

White Paper: IronPoint 200 Installation Guide WPA – 802.1x PEAP with Funk Odyssey

©2005 Foundry Networks, Inc.

All Rights Reserved.

Written By: Michael Hong February 2005

FOUNDRY NETWORKS WHITE PAPER

White Paper: IronPoint 200 Installation Guide WPA – 802.1x PEAP WITH FUNK ODYSSEY **FO**



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 maybe 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 Wwitch.

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 requi red
Foundry AP(if-wireless g:	VAP[0])#encrypti on
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**.

			IronPoin	t™ 200	(1) Logout
System Identification TCP/IP RADIUS Management Tunnel Authorition	III Radius Primary RADIL	JS Server Set	up		
Authentication Bridging Administration Syslog & Time VLAN		IP Address Port Secret Key	xxxx 1812 *******	1	
SNMP SNMP General SNMP Trap Filters SNMP Targets	Im Retrai Interim	eout (seconds) nsmit attempts Accounting Port Update Timeout	5 3 0 3600		
P Radio Interface 802.11a	Secondary RA	ADIUS Server	Setup		
Security P Radio Interface 802.11g Radio Settings		IP Address Port	0.0.0.0 1812		
Security	Tim	Secret Key eout (seconds) nsmit attempts	5		
AP Status Stations Event Log	Interim	Accounting Port Update Timeout	0 3600		
	Radius VLAN	ID Format Se	etup		
		VEAN ID Format	●ASCII ●HEX	Apply Cance	Help

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

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**.

		Iroi	nPoint [™] 200 (≞ Logo	ıt	
System Identification TCP/IP RADIUS Management Tunnel Authentication Bridging	■ 802.11g: ■ Security "Before enabling the security	ne radios you	must set the country selection v	a the CLI."	
Administration	VAP Number	Enable	SSID	Details	
Syslog & Time VLAN	VAP 0		My SSID	More	
SNMP	VAP 1		Foundry AP 1	More	
SNMP Trap Filters SNMP Targets	VAP 2		Foundry AP 2	More	
1 Radio Interface 802.11a	VAP 3		Foundry AP 3	More	
Radio Settings Security				· · · · · · · · · · · · · · · · · · ·	
Radio Interface 802.11g Radio Settings Security					
P Status AP Status Stations Event Log				Apply Cancel	Help

White Paper: IronPoint 200 Installation Guide **FOUNDRY® NOT STALLATION GUIDE**

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.

		Iroi	nPoint [™] 200 © Log	gout	
System Identification TCP/IP RADIUS Management Tunnel Authentication Bridging	₩ 802.11g: ₩Security "Before enabling th	ne radios you	must set the country selection	via the CLI.''	
Administration	VAP Number	Enable	SSID	Details	
Syslog & Time VLAN	VAP 0		My SSID	More	
SNMP	VAP 1		Foundry AP 1	More	
SNMP Trap Filters SNMP Targets	VAP 2		Foundry AP 2	More	
🌮 Radio Interface 802.11a	VAP 3		Foundry AP 3	More	
Radio Settings Security				n de la companya de	
Radio Interface 802.11g Radio Settings Security					
Status AP Status Stations Event Log				Apply Cancel	Help

White Paper: IronPoint 200 Installation Guide

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**.



	IronPoint [™] 200 ^(I) Logout
FOUNDERY Ketworks	<section-header><pre>CremePair Page Page Page Page Page Page Page Page</pre></section-header>
	Apply Cancel Help

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

- 1. On the Internet, go to: <u>http://www.funk.com/</u>
- 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

- 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.
- 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.

Odyssey Server Administrate	or - [Odyssey Ser	ver]	
] <u>A</u> ction ⊻iew] ← → @	📧 🗟 🔮		
Tree	Name	Description	
🐼, Odyssey Server	🔣 Settings	Configure general server settings	
Settings	😤 Access Points	Configure access points	
Access Points	🚮 Groups	Set access policies for groups	
- 🚮 Groups	😚 Users	Set access policies for users	
	関 Policies	Configure access policies	
👸 Policies	🔛 Domains	Configure TTLS forwarding domains	
🚰 Domains	📕 Log Streams	Configure log streams	
Log Streams	强 Accounting	Configure accounting settings	
	Common Keys	Configure common keys	
Common Keys			

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

Odyssey	Server Administrator	x
٩	The Odyssey service is not currently runnin	ıg
	OK	

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**

olick OR.	
Odyssey CA	X
	_
A	
<u> </u>	
Welcome to Odyssey CA. Click OK to create a new root CA	i.
OK Cancel	

Enter My CA for CA name.





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
C Create intermediate CA issued by this CA:
C Create CA by importing this certificate:
Browse
< Back Next > Cancel

Enter My CA for Common name:. Click Next >.

