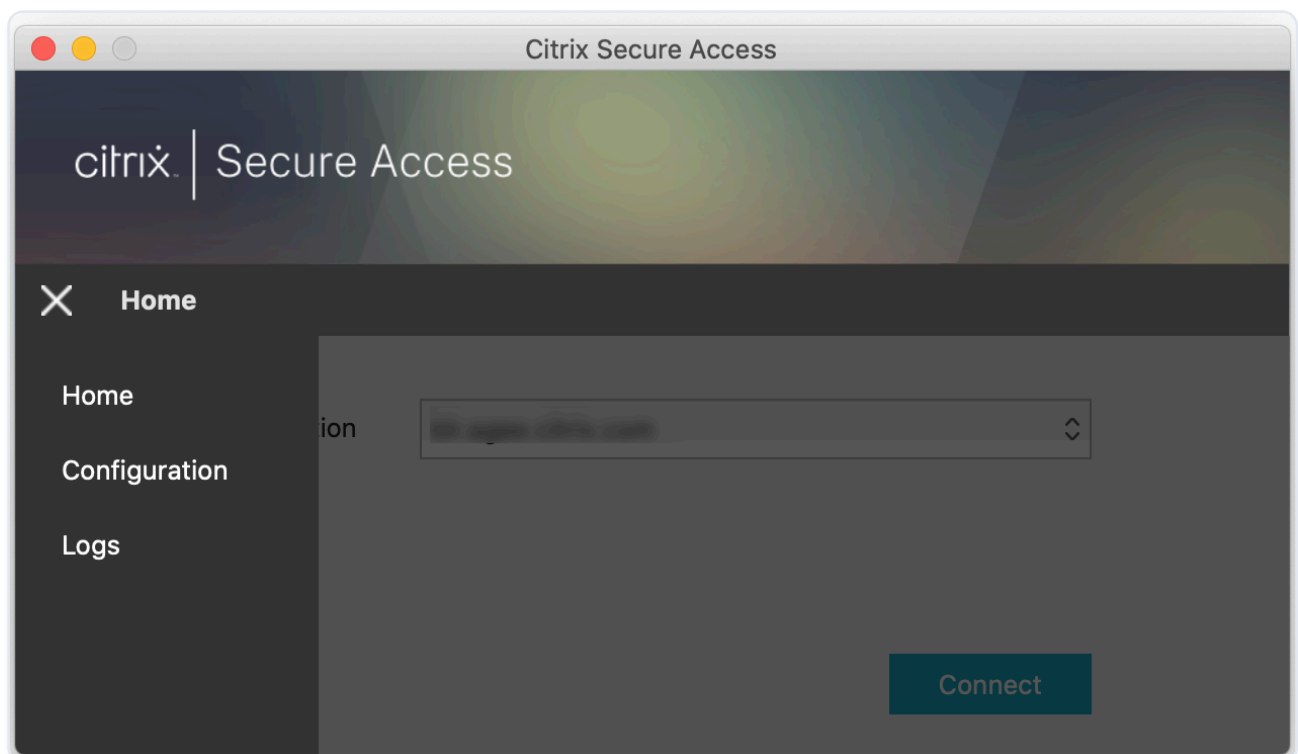
注意事项：

- 如果最终用户在使用此功能之前已登录到 Citrix Workspace 应用程序，他们必须重新登录 Citrix Workspace 应用程序，以便该应用程序可以触发对 Citrix Secure Access 客户端的单点登录。
- 当用户因超时、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（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。



发送日志

捕获调试日志是故障排除或向 Citrix 支持报告问题的关键部分。要对日志进行故障排除，请导航到主页 > 日志。



选择以下会话日志级别之一：

- **默认**：打印用于基本故障排除的最小日志。
- **调试消息**：打印所有日志。
- **详细**：打印详细日志，包括隧道消息和配置信息。

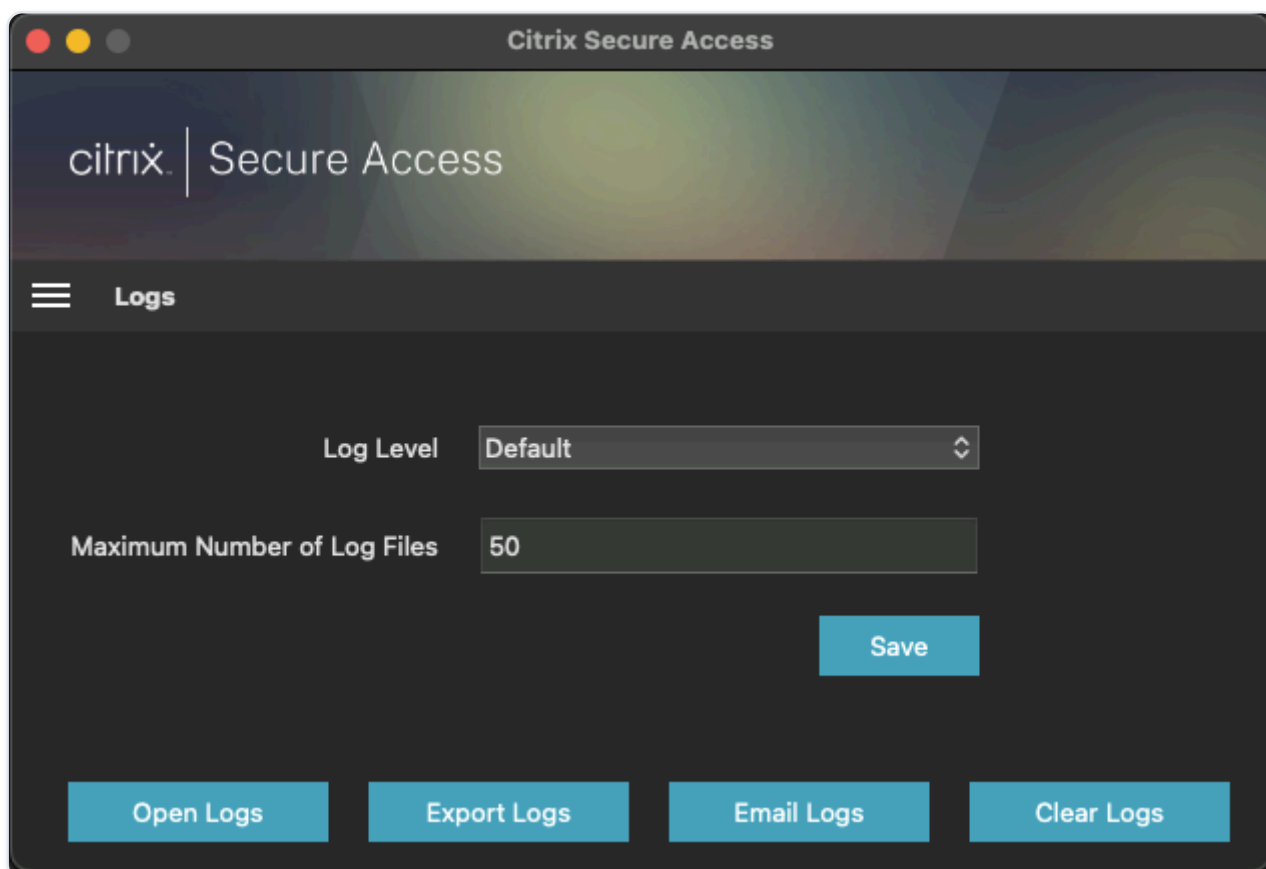
从版本 23.07.1 开始，您可以使用**最大日志文件数**字段指定要添加用于日志收集的文件数。您最多可以添加 50 个日志文件。

- 单击**打开日志**以查看日志。
- 单击**导出日志**以将日志导出到本地目录。

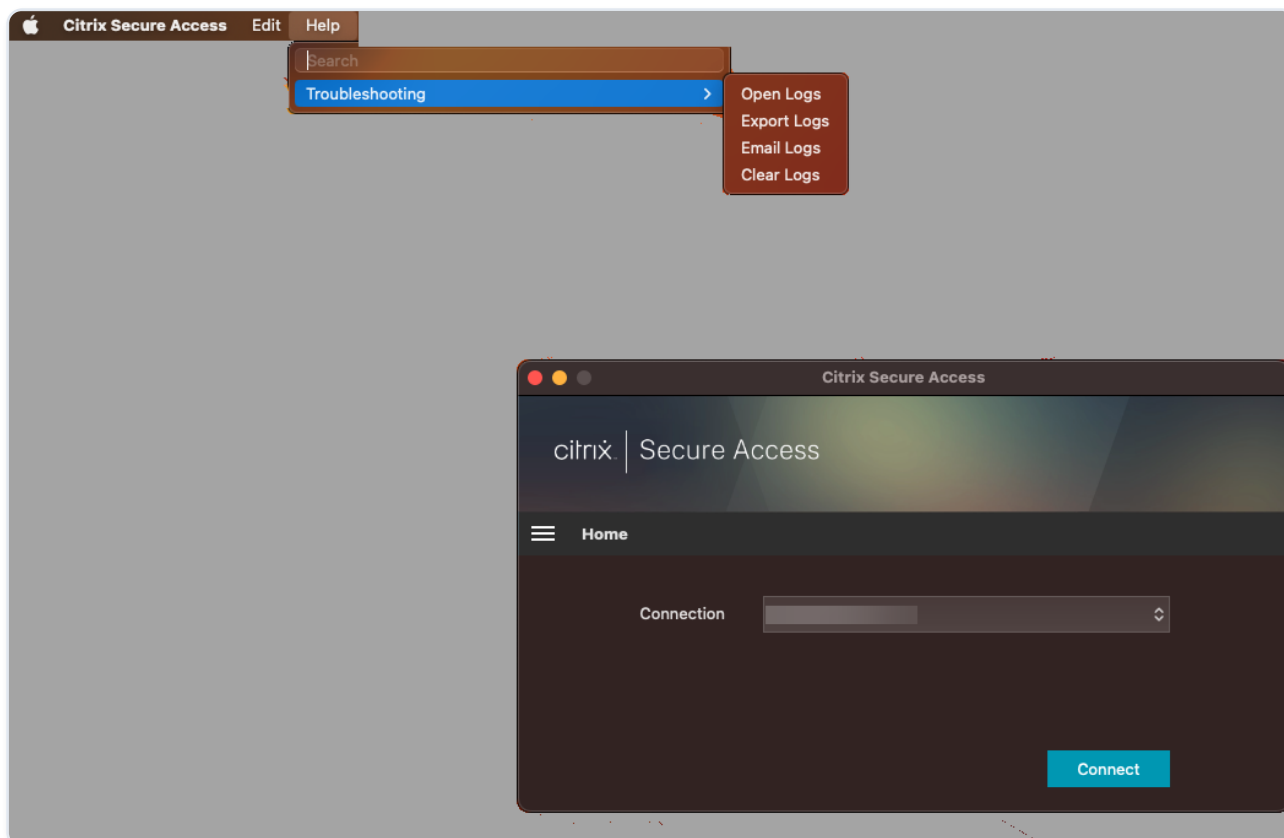
- 点击 **Email Logs** 通过电子邮件发送日志。
- 点击 **Clear Logs** 删除旧日志。

