

AlliedWare Plus™ OS

How To | Use the local RADIUS server to authenticate 802.1x supplicants using X.509 certificates

Introduction

The local RADIUS server within AlliedWare Plus can authenticate 802.1x supplicants either via username and password, or by using X.509 certificates.

This How To Note describes how to configure the local RADIUS server to authenticate an 802.1x supplicant using X.509 certificates. It also explains how to generate the required certificates, how to configure ports as authenticator ports, and how to install certificates on the supplicant workstation.

What information will you find in this document?

This How To Note explains the following processes:

- "Configuring the local RADIUS server" on page 2
- "Creating X.509 certificates" on page 3
- "Configuring a set of ports as 802.1x authenticator ports" on page 4
- "Creating the VLAN to which the user Engineer01 will be dynamically allocated" on page 4
- "Installing X.509 certificates on a supplicant workstation" on page 5

Which products and software versions does it apply to?

This How To Note applies to AlliedWare Plus software version 5.2.1 and above, for the following Allied Telesis switches:

- SwitchBlade x908
- x900-12XT/S
- x900-24 Series
- x600 Series

Configuring the local RADIUS server

There are three steps to configuring the local RADIUS server so that an AlliedWare Plus switch can authenticate 802.1x supplicants.

Initial configuration

1. Enable the server.

```
awplus(config)#radius-server local
awplus(config-radsrv)#server enable
```

2. Add the switch to the client (NAS) list for the RADIUS server.

```
awplus(config-radsrv)#nas 127.0.0.1 key awplus-local-radius-server
awplus(config-radsrv)#exit
```

3. Add the switch as a RADIUS server to be used for 802.1x authentication.

```
awplus(config)#radius-server host 127.0.0.1 key awplus-local-radius-server
awplus(config)#aaa authentication dot1x default group radius
```

When you enable the RADIUS server, this also sets up the switch as a certificate authority, and creates a root Certificate Authority X.509 certificate on the switch. This certificate can be viewed using the command: **show crypto pki certificates local-ca**

```
awplus#show crypto pki certificates local-ca
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
    Validity
      Not Before: Apr 17 05:42:09 2009 GMT
      Not After : Apr 12 05:42:09 2029 GMT
    Subject: O=Allied-Telesis, CN=AlliedwarePlusCA
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
```

Create a RADIUS group and a RADIUS user

Next, you must create a RADIUS group specifically for the purpose of associating a VLAN with the user. When the user is authenticated on a port, this is the VLAN to which the port will be dynamically allocated:

```
awplus(config)#radius-server local
awplus(config-radsrv)#group Engineers
awplus(config-radsrv-group)#vlan 40
awplus(config-radsrv-group)#exit
awplus(config-radsrv)#user Engineer01 password secret group Engineers
awplus(config-radsrv)#exit
```

Creating X.509 certificates

In order for the user to be authenticated by an X.509 certificate, certificates have to be created, and then transferred to the supplicant workstation.

1. Create a certificate for the user.

Enroll the user into the local certificate authority:

```
awplus(config)#crypto pki enroll local user Engineer01
Enrolling Engineer01 to local trustpoint...OK
awplus(config)#
```

2. Write the certificates to files, and upload them to a TFTP server.

Export the Certificate Authority certificate

Write the Certificate Authority certificate to a PEM file:

```
awplus(config)#crypto pki export local pem url tftp://10.32.4.73/lrad.pem
Copying..
Successful operation
```

Export the user certificate

Write the user certificate to a PK CS12 file:

```
awplus(config)#crypto pki export local pkcs12 Engineer01
tftp://10.32.4.73/Engineer01.pfx
Copying..
Successful operation
```

Configuring a set of ports as 802.1x authenticator ports

Configure the ports to perform 802.1x authentication, and to be dynamically allocated to a VLAN upon successful authentication.

```
awplus(config)#int port1.0.1-1.0.24
awplus(config-if)#dot1x port-control auto
awplus(config-if)#auth dynamic-vlan-creation
awplus(config-if)#spanning-tree portfast
awplus(config-if)#exit
```

Note: It is advisable to configure 802.1x authenticating ports as spanning-tree port-fast ports if they are to be directly connected to workstations.

Creating the VLAN to which the user Engineer01 will be dynamically allocated

```
awplus(config)#vlan database
awplus(config-vlan)#vlan 40
```

The switch is now configured to act as a RADIUS server and 802.1x authenticator.

Now, let's look at the process of installing the X.509 certificates onto the PC, and configuring the PC's NIC card to operate as an 802.1x supplicant, using Engineer01's X.509 certificate.

Installing X.509 certificates on a supplicant workstation

You must install both the switch's Certificate Authority certificate and the user's certificate into the PC.

The switch's Certificate Authority certificate must be installed into the PC so that the PC will recognise the switch as a trusted Certificate Authority. Once the PC recognises the switch as a trusted Certificate Authority, it will:

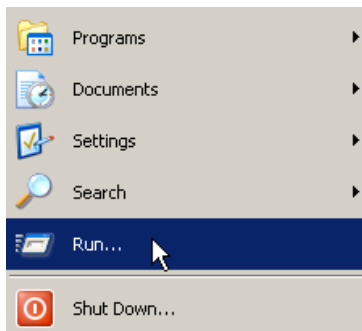
- Recognise the user's certificate as having been signed by a trusted certificate authority (as the user's certificate has been signed by the switch).
- Successfully validate the switch's certificate during the 802.1x authentication.

