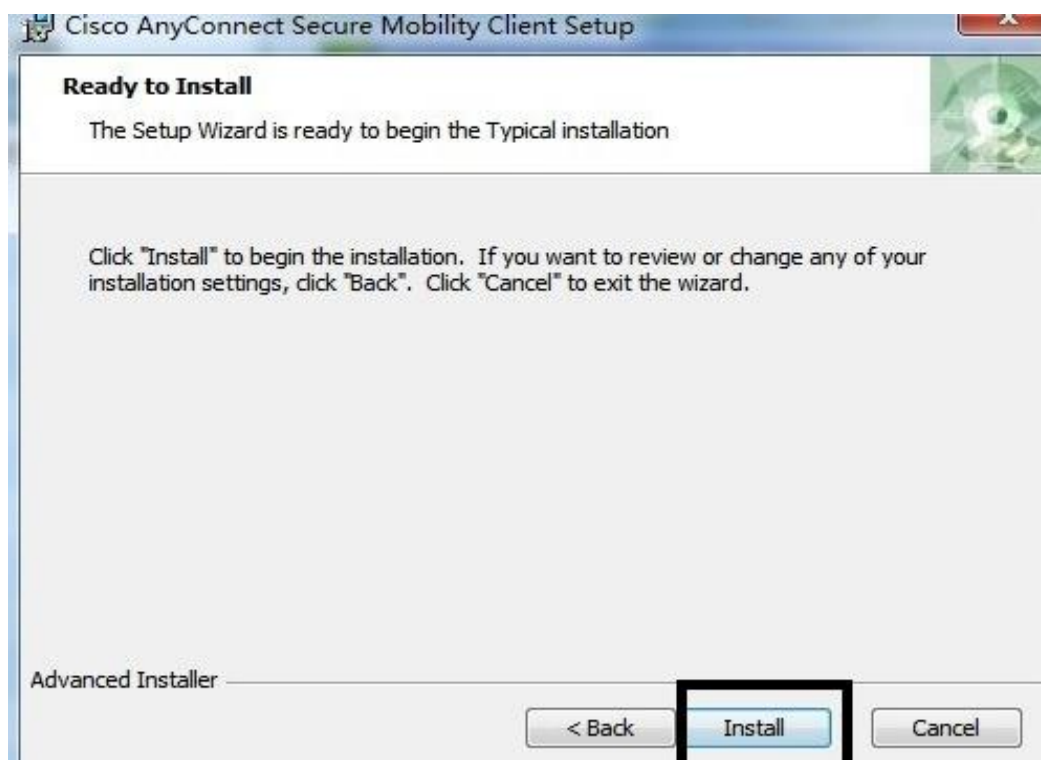


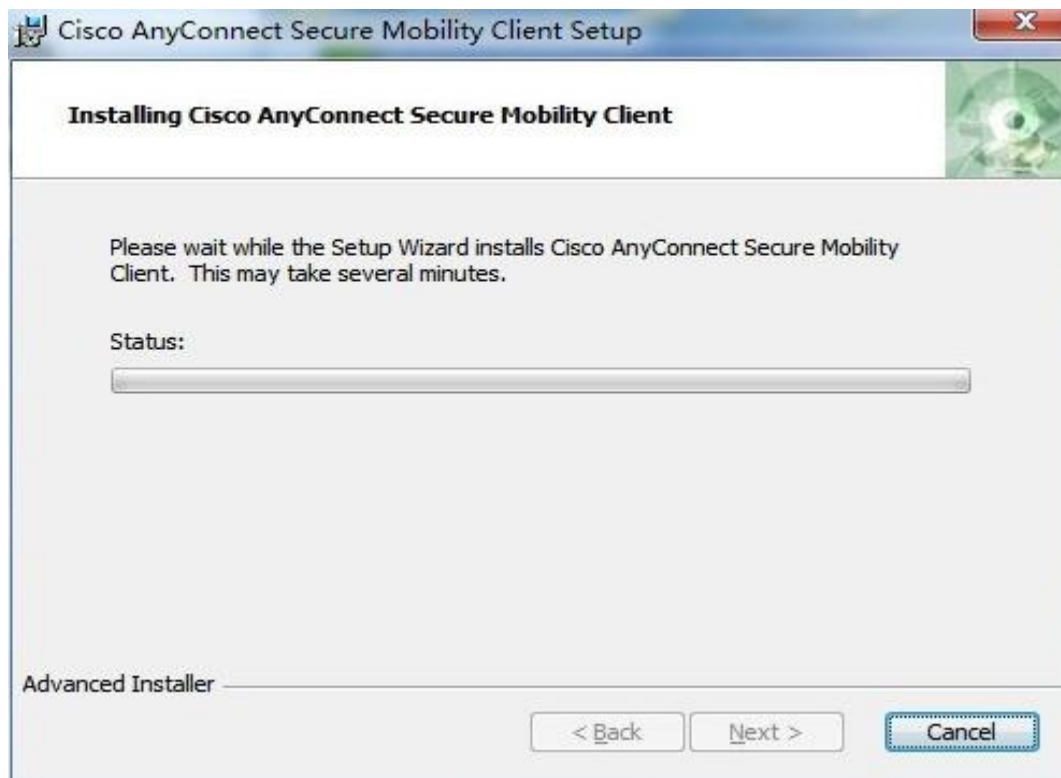
客户端安装

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：



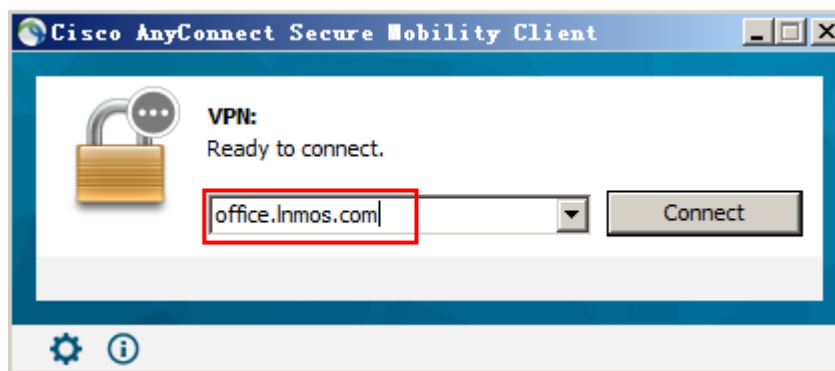




注意：安装后不会在桌面创建图标，请在开始菜单-所有程序，找到程序 Cisco AnyConnect Secure Mobility client，点击打开。



2. 打开 CISC0 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。



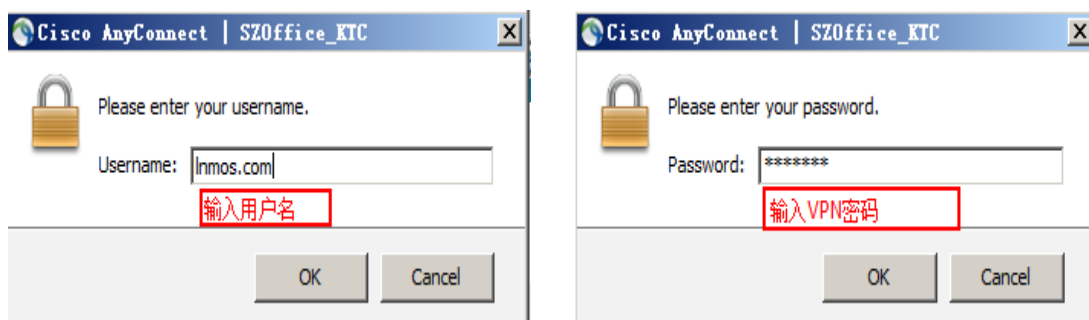
如果之前没用过我们的 VPN 会出现下面的界面(即没有导入我们的 CA 证书)，点击 Change settings 请修改设置为允许连接不信任的服务器地址，如下图所示：



