Configuring 802.1X Authentication for Wi-Fi

(Windows Server 2008 NPS)

Application Note

Table of Contents

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

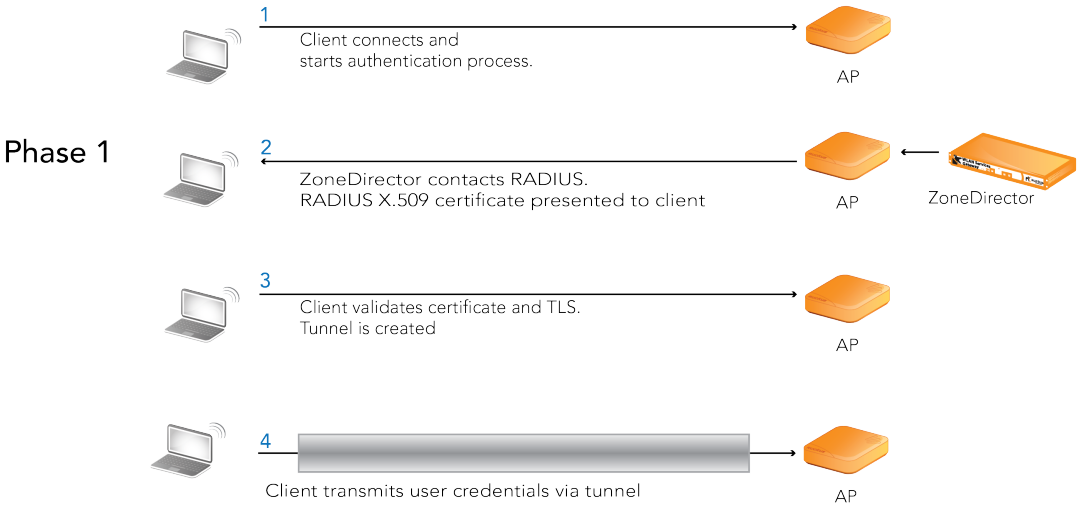


Figure 1 - 802.1X Authentication Phase 1

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

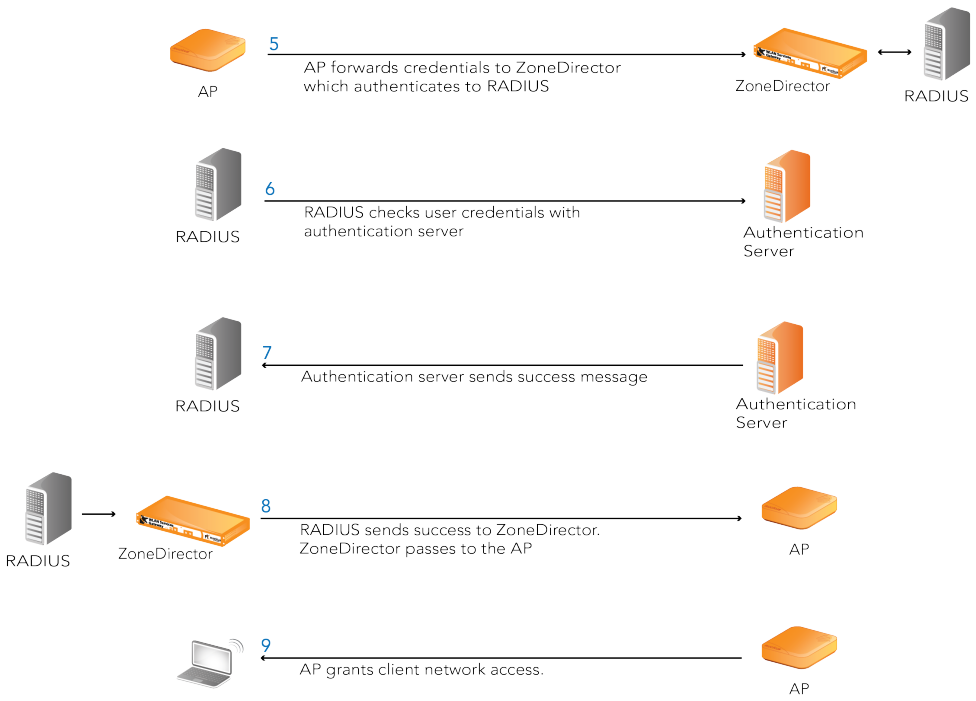


Figure 2 - 802.1X Authentication Phase 2

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, 802.1X 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.[1] Many standards that require 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 Microsoft 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 the recommended readings in Appendix A.

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

Installation & Configuration Overview

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

1. Determine authentication protocol
2. Generate an X.509 SSL certificate for NPS[2]
3. Install NPS and related components on a Windows 2008 Server
4. Define NAS clients
5. Configure your first set of connection and access policies
6. Configure the supplicant
7. Test
8. Troubleshooting

Authentication

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. This examples in this document use PEAP with MS-CHAPv2. This is by far the most popular EAP method today and is supported by virtually all supplicants.

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[3]. This will provide many similar benefits, but not all.

[2] 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.

[3] 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[4]. From there the two machines will negotiate the TLS tunnel.

How do I create an SSL certificate?

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 NPS server. There are free alternatives.

You can either build you own private CA or you can create a self-signed certificate at the time of NPS installation; in that case NPS is its own CA. These are workable alternative that only cost the time it takes to install a Certificate Authority, configure it, use it to issue certificates and make sure the root CA certificate is installed on all clients.

These steps have the advantage of being free but they usually end up being a very expensive free service. There are several reasons:

[4] 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.

Build Your Own Certificate Authority

Setting up a real private CA that works well takes some time and skill. It's not complex if you understand some basic concepts. Microsoft Server has an optional certificate authority server role that can be installed from the Server Manager program[5].

When you have finished configuring this, you will have a Microsoft-based server with a simple web interface for submitting CSRs an downloading certificates. These certificates must include the CA's own public certificate so clients know they are talking to the right server. A client supplicant should never accept a certificate that doesn't came from a machine that can establish some level of trust.

Distribute Your CA Root Certificates

Your NPS server was the very first machine to get its own certificate installed. Next we need to get the CA's root certificate installed on any potential supplicant (client).

Self-Signed Certificates

Another option for the impatient is allowing the NPS server to generate its own certificate. This is functionally the same as a private CA. NPS runs its own CA service and automatically creates a certificate for itself. It's quicker than setting up a formal CA if all you want is a certificate for the RAIDUS server and nothing else. Other than that, it is subject to all of the restrictions mentioned above for private CAs.

During the initial 4-way handshake, the authentication server must present a certificate to the client. The only way the client can validate the certificate is if it has the corresponding CA's root certificate already installed and trusted.

Once your private CA is setup, the next step is to distribute its root certificate to all clients. This can be done by allowing clients to download the certificate from a link, during the imaging process, or pushed down to the machine by Windows group policies.

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

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

[5] For more information on how to set up a Microsoft CA, please refer to the appropriate Ruckus application note

Configure each client device so it will not attempt to validate NPS' certificate. This is a security flaw, but it will work. The downside to this is you still have to touch every client.

On the other hand, if the certificate for NPS was issued from a well-known public CA (such as VeriSign) this step would not be required. That's because 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). No server certificate, 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 Windows server running NPS. Otherwise 802.1X will fail.

You do not have the option of installing NPS without a certificate. The NPS installation itself will require it which is why discuss it first before even beginning to describe the NPS 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 previously installed on the client. If the certificate match and the hostname is correct, the server's certificate is considered valid and trusted. If the certificates do not match or the client does not have the complete CA certificate chain[6], it will reject the certificate as not valid/untrusted. This will typically stop (fail) the authentication process.

[6] 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)

To avoid installing additional CA certificates on clients, it is best to obtain a certificate for your NPS 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.

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
2. Generate SSL certificate
3. Install the NPS role

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[7]
- ✓ The server is a member of the domain.[8]

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.