The PC is configured to request the switch's certificate during authentication, so that it can validate that it is connecting to a trusted authenticator. If the switch's certificate is already installed into the PC as a trusted certificate authority's certificate, then when it receives that certificate again during the 802.1x authentication, it will recognise that certificate as belonging to a trusted authenticator.

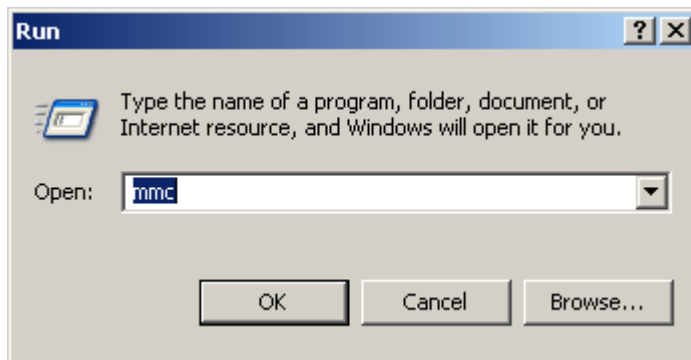
The user's certificate must be installed into the PC so that it can be sent to the switch during the 802.1x authentication.

Preparing to install certificates

1. Select **Run...** from your system **Start** menu.

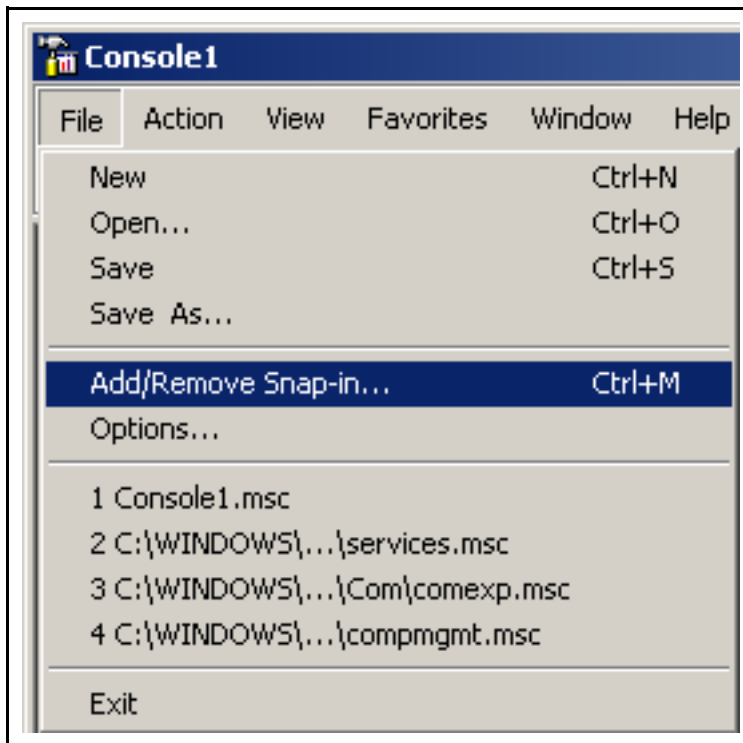


2. Type in **mmc**, and click **OK**.



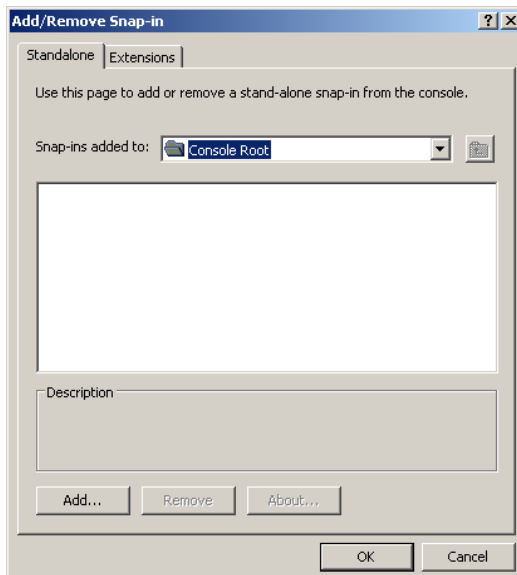
The system **Console** opens.

3. Select **File > Add/Remove Snap-in...**



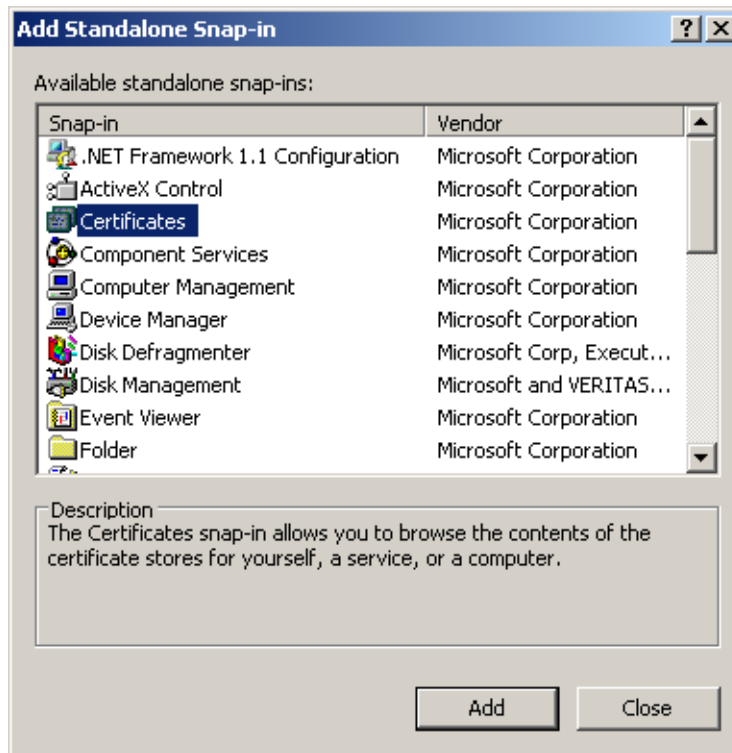
The **Add/Remove Snap-in** window opens.

