适用于 Android 的 Citrix Secure Access

Contents

适用于 **Android** 设备的 **Citrix Secure Access**

March 15, 2024

适用于 Android 的 Citrix Secure Access 客户端（以前称为适用于 Android 的 Citrix SSO 应用程序）提供 NetScaler Gateway 提供的最佳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。

> 备注：
>
> - 自版本 23.12.1 起，适用于 Android 的 Citrix SSO 更名为 Citrix Secure Access。我们正在更新我们的文档和用户界面屏幕截图以反映此次名称的更改。
> - 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。

如何从您的 **Android** 设备使用 **Citrix Secure Access**

March 15, 2024

> 备注：
>
> - 自版本 23.12.1 起，适用于 Android 的 Citrix SSO 更名为 Citrix Secure Access。我们正在更新我们的文档和用户界面屏幕截图以反映此次名称的更改。
> - 有关如何使用适用于 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。

从您的 Play 应用商店安装 Citrix Secure Access。首次使用的用户必须通过在非 MDM 案例中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，同时编辑现有连接（如果您的管理员允许在 MDM 部署中执行此操作）。还可以查看日志并相应地执行恰当的操作。

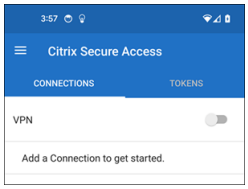
> 备注：
>
> - 无法编辑通过 MDM 部署的连接。
> - 自 Citrix SSO for Android 23.8.1 起，系统可能会提示您向 Citrix SSO 应用程序同意查询所有软件包。同意后，Citrix SSO 应用程序将：
>   - Receives the package install notification from the operating system.
>   - Restarts the Always On VPN.
>
>   当您首次连接到 VPN 配置文件时，系统会提示您同意收集已安装的软件包的信息（Google 政策要求您同

