How To Note

Allied Telesis™

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:

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	x600 Series
x900-12XT/S	x610 Series
x900-24 Series	SwitchBlade x8112

AlliedWare Plus™ OPERATING SYSTEM

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.

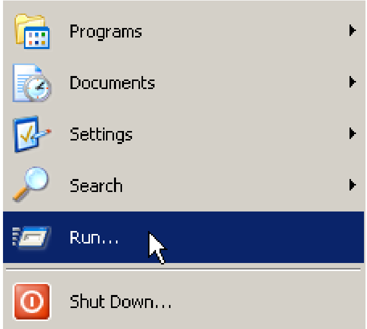
The switch's Certificate Authority certificate must be installed into the PC so that the PC will recognise the switch as a trusted Certificate Authority. Once the PC recognises the switch as a trusted Certificate Authority, it will:

- 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.

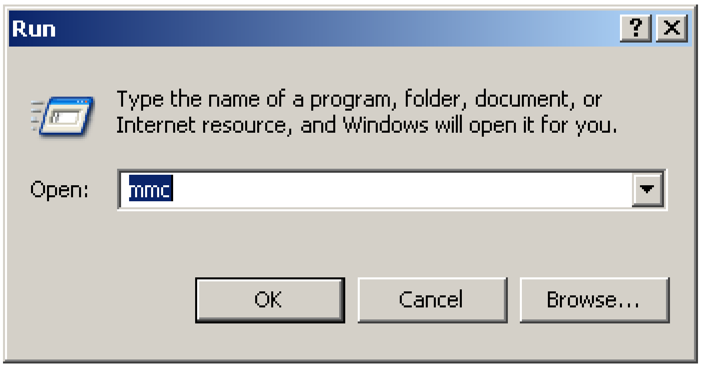
The user's certificate must be installed into the PC so that it can be sent to the switch during the 802.1x authentication.

Preparing to install certificates

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



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

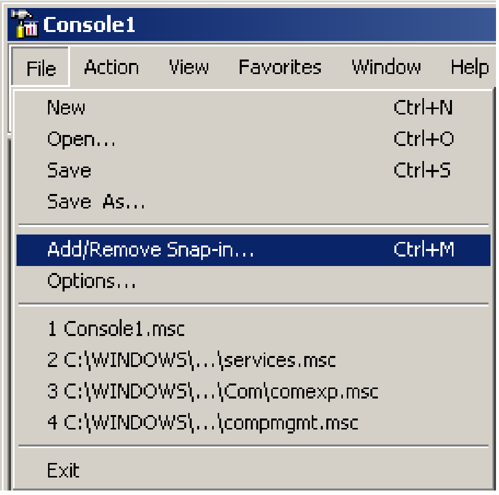


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

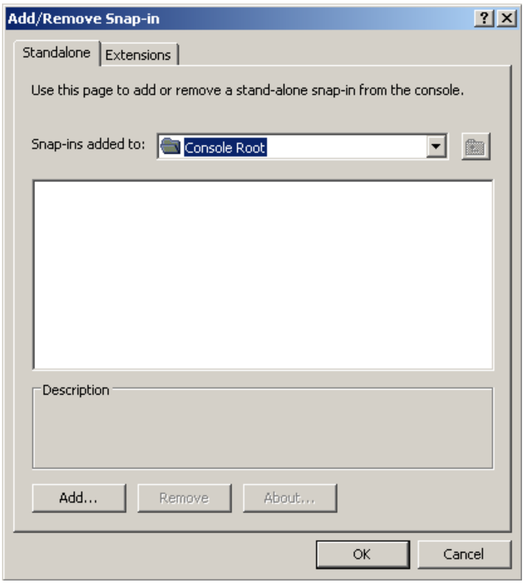
The system Console opens.

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


Console1
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 Console1.msc
2 C:\WINDOWS\...\services.msc
3 C:\WINDOWS\...\Com\comexp.msc
4 C:\WINDOWS\...\compmgmt.msc
Exit

The Add/Remove Snap-in window opens.

4. Click **Add..**.



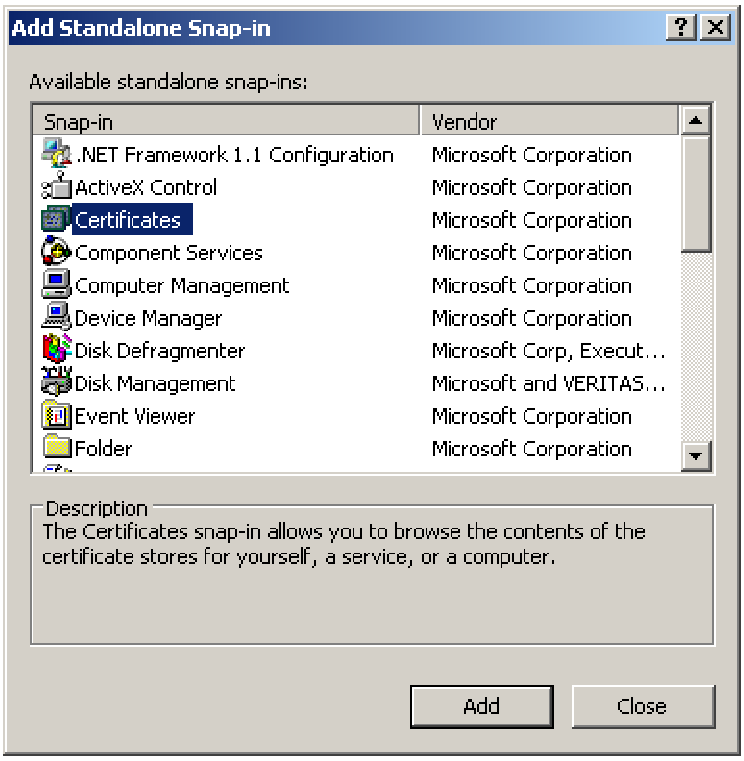
Use this page to add or remove a stand-alone snap-in from the console.

