iMC EIA无线802.1X EAP-TLS认证的典型配置案例

iMC 802.1X zhiliao_4Dtat 2018-08-25 发表

组网及说明

本案例适用无线802.1X EAP-TLS的认证方式。

本案例中EIA和接入设备使用的版本如下：

EIA版本为iMC EIA 7.3(E0511)

接入设备为H3C WX3540H Comware Software, Version 7.1.064, Release 5215P01

iNode客户端版本为iNode 7.3(E0522)

配置步骤

1、设备802.1X认证关键配置

配置主认证/计费RADIUS服务器的IP地址为192.168.127.110，认证、计费RADIUS服务器的共享密钥为明文字符串admin，配置设备发送RADIUS报文使用的源IP地址为192.168.127.33。

```
radius scheme 1x
 primary authentication 192.168.127.110
 primary accounting 192.168.127.110
 key authentication simple admin
 key accounting simple admin
 nas-ip 192.168.127.33
```

配置802.1X用户使用RADIUS方案1x进行认证、授权、计费。

```
domain 1x
 authentication lan-access radius-scheme 1x
 authorization lan-access radius-scheme 1x
 accounting lan-access radius-scheme 1x
```

使能RADIUS session control功能。

```
radius session-control enable
```

配置802.1X系统的认证方法为EAP。

```
dot1x authentication-method eap
```

创建并配置无线服务模板1x。

```
wlan service-template 1x
 ssid 1x
 vlan 10
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain 1x
 service-template enable
```

将无线服务模板1x绑定到radio 1和radio 2，并开启射频。

```
wlan ap l2-software model WA2620i-AGN
 serial-id 210235AXXXXXXX000007
radio 1
  radio enable
  service-template 1x
radio 2
  radio enable
  service-template 1x
```

2、iMC服务器的配置

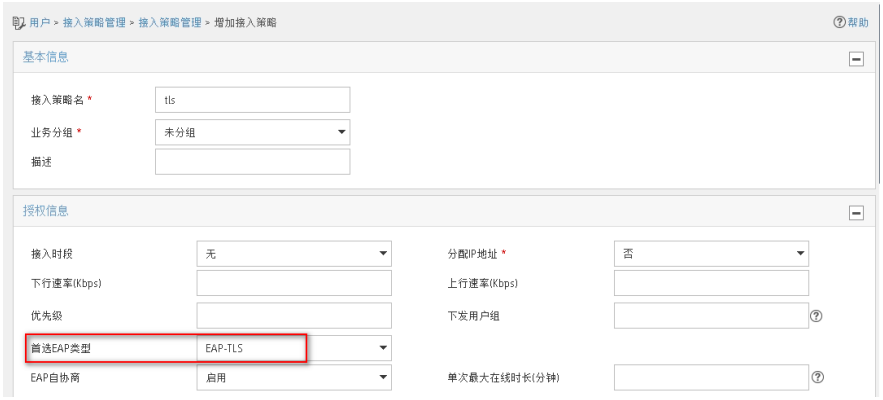
（1）由于采用EAP-TLS证书认证，iMC服务器侧需要导入根证书和服务器证书，客户端需要导入客户端证书，如果客户端验证服务器证书，客户端还需要安装根证书，本案例中客户端不验证服务器证书。

