Odyssey Access Client for Windows
User Guide

Enterprise Edition
FIPS Edition

Release 5.5
October 2012

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

Copyright Notice

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with the instruction manual, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device and may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

U.S. Government Rights

Commercial software and commercial software documentation: This documentation is commercial computer software documentation and the products (whether hardware or software) covered by this documentation are or contain commercial computer software. Government users are subject to the Juniper Networks, Inc. standard end user license agreement and any applicable provisions of the FAR and its supplements. No further rights are granted.

Products (whether hardware or software) covered by, and information contained in, this documentation are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical, biological weapons end uses or end users, whether direct or indirect, are strictly prohibited. Export or re-export to countries subject to U.S. embargo or to entities identified on US export exclusion lists, including, but not limited to, the denied persons and specially designated national lists, is strictly prohibited.

Disclaimer

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Table of Contents

About This Guide

This guide describes how to install, configure, and use the Juniper Networks Odyssey Access Client (OAC) for wired or wireless network access. It addresses these licensed editions of OAC:

- OAC Enterprise Edition
- OAC Federal Information Processing Standard (FIPS) Edition

Some OAC features and options require a specific OAC license. For example, FIPS mode requires a FIPS Edition license. Such distinctions are identified as they occur in this guide.

You can deploy OAC in a network that includes the Juniper Networks Unified Access Control (UAC) security solution, where authenticated access to protected network resources is managed by an Infranet Controller. Alternatively, you can deploy OAC in a traditional network where OAC might negotiate with an authentication, authorization, and accounting (AAA) server for authenticated access.

For general information about network security, see Appendix A, "Network Security Concepts."

Audience

This guide is intended for any Windows user who uses Odyssey Access Client to obtain access to wired or wireless network.

This guide is also intended for network administrators responsible for maintaining configurations for OAC end users.

Conventions

The following tables show the conventions used throughout this book. Table 1 defines notice icons; Table 2 defines text conventions; Table 3 defines CLI conventions; and Table 4 defines GUI conventions.

Table 1: Notice Icons

Icon	Meaning	Description
	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

Convention	Description
Plain sans serif type	URLs, filenames, and directory names.
Italics	■ Terms defined in text. ■ Variable elements for which you supply values. ■ Book titles.
+ (plus sign)	Key names linked with a plus sign indicate that you must press two or more keys simultaneously.

Table 3: CLI Conventions

Convention	Description
Bold type	Commands that you enter; command names and options.
Plain sans serif type	■ Filenames and directory names. ■ Code and system output.
Italics	Variables for which you supply values.
[ ] Square brackets	Elements in square brackets indicate optional keywords or variables.
| Pipe symbol	Elements separated by the pipe symbol indicate a choice between mutually exclusive keywords or variables.
{ } Braces	Elements in braces indicate required keywords or variables.

Table 4: GUI Conventions

Convention	Description
> (chevron)	Navigation paths through the UI.
Bold type	User interface elements that you select in a procedure, such as tabs, buttons, and menu options.

Table 4: GUI Conventions (continued)

Convention	Description
Italics	Variables for which you supply values.

Documentation

Table 5 describes the available OAC and UAC documentation.

Table 5: OAC/UAC Documentation Set

Title	Purpose
Odyssey Access Client Quick Start	Help basic users to install OAC and connect quickly to a wired or wireless network
Odyssey Access Client User Guide	Provide an overview of OAC to basic and advanced users, provide detailed discussions and instructions for configuring network and authentication settings, and offer basic troubleshooting advice.
Odyssey Access Client Administration Guide	Describe how to plan, configure, and deploy OAC to multiple users, how to control access to OAC options based on the needs and skill levels of user groups, how to manage updates, and how to deploy updates using scripts.
Unified Access Control Administration Guide	Describe the UAC solution and provide instructions for configuration and maintenance.
Unified Access Control Quick Start Guide	Describe the basic tasks for configuring the Infranet Controller and the Infranet Enforcer.
Unified Access Control Client-Side Changes Guide	Describe the changes that OAC and the Infranet Controller make on client computers, including the installed files and registry changes.
Unified Access Control Custom Sign-in Pages Solutions Guide	Describe how to personalize the look and feel of the pre-authentication and sign-in pages that the Infranet Controller displays to users and administrators.
Unified Access Control J.E.D.I. Solutions Guide	Describe how to write and implement solutions through the Host Checker client and server APIs.
Unified Access Control Deployment Scenarios Guide	Provide recommendations for deploying the UAC solution.