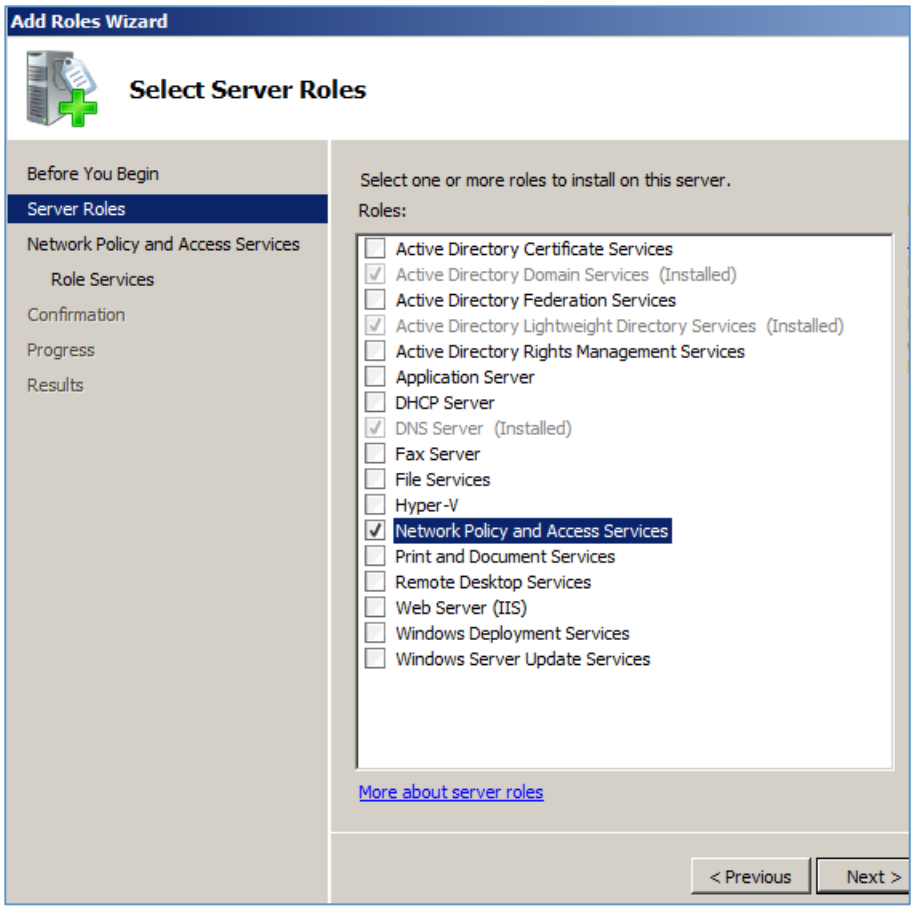
Install NPS

Now we'll install NPS itself.

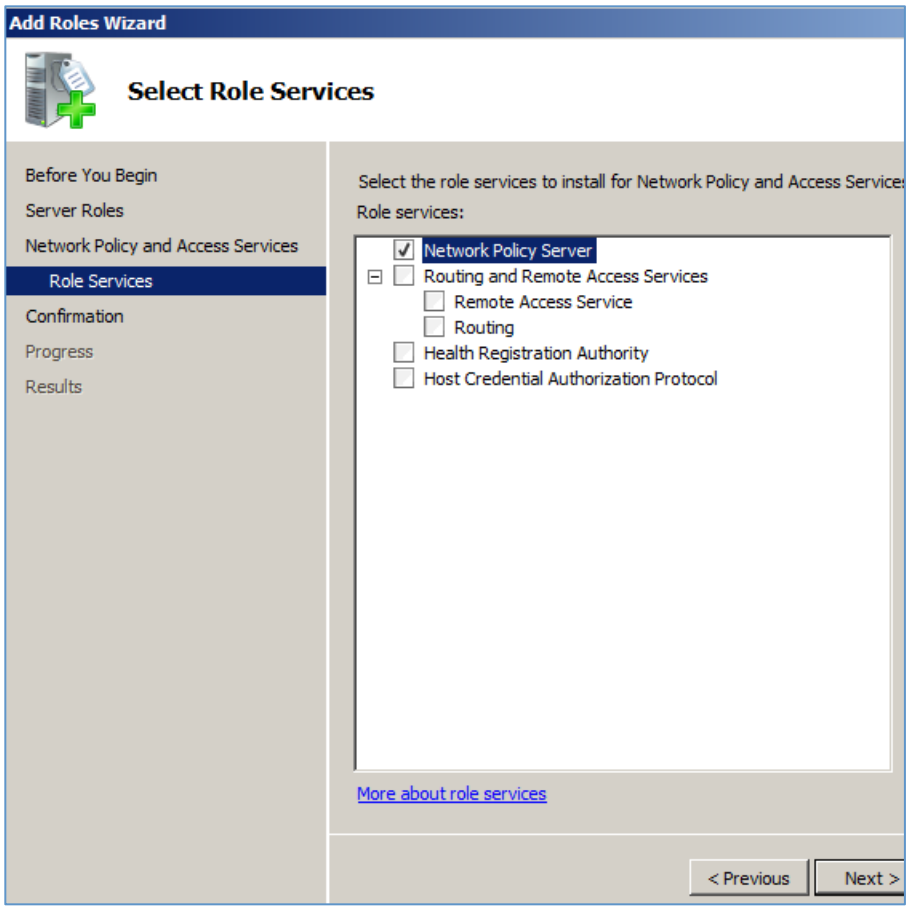
6. Launch the Server Manager application and make sure you are on the main, root-level screen
7. Under Role Summary, click Add Roles
8. Select Network Policy and Access Services from the available roles
9. Under Role Services, select Network Policy Server[9]

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

[9] 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.



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

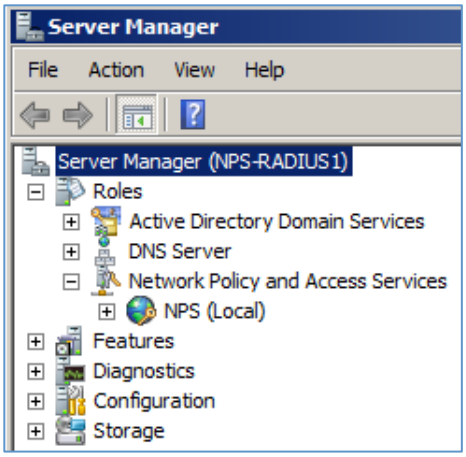


11. Depending on the options you install previously, you may be asked to install additional software such as IIS
12. At the end, you will be presented with a summary screen listing the installation and configuration options. Check this screen carefully before clicking the Install button.

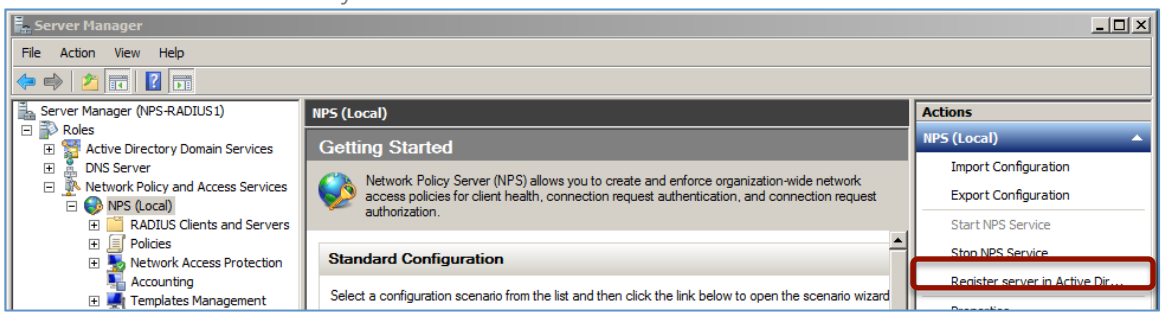
Register NPS in Active Directory

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
2. In the left-hand navigation window, click Roles
3. Click Network Policy and Access Services from the available roles
4. Click on the local NPS instance
5. Under Roles, select Network Policy Server



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



7. Click OK when prompted to proceed with the authorization

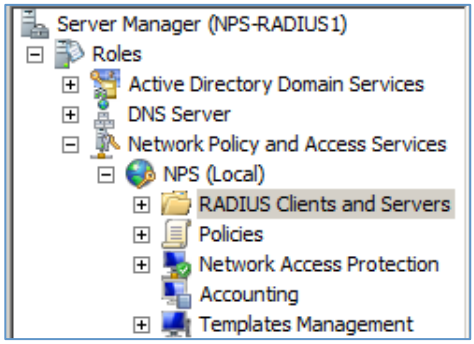
NPS is now installed and permitted to interact with Active Directory. The next step is to tell NPS which devices are allowed to use it to authenticate users.

