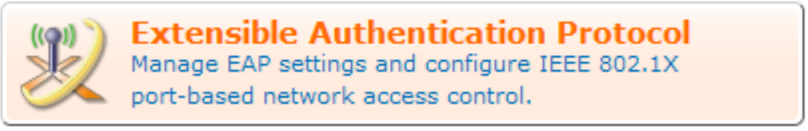
RADIUS 802.1X/EAP Setup

This is a draft guide until a full technote with a walkthrough is available.

Tested with amigopod RADIUS Services 2.0.16 which is the current 2.1 release candidate.

802.1X/EAP Configuration

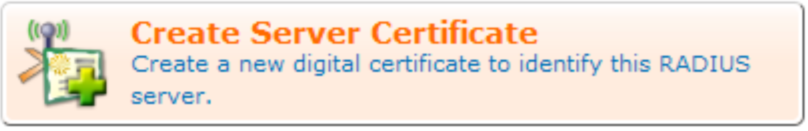
First navigate to RADIUS Services > EAP & 802.1X



Extensible Authentication Protocol

Manage EAP settings and configure IEEE 802.1X port-based network access control.

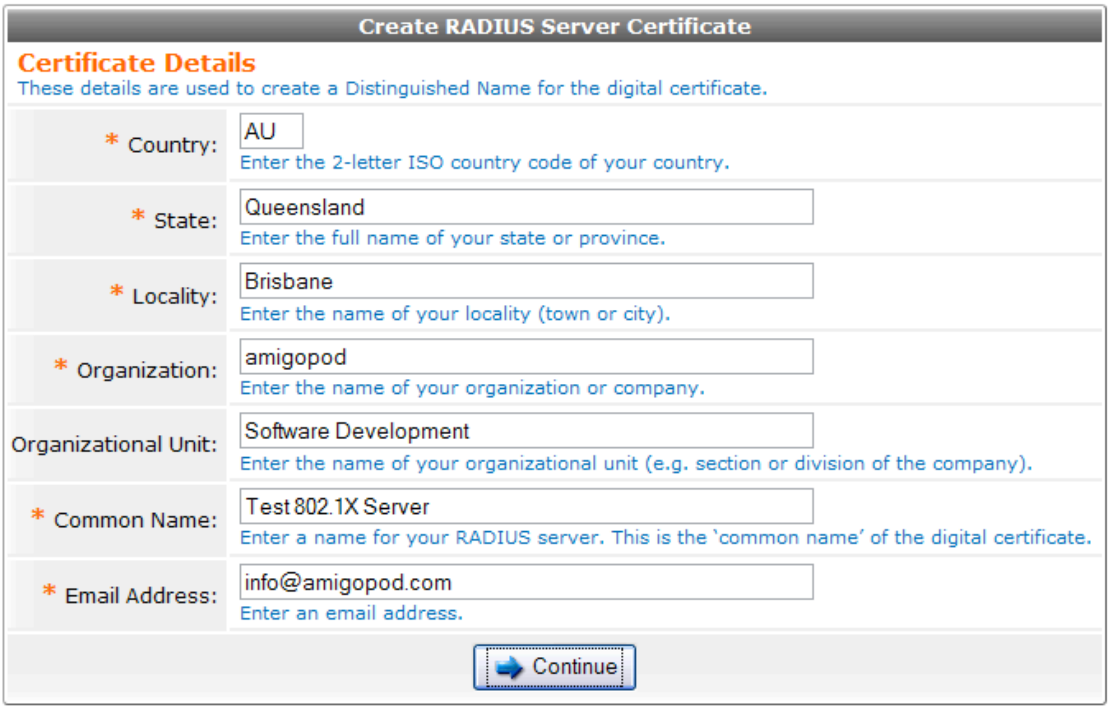
Now create a self-signed digital certificate for this server by clicking the **Create Server Certificate** link



Create Server Certificate

Create a new digital certificate to identify this RADIUS server.

Complete the **Create RADIUS Server Certificate** form – this certificate will be used to identify the server in EAP-TLS protocol (and derived protocols i.e. PEAP)



