



**Juniper Networks**  
**Odyssey Access Client for Windows Mobile**

**User Guide**

**Enterprise Edition**  
**OEM Edition**

*Release 4.5*

**Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Copyright 2002-2006 Juniper Networks, Inc. All rights reserved. Printed in USA.

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

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

# Table of Contents

	<b>About This Guide</b>	<b>i</b>
	Requirements .....	i
	Licenses .....	i
	Conventions .....	ii
	Documentation .....	iii
	Release Notes .....	iii
	Web Access .....	iii
	Contacting Customer Support .....	iii
<b>Chapter 1</b>	<b>Installing Odyssey Access Client</b>	<b>1</b>
	Installing OAC from an Installer File.....	1
	Installing OAC from a .CAB File .....	2
<b>Chapter 2</b>	<b>Network Security and Authentication</b>	<b>3</b>
	Network Security Overview.....	3
	Encryption and Association for Secure Authentication.....	4
	802.11 Wireless Networking .....	5
	Wireless Network Types .....	6
	Access Point Networks .....	6
	Peer-to-Peer Networks .....	7
	Wireless Network Names.....	7
	Wired-Equivalent Privacy (WEP).....	7
	Wi-Fi Protected Access: WPA or WPA2 and TKIP or AES.....	8
	Overview of IEEE 802.1X.....	9
	Extensible Authentication Protocol (EAP) .....	10
	Mutual Authentication .....	10
	Certificates .....	11
	EAP-TLS .....	12
	EAP-TTLS .....	12
	EAP-PEAP .....	12
	EAP-FAST .....	12
	EAP-LEAP .....	12
	Reauthentication .....	13
	Session Resumption .....	13
<b>Chapter 3</b>	<b>Using Odyssey Access Client</b>	<b>15</b>
	Opening the OAC Manager .....	15
	OAC Licenses.....	15
	OAC Manager Controls.....	15
	Making Connections and Viewing Connection Status.....	16
	Reconnecting.....	16
	Disabling Network Connections.....	16

Scanning for Wireless Networks .....	16
Viewing Connection Status Details.....	17
Signal Status.....	18
Authentication Status .....	18
Encryption Status.....	18
Connection status .....	19
Configuration Tasks .....	19
Network Connections.....	20
Setting the Network Name Description and Connection Mode .....	21
Specifying Association Modes, Authentication, and Encryption .....	21
Association Mode Options.....	22
Setting EAP Authentication Methods .....	23
Setting TTLS Inner Authentication Methods .....	24
Using EAP as Inner Authentication Protocol for TTLS .....	25
Setting Inner Authentication Protocols for EAP-PEAP .....	25
Adding an EAP-PEAP Inner Protocol .....	25
Reordering EAP-PEAP Inner Protocols .....	26
Removing an EAP-PEAP inner protocol.....	26
Specifying Credentials .....	26
Using an Anonymous Name.....	27
Setting EAP-GenericTokenCard Protocol Options.....	28
Selecting a Certificate for Certificate Credentials (EAP-TLS) .....	28
Automatic Certificate Selection for TLS .....	29
Setting an Ad-hoc Connection Channel Number .....	29
Using WEP Encryption .....	30
Specifying WEP Keys.....	30
Completing a Network Configuration .....	30
Setting Server Certificates and Trust .....	31
Using Simple Trust Configuration .....	31
Managing Untrusted Servers.....	32
Configuring SIM card Features .....	33
Setting Up EAP Authentication Methods .....	33
Configuring SIM card ID and PIN Options.....	34
SIM Card Settings: for EAP-SIM Identity .....	34
SIM Card PIN Options .....	35
Menus .....	35
Settings Menu.....	36
Security Settings .....	36
EAP-FAST Settings.....	38
Commands Menu .....	39
About Reconnecting and Reauthenticating.....	39
Using the Forget Temporary Trust Setting.....	40
Using the Forget Password Setting .....	40
Tools Menu.....	40
Importing a User Certificate .....	40
Using Certificate Enroller .....	41
Using SIM Card PIN Manager .....	43
Help Menu.....	44
License Keys .....	44
OAC Deployment Using Client Scripts (EE Only) .....	45
<b>Index.....</b>	<b>46</b>

# About This Guide

Thank you for selecting Odyssey Access Client (OAC).

Odyssey Access Client lets you connect your mobile device to a wireless network easily and securely. Odyssey Access Client allows you to accomplish the following:

- Connect to wireless network access points.
- Connect to other wireless devices in a peer-to-peer fashion.
- Create multiple network configurations to connect to different networks possibly using different credentials and/or authentication methods.
- Use 802.1X to authenticate to the network.
- Use a wide variety of authentication methods, including powerful methods such as EAP-TTLS, EAP-PEAP, and EAP-TLS, to keep your credentials secure.

## Requirements

---

To use wireless capabilities, your mobile device must be equipped with a wireless adapter card and a NIC driver that is 802.1X compliant if you require 802.1X authentication.

The README.TXT file included with this software lists some of devices that work with Odyssey Access Client.

The most recently updated list of compatible devices can be found on the Odyssey Access Client User Page located on the Juniper Networks, Inc. Web site.

## Licenses

---

You must enter a license key as part of the installation process of Odyssey Access Client. You can also enter the license key after you install the product.

Some Odyssey Access Client features are licensed separately. Depending on which license you have purchased, some feature sets of OAC may not apply. Additionally, some portions of the user interface may be disabled and the appearance of dialogs may vary, based on your license.



Some OAC features are supported only in the Enterprise Edition. Those restrictions are indicated clearly in the documentation wherever they apply.

See “License Keys” on page 44.

## Conventions

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

**Table 1: Notice icons**

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates that you may risk losing data or damaging your hardware.
	Warning	Alerts you to the risk of personal injury.

**Table 2: Text conventions (except for command syntax)**

Convention	Description	Examples
<b>Bold typeface</b>	Indicates buttons, field names, dialog box names, and other user interface elements.	Use the <b>Scheduling</b> and <b>Appointment</b> tabs to schedule a meeting.
Plain sans serif typeface	Represents: <ul style="list-style-type: none"> <li>■ Code, commands, and keywords</li> <li>■ URLs, file names, and directories</li> </ul>	Examples: <ul style="list-style-type: none"> <li>■ Code: certAttr.OU = 'Retail Products Group'</li> <li>■ URL: Download the JRE application from: <a href="http://java.sun.com/j2se/">http://java.sun.com/j2se/</a></li> </ul>
<i>Italics</i>	Identifies: <ul style="list-style-type: none"> <li>■ Terms defined in text</li> <li>■ Variable elements</li> <li>■ Book names</li> </ul>	Examples: <ul style="list-style-type: none"> <li>■ Defined term: An <i>RDP client</i> is a Windows component that enables a connection between a Windows server and a user's machine.</li> <li>■ Variable element: Use settings in the <b>Users &gt; Roles &gt; Select Role &gt; Terminal Services</b> page to create a terminal emulation session.</li> <li>■ Book name: See the <i>IVE Supported Platforms</i> document.</li> </ul>

## Documentation

---

### Release Notes

Release notes are included with the product software and are available on the Web.

In the *Release Notes*, you can find 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 the documentation on the Web, go to:

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

### Contacting Customer Support

---

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



## Chapter 1

# Installing Odyssey Access Client

You can install Odyssey Access Client (OAC) in the following ways:

- Installing OAC from an Installer File
- Installing OAC from a .CAB File.



**NOTE:** You may be required to soft-reset your mobile device after installing Odyssey Access Client.

---

## Installing OAC from an Installer File

To install OAC onto your local machine from an installer file, follow these steps:

1. Connect your device to your computer using Microsoft ActiveSync.
2. Run the installation program **Odyssey Access Client for Windows Mobile.exe** provided on your CD or via download.
3. Proceed through the installation wizard process by providing the required information requested on each screen. In particular, enter a valid license key or select one of the following license key options:
  - Use 30-day license
  - Use existing license
4. Once all the required information is entered, click **Install** to begin the installation process.

When the installation process completes, Odyssey Access Client is installed on your device. You may be required to address some tasks on your device.



**NOTE:** The installer will not proceed unless your mobile device is connected through ActiveSync.

---

---

## Installing OAC from a .CAB File

You can install OAC from a .CAB file included on the CD. In addition, if you are a network or product administrator, you can create configuration scripts in advance of running the .CAB file so that OAC is ready to use on installation. To do so, follow these steps:

1. Create a file called **OdyLicense.txt**, whose sole contents is your OAC license key.
2. Save this file to the top level (root) directory of your device.
3. For network administrators: Use the Enterprise Edition of OAC on your desktop computer to access Odyssey Access Client Administrator to create configuration scripts (auto-scripts) that specify the device network connection configuration. See the *OAC Administration Guide* for more information on creating auto-scripts.

To have scripts applied automatically to the device at installation time, be sure to save any script you create for the device in the top-level (root) directory of your device.

