

# WinServer AD/NPS + IAP 实现 EAP-TLS 认证

Hao.liu2@hpe.com

## Table of Contents

<b>第一步：IAP 配置</b> .....	<b>2</b>
1.1 不开启 EAP 卸载模式.....	2
1.2 开启 EAP 卸载模式.....	2
<b>第二步：AD CS/NPS 安装</b> .....	<b>4</b>
<b>第三步：签发 Server 证书</b> .....	<b>4</b>
3.1 证书查看.....	4
3.2 生成 Server 证书 CSR 文件.....	7
3.3 签发证书.....	12
<b>第四步：NPS 开启证书认证</b> .....	<b>16</b>
4.1 修改原有认证方式.....	16
4.2 初始化配置 NPS.....	17
<b>第五步：客户端证书签发</b> .....	<b>21</b>
5.1 客户端 CSR 生成.....	21
5.2 客户端证书签发.....	25
<b>第六步：客户端证书安装</b> .....	<b>26</b>
6.1 Windows PC.....	26
6.2 Android.....	31
6.3 IOS.....	37
6.4 MacOS.....	39

## 第一步：IAP 配置

IAP 有 2 种配置模式，是否开启 IAP EAP 卸载：启用 EAP 卸载功能，可以通过终止 AP 上的认证协议，减少到外部 RADIUS 服务器的网络流量。

默认情况下，在启用此功能后，对于 802.1X 认证，客户端与 RADIUS 服务器进行 EAP 交换，AP 充当此交换的中继站。当启用此功能后，AP 本身充当认证服务器的作用。AP 终止 EAP 协议的外层，仅仅中继最内层到外部 RADIUS 服务器。

**注意：当使用 LDAP 用于认证时，需要 AP 终结，因为 LDAP 不支持 EAP。**

### 1.1 不开启 EAP 卸载模式

此模式下客户端与 Radius 服务器直接交互，IAP 无需特殊配置。

编辑 2222

1 基本 2 VLAN 3 安全 4 接入

安全级别

安全级别 企业

密钥管理 WPA2-企业

认证服务器 1 cppm

认证服务器 2 -- Select Server --

EAP 卸载

重认证间隔  hrs.

认证缓存

MAC 认证  执行 802.1X 前的 MAC 认证  MAC 认证失败

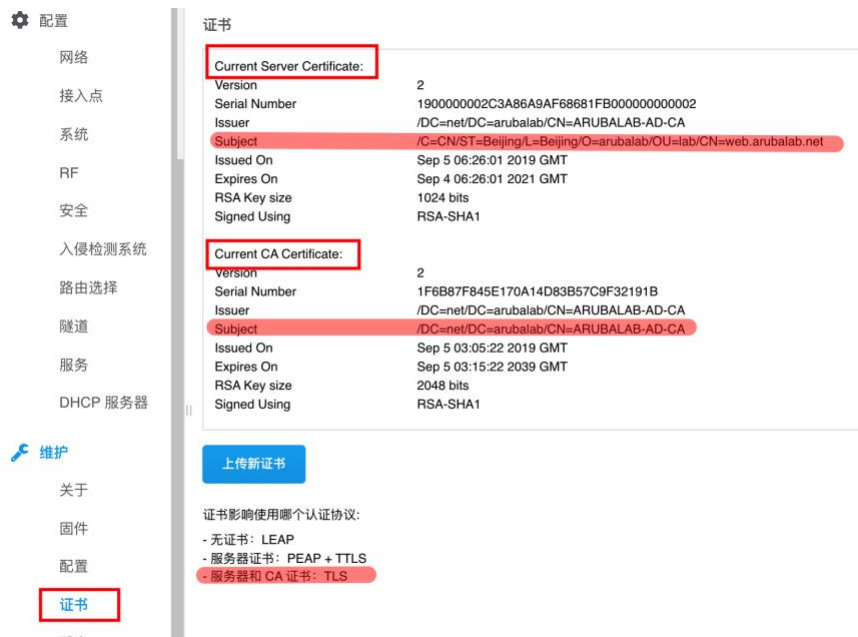
计费 已禁用

### 1.2 开启 EAP 卸载模式

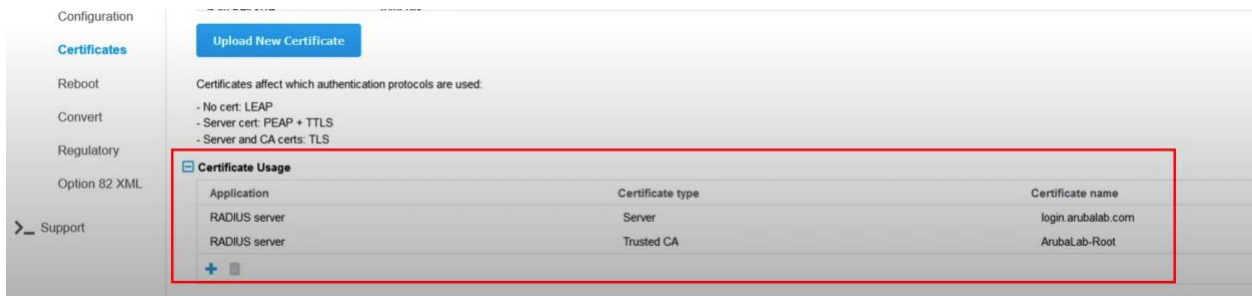
**此模式下必须要给 IAP 导入 root CA 和 Server 证书。**



Web UI 第一种 (此版本界面同一类型证书不能上传多个, 上传正确的证书即可影响相关认证)



Web UI 第二种 (此版本界面同一类型证书可以上传多个, 需要点击加号选用相应 root CA 和 server 证书)



## 第二步：AD CS/NPS 安装

过程略，参考 <https://arubase.club/archives/5601> 或者其他资料。

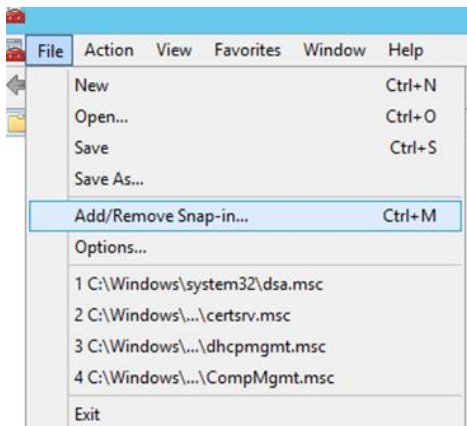
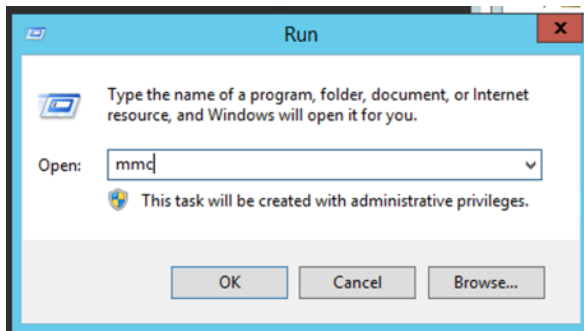
## 第三步：签发 Server 证书

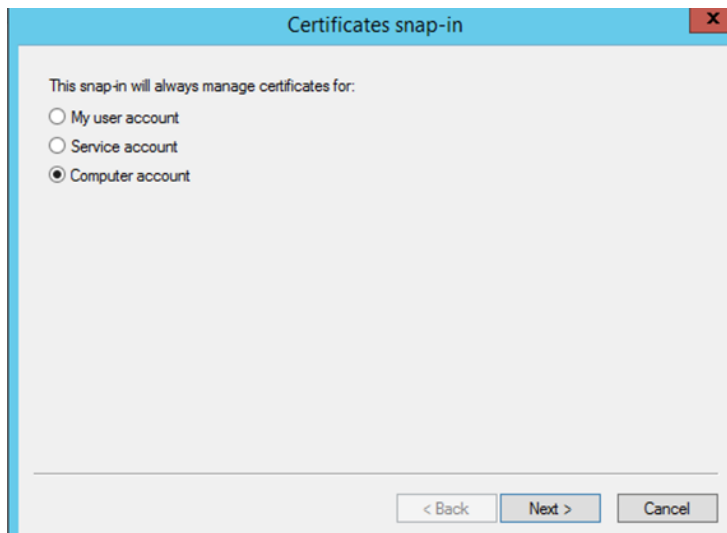
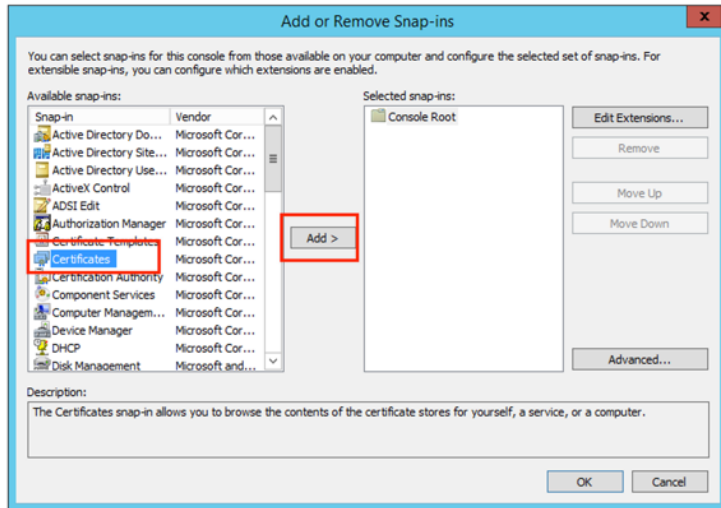
实现 EAP-TLS 认证需要 3 个证书：Root CA 证书、Server 证书、终端证书。Radius Server 需要安装 Root CA 证书和 Server 证书，终端需要安装 root CA 证书和终端证书。

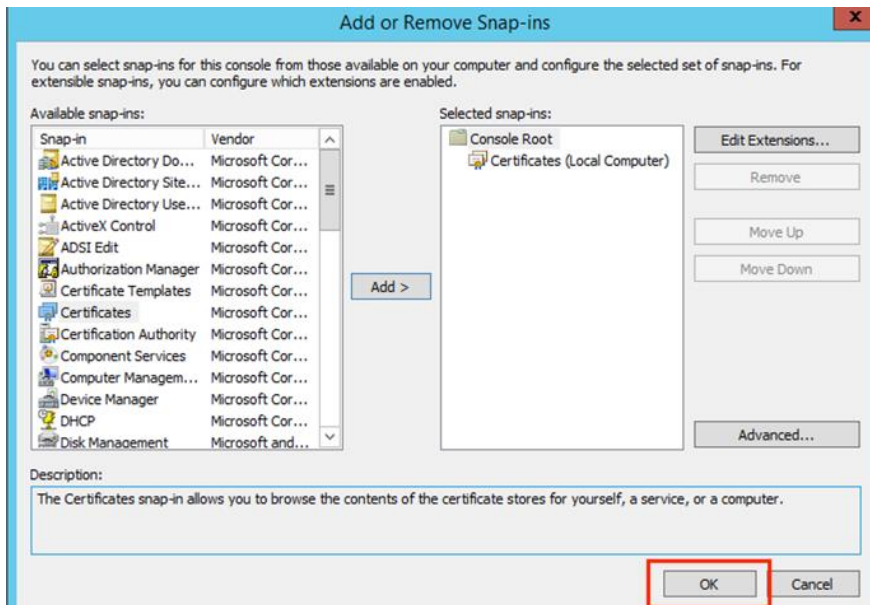
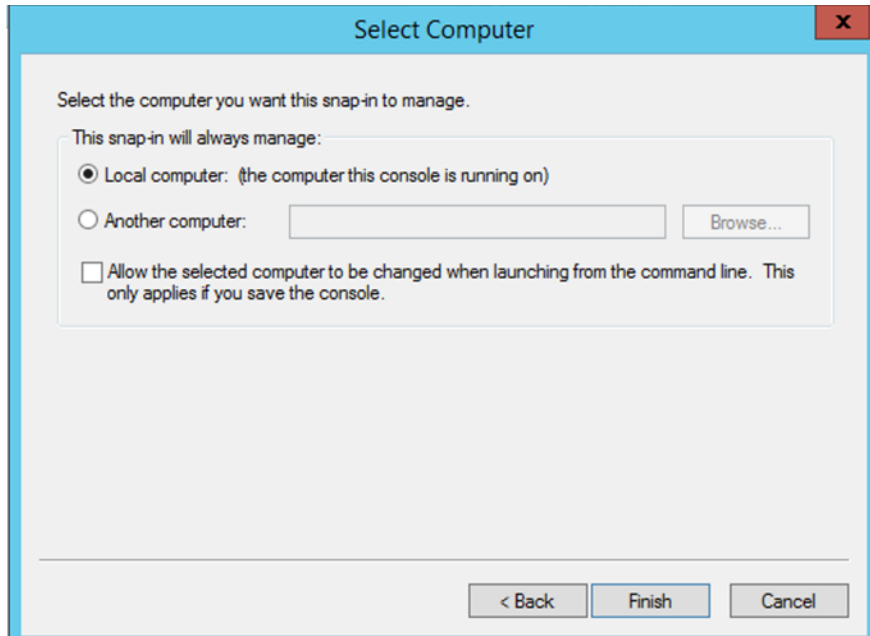
以下步骤表示你的 NPS/CA 是同一台设备（也就是 NPS Radius 跟 CA 是一台服务器），如果是 2 台独立设备，需要在 NPS Server 部署 root CA 和 Server 证书。