Release Notes and Product Documentation

You can access this manual, as well as the OAC release notes, the *Odyssey Access Client Quick Start Guide*, and the *Odyssey Access Client Administration Guide* on the Web at:

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

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

Context-Sensitive Help

OAC includes online help that you can access from **Help > Help Topics** on the Odyssey Access Client Manager menu bar.

To access context-sensitive online help for OAC, press the F1 key. The resulting help describes the active OAC dialog box and provides links to information on OAC features and functions, to configuration and administration procedures, and to descriptions of other OAC dialog boxes.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings—http://www.juniper.net/customers/support/
- Find product documentation—http://www.juniper.net/techpubs/
- Search for known bugs or find solutions and answer questions using our Knowledge Base— http://kb.juniper.net/
- Download the latest versions of software and review your release notes—http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications—http://www.juniper.net/alerts/
- Participate in the Juniper Networks Community Forum—http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Manager—http://www.juniper.net/customers/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool, which can be found on https://tools.juniper.net/SerialNumberEntitlementSearch/.

Open a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Manager tool in the CSC at http://www.juniper.net/customers/cm/.
- Call 1-888-314-JTAC (1-888-314-5822) toll free in USA, Canada, and Mexico.

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/customers/support/requesting-support/.

Chapter 1

Odyssey Access Client Overview

Odyssey Access Client (OAC) is networking software that runs on endpoint computers (desktop, laptop, or notepad computers and supported wireless devices). Use OAC to establish secure wireless and wired connections in a corporate network. You can also use OAC to connect to public and home wireless networks.

In corporate networks, OAC negotiates with 802.1X wireless access points, 802.1X switches, and Infranet Controllers for authenticated, secure access to protected networks. An authentication server, such as Juniper Networks Steel-Belted Radius, must validate each user. In a Juniper Networks Unified Access Control (UAC) environment, the user's computer is checked for security compliance before being allowed network access. In networks with 802.1X switches, the switches become enforcement points in the network security architecture.

Corporate networks usually have both wired and wireless networks to support mobile computing at work. OAC supports secure, authenticated network access for both wired and wireless connections, so you can have a secure wired connection from your office and a secure wireless connection when you take your laptop to meetings. OAC supports extensive configuration options, making it an effective solution for any networking environment. Use OAC for the following tasks:

- Manage network adapters.
- Configure and control connections to wired and wireless networks.
- Configure and use authentication profiles to connect to secure networks.
- Connect to an Infranet Controller to access protected resources.
- Set up a list of frequently used wireless networks in order of preference.
- Manage server trust settings.
- Use certificate-based authentication methods with smart cards.
- Run a script to update your current OAC configuration settings.
- If you have an OAC FIPS license, configure FIPS 140-2 certified encryption when you connect to a network.

How OAC Operates in a Network

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

With 802.1X, you are authenticated for network access based on matching authentication protocols, such as the Extensible Authentication Protocol (EAP), and on your user credentials, such as a password, certificate, or a token card. For details about configuring EAP protocols, see "Configuring Outer EAP Authentication Protocols" on page 60. For details about setting up credentials, see "Configuring User Information" on page 51.

OAC can be deployed in two distinct network environments:

- A network with the UAC solution manages authentication using an Infranet Controller (see "Authentication in a Unified Access Control Network" on page 2). The Infranet Controller includes an integrated Steel-Belted Radius server.
- A traditional network manages authentication with a standard AAA server, such as Steel-Belted Radius.

Authentication in a Unified Access Control Network

UAC provides enhanced security measures that not only authenticate users but verify that the software running on the user's computer complies with corporate security policies.

UAC encompasses a variety of components that, together, provide secure authenticated access to network resources. These components include:

- Infranet Controller—A central policy management server that validates the user's identity and the computer's security compliance and manages network policies. Those policies are created on the Infranet Controller and are used for configuring OAC, Host Checker, and access to protected resources. The Infranet Controller distributes the policies to OAC, Host Checker, and the Infranet Enforcer.
- Infranet Enforcer—A Juniper Networks security device that operates with the Infranet Controller to enforce security policies. The Infranet Enforcer is deployed in front of the servers and protected resources.
- Host Checker—A software component of OAC that checks your computer for compliance with the security policies that your Infranet Controller administrator specifies. For example, Host Checker might verify that your computer has the current antivirus software version and security setting or that it has the latest operating system patch or service pack installed.