4. Copy the **ODCeClientPPC.ARMV4.CAB** file from the product CD (or from your computer) to your device. Note the following:
  - The name of the .CAB file you must use depends on your device processor, so you may need to choose a different .CAB file.
  - You can copy the .CAB file to your device when it is connected to your computer via ActiveSync, or by some other means.
5. Run the .CAB file on your device to install it.



**NOTE:** Scripts can be applied to user devices, after OAC is installed on the device. In order for scripts to be applied automatically to the device, any script you create for the device must be placed in the **/newScripts** directory that is located under the product install directory on the device.

**Client Scripts are supported only in the OAC Enterprise Edition.**

---

## Chapter 2

# Network Security and Authentication

This chapter discusses the concepts and terminology behind wireless and wired networking that underlie the design of OAC. Read this material to learn about networking choices that allow you to use OAC to best advantage and to learn how to maximize the security of your connections over wireless LANs.

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

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

- “Network Security Overview” on page 3
  - “Encryption and Association for Secure Authentication” on page 4
- “802.11 Wireless Networking” on page 5
  - “Wireless Network Types” on page 6
  - “Wireless Network Names” on page 7
  - “Wired-Equivalent Privacy (WEP)” on page 7
  - “Wi-Fi Protected Access: WPA or WPA2 and TKIP or AES” on page 8
- “Overview of IEEE 802.1X” on page 9
  - “Extensible Authentication Protocol (EAP)” on page 10
  - “Reauthentication” on page 13
  - “Session Resumption” on page 13

---

## Network Security Overview

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

With wireless networks, physical access to the network requires only device with a wireless card and a comfortable spot in the parking lot outside of the building or in the office next door.

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

- The IEEE (Institute of Electrical and Electronic Engineers) standards for wireless LANs known as 802.11. These standards include 802.11a, 802.11b, and 802.11i.
- The IEEE 802.11i enhancements to 802.11 were introduced to overcome some of the security weaknesses of 802.11.
- Wi-Fi Alliance's WPA2 (with AES encryption) adheres to the strong 802.11i enhancements.
- Wi-Fi Alliance's WPA (with AES or TKIP encryption) complies with a subset of 802.11i and, although not as strong as WPA2, addresses some of the security weakness of 802.11 as well.
- The IEEE has also created the 802.1X standard to supplement the 802.11 standards with secure server-based wireless authentication.

The following features can make wireless networks secure:

- A user must be authenticated by the network before he or she is allowed access, to make the network safe from intruders. For information on configuring authentication, see "Specifying Association Modes, Authentication, and Encryption" on page 21.
- The wireless connection between a PC and access point can be encrypted, so eavesdroppers cannot access data that is supposed to be private.
- The network must be authenticated (trusted) by the user before the user allows his or her credentials to be released to the network to make a network connection. This prevents a wireless device that may be posing as a legitimate network from impersonating the network and gaining access to the user's PC. For information on configuring authentication, see "Using Simple Trust Configuration" on page 31.
- The mutual authentication between user and network must be cryptographically protected.

### ***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 client must have authenticated access to the network. The following list briefly defines terminology necessary to understand association, data encryption, and authentication:

- Association is the method by which a client first establishes a relationship with an access point.

- Data encryption is used to secure data that is exchanged between a client device and an access point (or another client device).
- Each data encryption algorithm requires encryption keys. Encryption keys may also be used for access point association.
- Once a wireless client has associated with an access point, the user of that client device may be authenticated to the network. Authentication is used to secure the relationship between a user of a wireless client device and an authentication server. For example, wireless network authentication that is based on the 802.1X standard can make use of cryptographically strong (and dynamically generated) encryption keys.

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

- Preconfigured secrets, called WEP keys. These keys are intended to encrypt the data transferred between the client and the access point and can be used to keep unauthorized users off the wireless network, as well as to encrypt the data of legitimate users. See “Wired-Equivalent Privacy (WEP)” on page 7 for a description of WEP-based encryption that complies with 802.11 standards.
- Pre-shared passphrases used to generate keys for WPA or WPA2 association. Pre-shared passphrases allow you to configure a simple phrase that is used to generate cryptographically strong encryption keys to be used with AES or TKIP encryption. AES and TKIP also periodically change the encryption keys in use. The generated keys keep unauthorized users off the wireless network and encrypt the data of legitimate users. See “Wi-Fi Protected Access: WPA or WPA2 and TKIP or AES” on page 8 for a description of AES or TKIP encryption methods that enhance the 802.11 standards.
- Authentication using an 802.1X-based protocol. This method uses a variety of underlying authentication protocols to control network access. The strongest of these protocols provides cryptographically protected mutual authentication of the user and the network. In addition, keys that are used to encrypt wireless data are generated dynamically with these strong protocols. 802.1X-based authentication can use WEP, AES, or TKIP encryption, depending on network hardware/firmware. See 802.11 Wireless Networking for information on authentication using 802.1X. See “Wi-Fi Protected Access: WPA or WPA2 and TKIP or AES” on page 8 for a description of some of the strongest available association and encryption modes. The 802.1X methods are also viable for wired 802.1X-based network connections.

---

## 802.11 Wireless Networking

OAC 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.

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

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.

The following attributes of the 802.11 standard are described here:

- Wireless Network Types
- Wireless Network Names
- Wired-Equivalent Privacy (WEP)

See also the following topics:

- “Wi-Fi Protected Access: WPA or WPA2 and TKIP or AES” on page 8 for information on enhancements to 802.11 association and encryption.
- “802.11 Wireless Networking” on page 5 for information on secure wireless authentication.

## **Wireless Network Types**

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

### **Access Point Networks**

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

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

A single network can make use of many different access points. 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.

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

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

When you connect to a network via an access point, you are using the 802.11 *infrastructure mode*. See “Setting the Network Name Description and Connection Mode” on page 21 for information on configuring infrastructure network connections.

## Peer-to-Peer Networks

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

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

The 802.11 standard refers to peer-to-peer of network connectivity as *ad-hoc mode*. See “Setting the Network Name Description and Connection Mode” on page 21 and “Specifying Association Modes, Authentication, and Encryption” on page 21 for information on configuring ad-hoc network connections.

## Wireless Network Names

Each wireless network has a name (SSID). You can select the wireless network to which you want to connect by specifying its name.

Network names allow different wireless networks in the same vicinity to coexist without intruding on each other. For example, the company next door to yours may also use wireless networking. Network names allow you to distinguish access points located within your enterprise wireless network from access points that are not within your corporate LAN.

Network names do not, in themselves, offer any security features and cannot prevent you from connecting to a phony network. However, 802.11 does allow for you to use a shared secret for access point association. See “Wired-Equivalent Privacy (WEP)” on page 7 and “Wi-Fi Protected Access: WPA or WPA2 and TKIP or AES” on page 8. Additionally, using secure 802.1X-based authentication methods, your company can prevent intruders from connecting to the network and you can avoid associating with phony networks. See “802.11 Wireless Networking” on page 5 for more information.

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

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

## Wired-Equivalent Privacy (WEP)

You can use WEP (Wired-Equivalent Privacy) to provide security during association with access points (or other clients) and 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, both 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 same preconfigured WEP keys assigned to the access point.

*Open*: Use this mode for WEP-based data encryption (or no with data encryption) when the access point does not require that you preconfigure a WEP key for association. See the following topics:

- “Setting the Network Name Description and Connection Mode” on page 21 for directions on selecting a connection mode (infrastructure or ad-hoc).
- “Specifying Association Modes, Authentication, and Encryption” on page 21 for directions for selecting WEP encryption when using the shared or open association mode
- “Specifying WEP Keys” on page 30 to use static WEP keys with OAC.



**NOTE:** You can also use preconfigured keys for WEP data encryption that is used for securing 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: WPA or WPA2 and TKIP or AES**

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

- Improved data encryption via TKIP (temporal key integrity protocol) for WPA. TKIP provides stronger encryption than WEP.
- Improved data encryption for WPA2 via AES. AES provides stronger encryption than WEP or TKIP.
- WPA and WPA2 allow for keys to be generated for TKIP (or AES) encryption from a pre-shared passphrase. Although your passphrase may be simple, these encryption methods can generate cryptographically strong encryption keys from a simple passphrase. Consequently, these encryption methods are stronger than WEP encryption based on preconfigured WEP keys. If you configure a passphrase for key generation for your access points, you cannot use 802.1X based authentication and you must configure the same passphrase in OAC.

When the access point hardware in your network requires that you associate via the enhanced WPA or the stronger WPA2 association mode, you can configure OAC to associate in that mode. If the hardware is configured for TKIP or the stronger AES encryption, you can configure OAC for either of these enhanced data encryption methods as well. You should configure your access points and clients

for network connections that use the strongest association and encryption methods that are supported by your network access points.



**NOTE:** With WPA2 (or WPA) enabled access points, you can obtain the stronger network security when you use dynamic encryption key generation and 802.1X-based authentication. See “Extensible Authentication Protocol (EAP)” on page 10 for more information.

