

Odyssey Client

User and Administrator Guide

Funk Software, Inc.
222 Third Street
Cambridge, MA 02142

(617) 497-6339
(617) 491-6503 (Technical Support)
www.funk.com

Fifth Edition, June, 2003

© Copyright 2002-2003 Funk Software, Inc. All rights reserved.

Odyssey Client © 2002-2003 Funk Software, Inc. All rights reserved. Odyssey® is a registered trademark and Funk® is a registered trademark of Funk Software, Inc. Microsoft, Windows, Windows XP, Windows NT, Windows 2000, Internet Explorer, and other Microsoft products referenced herein are either trademarks or registered trademarks of the Microsoft Corporation in the United States and other countries. 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 (eay@cryptsoft.com).

Table of Contents

Introduction	5
Welcome	6
Requirements	6
Operating systems	6
Wireless adapter card and/or wired network card	7
Network hardware	7
Browsers	7
Documentation	7
Technical support	8
 Installation	 9
Installation Process	10
Installation requirements	10
Installation instructions	10
Install	10
Configure	11
 Networking with Odyssey Client	 13
Introduction to networking with Odyssey Client	14
The 802.11 wireless networking standard	14
Types of wireless networks	15
Wireless network names	16
802.11 network security	16
Wired-Equivalent Privacy (WEP) with preconfigured keys	17
Wi-Fi Protected Access (WPA) and TKIP encryption	18
The 802.1X standard	19
Extensible Authentication Protocol (EAP)	19
Session resumption	22
Reauthentication	23
 Using Odyssey Client Manager	 25
Odyssey Client Manager Overview	26
Starting Odyssey Client Manager	27
Odyssey Client Manager display	27
Connection panel	29
Select an adapter	30
Connect to a network (wireless connections only)	30
Connect using profile (wired connections only)	31

Table of Contents

Configure multiple simultaneous network connections.....	31
Scan for wireless networks	32
Reconnect to a network.....	32
Reauthenticate to a network.....	33
Disconnect from a network connection	33
View connection information	33
View informational graphics and detailed status	34
Profiles panel	36
Profile Properties dialog	37
Networks panel	47
Network Properties	48
Auto-Scan Lists panel.....	53
Auto-Scan List properties	55
Trusted Servers panel.....	56
Using the simple method to configure trust.....	56
Using the advanced method to configure trust	58
Untrusted servers	63
Adapters panel	64
Adding a wireless or wired adapter	65
Removing an adapter from the list of adapters	65
Settings menu.....	66
Preferences.....	66
Security settings.....	67
Windows Logon Settings.....	69
Odyssey Client Administrator	75
Enable/Disable Odyssey	75
Close	76
Commands Menu.....	76
Forget Password.....	76
Forget Temporary Trust.....	77
Web Menu.....	77
Odyssey User Page	77
Funk Software Home Page	77
Register Odyssey	78
Help Menu	78
Help topics	78
License keys.....	78
View Readme File	79
About	79
Tray icon menu commands.....	79

Table of Contents

Odyssey Client Manager.....	79
Enable Odyssey or Disable Odyssey	79
Help commands	80
Exit.....	80
Shortcut keys.....	80
Interaction with other adapter software	81
 Odyssey Client Administration	 83
Overview of Odyssey Client Administration	84
Odyssey Client Administrator	84
Launching Odyssey Client Administrator	85
Connection Settings	85
Initial Settings	92
Machine Account	94
Custom Installer	96
Testing your settings	98
Sample workflows with Odyssey Client Administrator	99
Preconfiguring Odyssey Client for a group of users.....	99
Configuring machine only connection.....	101
Configuring machine connection followed by user authentication	101
Configuring user authentication without machine connection	102
 Index	 104

Introduction

1

Welcome

Thank you for selecting Odyssey® Client.

With Odyssey Client, you can connect to your network easily and securely. You can use Odyssey Client to perform the following tasks:

- Configure and control your 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 802.1X to authenticate to the network.
- Use a wide variety of authentication methods, including powerful methods such as EAP-TTLS, PEAP, and EAP-TLS, to keep your credentials secure.

For more introductory information, see the following topics:

- Requirements
- Documentation
- Technical support

Requirements

Odyssey Client Manager has the following requirements with respect to hardware and software:

- “Operating systems” on page 6
- “Wireless adapter card and/or wired network card” on page 7
- “Network hardware” on page 7
- “Browsers” on page 7

Operating systems

Odyssey Client Manager runs under the following operating systems:

- Windows 98
- Windows 98 SE
- Windows Me

- Windows 2000 Professional or Server
- Windows XP Home or Professional

Wireless adapter card and/or wired network card

In order to use wireless capabilities, your computer must be equipped with a wireless adapter card and a driver that supports the Microsoft-defined 802.11 OIDs, and is 802.1X compliant. In order to authenticate to a network using a wired connection, you need any network card that is adapted for a wired connection.

The most recently updated list of compatible adapter cards can be found on the Odyssey User Page on our web site. For a shortcut to this page, select **Web > Odyssey User Page** from the menu.

Network hardware

For wireless network authentication, your network must include at least one 802.1X compliant access point.

For wired network authentication, your network must include at least one 802.1X compatible switch or hub.

Browsers

Your computer must be running Microsoft Internet Explorer 5.5 or later.

Documentation

Your **Odyssey Client Manager** software includes a help system that allows you to access this documentation on your computer. To bring up this help system, select the **Help > HelpTopics** menu command from the **Odyssey Client Manager**. You can also read the manual in PDF format. The manual is called *OdysseyClientAdmin.pdf*, and is located on your product CD under **Docs**.

You can also get context-sensitive help at any time by clicking **F1**. The help system appears opened at the section that best explains your current situation.

The **Help > View Readme File** menu command located on the **Odyssey Client Manager** opens the *readme.txt* file. This file may have important information about Odyssey Client that is not included in this manual.

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 look at the README.TXT file, select the **Help > View Readme File** menu command from the **Odyssey Client Manager**.

- Check our web site <http://www.funk.com> 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.
- E-mail your questions or issues to support@funk.com.
- We provide 30 days of technical support by phone at no charge, starting from your first support call. For technical support by phone, you can call (617) 491-6503, Monday through Friday, 9:00 A.M. to 5:00 P.M., Eastern time.

For support beyond the initial 30-day 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. Select **Web > Funk Software Home Page** from the menu bar, then 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 Funk Software partner in your country or by contacting us directly. You can find the name of the support provider nearest you on our web site. Select **Web > Funk Software Home Page** from the menu bar, then navigate to the **Contact Info > International** section of the web site.

Please take a moment to register your copy of Odyssey Client with us. Doing so allows you to receive notifications of product upgrades and special offers and will expedite your first contact with our Technical Support department. To register Odyssey, select the **Web > Register Odyssey** menu command.

Installation

2

Installation Process

If you are running Windows 2000 or Windows XP, you can only install Odyssey Client if you have administrator privileges.

You can find the following basic installation instructions in the following topics:

- Installation requirements
- Installation instructions

Installation requirements

Before you install, please note the following:

- Your wireless (and/or wired) network adapter card and associated driver software should have already been installed.
- On Windows 2000 and Windows XP, you must have administrative privileges to install Odyssey Client.

Installation instructions

Installation of Odyssey Client has two phases:

- Install
- Configure

Install

To install Odyssey Client:

- 1 Insert the installation CD into your CD-ROM drive. The installation process starts automatically.
- 2 The installation wizard asks you a series of questions. Your answers determine how the software is installed and configured. Follow the instructions as they appear.
- 3 After you supply all of the necessary information to the installation wizard, you can click the **Install** button to begin the installation process.

Configure

Once the first phase of the install process is complete, use the **Configure and Enable Odyssey Wizard** to configure Odyssey Client for use by you (the current user who is performing the installation). If this wizard does not open for you automatically, your installation is already complete.

Read the following topics to learn more about configuring Odyssey Client:

- Configure Odyssey Client for each user on a single PC
- Configuring Odyssey Client for multiple machines

Configure Odyssey Client for each user on a single PC

Your computer may have multiple user accounts. Once installed on a single PC, Odyssey Client is available to all users. However, the settings that control Odyssey Client's operation are separate for each user.

Whenever you use Odyssey for the first time, the **Configure and Enable Odyssey Wizard** may appear, so that you configure Odyssey Client for own use. If there are multiple users of the same client machine, they are each offered the option to configure Odyssey through this wizard when the configuration is incomplete. If this wizard does not appear, your initial configuration is complete. In the case that the wizard does appear, you have the following options with respect to personal configuration of Odyssey:

- Accept the option for configuration with the wizard
- Decline the option for configuration at the current time, but be asked again upon subsequent log in
- Decline the option for configuration, and not be asked again

NOTE: *Even if you decline to install Odyssey Client for a particular user account, you can later change your mind and perform the installation. Simply run **Odyssey Client Manager** from the **Start** menu. The **Configure and Enable Odyssey Wizard** automatically starts up.*

Configuring Odyssey Client for multiple machines

Once you install Odyssey Client on a PC, you can create a custom installer to customize a default configuration for users of multiple machines. See “Preconfiguring Odyssey Client for a group of users” on page 99.

Networking with Odyssey Client

3

Introduction to networking with Odyssey Client

This chapter introduces the basic concepts and terminology behind wireless and wired networking, particularly as these concepts relate to configuring and using Odyssey Client.

Read this material if you are configuring Odyssey Client yourself or for a set of users, or, if you are curious to learn about networking with Odyssey Client. In doing so, you can learn about how you can use Odyssey Client to best advantage, and, in particular, how you can maximize the security of your connections over wireless 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.

The network protocols used by Odyssey adhere to the IEEE (Institute of Electrical and Electronic Engineers) 802.1X standard. The 802.1X standard includes the set of standards for wireless LANs, known as 802.11.

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

- “The 802.11 wireless networking standard” on page 14
- “The 802.1X standard” on page 19

The 802.11 wireless networking standard

There are many types of wireless communication. Odyssey is designed to work over a particular type of wireless network known as *802.11*. 802.11 has been standardized by the IEEE, and is rapidly gaining popularity as a complement, as well as an alternative to the wired LAN.

In addition to describing modulation and data framing, this standard includes an authentication and encryption method called Wired Equivalent Privacy (WEP).

Many corporations are deploying wireless 802.11 networks, and 802.11 networks are beginning to appear in hotels, airports, and other “hotspots” as a means of internet access.

The following attributes of the 802.11 standard are described here:

- Types of wireless networks
- Wireless network names

- 802.11 network security
- Wired-Equivalent Privacy (WEP) with preconfigured keys
- Wi-Fi Protected Access (WPA) and TKIP encryption

Types of 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 by far the more common, as it can allow you to get onto your corporate network and, consequently, the internet.

In an access point 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 make use of many different access points and each access point typically has a range of several hundred feet. A company that uses wireless networking can strategically place access points so that wherever you are in the company, you are always in range of an access point that can link you to the corporate network.

Normally, you must log in, or authenticate to the network before you are allowed onto the network. Authentication can be done in various ways described subsequent sections.

Once you log in to the network, your PC is assigned an IP address on the local network. This address is provide by a network device called a *DHCP server*.

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*.

Peer-to-Peer networks

Even when no access point is available, two or more people can use *peer-to-peer* networking to create a private wireless network to connect their PCs together. You may want to do this in order 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, located within range of each other. As a result, this mode of authentication does not involve a RADIUS server, and authentication that is based on 802.1X is not implemented.

Normally, there is no DHCP server on a peer-to-peer network to assign IP addresses. Instead, you are connected using an “automatic private IP address” that is assigned by Windows. These addresses are in the range 169.254.0.0 to 169.254.255.255. Each PC in the peer-to-peer network is assigned such an address, enabling it to communicate with the others.

The 802.11 standard refers to this type of network connectivity as *ad-hoc mode*.

Wireless network names

Each wireless network has a name. You can select the wireless network you want to connect to, by specifying its name.

Network names allow different wireless networks in the same vicinity to coexist without intruding on each other. For example, the company next door to yours may also use wireless networking, and you want to make sure that your PC connects to your company’s network, and not the other’s, even though your PC is within range of their access points. (How to prevent intruders from connecting to your company’s network is the subject of the security discussion, below.)

A network name is simply a text sequence up to 32 characters long, such as Bayonne Office, or Acme-Marketronics, or BE45789, for example. A network name is case-sensitive, so you have to be careful if you type it in. You always have the option to scan for available networks. This allows you select the network from a list, preventing any network naming errors.

The 802.11 standard refers to network names as *Service Set Identifier*, or *SSID* for short.

802.11 network security

With the advent of wireless networking, security becomes a critical concern to a far greater extent than it had been previously, for the simple reason that it is easy for an attacker to eavesdrop on such connections.

With wired networking, most organizations can rely on physical security to protect their networks. An attacker would have to get inside a company’s offices to be able to plug in to the LAN and observe network traffic.

All it takes to observe wireless network traffic is a PC with a wireless card and a comfortable spot in the parking lot outside or in the office next door. The following are some of the things that are required to make a wireless network safe:

- A user must be authenticated by the network before he or she is allowed access, to make the network safe from intruders.
- The network must be authenticated by the user before the user allows his or her PC to connect to the network, to prevent a wireless device posing as a legitimate network from gaining access to the user's PC.
- The mutual authentication between user and network must be cryptographically protected. This insures that you are connecting to the network you want, and not some phony one.
- The wireless connection between a PC and access point must be encrypted, so eavesdroppers cannot access data that is supposed to be private.

There are two basic mechanisms for providing this type of secure encryption over a wireless network:

- Preconfigured secrets, called *WEP keys*. These keep unauthorized users off the wireless network and encrypt the data of legitimate users.
- Authentication using a protocol called *802.1X*. This uses a variety of underlying authentication protocols to control network access. The strongest of these protocols can provide mutual authentication of user and network, and can dynamically create keys to encrypt wireless data.

Wired-Equivalent Privacy (WEP) with preconfigured keys

With preconfigured WEP (Wired-Equivalent Privacy), both the client PC and access point are assigned the same secret key. This key is used to encrypt all the data between the PC and access point.

In addition, the WEP key can be used to authenticate the client PC to the access point — unless the PC can prove it knows the WEP key, it is not allowed onto the network.

- When the access point requires that you configure WEP keys for association, you associate to the access point using *shared mode*. You can specify to associate to your access point in shared mode through **Network Properties**.
- When WEP keys are not required by your access point for the purpose of association, it is called *open mode*. You can specify to associate to your access point in open mode through **Network Properties**.
- If your access points are configured for WPA association with WEP encryption, rather than TKIP, you can configure Odyssey Client for this type

of network as well. In this case, all required WEP keys are generated from an ASCII passphrase that you configure for your access point, as well as for Odyssey Client.

See the following topics:

- “Specify the association mode” on page 50, for directions for selecting an association mode in Odyssey Client
- “Specify an appropriate encryption method for your association mode” on page 51, for directions for selecting WEP encryption when using shared association mode
- “Preconfigured keys (WEP)” on page 52, to use static WEP keys with Odyssey Client
- “Pre-shared keys (WPA)” on page 52, to configure WEP encryption when you associate in WPA mode

Wi-Fi Protected Access (WPA) and TKIP encryption

As an enhancement to the 802.11 wireless standard, Wi-Fi Protected Access (WPA) encompasses a number of security enhancements over Wired-Equivalent Privacy. These enhancements include the following:

- Improved data encryption via TKIP (temporal key integrity protocol). TKIP provides stronger encryption than WEP, by dynamically updating the encryption keys every 10,000 packets.
- 802.1X authentication with EAP. See “The 802.1X standard” on page 19, and “Extensible Authentication Protocol (EAP)” on page 19 for more information on these topics.

When the access point hardware in your network requires that you associate via the enhanced WPA association mode, you can configure Odyssey Client to associate in WPA mode. If the hardware is configured for TKIP encryption, you can configure Odyssey Client for this enhanced data encryption method as well.

In addition to conforming to 802.1X specifications for dynamic key generation (available with the strongest authentication methods), WPA allows for pre-shared keys to be generated for TKIP (or WEP) encryption from a passphrase. If you configure a passphrase for key generation in your access points, you must configure the same passphrase in Odyssey Client.

See the following topics:

- “Specify the association mode” on page 50, to use WPA association mode with Odyssey Client

- “Specify an appropriate encryption method for your association mode” on page 51, to use TKIP encryption with WPA association
- “Pre-shared keys (WPA)” on page 52 to configure a static passphrase

The 802.1X standard

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 802.11 associations are implemented. Wired networks use the 802.1X standard without any 802.11 association.

The WEP protocol using preconfigured keys has various shortcomings, both in terms of ease of administration, as well as security. To alleviate these problems, the IEEE introduced another standard, *802.1X*. 802.1X provides better security than preconfigured WEP keys, and is easier to deploy, particularly on large networks.

Using preconfigured WEP keys, it is the wireless client PC that is authenticated to the network. With 802.1X, it is the *user* that is authenticated to the network with the user credentials, which may be a password, a certificate, or a token card. 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 (EAP)
- Session resumption
- Reauthentication

Extensible Authentication Protocol (EAP)

802.1X uses the protocol called *EAP* (Extensible Authentication Protocol), 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 create keys that can be transformed into WEP keys to encrypt data between the PC and 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 a WEP key remains in use.

