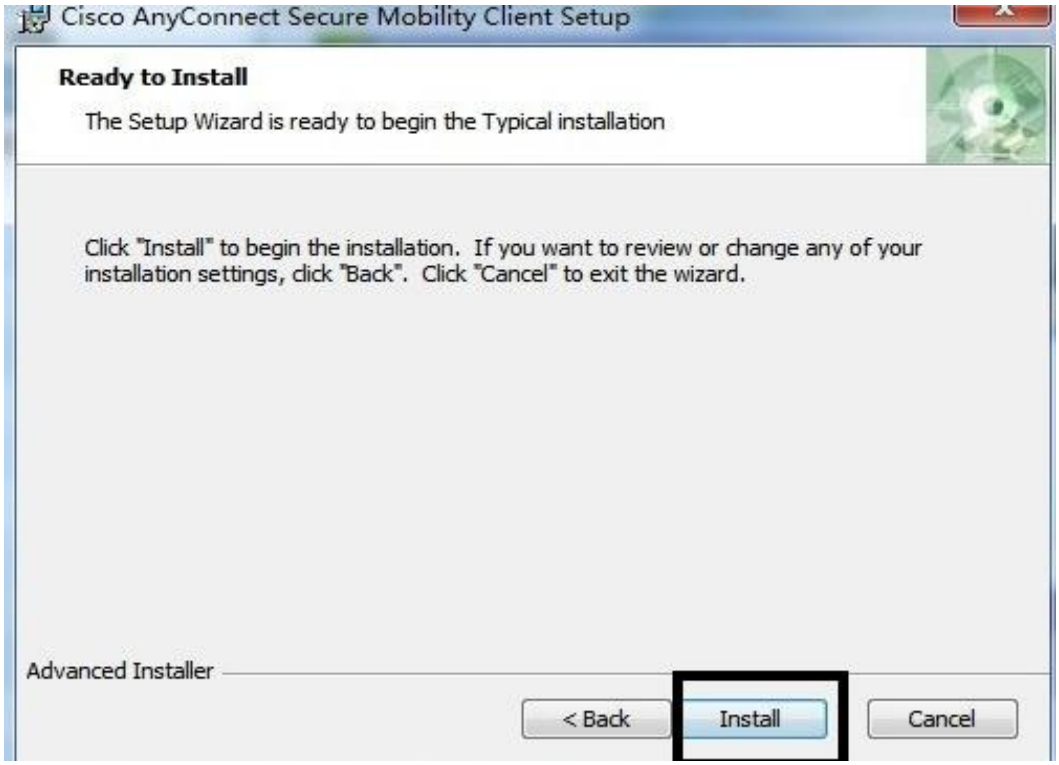
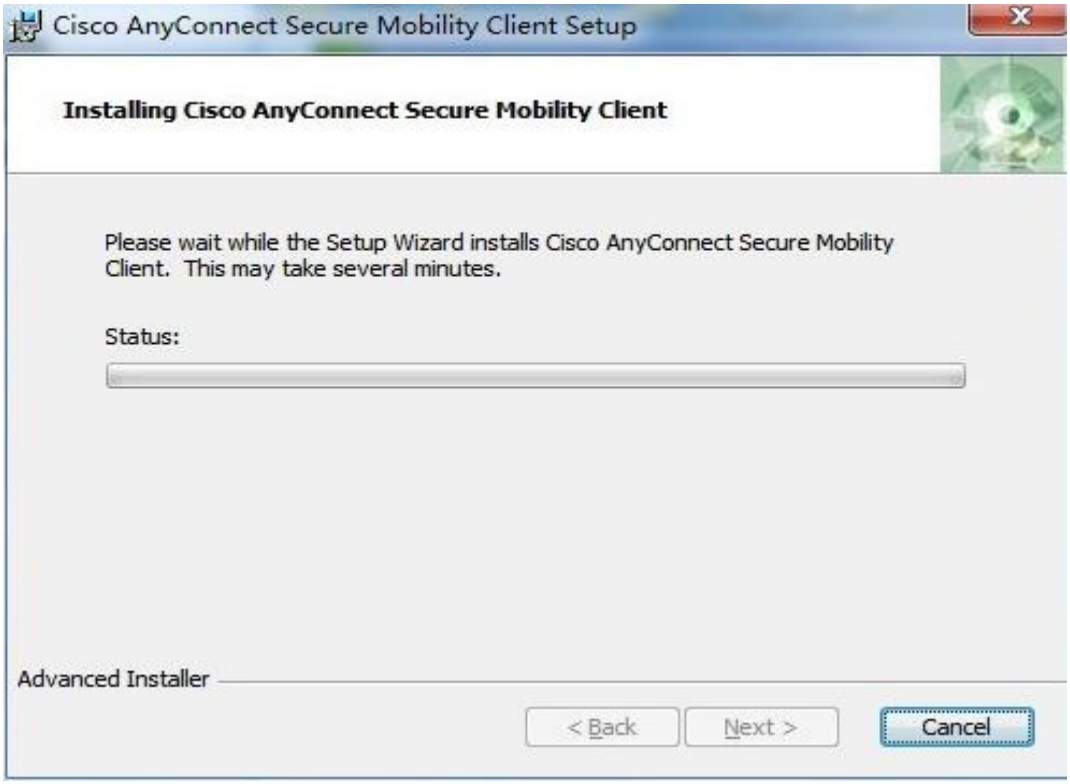
客户端安装

Windows Anyconnect 密码连接

1. 首先下载安装 CISCO AnyConnect Secure MobilityClient，然后安装。安装步骤也是傻瓜式的，一直点下一步，然后接受协议就 OK 了。使用方法如下：

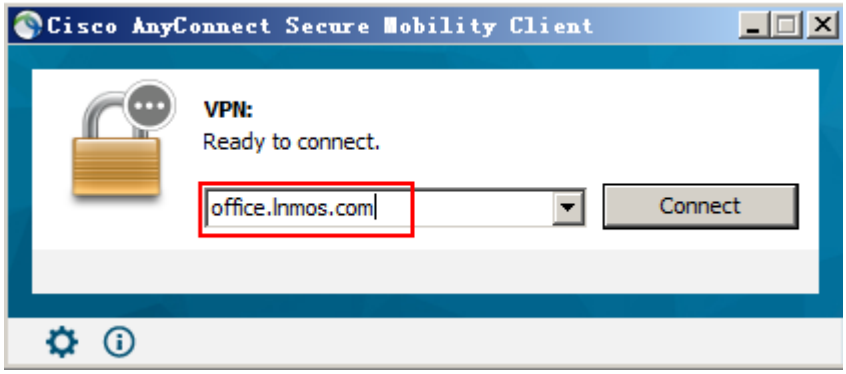

Cisco AnyConnect Secure Mobility Client Setup
End-User License Agreement
Please read the following license agreement carefully
Supplemental End User License Agreement for AnyConnect® Secure Mobility Client v4.x and other VPN-related Software
IMPORTANT: READ CAREFULLY
This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
Advanced Installer
< Back
Next >
Cancel


