量子金钱包使用说明书

2017年11月

目录

量子金钱包使用说明书 1

1 基本需求 4

1.1 硬件需求 4

1.2 软件需求 4

1.3 运维和安全需求 4

2 实现方案 5

3 使用说明 5

3.1 安装 5

3.2 操作 6

3.3 创建钱包 7

3.4 密码修改 8

3.5 进入钱包控制台 9

3.5.1 可能错误 9

3.6 退出钱包控制台 10

3.7 代币转出 10

3.8 余额查询 11

3.9 钱包账号查询 11

3.10 钱包账号详情查询 11

3.11 备份还原钱包 12

3.12 导入钱包 13

3.13 注意事项 13

4 安全配置 14

4.1 防火墙管理 14

4.1.1 防火墙设置 14

4.1.2 打开防火墙保护 19

4.1.3 阻止其他人发现您的Mac 20

4.1.4 防火墙 “高级”偏好设置 22

4.1.5 为服务和应用设定防火墙访问 23

4.2 通用安全 23

4.3 隐私 25

4.4 管理员 27

4.5 共享管理 28

# 基本需求

为了实现网上购买量子金，需要开发一个虚拟代币钱包用于代币的收取和量子金的发放。为了保障该钱包的安全性，要求在进行代币转出操作时，需要三方共同认证。

由于该钱包会管理巨额资金，所以对安全性要求极高。不建议使用Windows系统。

钱包计算机作为专机使用，不建议再做其他用途使用。

## 硬件需求

Mac，500G以上硬盘，8G以上内存。

该系统作为钱包操作专用。系统密码也只有三人掌握。不能作为其他工作系统使用。

## 软件需求

Mac OSX 10.12.6以上

我们定制开发的钱包软件，相当于geth 1.7.3以上。

## 运维和安全需求

该计算机的登录密码应该掌握在少数可信的人手里。

账号管理：只有一个有超级管理权限的账号，其余账号全部删除。

网络端口管理：关闭所有不需要的服务。

防火墙：阻止所有不需要的接入。

# 实现方案

为了实现上述需求，采用如下方案实现量子金钱包：

为量子金在以太坊申请一个钱包帐号，然后针对该钱包帐号的密码，采用分段加密的方式进行处理，即：三人按顺序分别输入各自的密码，系统对三人输入的密码进行拼接后再通过算法加密，生成钱包的最终密码，向区块链网络发起操作。

由于加密具有不可逆性，所以分段加密之后，系统无法知道每个人的密码是什么。此外，由于分段加密后得到的密码马上提交到以太坊，不在任何地方进行存储，因此系统也得不到钱包的最终密码。采用该方案实现的量子金钱包，能够保证除了设置密码的三人之外，任何人都无法通过技术手段获得量子金钱包的密码。从而在以太坊钱包本身的安全机制之外，增加了对于钱包密码的保密性，从而提高了钱包的安全性。

为了缩短开发周期，该钱包在以太坊geth钱包平台之上实现，用户操作界面采用命令行方式，预计开发时间为1～2周。

# 使用说明

量子金钱包面向不同的操作系统，提供不同的安装版本。第一版仅支持Mac，对Windows的支持会在后续版本实现。为了系统安全，建议直接在Mac系统上使用钱包， 不在Windows系统中安装钱包。

Mac钱包的具体使用方法如下。

## 安装

Step1: 根据本地计算机的操作系统，下载对应的量子金钱包安装程序。

Step2: 打开本地计算机的命令行操作界面，输入安装命令，安装钱包。

zhh@zmac qwallet $ ./install.sh

Welcome to install QTG wallet!

shell is /bin/zsh

The shell config file is /Users/zhh/.zshrc

==============================

install QTG geth successfully!

You MUST run the command below at fist

source /Users/zhh/.zshrc

to effect the enviroment.