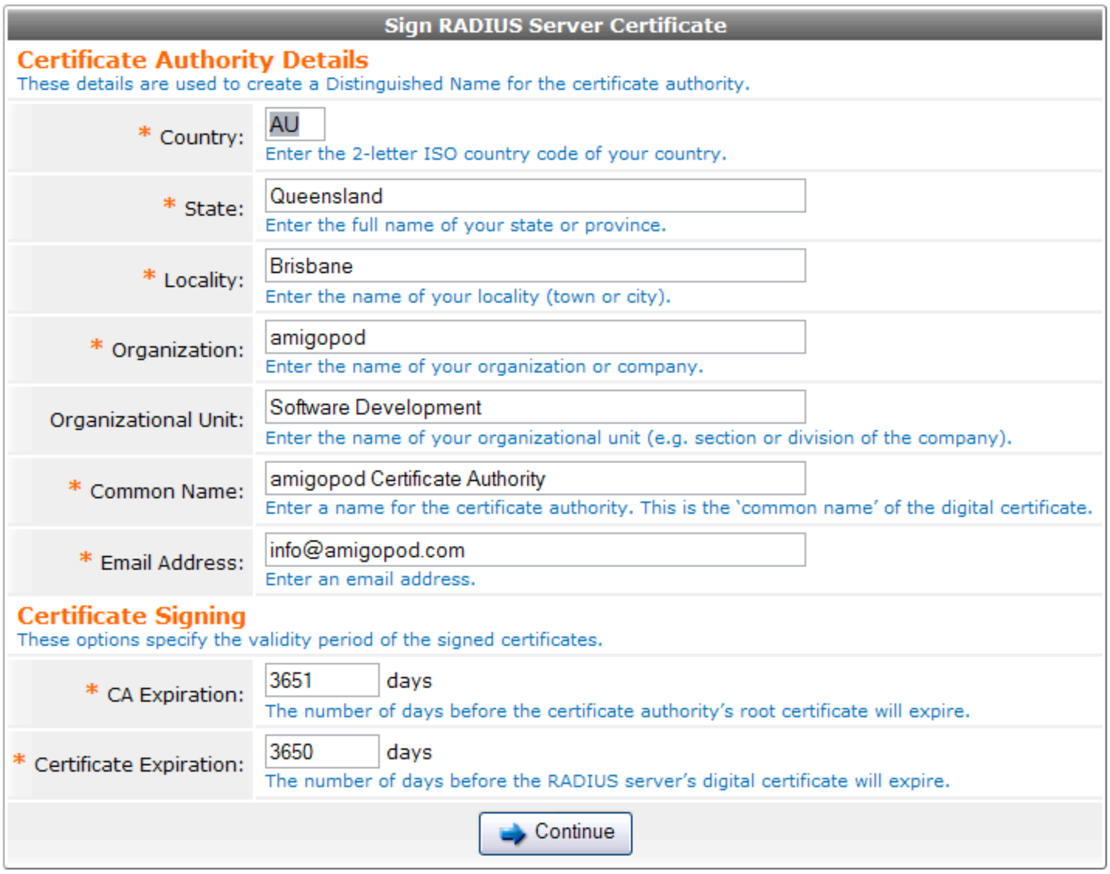
Create RADIUS Server Certificate

Certificate Details

These details are used to create a Distinguished Name for the digital certificate.

* Country:	AU Enter the 2-letter ISO country code of your country.
* State:	Queensland Enter the full name of your state or province.
* Locality:	Brisbane Enter the name of your locality (town or city).
* Organization:	amigopod Enter the name of your organization or company.
Organizational Unit:	Software Development Enter the name of your organizational unit (e.g. section or division of the company).
* Common Name:	Test 802.1X Server Enter a name for your RADIUS server. This is the 'common name' of the digital certificate.
* Email Address:	info@amigopod.com Enter an email address.

Click the **Continue** button to proceed to the **Sign RADIUS Server Certificate** form. This will be filled out with defaults based on the previous page.



Sign RADIUS Server Certificate

Certificate Authority Details

These details are used to create a Distinguished Name for the certificate authority.

* Country:	AU Enter the 2-letter ISO country code of your country.
* State:	Queensland Enter the full name of your state or province.
* Locality:	Brisbane Enter the name of your locality (town or city).
* Organization:	amigopod Enter the name of your organization or company.
Organizational Unit:	Software Development Enter the name of your organizational unit (e.g. section or division of the company).
* Common Name:	amigopod Certificate Authority Enter a name for the certificate authority. This is the 'common name' of the digital certificate.
* Email Address:	info@amigopod.com Enter an email address.

