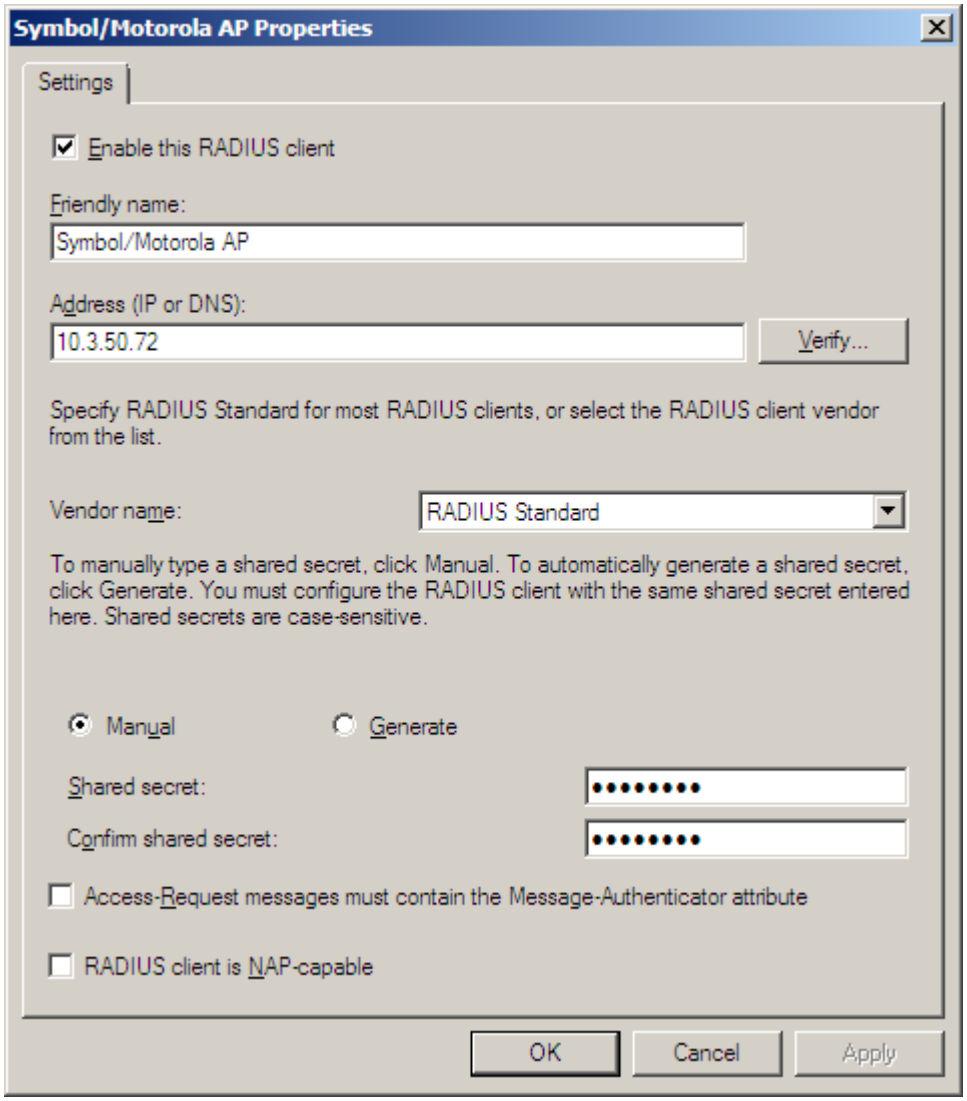
Zebra Setup Utility, Zebra Mobile Printer, NPS, Symbol / Motorola Access point, PEAP and WPA-PEAP

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

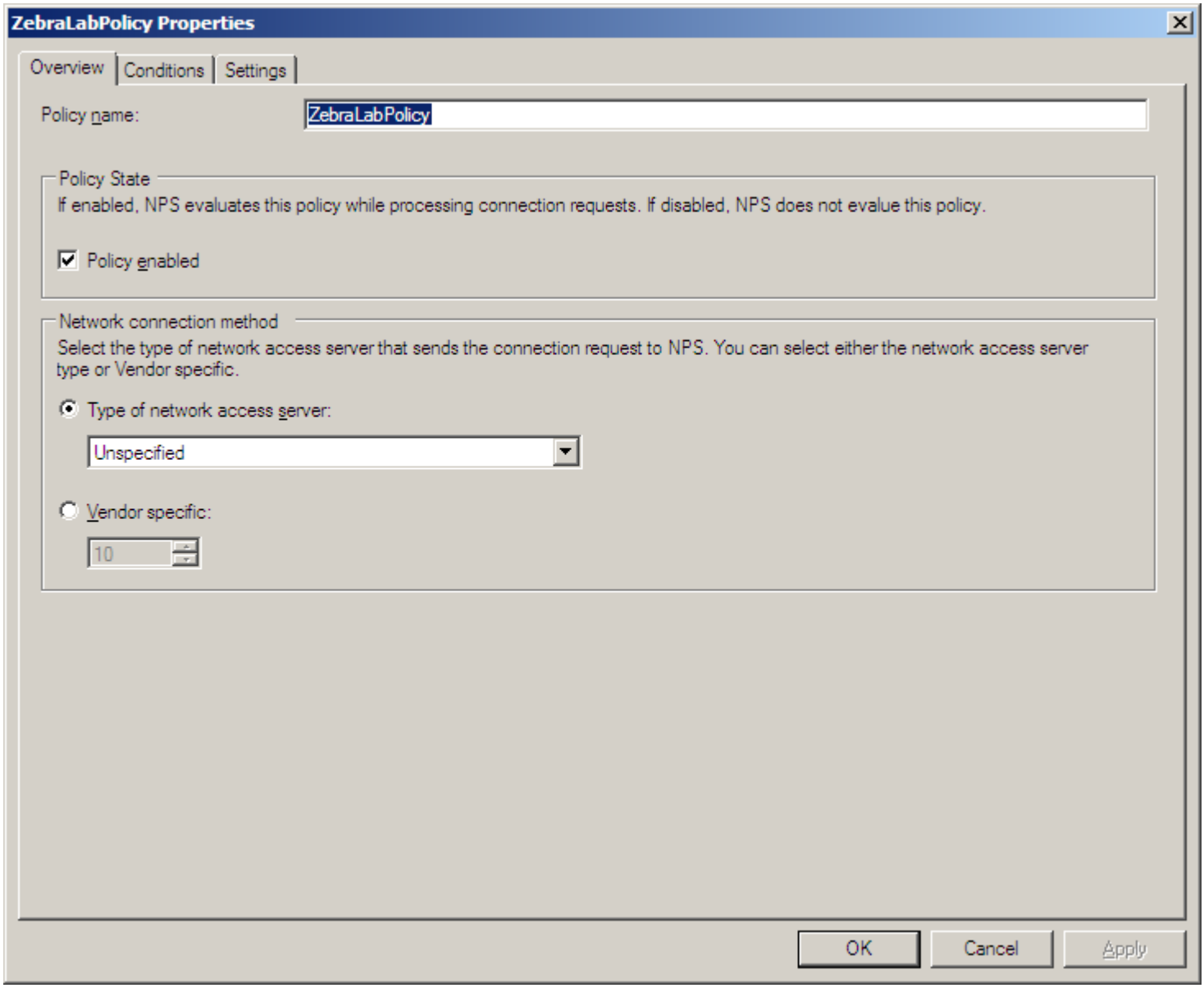
It is important to note that the setup on the NPS server did not differ when using WPA-PEAP or PEAP.

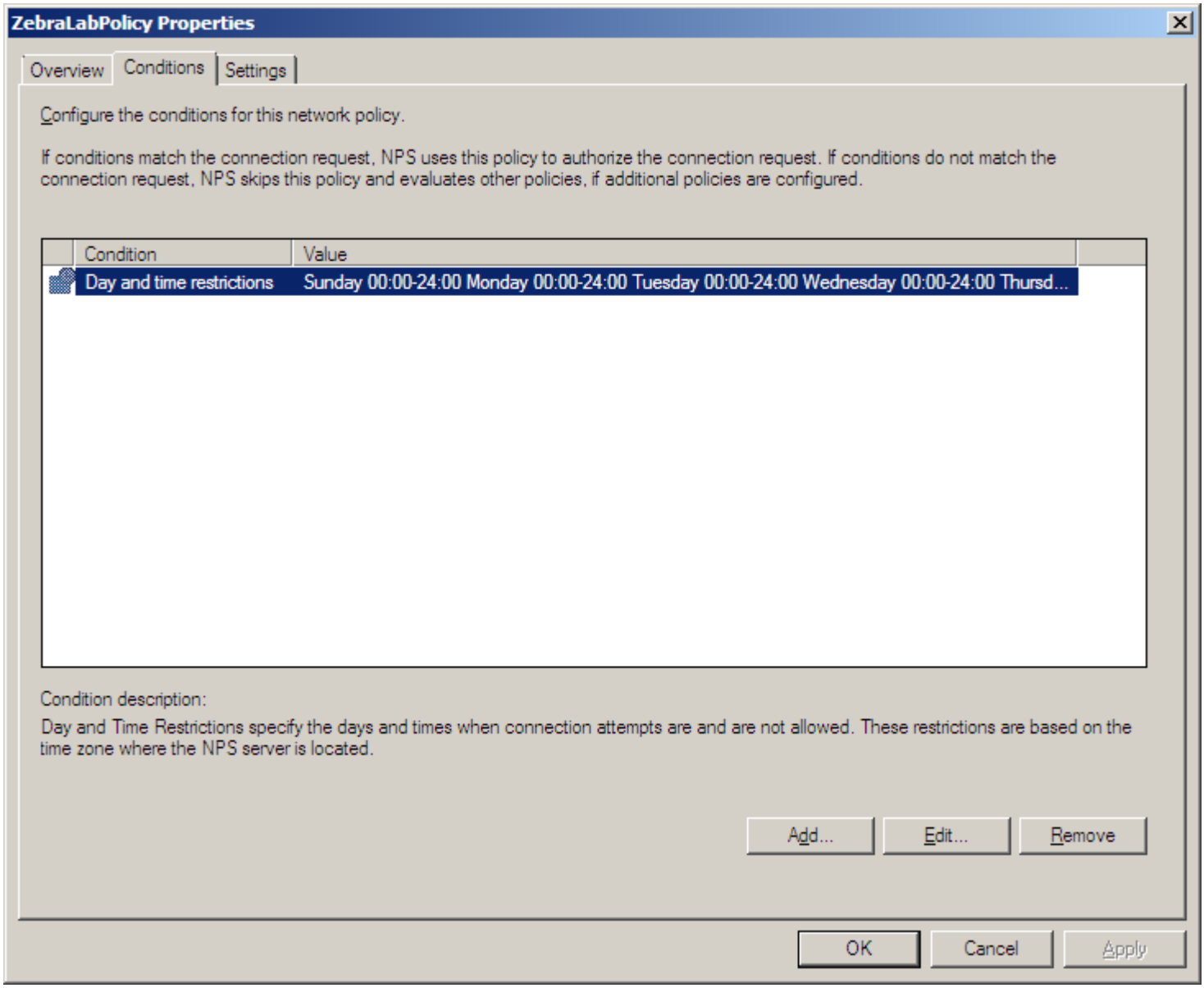
The first series of screenshots shows how a Radius client is added to NPS. In the screenshot below a Symbol / Motorola access point with the IP address of 10.3.50.72 is added. The NPS server needs to have a client in the clients table to ensure that authentication requests are only being received from valid clients.

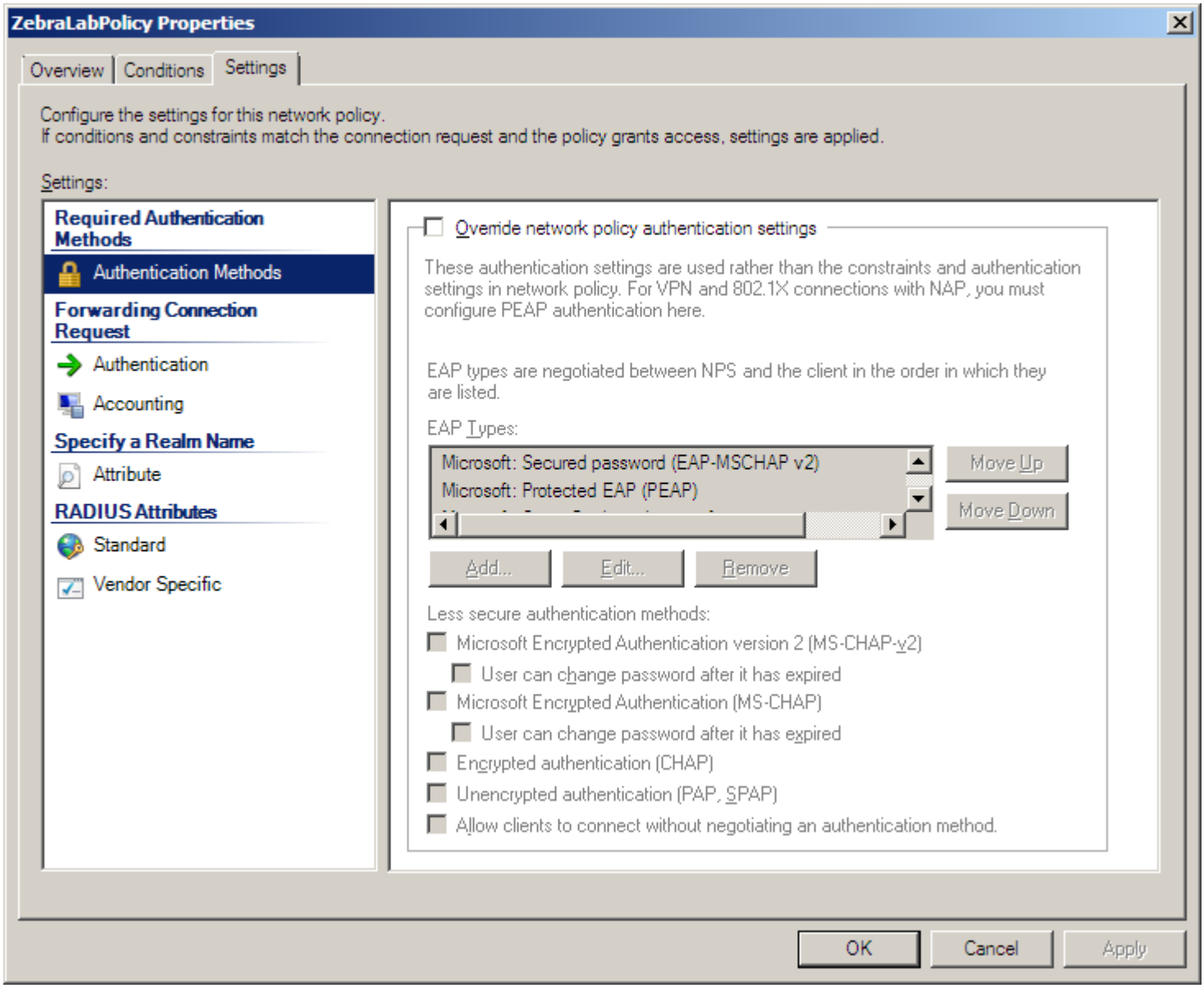
There is a shared secret key that must be entered. This secret key must match the secret key that is on the NAS device (In this example the Symbol / Motorola Access Point)

