Configurazione della protezione IPSec RADIUS per WLC e Microsoft Windows 2003 IAS Server

Sommario

Introduzione

In questa guida viene illustrato come configurare la funzionalità IPSec RADIUS supportata da WCS e dai seguenti controller WLAN:

- Serie 4400
- WiSM
- 3.750 G

La funzione IPSec RADIUS del controller si trova nella GUI del controller nella sezione **Sicurezza > AAA > Server di autenticazione RADIUS**. Questa funzionalità consente di crittografare tutte le comunicazioni RADIUS tra i controller e i server RADIUS (IAS) con IPSec.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze su LWAPP
- Informazioni sull'autenticazione RADIUS e su IPSec
- Informazioni sulla configurazione dei servizi nel sistema operativo Windows 2003 Server

Componenti usati

Per distribuire la funzionalità IPSec RADIUS del controller, è necessario installare e configurare i seguenti componenti di rete e software:

- Controller WLC 4400, WiSM o 3750G. In questo esempio viene usato WLC 4400 con software versione 5.2.178.0
- Lightweight Access Point (LAP). In questo esempio viene utilizzato il LAP serie 1231.
- Switch con DHCP
- Server Microsoft 2003 configurato come controller di dominio installato con Microsoft Certificate Authority e con Microsoft Internet Authentication Service (IAS).
- Microsoft Domain Security
- Cisco 802.11 a/b/g Wireless Client Adapter con ADU versione 3.6 configurato con WPA2/PEAP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione IPSec RADIUS

Questa guida alla configurazione non riguarda l'installazione o la configurazione di Microsoft WinServer, Certificate Authority, Active Directory o client WLAN 802.1x. Questi componenti devono essere installati e configurati prima della distribuzione della funzionalità RADIUS IPSec del controller. Nella parte restante di questa guida viene illustrato come configurare IPSec RADIUS su questi componenti:

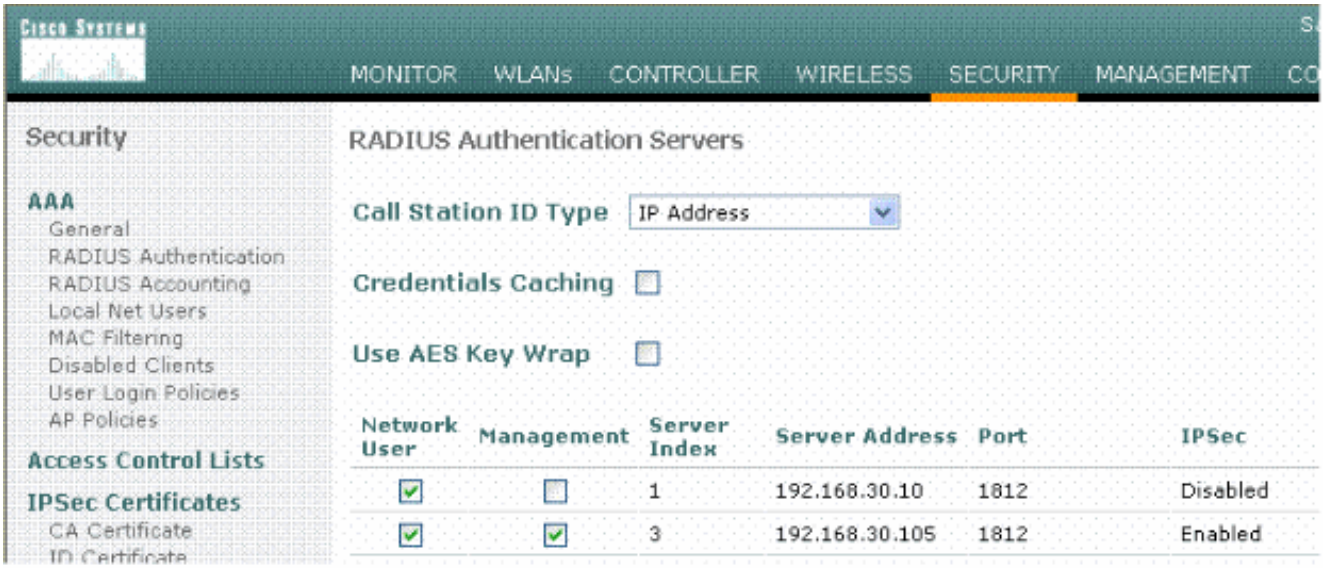
1. Cisco WLAN Controller
2. Windows 2003 IAS
3. Impostazioni protezione dominio di Microsoft Windows

Configurare il WLC

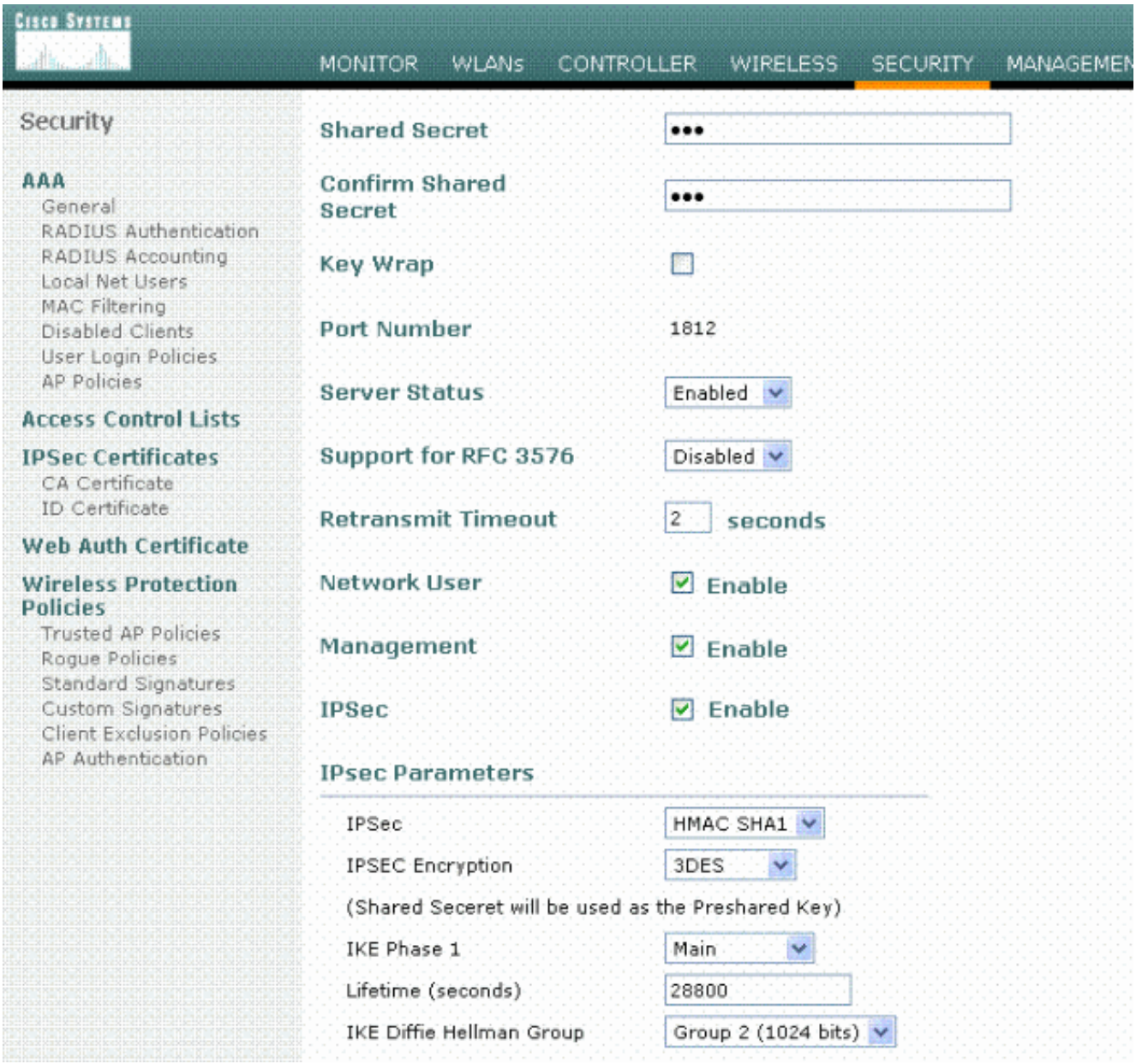
In questa sezione viene spiegato come configurare IPSec sul WLC tramite la GUI.

Dalla GUI del controller, attenersi alla seguente procedura.

1. Selezionare la scheda **Security > AAA > RADIUS Authentication** (Sicurezza > AAA > Autenticazione RADIUS) nella GUI del controller, quindi aggiungere un nuovo server RADIUS.



