Configuring RADIUS Authentication for Netvanta 150 802.11a/b/g Wireless Clients

Introduction

The use of AAA services (Authentication, Authorization, and Accounting) allows for several methods of controlling and recording access to AOS-based devices. The two methods of achieving this result involve either RADIUS or TACACS+ servers. This guide will specifically cover the use of controlling login authentication for 802.11a/b/g wireless clients to a wireless LAN controlled by a Netvanta 150.

Network Considerations

Using RADIUS for wireless clients involves more devices than the Netvanta 150 and the RADIUS server itself, and impacts several facets of the wireless network and the clients. Please review the following network considerations before implementing this feature:

- The Netvanta 150(s) must have IP address(s) that are routable through the network and are allowed to communicate with the RADIUS server.
  - The IP address assigned to the Netvanta 150 will exist on the native VLAN of the port it is connected to, if multiple VLANs are in use.
- On the RADIUS-authenticated wireless LAN(s) only, wireless roaming times between Netvanta 150s will increase due to the time delays introduced by the communication with the RADIUS server.
  - Standard authentication wireless LAN roaming times on the same Netvanta 150s will be unaffected.
  - Each roam requires a re-authentication with the RADIUS server under the current implementation of RADIUS for wireless clients. Because of this fact, it is recommended that the user credentials be saved within the wireless client so that the user is not forced to re-input the credentials each time the device roams to a new Netvanta 150.
- The wireless clients must support the desired type of EAP authentication to connect to the RADIUS-authenticated wireless LAN.
  - This document uses PEAP with MS-CHAPv2 as an example.
- An existing certificate infrastructure on the network is recommended. The RADIUS server is required to have a certificate in most cases, and is shown with a certificate in the example case in this document.

Command Line Configuration

RADIUS authentication for wireless clients does not require that the controller have AAA or RADIUS configured. The configuration is relevant only to the Netvanta 150 Virtual Access Point (VAP) it is configured for; not every VAP must use RADIUS authentication.

Applying an IP Address to the Netvanta 150

Each Netvanta 150 must have an IP address applied to it to facilitate communication with the RADIUS server. RADIUS authentication is the only operation within a Netvanta 150 that requires it has an IP address, so an existing non-RADIUS configuration may not already have one applied. To apply an IP address to the Netvanta 150, the configuration is as shown:

NOTE: *The RADIUS requests will be sourced from the IP address on the Netvanta 150, so the Netvanta 150's IP address must be routable on the network via its native VLAN.*

```
interface dot11ap 1 ap-type nv150
  access-point mac-address <MAC Address>
  ip address <IP Address> <Subnet Mask>
  ip default-gateway <Default Gateway>
```

Applying the RADIUS Settings to the Netvanta 150

Each VAP that will use RADIUS authentication must specify a RADIUS server and associated Pre-Shared Key for that server. The Netvanta 150 does not support the use of multiple RADIUS servers in a failover solution.

The security mode of the VAP once connected will be the same as a non-RADIUS authenticated VAP. The same security concerns once the client is connected apply equally to both RADIUS authenticated and non-RADIUS authenticated VAPs. The following security modes are available to a RADIUS authenticated VAP:

- WEP-OPEN
- WPA-TKIP
- WPA2-AES
- Hybrid WPA-TKIP & WPA2-AES

NOTE: *The recommended and most secure security mode is WPA2 with AES encryption.*

An example RADIUS authenticated VAP configuration using WPA2 with AES encryption is as shown:

```
interface dot11ap 1/1.1
  ssid broadcast-mode "RADIUS-WPA2-AES-EAP"
  security mode wpa aes-ccmp eap
  security wpa group-key
  radius-server host <Server IP> key <Pre-Shared Key>
  no shutdown
```