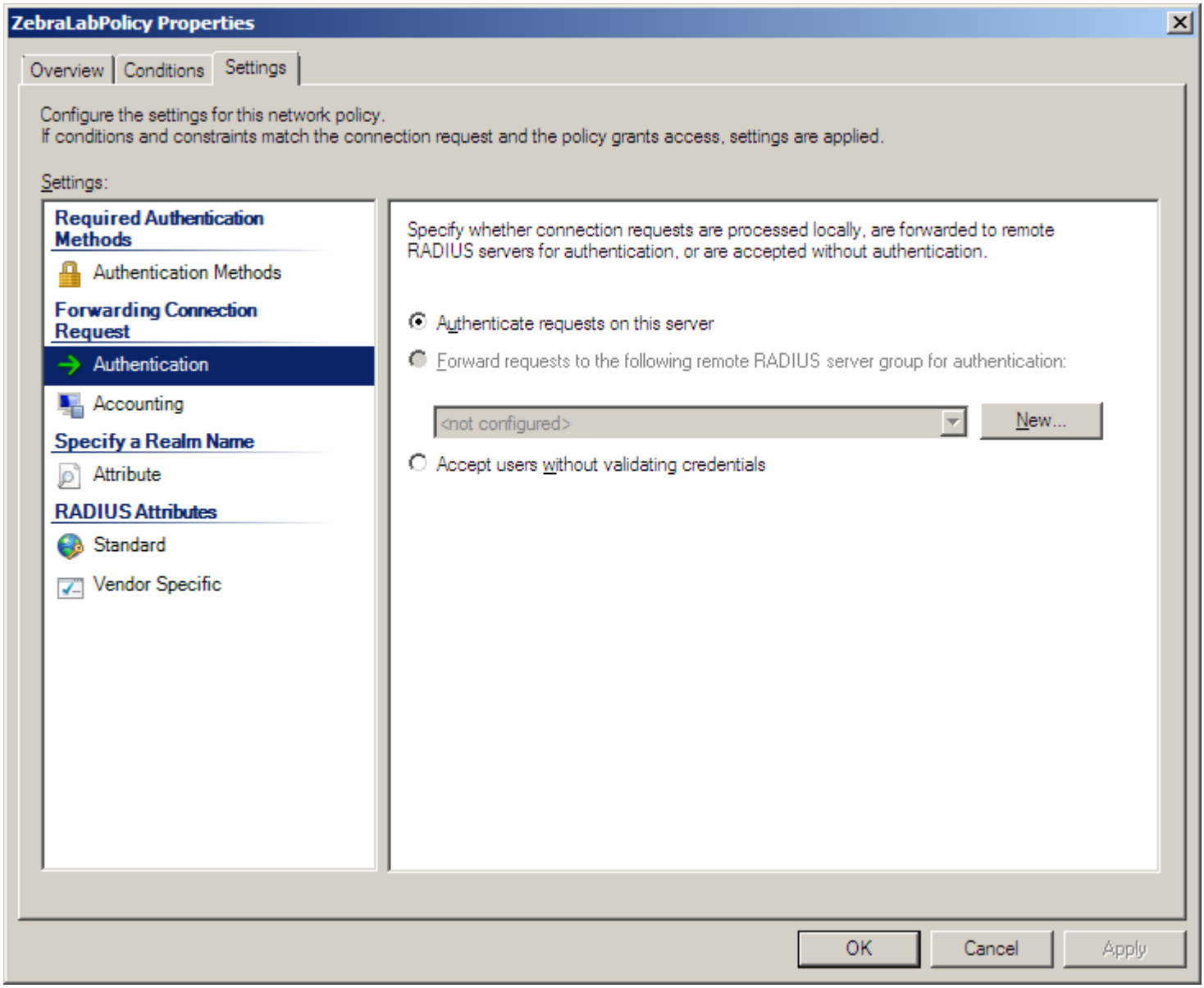


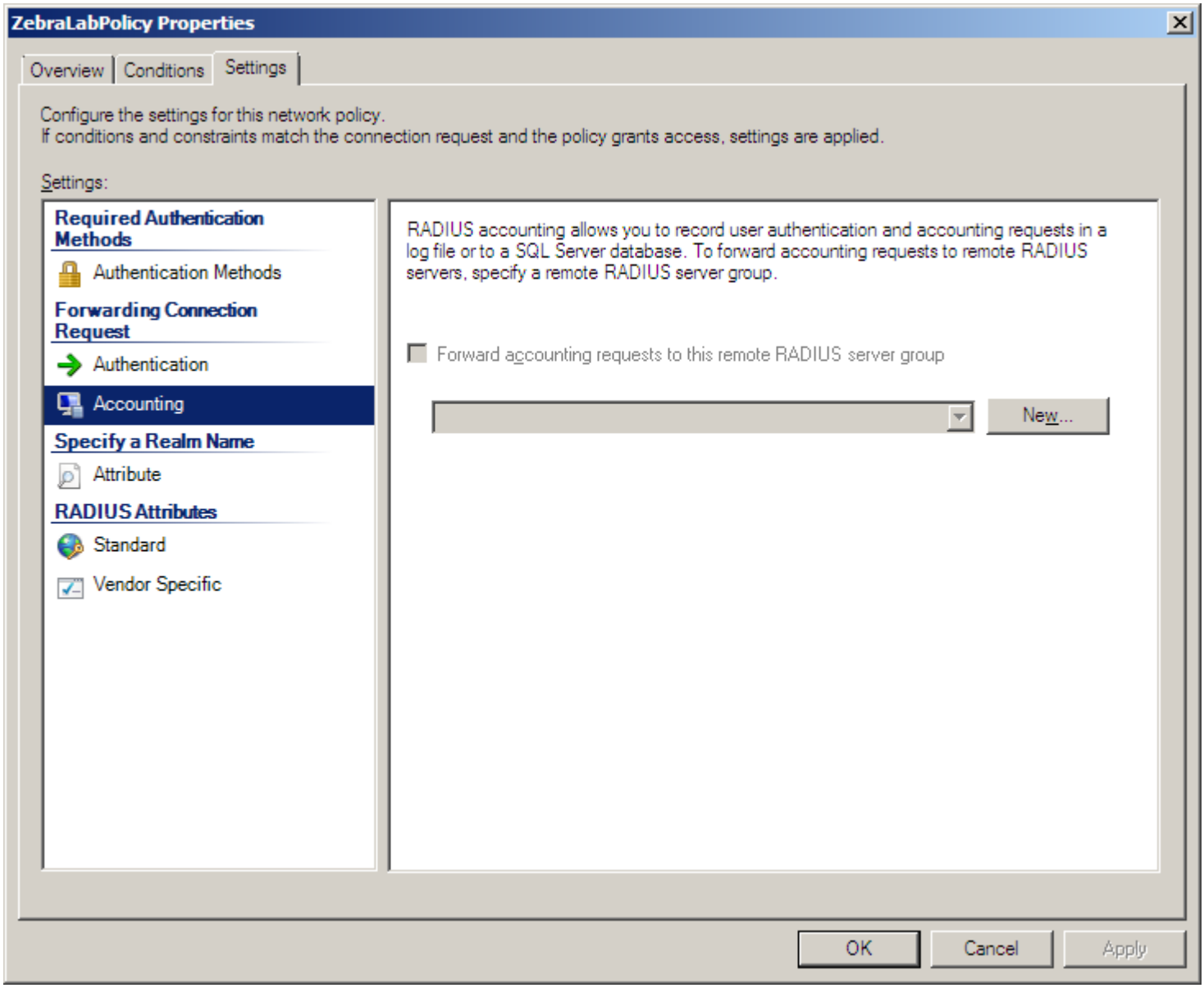
A connection policy for the NPS server is illustrated below.


ZebraLabPolicy Properties
Overview
Conditions
Settings
Policy name:
ZebraLabPolicy
Policy State
If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy.
Policy enabled
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.
Type of network access server:
Unspecified
Vendor specific:
10
OK
Cancel
Apply

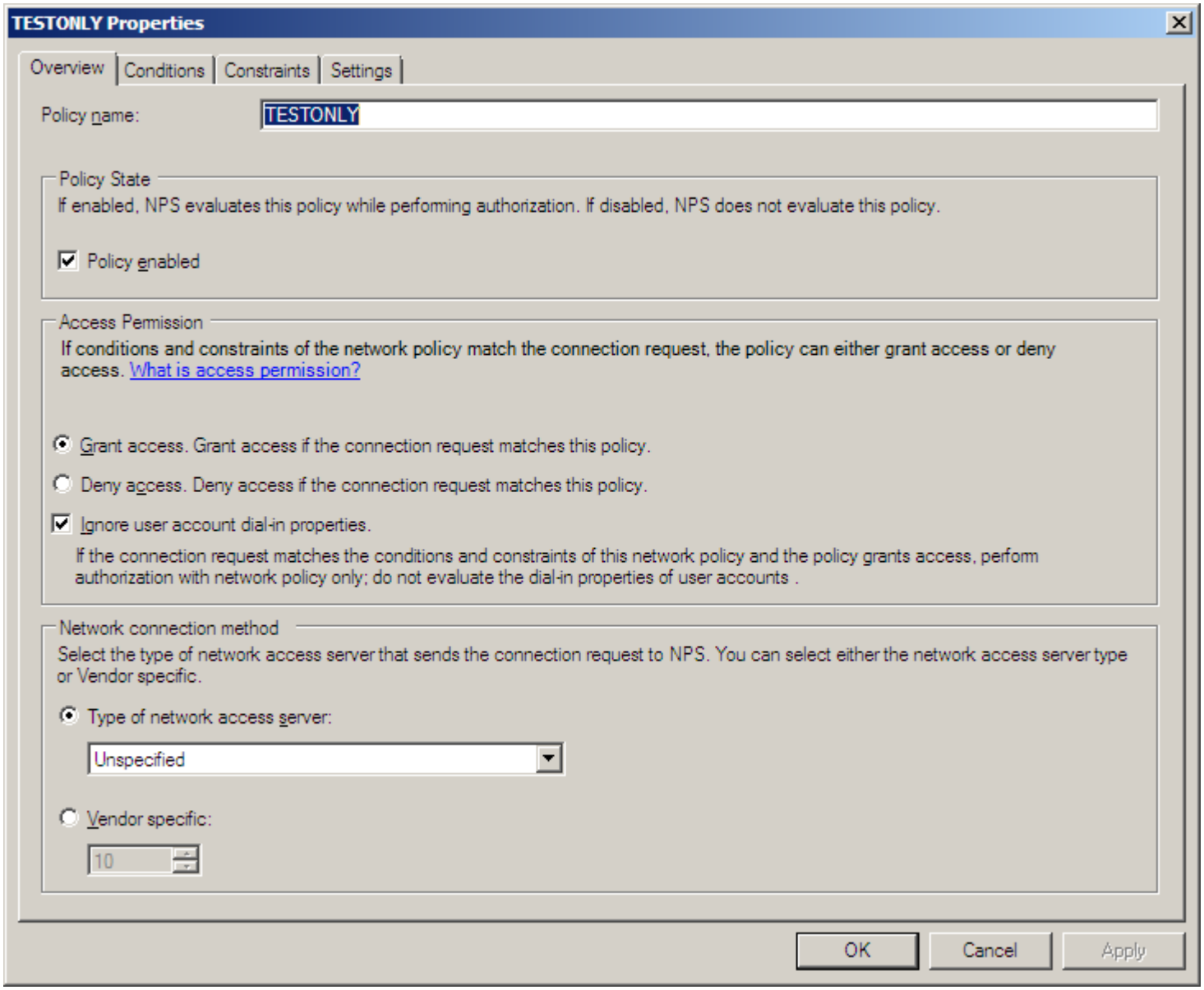

ZebraLabPolicy Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
Day and time restrictions
Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursd...
Condition description:
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.
Add...
Edit...
Remove
OK
Cancel
Apply

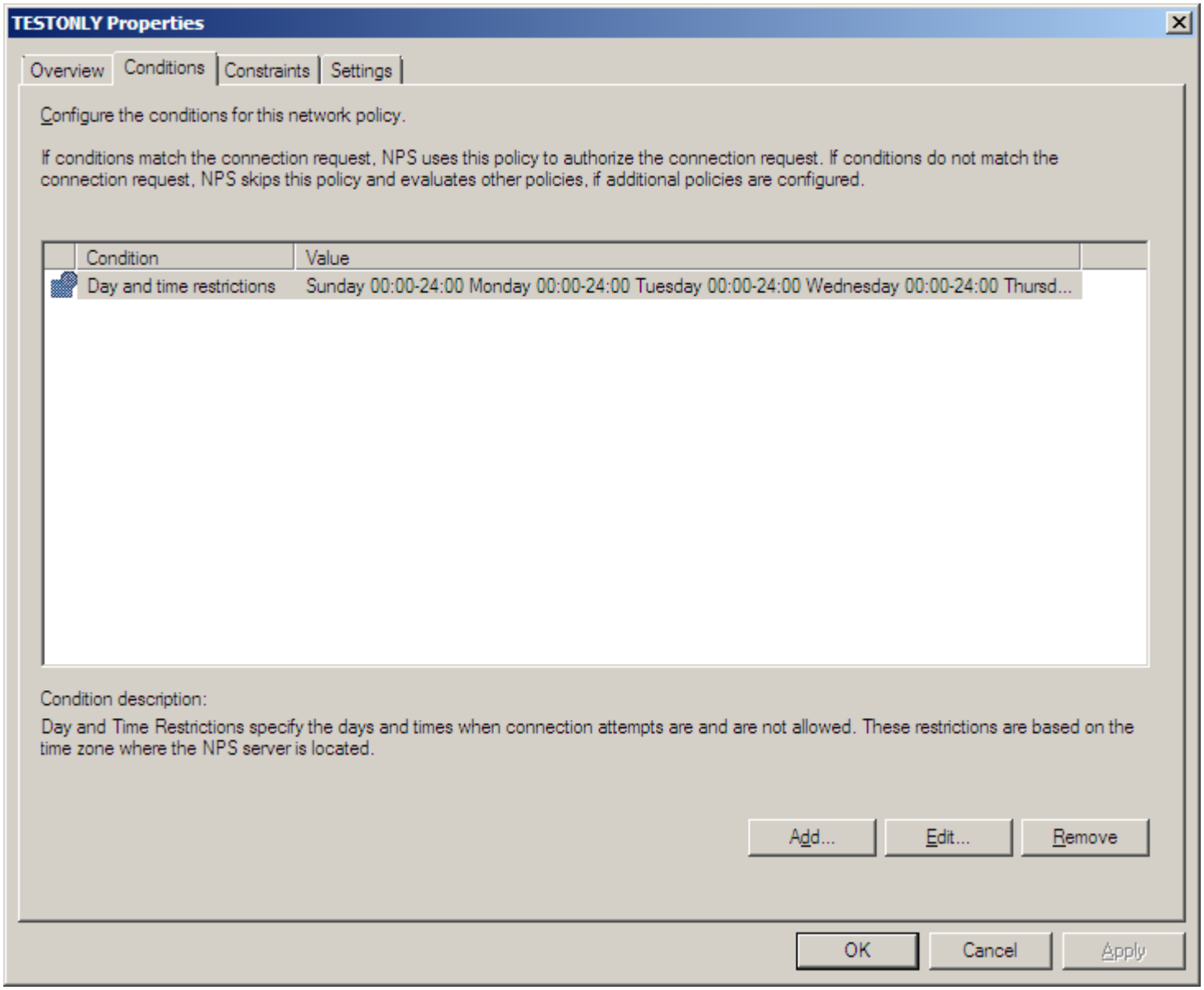

ZebraLabPolicy Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Vendor Specific
Override network policy authentication settings
These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Secured password (EAP-MSCHAP v2)
Microsoft: Protected EAP (PEAP)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication 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)
Allow clients to connect without negotiating an authentication method.
OK
Cancel
Apply

