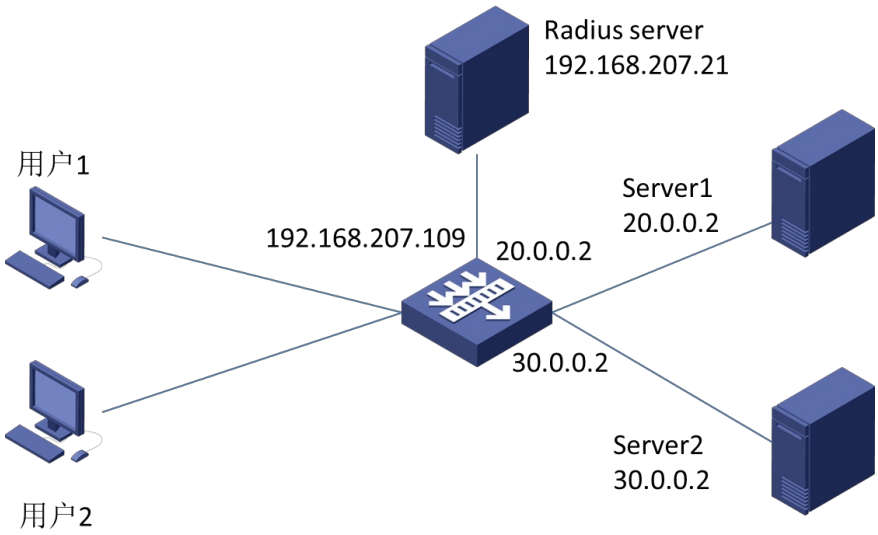
V7防火墙SSLVPN配合IMC密码+动态短信验证码认证配置指导

易予晴 2018-04-25 发表

此配置指导为sslvpn用户提供用户名 密码认证+短信动态密码验证，验证成功后不同的用户访问不同的资源，此处短信验证码由IMC模拟生成，也就是此处短信验证网关为IMC。



SSLVPN网关配置：

```
object-group ip address client
 security-zone Trust
 0 network subnet 100.0.0.0 255.255.255.0
#连接radius服务器接口
interface GigabitEthernet1/0/0
 port link-mode route
 ip address 192.168.207.109 255.255.255.0
#连接客户端接口
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.0.1 255.255.255.0
#连接server端
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 20.0.0.1 255.255.255.0
#连接server端
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 30.0.0.1 255.255.255.0
#
interface SSLVPN-AC0
 ip address 100.0.0.1 255.255.255.0
#
object-policy ip test
 rule 0 pass
#
security-zone name Local
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name DMZ
 import interface GigabitEthernet1/0/0
#
security-zone name Untrust
 import interface GigabitEthernet1/0/3
 import interface GigabitEthernet1/0/5
 import interface SSLVPN-AC0
```

```
#
line class console
 authentication-mode scheme
 user-role network-admin
#
line class vty
 user-role network-operator
#
snmp-agent
 snmp-agent community write simple public
 snmp-agent community read simple private
 snmp-agent sys-info version all #
 ssh server enable
#
acl advanced 3000
 rule 0 permit ip
#定义用户1要放通的资源
acl advanced 3001
 rule 0 permit ip destination 192.168.207.21 0
 rule 5 permit ip destination 20.0.0.0 0.0.0.255
#定义用户2要放通的资源
acl advanced 3002
 rule 0 permit ip destination 192.168.207.21 0
 rule 5 permit ip destination 30.0.0.0 0.0.0.255
#定义radius策略
radius scheme sslvpn
 primary authentication 192.168.207.21 key cipher $c$3$boCg8c0zTBdZfNqxnwb+lfY5np1v0A==
 primary accounting 192.168.207.21 key cipher $c$3$sGszy2vBnB1kqAh4zBjSPq6fmAEziQ==
 key authentication cipher $c$3$x128ZL/hdtnZnH977NGlgHp/wP0T1w==
 key accounting cipher $c$3$toEtuJMyfuE6m7QeGThQVBwdyS/oCQ==
 user-name-format without-domain
#
domain sslvpn
 authentication sslvpn radius-scheme sslvpn
 authorization sslvpn radius-scheme sslvpn
 accounting sslvpn radius-scheme sslvpn
#

#
user-group usergroup
 authorization-attribute sslvpn-policy-group pgroup
#
user-group usergroup1
 authorization-attribute sslvpn-policy-group pgroup1
#配置PKI域
pki domain sslvpn
 public-key rsa general name sslvpn
 undo crl check enable
#配置ssl策略
ssl server-policy ssl
 pki-domain sslvpn
#配置netconf参数
 netconf soap http enable
 netconf soap https enable
 netconf ssh server enable
#
 ip https enable
 webui log enable
#配置SSLVPN IP接入地址池
sslvpn ip address-pool ippool 100.0.0.2 100.0.0.254
#配置SSLVPN网关
sslvpn gateway gw
 ip address 10.0.0.1 port 2000
 ssl server-policy ssl
```