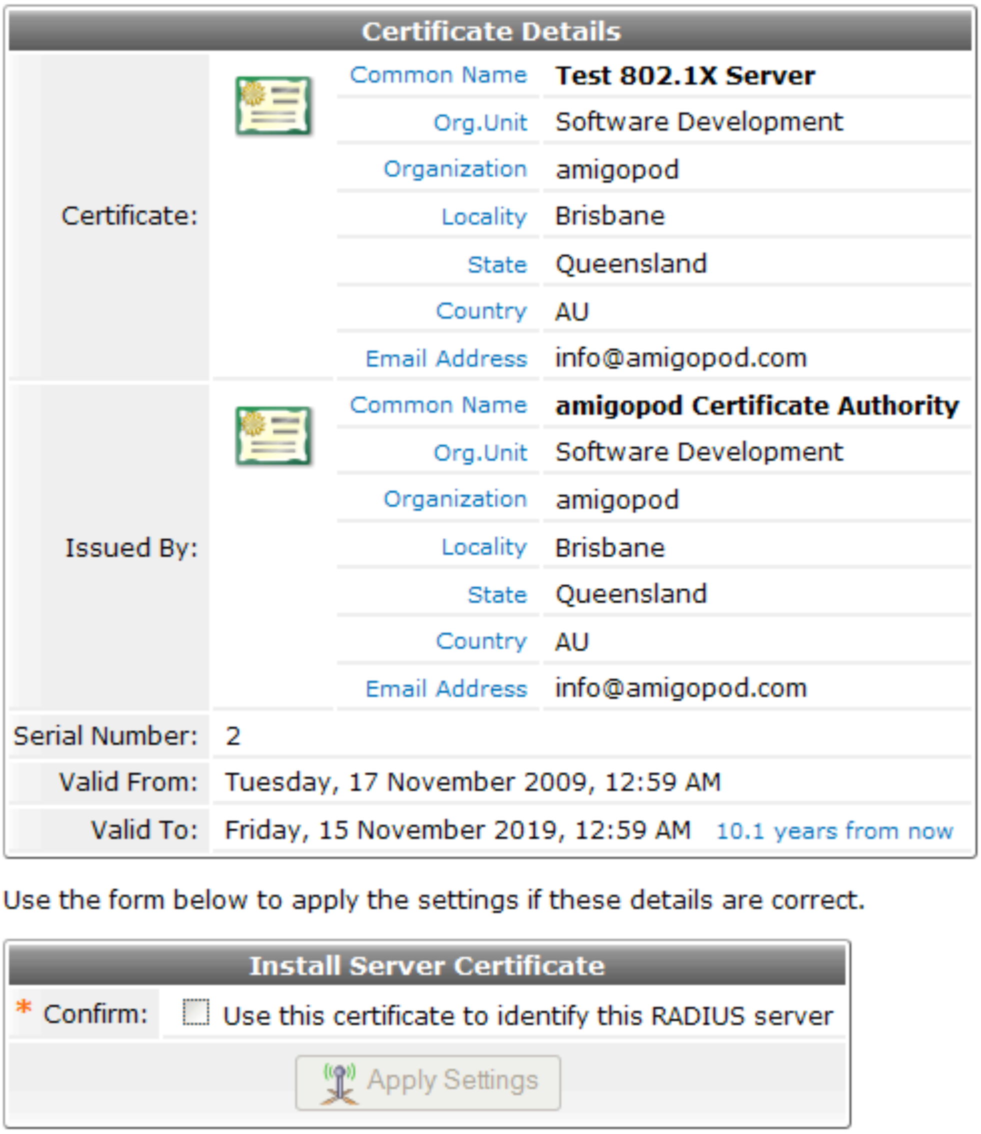
Certificate Signing

These options specify the validity period of the signed certificates.

* CA Expiration:	3651 days The number of days before the certificate authority's root certificate will expire.
* Certificate Expiration:	3650 days The number of days before the RADIUS server's digital certificate will expire.

Modify these parameters if appropriate – note that the default CA certificate expiration is set for 10 years. In particular, the "Common Name" of the certificate will be used to identify it to clients installing it as a trusted CA root, so choose a sensible name.

Click the **Continue** button to proceed to the summary screen.



Certificate Details

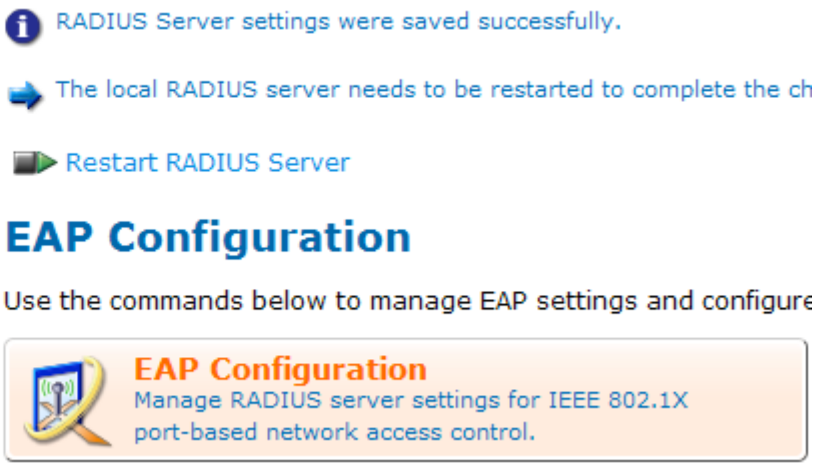
Certificate:	Common Name	**Test 802.1X Server**
	Org.Unit	Software Development
	Organization	amigopod
	Locality	Brisbane
	State	Queensland
	Country	AU
	Email Address	info@amigopod.com
Issued By:	Common Name	**amigopod Certificate Authority**
	Org.Unit	Software Development
	Organization	amigopod
	Locality	Brisbane
	State	Queensland
	Country	AU
	Email Address	info@amigopod.com
Serial Number:	2	
Valid From:	Tuesday, 17 November 2009, 12:59 AM	
Valid To:	Friday, 15 November 2019, 12:59 AM	10.1 years from now

Use the form below to apply the settings if these details are correct.

