Ruckus
Simply Better Wireless.

Tech Note

Configuring

NPS

WITH ACTIVE DIRECTORY

Table of Contents

Copyright Notice and Proprietary Information

Intended Audience

This document provides an overview of how to configure a Microsoft NPS RADIUS server for 802.1X authentication against Active Directory. Step-by-step procedures for installation, configuration and testing are demonstrated. Some knowledge of RADIUS and 802.1X is recommended.

Overview

This document describes how to install and configure a Microsoft NPS RADIUS server for 802.1X authentication. The document is broken into the following main categories:

1. Introduction and key concepts
2. Install NPS
3. Configure NPS
4. Configure ZoneDirector

What Is Covered Here

This document is not an exhaustive description of all possible solutions. It focuses on NPS and how it can be configured as a front-end server for 802.1X clients.

Requirements for this Document

In order to successfully follow the steps in this document, the following equipment (at a minimum) is required and assumed:

- Windows 2008 Server
- NPS
- Ruckus ZoneDirector and AP

[1] This document uses Microsoft Server 2008 R2.

Introduction & Key Concepts

What is 802.1X?

802.1X is an IEEE security standard for network access. Authentication is a key part of the 802.1X standard. Three devices participate in every 802.1X authentication:

Supplicant – the client device

Authenticator – the device that controls network access (port) and passes authentication messages to the authentication server

Authentication Server – AAA-compliant authentication server

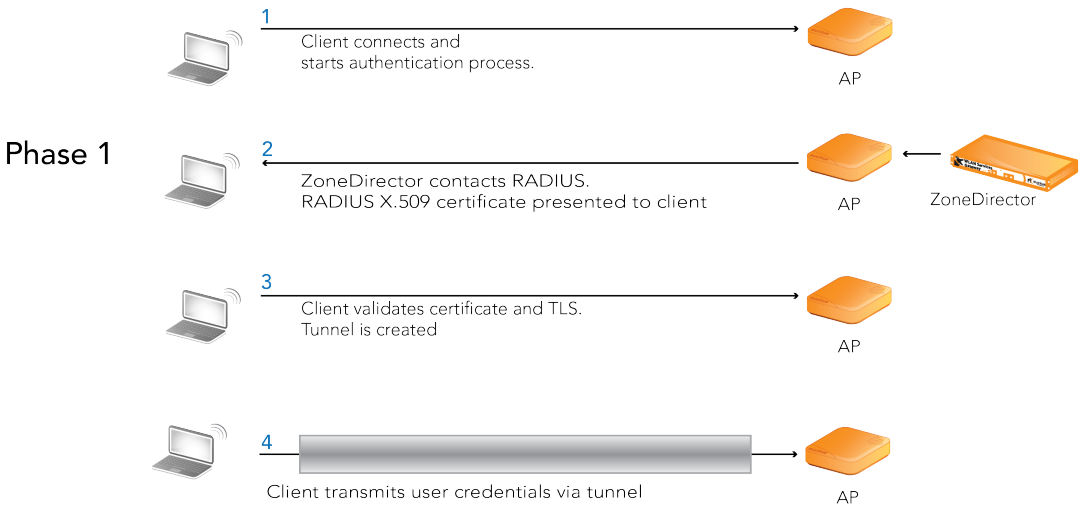


Figure 1 - 802.1X Authentication Phase 1

The supplicant responds to an authentication challenge from the authenticator and transmits its credentials. The goal of the first phase is to establish the protected tunnel (TLS) to encrypt the user credentials so they aren't sent in the clear.

Phase 2

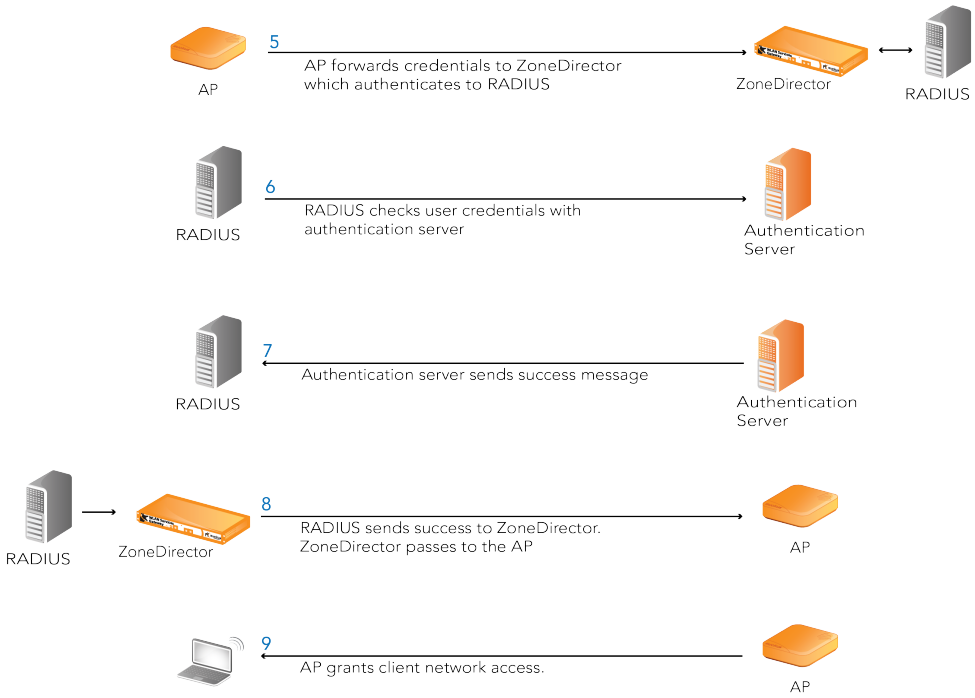


Figure 2 - 802.1X Authentication Phase 2

Once the user credentials are transmitted, the authenticator (AP) sends this information to the ZoneDirector. The ZoneDirector then submits it to the AAA server. If the authentication is successful, the authentication server notifies the authenticator, which opens the network port.

These stringent requirements create very secure network access – other than authentication attempts, no traffic of any kind will be allowed onto the network - including DHCP and DNS.

Why would I want to use 802.1X?

802.1X is a very secure authentication and encryption standard. Unlike pre-shared key (PSK) networks, it requires a user name and password that is checked against an authentication server for every authentication. PSKs rely on a single, shared secret for all machines. 802.1X is also well suited for single sign-on, in which 802.1X authentication occurs at the same time a user signs on to a computer.

Are there any alternatives to 802.1X?

802.1X is the most secure authentication method available. However the next best secure is Dynamic-PSK from Ruckus. This combines the simplicity of a PSK network with the

strength of unique keys that are assigned to individual devices. These keys are bound to a single device and cannot be shared. They may also have expiration dates and can be permanently revoked by an administrator.

Can I skip RADIUS and just use Active Directory directly instead?

No. You can use AD as your authentication database indirectly, but an additional step is required; namely, the installation of a RADIUS server as a front-end for AD.

The only authentication servers that an 802.1X-standards based infrastructure will recognize **must** be compliant with the IETF Authentication, Authorization and Accounting (AAA) standard. No other authentication servers are supported by the 802.1X standard. Microsoft's Active Directory (based on LDAP) is a popular example of a non-AAA-compliant authentication server.

The AAA standard is based on the Remote Authentication Dial-in User Service (RADIUS) protocol and is often considered interchangeable. AAA functionality is described in several IETF RFCs. Many standards requiring authentication have been written to use a AAA-compliant server. RADIUS is the most popular implementation of the AAA specification.

There are many flavors of RADIUS available today, each with slightly different optional features. Microsoft's RADIUS implementation on Windows Server 2008 R2 is called Network Policy Server (NPS).

This document is a quick, step-by-step guide to setting up 802.1X-based authentication with Active Directory and a Windows Server 2008 RADIUS system (NPS).