> 意）。如果您同意，VPN 连接即会启动。如果您拒绝同意，VPN 连接将中止。同意后，同意屏幕不会重新出现。

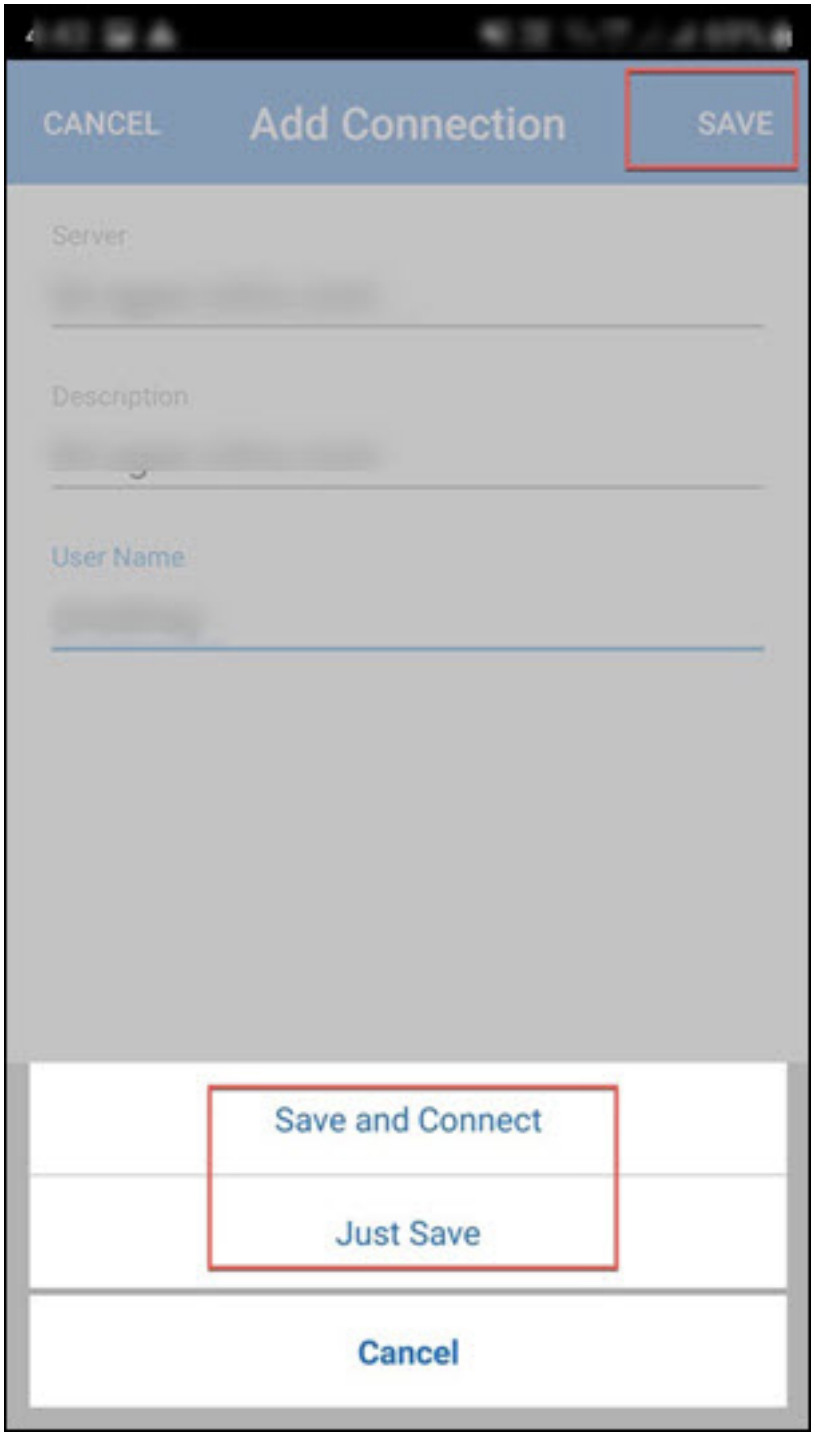
添加连接

注意：仅在非 MDM 案例中才需要执行此步骤。

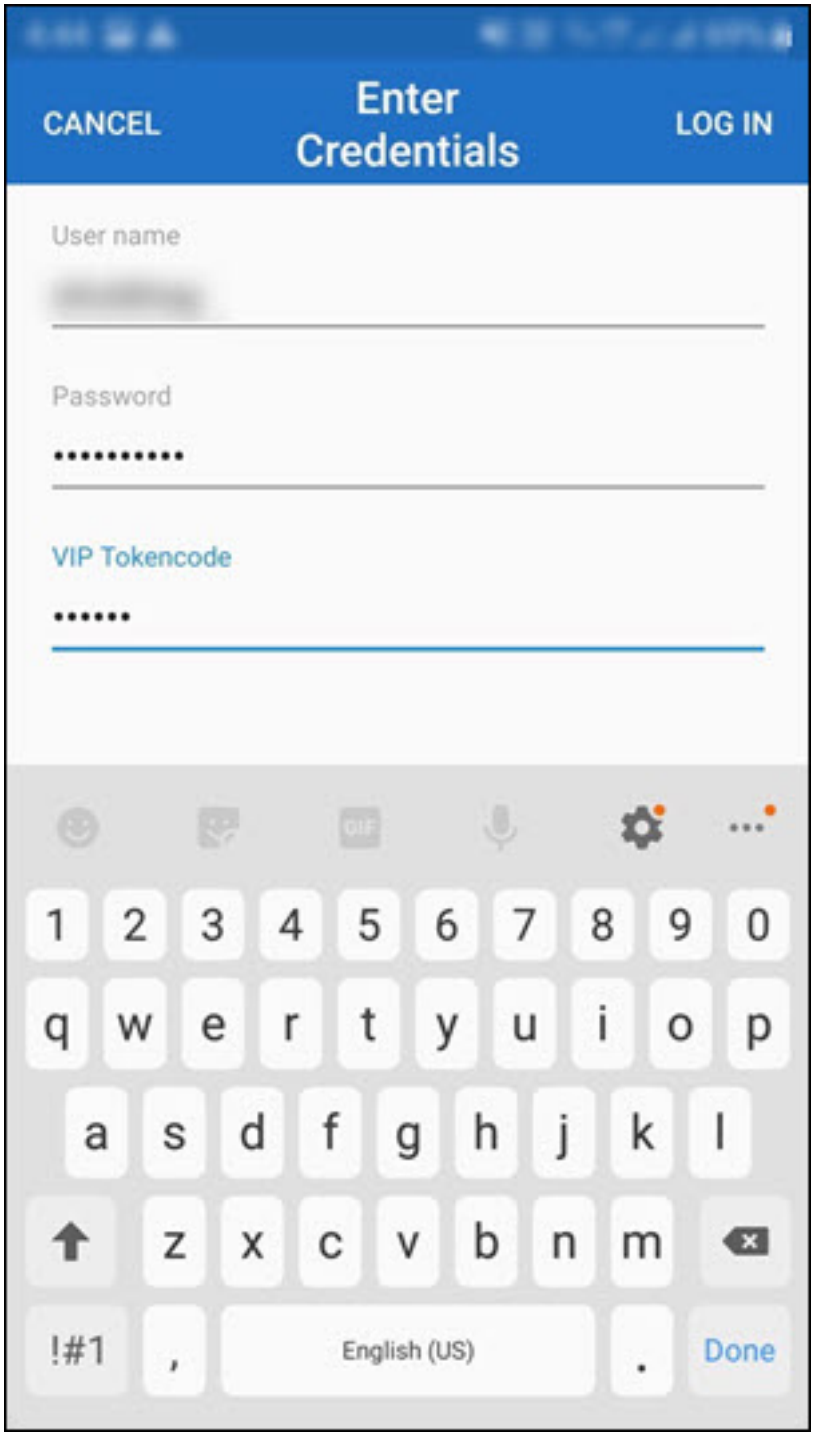
安装 Citrix Secure Access 并在 Android 设备上打开该应用程序后，将出现以下屏幕。



