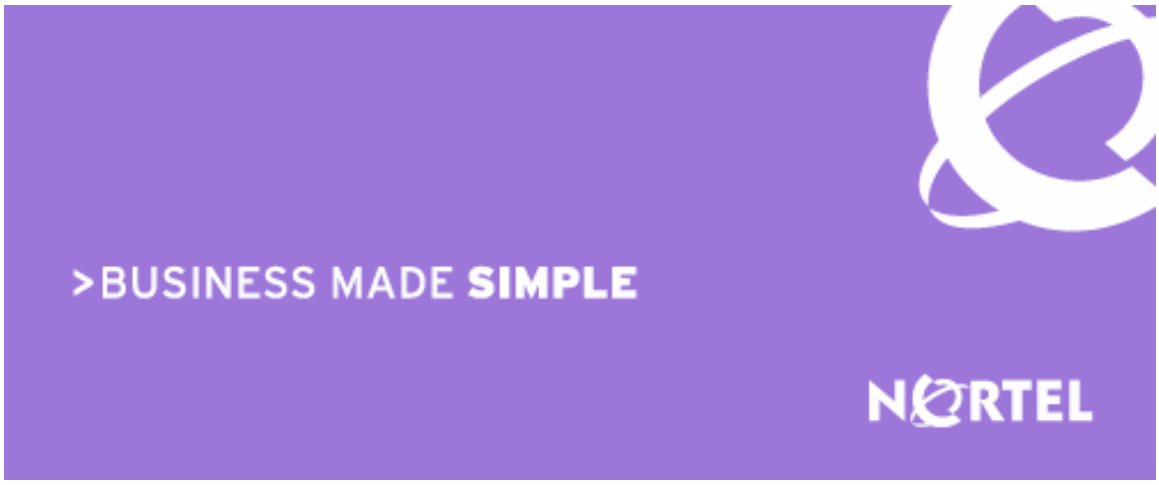


Ethernet Switch
Ethernet Routing Switch
Engineering

> Wired EAP-TLS Machine Authentication for ERS and ES Technical Configuration Guide

Enterprise Solutions Engineering
Document Date: February 2008
Document Number: NN48500-546
Document Version: 1.0

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

Abstract:

This document provides an overview on how to configure Wired EAP-TLS computer and user authentication on Nortel Ethernet Switches in a Microsoft environment. This document demonstrates configuring the Microsoft Internet Authentication Service on a Windows 2003 server, the Microsoft Windows XP 802.1X supplicant and the Nortel Ethernet Switch. This document does not address installing Certificate Services or managing Active Directory as this is out of the scope of this document.

Table of Contents:

Document Updates:

None.

Conventions:

This section describes the text, image, and command conventions used in this document.

Symbols:

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Caution – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text:

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

ERS5520-48T# ***show running-config***

Output examples from Nortel devices are displayed in a Lucida Console font:

ERS5520-48T# ***show running-config***

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.011
enable
configure terminal
```

1. Overview:

This document provides an overview on how to configure Wired EAP-TLS computer and user authentication on Nortel Ethernet Switches in a Microsoft environment. This document demonstrates configuring the Microsoft Internet Authentication Service on a Windows 2003 server, the Microsoft Windows XP 802.1X supplicant and the Nortel Ethernet Switch. This document does not address installing Certificate Services or managing Active Directory as this is out of the scope of this document.

1.1 What is Computer Authentication:

User authentication is a natural choice when considering identification to Wired or Wireless infrastructure. However, in most cases Enterprises will also want to also implement computer (or machine) authentication to ensure a complete solution.

There are a number of features in Windows that will only work correctly with an active network connection. Leveraging 802.1X computer authentication ensures that this network connection is established during the Windows boot sequence and prior to end users seeing the initial Windows logon screen. The following table provides a list of some of the common Windows features that require such a connection:

Feature	Scenario Requiring Computer Authentication
Active Directory computer Group Policies	Computer–based Group Policy is applied during computer start up and at timed intervals — even when no one is logged in to Windows.
Network logon scripts	Network logon scripts are run during initial user logon.
Systems management agents	Systems management application agents such as those that come with Microsoft Systems Management Server (SMS) frequently need network access without user intervention.
Remote Desktop Connection	Computers are accessible from Windows Remote Desktop Connection when no one is logged on to Windows.
Shared folders	Files and folders shared from a computer are still available, even when no user is logged on to Windows.

Table 1.1 – Scenarios Requiring Machine Authentication

1.2 Windows XP Boot Process:

Unlike 802.1X user authentication which occurs after the end user has logged into Windows, computer authentication occurs during the boot process before the end user is presented with the Windows Logon screen:

1. When machine authentication is enabled, the computer will authenticate to the switch port using its machine credentials as soon as an Ethernet link becomes active. If computer authentication is successful the EAPOL Ethernet port status will change to Authorized and the user placed in the appropriate VLAN which may be statically assigned or provided dynamically from the authentication server.
2. When a user logs onto the computer, the user authentication will supersede the computer authentication. The Ethernet switch will assign the user to the appropriate VLAN which may be statically assigned or provided dynamically from the authentication server.
3. When a user logs off the computer, computer authentication will re-occur and the Ethernet Switch will assign the computer to the appropriate VLAN which may be statically assigned or provided dynamically from the authentication server.

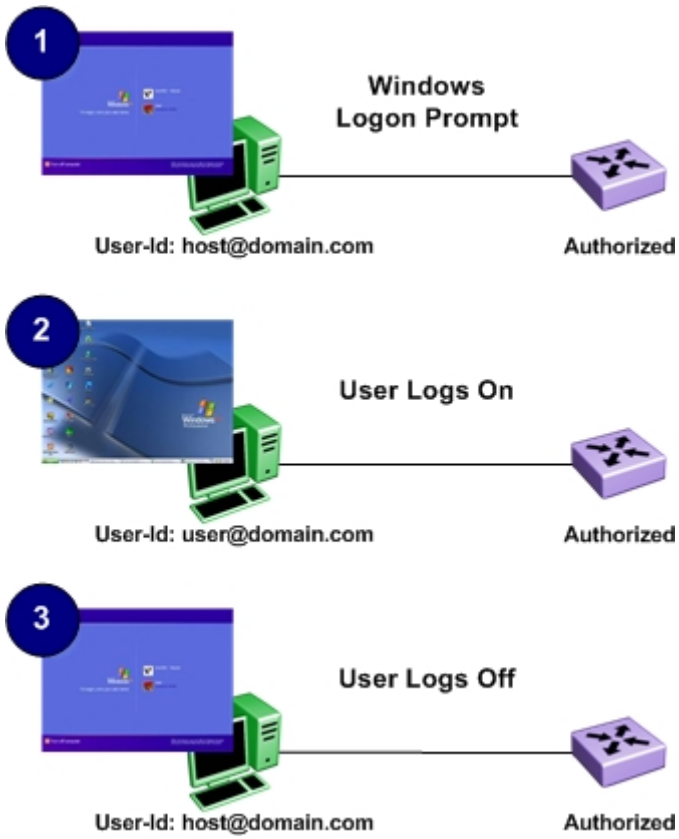


Figure 1.2.1 – Wired Machine Authentication Process

1.3 Pre-Requisites:

This document makes the following assumptions in regards to the Windows 2003 server, Windows XP workstation and Nortel Ethernet Switch:

1. A Windows 2003 Advanced or Enterprise Server is installed with the following:
    a. Latest service pack and updates installed
    b. Configured as an Active Directory Domain Controller.
        i. One or more Active Directory User accounts have been created.
        ii. A unique Group such as **EAPOL Users** has been created with User and Computer accounts that will be performing EAP authentication and has been added as members to the Group (**see Appendix 6.1**)
        iii. The **Remote Access Permission** for each of the User and Computer accounts performing EAP authentication are set to **Allowed Access** (see **Appendix 6.2**).
    c. Certificate Services is installed as an Enterprise Root CA.
    d. Internet Authentication Service is installed.
    e. IP communication with the Nortel Ethernet Switch.
2. Windows XP Workstation with the following:
    a. Latest service pack and updates installed.
    b. Is a member of the Windows Domain.
    c. The Microsoft Wireless Zero Configuration service is running (see **Appendix 6.4**).
3. Nortel Ethernet Switch with the following:
    a. One VLAN with a management IP address assigned.

1.4 Topology:

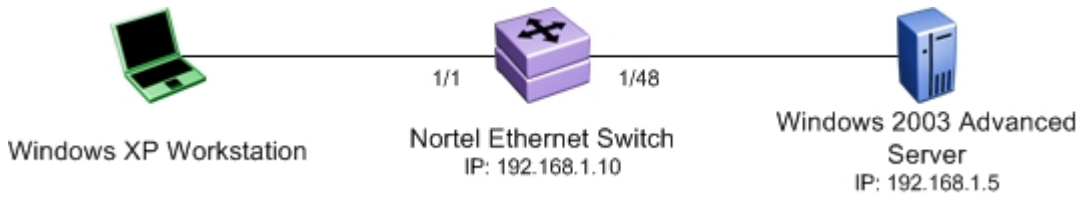


Figure 1.4.1 – Topology

2. Internet Authentication Service:

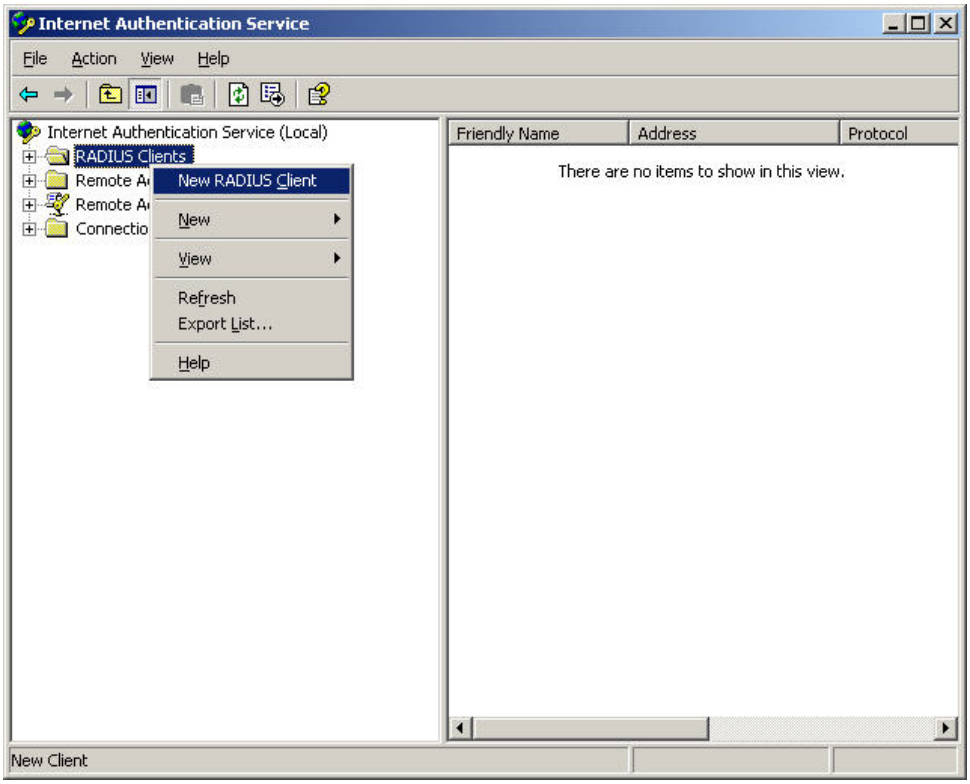
For the Microsoft Internet Authentication Service (IAS) to be able to authenticate EAP-TLS computers and users connected to a Nortel Ethernet switch the following configuration steps need to be performed:

1. The Nortel Ethernet Switch that will be forwarding RADIUS authentication requests to IAS will need to be defined as a RADIUS client.
2. A Remote Access Policy needs to be defined so that IAS knows how to authenticate the users as well as which authentication protocols to support.

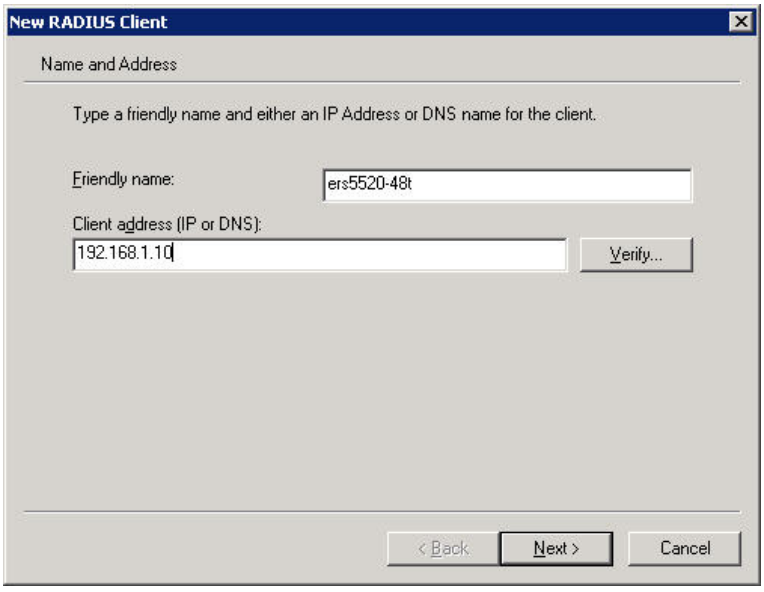
2.1 Add Radius Clients:

To add a Nortel Ethernet Switch as a RADIUS client to IAS:

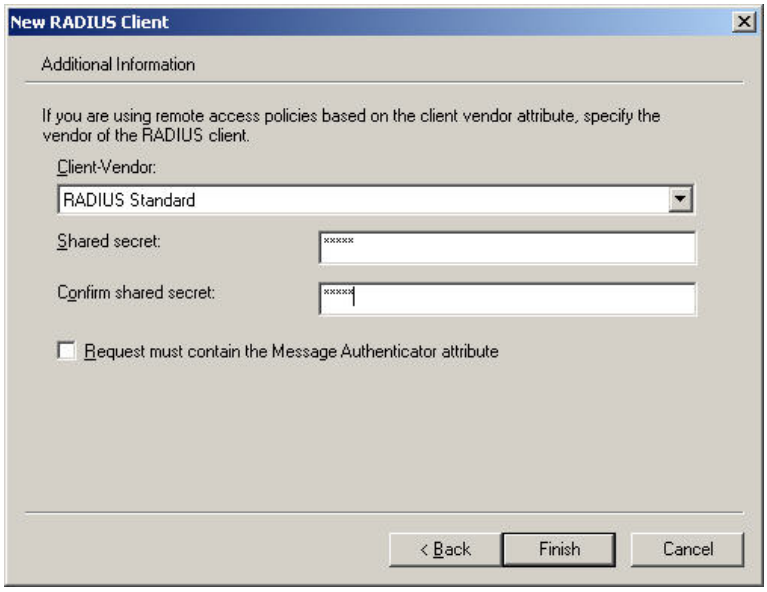
1. Open the IAS snap-in by clicking **Start**, **Programs**, **Administrative Tools** then **Internet Authentication Service**.
2. In the IAS snap-in, right click **RADIUS Clients** and then click **New RADIUS Client**.



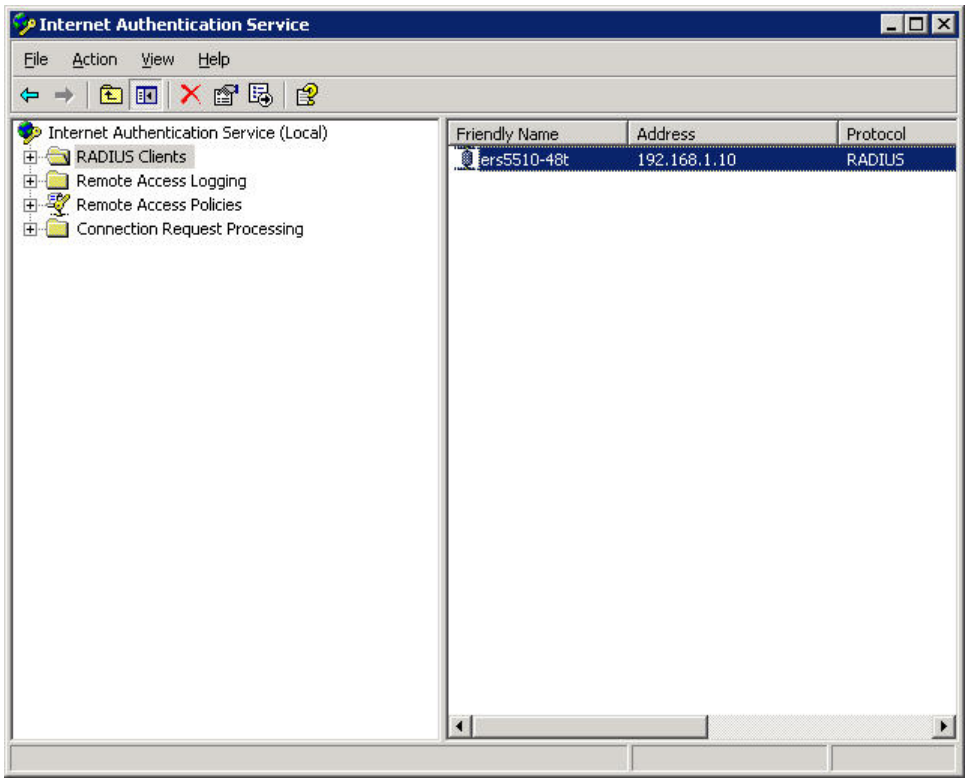
3. In the **Friendly name** field specify the hostname of the Ethernet switch. In the **Client address (IP or DNS)** field specify the management IP address of the Ethernet switch. Click **Next**.



4. Select the default **Client-Vendor** option **RADIUS Standard**. Specify and confirm a **Shared secret** which will match the shared secret defined on the Ethernet switch (for example **Nortel**). Click **Next**.



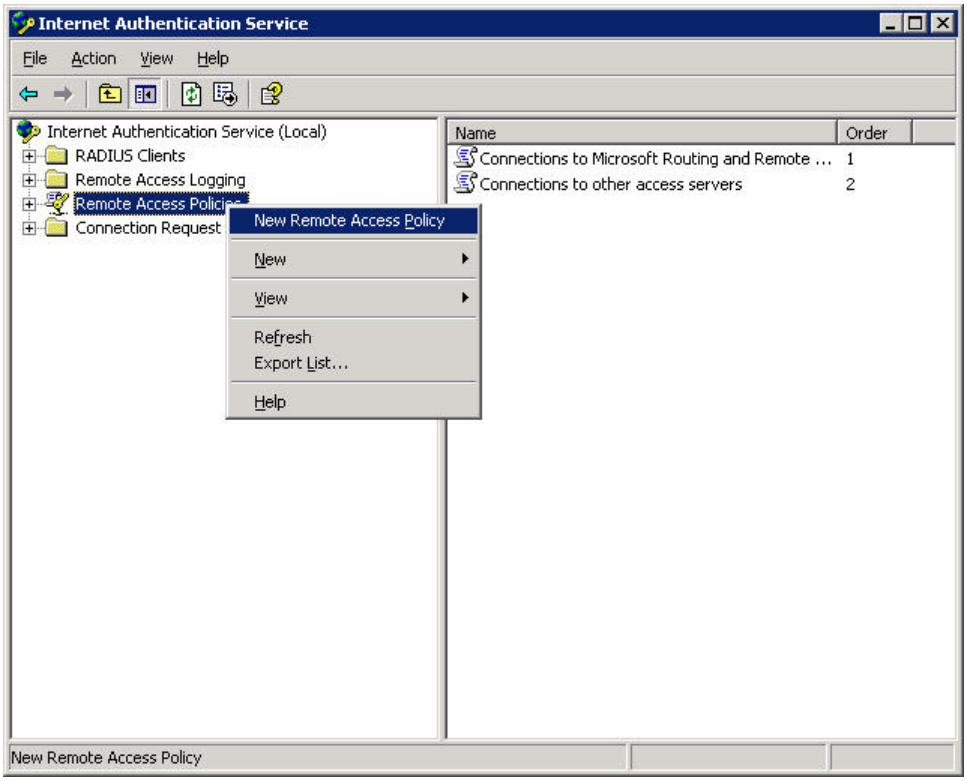
5. The Nortel Ethernet switch has now been added to IAS as a RADIUS client.



2.2 Create a Remote Access Policy:

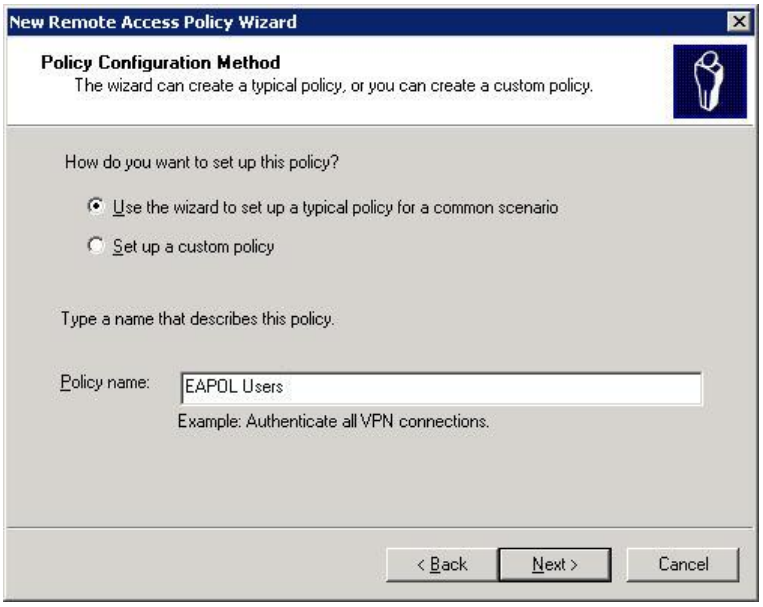
To create a Remote Access Policy in IAS to authenticate computers and users using EAP-TLS:

1. Open the IAS snap-in by clicking **Start**, **Programs**, **Administrative Tools** then **Internet Authentication Service**.
2. In the IAS snap-in right click **Remote Access Policies** and then click **New Remote Access Policy**.

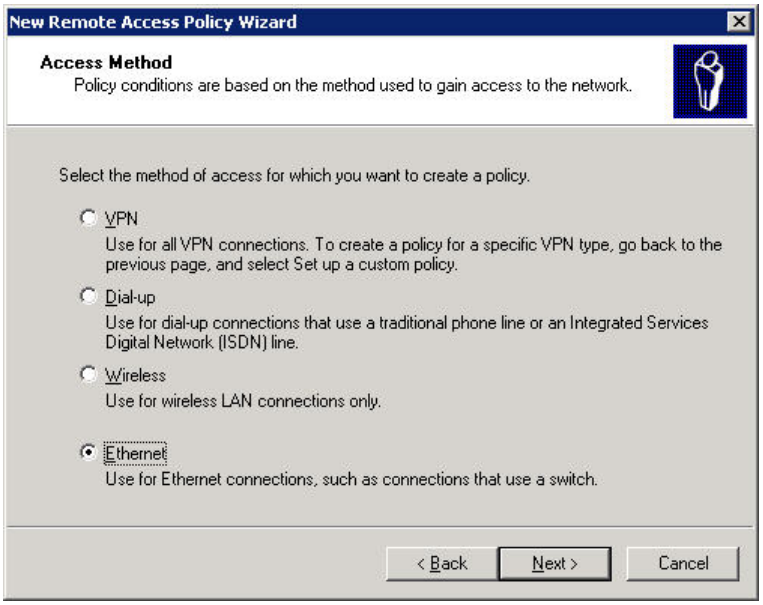


3. Click **Next**.

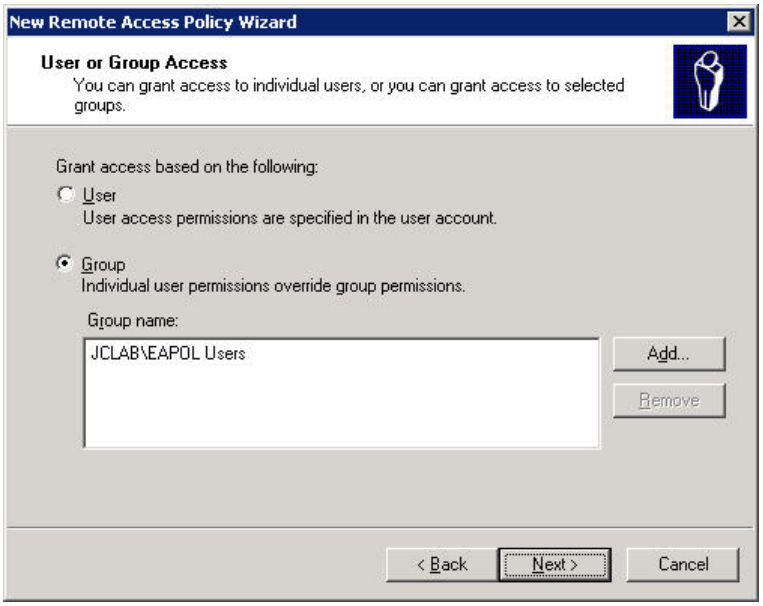
4. Select the option **Use the wizard to set up a typical policy for a common scenario**. In the **Policy name** field enter in the name for the policy (for example **EAPOL Users**). Click **Next**.



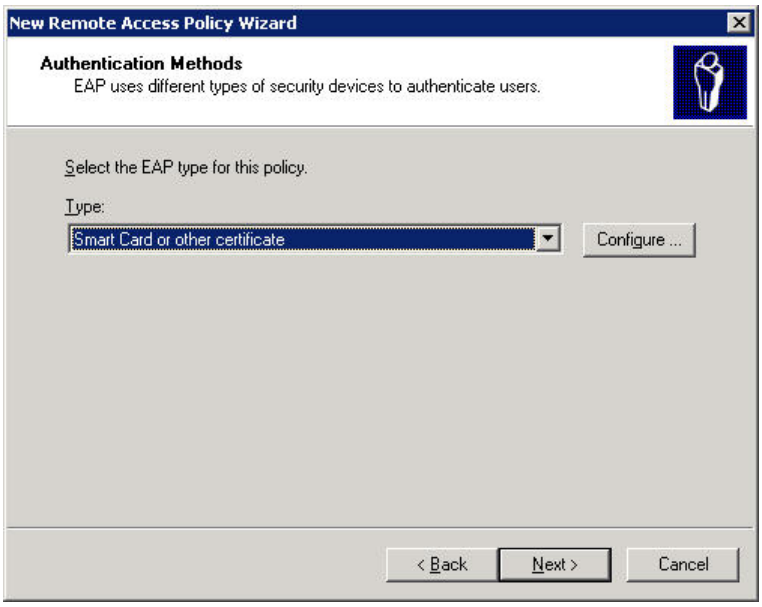
5. Select the **Access Method** option **Ethernet** then click **Next**. This sets the match criteria in the policy to only authenticate requests from Ethernet devices.



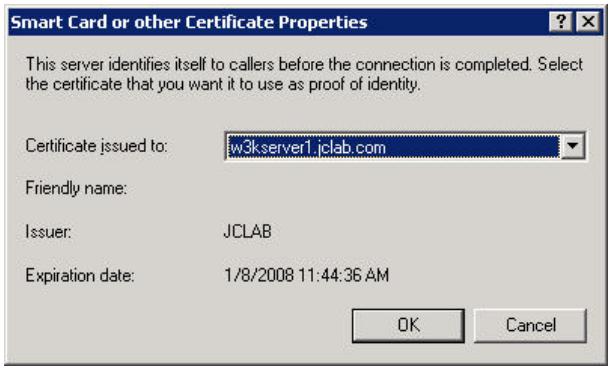
6. Specify the domain users or groups which the policy will apply to. For this example the domain group named **EAPOL Users** has been added. This sets the match criteria in the policy to only authenticate Users and Computers that are a member of this Domain Group. Click **Next**.



7. Select the EAP type **Smart Card or other certificate**. Click **Configure** to specify a server certificate to be used by the policy.

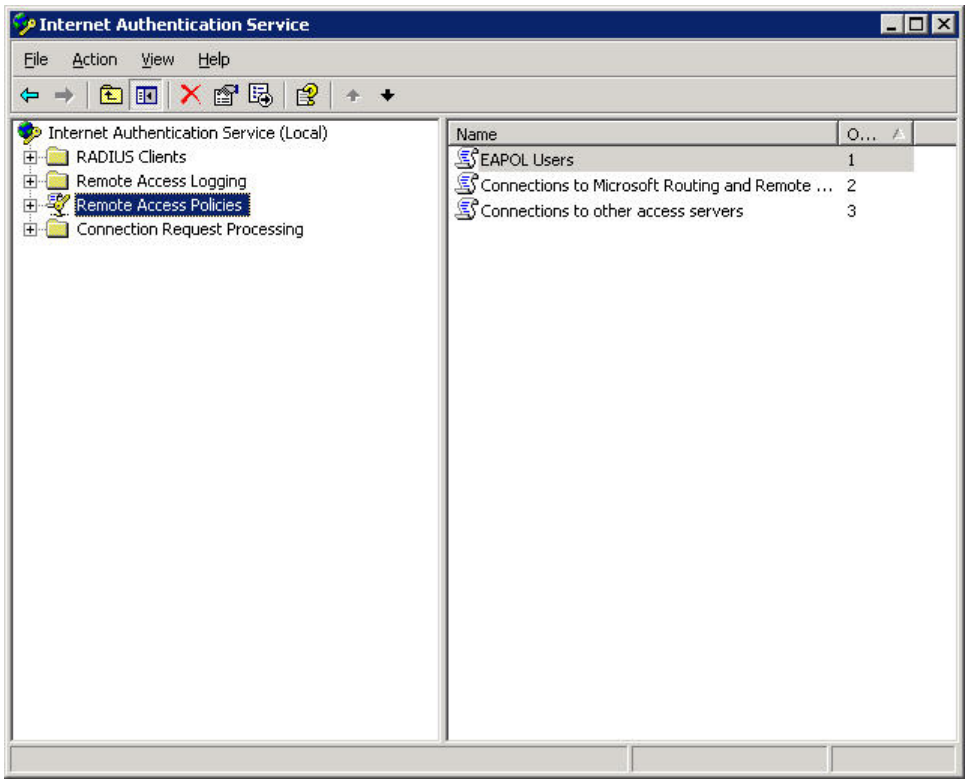


8. In the **Certificate issued to** pull down menu, select the server certificate you wish to use for the policy. For this example the default server certificate installed on the Windows 2003 Advanced server named **w3kserver.jclab.com** is used. Click **OK** and then **Next**.



9. Verify the information is correct and then click **Finish**.

10. The Remote Access Policy **EAPOL Users** has now been created.



3. Nortel Ethernet Switch:

For a Nortel Ethernet Switch to be able to support Windows XP workstations authenticating using EAP-TLS the following configuration steps need to be performed:

1. A RADIUS server IP addresses, port and shared key needs to be defined.
2. The EAPOL admin state for user ports needs to be set.
3. EAPOL needs to be globally enabled.

3.1 Define a RADIUS Server:

To add Microsoft IAS as a RADIUS authentication server to a Nortel Ethernet switch using NNCLI:

1 Enter the User EXEC mode by issuing the following command:

ers5510-48t> ***enable***

ers5510-48t#

2 Enter the Privilege EXEC command mode by issuing the following command:

ers5510-48t# ***config terminal***

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

ers5510-48t(config)#

3 Define a primary RADIUS server IP address, port and shared key. For this example the IP address of the IAS server is 192.168.1.5, the port is 1812 and the shared key is Nortel (Note: the shared key must match what was defined on IAS in section 2.1):

ers5510-48t(config)# ***radius-server host 192.168.1.5 port 1812 key Nortel***

4 You can verify the RADIUS server configuration by issuing the following command:

ers5510-48t(config)# ***show radius-server***