Snap-ins added to: Console Root

Description

The Add Standalone Snap-in window opens.

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



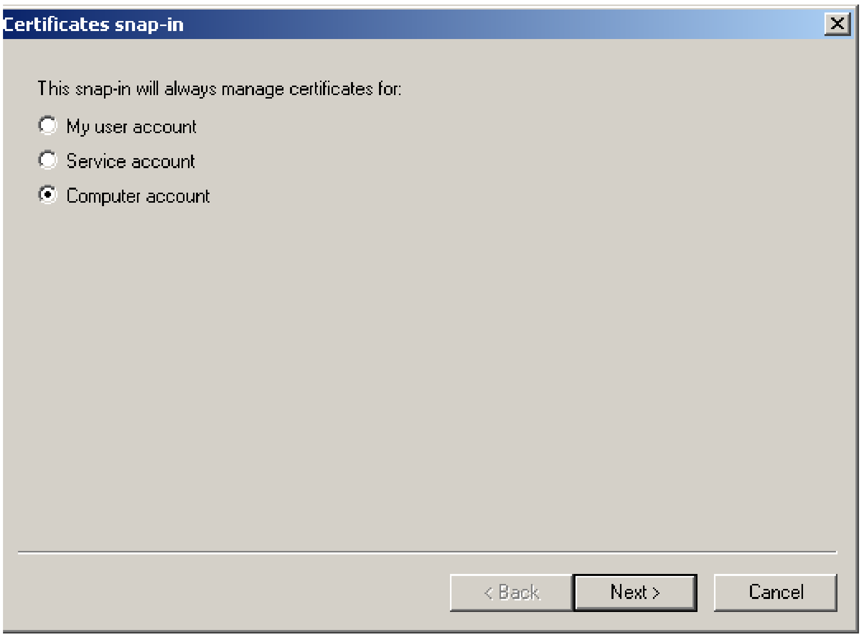
Available standalone snap-ins:

Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Microsoft Corp, Execut...
Disk Management	Microsoft and VERITAS...
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation

Description
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

The Certificates snap-in window opens.

- Choose **Computer account**.



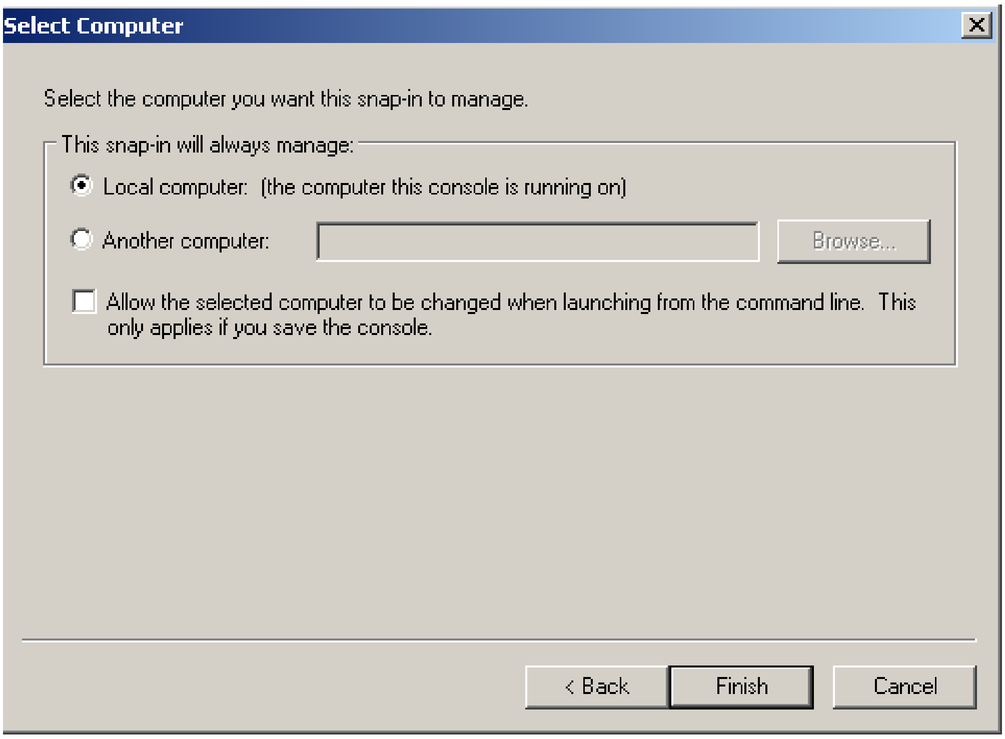
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

The Select Computer window opens.

