

# 配置WLCs &微软视窗2003 IAS的RADIUS IPsec安全服务器

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[IPSec RADIUS配置](#)

[配置 WLC](#)

[配置IAS](#)

[微软视窗2003域安全设置](#)

[Windows 2003个系统日志事件](#)

[无线局域网控制器RADIUS IPsec成功调试示例](#)

[Ethreal捕获](#)

[Related Information](#)

## [Introduction](#)

此指南文件如何配置WCS和这些WLAN控制器支持的RADIUS IPsec功能：

- 4400 系列
- WiSM
- 3750G

控制器RADIUS IPsec功能位于在**安全>AAA > RADIUS验证服务器**部分下的控制器GUI。功能为您提供一个方法加密控制器和RADIUS服务器(IAS)之间的所有RADIUS通信与IPsec。

## [Prerequisites](#)

## [Requirements](#)

Cisco 建议您了解以下主题：

- 在LWAPP的知识
- 在RADIUS认证和IPsec的知识
- 关于怎样的知识配置在操作系统Windows 2003的服务器的服务

## [Components Used](#)

这些必须安装和配置网络和软件组件为了设置控制器RADIUS IPsec功能：

- WLC4400、WiSM或者3750G控制器。运行软件版本5.2.178.0的此示例使用WLC4400
- 轻量级接入点(膝部)。此示例使用1231系列LAP。
- 交换与DHCP
- 作为域控制器被配置的Microsoft 2003服务器安装用微软认证授权和用Microsoft互联网认证服务(IAS)。
- Microsoft域安全
- Cisco 802.11 a/b/g无线客户端适配器用WPA2/的ADU版本3.6配置PEAP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

## IPsec RADIUS配置

此配置指南不说明Microsoft WinServer、认证机关、激活目录或者WLAN 802.1x客户端的安装或配置。必须在控制器IPsec RADIUS功能的配置之前安装和配置这些组件。此指南文件剩下的事如何配置在这些组件的IPsec RADIUS：

1. Cisco WLAN控制器
2. Windows 2003 IAS
3. 微软视窗域安全设置

## 配置 WLC

此部分说明如何通过GUI配置在WLC的IPsec。

从控制器GUI，请完成这些步骤。

1. 连接对在控制器GUI的**安全>AAA > RADIUS Authentication**选项，并且添加一个新的RADIUS服务器。

**RADIUS Authentication Servers**

Call Station ID Type: IP Address

Credentials Caching:

Use AES Key Wrap:

Network User	Management	Server Index	Server Address	Port	IPSec
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	192.168.30.10	1812	Disabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3	192.168.30.105	1812	Enabled

2. 配置IP地址、端口1812和新的RADIUS服务器的一个共有的秘密。检查IPSec Enable复选框，配置这些IPSec参数和然后点击适用。Note: 共有的秘密用于验证RADIUS服务器和作为预共享密钥(PSK) IPSec认证的。

**Shared Secret** [...]

**Confirm Shared Secret** [...]

**Key Wrap**

**Port Number** 1812

**Server Status** Enabled

**Support for RFC 3576** Disabled

**Retransmit Timeout** 2 seconds

**Network User**  Enable

**Management**  Enable

**IPSec**  Enable

**IPsec Parameters**

IPsec: HMAC SHA1

IPSEC Encryption: 3DES  
(Shared Secret will be used as the Preshared Key)

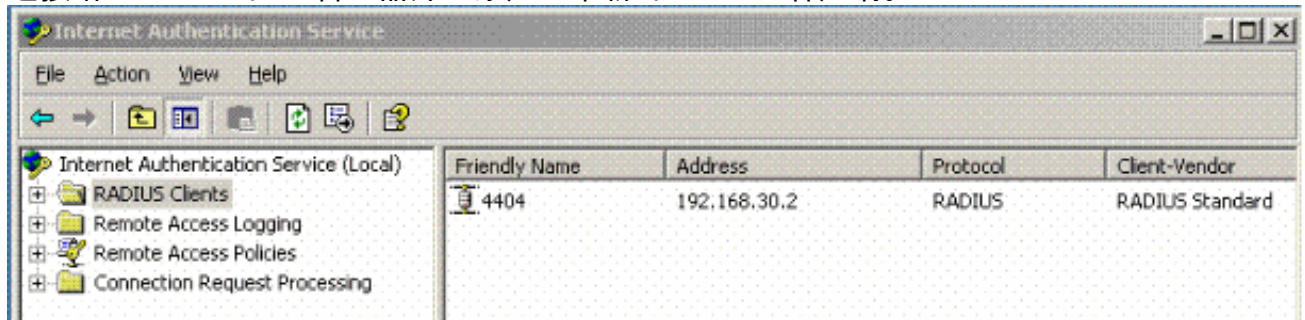
IKE Phase 1: Main

Lifetime (seconds): 28800

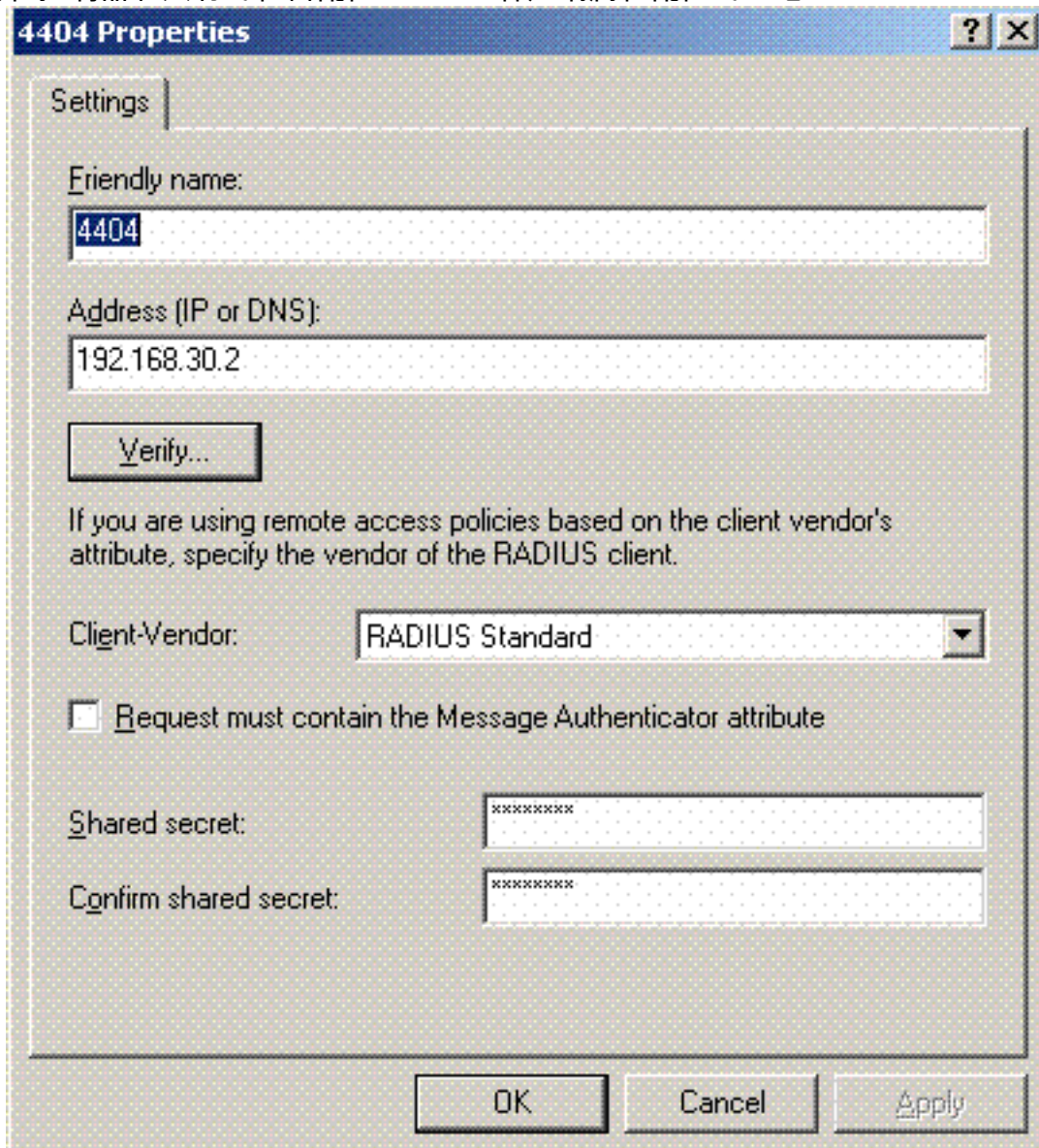
IKE Diffie Hellman Group: Group 2 (1024 bits)