```
Password Fallback:  Disabled
Primary Host:  192.168.1.5
Secondary Host:  0.0.0.0
Port:  1812
Time-out:  2
Key:  Nortel
Radius Accounting is  Disabled
AcctPort:  1813
```

3.2 Set the EAPOL Admin State:

By default all Ethernet ports on a Nortel Ethernet switch are configured with the EAPOL admin state set to **Forced Authorized** which grants access to clients without EAP authentication. To enable EAP authentication the EAPOL admin state for user ports needs to be changed to **Auto**.

Please note that the Windows 2003 Advanced Server in this example is connected to port 48. To maintain connectivity with the server the EAPOL admin state on port 48 will remain set to **Forced Authorized**.

1 To change the EAPOL admin state for user ports 1-47 issue the following commands:

```
ers5510-48t(config-if)# interface fastEthernet 1-47
ers5510-48t(config-if)# eapol status auto
```

2 To verify the EAPOL admin state for all ports issue the following command:

```
ers5510-48t(config-if)# show eapol port 1-48
```

```
     Admin          Admin Oper ReAuth ReAuth Quiet  Xmit   Supplic Server  Max
Port Status   Auth Dir   Dir  Enable Period Period Period Timeout Timeout Req
---- -------- ---- ----- ---- ------ ------ ------ ------ ------- ------- ---
1    Auto     Yes  Both  Both No     3600   60     30     30      30      2
2    Auto     Yes  Both  Both No     3600   60     30     30      30      2
..   ..       ..   ..    ..   ..     ..     ..     ..     ..      ..      .
45   Auto     Yes  Both  Both No     3600   60     30     30      30      2
46   Auto     Yes  Both  Both No     3600   60     30     30      30      2
47   Auto     Yes  Both  Both No     3600   60     30     30      30      2
48   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
```

3.3 Globally Enable EAPOL:

To globally enable EAPOL on a Nortel Ethernet switch using NNCLI:

1 Globally enable EAPOL mode issue the following command:

```
ers5510-48t(config)# eapol enable
```

2 You can verify the EAPOL global state by issuing the following command:

```
ers5510-48t(config)# show eapol

EAPOL Administrative State:  Enabled
```

4. Windows XP Workstation:

For Windows XP to be able to support computer and user authentication the following configuration steps need to be performed:

1. Install CA, computer and user certificates.
2. IEEE 802.1X needs to be enabled on the Local Area Network Connection.
3. The Windows XP 802.1X supplicant default behavior needs to be modified by adding two registry entries.

4.1 Certificates:

For EAP-TLS computer and user authentication there are three types of certificates that must be installed on the Windows XP workstation:

- CA Certificate – Allows all parties in the certificate chain to validate the identity of the certificates issued from the enterprise CA. A CA certificates for the CA is typically installed automatically for the Computer account when the workstation is added to the domain but not for the user account (unless Auto-Enrollment is enabled). CA certificates will need to be present for both the **Local Computer)** and **Users Personal Trusted Root Certification Authority** certificate stores.
- Computer Certificate – Must be issued to all Windows XP domain workstations that require EAP-TLS machine authentication. Computer certificates will be installed into the **Certificates (Local Computer) Personal** certificate store.
- User Certificate – Must be issued for all domain users that will be using the Windows XP workstation for EAP-TLS user authentication to occur. User certificates will be installed into the **Certificates - Current User Personal** certificate store.

4.1.1 Issuing CA certificates using Web Enrollment:

CA certificates are required for each device in the certificate chain. A CA certificate is also required on the Windows XP workstations for both computer and user accounts before any computer or user certificates can be obtained using the MMC certificate snap-in tool.

If CA certificates are already present for both the computer and user accounts this step may be skipped.

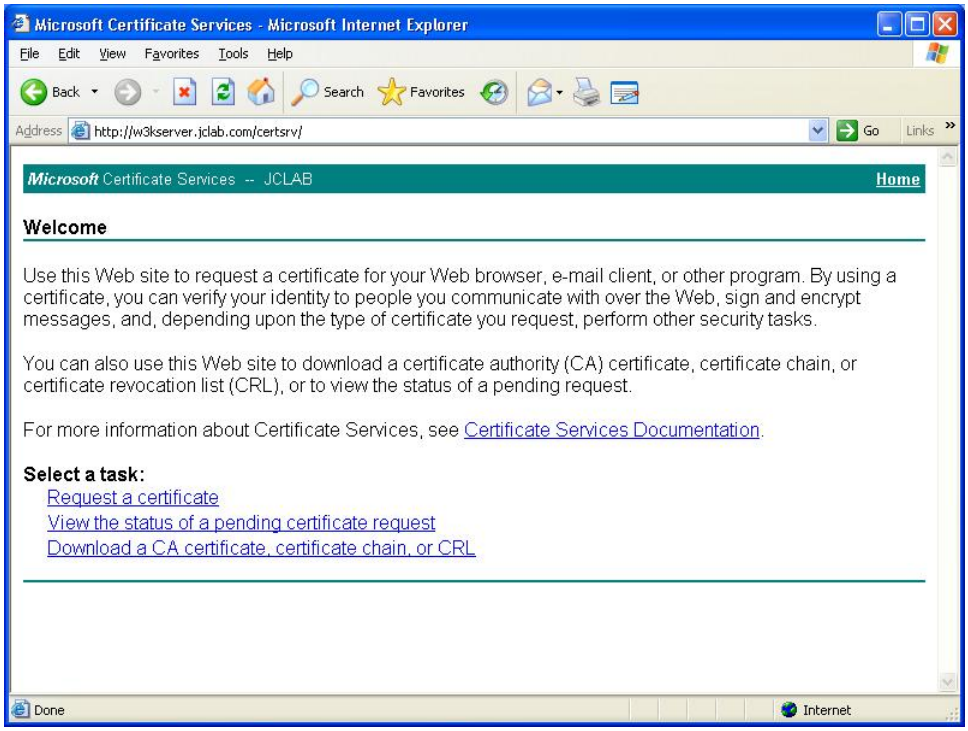
To issue a CA certificate using Web Enrollment:

1. On the Windows XP workstation open the web browser.
2. In the **Address** field type in the IP address or hostname of the Windows 2003 server that is running Certificate Services using the following format: **http://server-ip-address/CertSrv** or **http://servername.domain.com/CertSrv**.

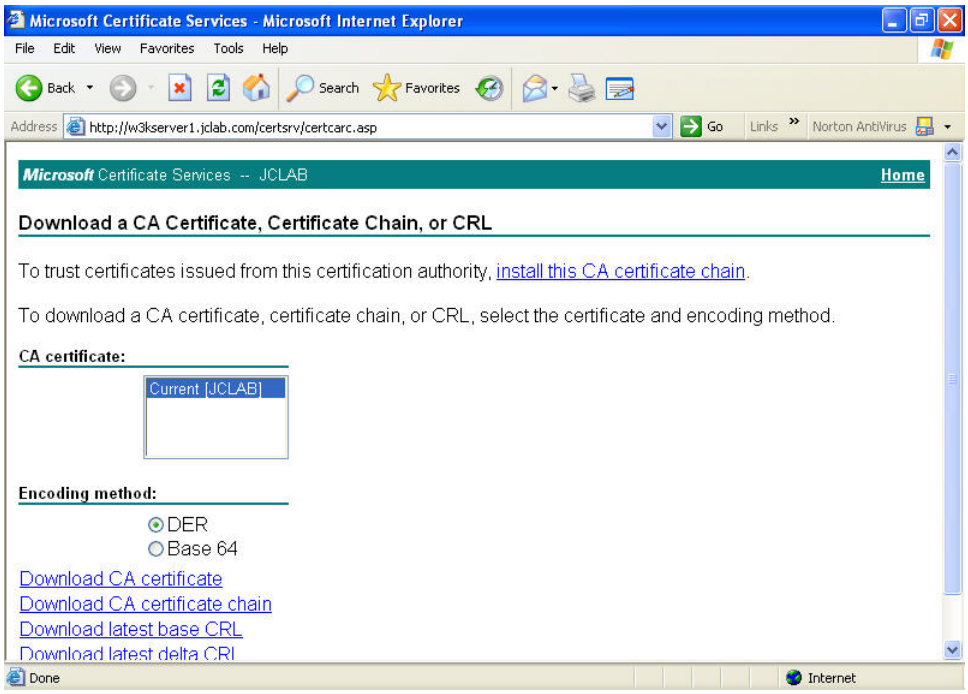
3. Enter in the domain **User name** and **Password** for the user that will be requiring the certificate.

It is important that you login to the web enrollment tool using the username and password of the user that will be using the user certificate. This ensures that the user certificate is issued to the correct username.

1. Click **Download a CA certificate, certificate chain or CRL**.

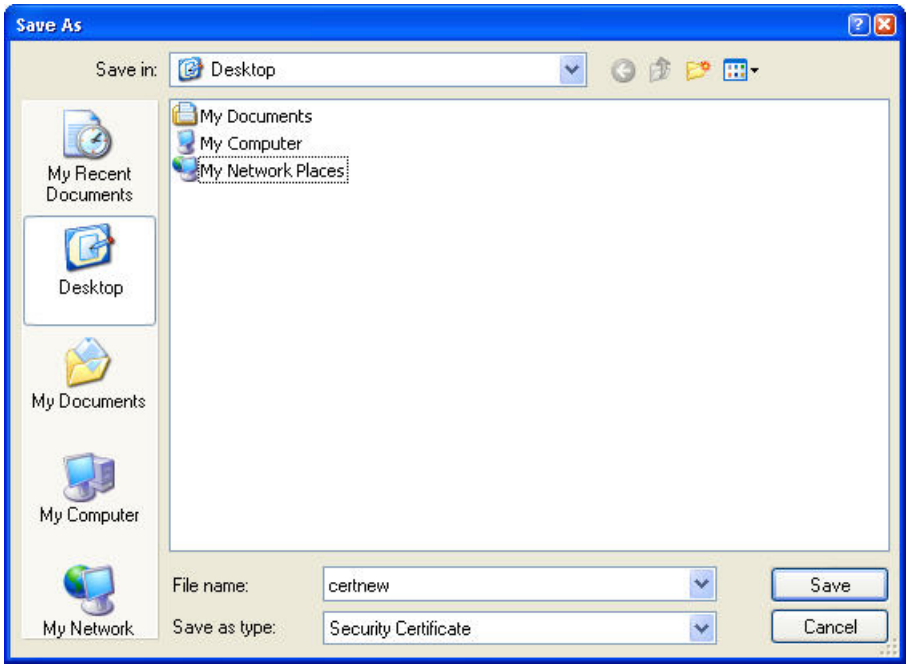


2. Click **Download CA certificate**.



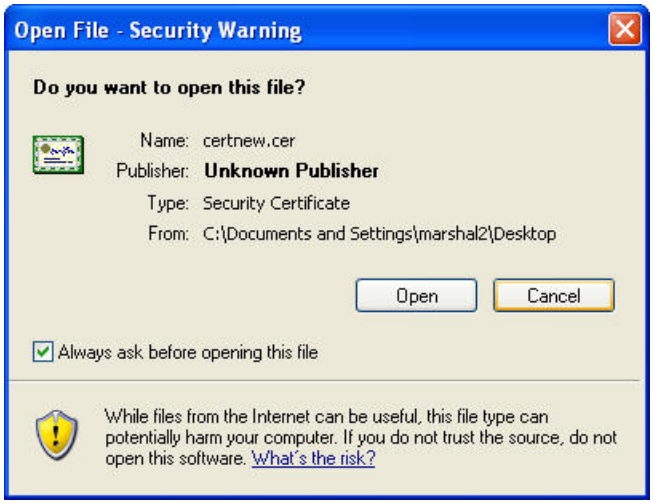
3. Click **Save**.

4. Select a location on the Windows XP workstation to save the CA certificate file too and click **Save**. Note the default filename is **certnew.cer**.

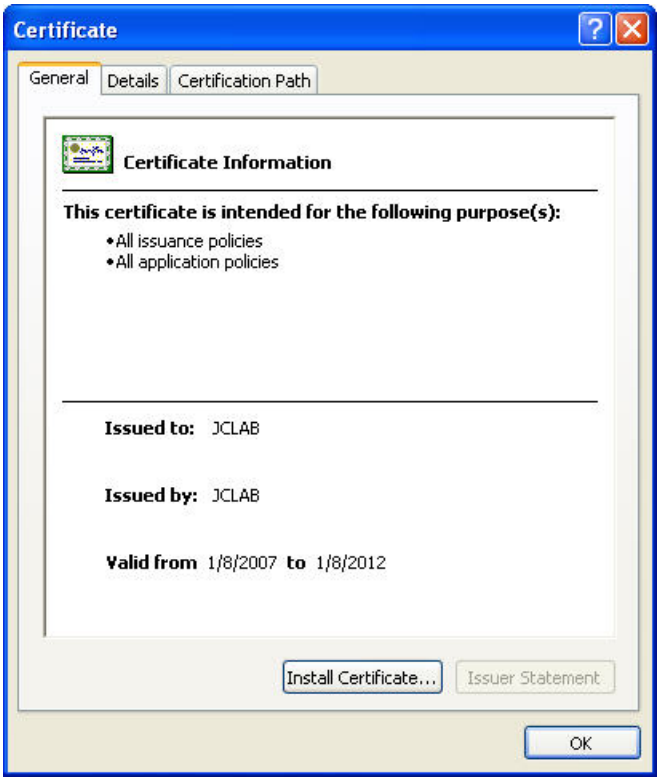


5. In Windows XP double click on the CA certificate file **certnew.cer** to import the CA certificate into Windows.

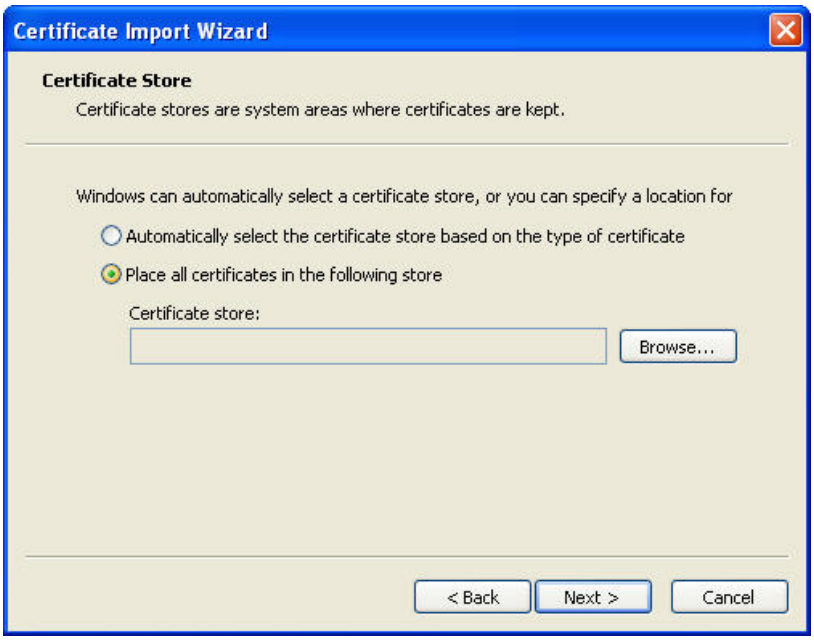
6. Click **Open**.



7. Click **Install Certificate**.

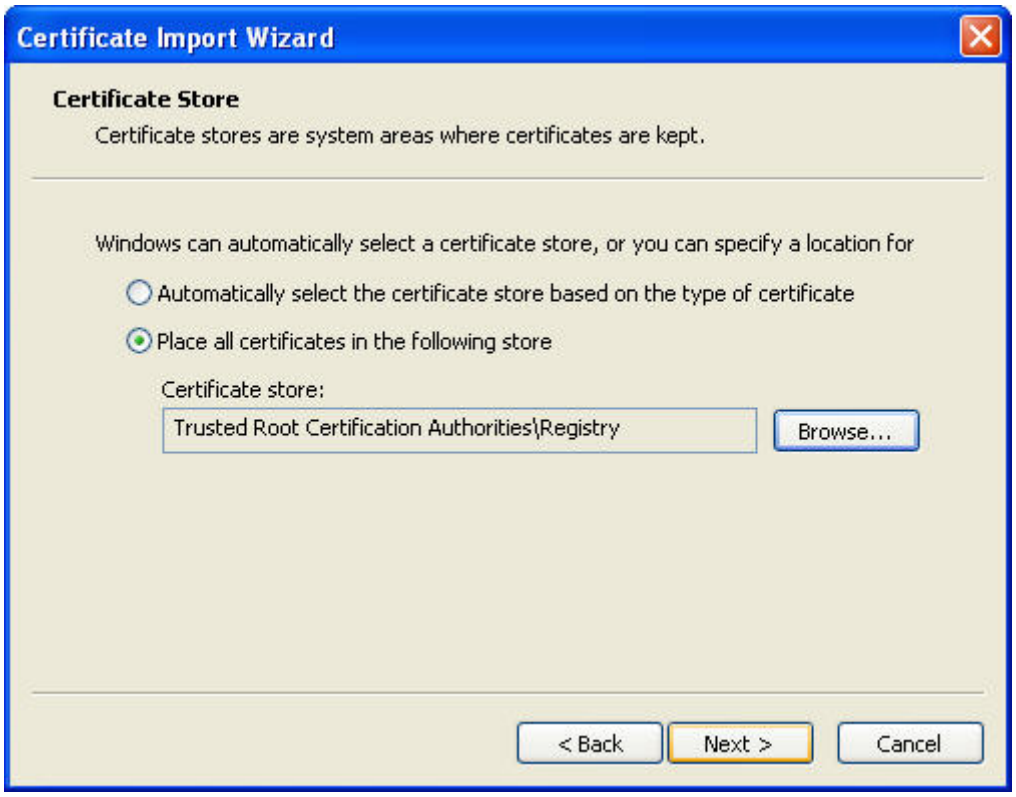


8. In the **Welcome to the Certificate Request Wizard** screen click **Next**.
9. Select **Place all certificates in the following store** and then click **Browse**.



10. Select **Show physical stores** and expand the **Trusted Root Certification Authorities** tree.
    a) To install a CA certificate into the **Local Computers Trusted Root Certification Authorities** certificate store select **Local Computer** and then **OK**.
    b) To install a CA certificate into the **Current Users Trusted Root Certification Authorities** certificate store select **Registry** and then **OK**.

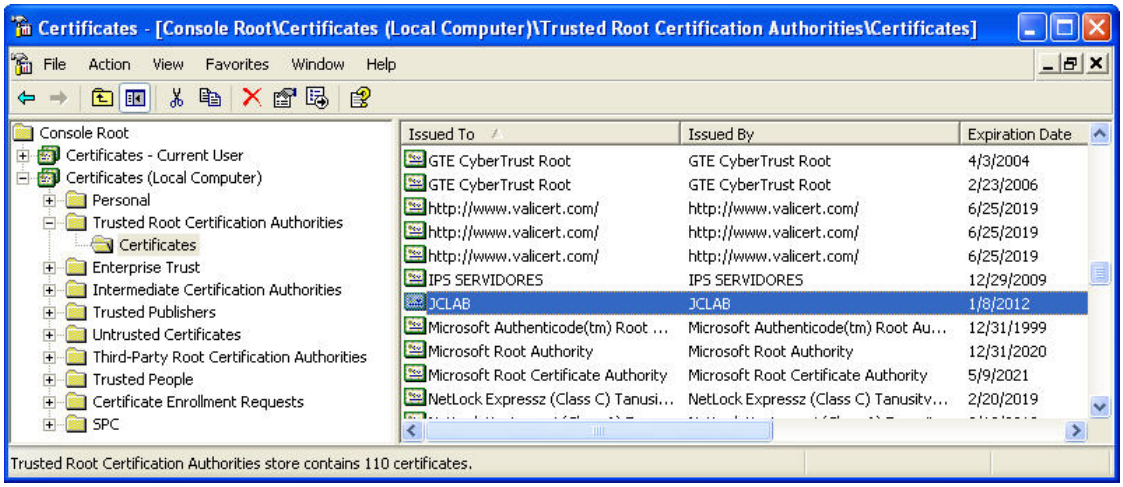
11. Verify the information and click **Next**.



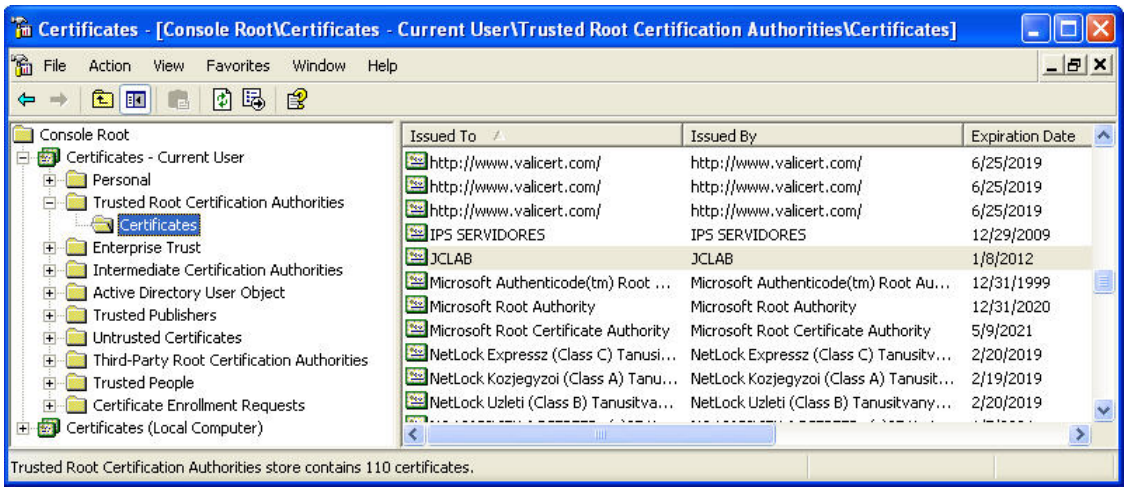
12. When presented with a **Security Warning** screen click **Yes**.
13. If successful you will see a **The import was successful** dialog window. Click **OK**.

14. Repeat until a CA certificate is installed into both the Local Computer and Users **Trusted Root Certification Authorities** certificate store.

