How To | Use 802.1x EAP-TLS or PEAP-MS-CHAP v2 with Microsoft® Windows® Server 2003 to Make a Secure Network

Introduction

This document describes how to create a secure LAN, using two servers and an 802.1x-compatible Allied Telesis switch. The servers are running Microsoft Windows Server 2003.

This How To note takes you step-by-step through the configuration required for PEAP-MS-CHAP v2 authentication, then through the steps required for EAP-TLS authentication.

By showing you how to configure each device, this How To note gives you the building blocks to create a secure LAN.

You can also use this fragment in a lab, for testing 802.1x configurations.

PEAP-MS-CHAP v2:
Protected Extensible Authentication Protocol—Microsoft Challenge Handshake Authentication Protocol version 2

EAP-TLS:
Extensible Authentication Protocol—Transport Layer Security

What information will you find in this document?

Which products and software versions does this information apply to?

- Products:
  Rapier, AT-8800, AT-8600, AT-8700XL, AT-8900, and AT-9900 series switches
  AR750S, AR450S, and AR44xS series routers (802.1x supported on Eth and switch ports)
  AR410 series routers (802.1x supported on Eth ports)
- Software version: 2.7.1 and later

PEAP-MS-CHAP v2 Authentication

The infrastructure for this example 802.1x secure LAN consists of three computers performing the following roles:

- A computer running Microsoft Windows Server 2003, Enterprise Edition, named **DC1-CA**, that acts as a domain controller, a Domain Name System (DNS) server, and a certification authority (CA).
- A computer running Microsoft Windows Server 2003, Standard Edition, named **RADIUS**, that acts as a Remote Authentication Dial-in User Service (RADIUS) server.
- A computer running Microsoft Windows XP Professional Service Pack 1 (SP1), named **CLIENT1**, that acts as an 802.1x client.

Additionally, an Allied Telesis switch acts as an 802.1x authenticator to provide connectivity to the Ethernet intranet network segment for the 802.1x client (or supplicant).

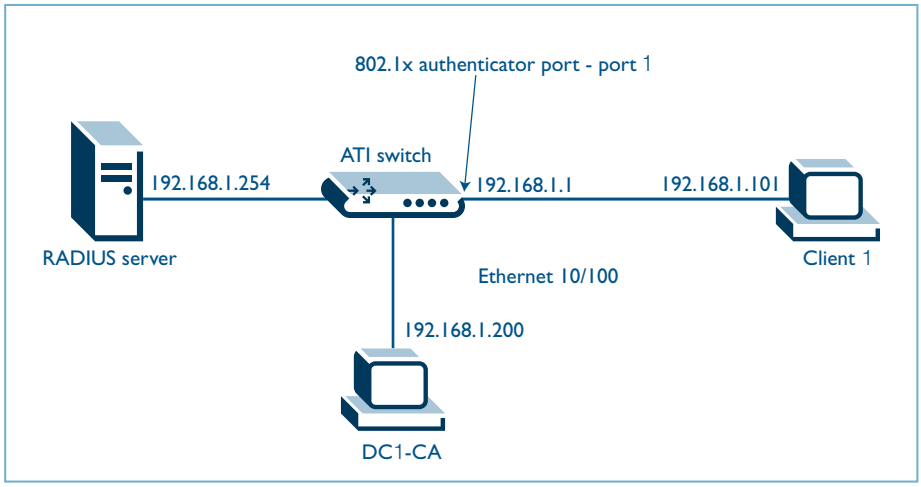


Figure 1: 802.1x LAN fragment

The four devices represent a network segment in a corporate intranet. In this example, all computers on the LAN are connected to a common 802.1x authenticating Allied Telesis switch. Private addresses of 192.168.1.0/24 are used on the LAN segment.

In this example all devices are configured with fixed addresses. To reconstruct this segment, configure the computers in the order presented.

DC1-CA

DC1-CA is a computer running Windows Server 2003, Enterprise Edition that is performing the following roles:

- A domain controller (DC) for the *example.com* domain, including Active Directory.
- The enterprise root certification authority (CA) for the *example.com* domain.
- A DNS server for the *example.com* DNS domain.

This PC uses Windows Server 2003, Enterprise Edition, so that you can configure autoenrollment of user and workstation certificates for EAP-TLS authentication, as described in "EAP-TLS Authentication" on page 24. Certificate autoenrollment and autorenewal make it easier to deploy certificates and improve the security by automatically expiring and renewing certificates.

To configure DC1-CA for these services, perform the following steps:

▶ Perform basic installation and configuration

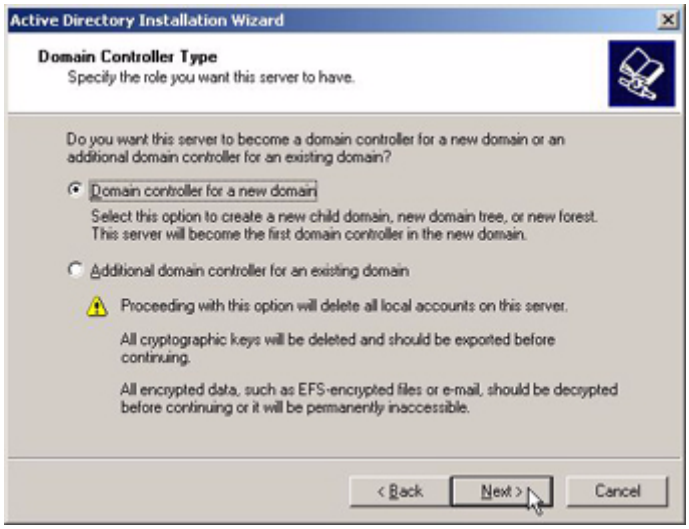
1. Install Windows Server 2003, Enterprise Edition, as a stand-alone server.
2. Click **Start**, right click **My Computer**, select **Properties**, click the **Computer Name** tab and type DC1-CA in **Computer Name**. Click **OK**.
3. Configure the TCP/IP protocol with the IP address of **192.168.1.200** and the subnet mask of 255.255.255.0.

   Ensure that the NIC card is plugged in.

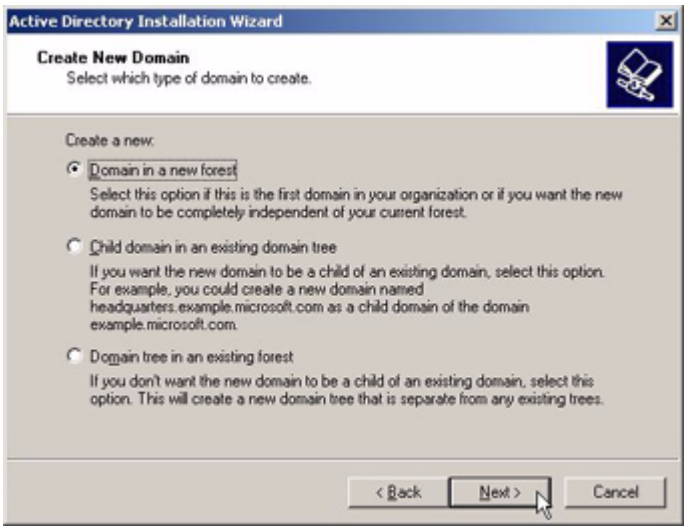
▶ Configure the computer as a domain controller

During the Active Directory you may accept defaults (as shown below) or specify your own preferences. You may be asked to insert the Windows Server 2003, CD ROM, and to restart the machine.

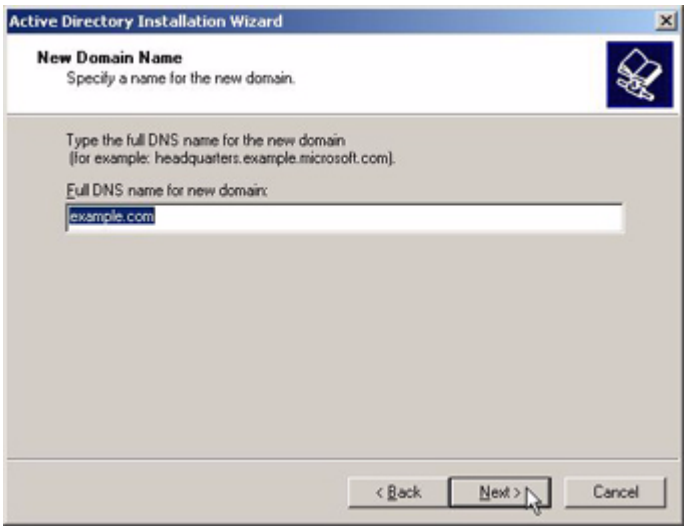
1. Click **Start**, click **Run**, type **dcpromo.exe**, and then click **OK** to start the Active Directory Installation Wizard.
2. In the Domain Controller Type page, select **Domain controller for a new domain**. Click **Next**.



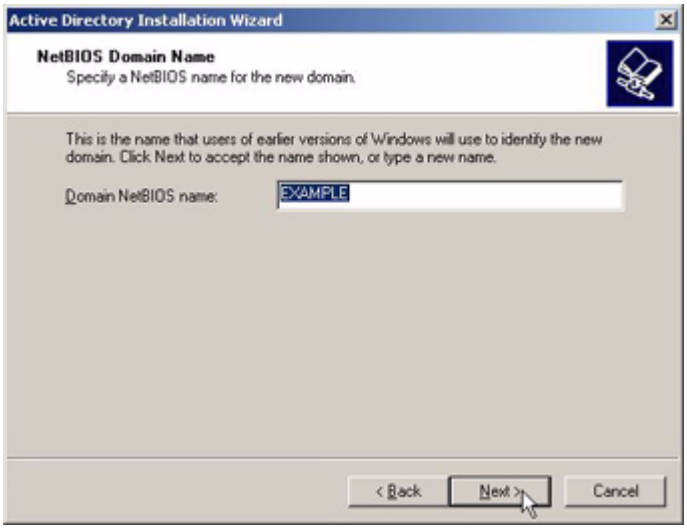
3. Select **Domain in a new forest.** Click **Next**.