Run "qgeth new account" to create a wallet

Run "qconsole" to enter QTG Console

根据提示，复制后执行命令,初始化环境

zhh@zmac qwallet $ source /Users/zhh/.zshrc

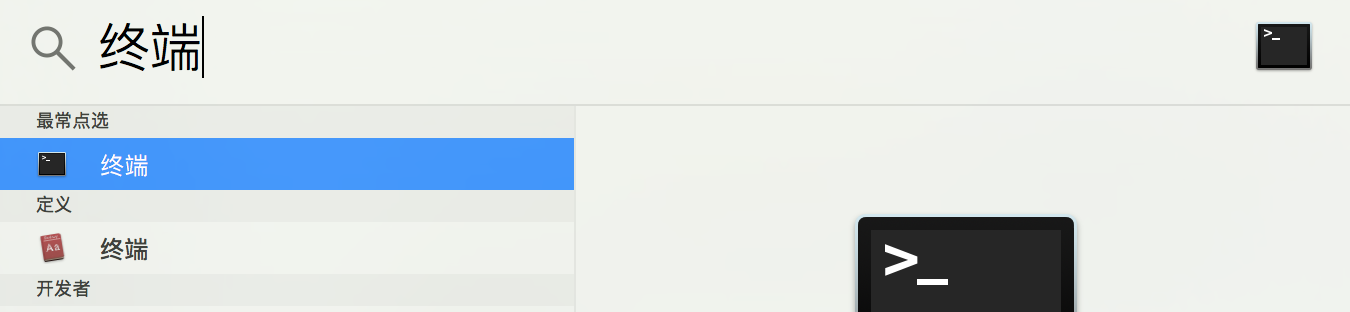
Step3: 在命令行操作界面输入操作命令，使用钱包相应功能。

## 操作

量子金钱包具有下列功能：

* 创建钱包
* 代币转出
* 余额查询
* 密码修改
* 账号查询
* 账号详情查询
* 备份钱包
* 导入钱包

Mac下进入终端（command+空格），搜索“终端”，打开终端。



或者按F4进入Launchpad，在上面搜索“终端”。



进入终端后，可以直接创建钱包和更新密码。其余必须从终端进入钱包控制台交互环境。

控制台交互环境命令输入提示为">".

操作系统终端命令输入提示为"$"

## 创建钱包

可以在终端中直接执行qgeth account new 或者进入钱包控制台执行personal.newAccount()

$ qgeth account new

WARN [11-07|06:42:24] No etherbase set and no accounts found as default

Your new account is locked with passwords. Please give your passwords. Do not forget your passwords.

------------------

Admin 1 Passphrase:

Admin 1 repeat passphrase:

Admin 1 finished.

------------------

Admin 2 Passphrase:

Admin 2 repeat passphrase:

Admin 2 finished.

------------------

Admin 3 Passphrase:

Admin 3 repeat passphrase:

Admin 3 finished.

Address: {c9c00288718cd9d96138cd99a1ec9ada4d17ac2b}

## 密码修改

$ qgeth account update c9c00288718cd9d96138cd99a1ec9ada4d17ac2b

Unlocking account c9c00288718cd9d96138cd99a1ec9ada4d17ac2b | Attempt 1/3

------------------

Admin 1 Passphrase:

Admin 1 finished.

------------------

Admin 2 Passphrase:

Admin 2 finished.

------------------

Admin 3 Passphrase:

Admin 3 finished.

INFO [11-07|06:43:21] Unlocked account address=0xc9C00288718Cd9D96138Cd99a1Ec9ADa4D17aC2B

Please give your new passwords. Do not forget your passwords.

------------------

Admin 1 Passphrase:

Admin 1 repeat passphrase:

Admin 1 finished.

------------------

Admin 2 Passphrase:

Admin 2 repeat passphrase:

Admin 2 finished.

------------------

Admin 3 Passphrase:

Admin 3 repeat passphrase:

Admin 3 finished.

