6ABSCG0002-29C
April 2018

ADTRAN

Configuration Guide

vWLAN External RADIUS 802.1x Authentication

This configuration guide provides an in-depth look at external Remote Authentication Dial-In User Service (RADIUS) 802.1x authentication and its configuration and use with ADTRAN Bluesocket virtual wireless local area network (vWLAN) products. Included in this guide are an overview of RADIUS authentication, information about authentication with Microsoft Windows Server 2008 R2 Enterprise, Network Policy Server (NPS), and Microsoft Windows 7 clients, step-by-step configurations for external vWLAN machine and user authentication, and general troubleshooting information.

This guide consists of the following sections:

- *802.1x Authentication Protocols on page 4*
- *802.1x Authentication Certificates on page 6*
- *802.1x Authentication Methods on page 9*
- *Configuring vWLAN and BSAPs for Machine and User Authentication on page 11*
- *Configuring Windows Server 2008 R2 Enterprise for Authentication on page 18*
- *Configuring the Windows 7 Client for Authentication on page 48*
- *Additional vWLAN Authentication Configurations on page 57*
- *Troubleshooting on page 64*

RADIUS 802.1x Authentication Overview

802.1x is an Institute of Electrical and Electronics Engineers (IEEE) standard for port-based network access control that provides a framework for authentication, authorization, and dynamic encryption key management. With 802.1x, all non-authenticated traffic entering the network is blocked at the ingress port until it is successfully authenticated. Once the traffic is authenticated, it passes through the port, and the source user or device is authorized to access network resources. Although it was originally designed for use in wired networks, 802.1x has been adapted for use in WLANs, where the port of entry is the virtual port or port entity.

Three main components comprise the 802.1x authentication framework: the supplicant, the authenticator, and the authentication server. Each component has a specific function and works with the other components to ensure only successfully authenticated users and devices are authorized to access network resources. Users and devices are validated using the Layer 2 Extensible Authentication Protocol (EAP). *Figure 1* illustrates the three components of 802.1x authentication.

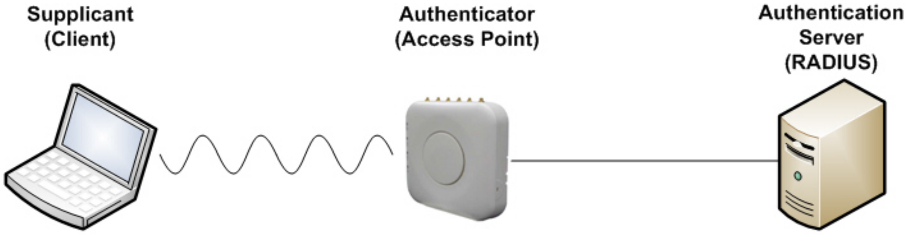


Figure 1. Components of 802.1x Authentication

The Supplicant

The first component of 802.1x authentication is the supplicant. The supplicant is a client-side device, such as a laptop, tablet, or handheld device, which requests authentication and authorization to the WLAN using credentials, such as a user name and password, or a certificate. The term supplicant can also refer to the software running on the client device. Each supplicant sends EAP authentication messages to the authentication server using Layer 2 EAP over LAN (EAPOL) encapsulation to request authorization to access the WLAN.

Supplicants can be built into operating systems, such as with the Microsoft Windows 7 WLAN AutoConfig supplicant, they can be provided by the WLAN client adapter vendor, as with Intel PROSet Utility, or they can be purchased from a third party, as with the Juniper networks' Odyssey Access Client (OAC). Best practices suggest that only one supplicant type per device should be used. For example, choose the built-in WLAN AutoConfig supplicant on all Microsoft Windows 7 devices.

The Authenticator

The authenticator is a network device, such as an access point (AP), that blocks all traffic through its port entity with the exception of EAP authenticated traffic, until successful authentication occurs. The authenticator encapsulates the EAP authentication messages received from the supplicant into the RADIUS protocol and forwards them to the authentication server. The authenticator plays the role of the intermediary, passing authentication messages between the supplicant and authentication server. Each authenticator maintains two virtual ports: an uncontrolled and a controlled port. The uncontrolled port allows EAP authenticated traffic to pass through, while the controlled port blocks all other traffic until successful authentication occurs.

As the authenticator, the AP or WLAN controller must be configured to point to the IP address of one or more authentication or RADIUS servers, it must be configured with the appropriate User Datagram Protocol (UDP) ports being used by the RADIUS server, and it must be configured with a shared secret. RADIUS servers use ports 1645 and 1812 for authentication and ports 1646 and 1813 for accounting. A shared secret exists between the authenticator and authentication server so that they can validate each other.

The Authentication Server

The authentication server is a server that validates the credentials of the supplicant that is requesting authentication and authorization to the WLAN. This server is typically a RADIUS server that maintains a user data base (or it can proxy to another external database, such as Microsoft Active Directory (AD) or Lightweight Directory Access Protocol (LDAP)). Upon successful authentication, the server sends a RADIUS accept packet to the supplicant via the authenticator. The authenticator forwards the message to the supplicant in an EAP success frame, completes a 4-way handshake negotiation to generate dynamic encryption keys, unblocks the controlled port of the authenticator, and authorizes the supplicant to access network resources. After authorization is given, the supplicant can then obtain an IP address using Dynamic Host Control Protocol (DHCP).

The 802.1x authentication exchange between the three components is described in *Figure 2*.

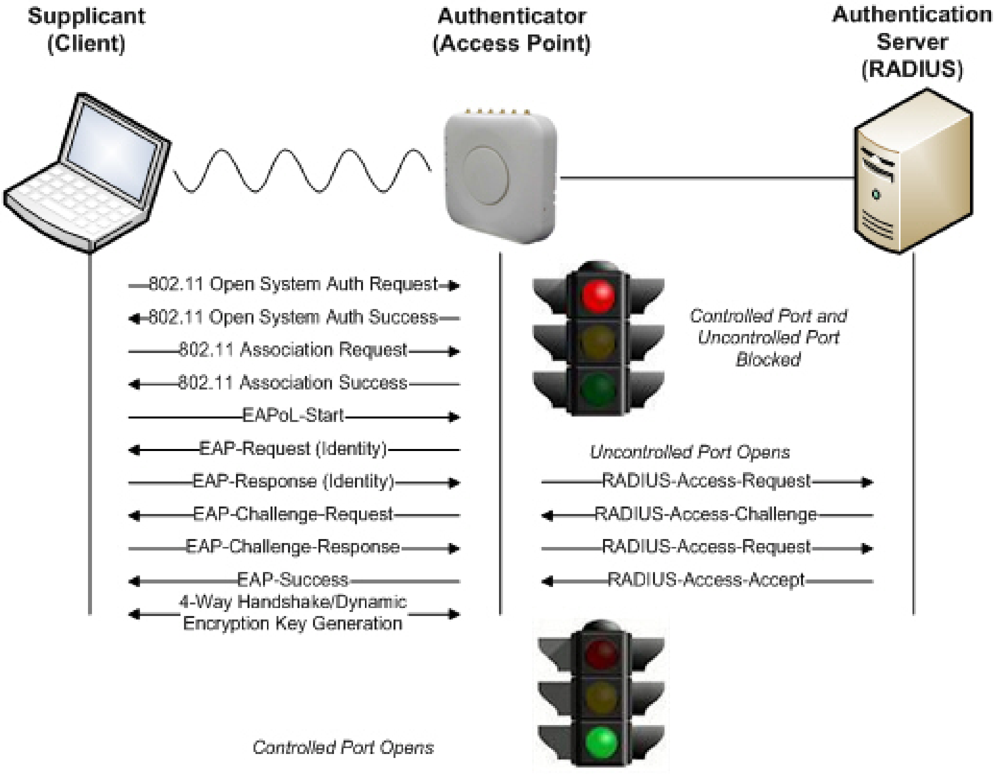
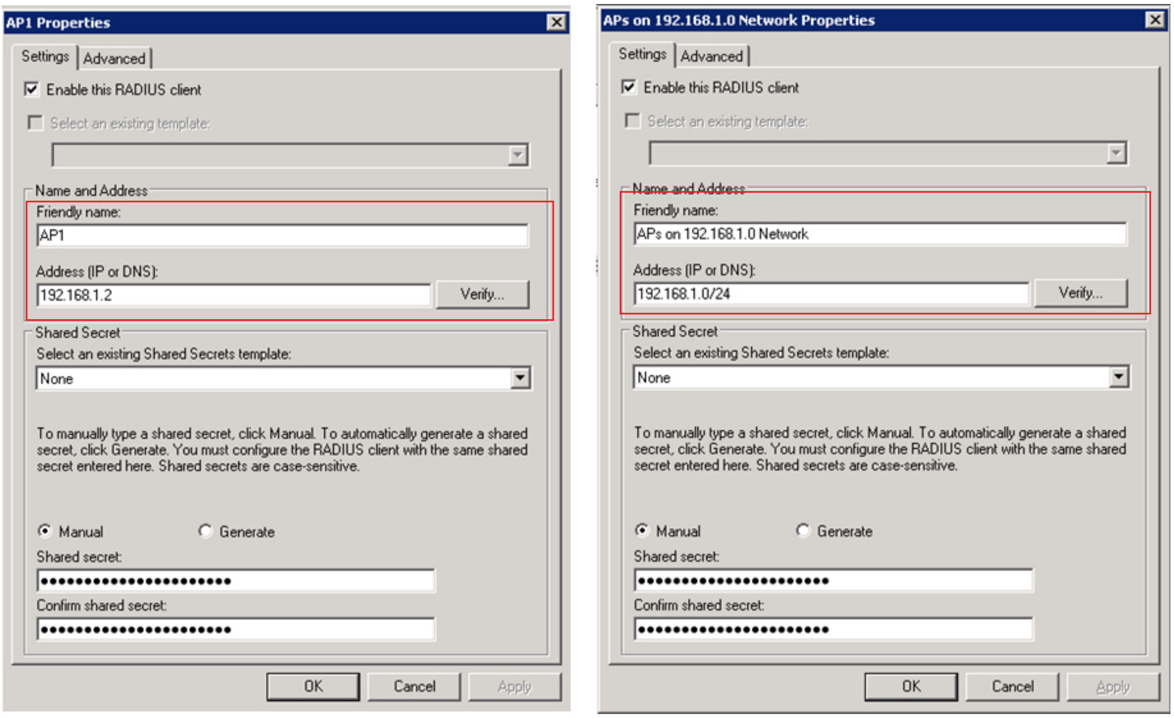


Figure 2. The 802.1x Authentication Exchange

When configuring the authentication server, you must create a RADIUS client with the IP address and shared secret for each AP or WLAN controller. When using external RADIUS 802.1x on the vWLAN, the APs send the RADIUS requests directly to the RADIUS server. This means the RADIUS server should be configured with a RADIUS client for each AP. Alternatively, a RADIUS client can be configured in the

RADIUS server with a range of IP addresses. Microsoft Windows Server 2008 R2 Enterprise NPS allows you to configure a range of IP addresses in the address field by using Classless Inter-Domain Routing (CIDR) notation. For example, if the APs are all on the 192.168.1.0/255.255.255.0 network, you can enter 192.168.1.0 /24 in the address field. *Figure 3* displays the NPS configurations of a RADIUS client for a single AP and for an entire subnet of APs using CIDR notation.



AP1 Properties

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: AP1

Address (IP or DNS): 192.168.1.2

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••••••••••••••••

Confirm shared secret: ••••••••••••••••••••••

APs on 192.168.1.0 Network Properties

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: APs on 192.168.1.0 Network

Address (IP or DNS): 192.168.1.0/24

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: •••••••••••••••••••••

Confirm shared secret: •••••••••••••••••••••

NPS configuration of RADIUS client for a single AP.

NPS configuration of a RADIUS client for a subnet of APs.

Figure 3. NPS Configurations of RADIUS Client

> NOTE
>
> *A range of IP addresses can be entered with Microsoft Windows Server 2008 R2 Enterprise NPS, however, Microsoft Windows Server 2008 R2 Standard NPS does not support configuring a RADIUS client with a range of IP addresses. In addition, the standard version will only support up to 50 RADIUS clients.*

802.1x Authentication Protocols

802.1x authentication and authorization uses EAP to validate clients on the network. There are, however, several types of EAP that can be used in 802.1x authentication. The types of EAP that are available are discussed in the following sections.

EAP

EAP, as defined in RFC 3748, and later updated in RFC 5247, supports multiple authentication methods. EAP was originally adopted for use with Point-to-Point Protocol (PPP), but has since been redefined for use with 802.1x port-based network control. EAP is a Layer 2 protocol used within the 802.1x framework to validate users and devices. It is flexible in that there are many different EAP methods available. Some are proprietary, while others are standards based; some provide mutual authentication while others do not; some require both server and client-side certificates, while some require only server-side certificates and others require no certificates at all. Some methods use user names and passwords, others use tokens; some support machine or computer authentication, while others do not; and some send credentials inside an encrypted tunnel (resulting in stronger security), while others do not. Although there are many EAP methods from which to select, this document focuses on the most common EAP method: EAP-Protected Extensible Authentication Protocol version 0 (EAP-PEAPv0).

EAP-PEAP

To discuss EAP-PEAPv0, you must first know the basics of EAP-PEAP, also known as PEAP. This protocol offers flexibility similar to EAP, by providing many different PEAP methods. Unlike EAP, however, PEAP has two supplicant identities and phases rather than one. The supplicant identities in PEAP are called the inner and outer identities. The outer identity is effectively a bogus user name sent in clear text outside of a Transport Layer Security (TLS) encrypted tunnel. For many supplicants, this identity is anonymous; however, it can be configured in certain supplicants. The inner identity is the true identity of the supplicant, which is sent inside an encrypted TLS tunnel and therefore is protected. This protection is particularly important in wireless applications because EAP occurs during the 802.1x authentication process, before wireless frames are encrypted. Each identity is sent in a different phase of PEAP authentication: the outer identity is sent in phase one, and the inner identity is sent in phase two.

NOTE

The encryption that occurs for the inner identity in the second phase of authentication is not the same as the Layer 2 encryption used to encrypt wireless data over the air (such as, AES/TKIP). This encrypted TLS tunnel is created and only exists for a matter of milliseconds with the sole purpose of providing a secure channel to protect user credentials. In order for the TLS tunnel to be established, a server-side certificate must be installed on the RADIUS Server. Certificates are discussed in detail in 802.1x Authentication Certificates on page 6.

PEAPv0 refers to the outer EAP method, and is the mechanism used in phase one of the authentication process to create a secure TLS tunnel. The tunnel then protects subsequent authentication transactions in phase two. Because the TLS tunnel protects authentication transactions in phase two, password-based authentication protocols that are normally susceptible to offline dictionary attacks (like Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)) can be used for authentication. EAP-MSCHAPv2 is referred to as the inner EAP method.

EAP-PEAPv0 (EAP-MSCHAPv2)

EAP-PEAPv0 with EAP-MSCHAPv2 is also known as PEAP-MSCHAPv2, and is a mutual authentication method that supports password-based user or computer authentication. EAP-PEAPv0 (EAP-MSCHAPv2) is the most common form of PEAP in use today because it uses simple user names and passwords instead of complex client-side certificates. It also has extensive operating system support, including Microsoft Windows, Apple OS X/iOS, Linux, Android, Blackberry, and others. MSCHAPv2, defined in RFC 2759, is Microsoft’s version of CHAP. Like CHAP, the password of the user identity is encrypted using a hash value. Microsoft initially developed MS-CHAP as a proprietary version of CHAP and subsequently released MS-CHAPv2 to address security vulnerabilities in the original version. MS-CHAPv2 introduced a much stronger hashing algorithm and also added support for mutual authentication during the

MS-CHAPv2 exchange. Like MS-CHAP, however, MS-CHAPv2 has since been found to be vulnerable and therefore should only be used inside a TLS tunnel. *Figure 4* illustrates the authentication process using EAP, EAP-PEAP, and EAP-PEAPv0 (EAP-MSCHAPv2).

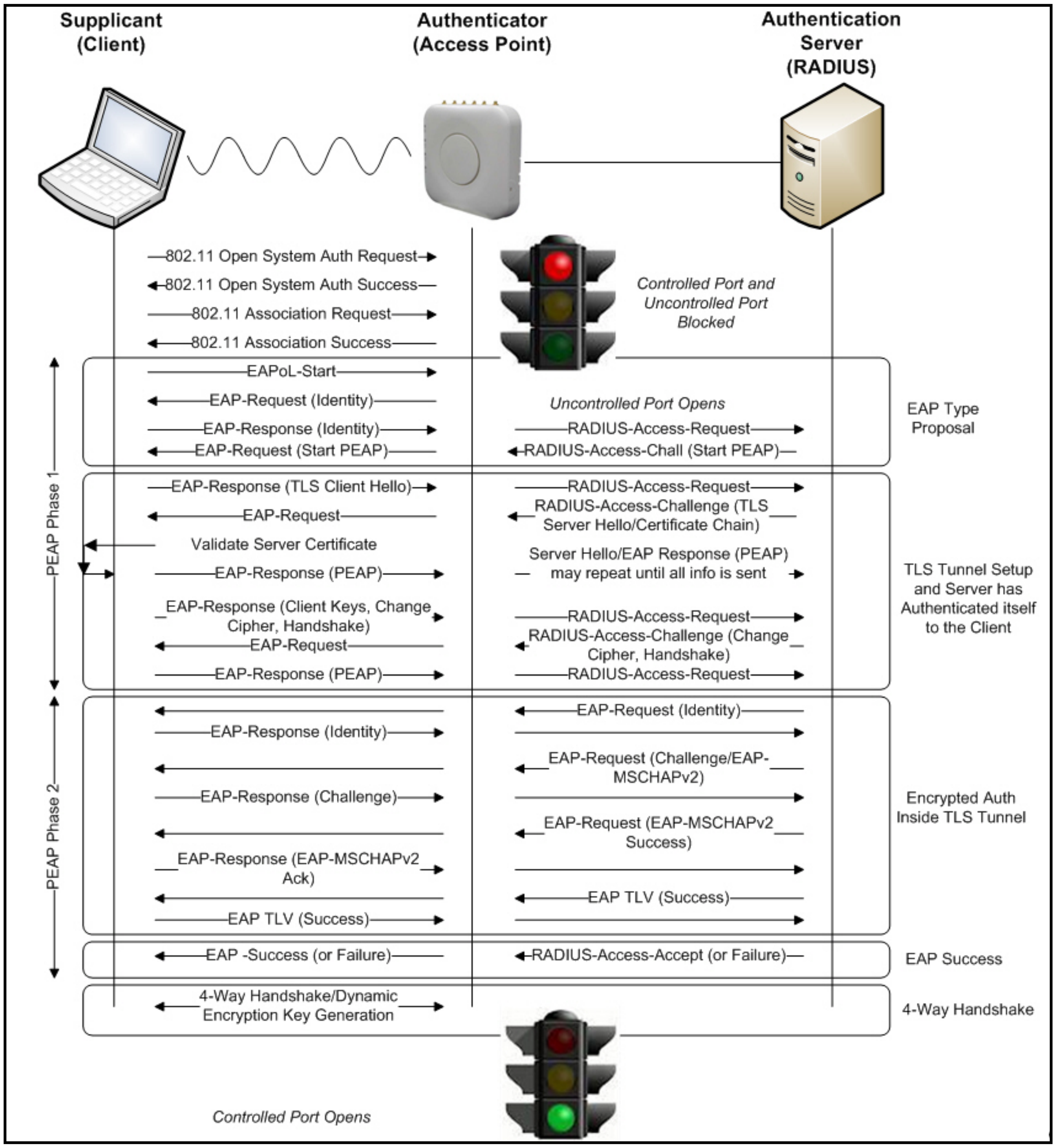

Supplicant (Client)
Authenticator (Access Point)
Authentication Server (RADIUS)
802.11 Open System Auth Request
802.11 Open System Auth Success
802.11 Association Request
802.11 Association Success
Controlled Port and Uncontrolled Port Blocked
EAPoL-Start
EAP-Request (Identity)
EAP-Response (Identity)
EAP-Request (Start PEAP)
Uncontrolled Port Opens
RADIUS-Access-Request
RADIUS-Access-Chall (Start PEAP)
EAP Type Proposal
PEAP Phase 1
EAP-Response (TLS Client Hello)
EAP-Request
Validate Server Certificate
EAP-Response (PEAP)
EAP-Response (Client Keys, Change Cipher, Handshake)
EAP-Request
EAP-Response (PEAP)
RADIUS-Access-Request
RADIUS-Access-Challenge (TLS Server Hello/Certificate Chain)
Server Hello/EAP Response (PEAP) may repeat until all info is sent
RADIUS-Access-Request
RADIUS-Access-Challenge (Change Cipher, Handshake)
RADIUS-Access-Request
TLS Tunnel Setup and Server has Authenticated itself to the Client
PEAP Phase 2
EAP-Response (Identity)
EAP-Response (Challenge)
EAP-Response (EAP-MSCHAPv2 Ack)
EAP TLV (Success)
EAP-Request (Identity)
EAP-Request (Challenge/EAP-MSCHAPv2)
EAP-Request (EAP-MSCHAPv2 Success)
EAP TLV (Success)
Encrypted Auth Inside TLS Tunnel
EAP -Success (or Failure)
RADIUS-Access-Accept (or Failure)
EAP Success
4-Way Handshake/Dynamic Encryption Key Generation
4-Way Handshake
Controlled Port Opens

Figure 4. Authentication Process Using EAP, EAP-PEAP, and EAP-PEAPv0 (EAP-MSCHAPv2)

802.1x Authentication Certificates

EAP-PEAPv0 (EAP-MSCHAPv2) requires a server certificate to be installed on the RADIUS server in order to establish a secure TLS tunnel. Client computer and user certificates are not required for EAP-MSCHAPv2 because it is password-based. If mutual authentication is configured, the server certificate must be trusted by the client. This requires the certificate authority (CA) certificate to be installed on the client (refer to *Mutual Authentication on page 9* for more information). Server, client computer, user, and CA certificates used for authentication are described in the following sections.

Server Certificates

The server certificate is issued to a RADIUS server by a public or private CA. It is used to establish a secure TLS tunnel and is necessary when the RADIUS server needs to prove its identity to the client. EAP-PEAPv0 (EAP-MSCHAPv2) requires a server certificate to be installed on the RADIUS server.

Client Computer Certificates

Client computer certificates are issued to client computers by a public or private CA and are used when the client computer needs to prove its identity to the RADIUS server. Client computer certificates are not required for EAP-PEAPv0 (EAP-MSCHAPv2) because it is password-based.

User Certificates

User certificates are issued to individuals by a public or private CA and are typically distributed as a certificate that is embedded on a smart card. The certificate on the smart card is used along with a smart card reader attached to the client computer and provides a method for individuals to prove their identity to NPS servers during the authentication process (refer to *Certificates and NPS Servers on page 7* for information about certificates and NPS servers). User certificates are not required for EAP-PEAPv0 (EAP-MSCHAPv2) because it is password-based.

CA Certificates

When CA certificates are present on client and server computers, they tell the client or server that it can trust other certificates (such as, certificates used for client or server authentication) issued by this CA. If mutual authentication is configured, the server certificate must be trusted by the client. This requires that the CA certificate is installed on the client. Refer to *Mutual Authentication on page 9* for more information.

Certificates and NPS Servers

There are two methods for deploying NPS server certificates. They can be purchased from a public root CA, such as VeriSign, that is already trusted by the client or a private CA can be deployed on your network using Active Directory Certificate Services (AD CS). There are advantages and disadvantages to both methods.

Public Root CAs

Advantages of purchasing a certificate from a public root CA that is already trusted by the client include:

- Installation of purchased certificates does not require as much specialized knowledge as deploying a private CA on the network, and it can be easier to deploy in networks that only have a few NPS servers.
- The use of purchased certificates can prevent specific network security vulnerabilities that can exist if the proper precautions were not taken when a private CA was deployed on the network.
- There is no requirement to distribute private CA certificates to clients. The NPS server is trusted by the client because the client already trusts the public root CA that issued the NPS certificate.

> NOTE *This is required for mutual authentication.*

Disadvantages of purchasing a certificate from a public root CA that is already trusted by the client include:

- Public root CA deployments to not scale as well as deployments using a private CA because each NPS server requires a different certificate. Therefore, deployment costs increase with each NPS server deployed.
- Purchased certificates have recurring costs because they must be renewed.

Private CAs

Advantages of deploying private CAs by using AD CS include:

- Windows Server 2008 includes AD CS.
- Network scaling is easier using private CAs and AD CS than with public CAs. After a private CA is deployed in the network, AD CS can automatically distribute certificates to all NPS servers in your domain with no incremental increases in cost, even if NPS servers are added to the network later.
- With AD CS, server certificates can be automatically distributed to any new NPS servers that are added to the network.
- Private CA certificates are automatically distributed to domain users and computers by AD CS to the Trusted Root Certificate Authorities store of the user and computer. The NPS server is trusted by the client because the client trusts the private CA that issued the NPS server certificate.

> NOTE *This is required for mutual authentication.*

- Using an AD CS-based private CA allows you to more easily change your authentication infrastructure from secure password authentication (using PEAP) to one that requires client certificates (using either EAP-TLS or PEAP-TLS).

Disadvantages of deploying private CAs by using AD CS include:

- Deployment of a private CA on the network requires more specialized knowledge than purchased certificates and they can be more difficult to deploy.
- Your network can be exposed to specific security vulnerabilities if the proper precautions are not taken when deploying private CAs on the network.
- Non-domain computers must have the private CA certificate manually installed in the Trusted Root Certification Authorities store for them to trust the NPS server certificate that was issued by the private CA, or the client will have to accept the certificate manually upon their first connection.

> NOTE *This is required for mutual authentication.*

802.1x Authentication Methods

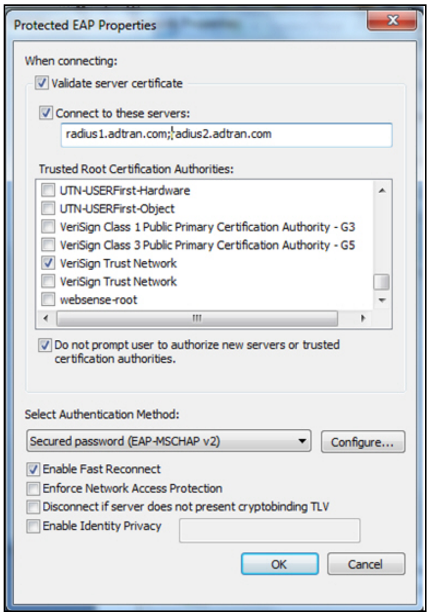
There are several methods that can be used for 802.1x authentication, including mutual authentication, machine (computer) authentication, and fast reconnect or session resumption. These authentication methods are described in the following sections.

Mutual Authentication

Mutual authentication requires both the server and client to authenticate each other. In order to configure mutual authentication, the NPS server must have a server certificate installed, the client must trust that server certificate, and the client must be configured to validate that server certificate. Validating the server certificate reduces potentials risks of man-in-the-middle and password-based attacks. In addition, the client should be configured by the administrator to connect to specific authentication servers, limit the trusted root CAs available for use with PEAP, and not give users the ability to authorize new servers or trusted CAs. Although client computer and user certificates are not required with EAP-PEAPv0 (EAP-MSCHAPv2), in order for the client to trust the server certificate the private CA certificate from the CA that issued the NPS certificate must be installed in the Trusted Root Certification Authorities store on the client.

Ideally, these settings and the private CA certificates are distributed to the clients using group policies and AD CS. Alternatively, a certificate purchased from a public root certificate authority that is already trusted by the client can be installed on the server and would not require the distribution of private CA certificates to the clients.