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

In a UAC network, OAC users can be authenticated for network access in the following ways:

- A wired (Layer 2) connection through an 802.1X switch (see Figure 1).
- A wireless (Layer 2) connection through an 802.1X wireless access point (see Figure 1).
- A direct (Layer 3) connection to an Infranet Controller. In this case, OAC connects to the Infranet Controller and authentication occurs using EAP-over-HTTP (see Figure 2).

Figure 1: OAC Authentication in a Network with 802.1X (Layer 2)

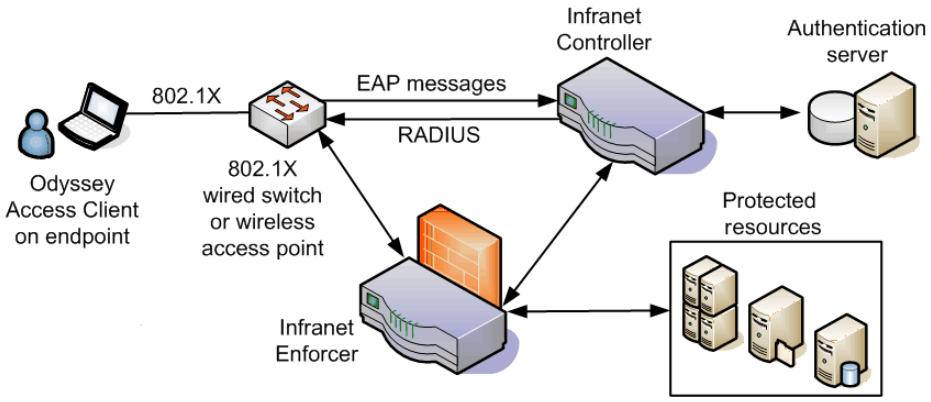
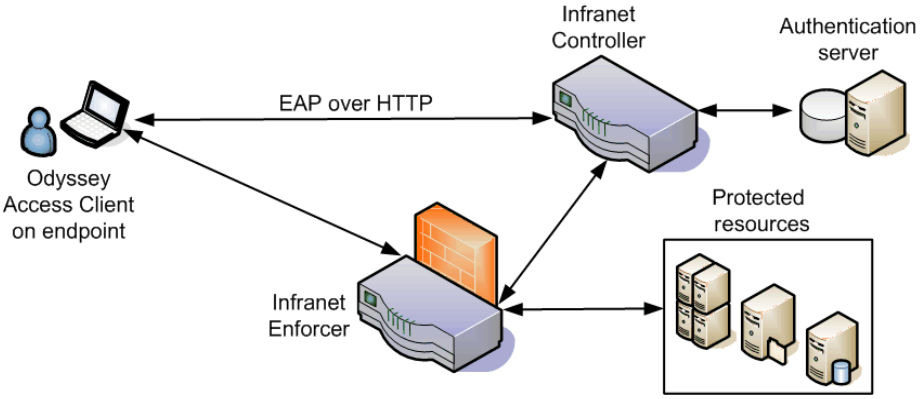


Figure 2: Authentication in a Network Without 802.1X (Layer 3)



In a UAC network, you can connect to more than one network and to more than one Infranet Controller. When you connect to a UAC network, your network connection might be authenticated by an AAA server that is integrated with the Infranet Controller or by a separate AAA server external to the Infranet Controller.

The Infranet Controller authenticates you as a user and determines which protected resources you can access based on your username and the realm and role to which you belong. After you are authenticated, the Infranet Controller tells another device on the network, called the Infranet Enforcer, about the networks and resources that you are allowed to access. The Infranet Enforcer then manages your access to protected network resources.

For information on realms and roles, see "Setting a Preferred Realm and Role" on page 70. For a broader discussion of UAC components and concepts, see the *Unified Access Control Administration Guide*.

Quarantine and Remediation

A network security policy defines the rules and requirements that must be met by devices requesting access to the network. Security enforcement checking ensures that all endpoints (computing devices) comply with the network's security policy. *Remediation* is the process of bringing a device into compliance with an organization's security policy.