! 以下命令都需进入钱包控制台交互环境。

## 进入钱包控制台

zhh@zmac ~ $ qconsole

…

>

### 可能错误

zhh@zmac ~ $ qconsole

…

Fatal: Error starting protocol stack: listen udp :30303: bind: address already in use

已经启动了钱包控制台， 可以杀掉该进程。如果不知道是否有进程占用端口，可以重启系统。

## 退出钱包控制台

> exit

INFO [11-11|18:58:28] IPC endpoint closed: /Users/zhh/data/geth.ipc

INFO [11-11|18:58:28] Blockchain manager stopped

INFO [11-11|18:58:28] Stopping Ethereum protocol

INFO [11-11|18:58:28] Ethereum protocol stopped

INFO [11-11|18:58:28] Transaction pool stopped

INFO [11-11|18:58:28] Database closed database=/Users/zhh/data/geth/chaindata

zhh@zmac $

## 代币转出

> personal.unlockAccount(eth.coinbase)

Unlock account 0xa6e81d360ec847ced9cfe44304db9b5a04d0c008

------------------

Admin 1 Passphrase:

Admin 1 finished.

------------------

Admin 2 Passphrase:

Admin 2 finished.

------------------

Admin 3 Passphrase:

Admin 3 finished.

true

> v=100

> tow="0x1b9162042358d9e409f19d3233a9e4449d31ee2e"

> eth.sendTransaction({from:eth.coinbase,to:tow,value: web3.toWei(v,"ether")})

清空值，避免误操作

> v=0

>tow=""

或者直接执行：

> eth.sendTransaction({from:eth.coinbase,to: "0x1b9162042358d9e409f19d3233a9e4449d31ee2e",value: web3.toWei(100,"ether")})

执行完转账后，立即执行lockAccount将钱包锁住。

> personal.lockAccount(eth.coinbase)

true

## 余额查询

> eth.getBalance(eth.coinbase)

10000000000000000000

## 钱包账号查询

eth.accounts 查询全部钱包key

eth.accounts[0]是第一个钱包。

> eth.accounts

["0xa6e81d360ec847ced9cfe44304db9b5a04d0c008", "0x1b9162042358d9e409f19d3233a9e4449d31ee2e", "0x3049a9a1c7841e247e8f3b3b9b6658e3001cc0de"]

## 钱包账号详情查询

> personal.listWallets[0]

{

accounts: [{

address: "0xa6e81d360ec847ced9cfe44304db9b5a04d0c008",

url: "keystore:///Users/zhh/data/keystore/UTC--2017-11-06T22-58-47.642296732Z--a6e81d360ec847ced9cfe44304db9b5a04d0c008"

}],

status: "Locked",

url: "keystore:///Users/zhh/data/keystore/UTC--2017-11-06T22-58-47.642296732Z--a6e81d360ec847ced9cfe44304db9b5a04d0c008"

}

上面示例中，status 为Locked，是不能转账的。

## 备份还原钱包

钱包key文件是用户的钱包关键文件， 必须定期做3份备份，放到不同的介质中，以确保安全。key文件一旦因为硬件等原因损坏，上面的数字币将无法找回。

key文件让账号有发送交易的能力。

key文件存储在以太坊节点数据目录的子目录‘keystore’中，不同的平台默认数据目录是不一样的：

* Windows: C:\Users\username\%appdata%\Roaming\Ethereum\keystore
* Linux: ~/.ethereum/keystore
* Mac: ~/Library/Ethereum/keystore

备份整个keystore目录。

还原的时候，把这些文件还原到原先的目录即可。

## 导入钱包

geth wallet import /path/keyfile

$ geth wallet import /Users/zhh/data/keystore/UTC--2017-11-06T22-58-47.642296732Z--a6e81d360ec847ced9cfe44304db9b5a04d0c008

Your passwords please.

------------------

Admin 1 Passphrase:

Admin 1 finished.

------------------

Admin 2 Passphrase:

Admin 2 finished.

------------------

Admin 3 Passphrase:

Admin 3 finished.