See the following topics:

- “Overview of IEEE 802.1X” on page 9 to use WPA2 or WPA association mode with OAC
- “Setting the Network Name Description and Connection Mode” on page 21 to configure a passphrase that is used in encryption key generation.



**NOTE:** You can also 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.

## Overview of IEEE 802.1X

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

The WEP protocol has various shortcomings when preconfigured keys are in use. Preconfigured WEP keys not only contribute to administrative overhead, but using them poses security weaknesses.

Although the encryption methods calculated from keys generated from pre-shared passphrases are stronger than WEP encryption calculated from static WEP keys, the use and distribution of passphrases can also pose administrative and security problems. The use of 802.1X protocols in wireless networks alleviates these problems because keys can be derived dynamically during authentication.

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

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

See the following topics for details:

- Extensible Authentication Protocol (EAP)

- Session Resumption
- Reauthentication

### **Extensible Authentication Protocol (EAP)**

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

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

The newer EAP protocols have an additional advantage. They can dynamically generate the keys that are used to encrypt data between the client and the access point using WEP, TKIP, or AES. 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 pre-shared passphrases.

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

- EAP-TTLS
- EAP-PEAP
- EAP-TLS
- EAP-FAST
- EAP-LEAP
- EAP-POTP

### **Mutual Authentication**

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

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 some access point that is pretending to be your network.

EAP-TTLS, EAP-PEAP, and EAP-TLS all let you authenticate the network by validating the certificate of the authentication server. If the certificate identifies a server that you trust and if the authentication server can prove that it is the owner of that certificate, then you can safely connect to this network. These are the

strongest authentication methods available and, consequently, it is highly recommended that you use only 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* and a *private key*. You keep your private key secret, but reveal your public key to the whole world. Anyone can encrypt data using your public key with the certain knowledge that only your private key can decrypt it. 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.

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

Each certificate has an expiration date. 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 and a root certificate.

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

### **EAP-TLS**

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

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

### **EAP-TTLS**

EAP-TTLS is a protocol devised by Funk Software and Certicom. It is designed to provide authentication that is cryptographically as strong as EAP-TLS, while not requiring that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed using a password or other credentials. The credentials are transported in a securely encrypted “tunnel” that is established using the server certificate. Within the EAP-TTLS tunnel, you can employ any of a number of inner authentication protocols. See “Setting TTLS Inner Authentication Methods” on page 24 for more information on configuring inner protocols for tunneled authentication.

With EAP-TTLS, it is not necessary to create a new infrastructure of user certificates. User authentication can be performed against the same security database that is already in use on the corporate LAN. For example, Windows Active Directory, or an SQL or LDAP database may be used.

### **EAP-PEAP**

EAP-PEAP is comparable to EAP-TTLS, both in its method of operation and its security. However, EAP-PEAP is not as flexible as EAP-TTLS and it does not support the range of inside-the-tunnel authentication methods that EAP-TTLS supports. Commercial implementations of this protocol that started appearing at the beginning of 2003 were beset with interoperability problems. Nevertheless, this protocol is supported by Microsoft and Cisco and is in widespread use. EAP-PEAP is a suitable protocol for performing secure authentication against Windows domains and directory services. See “Setting Inner Authentication Protocols for EAP-PEAP” on page 25 for more information on configuring inner protocols for EAP-PEAP authentication.

### **EAP-FAST**

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

### **EAP-LEAP**

EAP-LEAP (Lightweight EAP, also known as EAP-Cisco Wireless) is a protocol developed by Cisco to allow users to be authenticated using their Windows credentials, without the use of certificates. The data exchange in EAP-LEAP is

fundamentally similar to the exchange that occurs when a user logs in to a Windows Domain Controller.

EAP-LEAP is very convenient because it is Windows compatible. However, because EAP-LEAP does not use 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 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 PC and access point. The access point may use these shared keys to refresh the keys used to encrypt data. By frequently refreshing keys, you can thwart cryptographic attacks.

See “Security Settings” on page 36 for more information on configuring this feature.

## **Session Resumption**

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

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

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

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

See “Security Settings” on page 36 for more information on using this feature.

---



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

---

## Chapter 3

# Using Odyssey Access Client

Odyssey Access Client (OAC) provides authenticated network access from a Windows Mobile or Windows CE device. To use OAC, it must be installed on the mobile device. See “Installing Odyssey Access Client” on page 1.

---

## Opening the OAC Manager

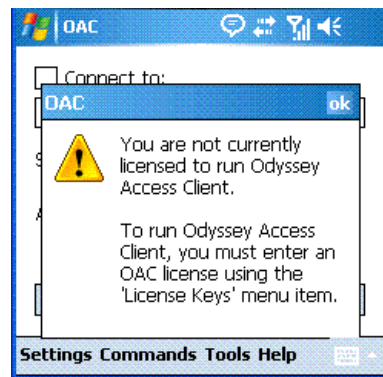
To open OAC Manager, the user interface for managing OAC settings and network connections:

Go to **Start > Programs > OAC** and tap the OAC icon.

### OAC Licenses

If you launch OAC and do not yet have a license, a pop-up message (Figure 1) instructs you to obtain a license first.

**Figure 1: Prompt for a Valid License**



To obtain a license, contact Juniper Networks, Inc. at <http://juniper.net/howtobuy>.

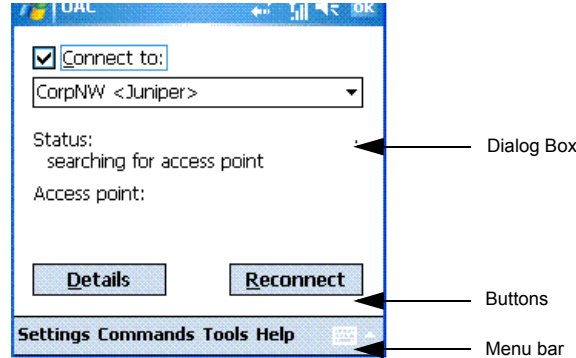
---

## OAC Manager Controls

The **Connect to** dialog (Figure 2) is the main control dialog of Odyssey Access Client that appears when you start it up. Use this dialog to control your wireless network connection and to view your current connection status from this dialog.

The dialog box has the following sections:

**Figure 2: Layout of the OAC Management Screen**



## Making Connections and Viewing Connection Status

If you already have a network configured on Odyssey Access Client, you must be within range of an access point to initiate network authentication from the main connection dialog. From there, select a network from the drop-down list and select the **Connect to** box on the main dialog of Odyssey Access Client.

The dialog box (see Figure 2 on page 16) gives you the basic information about your connection:

- **Status**—Describes the state of your current connection.
- **Access point**—Shows the identification of the access point to which you are currently connected.

## Reconnecting

To reconnect to a network, tap **Reconnect**. This re-establishes a connection with the current network using the access point with the strongest signal and the correct SSID.

## Disabling Network Connections

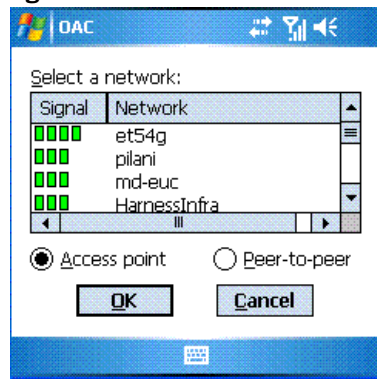
To disable your current network connection:

1. Open the OAC management interface.
2. Select **Settings > Exit** or deselect **Connect to**.

## Scanning for Wireless Networks

OAC can scan for wireless networks in your current vicinity and display them so that you can select the one you want.

To scan for networks, select **Commands > Scan**. The Scan for Wireless Networks dialog (Figure 3) appears.

**Figure 3: Scan for Wireless Networks Dialog**

The scan list shows the infrastructure networks in your vicinity by default. To change the display to show ad-hoc networks within your vicinity, select **Ad-hoc** and all potential peer-to-peer wireless clients are displayed.

To connect to a network in the scan list:

1. Select one of the networks (or peer-to-peer clients).
2. Tap **OK**.

A configuration wizard appears so that you can specify the network settings. See “Network Connections” on page 20 for more information on network connection configuration.

Tap **Cancel** to have Odyssey Access Client return to the previous dialog without disrupting your current connection.

### Viewing Connection Status Details

Select **Details** on the main connection dialog to view detailed status about your current connection. The View Connection Status dialog shown in Figure 4 appears.

**Figure 4: View Connection Status**

Three tabs allow you to view different aspects of your connection:

- Signal Status

- Authentication Status
- Encryption Status

### **Signal Status**

The **Signal** tab displays one of the following signal status comments that indicate the strength of the radio signal used by your wireless connection:

- Strong
- Moderate
- Weak
- Faint
- Signal power not available

The Signal tab also indicates the signal power measured in decibels.

