# Citrix SSO

**Machine translated content**

## Disclaimer

# Contents



# 适用于 **iOS /macOS** 设备的 **Citrix SSO**

January 18, 2024

传统的 Citrix VPN 客户端是使用现已弃用的 Apple 私有 VPN API 构建的。Citrix SSO 中的 VPN 支持将使用 Apple 的公共网络扩展框架从头开始重写。

以下是 Citrix SSO 应用程序引入的一些主要功能：

- 密码令牌：密码令牌是 6 位数的代码，可替代 VIP、OKTA 等辅助密码服务。此代码使用基于时间的一次性密码 (T-OTP) 协议生成类似于 Google Authenticator、Microsoft Authenticator 等服务的 OTP 代码。在对给定 Active Directory 用户的 Citrix Gateway 进行身份验证期间，系统会提示用户输入两个密码。第二个因素是用户从已注册的第三方服务（如 Google 或 Microsoft 身份验证器）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 Citrix ADC 设备上注册 T-OTP。有关注册步骤，请参阅https://support.citrix.com/article/CTX228454。在应用程序中，用户可以通过扫描 Citrix ADC 上生成的二维码或手动输入 TOTP 密钥来添加 OTP 功能。OTP 令牌一旦添加就会显示在用户界面的密码令牌段中。

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。

Citrix SSO 应用程序可用于在注册本机 OTP 支持时扫描二维码。
Citrix Gateway 推送通知功能仅对 Citrix SSO 应用程序用户可用。

- 推送通知： Citrix Gateway 在已注册的移动设备上发送推送通知，以获得简化的双重身份验证体验。您可以通过为已注册设备提供设备 PIN 码/Touch ID/面容 ID 来验证身份，而不是打开 Citrix SSO 应用程序以在 Citrix ADC 登录页面上键入第二个因素 OTP。

将设备注册为推送通知后，还可以使用 Citrix SSO 应用程序将设备用于本机 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 Citrix ADC 支持设备，也会为推送通知注册该设备。

## 发行说明

January 18, 2024

Citrix SSO 发行说明描述了服务版本中可用的新功能、现有功能的增强功能、已修复问题和已知问题。发行说明包含下面的一个或多个部分：

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：当前版本中已修复的问题。

已知问题：当前版本中存在的问题及其解决方法（无论是否适用）。

### V1.2.6

已知问题

- 在 macOS 从睡眠中醒来后，VPN 有时会被冻结。

  [NSHELP-20656 - macOS]

### V1.2.5

已知问题

- 在 macOS 从睡眠中醒来后，VPN 有时会被冻结。

  [NSHELP-20656 - macOS]

### V1.2.4

已知问题

- 有时，Mac 从睡眠模式唤醒后 VPN 会话不响应。

  [NSHELP-20656 - macOS]

### V1.2.3

新增功能

- Citrix SSO URL 方案—Citrix SSO 现在注册一个 URL 方案，以便其他应用程序可以确定 Citrix SSO 是否安装在 iOS 设备上。URL 方案是“柠檬酸。“

  [CGOP-11979 - iOS]

已修复的问题

- Citrix SSO 应用程序在发送大量 UDP 流量时崩溃。

  [CGOP-11603 - macOS]

- 当应用程序从 iOS 13 上的通知启动时，适用于 iPad 的 Citrix SSO 崩溃。

  [NSHELP-21087 - iOS]

## V1.2.2

已修复的问题

- 在某些 GSLB 部署中，Citrix SSO 会多次解析 Gateway 名称，导致连接失败。

  [CGOP-12013]

- 适用于 iOS 的 Citrix SSO 无法扫描大于 16 字节的 OTPSecret。

  [CGOP-11978 - iOS]

- 将提示配置文件配置为仅证书身份验证和 NAC 检查的用户输入登录凭据，并且无法创建 VPN 连接。

  [CGOP-11925 - iOS]

- 虽然每个应用程序分割隧道标志仅针对 TCP 流量检查，但 ICMP 流量即使在必须直接发送 ICMP 流量的情况下也是如此。

  [CGOP-11614 - iOS]

已知问题

- 适用于 macOS 的 Citrix Gateway 插件不支持在 Citrix Workspace 应用程序上打开登录页面的功能。

  [NSHELP-7047]

## V1.2.0

新增功能

- **nFactor** 身份验证支持。现在，iOS 和 macOS 都支持 nFactor 身份验证。

  [CGOP-11251]

- **Citrix SSO** 应用程序支持。Citrix SSO 应用程序现在支持 iOS 13 和 macOS 卡塔利娜.

  [CGOP-11714]

已修复的问题

- 客户端 IP 地址将向后显示在 SSO 应用程序的“连接”页面中。

  [CGOP-11596]

- Citrix SSO 不支持 Citrix ADC 版本 13.0 中的 DNS 标志中的 DNS 截断位。

  [CGOP-11777]

- 每个应用程序拆分隧道与 Citrix ADC 版本 13.0 不兼容。

  [CGOP-11464]

- Citrix SSO 忽略来自 Citrix Gateway 关的一些超时消息。

  [CGOP-11310]

- 用户首次登录应用程序时，应用程序描述的最后一行不会显示在用户屏幕上。

  [CGOP-11595 - macOS]

- 当您重复单击“登录”按钮时，Citrix SSO 应用程序登录窗口大小不断增加。

  [CGOP-11594 - macOS]

- 当超过授权用户的最大数量限制时，系统级别将显示一条错误消息，而不是在应用程序窗口中。

  [CGOP-11600 - macOS]

## V1.1.12

新增功能

- **macOS** 的遥测数据收集。Citrix SSO 收集与应用中 VPN 使用情况相关的自定义分析事件。

  [CGOP-9789 - macOS]

- 每个应用程序分割隧道支持。管理员可以配置每个应用程序拆分隧道。与 Citrix Gateway 的 Intranet 路由匹配的每个应用程序流量将通道传送到 Citrix Gateway 设备。

  [CGOP-657]

- 基于系统 **FQDN** 的 **FQDN** 分裂隧道隧道流量。FQDN 拆分隧道基于系统的 FQDN 而不是 DNS 服务器解析的 IP 隧道通信。

  [CGOP-316]

已修复的问题

- 用户界面元素（如按钮、文本字段、标签等）在 iPad 屏幕上不对齐。

  [CGOP-10141 - iOS]

- 如果用户没有添加 VPN 配置文件，则不会收到远程登录通知。

  [CGOP-9731 - iOS]

### V1.1.10

已修复的问题

- Citrix SSO 应用程序不会在达到用户的最大数量时显示正确的错误消息。

  [CGOP-231]

- 默认情况下不会清除 EULA 复选框。

  [CGOP-245]

- “终端分析”中的“启用”扫描不支持添加功能。

  [CGOP-249]

- 即使钥匙串中仅存在一个客户端/设备，也不会自动选择用于身份验证的客户端/设备证书。

  [CGOP-251]

- 在 Citrix SSO 应用程序中编辑“连接记录”后，无法添加“连接记录”。

  [CGOP-7256]

## 为 **iOS** 用户设置 **Citrix SSO**

February 1, 2024

> 重要提示： Citrix VPN 不能在 iOS 12 及更高版本上使用。要继续使用 VPN，请使用 Citrix SSO 应用程序。

下表比较了 Citrix VPN 和 Citrix SSO 之间的各种功能的可用性。

| 功能 | Citrix VPN | Citrix SSO |
| --- | --- | --- |
| 设备级 VPN | 支持 | 支持 |
| 每个应用程序 VPN（仅限 MDM） | 支持 | 支持 |
| 每个应用程序分割隧道 | 不支持 | 支持 |
| MDM 配置的 VPN 配置文件 | 支持 | 支持 |
| 按需 VPN | 支持 | 支持 |
| 密码令牌（基于 T-OTP） | 不支持 | 支持 |
| 基于推送通知登录（来自注册手机的第二个因素） | 不支持 | 支持 |

| 功能 | Citrix VPN | Citrix SSO |
| --- | --- | --- |
| 基于证书的身份验证 | 支持 | 支持 |
| 用户名/密码身份验证 | 支持 | 支持 |
| 使用 Citrix Endpoint Management（以前称为 XenMobile）进行网络访问控制检查 | 不支持 | 支持 |
| 使用 Microsoft Intune 进行网络访问控制检查 | 支持 | 支持 |
| DTLS 支持 | 不支持 | 支持 |
| 阻止用户创建的 VPN 配置文件 | 支持 | 支持 |
| 适用于 Citrix Cloud 托管的本机应用程序的单点登录 | 不支持 | 支持 |
| 支持的操作系统版本 | iOS 9，10，11（不适用于 iOS 12 以上） | iOS 系统 9 以上 |

### 与 **MDM** 产品的兼容性

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

Citrix SSO 还支持称为网络访问控制 (NAC) 的功能。有关 NAC 的更多信息，请单击此处。借助 NAC，MDM 管理员可以在连接到 Citrix ADC 之前强制执行最终用户设备合规性。Citrix SSO 上的 NAC 需要 MDM 服务器，例如 Citrix Endpoint Management 或 Intune 和 Citrix ADC。

### 为 **Citrix SSO** 配置 **MDM** 托管 **VPN** 配置文件

以下部分以使用 Citrix Endpoint Management（以前称为 XenMobile）为例介绍了为 Citrix SSO 配置设备范围和 PerApp VPN 配置文件的分步说明。使用 Citrix SSO 时，其他 MDM 解决方案可以使用此文档作为参考。

> 注意：本部分介绍了基本设备范围和每个应用程序 VPN 配置文件的配置步骤。此外，您还可以按照 Citrix Endpoint Management（以前称为 XenMobile）文档或 Apple 的 MDM VPN 有效负载配置来配置始终启用的按需代理。