完成在IAS的这些步骤：

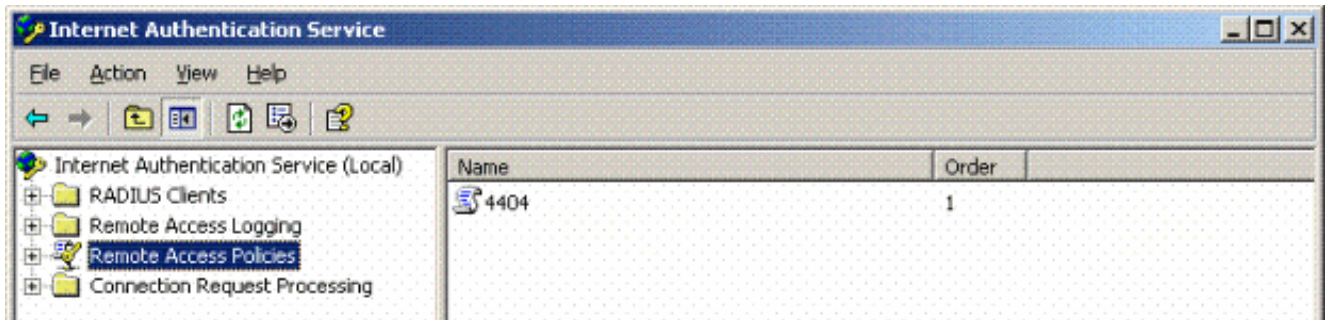
1. 连接给Win2003的IAS管理器并且添加一个新的RADIUS客户端。



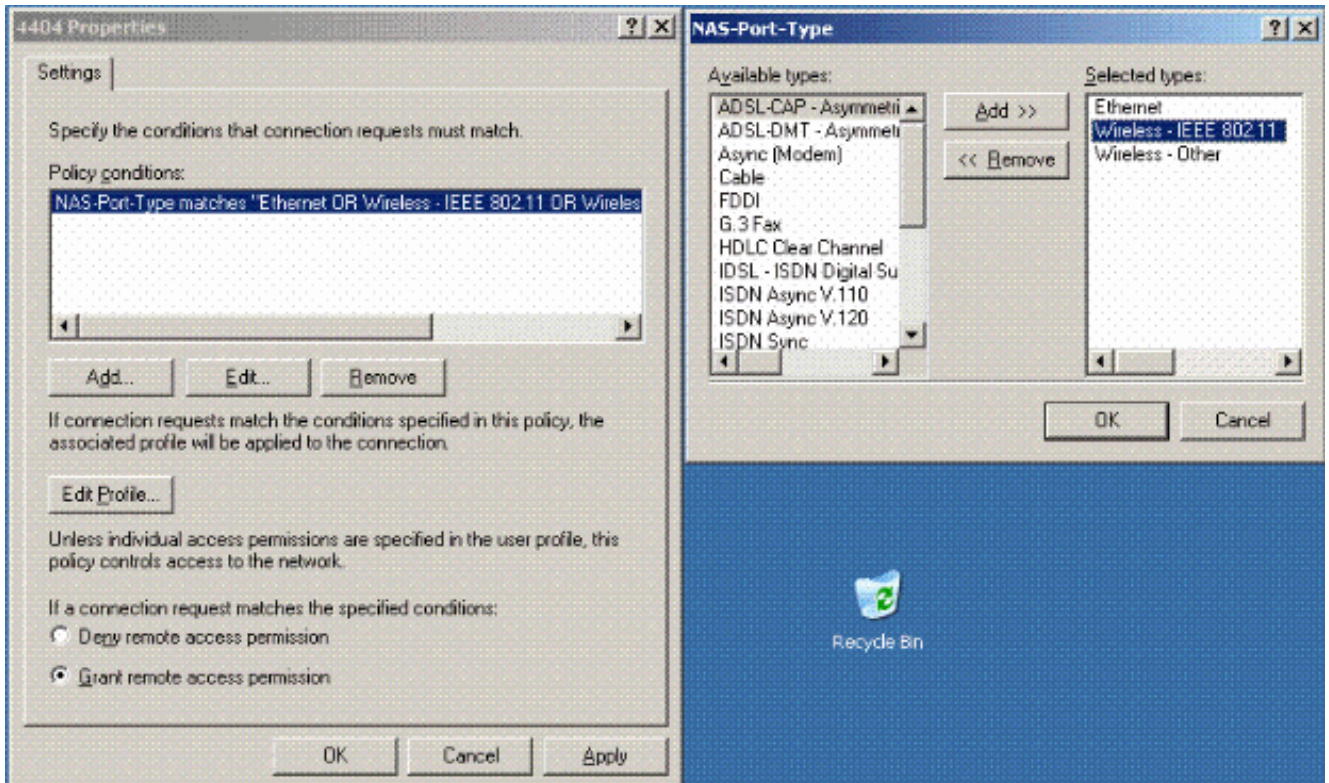
2. 用在控制器和共有的秘密配置RADIUS客户端属性配置的IP地址



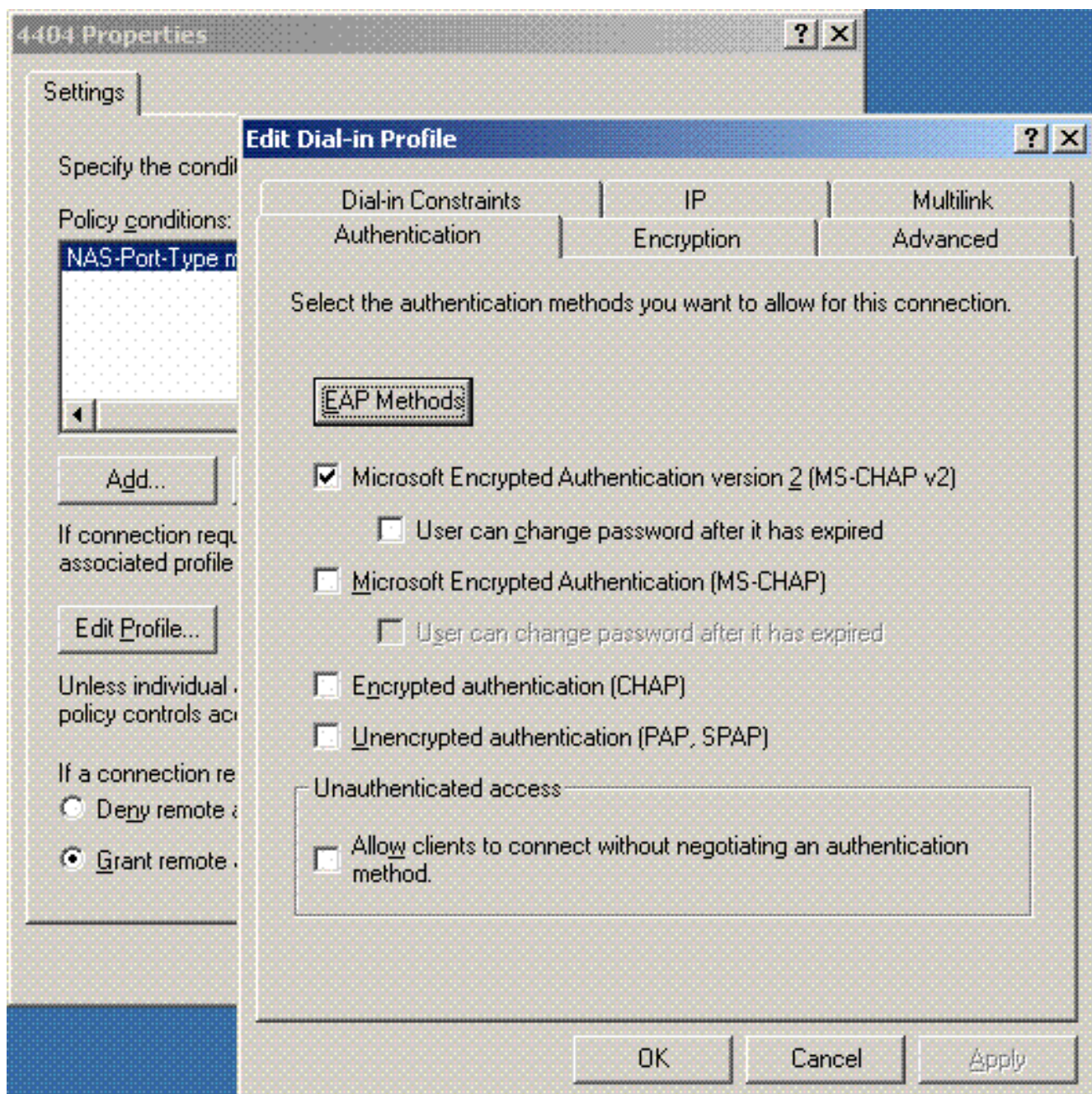
3. 配置控制器的一新的Remote access Policy