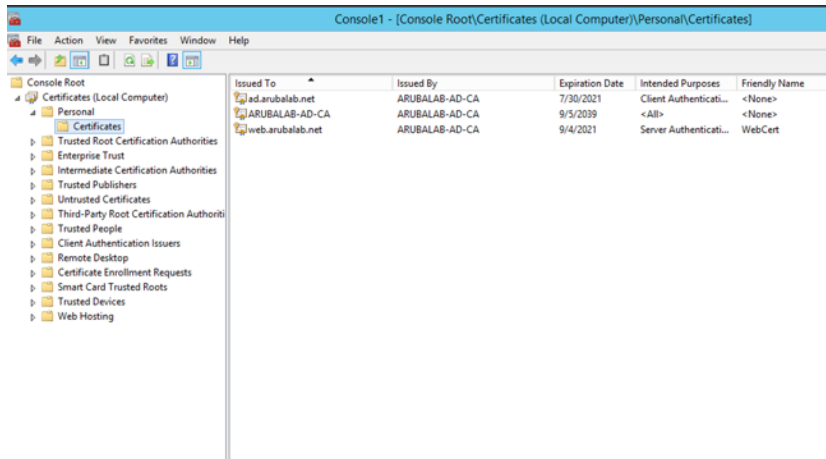
### 3.1 证书查看

运行 mmc

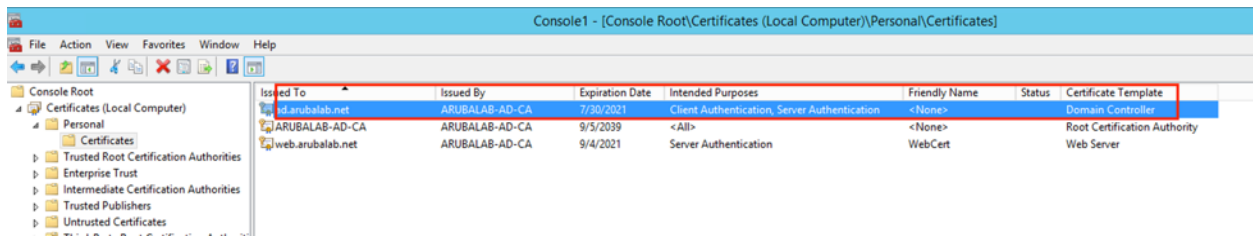








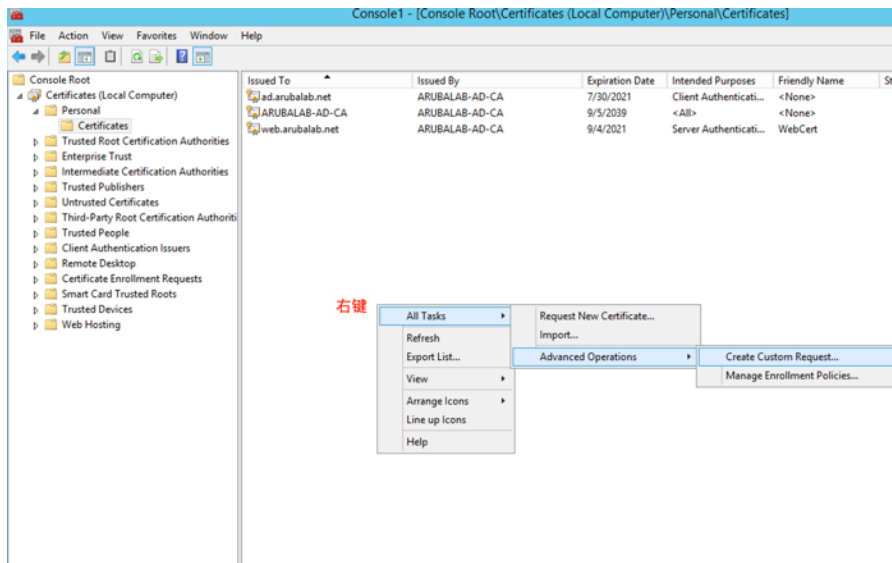
查看有无 Server 证书，注意『Intended Purpose』是 Server Authentication，其他类型不可用，包括 rootCA（例如下图 1、3 可做 Server 证书，2 不可以）

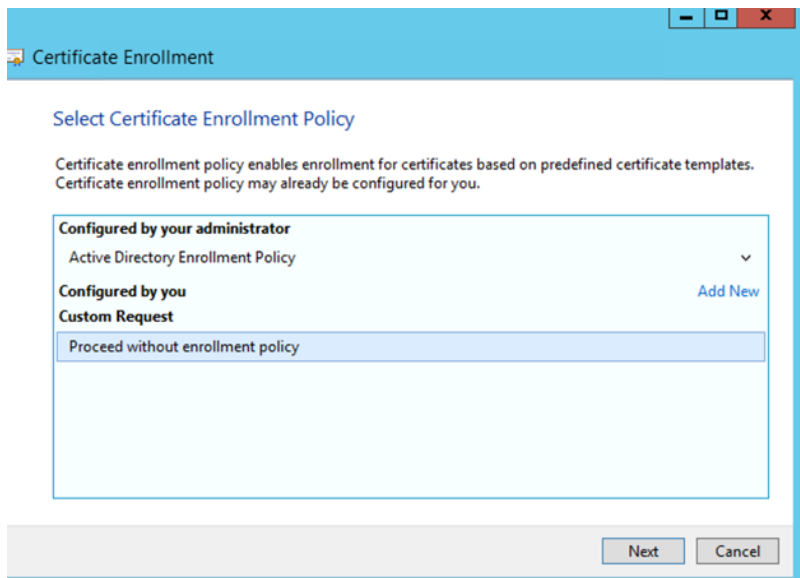
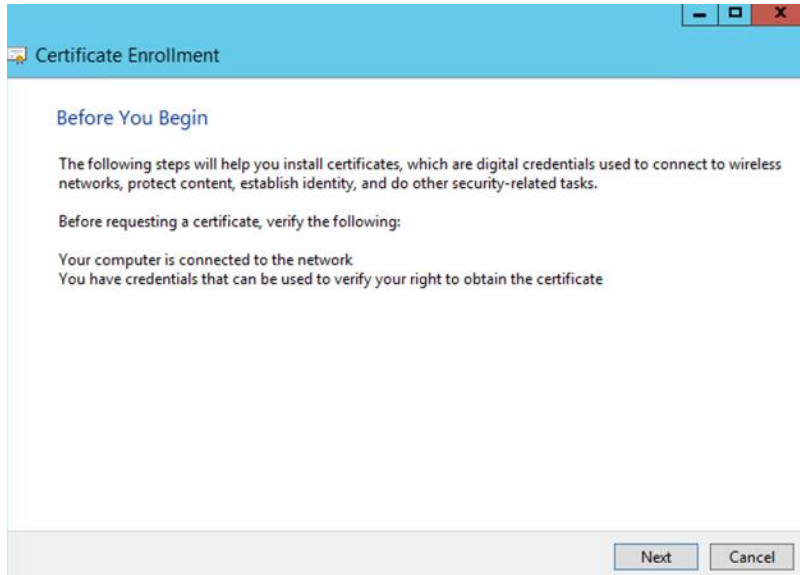


如果没有 Server 证书，继续以下步骤，如有跳过步骤二。

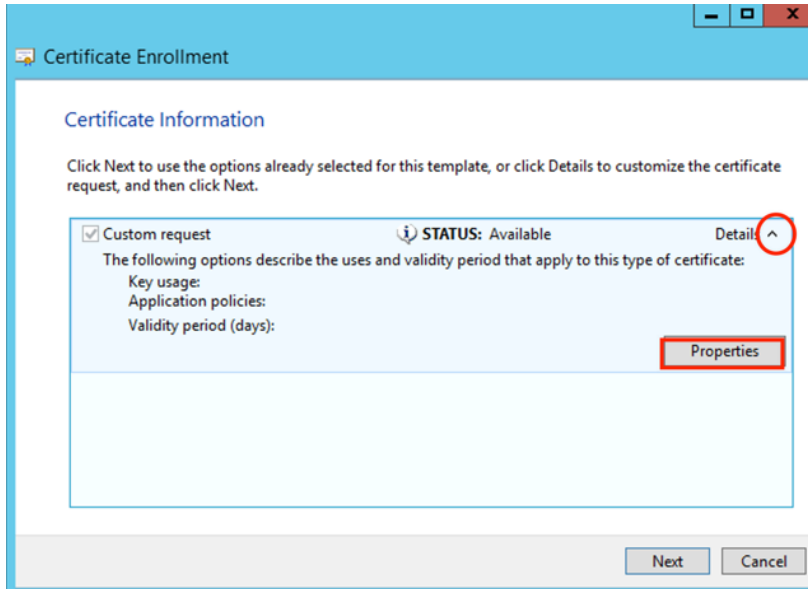
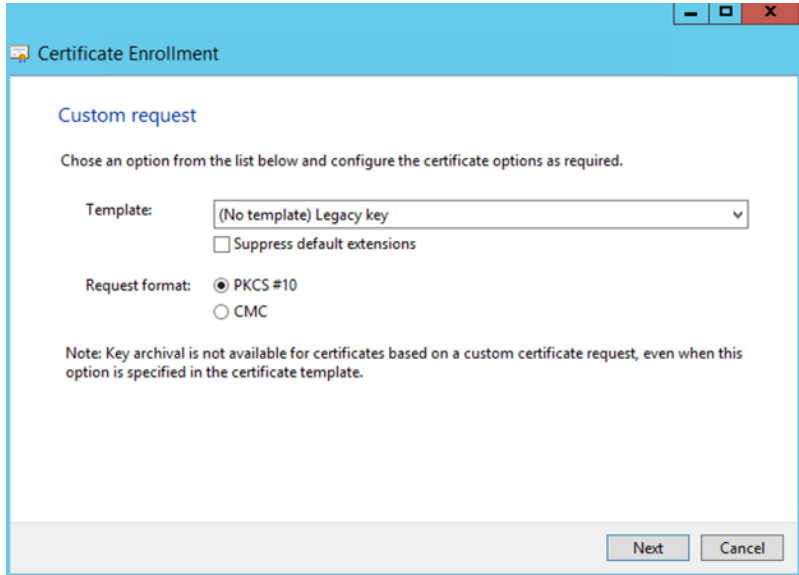
## 3.2 生成 Server 证书 CSR 文件

