

# ***Odyssey<sup>®</sup> Client for Linux***

## ***User Guide***

***Version 4.3***

***July 2006***

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Copyright © 2002-2006 Juniper Networks<sup>®</sup>, Inc. All rights reserved. Printed in USA.

Odyssey<sup>®</sup>, Funk<sup>®</sup>, Juniper Networks, and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org>) and cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software developed by Computer Associates (<http://www.ca.com/>).

Juniper Networks, Inc. assumes no responsibility for any inaccuracies in this document. Juniper Networks, Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

# Contents

## Preface

Documentation Overview.....	vii
Audience.....	vii
What's in This Manual.....	vii
Context-Sensitive Help and Other Product Information.....	viii
Typographical Conventions Used in this Manual.....	viii
Third-Party Product Documentation.....	ix

## Chapter 1

### Welcome

Welcome to Odyssey Client.....	1
Technical Support.....	1

## Chapter 2

### Networking with Odyssey Client

Overview.....	3
Network Security.....	3
Encryption and Association for Secure Authentication.....	4
Odyssey Client Features for a Secure Network.....	5
802.11 Wireless Networking.....	6
Types of 802.11 Wireless Networks.....	6
Wireless Network Names.....	7
Wired-Equivalent Privacy.....	7
Wi-Fi Protected Access and its Encryption Methods.....	8
802.1X Authentication.....	9
Extensible Authentication Protocol.....	9
Reauthentication.....	13
Session Resumption.....	13

## Chapter 3

### Installation

Installation Process.....	15
Before You Begin.....	15
Installation Instructions.....	15

## Chapter 4

## Using Odyssey Client Manager

Odyssey Client Manager Overview .....	17
Starting Odyssey Client Manager .....	18
Odyssey Client Manager Display.....	18
Connection Panel.....	19
Select an Adapter .....	20
Connect to a Network (Wireless Connections Only) .....	20
Connect Using Profile (Wired Connections Only).....	21
Configure Multiple Simultaneous Network Connections .....	21
Scan for Wireless Networks .....	21
Reconnect to a Network.....	22
Reauthenticate to a Network .....	23
Disconnect from a Network.....	23
View Connection Information .....	23
View Informational Graphics and Detailed Status.....	24
Profiles Panel .....	26
Profile Properties .....	27
Networks Panel .....	37
Network Titles .....	38
Network Properties .....	39
Auto-Scan Lists Panel.....	44
Auto-Scan List Properties .....	45
Trusted Servers Panel .....	46
Setting up Certificates .....	47
Configuring Trust .....	48
Untrusted Servers .....	50
Adapters Panel.....	51
Adding a Wireless or Wired Adapter.....	52
Removing an Adapter from the List of Adapters.....	52
Settings Menu .....	52
Preferences.....	53
Security Settings .....	53
PAC Manager .....	56
Enable/Disable Odyssey .....	57
Close .....	57
Commands Menu.....	57
Forget Password .....	57
Forget Temporary Trust.....	58
Web Menu.....	58
Odyssey User Page .....	58
Funk Software Home Page .....	59
Register Odyssey Client .....	59
Purchase Odyssey Client .....	59
Help Menu.....	59
Help Topics .....	59
License Keys.....	59
View Readme File.....	60
About.....	60

System Tray Icon Menu Commands .....	60
Odyssey Client Manager.....	61
Exit .....	61
Other Odyssey Client Features.....	61
Shortcut Keys.....	61
Interaction with Other Adapter Software.....	62
Hard Token Authentication Run-Time Dialogs.....	62

<b>Index.....</b>	<b>63</b>
-------------------	-----------



# Preface

## Documentation Overview

This guide describes how to install and configure the Odyssey Client software.

Your Odyssey Client software includes a help system that allows you to access this documentation on your computer. To bring up this help system, select the **Help > Help Topics** menu command from the Odyssey Client Manager.

You can also read the manual in PDF format. The manual file `OdysseyClientManLinux.pdf` is provided with Odyssey Client.

## Audience

This manual is intended as a reference and configuration guide for users of Odyssey Client. If you have any questions about your configuration, see your network administrator.

This manual is intended as a reference and configuration guide for users of Odyssey Client. If you have any questions about your configuration, see your network administrator.

## What's in This Manual

This manual includes the following topics:

- ▶ **“Welcome” on page 1** describes an overview of Odyssey Client, and provides information on contacting technical support.
- ▶ **“Installation Process” on page 15** describes how to install Odyssey Client.
- ▶ **“Networking with Odyssey Client” on page 3** provides an overview of 802.1X networking.
- ▶ **“Using Odyssey Client Manager” on page 17** provides information on configuring the main user interface, Odyssey Client Manager.

## Context-Sensitive Help and Other Product Information

You can get context-sensitive help for the Odyssey Client Manager and the Odyssey Client Administrator by pressing **F1** on your keyboard for any open dialog. The resulting help provides information that is relevant to your current context.

In addition, you can use the **Help > View Readme File** menu command located on the Odyssey Client Manager to open the `readme.txt` file. This file may have important information about Odyssey Client that is not included in this manual.

## Typographical Conventions Used in this Manual

The typographical conventions used in this manual are described in the following topics:

- ▶ Computer Text
- ▶ Screen Interaction
- ▶ Variable Text
- ▶ Keyboard Keys
- ▶ Definitions

### Computer Text

File names, directory names, IP addresses, URLs, commands, and file listings appear in a plain fixed-width font:

    Edit the `radius.ini` file.

    For more information, go to `http://www.juniper.net`.

In examples, text that you type literally is shown in a bold font.

```
C:\>cd \Radius\Service
```

### Screen Interaction

Text related to the user interface appears in **bold**.

    Click **OK**.

    Enter your username in the **Login** field.

Menu commands are presented as the name of the menu, followed by the **>** sign and the name of the command. If a menu item opens a submenu, the complete menu path is given.

    Choose **Edit > Cut**.

    Choose **Edit > Paste As... > Text**.

## Variable Text

Variable text that you must replace with your own information appears in *italics*. For example, you would enter your name and password in place of **YourName** and **YourPassword** in the following interaction.

```
Enter your name: YourName  
Password: YourPassword
```

File names and computer text can also be displayed in italics to indicate that you should replace the values shown with values appropriate for your enterprise. For example, you would enter your own profile name in place of the italicized *profileName* text in the following example:

```
[Integrity_Settings]  
Quarantine_Profiles=profileName
```

## Keyboard Keys

Names of keyboard keys appear in SMALL CAPS. When you need to press two or more keys simultaneously, the key names are joined by a + sign:

Press RETURN.

Press CTRL+ALT+DEL.

## Definitions

Terms that may be unfamiliar appear in italics when they are defined.

## Third-Party Product Documentation

For more information about configuring your access servers, access points, and firewalls, consult the documentation provided with each product.



# Chapter 1

## Welcome

### Welcome to Odyssey Client

Thank you for selecting Odyssey<sup>®</sup> Client.

With Odyssey Client, you can connect to your wireless or wired 802.1X network easily and securely. You can use Odyssey Client for the following:

- ▶ Configure and control connections for a wireless or wired adapter.
- ▶ Connect to access points as well as to peer-to-peer networks.
- ▶ Configure authentication profiles to allow you to connect to different networks with different credentials.
- ▶ Use the secure 802.1X standard to authenticate to the network.
- ▶ Use a wide variety of authentication methods, including powerful methods such as EAP-TTLS, EAP-PEAP, EAP-TLS, and EAP-FAST to keep your credentials secure.

### Technical Support

If you have any problems installing or using Odyssey Client, there are various resources available to help you at no charge:

- ▶ This manual and the `README.TXT` file may contain the information you need to solve the problem you are having. Please re-read the relevant sections. You may find a solution you overlooked. To view the `README.TXT` file, select the **Help > View Readme File** menu command from the Odyssey Client Manager.
- ▶ Check our web site <http://www.juniper.net> and navigate to the **Tech Support > Support Options** section of the web site for additional information and technical notes. You can also select **Web > Odyssey User Page** from the menu bar to go to a special home page for Odyssey Client users.

- ▶ For technical support by phone, you can call (617) 491-6503, Monday through Friday, 9:00 A.M. to 5:30 P.M., Eastern time.

Within six months of the product purchase date, Juniper Network provides for two technical support incidents by phone at no charge. For support beyond this initial warranty period, or beyond two incidents within that period, we offer a range of support options, including support and maintenance contracts and pay-per-call. Consult our web site for the support plan that best meets your needs. Go to <http://www.juniper.net> and navigate to the **Tech Support > Support Options** section of the web site.

If you are located outside North America, you can receive support either by contacting the Juniper Network partner in your country or by contacting us directly. You can find the name of the support provider nearest you on our web site. Go to <http://www.juniper.net> and navigate to the **Contact Info > International** section of the web site.

Please take a moment to register your copy of Odyssey Client with us. By registering Odyssey Client, you can be notified of product upgrades and special offers. This also expedites your first contact with our Technical Support department. To register Odyssey, select the **Web > Register Odyssey Client** menu command from the Odyssey Client Manager.

# Chapter 2

## Networking with Odyssey Client

### Overview

This chapter introduces the basic networking and security concepts that underlie the design of Odyssey Client. Read this material to learn about networking choices that allow you to use Odyssey Client to best advantage, and to learn how to maximize the security of your connections over wireless or wired local area networks (LANs).

If you already know all about wireless networking, or if Odyssey has been configured for you by your network administrator, you can safely skip over this material.

Some of the basic concepts used by Odyssey Client for network authentication are described in the following topics:

- ▶ [“Network Security” on page 3](#)
- ▶ [“802.11 Wireless Networking” on page 6](#)
- ▶ [“802.1X Authentication” on page 9](#)

### Network Security

Most organizations can rely on physical security to protect their wired networks. An attacker would have to be physically inside company offices to plug in to the LAN and generate or observe network traffic.

With wireless networks, all it takes to gain access to the network is a device with a wireless card and a comfortable spot in the parking lot outside of the building or in the office next door.

Odyssey Client provides you with the ability to make network connections using protocols that adhere to one or more of these sets of standards:

- ▶ The IEEE (Institute of Electrical and Electronic Engineers) standards for wireless LANs include 802.11a, 802.11b, and 802.11g. See [“802.11 Wireless Networking” on page 6](#).
- ▶ The IEEE 802.11i enhancements to 802.11 that were introduced to overcome some of the security weaknesses of 802.11.
- ▶ The Wi-Fi Alliance second generation of Wi-Fi protected access, Wi-Fi protected access 2 (WPA2) (with advanced encryption standard (AES) encryption), which adheres to the strong 802.11i enhancements. See [“Wi-Fi Protected Access and its Encryption Methods” on page 8](#) for definitions.
- ▶ WPA (with AES or temporal key integrity protocol (TKIP) encryption), which complies with a subset of 802.11i, and, although not as strong as WPA2, addresses some of the security weakness of 802.11 as well. See [“Wi-Fi Protected Access and its Encryption Methods” on page 8](#) for definitions.
- ▶ The IEEE 802.1X standard that supplements the 802.11 standards with secure server-based wireless or wired network connections. See [“802.1X Authentication” on page 9](#).

## Encryption and Association for Secure Authentication

To establish a wireless connection with an access point, a wireless client must associate with the access point. For a wireless client device to access a secure network, the user of the client device must be authenticated by the network. The following list briefly defines terminology necessary to understand association, data encryption, and authentication:

- ▶ Association is the method by which a client establishes a relationship with an access point.
- ▶ Data encryption is used to secure data that is exchanged between a client device and an access point (or another computer).
- ▶ Encryption keys are key components of data encryption algorithms. Encryption keys may also be used for access point association.
- ▶ Once a wireless client has associated with an access point, the user of that client device may be authenticated to the network. Authentication is used to secure the relationship between a user of a wireless-equipped computer and an authentication server. For example, wireless network authentication that is based on the 802.1X standard can make use of cryptographically strong (and dynamically generated) encryption keys.

There are several methods for providing secure authentication over a wireless network. Each method requires data encryption, and consequently requires some method for specifying or generating encryption keys. Some of these methods are known to be more secure than others:

- ▶ Preconfigured secrets, called WEP (wired-equivalent privacy) keys. These keys are intended to encrypt the data transferred between the client and the access point and can be used to keep unauthorized users off the wireless network, as well as to

encrypt the data of legitimate users. See [“Wired-Equivalent Privacy” on page 7](#) for a description of WEP-based encryption that complies with 802.11 standards.

- ▶ Preshared passphrases used to generate keys for WPA or WPA2 association. Preshared passphrases allow you to configure a simple phrase that is used to generate cryptographically strong encryption keys to be used with AES or TKIP encryption. AES and TKIP also periodically change the encryption keys in use. The generated keys keep unauthorized users off the wireless network and encrypt the data of legitimate users. See [“Wi-Fi Protected Access and its Encryption Methods” on page 8](#) for a description of AES or TKIP encryption methods that enhance the 802.11 standards.
- ▶ Authentication using an 802.1X-based protocol. This method uses a variety of underlying authentication protocols to control network access. The stronger among these protocols provide cryptographically protected mutual authentication of the user and the network. In addition, you can configure Odyssey Client so that keys that are used to encrypt wireless data are generated dynamically. 802.1X-based authentication can use WEP, AES, or TKIP encryption, depending on network hardware/firmware. See [“802.1X Authentication” on page 9](#) for information on authentication using 802.1X. See [“Wi-Fi Protected Access and its Encryption Methods” on page 8](#) for a description of some of the strongest available association and encryption modes. The 802.1X methods are also viable for wired 802.1X-based network connections.

## Odyssey Client Features for a Secure Network

You can use the following Odyssey Client features to make wireless networks secure:

- ▶ You can require user authentication. A user must be authenticated by the network before he or she is allowed access, to make the network safe from intruders. See [“Extensible Authentication Protocol” on page 9](#) for an overview of the Odyssey Client authentication protocols. For protocol configuration details, see [“Profile Properties” on page 27](#).
- ▶ You can require data encryption between the wireless client and the access point. The wireless connection between a client and an access point must be encrypted so that eavesdroppers cannot access data that is supposed to be private. For configuration details, see [“Network Properties” on page 39](#).
- ▶ You can configure server trust for mutual authentication. The network must be authenticated (trusted) by the user before the user allows their credentials to be released to the network in order to make a network connection. This prevents a wireless device that may be posing as a legitimate network from impersonating the network and gaining access to the user’s PC. For configuration details, see [“Trusted Servers Panel” on page 46](#), and [“Validate the Server Certificate” on page 32](#).
- ▶ The mutual authentication between user and network must be cryptographically protected. This type of mutual authentication requires 801.1X-based protocols and prevents connections to phony networks. For configuration details, see [“Authentication” on page 30](#).

## 802.11 Wireless Networking

There are many types of wireless communication. Odyssey Client is designed to work over networks that adhere to the IEEE 802.11 wireless LAN standards, as well as the Wi-Fi Alliance enhancements to these standards.

Many corporations deploy secure wireless 802.11 networks, and 802.11 networks are commonly found in hotels, airports, and other “hotspots” as a means of internet access.

### Types of 802.11 Wireless Networks

Your wireless adapter (network interface card) allows you to connect to wireless networks of two types: *access point* networks and *peer-to-peer* networks.

#### Access Point Networks

Access point networking is the most common type of wireless networking, providing for wireless access to a corporate network and the internet.

In this type of wireless network, your PC establishes a wireless connection to a device called an *access point*. The access point links your wireless PC to the rest of the network. An access point typically provides general network connectivity for many PCs.

A single network can include many access points. Each access point typically has a range of several hundred feet. An enterprise that uses wireless networking can strategically place access points so that, wherever you are located in the company, you are always within range of an access point that can link you to the corporate network.

You may also find access points at other locations outside of your company building. For example, you may find access points at hotels, airports, or internet cafes, or you may have your own access point on your home network. Some of these locations require that you log in. Others may provide network access to anyone within range.

When you connect to a network via an access point, you are using the 802.11 *infrastructure mode*. See [“Specify the Network Type” on page 40](#) for information on configuring infrastructure network connections.

#### Peer-to-Peer Networks

Even when no access point is available, two or more wireless clients can use *peer-to-peer* networking to create a private wireless network. You may want to do this to share files, run groupware applications, or play games. The peer-to-peer network requires no additional equipment beyond a set of two or more wireless-enabled PCs that are located within range of each other. As a result, this networking mode does not involve an authentication server, and cannot use 802.1X-based authentication.

The 802.11 standard refers to peer-to-peer network connectivity as *ad-hoc mode*. See [“Specify the Network Type” on page 40](#) and [“Specify the Association Mode” on page 41](#) for information on configuring ad-hoc network connections.

## Wireless Network Names

Each wireless network has a name. The 802.11 standard refers to a network name as *service set identifier (SSID)*. You can select the wireless network to which you want to connect by specifying its name.

Network names allow for the coexistence of more than one wireless network in the same vicinity. For example, the company next door to yours may also use wireless networking. Network names allow you to distinguish access points located within your enterprise wireless network from access points that are not within your corporate LAN.

Network names do not, in themselves, offer any security, and cannot prevent you from connecting to a phony network.

A network name is simply a text sequence up to 32 characters long, such as Bayonne Office, Acme-Marketronics, or BE45789. A network name is case-sensitive. You always have the option to scan for available networks. Scanning allows you to select the network from a list, preventing any data entry errors.