#### 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 Citrix ADC 中定义的 VPN 策略（如全隧道、分割隧道、反向拆分隧道），来自所有应用程序和服务的流量都会通道到 Citrix Gateway。

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

1. 在 Citrix Endpoint Management MDM 控制台上，导航至配置 > 设备策略 > 添加新策略。

2. 在左侧的策略平台窗格中选择 **iOS** 。在右侧窗格中选择 **VPN** 。

3. 在“策略信息”页面上，输入有效的策略名称和描述，然后单击“下 一步”。

4. 在 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** 。

注意：在 MDM VPN 负载中，连接名称对应于 **UserDefinedName** 键，**VPN** 类型键必须设置为 **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 SSO 应用程序的捆绑标识符。

注意：在 MDM VPN 负载中，自定义 SSL 标识符对应于 **VPNSubType** 键。

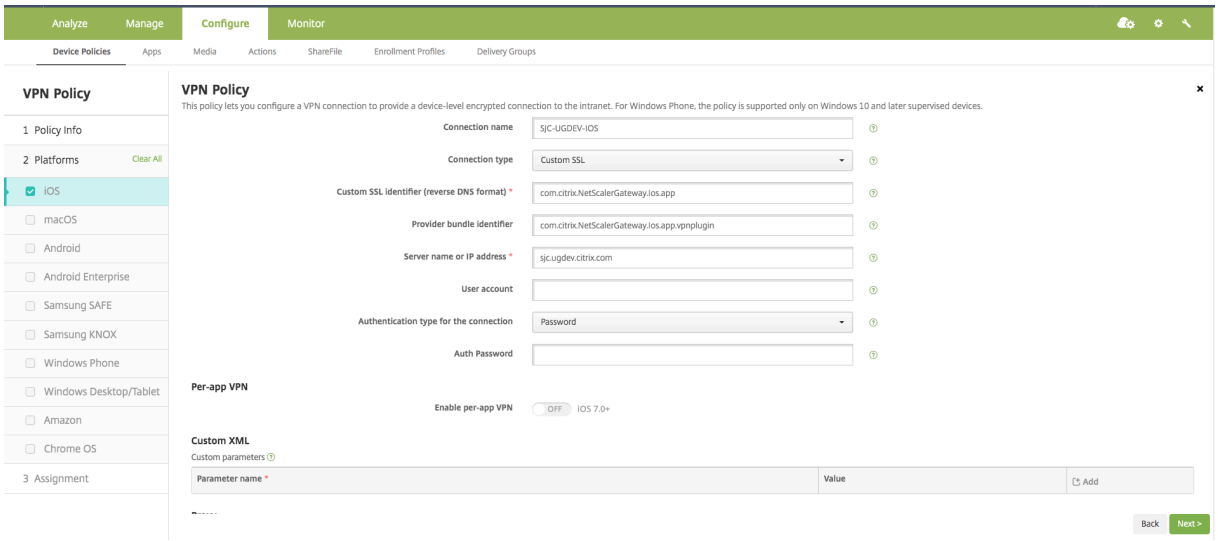
6. 在提供商捆绑标识符中，输入 **com.citrix.NetScalerGateway.ios.app.vpnplugin**。这是 Citrix SSO iOS 应用程序二进制文件中包含的网络扩展的捆绑标识符。

注意：在 MDM VPN 负载中，提供程序捆绑标识符对应于 **ProviderBundleIdentifier** 键。

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

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

8. 点击 下一步。




9. 单击保存。

每个应用程序 **VPN** 配置文件

每个应用程序的 VPN 配置文件用于为特定应用程序设置 VPN。只有特定应用程序的流量才会被隧道传送到 Citrix Gateway。每个应用程序 VPN 负载支持设备范围 VPN 的所有密钥以及一些附加密钥。

在 **Citrix Endpoint Management** 上配置每个 **PerApp** 级 **VPN**　执行以下步骤来配置每个应用程序的 VPN：

1. 完成 Citrix Endpoint Management 上的设备级 VPN 配置。

2. 打开“每个应用程序 **VPN**”部分中的“启 用每个应用程序 VPN”开关。

3. 如果应 在启动匹配应用程序 时自动启动 Citrix SSO，则启用按需匹配应用程序开关。建议在大多数每个应用程序的情况下使用此功能。

注意：在 MDM VPN 有效负载中，此字段对应于 **OnDemandMatchAppEnabled** 键。

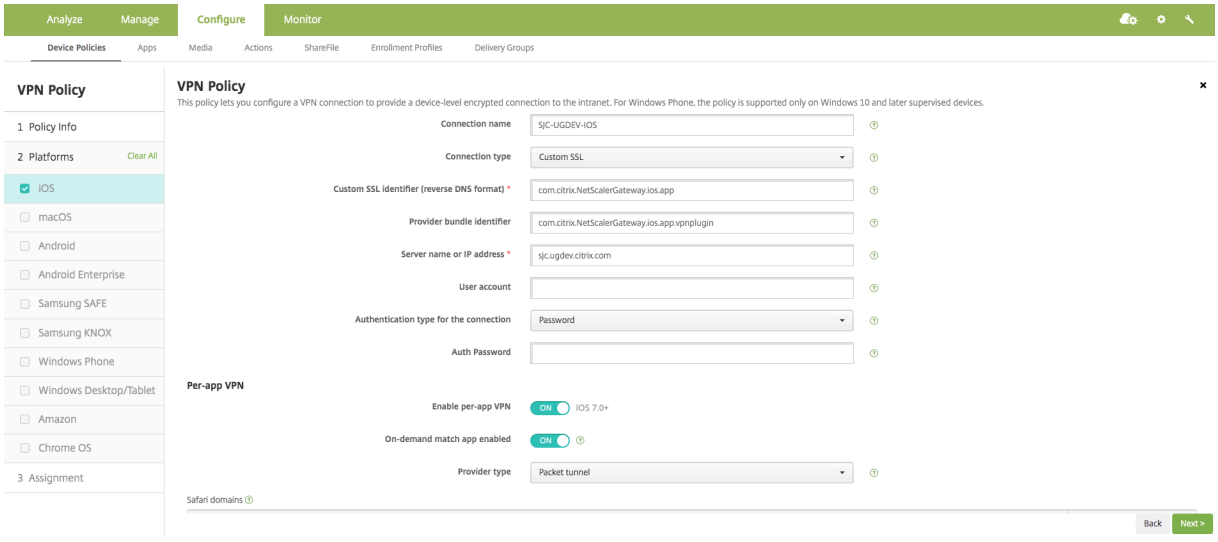
4. 在“提供程序类型”中，选择“数据包隧道”。

注意：在 MDM VPN 负载中，此字段对应于密钥提 供程序类型。

5. Safari 域配置是可选的。配置 Safari 域后，Citrix SSO 会在用户启动 Safari 并导航到与“域”字段中的 URL 匹配的 URL 时自动启动。如果您想限制特定应用的 VPN，则不建议使用此操作。

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

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




14. 点击 下一步。

15. 单击保存。

要将此 VPN 配置文件关联到设备上的特定应用程序，您必须按照本指南创建
应用程序库存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/。

### 在每个应用程序 **VPN** 中配置分割隧道

MDM 客户可以在每个应用程序 VPN 中为 Citrix SSO 配置分割隧道。为此，必须将以下键/值对添加到 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-->
```

密钥区分大小写，并且应该完全匹配，而值不区分大小写。

注意：用于配置供应商配置的用户界面不是 MDM 供应商的标准。您必须与 MDM 供应商联系，以查找 MDM 用户控制台上的供应商配置部分。

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

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

### 禁用用户创建的 **VPN** 配置文件

MDM 客户可以阻止用户从 Citrix SSO 应用程序中手动创建 VPN 配置文件。为此，必须将以下键/值对添加到 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"
<!--NeedCopy-->
```

密钥区分大小写，并且应该完全匹配，而值不区分大小写。

注意：用于配置供应商配置的用户界面不是 MDM 供应商的标准。您必须与 MDM 供应商联系，以查找 MDM 用户控制台上的供应商配置部分。

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

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

### 已知问题

问题描述：针对每个应用程序 VPN 或按需 VPN 配置中包含“.local”域的 FQDN 地址的隧道。Apple 的网络扩展框架中存在一个错误，它阻止在域部分（例如http://wwww.abc.local）中包含.local 的 FQDN 地址通过系统的 TUN 接口进行隧道。此地址的流量将通过设备的物理接口发出。仅在每个应用程序 VPN 或按需 VPN 配置中观察到此问题，在系统范围的 VPN 配置中看不到此问题。Citrix 已向 Apple 提交了一份雷达缺陷报告，Apple 指出，根据 RFC-6762：https://tools.ietf.org/html/rfc6762，.local 是一个多播 DNS (mDNS)
查询，因此不属于缺陷。但是，Apple 还没有关闭这个错误，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：为替代方法等地址分配非.local 域名。

限制

- 尚未完全支持基于 FQDN 的分割隧道。
- iOS 上不支持端点分析 (EPA)。
- 不支持基于端口/协议的分割隧道。

## 将用户证书标识作为电子邮件附件发送给 iOS 用户

January 18, 2024

iOS 上的 Citrix SSO 支持使用 Citrix 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传递到 Citrix SSO 应用程序：

- MDM 服务器-这是 MDM 客户的首选方法。证书直接在 MDM 托管 VPN 配置文件上配置。然后，当设备注册到 MDM 服务器时，VPN 配置文件和证书都会推送到已注册的设备。请按照 MDM 供应商特定的文档进行此方法。
- 电子邮件-仅适用于非 MDM 客户的方法。在这种方法中，管理员向用户发送附加的用户证书标识（证书和私钥）的电子邮件。#12 用户需要在 iOS 设备上配置他们的电子邮件帐户才能接收附件的电子邮件。然后，该文件可能会导入到 iOS 上的 Citrix SSO 应用程序。以下部分介绍了此方法的配置步骤。