Cisco AnyConnect Secure Mobility Client Setup
Ready to Install
The Setup Wizard is ready to begin the Typical installation
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.
Advanced Installer
< Back
Install
Cancel



注意：安装后不会在桌面创建图标，请在开始菜单-所有程序，找到程序 Cisco AnyConnect Secure Mobility client，点击打开。

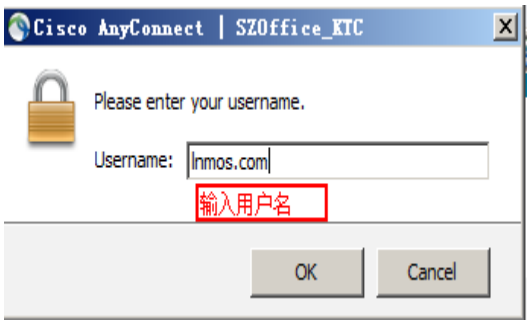
2. 打开 CISCO AnyConnect Secure MobilityClient 后，在框里输入服务器 IP 地址，然后点击 Connect，如下图所示。

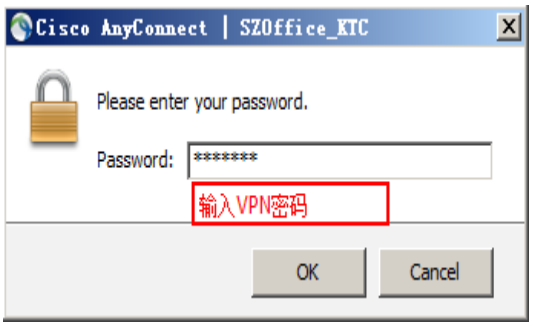


如果之前没用过我们的 VPN 会出现下面的界面(即没有导入我们的 CA 证书)，点击 Change settings 请修改设置为允许连接不信任的服务器地址，如下图所示：