Add CA	×
Specify the componen (DN). It is not necessa	s of the CA certificate's distinguished name ry to specify every component.
Common name:	CN= My CA
Organizational unit:	OU=
Organizational unit:	OU=
Organization:	O=
Locality:	L=
State or province:	ST=
Country code:	C= Browse
	< Back Next > Cancel



Click Next >.

Add CA	×
Specify the fully qualified host name of the CA's server machine as a subject alternative name for the CA's certificate.	5
☐ Include a DNS subject alternative name for this CA certificate.	
Subject alternative name (DNS): cse-win2k	-
< Back Next > Cancel	

Click Next >.

Add CA	×
Choose the parameters of the CA's signature algori	of the CA's generated key pair and choose thm.
Key algorithm:	RSA
Digest algorithm:	SHA1
Key <u>s</u> ize:	1024
	< Back Next > Cancel



Click Next >.

Add CA X				
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 o	Choose the duration of this CA's certificate.				
Time until exp	piration:				
Years:	10				
Months:	0				
Days:	0				
Expires:	Jan 22, 2015				
	< Back Finish Cancel				

White Paper: IronPoint 200 Installation Guide WPA – 802.1x PEAP WITH FUNK ODYSSEY **FO**



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

Creating CA X This may take several minutes for the keys to be created, depending on the key strength.

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.

😣 Odyssey CA Administrator				
File Help				
Add CA	_			
🕀 🚞 Odyssey CA	🚞 My CA			

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 >**.

Odyssey Certificate Requester				
Welcome to the Odyssey Certificate Requester				
If your organization uses the Odyssey CA (Certificate Authority), you can request a certificate from it. It can be for use by an Odyssey or Steel Belted Radius server. The certificate can be used to perform EAP-TLS, TTLS and PEAP authentications.				
To continue, click Next.				
< <u>B</u> ack <u>Next</u> <u>Cancel</u>				



Click **Next >**.

Odyssey Certificate Requester	
Specify server name	
Enter the name of this server. Normally, this is (FQDN).	the server's fully-qualified DNS name
The name you enter will be included in the ca	artificate's Subject Name.
Name of this <u>s</u> erver: cse-win2k.domain.m	y
To continue click Next	
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.
<u>A</u> lgorithm: RSA Key size: 1024 ▼
< <u>B</u> ack Cancel

White Paper: IronPoint 200 Installation Guide WPA – 802.1x PEAP WITH FUNK ODYSSEY **FO**



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

Odyssey Certificate Requester				
Specify CA address/port	Ø			
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:	x.x.x			
Port number:	8080			
Click Next to request a certificate from the CA.				
	< <u>B</u> ack <u>Next</u> > <u>C</u> ancel			

You will see the Certificate request pending window.

Ddyssey 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 <u>Close</u>				

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**.

😂Odyssey CA Administrator			
<u>File H</u> elp			
Refresh Process Deny			
🛛 🖂 Odyssey CA	Thumbprint 🛆	Subject	
E- My CA	2BAFC4918C8892E8FDAF8F1A9A63E	CN=cse-win2k.domain.my	
- Settings			-
Pending Certificate Requests			
Completed Certificate Requests			
Certificates			
Pending CRL Operations			
CRI Schedule			

Click Next >.

Certificate Request				
Click the 'next' button to continue.				
Request thumbprint: 2BAFC4918C8892E8FDAF8F1A9A63E0C12905D21D				
<u>S</u> ubject:	CN=cse-win2k.domain.my			
	Preview Deny			
	< Back Next > Cancel			

Click Finish

Certificate	Request			×	
Choose the duration of this certificate. Click the 'Finish' button to issue the certificate.					
Years: Months: Days:	1 0 0				
			Preview	Deny	
		< Back	Finish	Cancel	

Return to the Odyssey Certificate Requester Certificate request pending window.



Click Next >.

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 < <u>Back</u>	ose

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

Ddyssey Certificate Requester (My CA)
Certificate request approved
Your certificate request has been approved by the Odyssey CA administrator, and a certificate for this server has been issued.
Install this certificate into the local machine's certificate store
Save this certificate to a <u>fi</u> le
Configure the local copy of SBR with this certificate
Configure the local copy of Odyssey Server with this certificate
Click Next to continue
<u>V</u> iew < <u>B</u> ack <u>Next</u> > <u>C</u> ancel

Click OK.

February 2005

White Paper: IronPoint 200 Installation Guide WPA – 802.1x PEAP WITH FUNK ODYSSEY FO



X

Odyssey Certificate Requester

In order to configure Odyssey to use this certificate, it will also be installed in the Local Machine certificate store. Press OK to continue or Cancel to change your selections.

Click Finish.

lyssey Certificate Requester (My CA)
Finishing the request
You have select the following actions:
Install this certificate as a Personal Certificate in the Local Machine certificate store of this machine.
Configure Odyssey server to use this certificate during EAP authentications.
Click Finish to perform these actions.
< <u>B</u> ack <u>Finish</u> <u>C</u> ancel



Click Close.