Odyssey offers a number of EAP authentication mechanisms. The following are the strongest methods:

- EAP-TTLS
- PEAP
- EAP-TLS

Each of these authentication methods provides secure mutual authentication of the user and the network, and produce dynamic keys that can be used to encrypt communications between the PC and access point. With mutual authentication, not only does the network authenticate you, but you also authenticate the network. Odyssey Client also offers LEAP and EAP-MD5-Challenge, and EAP-Token Card protocols for authentication.

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

EAP-TTLS, PEAP, and EAP-TLS all let you authenticate the network by validating the certificate of the authentication server. 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. Before understanding some of the stronger EAP protocols, you must first understand certificates.

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.

Previously, 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 you share your key with, 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*, and 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.

However, only you can “sign” data with your private key. Anyone can use your public key to determine that the data could come from you and you alone.

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 could be an individual or a computer. A certificate contains a public key and the name of the entity that owns it.

Each certificate is signed, or “issued”, by a *certificate authority*. By issuing a certificate, the certificate authority guarantees 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 Certicom are root certificate authorities. Many corporations have set up their own private root certificate authorities as well.

The sequence of certificates from the end entity through 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 and a root certificate.

Certificates are ideally suited for authentication. The disadvantage of certificates 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 company, the number of servers that may require certificates is relatively small, but the number of users can be enormous. For your company to provide certificates to each of its employees can be a daunting management task, and may require a level of administration that your company is not prepared to undertake. However, depending on the position of your company with respect to end-user certificates, you may be required to use certificate-based authentication methods.

EAP-TTLS

EAP-TTLS is a protocol devised by Funk Software and Certicom. It is designed to provide authentication that is every bit as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed using a password, or other credentials. The credentials are transported in a securely encrypted “tunnel” that is established using the server certificates. Within the EAP-TTLS tunnel, you can use a set of inner authentication protocols. See “Using EAP as an inner authentication protocol” on page 44 for more information.

With EAP-TTLS, it is not necessary to create a new infrastructure of user certificates. User authentication is performed against the same security database that

is already in use on the corporate LAN. For example, Windows domain controllers or an SQL or LDAP database can be used.

PEAP

PEAP is comparable to EAP-TTLS, both in its method of operation and its security, although it is not as flexible, and 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 can be expected to find widespread use. PEAP is a suitable protocol for performing secure authentications against Windows domains and directory services.

EAP-TLS

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

While EAP-TLS is cryptographically strong, it requires that the corporation that deploys it maintain a certificate infrastructure for all of its users.

Session resumption

For security purposes, it is good practice to periodically reauthenticate to your network. When you first authenticate using EAP-TTLS, 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.

However, once you authenticate to the network, any subsequent authentications to the same network server can be accelerated, by reusing the secret information that is developed during the first authentication. This is called *session resumption*.

It is usually a good idea to enable session resumption. Reauthentication can happen 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 when transferring data. Plus, using session resumption puts less load on the authentication server.

Session resumption results in the distribution of new keys to client and access point, just as a fresh authentication does. See “Session resumption” on page 67 for more information on using this feature.

Reauthentication

The ability to reauthenticate to the network is a feature of Odyssey Client.

Periodic reauthentication serves two purposes:

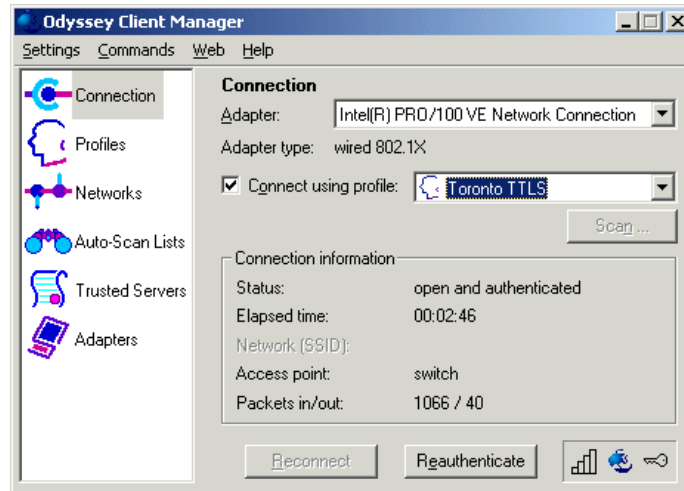
- As a general security measure, it verifies that you are still on a trusted network.
- It results in distribution of fresh shared keys to your PC and access point. The access point may use these shared keys to refresh the keys used to encrypt data. By frequently refreshing keys, you can thwart cryptographic attacks.
- See “Automatic reauthentication” on page 68 for more information on configuring this feature.

Using Odyssey Client Manager

4

Odyssey Client Manager Overview

Odyssey Client Manager is the Windows interface that allows you to control and configure the Odyssey Client product. This interface is consistent for all platforms on which you can run the product.



If your system administrator has configured Odyssey Client for you in advance, chances are that you only need to use the main **Connection** panel of the **Odyssey Client Manager**. Depending on your configuration, you can use this panel for the some or all of the following tasks:

- Connect to a network using a wireless or wired connection
- Reconnect to a network
- Reauthenticate to a network
- View connection information

More advanced tasks that you or your system administrator may want to perform include the following:

- Adding a wireless or wired adapter
- Creating a user profile and configuring authentication for that profile
- Adding or editing network properties
- Configuring trusted servers

See the following topics to learn about operating all features of **Odyssey Client Manager**:

- “Starting Odyssey Client Manager” on page 27


- “Connection panel” on page 29
- “Profiles panel” on page 36
- “Networks panel” on page 47
- “Auto-Scan Lists panel” on page 53
- “Trusted Servers panel” on page 56
- “Adapters panel” on page 64
- “Settings menu” on page 66
- “Commands Menu” on page 76
- “Web Menu” on page 77
- “Help Menu” on page 78
- “Tray icon menu commands” on page 79
- “Interaction with other adapter software” on page 81

Starting Odyssey Client Manager

You can start **Odyssey Client Manager** 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 Control Panel on your PC:* Double-click the **Odyssey Client Manager** icon
- *From the Windows taskbar:* Select **Start > Programs > Funk Software > Odyssey Client > Odyssey Client Manager**

NOTE: *The System Tray is the lower right corner of your monitor, where some application icons are displayed.*

The Odyssey icon looks as like this , although it may not have the same color.

Odyssey Client Manager display

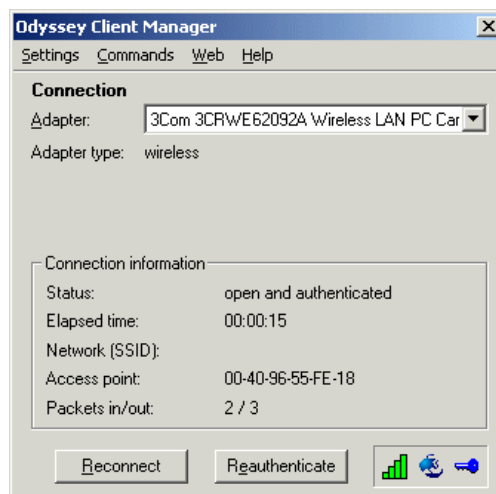
For most network connections, **Odyssey Client Manager** consists of a number of panels that allow you to control different aspects of its operation:

- 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 groups of wireless networks for seamless connection.
- Use the **Trusted Servers** panel to set certificate and identity information about the servers that may authenticate you when you connect, to ensure that you are logging in to the network that you intend.
- 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 it.

NOTE: *If you are connected to the network via the credentials of your client machine (as opposed to your own user credentials), then **Odyssey Client Manager** (pictured below) does not have most of these features, since there is no data to configure. In this case few of these features are available.*



If you are a system administrator, find more information about configuring connections with machine credentials in the following topics:

- “Machine Account Settings” on page 87
- “Machine Account” on page 94
- “Test machine connection settings” on page 98

In addition to the panels, a number of less-frequently used commands are available from the menus:

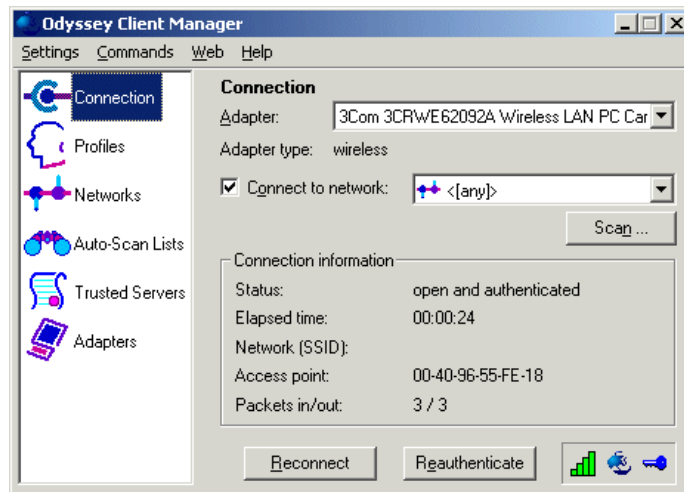
- Settings menu

- Commands Menu
- Web Menu
- Help Menu

Finally, some commands are available if you right-click the Odyssey icon in the System Tray.

Connection panel

The **Connection** panel lets you select an adapter, establish a connection on it, and display your current connection status.



You can perform the following tasks in the **Connection** panel:

- Select an adapter with which to make your network connection
- Connect to a network (wireless connections only)
- Connect using profile (wired connections only)
- Configure multiple simultaneous network connections
- Scan for wireless networks
- Reconnect to a network
- Reauthenticate to a network
- Disconnect from a network connection
- View connection information

- View informational graphics and detailed status

***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, then you can use the **Adapter** drop-down 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.

The **Connect to network** checkbox on the **Connection** panel lets you connect and disconnect from the wireless network. If you want to be connected to a wireless network, make sure this box is checked.

The drop-down list to the right of **Connect to network** lets you select a wireless network or auto-scan list to connect to. The only items that appear on this list are the individual networks that you have already configured using the **Networks** panel, and auto-scan lists that you have specified using the **Auto-Scan Lists** panel.

Any auto-scan lists that you have already 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.

Both networks and auto-scan lists have icons before the name:

-  for networks
-  for auto-scan lists

To connect to a network that you have already configured:

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

If you have selected an auto-scan list, then the first network in the list that responds to the authentication request is generally 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 profile.

The **Connect using profile** checkbox lets you connect and disconnect from the wired 802.1X network switch. If you want to be connected, make sure this box is checked.

The drop-down list to the right of **Connect using profile** lets you select the profile you want to use for the wired connection. All profiles that you have already specified in Odyssey appear on the list.

To connect using a profile that you have already specified:

- 1 Select the profile from the drop-down list to the right of **Connect using profile**.
- 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 installed on your machine and configured with Odyssey Client.

To connect to more than one configured network using multiple adapters:

- 1 Select an adapter from the **Adapter** drop-down 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 these steps for each adapter whose network connection you want to establish.

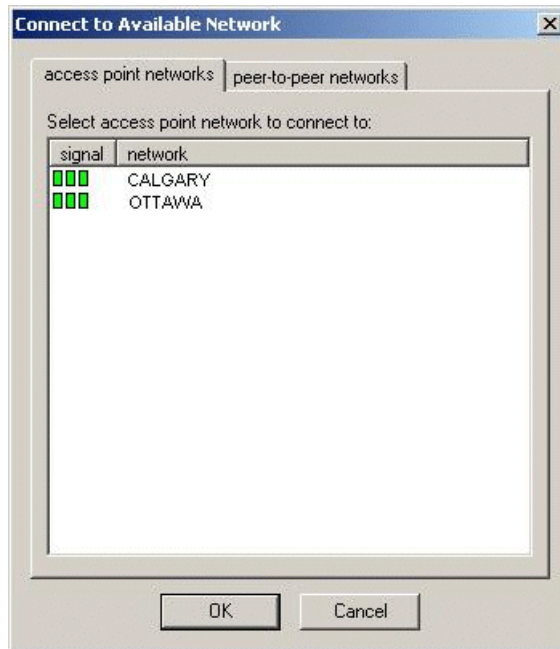
You can use the **Adapter** drop-down list on the **Connection** panel to toggle between the adapters you have configured for multiple network connections, and hence monitor your multiple network connections.

Scan for wireless networks

If you travel frequently, you may want to 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.



- 2 Select the network to which you want to connect, and click **OK**.
 - If you have already configured the settings for this network, Odyssey Client attempts to connect to it using those settings.
 - If you have not yet configured settings for this network, the **Network Properties** dialog first appears. Specify settings and click **OK**. 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 enter the network from the **Networks** 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 brand new

connection to the selected wireless network. The new connection may be with a different access point (on the same network) than your previous connection, depending on factors such as signal strength. If authentication is in use on this network, you are reauthenticated when the new connection starts. If dynamic encryption keys are in use, they are refreshed. 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 is able to provide better service.

Reauthenticate to a network

When you click **Reauthenticate** on the **Connection** panel, Odyssey Client reauthenticates you over the 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 connection

To disconnect a network connection, uncheck **Connect to network** for wireless connections, or **Connect using profile** for wired connections.

View connection information

The **Status** field on the **Connection** panel displays the current status of your connection to the network through this adapter. One of the following messages appears:

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.

Status message	Definition
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.
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
disconnected	You are not connected, and Connect to network may be unchecked. <i>See “Connect to a network (wireless connections only)” on page 30 for how to connect.</i>
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.

The **Elapsed time** field on the **Connection** panel displays the time that has elapsed since the current connection has begun.

The **Network (SSID)** field displays the name of the wireless network to which you are connected. See “Wireless network names” on page 16. 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 MAC address of the wireless access point to which you are connected. (A MAC address is a unique 48-bit number encoded into a device by the manufacturer.)

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

Three graphical status buttons at the bottom right corner of the **Connection** panel give you a visual indication of the status of your connection:

- 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 these buttons:

- *Using the mouse:* Point to a graphical status button with the mouse, and hold down the left-click button.
- *Using the keyboard:* **Tab** over to 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 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 or not encryption keys are in use over 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 types of keys in use and their lengths, measured in bits.

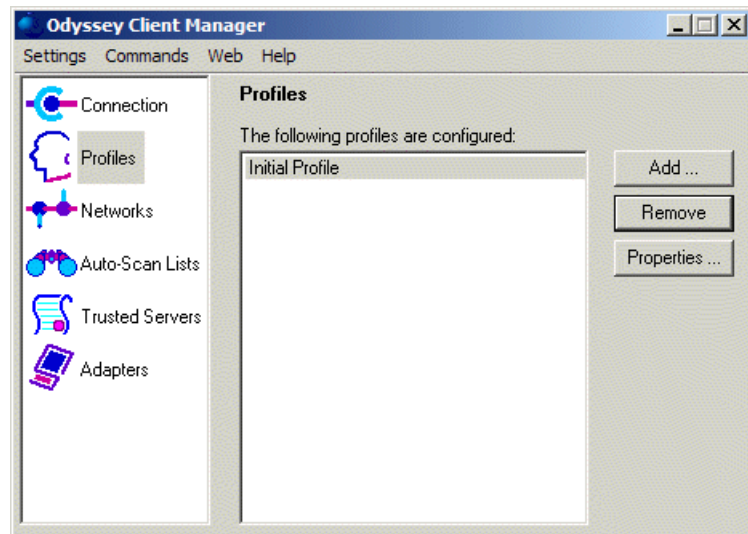
NOTE: An encryption key has a secret part that is either 40 or 104 bits long, and a 24-bit long non-secret part that changes for each packet. Thus, the total key is either 64 or 128 bits long. **Odyssey Client Manager** reports the length of the secret part, which is either 40 or 104 bits.

Profiles panel

An Odyssey Client *profile* contains all the information necessary to authenticate you to the network. This includes information such as your login name, your password or certificate, and the protocols by which you can be authenticated. Your profile is, in effect, the identity that you present to the network and the means that you use to prove that identity.

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 all the profiles that have been 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.



Each profile you configure is displayed in the list.

- To add a profile, click **Add**. The **Profile Properties** 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 dialog

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 new profile to Odyssey Client, type a unique name for the profile in the **Profile name** field of the **Add Profile Properties** dialog. For example, you may want to use **Office**, for your profile associated with your place of employment, and **Home** for your home network.

Once you specify and save a profile, you do not have the ability to edit the profile name when you edit any of its other profile properties. You can, however, remove the profile and create a new one with a different name.

In addition to the profile name, you can configure (and edit) the following information in a profile:

- Login name
- Password and/or certificate
- A specification of the authentication protocols that can 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

The **User Info** tab lets you configure the name you use to log in, as well as your password and/or certificate information.