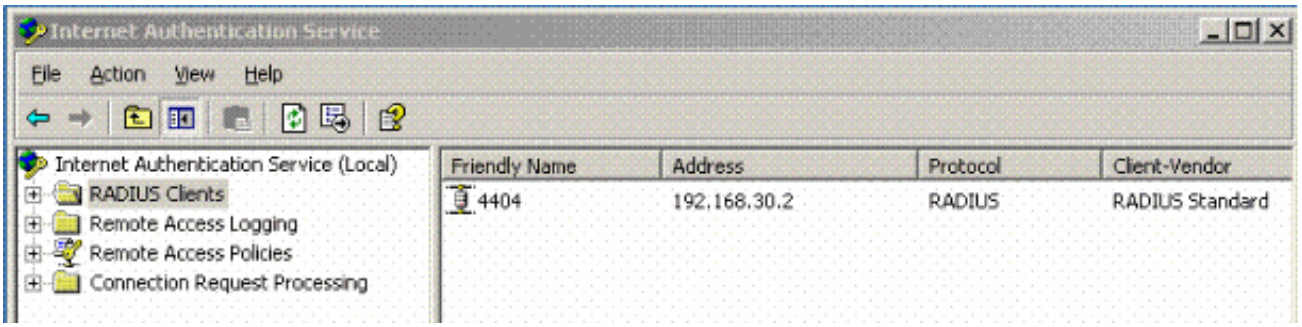
2. Configurare l'indirizzo IP, la porta 1812 e un segreto condiviso del nuovo server RADIUS. Selezionare la casella di controllo **Attiva IPSec**, configurare i parametri IPSec e quindi fare clic su **Applica**.**Nota:** il segreto condiviso viene utilizzato sia per autenticare il server RADIUS che come chiave precondivisa (PSK) per l'autenticazione IPSec.



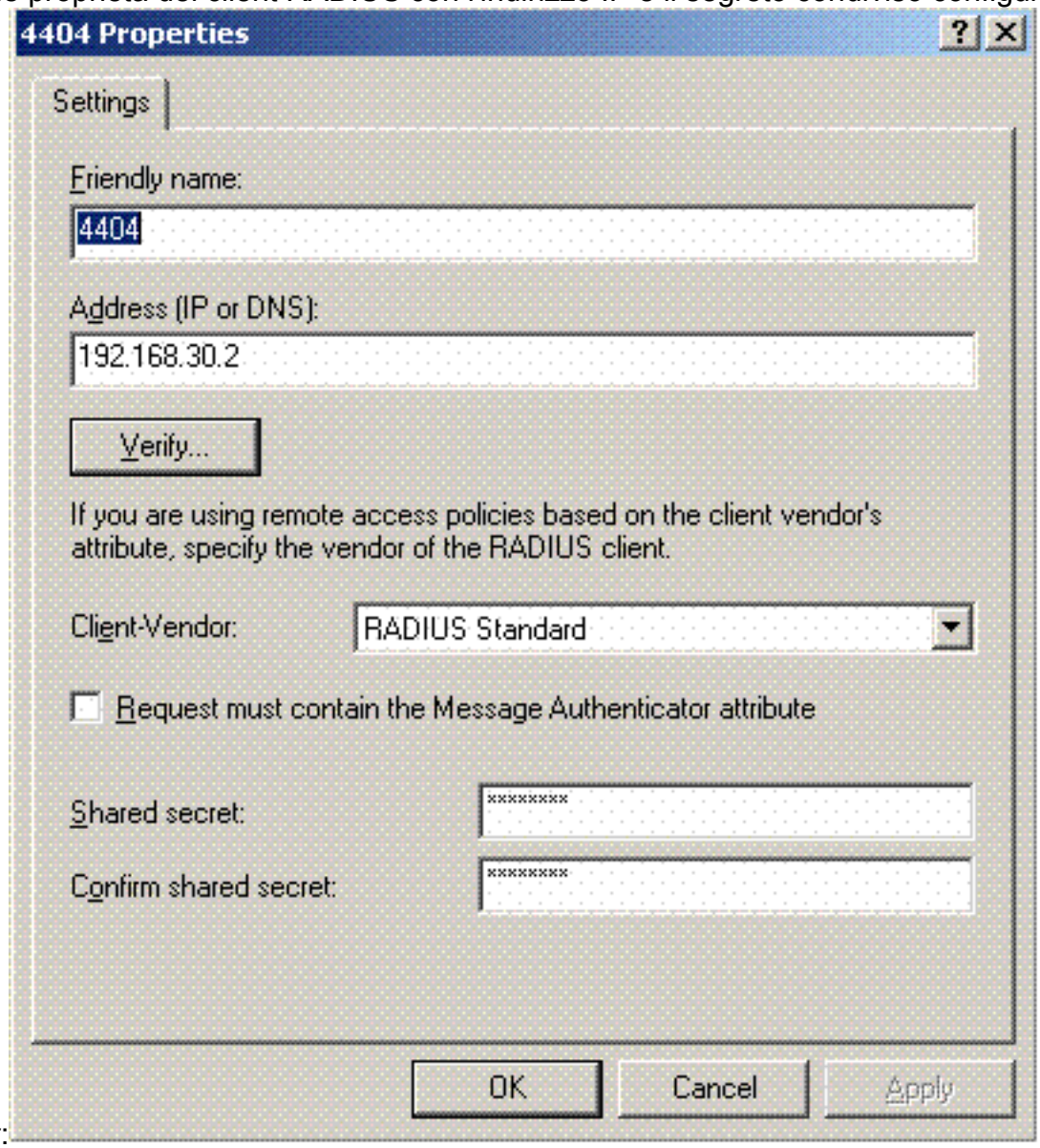
Configurare IAS

Completare i seguenti passaggi sullo IAS:

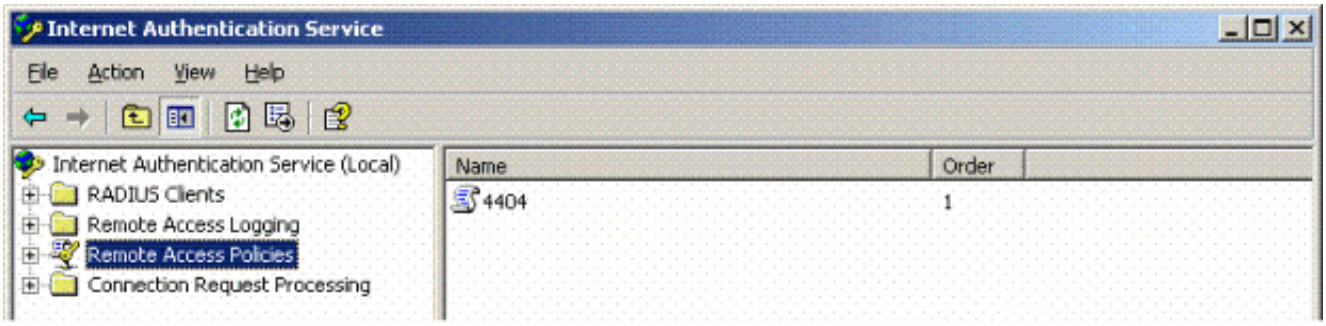
1. Passare al gestore IAS in Win2003 e aggiungere un nuovo client RADIUS.



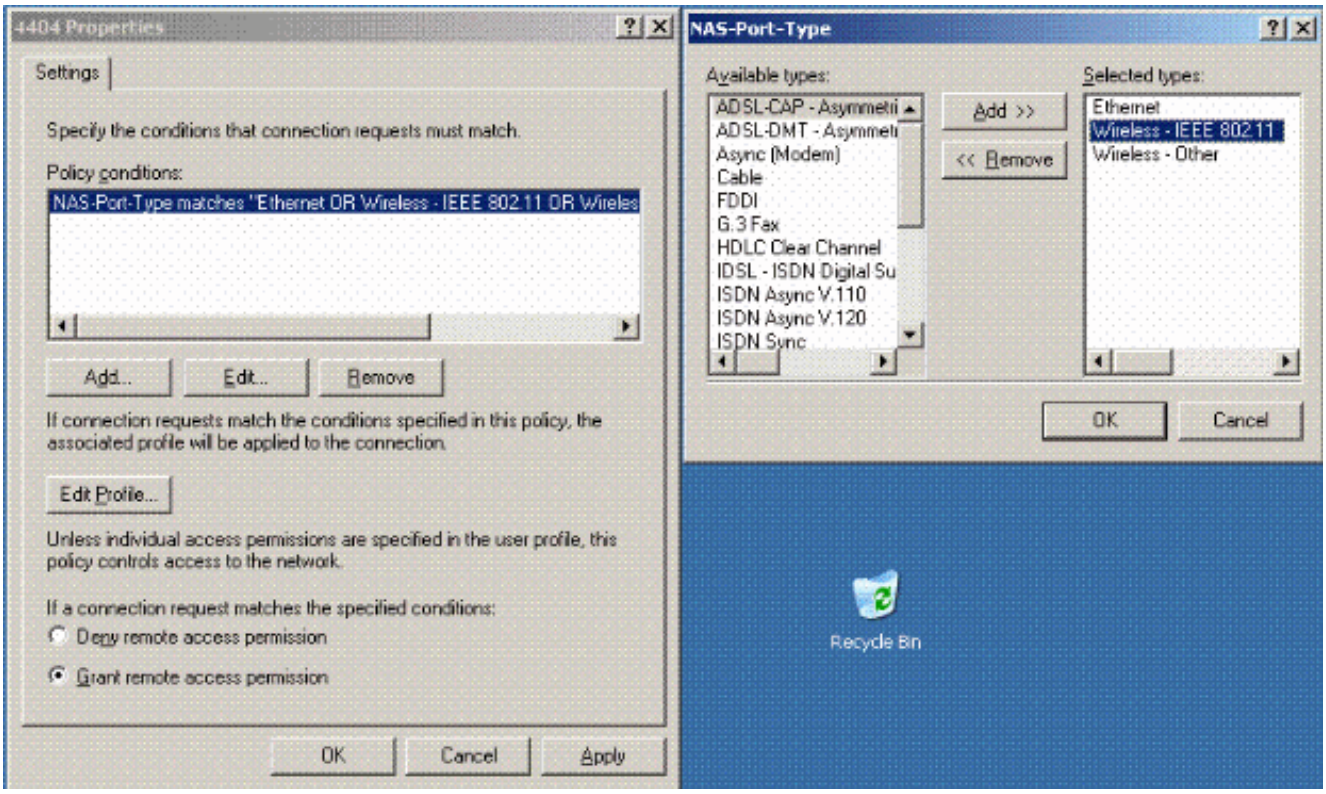
2. Configurare le proprietà del client RADIUS con l'indirizzo IP e il segreto condiviso configurati sul controller:



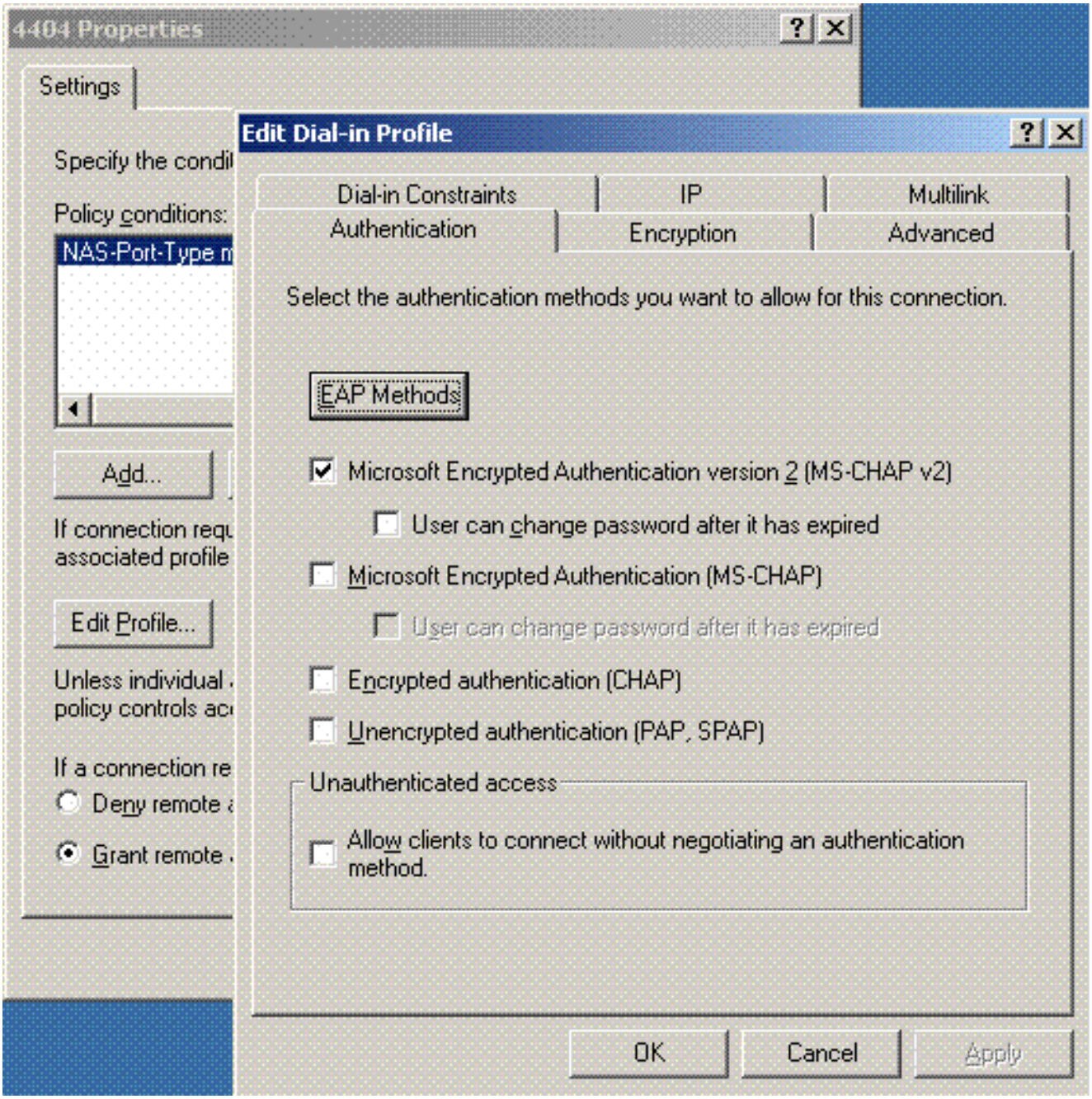
3. Configurare un nuovo criterio di accesso remoto per il controller:



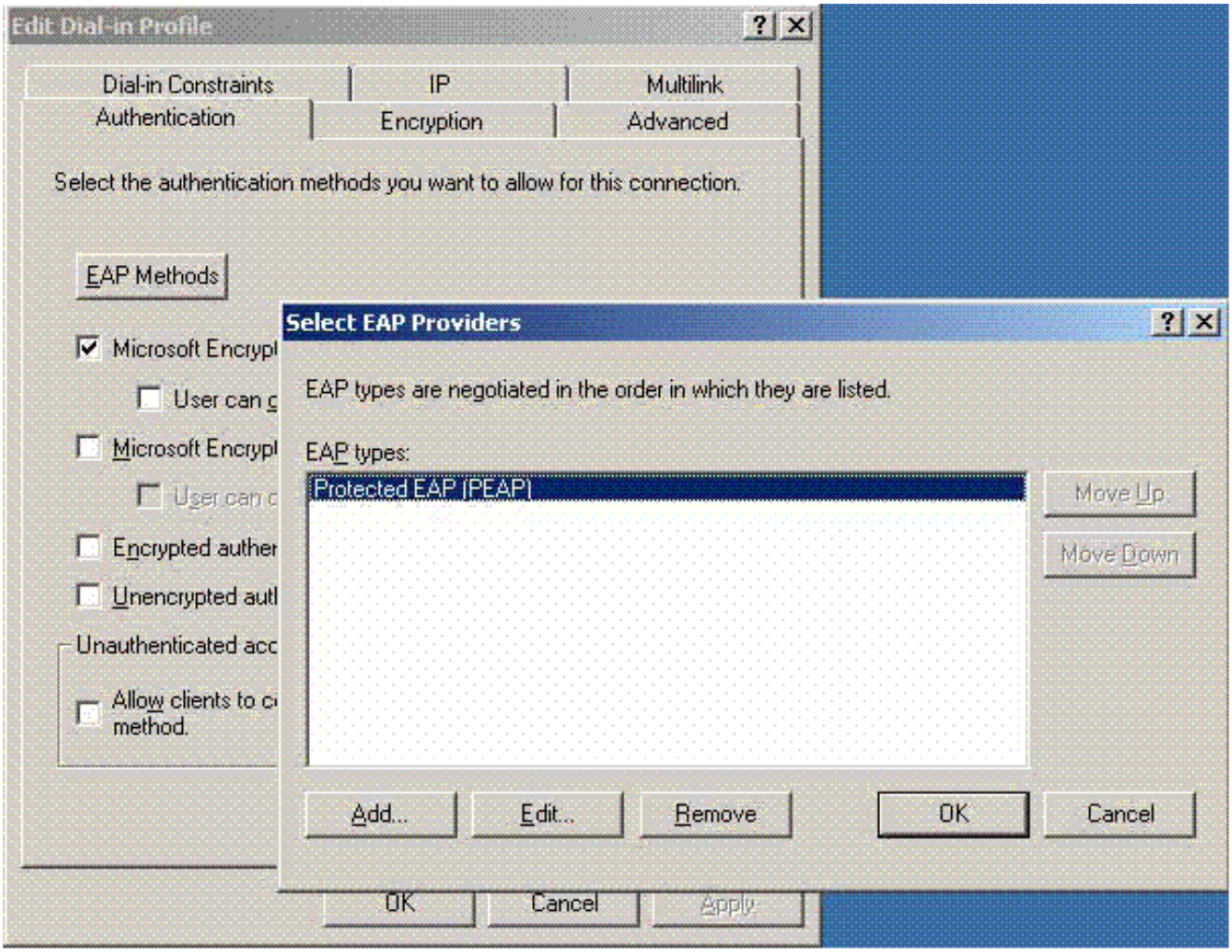
4. Modificare le proprietà del criterio di accesso remoto del controller. Assicurarsi di aggiungere il tipo di porta NAS - Wireless - IEEE 802.11:



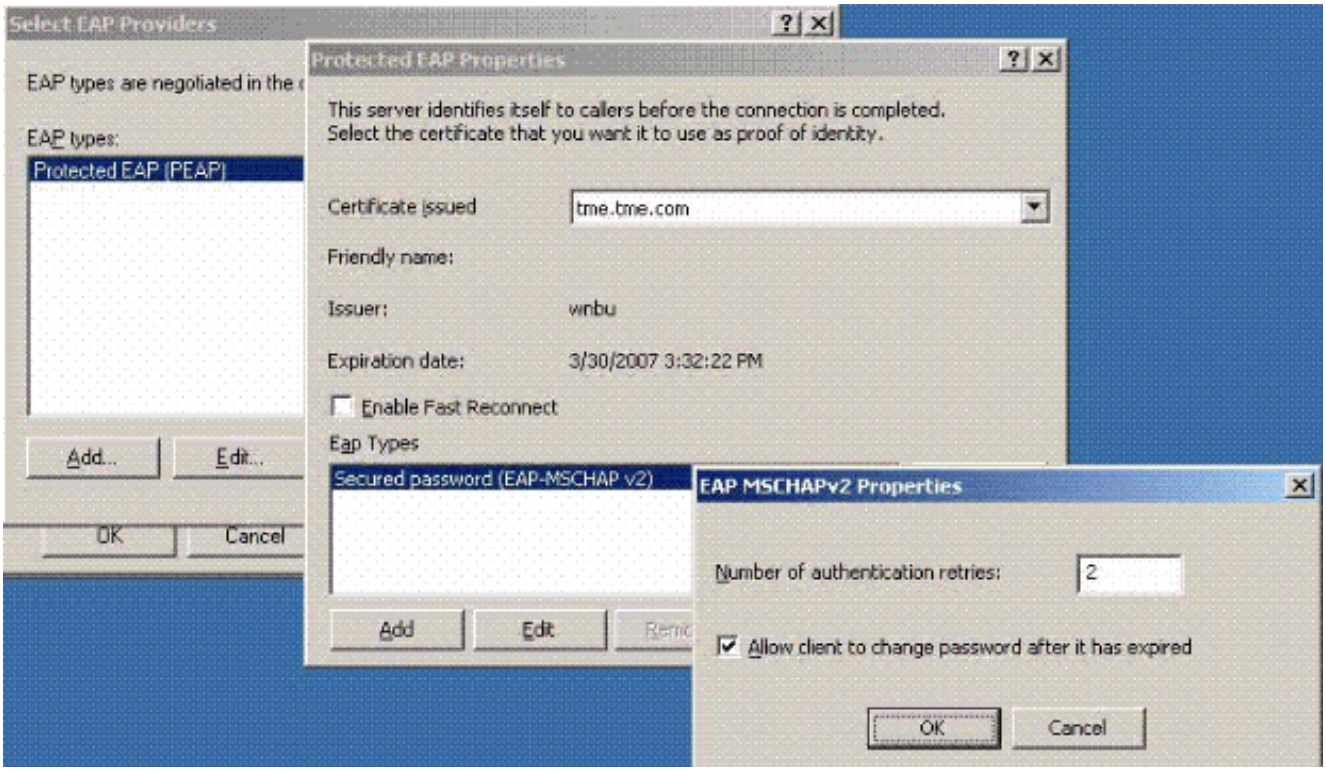
5. Fare clic su **Modifica profilo**, fare clic sulla scheda **Autenticazione** e selezionare MS-CHAP v2 per
Autenticazione:



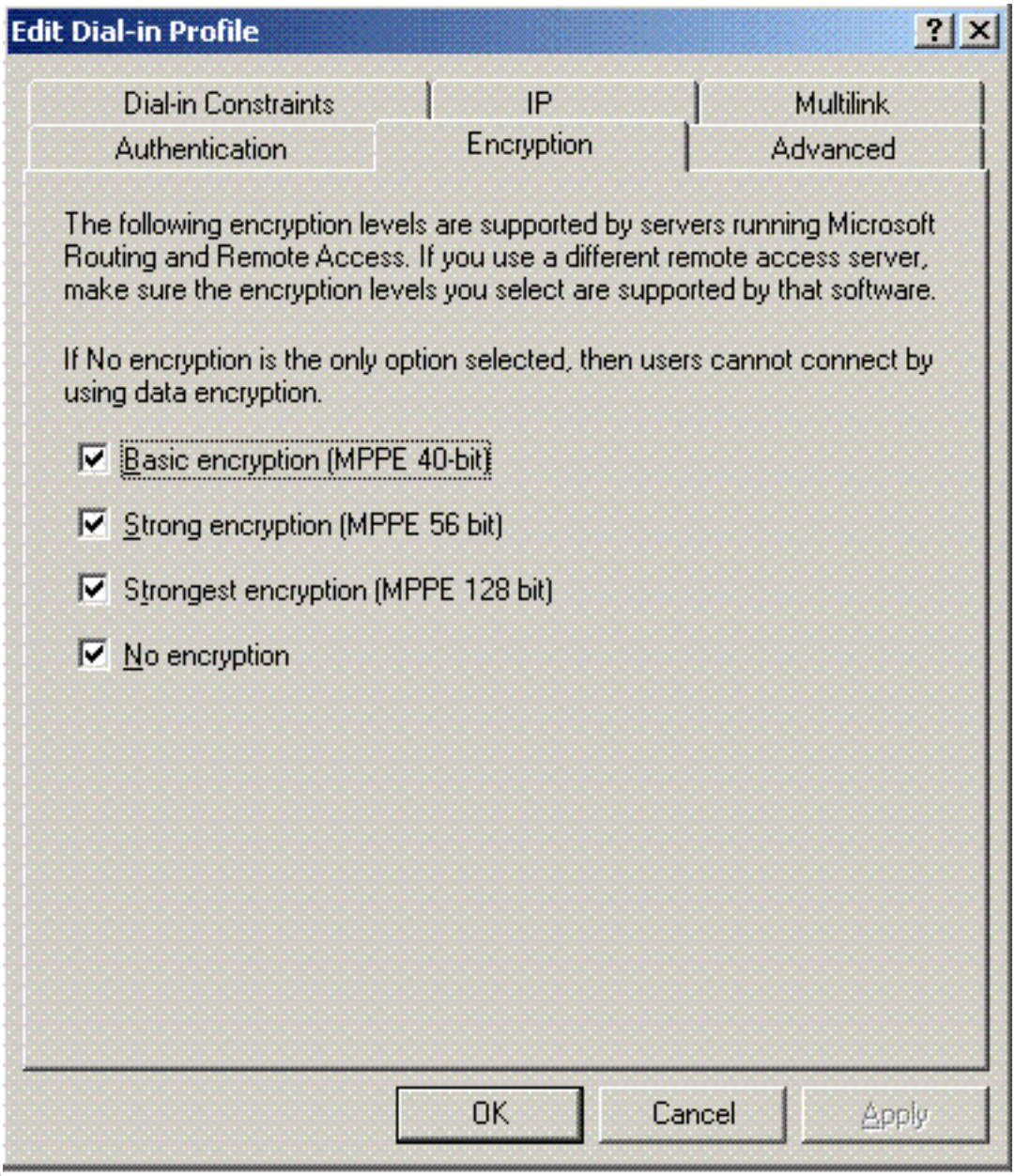
6. Fare clic su **Metodi EAP**, selezionare Provider EAP e aggiungere PEAP come tipo EAP:



7. Fare clic su **Modifica** in Seleziona provider EAP e scegliere dal menu a discesa il server associato agli account utente e alla CA di Active Directory (ad esempio, tme.tme.com). Aggiungere il tipo EAP MSCHAP v2:

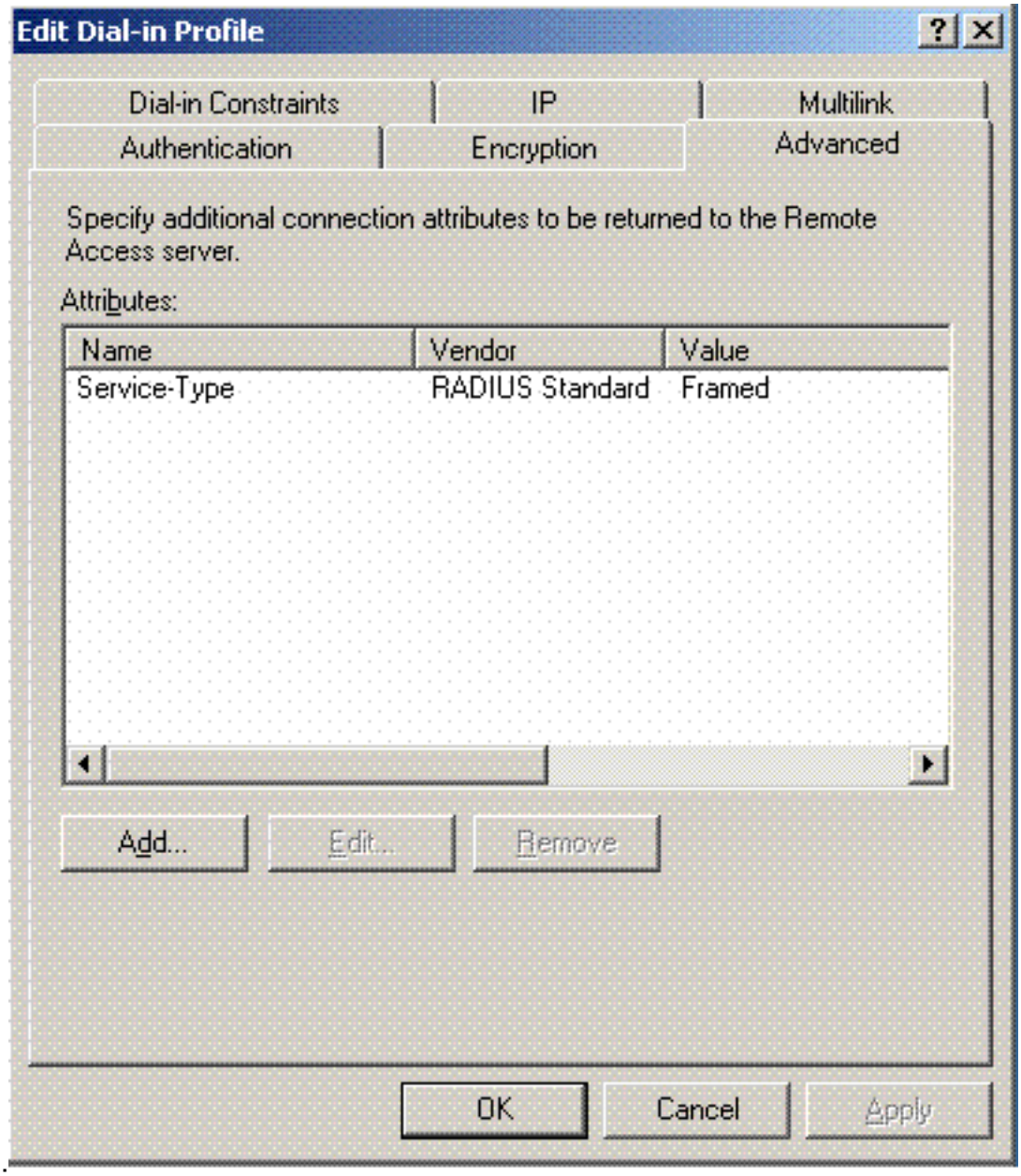


8. Fare clic sulla scheda **Crittografia** e verificare che tutti i tipi di crittografia siano accessibili in



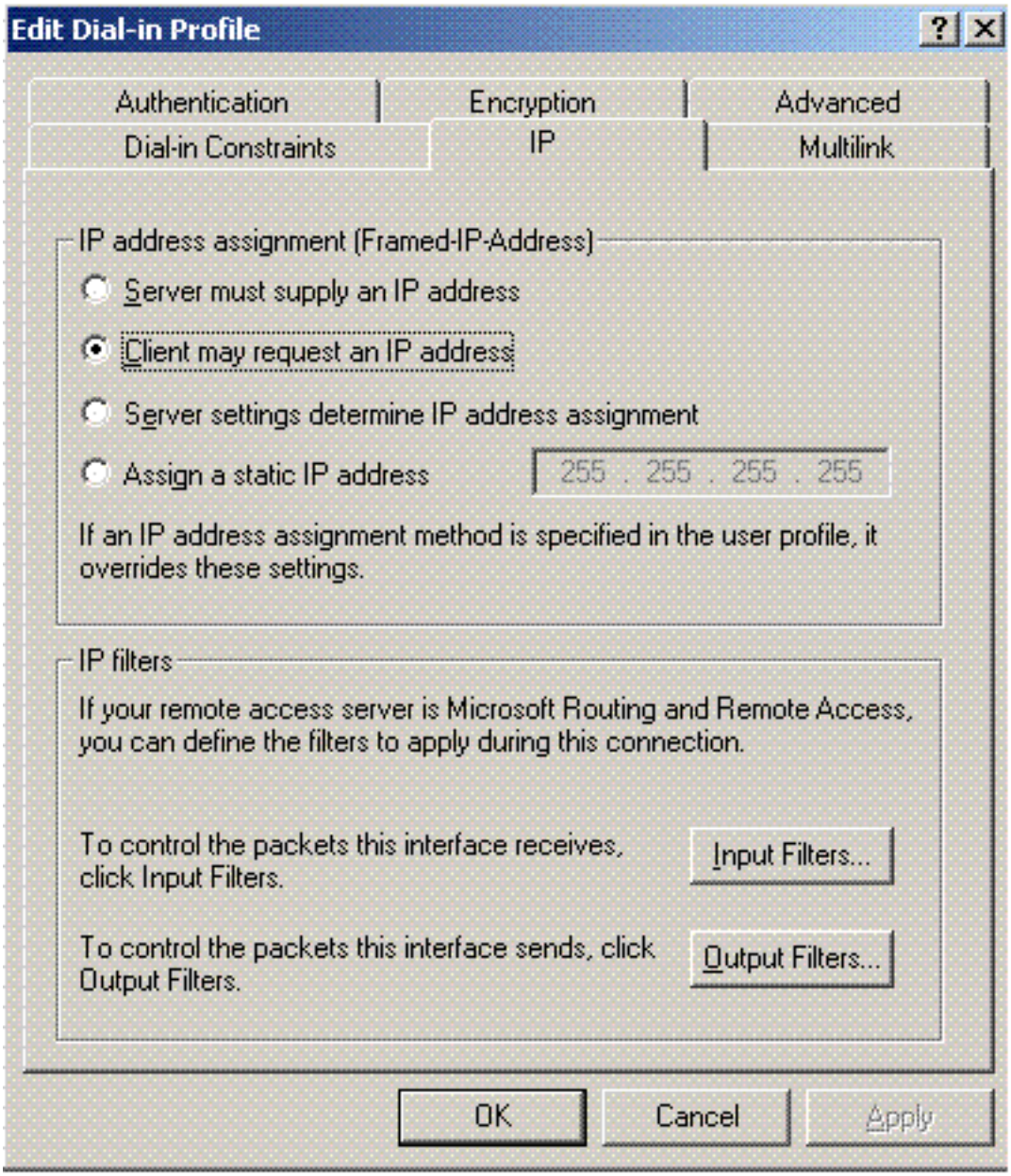
remoto:

9. Fare clic sulla scheda **Advanced** (Avanzate), quindi aggiungere RADIUS Standard/Framed come Service-Type (Tipo di



servizio):

10. Fare clic sulla scheda **IP** e selezionare **Client may request an IP address** (Il client potrebbe richiedere un indirizzo IP). Ciò presuppone che il protocollo DHCP sia abilitato su uno switch o su

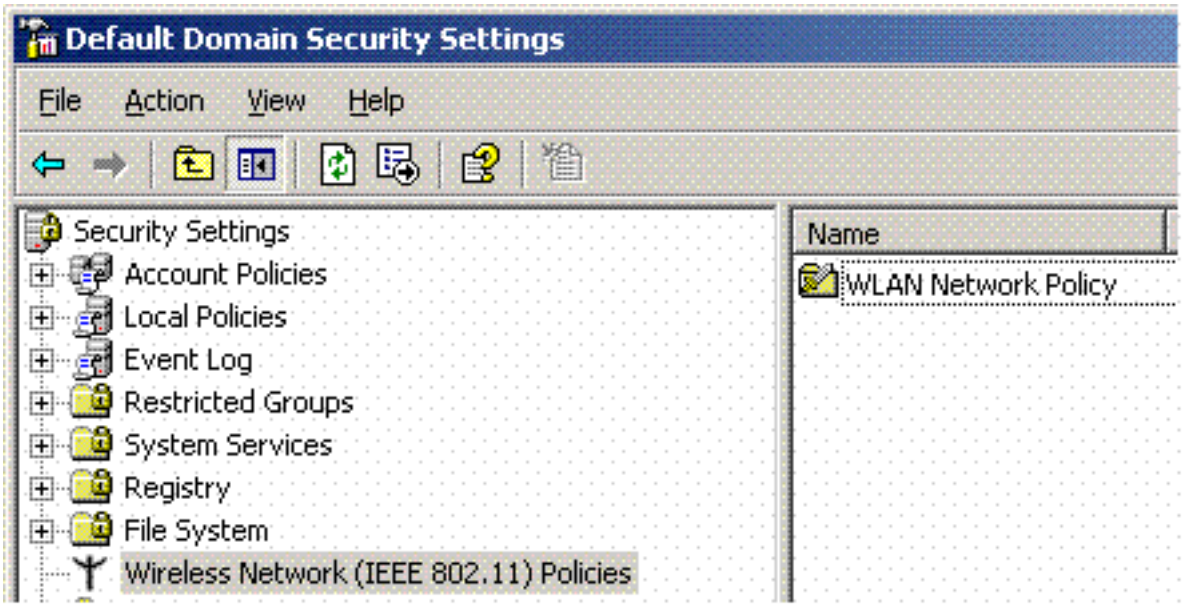


WinServer.