用户>接入策略管理>业务参数配置>证书配置，分别导入根证书和服务器证书。

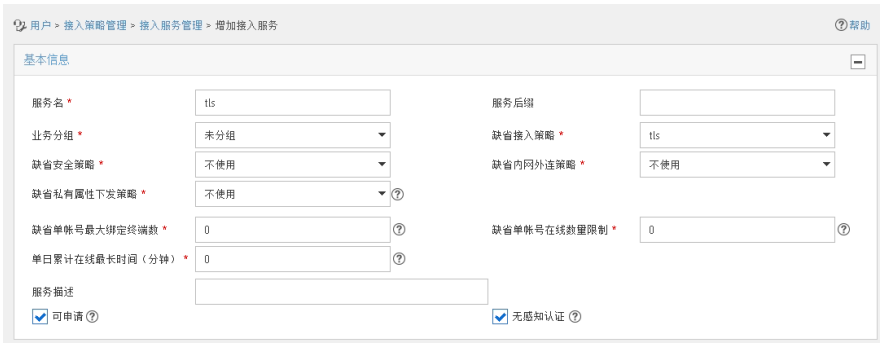
（2）用户>接入策略管理>接入设备管理>接入设备配置，增加认证接入设备192.168.127.33。

注意：增加的接入设备IP需要和认证设备radius scheme下的nas-ip一致，共享密钥需要和radius scheme下的认证、计费radius服务器的密钥一致。

（3）用户>接入策略管理>接入策略管理，增加接入策略tls，首选EAP类型选择EAP-TLS，其他参数保持缺省即可。



（4）用户>接入策略管理>接入服务管理，增加接入服务tls，服务后缀配置为空，缺省接入策略选择tls。



（5）用户>接入用户，增加并配置接入用户whjuser2，接入服务分配tls。

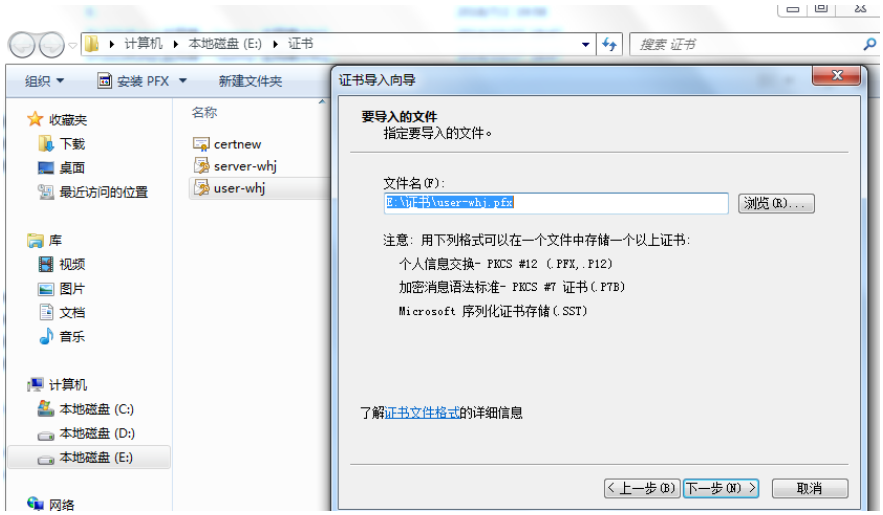
3、客户端的配置

（1）使用iOS手机终端拨号测试

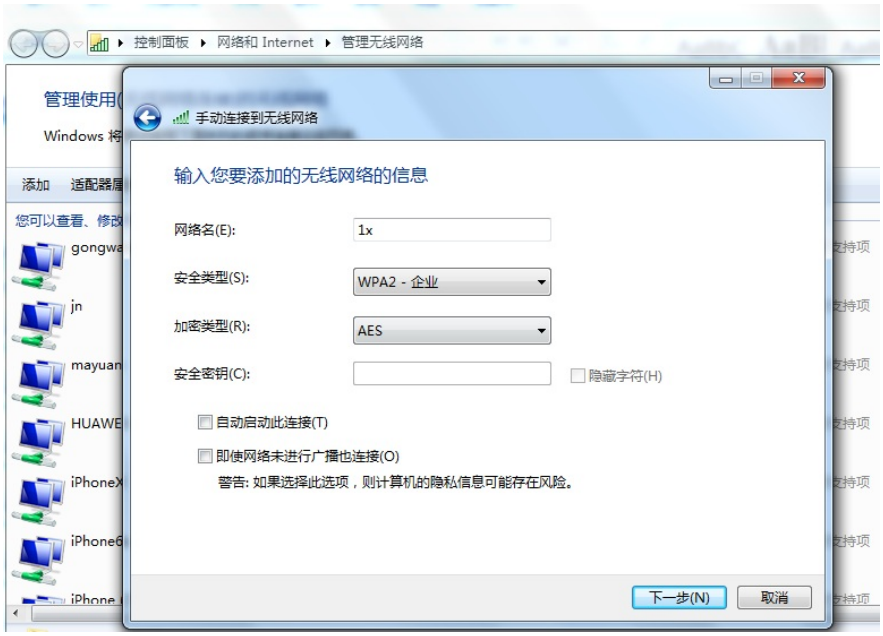
连接SSID为1x的信号，输入用户名001@1x和密码，点击信任证书，终端上线。