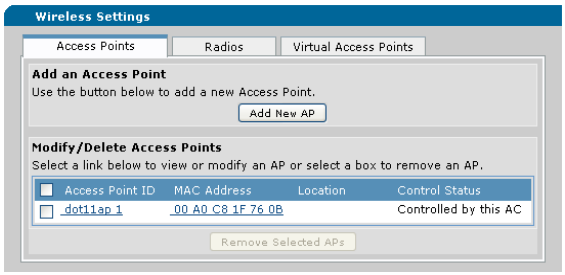
Web Interface Configuration

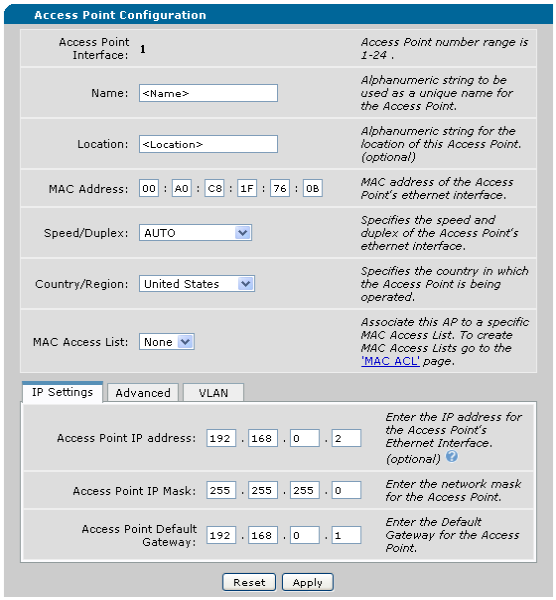
This section will define the methods for configuring this functionality through the GUI. The technology definitions and explanations will not be repeated; please refer to the relevant command line configuration section for more information.

The RADIUS configuration is accomplished from the "Data → Wireless → APs / Radios / VAPs" page, in the tabs entitled "Access Points" and "Virtual Access Points".

Applying an IP Address to the Netvanta 150

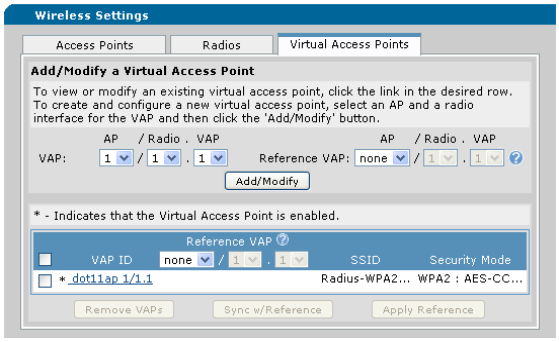
Each Netvanta 150 will be listed under the "Access Points" tab. Select each one to enter the sub-page for that device where the IP address can be defined, as shown:

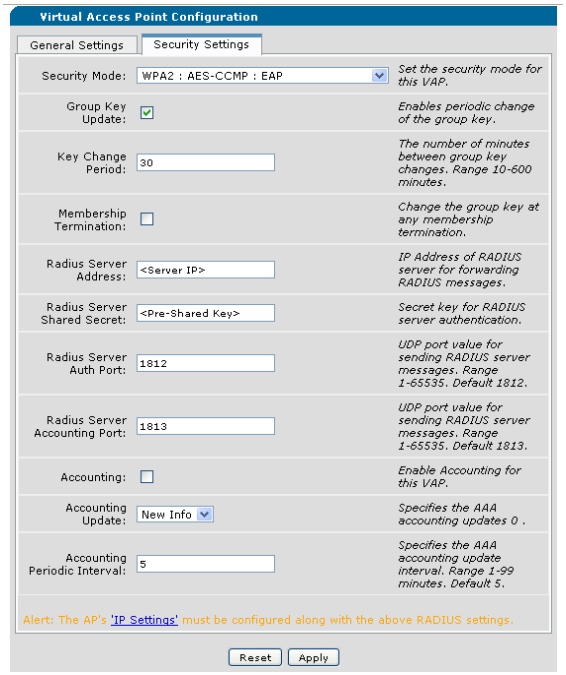




Applying the RADIUS Settings to the Netvanta 150

Each VAP will be listed under the “Virtual Access Points” tab. Select each one to enter the sub-page for that VAP where the “Security Mode”, “RADIUS Server Address”, and “RADIUS Server Shared Secret”, as shown:





Configuring the RADIUS Server

This section will define the relevant portions of the RADIUS message that the server should be looking for, and use the IAS function of a Windows 2003 Server as an example.