## Wired-Equivalent Privacy

You can use wired-equivalent privacy (WEP) to encrypt data transferred between your client device and the access point. When you use WEP for data encryption, you can configure access point association in one of two modes:

- ▶ **Shared**—Use this mode when the access point requires that you preconfigure a WEP key for association. When 802.11-based preconfigured (static) WEP keys are in use, the client and the access point share the same secret keys, and a client is not allowed to access the network unless it can prove it knows the preconfigured WEP keys assigned to the access point. This is not as secure as authenticating with 802.1X methods. See [“802.1X Authentication” on page 9](#). You can configure shared association according to directions in [“Network Properties” on page 39](#).
- ▶ **Open**—Use this mode for WEP-based data encryption when the access point does not require that you preconfigure a static WEP key for association. You can configure open association according to directions in [“Network Properties” on page 39](#).

**NOTE:** You can obtain stronger network security when you use dynamic encryption key generation and 802.1X-based authentication. For shared association, a preconfigured key that is used only for access point association is still required. See [“802.1X Authentication” on page 9](#), and [“Extensible Authentication Protocol” on page 9](#) for more information.

See the following topics:

- ▶ [“Specify the Association Mode” on page 41](#) for directions for selecting an association mode in Odyssey Client.
- ▶ [“Specify an Encryption Method for the Selected Association Mode” on page 41](#) for directions for selecting WEP encryption when using the shared or open association mode
- ▶ [“Specify Preconfigured Keys for WEP” on page 43](#) to use static WEP keys with Odyssey Client

**NOTE:** You can also use preconfigured keys for WEP data encryption in peer-to-peer network connections. In this case, all clients in the peer-to-peer network must share the same WEP keys.

## Wi-Fi Protected Access and its Encryption Methods

As an enhancement to the 802.11 wireless standard, the Wi-Fi Protected Access (WPA) and the stronger Wi-Fi Protected Access 2 (WPA2) association modes encompass a number of security enhancements over Wired-Equivalent Privacy. These enhancements include the following:

- ▶ Improved data encryption with the TKIP algorithm. TKIP provides stronger encryption than WEP.
- ▶ Improved data encryption with the AES algorithm. AES provides stronger encryption than WEP or TKIP.
- ▶ WPA and WPA2 can generate TKIP or AES encryption keys from a preshared passphrase. Although your passphrase may be simple, these encryption methods can generate cryptographically strong encryption keys from a simple passphrase. Consequently, these encryption methods are stronger than WEP encryption based on preconfigured WEP keys. If you configure a passphrase for key generation for your access points, you cannot use 802.1X-based authentication and you must configure the same passphrase in Odyssey Client.

When the access points in your network require that you associate via WPA or WPA2, you can configure Odyssey Client to associate in that mode. If the access points are configured for TKIP or AES encryption, you can configure Odyssey Client for either of these enhanced data encryption methods as well. You should configure your access points and clients for network connections that use the strongest association and encryption methods that are supported by your network access points.

**NOTE:** With access points enabled for WPA2 or WPA, you can obtain the stronger network security when you use dynamic encryption key generation and 802.1X-based authentication. See [“802.1X Authentication” on page 9](#), and [“Extensible Authentication Protocol” on page 9](#) for more information.

See the following topics:

- ▶ [“Specify the Association Mode” on page 41](#) to use WPA2 or WPA association mode with Odyssey Client
- ▶ [“Specify an Encryption Method for the Selected Association Mode” on page 41](#) to use AES or TKIP encryption with WPA2 or WPA association
- ▶ See [“Specify Preshared Keys for WPA or WPA2” on page 43](#) to configure a passphrase that is used in encryption key generation.

**NOTE:** You can use a preshared passphrase to generate encryption keys for TKIP or AES data encryption for securing peer-to-peer network connections. In this case, all clients in the peer-to-peer network must share the same passphrase.

## 802.1X Authentication

The IEEE 802.1X protocol provides authenticated access to a LAN. This standard applies to wireless as well as wired networks. In a wireless network, the 802.1X authentication occurs after the client has associated to an access point using an 802.11 association method. Wired networks use the 802.1X standard without any 802.11 association.

The WEP protocol has various shortcomings when preconfigured keys are in use. Preconfigured WEP keys not only contribute to administrative overhead, but using them poses security weaknesses. Although the encryption methods calculated from keys generated from preshared passphrases are stronger than WEP encryption calculated from static WEP keys, the use and distribution of passphrases can also pose administrative and security problems. The use of 802.1X protocols in wireless networks addresses these problems.

When preconfigured WEP keys are used, it is the wireless client PC that is authenticated to the network. With 802.1X, it is the *user* who is authenticated to the network with the user credentials, which may be a password, a certificate, or a token card. Moreover, the keys used for data encryption are generated dynamically. The authentication is not performed by the access point, but rather by a central server. If this server uses the RADIUS protocol, it is called a *RADIUS server*.

With 802.1X, a user can log in to the network from any PC, and many access points can share a single RADIUS server to perform the authentication. This makes it much easier for the network administrator to control access to the network.

See the following topics for details:

- ▶ Extensible Authentication Protocol
- ▶ Session Resumption
- ▶ Reauthentication

### Extensible Authentication Protocol

802.1X uses the Extensible Authentication Protocol (EAP) to perform authentication. EAP is not an authentication mechanism *per se*, but is a common framework for transporting actual authentication protocols. The advantage of EAP is that the basic EAP mechanism does not have to be altered as new authentication protocols are developed.

Odyssey provides a number of EAP protocols, allowing a network administrator to choose the protocols that work best for a particular network.

The newer EAP protocols have an additional advantage. They can dynamically generate the WEP, TKIP, or AES keys that are used to encrypt data between the client and the access point. Dynamically created keys have an advantage over preconfigured keys because their lifetimes are much shorter. Known cryptographic attacks against WEP can be thwarted by reducing the length of time that an encryption key remains in use. Furthermore, encryption keys generated using EAP protocols are generated on a per-user and per-session basis. The keys are not shared among users, as they must be with preconfigured keys or preshared passphrases.

Odyssey offers a number of EAP authentication methods, including the following:

- ▶ EAP-TTLS (tunneled transport layer security)
- ▶ EAP-PEAP (protected EAP)
- ▶ EAP-TLS (transport layer security)
- ▶ EAP-FAST (flexible authentication via secure tunneling)
- ▶ EAP-LEAP (lightweight EAP)

## Mutual Authentication

EAP-TTLS, EAP-PEAP, EAP-TLS, and EAP-FAST all provide *mutual authentication* of the user and the network, and produce dynamic keys that can be used to encrypt communications between the client device and access point. With mutual authentication, not only does the network authenticate the user credentials, but the client software also authenticates the network credentials.

Requiring mutual authentication is an important security precaution to take when using wireless networking. By verifying the identity of the authentication server, mutual authentication provides assurance that you connect to your intended network, and not to some access point that is pretending to be your network.

You can authenticate the network with Odyssey Client when you configure it to validate the certificate of the authentication server using EAP-TTLS, EAP-PEAP, or EAP-TLS. If the certificate identifies a server that you trust, and if the authentication server can prove that it is the owner of that certificate, then you can safely connect to this network. These are the strongest authentication methods available, and consequently, it is highly recommended that you use these methods for network authentication within your enterprise wireless network.

## Certificates

Certificates are based on public/private key cryptography (or *asymmetric cryptography*). Public/private key cryptography is used to secure banking transactions, online web commerce, email, and many other types of data exchange.

Prior to the use of modern cryptographic techniques for networking, if two people wanted to communicate securely, they had to share the same secret key. This one secret key had to be used to both encrypt and decrypt data. Sharing keys, however, is limiting. The more people with whom you share your key, the more likely it becomes that your key can be revealed.

With public/private key cryptography, there are two keys that have different values but work together:

- ▶ A public key
- ▶ A private key

You keep your private key secret, but reveal your public key to the whole world. Anyone can encrypt data using your public key with the certain knowledge that only your private key can decrypt it. Furthermore, only you can encrypt data with your private key, and anyone can use your public key to decrypt the data.

A certificate is a piece of cryptographic data that guarantees that a particular public key is associated with the private key of a particular entity. This entity can be an individual or a computer. A certificate contains many pieces of information that are used in mutual authentication, including a public key and the name of the entity that owns the certificate.

Your enterprise certificate authority may issue certificates to smart cards. Odyssey Client supports all types of user certificates, including smart card certificates.

Each certificate is issued by a *certificate authority*. By issuing a certificate, the certificate authority warrants that the name in the certificate corresponds to the certificate's owner (much as a notary public guarantees a signature). The certificate authority also has a certificate, which in turn is issued by a higher certificate authority. At the top of this pyramid of certificates is the *root certificate authority*. The root certificate authority is typically a well-known entity that people trust, whose self-signed certificate is widely known. For example, Verisign and Thawte are public root certificate authorities. Many corporations have set up their own private root certificate authorities as well.

There is a date on which each certificate expires. Additionally, a certificate granting authority can revoke a certificate. Expired or revoked certificates are not valid, but certificates can be re-issued or renewed.

A set of certificates in sequence, including any intermediate certificate authorities up to the root certificate authority is called a *certificate chain*. Certificate chains are typically no more than several certificates in length. In many cases, a chain consists of two certificates:

- ▶ An end entity certificate
- ▶ A root certificate

Certificates are well-suited for authentication from a security perspective. The disadvantage of using certificates for authentication is that, while it is fairly easy to provide certificates to servers, it is much harder to provide certificates to users. This is because at any given enterprise, the number of servers that may require certificates is relatively small, but the number of users can be enormous. Providing certificates to each employee can be a daunting management task, and may require a level of administration that your company is not prepared to undertake.

## EAP-TLS

EAP-TLS is a protocol devised by Microsoft, based on the TLS protocol that is widely used to secure web sites. It requires that both the user and authentication server have certificates for mutual authentication.

While EAP-TLS is cryptographically strong, it requires a certificate infrastructure that maintains and supplies certificates to all network users.

## EAP-TTLS

EAP-TTLS is a protocol devised by Funk Software and Certicom. It is designed to provide authentication that is cryptographically as strong as [EAP-TLS](#), while not requiring that each user be issued a certificate. Instead, only the authentication servers require certificates.

EAP-TTLS authentication is performed using a password or other credentials. Password-type credentials are transported in a securely encrypted “tunnel” that is established using the server certificate. Within the EAP-TTLS tunnel, you can employ any of a number of inner authentication protocols. With tunneled password credentials, user authentication can be performed against the same security database that is already in use on the corporate LAN. For example, Windows Active Directory or an SQL or LDAP database may be used. See [“TTLS Settings” on page 34](#) for more information on configuring inner protocols for tunneled authentication.

If your enterprise has a user-based certificate infrastructure in place, you have the option to configure user certificate-based credentials for EAP-TTLS authentication, with or without tunneled password credentials. See [“PEAP Settings” on page 36](#).

## EAP-PEAP

EAP-PEAP is comparable to EAP-TTLS, both in its method of operation and its security. However, EAP-PEAP is not as flexible as EAP-TTLS and it does not support the range of inside-the-tunnel authentication methods that EAP-TTLS supports. Commercial implementations of this protocol that started appearing at the beginning of 2003 were beset with interoperability problems. Nevertheless, this protocol is supported by Microsoft and Cisco and is in widespread use. EAP-PEAP is a suitable protocol for performing secure authentication against Windows domains and directory services. See [“PEAP Settings” on page 36](#) for more information on configuring inner protocols for EAP-PEAP authentication.

## EAP-FAST

EAP-FAST is an EAP authentication method created by Cisco. Like EAP-TTLS and EAP-PEAP, EAP-FAST offers password-based 802.1X authentication that encapsulates user credentials inside a TLS tunnel. Unlike other tunneled protocols, however, a server certificate is not required as a means of establishing a tunnel. Without the protection of a server certificate, EAP-FAST authentication can be vulnerable to man-in-the-middle attacks (and subsequent off-line dictionary attacks).

## EAP-LEAP

EAP-LEAP (Lightweight EAP, also known as EAP-Cisco Wireless) is a protocol developed by Cisco to allow users to be authenticated using their password credentials, without the use of certificates. The data exchange in EAP-LEAP is fundamentally similar to the exchange that occurs when a user logs in to a Windows Domain Controller.

EAP-LEAP is very convenient because it is Windows-compatible. However, because EAP-LEAP does not use server certificates, it relies on the randomness of the user password for its cryptographic strength. As a result, when user passwords are relatively short or insufficiently random, a wireless eavesdropper observing an EAP-LEAP exchange can easily mount a dictionary attack to discover these weak passwords.

## Reauthentication

When you reauthenticate to your network, encryption keys are refreshed, and any new or updated security policies that are implemented on the network are applied to your network connection.

You can configure automatic periodic reauthentication to the network using Odyssey Client.

Periodic reauthentication serves two purposes:

- ▶ As a general security measure, it verifies that you are still on a trusted network.
- ▶ It results in distribution of fresh shared keys to your PC and access point. The access point may use these shared keys to refresh the keys used to encrypt data. By frequently refreshing keys, you can thwart cryptographic attacks.

See [“Automatic Reauthentication” on page 54](#) for information on configuring this feature.

## Session Resumption

When you first authenticate using [EAP-TTLS](#), [EAP-PEAP](#), or [EAP-TLS](#), a fair amount of intensive computation is performed, both on your client PC and on the network authentication server. Private keys must be used to encrypt or sign data, signatures on certificates must be validated, password credentials must be checked, and so on.

Once you have authenticated a connection to the network, your network session begins. During a session, any subsequent authentications to the same network server can be accelerated by reusing the secret information that is derived during the first authentication. This is called *session resumption*. You can configure client-side session resumption features that apply to the certificate-based protocols using Odyssey Client.

It is usually a good idea to enable session resumption. The necessity for some form of reauthentication occurs fairly frequently in wireless networking, particularly when you are moving between access points. Each time you connect with a new access point, a new authentication occurs. The less time it takes to perform that authentication, the less likely you are to experience a momentary stall in your network applications. Additionally, using session resumption rather than reauthentication puts less load on the authentication server.

Session resumption results in the distribution of new keys to the client and to the access point, just as a fresh authentication does.

See [“Session Resumption” on page 54](#) for more information on using this feature.

**NOTE:** *If your network does not permit session resumption, then any configured client-side session resumption features are ignored.*



# Chapter 3

## Installation

### Installation Process

You can install Odyssey Client only if you have root privileges on the client machine.

You can find installation information in the following topics:

- ▶ [Before You Begin](#)
- ▶ [Installation Instructions](#)

### *Before You Begin*

You or your network administrator should perform the following network administration tasks prior to installing Odyssey Client for use:

- ▶ Select and prioritize the authentication protocols required for your authentication server.
- ▶ Configure the server certificate on your authentication server.
- ▶ Configure the authentication server policies for your enterprise users.
- ▶ Configure the access points and/or 802.1X switches in your network.
- ▶ Have in place a certificate infrastructure if you require your users to use personal certificates for authentication.
- ▶ Install your wireless (and/or wired) network adapter card and associated driver software.

### *Installation Instructions*

Before you install Odyssey Client, please locate the Odyssey Client installation file (of type `.rpm.bin`).

To install Odyssey Client as a root user of the client machine, follow these steps:

**1** Set the current directory to the one in which the Odyssey Client installation file is located.

**2** Type one of the commands below, based on your version of RedHat Linux (3 or 4):

```
./OdysseyClientLinuxRH3.rpm.bin
```

or

```
./OdysseyClientLinuxRH4.rpm.bin
```

Note that the file must be executable. If it fails to execute, use the `chmod` command and run the install again, as follows:

```
chmod a+x ./OdysseyClientLinuxRH3.rpm.bin
```

This command installs and starts the Odyssey Client service and installs the Odyssey Client Manager, from which you can configure Odyssey Client.

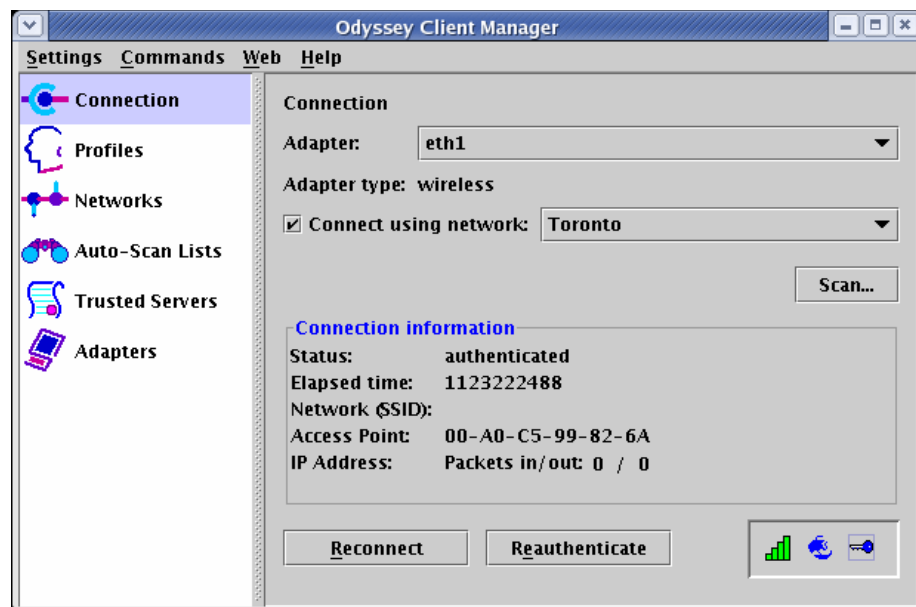
Once you install Odyssey Client, you can configure it using the Odyssey Client Manager. See [“Starting Odyssey Client Manager” on page 18](#) for more information.

