

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE WPA – 802.1X PEAP WITH FUNK ODYSSEY

Written By: Michael Hong

February 2005



Summary

This installation guide provides step-by-step instructions for configuring WPA-802.1x PEAP wireless LAN security on Foundry Networks IronPoint 200 with Funk Software Odyssey. This installation guide may be useful for proof-of-concept tests, customer demonstrations or hands-on training.

Content

Before You Begin	3
Physical Network Configuration	3
Configuring IP 200 Access Point	4
Obtaining Funk Software Odyssey Server, Certificate Authority & Requester and Client	12
Installing Funk Software Odyssey Server	13
Installing and Configuring Funk Software Certificate Authority	14
Installing and Configuring Funk Software Certificate Requester	19
Approving Certificate Request	22
Configuring Funk Software Odyssey Server	26
Exporting the Server Certificate	32
Installing Funk Software Odyssey Client	40
Importing the Server Certificate	42
Configuring Funk Software Odyssey Client	46
Appendix A: Configuring IP 200 – Non-Virtual AP Versions	56
Appendix B: Disabling IAS on Microsoft Windows Server	62
Appendix C: Starting the Odyssey Service	64
Appendix D: Uninstalling Microsoft Active Directory	66



Before You Begin

This installation guide requires the following:

A Foundry Networks IronPoint 200 (IP 200) Access Point with firmware version 01.2.10 or newer.
 An Ethernet Wswitch.

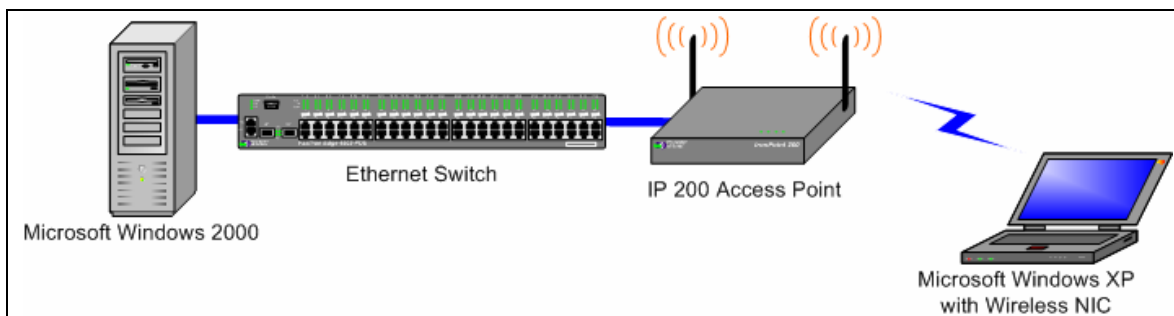
A computer that supports Funk Software's Odyssey Server¹. This installation guide uses Microsoft Windows 2000 Professional with SP4.

Another computer that supports Funk Software's Odyssey Client with a wireless NIC that is Wi-Fi certified for WPA – Enterprise². This installation guide uses Microsoft Windows XP computer with SP2 with an 802.11g wireless NIC.

Basic knowledge of wired and wireless LANs, Microsoft Windows operating systems and Foundry Networks IP 200 Access Points.

Physical Network Configuration

This installation guide uses the network configuration:



¹ For more information on supported computers, please refer to Funk Software's documentation. Information on obtaining Funk Software's documentation can be found in the section **Obtaining Funk Software Odyssey Server, Certificate Authority & Requester and Client**.

² To see if your wireless NIC is Wi-Fi certified for WPA – Enterprise, look for the Wi-Fi certification logo or check the list of Wi-Fi certified products at www.wi-fi.org/certified_products.



Configuring IP 200 Access Point

The IP 200 Access Point must be using firmware version 01.2.10 or newer.

Configuration of the IP 200 in this installation guide starts with the IP 200 in factory default configuration and with the country code and Ethernet interface IP address already configured. To configure the country code and Ethernet interface IP address, please refer to the **Foundry IronPoint 200 Installation Guide**.

This section of the installation guide configures an IP 200 using firmware version that supports Virtual AP (1.3.01 or newer). For firmware versions that do not support Virtual AP (01.3.00, 01.2.x and older), the IP 200 configuration can be found in the **Appendix A: Configuring IP 200 – Non-Virtual AP Versions**.

This installation guide includes configuration of the IP 200 from the CLI and the Web Interface. If you prefer configuring the IP 200 from the Web Interface, you can skip the next section **Configuring from the CLI** and go to the following section **Configuring from the Web Interface**.

Configuring from the CLI

If you prefer configuring the IP 200 from the web interface, you can skip this section and go to the next section **Configuring from the Web Interface**.

From the CLI, go to the configure context. Enter the following commands:

```
Foundry AP(config)#radius-server address x.x.x.x
Foundry AP(config)#radius-server key *****
```

Where:

x.x.x.x is the IP address of the computer that will have Odyssey Server installed on it. In this installation guide, this is the Windows 2000 computer.

********* is a Secret key. This Secret key can be any length and use any character.

Note: You will need to remember this Secret key when you configure the Odyssey Server.

Next, go to the context for VAP 0 on any one of the wireless interfaces. This installation guide will use the 802.11g wireless interface. Enter the following commands:

```
Foundry AP(if-wireless g: VAP[0])#802.1x required
Foundry AP(if-wireless g: VAP[0])#encryption
Foundry AP(if-wireless g: VAP[0])#wpa-clients Required
Foundry AP(if-wireless g: VAP[0])#wpa-mode Dynamic
Foundry AP(if-wireless g: VAP[0])#multicast-cipher TKIP
Foundry AP(if-wireless g: VAP[0])#ssid My SSID
Foundry AP(if-wireless g: VAP[0])#no shutdown
```

This completes the configuration of the IP 200 from the CLI. You can skip the next section **Configuring from the Web Interface** and proceed to the following section **Obtaining Funk Software Odyssey Server, Certificate Authority & Requester and Client**.

Configuring from the Web Interface

If you have configured the IP 200 using the previous section **Configuring from the CLI**, you do not need to configure the IP 200 using the Web Interface.

From the Web Interface, go to the **RADIUS** webpage.

For the **IP Address** of the **Primary Radius Server Setup**, enter the IP address of the computer that will have Odyssey Server installed on it. In this installation guide, this is the Windows 2000 computer.

Enter a **Secret Key**. This Secret Key can be any length and use any character.

Note: You will need to remember this Secret Key when you configure the Odyssey Server.

Click **Apply**.

FOUNDRY
NETWORKS

IronPoint™ 200

Logout

System

Identification

TCP/IP

RADIUS

Management Tunnel

Authentication

Bridging

Administration

Syslog & Time

VLAN

SNMP

SNMP General

SNMP Trap Filters

SNMP Targets

Radio Interface 802.11a

Radio Settings

Security

Radio Interface 802.11g

Radio Settings

Security

Status

AP Status

Stations

Event Log

Radius

Primary RADIUS Server Setup

IP Address

xxxx

Port

1812

Secret Key

XXXXXXXXXX

Timeout (seconds)

5

Retransmit attempts

3

Accounting Port

0

Interim Update Timeout

3600

Secondary RADIUS Server Setup

IP Address

0.0.0.0

Port

1812

Secret Key

XXXXXXXXXX

Timeout (seconds)

5

Retransmit attempts

3

Accounting Port

0

Interim Update Timeout

3600

Radius VLAN ID Format Setup

VLAN ID Format

ASCII

HEX

Apply

Cancel

Help

WPA – 802.1x PEAP WITH FUNK ODYSSEY



FOUNDRY
NETWORKS

When **Configuration has been saved!** appears, click **Security** for any one of the Radio Interfaces. This guide configures **Security** for **Radio Interface 802.11g**.





For **VAP 0**, check **Enable** and enter **My SSID** for the **SSID**.
Click **Apply**.

FOUNDRY NETWORKS IronPoint™ 200 Logout

System

- Identification
- TCP/IP
- RADIUS
- Management Tunnel
- Authentication
- Bridging
- Administration
- Syslog & Time
- VLAN

SNMP

- SNMP General
- SNMP Trap Filters
- SNMP Targets

Radio Interface 802.11a

- Radio Settings
- Security

Radio Interface 802.11g

- Radio Settings
- Security

Status

- AP Status
- Stations
- Event Log

802.11g:

Security

"Before enabling the radios you must set the country selection via the CLI."

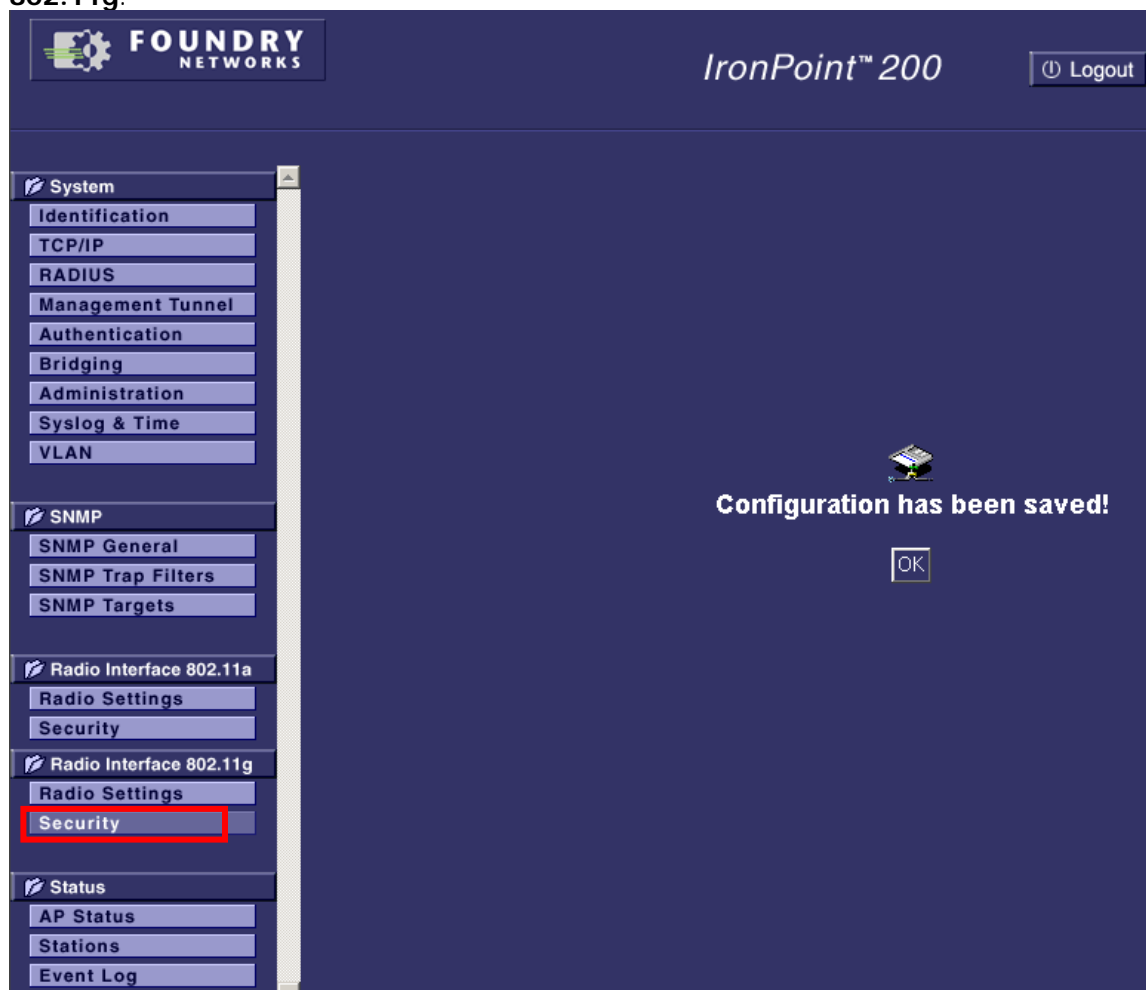
VAP Number	Enable	SSID	Details
VAP 0	<input checked="" type="checkbox"/>	My SSID	More
VAP 1	<input type="checkbox"/>	Foundry AP 1	More
VAP 2	<input type="checkbox"/>	Foundry AP 2	More
VAP 3	<input type="checkbox"/>	Foundry AP 3	More

Apply Cancel Help

WPA – 802.1x PEAP WITH FUNK ODYSSEY

**FOUNDRY**
NETWORKS

When **Configuration has been saved!** appears, click **Security** for the Radio Interface that was configured in the previous step. This guide configures **Security** for **Radio Interface 802.11g**.





For **VAP 0** click **More**.

The screenshot shows the IronPoint 200 web interface. The sidebar on the left contains the following menu items: System (Identification, TCP/IP, RADIUS, Management Tunnel, Authentication, Bridging, Administration, Syslog & Time, VLAN), SNMP (SNMP General, SNMP Trap Filters, SNMP Targets), Radio Interface 802.11a (Radio Settings, Security), Radio Interface 802.11g (Radio Settings, Security), and Status (AP Status, Stations, Event Log). The main content area is titled 'IronPoint™ 200' and has a 'Logout' button. It shows the '802.11g' configuration page, which includes a 'Security' section. A message states: "Before enabling the radios you must set the country selection via the CLI." Below this is a table with the following data:

VAP Number	Enable	SSID	Details
VAP 0	<input checked="" type="checkbox"/>	My SSID	More
VAP 1	<input type="checkbox"/>	Foundry AP 1	More
VAP 2	<input type="checkbox"/>	Foundry AP 2	More
VAP 3	<input type="checkbox"/>	Foundry AP 3	More

At the bottom right of the main content area are buttons for 'Apply', 'Cancel', and 'Help'.

WPA – 802.1x PEAP WITH FUNK ODYSSEY

**FOUNDRY®**
NETWORKS

This will take you to the **802.11g (VAP 0) Security** page. (See the screen image on the next page)

For 802.1x Setup: select Required.

For WEP Authentication Type Setup, select Open System.

For Data Encryption Setup, select Enable.

For WPA Clients, select Required.

For WPA Key Management, select WPA Authentication over 802.1x.

For Multicast Cipher Mode, select TKIP.

Click **Apply**.

This completes the configuration of the IP 200 from the Web Interface. Proceed to the next section **Obtaining Funk Software Odyssey Server, Certificate Authority & Requester and Client**.

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

WPA – 802.1x PEAP WITH FUNK ODYSSEY



IronPoint™ 200
Logout

System

Identification
TCP/IP
RADIUS
Management Tunnel
Authentication
Bridging
Administration
Syslog & Time
VLAN

SNMP

SNMP General
SNMP Trap Filters
SNMP Targets

Radio Interface 802.11a

Radio Settings
Security

Radio Interface 802.11g

Radio Settings
Security

Status

AP Status
Stations
Event Log

802.11g: (VAP 0)

Security

Authentication

802.1x Setup :

☐ Disable 802.1x authentications not allowed
☐ Supported Clients may or may not use 802.1x
☒ Required Client must use 802.1x

If 802.1x supported or required is selected, then Radius setup must be completed

Broadcast Key Refresh Rate minutes (0 = Disabled)

Session Key Refresh Rate minutes (0 = Disabled)

802.1x Authentication Refresh Rate minutes (0 = Disabled)

WEP

Authentication Type Setup

☒ Open System Allow everyone to access
☐ Shared Key Allow users with a correct key to access

Data Encryption Setup

☐ Disable
☒ Enable

WPA

WPA Clients

☐ Disabled MU must have WEP enabled to access AP
☐ Supported MU may have WPA enabled to access AP
☒ Required MU must have WPA enabled to access AP

WPA Key Management

☒ WPA authentication over 802.1x
☐ WPA Pre-shared Key

Multicast Cipher Mode

☐ WEP Use WEP as WPA Multicast cipher mode
☒ TKIP Use TKIP as WPA Multicast cipher mode
☐ AES Use AES as WPA Multicast cipher mode

WPA Pre-Shared Key Type

☒ Hexadecimal Enter 64 digits
☐ Alphanumeric Enter between 8 and 63 characters

WPA Pre-Shared Key

Apply

Cancel

Help

February 2005

© 2005 Foundry Networks, Inc.
All Rights Reserved.

11



Obtaining Funk Software Odyssey Server, Certificate Authority & Requester and Client

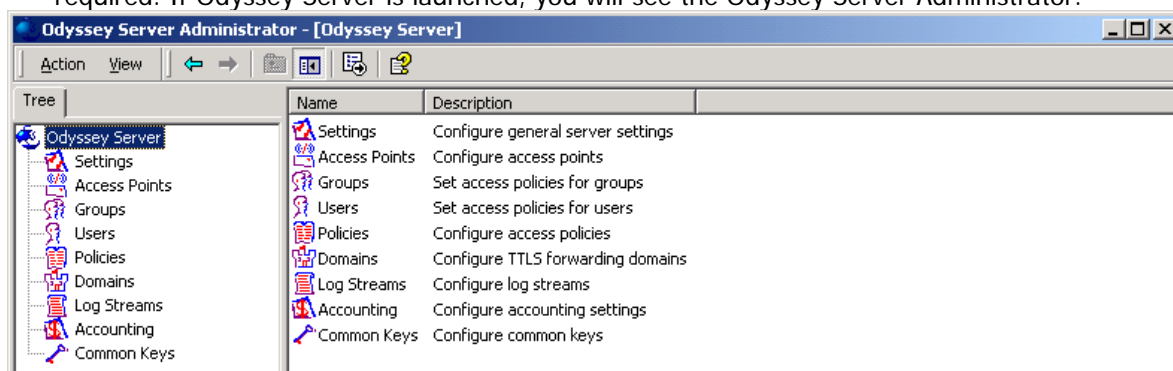
1. On the Internet, go to: <http://www.funk.com/>
2. From the Choose a Product/Download Demo drop down menu, select Odyssey.
3. From the Odyssey webpage, select the link "Download demo".
4. This may redirect you to a registration webpage. Enter the required information and submit.
5. This will redirect you to the Odyssey – Download Demo webpage. Download the following files:
 - odys201.msi: Odyssey Server
 - Odyssey_CA.msi: Odyssey Certificate Authority
 - Odyssey_CR.msi: Odyssey Certificate Requester
 - odyc303.msi: Odyssey Client. There may be other versions. Select the version that supports the computer that you will be installing the Odyssey Client on. This installation guide will be installing odyc303.msi.

Note: You may also download the Readme, Manuals and other files for additional information on Odyssey such as supported computers and configurations. Downloading this additional information is not required for this installation guide.



Installing Funk Software Odyssey Server

1. While it is possible to run multiple RADIUS servers on the same computer, configuring this falls outside of the scope of this installation guide. Therefore, ensure that no other RADIUS servers are installed or enabled on the computer that you will be installing Odyssey Server on. If using Microsoft Windows Server, ensure that IAS is uninstalled or disabled. For instructions on how to disable IAS, see **Appendix B: Disabling IAS on Microsoft Windows Server**.
2. While it is also possible to run Odyssey Server with Microsoft Active Directory, configuring this also falls outside of the scope of this installation guide. Therefore, ensure that Microsoft Active Directory is not installed on the computer that you will be installing Odyssey Server on. For instructions on how to uninstall Active Directory, see **Appendix D: Uninstalling Active Directory**.
3. Copy the file odys201.msi to the computer you want to install Odyssey Server on. In this installation guide, this will be the Windows 2000 computer.
4. Open odys201.msi to run the installation program. This installation guide selects the default installation settings when provided.
5. When the installation completes, you may launch Odyssey Server. This is step not required. If Odyssey Server is launched, you will see the Odyssey Server Administrator.



6. If you see the message below when launching Odyssey Server, see **Appendix C: Starting the Odyssey Service**.



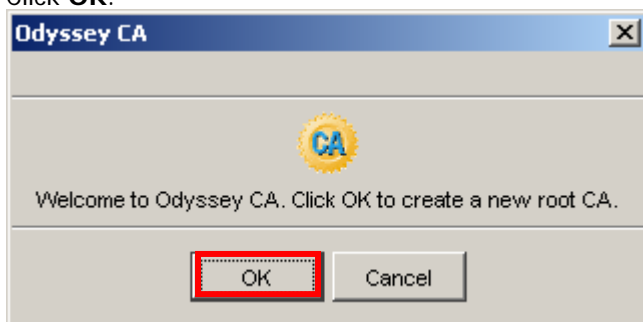
Proceed to the next section, **Installing and Configuring Funk Software Certificate Authority**.