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



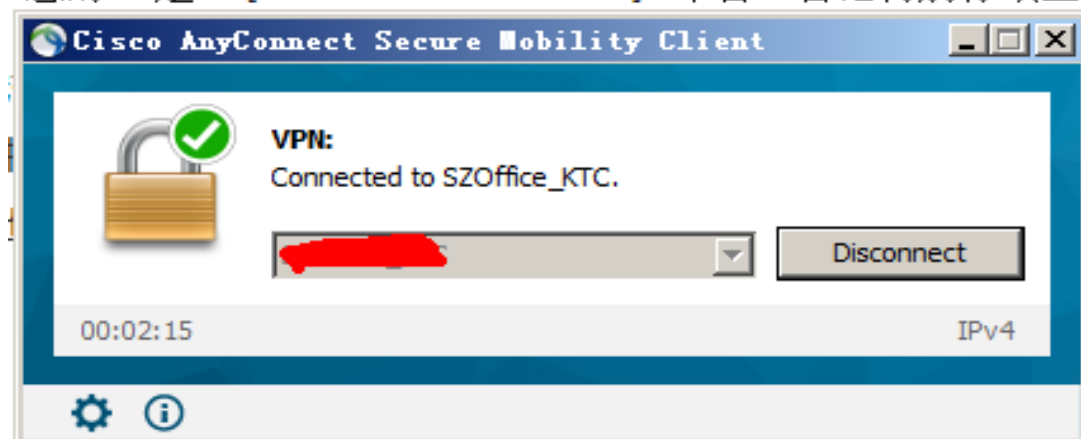
3. 再点击 Connect 来连接，有时会弹出对话框，点继续就可以了，输入



4. 连接成功，我们查 IP 显示异地 IP，就说明连接成功了

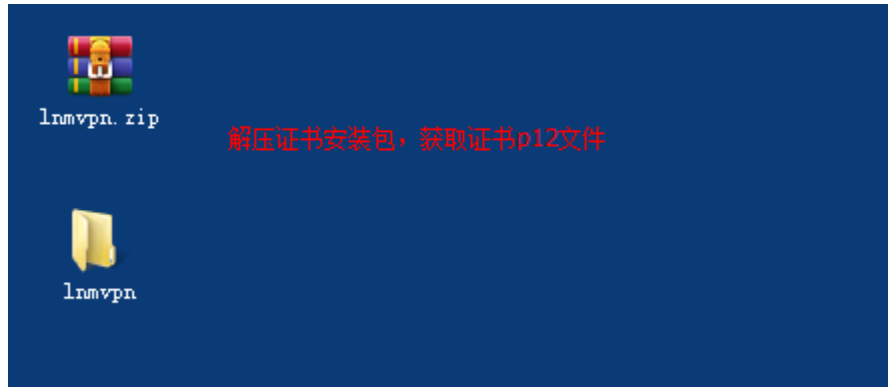
www.ip138.com IP查询(搜索IP地址的地理位置)