Odyssey Certificate Requester (My CA)	
Completing the Odyssey Certificate Requester	
The following actions have been completed:	
This certificate has been installed as a Personal Certificate in the Local Machine certificate store of this machine.	
The local Odyssey Server has been configured to use this certificate during EAP authentications.	
< <u>B</u> ack <u>N</u> ext >	<u>C</u> lose



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.

Odyssey !	Server Administrator	×
٩	The Odyssey service is not currently running	g
	OK	

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

Odyssey Server Administrator - [Odyssey Server\Settings] Action View Image: Settings Image: Setings Image: Settings	Select Authentication 3	settings.							
Action ¥iew Image: Action View	💮 Odyssey Server Administrate	or - [Odyssey	Server\Setti	ngs]					
Tree Image: Construction of the section of the sec	_ Action ⊻iew 🗍 🗢 ⇒ 🔁) 🖪 🖪 🛛	3			1			
	Tree	RADIUS Settings	Access Point Defaults	Policy Defaults	Authentication Settings User Identificati	ILS/TTLS/P Settings TLS TTLS Accounting	User Trust	TTLS Inner Authentication	

This will open **Authentication Settings**. Click **Add...**

A	uthentication Settings	×
	Authentication protocols, in order of preference:	
	TTLS TLS	* *
		<u>A</u> dd
		<u>R</u> emove
	OK	Cancel



This will open **Add EAP Protocol**. Select **PEAP**. Click **OK**.

Add EAP Protocol	×
Select one or more protocols to add:	
OK Cancel	1
	1

This will take you back to **Authentication Settings**. Select **PEAP** Click the **UP arrow** twice.

Authentication Settings	×
	▲dd
	<u>R</u> emove
ОКС	ancel

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

Authentication Settings	×
Authentication <u>p</u> rotocols, in order of preference:	
PEAP	☆ ¥
TLS	<u>A</u> dd
	<u>R</u> emove
<u>ОК</u>	Cancel



This will return you to the **Odyssey Server Administrator**. From the left side menu, right click on **Access Points** and select **Add Access Point**.

Action Wew Tree Name Codyssey Server Common K Help Addaress Adaress Adaress<	🍭 Odyssey Ser	ver Administrator - [Odyssey Se	rver\Access Points]	_	
Tree Name Description Address Odyssey Server Settings Access Point Access Point Orapis Add Access Point View Pointies Domains Refresh Export List Accounting Help	Action ⊻iew				
Common K Help	Tree	Name	Description	Address	
	Codyssey Server Codyssey Server Cody Settings Cody Settings Cody Settings Cody Settings Cody Settings Cody Settings Cody Server Cody Server Common Market Common Market Common Market Common Market	Add Access Point View View Refresh Export List Help	Description	Aduress	

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 P	oint 🖸	×		
<u>N</u> ame:	My Foundry IP 200 Access Point	1		
Description: This is my Foundry IP 200 Access Point				
<u>A</u> ddress:	172 . 1 . 1 . 3 <u>R</u> esolve			
<u>M</u> odel:	- standard access point -			
Shared secre	t: <u>E</u> nter <u>V</u> alidate			
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			



This will open Enter Shared Secret.

Enter the same shared secret that was configured in your IP 200. Click $\ensuremath{\text{OK}}$

Enter Shared Secre	×
Enter shared secret:	*****
🔲 <u>U</u> nmask	
OK	Cancel

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

Add Access I	Point	×
<u>N</u> ame:	My Foundry IP 200 Access Point	
Description:	This is my Foundry IP 200 Access Point	
<u>A</u> ddress:	172.1.1.3 <u>R</u> esolve	
<u>M</u> odel:	- standard access point -]
Shared secre	et: <u>E</u> nter ⊻alidate	
Address rai If you dep and with them colle here.	nge bloy multiple access points of the same model the same shared secret, you can configure ectively by specifying a range of addresses	
🗌 Aļlow a	ny access point in address range	
N <u>u</u> mber of	addresses in range: 1	
Range:		
	OK Cancel	

White Paper: IronPoint 200 Installation Guide 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)**.