4. Click **Add...**



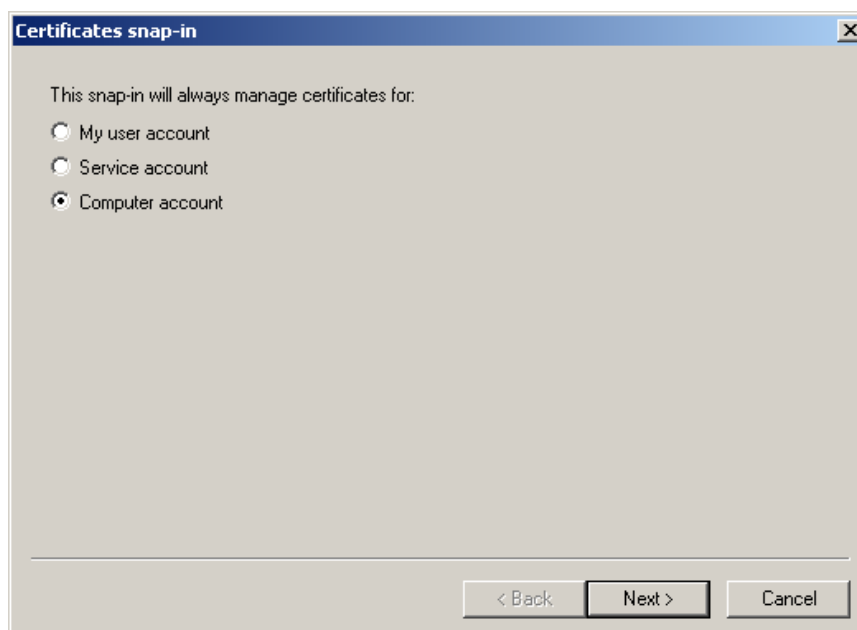
The **Add Standalone Snap-in** window opens.

5. Select **Certificates**, and then click **Add**.



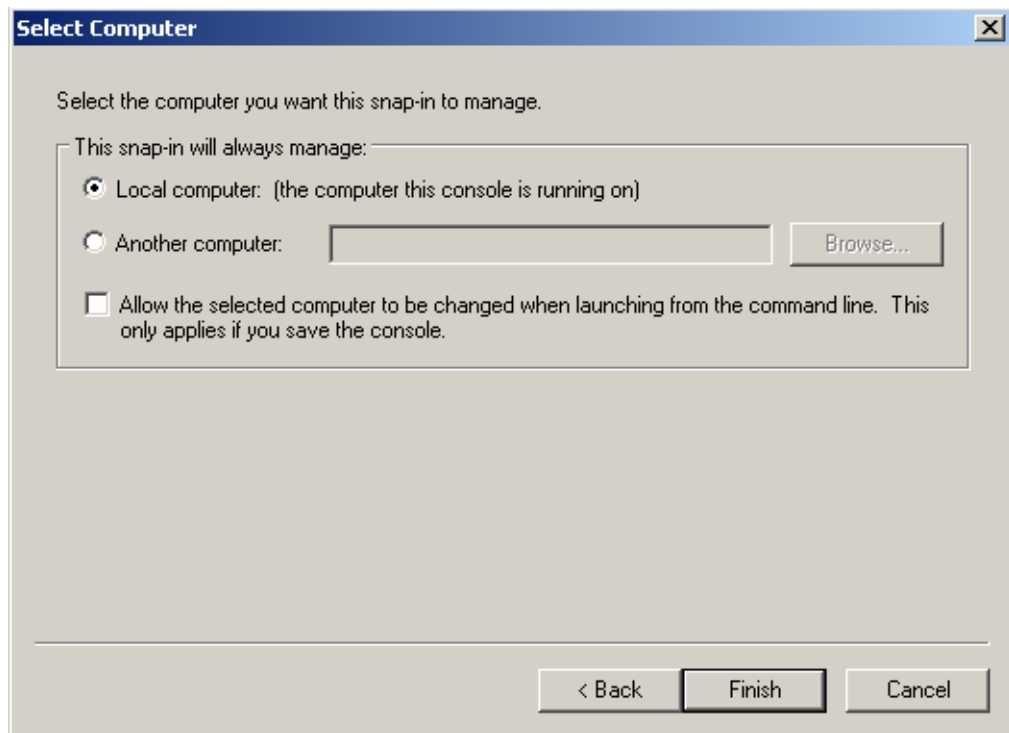
The **Certificates snap-in** window opens.

- Choose **Computer account**.



The **Select Computer** window opens.

