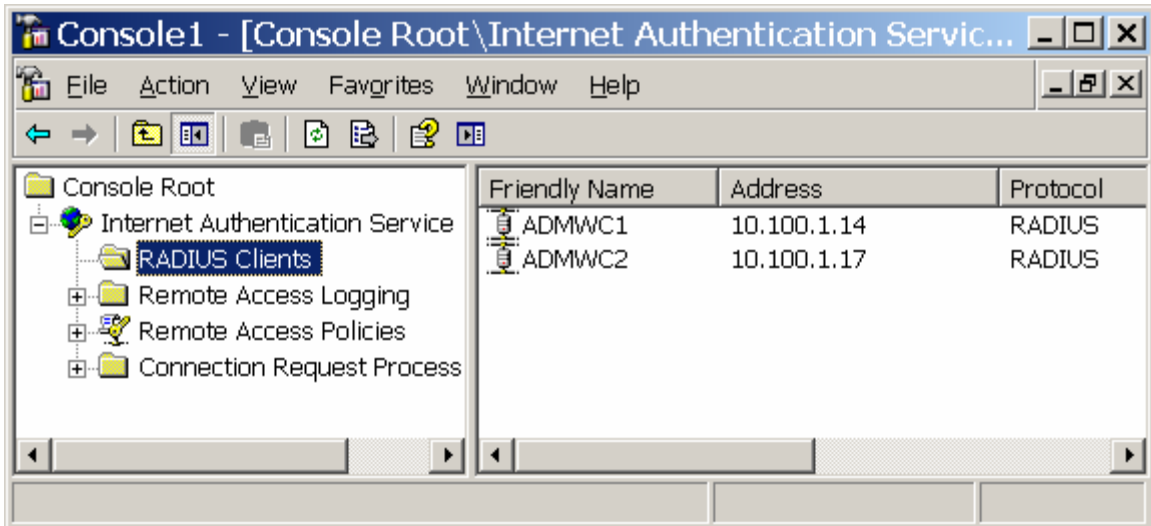


Windows IAS setting for Cisco WLC, Windows XP, Vista, 802.1x using PEAP

Adding a Radius Client

Right click on Radius Clients

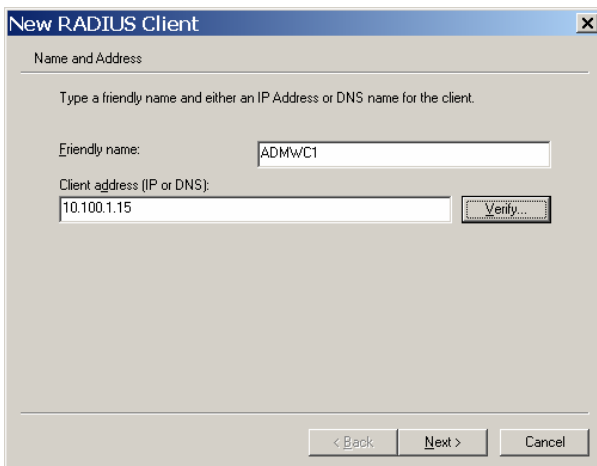
- New Radius Client



Type in a Friendly Name for WLC

Type in the IP address of WLC

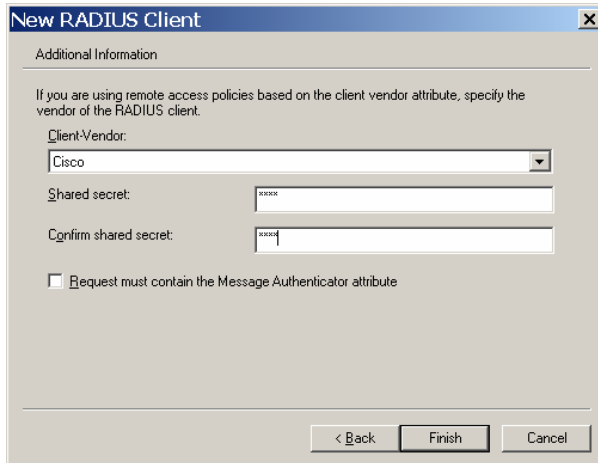
Click Next



Client-Vendor: select Cisco

- Type in Shared Secret

Click Finish



New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: Cisco

Shared secret: [masked]

Confirm shared secret: [masked]

Request must contain the Message Authenticator attribute

< Back Finish Cancel

- Follow steps for additional Wireless Controllers

Adding a Remote Access Policy

Click on Remote Access Policies

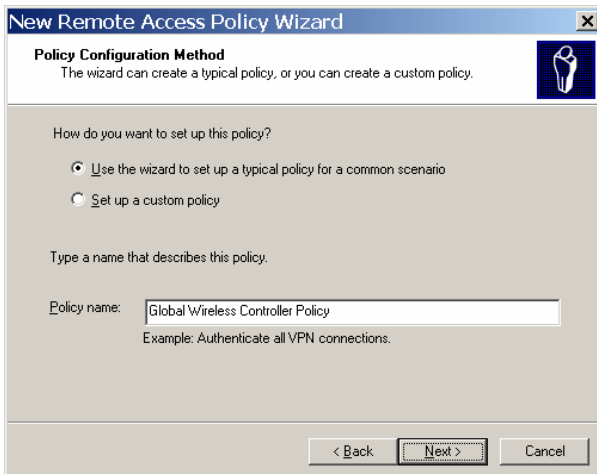
- Right Click on Remote Access Policies
 - Click on New Remote Access Policy



Click Next



Select: Use the wizard to set up a typical policy for a common scenario
In the Policy name type: Global Wireless Controller Policy



Select Wireless

Next

New Remote Access Policy Wizard

Access Method
Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

- VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
- Dial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
- Wireless
Use for wireless LAN connections only.
- Ethernet
Use for Ethernet connections, such as connections that use a switch.