Odyssey Server Administrate	or - [Odyssey 9	5erver\Setti	ngs]			
🛛 Action View 🗍 🗢 🔿 主) 📧 🕾 🖆	?				
Tree	র্থ	R	Z	X	1 I I	Z
Settings	RADIUS Settings	Access Point Defaults	Policy Defaults	Authentication Settings	TLS/TTLS/P Settings	User Trust
Groups	র্	Z	Z	Z	Z	Z
Dor Help Log-screams	TTLS Inner Authentication	Forwarded Attributes	Returned Attributes	Self- Identification	User Identificati	TTLS Accounting
Common Keys						

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.

sers:		
lame	Full Name	Description
DOMAIN\john	john	
DOMAIN\krbtgt		Key Distribution Center Service Acc
DOMAIN\senthil	senthil	
DOMAIN\testuser	test user	
UUMAIN\I sinternetUser	TsInternetUser	This user account is used by Termin
DOMAIN\ttt	ttt	
		>
Add pe names separated by semicolons	into the list below, or select them l	from the list above:
Add pe names separated by semicolons plicy: Allow	s into the list below, or select them l	from the list above:
▲dd ype names separated by semicolons	: into the list below, or select them l	from the list above:



The selected user will appear in the list below. Click $\ensuremath{\text{OK}}$

Add User(s)		×
Domain: DOMAIN	•	
	[-	
Name	Full Name	Description
DOMAIN\john	john	
2 DOMAIN\krbtgt		Key Distribution Center Service Acc.
DOMAIN\senthil	senthil	
DOMAIN\testuser	test user	
🕅 DOMAIN\TsInternetUser	TsInternetUser	This user account is used by Termin
🕅 DOMAIN\ttt	ttt	_
•		
Add Type names separated by semicolons in DOMAIN\testuser	to the list below, or select them from the li	st above:
Policy: Allow		
	OK Cancel	



Exporting the Server Certificate

From the Odyssey Server Administrator, Select **Settings** from the left side menu. Open TLS/TTLS/PEAP Settings

	ottingo							
Odyssey Server Administrato	or - [Odyssey	Server\Setti	ngs]					<u>_ ×</u>
] Action ⊻iew] 🗢 ⇒ 🔁	1 🖪 🖪 1	3						
Tree	1 I I I	X	X	X	M	Z	X	
	RADIUS Settings	Access Point Defaults	Policy Defaults	Authentication Settings	TLS/TTLS/PEA P Settings	User Trust	TTLS Inner Authentication	
Groups GUsers	Z	X	Z	ন্থ	Ĭ			
Policies Domains Log Streams Accounting Common Keys	Forwarded Attributes	Returned Attributes	Self- Identification	User Identificati	TTLS Accounting			

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

TLS Settings (for EAP-TLS, EAP-TTLS, and PEAP)							
Server certificate:							
symbol-tm233							
<u>V</u> iew <u>B</u> rowse							
Session resumption							
Enable session resumption							
Do not resume sessions older than: 12 hours							
<u>C</u> ipher suites (check to enable):							
DHE-RSA, 3DES-EDE-CBC, SHA							
DHE-DSS,3DES-EDE-CBC,SHA							
☑ DHE-DSS,DES-CBC,SHA							
RSA.3DES-EDE-CBC.SHA							
Diffie-Hellman settings							
Prime bits: 1024							
Regenerate daily at:							
OK Cancel							



This will open the certificate.

Click Details.	
Certificate	<u>?</u> ×
General Details Certification Path	
Certificate Information	
This certificate is intended to:	
•Ensures the identity of a remote computer	
Issued to: changeme	
Issued by: My CA	
Valid from 1/25/2005 to 1/27/2010	
\mathscr{P} You have a private key that corresponds to this certificate.	
Issuer Stateme	int
	ĸ



Click Copy to Files...

Certificate	<u>? ×</u>
General Details Certification Path	1
Show: <a>All>	
Field	Value 🔺
🚍 Version	V3
💳 Serial number	01
Signature algorithm	sha1RSA
Issuer	My CA
Valid from	Tuesday, January 25, 2005 4:
Valid to	Wednesday, January 27, 201
Subject	changeme
Public key	RSA (1024 Bits)
Ec	it Properties
	ОК



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



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

Certificate Export Wizard	×				
Export Private Key You can choose to export the private key with the certificate.					
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.					
Do you want to export the private key with the certificate? $\ \ \ \underline{\bullet} \ \underline{\bullet} \ \underline{\bullet}$ export the private key					
C No, do not export the private key					
< <u>B</u> ack <u>Next</u> Cancel					

White Paper: IRONPOINT 200 INSTALLATION GUIDE

Check Include all certificates in the certification path if possible and Enable strong protection. Click Next >.

ertificate Export Wizard	×
Export File Format Certificates can be exported in a variety of file formats.	_
Select the format you want to use:	
C DER encoded binary X.509 (.CER)	
C Bage-64 encoded X.509 (,CER)	
€ _ryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
\square Include all certificates in the certification path if possible	
Personal Information Exchange - PKCS #12 (.PEX)	
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	
< <u>Back</u> 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.	
***** <u>Confirm password:</u>	

< <u>B</u> ack <u>Next</u> Cancel	

White Paper: IronPoint 200 Installation Guide **FO WPA – 802.1x PEAP WITH FUNK ODYSSEY**



	Click Browse …	
Ce	rtificate Export Wizard	×
	File to Export Specify the name of the file you want to export	
_	File name:	
-	< <u>B</u> ack <u>N</u> ext > Cancel	

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.