1. 单击 **+** 以添加连接。
2. 输入 VPN 连接的基本 URL（例如，https://gateway.mycompany.com）和名称。或者，您可以输入用户名。
3. 单击保存，然后单击保存并连接或仅保存（视情况而定）。

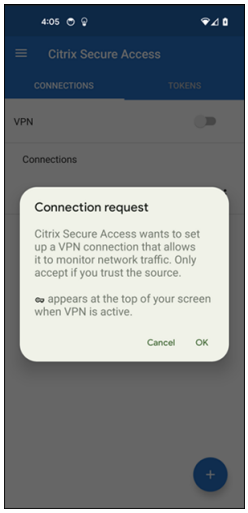


4. 提供服务器的身份验证凭据，然后在键盘上轻按登录或完成。

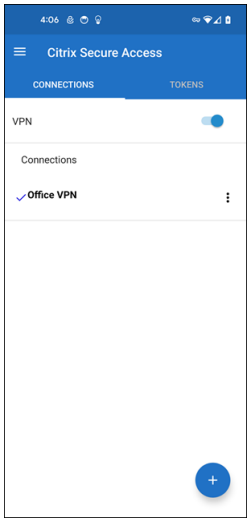


此时将显示连接请求消息。单击确定。

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，则直到用户卸载并重新安装应用程序后，才会再次显示此消息。



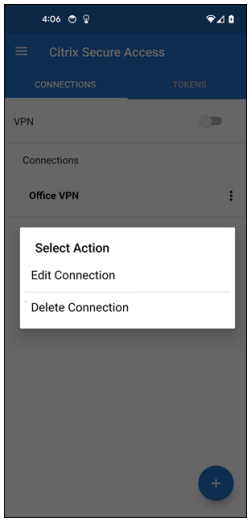
注意：要从 Citrix Secure Access 中注销，请关闭 **VPN** 开关。



修改或删除现有连接

注销 Citrix Secure Access 后，您可以编辑或删除连接。

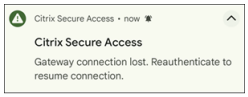
轻按住服务器名称，然后选择编辑连接或删除连接。



VPN 连接失败后重新连接到 **NetScaler Gateway -** 预览版

自 23.10.1 版本起，Citrix SSO for Android 会在 VPN 连接断开时提示您使用 NetScaler Gateway 重新进行身份验证。您会在用户界面和 Android 设备的通知面板上收到通知，指出与 NetScaler Gateway 的连接已断开，必须重新进行身份验证才能恢复连接。

> 注意：
>
> 此功能在预览版中提供。

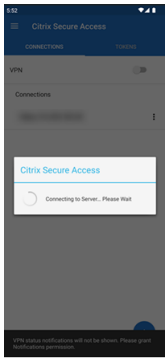


在 **Android 13+** 设备上接收或屏蔽通知

自适用于 Android 的 Citrix Secure Access 版本 23.12.1 起，当您在 Android 13+ 设备上安装或重新安装 Citrix Secure Access 客户端时，系统会提示您提供接收来自 Citrix Secure Access 客户端通知的权限。如果您拒绝权限，则不会在 Android 设备上收到来自 Citrix Secure Access 客户端的任何 VPN 状态或推送通知。