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



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

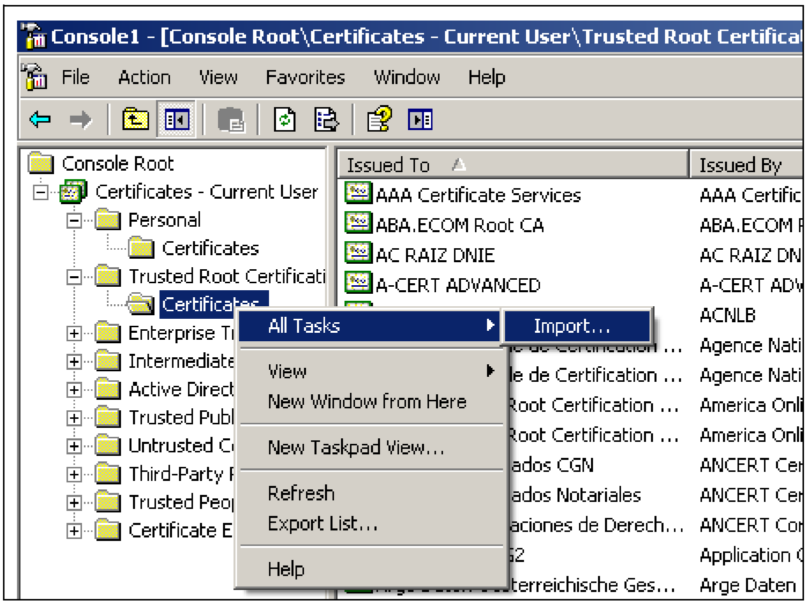
● Local computer: (the computer this console is running on)
○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

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

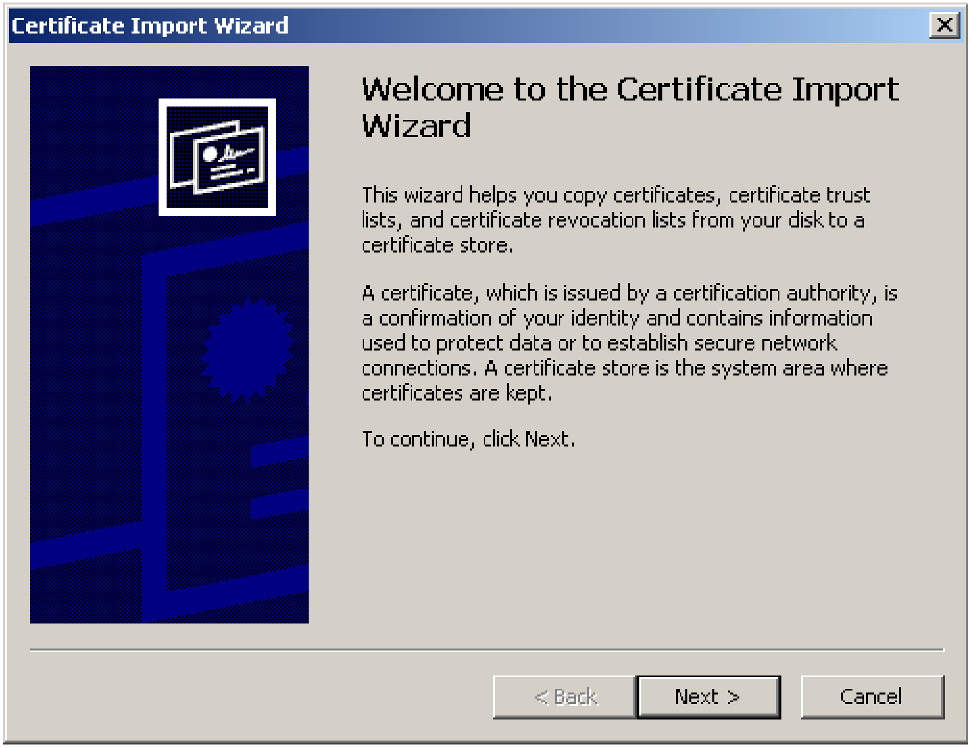
Install the switch's Certificate Authority certificate

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**.