去掉 Block connections to untrusted servers 勾选，设置好了之后关闭。

3. 再点击 Connect 来连接，有时会弹出对话框，点继续就可以了，输入

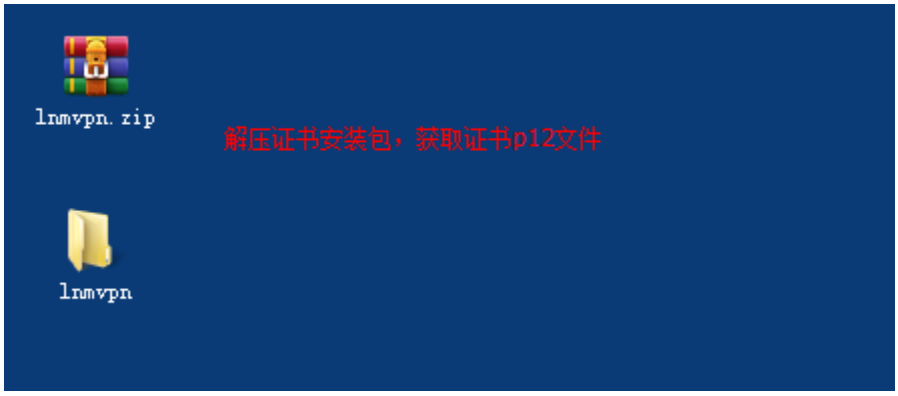




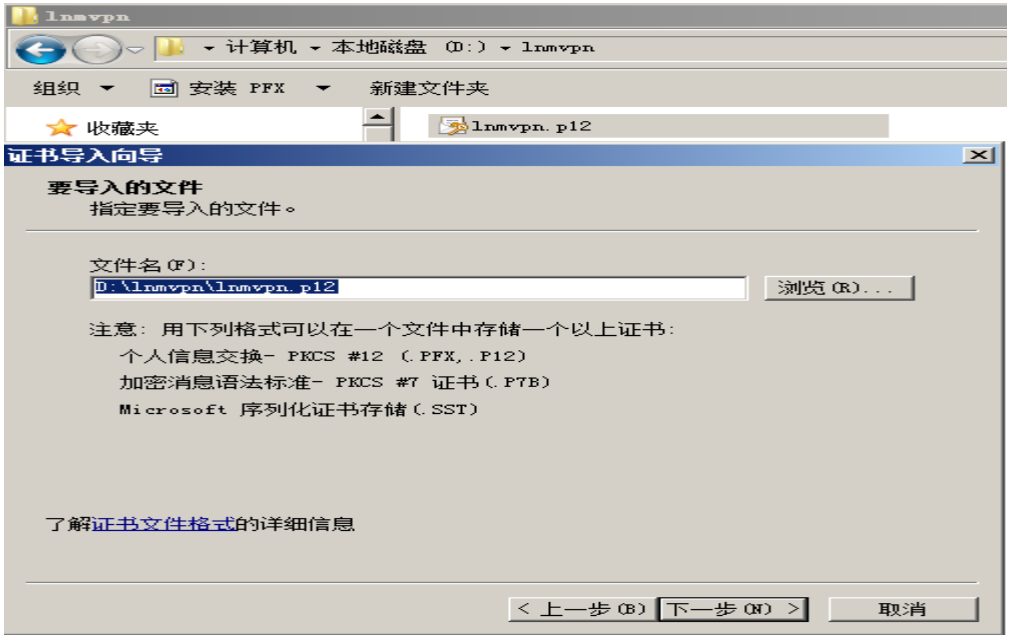
4. 连接成功，我们查 IP 显示异地 IP，就说明连接成功了

Windows Anyconnect 证书连接

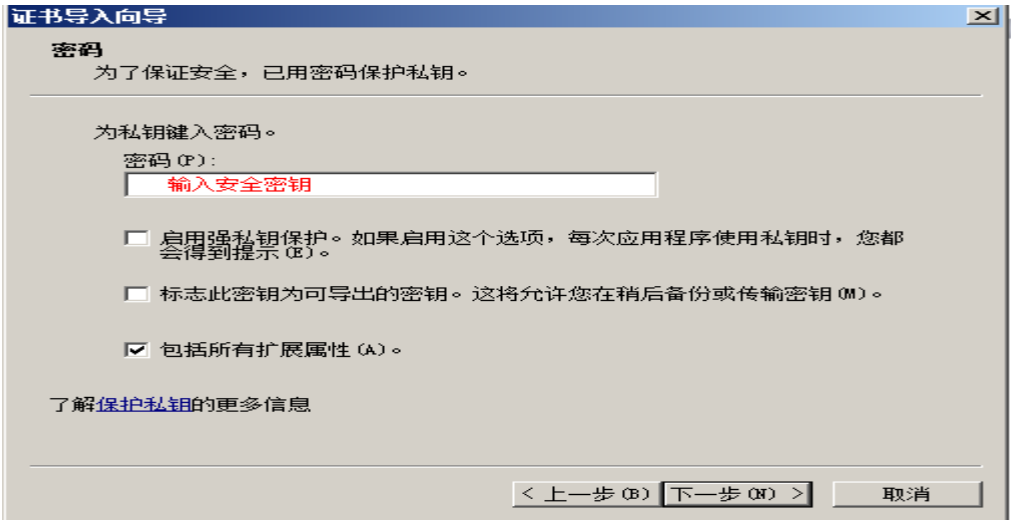
1. 向管理员索取客户端证书



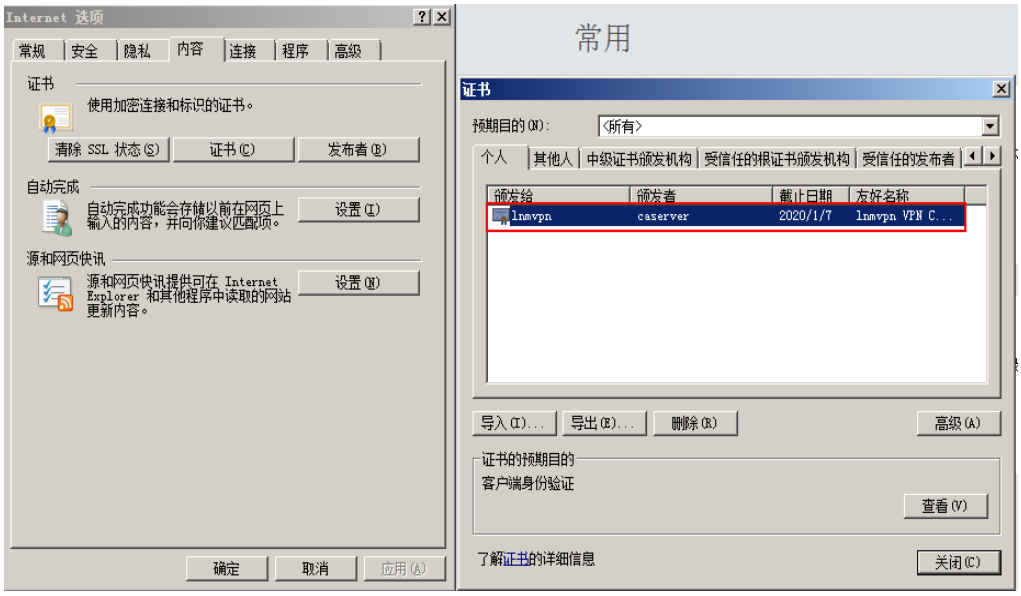
2. 导入 p12 证书



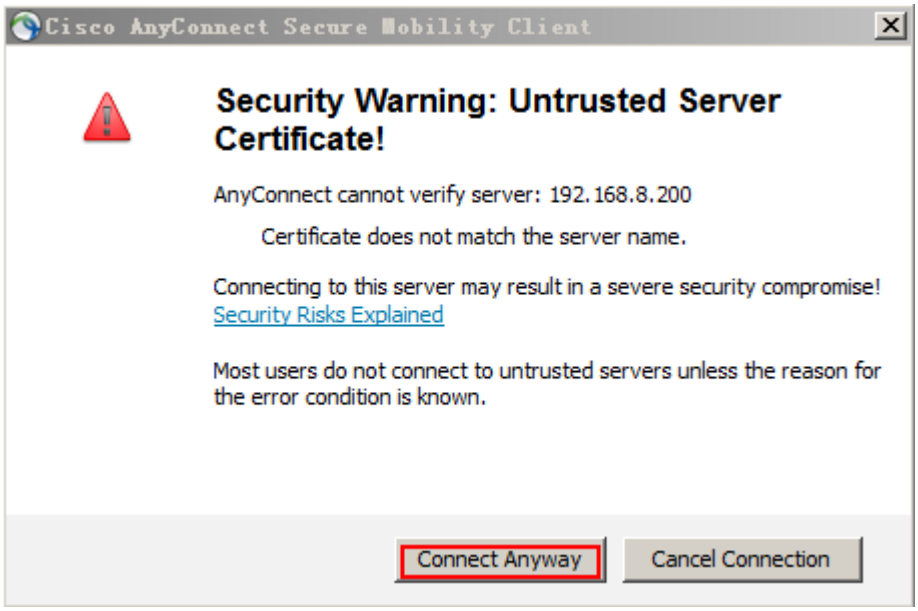
3. 输入 p12 导入安全密钥



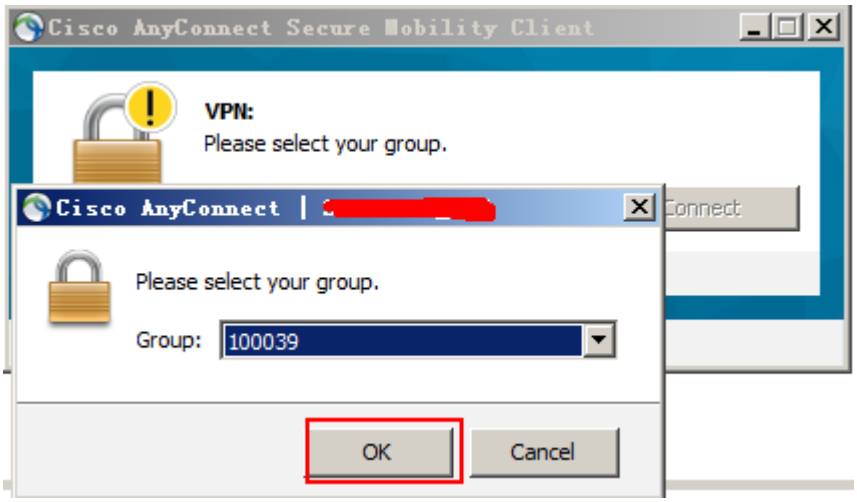
4. 确认导入是否成功（以 IE 为例，打开 Internet 选项--内容--证书）