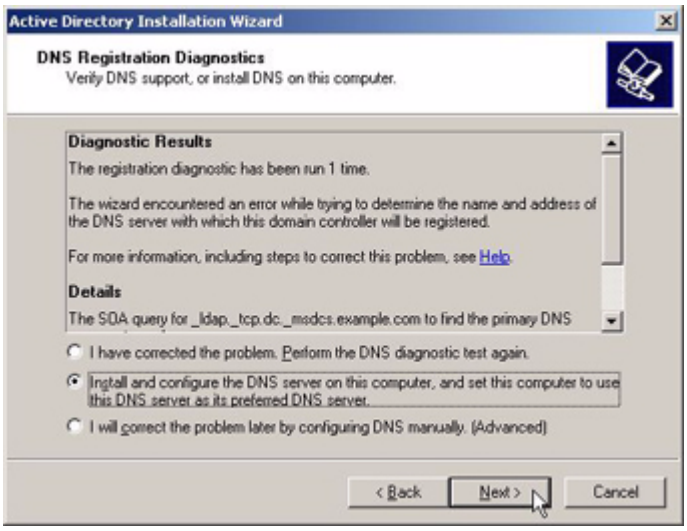
4. In the Full DNS name for new domain field, type **example.com**. Click **Next**.



5. In the Domain NetBIOS name field, EXAMPLE appears. If not, type it in. Click **Next**.



6. In the Database and Log Folders window, specify where you want to store the Active Directory database. Click **Next**.
7. In the Shared System Volume window, specify the folder and its location to be shared as the **SYSVOL** folder. Click **Next**.
8. In the DNS Registration Diagnostics window, select **Install and configure the DNS server on this computer to use this DNS server as its preferred DSN server**. Click **Next**.

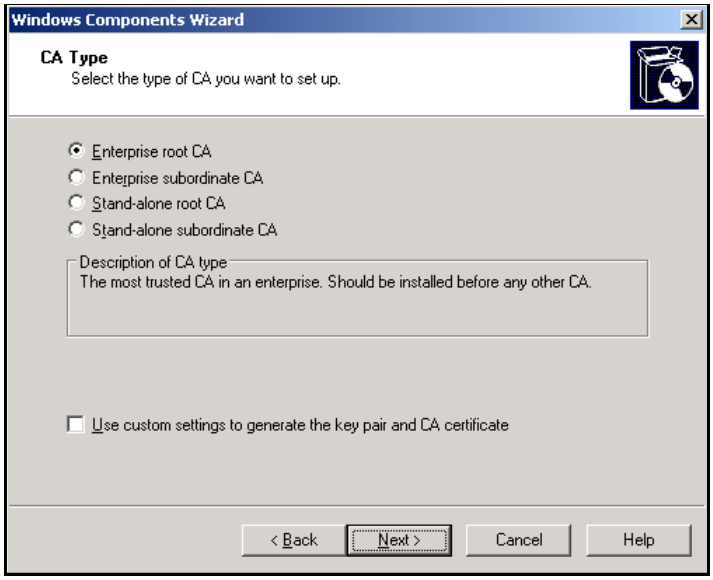


9. In the Permissions window, select **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**. Click **Next**.

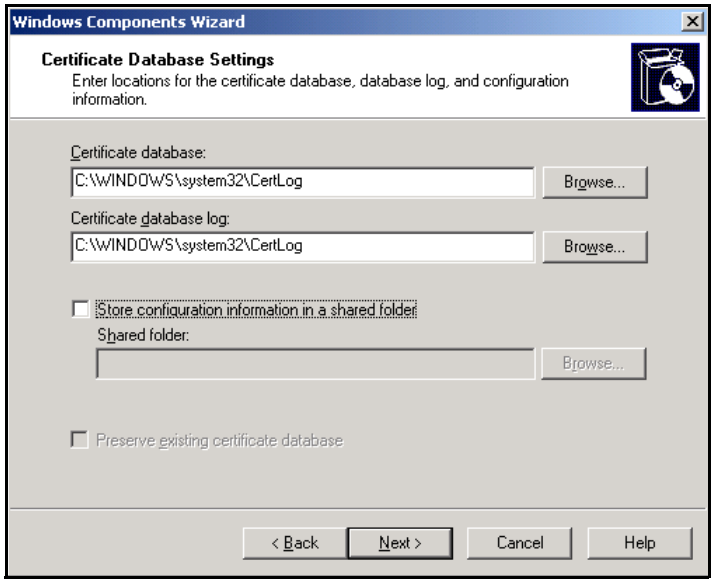
10. In the Directory Services Restore Mode Administrator Password window, enter passwords for the Administrator account. Click **Next** twice.

▶ Install Certificate Services

1. In **Control Panel**, open **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
2. In the **Windows Components Wizard** page, select **Certificate Services**, and then click **Next**.
3. In the **CA Type** page, select **Enterprise root CA**. This is shown in the following figure. Click **Next**.



4. Type **Example CA** in the **Common name for this CA** field, and then click **Next**. Accept the default **Certificate Database Settings**. This is shown in the following figure.

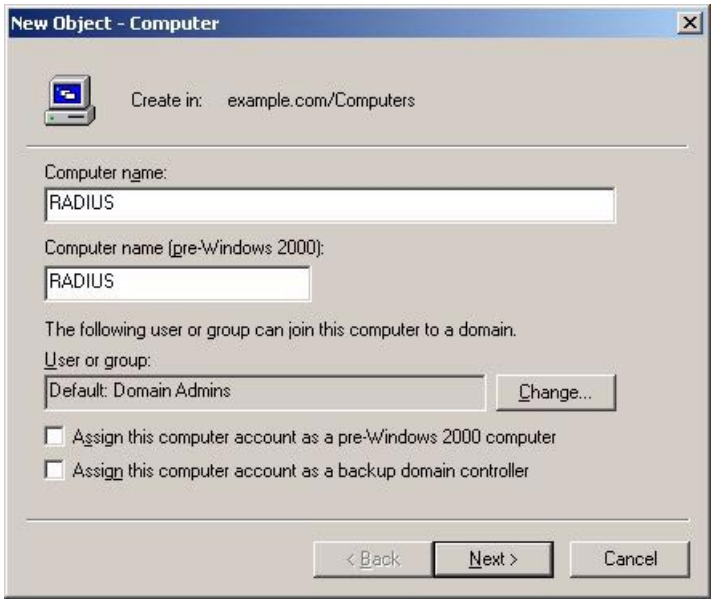


5. Click **Next**. Upon completion of the installation, click **Finish**. You may be asked to insert the Windows Server 2003 CD-ROM.

   Don't worry about IIS not being installed, click **OK** and continue.

▶ Add computers to the domain

1. Open the **Active Directory Users and Computers** snap-in (available from administrative tools).
2. In the console tree, expand *example.com*.
3. Right-click **Computers**, click **New**, and then click **Computer**.
4. In the **New Object - Compute**r dialog box, type **RADIUS** in **Computer name**. This is shown in the following figure.



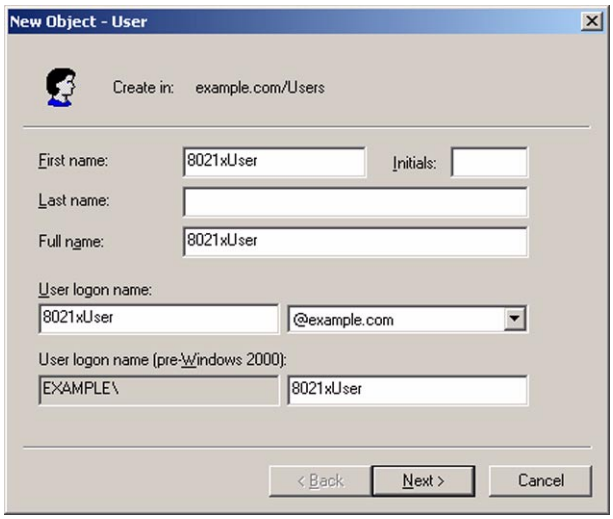
5. Click **Next**. In the **Managed** dialog box, click **Next**. In the **New Object - Computer** dialog box, click **Finish**.
6. Repeat steps 3-5 to create the additional computer account called: CLIENT1 (with no spaces).

▶ Allow 802.1x access to computers

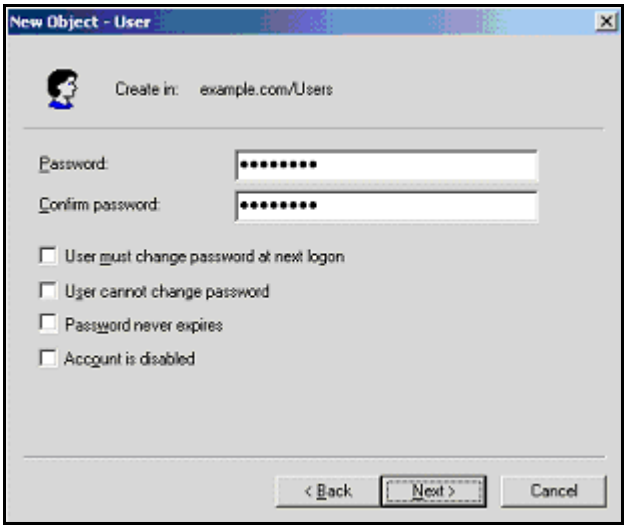
1. In the **Active Directory Users and Computers** console tree, click the **Computers** folder, right-click **CLIENT1**, click **Properties**, and then click the **Dial-in** tab.
2. Select **Allow access** and then click **OK**.

▶ Add users to the domain

1. In the **Active Directory Users and Computers** console tree, right-click **Users**, click **New**, and then click **User**.
2. In the **New Object - User** dialog box, type **8021xUser** in **First name** and type **8021xUser** in **User logon name**. This is shown in the following figure.