（1）使用Windows 7电脑终端拨号测试

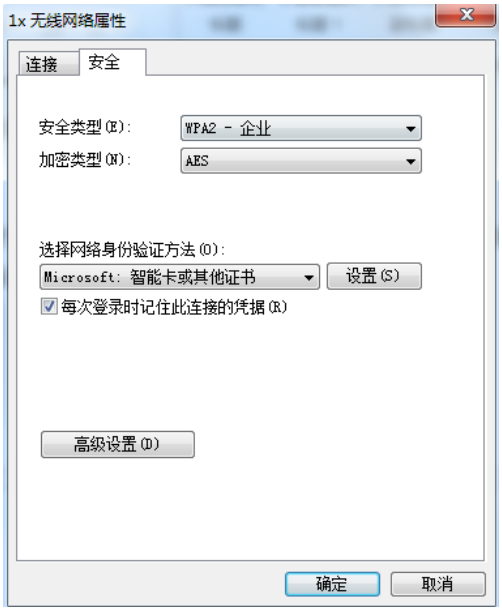
双击客户端证书文件开始导入客户端证书，打开Internet选项>内容>证书，可以查看客户端证书whjuser2已安装导入成功。



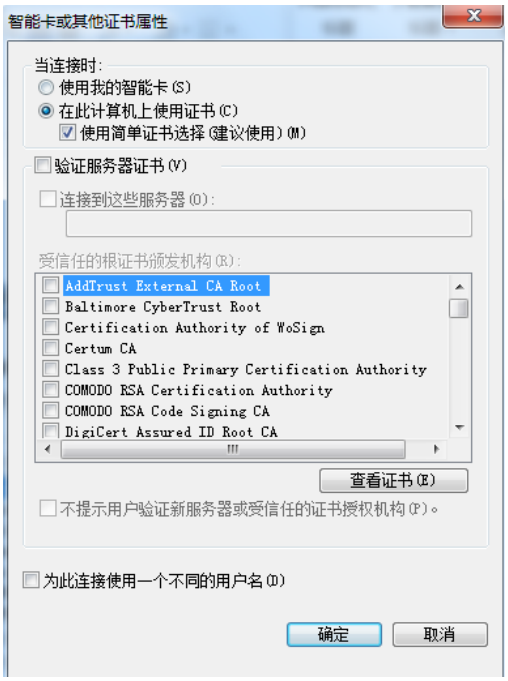
管理无线网络下手动添加SSID 1x的无线网络连接：



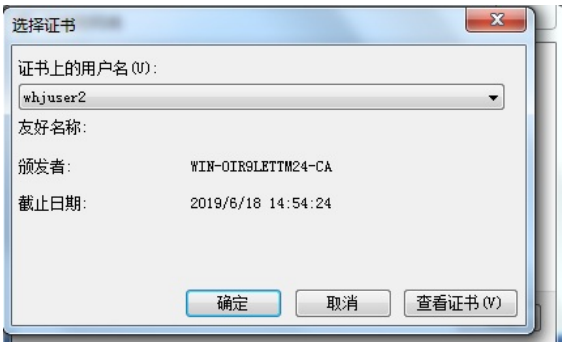
手动添加无线网络连接后，右键设置属性：



网络身份验证方法选择智能卡或其他证书，点击设置，这里客户端不验证服务器证书，去勾选“验证服务器证书”：



设置无线网络连接属性后，连接信号1x，弹出的网络身份验证中选择证书whjuser2，点击确定进行认证：



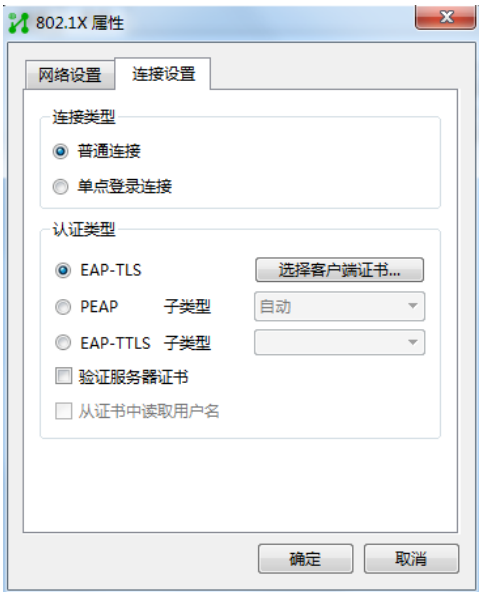
终端连接SSID 1x成功之后，用户>在线用户，可以查看到whjuser2的在线信息：

（2）Windows 7电脑使用iNode客户端拨号

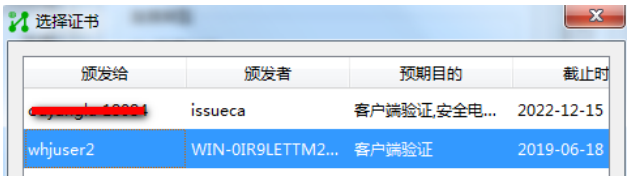