Configure RADIUS (NAS) Clients

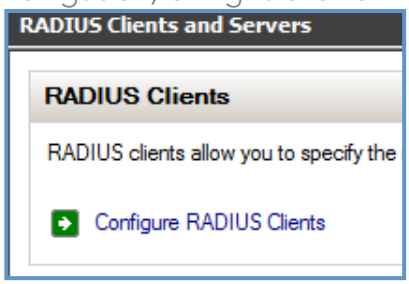
The first step to configure NPS is to define the RADIUS clients. A RADIUS client is a device that is allowed to communicate with the RADIUS (NPS) server. In 802.1X terminology, this is the *authenticator*. This is normally a ZoneDirector or a standalone AP.

Installation steps:

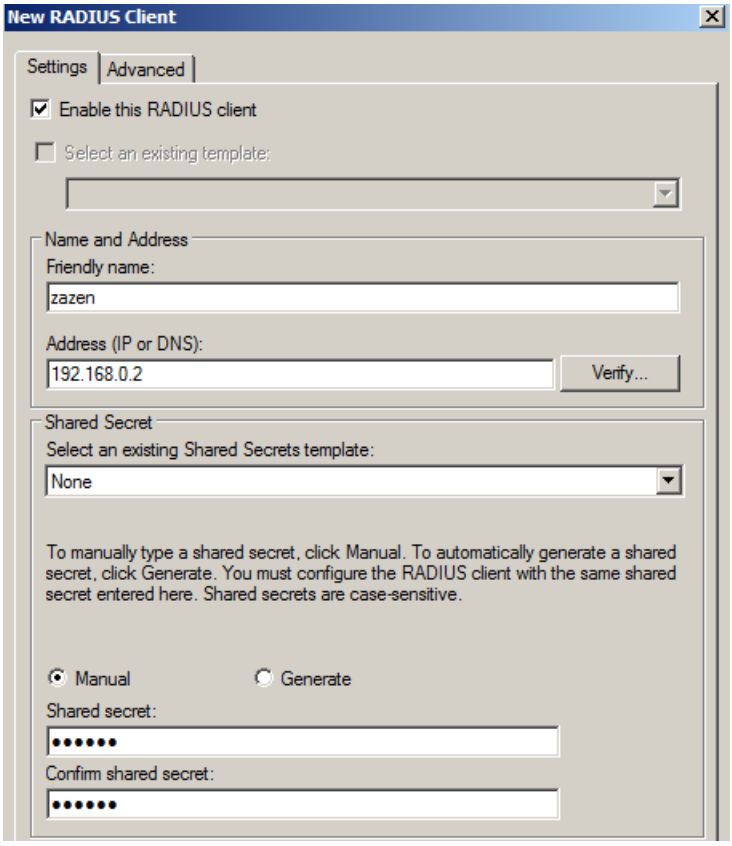
1. Launch the Server Manager application
2. In the Navigation pane on the left, navigate down to the local NPS instance and select RADIUS Clients and Servers



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



4. Click New
5. 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



6. 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!***

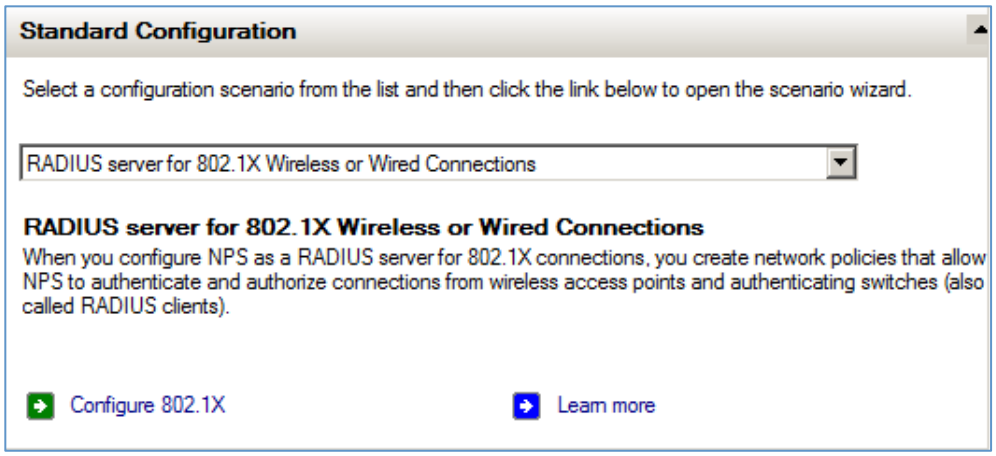
To setup an 802.1X configuration, only the first two types of polices are necessary. At least one Connection Request policy and one Network policy must be configured. The Health policies are optional and only required if you are performing NAP/health checks[10].

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

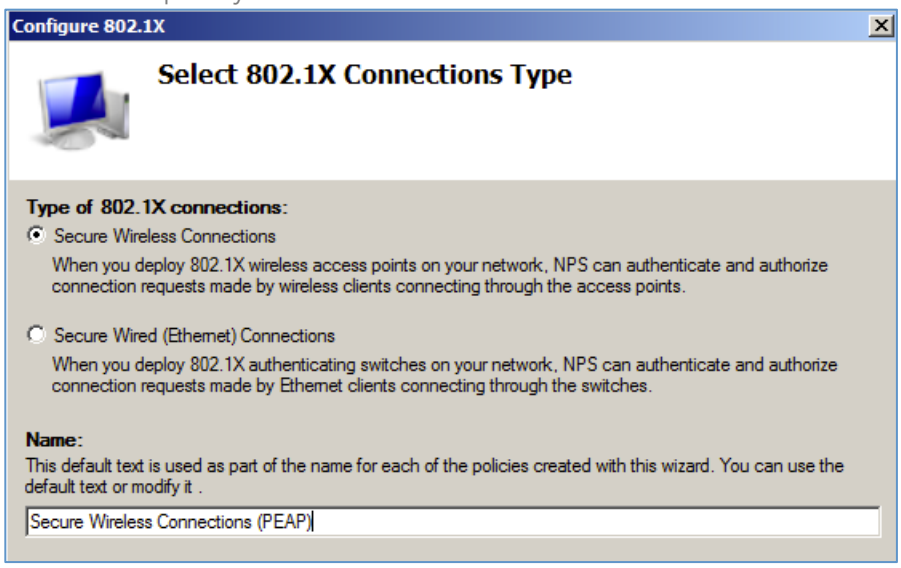
Configuration steps:

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

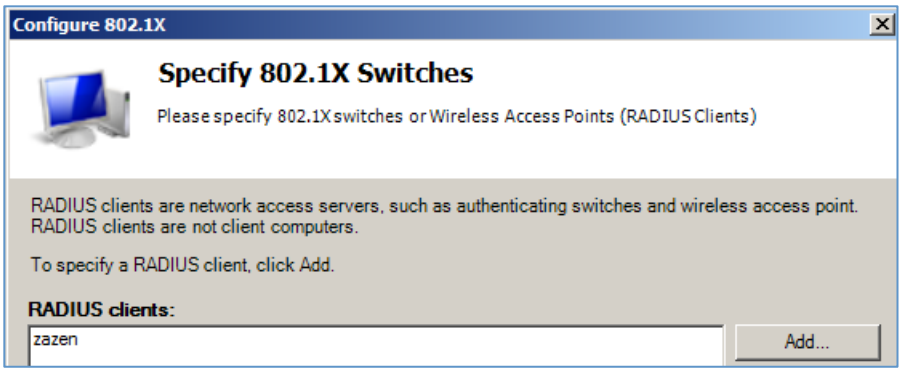
[10] Network Access Policy (NAP) configuration is out of the scope of this document. For more information please refer to Microsoft's documentation.