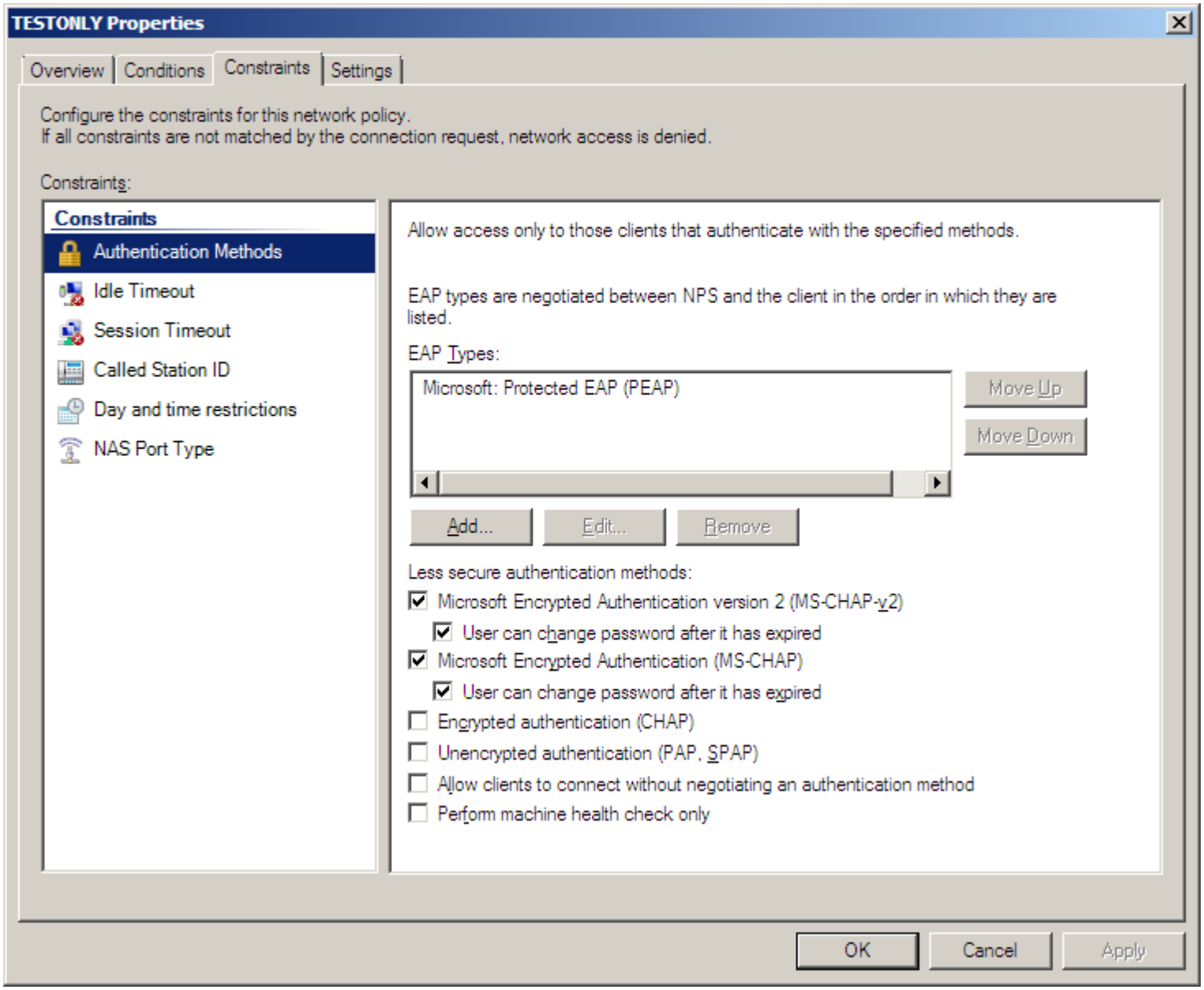

ZebraLabPolicy Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Vendor Specific
Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.
Authenticate requests on this server
Forward requests to the following remote RADIUS server group for authentication:
<not configured>
New...
Accept users without validating credentials
OK
Cancel
Apply

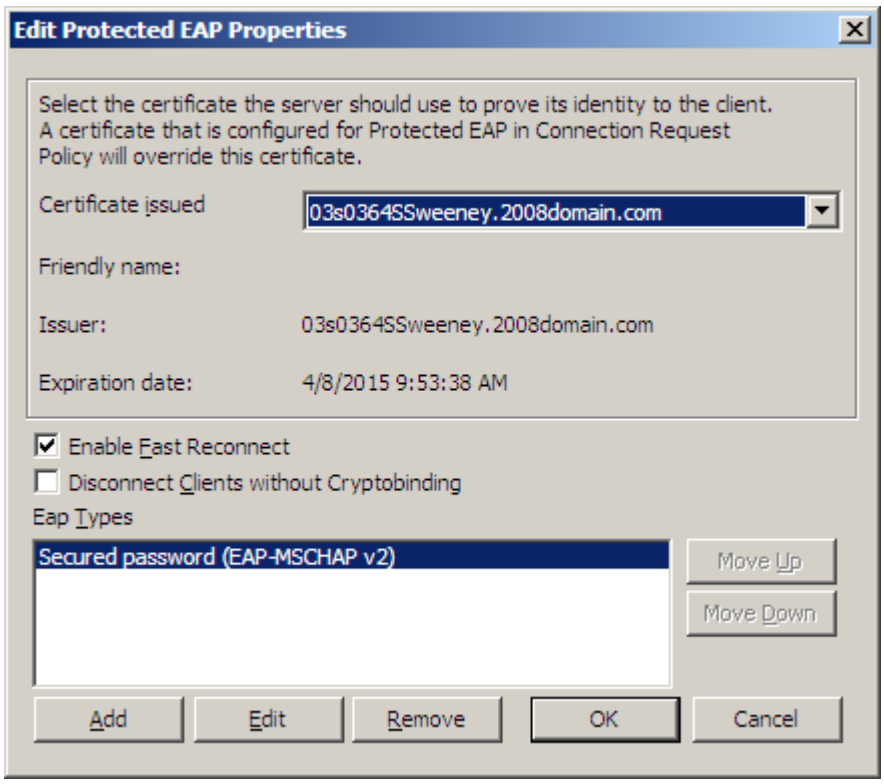


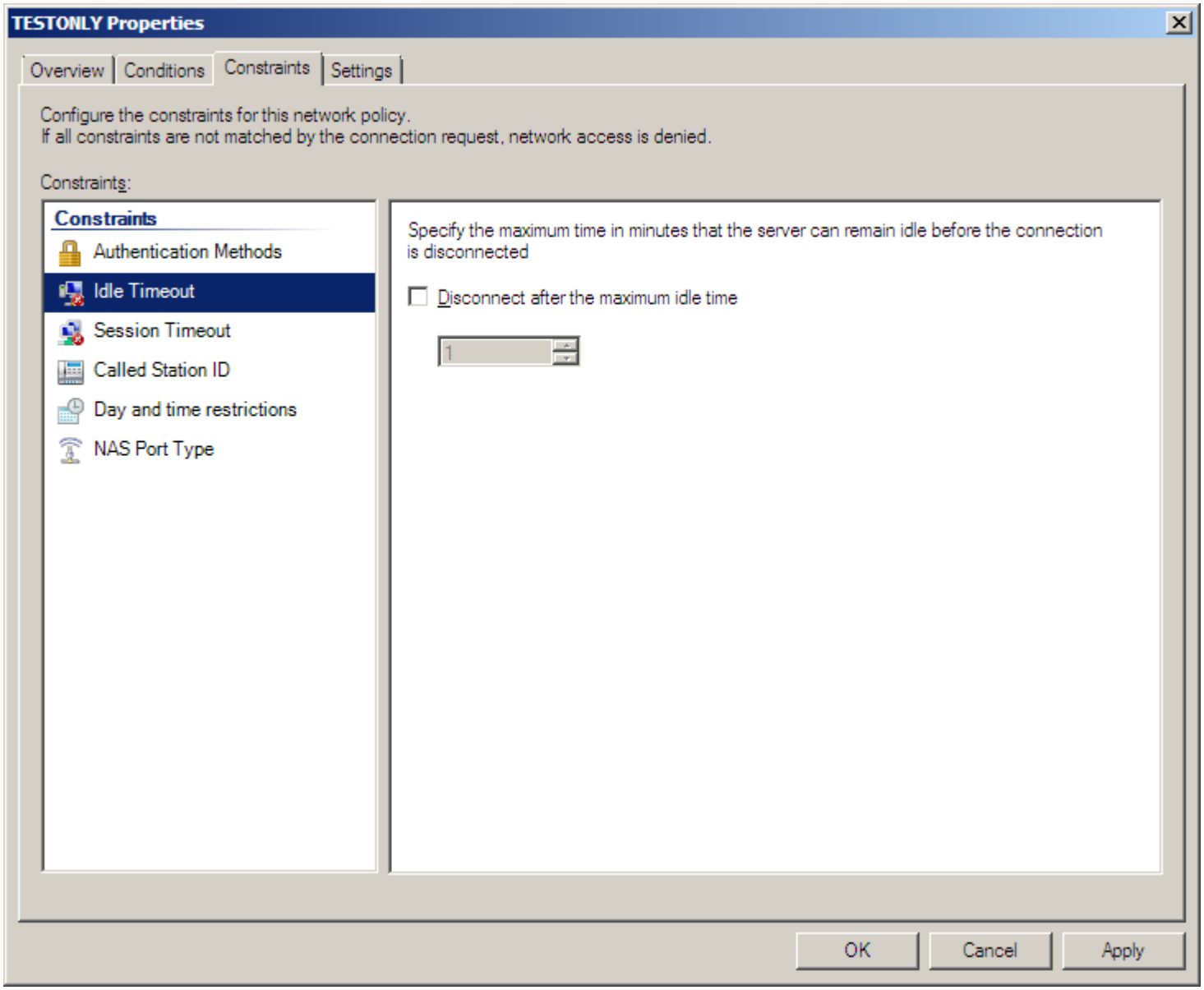
An illustration of a Network policy is shown below.

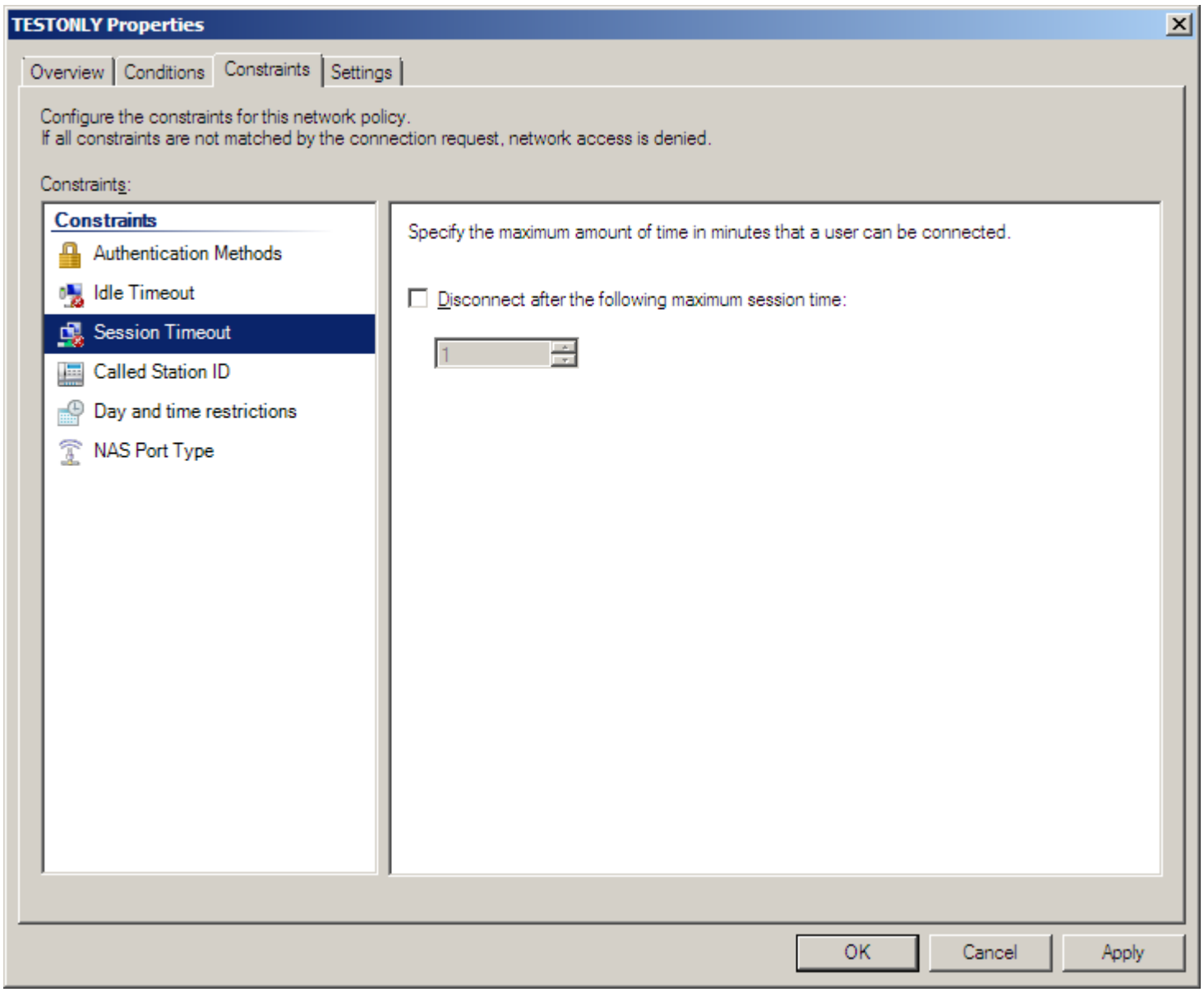

TESTONLY Properties
Overview
Conditions
Constraints
Settings
Policy name:
TESTONLY
Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.
Policy enabled
Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?
Grant access. Grant access if the connection request matches this policy.
Deny access. Deny access if the connection request matches this policy.
Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.
Type of network access server:
Unspecified
Vendor specific:
10
OK
Cancel
Apply

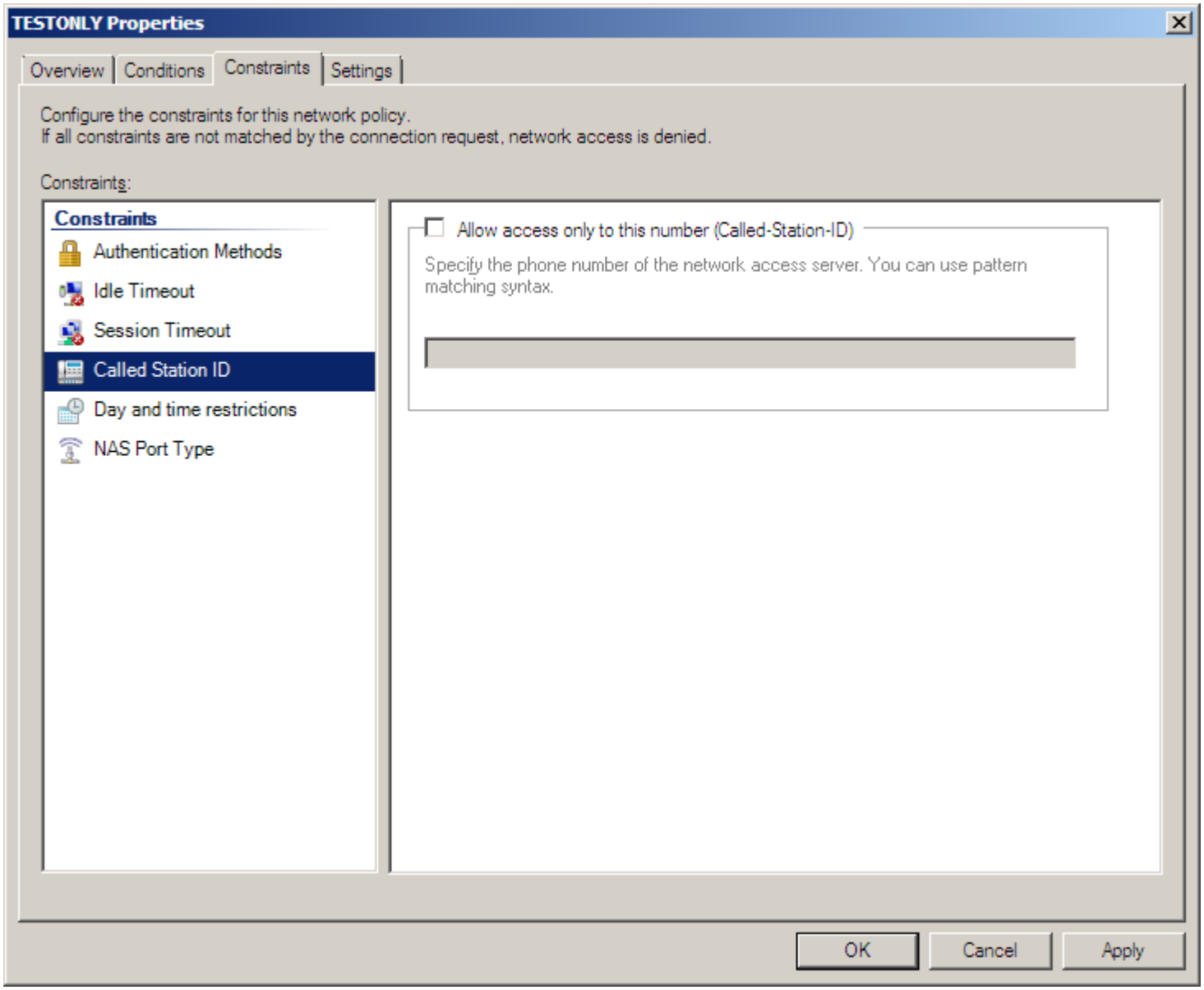

TESTONLY Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
Day and time restrictions
Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursd...
Condition description:
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.
Add...
Edit...
Remove
OK
Cancel
Apply