3. Click **Next**.
4. In the **New Object - User** dialog box, type a password of your choice in **Password** and **Confirm password**. Clear the **User must change password at next logon** check box. This is shown in the following figure.



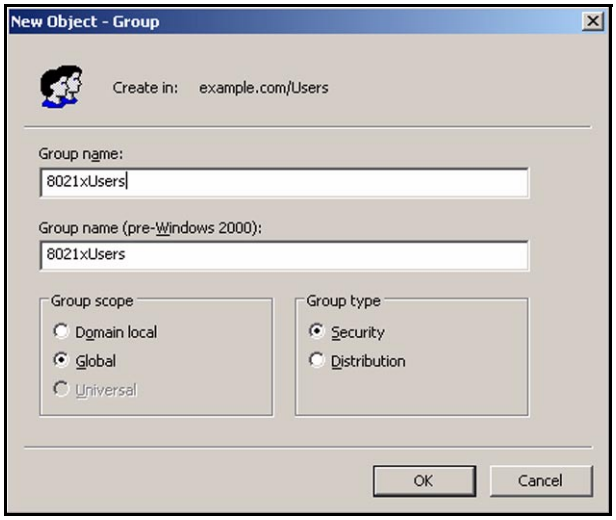
5. Click **Next** to continue the installation. Strictly speaking, you should give the 802.1x account an email address. However, if you are simply setting up for a test, that is not necessary.
6. Upon completion of the installation, click **Finish**.

▶ Allow 802.1x access to users

1. In the **Active Directory Users and Computers** console tree, click the **Users** folder, right-click **8021xUser**, click **Properties**, and then click the **Dial-in** tab.
2. Select **Allow access** and then click **OK**.

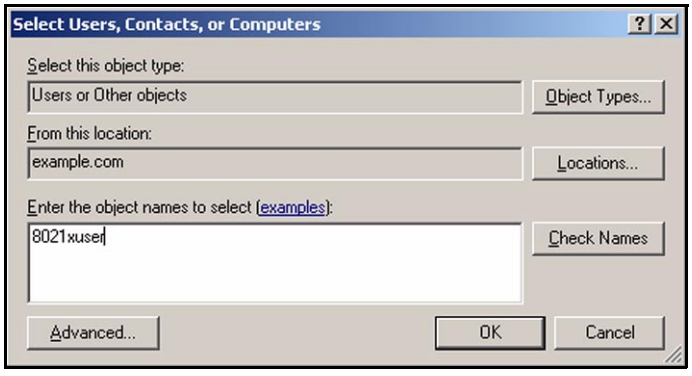
▶ Add groups to the domain

1. In the **Active Directory Users and Computers** console tree, right-click **Users**, click **New**, and then click **Group**.
2. In the **New Object - Group** dialog box, type **8021xUsers** in **Group name**, and then click **OK**. This is shown in the following figure.

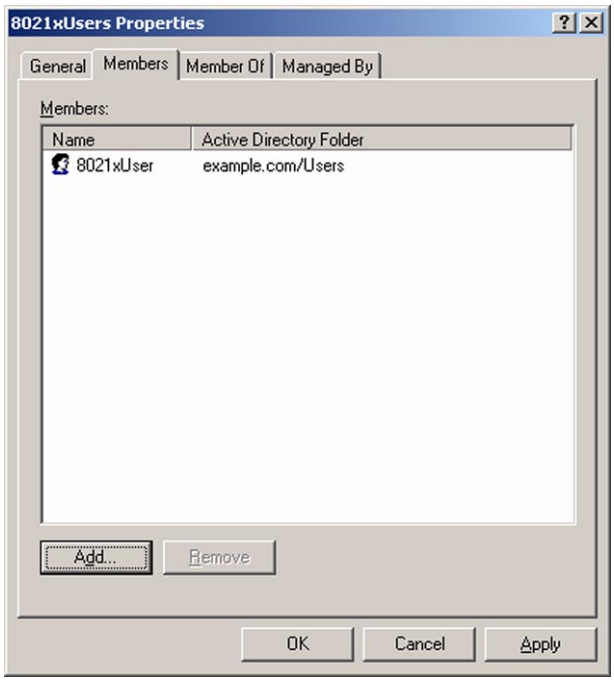


▶ Add users to 8021xUsers group

1. In the details pane of the **Active Directory Users and Computers**, double-click **8021xUsers**.
2. Click the **Members** tab, and then click **Add**.
3. In the **Select Users, Contacts, or Computers** dialog box, type **8021xUser** in **Enter the object names to select**. This is shown in the following figure.



4. Click **OK**.
5. The 8021xUser user account is added to the 8021xUsers group. This is shown in the following figure.

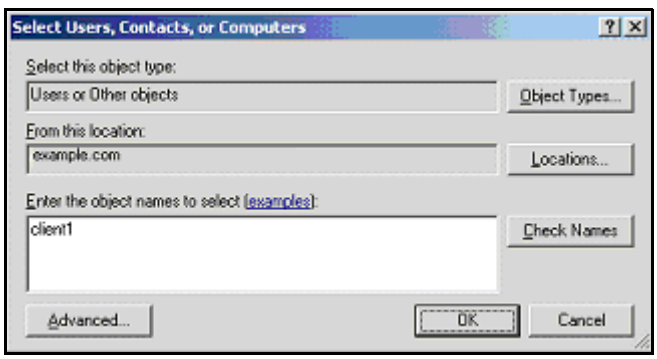


6. Click **OK** to save changes to the 8021xUsers group.

▶ Add the client computer to 8021xUsers group

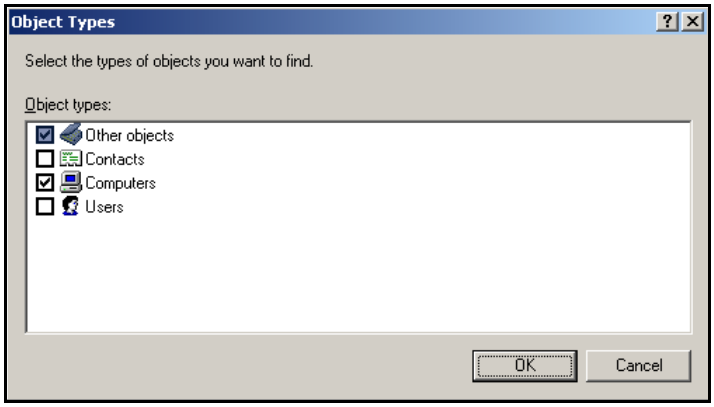
Note: *Adding client computers to the 8021xUsers group allows computer authentication. Computer authentication is needed so that the computer can attach to the 8021x network, obtain an IP address configuration (if DHCP is being used), locate Active Directory domain controllers, download the latest Computer Configuration Group Policy settings, and other computer startup processes.*

1. Repeat steps 1 and 2 in the preceding "Add users to 8021xUsers group" procedure.
2. In the **Select Users, Contacts, or Computers** dialog box, type **client1** in **Enter the object names to select**. This is shown in the following figure.

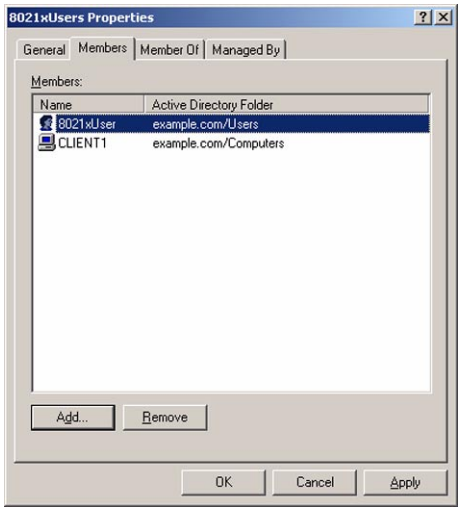


3. Click **Object Types**.

4. Clear the **Users** check box, and then select the **Computers** check box. This is shown in the following figure.



5. Click **OK** twice. The Client1 computer account is added to the 8021xUsers group.



6. Click **OK** to finish.

RADIUS

RADIUS is a computer running Windows Server 2003, Standard Edition, that provides RADIUS authentication and authorisation for the 802.1x Allied Telesis access switch. During this process the server PC named RADIUS will join as a member to the *example.com* domain.

Whenever you restart the PC, remember to log into the EXAMPLE domain.

To configure RADIUS as a RADIUS server, perform the following steps:

▶ Perform basic installation and configuration

1. Install Windows Server 2003, Standard Edition.
2. For the intranet local area connection, configure the TCP/IP protocol with the IP address of 192.168.1.254, the subnet mask of 255.255.255.0, and the DNS server IP address of 192.168.1.200.
3. Click **Start**, right click **My Computer**, select **Properties**, type RADIUS in **Computer Name**.
4. Click the **Change** button.
5. Type **example.com** in the **Member of Domain** field.
6. Click **OK**.

7. Enter the Administrator User name and password.
8. Click **OK**
9. Restart the machine.
10. Logout and login to the RADIUS server as "administrator" in the example.com domain. Domain selection is available under login options.

▶ Install and configure Internet Authentication Service

1. From **Control Panel** select **Add or Remove Programs**, click **Add/Remove Windows Component** and install the part of **Networking Services** called **Internet Authentication**.

