Ashby School

[Network Services]

Wireless 802.1x Authentication Using Microsoft IAS Server.

Contents

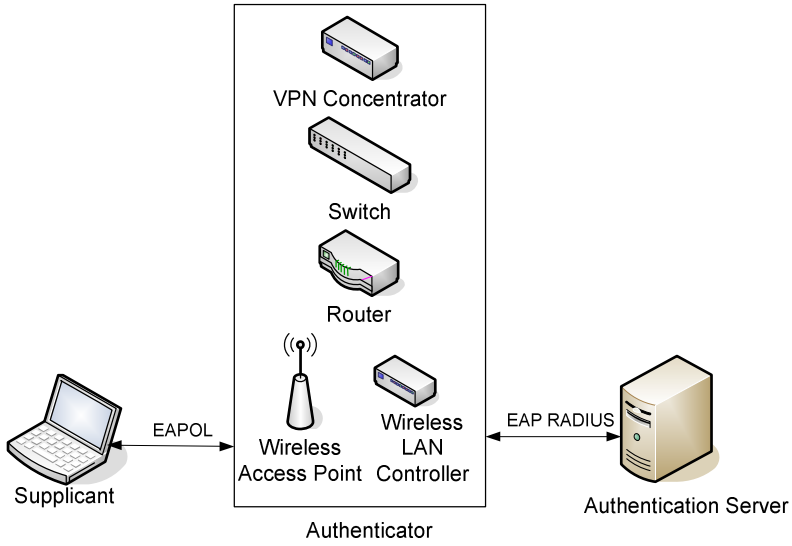
1. Introduction

1.1 802.1x

IEEE 802.1X is an IEEE (Layer 2) standard for port-based network access control mechanism, part of the IEEE 802 (802.1) group of protocols. It provides authentication for devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. It is often used for wireless access points, and is based on the EAP, Extensible Authentication Protocol (RFC 2284).

In a wireless LAN with 802.1X, a user or computer (referred to as the ***supplicant***) requests access to an access point (the ***authenticator***). The access point forces the user or computer into an unauthorized state that allows the client to send only an EAP start message. The access point returns an EAP message requesting the user's identity. The ***supplicant*** returns the identity, which is then forwarded by the access point to the ***authentication server (RADIUS)***, which uses policies and other checks (i.e. checking if the user and/or computer exists in the database i.e. LDAP, Active Directory), to authenticate the user and then returns an accept or reject message back to the access point. Assuming an accept was received, the access point changes the client's state to authorized and normal traffic can now take place.

802.1x operates at Layer 2 which means the supplicant's (i.e. wireless enabled devices in this case) are not granted an IP address until they are fully authenticated and authorised). 802.1x authentication is not just limited to wireless access it can also be used for **wired LAN**, **VPN connections** as well as **dial-up** connections.



As you can see from the above diagram, the authenticator can be a **Wireless Access Point**, **Wireless LAN Controller**, **Router**, **Wired switch** or a **VPN concentrator**.

To summarise a supplicant is a wireless enabled device, i.e. Windows XP Laptop with a wireless network card that is trying to gain access to the network.

The authenticator is an access point that forces the supplicant to provide identity (forces authentication) before allowing the device (supplicant) onto the network.

Authentication server, usually a RADIUS (**Remote Access Dial-in User Service**) server is responsible for actually making the decision to allow the device onto the network or not by checking policies (conditions) that have been setup and matching then up with the credentials received from the wireless device. The Authentication server can read information from external databases and directory services such as Microsoft's Active Directory or other LDAP service providers.

1.2 IAS (Internet Authentication Service)

IAS server is a RADIUS server from Microsoft and it comes free with Microsoft Windows 2000 and Windows 2003 Server. It is used to provide centralised **authentication**, **authorisation** and **accounting** (AAA) for different types of network access such as wireless, wired, Virtual Private Network (VPN) and dial-up connections. IAS can also be used as a RADIUS proxy which can forward authentication messages to other RADIUS servers.

Microsoft IAS server can read information from MS Active Directory to provide seamless authentication by querying AD directly. In addition to this IAS server can log accounting information to a file or SQL Server providing flexibility in logging and querying accounting data.

IAS server is not to be confused with another Microsoft product called ISA (Internet Security and Acceleration) Server. This is a completely different product that provides firewall and proxy capabilities.

1.3 EAP (Extensible Authentication Protocol)

EAP is an authentication framework that provides negotiation of various authentication mechanisms such as MS-CHAPv2, TLS, EAP-MD5, EAP-OTP etc. EAP only defines message format and is not an authentication method. When an 802.1x device wants to communicate with the network it starts to send EAPOL (EAP over LAN) messages to the **authenticator** or **Network Access Server** (NAS).

When EAP is invoked by an 802.1x enabled NAS (Network Access Server) device such as an 802.11 a/b/g Wireless Access Point, modern EAP methods can provide a secure authentication mechanism and negotiate a secure PMK (Pair-wise Master Key) between the client and NAS. The PMK can then be used for the wireless encryption session which uses TKIP or CCMP (based on AES) encryption. [1]

EAP is not a wire protocol; instead it only defines message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages. In the case of 802.1X, this encapsulation is called **EAPOL**, "EAP over LANs". [1]

1.4 PEAP (Protected EAP) / MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol)

Protected Extensible Authentication Protocol, **Protected EAP**, or simply **PEAP** (pronounced *"peep"*), is a method to securely transmit authentication information, including passwords, over wired or wireless networks. It was jointly developed by Cisco Systems, Microsoft, and RSA Security. Note that **PEAP** is not an encryption protocol; as with other EAP types it only authenticates a client into a network. [2]

PEAP-MS-CHAP v2 is a password-based authentication method for wired and wireless connections.

Behind EAP-TLS, PEAPv0/EAP-MSCHAPv2 is the second most widely supported EAP standard in the world.

PEAP only requires a certificate to be issued to the authentication (RADIUS) server and not the end devices.

2. Installing IAS Server

Internet Authentication Service (IAS) is a built in component of Windows Server 2000/2003. It can be used as a separate service running on a separate server but can also be used on an existing Domain Controller (DC). IAS is the RADIUS server's (Remote Access Dial-In User Service) implementation from Microsoft. Below is a list of pre-requisites for IAS.

2.1 Prerequisites

- Microsoft Windows Server 2000 or 2003 (Windows 2003 SP1 or above preferred)
- To authenticate devices or users against Active Directory the server which is running IAS must be joined to the domain.
- Certification server (or, you could buy a certificate from a third party certificate authority or generate a self-signed certificate).

  Note: RM CC3 networks have an Enterprise Certificate Authority (CA) installed

- RADIUS server (comes with Windows 2000/2003 server - IAS).
- Your domain functional level must be at least Windows 2000 native or Windows 2003 Server. (**By default on RM CC3 network it is Windows 2000 native**).

  This option allows you to control access using the "**dial-in**" properties of users in AD.

- Wireless Access point that supports WPA with Radius authentication (802.1x).
- Wireless network card (with drivers that supports WPA/802.1x supplicant services).
- Windows 2000 or 2003 CD

2.2 Installing and configuring IAS on Windows 2003 Server

If you have a RM Community Connect 3 network, do not install IAS on any of your Domain Controllers. It is best to install IAS on a member server.

1. Open **Add or Remove Programs** in **Control Panel**
2. Click **Add/Remove Windows Components**.
3. In the **Windows Components Wizard** dialog box, click **Networking Services**, and then click **Details**
4. In the **Networking Services** dialog box, select **Internet Authentication Service**, click **OK**, and then click **Next**.
5. If prompted, insert your Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition CD.
6. After **IAS** is installed, click **Finish**, and then click **Close.**

2.3 Registering IAS and Configuring Logging/Ports

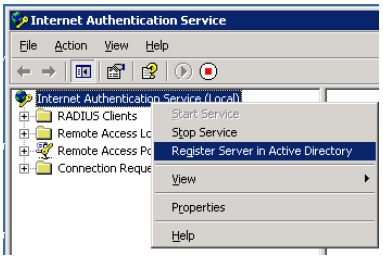
After the IAS component has been installed on a windows 2003 server you will notice that there is an **Internet Authentication Service** snap in, located in **Start > Programs > Administrative Tools.**

The next task is to register IAS with active directory so that it can read the user and computer accounts for authentication.

1. Log on to the IAS server with an account that has administrative rights for your domain.

2. Open **Internet Authentication Service**.

3. Right-click **Internet Authentication Service** and then click **Register Server in Active Directory**. When the **Register Internet Authentication Service in Active Directory** dialog box appears, click **OK.**



The next task after registering IAS in Active Directory is to configure the ports that IAS uses for its authentication and accounting.

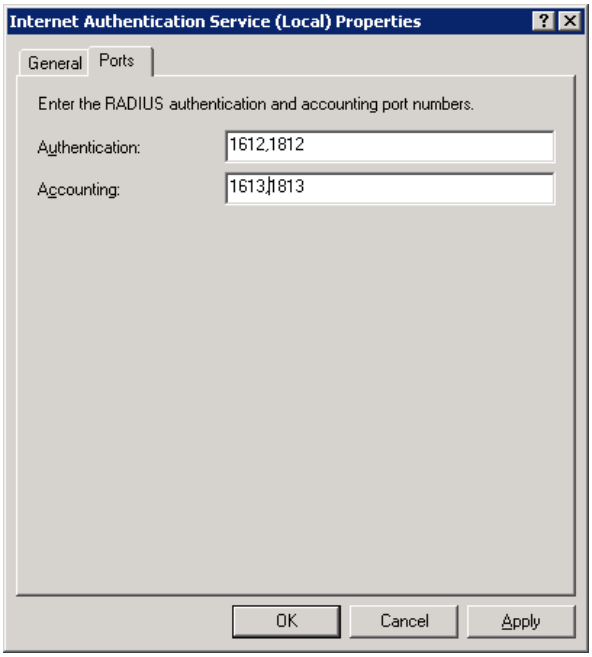
1. Open **Internet Authentication Service**.

2. Right-click **Internet Authentication Service** and then click **Properties**.

3. Click the **Ports** tab, and then check the settings for ports.

4. By default IAS uses UDP ports 1812, 1612 for authentication and 1813, 1613 for accounting messages.

5. If your RADIUS authentication and RADIUS accounting UDP ports are different from the default values then type your port settings in Authentication and Accounting and click on the **Apply** button and then the **OK** button to close the Properties.



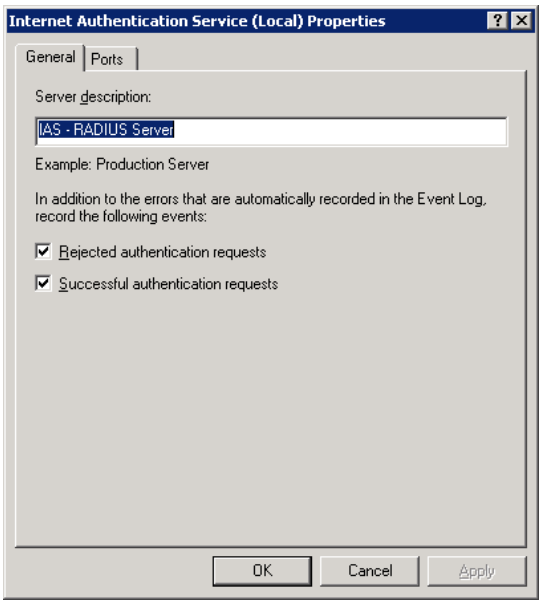
Note: If your have a firewall between the IAS server and the Access points then make sure that you allow the above UDP ports access so the access points can communicate with the IAS (Radius) server.

If you wish you may use only one set of ports i.e. 1812 for authentication and 1813 for accounting.

It is important that event logging is enabled for IAS. This allows administrators to troubleshoot issues with connections. Events generated by IAS server will be displayed in **Event Viewer** under the **System Log**.

To enable event logging:

1. Open **Internet Authentication Service**.
2. Right-click **Internet Authentication Service** (IAS), and then click **Properties.**
3. On the **General** tab, select both options, and then click **OK.**



Notes:

It is also good practice to give the server a description such as IAS – RADIUS Server.

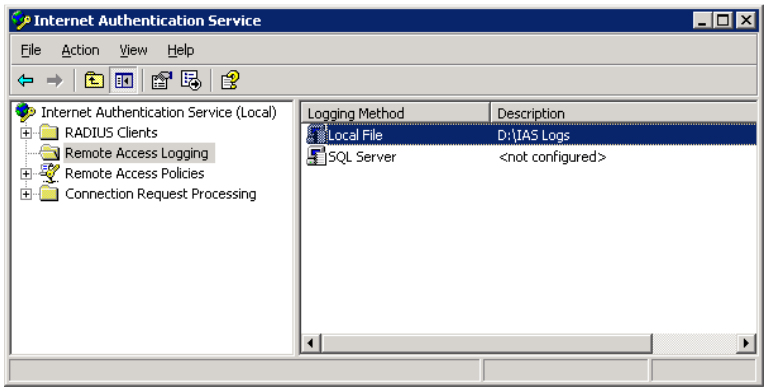
Selecting **Successful authentication requests** can result in logging extremely large volumes of data. Before selecting this option, check that the Event Viewer is configured with appropriate maximum log size to accommodate this type of event logging.

Logs can be stored on file on the IAS server computer or they can be setup so they are logged to a SQL Server database. If you are unsure what is the best option select Logging to a file.

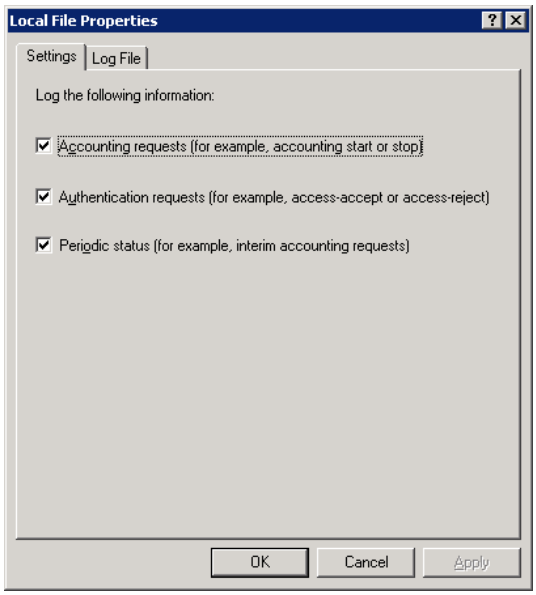
To enable logging to a file:

1. Open **Internet Authentication Service**.

2. Click on the **Remote Access Logging** option and then on the right hand side double-click on **Local File**.



3. On the **Settings** tab, select all options.



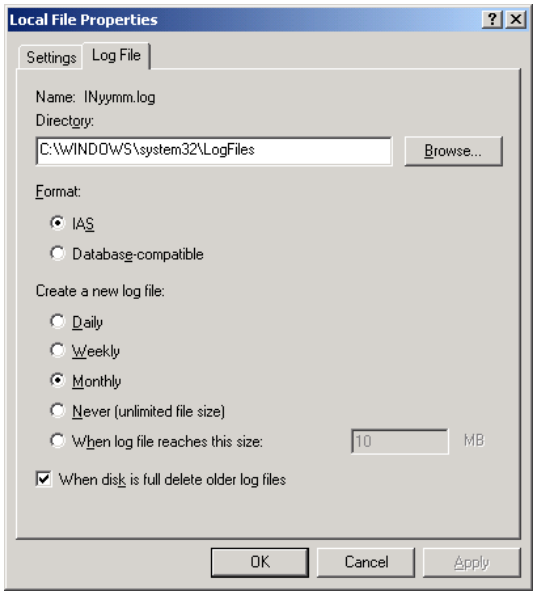
4. To specify the drive and file paths where logs will be stored click on the **Log File** tab.