Impostazioni protezione dominio di Microsoft Windows 2003

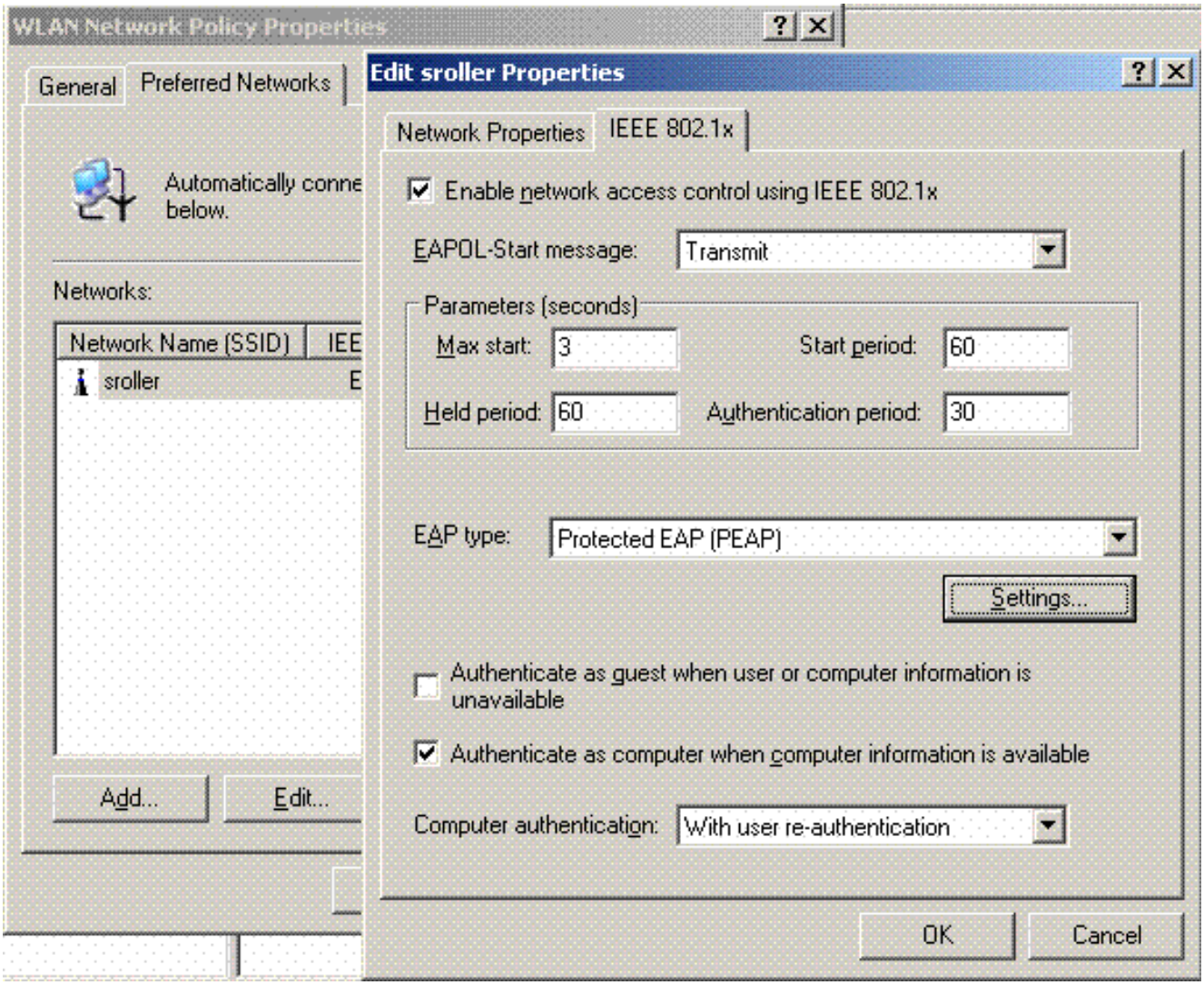
Completare questa procedura per configurare le impostazioni di protezione del dominio di Windows 2003:

1. Avviare lo strumento di gestione delle impostazioni predefinite di protezione del dominio e creare un nuovo criterio di protezione per i criteri di rete wireless (IEEE



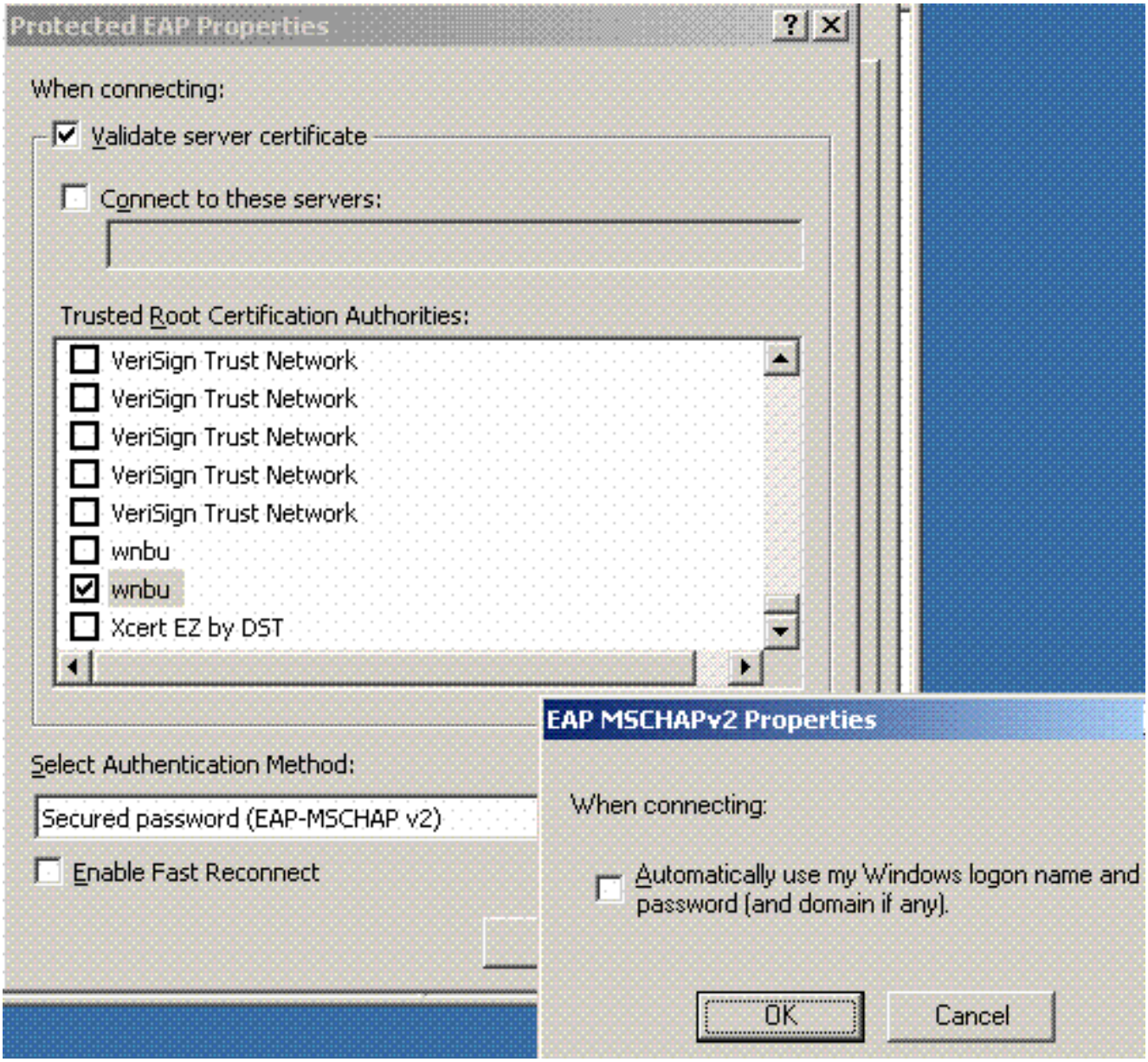
802.11).

2. Aprire Proprietà criteri di rete WLAN e fare clic su **Reti preferite**. Aggiungere una nuova WLAN preferita e digitare il nome dell'SSID della WLAN, ad esempio `Wireless`. Fare doppio clic sulla nuova rete preferita e fare clic sulla scheda **IEEE 802.1x**. Scegliere PEAP come tipo EAP:

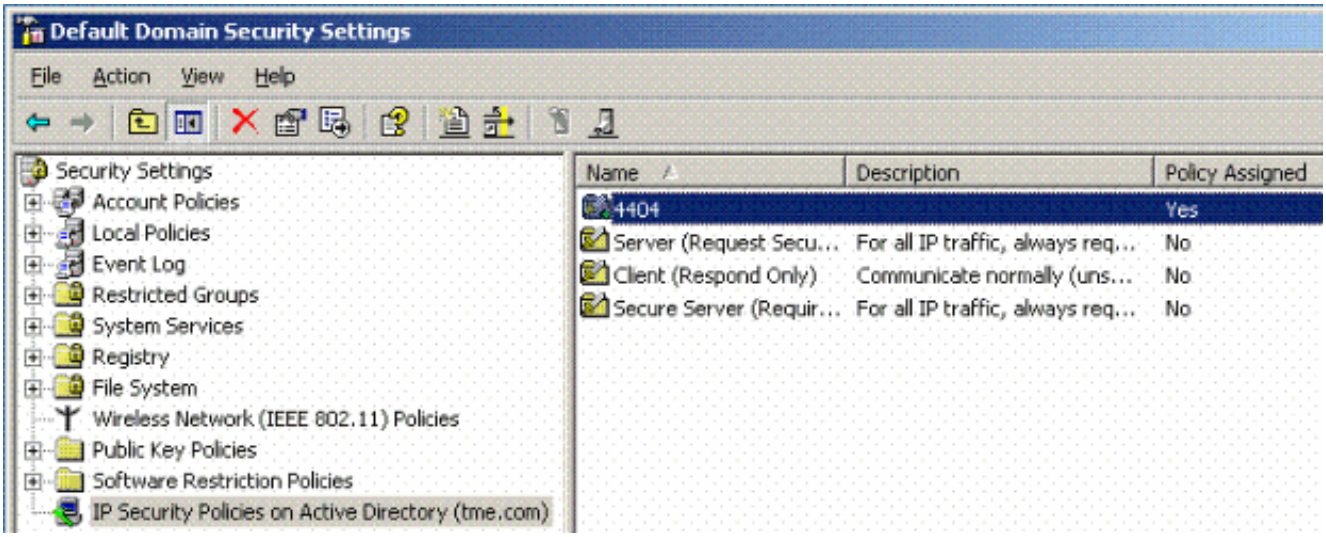


3. Fare clic su **PEAP Settings**, selezionare **Validate server certificate** (Convalida certificato server), quindi selezionare il certificato radice attendibile installato in Certificate Authority (Autorità di certificazione). A scopo di prova, deselezionare la casella MS CHAP v2 per Usa automaticamente il mio account di accesso e la mia password di

Windows.

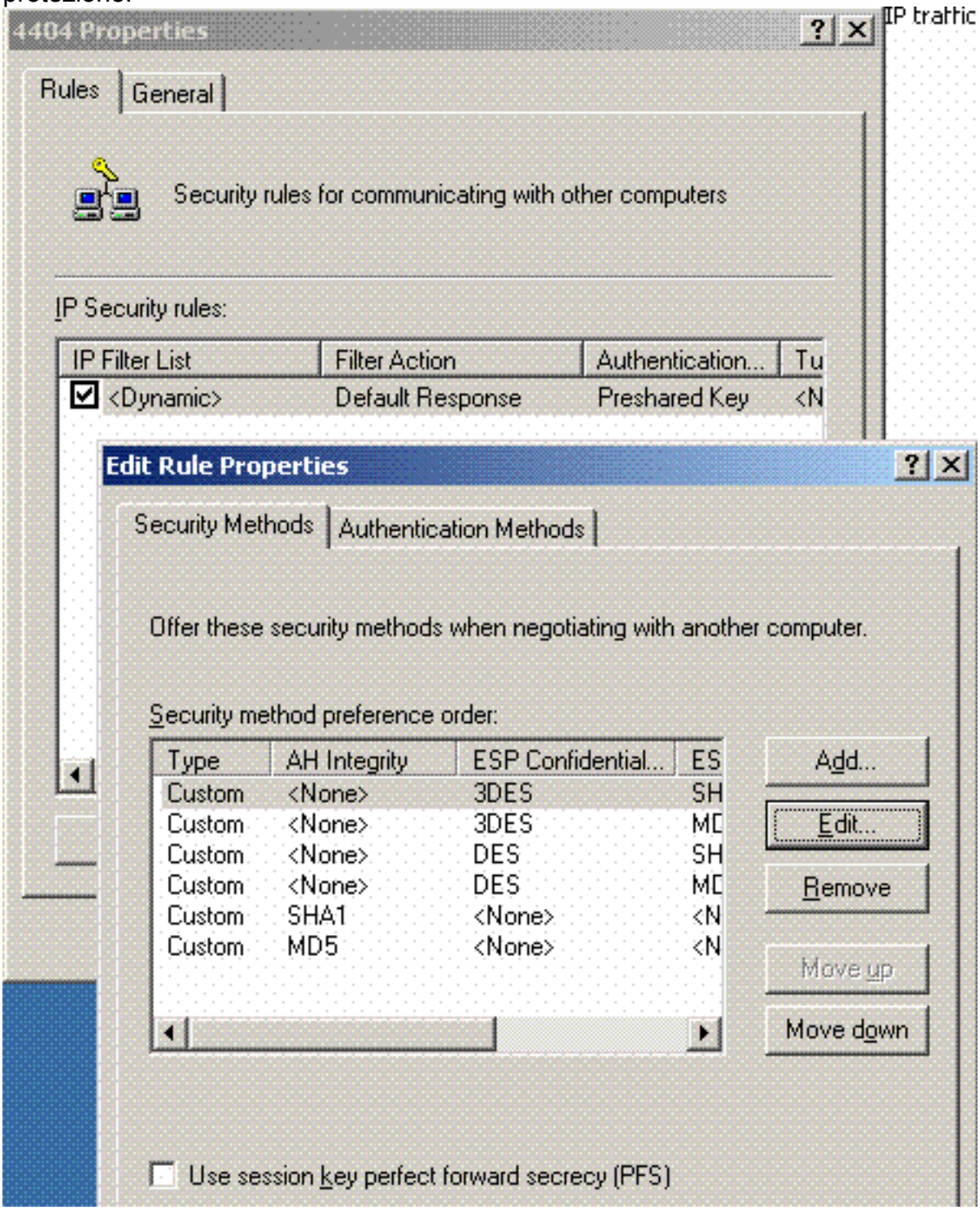


4. Nella finestra Gestione impostazioni di protezione del dominio predefinito di Windows 2003 creare un altro nuovo criterio di protezione IP per i criteri di Active Directory, ad esempio **4404**.

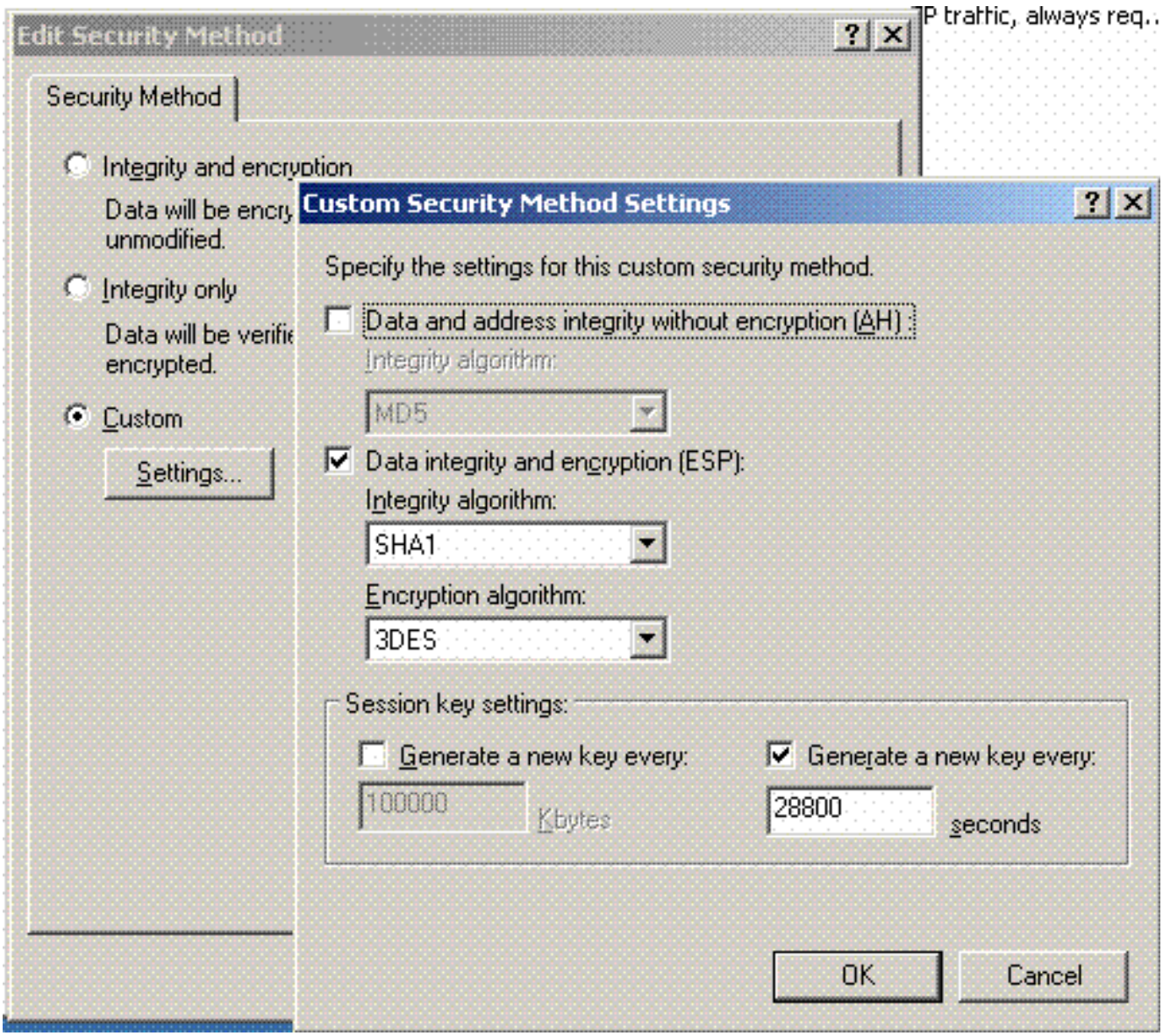


5. Modificare le proprietà del nuovo criterio 4404 e fare clic sulla scheda **Regole**. Aggiungere una nuova regola di filtro - Elenco filtri IP (dinamico); Operazione filtro (risposta predefinita);