注意：

从 Citrix Secure Access for macOS 23.07.1 版本开始，**Email Logs** 选项在 **Logs** 页面上可用。



从 Citrix Secure Access for macOS 23.06.1 开始，Citrix Secure Access 客户端的导航栏上引入了帮助菜单。此菜单可用作捕获和发送调试日志的备用位置。



参考

有关 Citrix SSO for iOS 的管理员特定说明, 请参阅 [Citrix SSO for iOS](#) 和 [Citrix Secure Access for macOS](#)。

适用于 Linux 的 Citrix Secure Access 客户端

适用于 Linux 的 Citrix Secure Access 客户端是一款由 NetScaler Gateway 管理的 VPN 客户端软件，可让您远程访问企业数据和应用程序。

Citrix 端点分析 (EPA) 客户端是一款由 NetScaler Gateway 管理的客户端软件。它在通过 NetScaler Gateway 授予对企业数据的访问权限之前，会检查端点条件。Citrix EPA 客户端和 Citrix Secure Access 客户端相互独立。

只有在管理员已配置的情况下，您才能安装 Citrix EPA 客户端。有关管理员特定的说明，请参阅[适用于 Linux 的 Citrix Secure Access 客户端](#)。

重要更新：

我们正在将用户界面和产品文档更新为新的 NetScaler 品牌。在此过渡期间，您可能会看到 Citrix 和 NetScaler 引用互换使用。

安装 Citrix Secure Access 客户端和 Citrix EPA 客户端

注意：

- 从软件中心安装 Citrix Secure Access 客户端和 Citrix EPA 客户端时，如果现有版本不是最新版本，则必须先将其卸载，然后才能升级到最新版本。这是必要的，因为与 Ubuntu 18.04 不同，当前版本无法直接替换为最新版本。
- 在 Ubuntu 20.x 上，如果您从 Firefox 浏览器下载 Citrix Secure Access 客户端，然后使用“**打开方式**”选项打开它，则安装可能会失败。这是因为 Firefox 将客户端下载到临时位置，并且 Citrix Secure Access 客户端无法从该位置进行安装。

作为一种解决方法，我们建议您选择“**保存文件**”选项。此选项会将 Citrix Secure Access 客户端下载到“**下载**”文件夹中。然后，您可以双击下载的文件并安装 Citrix Secure Access 客户端。

- 在 eLux 和 IGEL OS 等精简 Linux 客户端中，Citrix Secure Access 客户端和 Citrix EPA 客户端由管理员管理。用户无法直接安装 Citrix Secure Access 客户端和 Citrix EPA 客户端。

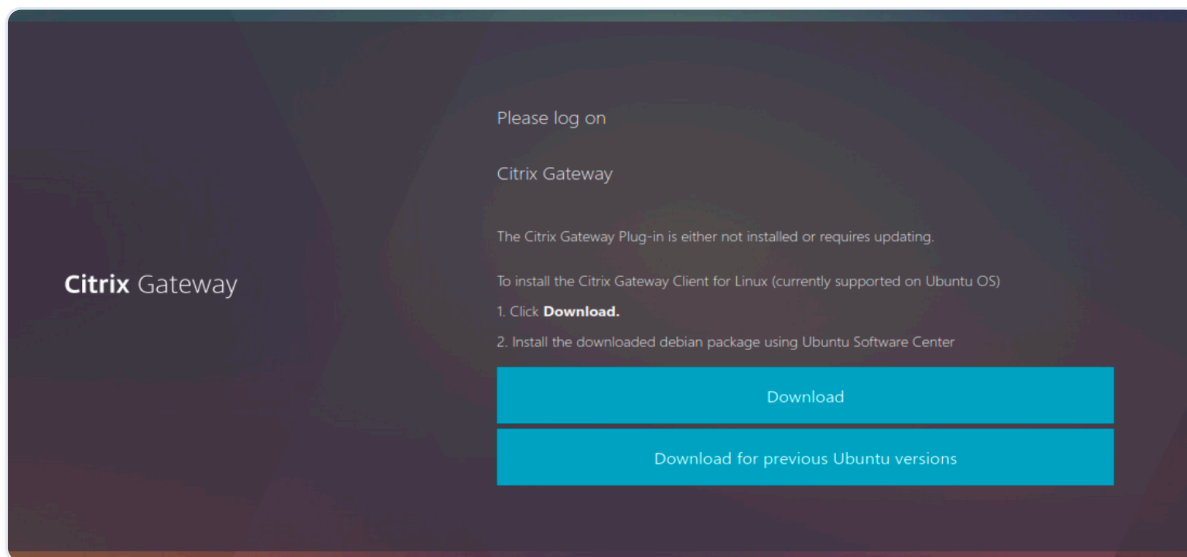
安装适用于 Ubuntu 20.04 的 Citrix Secure Access 客户端和 Citrix EPA 客户端

您可以使用以下说明安装 Citrix Secure Access 客户端和 Citrix EPA 客户端：

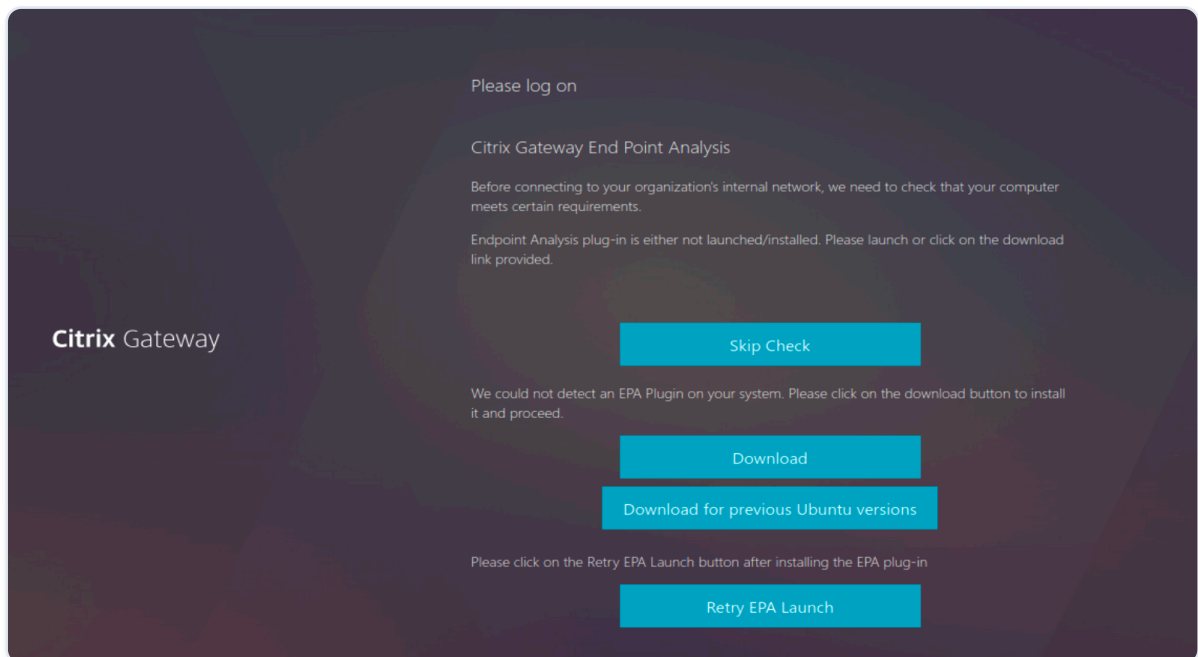
1. 下载 Citrix Secure Access 客户端和 Citrix EPA 客户端，方法如下：

- **选项 1：** 打开 Web 浏览器并输入管理员提供的 NetScaler Gateway URL。在几秒钟后出现的下载屏幕上，单击“**下载适用于以前的 Ubuntu 版本**”按钮。