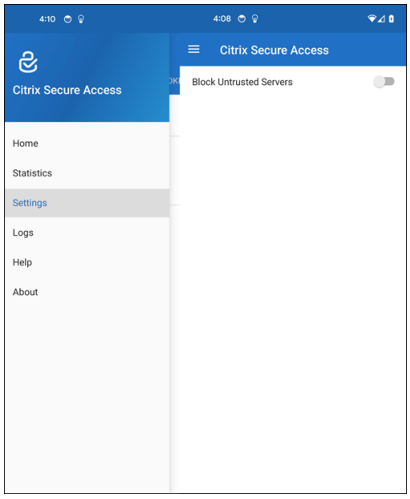
您可以在 Android 设备上导航到设置 **>** 通知来更改通知权限。

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

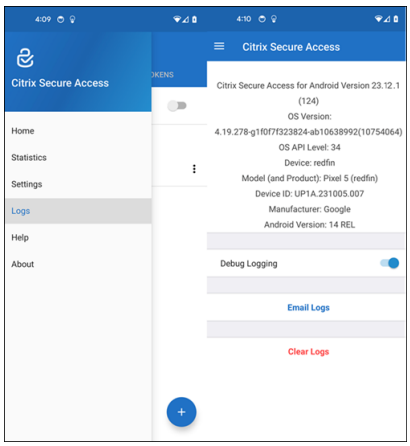
默认情况下，Citrix Secure Access 不会连接到不受信任的服务器。不受信任的服务器是指使用自签名证书或没有网关的可信根证书的服务器。要允许建立这些类型的连接，您可以将阻止不受信任的服务器开关切换到关。



启用调试日志

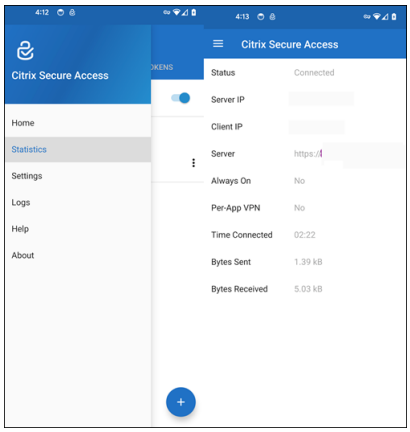
捕获调试日志是故障排除或向 Citrix 支持部门报告问题的关键部分。

轻按调试日志记录开关开以打开 Citrix Secure Access 的调试日志记录。对连接问题进行故障排除时，可以使用电子邮件日志链接通过电子邮件发送日志。



查看统计信息

可以在连接了 VPN 时查看连接统计信息。



密码令牌

可以添加 6 位数的密码令牌作为第二重身份验证。此代码使用基于时间的一次性密码协议来生成 OTP 代码。

可以手动添加密码令牌或使用 QR 代码扫描方法注册密码令牌。如果选择手动输入令牌，则不会启用使用推送通知的第二重身份验证。

注册密码令牌

1. 在桌面或便携式计算机上的 Web 浏览器中登录组织的管理一次性 PIN 码页面。
2. 单击添加设备。
3. 输入设备的名称，然后单击转到。

   生成一个 QR 代码。

通过扫描浏览器上的 **QR** 代码添加密码令牌

1. 导航到主页视图上的令牌选项卡。
2. 轻按 **+** 并轻按扫描 **QR** 代码。
3. 将相机对焦于浏览器上的 QR 代码。

Citrix Secure Access 将自动填充设备名称和密钥。

或者，您可以手动输入 QR 代码上方显示的密钥。

Citrix Secure Access 验证 QR 代码，然后向网关注册以获取推送通知。如果注册过程中没有错误，令牌将成功添加到令牌选项卡中。

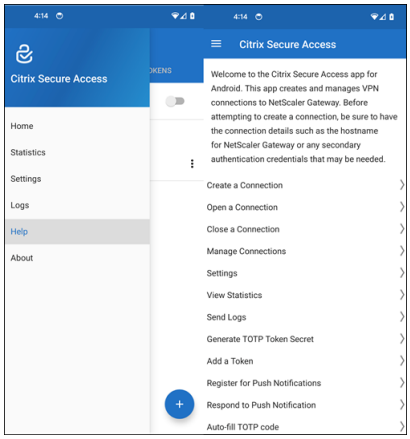
> 注意：
>
> - 必须允许 Citrix Secure Access 的相机权限才能捕获 QR 代码。
> - 必须在设备上启用设备 PIN 码/密码。