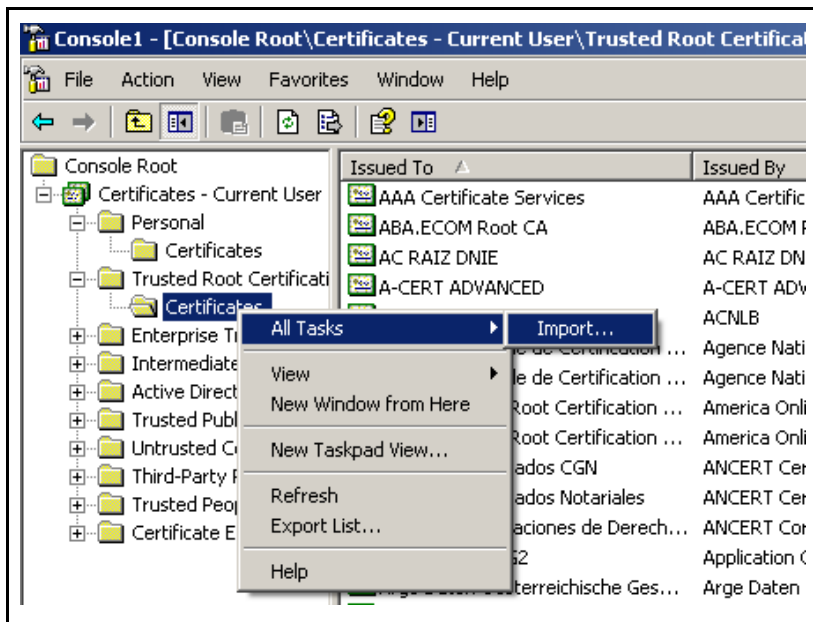
6. Choose **Local Computer** and click **Finish**.



The snap-in is now installed into the System Console. You can now start installing the certificates that you exported from the switch.

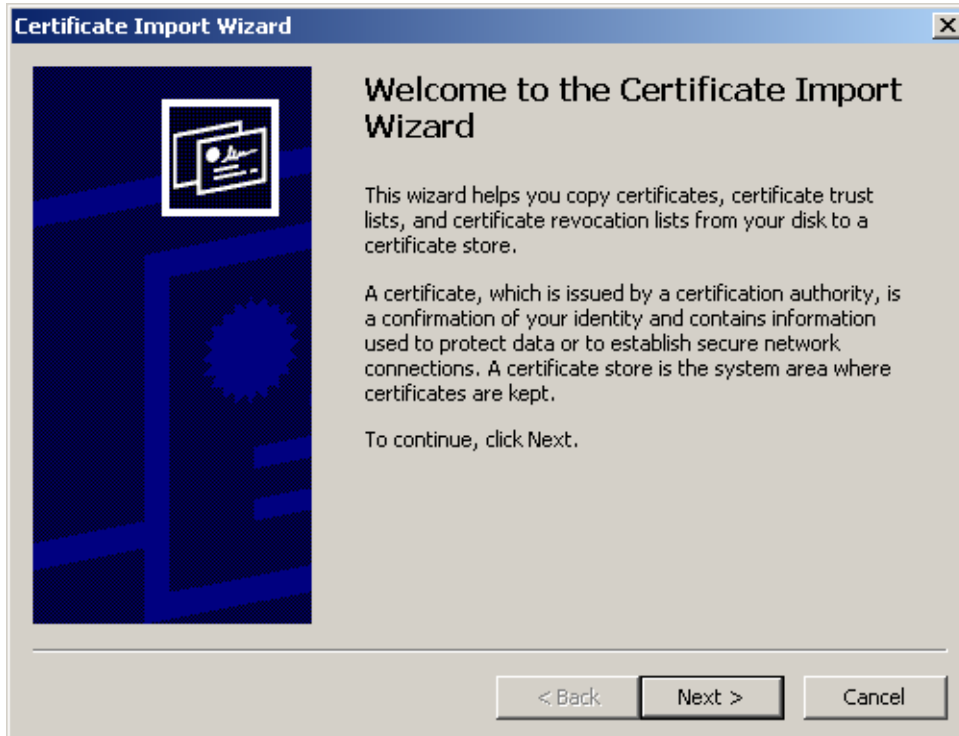
Install the switch's Certificate Authority certificate

1. Within the console, right-click on **Certificates** under **Trusted Root Certificates**. Then select **All Tasks > Import...**



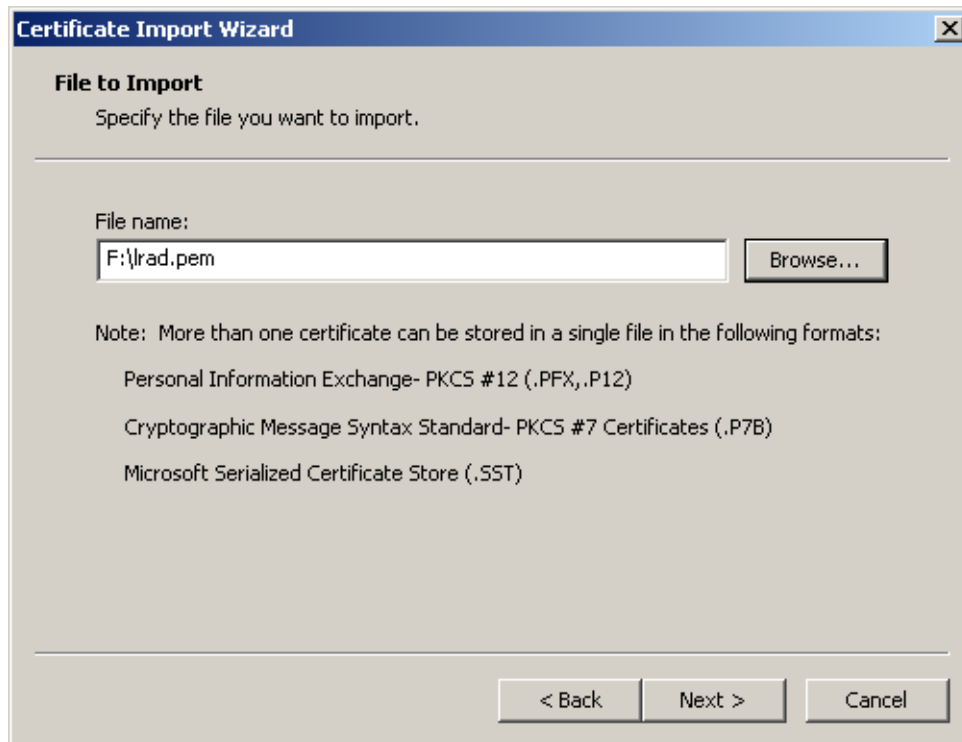
The **Certificate Import Wizard** opens.

