Citrix SSO for iOS

Contents

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

March 15, 2024

适用于 iOS 的 Citrix Secure Access 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。

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 PerApp VPN 配置文件。

> 重要提示：
>
> - 自版本 23.11.1 起，适用于 iOS 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 iOS 的 Citrix SSO 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。

在 **Citrix Secure Access** 应用程序中导入和安装证书

March 15, 2024

> 重要提示：
>
> - 自版本 23.11.1 起，适用于 iOS 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 iOS 的 Citrix Secure Access 的管理员特定说明，请参阅适用于 iOS 的 Citrix Secure Access 和适用于 macOS 的 Citrix Secure Access。

iOS 上的 Citrix Secure Access 支持使用 NetScaler Gateway 进行客户端证书身份验证。可以通过以下方式将证书传递到 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。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。按照 MDM 供应商特定的文档执行此方法。
- 电子邮件 - 仅适用于非 MDM 客户的方法。管理员向用户发送包含以 PKCS#12 文件格式附加的用户证书标识（证书和私钥）的电子邮件。用户必须在其 iOS 设备上配置其电子邮件帐户才能接收带附件的电子邮件。然后，可以将该文件导入到 iOS 上的 Citrix Secure Access。

  > 注意：
  >
  > 文件扩展名 `.pfx` 和 `.p12` 由 iOS 系统声明，不能由第三方应用程序（例如 Citrix Secure Access）声明。

> 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. 打开包含以 PKCS#12 文件格式附加的用户证书标识（证书和私钥）的电子邮件。

   - 轻按附件以显示系统打开方式菜单。
   - 轻按复制到 **Citrix SSO**。

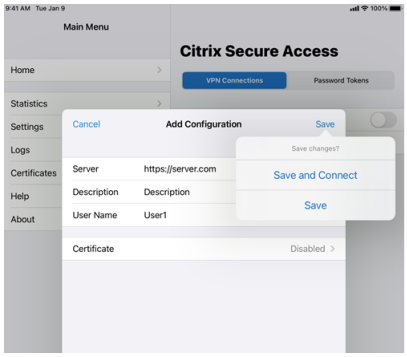
2. 在 Citrix Secure Access 中安装证书。

   应用程序现在已启动，并显示输入证书密码的提示。输入要安装到应用程序的钥匙串中的证书的正确密码，然后单击导入。

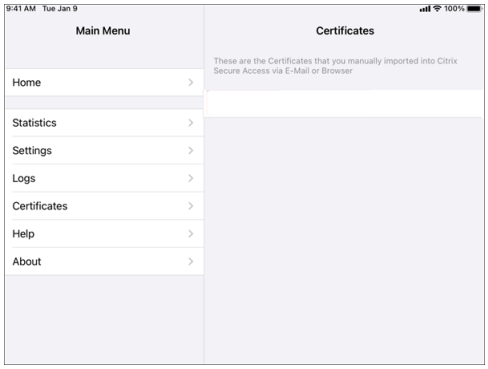
   验证成功后，将导入证书。

3. 将基于证书的身份验证与 VPN 结合使用。

   - 要将证书用于 VPN 身份验证，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，然后轻按添加 **VPN** 配置。
     - 在 VPN 配置文件的配置视图中，可以在证书部分中选择导入的证书。



   - 轻按保存以导入证书。



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**

March 15, 2024

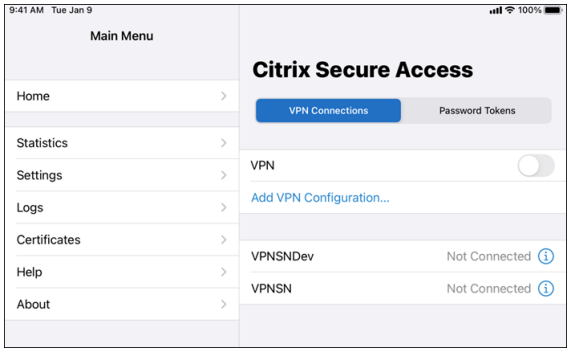
> 重要提示：
>
> - 自版本 23.11.1 起，适用于 iOS 的 Citrix SSO 更名为 Citrix Secure Access。我们正在更新我们的文档和用户界面屏幕截图以反映此次名称的更改。
> - 有关适用于 iOS 的 Citrix Secure Access 的管理员特定说明，请参阅适用于 macOS/iOS 的 Citrix Secure Access。