### **Authentication Status**

The **Authentication** tab describes the state of your connection and whether or not you are authenticated. The following is the list of possible authentication status comments:

- No connection to authenticate
- Not connected, due to failed authentication
- Connected, but authentication not in use
- Connected and authenticated
- EAP type
- Elapsed time
- Cipher suite being used

### **Encryption Status**

The **Encryption** tab displays whether or not encryption keys are in use. There are three possible encryption status comments:

- Not connected
- Data is encrypted using static keys
- Data is encrypted using dynamic keys (802.1X)

The Encryption tab also displays the types of keys in use and their lengths, measured in bits.



**NOTE:** Odyssey Access Client only reports the *length* of the secret part of the encryption key (either 40 or 104 bits).

### Connection status

The connection status button (with the Odyssey Access Client “sailing boat” icon) shows the state of your connection and whether or not you are authenticated.



(outline) Not connected



(red) Not connected, due to failed authentication



(black) Connected, but authentication not in use



(blue) Connected and authenticated

## Configuration Tasks

The following topics describe the configuration tasks and dialogs that may appear during the process of configuring OAC.

- “Setting the Network Name Description and Connection Mode” on page 21
- “Specifying Association Modes, Authentication, and Encryption” on page 21
- “Setting EAP Authentication Methods” on page 23
- “Using an Anonymous Name” on page 27
- “Setting EAP-GenericTokenCard Protocol Options” on page 28
- “Setting TTLS Inner Authentication Methods” on page 24
- “Using EAP as Inner Authentication Protocol for TTLS” on page 25
- “Setting Inner Authentication Protocols for EAP-PEAP” on page 25
- “Specifying Credentials” on page 26
- “Selecting a Certificate for Certificate Credentials (EAP-TLS)” on page 28
- “Setting an Ad-hoc Connection Channel Number” on page 29
- “Using WEP Encryption” on page 30
- “Specifying WEP Keys” on page 30
- “Completing a Network Configuration” on page 30

## Network Connections

OAC retains a list of the network connection configurations you have specified. When you configure a network connection, however, the wizard presents only the dialogs that are necessary to complete the configuration.

These configurations include information such as the following:

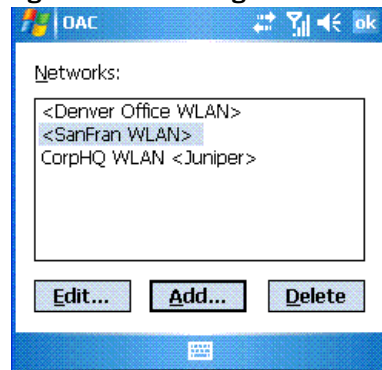
- Network names (SSIDs)
- Optional network descriptions
- Authentication protocols
- Access point association mode and encryption method
- Credentials (authentication identity)



**NOTE:** If you plan to use any authentication methods that require server certificates (such as EAP-TLS) you must first install a server certificate before you configure a network connection. See “Setting Server Certificates and Trust” on page 31. If you plan to use EAP-TLS, you must also install a user certificate on your device before configuring the network connection. See “Importing a User Certificate” on page 40 and “Using Certificate Enroller” on page 41.

Select **Settings > Configure** to view a list of networks (Figure 5) that you have already configured. The names of these network connection configurations are also listed on the drop-down list of the **Connect to** dialog.

**Figure 5: View Configured Networks Dialog**



You can perform the following tasks:

- Edit a selected network connection configuration.
- Create a new network connection configuration and add it to the list.
- Remove a selected network connection configuration from the list.

A configuration wizard guides you through the process of adding a new network definition or editing settings for a pre-existing network definition.

### Setting the Network Name Description and Connection Mode

The first setting that you must provide to configure a network is the name of the network—the network SSID (see Figure 6).

**Figure 6: Network Name Dialog**

To find a network that is currently within range, tap **Scan**. This allows you to select from the list of local wireless networks that OAC can detect.

To connect to any wireless network within range, check **Any**.

You can supply an optional description for this network connection configuration. A network configuration that includes a network description displays the description next to the network name on the list of networks.

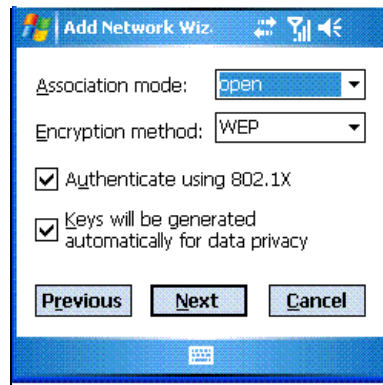
You must also specify the type of connection:

- **Ad-hoc** (peer-to-peer)
- **Infrastructure** (a wireless network that communicates via access points)

When you have made the settings, tap **Next**.

### Specifying Association Modes, Authentication, and Encryption

There are several options for setting an association mode and data encryption method. Use the Association Mode dialog (Figure 7) to provide this information.

**Figure 7: Association Mode Dialog**

### Association Mode Options

Association mode options are:

- **Open**—Select this for connecting to a network through an access point that allows open association as defined by 802.11. Choose this mode if you are not required to select shared mode or WPA
- **Shared**—Select this for connecting to a network through an access point that requires at least one preconfigured WEP key for association
- **WPA**—Select this for connecting to an access point that implements WPA (Wi-Fi Protected Access)
- **WPA2**—Select this for connecting to an access point that implements WPA2 (802.11i, Wi-Fi Protected Access 2)

You have the following association mode-dependent encryption method options:

- **None**—Select this if no encryption will be used. This option is only available to you when you configure access point association in open mode.
- **WEP**—Select this for WEP keys with data encryption. This option is available for open or shared association and is required when you associate in shared mode. When you use WEP encryption, you must fill in at least one preconfigured WEP key, unless you authenticate using a 802.1X and check **Keys will be generated automatically for data privacy**. You must choose WEP when the access points in your network require shared mode association with WEP keys, or when your access points require WEP encryption.
- **TKIP**—Select this for a temporal key integrity protocol. Choose this option when the access points in your network require WPA association and are configured for TKIP.
- **AES**—Select this for 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.

Depending on your association and encryption selections, you can tap one or both of the following:

- **Authenticate using 802.1X**—Select this for using the secure 802.1X authentication methods
- **Keys will be generated automatically for data privacy**—Select this for generating data encryption keys automatically, rather than specifying static keys. If you do not check this option and you associate in open mode with WEP encryption, then you must specify WEP keys for data encryption.

If you do not use 802.1X authentication and you select WPA2 or WPA as your association mode, then you can enter a passphrase under **Pre-shared key (WPA or WPA2)** for authentication.

Use this option if you are required to enter a passphrase to associate with your access point. This option prevents you from using 802.1X authentication.




---

**NOTE:** If you associate in WPA or WPA2 mode and if you select **Authenticate using 802.1X**, this choice provides for automatic data encryption key generation by default and allows you to use the strong 802.1X EAP authentication methods. Do not use this option with WPA or WPA2 if you are required to enter a passphrase to associate with your access point.

---

When have set up all of the authentication settings, tap **Next**.

The next dialog that appears depends on the previous configuration settings you have made. The following dialogs may appear:

- Setting EAP Authentication Methods
- Setting TTLS Inner Authentication Methods
- Specifying Credentials
- Selecting a Certificate for Certificate Credentials (EAP-TLS)
- Setting an Ad-hoc Connection Channel Number
- Using WEP Encryption
- Specifying WEP Keys
- Completing a Network Configuration

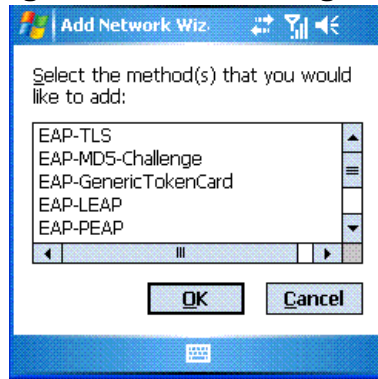
---

## Setting EAP Authentication Methods

Use the EAP Methods dialog (Figure 8) to specify and set up the order of the EAP authentication methods to use for authentication. EAP authentication uses an outer and an inner authentication protocol.

The outer authentication protocol sets up an encrypted tunnel so that the actual authentication process is secure. The inner protocol supports the actual authentication activity during which a user provides authentication credentials.

**Figure 8: EAP Methods Dialog**



The EAP authentication methods that you have currently enabled appear in order of preference.

You can perform the following actions:

- Tap **Add** to add an EAP method to your current list.  
Select the methods to add and click **OK** to close this dialog.
- Tap **Remove** to remove the currently selected EAP method from the list.

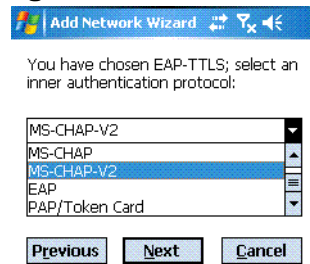
When a server attempts to authenticate your credentials, OAC responds with each of the authentication methods in the order in which they appear in this list:

- Tap the up arrow to move a selected EAP method up in the list.
- Tap the down arrow to move a selected EAP method down in the list.
- Optionally, you can check **Validate server certificate** to validate the server certificate you have installed for authentication when you authenticate using EAP-TTLS or EAP-PEAP. See “Using Simple Trust Configuration” on page 31 for information on how to install this certificate.