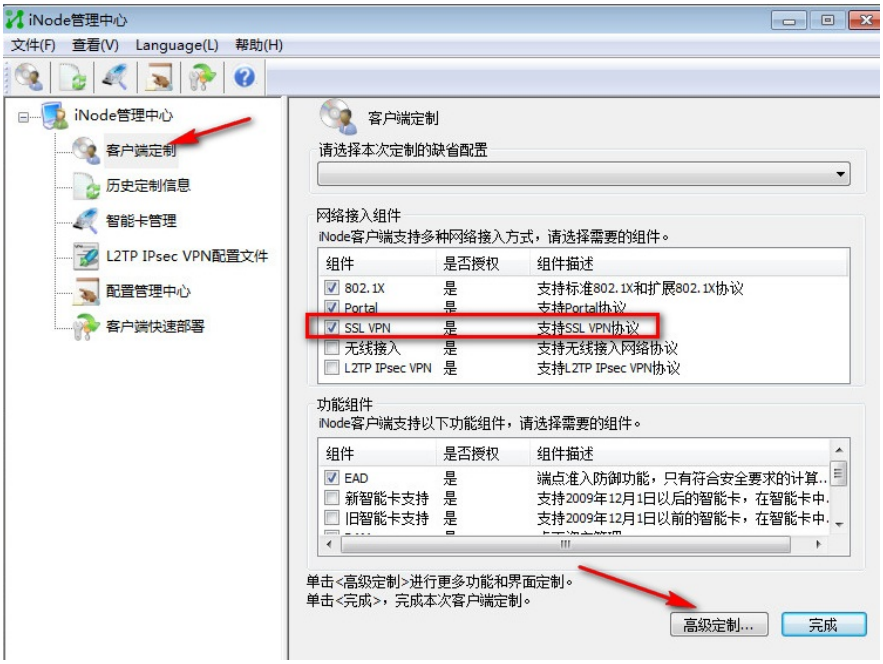
```
 service enable
#
sslvpn context ctx
 gateway gw
 ip-tunnel interface SSLVPN-AC0
 ip-tunnel address-pool ippool mask 255.255.255.0
#配置用户1可以访问的路由列表
 ip-route-list iplist
  include 20.0.0.0 255.255.255.0
  include 192.168.206.0 255.255.254.0
#配置用户2可以访问的路由列表
 ip-route-list iplist1
  include 30.0.0.0 255.255.255.0
  include 192.168.206.0 255.255.254.0
#配置IP接入要访问的资源快捷方式
 shortcut resource1
  execution url(&＃39;20.0.0.3:81&＃39;)
 shortcut-list resource1
  resources shortcut resource1

shortcut resource2
  execution url(&＃39;30.0.0.3:81&＃39;)
 shortcut-list resource2
  resources shortcut resource2
#配置用户1的资源池
 policy-group pgroup
  filter ip-tunnel acl 3001
  ip-tunnel access-route force-all
  ip-tunnel access-route ip-route-list iplist
  resources shortcut-list resource1
#配置用户2的资源池
 policy-group pgroup1
  filter ip-tunnel acl 3002
  ip-tunnel access-route ip-route-list iplist1
  resources shortcut-list resource2
 aaa domain sslvpn
#配置短信网关
 sms-imc address 192.168.207.21 port 8080
 sms-imc enable
 service enable
#配置安全策略
security-policy ip
 rule 0 name test
  action pass
  source-zone Trust
  source-zone Local
  destination-zone Local
  destination-zone Trust
 rule 1 name managent
  action pass
  source-zone DMZ
  source-zone Local
  destination-zone Local
  destination-zone DMZ
 rule 2 name sslvpn
  action pass
  source-zone Trust
  destination-zone Untrust
  source-ip client
 rule 3 name radius
  action pass
  source-zone Trust
  source-zone DMZ
  destination-zone Trust
```

```
 destination-zone DMZ
rule 4 name untrust-untrust
 action pass
 source-zone Untrust
 destination-zone Untrust
rule 5 name dmz-untrust
 action pass
 counting enable
 source-zone Untrust
 destination-zone DMZ
#
```