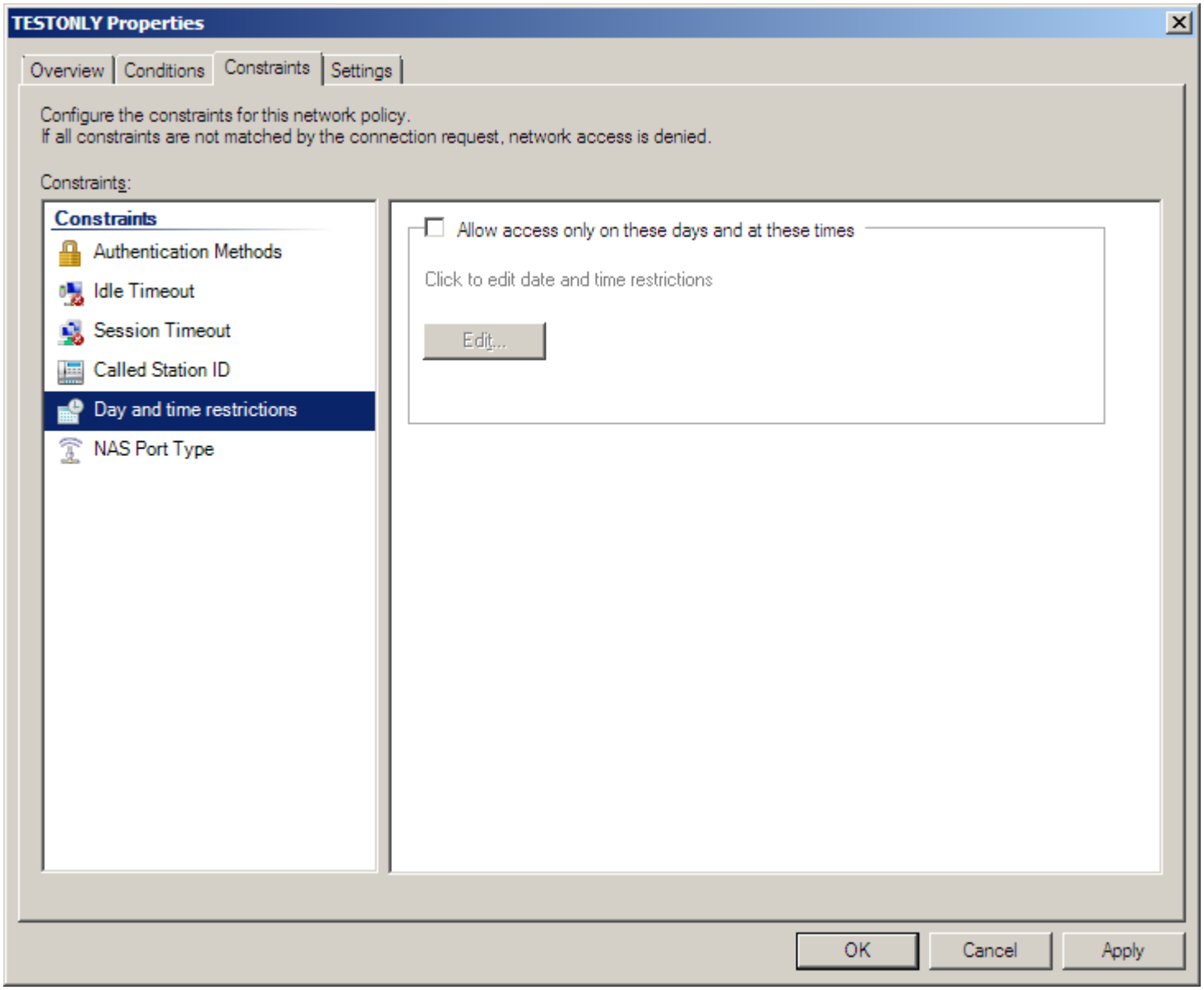

TESTONLY Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Protected EAP (PEAP)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication 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)
Allow clients to connect without negotiating an authentication method
Perform machine health check only
OK
Cancel
Apply

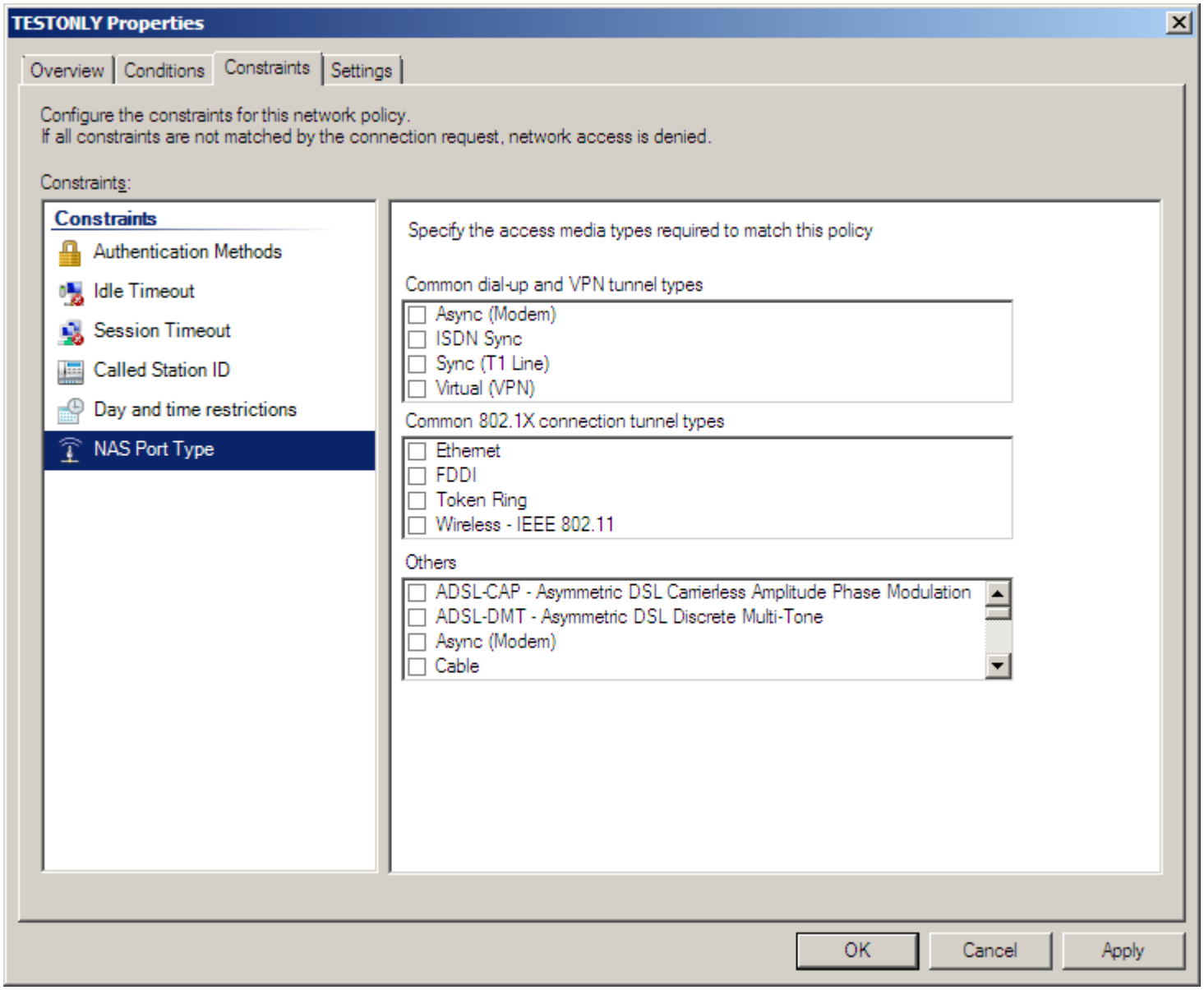

Edit Protected EAP Properties
Select the certificate the server should use to prove its identity to the client.
A certificate that is configured for Protected EAP in Connection Request
Policy will override this certificate.
Certificate issued
03s0364SSweeney.2008domain.com
Friendly name:
Issuer:
03s0364SSweeney.2008domain.com
Expiration date:
4/8/2015 9:53:38 AM
Enable Fast Reconnect
Disconnect Clients without Cryptobinding
Eap Types
Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add
Edit
Remove
OK
Cancel


TESTONLY Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected
Disconnect after the maximum idle time
1
OK
Cancel
Apply

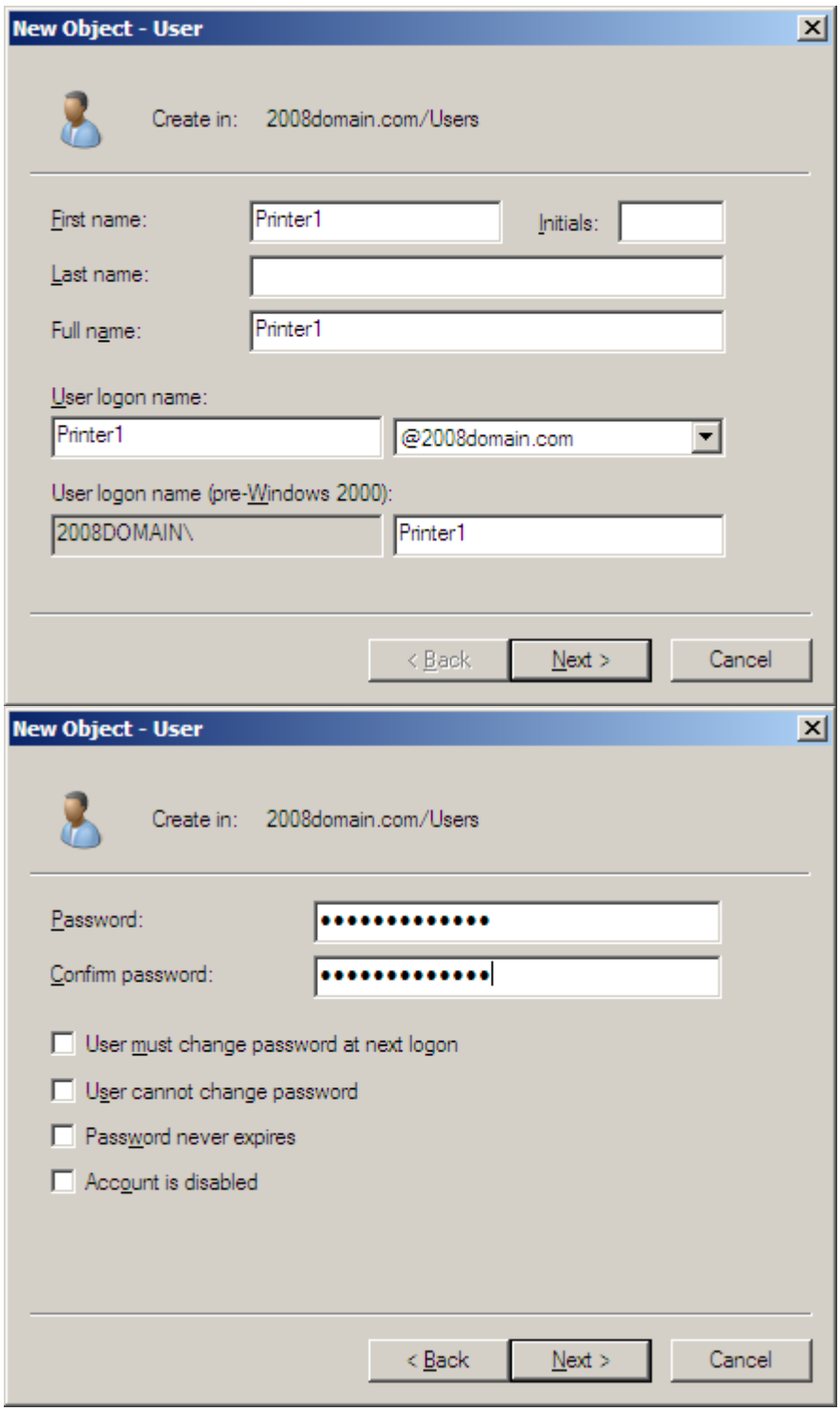

TESTONLY Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Specify the maximum amount of time in minutes that a user can be connected.
Disconnect after the following maximum session time:
1
OK
Cancel
Apply

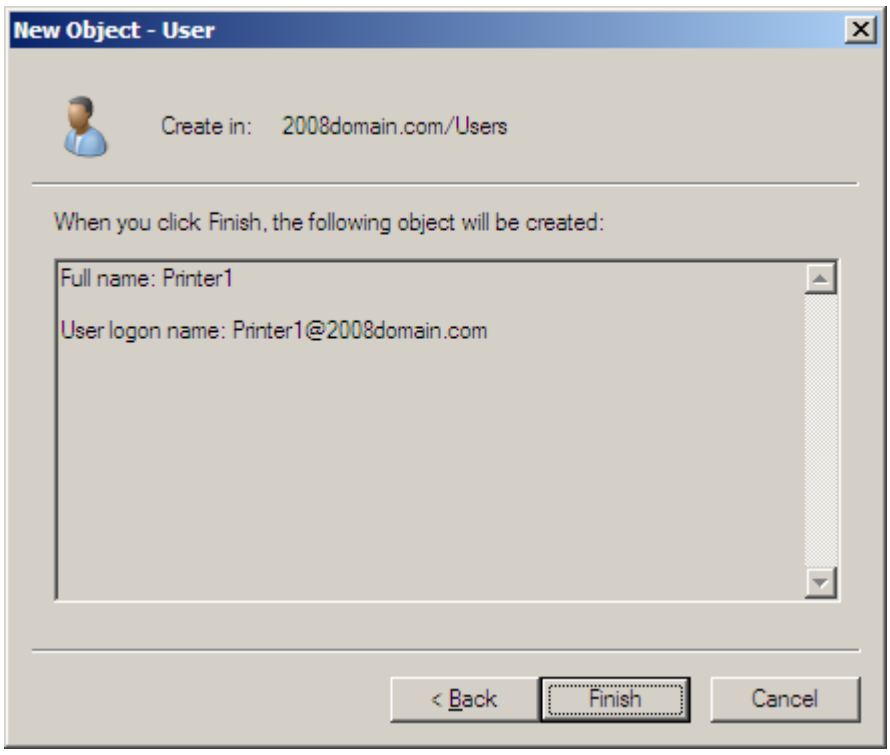

TESTONLY Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to this number (Called-Station-ID)
Specify the phone number of the network access server. You can use pattern matching syntax.
OK
Cancel
Apply


TESTONLY Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only on these days and at these times
Click to edit date and time restrictions
Edit...
OK
Cancel
Apply