When you have completed the EAP settings, tap **Next**.

### **Setting TTLS Inner Authentication Methods**

If you select EAP-TTLS as one of your authentication methods, an encrypted tunnel opens between your device and the authentication server. The tunnel provides a secure means of passing credentials. Once the tunnel is established, the server attempts to authenticate you using a traditional EAP authentication method, the inner authentication method.

**Figure 9: Select EAP-TTLS Inner Authentication Dialog**

Choose the inner authentication method you prefer from the list (see Figure 9).

When you have made the settings, tap **Next**.

### Using EAP as Inner Authentication Protocol for TTLS

If you select EAP as the inner authentication method for EAP-TTLS, you must also specify the EAP secondary protocols to use for inner authentication.

The inner EAP authentication methods you select appear in order of preference.

You can perform the following tasks:

- Add an EAP method to your current list by tapping **Add**.
- Remove the currently selected EAP method from the list by tapping **Remove**.
- Move the currently selected EAP method up or down in the list by using the up or down arrow keys.

When you have made the settings, tap **Next**.

### Setting Inner Authentication Protocols for EAP-PEAP

When you select EAP-PEAP as an authentication protocol, you must select an inner protocol that is used to negotiate authentication using EAP-PEAP.

The procedure and screens for setting up inner authentication for PEAP are almost identical to those for TTLS.



**NOTE:** If you select TLS as an inner authentication protocol for PEAP, the configuration Wizard prompts you for the name of a valid client certificate.

### Adding an EAP-PEAP Inner Protocol

To add an inner EAP protocol for PEAP:

1. Click **Add**.

2. Select the inner authentication methods you require from the list.
3. Tap **OK**.

The selected methods are added to the list of EAP-PEAP inner protocols.

### Reordering EAP-PEAP Inner Protocols

You can prioritize the inner protocols that are used when you negotiate authentication with EAP-PEAP. You can order the protocols from most preferred to least preferred.

To reorder the list of EAP-PEAP inner protocols:

1. Select a protocol.
2. Tap the up or down arrow until you place the authentication protocol where you want it on the list.

### Removing an EAP-PEAP inner protocol

Select any protocols you want to remove from the list and tap **Remove**.

## Specifying Credentials

This dialog shown in Figure 10 allows you to specify your identity (credentials) for authentication. The wizard prompts you for the credentials that are required for the authentication methods you selected.

**Figure 10: Setting Username Credentials**

For all authentication methods, you must supply a **Login name** that identifies you during authentication.



**NOTE:** User name login prompts are supported only in the Enterprise Edition of Odyssey Access Client for Windows Mobile.

The following authentication methods require tokens or passwords:

- EAP-TTLS (with specific inner authentication protocols)
- EAP-PEAP (with specific inner authentication protocols)

- EAP-FAST
- EAP-LEAP
- MD5-Challenge

### ***Authentication with a Password***

Check **Permit login using password** if you plan to enable authentication methods that require your password for authentication.

Once you enable password authentication, you can use either of the following methods for providing password credentials at authentication time:

- **Stored password:** For this option, enter your password in the field provided. You can optionally check **Unmask** to view the characters in your password on the dialog as you enter them.
- **Prompt for password each time you establish a connection:** For this option, tap **Prompt for password**.

### ***Authentication with a Certificate***

You can choose to identify yourself through a certificate. User certificate credentials for authentication apply only if you are using the EAP-TLS protocol. Check **Permit login using my certificate** to do so.

If you have a valid license for using SIM card features and if you selected EAP-SIM and/or EAP-AKA as one of your authentication methods, you can check **Permit login using my SIM card** to enable SIM card features. It is recommended that you uncheck **Permit login using password** to use SIM card authentication.

### **Using an Anonymous Name**

If you use EAP-TTLS, EAP-FAST, or EAP-PEAP for authentication, you can hide your identity using an anonymous name in your credentials. These authentication methods establish an encrypted tunnel between your device and the server.

As a general rule, set **Anonymous name** to **anonymous**, the default value. If your network has different requirements, your network administrator must tell you how to configure this field differently:

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

When you have completed this setting, tap **Next**.

### Setting EAP-GenericTokenCard Protocol Options

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

- If you use EAP-FAST as an outer authentication method
- If you choose EAP-GenericTokenCard as the inner protocol for EAP-PEAP

You have two options when EAP-GenericTokenCard is an inner protocol (see Figure 11):

- Tap **My password** to use your password for authentication.
- Tap **Prompt for token information** to use your token card information for authentication.

**Figure 11: EAP-GenericTokenCard Credentials Dialog**



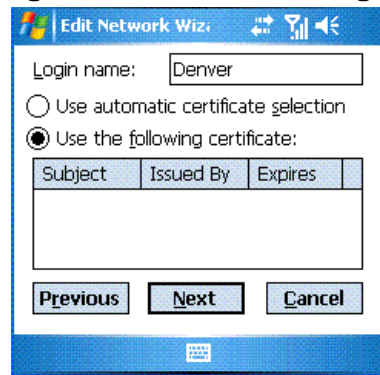
When you have specified the settings, tap **Next**.

### Selecting a Certificate for Certificate Credentials (EAP-TLS)

If you choose to provide certificate credentials for authentication, you must select a certificate from any listed on the **Add Certificate** dialog (Figure 12) or use automatic certificate selection. You have access to this dialog only if you choose to allow certificate credentials with this connection. This dialog contains any certificates that you have inserted directly into your device personal certificate store.

If you do not have any user certificates but you do have a **.pfx** certificate file (along with the RSA-type password), you can use **Tools > Importing a User Certificate** to install this certificate on your device for use with OAC.

Alternatively, you can request a certificate from your network certificate granting authority using **Tools > Using Certificate Enroller**.

**Figure 12: Add Certificate Dialog**

After you select a certificate, tap **Next**.



**NOTE:** This is an advanced feature. See your network administrator for information on which certificate to select if you require one. See “Importing a User Certificate” on page 40 for information on importing certificates to your device.

### Automatic Certificate Selection for TLS

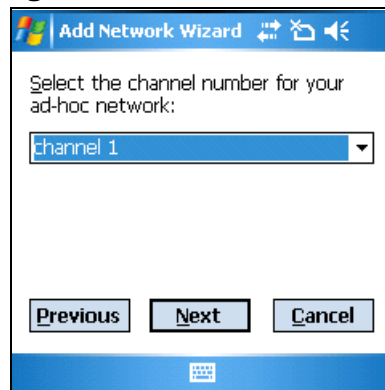
If you have TLS selected as an authentication method and if there is a single, valid client certificate, OAC recognizes the certificate and does not prompt for one.

If there is a single certificate configured that has expired, OAC searches for a new certificate with the same common name and then replaces the certificate and updates the configuration without prompting.

If there is currently no valid client certificate, or if there is more than one valid client certificate, OAC prompts for you to select one.

### Setting an Ad-hoc Connection Channel Number

If you use an ad-hoc (peer-to-peer connection), you must select one of the channels (1 through 11) over which the devices communicate when you configure the network connection (see Figure 13). You can also select the default channel.

**Figure 13: Ad-Hoc Channel Number Dialog**

When you have made the settings, tap **Next**.

### Using WEP Encryption

When you make a peer-to-peer connection, you can choose to enter WEP keys for data encryption. Check **Use static WEP keys to encrypt data** if you want to use static WEP keys to encrypt peer-to-peer data.

### Specifying WEP Keys

You can enter up to four WEP keys for encrypting data (see Figure 14). You must specify whether or not you are entering them as **Alphanumeric** strings or as **Hexadecimal** numbers.

**Figure 14: WEP Keys Dialog**

When you have made the settings, tap **Next**.

### Completing a Network Configuration

When your network configuration is complete, the final dialog appears. Tap **Finish**, to complete the network configuration process.

## Setting Server Certificates and Trust

Odyssey Access Client only allows you to authenticate with servers who can provide a certificate which you have indicated that you ultimately trust. See “Certificates” on page 11. You can configure simple trust on your device.

See the following topics:

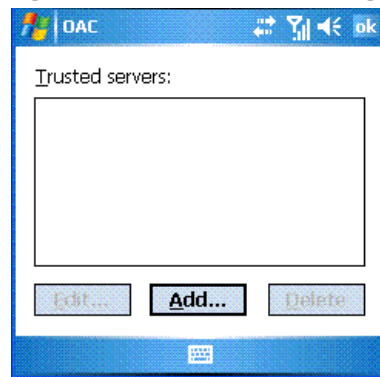
- Using Simple Trust Configuration
- Managing Untrusted Servers

### Using Simple Trust Configuration

You can configure simple trust directly on your device. To do so, follow these steps:

1. Select **Settings > Trusted Servers** on the device. The **Trusted Servers** dialog (Figure 15) appears.

**Figure 15: Trusted Servers Dialog**



2. Tap **Add**, to add the server trust specification (see Figure 16), or tap **Edit**, to edit a selected trusted server.