签发证书需要 CSR 文件，以下步骤为在相应 Server 生成 CSR 文件

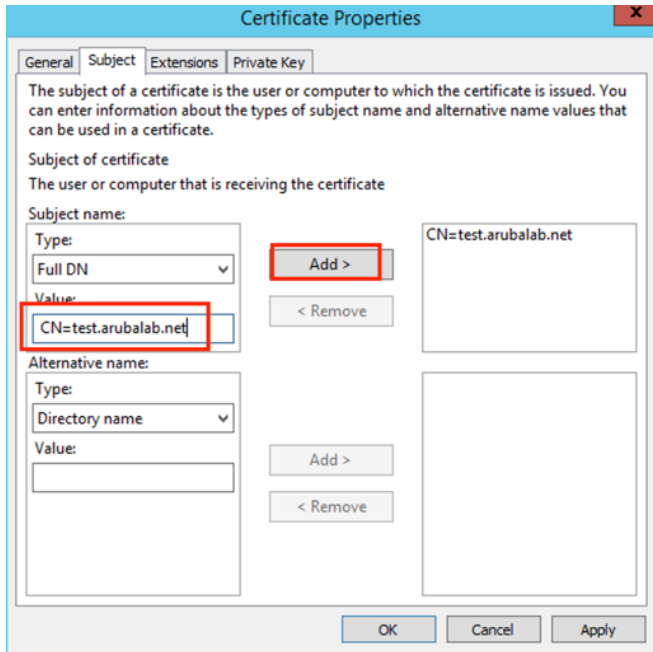




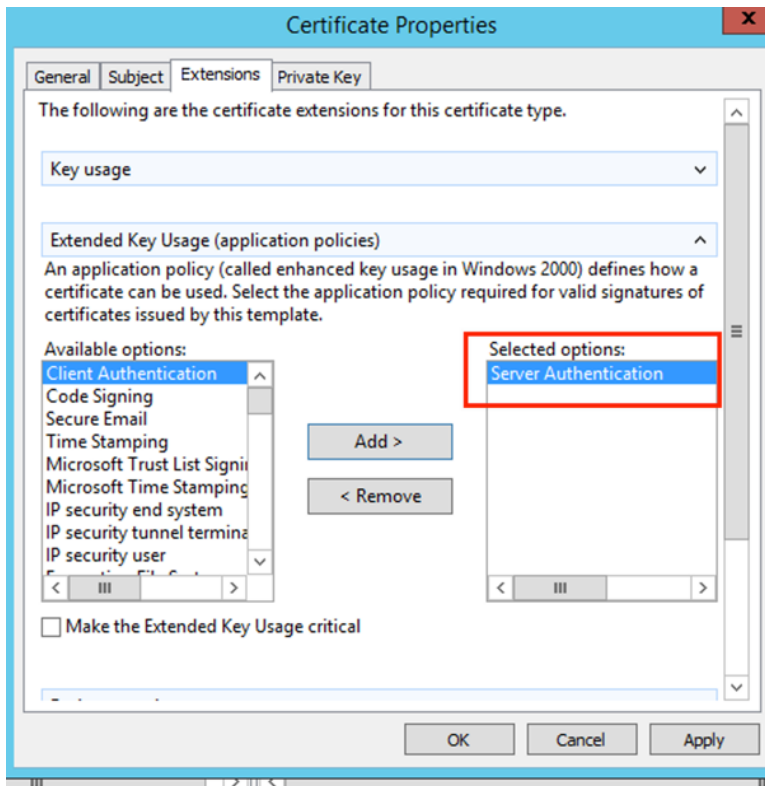




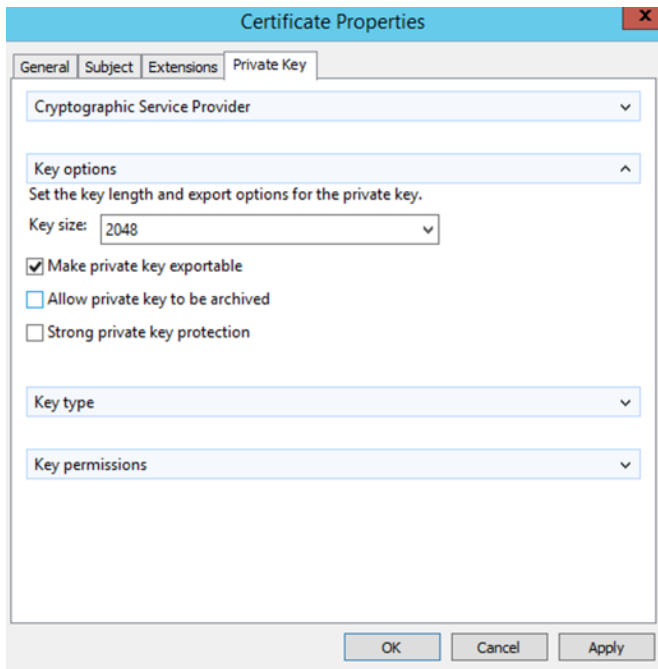
填写 CN 或其他必要信息，例如 OU 等等，根据实际情况。**Server 证书 CN 为必须项。**



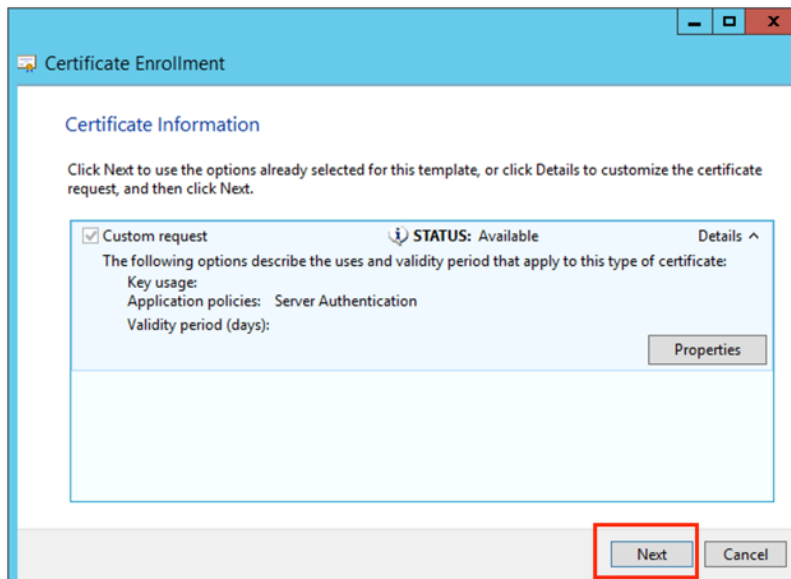
选择证书类型



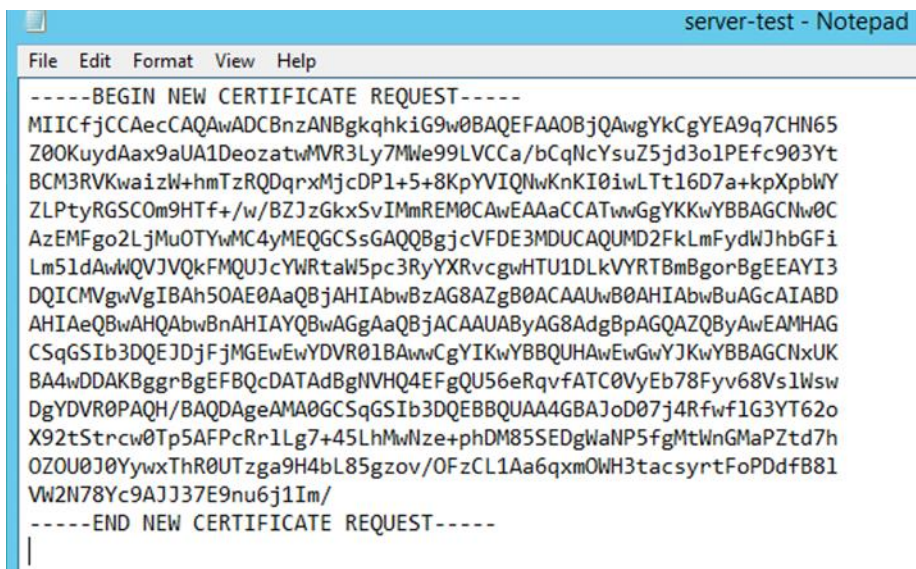
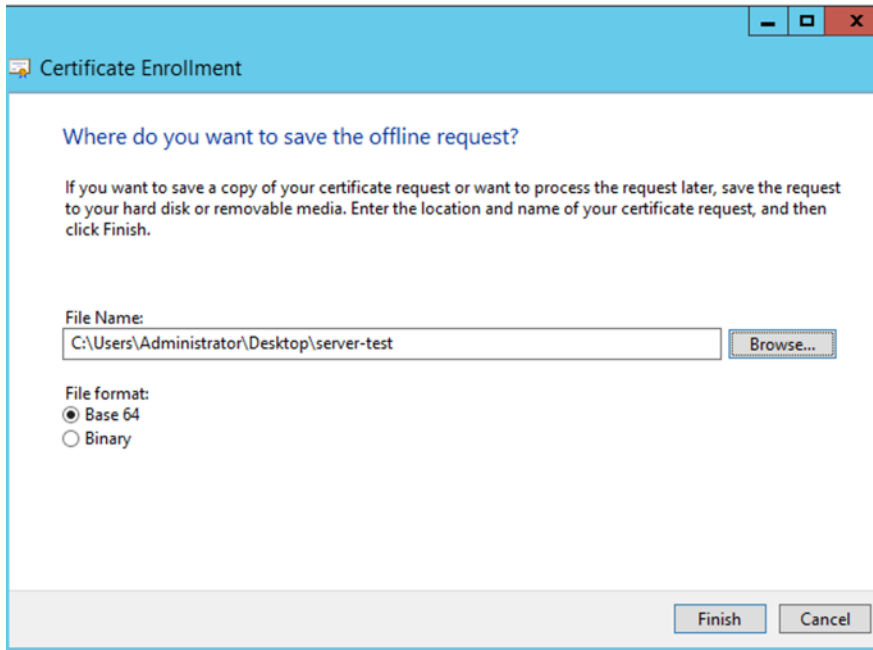
## 选择私钥加密方式



## 下一步完成



存放在桌面，然后用记事本打开



以上步骤已经成功生成 CSR 文件。

### 3.3 签发证书

接下来需要通过 CSR 签发证书。

登录 <http://ServerIP/certsrv>

Sign in  
http://10.0.50.20  
Your connection to this site is not private

Username

Password

Cancel Sign In

## 签发 Server 证书用 AD 管理员账户密码 (Administrator) 登录

← → ↻ ⓘ Not secure | 10.0.50.20/certsrv/Default.asp

Microsoft Active Directory Certificate Services -- ARUBALAB-AD-CA

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate r

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Docu](#)

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

## 选择高级

← → ↻ ⓘ Not secure | 10.0.50.20/certsrv/certrqus.asp

Microsoft Active Directory Certificate Services -- ARUBALAB-AD-CA

### Request a Certificate

Select the certificate type:

- [User Certificate](#)

Or, submit an [advanced certificate request](#).