Install Server Certificate

* Confirm: □ Use this certificate to identify this RADIUS server

The details of the certificates are shown. To enable these certificates for use in EAP-TLS, EAP-TTLS and PEAP, select the **Use this certificate to identify this RADIUS server** checkbox and click **Apply Settings**.



RADIUS Server settings were saved successfully.

The local RADIUS server needs to be restarted to complete the ch

EAP Configuration

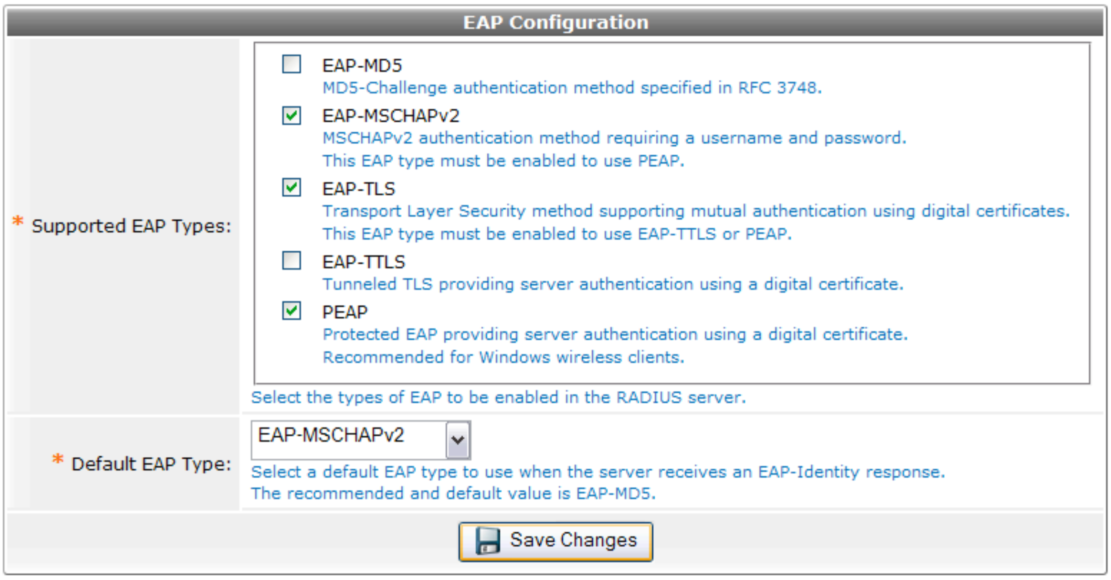
Use the commands below to manage EAP settings and configure

EAP Configuration
Manage RADIUS server settings for IEEE 802.1X port-based network access control.

RADIUS server will need to be restarted to complete these changes, but don't do this just yet as some additional configuration options must be selected. Click the **EAP Configuration** command link.

In the EAP Configuration form, select the EAP types that are to be supported.

To enable the common case of PEAPv0/MS-CHAPv2 (broadly supported by all wireless clients that implement 802.1X), complete the form as shown below:



EAP Configuration

* Supported EAP Types:

□ EAP-MD5
MD5-Challenge authentication method specified in RFC 3748.

☑ EAP-MSCHAPv2
MSCHAPv2 authentication method requiring a username and password.
This EAP type must be enabled to use PEAP.

☑ EAP-TLS
Transport Layer Security method supporting mutual authentication using digital certificates.
This EAP type must be enabled to use EAP-TTLS or PEAP.

□ EAP-TTLS
Tunneled TLS providing server authentication using a digital certificate.

☑ PEAP
Protected EAP providing server authentication using a digital certificate.
Recommended for Windows wireless clients.

Select the types of EAP to be enabled in the RADIUS server.

* Default EAP Type: EAP-MSCHAPv2
Select a default EAP type to use when the server receives an EAP-Identity response.
The recommended and default value is EAP-MD5.

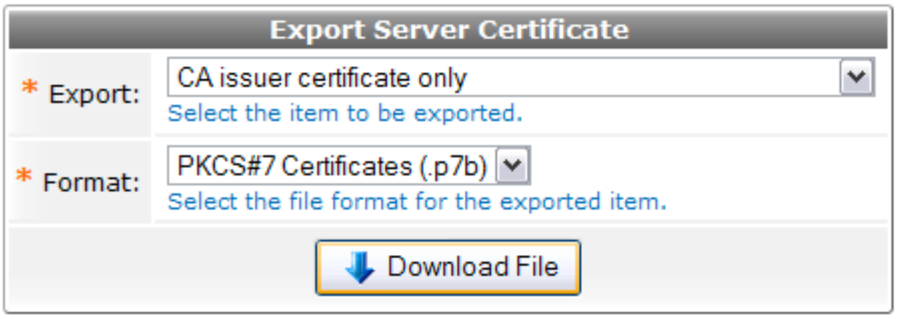
Click the **Save Changes** button. Now restart the RADIUS Server. This will apply the configuration and make it live.

