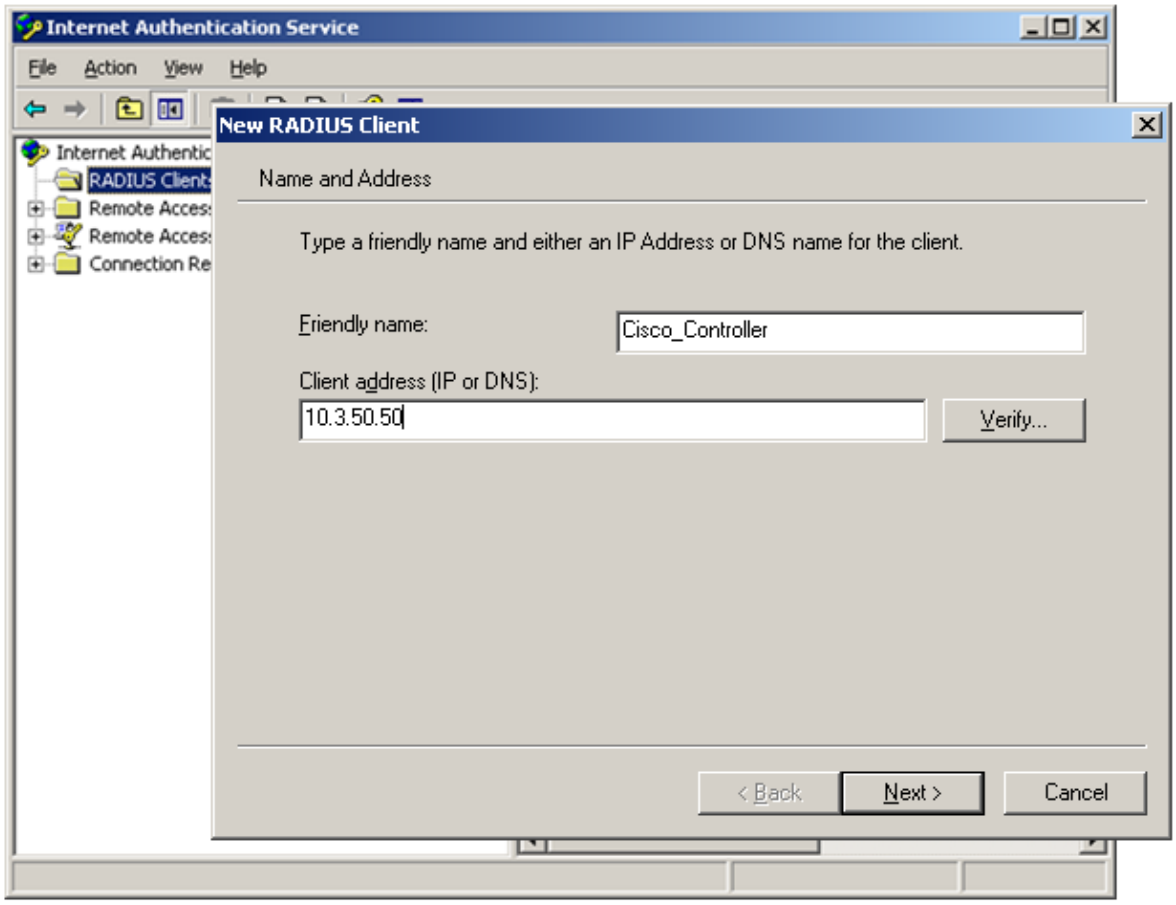
Zebra Setup Utility, Zebra Mobile Printer, Microsoft IAS, Cisco Controller PEAP and WPA-PEAP

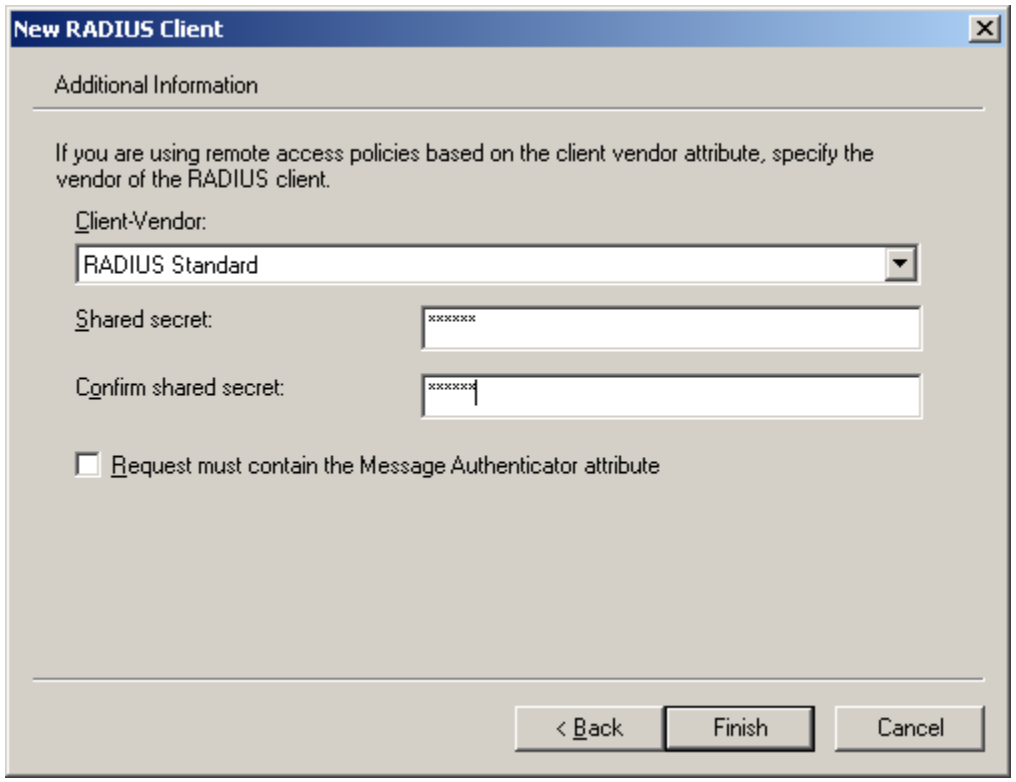
This section of the document illustrates the Microsoft Internet Authentication Service and how PEAP and WPA-PEAP was configured on this server.
This document is meant as an illustration only. Questions on the setup of IAS should be directed to Microsoft. It should be Microsoft that is used to determine if the illustration below is appropriate for your environment.

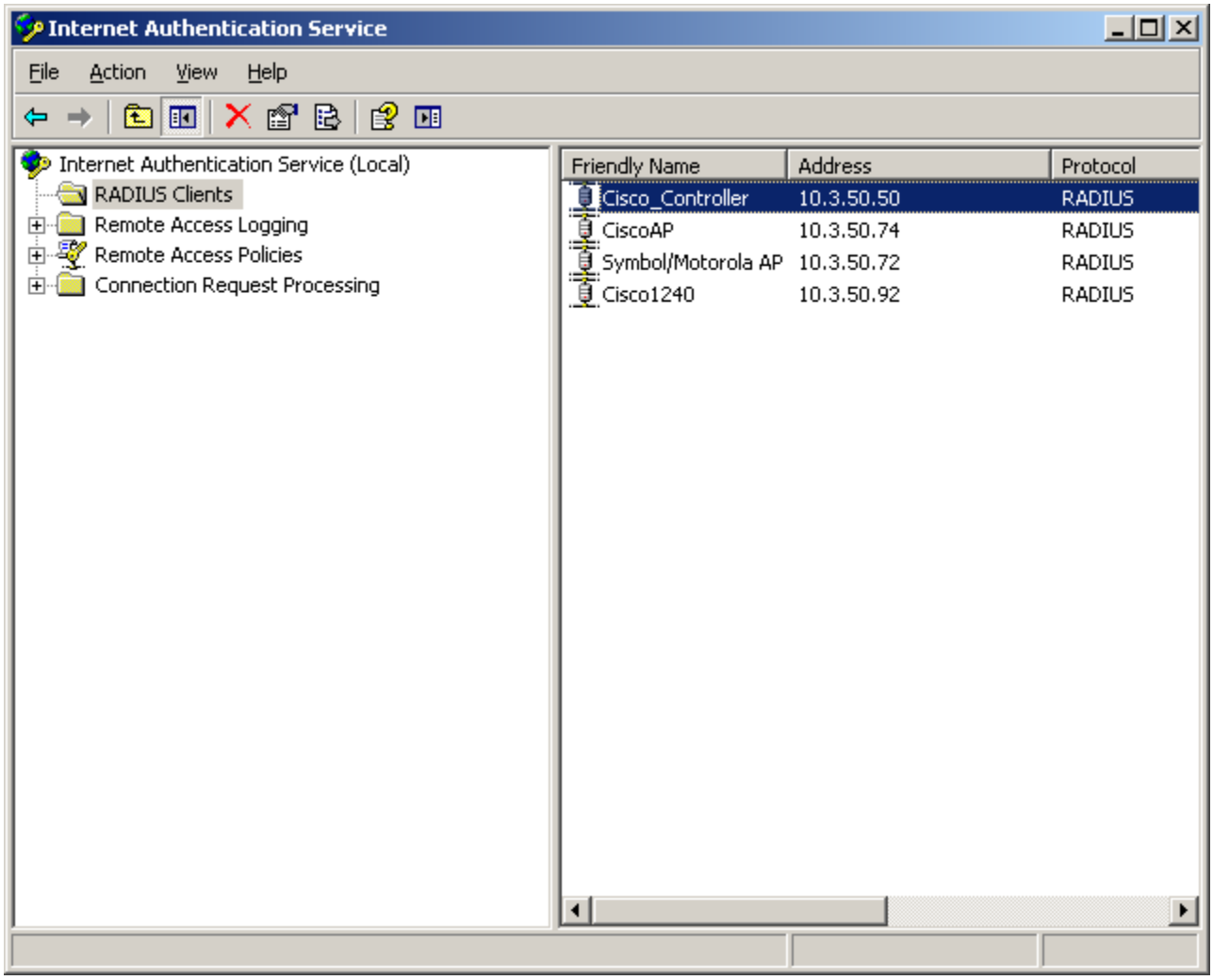
It is important to note that the setup on the IAS server did not differ when using WPA-PEAP or PEAP.

The first series of screenshots shows how a Radius client is added to IAS. In the screenshot below a Cisco controller with the IP address of 10.3.50.50 is added. The IAS server needs to have a client in the clients table to ensure that authentication requests are only being received from valid clients.

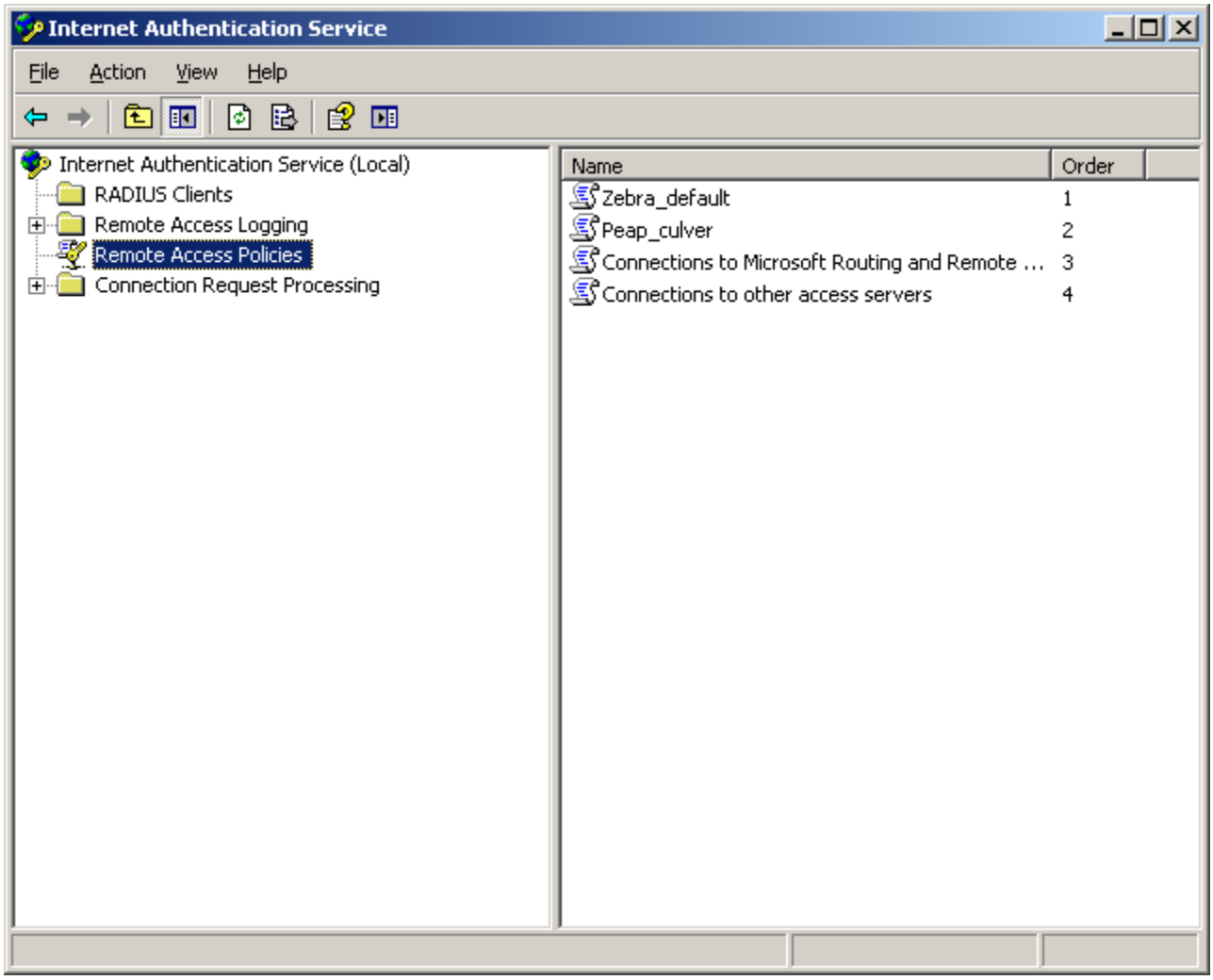


A secret key is entered on the IAS server. This secret key needs to match the secret key on the radius client (in this example the Cisco controller).