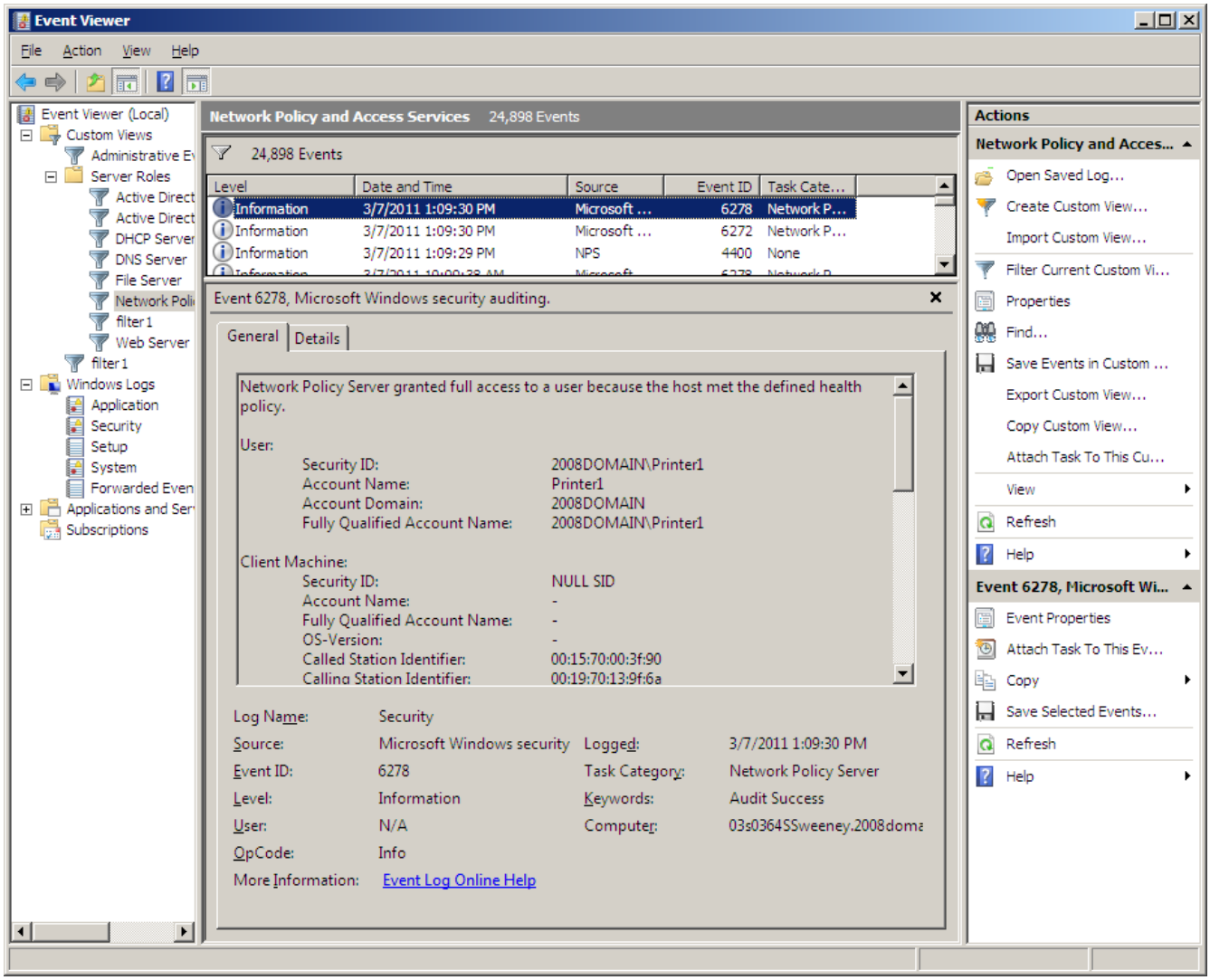


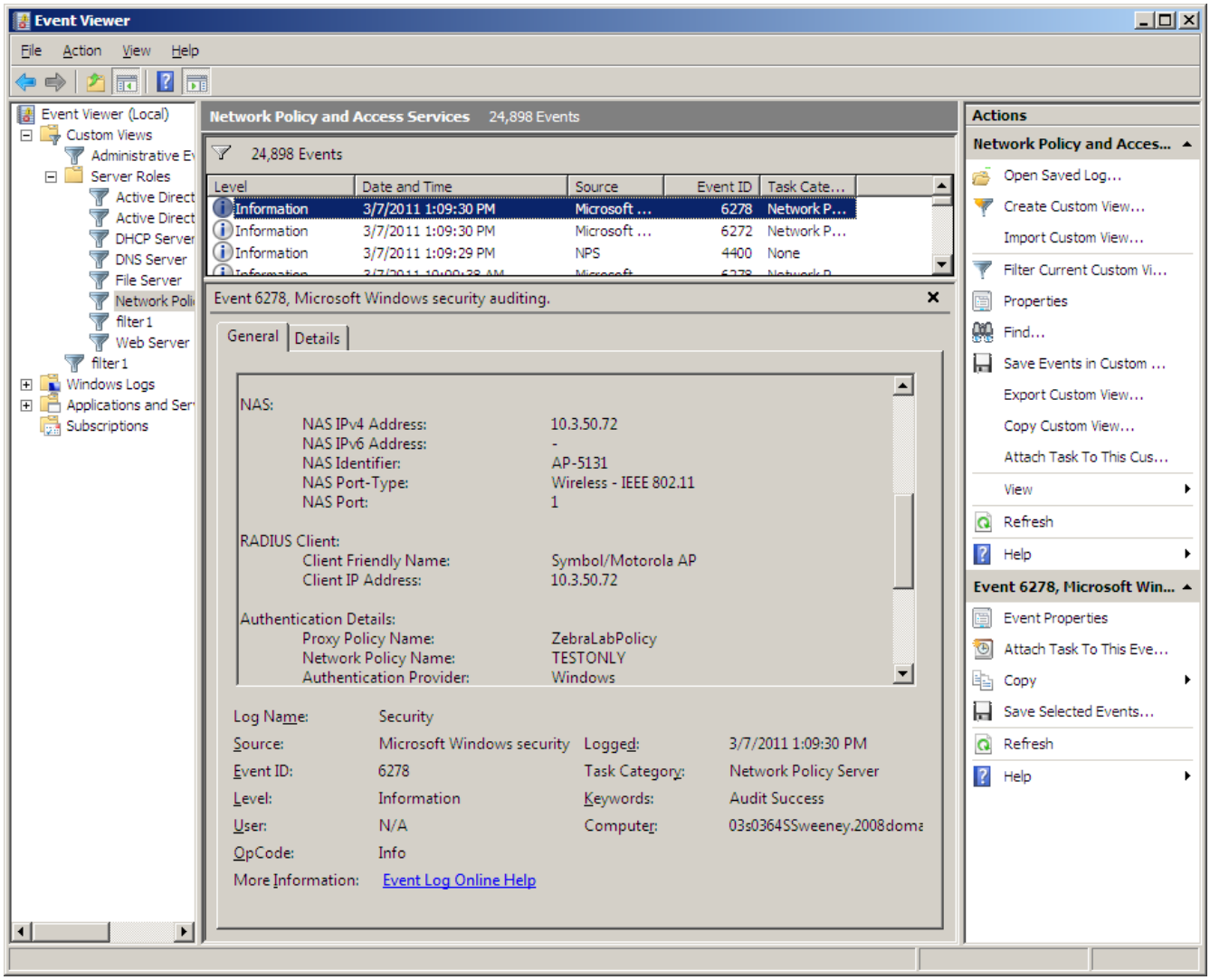
The screenshots below illustrate how a username and password is added to the 2008 Server. This is the username and password that is used on the printer.

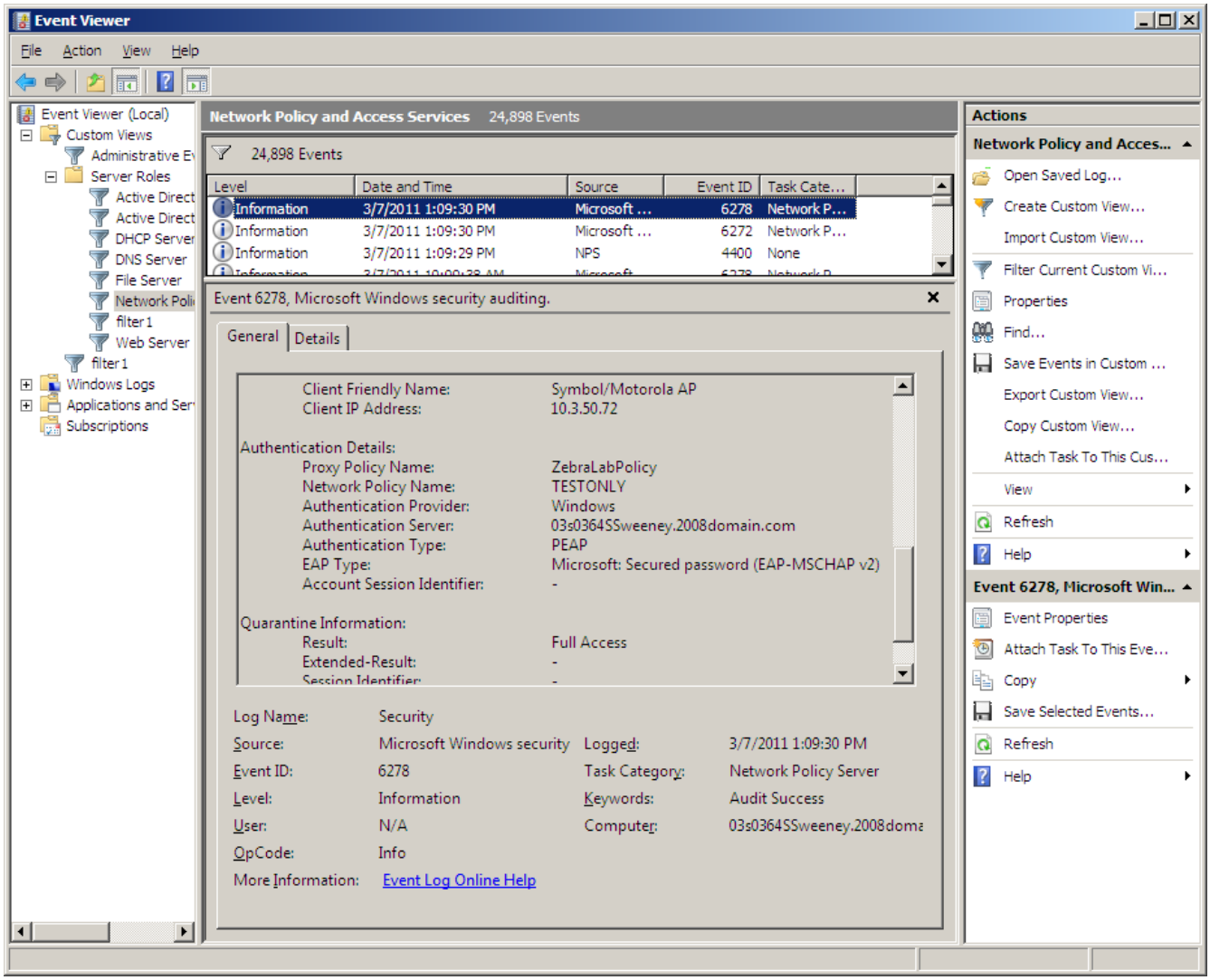

New Object - User
Create in: 2008domain.com/Users
First name:
Printer1
Initials:
Last name:
Full name:
Printer1
User logon name:
Printer1
@2008domain.com
User logon name (pre-Windows 2000):
2008DOMAIN\
Printer1
< Back
Next >
Cancel
New Object - User
Create in: 2008domain.com/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel



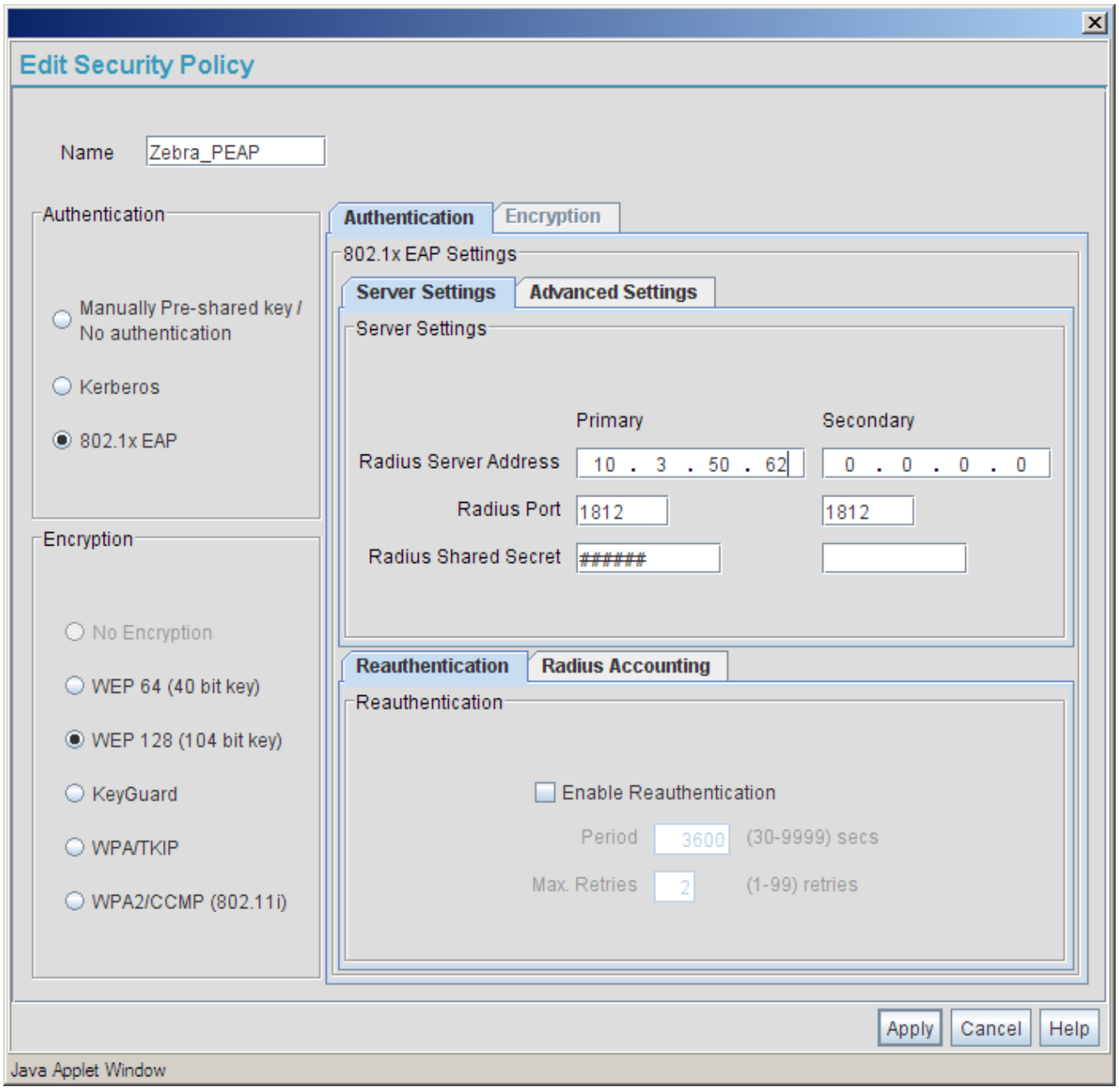
The Event viewer can be used to assist in troubleshooting.
Below is an example of the successful connection.