必备条件

- 用户证书-具有给定用户的.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。
- 安装在 iOS 设备上的 Citrix SSO 应用程序。

配置步骤

1. 重命名用户证书的扩展/MIME 类型。

用于用户证书最常用的文件扩展名是“.pfx”、“.p12”等。这些文件扩展名是不标准的 iOS 平台，不像格式，如.pdf, .doc。“.pfx”和“.p12”均由 iOS 系统声明，并且无法由 Citrix SSO 等第三方应用程序声明。因此，Citrix SSO 定义了一个新的扩展/MIME 类型，名为“.citrixsso-pfx”和“.citrixsso-p12”。管理员必须将用户证书的扩展名/MIME 类型分别从标准的“.pfx”或“.p12”更改为“.Citrixsso-pfx”或“.Citrixsso-p12”
。要重命名扩展，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 SSO 应用程序中安装证书。

## 为 **macOS** 用户设置 **Citrix SSO**

February 1, 2024

适用于 macOS 的 Citrix SSO 应用程序提供 Citrix 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访问关键业务应用程序、虚拟桌面和企业数据。
Citrix SSO 是 Citrix Gateway 的下一代 VPN 客户端，用于从 macOS 设备创建和管理 VPN 连接。Citrix SSO 是使用 Apple 的网络扩展 (NE) 框架构建的。来自 Apple 的 NE 框架是一个现代化的库，其中包含可用于自定义和扩展 macOS 的核心网络功能的 API。支持 SSL VPN 的网络扩展可在运行 macOS 10.11+ 的设备上使用。

Citrix SSO 应用程序替换了基于内核扩展 (KE) 的旧版 Citrix Gateway 插件，该插件将很快被 Apple 弃用。Citrix SSO 应用程序支持高级功能，如服务器启动的连接和 DTLS。

Citrix SSO 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 配置文件和每个应用程序 VPN 配置文件。
适用于 macOS 的 Citrix SSO 应用程序可以从 Mac 应用程序商店安装。

### **Citrix VPN** 与 **Citrix SSO** 之间的功能比较

下表比较了 Citrix VPN 和 Citrix SSO 之间的各种功能的可用性。

| 功能 | Citrix VPN | Citrix SSO |
| --- | --- | --- |
| 应用程序分发方法 | Citrix 下载页面 | App Store |
| 隧道连接数 | 128 | 128 |
| 从浏览器访问 | 支持 | 不支持 |
| 从本机应用程序访问 | 支持 | 支持 |
| 分割隧道（关闭/反向） | 支持 | 支持 |

| 功能 | Citrix VPN | Citrix SSO |
| --- | --- | --- |
| 拆分 DNS（本地/远程/两者） | 远程 | 远程 |
| 局域网接入 | 启用/禁用 | 始终启用 |
| 服务器启动的连接 (SIC) 支持 | 不支持 | 支持 |
| 转移登录 | 支持 | 支持 |
| 客户端代理 | 支持 | 不支持 |
| 经典/Opswat EPA 支持 | 支持 | 支持 |
| 设备证书支持 | 支持 | 支持 |
| 会话超时支持 | 支持 | 支持 |
| 强制超时支持 | 支持 | 支持 |
| 空闲超时支持 | 支持 | 不支持 |
| IPV6 | 不支持 | 支持 |
| 网络漫游（在 Wi-Fi、以太网等之间切换） | 支持 | 支持 |
| 内联网应用程序支助 | 支持 | 支持 |
| 对 UDP 的 DTLS 支持 | 不支持 | 支持 |
| EULA 支持 | 支持 | 支持 |
| 应用程序 + Receiver 集成 | 支持 | 不支持 |
| 身份验证—本地、LDAP、RADIUS | 支持 | 支持 |
| 客户端证书身份验证 | 支持 | 支持 |
| TLS 支持（TLS1、TLS1.1 和 TLS1.2） | 支持 | 支持 |
| 双重身份验证 | 支持 | 支持 |

### 与 **MDM** 产品的兼容性

Citrix SSO for macOS 与大多数 MDM 提供商兼容，例如 Citrix XenMobile、Microsoft Intune 等。它支持名为“网络访问控制 (NAC)”的功能，MDM 管理员可以通过该功能在连接到 Citrix Gateway 之前强制执行最终用户设备合规性。Citrix SSO 上的 NAC 需要 MDM 服务器，例如 XenMobile 或 Intune 和 Citrix Gateway。有关 NAC 的更多信息，请点击此处。

## 为 **Citrix SSO** 配置 **MDM** 托管 **VPN** 配置文件

以下部分以使用 Citrix Endpoint Management（以前称为 XenMobile）为例介绍了为 Citrix SSO 配置设备范围和 PerApp VPN 配置文件的分步说明。使用 Citrix SSO 时，其他 MDM 解决方案可以使用此文档作为参考。

> 注意：本部分介绍了基本设备范围和每个应用程序 VPN 配置文件的配置步骤。此外，您还可以按照 Citrix Endpoint Management（以前称为 XenMobile）文档或 Apple 的 MDM VPN 有效负载配置来配置始终启用的按需代理。

### 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 Citrix ADC 中定义的 VPN 策略（如全隧道、分割隧道、反向拆分隧道），来自所有应用程序和服务的流量都会通道到 Citrix Gateway。

**在 Citrix Endpoint Management 上配置设备级 VPN** 执行以下步骤来配置设备级 VPN。

1. 在 Citrix Endpoint Management MDM 控制台上，导航至配置 > 设备策略 > 添加新策略。
2. 在左侧的策略平台窗格中选择 **macOS** 。在右侧窗格中选择 **VPN** 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** 。

注意：在 MDM VPN 负载中，连接名称对应于 **UserDefinedName** 键，**VPN** 类型键必须设置为 **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 SSO 应用程序的捆绑标识符。

注意：在 MDM VPN 负载中，自定义 SSL 标识符对应于 **VPNSubType** 键。

6. 在提供程序捆绑包标识符中，输入 **com.citrix.NetScalerGateway.macOS.app.vpnplugin** 这是 Citrix SSO macOS 应用程序二进制文件中包含的网络扩展的捆绑标识符。

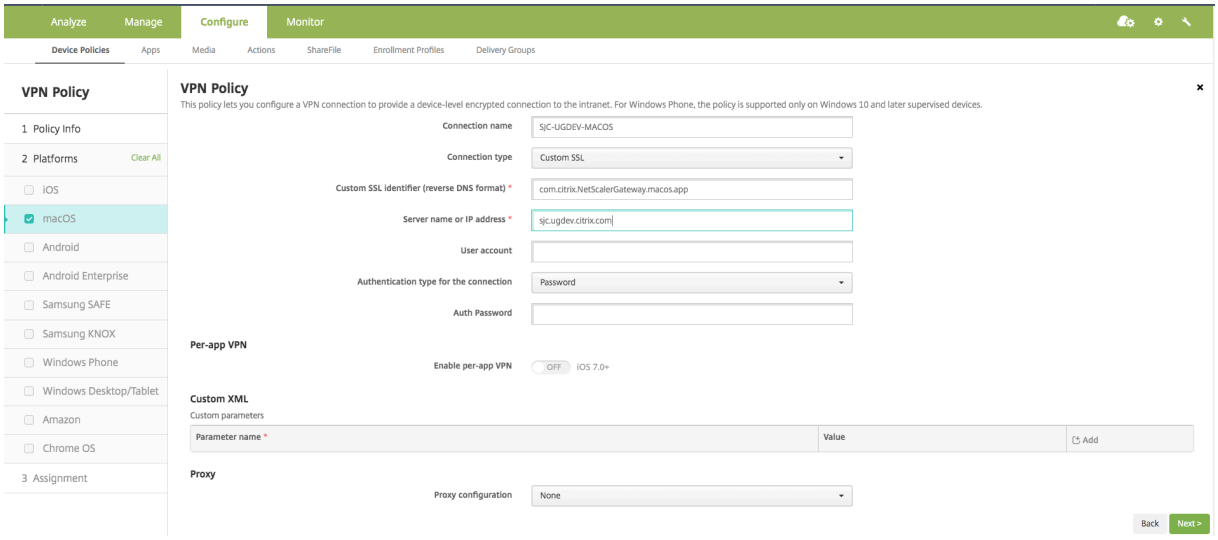
注意：在 MDM VPN 负载中，提供程序捆绑标识符对应于 **ProviderBundleIdentifier** 键。

7. 在服务器名称或 **IP** 地址中，输入与此 Citrix Endpoint Management 实例关联的 Citrix ADC 的 IP 地址或 FQDN。

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

8. 点击 下一步。




9. 单击保存。

每个应用程序 **VPN** 配置文件

每个应用程序的 VPN 配置文件用于为特定应用程序设置 VPN。只有特定应用程序的流量才会被隧道传送到 Citrix Gateway。每个应用程序 VPN 负载支持设备范围 VPN 的所有密钥以及一些附加密钥。

在 **Citrix Endpoint Management** 上配置每个 **PerApp** 级 **VPN**　执行以下步骤以在 Citrix Endpoint Management 上配置 PerApp VPN。