   Specify the Drive and file path where logs are to be stored by clicking on the **Browse** button and selecting the desired path.

5. Leave the Format option as **IAS**

6. Change the **Create a new log file** option as desired, the default is **Monthly**.

7. You may also wish to check the bottom option – "**When the disk is full delete older files**" to prevent the logs taking up all of your disk space.



8. Click on **OK** to return to Remote Access Logging screen.

3. Adding and Configuring Radius Clients

The next stage of the configuration is to add clients which are going to be used for authenticating users and computers.

In RADIUS terminology client(s) represents the **authenticator** which could be **wired switches**, **Wireless Access Points, Wireless LAN Controllers**, **VPN concentrators** or **routers** which are capable of 802.1x Authentication. The client or authenticator is also sometimes referred to as a Network Access Server (NAS) especially in the case of a VPN Concentrator. To the radius server these are all considered as radius client(s). The end wireless devices (supplicants) do not communicate directly with the authentication (Radius) server.

Do not confuse radius clients with normally understood clients such as laptop or desktop PCs.

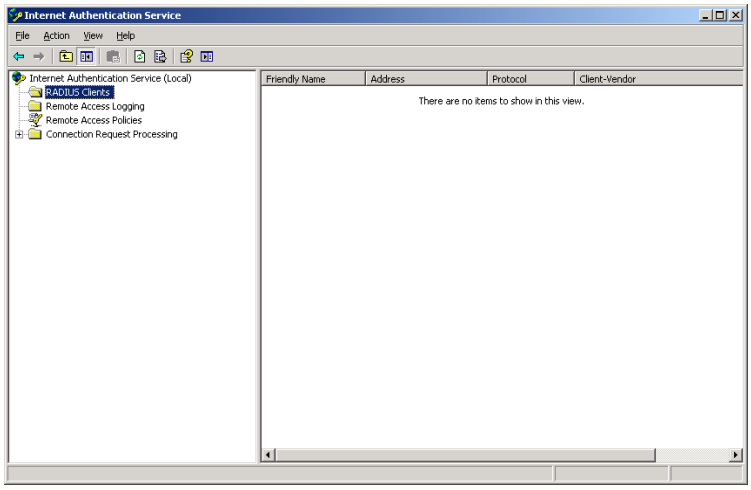
In Windows Server 2003 Standard Edition, you can configure a maximum of 50 Radius clients and a maximum of 2 remote Radius server groups. You can define a Radius client using a fully qualified domain name or an IP address, but you cannot define groups of Radius clients by specifying an IP address range. If the fully qualified domain name of a Radius client resolves to multiple IP addresses, the IAS server will use the first IP address returned in the DNS query.

In Windows Server 2003 Enterprise Edition, and Windows Server 2003, Datacenter Edition, you can configure an unlimited number of Radius clients and remote Radius server groups. Furthermore you, you can configure Radius clients by specifying an IP address range.

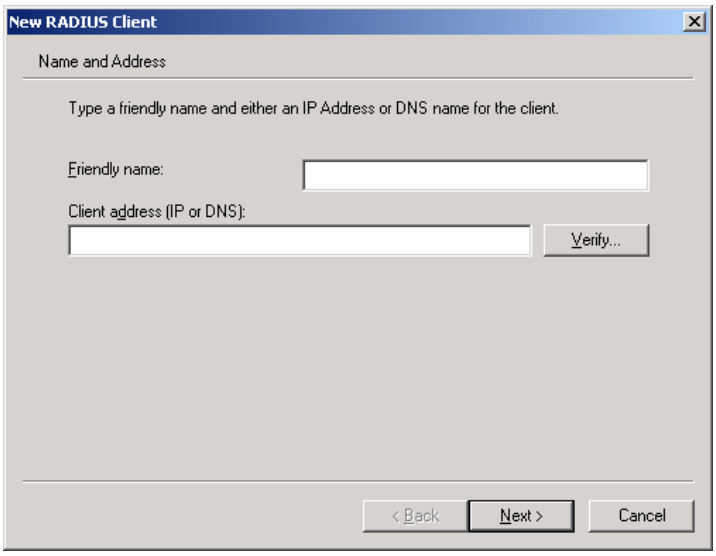
3.1 Adding Radius Clients to IAS:

1. Open **Internet Authentication Service**.

2. Right-click **RADIUS Clients** and then click **New RADIUS Client**.



3. This will start the New Radius Client wizard and display the **Name and Address** screen.



4. Enter a friendly name for the radius client i.e. **Cisco1131-LibraryAP** in the **Friendly name** box. In the client address box enter the **IP address** or fully qualified domain name (FQDN) of the access point and click **Next**.

5. In the **Additional Information** screen at **Client-Vendor** leave the default of **RADIUS Standard.**

   Note: If you have a Cisco Access Point or Cisco Wireless LAN Controller then select **Cisco** from the drop-down menu.

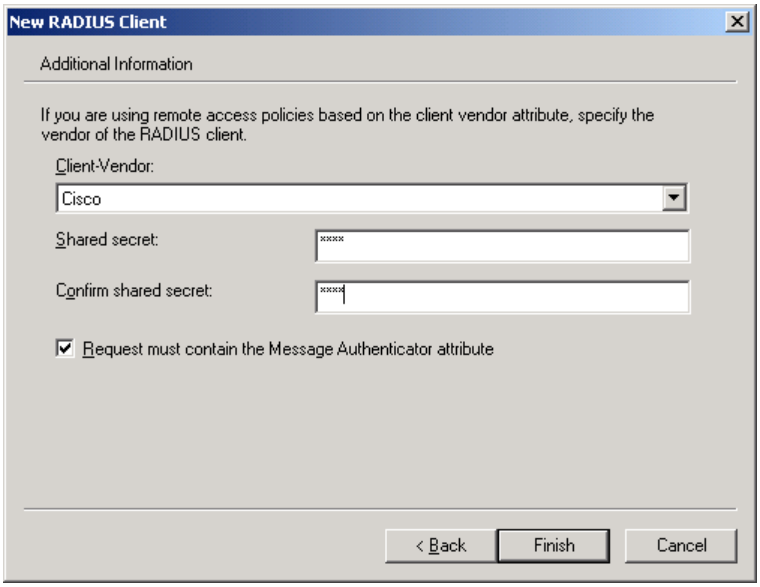
6. In the **Shared Secret** box type in a shared secret which is longer than 12 characters and contains both letters and numbers. The shared secret acts as password between the Radius server and the radius client and will need to be entered on both the access point and the RADIUS client entries on the IAS server. The shared secret that is entered on the RADIUS server and the access point must match in order for the AP to communicate with the RADIUS server for authentication messages/requests.

Shared secret is case sensitive so make sure that you enter it correctly on both the IAS server and in the access point.

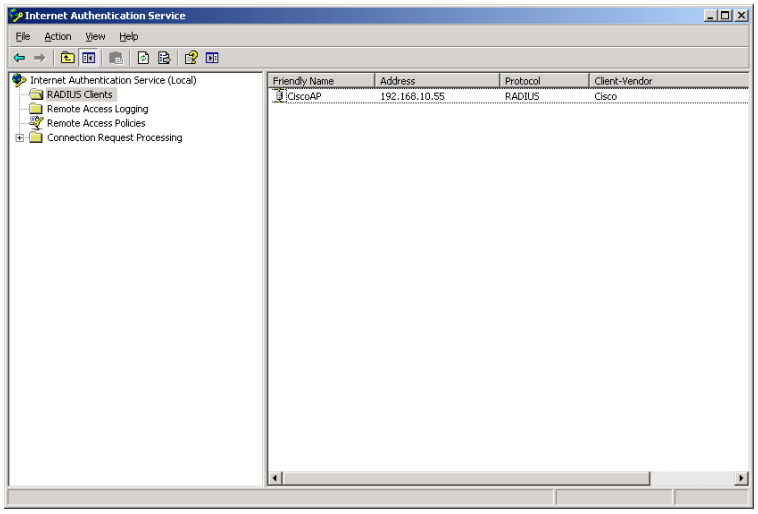
Strictly speaking the shared secret does not need to be 12 characters long but to provide better security a longer entry is preferred.

7. Leave the box ticked next to **Request must contain the Message Authenticator attribute**.

   This option tells the Radius server to use the shared secret as the key in encrypting the RADIUS message. It provides additional security when using authentication methods such as MS-CHAPv2.



8. Click on **Finish** to add the Radius client. You will then return to the **Radius Clients** screen where you will see the Radius client you have just added.



In case some radius clients become redundant or need replacing then these radius clients will need to be removed from IAS.

3.2 Deleting Radius Clients from IAS:

1. Open **Internet Authentication Service**.

2. In the console tree, click **RADIUS Clients**.
3. In the details pane, right-click the client that you want to delete, and then click **Delete**.
4. In the **Delete Client** dialog box, click **Yes**

3.3 Editing Radius Clients in IAS:

1. Open **Internet Authentication Service**.
2. In the console tree, click **RADIUS Clients**.
3. In the details pane, double-click the client for which you want to edit the configuration.
4. Make changes to the RADIUS client configuration.
5. Click **OK** to save your changes

4. Adding and Configuring Remote Access Policies

Remote access policies are an ordered set of rules that define how connections are either authorised or rejected. For each rule, there are one or more conditions, a set of profile settings, and a remote access permission setting.

If a connection is authorised, the remote access policy profile specifies a set of connection restrictions. The **dial-in** properties of the user account also provide a set of restrictions. Where applicable, user account connection restrictions override the remote access policy profile connection restrictions.

If all conditions of a remote access policy are met, remote access permission is either granted or denied.

When IAS server evaluates a policy, it works from the top of the list and work down trough to the bottom. If any policy matches then that policy is used and further processing does not take place i.e. all other policies below the matched policy are not evaluated.

Remote Access Policies are the heart of the decision making in allowing or denying a device onto the network.

Remote access permission is also granted or denied for each user account. The user remote access permission overrides the policy remote access permission. When remote access permission on a user account is set to the **Control access through Remote Access Policy** (*this option is only available if the domain functional level is at Windows 2000 native or Windows 2003 Server*) option, the policy remote access permission determines whether the user is granted access.

Granting access through either the user account permission setting or the policy permission setting is only the first step in accepting a connection. The connection attempt is subject to the settings of both the user account **dial-in** properties and policy profile properties. If the connection attempt does not match the settings of the user account or policy profile properties, the connection attempt is rejected.

To check the functional level of your domain follow the steps below:

1. On your domain controller logon as administrator
2. Click on **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**
3. In the **Active Directory Users and Computers'** console right-click on your domain and select **Properties**.

4. On the **General** tab under the **Domain functional level:** the text will show what your current domain functional level is at present. i.e. **Windows 2000 native** or **Windows Server 2003 Server** or **Mixed**

   On RM CC3 Network the default functional level is Windows 2000 native

5. If its set to Windows 2000 native or Windows Server 2003 then you do not need to do anything and can exit the console.

6. If the functional level is **Mixed** then in order to **Control access through Remote Access Policy** you need to raise your domain functional level to either Windows **2000 native** or **Windows Server 2003**.

   It is important that you understand what the result of rising the functional level is i.e. what it affects. If you raise your functional level to **Windows 2000 native** then all your domain controllers will need to be running Windows 2000 or above i.e. no Windows NT servers will be allowed access.

   There are other things to consider as well. Review what raising functional level does before carrying out the procedure.

   On RM CC3 network do not raise the domain functional level without speaking to their Technical Support first.

   You should not need to do this on a RM CC3 network unless you have co-existence with a Connect 2.4 network.

4. 1 Creating a Remote Access Policy

In order to complete this procedure you should have assigned a certificate to the IAS (Radius) server by either requesting a certificate from your CA, purchasing a commercial certificate or using a self-signed certificate.

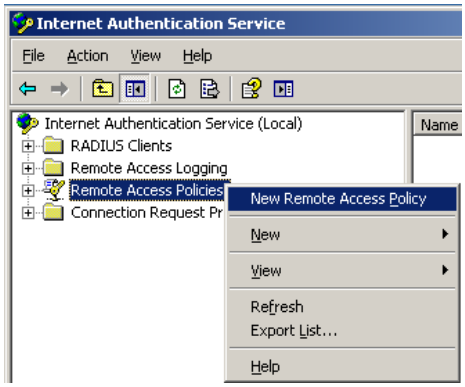
This procedure takes you through creating a Remote Access Policy based on **PEAP** with **MS-CHAPv2** authentication method.