复制粘贴 CSR 文件内容。选择证书模板为 **Web Server**

Microsoft Active Directory Certificate Services – ARUBALAB-AD-CA

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 or PKCS #7:

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
DgYDVR0PAQH/BAQDAgeAMA0GCSqSgSIb3DQEBBQI
X92tStrcw0Tp5AFpCrr1Lg7+45LhMwNze+phDM
OZOU0J0YywxThR0UTzga9H4bL85gzov/OFzCL1
VW2N78Yc9AJJ37E9nu6j1Im/
-----END NEW CERTIFICATE REQUEST-----
```

**Certificate Template:**

Web Server

**Additional Attributes:**

Attributes:


Submit >

Microsoft Active Directory Certificate Services – ARUBALAB-AD-CA

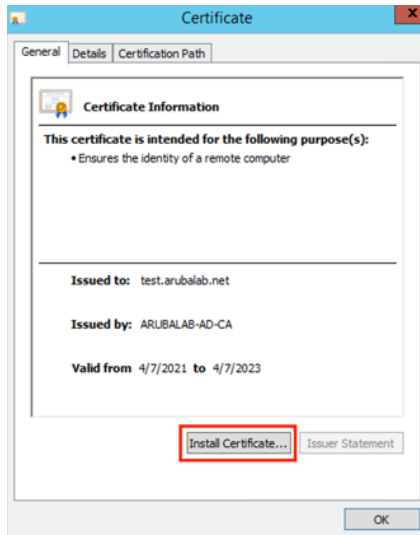
### Certificate Issued

The certificate you requested was issued to you.

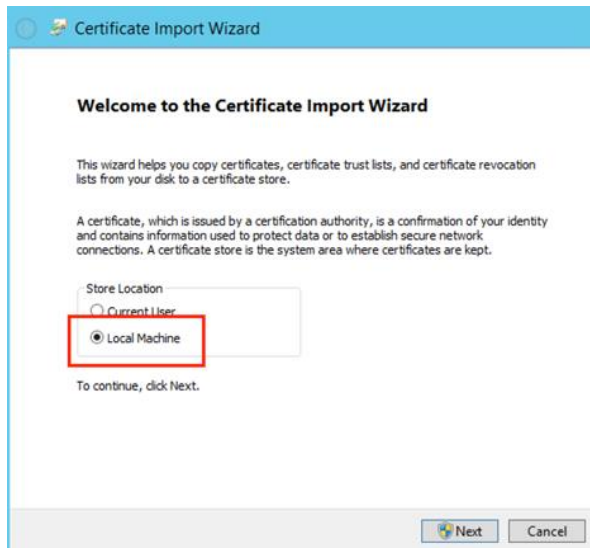
DER encoded or  Base 64 encoded

 [Download certificate](#)  
[Download certificate chain](#)

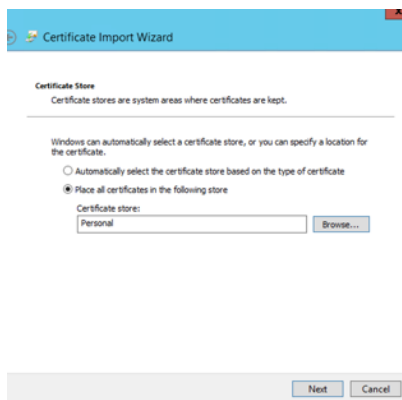
下载并安装证书。双击证书，点击安装，注意查看被颁发者：test.arubalab.net



选择本计算机



选择个人



刷新查看

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
ad.arubalab.net	ARUBALAB-AD-CA	7/30/2021	Client Authentication, Server Authentication	<None>		Domain Controller
ARUBALAB-AD-CA	ARUBALAB-AD-CA	9/5/2039	<All>	<None>		Root Certification Authority
test.arubalab.net	ARUBALAB-AD-CA	4/7/2023	Server Authentication	<None>		Web Server
web.arubalab.net	ARUBALAB-AD-CA	9/4/2021	SERVER AUTHENTICATION	webcert		Web Server

## 第四步：NPS 开启证书认证

### 4.1 修改原有认证方式

如果已有 NPS 采用 PEAP 认证，更改认证方式即可。

Network Policies

Policy Name	Status	Processing Order	Access Type	Source
Secure Wireless Connections	Enabled	1	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999999	Deny Access	Unspecified
Connections to other access servers	Enabled	1000000	Deny Access	Unspecified

Secure Wireless Connections Properties

Configure the constraints for this network policy.  