手动添加密码令牌

1. 导航到主页视图上的令牌选项卡。
2. 轻按 + 并轻按手动输入。
3. 输入在浏览器上生成的密码令牌上显示的设备名称和密钥。

帮助主题

有关如何使用 Citrix Secure Access 的详细信息，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

March 15, 2024

> 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。

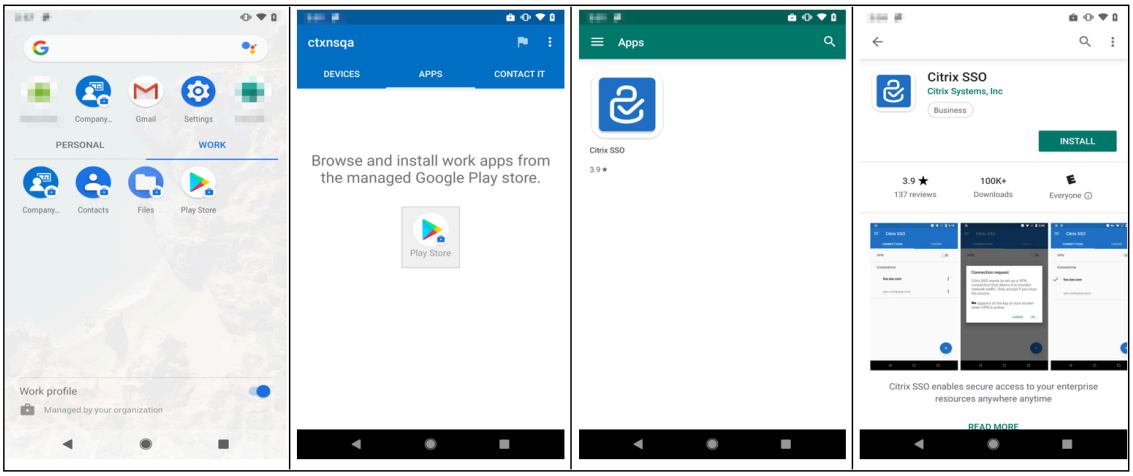
本主题捕获有关使用在 Microsoft Intune Android Enterprise 环境中配置的 Citrix Secure Access 客户端连接到企业网络的详细信息。

假设：

- 您已使用 Intune 公司门户应用程序在 Intune 中注册设备。
- 在设备上设置了工作配置文件以供用户使用。

1. 在设备上从工作配置文件打开 **Intune** 公司门户应用程序。
2. 单击三点菜单打开应用程序的设置，然后滚动到屏幕底部。轻按同步以与 Intune 服务器同步，然后导航到主应用程序屏幕。
3. 轻按应用程序选项卡，然后轻按托管 **Google Play** 应用商店链接。