To create a new remote access policy, follow the steps below:

1. Logon to your **IAS** server as administrator

2. Click on **Start** > **All Programs** > **Administrative Tools** > **Internet Authentication Service**

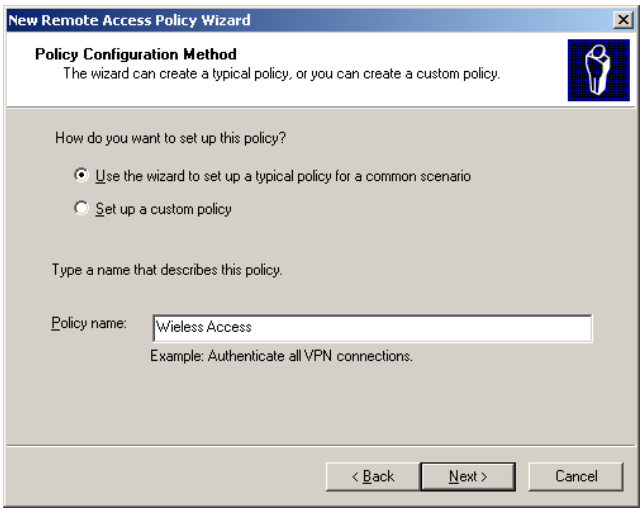
3. On the left hand of the console right-click on **Remote Access Policies** and select **New Remote Access Policy**



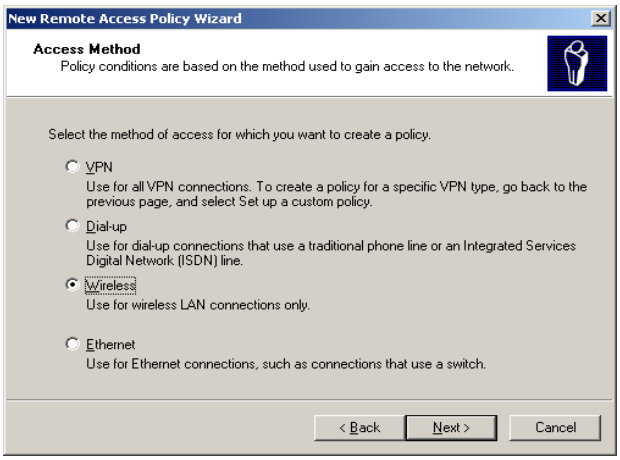
4. At **Welcome to the New Remote Access Policy** wizard click **Next**

5. At the **Policy Configuration Method** screen under the **How do you want to set up this policy?** section leave the default option of **Use the wizard to set up a typical policy for a common scenario**

6. In the **Policy name** box enter a meaningful name for the policy i.e. **Wireless Access** and click **Next**



7. At the **Access Method** screen select the **Wireless** option and click **Next**

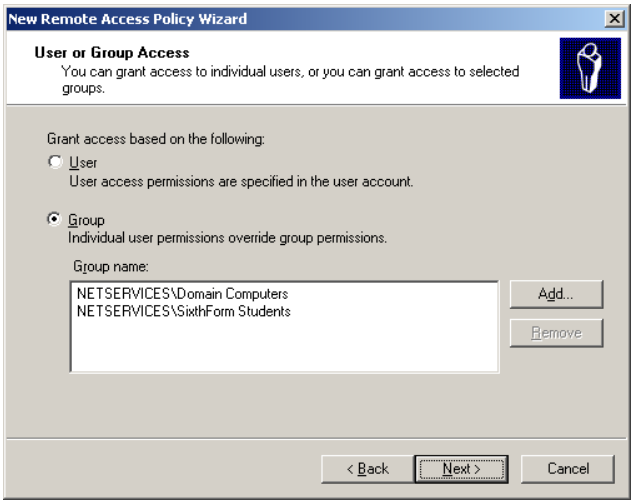


8. At the **User or Group Access** screen select the **Group** option if it is not selected and click the **Add** button to add the groups.

9. At the **Select Group** screen add the Group(s) you would like to be allowed wireless access.

   These groups will be either local or AD security group(s) which contain users and computers who are allowed to access the wireless network. You may want to create group(s) especially for wireless access to narrow down on who has access to wireless network.

   You can also create groups of computers and add in the relevant wireless stations i.e. all Laptops and only allow wireless on these devices.



   By allowing computer access you can get the wireless stations to connect to the network before the user logs in (available on Windows wireless supplicant). This allows for group policy and start-up scripts to be executed prior to the user logging on.

   The computer performs its authentication using the computer account of the station (**machine authentication**). This provides a wired type of connection where connection is available even if the user is not logged on and also lets non-cached (i.e. users who have not logged on to the station) users logon to the station.

10. In the above example the **Domain Computers** group has been added implying that all domain computers can authenticate on the wireless network. At the same time there is a group for users i.e. **SixthForm Students** that only contains 6th form Users.

    On a RM CC3 network there are already various groups created for example XXX Teaching Staff, XXX Non-Teaching Staff, XXX Students where XXX is your three letter site code.

11. Click **Next** when you have added the relevant groups.

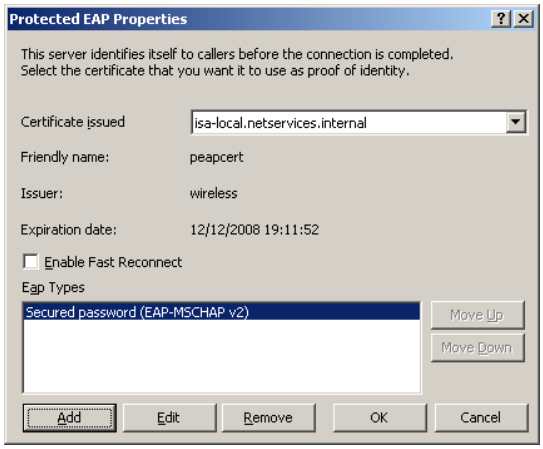
12. At the **Authentication Methods** screen leave the **Protected EAP (PEAP)** selected and click on **Configure**

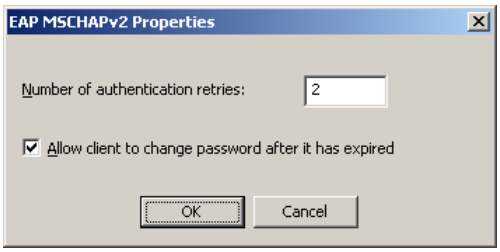
    At this stage if you have not assigned the IAS a certificate then you will get an error message regarding this. Refer to section 6 - ***Assigning Certificate to IAS (RADIUS) server*** *for more information on how to do this.*

13. At the **Protected EAP Properties** screen verify that the certificate issued is correct and is also valid by looking at the **Expiration date.** Also make sure of the following

    Under **EAP Types** the entry reads **Secured Password (EAP-MSCHAP v2).** If it does not, then use the **Add** button, to add it.

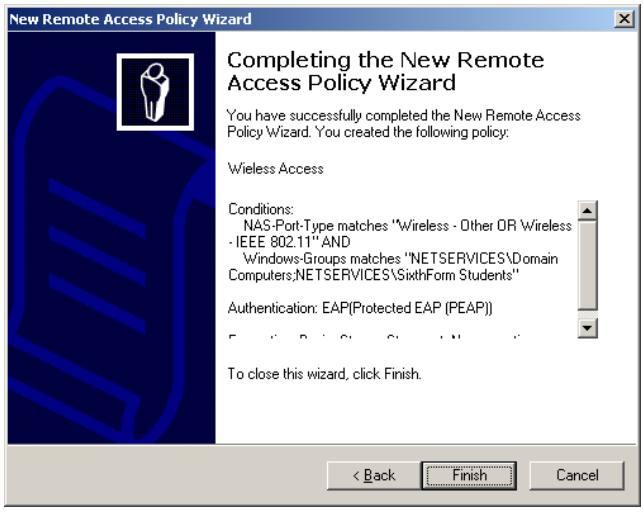
14. At the **Protected EAP Properties** screen select **Secured Password (EAP-MSCHAP v2)** and click the **Edit** button and verify that **Number of authentication retries** is set to **2** and that there is a tick next to **Allow clients to change password after it has expired**



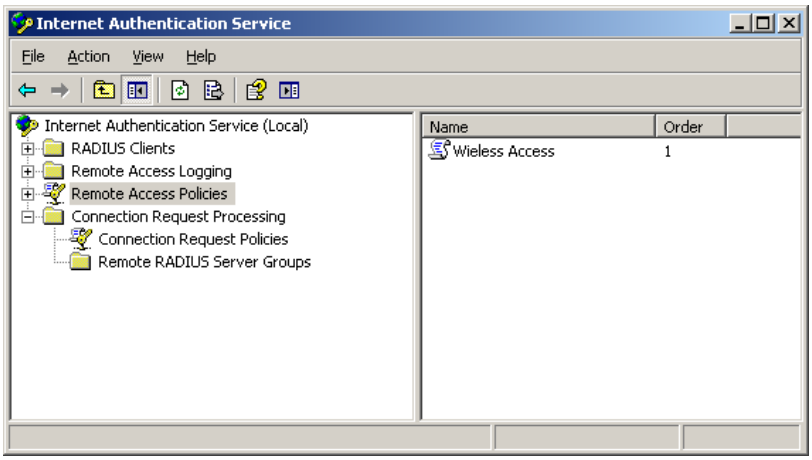


15. Click **OK** > **OK** to return to **Authentication Methods** screen and click **Next**.

16. Click on **Finish** when the **Completing New Remote Access Policy** wizard screen appears.



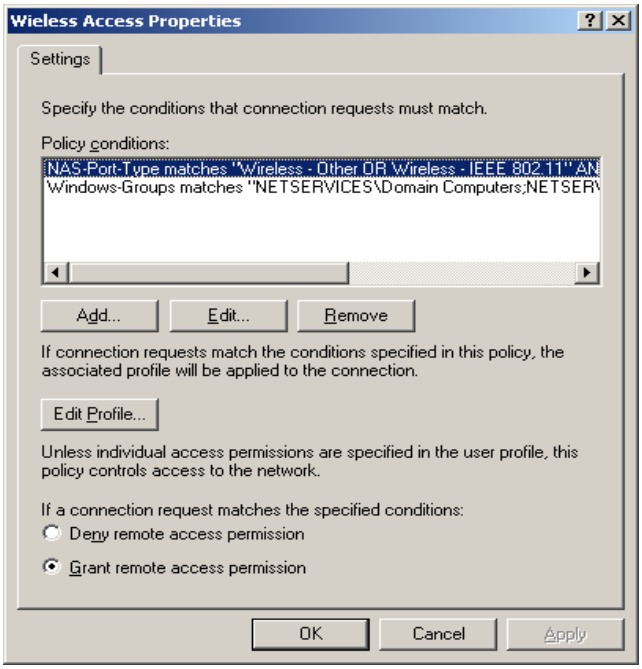
17. You will now see in the Remote Access Policies list on the right-hand side the newly created policy listed.



4.2 Configuring Remote Access Policy

After the policy has been created we need to configure/tweak it so it works the way we want it to i.e. PEAP authentication.

1. **Double-click** on the newly created Remote Access Policy to display the properties of the policy.

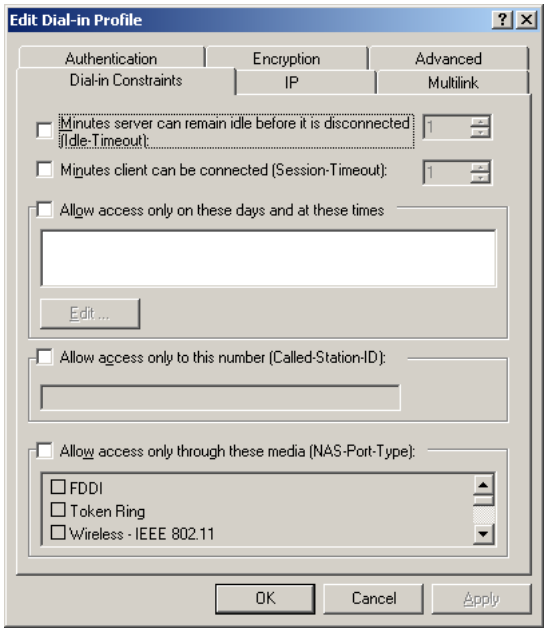


2. The **Settings** tab will be displayed and under the **Policy Conditions** section you will see two entries **NAS-Port-Type** and **Windows-Groups**. These are the two conditions that are set for this policy by the wizard. The **Windows-Groups** will contain the groups that were added in step 9.

   You can add all other conditions as required. Click on the **Add** button to see the list of other conditions.

3. At the bottom under the section **If a connection request matches the specified conditions:** you will see that the **Grant remote access permission** option is selected. This implies that if the above two conditions matche then allow the wireless device onto the network otherwise skip onto the next remote access policy.

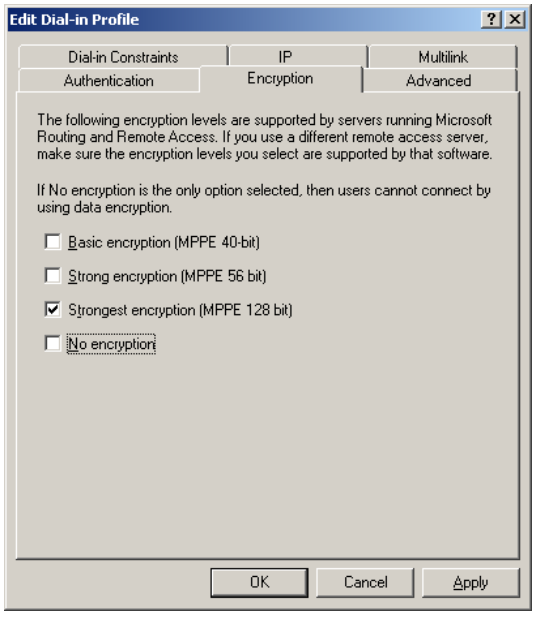
4. We need to edit the **EAP profile** to get the configuration correct for our wireless access. Click the **Edit Profile** button to open the EAP properties.



5. The **Dial-in Constraints** tab will open up as default. On this screen you can set options such as drop the connection after x amount of time, restrict the wireless users to connect at various days and or times only and can drop devices' connection if they are idle for x amount of time. Select the desired settings and click on the **Encryption** tab.

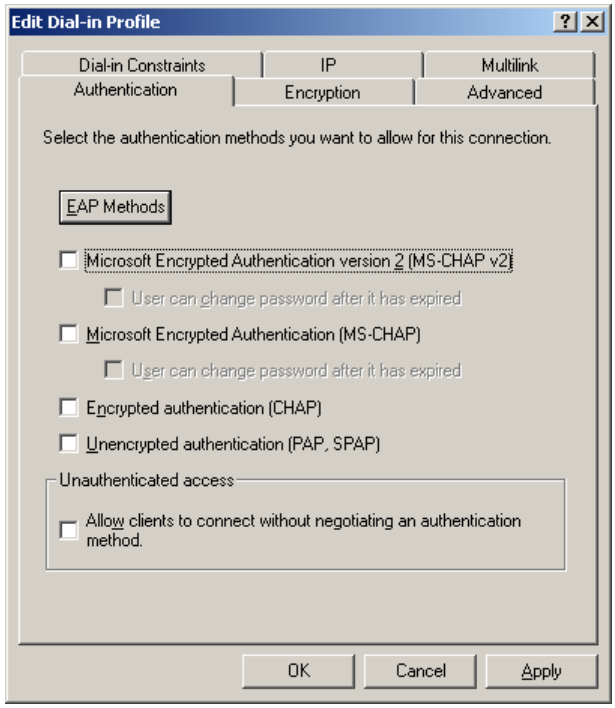
6. At the **Encryption** tab deselect all options except **Strongest Encryption (MPEE 128bit)** to enforce the strongest encryption on the connection and click on the **Authentication** tab.