For more information about details not covered by this document or to just learn more about 802.1X authentication and RADIUS in general, please refer to Appendix A: Further Reading

How hard is it to setup RADIUS?

Although not trivial, setting up a RADIUS server is not that difficult either. It mainly requires planning and a careful understanding of how the different pieces (supplicant, authenticator, authentication server) interact with each other. Or you need to be really, really good at reading troubleshooting logs.

The RADIUS Mantra for Success

Follow these guidelines and you will be much happier and successful with RADIUS:

- Use certificates issued by a well-known root Certificate Authority to your server's exact hostname

[1] RADIUS RFC 2039 and 2865 (current implementation)

- If you are new Windows Server 2008 or RADIUS – start off with a virtual machine installation (VMware, Parallels, VirtualBox) instead of a live box – it's much easier to recover from mistakes
- Take snapshots of your virtual machine early and often for easy recovery if something goes wrong
- Test every change you make before proceeding to the next step (hint: this is a good time for those snapshots!)
- Turn the firewall off until you're sure everything is working
- Make sure DNS is working correctly
- Follow this guide step by step – if you can use the same operating system, do so
- If at first you don't succeed, try rebooting - ☺
- If something goes wrong, don't panic – try the troubleshooting hints and technical resources here first. Try starting over from a known good point. If those don't help, seek help from knowledgeable folks on the Microsoft forums. Be polite and give details of your situation (debug files, configuration) and they will help you
- Use certificates issued by a well-known root Certificate Authority to your server's *exact* hostname

Installation & Configuration Overview

The following is an outline of the overall procedure and steps described by this document:

1. Determine the required authentication protocols
5. Generate an X.509 SSL certificate for NPS
6. Install NPS and related components on a Windows 2008 Server
7. Define NAS clients
8. Configure your first set of connection and access policies
9. Configure the supplicant
10. Test
11. Troubleshooting

Authentication Protocols

Part of the authentication process is exchanging credentials between the supplicant and the AAA server. The IEEE 802.1X standard has quite a few EAP (Extensible Authentication Protocol) methods that can be used for this purpose. There are several types from which to choose. Each has its own advantages and disadvantages. Some are relatively simple to configure while others are not. The most important step is to determine which one provides you with the right balance between client support, security and complexity.

For more information on EAPs, please see Appendix A: Further Reading. This examples in this document use PEAP with MS-CHAPv2 and EAP-TLS. PEAP is by far the most popular EAP method today and is supported by virtually all supplicants. EAP-TLS, which is based on client certificates for mutual authentication, is much more secure.

How hard is it to do this?

Although not trivial, setting up a RADIUS server is not that difficult either. It mainly requires a careful understanding of how the different pieces (supplicant, authenticator, authentication server) interact with each other. Or you need to be really, really good at reading troubleshooting logs.

Can I skip any of these steps?

Sure. Use an authentication method other than 802.1X like Dynamic PSK. This will provide many similar benefits, but not all.

· It is desirable is get a server certificate from a well-known root Certificate Authority (CA) – preferably an unchained CA. However if this is not practical, a self-signed certificate can be generated as part of installing NPS.

· For more information on Dynamic PSK, please refer to the Ruckus ZoneDirector User Guide.

Generate an X.509 Certificate for NPS

Why do I need SSL? Can I just skip this step?

Unfortunately, no. The Protected-EAP (PEAP) protocol uses to transmit user credentials. This means user names and passwords are sent in the clear. Therefore, to protect this sensitive information it must be encrypted before sent over the air. The "Protected" part of PEAP refers to establishing an SSL/TLS-encrypted tunnel between the supplicant and the authenticator that is used to safely and secure exchange credentials.

Creating an SSL-encrypted tunnel is similar to what happens when you go to a secure web site to buy something. Before you send your credit card information, the server will encrypt it. You can see this happen in the browser when the URL starts with "https://" . Encryption is performed when the web server sends a digital certificate (X.509) to your browser that proves it is the right server and not an imposter. From there the two machines will negotiate the TLS tunnel.

How do I create an SSL certificate?

Do not install NPS until you have completed this step!

A certificate for the Windows NPS server is generated with these simple steps:

1. Do not start to install NPS until you have done this step!
2. Generate a Certificate Signing Request (CSR) on the NPS server
3. Submit the CSR to a public Certificate Authority (CA)
4. Install the certificate sent to you by the CA (usually takes 24-48 hours)
5. Now begin installing NPS

Real certificates cost money and I don't want to buy one

You don't *have* to purchase a certificate for your RADIUS server. There are free alternatives such as building your own private CA.

A private CA functions exactly like a public CA – it can issue a certificate for the RADIUS server as well as other servers, client machines and users. The advantage of a private CA is primarily cost – it's free.

---

[1] If you ever get an error from the browser that it doesn't trust a certificate, find out why. Errors can be anything from the hostname not matching what's in the certificate, an unknown issuing CA, to an expired or even revoked certificate.

The downside is that setting up a private CA to work correctly takes time and skill. It will take longer to setup a private CA versus letting a public CA do the work for you. Another disadvantage is private CAs typically require the installation of the private CA's certificate on every client. This can be time consuming and possibly result in errors and failed authentication.

A second alternative is a self-signed certificate. A set of self-signed certificates can be created with the optional Certificate Services module for Windows Server.

The disadvantage of self-signed certificates is that they too will require some client-side configuration.

For more information on creating your own CA, please refer to the Ruckus Tech Note: *Creating Private PKIs with Windows Server*.

But I don't want to install private certificates on my clients either!

There are several ways to distribute client certificates from a private CA in a Windows domain: group policies, auto enrollment, email, etc. But if none of these are feasible, there are two options:

- Configure each client device so it will not attempt to validate the RADIUS server's certificate. This is a security flaw, but it will work. The downside to this is you still have to touch every client.
- Use an automated method such as auto-enrollment (available for Windows domain machines only)

On the other hand, if the certificate for RADIUS was issued from a well-known public CA (such as VeriSign) this step is not required. All web browsers come pre-installed with the root certificates for all well-known CAs. This is the largest advantage of using a public CA instead of a private CA or self-signed certificate. The time consumed in these free alternatives could easily outstrip the $60 or so that a public CA would charge for a certificate.

What if I turn off client-side certificate validation? Do I still need a server certificate if it's being ignored?

Nice try. But yes you do. The certificate is necessary. Turning off validating means the client just won't try to determine if it is genuine or not. Without the server's certificate you can't use SSL (the "P" in PEAP or TLS in EAP-TLS). No server certificate and no encrypted tunnel means no secure credential transmission. And that means all authentication attempts will fail and 802.1X not work.

Do I really need to do this? Be honest now

Yes, You really, really, really **must** do this. You can go with any of the options above, but you **must** have an SSL certificate installed on the RADIUS server. Otherwise 802.1X will fail.

You do not have the option of installing RADIUS without a certificate of some kind (self-signed or otherwise). The installation itself will require it, which is why it is discussed first before even beginning to describe the NP software installation.

Caveats and Common Mistakes

All CAs are not created equal!

When a client validates a server certificate it checks the digital signature on that certificate and matches it with the public CA's certificate. The CA's certificate must already be installed on the client. If the name on the certificate and the hostname match, the server's certificate is considered valid and trusted. If the names do not match or the client does not have the complete CA certificate chain[1], it will reject the certificate as not valid/untrusted. This will typically stop (fail) the authentication process.

To avoid installing additional CA certificates on clients, it is best to obtain a certificate for your RADIUS server directly from a root (unchained) CA that is well known and already installed in the client browser or certificate repository. This is the simplest process by far and less prone to errors.

CSR Fields

If you decide to generate a CSR to request a certificate for your server, you must fill out all mandatory fields. The common or subject name should be the fully qualified DNS name for your server. If asked what kind of application this certificate is for, it is safe to use "generic server" or "web server". If your server might have two different names it resolves to, enter the second value in the *Alternative Subject Name* field of the CSR.