Welcome to the Certificate Import Wizard

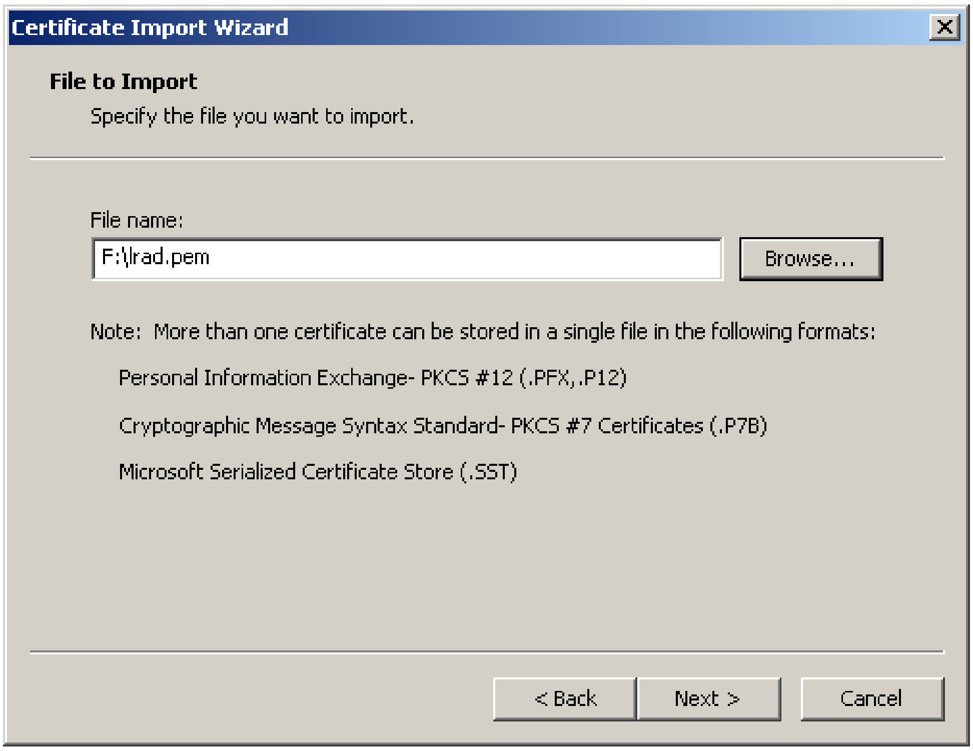
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, 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.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

F:\lrad.pem

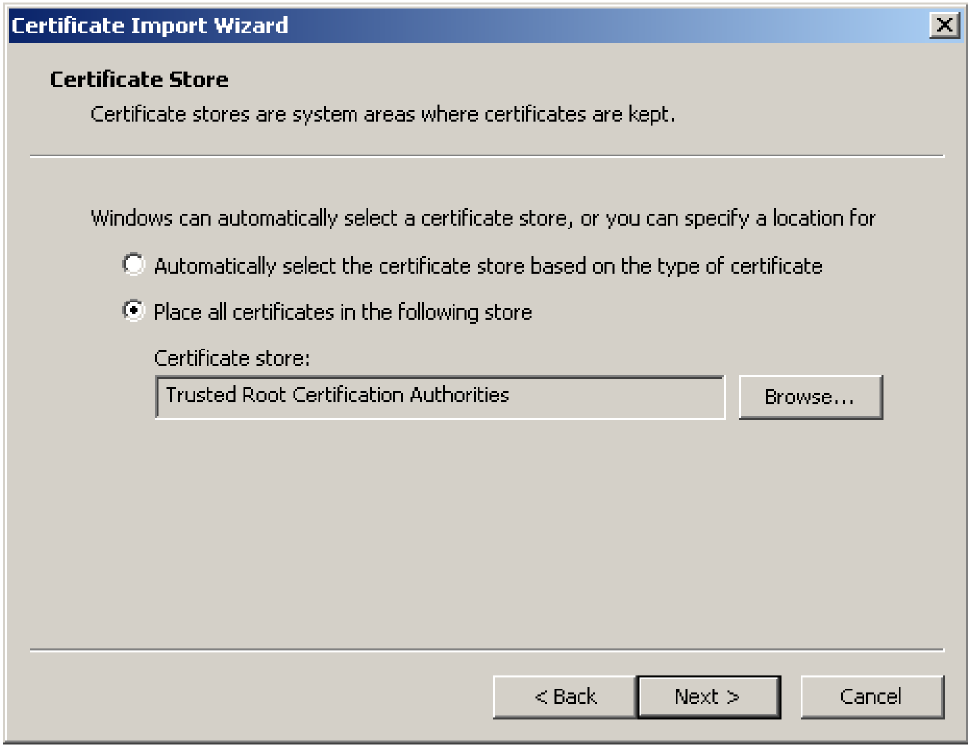
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

