

# Lantern VPN

2026-02-01

## 目录

<b>下载与更新</b>	<b>2</b>
下载	2
GitHub	2
网站	2
电子邮件	2
正在更新	2
检查版本	3
<b>特征</b>	<b>4</b>
分裂隧道	4
<b>安装</b>	<b>4</b>
桌面	4
iOS	4
安卓	5
Google Play 商店	5
侧装式	5
<b>Lantern Pro</b>	<b>5</b>
兑换 Lantern Pro 许可证/激活码	5
设置和重置 Lantern Pro 密码	6
<b>安全</b>	<b>6</b>
推荐资源	6
验证文件下载	6
MacOS 或 Linux	7
	7
<b>故障排除</b>	<b>7</b>
设备关联码邮件未送达。	7
重置代理配置	8
视窗	8

将网站安装为应用程序（桌面版）	8
火狐浏览器	8
铬合金	8
Microsoft Edge	8
Safari（macOS Sonoma 14 或更高版本）	9
提交问题报告	9
应用程序问题报告	9
其他问题报告方法	9
日志检索	10
高级诊断	11

## 下载与更新

### 下载

#### GitHub

所有下载文件，包括备份和测试版，均可在以下网址获取：<https://github.com/getlantern>

#### 网站

请从以下网址下载我们的最新稳定版本：<https://lantern.io/download>

#### 电子邮件

电子邮件为分发应用程序下载提供了一个可靠且不易被屏蔽的渠道。

向以下任一电子邮件地址发送电子邮件，即可收到我们针对每个平台的最新稳定版本的链接。

使用	地址
通用的	downloads@getlantern.org, download@getlantern.org
中国	chinadownloads@getlantern.org, chinadownload@getlantern.org
俄罗斯	russiadownloads@getlantern.org, russiadownload@getlantern.org
伊朗	irandownloads@getlantern.org, irandownload@getlantern.org

### 正在更新

1. 打开灯笼
2. 导航至Account

3. 选择Settings

4. 选择Check for Updates

如果应用程序无法完成更新，请按照下载说明进行更新。

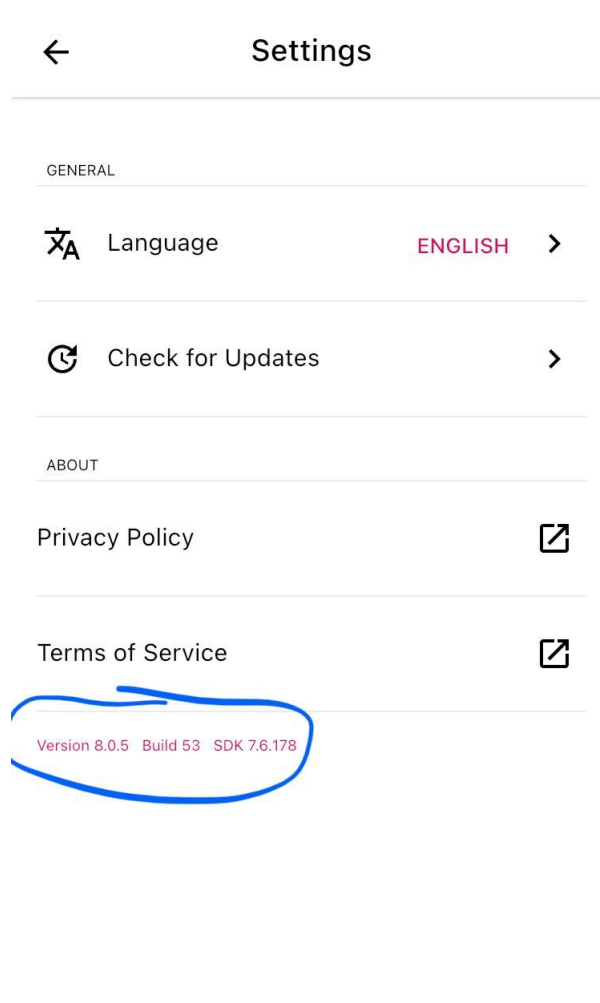
### 检查版本

1. 打开灯笼

2. 导航至Account

3. 选择Settings

4. 版本号显示在屏幕底部。



查看我们的发行说明，了解哪个版本是最新版本，并始终确保您已更新到最新版本，以便访问最新的协议和最有效的代理。

## 特征

### 分裂隧道

分离隧道技术可以指定哪些应用和网站使用代理，哪些直接连接。由于通过代理路由 VPN 连接会增加延迟并降低速度，因此最快的连接只会代理那些需要代理的流量。被屏蔽或受限的内容可以通过代理路由，而其余流量则直接连接以获得尽可能快的速度。