## 注意事项

* 钱包初始化结束后，请妥善保存钱包地址。该地址一旦丢失，则钱包无法继续使用，**所有钱包内的代币永久丢失**！
* 由于该钱包采用了分段加密的方式，对以太坊的钱包密码进行了再次加密处理，从而保证了除了设置密码的三人之外，任何人都无法通过技术手段获得量子金钱包的密码，极大地保证了钱包的安全性。因此，请设置密码的三人妥善保存设置的密码。该密码一旦丢失，则钱包无法继续使用，**所有钱包内的代币永久丢失**！
* 设置密码的三人每次输入密码的顺序必须保证一致。
* 由于该钱包运行在以太坊环境中，每次使用钱包时会首先自动同步以太坊最新结点。因此，为了缩短同步时间，建议在固定终端上使用该钱包。
* 该钱包在以太坊geth钱包的基础上，进行了针对密码保密性的二次开发。因此该钱包无法排除由于geth钱包自身具有的漏洞而受到的攻击。
* 在进行代币转出和密码修改的操作时，需要先对钱包解锁。完成操作后，请务必输入命令锁定钱包，以保证钱包的安全性。如果没有输入钱包锁定命令，钱包会在解锁5分钟后自动锁定。
* 定期备份钱包，账号信息如密码等有改动时必须备份钱包。钱包必须备份在三份以上不同介质。

# 安全配置

## 防火墙管理

### 防火墙设置

在您连接到互联网或网络时，防火墙可保护您的 Mac 免遭其他电脑发起的不必要联系。但是，Mac 仍可允许某些服务和应用通过防火墙进行访问。例如：

* 如果您打开共享服务（比如文件共享），macOS 将打开特定的端口，以供服务进行通信。
* 另一系统上的应用或服务可以请求并被允许通过防火墙来访问，或可能具有可信证书并因此被允许访问。