RADIUS Attribute Value Pairs (AVPs)

The RADIUS authentication request will contain several Attribute Value Pairs (AVPs) that facilitate the required functions of authentication. They allow the authentication method defined within the RADIUS server to be specific enough to match only on traffic from this client (or class of clients). If the RADIUS server supports logging at high level of verbosity, they contain information about where the client is originating from for logging purposes. The AVPs that the device will send are:

- Message-Authenticator
  - Used in password authentication.
- Service-Type
  - Set to “Framed-User”.
- Username
  - Contains the unencrypted username attempting to authenticate.
- Framed MTU
  - Set to twelve (12) less than the network MTU to account for the 802.11 overhead.
  - In a typical 1500 MTU network, this will be set to “1488”.
- Called-Station-Id
  - Set to the MAC address of the Netvanta 150, followed by a colon, followed by the SSID the client is attempting to connect to.
  - Example is “<Netvanta 150 MAC Address>:<SSID>”.
- Calling-Station-Id
  - Set to the MAC address of the client attempting to connect.
- NAS-Identifier
  - Set to the “Name” parameter of the Netvanta 150 configuration.
  - If not specified in the configuration, “ADTRAN” & the last half of the MAC address will be used.
    - Example is “ADTRAN1F760B”.
- NAS-Port-Type
  - Set to “Wireless-802.11”.
- Connect Info
  - Set to “CONNECT”, followed by the maximum speed of the connection, followed by “802.11a/b/g”.
  - Example is “CONNECT 54Mbps 802.11a”.
- EAP-Message
  - An encapsulated version of the *EAP-Identity-Response* message from the client.
- NAS-IP-Address
  - Indicates the primary IP of the interface that the RADIUS request packet is sourced from.
- NAS-Port
  - Set to “1”.
- NAS-Port-Id
  - Set to “STA Port # 1”.

Configuring the RADIUS Server

The RADIUS server, using Windows Server 2003's IAS as an example, can specify multiple dependencies that must match before a particular policy is allowed to be used to authenticate a request. It is recommended that these be used to protect the RADIUS server from client authentication requests from unauthorized sources, or to ensure that each RADIUS client has the correct policy applied to it if there are multiple devices sending authentication requests. Examples of such client groups are Device Administrators, Wireless Clients, Port-Authentication, and VPN Clients.

NOTE: *Windows IAS functionality and configuration style may change. The procedures described within this document are only used as an example. ADTRAN is not responsible for configuring the RADIUS server, and will not support the RADIUS server should it be found to be the source of any errors in the authentication process. This article will only cover the Netvanta-specific configuration options within IAS; there may be further configuration on the server required to utilize IAS in this manner.*

For further information, please refer to the Microsoft KB article on IAS, which can be accessed here:

http://technet.microsoft.com/en-us/library/cc738432(WS.10).aspx

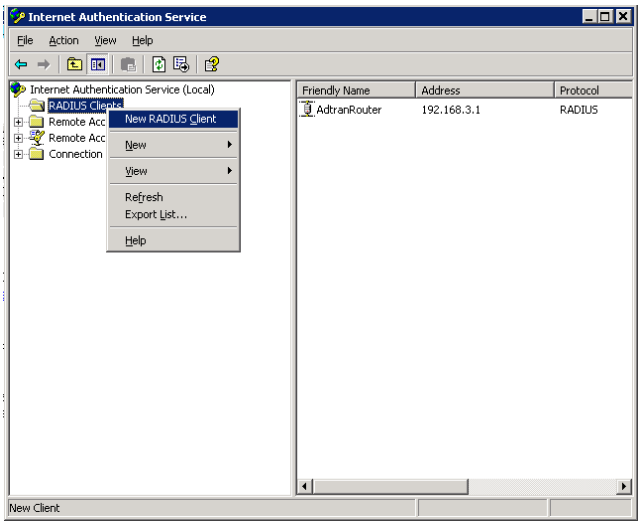
NOTE: *RADIUS implementations require the use of a SSL certificate when using PEAP authentication, and a certificate infrastructure in place if the client is intended to verify the certificate. In Windows 2003 Server, the same server that is running IAS is typically also running a Certificate server, if only for the purposes of providing IAS with a suitable certificate. Most other stand-alone RADIUS servers either require an outside certificate infrastructure, or have the ability to generate a suitable certificate for itself.*

