



Odyssey Access Client for Macintosh User Guide





**Juniper Networks
Odyssey Access Client
for Macintosh**

User Guide

*Release 4.3
April 2007*

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Copyright© 2002-2007 Juniper Networks, Inc. All rights reserved. Printed in USA.

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

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

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

Table of Contents

About This Guide	ix
Licenses	ix
Audience	ix
Conventions	ix
Documentation	x
Release Notes	x
Web Access	x
Product Release Information	xi
Context-Sensitive Help and Product Release Information	xi
Glossary	xi
Contacting Customer Support	xi
Chapter 1 Odyssey Access Client Overview	1
How OAC Operates in a Network	1
Authentication	2
Chapter 2 Installing Odyssey Access Client	3
Before You Begin	3
Requirements	3
Supported Platforms	3
Network Adapter Cards	3
Network Hardware	3
Browsers	4
Licenses	4
Installing OAC	4
OAC Deployment Using Client Scripts	4
Chapter 3 Using Odyssey Access Client Manager	7
Running Odyssey Access Client Manager	7
Login Credentials	7
Overview of Odyssey Access Client Manager	7
Sidebar and Content Dialogs	8
Connection Dialog	8
Profiles Dialog	9
Networks Dialog	9
Auto-Scan Lists Dialog	9
Trusted Servers Dialog	9
Adapters Dialog	9
Menu Options	9
Settings Menu	9
Preferences	10
Security	10
PAC Manager	12
Disable Odyssey	12
Close Odyssey	13
Commands Menu	13
Forget Password	13

	Forget Temporary Trust	13
	Check New Scripts	13
	Run Script	14
	Web Menu	14
	Odyssey Access Client User Page	14
	Juniper Networks Home Page	14
	Register Odyssey Access Client	14
	Purchase Odyssey Access Client	14
	Help Menu	14
	Help Topics	14
	License Keys	15
	Readme	15
	About	15
	Informational Graphics and Detailed Status	15
	Displaying Status Details	15
	Signal Power Status	15
	Connection Status	15
	Encryption Key Information	16
	Exiting from OAC	16
Chapter 4	Managing Network Adapters	17
	Adding Network Adapters	17
	Removing an Adapter	18
	Checking Adapter Status	19
	Connection Status	19
	Interaction with Other Adapter Software	21
Chapter 5	Managing Network Connections	23
	OAC Connection Dialog	23
	Selecting an Adapter	24
	Connecting to a Network	24
	Connecting to a Wireless Network	24
	Connecting to a Wired Network	25
	Connecting to a Different Network	25
	Simultaneous Network Connections	25
	Scanning for Wireless Networks	26
	Reconnecting to a Network	26
	Reauthenticating a Network Connection	26
	Disconnecting from a Network	26
Chapter 6	Managing Profiles	29
	Adding or Modifying a Profile	29
	Specifying a Profile Name	30
	Specifying User Information	31
	Setting Passwords	31
	Using Certificates	32
	Using Certificates for Authentication	32
	Setting Up Authentication	32
	Selecting Authentication Protocols	33
	Validating a Server Certificate—Mutual Authentication	34
	Setting Tunneled Token Card Credential Options	35
	Setting an Anonymous Name	35
	TTLS Settings	36

	PEAP Settings.....	36
	Setting EAP Inner Authentication Protocols.....	37
	EAP as an Inner Authentication Protocol	38
	Removing a Profile.....	39
	Sample Profile Configuration	40
Chapter 7	Managing Network Access	41
	Networks Dialog.....	41
	Adding or Modifying Network Properties	42
	Network Settings	43
	Specifying a Network Name (Network SSID)	43
	Connecting to Any Available Network	43
	Scanning for Available Networks.....	43
	Adding a Network Description	43
	Specifying a Network Type.....	44
	Specifying a Channel.....	44
	Specifying an Association Mode	44
	Encryption Methods for an Association Mode	45
	Authentication Settings.....	45
	Authenticating with a Profile	45
	Automatic Key Generation	46
	Preconfigured Key Settings	46
	Preshared Keys (WPA or WPA2)	46
	Preconfigured Keys (WEP)	47
	Removing a Network	48
	Sample Network Configuration Setups	48
	Sample Configuration for a Corporate Wi-Fi Network	48
	Sample Configuration for a Wireless Hotspot Network	48
	Sample Configuration for a Home Wireless Network	49
Chapter 8	Managing Auto-Scan Lists	51
	Using the Auto-Scan List Dialog.....	52
	Adding an Auto-Scan List.....	52
	Removing an Auto-Scan List	53
	Modifying an Auto-Scan List	53
	Viewing Network Names in an Auto-Scan List	53
Chapter 9	Managing Trusted Servers	55
	Configuring Trust in OAC	56
	Selecting Trust Servers	56
	Adding a Trusted Server Entry	56
	Server Identity	57
	Editing a Trusted Server Entry	58
	Removing a Trusted Server Entry	58
	Setting Up Certificates	58
	Trusted Root Certificates	58
	Intermediate Certificates.....	59
	Personal Certificates.....	59
	Adding a Certificate.....	59
Chapter 10	PAC Manager	61
	Using PAC Manager	61

Refreshing the Pac Manager Display.....	61
Deleting a PAC.....	61
Exiting from the PAC Manager	61

Appendix A	Network Security Concepts	63
-------------------	----------------------------------	-----------

Network Security	63
Encryption and Association for Secure Authentication.....	64
Authentication Overview.....	64
Odyssey Access Client Features for a Secure Network	65
802.11 Wireless Networking.....	65
Types of 802.11 Wireless Networks.....	66
Access Point Networks.....	66
Peer-to-Peer Networks	66
Wireless Network Names.....	66
Wired-Equivalent Privacy	67
Wi-Fi Protected Access and its Encryption Methods	67
802.1X Authentication	68
Extensible Authentication Protocol.....	69
Mutual Authentication.....	69
Certificates.....	70
EAP-TLS	71
EAP-TTLS	71
EAP-PEAP	72
EAP-FAST.....	72
EAP-LEAP.....	72
Reauthentication	72
Session Resumption	73

Appendix B	Glossary	75
-------------------	-----------------	-----------

Index	89
--------------	-----------

About This Guide

This guide describes how to install, configure, and use Odyssey Access Client (OAC) for wired or wireless network access on a Macintosh computer.

This manual is available in PDF format on the OAC CD and on the Juniper Networks Web site at

http://www.juniper.net/customers/support/products/aaa_802/oac_client_user.jsp

Licenses

You must have a valid license key to run OAC. If you do not know the license key, consult your network administrator. You enter the license key after you install the product.

Audience

This manual is intended for all OAC users who need wired or wireless network access and who need to manage and configure the available features and controls.

Conventions

Table 1 defines notice icons used in this guide, and Table 2 defines text conventions used throughout the book.

Table 1: Notice icon


Icon	Meaning	Description
	Informational note	Indicates important features or instructions.

Table 2: Text conventions (except for command syntax)

Convention	Description	Examples
Bold typeface	Indicates buttons, field names, dialog box names, and other user interface elements.	Use the Scheduling and Appointment tabs to schedule a meeting.
Plain sans serif typeface	Represents: <ul style="list-style-type: none"> ■ Code, commands, and keywords ■ URLs, file names, and directories 	Examples: <ul style="list-style-type: none"> ■ Code: certAttr.OU = 'Retail Products Group' ■ URL: Download the JRE application from: http://java.sun.com/j2se/
<i>Italics</i>	Identifies: <ul style="list-style-type: none"> ■ Terms defined in text ■ Variable elements ■ Book names 	Examples: <ul style="list-style-type: none"> ■ Defined term: A <i>Service Set Identifier</i> (SSID) is the actual name of a wireless network. Variable element: <i>/Users/username/Library/Scripts</i> ■ Book name: See the <i>Odyssey Access Client User Guide</i>.

Documentation

The following sections describe how to access copies of the product documentation and the latest information about the release.

Release Notes

Release notes are included with the product software and are available on the product CD or on the Web at:

<http://www.juniper.net/techpubs/>

Release notes provide the latest information about features, changes, known problems, and resolved problems. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Web Access

To view Juniper product documentation on the Web, go to:

<http://www.juniper.net/techpubs/>

Product Release Information

OAC includes online help that enables you to access this documentation from your computer. To invoke the Help system, select the **Help > Help Topics** menu command.

Context-Sensitive Help and Product Release Information

OAC includes online help that you can access any time. To invoke the Help system, select the **Help > Help Topics** menu command.

For context-sensitive help, hold down the Function key and press the F1 key in any active OAC dialog.

You can use the **Help > View Readme File** menu command located to open the `readme.txt` file, which contains the latest information about features, changes, known problems, and resolved problems. If the information differs from the information found in the documentation set, defer to the information in the `readme.txt` file.

Glossary

This manual includes an extensive glossary.

Contacting Customer Support

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (within the United States) or 408-745-9500 (from outside the United States).

Chapter 1

Odyssey Access Client Overview

Odyssey Access Client (OAC) is networking software that runs on endpoints (desktop, laptop, and notepad computers and other supported wireless devices). OAC communicates with wireless access points, 802.1X switches, and network authentication servers such as Juniper Steel-Belted Radius to provide authenticated, secure access to wired and wireless 802.1X networks. OAC supports secure, authenticated network connections for both wired and wireless communication in the workplace, as well as wireless connections to wireless fidelity (Wi-Fi) hotspots and home wireless networks.

Corporate networks frequently have both a wired and wireless infrastructure to support mobile computing at work. Mobile computing must be secure, especially for wireless communications, because a wireless connection is more vulnerable than a wired connection.

OAC provides extensive configuration options, making it an effective solution for connecting to any type of network.

OAC enables you to connect to a network easily and securely. You can use OAC to perform the following tasks:

- Configure and control connections for wired and wireless adapters (see “Managing Network Adapters” on page 17).
- Connect to access points and to peer-to-peer networks (see “Managing Network Access” on page 41).
- Configure individual profiles required for authenticated access to specific networks (see “Managing Profiles” on page 29).
- Use a wide variety of powerful authentication methods, such as EAP-TTLS, EAP-PEAP, EAP-TLS, and EAP-FAST to keep your credentials secure. See “Authentication Settings” on page 45 and the “Glossary” on page 75.

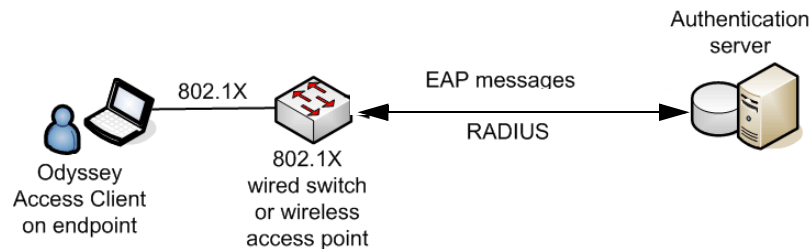
How OAC Operates in a Network

When you attempt to connect to an 802.1X network, OAC requests authenticated access through a wireless access point or through an 802.1X switch. The authentication sequence is the same whether you use a wired or a wireless connection. In either case, your access to protected resources requires authentication.

With 802.1X, you get authenticated to a network based on matching authentication (EAP) protocols and on your user credentials, such as a password, certificate, or a token card. For details about configuring EAP protocols, see “Selecting Authentication Protocols” on page 33. For details about setting up credentials, see “Specifying User Information” on page 31.

In a wireless network, the 802.1X authentication occurs after the client has associated to an access point using an 802.11 association method.

Figure 1: OAC in a Corporate Network



Authentication

The steps in a typical 802.1X authentication process are:

1. When a wireless client attempts to connect to an 802.1X network, it signals an access point that it is making an authentication request. This step is commonly known as *association*.
2. In the case of either a wired or a wireless connection, the network access device (an access point or 802.1X switch) forwards the authentication request to the authentication server.

The authentication process might involve a secure tunnel between the access point and the authentication server, depending on the authentication protocol being used, such as Tunneled Transport Layer Security (TTLS).

3. The authentication server examines the request and, in some cases, forwards the request to another server or manages the authentication directly.
4. If the authentication succeeds, the server informs the network access device to allow access to the client endpoint.
5. The network access device then informs the client that it has been authenticated and now has access to the network.

Authentication for a wired connection is similar but, in this case, the client connects directly to an 802.1X switch on the network. The switch provides the authentication interface to the authentication server and there is no secure tunnel required.

Appendix A, “Network Security Concepts,” describes the networking choices that you can make and how those choices allow you to use OAC to maximize the security of your connections over any wireless or wired network.

Chapter 2

Installing Odyssey Access Client

Before installing OAC, you should be familiar with networking concepts relating to your wireless or wired network. See Appendix A, “Network Security Concepts,” for basic networking information.

Before You Begin

You must have administrative privileges on your computer to install OAC. The following administration tasks should be performed before installing OAC:

- Select and prioritize the authentication protocols required for your authentication server. Your network administrator can provide the specific protocols required for your corporate network.
 - Install a network adapter and the associated driver software if your computer does not have these built in.
-

Requirements

The following sections describe hardware and software requirements for OAC.

Supported Platforms

OAC runs on any PowerPC or Intel-based Macintosh computer running OS X 10.4.

Network Adapter Cards

OAC currently supports the built-in wireless adapter that comes with a Macintosh computer.

Network Hardware

For network authentication, your network might include:

- At least one 802.1X-compliant switch (for wired authentication).
- At least one 802.1X-compliant access point (for wireless authentication).
- An AAA server.

Browsers

OAC currently supports the Safari browser.

Licenses

You must have a valid license key to run OAC. You can purchase licenses from Juniper Networks, Inc. For details, select **Help > License Keys** from the Odyssey Access Client Manager.

Installing OAC

This section discusses how to access and install Odyssey Access Client. To install OAC, follow these steps:

1. Open a Web browser and enter the following URL to download the installer:
http://www.juniper.net/customers/support/products/aaa_802/oac_client
2. Select the option to download Odyssey Access Client.
3. Save the **Odyssey.dmg** disk image file containing the files needed to install OAC.
4. Double-click **Odyssey.dmg** to open it.
5. Double-click **Odyssey.pkg**. When the file opens, a welcome screen appears.
6. Click **Continue**. A **readme.txt** file opens. This file contains the installation instructions.
7. Click **Continue**. The End User License Agreement (EULA) appears. Read this carefully, then click **Agree** to continue.
8. Specify a destination hard drive for installing OAC when you see the prompt, then click **Continue**.
9. At the next prompt, click **Install**.
10. When the installation has completed, close the installer.

OAC Deployment Using Client Scripts

This section discusses the general procedure for deploying OAC to mobile devices.

In a corporate environment, a network administrator typically creates the configuration settings using a desktop version of OAC and then distributes the configuration settings to one or more mobile devices by placing a script file in a specific folder in the mobile device's file system. Scripts allow an administrator to deploy an OAC configuration to multiple endpoints without having to perform a manual configuration update on each device. This is true for the initial OAC deployment for new mobile devices and for deploying updated configuration settings.

Use the Odyssey Access Client Administrator Script Composer tool (in the OAC Enterprise Edition for the desktop) to create a script file to export the configuration from your desktop Odyssey Access Client. (Refer to the *Odyssey Access Client Administration Guide* for details on using the Administrator tools.) Then place the script on the mobile device in the **Scripts** folder under the OAC install directory on the mobile device which is typically `/Users/username/Library/Scripts`.

To use a script to deploy a configuration to mobile devices:

1. Open the Odyssey Access Client Manager on the desktop and set up the desired OAC configuration settings.
2. Open the Script Composer tool and select the profiles and networks to export to the mobile device.
3. Use a flash memory card, a shared network drive, or any other appropriate out-of-band transfer method you prefer to distribute the script file to users.