Save As					? ×
Savejn: 🔂	temp	•	(-	🗳 🎟 •	
File <u>n</u> ame:	cert4me.pfx		•	<u>S</u> av	e
Save as <u>t</u> ype:	Personal Information Exchange (*.	pfx)	•	Cano	el



Click Next > .	
Certificate Export Wizard	<u><</u>
File to Export Specify the name of the file you want to	export
<u>F</u> ile name:	
C:\Backup\temp\cert4me.pf×	Browse
	(Date Nation Count

Click Finish. Certificate Export Wizard X Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings: File Name C:\Back Export Keys Yes Include all certificates in the certification path Yes File Format Person Þ < <u>B</u>ack Finish Cancel



Click OK.

Certificate Export Wizard	×
The export was successful.	
OK	

Click OK.

Certificate	<u>? ×</u>
General Details Certification Path	1
Show: <a>All>	•
Field	Value 🔺
Version	V3
Serial number	01
Signature algorithm	sha1RSA
Issuer	My CA
Valid from	Tuesday, January 25, 2005 4:
Valid to	Wednesday, January 27, 201
Subject	changeme
Public key	RSA (1024 Bits)
Ec	it Properties
	ОК



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 odyc303.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 odyc303.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 >.

Configure and Enable Ody	ssey Wizard 🛛 🔀
EUNIX WAIRE	Welcome to the Configure and Enable Odyssey Wizard Odyssey will now allow you to configure it, and it will be set up to run on startup.
	If you have not yet inserted your wireless adapter card, please do so before pressing the Next button. Do not ask again Click Next to continue or Cancel to stop configuration.
	< <u>B</u> ack. <u>N</u> ext > Cancel

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE



Click Finish .					
Configure and Enable Odyssey Wizard 🛛 🛛 🔀					
	Completing the Configure and Enable Odyssey Wizard You have completed the initial configuration of Odyssey. You can modify these settings by using the Odyssey Client Manager, which will now run.				
	Click Finish to enable obyssey .				
	< <u>B</u> ack Finish Cancel				



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.	

😂 C: \temp			
<u> Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>I</u> ools <u>H</u> elp			
🚱 Back 👻 🕥 🖌 🏂 🔎 Search 🞼 Folders 💷			
Address 🛅 C:\temp			
Folders X Name A	Size	Туре	Date Modifie
Image: Second	2 KB 3 KB	Text Document Personal Informatio	10/21/2004 1 1/26/2005 8;

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



WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE **FO**



FOUNDRY NETWORKS WHITE PAPER – DRAFT: DO NOT DI STRBIUTE

Click Next >.	
Certificate Import Wizard	
File to Import	
Specify the file you want to import.	
<u>File name:</u>	
C:\temp\cert4me.pfx	Browse
Personal Information Exchange- Pl Cryptographic Message Syntax Sta Microsoft Serialized Certificate Sto	KCS #12 (.PFX,.P12) andard- PKCS #7 Certificates (.P7B) re (.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.			

White Paper: IronPoint 200 Installation Guide WPA – 802.1x PEAP WITH FUNK ODYSSEY **FO**



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

С	ertificate 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:	
-	< <u>B</u> ack <u>N</u> ext > Cancel	

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

Select Certificate Store
Select the <u>c</u> ertificate store you want to use.
🕀 🦳 Personal 💦 💦
Trusted Root Certification Authorities
Local Computer
Show physical stores
OK Cancel



FOUNDRY NETWORKS WHITE PAPER – DRAFT: DO NOT DI STRBIUTE

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
\bigcirc Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities\Local Computer Browse
< <u>B</u> ack <u>Next</u> > Cancel

Click Finish.

Click **Next** >.



Click OK.





Configuring Funk Software Odyssey Client

Open the Odyssey Client Manager. Select **Profiles**. Click **Add**

🌒 Odyssey Client Ma	nager	
Settings Commands	<u>W</u> eb <u>H</u> elp	
Connection Profiles Networks Auto-Scan Lists S Trusted Servers Adapters	Profiles The following profiles are configured: Initial Profile	<u>A</u> dd <u>R</u> emove <u>P</u> roperties

White Paper: IronPoint 200 Installation Guide 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		
Pr <u>o</u> file name: testuser		
User Info Authentication ITLS Settings PEAP Settings		
Login name: testuser		
Password		
Permit login using password		
<u>Construction device preserver</u> d <u>Figure 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.</u>		
🗖 U <u>n</u> mask		
Certificate		
Permit login using my <u>c</u> ertificate:		
View Browse		
OK Cancel		



Select Authentication Click **Add**

Add Profile
Profile name: testuser
User Info Authentication TLS Settings PEAP Settings
Authentication protocols, in order of preference:
EAP / TTLS
I Validate server certificate
OK Cancel

Select **EAP/PEAP**. Click **OK**.