2. Click **Next**.

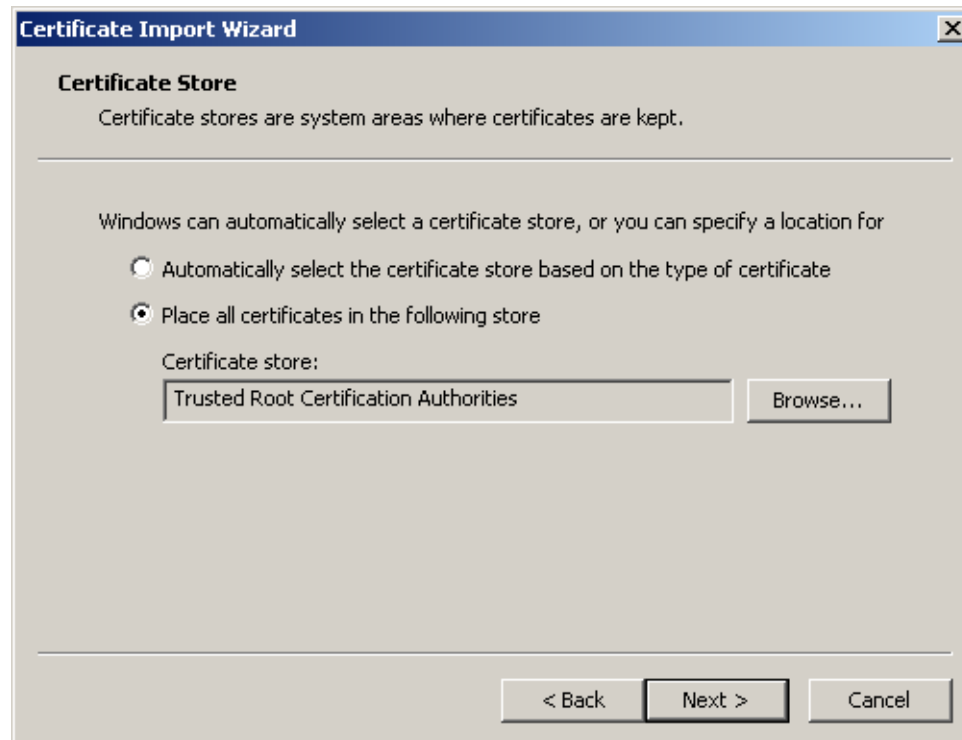


The **File to Import** window opens.

3. In the **File to Import** window, specify the file to which you exported the Switch's Certificate Authority certificate.



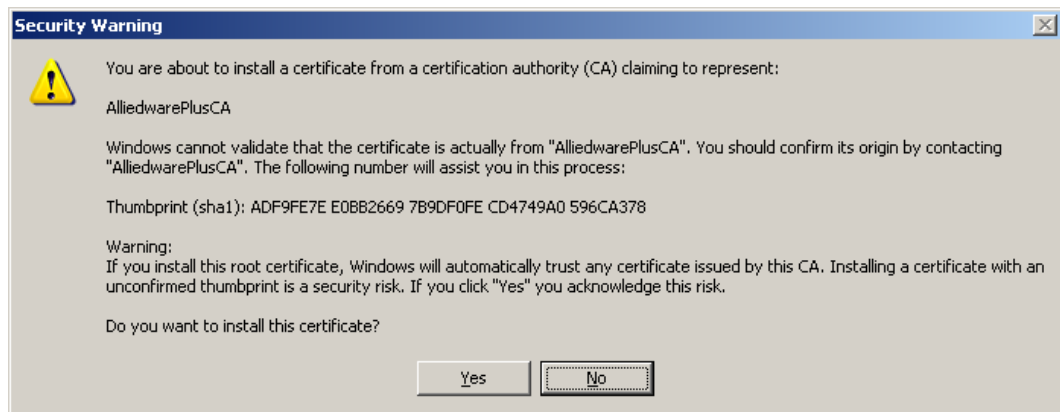
4. In the **Certificate Store** window, leave the default setting and click **Next**.



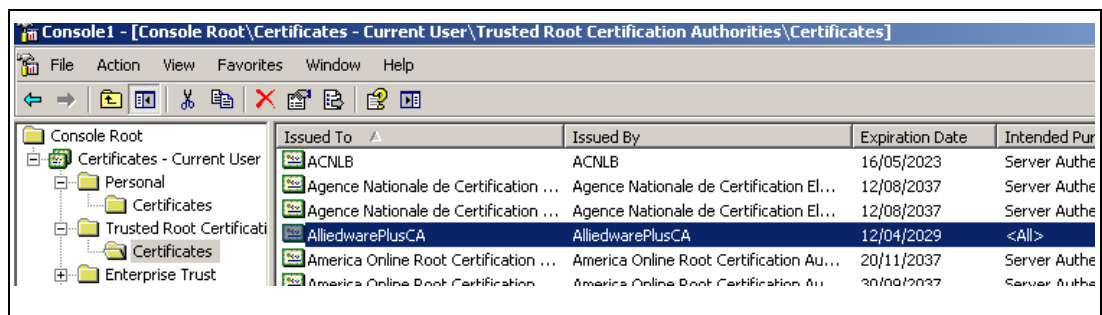
- The Certificate Import Wizard is now complete. Click **Finish**.