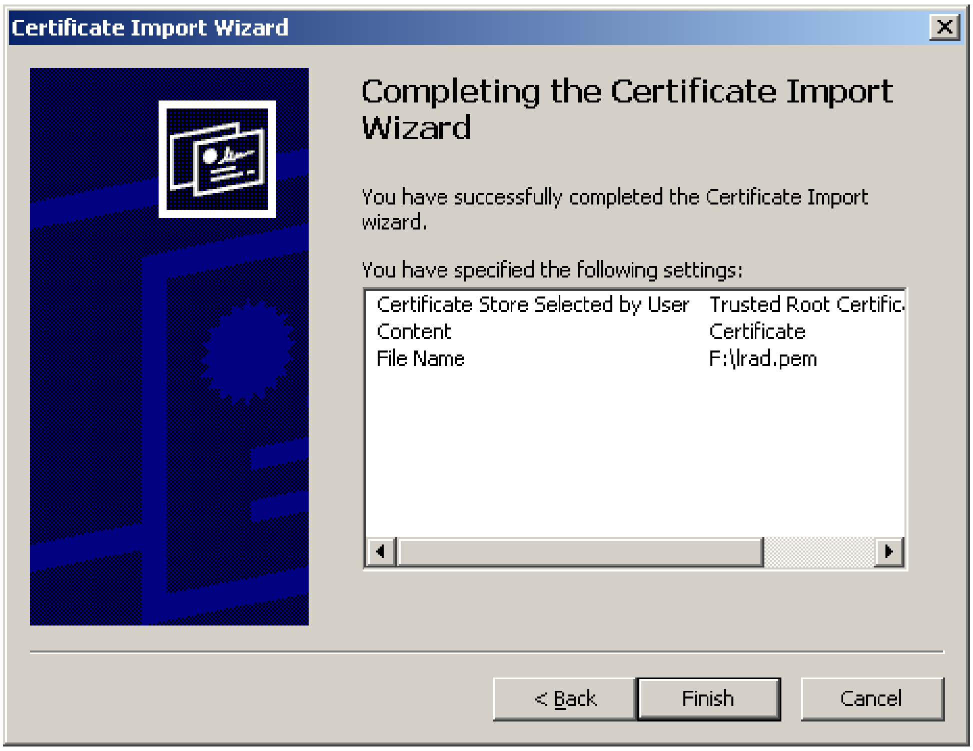
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

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



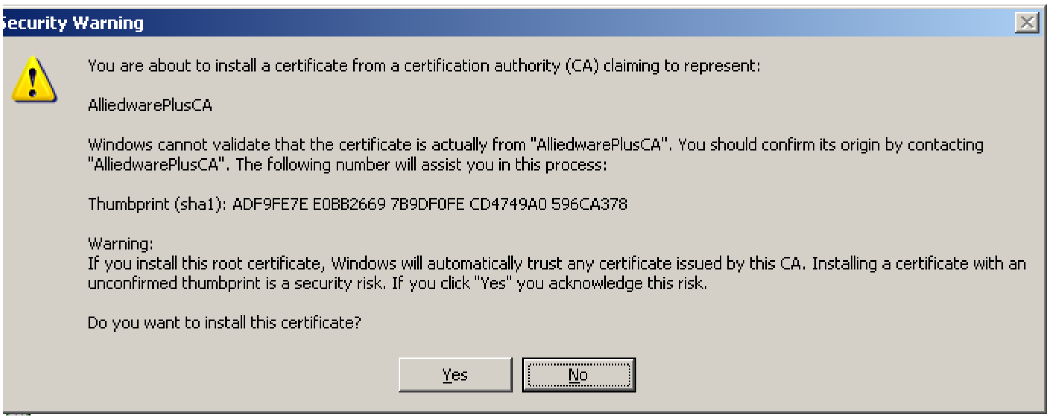
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	Certificate
File Name	F:\lrad.pem

6. 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.



You are about to install a certificate from a certification authority (CA) claiming to represent:

AlliedwarePlusCA

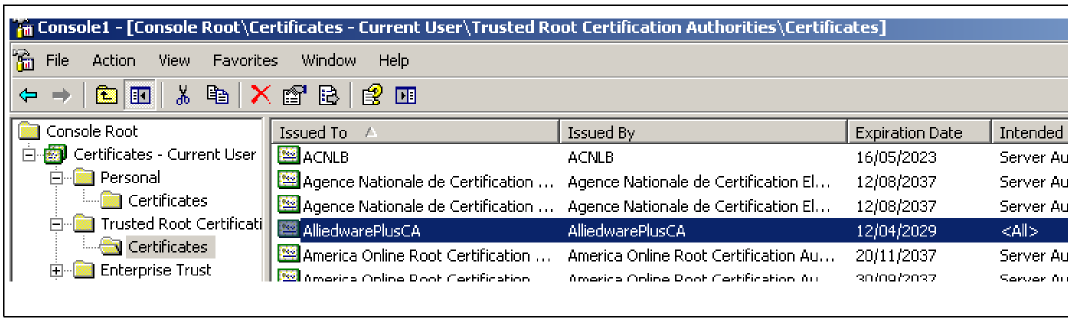
Windows cannot validate that the certificate is actually from "AlliedwarePlusCA". You should confirm its origin by contacting "AlliedwarePlusCA". The following number will assist you in this process:

Thumbprint (sha1): ADF9FE7E E0BB2669 7B9DF0FE CD4749A0 596CA378

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

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


Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certificati
Certificates
Enterprise Trust