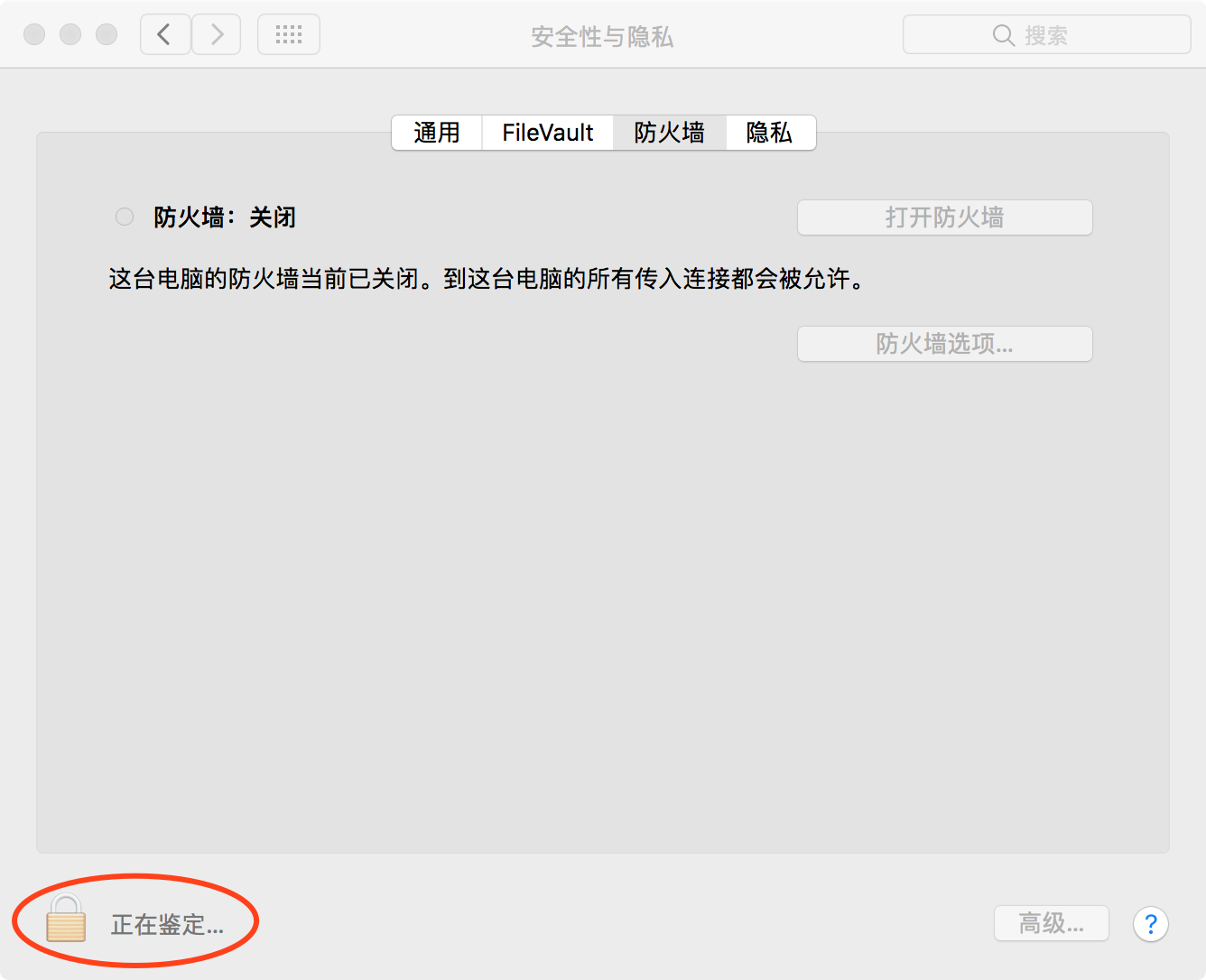
若要进一步控制，您可以选择应用和服务，并指定它们是否可以通过防火墙访问。

使用“安全性与隐私”偏好设置中的“防火墙”面板可打开 macOS 中的防火墙，来防止来自互联网或其他网络的不想要的连接。

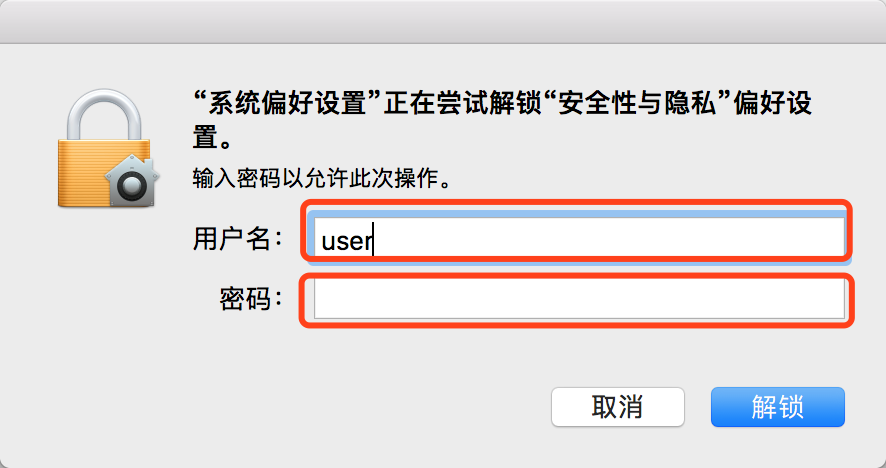


若要打开此面板，请选取苹果菜单 >“系统偏好设置”，点按“安全性与隐私”，然后点按“防火墙”。





解锁，输入管理员用户名密码。



|  |  |
| --- | --- |
| 打开防火墙 | 如果防火墙关闭，请点按“打开防火墙”以打开防火墙保护。 |
| 防火墙选项 | 点按“防火墙选项”按钮以更改防火墙设置。 |
| 阻止所有传入连接 | 在“防火墙选项”中，选择可防止非必要服务和应用的传入连接。  基本的互联网服务是一组应用，允许您的 Mac 在网络上查找由其他电脑所提供的服务。此设置会防止与其他所有共享服务的连接。 |
| 添加 | 在“防火墙选项”中，若要添加应用或服务，请点按添加按钮 ，在列表中选择项目，然后使用上箭头键和下箭头键来设定应用的限制。 |
| 移除 | 在“防火墙选项”中，若要移除应用，请在列表中选择该应用，然后点按移除按钮 。 |
| 自动允许内建软件接收传入连接 | 在“防火墙选项”中，选择以允许将由有效的证书颁发机构签名的内建应用和服务自动添加到允许的应用列表，而无需您授权。例如，iTunes 由 Apple 签名，因此可以自动通过防火墙接收传入连接。 |
| 自动允许已下载的签名软件接收传入连接 | 在“防火墙选项”中，选择以允许将由有效的证书颁发机构签名的已下载应用和服务自动添加到允许的应用列表，而无需您授权。 |
| 启用秘密行动模式 | 在“防火墙选项”中，选择可防止 Mac 对那些用来显现其存在的探测请求作出响应。Mac 仍将响应来自经授权的应用的请求，而未经授权的请求，如 ICMP (ping)，则无法获得响应。 |
| 锁定 | 锁定或解锁“安全性与隐私”偏好设置。点按锁图标  以将它解锁，然后输入管理员的名称和密码。 |
| 高级 | 点按可增加 Mac 上的安全性，方法是调整“高级”偏好设置中的特定设置。 |