The screenshot shows the 'Add Profile' dialog box with the 'User Info' tab selected. The 'Profile name' field contains 'Office'. The 'Login name' field contains 'ACME\george'. Under the 'Password' section, the 'Permit login using password' checkbox is checked, and the 'use Windows password' radio button is selected. There is an empty text field for a password and an 'Unmask' checkbox. Under the 'Certificate' section, the 'Permit login using my certificate:' checkbox is unchecked, and there is an empty text field. At the bottom of the certificate section are 'View ...' and 'Browse ...' buttons. The dialog has 'OK' and 'Cancel' buttons at the bottom.

Login name

Enter your user name into the **Login name** field. This is the name that is presented to the network when you authenticate. If you are authenticating 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.

Note the following:

- If you are logged in to 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 populates this field with your user name only.
- 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.

Password

Check **Permit login using password** 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 **use Windows password** if you want to authenticate to the network using the same password you present when you log in to Windows. *You cannot select this option if you are running under Windows 98, 98 SE, or Me.*
- Select **prompt for password** if you want Odyssey Client to prompt you when it is time to authenticate.
- 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.

NOTE: *If you are running under Windows 98, 98 SE, or Me, and you have selected the **use the following password** option, you must reenter the password in this field whenever you change your Windows password.*

If you select **prompt for password**, you are generally only prompted the first time you are authenticated after startup. Odyssey Client remembers this password and reuses it for the duration of your Windows session. The password you enter applies 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 Windows password when connecting to the network on some occasions, including the following:

- If 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.
- If you are required to change your Windows password periodically, and you are accessing the network with EAP-TTLS or PEAP authentication before Windows logon

Certificate

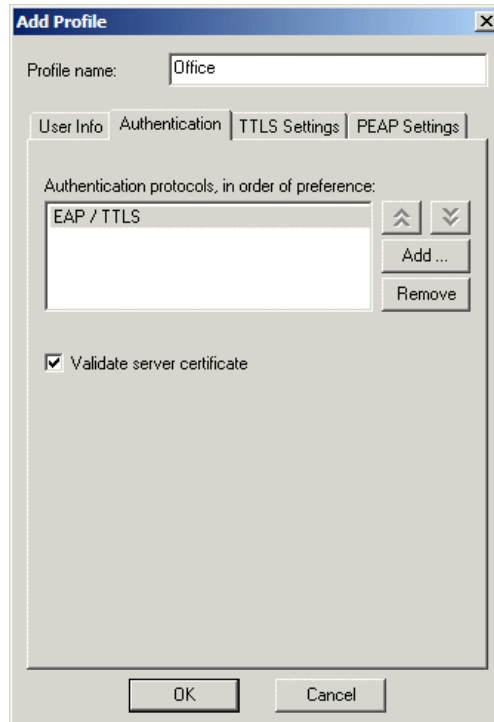
Check **Permit login using my certificate** to enable authentication methods that use your certificate for authentication.

To select a personal certificate with which to authenticate, click **Browse**. A list of your personal certificates appears. Select a certificate and click **OK**.

***NOTE:** This is an advanced feature. See your network administrator for information on which certificate to select if you require one.*

Authentication

The **Authentication** tab lets you specify the protocols that authenticate you to the network.



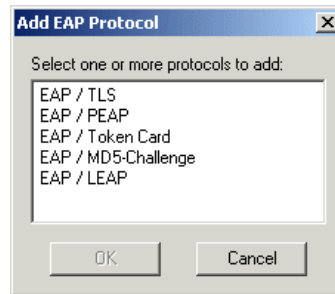
Selecting Authentication Protocols

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:

- To add a protocol to the list, click **Add**. The **Add EAP Protocol** dialog 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.



- To remove a protocol, select the protocol, and click **Remove**.
- To reorder protocols, select a protocol and use the up and down arrow buttons to reposition it.

Validating 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.

Check **Validate server certificate** to verify the identity of the authentication server based on its certificate when using EAP-TTLS, PEAP, and EAP-TLS. (This is checked by default.)

You can select trusted authentication server certificates using the Trusted Servers panel. See *“Trusted Servers panel”* on page 56.

You should, as a general rule, check **Validate server certificate**. You do have the option of turning off this important security precaution, only because there may be circumstances that require it. You should only do so when your network administrator instructs you to.

TTLS Settings

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

The screenshot shows the 'Add Profile' dialog box with the 'TTLS Settings' tab selected. The 'Profile name' field contains 'Office'. The 'Inner authentication protocol' dropdown menu is set to 'MS-CHAP-V2'. Below this, there is a section for 'Inner EAP protocols, in order of preference' with an empty list box and 'Add...' and 'Remove' buttons. At the bottom, there is an 'Anonymous name' section with a text box containing 'anonymous'.

Profile name:

User Info | Authentication | **TTLS Settings** | PEAP Settings

Inner authentication protocol:

Inner EAP protocols, in order of preference:

↑ ↓

Add ...

Remove

Anonymous name

When using EAP-TTLS exclusively, you can keep your login name private and reveal only an anonymous name on the network; for example, "anonymous" or "anonymous@myisp.com".

Anonymous name:

OK Cancel

EAP-TTLS works by creating a secure, encrypted tunnel through which you present your credentials to the authentication server. Thus, inside EAP-TTLS there is yet another *inner authentication protocol* that you must configure. See “EAP-TTLS” on page 21.

Selecting the Inner Authentication Protocol

Select from the drop-down list at the right, the **Inner authentication protocol** you want to use. You can select any of the following:

- PAP
- CHAP
- MS-CHAP
- MS-CHAP-V2
- PAP/Token

- EAP

The most commonly used protocol is MS-CHAP-V2. It allows you to be authenticated against a Windows Domain Controller as well as other, non-Windows user databases.

CHAP is the most common protocol for authenticating against non-Windows user databases.

***NOTE:** You cannot use CHAP as your inner authentication method if you are authenticating against a Windows NT Domain or Active Directory. As a result, do not choose CHAP when authenticating against the Odyssey server since it can only authenticate against a Windows Domain or Active Directory.*

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

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

Using EAP as an inner authentication protocol

If you select EAP as your inner authentication protocol, you must configure the list of **Inner EAP protocols** with one or more protocols.

- To add a protocol to the list, click **Add**. The **Add EAP Protocol** dialog 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 only the protocols you have not already added are available.
- To remove a protocol, select the protocol and click **Remove**.
- To reorder protocols, select a protocol and use the up and down arrow buttons to reposition it.

Setting an anonymous name

EAP-TTLS has a unique feature that other protocols do not offer. Because it sets up an encrypted tunnel for your credentials, it is also able to pass your login name through that tunnel. That means that not only are your credentials secure from eavesdropping, but your identity is protected as well.

Thus, with EAP-TTLS you have two identities: an inner one, and an outer one. The inner identity is your actual login name, and is taken from the **Login name** field in the User Info tab. Your outer identity can be completely anonymous. Set your outer identity in the **Anonymous name** field.

As a general rule, set **Anonymous name** to `anonymous`, that is, its default value. 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, and you may be required to use `anonymous@acme.com`. Your network administrator can tell you how to configure this field correctly.

***NOTE:** Your outer identity can be anonymous only if EAP-TTLS is the only authentication protocol configured on the **Authentication Protocols** tab. If other protocols are also enabled, Odyssey Client cannot keep your identity private, and the **Anonymous name** field is disabled. If you would like the anonymity EAP-TTLS provides, you must configure EAP-TTLS as the sole authentication protocol.*

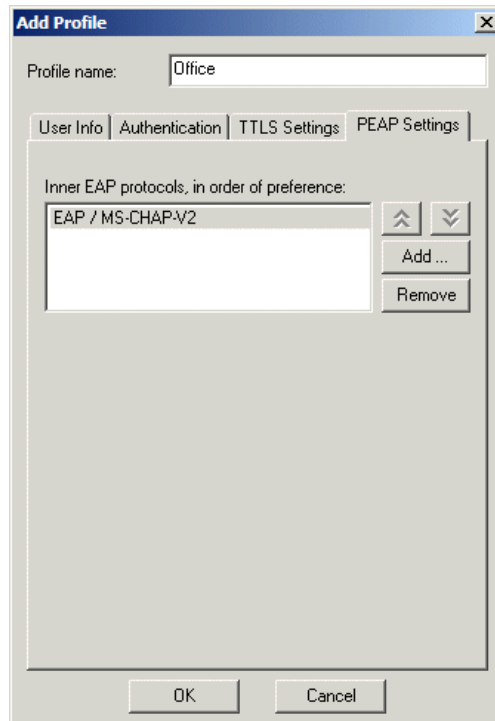
PEAP Settings

If you select **EAP/PEAP** as an authentication method in the **Authentication** tab, then you can use up to three inner EAP authentication methods:

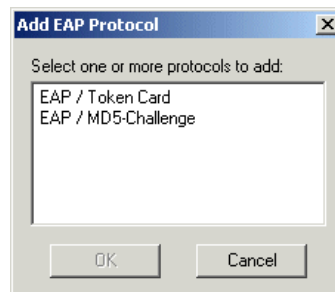
- EAP/MS-CHAP-V2
- EAP/Token Card
- EAP/MD5-Challenge

To add or remove any inner authentication methods used with PEAP:

- 1 Go to the **PEAP** tab.



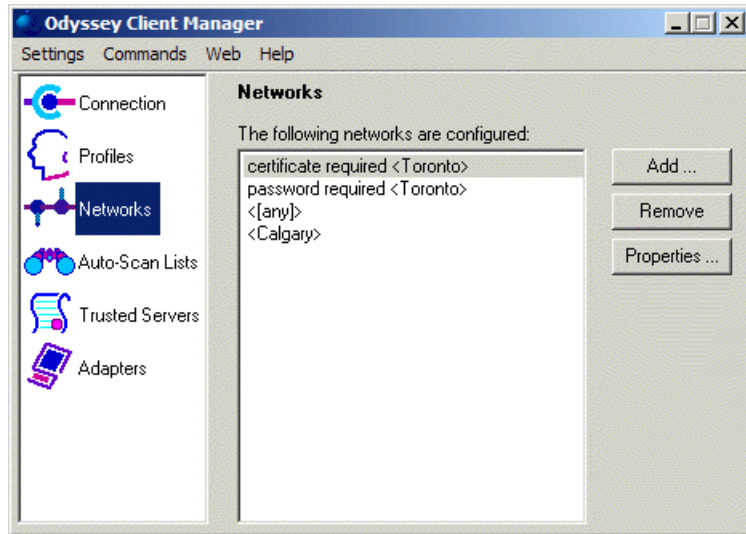
- 2 Click **Add** to add a protocol. The **Add EAP Protocol** dialog appears. Select one or more protocols to add and click **OK**. Note that any protocols you have already selected are not listed in this dialog.



- 3 Select any protocols you want to remove and click **Remove**.
- 4 Click **OK** when you are completely done modifying the profile configuration.

Networks panel

The **Networks** panel allows you to configure settings for connecting to any number of wireless networks.



Each configured network is listed. You can perform the following tasks in the **Networks** panel:

- To add a network, click **Add**. The **Network Properties** dialog 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 listed 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 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

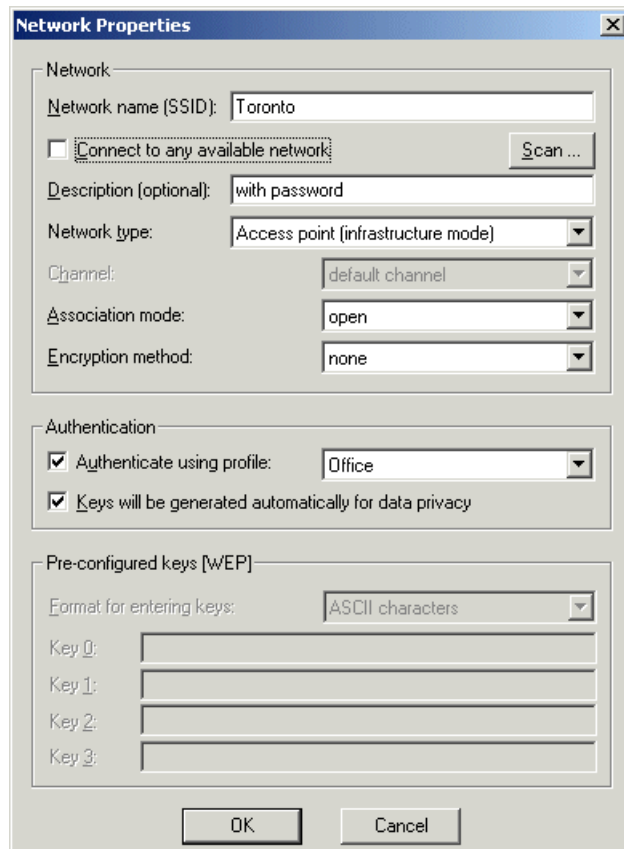
can add your own description to any network you configure. This helps you to distinguish networks.

The network description field is useful for situations that advanced users might encounter. It lets you easily switch among different “personalities” on the same network. For example, you may want to use different credentials at different times. The description field also lets you distinguish two different networks that happen to have the same network name. Network names are arbitrary text chosen by an administrator, so it is possible for two unrelated networks to have the same name.

In the illustration above, there are two `Toronto` networks. The configured descriptions indicate that password credentials are used with one and certificate credentials with the other.

Network Properties

You can configure wireless network settings in **Network Properties**. Click **Add** or **Properties** from the **Networks** panel to view it.



The screenshot shows the "Network Properties" dialog box with the following settings:

- Network**
 - Network name (SSID): Toronto
 - ☐ Connect to any available network (with a Scan ... button)
 - Description (optional): with password
 - Network type: Access point (infrastructure mode)
 - Channel: default channel
 - Association mode: open
 - Encryption method: none
- Authentication**
 - ☒ Authenticate using profile: Office
 - ☒ Keys will be generated automatically for data privacy
- Pre-configured keys [WEP]**
 - Format for entering keys: ASCII characters
 - Key 0: (empty)
 - Key 1: (empty)
 - Key 2: (empty)
 - Key 3: (empty)

At the bottom are OK and Cancel buttons.

You can configure the following network attributes here:

- Network fields
- Authentication fields
- Preconfigured keys (WEP or WPA)

Network fields

You can perform the following tasks in this section of the **Network Properties** dialog:

- Specify the network name
- Scan for a network
- Configure Odyssey to connect to any available network
- Specify a description of the network
- Specify the network type
- Specify the association mode
- Specify an appropriate encryption method for your 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. This name must be entered correctly in order to successfully connect.

Scan for a network

You can type in the name of the network directly, 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 not only easier than typing, but also 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 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 practice is to use **[any]** without 802.11 or 802.1X authentication.

Specify a description of the network

Network descriptions are useful for distinguishing 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.

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 one or more other PCs.

Specify the association mode

Before authentication can take place, you must associate your client 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 (WEP) with preconfigured keys” on page 17 and “Wi-Fi Protected Access (WPA) and TKIP encryption” on page 18 for more information on these encryption and association mode choices.

You can choose one of three 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 WPA.
- **Shared**, for connecting to a network through an access point that requires WEP keys for association and data encryption.
- **WPA**, for connecting to a network through an access point that implements WPA (Wi-Fi Protected Access).

Specify an appropriate encryption method for your association mode

Your choice of encryption method also depends on the access point requirements. Your choices vary according to the association mode you choose. See “Wired-Equivalent Privacy (WEP) with preconfigured keys” on page 17 and “Wi-Fi Protected Access (WPA) and TKIP encryption” on page 18 for more information.

You have the following options:

- **none**, for using 802.1X authentication without WEP keys. This option is only available to you when you configure access point association in open mode.
- **WEP**, for using WEP keys for data encryption. This option is available for all association modes, and is required when you associate in shared mode. When you select this option, you must fill in WEP keys in the lower portion of **Network Properties**. You must choose this option when the access points in your network require shared mode association with WEP keys.
- **TKIP**, for using the temporal key integrity protocol. Choose this option when the access points in your network require WPA 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 association, and are configured for AES data encryption.

Authentication fields

You can configure network authentication with the following characteristics:

- Authenticate using profile
- Automatic key generation

Authenticate using profile

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 onto this network.*

When you check **Authenticate using profile**, Odyssey Client performs an 802.1X authentication using your password, certificate, or by other means, as is configured in the selected profile.

Automatic key generation

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, PEAP, and EAP-TLS, generate keys. Others do not. If you use EAP-TTLS, PEAP, 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. Leave this option unchecked if you are required to use preconfigured WEP keys, or, in the case of WPA association, a pre-shared key.

Preconfigured keys (WEP or WPA)

The wireless network may require that you preconfigure WEP keys, or that you pre-share a passphrase, in the case of WPA association. You can enter keys in the lower portion of **Network Properties**.

Pre-shared keys (WPA)

If you associate in WPA mode, and you do not generate keys automatically when you associate an authentication profile to the network connection, then you must supply a pre-shared ASCII passphrase in **Passphrase** field. This passphrase is used as a seed to generate the required keys.

Preconfigured keys (WEP)

If you associate in shared mode, you must configure at least one WEP key. You must also configure at least one WEP key when you select WEP encryption for the open association mode, and you do not generate keys automatically when you associate an authentication profile to the network connection. WEP keys serve the following purposes:

- Associate with an access point before a connection can be established (shared mode).
- Encrypt data between your PC and the access point (or other PCs in a peer-to-peer network)

See “Wired-Equivalent Privacy (WEP) with preconfigured keys” on page 17.