Citrix Secure Access 客户端下载将显示以下屏幕：



Citrix EPA 客户端下载将显示以下屏幕：



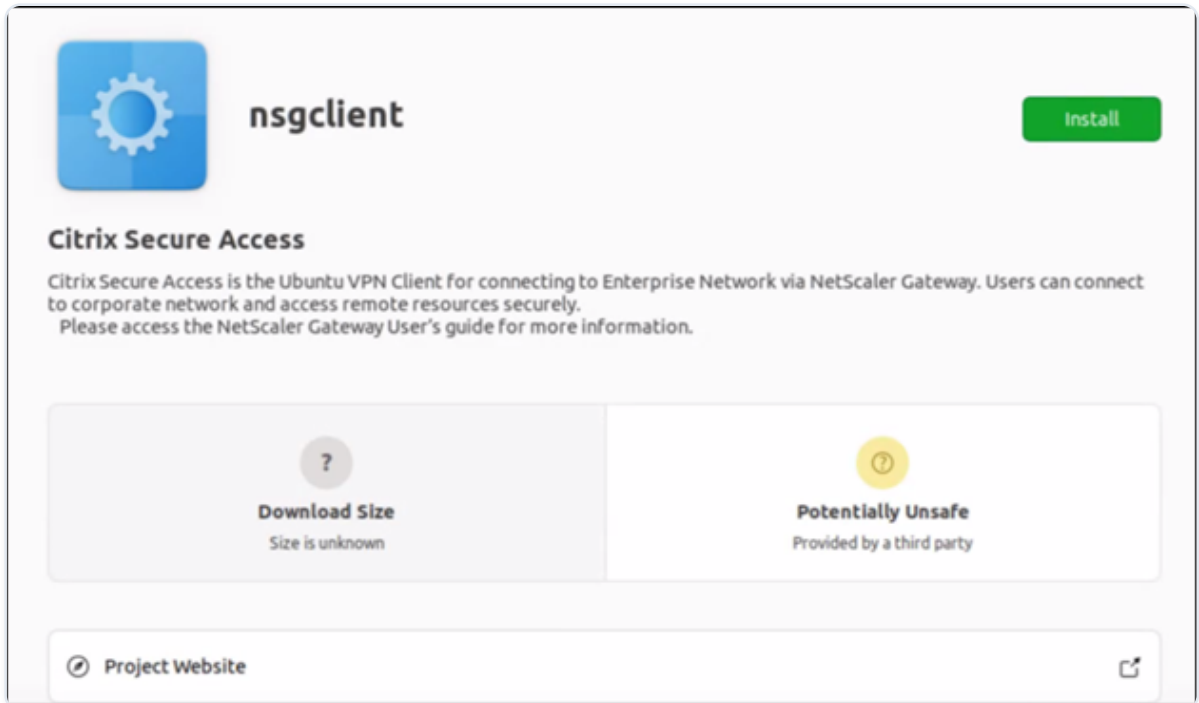
- **选项 2：** 转到 适用于 Ubuntu 的 Citrix Secure Access 客户端，然后单击 Ubuntu 20 部分下方的“下载”按钮以下载 Citrix Secure Access 客户端和 Citrix EPA 客户端。

Citrix EPA client 25.5.3 for Ubuntu 20 May 19, 2025 9.9 M - (.deb) Download File Checksums SHA-256 - eb4feda271c9be8e4392b5a8ec733565ae29b5ce4bf32c338352757554824138
Citrix EPA client 25.5.3 for Ubuntu 22/24 May 19, 2025 9.9 M - (.deb) Download File Checksums SHA-256 - 460081aaae9d4625e27a07fcdcdb3646c8ff791d88da1a07200315954bdb7f40
Citrix Secure Access client 25.5.3 for Ubuntu 20 May 19, 2025 4.9 M - (.deb) Download File Checksums SHA-256 - c802dc70e762245150a2741816a4b9b299fb8762ace8f56868ba2f66ae2b1b10
Citrix Secure Access client 25.5.3 for Ubuntu 22/24 May 19, 2025 4.9 M - (.deb) Download File Checksums SHA-256 - 66458c71b6ff6039686939954519c57fdb745b13707473ded9c00de996318766

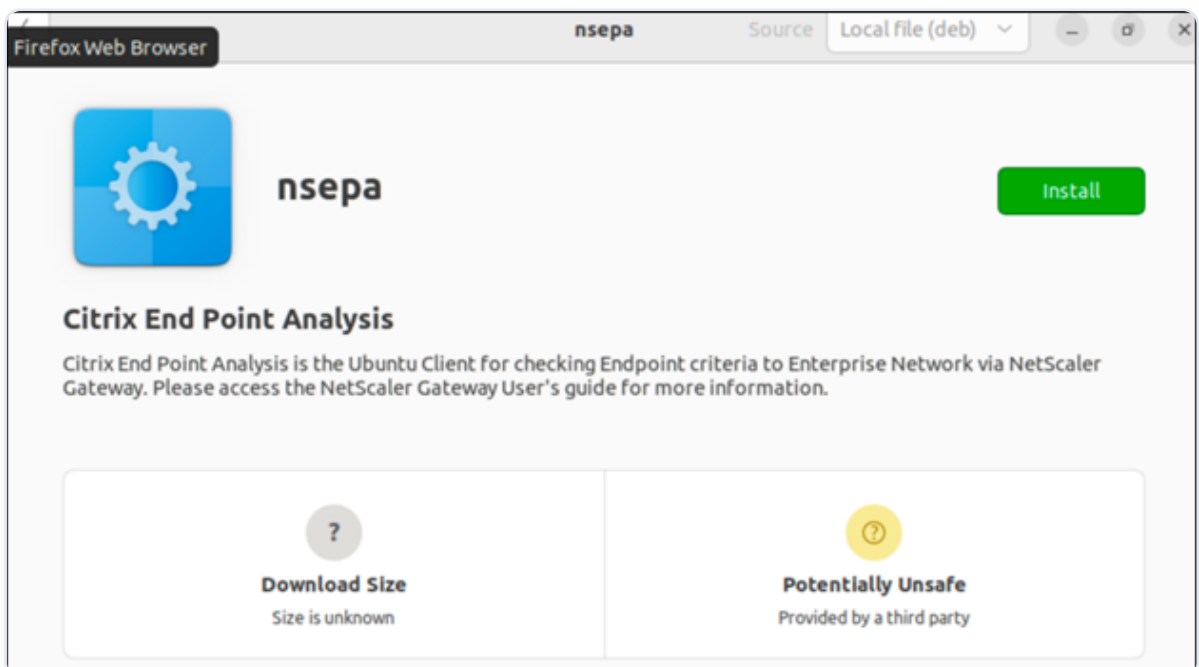
2. 从 GUI 或使用 Ubuntu 终端安装 Citrix Secure Access 客户端和 Citrix EPA 客户端。

- 双击下载的文件，然后安装 Citrix Secure Access 客户端和 Citrix EPA 客户端。

双击下载的 Citrix Secure Access 客户端后，将显示以下屏幕：

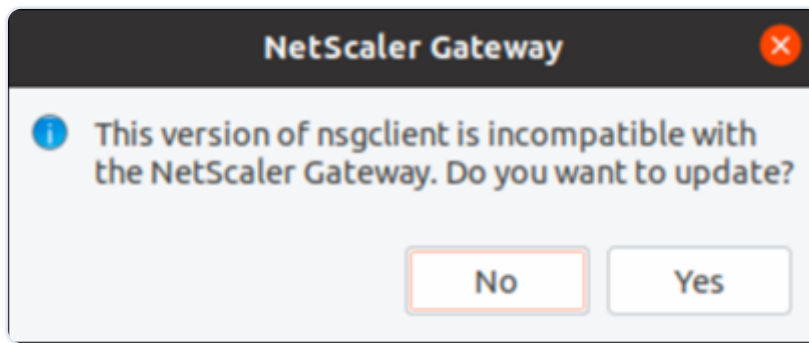


双击下载的 Citrix EPA 客户端后，将显示以下屏幕：



如果 Citrix Secure Access 客户端已安装但未升级，系统会提示您升级到最新版本。单击 **Yes** 升级到最新版本，如以下屏幕所示：

此升级不适用于 Citrix EPA 客户端。



- 使用 Ubuntu 终端安装 Citrix Secure Access 客户端和 Citrix EPA 客户端。

要在终端中安装 Citrix Secure Access 客户端，请键入：

```
sudo apt install ./nsgclient18_64.deb  
  
sudo apt install -f
```

要在终端中安装 Citrix EPA 客户端，请键入：

```
sudo apt install ./nsepa18.deb  
  
sudo apt install -f
```

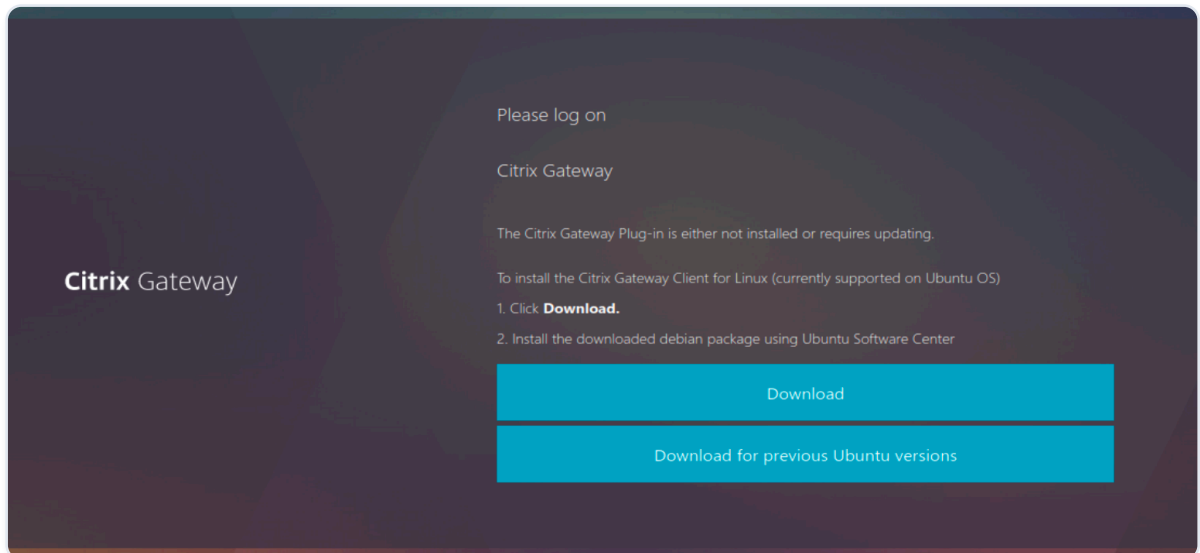
为 Ubuntu 22.04 及更高版本安装 Citrix Secure Access 客户端和 Citrix EPA 客户端