Figure 5 displays the Microsoft Windows 7 recommended settings for mutual authentication. These settings reduce the potential risks against man-in-the-middle and password-based attacks by validating server certificates, only allowing connections to specific RADIUS server, limiting trusted roots CAs, and not prompting users to authorize new servers or trusted CAs.



Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

radius1.adtran.com;radius2.adtran.com

Trusted Root Certification Authorities:

- ☐ UTN-USERFirst-Hardware
- ☐ UTN-USERFirst-Object
- ☐ VeriSign Class 1 Public Primary Certification Authority - G3
- ☐ VeriSign Class 3 Public Primary Certification Authority - G5
- ☑ VeriSign Trust Network
- ☐ VeriSign Trust Network
- ☐ websense-root

☑ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

☐ Enforce Network Access Protection

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

Figure 5. Windows 7 Recommended Mutual Authentication Settings

Machine (Computer) Authentication

External RADIUS 802.1x authentication on vWLAN is required to support EAP-PEAPv0 (EAP-MSCHAPv2) machine (computer) authentication. Machine authentication allows the domain computer to authenticate before the user logs into vWLAN, and uses the host or machine name (host/computername.domain) as the user name and the domain computer's account password as the password. The domain computer account password is automatically created when the computer is registered to the vWLAN domain, thus allowing group policies and login scripts to be applied and executed when the user logs into vWLAN and allowing a user who does not have a locally cached profile on the domain computer to log into vWLAN.

Machine authentication emulates a wired connection. Without machine authentication, you cannot apply group policies or run login scripts in order to map drives or connect printers. Users who have not logged on to the domain computer previously will not be able to login.

If you do not require group policies, login scripts, or the ability for non-cached domain users to log in, you may not be required to implement machine authentication.

Machine authentication is enabled by default on Microsoft Windows 7.

Fast Reconnect and Session Resumption

Fast reconnect, also known as session resumption, allows faster reauthentication and roaming between APs. This process caches the TLS session created during PEAP phase one authentication after a successful PEAP phase two authentication for both the client and the server. Upon subsequent reauthentications, the session can be resumed using a simpler and shorter TLS handshake process and skipping the inner authentication method. Fast reconnect results in an overall 50 percent reduction in traffic exchanged with the RADIUS server, and usually takes approximately 300 ms to complete. Roam times can be longer if, for example, the RADIUS server is on a wide area network (WAN) circuit.

Although this is a significant improvement over full authentication, fast reconnect is still not fast enough to support real time applications such as voice over IP (VoIP), and is therefore not supported by vWLAN. Therefore, fast reconnect should be disabled on both the client and RADIUS server when configuring PEAP with vWLAN. If fast reconnect is enabled, a full RADIUS exchange is not completed and the user might not be placed into the proper role.

Configuring vWLAN and BSAPs for Machine and User Authentication

vWLAN and its associated Bluesocket APs (BSAPs) can be configured for machine and user authentication using the vWLAN graphical user interface (GUI). The vWLAN and any APs must be configured prior to configuring authentication, and the APs must have discovered the vWLAN, its locations (virtual local area networks (VLANs), subnets, and subnet masks), and they must be licensed. For information about these topics, refer to the *Bluesocket vWLAN Administrator's Guide* for vWLAN version 2.2.1 and later, available online at https://supportforums.adtran.com.

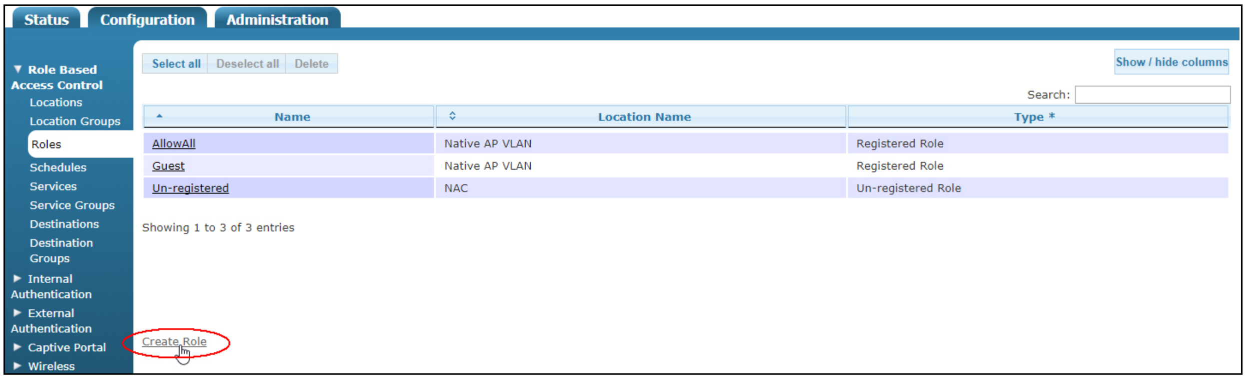
The configuration of machine and user authentication on vWLAN requires connecting to the vWLAN GUI and following these steps:

- *Step 1: Creating Roles for Machine and User Authentication on page 11*
- *Step 2: Configuring the External RADIUS 802.1x Authentication Server on page 14*
- *Step 3: Configure the SSID on page 16*

Step 1: Creating Roles for Machine and User Authentication

To create the roles in vWLAN for machine and user authentication, you will first create a role for the machines that require authentication on the domain, and then create a role for user authentication. Follow these steps:

1. In the vWLAN GUI, navigate to the **Configuration** tab, and select **Role Based Access Control** > **Roles**. Select **Create Role** at the bottom of the menu, or select **Domain** > **Role** from the **Create** drop-down menu.



Name	Location Name	Type *
AllowAll	Native AP VLAN	Registered Role
Guest	Native AP VLAN	Registered Role
Un-registered	NAC	Un-registered Role

Showing 1 to 3 of 3 entries

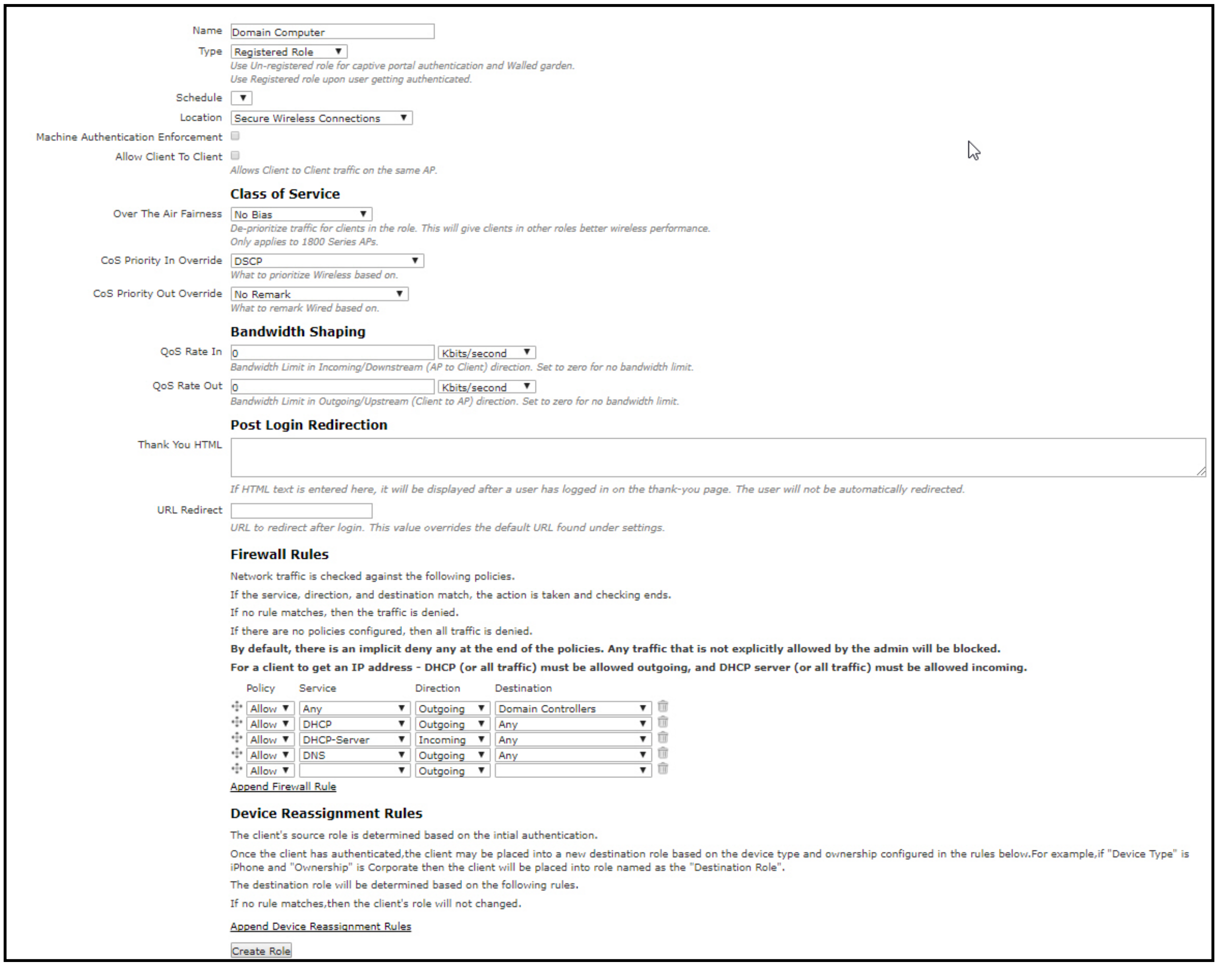
Figure 6. Navigating to the Create Role Menu

2. In the role creation menu, create a new role for the domain computers. Upon successful machine authentication, the devices will be placed in this role.

> *If machine authentication is not required, you do not have to create a role for the machines or computers.*

This role is typically called **Domain Computer**, and generally has the same location assigned as the role used for user authentication (Step 3). This role normally only allows access to a destination group containing the domain controllers in order to be able to perform authentication and run login scripts. If the domain controllers are not providing DHCP or domain name system (DNS), you will have to configure the role to allow DHCP and DNS. This role is typically configured so that access is only allowed to a destination group containing the domain controllers in order to prevent a stolen machine from having full network access without a user logging in.

Configure the Domain Computer role by specifying the name, location, and the appropriate firewall rules. You can optionally specify any quality of service (QoS) or class of service (CoS) parameters for the role, as well as assign any post-login redirections. The example in *Figure 7* below configures the **Domain Computer** role with a location of the previously created location group **Secure Wireless Connections**. In addition, the role is configured to allow a service of **Any** for outgoing traffic to the previously created destination group **Domain Controllers**, and to allow DHCP, DHCP server, and DNS to a destination of **Any**. Select **Create Role** to create the machine authentication (Domain Computer) role.



Name: Domain Computer
Type: Registered Role ▼
Use Un-registered role for captive portal authentication and Walled garden.
Use Registered role upon user getting authenticated.
Schedule: ▼
Location: Secure Wireless Connections ▼
Machine Authentication Enforcement ☐
Allow Client To Client ☐
Allows Client to Client traffic on the same AP.

Class of Service

Over The Air Fairness: No Bias ▼
De-prioritize traffic for clients in the role. This will give clients in other roles better wireless performance.
Only applies to 1800 Series APs.
CoS Priority In Override: DSCP ▼
What to prioritize Wireless based on.
CoS Priority Out Override: No Remark ▼
What to remark Wired based on.

Bandwidth Shaping

QoS Rate In: 0 Kbits/second ▼
Bandwidth Limit in Incoming/Downstream (AP to Client) direction. Set to zero for no bandwidth limit.
QoS Rate Out: 0 Kbits/second ▼
Bandwidth Limit in Outgoing/Upstream (Client to AP) direction. Set to zero for no bandwidth limit.

Post Login Redirection

Thank You HTML:
If HTML text is entered here, it will be displayed after a user has logged in on the thank-you page. The user will not be automatically redirected.
URL Redirect:
URL to redirect after login. This value overrides the default URL found under settings.

Firewall Rules

Network traffic is checked against the following policies.

If the service, direction, and destination match, the action is taken and checking ends.

If no rule matches, then the traffic is denied.

If there are no policies configured, then all traffic is denied.

By default, there is an implicit deny any at the end of the policies. Any traffic that is not explicitly allowed by the admin will be blocked.

For a client to get an IP address - DHCP (or all traffic) must be allowed outgoing, and DHCP server (or all traffic) must be allowed incoming.

Policy	Service	Direction	Destination
Allow ▼	Any ▼	Outgoing ▼	Domain Controllers ▼
Allow ▼	DHCP ▼	Outgoing ▼	Any ▼
Allow ▼	DHCP-Server ▼	Incoming ▼	Any ▼
Allow ▼	DNS ▼	Outgoing ▼	Any ▼
Allow ▼	▼	Outgoing ▼	▼

Append Firewall Rule

Device Reassignment Rules

The client's source role is determined based on the intial authentication.

Once the client has authenticated,the client may be placed into a new destination role based on the device type and ownership configured in the rules below.For example,if "Device Type" is iPhone and "Ownership" is Corporate then the client will be placed into role named as the "Destination Role".

The destination role will be determined based on the following rules.

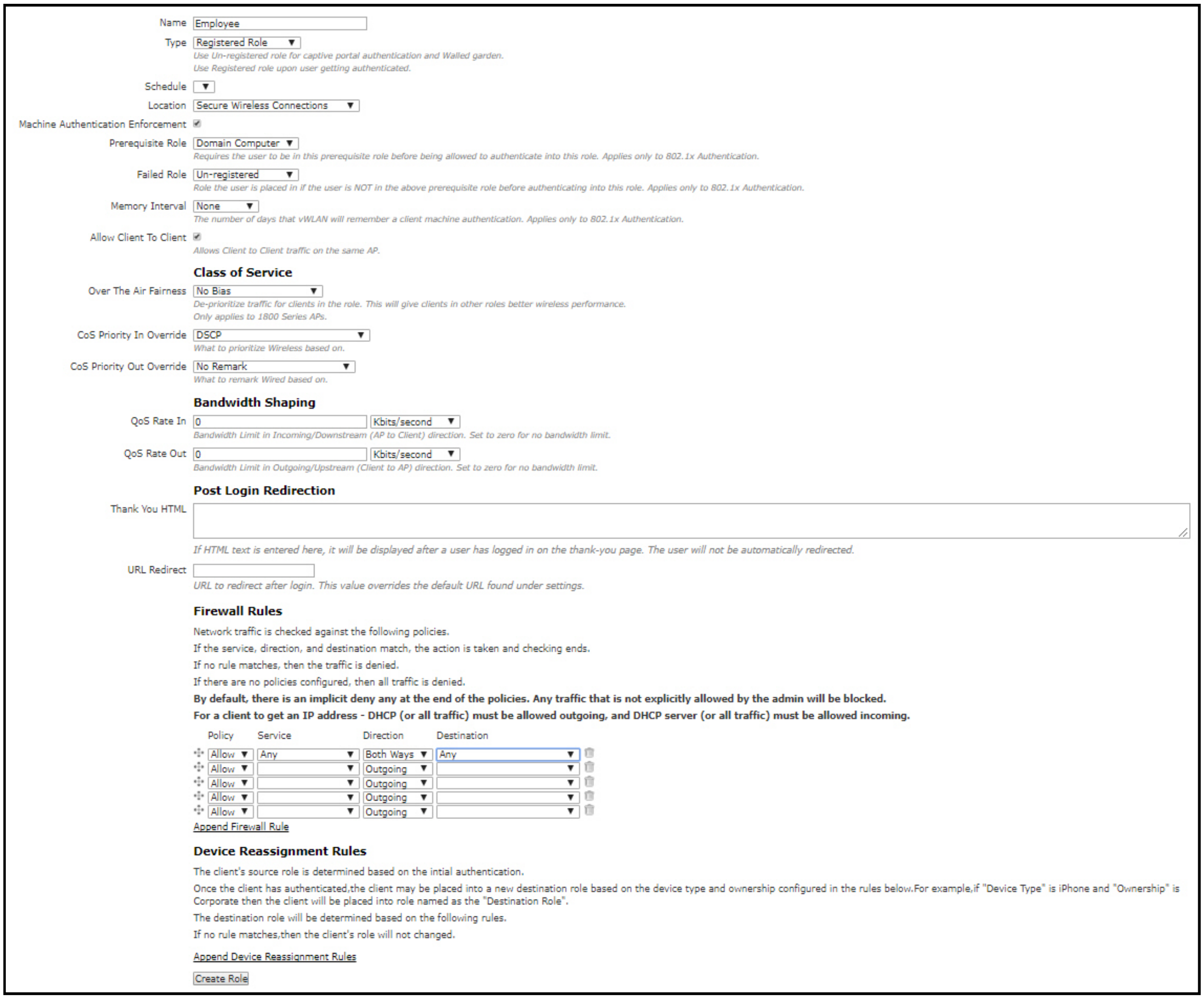
If no rule matches,then the client's role will not changed.

Append Device Reassignment Rules

Figure 7. Configuring the Domain Computer Role

3. After creating the machine authentication (Domain Computer) role, repeat Step 1 to create a role for user authentication where machine authentication will be enforced. In the role creation menu, specify the name, location, enable machine authentication enforcement, select the Domain Computer role that was just created as the **Prerequisite role.**, optionally configure a **Failed role** for clients that are not domain computers, specify whether client-to-client traffic is enabled, any bandwidth limitations, and firewall rules. Upon successful user authentication, users will be placed in this role.

   In *Figure 8* below, the user authentication role **Employee** is configured with the previously created location **Secure Wireless Connections** (the same location as for machine authentication), client-to-client traffic is allowed, machine authentication is enforced, bandwidth is not limited, and the firewall rules are configured so that **Any** service is allowed both directions. Select **Create Role** to create the user authentication role.



Name: Employee

Type: Registered Role

Use Un-registered role for captive portal authentication and Walled garden.
Use Registered role upon user getting authenticated.

Schedule:

Location: Secure Wireless Connections

Machine Authentication Enforcement: ☑

Prerequisite Role: Domain Computer

Requires the user to be in this prerequisite role before being allowed to authenticate into this role. Applies only to 802.1x Authentication.

Failed Role: Un-registered

Role the user is placed in if the user is NOT in the above prerequisite role before authenticating into this role. Applies only to 802.1x Authentication.

Memory Interval: None

The number of days that vWLAN will remember a client machine authentication. Applies only to 802.1x Authentication.

Allow Client To Client: ☑

Allows Client to Client traffic on the same AP.

Class of Service

Over The Air Fairness: No Bias

De-prioritize traffic for clients in the role. This will give clients in other roles better wireless performance.
Only applies to 1800 Series APs.

CoS Priority In Override: DSCP

What to prioritize Wireless based on.

CoS Priority Out Override: No Remark

What to remark Wired based on.

Bandwidth Shaping

QoS Rate In: 0 Kbits/second

Bandwidth Limit in Incoming/Downstream (AP to Client) direction. Set to zero for no bandwidth limit.

QoS Rate Out: 0 Kbits/second

Bandwidth Limit in Outgoing/Upstream (Client to AP) direction. Set to zero for no bandwidth limit.

Post Login Redirection

Thank You HTML:

If HTML text is entered here, it will be displayed after a user has logged in on the thank-you page. The user will not be automatically redirected.

URL Redirect:

URL to redirect after login. This value overrides the default URL found under settings.

Firewall Rules

Network traffic is checked against the following policies.

If the service, direction, and destination match, the action is taken and checking ends.

If no rule matches, then the traffic is denied.

If there are no policies configured, then all traffic is denied.

By default, there is an implicit deny any at the end of the policies. Any traffic that is not explicitly allowed by the admin will be blocked.

For a client to get an IP address - DHCP (or all traffic) must be allowed outgoing, and DHCP server (or all traffic) must be allowed incoming.

Policy	Service	Direction	Destination
Allow	Any	Both Ways	Any
Allow		Outgoing	
Allow		Outgoing	
Allow		Outgoing	
Allow		Outgoing	

Append Firewall Rule

Device Reassignment Rules

The client's source role is determined based on the intial authentication.

Once the client has authenticated,the client may be placed into a new destination role based on the device type and ownership configured in the rules below.For example,if "Device Type" is iPhone and "Ownership" is Corporate then the client will be placed into role named as the "Destination Role".

The destination role will be determined based on the following rules.

If no rule matches,then the client's role will not changed.

Append Device Reassignment Rules

Create Role

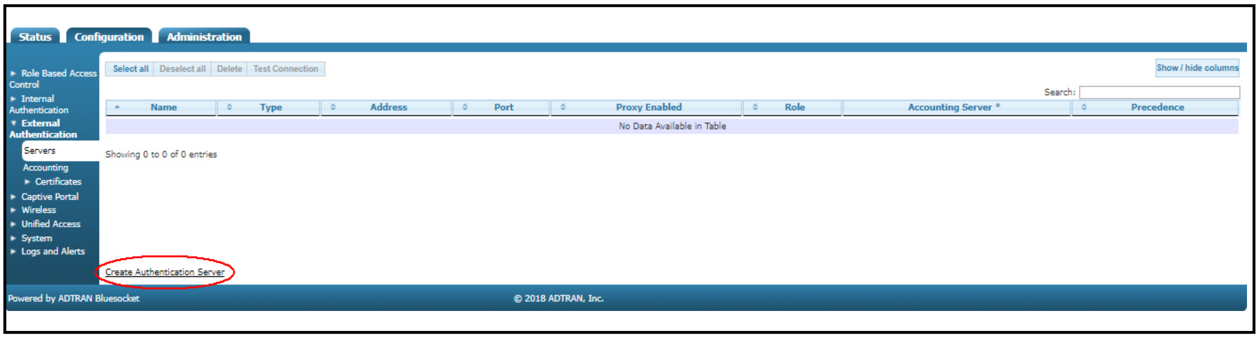
Figure 8. Configuring the User Authentication Role

After creating the machine (Domain computer) and user (Employee) authentication roles, you have completed Step 1 of vWLAN machine and user authentication. Next you will configure the external RADIUS 802.1x authentication server.

Step 2: Configuring the External RADIUS 802.1x Authentication Server

After configuring the machine and user authentication roles, begin configuring the external RADIUS 802.1x server. Follow these steps:

1. In the vWLAN GUI, navigate to the **Configuration** tab and select **External Authentication** > **Servers**. Select **Create Authentication Server** in the servers menu.



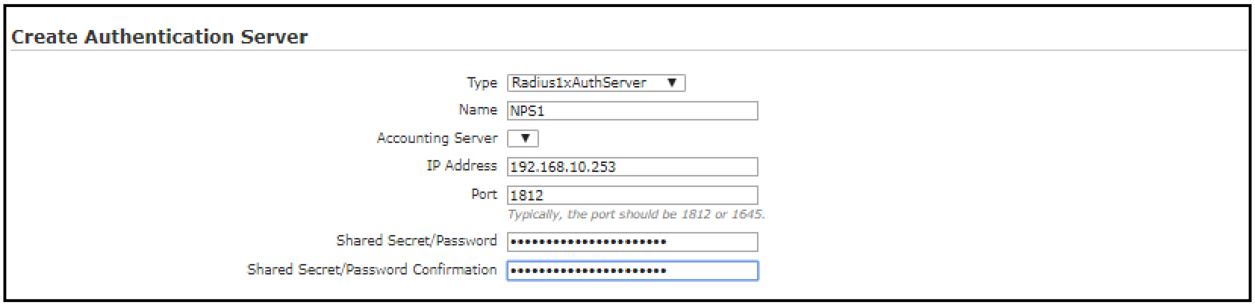
Name	Type	Address	Port	Proxy Enabled	Role	Accounting Server *	Precedence
No Data Available in Table							

Showing 0 to 0 of 0 entries

Figure 9. Navigating to the New Authentication Server Menu

2. In the server creation menu, select **RADIUS1xAuthServer** from the **Type** drop-down menu and enter the server name in the **Name** field. Specify the IP address of the server in the **IP Address** field and specify the port being used by the server in the **Port** field. By default, NPS uses ports **1812** and **1645** for authentication. Configure the shared secret and password for this server by entering the appropriate shared secret/password in the **Shared Secret/Password** and **Shared Secret/Password confirmation** fields. These values must match the RADIUS client configured for each AP in the RADIUS server (configured later). It is recommended that the shared secret be at least 22 characters and consist of a random sequence of upper and lowercase letters, numbers, and punctuation.

> NOTE
>
> *If this RADIUS server will communicate with an accounting server, select the appropriate server from the **Accounting server** drop-down menu. For more information about accounting servers, refer to Configuring vWLAN RADIUS Accounting on page 57. Accounting is optional and has no impact on authentication.*

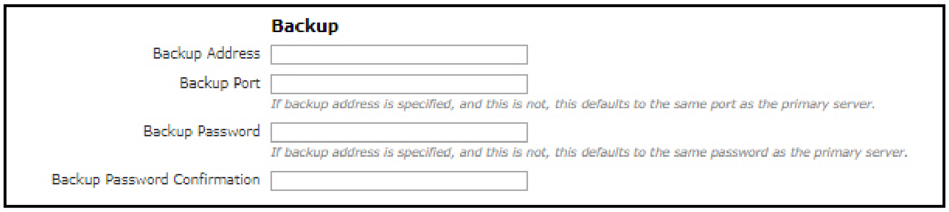


Create Authentication Server

Type	Radius1xAuthServer ▼
Name	NPS1
Accounting Server	▼
IP Address	192.168.10.253
Port	1812 Typically, the port should be 1812 or 1645.
Shared Secret/Password	••••••••••••••••••••••
Shared Secret/Password Confirmation	••••••••••••••••••••••

Figure 10. Authentication Server Type, Name, IP Address, Port, and Shared Secret Password

3. Optionally configure a backup IP address and port for this server by entering the information in the appropriate fields. Optionally configure a backup shared secret/password.



Backup

Backup Address

Backup Port

If backup address is specified, and this is not, this defaults to the same port as the primary server.

Backup Password

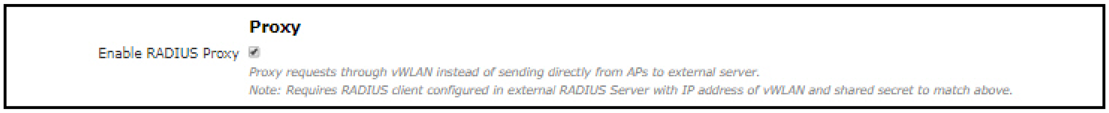
If backup address is specified, and this is not, this defaults to the same password as the primary server.

Backup Password Confirmation

Figure 11. Optional Backup Information

4. Optionally, proxy all requests through the vWLAN to the RADIUS server versus from the AP directly to the RADIUS server by selecting the box next to **Enable RADIUS Proxy**.

> *This feature requires a RADIUS client to be configured for the IP address of vWLAN and the shared secret to match above.*



Proxy

Enable RADIUS Proxy ☑

Proxy requests through vWLAN instead of sending directly from APs to external server.

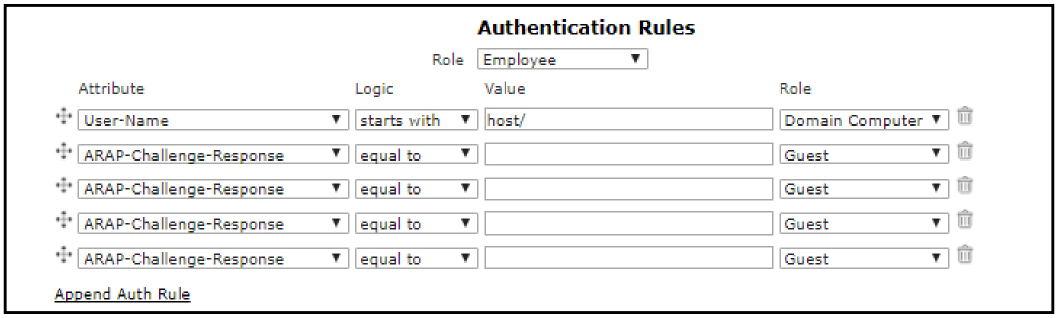
Note: Requires RADIUS client configured in external RADIUS Server with IP address of vWLAN and shared secret to match above.