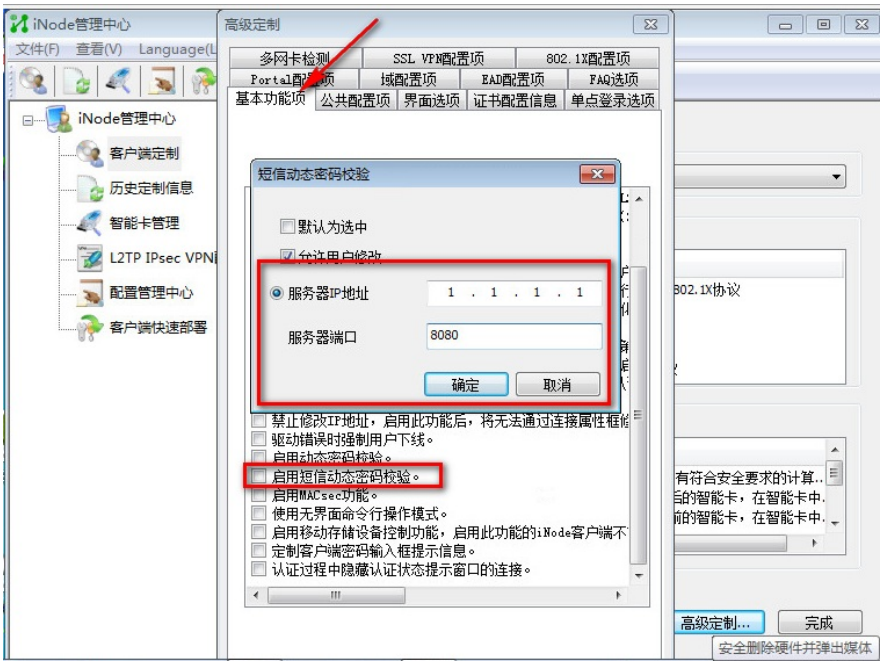
客户端配置：

INODE客户端默认是不支持短信验证码的，需要手工定制SSLVPN支持短信验证码。

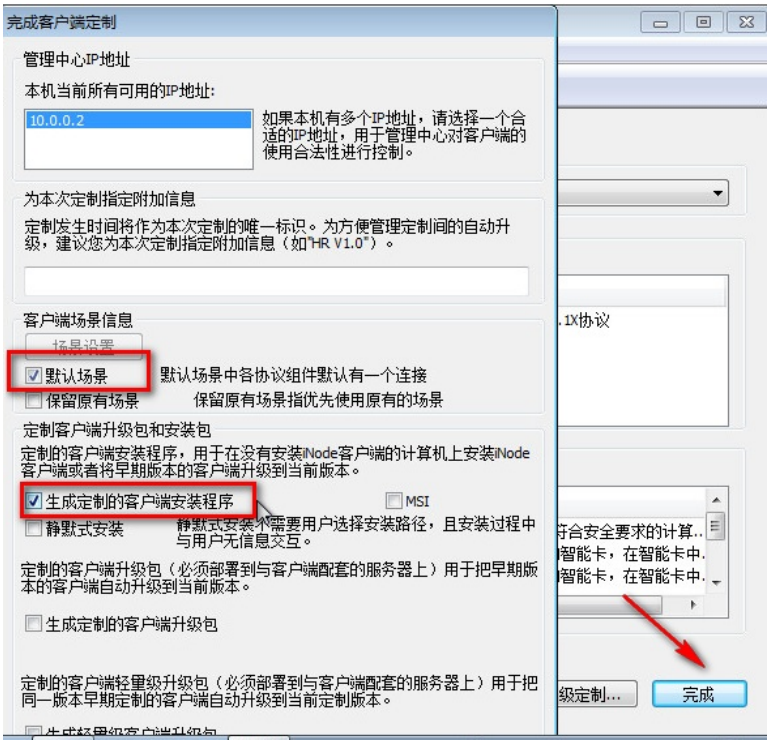
1） 打开INODE管理中心，点击客户端定制，在网络接入组件中勾选SSLVPN，点击高级定制，进入高级定制配置页面。