您可以使用以下说明安装 Citrix Secure Access 客户端和 Citrix EPA 客户端：

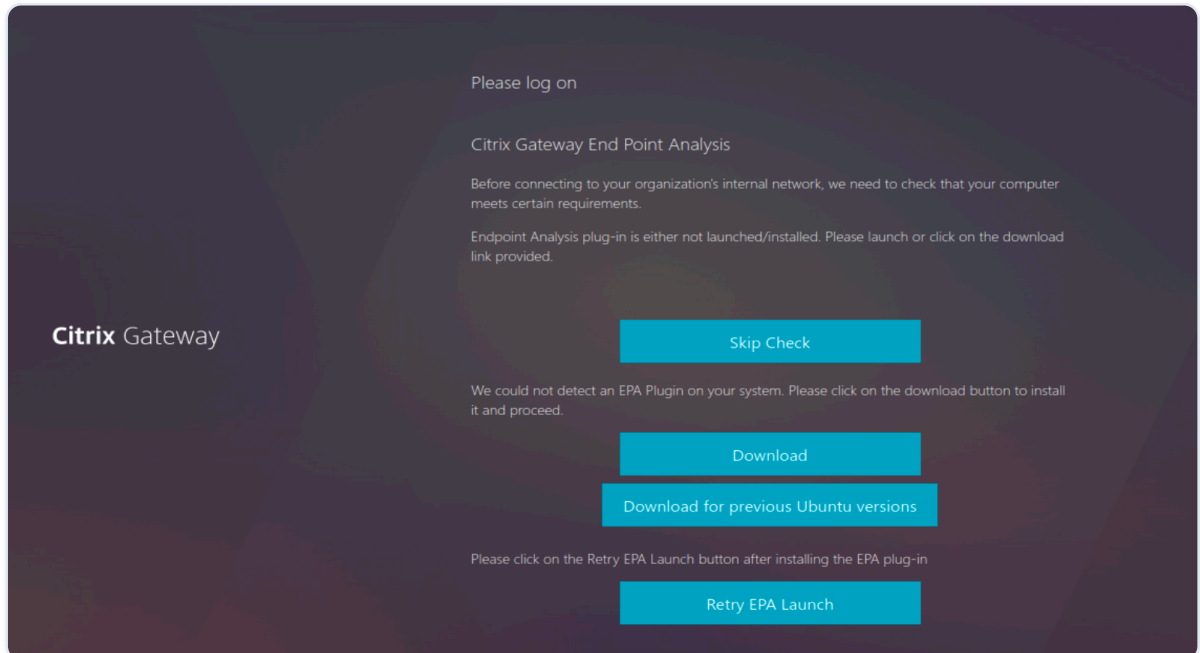
1. 使用以下任一选项下载 Citrix Secure Access 客户端和 Citrix EPA 客户端：

- **选项 1：** 打开 Web 浏览器并输入管理员提供的 NetScaler Gateway URL。点击几秒钟后出现的下载屏幕上的“下载”按钮

Citrix Secure Access 客户端下载将显示以下屏幕：



Citrix EPA 客户端下载将显示以下屏幕：



- **选项 2：** 转到 [适用于 Ubuntu 的 Citrix Secure Access 客户端](#) 并点击 Ubuntu 22/24 部分下方的“**下载**”按钮，以下载 Citrix Secure Access 客户端和 Citrix EPA 客户端。

Citrix EPA client 25.5.3 for Ubuntu 20

May 19, 2025
9.9 M - (.deb) [Download File](#)

Checksums
SHA-256 - eb4feda271c9be8e4392b5a8ec733565ae29b5ce4bf32c338352757554824138

Citrix EPA client 25.5.3 for Ubuntu 22/24

May 19, 2025
9.9 M - (.deb) [Download File](#)

Checksums
SHA-256 - 460081aaae9d4625e27a07fcdcdb3646c8ff791d88da1a07200315954bdb7f40

Citrix Secure Access client 25.5.3 for Ubuntu 20

May 19, 2025
4.9 M - (.deb) [Download File](#)

Checksums
SHA-256 - c802dc70e762245150a2741816a4b9b299fb8762ace8f56868ba2f66ae2b1b10

Citrix Secure Access client 25.5.3 for Ubuntu 22/24

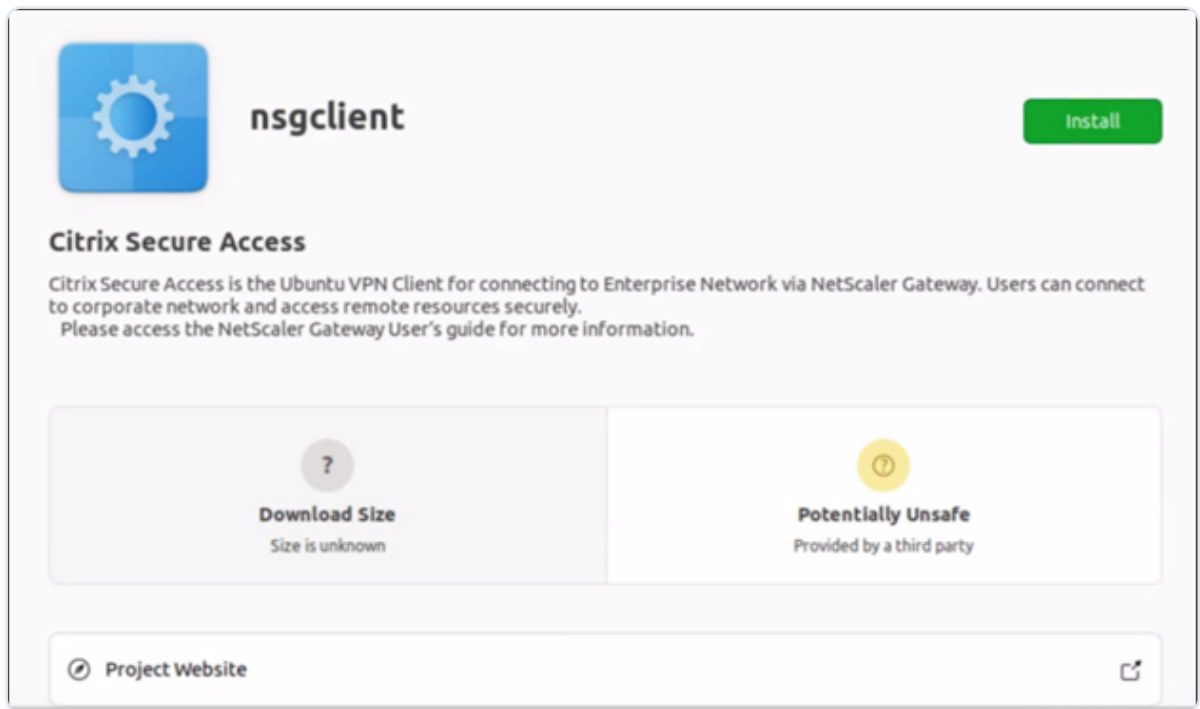
May 19, 2025
4.9 M - (.deb) [Download File](#)

Checksums
SHA-256 - 66458c71b6ff6039686939954519c57fdb745b13707473ded9c00de996318766

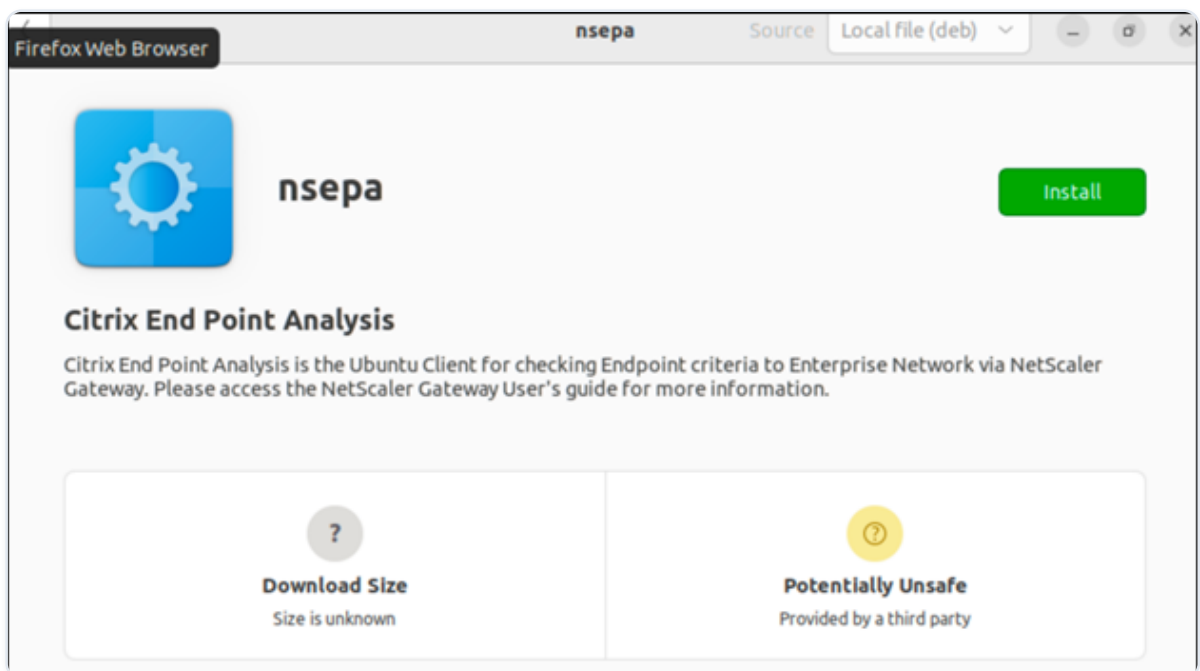
2. 通过 GUI 或使用 Ubuntu 终端安装 Citrix Secure Access 客户端和 Citrix EPA 客户端。