4. 编辑控制器Remote access Policy的属性。保证添加Nas-port类型-无线- IEEE 802.11

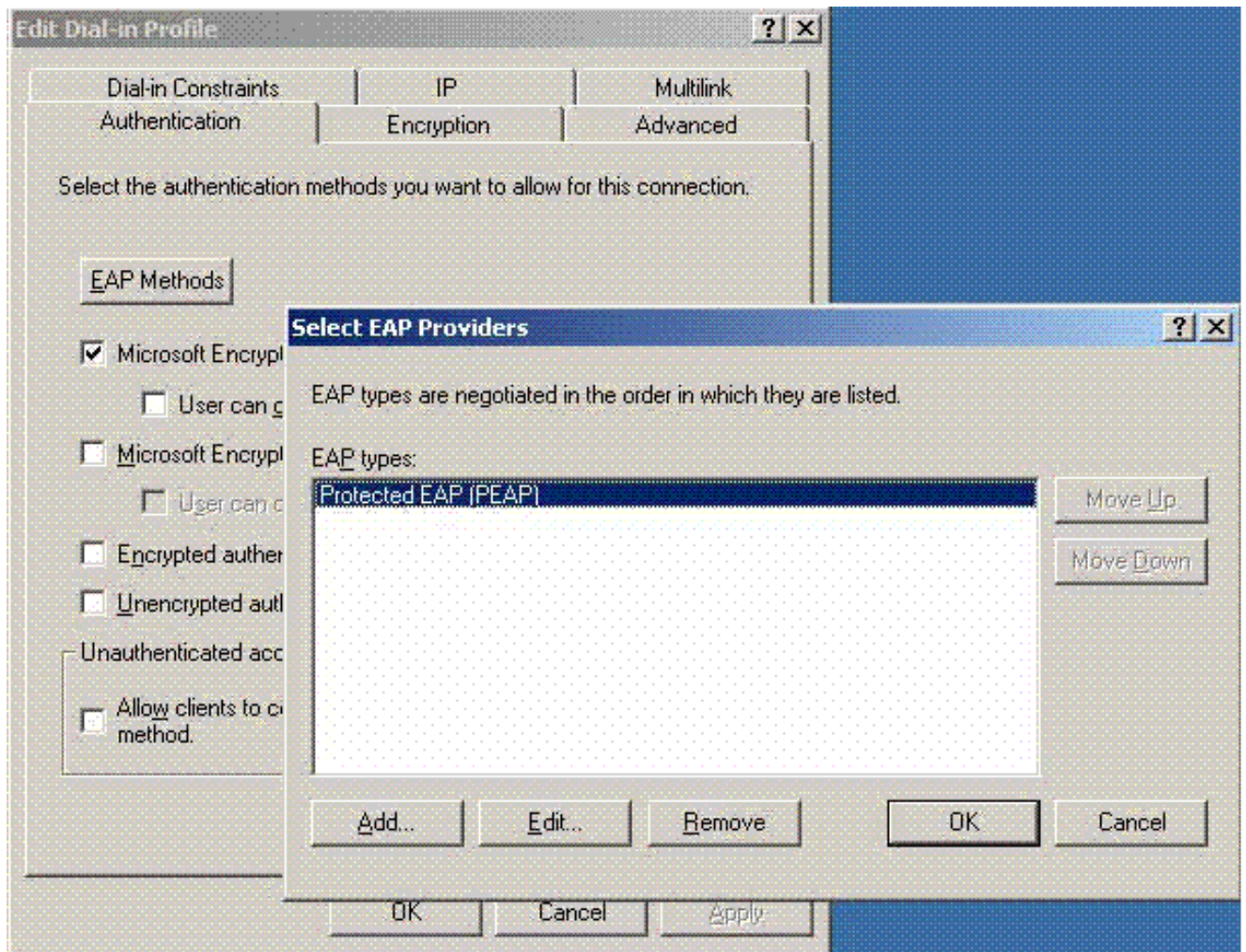


5. 点击编辑配置文件，点击Authentication选项，并且检查MS-CHAP v2认证

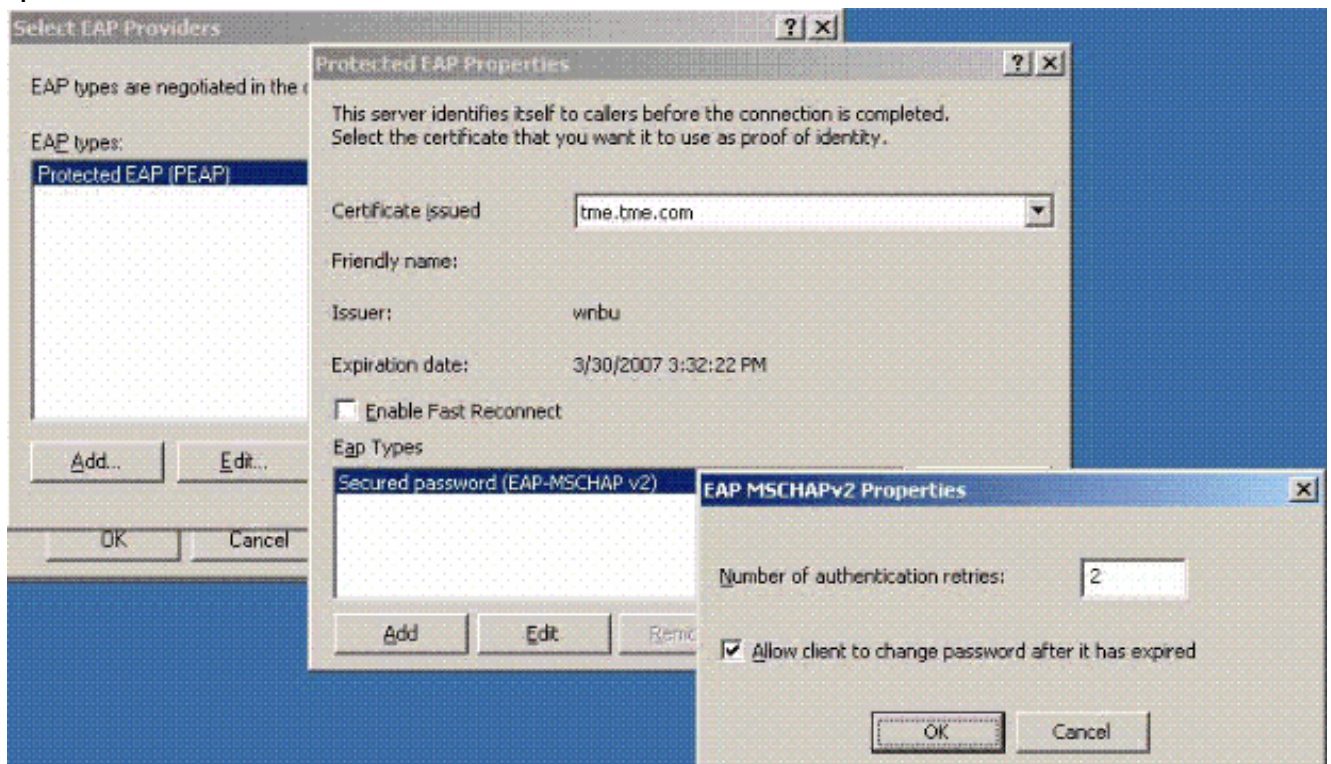


6. 点击**EAP方法**，选择EAP供应商，并且添加PEAP作为EAP类型

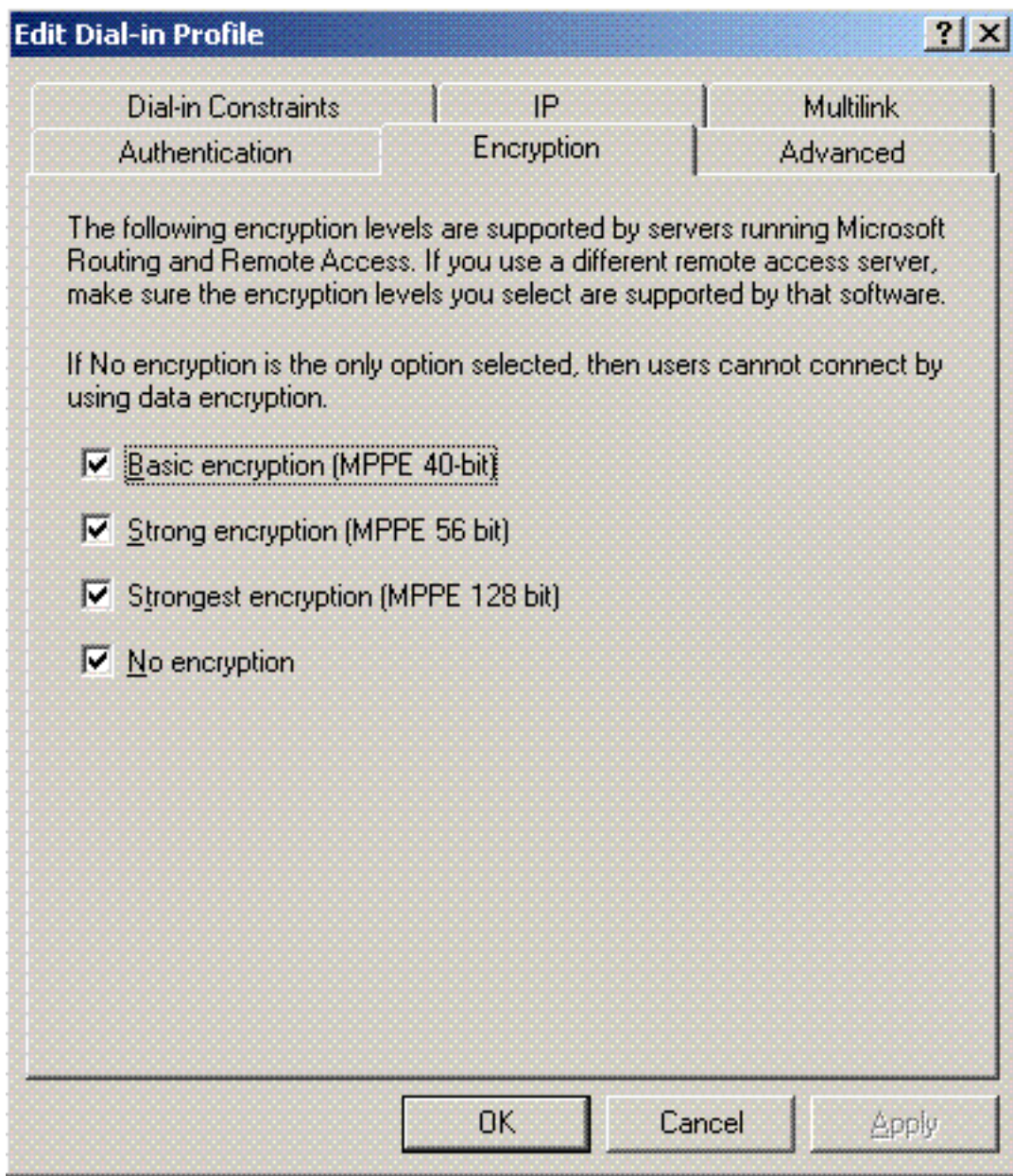
:



7. 点击**编辑**在Select EAP供应商并且从即服务器与您的激活目录用户帐户和CA的下拉菜单选择 (tme.tme.com)产生关联。添加EAP类型MSCHAP v2

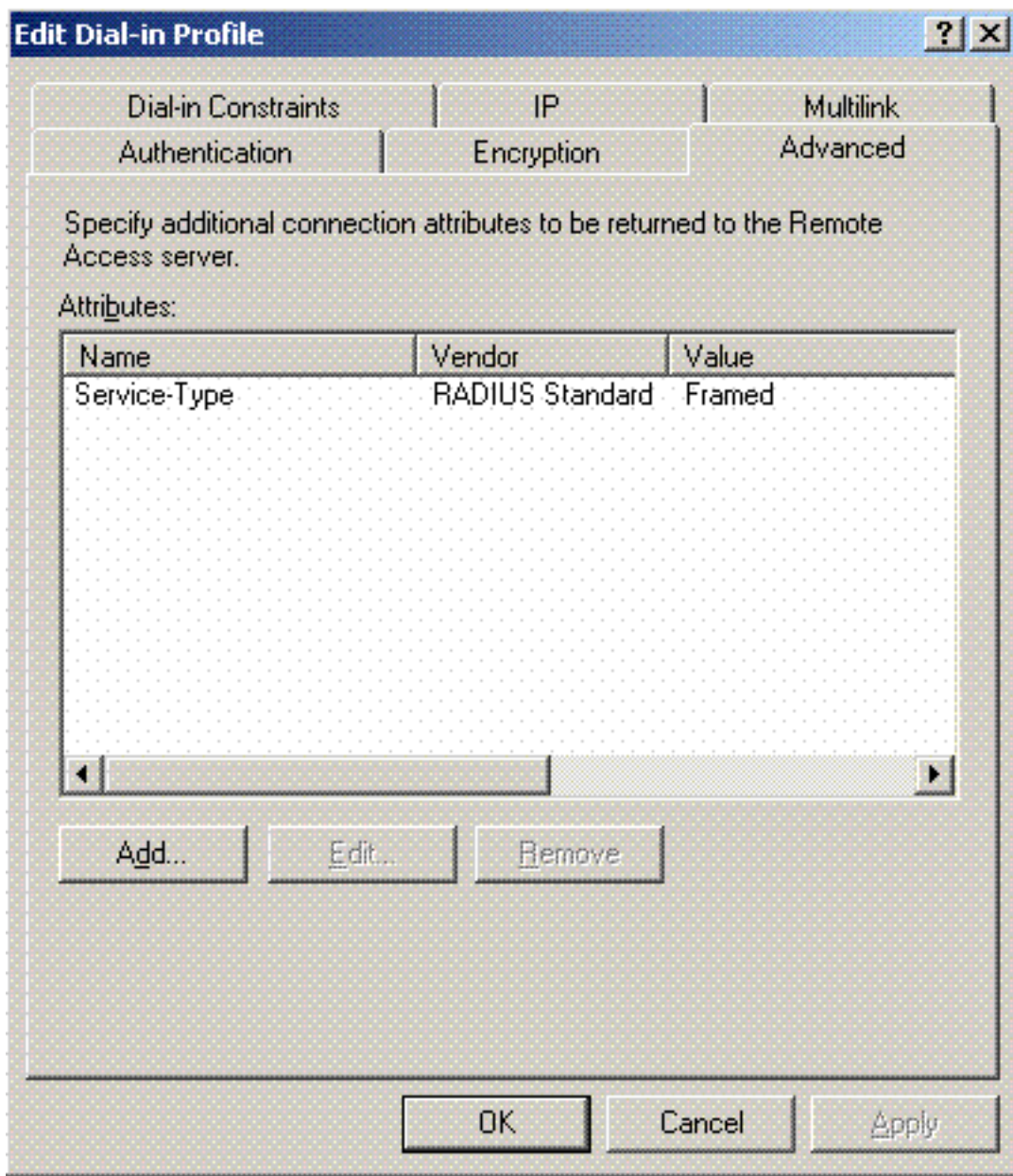


8. 点击**Encryption**选项，并且检查所有加密类型远程访问

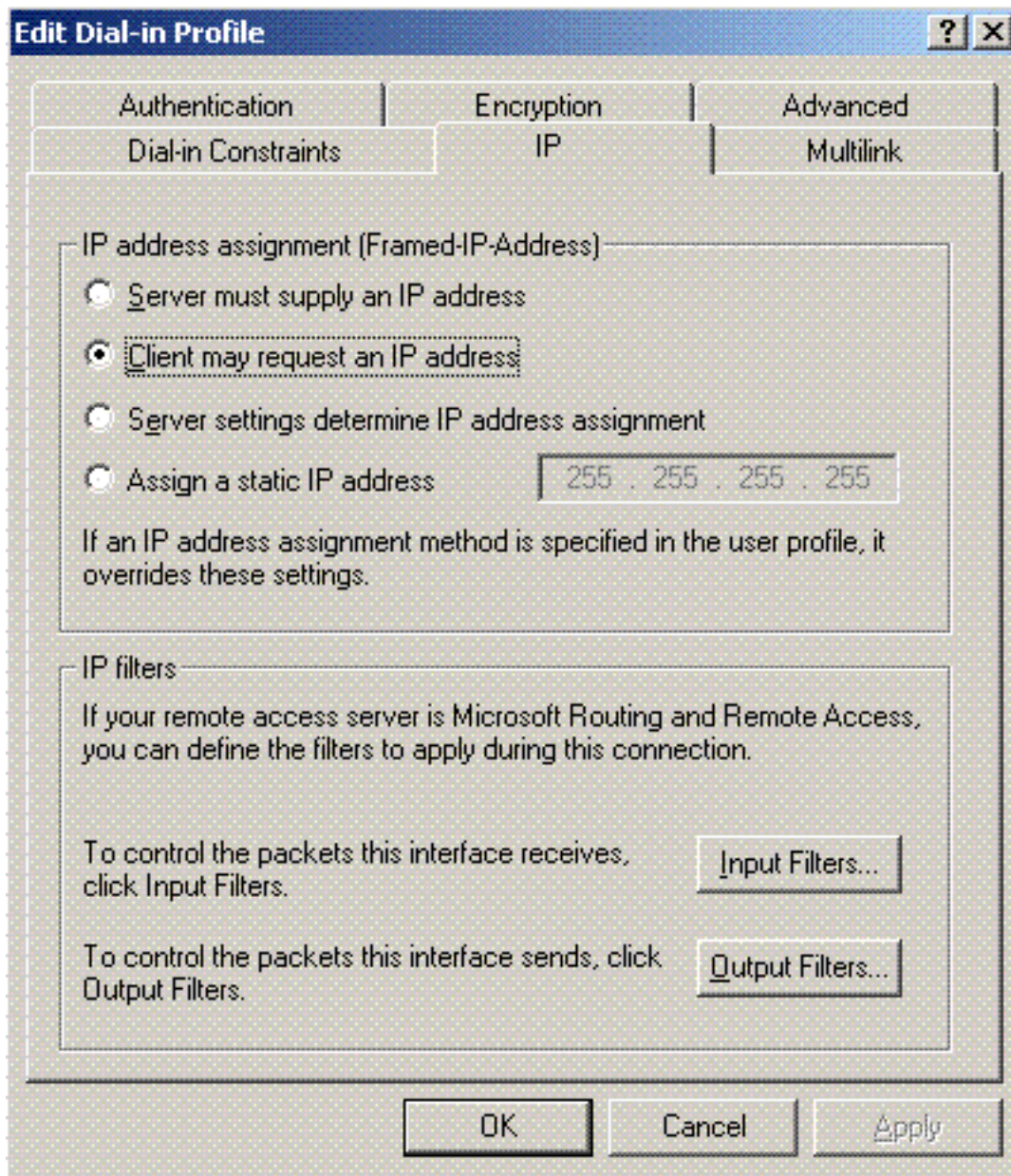


9. 点击高级选项卡。 ，并且添加RADIUS标准/构筑作为服务类型