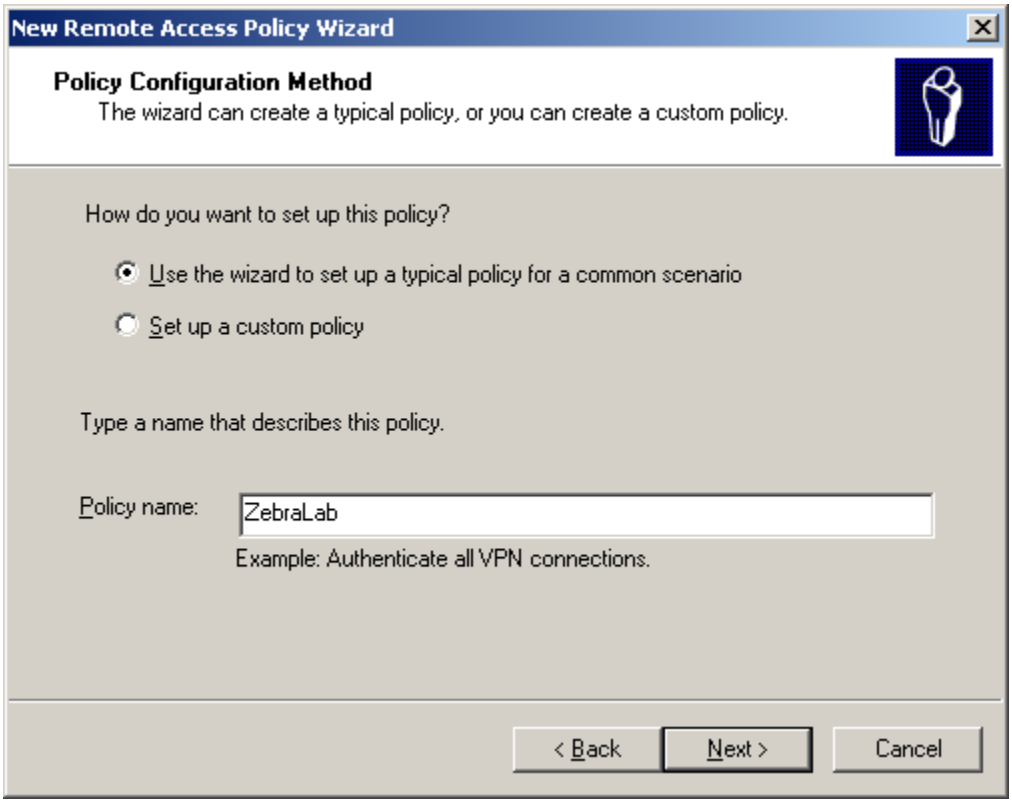

New RADIUS Client
Additional Information
If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.
Client-Vendor:
RADIUS Standard
Shared secret:
Confirm shared secret:
Request must contain the Message Authenticator attribute
< Back
Finish
Cancel

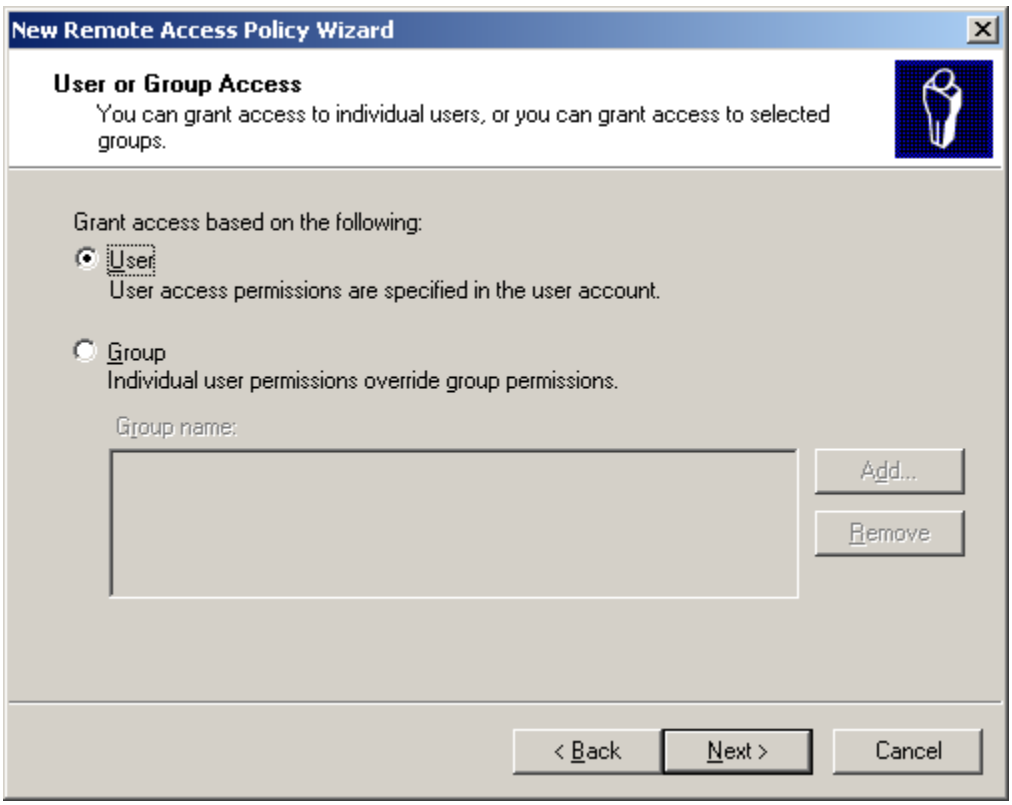


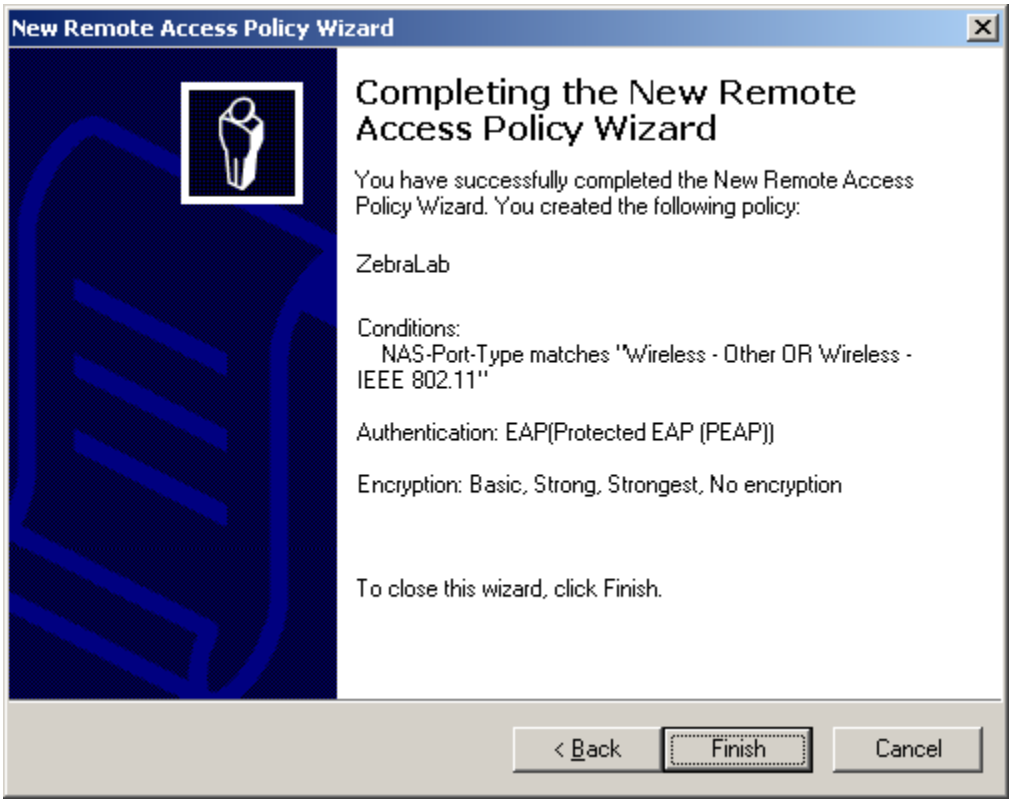
A Remote access policy is included in the IAS server. The following screenshots illustrate how a remote policy is added.

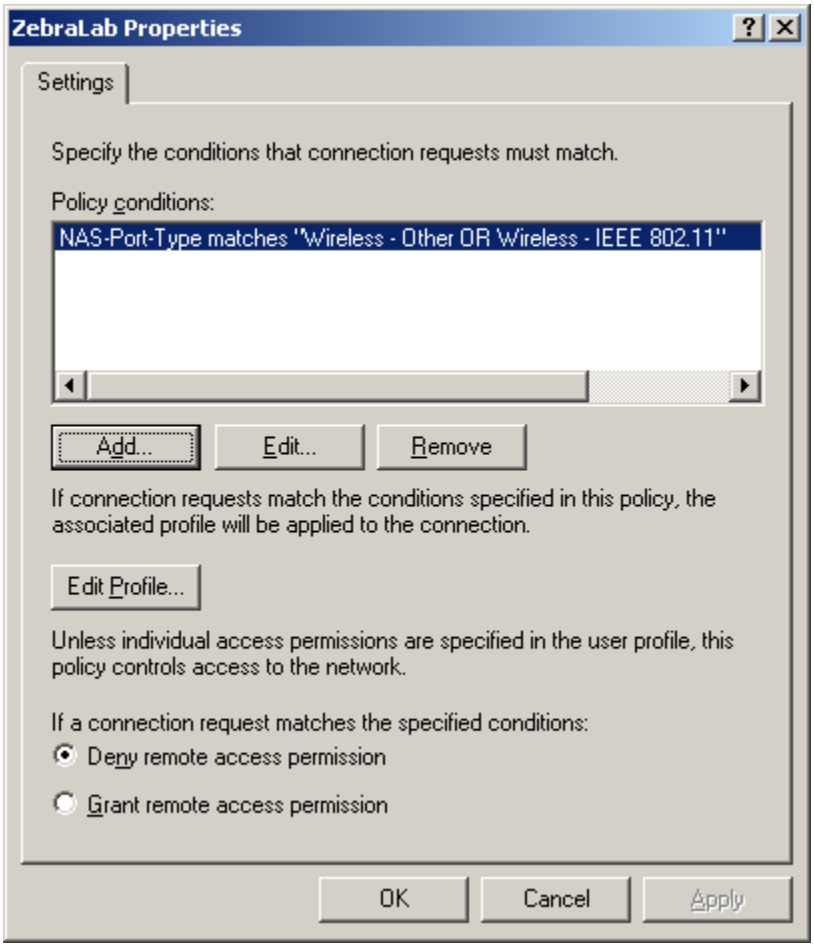

Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
Name
Order
Zebra_default
1
Peap_culver
2
Connections to Microsoft Routing and Remote ...
3
Connections to other access servers
4


New Remote Access Policy Wizard
Welcome to the New Remote Access Policy Wizard
This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.
To continue, click Next.
< Back
Next >
Cancel

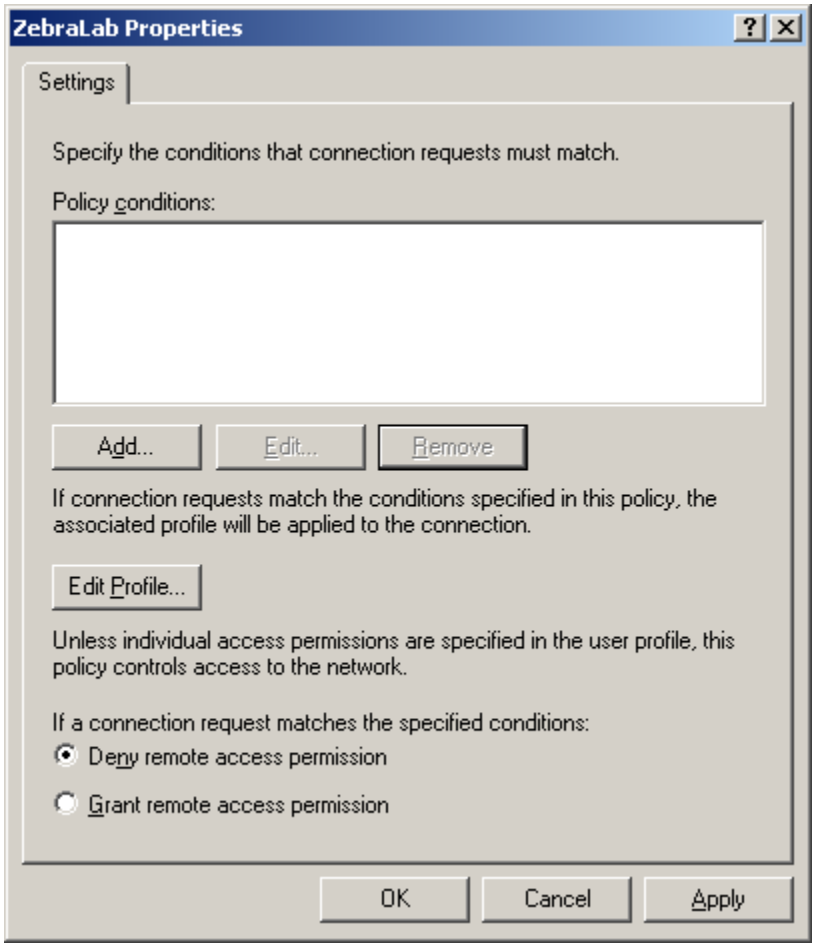

New Remote Access Policy Wizard
Policy Configuration Method
The wizard can create a typical policy, or you can create a custom policy.
How do you want to set up this policy?
Use the wizard to set up a typical policy for a common scenario
Set up a custom policy
Type a name that describes this policy.
Policy name:
ZebraLab
Example: Authenticate all VPN connections.
< Back
Next >
Cancel

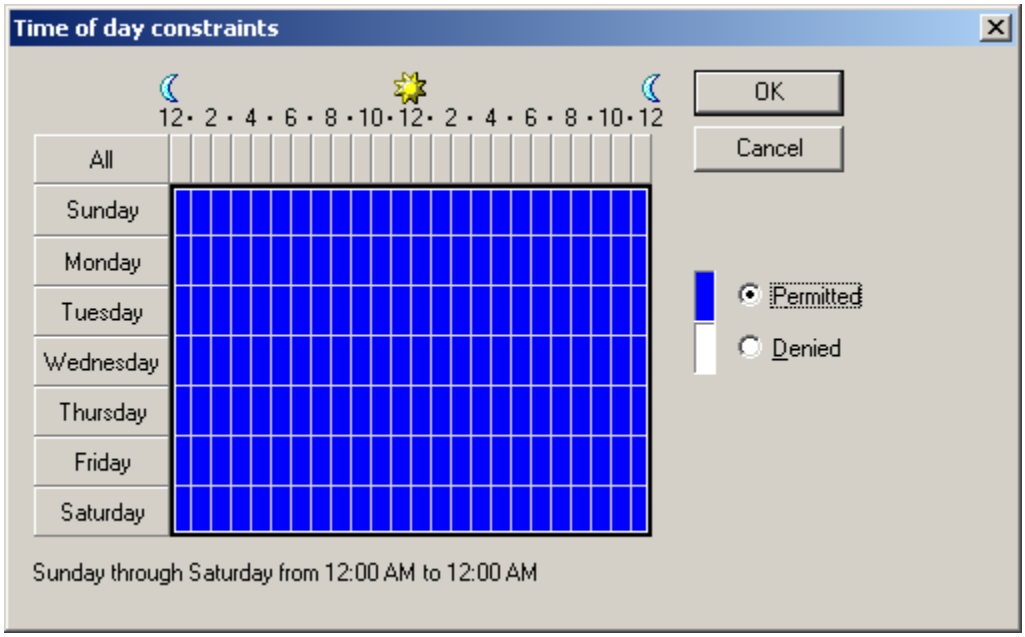

New Remote Access Policy Wizard
User or Group Access
You can grant access to individual users, or you can grant access to selected groups.
Grant access based on the following:
User
User access permissions are specified in the user account.
Group
Individual user permissions override group permissions.
Group name:
Add...
Remove
< Back
Next >
Cancel