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Administrative Ev
Server Roles
Active Direct
Active Direct
DHCP Server
DNS Server
File Server
Network Poli
filter1
Web Server
filter1
Windows Logs
Application
Security
Setup
System
Forwarded Even
Applications and Ser
Subscriptions
Network Policy and Access Services 24,898 Events
24,898 Events
Level Date and Time Source Event ID Task Cate...
Information 3/7/2011 1:09:30 PM Microsoft ... 6278 Network P...
Information 3/7/2011 1:09:30 PM Microsoft ... 6272 Network P...
Information 3/7/2011 1:09:29 PM NPS 4400 None
Event 6278, Microsoft Windows security auditing.
General Details
Network Policy Server granted full access to a user because the host met the defined health policy.
User:
Security ID: 2008DOMAIN\Printer1
Account Name: Printer1
Account Domain: 2008DOMAIN
Fully Qualified Account Name: 2008DOMAIN\Printer1
Client Machine:
Security ID: NULL SID
Account Name: -
Fully Qualified Account Name: -
OS-Version: -
Called Station Identifier: 00:15:70:00:3f:90
Calling Station Identifier: 00:19:70:13:9f:6a
Log Name: Security
Source: Microsoft Windows security
Logged: 3/7/2011 1:09:30 PM
Event ID: 6278
Task Category: Network Policy Server
Level: Information
Keywords: Audit Success
User: N/A
Computer: 03s0364SSweeney.2008doma
OpCode: Info
More Information: Event Log Online Help
Actions
Network Policy and Acces...
Open Saved Log...
Create Custom View...
Import Custom View...
Filter Current Custom Vi...
Properties
Find...
Save Events in Custom ...
Export Custom View...
Copy Custom View...
Attach Task To This Cu...
View
Refresh
Help
Event 6278, Microsoft Wi...
Event Properties
Attach Task To This Ev...
Copy
Save Selected Events...
Refresh
Help

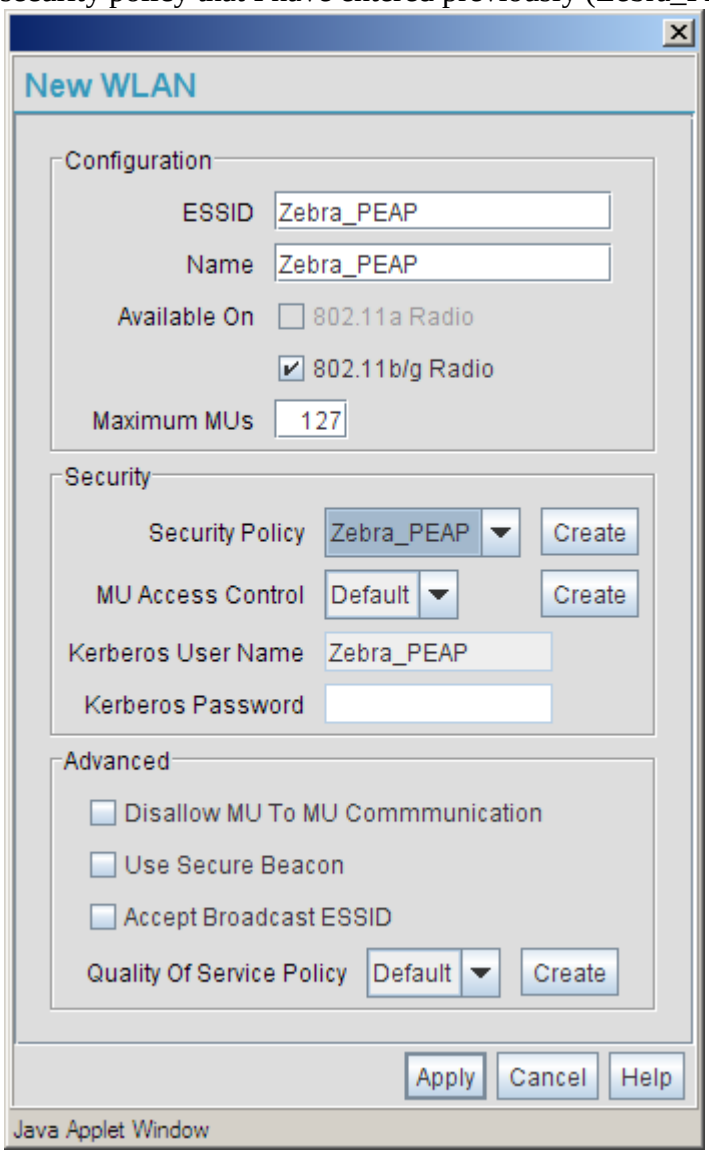

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Administrative Ev
Server Roles
Active Direct
Active Direct
DHCP Server
DNS Server
File Server
Network Poli
filter 1
Web Server
filter 1
Windows Logs
Applications and Ser
Subscriptions
Network Policy and Access Services 24,898 Events
24,898 Events
Level Date and Time Source Event ID Task Cate...
Information 3/7/2011 1:09:30 PM Microsoft ... 6278 Network P...
Information 3/7/2011 1:09:30 PM Microsoft ... 6272 Network P...
Information 3/7/2011 1:09:29 PM NPS 4400 None
Event 6278, Microsoft Windows security auditing.
General Details
NAS:
NAS IPv4 Address: 10.3.50.72
NAS IPv6 Address: -
NAS Identifier: AP-5131
NAS Port-Type: Wireless - IEEE 802.11
NAS Port: 1
RADIUS Client:
Client Friendly Name: Symbol/Motorola AP
Client IP Address: 10.3.50.72
Authentication Details:
Proxy Policy Name: ZebraLabPolicy
Network Policy Name: TESTONLY
Authentication Provider: Windows
Log Name: Security
Source: Microsoft Windows security
Logged: 3/7/2011 1:09:30 PM
Event ID: 6278
Task Category: Network Policy Server
Level: Information
Keywords: Audit Success
User: N/A
Computer: 03s0364SSweeney.2008doma
OpCode: Info
More Information: Event Log Online Help
Actions
Network Policy and Acces...
Open Saved Log...
Create Custom View...
Import Custom View...
Filter Current Custom Vi...
Properties
Find...
Save Events in Custom ...
Export Custom View...
Copy Custom View...
Attach Task To This Cus...
View
Refresh
Help
Event 6278, Microsoft Win...
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Administrative Ev
Server Roles
Active Direct
Active Direct
DHCP Server
DNS Server
File Server
Network Poli
filter 1
Web Server
filter 1
Windows Logs
Applications and Ser
Subscriptions
Network Policy and Access Services 24,898 Events
24,898 Events
Level Date and Time Source Event ID Task Cate...
Information 3/7/2011 1:09:30 PM Microsoft ... 6278 Network P...
Information 3/7/2011 1:09:30 PM Microsoft ... 6272 Network P...
Information 3/7/2011 1:09:29 PM NPS 4400 None
Event 6278, Microsoft Windows security auditing.
General Details
Client Friendly Name: Symbol/Motorola AP
Client IP Address: 10.3.50.72
Authentication Details:
Proxy Policy Name: ZebraLabPolicy
Network Policy Name: TESTONLY
Authentication Provider: Windows
Authentication Server: 03s0364SSweeney.2008domain.com
Authentication Type: PEAP
EAP Type: Microsoft: Secured password (EAP-MSCHAP v2)
Account Session Identifier: -
Quarantine Information:
Result: Full Access
Extended-Result: -
Log Name: Security
Source: Microsoft Windows security
Logged: 3/7/2011 1:09:30 PM
Event ID: 6278
Task Category: Network Policy Server
Level: Information
Keywords: Audit Success
User: N/A
Computer: 03s0364SSweeney.2008doma
OpCode: Info
More Information: Event Log Online Help
Actions
Network Policy and Acces...
Open Saved Log...
Create Custom View...
Import Custom View...
Filter Current Custom Vi...
Properties
Find...
Save Events in Custom ...
Export Custom View...
Copy Custom View...
Attach Task To This Cus...
View
Refresh
Help
Event 6278, Microsoft Win...
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help

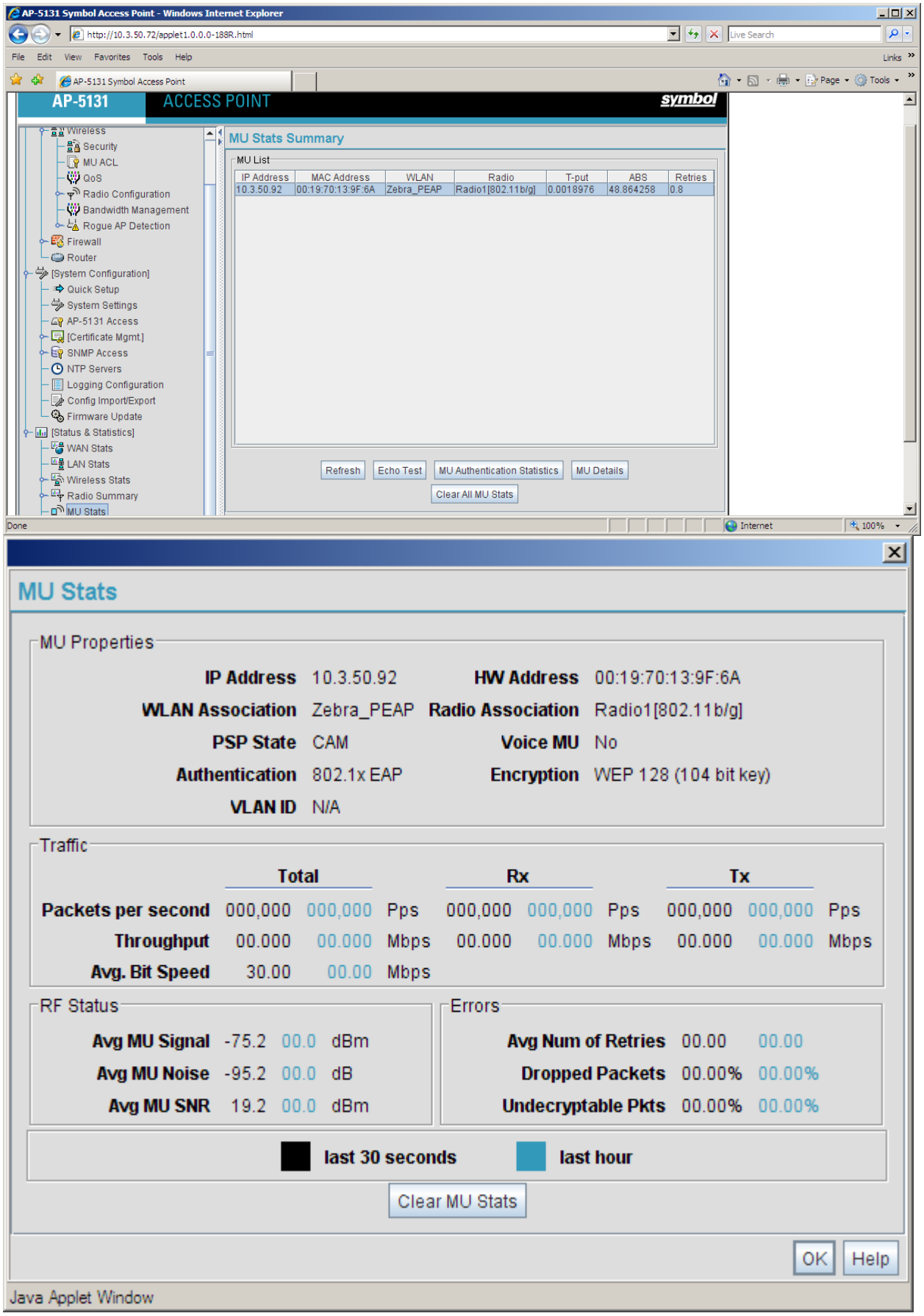
This section of the document illustrates a **Symbol / Motorola Access Point**
This document is meant as an illustration only. Questions on the setup of your Symbol / Motorola Access Point should be directed to Motorola. It should be Motorola that is used to determine if the illustration below is appropriate for your environment
This illustration shows how the Symbol/Motorola Access Point was configured for PEAP initially and then configured for WPA-PEAP.
With PEAP or WPA-PEAP the authentication request is forwarded to a Radius server.
The first step in this illustration is adding a security policy for **PEAP.**
The example below shows an entry of a radius server with an IP address of 10.3.50.62 (Microsoft NPS server) 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 next step illustrated here is how an ESSID is created. The ESSID in this illustration is "Zebra_PEAP". Please note that ESSID's are case sensitive. In this illustration, I have assigned the security policy that I have entered previously (Zebra_PEAP)

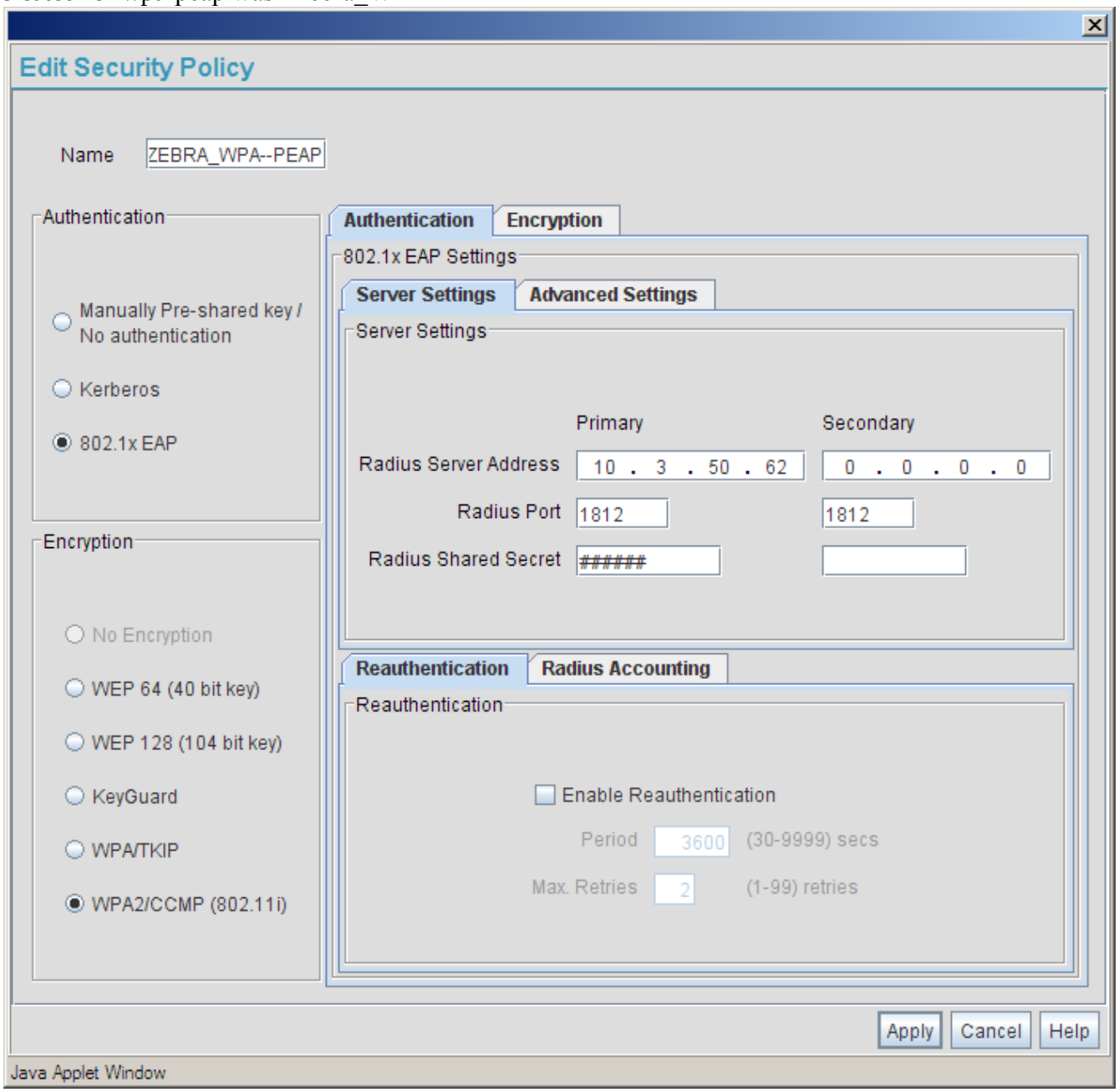


The screenshots below show views on the Access Point of a successful PEAP connection.