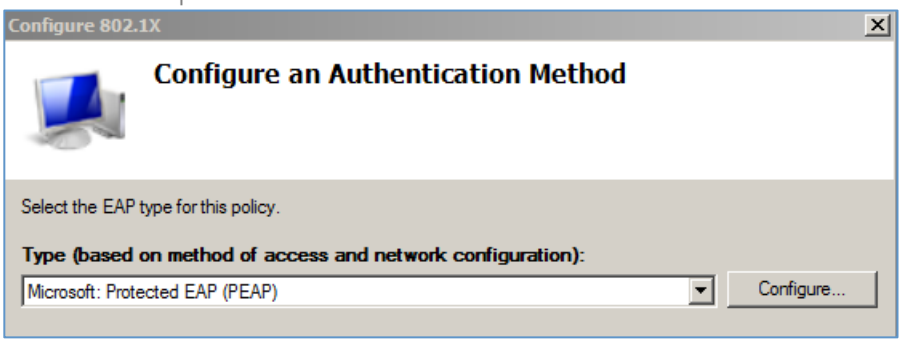
3. Under Standard Configuration (the middle screen), select RADIUS server for 802.1X Wireless or Wired Connections from the drop-down box
4. Click Configure 802.1X
5. Click Secure Wireless Connections for the connection type. You may change the default policy name here



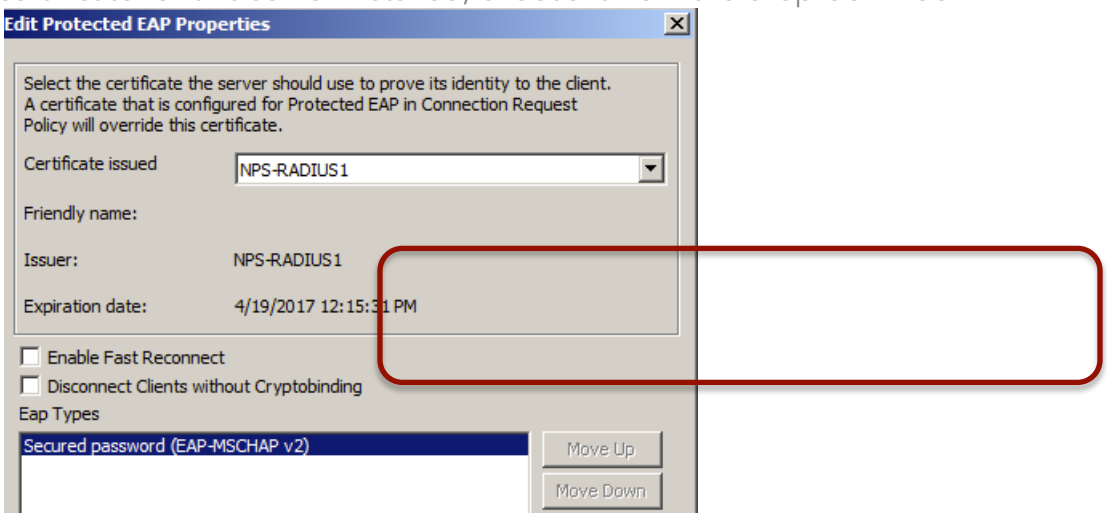
6. Click Next
7. Select your previously created RADIUS client(s). You may also add clients from here



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

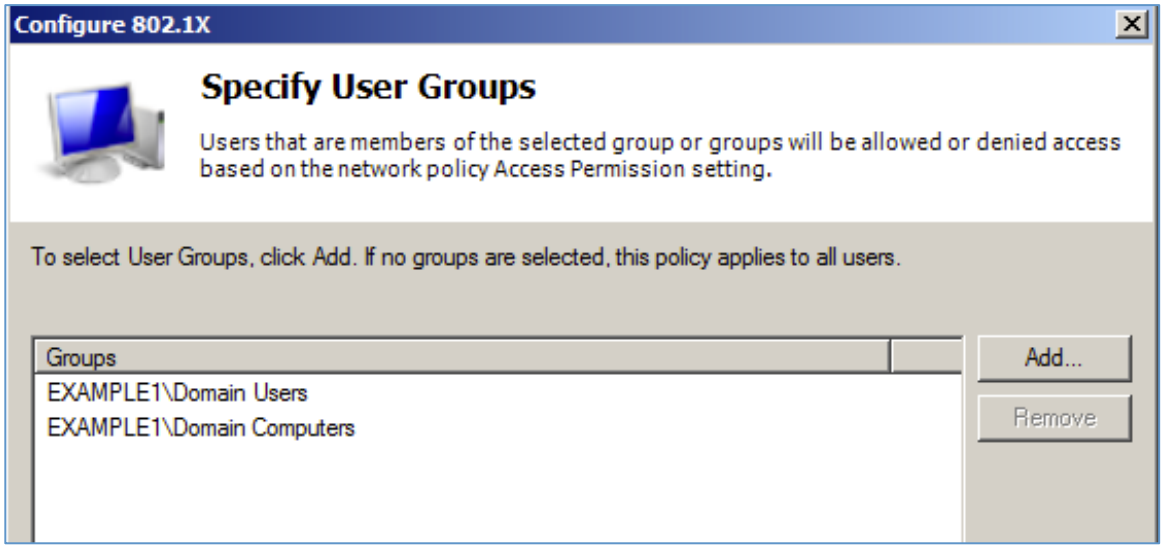


10. Click the Configure button and make sure you have the right certificate installed for RADIUS in the Certificate Issued box. If you have more than one certificate for this server installed, choose it from the drop-down box

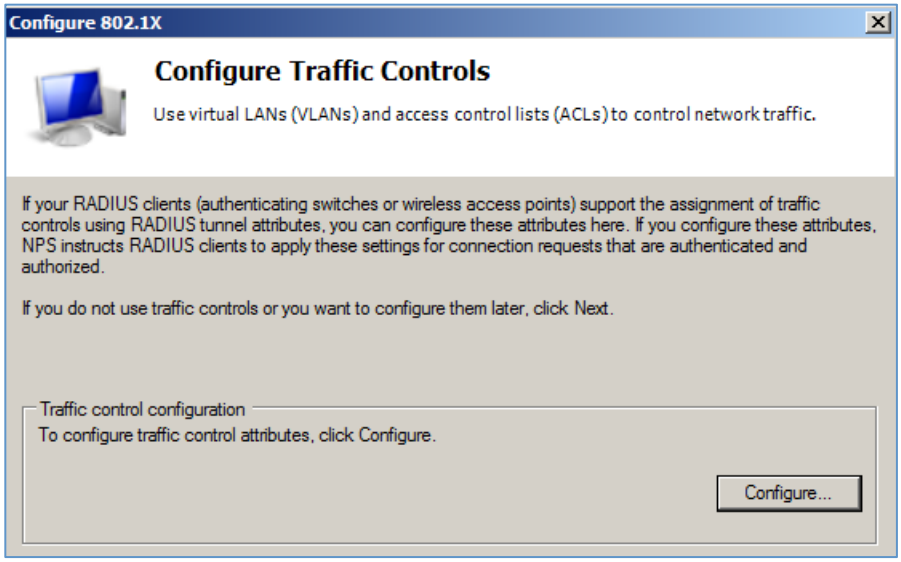


11. If the server certificate it is missing, you can add it here
12. In the next screen, you can choose conditions that control who gets network access. These conditions can apply to groups of domain computers or users.

13. 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.