如果“共享”偏好设置中的某些共享服务已打开，则它们可以经过防火墙连接。若要实现附加安全性，可以通过在“共享”偏好设置中关闭服务，来防止连接到此类传入服务。

### 打开防火墙保护

* 选取苹果菜单 >“系统偏好设置”，点按“安全性与隐私”，然后点按“防火墙”。
* 点按锁图标  以将它解锁，然后输入管理员名称和密码。
* 点按“打开防火墙”。
* 若要指定附加安全性设置，请点按“防火墙选项”并执行以下任一项操作：
  + **只允许连接指定的应用和服务：**点按添加按钮 ，然后在出现的对话框中选择应用或服务。
  + **只允许连接基本的应用和服务：**选择“阻隔所有传入连接”复选框。
  + **自动允许内建软件接收传入连接：**选择“自动允许内建软件接收传入连接”复选框。
  + **自动允许已下载的签名的软件接收传入连接：**选择“自动允许已下载的签名的软件接收传入连接”复选框。



### 阻止其他人发现您的Mac

在防火墙选项中设置“隐身模式”，以阻止计算机被测试程序进行端口扫描。





### 防火墙 “高级”偏好设置

使用“安全性与隐私”偏好设置的“高级”面板来调整 Mac 的安全性设置。

若要打开此面板，请选取苹果菜单 >“系统偏好设置”，点按“安全性与隐私”，然后点按“高级”。

|  |  |
| --- | --- |
| 在…分钟不活跃后注销 | 选择以在 Mac 闲置指定分钟数后自动注销用户。 |
| 访问系统范围偏好设置需要输入管理员密码 | 选择以防止用户在不使用管理员密码的情况下更改锁定的系统偏好设置。 |
| 停用遥控红外接收机 | 选择可防止您的 Mac 接收来自红外遥控器的命令。（此选项出现在具有红外线端口的 Mac 电脑上。）  若要配置您的 Mac 以响应红外遥控器控制，请取消选择复选框，点按“配对”，然后按照屏幕指示进行操作。 |

### 为服务和应用设定防火墙访问

1. 选取苹果菜单 >“系统偏好设置”，点按“安全性与隐私”，然后点按“防火墙”。
2. 点按锁图标  以将它解锁，然后输入管理员名称和密码。
3. 点按“防火墙选项”。 如果“防火墙选项”按钮被停用，请先点按“打开防火墙”以打开 Mac 的防火墙。
4. 点按服务列表下的添加按钮 ，然后选择要添加的服务或应用。添加应用后，点按它的上箭头和下箭头，以允许或阻止通过防火墙进行连接。 阻止应用通过防火墙进行访问可能会干扰或影响该应用或可能依赖于该应用的其他软件的性能。

**【重要事项】未在列表中出现的特定应用可能具有通过防火墙访问的权限。其中可以包括其他应用自动打开的系统应用、服务、进程以及数字签名应用。若要阻止这些程序的访问，请将它们添加到列表中。  当 Mac 检测到有尝试连接到您未添加到列表和允许访问的应用时，将出现对话框，询问您是否要允许或拒绝通过网络或互联网连接。如果没有执行操作，信息将保持显示状态，并且会拒绝任何尝试连接到应用的操作。**