5. Anyconnect 证书自动识别认证（点击继续连接）

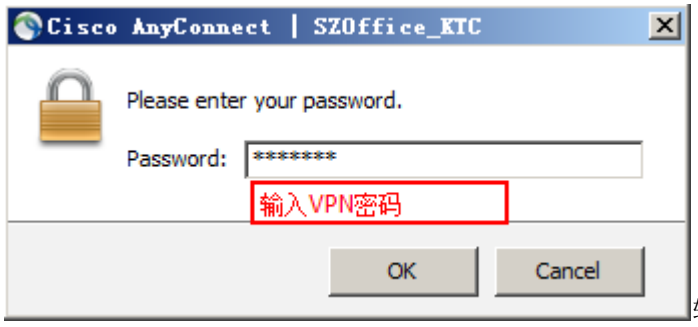


6. 证书策略组别确认



7. 首次需要输入用户名密码验证（证书名称+证书安全密匙）

输入证书名称



输入安全密匙

8. 一直继续，连接成功，下次登录就直接继续，无须再次手动输入密码

Android Anyconnect 密码连接(IOS 类似)

1. 首先下载安装 AnyConnect_4.6.0xxx.apk，然后安装完成。

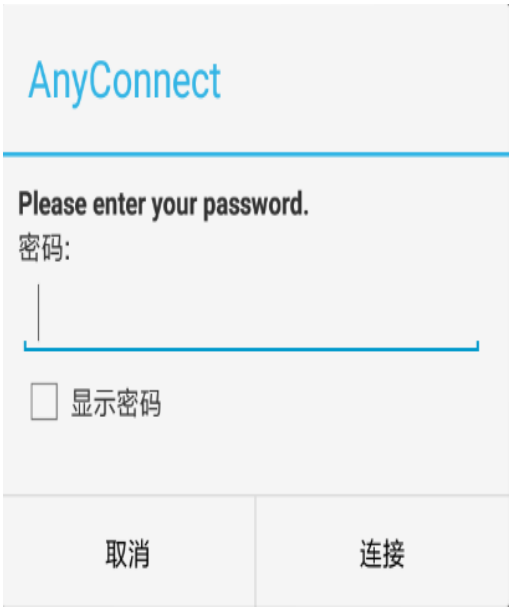
2. 打开 APP 应用

3. 点击连接，并添加新连接配置

3. 填写相应的配置信息（主要是服务器地址）

4. 保存配置点击连接开关

5. 输入连接用户名和密码

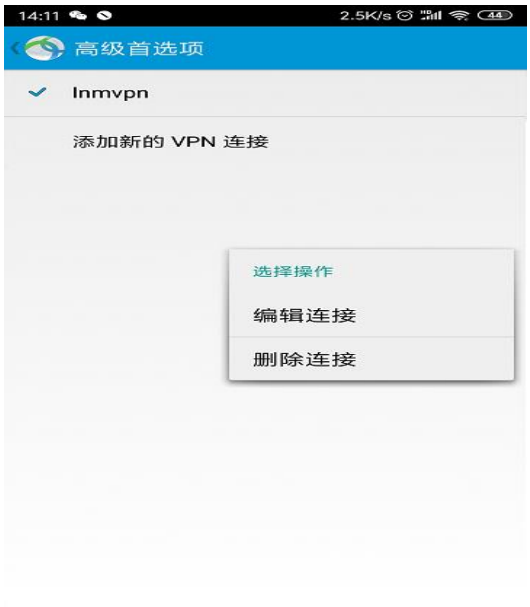


6. 如果界面出现已连接表示连接成功

Android Anyconnect 证书连接(IOS 类似)

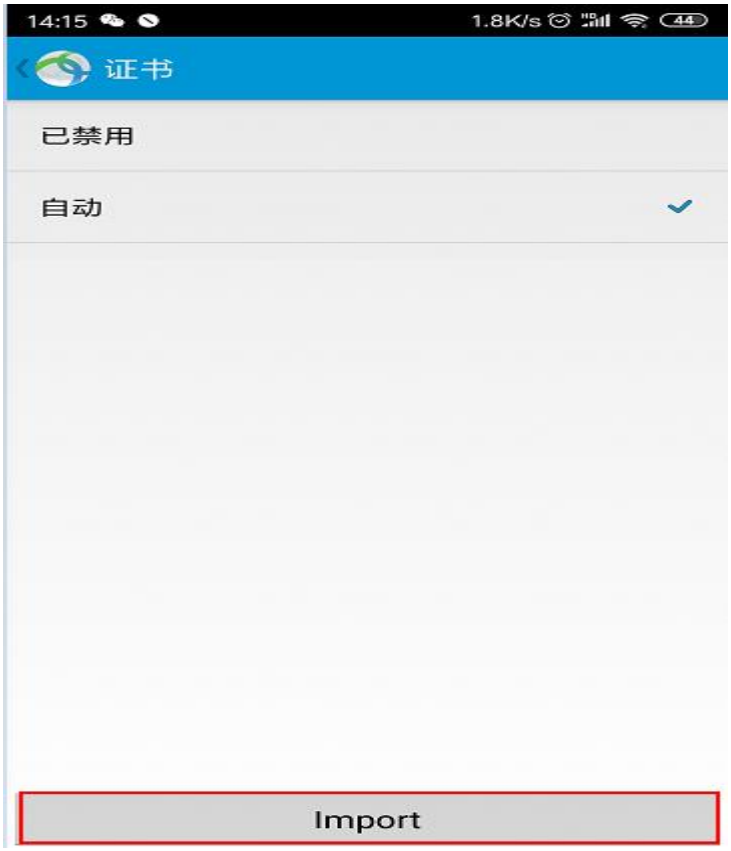
1. 证书配置与密码配置区别于连接配置不一样，我们在添加密码认证的时候是只要配置一个服务器地址即可，但证书认证需要首先导入证书到移动端上