A key requirement of deployment is that the script file must be delivered to the **Scripts** folder located in the OAC installation directory on the device. OAC polls the **Scripts** directory for update scripts each time the mobile device restarts, as well as every 20 minutes. When OAC finds a new script, it executes the script automatically and transparently.


Chapter 3

Using Odyssey Access Client Manager

This chapter discusses how to use the Odyssey Access Client Manager to configure OAC. Odyssey Access Client Manager is the OAC management interface.

Running Odyssey Access Client Manager

Once OAC is installed on your computer, it runs as a daemon. To start OAC, use either of the following methods:

- Navigate to **Applications > Odyssey** and click the Odyssey icon. 
- Click the Odyssey icon from the Menu Bar.

When OAC starts up, the Odyssey Access Client Manager (Figure 2 on page 8) appears on the desktop.

Login Credentials

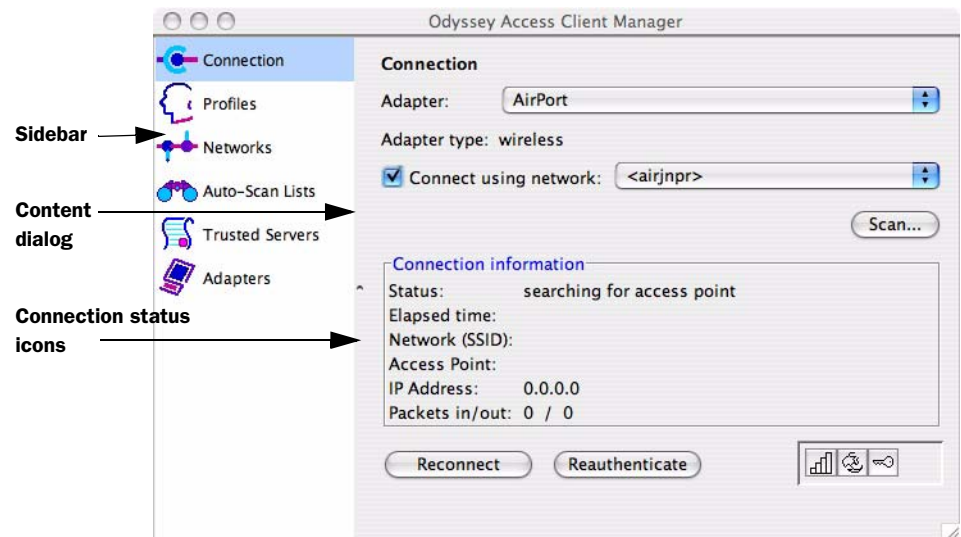
Depending on how OAC is configured, a dialog box may prompt you for credentials. The credentials may include your user name and password or a soft token.

Overview of Odyssey Access Client Manager

This section describes the Odyssey Access Client Manager and the operations that you can perform.

The Odyssey Access Client Manager (Figure 2) consists of the following sections:

- Menu options (see “Menu Options” on page 9).
- Sidebar and Content Dialogs (see “Sidebar and Content Dialogs” on page 8).

Figure 2: Connection Dialog

A *menu bar* is located at the top of the screen. It provides a range of pull-down options. Below the menu bar, the left panel is the *sidebar*. The sidebar contains icons for various configuration tasks:

- Connection
- Profiles
- Networks
- Auto-Scan Lists
- Trusted Servers
- Adapters

The *content dialog* lets you view status, make network connections, and make configuration settings. The type of configurations settings you make is based on the icon you select from the sidebar. Figure 2 shows the initial screen that appears when you open Odyssey Access Client Manager.

Sidebar and Content Dialogs

The sidebar contains a list of named icons, each of which opens a different content dialog. Each content dialog shows configuration options and controls pertaining to the selected sidebar icon. The following sections summarize each top-level dialog.

If this is your first experience with Odyssey Access Client Manager, spend some time exploring each icon and the related dialog and notice how each dialog differs.

Connection Dialog

Use this dialog to select an adapter, establish a network connection, scan for available wireless networks, and display current connection status. See “Managing Network Connections” on page 23.

Profiles Dialog

Use this dialog to configure login and authentication information, such as your password or a certificate, that may be used when you authenticate or to a network. See “Managing Profiles” on page 29.

Networks Dialog

Use this dialog to configure individual networks, connection type, encryption type, and whether to use 802.1X authentication. See “Managing Network Access” on page 41.

Auto-Scan Lists Dialog

Use this dialog to set up an ordered list of wireless networks that you have configured. An auto-scan list is a convenient feature if you move from one wireless network to another. See “Managing Auto-Scan Lists” on page 51.

Trusted Servers Dialog

Use this dialog to add, remove, and configure trusted network servers and to set certificate and identity information for the servers that might authenticate you when you connect. Configuring this feature is necessary for EAP protocols that implement mutual authentication and is a recommended security measure. See “Managing Trusted Servers” on page 55. Contact your network administrator before changing any trust configuration settings.

Adapters Dialog

This dialog lists the network adapters, wired and wireless, currently configured in OAC. Use it to add or remove wired and wireless adapters that are in the current configuration. See “Managing Network Adapters” on page 17.

Menu Options

The OAC menu bar appears at the top of the Macintosh screen. The options are as follows:

- Settings menu
- Commands menu
- Web menu
- Help menu

The following sections describe each menu category and the individual options.

Settings Menu

The following sections describe each of the Settings menu options.

Preferences

Use this option to toggle the display of OAC tray icon and the OAC splash screen.

Security

The Settings menu has two separate tabs. The General tab addresses the following categories:

- Session resumption.
- Automatic reauthentication.
- Server temporary trust.

Enable session resumption

During a network session, any subsequent authentication to the same network server can be accelerated by reusing information derived during the first authentication. If enabled, you can restrict session resumption for any session older than the length of time that you set. The default is 12 hours.

The practical application for using this feature is that it turns on wireless roaming so that you can take your wireless computer anywhere in the building and stay connected without having to reconnect or reauthenticate.

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

To enable session resumption:

1. Go to **Settings > Security Settings**.
2. Click **Enable session resumption**.
3. Set **Do not resume sessions older than** to the maximum number of hours that a session can last after initial authentication before requiring reauthentication. After the time limit has elapsed, the next reauthentication will be a completely new one. The number of hours can have up to three decimal places.

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

To disable this feature, clear the **Enable session resumption** setting.

Enable automatic reauthentication

If enabled, this option enables automatic reauthentication and sets the reauthentication frequency setting. The default is one hour.

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

You can configure automatic periodic reauthentication to the network using OAC. 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 Macintosh computer and access point. The access point might use these shared keys to refresh the keys used to encrypt data. By frequently refreshing keys, you can thwart cryptographic attacks.

To enable automatic reauthentication:

1. Go to **Settings > Security Settings**.
2. Click **Enable automatic reauthentication**.
3. Set the automatic reauthentication frequency, enter the time period (in hours) in the checkbox next to **Reauthenticate every**. You can use up to three decimal places to indicate the number of hours.

By default, automatic reauthentication is disabled. This is because your network administrator might have already configured your access points or authentication server to perform periodic reauthentication. Contact your network administrator for the proper settings for this option.

To disable this feature, clear the **Enable automatic reauthentication** setting.

Enable server temporary trust

This option enables temporary trust of a server and lets you set the maximum length of time for trusting that server. The default is 12 hours.

Most of the time, you can use the Trusted Servers dialog to configure the servers you trust for authentication. However, you might negotiate a connection to a network whose authentication server has not yet been configured for trust in the Trusted Servers dialog. In this case, you might can enable *temporary trust* for that untrusted server.

If temporary trust is not enabled, any authentication attempt that requires the validation of a server certificate fails when the server is not explicitly trusted.

To enable temporary trust:

1. Go to **Settings > Security Settings**.
2. Click **Enable server temporary trust**. If temporary trust is enabled, you have the following options:
 - Trust an untrusted server temporarily when you attempt to authenticate to it.

- Add the server to your trust tree in the Trusted Servers dialog. Consequently, the temporary trust feature serves as an alternative to configuring trusted servers through the Trusted Servers dialog.

To disable this feature, clear the **Enable server temporary trust** field.

3. Set the maximum time (in hours) that you want OAC to continue to trust a server once you accept it. By default, temporary trust is enabled. The maximum time that a particular server is temporarily trusted after you accept it is 12 hours.



NOTE: These settings do not apply to servers that you choose to trust permanently if you click **Add this trusted server to the database** when you are prompted for temporary trust.

The EAP-FAST tab provides options for when to prompt for server credentials when you use EAP-FAST for authentication.

EAP-FAST Settings

EAP-FAST is an EAP authentication method that offers password-based 802.1X authentication to encapsulate user credentials inside a TLS tunnel. Unlike other tunneled protocols, however, a server certificate is not required as a means of establishing a tunnel. Instead, EAP-FAST uses Protected Access Credentials (PACs) when establishing the tunnel. One or more of the following options to specify when to prompt for server credentials:

- Check **Acquiring new credentials from a new server** to have OAC prompt for credentials when you authenticate with a server to which you have not previously authenticated using EAP-FAST.
- Check **Replacing credentials existing credentials from a known server when your existing credentials have failed** to have OAC prompt for credentials upon authentication with a known server for which an earlier authentication attempt resulted in failure.
- Click **Reset Defaults** to return to the default configuration (both options checked).

PAC Manager

Protected Access Credentials (PAC) are used for mutual authentication with an ACS or Steel-Belted Radius authentication server during EAP-FAST authentication. Use the PAC Manager option to provision Protected Access Credentials (PACs) for use with EAP-FAST authentication.

Disable Odyssey

The **Disable/Enable** option toggles the OAC off or on, respectively. OAC is enabled by default; you should not need to disable it. Disabling OAC prevents you from using OAC for network connections until you enable it again.

Close Odyssey

The **Close** option lets you close the Odyssey Access Client Manager while OAC continues to run. To reopen Odyssey Access Client Manager, click the Odyssey icon on the menu bar and click Odyssey Access Client Manager.

Commands Menu

Forget Password

Use this option if you want OAC to discard the current password that you use to start an authenticated network connection. If your password is required again, you will be prompted to enter it.

When you are authenticated for the first time, you have to enter a valid password as part of the login process. OAC remembers the password that you enter and uses it for any subsequent authentications without prompting you again.

Normally, OAC does not forget the password until you reboot your Macintosh computer or restart OAC. However, if you leave the system unattended and want to protect it from unauthorized access or if you share a computer with other users (such as in a test lab), you might want to click **Forget Password** as a security measure.

Forget Temporary Trust

Use this option to discontinue the temporary trust setting for a server. See “**Enable server temporary trust**” on page 11 and “**Managing Trusted Servers**” on page 55 for more information about trusted servers.

Check New Scripts

Use this option to check for new scripts that your administrator asks you to run. Scripts can contain configuration updates such as new authentication settings, new networks, or trust configurations that reflect changes in your corporate security policy.

There are two types of scripts: those that execute automatically and those that you execute manually. Scripts that execute automatically have the file extension `odyClientScriptAuto`. These scripts do not appear in the dialog that appears when you select **Commands > Check New Scripts**. Only scripts with an `odyClientScript` file extension appear in this dialog.

If you are unsure about a script, contact your administrator.

Your administrator might send you email with one or more scripts to run, in which case you must save the scripts in the following directory before running them:

```
/Users/username/Library/Scripts
```

To check for new scripts:

Select **Commands > Check New Scripts** from the OAC menu bar.

The Check New Scripts dialog displays a list of new configuration scripts and the date that they were made available.

To delete a script:

1. Select the script from the Run Script dialog.
2. Click **Delete**.

To save a script:

1. Select the script from the Run Script dialog.
2. Click **Save**. A file browser opens at your home directory and lets you navigate to the location where you intend to save the script.

Run Script

This section discusses how to use the **Run Script** command.

To run a script:

1. Select the script from the Run Script dialog.
2. Click **Open** to execute the script and update your OAC configuration. You can run only one script at a time.

Web Menu

Odyssey Access Client User Page

Select this option to open your Web browser to a page devoted to OAC users. You can find technical notes that can help you get the most out of Odyssey Access Client, along with product news and information about new versions.

Juniper Networks Home Page

Select this option to open the Juniper Networks home page in your browser. Here you can find more information about Juniper Networks, Inc. and its products.

Register Odyssey Access Client

Select this option to register Odyssey Access Client online.

Once you register OAC, you will be notified automatically about product upgrades and special offers. Additionally, should you need to call the technical support hotline, your call can be expedited if registration is on file.

Purchase Odyssey Access Client

Select this option to purchase Odyssey Access Client.

Help Menu

Help Topics

Use this option to access online help files for OAC.

To access context-sensitive help, hold down the Function key and press the F1 key from any OAC dialog.

License Keys

Use this option to determine when the current OAC license expires and to add or remove an OAC license key.

Readme

Use this option to read about OAC requirements, new features, and other release-specific information.

About

Use this option to review the release version of OAC.

Informational Graphics and Detailed Status

Status icons appear in the lower right of the Connection dialog for an adapter. They provide visual status for your connection. Use the mouse or the keyboard to view detailed connection status information from any of the status icons.


Displaying Status Details


To see status details for any given status icon, point to a graphical status button with the mouse and hold down the mouse button.

Signal Power Status

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

 Strong signal power

 Moderate signal power


 Weak signal power


 Faint signal power


 No signal power

Connection Status

The connection status icon (the OAC “sail boat” icon) shows your connection and authentication status.

 (outline) – Not connected

 (red) – Not connected, due to failed authentication

 (black) – Connected, but authentication not in use

 (blue) – Connected and authenticated


The status details that you see depends on your authentication method and access point and might include the following:

- Result of your last connection attempt
- Type of authentication
- Elapsed time (since last connection)
- Cipher suite used to secure credential exchange
- Access point identification information

Encryption Key Information

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

 (outline) – Data is not encrypted

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

Status details for these icons can show the following information:

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



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

Exiting from OAC

To exit from OAC, right-click the OAC icon in the system tray and click **Quit**. OAC closes but you can re-launch it at any time. OAC runs as a daemon program unless you remove it, so you can run OAC at any time.

Chapter 4

Managing Network Adapters

This chapter describes how to add or remove a wired or wireless network adapter in an OAC configuration and how to connect to a network using that adapter.

You can set up one or more network adapters by clicking **Adapters** in the Odyssey Access Client Manager sidebar. Any adapter that you intend to use to connect to a network with OAC must be installed on your computer before it can be configured.

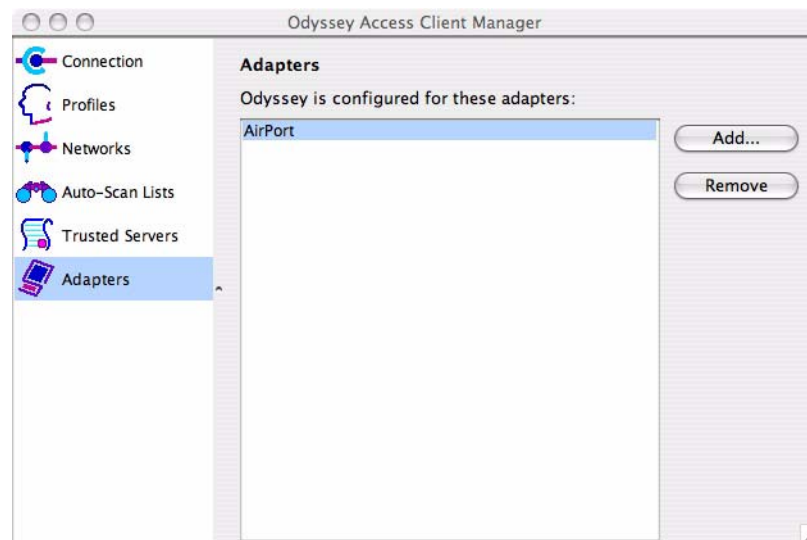
Adding Network Adapters

When you add an adapter to the OAC configuration, OAC binds to that adapter and has control of it as long as the adapter is still configured in OAC. This means that you cannot use other software to connect to a network with that adapter unless you remove the adapter from the OAC configuration. See “Removing an Adapter” on page 18.