If the wireless network uses 802.1X authentication and dynamic WEP keys are generated (i.e., 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 one when your profile is set to authenticate with this method.

If you implement either of these uses of preconfigured WEP keys, you must check the appropriate boxes and set one or more WEP keys appropriately:

- Check **to authenticate to access points (shared mode)** if preconfigured WEP keys are required to authenticate to an access point prior to connection to the wireless network.
- Check **for data privacy** to use preconfigured WEP keys for encryption of data over the wireless network.

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.

# of bits in key	# of ASCII chars	# of hex digits
40	5	10
104	13	26

To enter any preconfigured WEP keys:

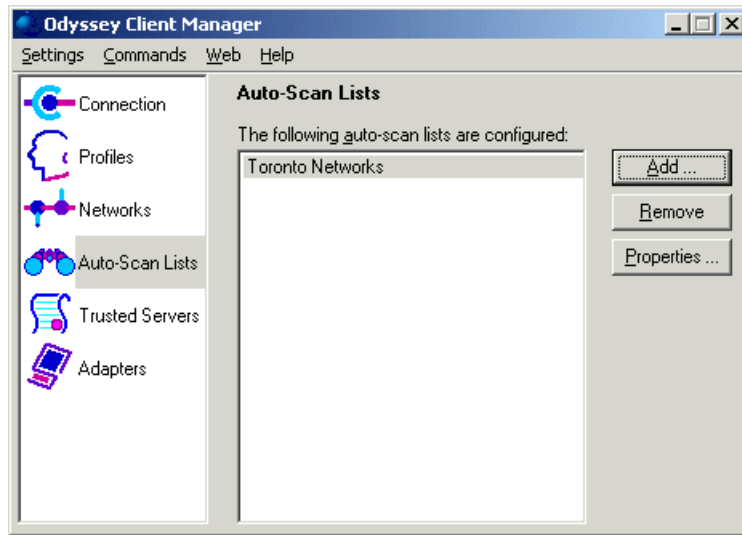
- 1 In **Format for entering keys**, select either **ASCII characters** or **hexadecimal digits**, depending on how you want to enter the keys.
- 2 Type in the text fields **Key 0** through **Key 3**, each key that you want to preconfigure.

Auto-Scan Lists panel

You can associate an ordered group of wireless networks with an *auto-scan list*, so that you can be connected to any of the networks available in the list. 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 connections panel to an auto-scan list, rather than a single network, Odyssey scans sequentially through the listed networks for an available network. You may want to use this feature if you are moving your client machine between locations that access different networks.

You can specify auto-scan lists from the **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.

The **Auto-Scan Lists** panel displays the lists that you have created so far.

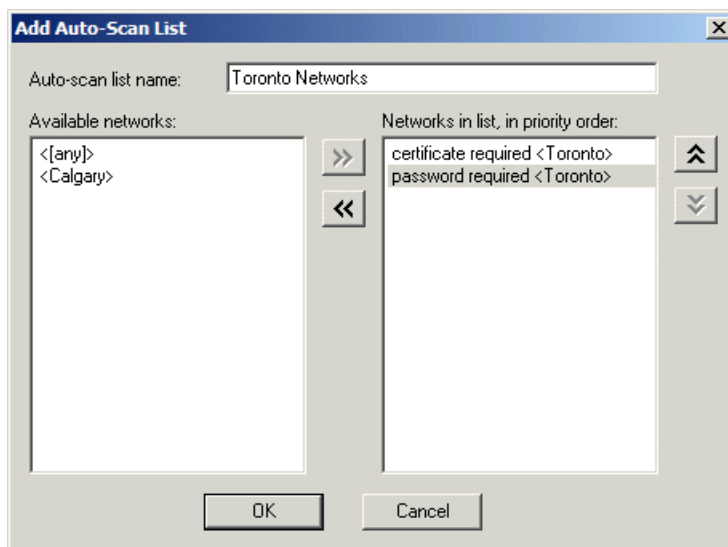
You can perform the following tasks in the **Auto-Scan Lists** panel:

- To add an auto-scan list, click **Add**. The **Auto-Scan List Properties** dialog appears.
- To remove an auto-scan list, select it from the list and click **Remove**.
- To modify the settings for a network, select it from the list and click **Edit**, or double-click the auto-scan list name. The **Auto-Scan List Properties** dialog appears.

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

Auto-Scan List properties

You can add or edit auto-scan list properties when you click **Add** or **Properties** from the **Auto-Scan Lists** panel. The resulting dialog allows you to manage lists of the wireless networks that you have configured with the **Networks** panel.



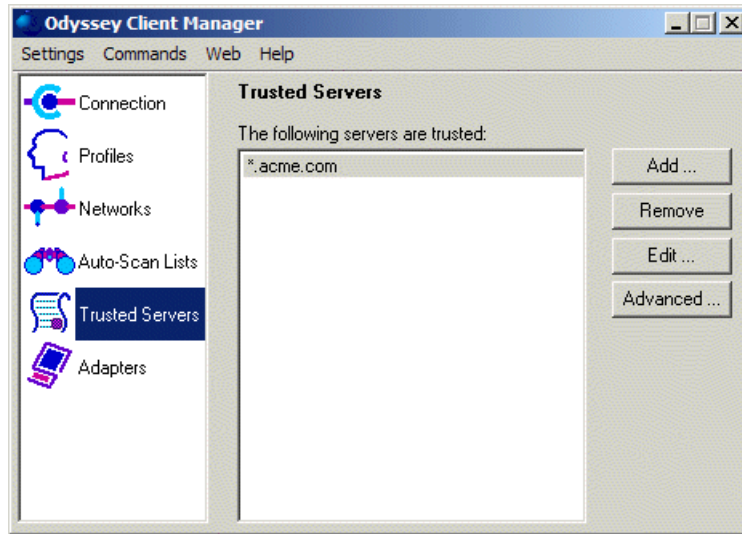
To specify a new auto-scan list:

- 1 Provide the **List name**. You must fill this field in before you click **OK**. You cannot choose a list name you have already used, and you cannot edit this name later when you click **Properties** for a selected list in the **Auto-Scan Lists** panel.
- 2 Sequentially 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 **Selected Networks** 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. You can use the up and down arrows to reorder the list. You can modify this list order or contents at any time when you click **Properties** of the list by this name from the **Auto-Scan Lists** panel.

In general, you increase likelihood of connection to a given network (in comparison with other available networks in the same auto-scan list) by moving it up towards the top of the list.

Trusted Servers panel

The **Trusted Servers** panel allows you to configure which authentication servers you trust for the purpose of logging you in to the network.



When you configure trust in a server, you must not only specify the name of the server, but also the certificate chain to which it belongs. Odyssey Client is very flexible in how trust can be configured, and provides both a simple and an advanced method for specifying trusted servers.

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

- “Extensible Authentication Protocol (EAP)” on page 19
- “Certificates” on page 20

Using the simple method to configure trust

In the large majority of cases, you can use the simple method of configuring trust.

With this method, you must specify two items:

- The server domain name, or the ending of the domain name (for example, acme.com)
- The certificate of any certificate authority in the chain. This could be the certificate of a root or an intermediate certificate authority

Domain Names

Each server has a domain name that uniquely identifies it and that domain name is normally contained in the Subject CN field of the server certificate.

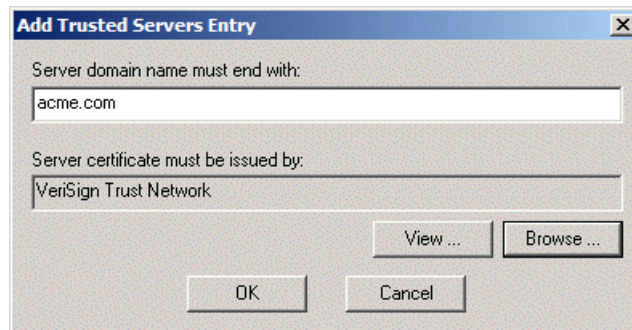
A server domain name ends with the name of a larger administrative domain, to which the server belongs. For example, the Acme company might have the a domain name, such as `acme.com`. The company might also have several authentication servers, with the names `auth1.acme.com`, `auth2.acme.com`, and `auth3.acme.com`, for example.

As is apparent from this example, by specifying what the server domain name must end with, you can configure trust for all the servers in an organization with a single entry.

Adding a trusted server entry

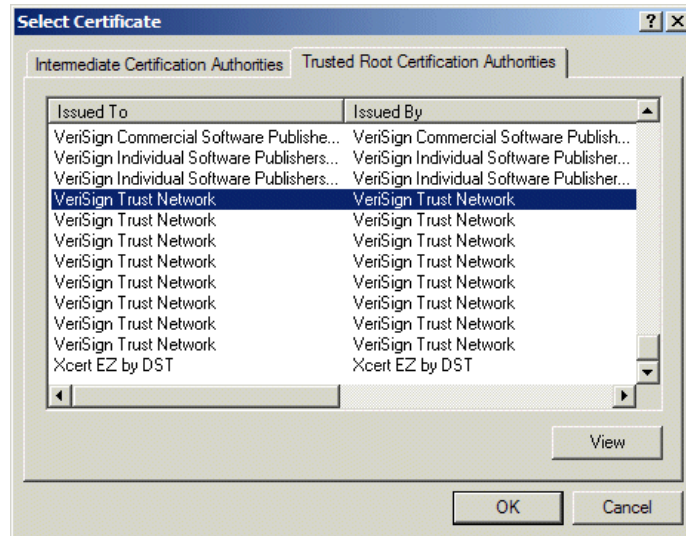
To add an entry to the trusted servers list, follow these steps:

- 1 Click **Add**. The **Add Server** dialog appears.



- 2 In the **Server domain name must end with** field, enter the name (or final elements of the name) of the domain to which the trusted server must belong. You are not allowed to leave this entry blank.
- 3 Set the **Server certificate must be issued by** field to the certificate of the certificate authority that must have directly or indirectly issued the server certificate. To assign a certificate, follow these steps:
 - a Click **Browse** to get a list of certificates.

- b Select one from the list, and click **OK**.



The certificate you select may be that of a root or intermediate certificate authority. It need not be the certificate that directly issued the server certificate. It may be any certificate in the chain.

Removing a trusted server entry

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

Editing a trusted server entry

To edit an entry in the trusted servers list, select the entry and click **Edit**. The **Edit Trusted Servers Entry** dialog appears, allowing you to modify the server domain and the certificate of the issuer.

Using the advanced method to configure trust

If you need more control over trust, you can use the advanced method.

***NOTE:** If you do not have a working knowledge of certificates and certificate chains, you should not attempt to configure trust using the advanced method. Consult your network administrator as to how to configure trusted servers.*

With this method, the entire tree of trust is displayed. The trust tree shows trusted servers added using the simple method as well as the advanced.

Each path through the trust tree defines a set of rules for matching a certificate chain. Odyssey Client trusts an authentication server only if its certificate chain matches at least one path through the trust tree.

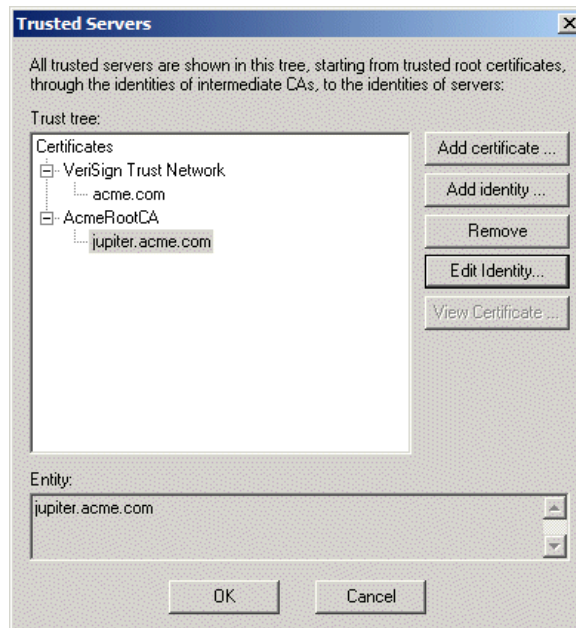
A path through the trust tree is composed of two or more nodes:

- Each top-level node is the certificate of a root or intermediate certificate authority.
- Each intermediate node (if present) is the name of an intermediate certificate authority in the chain.
- Each final, or leaf, node is the name of a server that you trust to authenticate you.

The names of certificate authorities and servers may be specified as subject names or as domain names. In addition, you may specify that the name in a certificate must match the configured name exactly or that it must end in the configured name.

Displaying the trust tree

To display the trust tree, click **Advanced**. The **Trusted Servers** dialog appears, allowing you to view and modify trust rules.

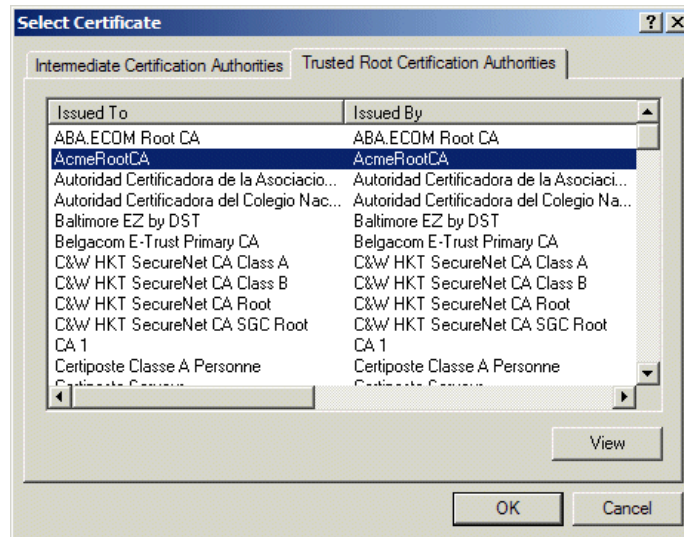


Adding certificate nodes

To add a new certificate to the top level of the trust tree:

- 1 Click **Add certificate**. The **Select Certificate** dialog appears.
- 2 Select a certificate and click **OK**. You may select either from the list of intermediate or trusted root certificates.

For detailed information about any certificate before you add it, select the certificate and click **View**.



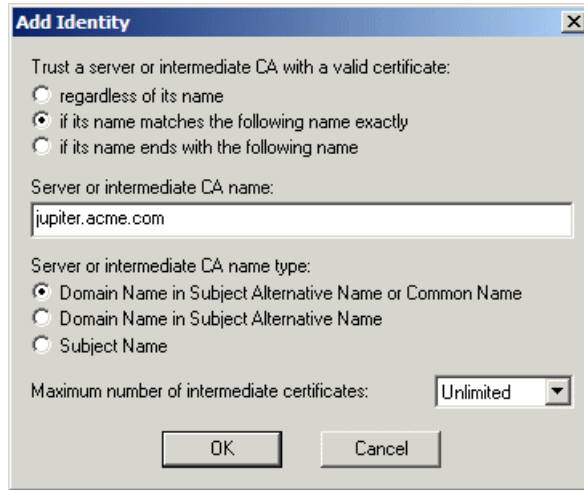
Adding authentication servers or intermediate CA nodes

All nodes below the top level identify either authentication servers or intermediate certificate authorities. If the node is a leaf node, it is assumed to identify an authentication server. Otherwise, it is assumed to identify an intermediate certificate authority.

To add an authentication server or intermediate certificate authority to the tree:

- 1 Select the node in the tree, beneath which you want to add the new item.
- 2 Click **Add Identity**. The **Add Identity** dialog appears.
- 3 Enter the information that defines the rules that Odyssey Client uses to match a certificate in the server certificate chain to this node.

4 Click **OK**.



The **Add Identity** dialog lets you set the matching rules for a single node in the trust tree.

For **Trust a server or intermediate CA with a valid certificate**, select:

- **regardless of its name** to match any certificate, provided it is signed by the certificate authority in the node above
- **if its name matches the following name exactly** to require that the name in the certificate exactly match the name you specify
- **if its name ends with the following name** to require that the name in the certificate is subordinate to the name you specify. For example, a certificate with name sales.acme.com would match an entry of acme.com

For **Name of server or intermediate CA**, enter the name (or final elements of a name) you want to match. (This field is not required if you select **regardless of its name**). The form of the name depends on your choice of **Name type**.

For the certificate authority **Name type**, you must indicate how the name is interpreted and where in the certificate the name is found. Select one of the following:

- **Domain name in Subject Alternative Name or Common Name** if the domain name (e.g., acme.com) is found in the Subject Alternative Name field in the certificate or, if that is not present, the Common Name within the Subject field of the certificate (*this is the most typical choice*).
- **Domain name in Subject Alternative Name** if the domain name is found in the Subject Alternative Name field in the certificate. This is similar to, but more restrictive than, the previous choice.

- **Subject Name** if the name is an X.500 name and is found in the Subject field in the certificate. If you enter a full or partial Subject name, it must be in X.500 form. It matches any certificate Subject name that is equal or subordinate to it.