10. 点击IP选项，并且检查客户端可能要求IP地址。这假设您有在交换机或WinServer的启用

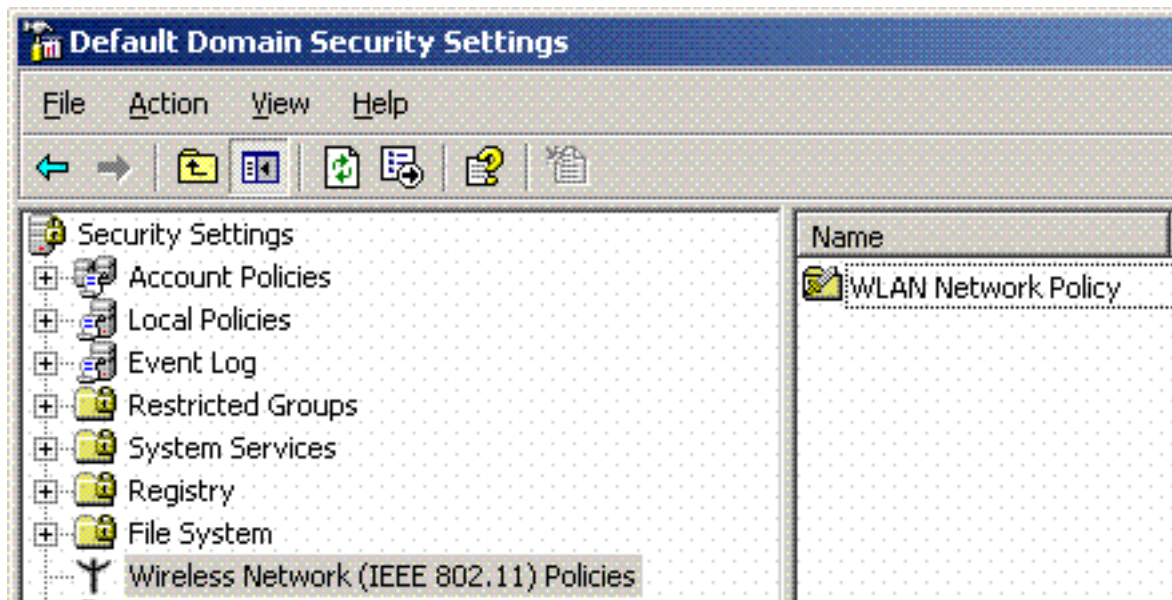


DHCP。

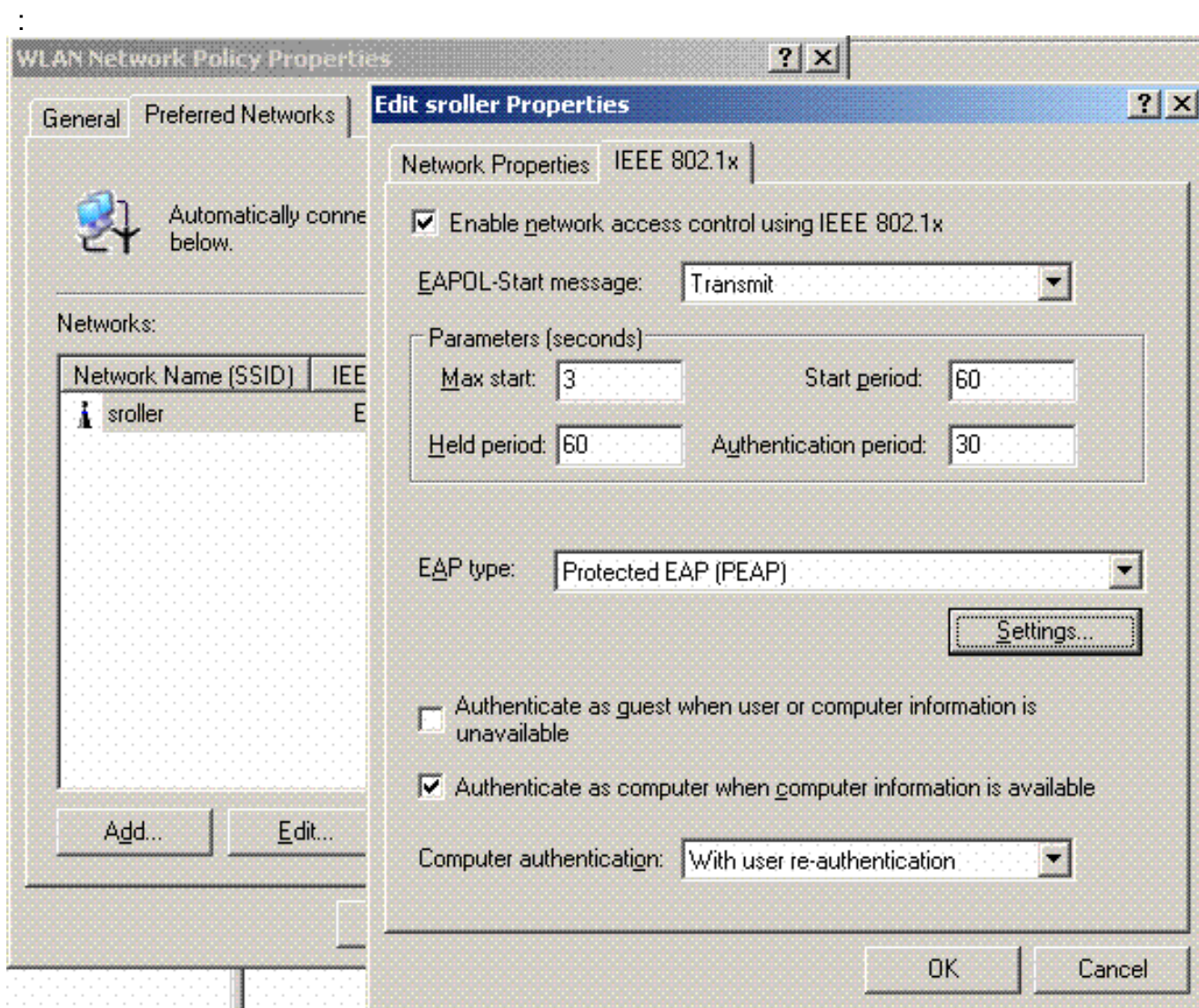
## [微软视窗2003域安全设置](#)

完成这些步骤为了配置Windows 2003域安全设置：

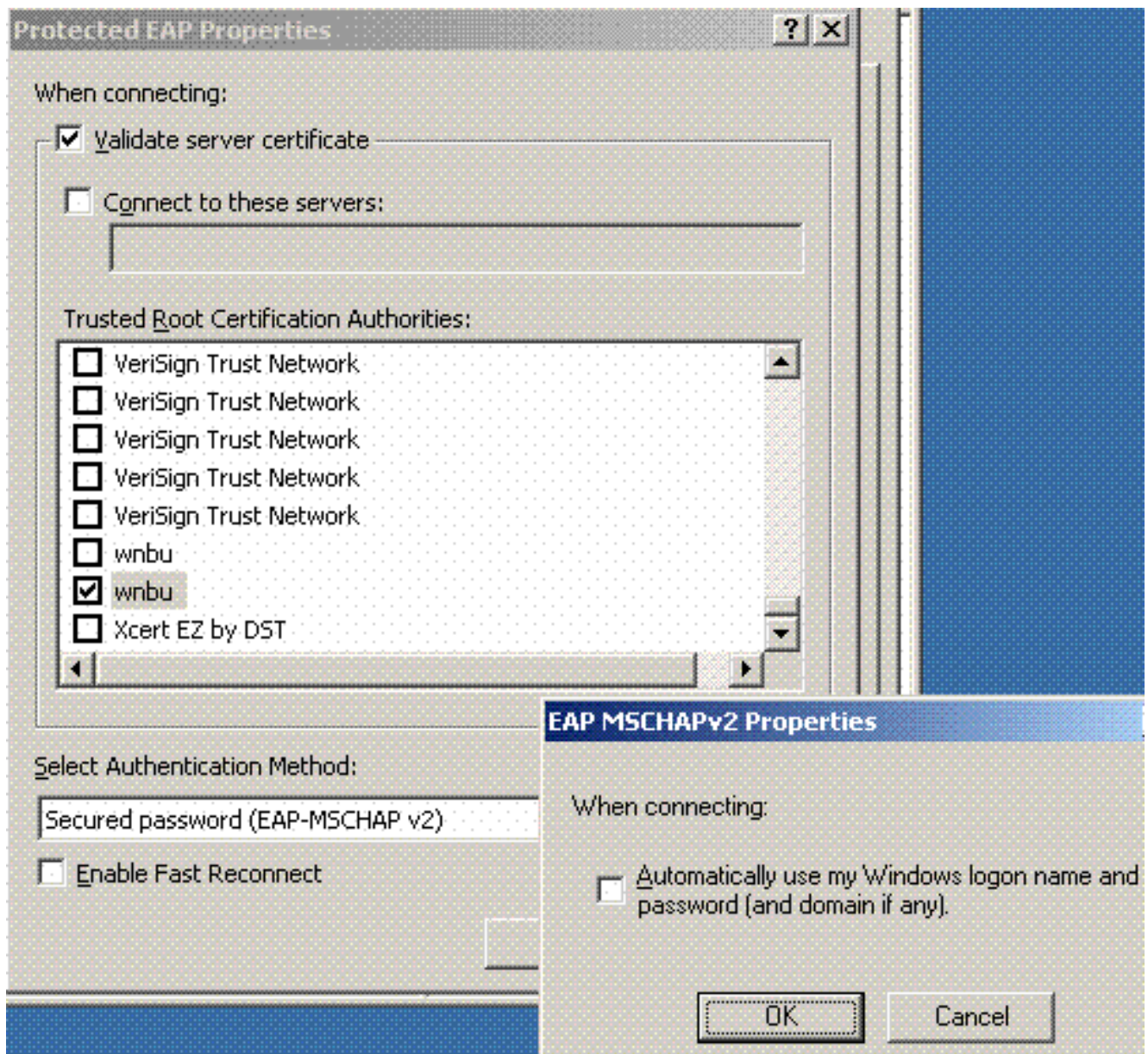
1. 启动默认域安全设置管理器，并且创建无线网络(IEEE 802.11)策略的一个新的安全策略。