You can verify that the EAP configuration is loaded by checking for a certain startup message on the **RADIUS Server Control** screen:

```
Tue Nov 17 01:04:05 2009 : Info: rlm_eap_tls: Loading the
certificate file as a chain
```

Now, the certificate authority used to issue the server's certificate must be exported. To do this, navigate to RADIUS Services > EAP & 802.1X and click the **Export Server Certificate** command link.

In the **Export Server Certificate** form, select "CA issuer certificate only" and use the default PKCS#7 container format.



Export Server Certificate

* Export: CA issuer certificate only
Select the item to be exported.

* Format: PKCS#7 Certificates (.p7b)
Select the file format for the exported item.

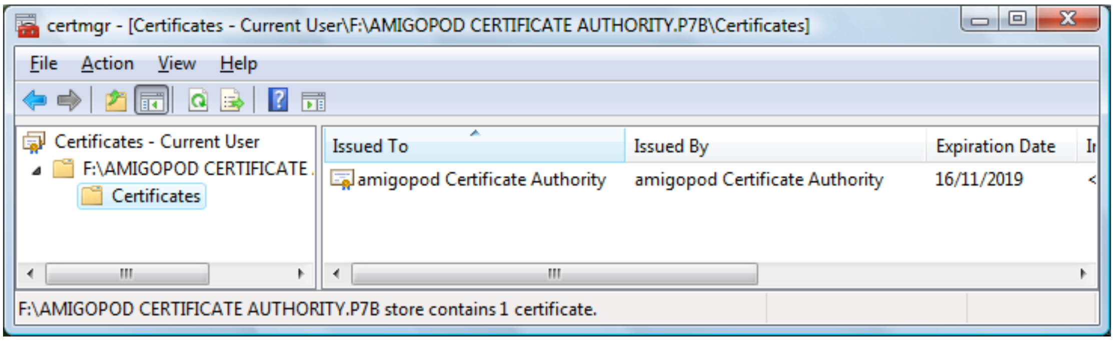
Click the **Download File** button and a file named **amigopod Certificate Authority.p7b** will be downloaded (the precise name depends on the common name for the CA certificate).

This file must be imported as a trusted root certification authority on any client wishing to authenticate using this RADIUS Server. The reason for this is that the server's identity must be established via a trusted root CA in order for authentication to proceed. When using a well-known third party CA, this step does not need to be performed as the necessary trust relationship already exists in most clients.

Importing a root CA in Windows Vista

See the following screenshots for guidance.

Open the .p7b file from Windows Explorer:

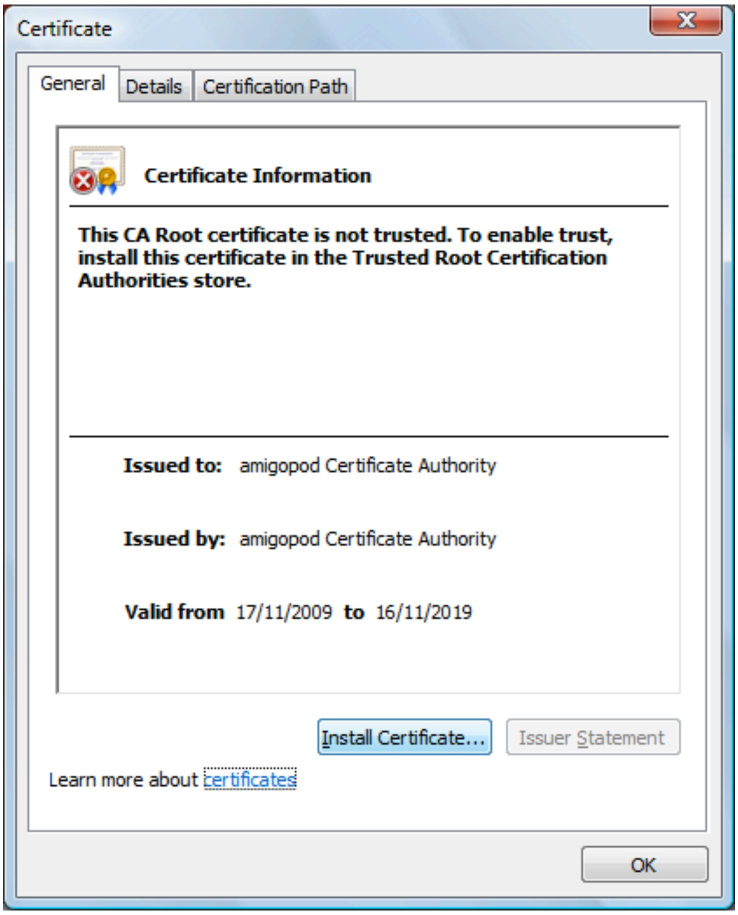


certmgr - [Certificates - Current User\F:\AMIGOPOD CERTIFICATE AUTHORITY.P7B\Certificates]

Issued To	Issued By	Expiration Date	I
amigopod Certificate Authority	amigopod Certificate Authority	16/11/2019	<

F:\AMIGOPOD CERTIFICATE AUTHORITY.P7B store contains 1 certificate.