Note: *To install individual parts of Networking Services, click on the **Details** button, and select the elements you require. You may be required to insert the Windows Server 2003, CD-ROM.*

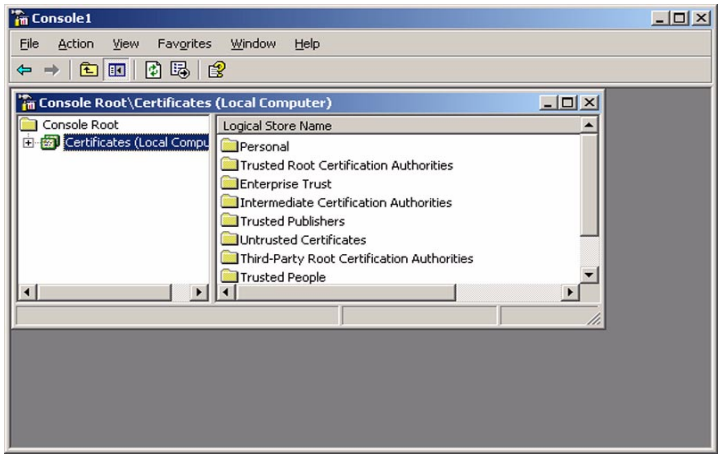
2. In the Administrative Tools folder, open the **Internet Authentication Service** snap-in.
3. Right-click **Internet Authentication Service**, and then click **Register Server in Active Directory**. When the **Register Internet Authentication Server in Active Directory** dialog box appears, click **OK**. This is shown in the following figure.

A message should confirm registration and authorisation to refer to users properties. If you see the following error, you need to make sure you are logged in as the example.com administrator.

▶ Create the certificates (Local Computer) console

Use the following steps to create an MMC console on your RADIUS server that contains the Certificates (Local Computer) snap-in.

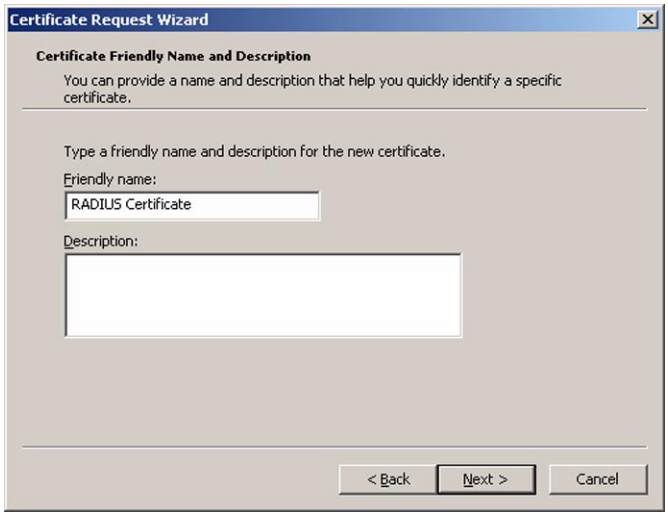
1. Click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the Console **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Under **Snap-in**, double-click **Certificates**, click **Computer account**, and then click **Next**.
4. Select **Local computer**, click **Finish**, click **Close**, and then click **OK**. The Certificates (Local Computer) snap-in is shown in the following figure.



Note: *PEAP with MS-CHAP v2 requires certificates on the RADIUS servers but not on the 802.1x clients. Autoenrollment of computer certificates for the RADIUS servers can be used to simplify a deployment. However, in this "PEAP-MS-CHAP v2 Authentication" section, a certificate is manually requested for the RADIUS computer because the autoenrollment of the certificates is not yet configured. This is described in "EAP-TLS Authentication" on page 24.*

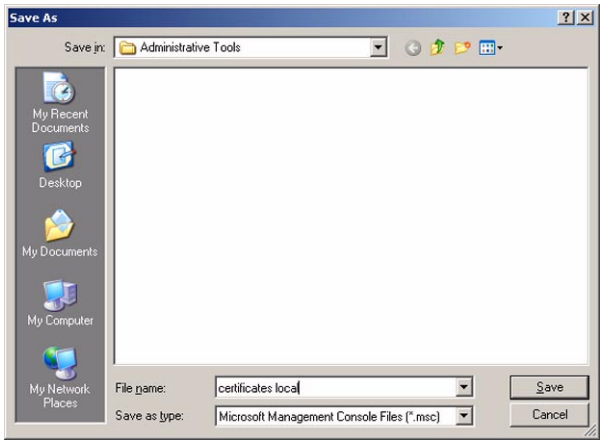
▶ Request computer certificate

1. Right-click the **Personal** folder, click **All Tasks**, click **Request New Certificate**, and then click **Next**.
2. Click **Computer** for the **Certificate types**, and then click **Next**.
3. Type **RADIUS Certificate** in **Friendly name**. This is shown in the following figure.



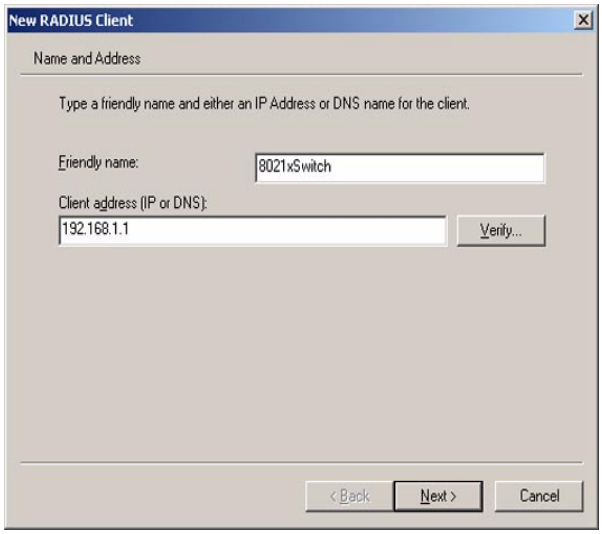
4. Click **Next**. On the **Completing the Certificate Request** Wizard page, Click **Finish**.
5. A "The certificate request was successful" message is displayed. Click **OK**.

6. You may wish to save mmc console settings as "certificates_local".



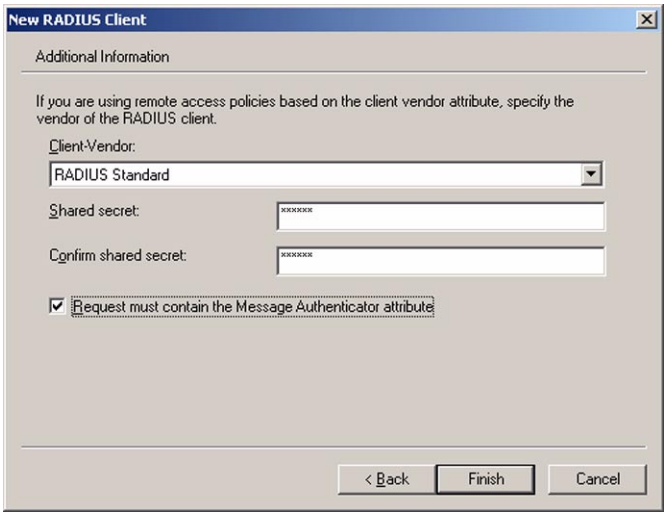
▶ Add the 802.1x Allied Telesis switch as RADIUS client

1. Click **Start**, select **Admin Tools**, then select **Internet Authentication Service**.
2. In the console tree of the **Internet Authentication Service** snap-in, right-click **RADIUS Clients**, and then click **New RADIUS Client**.
3. In the **Name and Address** page of the New RADIUS Client wizard, for **Friendly name**, type **8021xSwitch**. In **Client address (IP or DNS)**, type **192.168.1.1**, and then click **Next**. This is shown in the following figure.



4. Click **Next**. In the **Additional Information** page of the New RADIUS Client wizard, for **Shared secret**, type a shared secret for the 802.1x access switch, and then type it again in **Confirm shared secret**. Tick **Request must contain the Message Authenticator attribute**. This is shown in the following figure.

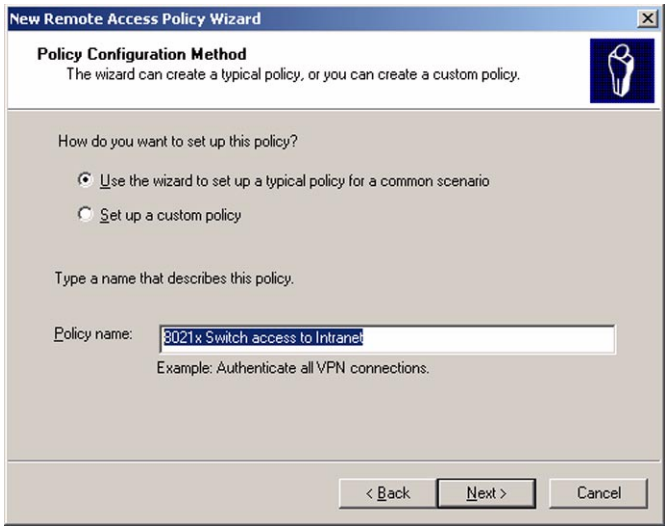
Note: *The shared secret entered here needs to match the shared secret on the configuration of the 802.1x access switch. Refer to "802.1x Edge Switch" on page 19.*



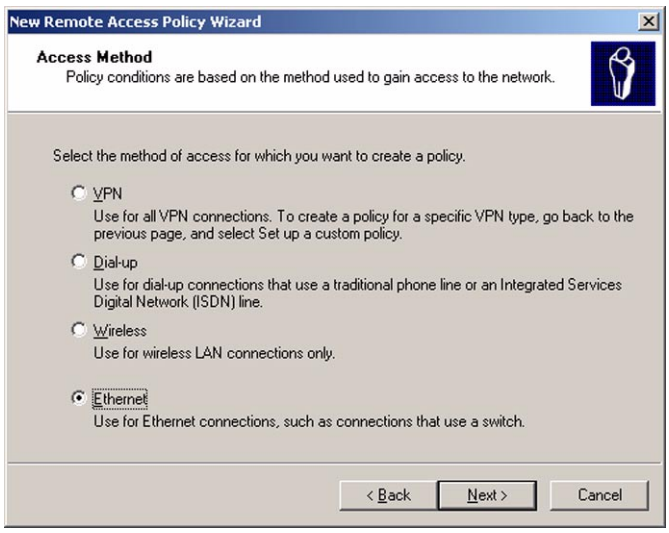
5. Click **Finish**.