If all constraints are not matched by the connection request, network access is denied.

Constraints:

- Authentication Methods
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

EAP Types:

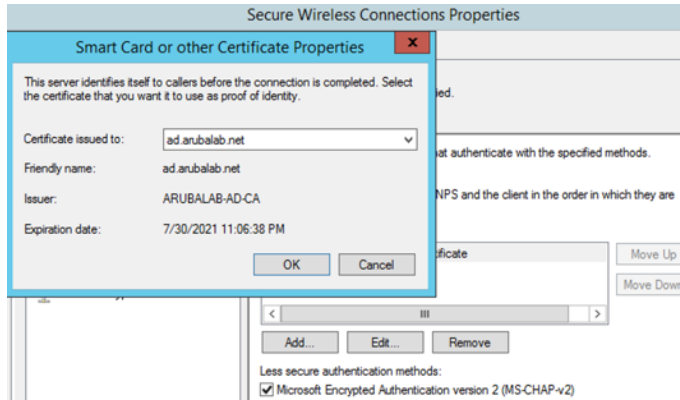
- Microsoft: Smart Card or other certificate

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
- User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
- User can change password after it has expired

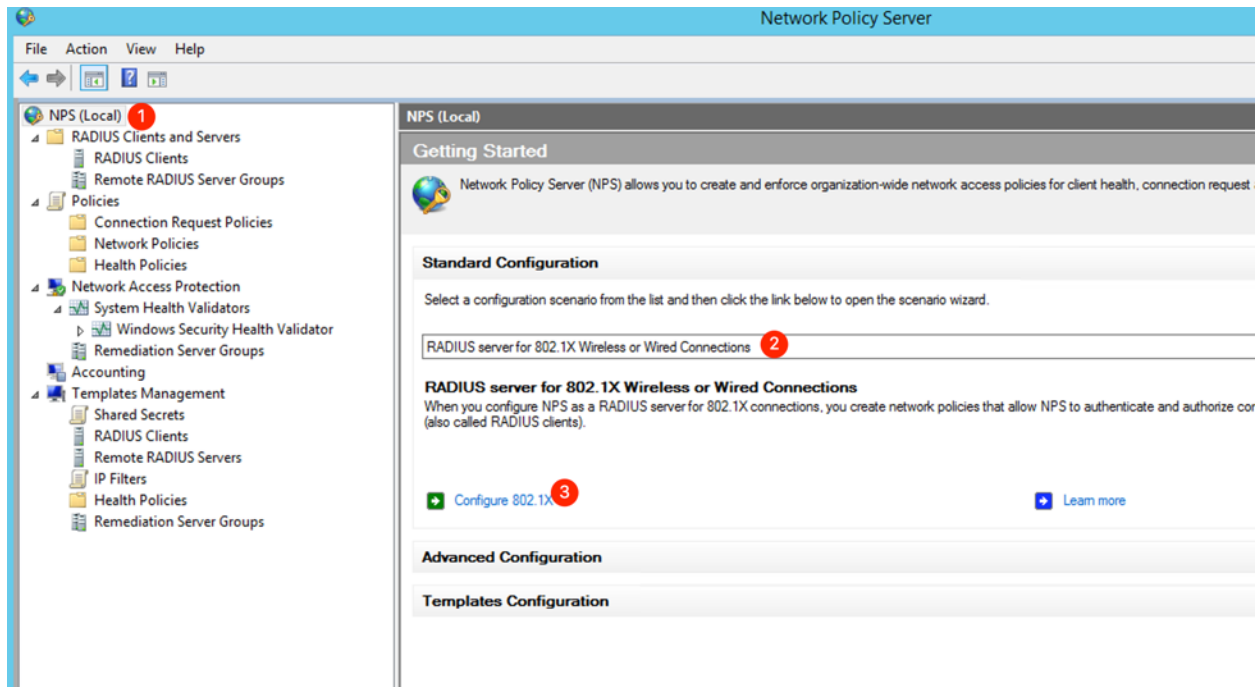
点击 edit 选择 Server 证书（此处必须选择 Server 类型证书，例如步骤二中的 test 亦可）。

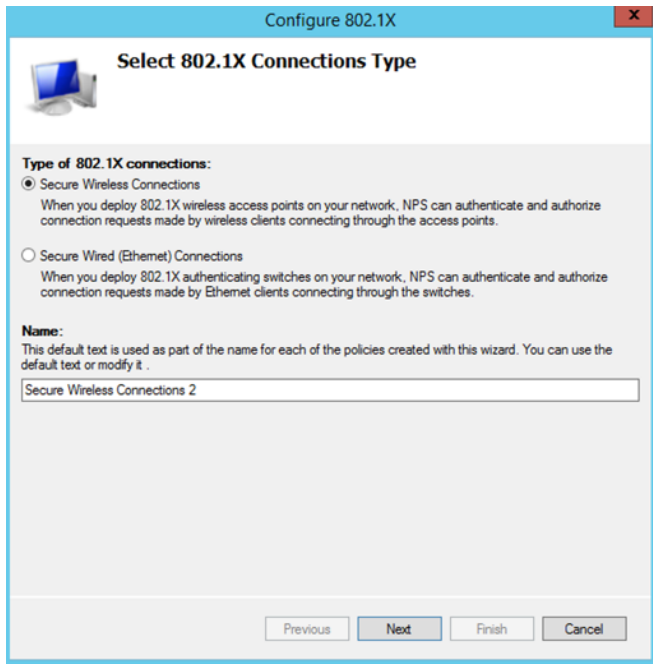




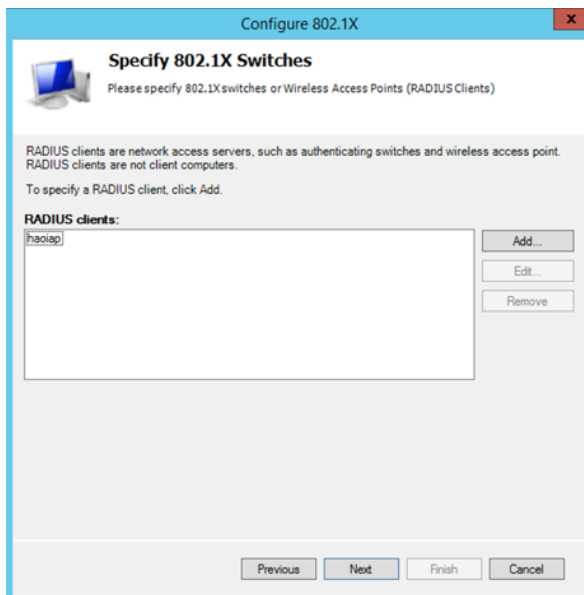
## 4.2 初始化配置 NPS

如果第一次配置 NPS，利用 NPS 向导步骤，如下：





如果没有添加 IAP(NAS 设备), 点击 ADD 添加。已有直接勾选即可。



新建需要填写的内容。

**New RADIUS Client**

Settings

Select an existing template:

Name and Address

Friendly name:

Address (IP or DNS):

Shared Secret

Select an existing Shared Secrets template:

None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual  Generate

Shared secret:

Confirm shared secret:

选择证书认证，选择对应 Server 证书

**Configure an Authentication Method**

Select the EAP type for this policy.

Type (based on method of access and network configuration):

Microsoft: Smart Card or other certificate

**Smart Card or other Certificate Properties**

This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.

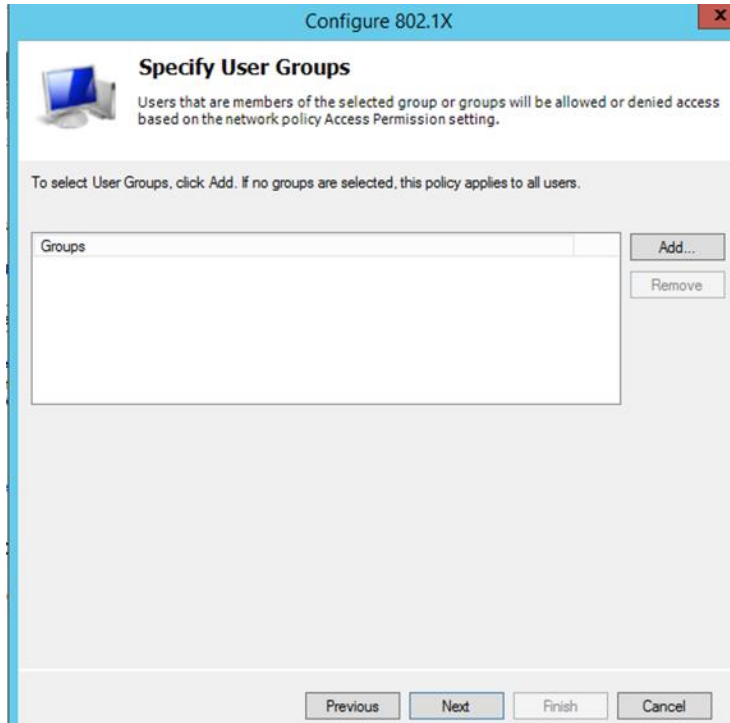
Certificate issued to: ad.arubalab.net

Friendly name: ad.arubalab.net

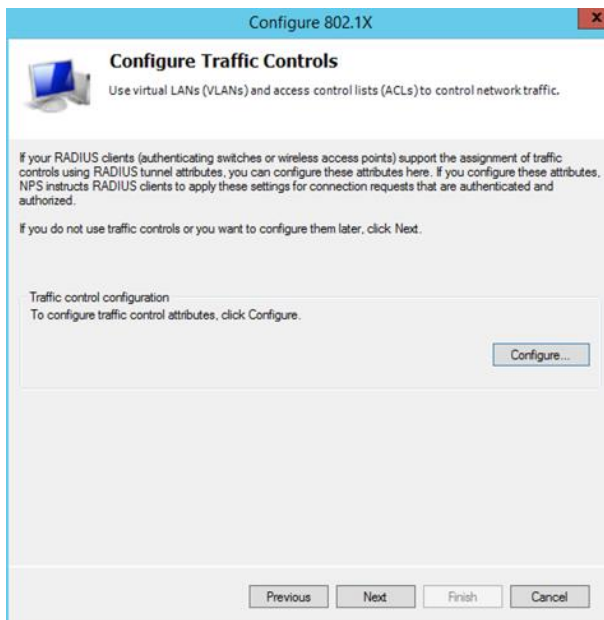
Issuer: ARUBALAB-AD-CA

Expiration date: 7/30/2021 11:06:38 PM

下一步选择添加用户组，通常是 Domain/User

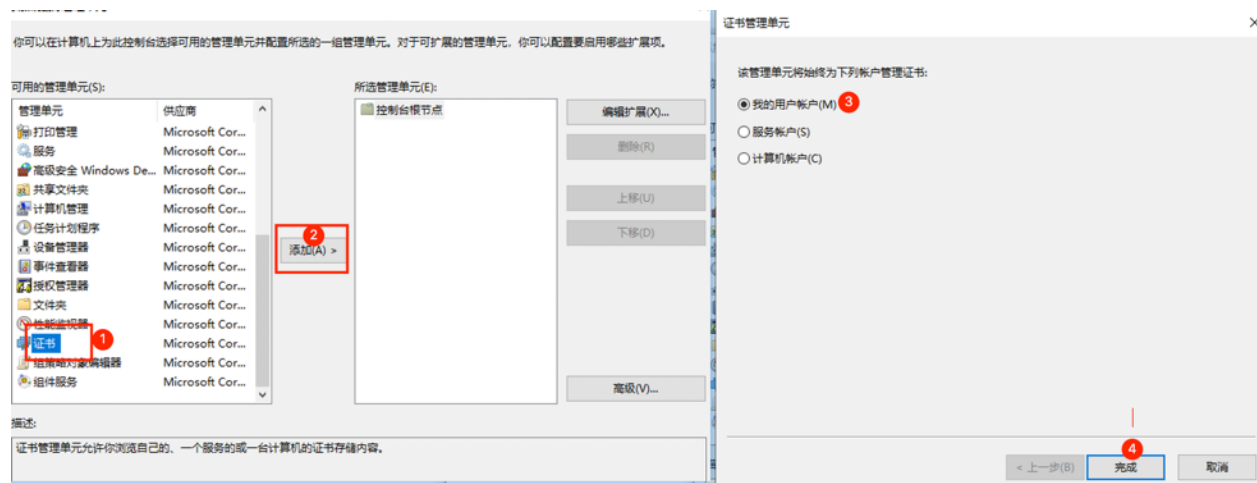
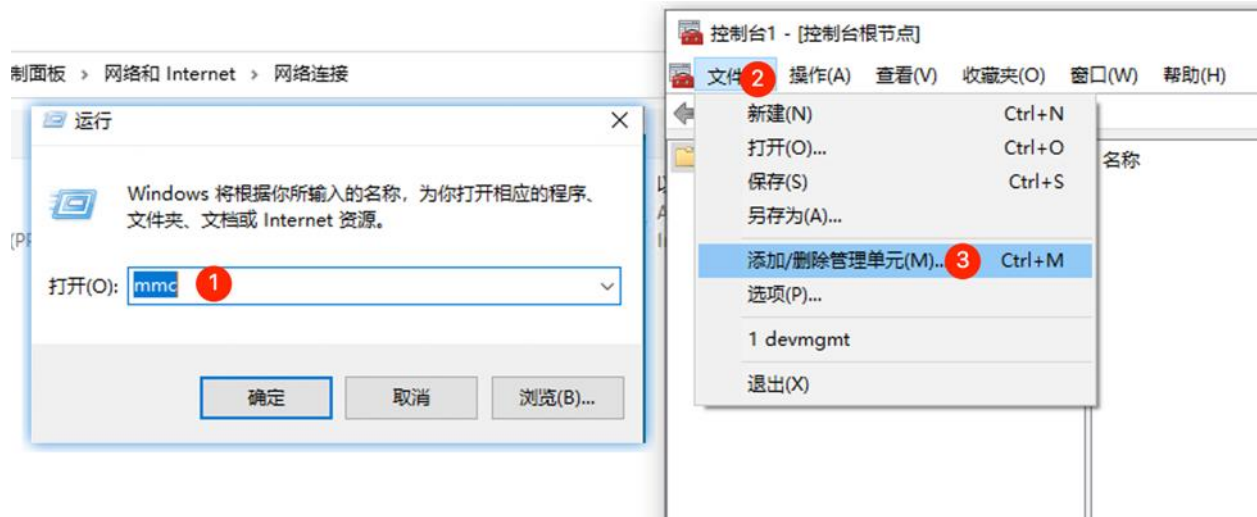


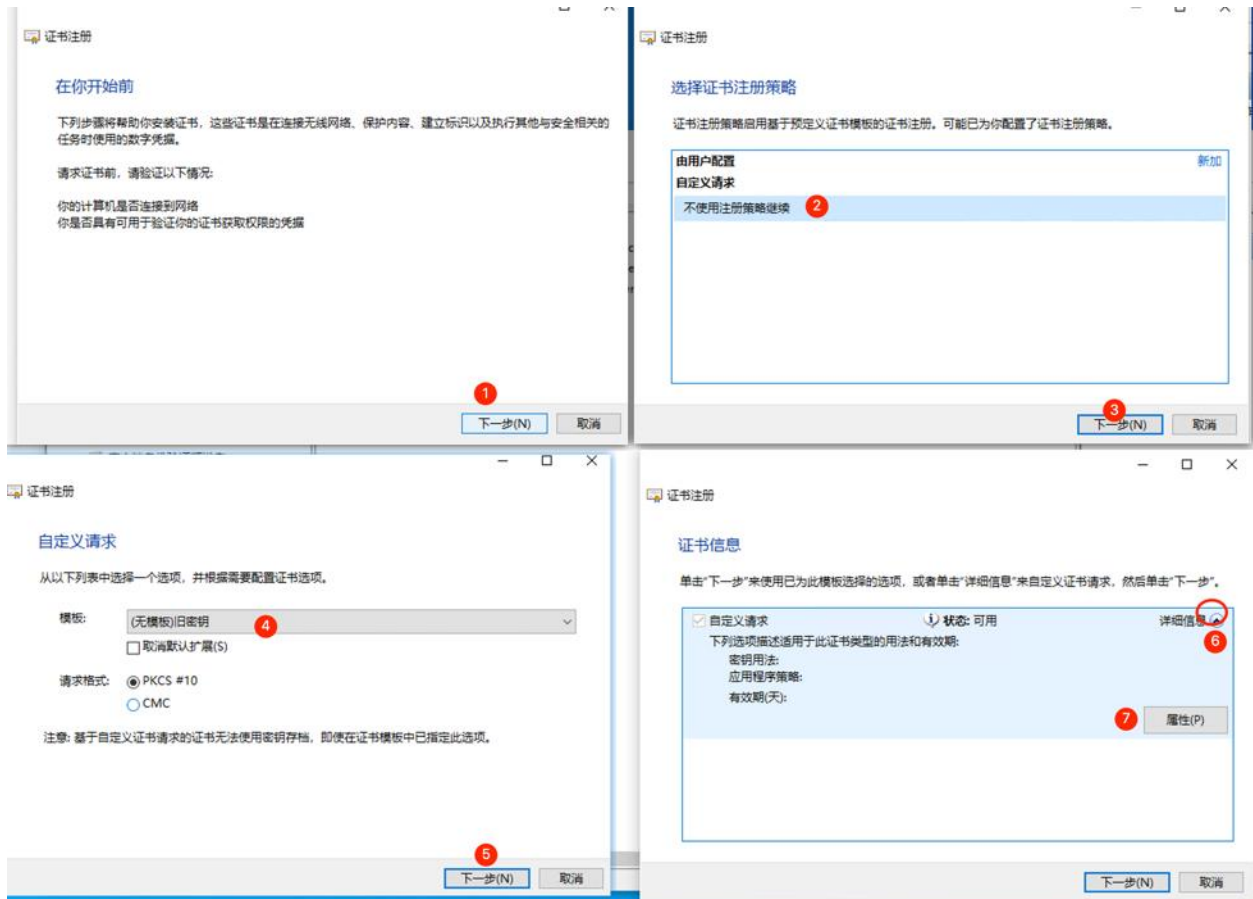
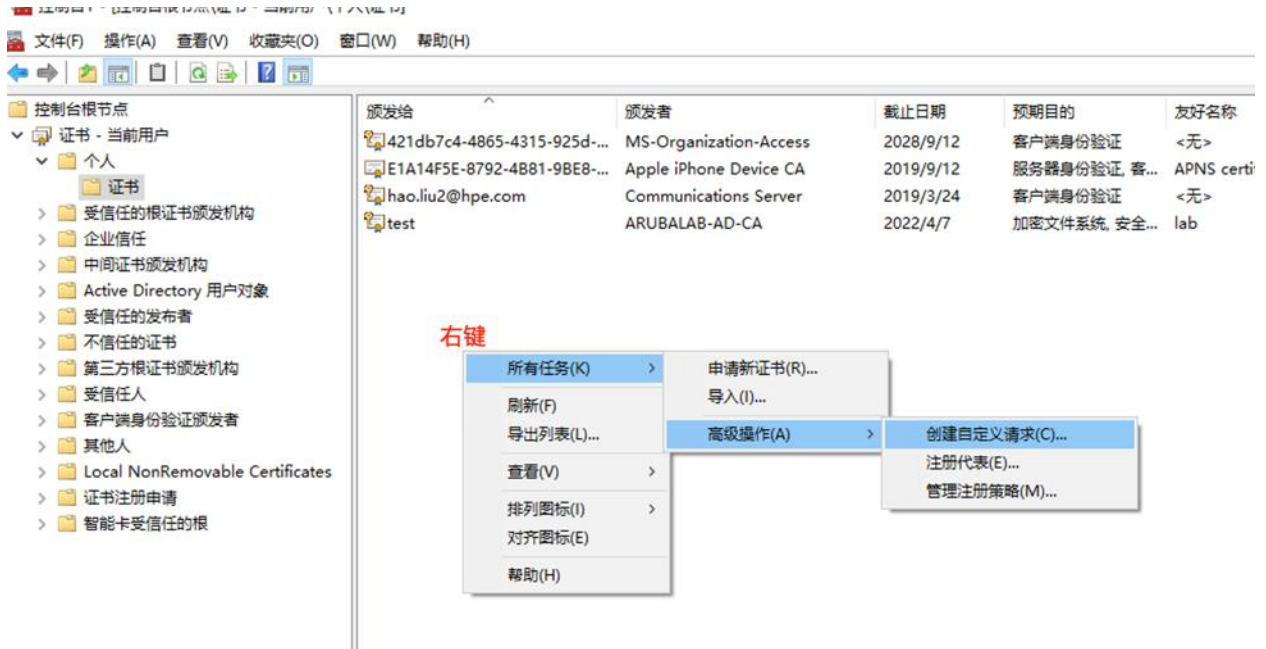
下一步下一步完成即可



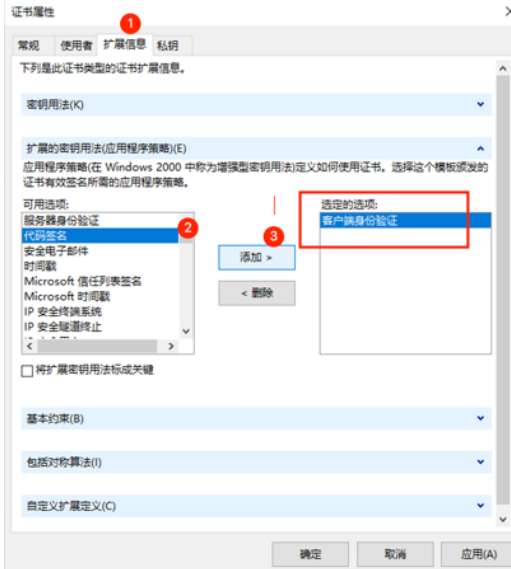
