

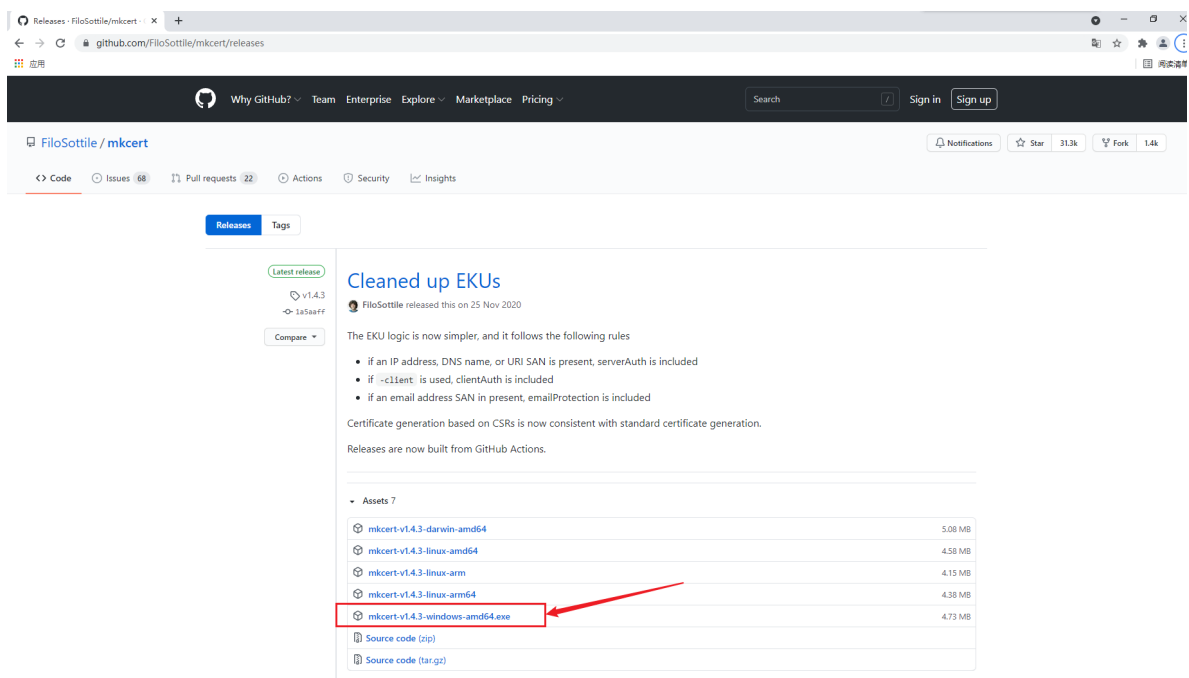
使用mkcert工具生成受信任的SSL证书，解决局域网本地https访问问题

1、mkcert 简介

mkcert 是一个简单的工具，用于制作本地信任的开发证书。它不需要配置。简化我们在本地搭建 https 环境的复杂性，无需操作繁杂的 openssl 实现自签证书了，这个程序就可以帮助我们自签证书，在本机使用还会自动信任 CA，非常方便。使用来自真实证书颁发机构 (CA) 的证书进行开发可能很危险，但自签名证书会导致信任错误。管理您自己的 CA 是最好的解决方案，但通常涉及晦涩的命令、专业知识和手动步骤。mkcert 在系统根存储中自动创建并安装本地 CA，并生成本地信任的证书。