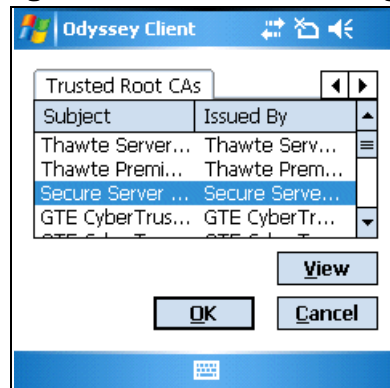
**Figure 16: Add Trusted Server Dialog**



3. You have two options with respect to specifying a domain name for trusting servers that issue a given certificate:

- Select **Any name**, to allow any server issuing your selected certificate to be trusted.
  - Type in the domain name ending under **Name must end with**.
4. Tap **Browse**, to select a server certificate.

**Figure 17: Select Certificate Dialog**

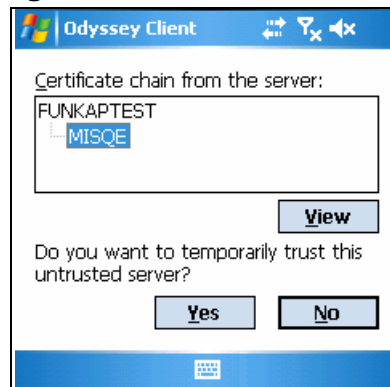


5. Select the server certificate you require (see Figure 17) and tap **OK** to close **Select Certificate**. Ask your administrator if you do not know which certificate to select.
6. Tap **View** to see details about your server certificate.
7. Tap **OK** to close each dialog.

You can also remove selected trusted servers from **Settings > Trusted Servers** by tapping **Delete** on the **Trusted Servers** dialog.

### **Managing Untrusted Servers**

There are times when you may be unable to communicate with a server because you do not have OAC configured to trust it, even though you have the root certificate that signed the certificate of that server on your device. In such a case, a message dialog appears (Figure 18) that provides information about the server when you try to connect, so that you may choose whether or not to trust it temporarily.

**Figure 18: Authenticate Untrusted Server Dialog**

Tap **Yes** to grant temporary trust and tap **No** to deny it.

---

## Configuring SIM card Features

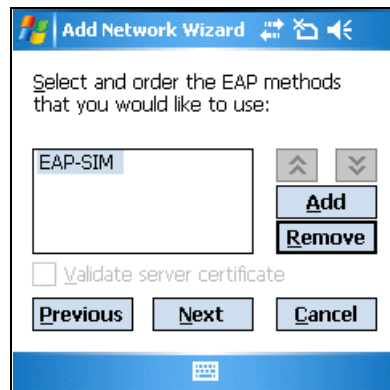
If you are licensed for using EAP-SIM and EAP-AKA with Odyssey Access Client, you can address the following additional features when you configure your SIM card for use with Odyssey Access Client:

- Setting Up EAP Authentication Methods
- Configuring SIM card ID and PIN Options
- SIM Card Settings: for EAP-SIM Identity

See also “Using SIM Card PIN Manager” on page 43, for information on using OAC to configure some SIM card PIN options and “Specifying Credentials” on page 26 for SIM card-specific configuration options.

### **Setting Up EAP Authentication Methods**

Before you can connect to a network using a SIM card, you must use EAP-SIM and/or EAP-AKA as the authentication protocol with this connection (see Figure 19). You can also configure other authentication methods that require passwords, but this is not recommended in combination with SIM card authentication.

**Figure 19: Select EAP Methods Dialog**

If you must add, reorder, or remove any authentication protocols, follow the instructions for adding and removing protocols in “Setting EAP Authentication Methods” on page 23.

When you have made the settings, tap **Next** to continue.

### Configuring SIM card ID and PIN Options

There are two ways to configure SIM card network connections with Odyssey Access Client:

- Allow your device to connect to the network using any SIM card ID. To do this, select [any] from the list provided.
- Make your SIM card ID known to Odyssey Access Client. You can do this by either typing its ID in, or by selecting it from the list provided (see Figure 20). Your SIM card ID appears on the SIM card settings page of the network configuration wizard when you insert the SIM card in your device.

**Figure 20: Configure SIM Card ID Dialog**

### SIM Card Settings: for EAP-SIM Identity

You have options with respect to how your EAP-SIM identity is presented to your provider for network authentication. The option you choose depends on your provider’s requirements.

You have two choices for presenting your EAP-SIM identity for authentication:

- Select **The IMSI from my SIM card** (default) if your provider requires you to use your IMSI for identification.
- Select **The login name I entered in this profile** if you are required to use an identity (usually of the form *username@realm*) rather than your IMSI. In this case, you must make sure that your login name is in the form that is required by your provider. Note that for this option, if you allow more than one authentication protocol with this profile, then you may have a conflict with your login name. If you are required to select this option, then create a separate network configuration for any connections that use other protocols.

Click **Next** when you have made the settings with this dialog.

### SIM Card PIN Options

You have three mutually exclusive PIN options on the main SIM card setting dialog (Figure 21):

- **Do not use a PIN.** Select this option if no PIN is required.
- **Prompt for PIN.** Select this option if an PIN is required and you want to be prompted for the PIN on your SIM card. Use this option when you set your SIM card ID to **[any]** (rather than specifying a SIM card ID).
- **Use the following PIN.** Select this option when you are required to use the PIN on your SIM card and you do not want to be prompted to enter it every time you connect. To use this option you must type the PIN in the text box provided. You can optionally check **Unmask** to view the PIN as you type it.

**Figure 21: Configure Prompt for PIN Dialog**



Click **Next** when you have made the settings for this section.

---

## Menus

You can use the following menus to help execute commands and configure wireless connections using your device:

- Settings Menu
- Commands Menu
- Tools Menu
- Help Menu

## Settings Menu

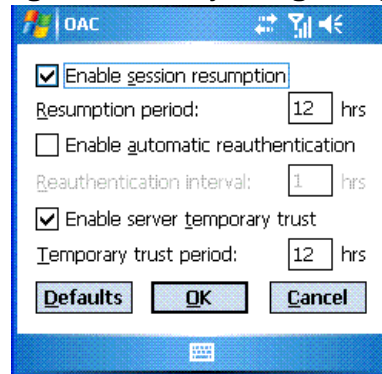
You have several settings menu options:

- **Configure**—Create a new network configuration definition.
- **Detailed Status**—Display detailed status information about a current connection. See “Viewing Connection Status Details” on page 17.
- **Disable/Enable Odyssey**—Disable Odyssey Access Client when it is enabled. Enable Odyssey Access Client when it is disabled.
- **Trusted Servers**—Configure, edit, or remove your trusted server specification. See “Using Simple Trust Configuration” on page 31.
- **Security Settings**— Set general security settings. See “Security Settings” on page 36.
- **EAP-FAST**— Configure security options EAP-FAST authentication. See “EAP-FAST Settings” on page 38.
- **Exit**—Terminate the current connection and stop the Odyssey Access Client program.

## Security Settings

There are three security settings options from **Settings > Security Settings** (Figure 22).

**Figure 22: Security Settings Dialog**



- **Enable session resumption.** You can specify the maximum length of a session before it expires when you choose this option. See “Setting Up Session Resumption” on page 37.

- **Enable automatic reauthentication.** You can specify the reauthentication period when you choose this option. See “Automatic Reauthentication” on page 37.
- **Enable server temporary trust.** You can specify the maximum length of a session with a temporarily trusted server when you choose this option. See “Server Temporary Trust” on page 38.



**NOTE:** You can restore the defaults at any time by tapping **Reset Defaults**. In addition, you can specify the time (in hours) for session resumption and automatic reauthentication using up to three decimal places.

### **Setting Up Session Resumption**

You can enable the use of session resumption from **Settings > Security Settings**. See “Session Resumption” on page 13 for more information on session resumption.

To use enable session resumption, do the following:

- Check **Enable session resumption**.
- Set **Do not resume sessions older than** to the maximum number of hours that an initial authentication can be used to accelerate reauthentication. Once the time limit has elapsed, a completely fresh authentication is performed on your next reauthentication. You can specify the number of hours with 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, uncheck **Enable session resumption**.

### **Automatic Reauthentication**

You can enable or disable the automatic reauthentication feature of OAC. For information about why you might want to reauthenticate, see “Session Resumption” on page 13.

When you check **Enable automatic reauthentication** in **Settings > Security Settings**, OAC periodically initiates reauthentication with the server.

Next to **Reauthenticate every**, type the time period (in hours) for reauthentication to take place automatically. You can use up to three decimal places to indicate the number of hours.

Uncheck **Enable automatic reauthentication** in **Settings > Security Settings** to disable this feature.

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

### Server Temporary Trust

Under normal circumstances, you can use the **Trusted Servers** dialog from **Settings > Trusted Servers** (see “Using Simple Trust Configuration” on page 31) to configure the servers you trust for authentication. However, there may be times when you visit a network whose authentication server is not yet configured as trusted. In this case, you may want the ability to enable *temporary trust* for that *untrusted server*.