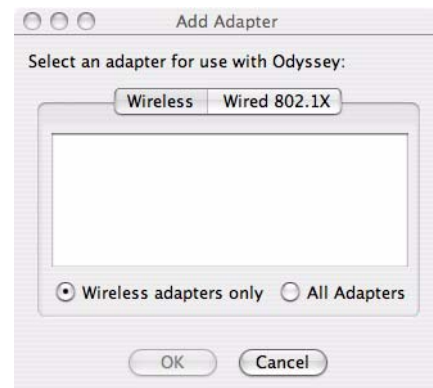
You can configure an external wireless adapter in addition to the built-in adapters on your machine and, thus, have multiple wireless adapters configured at the same time. You can use each adapter to connect to the same or to different networks.

To add a network adapter:

1. Most current Macintosh laptop computers have wired and wireless network adapters built in. OAC currently supports only built-in adapters.
2. Click **Adapters** in the sidebar. The Adapters dialog (Figure 3) appears.

Figure 3: Adapters Dialog

3. Click **Add**. The Add Adapters dialog appears (Figure 4). Note that only adapters that you have not yet added to the Adapters dialog appear.

Figure 4: Add Adapter Dialog

4. Select the adapter to be added from the list and click **OK**.



NOTE: If your wireless adapter is not in the list, click **All Adapters**. Make sure that each of the adapters that you select under the Wireless tab is wireless. You cannot configure OAC for wireless connections unless you have a wireless adapter.

Removing an Adapter

To remove an adapter using the Adapter dialog:

1. Click **Adapter** in the sidebar.
2. In the Adapter dialog, select the wired or wireless adapter(s) that you want to remove.
3. Click **Remove**.

When you remove an adapter, OAC stops using it. While the adapter might still be installed on your system, it does not operate with OAC unless you add it back to the OAC configuration.

Checking Adapter Status

To check adapter status, click **Connection** and select the specific adapter whose status you want to check.

The Connection dialog displays the following information:

- The adapter name (such as Airport).
- The adapter type.
- A network name and, next to it, a list of the current configured networks. (See “OAC Connection Dialog” on page 23.)
- A **Connect to the network** check box for toggling a network connection on or off.
 - If you are using a wired adapter, use the **Profiles** list to select an authentication profile.
 - If you are using a wireless adapter, use the **Network** list to select the network to which you want to connect.

Connection Status

The Connection dialog shows summary information for the current adapter and network connection. This includes:

- Status: see Table 3
- Elapsed time: the duration (in hours, minutes, and seconds) of current network connection
- Network SSID: the name of the wireless adapter to which you are connected
- Access point: the MAC address or the name of the access point to which you are connected
- IP address: the IP address assigned to your computer when you logged on.
- Packets in/out: the number of data packets exchanged during the current network connection.

Table 3: Connection Status Information

Status Message	Definition
open and authenticated	The connection is authenticated and you are connected.
open / authenticating	Reauthentication is in progress and you are connected.

Table 3: Connection Status Information (continued)

Status Message	Definition
open / requesting authentication	You have requested reauthentication and you are connected.
open	The connection is not authenticated but you are connected.
peer-to-peer	The network type is peer-to-peer (ad hoc) and you are connected.
authenticating	You are not yet connected but authentication is in progress.
requesting authentication	You are not yet connected but you have requested authentication from the access point.
waiting to authenticate	You are not yet connected and the last authentication failed but you are waiting to retry. If you see this message for a considerable length of time, there might be an association problem. If so, select the association mode required for your access point.
searching for access point	You are not connected and communication with an access point on the requested network has not been established. This might occur when your adapter does not support 802.1X or if your access point is not within range.
disconnected	You are not connected and Connect to the network might not be selected. See “OAC Connection Dialog” on page 23 for information about how to connect.
Odyssey is disabled	You are not connected and OAC has been disabled.
Odyssey is not running	The Odyssey service has crashed, has been disabled, or is stopped.
adapter not present	You are not connected and the configured adapter is not currently available. This might occur if your adapter does not support 802.1X.
cable unplugged	You are not connected. This can occur if you have a wired connection but your cable is unplugged.
adapter in use by another program	Your adapter is being used by another program installed on your machine.
disabled by wired connection	Your wired connection has disabled your OAC wireless connection based on your security settings. See “Web Menu” on page 14.

Interaction with Other Adapter Software

Your wireless adapter might come with its own user interface software to help you control its operation and might allow you to operate non-standard features of your wireless adapter to which OAC has no access.

In most cases, OAC and the user interface that comes with your wireless adapter can coexist without problems. However, we recommend that you do not use both products for similar purposes to avoid conflicts that could result when both programs are attempting to control the adapter at the same time. If you use OAC for network communications, use the software supplied with your adapter to operate only those features that cannot be controlled by OAC.

Chapter 5

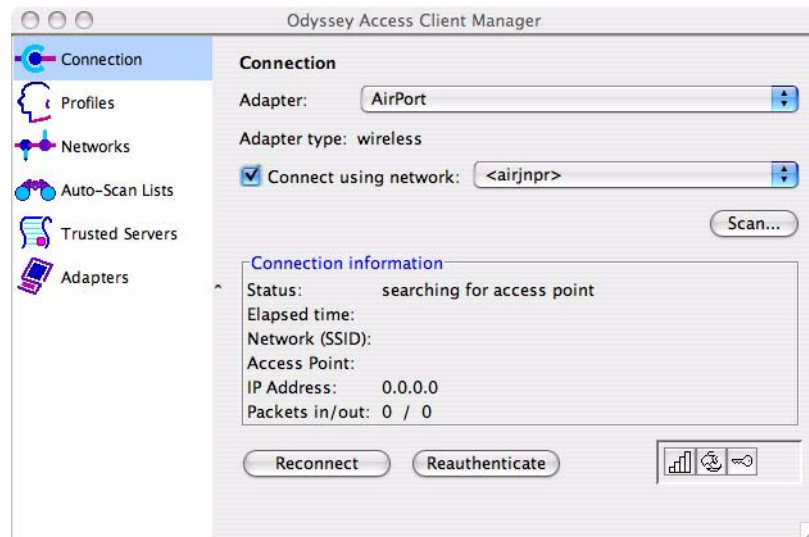
Managing Network Connections

This chapter describes how to use the Connection dialog to manage network connections using a wired or wireless network adapter.

OAC Connection Dialog

The Connection dialog (Figure 5 on page 24) enables you to perform the following tasks:

- Select a wired or wireless adapter from a list of configured adapters.
- Use that adapter to connect to a specific network.
- Set up simultaneous network connections using multiple adapters.
- Scan for available wireless networks.
- Reconnect to a network
- Reauthenticate to a network.
- Disconnect from a network.

Figure 5: OAC Connection Dialog

Selecting an Adapter

If you or your administrator configured more than one adapter to use with OAC, select which adapter to use for the network connection.

To select a network adapter:

1. Click **Adapters** in the sidebar. The Adapters dialog (Figure 3 on page 18) opens and displays the adapters configured in OAC.
2. Select the wired or wireless adapter to use.

Connecting to a Network

When you connect to a network, OAC uses the adapter that you select to establish an authenticated connection to the network. If you attempt a wired connection to a network switch that does not support 802.1X—for example, to a wireless network at home—OAC makes the connection without authentication. You do not need a profile in this case.

Connecting to a Wireless Network

To connect to a wireless network:

1. Select a network from the list (Figure 5) located to the right of the **Connect using network** check box.

The networks in this list are the ones that you have created already in the Networks dialog. To add a new network, see “Adding or Modifying Network Properties” on page 42.

You can connect to any available wireless network if your configuration supports this option. See “Connecting to Any Available Network” on page 43.

2. Click **Connect using network** to start the network connection.

Connecting to a Wired Network

To connect to a wired 802.1X network:

1. Select an authentication profile from the **Profile** list located to the right of the **Connect using network** check box.

The profiles that appear in this list are the ones that you have created in the Profiles dialog. See “Adding or Modifying a Profile” on page 29.

2. Click **Connect using network** to start the network connection.

Connecting to a Different Network

You can change your network connection at any time—for example, when you move from one physical location to another (a different building, a different city, or to your home). You can also change the connection type from a wired network connection at the office to a wireless hotspot at a coffee shop or an airport. Doing this requires that you have each network configured in OAC unless you are connecting to any available network.

To connect to a different network:

1. Select the network adapter whose current network connection you want to change.
2. Clear the **Connect using network** check box.
3. Based on the type of adapter you are using, wireless or wired, select a network or profile name from the list that corresponds to the network to which you want to connect.
4. Click **Connect using network**.

Simultaneous Network Connections

Each adapter on your computer can connect to a different network. This means that if you have one wired and one or more wireless adapters, you can maintain simultaneous network connections to one or more networks. With both connection types configured, you can use a wired connection when you are at your desk and then unplug your wired connection and take your laptop to other locations in the building using a wireless connection as long as you have wireless access.

Use the **Adapter** list on the Connection dialog to switch between the adapters that you configured for multiple network connections and monitor the status of your network connections.

Scanning for Wireless Networks

If you travel frequently, you might be authenticated by locally available wireless networks that you have not configured already.

To connect to a wireless network that is not configured:

1. Click **Scan** on the Connection dialog.

The Scan dialog displays a list of all wireless networks that are currently reachable.

2. Select the network from the scan list.
3. Click **OK**.



NOTE: A *beacon* is a signal broadcast by a wireless access point to identify its location. Only wireless networks that are configured by an administrator to “send beacons” are visible to you when you scan. If “send beacons” is off, then you must specify the network from the Networks dialog or choose the default **[any]** network from the Connection dialog.

Reconnecting to a Network

Click the **Reconnect** button (located at the bottom of the Connection dialog) to re-initialize your network connection if the current connection is not performing as expected. The reconnect option disconnects the existing connection for the currently selected adapter and starts a new connection to the network. The new connection might be to a different access point (on the same network) from your previous access point connection. If you are authenticated by the network, you will remain authenticated when the new connection starts. Any dynamic encryption keys will be refreshed with the reconnection.

This option is useful when you are moving from one access point to another on the same network. Clicking **Reconnect** can sometimes provide a connection with an access point that provides better service.

Reauthenticating a Network Connection

When you click **Reauthenticate** at the bottom of the Connection dialog, OAC reauthenticates your existing connection without starting a new connection. If dynamic encryption keys are in use, they are refreshed automatically.

Disconnecting from a Network

Disconnecting from a network terminates the network connection between the computer and the network. The adapter remains part of the OAC configuration unless you remove it from the list of configured adapters. Thus, you can use the same adapter to connect to a network later.

To disconnect from a wireless network:

1. Open the Connection dialog and select the adapter that you want to disconnect from the **Adapter** list.
2. Clear the **Connect using network** check box.

You can check other adapter status, as described below.

Chapter 6

Managing Profiles

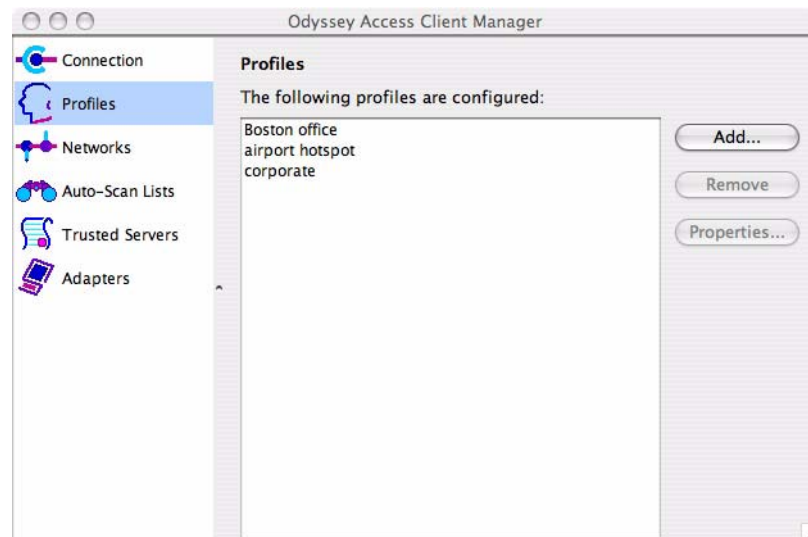
This chapter describes how to configure an OAC profile for authenticated network access.

A profile contains all of the information necessary for authenticating a connection to a specific network. This includes information such as your identity (user credentials) and the EAP protocols used to authenticate to that network.

You must have a profile for each network that requires an authenticated (secure) connection.

To begin, click **Profiles** in the sidebar. The Profiles dialog (Figure 6) opens.

Figure 6: Profiles Dialog



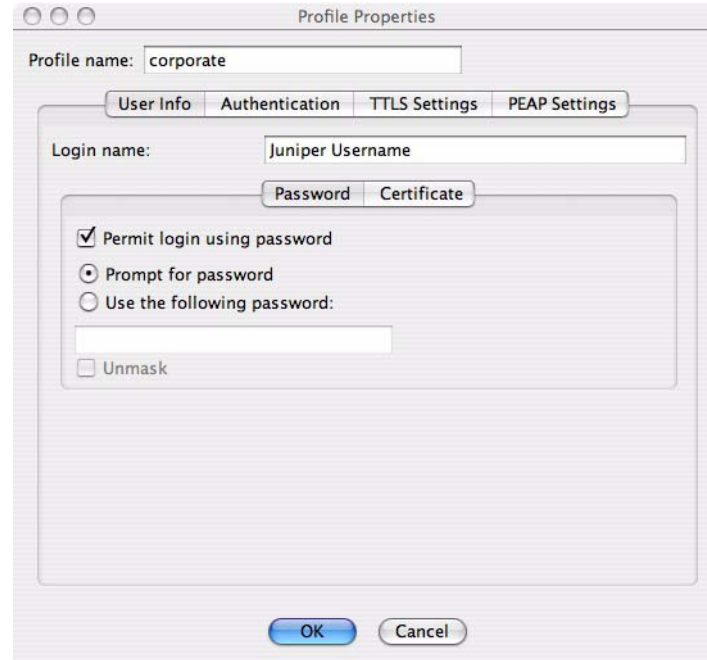
The Profiles dialog lists your current network profiles. You can use the settings in this profile as a guideline for setting up other profiles.

Adding or Modifying a Profile

This section describes how to create an authentication profile. It describes each of the configuration settings and walks you through each element in the Profile Properties dialog.

To add a profile, click **Add** in the Profile Properties dialog (Figure 7). To modify profile properties, click **Properties**.

Figure 7: Profile Properties Dialog



Each profile reflects the logon and authentication information required for that network and contains the following categories of information:

- **Profile name**—The name of the profile that you are creating or editing.
- **User information**—Your login name and the means used to authenticate your identity (password, certificate, or other user credentials).
- **Authentication**—The authentication protocol to be used. Depending on the authentication protocol that you specify, there are other settings that might apply. See “Setting Up Authentication” on page 32.
- **TTLS**—If you are using TTLS, the EAP-TTLS outer protocols and, where they apply, one or more inner protocols. See “TTLS Settings” on page 36.
- **PEAP**—If you are using PEAP, the EAP-PEAP outer protocols and, where they apply, one or more inner protocols. See “PEAP Settings” on page 36.