Select the certificate in the list. Right-click it and choose **Open**



Certificate Information

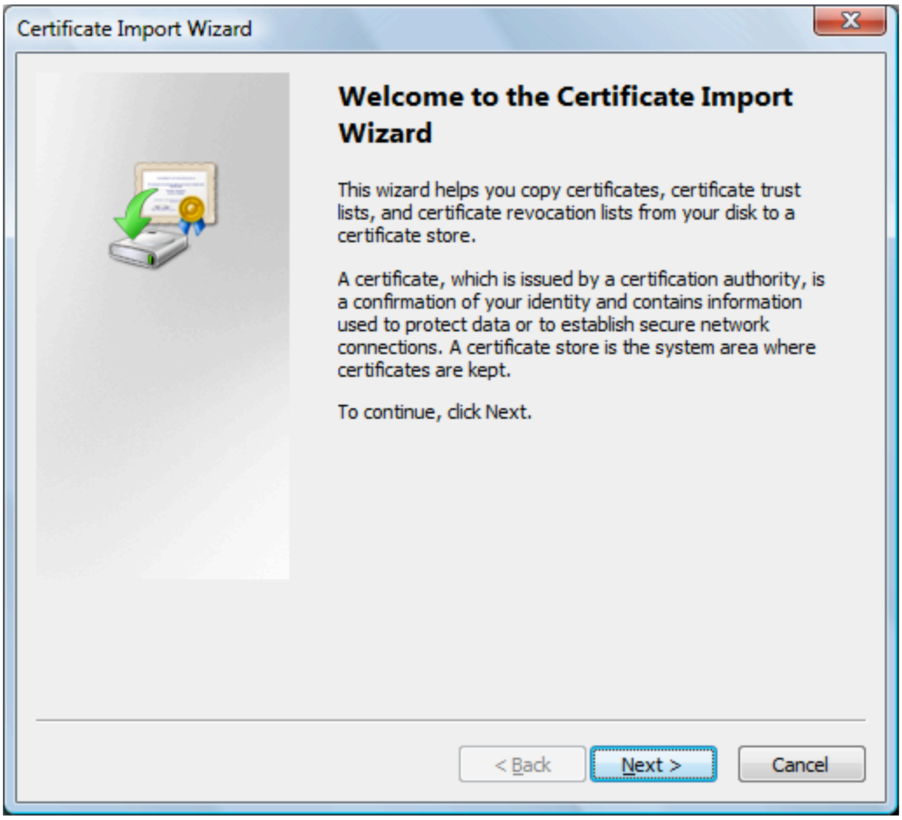
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: amigopod Certificate Authority

Issued by: amigopod Certificate Authority

Valid from 17/11/2009 to 16/11/2019

Click the Install Certificate… button

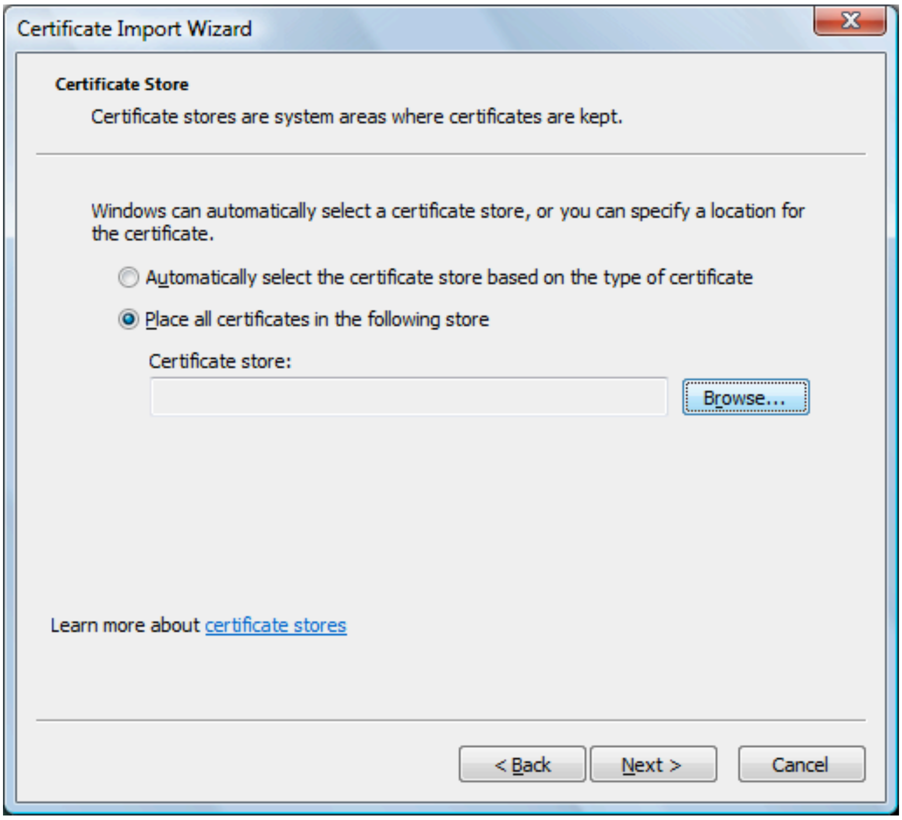


Welcome to the Certificate Import Wizard

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.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