   If you have Access Points that do not support 128bit encryption you can leave the other lower encryption settings but this will obviously reduce the encryption level.



7. The **Authentication** tab lets you specify which authentication method to use for this connection/policy. Since we are encapsulating the authentication inside EAP packets we don't want to select any authentication methods. PEAP will allow us to authenticate using MSCHAP v2).

   Uncheck all options on this screen and click the **Apply** button and then click on the **EAP Methods** button.



8. The **Advanced** tab lets you configure advance settings such as sending VLAN information to the supplicant (wireless APs, VPN Concentrators, wired switch etc) so that the end station/device is automatically placed in the correct VLAN based on it's identity. This option is beyond the scope of this guide and will not be covered in this guide. This is also the tab where you can specify **Vendor Specific Attributes** (VSAs).

9. Click on the **EAP Methods** button to display the **Select EAP Methods** screen and verify the following:

    a. **EAP Types** lists an entry called **Protected EAP (PEAP)**
    b. Click the **Edit** button to display **Protected EAP Properties** screen
    c. Check that the certificate issued to is correct and valid
    d. Verify the **Enable Fast Connect** box is ticked (do not tick this box if you have Cisco Access Points)
    e. Check the **Eap Types** has **Secured password (EAP-MSCHAP v2)** listed.
    f. Click **OK** to return to previous screen
    g. Click **OK** to close **Select EAP Providers** screen.

10. Click **OK** button to return the **Remote Access Policies** screen.

The remote access policy has now been setup and can be used to authenticate wireless devices.

After you created the remote access policy you can configure it to your needs and add further policies or conditions to the existing policy to get the desired restrictions if required.

5. Configuring Windows Wireless Stations with 802.1x authentication using PEAP

Windows Wireless Client is a built-in 802.1x supplicant of Windows XP. Windows XP SP2 provides better support for wireless in terms of flexibility and support for better encryption. It is recommended that you use Windows XP SP2 (if using MS Windows as your OS). The screenshots are based on configuring a wireless network on Windows XP Professional with SP2.

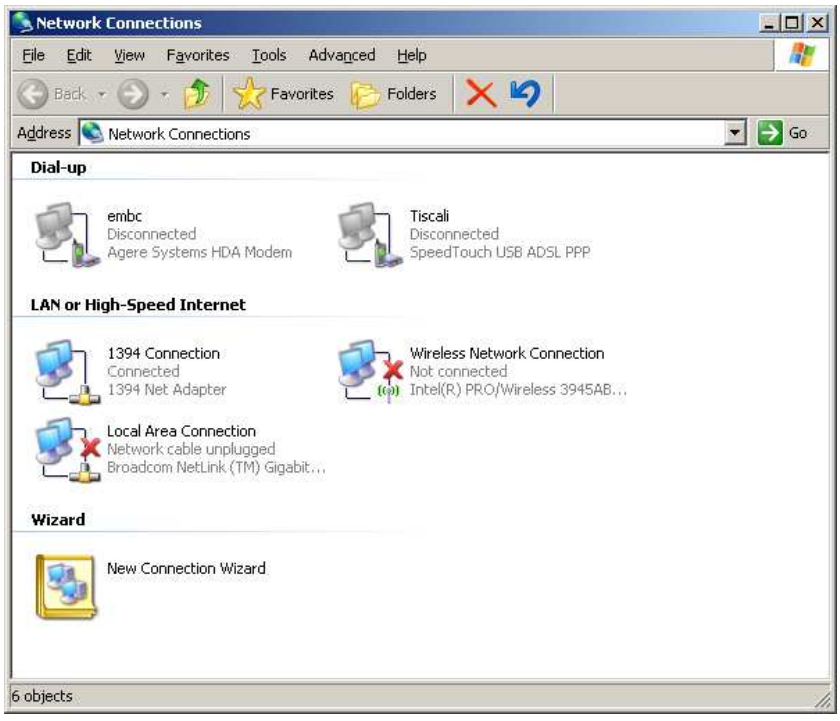
Note: The Windows Wireless Client is not the only supplicant that is available, there are various commercial 802.1x supplicants that can be used as well i.e. **Intel ProSet software**, **Cisco Secure Services Client**, **Juniper Odyssey**.

Intel ProSet software can be downloaded and used for free if you have an Intel wireless card and this will only work with Intel Wireless cards.

5.1 Manually Configuring 802.1x Authentication on Windows XP (PEAP)

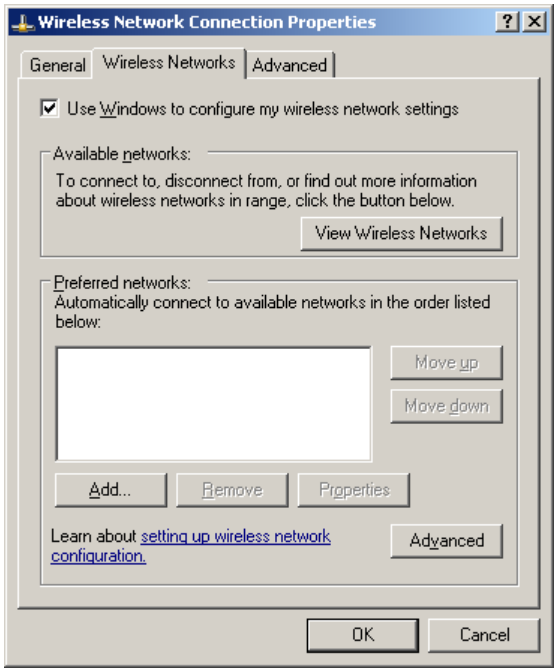
To manually create a new wireless network profile, with 802.1x authentication follow the steps below:

1. Go to **Start** > **Settings** > **Control Panel** > **Network Settings**

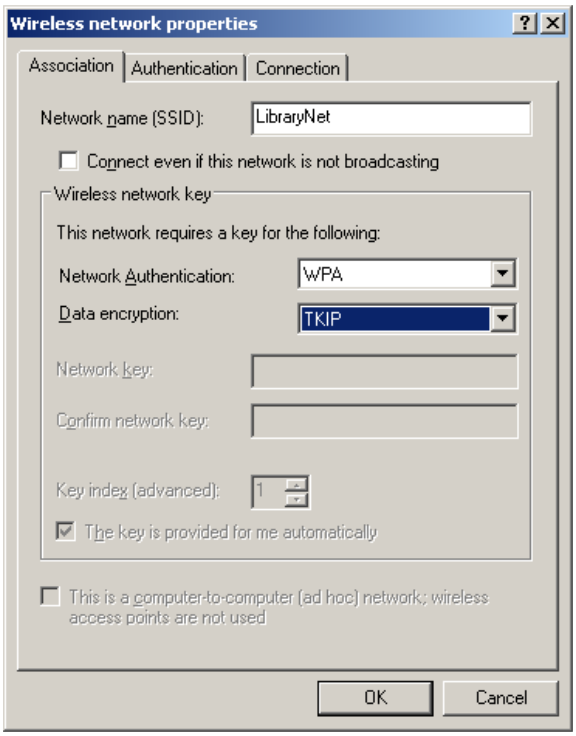


2. Right-click on **Wireless Network Connection** or what ever is the name you have for the wireless network card and select **Properties**

3. Click on **Wireless Networks** tab and make sure that **Use windows to configure my wireless network settings** is ticked.



4. Under the **Preferred Networks** section click on the **Add** button and enter the SSID for your wireless network. SSID is like a name for your wireless network and must match the SSID(s) you configured on your Access Point(s).



If you have disabled the broadcasting of SSID on the access point of Wireless LAN controller you can also put a tick next to **Connect even if this network is not broadcasting** box.

5. In the **Wireless network key** section next to **Network Authentication** select **WPA** (***not WPA-PSK***) from the drop down menu.

In order to have **WPA**, **Windows XP SP2** or above is required. You can also select **WPA2** if your access point supports this level of authentication.

WPA2 also known as **802.11i** and uses **AES** for data encryption which is better than **TKIP**. WPA2 is available by installing the WPA2 post-SP2 patch for Windows XP (**KB893357** – ***http://support.microsoft.com/kb893357***). This patch is included in Windows XP SP3.

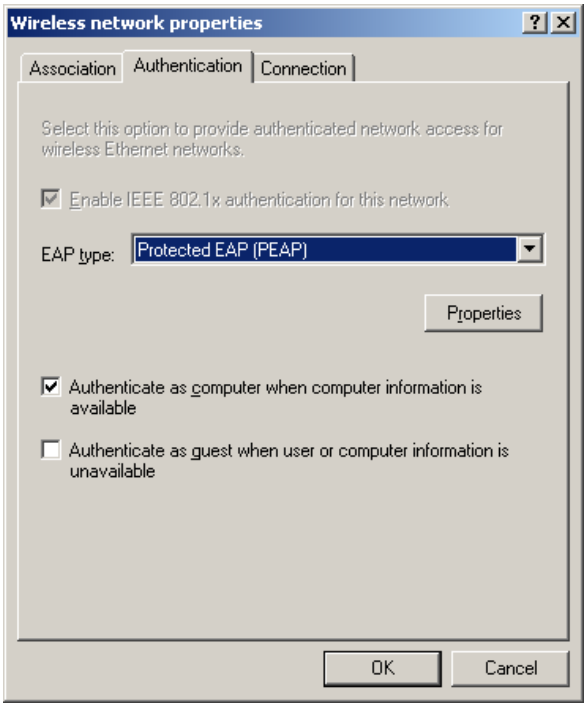
WPA2 is relativity new, and not all Access Points support it, so before you select this option make sure that your Access Point is capable of supporting this feature and that the SSID is configured on the Access Point or Wireless LAN controller to use WPA2.

6. Next select **Data Encryption** and from the drop down menu select **TKIP**

7. You will notice that as soon as you do this the rest of the settings will be greyed out - this is normal.

8. Leave the bottom box **Unticked** - **This computer is a computer-to-computer connection**

9. Now click on the **Authentication** tab and make sure that it appears as in the screenshot below:



10. You will notice that first option (**Enable IEEE 802.1x authentication on this network**) is already ticked and greyed out this is normal.

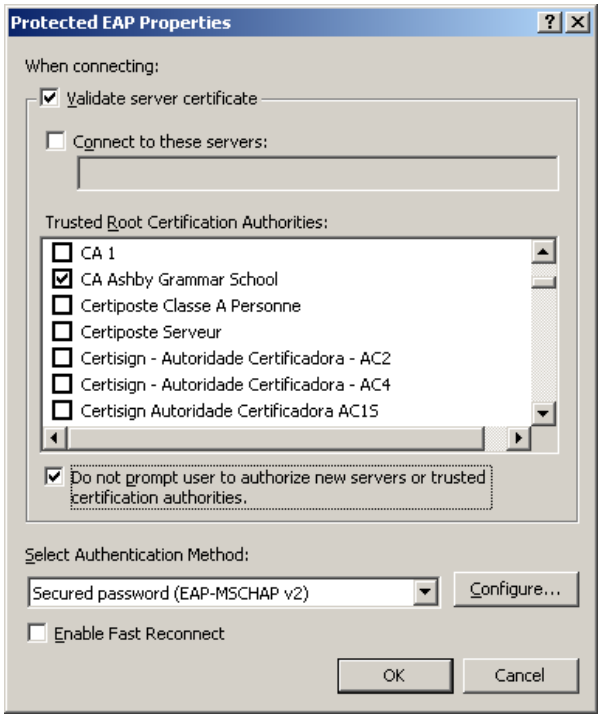
11. Next to **EAP Type** select **Protected EAP (PEAP)** and make sure that there is a tick next to the **Authenticate as computer when computer information is available** option.

    This is a very important option.

    By having this option ticked it tells the supplicant to authenticate using the computer account's password (if joined to a domain). This setting provides a wired like experience where the connection is authenticated and established (using the computer account) prior to the user logging in.

    This allows group policies and other computer specific settings such as start-up scripts to be applied before the user logs into the computer. It also allows other users who do not have a cached profile on the station to login.

12. Once you select **Protected EAP** click on the **Properties** button to display **Protected EAP Properties**.



13. You will notice that "**Validate server certificate**" is ticked. This option tells the client to validate the server certificate of the RADIUS server (IAS) before connecting. This ensures that man-in-the-middle attacks are prevented by actually checking the IAS server's certificate.

14. Under **Trusted Root Certification Authorities**, select the **Root Certificate** of the CA and place a tick next to it. This could be the certificate you bought from a commercial company or your Certificate Authority or self-signed certificate that you imported to the station's **Certificate Trusts List (CTL)**

    For stand-alone CA's (in non-AD environment) and self-signed certificate's you will need to manually import the certificate to the appropriate store on the wireless enabled device. If you have an Enterprise CA or stand-alone CA (in an AD environment) installed on your domain then all your computers joined to the domain will automatically have the Root Certificate (of CA) installed in the correct place:

    Refer to section 6 - **Assigning Certificate to the IAS (RADIUS) server** for more information.

15. Tick the box next to **Do not prompt user to authorize new servers or trusted certification authorities**

16. Make sure **Secured password (EAP-MSCHAP v2)** is selected under **Select Authentication Method:** section

17. At the bottom, put a tick on "**Enable Fast Reconnect**". Do not tick this box if your APs are from Cisco systems. There are issues with these at present, however do test it to see if it does work, if not then disable this option.

18. Now click on the **Configure** button and make sure that in the **EAP MSCHAPv2 Properties** window, the option **Automatically use my Windows logon name and password (and domain if any).** is ticked.

19. Click on **OK**| **OK** | **OK** | **OK** to close all the properties windows.

20. This completes the setup and configuration of the wireless station.

5.2 Automatically Configuring 802.1x authentication (PEAP) using GPO

Windows Server 2003 with SP1 and above (including Windows Server 2003 R2) allows wireless configuration to be deployed (pushed out) using a group policy. This provides an ideal way to configure multiple stations with the same wireless settings and profile(s).

In order for this procedure to be completed you need to have a working Microsoft Active Directory environment.

Note: This procedure will disable any third-party supplicants such as **Intel ProSet software**, **Cisco Secure Services Client (AEGIS)**, **Odyssey** etc if they are installed on the wireless station. It will make the windows supplicant the default and will populate the wireless settings as per group policy.