< Back Next > Cancel

Select Group

Click Add

New Remote Access Policy Wizard

User or Group Access
You can grant access to individual users, or you can grant access to selected groups.

Grant access based on the following:

- User
User access permissions are specified in the user account.
- Group
Individual user permissions override group permissions.

Group name:

Add...
Remove

< Back Next > Cancel

Add Domain Users; domain computers

Click OK

Select Groups

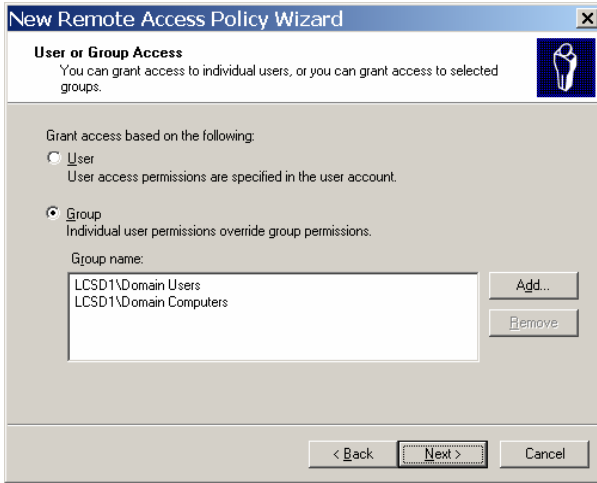
Select this object type:
 Object Types...

From this location:
 Locations...

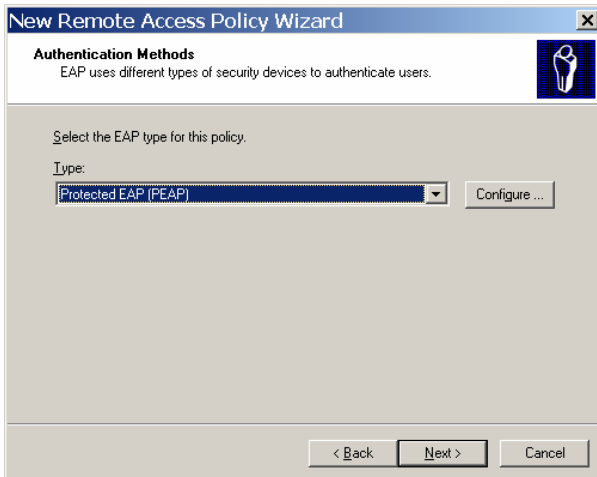
Enter the object names to select [examples](#):
 Check Names

Advanced... OK Cancel

Next

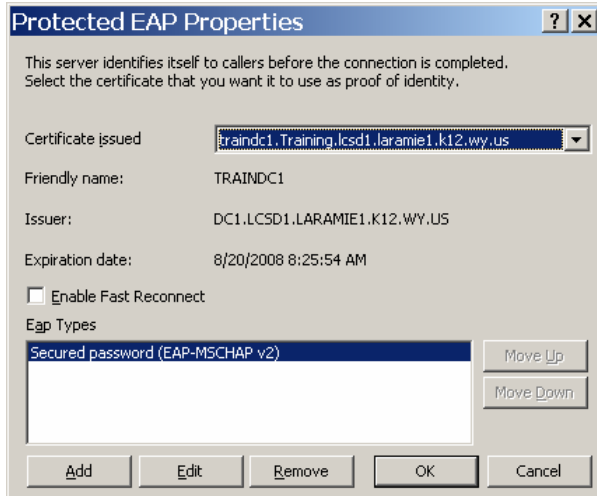


Select Protected EAP (PEAP)
Click Configure...



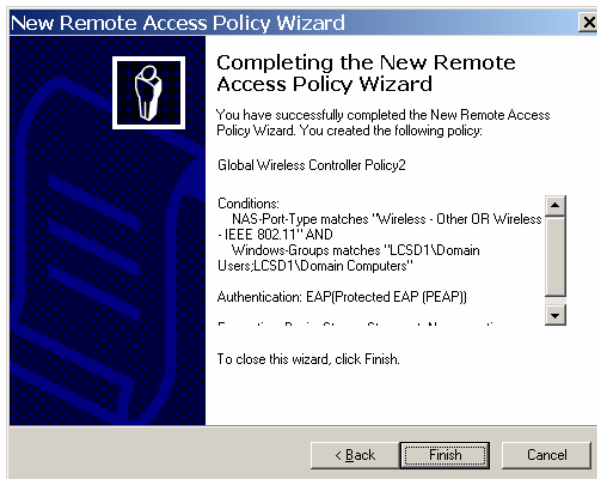
Make sure certificate issued to IAS server is selected.

- Uncheck Enable Fast Reconnect.
- Click OK
- Click Next



Review Settings

Click Finish



- **NOTE:** Some of these steps have already completed by using the Wizard. Skip steps if already completed

Be sure the Global Wireless Controller Policy is on top of list order.