▶ Create and configure remote access policy

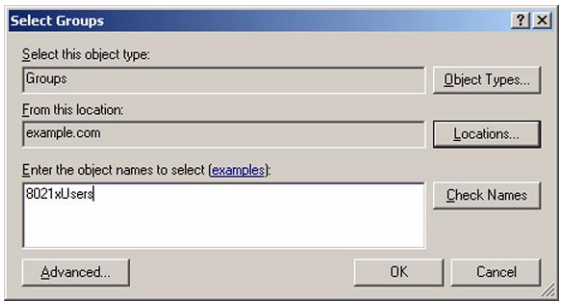
1. In the console tree of the Internet Authentication Service snap-in, right-click **Remote Access Policies**, and then click **New Remote Access Policy**.
2. On the **Welcome to the New Remote Access Policy Wizard** page, click **Next**.
3. On the **Policy Configuration Method** page, type **8021x Switch access to intranet** in **Policy name**. This is shown in the following figure.



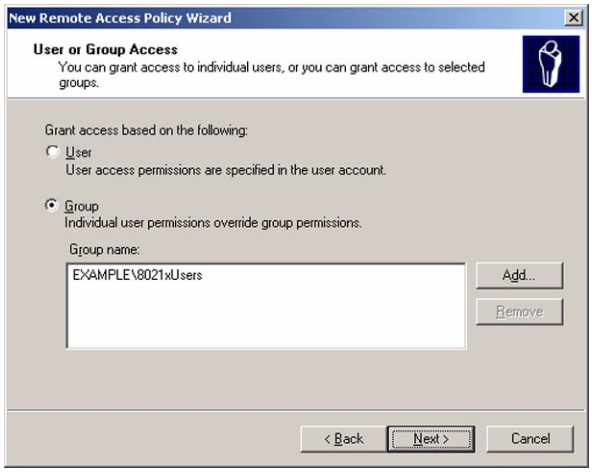
4. Click **Next**. On the **Access Method** page, select **Ethernet**.This is shown in the following figure.



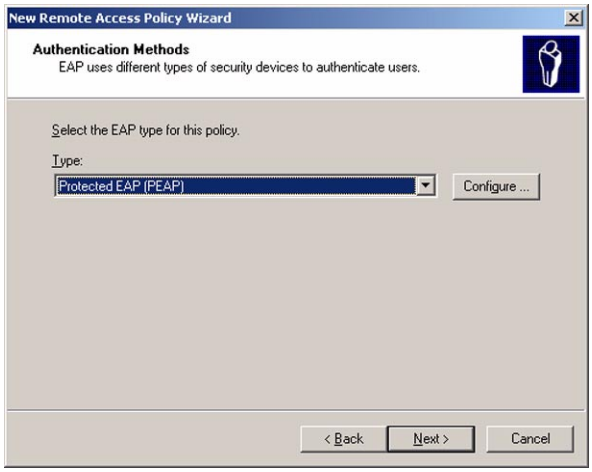
5. Click **Next**. On the **User or Group Access** page, select **Group**.
6. Click **Add**. In the **Select Groups** dialog box, type **8021xUsers** in the **Enter the object names to select** box. Verify that *example.com* is listed in the **From this location** field. This is shown in the following figure. If it's not listed - click on the **Locations** button to select a location.



7. Click **OK**. The 8021xUsers group in the example.com domain is added to the list of groups on the Users or Groups page. This is shown in the following figure.



8. Click **Next**. On the **Authentication Methods** page, select **Protected EAP (PEAP)** from the **Type** drop down list.



9. Click **Next**. On the **Completing the New Remote Access Policy** page, click **Finish**.

802.1x Edge Switch

An Allied Telesis L3 switch takes on the 802.1x challenger role. The switch is used as a secure access point, rather than using a wireless access point.

▶ Configure the Allied Telesis switch

1. Connect the console port of the switch to a Com port on a PC running a terminal emulator.

2. Login to your switch.

The login prompt appears on the terminal emulator. If the login prompt does not appear, press [Enter] two or three times. When the switch boots for the first time it automatically creates an account with manager privileges. The account has the login name “manager” and the password is “friend”. Passwords are case sensitive.

At the login prompt, enter the login name and password.

```
Login: manager
Password: friend
```

The switch’s command prompt appears and you can now configure the switch using the command line interface.

3. Name the switch:

```
set sys name="8021x authenticator"
```

4. Define an IP address for VLAN1:

```
ena ip
add ip int=vlan1 ip=192.168.1.1 mask=255.255.255.0
```

5. Define a RADIUS server and it's shared secret. The RADIUS server will be used for user authentication:

```
add radius server=192.168.1.254 secret="secret"
```

6. Define 802.1x port authentication. Port 1 is the authenticator for this example segment. In a real network, configure multiple ports as required:

```
enable portauth
enable portauth port=1 type=authenticator
```

Note: *The shared secret entered here needs to match the shared secret on the "Add the 802.1x Allied Telesis switch as RADIUS client" on page 15*

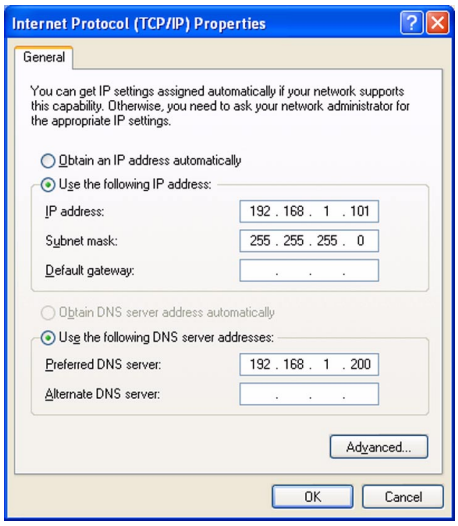
CLIENT 1

CLIENT1 is a computer running Windows XP Professional SP1 that is acting as an 8021x Access client. It will obtain access to intranet resources through the 8021x Access Switch. To configure CLIENT1 as an 8021x Access client, perform the following steps:

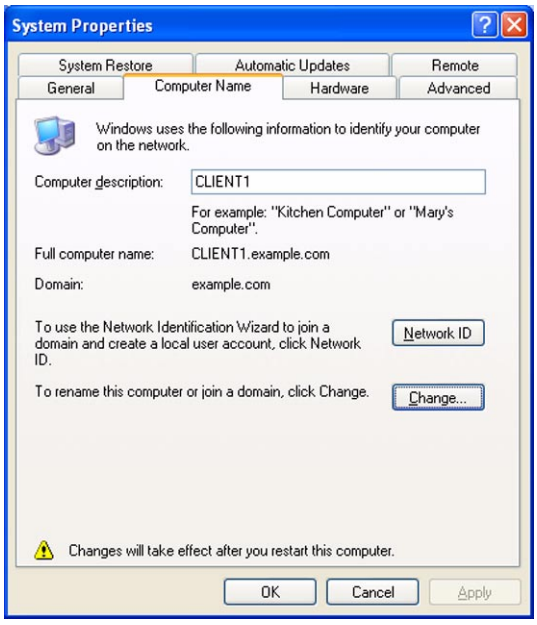
▶ Perform basic installation and configuration

Use the following steps on CLIENT1 to install Windows XP Professional as a member computer named CLIENT1 of the example.com domain.

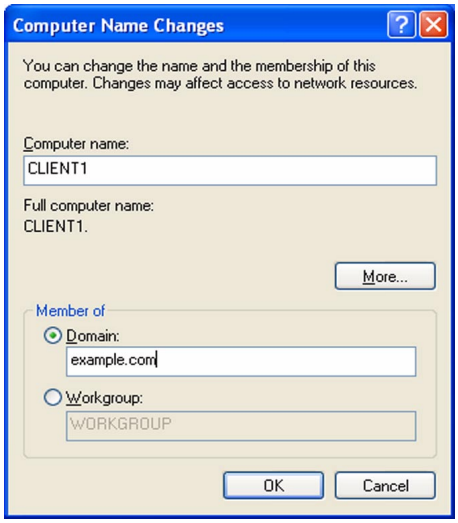
1. Connect CLIENT1 to a **non-authenticating port** on the Allied Telesis switch, and define a valid network address - such as 192.168.1.101. You also need to define the DNS address, 192.168.1.200.



2. Click **Start**, right click **My Computer**, select **Properties**, type CLIENT1 in **Computer Name**, and then click the **Change** button.



3. Type example.com in **Member of Domain**.



4. Click **OK**
5. Login.

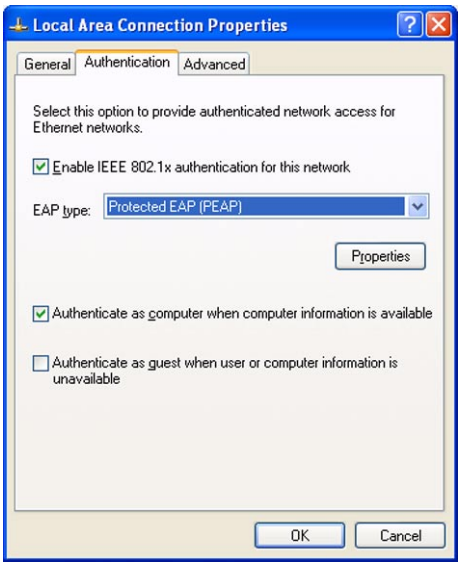
6. Click **OK** twice, and restart the machine.
7. Login to example.com domain using the 8021xUser name and password.

Note: *After restart, you must log in as 8021x User, NOT administrator.*

▶ Setup Local Area Connection Network Properties

Note: Windows XP SP1must be installed in order to have PEAP support.

1. Click **Start / Control Panel / Network and Internet Connections / Internet Connections**
2. On the **Authentication** tab, configure the LAN network properties for PEAP-MS-CHAP v2 authentication. The configuration is shown in the following figure. Click **OK**.