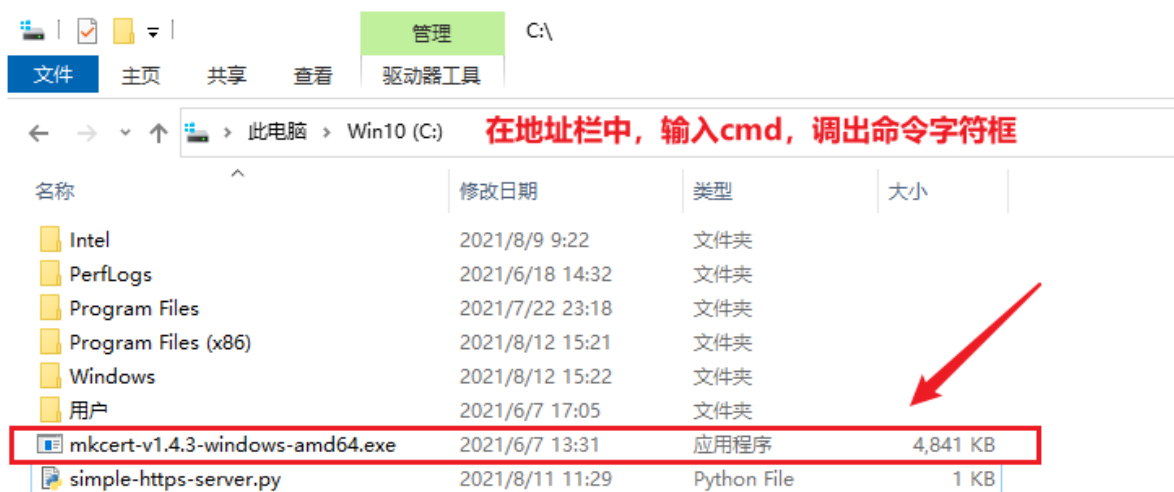
2、mkcert 下载

- 本实验使用 Windows 操作系统进行演示说明。mkcert 也支持其它平台的安装与使用，自行下载对应的版本安装即可。



3、mkcert 安装配置

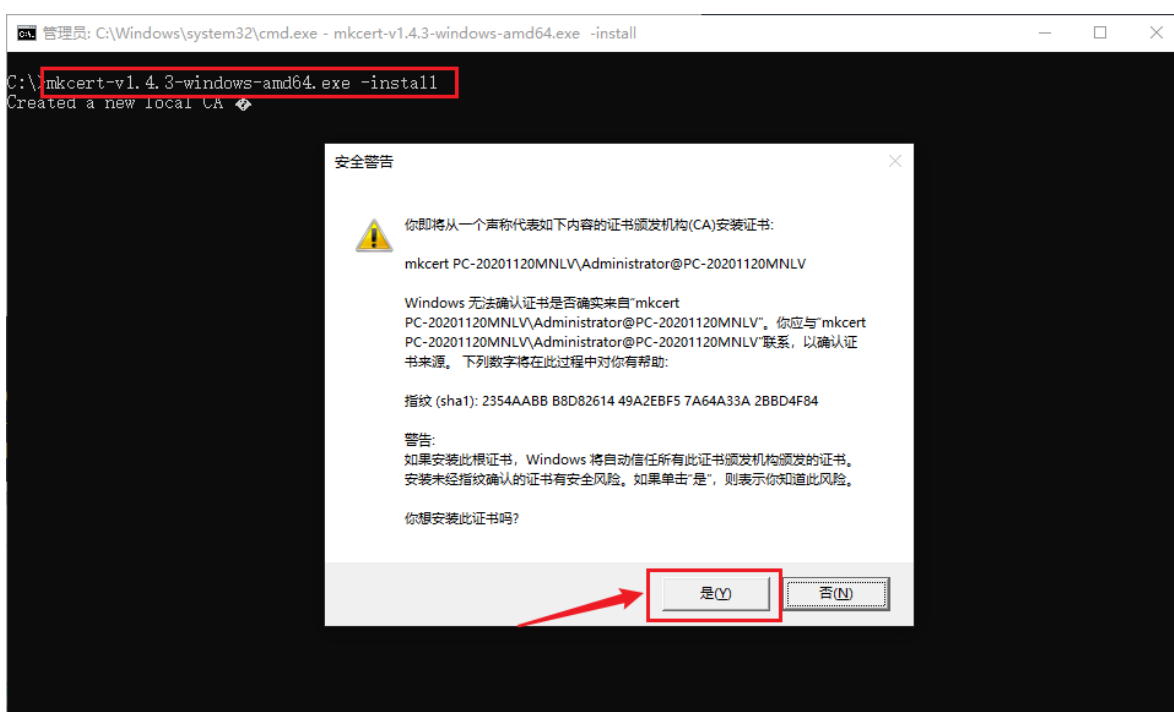
(1) 输入 CMD，调出命令提示符



(2) 初次安装 mkcert

输入 `mkcert-v1.4.3-windows-amd64.exe -install` 命令，安装 mkcert。将 CA 证书加入本地可信 CA，使用此命令，就能帮助我们将 mkcert 使用的根证书加入了本地可信 CA 中，以后由该 CA 签发的证书在本地都是可信的。

卸载命令 `mkcert-v1.4.3-windows-amd64.exe -uninstall`



安装成功成功。提示创建一个新的本地 CA，本地 CA 现在已安装在系统信任存储中。

```
管理员: C:\Windows\system32\cmd.exe
C:\>mkcert-v1.4.3-windows-amd64.exe -install
Created a new local CA
The local CA is now installed in the system trust store!
Warning: "keytool" is not available, so the CA can't be automatically installed in Java's trust store!
C:\>
```

(3) 测试 mkcert 是否安装成功（成功后会显示如下信息）

```
管理员: C:\Windows\system32\cmd.exe
C:\>mkcert-v1.4.3-windows-amd64.exe -help
Usage of mkcert:

$ mkcert -install
Install the local CA in the system trust store.

$ mkcert example.org
Generate "example.org.pem" and "example.org-key.pem".

$ mkcert example.com myapp.dev localhost 127.0.0.1 ::1
Generate "example.com+4.pem" and "example.com+4-key.pem".