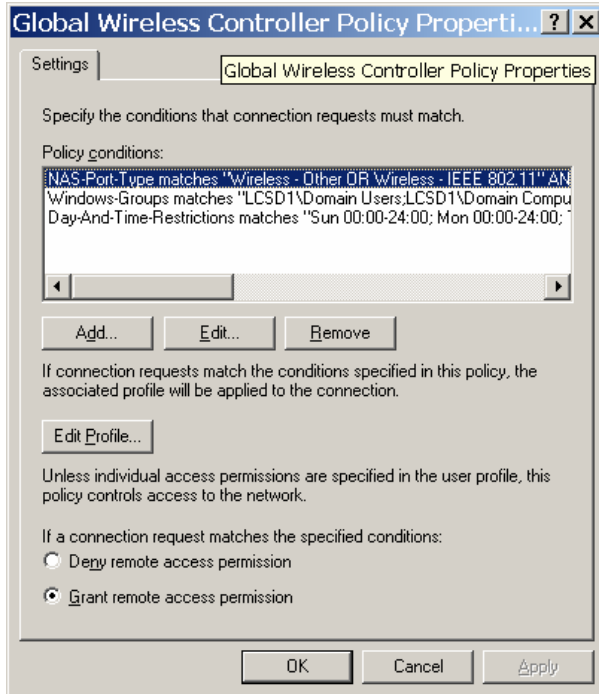
- If not at the top of the list, click on the Global Wireless Controller Policy and use the arrows on the task bar to move the policy up.

Right Click on Global Wireless Controller Policy

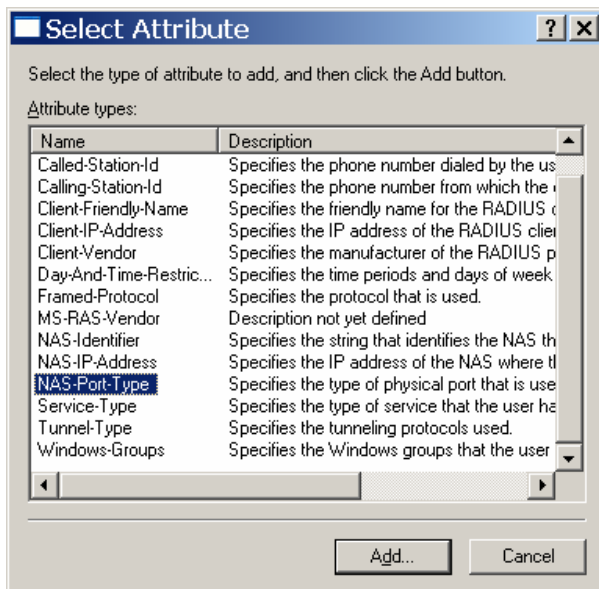
- Properties



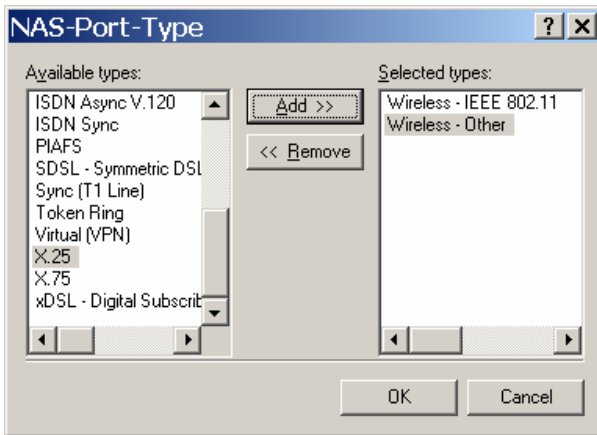
Be sure "Grant remote access permissions" is selected.



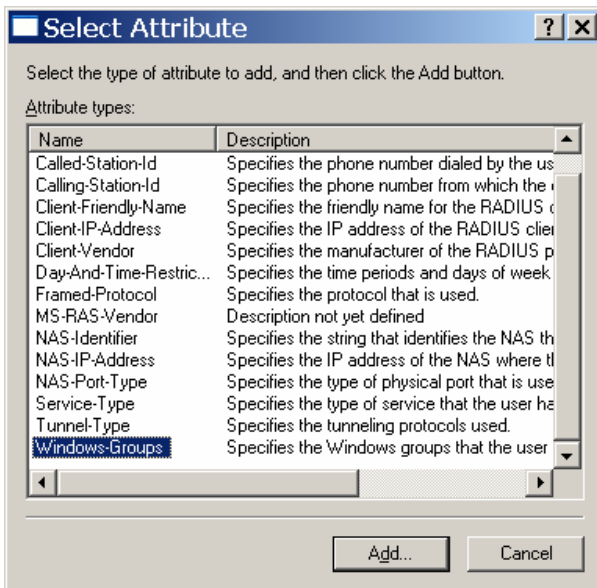
Click Add,
Select Attribute
NAS-Port-Type