2. 选中配置（选中等待 3 秒），并点击编辑连接



3. 找到配置的高级选项

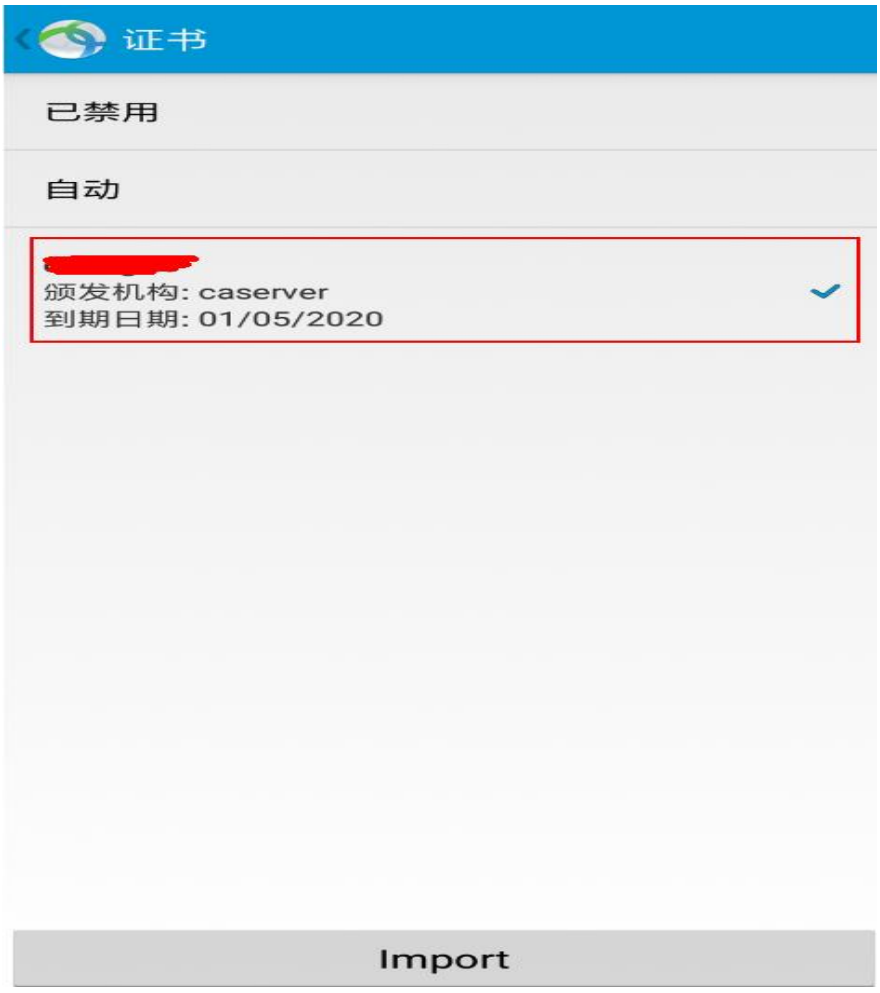
4. 选择证书自动或指定，点击 IMPORT 按钮导入证书


14:15
1.8K/s
证书
已禁用
自动
Import

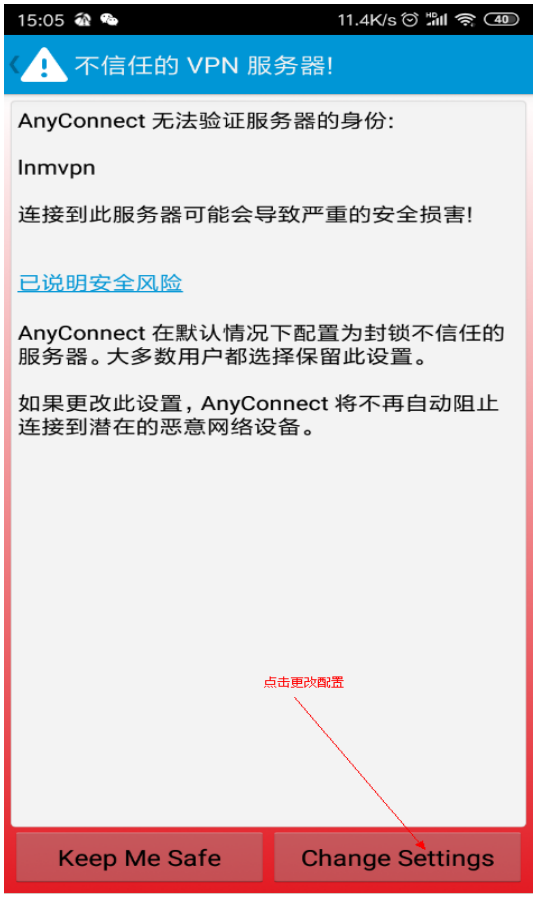

导入证书
文件系统
网络位置(URI)
设备凭据存储

5. 输入证书安全密匙，导入完成。


颁发机构: caserver
AnyConnect
请输入用于进行证书导入的密码。
密码
显示密码
取消
导入


证书
已禁用
自动
[redacted]
颁发机构: caserver
到期日期: 01/05/2020
Import

6. 点击连接，更改安全配置及首次同样需要输入证书名和安全密钥



选择组策略 ID，默认即可


AnyConnect
Please enter your username.
用户名:
取消
连接

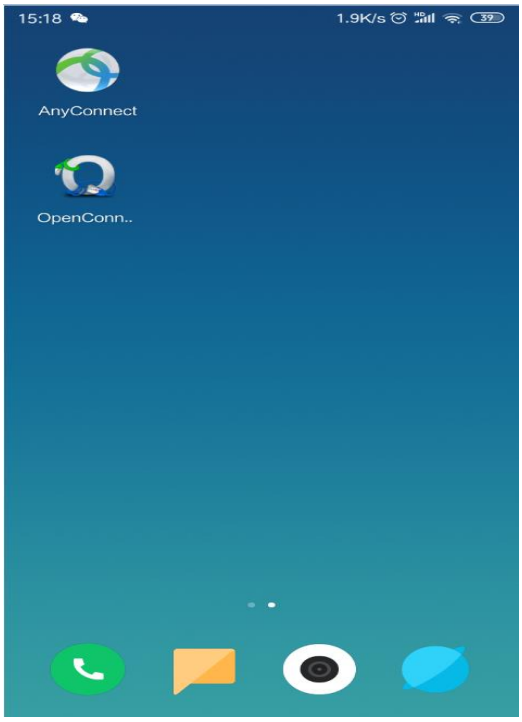

AnyConnect
Please enter your password.
密码:
显示密码
取消
连接

7. 连接成功

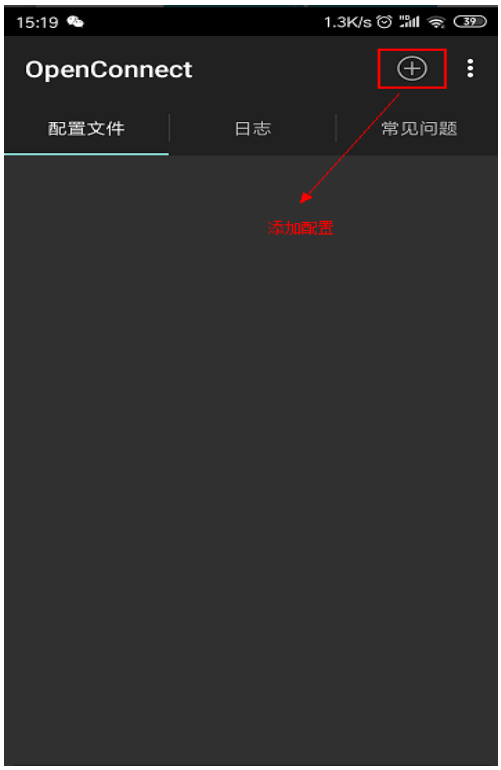

15:06
11.5K/s
AnyConnect
VIRTUAL PRIVATE NETWORK
AnyConnect VPN
已连接
开
连接
lnmvpn
详细信息
cisco