2） 进入“基本功能项”，勾选“启用短信动态密码校验”，输入短信网关的地址和端口，这的地址和端口随便输入，因为短信网关在sslvpn网关设备上配置了。



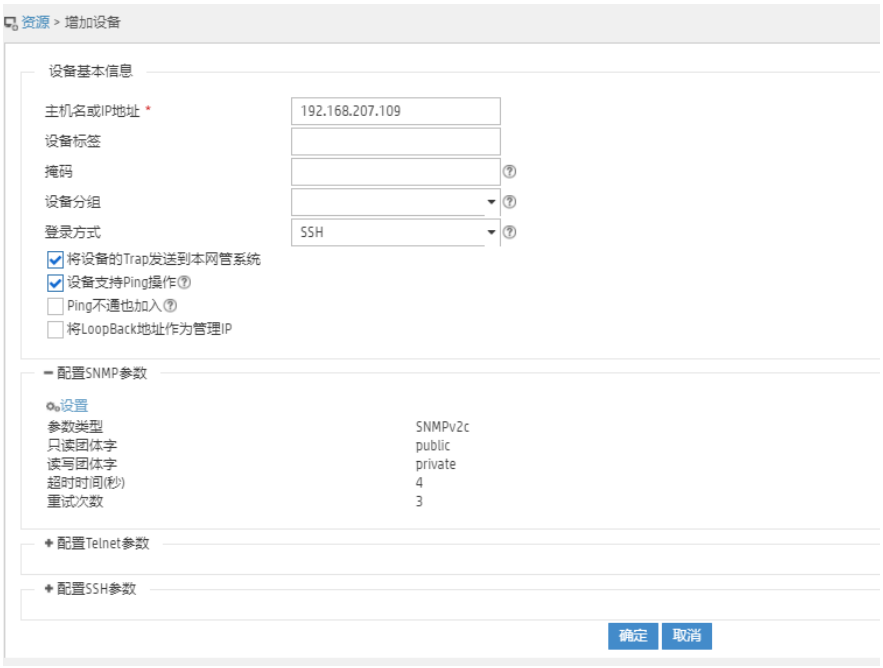
3） 点完成进入客户端定制页面，此处勾选生成客户端安装包或者静默安装都可以。

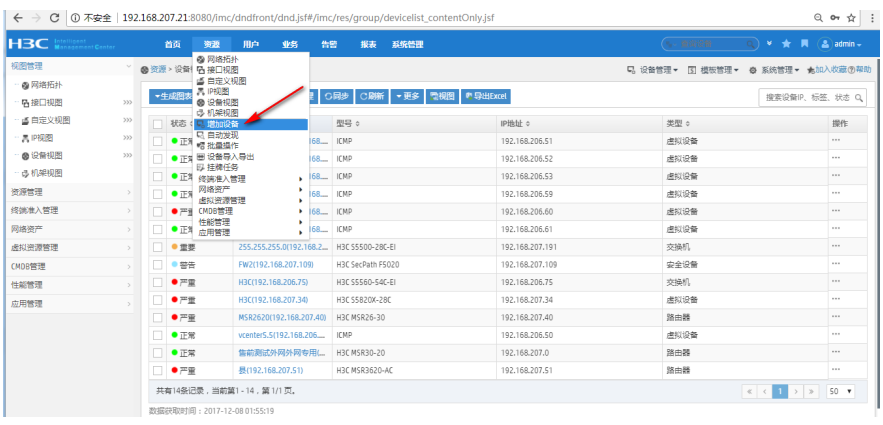


4） 安装定制好的inode客户端。

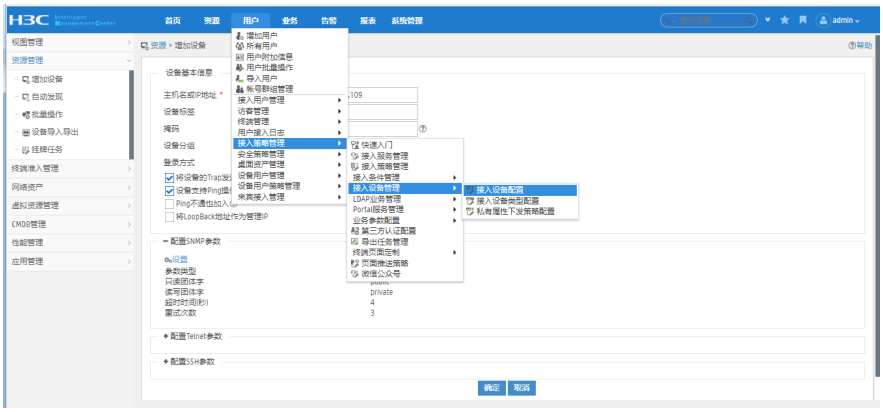