请从 App Store 安装 Citrix Secure Access 应用程序。安装应用程序后，首次使用时必须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新连接，同时编辑现有连接。还可以查看日志并相应地执行恰当的操作。

对于 MDM 客户，您的管理员可能具有预配置的 VPN 连接，这些连接在您注册设备时自动显示。您可以通过选择连接并打开 VPN 开关直接启动连接。这些 VPN 连接不可由用户编辑。

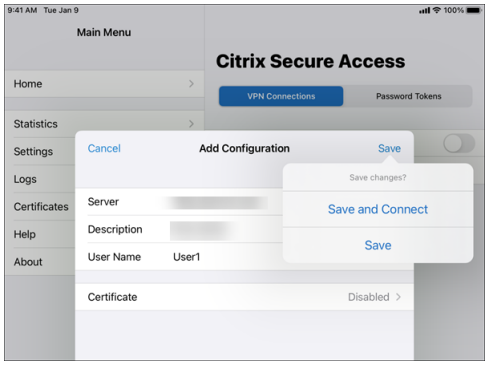
添加连接

安装 Citrix Secure Access 并打开应用程序后，将出现以下屏幕。

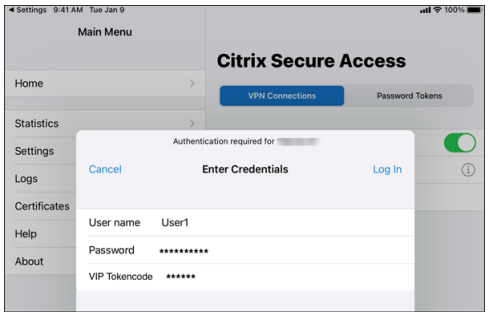


1. 轻按添加 **VPN** 配置以添加新连接。
2. 输入服务器详细信息。

   还可以选择性添加用户名。
3. 轻按保存，然后轻按保存并连接或保存（视情况而定）。



4. 提供服务器的身份验证凭据，然后轻按登录。



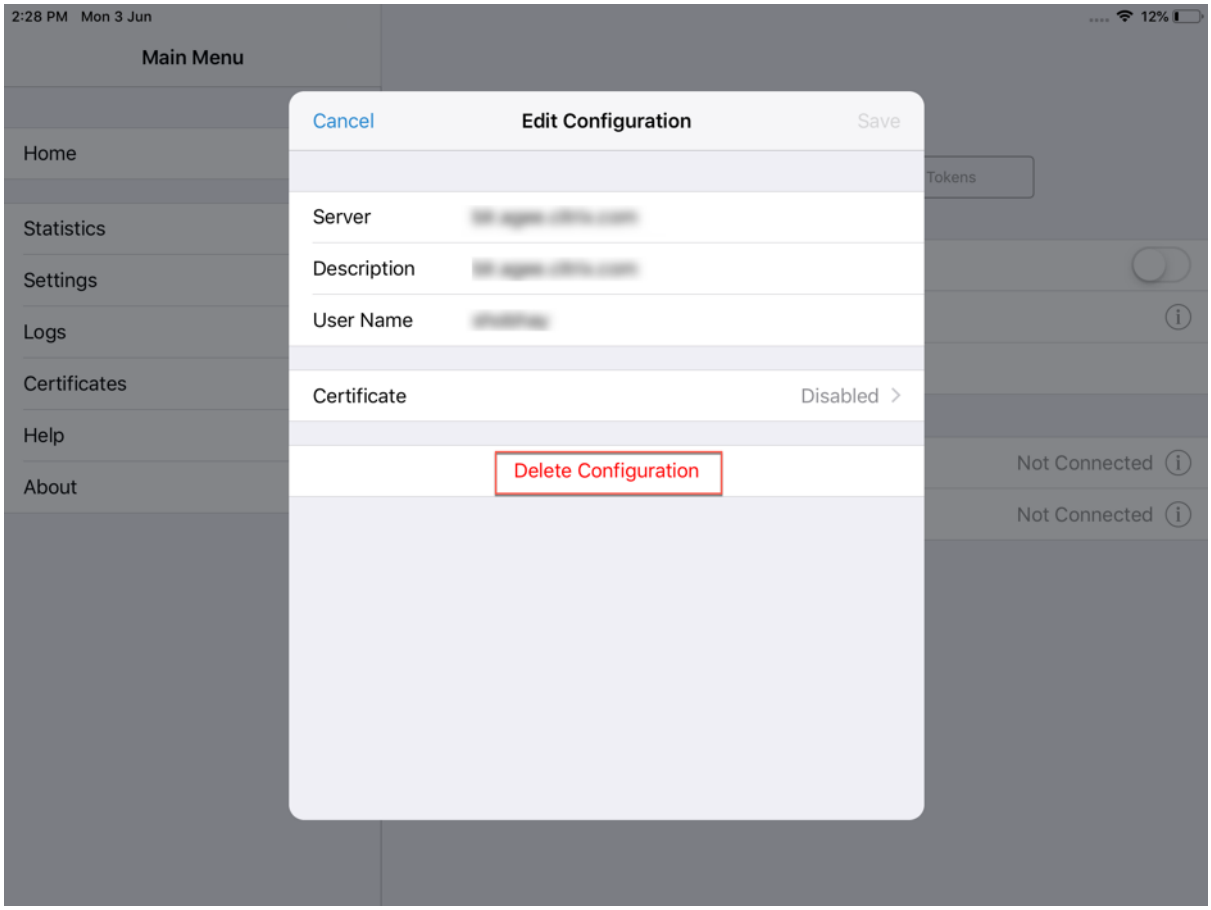