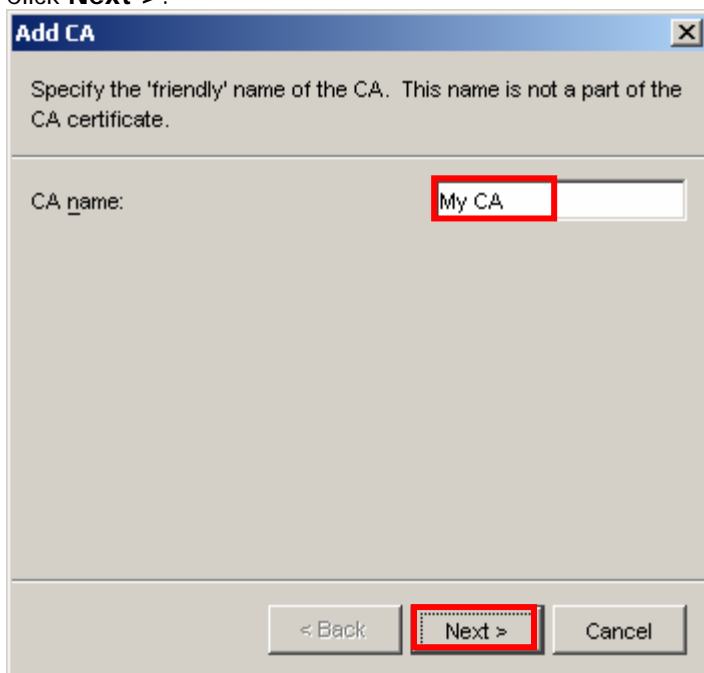
Installing and Configuring Funk Software Certificate Authority

1. Copy the file Odyssey_CA.msi to the computer you've installed Odyssey Server on. In this installation guide, this will be the Windows 2000 computer.
2. From the Windows 2000 computer, open the Odyssey_CA.msi file. This will install the Odyssey CA on the computer. This installation guide selects the default installation settings when provided.
Note: Installation of the Certificate Authority requires administrative privileges on the computer. The installation will not succeed without administrative privileges.
3. When the installation completes, launch Odyssey CA.

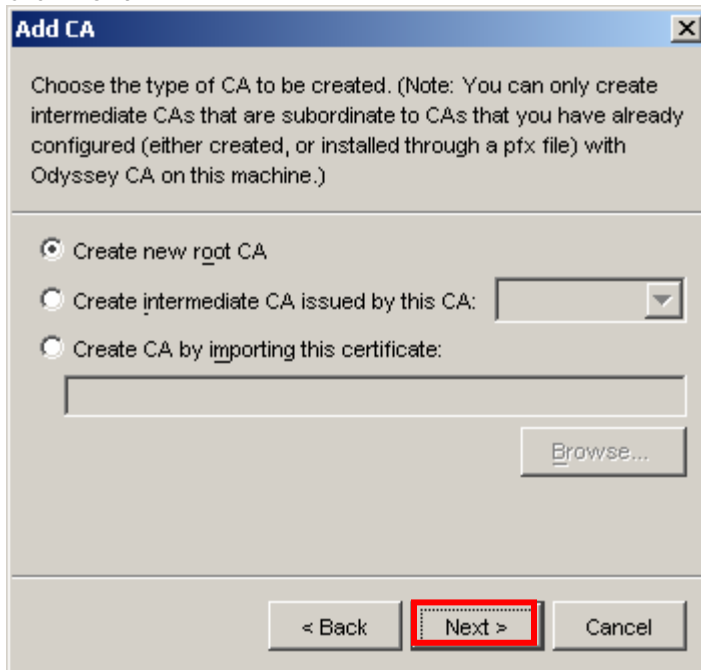
This will open a **Welcome to Odyssey CA** window.
Click **OK**.



Enter **My CA** for **CA name**.
Click **Next >**.



Click **Next >**.



Add CA

Choose the type of CA to be created. (Note: You can only create intermediate CAs that are subordinate to CAs that you have already configured (either created, or installed through a pfx file) with Odyssey CA on this machine.)

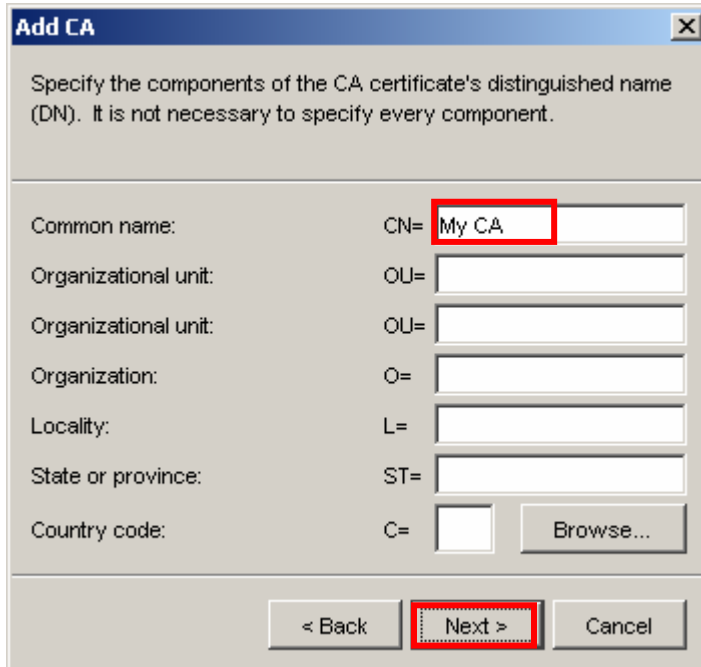
☒ Create new root CA

☐ Create intermediate CA issued by this CA:

☐ Create CA by importing this certificate:

Enter My CA for Common name:.

Click Next >.

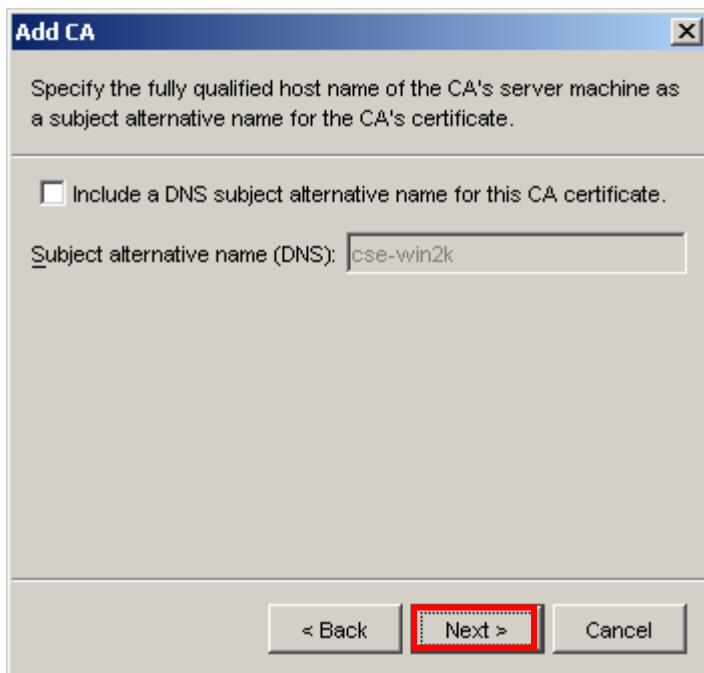


Add CA

Specify the components of the CA certificate's distinguished name (DN). It is not necessary to specify every component.

Common name:	CN=	<input style="border: 2px solid red;" type="text" value="My CA"/>
Organizational unit:	OU=	<input type="text"/>
Organizational unit:	OU=	<input type="text"/>
Organization:	O=	<input type="text"/>
Locality:	L=	<input type="text"/>
State or province:	ST=	<input type="text"/>
Country code:	C=	<input type="text"/> <input type="button" value="Browse..."/>

Click **Next >**.



Add CA [X]

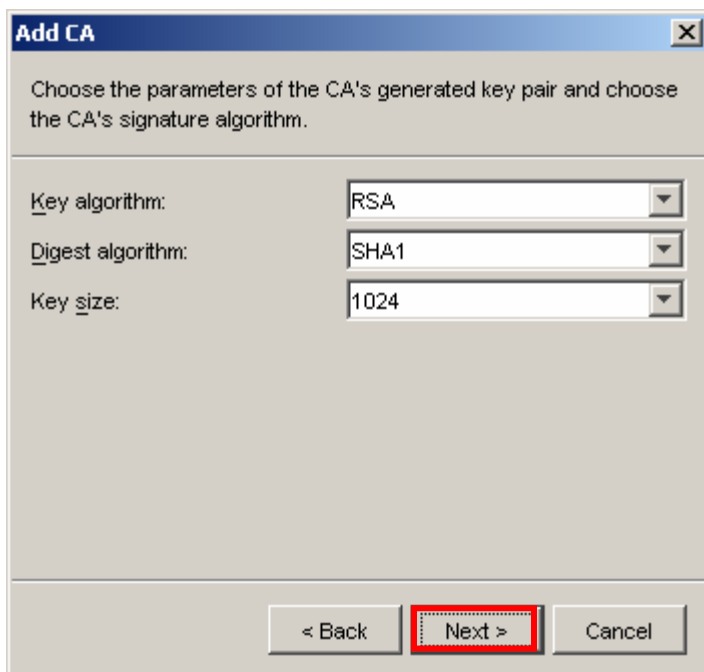
Specify the fully qualified host name of the CA's server machine as a subject alternative name for the CA's certificate.

☐ Include a DNS subject alternative name for this CA certificate.

Subject alternative name (DNS):

< Back **Next >** Cancel

Click Next >.



Add CA [X]

Choose the parameters of the CA's generated key pair and choose the CA's signature algorithm.

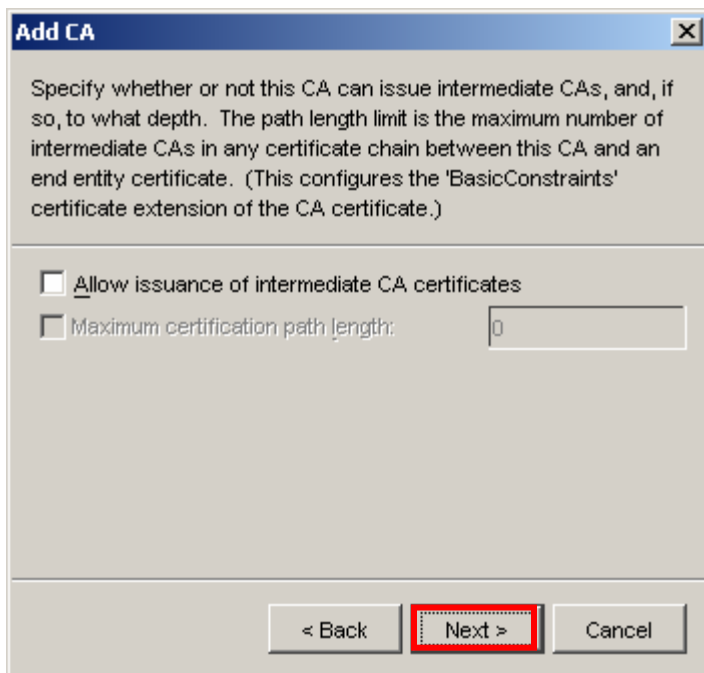
Key algorithm:

Digest algorithm:

Key size:

< Back **Next >** Cancel

Click **Next** >.



Add CA

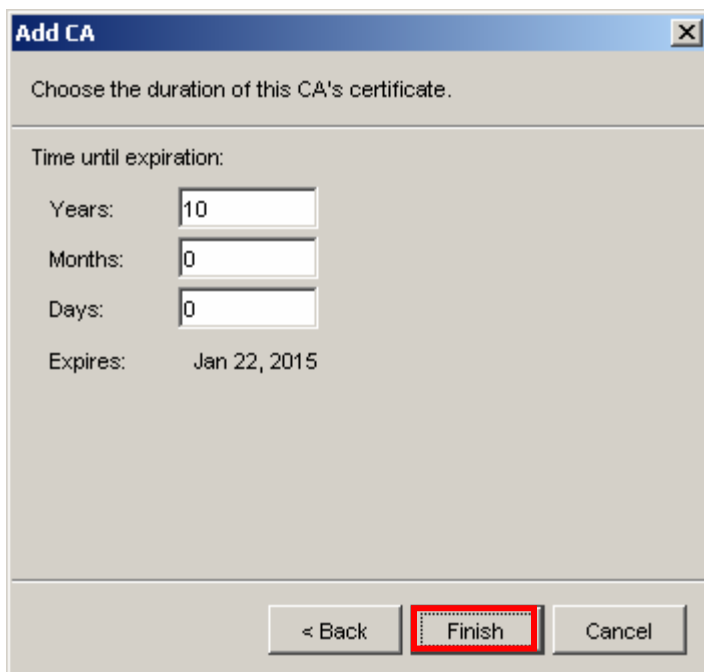
Specify whether or not this CA can issue intermediate CAs, and, if so, to what depth. The path length limit is the maximum number of intermediate CAs in any certificate chain between this CA and an end entity certificate. (This configures the 'BasicConstraints' certificate extension of the CA certificate.)

☐ Allow issuance of intermediate CA certificates

☐ Maximum certification path length:

< Back **Next >** Cancel

Click **Finish**.



Add CA

Choose the duration of this CA's certificate.

Time until expiration:

Years:

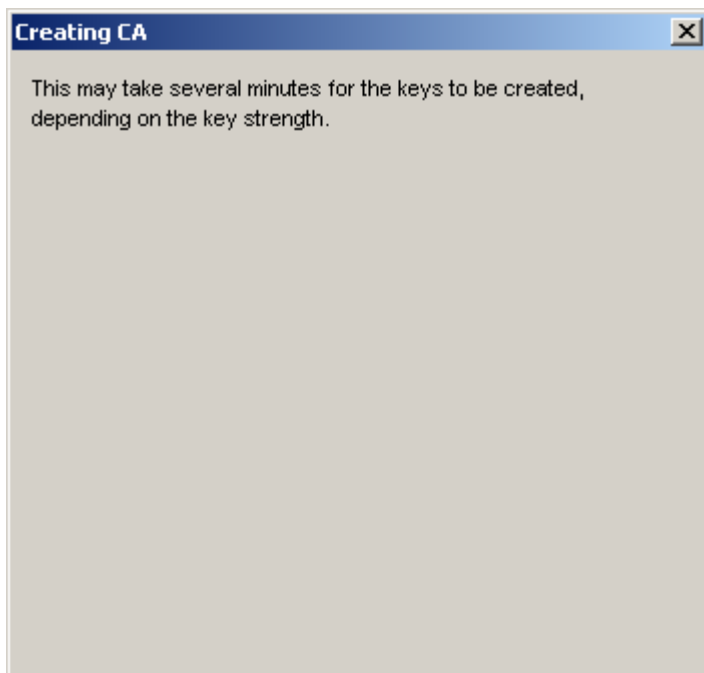
Months:

Days:

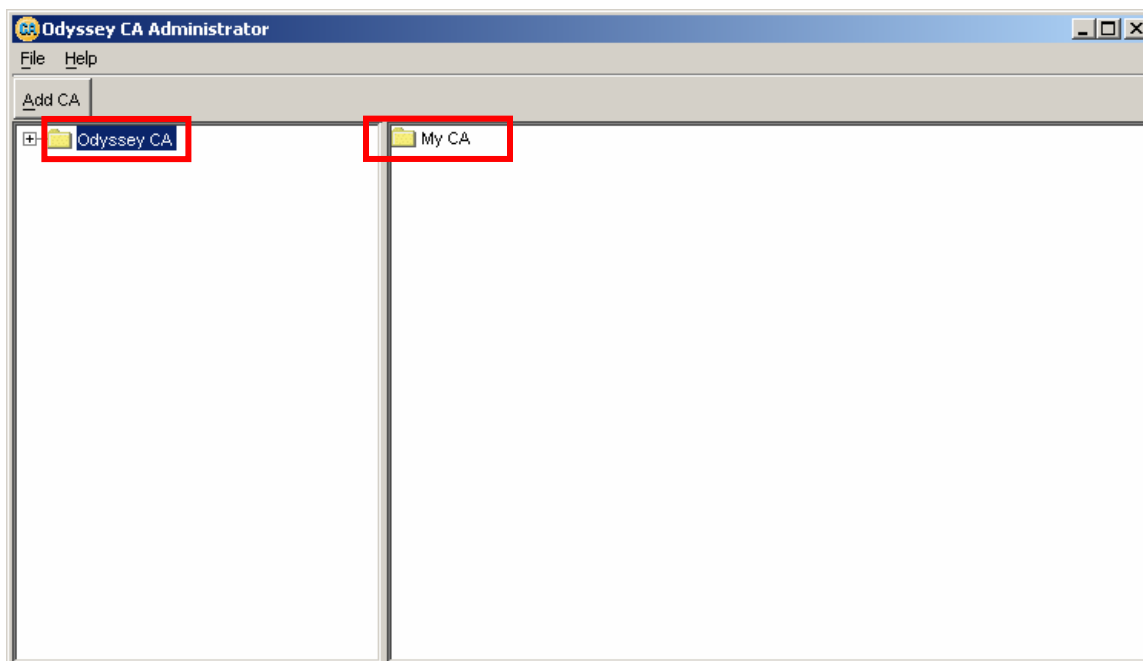
Expires: Jan 22, 2015

< Back **Finish** Cancel

You will see this window while the keys are being created.



When the keys have been created, you will see the **Odyssey CA Administrator**. Select **Odyssey CA** on the left hand column. Confirm that **My CA** appears on the right hand column.



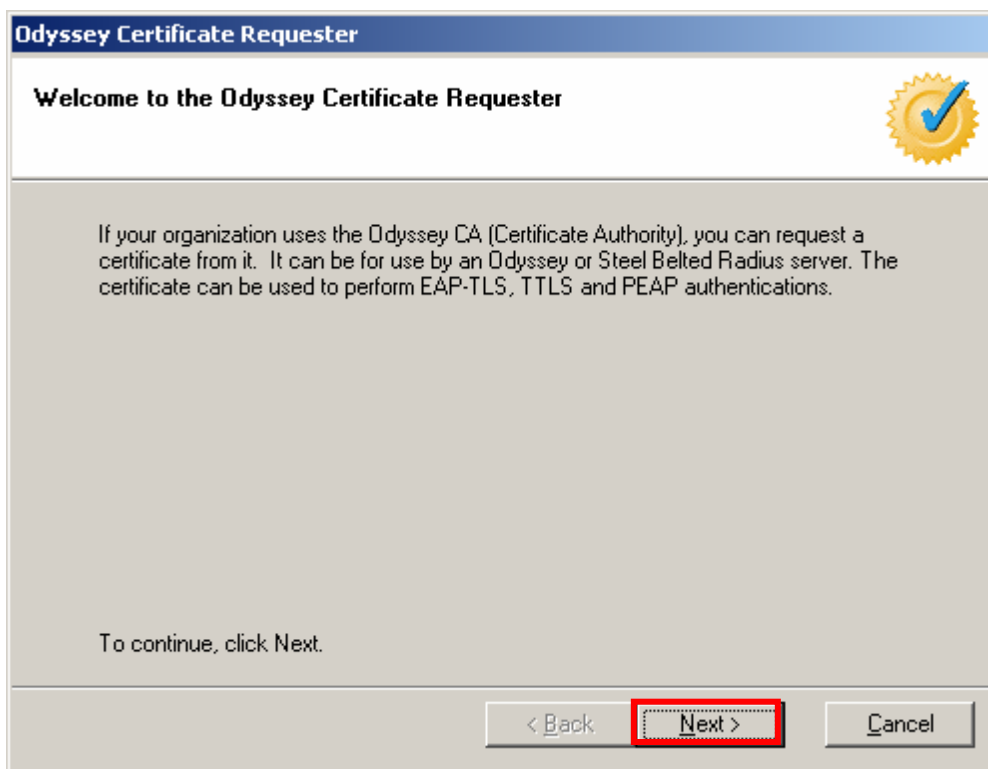
Proceed to the next section **Installing and Configuring Funk Software Certificate Requester**.



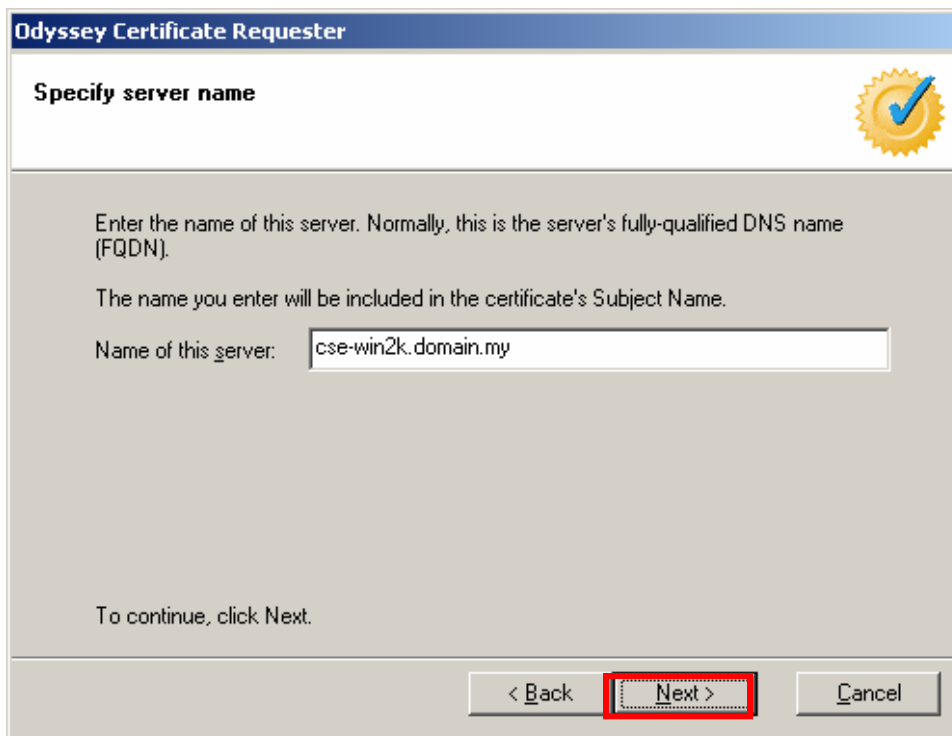
Installing and Configuring Funk Software Certificate Requester

1. Copy the file Odyssey_CR.msi to the computer you installed Odyssey Server on. In this installation guide, this will be the Windows 2000 computer.
2. From the Windows 2000 computer, open the Odyssey_CR.msi file. This will install the Odyssey Certificate Requester on the computer.
3. Follow all of the instructions in the installation program. Select the default settings when provided.
4. When the installation completes, you may be asked to reboot your computer. If so, reboot your computer.
5. When the computer reboots, launch Odyssey Certificate Requester.