## 通用安全

使用“安全性与隐私”偏好设置的“通用”面板以防止 Mac 被恶意软件侵害和篡改。

若要打开此面板，请选取苹果菜单 >“系统偏好设置”，点按“安全性与隐私”，然后点按“通用”。

|  |  |
| --- | --- |
| 更改密码 | 点按可更改当前用户的登录密码。 |
| 进入睡眠或开始屏幕保护程序后...要求输入密码 | 使用此设置可锁定处于闲置状态的 Mac。唤醒 Mac 时，必须先输入用户登录密码，才能使用 Mac。您可以选择进入屏幕保护程序或睡眠状态多长时间后用户需要输入密码来激活电脑。 |
| 屏幕锁定时显示信息 | 选择以在 Mac 锁定时，在登录窗口显示一条短信息。该信息将向尝试登录的任何用户显示。它也可以用于为丢失的 Mac 提供联系信息。 |
| 停用自动登录 | 选择以要求用户在重新启动 Mac 后登录时使用密码鉴定。FileVault 打开时，此功能不可用。 |
| 允许 Apple Watch 解锁 Mac | 从闲置状态唤醒 Mac 时，可使用 Apple Watch（而不是输入密码）来解锁您的 Mac。 |
| 允许从以下位置下载的应用： | 您可以通过仅允许来自 App Store 或被认可开发者的应用，保护 Mac 免遭恶意软件侵害。   * **App Store：**选择以仅允许从 App Store 下载的应用。 * **App Store 和被认可的开发者：**选择以仅允许来自 App Store 以及来自 Apple 所认可开发者的应用。 |
| 锁定 | 锁定或解锁“安全性与隐私”偏好设置。点按锁图标  以将它解锁，然后输入管理员的名称和密码。 |
| 高级 | 点按可增加 Mac 上的安全性，方法是调整“高级”偏好设置中的特定设置。 |

睡眠或屏幕保护程序要设为“立即”要求输入密码。

下载应用只允许App Store。除非有例外单独处理。

****

## 隐私

使用“安全性与隐私”偏好设置的“隐私”面板以管理 Mac 上可供互联网或网络中其他用户访问的信息。

若要打开此面板，请选取苹果菜单 >“系统偏好设置”，点按“安全性与隐私”，然后点按“隐私”。

|  |  |
| --- | --- |
| 定位服务 | 启用“定位服务”后，将允许应用、系统服务和网站使用 Mac 的当前位置，以提供与您所在位置相关的信息、服务和功能。  若要查看使用您位置信息的特定系统服务，请点按“详细信息”按钮。 |
| “通讯录”、“日历”和“提醒事项” | 显示想要访问您的联系人、日历或提醒事项的应用。如果您想要阻止其访问此类信息，请取消选择该应用。 |
| 辅助功能 | 显示通过运行脚本和系统命令来控制您的 Mac 的应用。如果您想要阻止其控制您的 Mac，请取消选择该应用。 |
| 分析 | 若要帮助 Apple 和其他开发者更好地服务客户及改进其产品的质量，您可以选取自动将分析信息发送给 Apple 和应用开发者。 |
| 其他帐户 | 登录到社交媒体帐户或其他互联网帐户时，想访问这些帐户的应用会显示出来。 |
| 锁定 | 锁定或解锁“安全性与隐私”偏好设置。点按锁图标  以将它解锁，然后输入管理员名称和密码。 |

辅助功能中允许控制电脑的程序全部去掉。



## 管理员

管理员可以添加和管理其他用户、安装应用以及更改设置。首次设置 Mac 时创建的新用户就是管理员。

您的 Mac 可以具有多个管理员。您可以创建新管理员，以及将普通用户转换为管理员。

请勿为管理员设置自动登录。如果您这样做，那么其他人只需重新启动 Mac 就能获得管理员访问权限。为了保证 Mac 的安全，请不要共享管理员名称和密码。

1. 选取苹果菜单 >“系统偏好设置”，点按“安全性与隐私”，然后点按“防火墙”。
2. 点按锁图标  以将它解锁，然后输入管理员名称和密码。
3. 点按“防火墙选项”。 如果“防火墙选项”按钮被停用，请先点按“打开防火墙”以打开 Mac 的防火墙。

## 共享管理

将所有共享全部关闭。除非为了临时调试或部署需要打开。调试和部署完毕，必须关闭。文件备份和复制只使用钱包专用U盘。

如果尚未打开，请打开“共享”偏好设置（选取苹果菜单 >“系统偏好设置”，然后点按“共享”）。