   注意：要注销 Citrix Secure Access，请关闭 VPN。

VPN 连接失败后重新连接到 **NetScaler Gateway**

自 23.09.1 版本起，适用于 iOS 的 Citrix SSO 应用程序会在 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。

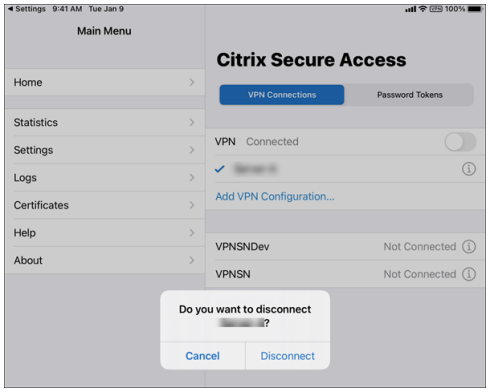
删除现有连接

轻按连接旁边的图标，然后轻按“删除配置”。



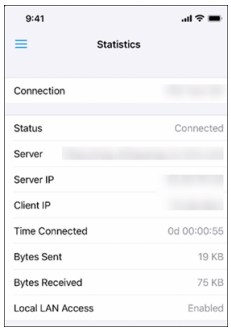
断开连接

将 VPN 开关切换到“关”，然后轻按“断开连接”。



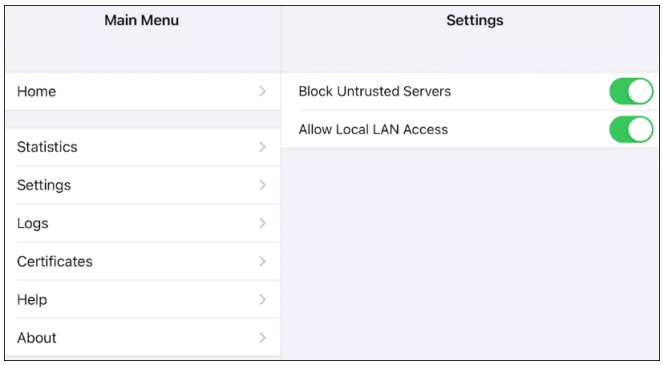
查看统计信息

可以在连接了 VPN 时查看连接统计信息。



阻止不受信任的服务器

默认情况下，Citrix SSO 不连接到不受信任的服务器（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。