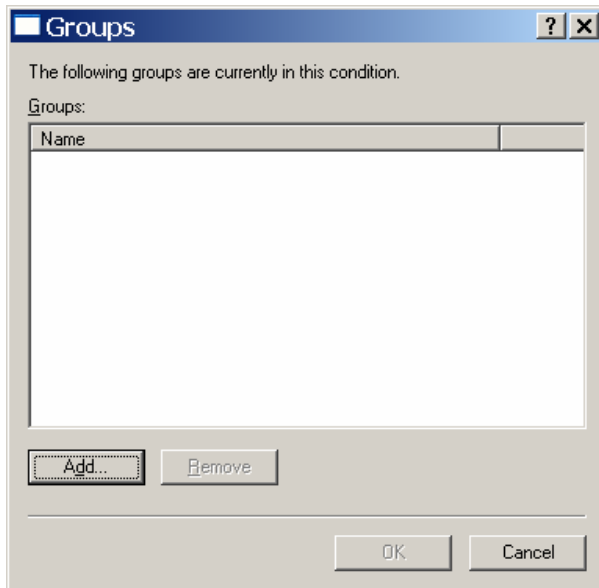
Add: Wireless – IEEE 802.1
Add: Wireless – Other
Click OK



Click Add,
Select Windows-Groups

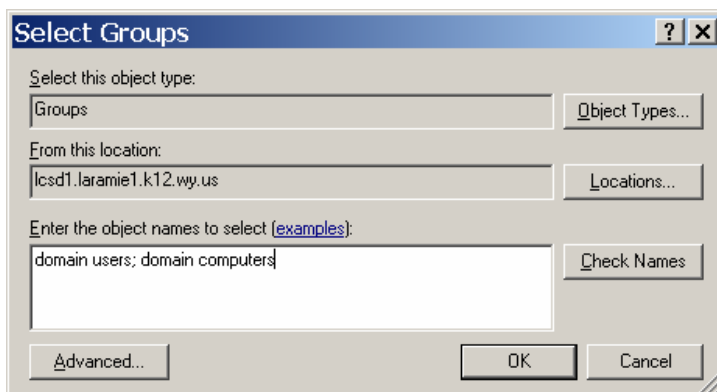


Click Add

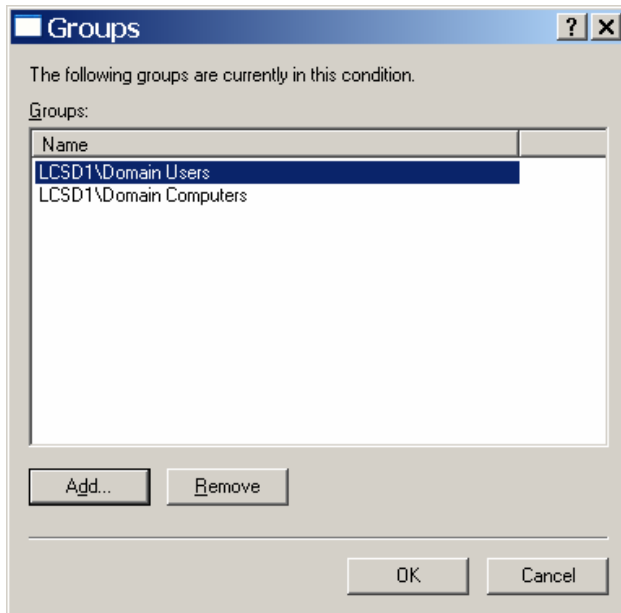


Click Add,
Add: domain users; domain computers

- If users and computer in a sub domain need to be authenticated
 - Select Location
 - Browse to domain
 - Add domain users and domain computers for that domain