[1] Certificate Authorities can not only grant certificates to servers, clients and users, they can also give special certificates to intermediate CAs which can also issues intermediate CA certificates. An intermediate CA can sign server certificates, just like the original root CA. However, in order for a client to validate a server's certificate it must have all of the intermediate CA public certificates back to and including the root CA. (CA chain)

Installing NPS

If you are planning to use an SSL certificate that is not self-signed, make sure it is installed on the server before continuing to the rest of this section. If you are planning to generate a self-signed certificate you will be given a chance to do this as part of the NPS installation.

Installation steps:

1. Install Windows Server 2008 R2
    6. Join Windows server to the domain
    7. Install production SSL certificate
    8. Install the NPS role
    9. Register NPS in Active Directory
    10. Configure and test ZoneDirector as a NAS client
    11. Configure the NPS connection policies
    12. Configure client supplicant and test
    13. Troubleshooting

Install Windows Server 2008 R2

Installation of Windows Server is beyond the scope of this document. Please refer to the documentation from Microsoft for details. Requirements for this document are as follows:

- Windows Server 2008
- The server is a member of the domain.[1]

Install X.509 Certificate

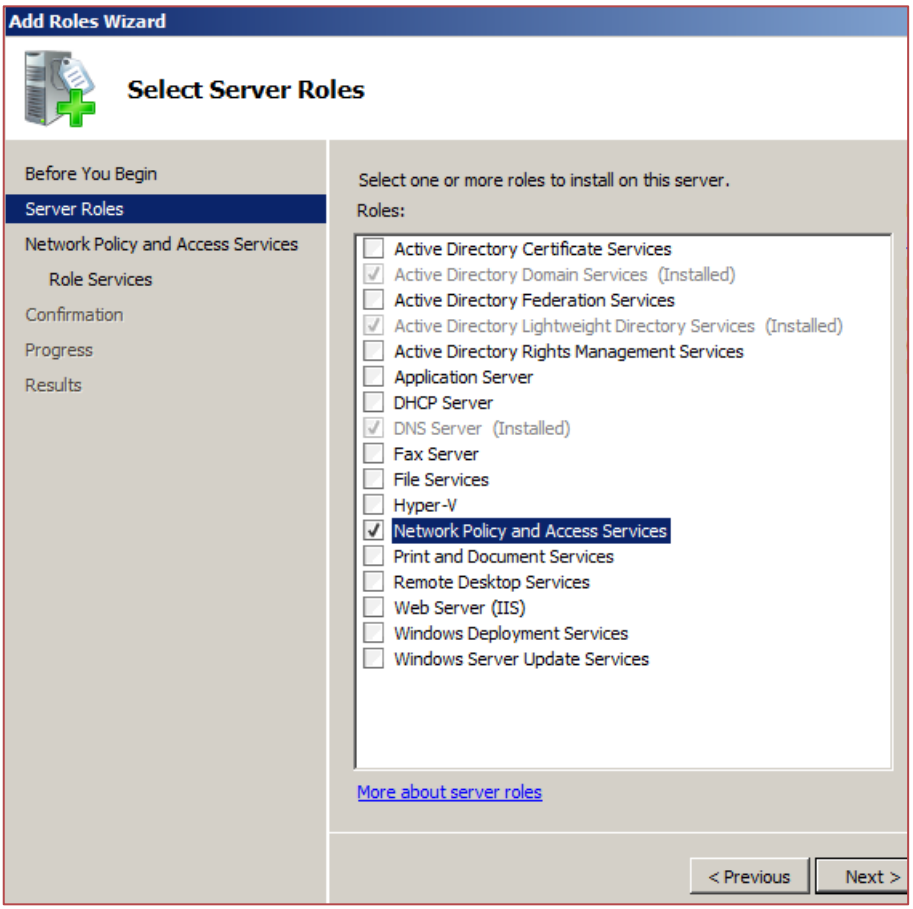
If you haven't already done so, install the digital certificate that will be used by NPS to authenticate itself to clients. Simply double-clicking the certificate typically does this. Windows will automatically install it into its repository. If using a certificate from a CA that is not already known (doesn't show up in the repository under trusted CAs) installs its public root certificate as well.

Install NPS

Now we'll install NPS itself.

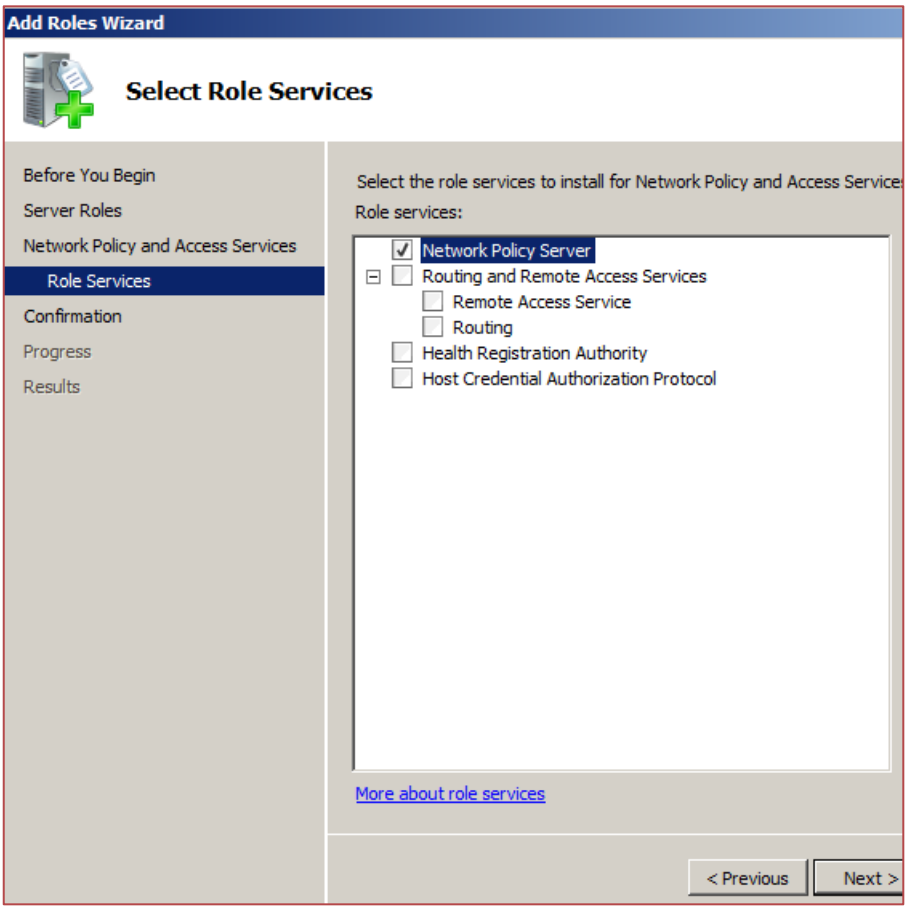
1. Launch the Server Manager application and make sure you are on the main, root-level screen
    14. Under Role Summary, click Add Roles
    15. Select Network Policy and Access Services from the available roles
    16. Under Role Services, select Network Policy Server

[1] NPS may be run on any version of Windows 2008 server including domain controllers although that is not considered best practice.



17. The minimum role services required for NPS is the Network Policy Server itself. Nothing else is required for basic RADIUS features.

· If you're feeling frisky and want to try Microsoft's version of NAC – called NAP – you'll be able to do so after this installation.