Figure 12. Optional RADIUS Proxy

5. Optionally, in the **Authentication Rules** menu, select **Employee** from the drop down menu beside **Role**. Users are placed in this role upon successful authentication.

> *If machine authentication is not required, you do not have to specify the authentication rules as outlined in the next step. Skip to Step 9 on page 16.*

Next, in the first row use the drop-down menus to select the following options: *Attribute* **User-Name**, *Logic* **starts with**, *Value* **host/**, and *Role* **Domain Computer**. Machine authentication uses **host/comutername.domain** as the **User-Name**, so domain computers will be placed in the **Domain Computer** role upon successful authentication.



Authentication Rules

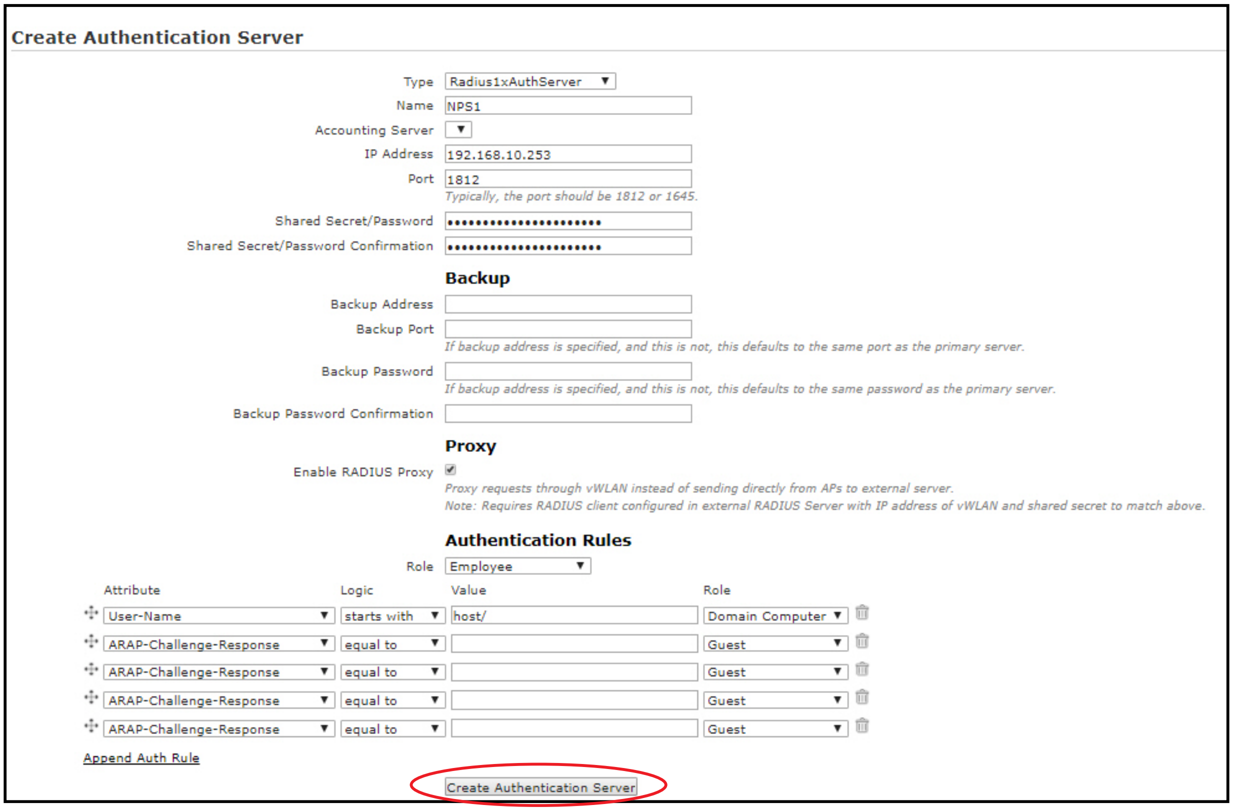
Role Employee

Attribute	Logic	Value	Role
User-Name	starts with	host/	Domain Computer
ARAP-Challenge-Response	equal to		Guest
ARAP-Challenge-Response	equal to		Guest
ARAP-Challenge-Response	equal to		Guest
ARAP-Challenge-Response	equal to		Guest

Append Auth Rule

Figure 13. Optional Authentication Rules for Machine Authentication

6. Select **Create Authentication Server** to create the server in vWLAN.



Create Authentication Server

Type: Radius1xAuthServer ▼
Name: NPS1
Accounting Server: ▼
IP Address: 192.168.10.253
Port: 1812
Typically, the port should be 1812 or 1645.
Shared Secret/Password: ••••••••••••••••••••••
Shared Secret/Password Confirmation: ••••••••••••••••••••••

Backup

Backup Address:
Backup Port:
If backup address is specified, and this is not, this defaults to the same port as the primary server.
Backup Password:
If backup address is specified, and this is not, this defaults to the same password as the primary server.
Backup Password Confirmation:

Proxy

Enable RADIUS Proxy ☑
Proxy requests through vWLAN instead of sending directly from APs to external server.
Note: Requires RADIUS client configured in external RADIUS Server with IP address of vWLAN and shared secret to match above.

Authentication Rules

Role: Employee ▼

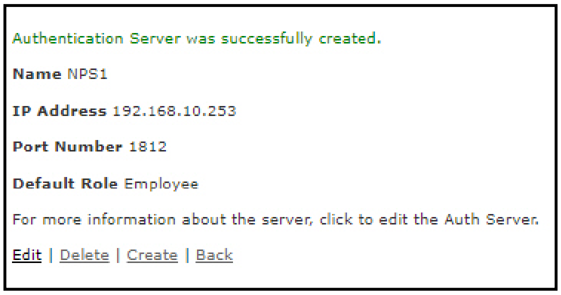
Attribute	Logic	Value	Role
User-Name ▼	starts with ▼	host/	Domain Computer ▼
ARAP-Challenge-Response ▼	equal to ▼		Guest ▼
ARAP-Challenge-Response ▼	equal to ▼		Guest ▼
ARAP-Challenge-Response ▼	equal to ▼		Guest ▼
ARAP-Challenge-Response ▼	equal to ▼		Guest ▼

Append Auth Rule

Create Authentication Server

Figure 14. Create the Authentication Server

7. You will receive confirmation that the server has been successfully created.



Authentication Server was successfully created.

Name NPS1

IP Address 192.168.10.253

Port Number 1812

Default Role Employee

For more information about the server, click to edit the Auth Server.

Edit | Delete | Create | Back

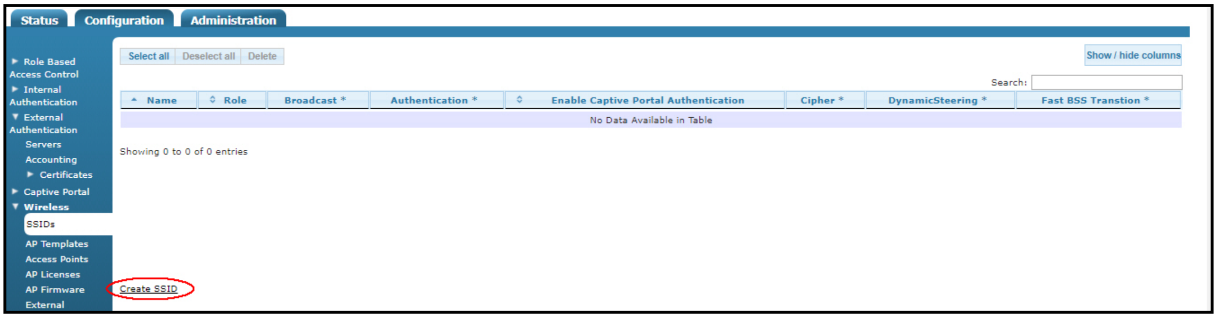
Figure 15. Authentication Server was Successfully Created

8. Repeat these steps for any additional RADIUS servers. Once all servers are created, they will appear in the server list displayed in the **Configuration** tab, under **External Authentication** > **Servers**.

Step 3: Configure the SSID

After configuring the machine and user authentication roles and the RADIUS authentication server, configure the service set identifier (SSID) for the domain. To configure the SSID, follow these steps:

1. In the vWLAN GUI, navigate to the **Configuration** tab and select **Wireless** > **SSIDs**. Select **Create SSID** in the SSID menu.



Name	Role	Broadcast *	Authentication *	Enable Captive Portal Authentication	Cipher *	DynamicSteering *	Fast BSS Transtion *
No Data Available in Table							

Showing 0 to 0 of 0 entries

Figure 16. Navigating to the Create SSID Menu

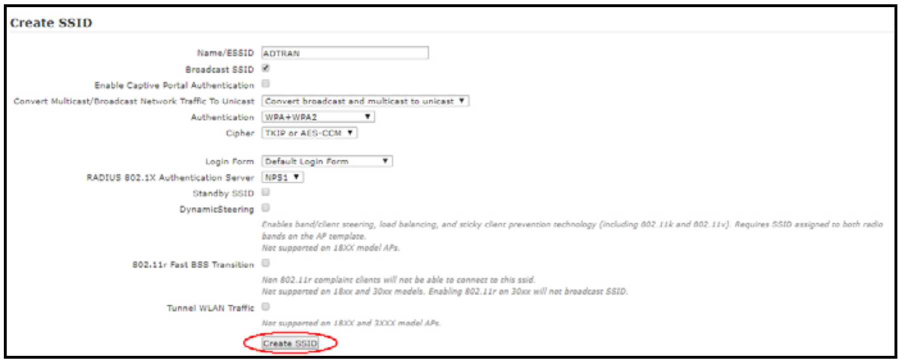
2. In the SSID creation menu, specify the name for the SSID in the **Name/ESSID** field. Enable broadcasting of the SSID by selecting the **Broadcast SSID** check box. Specify the multicast broadcast behavior by selecting the appropriate option from the **Convert multicast/broadcast network traffic to unicast** drop-down menu.

> *If you do not choose to convert multicast network traffic to unicast traffic, you must allow multicast traffic in the default role of the SSID. If you do not allow multicast traffic in the SSID's default role, and you do not choose to convert multicast traffic to unicast traffic in the SSID, then multicast traffic from a wired host or wireless client on another AP will not be seen.*

Specify the authentication type by selecting **WPA+WPA2** from the **Authentication** drop-down menu. Select **TKIP or AES-CCM** from the **Cipher** drop-down menu. It is recommended that all clients connect using WPA2/AES because it is the most secure. However, there is backward compatibility for clients that only support Wi-Fi protected access Temporal Key Integrity Protocol (WPA/TKIP).

> *Clients using TKIP are not able to take advantage of 802.11n data rates and are limited to a maximum data rate of 54 Mbps.*

Optionally specify a login form from the **Login form** drop-down menu. Specify the RADIUS server as **NPS1** (or the RADIUS server configured in *Step 2: Configuring the External RADIUS 802.1x Authentication Server on page 14*) from the **Radius1x auth server** drop-down menu.



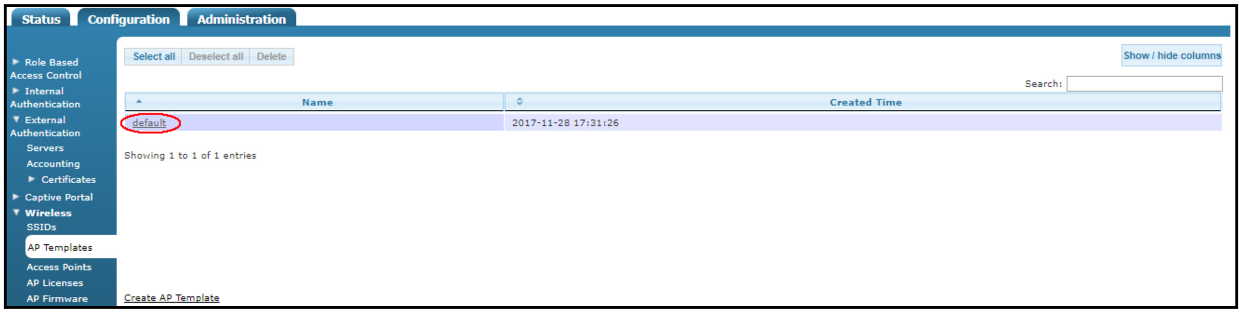
Create SSID

Name/ESSID ADTRAN
Broadcast SSID ☑
Enable Captive Portal Authentication ☐
Convert Multicast/Broadcast Network Traffic To Unicast Convert broadcast and multicast to unicast ▼
Authentication WPA+WPA2 ▼
Cipher TKIP or AES-CCM ▼

Login Form Default Login Form ▼
RADIUS 802.1X Authentication Server NPS1 ▼
Standby SSID ☐
DynamicSteering ☐
Enables band/client steering, load balancing, and sticky client prevention technology (including 802.11k and 802.11v). Requires SSID assigned to both radio bands on the AP template.
Not supported on 18XX model APs.
802.11r Fast BSS Transition ☐
Non 802.11r complaint clients will not be able to connect to this ssid.
Not supported on 18xx and 30xx models. Enabling 802.11r on 30xx will not broadcast SSID.
Tunnel WLAN Traffic ☐
Not supported on 18XX and 3XXX model APs.

Figure 17. Configure the SSID

3. After configuring the SSID, you must adjust the AP template assigned to the APs that use this SSID. Navigate to the **Configuration** tab, and select **Wireless** > **AP Templates**. Select the name of the appropriate AP template in the list to edit that template.



Name	Created Time
default	2017-11-28 17:31:26

Showing 1 to 1 of 1 entries

Figure 18. Select an AP Template to Edit

4. In the AP template menu, scroll down to the SSIDs block and select the SSID associated with the correct RADIUS server. Select the + (plus) sign to add the SSID to both the 802.11 b/g/n and 802.11 a/n radios. Select **Update AP Template** at the bottom of the menu to apply the changes.

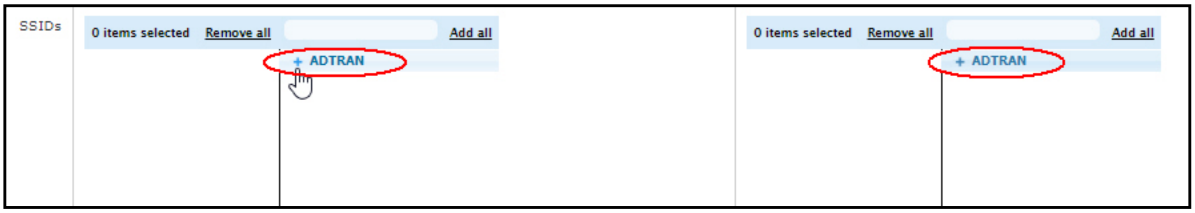


Figure 19. Add the SSID to the AP Template for Both Radios

5. After you have made changes to the AP template, you will be prompted to apply those changes to the APs using that template. An **Admin Task** is created, and the template changes will only take effect once the configuration is applied. The vWLAN and BSAP configuration for machine and user authentication is complete.

Configuring Windows Server 2008 R2 Enterprise for Authentication

To configure Windows Server 2008 R2 Enterprise for machine and user authentication, you must have the server installed and configured as a domain controller. Microsoft recommends that NPS be installed on a domain controller in order to optimize authentication and authorization response times and minimize network traffic. A private CA must have already been deployed on the network using AD CS in order to configure machine and user authentication on the Windows Server 2008.

> NOTE
>
> *For information about installing AD CS, refer to* ***Deploy a CA and NPS Server Certificate*** *at http://technet.microsoft.com/en-us/library/cc730811.aspx and* ***NPS Server Certificate: CA Installation*** *at http://technet.microsoft.com/en-us/library/cc731431.aspx.*

By default, AD CS automatically distributes a server certificate to domain controllers using the Domain Controller Certificate Template in AD CS. This server certificate is installed in the personal certificates store of the local computer. AD CS automatically distributes its private CA certificate to domain controllers as well. The private CA certificate is installed in the trusted root certification authorities store on the local computer and user. By default, AD CS automatically distributes its private CA certificate to domain computers and users. The private CA certificate is installed in the Trusted Root Certificate Authorities store of the local computer and user. The NPS server is trusted by the client because the client trusts the private CA that issued the NPS server certificate. Non-domain computers must have the private CA certificate manually installed in the Trusted Root Certification Authorities store for them to trust the NPS server certificate that was issued by the private CA. This is a requirement for mutual authentication.

Since NPS is installed on a domain controller, and the server certificate that is automatically distributed by AD CS meets the minimum server certificate requirements, there is no further action required pertaining to certificates (beyond selecting the server certificate in NPS under PEAP). If, however, certificate auto-enrollment is enabled in a group policy, the domain controller authentication certificate template supersedes the domain controller certificate template. The domain control authentication certificate template does not meet the minimum server certificate requirements for PEAP because the subject name does not contain a value. Therefore, it is required to configure a certificate template and auto-enrollment for NPS as described by Microsoft. This is also required if NPS was not installed on a domain controller.

> NOTE
>
> *Minimum server certificate requirements are described by Microsoft in* ***Certificate Requirements for PEAP and EAP*** *(http://technet.microsoft.com/en-us/library/a1ac8d7e-3479-46b4-932b-ab43362e012b). Certificate template and auto-enrollment for NPS is described by Microsoft in* ***NPS Server Certificate: Configure the Template and Auto-enrollment*** *(http://technet.microsoft.com/en-us/library/cc754198.aspx).*

Configuring Windows Server 2008 R2 Enterprise for machine and user authentication requires the following steps:

- *Step 1: Creating User and Computer Groups in Active Directory on page 19*
- *Step 2: Installing NPS on page 21*
- *Step 3: Configuring the NPS Server on page 22*
- *Step 4: Registering the NPS Server in Active Directory are listed on page 47*.
- *Step 5: Configure the NPS Server to Ignore User Account Dial-in Properties are listed on page 47*.

Step 1: Creating User and Computer Groups in Active Directory

In **Active Directory Users and Computers**, create a universal security group for users and computers that has access to the secure wireless network. Do not put all of your users and computers directly into this universal group, especially if you have a large number of them, but rather create separate global groups as members of the universal group, and then add users and computers to those global groups.

In the following sections, an organizational unit (OU) is created called **Employee**. All employee users and computers are placed in this group. Inside the employee OU, a global security group called **EmployeeWireless** is created. All the employee users and computers are members of the **EmployeeWireless** global security group. Then, a universal security group called **WirelessUsersandComputers** is created at the root of the domain. The **EmployeeWireless** global security group is a member of the **WirelessUsersandComputers** universal security group. If you have existing OUs and security groups, you can configure them similarly.

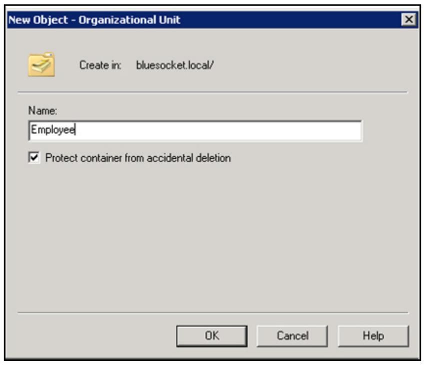
The steps necessary to configure user and computer groups in AD are as follows:

- *Creating an OU on page 20*
- *Creating a Global Security Group on page 20*
- *Creating a Universal Security Group on page 21*
- *Adding Users and Computers as Members of the Global Security Group on page 21*
- *Adding the Global Security Group as a Member of the Universal Security Group on page 21*

Creating an OU

To create an OU, follow these steps:

1. In the Windows Server 2008 domain controller, navigate to **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
2. Right-click on the domain and select **New** > **Organizational Unit**.
3. Specify the name for the unit in the appropriate field and select **OK**. All your employee users and computers should be placed in this OU.



New Object - Organizational Unit

Create in: bluesocket.local/

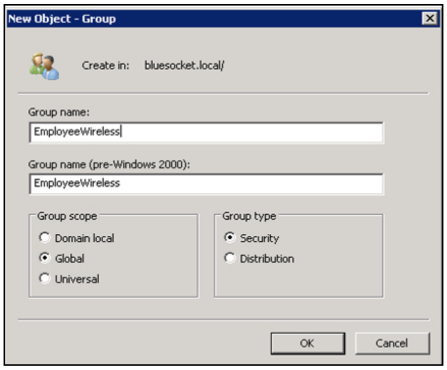
Name: Employee

☑ Protect container from accidental deletion

Creating a Global Security Group

To create a global security group, follow these steps:

1. Right-click on the new OU (**Employee**) and select **New** > **Group**.
2. Specify the name for the group in the appropriate field. Select **Global** under **Group scope** and **Security** under **Group type**. Select **OK** to create the group.



New Object - Group

Create in: bluesocket.local/

Group name: EmployeeWireless

Group name (pre-Windows 2000): EmployeeWireless

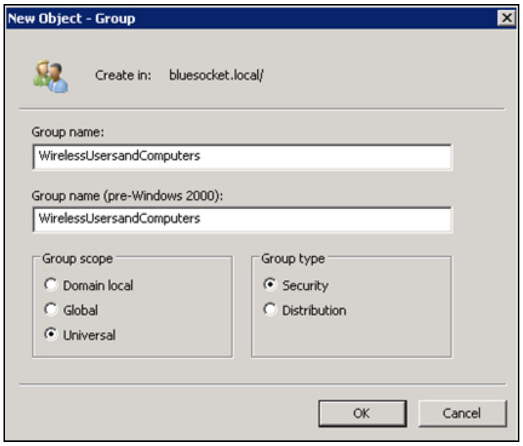
Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Creating a Universal Security Group

To create a universal security group, follow these steps:

1. Right-click on your domain and select **New** > **Group**.
2. Specify the name for the group in the appropriate field. Select **Universal** under **Group scope** and **Security** under **Group type**. Select **OK** to create the group.



Create in: bluesocket.local/

Group name:
WirelessUsersandComputers

Group name (pre-Windows 2000):
WirelessUsersandComputers

Group scope
○ Domain local
○ Global
● Universal

Group type
● Security
○ Distribution

Adding Users and Computers as Members of the Global Security Group

Add all the employee users and computers as members of the **EmployeeWireless** global security group by following these steps:

1. Select all the employee users and computers in the **Employee OU** by selecting **Shift** + click.
2. Right-click and select **Add to Group**.
3. Enter **EmployeeWireless** in the object name field and select **OK**.

Adding the Global Security Group as a Member of the Universal Security Group

Add the **EmployeeWireless** global security group as a member of the **WirelessUsersandComputers** universal security group by following these steps:

1. In the **Employee OU**, right-click on the **EmployeeWireless** global security group and select **Add to Group**.
2. Enter **WirelessUsersandComputers** in the object name field and select **OK**.

Step 2: Installing NPS

NPS is a role service of the Network Policy and Access Services server role. By default, NPS listens for RADIUS traffic on ports 1812, 1813, 1645, and 1646 on all installed network adapters. NPS can be installed on the domain controller by using the **Add Roles** wizard. If Windows firewall with advanced security is enabled when you install NPS, firewall exceptions for the default ports are automatically created during the installation process for both Internet Protocol version 4 (IPv4) and IPv6 traffic.

NOTE *If your network access servers are configured to send RADIUS traffic over ports other than the default ports, you must remove the exceptions for the default ports created in the Windows firewall during NPS installation. In addition, you will have to create exceptions in the firewall for the ports that you are using.*

To install NPS, follow these steps:

1. Navigate to the **Add Roles** wizard by either selecting **Initial Configuration Tasks** > **Customize This Server** > **Add Roles**, or by selecting **Start** > **Server Manager** > **Roles** > **Roles Summary** > **Add Roles**. Once you have selected **Add Roles**, the **Add Roles** wizard will open.
2. In the **Before You Begin** menu, select **Next**.

NOTE *The **Before You Begin** menu of the **Add Roles** wizard does not display if you have previously select **Do Not Show This Page Again** the first time the wizard was used.*

3. In the **Roles** > **Select Server Roles** menu, select **Network Policy and Access Services** and then select **Next**.
4. In the **Network Policy and Access Services** menu, select **Next**.
5. In **Role Services** > **Select Role Services**, select **Network Policy Server** and then select **Next**.
6. In the **Confirm Installation Selections** menu, select **Install**.
7. In the **Installation Results** menu, review your installation results and select **Close**.

Step 3: Configuring the NPS Server

After installing NPS, you can configure the NPS server by using one of three methods described in the following sections:

- *Configuring NPS Using the NPS Console on page 22*
- *Configuring NPS Using the Scenario Wizard on page 23*
- *Configuring the NPS Server Manually on page 32*

Configuring NPS Using the NPS Console

You can configure and manage the local NPS server using the NPS Microsoft Management Console (MMC). The NPS console differs from use of the NPS MMC snap-in in the following ways:

- The NPS console is installed by default when you install NPS.
- The NPS console is used to manage the local NPS only; you cannot use the NPS console to manage remote NPSs.
- You can use the NPS MMC snap-in to create a custom MMC console that allows you to manage remote NPSs in addition to managing the local NPS.

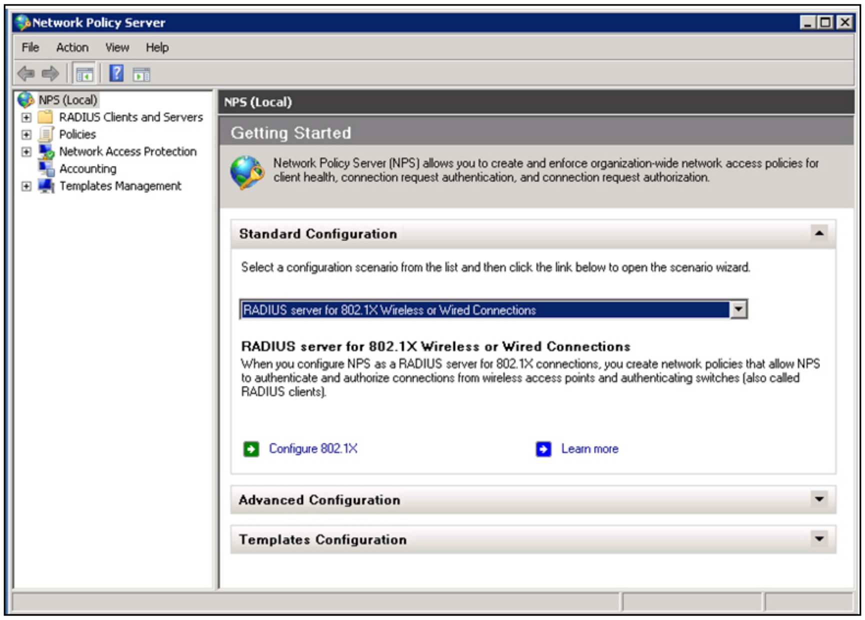
To configure the local NPS server by using the NPS console, follow these steps:

1. Select **Start** > **Administrative Tools** > **Network Policy Server**. The NPS console will open.
2. In the NPS console menu, select **NPS (Local)**. In the **Details** pane, select either **Standard Configuration** or **Advanced Configuration**, and do one of the following:
    - If you choose **Standard Configuration**, select a scenario from the list and follow the instructions to begin the Scenario wizard (refer to *Configuring NPS Using the Scenario Wizard* below).
    - If you choose **Advanced Configuration**, select the arrow to expand **Advanced Configuration** options. Review and configure the available options based on the NPS functionality you want.