- 双击下载的文件并安装 Citrix Secure Access 客户端和 Citrix EPA 客户端。

双击下载的 Citrix Secure Access 客户端时，将显示以下屏幕：

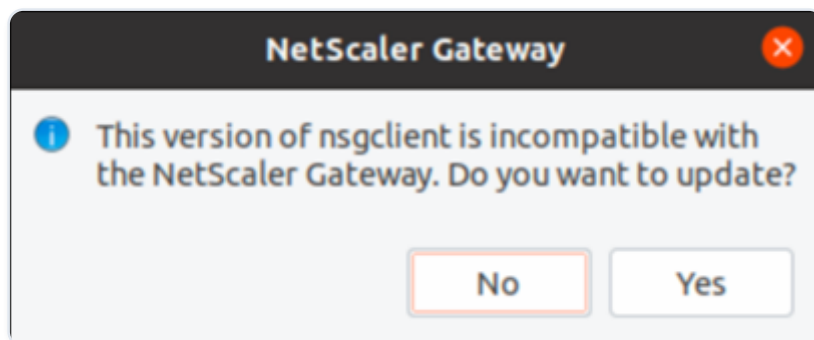


双击下载的 Citrix EPA 客户端时，将显示以下屏幕：



如果 Citrix Secure Access 客户端已安装但未升级，系统会提示您升级到最新版本。点击“是”以升级到最新版本，如以下屏幕所示：

此升级不适用于 Citrix EPA 客户端。



- 使用 Ubuntu 终端安装 Citrix Secure Access 客户端和 Citrix EPA 客户端。

要在终端中安装 Citrix Secure Access 客户端，请键入：

```
sudo apt install ./nsginstaller64.deb

sudo apt install -f
```

要在终端中安装 Citrix EPA 客户端，请键入：

```
sudo apt install ./nsepa.deb

sudo apt install -f
```

如何在 Linux 上使用 Citrix Secure Access 客户端

在浏览器中输入 NetScaler Gateway URL 以使用 Citrix Secure Access 客户端进行身份验证。身份验证成功后，浏览器会提示您启动 Citrix Secure Access 客户端。

- 在任务栏上选择 Citrix Secure Access 客户端图标，然后单击**设置**。

Citrix Secure Access 客户端设置(/en-us/citrix-ssso/media/secure-access-client-settings.png)

- **连接**选项卡显示连接状态、用户信息、隧道连接和数据使用情况等详细信息。

Citrix Secure Access 客户端连接设置(/en-us/citrix-ssso/media/secure-access-client-connections.png)

- **配置**选项卡显示 NetScaler Gateway 信息、上传客户端证书的选项以及日志记录选项。

Citrix Secure Access 客户端配置(/en-us/citrix-ssso/media/secure-access-client-configuration.png)

- 证书：导航到此部分以配置客户端证书。仅当您的管理员已向您提供客户端证书以通过 NetScaler Gateway 进行身份验证时，才需要执行此步骤。

Citrix Secure Access 客户端证书(/en-us/citrix-sso/media/secure-access-client-certificate.png)

- 日志记录：导航到此部分以捕获调试日志。捕获调试日志是故障排除或向 Citrix 支持报告问题的关键部分。

Citrix Secure Access 客户端日志记录(/en-us/citrix-sso/media/client-logging.png)

或者，您可以启动 Citrix Secure Access 客户端并单击**登录**。如果您是首次使用，系统会提示您提供 NetScaler Gateway URL 或您的工作区 URL。

Citrix Secure Access 客户端启动(/en-us/citrix-sso/media/linux-client-logon.png)

发送日志

您发送给管理员的日志文件格式为 `nsgcepa.txt`、`nsepa.txt`、`nssslvpn.txt` 和 `epalibv2.log`。这些文件位于 `~/.citrix/` 目录中。它们捕获以下详细信息：

- **信息**：打印基本日志和错误日志。
- **调试**：打印所有日志。我们建议您选择此选项以收集日志并与管理员共享。
- **详细**：打印详细日志，包括隧道消息和配置信息。

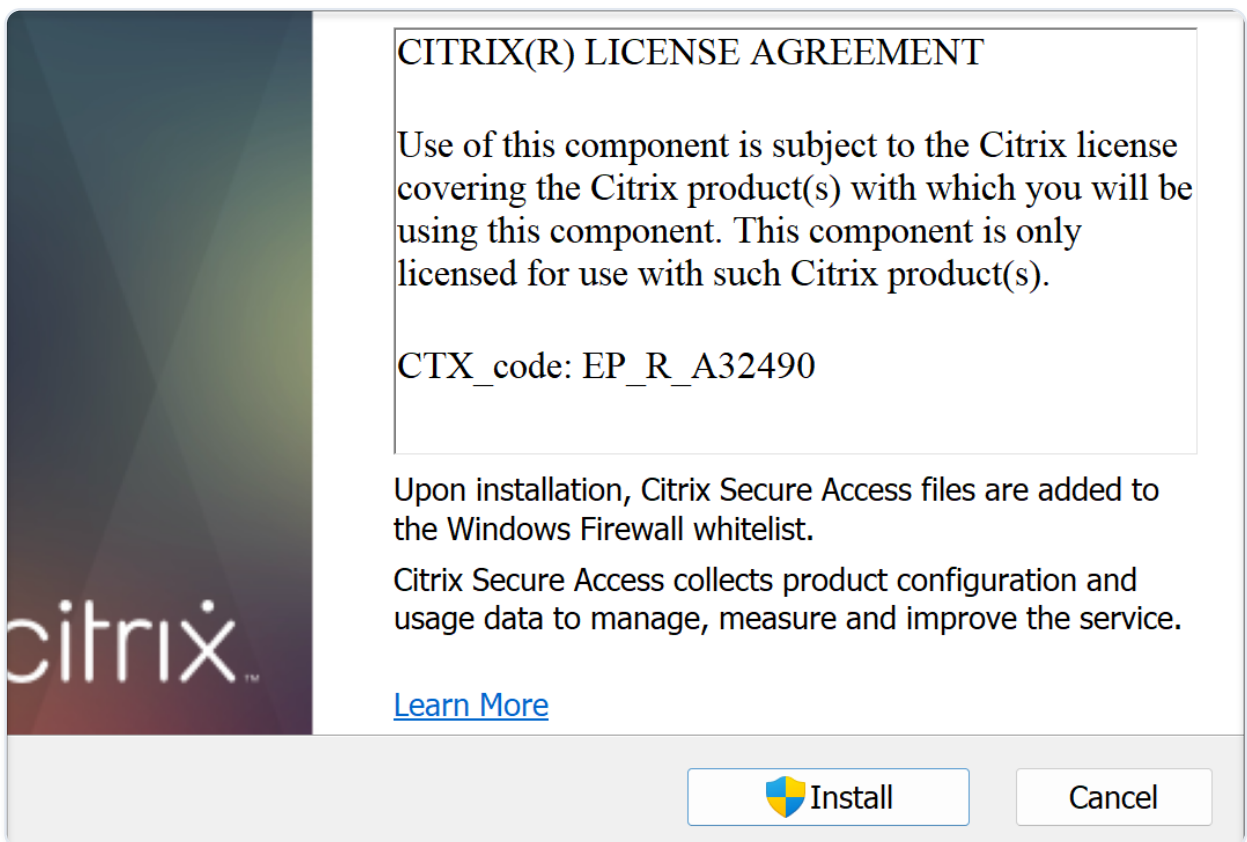
适用于 Windows 的 Citrix Secure Access 客户端

适用于 Windows 的 Citrix Secure Access 客户端是一款 VPN 客户端软件，可让您使用 NetScaler Gateway 和 Secure Private Access 远程访问公司数据和应用程序。

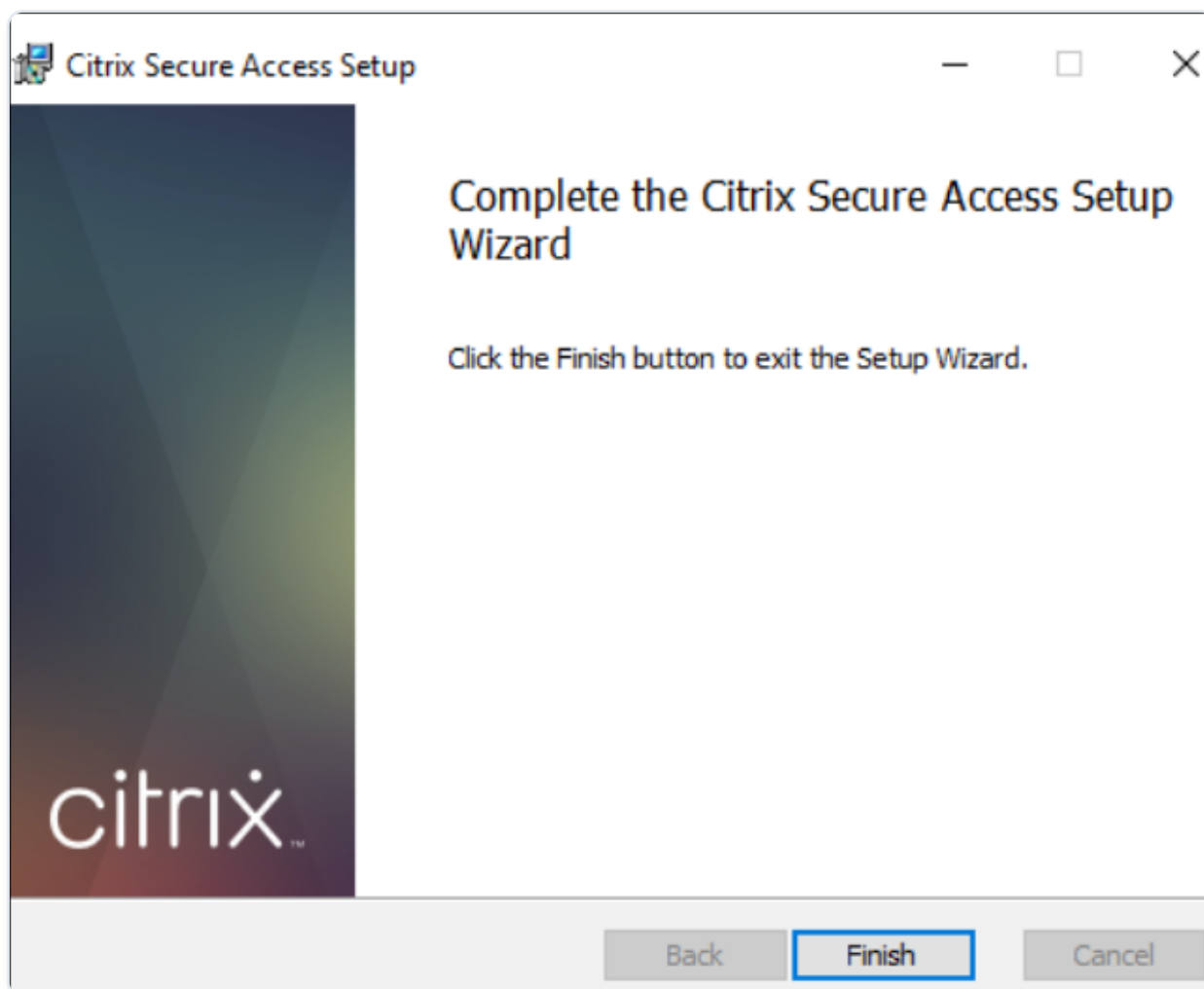
安装适用于 Windows 的 Citrix Secure Access 客户端