This will open the “Welcome to the Odyssey Certificate Requester” window. Click **Next >**.



Click **Next >**.



Odyssey Certificate Requester

Specify server name

Enter the name of this server. Normally, this is the server's fully-qualified DNS name (FQDN).

The name you enter will be included in the certificate's Subject Name.

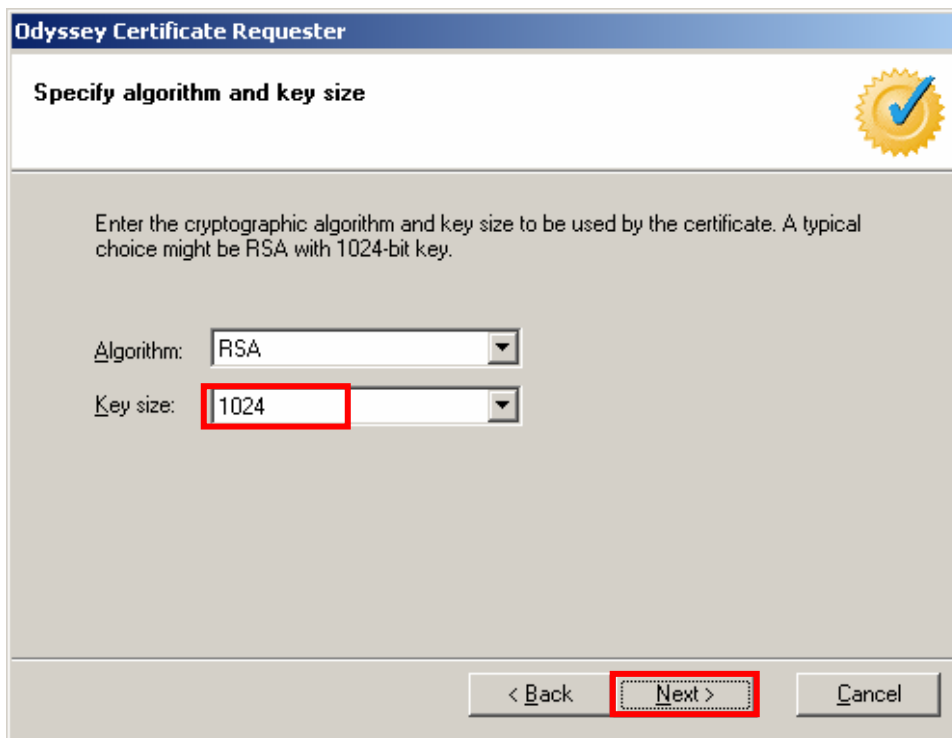
Name of this server:

To continue, click Next.

< Back **Next >** Cancel

Set Key size: to 1024.

Click Next >.



Odyssey Certificate Requester

Specify algorithm and key size

Enter the cryptographic algorithm and key size to be used by the certificate. A typical choice might be RSA with 1024-bit key.

Algorithm:

Key size:

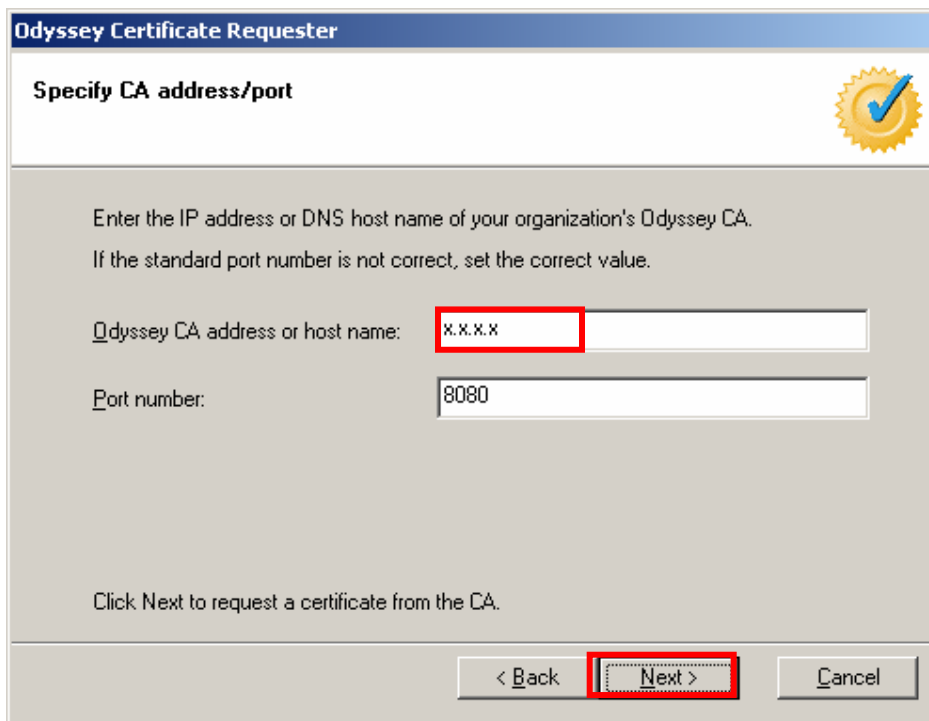
< Back **Next >** Cancel

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

WPA – 802.1x PEAP WITH FUNK ODYSSEY

**FOUNDRY**[®]
NETWORKS

For **Odyssey CA address or host name**, enter the IP address of this computer.
Click **Next >**.



Odyssey Certificate Requester

Specify CA address/port

Enter the IP address or DNS host name of your organization's Odyssey CA.
If the standard port number is not correct, set the correct value.

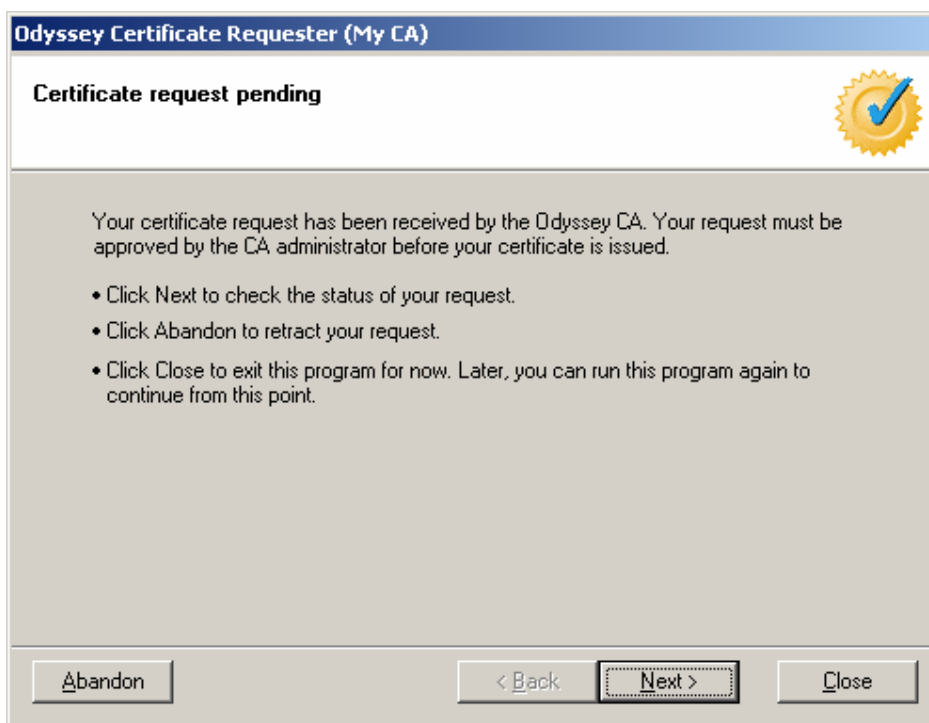
Odyssey CA address or host name:

Port number:

Click Next to request a certificate from the CA.

< Back **Next >** Cancel

You will see the Certificate request pending window.



Odyssey Certificate Requester (My CA)

Certificate request pending

Your certificate request has been received by the Odyssey CA. Your request must be approved by the CA administrator before your certificate is issued.

- Click Next to check the status of your request.
- Click Abandon to retract your request.
- Click Close to exit this program for now. Later, you can run this program again to continue from this point.

Abandon < Back **Next >** Close

Leave this window open and proceed to the next section **Approve Certificate Request**.



Approving Certificate Request

Launch Odyssey CA Administrator.

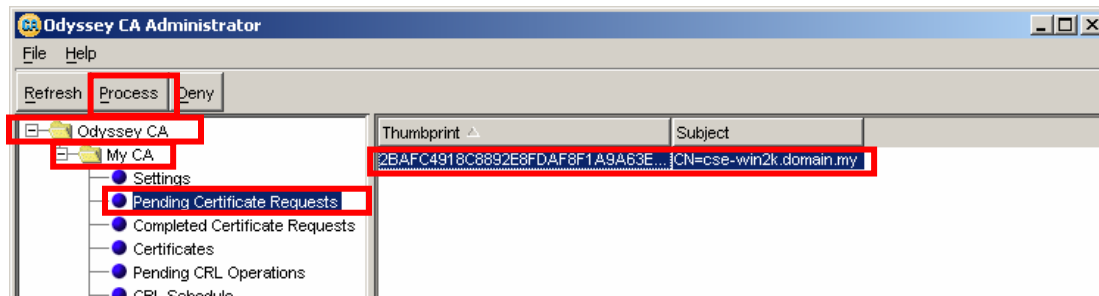
Select **Odyssey CA** in the left hand column. This will open the folder to show **My CA**.

Select **My CA**. This will open the folder to show information for **My CA**.

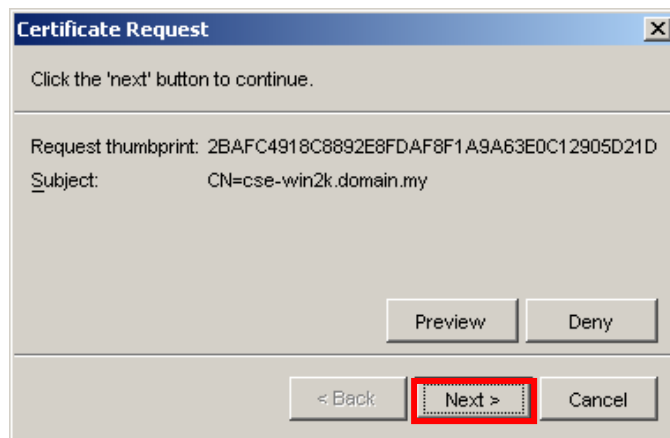
Select **Pending Certificate Requests**. This will show all pending certificate requests on the right hand column.

Select the pending certificate request.

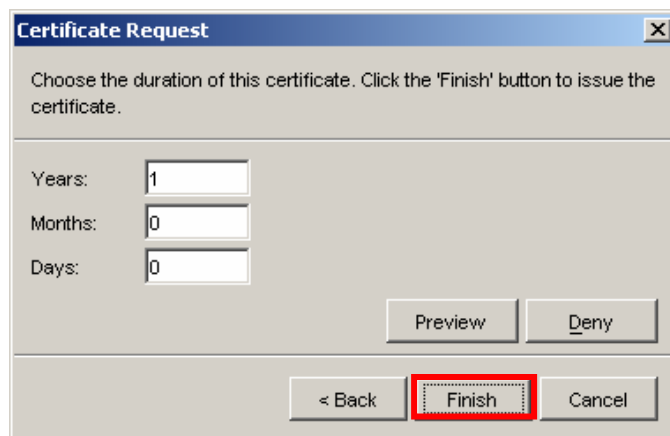
Click **Process**.



Click **Next >**.

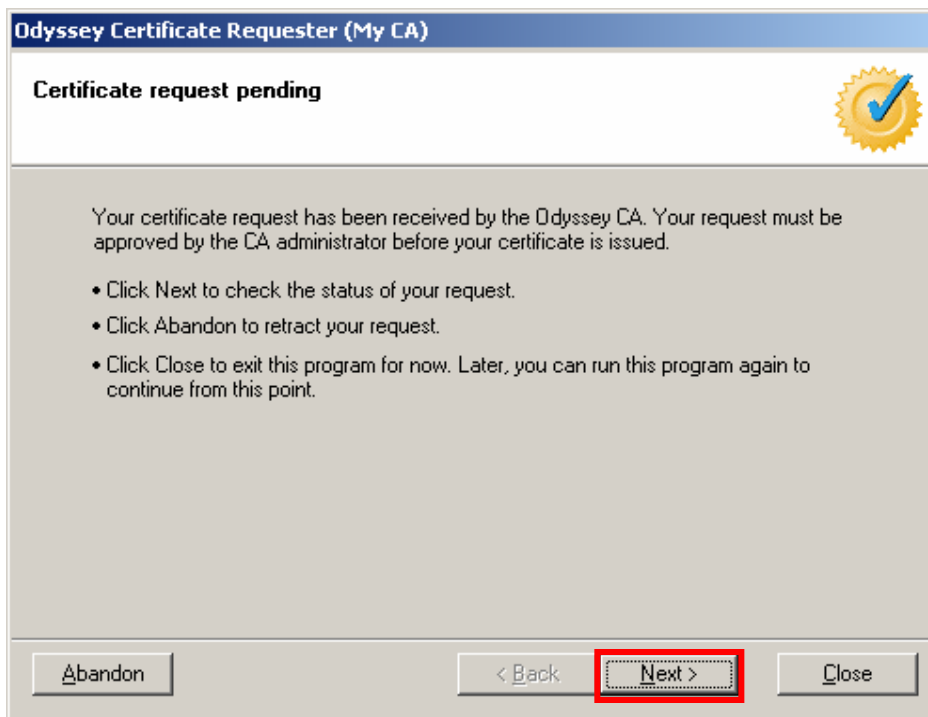


Click **Finish**



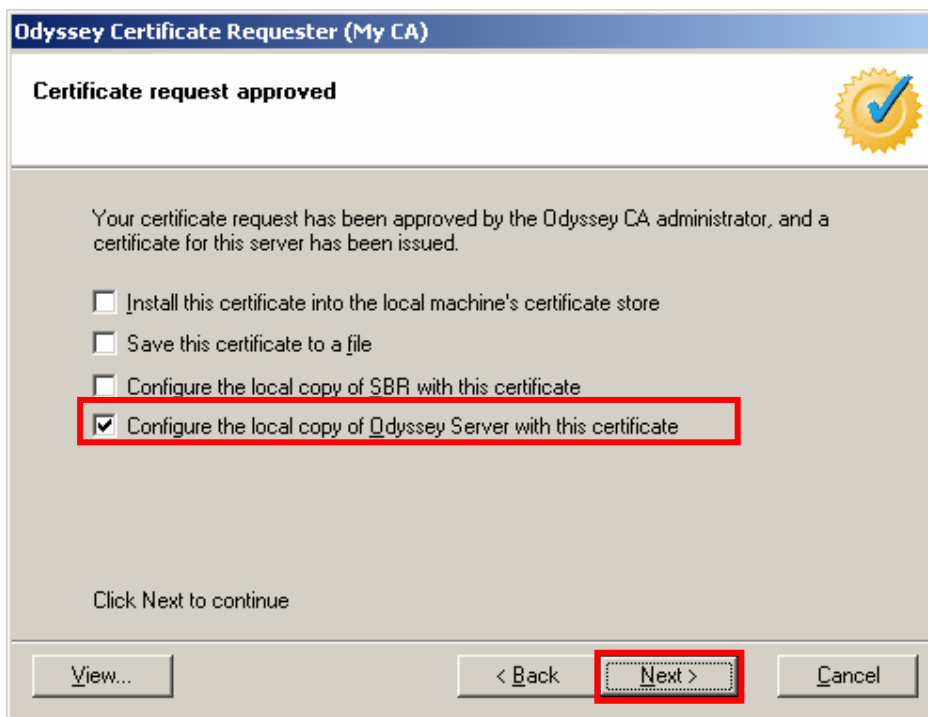
Return to the Odyssey Certificate Requester **Certificate request pending** window.

Click **Next >**.

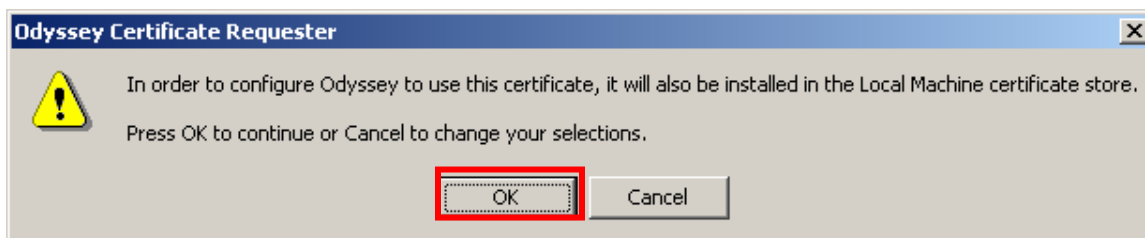


Select Configure the local copy of Odyssey Server with this certificate.

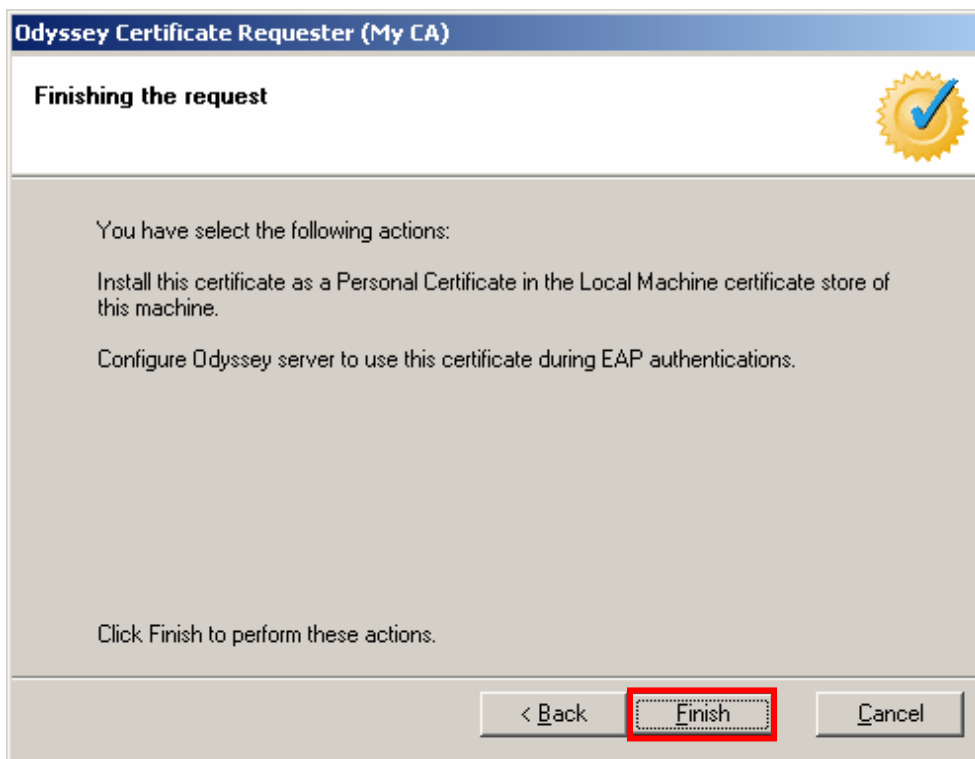
Click **Next >**.



Click **OK**.

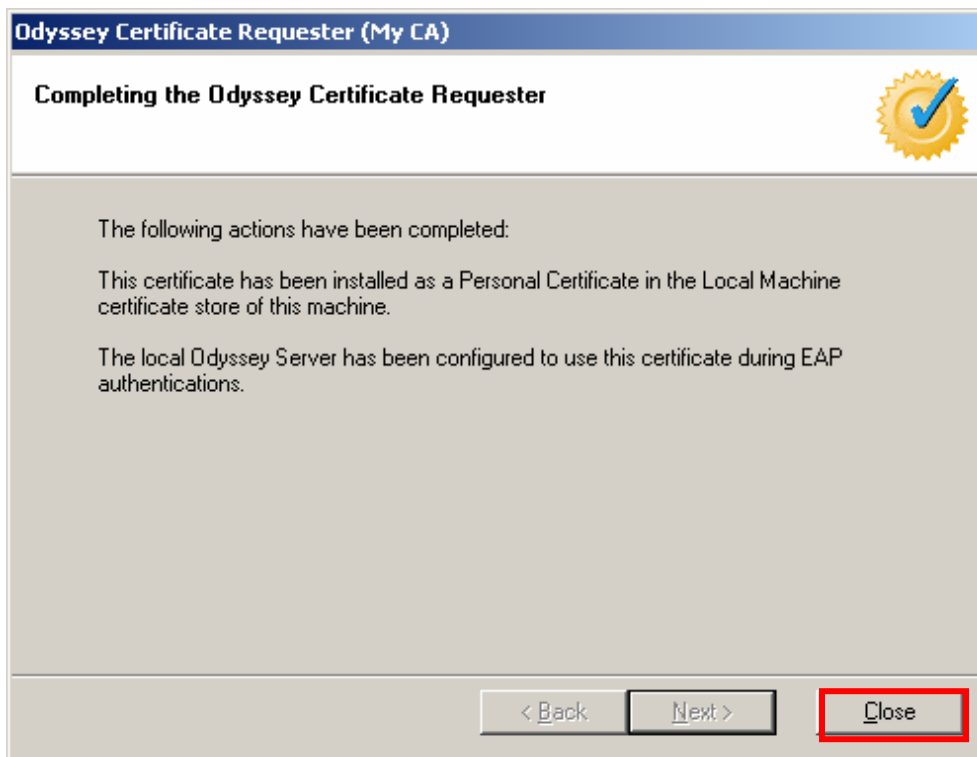


Click **Finish**.