Configuring NPS Using the Scenario Wizard

The Scenario wizard is used when configuring NPS using the **Standard Configuration** option. To configure NPS using the Scenario wizard, follow these steps:

1. Select **Standard Configuration** and then select **RADIUS server for 802.1x Wireless or Wired Connections**.
2. Select **Configure 802.1x**.



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Standard Configuration

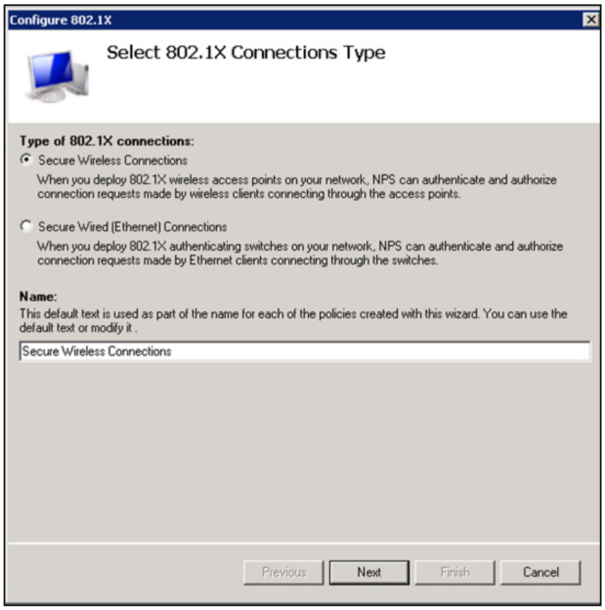
Select a configuration scenario from the list and then click the link below to open the scenario wizard.

RADIUS server for 802.1X Wireless or Wired Connections

RADIUS server for 802.1X Wireless or Wired Connections

When you configure NPS as a RADIUS server for 802.1X connections, you create network policies that allow NPS to authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).

3. Select **Secure Wireless Connections**, and then select **Next**.



Configure 802.1X

Select 802.1X Connections Type

Type of 802.1X connections:

● Secure Wireless Connections

When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.

○ Secure Wired (Ethernet) Connections

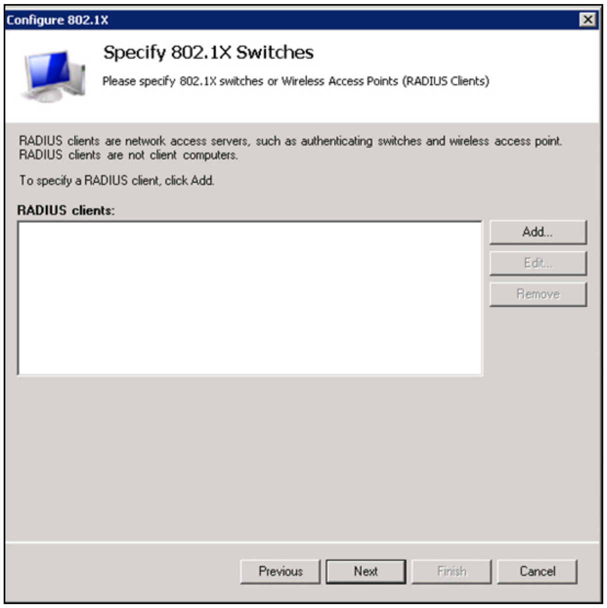
When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

Name:

This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it .

Secure Wireless Connections

4. In the **RADIUS clients** field, select **Add**.



Configure 802.1X

Specify 802.1X Switches

Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)

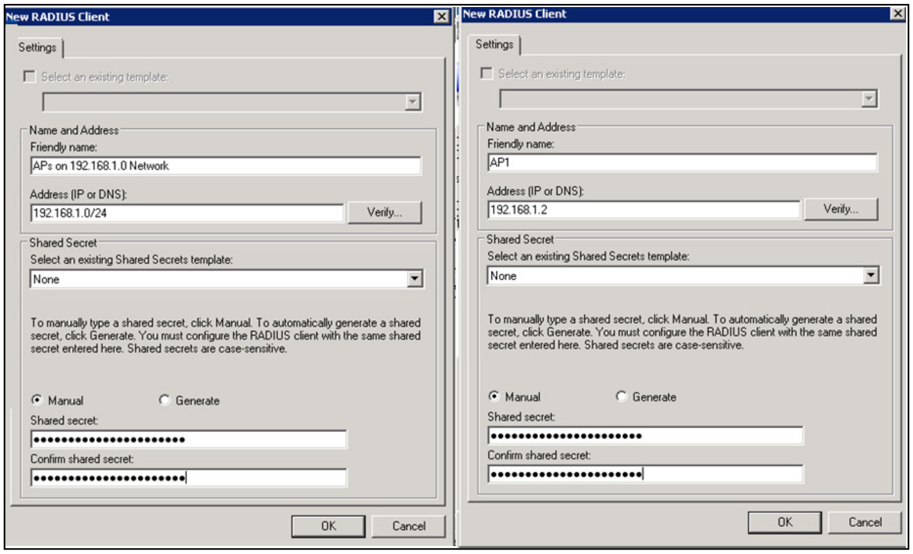
RADIUS clients are network access servers, such as authenticating switches and wireless access point. RADIUS clients are not client computers.

To specify a RADIUS client, click Add.

RADIUS clients:

5. Configure the **New RADIUS Client** by entering the AP name, IP address, and shared secret. The shared secret is the same shared secret used in *Step 2: Configuring the External RADIUS 802.1x Authentication Server on page 14*. You must add a RADIUS client with the IP address and shared secret for each AP. It is possible to configure a RADIUS client in the RADIUS server with a range of IP addresses. Microsoft Windows Server 2008 R2 Enterprise NPS allows you to configure a range of IP addresses in the **Address** field using CIDR notation.

For example, if the APs are all on the 192.168.1.0 255.255.255.0 network, you can enter 192.168.1.0 /24 in the **Address** field. The images below illustrate entering a single IP address and a range of IP addresses.



New RADIUS Client

Settings

☐ Select an existing template:

Name and Address

Friendly name: APs on 192.168.1.0 Network

Address (IP or DNS): 192.168.1.0/24

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••••••••••••••••

Confirm shared secret: ••••••••••••••••••••••

New RADIUS Client

Settings

☐ Select an existing template:

Name and Address

Friendly name: AP1

Address (IP or DNS): 192.168.1.2

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

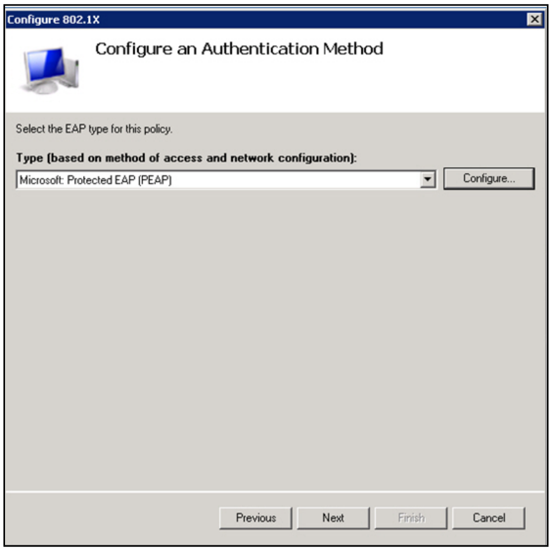
Shared secret: ••••••••••••••••••••••

Confirm shared secret: ••••••••••••••••••••••

> **NOTE** *Microsoft Windows Server 2008 R2 Standard NPS does not support configuring a RADIUS client with a range of IP addresses. With the standard version you are limited to a maximum of 50 RADIUS clients.*

Select **OK** once the RADIUS client information has been entered.

6. After all APs have been added as RADIUS clients (or a range of APs has been added), select **Next**.
7. In the authentication method menu, select **Microsoft: Protected EAP (PEAP)** from the **Type** drop-down menu.



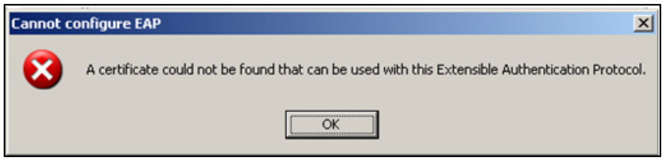
Configure 802.1X

Configure an Authentication Method

Select the EAP type for this policy.

Type (based on method of access and network configuration): Microsoft: Protected EAP (PEAP)

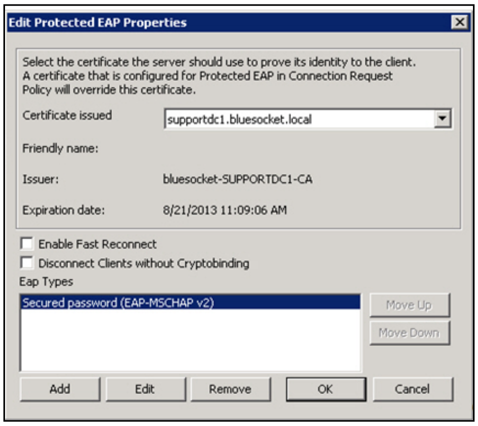
8. If a server certificate has not been installed, or the server certificate does not meet Microsoft's minimum server certificate requirements for PEAP, you will receive an error. You must cancel the configuration and resolve the certificate issue before proceeding.



Cannot configure EAP

A certificate could not be found that can be used with this Extensible Authentication Protocol.

9. If you have a certificate configured, and you did not receive an error message, select **Configure** to continue, and then select the appropriate server certificate from the drop-down menu. Deselect **Enable Fast Reconnect** to disable the feature since it is not supported by vWLAN. Verify that **Secured password (EAP-MSCHAP v2)** is displayed under **Eap Types**, select **OK**, and then **Next**.



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: supportdc1.bluesocket.local

Friendly name:

Issuer: bluesocket-SUPPORTDC1-CA

Expiration date: 8/21/2013 11:09:06 AM

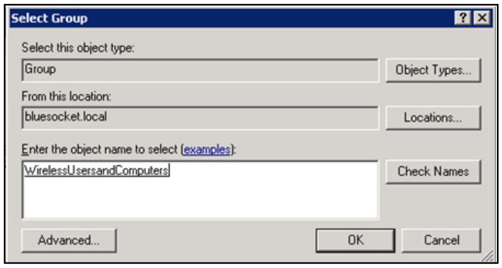
□ Enable Fast Reconnect

□ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

10. In the **Specify User Groups** menu, select **Add**. Enter **WirelessUsersandComputers** in the object name field, select **OK**, and then **Next**.



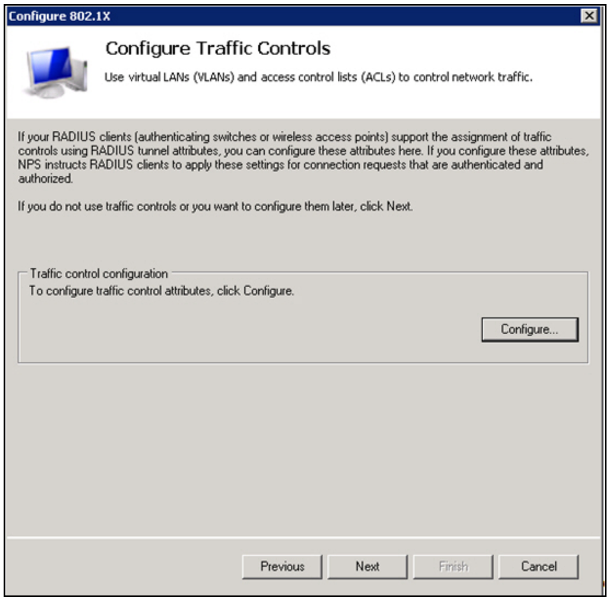
Select Group

Select this object type: Group

From this location: bluesocket.local

Enter the object name to select (examples): WirelessUsersandComputers

11. In the **Configure Traffic Controls** menu, select **Next**.



Configure Traffic Controls

Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

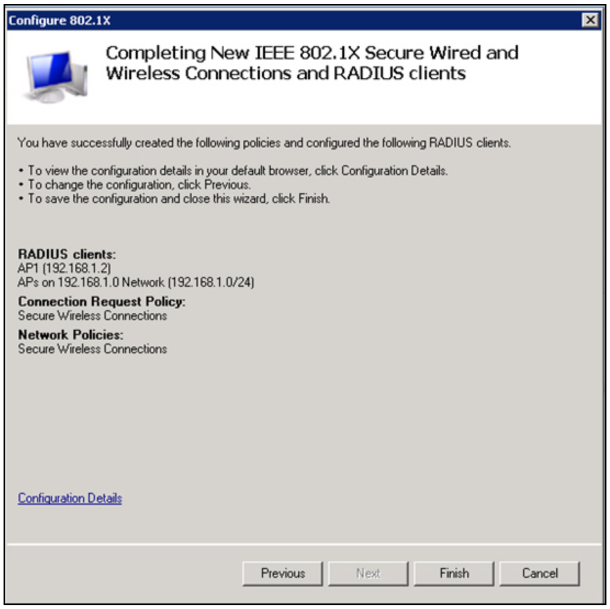
If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes, NPS instructs RADIUS clients to apply these settings for connection requests that are authenticated and authorized.

If you do not use traffic controls or you want to configure them later, click Next.

Traffic control configuration

To configure traffic control attributes, click Configure.

12. Review the configuration details and select **Finish**.



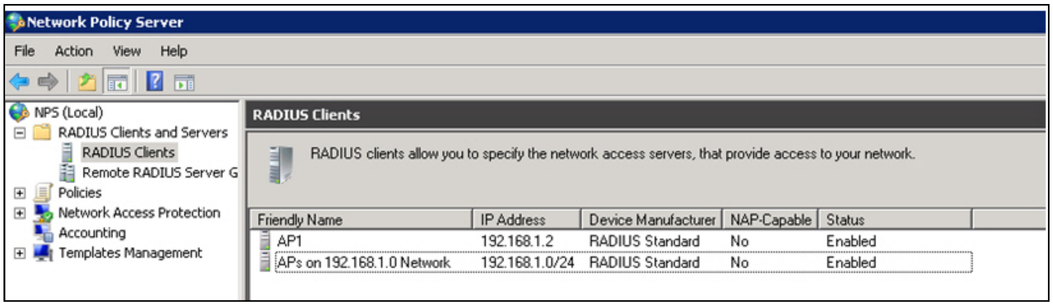
Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

RADIUS clients:
AP1 (192.168.1.2)
APs on 192.168.1.0 Network (192.168.1.0/24)
Connection Request Policy:
Secure Wireless Connections
Network Policies:
Secure Wireless Connections

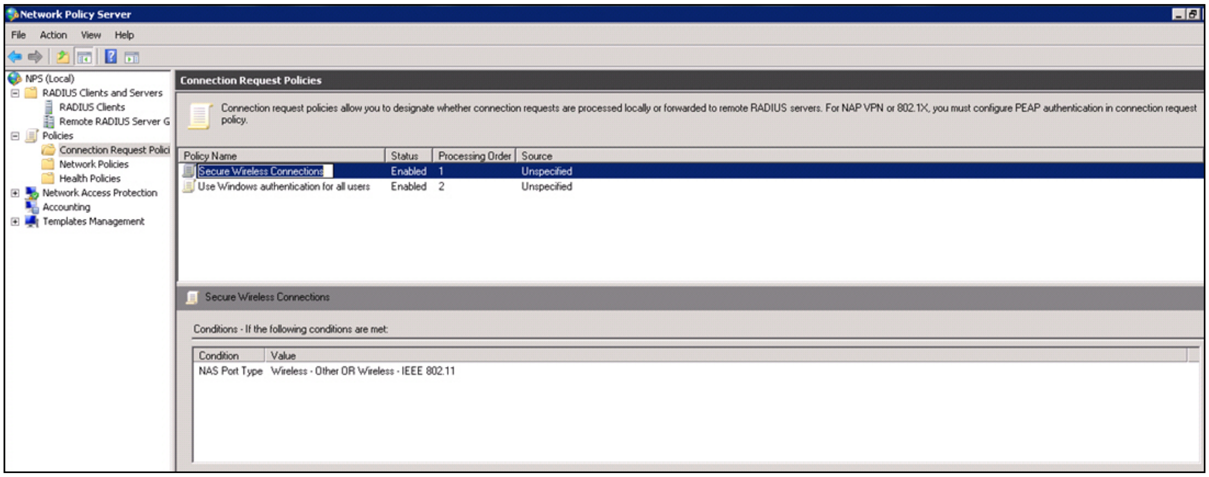
13. After completing the wizard, in the **Network Policy Server** menu, expand the **RADIUS Clients and Servers** tab under **NPS (Local)**, then select **RADIUS Clients**. The RADIUS clients configured by the Scenario wizard are displayed. After viewing the clients, the next configuration steps involve verifying the other parts of the NPS server configuration.



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
AP1	192.168.1.2	RADIUS Standard	No	Enabled
APs on 192.168.1.0 Network	192.168.1.0/24	RADIUS Standard	No	Enabled

14. In the **Network Policy Server** menu, expand the **Policies** tab under **NPS (Local)**. Select **Connection Request Policies**. Double-click the **Secure Wireless Connections** policy in the **Policy Name** pane. This policy is the connection request policy created by the Scenario wizard.



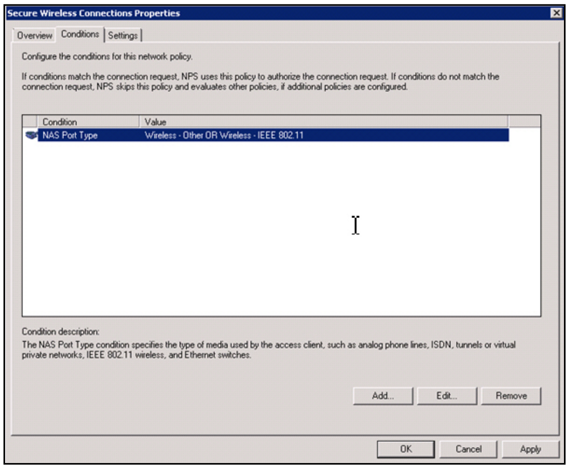
Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

Policy Name	Status	Processing Order	Source
Secure Wireless Connections	Enabled	1	Unspecified
Use Windows authentication for all users	Enabled	2	Unspecified

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11

15. In the **Secure Wireless Connections Properties** menu, select the **Conditions** tab. Notice that the **NAS Port Type** condition has a value of **Wireless**. This means that the type of media used by clients requesting connection must be IEEE 802.11 wireless.



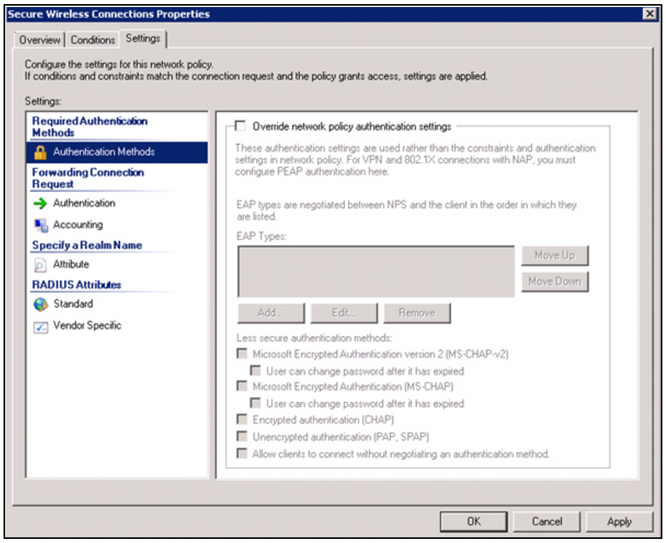
Configure the conditions for this network policy.

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
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11

Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

16. In the **Secure Wireless Connections Properties** menu, select the **Settings** tab, and then navigate to **Required Authentication Methods** > **Authentication Methods**. Here you will notice that the settings are grey and not configurable. These settings will come from the network policy. The connection request policy (**Secure Wireless Connections**) merely specifies whether connection requests are processed locally on this RADIUS server or are forwarded to remote RADIUS servers and does not specify authentication methods.



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

☐ 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.

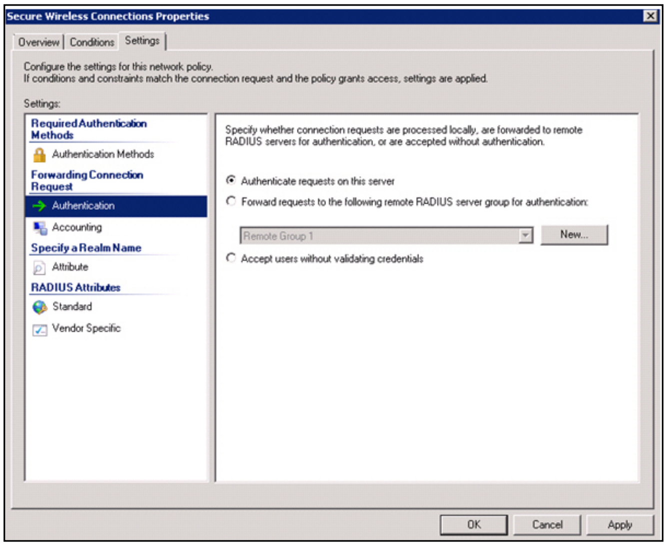
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

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.

17. Next, in the **Settings** tab, select **Forwarding Connection Request** > **Authentication**. In this menu you can see that the Scenario wizard configured connection requests to be processed locally on this server. Select **Cancel** after viewing these settings.



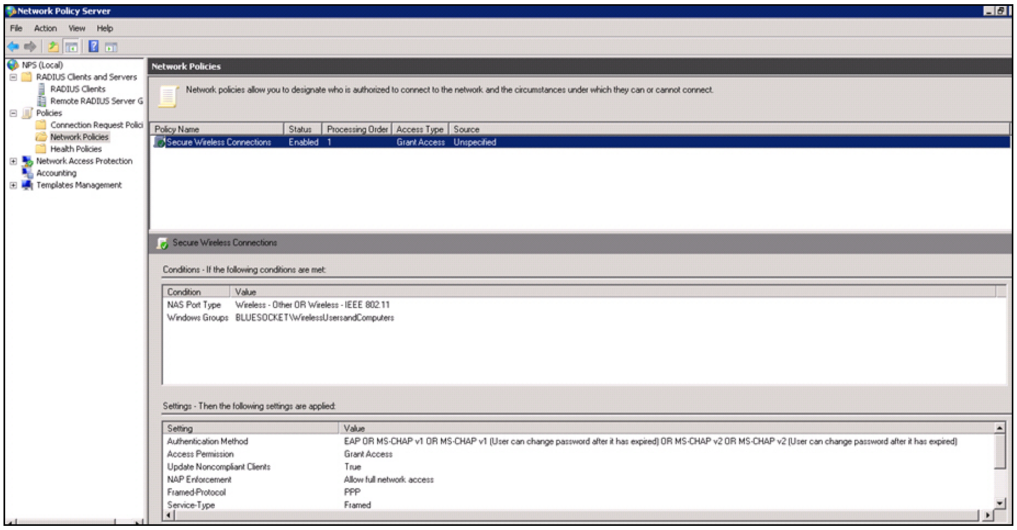
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

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:
  Remote Group 1
○ Accept users without validating credentials

18. In the **Network Policy Server** menu, expand the **Policies** tab under **NPS (Local)**, and select **Network Policies**. In the **Network Policies** pane, the network policy created by the Scenario wizard (**Secure Wireless Connections**) is displayed. Double-click **Secure Wireless Connections** to view details of the policy.



Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Secure Wireless Connections	Enabled	1	Grant Access	Unspecified

Secure Wireless Connections

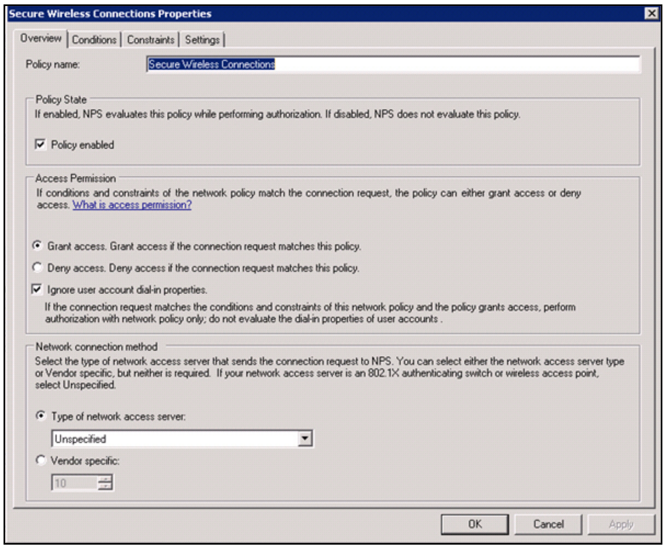
Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	BLUESOCKET\WirelessUsersandComputers

Settings - Then the following settings are applied:

Setting	Value
Authentication Method	EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 OR MS-CHAP v2 (User can change password after it has expired)
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

19. In the **Secure Wireless Connections Properties** menu, select the **Overview** tab. In the **Access Permission** menu, notice that the Scenario wizard enabled **Grant access** and **Ignore user account dial-in properties**. These options allow access to be granted if the connection request matches this policy, and that the dial-in properties of user accounts are not evaluated.



Policy name: Secure Wireless Connections

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, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

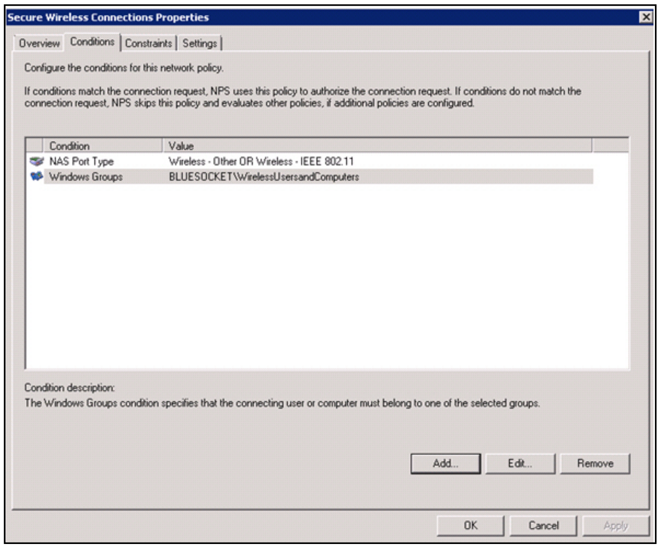
● Type of network access server:

Unspecified

○ Vendor specific:

10

20. Select the **Conditions** tab in the **Secure Wireless Connections** menu. This policy specifies that the **NAS Port Type** must be **Wireless**, and the **Windows Groups** must be **WirelessUsersandComputers**.



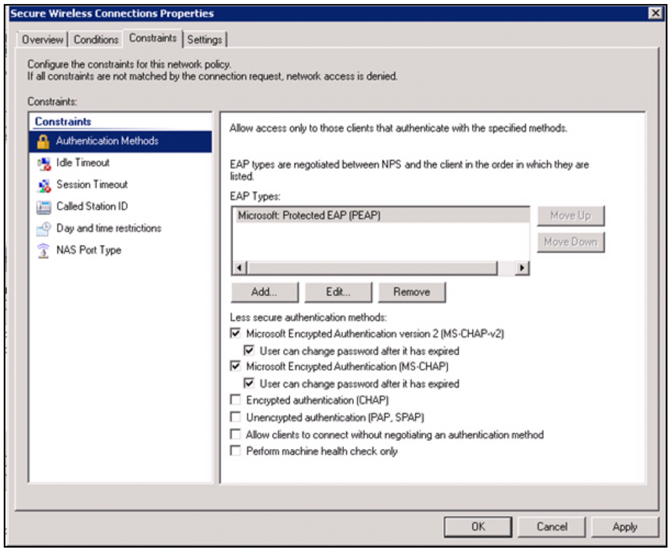
Configure the conditions for this network policy.