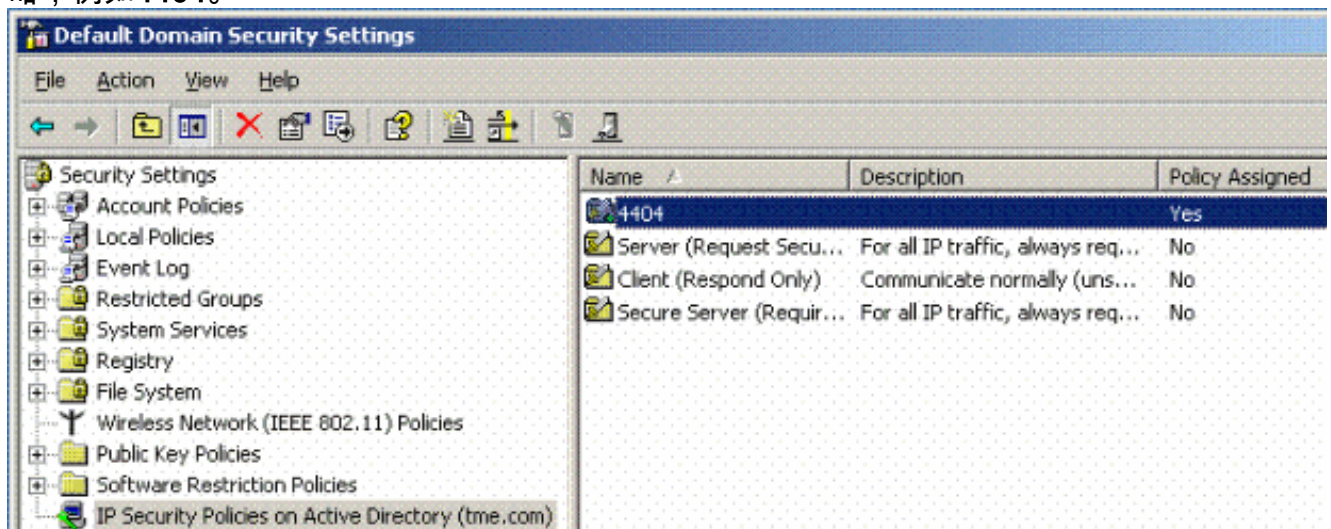
2. 打开WLAN网络策略属性，并且点击**首选网络**。添加一新的首选WLAN并且键入您的WLAN SSID的名字，例如。双击该新的首选网络，并且点击**IEEE 802.1x**选项。选择PEAP作为EAP类型



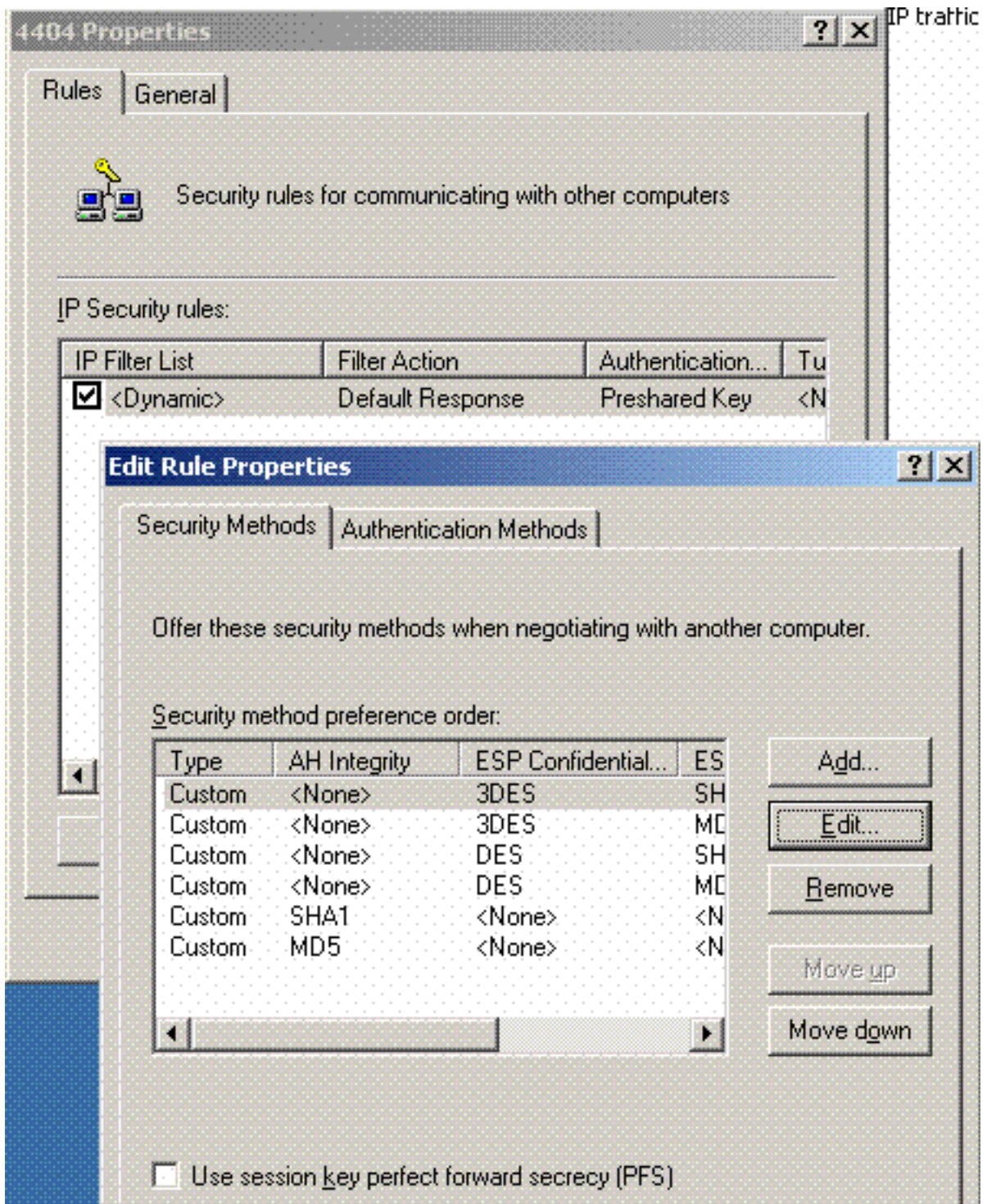
3. 点击**PEAP设置**，检查**验证服务器证明**，并且选择可信的根Cert安装在认证机关上。为了便于测试，请非选定自动地的MS CHAP v2机箱使用我的Windows登录和密码。