IMC配置：

1）资源---增加设备

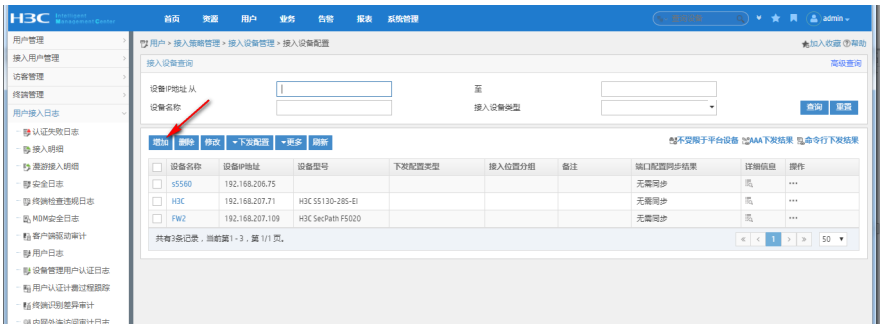




2）增加接入设备

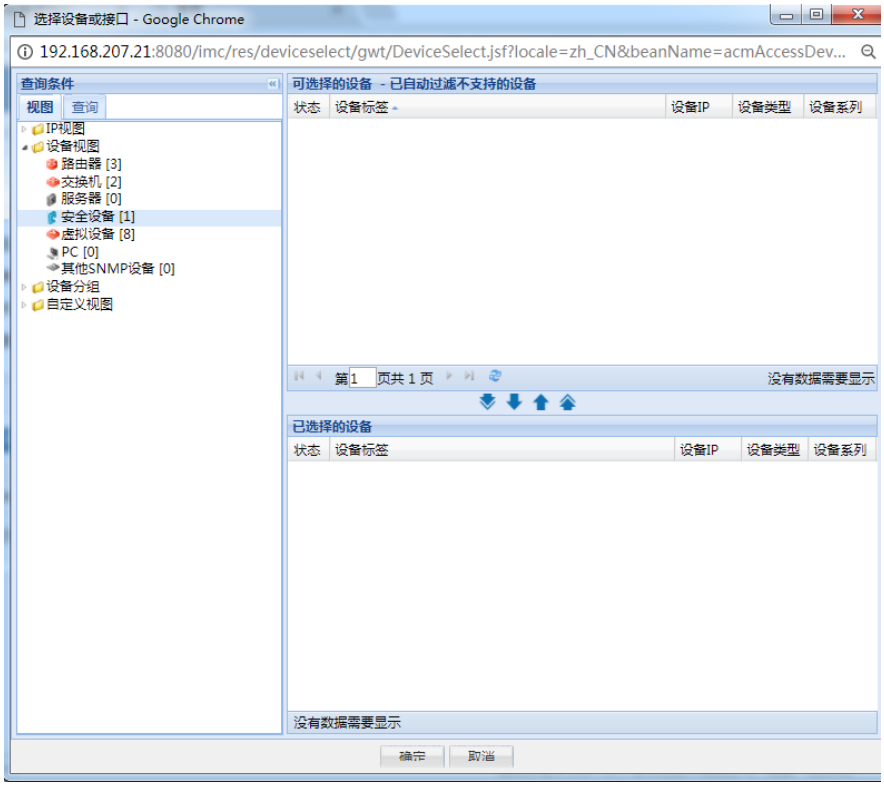


点击增加。



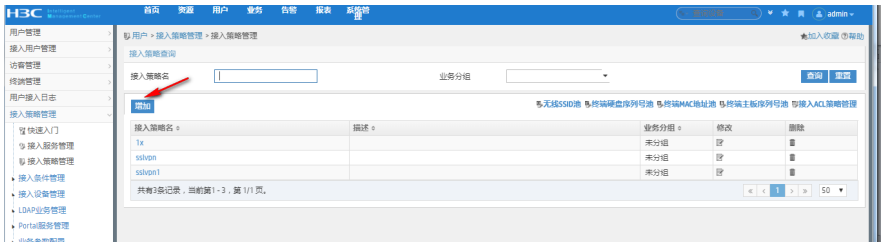
输入 认证端口 计费端口 共享密钥，选择接入设备。

选择接入设备。

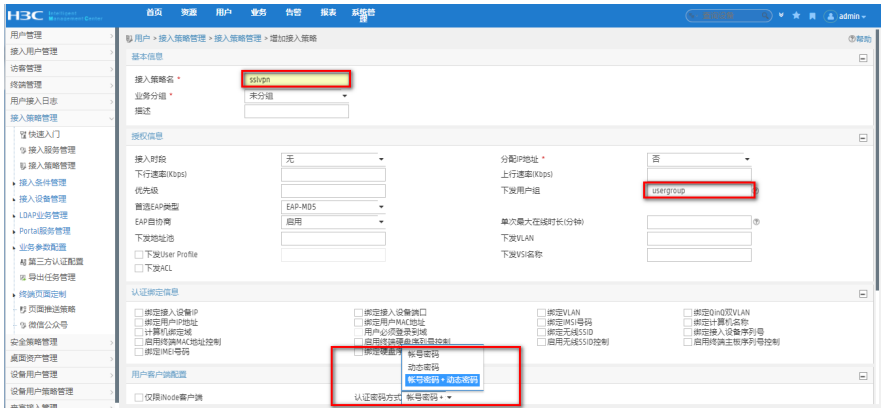