1. 完成 Citrix Endpoint Management 上的设备级 VPN 配置。

2. 打开“每个应用程序 **VPN**”部分中的“启 用每个应用程序 VPN”开关。

3. 如果应 在启动匹配应用程序 时自动启动 Citrix SSO，则启用按需匹配应用程序开关。建议在大多数每个应用程序的情况下使用此功能。

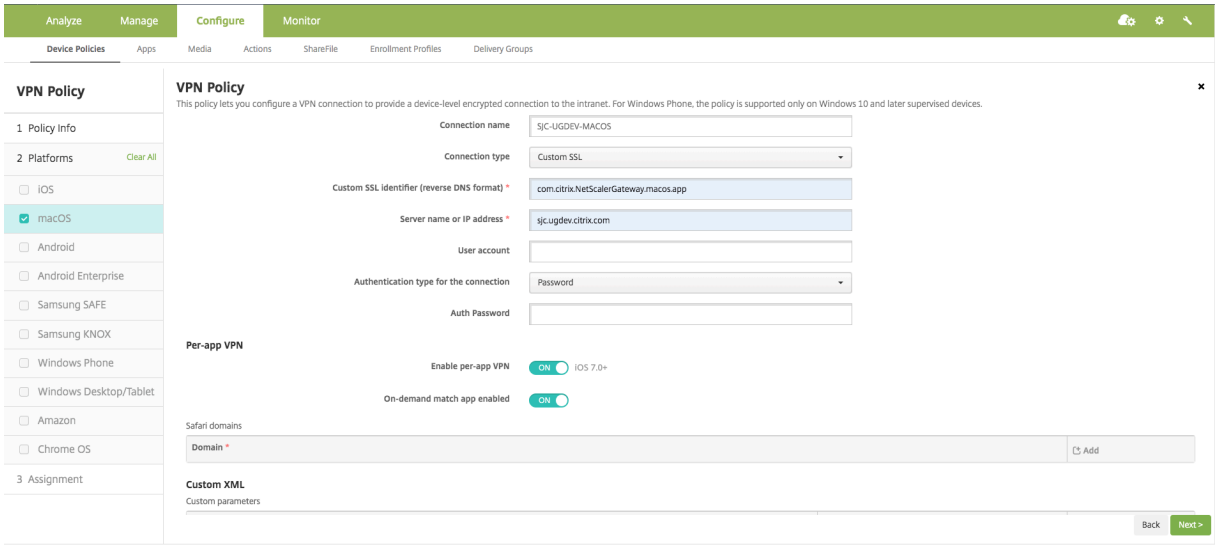
注意：在 MDM VPN 有效负载中，此字段对应于 **OnDemandMatchAppEnabled** 键。

5. Safari 域配置是可选的。配置 Safari 域后，Citrix SSO 会在用户启动 Safari 并导航到与“域”字段中的 URL 匹配的 URL 时自动启动。如果您想限制特定应用的 VPN，则不建议使用此操作。

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

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




13. 单击下一步。

14. 单击保存。

要将此 VPN 配置文件关联到设备上的特定应用程序，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/

### 在每个应用程序 **VPN** 中配置分割隧道

MDM 客户可以在每个应用程序 VPN 中为 Citrix SSO 配置分割隧道。为此，必须将以下键/值对添加到 MDM 服务器上创建的 VPN 配置文件的供应商配置部分。

```
- Key = "PerAppSplitTunnel"
- 值 = “真 或 1 或 是”
```

密钥区分大小写，并且应该完全匹配，而值不区分大小写。

注意：用于配置供应商配置的用户界面不是 MDM 供应商的标准。您必须与 MDM 供应商联系，以查找 MDM 用户控制台上的供应商配置部分。

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

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

### 禁用用户创建的 **VPN** 配置文件

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

```
- Key = "disableUserProfiles"
- 值 = “真 或 1 或 是”
```

密钥区分大小写，并且应该完全匹配，而值不区分大小写。

注意：用于配置供应商配置的用户界面不是 MDM 供应商的标准。您必须与 MDM 供应商联系，以查找 MDM 用户控制台上的供应商配置部分。

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

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

### 已知问题

以下是目前已知的问题。

- 如果用户被置于隔离组，则 EPA 登录失败。
- 不显示强制超时警告消息。
- 如果分割隧道处于开启状态且未配置 Intranet 应用程序，则 SSO 应用程序允许登录。

### 限制

以下是目前的限制。

- 某些 EPA 扫描（例如修补程序管理扫描、Web 浏览器扫描、终止进程）可能会失败，因为沙箱导致对 SSO 应用程序的访问受到限制。
- 不支持基于端口/协议的分割隧道。

### 常见问题解答

本部分捕获 Citrix SSO 应用程序的常见问题。

**Citrix SSO** 应用程序与 **Citrix VPN** 应用程序有何差别**?**
Citrix SSO 是适用于 Citrix ADC 的下一代 SSL VPN 客户端。该应用程序使用 Apple 的网络扩展框架来创建和管理 iOS 和 macOS 设备上的 VPN 连接。Citrix
VPN 是使用 Apple 的专用 VPN API 的旧版 VPN 客户端，现已弃用。对 Citrix VPN 的支持将在未来几个月从应用商店中删除。

什么是 **NE?** Apple
的网络扩展 (NE) 框架是一个现代化的库，其中包含可用于自定义和扩展 iOS 和 macOS 的核心网络功能的 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。

哪些版本的 **Citrix ADC** 与 **Citrix SSO** 兼容**?**
Citrix ADC 10.5 及更高版本支持 Citrix SSO 中的 VPN 功能。TOTP 在 Citrix ADC 12.0 及更高版本上可用。Citrix ADC 上的推送通知尚未
公开公布。该应用程序需要 iOS 9 以上和 macOS 10.11 以上版本。

非 **MDM** 客户的基于 **CERT** 的身份验证如何工作**?** 之前通过电子邮件或浏览器分发证书以便在 Citrix VPN 中执行客户端证书身份验证的客户必须在使用 Citrix SSO 时注意此更改。这主要适用于不使用 MDM 服务器分发用户证书的非 MDM 客户。请参阅“通过电子邮件将证书导入 Citrix SSO”以便能够分发证书。

什么是网络访问控制 **(NAC)?** 我如何使用 **Citrix SSO** 和 **Citrix Gateway** 配置 **NAC?**
Microsoft Intune 和 Citrix Endpoint Management（以前称为 XenMobile）MDM 客户可以利用 Citrix SSO 中的网络访问控制 (NAC) 功能。借助 NAC，管理员可以通过为由 MDM 服务器管理的移动设备添加额外的身份验证层来保护其企业内部网络的安全。管理员可以在 Citrix SSO 中进行身份验证时强制执行设备
合规性检查。

要将 NAC 与 Citrix SSO 一起使用，必须在 Citrix Gateway 和 MDM 服务器上启用它。

- 要在 Citrix ADC 上启用 NAC，请参阅此链接。
- 如果 MDM 供应商是 Intune，请参阅此链接。
- 如果 MDM 供应商是 Citrix Endpoint Management（以前称为 XenMobile），请参阅此链接。

注意：最低支持的 Citrix SSO 版本为 1.1.6 及更高版本。

## 在 **iOS** 和 **macOS** 上对 **Citrix SSO** 的 **nFactor** 支持

January 18, 2024

多因素 (nFactor) 身份验证通过要求用户提供多个识别证明来获取访问权限，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求按任意顺序进行配置。

Citrix SSO 支持以下身份验证协议：

- **nFactor** —当身份验证虚拟服务器绑定到 Gateway 关上的 VPN 虚拟服务器时，使用 nFactor 协议。由于身份验证因素的顺序是动态的，因此客户端使用在应用程序的上下文中呈现的浏览器实例来呈现身份验证 GUI。
- **Classic** —经典协议是在 Gateway 关上的 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 对于特定身份验证方法（如 NAC）失败，则传统协议是回退协议。
- **Citrix** 身份平台—在对 CloudGateway 或网关服务进行身份验证时使用 Citrix 身份平台协议，并且需要在 Citrix Cloud 中注册 MDM。

下表总结了每个协议支持的各种身份验证方法。

| 身份验证方法 | nFactor | 经典 | Citrix IdP |
| --- | --- | --- | --- |
| 客户端证书 | 支持 | 支持 | 不支持 |
| LDAP | 支持 | 支持 | 不支持 |
| 本地 | 支持 | 支持 | 不支持 |
| RADIUS | 支持 | 不支持 | 不支持 |
| SAML | 支持 | 不支持 | 不支持 |
| OAuth | 支持 | 不支持 | 不支持 |
| TACACS | 支持 | 不支持 | 不支持 |
| WebAuth | 支持 | 不支持 | 不支持 |
| 谈判 | 支持 | 不支持 | 不支持 |
| EPA | 支持 | 支持 | 不支持 |
| NAC | 不支持 | 支持 | 不支持 |
| StoreFront | 不支持 | 不支持 | 不支持 |
| 阿达尔 | 不支持 | 不支持 | 不支持 |
| DS-身份验证 | 不支持 | 不支持 | 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：要将 nFactor 协议与 Citrix SSO 结合使用，建议使用本地版本的 Citrix Gateway 为 12.1.50.xx 及更高版本。

限制

- nFactor 协议在默认情况下处于禁用状态。想要使用 nFactor 的客户必须明确请求 Citrix 支持并提供其 VPN 虚拟服务器 FQDN。
- 移动特定身份验证策略（如 NAC（网络访问控制））要求客户端发送签名设备标识符，作为 Citrix 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。此密钥嵌入到由 MDM 服务器管理的 VPN 配置文件中。可能无法将此密钥注入到 WebView 上下文中。如果在 MDM VPN 配置文件上启用了 NAC，Citrix SSO 会自动回退到传统身份验证协议。