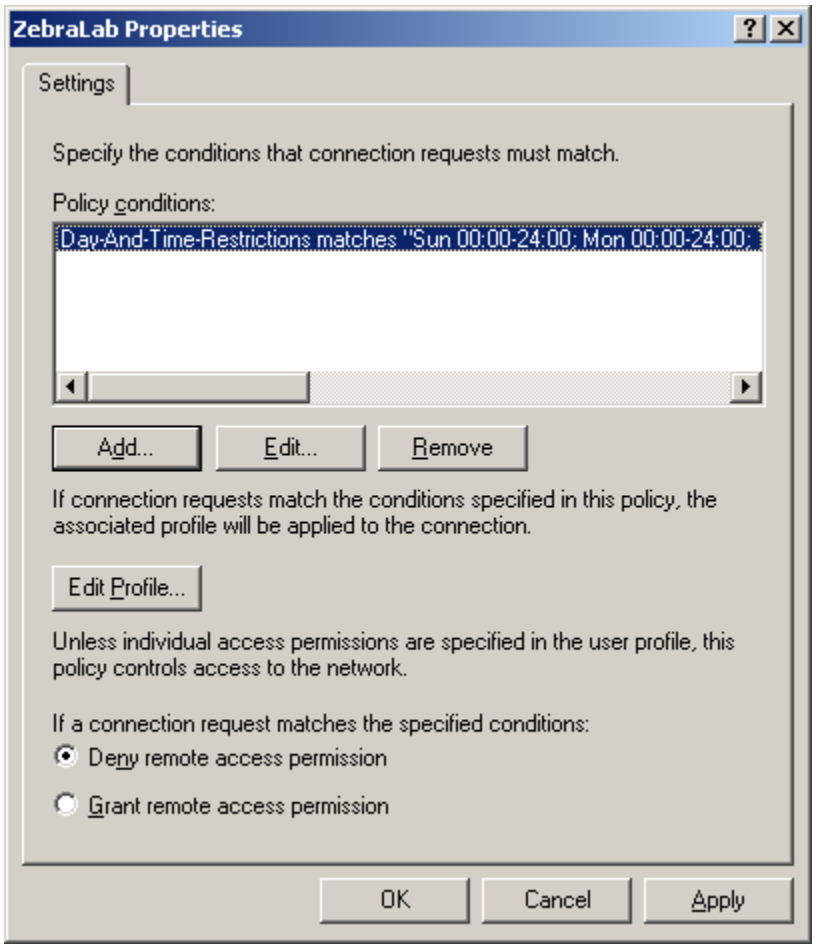

New Remote Access Policy Wizard
Completing the New Remote Access Policy Wizard
You have successfully completed the New Remote Access Policy Wizard. You created the following policy:
ZebraLab
Conditions:
NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11"
Authentication: EAP(Protected EAP (PEAP))
Encryption: Basic, Strong, Strongest, No encryption
To close this wizard, click Finish.
< Back
Finish
Cancel

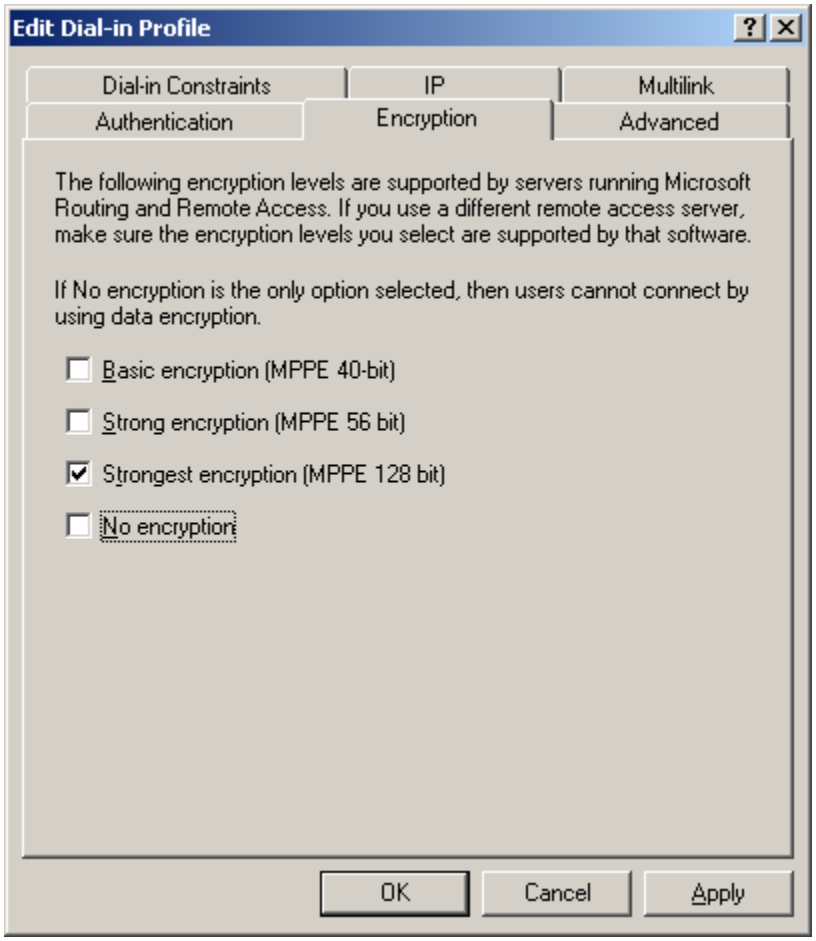


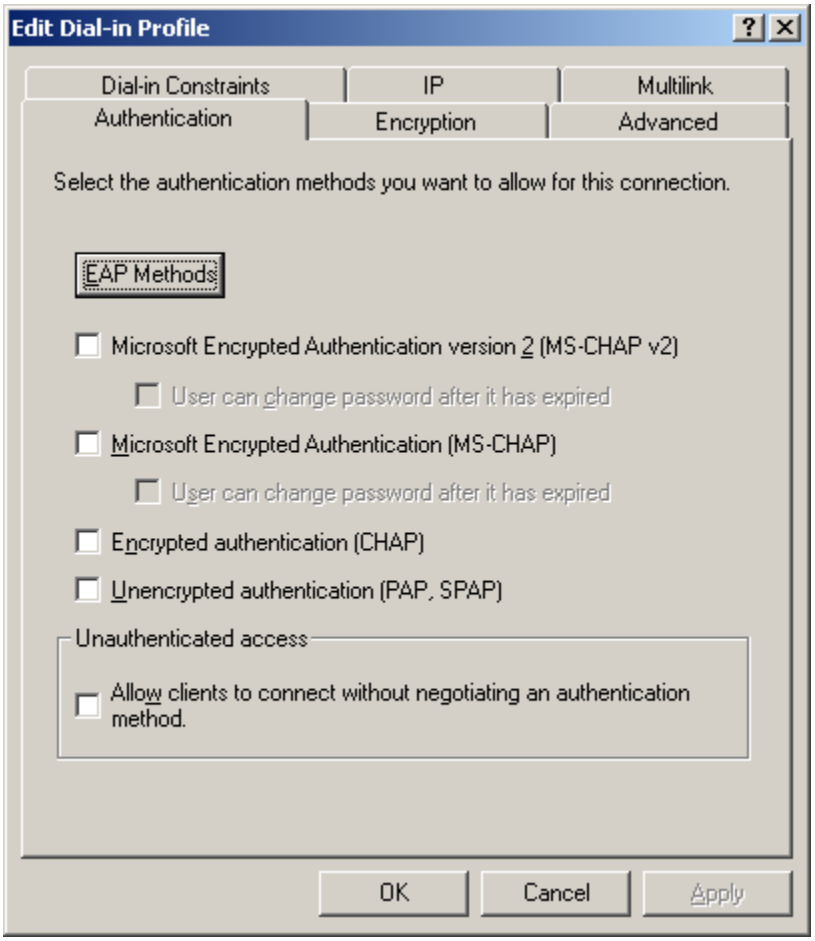
In the next few screenshots I have illustrated how a policy can be added.


ZebraLab Properties
Settings
Specify the conditions that connection requests must match.
Policy conditions:
Add...
Edit...
Remove
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.
Edit Profile...
Unless individual access permissions are specified in the user profile, this policy controls access to the network.
If a connection request matches the specified conditions:
Deny remote access permission
Grant remote access permission
OK
Cancel
Apply

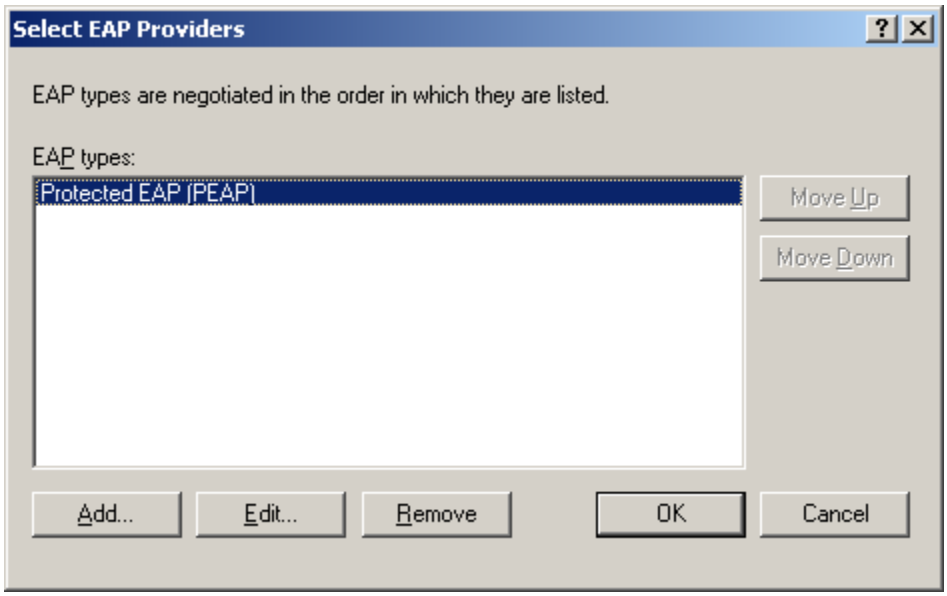

Time of day constraints
12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12
All
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
OK
Cancel
Permitted
Denied
Sunday through Saturday from 12:00 AM to 12:00 AM

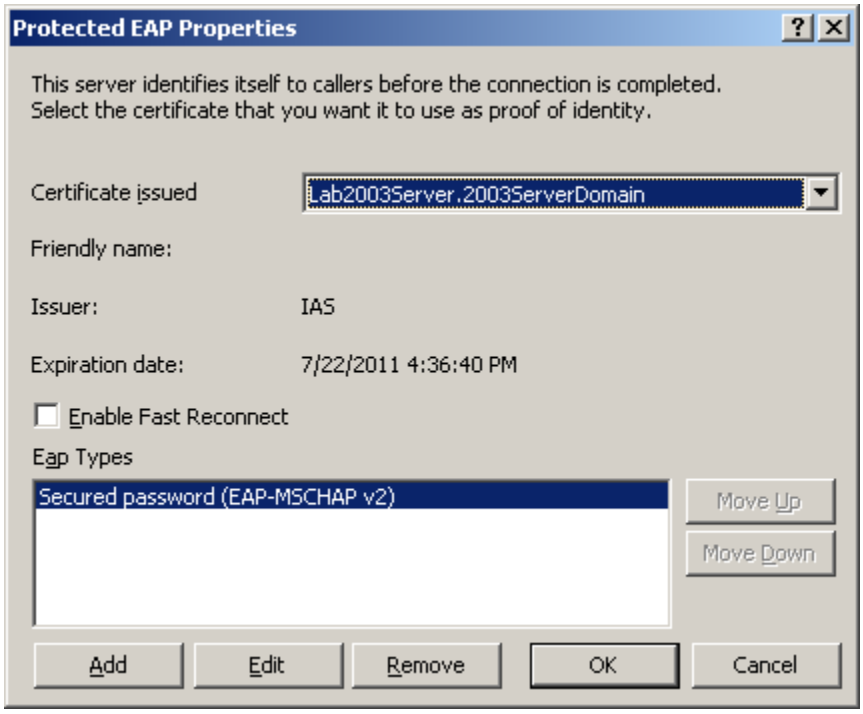

ZebraLab Properties
Settings
Specify the conditions that connection requests must match.
Policy conditions:
Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00;
Add...
Edit...
Remove
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.
Edit Profile...
Unless individual access permissions are specified in the user profile, this policy controls access to the network.
If a connection request matches the specified conditions:
Deny remote access permission
Grant remote access permission
OK
Cancel
Apply