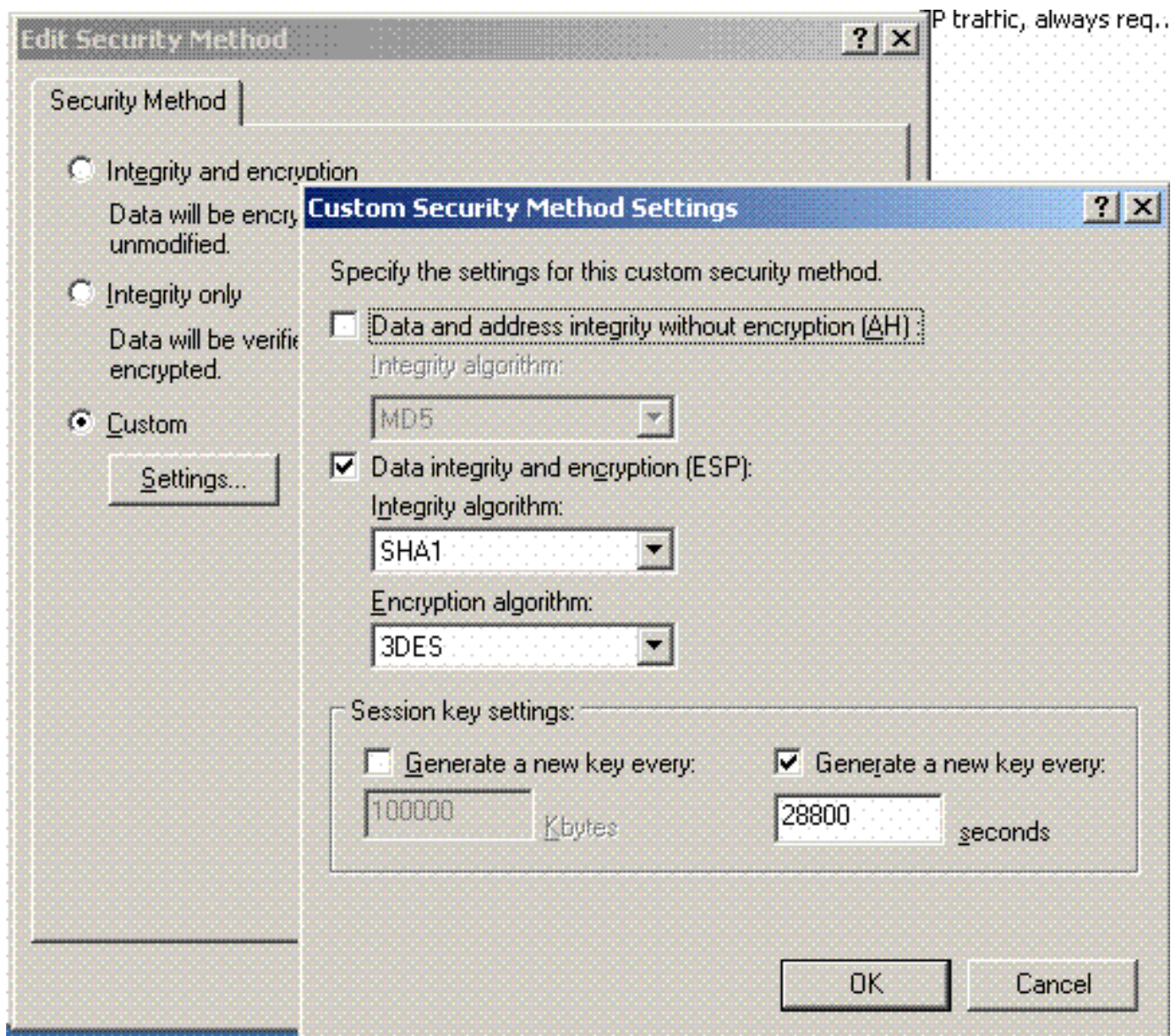
4. 在Windows 2003默认域安全设置管理器窗口，请创建在激活目录策略的另一个新的IP安全策略，例如4404。



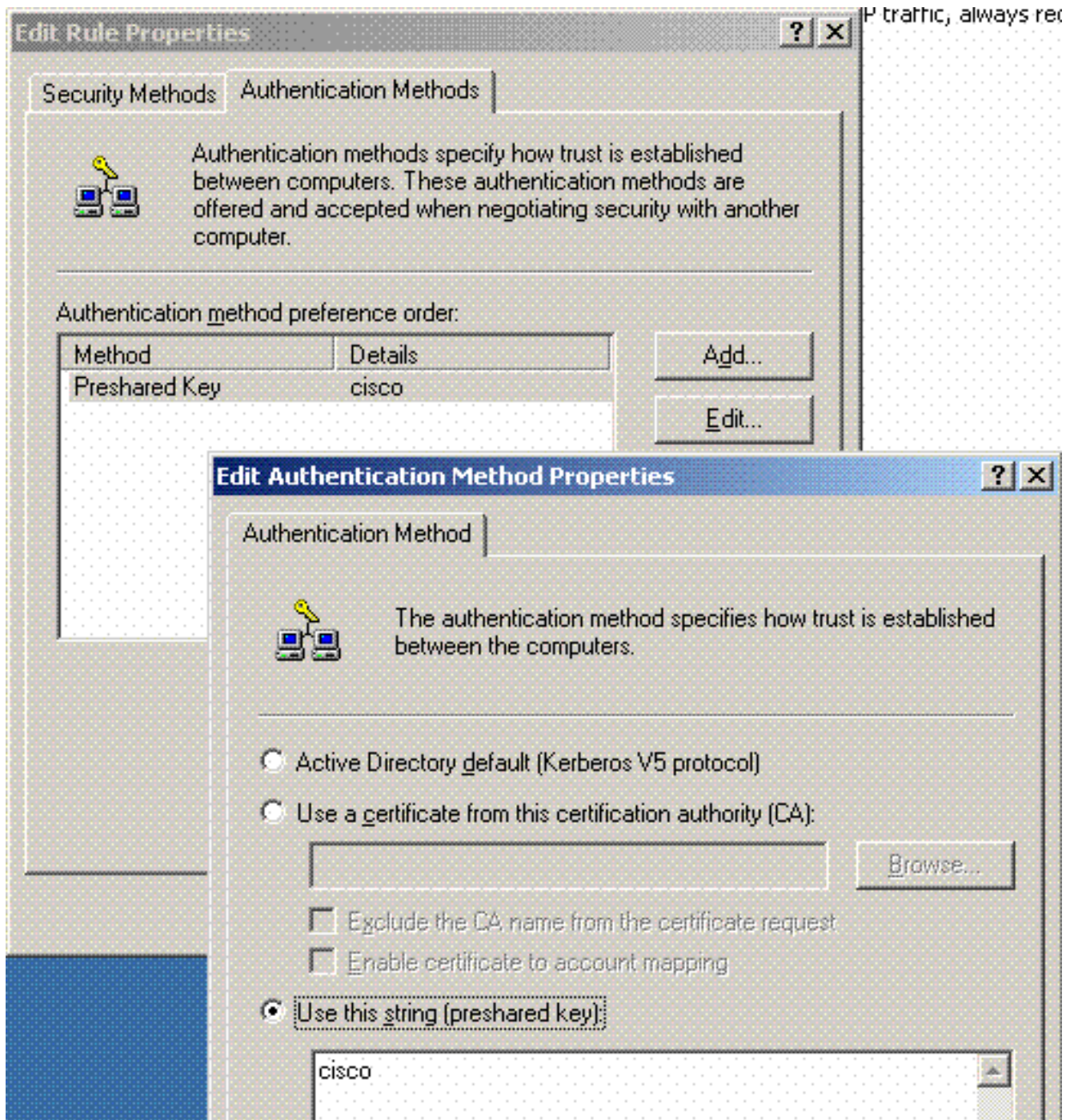
5. 编辑新的4404个策略属性，并且点击规则选项。增加一个新的过滤规则- IP去骨切片列表(动态);过滤器操作(默认回应);认证(PSK);隧道(无)。双击新建立的过滤规则并且选择安全方法



6. 点击编辑安全方法，并且点击自定义Settings单选按钮。选择这些设置。**Note:** 这些设置必须匹配控制器RADIUS IPsec安全设置。



7. 点击**认证方法**选项在编辑规则属性下。输入您在控制器RADIUS配置以前输入的同一个共有的秘密。



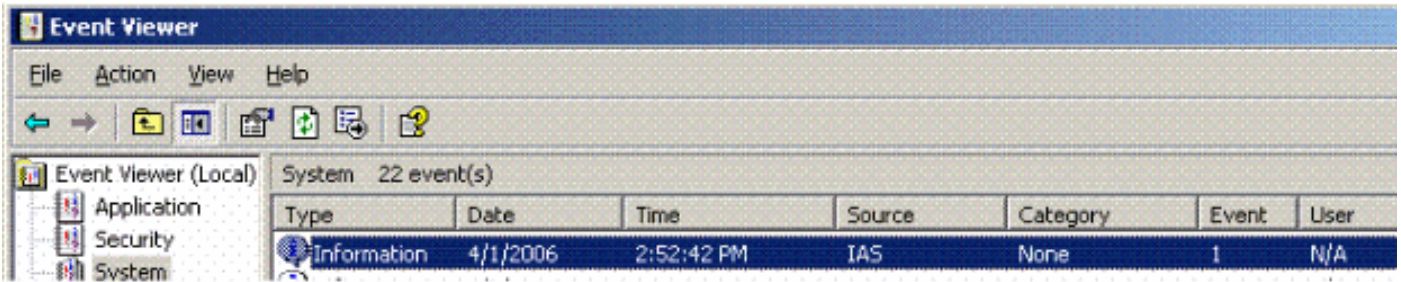
这时，控制器的所有配置，IAS和域安全设置完成。保存所有配置在控制器和WinServer并且重新启动所有机器。在使用测试的WLAN客户端，请安装根cert并且为WPA2/PEAP配置。在根cert在客户端上后安装，请重新启动客户端机器。在所有机器重新启动后，请联络客户端到WLAN并且捕获这些日志事件。

**Note:** 要求客户端连接为了设置控制器和WinServer RADIUS之间的IPSec连接。

## Windows 2003个系统日志事件

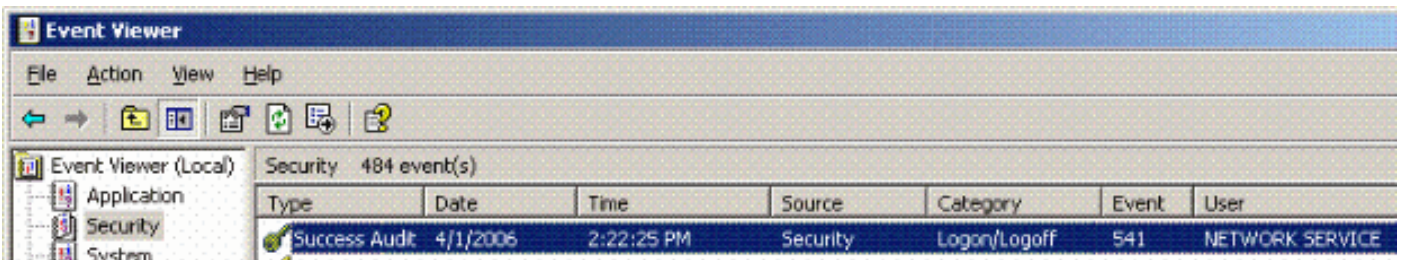
为WPA2/PEAP配置的成功WLAN客户端连接有IPSec RADIUS功能在WinServer生成此系统事件：