# Chapter 4

## Using Odyssey Client Manager

### Odyssey Client Manager Overview

You can use Odyssey Client Manager to control and configure the Odyssey Client product.



**Figure 1** Connection Panel for Authenticated User Connections

If your system administrator has configured Odyssey Client for you in advance, you may need to use only the main Connection panel of the Odyssey Client Manager.

See “[Connection Panel](#)” on page 19 for information on the basic tasks you can perform from the Connection panel.

More advanced tasks that you or your system administrator may want to perform before connecting to a network are described in the following topics:

- ▶ Adding a wireless adapter. See [“Adding a Wireless or Wired Adapter”](#) on page 52.
- ▶ Creating a user profile and configuring authentication for that profile. See [“Profile Properties”](#) on page 27.
- ▶ Adding or editing network properties. See [“Network Properties”](#) on page 39.
- ▶ Configuring trusted servers. See [“Configuring Trust”](#) on page 48.

## Starting Odyssey Client Manager

You can restart Odyssey Client Manager at any time in any of the following ways:

- ▶ From the system tray – Double-click the Odyssey icon, or right-click it and choose Odyssey Client Manager.

To start Odyssey Client, select Odyssey Client Manager from the main applications menu, or double-click the Odyssey icon.

**NOTE:** *You cannot use Odyssey Client unless the Odyssey Client service is running. For Linux systems, you can start or stop the service with one of the following commands:*

```
/sbin/service odyssey start  
/sbin/service odyssey stop
```

## Odyssey Client Manager Display

The features available from the Odyssey Client Manager depend on your connection, as well as on your configuration. The available features are described in the following topics:

- ▶ [“Display for User-Authenticated Connections”](#) on page 18
- ▶ [“Menu and System Tray Commands”](#) on page 19
- ▶ [“Menu and System Tray Commands”](#) on page 19
- ▶ [“Connection Panel”](#) on page 19

### Display for User-Authenticated Connections

For most network connections, Odyssey Client Manager consists of a number of panels that allow you to control different aspects of its operation:

- ▶ Use the Connection panel to control your network connection and display your current connection status.
- ▶ Use the Profiles panel to set information that is used when you authenticate, or log in, to the network, such as your password or certificate.
- ▶ Use the Networks panel to configure different wireless networks and how you want to connect to them.
- ▶ Use the Auto-Scan Lists panel to specify ordered lists of wireless networks to which to connect.

- ▶ Use the Trusted Servers panel to set certificate and identity information about the servers that may authenticate you when you connect. Configuring this feature is required for protocols that implement mutual authentication, and is a recommended security measure.
- ▶ Use the Adapters panel to configure one or more network adapters (interface cards) for wired or wireless networking.

All of the panels are listed at the left of the Odyssey Client Manager display. Click the name of any panel to view or modify its settings.

## Menu and System Tray Commands

In addition to the Odyssey Client Manager panels, the display includes a number of commands that you can use from the menus. The menus are described in the following topics:

- ▶ “Settings Menu” on page 52
- ▶ “Commands Menu” on page 57
- ▶ “Web Menu” on page 58
- ▶ “Help Menu” on page 59

Some commands are also available if you right-click the Odyssey icon in the system tray.

## Connection Panel

You can use the Connection panel (Figure 2) to select an adapter, establish a network connection, and display your current connection status.

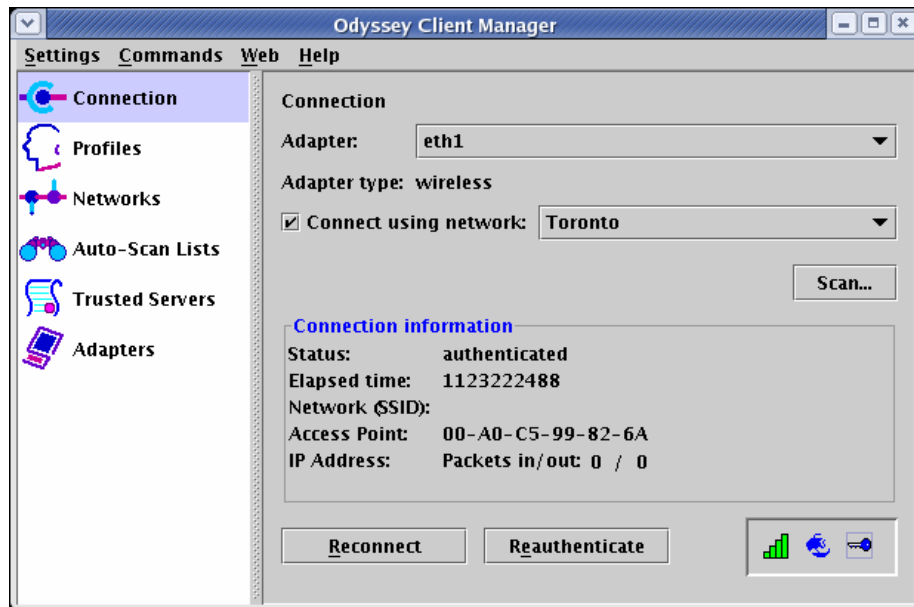


Figure 2 Connection Panel

You can perform tasks from the Connection panel that are described in the following topics:

- ▶ “Select an Adapter” on page 20
- ▶ “Connect to a Network (Wireless Connections Only)” on page 20
- ▶ “Connect Using Profile (Wired Connections Only)” on page 21
- ▶ “Configure Multiple Simultaneous Network Connections” on page 21
- ▶ “Scan for Wireless Networks” on page 21
- ▶ “Reconnect to a Network” on page 22
- ▶ “Reauthenticate to a Network” on page 23
- ▶ “Disconnect from a Network” on page 23
- ▶ “View Connection Information” on page 23
- ▶ “View Informational Graphics and Detailed Status” on page 24

**NOTE:** The Connection panel display and features vary when you connect from a wired adapter, or if you connect to the network via machine credentials. For example, the scanning feature is unavailable in these cases.

## Select an Adapter

If you or your administrator has configured more than one adapter for use with Odyssey Client, then you can use the **Adapter** list in the Connection panel to associate any of those adapter cards with a network connection.

Once you select an adapter, the **Adapter type** field on the Connection panel is updated to reflect the type (wireless or wired) of adapter you select.



## Connect to a Network (Wireless Connections Only)

When you connect to a network using a wireless adapter, you specify all the information required for the connection using an Odyssey Client network definition. When you define a network in Odyssey Client, you also must associate the user authentication information you specify in an Odyssey Client profile definition.

You can select a wireless network or auto-scan list from the list that is located to the right of the **Connect to network** field. The only items that appear on this list are the individual networks that you create in the Networks panel and the auto-scan lists that you create in the Auto-Scan Lists panel.

Any auto-scan lists that you have created appear at the top of the list. These are followed by the names of configured networks. Network names appear in angled brackets, after any network description text that you have specified.

Networks and auto-scan lists have icons before the name:

- ▶  for networks
- ▶  for auto-scan lists

The list that is located to the right of **Connect to network** contains the networks and auto-scan lists that you have configured.

To connect to a network or auto-scan list that you have configured, follow these steps:

- 1 Select the network or the auto-scan list to which you want to connect.
- 2 Check **Connect to network**, if it is not already checked.

If you select an auto-scan list, then the first network in the list that responds to the authentication request is the network to which you connect.

To disconnect from a wired network, uncheck **Connect to network**.

## Connect Using Profile (Wired Connections Only)

When you make a network connection using a wired connection, you specify all of the required connection information in a user profile. As a result, when you configure a wired connection, you connect using an Odyssey Client profile.

To connect to a wired 802.1X network switch using a profile that you have specified in the Profiles panel, follow these steps:

- 1 Select the profile from the **Connect using profile** list.
- 2 Check **Connect using profile** if it is not already checked.

To disconnect from a wired network, uncheck **Connect using profile**.

## Configure Multiple Simultaneous Network Connections

Each adapter on your computer can have its own connection. This means that if you have two wireless adapters, for example, you can have two simultaneous connections to wireless networks. Similarly, you can simultaneously run a wired connection and a wireless one. You can have as many network connections running simultaneously as you have adapters configured for use with Odyssey Client.

To connect to more than one configured network using multiple adapters, follow these steps:

- 1 Select an adapter from the **Adapter** list on the Connection panel.
- 2 Assign a network or an auto-scan list to this connection for wireless connections, or assign a profile for wired connections.

Repeat this procedure for each adapter whose network connection you want to establish.

You can use the **Adapter** list on the Connection panel to toggle between the adapters you have configured for multiple network connections, and hence monitor the status of multiple network connections.

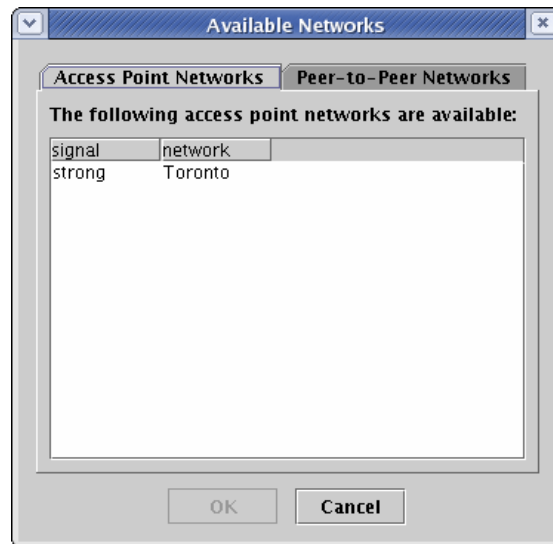
## Scan for Wireless Networks

If you travel frequently, you may want to authenticate through locally available wireless networks that you have not already configured.

To connect to a wireless network that is not yet configured, follow these steps:

- 1 Click **Scan** on the Connection panel.

Odyssey Client surveys the air waves and displays a list of all wireless networks that are currently reachable.



**Figure 3** Available Networks that Result from Scanning

- 2 Select the network to which you want to connect, and click **OK**.

If you have not yet configured settings for this network, the Add Network dialog appears. Specify settings and click **OK**. Once you check **Connect to network** on the Connection panel, Odyssey Client attempts to connect to the network.

**NOTE:** Only those wireless networks that are configured by an administrator to “send beacons” are visible to you when you scan. If “send beacons” is off, then you must specify the network from the Networks panel, or choose the default [any] network from the Connection panel.

## Reconnect to a Network

When you click **Reconnect** on the Connection panel, Odyssey Client disconnects any existing connection for the currently selected adapter and starts a new connection to the selected wireless network. The new connection may be with a different access point (on the same network) than was used with your previous connection. The access point in use depends on factors such as signal strength. If you are already authenticated with this network, you are reauthenticated when the new connection starts. If dynamic encryption keys are in use, they are refreshed when you reconnect. Note that you do not have this feature available if you are connected using a wired adapter.

You probably do not need to use this button often. However, there may be times when your connection is not performing as well as it should. Clicking **Reconnect** can sometimes help, particularly if it results in a connection with an access point that can provide better service.

## Reauthenticate to a Network

When you click **Reauthenticate** on the Connection panel, Odyssey Client reauthenticates your existing connection shown in the display, without starting a new connection. If dynamic encryption keys are in use, they are refreshed.

## Disconnect from a Network

To disconnect a wireless network connection, uncheck **Connect to network**.

To disconnect a wired network connection, uncheck **Connect using profile**.

## View Connection Information

The **Status** field on the Connection panel displays the current status of your connection to the network through this adapter. The status messages are defined in [Table 1](#).

**Table 1.** Connection Status Information

Status Message	Definition
open and authenticated	The connection is authenticated, and you are connected.
open / authenticating	Reauthentication is in progress, and you are connected.
open / requesting authentication	You have requested reauthentication, and you are connected.
open	The connection is not authenticated, but you are connected.
peer-to-peer	The network type is peer-to-peer (ad hoc), and you are connected.
authenticating	You are not yet connected, but authentication is in progress.
requesting authentication	You are not yet connected, but you have requested authentication from the access point.
waiting to authenticate	You are not yet connected, and the last authentication failed, but you are waiting to retry. If you see this message for a considerable length of time, you may be experiencing an association problem. If so, check the association mode required for your access point.
searching for access point	You are not connected, and communication with an access point on the requested network has not been established. This may occur when your adapter does not support 802.1X, or if your access point is not within range.
searching for peer(s)	You are not connected, and communication with other PCs on the peer-to-peer network has not been established. This message appears only for ad-hoc (peer-to-peer) connections.

**Table 1. Connection Status Information (Continued)**

Status Message	Definition
disconnected	You are not connected, and <b>Connect to network</b> may be unchecked. See <a href="#">“Connect to a Network (Wireless Connections Only)” on page 20</a> for how to connect.
Odyssey is disabled	You are not connected, and Odyssey Client has been disabled.
adapter not present	You are not connected, and the configured adapter is not currently available. This may occur when your adapter does not support 802.1X.
cable unplugged	You are not connected. This can occur if you have a wired connection, but your cable is unplugged.
adapter in use by another program	Your adapter is being used by another program installed on your machine.
disabled by wired connection	Your wired connection has disabled your Odyssey Client wireless connection based on your security settings. See <a href="#">“The options on the General tab of the Security Settings dialog are initially set to default values that should suit most purposes. You can restore the defaults at any time by clicking the Reset Defaults button.” on page 54.</a>

The **Elapsed time** field on the Connection panel displays the time that has elapsed since the time at which you started the current connection.

The **Network (SSID)** field displays the name of the wireless network to which you are connected. See [“Wireless Network Names” on page 7](#). This field is not displayed when you view the status of a network connection that uses a wired adapter.

The **Access point** field displays the name of the wireless access point to which you are connected. If this name is not available, the access point MAC (media access control) address is displayed instead. A MAC address is a unique 48-bit number encoded into a device by the manufacturer.

The **IP address** field displays the IP address that is assigned to your Odyssey Client connection.

The **Packets in/out** field displays the total number of network packets received and transmitted since this connection began.

## **View Informational Graphics and Detailed Status**

The graphical status buttons at the bottom right corner of the Connection panel give you a visual indication of the status of your connection. See the following topics for information on these buttons:

- ▶ [Signal Power Status](#)
- ▶ [Connection Status](#)

### ► Encryption Key Information


You can use the mouse or the keyboard to view detailed connection status information from any of the status buttons:


- Using the mouse—Point to a graphical status button with the mouse, and hold down the left-click button.
- Using the keyboard—Press the **TAB** key until you select a graphical status button, and hold down the space bar.


## Signal Power Status


The signal power graphic shows you how strong the signal is between your PC and the access point. The more bars that are filled in, the stronger the signal.

You can interpret the signal power status graphic as follows:

 Strong signal power

 Moderate signal power

 Weak signal power


 Faint signal power


 No signal power


Hold down your mouse button while clicking this icon to see the signal power measured in decibels.

## Connection Status

The connection status button (with the Odyssey “sailing boat” icon) shows the state of your connection and whether you are authenticated.

 (outline) – Not connected

 (red) – Not connected, due to failed authentication

 (black) – Connected, but authentication not in use

 (blue) – Connected and authenticated

Hold down your left mouse button while clicking this icon to see details of the last authentication that was performed over this connection. The information you see depends on your authentication method and access point, and may include the following:

- Result of your last connection attempt
- Type of authentication
- Elapsed time (since last connection)


- ▶ Cipher suite used to secure credential exchange
- ▶ Access point identification information

## Encryption Key Information

The encryption key information button indicates whether encryption keys are in use for this connection.

 (outline) – Data is not encrypted

 (black) – Data is encrypted using static keys

 (blue) – Data is encrypted using dynamic keys (802.1X)

Hold down this button to see the following information:

- ▶ Global encryption: The size (in bits) of global encryption keys
- ▶ Access point encryption: The size (in bits) of access point encryption keys

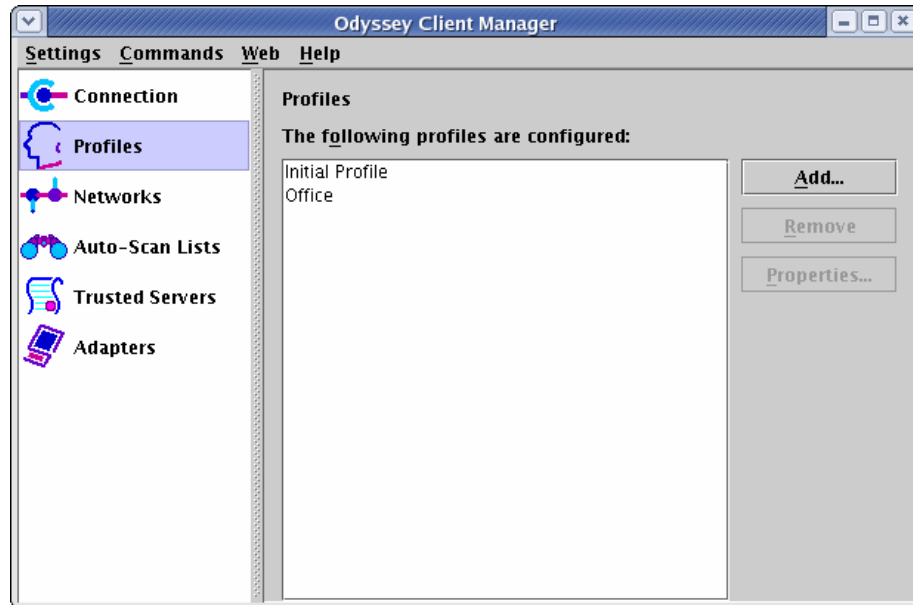
**NOTE:** A WEP encryption key has a secret part whose length is either 40 or 104 bits, and a 24-bit non-secret part that changes for each packet. Thus, the total key length is either 64 or 128 bits. Odyssey Client Manager reports the length of the secret part, which is either 40 or 104 bits.