# 常见问题解答

January 18, 2024

本部分捕获 Citrix SSO 应用程序的常见问题。

**Citrix SSO** 应用程序与 **Citrix VPN** 应用程序有何差别**?**
Citrix SSO 是适用于 Citrix ADC 的下一代 SSL VPN 客户端。该应用程序使用 Apple 的网络扩展框架来创建和管理 iOS 和 macOS 设备上的 VPN 连接。Citrix
VPN 是使用 Apple 的专用 VPN API 的旧版 VPN 客户端，现已弃用。对 Citrix VPN 的支持将在未来几个月从应用商店中删除。

什么是 **NE?** Apple
的网络扩展 (NE) 框架是一个现代化的库，其中包含可用于自定义和扩展 iOS 和 macOS 的核心网络功能的 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。

哪些版本的 **Citrix ADC** 与 **Citrix SSO** 兼容**?**
Citrix ADC 10.5 及更高版本支持 Citrix SSO 中的 VPN 功能。TOTP 在 Citrix ADC 12.0 及更高版本上可用。Citrix ADC 上的推送通知尚未
公开公布。该应用程序需要 iOS 9 以上和 macOS 10.11 以上版本。

非 **MDM** 客户的基于 **CERT** 的身份验证如何工作**?** 之前通过电子邮件或浏览器分发证书以在 Citrix VPN 中执行客户端证书身份验证的客户应在使用 Citrix SSO 时注意此更改。这
主要适用于不使用 MDM 服务器分发用户证书的非 MDM 客户。请参阅“通过电子邮件将证书导入 Citrix SSO”以便能够
分发证书。

什么是网络访问控制 **(NAC)?** 我如何使用 **Citrix SSO** 和 **Citrix Gateway** 配置 **NAC?**
Microsoft Intune 和 Citrix Endpoint Management（以前称为 XenMobile）MDM 客户可以利用 Citrix SSO 中的网络访问控制 (NAC) 功能。借助 NAC，管理员
可以通过为由 MDM 服务器管理的移动设备添加额外的身份验证层来保护其企业内部网络的安全。管理员可以在 Citrix SSO 中进行身份验证时强制执行设备
合规性检查。

要将 NAC 与 Citrix SSO 一起使用，必须在 Citrix Gateway 和 MDM 服务器上启用它。

- 要在 Citrix ADC 上启用 NAC，请参阅此链接。
- 如果 MDM 供应商是 Intune，请参考这个链接。
- 如果 MDM 供应商是 Citrix Endpoint Management（以前称为 XenMobile），请参阅此链接。

注意：最低支持的 Citrix SSO 版本为 1.1.6 及更高版本。

# 适用于 **Android** 设备的 **Citrix SSO**

January 18, 2024

Citrix SSO 提供 Citrix 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。

## 发行说明

January 19, 2024

Citrix SSO 发行说明描述了服务版本中可用的新功能、现有功能的增强功能、已修复问题和已知问题。发行说明包含下面的一个或多个部分：

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：当前版本中已修复的问题。

已知问题：当前版本中存在的问题及其解决方法（无论是否适用）。

### V2.3.14

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]

已知问题

- 在应用程序用户界面中，始终在 VPN 状态并不总是正确更新。

  [NSHELP-21709]

### V2.3.13

已修复的问题

- Citrix Gateway IP 地址现在只解析一次。

  之前，Citrix Gateway IP 地址已多次解析，有时会导致连接失败。

  [CGOP-12101]

已知问题

- 在应用程序用户界面中，始终在 VPN 状态并不总是正确更新。

  [NSHELP-21709]

## V2.3.12

已修复的问题

- Citrix SSO 可能会在保存 VPN 配置文件时崩溃。

  [CGOP-12137]

## V2.3.11

已修复的问题

- Citrix SSO 可能会在保存 VPN 配置文件时崩溃。

  [CGOP-12137]

- 当新的 VPN 配置文件或更新到现有配置文件导致 disableUserProfile 值的更改时，disableUserProfile 设置未正确反映在用户界面中。

  [CGOP-11899]

- 适用于 Android 的 Citrix SSO 不处理设备所有者 (DO) 模式下的 VPN 配置文件。

  [CGOP-11981]

- 如果只有 IPv6 本地 DNS 服务器，则不会建立 VPN 连接。

  [CGOP-12053]

## V2.3.10

已修复的问题

- VPN 连接在设备上的一段空闲时间后丢失。

  [CGOP-11381]

## V2.3.8

新增功能

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

  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** 设置 **VPN** 配置文件

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

  [CGOP-631]

已修复的问题

- 如果您保存已保存的令牌，然后尝试打开它，则令牌名称中会显示乱码字符。

  [CGOP-11696]

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

  [CGOP-11259]

## V2.3.6

新增功能

- **Citrix SSO** 的 **AlwaysON** 支持

  Citrix SSO 的 AlwaysOn 功能可确保用户始终连接到企业网络。这种持久的 VPN 连接是通过自动建立 VPN 隧道来实现的。

  [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，则会显示一条通知，提示用户重新登录到 Citrix Workspace。

  - 在 Citrix Workspace 预配置的 VPN 配置文件中启用了 AlwaysOn 功能
  - 雅典娜身份验证用于 SSO
  - 由于雅典娜令牌过期，用户已退出 Citrix Workspace 应用程序

  [CGOP-10016]

- 推送通知服务的注册使用 **Citrix Gateway** 完成

  现在，您可以使用 Citrix Gateway 设备注册推送通知服务。早些时候，在客户端设备上完成了注册。

  [CGOP-10542]

已修复的问题

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

[CGOP-10818]

## V2.3.1

新增功能

- 更新托管配置以包含更多用户设置

  托管配置更新为包括 Android Enterprise 环境的 “BlockUntrustedServers”、“DefaultProfileName” 和 “DisableUserProfiles” 设置。

  [CGOP-10033]

- 增强的推送通知支持

  在将 Citrix Gateway 配置为类型为 “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进行身份验证的推送通知后，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 应用程序的使用信息。该增强功能适用于粗糙的地理定位、屏幕使用、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 https://info.citrite.net/x/8TIFTw

### V2.2.9

新增功能

- 推送通知支持

  Citrix Gateway 在已注册的移动设备上发送推送通知，以获得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 SSO** 应用

January 18, 2024

要在 MDM 环境中设置 Citrix SSO 应用程序，请参阅为 Android 配置 Citrix SSO 协议。

注意：

- 在非 MDM 电子商务中，用户手动创建 VPN 配置文件。
- 还可以为 Citrix SSO 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。

## 在 **Intune Android Enterprise** 环境中设置 **Citrix SSO** 应用程序

February 1, 2024

本主题捕获有关通过 Microsoft Intune 部署和配置 Citrix SSO 应用程序的详细信息。本文档假定 Intune 已配置为 Android Enterprise 支持，并且设备注册已完成。

必备条件

- Intune 配置为 Android Enterprise 支持
- 设备注册完成

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

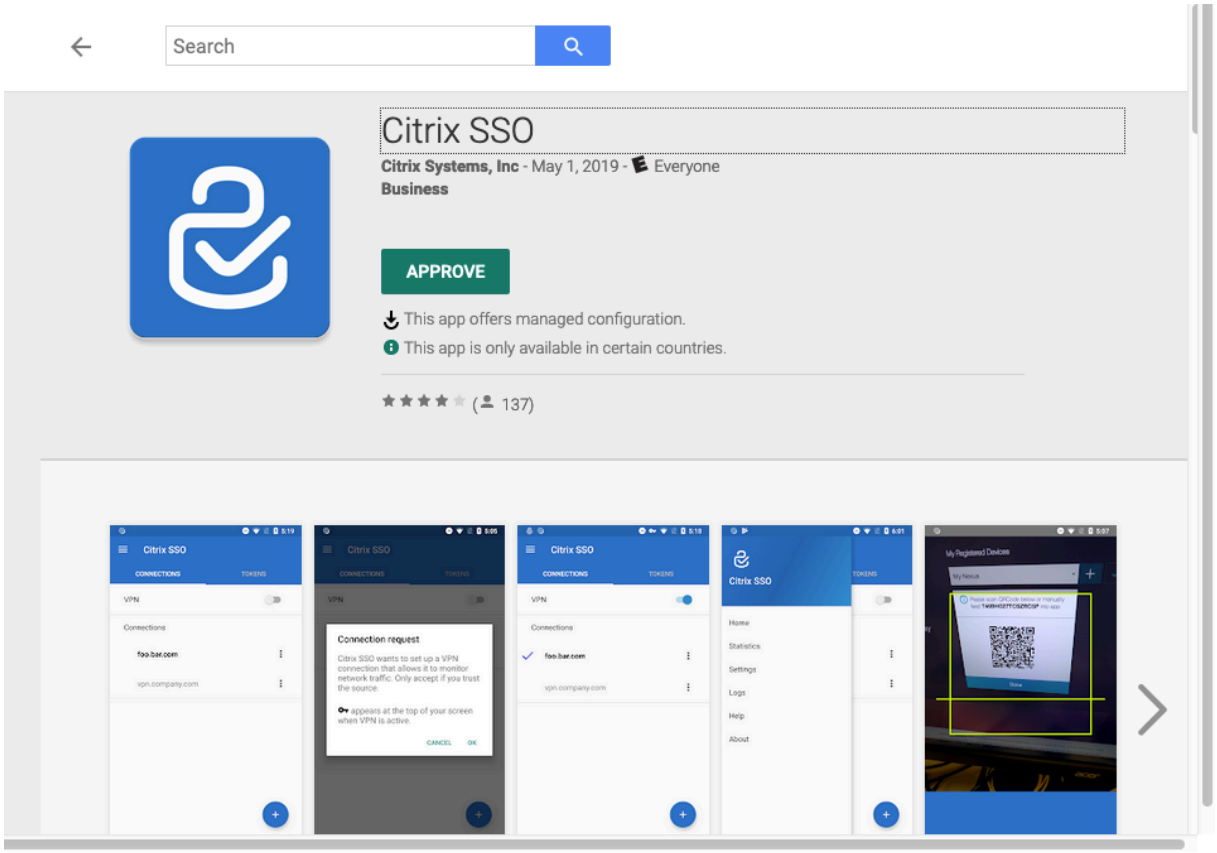
- 将 Citrix SSO 应用程序添加为托管应用程序
- 为 Citrix SSO 应用配置托管应用策略

将 **Citrix SSO** 应用程序添加为托管应用程序

1. 登录到 Azure 门户。
2. 单击左侧导航刀片上的 **Intune**。
3. 单击 Microsoft Intune 刀片中的客户端应用程序，然后单击客户端应用程序刀片中的应用程序。
4. 单击右上角菜单选项中的 **+** 添加 链接。此时将显示“添加应用程序配置”刀片。
5. 为应用类型选择 托管 **Google Play** 。

这增加了管理 Google Play 搜索和批准刀片，如果你已经配置了 Android Enterprise.