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
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11
Windows Groups	BLUESOCKET\WirelessUsersandComputers

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

21. Select the **Constraints** tab in the **Secure Wireless Connections** menu. The supported **EAP Type** for this policy is **Microsoft: Protected EAP (PEAP)**. You can optionally deselect the check boxes for **Less secure authentication methods** and select **Apply**.



Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Allow access only to those clients that authenticate with the specified methods.

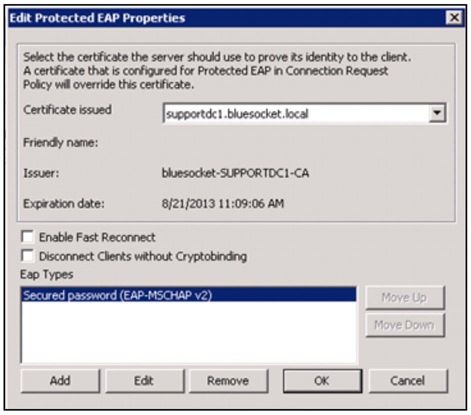
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:
Microsoft: Protected EAP (PEAP)

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

22. Select the **Edit** button under **EAP Types**. The certificate issued, the issuer, and the expiration date of the policy are displayed. In addition, fast reconnect is disabled, and the **EAP Type** supported is **Secured Password (EAP-MSCHAP v2)**. After viewing these details, select **OK**. The NPS server is now configured.



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: supportdc1.bluesocket.local

Friendly name:

Issuer: bluesocket-SUPPORTDC1-CA

Expiration date: 8/21/2013 11:09:06 AM

☐ Enable Fast Reconnect

☐ Disconnect Clients without Cryptobinding

Eap Types: Secured password (EAP-MSCHAP v2)

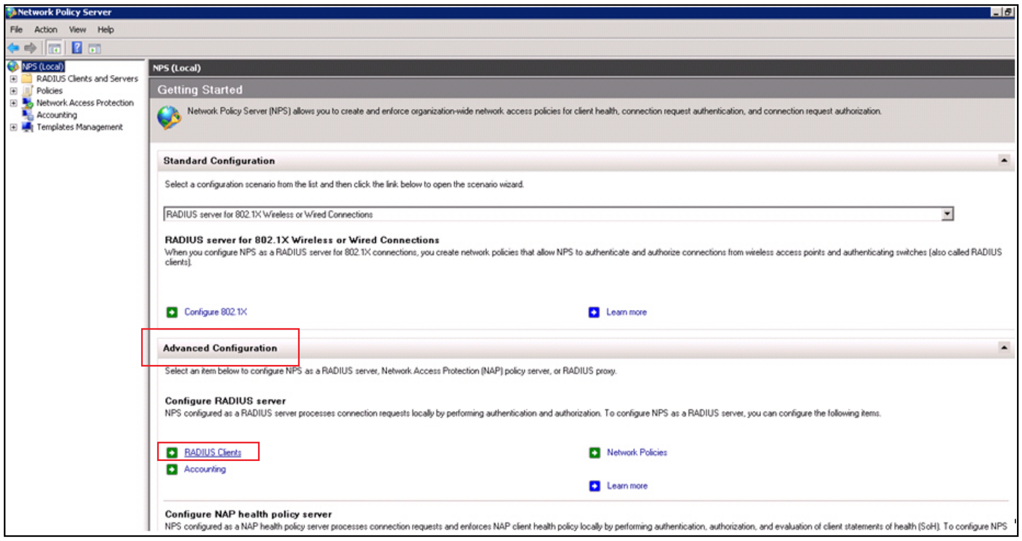
Configuring the NPS Server Manually

You can configure the NPS server manually without the use of the Scenario wizard. To configure the NPS server manually, you must configure the RADIUS clients, connection request policy, and the network policy.

Configuring RADIUS Clients

To configure the RADIUS clients for the NPS server, follow these steps:

1. In the **Network Policy Server** menu, select **NPS (Local)**. In the **NPS (Local)** configuration pane, select **Advanced Configuration** > **RADIUS Clients**.



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

RADIUS server for 802.1X Wireless or Wired Connections

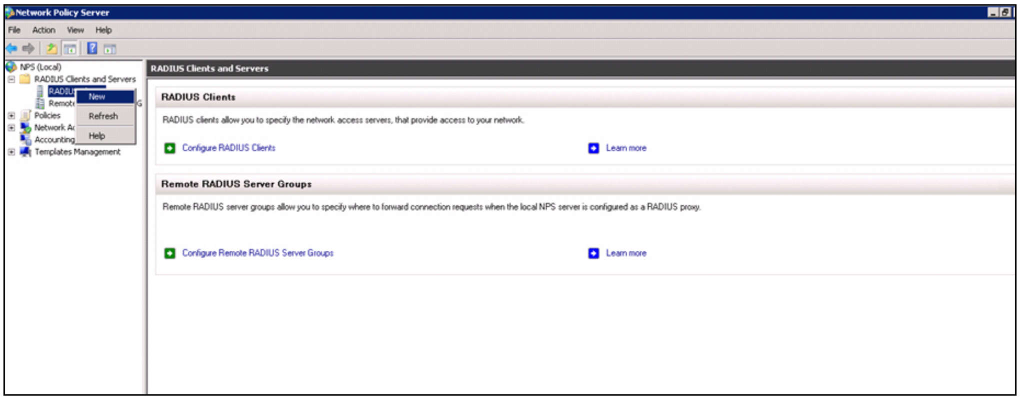
RADIUS server for 802.1X Wireless or Wired Connections
When you configure NPS as a RADIUS server for 802.1X connections, you create network policies that allow NPS to authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).

Select an item below to configure NPS as a RADIUS server, Network Access Protection (NAP) policy server, or RADIUS proxy.

Configure RADIUS server
NPS configured as a RADIUS server processes connection requests locally by performing authentication and authorization. To configure NPS as a RADIUS server, you can configure the following items.

Configure NAP health policy server
NPS configured as a NAP health policy server processes connection requests and enforces NAP client health policy locally by performing authentication, authorization, and evaluation of client statements of health (SoH). To configure NPS

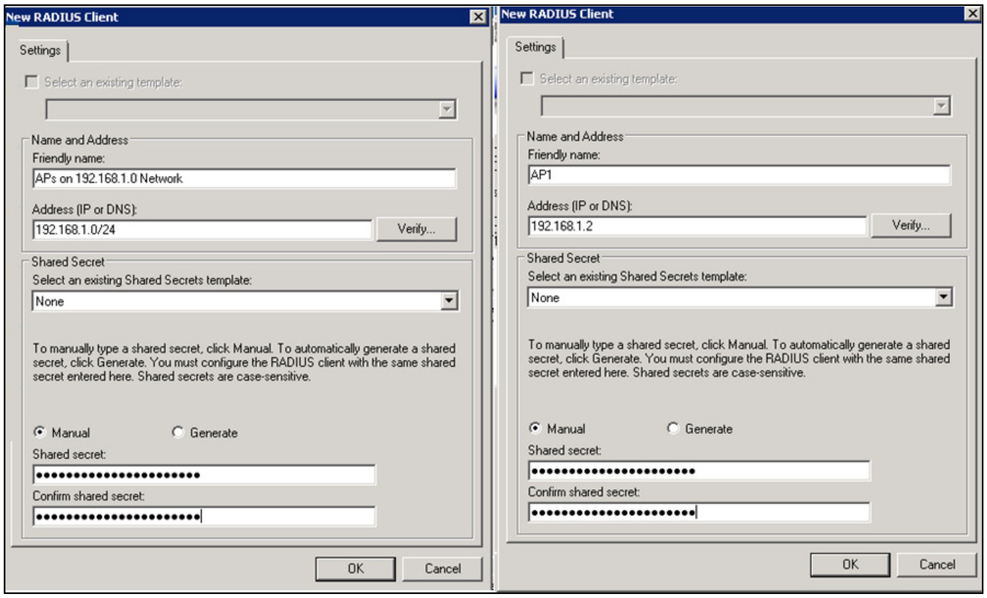
2. In the **Network Policy Server** menu, select **RADIUS Clients and Server**s. Right-click on **RADIUS Clients** and select **New**.



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Remote RADIUS server groups allow you to specify where to forward connection requests when the local NPS server is configured as a RADIUS proxy.

3. In the **New RADIUS Client** configuration menu, enter the AP's name, IP address, and shared secret. The shared secret is the same secret used to configure the authentication server in *Step 2: Configuring the External RADIUS 802.1x Authentication Server on page 14*. You must add a RADIUS client with the IP address and shared secret for each AP. It is possible to configure a RADIUS client in the RADIUS server with a range of IP addresses. Microsoft Windows Server 2008 R2 Enterprise NPS allows you to configure a range of IP addresses in the **Address** field using CIDR notation. For example, if the APs are all on the 192.168.1.0 255.255.255.0 network, you can enter 192.168.1.0 /24 in the **Address** field. The images below illustrate entering a single IP address and a range of IP addresses.



□ Select an existing template:

Friendly name: APs on 192.168.1.0 Network

Address (IP or DNS): 192.168.1.0/24

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●

Confirm shared secret: ●●●●●●●●●●●●●●●●●●●●●●

□ Select an existing template:

Friendly name: AP1

Address (IP or DNS): 192.168.1.2

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ●●●●●●●●●●●●●●●●●●●●●●

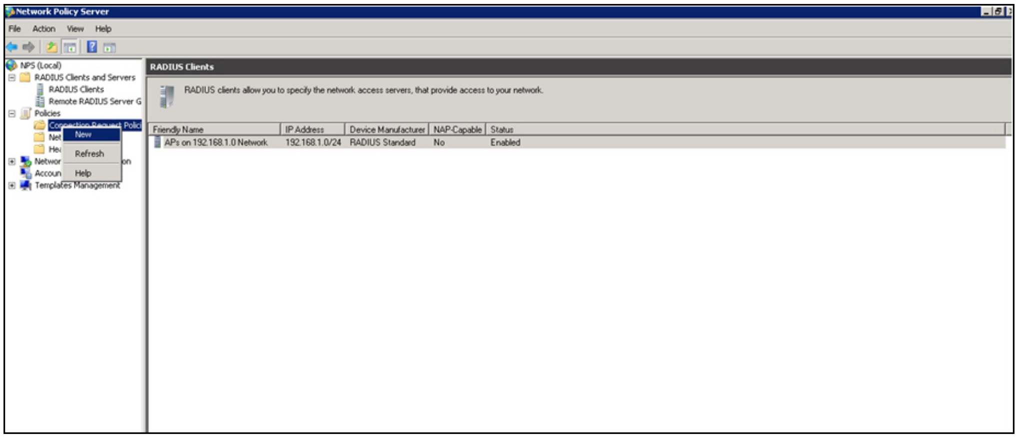
Confirm shared secret: ●●●●●●●●●●●●●●●●●●●●●●

NOTE *Microsoft Windows Server 2008 R2 Standard NPS does not support configuring a RADIUS client with a range of IP addresses. With the standard version you are limited to a maximum of 50 RADIUS clients.*

Configuring the Connection Request Policy

To configure the NPS server connection request policy, follow these steps:

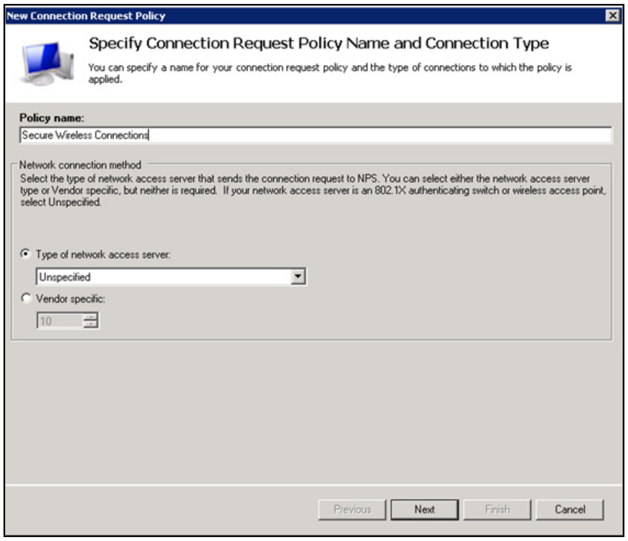
1. In the **Network Policy Server** menu, expand the **Policies** tab. Right-click **Connection Request Policies** and select **New**.



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
APs on 192.168.1.0 Network	192.168.1.0/24	RADIUS Standard	No	Enabled

2. In the **New Connection Request Policy** menu, enter **Secure Wireless Connections** in the **Policy name** field and select **Next**.



Specify Connection Request Policy Name and Connection Type

You can specify a name for your connection request policy and the type of connections to which the policy is applied.

Policy name: Secure Wireless Connections

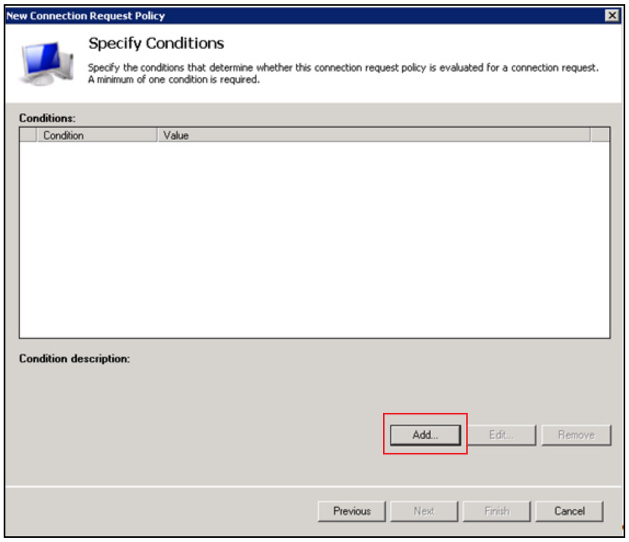
Network connection method

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, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server: Unspecified

○ Vendor specific: 10

3. In the **Specify Conditions** menu, select **Add**.



New Connection Request Policy

Specify Conditions

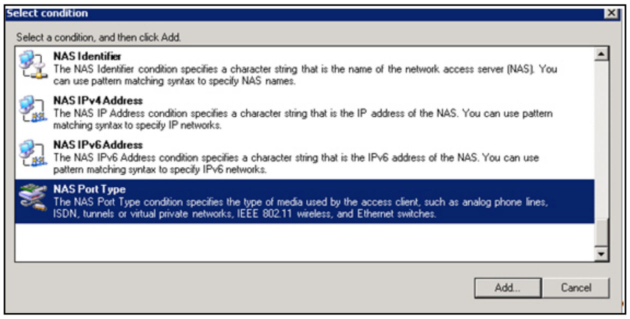
Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value

Condition description:

4. In the **Select condition** menu, select **NAS Port Type** and select **Add**.



Select condition

Select a condition, and then click Add.

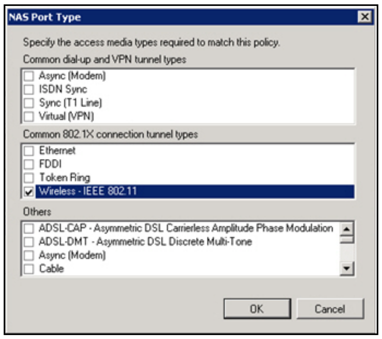
NAS Identifier
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.

NAS IPv4 Address
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.

NAS IPv6 Address
The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.

NAS Port Type
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

5. In the **NAS Port Type** menu, in the **Common 802.1x connection tunnel types** pane, select **Wireless-IEEE 802.11** and select **OK**.



NAS Port Type

Specify the access media types required to match this policy.

Common dial-up and VPN tunnel types

- ☐ Async (Modem)
- ☐ ISDN Sync
- ☐ Sync (T1 Line)
- ☐ Virtual (VPN)

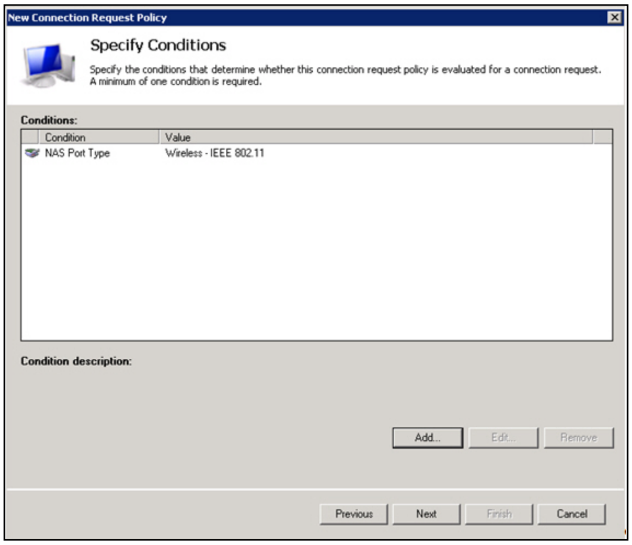
Common 802.1X connection tunnel types

- ☐ Ethernet
- ☐ FDDI
- ☐ Token Ring
- ☑ Wireless - IEEE 802.11

Others

- ☐ ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation
- ☐ ADSL-DMT - Asymmetric DSL Discrete Multi-Tone
- ☐ Async (Modem)
- ☐ Cable

6. The **NAS Port Type** with a value of **Wireless-IEEE 802.11** appears in the **Specify Conditions** menu. Select **Next** to continue.



New Connection Request Policy

Specify Conditions

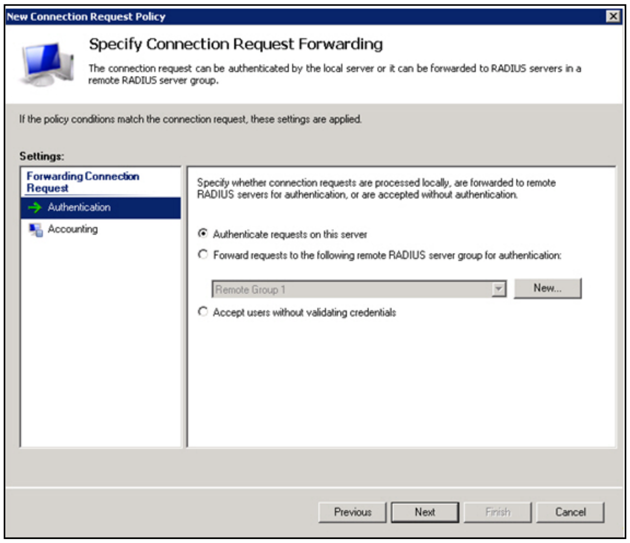
Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
NAS Port Type	Wireless - IEEE 802.11

Condition description:

7. In the **Specify Connection Request Forwarding** menu, select **Authenticate requests on this server** (default value) and select **Next**. This setting indicates that connection requests are processed locally on this server.



New Connection Request Policy

Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Forwarding Connection Request
- Authentication
- Accounting

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

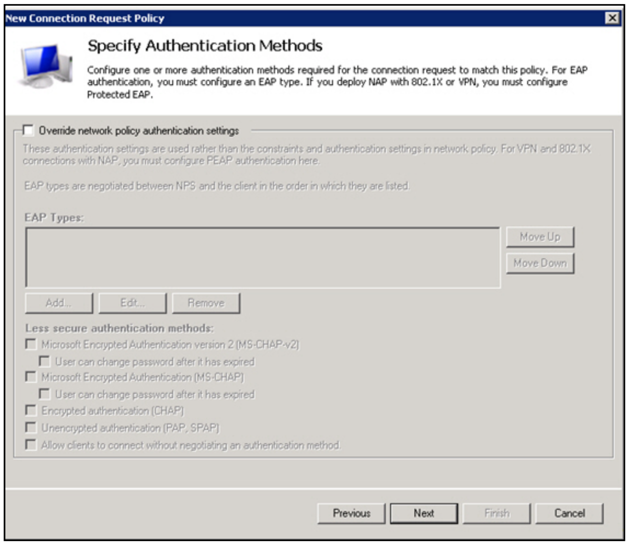
● Authenticate requests on this server

○ Forward requests to the following remote RADIUS server group for authentication:

Remote Group 1

○ Accept users without validating credentials

8. In the **Specify Authentication Methods** menu, select **Next** to accept the default values. Here you will notice that the settings are grey and not configurable. These settings will come from the network policy. The connection request policy (**Secure Wireless Connections**) merely specifies whether connection requests are processed locally on this RADIUS server or are forwarded to remote RADIUS servers and does not specify authentication methods.



New Connection Request Policy

Specify Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP.

☐ 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:

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)

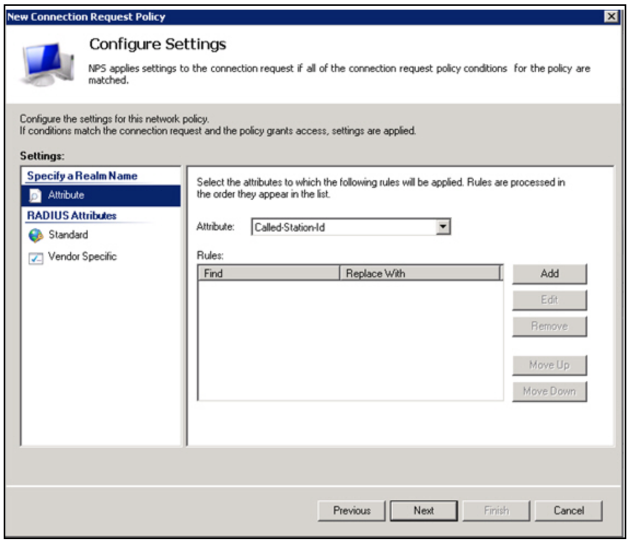
☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

9. In the **Configure Settings** menu, select **Next** to accept the default configuration.



New Connection Request Policy

Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are applied.

Settings:

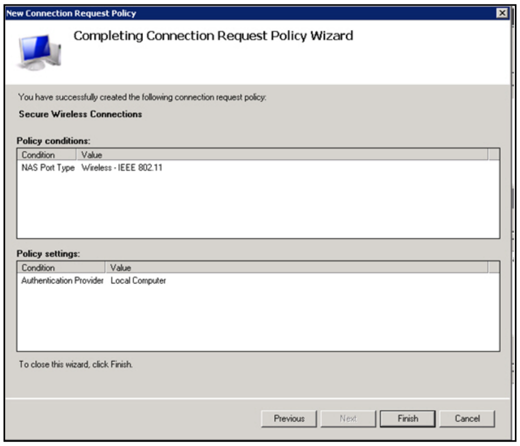
Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.

Attribute: Called-Station-Id

Rules:

Find	Replace With

10. Select **Finish** to create the connection request policy.


New Connection Request Policy
Completing Connection Request Policy Wizard
Previous
Next
Finish
Cancel

You have successfully created the following connection request policy:

Secure Wireless Connections

Policy conditions:

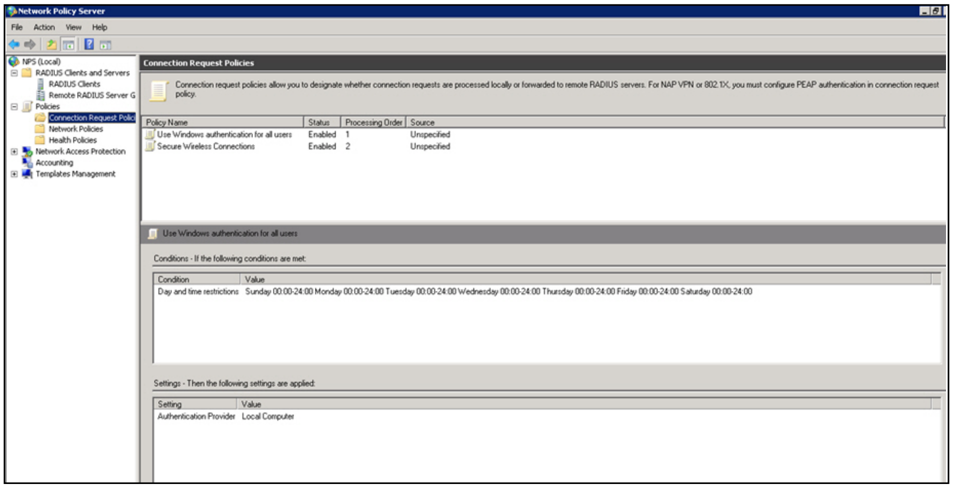
Condition	Value
NAS Port Type	Wireless - IEEE 802.11

Policy settings:

Condition	Value
Authentication Provider	Local Computer

To close this wizard, click Finish.

11. The newly created connection request policy (**Secure Wireless Connections**) appears in the **Connection Request Policies** pane of the **Network Policy Server** menu.



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

Policy Name	Status	Processing Order	Source
Use Windows authentication for all users	Enabled	1	Unspecified
Secure Wireless Connections	Enabled	2	Unspecified

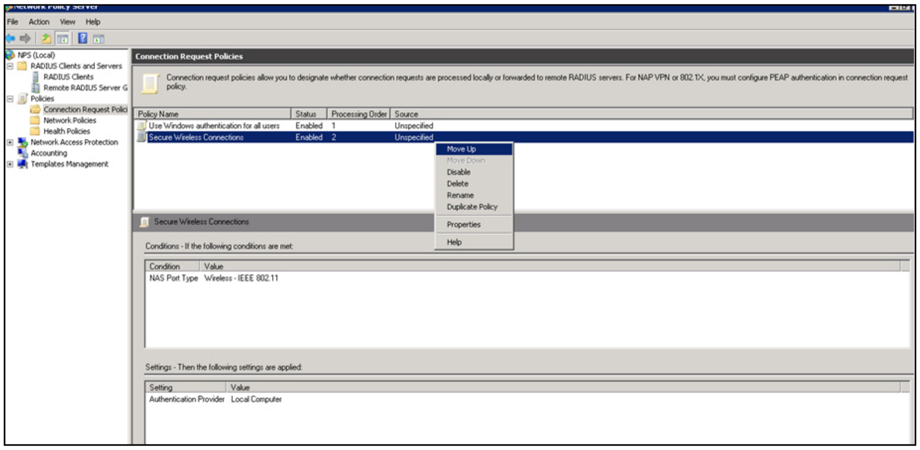
Conditions - If the following conditions are met:

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 Thursday 00:00-24:00 Friday 00:00-24:00 Saturday 00:00-24:00

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer

Connection request policies are processed in order, therefore the **Secure Wireless Connections** policy must be the first policy in the list. If the **Use Windows authentication for all users** policy is first in the list, right-click the **Secure Wireless Connections** policy and select **Move Up** to move it to the first position in the list. Once at the top, the **Secure Wireless Connections** policy will be processed first.