WPA – 802.1x PEAP WITH FUNK ODYSSEY

Click **Close**.



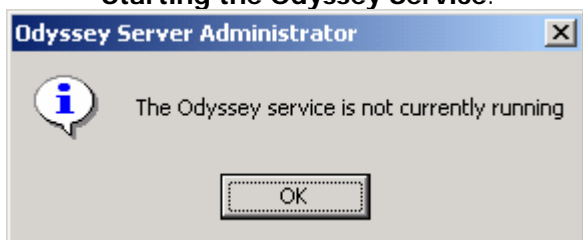


Configuring Funk Software Odyssey Server

Launch the Funk Software Odyssey Server.

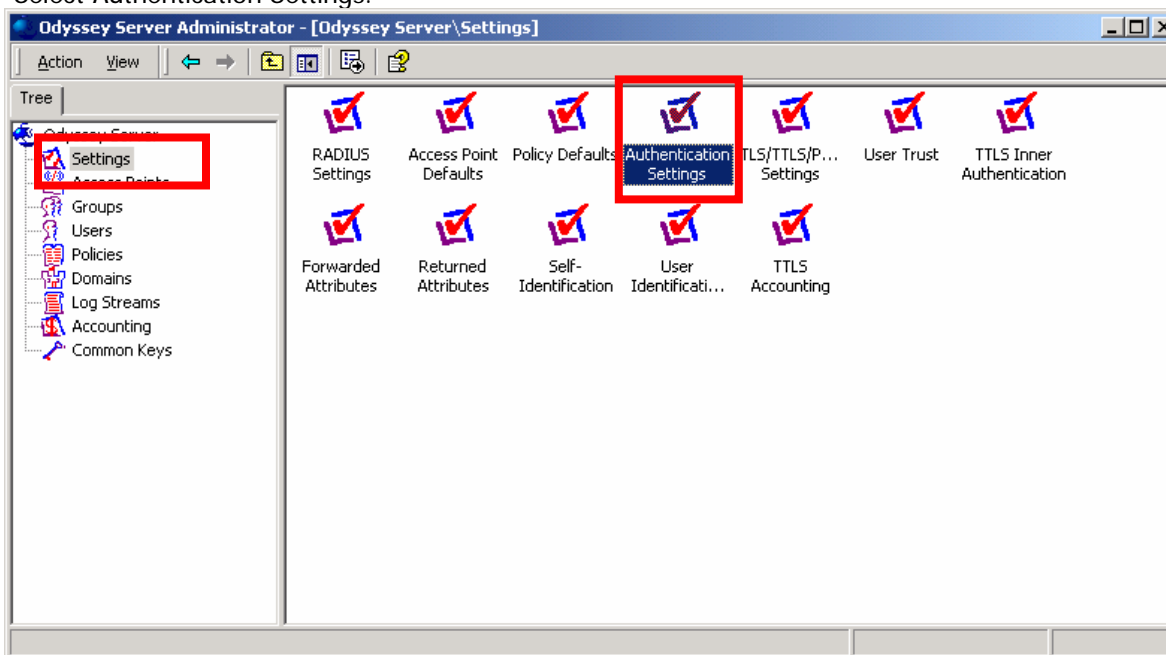
- If you see the message below when launching Odyssey Server, see **Appendix C:**

Starting the Odyssey Service.



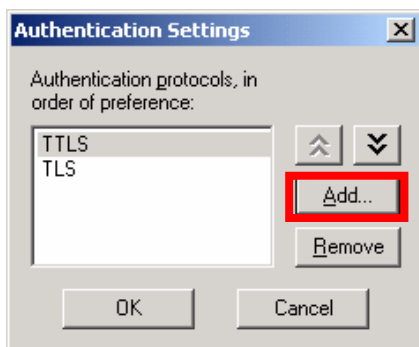
From the Odyssey Server menu on the left side, select **Settings**.

Select Authentication Settings.



This will open **Authentication Settings**.

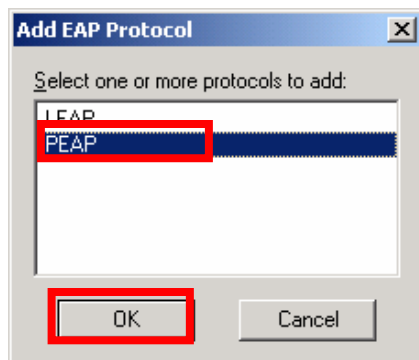
Click **Add...**



This will open **Add EAP Protocol**.

Select **PEAP**.

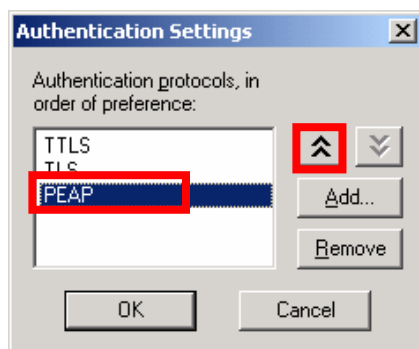
Click **OK**.



This will take you back to **Authentication Settings**.

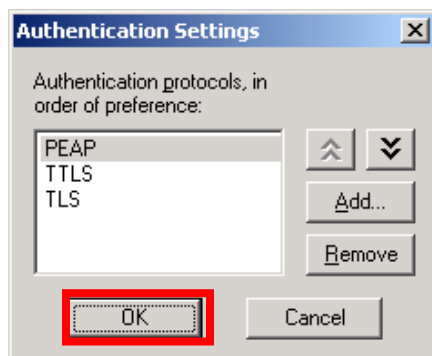
Select **PEAP**

Click the **UP arrow** twice.



This will move **PEAP** to the top of the list.

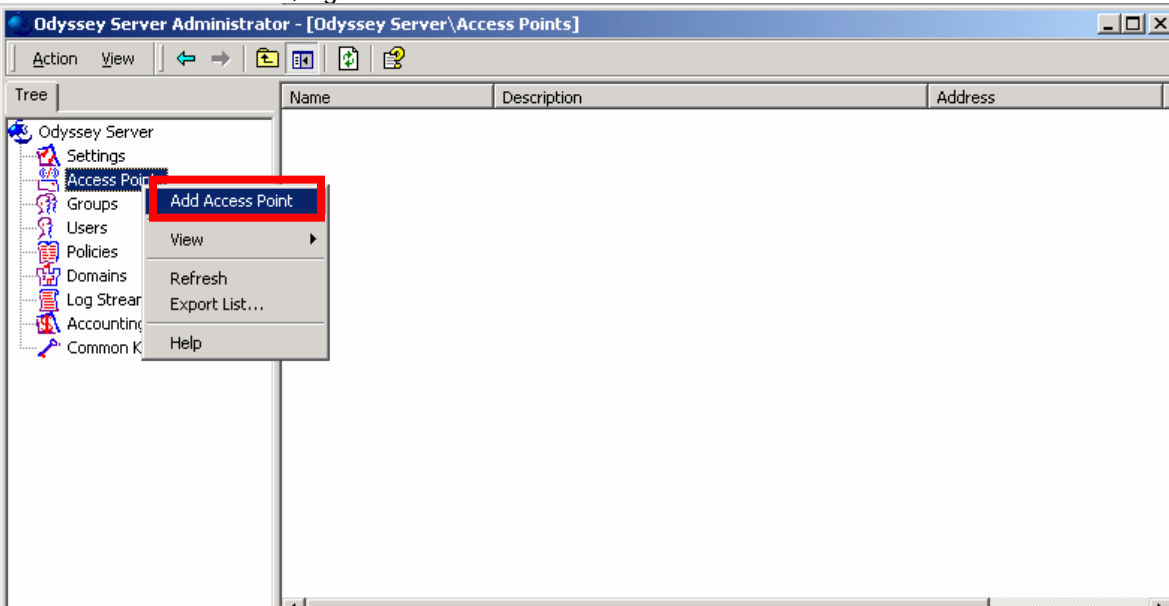
Click **OK**.





This will return you to the **Odyssey Server Administrator**.

From the left side menu, right click on **Access Points** and select **Add Access Point**.



This will open **Add Access Point**.

Enter a **Name** and **Description**.

For **Address**, enter the IP address for the IP 200 access point.

For Shared secret: click Enter.

Add Access Point

Name: My Foundry IP 200 Access Point

Description: This is my Foundry IP 200 Access Point

Address: 172 . 1 . 1 . 3 Resolve...

Model: - standard access point -

Shared secret: Enter Validate...

Address range

If you deploy multiple access points of the same model and with the same shared secret, you can configure them collectively by specifying a range of addresses here.

☐ Allow any access point in address range

Number of addresses in range: 1

Range:

OK Cancel

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

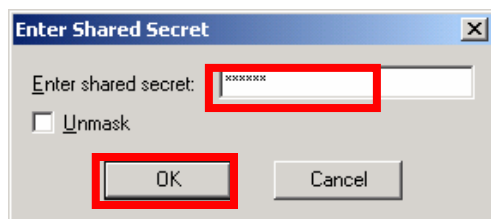
WPA – 802.1x PEAP WITH FUNK ODYSSEY



This will open Enter Shared Secret.

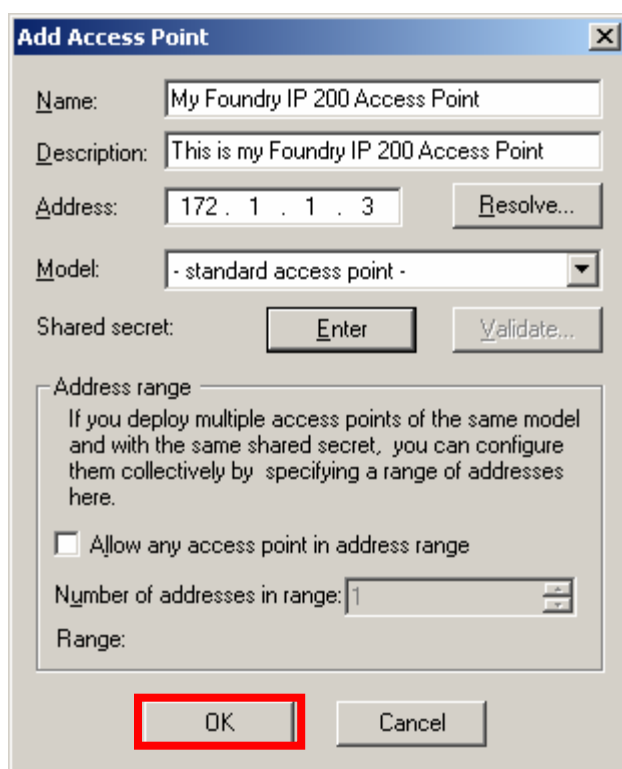
Enter the same shared secret that was configured in your IP 200.

Click **OK**.



This will return you to **Add Access Point**.

Click **OK**.

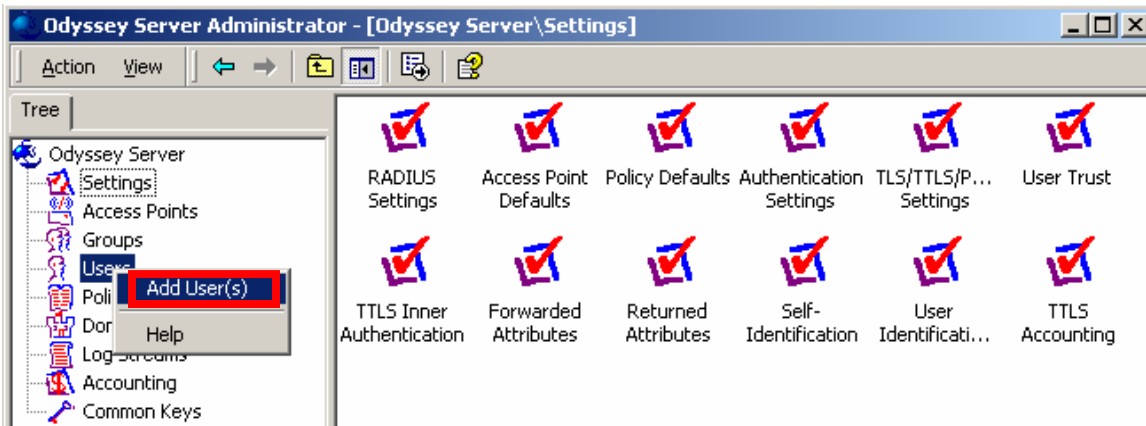


WPA – 802.1x PEAP WITH FUNK ODYSSEY



This will return you to the **Odyssey Server Administrator**.

From the left side menu, right click on **User** and select **Add User(s)**.

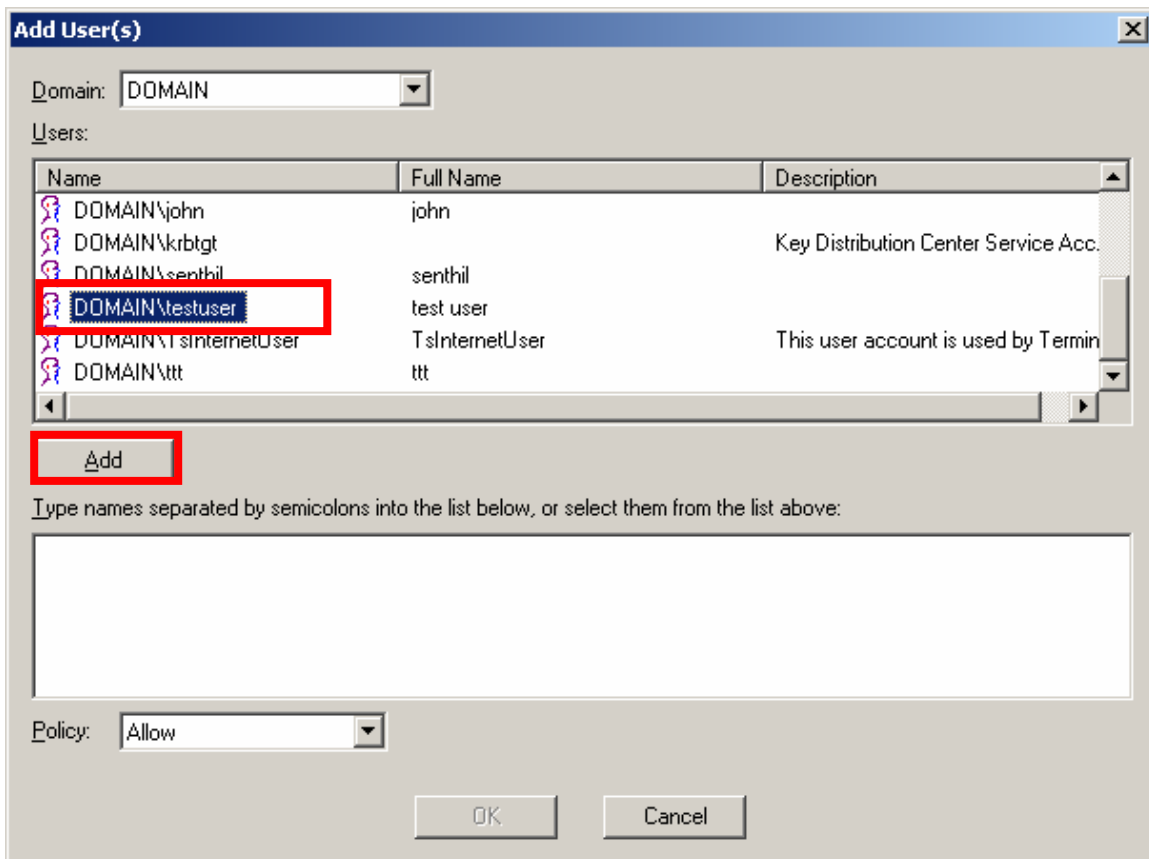


This will open **Add User(s)**.

Select a user.

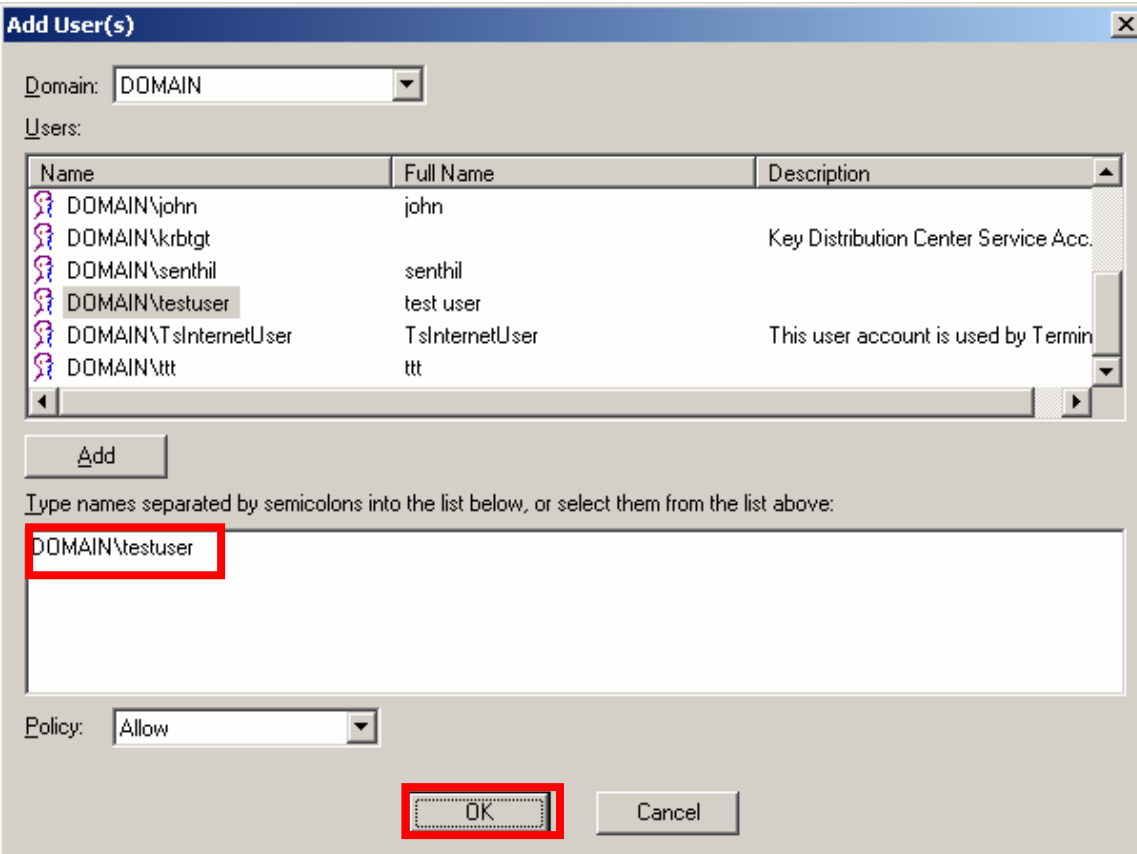
Click **Add**.

Note: Select a user with a known password. Remember the user and password. You will need them when you configure the Odyssey Client.





The selected user will appear in the list below.
Click **OK**.



The 'Add User(s)' dialog box is shown. It has a 'Domain' dropdown set to 'DOMAIN'. Below it is a 'Users' section with a table of users. The 'DOMAIN\testuser' entry is selected. Below the table is an 'Add' button. Underneath is a text box containing 'DOMAIN\testuser'. At the bottom, there is a 'Policy' dropdown set to 'Allow', and 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red box.