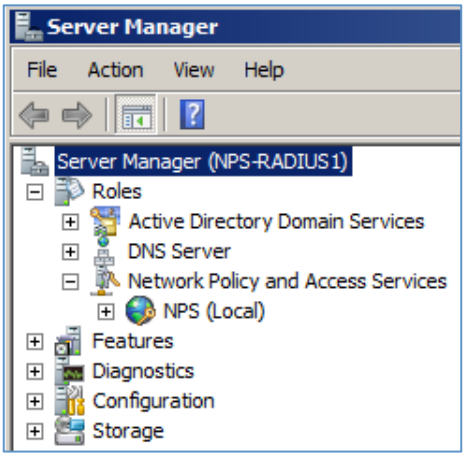


18. Depending on the options already installed, you may be asked to install additional software such as IIS
19. At the end, you will be presented with a summary screen listing the installation and configuration options. Check this screen carefully before clicking the Install button.

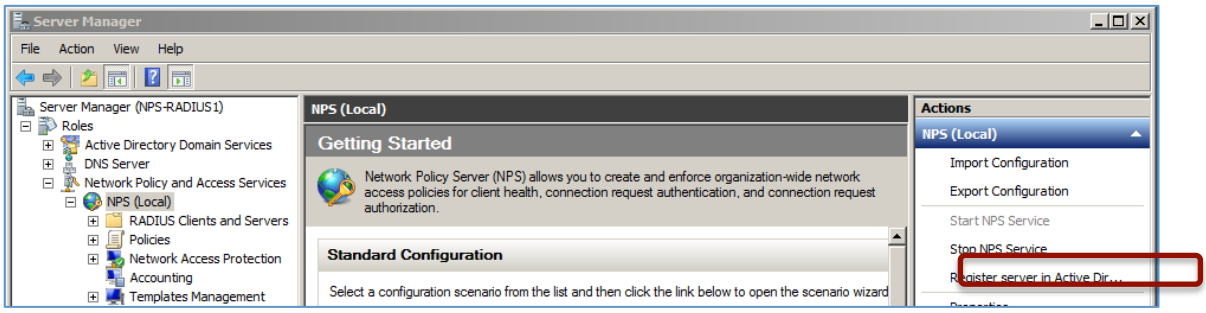
Register NPS in Active Directory

In order to perform authentication, we need to give the NPS server permission to lookup user names in Active Directory. We'll do this from the Server Manager:

1. Launch the Server Manager application and make sure you are on the main, root-level screen
    20. In the left-hand navigation window, click Roles
    21. Click Network Policy and Access Services from the available roles
    22. Click on the local NPS instance
    23. Under Roles, select Network Policy Server



24. Find the Actions window on the right side of the screen and click Register server in Active Directory



25. Click OK when prompted to proceed with the authorization

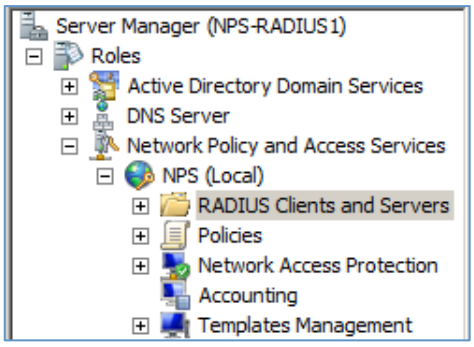
NPS is now installed and permitted to interact with Active Directory. The next step is to tell NPS which devices are allowed to use it to authenticate users.

Configure RADIUS (NAS) Clients

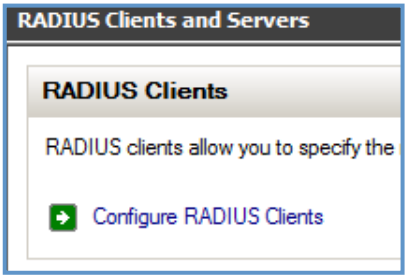
The first step to configure NPS is to define the RADIUS clients. A RADIUS client is a device that is allowed to communicate with the RADIUS (NPS) server. In 802.1X terminology, this is the *authenticator*. This is normally a ZoneDirector or a standalone AP.

Installation steps:

1. Launch the Server Manager application
   26. In the Navigation pane on the left, navigate down to the local NPS instance and select RADIUS Clients and Servers

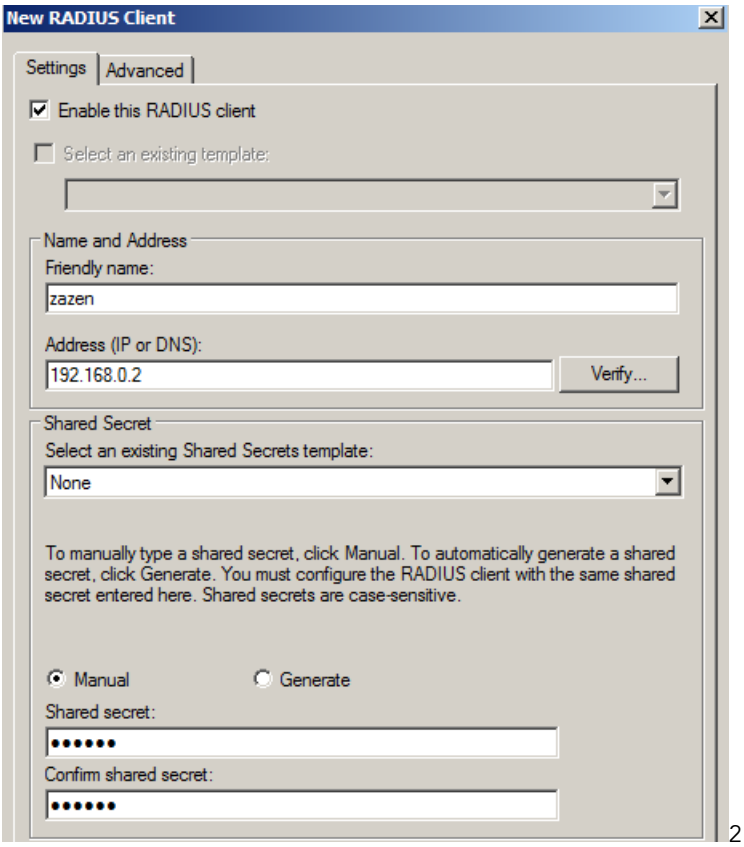


   27. Click Configure RADIUS Clients in the main window (to the right of navigation) or right-click on RADIUS Clients



   28. Click New
   29. Enter the information for your authenticator (ZoneDirector or AP) in the dialogue box. At a minimum you will need:

       - A friendly name – usually the hostname or FQDN
       - The IP address or DNS entry for the authenticator
       - A shared secret – the password the authenticator uses to prove it is allowed to communicate with NPS



2

30. Click OK when done to create the RADIUS client

Continue this process until all NAS clients have been created (if you have more than one).

Now it's time to configure policies to control what devices may connect to NPS and how to authenticate users.

Configuring NPS Policies

NPS policies determine how devices and users may connect and gain network access. There are several different types of policies:

- **Connection Request policies** - Describe who/what/how a NAS client may connect
- **Network policies** - Sets conditions and requirements for wireless devices and/or users before network access is granted
- **Health policies** - Determines whether/how a client passes health check

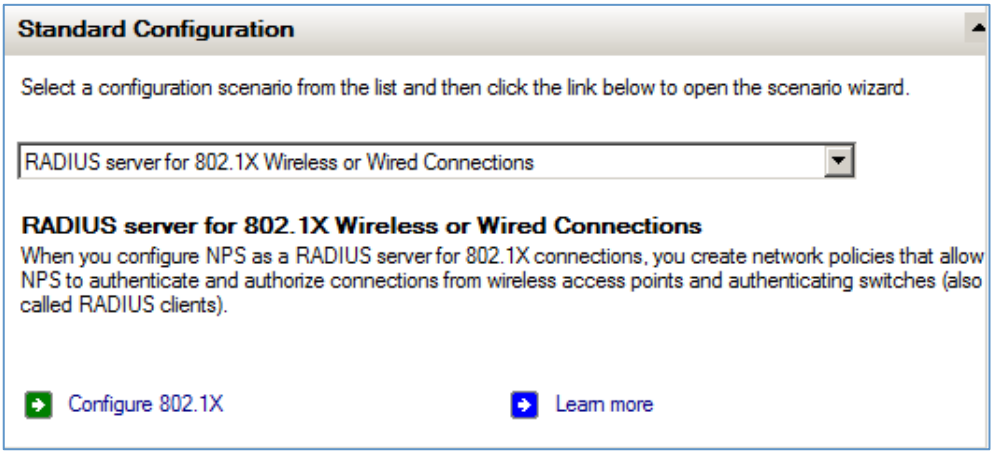
All polices are fail-through, i.e. if a client fails the first policy, it tries the next and so on until all policies have been tried. The first match wins, even if there are other policies that could match. **Make sure your policies are placed in the correct order!**

To setup an 802.1X configuration, only the first two types of polices are necessary. At least one Connection Request policy and one Network policy must be configured. The Health policies are optional and only required if you are performing NAP/health checks[1].