To configure configuration of wireless profile using GPO follow the steps below:

1. On your domain controller logon as administrator

2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**

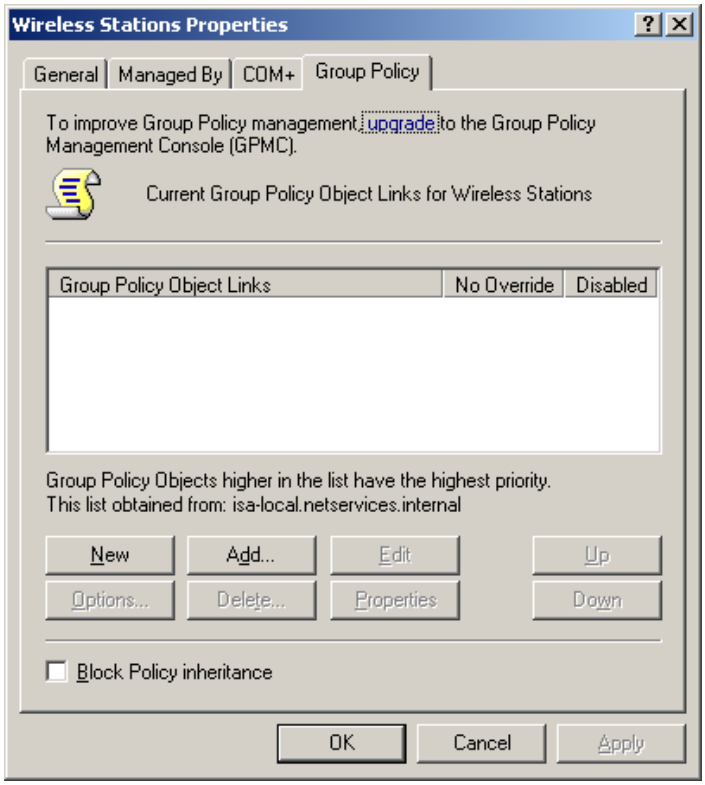
3. Expand the domain and select an **OU** (**Organisation Unit**) to which you want to apply the wireless configuration (via group policy)

   It is best to create a security group in Active Directory with all the wireless stations that are joined to the domain i.e. **All Wireless Laptops**.

   You can then use this group in group policy security settings to only apply the group policy to this group or to target only the stations that are members of the group rather than the whole OU or domain.

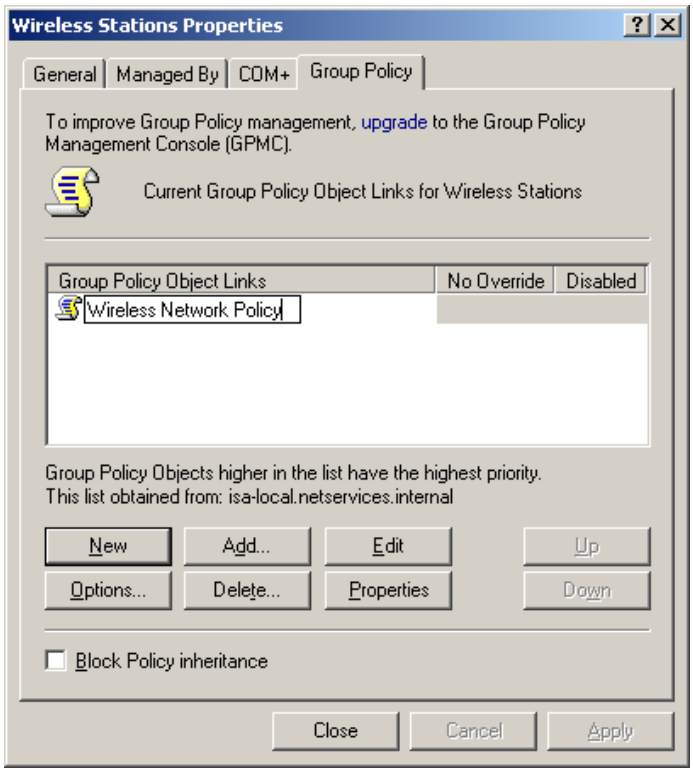
4. Right-click on the selected **OU** and choose **Properties** (in the example the OU is **Wireless Stations**)

5. Click on the **Group Policy** tab to display and list all the group policies located at this **OU**.



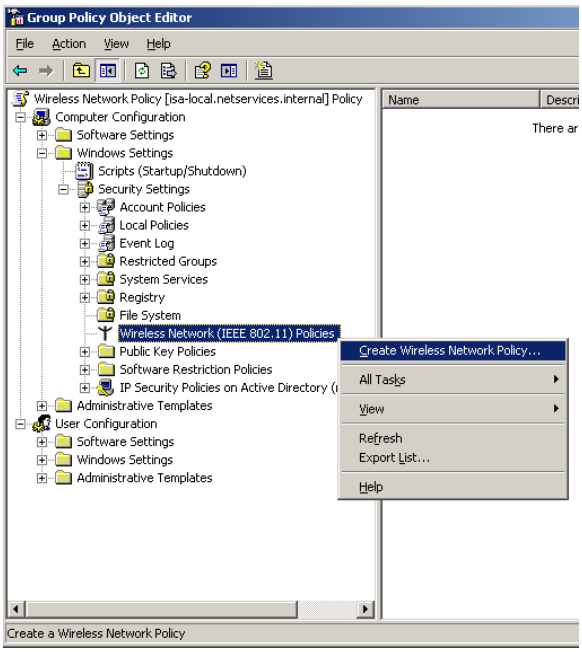
6. Click the **New** button to create a new group policy object (GPO).

7. The newly created GPO will have the name of **New Group Policy Object** and will be highlighted. Rename the newly created GPO to something meaningful i.e. **Wireless Network Policy** and click the **Edit** button.



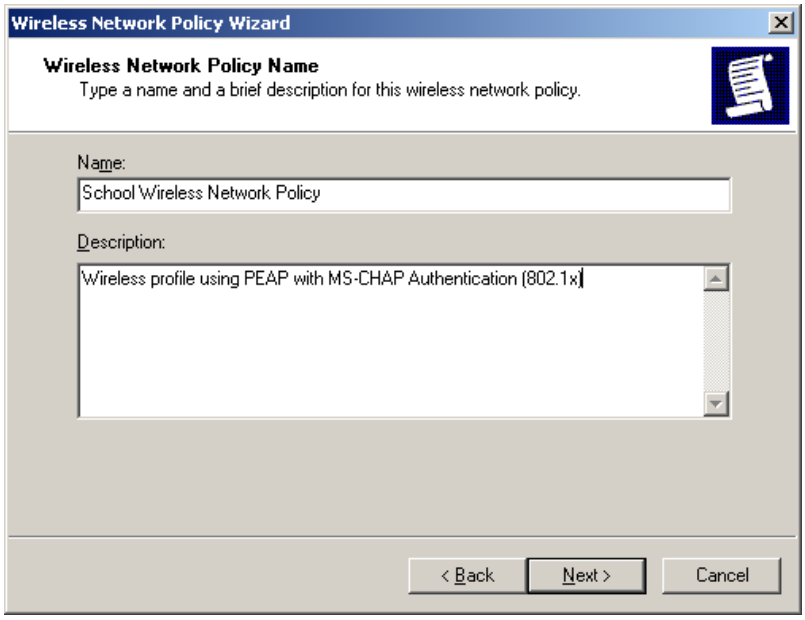
8. The Wireless Network Policy settings will be displayed. Expand **Computer Configuration** > **Windows Settings** > **Security Settings**

9. Under **Security Settings** right-click on **Wireless Network (IEEE 802.11) Policies** and select **Create Wireless Network Policy**



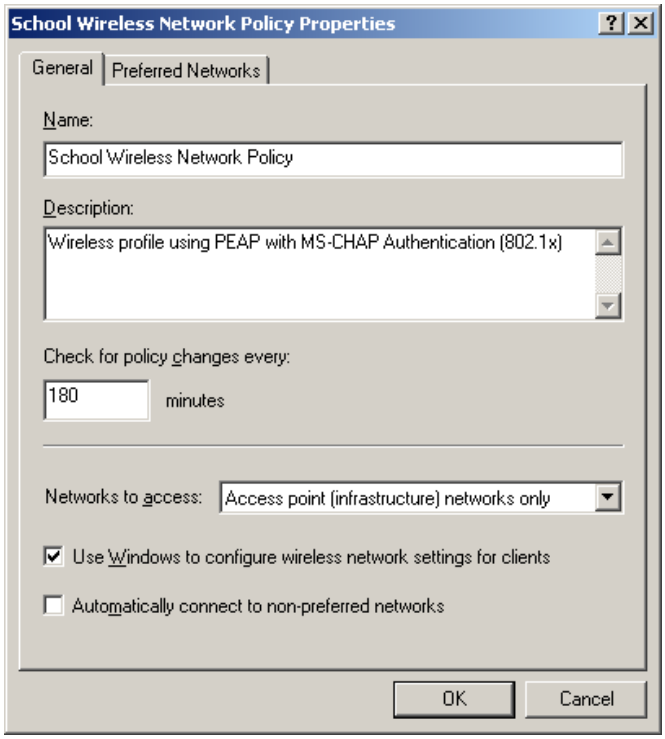
10. At **Welcome to the Wireless Network Policy wizard** click **Next**

11. At **Wireless Network Policy Name** screen give a suitable name to the wireless policy and enter a description for it's purpose and any other information or comments and click **Next**

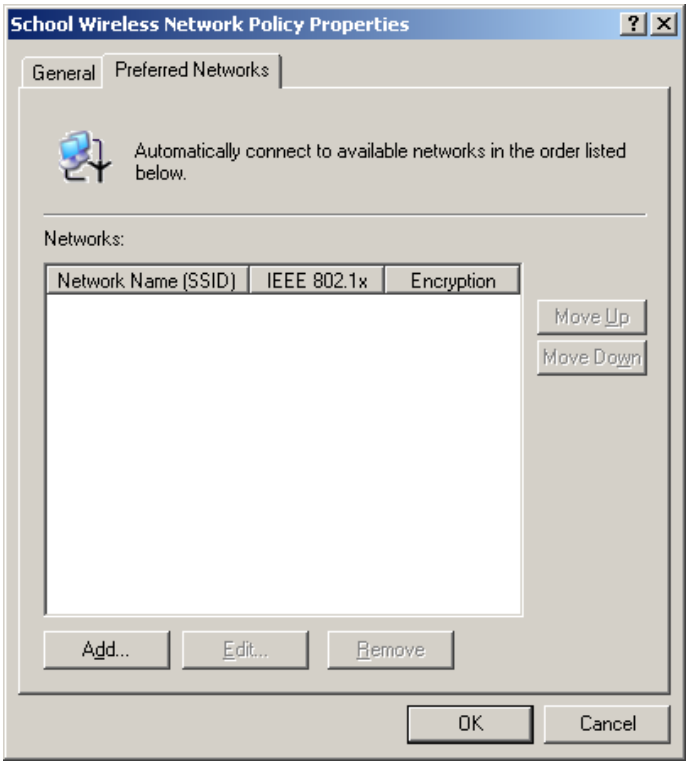


12. At **Completing the Wireless Network Policy wizard** leave the tick next to **Edit Properties** and click **Finish**

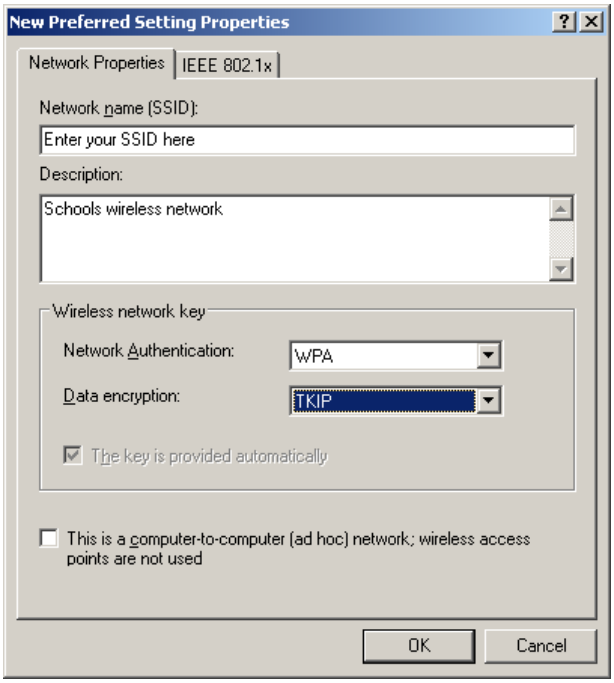
13. The **General** tab of the newly created Policy is displayed. Select **Access Point (infrastructure) networks only** from the drop menu next to the **Networks to access:** section. Leave the rest of the settings as they are and click on **Preferred Networks** tab.



14. At the **Preferred Network** screen click the **Add** button to add a new network profile.



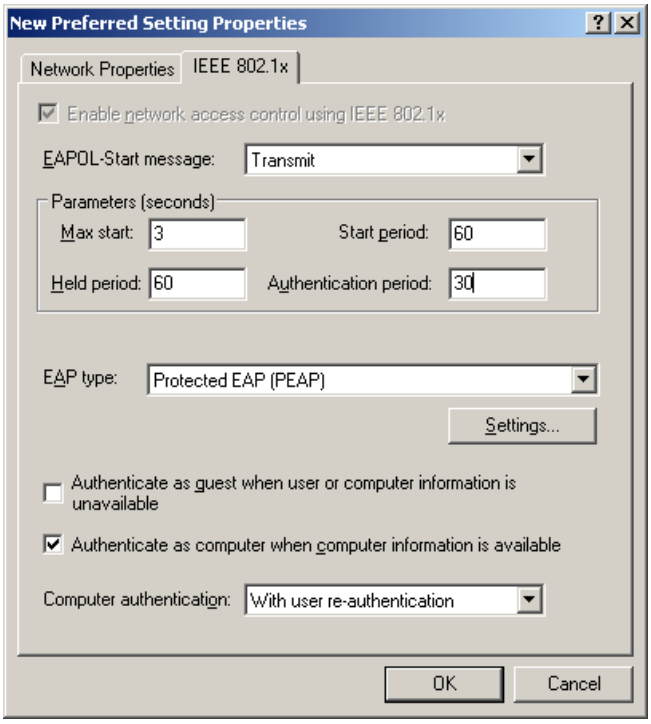
15. At the **New Preferred Settings Properties** screen enter the SSID of your wireless network under the **Network name (SSID):** box and enter a meaningful description in the **Description** box.



16. Under the **Wireless network key** section select **WPA** as the **Network Authentication** and **TKIP** as the **Data Encryption**.