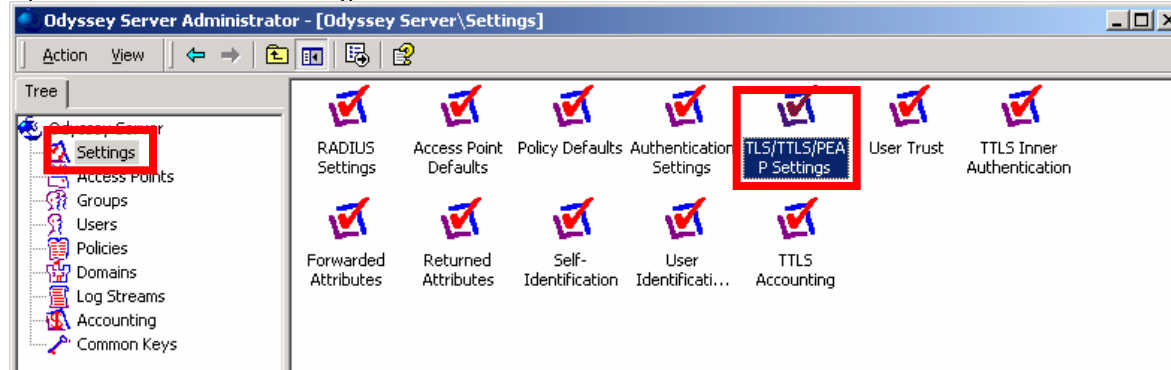
Name	Full Name	Description
DOMAIN\john	john	
DOMAIN\krbtgt		Key Distribution Center Service Acc.
DOMAIN\senthil	senthil	
DOMAIN\testuser	test user	
DOMAIN\TslnternetUser	TslnternetUser	This user account is used by Termin
DOMAIN\ttt	ttt	



Exporting the Server Certificate

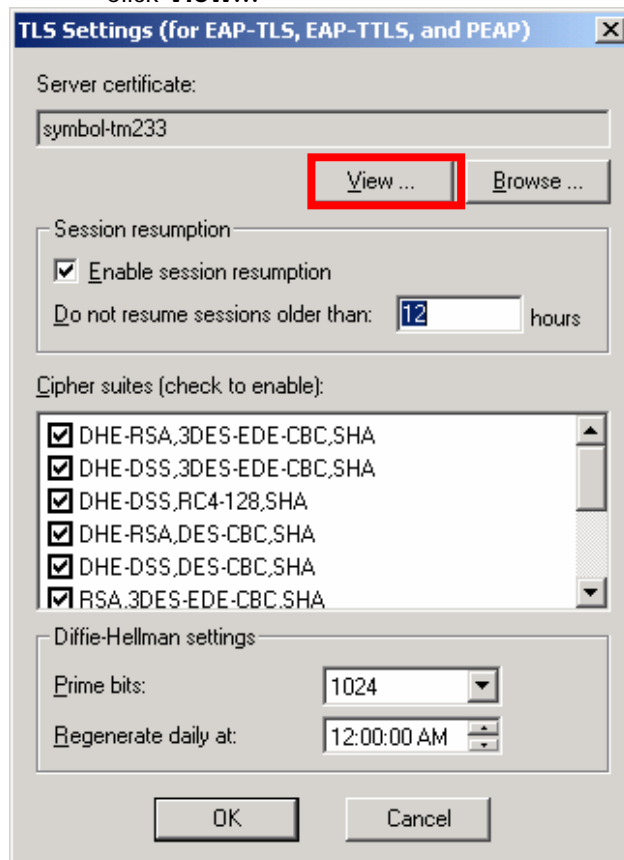
From the Odyssey Server Administrator,
 Select **Settings** from the left side menu.

Open TLS/TLS/PEAP Settings

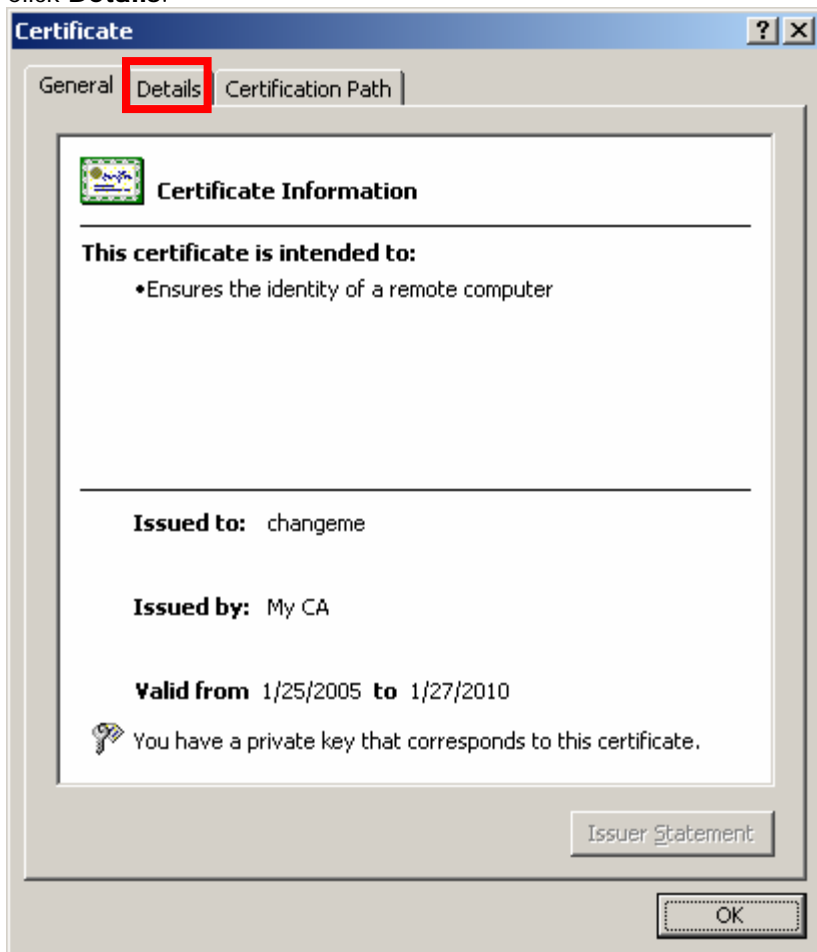


This will open TLS Settings (for EAP-TLS, EAP-TTLS, and PEAP).

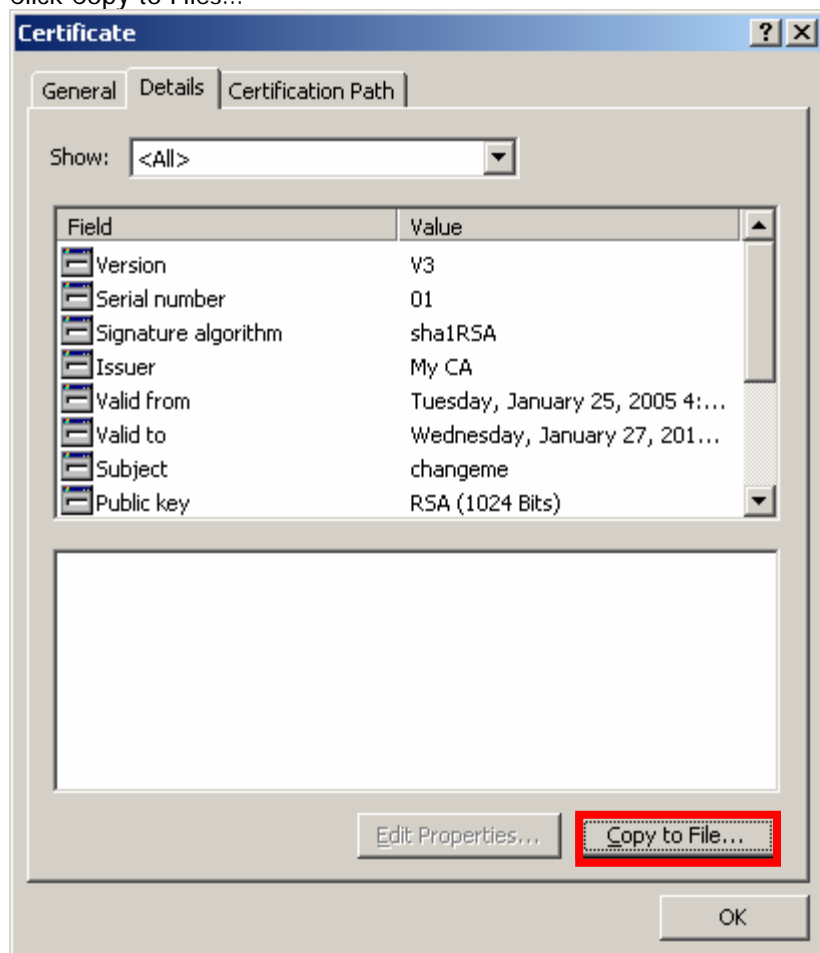
- Click **View...**



This will open the certificate.
Click **Details**.



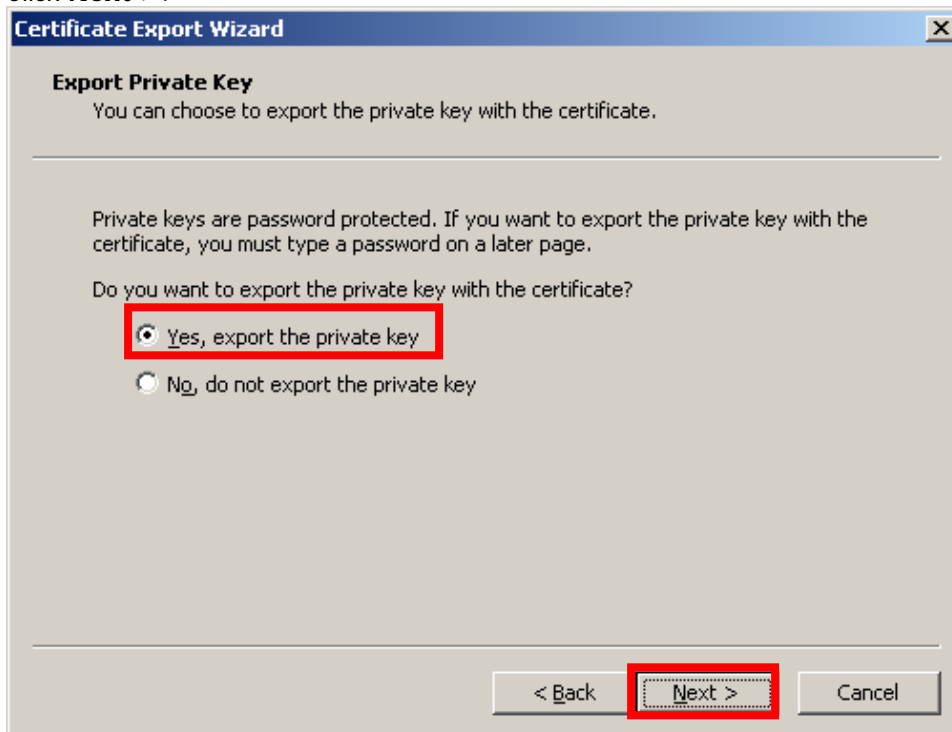
Click Copy to Files...



This will open **Welcome to the Certificate Export Wizard**.
Click **Next >**.



Select Yes, export the private key.
Click **Next >**.





Check **Include all certificates in the certification path if possible** and **Enable strong protection**.

Click **Next >**.

Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ☐ DER encoded binary X.509 (.CER)
- ☐ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - ☐ Include all certificates in the certification path if possible
- ☒ Personal Information Exchange - PKCS #12 (.PFX)
 - ☒ Include all certificates in the certification path if possible
 - ☒ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
 - ☐ Delete the private key if the export is successful

< Back **Next >** Cancel

Enter a Password: and Confirm password:.

Click **Next >**

Note: Remember this password. You will need it when you import the certificate.

Certificate Export Wizard

Password
To maintain security, you must protect the private key by using a password.

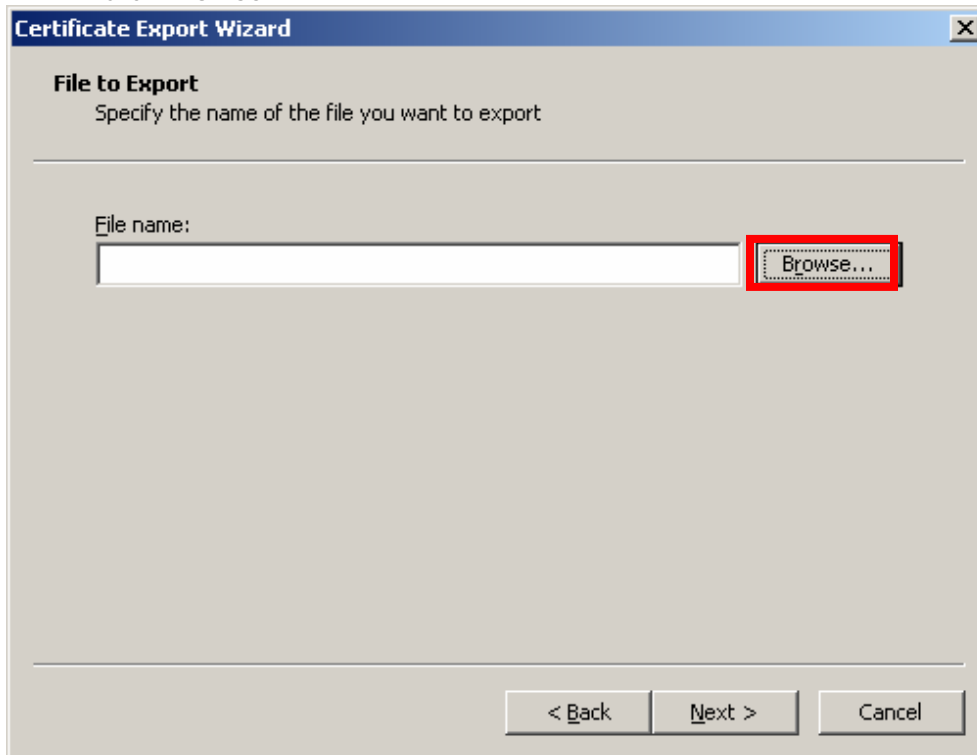
Type and confirm a password.

Password:

Confirm password:

< Back **Next >** Cancel

- Click **Browse ...**

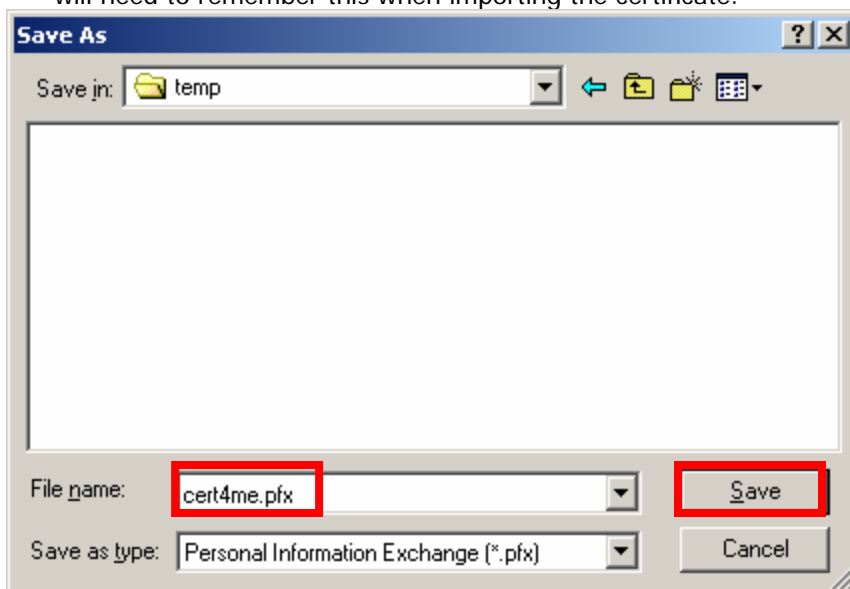


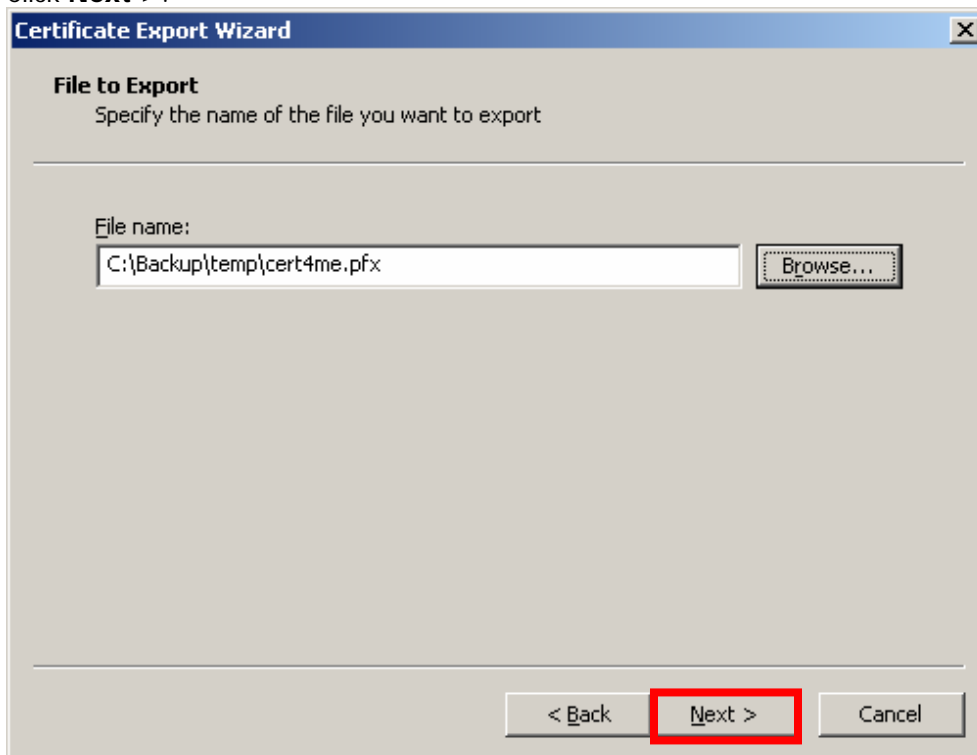
Browse to a folder to export the certificate to.

Enter a File name:.

Click **Save**.

Note: Remember the location and name of the file you are exporting the certificate to. You will need to remember this when importing the certificate.

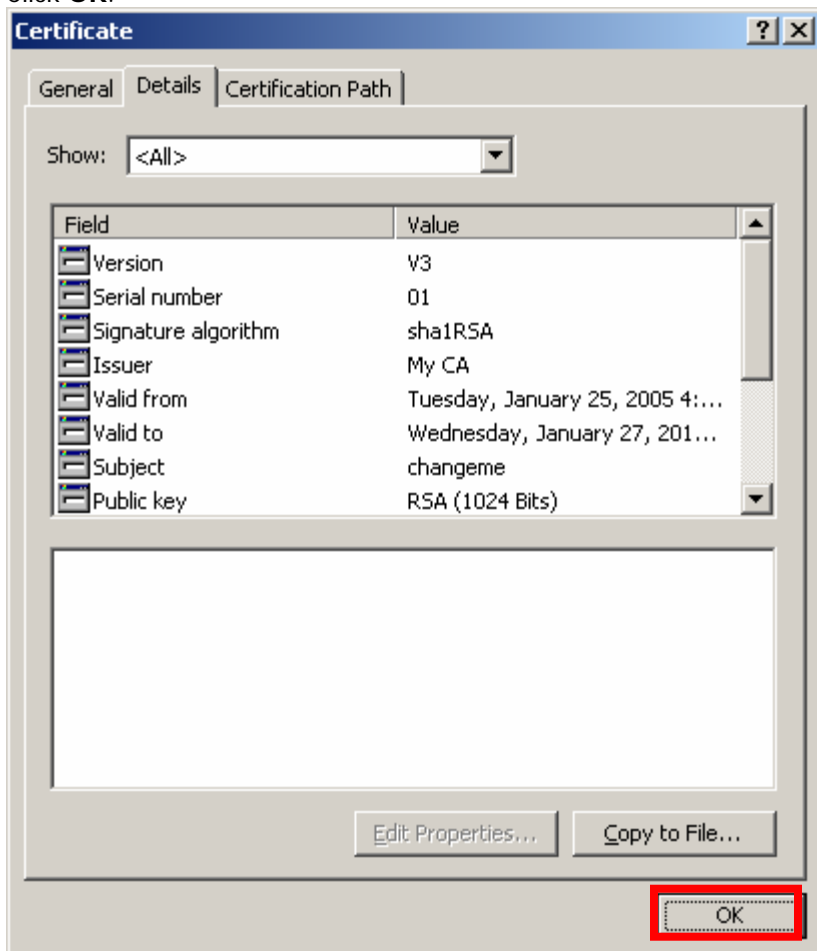


Click **Next >**.Click **Finish**.

Click **OK**.



Click **OK**.