Specifying a Profile Name

When you add a profile to OAC, specify a unique name for the profile in the **Profile name** field of the Profile Properties dialog. For example, you can use **Office** for the profile name of your corporate network and **Home** for your home network. You can use the IP address of the network for the profile name. If you use one or more hotspot networks frequently, you can add a named profile for each of them.

You cannot change the name of a profile after you save it. To change the name of a profile, remove the profile and recreate it.

Specifying User Information

Enter your user name in the **Login name** field. This is the name presented to the network when you request a network connection. If you authenticate against a user database, use the form *domain\user_name* (for example, **Acme\george**). See your network administrator for the required format.

The **User Info** tab has sections that you can configure from the following subtabs:

Setting Passwords

Configure this section when you use authentication protocols that require a password. The following EAP authentication methods require a token or a password:

- EAP-TTLS e
- EAP-PEAP
- EAP-MD5-Challenge
- EAP-LEAP
- EAP-FAST

To set a password, click **Permit login using password** on the **Password** subtab of the **User Info** tab of the Profile Properties dialog. This lets you enable the authentication methods that use your password for authentication.

OAC can obtain your password in one of the following ways:

- Click **Prompt for password** to have OAC prompt you when you connect to the network. In general, this is the most secure option.
- Click **Use the following password** and enter a password in the box below this option to have OAC save your password and use it each time you authenticate with this profile.



NOTE: If you change your password, be sure to update the new password in the **Use the following password** field.

If you click **Prompt for password**, you are usually prompted only the first time that you are authenticated after startup. OAC remembers your credentials and reuses them for the duration of your session. The credentials that you enter apply only to a profile. If you are authenticated using a different profile, you will be prompted again.

You might be prompted to enter your password when connecting to the network under some conditions, including entering an incorrect password or if any other authentication failure occurs. This feature is in place, in part, to prevent accidental lockout due to the reuse of bad passwords.



NOTE: When OAC prompts for your password, you can choose to disable the OAC network connection (temporarily) and use a wired network connection when one is available. To do this, click **Yes** when the prompt to disable your OAC connection appears.

You can return to the Connection dialog to connect to a network any time.

Using Certificates

OAC reads personal certificate information from your personal certificate store on your computer or device. Configure this section when you use authentication protocols that require a client-side certificate (for EAP-TLS) for authentication.

Use EAP-TLS as the authentication protocol to negotiate authentication with certificate credentials. See “Setting Up Certificates” on page 58 for more information on setting up certificates.

Using Certificates for Authentication

To use certificate credentials for authentication:

1. Select the **Certificate** subtab of the **User Info** tab.
2. Click **Permit login using my certificate** to enable authentication methods that use your certificate for authentication.
3. Click **Browse** to select a personal certificate from your computer. A list of your personal certificates appears. Select a certificate and click **OK**. Once you configure a certificate, you can click **View** to view the certificate.



NOTE: Before you can create a profile that uses a personal certificate from your computer, you must install the certificate in the **Login** keychain of your computer. Double-click on the certificate and choose **Login** from the drop-down list. See your network administrator for information about installing and selecting a user certificate for authentication if you require one.

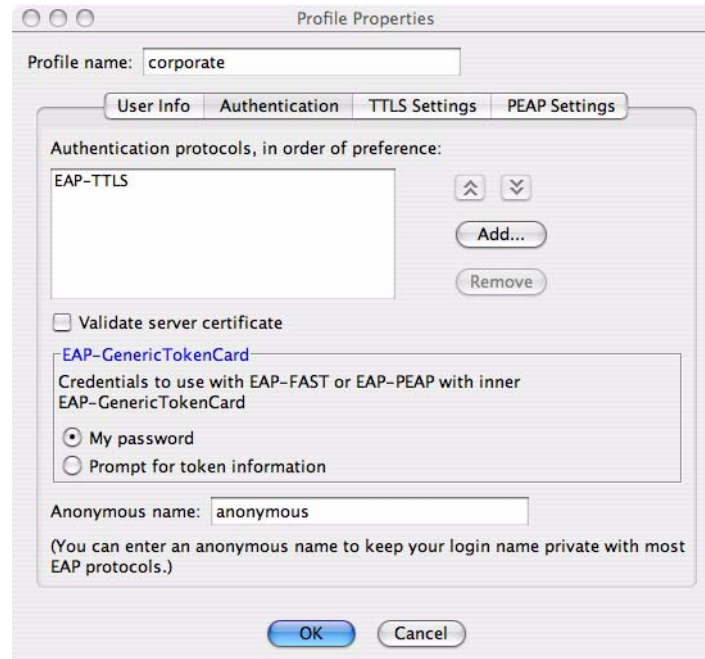
Setting Up Authentication

Different networks use different authentication protocols. You need the correct settings configured in your profile for your network. Before changing or specifying any authentication settings in OAC, consult your network administrator to determine if those changes reflect corporate policy. If your settings are incorrect, you might not be authenticated to access your network.

To specify network authentication protocols, open the **Authentication** tab in the Profile Properties dialog (Figure 8).

The authentication protocols specified on the **Authentication** tab are the *outer authentication* methods, which create a secure tunnel between OAC and the authentication server. Some authentication protocols, such as PEAP and TTLS, require that you specify an *inner authentication* method. If you select EAP as an inner authentication method, OAC prompts you to select a secondary inner authentication method.

Figure 8: Profile Properties for Authentication Settings



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

Selecting Authentication Protocols

The **Authentication protocols** list shows the authentication protocols that you enabled. You can have one or more authentication protocols in the list and add more if necessary. If you have more than one protocol in the list, you can order them by preference (top down). The ordering affects the protocol that the server uses if it has more than one protocol in common with the ones that you select here. Consult your network administrator before changing these settings.

To add a protocol to the list:

1. Click **Add** to open the Add EAP Protocol dialog.
2. Select one or more protocols to add.
3. Click **OK**.

To select more than one protocol at a time, hold down Command (Apple) key on the keyboard as you select them with your mouse. Any protocols already enabled are not listed in this dialog.

To remove a protocol from the list:

1. Select the protocol.
2. Click **Remove**.

To reorder protocols:

1. Select a protocol.
2. Use the up or down arrow button on the **Authentication** tab to reposition the protocol in the list.

Validating a Server Certificate—Mutual Authentication

Certain protocols, such as EAP-TTLS, EAP-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*. Typically, you need to install the server certificate on your computer so server validation occurs transparently each time you connect to that network.

Click **Validate server certificate** to verify the identity of the authentication server using a certificate if you are authenticating with EAP-TLS.



NOTE: If you select this option, you must have the same root CA or intermediate CA for the server certificate chain installed in the trusted root or intermediate certificate store of your machine.

To check this on Macintosh systems, open **Applications > Utilities > Keychain Access**. Click **Show Keychains** in the bottom left. Then click **X509Anchors** from the list of keychains.

On a Macintosh computer, you must install the server certificate manually in **X509Anchors**. If the server certificate is yet not installed on your computer and if you have **Validate server certificate** enabled, a prompt dialog will ask if you would like to connect to the server anyway. This happens each time you try to connect to the server without having the server certificate installed (as long as you have **Validate server certificate** enabled). When you have the server certificate installed on your machine, the prompt does not appear.

In general, click **Validate server certificate**. You have the option of turning off this important security precaution because there might be circumstances that require it. For example, if you are unable to configure trust because you do not have an intermediate root CA certificate installed on your machine, you might want to turn off certificate validation. Do this only if instructed by your network administrator.

Setting Tunneled Token Card Credential Options

EAP-GenericTokenCard defines an EAP envelope to carry one-time passwords generated by token cards like RSA SecurID. EAP-GenericTokenCard can be the inner protocol for tunneled authentication if you use EAP-FAST or EAP-PEAP.

If you select EAP-FAST as an outer authentication method on the **Authentication** tab, you can use EAP-GenericTokenCard as the inner authentication protocol.

If you select EAP-PEAP as an outer authentication method, you can use EAP-GenericTokenCard as the inner protocol. In this case, the **Token Card Credentials** settings in the **Authentication** tab apply. They allow you to choose to use your password credentials or your token card ID for authentication:

- Click **Use my password** if your network requires that you use the password credentials assigned with this profile instead of your token card ID for authentication.
- Click **Prompt for token information** if your network requires a token ID for authentication.



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

Setting an Anonymous Name

With EAP-TTLS, EAP-PEAP, and EAP-FAST, you can establish an encrypted tunnel anonymously and pass your credentials through the encrypted tunnel.

You can set up two identities when you use any of the following methods:

- An inner identity (your login name) is taken from the **Login name** field in the **User Info** tab.
- An outer identity that can be anonymous. You can set your outer identity in the **Anonymous name** field.

Note that Anonymous outer identities are implemented only when you enter a name in **Anonymous name**. When you leave **Anonymous name** blank, your inner identity is used as your outer identity.

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

In some cases, you might need to add additional text. For example, if this outer identity is used to route your authentication to the proper server, you might be required to use a format such as **anonymous@acme.com**.

It is possible that anonymous EAP-PEAP authentication does not work with your network authentication server, in which case leave the **Anonymous name** blank.



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

TTLS Settings

If you selected EAP-TTLS in the **Authentication** tab, use the **TTLS Settings** tab to configure EAP-TTLS and any related inner authentication protocols.

EAP-TTLS creates a secure encrypted tunnel through which your credentials are presented to the authentication server. If you use EAP-TTLS with password credentials, an inner authentication protocol completes the authentication. See “EAP-TTLS” on page 71 for more information about this protocol.

To add an inner TTLS protocol:

1. From the **TTLS** tab in the Profile Properties dialog, click **Add**. Any protocols that you have selected already do not appear in the list.
2. Select a TTLS inner protocol from the list.
3. Click **Add** to display the list from which you can choose inner EAP protocols. Any protocols that you selected previously are not listed.

To delete an inner TTLS protocol:

1. From the **TTLS** tab in the Profile Properties dialog, select the protocol in the list that you want to remove.
2. Click **Remove**.

To reorder protocols:

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

Click **OK** to update the profile configuration.

PEAP Settings

If you selected EAP-PEAP as an authentication method in the **Authentication** tab, use the **PEAP Settings** tab to configure EAP-PEAP and any related inner authentication protocols. Table 4 on page 38 shows the valid inner EAP authentication methods.

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

To add an inner PEAP protocol:

1. From the **PEAP** tab in the Profile Properties dialog, click **Add**.
2. Select an inner protocol list of inner authentication protocols.
EAP-GenericTokenCard and EAP-MS-CAHP-V2 are valid options.
3. Click **OK**.

To delete an inner PEAP protocol:

1. From the **PEAP** tab in the Profile Properties dialog, select the protocol in the list that you want to remove.
2. Click **Remove**.

To reorder protocols:

1. Select a protocol to move.
2. Use the up and down arrow buttons on the **PEAP** tab of the Profile Properties dialog to reposition the protocol on the list.

If you select EAP-GenericTokenCard as one of your PEAP inner authentication methods, you can configure the EAP-GenericTokenCard settings under the Setting Up Authentication tab. These settings allow you to choose to use your password credentials or your token card ID for authentication.

3. Click **OK** to update the profile configuration.



NOTE: If you select EAP-TLS as an inner authentication method, you must configure certificate-based user credentials on the **Using Certificates** subtab of the **Specifying User Information** tab.

Setting EAP Inner Authentication Protocols

TTLS and PEAP support inner authentication tunnels. Inner authentication provides an additional level of security by transferring password credentials through an encrypted tunnel between the client and the authentication server. Table 4 on page 38 lists the compatible inner and outer authentication protocols for TTLS and PEAP.

Use the **Inner authentication protocol** list to select the inner authentication protocol to use. Consult your network administrator for the recommended corporate settings for your network.

Table 4: Outer EAP Protocols and Supported Inner Protocols

Compatible Inner Authentication Methods	EAP-TTLS for Outer Authentication	EAP-PEAP for Outer Authentication
PAP	Yes	No
CHAP	Yes	No
MS-CHAP	Yes	No
MS-CHAP-V2	Yes	Yes
PAP/Token Card	Yes	No
EAP	Yes	No
GenericTokenCard	No	Yes
TLS	No	Yes

To select an inner authentication protocol:

1. Select a profile and open the Profile Properties dialog.
2. Select the **TTLS** or the **PEAP** tab, based on the outer EAP authentication method being used.
3. Next to **Inner authentication protocol**, select the pull-down menu to display the list of inner authentication protocols.
4. Select a protocol from the list.

To set up a preferred order of multiple inner authentication protocols, select a protocol from the list that you created and use the arrow buttons (located above the **Add** button) to move it up or down in the list.

The most commonly used protocol, MS-CHAP-V2, authenticates you against user databases.

When you use PAP/Token Card, the password value that you enter into the Password dialog is never cached, because any token-based password is good for one use.

Select with your network administrator to determine which inner authentication protocols to use on your network.

EAP as an Inner Authentication Protocol

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

To add an inner EAP protocol:

1. From the **TTLS** tab in the Profile Properties dialog, select **EAP** from the list of inner authentication protocols.
2. Click **Add** to display the list from which you can choose inner EAP protocols.
3. Select an inner EAP protocol from the list and click **OK**.
4. To add other inner EAP protocol to the list, repeat this procedure.

See Table 4 on page 38 for a list of outer EAP protocols and the corresponding inner protocols.

To remove a protocol:

1. Select the protocol to remove.
2. Click **Remove**.

To reorder protocols:

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

Removing a Profile

To remove an authentication profile, select the profile name in the Profiles dialog (Figure 6) list and click **Remove**.

Sample Profile Configuration

This section shows a sample authentication profile for a corporate network. (You do not typically need a profile for a hotspot or a home Wi-Fi network unless being authenticated to the wireless network is a requirement.)

Table 5: Sample Profile for a Corporate Network

Setting	Value
Profile name	ACME_NYC
Login name	this user
Permit using password	Yes
Use password	Yes
Authentication	EAP-TTLS
Validate server certificate	Yes
Token card credentials	Use my password
TTLS inner authentication	EAP-MS-CHAP-V2 (See Table 4 on page 38.)

The EAP protocol is a sample. Your corporate network may use a different EAP protocol such as EAP-TLS or EAP-PEAP. Similarly, the credentials and inner authentication protocol requirements may be different. Before configuring these settings in OAC, check with your network administrator about recommended settings.

Chapter 7

Managing Network Access

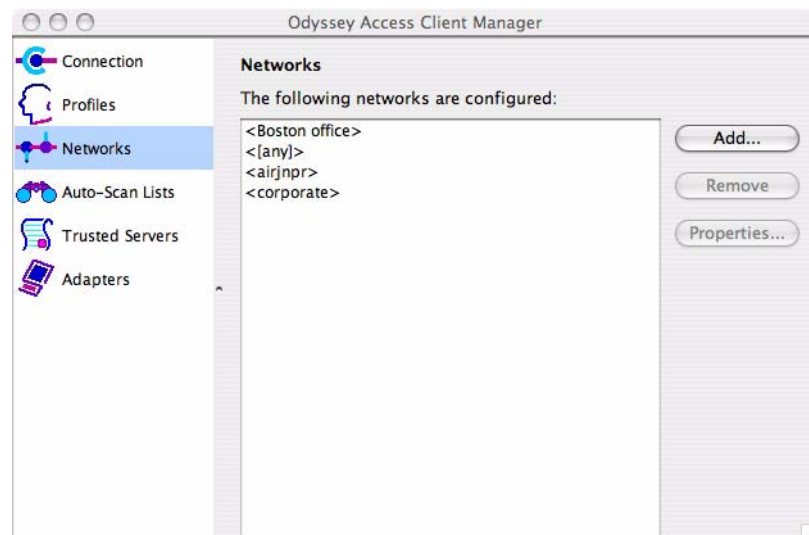
This chapter describes how to define and configure the networks you intend to use.