$ mkcert "*.example.it"
Generate "_wildcard.example.it.pem" and "_wildcard.example.it-key.pem".

$ mkcert -uninstall
Uninstall the local CA (but do not delete it).

Advanced options:

-cert-file FILE, -key-file FILE, -p12-file FILE
    Customize the output paths.

-client
    Generate a certificate for client authentication.

-ecdsa
    Generate a certificate with an ECDSA key.

-pkcs12
    Generate a ".p12" PKCS #12 file, also know as a ".pfx" file,
    containing certificate and key for legacy applications.

-csr CSR
    Generate a certificate based on the supplied CSR. Conflicts with
    all other flags and arguments except -install and -cert-file.

-CAROOT
    Print the CA certificate and key storage location.

$CAROOT (environment variable)
    Set the CA certificate and key storage location. (This allows
    maintaining multiple local CAs in parallel.)

$TRUST_STORES (environment variable)
    A comma-separated list of trust stores to install the local
    root CA into. Options are: "system", "java" and "nss" (includes
    Firefox). Autodetected by default.

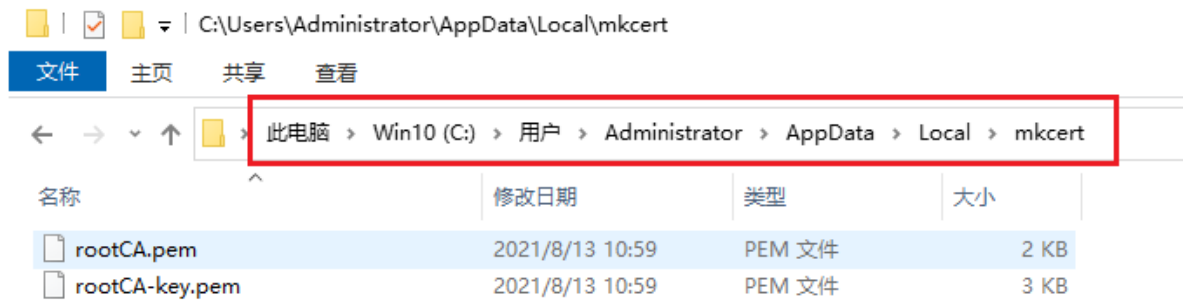
C:\>
```