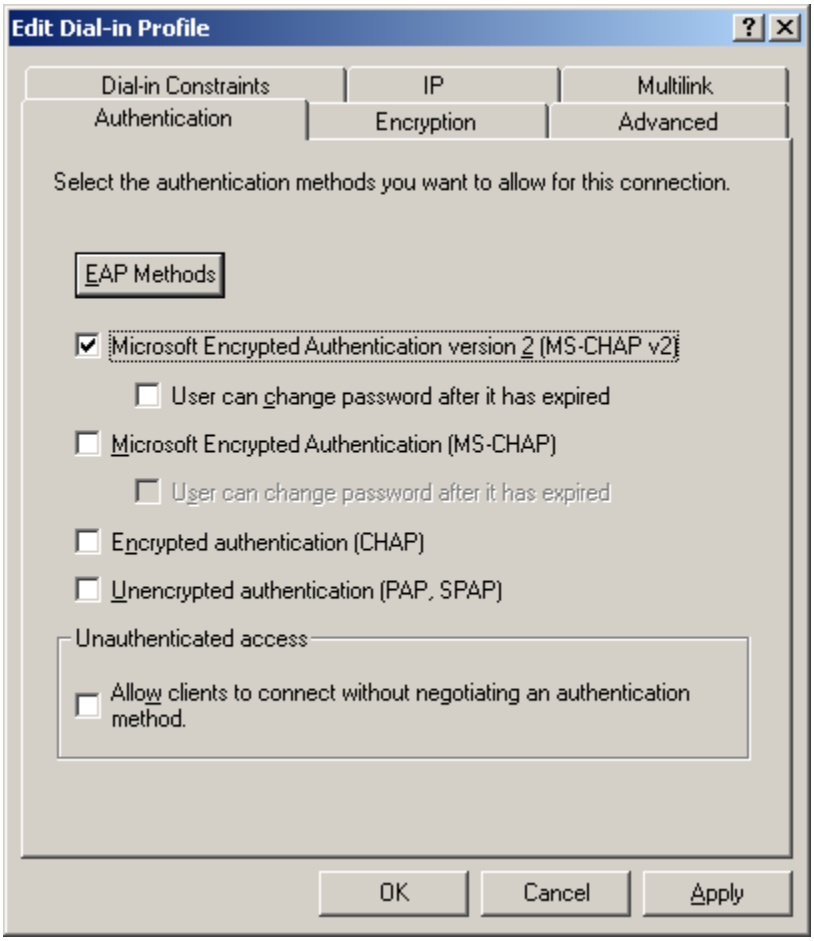

Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
The following encryption levels are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the encryption levels you select are supported by that software.
If No encryption is the only option selected, then users cannot connect by using data encryption.
Basic encryption (MPPE 40-bit)
Strong encryption (MPPE 56 bit)
Strongest encryption (MPPE 128 bit)
No encryption
OK
Cancel
Apply



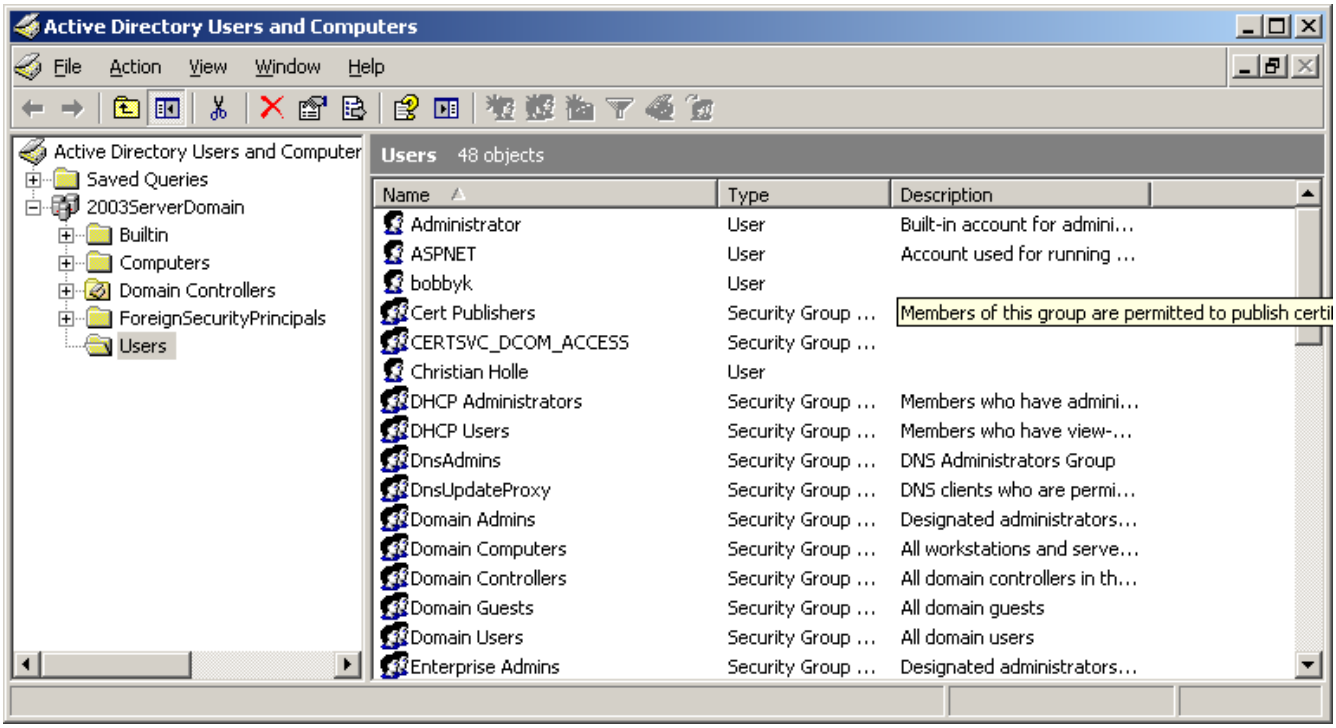
The example that is provided illustrates PEAP and MSCHAP v2

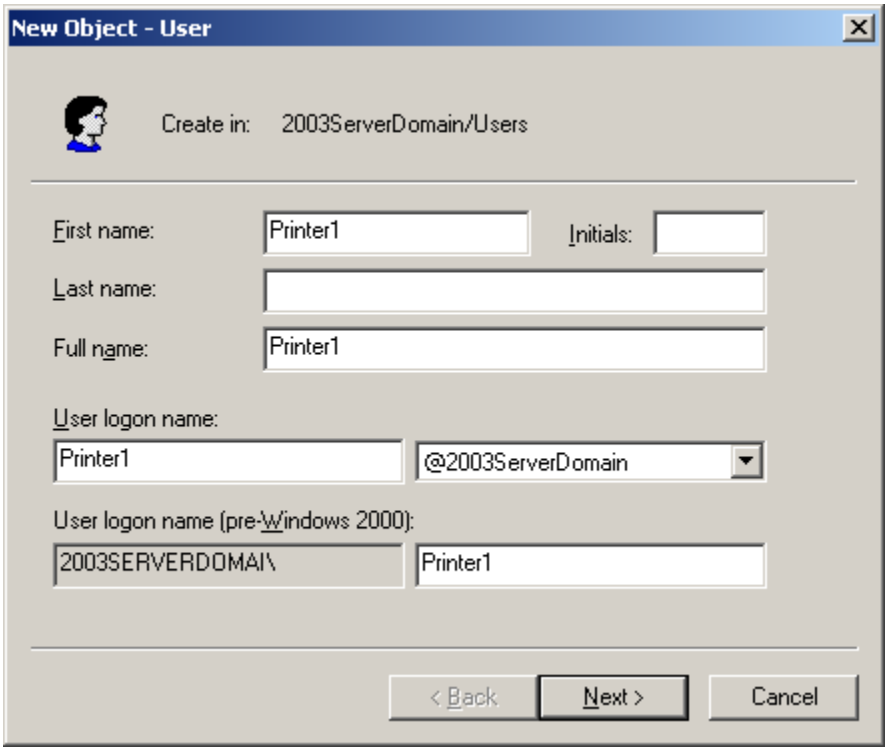


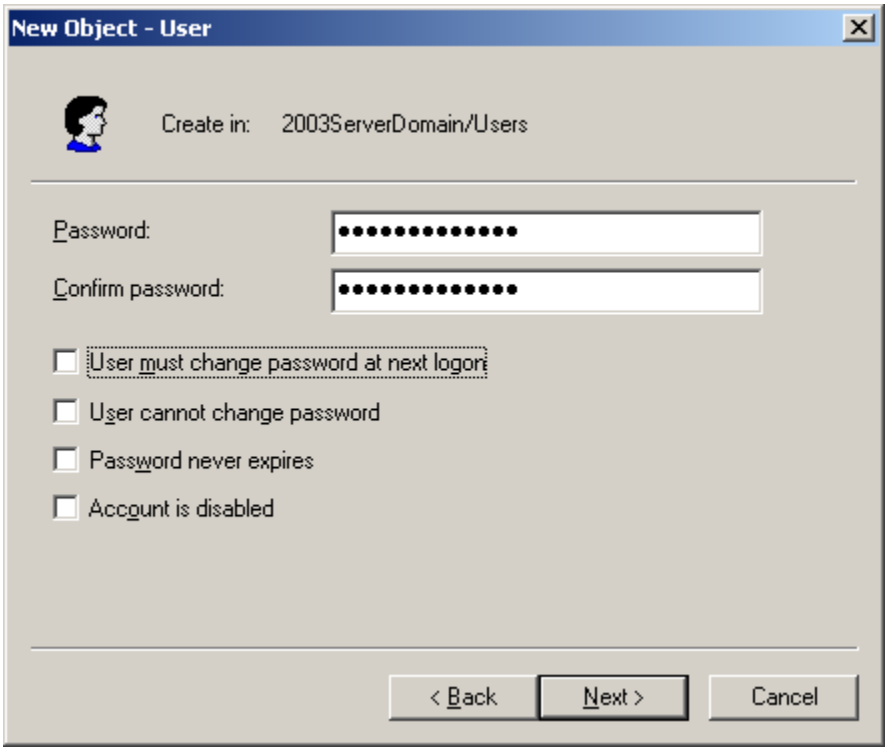

Protected EAP Properties
This server identifies itself to callers before the connection is completed.
Select the certificate that you want it to use as proof of identity.
Certificate issued
Lab2003Server.2003ServerDomain
Friendly name:
Issuer:
IAS
Expiration date:
7/22/2011 4:36:40 PM
Enable Fast Reconnect
Eap Types
Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add
Edit
Remove
OK
Cancel

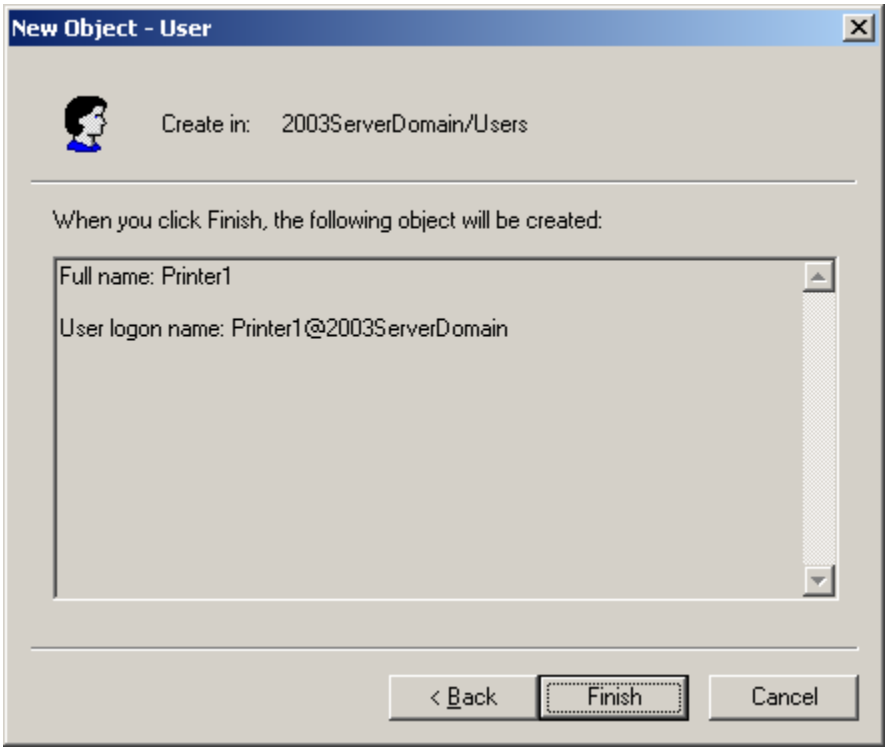

Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
Select the authentication methods you want to allow for this connection.
EAP Methods
Microsoft Encrypted Authentication version 2 (MS-CHAP v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Unauthenticated access
Allow clients to connect without negotiating an authentication method.
OK
Cancel
Apply

The next series of screenshots shows how one is able to add a user in the active directory. The username and password that is added in the active directory is the same username and password that is added on the printer.



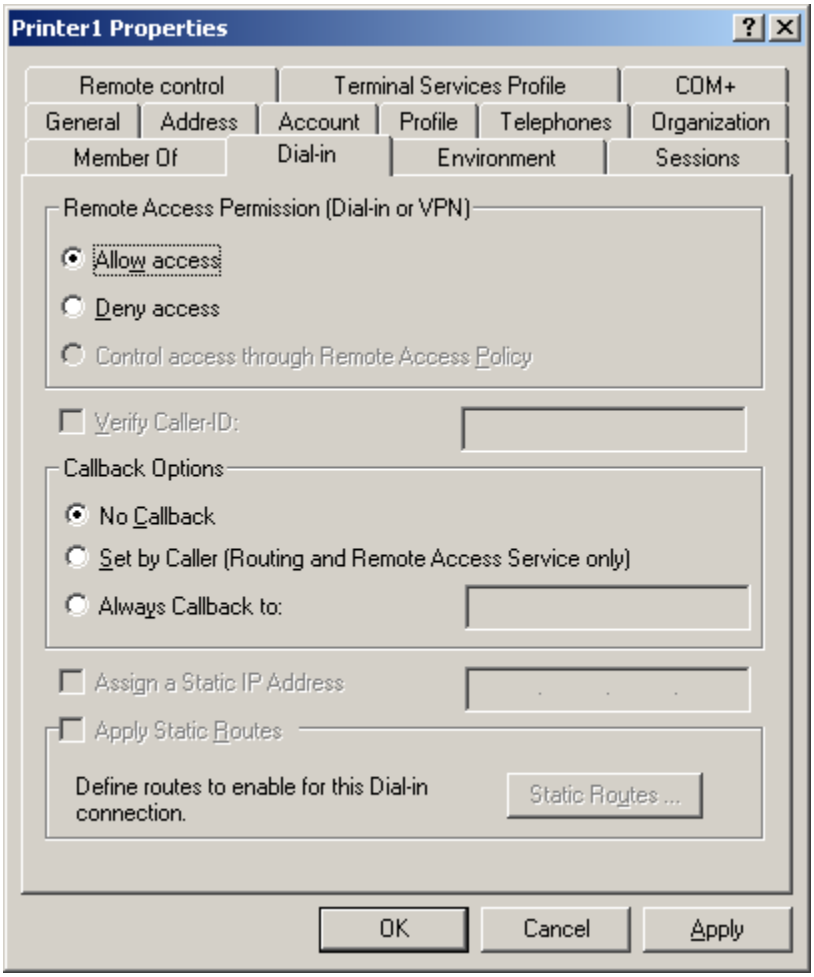

New Object - User
Create in: 2003ServerDomain/Users
First name: Printer1
Initials:
Last name:
Full name: Printer1
User logon name:
Printer1
@2003ServerDomain
User logon name (pre-Windows 2000):
2003SERVERDOMAI\
Printer1
< Back
Next >
Cancel


New Object - User
Create in: 2003ServerDomain/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel

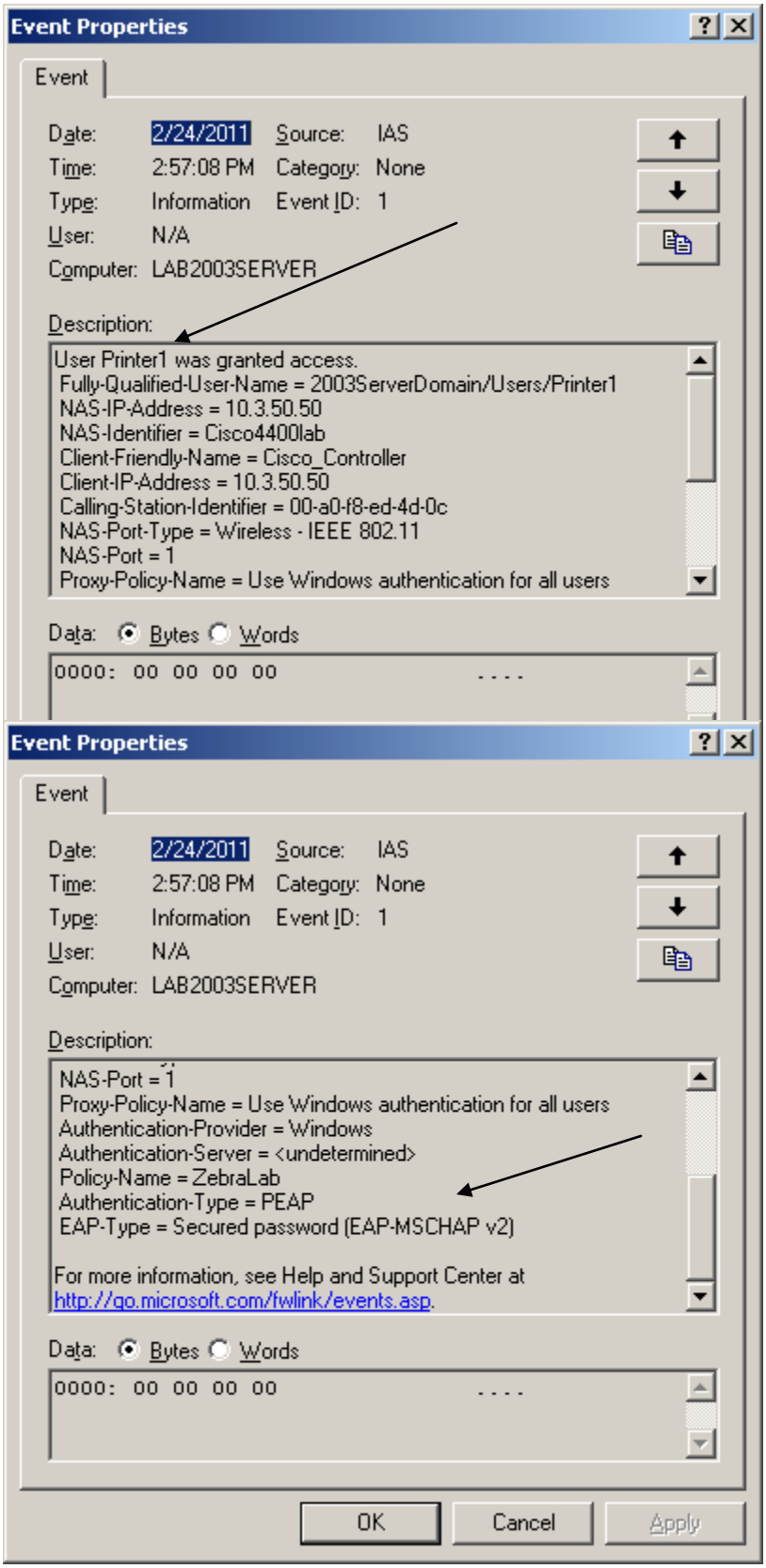


The following screenshot shows how the properties of the user is modified to grant dial-in permission.

The event log on the IAS server can be used for troubleshooting purposes.



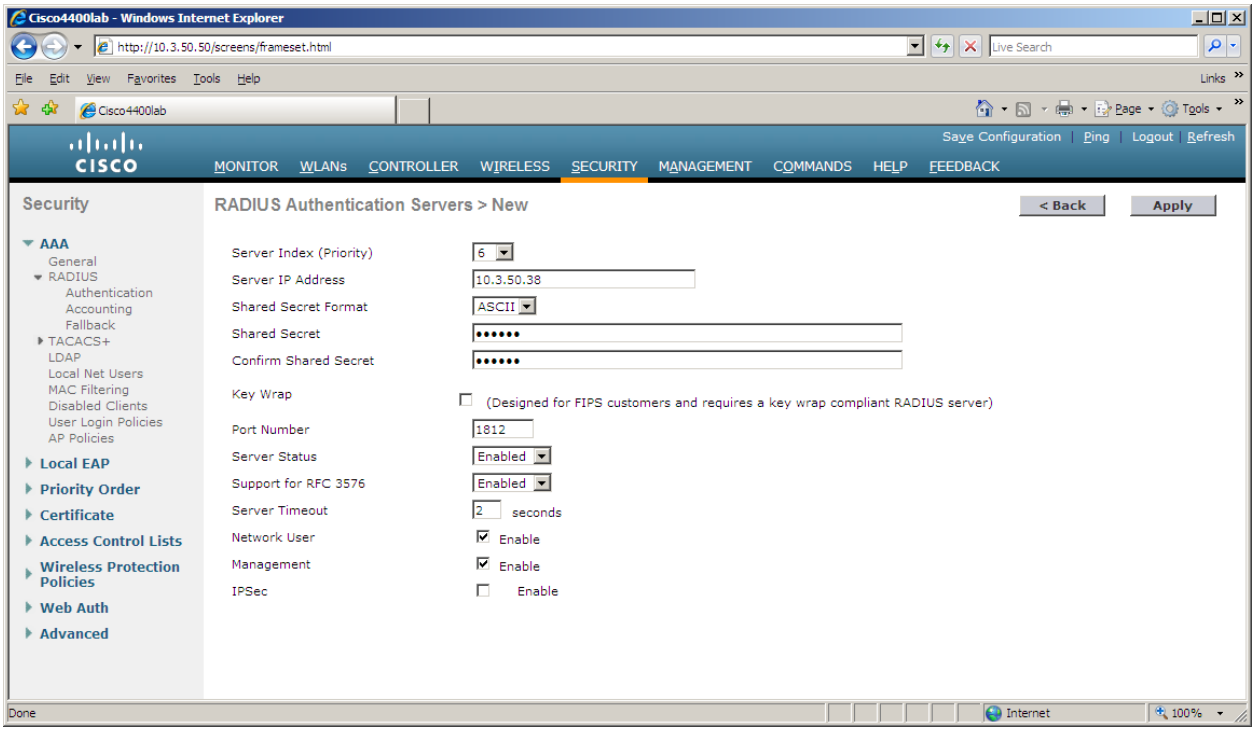
The Event Viewer on the IAS server can be used for troubleshooting purposes. In the screenshots below the event viewer is showing a successful authentication.


Event Properties
Event
Date: 2/24/2011 Source: IAS
Time: 2:57:08 PM Category: None
Type: Information Event ID: 1
User: N/A
Computer: LAB2003SERVER
Description:
User Printer1 was granted access.
Fully-Qualified-User-Name = 2003ServerDomain/Users/Printer1
NAS-IP-Address = 10.3.50.50
NAS-Identifier = Cisco4400lab
Client-Friendly-Name = Cisco_Controller
Client-IP-Address = 10.3.50.50
Calling-Station-Identifier = 00-a0-f8-ed-4d-0c
NAS-Port-Type = Wireless - IEEE 802.11
NAS-Port = 1
Proxy-Policy-Name = Use Windows authentication for all users
Data: Bytes Words
0000: 00 00 00 00 ....
Event Properties
Event
Date: 2/24/2011 Source: IAS
Time: 2:57:08 PM Category: None
Type: Information Event ID: 1
User: N/A
Computer: LAB2003SERVER
Description:
NAS-Port = 1
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = ZebraLab
Authentication-Type = PEAP
EAP-Type = Secured password (EAP-MSCHAP v2)
For more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp.
Data: Bytes Words
0000: 00 00 00 00 ....
OK
Cancel
Apply

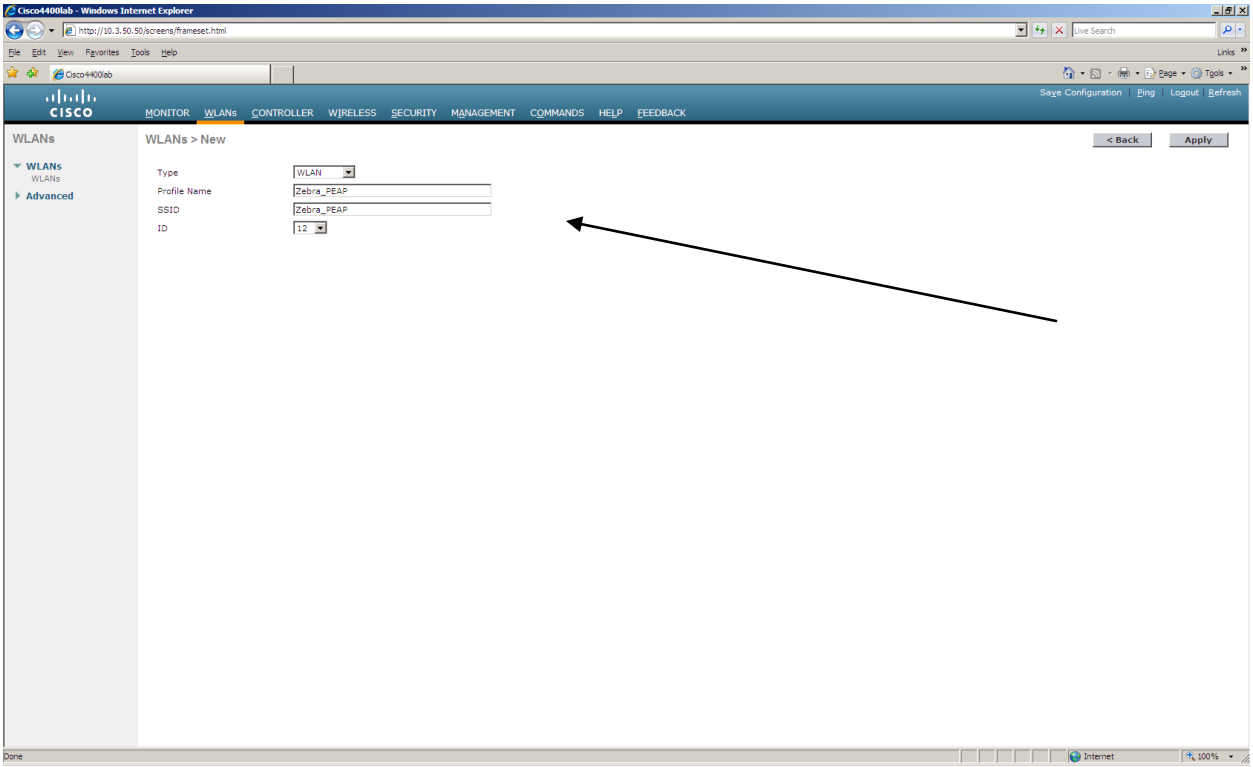
This section of the document illustrates a Cisco Wireless controller.
This document is meant as an illustration only. Questions on the setup of your Cisco controller should be directed to Cisco. It should be Cisco that is used to determine if the illustration below is appropriate for your environment

This illustration shows how the Cisco Controller was configured for PEAP initially and then WPA-PEAP.

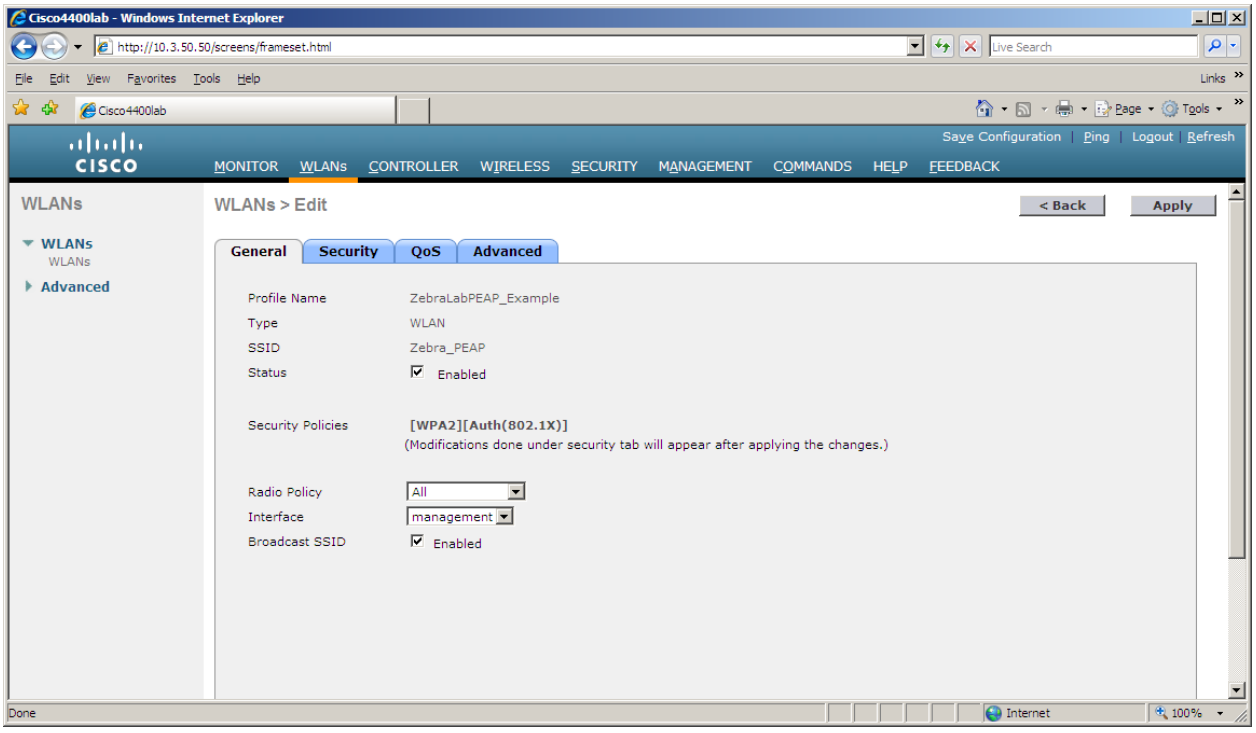
With PEAP or WPA-PEAP the authentication request is forwarded to a Radius server.
The following screenshots illustrate how a radius server can be added.
The example below shows an entry of a radius server with an IP address of 10.3.50.38 and utilizing the port number of 1812. 1645 and 1812 are common port numbers used with the RADIUS protocol. A secret key is also entered. This secret key needs to match the secret key that is entered on the RADIUS server.