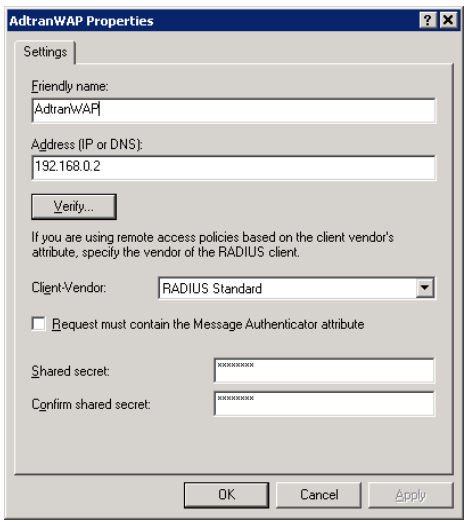
The RADIUS server's certificate is either already verifiable via the client's existing certificate infrastructure, or is pre-installed on the clients that will authenticate to the server during the setup of the client connection. The client also has the option of not verifying the certificate of the authentication server if server identity verification is not desired or required by the network administrator.

The setup of Microsoft Certificate Services will not be covered in this document. For further information, please refer to the Microsoft KB article on Certificate Services, which can be accessed here:

http://technet.microsoft.com/en-us/library/cc776207(WS.10).aspx

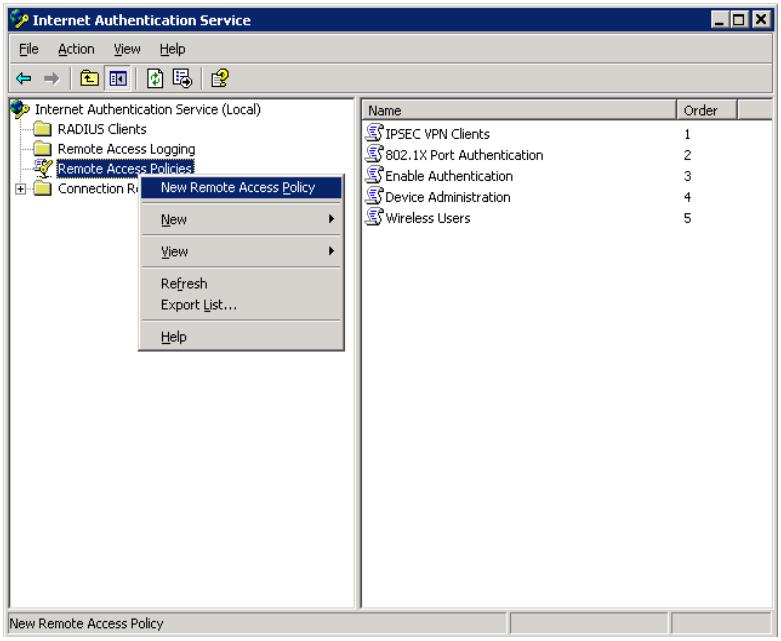
The first step to be completed in most RADIUS servers is to define the RADIUS client device, which involves specifying the Pre-Shared Key and the IP address it will be coming from. This will allow the RADIUS server to receive messages from this RADIUS client. In IAS, it is done in the following manner:

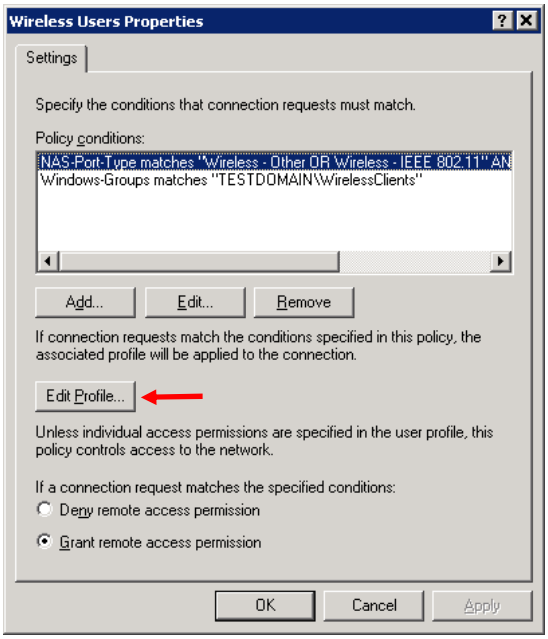


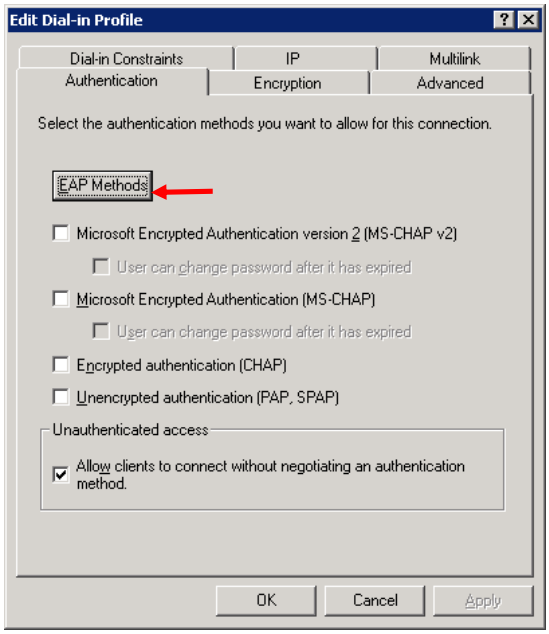


The next step is to create the policy that will process the request, ensure that it matches the required AVPs for this connection type, and permit or deny the request.

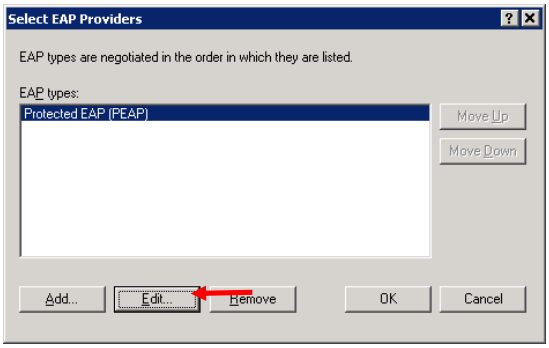
The RADIUS server will need to define the AVPs that will remain static within all authentication attempts from this RADIUS client & change the authentication process to allow PAP authentication without negotiation. In IAS, it is done in the following manner:

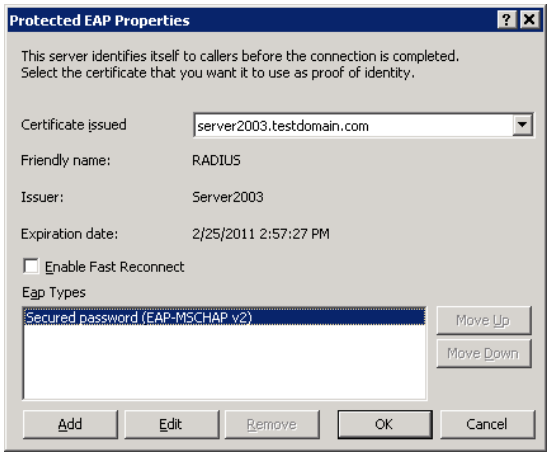






NOTE: *The "NAS-Port-Type" is sufficient to distinguish this policy from other AOS / Netvanta RADIUS requests. Additional AVPs can be matched upon if the policy conditions are required to be more specific.*