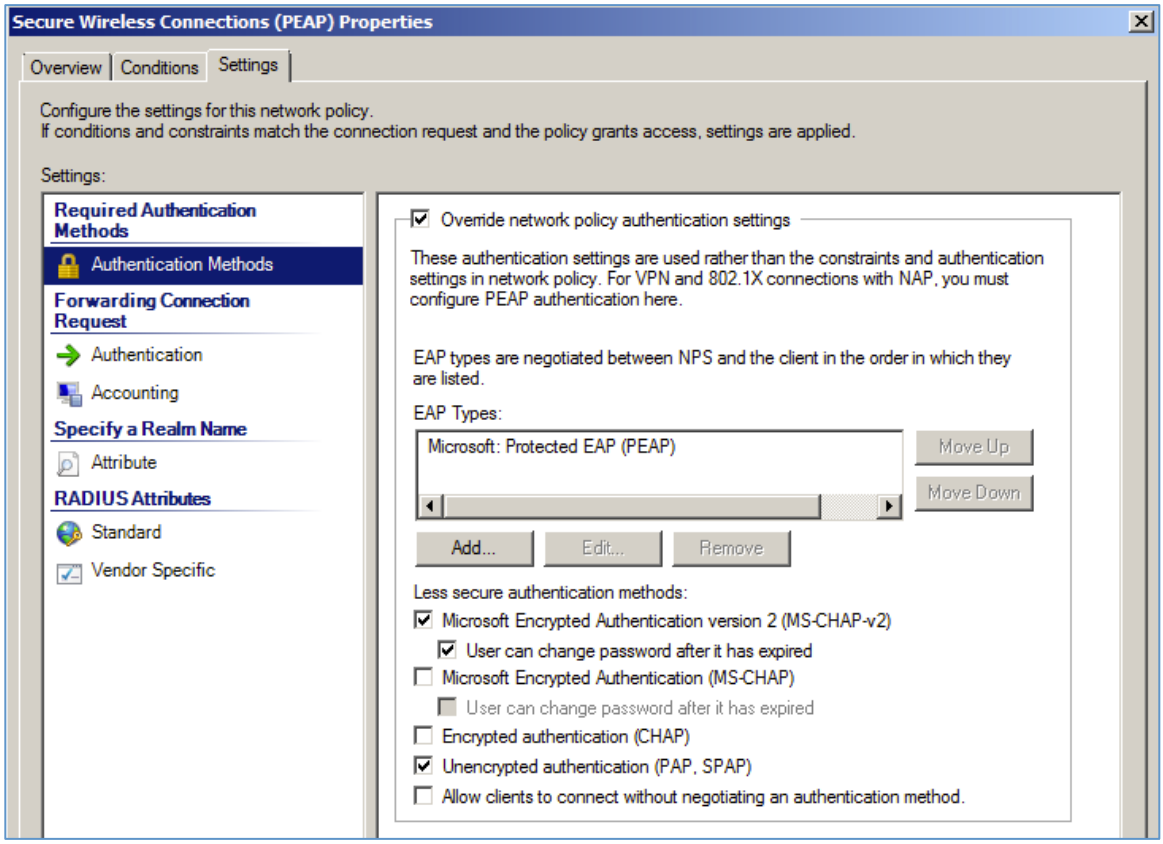
14. Click Next
15. The next dialogue allows you to configure traffic controls. This includes configuring Dynamic VLANs. It is not required for basic RADIUS service[11].



16. Click Next

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

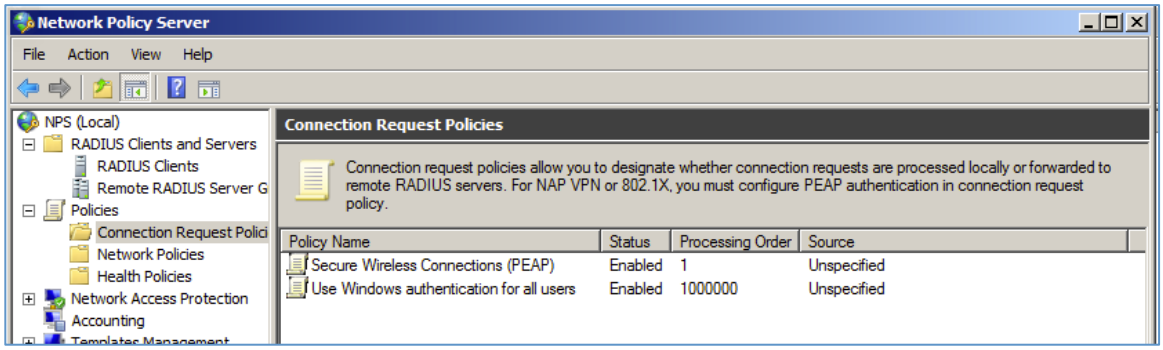
17. Review the NPS settings. If they are correct click Finish to end the wizard or go back and make any changes.
18. Click Next
19. Click Finish to close the wizard and save your policies
20. Next double-click to re-open the connection request policy for one additional edit
21. Click the Settings tab



22. Select the box at the top labeled Override network policy authentication settings
23. Click the Add button
24. Choose Microsoft: Protected EAP (PEAP) from the list
25. Click OK
26. Select the box marked Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
27. If you want to test the AAA server connection on the ZoneDirector you must also select either PAP or CHAP as well
28. 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.

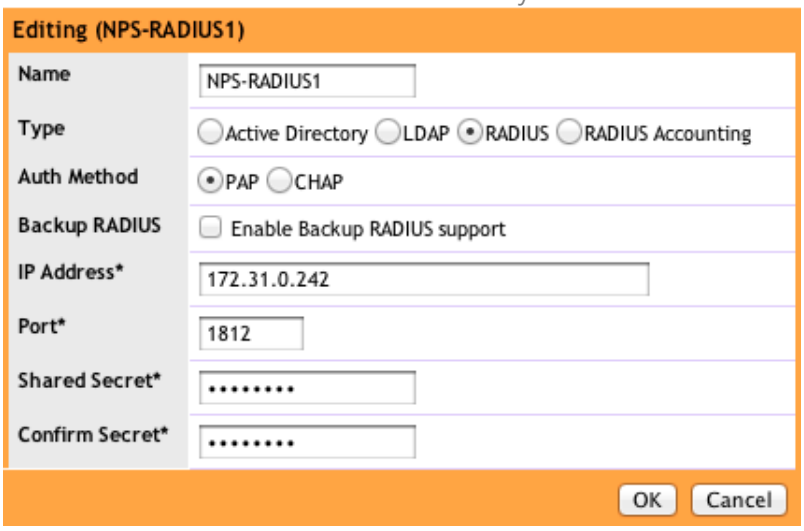
Configuring 802.1X on the ZoneDirector

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[12].

1. Log on to the ZoneDirector's web UI
2. Go to Configure->AAA Servers
3. Click Create New and enter the information for the NPS 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



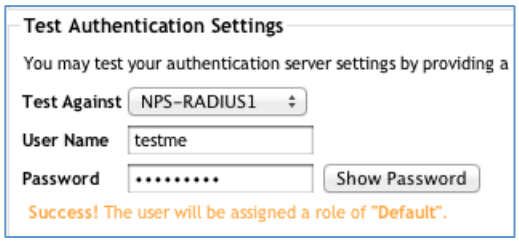
4. Click OK

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.[13] If you

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

[13] 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.

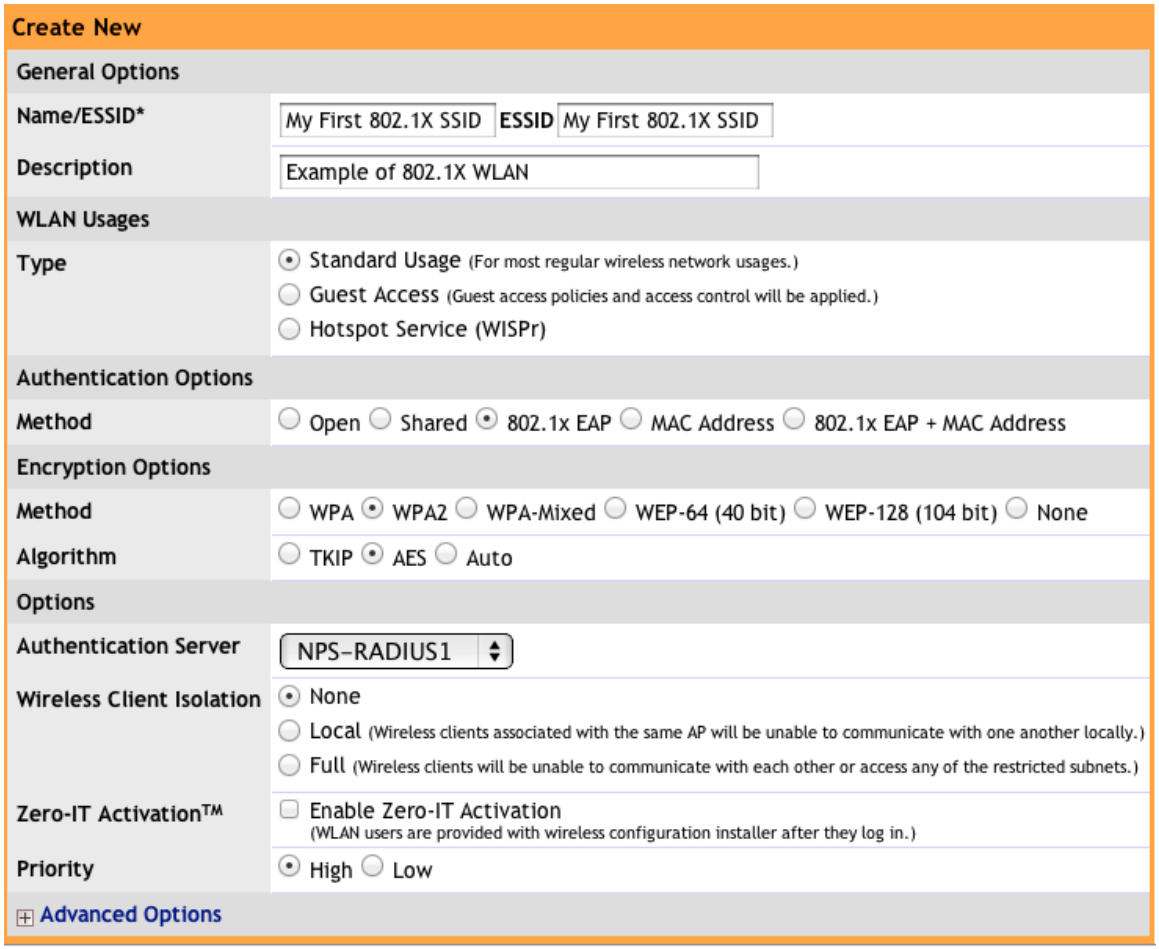
didn't set this up or are not sure how to do it, check out the instructions in Appendix B.