   此时将显示用户的已批准应用程序列表。

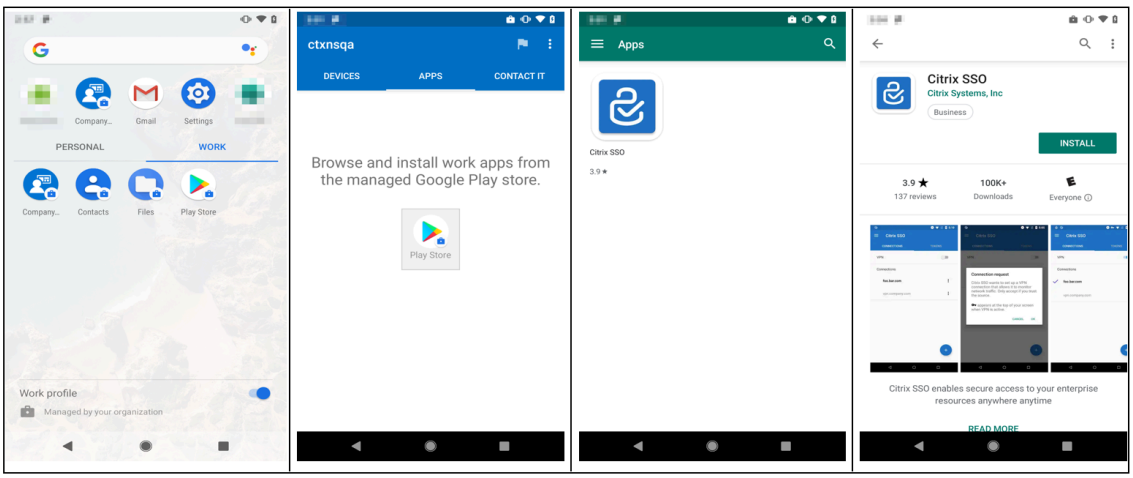


4. 轻按 **Citrix Secure Access**。

   Citrix Secure Access 客户端显示在托管 Google Play 应用商店中。

5. 轻按安装。
6. 导航回工作配置文件应用程序列表。Citrix Secure Access 已添加到已安装的应用程序列表中。

7. 轻按工作配置文件应用程序列表中的 Citrix Secure Access 图标将其打开。



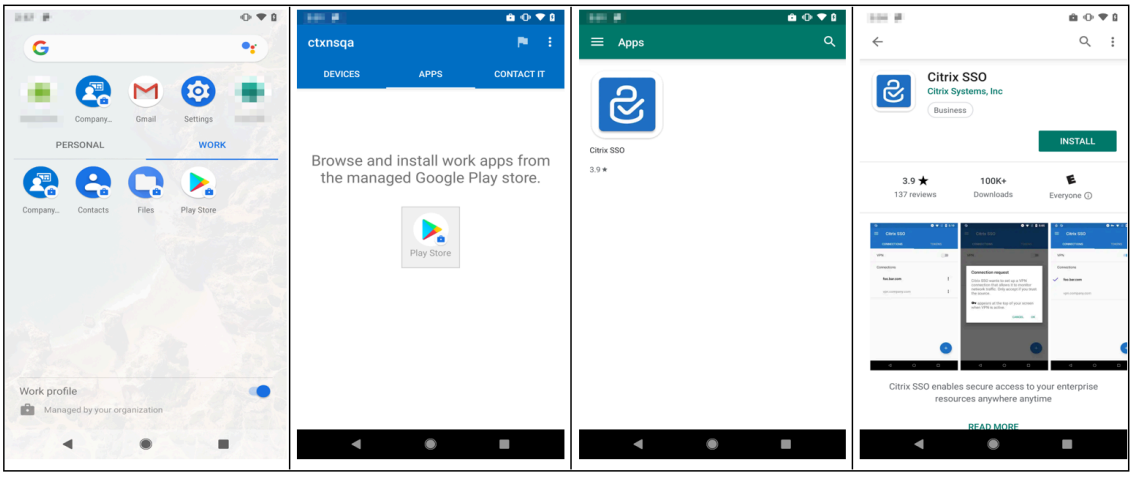
Citrix Secure Access 已打开。系统会提示您允许或禁止与公司内部网络安全通信的权限。

8. 轻按允许以授予权限。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）。轻按允许以授予权限。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，则在授予此权限之前，您无法连接到公司的内部网络。

9. 我的企业 **VPN**（或您在 Intune 中的 Citrix Secure Access 配置中选择的名称）在连接选项卡的“托管连接”部分中列出。轻按此连接，系统将提示您输入凭据以使用 NetScaler Gateway 进行身份验证。

10. 提供凭据以使用 NetScaler Gateway 进行身份验证，然后轻按登录。



如果在 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 VPN 通道设置的连接请求。轻按确定向 Citrix Secure Access 授予与公司内部网络建立安全连接的权限。

    注意：仅当您首次建立与 NetScaler Gateway 的安全连接时才会显示此提示。在卸载 Citrix Secure Access 并在设备上重新安装之前，该应用程序不会显示以供后续连接尝试使用。

您已连接到您的内部公司网络。设备状态栏中显示一个密钥图标，通知您 VPN 连接处于活动状态。Citrix Secure Access 客户端的 VPN 服务通知图标也显示在状态栏上。连接开关将其状态更改为已连接，VPN 配置文件名称旁边会显示一个复选标记图标。