Fortunately, NPS has a policy wizard, which can speed up the process of policy creation.

Configuration steps:

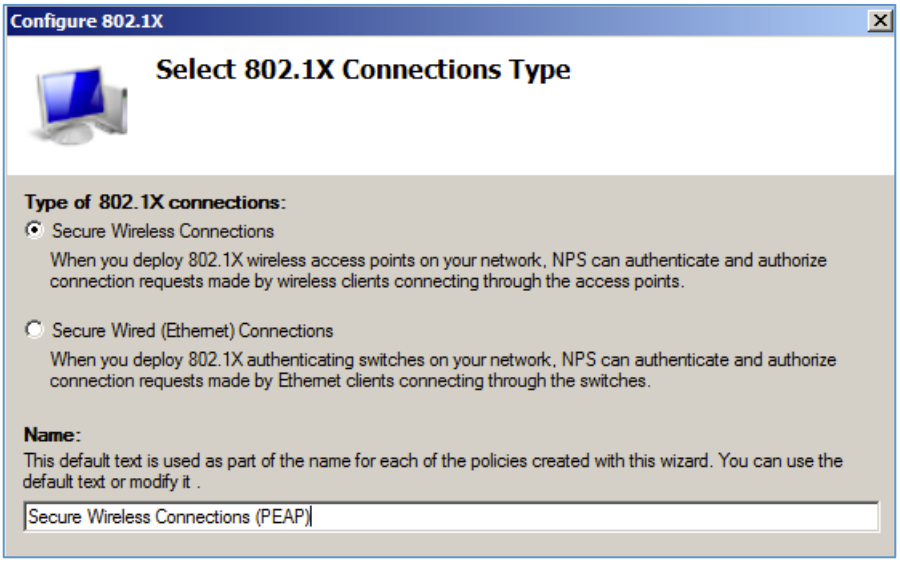
1. Launch the Server Manager application
   31. In the Navigation pane on the left, navigate down to the local NPS instance and click on it



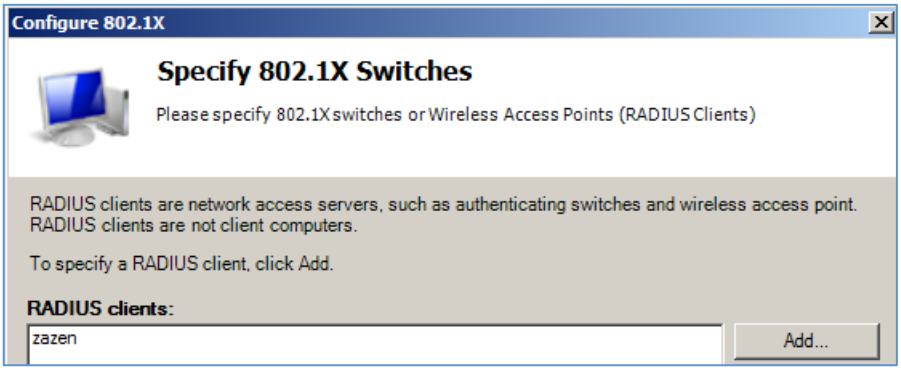
   32. Under Standard Configuration (the middle screen), select RADIUS server for 802.1X Wireless or Wired Connections from the drop-down box
   33. Click Configure 802.1X

[1] Network Access Policy (NAP) configuration is out of the scope of this document. For more information please refer to Microsoft's documentation.

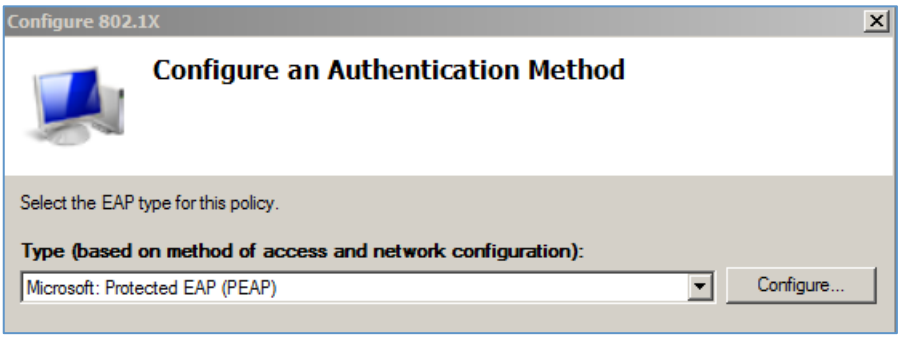
34. Click Secure Wireless Connections for the connection type. You may change the default policy name here



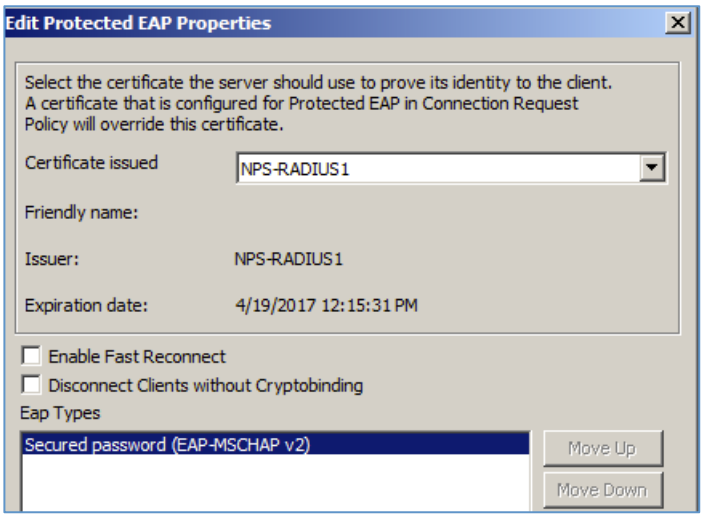
35. Click Next
36. Select your previously created RADIUS client(s). You may also add clients from here



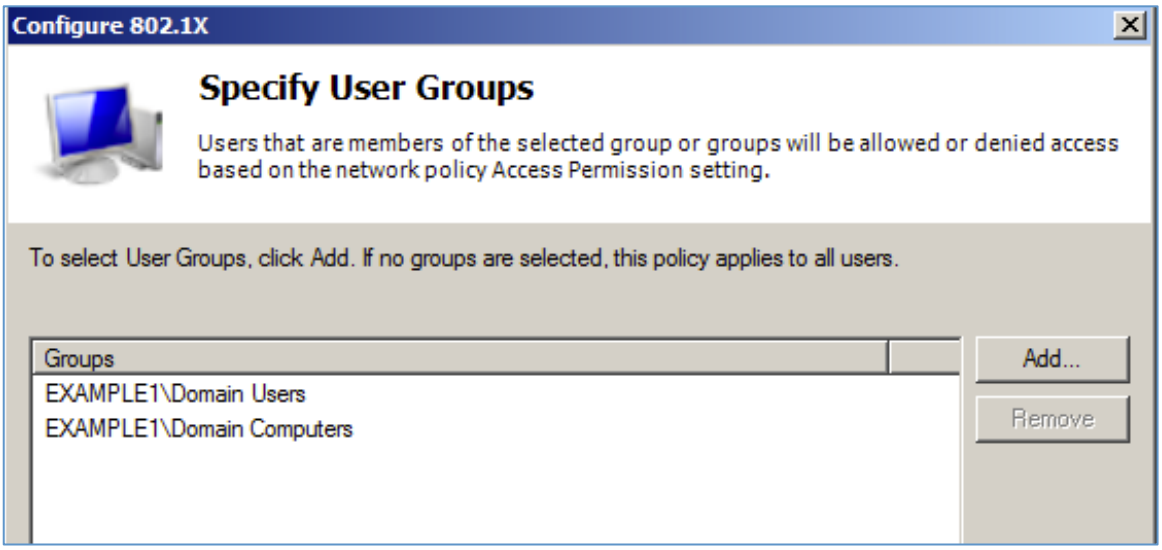
37. Click Next
38. When prompted for the EAP type, choose Microsoft: Protected EAP (PEAP) from the drop-down box