15. A CA certificate for the Enterprise CA will now be displayed in the **Certificates (Local Computer) Trusted Root Certification Authorities Certificates** store.



16. A CA certificate for the Enterprise CA will now be displayed in the **Certificates - Current User Trusted Root Certification Authorities Certificates** store.



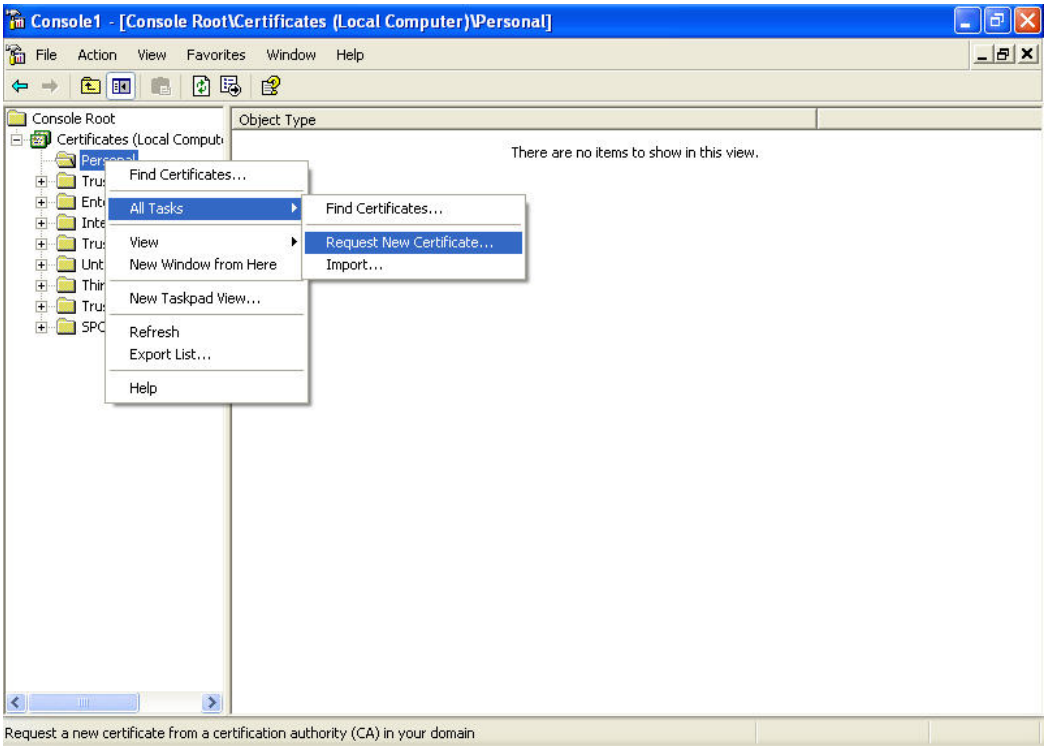
4.1.2 Issuing Computer Certificates using MMC Certificate Snap-In:

Computer certificates may manually requested from Certificate Services and installed for domain computers using the MMC certificate snap-in tool. Alternatively computer certificates maybe automatically installed using Auto-Enrollment (see Reference Documentation).

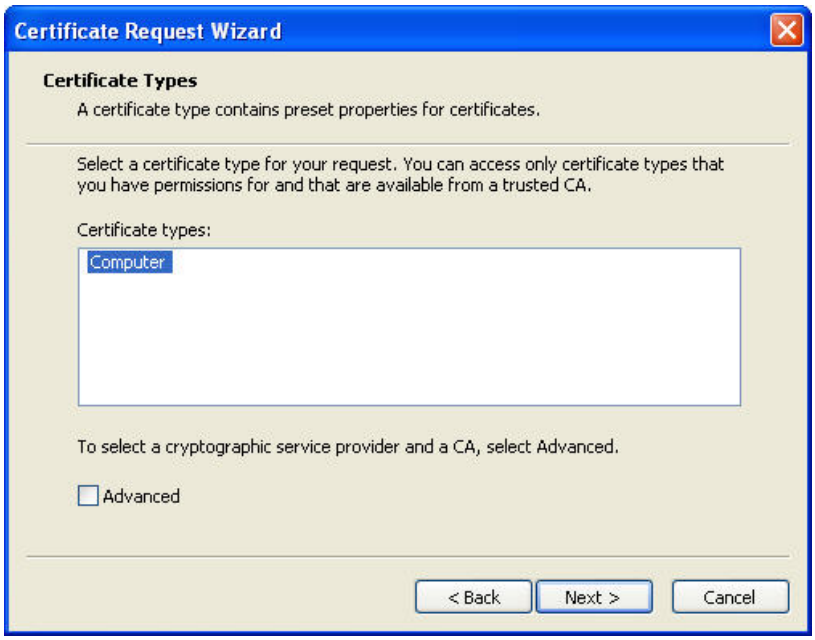
Please note that the domain user will require administrative privileges on the workstation before a computer certificate can be issued to the Windows workstation. Additionally a CA certificate for the CA must be installed or MMC will not be able to request the computer certificate.

To manually request and issue a computer certificate for domain computer using the MMC certificate snap-in tool:

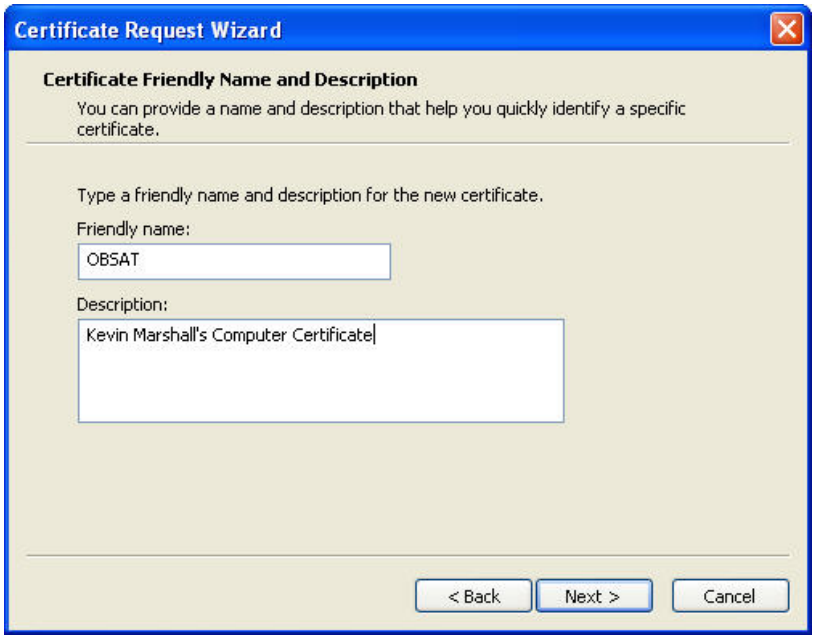
1. Click the **Start** button and then click **Run**.
2. In the **Run** dialog box type **mmc.exe**, and then click **OK**.
3. On the **File** menu, click **Add/Remove Snap-In**.
4. In the **Add/Remove Snap-In** window, click **Add**.
5. In the **Available Standalone Snap-ins** window, click **Certificates** and then **Add**.
6. In the **Certificates snap-in** window click **Computer account** and then click **Finish**.
7. Select **Certificates (Local Computer)** and **Personal**. Right click and select **All Tasks** then **Request New Certificate**.



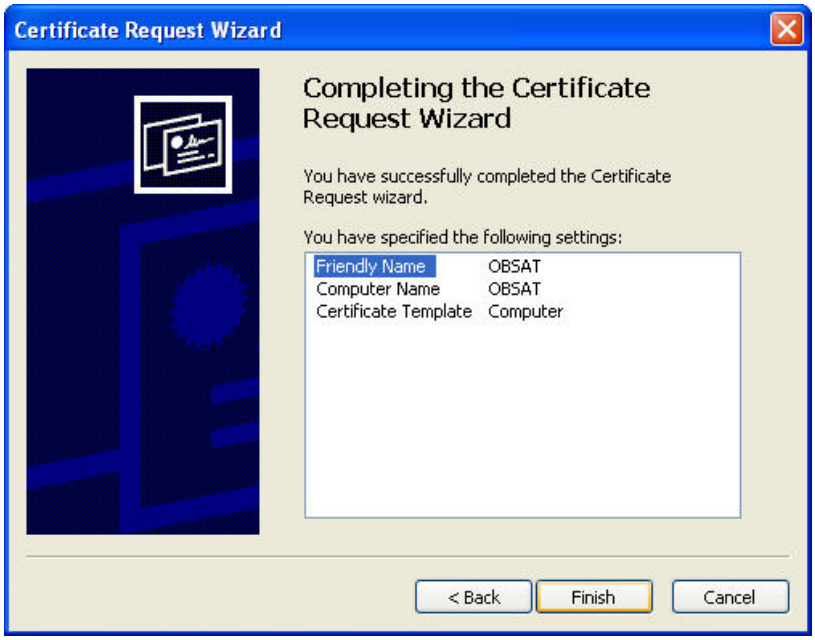
8. In the **Welcome to the Certificate Request Wizard** screen click **Next**.
9. Select **Computer** and then click **Next**.



10. In the **Friendly name** field type in a name of the computer certificate.
11. In the **Description** field type in a description of the computer certificate. Click **Next**.

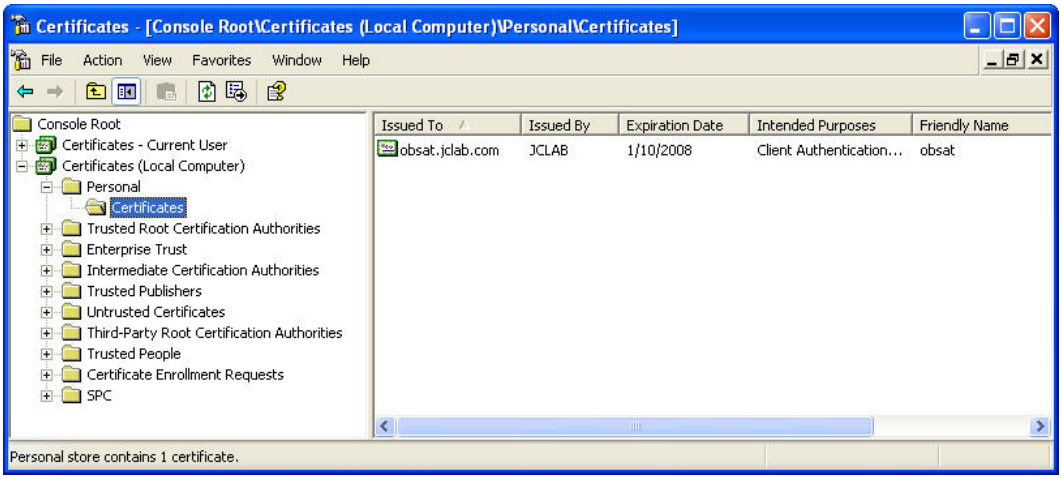


12. Verify the certificate information and if correct click **Finish**.



13. If successful you will see a **The certificate request was successful** dialog window.

14. A computer certificate for the Windows XP domain workstation should now be installed in the **Certificates (Local Computer)** / **Personal / Certificates** store.



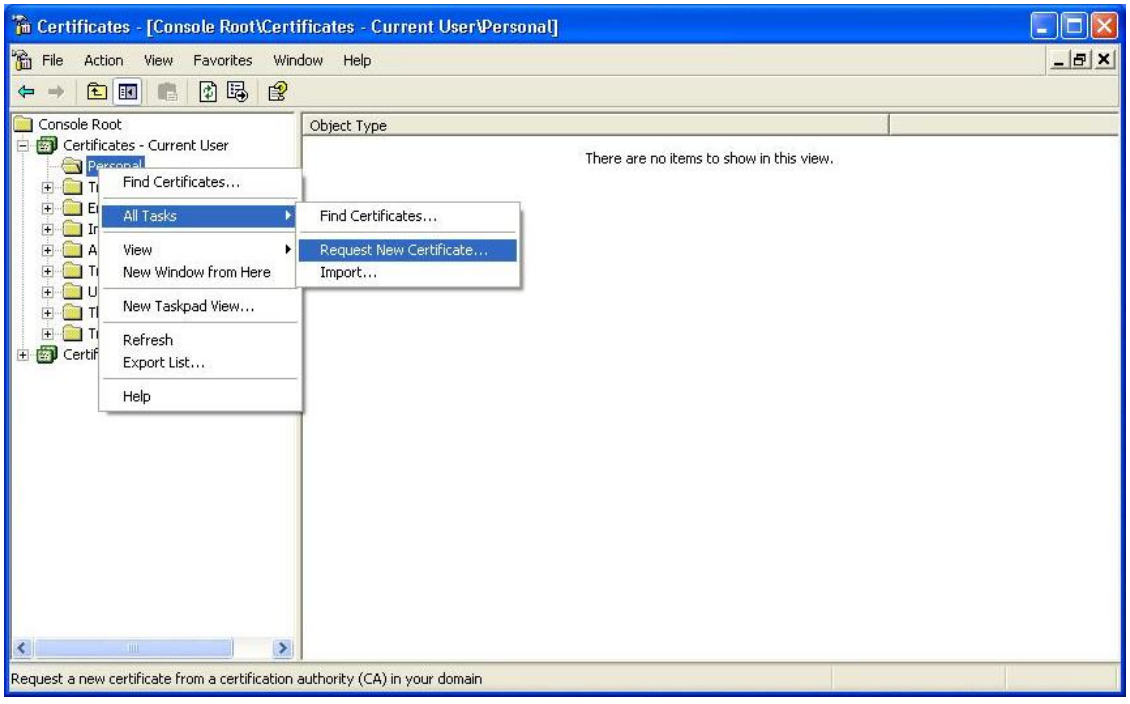
4.1.3 Issuing User Certificates using MMC Certificate Snap-In:

User certificates may manually requested from Certificate Services and installed for domain users using the MMC certificate snap-in tool. Alternatively user certificates maybe automatically installed using Auto-Enrollment (see Reference Documentation).

Please note that the MMC certificate snap-in tool will issue a user certificate for the domain user that is currently logged into the Windows workstation. Additionally a CA certificate for the CA must be installed or MMC will not be able to request the computer certificate.

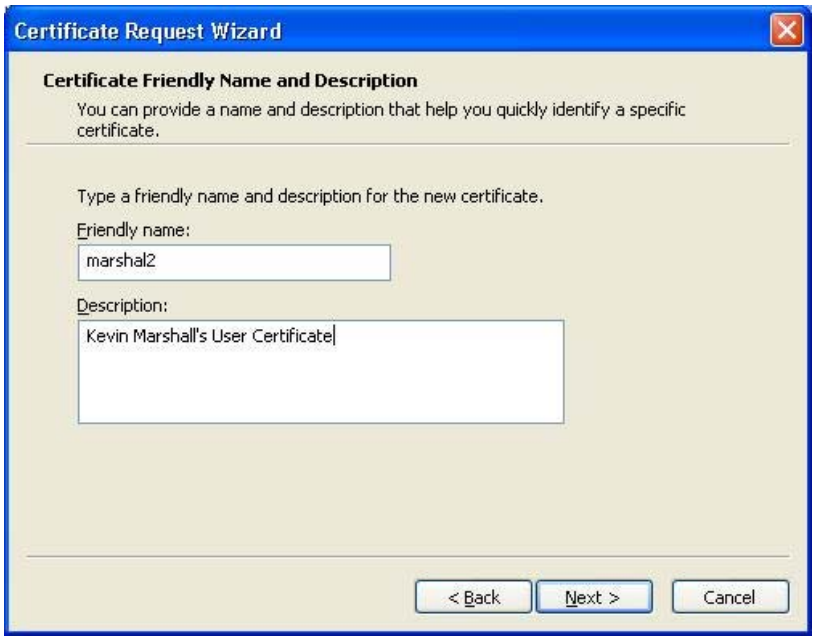
To manually request and issue a user certificate for domain user using the MMC certificate snap-in tool:

1. Click the **Start** button and then click **Run**.
2. In the **Run** dialog box type **mmc.exe**, and then click **OK**.
3. On the **File** menu, click **Add/Remove Snap-In.**
4. In the **Add/Remove Snap-In** window, click **Add**.
5. In the **Available Standalone Snap-ins** window, click **Certificates** and then **Add**.
6. In the **Certificates snap-in** window click **My user account** and then click **Finish**.
7. Select **Certificates – Current User** and **Personal**. Right click and select **All Tasks** then **Request New Certificate**.



8. In the **Welcome to the Certificate Request Wizard** screen click **Next**.
9. Select **User** and then click **Next**.

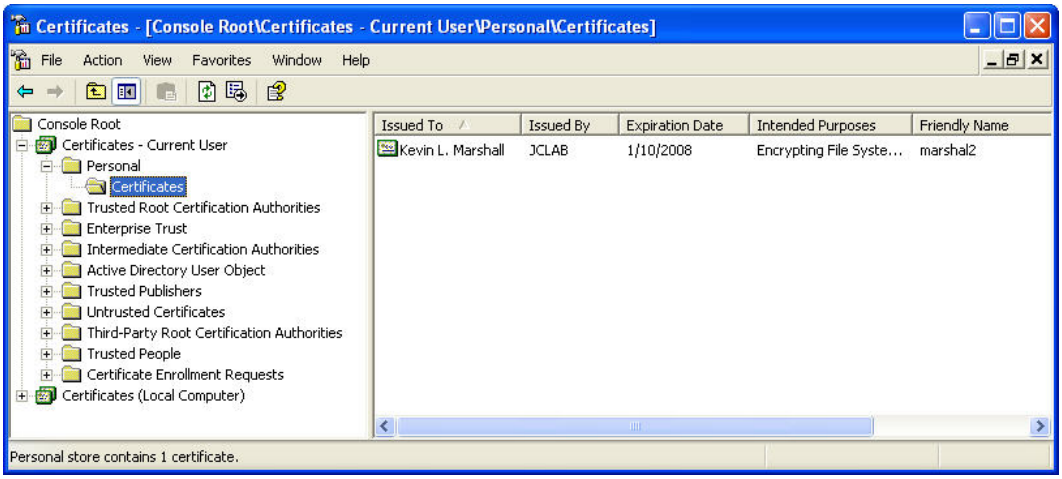
10. In the **Friendly name** field type in a name of the user certificate.
11. In the **Description** field type in a description of the user certificate. Click **Next**.



12. Verify the certificate information and if correct click **Finish**.

13. If successful you will see a **The certificate request was successful** dialog.

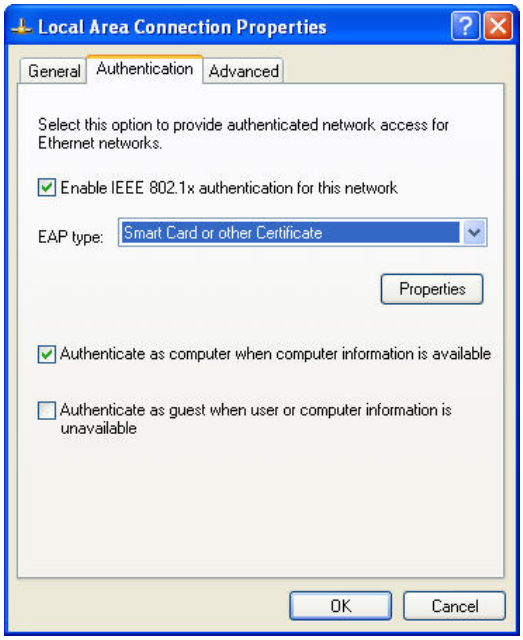