Android Openconnect 密码连接

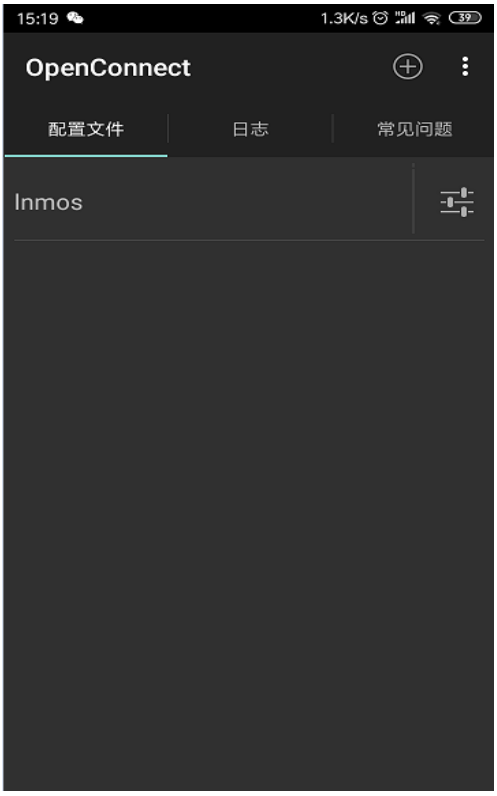
1. 首先下载安装 OpenConnect_xxxxx.apk，然后安装完成。

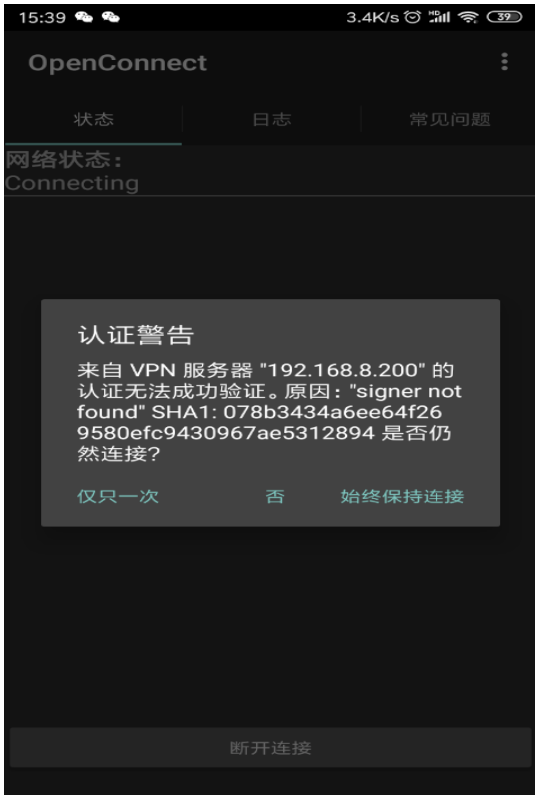


2. 打开应用并添加 VPN 配置，保存

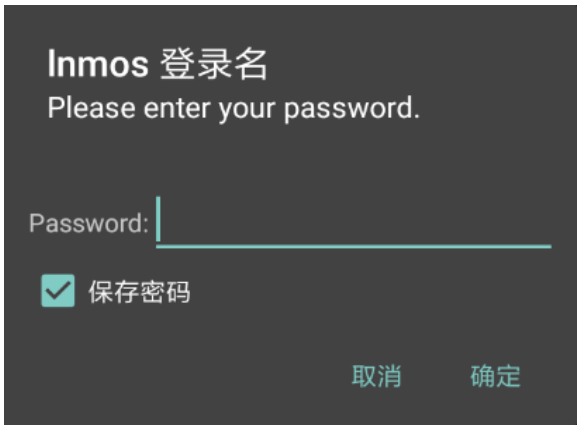


3. 查看保存的服务列表，并选中单击即表示选中连接





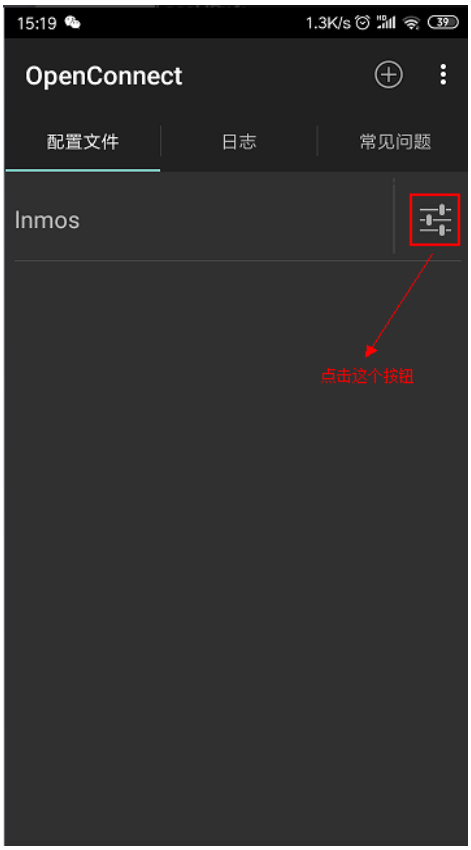
4. 输入连接用户名密码

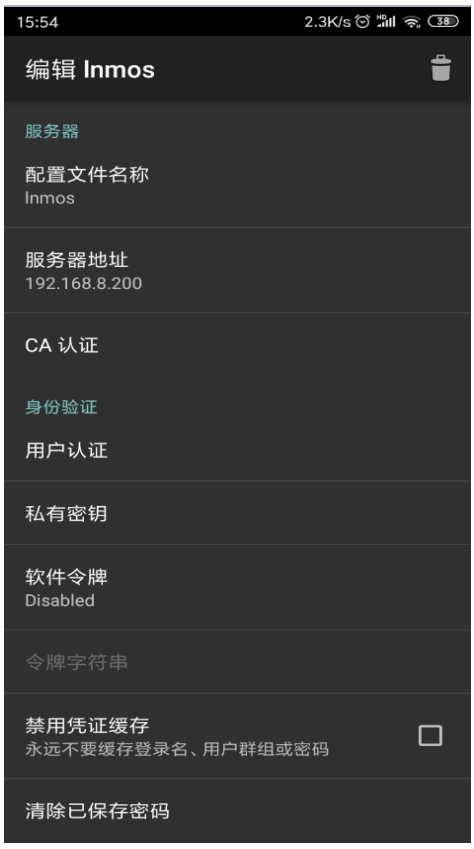


5. 连接成功 （openconnect 可记住密码）

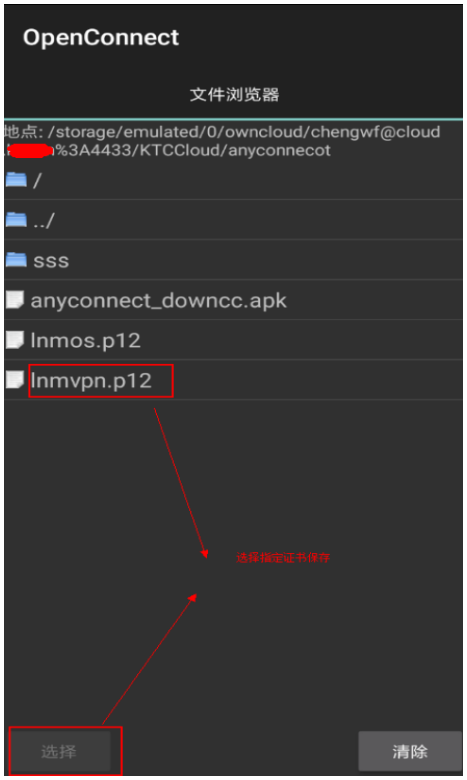
Android Openconnect 证书连接

1. 在已保存的服务列表，并点击编辑设置按钮

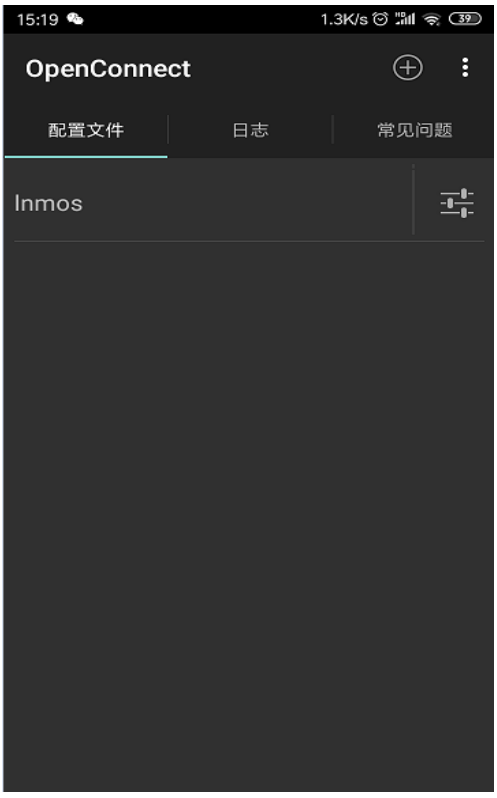


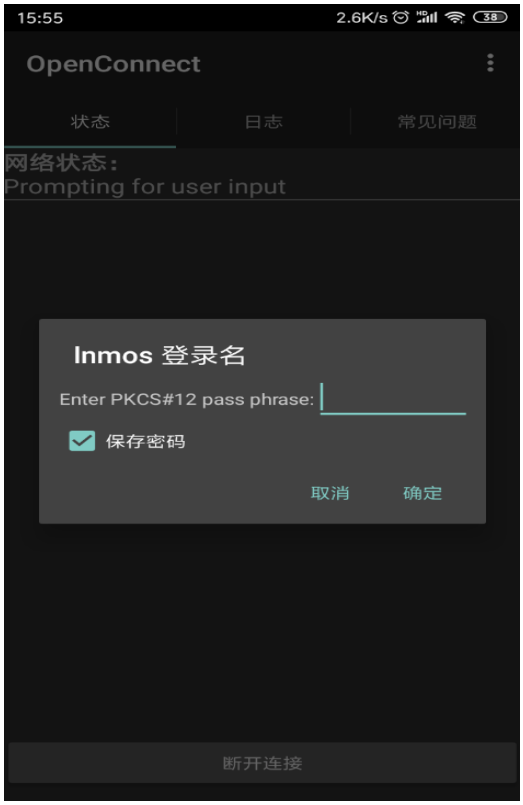


2. 导入证书文件，保存新服务列表