Add EAP Protocol	×
Select one or more protocols to add:	
EAP / Token Card EAP / MD5-Challenge EAP / LEAP	
OK Cancel]

White Paper: IronPoint 200 Installation Guide

Select EAP/PEAP.

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

Click OK.

Add Profile	×
Pr <u>o</u> file name:	testuser
LL L C Autho	
User Info Augu	encoation 11LS Settings PEAP Settings
Authentication p	rotocols, in <u>o</u> rder of preference:
EAP / TTLS	× ↓
	<u>A</u> dd
	<u>R</u> emove
E V PL	
I Validate serv	/er certificate
	OK Cancel



Select Networks. Click Add

🌒 Odyssey Client Ma	nager	
<u>S</u> ettings <u>C</u> ommands	<u>W</u> eb <u>H</u> elp	
-Connection	Networks	
	The following <u>n</u> etworks are configured:	
Profiles	<[any]>	<u>A</u> dd
Networks		<u>R</u> emove
Auto-Scan Lists		Properties
Trusted Servers		
Adapters		

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE **FO**



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**

Add Network			x	
Network				
Network name (SSID): My SSID				
Connect to any ava	Connect to any available network <u>S</u> can			
Description (optional):				
Network <u>t</u> ype:	Access poin	t (infrastructure mode)	•	
C <u>h</u> annel:	default chan	nel	-	
Association mode:	WPA		•	
Encryption method:	TKIP		•	
-				
Authentication				7
Authenticate using (profile:	testuser	•	
✓ Keys will be generated automatically for data privacy				
Pre-shared key (WPA)-				
Passphrase:				
OK Cancel				

February 2005

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE



Select Trusted Servers Click Add ...

🍭 Odyssey Client Ma	nager	
Settings Commands	<u>W</u> eb <u>H</u> elp	
Connection	Trusted Servers	
	<u>The following servers are trusted:</u>	
Profiles		<u>A</u> dd
+++ Networks		<u>R</u> emove
Auto-Scan Lists		<u>E</u> dit
Trusted Servers	1	Ad <u>v</u> anced
Adapters		

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

Add Trusted Servers Entry	×
Server name must end with:	
<any></any>	
Irust any server with a valid certificate regardless of its name	
Server certificate must be issued by:	
jew	
OK Cancel	



Select Trusted Root Certification Authorities Select the certificate issued by **My CA** Click **OK**

Select Certificate		
Intermediate Certification Authorities		
Issued To	Issued By 🔼 🔼	
Certiposte Classe A Personne Certiposte Serveur Certisign - Autoridade Certificadora - AC2 Certisign - Autoridade Certificadora - AC4 Certisign Autoridade Certificadora AC1S Certisign Autoridade Certificadora AC3S	Certiposte Classe A Personne Certiposte Serveur Certisign - Autoridade Certificadora - A Certisign - Autoridade Certificadora - A Certisign Autoridade Certificadora AC1S Certisign Autoridade Certificadora AC3S	
changeme	Му СА	
Class 1 Primary CA Class 1 Public Primary Certification Aut Class 1 Public Primary Certification Aut Class 2 Primary CA	Class 1 Public Primary Certification Au Class 1 Public Primary Certification Au Class 1 Public Primary Certification Au Class 2 Primary CA	
Class 2 Public Primary Certification Aut	Class 2 Public Primary Certification Au	
	⊻iew	
	OK Cancel	

Click OK

Add Trusted Servers Entry	×
Server name must end with:	
<any></any>	
✓ Irust any server with a valid certificate regardless of its name	
Server certificate must be issued by:	
changeme	
<u>V</u> iew <u>B</u> rowse .	
OK Cancel	

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE



Select Connection. Check Connect to network: From the pull down menu, select **<My SSID>** Click Reconnect

👶 Odyssey Client A	lanager 📃 🗖 🗙
Settings Commands	<u>W</u> eb <u>H</u> elp
Connection	Adapter: Dell Wireless WLAN 1450 Dual Band WLAN
	Adapter type: wireless
+++Networks	Connect to network:
Auto-Scan Lists	Connection information
Trusted Servers	Status: open
Adapters	Elapsed time: 00:00:06 Network (SSID): rangetest_b Access point: 00:00:0B-81-39-04 IP address: IP address:
	Packets in/out: 0 / 0
	Reconnect Reauthenticate 🚮 🐔 🖘

Status will display the connection status.

🛎 Odyssey Client M	Aanager 📃 🗖 🔀
<u>S</u> ettings <u>C</u> ommands	Web Help
	Adapter: Dell Wireless WLAN 1450 Dual Band WLAN
	Adapter type: wireless
++++ Networks	Connect to network: ++ <my ssid=""></my>
Auto-Scan Lists	Scan
	Status: Searching for My SSID
Adapters	Elapsed time: Network (SSID): Access point:
	IP address: 172.1.1.233
	Packets in/out:
	Reauthenticate Image: Constraint of the second se

White Paper: IRONPOINT 200 INSTALLATION GUIDE

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.