17. Click on the **IEEE 802.1x tab** to display 802.1x settings

18. On the **IEEE 802.1x** tab select **Protected EAP (PEAP)** as the **EAP type:**

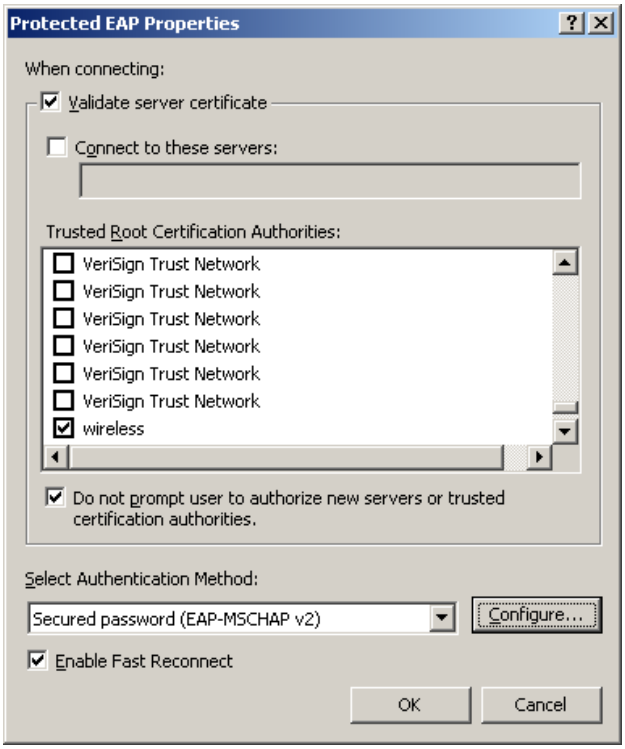


19. Ensure there is a tick next to **Authenticate as computer when computer information is available**

20. Click on the **Settings….** button to display **Protected EAP Properties**

21. At the **Protected EAP Properties** screen make sure that **Validate server certificate** is ticked.

22. Under the **Trusted Root Certification Authorities** box put a tick next to your Certificate Authority's **Root certificate** or **self-signed certificate**.



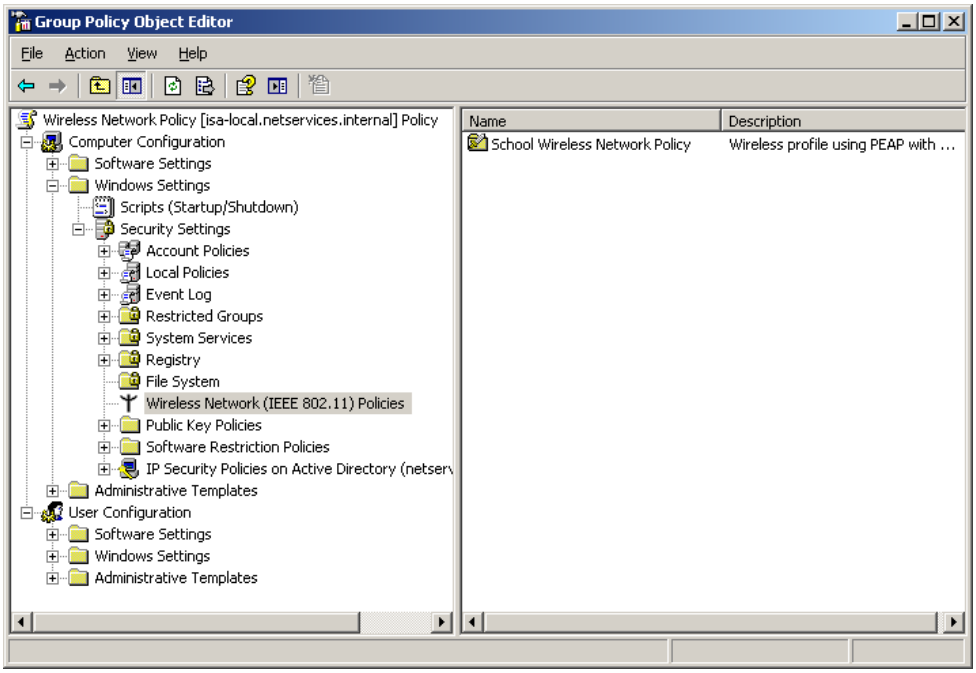
23. Ensure that the **Do not prompt user to authorize new servers or trusted certification authorities** box is ticked as well as **Enable Fast Connect** (Do not tick this box if are using Cisco Access Points)

24. Select **Secured password (EAP-MSCHAP v2**) if it is not already selected below the **Select Authentication Method** section.

25. Click the **Configure…** button and ensure that the **automatically use my Windows logon name and password (and domain if any)** option is ticked.

Enabling this option allows the supplicant to present logged in user or computer credentials to the RADIUS server.

26. Click **OK | OK | OK | OK | OK | OK** to return to the Group Policy Settings screen where you will see that the newly created Wireless Policy will be listed.



27. Close the Group Policy window and exit the **Active Directory Users and Computers console**.

When the station next time refreshes the group policy the new wireless network settings configured in the above policy will be applied to the end stations.

The above example was based on configuring a GPO at an OU level called Wireless Stations.

Just to re-iterate the brief comment on Step 3 regarding OU and group policy, a more flexible way to apply specific group policies (where you want to target a specific set of stations) is to create and use security groups. These group(s) should contain all stations that you want the policy to apply to. This allows you to add the GPO on any OU and still achieve the goal of applying the policy to specific stations.

Note about speeding up GPO

As you can see the above group policy only contains settings in the **Computer Configuration** part and does not alter anything in the **User Configuration** so we don't need to process the **User Configuration** part. In order to speed up the GPO process we could disable the User Configuration for this GPO so it is not processed.

To do this at the group policy tab locate the GPO you created and click on the **Properties** button. When the **Properties** screen is displayed place a tick next to **Disable User Configuration settings** under the **Disable** section and click **OK**.

5.3 Forcing Machine Authentication Only

By default on Windows XP SP2 and Windows 2003 Server the windows supplicant (**Windows Wireless Client)** will attempt to authenticate using the machine authentication first and then will re-authenticate the user when he/she logs in. In some situations you don't want to use user authentication since the station is used by multiple users but you only want to allow domain-joined wireless stations to authenticate and connect to the wireless network.

The default behaviour of Windows XP SP2 will require the remote access policy on your IAS server to be configured to allow both the wireless stations (computer accounts) and user groups.

If your situation does not demand machine authentication only then ignore this section.

The above is achieved by modifying the windows registry.

1. On the wireless station i.e. Windows XP PC logon as administrator.
2. Click **Start** > **Run** and type **regedit** in the **Ru**n box and press **Enter**.
3. In Registry Editor navigate to the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\General\Global

4. On the right-hand side double-click on the **AuthMode** entry and in the **Value box** type in **2**

   If the entry does not exist then create an entry called **AuthMode** as a **DWORD** and give it a value of **2**.

5. Close the Registry Editor

You will find that the supplicant will now not perform any user authentication after the computer authentication is successful.

6. Assigning Certificate to the IAS (RADIUS) server

In a PEAP/MS-CHAPv2 environment the IAS server requires a certificate to be installed so the supplicants can validate the identity of the IAS (Radius) server before connecting. Certificates can be obtained in various ways. Here are the following ways in which you can generate and assign certificates to the IAS (Radius) server.

Enterprise Certificate Authority/Stand-Alone Certificate Authority

If your domain has an Enterprise CA or Stand-Alone CA installed then the procedure for assigning the certificate will be greatly simplified. The Enterprise CA is the highest trust in the Certificate hierarchy. You can install a CA on any of your domain controller or member servers. This will be responsible for generating the certificate to your clients.

An RM CC3 network has a CA running on their forest root server (first Domain Controller (DC)) by default so if you are using a RM CC3 network then you do not need to install a CA and can use this method to generate and assign a certificate to your IAS server.

Purchasing a Certificate from a Company

You can also purchase a certificate from a commercial company such as VeriSign, Thawte etc. However this do incur a cost but the benefit is that most of the computers would automatically trust a certificate from these companies since they are already installed in the **Trusted Root Certification Authorities** store on most computers. This section is not covered in this guide.

Self-Signed Certificate

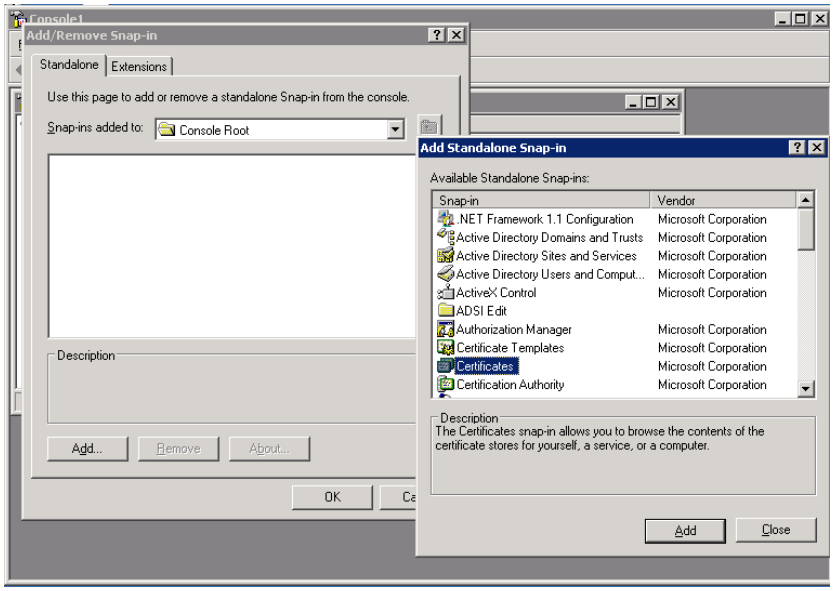
You can also generate a self-signed certificate if you don't want to purchase a certificate from a company or install a CA. You can do this using the IIS 6.0 resource kit tool call **selfssl.exe**. This allows you to generate a self-signed certificate which you then export (with public key) and deploy to wireless devices.

6.1 Obtaining a Certificate using a Enterprise CA/Stand-Alone CA

This procedure assumes that you have a working Enterprise CA/Stand-alone CA installed on your domain and that it is reachable.

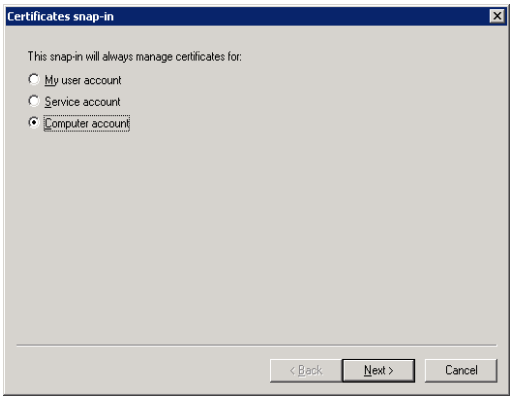
Only follow this procedure if you have Enterprise or Stand-Alone CA available on your domain. RM CC3 network has a Enterprise CA installed on the first DC (forest root server)

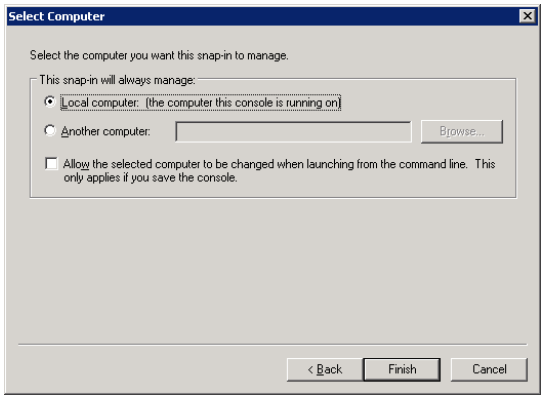
1. On your IAS server logon with a domain administrator account such as administrator.
2. Click **Start > Run** and type **MMC** to open management console.
3. Click **File** > **Add/Remove Snap In**
4. There will now be an **Add/Remove Snap In** box which allows you to **Add** or **Remove** different snap-ins for management.
5. On the drop down menu select **Console Root** and then click **Add.**



6. This will bring up a box with all the Snap-Ins available. Select the **Certificates** snap in and then click **Add.**

7. Click **Computer Account** > **Next** make sure **Local Computer: (the computer this console is running on)** is selected and then click on **Close** and then click **OK**





8. You will now see that the certificate snap in has been added.

Now that the certificate snap in has been loaded, you can assign a certificate to the IAS server by requesting a certificate from a CA.

9. Expand the **Certificate (Local Computer)** click on **Personal** store

10. Right click on **Certificates** select **All Tasks > Request New Certificate.**

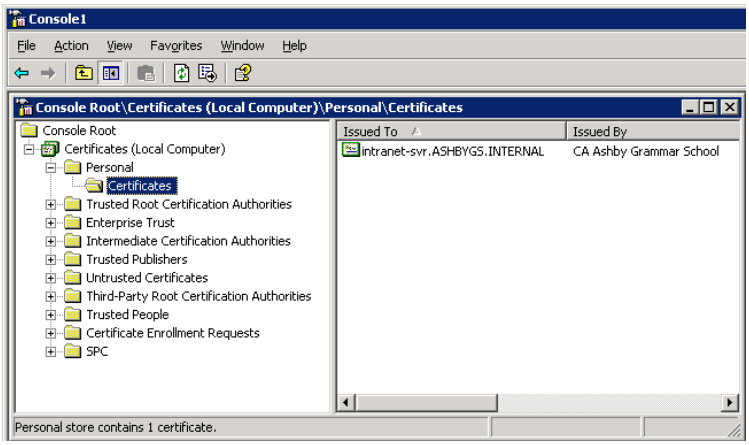
11. This will open a wizard which will take you through creating a new certificate.

12. The first step is to select the certificate type. Make sure **Server** or **Computer** is selected and then click **Next**. (Make sure Advanced is deselected unless you are competent with cryptographic properties)

13. Give a friendly name to the certificate and also provide a description for what the certificate is going to be used for and click **Next**

14. The final box will give you a summary of the details entered and issue a certificate.

15. The certificate will now be listed in the right-hand pane.



If you have an Enterprise CA installed and you have obtained a certificate from this CA then you **do not need** to copy the Enterprise CA's **Root certificate** to your stations, since this will be done automatically when the station is joined to the domain.

If you are going to be authenticating non-domain stations or devices then you need to export the Root certificate from your Enterprise CA server and copy it to your non-domain member station or device's **Certificate Trust List** (**CTL**). You will need to import the exported certificate in the **Trusted Root Certification Authorities** store.

If you are using a stand-alone CA (in a ***non-AD environment***) to obtain a certificate then you will again need to copy the stand-alone CA's Root certificate to the stations.