## Profiles Panel

An Odyssey Client profile contains all the information that is necessary to authenticate you to the network. This includes information such as your identity (login name, and password or certificate) and the protocols by which you can be authenticated.

You can have different profiles for different networks. For example, you may have different login names or passwords on different networks, or you may use a password on one network, and a certificate on another.

The Profiles panel lists the profiles that you or your administrator have configured. When you first use Odyssey Client Manager, you may find a profile called **Initial Profile**, containing commonly used settings. Alternatively, your network administrator may have already created one or more profiles for you.



**Figure 4 Profiles Panel**

Each profile you configure is displayed in the list.

- ▶ To add a profile, click **Add**. The Add Profile dialog appears. Set the name for the new profile, configure the settings, and click **OK**.
- ▶ To remove a profile, select the profile and click **Remove**.
- ▶ To modify a profile, select the profile and click **Properties**, or double-click the profile. The [Profile Properties](#) dialog appears. Modify the settings and click **OK**.

## Profile Properties

The Add Profile dialog (or the Profile Properties dialog) allows you to configure a profile. It is displayed when you click **Add** (or **Properties**) from the Profiles panel.

When you add a profile to Odyssey Client, type a unique name for the profile in the **Profile name** field of the Profile Properties dialog. For example, you can type **Office** for the name of your profile to use for networks at your place of employment, and **Home** for your home network.

You cannot change the name of a profile after you save it. You can edit any of its other profile properties. You can also remove a profile and create a new one with a different name.

In addition to the profile name, you can specify the following information in a profile:

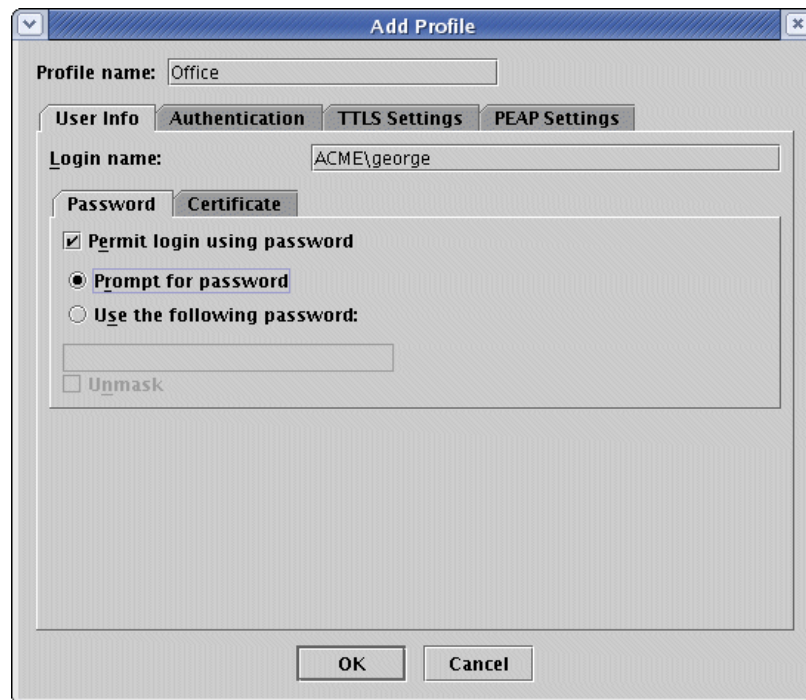
- ▶ Login name
- ▶ Password, certificate, or other user credentials
- ▶ A list according to preference of one or more authentication protocols to be used to authenticate you to the network

You can specify these using the four tabs of the Profile Properties dialog:

- ▶ User Info
- ▶ Authentication
- ▶ TTLS Settings
- ▶ PEAP Settings

## User Info

You can configure the name you use to log in, as well as your password, or certificate from the **User Info** tab.



**Figure 5** Password Subtab of the User Info Tab of the Add Profile Dialog

Enter your user name into the **Login name** field. This is the name that is presented to the network when you authenticate. If you authenticate against a Windows Active Directory, use the form, *domain\user\_name*, (for example, *Acme\george*). Otherwise, use a login name that matches the form of the user name as it is stored in the authentication database. See your network administrator for the required format.

Note the following:

- ▶ If you are logged into your network domain (as opposed to your machine), by default, Odyssey Client populates this field with the standard network form, *domain\user\_name*, where *user\_name* is your user name.
- ▶ If you are logged in to your client machine (as opposed to any network domain), Odyssey Client only populates this field with your user name.

It is possible that you must add some text after your login name for the purpose of routing your authentication to the proper server. For example, *acme\george@sales.acme.com*. Your network administrator can tell you how to

set this field correctly. The **User Info** tab has two sections that you can configure from the subtabs:

- ▶ **Password:** You must configure this section when you use authentication protocols that require or permit a password (for example, EAP-TTLS).
- ▶ **Certificate:** You must configure this section when you use authentication protocols that use a client-side certificate (for example, EAP-TLS).

## Password

You must configure passwords when you select authentication methods for this profile that require passwords. The following authentication methods require passwords:

- ▶ EAP-TTLS (except when used solely with certificate credentials)
- ▶ EAP-PEAP
- ▶ EAP-LEAP
- ▶ EAP-FAST
- ▶ EAP- MD5-Challenge

Check **Permit login using password** on the **Password** subtab of the **User Info** tab of the Profile Properties dialog to enable authentication methods that use your password for authentication.

When the time comes to authenticate, Odyssey Client can obtain your password in one of several ways:

- ▶ Select **Prompt for password** if you want Odyssey Client to prompt you when you start to connect to the network.
- ▶ Select **Use the following password** and enter a password in the box below, if you want Odyssey Client to save your password and use it each time you authenticate with this profile.

If you select **Prompt for password**, you are generally prompted only the first time that you are authenticated after startup. Odyssey Client remembers credentials and reuses them for the duration of your session. The credentials you enter apply only to a single profile. If you are authenticated using a different profile, you are prompted again.

You may also be prompted to enter your password when connecting to the network under some conditions, including when you accidentally enter an incorrect password or have any other type of authentication failure. This feature is in place, in part, so as to prevent accidental lockout due to the reuse of bad passwords. You may also be prompted to enter your password when connecting to the network on some occasions, including if you accidentally enter an incorrect password.

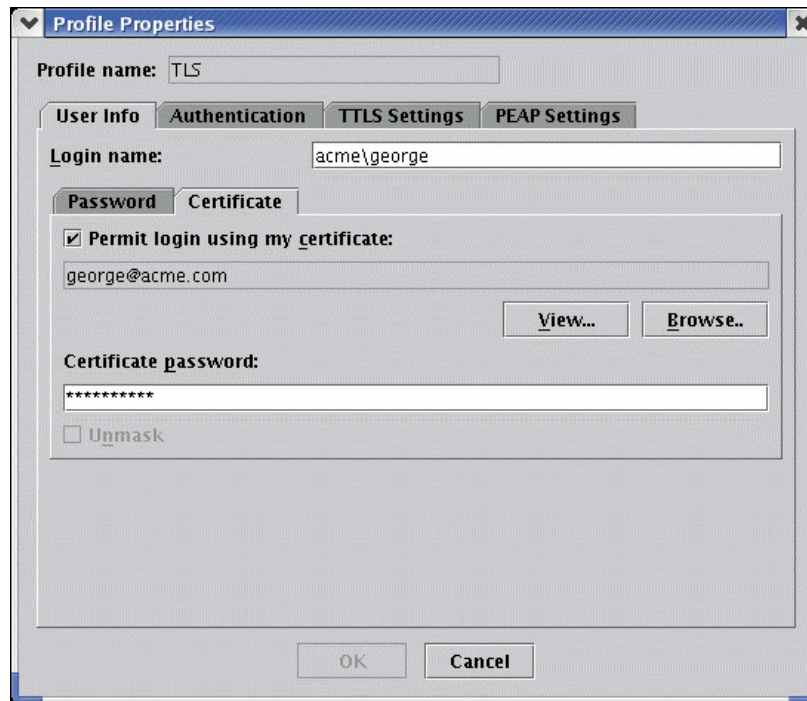
**NOTE:** When you are prompted for your password, you are given the option to bypass the Odyssey Client network connection. This option lets you use a wired network connection when it is available, without having to change your Odyssey Client wireless connection settings. To use this feature, click **Yes** when the prompt appears.

**NOTE:** You can return to the Connection panel to connect to a network using Odyssey Client at any time.

## Certificate

Odyssey Client reads your personal certificate information from your personal certificate store on your computer or device.

To use certificate credentials for authentication, specify them under the **Certificate** subtab of the **User Info**.



**Figure 6** Certificate Subtab of the User Info Tab of the Profile Properties Dialog

Note that you are required to select EAP-TLS as an authentication protocol for this profile to negotiate authentication using certificate credentials.

Check **Permit login using my certificate** to enable authentication methods that use your certificate for authentication.

You can click **Browse** to select a personal certificate from your computer. A list of your personal certificates appears. Select a certificate and click **OK**. Once you configure a certificate, you can click **View** to view the certificate.

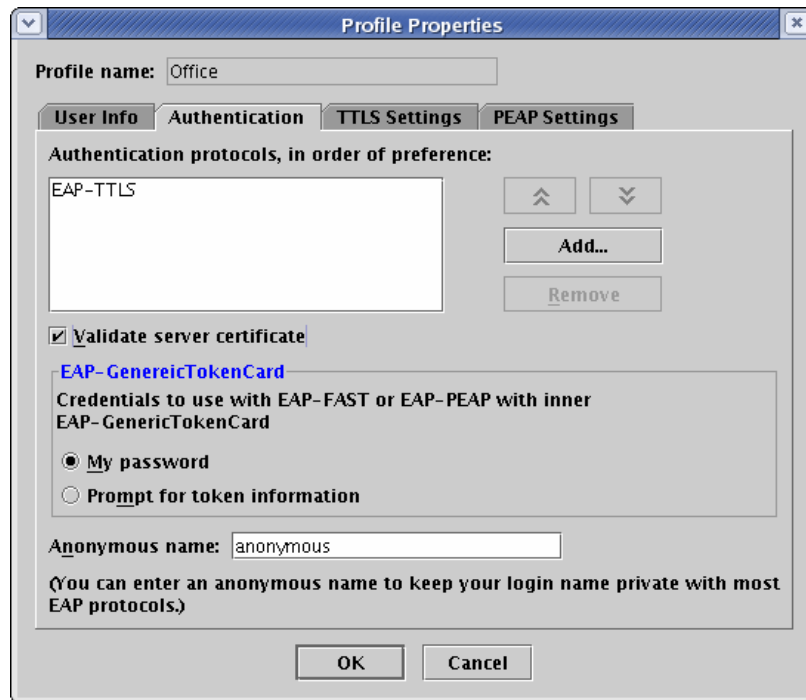
If the certificate requires a password, enter it in the **Certificate password** field.

**NOTE:** This is an advanced feature. Before you can create a profile that uses a personal certificate from your computer, you must install the certificate in the `current_user` store of your computer. See “Setting up Certificates” on page 47. Also check with your network administrator for more information on installing and selecting a user certificate for authentication if you require one.

## Authentication

You can specify network authentication protocols as well as EAP protocol-specific options from the **Authentication** tab of the Profile Properties dialog. The authentication

protocols you specify on the **Authentication** tab of the Profile Properties dialog are the outer authentication methods. Some of these protocols use encrypted credentials and require that you specify an inner authentication method as well.



**Figure 7** Authentication Tab of the Profile Properties Dialog

You can specify authentication-specific features of the profile from the **Authentication** tab. See the following topics:

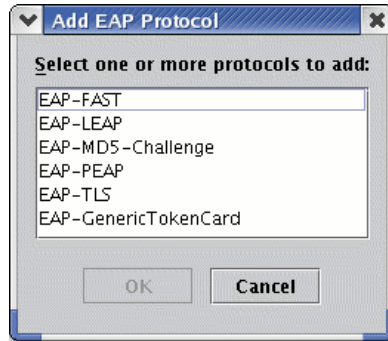
- ▶ [Select Authentication Protocols](#)
- ▶ [Validate the Server Certificate](#)
- ▶ [Set EAP-GenericTokenCard Options](#)
- ▶ [Set an Anonymous Name](#)

## Select Authentication Protocols

The **Authentication protocols** list displays the protocols that you have enabled for authentication. You may have a single authentication protocol in the list, or you may have several. If you have more than one, you can order them by preference. The ordering you choose affects the protocol that the server uses when it has more than one protocol in common with the ones you select here.

You have several options for managing authentication protocols:

- ▶ To add a protocol to the list, click **Add**. The Add EAP Protocol dialog ([Figure 8](#)) appears. Select one or more protocols to add, and click **OK**. You can select more than one protocol if you hold down CTRL on your keyboard as you select with your mouse. Note that any protocols you have already selected are not listed in this dialog.



**Figure 8** Add EAP Protocol

- ▶ To remove a protocol listed in the **Authentication** tab, select the protocol and click **Remove**.
- ▶ To reorder protocols, select a protocol, and use the up and down arrow buttons on the **Authentication** tab to reposition it.

**NOTE:** *EAP-TTLS, EAP-PEAP, and EAP-FAST all use inner (tunneled) protocols. EAP-FAST uses EAP-GenericTokenCard as its inner protocol. You can choose among one or more inner protocols for EAP-TTLS or EAP-PEAP. See “TTLS Settings” on page 34 and “PEAP Settings” on page 36.*

### Validate the Server Certificate

Certain protocols, such as EAP-TTLS, PEAP, and EAP-TLS, allow you to verify the identity of the authentication server as the server verifies your identity. This is called mutual authentication.

From the Trusted Servers panel, you can configure Odyssey Client with a certificate that is issued by a member of the same certificate chain that issued a certificate to the authentication server. See “Trusted Servers Panel” on page 46.

Check **Validate server certificate** (checked by default) to verify the identity of the authentication server based on its certificate when authenticating with EAP-TTLS, PEAP, and EAP-TLS. By checking this option, you must already have the root CA or intermediate CA for the server certificate chain installed in the trusted root or intermediate certificate store of your machine.

You should, as a general rule, check **Validate server certificate**. You have the option of turning off this important security precaution because there may be circumstances that require it, for example, if you are unable to configure trust because you do not have an intermediate root CA certificate installed on your machine. You should do so only if your network administrator instructs you to uncheck this option.

### Set EAP-GenericTokenCard Options

There are two circumstances under which EAP-GenericTokenCard can be the inner protocol for tunneled authentication:

- ▶ If you select EAP-FAST as an outer authentication method on the **Authentication** tab, since EAP-GenericTokenCard is the inner authentication protocol used with EAP-FAST.

- ▶ If you choose EAP-GenericTokenCard as the inner protocol for EAP-PEAP

If you use EAP-GenericTokenCard as one of your inner authentication methods, then the **EAP-GenericTokenCard** settings under the **Authentication** tab apply. These settings allow you to choose to use your password credentials or your token card ID for authentication:

- ▶ Select **My password** if your network requires that you use the password credentials assigned with this profile instead of your token card ID for authentication.
- ▶ Select **Prompt for token information** if your network requires that you use your token ID for authentication.

**NOTE:** *These token card settings do not apply when you configure EAP-GenericTokenCard as an inner authentication method for EAP-TTLS (with EAP). Additionally, these settings do not apply when you choose EAP-GenericTokenCard as an outer authentication method from the **Authentication** tab.*

## Set an Anonymous Name

With EAP-TTLS, EAP-PEAP, and EAP-FAST, you can appear to log in anonymously, while passing your actual login name through an encrypted tunnel. As a result, not only are your credentials secure from eavesdropping, but your identity is protected as well.

You can have two identities with when you use any of these three protocols:

- ▶ An inner identity, your actual login name, which is taken from the **Login name** field in the **User Info** tab.
- ▶ An outer identity, which can be completely anonymous. You can set your outer identity in the **Anonymous name** field.

Note the following:

- ▶ Anonymous outer identities are implemented only when you fill in **Anonymous name**.
- ▶ When you leave **Anonymous name** blank, your inner identity is also used as your outer identity.