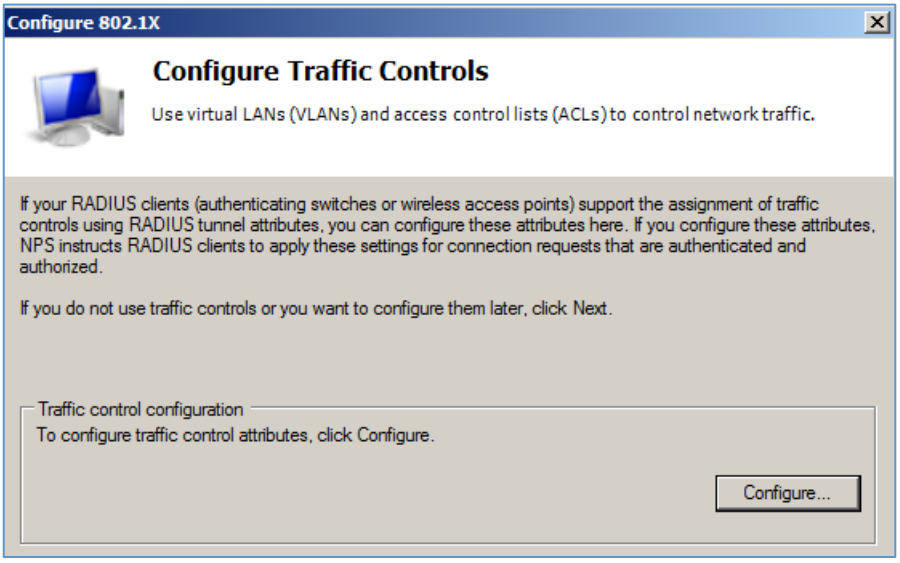
39. Click the Configure button and make sure you have the right certificate installed for RADIUS in the Certificate Issued box. If you have more than one certificate for this server installed, choose it from the drop-down box



40. If the server certificate it is missing, you can add it here
41. In the next screen, you can choose conditions that control who gets network access. These conditions can apply to groups of domain computers or users.
42. Click the Next button twice to get to the User Groups window. This dialogue allows you to restrict wireless access. Only a user or device that is a member of one of the specified Windows security groups (not local groups) will be granted access. All others are denied. If you do not enter anything all users and computers with valid AD credentials will be granted access. Note: a client only needs to be a member of one group in this list. Adding more groups does not require it to be a member of all of the groups.



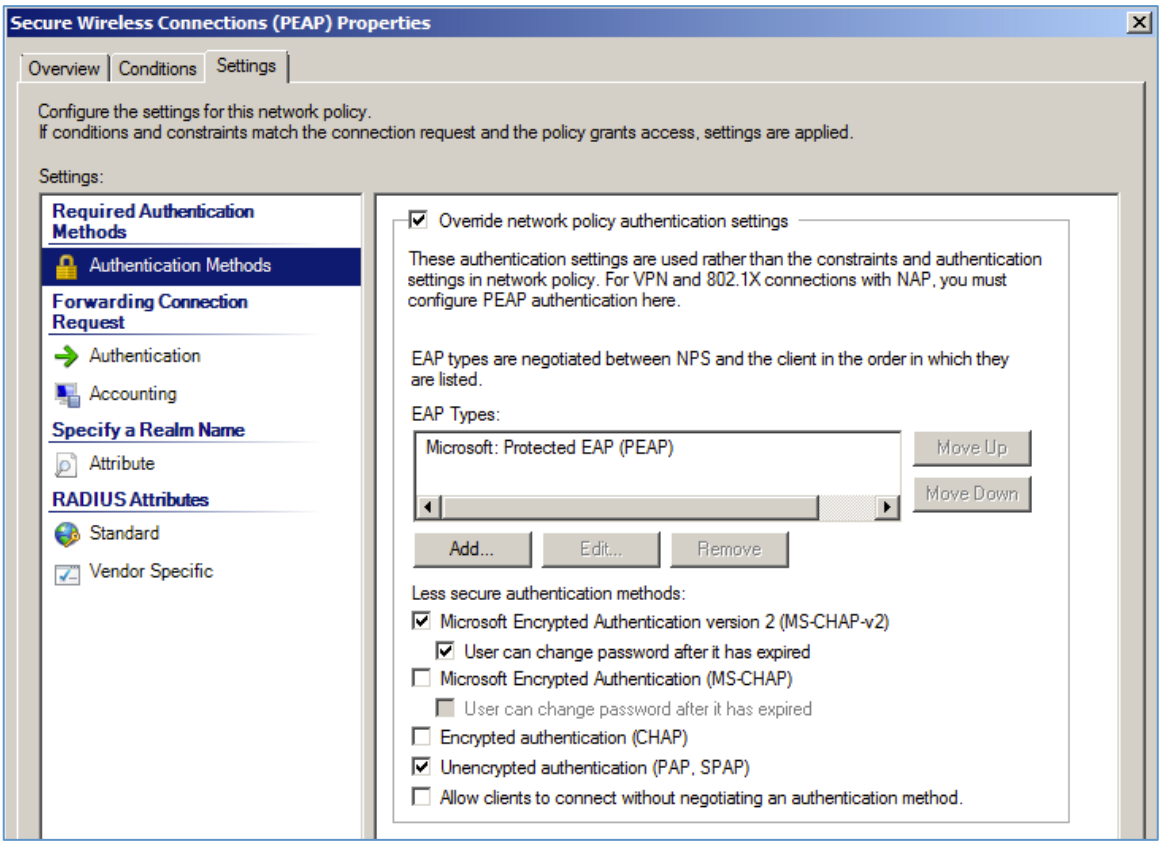
12. Click Next
13. The next dialogue allows you to configure traffic controls. This includes configuring Dynamic VLANs. It is not required for basic RADIUS service[1].



14. Click Next
15. Review the NPS settings. If they are correct click Finish to end the wizard or go back and make any changes.
16. Click Next
17. Click Finish to close the wizard and save your policies
18. Next double-click to re-open the connection request policy for one additional edit

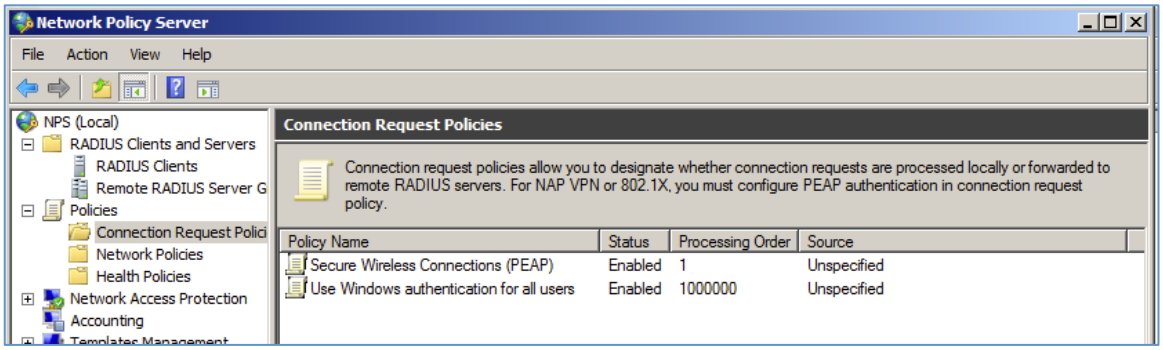
[1] For more information on Dynamic VLAN configuration please see the Ruckus application note, Ruckus Wireless ZoneFlex user guide or Microsoft's documentation.