- A **Security Warning** may display. Since you just created this Certificate Authority on the switch, you know that you can trust it, so click **Yes** and proceed.

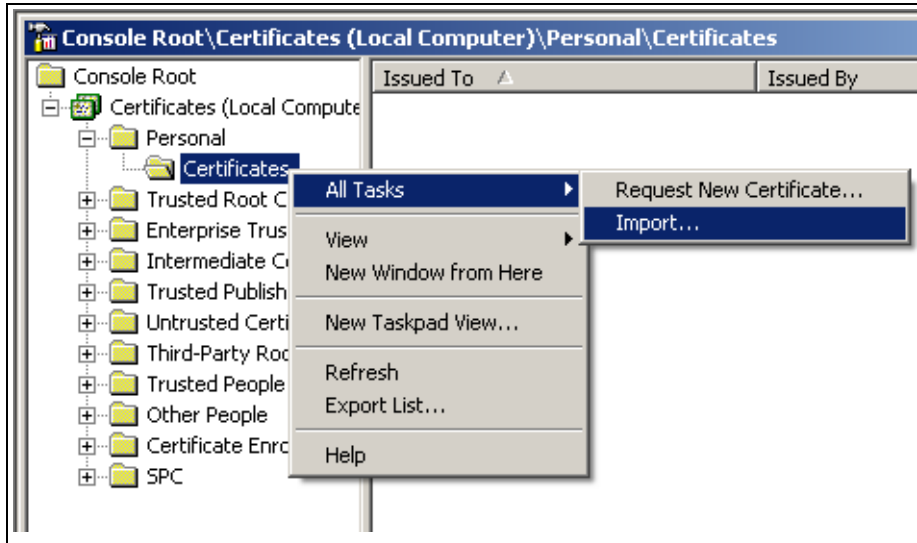


- The certificate is now installed into the list of Trusted Root Certificates, as shown below:



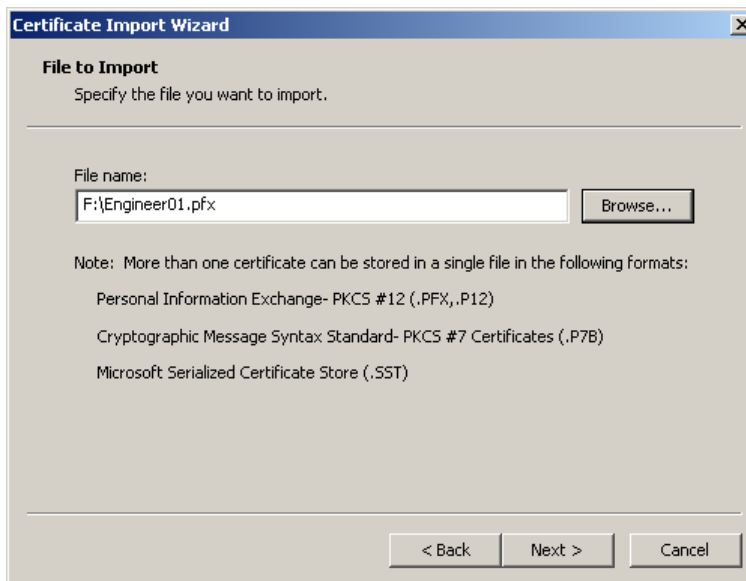
Install the user's certificate

1. Right-click on **Certificates** under **Personal**. Then select **All Tasks > Import...**

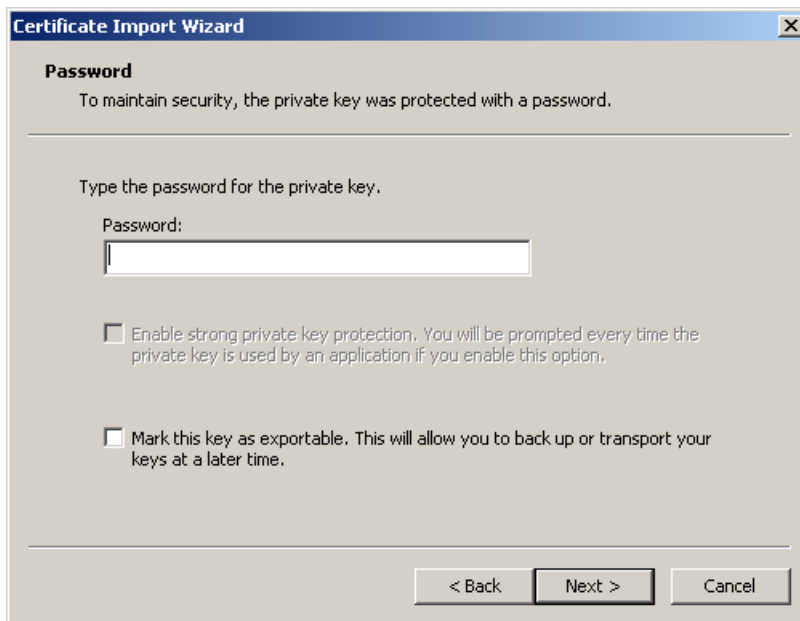


The **Import Certificate Wizard** opens for the second time.