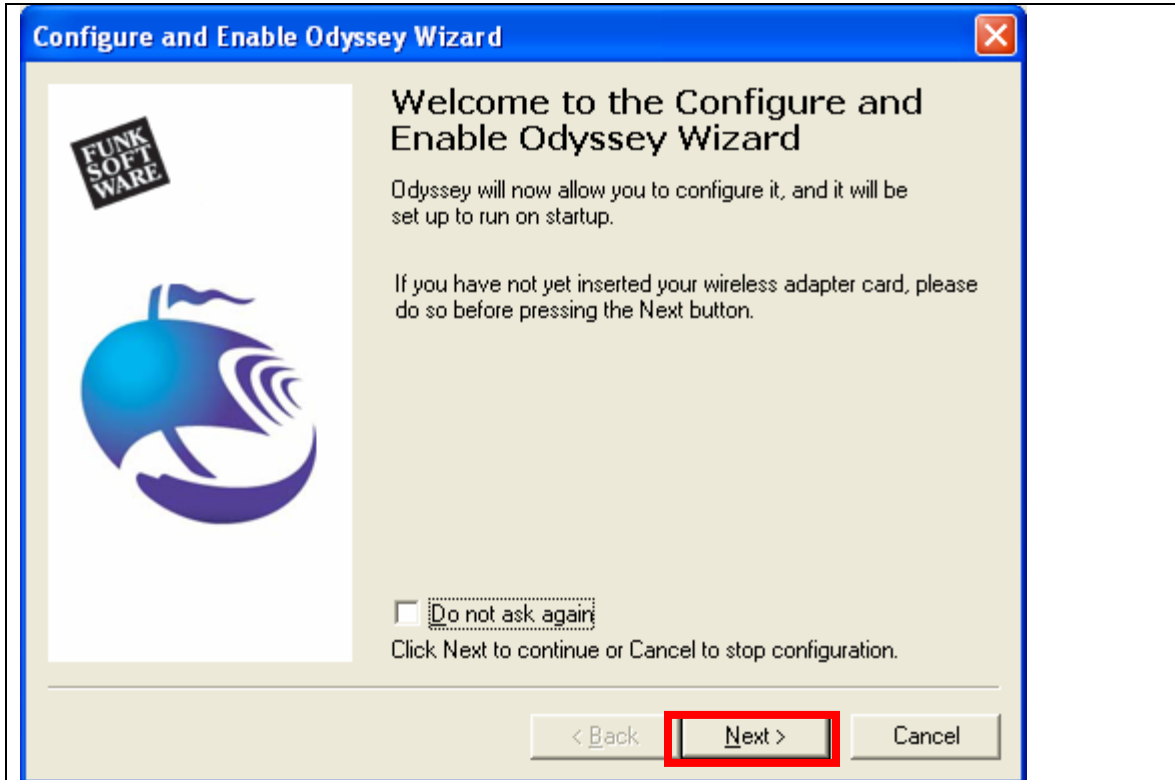




Installing Funk Software Odyssey Client

1. Copy the file Odyssey Client installation program to the computer that will run the Odyssey Client. In this installation guide, this will be the Windows XP computer with the wireless NIC. The installation program will be odc303.msi.
2. Uninstall or disable any other 802.1x supplicants or 3rd party NIC vendor utilities from the computer that will run the Odyssey Client. This includes Microsoft Windows Wireless Zero Configuration. To disable Wireless Zero Configuration on Windows XP, see the Appendix at the end of this guide.
3. Open the odc303.msi file. This will install the Odyssey Client on the computer.
4. Follow all of the instructions in the installation program. Select the default settings when provided.
5. When the installation is complete, launch the Odyssey Client. When launching the Odyssey Client, you may see the following screens:

Click **Next >**.



Click **Finish**.



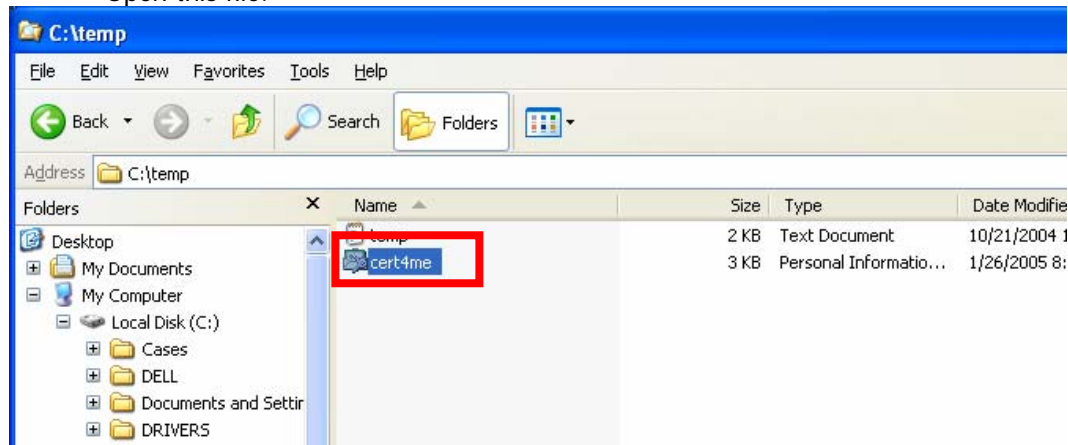


Importing the Server Certificate

This section guides you through importing the server certificate on to the computer with Odyssey Client. In this installation guide, this is the Windows XP computer.

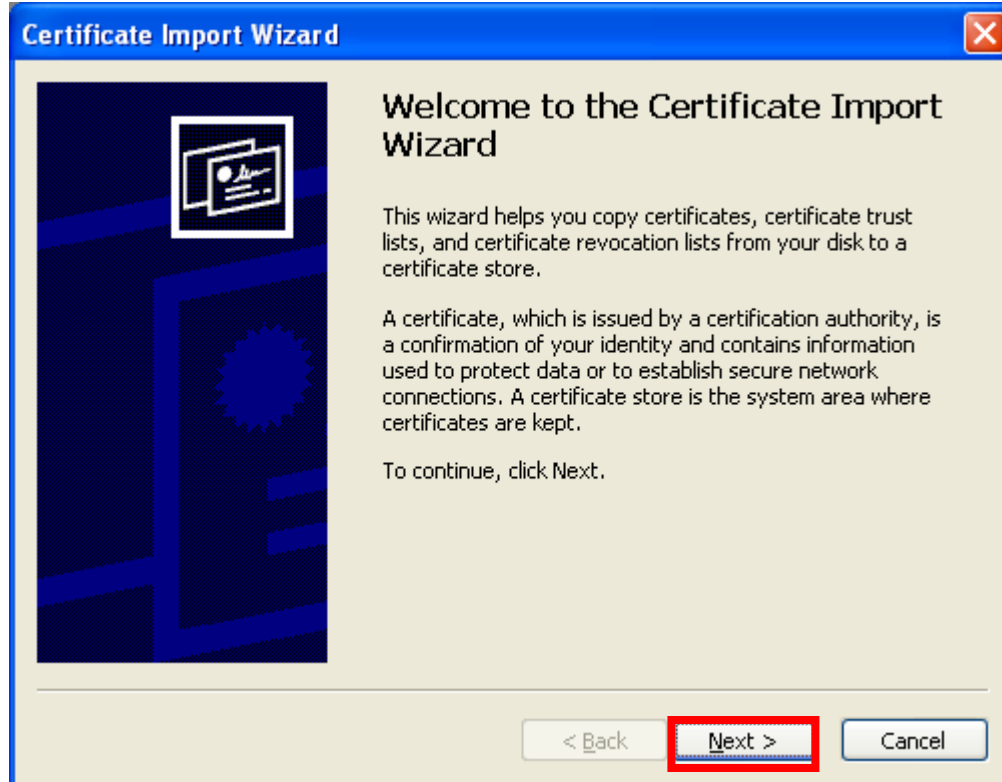
Copy the file that was exported in the previous section **Exporting the Server Certificate** to the computer with Odyssey Client. In this installation guide, this file is called cert4me.pfx and the computer is the Windows XP computer.

- Open this file.

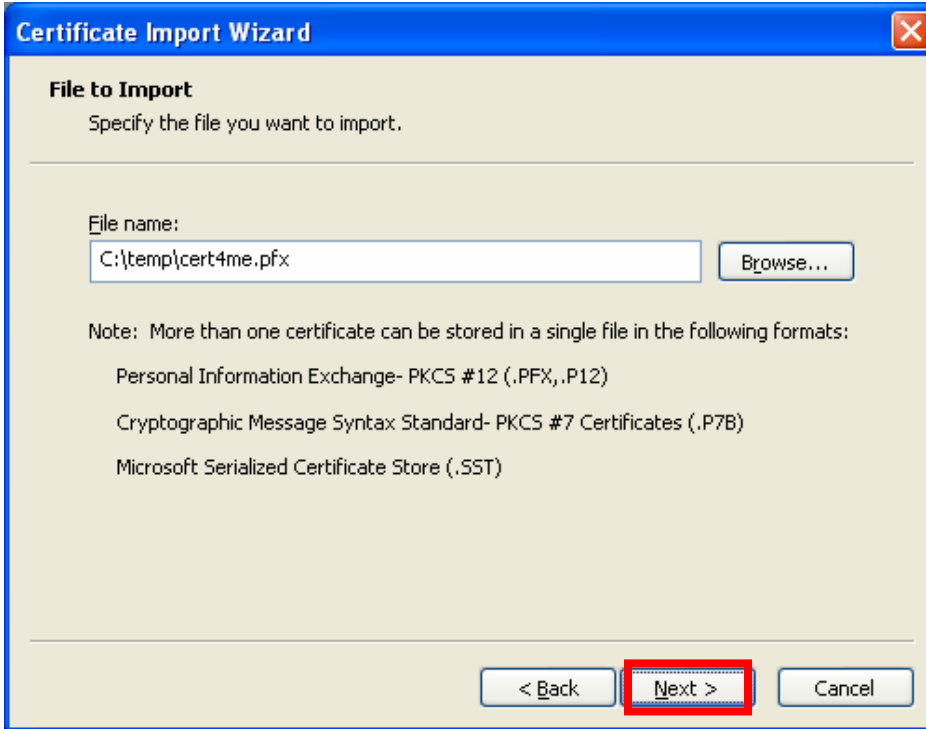


This will open the **Welcome to the Certificate Import Wizard**.

Click Next >.



Click **Next >**.



Certificate Import Wizard

File to Import
Specify the file you want to import.

File name:
C:\temp\cert4me.pfx Browse...

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

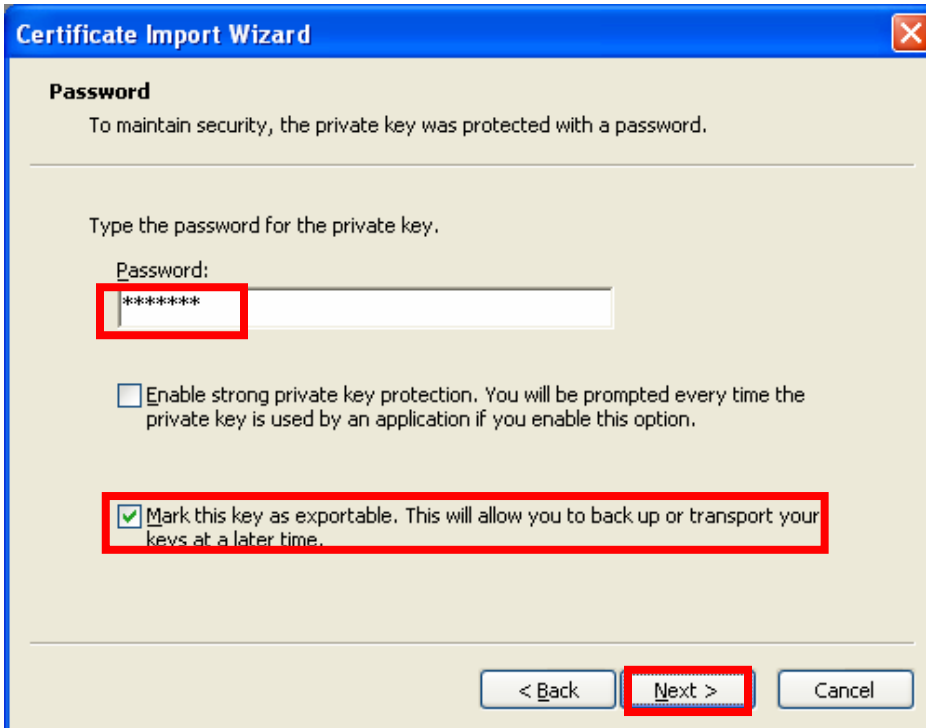
- Personal Information Exchange- PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

< Back **Next >** Cancel

Enter the password that was used when exporting this certificate.

Check Mark this key as exportable.

Click Next >.



Certificate Import Wizard

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

Type the password for the private key.

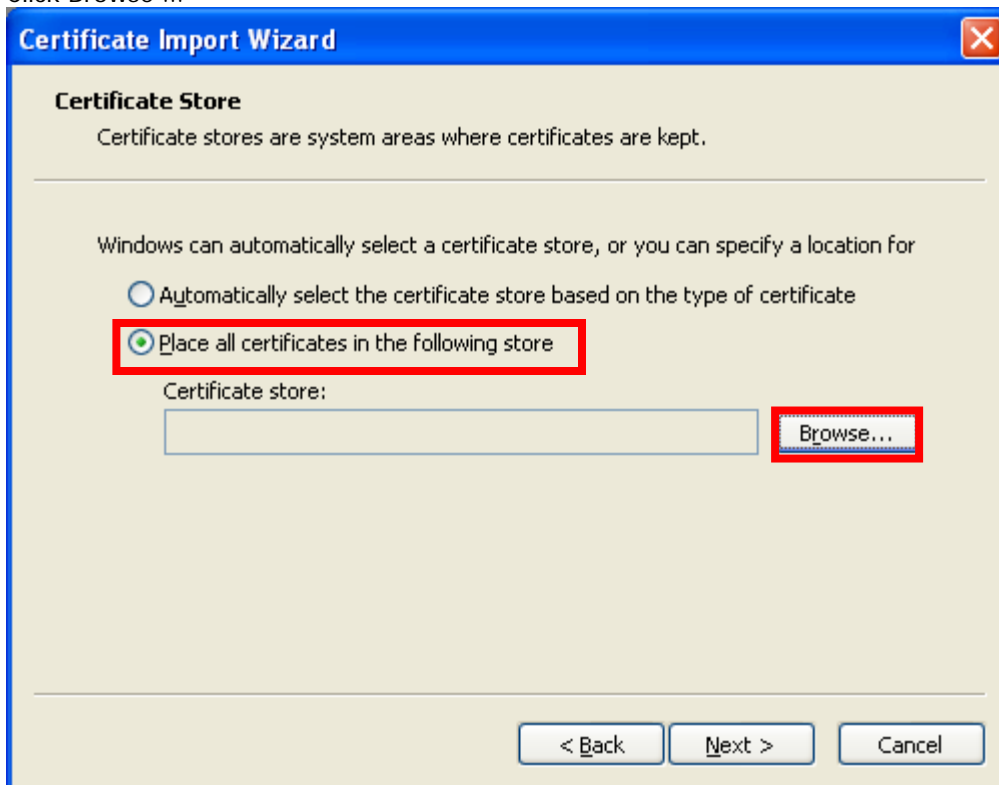
Password:

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

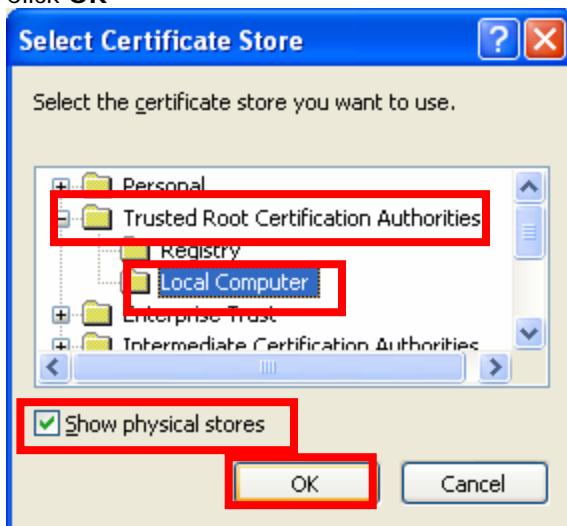
☒ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

< Back **Next >** Cancel

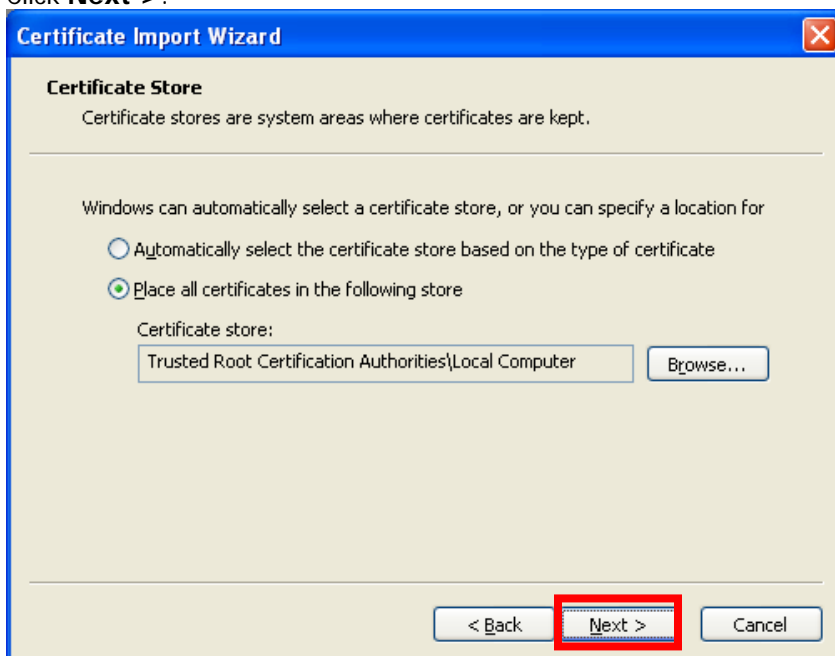
Select Place all certificates in the following store.
Click Browse ...



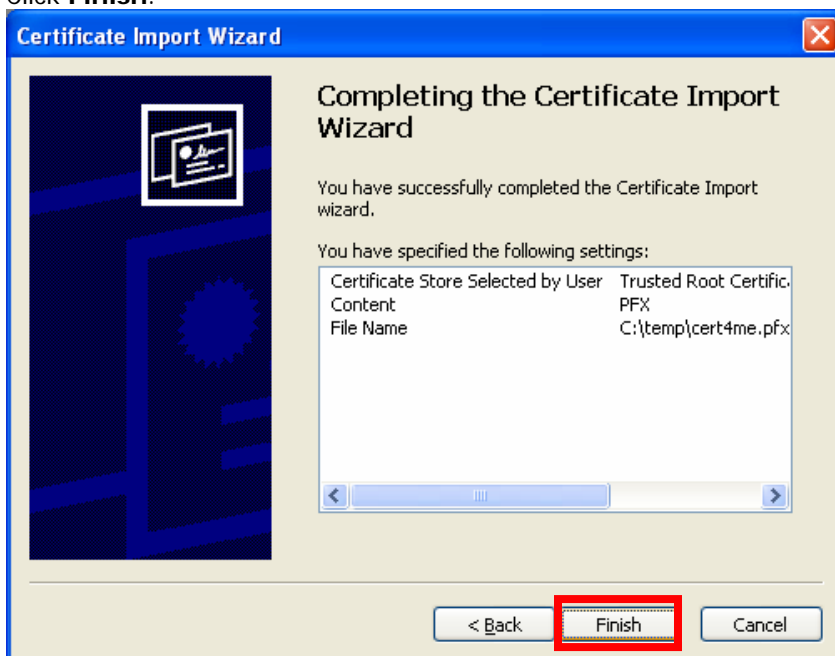
Check Show physical stores
Select Trusted Root Certification Authorities
Select Local Computer
Click OK



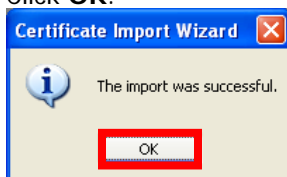
Click **Next** >.



Click **Finish**.



Click **OK**.

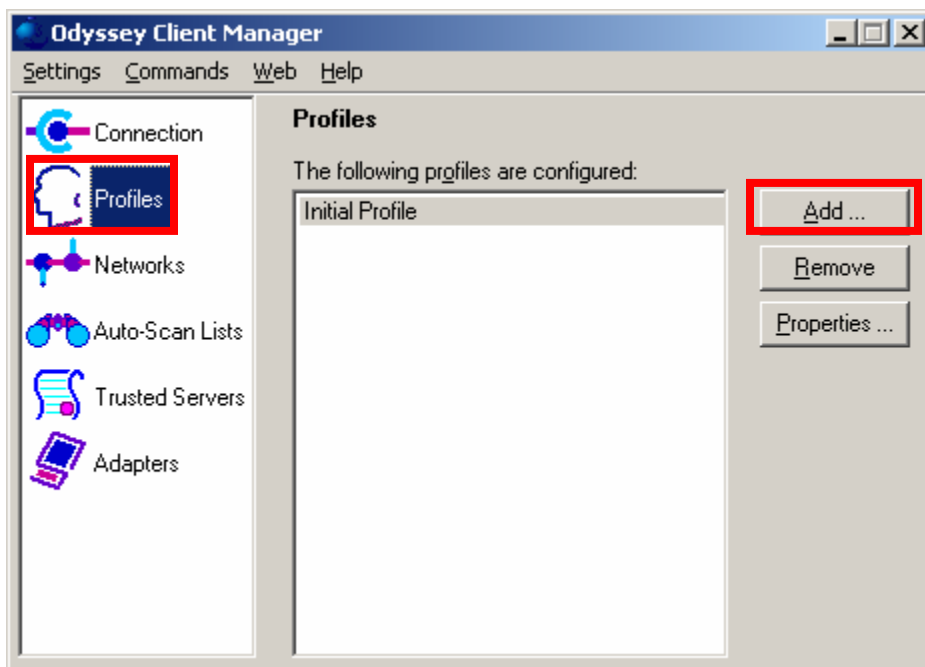


Configuring Funk Software Odyssey Client

Open the Odyssey Client Manager.

Select **Profiles**.

Click **Add ...**.



WPA – 802.1x PEAP WITH FUNK ODYSSEY



This will open **Add Profile**.

Enter a Profile name.