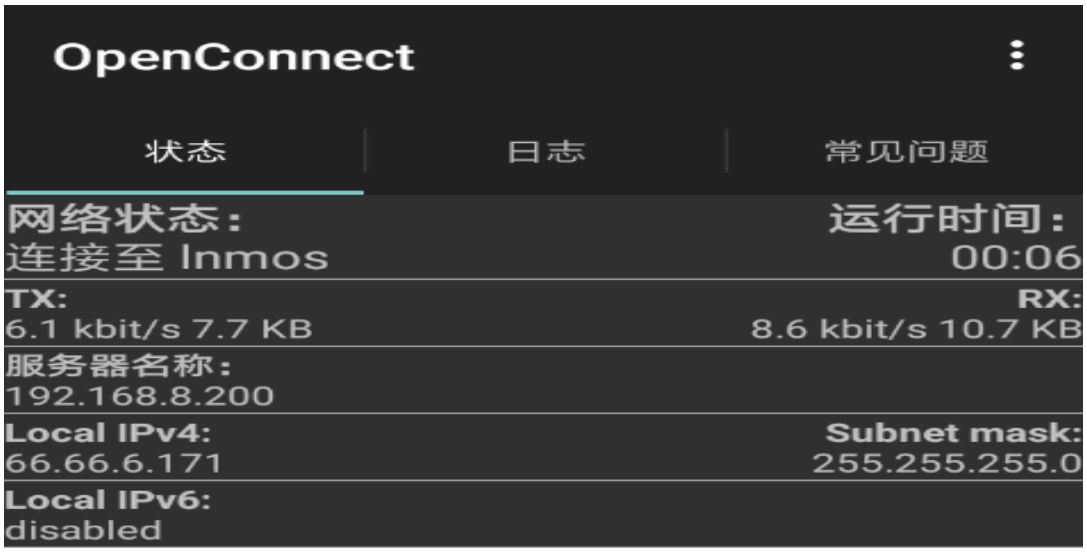


3. 选择连接服务列表，输入安全密匙





4. 选择证书策略组，默认即可，直到连接成功



资源下载

Anyconnect、OpenConnect 客户端：（链接分享密码:vzfn）

百度网盘：https://pan.baidu.com/s/1xDAfspJdBEm9ilipT61PbQ

备注：按指定系统分类进行下载

FTP 客户端下载：

Filezilla: https://www.filezilla.cn/download

想要获取更多好的资源，请联系 master@lnmos.com

常见问题

anyconnect 证书验证出现 sec-mod: user '' requested group

分析： 应该属于软件 ocserv 与 anyconnect 兼容性问题，测试 openconnect 1.5.3 客户端不会

```
Message from syslogd@centosexp at Jan  4 18:24:40 ...
 ocserv[27485]: sec-mod: user '' requested group '100036' but is not included on his certificate groups
```