3）配置接入策略，不同的用户组下发不同的接入策略。

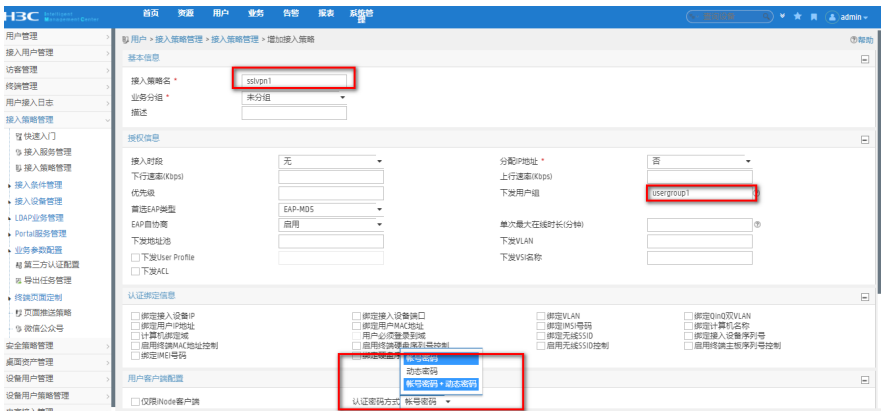
进入接入策略配置视图，点击增加。



配置用户1的接入策略sslvpn，下发用户组usegroup,认证密码方式选择 账号密码+动态密码。



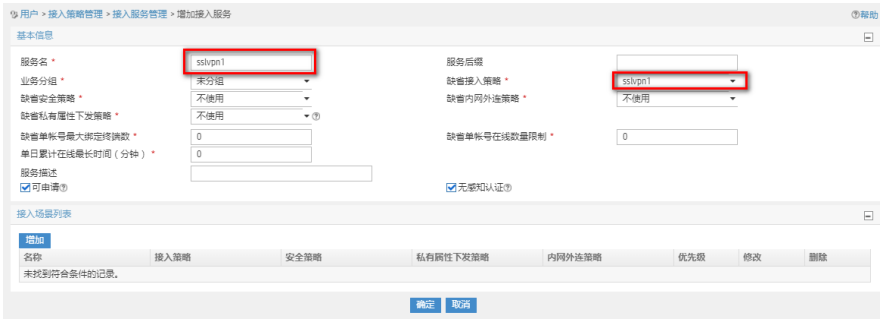
配置用户2的接入策略，下发用户组usergroup1,认证密码方式选择 账号密码+动态密码。