您可以使用以下说明安装 Citrix Secure Access 客户端，这需要管理员权限：

1. 从 [适用于 Windows 的 Citrix Secure Access 客户端](#) 下载 Citrix Secure Access 客户端。
2. 单击 **安装** 以在您的 Windows 计算机上安装客户端。如果您已有 Citrix Secure Access 客户端，则会对其进行升级。



3. 单击 **完成** 以完成安装。



如何使用适用于 Windows 的 Citrix Secure Access 客户端

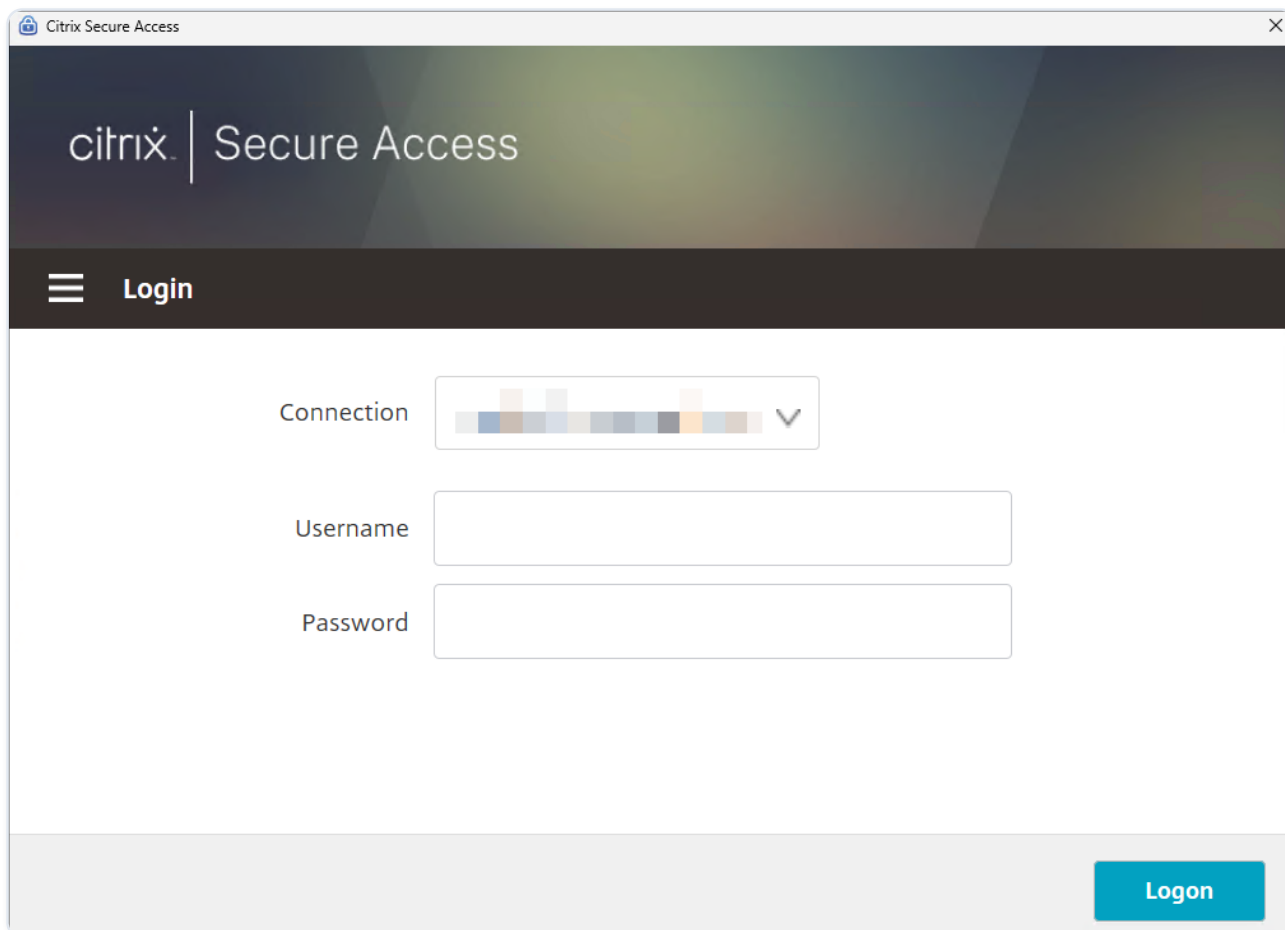
首次使用的用户必须通过添加连接 URL 来创建与 NetScaler Gateway 或 Secure Private Access 的连接，如果您的管理员尚未为您的应用程序添加连接 URL。对于后续使用，您可以连接到现有连接、添加连接以及编辑现有连接。您还可以查看日志并采取相应的操作。

添加连接

重要提示：

添加连接后，Citrix Secure Access 客户端会提示进行身份验证。提示取决于在 NetScaler Gateway 或 Secure Private Access 中配置的身份验证方法。您可能需要输入密码或一次性密码。或者，您可能会被重定向到 SAML 身份验证 URL。

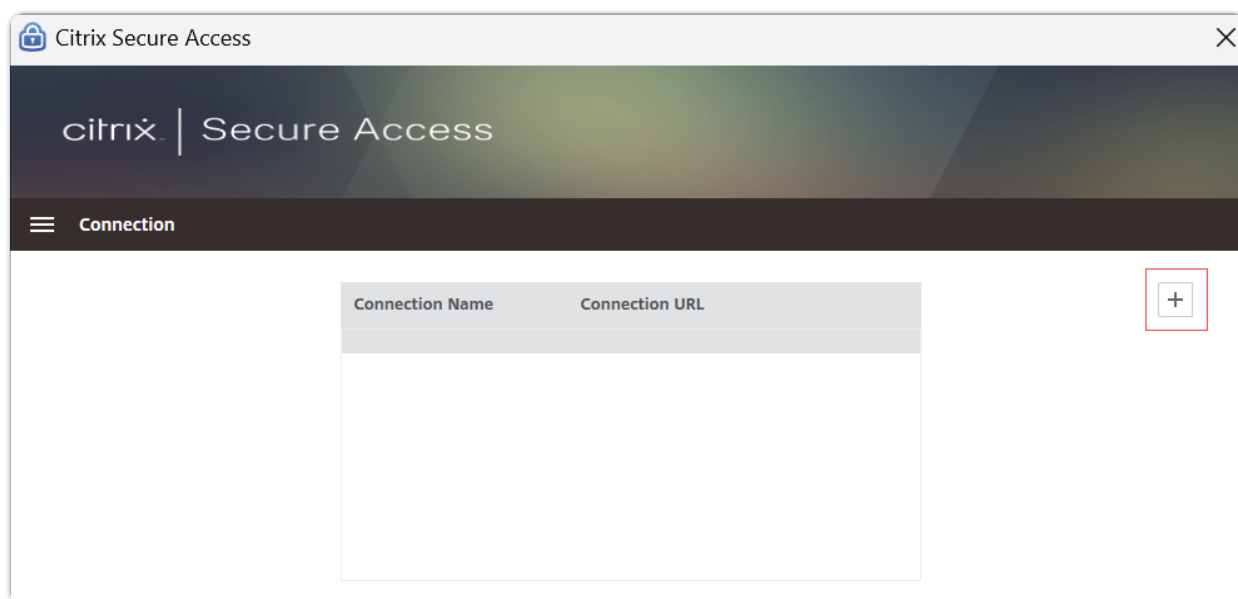
如果您的管理员已为您的应用程序添加了连接，请从“主页”中的下拉列表中选择连接，输入您的用户名和密码（或一次性密码），然后单击“登录”。



The image shows the Citrix Secure Access login interface. At the top, there's a header with the Citrix logo and 'Secure Access'. Below this is a dark navigation bar with a hamburger menu icon and the word 'Login'. The main area contains a 'Connection' dropdown menu with a color-coded bar and a downward arrow. Below the dropdown are two text input fields labeled 'Username' and 'Password'. At the bottom right, there is a blue 'Logon' button.