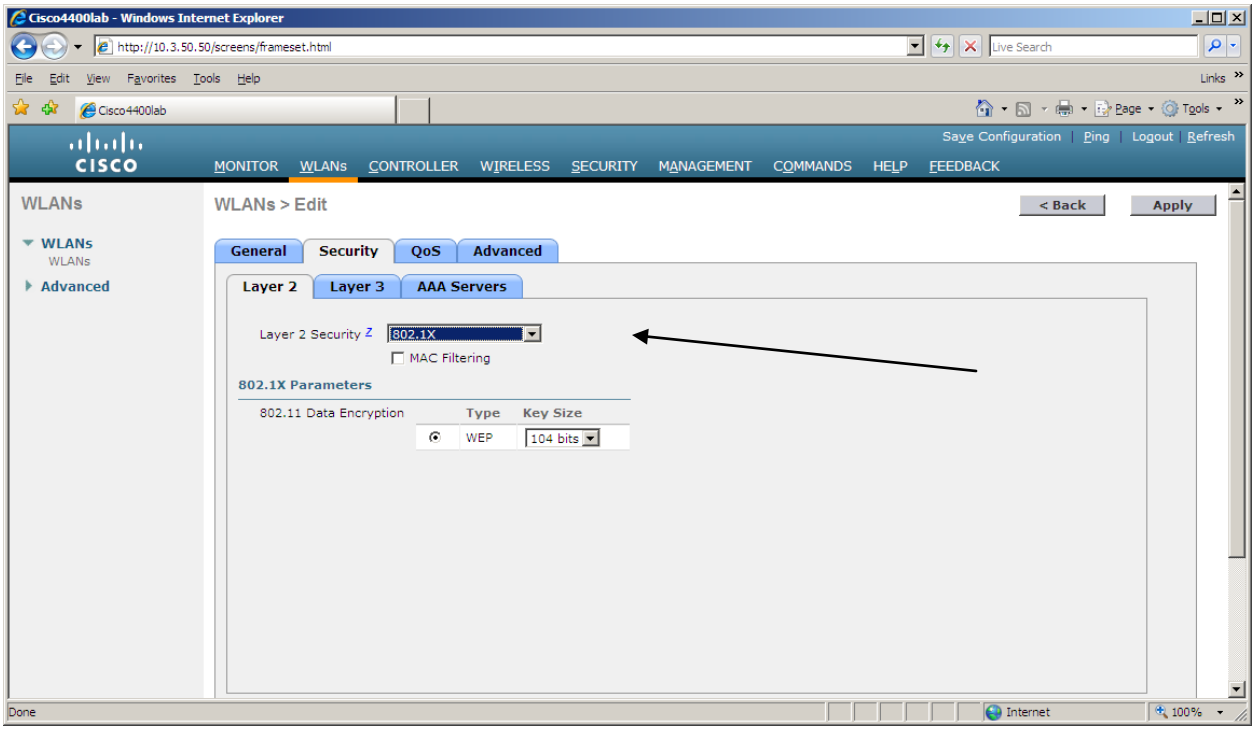
The first step illustrated here is how an ESSID is created.



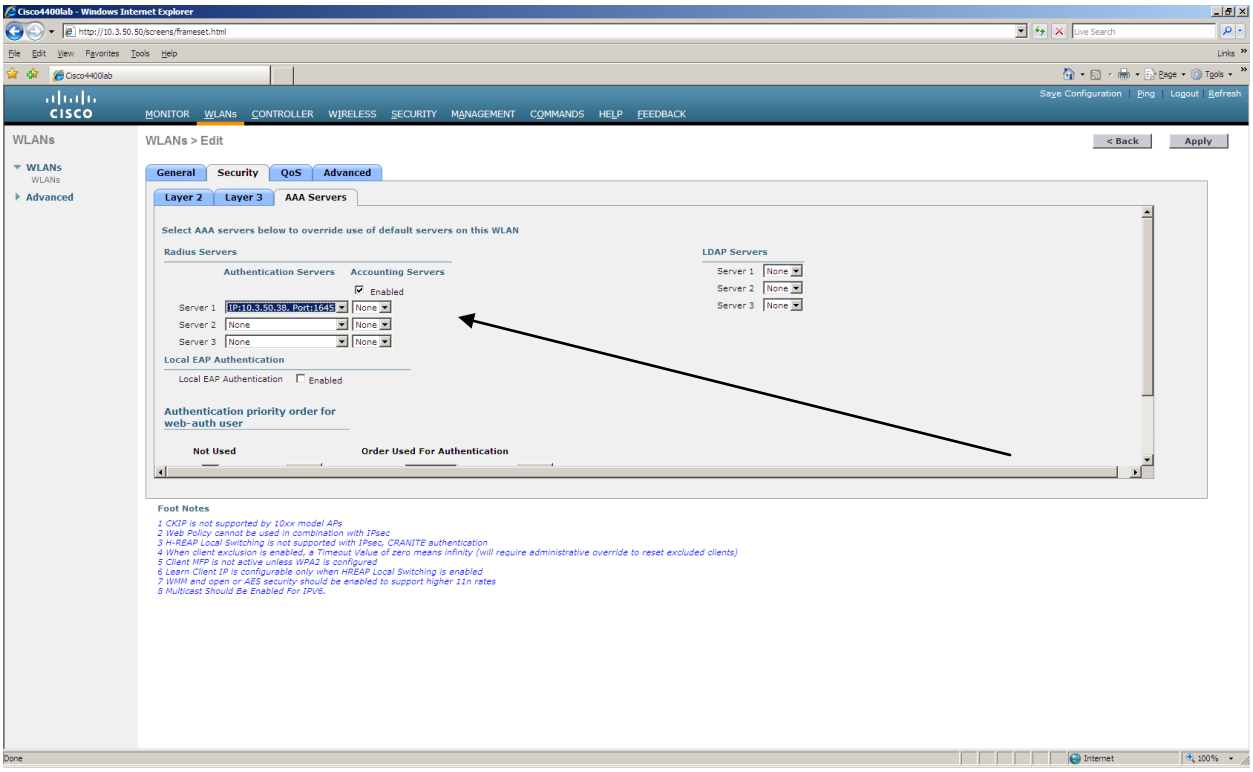
In this example the ESSID is “Zebra_PEAP” Please note that ESSID’s are case sensitive.



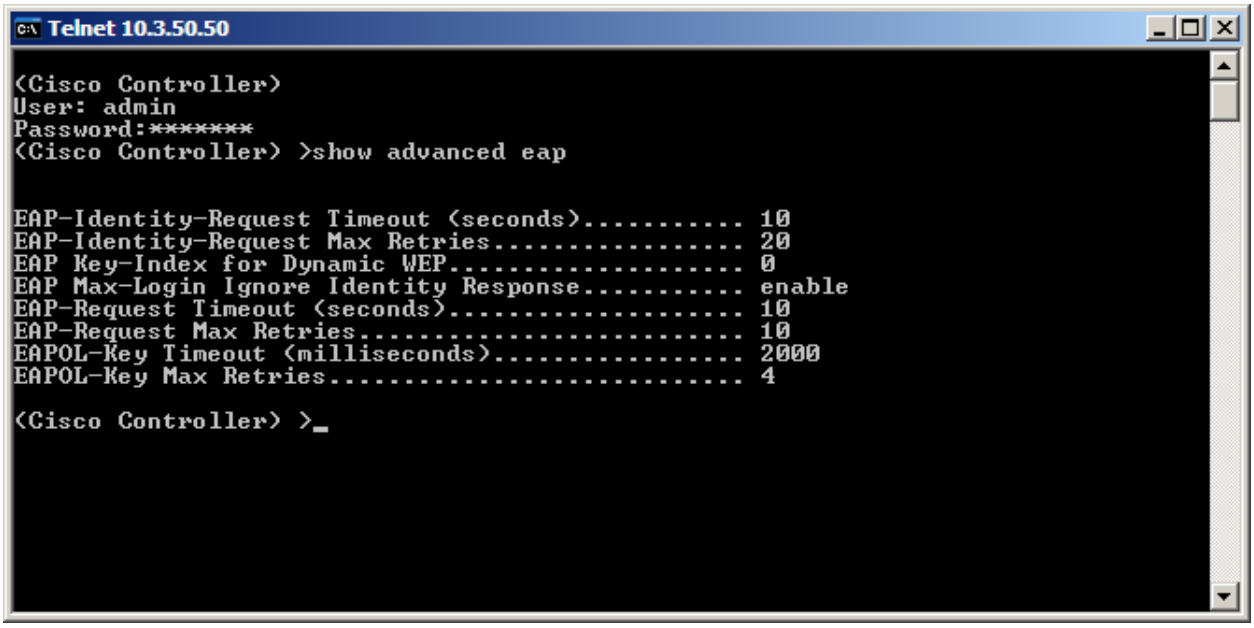
This screenshot shows how to configure **802.1x (PEAP)**



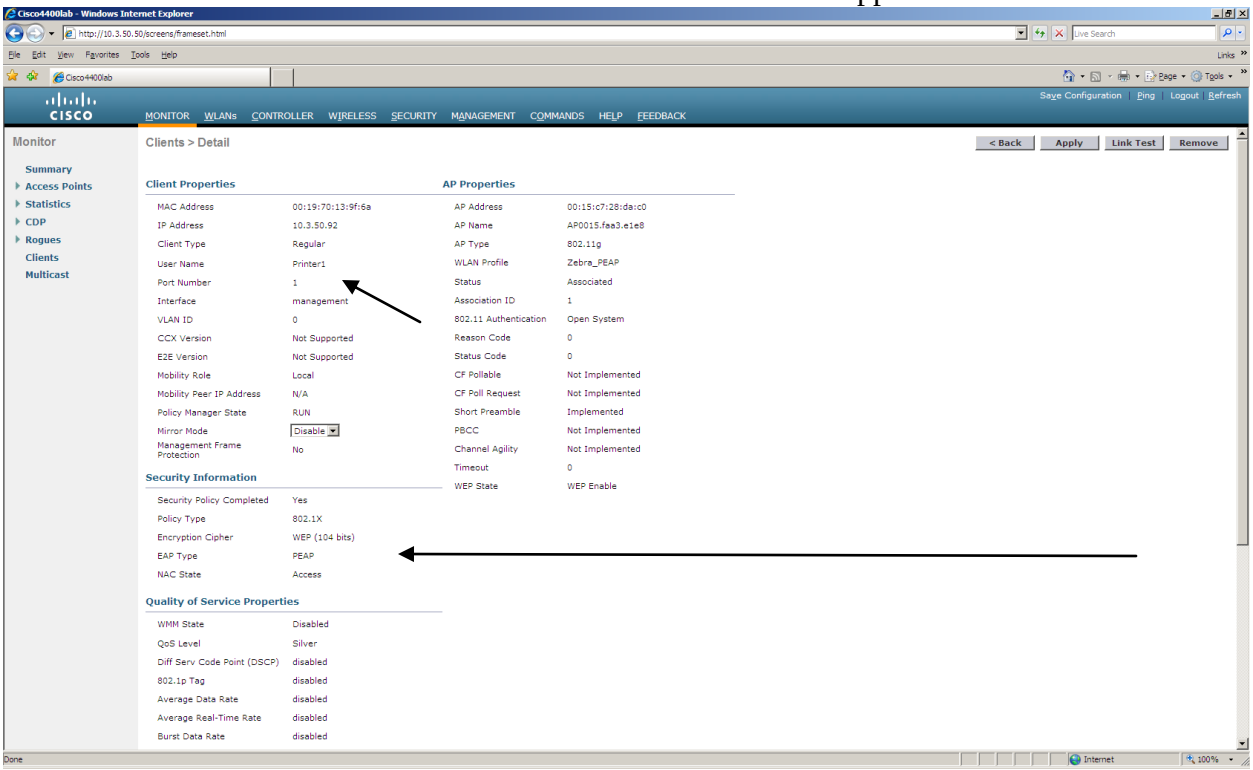
The next screen is showing where the controller is passing the authentication packets to.



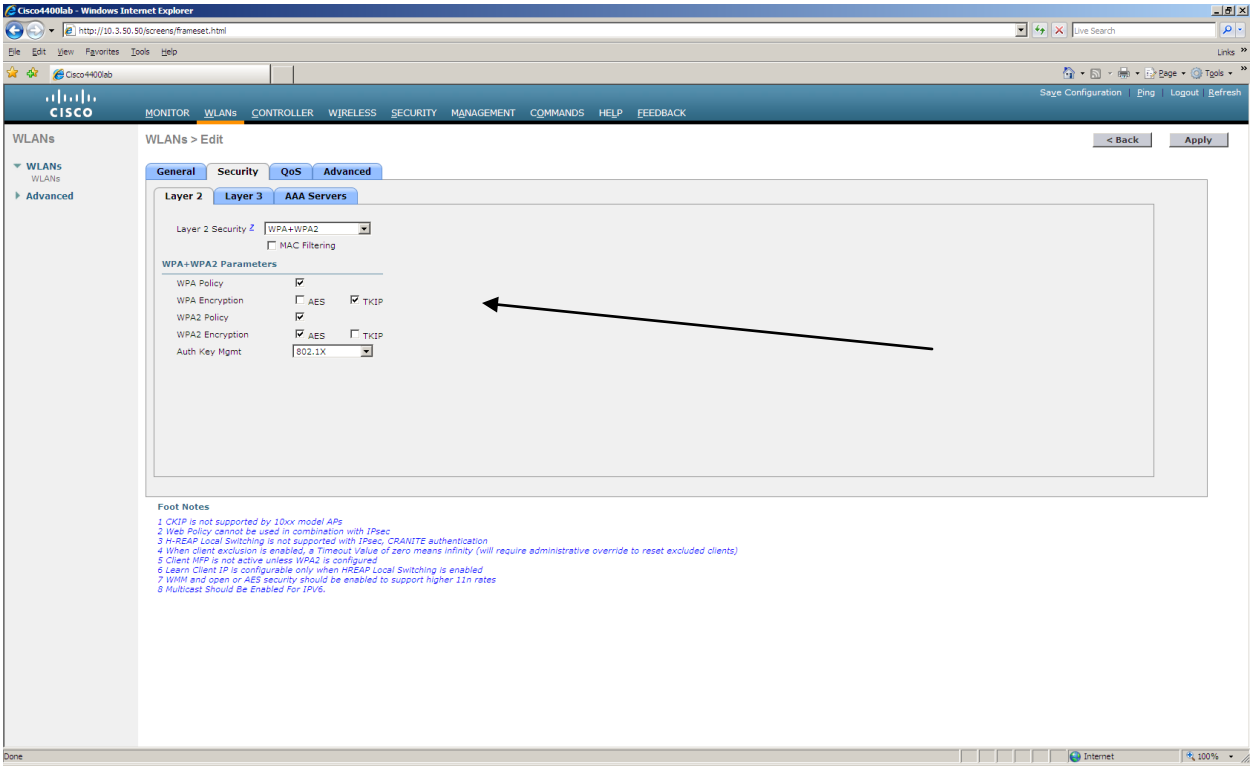
The screenshots below show the advanced eap settings used in the illustration.
Please consult with Cisco to determine the appropriate values for your environment.