19. Click the Settings tab



20. Select the box at the top labeled Override network policy authentication settings
21. Click the Add button
22. Choose Microsoft: Protected EAP (PEAP) from the list
23. Click OK
24. Select the box marked Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
25. If you want to test the AAA server connection on the ZoneDirector you must also select either PAP or CHAP as well
26. Click the OK button to save the changes

By default, the wizard creates two policies: a Connection Request Policy and a Network Policy. The next step is to review these policies and make sure they are listed in the correct order. To view the policies, navigate to them using the left-hand navigation window. Each policy has the same name "Secure Wireless Connections (PEAP)" below: one is located under Connection Request Policies and the other is under Network Policies. It's a good idea to move these policies to first place in processing order. This makes sure any RADIUS authentication requests will always use the Wi-Fi policies first. If another policy is processed before wireless, it can potentially prevent users from connecting to the WLAN.



NPS should now be available for wireless authentication. The next step is to configure the ZoneDirector as a NAS client and make sure it can communicate with the RADIUS server.

Configuring NPS for User Roles

User roles are defined on the ZoneDirector and are used to determine what privileges and WLAN access are granted to members of a particular group. A list of all domain group membership is sent back to ZoneDirector as part of the authentication success message.

The default behavior for NPS does not send this information. If this information is required, NPS must be configured to do so.

Configuration steps:

1. Launch the Server Manager application
2. In the Navigation pane on the left, navigate down to the local NPS instance and click on it
3. Click on Network Policies
4. Click the Settings tab
5. Select Vendor Specific
6. Click Add
7. Click Custom
8. Click Vendor-specific
9. Click Add
10. Enter vendor code: 25053
11. Click Yes It Conforms
12. Click Configure Attribute
13. Set Vendor-assigned attribute number: 1
14. Set Attribute format to String

Attribute Value: Whatever you put in the Group Attribute field on the ZD role for that WLAN. Eg. above I gave example of 'STAFF' so my value here would be 'STAFF' without quotes.
Click 'OK' 'OK' 'APPLY' 'OK'

Restart NPS service by right clicking NPS in server manager.

You are done.

Configuring 802.1X on the ZoneDirector

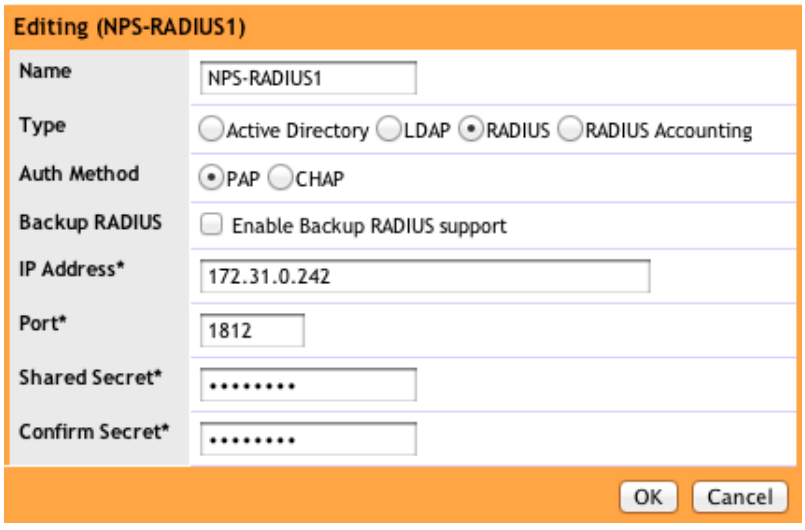
Before a ZoneDirector can use our RADIUS server for user authentication, it must be configured. This procedure consists of creating a AAA entry for the NPS server and an 802.1X-enabled SSID.

Create a AAA Entry on NPS

The first step is to create the AAA NAS client entry[1].

1. Log on to the ZoneDirector's web UI
27. Go to Configure->AAA Servers
28. Click Create New and enter the information for the RADIUS server. Required information includes:

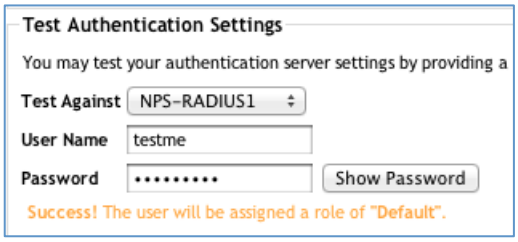
- Server name
- Type (RADIUS)
- IP Address of RADIUS server
- Port number (NPS uses 1812 by default)
- Shared Secret – the secret you entered previously on NPS for the ZoneDirector NAS Client entry



29. Click OK

[1] Why not create the SSID first? Because an 802.1X-enabled SSID requires a AAA server as part of its configuration. Chicken. Egg

If you allowed PAP or CHAP in your connection request policy on NPS, you may test communications with the NPS server now to make sure it works.[1] If you didn't set this up or are not sure how to do it, check out the instructions in Configuring NPS Policies.

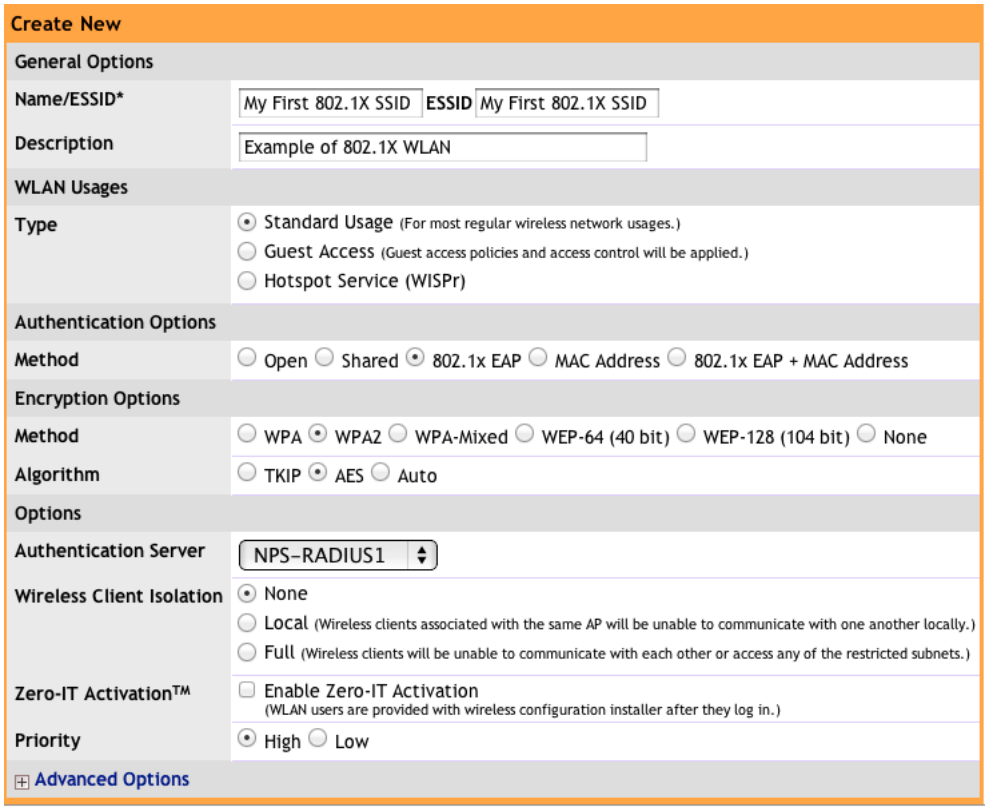


Create an 802.1X-enabled SSID

Next create the SSID.