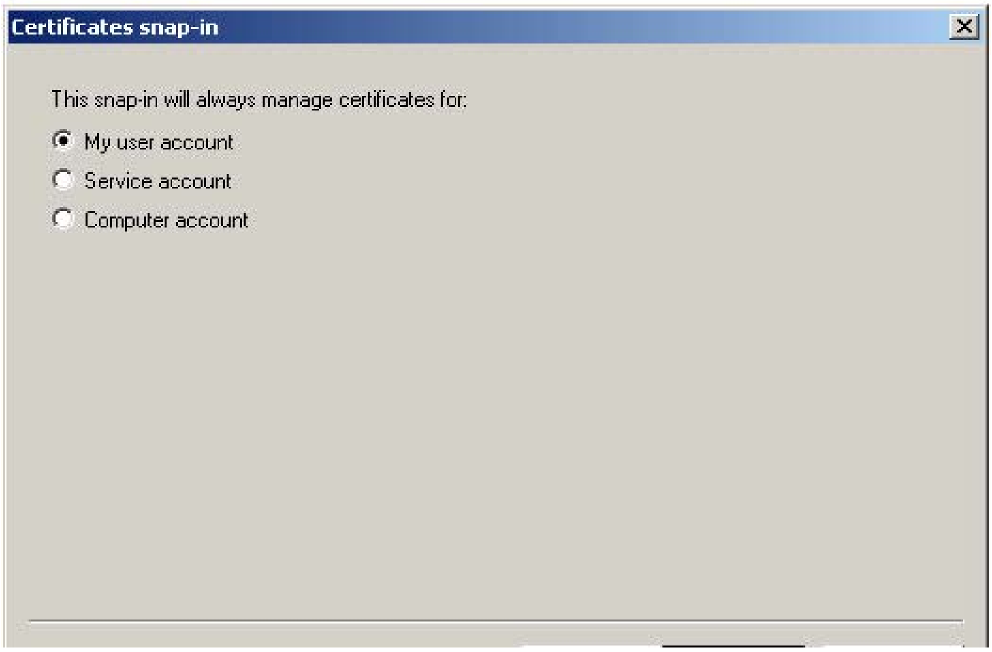
Issued To	Issued By	Expiration Date	Intended
ACNLB	ACNLB	16/05/2023	Server Au
Agence Nationale de Certification ...	Agence Nationale de Certification El...	12/08/2037	Server Au
Agence Nationale de Certification ...	Agence Nationale de Certification El...	12/08/2037	Server Au
AlliedwarePlusCA	AlliedwarePlusCA	12/04/2029	<All>
America Online Root Certification ...	America Online Root Certification Au...	20/11/2037	Server Au
America Online Root Certification	America Online Root Certification Au	30/09/2037	Server Au

Install the user's certificate

Under Windows **XP,** you can now go straight on and add the User's Certificate, using the Current MMC snap-in.

But, under Windows **Vista** and Windows **7**, at this point you must:

- Close the MMC Console
- Once again go through steps 1-6 on pages 5-8
- When re-doing step 5, choose **My user account** as shown below, rather than **Computer account**.



Certificates snap-in

This snap-in will always manage certificates for:

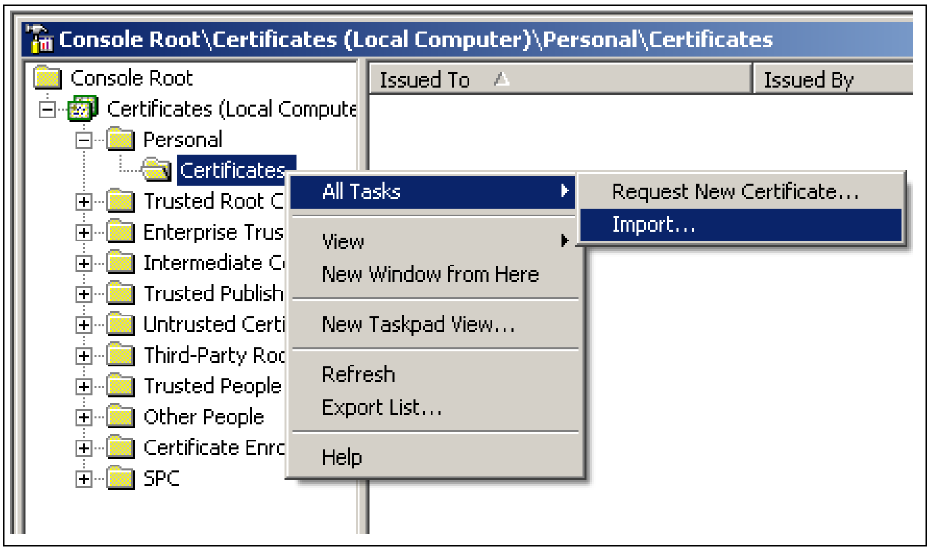
● My user account

○ Service account

○ Computer account

Then, having completed the setup of the Snap-in, you can proceed to install the certificate, starting from step 1 below.