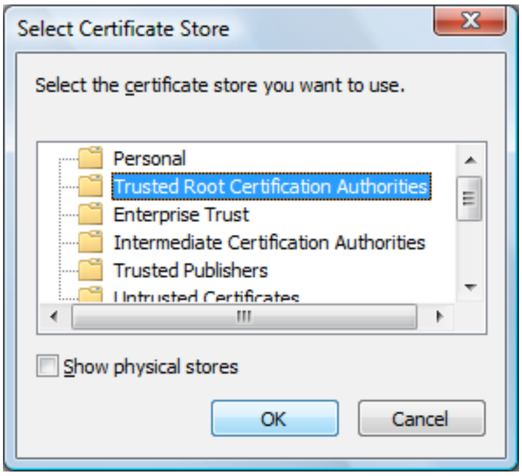
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

● Place all certificates in the following store

Certificate store:

Click the Browse… button to select the Trusted Root Certification Authorities store:

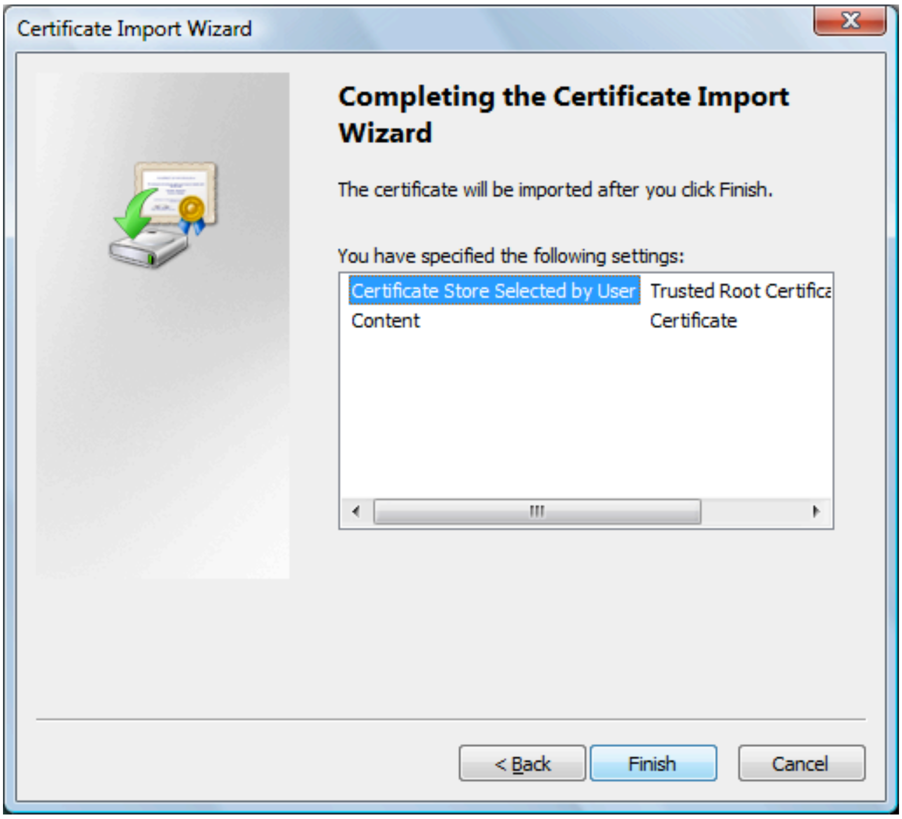


Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores



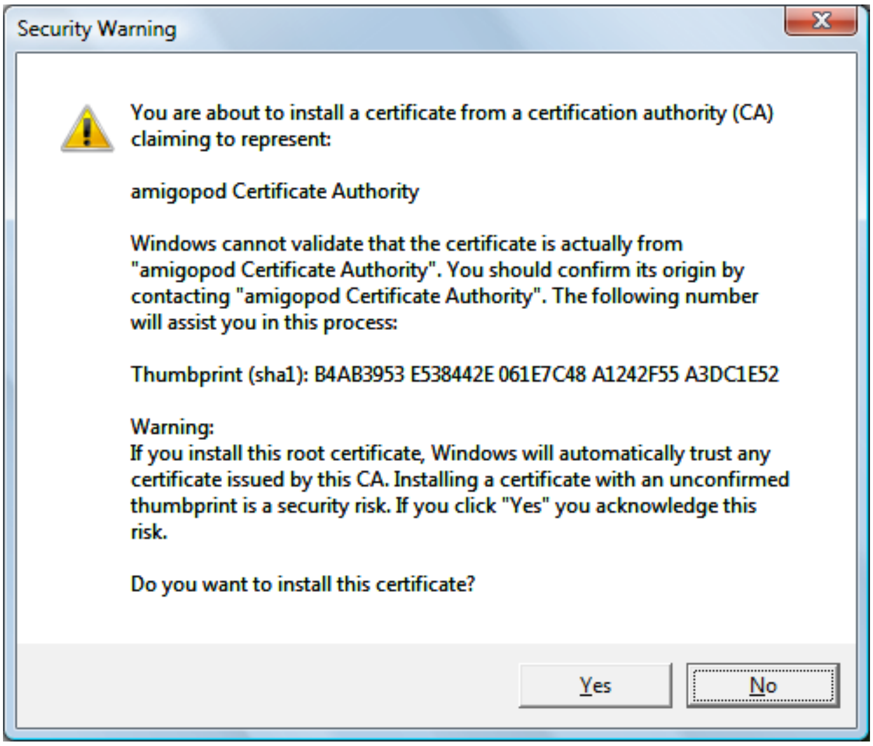
Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate



Security Warning

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

amigopod Certificate Authority

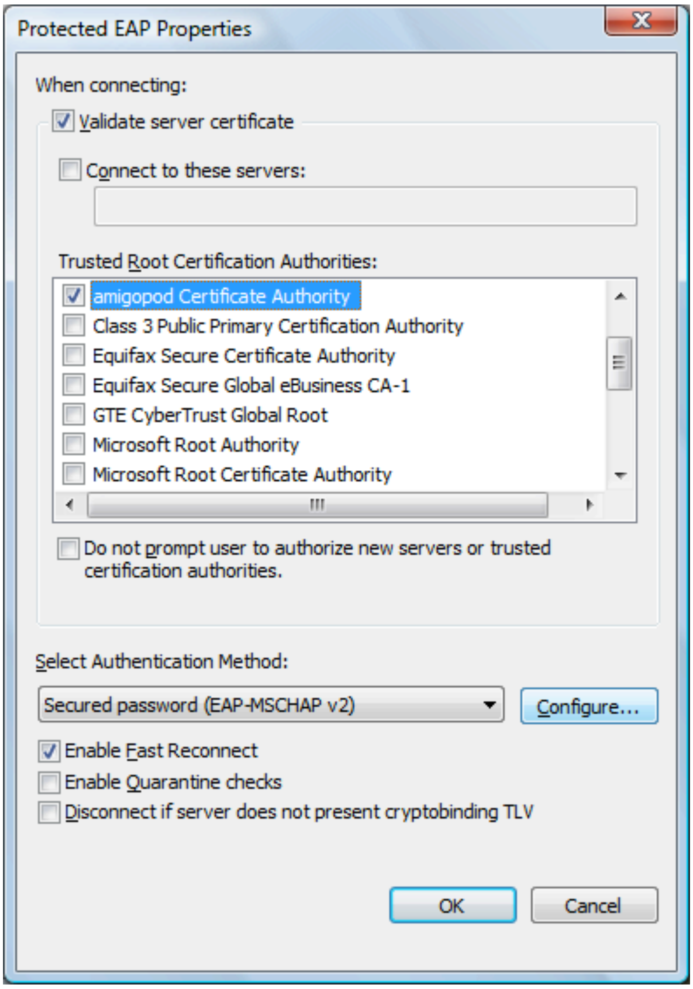
Windows cannot validate that the certificate is actually from "amigopod Certificate Authority". You should confirm its origin by contacting "amigopod Certificate Authority". The following number will assist you in this process:

Thumbprint (sha1): B4AB3953 E538442E 061E7C48 A1242F55 A3DC1E52

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?

Make sure that the imported CA is specified as a Trusted Root Certification Authority for the wireless network connection that is using PEAP.



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

☑ amigopod Certificate Authority
□ Class 3 Public Primary Certification Authority
□ Equifax Secure Certificate Authority
□ Equifax Secure Global eBusiness CA-1
□ GTE CyberTrust Global Root
□ Microsoft Root Authority
□ Microsoft Root Certificate Authority

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

□ Enable Quarantine checks

□ Disconnect if server does not present cryptobinding TLV

Successful PEAP Authentication

```
Tue Nov 17 01:20:13 2009 : Auth: Login OK:
[demo@example.com] (from client linksys port 21 cli
001c2603de08)
Tue Nov 17 01:20:13 2009 : Auth: Login OK:
[demo@example.com] (from client localhost port 0)
Tue Nov 17 01:20:13 2009 : Info: rlm_eap_mschapv2:
Issuing Challenge
Tue Nov 17 01:20:13 2009 : Error: rlm_eap: SSL error
error:00000000:lib(0):func(0):reason(0)
Tue Nov 17 01:20:13 2009 : Error: rlm_eap: SSL error
error:00000000:lib(0):func(0):reason(0)
Tue Nov 17 01:20:13 2009 : Error: TLS_accept:error in
SSLv3 read client certificate A
Tue Nov 17 01:20:13 2009 : Info: rlm_eap_mschapv2:
Issuing Challenge
```

Note that the “SSL error” messages indicated are not in fact errors – there is no client certificate in PEAP, and so these spurious error messages are generated.