3）配置接入服务

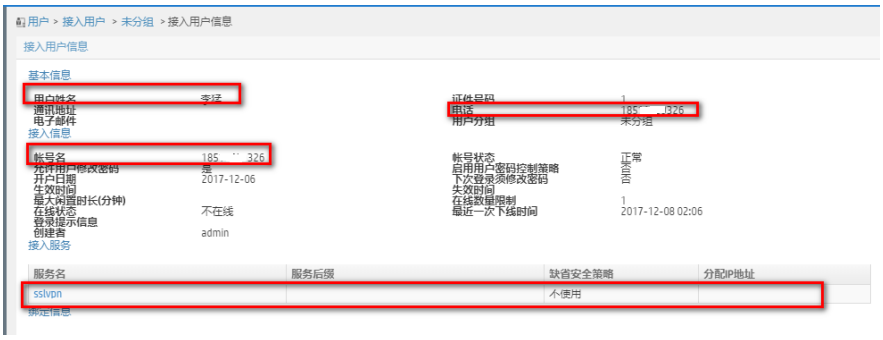
配合用户1的接入服务sslvpn，引用用户1的接入策略sslvpn。

配置用户2的接入服务sslvpn1，引用用户2的接入策略sslvpn。

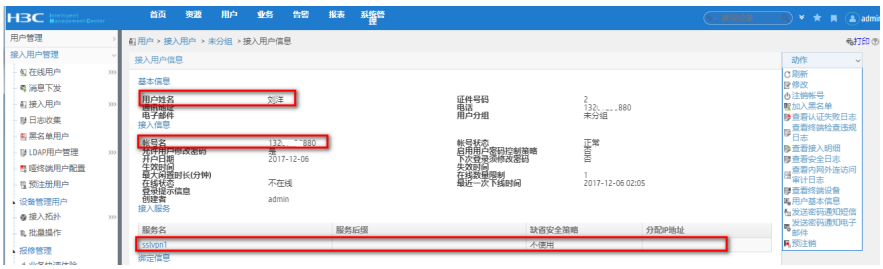


4) 配置接入用户

配置用户1，引用接入服务sslvpn。



配置用户2，引用接入服务sslvpn1。



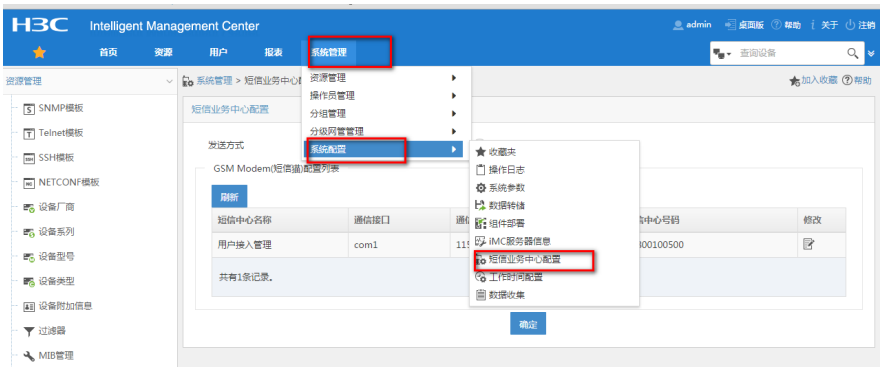
5) 配置短信网关

放入jar包，将imc_sms_test(2014-2-11.new).jar包放入iMC安装环境下的一下目录

C:\Program Files\iMC\client\repository\imc\jars