For example, if you enter OU=acme.com, C=US it matches any of the following subject names:

O=sales, OU=acme.com, C=US
CN=george, O=sales, OU=acme.com, C=US

***NOTE:** If you enter text that includes commas, each comma must be enclosed by single quotation marks.*

For **Maximum number of intermediate certificates**, set the maximum number of certificates that may appear in the chain between this node and the node directly above this node. You may select a number between **0** and **5**, or **unlimited**:

- If you choose **0**, the certificate that matches this node must have been signed using the certificate that matches the node above this node.
- If you choose **1**, the certificate that matches this node may have been signed by the certificate that matches the node above, or by a certificate that in turn has been signed by the certificate that matches the node above.
- If you choose **unlimited**, any number of certificates may appear in the chain between the certificate that matches this node and the one that matches the node above.

Removing nodes

To remove a node, select the node in the tree you want to remove, and click **Remove**. The selected node, and any node beneath it is removed from the tree.

The node you remove may be of any of the following:

- Top level certificate node
- Intermediate CA node
- Server node

Viewing certificate information

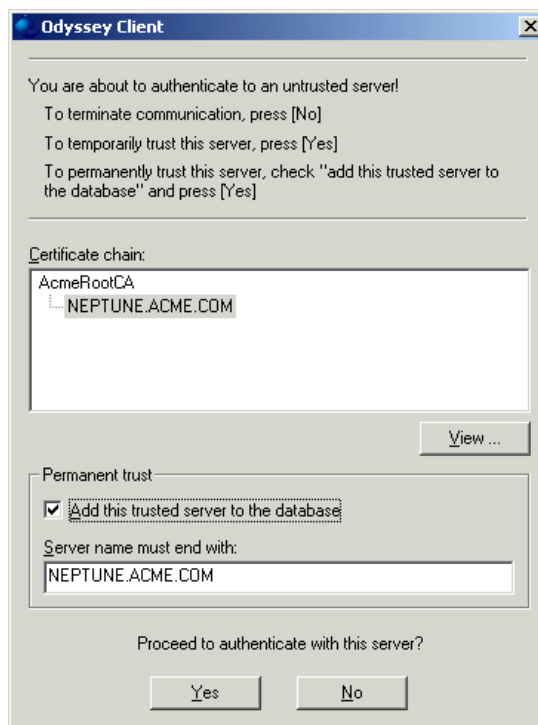
For detailed information about any certificate at the top level of the trust tree, select the certificate and click **View Certificate**.

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 of the server certificate (in the example shown below, the certificate ACMERootCA) is installed on your client machine.

If this is the case, the following dialog appears while you are authenticating to the network.



The 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 temporarily trust this server (i.e., until Odyssey is restarted) in order to 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 want to permanently trust this server by adding to the **Trusted Servers** list, check **Add this trusted server to the database** and click **Yes**. The server is added to the **Trusted Servers** list, using the name shown in the **Server name must end with** field. 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

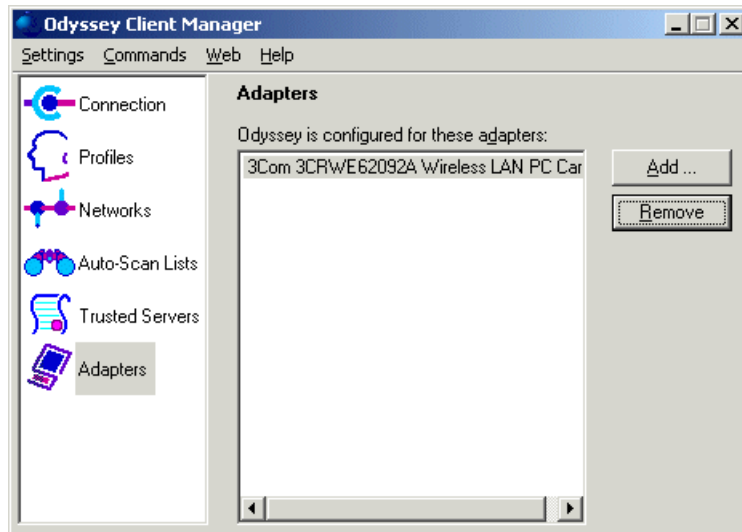
The **Adapters** panel lets you select one or more network adapters (interface cards) for wired or wireless networking. You can select more than one adapter if you hold down **Ctrl** on your keyboard as you select with your mouse.

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

You can use the **Adapters** panel for the following tasks:

- Adding a wireless or wired adapter
- Removing an adapter from the list of adapters

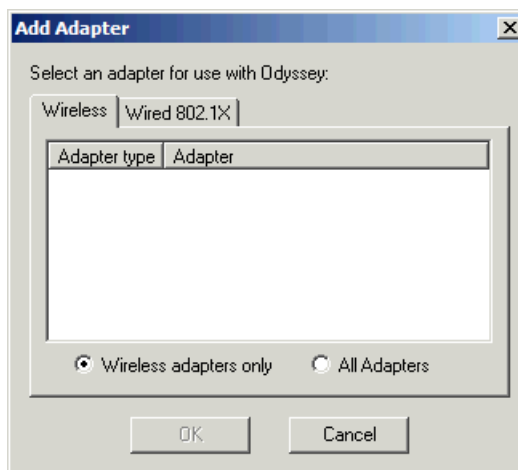
NOTE: *Your adapter must already have been installed on your system before you can configure Odyssey Client to use it.*



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 appears, displaying a list of all network adapters that are installed on your PC (except for the ones Odyssey Client is already configured to use).
- 2 Select either the **Wireless** or **Wired 802.1X** tab.



- 3 Select your desired adapter from the list of adapters displayed, and click **OK**. Note that you only adapters that you have not yet added to the **Adapters** panel are displayed.

While in most cases, **Odyssey Client Manager** can distinguish between wireless and non-wireless network adapters, in certain cases it cannot. If you do not see your wireless adapter in the list, select **All Adapters**.

WARNING: Make sure that all adapters you select on the **Wireless** tab are indeed wireless. A wired adapter does not behave correctly if you configure Odyssey Client to install it as 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**.

Odyssey Client stops using the adapter. The adapter is still installed on your system, but operates as if Odyssey Client is not present.

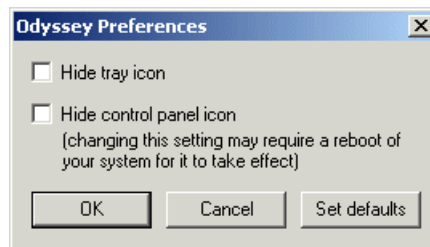
Settings menu

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

- Preferences
- Security settings
- Windows Logon Settings
- Enable/Disable Odyssey
- Close

Preferences

You can change the way that Odyssey Client operates by selecting the **Preferences** command. The Odyssey **Preferences** dialog appears.



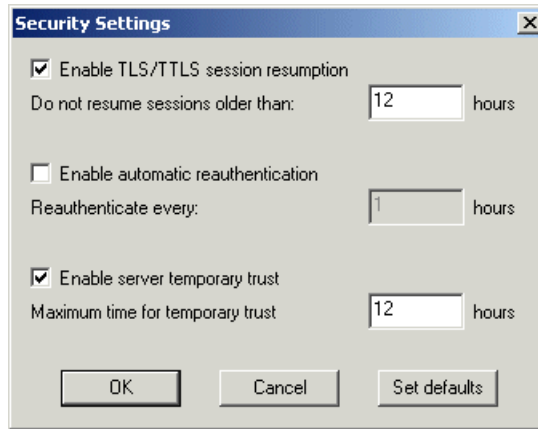
Set your preferences, and click **OK** to make them effective:

- If you select **Hide tray icon**, then the Odyssey icon is not displayed on the System Tray (at the bottom right of your screen).
- If you select **Hide control panel icon**, then the Odyssey icon is not displayed on the Windows Control Panel.

NOTE: *If you have the Windows Control Panel open when you select **Hide control panel icon** and click **OK**, then refresh your control panel (press **F5**) to see the effects. In some cases, you may only see the effect after rebooting.*

Security settings

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



The security options are initially set to default values that should suit most purposes. You can restore the defaults at any time by clicking **Set defaults**.

Time fields are expressed in hours, with up to two decimal places. For example, to specify one hour and fifteen minutes, enter **1.25**.

Session resumption

You can enable the use of session resumption from the **Security Settings** dialog. See "Session resumption" on page 22 for more information on session resumption.

To use enable session resumption:

- Check **Enable session resumption**.
- Set **Do not resume sessions older than** to the maximum number of hours that an initial authentication can be used to accelerate reauthentication. Once the time limit has elapsed, a completely fresh authentication is performed on your next reauthentication. The number of hours can have up to two decimal places. For example, enter **1.25** to indicate one hour and fifteen minutes.

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 as well. For information about why you might want to reauthenticate, see “Reauthentication” on page 23.

Check **Enable automatic reauthentication** in the **Security Settings** dialog, in order to cause Odyssey Client to periodically initiate reauthentication with the server.

Set in **Reauthenticate every**, the time period, in hours, for reauthentication to take place automatically.

Uncheck **Enable automatic reauthentication** in the **Security Settings** dialog, in order to disable this feature.

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.

Server temporary trust

Normally, you can use the **Trusted Servers** panel to configure the servers you trust for authentication. However, there may be times when you are visiting 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 **Security Settings** dialog, in order 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 option of whether or not to trust an untrusted server temporarily when you attempt to authenticate to an untrusted server. See “**Untrusted servers**” on page 63.
- The **Untrusted Server** dialog that opens when you attempt to authenticate to a server for which you have not configured trust, permits you to permanently add the server to your trust tree. Thus, you can use temporary trust as an alternative to the **Trusted Servers** panel, and configure trusted servers as they are encountered.
- 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.

The default behavior is that temporary trust is enabled, and that 12 hours is the maximum time that a particular server is trusted once you accept.

NOTE: These settings are not relevant if you decide to permanently trust the server by checking **Add this trusted server to the database** in the **Untrusted Server** dialog.

Windows Logon Settings

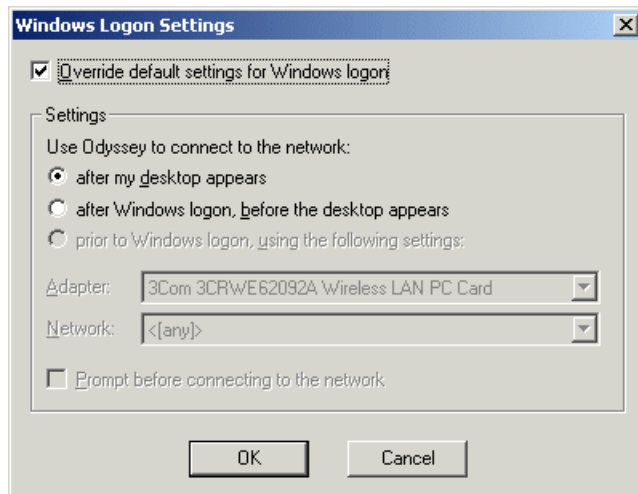
Your default network connection settings are either of the following:

- Factory-default network connection settings, which result in establishing a network connection after your desktop appears
- Default network connection settings that have been set by your system administrator

There may be some circumstances for which you want to override the default network connection settings. For example, if you can logon to your domain using cached credentials, and your administrator has configured your network connection to occur prior to Windows logon time, you can change your connection timing so that you connect to the network before your desktop appears.

You can modify your network connection timing by selecting the **Windows Logon Settings** item from the **Settings** menu.

The following dialog opens when you select **Windows Logon Settings**.



Some of the Windows logon features may not be available to you, depending your how your administrator has set up your installation.

To override the default network connection settings for your client machine, check **Override default settings for Windows logon**. To modify the default timing for network connections through Odyssey, select one of the following Windows logon timing options:

- **after my desktop appears**, for establishing your network connection after your Windows startup, Windows logon, and desktop processes are completed. This is the latest possible time you can make a network connection.
- **after Windows logon, before my desktop appears**, for establishing your network connection after your Windows startup, and Windows logon, processes are completed, but before your desktop processes take place.
- **prior to Windows logon**, for establishing your network connection prior to Windows logon. This is the earliest time you can make a network connection.

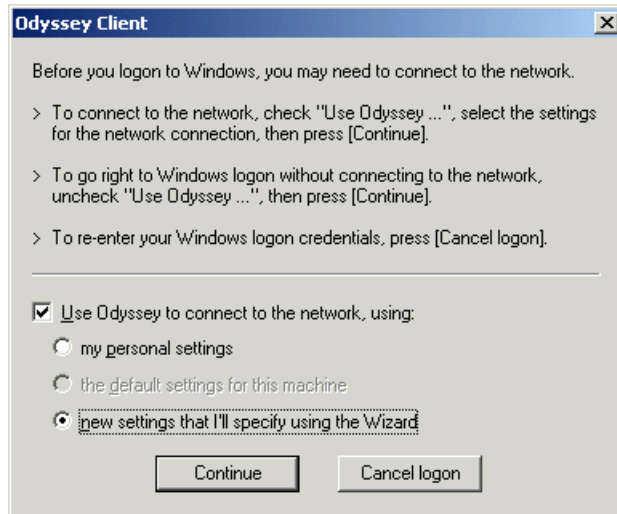
Select one of the timing options that is available to you.

If you select **prior to Windows logon**:

- Select the adapter and network (or profile, in the case of a wired connection) from the lists provided. Note that for any profiles associated with the network connection you select here, you must check **Validate server certificate** on the **Authentication** tab of the **Profile Properties**. You also cannot assign to the network connection a profile that uses a stored password. See “Restrictions on early network connections” on page 91 for more information.
- You can optionally request that a pre-connection prompt dialog appear prior to making the network connection at logon time every time you logon to Windows, by checking **Prompt before connecting to the network**. This can be useful if you experience network authentication problems, as it gives you the option to opt out of connecting to the network at logon time.
 - If you or your administrator have omitted any required configuration elements, you are prompted at logon via the pre-connection prompt dialog configure part or all of the network connection through a wizard. See “Windows logon pre-connection wizard” on page 73 for more information on the pre-connection prompt dialog and the wizard.
 - See “Avoiding the pre-connection prompt dialog” on page 72 for information on how to suppress the appearance of the pre-connection prompt dialog.

Odyssey Client pre-connection prompt dialog

Odyssey Client may give you some options for settings to use at Windows logon through the main pre-connection prompt dialog.



This dialog appears under the following circumstances:

- You or your administrator have configured this dialog to appear each time you attempt a network connection when you logon to Windows. See “Windows Logon Settings” on page 69.
- Your default Windows logon network configuration is not complete.

If your network connection configuration is complete, you have three options for connection settings:

- Use the settings (your personal settings) you have previously specified in the **Odyssey Client Manager**.
- Use the default prior to Windows logon connection settings configured for your machine by your network administrator.
- Use new settings that you can specify using the Windows logon pre-connection wizard.

Specify your preferences, and click **Continue**. You can also opt to cancel the network connection at this time, by clicking **Cancel logon**.

Note the following:

- In the event that your network connection is incomplete, the first two settings are disabled.

- If you want to connect to the network after logon, or if you are having any problems connecting to the network, uncheck **Use *Odyssey* to connect to the network**.
- Odyssey Client does not remember the network choices you enter in the pre-connection prompt dialog. Should you have an incomplete network configuration, you are presented with the pre-connection prompt dialog each time you logon, until you correct any problems. In order to correct any problems and/or not see this screen every time you logon, follow the instructions in “Avoiding the pre-connection prompt dialog” on page 72.

Avoiding the pre-connection prompt dialog

The Odyssey Client pre-connection prompt dialog occurs for one of two reasons:

- You or your administrator have set Odyssey Client to prompt you with this dialog each time you attempt a network connection when you logon to Windows. See “Windows Logon Settings” on page 69.
- Your prior to Windows logon network configuration is not complete.

In either case, you are prompted to interact with Odyssey Client each time you logon to Windows.

To avoid future prompts at pre-connection time:

- 1 Correct network connection problems, as necessary.
- 2 Suppress the appearance of the pre-connection prompt.

Correct network connection problems

Once you are logged on and connected, you can correct any network connection problems that have occurred. To do so, follow these steps in the **Odyssey Client Manager**:

- 1 Specify a profile, network (required for wireless adapters), and adapter, as well a network (if necessary) for your network connection at Windows logon time.
- 2 Test the connection by connecting through the **Connection** panel.

Suppress the appearance of the pre-connection prompt

To keep the pre-connection prompt dialog from appearing every time you logon, follow these steps in the **Odyssey Client Manager**:

- 1 In **Settings > Windows Logon Settings**, check **Override default settings for Windows logon**, select the network (or profile) and adapter you want for this

connection, and uncheck **Prompt before connecting to the network**. Note that any network configuration you assign using the Windows logon pre-connection wizard may include network and profile records stored in the **Odyssey Client Manager** with the name **Windows logon** attached to their labels. If so, you can use these to configure your network connection in Windows Logon Settings.

- 2 Click **OK**.