6. 搜索 Citrix SSO 应用并从应用列表中选择它。




注意：如果 Citrix SSO 未显示在列表中，则表示该应用在您的国家/地区不可用。

7. 单击 批准 以批准 Citrix SSO 通过托管 Google Play 商店进行部署。

将列出 Citrix SSO 应用程序所需的权限。

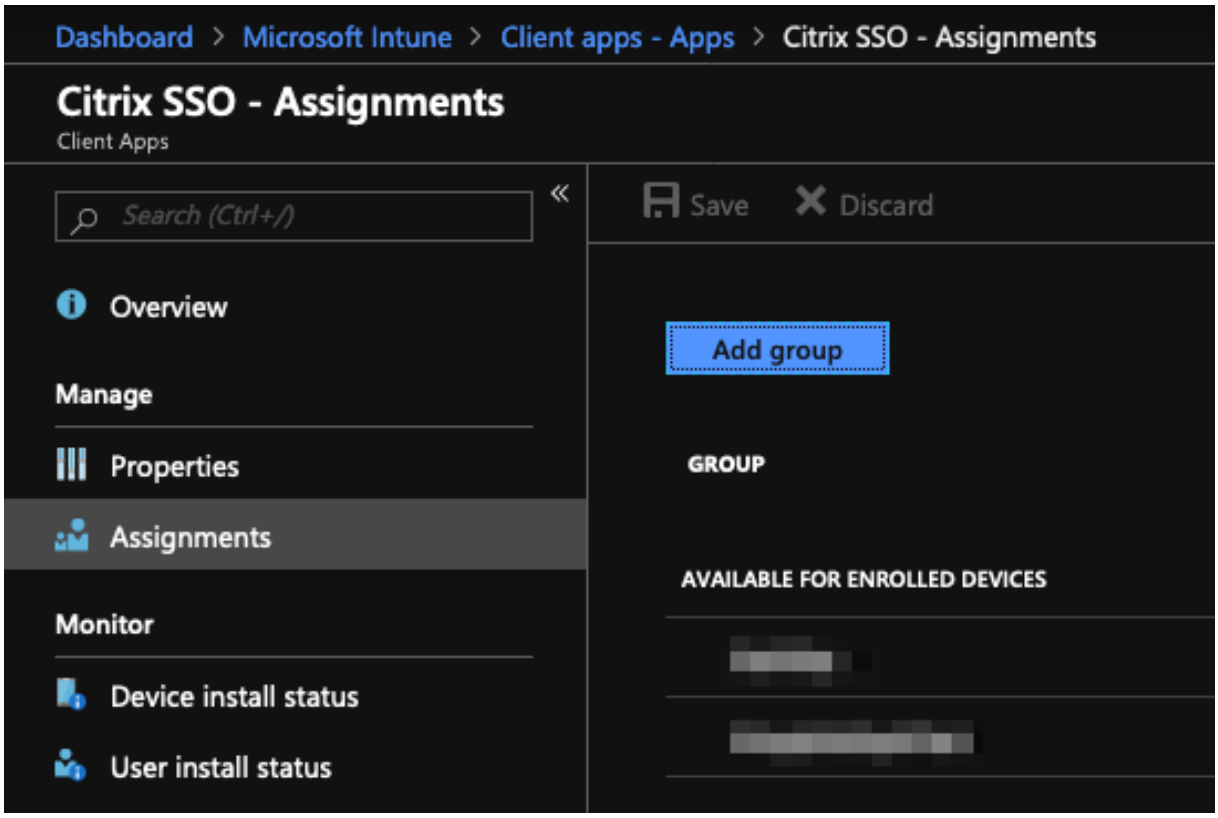
8. 单击 批准 以批准部署应用程序。

9. 单击“同步”以将此选择与 Intune 同步。

Citrix SSO 应用程序将添加到客户端应用程序列表中。如果添加了多个应用程序，则可能需要搜索 Citrix SSO 应用程序。

10. 单击 **Citrix SSO** 应用以 打开应用详细信息刀片。

11. 单击详细信息刀片中的 任务。**Citrix SSO**-分配 刀片出现.




12. 单击“添加组”以分配要向其授予安装 Citrix SSO 应用权限的用户组，然后单击“保存”。

13. 关闭 Citrix SSO 应用详细信息刀片。

将添加并启用 Citrix SSO 应用程序，以便将其部署到您的用户。

### 为 **Citrix SSO** 应用配置托管应用策略

添加 Citrix SSO 应用程序后，必须为 Citrix SSO 应用程序创建托管配置策略，以便可以将 VPN 配置文件部署到设备上的 Citrix SSO 应用程序。

1. 在 Azure 门户中打开 **Intune** 刀片。

2. 从 Intune 刀片打开客户端应用程序刀片。

3. 从客户端 应用程序刀片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 刀片。

4. 输入策略的名称并为其添加描述。

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 关联的应用程序，然后选择 **Citrix SSO** 应用程序。

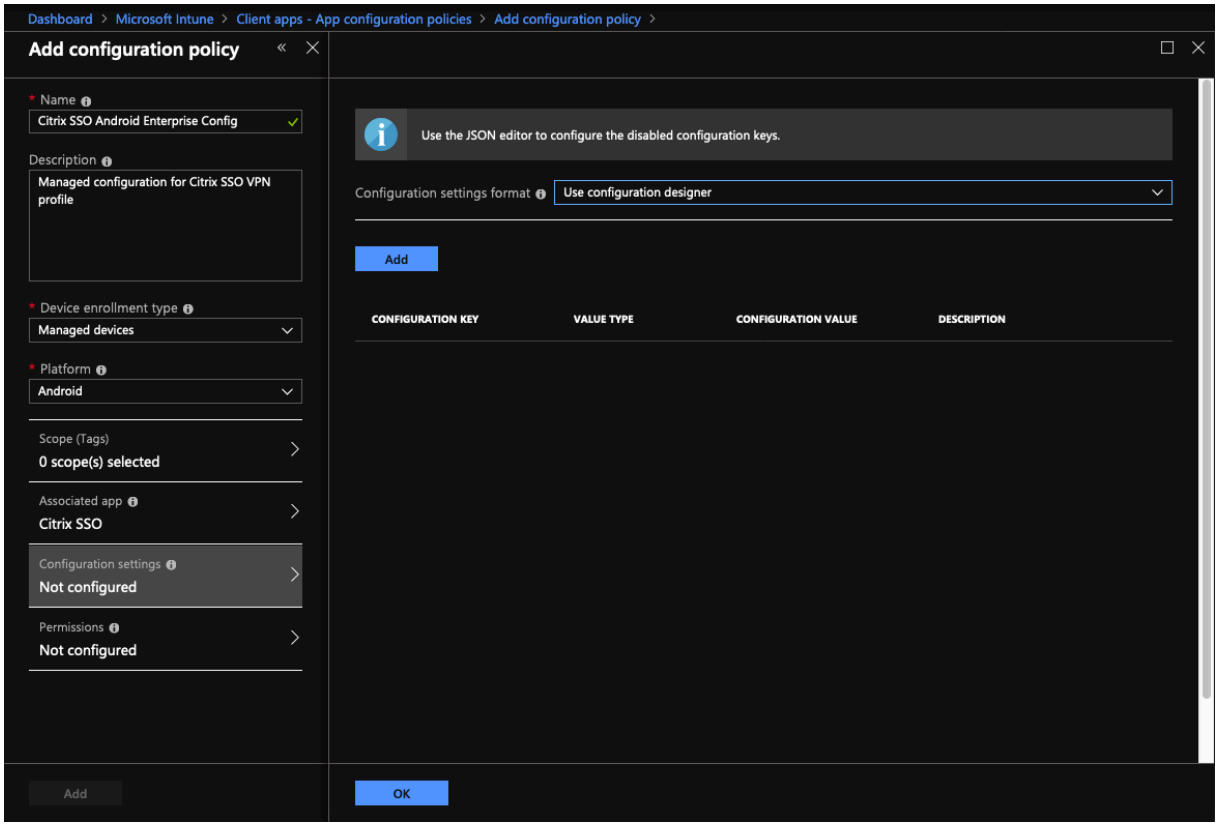
如果你有很多应用程序，你可能需要搜索它。

8. 单击确定。添加配置策略叶片中添加了配置设置选项。

9. 点击 配置 设置。

此时将显示用于配置 Citrix SSO 应用的刀片。

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 SSO 应用程序。




注意：对于简单的 VPN 配置，建议使用配置设计器。

使用用户配置设计器的 **VPN** 配置　1. 在“配置设置”中，选择“使用配置设计器”，然后单击“添加”。

将显示一个键值输入屏幕，用于配置 Citrix SSO 应用程序支持的各种属性。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 描述 部分以获取有关每个属性的详细信息。