如果您发现整体网络速度低于理想水平，请尝试启用拆分隧道，并测试哪些应用程序或网站受益最大！

另请参阅：<https://lantern.io/faq#privacy-4>

## 安装

### 桌面

直接从GitHub下载适用于 Windows、MacOS 或 Linux 的 Lantern。

参与 Beta 测试的用户和新版本早期用户在安装时可能会看到恶意软件警告。此消息可以忽略。

### iOS

下载适用于 iOS 的 Lantern 需要使用位于非限制国家或地区的 Apple ID。如果您目前拥有有效的付款方式，且账单地址位于非限制地区，您可以按照Apple的说明将您的 Apple ID 位置更新为该国家或地区。否则，您需要创建一个备用 Apple ID：

1. 在不受限制的国家或地区设置新的 Apple ID
2. 退出 iCloud（数据和资金可能无法转移到新帐户。）
3. 创建新帐户
4. 使用未关联的电子邮件进行验证
5. 选择一个不受限制的国家/地区

更多详情请参阅CNET 的这篇文章。

【注意】“账单详情”需要填写地址，但您可以选择新国家或地区的任何公共地址（例如图书馆地址）继续操作。付款方式并非必填项。

## 安卓

### Google Play 商店

从Google Play 商店下载 Lantern，安装最简便。

### 侧装式

无法通过应用商店获取 Lantern 的用户可以手动安装 Lantern APK。

在 Android 14 上：

1. 从应用启动器打开Settings
2. 选择Apps
3. 选择Special app access
4. 选择Install unknown apps ，然后通过切换Allow from this source选项，选择要允许哪些应用（文件管理器或浏览器）将 APK 文件安装到您的设备上。
5. 从GitHub下载适用于 Android 的 Lantern APK。
6. 下载完成后，在网页浏览器或文件管理器中打开下载文件夹中的 APK 文件，然后选择Install
7. 如果安装成功，应用安装完成后，您会收到确认信息。

【注意】如果您使用网页浏览器或 Chrome 安装 Lantern，系统会提示您即将下载的文件可能有害。下载 APK 文件时始终会显示此警告，您可以忽略它。

## Lantern Pro

### 兑换 Lantern Pro 许可证/激活码

1. 在当前未登录的设备上，从主屏幕选择“升级到专业版”按钮
2. 选择屏幕右上角的三个点菜单图标
3. 选择“Lantern Pro 许可证”选项

4. 输入电子邮件地址，或者选择“使用 Google 帐户继续”或“使用 Apple 帐户继续”选项（如果适用）（**注：如果您拥有专业帐户，只需返回菜单并选择登录即可**）
5. 请输入发送到您邮箱的确认码（**不适用于“使用 Google 继续”或“使用 Apple 继续”选项**）
6. 将 25 位数的 Lantern Pro 许可证代码复制粘贴到文本框中，然后选择“激活 Lantern Pro”。

## 设置和重置 Lantern Pro 密码

在版本 9 中，我们引入了新的登录选项，允许用户使用电子邮件地址和自定义密码来授权设备。要设置密码，请按照以下说明操作：

1. 从主屏幕左上角的菜单中选择“登录”。
2. 请输入您的 Lantern Pro 电子邮件地址
3. 选择“忘记密码”
4. 请按照屏幕和电子邮件收件箱中的说明进行操作
5. 使用相同的 Lantern Pro 电子邮件地址和新密码登录 Lantern Pro

## 安全

### 推荐资源

您的安全需求可能因您所在的位置、您的具体需求以及您所面临的威胁模型而异。Lantern 推荐以下资源，帮助您了解和确定您的特定安全需求。

- 《消费者报告》| 安全规划师 ( <https://securityplanner.consumerreports.org/> )
- Miaan 数字安全服务台 | 协助 ( <https://miaan.org/projects/miaan-digital-security-helpdesk/> )

### 验证文件下载

如何验证客户端应用程序文件的真实性，即使该文件是通过不受信任的网络下载的。

哈希函数可用于为任何文件创建唯一的数字签名——哈希值。Lantern 会在应用程序编译时捕获此哈希值，并将其发布到 GitHub 上的 lantern-binaries 仓库。用户可以对下载的文件副本运行相同的哈希函数（SHA256），以确保它们完全匹配，从而证明该文件是原始文件的真实且未被篡改的副本。

大多数操作系统都内置了哈希函数。请按照以下步骤，根据您的操作系统生成文件的哈希值。

**【重要】** 请务必将C:\file\path\my\_file.exe或/ path/ to/ my\_file替换为文件的实际路径。

## MacOS 或 Linux

在您常用的终端应用程序中，运行以下命令：

```
openssl dgst -sha256 /path/to/my_file
```

## 命令提示符

1. 按Windows + R打开“运行”对话框
2. 输入cmd并单击确定。
3. 命令提示符窗口将会打开。
4. 运行以下命令：

```
Power Shell certutil -hashfile C:\file\path\my_file.exe SHA256
```