打开iNode客户端，右上角无线图标选择使用iNode客户端管理无线网络，然后选择无线网络SSID信号1x：

点击连接旁边的下拉选项选择属性进行设置：

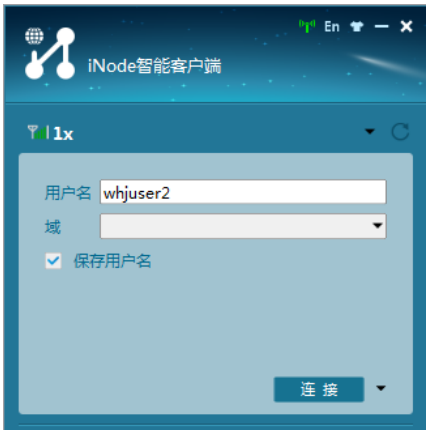
点击802.1X属性进行设置，认证类型选择EAP-TLS，本案例中客户端不验证服务器证书，去勾选验证服务器证书：



选择客户端证书中选择客户端证书whjuser2：



输入用户名whjuser2，点击连接开始认证：



认证成功：

配置关键点

1、EAP-TLS认证iMC服务器侧必须导入服务器证书和客户端证书对应的根证书。

客户端侧必须导入客户端证书，如果客户端验证服务器证书，客户端还需要导入服务器证书对应的根证书。

2、在iMC服务器勾选“检查帐号名与证书中的属性”的情况下，客户端证书名必须和iMC服务器接入用户名一致，否则会认证失败，提示“E63500：证书标识与用户名不匹配。”

如果不勾选“检查帐号名与证书中的属性”，客户端输入的用户名可以和客户端证书名不一样，但是必须保证在iMC服务器上已经创建好此接入用户并分配了EAP-TLS认证对应的接入服务。

其中是否检查帐号名与证书中的属性可以在用户>接入策略管理>业务参数配置>系统配置>系统参数配置页面进行配置，缺省为勾选。