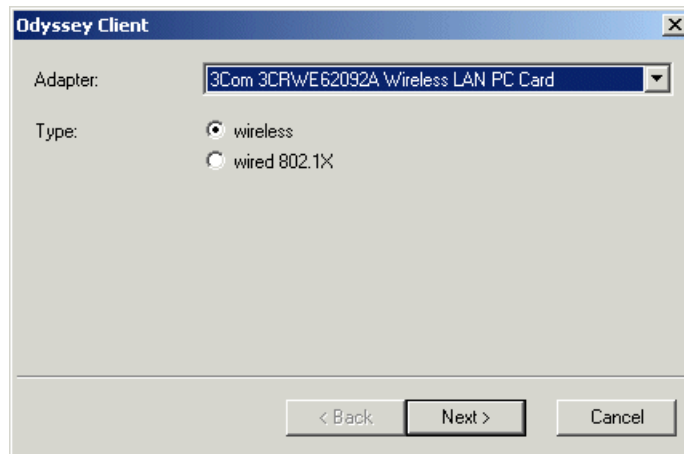
Windows logon pre-connection wizard

It is possible that your configuration is incomplete for Odyssey Client to log you into the network before Windows logon takes place. In this case, once you select to configure your network connection through the Windows logon pre-connection wizard (via the pre-connection dialog), you are prompted with a series of dialogs that request you to specify the following information:

- Adapter for Windows logon
- Network for Windows logon
- Authentication protocols for Windows logon
- User name and password options for Windows logon

Adapter for Windows logon

If you have to configure an adapter for Windows logon, the following dialog appears.

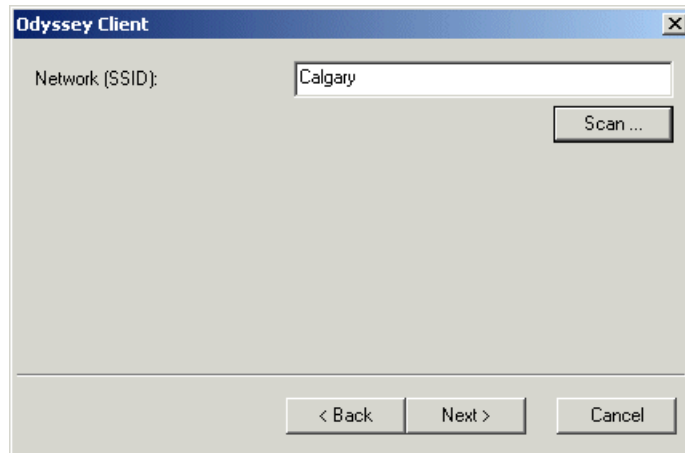


- 1 Select an adapter type. Select **wireless** for a wireless adapter, and **wired 802.1X** for a wired adapter connection.

- 2 Select an adapter from the list, and click **Next**.

Network for Windows logon

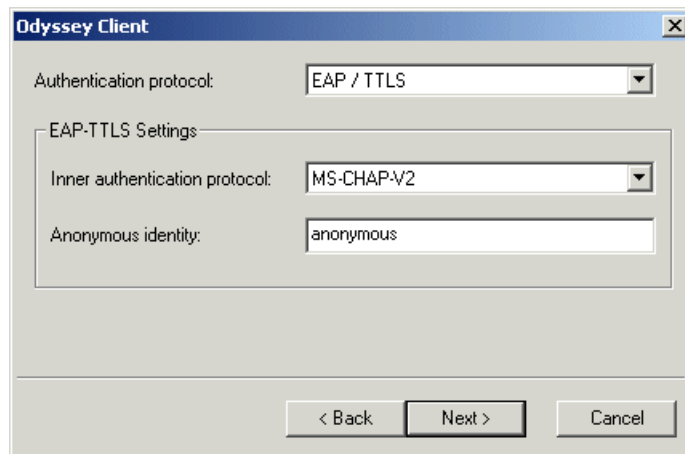
If you have to configure a network for Windows logon, the following dialog appears.



Type in the network name, or click **Scan** to scan for an available configured network. Note that you cannot use any auto-scan lists for this selection.

Authentication protocols for Windows logon

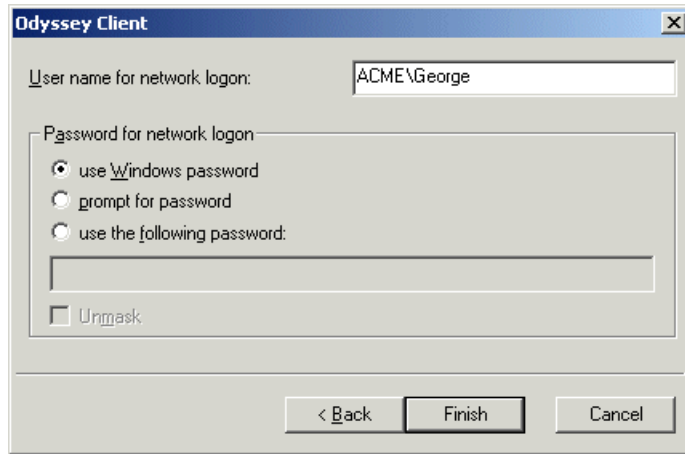
If you have to configure authentication protocols for Windows logon, the following dialog appears.



Select the authentication protocol from the list. If you specify EAP/TTLS as the authentication protocol, specify the required EAP/TTLS settings as well. Note that EAP/TLS is not available to you.

User name and password options for Windows logon

If you have to configure your user name and password settings for Windows logon, the following dialog appears.



Type your user name (in the correct format, usually domain\user name) in the text box, and select your password setting:

- Select **use Windows password** to use your regular Windows logon password for logging into the network.
- Select **prompt for password** if you want to be prompted to type in your required password at login time.
- Select **use the following password:** to type in a password that is not your Windows password. Note that this password is not stored for future use.

Odyssey Client Administrator

You can launch the **Odyssey Client Administrator** from the **Settings** menu. This allows you to configure settings for new users of this machine, as well as created a custom installer for a set of users. See “Odyssey Client Administration” on page 83 for more information.

Enable/Disable Odyssey

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

Odyssey Client is initially enabled, and normally you should not need to disable it. If you choose to disable Odyssey Client, it disconnects all adapters without changing any Connection panel settings. The Odyssey Client program still runs, but it is totally isolated from wireless network connections.

You would only want to disable Odyssey Client if you had concerns about your current Odyssey configuration. You might disable Odyssey Client, for example, if you are worried that Odyssey Client is in an insecure state and you just want to make sure you are off the network until you get a chance to inspect your settings.

Odyssey Client can also be enabled and disabled from the pop-up menu that appears when you right-click the Odyssey icon in the System Tray.

NOTE: To stop Odyssey Client from running entirely, select the **Exit** command when you right-click the Odyssey icon in the System Tray.

Close

Select **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 Control Panel:* Double-click the **Odyssey Client Manager** icon.
- *from the Windows taskbar:* Select **Start > Programs > Funk Software > Odyssey Client > Odyssey Client Manager**.

NOTE: To stop Odyssey Client from running entirely, you should select the **Exit** command when you right-click the Odyssey icon in the System Tray.

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 immediately discard any passwords you type in, 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 dialog pops up, allowing you to trust that server temporarily. Odyssey Client remembers to trust that server for as long a period of time as is configured in **Security Settings**.

If you want Odyssey Client to immediately discard its list of temporarily trusted servers, select **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 **Reconnect** on the **Connection** panel.

Web Menu

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

- Odyssey User Page
- Funk Software Home Page
- Register Odyssey

Odyssey User Page

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

Register Odyssey

Select **Register** Odyssey 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, we can expedite your call if we have your registration on file.

Help Menu

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

- Help topics
- License keys
- View Readme File
- About

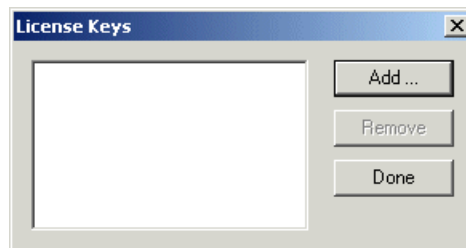
Help topics

Select **Help Topics** to bring up the Odyssey Client help system.

You can also get context-sensitive help at any time by pressing **F1**. The help system appears opened at the section that best explains your current situation.

License keys

Select **License Keys** from the **Help** menu, to manage your Odyssey Client license keys.



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 first install Odyssey Client. However, you may need to install additional license keys in the future. For

example, you must use 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.

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

***NOTE:** On Windows 2000 or XP you must have administrative rights in order to add or remove licenses. If you do not have such rights, you are able to view the license keys, but not to add or delete them, and you must contact your system administrator to do so.*

View Readme File

Select **View Readme File** to open the file readme.txt. This file has important information about Odyssey Client that could not be included in this manual.

About

Select **About** to view version and copyright information.

Tray icon menu commands

If you right-click on the Odyssey icon in the System Tray, the following menu items appear:

- **Odyssey Client Manager**
- **Enable Odyssey or Disable Odyssey**
- **Help commands**
- **Exit**

Odyssey Client Manager

If you select the **Odyssey Client Manager** menu command, **Odyssey Client Manager** (the user interface for Odyssey Client) appears.

Enable Odyssey or Disable Odyssey

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

Odyssey Client is initially enabled, and normally you should not need to disable it. If you choose to disable Odyssey Client, it disconnects all adapters without changing any Connection panel settings. The Odyssey Client program still runs, but it is totally isolated from wireless network connections.

You would only want to disable Odyssey Client if you had concerns about your current Odyssey configuration. You might disable Odyssey Client, for example, if you are worried that Odyssey Client is in an insecure state and you just want to make sure you are off the network until you get a chance to inspect your settings.

Odyssey Client can also be enabled and disabled from the **Odyssey Client Manager** menu.

Help commands

One of the options on the menu that appears when you right-click on the Odyssey icon in the System Tray is Help. There are two further options: **Help Topics** and **About**.

If you select **Help Topics**, the Help system appears in a window opened to the table of contents.

If you select **About**, product version and copyright information are displayed.

Exit

If you select the **Exit** command, Odyssey Client immediately stops running in the background. You may want to use this option when you are not using wireless networking for an extended period.

You can restart Odyssey Client by running **Odyssey Client Manager** from the **Start** menu.

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 use the following keyboard shortcuts in order to select the graphical information buttons on the connection panel:

- **Alt-1**, to display the signal power information
- **Alt-2**, to display the connection status information
- **Alt-3**, to display the encryption key information

You can also press **Alt** in conjunction with the appropriate arrow key on your keyboard, in order 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 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 for network communications, use the adapter's user interface only to operate those features that cannot be controlled by **Odyssey Client Manager**.

Odyssey Client Administration

5

Overview of Odyssey Client Administration

Odyssey Client provides a set of special tools for performing administrative tasks for managing users of the product. These advanced tools are only available if you have administrative privileges. The administrative tasks you can perform include the following:

- Create a custom installer with preconfigured settings for a group of users.
- Configure the timing for user or machine connection.
- Configure the initial settings for all users of a given client machine.
- Configure machine account settings when you require a machine network connection at Windows startup.

You can perform most administrative tasks using the **Odyssey Client Administrator**. See also the following topics for some connection scenarios:

- “Configuring machine only connection” on page 101
- “Configuring machine connection followed by user authentication” on page 101
- “Configuring user authentication without machine connection” on page 102

***NOTE:** Before using the administrator tools, you should be completely familiar with the **Odyssey Client Manager** features.*

Odyssey Client Administrator

You can operate the following advanced administrative tools from the **Odyssey Client Administrator**:

- **Connection Settings** for configuring one or more of the following types of network connection timings:
 - Connection to the network as a machine (machine connection) at Windows startup time
 - Connection to the network with user credentials prior to Windows logon
 - Connection to the network with user credentials after Windows logon, but before the desktop appears
 - Connection to the network with user credentials after the desktop appears

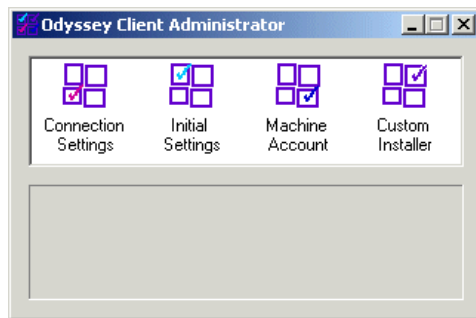
- **Initial Settings**, for modifying initial settings for your all users of this machine, and testing these settings before creating a custom installer.
- **Machine Account**, for configuring a machine network connection
- **Custom Installer**, for creating a preconfigured installer file from the initial user and/or machine settings you configure with the other **Odyssey Client Administrator** tools.

You may have occasion to use all, or some of these tools, depending on what you are trying to do.

Launching Odyssey Client Administrator

To launch the **Odyssey Client Administrator**, double-click the `odClientAdministrator.exe` application in the directory in which you have installed the Odyssey Client product.

Odyssey Client Administrator appears on your screen.

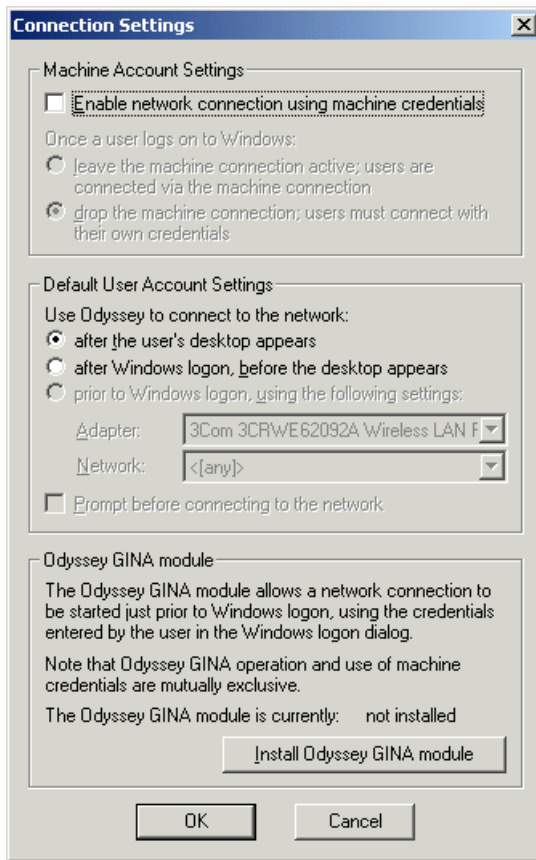


Connection Settings

You can use the **Connection Settings** tool to set the following connection options:

- **Machine Account Settings**, for configuring network connection options for network authentication with machine credentials at Windows startup time. The settings you choose may or may not require you to set additional default user account settings.
- **Default User Account Settings**, for configuring the timing of user logon connections
- **Odyssey GINA Module**, for installing or removing the ability for users to connect to the network before Windows logon.

Double-click **Connection Settings** in the **Odyssey Client Administrator** to open the **Connection Settings** tool.



See Network configuration scenarios for more information on the possible connection configurations.

Network configuration scenarios

You can configure one of six different network connection configurations:

- A machine only network connection, during which only machine credentials are authenticated
- A machine connection to the network at Windows startup time, with subsequent authentication of user credentials after the user logs on, but before the user's desktop appears
- A machine connection to the network at Windows startup time, with subsequent authentication of user credentials after the user's desktop appears
- A connection to the network with user credentials when they logon to Windows

- A connection to the network with user credentials after they logon to Windows, but before the user's desktop appears
- A connection to the network with user credentials after the user's desktop appears

Of these choices, only the last one is available for Windows 98 and Me machines.

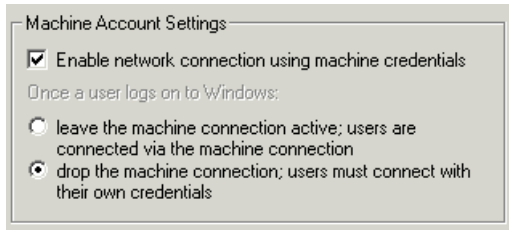
Note that some of these features are enabled or disabled according to the other features you select. See "Restrictions on early network connections" on page 91 for more information.

For more information on configuring the various network connection scenarios, as well as information about why you might select one scenario over another, see the following topics:

- "Configuring machine only connection" on page 101
- "Configuring machine connection followed by user authentication" on page 101
- "Configuring user authentication without machine connection" on page 102

Machine Account Settings

You can connect to the network at Windows startup time using your machine (rather than user) credentials by checking **Enable network connection using machine credentials** under the **Machine Account Settings** portion of **Connection Settings**.



Once you do so, you have two mutually exclusive options:

- To sustain your network connection as machine only, select **leave the machine connection active; all users are connected via the machine account**. With this option, users have little control of their network connection when they open the **Odyssey Client Manager**. They can view status information and reconnect or reauthenticate to the network.
- To have users login to the network with their own credentials once they have logged into Windows, select **drop the machine connection; users must connect with their own credentials**. With this option, you can account for

individual users of the network, and each user can modify his or her user account connection settings using the **Odyssey Client Manager**.