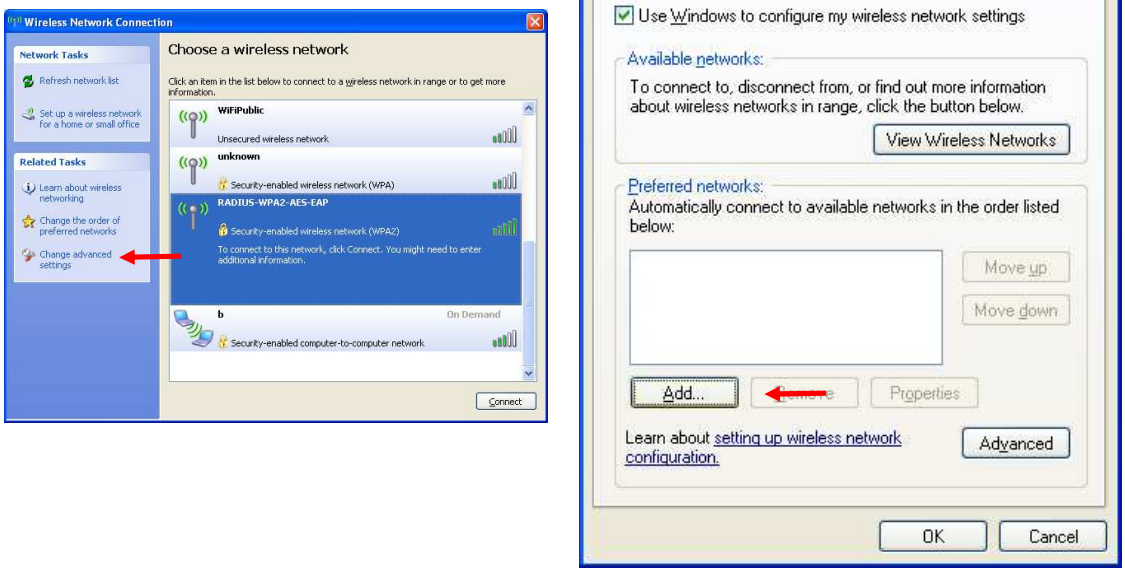


Configuring the Wireless Client

The wireless client must support 802.1X to connect to an EAP-authenticated wireless network. This section will provide an example setup for a wireless client using the Microsoft Wireless Zero utility under Windows XP as an example.

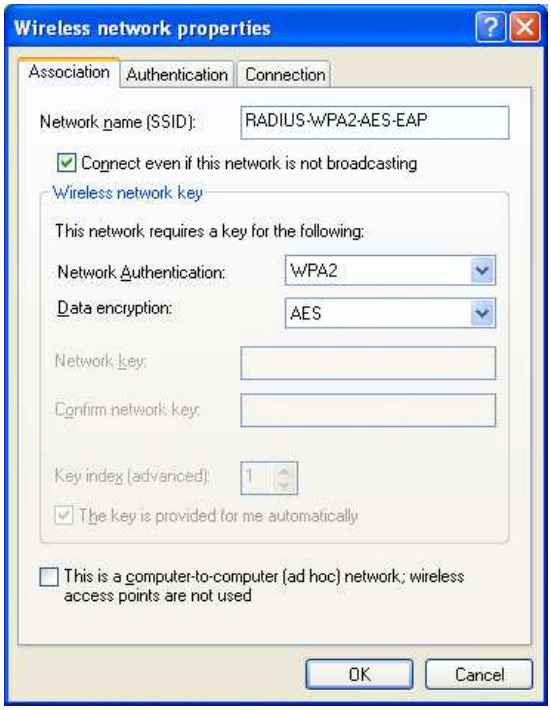
NOTE: *Microsoft Wireless Zero configuration style may change; other wireless clients may have different configuration procedures. The procedures described within this document are only used as an example. ADTRAN is not responsible for configuring the wireless client, and will not support the wireless client should it be found to be the source of any errors in the authentication process.*