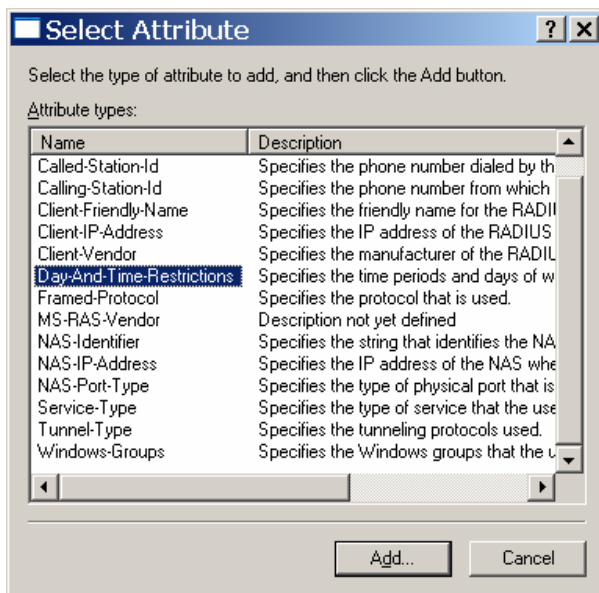
Click OK



Click OK

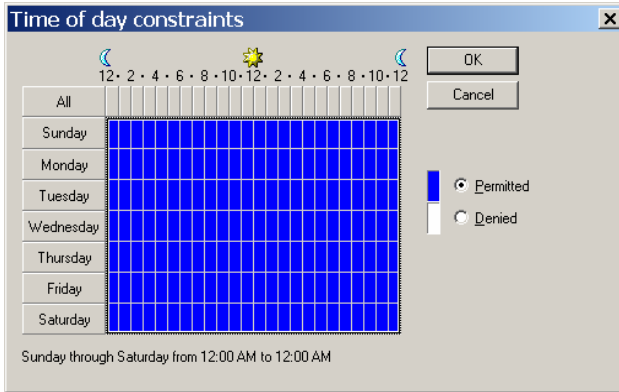
Click Add

Select Day-And-Time-Restrictions

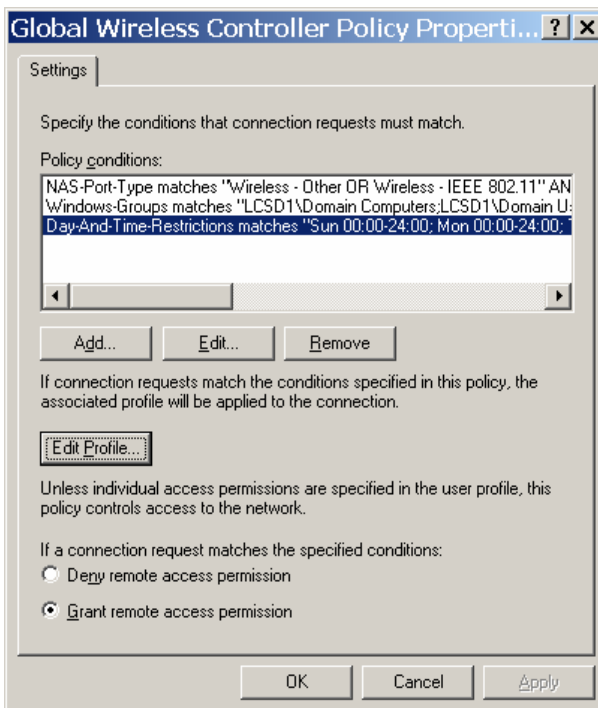


Click Add

Click on ALL
Click Permitted
Click OK

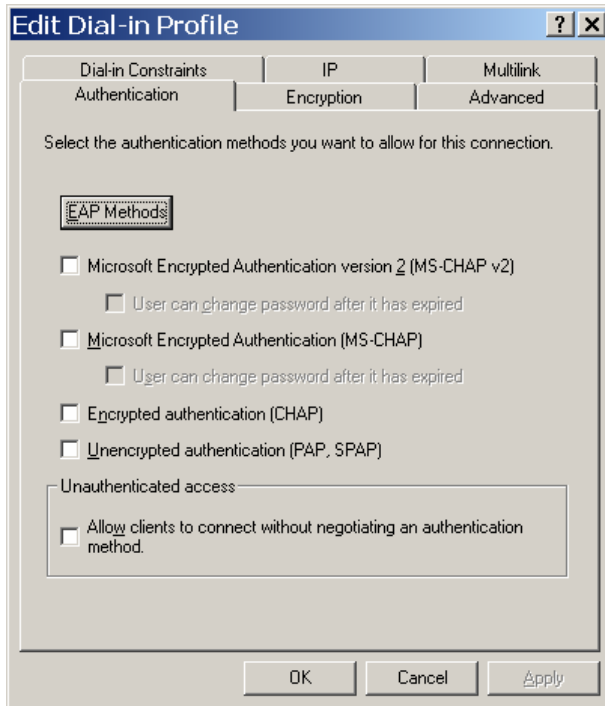


Click Edit Profile...