Create an 802.1X-enabled SSID

Next create the SSID.

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



4. 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 or LDAP do not know 802.1X is being used at all. The Ruckus AP and ZoneDirector need to know some type of 802.1X will be used, but they are completely agnostic as to the type[14]. 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 accept or reject message from RADIUS.

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

Configuring the Supplicant

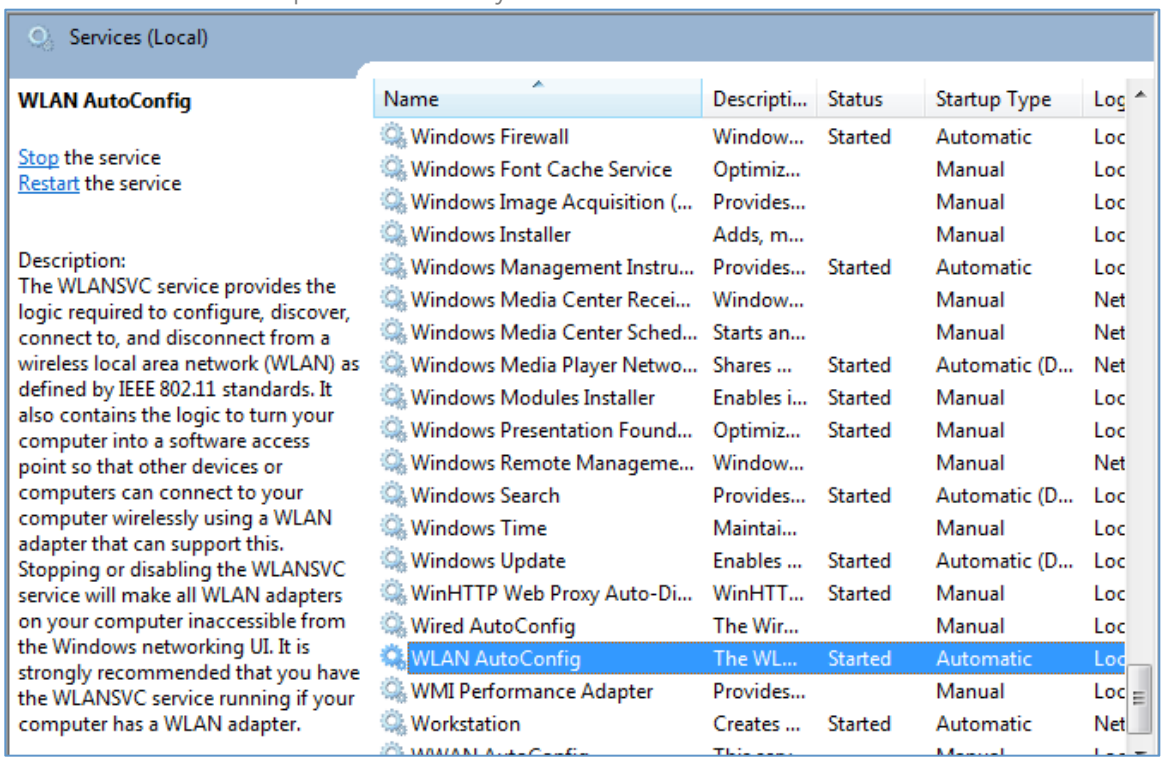
Most modern operating systems include an 802.1X supplicant. Although the details change from client to client, the process is the same.

Configure a Windows Supplicant

In this example, we will use a Microsoft Windows 7 client using Microsoft's WLAN AutoConfig supplicant. This process is very similar for other versions of Windows when you use the built-in Microsoft supplicant.

If you wish to use a 3rd-party supplicant, like Odyssey or the client utility that came with the wireless adapter, please consult their documentation for set up details.

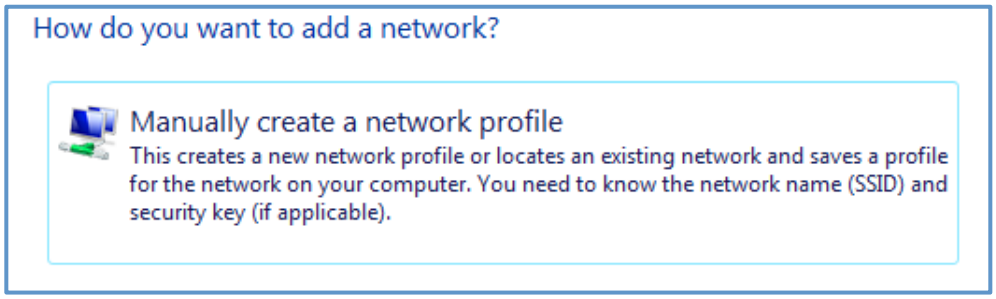
1. From the Control Panel, go to Administrative Tools and open the Services. Confirm the Microsoft WLAN AutoConfig service is running[15]. If it is not, start it and set it to start up automatically.[16]

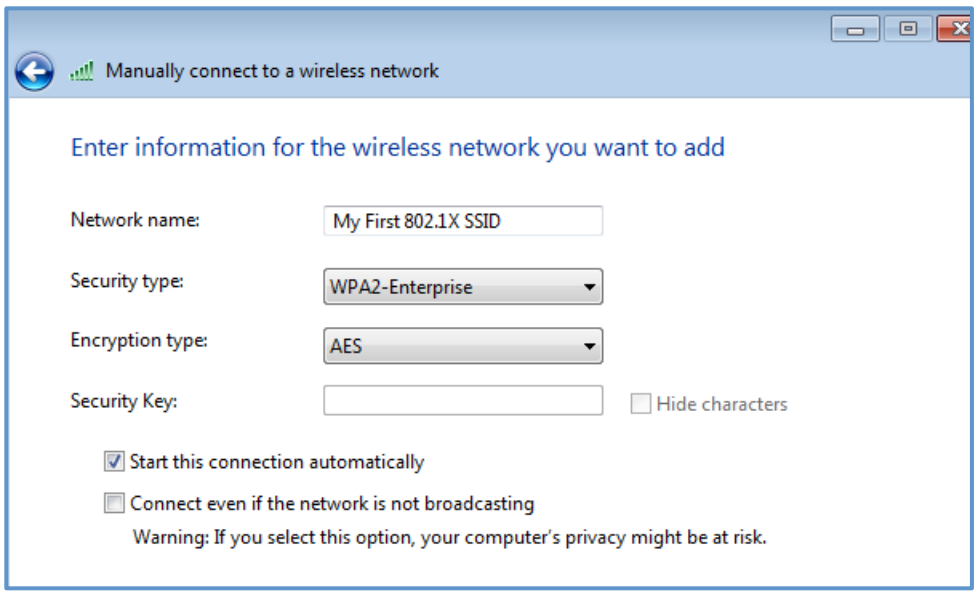


[15] On Windows XP this is called Wireless Zero Config, on Windows 7 it is WLAN AutoConfig
[16] Starting Microsoft's supplicant will automatically stop any other supplicants running on the machine.