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

Policy Name	Status	Processing Order	Source
Use Windows authentication for all users	Enabled	1	Unspecified
Secure Wireless Connections	Enabled	2	Unspecified

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Wireless - IEEE 802.11

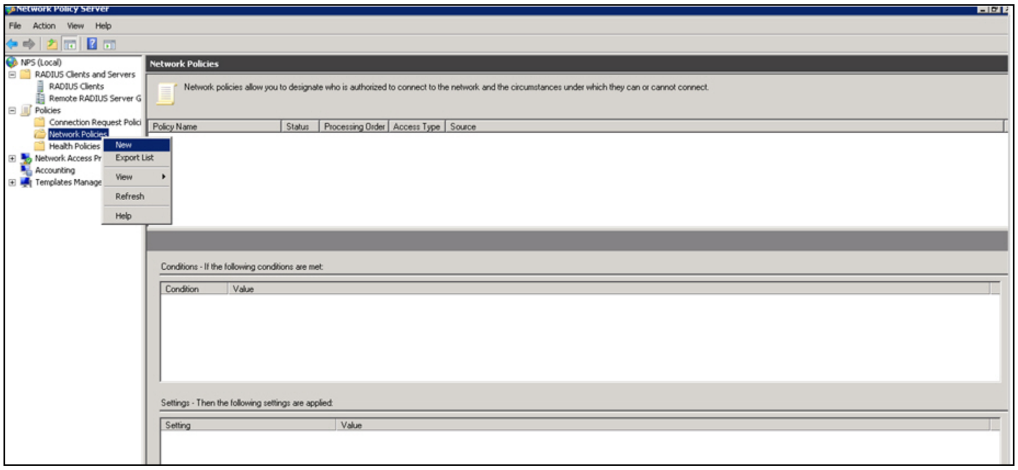
Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer

Configuring the Network Policy

To configure the NPS network policy, follow these steps:

1. In the **Network Policy Server** menu, expand the **Policies** tab, right-click **Network Policies**, and select **New**.

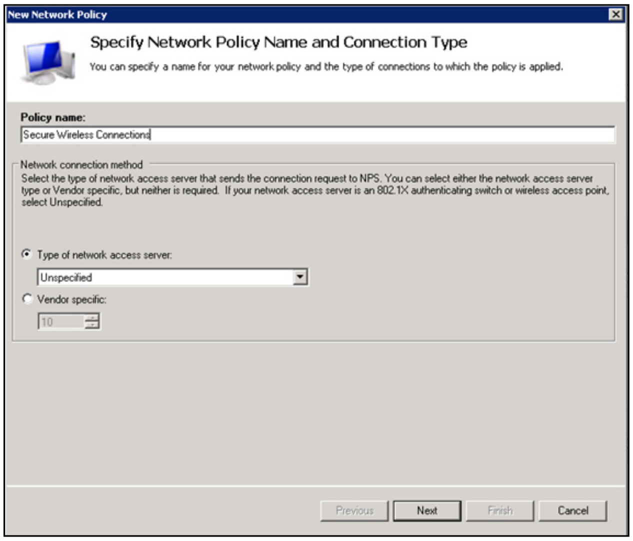


Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Conditions - If the following conditions are met:

Settings - Then the following settings are applied:

2. Configure the policy name as **Secure Wireless Connections** and select **Next**.



Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name: Secure Wireless Connections

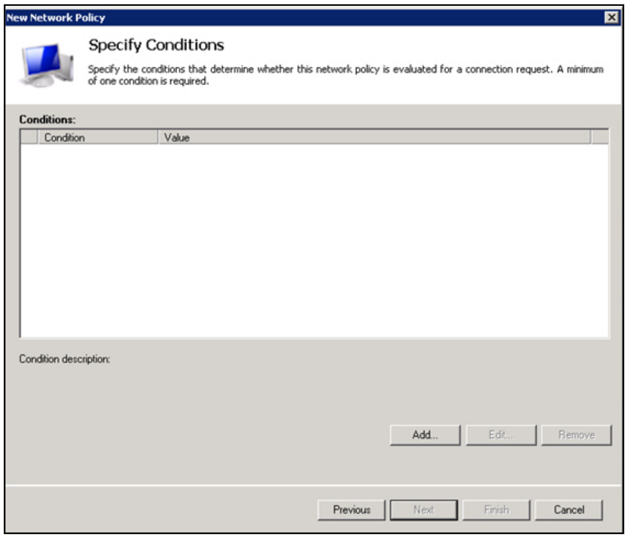
Network connection method

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, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server: Unspecified

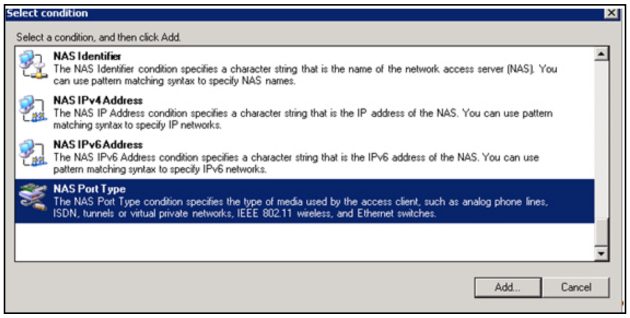
○ Vendor specific: 10

3. In the **Specify Conditions** menu, select **Add**.



Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

4. In the **Select condition** menu, select **NAS Port Type** and select **Add**.



Select a condition, and then click Add.

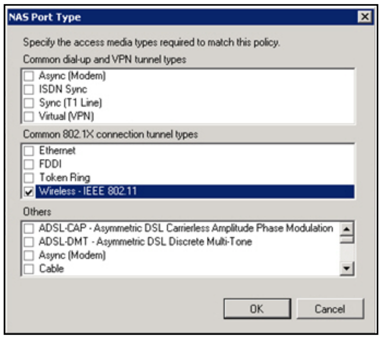
NAS Identifier
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.

NAS IPv4 Address
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.

NAS IPv6 Address
The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.

NAS Port Type
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

5. In the **NAS Port Type** menu, in the **Common 802.1x connection tunnel types** pane, select **Wireless-IEEE 802.11** and select **OK**.



Specify the access media types required to match this policy.

Common dial-up and VPN tunnel types

- ☐ Async (Modem)
- ☐ ISDN Sync
- ☐ Sync (T1 Line)
- ☐ Virtual (VPN)

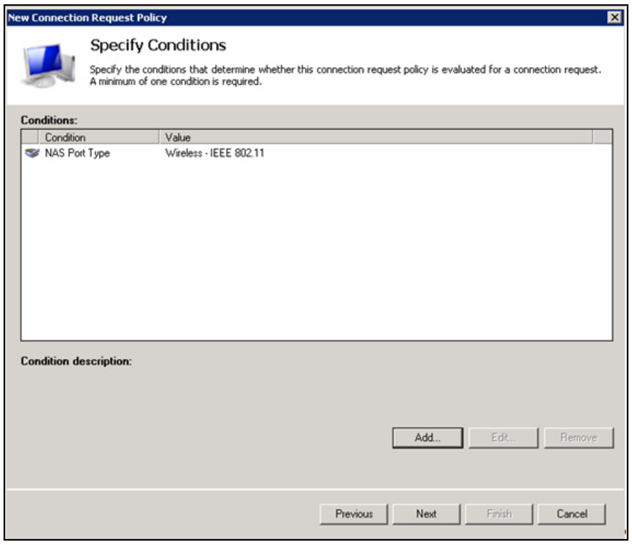
Common 802.1X connection tunnel types

- ☐ Ethernet
- ☐ FDDI
- ☐ Token Ring
- ☑ Wireless - IEEE 802.11

Others

- ☐ ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation
- ☐ ADSL-DMT - Asymmetric DSL Discrete Multi-Tone
- ☐ Async (Modem)
- ☐ Cable

6. The **NAS Port Type** with a value of **Wireless-IEEE 802.11** appears in the **Specify Conditions** menu. Select **Add** again.



New Connection Request Policy

Specify Conditions

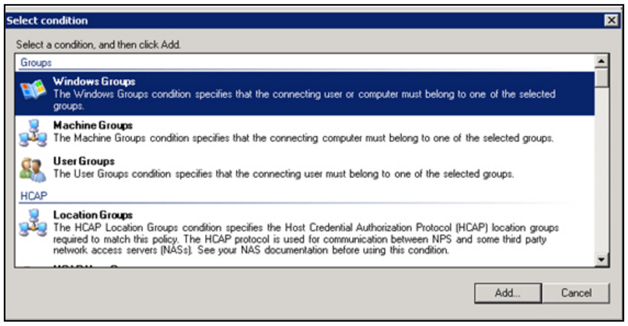
Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
NAS Port Type	Wireless - IEEE 802.11

Condition description:

7. In the **Select condition** menu, select **Windows Groups** and then **Add**.



Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

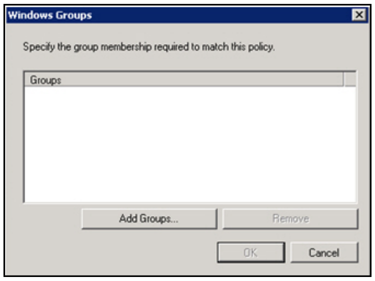
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

8. In the **Windows Groups** menu, select **Add Groups**.

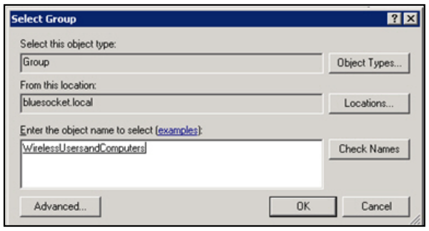


Windows Groups

Specify the group membership required to match this policy.

Groups

9. Enter **WirelessUsersandComputers** in the object name field and select **OK**.



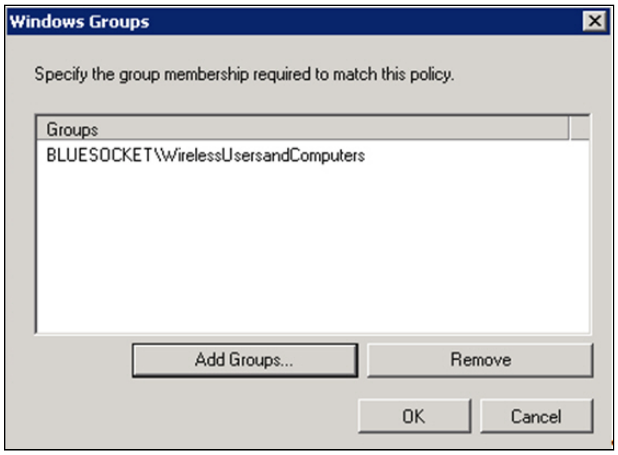
Select Group

Select this object type:
Group

From this location:
bluesocket.local

Enter the object name to select (examples):
WirelessUsersandComputers

10. In the **Windows Groups** menu, the **BLUESOCKET\WirelessUsersandComputers** group appears. Select **OK** to continue.

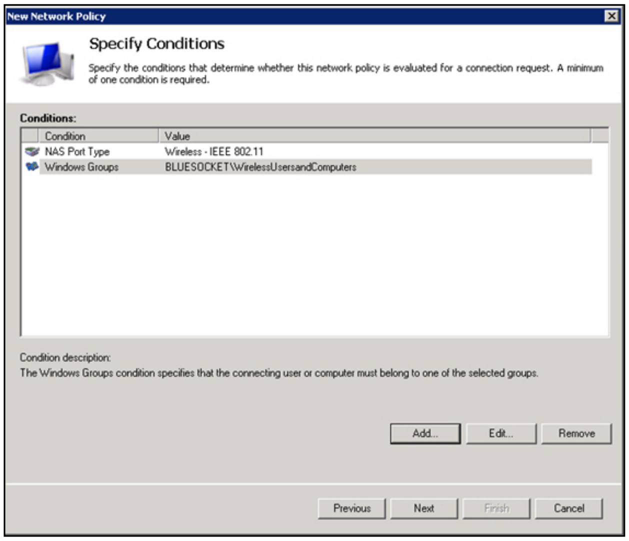


Windows Groups

Specify the group membership required to match this policy.

Groups
BLUESOCKET\WirelessUsersandComputers

11. In the **Specify Conditions** menu, the Windows group **BLUESOCKET\WirelessUsersandComputers** is displayed. Select **Next** to continue.



New Network Policy

Specify Conditions

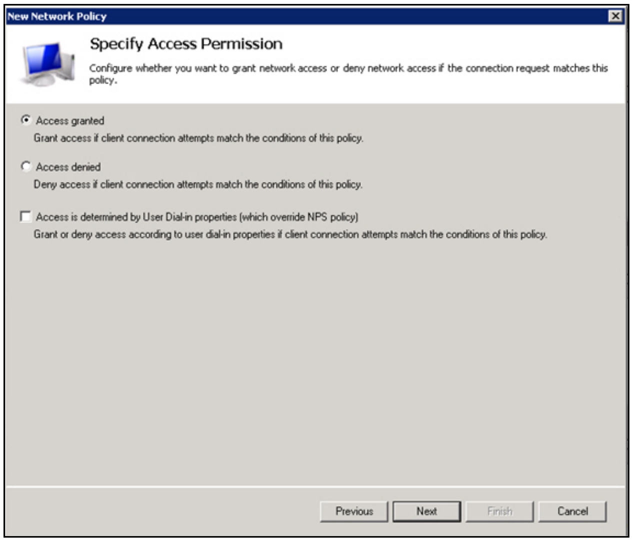
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
NAS Port Type	Wireless - IEEE 802.11
Windows Groups	BLUESOCKET\WirelessUsersandComputers

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

12. In the **Specify Access Permission** menu, select **Access Granted**. Do not select **Access is determined by User Dial-in properties**. Select **Next** to continue.



Specify Access Permission

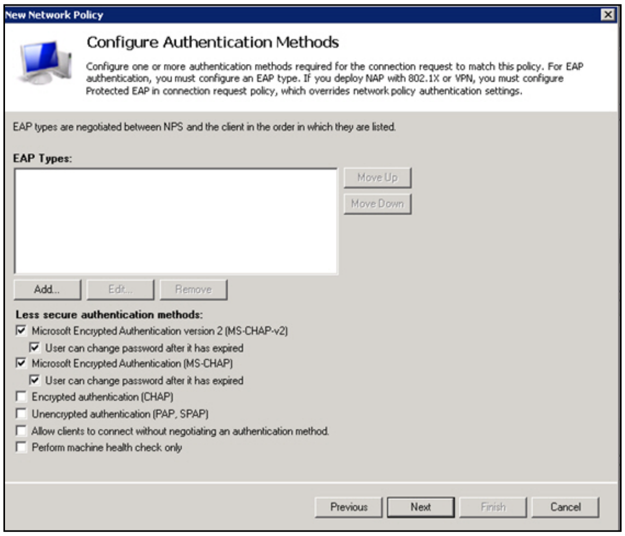
Configure whether you want to grant network access or deny network access if the connection request matches this policy.

● Access granted
Grant access if client connection attempts match the conditions of this policy.

○ Access denied
Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

13. In the **Configure Authentication Methods** menu, under **EAP types**, select **Add**.



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

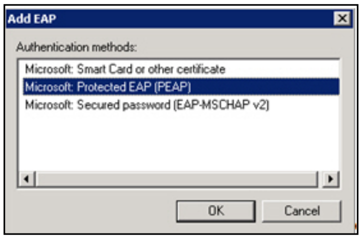
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

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

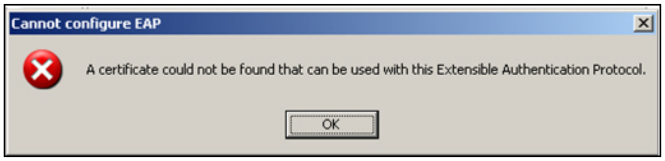
14. In the **Add EAP** menu, select **Microsoft: Protected EAP (PEAP)** and select **OK**.



Authentication methods:

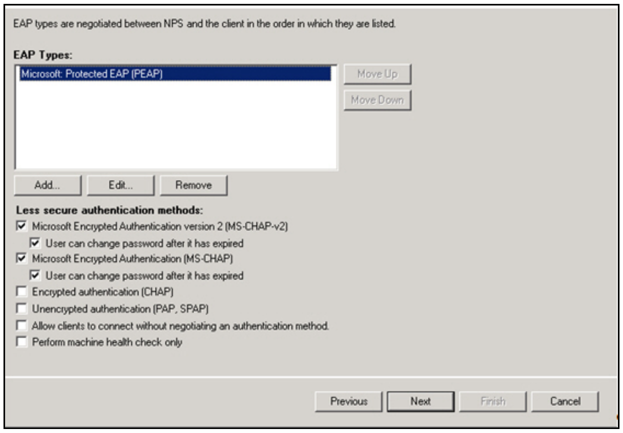
Microsoft: Smart Card or other certificate
Microsoft: Protected EAP (PEAP)
Microsoft: Secured password (EAP-MSCHAP v2)

15. If a server certificate has not been installed, or the server certificate does not meet Microsoft's minimum server certificate requirements for PEAP, you will receive an error. You must cancel the configuration and resolve the certificate issue before proceeding.


Cannot configure EAP

A certificate could not be found that can be used with this Extensible Authentication Protocol.

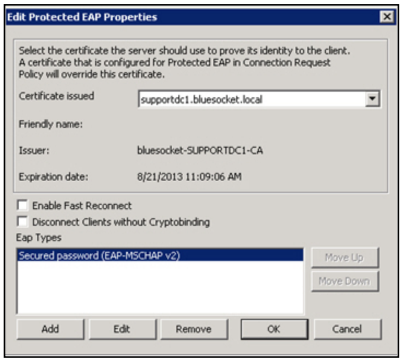
16. If you did not receive a certificate error, **Microsoft: Protected EAP (PEAP)** is now listed under **EAP Types**. Select **Microsoft: Protected EAP (PEAP)** and then select **Edit**.


EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:
Microsoft: Protected EAP (PEAP)

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

17. In the **Edit Protected EAP Properties** menu, select the appropriate server certificate from the **Certificate issued** drop-down menu. Deselect the fast reconnect check box since the feature is not supported by vWLAN. Verify that **Secured password (EAP-MSCHAP v2)** is shown in the **EAP Types** pane, and select **OK**.


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: supportdc1.bluesocket.local

Friendly name:

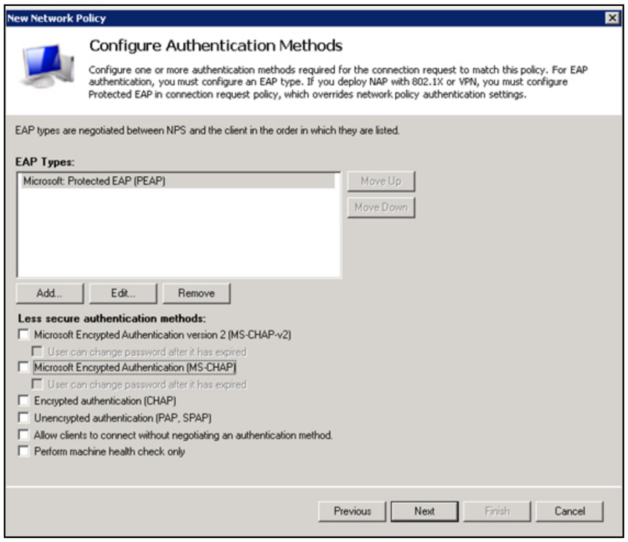
Issuer: bluesocket-SUPPORTDC1-CA

Expiration date: 8/21/2013 11:09:06 AM

□ Enable Fast Reconnect
□ Disconnect Clients without Cryptobinding

Eap Types
Secured password (EAP-MSCHAP v2)

18. In the **Configure Authentication Methods** menu, deselect any **Less secure authentication methods** that have been selected, and then select **Next**.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

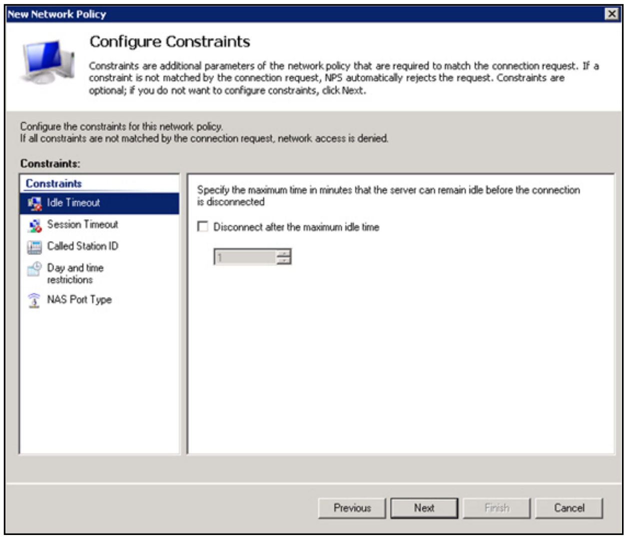
EAP Types:

Microsoft: Protected EAP (PEAP)

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

19. In the **Configure Constraints** menu, select **Next** to accept the default configuration.



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

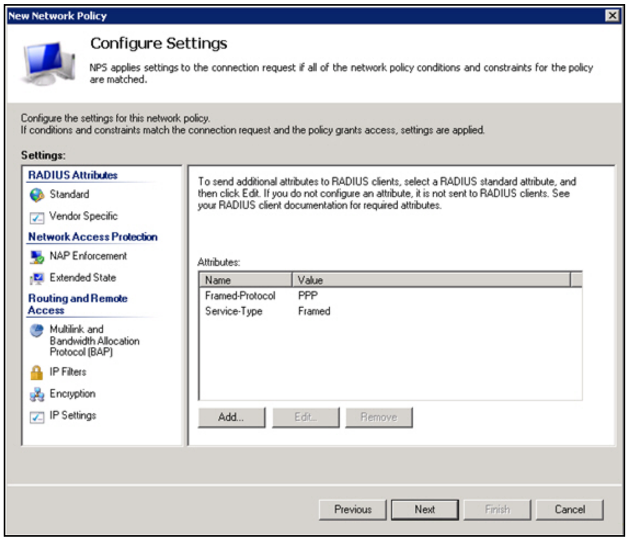
Constraints:

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

□ Disconnect after the maximum idle time

1

20. In the **Configure Settings** menu, select **Next** to accept the default configuration.



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

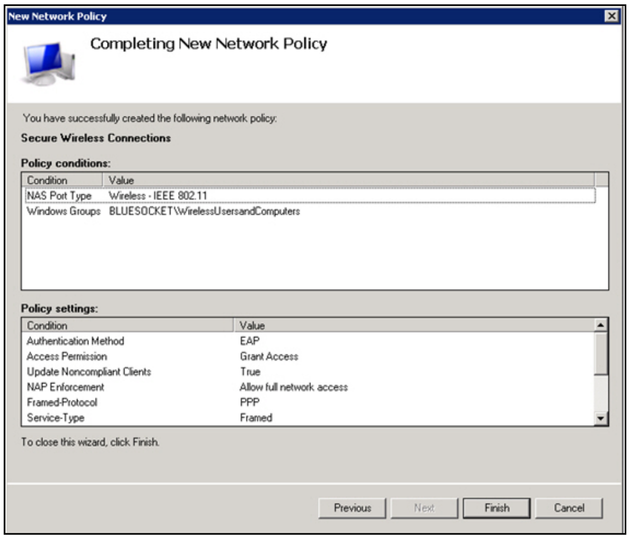
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

21. In the **New Network Policy** menu, select **Finish** to create the network policy.



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

Secure Wireless Connections

Policy conditions:

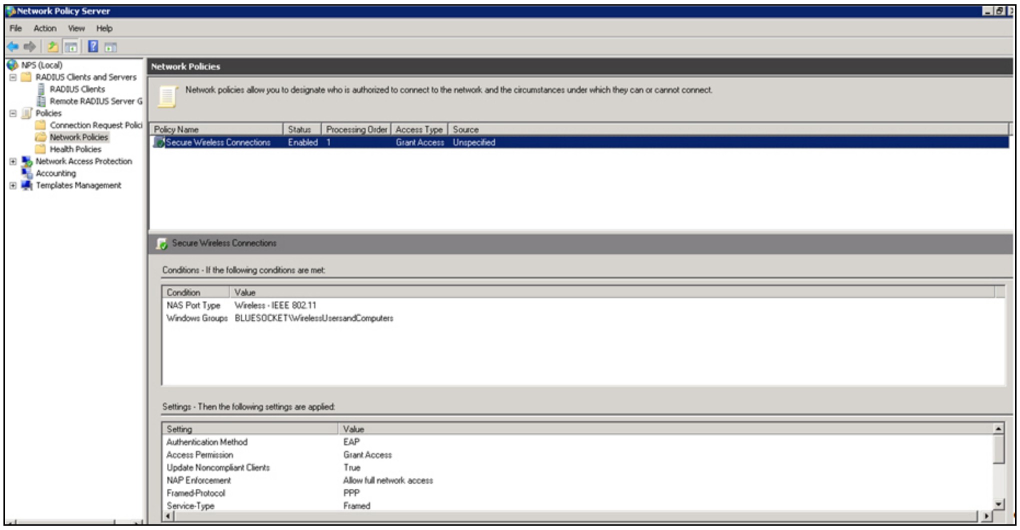
Condition	Value
NAS Port Type	Wireless - IEEE 802.11
Windows Groups	BLUESOCKET\WirelessUsersandComputers

Policy settings:

Condition	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

22. The **Secure Wireless Connections** network policy now appears in the **Network Policy Server** > **NPS (Local)** > **Policies** > **Network Policies** menu. NPS server configuration is now complete.



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Secure Wireless Connections	Enabled	1	Grant Access	Unspecified

Secure Wireless Connections

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Wireless - IEEE 802.11
Windows Groups	BLUESOCKET\WirelessUsersandComputers

Settings - Then the following settings are applied:

Setting	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

Step 4: Registering the NPS Server in Active Directory

NPS must be registered in Active Directory (AD) so that it has permission to read the dial-in properties of user accounts during the authorization process. Registering an NPS adds the server to the remote access software (RAS) and Internet authentication service (IAS) servers group in AD.

To register an NPS server in its default domain, follow these steps:

1. Open the NPS console.
2. Right-click **NPS (Local)** and select **Register Server in Active Directory**. The **Network Policy Server** menu appears.
3. In the **Network Policy Server** menu, select **OK** and then select **OK** again. Registration is complete.

Step 5: Configure the NPS Server to Ignore User Account Dial-in Properties

This step is used to configure an NPS network policy to ignore the dial-in properties of user accounts in AD during the authorization process. User accounts in AD UC have dial-in properties that NPS evaluates during the authorization process, unless the network access permission property of the user account is set to **Control access through NPS Network Policy**. This setting is enabled by default when using the Scenario wizard is used to configure the RADIUS server for 802.1x wireless or wired connections.

There are two situations in which configuring NPS to ignore the dial-in properties of user accounts in AD is beneficial:

- First, if you want to simplify NPS authorization by using a network policy, but not all of your user accounts have the network access permission property set to **Control access through NPS Network Policy**, ignoring the dial-in properties of user accounts can be necessary. For example, some user accounts might have the network access permission property of the user account set to **Deny access** or **Allow access**.

- Second, if other dial-in properties of user accounts are not applicable to the connection type configured in the network policy, ignoring the dial-in properties of user accounts can be beneficial. For example, properties other than the network access permission setting are applicable only to dial-in or virtual private network (VPN) connections, but the network policy you are creating is for wireless connections.

When NPS is configured to ignore the dial-in properties of user accounts, then NPS does not use the dial-in properties of the user account to determine whether the user or computer is authorized to access the network. Instead, only the settings in the network policy are used to determine authorization. To configure NPS to ignore user account dial-in properties, follow these steps:

1. Select **Start**, and navigate to **Administrative Tools** > **Network Policy Server**. The NPS menu appears.
2. In the **Network Policy Server** menu, double-click **Policies** and select **Network Policies**. Double-click the policy you want to configure from the list in the policy detail pane.
3. In the policy **Properties** menu, select the **Overview** tab and scroll to the **Access Permission** pane. Select the **Ignore user account dial-in properties** check box, and select **OK**.