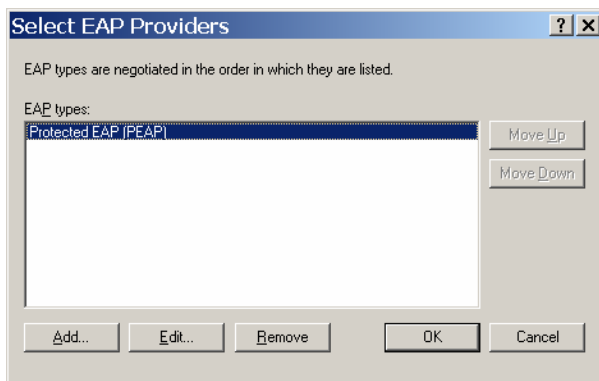
Click on the Authentication Tab

- Uncheck all
- Click on EAP Methods



Select PEAP

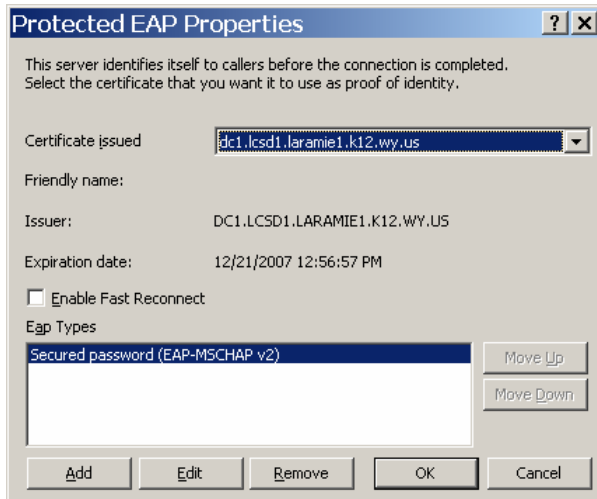
Click Edit



Certificate issued: Server name (dc1.lcsd1.laramie1.k12.wy.us) has been selected

- Uncheck Enable Fast Reconnect

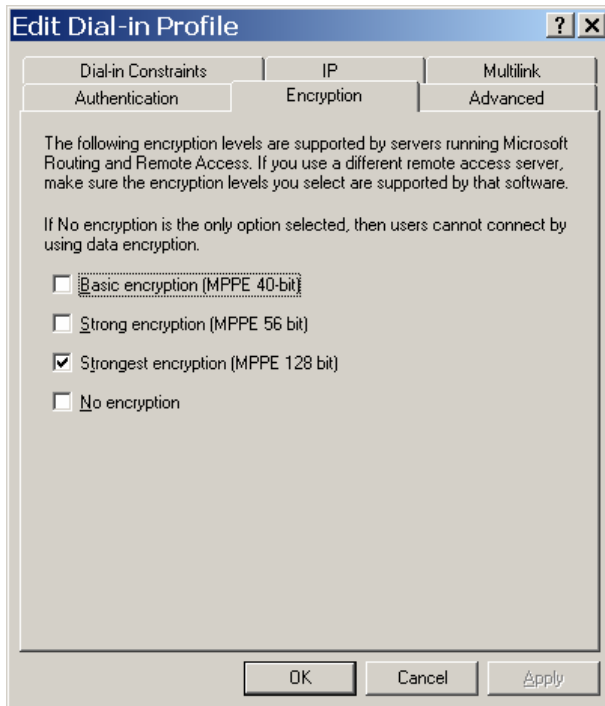
Click OK



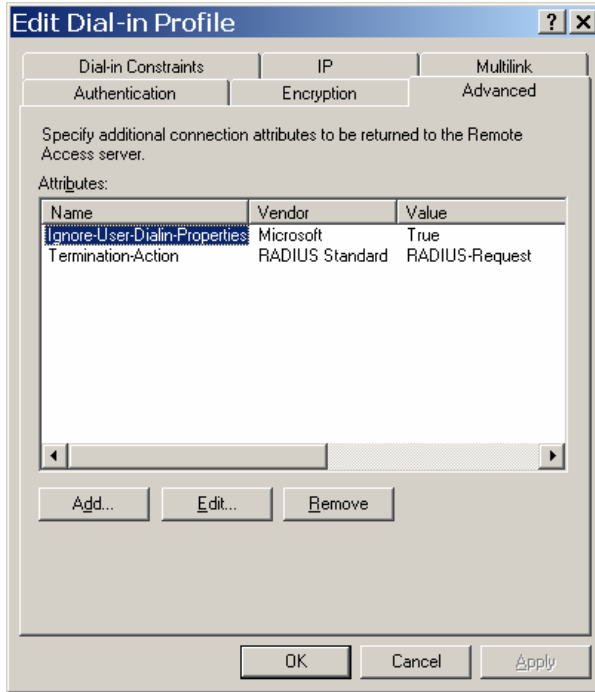
Click the Encryption Tab

Uncheck all except “Strongest encryption (MPPE 128 bit)”