A Stand-Alone CA installed onto an Active Directory domain environment (*installed by a member of domain administrators group*) will automatically copy the CA's Root Certificate to stations when they are joined to the domain.

The Root Certificate can be imported manually to non-domain stations or deployed automatically using GPO if stations are joined to the AD domain. (***Refer to section 5 for deploying Root Certificate to stations***).

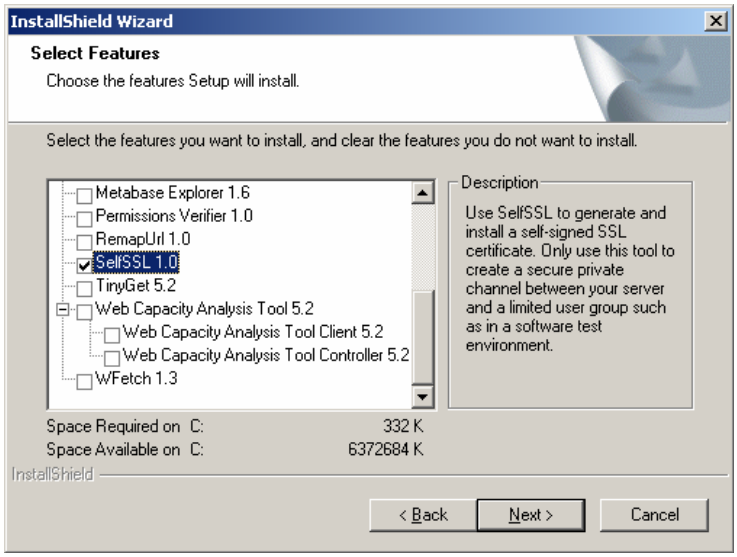
6.2 Generating and assigning a Self-Signed certificate using SelfSSL tool

If you use this method then you will need to export this root certificate and import it to all your stations (whether they are joined to your domain or not), again this can be done manually or automatically by using GPOs.

1. Download the **IIS 6.0 Resource Kit** from the Microsoft site to a location on the IAS server.

2. Double-click on the resource kit file you downloaded to start the installation.

3. Select the Path to install it to and then on the **Select Features** screen, untick all options except for SelfSSL 1.0 and click N**ext** and finish the finish the install.



4. Open a **Command Prompt** and go to where you installed the SelfSSL tool i.e. **C:\Program Files\IIS Resources\SelfSSL**.

5. To generate a self-signed certificate type the following:

   selfssl /N:CN=servername.domain.com /K:1024 /V:1095 /S:1 /P:443

   Where **servername** is the name of your IAS server and domain.com is the name of your domain.

   CN = is the common name for the certificate
   K = the number of bits for the RSA key
   V = the number of days the certificate will be valid for (1095 is 3 years assuming 365 days in a year)
   S = site number in IIS (not applicable to this, but you should still type it in)
   P = port number (not applicable to this, but you should still type it in)

6. Press **Enter** to generate the certificate. If you have not got IIS installed on this server then you may get an error message but this can be ignored since we don't need IIS in order to generate the certificate for our purpose.

To view the certificate you just created follow the steps below:

7. On your IAS server logon with a domain administrator account such as administrator.

8. Click **Start > Run** and type **MMC** to open management console.

9. Click **File** > **Add/Remove Snap In**

10. There will now be an **Add/Remove Snap In** box which allows you to **Add** or **Remove** different snap-ins for management.

11. On the drop down menu select **Console Root** and then click **Add.**

12. This will bring up a box with all the Snap-Ins available. Select the **Certificates** snap in and then click **Add.**

13. Click **Computer Account** > **Next** make sure **Local Computer: (the computer this console is running on)** is selected and then click on **Close** and then click on **OK**

14. Expand the **Certificate (Local Computer)** click on **Personal** store and check on the right hand side that your certificate is listed.

6.3 Exporting Self-signed certificate

Because self signed (i.e. the server itself is a signing authority as well) certificates are generated on the server itself using the **Selfssl.exe** tool, the certificate that you export is from the **Personal** store rather than the usual **Trusted Root Certification Authorities** store. Follow the steps below to export the certificate.

You should only carry out this procedure if you have used the selfssl tool to generate a certificate for your IAS server.

If you have obtained a certificate from an Enterprise CA on your domain then you do not need to complete this section.

To export the certificate, follow the steps below:

1. Click **Start > Run** and type **MMC** to open management console.

2. Click **File** > **Add/Remove Snap In**

3. There will now be an **Add/Remove Snap In** box which allows you to **Add** or **Remove** different snap-ins for management.

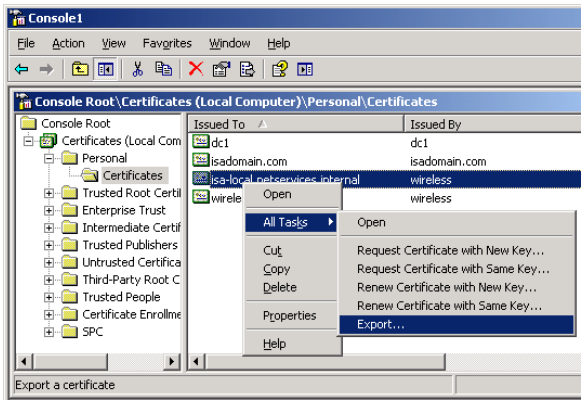
4. On the drop down menu select **Console Root** and then click **Add.**

5. This will bring up a box with all the Snap-Ins available. Select the **Certificates** snap in and then click **Add.**

6. Click **Computer Account** > **Next** make sure **Local Computer: (the computer this console is running on)** is selected and then click on **Close** and then click on **OK**

7. Expand the **Certificate (Local Computer)** click on **Personal** store.

8. Right-click on the certificate and select **All Tasks** > **Export** to start the export wizard.

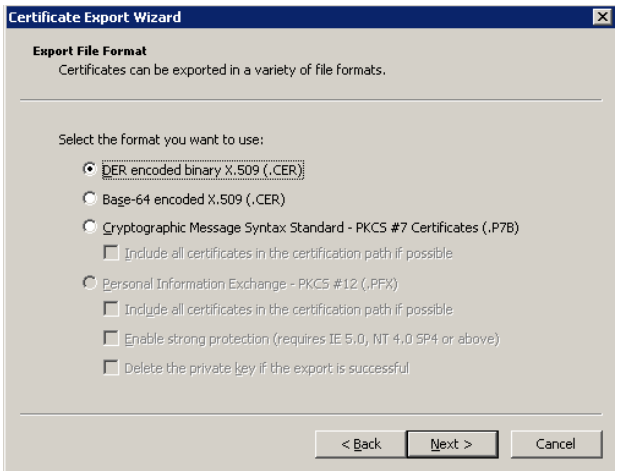


9. Click **Next** when the export wizard appears

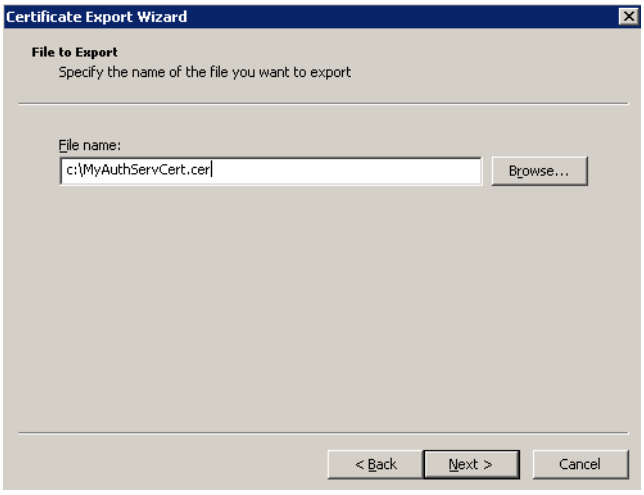
10. Choose **No, do not export private key** option and click **Next**

Private Key should not be exported unless for backup purposes or transferring to another server. Exporting the private key otherwise may be compromise your certificate.

11. Choose the **DER encoded binary X.509 (.CER)** option to allow importing to other devices such as Windows Mobile devices which can only import certificates in DER format.



12. Click **Next** to display the **File to Export** screen. Browse to a location where you want the certificate to be saved to and click **Next**



13. On the summary screen click on **Finish** to export and save the certificate to a file.

14. In the above example the certificate is saved to the root of the **C** drive with a filename of **MyAuthServCert.cer**

15. Click **OK** when the message **the export was successful** appears.

    You should now copy this certificate to your memory stick or other location from where you can deploy the certificate to your wireless devices.

    Importing this certificate to your wireless device's Certificate Trust List (CTL) will allow them to trust the IAS server and will aid the identification of the IAS server

6.4 Exporting Root Certificates of Enterprise CA/Stand-Alone CA

In order for the wireless devices to trust the certificate of the IAS (Radius) server your wireless devices need to have the Root Certificate **of the singing authority who signed the certificate to the IAS server.**

You only need to export this certificate (and later import it) if your wireless clients are not joined to the domain or you have a stand-alone CA installed that does not participate on the domain. As stated earlier in the guide if your IAS server was issued a certificate by an Enterprise CA on your domain then you don't need to have this certificate on your stations (that are joined to the domain) since it will be automatically completed when the station is joined to the domain.

It is a good idea to have a copy of this certificate just in case you want to authenticate non-domain devices.

To export the trusted root certificate from an Enterprise CA follow the steps below:

1. Logon to any of your domain controller or member servers or a workstation that is joined to the domain

   On a RM CC3 network it is best to use the forest root server (1st DC)

2. Click on **Start** > **Run** and type in **MMC**

3. Click **File** > **Add/Remove Snap In**

4. There will now be an **Add/Remove Snap In** box which allows you to **Add** or **Remove** different snap-ins for management.

5. On the drop down menu select **Console Root** and then click **Add.**

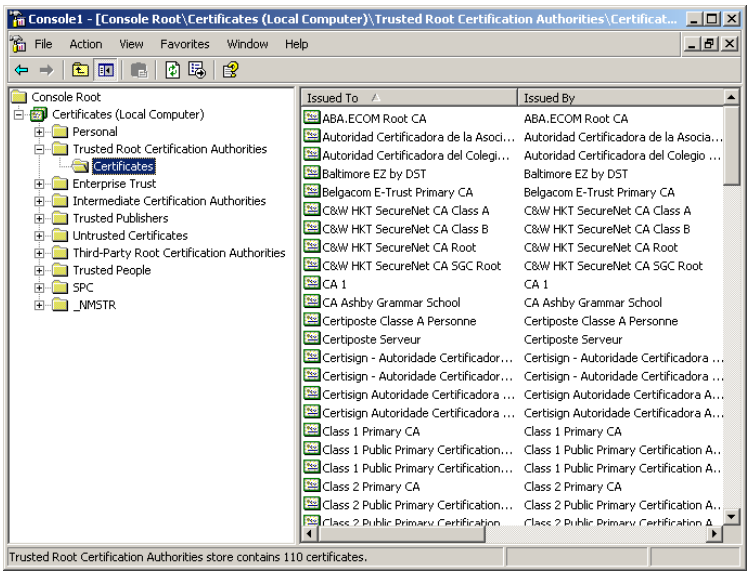
6. This will bring up a box with all the Snap-Ins available. Select the **Certificates** snap in and then click **Add.**

7. Click **Computer Account** > **Next** make sure **Local Computer: (the computer this console is running on)** is selected and then click on **Close** and then **OK**

8. Expand the **Certificate (Local Computer)** and then expand **Trusted Root Certification Authorities**.

9. Click on the **Certificates** under **Trusted Root Certification Authorities**

10. You should now see a list of all certificates (root certificates of all authorities) that your station trusts



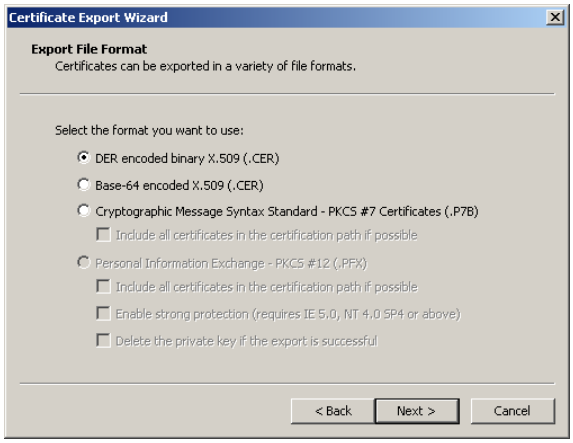
11. From the list right-click on the certificate that identifies your Enterprise CA's Trusted Root Certificate and select **All Tasks** > **Export**

On a RM CC3 Network it will be something like CA Schoolname where schoolname is the name of your school.

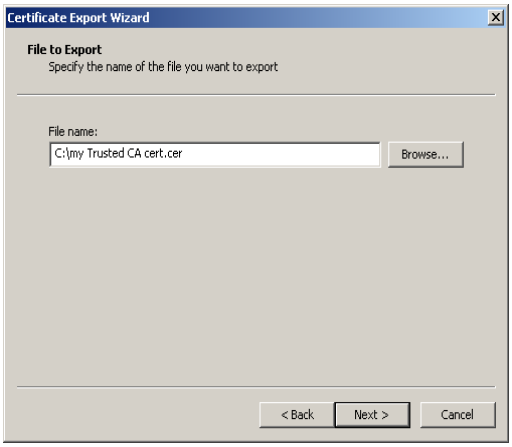
12. When the **Welcome to the Certificate Export wizard** appears click **Next**

13. If you are exporting the certificate from the server where the **Certificate Authority** (**CA**) is installed you will be asked if you want to export the **Private key.** Select the **No, do not export the private key** option and click **Next.**

    If not then the Export File Format screen will appear. Leave the default option selected **- DER encoded binary X.509 (.DER)** and click **Next**



14. At the **File to Export** screen click the **Browse** button and select a path to save the certificate to and give the certificate a friendly filename i.e. **C:\my Trusted CA cert.cer** and click **Next**



15. On the summary page click **Finish** to save the certificate to the path you specified in step 14.

16. When the message **export was successful** appears click **OK**. The Root certificate of your Enterprise CA is now exported.

7. Deploying Root Certificate of CA to stations

7.1 Manually installing a Root Certificate to your windows stations

You should only use this section if you are trying to authenticate non-domain stations or PDAs running an OS such as Windows Mobile.

Root certificate contains the public key of your certificate authority (CA) and is needed on the wireless devices to validate the identity of the authentication server i.e. IAS (Radius).

Since this is the same CA that has issued a certificate to the IAS server, if your station trusts this certificate authority then the station automatically trusts the IAS server's certificate because it was signed by the CA that your station now trusts.