您的IP是: [REDACTED] 来自: 香港特别行政区

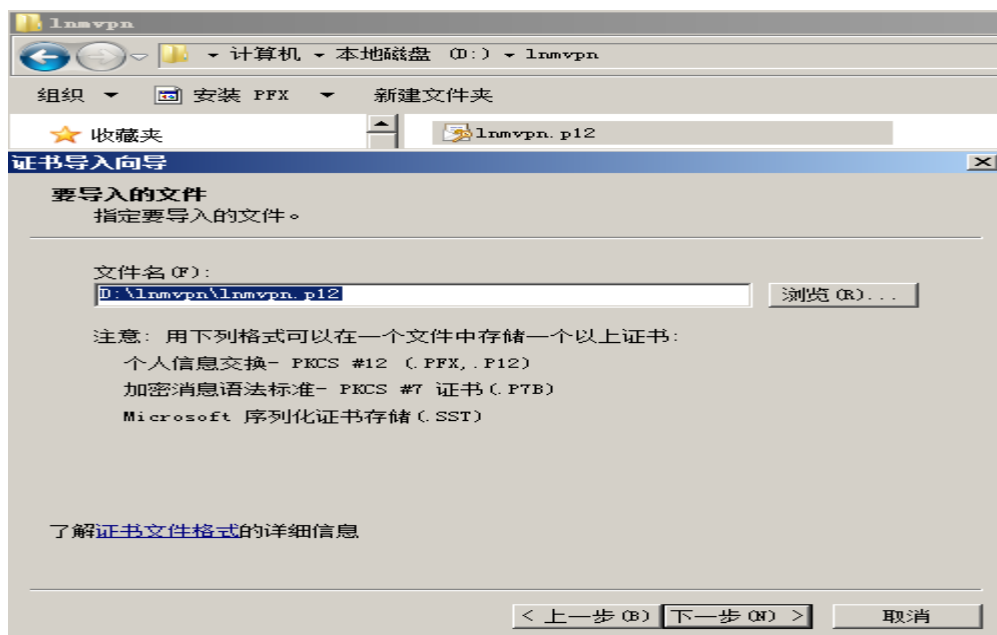


Windows Anyconnect 证书连接

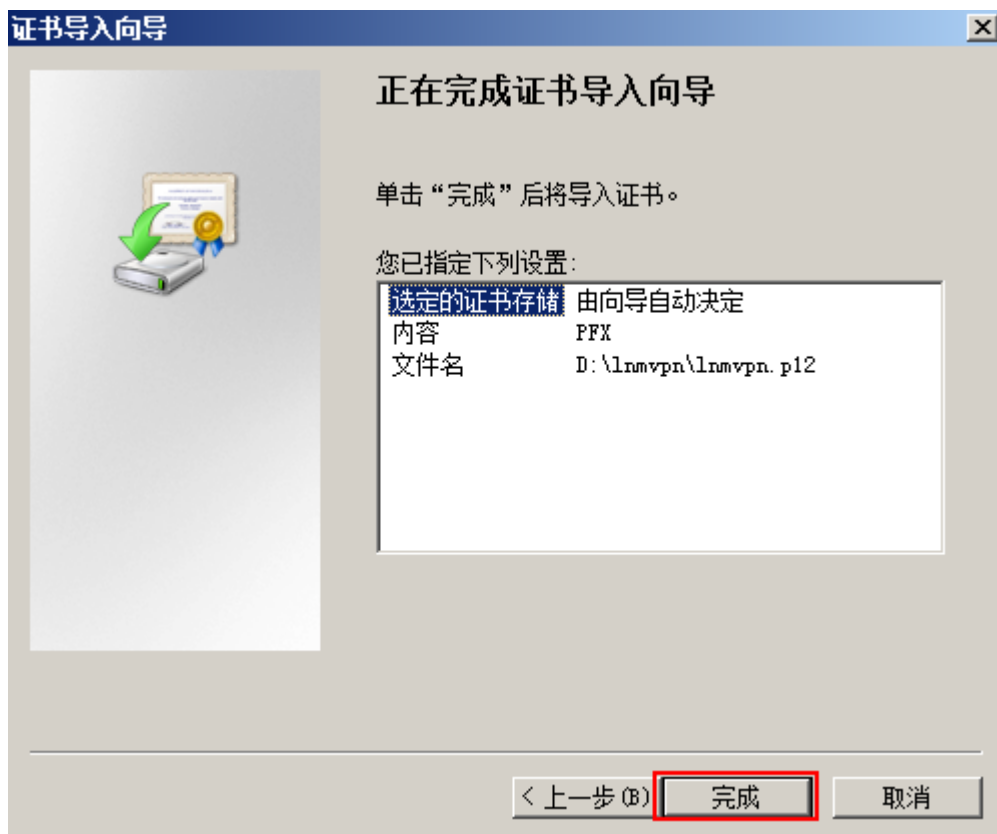
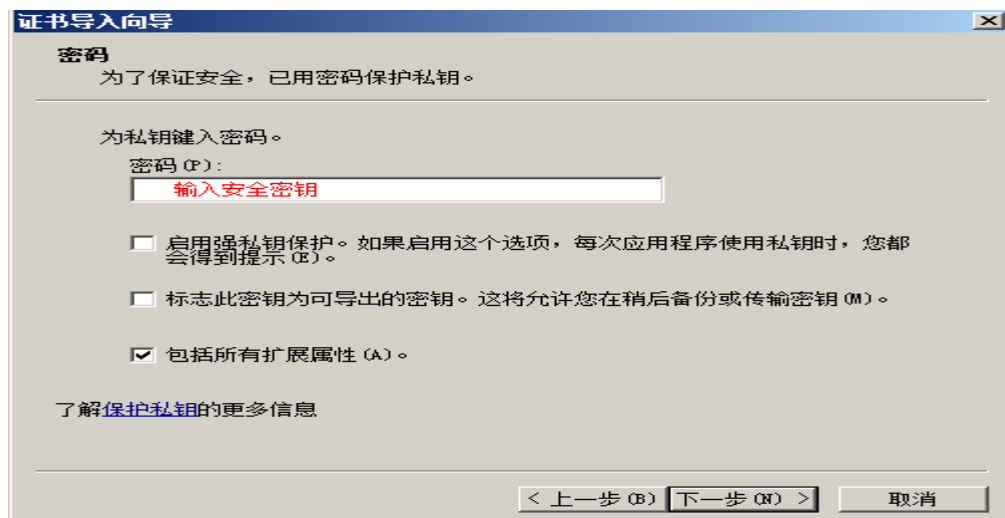
1. 向管理员索取客户端证书