(4) 查看 CA 证书存放位置

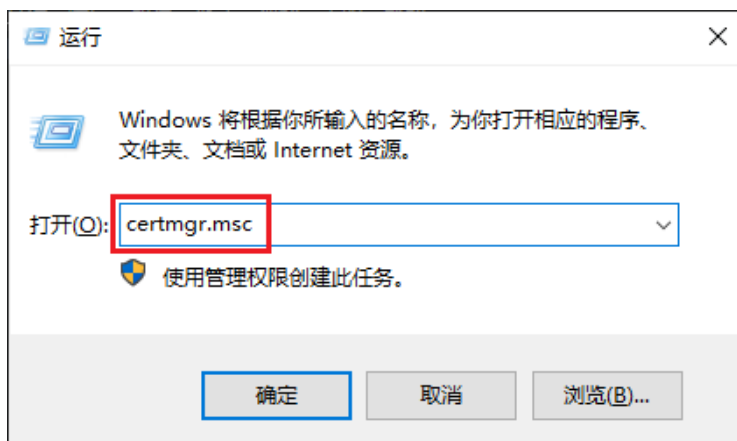
输入 `mkcert-v1.4.3-windows-amd64.exe -CAROOT` 命令。

```
管理员: C:\Windows\system32\cmd.exe

C:\>mkcert-v1.4.3-windows-amd64.exe -CAROOT
C:\Users\Administrator\AppData\Local\mkcert
C:\>_
```