Before you can connect to any network with OAC, you must configure it in OAC and name it. The networks that you define can include one or more corporate wired and wireless networks, your home wireless network, and one or more “hotspot” networks at airports, train stations, restaurants, or coffee shops. Configuration settings for each of these networks varies, so you must name and configure each one separately.

Networks Dialog

To configure the settings for connecting to a network, click **Networks** from the sidebar. The Networks dialog (Figure 9) opens.

Figure 9: Networks Dialog



Each currently configured network appears in the dialog.

Adding or Modifying Network Properties

To add a new network configuration, click **Add** in the Networks dialog. The Add Network dialog opens.

To modify the settings for an existing network configuration, click **Properties** in the Networks dialog. The Network Properties dialog opens.

The Add Network and the Network Properties dialogs have the same configuration options. Figure 10 shows the configuration options in the Add Networks dialog.

Figure 10: Sample Add Network Dialog

The dialog has three configuration categories:

- **Network**—Use these settings to provide a name for the network that you are configuring, to configure the method used to connect to the network, and to specify the encryption method to use.
- **Authentication**—Use these settings to specify whether you will use an authentication profile or WEP keys to authenticate.
- **Pre-configured keys (WEP)**—Use these settings to specify the WEP keys.

The settings you must provide depends on whether the network uses authentication and encryption.

Network Settings

The following sections describe each of the network configuration categories. Once you have defined a network, it is unlikely that you will need to change it unless your network administrator indicates that a change is necessary.

Specifying a Network Name (Network SSID)

The *network name* or SSID (service set identifier) is the actual name of the wireless network to which you want to connect. The network names that are currently configured appear in the Network dialog. A network name can be up to 32 alphanumeric characters and is case-sensitive. You must enter the name correctly to connect.

Connecting to Any Available Network

OAC provides a special network configuration called **[any]** that you can use to connect to any available network, regardless of the network name. The **[any]** network is useful when you are moving between conferences, hotels, or other locations that provide network access. When you select the **[any]** network from the Connection dialog, you can connect to such networks without having to configure them individually.

Click **Connect to any available network** to use the **[any]** option.



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

Scanning for Available Networks

Instead of entering the name of a configured network in the **Network name** field, you can click **Scan** to select from a list of all currently visible networks; that is, all the wireless networks that OAC can detect. If you are in the vicinity of the network that you are configuring, clicking **Scan** is easier than typing and guarantees that the network name is set correctly. Simply select the network from the scan list.

Adding a Network Description

Network names are chosen by an administrator and are not unique, so two unrelated networks could have the same name. Use the **Description** field to add text to distinguish between networks that have similar names.

You can use the network **Description** field to distinguish connections to the same network using different profiles. For example, you might want to use different credentials at different times.

The network description is optional.

Specifying a Network Type

There are two network types for a wireless connection. The more common type uses a wireless access point to connect to an existing network, such as in corporate, hotspot, and home WiFi networks. The other type of network is a Peer-to-Peer network, also known as an ad-hoc network. It is typically used for spontaneous connections between wireless computer users to exchange information or to play games without connecting to an existing wireless network infrastructure. Ad-hoc connections are short-range wireless connections set up directly between computers.

To specify the type of network you will use, click the **Network type** drop-down list.

- Click **Access point (infrastructure mode)** if this network uses wireless access points to provide connectivity to the corporate network or the Internet. This is the most common setting.
- Click **Peer-to-peer (ad-hoc mode)** to set up a private network and connect directly with other computers or devices.

Specifying a Channel

If you click **Peer-to-peer (ad-hoc mode)** as the network type, you must specify a channel on which all peers share data. There are 14 channels for 802.11b and 802.11g and 12 channels for 802.11a wireless networks. Choose the default channel or select a channel from the **Channel** list. Whoever initiates the peer-to-peer network connection chooses the channel on which the peer-to-peer session occurs.

Specifying an Association Mode

Before authentication can occur, your client must associate to an access point to request network access. The association mode that you choose depends on the access point hardware configuration. Your network administrator can help you configure the association mode that is required for your network.

In a wireless hotspot, such as a coffee shop, you can typically obtain the access configuration information from an employee.

In an airport or train station, click **[any]** as the network. Your Web browser may prompt for credit card payment information when attempt to connect to the network and displays the configuration information needed for that network.

Choose one of the following association modes:

- **Open**—Use this setting to connect to a network through an access point or switch that implements 802.1X authentication. Choose this mode if you are not required to select shared mode or Wi-Fi Protected Access (WPA).
- **Shared**—Use this setting to connect to a network through an access point that requires at least one preconfigured wired-equivalent privacy (WEP) key for association.
- **WPA**—Use this setting to connect to a network through an access point that implements WPA.

- **WPA2**—Use this setting to connect to a network through an access point that implements WPA2, the second generation of WPA that satisfies 802.11i.

Encryption Methods for an Association Mode

Your choice of encryption method depends on the access point requirements. The choices available to you depend on the association mode you choose.

You have the following options:

- **None**—Use this setting to select 802.1X authentication without WEP keys. This option is available to you only when you configure access point association in open mode. This is a typical setting to use for wireless hotspots.
- **WEP**—Use this setting to use WEP keys for data encryption. This is an option for open mode association and is required when you associate in shared mode. When you use WEP encryption, fill in at least one preconfigured WEP key at the bottom of the Add Network dialog—unless you use a profile for authentication and click **Keys will be generated automatically for data privacy**. Choose WEP encryption when the access points in your network require shared mode association with WEP keys or when your access points require WEP encryption.
- **TKIP**—Use this setting to use the Temporal Key Integrity Protocol for access points in your network require WPA or WPA2 association and are configured for TKIP data encryption.
- **AES**—Use this setting to use the Advanced Encryption Standard protocol. Choose this option when the access points in your network require WPA or WPA2 association and are configured for AES data encryption. If your client hardware and access point support AES, use AES encryption when you associate in WPA2 or WPA mode.

Authentication Settings

Use the **Authentication** fields to specify whether or not to use 802.1X authentication for the network and how to generate encryption keys.

Authenticating with a Profile

To authenticate using your personal credentials:

1. Click **Authenticate using profile**.
2. Select the name of profile to use for authentication from the drop-down list next to the **Authenticate using profile** check box. You must have a profile that is appropriate for being authenticated by this network.

Use this configuration setting if you are using an EAP protocol that requires user authentication, such as EAP-TTLS or EAP-PEAP. Contact your network administrator about which EAP protocol has been implemented on your network.

When you click **Authenticate using profile** and select a profile from the list of profiles next to the **Authenticate using profile** check box, OAC performs an 802.1X authentication using the options configured in the selected profile.



NOTE: If the profile you select for this network specifies MD-5 Challenge or EAP-GenericTokenCard as an outer authentication method, you must use a preconfigured WEP key for data encryption to authenticate using 802.1X. See “Preconfigured Keys (WEP)” on page 47.

Automatic Key Generation

If the authentication method specified in the selected profile results in the creation of dynamic WEP keys for use between your Macintosh computer and the access point, click **Keys will be generated automatically for data privacy**. Certain authentication methods, such as EAP-TTLS, EAP-PEAP, EAP-FAST, and EAP-TLS, generate keys; others do not.

If you associate this network with a profile that uses EAP-TTLS, EAP-PEAP, EAP-FAST, or EAP-TLS as an authentication protocol, click 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 and is available with all encryption methods (other than **None**), as long as you are not associating in shared mode.

Leave this option cleared if you are required to use preconfigured WEP keys or, in the case of WPA association, a preshared key.

Preconfigured Key Settings

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

You can enter keys in the lower portion of your network properties description, based on the selected association method.

Preshared Keys (WPA or WPA2)

If you associate using WPA or WPA2 and if you do not generate encryption keys automatically when associating an authentication profile to the network connection, you must supply a preshared 8–63 character ASCII passphrase in the **Passphrase** field. The passphrase is used as a seed to generate the required keys.

When you use a passphrase, you do not authenticate with a RADIUS server. You can use passphrases and static WEP keys if you are not connecting to a network that uses 802.1X authentication, such as home networks, hotspots, and small offices.



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

Preconfigured Keys (WEP)

WEP keys serve the following purposes:

- They allow you to associate with an access point before a connection can be established (shared mode).
- They encrypt data between your Macintosh computer and the access point (or other computer users in a peer-to-peer network).

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

- You associate in shared mode. See “Specifying an Association Mode” on page 44.
- You select WEP encryption for the open association mode and you do not generate encryption keys automatically. See “Encryption Methods for an Association Mode” on page 45.

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

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

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

Table 6: WEP Key Specifications

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

To enter any preconfigured WEP keys:

1. In **Format for entering keys**, click **ASCII** or **Hexadecimal**.
2. Type each WEP key that you want to preconfigure into the text fields **Key 0** through **Key 3**, based on the specifications in Table 6.

Removing a Network

To remove a network:

1. Open the Network dialog.
2. Select a network from the list of configured networks.
3. Click **Remove**.

Sample Network Configuration Setups

This section shows three examples of setting up wireless network configurations. The first is for a corporate wireless network. The second is for a wireless hotspot. The third is for a home wireless network.

Sample Configuration for a Corporate Wi-Fi Network

Table 7: Sample Configuration for a Corporate Wi-Fi Network

Setting	Value
Network name (SSID)	ACME_NYC_ Wi-Fi
Connect to any available network	No
Description	Corporate office wireless network
Network Type	Access point (infrastructure mode)
Association mode	WPA2
Encryption mode	AES
Authenticate using profile	ACME_NYC
Keys will be generated automatically for data privacy	Yes

Sample Configuration for a Wireless Hotspot Network

Table 8: Sample Configuration for a Hotspot Network

Setting	Value
Network name (SSID)	Hartsfield Airport
Connect to any available network	Yes
Description	Hartsfield Airport Wi-Fi Network
Network Type	Access point (infrastructure mode)
Association mode	open
Encryption mode	none
Authenticate using profile	Hartsfield

Sample Configuration for a Home Wireless Network

Table 9: Sample Configuration for a Home Wireless Network

Setting	Value
Network name (SSID)	< MyHome Wi-Fi >
Connect to any available network	Yes
Description	Home wireless network
Network Type	Access point (infrastructure mode)
Association mode	open
Encryption mode	WEP
Authenticate using profile	home

Chapter 8

Managing Auto-Scan Lists

An *auto-scan list* is an ordered list of configured networks. You can create one or more auto-scan lists and order them in a top-down hierarchy. If you connect to a network using an auto-scan list, rather than to an individual network, OAC scans sequentially through the listed networks for the *first available* network.

Using an auto-scan list means that you do not have to specify a new network connection each time that you move from one location to another. This is a convenient feature, especially when you move your client machine regularly to different locations and different networks. As an example, an auto-scan list could include your home network, your office network, and a favorite hotspot. A second auto-scan list could contain multiple corporate and customer networks that you visit regularly, along with the airport hotspots that you frequent when traveling from one customer to another.

An auto-scan list contains as many networks as you like. When OAC uses an auto-scan list, it attempts to connect to the *first* SSID in the list, then the next one, and so on. OAC remembers this connection so that, if you disconnect and reconnect, OAC selects the last auto-scan connection automatically. An exception to this rule is that OAC goes through the auto-scan list from the beginning each time if the SSIDs are being broadcast.

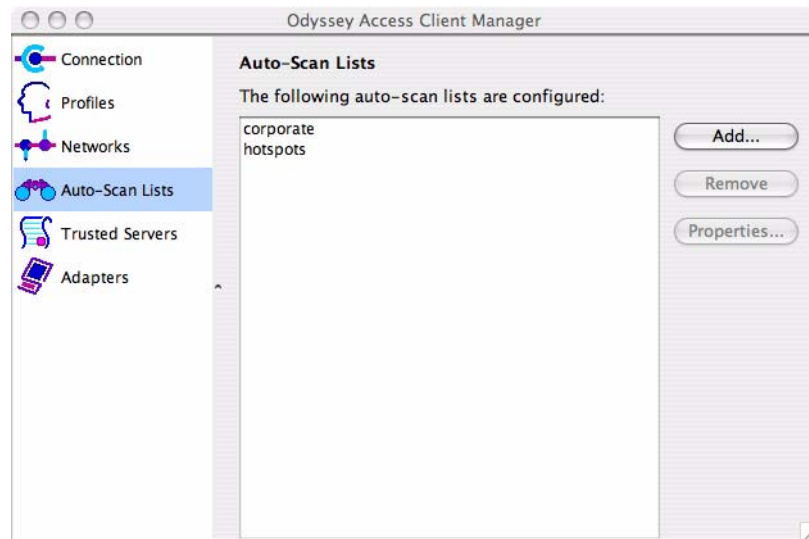


NOTE: Each of the networks in an auto-scan list must be configured in the Networks dialog. See “Adding or Modifying Network Properties” on page 42.

Using the Auto-Scan List Dialog

To set up or modify an auto-scan list, click **Auto-Scan Lists**. The Auto-Scan Lists dialog (Figure 11) opens.

Figure 11: Auto-Scan Lists Dialog



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

- Add an auto-scan list
- Remove an auto-scan list
- Modify an auto-scan list
- View the contents of an auto-scan list

Adding an Auto-Scan List

To add an auto-scan list:

1. Click **Auto-Scan Lists** in the sidebar.
2. Click **Add** in the Auto-Scan Lists dialog. The Add Auto-Scan List dialog appears.
3. Enter a unique name for the auto-scan list in the **Auto-Scan list name** field.
4. Select networks to add to the auto-scan list from the list of configured networks listed under **Available Networks** on the left. Use the right arrows to move networks from the left to the **Networks in list, in priority order** on the right.

5. Prioritize the selected networks based on the frequency with which you expect to connect to them. Place the highest priority networks at the top of the list. A network on this list is considered to be *preferred* over the networks listed below it. You can select one or more networks and use the up and down arrows to reorder the list.
6. Click **OK** when you complete the set up for the auto-scan list.

Removing an Auto-Scan List

To remove an auto-scan list:

1. Select the name of the auto-scan list from the Auto-Scan Lists dialog.
2. Click **Remove**.

Modifying an Auto-Scan List

To modify an auto-scan list:

1. Select the name of the auto-scan list from the Auto-Scan Lists dialog.
2. Click **Properties** or double-click the name of the auto-scan list. The Auto-Scan List Properties dialog appears.
3. Make the necessary modifications to the current settings.
4. Click **OK**.

Viewing Network Names in an Auto-Scan List

To view the names in an auto-scan list, select the name of the auto-scan list in the Auto-Scan List dialog. The Auto-Scan List Properties dialog then shows the networks in the auto-scan list in the preferred order.



NOTE: Test the network connection for each network in your auto-scan list separately. If a network connection on the auto-scan list is configured incorrectly so that authentication fails each time incorrect attempts are made to that connection, OAC does not skip that network to try the next network on the list. To test a single selected network connection, go to the Connection dialog of the OAC and click **Connect using network** after selecting the network you want to test.

Chapter 9

Managing Trusted Servers

Establishing server trust protects you from intrusion or hostile attacks from anyone who might be pretending to represent that server. This chapter describes trusted servers and the configuration tasks for managing trust, trusted servers, certificates, and certificate authorities.

You can add, remove, and configure trusted network servers and configure certificate and identity information for each server that must authenticate you when you connect. Configuring trust is required for protocols that implement mutual authentication and is a recommended security measure. See “Validating a Server Certificate—Mutual Authentication” on page 34.