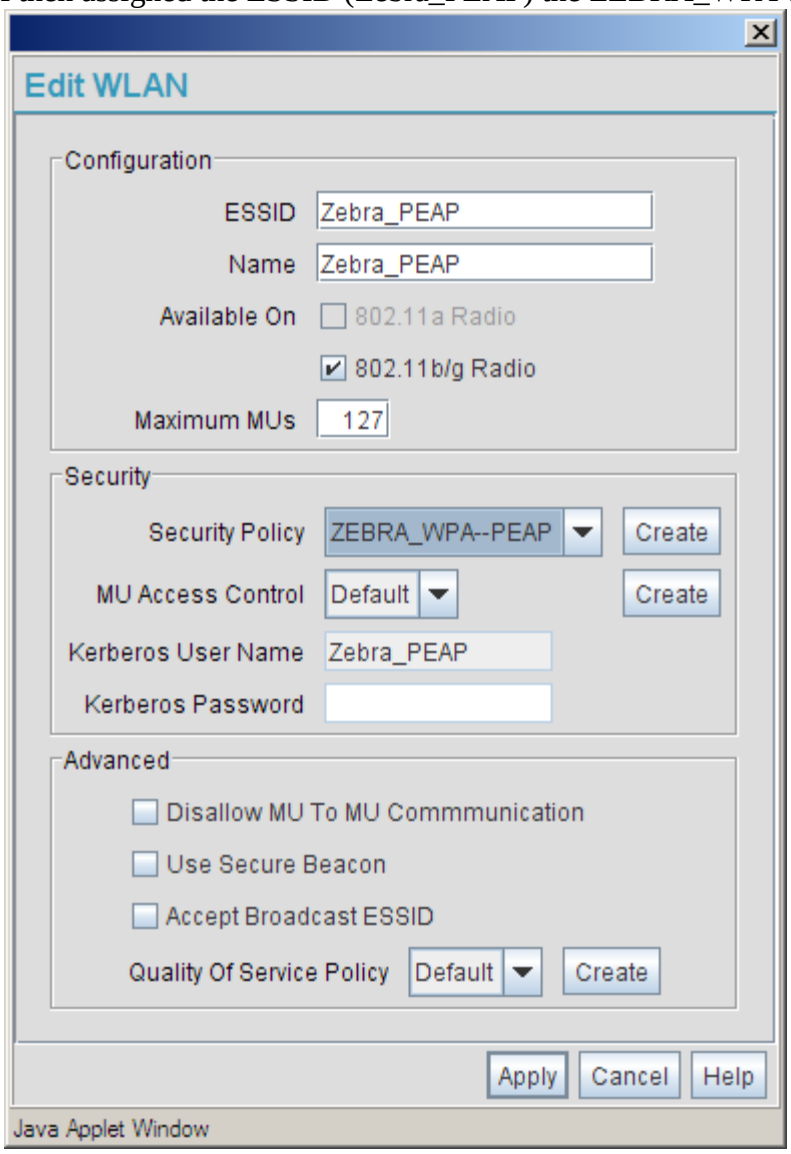

AP-5131 Symbol Access Point - Windows Internet Explorer
http://10.3.50.72/applet1.0.0.0-188R.html
File Edit View Favorites Tools Help
AP-5131 Symbol Access Point
AP-5131
ACCESS POINT
symbol
Wireless
Security
MU ACL
QoS
Radio Configuration
Bandwidth Management
Rogue AP Detection
Firewall
Router
[System Configuration]
Quick Setup
System Settings
AP-5131 Access
[Certificate Mgmt.]
SNMP Access
NTP Servers
Logging Configuration
Config Import/Export
Firmware Update
[Status & Statistics]
WAN Stats
LAN Stats
Wireless Stats
Radio Summary
MU Stats
MU Stats Summary
MU List
IP Address MAC Address WLAN Radio T-put ABS Retries
10.3.50.92 00:19:70:13:9F:6A Zebra_PEAP Radio1[802.11b/g] 0.0018976 48.864258 0.8
Refresh
Echo Test
MU Authentication Statistics
MU Details
Clear All MU Stats
Done
Internet
100%

MU Stats
MU Properties
IP Address 10.3.50.92
HW Address 00:19:70:13:9F:6A
WLAN Association Zebra_PEAP
Radio Association Radio1[802.11b/g]
PSP State CAM
Voice MU No
Authentication 802.1x EAP
Encryption WEP 128 (104 bit key)
VLAN ID N/A
Traffic
Total
Rx
Tx
Packets per second 000,000 000,000 Pps 000,000 000,000 Pps 000,000 000,000 Pps
Throughput 00.000 00.000 Mbps 00.000 00.000 Mbps 00.000 00.000 Mbps
Avg. Bit Speed 30.00 00.00 Mbps
RF Status
Avg MU Signal -75.2 00.0 dBm
Avg MU Noise -95.2 00.0 dB
Avg MU SNR 19.2 00.0 dBm
Errors
Avg Num of Retries 00.00 00.00
Dropped Packets 00.00% 00.00%
Undecryptable Pkts 00.00% 00.00%
last 30 seconds
last hour
Clear MU Stats
OK
Help
Java Applet Window

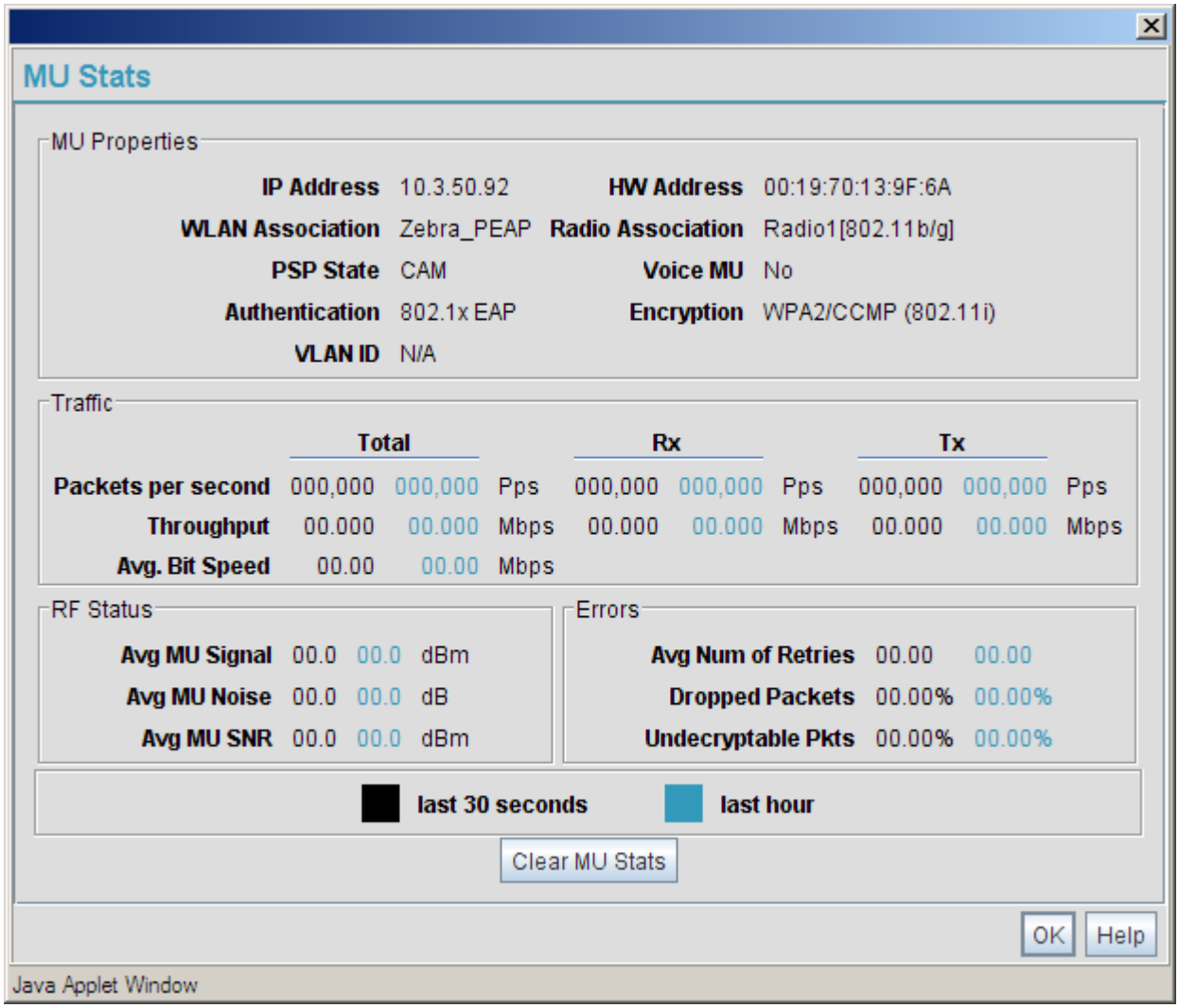
The next screenshots show how the Symbol / Motorola Access Point was set for **WPA-PEAP.** The access point is configured with a new security policy. In this example the security policy that was created for wpa-peap was “Zebra_WPA-PEAP”



I then assigned the ESSID (Zebra_PEAP) the ZEBRA_WPA-PEAP policy.

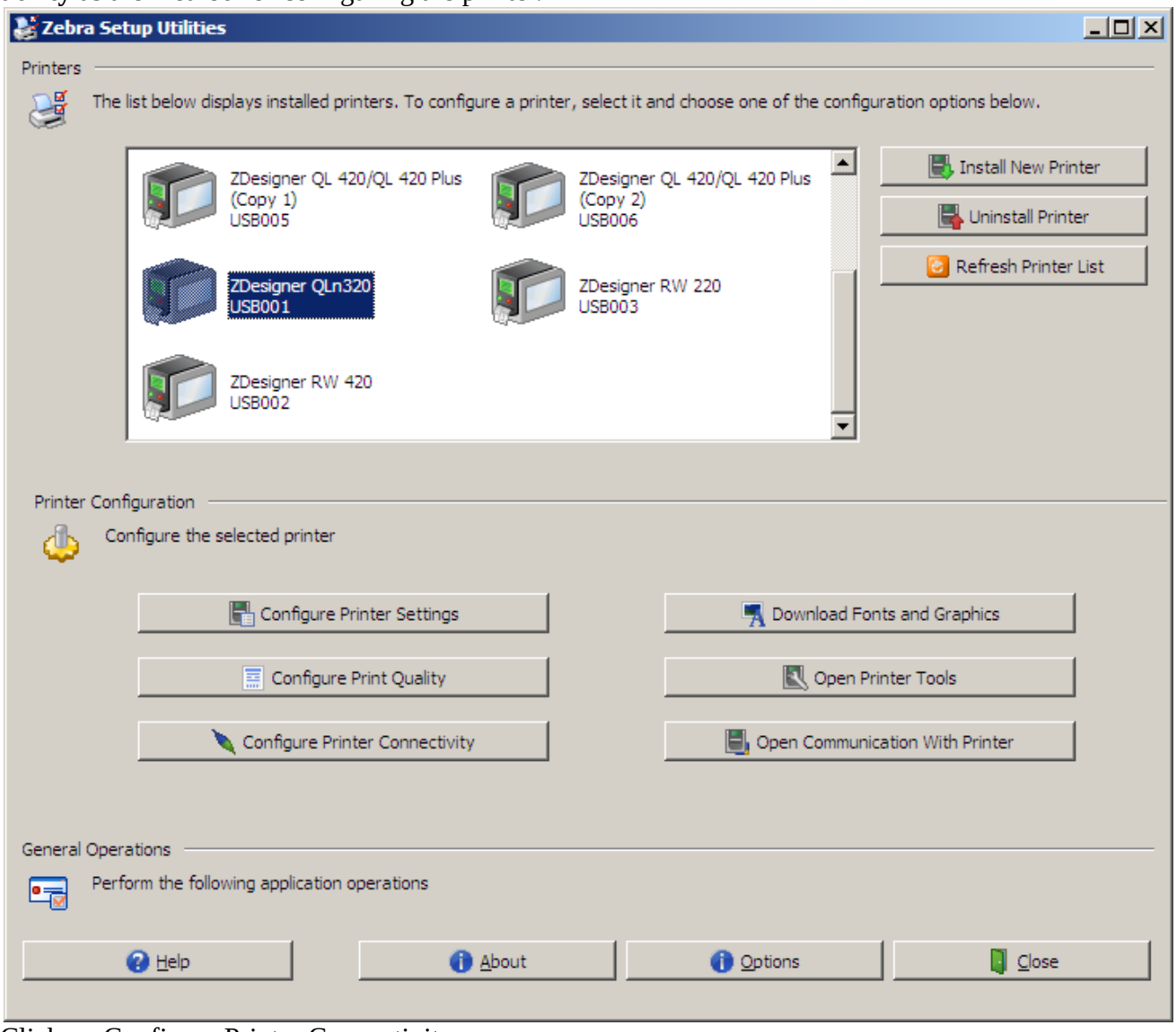


Below is an example of what the Symbol / Motorola Access point shows for a successful WPA-PEAP authentication.

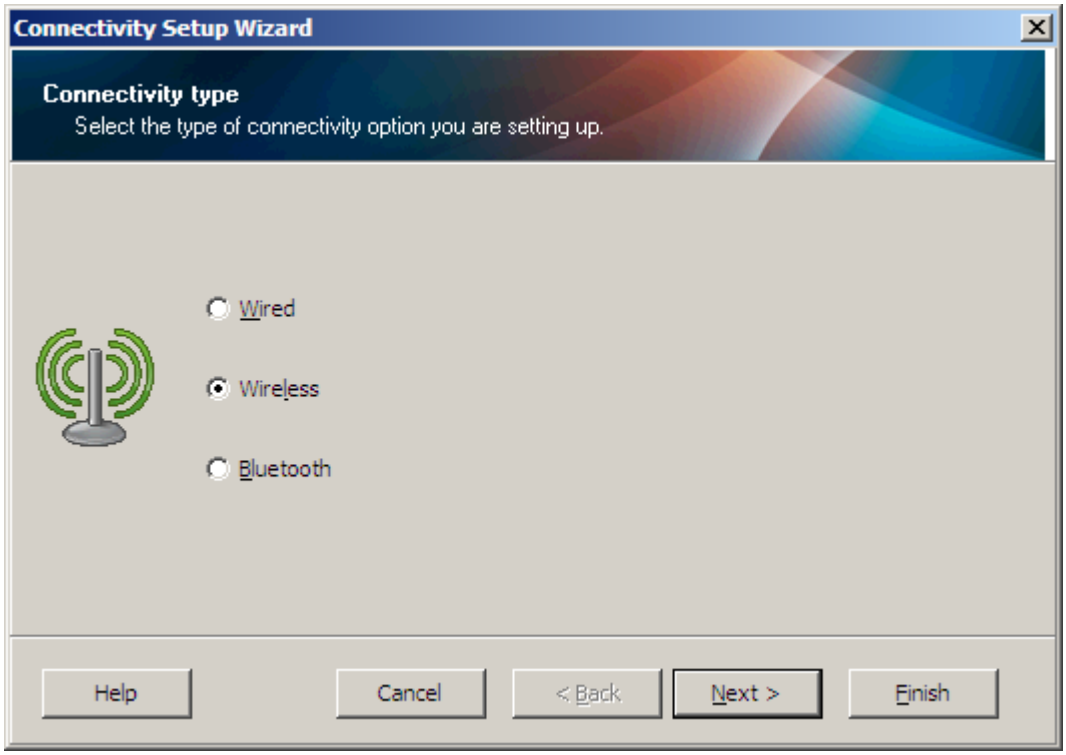

MU Stats
MU Properties
IP Address 10.3.50.92
HW Address 00:19:70:13:9F:6A
WLAN Association Zebra_PEAP
Radio Association Radio1[802.11b/g]
PSP State CAM
Voice MU No
Authentication 802.1x EAP
Encryption WPA2/CCMP (802.11i)
VLAN ID N/A
Traffic
Total
Rx
Tx
Packets per second 000,000 000,000 Pps 000,000 000,000 Pps 000,000 000,000 Pps
Throughput 00.000 00.000 Mbps 00.000 00.000 Mbps 00.000 00.000 Mbps
Avg. Bit Speed 00.00 00.00 Mbps
RF Status
Avg MU Signal 00.0 00.0 dBm
Avg MU Noise 00.0 00.0 dB
Avg MU SNR 00.0 00.0 dBm
Errors
Avg Num of Retries 00.00 00.00
Dropped Packets 00.00% 00.00%
Undecryptable Pkts 00.00% 00.00%
last 30 seconds
last hour
Clear MU Stats
OK
Help
Java Applet Window

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.