2. Work through this wizard again. This time, specify the file to which you exported the user's certificate.

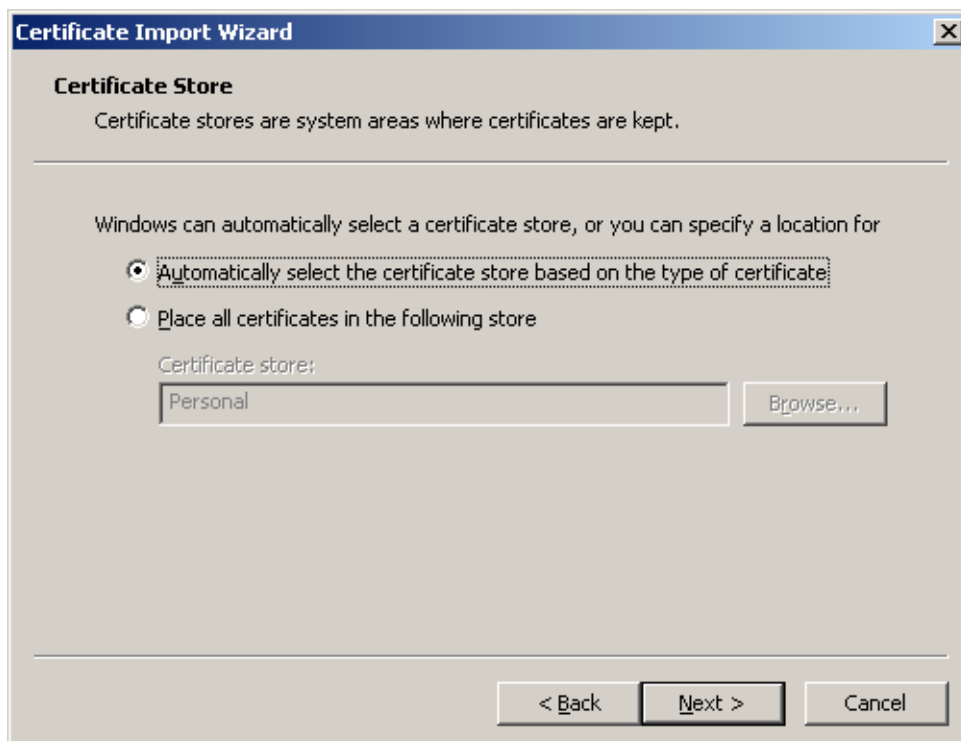


- The wizard will now prompt you to enter the password that protects the certificate file. The certificate file was not protected with a password, so leave the **Password** field blank, and click **Next**.



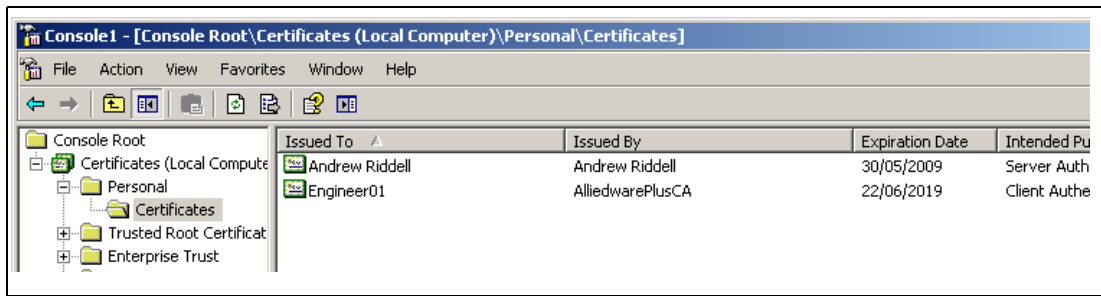
The screenshot shows the 'Certificate Import Wizard' dialog box. The title bar reads 'Certificate Import Wizard'. The main heading is 'Password'. Below the heading, it says 'To maintain security, the private key was protected with a password.' There is a horizontal line. Below that, it says 'Type the password for the private key.' There is a label 'Password:' followed by an empty text input field. Below the input field, there are two checkboxes. The first checkbox is unchecked and has the text 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' The second checkbox is also unchecked and has the text 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Choose **Automatically select the certificate store based on the type of certificate** and click **Next**.



The screenshot shows the 'Certificate Import Wizard' dialog box. The title bar reads 'Certificate Import Wizard'. The main heading is 'Certificate Store'. Below the heading, it says 'Certificate stores are system areas where certificates are kept.' There is a horizontal line. Below that, it says 'Windows can automatically select a certificate store, or you can specify a location for'. There are two radio buttons. The first radio button is selected and has the text 'Automatically select the certificate store based on the type of certificate'. The second radio button is unselected and has the text 'Place all certificates in the following store'. Below the second radio button, there is a label 'Certificate store:' followed by a text input field containing the word 'Personal' and a 'Browse...' button. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