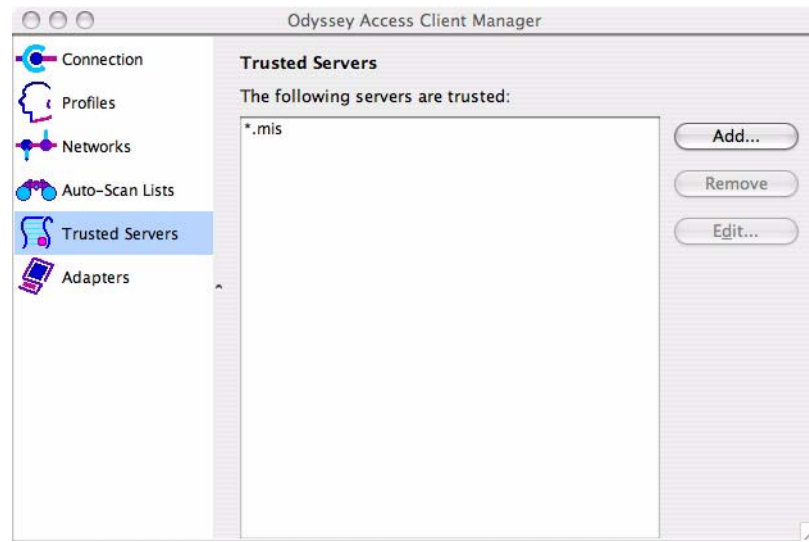
NOTE: Check with your network administrator before adding any trusted server or changing any current trust configuration settings. Specifying incorrect settings can prevent you from accessing your network.

Configure trust for authentication servers when you use EAP-TTLS, EAP-TLS, or EAP-PEAP authentication. During authentication with these EAP protocols, the authentication server sends a server certificate to OAC. The certificate represents the server’s trust credentials. OAC must trust that server certificate before it can continue communicating with that server. If OAC does not trust the server, the authentication process terminates.

Configuring Trust in OAC

To configure server trust in OAC, open the Trusted Servers dialog (Figure 12). Any trusted server that is currently configured appears there.

Figure 12: Trusted Servers Dialog



NOTE: There are two locations for trusted roots (intermediate and self-signed) on a Macintosh system. **X509Anchors** can be found in the system keychain. The other location is in the user login keychain.

You can allow OAC to trust any server that bears a specified signed certificate.

Selecting Trust Servers

You can use domain names to represent the servers to be trusted. To configure trust:

1. Specify the authentication server or intermediate CA server domain name or the ending of the domain name (for example, **acme.com**).
2. Specify a certificate from any Certificate Authority in your certificate authority chain. This can be the certificate of a root or an intermediate certificate authority.

Adding a Trusted Server Entry

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

Configuring trust offers you two choices for adding a trusted server:

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

To add a trusted server:

1. Click **Add** in the Trusted Servers dialog to display the Add Trusted Servers Entry dialog to begin the server configuration.
2. You can configure trust for any server that has been issued a specified signed certificate, or you can specify one or more servers to be trusted using domain names when those servers are issued a specified signed certificate:
 - To trust all servers that have a specified signed certificate, click **Trust any server with a valid certificate regardless of its name**.
 - To specify servers by name, enter the identity of the trusted server in the **Server name must end with** field.
3. Set the **Server certificate must be issued by** field to the name of the certificate authority that directly or indirectly issued the server certificate. This field is set automatically if you select a root or intermediate CA-issued certificate. The name that appears in the field need not be the name of the certificate authority that directly issued the server certificate. The server certificate can be issued by any authority in the chain.

To configure the **Server certificate must be issued by** field:

- a. Click **Browse** to display a list of certificates. The Select Certificate dialog appears.
 - b. Select the required certificate from the list and click **OK**.
4. Select **OK** to close the Add Trusted Servers Entry dialog.

Server Identity

Each server has a unique name that is usually located in the **Subject CN** field of the server certificate.

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

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

Editing a Trusted Server Entry

You might need to change the trusted server configuration. For example, you might want to change the setting from trusting any server with a valid certificate to just one or a small set of domain names.

To edit an entry in the trusted servers list:

1. Select the entry from the Trusted Servers dialog.
2. Click **Edit**.

The Trusted Server Properties dialog appears. From this dialog, you can change the server domain and select a different certificate. See the directions in “Adding a Trusted Server Entry” on page 56.

Removing a Trusted Server Entry

To remove an entry from the trusted servers list:

1. Select the entry from the Trusted Servers dialog.
2. Click **Remove**.

Setting Up Certificates

A certificate is cryptographic data which guarantees that a particular public key is associated with the private key of a particular entity. This entity can be an individual or a computer. A certificate contains many pieces of information that are used in mutual authentication, including a public key and the name of the entity that owns the certificate. Each certificate is issued by a certificate authority. By issuing a certificate, the certificate authority warrants that the name in the certificate corresponds to the certificate’s owner.

There are three types of certificates used by OAC:

- Trusted root certificates
- Intermediate CA certificates
- Personal certificates

The certificates must be installed in the correct keychain before use.

Trusted Root Certificates

If you use TLS, TTLS, or PEAP, you may need a Trusted Root CA certificate. The certificate must be in DER-encoded (Distinguished Encoding Rules) format and be present in either the root store, **X509Anchors**, or **login**. You must have administrative privileges to add certificates to **X509Anchors**. For purposes of trust calculation, root certificates in the **login** keychain are not considered completely trusted and always invoke a trust dialog. Root certificates in **X509Anchors** with trust settings of **Always trust** do not display this popup.

To add a trusted root certificate, double-click on a **.der** or **.cert** file and select the appropriate keychain at the prompt.

Intermediate Certificates

You may also use an Intermediate CA certificate with those EAP protocols. An Intermediate CA certificate has the same file format and extension as a trusted Root certificate and goes in the same locations.

Personal Certificates

If you use TLS, you must have a personal certificate. A personal certificate contains private data encoded in PKCS12 format.

Adding a Certificate

To add a personal certificate:

1. Double-click a `.pfx` file.
2. Select the **login** keychain at the prompt.

After certificates have been installed they can be viewed and used as part of OAC configuration. If you install the certificate files while OAC is running, toggle the checkbox in the Connection panel to make OAC check immediately for new certificates.

For more background about authentication, trusted certificates, and the protocols that use them, see “Extensible Authentication Protocol” on page 69 and “Certificates” on page 70.

Chapter 10

PAC Manager

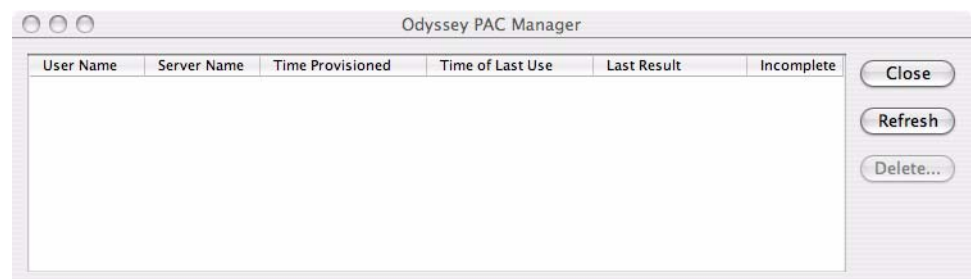
The EAP-FAST (Flexible Authentication via Secure Tunneling) protocol enables secure communication between a user and a server by using a TLS handshake to establish a mutually authenticated tunnel. EAP-FAST does not use a server certificate but, instead, a high-entropy secret called a Protected Access Credential (PAC) that is known to both the client and the AAA server to secure the TLS handshake.

PACs are provisioned manually by an administrator. The PAC Manager displays PAC status information and buttons to refresh the view or to remove a PAC that is out of date. See the *Steel-Belted Radius Administration Guide* or your Cisco ACS documentation for a further discussion of Protected Access Credentials and how to provision them.

Using PAC Manager

To open the PAC Manager tool (Figure 13), go to **Settings > PAC Manager**.

Figure 13: PAC Manager Tool



Refreshing the Pac Manager Display

To update the display for a selected PAC listing, click **Refresh**.

Deleting a PAC

To delete one or more selected PACs from the list, click **Delete**.

Exiting from the PAC Manager

To exit from the PAC Manager tool, click **Close**.

Appendix A

Network Security Concepts

This appendix contains background information for anyone needing a better understanding of the concepts and protocols that show how Odyssey Access Client operates in a network, particularly from the standpoint of network security and authentication.

Network Security

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

With wireless networks, a person can use a wireless adapter and a laptop computer to access a network, even from a location outside of the building.

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

- IEEE (Institute of Electrical and Electronic Engineers) standards for wireless LANs. These include 802.11a, 802.11b, and 802.11g. See “802.11 Wireless Networking” on page 65.
- IEEE 802.11i enhancements to 802.11. These were introduced to overcome some of the security weaknesses of 802.11.
- The Wi-Fi Alliance second generation of Wi-Fi protected access. Wi-Fi protected access 2 (WPA2) (with advanced encryption standard (AES) encryption) adheres to the strong 802.11i enhancements. See “Wi-Fi Protected Access and its Encryption Methods” on page 67 for definitions.
- WPA (with AES or temporal key integrity protocol (TKIP) encryption), which complies with a subset of 802.11i. While WPA is not as strong as WPA2, it addresses some of the security weakness of 802.11. See “Wi-Fi Protected Access and its Encryption Methods” on page 67 for definitions.
- The IEEE 802.1X standard. 802.1X supplements the 802.11 standards with secure server-based wireless network connections. See “802.1X Authentication” on page 68.

- IPsec is a set of protocols used to secure (encrypt) IP data packets being exchanged on a network. Best practices for network security usually call for encrypting the data being transferred between protected network resources and endpoint computers. A Juniper UAC network can include a firewall that provides an IPsec gateway deployed in front of protected resources to enforce the security policy. Odyssey Access Client supports IPsec encryption as part of conforming to that policy.

Encryption and Association for Secure Authentication

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

- Association is the method by which a client establishes a relationship with an access point.
- Data encryption is used to secure data that is exchanged between a client device and a network access device.
- Encryption keys are a sequence of characters that an encryption algorithm uses to make plain text unreadable unless you share the encryption keys to decode the encrypted message. Encryption keys are key components of data encryption algorithms. Encryption keys might also be used for access point association.
- Once a wireless client has associated with an access point, the user of that client device can be authenticated to the network. Authentication is used to secure the relationship between a user and an authentication server. For example, wireless network authentication that is based on the 802.1X standard can use cryptographically strong (and dynamically generated) encryption keys.

Authentication Overview

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

- Preconfigured secrets, called WEP (wired-equivalent privacy) keys. These keys are intended to encrypt the data transferred between the client and the access point and can be used to keep unauthorized users off the wireless network and to encrypt the data of legitimate users. See “Wired-Equivalent Privacy” on page 67 for a description of WEP-based encryption that complies with 802.11 standards.

- Preshared passphrases used to generate keys for WPA or WPA2 association. Preshared passphrases enable you to configure a simple phrase that is used to generate cryptographically strong encryption keys to be used with AES or TKIP encryption. AES and TKIP periodically change the encryption keys in use. The generated keys keep unauthorized users off the wireless network and encrypt the data of legitimate users. See “Wi-Fi Protected Access and its Encryption Methods” on page 67 for a description of AES or TKIP encryption methods that enhance the 802.11 standards.
- Authentication using an 802.1X-based protocol. This method uses a variety of underlying authentication protocols to control network access. The stronger protocols provide cryptographically protected mutual authentication of the user and the network. In addition, you can configure Odyssey Access Client so that keys that are used to encrypt wireless data are generated dynamically. 802.1X-based authentication can use WEP, AES, or TKIP encryption, depending on network hardware/firmware. See “802.1X Authentication” on page 68 for information about authentication using 802.1X. See “Wi-Fi Protected Access and its Encryption Methods” on page 67 for a description of some of the strongest available association and encryption modes.

Odyssey Access Client Features for a Secure Network

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

- You can require user authentication. A user must be authenticated by the network before being allowed access to the network and make it safe from intruders. See “Extensible Authentication Protocol” on page 69 for an overview of the Odyssey Access Client authentication protocols. For protocol configuration details, see “Setting Up Authentication” on page 32.
- You can require data encryption between the wireless client and the access point. The wireless connection between a client and an access point must be encrypted so that eavesdroppers cannot access private data. For configuration details, see “Networks Dialog” on page 41.
- You can configure server trust for mutual authentication. The network must be authenticated (trusted) by the user before the user enables their credentials to be released to the network to make a network connection. This prevents a wireless device that might be posing as a legitimate network from impersonating the network and gaining access to the user’s computer.

802.11 Wireless Networking

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

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

Types of 802.11 Wireless Networks

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

Access Point Networks

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

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

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

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

When you connect to a network via an access point, you are using the 802.11 *infrastructure mode*. See for information about configuring infrastructure network connections.

Peer-to-Peer Networks

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

The 802.11 standard refers to peer-to-peer network connectivity as *ad-hoc mode*. See and for information about configuring ad-hoc network connections.

Wireless Network Names

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

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

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

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

Wired-Equivalent Privacy

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

- **Shared**—Use this mode when the access point requires that you preconfigure a WEP key for association. When 802.11-based preconfigured (static) WEP keys are in use, the client and the access point share the same secret keys and a client is not allowed to access the network unless it can prove it knows the preconfigured WEP keys assigned to the access point. This is not as secure as authenticating with 802.1X methods.
- **Open**—Use this mode for WEP-based data encryption when the access point does not require that you preconfigure a static WEP key for association.



NOTE: You can obtain stronger network security when you use dynamic encryption key generation and 802.1X-based authentication. For shared association, a preconfigured key that is used only for access point association is still required. See “802.1X Authentication” on page 68 and “Extensible Authentication Protocol” on page 69 for more information.

See the following topics:

- “Specifying an Association Mode” on page 44.
 - “Wired-Equivalent Privacy” on page 67 to use static WEP keys with Odyssey Access Client.
-



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

Wi-Fi Protected Access and its Encryption Methods

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

- Improved data encryption with the TKIP algorithm. TKIP provides stronger encryption than WEP.
- Improved data encryption with the AES algorithm. AES provides stronger encryption than WEP or TKIP.

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

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



NOTE: With access points enabled for WPA2 or WPA, you can obtain the stronger network security when you use dynamic encryption key generation and 802.1X-based authentication. See “802.1X Authentication” on page 68 and “Extensible Authentication Protocol” on page 69 for more information.

See the following topics:

- “Specifying an Association Mode” on page 44 to use WPA2 or WPA association mode with Odyssey Access Client
- “Preconfigured Keys (WEP)” on page 47 to configure a passphrase that is used in encryption key generation



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

802.1X Authentication

The IEEE 802.1X protocol provides authenticated access to a LAN. This standard applies to wireless and wired networks. In a wireless network, the 802.1X authentication occurs after the client has associated to an access point using an 802.11 association method.

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

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

With 802.1X, a user can log in to the network from any Macintosh computer 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.

Extensible Authentication Protocol

802.1X uses the Extensible Authentication Protocol (EAP) to perform authentication. EAP is not an authentication mechanism but rather 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.

OAC supports a number of EAP protocols, enabling a network administrator to choose the protocols that work best for a particular network.

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

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

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

Mutual Authentication

EAP-TTLS, EAP-PEAP, EAP-TLS, and EAP-FAST provide *mutual authentication* of the user and the network and produce dynamic keys that can be used to encrypt communications between the client device and access point. With mutual authentication, the network authenticates the user credentials and the client software authenticates the network credentials.

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

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

Certificates

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

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

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

- A public key
- A private key

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

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

Your enterprise certificate authority might issue certificates to smart cards. Odyssey Access Client supports all types of user certificates.