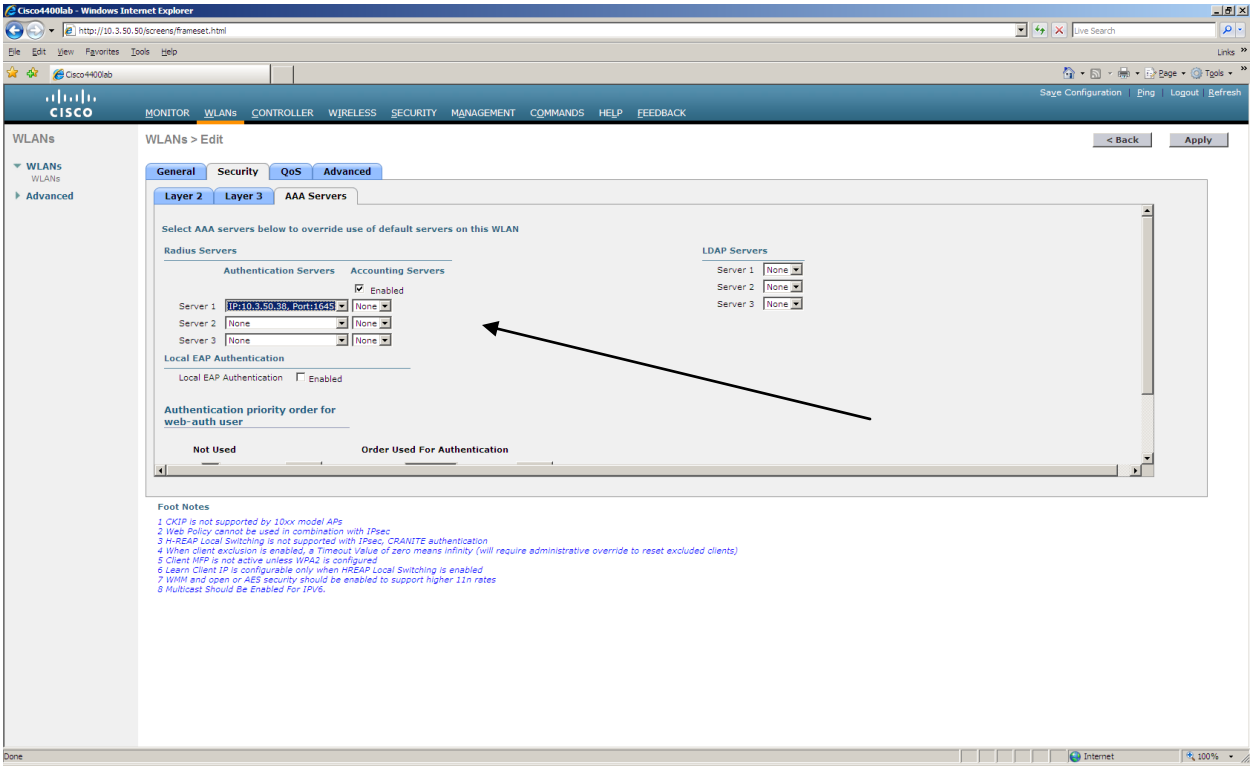
The screenshots below show what a successful PEAP connection appears on the controller.



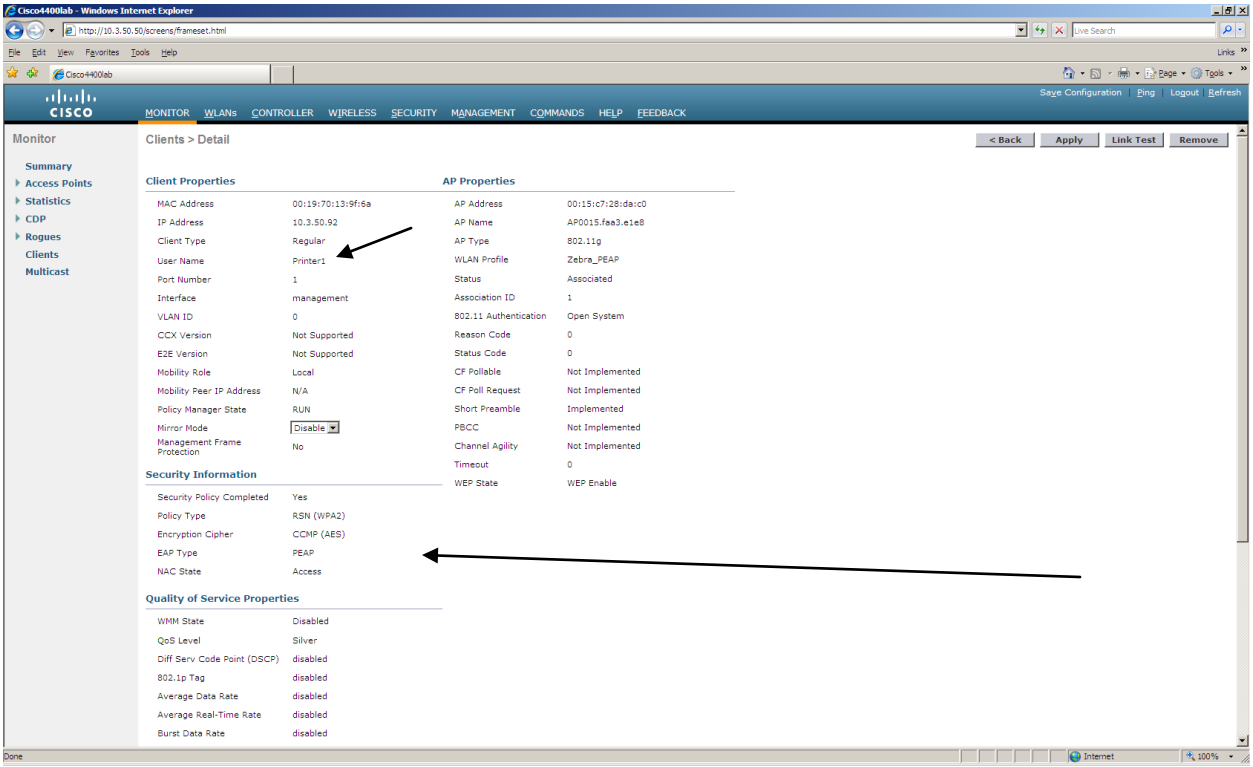
The next screenshots show how the controller was set for **WPA-PEAP.** In this example that I have enabled both wpa and wpa2 as shown below.



With WPA-PEAP, the authentication is often done by an external radius server.
In this example I have entered the ip address for the radius server as shown below.

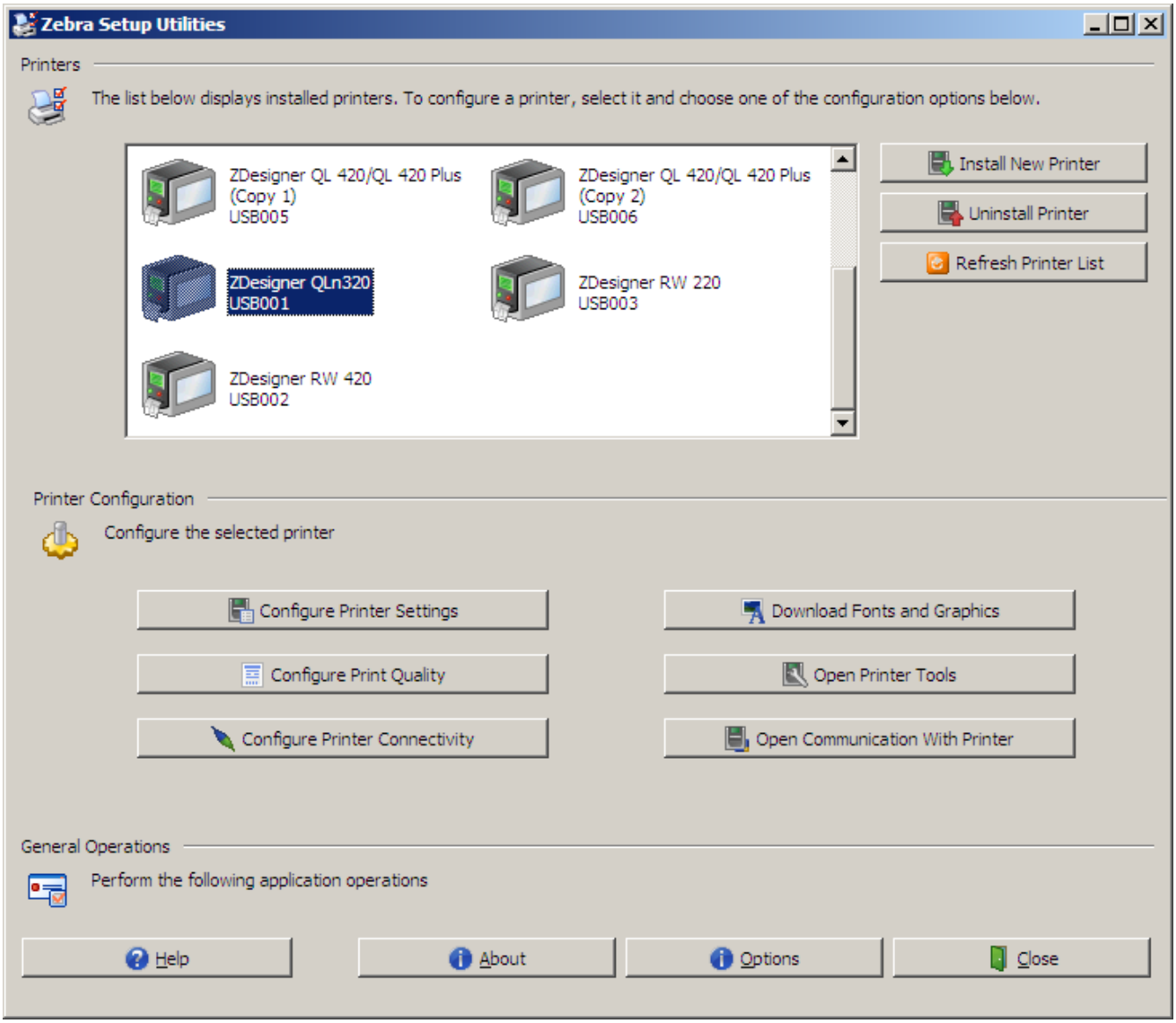


Below is an example of what the controller shows for a successful WPA-PEAP authentication.

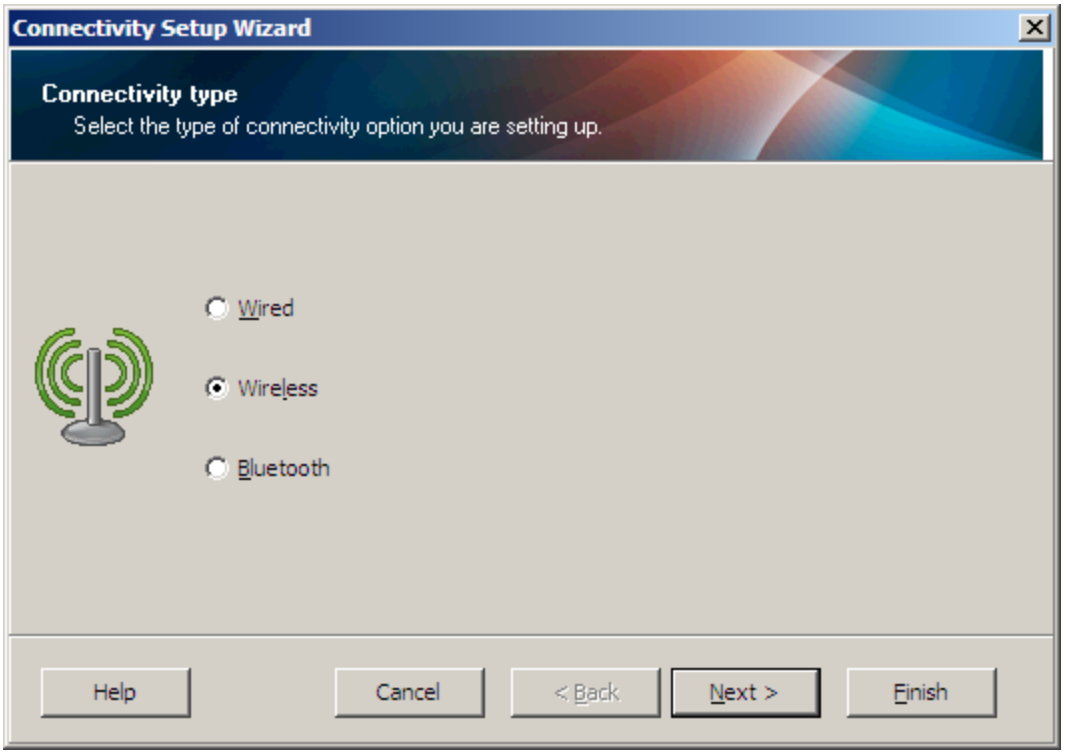


This section of the document illustrates how to configure the printer for PEAP and will continue by illustrating how to configure the printer for WPA-PEAP. The illustration will use the **Zebra Setup utility** as the method for configuring the printer.

This section of the document illustrates how to configure the printer for PEAP and will continue by illustrating how to configure the printer for WPA-PEAP. The illustration will use the **Zebra Setup utility** as the method for configuring the printer.