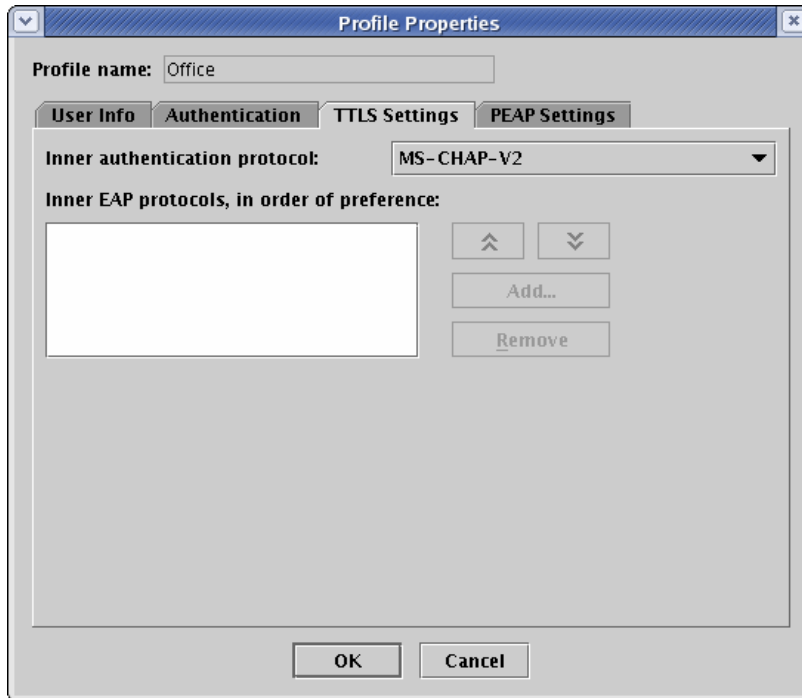
As a general rule, set **Anonymous name** to anonymous, its default value. Your network administrator can tell you how to configure this field correctly:

- ▶ In some cases, you are required to add additional text. For example, if this outer identity is used to route your authentication to the proper server, you may be required to use a format such as anonymous@acme.com.
- ▶ It is possible that anonymous EAP-PEAP authentication does not work with your network authentication server. If that is the case, you must leave **Anonymous name** blank.

**NOTE:** *Your outer identity can be anonymous if your list of configured authentication protocols for this profile only includes EAP-TTLS, EAP-PEAP, and/or EAP-FAST. If you enable any other protocols, Odyssey Client cannot keep your identity private, and the **Anonymous name** field is disabled.*

## TTLS Settings

The **TTLS Settings** tab lets you configure the use of EAP-TTLS as an authentication protocol. These settings are relevant only when you select EAP-TTLS as one of your authentication protocols in the **Authentication** tab.



**Figure 9** TTLS Settings Tab of the Profile Properties Dialog

EAP-TTLS works by creating a secure encrypted tunnel through which you may present your credentials to the authentication server. If you use EAP-TTLS with password credentials, an inner authentication protocol is used to complete the authentication. See “EAP-TTLS” on page 11 for more information on this protocol.

See the following topics:

- ▶ “Select an Inner Authentication Protocol” on page 34, for EAP-TTLS authentication with password credentials
- ▶ “EAP as an Inner Authentication Protocol” on page 35, for EAP-TTLS authentication with password credentials using an inner EAP method

### Select an Inner Authentication Protocol

Use the **Inner authentication protocol** list to select the inner authentication protocol you want to use. You can select any of the following:

- ▶ PAP
- ▶ CHAP
- ▶ MS-CHAP
- ▶ MS-CHAP-V2

- ▶ PAP/Token Card
- ▶ EAP

The most commonly used protocol is MS-CHAP-V2. It allows you to be authenticated against user databases.

PAP/Token Card is the protocol to use with token cards. When you use PAP/Token Card, the password value you enter into the Password dialog is never cached, since any token-based password is good for one use.

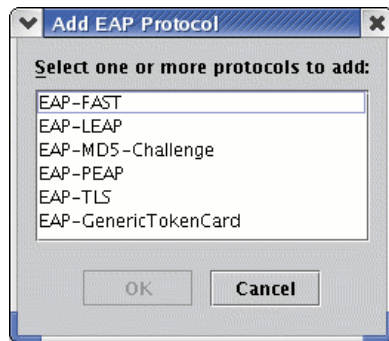
Check with your network administrator to determine which inner authentication protocols can be used on your network.

### EAP as an Inner Authentication Protocol

If you select EAP as your inner authentication protocol, you must configure the **Inner EAP protocols** list on the **TTLS Settings** tab of the Profile Properties dialog with one or more protocols.

To add a protocol to the list of inner EAP protocols, follow these steps:

- 1 Click **Add** on the **TTLS Settings** tab of the Profile Properties dialog. The Add EAP Protocol dialog (Figure 10) appears.



**Figure 10** Add EAP Protocol

- 2 Select one or more protocols to add, and click **OK**.

You can select more than one protocol if you hold down CTRL on your keyboard as you select with your mouse. Note that only the protocols you have not already added are available.

To remove a protocol listed on the **TTLS Settings** tab of the Profile Properties dialog, follow these steps:

- 1 Select the protocol you want to remove.
- 2 Click **Remove**.

To reorder protocols, follow these steps:

- 1 Select a protocol whose position you want to move.
- 2 Use the up and down arrow buttons on the **TTLS Settings** tab of the Profile Properties dialog to reposition the protocol on the list.

## PEAP Settings

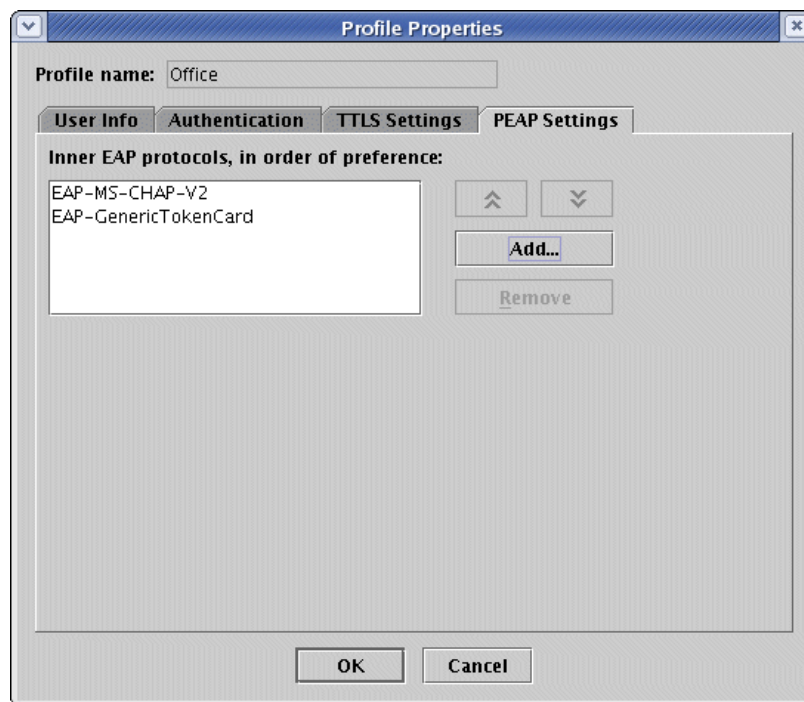
If you select EAP-PEAP as an authentication method in the **Authentication** tab, then you can use any of the following inner EAP authentication methods:

- ▶ EAP-MS-CHAP-V2
- ▶ EAP-GenericTokenCard

You can add, reorder, or remove any EAP-PEAP inner protocols from the **PEAP Settings** tab of the Profile Properties dialog.

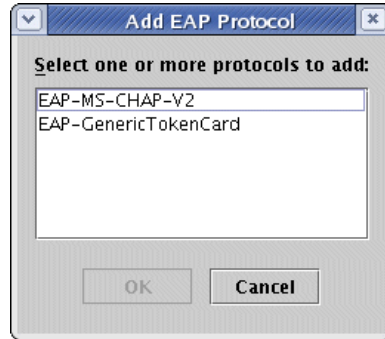
To add, reorder, or remove any inner authentication methods used with EAP-PEAP, follow these steps:

- 1 Click the **PEAP Settings** tab.



**Figure 11** PEAP Settings Tab of the Profile Properties Dialog

- 2 To add a new inner protocol for EAP-PEAP, click **Add**. The Add EAP Protocol dialog (Figure 12) appears.
  - a Select one or more protocols to add.
  - b Click **OK**. Note that any protocols you have already selected are not listed in the Add EAP Protocol dialog.

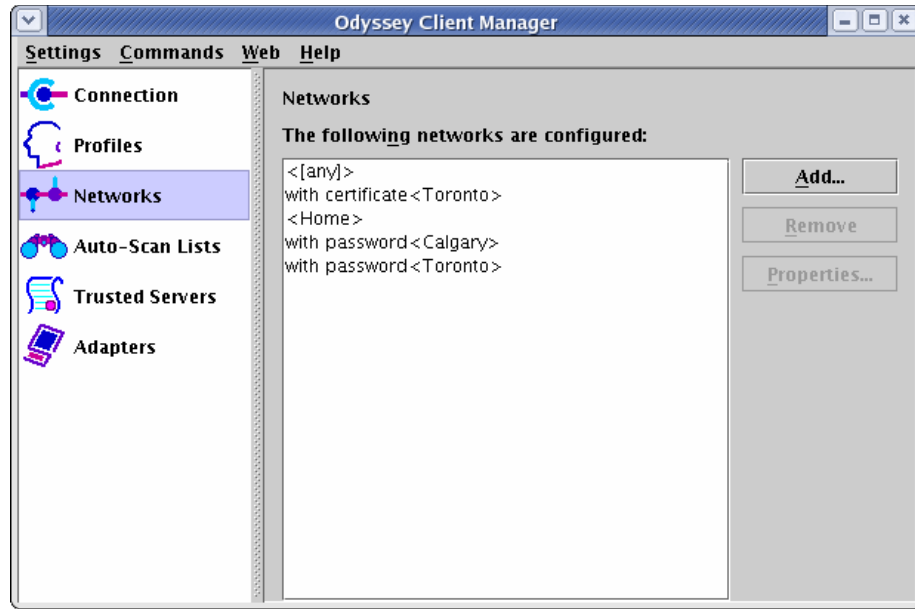


**Figure 12** Add EAP Protocol Dialog

- 3** Reorder protocols, as required. When you allow more than one inner protocol, you should order the protocols listed under **PEAP Settings** according to your preferences (requirements). Use the up and down arrows to move a selected protocol around in the list.
- 4** If you select EAP-GenericTokenCard as one of your PEAP inner authentication methods, then you can configure the **EAP-GenericTokenCard** settings under the **Authentication** tab. These settings allow you to choose to use your password credentials or your token card ID for authentication.
- 5** You may want to remove one or more of the inner protocols listed. Select any protocols you want to remove under the **PEAP Settings** tab, and click **Remove**.
- 6** Click **OK** when you are done creating or modifying the profile configuration.

## Networks Panel

You can use the Networks panel to configure settings for connecting to any number of wireless networks.



**Figure 13** Networks Panel

Each network that you configure is listed in the panel. You can perform the following tasks in the Networks panel:

- ▶ To add a network, click **Add**. The Add Network dialog (Figure 14) appears. Configure the settings for the new network and click **OK**.
- ▶ To remove a network, select the network and click **Remove**.
- ▶ To modify the settings for a network, select the network and click **Properties**, or double-click the network name. The Network Properties dialog appears. Modify the settings and click **OK**.

## Network Titles

The titles of networks that appear in the Networks panel are coded with special formatting:

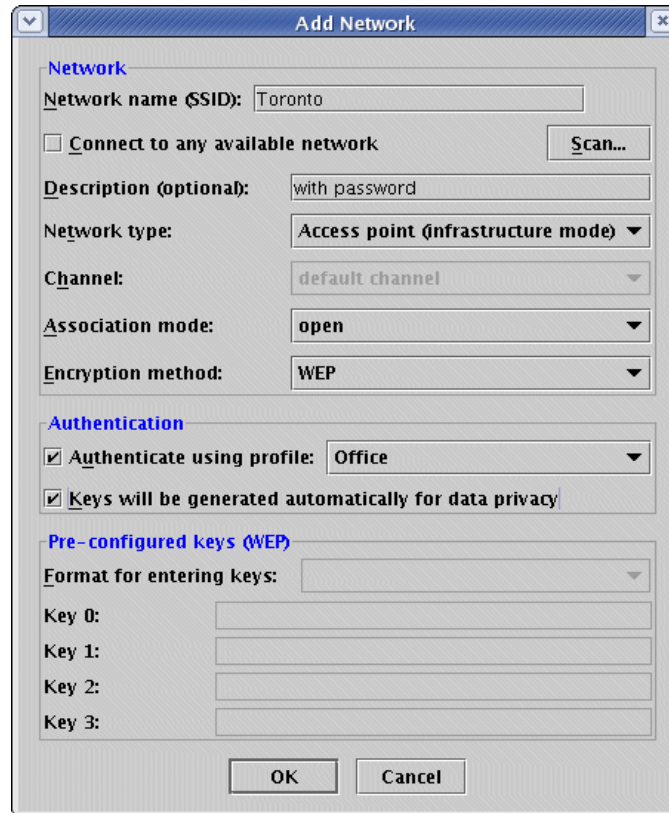
- ▶ The name of the network appears in angled brackets. If the name **[any]** is listed in angled brackets as an entry in the list of networks, then you can use this network configuration to connect to any available wireless network.
- ▶ The description of the network precedes the name. This description comes from the optional **Description** field in the Network Properties dialog. You can add your own description to any network you configure. This helps you to distinguish networks.

Network names are arbitrary text chosen by an administrator, so two unrelated networks can have the same name. You can use the description field to distinguish between networks that have the same name.

You can also use the network description field to distinguish connections to the same network using different profiles. For example, you may want to use different credentials at different times.

## Network Properties

You can configure wireless network settings in the Add Network (or Network Properties) dialog when you click **Add** (or **Properties**) from the Networks panel.



**Figure 14** Add Network Dialog

You can configure the network attributes according to the following topics:

- ▶ Network Fields
- ▶ Authentication Fields
- ▶ Preconfigured Keys (WEP, WPA2, or WPA)

### Network Fields

You can perform tasks under the **Network** field that are described in the following topics:

- ▶ Specify the Network Name.
- ▶ Scan for a Network.
- ▶ Configure Odyssey Client to Connect to any Available Network.
- ▶ Specify a Description of the Network.
- ▶ Specify the Network Type.
- ▶ Specify the Channel.

- ▶ Specify the Association Mode.
- ▶ Specify an Encryption Method for the Selected Association Mode.

## Specify the Network Name

Set **Network name (SSID)** to the name of the wireless network. The network name may be up to 32 characters long and is case-sensitive. You must enter this name correctly to connect.

## Scan for a Network

You can type the name of the network, or you can click **Scan** to select from a list of all currently visible networks. When you are in the vicinity of the network you are configuring, using the **Scan** button is easier than typing, and guarantees that the network name is set correctly.

Note that only access points that transmit beacons are visible to you when you use the **Scan** button.

## Configure Odyssey Client to Connect to any Available Network

Odyssey Client Manager provides a special network configuration called **[any]**. The **[any]** network connects to any available network, regardless of its name. The **[any]** network is useful when you are wandering through conferences, hotels, or other locations that provide network access. When you select the **[any]** network from the Connection panel, you can connect to such networks without having to configure them individually.

To configure an **[any]** network, check **Connect to any available network**.

Although you can use WEP keys and profiles with **[any]**, the more common (default) practice is to use **[any]** without 802.11 or 802.1X authentication.

## Specify a Description of the Network

You may want to use network descriptions to provide more information about your network than its SSID provides. You can also use the description to differentiate similar network names. You have the option to enter a description of this network in the **Description** field. The text you enter into this field allows two networks with the same name to remain distinct on the Odyssey Client Manager display. See [“Networks Panel” on page 37](#) for an example.

## Specify the Network Type

If you did not use the **Scan** button to select your network, you must specify the type of network by choosing one of the options from the **Network type** drop-down list.

- ▶ Select **Access point (infrastructure mode)** if this network uses access points to provide connectivity to the corporate network or the internet. This is the most common setting.
- ▶ Select **Peer-to-peer (ad-hoc mode)** to set up a private network with other PCs.

## Specify the Channel

If you select an peer-to-peer (ad-hoc) network type (see [“Specify the Network Type” on page 40](#)), then you must select a channel on which all peers share data. You can choose the default channel, or select a channel from the **Channel** list.

## Specify the Association Mode

Before authentication can take place, your client must associate to an access point. The association mode that is required of you depends on your access point hardware, and how it is configured. Your network administrator can help you configure the association mode that is required for your network.

See [“Wired-Equivalent Privacy” on page 7](#) and [“Wi-Fi Protected Access and its Encryption Methods” on page 8](#) for more information on these encryption and association mode choices.

You can choose one of the following association modes:

- ▶ **Open**, for connecting to a network through an access point or switch that implements 802.1X authentication. Choose this mode if you are not required to select shared mode or Wi-Fi Protected Access (WPA).
- ▶ **Shared**, for connecting to a network through an access point that requires at least one preconfigured wired-equivalent privacy (WEP) key for association.
- ▶ **WPA**, for connecting to a network through an access point that implements WPA.
- ▶ **WPA2**, for connecting to a network through an access point that implements WPA2, the second generation of WPA that satisfies 802.11i.

## Specify an Encryption Method for the Selected Association Mode

Your choice of encryption method also depends on the access point requirements. The choices available to you depend on the association mode you choose. See [“Wired-Equivalent Privacy” on page 7](#) and [“Wi-Fi Protected Access and its Encryption Methods” on page 8](#) for more information.