3. Now move CLIENT1 PC to the 802.1x **authenticator port** on the 8021x Allied Telesis switch. Our example uses port1.
4. Logout and login.

At this point you will test the 802.1x authentication using the PEAP method. Note that sometimes this may take a few minutes.

Confirmation of authenticated connection

You can verify the progress of 802.1x authentication by monitoring the Local Area Connection icon on the Network Connections window. It should pass through an authenticating stage to a connected stage. You can then verify basic connectivity from the command window by pinging other devices in the intranet, such as 192.168.1.254 (RADIUS) and 192.168.1.200 (DC1-CA).

- You can also check authentication on the Allied Telesis switch using the command:

  ```
  sh portauth port=1
  ```

- If needed, debugging can also be enabled using the command:

  ```
  ena portauth debug=all port=1
  ```

  To see all the relevant debug you may need to logout and login again as 8021xUser—in the example.com domain.

- Another possible reason for authentication failure is the interaction between the Allied Telesis switch and the RADIUS server. Check that you have configured the correct secret for the RADIUS server.

- You can also check RADIUS debugging. On the Allied Telesis switch, use the command:

  ```
  ena radius debug=decode
  ```

  On the RADIUS server you can use the event viewer, available from administrative tools.

EAP-TLS Authentication

This section describes how to modify the previous configuration to use Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication.

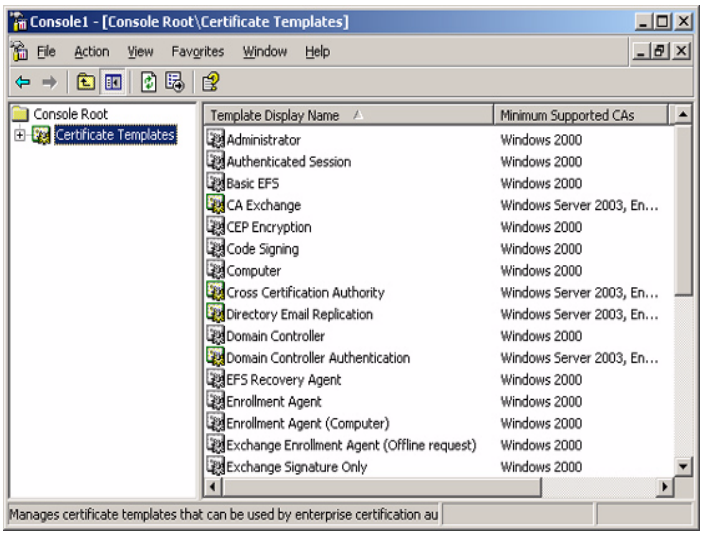
EAP-TLS authentication requires computer and user certificates on the 802.1x client, the addition of EAP-TLS as an EAP type to the remote access policy for Local Area Connection access, and a reconfiguration of the Local Area Connection.

DC1-CA

To modify DC1-CA so that it provides autoenrollment for computer and user certificates, perform the following steps.

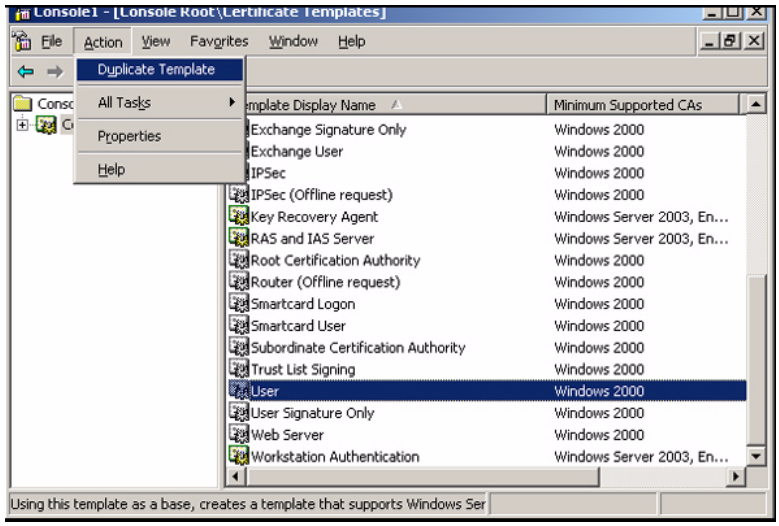
▶ Install Certificate Templates snap-in

1. Click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Under **Snap-in**, double-click **Certificate Templates**, click **Close**, and then click **OK**.
4. In the console tree, click **Certificate Templates**. All of the certificate templates will be displayed in the details pane. This is shown in the following figure:

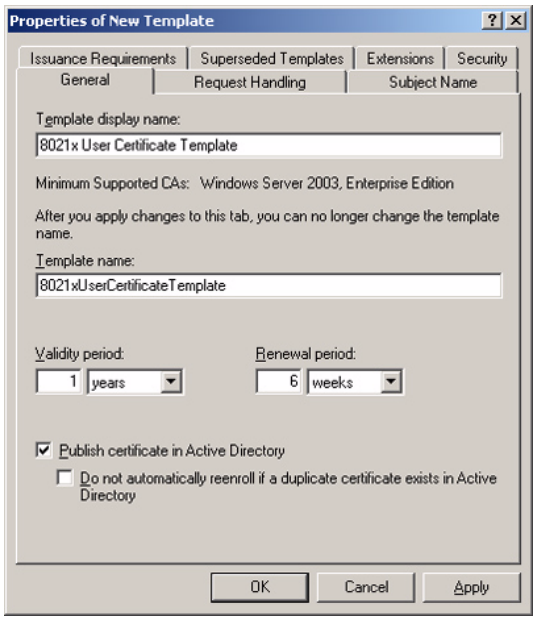


▶ Create certificate template for 802.1x users

1. In the details pane of the **Certificate Templates** snap-in, click the **User** template.
2. On the **Action** menu, click **Duplicate Template**. This is shown in the following figure.

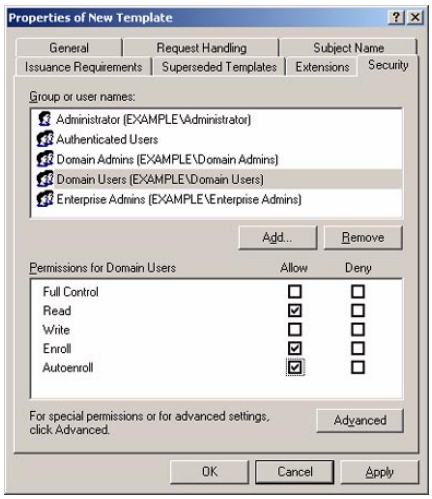


3. In the **Template display Name** field, type **8021x User Certificate Template**. This is shown in the following figure.

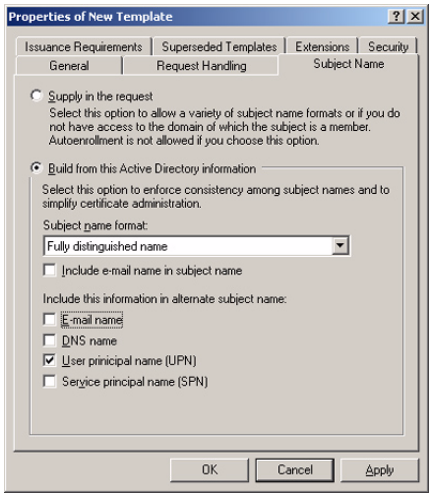


▶ Configure certificate template

1. In the **Properties of New Template** dialog box, make sure that the **Publish Certificate in Active Directory** check box is selected.
2. Click the **Security** tab.
3. In the **Group or user names** field, click **Domain Users**.
4. In the **Permissions for Domain Users** list, select the **Read**, **Enroll**, and **Autoenroll** check boxes. This is shown in the following figure.



5. If you are setting up for a test, click the **Subject Name** tab and ensure that **Include e-mail name in subject name** and **E-mail name** boxes are cleared. This is shown in the following figure.

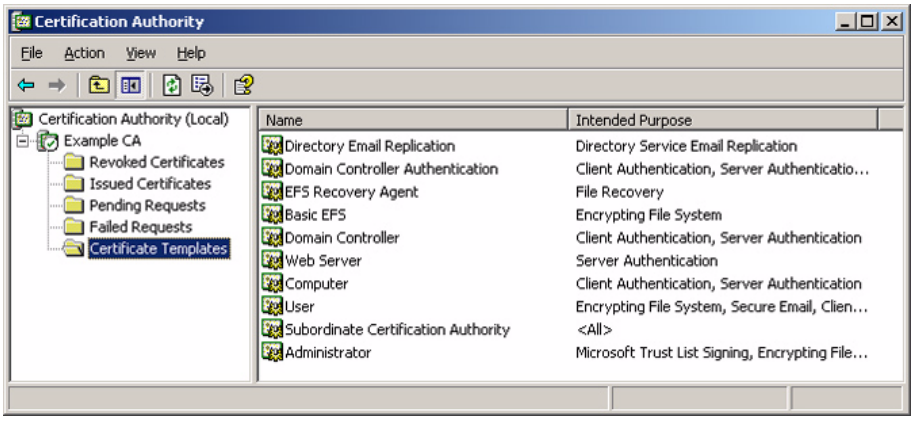


Note: *You need to clear these two boxes unless you either gave the 802.1xUser account a valid email address, or did not choose to have autoenrollment of the user certificate distributed to the client.*

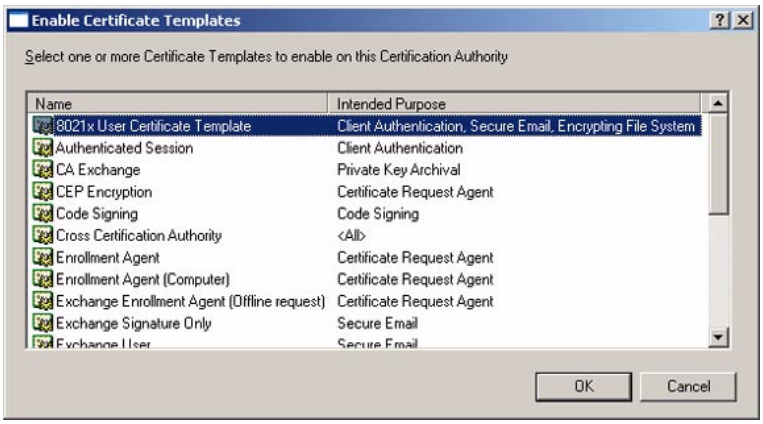
6. Click **OK**.