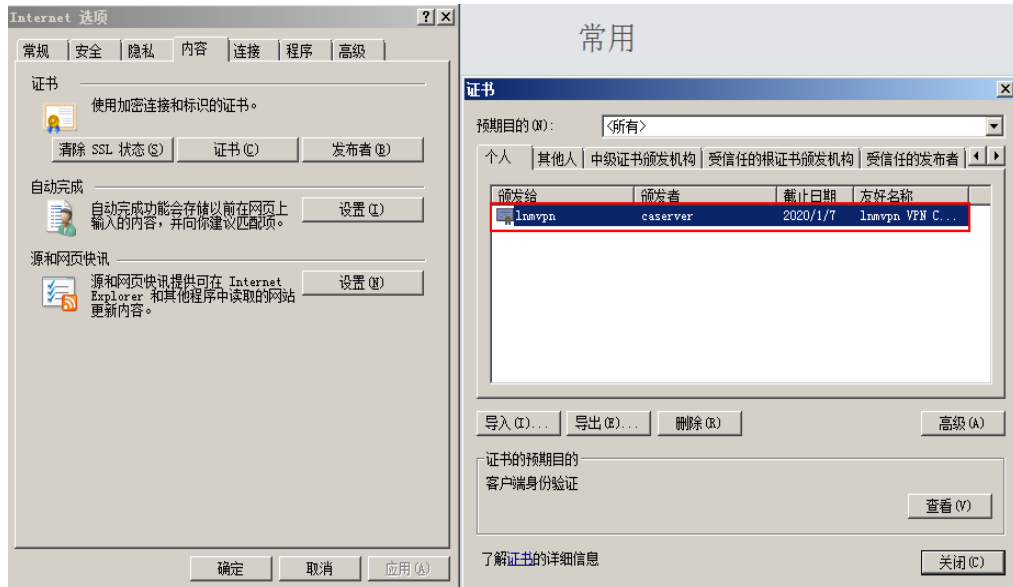
2. 导入 p12 证书



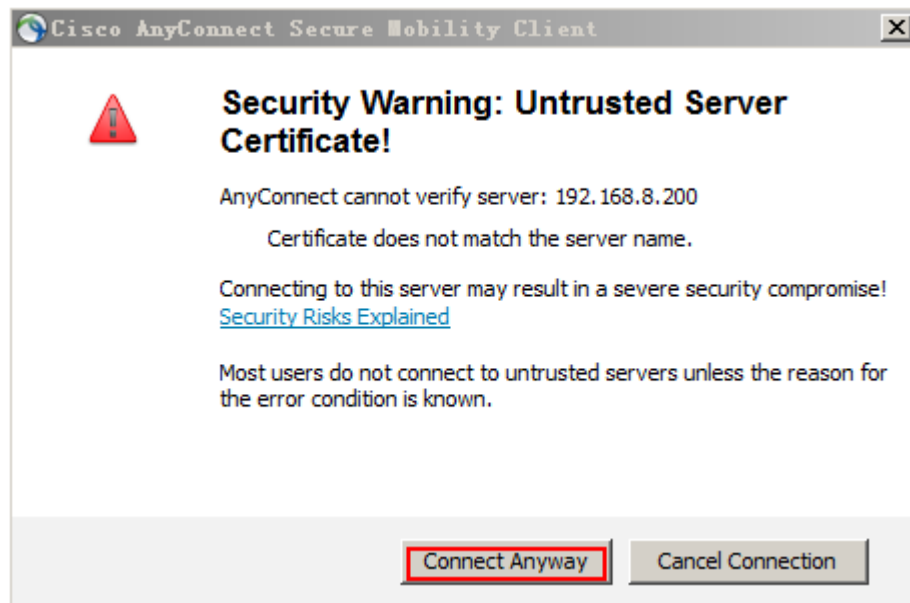
3. 输入 p12 导入安全密钥



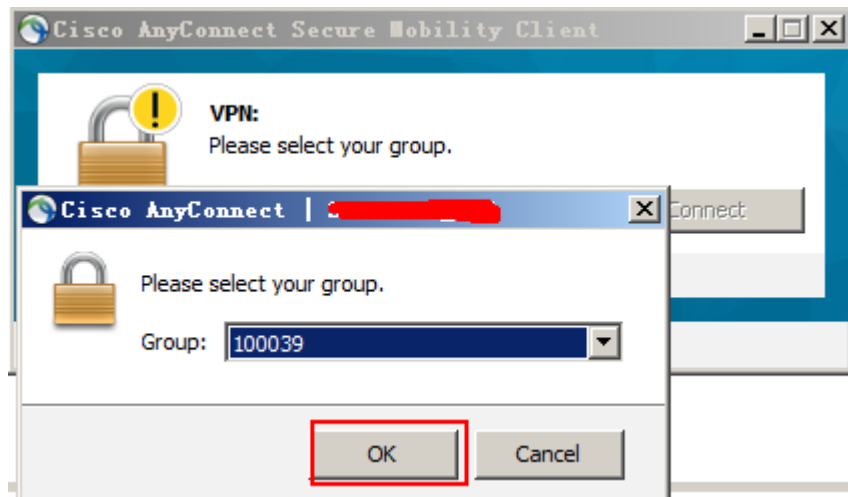
4. 确认导入是否成功（以 IE 为例，打开 Internet 选项--内容--证书）