***NOTE:** If you select the second machine connection option, then set the timing for the user connection in **Default User Account Settings**. The two timing options you can select are as follows:*

- **after the user's desktop appears**
- **after Windows logon, before the desktop appears**

Once you complete your selections, click **OK** to close the **Connection Settings** dialog.

You can configure your connection settings according to your selections:

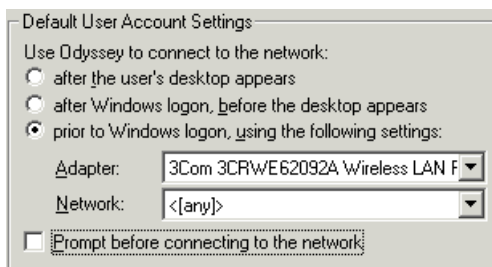
- Double-click **Machine Account** in the **Odyssey Client Administrator**, and configure the machine network connection.
- If you opt for users to connect with their own credentials after the machine connection is established, double-click **Initial Settings** in the **Odyssey Client Administrator** to configure user account settings.

***NOTE:** You do not have the option to enable a machine account connection if you have installed the Odyssey GINA Module. Remove this feature before you proceed to configure a machine account connection.*

See “Restrictions on early network connections” on page 91 for a listing of features unavailable when you configure a machine account connection.

Default User Account Settings

You have several options to configure the timing for network authentication with user credentials. You can configure such connections to occur prior to or after Windows logon time, using the **Default User Account Settings** portion of **Connection Settings**.



You can have up to three options available for configuring the timing of a user account connection with respect to the Windows logon time. These options are listed under **Use Odyssey to connect to the network**. They are listed in the order of the

latest time at which a network connection is established, to the earliest time at which a network connection is established through Windows logon:

- **after the user's desktop appears:** Choose this option if you do not require the user to establish a network connection before the desktop appears.
- **after Windows logon, before the desktop appears:** Choose this option if you require the user to establish a network connection before the desktop appears, but you do not require them to establish the network connection before the Windows logon process is complete.
- **prior to Windows logon, using the following settings:** Choose this option if you require the user to establish a network connection prior to establishing Windows logon.

Note the following:

- You do not have the **prior to Windows logon** option available when you set a machine connection for initial logon.
- You can only have the **prior to Windows logon** option available when you click **Install Odyssey GINA module**, in the **Odyssey "GINA" module** section of **Connection Settings**.
- If you do select the **prior to Windows logon** option, do not assign a network, auto-scan list, or profile connection for which you have selected EAP-TLS as the authentication method.

The success of your connection may depend on the timing you select. It is safest for you to choose to establish the network connection after the desktop appears. However, if you require that the user connects to the network before the desktop appears, select an earlier connection time.

If you select **prior to Windows logon**:

- Select the adapter and network (or auto-scan list, or profile, in the case of a wired 802.1X connection) from the lists provided. You must configure these using **Initial Settings**. See also "Configure connections that occur prior to Windows logon" on page 93.
- You can optionally require a prompt screen to appear prior to making the network connection at logon time every time your users logon to Windows, by checking **Prompt before connecting to the network**.

Click **OK** when you have completed selecting default user account settings.

NOTE: *If you want to install Windows logon features when creating a custom installer template, follow the guidelines in "Configure connections that occur prior to Windows logon" on page 93.*

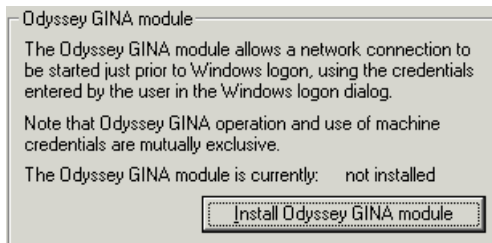
For information on compatibility with other applications that initiate at logon time, See “Compatibility with other applications running at logon” on page 91 for information on compatibility issues when using the Windows logon features.

Odyssey GINA Module

You can use Odyssey’s GINA module to allow users of Windows XP or 2000 to connect to the network using their Windows logon credentials prior to Windows logon. Connecting prior to Windows logon can be helpful when users have startup processes that require network connections. You cannot use this connection feature without installing Odyssey’s GINA module.

Installing Odyssey’s GINA module

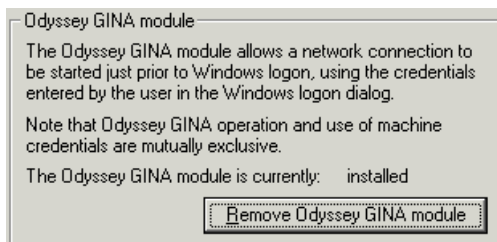
You can enable Odyssey’s GINA module features through the lower portion of **Connection Settings**.



To install the GINA module, click **Install Odyssey GINA module**, which is in the **Odyssey “GINA” module** section of **Connection Settings**. If you want to use this network connection option and have already checked a machine connection option, uncheck the machine connection option before clicking this.

Removing Odyssey’s GINA module

To remove Odyssey’s GINA module when it is installed, click **Remove Odyssey GINA module**.



Compatibility with other applications running at logon

The Odyssey GINA module works by replacing Windows Graphical Identification and Authentication (GINA) module. This is the module that presents the **Windows Logon** dialog. Odyssey is compatible with a number of logon modules, preserving single sign-on behavior.

It is possible that you have another application running a similar GINA process at logon that is not compatible with Odyssey's Windows logon process. In this case, Odyssey may prompt your users for information at logon, but both programs function correctly. In some cases, you must install Odyssey Client last, in order for it to work in conjunction with some applications that run processes at logon time.

Restrictions on early network connections

There are no restrictions for user account network connections that occur after the desktop appears, but otherwise, there may be restrictions on the features you can use when you select particular network connection timing options in **Connection Settings**. The following table summarizes the restrictions.

Feature	Machine account at Windows startup	User account at Windows logon	User account after logon, but before desktop
Ad-hoc	yes	no	yes
Ad-hoc	yes	no	yes
Preconfigured WEP keys	yes	no	yes
Windows password	no	yes	yes
Prompt for password	no	yes	no
use the following password	yes	no	yes
EAP-TLS	yes	no	yes
EAP-TTLS/PAP/Token Card	no	yes	no
EAP-TTLS/EAP/Token Card	no	yes	no
PEAP/Token Card	no	yes	no
Temporary trust	no	no	no
Uncheck "Validate server certificate"	yes	no	yes

A yes in a column implies the feature is valid for that connection setting, while no indicates that it is not.

You can configure all of the machine account network settings in the **Machine Account** tool. The restricted options are disabled for you in the **Machine Account** tool.

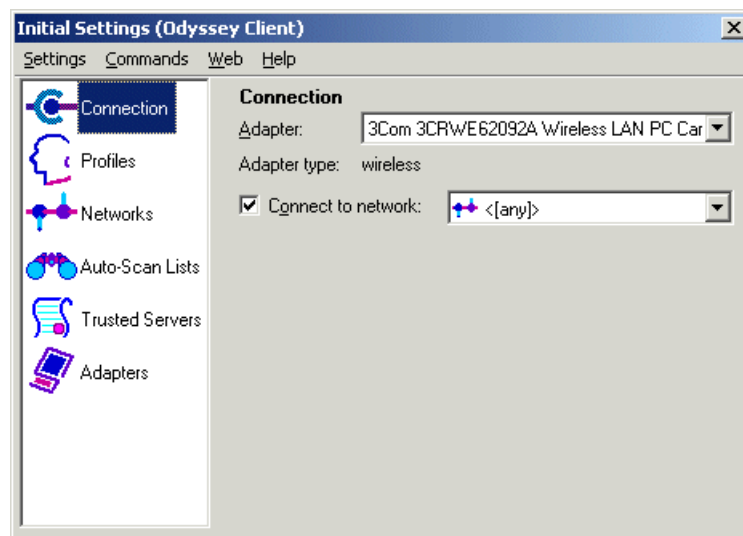
You can configure all of the user account network settings in the **Initial Settings** tool. However, the restricted options are not disabled for you in this tool, so make sure you configure the network connection properly.

Initial Settings

You can use the **Initial Settings** tool for the following tasks:

- Configure the initial user network connection settings for all *new* users of Odyssey on a given client machine.
- Configure the user network connections for a template for a custom installer.

To access the **Initial Settings** tool, double-click **Initial Settings** in the **Odyssey Client Administrator**.



Configure the following initial user network settings:

- Wireless connection(s)
- Wired connection(s)
- Profiles
- Networks
- Auto-Scan lists
- Trusted servers

- Adapters

See also the following topics:

- Configure connections that occur prior to Windows logon
- Setting default user override behavior
- Test user connection settings
- “Configuring user authentication without machine connection” on page 102
- “Configuring machine connection followed by user authentication” on page 101

Once you complete configuring your **Initial Settings**, all users who start up Odyssey for the first time on your client machine are presented with the default connection setup you have just configured.

Setting default user override behavior

The **Settings > Windows Logon Settings** menu in the **Odyssey Client Manager** gives users the option to override the default network connection timing. Do not check **Override default settings for Windows logon in Initial Settings**, or your users will, by default, have initial settings that override the settings you configure in **Connection Settings**.

If you do install Odyssey’s GINA module from **Connection Settings**, then your users have the ability to configure a network connection prior to Windows logon. If you do not install the GINA module, then your users have only the two post-logon connection options available to them through this menu on the **Odyssey Client Manager**.

Note that even though your users can override the default network connection settings that you configure, they cannot override configured trusted servers when they connect prior to logon time. The only way to change the trust you configure for a Windows logon connection on a given installation is for you (or someone with administrative privileges) to modify these settings in the **Trusted Servers** panel of **Initial Settings**.

Configure connections that occur prior to Windows logon

When installing Odyssey Client on Windows XP or 2000, you have the option to enable automatic network connections at the time the user logs on to the machine. This can be helpful when users have startup processes that require network connections. You can accomplish this using Odyssey Client’s Windows logon features.

There are some restrictions on the features you can use when you configure a network connection for user accounts prior Windows logon time. See “Restrictions on early network connections” on page 91 for more information.

Note the following additional instructions for any user account connections you want to configure to occur prior to Windows logon:

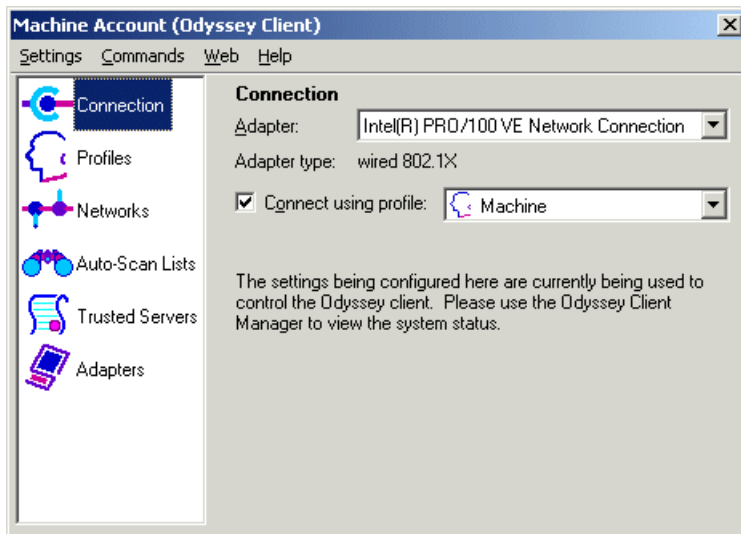
- To install or remove Odyssey’s Windows logon features, follow the instructions in “Odyssey GINA Module” on page 90.
- Select the third radio button and specify the network (or profile) and adapter in **Default User Account Settings** in **Connection Settings**.
- You must associate a profile and adapter (for wired connections) or a network (or auto-scan list) and adapter (for wireless connections) with a Windows logon configuration. The network configuration for Windows logon that you can select from the drop-down lists in **Connection Settings** reflects the adapters, networks, auto-scan lists, and profiles you specify in **Initial Settings**.
- When you specify in **Initial Settings** the profile that you intend to use with a prior to Windows logon connection, leave the **Login name** field blank.
- You must configure a trusted server in the **Trusted Servers** panel of **Initial Settings**. The trust you configure must include a certificate authority in the signing chain of the trusted server. If you have not already installed the certificate on your machine, you must do so prior to configuring this trust. In addition, you must check **Validate server certificate** on the **Authentication** tab of the profile you associate with this connection.
- If you are configuring a template for a custom installer, your users do not have to have exactly the same wireless or wired adapter as you have, so long as a similar type (wired or wireless) of equipment is installed on their client machines.

***NOTE:** There is some potential for interaction of the Windows logon feature with similar features in other products. See “Compatibility with other applications running at logon” on page 91. As a result, you should not enable the logon features unless you plan to use them.*

Machine Account

If you have configured a machine account network connection in **Connection Settings**, you can use **Machine Account** to configure network connections for a machine.

Double-click **Machine Account** in the **Odyssey Client Administrator** to configure **Machine Account**.



Configure a machine network login account in **Machine Account** in very much the same way you would configure a user account. At a minimum, configure at least one network, adapter, and profile for the machine logon. See the following relevant topics for more information:

- “Profiles panel” on page 36.
- “Networks panel” on page 47
- “Auto-Scan Lists panel” on page 53
- “Trusted Servers panel” on page 56
- “Adapters panel” on page 64

Note that you can configure multiple networks, profiles, and adapters, and only those for which you check the **Connect to network** (for wireless connections), and/or **Connect using profile** for (wired connections) are used by the machine connection.

To test machine connection settings, see “Preconfiguring Odyssey Client for a group of users” on page 99.

See also the following topics:

- “Configuring machine only connection” on page 101
- “Configuring machine connection followed by user authentication” on page 101

Note the following:

- Authentication methods that require user interaction, such as those associated with tokens, are not available with machine connection. As a result, this **Profiles Panel** varies slightly from that of the **Odyssey Client Manager**. See “Restrictions on early network connections” on page 91 for all restrictions on machine account connections.
- If you enter any passwords for machine account profiles or certificates, and intend to create a custom installer, the credentials you enter here are used by all copies of Odyssey Client that use this installer. It is better to manually enter credentials on each client machine, if these are required.

Custom Installer

You can use Odyssey’s custom installer features to create an installer with a customized user default configuration.

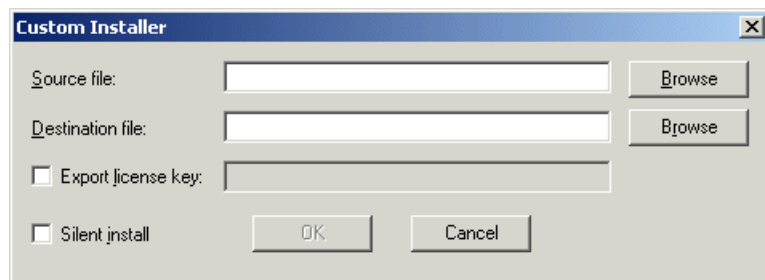
The custom install process is described extensively in the following topics:

- “Preconfiguring Odyssey Client for a group of users” on page 99
- “Installing and configuring Odyssey to create a template” on page 100
- “Custom Installer” on page 96
- “Custom install: Providing printable documentation” on page 101

After configuring and testing your custom installer template, you can use the **Custom Installer** in the **Odyssey Client Administrator** to create a new install file with user defaults that are configured from your template.

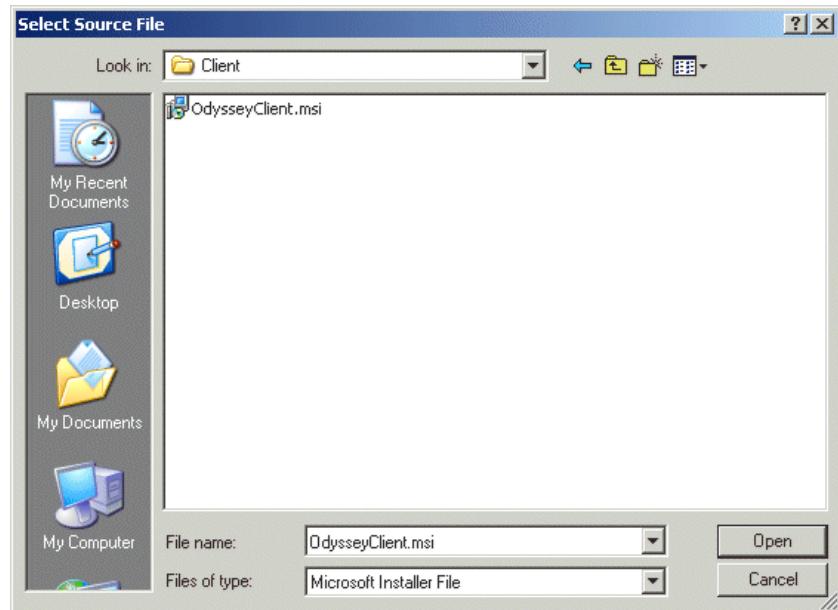
Follow these steps to complete the custom installation process:

- 1 Double-click **Custom Installer** in the **Odyssey Client Administrator** to configure **Custom Installer**. The following dialog appears.