Select User Info

Enter a **Login name**. The **Login name** must match the user that was configured in the Odyssey Server configuration for users.

Select prompt for password.

Profile Properties

Profile name: testuser

User Info | Authentication | ITLS Settings | PEAP Settings

Login name: testuser

Password

☒ Permit login using password

☐ use Windows password

☒ prompt for password

☐ use the following password:

☐ Unmask

Certificate

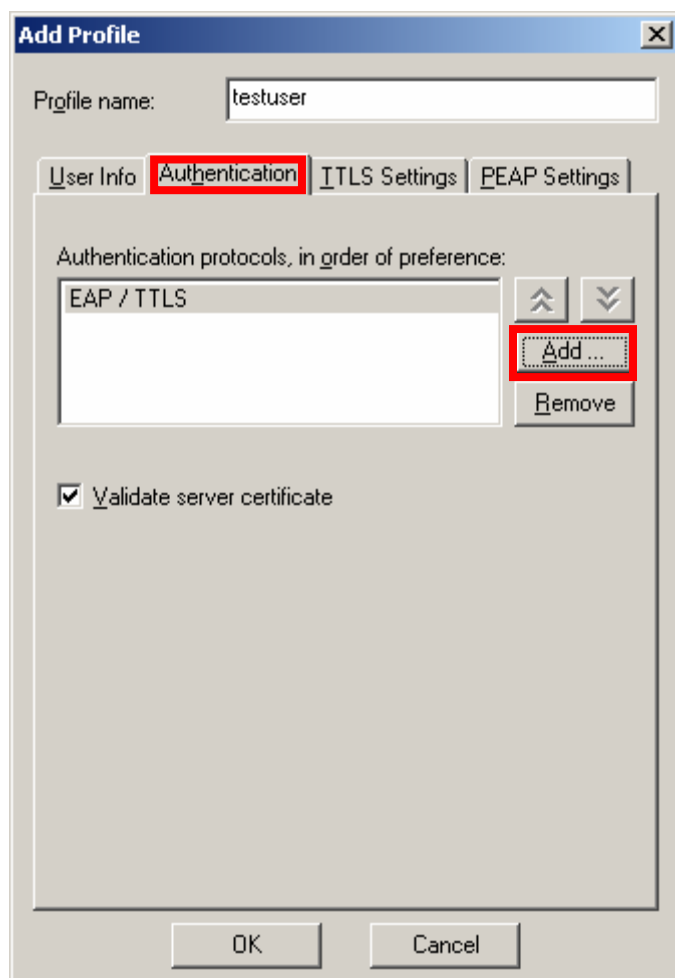
☐ Permit login using my certificate:

View ... Browse ...

OK Cancel

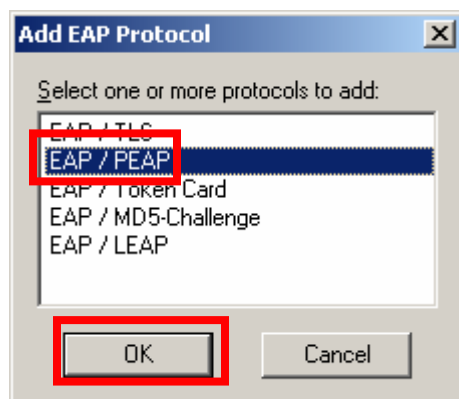
Select Authentication

Click **Add ...**



Select **EAP/PEAP**.

Click **OK**.



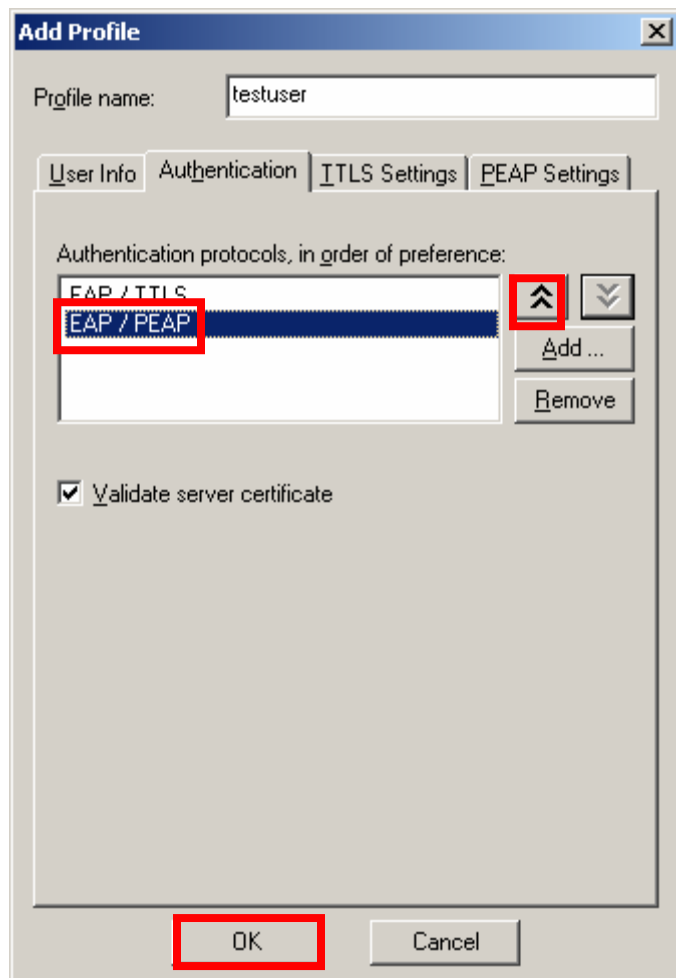
WPA – 802.1x PEAP WITH FUNK ODYSSEY



Select **EAP/PEAP**.

Click the **double up arrow**. This will move EAP/PEAP to the top of the Authentication protocols list.

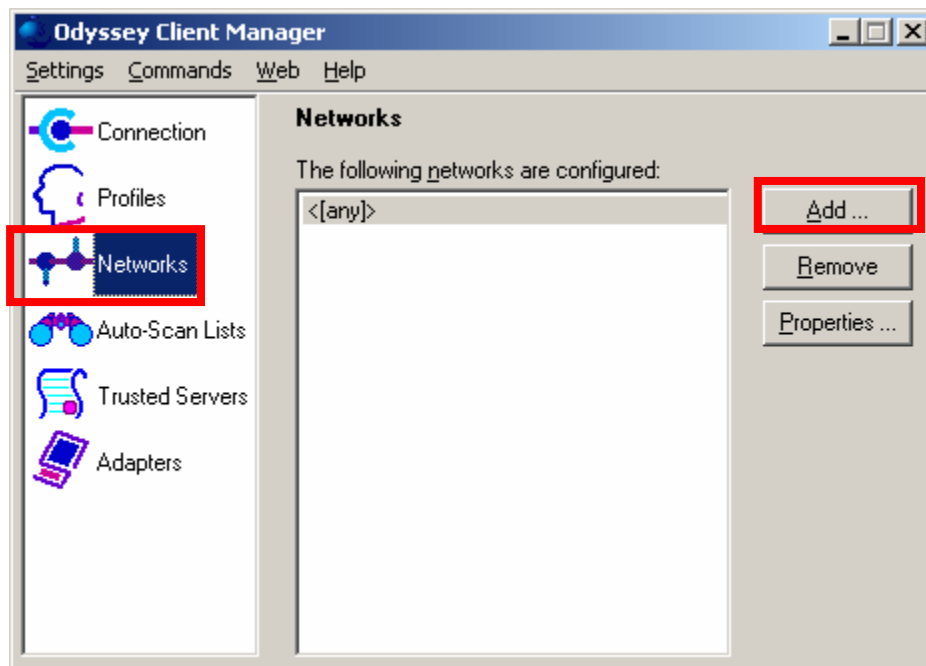
Click **OK**.



WPA – 802.1x PEAP WITH FUNK ODYSSEY

Select **Networks**.

Click **Add ...**.



WPA – 802.1x PEAP WITH FUNK ODYSSEY



This will open **Add Network**.

Enter My SSID for Network name (SSID).

For Association mode: select WPA

For Encryption method: select TKIP

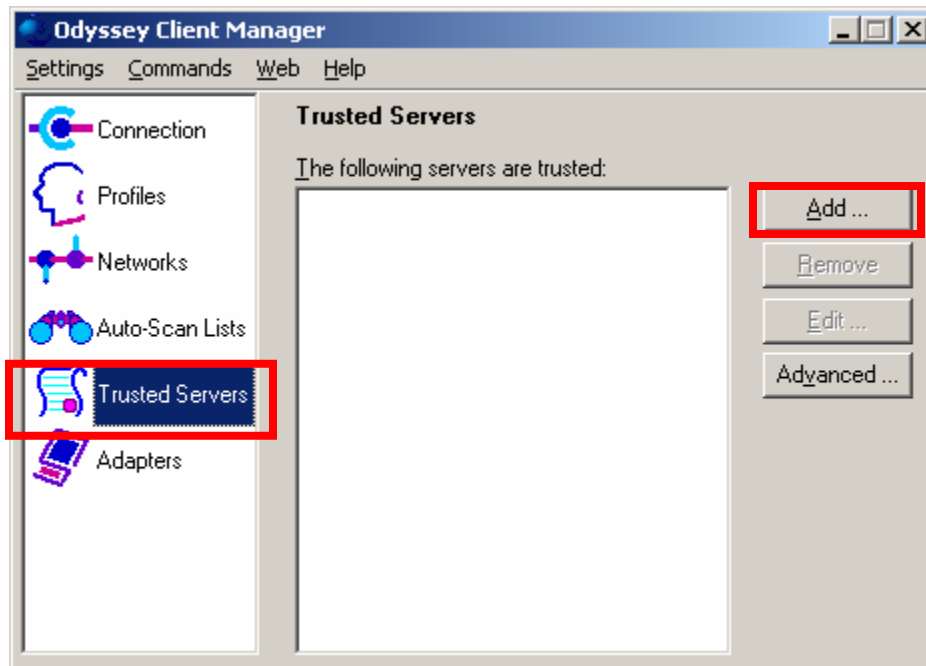
Check **Authenticate user profile**: and select the profile you just created in the previous step

Check Keys will be generated automatically for data privacy

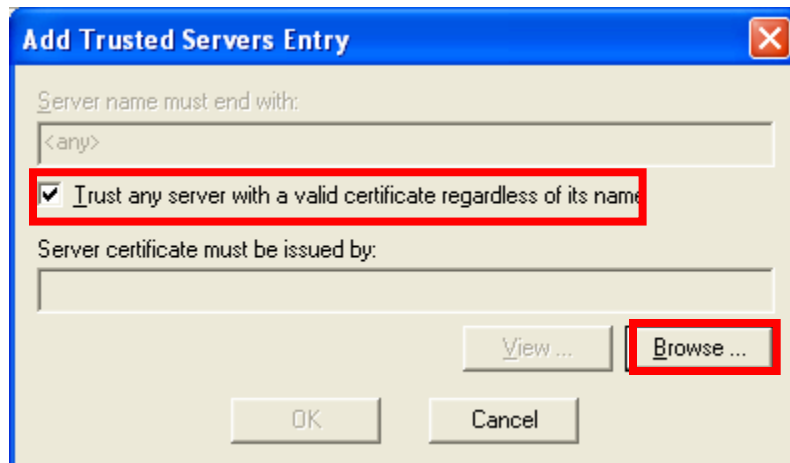
Click **OK**

The screenshot shows the 'Add Network' dialog box. The 'Network' section contains the following fields: 'Network name (SSID)' with the value 'My SSID', 'Connect to any available network' (unchecked), 'Description (optional)' (empty), 'Network type' (Access point (infrastructure mode)), 'Channel' (default channel), 'Association mode' (WPA), and 'Encryption method' (TKIP). The 'Authentication' section contains 'Authenticate using profile' (checked, with 'testuser' selected) and 'Keys will be generated automatically for data privacy' (checked). The 'Pre-shared key (WPA)' section contains 'Passphrase' (empty) and 'Unmask' (unchecked). The 'OK' button is highlighted with a red box.

Select Trusted Servers
Click **Add ...**



Check Trust any server with a valid certificate regardless of its name.
Click Browse ...

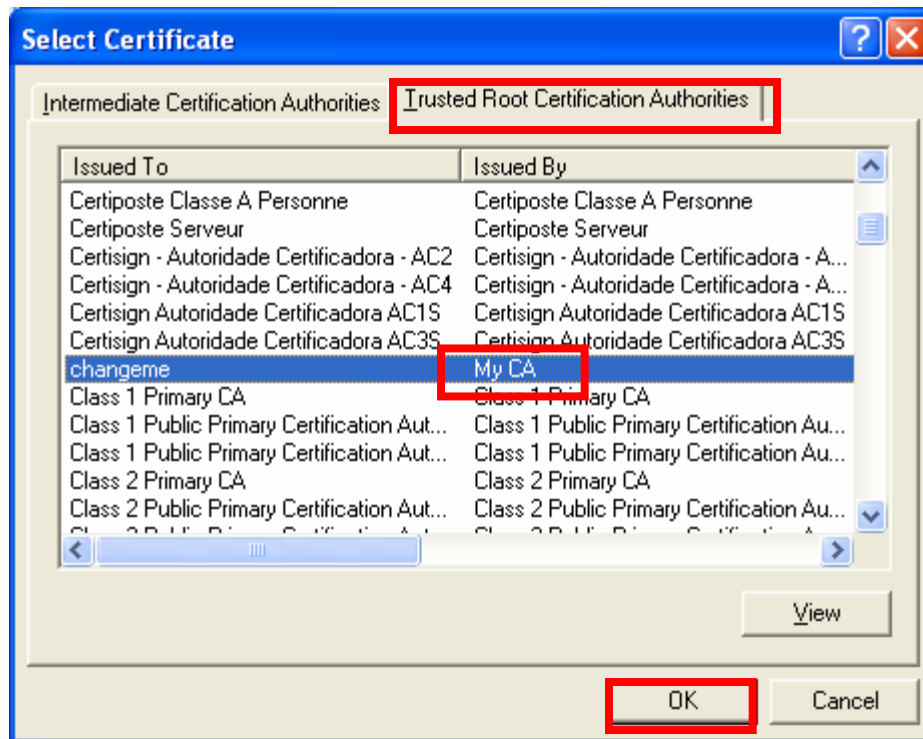


WPA – 802.1x PEAP WITH FUNK ODYSSEY

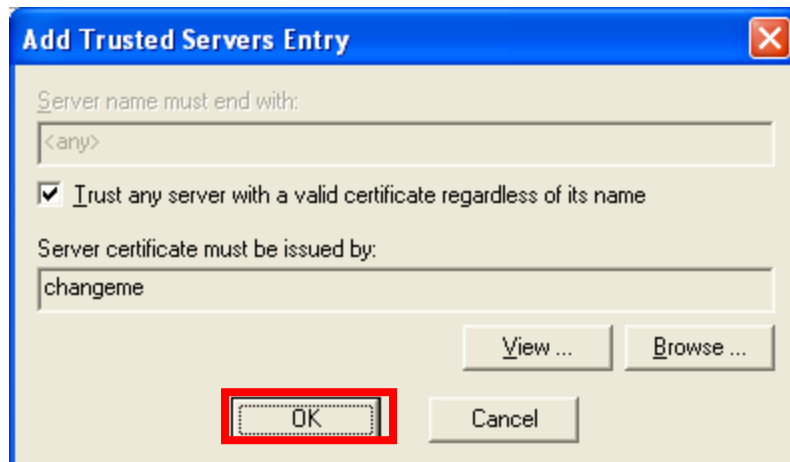
Select Trusted Root Certification Authorities

Select the certificate issued by **My CA**

Click **OK**



Click **OK**



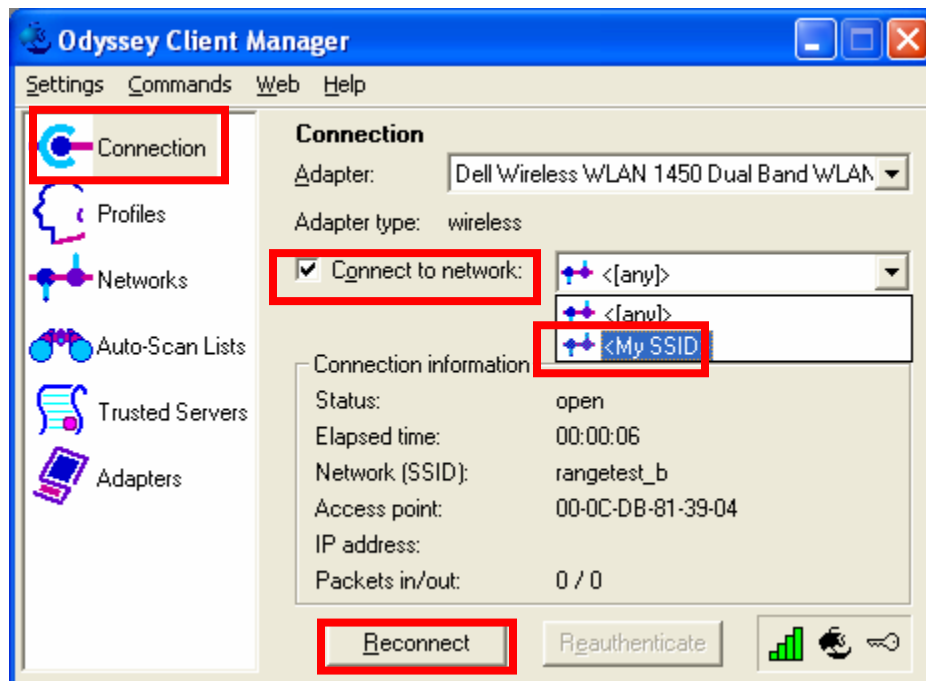
WPA – 802.1x PEAP WITH FUNK ODYSSEY

Select Connection.

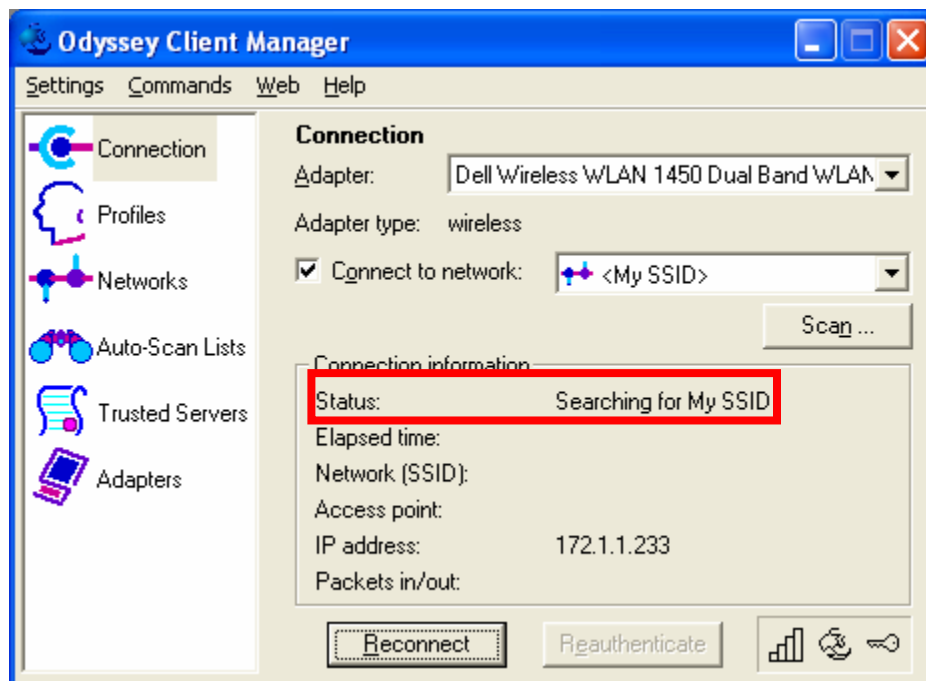
Check Connect to network:

From the pull down menu, select <My SSID>

Click Reconnect



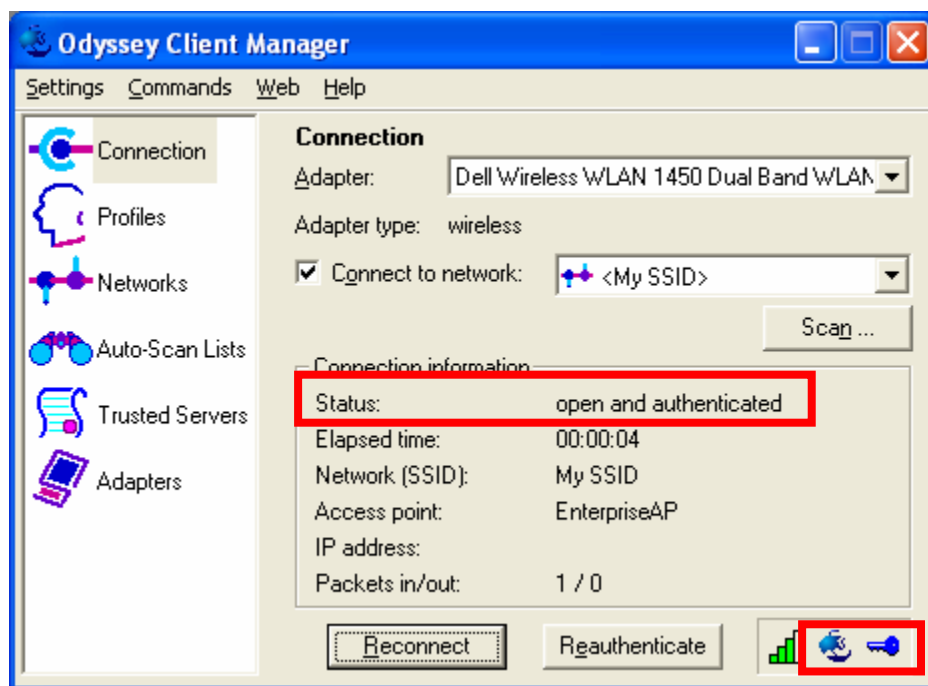
Status will display the connection status.