本地 **LAN** 访问

Citrix SSO for iOS 23.10.1 支持本地 LAN 访问功能，在建立 VPN 连接后，您可以在该功能中确定是否要访问客户端设备上的本地 LAN 资源。仅当管理员在 NetScaler Gateway 上配置了本地 LAN 访问设置后，您才能使用此功能。

要在 Citrix Secure Access 用户界面上配置本地局域网访问，请执行以下操作：

1. 导航到主菜单并单击设置。
2. 启用 **Allow Local LAN Access**（允许本地 LAN 访问）。

可以在 **Statistics**（统计信息）页面上验证本地 LAN 访问的状态。

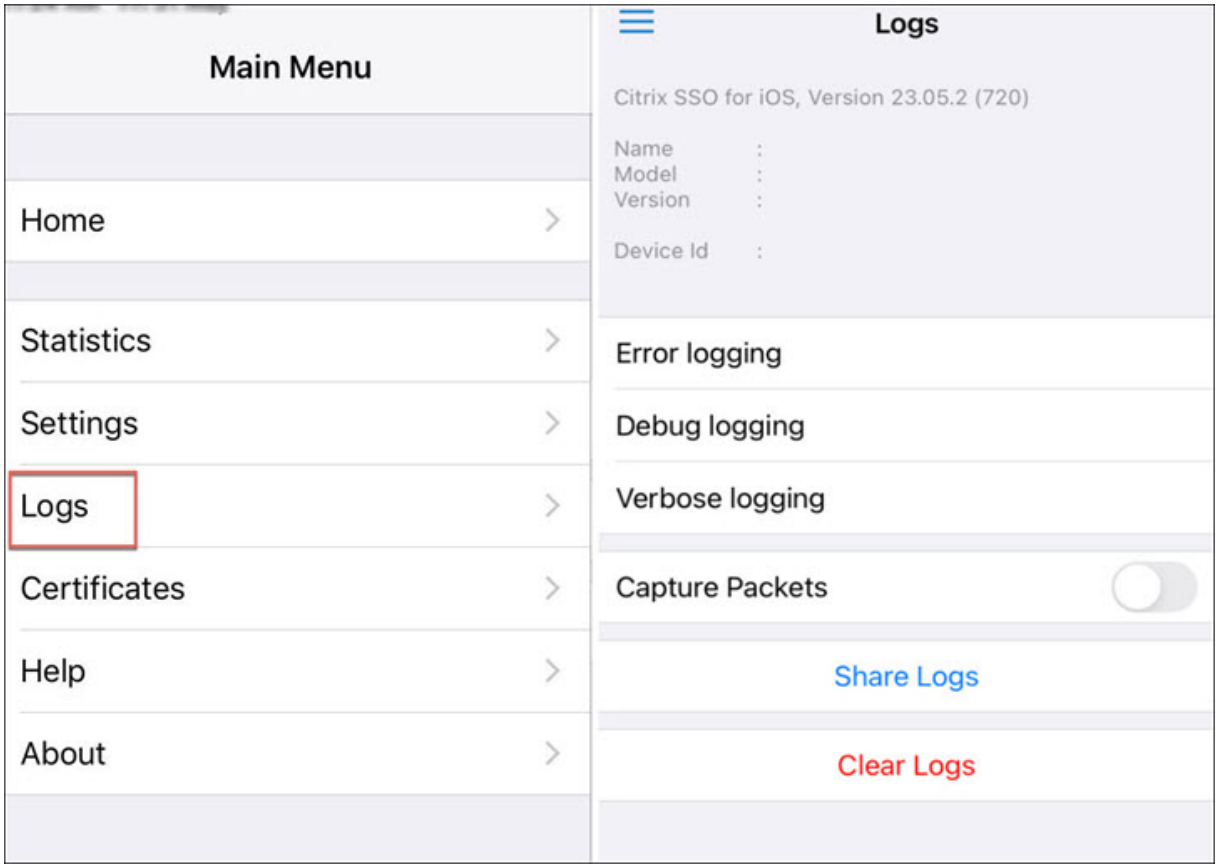
发送日志

捕获调试日志是故障排除或向 Citrix 支持部门报告问题的关键部分。