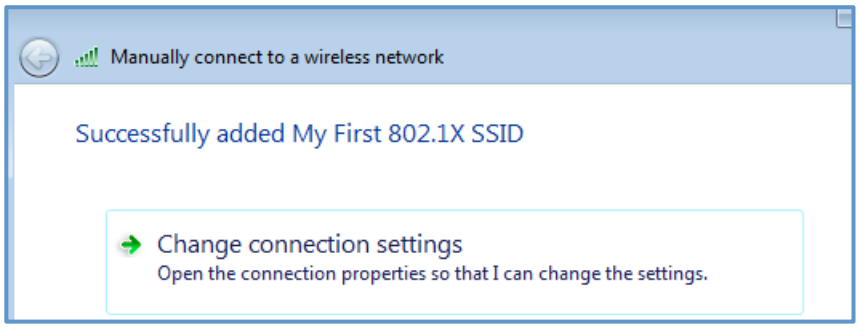
2. From the Control Panel, go to Network and Internet -> Manage Wireless Networks

3. Click Add
4. In the next screen, select Manually create a network profile





5. Enter your SSID name, security and encryption type
6. Click Next to create the profile



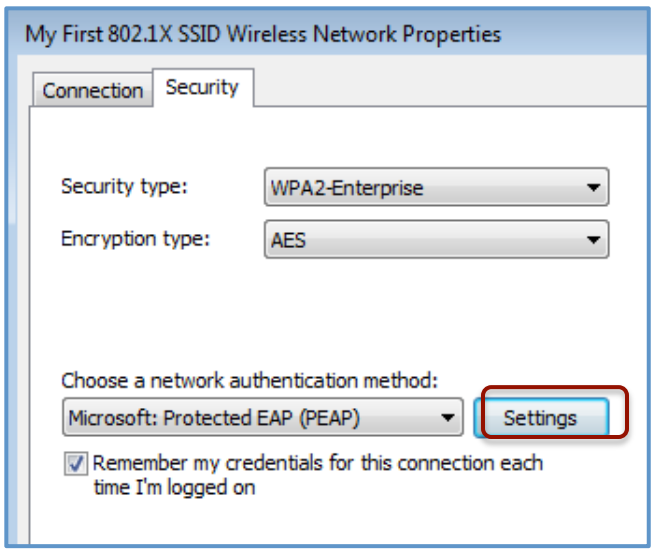
At this point, it's a good idea to review some of the more common options that may also be needed for this supplicant.[17]

Disable Server Certificate Validation

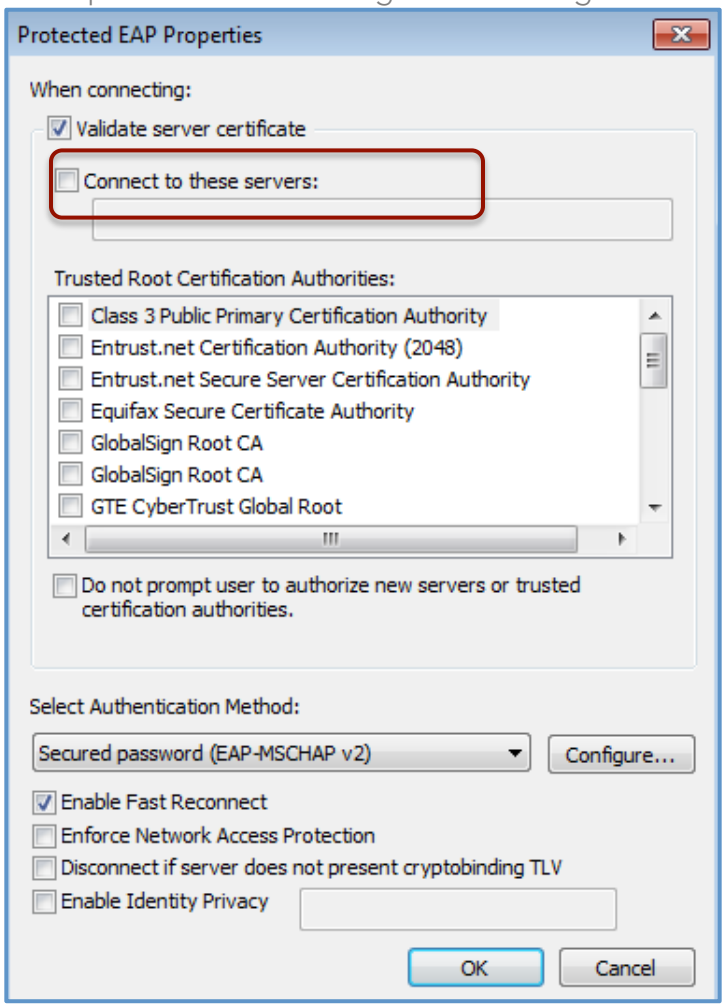
If you RADIUS server is not using a certificate from a known CA, you might want to temporarily disable the Validate server certificate box. This will prevent the client from validating the server's certificate – although it will still require a certificate.

1. From the list of profiles, right-click the 802.1X profile and Properties
2. Click the Security tab
3. Click the Settings button

[17] If you've done everything right and followed every step, you can probably skip the rest of this section. Or you could read it anyway – just in case.



4. This opens the PEAP configuration dialogue

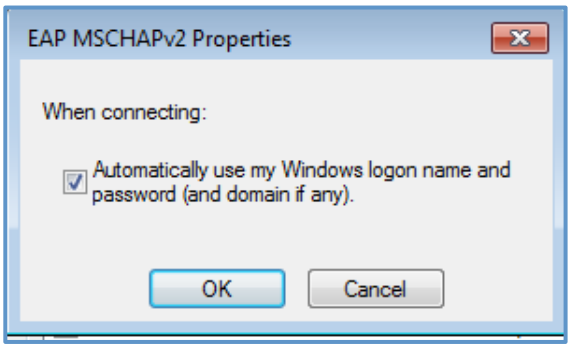


5. Unselecting the Validate server certificate option will cause the client to accept any correctly formatted certificate from the server.

Security best practices dictate the client should always validate the server certificate. This step is only recommended for troubleshooting certificate problems. Once they are resolved, the client should be configured to validate certificates again.

Automatically login with different credentials

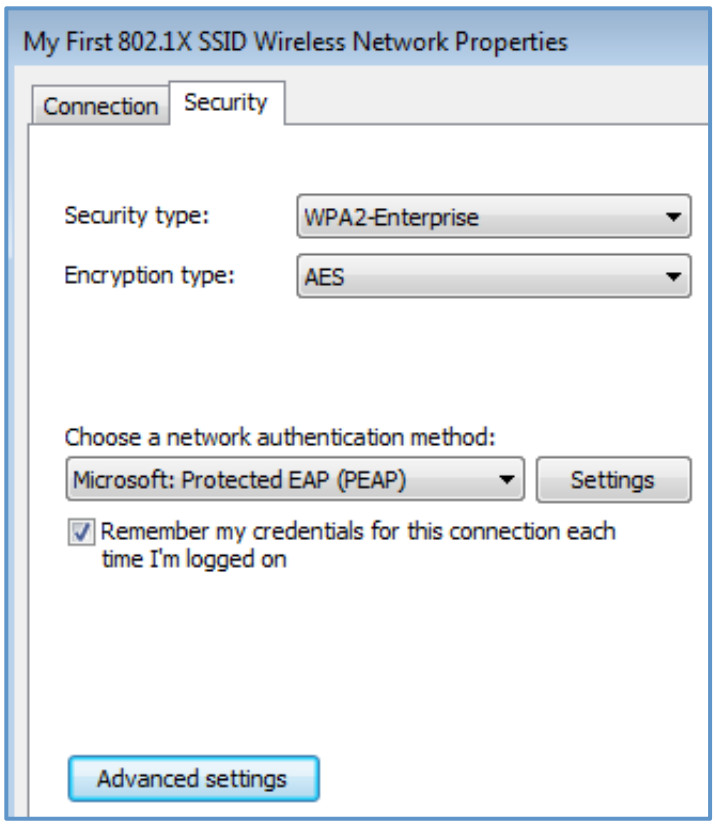
The default behavior for a Microsoft client is to attempt to authenticate with the user credentials that were used to log onto the machine itself. If you want to use a different set of credentials you can disable this behavior. If you do this you will be presented with a pop-up dialogue box asking for the user name and password.