Configuring the Windows 7 Client for Authentication

After configuring vWLAN and Windows Server 2008 for authentication, you must configure the Windows 7 client. You can configure the Windows 7 client for authentication using one of two methods:

- *Configuring the Windows 7 Client Manually using WLAN AutoConfig Supplicant on page 48*
- *Configuring the Windows 7 Client Automatically using Group Policies on page 54*

These configuration methods are described in the following sections.

Configuring the Windows 7 Client Manually using WLAN AutoConfig Supplicant

Ideally, the settings configured in this section and the private CA certificate are distributed to clients using group policies and AD CS. However, you might need to configure these settings manually. This section describes how to manually configure Windows 7 clients using the built-in WLAN AutoConfig supplicant. There are two main steps to manually configuring the Windows 7 clients:

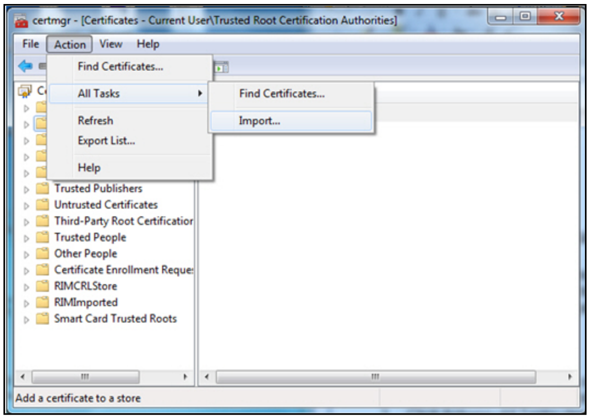
- *Manually Installing the Private CA Certificate on page 48*
- *Manually Configuring the Windows 7 Client using the WLAN AutoConfig Supplicant on page 51*

Manually Installing the Private CA Certificate

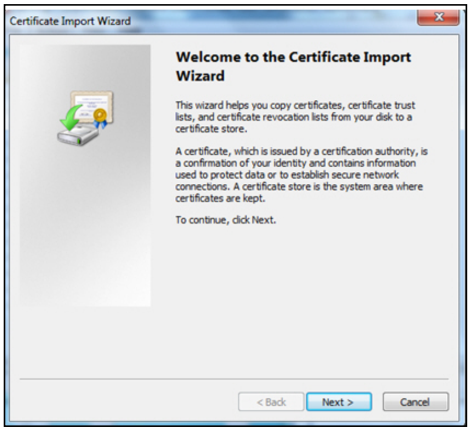
To manually install the private CA certificate for Windows 7 clients, follow these steps:

1. On the Windows 7 client, select **Start** and enter **certmgr.msc** in the **Search** field.
2. Select the **Trusted Root Certification Authorities** folder.

3. Select **Actions** > **All Tasks** > **Import**.



4. The **Certificate Import Wizard** menu appears. Select **Next** to continue.



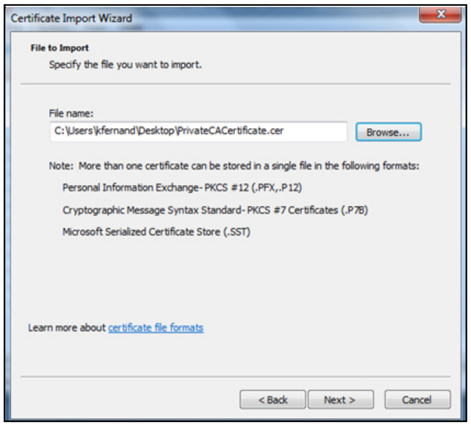
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

5. Select **Browse** and locate the private CA certificate to import. Select **Next** when you have chosen the appropriate certificate.



File to Import

Specify the file you want to import.

File name:
C:\Users\kfernand\Desktop\PrivateCACertificate.cer

Note: More than one certificate can be stored in a single file in the following formats:

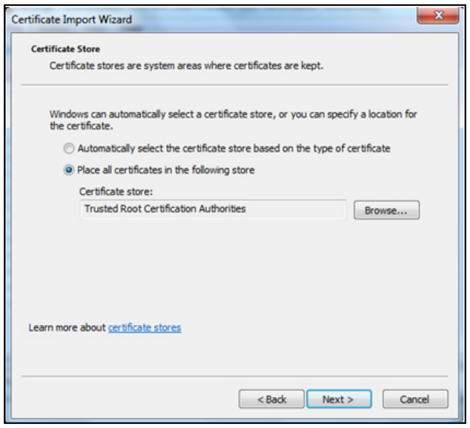
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

6. Select **Place all certificates in the following store** and select **Trusted Root Certification Authorities** using the **Browse** button. Select **Next** to continue.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

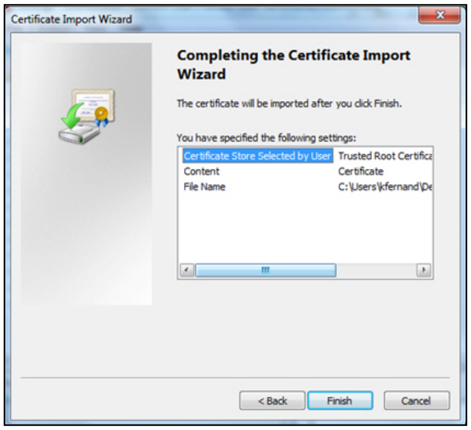
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

7. Select **Finish** to complete the certificate import.



Certificate Import Wizard

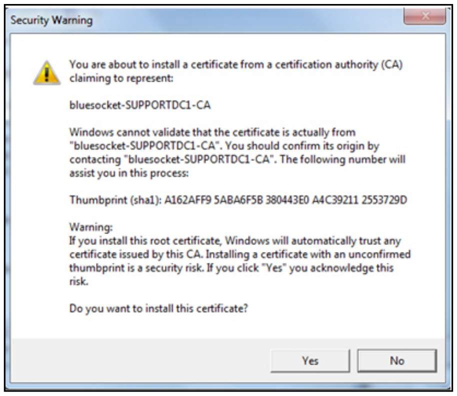
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate
File Name	C:\Users\kfernand\De

8. You will receive a security warning indicating you are about to install a certificate from a CA claiming to represent your organization. Review the warning to be certain you are installing the correct certificate. If the certificate is correct, select **Yes** to continue with the installation. The installation of the certificate is now complete and you can begin configuring the Windows 7 client.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

bluesocket-SUPPORTDC1-CA

Windows cannot validate that the certificate is actually from "bluesocket-SUPPORTDC1-CA". You should confirm its origin by contacting "bluesocket-SUPPORTDC1-CA". The following number will assist you in this process:

Thumbprint (sha1): A162AFF9 5ABA6F5B 380443E0 A4C39211 2553729D

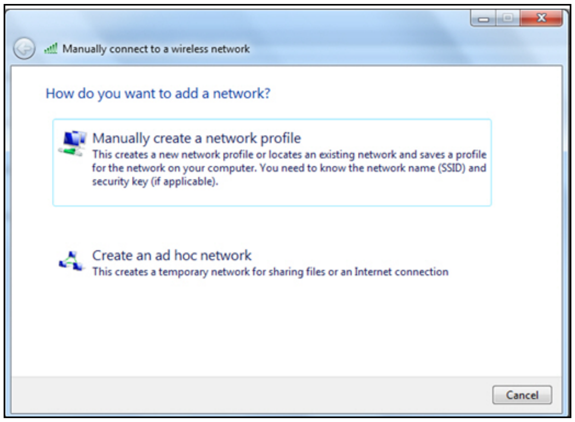
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Manually Configuring the Windows 7 Client using the WLAN AutoConfig Supplicant

After installing the private CA certificate, you can begin configuring the Windows 7 client. To configure the client using the WLAN AutoConfig supplicant, follow these steps:

1. On the Windows 7 client, select **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**. In this menu, select **Manage Wireless Networks** and then select **Manually create a network profile**.



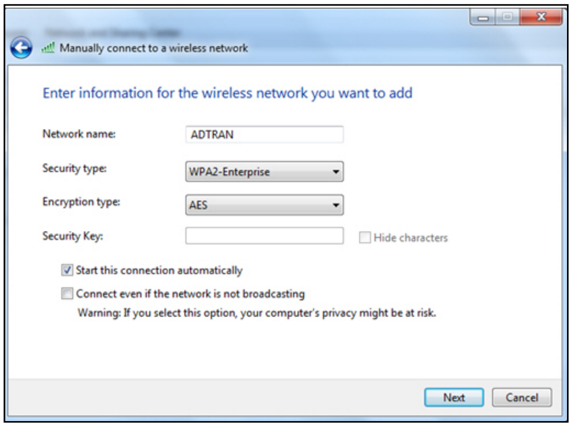
Manually connect to a wireless network

How do you want to add a network?

Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

2. Enter the client's SSID in the **Network name** field and select **WPA2-Enterprise** from the **Security type** drop-down menu. Select **AES** from the **Encryption type** drop-down menu, and select **Start this connection automatically**. If your SSID is not broadcast, select **Connect even if the network is not broadcasting**. If the SSID is broadcast, do not enable this feature. Select **Next** once the information has been entered.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: ADTRAN

Security type: WPA2-Enterprise

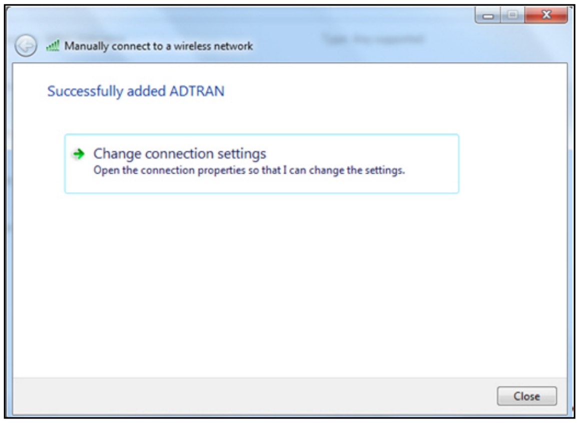
Encryption type: AES

Security Key: □ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting
Warning: If you select this option, your computer's privacy might be at risk.

3. You will receive a message indicating that you have successfully added the SSID. Select **Change connection settings** to continue.

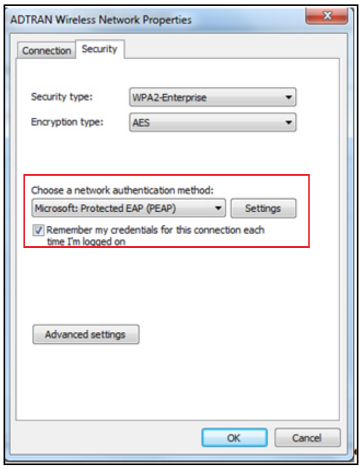


Manually connect to a wireless network

Successfully added ADTRAN

Change connection settings
Open the connection properties so that I can change the settings.

4. In the **Wireless Network Properties** menu, select the **Security** tab. Verify that **Microsoft: Protected EAP (PEAP)** is selected as the network authentication method, and then select **Settings**.



ADTRAN Wireless Network Properties

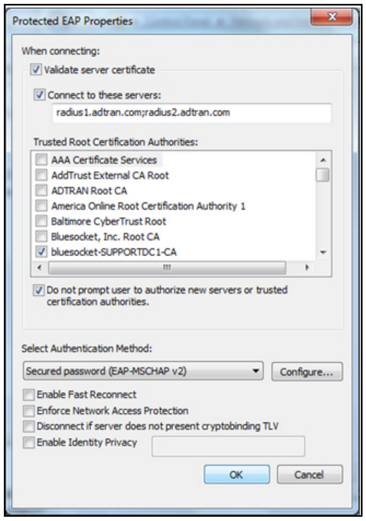
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:
Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

5. In the **Protected EAP Properties** menu, verify that **Validate server certificate** is selected. Select **Connect to these servers** and enter your RADIUS servers in the field. Separate multiple entries with a semicolon. In the **Trusted Root Certification Authorities** field, select the private CA certificate installed in *Manually Installing the Private CA Certificate on page 48*. Select **Do not prompt user to authenticate new servers or trusted certification authorities** and deselect **Enable Fast Reconnect**. Verify that **Secured password (EAP-MSCHAP v2)** is specified as the authentication method, and select **Configure**.



Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

radius1.adtran.com;radius2.adtran.com

Trusted Root Certification Authorities:

□ AAA Certificate Services
□ AddTrust External CA Root
□ ADTRAN Root CA
□ America Online Root Certification Authority 1
□ Baltimore CyberTrust Root
□ Bluesocket, Inc. Root CA
☑ bluesocket-SUPPORTDC1-CA

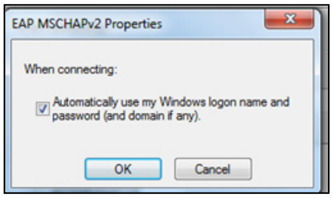
☑ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

6. In the **EAP MSCHAPv2 Properties** menu, verify that **Automatically use my Windows logon name and password** is selected, and then select **OK**.

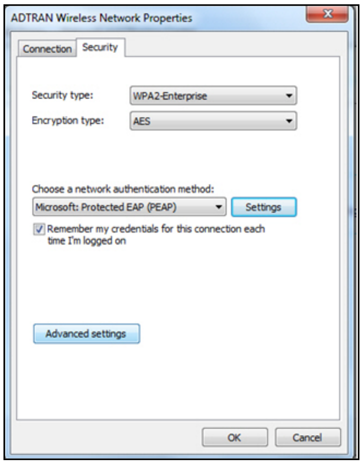


EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

7. In the **Wireless Network Properties** menu, select **Advanced settings**.



ADTRAN Wireless Network Properties

Security type: WPA2-Enterprise

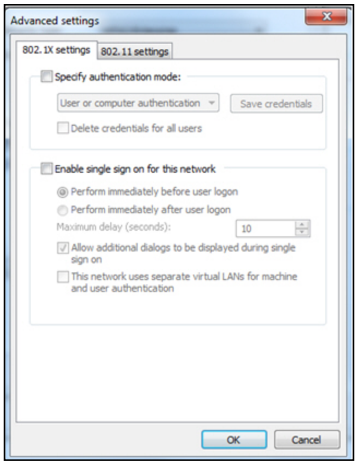
Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

8. On the **802.1x settings** tab, verify that **User or computer authentication** is selected. These configuration options are in gray and not configurable, but **User or computer authentication** should be enabled by default.



□ Specify authentication mode:

User or computer authentication

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

9. Select **OK**, then **OK** again, and then select **Close**. The configuration of the Windows 7 client is complete.

Configuring the Windows 7 Client Automatically using Group Policies

The previous configuration described how to manually configure Windows 7 clients using the built-in WLAN AutoConfig supplicant, but ideally these settings and the private CA certificate are distributed to the clients using group policies and AD CS. The following section describes how to distribute these settings and the private CA certificate to Windows 7 using group policies and AD CS. There are two main sections to this configuration:

- *Automatically Installing Private CA Certificates on page 54*
- *Automatically Configuring Windows 7 Clients using Group Policies on page 54*

Automatically Installing Private CA Certificates

By default, AD CS automatically distributes its private CA certificate to domain computers and users. The private CA certificate is installed in the Trusted Root Certificate Authorities store of the local computer and user. The NPS server is trusted by the client because the client trusts the private CA that issued the NPS server certificate.

Automatically Configuring Windows 7 Clients using Group Policies

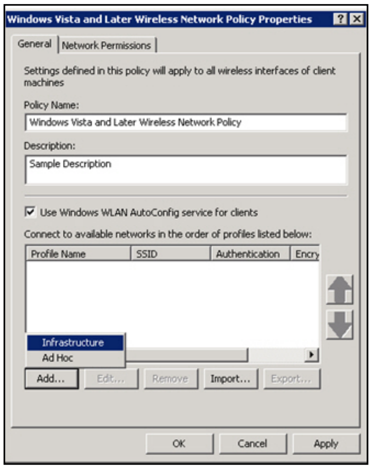
To automatically configure the Windows 7 client using a group policy, follow these steps:

1. On the Windows Server 2008 domain controller, navigate to **Start** > **Administrative Tools** > **Group Policy Management**.
2. Expand the **Domains** option and expand your domain folder. Right-click the **Default Domain Policy** and select **Edit**.

3. Expand the **Computer Configuration** option, and navigate to **Policies** > **Windows Settings** > **Security Settings**. Right-click the **Wireless Network (IEEE 802.11)** option and select **Create a New Wireless Network Policy for Windows Vista and Later Releases**.

> NOTE
>
> *Although this configuration is for Windows 7, Windows XP clients can be configured in a similar process. If you are configuring Windows XP clients, select **Create a New Windows XP Policy**.*

4. Select the **General** tab. Enter the name of the policy in the **Policy Name** field, enter a description of the policy in the **Description** field, and verify that **Use Windows WLAN AutoConfig service for clients** is selected. This option allows you to standardize the Windows built-in supplicant. In the profile list, select **Add** and then **Infrastructure**.



Windows Vista and Later Wireless Network Policy Properties

Settings defined in this policy will apply to all wireless interfaces of client machines

Policy Name: Windows Vista and Later Wireless Network Policy

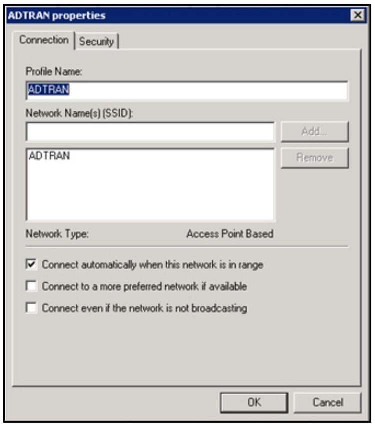
Description: Sample Description

☑ Use Windows WLAN AutoConfig service for clients

Connect to available networks in the order of profiles listed below:

Profile Name	SSID	Authentication	Encry

5. In the **Properties** menu, select the **Connection** tab. Enter a name for the profile in the **Profile Name** field and the SSID in the **Network Name(s) (SSID)** field. Verify that **Connect automatically when this network is in range** is selected, and deselect **Connect to a more preferred network if available**. Select **Add** in the SSID menu.



ADTRAN properties

Profile Name: ADTRAN

Network Name(s) (SSID): ADTRAN

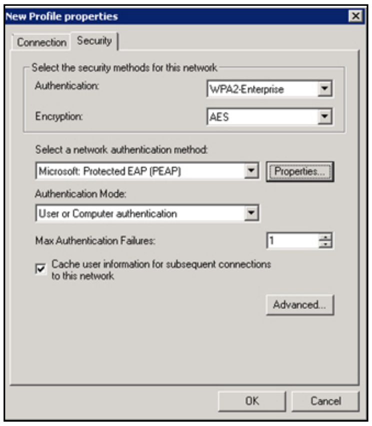
Network Type: Access Point Based

☑ Connect automatically when this network is in range

☐ Connect to a more preferred network if available

☐ Connect even if the network is not broadcasting

6. In the **New Profile properties** menu, select the **Security** tab. Select **WPA2-Enterprise** in the **Authentication** drop-down menu, and **AES** in the **Encryption** drop-down menu. Verify that **Microsoft: Protected EAP (PEAP)** is the authentication method, and select **Properties**.



New Profile properties

Select the security methods for this network

Authentication: WPA2-Enterprise

Encryption: AES

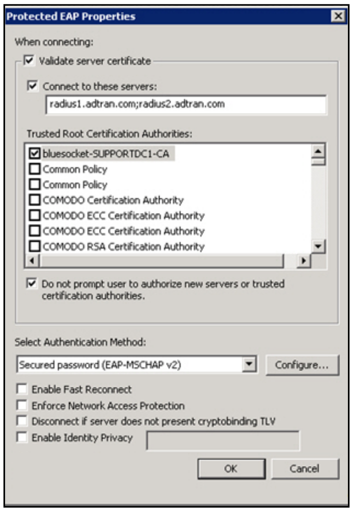
Select a network authentication method: Microsoft: Protected EAP (PEAP)

Authentication Mode: User or Computer authentication

Max Authentication Failures: 1

☑ Cache user information for subsequent connections to this network

7. In the **Protected EAP Properties** menu, verify that **Validate server certificate** is selected. Select the **Connect to these servers** option and enter your RADIUS servers in the appropriate field. Separate multiple entries with semicolons. Select the appropriate private CA certificate from the **Trusted Root Certification Authorities** list, and select **Do not prompt user to authorize new servers or trusted certification authorities**. Verify that **Secured password (EAP-MSCHAP v2)** is the authentication method, and verify that **Automatically use my windows logon name and password** is selected in the EAP MSCHAPv2 configuration (use the **Configure** button). Make sure that **Enable Fast Reconnect** is not selected, and select **OK**.



Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

radius1.adtran.com;radius2.adtran.com

Trusted Root Certification Authorities:

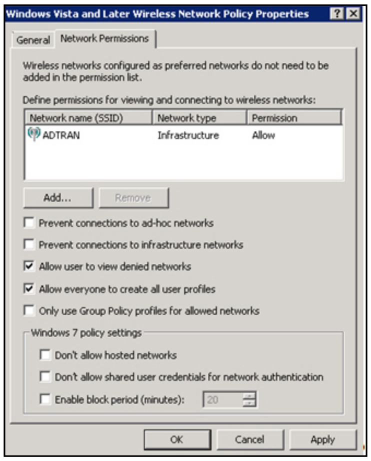
☑ bluesocket-SUPPORTDC1-CA
☐ Common Policy
☐ Common Policy
☐ COMODO Certification Authority
☐ COMODO ECC Certification Authority
☐ COMODO ECC Certification Authority
☐ COMODO RSA Certification Authority

☑ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method: Secured password (EAP-MSCHAP v2)

☐ Enable Fast Reconnect
☐ Enforce Network Access Protection
☐ Disconnect if server does not present cryptobinding TLV
☐ Enable Identity Privacy

8. In the **New Profile properties** menu, select the **Security** tab and verify that the **Authentication Mode** is set to **User or computer authentication**. Select **OK**.
9. In the **Windows Vista and later Wireless Network Policy Properties** menu, select the **Network Permissions** tab and set permissions as necessary for your organization. Select **OK** to complete the client configuration.



Wireless networks configured as preferred networks do not need to be added in the permission list.

Define permissions for viewing and connecting to wireless networks:

Network name (SSID)	Network type	Permission
ADTRAN	Infrastructure	Allow

☐ Prevent connections to ad-hoc networks

☐ Prevent connections to infrastructure networks

☑ Allow user to view denied networks

☑ Allow everyone to create all user profiles

☐ Only use Group Policy profiles for allowed networks

Windows 7 policy settings

☐ Don't allow hosted networks

☐ Don't allow shared user credentials for network authentication

☐ Enable block period (minutes): 20

Additional vWLAN Authentication Configurations

In addition to configuring external RADIUS 802.1x authentication, there are several other services you can configure for vWLAN that can be beneficial to your network. These configurations include:

- *Configuring vWLAN RADIUS Accounting on page 57*
- *Configuring vWLAN to Enforce Machine Authentication on page 59*
- *Configuring vWLAN for Dynamic Role Assignment Using RADIUS Attributes on page 61*

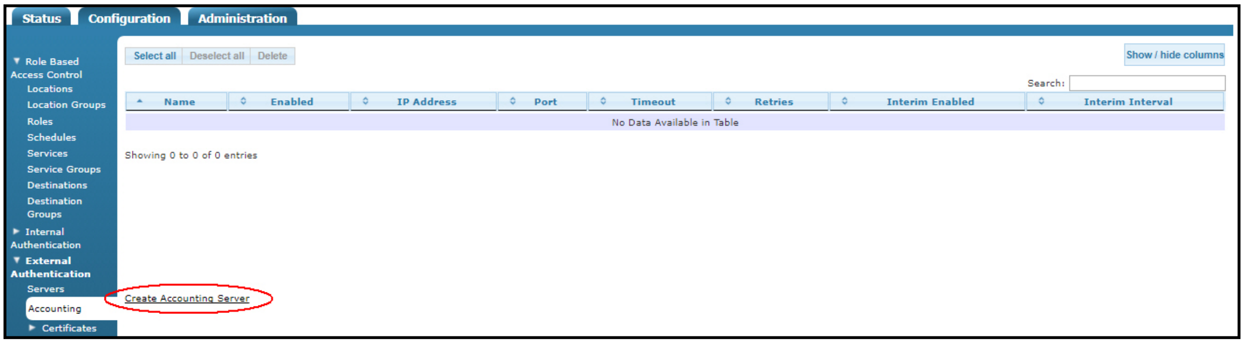
Configuring vWLAN RADIUS Accounting

RADIUS accounting can be used to notify external systems about user's usage of the vWLAN system. When a client is authenticated and joins the vWLAN system, a start request is sent to the accounting server. When the client leaves the vWLAN system, after a timeout period, a stop request is sent to the accounting server. Interim records can also be sent at periodic intervals, so that the external system can track vWLAN users. This can be helpful in tracking users that stay logged into the system for extended periods of time. To use accounting servers with vWLAN, you must configure the accounting server, and then associate the server with one of the methods of authentication; RADIUS 802.1x, RADIUS web, LDAP, or SIP2 authentication servers, or local or MAC authentication. Accounting can also be used for a client that is assigned a default role using an SSID or wired access group by selecting the server in the SSID or wired access group configuration.

When configuring a RADIUS accounting server to use with vWLAN, note that the standard RADIUS accounting attributes apply, as well a vendor-specific attribute under the vendor code (**9967**).

To configure a RADIUS accounting server in vWLAN, follow these steps:

1. Navigate to the **Configuration** tab, and select **External Authentication** > **Accounting**. Any previously configured accounting servers will be listed in the menu. If you want to edit a previously created accounting server, select the name of the server. To create a new accounting server, either select **Create Accounting Server** at the bottom of this menu, or select **Domain Accounting Server** from the **Create** drop-down menu (at the top of the menu).

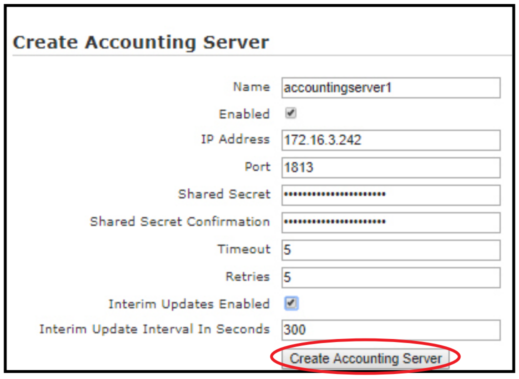


Name	Enabled	IP Address	Port	Timeout	Retries	Interim Enabled	Interim Interval
No Data Available in Table							

Showing 0 to 0 of 0 entries

Figure 20. Create a New Accounting Server

2. Enter the name of the server, the server's IP address, and the port used by the server (**1813** by default) in the appropriate fields. Enable the server by selecting the **Enabled** check box. Enter the shared secret for the accounting server, and the shared secret confirmation, in the appropriate fields. Specify the server timeout value (in seconds), and the number of times vWLAN will attempt to reconnect to the server in the appropriate fields. By default, the timeout value is set to **5** seconds, and the number of retries is set to **5**. Enable interim reporting updates by selecting the **Interim updates enabled** check box. Additionally, specify the interim update interval (in seconds) by entering a value in the appropriate field. By default, the interim update interval is set to **300** seconds. Select **Create Accounting Server** to create the server.