下面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。

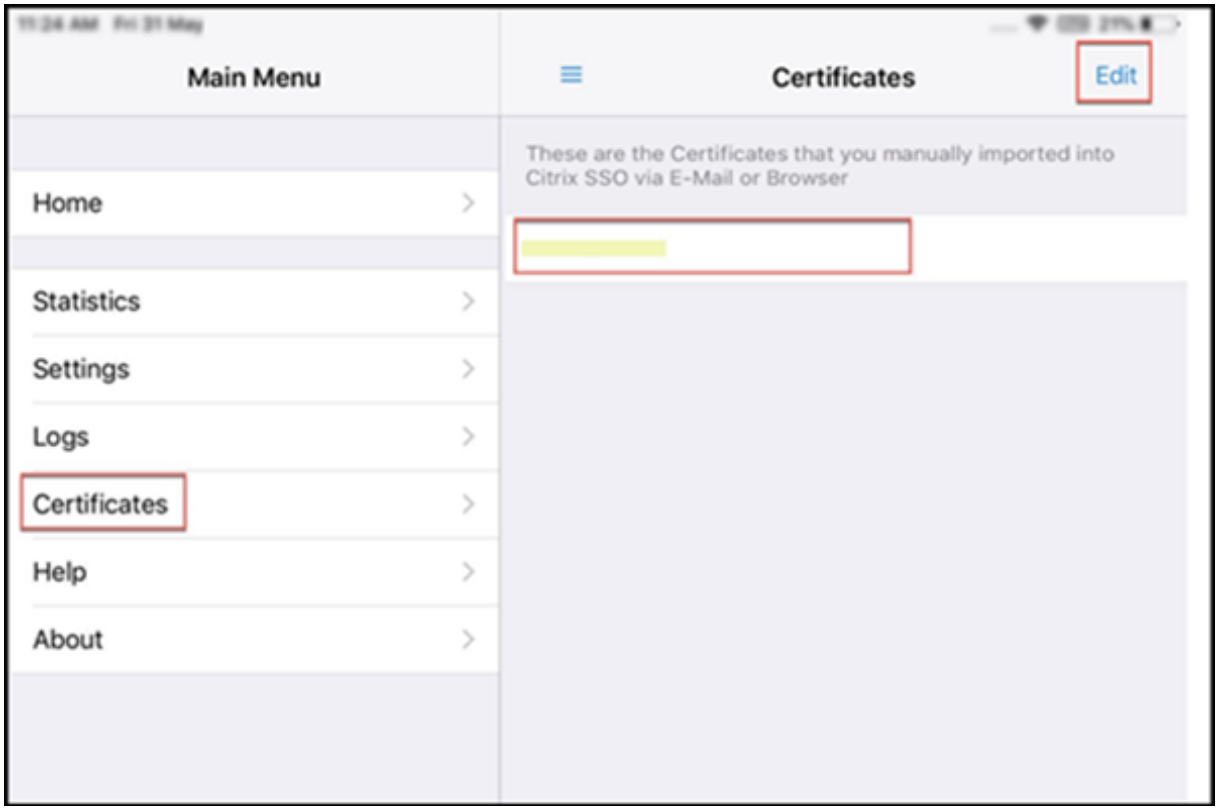
> 注意：
>
> - 要生成一组新的日志，请先使用清除日志删除较旧的日志。
> - 自 23.07.1 版本起，通过电子邮件发送日志选项将替换为共享日志选项。“共享日志”提供了多种用于共享压缩的日志文件的选项。



查看客户端证书

可以查看导入 Citrix Secure Access 的客户端证书。导入的证书显示在证书部分中。您可以通过以下方式之一删除证书。

- 在证书单元格上，从右到左执行滑动手势以显示删除按钮。然后轻按删除。
- 轻按编辑以显示删除按钮，然后轻按删除。



帮助主题

有关各种项目的帮助，请参阅帮助。