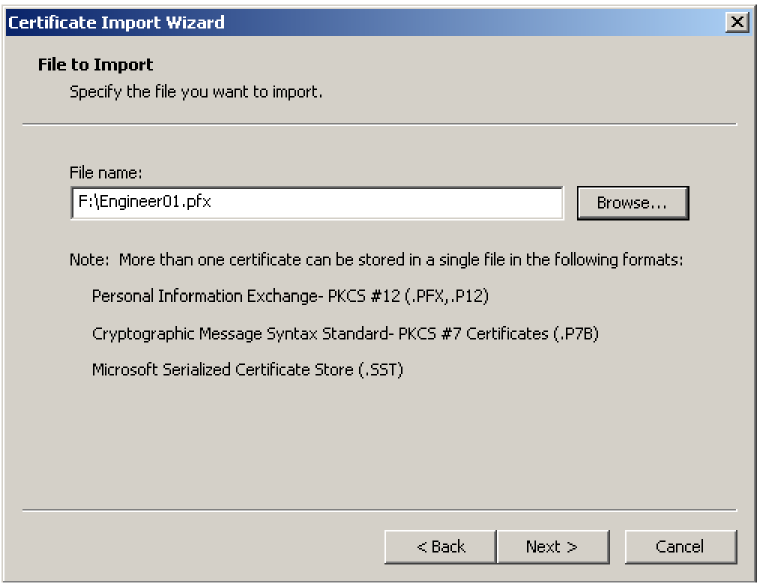
1. Right-click on **Certificates** under **Personal**. Then select **All Tasks** > **Import...**



Console Root\Certificates (Local Computer)\Personal\Certificates

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.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name: F:\Engineer01.pfx

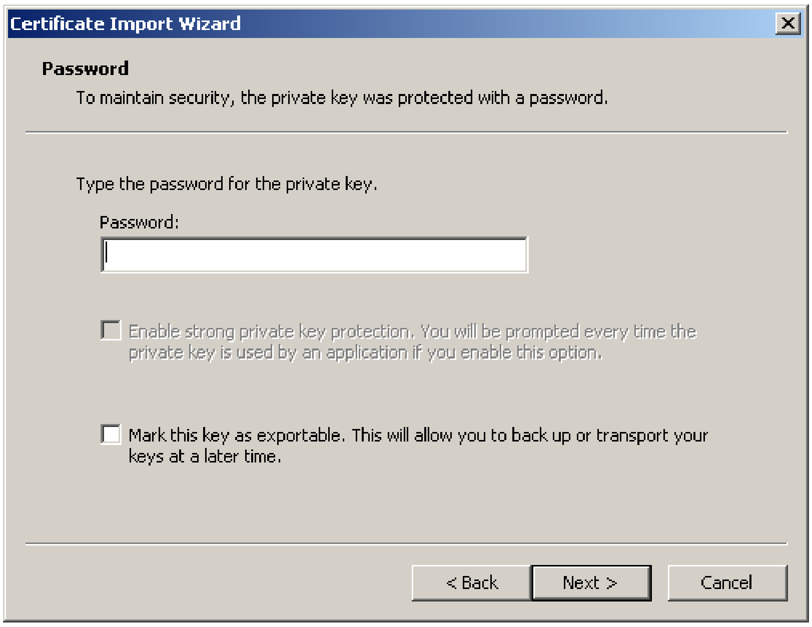
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

3. 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**.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

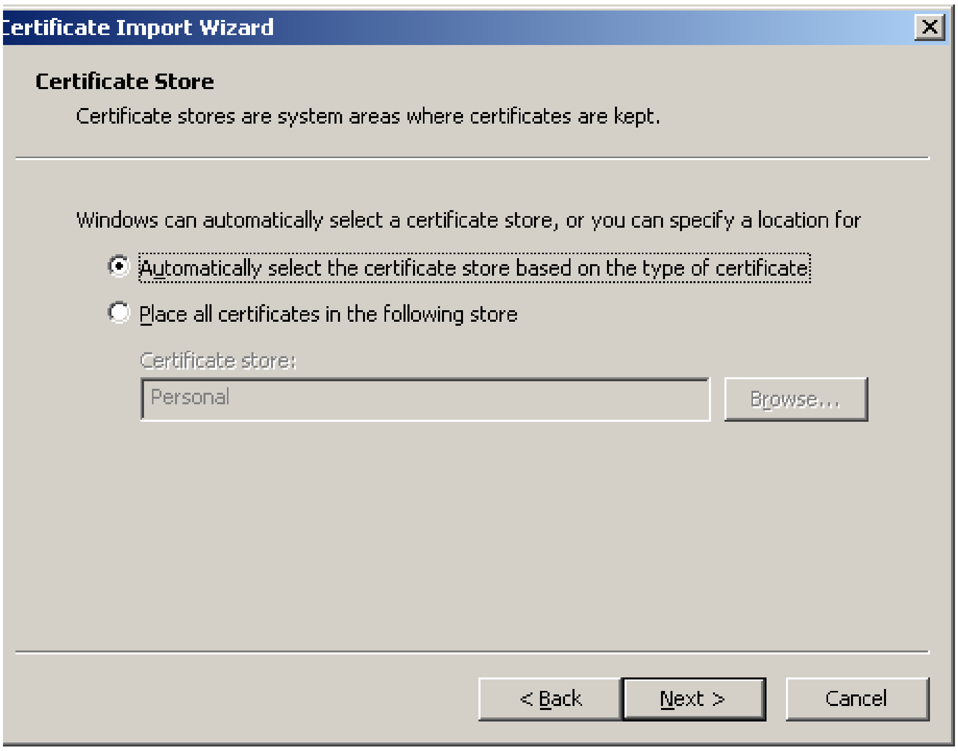
Type the password for the private key.

Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

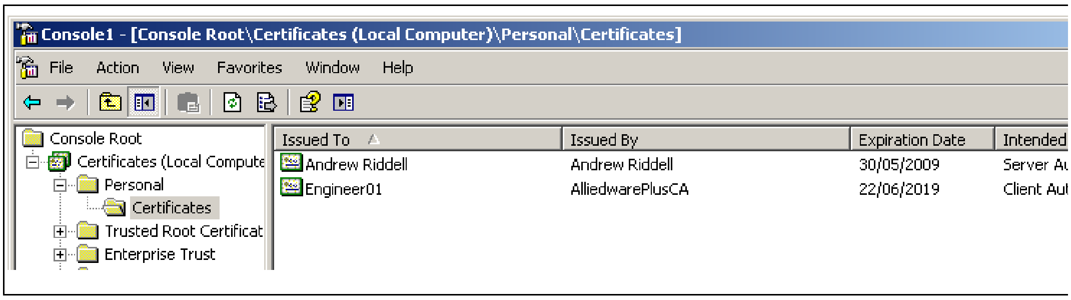
Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store: Personal

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



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended
Andrew Riddell	Andrew Riddell	30/05/2009	Server Au
Engineer01	AlliedwarePlusCA	22/06/2019	Client Aut

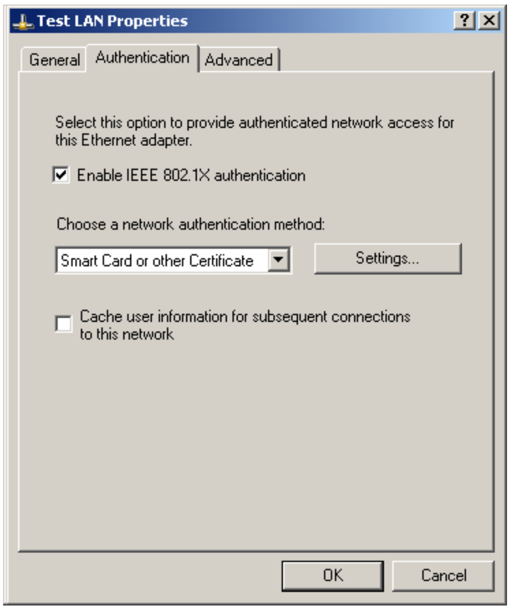
The certificates have now been successfully installed on to the PC.

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).



Test LAN Properties

General | Authentication | Advanced

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

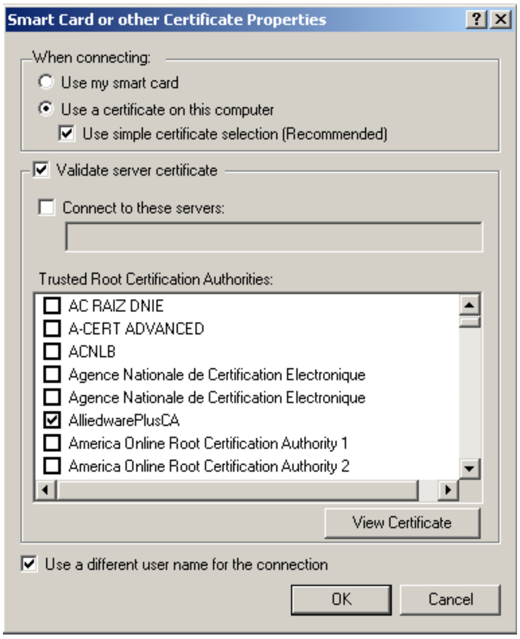
Smart Card or other Certificate ▾ | Settings...

□ Cache user information for subsequent connections to this network

2. Click **Settings...**

The Smart Card or other Certificate Properties window opens.

Choose **Use a certificate on this computer**, and select the connecting options as follows:



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ AC RAIZ DNIE
□ A-CERT ADVANCED
□ ACNLB
□ Agence Nationale de Certification Electronique
□ Agence Nationale de Certification Electronique
☑ AlliedwarePlusCA
□ America Online Root Certification Authority 1
□ America Online Root Certification Authority 2

☑ Use a different user name for the connection

- Use simple certificate selection (Recommended)
- 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:

```
awplus(config)#show dot1x supplicant
```

This will produce output similar to the following:

```
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 (Engineer01).
- MAC address of the PC (0002.b363.319f).
- ID of the VLAN that the port was dynamically allocated to (40).

Allied Telesis the solution : the network

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Antareslaan 18 | 2132 JE Hoofddorp | Netherlands | T: +31 23 5656800 | F: +31 23 5575466

alliedtelesis.com

© 2012 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.