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

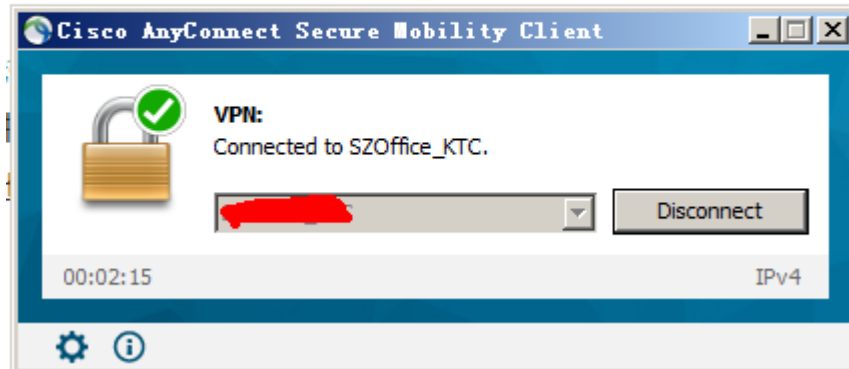


输入安全密匙

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

www.ip138.com IP查询(搜索IP地址的地理位置)

您的IP是: [REDACTED] 来自: 香港特别行政区



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。



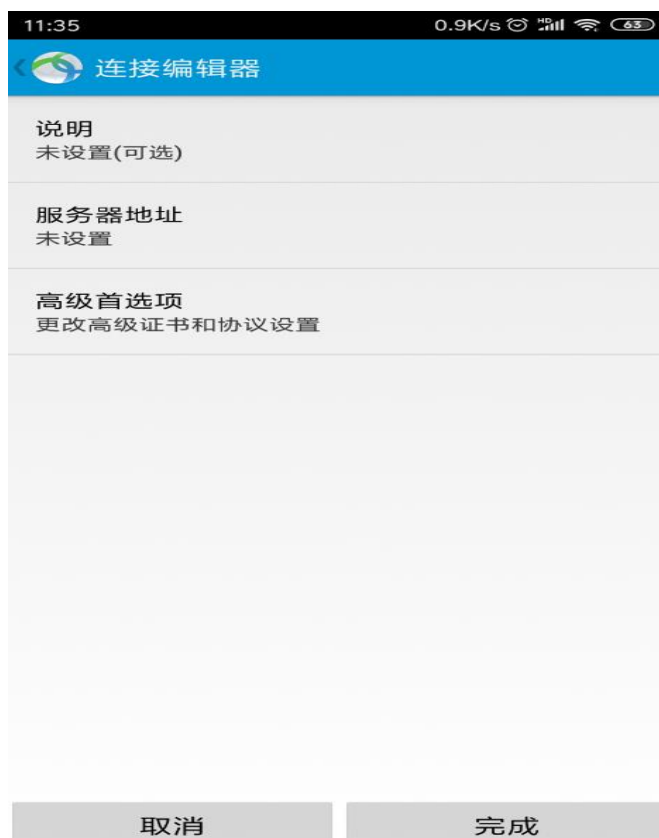
2. 打开 APP 应用

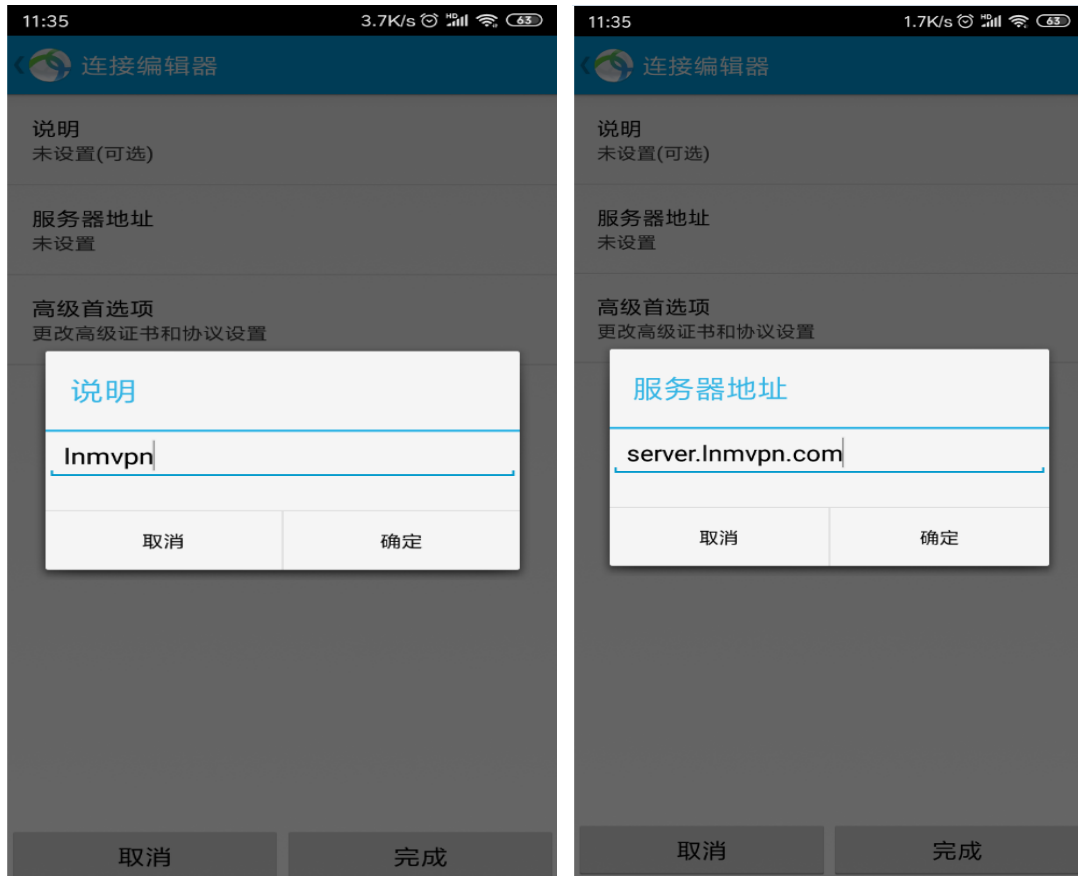


3. 点击连接，并添加新连接配置

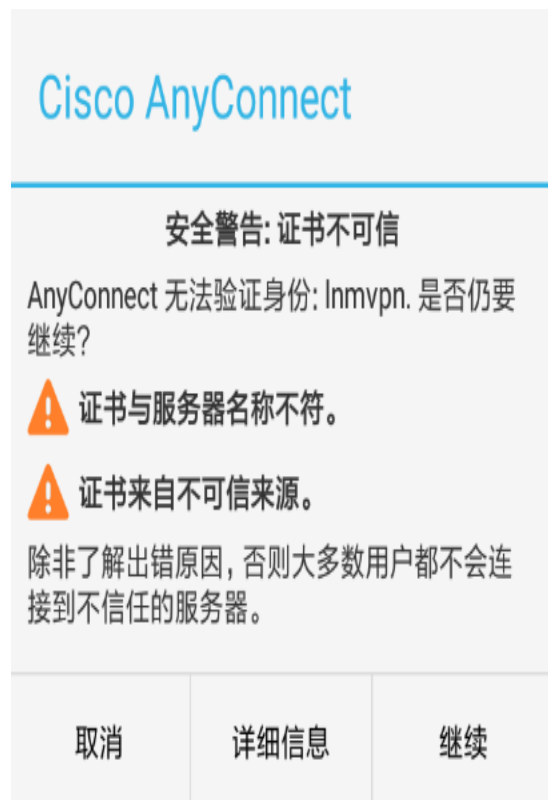


3. 填写相应的配置信息（主要是服务器地址）





4. 保存配置点击连接开关



5. 输入连接用户名和密码

AnyConnect	
Please enter your username. 用户名: <input type="text"/>	
取消	连接

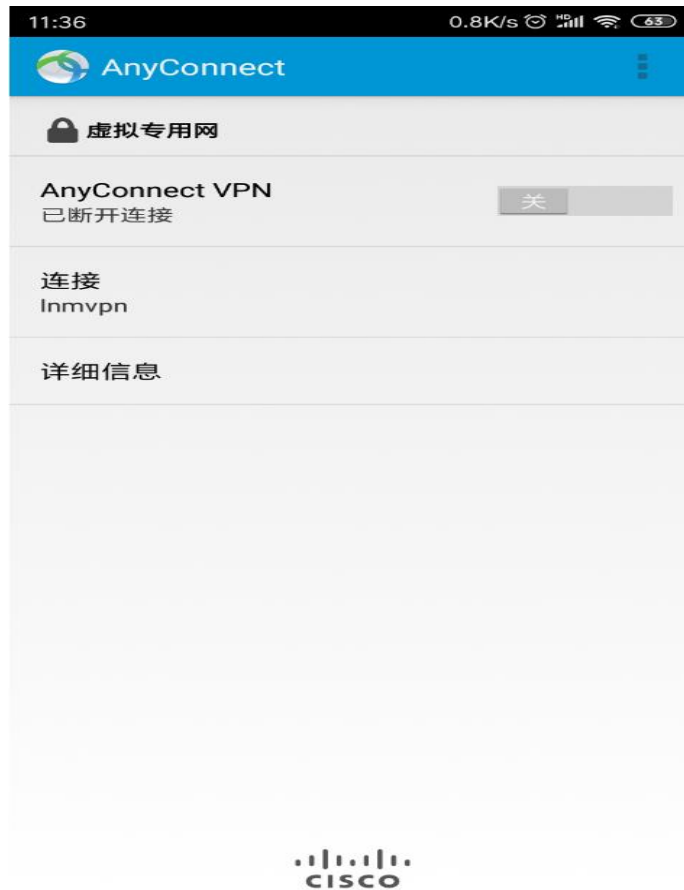
AnyConnect	
Please enter your password. 密码: <input type="password"/>	
<input type="checkbox"/> 显示密码	
取消	连接

6. 如果界面出现已连接表示连接成功

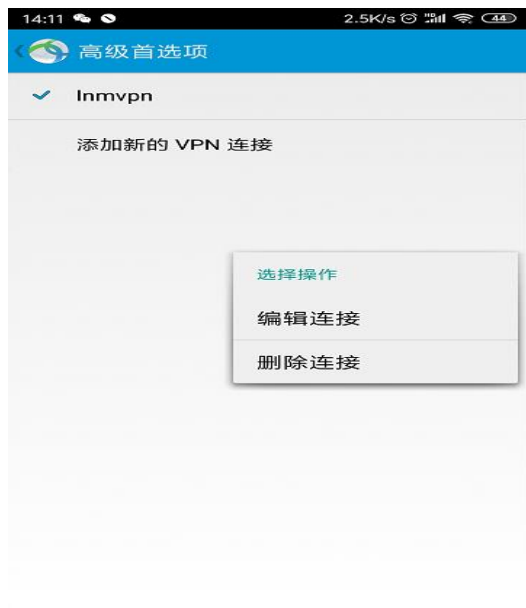


Android Anyconnect 证书连接(IOS 类似)