14. A user certificate for the domain user will now be installed in the **Certificates (Current User)** / **Personal / Certificates** store.



4.2 Modify Local Area Connection Properties:

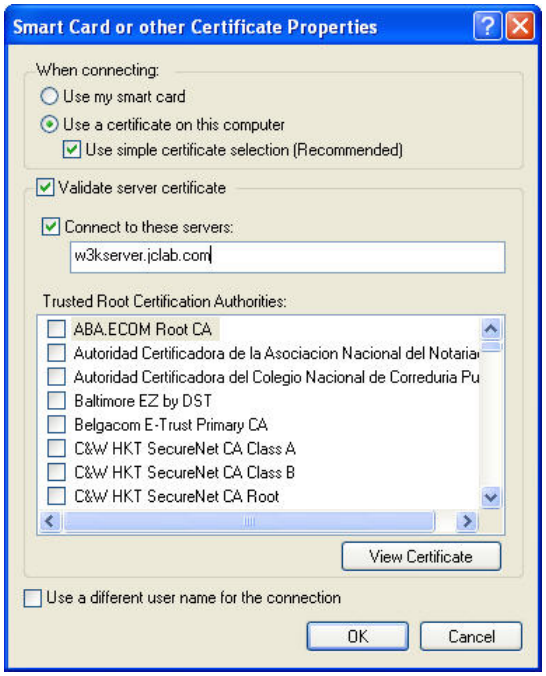
To enable 802.1X EAP-TLS computer and user authentication on a Windows XP Workstation:

1. Within Windows XP open the **Network Connections** Window Properties by clicking **Start**, **Control Panel**, **Network and Internet Connections** then **Network Connections**. Right click on the **Local Area Network Connection** and click **Properties**.
2. Click on the **Authentication** tab. In the **EAP type** pull-down menu select **Smart Card or other Certificate**.
3. Select the option **Authenticate as computer when computer information is available** which enables computer authentication.
4. Click **Properties**.



If the Authentication tab is not displayed in the Local Area Connection Properties window the Microsoft Wireless Zero Configuration service is not running. The Authentication tab will only display if the Microsoft Wireless Zero Configuration service is running (see **appendix 6.4**).

5. Select the default setting **Use simple certificate selection**.
6. Select the **Validate server certificate** checkbox. This allows Windows to verify the validity of the server certificate on the IAS RADIUS server.
7. Select the **Connect to these servers** checkbox and in the field ether type in the domain name upon which the RADIUS server must reside (example **jclab.com**) or the host and domain name of the IAS server (example **w3kserver.jclab.com**). This tells Windows XP to only authenticate against the servers in a domain that you specify.
8. Click **OK** and then **OK** again.



4.3 Modify Registry Settings:

By default the Windows XP 802.1X supplicant may not behave as expected when computer authentication is enabled. The Windows XP 802.1X supplicant behavior can be modified by adding the AuthMode and SupplicantMode registry entries:

4.3.1 AuthMode Registry Setting:

Purpose	Controls the computer and user authentication behavior on Windows XP Workstations.
Registry Path	HKEY_LOCAL_MACHINE\Software\Microsoft\EAPOL\Parameters\General\Global\AuthMode
Values	• 0 - Computer authentication mode. If computer authentication is successful, no user authentication is attempted. If the user logon is successful before computer authentication, user authentication is performed. This is the default setting for Windows XP (prior to Service Pack 1). • 1 - Computer authentication with re-authentication. If computer authentication is successful, a subsequent user logon results in a re-authentication with user credentials. The user logon has to complete in 60 seconds or the existing network connectivity is terminated. The user credentials are used for subsequent authentication or re-authentication. Computer authentication is not attempted again until the user logs off the computer. This is the default setting for Windows XP Service Pack 1 (SP1) and Windows Server 2003. • 2 - Computer authentication only. When a user logs on, it has no effect on the connection. Only computer authentication is performed. The exception to this behavior is when a user successfully logs on, and then roams between wireless APs. In that case, user authentication is performed. For changes to this setting to take effect, restart the Wireless Zero Configuration service for Windows XP or Windows Server 2003.

4.3.2 SupplicantMode Registry Setting:

Purpose	Controls the EAPOL-Start message behavior on Windows XP Workstations.
Registry Path	HKEY_LOCAL_MACHINE\Software\Microsoft\EAPOL\Parameters\General\Global\SupplicantMode
Values	• 1 - Do not transmit. Specifies that EAPOL-Start messages are not sent. • 2 - Transmit. Determines when to send EAPOL-Start messages and, if needed, sends an EAPOL-Start message. • 3 - Transmit per 802.1X. Sends an EAPOL-Start message upon association to initiate the 802.1X authentication process.

4.3.3 Nortel Recommendations:

Nortel recommends that the AuthMode registry entry be set to 1 and the SupplicantMode registry entry be set to 3 (see **Appendix 6.3**).

5. Verification:

5.1 Windows System Event Logs:

When a Windows XP workstation boots or the user logs out of Windows, EAP-TLS computer authentication will occur and the following log entry will be created in the Windows System Event Log:

```
Event Type:    Information
Event Source:  IAS
Event Category:       None
Event ID:      1
Date:          1/10/2007
Time:          11:34:05 AM
User:          N/A
Computer:      W3KSERVER1
Description:
User host/obsat.jclab.com was granted access.
 Fully-Qualified-User-Name = jclab.com/Computers/OBSAT
 NAS-IP-Address = 192.168.1.10
 NAS-Identifier = <not present>
 Client-Friendly-Name = ers5510-48t
 Client-IP-Address = 192.168.1.10
 Calling-Station-Identifier = 00-A0-D1-3D-A0-5E
 NAS-Port-Type = Ethernet
 NAS-Port = 1
 Proxy-Policy-Name = Use Windows authentication for all users
 Authentication-Provider = Windows
 Authentication-Server = <undetermined>
 Policy-Name = EAPOL Users
 Authentication-Type = EAP
 EAP-Type = Smart Card or other certificate
```

When a User logs into Windows XP EAP-TLS user authentication will occur and the following log entry will be created in the Windows System Event Log:

```
Event Type:    Information
Event Source:  IAS
Event Category:       None
Event ID:      1
Date:          1/10/2007
Time:          11:33:48 AM
User:          N/A
Computer:      W3KSERVER1
Description:
User marshal2@jclab.com was granted access.
 Fully-Qualified-User-Name = jclab.com/Users/Kevin L. Marshall
 NAS-IP-Address = 192.168.1.10
 NAS-Identifier = <not present>
 Client-Friendly-Name = ers5510-48t
 Client-IP-Address = 192.168.1.10
 Calling-Station-Identifier = 00-A0-D1-3D-A0-5E
 NAS-Port-Type = Ethernet
 NAS-Port = 1
 Proxy-Policy-Name = Use Windows authentication for all users
 Authentication-Provider = Windows
 Authentication-Server = <undetermined>
 Policy-Name = EAPOL Users
 Authentication-Type = EAP
 EAP-Type = Smart Card or other certificate
```

5.2 Ethernet Switch EAPOL Port Status:

When a computer or user is authenticated the EAPOL port status for the port will be displayed with the **Auth** status set to **Yes**. All unauthenticated ports will be displayed with the **Auth** status set to **No**.