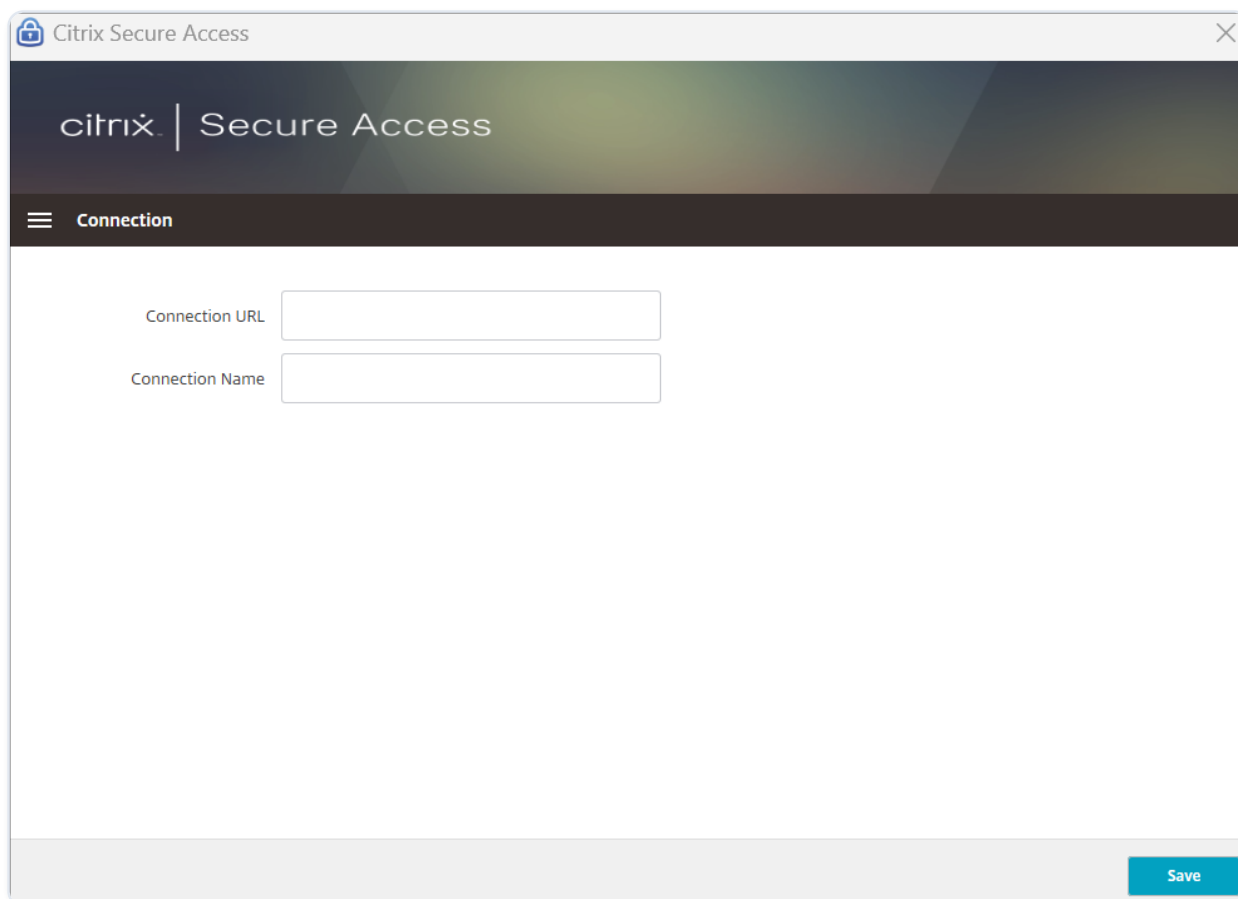
如果您的管理员尚未添加连接 URL，您必须按照以下步骤添加连接：

1. 在 Windows 计算机上安装 Citrix Secure Access 客户端后，打开该应用程序。
2. 导航到“**连接**”选项卡，然后单击“+”以添加连接。



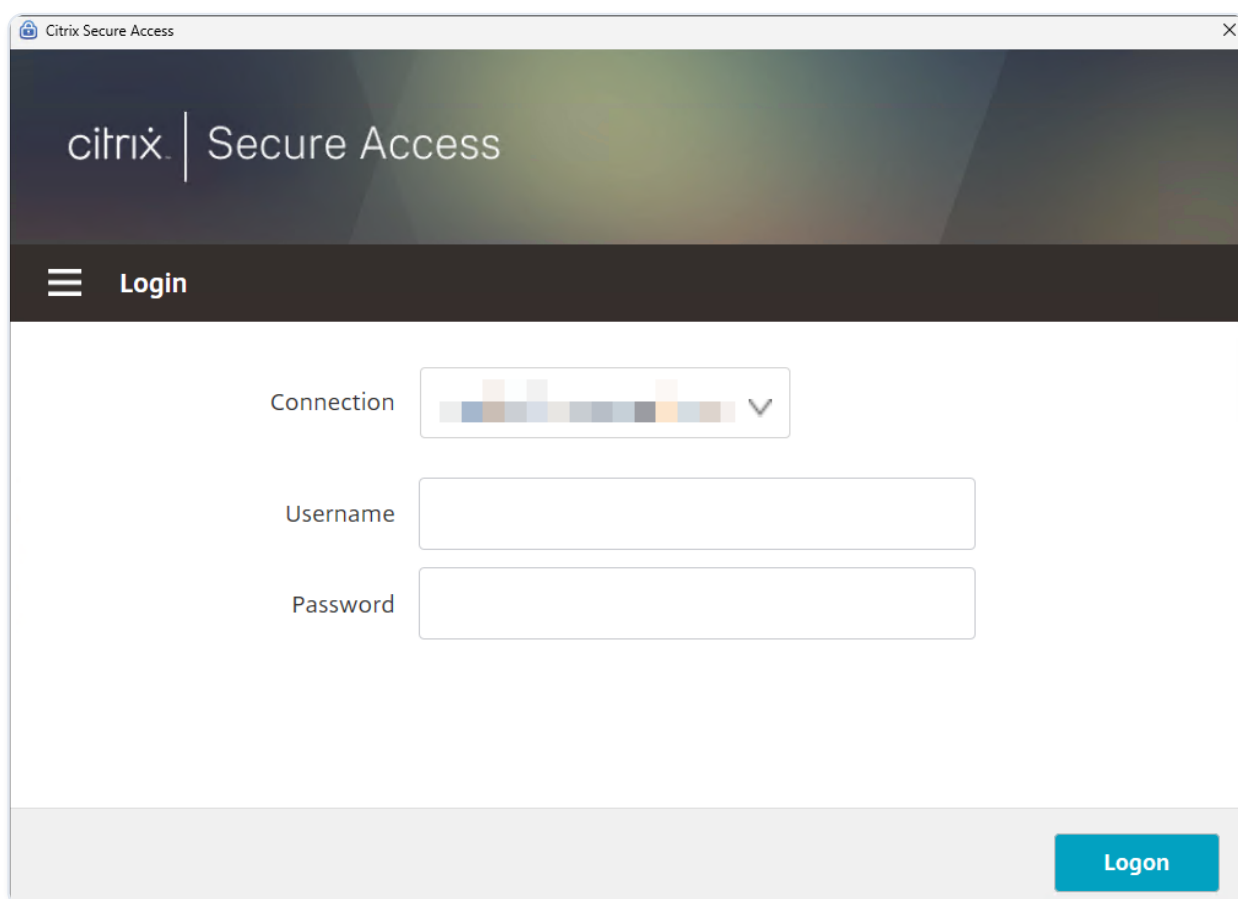
The image shows the Citrix Secure Access 'Connection' screen. At the top, there's a header with the Citrix logo and 'Secure Access'. Below this is a dark navigation bar with a hamburger menu icon and the word 'Connection'. The main area contains a table with two columns: 'Connection Name' and 'Connection URL'. The table is currently empty. To the right of the table, there is a red square button with a white plus sign (+).

3. 在“**连接 URL**”文本框中输入管理员提供的 URL，为连接提供一个名称，然后单击“**保存**”。



The image shows the Citrix Secure Access web interface. At the top, there is a header with the Citrix logo and the text "Secure Access". Below the header, there is a navigation bar with a hamburger menu icon and the word "Connection". The main content area contains two input fields: "Connection URL" and "Connection Name". At the bottom right, there is a blue button labeled "Save".

4. 添加连接后，导航到“主页”选项卡，从下拉列表中选择连接，输入您的用户名和密码（或一次性密码），然后单击“登录”。



The image shows the Citrix Secure Access web interface. At the top, there is a header with the Citrix logo and the text "Secure Access". Below the header, there is a navigation bar with a hamburger menu icon and the word "Login". The main content area contains a "Connection" dropdown menu with a color-coded bar and a downward arrow. Below the dropdown are two input fields: "Username" and "Password". At the bottom right, there is a blue button labeled "Logon".