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



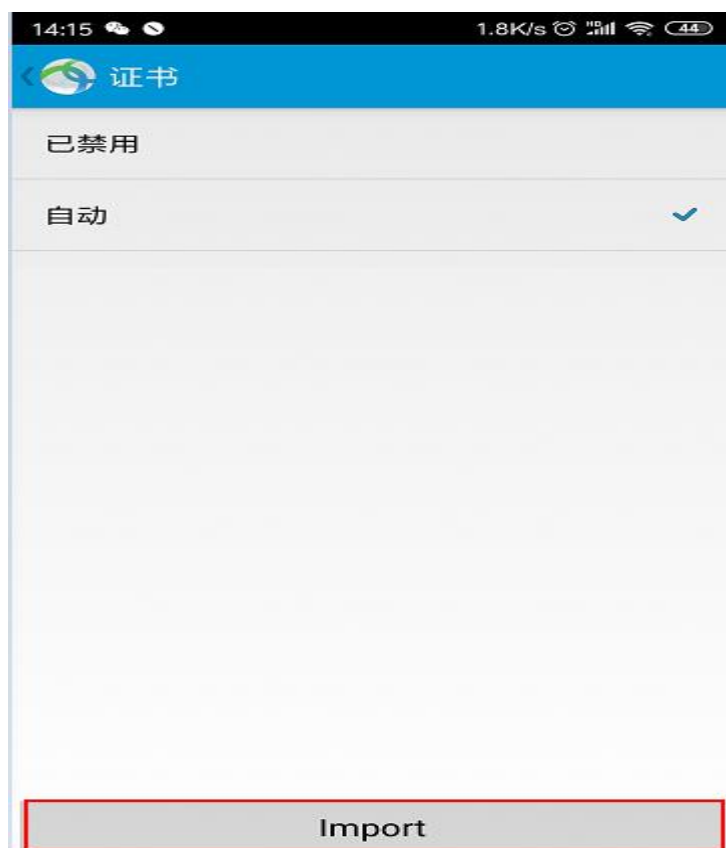
2. 选中配置（选中等待 3 秒），并点击编辑连接



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





5. 输入证书安全密匙，导入完成。

颁发机构: caserver

到期日期: 01/05/2020

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

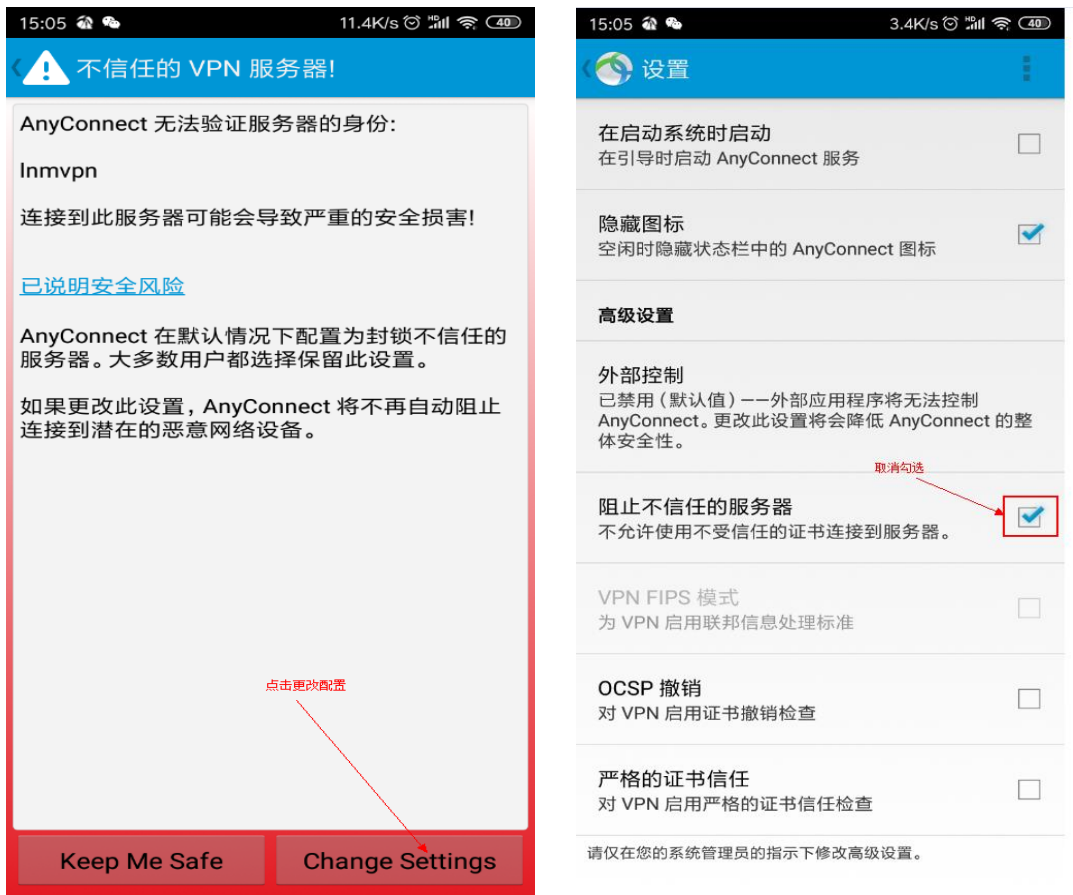
自动

颁发机构: caserver
到期日期: 01/05/2020

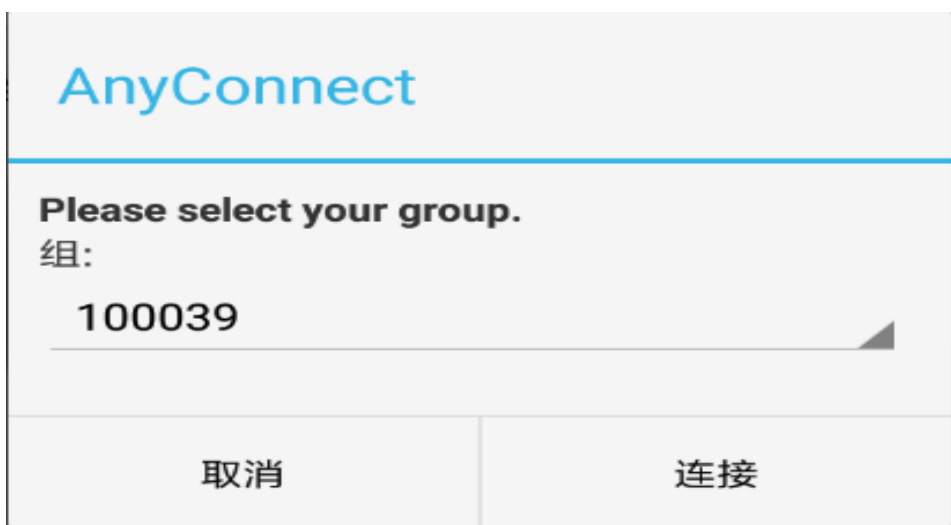


Import

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

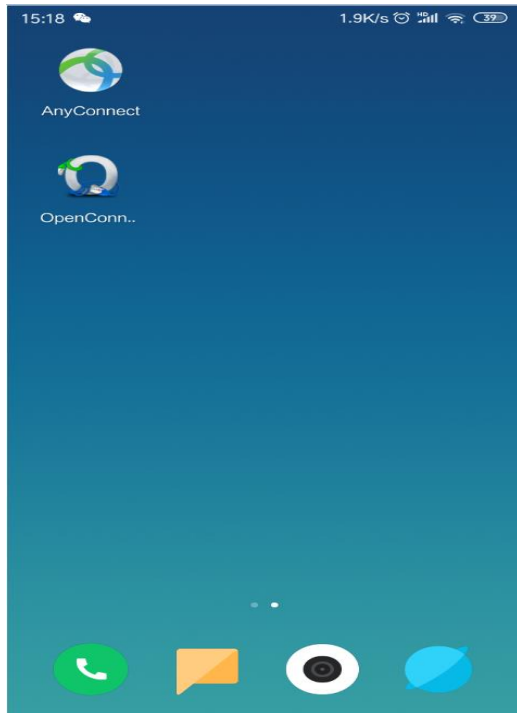
连接

7. 连接成功

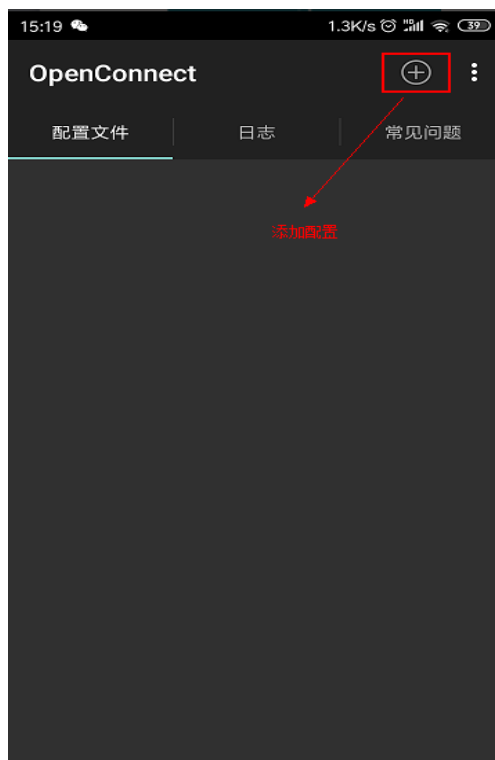