You have the following options:

- ▶ **None**, for using 802.1X authentication without WEP keys. This option is available to you only when you configure access point association in open mode. This is a typical setting to use for wireless hotspots.
- ▶ **WEP**, for using WEP keys for data encryption. This is an option for open mode association, and is required when you associate in shared mode. When you use WEP encryption, you must fill in at least one preconfigured WEP key at the bottom of the Add Network dialog, unless you authenticate using a profile and check **Keys will be generated automatically for data privacy**. You must choose WEP encryption when the access points in your network require shared mode association with WEP keys, or when your access points require WEP encryption.
- ▶ **TKIP**, for using the temporal key integrity protocol. Choose this option when the access points in your network require WPA or WPA2 association and are configured for TKIP data encryption.

- ▶ **AES**, for using the advanced encryption standard protocol. Choose this option when the access points in your network require WPA or WPA2 association, and are configured for AES data encryption. If your client hardware and access point support AES, use AES encryption when you associate in WPA2 or WPA mode.

## Authentication Fields

You can use the authentication fields to specify whether to use 802.1X authentication for the network, and how to generate the encryption keys. See the following topics for information on the fields in the **Authentication** section of the Network Properties dialog:

- ▶ [Specify a Profile for the 802.1X Network Connection](#)
- ▶ [Specify Automatic Key Generation for the 802.1X Network Connection](#)

### Specify a Profile for the 802.1X Network Connection

If the wireless network you are configuring requires that you authenticate using your personal credentials, check **Authenticate using profile**, and select the profile to use for authentication from the drop-down list at the right. You must have already configured a profile appropriate for authenticating to this network.

When you check **Authenticate using profile**, and then select a profile you listed on the Profiles panel, Odyssey Client performs an 802.1X authentication using the options configured on the selected profile.

**NOTE:** *If you configure a profile for this network that uses MD-5 Challenge or EAP-GenericTokenCard as an outer authentication method, then you must include a static WEP key for data encryption to authenticate using 802.1X. See [“Specify Preconfigured Keys for WEP”](#) on page 43.*

### Specify Automatic Key Generation for the 802.1X Network Connection

Check **Keys will be generated automatically for data privacy** if the authentication method specified in the profile results in the creation of dynamic WEP keys for use between your PC and the access point. Certain authentication methods, such as EAP-TTLS, EAP-PEAP, EAP-FAST, and EAP-TLS, generate keys. Others do not. If you associate this network with a profile that uses EAP-TTLS, EAP-PEAP, EAP-FAST, or EAP-TLS to authenticate, check this box. You can use any of these authentication methods if your access point implements 802.1X authentication. This option is more secure than using static (preconfigured) keys. This option is available with all encryption methods (other than **None**), as long as you are not associating in shared mode. Leave this option unchecked if you are required to use preconfigured WEP keys, or, in the case of WPA association, a preshared key.

## Preconfigured Keys (WEP, WPA2, or WPA)

The wireless network may require that you preconfigure WEP keys, or that you preshare a passphrase in the case of WPA or WPA2 association.

If you do not check **Keys will be generated automatically for data privacy**, you can enter keys in the lower portion of your network properties description, according to the association method you select.

### Specify Preshared Keys for WPA or WPA2

If you associate in WPA or WPA2 mode, and you do not generate encryption keys automatically when you associate an authentication profile to the network connection, then you must supply a preshared 8–63 character ASCII passphrase in the **Passphrase** field. This passphrase is used as a seed to generate the required keys. When you use a passphrase, you do not authenticate with a RADIUS server.

**NOTE:** *If you supply a 64-character passphrase that could form a hexadecimal number, Odyssey interprets it as a 32-byte hexadecimal value used as the master key.*

### Specify Preconfigured Keys for WEP

WEP keys serve the following purposes:

- ▶ WEP keys allow you to associate with an access point before a connection can be established (shared mode).
- ▶ WEP keys encrypt data between your PC and the access point (or other PCs in a peer-to-peer network).

See “Wired-Equivalent Privacy” on page 7.

You must configure at least one WEP key if you configure the following type of network configurations:

- ▶ You associate in shared mode. See “Specify the Association Mode” on page 41.
- ▶ You select WEP encryption for the open association mode and you do not generate encryption keys automatically. See “Specify an Encryption Method for the Selected Association Mode” on page 41.

If the wireless network uses 802.1X authentication and dynamic WEP keys are generated (if you check **Authenticate using profile** and **Keys will be generated automatically for data privacy**), then you do not need to enter preconfigured WEP keys for data privacy. However, it is possible, though not typical, to use preconfigured WEP keys for authentication in addition to 802.1X. For example, EAP-MD5 does not generate WEP keys for data encryption, so you must supply an encryption WEP key when your profile is set to authenticate with this method.

Enter the WEP keys in fields **Key 0** through **Key 3**. The values entered here must match those of the access points or peer computer to which you connect. It is most common for Key 0 to be used, although your network may require other keys as well. You can enter keys either as ordinary text characters (ASCII) or hexadecimal characters.

WEP keys are either 40 or 104 bits long. This corresponds to either 5 or 13 characters when you enter them as ASCII characters, or 10 or 26 characters when you enter them as hexadecimal digits.

**Table 2. WEP Key Specifications**

Bits in the Key	ASCII Characters	Hexadecimal Digits
40	5	10
104	13	26

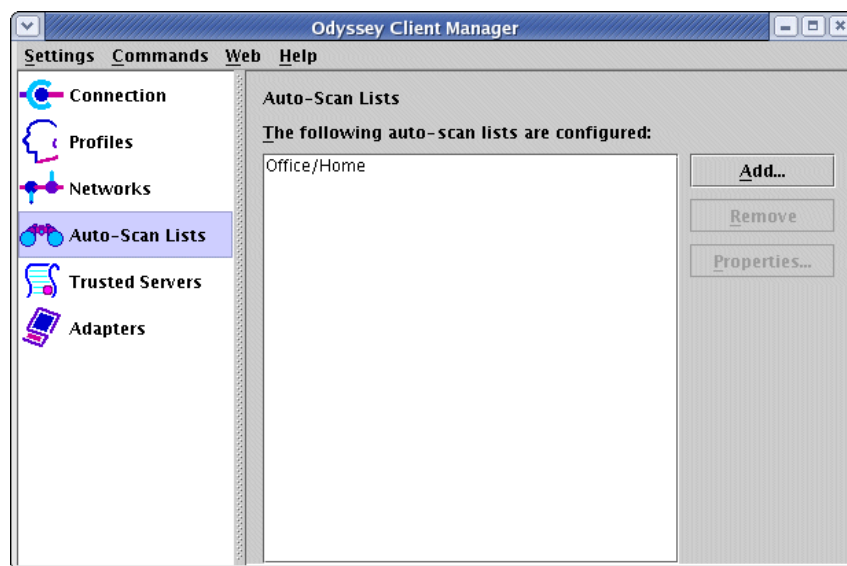
To enter any preconfigured WEP keys, follow these steps:

- 1 In **Format for entering keys**, select either **ASCII characters** or **hexadecimal digits**, depending on how you want to enter the keys.
- 2 Type each WEP key that you want to preconfigure into the text fields **Key 0** through **Key 3**, according to the specifications in [Table 2](#).

## Auto-Scan Lists Panel

You can associate an ordered list of wireless networks that you configure in the Networks panel with an *auto-scan list*. You can use auto-scan lists to attempt connection to any of the networks available in the ordered list. You may want to use this feature if you are moving your client machine between locations that access different networks. For example, you may want to associate your home network and your office network with the same auto-scan list, so that you do not have to change your network connection specification each time you change location.

When you specify a connection on the Connection panel to an auto-scan list rather than a single network, Odyssey scans sequentially through the listed networks for an available network.



**Figure 15 Auto-Scan Lists Panel**

Although you can create new lists of networks at any time, each of the individual networks in a list must have been previously configured with the Networks panel.

You can perform the following tasks in the Auto-Scan Lists panel:

- ▶ You can add an auto-scan list by clicking the **Add** button. The Add Auto-Scan List dialog appears.

**NOTE:** See also “PAC Manager” on page 56 for information on creating an auto-scan list that is prepended to any network connection you configure on the Connection panel of the Odyssey Client Manager.

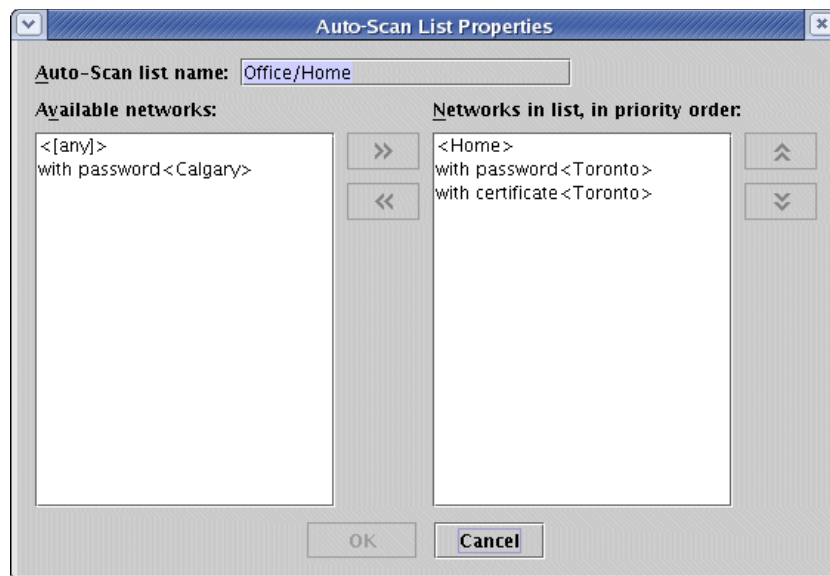
- ▶ You can remove an auto-scan list by select it from the list and clicking the **Remove** button.
- ▶ You can modify an auto-scan list by selecting it and clicking the **Properties** button, or by double-clicking the auto-scan list name. The Auto-Scan List Properties dialog appears.
- ▶ You can view the names of the auto-scan lists you create.

**NOTE:** Test each network connection for each network in your auto-scan list separately. If you misconfigure a network connection on the auto-scan list so that authentication fails at every connection attempt, Odyssey Client does not skip that network to try other networks on the list. To test a single selected network connection, go to the Connection panel of the Odyssey Client Manager and check **Connect to network** after selecting the network you want to test.

## Auto-Scan List Properties

You can use auto-scan lists to manage lists of the wireless networks that you configure with the Networks panel.

You can add (or edit) an auto-scan list when you click the **Add** (or **Properties**) button from the Auto-Scan Lists panel. The Add Auto-Scan List (Auto-Scan List Properties) dialog [Figure 16](#) appears.



**Figure 16** Auto-Scan List Properties Dialog

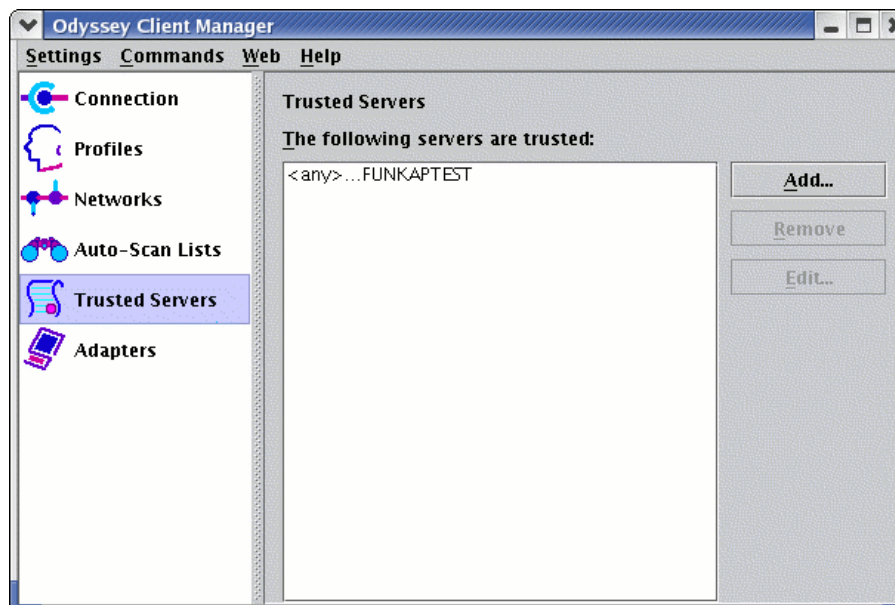
To create an auto-scan list, follow these steps:

- 1 Provide the name for the list in the **Auto-Scan list name** field. You must fill this field in before you click **OK**. You cannot choose a name you have already used for another auto-scan list, and you cannot edit this name later when you click the **Properties** button after selecting this auto-scan list from the Auto-Scan Lists panel.
- 2 Select networks for your auto-scan list from the list of configured networks listed under **Available Networks** on the left. Use the right arrows to move networks from the left to the **Networks in list, in priority order** on the right. This is your set of auto-scan networks.
- 3 Order your selected networks according to the frequency with which you expect to connect to them. Place your most frequently used networks at the top of the list. A network on this list is considered to be *preferred* as compared with the networks listed below it. You can select one or more networks and use the up and down arrows to reorder the list.

In general, you increase likelihood of connection to a given network in the list by moving it toward the top of the list.

## Trusted Servers Panel

You can configure trusted authentication servers for use with EAP-TTLS, EAP-TLS, or EAP-PEAP authentication from the Trusted Servers panel of the Odyssey Client Manager.



**Figure 17** Trusted Servers Panel

**NOTE:** To configure a trusted server with Odyssey Client, the root CA or intermediate CA for the server certificate chain must be installed in the trusted root or intermediate certificate store.

## Setting up Certificates

There are three types of certificates used by Odyssey Client:

- ▶ Trusted root certificates
- ▶ Intermediate CA certificates
- ▶ Personal certificates

The certificate files must be copied into specific folders under your home directory.

### Trusted Root Certificates

If you use TLS, TTLS, or PEAP, you need a Trusted Root CA certificate. This certificate must be in DER-encoded (Distinguished Encoding Rules) format, have the file extension `.cer`, and be copied into the folder `/home/<username>/.fsw/root/`.

### Intermediate Certificates

You may also use an Intermediate CA certificate with those EAP protocols. An Intermediate CA certificate has the same file format and extension as a trusted Root certificate but it goes in the folder `/home/<username>/.fsw/ca/`.

### Personal Certificates

If you use TLS, you need a personal certificate. A personal certificate has two files representing a public part and a private part. The public part is a DER-encoded file with the file extension `.cer`, and the private portion is a PKCS12 encoded file with the file extension `.pfx`. Both files go into the folder `/home/<username>/.fsw/my/`. The prefix for the pair of certificates files must be the same — for example `bob.cer` and `bob.pfx`.

After certificates have been installed they will be visible in the UI and can be used in user's the configuration. If you install the certificate files while the service and Odyssey Client are both running, toggle the checkbox in the Connection panel to make Odyssey check immediately for new certificates.

When you configure Odyssey Client to trust a server, you must specify the name of the server and the certificate chain to which it belongs. You also have the option to allow Odyssey Client to trust any server that bears a specified signed certificate.

See the following topics for configuring trust:

- ▶ [“Configuring Trust” on page 48](#)
- ▶ [“Untrusted Servers” on page 50](#)

See the following topics for information on certificates and the protocols that use them:

- ▶ [“Extensible Authentication Protocol” on page 9](#)
- ▶ [“Certificates” on page 10](#)

## Configuring Trust

You have two options in creating your list of trusted servers:

- ▶ You can allow any server that bears a specified signed certificate to be trusted. With this method, you must specify a certificate from any certificate authority in your certificate authority chain. This could be the certificate of a root or an intermediate certificate authority.
- ▶ You can specify a list of servers to be trusted using domain names. To do this, you must specify the following two items:
  - ▷ The authentication server or intermediate CA server domain name, or the ending of the domain name (for example, `acme.com`).
  - ▷ A certificate from any certificate authority in your certificate authority chain. This could be the certificate of a root or an intermediate certificate authority.

### Adding a Trusted Server Entry

When you click **Add** from the Trusted Servers panel, the Add Trusted Servers Entry dialog appears.



**Figure 18** Trusted Servers Properties Dialog

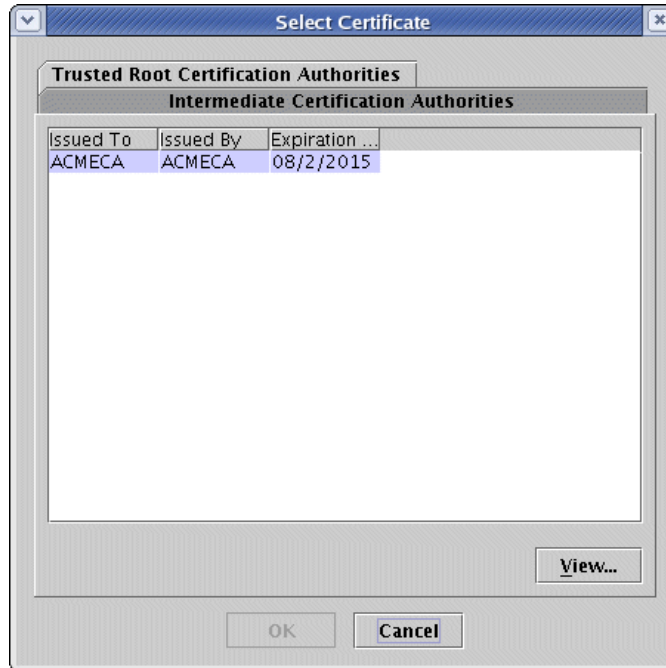
You can trust all servers whose certificates are issued by a specified (root or intermediate) CA, or you can use an intermediate CA or authentication server domain name to filter the certificate chain when you install the certificate that specifies the issuer of the trusted server certificates.