192.168.30.105 = WinServer  
192.168.30.2 = WLAN Controller



User TME0\Administrator was granted access.  
 Fully-Qualified-User-Name = tme.com/Users/Administrator  
 NAS-IP-Address = 192.168.30.2  
 NAS-Identifier = Cisco\_40:5f:23  
 Client-Friendly-Name = 4404  
 Client-IP-Address = 192.168.30.2  
 Calling-Station-Identifier = 00-40-96-A6-D4-6D  
 NAS-Port-Type = Wireless - IEEE 802.11  
 NAS-Port = 1  
 Proxy-Policy-Name = Use Windows authentication for all users  
 Authentication-Provider = Windows  
 Authentication-Server = <undetermined>  
 Policy-Name = 4404  
 Authentication-Type = PEAP  
 EAP-Type = Secured password (EAP-MSCHAP v2)

一个成功的控制器<> RADIUS IPsec连接在WinServer日志生成此安全事件：



IKE security association established.  
 Mode: Data Protection Mode (Quick Mode)  
 Peer Identity: Preshared key ID.  
 Peer IP Address: 192.168.30.2  
 Filter:  
 Source IP Address 192.168.30.105  
 Source IP Address Mask 255.255.255.255  
 Destination IP Address 192.168.30.2  
 Destination IP Address Mask 255.255.255.255  
 Protocol 17  
 Source Port 1812  
 Destination Port 0  
 IKE Local Addr 192.168.30.105  
 IKE Peer Addr 192.168.30.2  
 IKE Source Port 500  
 IKE Destination Port 500  
 Peer Private Addr  
 Parameters:  
 ESP Algorithm Triple DES CBC  
 HMAC Algorithm SHA  
 AH Algorithm None  
 Encapsulation Transport Mode  
 InboundSpi 3531784413 (0xd282c0dd)



```
OutBoundSpi 4047139137 (0xf13a7141)
Lifetime (sec) 28800
Lifetime (kb) 100000
QM delta time (sec) 0
Total delta time (sec) 0
```

## 无线局域网控制器RADIUS IPsec成功调试示例

您能使用在控制器的debug命令调试pm ikemsg enable (event)为了验证此配置。下面是一个示例。

```
(Cisco Controller) >debug pm ikemsg enable
(Cisco Controller) >***** ERR: Connection timed out or error, calling callback
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x0000000000000000
SA: doi=1 situation=0x1
Proposal 0, proto=ISAKMP, # transforms=1, SPI[0]
Transform#=0 TransformId=1, # SA Attributes = 6
EncrAlgo = 3DES-CBC
HashAlgo = SHA
AuthMethod = Pre-shared Key
GroupDescr =2
LifeType = secs
LifeDuration =28800
VID: vendor id[16] = 0x8f9cc94e 01248ecd f147594c 284b213b
VID: vendor id[16] = 0x27bab5dc 01ea0760 ea4e3190 ac27c0d0
VID: vendor id[16] = 0x6105c422 e76847e4 3f968480 1292aecd
VID: vendor id[16] = 0x4485152d 18b6bbcd 0be8a846 9579ddcc
VID: vendor id[16] = 0xcd604643 35df21f8 7cfdb2fc 68b6a448
VID: vendor id[16] = 0x90cb8091 3ebb696e 086381b5 ec427b1f
VID: vendor id[16] = 0x7d9419a6 5310ca6f 2c179d92 15529d56
VID: vendor id[16] = 0x12f5f28c 457168a9 702d9fe2 74cc0100
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
SA: doi=1 situation=0x1
Proposal 1, proto=ISAKMP, # transforms=1 SPI[0]
Transform payload: transf#=1 transfId=1, # SA Attributes = 6
EncrAlgo= 3DES-CBC
HashAlgo= SHA
GroupDescr=2
AuthMethod= Pre-shared Key
LifeType= secs
LifeDuration=28800
VENDOR ID: data[20] = 0x1e2b5169 05991c7d 7c96fcbf b587e461 00000004
VENDOR ID: data[16] = 0x4048b7d5 6ebce885 25e7de7f 00d6c2d3
VENDOR ID: data[16] = 0x90cb8091 3ebb696e 086381b5 ec427b1f
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
KE: ke[128] = 0x9644af13 b4275866 478d294f d5408dc5 e243fc58...
NONCE: nonce [16] = 0xede8dc12 c11be7a7 aa0640dd 4cd24657
PRV[payloadId=130]: data[20] = 0x1628f4af 61333b10 13390df8 85a0c0c2 93db6
c67
PRV[payloadId=130]: data[20] = 0xcf0bbd1c 55076966 94bccf4f e05e1533 191b1
378
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
KE: ke[128] = 0x9f0420e5 b13adb04 a481e91c 8d1c4267 91c8b486...
NONCE: nonce[20] = 0x011a4520 04e31ba1 6089d2d6 347549c3 260ad104
PRV payloadId=130: data[20] = 0xcf0bbd1c 55076966 94bccf4f e05e1533 191b13
78
PRV payloadId=130: data[20] = 0x1628f4af 61333b10 13390df8 85a0c0c2 93db6c
67
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
```

```
cookie=0x064bdcaf50d5f555
ID: packet[8] = 0x01000000 c0a81e69
HASH: hash[20] = 0x04814190 5d87caa1 221928de 820d9f6e ac2ef809
NOTIFY: doi=1 proto=ISAKMP type=INITIAL_CONTACT, spi[0]
NOTIFY: data[0]
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
cookie=0x064bdcaf50d5f555
ID: packet[8] = 0x01000000 c0a81e69
HASH: hash[20] = 0x3b26e590 66651f13 2a86f62d 1bd1e71 064b43f6
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
cookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0x00000000 00000000 00000000 00000000 00000000
SA: doi=1 situation=0x1
Proposal 1, proto=ESP, # transforms=1, SPI[4] = 0xbb243261
Transform#=1 TransformId=3, # SA Attributes = 4
AuthAlgo = HMAC-SHA
LifeType = secs
LifeDuration =28800
EncapMode = Transport
NONCE: nonce [16] = 0x48a874dd 02d91720 29463981 209959bd
ID: packet[8] = 0x01110000 c0a81e02
ID: packet[8] = 0x01110714 c0a81e69
RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
cookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0x2228d010 84c6014e dd04ee05 4d15239a 32a9e2ba
SA: doi=1 situation=0x1
Proposal 1, proto=ESP, # transforms=1 SPI[4] = 0x7d117296
Transform payload: transf#=1 transfId=3, # SA Attributes = 4
LifeType= secs
LifeDuration=28800
EncapMode= Transport
AuthAlgo= HMAC-SHA
NONCE: nonce[20] = 0x5c4600e4 5938cbb0 760d47f4 024a59dd 63d7ddce
ID: packet[8] = 0x01110000 c0a81e02
ID: packet[8] = 0x01110714 c0a81e69
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
cookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0x0e81093e bc26ebf3 d367297c d9f7c000 28a3662d
RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
cookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0xcb862635 2b30202f 83fc5d7a 2264619d b09faed2
NOTIFY: doi=1 proto=ESP type=CONNECTED, spi[4] = 0xbb243261
data[8] = 0x434f4e4e 45435431
```

## [Ethreal捕获](#)

这是示例Ethreal捕获。

```
192.168.30.105 = WinServer
192.168.30.2 = WLAN Controller
192.168.30.107 = Authenticated WLAN client
No. Time Source Destination Protocol Info
1 0.000000 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf.
   Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
2 1.564706 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
3 1.591426 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
4 1.615600 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
5 1.617243 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
6 1.625168 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
7 1.627006 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
8 1.638414 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
```

```
9 1.639673 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
10 1.658440 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
11 1.662462 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
12 1.673782 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
13 1.674631 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
14 1.687892 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
15 1.708082 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
16 1.743648 192.168.30.107 Broadcast LLC U, func=XID;
    DSAP NULL LSAP Individual, SSAP NULL LSAP Command
17 2.000073 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf.
    Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
18 4.000266 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf.
    Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
19 5.062531 Cisco_42:d3:03 Cisco_42:d3:03 LOOP Reply
20 5.192104 192.168.30.101 192.168.30.255 NBNS Name query NB PRINT.CISCO.COM<00>
21 5.942171 192.168.30.101 192.168.30.255 NBNS Name query NB PRINT.CISCO.COM<00>
22 6.000242 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf.
    Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
23 6.562944 192.168.30.2 192.168.30.105 ARP Who has 192.168.30.105? Tell 192.168.30.2
24 6.562982 192.168.30.105 192.168.30.2 ARP 192.168.30.105 is at 00:40:63:e3:19:c9
25 6.596937 192.168.30.107 Broadcast ARP 192.168.30.107 is at 00:13:ce:67:ae:d2
```

## [Related Information](#)

- [Cisco 无线局域网控制器配置指南 5.2 版](#)
- [Technical Support & Documentation - Cisco Systems](#)