▶ Enable certificate template

1. Open the **Certification Authority** snap-in (from administrative tools).
2. In the console tree, expand **Example CA**, and then click **Certificate Templates**. This is shown in the following figure.

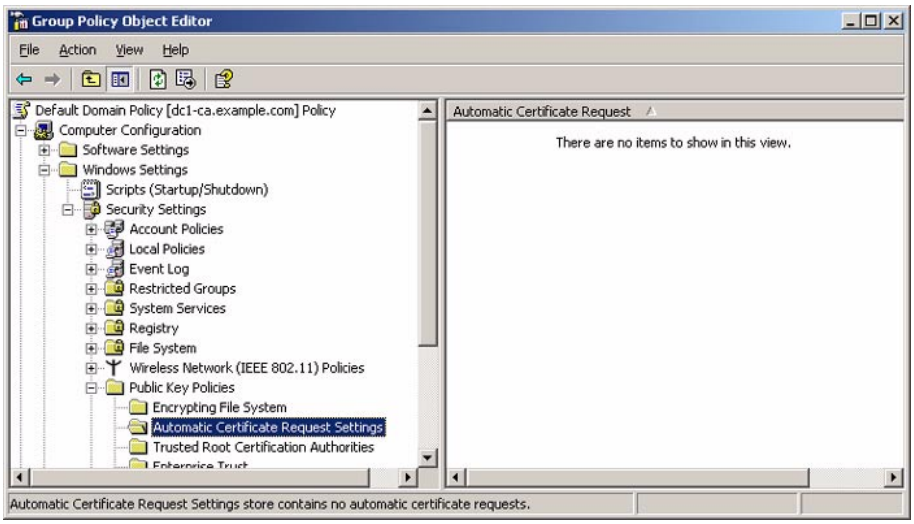


3. On the **Action** menu, point to **New**, and then click **Certificate Template to Issue**.
4. Click **8021x User Certificate Template**. This is shown in the following figure.

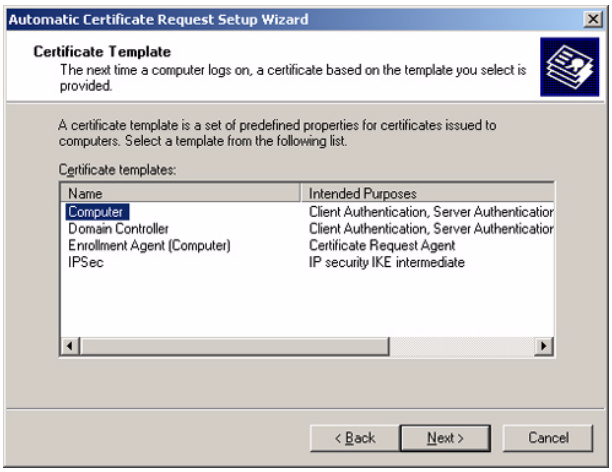


5. Click **OK**.
6. Open the **Active Directory Users and Computers** snap-in (from administrative tools).
7. In the console tree, double-click **Active Directory Users and Computers**, right-click the *example.com* domain, and then click **Properties**.
8. On the **Group Policy** tab, click **Default Domain Policy**, and then click **Edit**. This opens the Group Policy Object Editor snap-in.

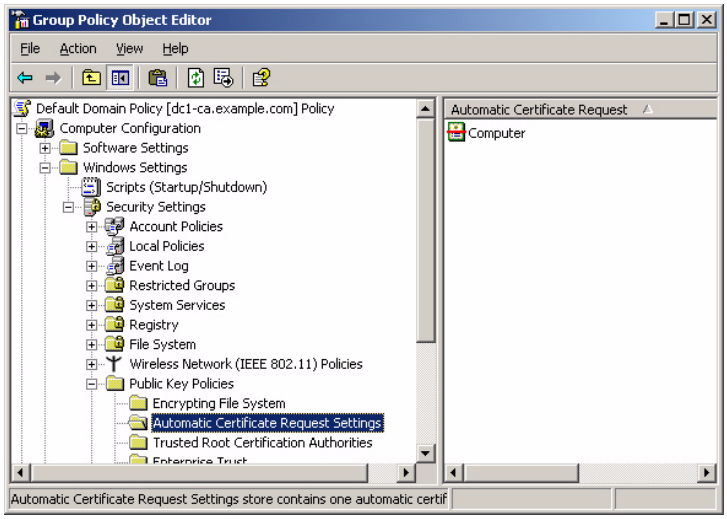
9. In the console tree, expand **Computer Configuration**, **Windows Settings**, **Security Settings**, and **Public Key Policies**, and then click **Automatic Certificate Request Settings**. This is shown in the following figure.



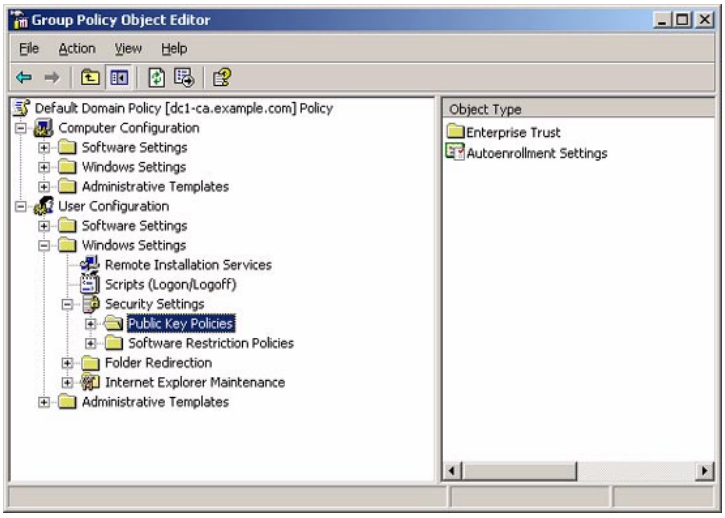
10. Right-click **Automatic Certificate Request Settings**, point to **New**, and then click **Automatic Certificate Request**.
11. On the **Welcome to the Automatic Certificate Request Setup Wizard** page, click **Next**.
12. On the **Certificate Template** page, click **Computer**. This is shown in the following figure.



13. Click **Next**. On the **Completing the Automatic Certificate Request Setup Wizard** page, click **Finish**. The **Computer** certificate type now appears in the details pane of the Group Policy Object Editor snap-in. This is shown in the following figure.



14. In the console tree, expand **User Configuration**, **Windows Settings**, **Security Settings**, and **Public Key Policies**. This is shown in the following figure.



15. In the details pane, double-click **Autoenrollment Settings**.
16. Click **Enroll certificates automatically**. Select the **Renew expired certificates**, **update pending certificates**, and **remove revoked certificates** check box. Select the **Update certificates that use certificate templates** check box. This is shown in the following figure.

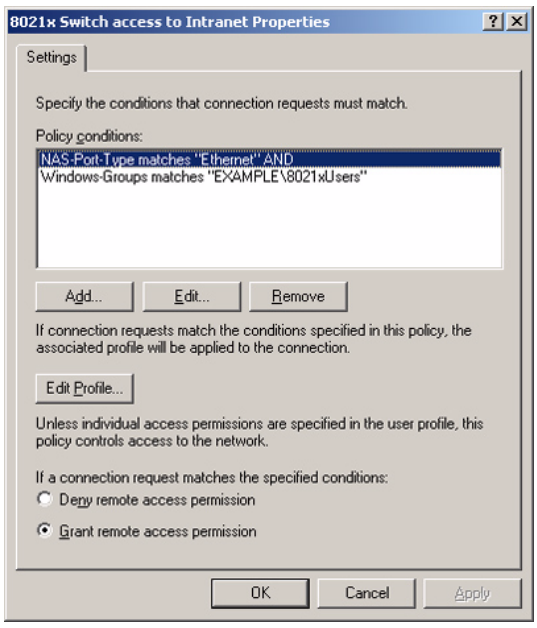
17. Click **OK**.

RADIUS

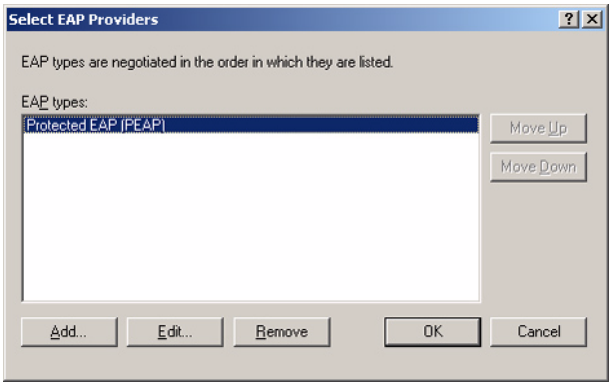
To modify RADIUS so that it uses EAP-TLS authentication, perform the following steps:

▶ Configure RADIUS to use EAP-TLS

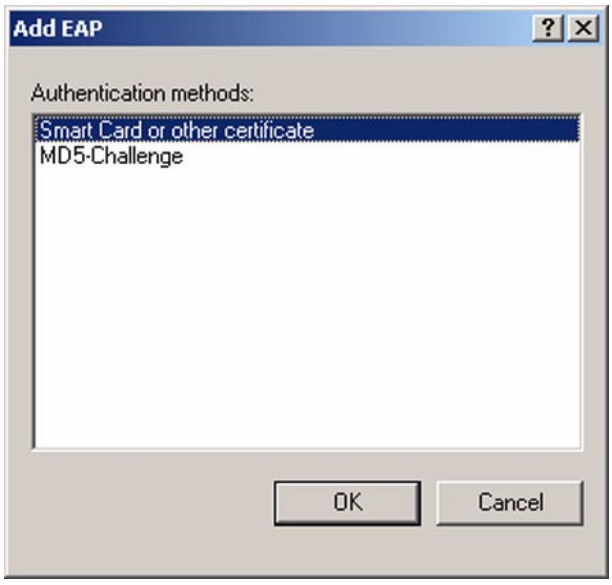
1. Open the **Internet Authentication Service** snap-in (from administrative tools).
2. In the console tree, click **Remote Access Policies**.
3. In the **details** pane, double-click **802.1x access to intranet**. The **802.1x access to intranet Properties** dialog box is displayed. This is shown in the following figure.