WPA – 802.1x PEAP WITH FUNK ODYSSEY



The Odyssey Client is successfully connected when the **Status** is **open and authenticated**.
The **Odyssey ship** and **key** icon will be colored **blue** when successfully connected.





Appendix A: Configuring IP 200 – Non-Virtual AP Versions

This Appendix is for IP 200 firmware versions that do not support Virtual AP (01.3.00, 01.2.x and older).

This installation guide includes configuration of the IP 200 from the CLI and the Web Interface. If you prefer configuring the IP 200 from the Web Interface, you can skip the next section **Configuring from the CLI** and go to the following section **Configuring from the Web Interface**.

Configuring from the CLI

From the CLI, go to the configure context. Enter the following commands:

```
Foundry AP(config)#radius-server address x.x.x.x
Foundry AP(config)#radius-server key *****
Foundry AP(config)#802.1x required
```

Where:

x.x.x.x is the IP address of the computer that will have Odyssey Server installed on it. In this installation guide, this is the Windows 2000 computer.

********* is a Secret key. This Secret key can be any length and use any character.

Note: You will need to remember this Secret key when you configure the Odyssey Server.

Next, go to the context for VAP 0 on any one of the wireless interfaces. This installation guide will use the 802.11g wireless interface. Enter the following commands:

```
Foundry AP(if-wireless)#ssid My SSID
Foundry AP(if-wireless)#encryption 128
Foundry AP(if-wireless)#wpa-clients Required
Foundry AP(if-wireless)#wpa-mode Dynamic
Foundry AP(if-wireless)#multicast-cipher TKIP
Foundry AP(if-wireless)#no shutdown
```




Configuring from the Web Interface

If you have configured the IP 200 using the previous section **Configuring from the CLI**, you do not need to configure the IP 200 using the Web Interface.

From the Web Interface, go to the **RADIUS** webpage.

For the **IP Address** of the **Primary Radius Server Setup**, enter the IP address of the computer that will have Odyssey Server installed on it. In this installation guide, this is the Windows 2000 computer.

Enter a **Secret Key**. This Secret Key can be any length and use any character.

Note: You will need to remember this Secret Key when you configure the Odyssey Server.

Click **Apply**.

The screenshot displays the Foundry Networks IronPoint 200 web interface. On the left is a navigation sidebar with a tree view containing categories like System, SNMP, Radio Interface, and Status, with 'RADIUS' selected under System. The main content area is titled 'Radius' and contains two sections: 'Primary Radius Server Setup' and 'Secondary Radius Server Setup'. Each section has a form with the following fields: IP Address, Port, Secret Key, Timeout (seconds), and Retransmit attempts. In the Primary setup, the IP Address is 172.1.1.1, Port is 1812, Secret Key is masked, Timeout is 5, and Retransmit attempts is 3. In the Secondary setup, the IP Address is 0.0.0.0, Port is 1812, Secret Key is masked, Timeout is 5, and Retransmit attempts is 3. At the bottom right of the form area, there are three buttons: 'Apply', 'Cancel', and 'Help', with 'Apply' being the active button.

Go to the **Authentication** webpage.

For 802.1x Setup: select Required.

Click **Apply**.



FOUNDRY NETWORKS *IronPoint™ 200* [Logout](#)

System

- Identification
- TCP/IP
- RADIUS
- Management Tunnel
- Authentication**
- Bridging
- Administration
- Syslog & Time
- VLAN

SNMP

- SNMP General
- SNMP Trap Filters
- SNMP Targets

Radio Interface 802.11a

- Radio Settings
- Security

Radio Interface 802.11g

- Radio Settings
- Security

Status

- AP Status
- Stations
- Event Log

Authentication

802.1x Setup :

☐ Disable 802.1x authentications not allowed
☐ Supported Clients may or may not use 802.1x
☒ **Required Client must use 802.1x**

If 802.1x supported or required is selected, then Radius setup must be completed

Broadcast Key Refresh Rate minutes (0 = Disabled)

Session Key Refresh Rate minutes (0 = Disabled)

802.1x Authentication Refresh Rate minutes (0 = Disabled)

802.1x Supplicant:

Supplicant ☒ Enable

Local MAC Selection:

MAC Authentication :

Local MAC Authentication :

System Default ☐ Deny ☒ Allow

MAC Authentication Settings :

MAC Address	Permission	Update
<input type="text"/>	<input type="radio"/> Deny <input checked="" type="radio"/> Allow <input type="radio"/> Delete	<input type="button" value="Update"/>

MAC Authentication Table :

MAC Address	Permission
-------------	------------

WPA – 802.1x PEAP WITH FUNK ODYSSEY

**FOUNDRY**[®]
NETWORKS

Go to the **Security** webpage for any one of the Radio Interfaces. This guide configures **Security** for **Radio Interface 802.11g**. (See the screen image on the next page)

For Data Encryption Setup, select Enable.

Enable Allow WPA Clients Only.

For WPA Key Management, select WPA authentication over 802.1x.

For Multicast Cipher Mode select TKIP.

Click **Apply**.



System

- Identification
- TCP/IP
- RADIUS
- Management Tunnel
- Authentication
- Bridging
- Administration
- Syslog & Time
- VLAN

SNMP

- SNMP General
- SNMP Trap Filters
- SNMP Targets

Radio Interface 802.11a

- Radio Settings
- Security

Radio Interface 802.11g

- Radio Settings
- Security**

Status

- AP Status
- Stations
- Event Log

802.11g:

Security

WEP

Authentication Type Setup

☒ Open System Allow everyone to access

☐ Shared Key Allow users with a correct key to access

Data Encryption Setup

☐ Disable ☒ Enable

Shared Key Setup ☐ 64 Bit ☐ 128 Bit

Key Type ☒ Hexadecimal For 64 Bit enter 10 digits, for 128 Bit enter 26 digits

☐ Alphanumeric For 64 Bit enter 5 characters, for 128 Bit enter 13 characters

Key Number	Transmit Key Select	Key
Key 1	<input checked="" type="radio"/>	
Key 2	<input type="radio"/>	
Key 3	<input type="radio"/>	
Key 4	<input type="radio"/>	

WPA

WPA Configuration Mode

☒ Allow WPA Clients Only

WPA Key Management

☒ WPA authentication over 802.1x

☐ WPA Pre-shared Key

Multicast Cipher Mode

☐ WEP Use WEP as WPA Multicast cipher mode

☒ TKIP Use TKIP as WPA Multicast cipher mode

☐ AES Use AES as WPA Multicast cipher mode

WPA Pre-Shared Key Type ☒ Hexadecimal Enter 64 digits

☐ Alphanumeric Enter between 8 and 63 characters

WPA Pre-Shared Key

Apply **Cancel** **Help**

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

WPA – 802.1x PEAP WITH FUNK ODYSSEY

**FOUNDRY**
NETWORKS

Go to the **Radio Settings** webpage for the same radio interface that you have just configured the Security for. This installation guide configures the **802.11g Radio Settings**.

Check **Enable**

Enter **My SSID** for the **SSID**.

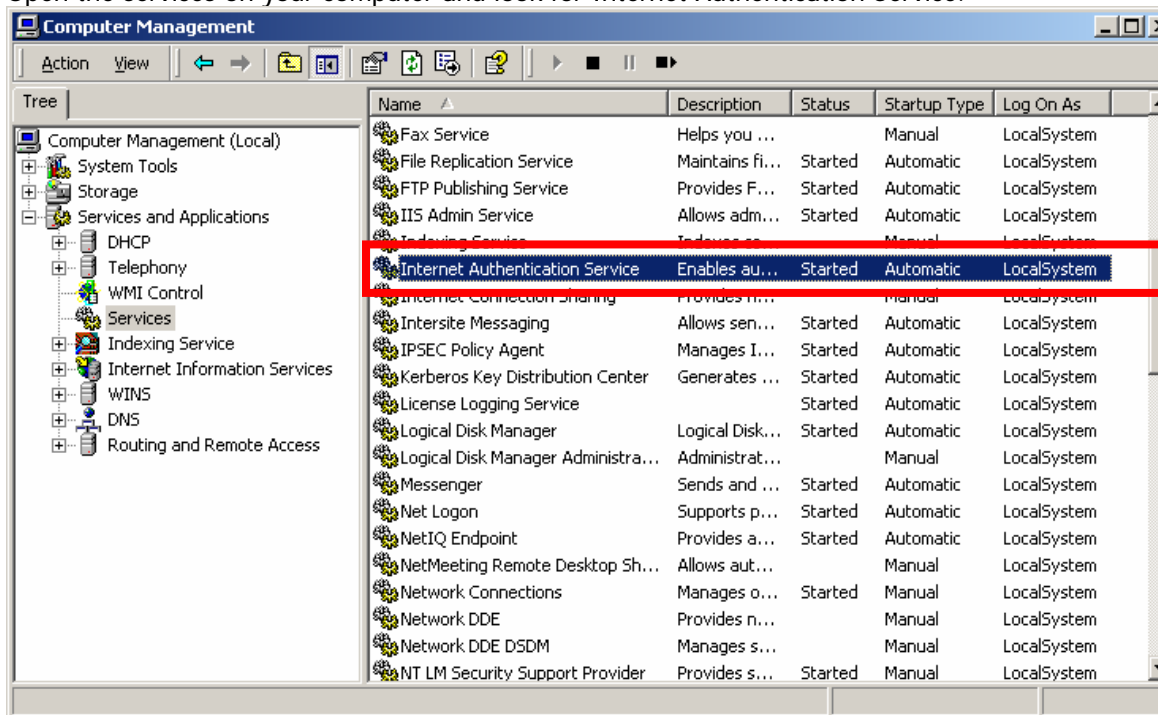
Click **Apply**.

The screenshot shows the Foundry Networks IronPoint 200 web interface. The left sidebar contains a navigation menu with the following items: System (Identification, TCP/IP, RADIUS, Management Tunnel, Authentication, Bridging, Administration, Syslog & Time, VLAN), SNMP (SNMP General, SNMP Trap Filters, SNMP Targets), Radio Interface 802.11a (Radio Settings, Security), Radio Interface 802.11g (Radio Settings, Security), and Status (AP Status, Stations, Event Log). The 'Radio Settings' link under 'Radio Interface 802.11g' is highlighted with a red box. The main content area is titled '802.11g: Radio Settings'. It includes a note: 'Before enabling the radios you must set the country selection via the CLI.' Below this, the 'Enable' checkbox is checked and highlighted with a red box. The 'SSID' field is set to 'My SSID' and is also highlighted with a red box. Other settings include: Antenna Mode (Fixed), Radio Mode (802.11b+g), Radio Channel (11), Auto Channel Select (Disable/Enable), Transmit Power (100%), Maximum Station Data Rate (54 Mbps), Beacon Interval (20-1000) (100 TUs), Data Beacon Rate (DTIM) (1-255) (2 Beacons), RTS Threshold (0-2347) (2347 Bytes), Maximum Associated Clients (0-64) (64 Clients), Native VLAN ID (1), and Hidden SSID (Disable/Enable). The 'Apply' button at the bottom right is highlighted with a red box.

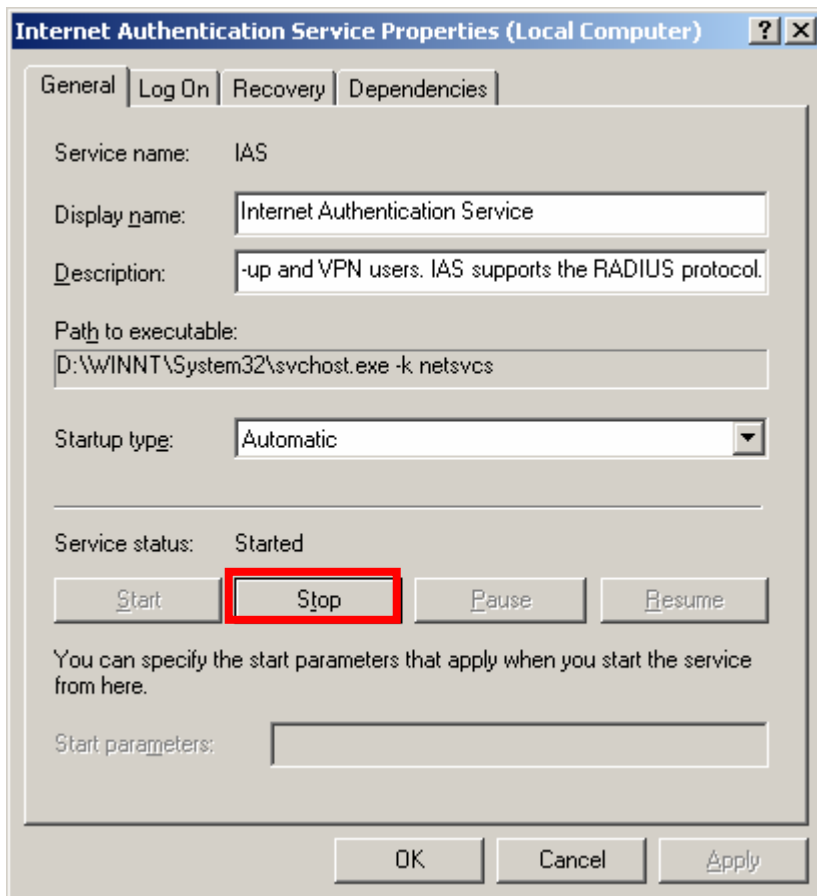


Appendix B: Disabling IAS on Microsoft Windows Server

Open the services on your computer and look for Internet Authentication Service.



Open Internet Authentication Service and Stop the service.

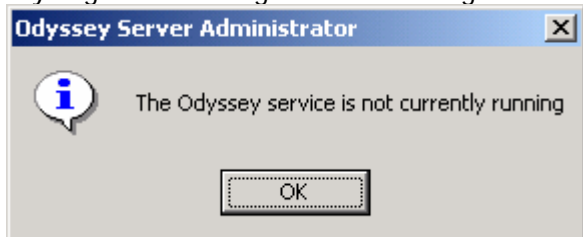


You may have to reboot the computer for the Internet Authentication Service to stop.

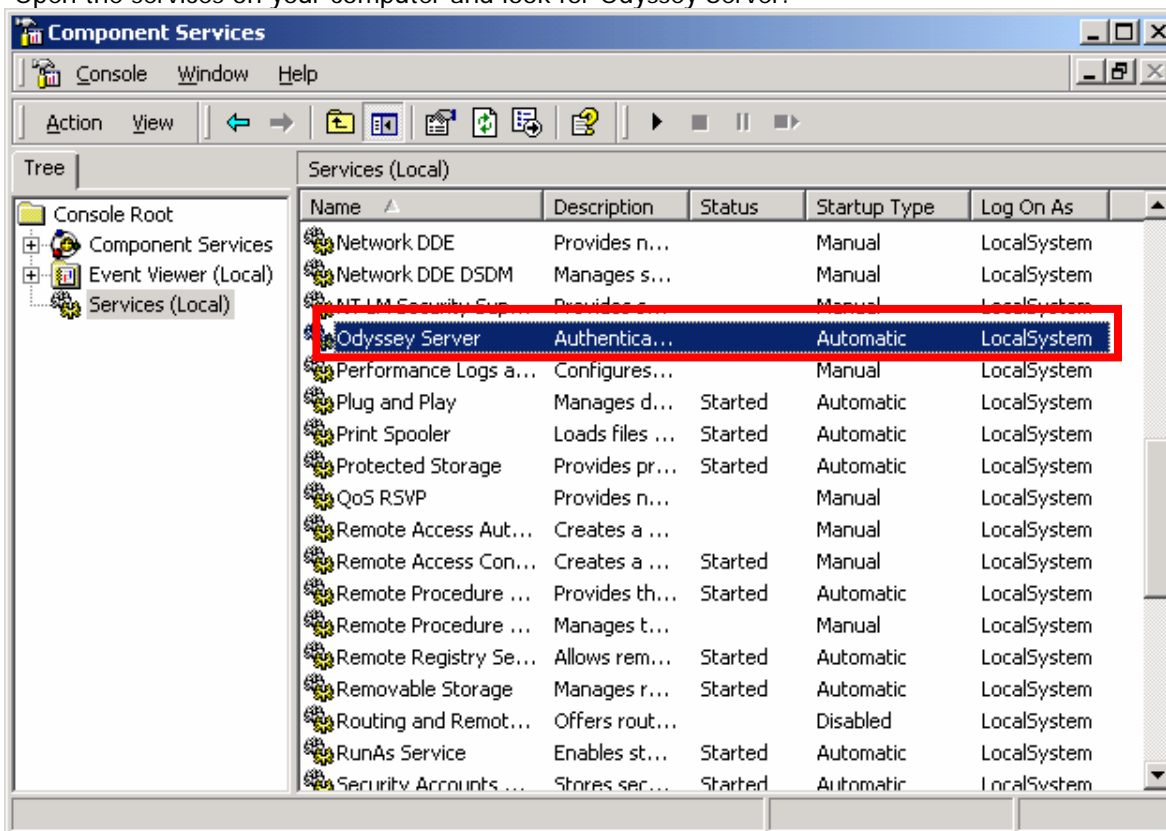


Appendix C: Starting the Odyssey Service

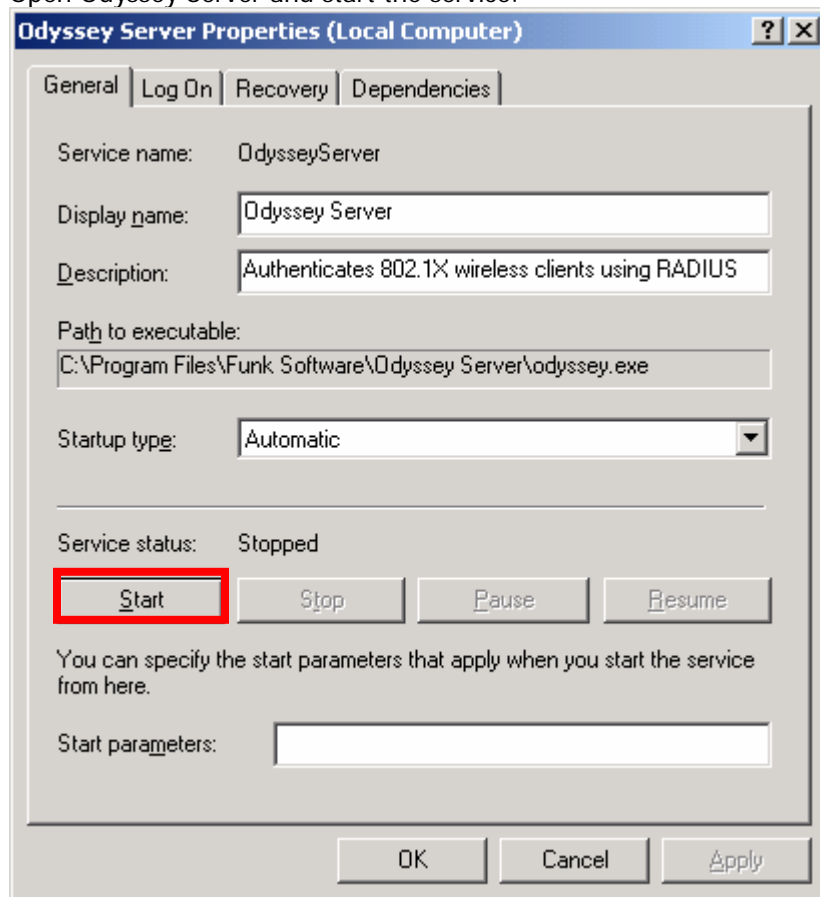
If you get this message when launching the Funk Software Odyssey Server:



Open the services on your computer and look for Odyssey Server.



Open Odyssey Server and start the service.





Appendix D: Uninstalling Microsoft Active Directory

To uninstall Microsoft Active Directory:

1. Click **Start** and then **Run**.
2. In **Open**, type **dcpromo**

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

WPA – 802.1x PEAP WITH FUNK ODYSSEY



FOUNDRY[®]
NETWORKS

Foundry Networks, Inc.
Headquarters
2100 Gold Street
P.O. Box 649100
San Jose, CA 95164-9100

U.S. and Canada Toll-free: (888) TURBOLAN
Direct telephone: +1 408.586.1700
Fax: +1 408.586.1900
Email: info@foundrynet.com
Web: <http://www.foundrynet.com>

Foundry Networks, BigIron, EdgeIron, FastIron, NetIron, ServerIron, and the "Iron" family of marks are trademarks or registered trademarks of Foundry Networks, Inc. in the United States and other countries. All other trademarks are the properties of their respective owners.

©2005 Foundry Networks, Inc. All Rights Reserved.