- 2 Select the source installer file. You can type in the name, or click the first **Browse** button. You can use the original Odyssey Client installer file (OdysseyClient.msi) as the source file. You can find this file in the Client

directory on the CD. Note, if you are configuring an installer for Windows 98 machines, select the other installer file, **OdysseyClient.exe**. The **Select Source File** window opens. You can use the **Files of type** drop-down list at the bottom of the **Select Source File** window to search for the correct file type. Double-click your file in the window, or click **Open**.



- 3 Click **Browse**, to browse for your desired destination directory (if you are not already there). Select the name of your new (destination) .MSI file. You can type in the name of the file, or select an existing file in the current directory, and click **Save**. Note that if you are configuring an installation for Windows 98, save the file as .EXE instead of .MSI.
- 4 Optionally check **Export license key**, and type in a license key that is valid for the number of copies you intend to distribute.
- 5 Optionally check **Silent install** if you want the installation to run without displaying any dialogs during the install process. Not that if you choose this option and you do not export a license key, your users' licenses expire in 30 days.
- 6 Click **OK** to create the custom installer.

Testing your settings

You can test your configuration for user and machine connections before creating a custom installer. Note that when you do so, you remove any configurations that you already have set in the **Odyssey Client Manager**.

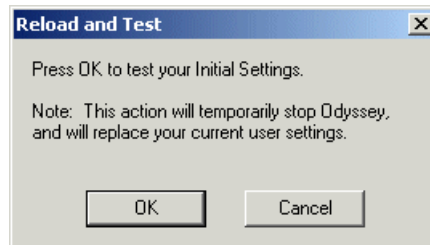
You can perform the following tests:

- Test user connection settings
- Test machine connection settings

Test user connection settings

To test your user connection settings:

- 1 Select **Commands > Reload and test user defaults** from **Initial Settings**.



- 2 Click **OK**. This permanently deletes your current **Odyssey Client Manager** settings, and loads your settings from **Initial Settings** into the **Odyssey Client Manager**. In addition, it starts the **Odyssey Client Manager** through the **Configure and Enable Odyssey Wizard**. Whatever you see in this wizard is what your users see when they first use the product.
- 3 Test all the connections through the **Connection panel**. Note that any modifications you make in the **Odyssey Client Manager** are not reflected in **Initial Settings**. Modify the configuration in **Initial Settings**, as necessary. Retest any modifications you require.
- 4 Return to **Initial Settings** to correct for any connection problems and verify these connections again, if necessary.

Test machine connection settings

To test your machine connection settings:

- 1 Make sure that the network connection(s) you want to test are configured and set for connection in the **Connection** panel of **Machine Account**.

- 2 Open **Network configuration scenarios**, and select **leave the machine connection active**. Click **OK**.
- 3 Double-click the Tray icon to open the **Odyssey Client Manager**, and check the status of your connection(s). Modify the configuration in **Machine Account**, as necessary. Retest any modifications you require.

If, in order to test your machine connection, you had to modify your connection settings setup, re-open **Network configuration scenarios**, and restore the previous settings.

Sample workflows with Odyssey Client Administrator

There are several tasks that require you to use the **Odyssey Client Administrator**, including those described in the following:

- “Preconfiguring Odyssey Client for a group of users” on page 99
- “Configuring machine only connection” on page 101
- “Configuring machine connection followed by user authentication” on page 101
- “Configuring user authentication without machine connection” on page 102

Preconfiguring Odyssey Client for a group of users

You can take advantage of your ability to preconfigure profiles and networks for an entire group of users by creating a custom installer in Odyssey.

You can create a customized installer that is based on a generic or *template* configuration to be used by a group of users. Each copy of the client that you install with this customized installer has a default network configuration that is assigned by your template.

If all of your users require the same network configuration, creating a custom installer reduces or eliminates the need for your end-users to enter configuration information.

To learn how to provide a custom installer to your users, see the following topics:

- “Installing and configuring Odyssey to create a template” on page 100
- “Machine Account” on page 94
- “Custom Installer” on page 96

- “Custom install: Providing printable documentation” on page 101

Installing and configuring Odyssey to create a template

Follow these steps to configure a template for a custom installer:

- 1 Put the product CD into the CD ROM drive of the client device. Use any Windows 2000 or Window XP device. The installation process should begin automatically. If it does not, browse the CD directory for the **setup.exe** file and double-click it. Note that if you have already installed a copy of Odyssey Client with a license key that is valid for your users, you can start with step 3. If you have installed the product, but want to change the license key, you can change it according to the instructions for adding and removing license keys in “License keys” on page 78.
- 2 Follow the installation instructions, using a license key that is valid for the installation machine. This may or may not be the license key you preconfigure for your users.
- 3 Configure your template according to your desired network configuration and connection option:
 - Configuring machine only connection
 - Configuring machine connection followed by user authentication
 - Configuring user authentication without machine connection

There are a few exceptions as noted below.

- Client certificates cannot be preconfigured. If you select **EAP-TLS** under the **Authentication** tab in the **Add Profile Properties** dialog on the **Profiles** panel, the user is prompted to select a client certificate the first time Odyssey Client runs on the client machine. You can, however, configure certificates for any trusted root server in the **Trusted Servers** panel.
 - Stored passwords or login names cannot be preconfigured.
- 4 When you are done configuring the default configuration for the template, test each network connection. See “Testing your settings” on page 98.

You have now set up a template configuration, and you are ready to create a preconfigured Odyssey Client installer.

See “Custom Installer” on page 96.

Custom install: Providing printable documentation

The custom installer file you create using the methods described in “Custom Installer” on page 96 includes the online help for the product, but does not include the manual in .PDF format.

There are two .PDF files in the Docs directory of your product CD:

- OdysseyClientAdmin.pdf
- OdysseyClientMan.pdf

OdysseyClientAdmin.pdf includes this administrative chapter, while OdysseyClientMan.pdf does not.

In addition to the .MSI (or .EXE, in the case of Window 98) file you create, you can also provide your users with the file OdysseyClientMan.pdf to give them access to printable documentation that does not include information on administrative tasks.

Configuring machine only connection

For the purposes of identifying a client machine on the network independent of user credentials, you have the option to connect all client machines to the network with a machine (rather than user) authentication. This can be useful if you have any machine-related startup processes. This feature also allows you to maintain network connections for the client machine, even when users are logged off.

To configure a machine only connection:

- 1 Double-click **Connection Settings** in the **Odyssey Client Administrator**.
- 2 Check **Enable network connection using machine credentials**, and select **leave the machine connection active**, and click **OK**.
- 3 Double-click **Machine Account** in the **Odyssey Client Administrator**. **Machine Account (Odyssey Client)** appears.
- 4 Run through the panels that are required for setting up your machine network connection, including **Networks**, **Adapters**, and **Profiles**, and close **Machine Account (Odyssey Client)**.

Configuring machine connection followed by user authentication

You have the option to connect all client machines to the network with a machine credentials, but subsequently require user authentication. This option allows you to perform network tasks at Windows startup, but subsequently account for the users on the network.

To configure a machine connection followed by user authentication:

- 1 Double-click **Connection Settings** in the **Odyssey Client Administrator**.
- 2 Check **Enable network connection using machine credentials**, and select **drop the machine connection**.
- 3 Select one of the two available user authentication timing options under **Default User Account Settings** and click **OK**. You can either have the users authenticate to the network before or after the desktop appears.
- 4 Double-click **Machine Account** in the **Odyssey Client Administrator**. **Machine Account (Odyssey Client)** appears.
- 5 Run through the panels that are required for setting up your machine network connection, including **Networks**, **Adapters**, and **Profiles**, and close **Machine Account (Odyssey Client)**.
- 6 Double-click **Initial Settings** in the **Odyssey Client Administrator**. **Initial Settings (Odyssey Client)** appears.
- 7 Run through the panels that are required for setting up your user network connection, including **Networks**, **Adapters**, and **Profiles**, and close **Initial Settings (Odyssey Client)**.

Configuring user authentication without machine connection

You have the option to connect all users to the network using only their user credentials. You have various options with respect to timing for network authentication with user credentials. For example, if you require any network-related startup processes, you can have your users connect to the network prior to Windows logon time.

To configure a user network connection:

- 1 Double-click **Initial Settings** in the **Odyssey Client Administrator**. **Initial Settings (Odyssey Client)** appears.
- 2 Run through the panels that are required for setting up your user network connection, including **Networks**, **Adapters**, and **Profiles**, and close **Initial Settings (Odyssey Client)**. If you plan to have users connect to the network before Windows logon time, make sure you create at least one profile that does not use EAP-TLS authentication. See “Configure connections that occur prior to Windows logon” on page 93 for more information.
- 3 Double-click **Connection Settings** in the **Odyssey Client Administrator**.
 - If you want users to connect to the network prior to Windows logon time, click **Install Odyssey GINA Module**, if it is not already installed. Select **prior to Windows logon** and select a wireless adapter and network (or a wired adapter and profile) that you have already

configured in step 2, and click **OK**. Make sure that the profile associated with this network connection does not use the EAP-TLS authentication method.

- If you want to require that users connect to the network after Windows logon time, make sure the Odyssey GINA module is not installed.
- If you want users to connect to the network after Windows logon time, (independent of whether or not you install the Odyssey GINA module), select one of the two available user authentication timing options under **Default User Account Settings** and click **OK**. You can either have the users authenticate to the network before or after the desktop appears.

Index

Numerics

- 802.11 14
 - ad-hoc mode 15
 - infrastructure mode 15
- 802.1X 19
 - authentication 51

A

- about the product 1
- access points 15
 - ad-hoc mode 50
 - infrastructure mode 50
 - IP addresses 15
- accounts
 - machine 87
 - users 88
- adapters
 - adding 65
 - multiple networks 31
- Adapters panel 64
- adding
 - auto-scan lists 55
 - wired adapters 65
 - wireless adapters 65
- ad-hoc mode 15
 - access points 50
- administrative tools 99
 - testing settings 98
 - UI for 84
- AES protocol, using 51
- anonymous name 44
- any network, configuring to connect to 49
- association method 50
- asymmetric cryptography 20
- authentication
 - network, specifying 51
 - protocols 41
 - servers, adding 60
 - X.500 names 60
- Authentication tab 41
- auto-scan lists
 - adding 55
 - connecting to 30
 - panel 53
 - properties 55

C

- certificate authority 21
 - root 21
- certificate chains
 - described 21
 - product, use of in 56
 - trust trees 58
- certificates
 - description 21
 - product, use of in 40
 - validation 42
- commands from tray icon 79
- compatibility, Windows logon 91
- configuring
 - connection to any network 49
 - machine connection 94
 - single clients 11
 - user authentication 85
- connecting
 - wired networks 31
 - wireless networks 30
- Connection panel 29
 - elapsed time 34
 - encryption key information button 36
 - informational fields 33
 - MAC address 34
 - scan for network 32
 - signal power 35
 - SSID 34
 - status field 33
- Connection Settings 85
- custom installer
 - notes 101
- custom installer, administrative tools 96
- custom preconfiguration 100
 - documentation, including 101

D

- defaults, setting for initial users 92
- descriptions of networks
 - specifying 50
- DHCP servers 15
- disconnecting
 - wired connections 31
 - wireless networks 30
- disconnecting networks 33

- documentation, including with custom preconfiguration 101
- domain
 - controller 43
 - login name 39
 - name 57
- driver software 10
- dynamic encryption keys
 - generation 51
 - reconnection effects 32

E

- EAP
 - as inner authentication 44
 - definition 19
- EAP-TLS
 - authentication 22
 - key generation 51
 - overview 22
- EAP-TTLS
 - description 21
 - key generation 51
 - overview 21
 - using 43
- elapsed time 34
- encryption keys
 - generation 51
 - information button 36
 - reconnection effects 32
- encryption method, networks panel 51
- Extensible Authentication Protocol 19

F

- forget password, setting 76
- forget temporary trust 77
- Funk Software information 1

G

- getting help 78
- GINA, installing 90

H

- Help
 - product, for 80
- Help menu 78
- help topics 78
- hiding icons 66
- hubs
 - 802.1X 15

I

- icons, hiding 66
- infrastructure mode
 - access points 50
 - defined 15

- Initial Settings, administrative tools 92
- inner authentication protocols 43
 - EAP 44
 - selecting 43
- installation
 - GINA 90
 - instructions 10
 - overview 10
 - requirements 10
 - wizard 11
- installers, customizing 96
- intermediate CAs 58
 - adding 60
 - overview 21

K

- keyboard shortcuts 80

L

- LDAP 22
- lead nodes 58
- license keys 78
- login names, specifying 39
- logon, Windows
 - caution 94
 - compatibility with other modules 103
 - configuration notes 93
 - dialog 69
 - features 103
 - installing 90
 - override defaults 93
 - preconfiguration of features 94
 - prompt dialog 71
 - prompts 73
 - suppressing 72
 - trust, setting 93
- logon, Windows, uninstalling 90

M

- MAC address 34
- machine account settings 87
- machine connection
 - before user logon 101
 - configuring 94
 - settings for 87
 - testing 98
 - user authentication, without 101
- Machine Settings
 - administrative tools 94
- maintenance contracts 8
- multiple connections 31
- mutual authentication 42
 - explained 20
 - implementing 42

N

- network cards, using 65
- network connections
 - machine and user 101
 - machine only 101
 - restrictions 91
 - user, without machine 102
- Network Properties
 - any network, configuring 49
 - Description field 50
 - network type 50
 - Scan button 49
- networks 49
 - authentication, specifying 51
 - configuring 47
 - connection to any 49
 - connecting to 30
 - logon time, at 88
 - machine authentication 87
 - description 47
 - specifying 50
 - disconnecting from 33
 - multiple connections 31
 - names
 - scanning for 49
 - specifying 49
 - reauthenticating 33
 - reconnecting 32
 - scanning for connection 32
 - titles 47
 - type, specifying 50
 - WEP keys 52
 - wired, connections 31
- Networks panel 47
- networks panel
 - association 50
 - encryption method 51

O

- Odyssey Client Administrator 84
- Odyssey Client Manager
 - overview 27
- Odyssey Client Manager, starting 27
- open mode, WEP 17
- override default connection settings 93

P

- passwords
 - entering 39
 - forgetting 76
 - prompts for 76

Windows 39

PEAP

- overview 22
- using 45
- PEAP protocol, using 45
- peer-to-peer networking
 - definition 15
 - IP addresses 15
 - product, using for 52
- preconfiguration 96
 - custom 100
 - initial product install 100
 - logon features 94
 - templates 100
- preferences
 - hide tray icon 66
 - setting 66
- private key 20
- product information page 1
- product registration 78
- Profile Properties
 - Login name 37
 - passwords 37
 - PEAP settings 45
 - User Info 38
 - Windows password 39
- Profiles panel 36
- prompt dialog
 - Windows logon 71
- public key 20

R

- RADIUS, server product 19
- reauthenticating
 - explained 22
 - networks 33
 - session resumption 67
 - why 23
- reconnecting
 - dynamic encryption keys, effect on 32
 - networks, to 32
- registering Odyssey 78
- requirements, installation 10
- restrictions, network connections 91
- root certificate authority 21

S

- scan button for connections 32
- Service Set Identifier 16
- session resumption 22, 67
- setting

- initial user defaults 92
- machine connections 87
- Settings menu
 - Windows Logon Settings 69
- shared mode, WEP 52
- shortcut keys 80
- signal power, viewing 35
- simultaneous connections 31
 - monitoring 31
- single clients, configuration 11
- SQL 22
- SSID 34
- starting the product main interface 27
- status from Connection panel 33
- subject name, trusted servers 62
- support information 8
- suppressing Windows logon prompts 72
- switches, 802.1X 15
- System Tray, commands from 79

T

- technical support 8
- template 99
- templates
 - creating 100
 - preconfiguration 99
- temporary trust 63
 - defined 68
 - disabling 68
 - forgetting 77
- testing
 - administrative settings 98
 - user connections 98
- TKIP
 - implementing 51
 - overview 18
- TLS authentication, overview 22
- token authentication 43
- trust trees 58
 - certificate chains 58
- trusted servers
 - advanced button 58
 - advanced method 58
 - editing 58
 - entering 57
 - leaf nodes 58
 - overriding 93
 - removing 58
- Trusted Servers panel 56
- TTLS settings, authentication 43
- tunnels 44

U

- uninstalling Windows logon features 90
- untrusted servers

- defined 68
- dialog 63
- upgrades 78
- user authentication, without machine logon 102
- user connection
 - settings 88
 - testing 98
- User Info 38

W

- WEP keys
 - any network connection 49
 - defined 17
 - open mode 17
 - shared mode 52
 - specifying 52
- Window logon
 - prompt dialog 71
- Windows Domain Controller 43
- Windows logon
 - administering 88
 - compatibility with other products 91
 - configuration notes 93
 - installing 90
 - override defaults 93
 - prompts 73
 - suppressing 72
 - settings for users 69
- Windows password 39
- wired adapters, adding 65
- Wired-Equivalent Privacy 17
- wireless adapters, adding 65
- wireless networks
 - connecting 30
 - disconnecting 30
- WPA
 - implementing 50
 - overview 18

X

- X.500 names 60