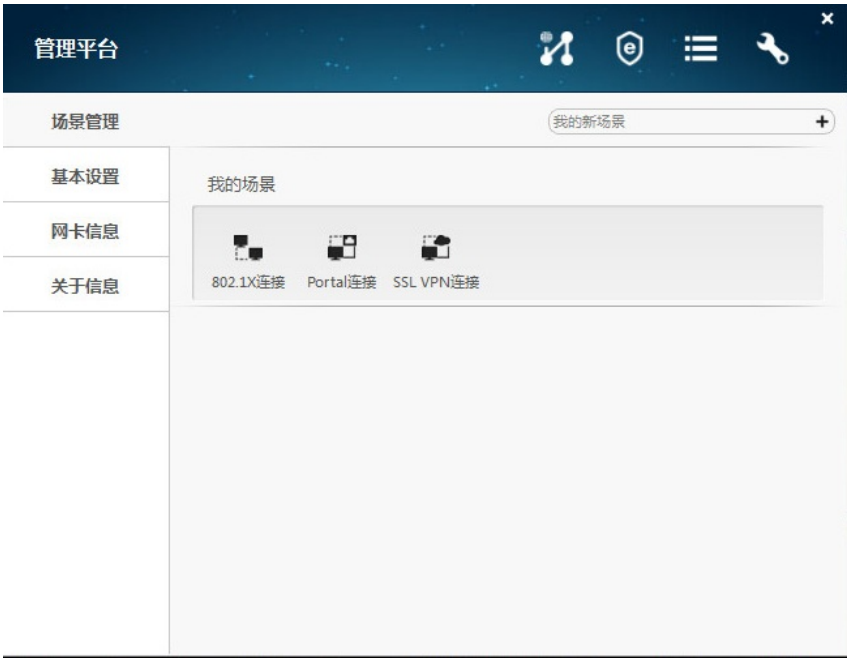
iMC前台短信网关配置，进入以下“短信业务中心配置”页面，选择“其他厂商短信平台”，点击“确定”即可

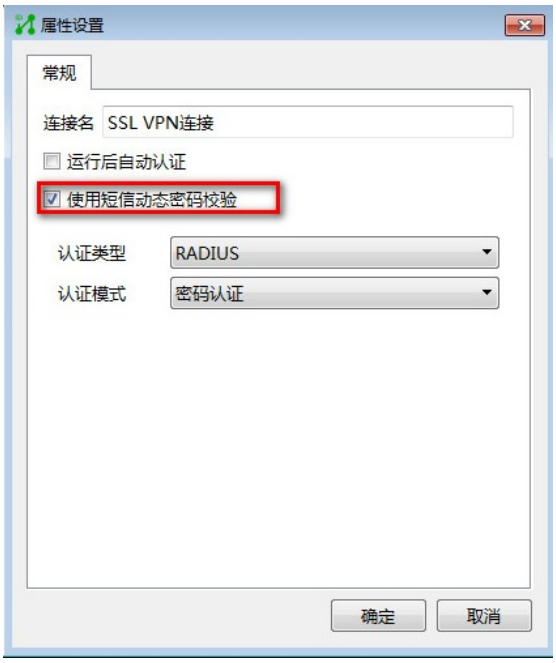
。



重启jserver进程即可，短信验证码记录在日志文件\iMC\client\log\imcforeground.log中。
请注意：必须是先放入jar包，再重启jserver，配置才能生效。有些旧的平台版本不支持，E0303版本及以上应该都支持。

注意事项：
Inode默认定制好后，虽然定制了短信验证码功能，但是短信验证码默认是不启用的，需要手工启用。打开inode客户端，点击右下角管理中心进入管理中心配置页面，选择SSL VPN右键属性，勾选“使用短信动态密码校验”。





输入sslvpn网关地址和端口号，用户名 密码 短信验证码点击连接。