## 第五步：客户端证书签发

### 5.1 客户端 CSR 生成

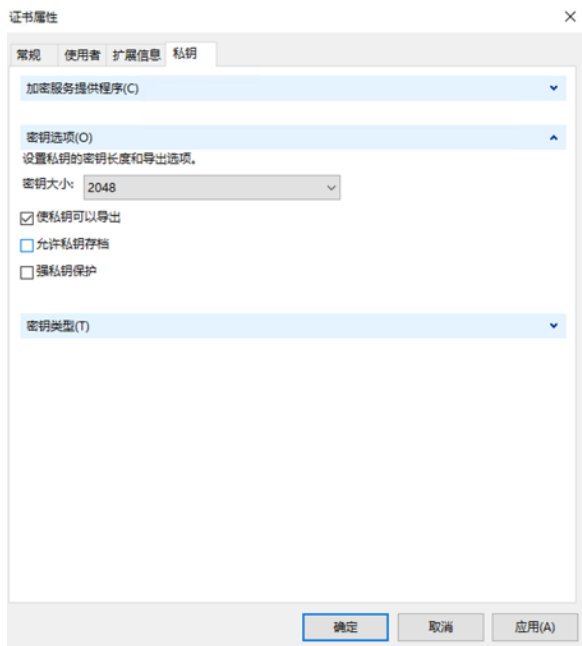




注意客户端证书类型为：客户端身份认证



私钥加密



证书注册

### 证书信息

单击“下一步”来使用已为此模板选择的选项，或者单击“详细信息”来自定义证书请求，然后单击“下一步”。

<input checked="" type="checkbox"/> 自定义请求	状态: 可用	详细信息 ^
下列选项描述适用于此证书类型的用法和有效期:		
密钥用法:		
应用程序策略: 客户端身份验证		
有效期(天):		
		属性(P)

下一步(N)

取消

证书注册

### 你想将脱机请求保存到何处?

如果要保存一份证书请求或者要稍后处理该请求，请将请求保存到硬盘或可移动媒体。输入证书请求的位置和名称，然后单击“完成”。

文件名:

C:\Users\Eoo\Desktop\123

浏览(B)...

文件格式:

Base 64

二进制(V)

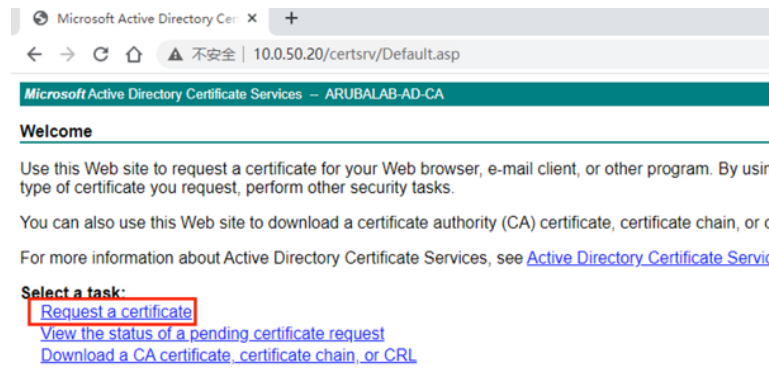
完成(F)

取消

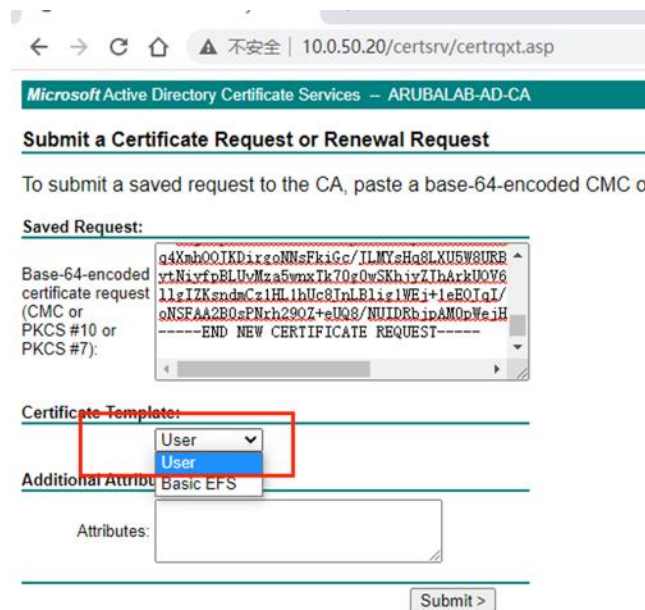


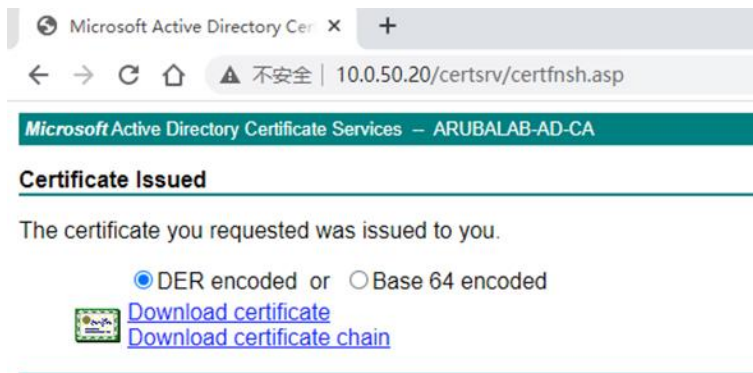
## 5.2 客户端证书签发

用 AD 域用户帐号登录（无需管理员权限），给哪个用户颁发证书，就用哪个用户帐号登录!!!

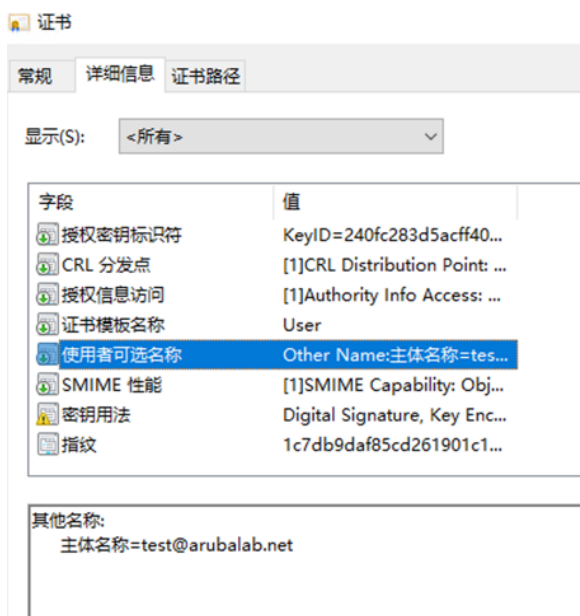


粘贴 CSR 内容，选择 User（非管理员只有 2 个选项!）





双击打开证书查看，证书是颁发给用户 test 的。

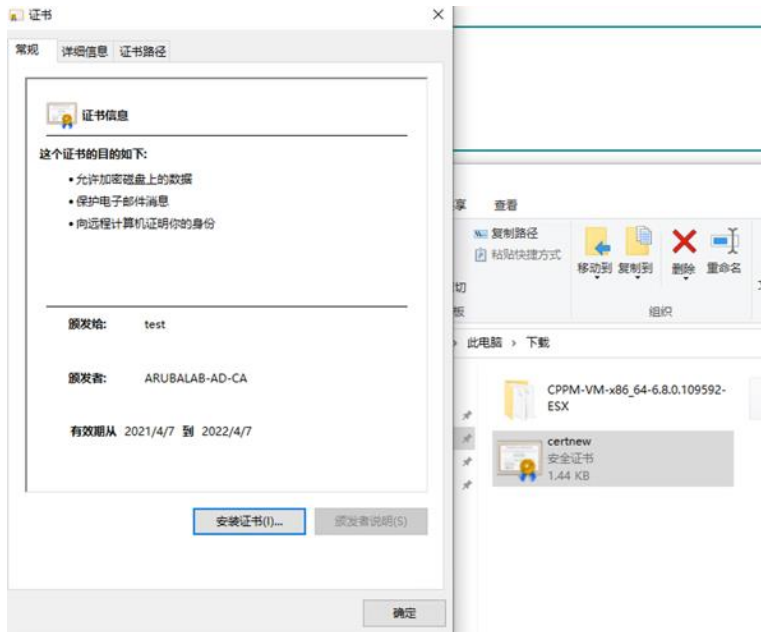


## 第六步：客户端证书安装

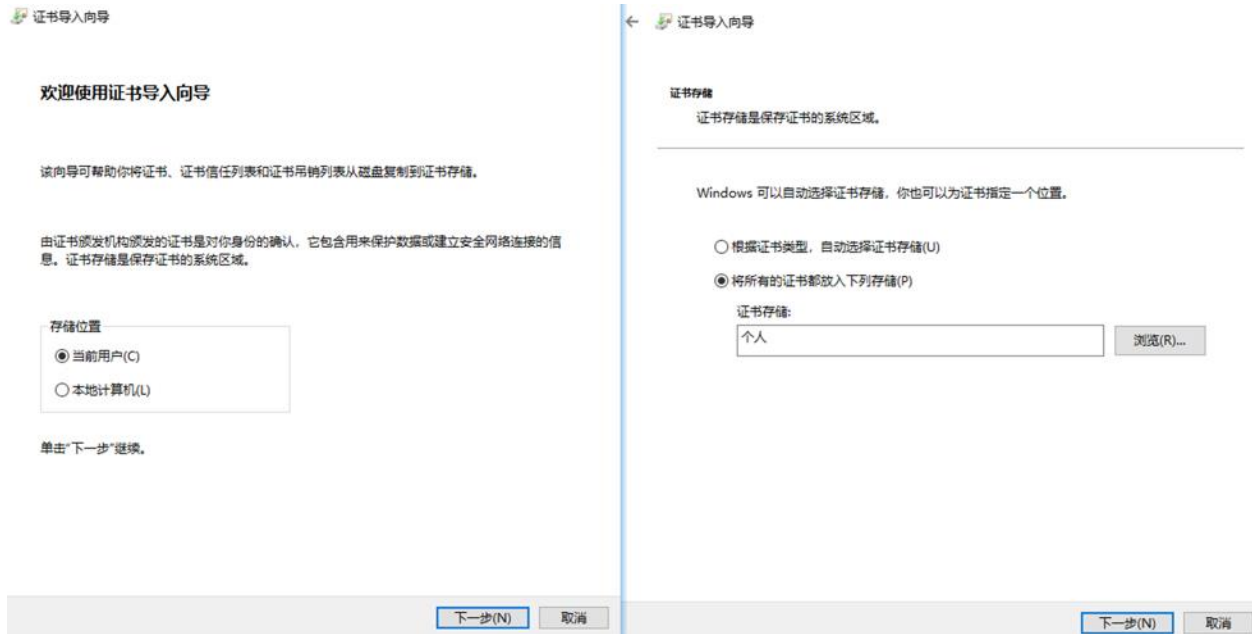
### 6.1 Windows PC

#### 6.1.1 安装终端证书

双击证书点击安装



选择当前用户、位置个人。

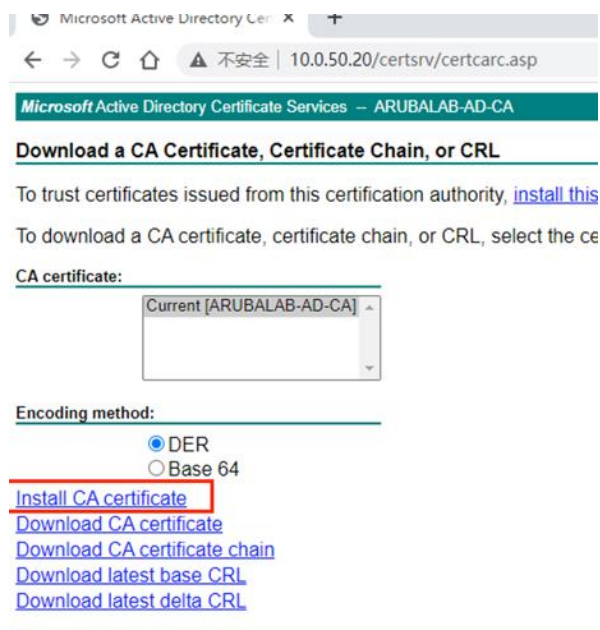
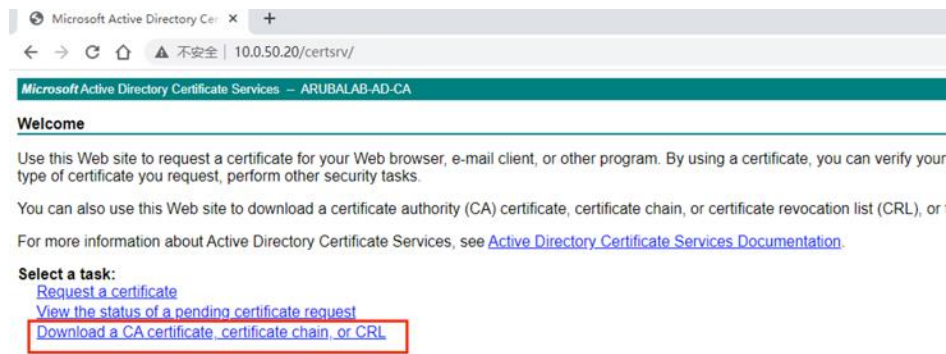


查看证书

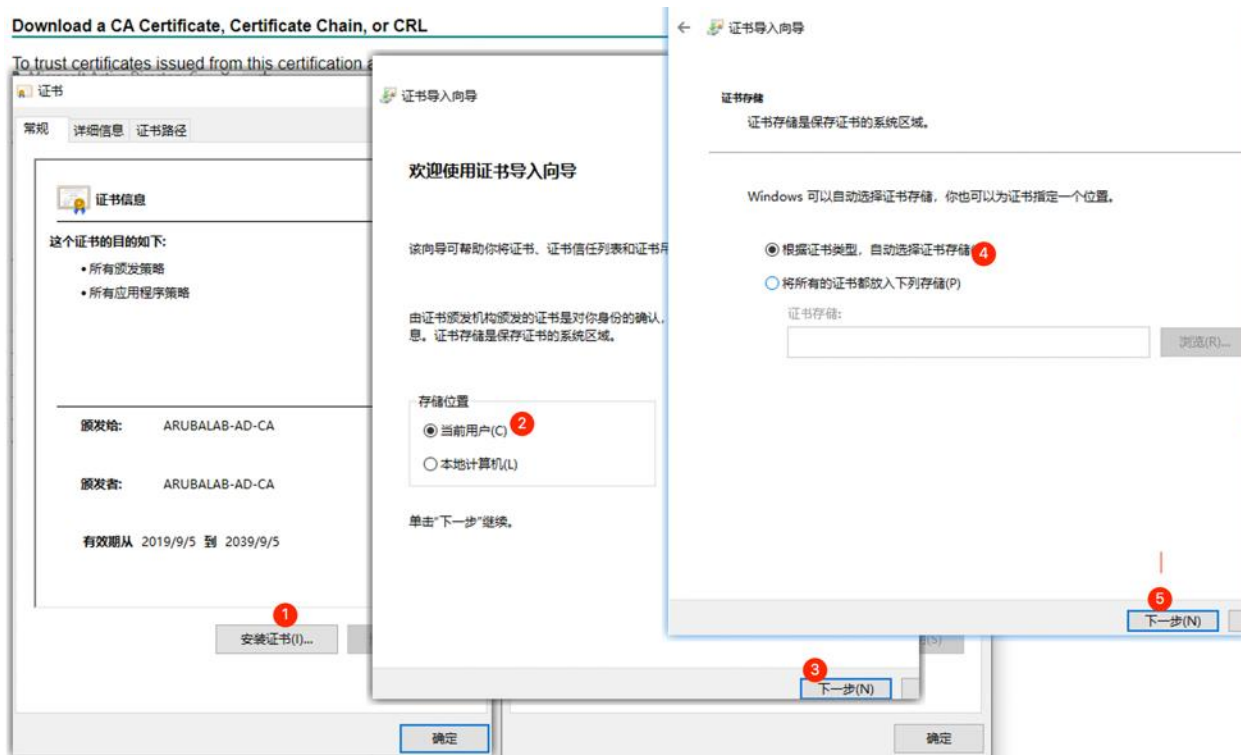


## 6.1.2 安装 root 证书

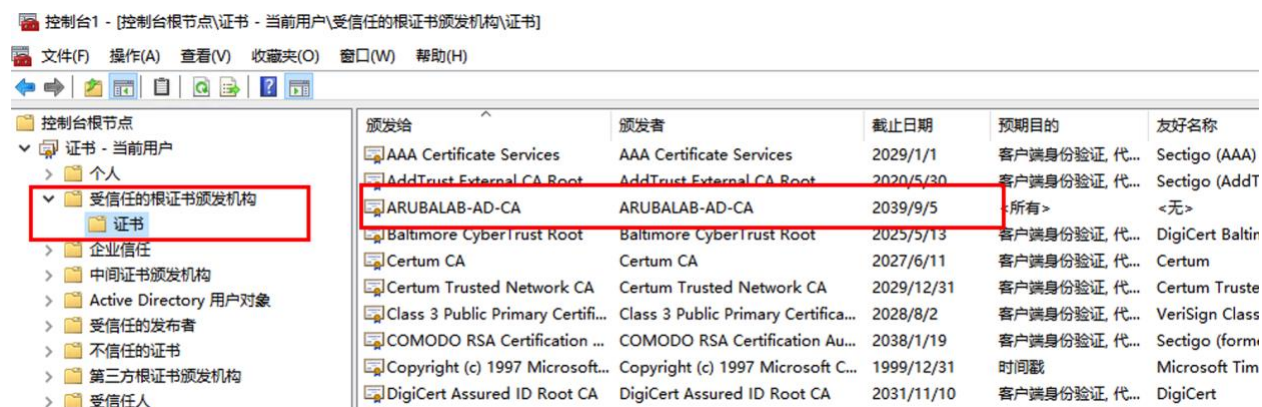
下载 Root 证书，回到首页（页面右上角 home）



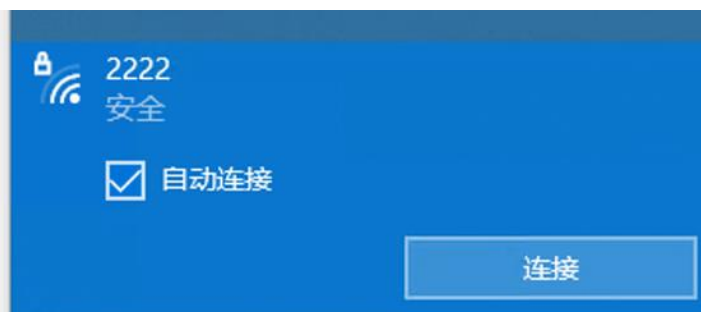
点击安装，会自动下载 root 证书

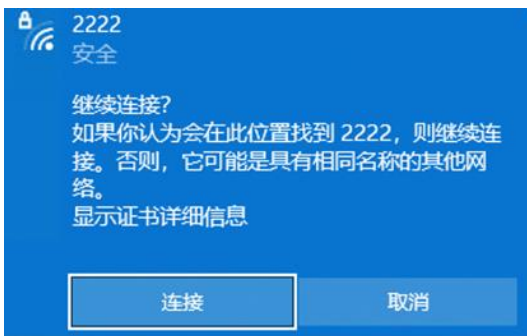


查看 root 证书（注意 root 证书在受信任目录中）



### 5.1.3 终端认证





认证成功

## 属性

SSID: 2222  
协议: Wi-Fi 5 (802.11ac)  
安全类型: WPA2-企业  
**登录信息的类型: Microsoft: 智能卡或其他证书**  
网络频带: 5 GHz  
网络通道: 36  
链接速度(接收/传输): 360/360 (Mbps)  
本地链接 IPv6 地址: fe80::ddc7:f076:747f:8ac8%4  
IPv4 地址: 192.168.10.112  
IPv4 DNS 服务器: 192.168.10.2  
223.5.5.5  
制造商: Intel Corporation  
描述: Intel(R) Dual Band Wireless-AC 7265  
驱动程序版本: 19.51.30.1  
物理地址(MAC): 34-02-86-1F-A0-77

复制