按“Windows 键 +R”调出运行框，输入 `certmgr.msc` 命令。打开证书控制台。



certmgr - [证书 - 当前用户受信任的根证书颁发机构\证书]						
文件(F) 操作(A) 查看(V) 帮助(H)						
证书 - 当前用户 受信任的根证书颁发机构 证书 企业信任 中间证书颁发机构 Active Directory 用户对象 受信任的发布者 不信任的证书 第三方根证书颁发机构 受信任人 客户端身份验证颁发者 Local Non-Removable Cert 证书注册申请 智能卡受信任的根						
颁发给	颁发者	截止日期	预期目的	友好名称	状态	
GlobalSign	GlobalSign	2029/3/18	客户端身份验证, 代...	GlobalSign Root ...		
GlobalSign	GlobalSign	2021/12/15	客户端身份验证, 代...	Google Trust Ser...		
GlobalSign	GlobalSign	2038/1/19	客户端身份验证, 代...	GlobalSign ECC R...		
GlobalSign Root CA	GlobalSign Root CA	2028/1/28	客户端身份验证, 代...	GlobalSign Root ...		
Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Authority	2034/6/30	客户端身份验证, 代...	Go Daddy Class 2...		
Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	2038/1/1	客户端身份验证, 代...	Go Daddy Root C...		
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	2043/12/8	客户端身份验证, 安...	Hotspot 2.0 Trust...		
ISRG Root X1	ISRG Root X1	2035/6/4	服务器身份验证	ISRG Root X1		
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	2000/1/1	安全电子邮件, 代码...	Microsoft Authent...		
Microsoft ECC Product Root Certificate Authority 2018	Microsoft ECC Product Root Certificate Authority 2018	2043/2/28	<所有>	Microsoft ECC Pr...		
Microsoft ECC TS Root Certificate Authority 2018	Microsoft ECC TS Root Certificate Authority 2018	2043/2/28	<所有>	Microsoft ECC TS...		
Microsoft Root Authority	Microsoft Root Authority	2020/12/31	<所有>	Microsoft Root A...		
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	2021/5/10	<所有>	Microsoft Root A...		
Microsoft Root Certificate Authority 2010	Microsoft Root Certificate Authority 2010	2035/6/24	<所有>	Microsoft Root C...		
Microsoft Root Certificate Authority 2011	Microsoft Root Certificate Authority 2011	2036/3/23	<所有>	Microsoft Root C...		
Microsoft Time Stamp Root Certificate Authority 2014	Microsoft Time Stamp Root Certificate Authority 2014	2038/10/23	<所有>	Microsoft Time St...		
mkcert PC-20201120MNLV\Administrator@PC-20201120MNLV	mkcert PC-20201120MNLV\Administrator@PC-20201120MNLV	2031/8/13	<所有>	<无>		
NO LIABILITY ACCEPTED, (c) 1997 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c) 1997 VeriSign, Inc.	2004/1/18	时间戳	VeriSign Time Sta...		
PC-20201120MNLV\Administrator@PC-20201120MNLV	mkcert PC-20201120MNLV\Administrator@PC-20201120MNLV	2023/9/10	服务器身份验证	<无>		
PC-20201120MNLV\Administrator@PC-20201120MNLV	mkcert PC-20201120MNLV\Administrator@PC-20201120MNLV	2023/9/10	服务器身份验证	<无>		
QuoVadis Root Certification Authority	QuoVadis Root Certification Authority	2021/3/18	客户端身份验证, 代...	QuoVadis Root C...		
SecureTrust CA	SecureTrust CA	2030/1/1	客户端身份验证, 代...	Trustwave		
Starfield Class 2 Certification Authority	Starfield Class 2 Certification Authority	2034/6/30	客户端身份验证, 代...	Starfield Class 2 ...		
Starfield Root Certificate Authority - G2	Starfield Root Certificate Authority - G2	2038/1/1	客户端身份验证, 代...	Starfield Root Cer...		
Symantec Enterprise Mobile Root for Microsoft	Symantec Enterprise Mobile Root for Microsoft	2032/3/15	代码签名	<无>		
thawte Primary Root CA	thawte Primary Root CA	2036/7/17	客户端身份验证, 代...	thawte		
Thawte Timestamping CA	Thawte Timestamping CA	2021/1/1	时间戳	Thawte Timestam...		
USERTrust RSA Certification Authority	USERTrust RSA Certification Authority	2038/1/19	客户端身份验证, 代...	Sectigo		
VeriSign Class 3 Public Primary Certification Authority - G5	VeriSign Class 3 Public Primary Certification Authority - G5	2036/7/17	客户端身份验证, 代...	VeriSign		
VeriSign Universal Root Certification Authority	VeriSign Universal Root Certification Authority	2037/12/2	客户端身份验证, 代...	VeriSign Universa...		

受信任的根证书颁发机构 存储含有 46 个证书。



(5) 生成自签证书,可供局域网内使用其他主机访问。

直接跟多个要签发的域名或 ip 就行了, 比如签发一个仅本机访问的证书(可以通过 `127.0.0.1` 和 `localhost`, 以及 ipv6 地址 `::1` 访问)

需要在局域网内测试 https 应用, 这种环境可能不对外, 因此也无法使用像 `Let's encrypt` 这种免费证书的方案给局域网签发一个可信的证书, 而且 `Let's encrypt` 本身也不支持认证 ip。

证书可信的三个要素:

- 由可信的 CA 机构签发
- 访问的地址跟证书认证地址相符
- 证书在有效期内

如果期望自签证书在局域网内使用，以上三个条件都需要满足。很明显自签证书一定可以满足证书在有效期内，那么需要保证后两条。我们签发的证书必须匹配浏览器的地址栏，比如局域网的 ip 或者域名，此外还需要信任 CA。