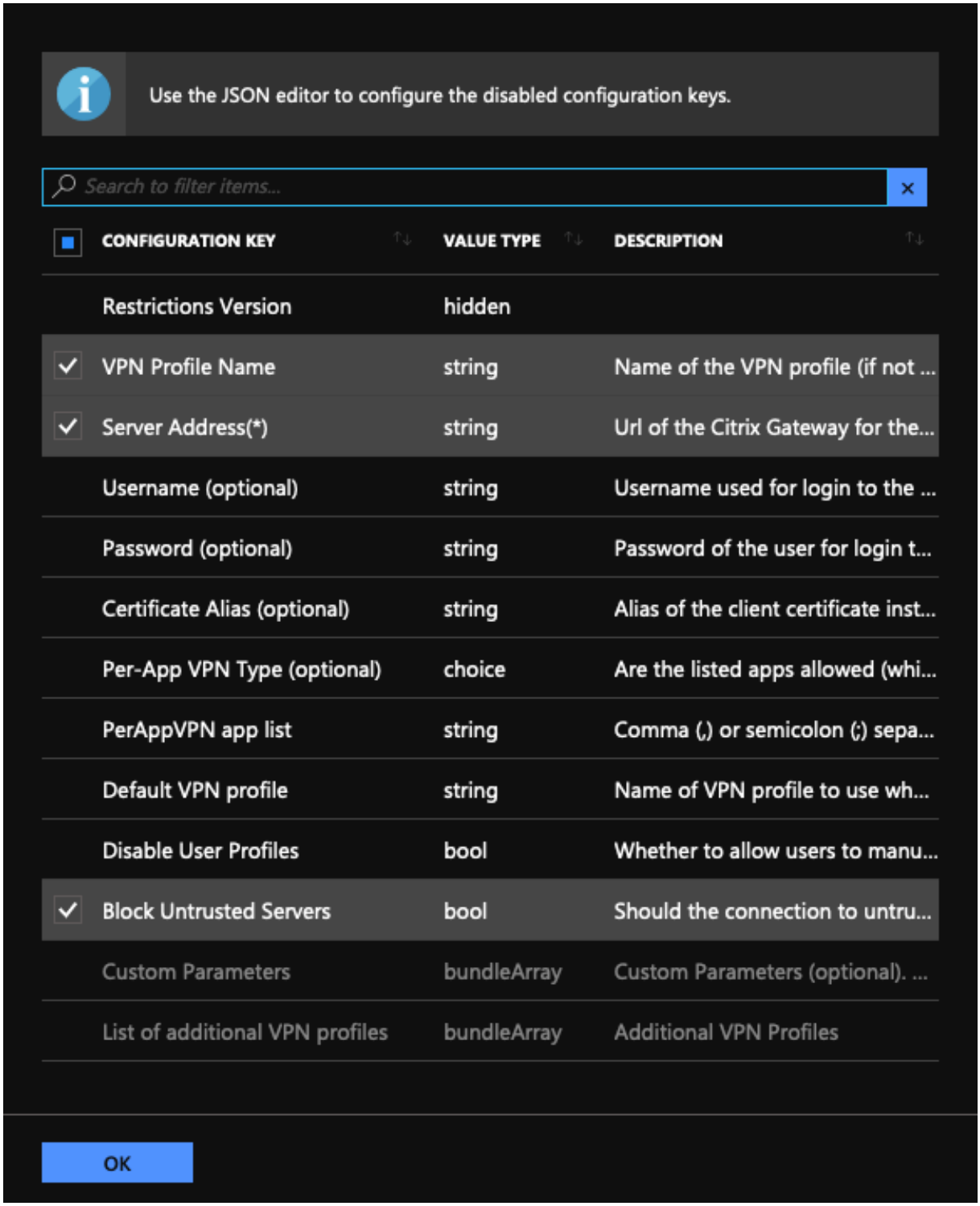
 

2. 例如，选择 **VPN** 配置文件名称 和 服务器地址 **(*)** 属性，然后单 击确定。

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，则您在“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 Citrix Gateway 基础 FQDN。如果 Citrix 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）。输入最终用户用于对 Citrix Gateway 进行身份验证的用户名。如果 Gateway 已配置为使用 Intune 配置值令牌，则可以为此字段使用该值令牌（请参阅配置值令牌）。如果不提供用户名，系统会提示用户在连接到 Citrix Gateway 时提供用户名。
- 密码（可选）。输入最终用户用于对 Citrix Gateway 进行身份验证的密码。如果不提供密码，系统会提示用户在连接到 Citrix Gateway 时提供密码。
- 证书别名（可选）。在 Android 密钥库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。
- 每个应用程序 **VPN** 类型（可选）。如果您使用 PerApp 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”，则 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“禁止”，则 PerAppVPN 应用程序列表中列出的应用程序包名称的网络流量将在 VPN 之外路由。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 SSO 应用配置始终在线 VPN 时使用的 VPN 配置文件名称。如果此字段为空，则主配置文件将用于连接。如果只配置了一个配置文件，则将其标记为默认 VPN 配置文件。




注意：

- 若要在 Intune 中使 Citrix SSO 应用程序成为永远在线 VPN 应用程序，请使用 VPN 提供商作为自定义，并使用 COM.CitrixVPN 作为应用程序包名称。

> - Citrix SSO 应用程序始终在线 VPN 仅支持基于证书的客户端身份验证。
> - 管理员必须在 Citrix Gateway 的 SSL 配置 文件或 **SSL** 属性 中选择 客户端 身 份验证，并将客户端证书设置为强制，以便 SSO 应用按预期工作。

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

  默认值为 false。
- 阻止不受信任的服务器
  - 为 Citrix Gateway 使用自签名证书时，或颁发 Citrix Gateway 证书的 CA 的根证书不在系统 CA 列表中时，请将此值设为 false。
  - 将此值设置为 true 以启用 Android 操作系统验证 Citrix Gateway 证书。如果验证失败，则不允许连接。

  默认值为 true。

3. 对于 服务器地址 **(*)** 属性，请输入您的 Gateway 基本 URL（例如，`https://vpn.mycompany.com`）。

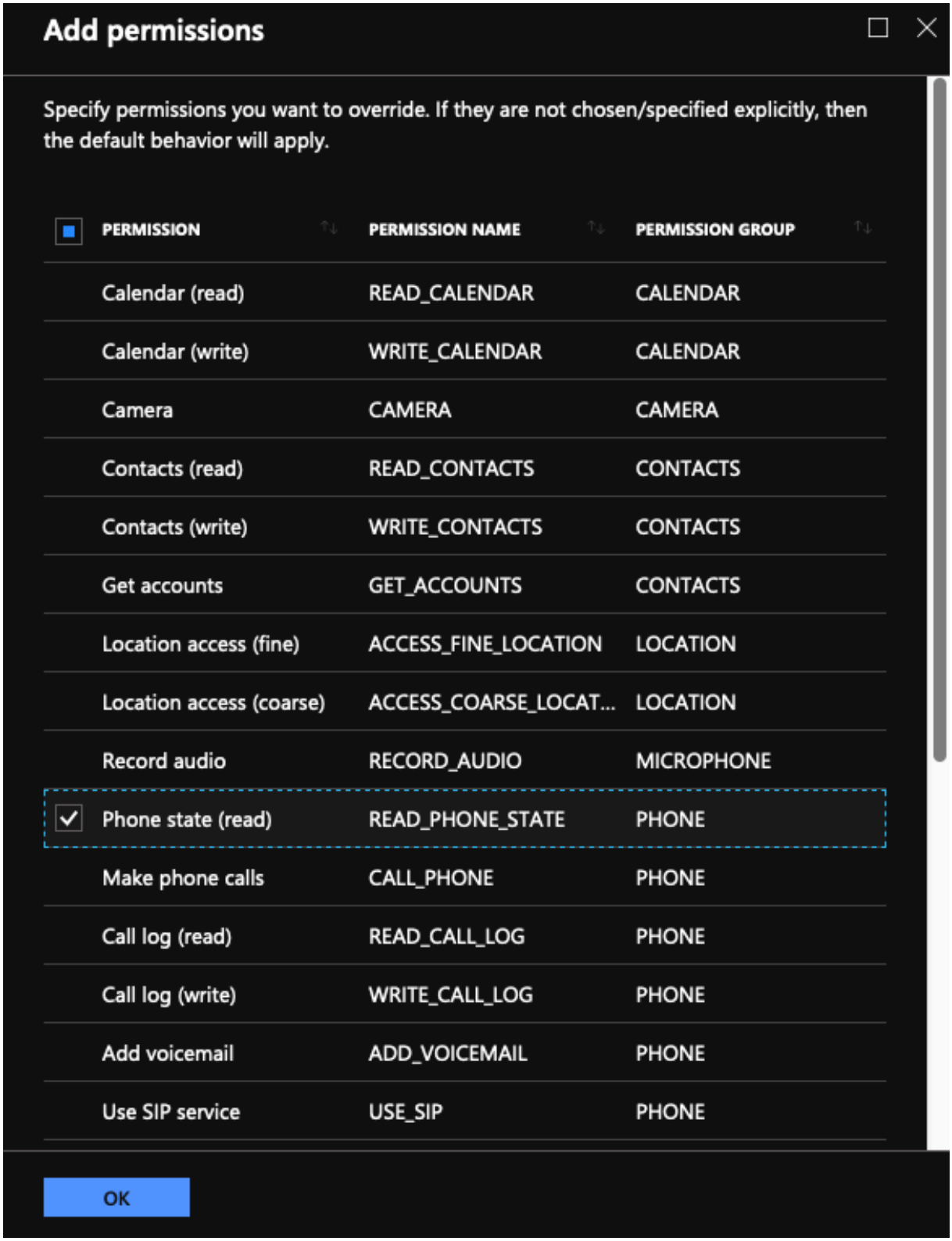
4. 对于 **VPN** 配置文件名称，请在 Citrix SSO 应用程序的主屏幕（例如，我的企业 VPN）中输入对最终用户可见的名称。