Follow these steps to configure server trust:

- 1** You can configure trust for any server issued a specified signed certificate, or you can specify one or more servers to be trusted using domain names, when those servers are issued a specified signed certificate:
  - ▷ To allow all servers issued a specified signed certificate to be trusted, check **Trust any server with a valid certificate regardless of its name**.
  - ▷ To specify servers by name, enter the identity of the trusted server in the **Server name must end with** field.
- 2** Set the **Server certificate must be issued by** field to the name of the certificate authority that must have directly or indirectly issued the server certificate. This field is set automatically when you select a (root or intermediate) CA-issued certificate.

The name that appears in this field need not be the name of the certificate authority that directly issued the server certificate. The server certificate may be issued by any authority in the chain. To set this field, follow these steps:

- a** Click **Browse** to get a list of certificates. The Select Certificate dialog (Figure 19) appears.
- b** Select the required certificate and click **OK**.



**Figure 19** Select Certificate Dialog

- 3** Click **OK** to close the Add Trusted Servers Entry dialog.

## Server Identity

Each server has an identity that uniquely identifies it, and that name is normally contained in the `Subject CN` field of the server certificate.

A server identity may end with the name of a larger administrative domain to which the server belongs. For example, the Acme company might have a domain name, such as `acme.com`. The company might also have authentication servers that are identified as `auth1.acme.com`, `auth2.acme.com`, and `auth3.acme.com`. In this case, Acme could configure its server certificates with a common name (`acme.com`), and fill in the **Server name must end with** field with `acme.com`.

As in this example, by specifying the ending for a server name, you can configure trust for all the servers in an organization with a single entry.

## Removing a Trusted Server Entry

To remove an entry from the trusted servers list, select the entry from the Trusted Servers panel and click **Remove**.

## Editing a Trusted Server Entry

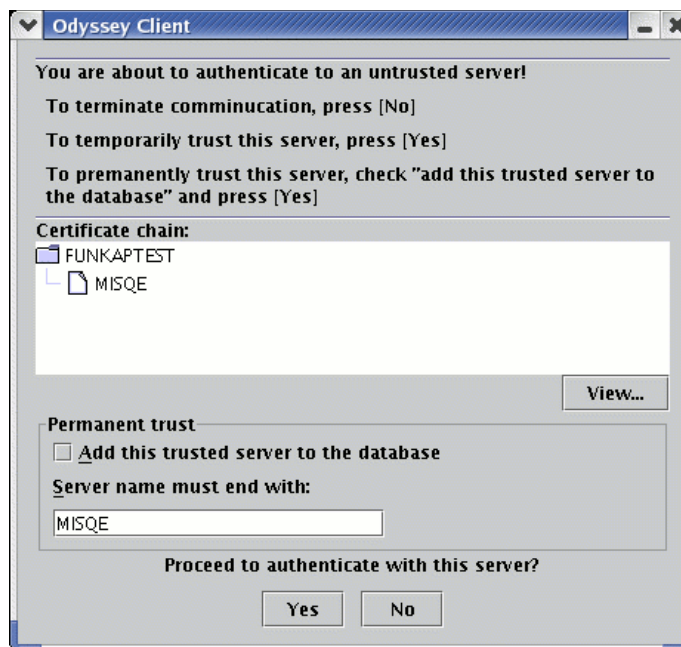
To edit an entry in the trusted servers list, select the entry from the Trusted Servers panel and click **Edit**. The Trusted Server Properties dialog appears, from which you can modify the server domain, and select a different certificate according to the directions in “Adding a Trusted Server Entry” on page 48.

## Untrusted Servers

Under the following conditions, you are given the option to trust a previously untrusted server during network authentication:

- ▶ You have enabled temporary trust.
- ▶ The authenticating profile mandates server validation.
- ▶ The trusted root certificate authority that issued the server certificate (in the example shown below, the certificate is issued by `AcmeRootCA`) is also the trusted root CA of a certificate installed on your client machine.

If this is the case, dialog such as the one in Figure 20 appears while you are authenticating to the network.



**Figure 20** Service Dialog for a Connection to an Untrusted Server

This service dialog shows the entire certificate chain between the authentication server and a trusted root certificate authority. To see detailed information about any certificate in the chain, select the certificate and click **View**.

If you want to trust this server temporarily while you authenticate and connect to the network, click **Yes**. Otherwise, click **No**. You may be asked to type in your password, depending on the profile you set up for this connection. If you click **Yes**, temporary trust is sustained until you restart Odyssey Client.

If you want to trust this server permanently by adding it to the list of trusted servers on the Trusted Servers panel (Figure 17), check **Add this trusted server to the database** and click **Yes**. The server is added to the list of trusted servers, using the name shown in the **Server name must end with** field (see “Adding a Trusted Server Entry” on page 48). You may edit the server name. For example, if the server name is `auth2.acme.com`, you can change it to `acme.com` if you want to trust all authentication servers belonging to the `acme.com` domain.

## Adapters Panel

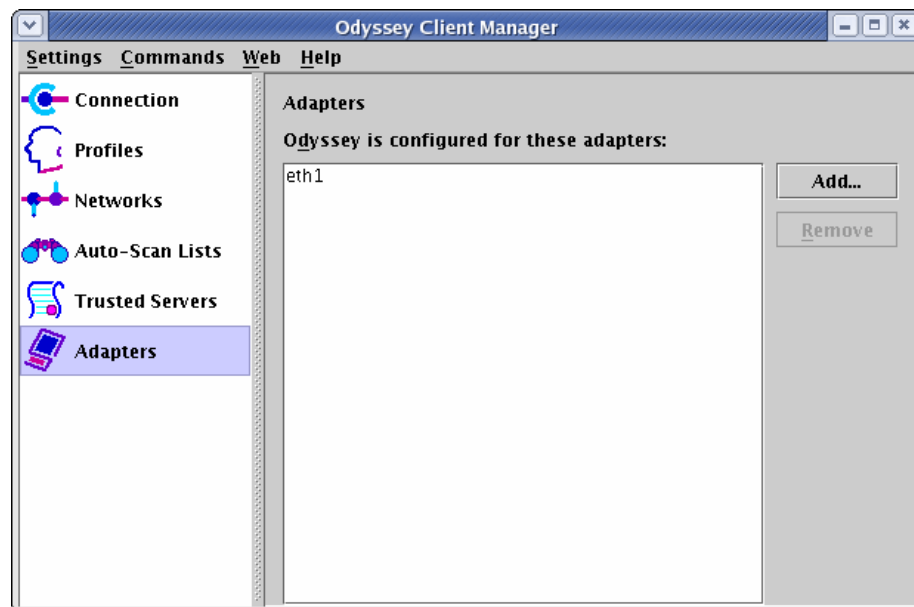
You can select one or more network adapters (interface cards) for wired or wireless networking from the Adapters panel. You can select more than one adapter if you hold down CTRL on your keyboard as you select entries with your mouse.

The Adapters panel lists all the wireless and wired adapters that are configured in Odyssey Client. Most likely, you have configured a single adapter. However, you may configure more than one adapter.

You can use the Adapters panel for the tasks described in the following topics:

- ▶ “Adding a Wireless or Wired Adapter” on page 52
- ▶ “Removing an Adapter from the List of Adapters” on page 52

**NOTE:** Your adapter must be installed on your system before you can configure Odyssey Client to use it.



**Figure 21** Adapters Panel

## Adding a Wireless or Wired Adapter

To add a wireless or wired adapter that Odyssey Client has not yet recognized, follow these steps from the Adapters panel of Odyssey Client Manager:

- 1 Click **Add**. The Add Adapter dialog (Figure 22) appears. The Add Adapter dialog displays a list of all network adapters that are installed on your PC (except for the ones Odyssey Client is already configured to use).



Figure 22 Add Adapter Dialog

- 2 Select the **Wireless** or the **Wired 802.1X** tab. Note that only adapters that you have not yet added to the Adapters panel are displayed.
- 3 Select the desired adapter from the list and click **OK**.

**NOTE:** The adapters that you select under the **Wireless** tab are used for wireless connections, and those that you select under the **Wired 802.1X** tab are used for wired connections. In most cases, Odyssey Client Manager can distinguish between wireless and non-wireless network adapters. However, in certain cases, it cannot. If you do not see your wireless adapter in the list, select **All Adapters**. Make sure that each of the adapters you select under the **Wireless** tab is wireless. You cannot configure Odyssey Client for wireless connections unless you have a wireless adapter. You must configure wired adapters from the **Wired 802.1X** tab.

## Removing an Adapter from the List of Adapters

To remove an adapter from the list of adapters in the Adapters panel, select the adapter you want to remove and click **Remove**. When you remove an adapter, Odyssey Client stops using it. The adapter is still installed on your system, but operates as if Odyssey Client is not present.

## Settings Menu

The following menu items are available from the **Settings** menu:

- ▶ Preferences
- ▶ Security Settings

- ▶ PAC Manager
- ▶ Enable/Disable Odyssey
- ▶ Close

## Preferences

You can change some operational preferences for Odyssey Client by selecting the **Settings > Preferences** command. The Odyssey Preferences dialog appears.



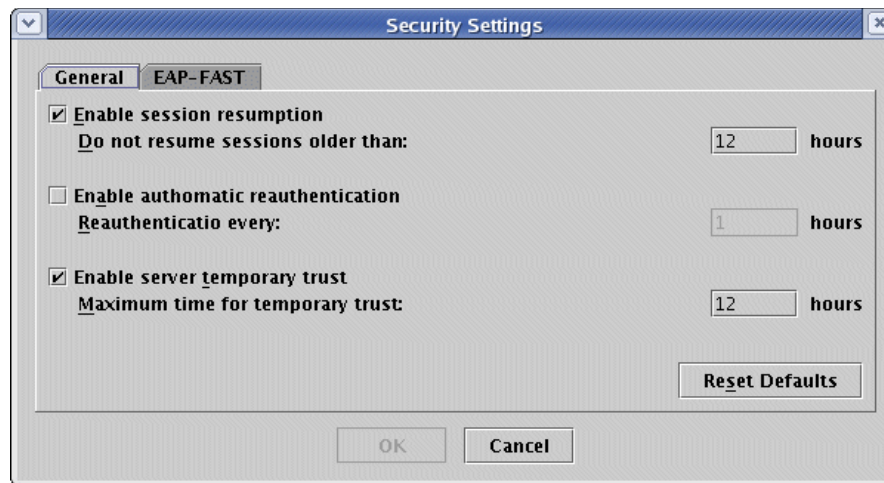
**Figure 23** Odyssey Preferences Dialog

To set Odyssey Client preferences, follow these steps:

- 1 Check your preferences:
  - ▶ If you check **Hide tray icon**, then the Odyssey icon is not displayed on the system tray (at the bottom right of your screen).
  - ▶ If you check **Disable splash screen**, then the Odyssey Client splash screen is not displayed when the Odyssey Client service starts up.
- 2 Click **OK**.

## Security Settings

To configure advanced security options related to authentication, select **Security Settings**. **Security Settings** appears.



**Figure 24** General Tab of the Security Settings Dialog

You can configure the following options:

- ▶ **General**
- ▶ **EAP-FAST**

## General

The options on the **General** tab of the Security Settings dialog are initially set to default values that should suit most purposes. You can restore the defaults at any time by clicking the **Reset Defaults** button.

You can configure time (up to three decimal places) in hours. For example, to specify one hour and fifteen minutes, enter **1.25**.

You have three options from the **General** tab of the Security Settings dialog:

- ▶ **Enable session resumption.** Check this option to enable session resumption and to specify the maximum length of a session before it expires. See [“Session Resumption” on page 13](#) for more details.
- ▶ **Enable automatic reauthentication.** Check this option to enable automatic reauthentication and to specify the reauthentication period. See [“Reauthentication” on page 13](#) for more details.
- ▶ **Enable server temporary trust.** Check this option to enable temporary trust of a server and to specify the maximum length of a session with a temporarily trusted server.

## Session Resumption

You can enable the use of session resumption from the Security Settings dialog. See [“Session Resumption” on page 13](#) for more information on session resumption.

To enable session resumption, follow this procedure from the **General** tab of the Security Settings dialog:

- 1** Check **Enable session resumption**.
- 2** Set **Do not resume sessions older than** to the maximum number of hours that a session can be maintained after initial authentication before reauthentication is required. After the time limit has elapsed, a completely fresh authentication is performed on your next reauthentication. The number of hours can have up to three decimal places. For example, enter **1.25** to indicate one hour and fifteen minutes, or **0.001** for about three seconds. The smallest value you can enter is **0.001**.

By default, session resumption is enabled, and an initial authentication is resumed for up to 12 hours.

To disable this feature, uncheck **Enable session resumption**.

## Automatic Reauthentication

You can enable or disable the automatic reauthentication feature of Odyssey Client. For information about why you might want to reauthenticate, see [“Reauthentication” on page 13](#).

To use automatic reauthentication, follow these steps from the **General** tab of the Security Settings dialog:

- 1 Check **Enable automatic reauthentication** so that Odyssey Client periodically initiates reauthentication with the server.
- 2 Next to **Reauthenticate every**, type the time period (in hours) for reauthentication to take place automatically. You can use up to three decimal places to indicate the number of hours. For example, enter **1 . 25** to indicate one hour and fifteen minutes, or **0 . 001** for about three seconds. The smallest value you can enter is **0 . 001**.

By default, automatic reauthentication is not enabled. This is because your network administrator may have already configured your access points or authentication server to perform periodic reauthentication. Check with your network administrator for the proper settings for this option.

To disable this feature, uncheck **Enable automatic reauthentication**.

## Server Temporary Trust

Under normal circumstances, you can use the Trusted Servers panel to configure the servers you trust for authentication. However, there may be times when you authenticate to a network whose authentication server is not yet configured as trusted in the Trusted Servers panel. In this case, you may want the ability to enable temporary trust for that untrusted server.

Check **Enable server temporary trust** from the **General** tab of the Security Settings dialog to enable temporary trust. Uncheck this field to disable this feature. Notice the following about this feature:

- ▶ If temporary trust is enabled, you are given the following options:
  - ▷ Whether to trust an untrusted server temporarily when you attempt to authenticate to it. See [“Untrusted Servers” on page 50](#).
  - ▷ Whether to add the server to your trust tree in the Trusted Servers panel. Consequently, the temporary trust feature serves as an alternative to configuring trusted servers through the Trusted Servers panel.
- ▶ If temporary trust is not enabled, then any authentication attempt that requires the validation of a server certificate fails when the server is not explicitly trusted.

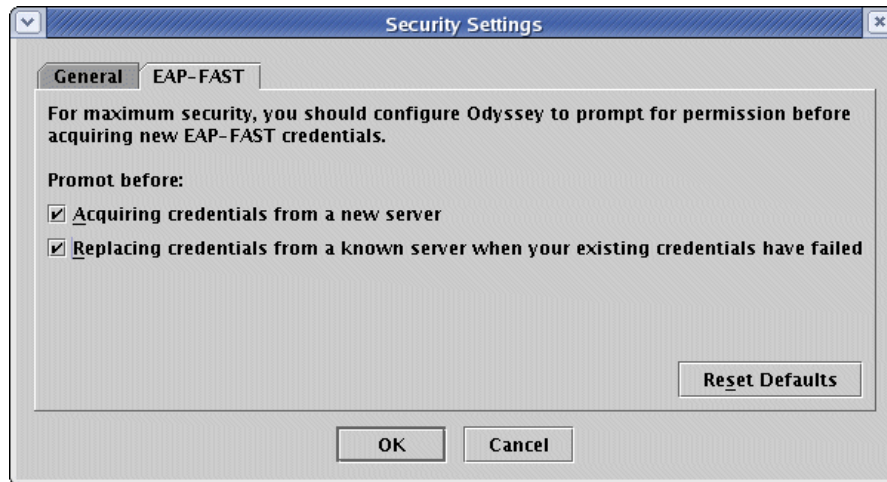
Set **Maximum time for temporary trust** to the maximum number of hours you want Odyssey Client to continue to trust a server once you accept it.

By default, temporary trust is enabled. The maximum time that a particular server is (temporarily) trusted after you accept it is 12 hours.

**NOTE:** *These settings do not apply to servers you choose to trust permanently if you check **Add this trusted server to the database** when you are prompted for temporary trust. See [“Untrusted Servers” on page 50](#).*

## EAP-FAST

When you use EAP-FAST authentication, you can select options that determine when you are prompted for credentials.