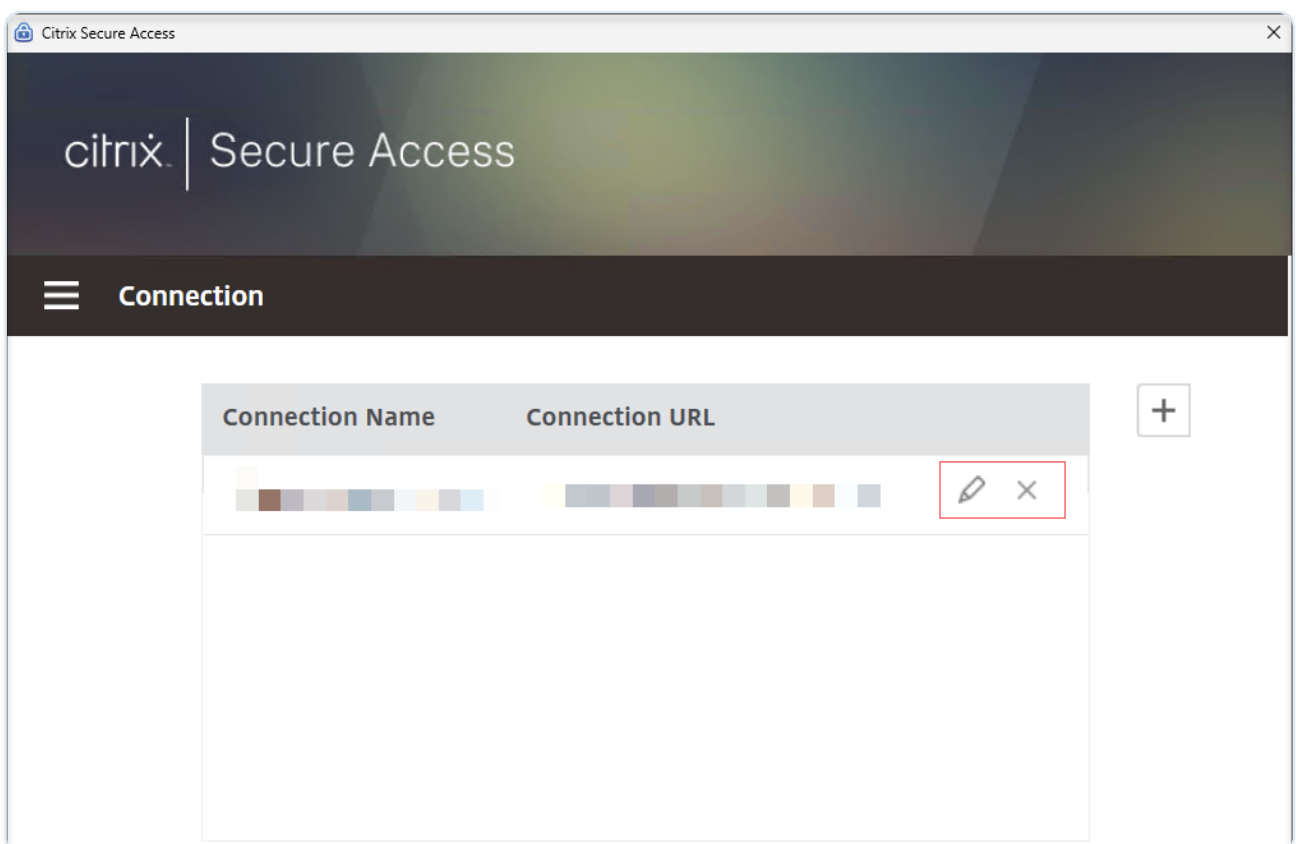
当身份验证成功后，您可以访问内部网应用程序。

注意：

首次登录后，如果管理员在 NetScaler Gateway 或 Secure Private Access 上启用了 **Always On** 或 **Always On before Windows Logon** 配置文件，则您无法手动连接或断开 VPN。

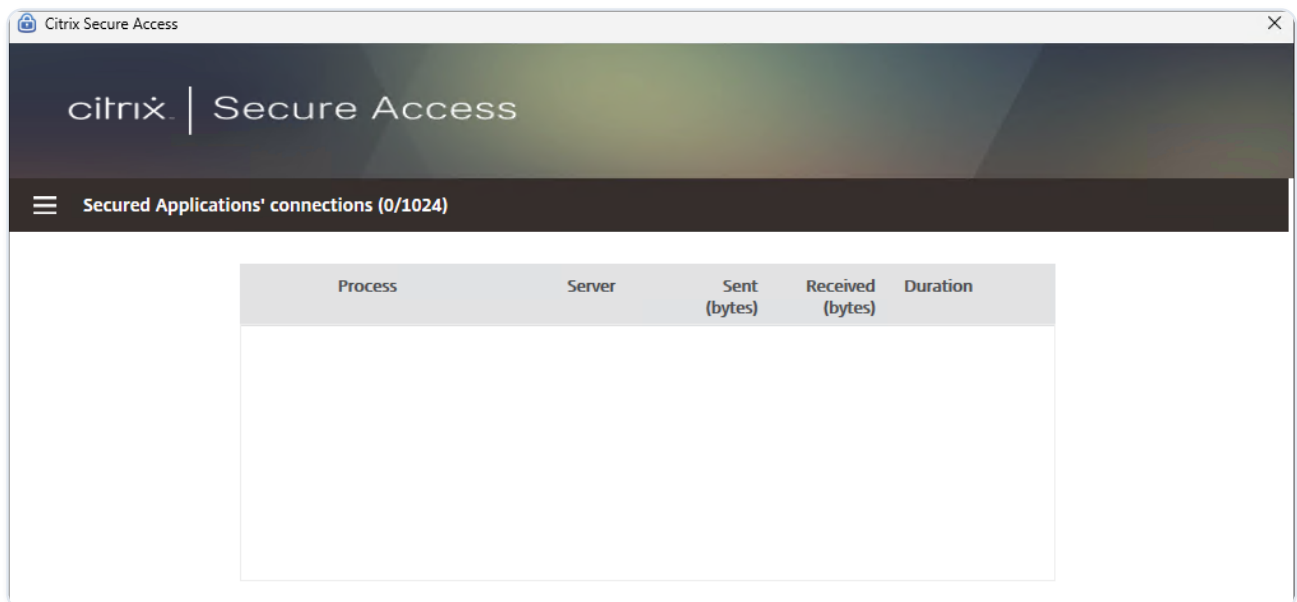
修改或删除现有连接

在**连接**选项卡上，单击编辑图标或取消图标以修改或删除现有连接。



查看安全应用程序

您可以在**安全应用程序**选项卡中查看连接到服务器的应用程序、服务器 IP、发送和接收的数据以及连接持续时间。



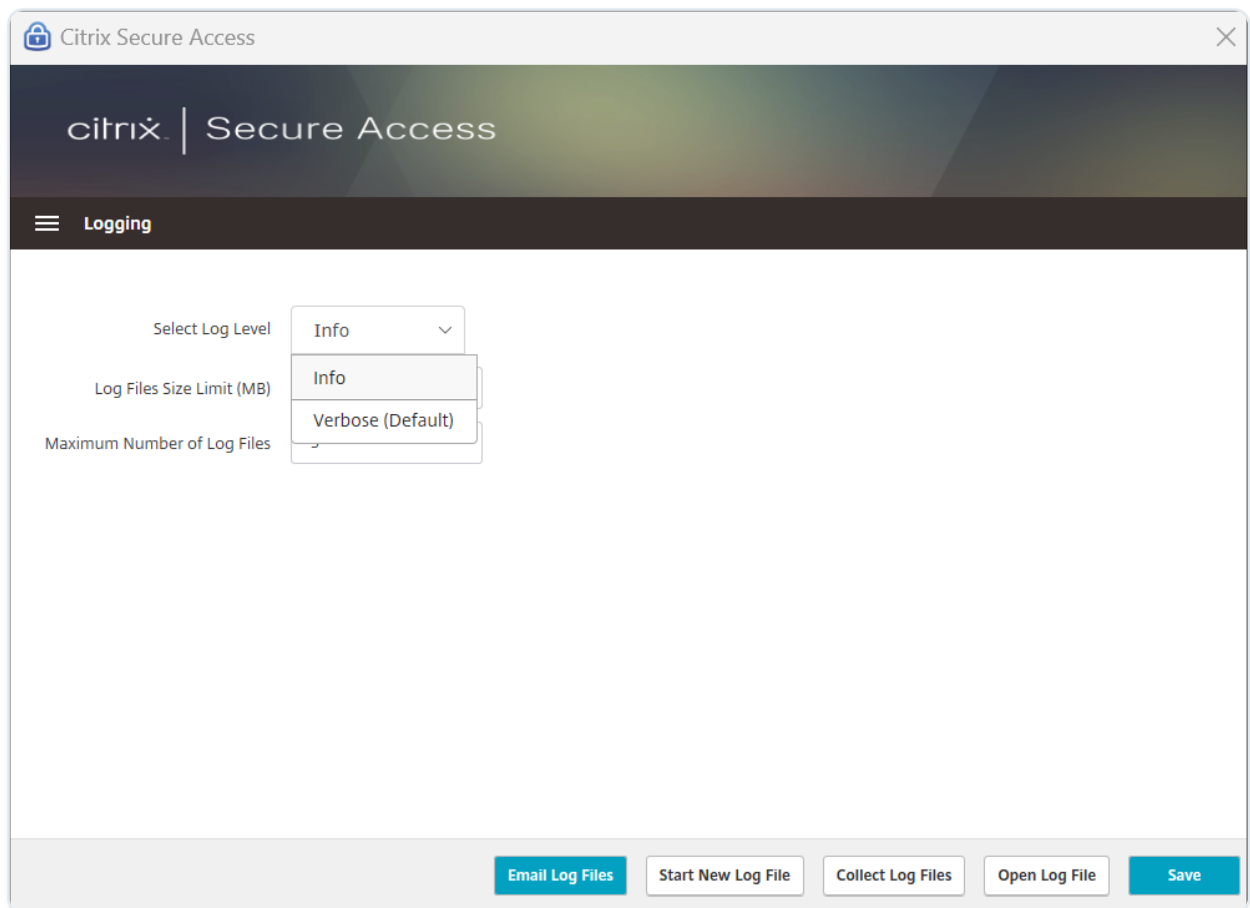
配置日志记录

您可以在**日志记录**选项卡中配置日志级别、文件大小和最大日志文件数。

1. ****选择日志级别：****适用于 Windows 的 Citrix Secure Access 客户端具有两个日志记录级别：
 - ****信息：****此级别包括与程序执行相关的信息性消息和事件。它还包括错误和异常。
 - **详细：**此级别包括信息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。
2. ****日志文件大小限制：****输入每个日志文件的大小。最大值为 600 MB。
3. **最大日志文件数：**输入要添加到日志收集的文件数。最大值为 5。
4. 单击 **保存** 以保存添加的日志配置。

日志记录 选项卡包括以下选项：

- **通过电子邮件发送日志文件：**以 nssslvpn.txt 格式将日志文件发送给管理员。
- **启动新日志文件：**创建一个新的日志文件，通常用于为新会话或在特定事件后重新开始日志记录以进行故障排除。
- **收集日志文件：**创建一个包含应用程序所有日志文件的 zip 文件。此 zip 文件将保存到您的桌面。
- **打开日志文件：**打开最新的 csa_nssslvpn*.txt 文件。



fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.