- (a) 按Windows + R打开“运行”对话框
- (b) 输入powershell并单击确定。
- (c) Windows PowerShell 窗口将会打开。
- (d) 运行以下命令： console Get-FileHash C:\file\path\my\_file.exe -Algorithm SHA256

## 故障排除

### 设备关联码邮件未送达。

部分邮箱服务商（@qq.com、@126.com、@163.com等）可能无法发送设备绑定码。请尝试将您的账户邮箱更改为已知可靠的邮箱服务商：

- 前景
- iCloud邮件
- 雅虎邮箱

- Gmail
- Proton Mail是一款免费、非营利、注重隐私的电子邮件服务提供商。在中国，使用 Proton Mail 需要 VPN。

## 重置代理配置

### 视窗

某些 Windows 应用程序（例如 WhatsApp）可能具有自定义代理规则，这些规则不会通过 Lantern 代理进行路由。最简单的解决方法是使用该应用程序的 Web 版本，因为 Lantern 默认会代理浏览器流量。另一种方法是重置任何特定于应用程序的代理规则：

1. 打开命令提示符或 PowerShell（右键单击“以管理员身份运行”）
2. 运行命令 `netsh winhttp reset proxy`
3. 重启电脑
4. 打开灯笼并连接

## 将网站安装为应用程序（桌面版）

### 火狐浏览器

1. 安装适用于 Firefox 的 Progressive Web Apps 扩展程序
2. 安装扩展程序后，导航至所需网站，然后单击地址栏中的 `Install This Web App` 按钮。
3. 按照安装提示操作。官方文档请点击[此处查看](#)。

### 铬合金

1. 导航至所需网站，然后点击浏览器右上角的 `More` 菜单。
2. 选择 `Cast, save, and share`，然后 `Install page as app`
3. 按照安装提示操作。官方文档请点击[此处查看](#)。

### Microsoft Edge

1. 如果 Microsoft Edge 检测到该网站符合安装为应用程序的条件，则会在地址栏右侧显示 `App Available` 图标。
2. 点击图标，然后选择 `Install`
3. 按照安装提示操作。官方文档请点击[此处查看](#)。



## **Safari (macOS Sonoma 14 或更高版本)**

1. 导航至所需网站
2. 点击 Safari 工具栏上的Share按钮，然后选择Add to Dock
3. 请按照安装程序提示操作。官方文档请点击此处查看。

## **提交问题报告**

### **应用程序问题报告**

请通过应用提交问题报告以获得最佳诊断：<https://lantern.io/report-issue>

如果上面的链接无法打开，请按照以下步骤进入问题提交页面：

### **桌面**

1. 前往支持
2. 选择“报告问题”
3. 选择问题类型
4. 包含更多细节
5. 发送报告

### **安卓**

1. 前往账户
2. 选择支持
3. 选择“报告问题”
4. 选择问题类型
5. 包含更多细节
6. 点击“发送报告”

### **其他问题报告方法**

**门户网站** 如果无法提交应用程序问题报告，您可以使用我们的门户网站：  
<https://support.lantern.io>

**电子邮件** 如果其他方法不可行，电子邮件是可靠的备选方案。发送至  
[support@lantern.io](mailto:support@lantern.io) 的任何邮件都会自动转换为服务台工单。

## 日志检索

由于日志是极其宝贵的调试资源，以下提供了一种备用流程，用于在 Lantern 完全阻塞且无法通过应用内提交问题时获取应用程序日志。这些日志可以附加到门户网站或通过电子邮件发送的问题报告中。

### macOS

1. 打开Terminal
2. 输入`open Library/Logs/Lantern`并按`return`
3. 选择最新的`lantern.log`文件，并将其发送至 `support@lantern.io`

### Linux (Ubuntu)

1. 打开Terminal
2. 输入`open $HOME/.lantern/logs`
3. 选择最新的`lantern.log`文件

### 视窗

1. 打开文件资源管理器并导航到Windows(C:)驱动器
2. 选择Users文件夹
3. 选择安装 Lantern 的用户帐户
4. 从功能区菜单中选择View按钮，将鼠标悬停在Show上，然后选择Hidden items
5. 导航至日志
  - (a) AppData
  - (b) Roaming
  - (c) Lantern
  - (d) Logs
6. 请将此文件通过电子邮件发送至 `support@lantern.io`

**iOS** iOS安全设置不允许用户访问应用程序数据。

**安卓** Android安全设置不允许用户访问应用数据。

## 高级诊断

如果仅凭日志难以诊断问题，则可能需要更高级的工具，例如数据包捕获。

<https://www.wireshark.org/download.html>

**【警告】** 数据包捕获会暴露记录期间所有流量的原始数据。我们建议只有能够确保数据包捕获中不包含任何个人数据的高级用户才使用此方法。

尽管 Lantern 确保提交到我们门户网站的所有数据都安全可靠，并在门户网站关闭后不久完全删除，但始终建议限制个人身份信息的记录和传输。