```
ers5510-48t# show eapol port 1

     Admin          Admin Oper ReAuth ReAuth Quiet  Xmit   Supplic Server  Max
Port Status   Auth Dir   Dir  Enable Period Period Period Timeout Timeout Req
---- -------- ---- ----- ---- ------ ------ ------ ------ ------- ------- ---
1    Auto     Yes  Both  Both No     3600   10     30     30      30      2
```

6. Appendix:

6.1 EAPOL Users Active Directory Group:

The example Remote Access Policy used in this document tells IAS to authenticate users that are a member of the Windows Domain Group called **EAPOL Users**.

For EAP-TLS computer and user authentication to occur, the **Kevin L. Marshall** user account and **OBSAT** computer account were added as members to the **EAPOL Users** group as shown in Figure 6.1.1.

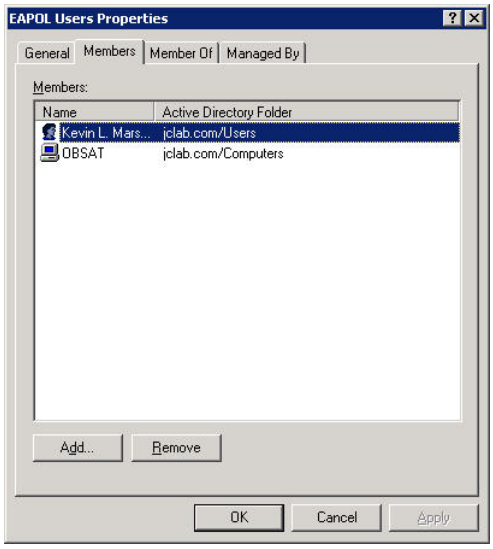


Figure 6.1.1 – EAPOL Users Active Directory Group

6.2 Active Directory Remote Access Permissions:

For EAP-TLS user and computer authentication to be successful, the remote access **Dial-In Access Permissions** for the user and computer accounts need to be set to **Allow access**. IAS cannot authenticate any user or computers unless the Dial-In permissions are set.

Figure 6.1.1 & 6.1.2 show the Remote Access Permission settings for the user account **Kevin L. Marshall** and computer account **OBSAT** used in this document.

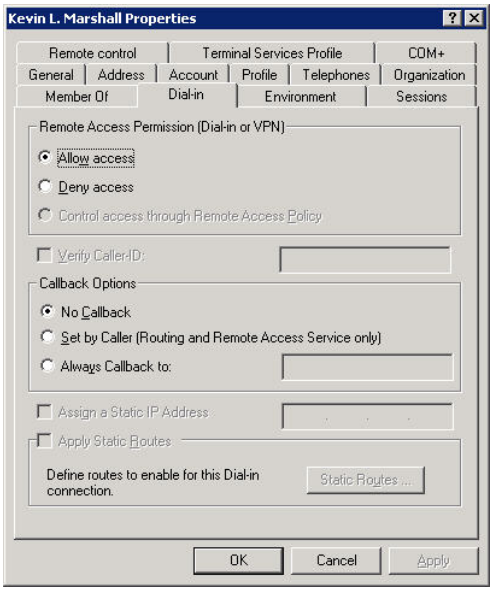


Figure 6.2.1 – Example Active Directory User Account Dial-In Permission Settings

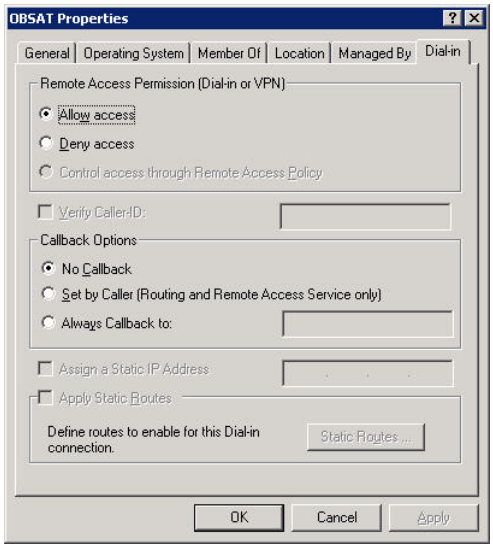


Figure 6.2.2 – Example Active Directory Computer Account Dial-In Permission Settings

6.3 Windows XP Registry Settings:

To ensure the correct Windows XP 802.1X supplicant behavior when performing computer and user authentication, the AuthMode and SupplicantMode registry keys were added. Figure 6.3.1 shows the recommended registry keys and DWORD values:

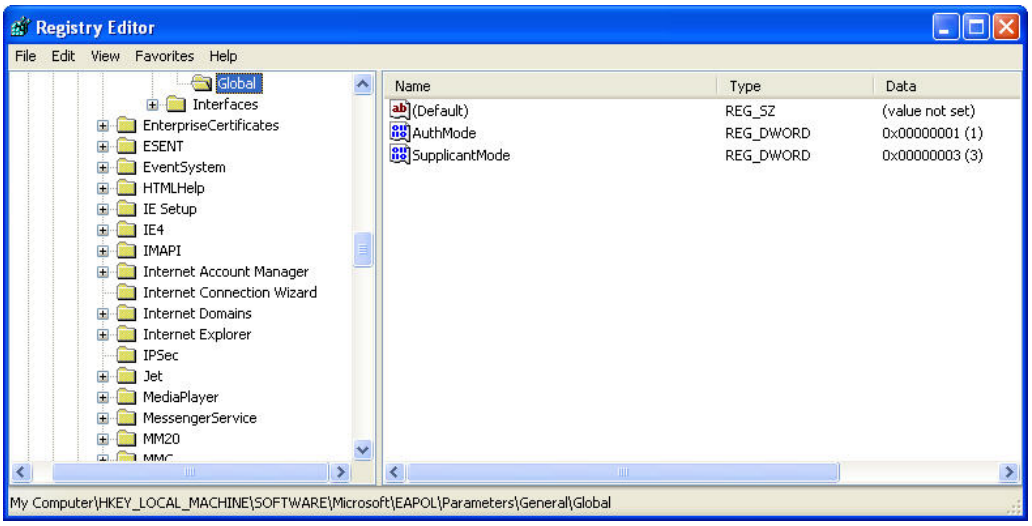


Figure 6.3.1 – Registry Entries

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\General\Global]
"AuthMode"=dword:00000001
"SupplicantMode"=dword:00000003
```

Figure 6.3.2 – Example Registry Entry File

6.4 Wireless Zero Configuration service:

The Microsoft Wireless Zero Configuration service provides native Windows support for 802.11 Wireless networking as well as 802.1X support for both Wired & Wireless networks.

Before you can enable or configure 802.1X wired computer and user authentication within Windows XP, the Microsoft Wireless Zero Configuration service has to be running. If the service is not in a Started state you will not be able to enable or configure or enable native 802.1X authentication for the Local Area Network connection.

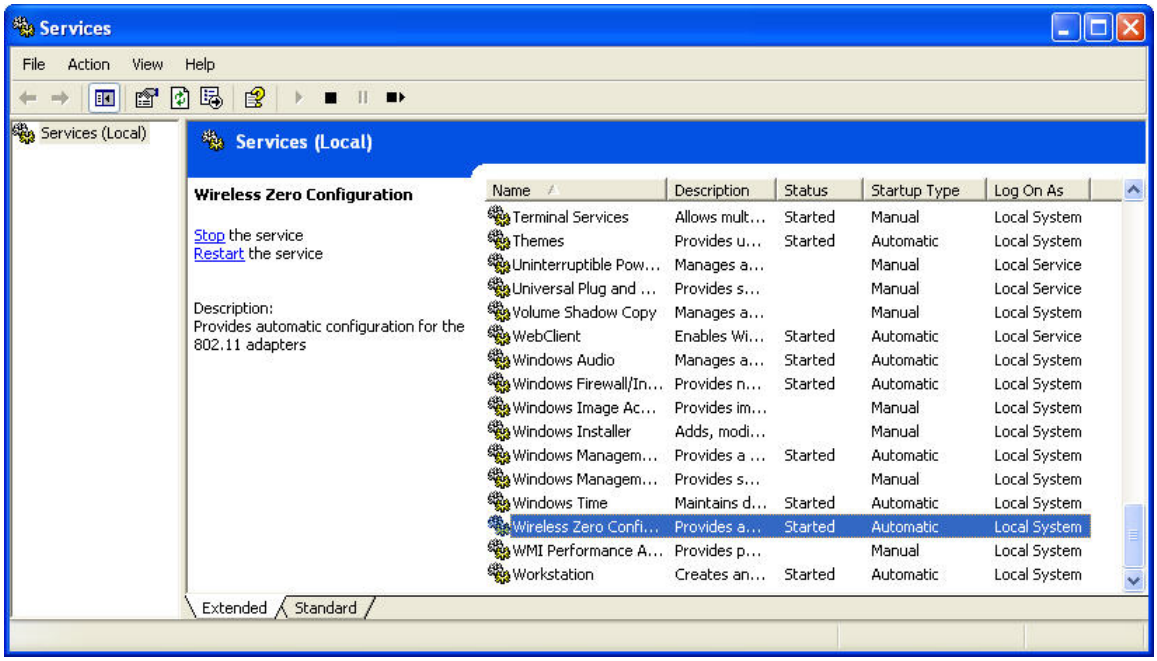


Figure 6.5.1 – Windows XP Services

By default the Microsoft Wireless Zero Configuration service is configured to automatically start and will have the service **Startup** type set to **Automatic**. If the service is disabled or stopped this may be due to a third-party 802.1X supplicant installed with a Wireless LAN NIC. Some third party 802.1X supplicants will disable or stop the Microsoft Wireless Zero Configuration service to eliminate conflict.

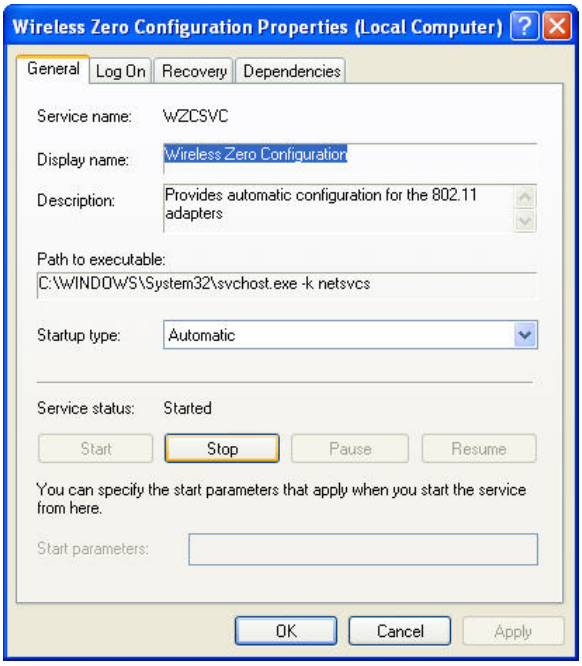


Figure 6.5.2 – Wireless Zero Configuration Service Properties

If you have a third-party 802.1X supplicant installed you can disable the third-party 802.1X supplicant on the NIC by disabling it in the Local Area Connection properties for the NIC. This will allow the Microsoft Wireless Zero Configuration service to start and also allow Windows to control the 802.1X authentication.

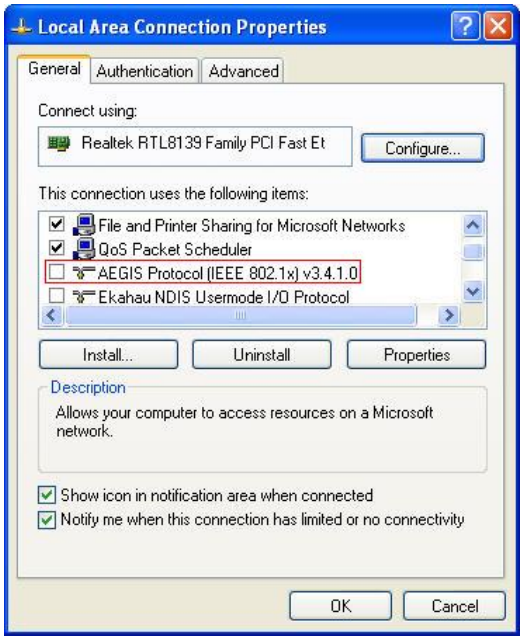


Figure 6.5.3 – Disabling a Third-Party 802.1X Driver

7. Reference Documentation:

Document Title	Publication Number	Description
Deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows	N/A	This Microsoft article describes the deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows and includes details on how to enable Auto-Enrollment for Computer certificates.
Certificate Autoenrollment in Windows Server 2003	N/A	This Microsoft article describes User / Smartcard certificate Autoenrollment Auto-Enrollment in Windows Server 2003 server environment.
Deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows	N/A	This article describes how to deploy IEEE 802.1X authentication for wired networks using authenticating switches, wired client computers running Microsoft® Windows® XP, Windows Server™ 2003, or Windows 2000, and a wired authentication infrastructure consisting of Windows Server 2003 or Windows 2000 Active Directory® directory service domain controllers, certification authorities, and Internet Authentication Service servers.
802.11 Wireless Tools and Settings	N/A	Microsoft TechNet article that includes details for modifying the 802.1X registry settings.

Contact us

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com/contactus.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.