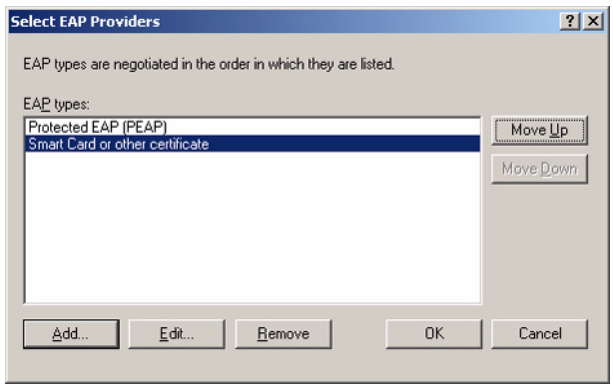
4. Click **Edit Profile**, and then click the **Authentication** tab.
5. On the **Authentication** tab, click **EAP Methods**. The **Select EAP Providers** dialog box is displayed. This is shown in the following figure.



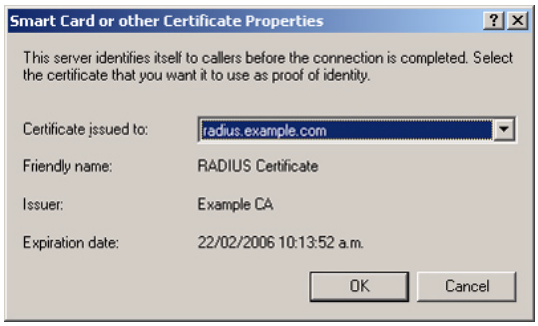
6. Click **Add**. The **Add EAP** dialog box is displayed. This is shown in the following figure.



7. Click **Smart Card or other certificate**, and then click **OK**. The **Smart Card or other certificate type** is added to the list of EAP providers. This is shown in the following figure.

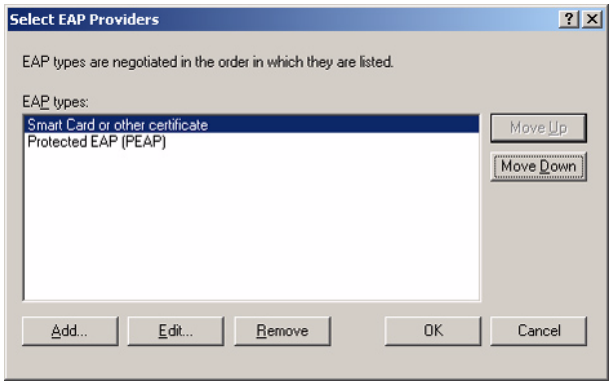


8. Click **Edit**. The **Smart Card or other Certificate Properties** dialog box is displayed. This is shown in the following figure.



9. The properties of the computer certificate issued to the RADIUS computer are displayed. This step verifies that IAS has an acceptable computer certificate installed to perform EAP-TLS authentication. Click **OK**.

10. Click **Move Up** to make the Smart Card or other certificate EAP provider the first in the list. This is shown in the following figure.



11. Click **OK** to save changes to EAP providers. Click **OK** to save changes to the profile settings.
12. Click **OK** to save changes to the remote access policy.

This will allow the **8021x access to intranet** remote access policy to authorize 802.1x connections using the EAP-TLS authentication method.

CLIENT 1

To modify CLIENT1 so that it uses EAP-TLS authentication, perform the following steps:

▶ Configure CLIENT1 to use EAP-TLS

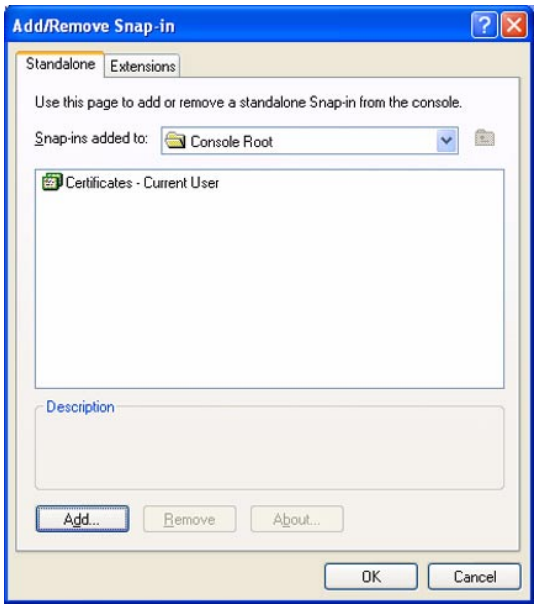
1. Update computer and user configuration Group Policy settings and obtain a computer and user certificate for the 802.1x client computer immediately, by logging off and then logging on. Otherwise type **gpupdate** at a command prompt.

Note: *After restart, you must log in as 8021x User, NOT administrator.*

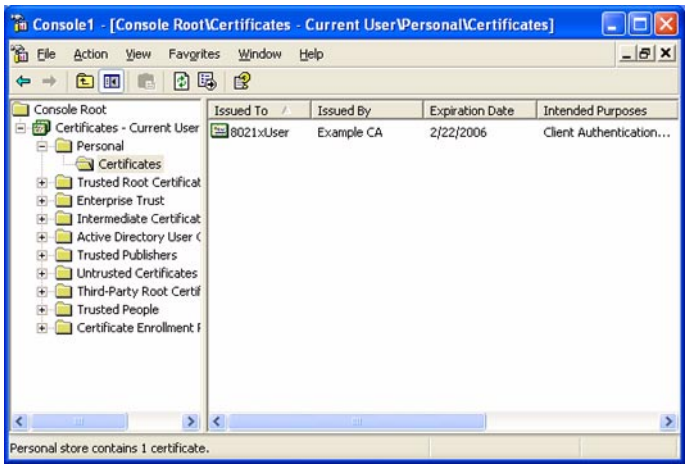
You must be logged on to the domain, either via your previously created Local Area Connection PEAP connection or by connecting using a non-authenticating port on the Allied Telesis switch.

2. To check the CLIENT1 certificate, you can run mmc then add the snap-in for **certificates - current user**.

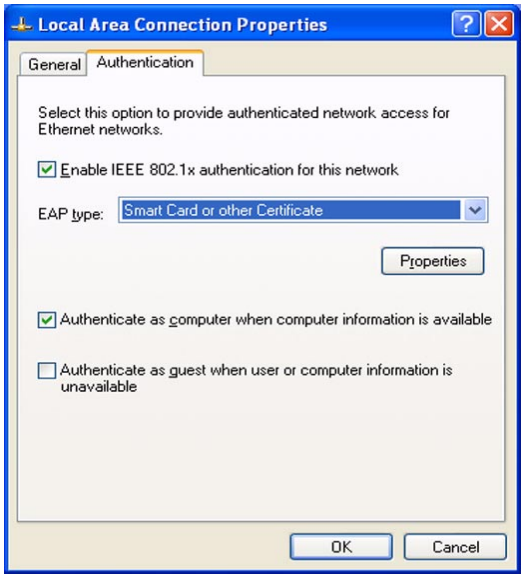
   This is shown in the following figure.



3. Then you can check the certificate under **Personal** >**Certificates**.



4. To obtain properties for the Local Area Connection, click **Start**, click **Control Panel**, double-click **Network Connections**, and then right-click **Local Area Connection**. Click **Properties**.
5. On the **Authentication** tab, select **Smart Card or other Certificate** for the **EAP type**. This is shown in the following figure.



6. Click **OK** to exit.
7. The **Local Area Connection** reconnects using EAP-TLS authentication. Remember to return CLIENT1 connection to an 802.1x authenticating port on the Allied Telesis switch. In our example, this is port 1.

Note: *If you want to monitor the authentication process, open the Network Connection window, before you shift CLIENT1 to the authenticated port.*

8. Test connectivity again by pinging devices on the intranet and testing other access such as intranet web server or file servers.

Confirmation of authenticated connection

As mentioned in the previous section, you can verify the progress of 802.1x authentication by monitoring the Local Area Connection icon on the Network Connections window. It should pass through an authenticating stage to a connected stage. You can then verify basic connectivity from the command window by pinging other devices in the intranet, such as 192.168.1.254 (RADIUS) and 192.168.1.200 (DC1-CA).

- You can also check authentication on the Allied Telesis switch using the command:

  ```
  sh portauth port=1
  ```

- If needed, debugging can also be enabled with the command:

  ```
  ena portauth debug=all port=1
  ```

  To see all the relevant debug you may need to logout and login again as 8021xUser, on the example.com domain.

- Another possible reason for authentication failure regards the interaction between the Allied Telesis switch and the RADIUS server. Check that you have configured the correct secret for the RADIUS server.

- You can also check RADIUS debugging. On the Allied Telesis switch, use the command:

  ```
  ena radius debug=decode
  ```

  On the RADIUS server you can use the event viewer, available from administrative tools.

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16057-00 REV C