👶 Odyssey Client M	lanager 📃 🗖 🔀
Settings Commands ∖	<u>W</u> eb <u>H</u> elp
Connection	Connection Adapter: Dell Wireless WLAN 1450 Dual Band WLAN
Profiles	Adapter type: wireless
+++Networks	Connect to network: ++ <my ssid=""></my>
Auto-Scan Lists	- Connection information
Trusted Servers	Status: open and authenticated
Adapters 🖉	Network (SSID): My SSID Access point: EnterpriseAP IP address:
	Packets in/out: 170
	Reauthenticate



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 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)#ssid My SSID Foundry AP(if-wireless g)#encryption 128 Foundry AP(if-wireless g)#wpa-clients Required Foundry AP(if-wireless g)#wpa-mode Dynamic Foundry AP(if-wireless g)#multicast-cipher TKIP Foundry AP(if-wireless g)#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**.

		IronPoint [™] 200	① Logout
System Identification RADIUS Management lunnel	₩ Radius Primary Radius Server Se	tup	
Authentication Bridging Administration Syslog & Time VLAN	IP Address Port Secret Key	172.1.1.1 1812	
SNMP SNMP General SNMP Trap Filters SNMP Targets	Retransmit attempts	5 3 5 Setup	
Radio Interface 802.11a Radio Settings Security	IP Address Port Secret Key	0.0.0.0	
 Radio Interface 802.11g Radio Settings Security 	Timeout (seconds) Retransmit attempts	5	
			Apply Cancel Help

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE



Go to the **Authentication** webpage. For 802.1x Setup: select Required.

Click Apply.

	gour
# System # # Authentication Identification # 802.1x Setup : FADUUS Disable 602.1x authentications not allowed Authentication Supported Clients may or may not use 002.1x Administration Supported Client must use 802.1x VLAN If 602.1x supported or required is selected, then Radius setup must be completed # Situp Concent Broadcast Key Refresh Rate 30 minutes (0 = Disabled) Status 802.1x Authentication Refresh Rate 0 minutes (0 = Disabled) # Radio Interface 902.1s 802.1x Authentication Refresh Rate 0 minutes (0 = Disabled) Status 802.1x Authentication Refresh Rate 0 minutes (0 = Disabled) # Radio Scattings Supplicant E nable # Local MAC Selection: MAC Authentication Settings : # Local MAC Authentication Settings : MAC Authentication Settings : System Default Dony Allow MAC Authentication Settings : MAC Authentication Settings : System Default Dony Allow MAC Authentication Settings : MAC Authentication Settings : MAC Authentication Table : MAC Authentication Table : MAC Addr	

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

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 Mulitcast Cipher Mode select TKIP. Click **Apply**.

White Paper: IronPoint 200 Installation Guide WPA – 802.1x PEAP WITH FUNK ODYSSEY **FO**



FOUNDRY NETWORKS WHITE PAPER – DRAFT: DO NOT DISTRBIUTE

📂 System 🔤	# 002.11g.
Identification	iii Security
TCP/IP	in Security
RADIUS	III WEP
Management Tunnel	
Authentication	Authentication Type Setup
Bridging	
Administration	Open System Allow everyone to access
Sysiog & Time	
VEAN	Shared Key Allow users with a correct key to access
(* O)1110	
SNMP	
SNMP General	Data Encryption Setun
SNMP Trap Filters	
SIMMP Targets	🗢 Disable 🔍 Enable
Padio Interrace 802.11a	
Security	
Security	Shared Key Setup 🔍 64 Bit 🔍 128 Bit
Radio Interface 802.11g	
Descusibus	Key Type 🔍 Hexadecimal For 64 Bit enter 10 digits, for 128 Bit enter 26 digits
Security	
	Approximation For 64 Bit enter 5 characters, for 128 Bit enter 13 characters
Status	Transmit Koy
AP Status	Key Number Select Key
Stations	Kay 1 0
Event Log	
	Key 2 C
	Key 3 💿 💿
	WPA Configuration Mode
	Allow WPA Clients Only
	WPA Key Management
	WELL and address over 002 for
	VVPA authentication over ouz.1x
	WPA Pre-shared Key
	Multicast Cipher Mode
	WEP Use WEP as WPA Multicast cipher mode
	TKIP Use TKIP as WPA Multicast cipher mode
	AFS Lise AFS as WPA Multicast rinker 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