## AP 端查看



The screenshot shows the Aruba Virtual Controller interface. The browser address bar displays 'iap.arubase.club:4343/monitoring/clients/34:2f:bd:ef:51:d2'. The page title is 'aruba | VIRTUAL CONTROLLER | SetMeUp-CE-C7-02'. On the left, there is a navigation menu with '仪表盘' (Dashboard) selected. The main content area shows a table of clients. The table has columns for '名称' (Name), 'IP 地址' (IP Address), 'MAC 地址' (MAC Address), '操作系统' (OS), 'ESSID', '接入点' (AP), '频道' (Channel), '类型' (Type), '角色' (Role), and 'IPv6'. Two rows are visible: one for a switch and one for a client named 'test@arubalab.net'. The client row is highlighted with a red border. Below the table, there are tabs for '概述' (Overview) and '客户端匹配' (Client Matching), with '概述' selected.

名称	IP 地址	MAC 地址	操作系统	ESSID	接入点	频道	类型	角色	IPv6
--	192.168.10.119	34:2f:bd:ef:51:d2	NOFP	Switch	44:48:c1:ce:c7:02	36	AC	Switch	--
test@arubalab.net	192.168.10.112	34:02:86:1f:a0:77	Win 10	2222	44:48:c1:ce:c7:02	36+	AC	2222	fe80::

## 6.2 Android

### 6.2.1 导出终端证书

移动终端无法生成 CSR 文件，可以将 PC 的证书导出后给移动终端使用。导出方法：



控制台1 - [控制台根节点\证书 - 当前用户\个人\证书]

文件(F) 操作(A) 查看(V) 收藏夹(O) 窗口(W) 帮助(H)



- 控制台根节点
  - 证书 - 当前用户
    - 个人
      - 证书
      - 受信任的根证书颁发机构
      - 企业信任
      - 中间证书颁发机构
        - 证书吊销列表
        - 证书
      - 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
      - 其他人
      - Local NonRemovable Ce
      - 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
421db7c4-4865-4315-925d-...	MS-Organization-Access	2028/9/12	客户端身份验证
E1A14F5E-8792-4B81-98E8-...	Apple iPhone Device CA	2019/9/12	服务器身份验证, 客户端身
hao.liu2@hpe.com	Communications Server	2019/3/24	客户端身份验证
test	MS-MAB-AD-CA	2022/4/7	加密文件系统, 安全电子邮
test	MS-MAB-AD-CA	2022/4/7	加密文件系统, 安全电子邮

- 打开(O)
- 所有任务(K) >
  - 打开(O)
  - 用新密钥申请证书(Q)...
  - 用新密钥续订证书(N)...
  - 高级操作(A) >
  - 导出(E)...
- 剪切(T)
- 复制(C)