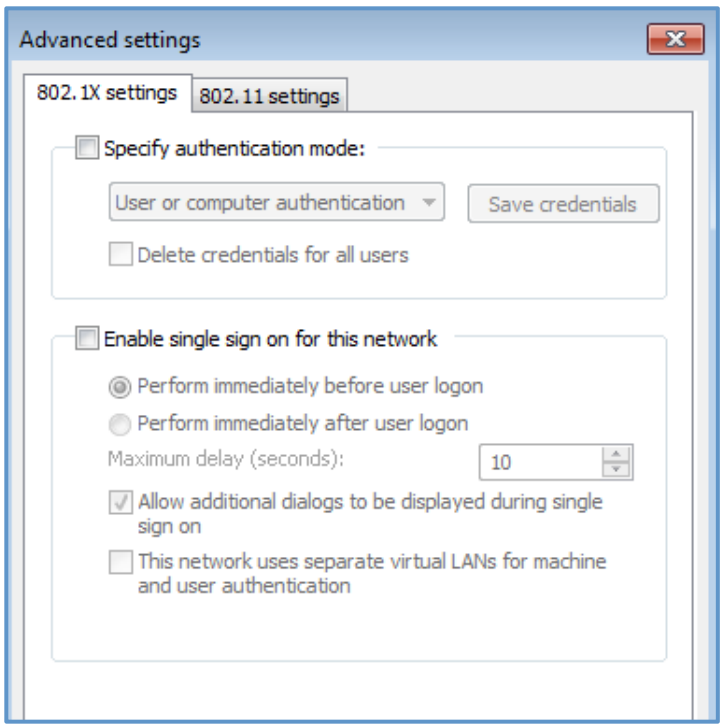
Single sign on

It's often useful to allow domain computers to authenticate to the wireless *before* a user logs on. This allows domain users to log onto the wireless from any domain machine, regardless of whether the user has ever used the machine before (i.e. has cached credentials).

1. From the wireless network properties window, click the Advanced settings button



2. The following dialogue box offers the ability to specify several behaviors:
3. Authentication mode – determines what entities can login to the wireless: users, machines, or user and machine
4. Enable single sign on – allows the machine to log onto the wireless network when a user is not logged on, this allows users with non-cached credentials to login to the wireless at the same time that they log onto the machine

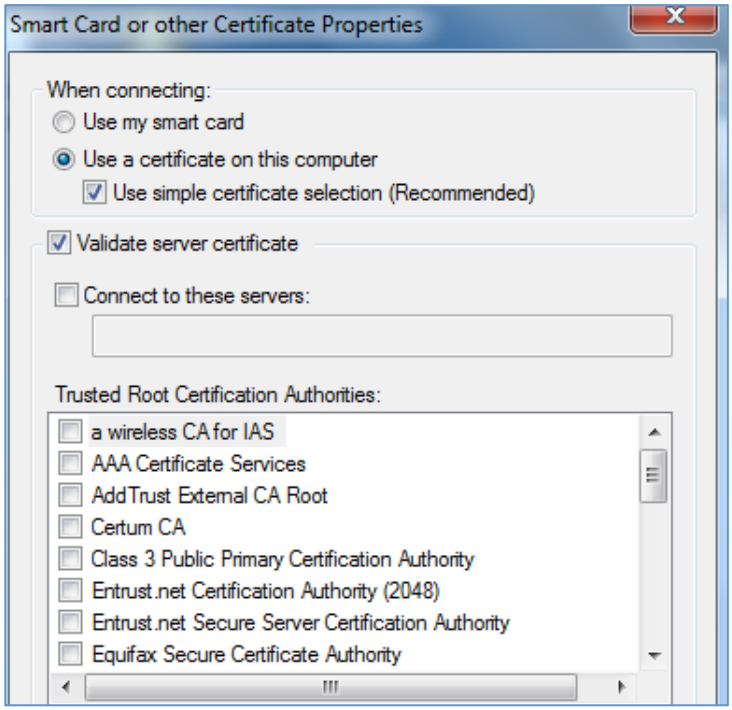


EAP-TLS Configuration

If you are using EAP-TLS, the configuration is very similar to PEAP with the following exceptions:

1. A client certificate (user or machine) must be loaded on the machine or installed as part of auto-enrollment prior to the first connection
2. During the wireless network setup, go to the Security tab and select Microsoft: Smart Card or other certificate as the authentication method

3. After choosing the authentication method, select Settings and make sure the checkbox next to Use a certificate on this computer is selected



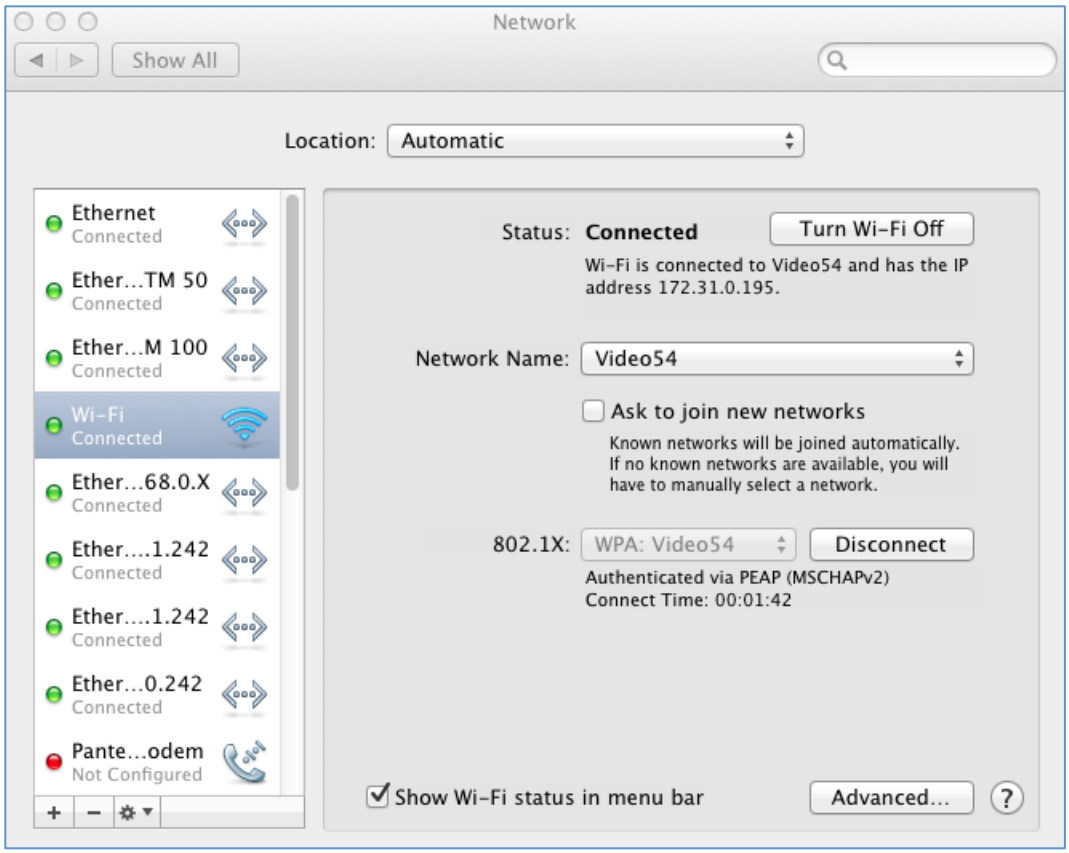
These are the only changes required to configure a client for EAP-TLS instead of PEAP.

Configure a Mac OS Supplicant

In this example, we will use an Apple Mac OS 10.7 (Lion) client using Apple's built-in supplicant. This process is very similar for other versions of Mac OS when you use the built-in supplicant.

If you wish to use a 3rd-party supplicant, like Odyssey or the client utility that came with the wireless adapter, please consult their documentation for set up details.

1. Install any certificates, if required
2. From the Settings application, go to Network and select Wi-Fi from the list of network interfaces on the left



3. Click the Advanced button
4. Click the plus (+) sign under Preferred Networks to define a new network

5. In the network profile dialogue, make sure the correct SSID, security type and credentials are entered[18]
6. Click OK
7. Click OK in the next dialogue box to save your changes
8. The new SSID should appear in the dropdown box of Network Names
9. Select the new SSID and connect. Enter your credentials if prompted

EAP-TLS Configuration

If you are using EAP-TLS instead of PEAP there is no change to the configuration. Simply make sure the client certificate is installed in the Keychain Access before connecting. If prompted, select the correct certificate from the TLS Certificate dropdown menu.

[18] User credentials are not required, however if not entered here you will be prompted for your credentials when you connect

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

Introduction & Key Concepts dffdfd