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

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

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

- An end entity certificate
- A root certificate

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

EAP-TLS

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

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

EAP-TTLS

EAP-TTLS is designed to provide authentication that is cryptographically as strong as EAP-TLS, while not requiring that each user be issued a certificate. Instead, only the authentication servers require certificates.

EAP-TTLS authentication is performed using a password or other credentials. Password-type credentials are transported in a securely encrypted “tunnel” that is established using the server certificate. Within the EAP-TTLS tunnel, you can employ any of a number of inner authentication protocols. With tunneled password credentials, user authentication can be performed against the same security database that is already in use on the corporate LAN. See for more information about configuring inner protocols for tunneled authentication.

If your enterprise has a user-based certificate infrastructure in place, you have the option to configure user certificate-based credentials for EAP-TTLS authentication, with or without tunneled password credentials. See “Using Certificates” on page 32.

EAP-PEAP

EAP-PEAP is comparable to EAP-TTLS, both in its method of operation and its security. However, EAP-PEAP is not as flexible as EAP-TTLS and it does not support the range of inside-the-tunnel authentication methods that EAP-TTLS supports. Commercial implementations of this protocol that started appearing at the beginning of 2003 had interoperability problems. Nevertheless, this protocol is in widespread use. See for more information about configuring inner protocols for EAP-PEAP authentication.

EAP-FAST

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

EAP-LEAP

EAP-LEAP (Lightweight EAP) enables users to be authenticated using password credentials without the use of certificates. The data exchange in EAP-LEAP is fundamentally similar to the exchange that occurs when a user logs in to a Domain Controller.

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

Reauthentication

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

You can configure automatic periodic reauthentication to the network using Odyssey Access 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 Macintosh computer and access point. The access point might use these shared keys to refresh the keys used to encrypt data. By frequently refreshing keys, you can thwart cryptographic attacks.

See “Enable automatic reauthentication” on page 10 for information about configuring this feature.

Session Resumption

When you first authenticate using EAP-TTLS, EAP-PEAP, or EAP-TLS, a fair amount of intensive computation occurs, both on your client computer and on the network authentication server. Private keys must be used to encrypt or sign data, signatures on certificates must be validated, and password credentials must be selected.

Once you have authenticated a connection to the network, your network session begins. During a session, any subsequent authentications to the same network server can be accelerated by reusing the secret information that is derived during the first authentication. This is called *session resumption*. You can configure client-side session resumption features that apply to the certificate-based protocols using Odyssey Access Client. This feature is particularly useful when you have a wireless connection and are moving (“roaming”) from one access point location in a building to another. With this feature enabled, along with automatic reauthentication, your network connection is not interrupted and there is no need to reconnect or reauthenticate.

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

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

See “Enable session resumption” on page 10 for more information about using this feature.



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

Appendix B

Glossary

A

AAA—Authentication, Authorization, and Accounting.

Access Control List (ACL)—A listing of users and their associated access rights. Used to implement discretionary and or mandatory access control between subjects and objects.

Accounting—Tracking users' access to resources primarily for billing purposes. See also AAA.

Advanced Encryption Standard (AES)—Standard approved by NIST for the next 20-30 years of use.

Advanced Research Projects Agency (ARPA)—An agency of the US Department of Defense that promotes exploratory research in areas that carry long-term promise for military applications. ARPA funded the major packet-switching experiments in the US that lead to the formation of the Internet.

Algorithm—A set of sequenced steps that are repeated each time. In encryption, the algorithm is used to define how the encryption is applied to the data.

Alias—An assumed name (dummy) mail address that routes messages to all real addresses associated with the assumed name.

American National Standards Institute (ANSI)—Represents the US in the ISO. A private standards body that develops, endorses, and publishes industry standards.

Application programming interface (API)—Provides means to take advantage of software features.

ARP—Address Resolution Protocol.

ASCII—American Standard Code for Information Exchange. ASCII is a code to represent letters, numerals, punctuation marks and control signals as seven-bit groups. It is used as a standard code by the transmission of data.

Association—The method by which a client establishes a relationship with an access point.

Asymmetric algorithm—A pair of key values, one public and one private, used to encrypt and decrypt data. Only the holder of the private key can decrypt data encrypted with the public key, which means anyone who obtains a copy of the public key can send data to the private key holder in confidence. Only data encrypted with the private key can be decrypted with the public key, this provides proof of identity, ensures nonrepudiation, and provides the basis for digital signatures.

Asynchronous—Character-by character or cell-by-cell or data unit-by date unit transfer.

Attribute certificate—Digital certificate that binds data items to a user or system by using a name or public key certificate.

Auditing—Tracking users' access to resources primarily for security purposes.

Authenticate—To verify the identity of a user, user device, or other entity, or the integrity of the data stored, transmitted, or otherwise exposed to unauthorized modification in an IS, or to establish the validity of a transmission.

Authentication—The process of validating users who want to access a secure network. See also AAA.

Authorization—The process of identifying what a given user is allowed to do. See also AAA.

Availability—Ensures any necessary data is available when it is requested.

B

Back door—A method of gaining access to a system or resource that bypasses normal authentication or access methods.

Binding—The process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information.

Biometrics—Authentication based on some part of the human anatomy, such as retina, fingerprint, or voice.

Block cipher—Transforms a message from plaintext (unencrypted form) to cipher text (encrypted form) one piece at a time, where the block size represents a standard chunk or data that is transformed in a single operation.

Brute force attack—The process of trying to recover a cryptographic key or password by trying all reasonable possibilities.

C

Centralized key management—A certificate authority that generates both public and private key pairs for a user and then distributes them to a user.

Certificate—An electronic document attached to a public key by a trusted third party that provides proof that the public key belongs to a legitimate owner and has not been compromised. Also called a digital certificate.

Certificate Authority (CA)—An online system that issues, distributes, and maintains currency information about digital certificates. Abbreviated as CA.

Certificate policy—A statement that governs the use of digital certificates.

Certificate revocation—The act of invalidating a digital certificate.

Certificate revocation list (CRL)—A list generated by a CA that enumerates digital certificates that are no longer valid and the reason they are no longer valid.

Certificate suspension—The act of temporarily invalidating a certificate while its validity is being verified.

Challenge Handshake Authentication Protocol (CHAP)—A session-based two-way password authentication scheme. Widely used authentication method in which a hashed version of a user's password is transmitted during the authentication process (instead of passing the password itself). Using CHAP, a remote access device transmits a challenge string, to which the client responds with a message digest (MD5) hash based on the challenge string and the users' password. Upon receipt, the remote access repeats the same calculation and compares the value sent to that value; if the values match, the client credentials are deemed authentic.

Cipher—A method of encrypting text. The term is also used to refer to an encrypted message (although the term cipher text is preferred). Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plaintext or in which units of plaintext are rearranged, or both.

Clear text—Characters in a human-readable form or bits on a machine-readable form. Also called plaintext.

COMSEC—Communications security.

Compliance—In a UAC network, compliance means that the user and endpoint computer meet network authentication and security requirements and are, therefore, allowed to access protected resources on the network.

Cookie—A file or token of sorts passed from the Web server to the Web client (your browser) that is used to identify you and could record personal information such as ID and password, mailing address, credit card number, and so on. Also called HTTP cookie.

Credentials—Information passed from one entity to another and used to establish the sending entity's access rights—commonly a user name and a password.

Cross certification—When two or more Certificate Authorities choose to trust one another and issue credentials on each other's behalf.

Cryptographic module—Any combination of hardware, firmware, or software that implements cryptographic functions such as encryption, decryption, digital signatures, authentication techniques, and random number generation.

D

Data Encryption Standard (DES)—A cryptographic algorithm designed for protection of unclassified data and published by the National Institute for Standards and Technology in Federal Information Processing Standard (FIPS) Publication 46.

Data integrity—Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Demilitarized zone—An area in your network that enables a limited and controlled amount of access from the public Internet. This network segment usually lies between the internal corporate network and public Internet.

Denial of Service (DoS)—A type of attack that denies legitimate users access to a server or services by consuming sufficient system resources or network bandwidth.

DES—Data Encryption Standard.

Dictionary attack—A brute-force attack in which software is used to compare the hashed data, such as a password, to a word in a hashed dictionary. This is repeated until a match is found in the hash, with the goal being to match the password exactly to determine the original password that was used as the basis of the hash.

Diffie-Hellman—The first public key algorithm, using discrete logarithms in a finite field. Invented in 1976.

Digital certificate—A signed electronic document (digital ID) that notarizes and binds the connection between a public key and its legitimate owner. Its main purpose is to prevent unauthorized impersonation and provide confidence in public keys.

Digital signature—A hash encrypted to a private key of the sender that proves user identity and authenticity of the message. Signatures do not encrypt the contents of an entire message. Also, in the context of certificates, a digital signature uses data to provide an electronic signature that authenticates the identity of the original sender of the message.

Disaster recovery plan (DRP)—A plan outlining actions to be taken in case a business is hit with a natural or man made disaster.

Domain—A domain represents a level of the hierarchy in the domain name space and is represented by a domain name.

DNS—Domain Name Service.

E

Encrypt—To convert plaintext into unintelligible forms by means of a cipher system. Term encompassing both encipher and encode.

Encryption algorithm—A mathematical formula or method used to scramble the information before transmitting it over an insecure media. Examples include RSA, DH, IDEA, Blowfish, MD5, DSS/DSA, and Firefly.

Encryption hash—A method in which a selection of data is mixed into a section of data based on an algorithm. The result is called a hashed value.

Encryption keys—A sequence of characters that an encryption algorithm uses to make plain text unreadable unless you share the same encryption key needed to decode the encrypted message.

Extensible Authentication Protocol (EAP)—An IETF standard that provides for mutual authentication between a client and a AAA authentication server.

EAP-LEAP—LEAP (Lightweight EAP) mutual authentication relies on a shared secret and the user's logon password, which is known by the client and the network.

EAP-TLS—Uses digital certificates for both user and server authentication and supports the three key elements of 802.1X/EAP.

EAP-TTLS—Tunneled Transport Layer Security extends the authentication negotiation by using the secure connection established by the TLS handshake to exchange additional information between client and server.

EAP-PEAP—Uses a digital certificate for server authentication. For user authentication, PEAP supports various EAP-encapsulated methods within a protected TLS tunnel. PEAP supports the three main elements of 802.1X/EAP.

Endpoint—An endpoint refers to the computer (desktop, laptop, or other mobile wireless computing device) that you use to access resources on a network.

Extensible Markup Language (XML)—Like HTML, this flexible markup language is based on standards from the World Wide Web Consortium. XML can be used to generate standard or fully customized content-rich Web pages, documents, and applications.

Extranet—A special internetwork architecture wherein a company's or organization's external partners and customers are granted access to some parts of its intranet and the services it provides in a secure, controlled fashion.

F

False negative—False negative acknowledgments of intrusion in an intrusion detection system, which means an intrusion has occurred but the IDS discarded related events or traces as false signals.

False positive—False affirmative acknowledgment of intrusion, which means intrusion detection has incorrectly identified certain events or traces as signaling an attack or intrusion when no such attack or intrusion is underway. Thus a false positive is a false alarm.

FIPS—Federal Information Processing Standards. Created for the evaluation of cryptographic modules.

Firewall—A hardware device or software application designed to filter incoming or outgoing traffic based on predefined rules and patterns. Firewalls can filter traffic based on protocol uses, source or destination address, and port addresses and can even apply state-based rules to block unwanted activities or transactions.

G

Granularity—The relative fineness to which an access control mechanism can be adjusted.

H

Hash value—The resultant output of data generated from an encryption hash when applied to a specific set of data. If computed and passed as part of an incoming message and then recomputed upon message receipt, a hash value can be used to verify the authenticity of the received data if the two hash values match.

Hashing—A methodology used to calculate a short, secret value from a data set of any size (usually for an entire message or for individual transmission units). This secret value is recalculated independently on the receiving end and compared to the submitted value to verify the sender's identity.

Host Checker—A software component of OAC that checks your computer for compliance to the security policies that your Infranet Controller administrator specifies. Examples of compliance might be that you have the correct antivirus software version and security setting or that you have the latest operating system patch level installed.

Host Enforcer—A software component of OAC that protects your computer from attacks from other computers by allowing only the incoming and outgoing traffic that your Infranet Controller administrator specifies for your assigned role. (A *role* defines settings for your user account, such as which resources you can access).

Hotspot—A wireless access zone, could be used for public or private network access.

HTML—Hypertext Markup Language.

HTTP—Hypertext Transfer Protocol. Used by WWW servers and clients to exchange hypertext data.

I

IEEE—Abbreviation for the Institute of Electrical and Electronics Engineers.

Infranet Controller—A server that verifies your identity and your computer's compliance with security requirements before allowing you to access protected resources.

Infranet Enforcer—A Juniper Networks security device that operates with the Infranet Controller to enforce security policies. The Infranet Enforcer is deployed in front of the servers and protected resources.

Integrity—A monitoring and management system that performs integrity checks and protects systems from unauthorized modifications to data, systems, and applications files. Normally, performing such checks requires access to a prior scan or original versions of the various files involved.

Internet—The global set of networks interconnected using TCP/IP.

Internet Key Exchange—A method used in the IPsec protocol suite for public key exchange, security association parameter negotiation, identification, and authentication.

Intranet—A portion of the information technology infrastructure that belongs to and is controlled by the company in question.

Intrusion Detection System (IDS)—A sophisticated software or hardware network protection system designed to detect attacks in progress, but not prevent potential attacks from occurring.

IP—Internet Protocol. A protocol that moves packets of data from node to node. Works above layer 3 (network) of the OSI reference model.

IP address—The standard way to identify a computer connected to the Internet. Each IP address consists of 8 octets expressed as 4 numbers between 0 and 255 separated by periods. For example: 129.86.8.1.

IP Security (IPsec)—Used for encryption of TCP/IP traffic, IP Security provides security extensions to the version of TCP/IP known as Ipv4. IPsec defines mechanisms to negotiate encryption between pairs of hosts that want to communicate with one another at the IP layer and can therefore handle all host-to-host traffic between pairs of machines. In a UAC network, access to protected resources behind an Infranet Enforcer can be configured to use IPsec to encrypt data. For details about using IPsec in a UAC network, refer to the *UAC Administration Guide*.

ISDN—Integrated Services Digital Network. A network that supports transmission of voice, data, and imaged based communications in an integrated form.

ISP—Internet Service Provider.

IT—Information technology.

K

Kerberos—A trusted third party authentication protocol developed at MIT. Takes its name from the 3-headed beast that guards the gates of hell in Greek mythology. Currently a default security setting for Microsoft.

Key—A sequence of symbols that when used with a cryptographic algorithm enables encryption and decryption. The security of the cryptographic systems is dependent on the security of the key itself.

Key exchange—A technique in which a pair of keys is generated and then exchanged between 2 systems (typically and client and server) over a network connection to allow a secure connection to be established between them.

Key Pair—A public key and its corresponding private key as used in public key cryptography.

Key recovery—A mechanism for determining the key used to encrypt some data.

L

Lightweight Directory Access Protocol (LDAP)—A TCP/IP protocol that enables client systems to access directory services and related data. LDAP is defined in RFCs 1777 and 2559.

Local Area Network (LAN)—A network that consists of a single type of data link and that can reside entirely within a physically protected area.

M

Man-in-the-Middle—An attack in which a hacker attempts to intercept data in a network stream and then inserts their own data into the communications with the goal of disrupting or taking over communications.

Mandatory Access Control (MAC)—A centralized security method that does not allow users to change permissions on objects.

MD4—Message digest algorithm 4.

MD5—Message digest algorithm 5.