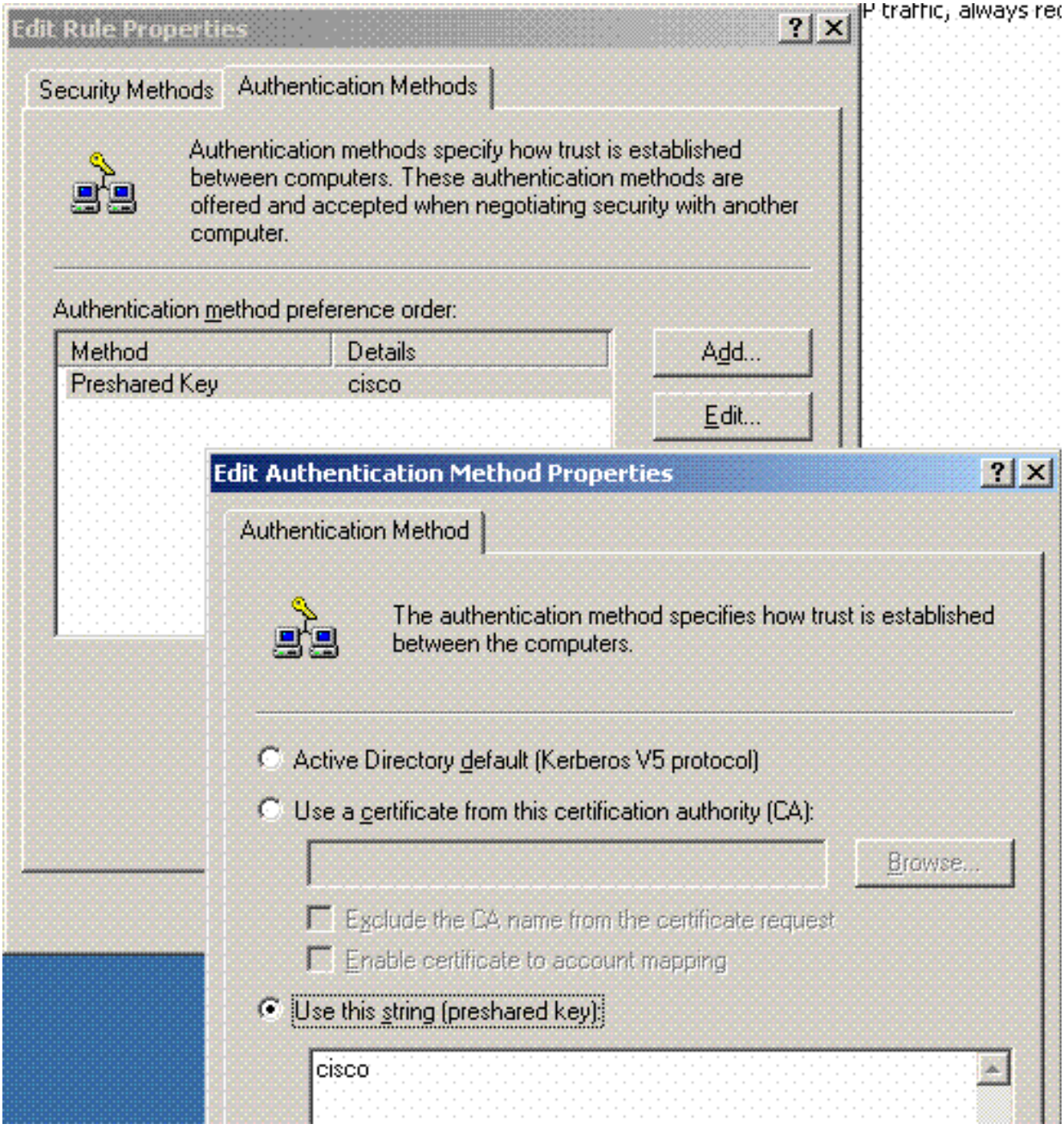
Autenticazione (PSK); Tunnel (nessuno). Fare doppio clic sulla nuova regola di filtro creata e selezionare Metodi di
protezione:



6. Fare clic su **Modifica metodo di protezione**, quindi sul pulsante di opzione Impostazioni **personalizzate**. Scegliere queste impostazioni.**Nota:** queste impostazioni devono corrispondere alle impostazioni di protezione IPSec RADIUS del
controller.



7. Fare clic sulla scheda **Metodo di autenticazione** in Modifica proprietà regola. Immettere lo stesso segreto condiviso immesso in precedenza nella configurazione RADIUS del controller.



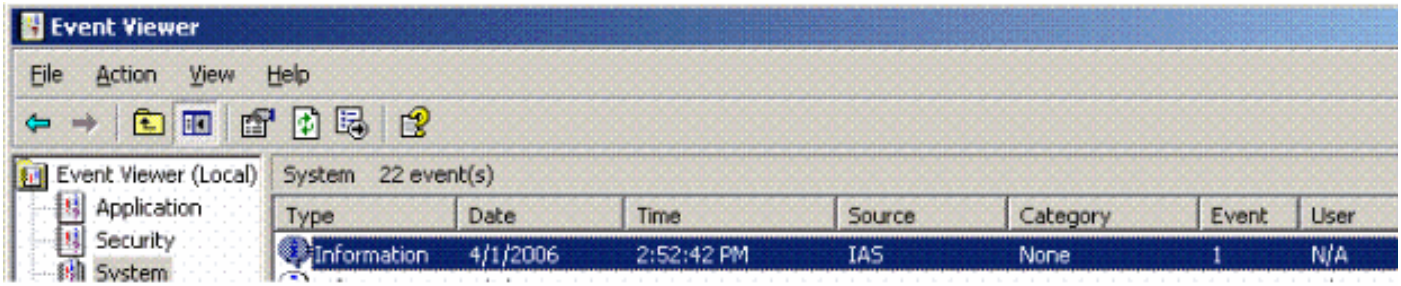
A questo punto, vengono completate tutte le configurazioni per il controller, le impostazioni IAS e le impostazioni di sicurezza del dominio. Salvare tutte le configurazioni sia sul controller che su WinServer e riavviare tutti i computer. Sul client WLAN utilizzato per il test, installare il certificato radice e configurare per WPA2/PEAP. Dopo aver installato il certificato radice nel client, riavviare il computer client. Dopo il riavvio di tutti i computer, connettere il client alla WLAN e acquisire questi eventi di registro.

Nota: è necessaria una connessione client per impostare la connessione IPSec tra il controller e WinServer RADIUS.

Eventi registro eventi di sistema di Windows 2003

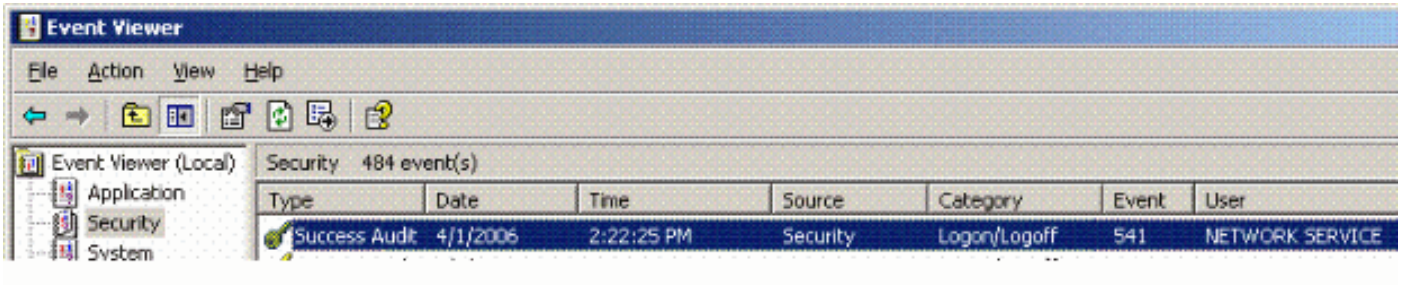
Se la connessione client WLAN configurata per WPA2/PEAP con IPSec RADIUS abilitato genera questo evento di sistema sul server WinServer:

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)
```

Se la connessione IPSec RADIUS del controller <> riesce, nei registri di WinServer verrà generato questo evento di protezione:




```
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
```

Esempio di debug riuscito del controller LAN wireless RADIUS IPSec

Per verificare questa configurazione, è possibile usare il comando debug **pm ikemsg enable** sul controller. Ecco un esempio.

```
(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
ookie=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
ookie=0x064bdcaf50d5f555
ID: packet[8] = 0x01000000 c0a81e69
HASH: hash[20] = 0x3b26e590 66651f13 2a86f62d 1b1d1e71 064b43f6
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=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
ookie=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
ookie=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
ookie=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
```

Cattura etreale

Di seguito è riportato un esempio di Cattura Etica.

```
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
```

Informazioni correlate

- Guida alla configurazione di Cisco Wireless LAN Controller, versione 5.2
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).