- 删除(D)
- 属性(R)
- 帮助(H)

← 证书导出向导

#### 导出私钥

你可以选择将私钥和证书一起导出。

私钥受密码保护。如果要私钥跟证书一起导出，你必须在后面一页上键入密码。

你想将私钥跟证书一起导出吗？

- 是，导出私钥(Y)
- 不，不要导出私钥(O)



导出文件格式

可以用不同的文件格式导出证书。

选择要使用的格式:

- DER 编码二进制 X.509 (.CER)(D)
- Base64 编码 X.509(.CER)(S)
- 加密消息语法标准 - PKCS #7 证书(.P7B)(C)
  - 如果可能, 则包括证书路径中的所有证书(I)
- 个人信息交换 - PKCS #12(.PFX)(P)
  - 如果可能, 则包括证书路径中的所有证书(U)
  - 如果导出成功, 删除私钥(K)
  - 导出所有扩展属性(A)
  - 启用证书隐私(E)
- Microsoft 系列证书存储(.SST)(T)

下一步(N)

取消

输入密码并记住密码, 证书在导入手机时需要输入

安全

若要维护安全, 必须保护安全主体的私钥或使用密码。

组或用户名(建议)(G)

添加(A)

移除(R)

密码(P):

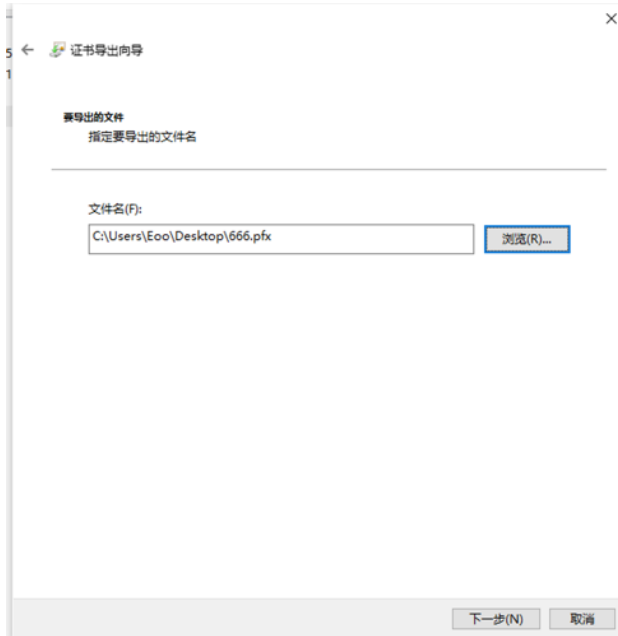
确认密码(C):

加密:

TripleDES-SHA1

下一步(N)

取消



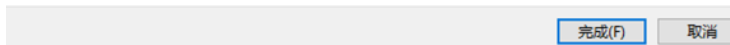
← 证书导出向导

### 正在完成证书导出向导

你已成功完成证书导出向导。

你已指定下列设置:

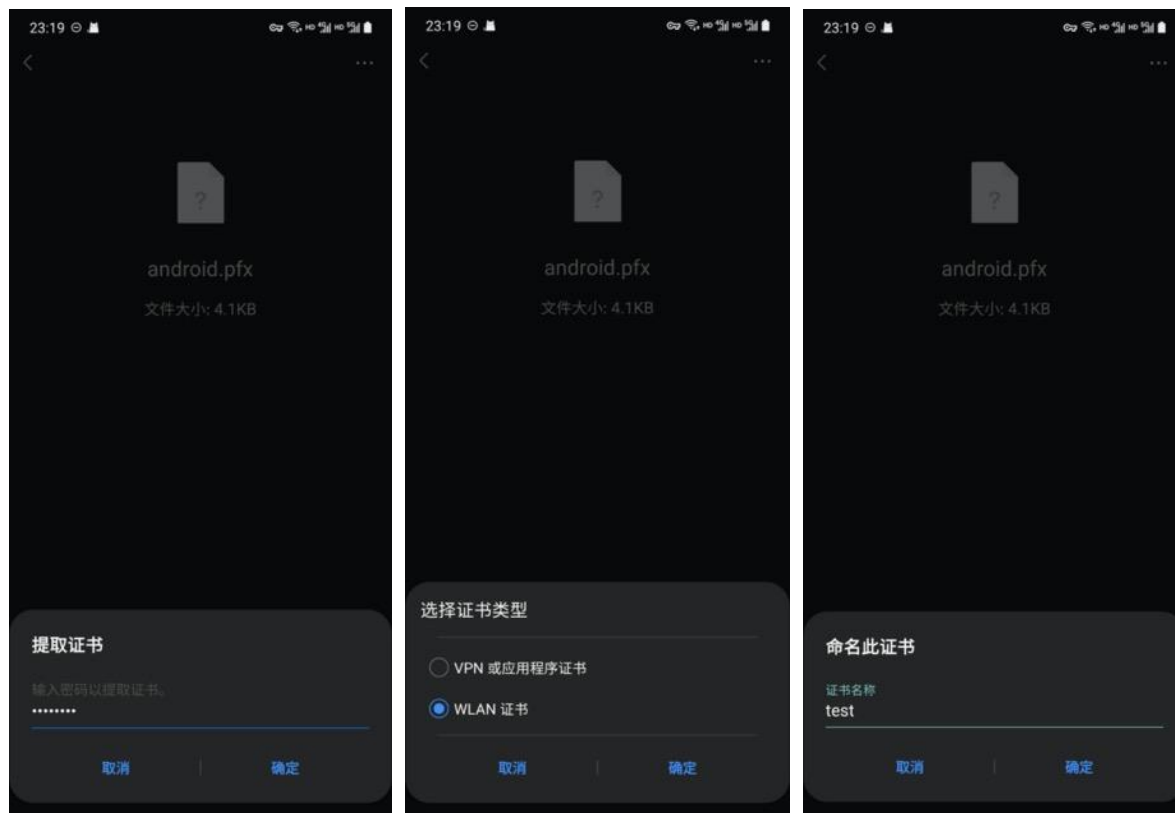
文件名	C:\Users\Eoo\Desktop\666.pfx
导出密钥	是
包括证书路径中的所有证书	是
文件格式	个人信息交换 (*.pfx)



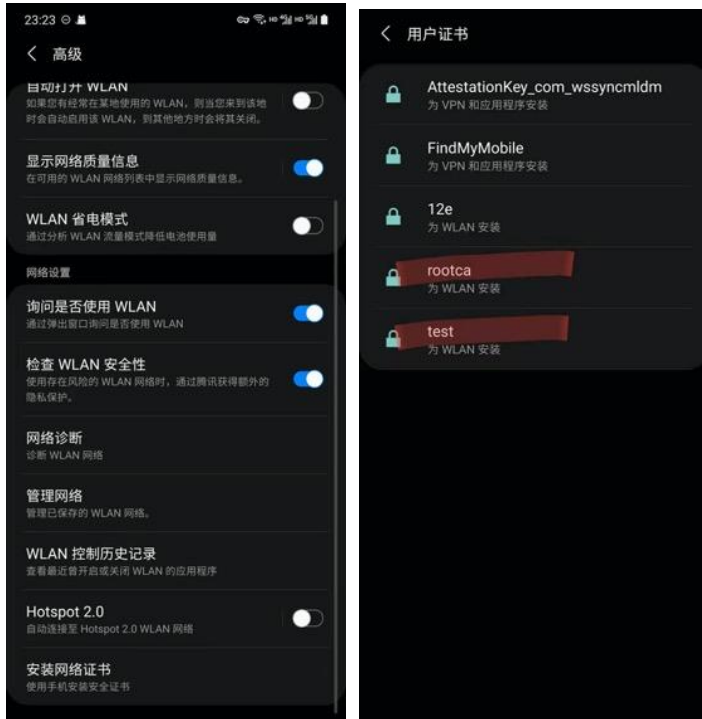
同样步骤导出 Root 证书，向导下一步下一步即可。过程略。

## 6.2.2 安装终端证书

请使用微信或者其他文件浏览器，将证书存放在手机相关位置，然后安装。以下以三星为例。

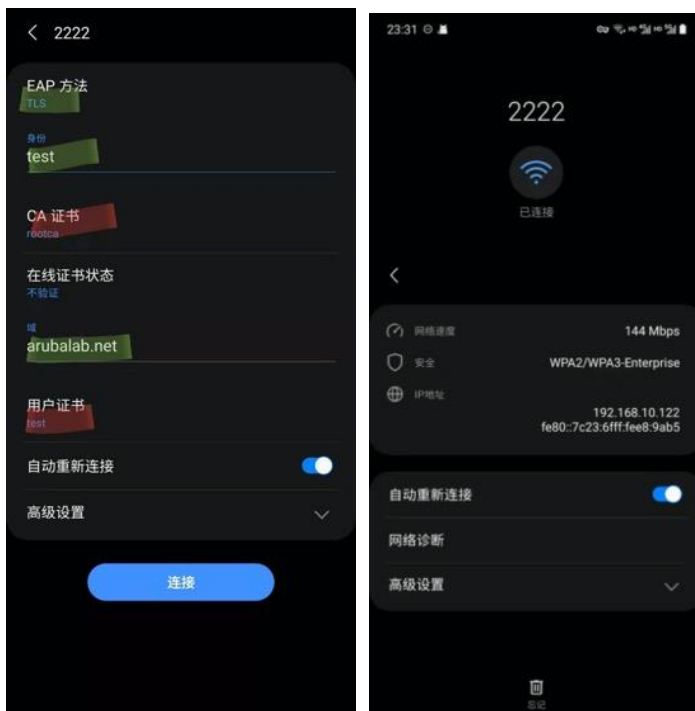


安装 root 证书



## 6.2.3 认证配置

其他手机参考设置。认证方式选择 EAP-TLS，CA 证书选择 root CA，用户证书选择对应的终端证书，填写用户名即可（无需密码）。即可链接。



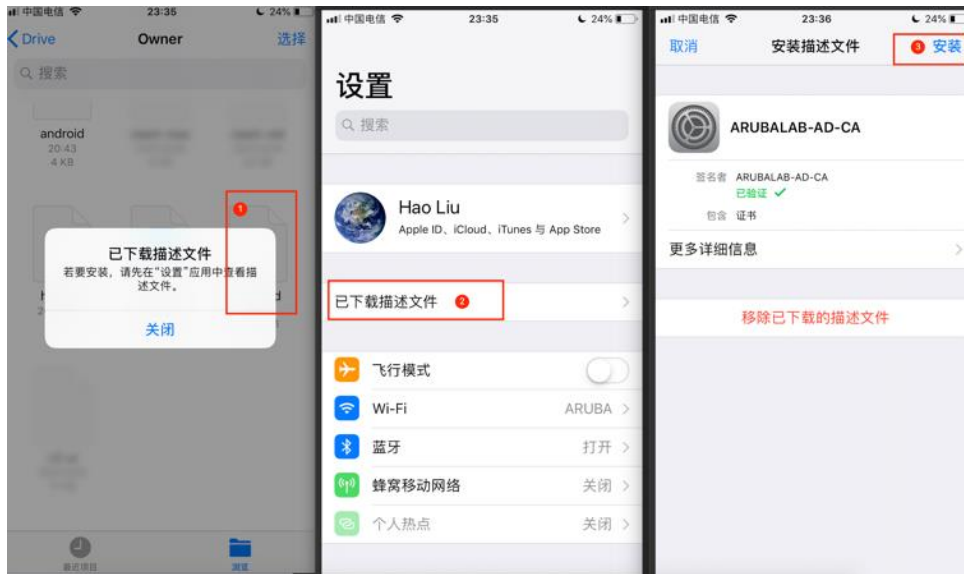
## 6.3 IOS

### 6.3.1 证书导出

略。跟 5.2.1 一样，需要 root 证书及终端证书。

### 6.3.2 证书安装

需要讲证书存在手机，通过『文件』安装。

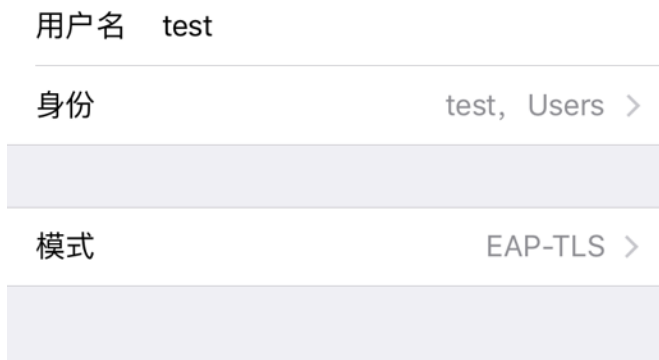


安装后查看描述文件，包含 root 和终端证书



### 6.3.3 认证配置

模式选择 EAP-TLS，输入用户名，身份选择终端证书即可。



由于采用私有证书，需要点击信任。



#### AP 端查看

名称	IP 地址	MAC 地址	操作系统	ESSID	接入点	频道	类型	角色
test	192.168.10.122	7e:23:6f:e8:9a:b5	Linux	2222	44:48:c1:ce:c7:02	11	GN	2222
--	192.168.10.119	34:2f:bd:ef:51:d2	NOFP	Switch	44:48:c1:ce:c7:02	36	AC	Switch
test@arubalab.net	192.168.10.112	34:02:86:1f:a0:77	Win 10	2222	44:48:c1:ce:c7:02	36+	AC	2222
test	192.168.10.110	10:41:7f:a5:e0:17	Apple	2222	44:48:c1:ce:c7:02	11	GN	2222

概述 客户端匹配