Message digest—A unique snapshot image of data that can be used for alter comparisons. Change a single character in the message and the message will have a different message digest. Also called a hash code.

Multifactor authentication—An authentication process that uses more than one authentication method to establish a users identity. (RSA SecurID is a multifactor authentication method with a pin and passcode required for authentication.)

N

Network—An organization of stations capable of intercommunications serviced by a single switching or processing station.

Network Address Translation (NAT)—TCP/IP protocol technology that maps internal IP addresses to one or more external IP addresses through the of a NAT server. NAT enables conversation of public IP address space by mapping private IP addresses used in an internal LAN to one or more external public IP addresses to communicate with the external world. NAT also provides address-hiding services so that NAT adds both security and simplicity to network addressing.

Network Intrusion Detection Systems—An IDS system that monitors traffic and activity on one or more network segments.

Node—A point of concentrated communications; a central point of communications.

Nonrepudiation—The condition when a receiver knows or has assurance that the sender of some data did in fact send the data, even though the sender later might want to deny ever having sent the data.

O

OSI—Open Systems Interconnect. Usually refers to the 7-layered protocol model for the exchange of information between open systems. The 7 layers in order are physical, data-link, network, transport, session, presentation, and application.

P

Packet—A sequence of data and control characters (binary digits) in a specified format that is switched/transferred as a whole.

PAP—Password Access Protocol. An authentication protocol that enables PPP peers to authenticate one another; it does not prevent unauthorized access but merely identifies the remote end.

PCMCIA card—A credit card size memory or PC card that meets the PC Card Standard developed jointly by the Personal Computer Memory Card International Association (PCMCIA) and the Japan Electronic Industry Development Association (JEIDA).

PKCS—Public Key Cryptography Standard. A set of standards for public key cryptography developed in cooperation with an informal consortium (Apple, DEC, Lotus, Microsoft, MIT, RSA, and Sun) that includes algorithm specific and algorithm independent implementation standards.

Point-to-point Tunneling Protocol (PPTP)—A TCP/IP technology used to create virtual private networks or remote access links between sites or remote access. PPTP is the work of a vendor group that includes Microsoft, 3Com, and Cooper Mountain Networks. It is generally regarded as less secure than L2TP and is used less frequently for that reason.

Policy—A broad statement of views and position. A policy states high-level intent with respect to a specific area of security and is more properly called a security policy.

Port number—A number carried in Internet transport protocols to identify which service or program is supposed to receive an incoming packet. Examples are Web services use port 80, email port 25, RADIUS uses either ports 1648-1649 or 1811-1812.

Pretty Good Privacy (PGP)—A shareware encryption technology for communication that uses both public and private encryption technology to speed up encryption without compromising security.

Private key—A piece of data generated by an asymmetric algorithm that's used by the host to encrypt data encrypted with a public key. This technique makes digital signatures and nonrepudiation possible.

Protocol—The procedures that two or more computer systems use so they can communicate with each other.

Proxy—A facility that indirectly provides some service for another facility.

Public branch exchange (PBX)—A telephone switch used on a company's or organizations premises to create a local telephone network.

Public key—A key used in public key cryptography that belongs to an individual entity and is distributed publicly. Others can use this key to encrypt data that only the key's owner can decrypt.

Public Key Infrastructure (PKI)—The framework established to issue, maintain, and revoke public key x.509 certificates.

R

RC4—Rivest cipher 4.

RC5—Rivest cipher 5.

Remediation—Remediation is the process of bringing an endpoint (computer) into compliance with an organization's security policies.

Remote Authentication Dial-in User Services (RADIUS)—An Internet protocol described in RFC 2138 used for remote access services. It conveys user authentication and configuration data between a centralized authentication server and a remote access device to permit the remote access device to authenticate requests to use its network access ports. Users present the remote access device with credentials, which are in turn passed to the RADIUS server for authentication.

Remote monitoring (RMON)—An Internet protocol that extends the Simple Network Management Protocol (SNMP) functionality to include messages about and techniques for exchanging data between network systems and devices and a centralized network management application.

Role—A role defines settings for your user account, such as which resources you can access.

Router—An Internetworking switch operating at the OSI level 3 (network layer) that connects multiple network segments and routes packets between them. Routers also split broadcast domains.

RSA—The RSA algorithm is used in cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.

S

Secure channel—A means of conveying information from one entity to another such that an adversary does not have the ability to reorder, delete, insert, or read. (Examples are SSL and IPSEC.)

Secure Hypertext Transfer Protocol (HTTPS)—An Internet protocol that encrypts individual messages used for Web communications rather than establishing a secure channel, like in SSL.

Secure Multipurpose Internet Mail Extensions (S/MIME)—An Internet protocol governed by RFC 2633 and used to secure email communications through encryption and digital signatures for authentication.

Secure Shell (SSH)—A protocol designed to support secure remote login, along with secure access to other services across an insecure network. SSH includes a secure transport layer protocol that provides server authentication, confidentiality, and integrity, along with a user authentication protocol and a connection protocol that runs on top of the user authentication protocol.

Secure Sockets Layer (SSL)—An Internet protocol originally created by Netscape Corp. that uses connection oriented, end-to-end encryption to ensure that client/server communications are confidential and meet integrity constraints. SSL operates between the HTTP application layer protocol and reliable transport layer protocol. (usually TCP)

SHA, SHA-1—Secure Hash Algorithm. SHA-1 being considered more secure.

Simple Network Management Protocol (SNMP)—A UDP based application layer Internet protocol used for network management, SNMPO is governed by RFC 2570 and 2574.

Single sign on (SSO)—The concept or process of using a single logon authority to grant users access to resources on a network regardless of what operating system or application is used to make or handle a request for access. The concept behind the term is that users need to authenticate only once but can then access any resources available on a network.

Smart card—A credit card sized device that contains an embedded chip. On this chip, varying and multiple types of data can be stored, such as a driver's license number, medical information, passwords or other authentication data, and even bank account data.

Spoofing—A technique for generating network traffic that contains a different source address from that of the machine actually generating the traffic. It foils identification of the true source.

Switch—A hardware device that manages multiple, simultaneous pairs of connections between communicating systems.

Symmetric encryption—An encryption technique in which a single encryption key is generated and used to encrypt data.

T

TACACS + —An enhanced version of Terminal Access Controller Access Control System. TACACS + is TCP based authentication and access control Internet protocol governed by RFC 1492.

TCP—Transmission Control Protocol. Verifies correct delivery of data from client to server; uses virtual circuit routing. Occupies layer 4 of the OSI reference model.

TCP/IP—Transmission Control Protocol/Internet Protocol.

Token—This is hardware or software based system for authentication wherein two or more sets of matched devices or software generate matching random passwords with a high degree of complexity.

Transport Layer Security (TLS)—An end-to-end encryption protocol originally specified in ISO standard 10736 that provides security services as part of the transport layer in a protocol stack. TLS refers to an Internet protocol defined also in RFC 2246. TLS is based on and similar to SSL v3.0, it is really misnamed because it operates at the application layer not the transport layer.

Tunnel—A secure virtual connection through the Internet.

U

Unified Access Control (UAC)—An IP-based enterprise infrastructure that coordinates network, application, and endpoint intelligence and provides the control required to support network applications, manage network use, and reduce threats.

UDP—User Datagram Protocol.

V

Validation—The process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an IS by one or more departments or agencies and their contractors.

Virtual Local Area Network (VLAN)—A software technology that enables grouping of network nodes connected to one or more network switches into a single logical network.

Virtual Private Network (VPN)—A private network built atop a public network. Hosts within the private network use encryption to talk to other hosts.

Vulnerability—A weakness in hardware or software that can be used to gain unauthorized or unwanted access to or information from a network or computer.

W

Wired Equivalent Privacy (WEP)—A security protocol used in 802.11 wireless networking, WEP is designed to provide security equivalent to that found in regular wired networks. This is achieved by using basic symmetric encryption to protect data sent over wireless connections, so that sniffing or wireless transmissions does not produce readable data and so drive-by attackers cannot access a wireless LAN without additional efforts and attacks.

WPA—Protocol enhancing the service and security offering delivered in WEP and basic 802.11. Includes support for TKIP and MIC encryption, a median step to supporting a true cryptographic algorithm such as AES.

WPA2 (or 802.11i)—Recently ratified protocol enhancing the service and security offering delivered in WEP and 802.11. Includes support for 128bit AES encryption and support for access point pre-authentication fast roaming capability.

WLAN—Wireless Local Area Network.

Wireless Transport Layer Security (WTLS)—A security level for applications based on the Wireless Application Protocol (WAP). WTLS is based on transport layer security (TLS) but has been modified to work with the low-bandwidth, high latency, and limited-processing capabilities found in many wireless networking implementations.

X

X.509 digital certificate—A digital certificate that uniquely identifies a potential communications party or participant. An X.509 certificate includes a party's name and public key, but it can also include organizations affiliation, service or access restriction, and a host of other access and security related information.

Index

Numerics

802.11	
ad-hoc mode	66
defined	64
infrastructure mode	66
802.1X	
authentication	45
overview	68

A

access point	
ad-hoc mode	44
infrastructure mode	44
introduction	66
network	66
adapter	
add network	17
disable wired connection	31
select	24
wireless	17
ad-hoc mode	
defined	66
setting	44
AES	
configuration	45
overview	67
peer-to-peer	68
use with association mode	45
anonymous name	
protocol restriction	36
set	35
any	
as a network	43
network, configuring connections	43
association mode	
defined	64
methods	44
open	44
shared	44
WPA	44
WPA2	45
asymmetric cryptography	70
authentication	
802.1X	65
profile	30
protocols	33
setting in profile properties	32
specify protocol	32
status	15

traditional networks	2
tunneled	35
user	65
wireless	64
authentication protocols	
add	33
inner	
most common	38
order of	38
multiple	33
ordering	33
remove	34
select inner	38
auto-scan list	
add	52
defined	51
modify	53
remove	53
testing	53
uses	51
view names in	53

B

beacon	
defined	26

C

certificate	
defined	70
for authentication	32
for Windows logon	32
overview	70
validate	34
validation	34
certificate authority	
chain	56
defined	70
intermediate	57
root	70
certificate chain	
defined	71
channel	
peer-to-peer	44
configuration	
adapter	17
network	41
profile	29
connection	
multiple network	25

status 15, 19
 types 25
 content dialog..... 8

D

data encryption
 purpose 64
 disconnect
 from network 27
 from wireless network..... 24
 domain
 controller
 EAP interaction 72
 login name 31
 driver software 3
 dynamic encryption keys
 reconnection effects 26

E

EAP
 as inner authentication 38
 definition 69
 EAP protocols
 outer and inner 38
 EAP-FAST 69
 overview 72
 settings for prompting..... 12
 token card 35
 tunneled method 35
 EAP-LEAP 69
 overview 72
 EAP-PEAP 69
 generic token card options 35
 inner protocols, selecting 36
 overview 72
 EAP-POTP
 password option 35
 EAP-TLS 69
 key generation 46
 overview 71
 EAP-TTLS 69
 certificate options 36
 generic token card options 35
 key generation 46
 overview 71
 settings 36
 encryption 16
 dynamic keys 46
 method, Networks panel 45
 methods 67
 methods for association mode 45
 pre-configured keys 42
 private key 70
 status 16
 Extensible Authentication Protocol 69

F

file menu options 13
 forget

password 13
 temporary trust 13

H

help menu options 14

I

identity
 server 57
 informational graphics 15
 infrastructure mode
 access point 44
 defined 66
 inner authentication 33
 defined 36
 select protocol 37
 inner authentication protocols
 add 38
 EAP 38
 remove 39
 installation
 OAC in traditional network 4
 intermediate CA
 overview 71

L

LAN, defined 63
 LEAP 72
 license key
 check expiration 15
 overview 4
 types 4
 license keys
 overview ix
 lightweight EAP 72
 login credentials
 certificate 32

M

menu bar 8
 menu options 9
 mutual authentication 34, 69
 explained 69
 server trust 65

N

network
 any network, configuring 43
 association 44
 configuration 41
 configuring
 connection to any 43
 description field 43
 encryption methods 45
 hardware requirements 3
 name
 SSID 43
 overview 43

- peer-to-peer 44
 - properties
 - add or modify 42
 - reconnecting 26
 - sample configuration 49
 - scan for available 43
 - scan for available connection 26
 - select 41
 - settings 42
 - type 44
 - WEP keys 46
 - wireless 802.11 65
 - network name
 - defined 43
- O**
- OAC
 - defined 1
 - installing 3
 - OAC Manager 7
 - exit 16
 - open mode
 - WEP 44
 - definition 67
 - options
 - preferences 10
 - security 10
- P**
- passphrases
 - hexadecimal 46
 - password
 - caution 31
 - configure in profile 31
 - forget 13
 - generic token card 35
 - POTP options 35
 - PEAP
 - overview 72
 - settings in profile properties 36
 - token card options 35
 - peer-to-peer network
 - definition 66
 - IP addresses 66
 - preshared passphrase 65
 - private key 70
 - product registration 14
 - profile
 - add 30
 - defined 29
 - modify 30
 - name 30
 - password 31
 - sample configuration 40
 - prompts
 - EAP-FAST 12
 - public key 70
- R**
- RADIUS server 69
 - reauthentication 10
 - automatic 11
 - purpose 72
 - uses 11
 - reconnecting
 - effect on encryption keys 26
 - to network 26
 - registering Odyssey 14
 - release notes x
 - requirements
 - installation 3
 - roaming
 - wireless 10
 - root certificate authority 70
- S**
- scan
 - list 52
 - secure authentication
 - methods 64
 - server
 - identity 57
 - identity formats 57
 - name 57
 - temporary trust 11
 - validate certificate 34
 - service set identifier 66
 - see SSID
 - session resumption 10
 - defined 10
 - enable 10
 - limit 10
 - settings options 9
 - shared mode
 - WEP 46
 - defined 67
 - sidebar 8
 - folders 8
 - signal power, viewing 15
 - single sign on 7
 - smart card
 - certificate 32
 - certificates 70
 - SSID
 - defined 66
 - status
 - connection 15
 - encryption 16
 - signal power 15
 - view 15
 - switch
 - 802.1X 66
- T**
- TKIP
 - implementing 45
 - overview 67

- peer-to-peer 68
- use with association mode 45
- TLS
 - overview 71
- token card
 - authentication
 - settings 37
- tools menu options 14
- trust
 - all servers 56
 - configuration
 - simple method 56
 - temporary 11
- trusted server
 - add 57
 - any 56
 - editing 58
 - entering 56
 - removing 58
- TTLS
 - overview 71
 - settings 36
- tunnel
 - encrypted 35

W

- WEP keys 42
 - any network connection 43
 - defined 67
 - dynamic 46
 - open mode 67
 - peer-to-peer 67
 - preconfigured 46, 47
 - shared mode 46
 - specify 46
 - static 46
 - use with association mode 45
- Wi-Fi network
 - scan for 26
- wired network
 - connect to 25
- Wired-Equivalent Privacy 67
- wireless
 - beacon 26
 - networks
 - scan 26
- wireless adapter
 - compatibility 21
- wireless network
 - connect to 24
 - disconnect from 24
- wireless roaming 10
- WPA 44
 - implementing 44
 - overview 67
 - passphrases 46
- WPA2 45
 - overview 67
 - passphrases 46

Juniper *your* Net™

www.juniper.net

CORPORATE HEADQUARTERS

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone 408 745 2000 or 888 JUNIPER
Fax 408 745 2100

Juniper Networks, Inc. has sales offices worldwide.

For contact information, refer to www.juniper.net.



Printed on recycled paper

OAC-TD-UG43M, Revision 01