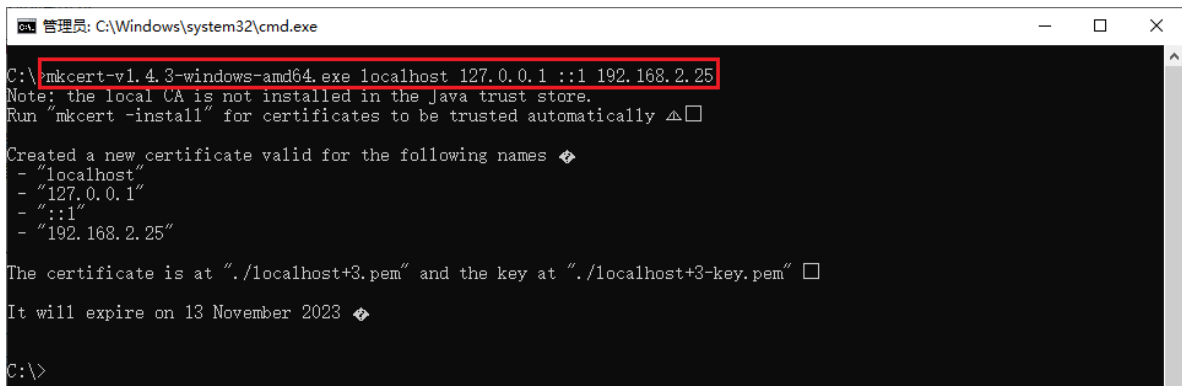
操作如下：签发证书，加入局域网 IP 地址。

```
C:\>mkcert-v1.4.3-windows-amd64.exe localhost 127.0.0.1 :::1 192.168.2.25
Note: the local CA is not installed in the Java trust store.
Run "mkcert -install" for certificates to be trusted automatically ⚠️

Created a new certificate valid for the following names 📋
- "localhost"
- "127.0.0.1"
- ":::1"
- "192.168.2.25"

The certificate is at "./localhost+3.pem" and the key at "./localhost+3-key.pem"
✅

It will expire on 13 November 2023 📅
```



```
管理员: C:\Windows\system32\cmd.exe
C:\>mkcert-v1.4.3-windows-amd64.exe localhost 127.0.0.1 :::1 192.168.2.25
Note: the local CA is not installed in the java trust store.
Run "mkcert -install" for certificates to be trusted automatically ⚠️

Created a new certificate valid for the following names 📋
- "localhost"
- "127.0.0.1"
- ":::1"
- "192.168.2.25"

The certificate is at "./localhost+3.pem" and the key at "./localhost+3-key.pem" □

It will expire on 13 November 2023 ⚡

C:\>
```