Android Openconnect 密码连接

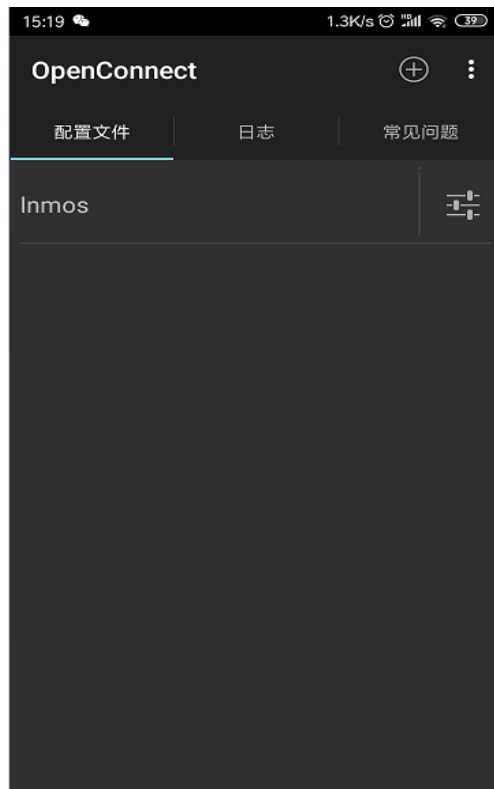
1. 首先下载安装 OpenConnect_xxxxx.apk，然后安装完成。



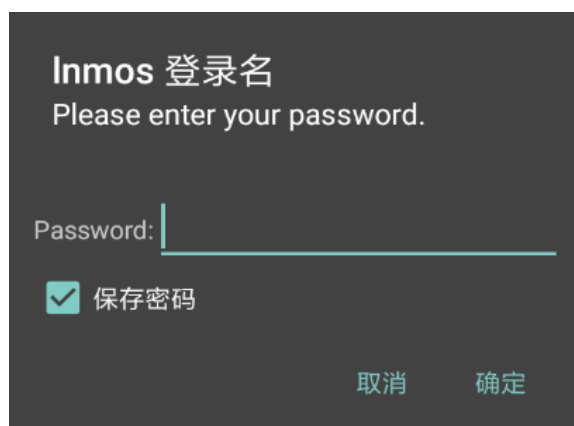
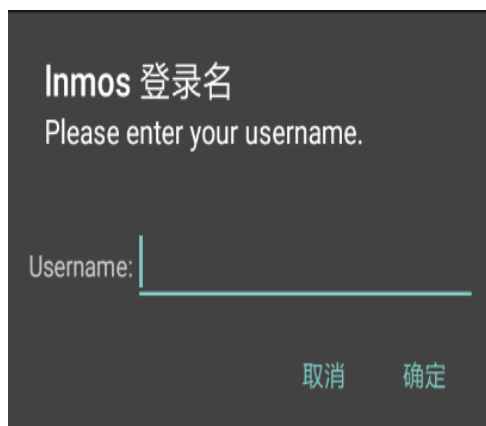
2. 打开应用并添加 VPN 配置，保存



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

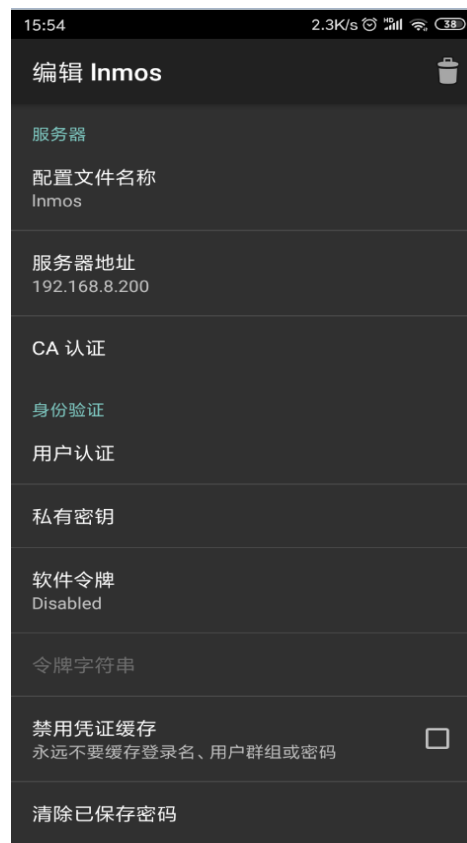
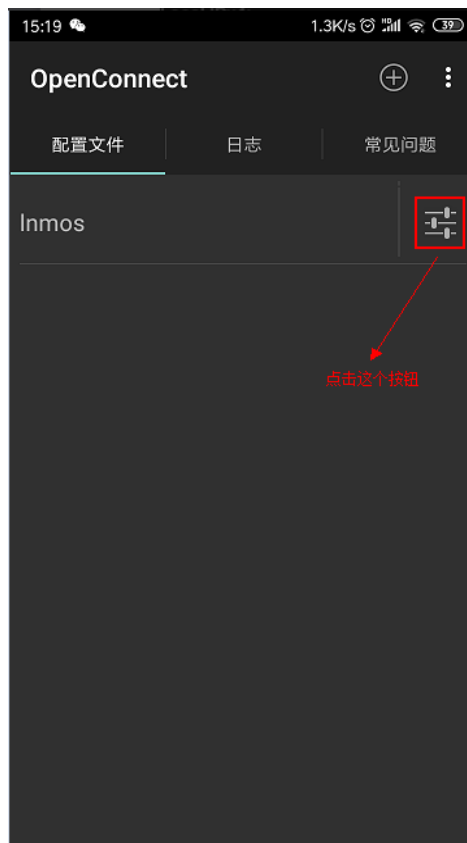


5. 连接成功（openconnect 可记住密码）

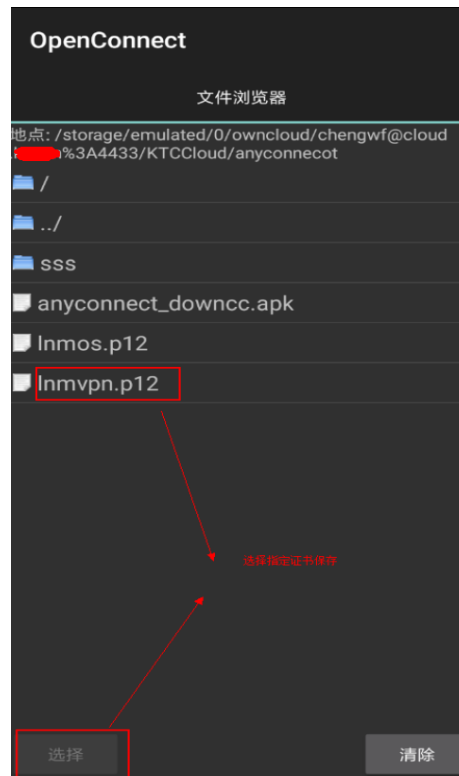


Android Openconnect 证书连接

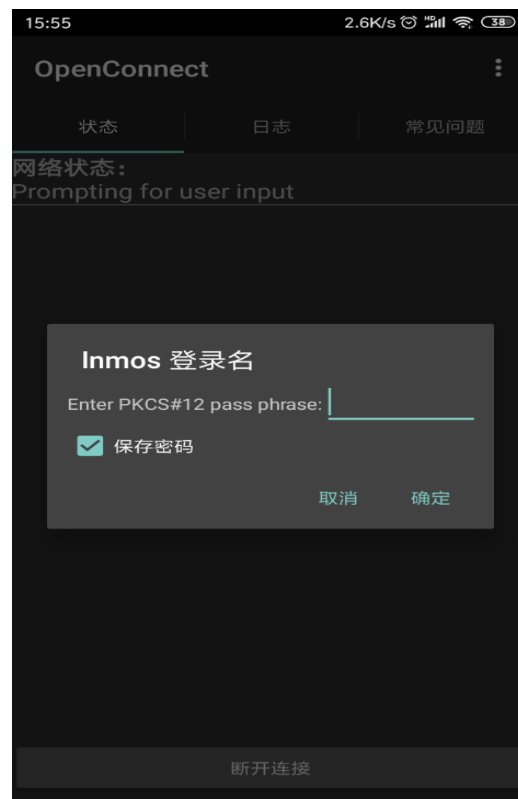
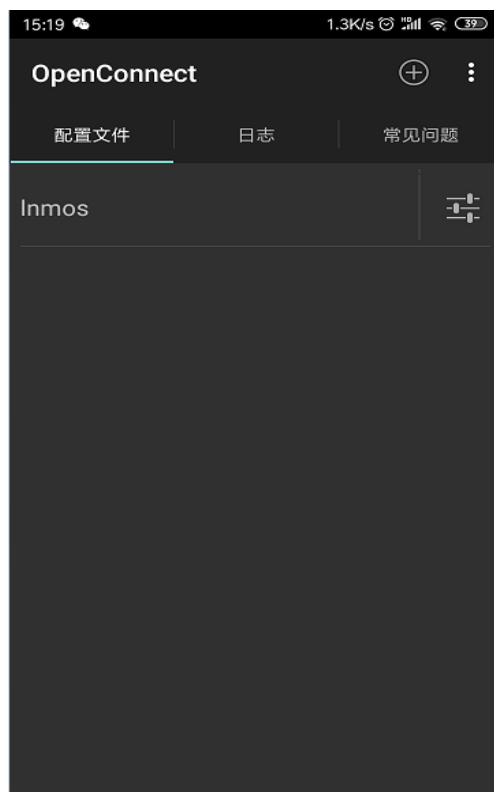
1. 在已保存的服务列表，并点击编辑设置按钮