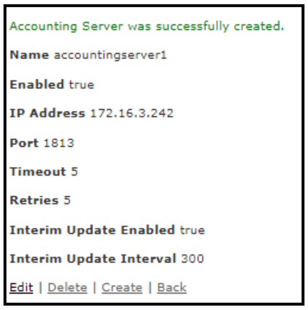


Create Accounting Server

Name	accountingserver1
Enabled	☑
IP Address	172.16.3.242
Port	1813
Shared Secret	••••••••••••••••••••••
Shared Secret Confirmation	••••••••••••••••••••••
Timeout	5
Retries	5
Interim Updates Enabled	☑
Interim Update Interval In Seconds	300

Figure 21. Configure the Accounting Server

3. A confirmation is displayed indicating that the server has been created. The server will now appear in the accounting server list (**Configuration** tab, **External Authentication** > **Accounting**), where you can display, edit, or delete the server.



Accounting Server was successfully created.

Name accountingserver1

Enabled true

IP Address 172.16.3.242

Port 1813

Timeout 5

Retries 5

Interim Update Enabled true

Interim Update Interval 300

Figure 22. Accounting Server was Successfully Created

Once the accounting server has been created, you can associate the accounting server with an authentication server as described in *Step 2: Configuring the External RADIUS 802.1x Authentication Server on page 14*.

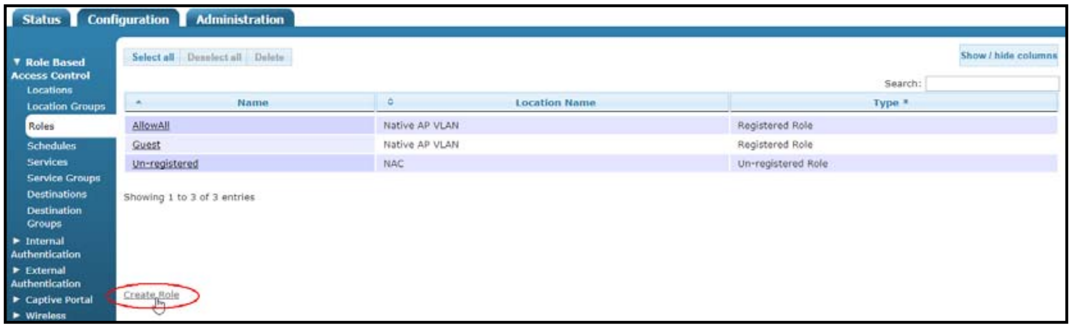
With NPS, you can log user authentication and accounting requests to files in text or database format, or you can log files to a stored procedure in a Structured Query Language (SQL) Server 2000, SQL Server 2005, or SQL Server 2008 database. The NPS configuration of RADIUS accounting is beyond the scope of this document.

Configuring vWLAN to Enforce Machine Authentication

Machine and user authentication are two separate processes by default. It is not required that machine authentication be performed before user authentication, or that the user be on a domain computer in order to perform user authentication and be placed into an often unrestricted employee role. This means that domain users can log in to vWLAN using those same domain user credentials on non-domain devices, such as iPhones, iPads, and Androids. Enforcing machine authentication allows you to require users to perform machine authentication before user authentication and be on a domain computer before users are placed in an unrestricted role. If a user has not completed machine authentication before user authentication, and they are not on a domain computer, they are considered using a non-domain device. Therefore, instead of being placed in the unrestricted role, they are placed in the unregistered role by default. Alternatively, they can be placed into a configurable failed machine authentication role (such as the Guest role), with only access to the Internet.

Enabling forced machine authentication is done in the role configuration of vWLAN. To configure a role with machine authentication enforced, follow these steps:

1. Navigate to the **Configuration** tab, and select **Role Based Access Control** > **Roles**. Any previously configured domain roles will be listed in the menu. If you want to edit a previously created domain role, select the name of the role you want to edit. To create a new domain role, either select **Create Role** at the bottom of this menu, or select **Domain Role** from the **Create** drop-down menu (at the top of the menu).

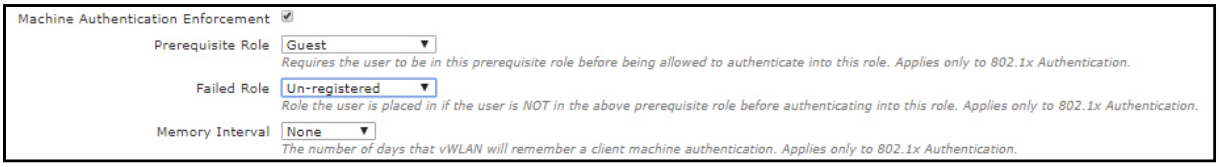


Name	Location Name	Type
AllowAll	Native AP VLAN	Registered Role
Guest	Native AP VLAN	Registered Role
Un-registered	NAC	Un-registered Role

Showing 1 to 3 of 3 entries

Figure 23. Creating a New Role

2. Specify whether 802.1x machine authentication will be enforced on the role by selecting the **Machine authentication enforcement** check box. Machine (computer) authentication allows the domain computer to authenticate before the user logs in when using a host name as the user name and the computer's domain machine account password as the password. Enabling this feature means that users who do not directly progress from machine authentication to user authentication are placed in the un-registered role, and allows group policies to be applied and login scripts to execute when the user logs in, as well as allows users who do not have locally cached profiles on the domain computer to login. A valid 802.1x user without a valid device can also be placed in a role other than un-registered (for example, the guest role) to allow a user to use smart phones and other devices that cannot access the domain. When this feature is enabled, the vWLAN system will only allow the user to be placed in a role as long as valid machine authentication occurred. vWLAN can be configured to remember machine authentication (using the **Memory interval** field), which keeps devices that time out and then reconnect from being left in an un-registered role. Enable the feature by selecting the **Machine authentication enforcement** check box. Once you have enabled this feature, you will specify the role into which users are placed when authenticating, the role in which users are placed if their authentication fails, and the number of days the vWLAN will remember the machine authentication. Select these 802.1x authentication values from the appropriate drop-down menu.


Machine Authentication Enforcement ☑

Prerequisite Role: Guest ▼
Requires the user to be in this prerequisite role before being allowed to authenticate into this role. Applies only to 802.1x Authentication.

Failed Role: Un-registered ▼
Role the user is placed in if the user is NOT in the above prerequisite role before authenticating into this role. Applies only to 802.1x Authentication.

Memory Interval: None ▼
The number of days that vWLAN will remember a client machine authentication. Applies only to 802.1x Authentication.

Figure 24. Parameters for Machine Authentication

3. If all other parameters of the role are configured correctly, select **Create Role** at the bottom of the menu to create the role.

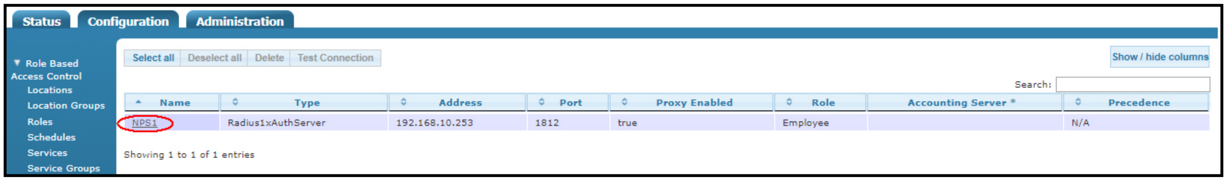
4. A confirmation is displayed indicating that the role has been created. The role will now appear in the role list (**Configuration** tab, **Role Based Access Control** > **Roles**), where you can display, edit, or delete the role. For more information about configuring roles in vWLAN, refer to the *vWLAN Administrator's Guide*, available online at https://supportforums.adtran.com.

Configuring vWLAN for Dynamic Role Assignment Using RADIUS Attributes

RADIUS attributes can be used to automatically assign users to a specific role if the attributes returned by the RADIUS server match the user credentials presented at login. For example, RADIUS attributes were used in *Step 2: Configuring the External RADIUS 802.1x Authentication Server on page 14* to specify that clients with user names beginning with **host/** were placed in the **Domain Computer** role. External RADIUS servers can be configured to match credentials based on user name, EAP method, or all standard Internet Engineering Task Force (IETF) RADIUS attributes. RADIUS attributes are specified in the external authentication server configuration. Each of the matching rules are processed in order. If a rule produces a match, then the corresponding role is assigned to the user and no further rules are processed. If there is no match, the default role is assigned. You can use the **Filter-Id** RADIUS attribute for dynamic role assignment. This attribute functions well because it contains human readable text. For example, if the RADIUS server is configured with the Filter-Id to equal Student, then the role assigned to users that match that criteria is Student. The following steps describe how to configure the RADIUS server for dynamic role assignment using RADIUS attributes.

To configure vWLAN for dynamic role assignment using RADIUS attributes, follow these steps:

1. In the vWLAN GUI, navigate to the **Configuration** tab and select **Role Based Access Control** > **Roles**. Create a new role to be assigned by the RADIUS server. Role configuration is described in *Configuring vWLAN to Enforce Machine Authentication on page 59* and in the *vWLAN Administrator's Guide*, available online at https://supportforums.adtran.com. In the current example, a role of **Student** is created. The RADIUS server is configured so that it assigns students to the Student role dynamically when the RADIUS server returns the Filter-Id RADIUS attribute with a value of Student.
2. After the role has been created, navigate to the **Configuration** tab and select **External Authentication** > **Servers**. Select the name of the primary RADIUS 802.1x server.

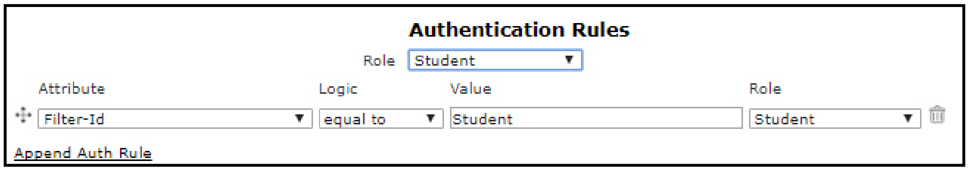


Name	Type	Address	Port	Proxy Enabled	Role	Accounting Server *	Precedence
NPS1	Radius1xAuthServer	192.168.10.253	1812	true	Employee		N/A

Showing 1 to 1 of 1 entries

Figure 25. Navigating to the Primary RADIUS 802.1X Server

3. In the server's configuration menu, scroll to the **Authentication Rules** section. Specify that the authentication rule uses the **Filter-Id** attribute, set **equal to** the **Student** value, and that it results in the **Student** role. Use the appropriate drop-down menus to make these selections. Once these settings are configured, select **Update Authorization Server**. Repeat these steps for a secondary RADIUS server.



Authentication Rules

Role: Student

Attribute	Logic	Value	Role
Filter-Id	equal to	Student	Student

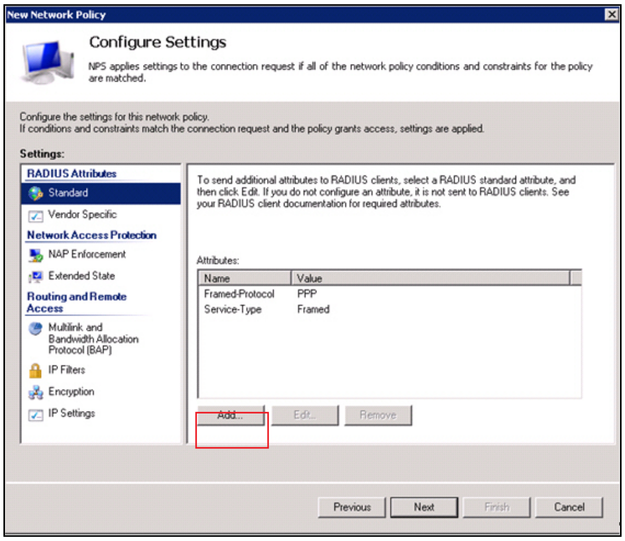
Figure 26. Adding Authentication Rules

4. After configuring the Student role and the RADIUS server, you must create an OU called **Student** in AD. All student users and computers should be placed in the OU. In addition, create a global security group called **StudentWireless** in the **Student** OU. Set all student users to be members of this group. Do

not, however, make the **StudentWireless** global security group a member of the **WirelessUsersandComputers** universal security group. The steps for creating the OU and global security group are outlined in *Step 1: Creating User and Computer Groups in Active Directory on page 19*.

5. After configuring AD with the student OU and group information, you must configure a policy in NPS to allow the **StudentWireless** global security group to access the secure wireless network and return the Filter-Id RADIUS attribute with a value of Student. This configuration is achieved by using the steps outlined in *Step 3: Configuring the NPS Server on page 22*. Make sure to enter **StudentWireless** as the Windows group (rather than **WirelessUsersandComputers**) when configuring the network conditions for the NAS Port Type.

6. In the **Configuration Settings** menu of the **New Network Policy** configuration, select **RADIUS Attributes** > **Standard**. Then select **Add**.



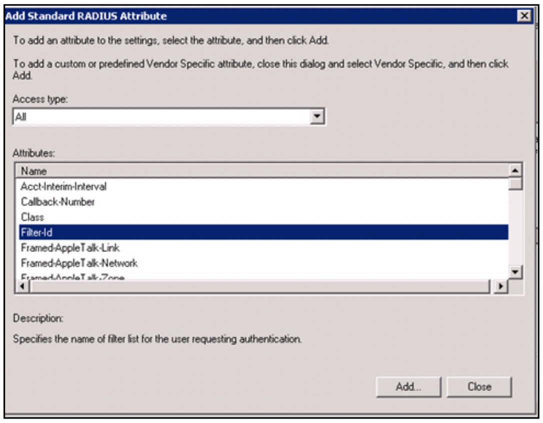
NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

7. Select **Filter-Id** from the **Attributes** list and then select **Add** again.



To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

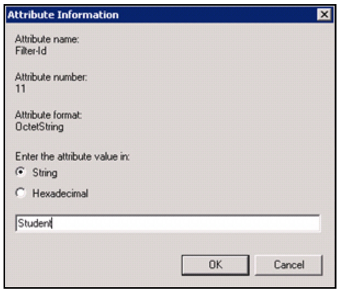
Access type: All

Name
Acct-Interim-Interval
Callback-Number
Class
Filter-Id
Framed-AppleTalk-Link
Framed-AppleTalk-Network
Framed-AppleTalk-Zone

Description:

Specifies the name of filter list for the user requesting authentication.

8. In the **Attribute Information** menu, select **String** and enter **Student** in the field. Select **OK**.



Attribute Information

Attribute name:
Filter-Id

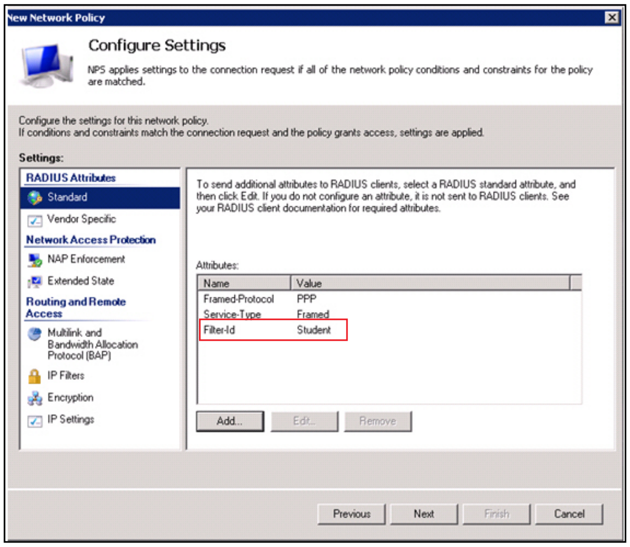
Attribute number:
11

Attribute format:
OctetString

Enter the attribute value in:
● String
○ Hexadecimal

Student

9. Select **OK**, and then select **Close**. In the **Configure Settings** menu the **Filter-Id** attribute, with a value of **Student** is now listed in the **Attributes** field.



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

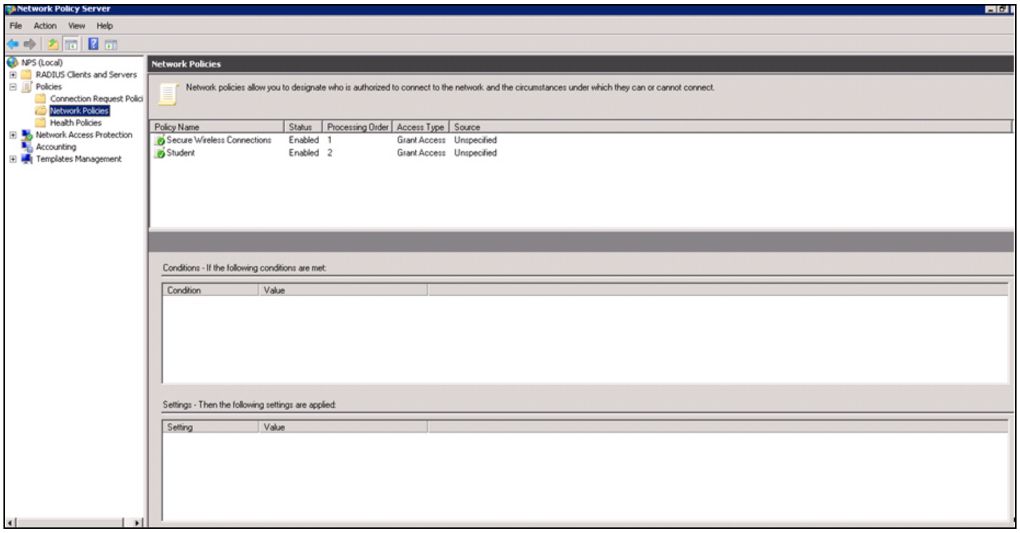
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed
Filter-Id	Student

10. Continue with the network policy configuration as described in *Step 3: Configuring the NPS Server on page 22*. Once the configuration is complete, the new **Student** network policy is displayed in the **Network Policy Server** configuration menu. The new policy returns the Filter-Id RAIDUS attribute with a value of Student, and since the Filter-Id is equal to Student in the vWLAN configuration, student users are placed in the Student role upon login (rather than the default role of Employee).



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Secure Wireless Connections	Enabled	1	Grant Access	Unspecified
Student	Enabled	2	Grant Access	Unspecified

Conditions - If the following conditions are met:

Condition	Value

Settings - Then the following settings are applied:

Setting	Value

> NOTE
>
> *In this section a new network policy was created to return the Filter-Id RADIUS attribute. An existing network policy can also be modified to return the Filter-Id RADIUS attribute (or other attributes) by double-clicking the network policy name and selecting the **Settings** tab. In the **Settings** menu, you can add RADIUS attributes to existing network policies.*

Troubleshooting

The following section contains helpful information that can be used to troubleshoot the external RADIUS 802.1x authentication operation. Troubleshooting can be accomplished using NPS logs, NPS reason codes, or vWLAN packet captures.

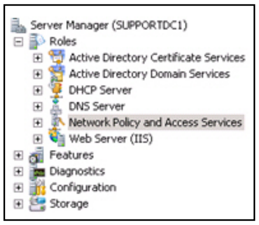
NPS Logs

Since RADIUS requests are sent by the APs directly to the RADIUS server when using external RADIUS 802.1x authentication (rather than sent to the vWLAN), RADIUS server logs (NPS logs) can be the most beneficial place to begin troubleshooting. NPS logs can be found in the Windows Server 2008 Server Manager or in the event viewer.

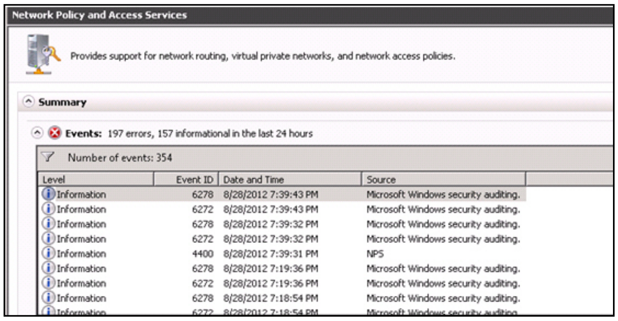
To open NPS logs in the Server Manager, follow these steps:

1. On the Windows Server 2008 domain controller that is running NPS, navigate to **Start** > **Administrative Tools** > **Server Manager**.

2. Expand the **Roles** menu and select **Network Policy and Access Services**.


Server Manager (SUPPORTDC1)
Roles
Active Directory Certificate Services
Active Directory Domain Services
DHCP Server
DNS Server
Network Policy and Access Services
Web Server (IIS)
Features
Diagnostics
Configuration
Storage

3. In the **Network Policy and Access Services** menu, expand the **Events** area.



Network Policy and Access Services

Provides support for network routing, virtual private networks, and network access policies.

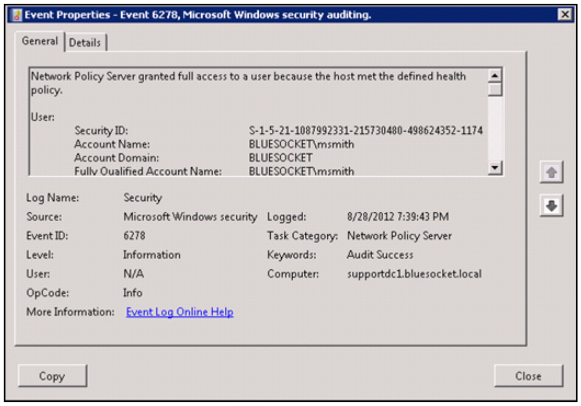
Summary

Events: 197 errors, 157 informational in the last 24 hours

Number of events: 354

Level	Event ID	Date and Time	Source
Information	6278	8/28/2012 7:39:43 PM	Microsoft Windows security auditing.
Information	6272	8/28/2012 7:39:43 PM	Microsoft Windows security auditing.
Information	6278	8/28/2012 7:39:32 PM	Microsoft Windows security auditing.
Information	6272	8/28/2012 7:39:32 PM	Microsoft Windows security auditing.
Information	4400	8/28/2012 7:39:31 PM	NPS
Information	6278	8/28/2012 7:19:36 PM	Microsoft Windows security auditing.
Information	6272	8/28/2012 7:19:36 PM	Microsoft Windows security auditing.
Information	6278	8/28/2012 7:18:54 PM	Microsoft Windows security auditing.
Information	6272	8/28/2012 7:18:54 PM	Microsoft Windows security auditing.

4. Double-click an event for more detailed information.



Event Properties - Event 6278, Microsoft Windows security auditing.

Network Policy Server granted full access to a user because the host met the defined health policy.

User:
Security ID: S-1-5-21-1087992331-215730480-498624352-1174
Account Name: BLUESOCKET\msmith
Account Domain: BLUESOCKET
Fully Qualified Account Name: BLUESOCKET\msmith

Log Name: Security
Source: Microsoft Windows security
Logged: 8/28/2012 7:39:43 PM
Event ID: 6278
Task Category: Network Policy Server
Level: Information
Keywords: Audit Success
User: N/A
Computer: supportdc1.bluesocket.local
OpCode: Info
More Information: Event Log Online Help

To view the NPS logs from the Event Viewer, follow these steps:

1. On the Windows Server 2008 domain controller that is running NPS, navigate to **Start** > **Administrative Tools** > **Event Viewer**.
2. In the **Event Viewer**, expand the **Custom Views** list.
3. In the **Custom Views** list, expand the **Server Roles** list.
4. In the **Server Roles** list, select **Network Policy and Access Services**. From this menu select **Events**.

> *In the Event Viewer, you can also select **Windows Logs** instead of **Custom Views**. NPS logs are displayed with standard Windows logs under **Security and System**.*

NPS Reason Codes

When NPS writes an event to the log, the event can contain a reason code. Reason codes provide specific information about the cause for the event being written to the log. Microsoft provides information about NPS reason codes online at http://technet.microsoft.com/en-us/library/dd197570(v=ws.10).aspx.

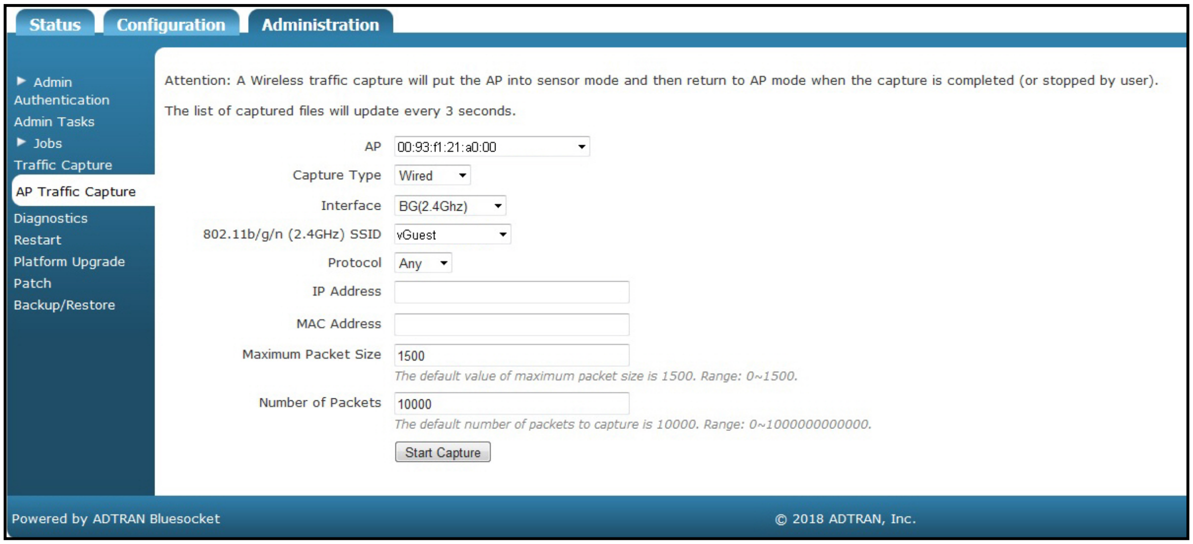
vWLAN Packet Captures

If NPS logs do not provide the information you need for troubleshooting purposes, you can get packet captures from vWLAN. There are two types of packet captures that are beneficial to RADIUS 802.1x authentication troubleshooting: captures of the RAIDUS traffic between an AP and a RADIUS server, and a capture of EAPOL traffic between an AP and a client.

Capturing RADIUS Traffic Between an AP and a RADIUS Server

To capture RADIUS traffic between an AP and a RADIUS server, follow these steps:

1. In the vWLAN GUI, navigate to the **Administration** tab and select **AP Traffic Capture**.
2. Select the AP to which the wireless clients are connecting from the drop-down menu. Select **Wired** from the **Capture Type** drop-down menu. Leave all other fields at the default value and select **Start Capture**. Optionally specify the port and IP address of the RADIUS server to streamline the capture.



Attention: A Wireless traffic capture will put the AP into sensor mode and then return to AP mode when the capture is completed (or stopped by user).

The list of captured files will update every 3 seconds.

AP: 00:93:f1:21:a0:00
Capture Type: Wired
Interface: BG(2.4Ghz)
802.11b/g/n (2.4GHz) SSID: vGuest
Protocol: Any
IP Address:
MAC Address:
Maximum Packet Size: 1500
The default value of maximum packet size is 1500. Range: 0~1500.
Number of Packets: 10000
The default number of packets to capture is 10000. Range: 0~1000000000000.

Figure 27. Capturing RADIUS Traffic

3. After selecting **Start Capture**, select **Stop** to stop the capture. After stopping the traffic capture, the file name becomes a hyperlink. Select the link to download the file to your desktop where you can open and analyze the file.

Capturing EAPOL Traffic Between an AP and a Client

To capture EAPOL traffic between an AP and a client, repeat the steps in the previous section. In this configuration, however, filter the traffic by the wired interface of the AP by selecting the appropriate wireless interface from the **Interface** drop-down menu in the traffic capture configuration menu. Select either **BG (2.4 GHz)** or **A (5 GHz)**, and also specify an SSID in the **SSID** drop-down menu before beginning the traffic capture.