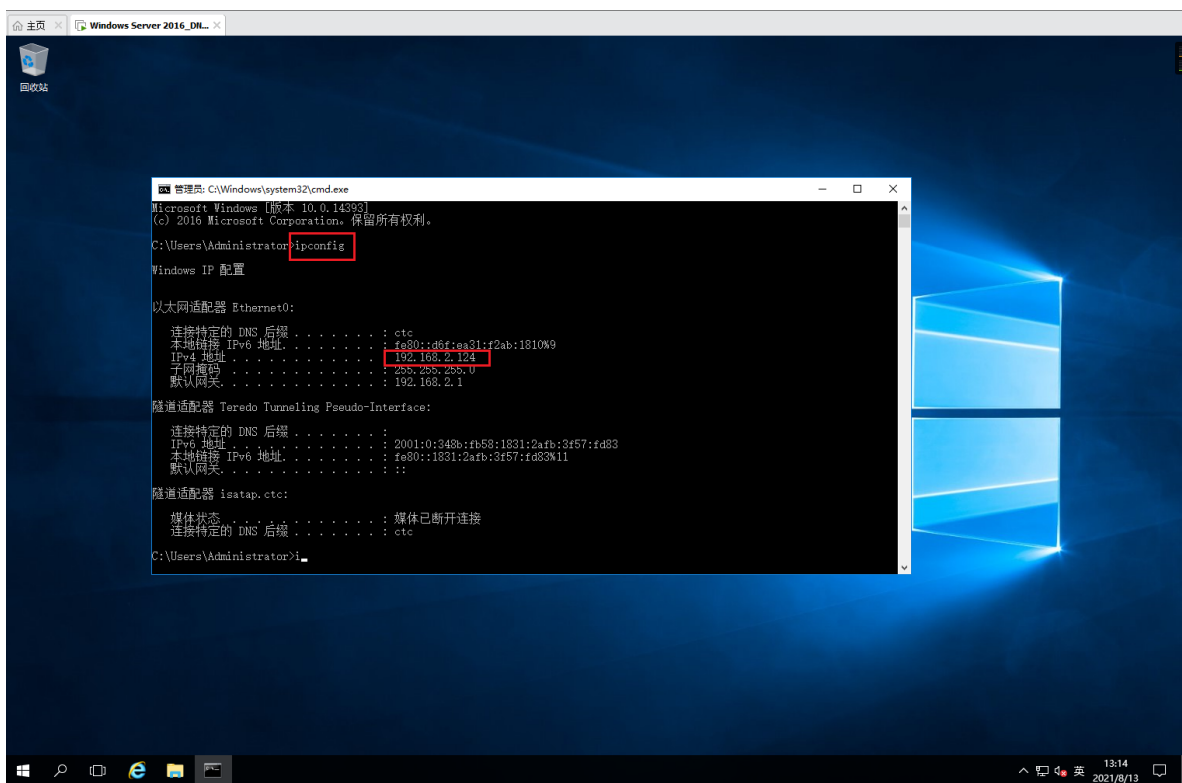
在 mkcert 软件同目录下，生成了自签证书。如图所示。

通过输出，我们可以看到成功生成了 `localhost+3.pem` 证书文件和 `localhost+3-key.pem` 私钥文件，只要在 web server 上使用这两个文件就可以了。



4、mkcert 测试验证

- Windows 系统操作访问演示



点击“安装证书”。



单击下一步。



←  证书导入向导

欢迎使用证书导入向导

该向导可帮助你将证书、证书信任列表和证书吊销列表从磁盘复制到证书存储。

由证书颁发机构颁发的证书是对你身份的确认，它包含用来保护数据或建立安全网络连接的信息。证书存储是保存证书的系统区域。

存储位置

☒ 当前用户(C)

☐ 本地计算机(L)

单击“下一步”继续。

下一步(N)

取消

windows 导入证书的方法是双击这个文件，在证书导入向导中将证书导入`受信任的根证书颁发机构`。

证书存储

证书存储是保存证书的系统区域。

Windows 可以自动选择证书存储，你也可以为证书指定一个位置。

☐ 根据证书类型，自动选择证书存储(U)

☒ 将所有的证书都放入下列存储(P)

证书存储:

受信任的根证书颁发机构

浏览(R)...

下一步(N)

取消

点击“完成”。

正在完成证书导入向导

单击“完成”后将导入证书。

你已指定下列设置:

用户选定的证书存储	受信任的根证书颁发机构
内容	证书

完成(F)

取消

点击“是”。



你即将从一个声称代表如下内容的证书颁发机构(CA)安装证书:

mkcert PC-20201120MNLV\Administrator@PC-20201120MNLV

Windows 无法确认证书是否确实来自“mkcert PC-20201120MNLV\Administrator@PC-20201120MNLV”。你应与“mkcert PC-20201120MNLV\Administrator@PC-20201120MNLV”联系，以确认证书来源。 下列数字将在此过程中对你有帮助:

指纹 (sha1): 05B12263 D631A547 949F29B6 183F8DBA 2E48FE0B

警告:

如果安装此根证书，Windows 将自动信任所有此证书颁发机构颁发的证书。安装未经指纹确认的证书有安全风险。如果单击“是”，则表示你知道此风险。

你想安装此证书吗?

是(Y)

否(N)



导入成功。

确定

再次点击此证书。已被添加为信任。



使用浏览器验证。输入 <https://192.168.2.25:8000>，发现可信任。