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

- If temporary trust is enabled, a message appears when you attempt to authenticate to a server for which you have not configured trust. You are given the option of whether or not to trust the untrusted server temporarily. See “**Managing Untrusted Servers**” on page 32.
- If you do not enable temporary trust, then any authentication attempt that requires the validation of a server certificate fails when the server is not explicitly trusted.

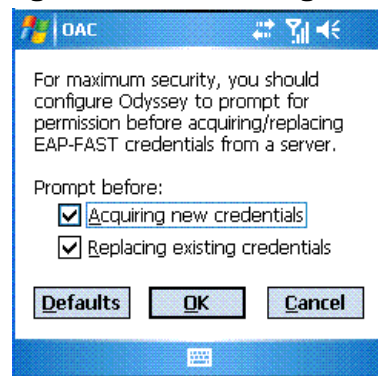
Set **Maximum time for temporary trust** to the maximum number of hours you want OAC to continue to trust a server once you accept it.

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

### EAP-FAST Settings

You have the following options available from **Settings > EAP-Fast Settings** that determine when you are prompted for credentials when you use EAP-FAST authentication.

**Figure 23: EAP-FAST Dialog**



- Check **Prompt before acquiring credentials from a new server** to be prompted for credentials when you authenticate with a server to which you have not previously authenticated using EAP-FAST.

- Check **Prompt before replacing credentials from a known server when your existing credentials have failed** to be prompted for credentials upon authentication with a known server for which an earlier authentication attempt resulted in failure.
- Tap **Reset Defaults** to return to the default configuration (both options checked).

## Commands Menu

You have several commands menu options:

- **Scan**—Search for networks in your vicinity. See “Scanning for Wireless Networks” on page 16.
- **Reauthenticate**—Perform the authentication again, generating new dynamic encryption keys. See “About Reconnecting and Reauthenticating” on page 39.
- **Reconnect**—Re-establish a connection with the current network, via the access point with the strongest signal and SSID (unless you are using the [Any] network) and reauthenticate. See “About Reconnecting and Reauthenticating” on page 39.
- **Forget temporary trust**—Withdraw your temporary trust of the current server immediately. See “Using the Forget Temporary Trust Setting” on page 40.
- **Forget password**—Clear the password entry so that you are prompted the next time a password is needed. See “Using the Forget Password Setting” on page 40.

### About Reconnecting and Reauthenticating

You can reconnect either from the **Reconnect** button on the main OAC dialog or from **Commands > Reconnect**. When you reconnect, Odyssey Access Client disconnects any existing connection and starts a new connection to your current wireless network. The new connection may be with a different access point (on the same network) than was used with your previous connection. The access point in use depends on factors such as signal strength. If you are already authenticated with this network, you are reauthenticated when the new connection starts. If dynamic encryption keys are in use, they are refreshed when you reconnect.

You can reauthenticate from the **Commands** menu. When you select **Commands > Reauthenticate**, Odyssey Access Client uses the existing connection shown on the dialog, without starting a new connection. If dynamic encryption keys are in use, they are refreshed.

It is unlikely that you need to perform these actions very often. However, if you feel that your connection is not performing as well as it should. Reconnecting can sometimes help, particularly if it results in a connection with an access point that is able to provide better service.

### Using the Forget Temporary Trust Setting

If you enable temporary trust in **Security Settings** on your device, whenever you encounter an untrusted authentication server a dialog pops up, allowing you to trust that server temporarily if you have the server certificate installed. Odyssey Access Client remembers to trust that server for the period of time that you configure in **Settings > Security Settings** on your device.

If you want Odyssey Access Client to immediately discard its list of temporarily trusted servers, select **Commands > Forget temporary trust**.

### Using the Forget Password Setting

When you first authenticate using a profile set to **prompt for password**, you are asked to type in your password. Odyssey Access Client remembers the password you entered and uses it for all subsequent authentications using that profile, without prompting you again.

If you want Odyssey Access Client to discard any passwords you type in, select **Commands > Forget password**. You are prompted when your password is needed again.

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

## Tools Menu

You can use the following tools to assist with configuring your device for use with OAC:

**Importing a User Certificate**—Import a user certificate from a **.pfx** file for use with TLS authentication.



**NOTE:** The ability to import certificates is supported only in the Enterprise Edition of Odyssey Access Client for Windows Mobile.

---

- **Using Certificate Enroller**—Request user certificates for use with EAP-TLS from a certificate authority within your enterprise.
- **Using SIM Card PIN Manager**—Manage PIN and related settings for your SIM card if you have this licensed feature.

### Importing a User Certificate

To import a user certificate from a **.pfx** file on your device for use with EAP-TLS authentication, select **Tools > Import User Certificate** (see Figure 24).

**Figure 24: Import User Certificate Dialog**

Follow these steps to install a user certificate on your device for use with Odyssey Access Client:

1. Tap **Browse** to find the .pfx file located on your device. Select the file and tap **OK**.
2. Type in the RSA-type private key password for this .pfx file. Ask your administrator for help if necessary. Check **Unmask** to view the password as you type it.
3. Tap **Install Certificate** to import the certificate. A dialog pops up, reporting the certificate import success or failure. Tap **OK** to close this dialog.
4. You can optionally repeat steps 1-3 to import multiple user certificates.



**NOTE:** If you do not already have a .pfx file to import, but can obtain a user certificate from your certificate granting authority within your network, use **Tools > Using Certificate Enroller**.

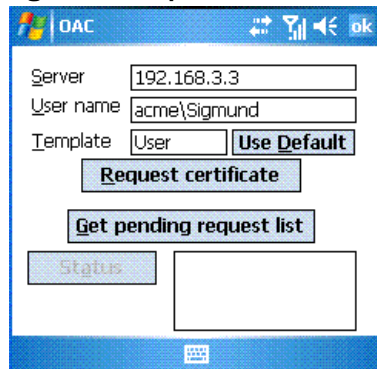
### Using Certificate Enroller

The EAP-TLS authentication protocol requires a user certificate to be installed on your device. See “Selecting a Certificate for Certificate Credentials (EAP-TLS)” on page 28.



**NOTE:** The certificate enroller is supported only in the Enterprise Edition of Odyssey Access Client for Windows Mobile.

If your device uses a Windows Mobile operating system, use **Tools > Certificate Enroller** while you are connected to your certificate authority network to request and install a user certificate using Microsoft Certificate Services. Once installed, you can use the requested certificate when you configure authentication with the EAP-TLS protocol. See your network administrator for help in using this tool.

**Figure 25: Request Certificate Dialog**

Select **Certificate Enroller** from the **Tools** menu to use this tool.

To request a certificate:

1. Enter the DNS server name or IP address of your Microsoft Certificate Services server in the **Server** field.
2. Enter the user name required for this request in the **User name** field.

The default certificate template for user certificates has the name **User**.

To change of the name of the certificate template:

1. Tap **Options**.
2. Change the name of the certificate template if necessary and tap **OK**.

To restore the default certificate template name, tap **Use Default**.

1. Once you fill in a server name or address and user name, tap **Request** to request a user certificate. There are four possible outcomes:
  - Your request fails for some reason.
  - Your request is successful and a user certificate is issued immediately. In this case, you are prompted to install the new certificate. If you decline certificate installation at this time, you must repeat your request at some other time.
  - Your request is successful but is denied.
  - Your request is successful and is waiting to be addressed by a certificate authority administrator at some point in the future. You can exit the certificate enroller while a request is pending without losing the request.
2. You can optionally repeat steps 1-4 to submit multiple requests and install multiple user certificates.
3. Tap **OK** to exit.

### Managing Pending Certificate Requests

You can process any pending certificate requests once they have been addressed by your certificate authority administrator.

To process pending certificate requests, follow these steps:

1. Tap **Get List** to list any pending certificate requests.
2. Select a listed certificate request and tap **Status**.

If your certificate is issued, then you are prompted to install it on your device for use with Odyssey Access Client.

If your request is denied, you may see it listed under **Pending Requests** for several days.

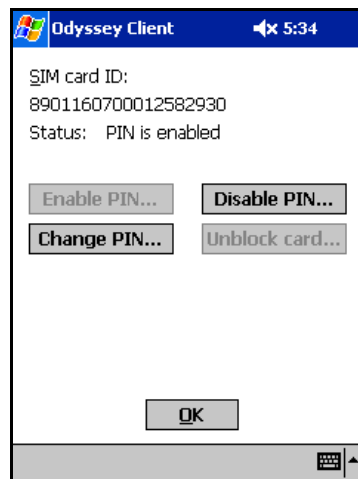


**NOTE:** You cannot abandon pending certificate requests using the certificate enroller. Consequently, pending requests that are not processed by your certificate authority persist when you tap **Get List**.