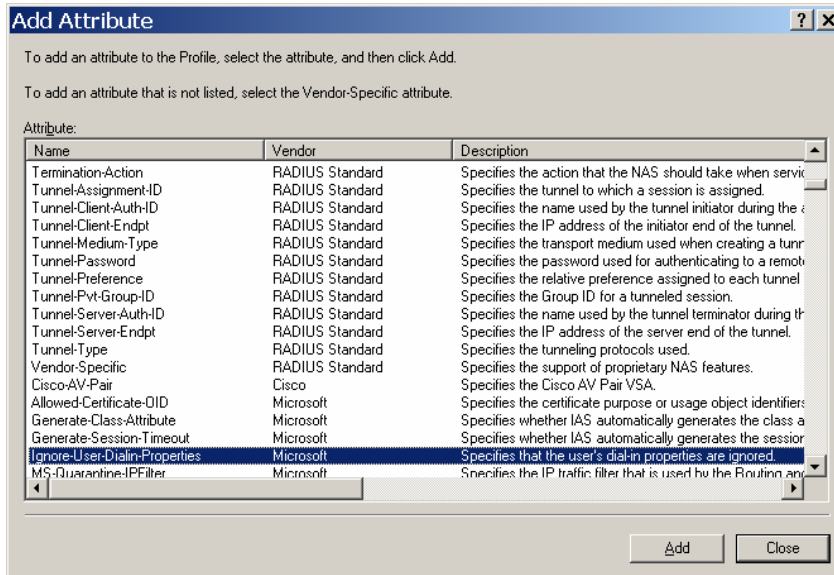
Click the Advanced Tab



Remove all attributes by selecting the attribute and click remove



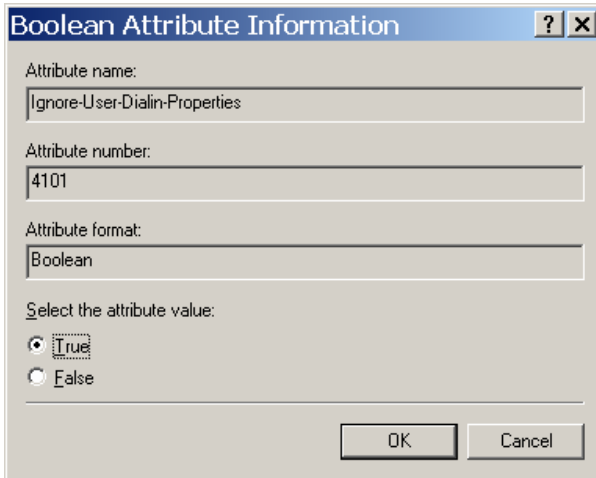
Click Add



Select Ignore-User-Dialin-Properties

Click Add

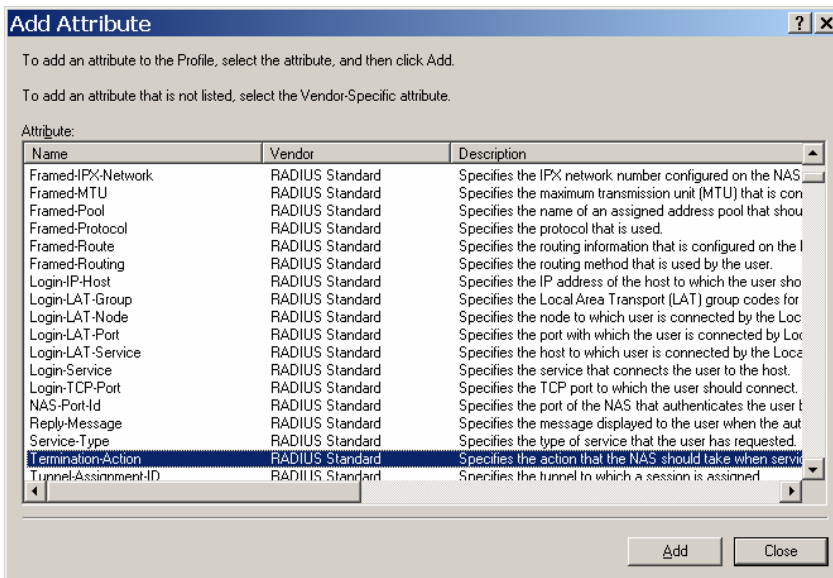
Set attribute value: True
Click OK



The dialog box is titled "Boolean Attribute Information". It contains the following fields and options:

- Attribute name: ignore-User-Dialin-Properties
- Attribute number: 4101
- Attribute format: Boolean
- Select the attribute value: True, False
- Buttons: OK, Cancel

Click Add to add another Attribute

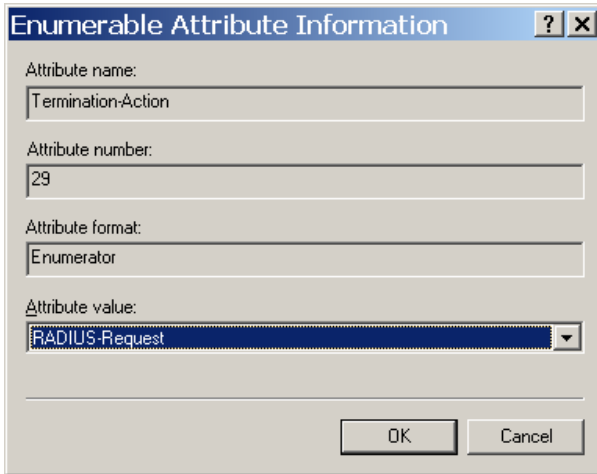


The dialog box is titled "Add Attribute". It contains the following elements:

- Instructions: "To add an attribute to the Profile, select the attribute, and then click Add." and "To add an attribute that is not listed, select the Vendor-Specific attribute."
- Table with columns: Name, Vendor, Description
- Buttons: Add, Close

Name	Vendor	Description
Framed-IPX-Network	RADIUS Standard	Specifies the IPX network number configured on the NAS
Framed-MTU	RADIUS Standard	Specifies the maximum transmission unit (MTU) that is con
Framed-Pool	RADIUS Standard	Specifies the name of an assigned address pool that shou
Framed-Protocol	RADIUS Standard	Specifies the protocol that is used.
Framed-Route	RADIUS Standard	Specifies the routing information that is configured on the l
Framed-Routing	RADIUS Standard	Specifies the routing method that is used by the user.
Login-IP-Host	RADIUS Standard	Specifies the IP address of the host to which the user sho
Login-LAT-Group	RADIUS Standard	Specifies the Local Area Transport (LAT) group codes for
Login-LAT-Node	RADIUS Standard	Specifies the node to which user is connected by the Loc
Login-LAT-Port	RADIUS Standard	Specifies the port with which the user is connected by Loc
Login-LAT-Service	RADIUS Standard	Specifies the host to which user is connected by the Loca
Login-Service	RADIUS Standard	Specifies the service that connects the user to the host.
Login-TCP-Port	RADIUS Standard	Specifies the TCP port to which the user should connect.
NAS-Port-Id	RADIUS Standard	Specifies the port of the NAS that authenticates the user t
Reply-Message	RADIUS Standard	Specifies the message displayed to the user when the aut
Service-Type	RADIUS Standard	Specifies the type of service that the user has requested.
Termination-Action	RADIUS Standard	Specifies the action that the NAS should take when servi
Tunnel-Assignment-ID	RADIUS Standard	Specifies the tunnel to which a session is assigned

Select Termination-Action
Click Add

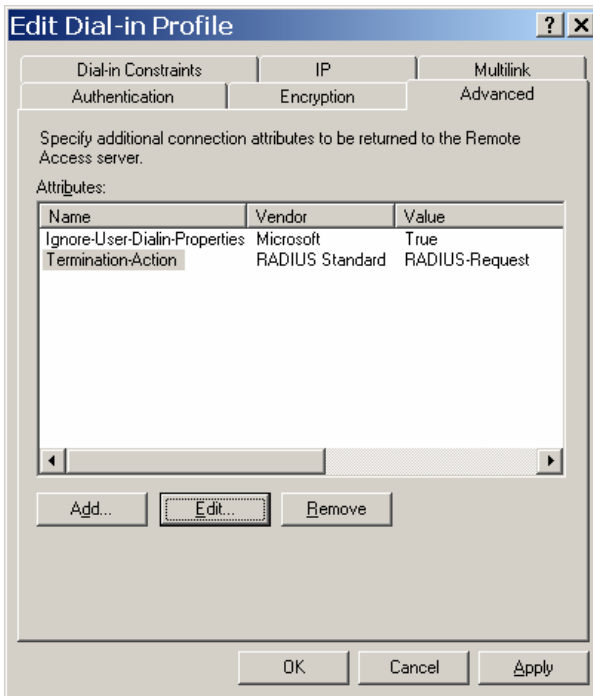


The dialog box titled "Enumerable Attribute Information" contains the following fields:

- Attribute name: Termination-Action
- Attribute number: 29
- Attribute format: Enumerator
- Attribute value: RADIUS-Request (selected in a dropdown menu)

Buttons: OK, Cancel

Set Attribute value: RADIUS-Request
Click Ok



The dialog box titled "Edit Dial-in Profile" has tabs for Dial-in Constraints, IP, Multilink, Authentication, Encryption, and Advanced. The "Advanced" tab is selected.

Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Ignore-User-Dialin-Properties	Microsoft	True
Termination-Action	RADIUS Standard	RADIUS-Request

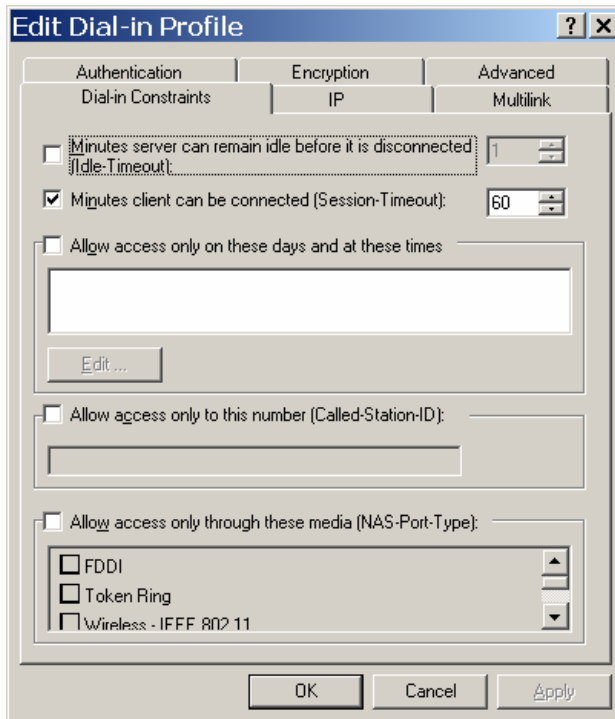
Buttons: Add..., Edit..., Remove, OK, Cancel, Apply

Click on the Dial-in Constraints

Check “Minutes clients can be connected (Session-Timeout)”

- Set to 60

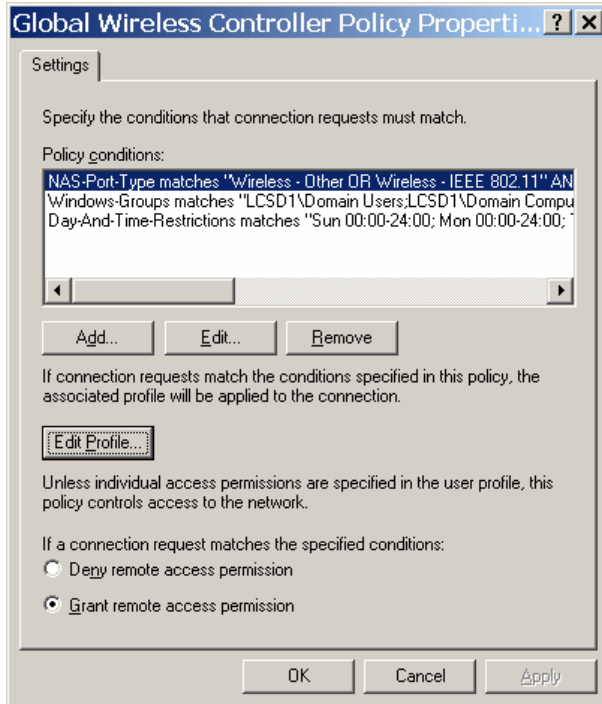
Click OK



Important: Using a session timeout of 10 minutes may be too short for many scenarios. Short timeouts place a high load on the IAS servers. Short timeouts also increase the possibility of making your IAS server temporarily unavailable, which will result in disconnecting clients from the WLAN. For these reasons, you can use a longer timeout of 60 minutes without significantly compromising the WLAN security.

<http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/PGCH06.msp?mfr=true>

Click OK



References:

Designing the Wireless LAN Security Using 802.1X

<http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/PGCH06.mspx?mfr=true>

IAS Operations Guide

<http://www.microsoft.com/downloads/details.aspx?familyid=27C432BF-5ED0-4763-8909-36E7C310AE3C&displaylang=en>

Step-by-Step Guide for Securing Wireless Deployments for Small Office/Home Office or Small Organization Networks

<http://www.microsoft.com/downloads/details.aspx?FamilyID=269902E8-FC41-4EB1-9374-44612E64F0FB&displaylang=en>

IEEE 802.11 Wireless LAN Security with Microsoft Windows

<http://www.microsoft.com/downloads/details.aspx?familyid=67FDEB48-74EC-4EE8-A650-334BB8EC38A9&displaylang=en>

Internet Authentication Service

<http://technet.microsoft.com/en-us/network/bb643123.aspx>

Wireless Networking

<http://technet.microsoft.com/en-us/network/bb530679.aspx>