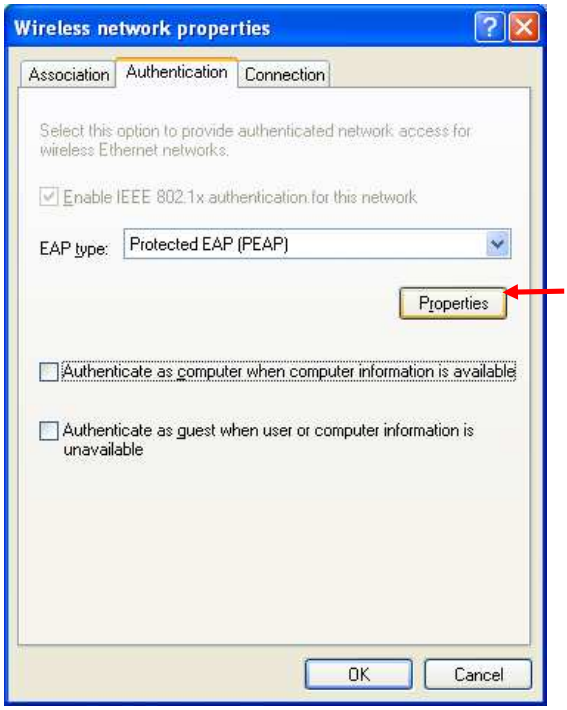
The first step is to identify the wireless network that the client will connect to and note the SSID. If the network is in non-broadcast mode, the SSID will need to be known in advance. Enter the "Advanced" setting page:



The next step is to add a new "Preferred Network". Under the "Association" tab, enter the SSID, Network Authentication and Data Encryption. If the network is non-broadcast the "Connect even it this network is not broadcasting" checkbox should also be checked.

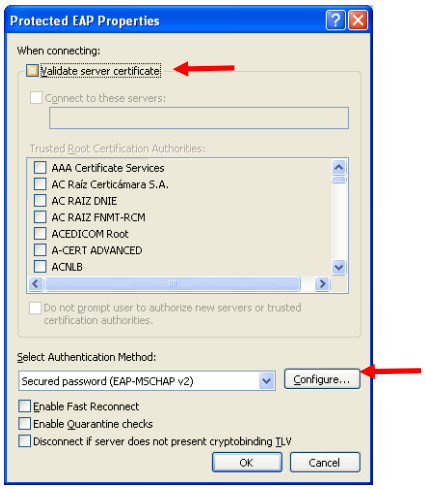
Under the "Authentication" tab, the "EAP type" should be set to "PEAP" and both checkboxes unchecked.

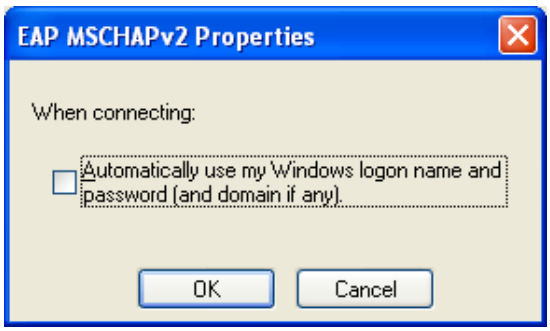




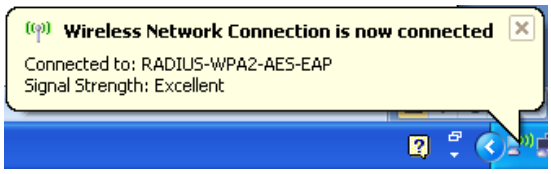
If the server certificate is part of an existing certificate infrastructure that can be validated, or if the server certificate will be pre-installed on the wireless client, the "Validate server certificate" option can be used. In every other case, this option should be disabled.

The authentication method should be set to "EAP-MSCHAP v2". If the Windows logon username and password will match what the RADIUS server is expecting, then that can be used. If it will not match, that option should be disabled.





After applying the new settings and locating the wireless network, Windows will prompt for the logon credentials. After the correct logon credentials have been entered and the authentication process succeeds, the user can access the wireless network.



Troubleshooting

The Netvanta 150 does not have a local management interface, and the controller is not involved in the authentication scheme. Therefore, any troubleshooting must be done with packet captures and/or from the perspective of the RADIUS server. Please contact Adtran Technical Support if you believe the Netvanta 150 is not transmitting the RADIUS Request packets, or is not operating properly in response to a particular RADIUS message.