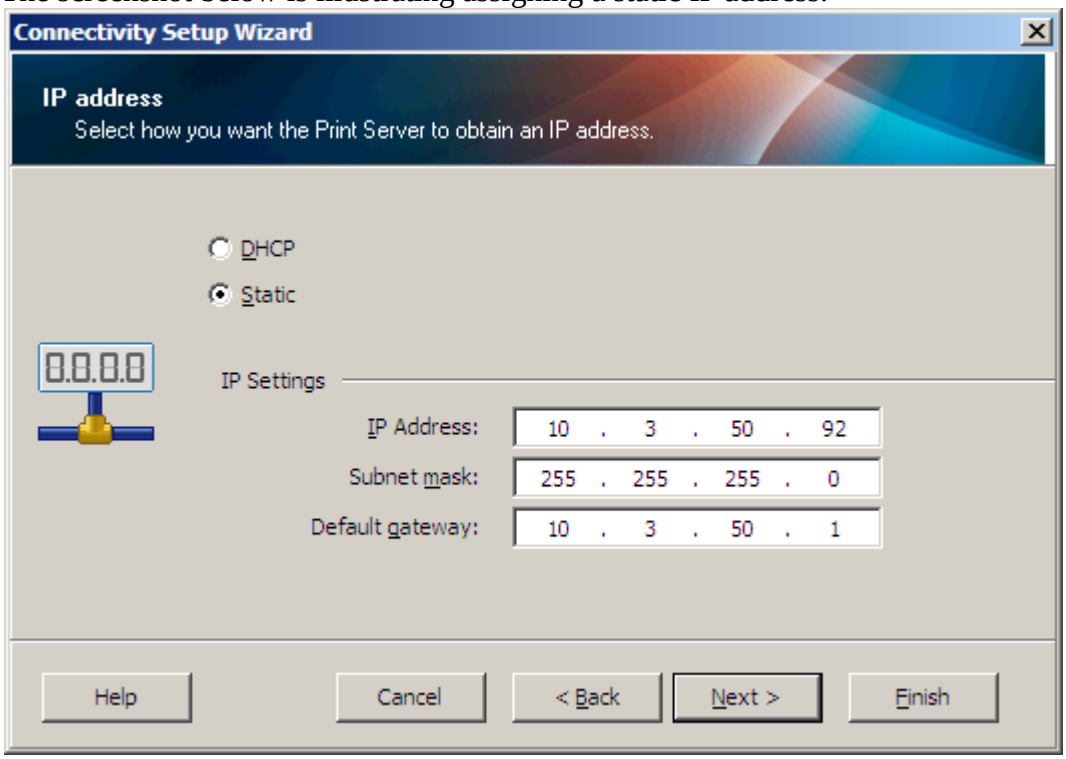


Click on Configure Printer Connectivity

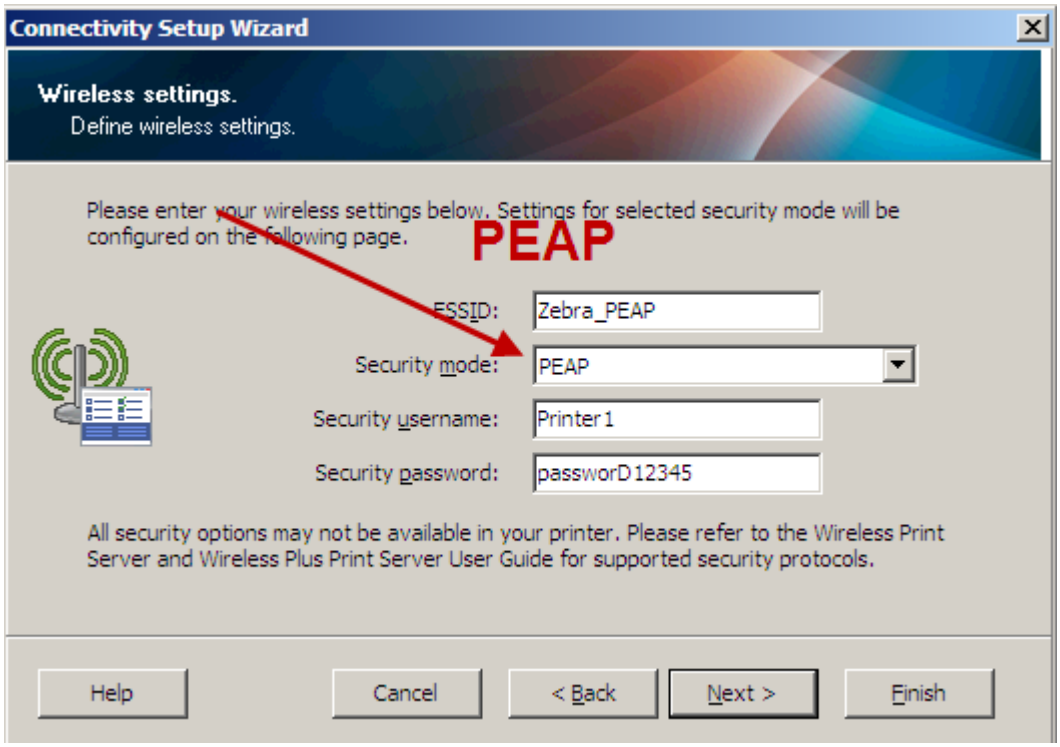


Choose Wireless

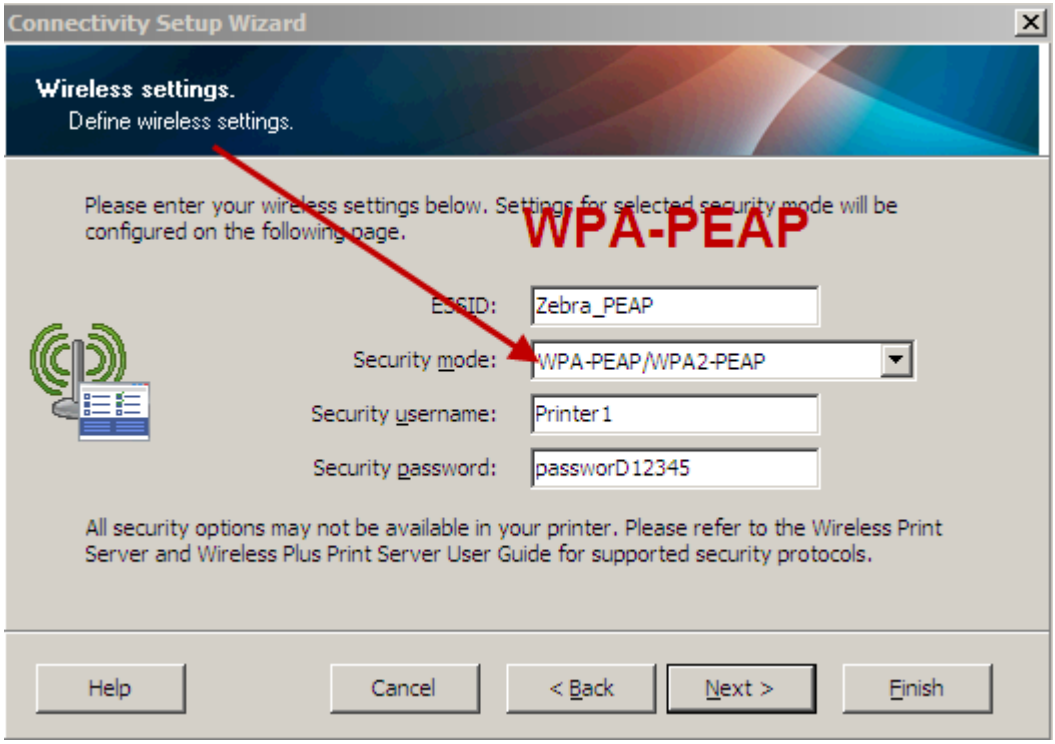
The screenshot below is illustrating assigning a static IP address.

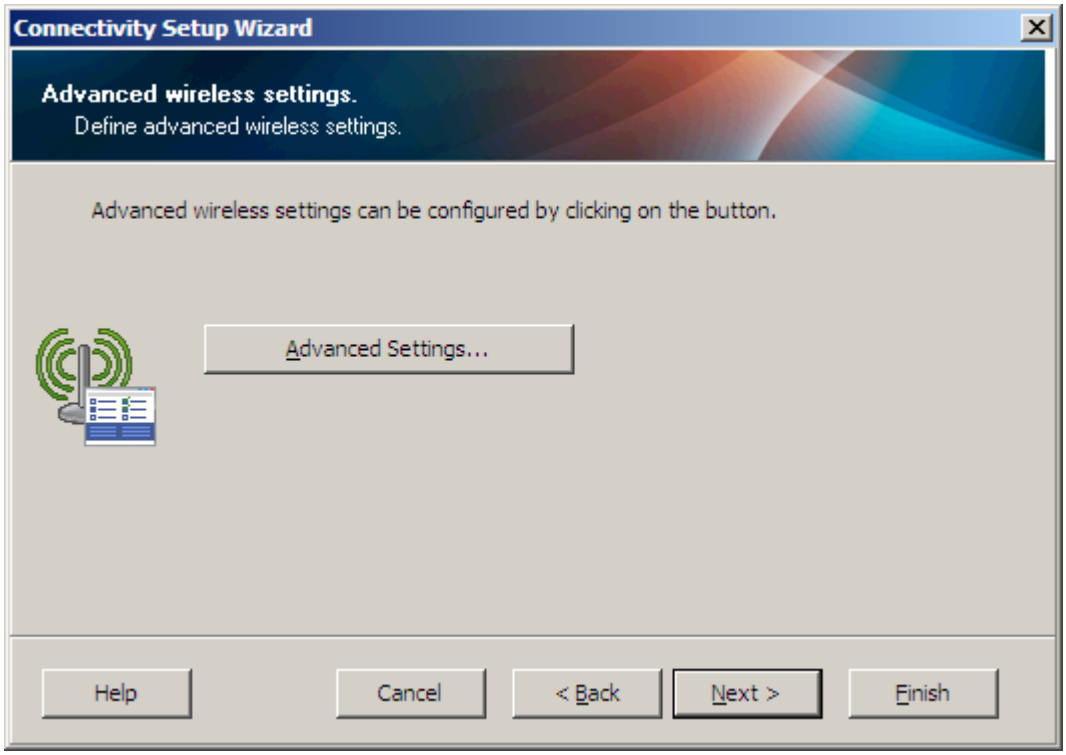


The screenshot below shows a 802.1x PEAP connection

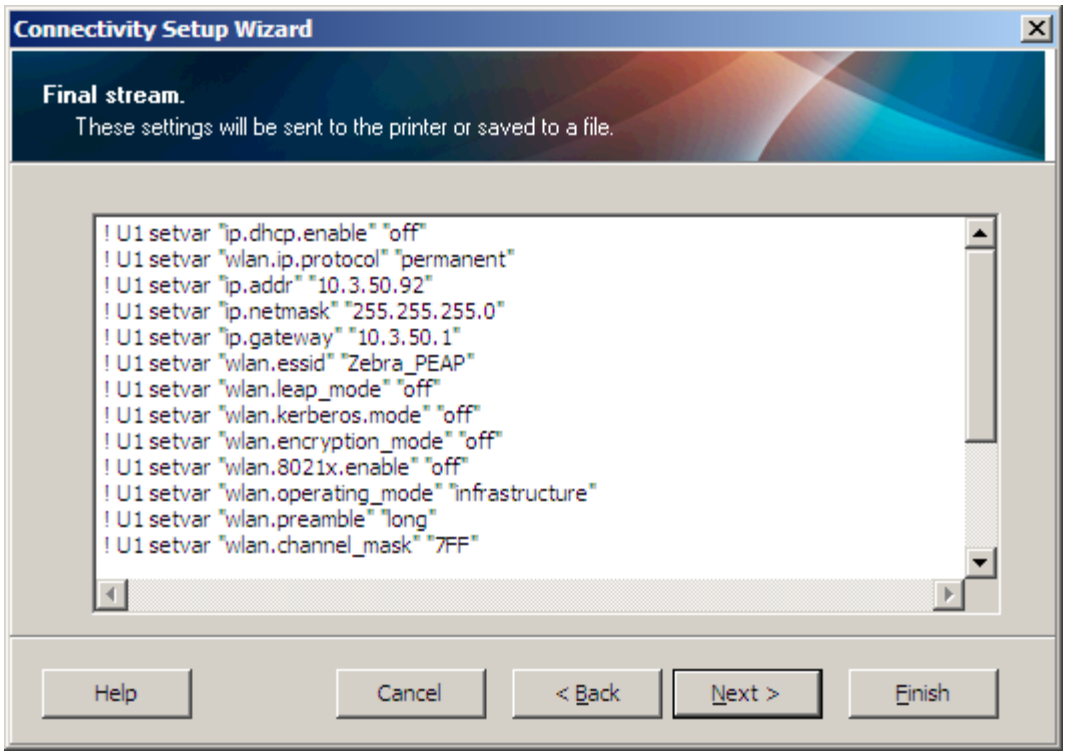


The screenshot below shows a WPA-PEAP connection

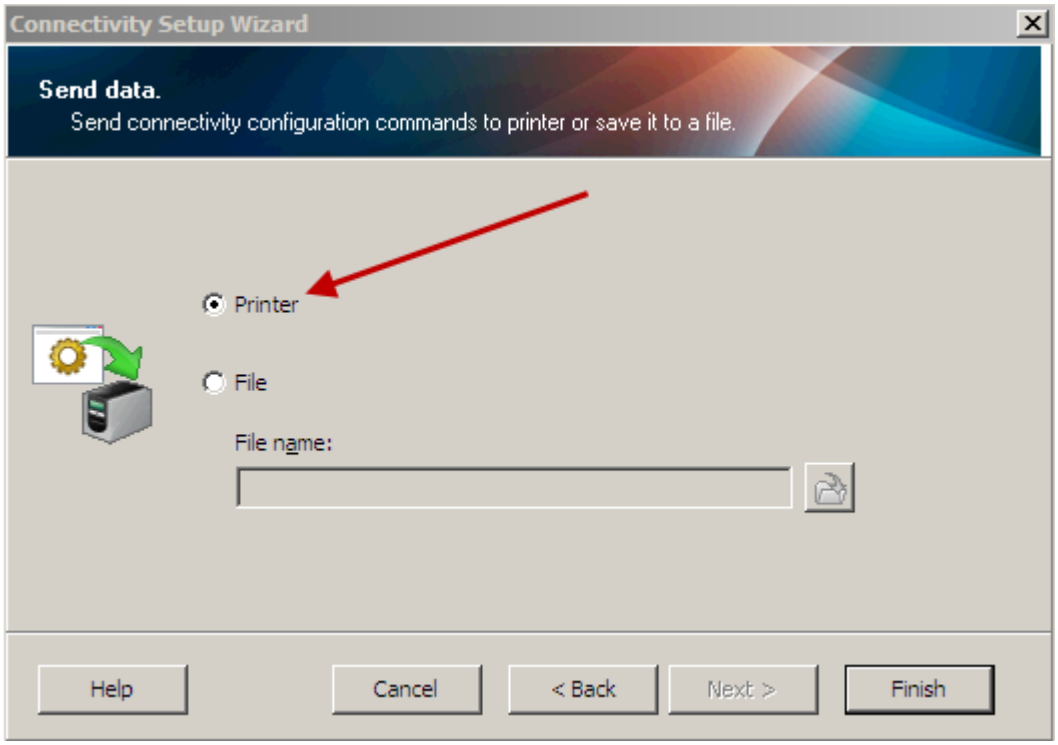




Choose NEXT



Choose NEXT



Choose Printer then FINISH

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