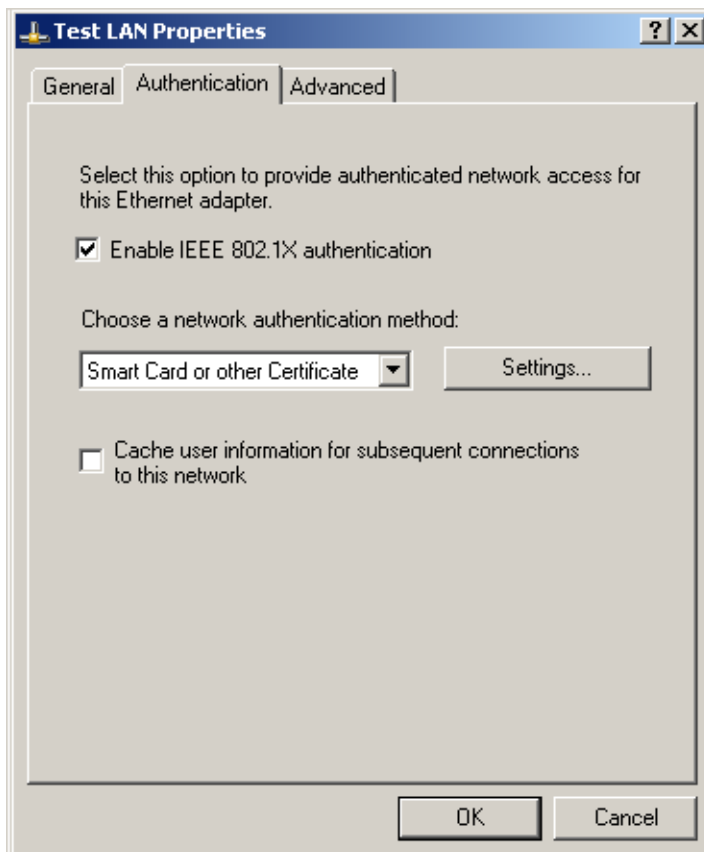
5. The certificate now appears in the **Certificates** store.



The certificates have now been successfully installed on to the PC.

Set up the PC's NIC card as an 802.1x supplicant

1. Open the NIC's properties window, and go to the **Authentication** tab. In that tab:
 - Select **Enable IEEE 802.1x authentication**.
 - Choose **Smart Card or other Certificate** from the drop down box.
NOTE: Do NOT choose **Protected EAP (PEAP)**.

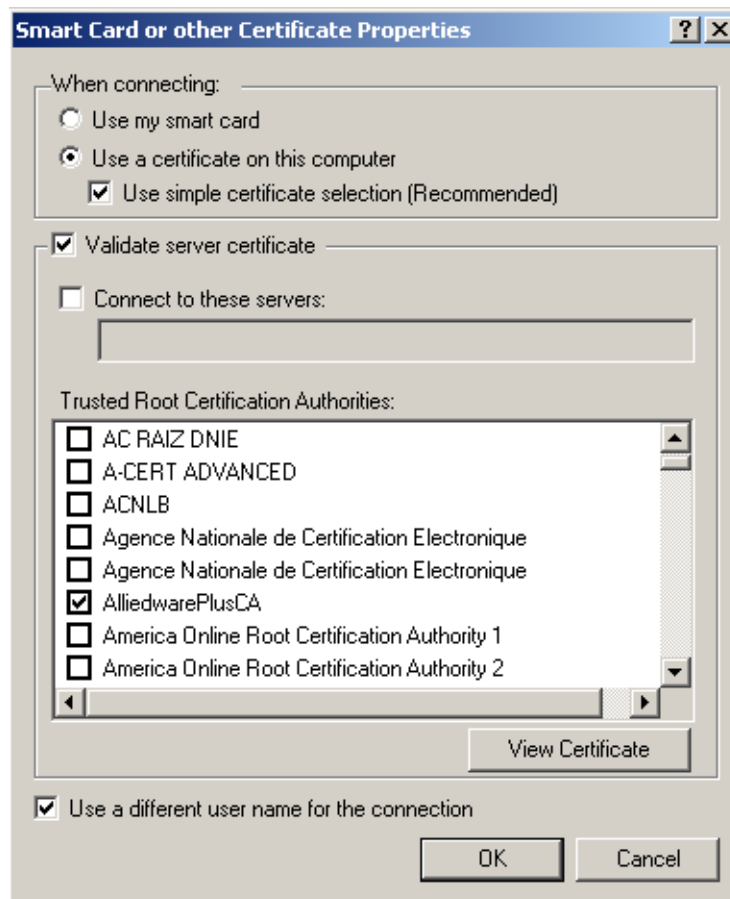


2. Click **Settings...**

The **Smart Card or other Certificate Properties** window opens.

Choose **Use a certificate on this computer**, and select:

- **Use simple certificate selection**
- **Validate server certificate**
- **AlliedwarePlusCA** from the list of **Trusted Root Certificate Authorities**
- **Use a different user name for the connection**



Attach the PC NIC to the switch

Attach the PC NIC to an authenticating port on the switch. The switch and the PC will exchange certificates, and authentication will succeed. To verify that the PC has been successfully authenticated, use the command:

```
show dot1x supplicant
```

This will produce output like:

```
Interface port1.0.1
 authenticationMethod: dot1x
 totalSupplicantNum: 1
 authorizedSupplicantNum: 1
   macBasedAuthenticationSupplicantNum: 0
   dot1xAuthenticationSupplicantNum: 1
   webBasedAuthenticationSupplicantNum: 0
   otherAuthenticationSupplicantNum: 0

Supplicant name: Engineer01
Supplicant address: 0002.b363.319f
 authenticationMethod: 802.1X
 portStatus: Authorized - currentId: 7
 abort:F fail:F start:F timeout:F success:T
 PAE: state: Authenticated - portMode: Auto
 PAE: reAuthCount: 0 - rxRespId: 0
 PAE: quietPeriod: 60 - maxReauthReq: 2
 BE: state: Idle - reqCount: 0 - idFromServer: 6
 CD: adminControlledDirections: both - operControlledDirections: both
 CD: bridgeDetected: false
 KR: rxKey: false
 KT: keyAvailable: false - keyTxEnabled: false
 dynamicVlanId: 40
```

You can see that this output displays the:

- User name under which the PC was authenticated
- MAC address of the PC
- ID of the VLAN that the port was dynamically allocated to.