1. Log on to the ZoneDirector's web UI
30. Go to Configure->WLANs
31. Click Create New and enter the appropriate information for your SSID name, encryption, etc.

[1] Enabling PAP or CHAP is a security risk as it is a very insecure protocol. However you can always go back to your connection request policy and enable it temporarily to do this test.



32. Click OK to save your changes.

That's it for the ZoneDirector. Now it's time to setup the client.

Don't I Need to Tell the ZoneDirector If I'm Using P-EAP or EAP-TLS?

No. The EAP negotiation and messaging is strictly between the supplicant (client) and the RADIUS server. No other device is involved. Active Directory doesn't even know 802.1X is being used at all. The EAP messages stop at the RADIUS server.

The Ruckus AP and ZoneDirector need to know some type of 802.1X will be used in the initially WLAN definition, but they are completely agnostic as to the type[·]. All the AP and ZoneDirector do are forward the messages to the RADIUS server. They do not alter them or change their actions in any way other than to allow or disallow access based on an Access-Accept or Access-Reject message from RADIUS. VLAN membership or WLAN access can also be specified via return attributes from RADIUS as well. For more information, please refer to the Ruckus Wireless application note: *Configuring Dynamic VLANs with RADIUS*.

[·] The exceptions to this are proprietary solutions such as Cisco LEAP or Aruba's xSec

Final Configuration – Setting Up the Client Supplicant

At this point the system should be ready for a client test of 802.1X over wireless. Details on setting up client supplicants are very different depending on the OS. For tips and instructions on how to configure a variety of clients, please refer to the Ruckus application note *Configuring 802.1X Wireless Supplicants* or the vendor's documentation.

Appendix A: Further Reading

802.1X

An Introduction to 802.1X for Wireless Local Area Networks

http://www.lucidlink.com/media/pdf_autogen/802_1X_for_Wireless_LAN.pdf

Digital Certificates and Certificate Authorities

Microsoft – Understanding Digital Certificates and Public Key Cryptography

http://technet.microsoft.com/en-us/library/bb123848(v=exchg.65).aspx

Installing a Certificate Server with Microsoft Windows Server 2008

Application note available from Ruckus Wireless

Microsoft Network Policy Server

Network Policy and Access Services

http://technet.microsoft.com/en-us/library/cc754521(WS.10).aspx

Tools & Troubleshooting

Decoding RADIUS with Wireshark

http://wiki.wireshark.org/Radius

RADIUS Attribute Types and Values

http://www.iana.org/assignments/radius-types/radius-types.xml

EAP Testing (eapol_test)

http://deployingradius.com/scripts/eapol_test/

Appendix B: Troubleshooting Tips

There are several components involved in 802.1X authentication. To troubleshoot, first isolate the problem component – or at least the first component failure in the process. Specific steps can be taken from there.

Determine Which Component Failed

It is often easiest to begin troubleshooting from the endpoint (client supplicant).

Troubleshooting the Supplicant

Certificates

The number one reason an 802.1X connection fails on the client is when there is a problem with the server certificate[1]. This is particularly true if a private CA or a self-signed certificate is used.

WLAN Configuration

Most clients are able to determine the correct authentication type on their own, but some may need manual configuration. It is important to make sure this is correct. For example, a client using WPA-TKIP will not be able to connect to a WLAN configured for WPA2-AES only.

Similarly, a client may not be able to negotiate a common authentication protocol with the RADIUS server. This is particularly true if the client can only do PEAP but the RADIUS server is configured to only support EAP-TLS.

OS Limitations

Most modern devices support 802.1X for PEAP and EAP-TLS. A notable exception is Windows XP. A common problem is being unable to select WPA2-Enterprise from the WLAN configuration box. These clients require a hotfix from Microsoft that adds support for 802.1X[2].

[1] This has been found to be the case at least 75% of the time when 802.1X fails. It cannot be stressed enough how important this component is for successful 802.1X deployment.

[2] Available from Microsoft - http://www.microsoft.com/en-us/download/details.aspx?id=1974.

Client Messages

Warning: The server "NPSServer (ServerC)" presented a valid certificate issued by "RootCA (ServerA)", but "RootCA (ServerA)" is not configured as a valid trust anchor for this profile. Further, the server "NPSServer (ServerC)" is not configured as a valid NPS server to connect to for this profile.

The client does not have the root CA certificate or that certificate has not been marked as valid or trusted.

Troubleshooting Certificates

FreeRADIUS

A problem with a certificate on the RADIUS side is usually easy to uncover: simply stop radiusd and start it manually in debug mode. If there is a problem with the certificates it will refuse to start. The messages should help you figure out which certificate is the problem.

The exception to this is if an EAP-TLS client presents an invalid certificate (expired, wrong hostname, etc.) or one signed by an unknown or untrusted CA. This will not stop the radiusd process. However messages indicating the problem will still show up if radiusd is run in debug mode.

Client

There are several reasons why a client may have a problem with a certificate. These include:

- RADIUS presented a certificate that is signed by an unknown/untrusted CA
- RADIUS presented a certificate that does not match its hostname
- The RADIUS certificate has expired
- The client does not have a valid certificate to present to the server for an EAP-TLS connection

Any of these problems will cause the client to (often silently) fail to connect. In the case of a Windows client, the system will show messages similar to "*Attempting to connect … Attempting to connect ... unable to connect*". It will repeat this cycle on and on.

The simplest way to test a server-side certificate problem is to disable server certificate validation. If the client is able to connect, the problem is definitely on the server side. One other thing to try is to connect with a different client (different OS) and see if it exhibits similar behavior.

Troubleshooting NAS Client to RADIUS Communications

The most common causes are:

- Shared secret is not the same on the NAS and RADIUS – try typing it again

- No IP connectivity – try pinging from one to the other
- Wrong RADIUS ports or a firewall is blocking the ports
- If the AAA test (from the ZoneDirector) doesn't work, make sure PAP/CHAP is enabled. This test only works with PAP or CHAP

Troubleshooting NPS

The easiest way to see what NPS is doing is with the Event Viewer.

1. Launch the program from Administrative Tools ->Event Viewer.
33. Click the plus (+) sign to open Custom Views
34. Click the plus sign to open Server Roles
35. Click to select Network Policy and Access Services
36. Events pertaining to NPS are listed here

Common Error Messages

Windows Clients

An error occurred during the Network Policy Server use of the Extensible Authentication Protocol (EAP). Check EAP log files for EAP errors.

This is often caused when the client cannot validate the server's certificate. The client will terminate the session, which generates this message.

NPS Server Event Log

Network Policy Server discarded the request for a user.
This is an audit failure. NPS could not log data to the accounting log file. If auditing is not enabled, turn it on. If sending audit data to a remote SQL server, try switching to a local file. Or enable the discard option.

NPS Server Log Files

NPS can save messages directly to a text log file as well. For information on how to parse this, see the Microsoft Tech Net page:

http://technet.microsoft.com/en-us/library/cc771748(v=ws.10).aspx

The domain controller certificate had expired.

This will prevent connections requiring PEAP. Re-issuing the domain controller certificate should allow RADIUS requests to authenticate normally.

Troubleshooting Domain Communications

NPS requires permission to communicate with AD for client authentications. To do so, it must be a member of the domain. Verify it is a domain member on the domain controller using the Active Directory Computers and Users tool.

Also, verify NPS is still registered with Active Directory.