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**

	IronPoint [™] 200		(U) La	ogout
System Identification TCP/IP RADIUS Management Tunnel Authentication Bridging Administration Syslog & Time VLAN	# 802.11g: # Radio Settings "Before enabling the radios you must set the country selection via the CLL." I Enable SSID : My SSID Antenna Mode Fixed ▼			
SNMP SNMP General SNMP Trap Filters SNMP Targets	Radio Mode 802.11b+g 🔽 Radio Channel : 11 💌			
Radio Interface 802.11a Radio Settings Security Radio Interface 902.111 Radio Settings Security	Auto Channel Select : O Disable O Enable Transmit Power 100% I Maximum Station Data Rate 54 I Mbps Beacon Interval (20-1000) 100 TUs			
Status AP Status Stations Event Log	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 Hidden SSID : O Disable O Enable			
		Apply	Canaal	Holp



Appendix B: Disabling IAS on Microsoft Windows Server

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

E computer Management					_	
Action ⊻iew	🖆 🔁 🗟 😫 🛛 🕨 🔳 🖷	Þ				
Tree	Name 🔺	Description	Status	Startup Type	Log On As	
Computer Management (Local) System Tools Storage DHCP DHCP Computer Management (Local) Storage DHCP DHCP Computer Management (Local) Storage DHCP	Fax Service File Replication Service FTP Publishing Service IIS Admin Service Internet Authentication Service Internet Connection Sharing Intersite Messaging IPSEC Policy Agent Kerberos Key Distribution Center License Logging Service Logical Disk Manager Logical Disk Manager Net Logon Net Logon Net Logon Net IQ Endpoint NetMeeting Remote Desktop Sh Network Connections Network DDE Network DDE DSDM Net I M Security Support Provider	Helps you Maintains fi Provides F Allows adm Enables au Provides n Allows sen Manages I Generates Cogical Disk Administrat Sends and Supports p Provides a Manages o Provides n Manages s Provides s	Started Started Started Started Started Started Started Started Started Started Started Started	Manual Automatic Automatic Automatic Automatic Manual Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Manual Manual Manual Manual	LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem LocalSystem	
,	a second booteney support for doi		200,000	r rannarat	cocale y sconn	



Open Internet Authentication Service and Stop the service.

Internet Authentie	cation Service Properties (Local Computer) 💦 🔀
General Log On	Recovery Dependencies
Service name:	IAS
Display <u>n</u> ame:	Internet Authentication Service
Description:	-up and VPN users. IAS supports the RADIUS protocol.
Pat <u>h</u> to executabl D:\WINNT\Syste	e: m32\svchost.exe -k netsvcs
Startup typ <u>e</u> :	Automatic
Service status:	Started
<u>S</u> tart	Stop Pause Besume
You can specify t from here.	he start parameters that apply when you start the service
Start parameters:	
	OK Cancel Apply

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 you	ar compater and loor	Citil Ouysse	y Jerver.			
🚡 Component Services					_	
] 🚡 <u>C</u> onsole <u>W</u> indow <u>H</u> e	۱p				_	Ð×
$]$ Action View $] \Leftrightarrow \Rightarrow$	🗈 📧 🖆 🕏	😫] 🕨	■ ■>			
Tree	Services (Local)					
Console Root	Name 🛆	Description	Status	Startup Type	Log On As	
Component Services Event Viewer (Local) Services (Local)	Ketwork DDE	Provides n Manages s Provides s		Manual Manual Manual	LocalSystem LocalSystem LocalSystem	
	Codyssey Server	Authentica Configures		Automatic Manual	LocalSystem	
	Plug and Play	Manages d	Started	Automatic	LocalSystem	
	Ne station and the second s	Loads files	Started	Automatic	LocalSystem	
	Storage	Provides pr	Started	Automatic Manual	LocalSystem LocalSystem	
	Remote Access Aut	Creates a		Manual	LocalSystem	
	🆓 Remote Access Con	Creates a	Started	Manual	LocalSystem	
	🆓 Remote Procedure	Provides th	Started	Automatic	LocalSystem	
	🆓 Remote Procedure	Manages t		Manual	LocalSystem	
	🆓 Remote Registry Se	Allows rem	Started	Automatic	LocalSystem	
	🆓 Removable Storage	Manages r	Started	Automatic	LocalSystem	
	🆓 Routing and Remot	Offers rout		Disabled	LocalSystem	
	RunAs Service	Enables st	Started	Automatic	LocalSystem	
	Security Accounts	Stores sec	Started	Automatic	LocalSystem	-

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



Open Odyssey	Server	and	start	the	service.

Odyssey Server Pr	operties (Local Computer)
General Log On	Recovery Dependencies
Service name:	OdysseyServer
Display <u>n</u> ame:	Odyssey Server
Description:	Authenticates 802.1X wireless clients using RADIUS
Pat <u>h</u> to executabl C:\Program Files\	e: Funk Software\Odyssey Server\odyssey.exe
Startup typ <u>e</u> :	Automatic
Service status:	Stopped
<u>S</u> tart	Stop <u>P</u> ause <u>R</u> esume
You can specify the start parameters that apply when you start the service from here.	
Start parameters:	
	OK Cancel Apply

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

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

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.

DRY® works