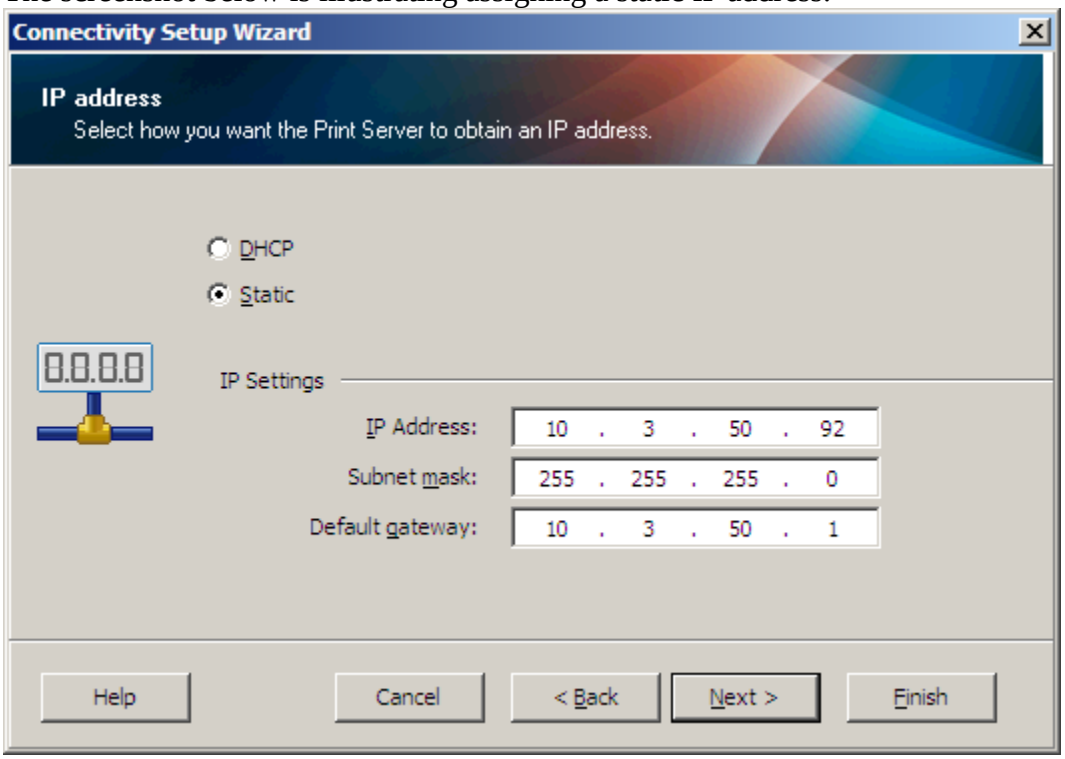


Click on Configure Printer Connectivity

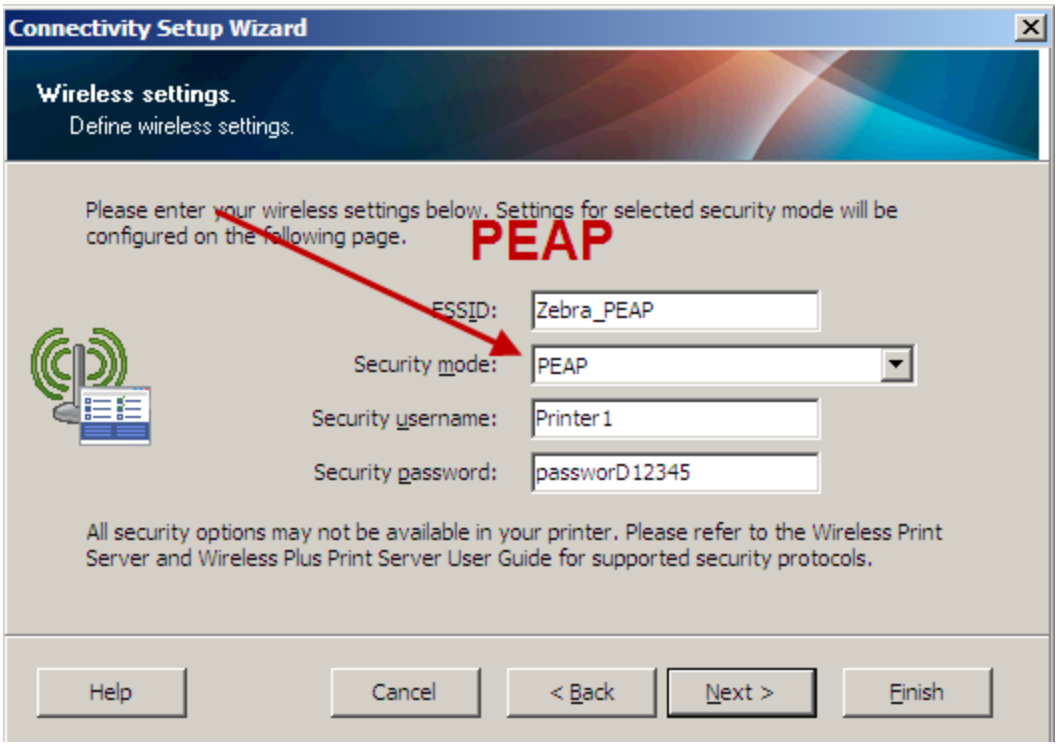


Choose Wireless

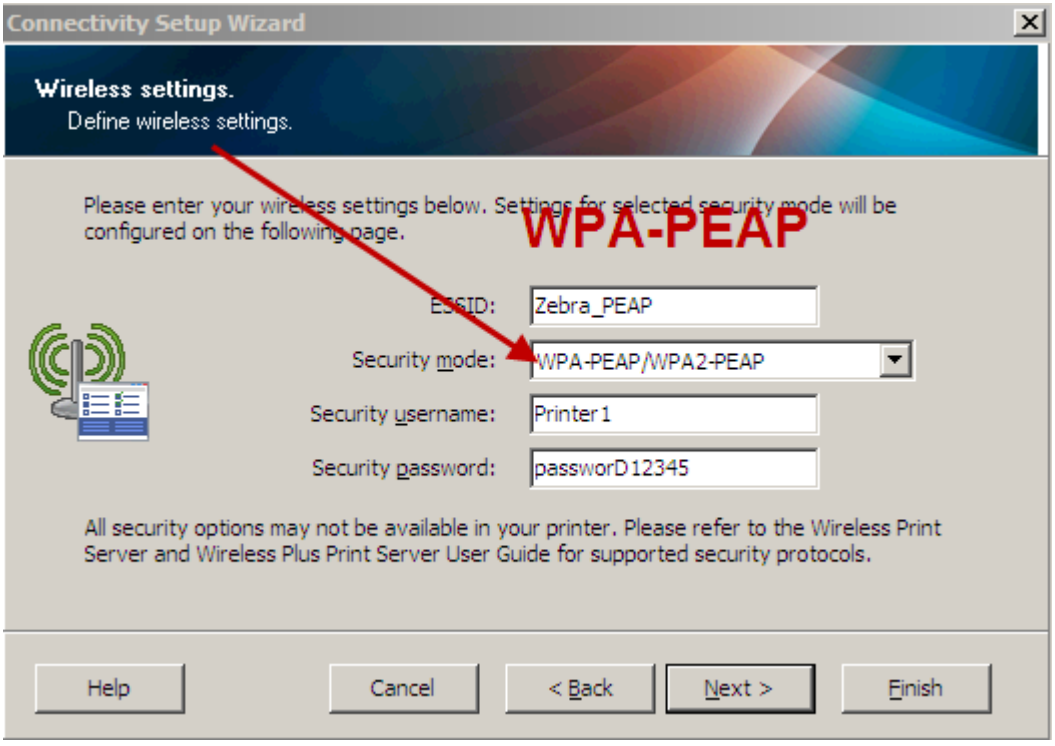
The screenshot below is illustrating assigning a static IP address.

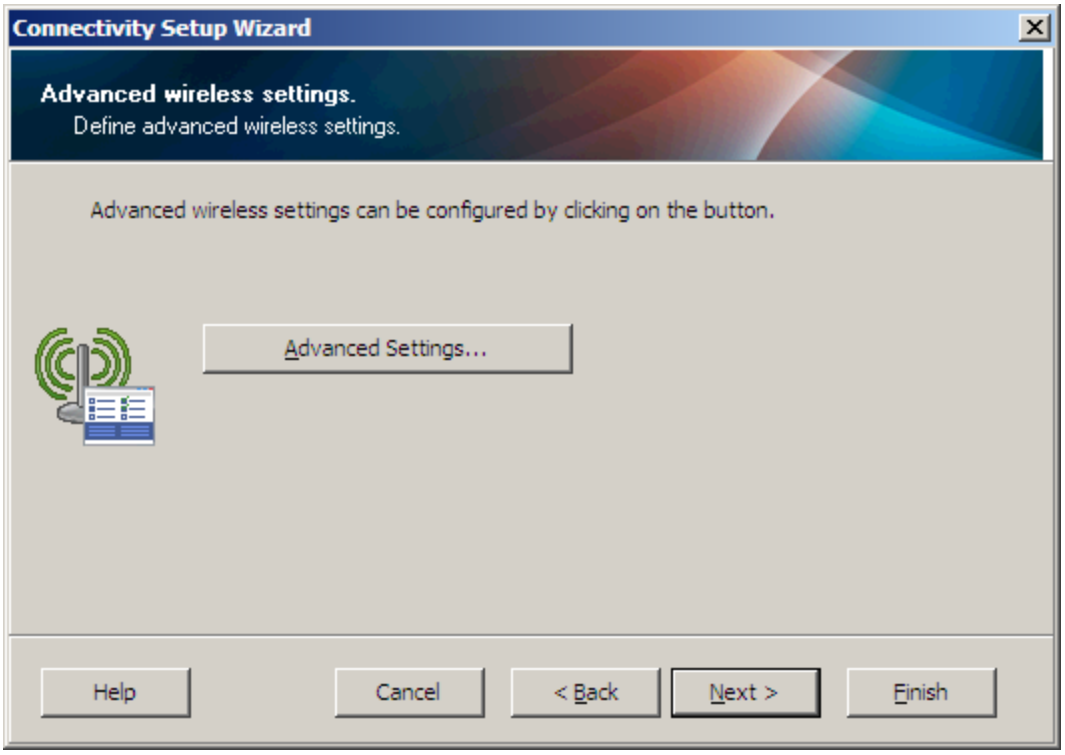


The screenshot below shows a 802.1x PEAP connection

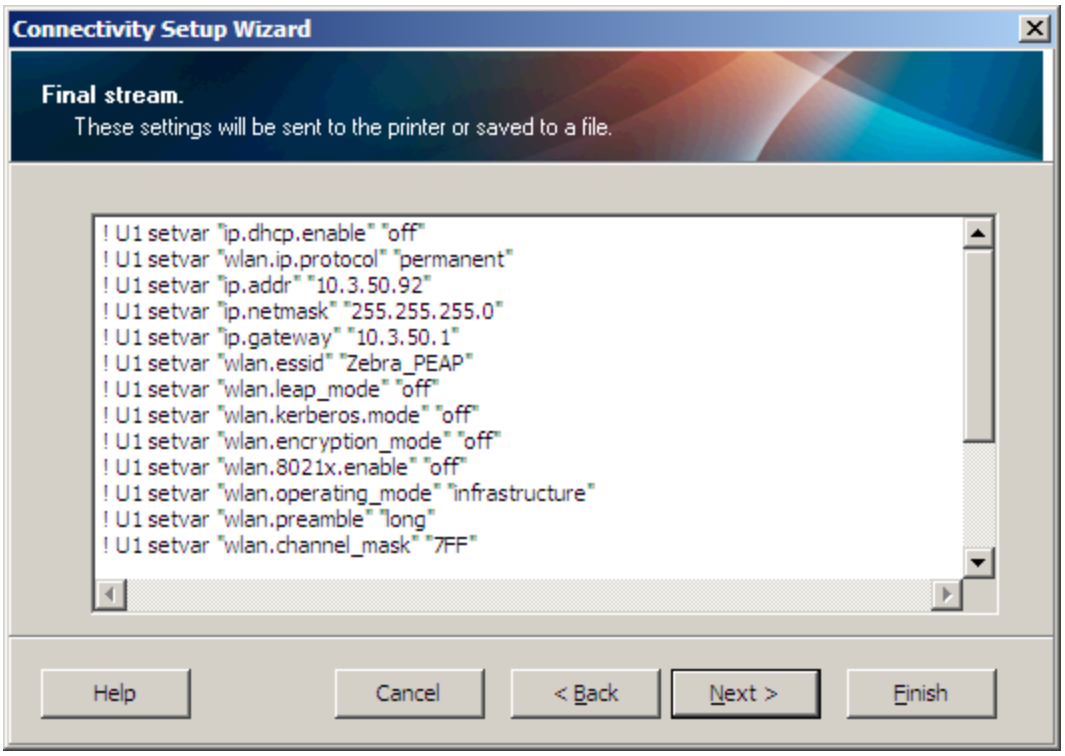


The screenshot below shows a WPA-PEAP connection

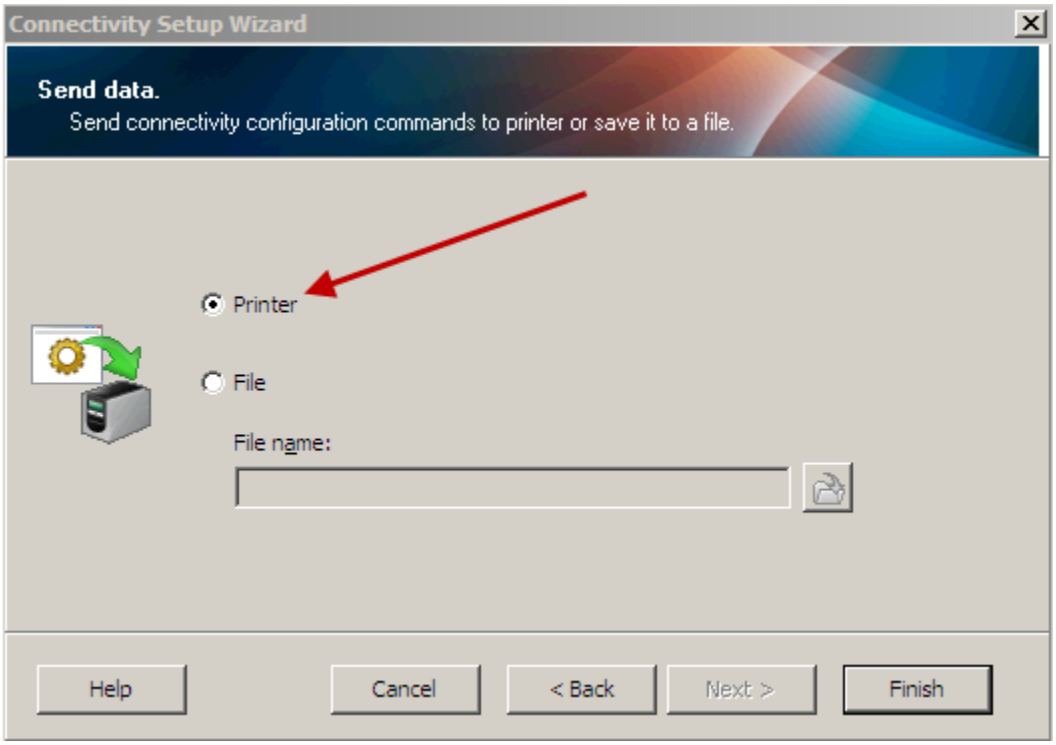




Choose NEXT



Choose NEXT



Choose Printer then FINISH

The wireless setup commands will be sent directly to the printer and the printer will reboot.