2. 导入证书文件，保存新服务列表



3. 选择连接服务列表，输入安全密钥



4. 选择证书策略组，默认即可，直到连接成功

OpenConnect

状态

日志

常见问题

网络状态：

运行时间：

连接至 Inmos

00:06

TX:

RX:

6.1 kbit/s 7.7 KB

8.6 kbit/s 10.7 KB

服务器名称：

192.168.8.200

Local IPv4:

Subnet mask:

66.66.6.171

255.255.255.0

Local IPv6:

disabled

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

```
配置文件 日志 常见问题
Disconnected
17:13:09 LIB: X-DTLS-Content-Encoding: oc-lz4
17:13:09 LIB: X-CSTP-Content-Encoding: oc-lz4
17:13:09 LIB: CSTP connected. DPD 300, Keepalive 32400
17:13:09 LIB: CSTP Ciphersuite:
TLS1.2)-(ECDHE-RSA-SECP256R1)-(AES-256-GCM)
17:13:09 IPv4: 66.66.6.140/24
17:13:09 MTU: 1434
17:13:09 ROUTE: 0.0.0.0/0
17:13:09 DNS: 8.8.8.8
17:13:09 DOMAIN: Inmos.com
17:13:09 LIB: DTLS option X-DTLS-DPD : 300
17:13:09 LIB: DTLS option X-DTLS-Port : 443
17:13:09 LIB: DTLS option X-DTLS-Rekey-Time : 172821
17:13:09 LIB: DTLS option X-DTLS-Rekey-Method : ssl
17:13:09 LIB: DTLS option X-DTLS-Keepalive : 32400
17:13:09 LIB: DTLS option X-DTLS-Session-ID :
14bcf529d8b05418a9abdab05c37b04c9fbda244fc94f02
08eaf1ef2203360f1
17:13:09 LIB: DTLS option X-DTLS-CipherSuite :
OC-DTLS1_2-AES256-GCM
17:13:09 LIB: DTLS option X-DTLS-MTU : 1434
17:13:09 LIB: DTLS option X-DTLS-Content-Encoding :
oc-lz4
17:13:09 LIB: DTLS initialised. DPD 300, Keepalive 32400
17:13:21 LIB: DTLS handshake timed out
17:13:21 LIB: DTLS handshake failed: Resource
temporarily unavailable, try again.
17:13:35 LIB: SSL read error: Error in the pull function.;
reconnecting.
```

```
OpenConnect
配置文件 日志 常见问题
Disconnected
17:13:38 LIB: X-CSTP-Rekey-Method: ssl
17:13:38 LIB: X-CSTP-Session-Timeout: none
17:13:38 LIB: X-CSTP-Disconnected-Timeout: none
17:13:38 LIB: X-CSTP-Keep: true
17:13:38 LIB: X-CSTP-TCP-Keepalive: true
17:13:38 LIB: X-CSTP-License: accept
17:13:38 LIB: X-DTLS-DPD: 300
17:13:38 LIB: X-DTLS-Port: 443
17:13:38 LIB: X-DTLS-Rekey-Time: 172804
17:13:38 LIB: X-DTLS-Rekey-Method: ssl
17:13:38 LIB: X-DTLS-Keepalive: 32400
17:13:38 LIB: X-DTLS-Session-ID: 01f3c15ce24f1976af34
3e55998a87a283a0efaa95b4bc3717ea0223db41b75f
17:13:38 LIB: X-DTLS-CipherSuite:
OC-DTLS1_2-AES256-GCM
17:13:38 LIB: X-DTLS-MTU: 1434
17:13:38 LIB: X-CSTP-Base-MTU: 1500
17:13:38 LIB: X-CSTP-MTU: 1434
17:13:38 LIB: X-DTLS-Content-Encoding: oc-lz4
17:13:38 LIB: X-CSTP-Content-Encoding: oc-lz4
17:13:38 LIB: CSTP connected. DPD 300, Keepalive 32400
17:13:38 LIB: CSTP Ciphersuite:
TLS1.2)-(ECDHE-RSA-SECP256R1)-(AES-256-GCM)
17:13:38 LIB: DTLS handshake failed: Error in the push
function.
17:13:38 LIB: (Is a firewall preventing you from sending
UDP packets?)
17:13:49 STOP
17:13:49 LIB: Send BYE packet: Aborted by caller
```

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”

```
Aug 25 09:59:04 hnktcvpn openconnect[18239]: Using client certificate '/OU=100041/CN=hnktcvpn'
Aug 25 09:59:04 hnktcvpn openconnect[18239]: SSL negotiation with cloud.ktc.cn
Aug 25 09:59:04 hnktcvpn openconnect[18239]: Server certificate verify failed: unable to get local issuer certificate
Aug 25 09:59:05 hnktcvpn openconnect[18239]: Connected to HTTPS on cloud.ktc.cn
Aug 25 09:59:05 hnktcvpn openconnect[18239]: XML POST enabled
Aug 25 09:59:05 hnktcvpn openconnect[18239]: POST https://cloud.ktc.cn:8443/auth
Aug 25 09:59:05 hnktcvpn openconnect[18239]: SSL negotiation with cloud.ktc.cn
Aug 25 09:59:05 hnktcvpn openconnect[18239]: Server certificate verify failed: unable to get local issuer certificate
Aug 25 09:59:29 hnktcvpn openconnect[20012]: POST https://cloud.ktc.cn:8443/
Aug 25 09:59:29 hnktcvpn openconnect[20012]: Connected to https://cloud.ktc.cn:8443
Aug 25 09:59:29 hnktcvpn openconnect[20012]: Using client certificate '/OU=100041/CN=hnktcvpn'
Aug 25 09:59:29 hnktcvpn openconnect[20012]: SSL negotiation with cloud.ktc.cn
Aug 25 09:59:29 hnktcvpn openconnect[20012]: Server certificate verify failed: unable to get local issuer certificate
Aug 25 09:59:30 hnktcvpn openconnect[20012]: Connected to HTTPS on cloud.ktc.cn
Aug 25 09:59:30 hnktcvpn openconnect[20012]: XML POST enabled
Aug 25 09:59:30 hnktcvpn openconnect[20012]: POST https://cloud.ktc.cn:8443/auth
Aug 25 09:59:30 hnktcvpn openconnect[20012]: SSL negotiation with cloud.ktc.cn
Aug 25 09:59:30 hnktcvpn openconnect[20012]: Server certificate verify failed: unable to get local issuer certificate
Aug 25 09:59:30 hnktcvpn openconnect[20012]: Connected to HTTPS on cloud.ktc.cn
Aug 25 09:59:30 hnktcvpn openconnect[20012]: XML POST enabled
Aug 25 09:59:30 hnktcvpn openconnect[20012]: SSL negotiation with cloud.ktc.cn
Aug 25 09:59:30 hnktcvpn openconnect[20012]: Server certificate verify failed: unable to get local issuer certificate
Aug 25 09:59:30 hnktcvpn openconnect[20012]: Connected to HTTPS on cloud.ktc.cn
```

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
```