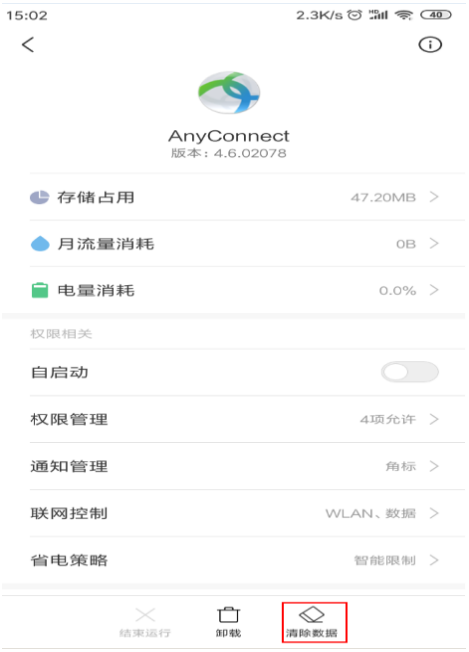
主要是无法正确识别用户默认 group 组

解决： 清理掉用户配置文件”C:\Users\%USERNAME%\AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml”，重新拨入

```
[root@developer lnmVPN]# occtl show users
     id     user     vhost              ip          vpn-ip device   since    dtls-cipher    status
  28426      aaa   default   192.168.0.87    66.66.6.141  vpns0     8s (AES-128-CBC)-(SHA1) connected
```

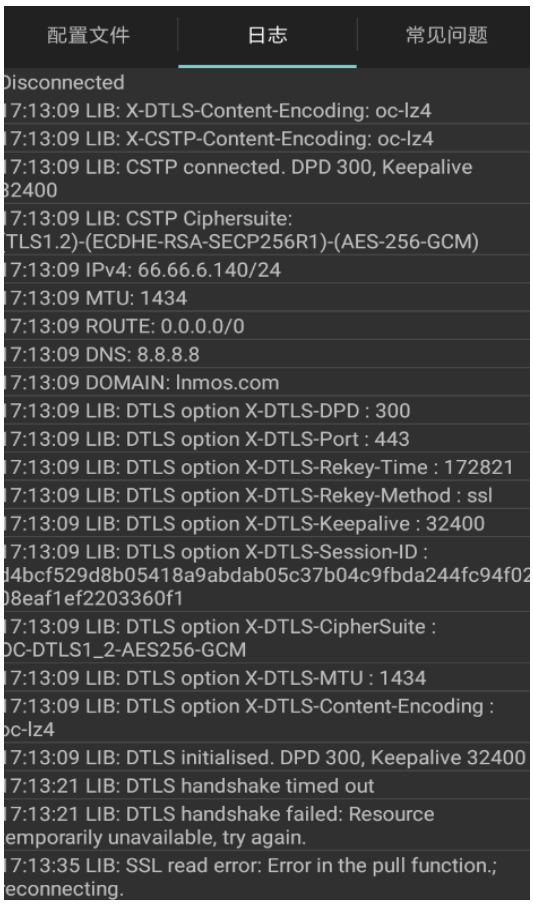
调试:　可以打开 ocserv 服务器地址尝试选择证书后贴出内容供分析

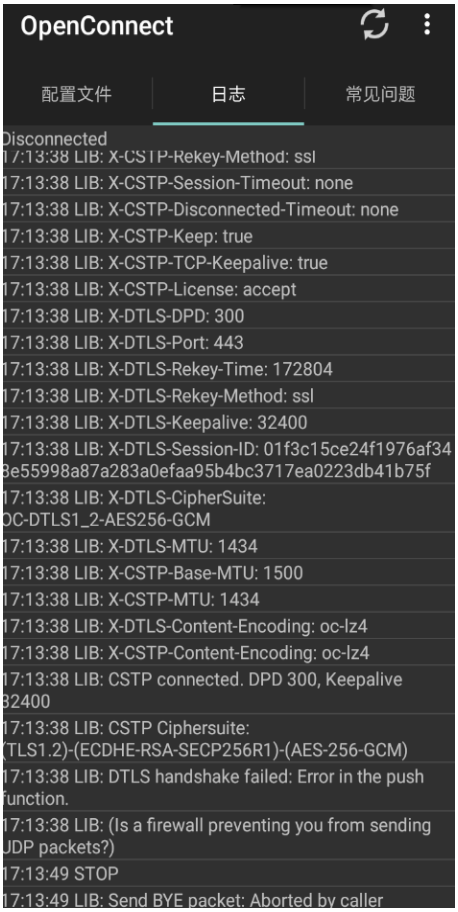
经测试手机端也存在类似问题：原有验证过其他证书且旧的应用策略和现在证书的应用策略不一致时就会有该问题，手机端需要应用配置或卸载重装



openconnect 连接出现 DTLS handshake failed

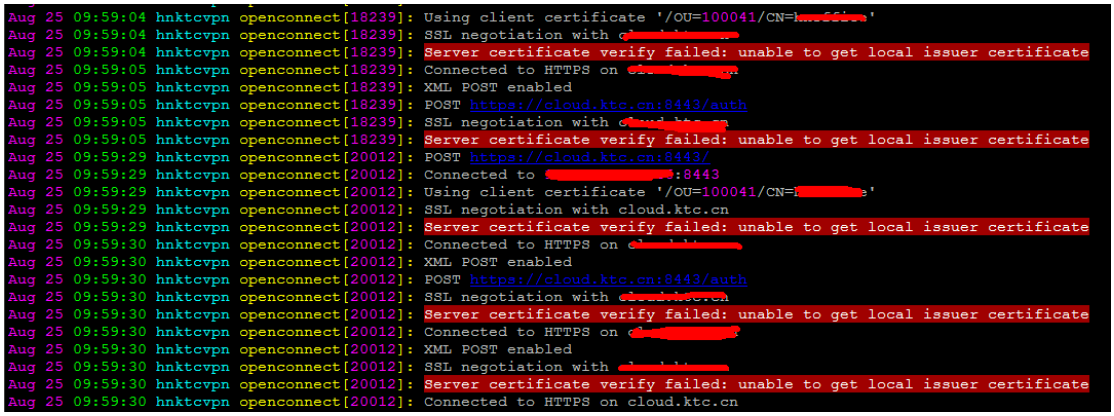
分析：　DTLS 在建立连接阶段失败





解决： 主要是因为 DTLS 验证的端口和连接端口不一致造成，如果前段有防火墙映射的时候，应尽量保持映射端口一致即可避免该问题

客户端连接服务端出现”Server certificate verify failed: unable to get local issuer certificate”



分析：出现这个问题主要是因为客户端 SSL 体系对服务端 SSL 证书无法正确识别信任，在有些主机可能可以忽略正常验证通过，但是大部分都存在一些问题。

解决方案：

证书管理---CA

打包下载服务端的 CA 证书并把 ca.crt 文件上传到客户端

执行下列指令：导入信任证书

```
cat ca.crt >> /etc/pki/tls/certs/ca-bundle.crt
```