5. 您可以根据 Citrix Gateway 部署添加和配置其他属性。完成配置后，单 击确定。

6. 点击 权限 部分。在本节中，您可以授予 Citrix SSO 应用所需的权限。

- 如果您使用的是 Intune NAC 检查，Citrix SSO 应用程序要求您授予电话状态（读取）权限。单击 添加 按钮以打开权限刀片。目前，Intune 显示可供所有应用程序使用的权限的重要列表。
- 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。这将其添加到应用程序的权限列表中。选择“提示”或“自动授予”，以便 Intune NAC 检查可以工作，然后单击“确定”。




7. 单击应用配置策略刀片底部的“添加”以保存 Citrix SSO 应用的托管配置。

8. 单击应用程序配置策略刀片中的任务以打开 任务 刀片。

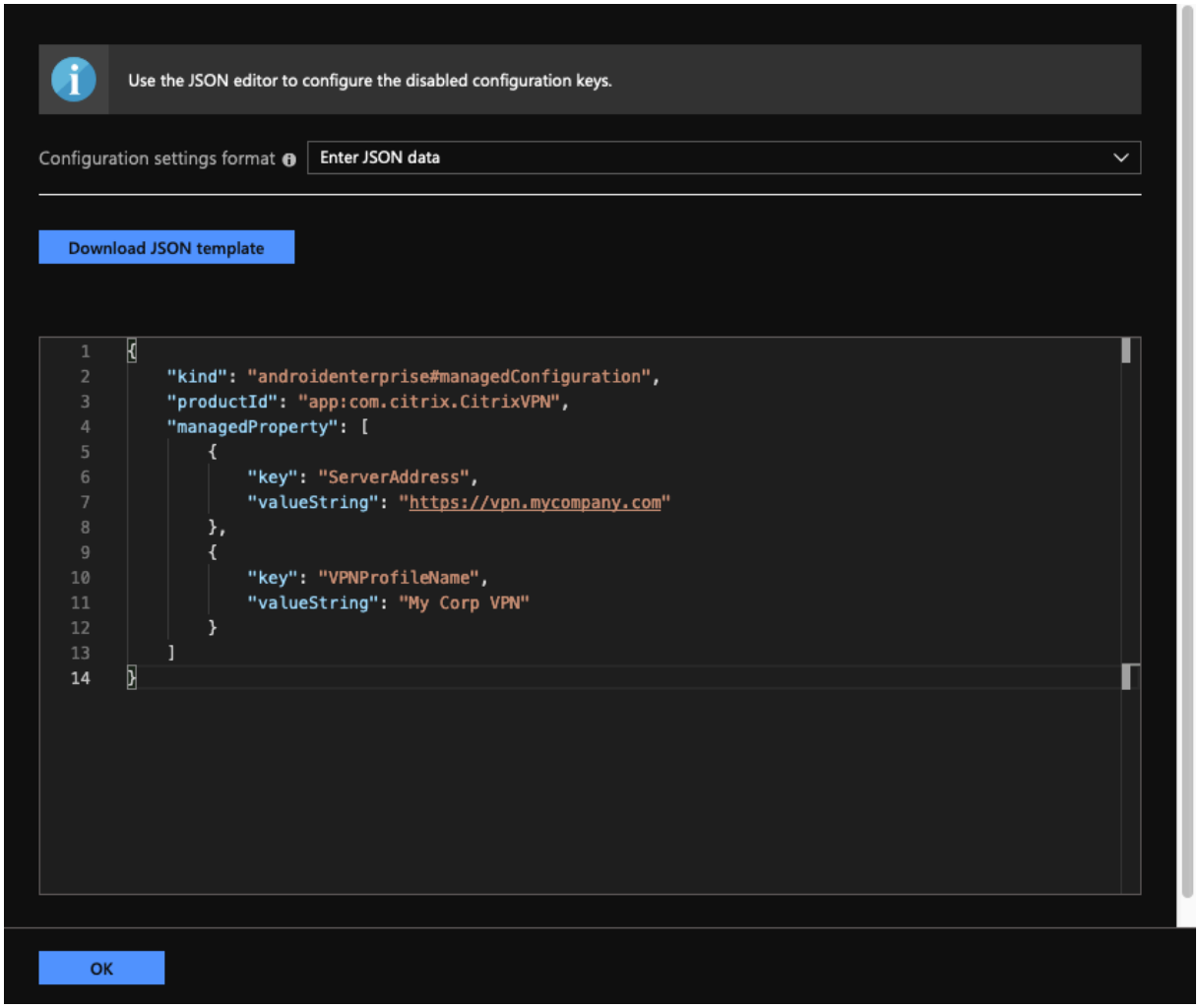
9. 选择要为其传递和应用此 Citrix SSO 配置的用户组。

通过输入 **JSON** 数据进行 **VPN** 配置　1. 在“配置设置”中，选择“输入 **JSON** 数据以配置 Citrix SSO 应用程序”。

2. 使用“下载 JSON 模板”按钮下载允许为 Citrix SSO 应用程序提供更详细/复杂配置的模板。此模板是一组 JSON 键值对，用于配置 Citrix SSO 应用程序理解的所有可能属性。

有关可配置的所有可用属性的列表，请参阅用于在 Citrix SSO 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，以下是上面使用配置设计器选项创建的基本配置的 JSON 模板。




这完成了在 Microsoft Intune Android Enterprise 环境中配置和部署 Citrix SSO 应用的 VPN 配置文件的过程。

重要提示：用于基于客户端证书的身份验证的证书通常使用 Intune SCEP 配置文件进行部署。应在 Citrix SSO 应用的托管配置的“证书别名”属性中配置此证书的别名。

用于在 **Citrix SSO** 应用程序中配置 **VPN** 配置文件的可用属性

| 配置密钥 | 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（如果未将默认设置为服务器地址）。 |
| 服务器地址 (*) | ServerAddress | URL | 连接的 Citrix Gateway 的基本 URL (https://host[:port])。这是必填字段。 |
| 用户名 (可选) | 用户名 | 文本 | 用于使用 Citrix Gateway 进行身份验证的用户名（可选）。 |
| 密码 (可选) | 密码 | 文本 | 用于使用 Citrix Gateway 进行身份验证的用户密码（可选）。 |
| 证书别名 (可选) | ClientCertAlias | 文本 | 安装在 Android 凭据存储中的用于基于证书的客户端身份验证的客户端证书别名（可选）。 |
| PerApp VPN 类型 (可选) | PerAppVPN_Allow_Disallow_Setting | 枚举 (允许, 不允许) | 列出的应用程序是否允许（白名单）或禁止（黑名单）使用 VPN 隧道。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 进行隧道。如果设置为“禁 止”，则允许除列出的应用以外的所有应用程序通过 VPN 进行隧道。如果未列出任何应用程序，则允许所有应用程序通过 VPN 进行隧道。 |
| PerAppVPN 应用程序列表 | PerAppName_Appnames | 文本 | 每个应用 VPN 的应用程序包名称的逗号 (、) 或分号 (;) 分隔列表。软件包名称必须与 Google Play 商店应用列表页面 URL 中显示的完全相同。软件包名称区分大小写。 |

| 配置密钥 | JSON 字段名称 | 值类型 | 说明 |
| --- | --- | --- | --- |
| 默认 VPN 配置文件 | DefaultProfileName | 文本 | 系统启动 VPN 服务时要使用的 VPN 配置文件的名称。此设置用于识别在设备上配置始终在线 VPN 时要使用的 VPN 配置文件。 |
| 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** 可禁用用户创建 VPN 配置文件。默认值为 **false**。 |
| 阻止不受信任的服务器 | BlockUntrustedServers | 布尔值 | 用于确定与不受信任网关的连接（例如，使用自签名证书或颁发 CA 时不受 Android 操作系统信任）是否被阻止？默认值为 true（阻止与不受信任网关的连接）。 |
| 自定义参数（可选） | CustomParameters | 列表 | Citrix SSO 应用程序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 Citrix Gateway 文档以获取可用的选项。 |
| 其他 VPN 配置文件的列表 | bundle_profiles | 列表 | 附加 VPN 配置文件列表。支持每个配置文件的上述大多数值。有关详细信息，请参阅 支持的属性列表。 |

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。 |

**VPN** 配置文件列表中每个 **VPN** 的支持属性　使用 JSON 模板配置多个 VPN 配置文件时，每个 VPN 配置文件都支持以下属性。

| 配置密钥 | JSON 字段名称 | 值类型 |
| --- | --- | --- |
| VPN 配置文件名称 | bundle_VPNProfileName | 文本 |
| 服务器地址 (*) | bundle_ServerAddress | URL |
| 用户名 | bundle_Username | 文本 |
| 密码 | bundle_Password | 文本 |
| 客户 | bundle_ClientCertAlias | 文本 |
| 每个应用程序 VPN 类型 | bundle_PerAppVPN_Allow_Disallow_Setting | 枚举（允许，不允许） |
| PerAppVPN 应用程序列表 | bundle_PerAppVPN_Appnames | 文本 |
| 自定义参数 | bundle_CustomParameters | 列表 |