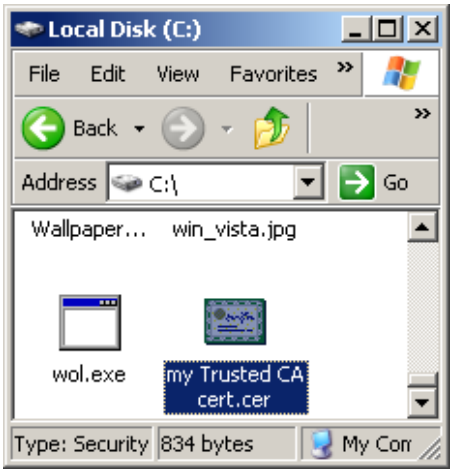
Now read the above paragraph again.

If you have exported the Root certificate of an Enterprise CA that is installed on your domain then you do not need to import the root certificate to your domain joined stations, since they will automatically have had this certificate installed when they were joined to the domain.

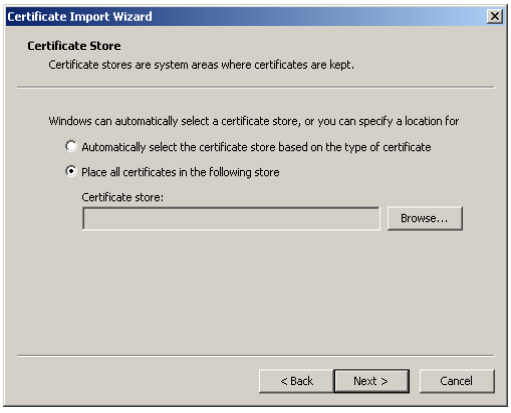
You will need to have the exported certificate file available (i.e. on a floppy disk, memory stick or on accessible network location) before you can follow this procedure.

To import the Certificate Authority's root certificate into the stations' **Certificate Trust Lists** (CTL) follow the steps below: (the screenshots shown here are based on MS Windows XP SP2)

1. On your station locate the exported root certificate file (in this case it is stored on the root of the C drive on the station).



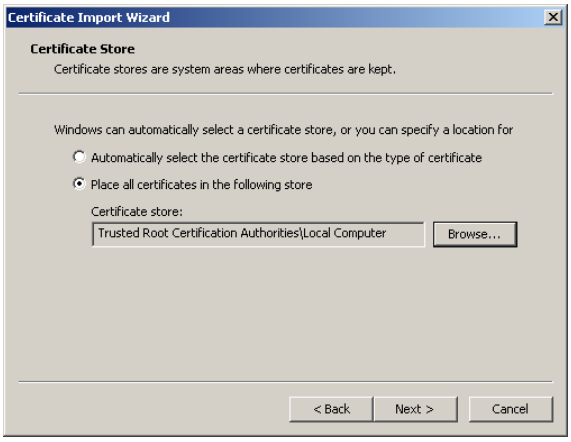
2. Right-click on the root certificate file and select **Install Certificate**
3. At the **Welcome to the Certificate Import Wizard** click **Next**
4. At the **Certificate Store** screen select the second option **Place all certificates in the following store**



5. Click the **Browse** button and from the **Select Certificate Store** screen put a tick in the box next to **Show Physical store** to reveal extra stores.

6. Expand the store called **Trusted Root Certificate Authorities** and select **Local Computer**. (You may need to scroll up/down to select this option). **It is important that you select Local Computer.**

7. Click **OK** to return to the **Certificate Store** screen and click **Next**



8. At the **Completing Certificate Import Wizard** summary screen click on **Finish**

9. When the **export was successful message** appears click **OK**. The root certificate is now imported onto your station's **Certificate Trust Lists (CTL)**.

It is possible to import the certificate to Mac OS X and Linux and get these stations/devices authenticated. These will need to have the correct 802.1x supplicant installed in order to authenticate correctly.

7.2 Automatically Deploying Root Certificates using GPO

You should only follow this procedure if you have used the selfssl.exe tool to generate a self-signed certificate.

You will need the exported root certificate file to complete this procedure. The procedure outlined here will make the whole of your domain trust the IAS server's self-signed certificate.

Once again on a RM CC3 network this procedure is not required since it has an Enterprise CA installed and you should have requested a certificate from this CA.

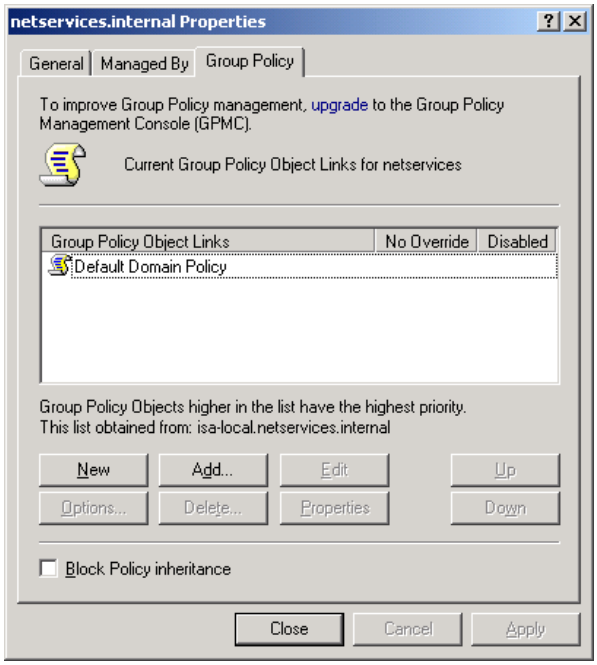
To deploy the root certificate using group policy object follow the steps below:

1. On your domain controller or a workstation that has AD tools installed Click on **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

2. The **Active Directory Users and Computers** console will appear.

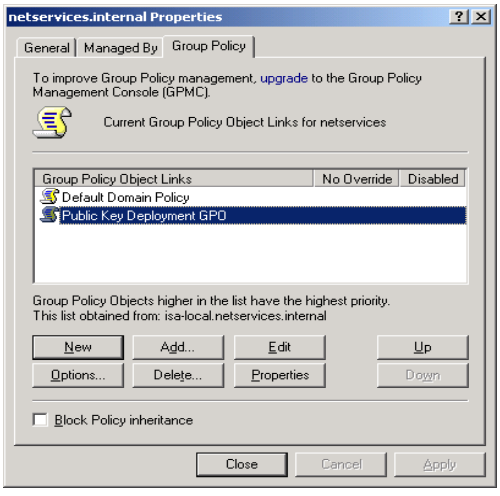
3. Right-click on your domain (the icon that has servers clustered together) and select **Properties**.

4. Click on the **Group Policy** tab. When the Group Policy tab appears you will find that there is an existing GPO entry called **Default Domain Policy** listed.



5. Leave **Default Domain Policy** GPO entry as it is and click on the **New** button at the bottom to create a new GPO.

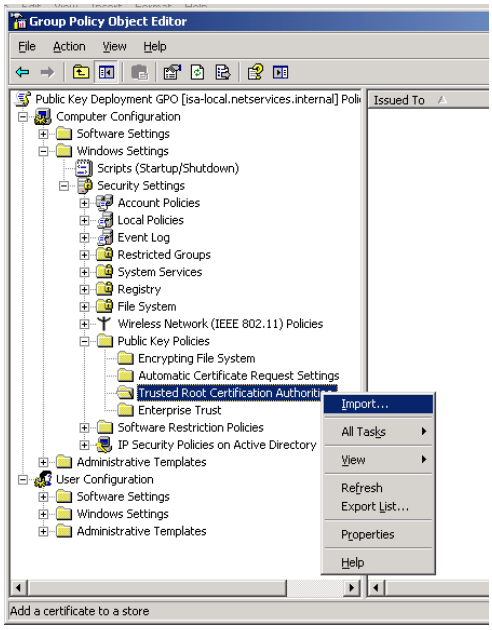
6. You will now see that it has created a new GPO called **New Group Policy Object** and that it is currently selected. Give the GPO a meaningful name i.e. **Public Key Deployment GPO**



7. Click on the newly created GPO entry and then click the **Edit** button to open the GPO Editor

8. When the GPO Editor settings screen appears expand **Computer Configuration** > **Windows Settings** > **Security Settings** > **Public Key Policies**

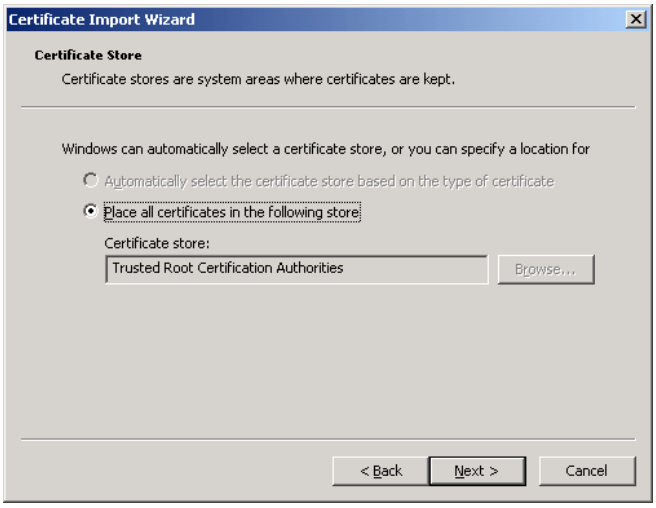
9. Under **Public Key Policies** right-click on **Trusted Root Certification Authorities** and select **Import**.



10. At **Welcome to the Certificate Import Wizard** click **Next**

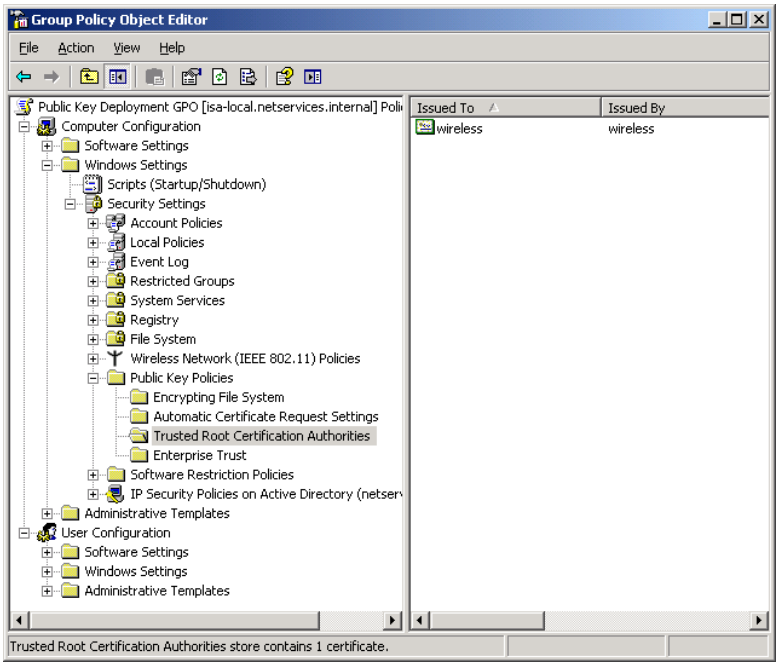
11. On the **File to Import** screen click on the **Browse** button and locate the root certificate file and click **Open** and then click **Next**.

12. At the **Certificate Store** screen click **Next**



13. At the **Completing the Certificate Import Wizard** summary screen click on **Finish** and **OK** when the **certificate import was successful** message appears.

14. You will now see that the root certificate has been imported to the correct place and will be listed under **Trusted Root Certification Authorities** store.



15. Close the GPO editor screen and exit the **Active Directory Users and Computers** console.

Your whole domain will now trust the root certificate that you have just imported.

Depending on your GPO refresh interval the certificate will be automatically imported to all your stations to which this GPO applies. This will happen next time when the group policy is refreshed/updated on the client(s).

To manually update the group policy open up a command prompt on the station and type in **gpupdate /force** (Windows XP/Vista) or **secedit /refreshpolicy machine_policy /enforce** (Windows 2000) and press **Enter**. You may need to reboot the station for it to take effect.

Wireless laptops will need to be connected to your wired network for the initial group policy to apply.

Note: If you only want to deploy the root certificate to a subset of the stations then you can create an AD security group. You need to add the relevant stations into this group and only make the GPO apply to the stations that are members of the security group you created. This is referred to as GPO filtering in which you edit the security of the GPO. You need to remove the “Authenticated Users” group and add your group and select the Apply Group Policy tick only for the group you selected. I.e. the group which contains the only stations you would like this GPO to apply to.

8. Backup and Restore IAS Settings

Backing up settings and polices is an essential part of network management and you should take a backup every time you modify the IAS configuration. You may wish to take a backup of the settings for Disaster Recovery purposes (if you accidentally deleted any entries or settings or misconfiguration) or for duplicating the settings to a redundant IAS (RADIUS) server.

8.1 Backing up IAS Settings and Policies

To backup the IAS settings follow the steps below:

1. On your IAS (Radius) server logon as administrator
2. Click **Start** > **Run** and type in **cmd** in the Run box and press **Enter**
3. At the Command Prompt window type the following:

   netsh aaaa show config > c:\IAS Radius Backup.txt (**Note** - it is 4 x a i.e. aaaa) and press **Enter**

4. The **C:\IAS Radius Backup.txt** states the drive and path to where the backup file will be created. In the example above it is on the root of the **C** drive with the file name of **IAS Radius Backup.txt**
5. You can now copy the file **IAS Radius Backup.txt** or whatever you called the filename from the server to another location.

8.2 Restoring IAS Settings and Policies

To restore the IAS settings from a backup follow the steps below:

1. On your IAS (Radius) server logon as administrator
2. Locate and copy the backup file to the root of the **C** drive or another local location
3. Click **Start** > **Run** and type in **cmd** in the Run box and press **Enter**
4. At the Command Prompt window type the following:

   netsh exec C:\IAS Radius Backup.txt and press **Enter**

5. The above example implies the file is called **IAS Radius Backup.txt** and that its store at the root of the **C** Drive on the IAS server. If it is stored elsewhere on the server then enter the path to the backup file.

9. Troubleshooting

10. References

[1] Wikipedia Entry - EAP

http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

[2] Wikipedia Entry - PEAP

http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol

[3] TechRepublic ultimate guide to enterprise wireless LAN security – George Ou

http://articles.techrepublic.com.com/5100-1035-6148579.html

[4] Microsoft TechNet Website

http://technet2.microsoft.com/WindowsServer/en/Library/fc353fbb-4df4-4b36-b14a-20cbbad434941033.mspx?mfr=true

[5] TechRepublic Downloads

http://downloads.techrepublic.com

Configuring Cisco Access Point to be used with 802.1x (Aironet 1131AG)