**Figure 25** EAP-FAST Tab of the Security Settings Dialog

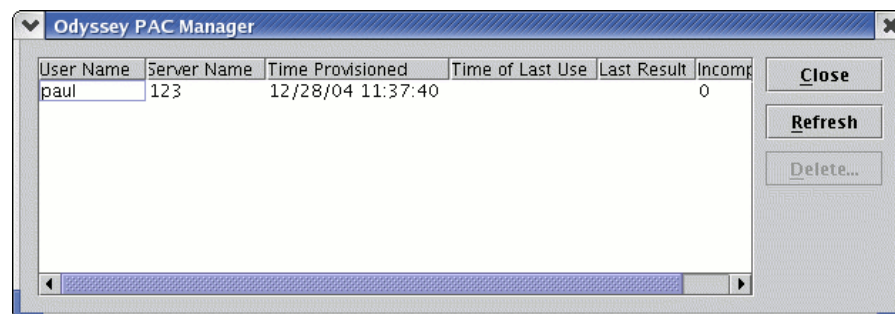
You can select from the following options on the **EAP-FAST** tab of the Security Settings dialog:

- ▶ Check **Prompt before acquiring credentials from a new server** to be prompted for new credentials when you authenticate with a new server.
- ▶ Check **Prompt before replacing credentials from a known server when your existing credentials have failed** to be prompted for new credentials when a previous authentication attempt fails.

By default, the EAP-FAST options are checked. You can restore the defaults at any time by clicking the **Reset Defaults** button.

## PAC Manager

From **Settings > PAC Manager**, you can use the Odyssey PAC Manager to manually provision Protected Access Credentials (PACs) for use with EAP-FAST authentication.



**Figure 26** Odyssey PAC Manager

You can perform the following tasks using the **Odyssey** PAC Manager:

- ▶ Once a PAC file has been created, you can import the PAC by clicking **Import**. When the **Open** dialog appears, browse for the directory containing the PAC file and double-click it to import. If the PAC file you select is password protected, you are prompted for the password before you can successfully import the PAC.
- ▶ To refresh a selected PAC listing, click **Refresh** to update the display of the PAC usage.
- ▶ To delete one or more selected PACs from the list, click **Delete**.
- ▶ Click **Close** when you are done.

## Enable/Disable Odyssey

Select **Settings > Enable Odyssey** or **Settings > Disable Odyssey** to turn Odyssey Client on or off.

Odyssey Client is initially enabled, and you should not need to disable it. If you choose to disable Odyssey Client, you are no longer able to use Odyssey Client for network connections until you enable it again.

You may want to disable Odyssey Client if you have concerns about your current Odyssey configuration. For example, if you are worried that Odyssey Client is in an insecure state, you can use this feature to take yourself off the network until you get a chance to inspect your settings.

## Close

Select **Settings > Close** to close the Odyssey Client Manager window. Although the user interface is no longer visible, Odyssey Client continues to perform its networking operations normally.

You can restart Odyssey Client Manager at any time in any of the following ways:

- ▶ From the system tray – Double-click the Odyssey icon, or right-click it and choose Odyssey Client Manager.
- ▶ From the main menu, select Odyssey Client Manager to start Odyssey Client.

## Commands Menu

The following commands are available from the **Commands** menu:

- ▶ Forget Password
- ▶ Forget Temporary Trust

## Forget Password

When you first authenticate using a profile set to **prompt for password**, you are asked to type in your password. Odyssey Client remembers the password you enter, and uses it

for all subsequent authentications using that profile without prompting you again. Normally, Odyssey Client does not forget the password you type in until you reboot your PC or restart Odyssey Client.

If you want Odyssey Client to discard any passwords or PINs you enter when you attempt a network connection, select **Forget Password**. When your password is needed again, you are prompted to enter it.

You might need to use this command if you enter your password incorrectly or if your password has been changed on the authentication server.

## Forget Temporary Trust

If you enable temporary trust from **Settings > Security Settings**, then whenever you encounter an untrusted authentication server, a service dialog appears, allowing you to trust that server temporarily. Odyssey Client remembers to trust that server for the period of time you configure in **Settings > Security Settings**. See “Untrusted Servers” on page 50 and “The options on the **General** tab of the Security Settings dialog are initially set to default values that should suit most purposes. You can restore the defaults at any time by clicking the **Reset Defaults** button.” on page 54.

If you want Odyssey Client to discard its list of temporarily trusted servers, select **Commands > Forget Temporary Trust**.

You might need to use this command if you accept a server as temporarily trusted and then decide to break your connection with it. If you want to be sure the connection is broken immediately, you should disable session resumption and then click the **Reconnect** button on the Connection panel. See “Session Resumption” on page 54.

## Web Menu

The **Web** menu provides several Web links. These include the following:

- ▶ Odyssey User Page
- ▶ Funk Software Home Page
- ▶ Register Odyssey Client
- ▶ Purchase Odyssey Client

## Odyssey User Page

Select **Web > Odyssey User Page** to open your browser to a page devoted to Odyssey users. You can find technical notes that can help you get the most out of Odyssey, as well as product news and information about new versions at this web site.

## ***Funk Software Home Page***

Select **Web > Funk Software Home Page** to open the Funk Software home page in your browser. Here you can find more information about Funk Software, Inc. and its products.

## ***Register Odyssey Client***

Select **Web > Register Odyssey Client** to register your Odyssey Client online.

Once you register your software, you are automatically notified about product upgrades and special offers. Additionally, should you need to call our technical support hotline, your call can be expedited if we have your registration is on file.

## ***Purchase Odyssey Client***

Select **Web > Purchase Odyssey Client** to purchase the product.

## **Help Menu**

The **Help** menu has the following items:

- ▶ Help Topics
- ▶ License Keys
- ▶ View Readme File
- ▶ About

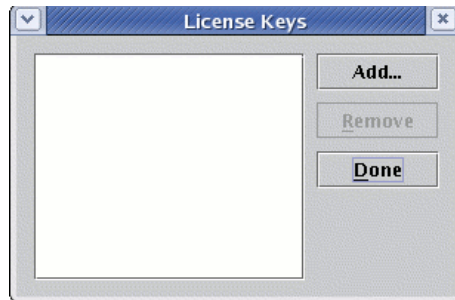
## ***Help Topics***

Select **Help > Help Topics** to open the Odyssey Client help system.

You can also get context-sensitive help at any time by pressing **F1**. The help system opens to the section that is most relevant to your current view of Odyssey Client.

## ***License Keys***

Select **Help > License Keys** to manage your Odyssey Client license keys.



**Figure 27** License Keys Dialog

A license key is a text sequence that represents your license to use Odyssey Client. Under most circumstances, you set a license key when you install Odyssey Client. However, you may need to enter additional license keys over time. For example, you must enter an additional license key when you upgrade to a new version or when you want to enable special features.

In this example, no license key is visible. Click **Add** to add a new license key. Type a valid license string in the Add License Key dialog when it appears, and click **OK**.

To remove a license, select it and click **Remove**.

Click **Done** when you are done modifying license keys.

## Upgrade Licenses

If you are upgrading Odyssey Client from a previous version, you must have at least two license keys listed when you select **Help > License Keys**:

- ▶ An upgrade license key
- ▶ An original product license key that is valid for the previous version

## View Readme File

Select **Help > View Readme File** to open the file `readme.txt`. This file has important information about Odyssey Client.

## About

Select **Help > About** to view product and copyright information.

## System Tray Icon Menu Commands

If you right-click the Odyssey icon in the system tray, the following menu items appear:

- ▶ Odyssey Client Manager
- ▶ Exit

## Odyssey Client Manager

You can start Odyssey Client Manager (the user interface for Odyssey Client) by selecting the Odyssey Client Manager menu command when you right-click the system tray icon.

### Exit

If you select the **Exit** command when you right-click the system tray icon, you are prompted with the following dialog.

When you click **Yes**, the Odyssey Client user interface shuts down. You may want to use this option when you are not using wireless networking for an extended period.

## Other Odyssey Client Features

In addition to panels and menu items, you may interact with Odyssey Client using methods described in the following topics:

- ▶ [Shortcut Keys](#)
- ▶ [Interaction with Other Adapter Software](#)

### Shortcut Keys

In addition to using your mouse to access buttons, tabs, and panels on Odyssey Client Manager, you can also use your keyboard to access all of the Odyssey Client features.

Most keyboard shortcuts are indicated by letters that are underlined in the Odyssey Client Manager. To use the keyboard shortcuts for these features, press **ALT** and then the letter. For example, to scan for a network from the Connection panel, you can press **ALT+N**.

To move between the panels of the Odyssey Client Manager, use the up and down arrows on your keyboard. You can also use the keyboard arrows to move through radio button (mutually exclusive) selections.

You can also press **ALT** in conjunction with the appropriate arrow key on the keyboard to implement the corresponding arrow button features, such as those in the Auto-Scan Lists dialog.

## Interaction with Other Adapter Software

Your wireless adapter may provide its own user interface software to help you control its operation. This other software may allow you to operate non-standard features of your wireless adapter to which Odyssey Client Manager has no access.

In most cases, Odyssey Client Manager and the user interface that comes with your wireless adapter can coexist without problems, but you should avoid using both

products for similar purposes. If you use Odyssey Client for network communications, use the software supplied with your adapter to operate only those features that cannot be controlled by Odyssey Client Manager.

## Hard Token Authentication Run-Time Dialogs

After you configure Odyssey Client for authentication using one or more token card authentication methods and check **Connect to network** on the Connection panel, an exchange of messages between Odyssey Client and the token card authentication server begins. This exchange of messages is referred to as the challenge-response dialog between the server and Odyssey Client, as the server prompts (challenges) the user to enter private information (response). Odyssey Client presents one or more authentication dialogs according to your state in the token card authentication server challenge-response process.



**Figure 28** Odyssey Client Hard Token Service Dialog

If the service dialog in [Figure 28](#) appears, enter the PIN followed by the current sequence of digits on your hardware token card.

Under some circumstances, you may be required to provide a new PIN. Follow this procedure when you are required to enter a new PIN:

- 1 Enter a new 4–8 digit PIN, and click **OK**.
- 2 You can click **Unmask** to see your PIN as you type it before you click **OK**. You are prompted ([Figure 2](#)) for this new PIN again. Re-enter a new 4–8 digit PIN, and click **OK**.

## Numerics

- 802.11
  - ad-hoc mode 6
  - definition 4
  - infrastructure mode 6
- 802.1X
  - authentication 42
  - definition 9

## A

- access points
  - ad-hoc mode 40
  - infrastructure mode 40
  - introduction 6
- adapters
  - adding 52
  - disabling through password prompt 29
  - multiple networks 21
- Adapters panel 51
- adding
  - auto-scan lists 45
  - licenses 59
  - wired adapters 52
  - wireless adapters 52
- ad-hoc mode
  - defined 6
  - setting 40
- AES
  - configuration 41
  - overview 8
  - peer-to-peer 8
- anonymous name 33
- any
  - network, configuring connections 40
  - server, trusting 48
- association
  - defined 4
  - methods, configuring 41
- asymmetric cryptography 10
- authentication
  - network, specifying 42
  - protocols 31
  - setting in profile properties 30

- auto-scan lists
  - adding 45
  - connecting to 20
  - properties 45
- Auto-scan lists panel 44

## B

- buying the product 60

## C

- certificate authorities
  - defined 11
  - root 11
- certificate chains
  - defined 11
  - use of 46
- certificates
  - overview 11
  - use of 30
  - validation 32
- channels, peer-to-peer 41
- commands from system tray icon 60
- configuring
  - connection to any network 40
- connecting
  - wired networks 21
  - wireless networks 20
- Connection panel
  - elapsed time 24
  - encryption key information button 26
  - informational fields 23
  - MAC address 24
  - overview 19
  - scan for network 21
  - signal power 25
  - SSID 24
  - status field 23

## D

- descriptions of networks 40

- disabling
  - adapters for wired connections 29
  - connections at password prompt 29
- disconnecting
  - network connections 23
  - wired connections 21
  - wireless networks 20
- domain
  - controller 34
    - EAP interaction 12
  - login name 28
- driver software 15
- dynamic encryption keys
  - generation 42
  - reconnection effects 22

## E

- EAP
  - as inner authentication 35
  - definition 9
- EAP-AKA
  - overview 12
- EAP-Cisco Wireless 12
- EAP-FAST
  - overview 12
  - PAC Manager 56
  - security settings 56
  - token cards 32
  - tunneled method 32
- EAP-LEAP 12
- EAP-PEAP
  - generic token card options 32
  - inner protocols, selecting 36
  - overview 12
- EAP-TLS
  - key generation 42
  - overview 11
- EAP-TTLS
  - certificate options 34
  - generic token card options 32
  - key generation 42
  - overview 11
  - settings 34
  - using 34
- elapsed time 24
- enabling Odyssey 61
- encryption
  - keys
    - defined 4
    - generation 42

- information button 26
  - reconnection effects 22
- method, Networks panel 41

Extensible Authentication Protocol 9

## F

- forgetting
  - password, setting 57
  - temporary trust 58

## G

- generic token card options 33
- getting help 59

## H

- hardware-based tokens
  - run-time dialogs 62
- help
  - menu 59
  - topics 59
- hexadecimal passphrases 43
- hiding icons 53
- hubs, 802.1X 6

## I

- icons, hiding 53
- identity, server 49
- infrastructure mode
  - access points 40
  - defined 6
- inner authentication protocols
  - definition 34
  - EAP 35
  - selecting 34
- installation
  - instructions 15
  - overview 15
  - requirements 15
- intermediate CAs
  - overview 11
- IP address status 24

## K

keyboard shortcuts 61

## L

LAN, defined 3

LDAP 12

LEAP 12

license keys

    specifying 59

    upgrading 60

lightweight EAP 12

login names

    specifying 28

## M

MAC address 24

maintenance contracts 2

managing

    PACs 56

managing PINs 56

multiple connections 21

mutual authentication

    explained 10

    implementing 32

## N

network cards, using 52

networks

    any network, configuring 40

    association 41

    authentication, specifying 42

    configuring 37

        connection to any 40

    connecting to 20

    description 38

    description field 40

    disabling at password prompt 29

    disconnecting from 23

    encryption methods 41

    multiple connections 21

    names

        scanning for 40

        specifying 40

    network type 40

    overview 40

    reauthenticating 23

    reconnecting 22

    scan button 40

    scanning for connection 21

    SSIDs 40

    titles 38

    type, specifying 40

    WEP keys 42

    wired, connections 21

Networks panel 37

## O

Odyssey Client Manager

    overview 18

    starting 18

open mode, WEP

    configuring 41

    definition 7

options

    session resumption 54

    temporary trust 55

outer authentication protocols 30

## P

PAC manager 56

packets, status information 24

passphrases 43

passwords

    configuring in profiles 29

    forgetting 57

    generic token card 32

    Linux 29

    prompts for 57

    saved, caution 29

PEAP

    overview 12

    settings in profile properties 36

    token card options 32

    token card settings 33

peer-to-peer networking

    channels 41

    definition 6

    IP addresses 6

    product, using for 42

preconfigured WEP keys 43

- preferences
  - hide tray icon 53
  - setting 53
- preshared keys 43
- private key 10
- product registration 59
- profiles
  - adding 27
  - login name 27
  - password 29
  - passwords 27
  - PEAP settings 36
  - properties 27
  - user info 28
- Profiles panel 26
- Protected Access Credentials 56
- public key 10

## R

- RADIUS, server product 9
- reauthenticating
  - explained 13
  - networks 23
  - session resumption 54
  - why 13
- reconnecting
  - dynamic encryption keys, effect on 22
  - networks, to 22
- registering Odyssey 59
- requirements, installation 15
- root certificate authority 11

## S

- Scan button, connections for 21
- security settings
  - command 53
  - EAP-FAST 56
  - general 54
- server certificates, validating 32
- servers, name 49
- service
  - Odyssey Client 18
- session resumption
  - definition 13
  - setting 54

- settings menu
  - EAP-FAST settings 56
  - overview 52
  - preferences 53
  - security settings 53
- shared mode, WEP
  - configuring 42
  - definition 7
- shortcut keys 61
- signal power, viewing 25
- simultaneous connections
  - establishing 21
  - monitoring 21
- smart cards
  - certificates
    - overview 11
    - Windows 9x restrictions 30
- splash screen, hiding 53
- SQL 12
- SSIDs
  - definition 7
  - networks, for 24
- starting the product, main interface 18
- status from Connection panel 23
- support information 1
- switches, 802.1X 6
- system tray icon 19
  - commands from 60

## T

- technical support 1
- temporary trust
  - defined 55
  - disabling 55
  - forgetting 58
  - untrusted servers, of 50
- TKIP
  - implementing 41
  - overview 8
  - peer-to-peer 8
- TLS, overview 11
- token cards
  - authentication
    - dialogs 62
    - passwords 33
    - settings 34
  - run-time dialogs 62
- tray, commands from 60

- trusted servers
  - any 48
  - editing 50
  - entering 48
  - removing 49
- Trusted Servers panel 46
- TTLS
  - overview 11
  - settings 34
- tunnels 33

- WPA2
  - overview 8
  - passphrases 43
  - specifying 41

## U

- untrusted servers
  - defined 55
  - dialog 50
- upgrades
  - licenses 60
- user info
  - profile properties, in 28

## V

- validating server certificates 32

## W

- WEP keys
  - any network connection 40
  - defined 7
  - open mode 7
  - peer-to-peer 8
  - shared mode 42
  - specifying 42
- Windows logon
  - certificates 30
- wired adapters, adding 52
- Wired-Equivalent Privacy 7
- wireless
  - adapters, adding 52
  - networks
    - connecting 20
    - disconnecting 20
- WPA
  - implementing 41
  - overview 8
  - passphrases 43