### Using SIM Card PIN Manager

Your SIM card may require some PIN management. Odyssey Access Client provides a SIM card PIN manager for your convenience. You have several options available, depending on the state of your SIM card PIN settings:

**Figure 26: SIM Card PIN Manager Dialog**



- Tap **Enable PIN** if the SIM card PIN is disabled, to enable it.
- Tap **Disable PIN** if the SIM card PIN is enabled, to disable it.
- Tap **Change PIN** to change the PIN when the SIM card PIN is enabled.
- If your PIN fails, your card may be blocked. If your card becomes blocked, you can unblock it. To do so, you must first contact your service provider for a PIN unblock key (PUK). Once you do so, tap **Unblock Card**.

For any of these, follow the instructions on the dialogs that appear and tap **OK** when you have made the settings.

## Help Menu

Select Help from the Tool bar for following help features:

- **Help Topics**—Invoke the online Odyssey Access Client device help system. To get help for a particular dialog while using Odyssey Access Client, however, select **Start > Help** on your device.
- **License Keys**—Enter license keys for software registration.
- **View Readme File**—Display the readme.txt file that comes with your software. The **readme** file often has last-minute information of which you should be aware.
- **About**—Display information about the version of this software.

## License Keys

You can view, add, or delete license keys from **Help > License Keys**.

**Figure 27: Software License Dialog**



You can perform the following licensing tasks:

- To add a license key, type the valid license key under **New License** and tap **Add**. The new license is listed under **Licenses**.
- To remove a license key, select the license key under **Licenses** and tap **Delete**.

Note that if you are upgrading OAC from a previous version, you must have at least two license keys listed when you select **Help > License Keys**:

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

---

## OAC Deployment Using Client Scripts (EE Only)

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

A network administrator can distribute configuration settings to one or more mobile devices by placing a script file in a specific folder in the mobile device's file system. You can use a script to deploy an OAC configuration to multiple devices 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. Then place the script on the mobile device in the `newScripts` folder under the OAC install directory on the mobile device which is typically `/Program Files/Juniper Networks/Odyssey Access Client/newScripts`. Refer to the *Odyssey Access Client Administration Guide* for details on using the Odyssey Access Client Administrator tools.

To deploy a configuration to mobile devices using a script:

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. Refer to the *Odyssey Access Client Administration Guide* for details on using the Administrator tools.
3. Use ActiveSync, a flash memory card, a shared network drive, or other available out-of-band transfer method you prefer to make the script file available to the mobile device users.

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



**NOTE:** Client Scripts are supported only in the OAC Enterprise Edition.

---

# Index

## Numerics

802.11 .....	4
ad-hoc mode .....	7
infrastructure mode .....	6

## A

access points	
introduction .....	6
IP addresses .....	6
ActiveSync .....	1
adding	
EAP-SIM .....	34
licenses .....	44
PEAP inner protocols .....	25
ad-hoc mode	
configuring .....	29
defined .....	7
AES	
implementing .....	21
overview .....	8
peer-to-peer .....	9
anonymous	
authentication .....	27
any	
server, trusting .....	32
association	
defined .....	4
modes .....	21
asymmetric cryptography .....	11
authentication	
methods .....	18
protocols, choosing .....	21
auto-scripts .....	2

## C

CAB file installation .....	2
certificate	
certificate authorities	
defined .....	11
root .....	11
chains	
defined .....	11
Certificate Enroller .....	41
certificates	
importing .....	40
installing .....	41
overview .....	11
pending .....	43
requesting .....	41

changing PINs .....	43
channel numbers, peer-to-peer .....	29
CHAP .....	24
commands menu .....	39
configuring	
network connections .....	20
trusted servers .....	31
Connect to .....	16
connections	
breaking .....	16
making .....	16
reconnecting .....	16
status .....	19
credentials, configuring .....	26

## D

deleting trusted servers .....	32
descriptions of networks .....	21
detailed status .....	17
DHCP servers .....	6
domain	
controller, EAP interaction .....	13
specifying .....	34

## E

EAP	
authentication methods, configuring .....	23
configuring inner .....	24
definition .....	10
inner authentication method .....	25
EAP-AKA	
configuring .....	33
ID .....	34
identities .....	34
provider options .....	34
using .....	23
EAP-Cisco Wireless .....	12
EAP-FAST	
overview .....	12
settings for prompting .....	38
token card options .....	28
using .....	23
EAP-GenericTokenCard	
options .....	28
using .....	23
EAP-LEAP	
overview .....	12
using .....	23
EAP-MD5-Challenge .....	23

- EAP-PEAP
  - overview ..... 12
  - settings ..... 25
  - using ..... 23
- EAP-SIM
  - configuring ..... 33
  - ID ..... 34
  - identities ..... 34
  - provider options ..... 34
  - using ..... 23
- EAP-TLS
  - overview ..... 12
  - using ..... 23
- EAP-TTLS
  - overview ..... 12
  - using ..... 23
- encryption
  - detailed status ..... 18
  - keys
    - auto-generation, configuring ..... 18
    - defined ..... 4
- Extensible Authentication Protocol ..... 10
  
- F**
  - forget
    - password, setting ..... 40
    - temporary trust ..... 40
  
- G**
  - Generic Token Card ..... 28
  - graphics
    - connection ..... 19
  
- H**
  - help
    - getting ..... 44
    - menu ..... 44
  
- I**
  - importing user certificates ..... 40
  - IMSI, EAP-SIM ..... 34
  - infrastructure mode
    - configuring ..... 21
    - defined ..... 6
  - inner authentication protocols ..... 24
  - installing
    - cab ..... 2
    - certificates ..... 41
    - exe ..... 1
  - intermediate CAs
    - configuring ..... 32
    - overview ..... 11
  
- L**
  - LDAP ..... 12
  - LEAP ..... 12
  - license keys
    - adding/removing ..... 44
    - CAB installation ..... 2
    - overview ..... i
    - upgrading ..... 44
  - lightweight EAP ..... 12
  
- M**
  - managing PINs ..... 43
  - MS-CHAP ..... 24
  - MS-CHAP-V2 ..... 24
  - mutual authentication ..... 10
  
- N**
  - Network ..... 20
  - networks
    - configuring ..... 20
    - descriptions, configuring ..... 21
    - editing ..... 20
  - newlink LicenseKeys ..... 44
  
- O**
  - open mode, WEP ..... 8
  - operating the product ..... 15
  
- P**
  - PAP protocol ..... 24
  - passwords
    - configuring ..... 26
    - forgetting on authentication ..... 40
  - PEAP
    - inner protocols
      - adding ..... 25
      - removing ..... 26
      - reordering ..... 26
    - overview ..... 12
    - settings ..... 25
  - peer-to-peer networking
    - configuration ..... 21
    - definition ..... 7
    - IP addresses ..... 7
  - pending certificate requests ..... 43
  - PINs
    - managing ..... 43
    - private key ..... 11
    - profiles, adding ..... 26
  - prompts
    - EAP-FAST ..... 38
    - token information ..... 28
  - Provide my password ..... 28
  - provider-specific options, EAP-SIM ..... 34
  - public key ..... 11
  
- R**
  - RADIUS, server product ..... 9
  - readme file ..... 44
  - realms ..... 34
  - reauthenticating
    - explained ..... 13
    - session resumption ..... 37

- why ..... 13
- reconnecting..... 16
- refresh, detailed status..... 17
- requesting certificates..... 41
- roaming anonymously..... 27
- root certificate authority ..... 11
- running the product..... 15

**S**

- scanning for networks
  - configuring networks..... 21
  - main screen ..... 16
- scripting ..... 2
- security settings..... 36
- servers, untrusted ..... 32
- Service Set Identifier (SSID) ..... 7
- session resumption
  - overview ..... 13
  - settings..... 37
- settings menu..... 36
- shared mode, WEP ..... 8
- signal tab ..... 18
- SIM cards
  - any, selecting ..... 34
  - changing PINs ..... 43
  - configuring..... 33
  - IDs ..... 34
  - provider-specific options ..... 34
  - settings..... 33
  - unblocking ..... 43
- simple trust ..... 31
- smart cards ..... 33
- soft-reset ..... 1
- SQL ..... 12
- SSIDs
  - specifying..... 20
- starting the product ..... 15
- switches, 802.1X ..... 6

**T**

- temporary trust ..... 40
  - defined..... 38
  - disabling..... 38
- TKIP
  - overview ..... 8
  - peer-to-peer..... 9
  - using ..... 21
- TLS, overview ..... 12
- token card options..... 24
- tools menu ..... 40
- trusted servers
  - deleting ..... 32
  - simple method ..... 31
  - trusting any ..... 31
- TTLS
  - inner authentication methods ..... 24
  - overview ..... 12

**U**

- unblocking PINs..... 43
- untrusted servers
  - defined ..... 38
  - trusting..... 32
- upgrades..... 44
- user names, setting..... 34

**V**

- validating server certificate ..... 24

**W**

- WEP keys
  - configuring ..... 30
  - defined ..... 7
  - open mode..... 8
  - peer-to-peer..... 8
  - using, ad-hoc ..... 30
- Wired-Equivalent Privacy..... 7
- WPA
  - overview..... 8
- WPA2
  - overview..... 8