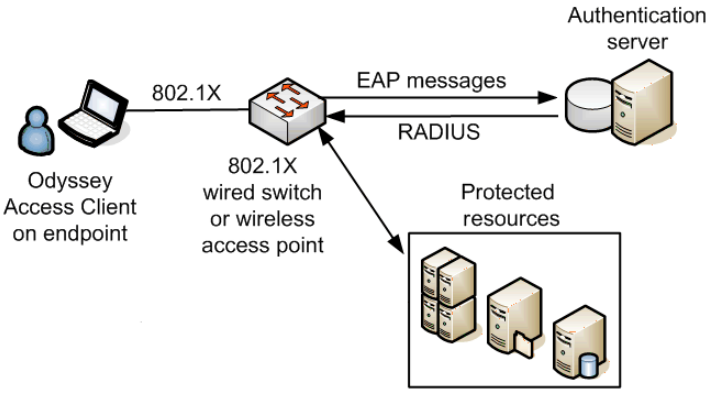
The Infranet Controller checks your computer periodically to verify compliance with all prescribed security requirements. For example, the Infranet Controller might confirm that antivirus software is running on your computer.

- If a computer complies with a site's network security policy, the user is granted access to protected network resources based on the user realm and role configured in the Infranet Controller.
- If a computer does not comply with a site's network security policy, the user might be denied access or redirected to a special network for remediation.
    - Access denied—The computer might be denied network access until it meets security compliance requirements. In some cases, the network denial might last a few seconds, while the computer's antivirus software settings are updated automatically. In other cases, the computer might be denied network access until the user takes a specific action, such as installing necessary software or running an antivirus scan.
    - Access granted—The computer might be granted access to protected networks while being brought into compliance in the background.
    - Access redirected—The computer might be redirected to a special quarantine network or VLAN, which provides remediation instructions and access to update files or other resources needed for compliance. For example, a quarantine network might instruct the user to install Windows update patches or service packs in order to be granted access to protected resources. When the quarantined computer complies with the network security policy, the Infranet Controller can redirect it to the protected network automatically.

Authentication in a Traditional Network (Without UAC)

When deployed in traditional networks that do not include UAC components, OAC can negotiate authentication to the network through an 802.1X switch or through an 802.1X wireless access point (see Figure 3).

Figure 3: OAC in a Traditional Network (Without UAC)



The following steps describe a typical 802.1X authentication process.

1. When a client attempts to connect to an 802.1X network, it signals a network access device (802.1X wired switch or wireless access point) that it is making an authentication request.

   - In a wired network, the 802.1X switch brokers the request for network access, which triggers a prompt for authentication credentials from the authentication server.
   - In a wireless network, the 802.1X authentication occurs after the client connects to (associates with) an access point.

   For more information on 802.1X association, see “Specifying an Association Mode” on page 74 and “802.11 Wireless Networking” on page 105.

2. The network access device (access point or 802.1X switch) forwards the authentication request to the authentication server.

3. The authentication server compares the credentials submitted in the access request with the information in the authentication database.

4. If the authentication succeeds, the server instructs the network access device to grant access to the client computer. Depending on the information returned for the user, the server might restrict the user’s access to specific networks or resources.

5. The network access device then informs the client that it has been authenticated and is granted access to the network.

About FIPS Mode (FIPS Edition Only)

The Federal Information Processing Standard (FIPS) is a U.S. government security standard used to certify hardware and software cryptographic modules. After a module is certified as FIPS-compliant by an accredited testing laboratory, federal agencies and departments can reference the module's FIPS certificate to confirm the module is appropriate for their use.

The FIPS edition of OAC provides an encryption module that runs on your computer before data is transmitted. When you use OAC in FIPS mode, all cryptographic operations, such as exchange of keys and encryption of network traffic, take place using a validated FIPS encryption module. In FIPS mode, the number of cryptographic operations that are allowed for authentication and data encryption are restricted. For example, WEP and TKIP use RC4 encryption, which is not allowed, so FIPS mode disables WEP and TKIP in OAC.

xSec

xSec is a data link layer (Layer 2) protocol that provides a framework for securing wired and wireless connections using strong encryption and authentication. If you have xSec-compliant (Aruba) switches in your network, you can use xSec for association and AES for encryption. The xSec protocol operates a network adapter in open/unencrypted mode, but data packets are encrypted by an intermediate driver before they are forwarded to the network.

There are no network interface cards that operate in 802.11i FIPS mode with OAC on Windows Vista and Windows 7. If FIPS mode is required on Windows Vista or Windows 7, you must use xSec for encryption.

Table 6 illustrates support for FIPS mode settings and for xSec by platform.

Table 6: Support for FIPS Mode and xSec by Platform

FIPS	Support for	Windows XP 32-bit	Windows Vista and Windows 7 32-bit and 64-bit
No License	802.11i	Y	Y
	xSec	N	N
FIPS License: FIPS Mode Off	802.11i	Y	Y
	xSec	Y	Y
FIPS License: FIPS Mode On	802.11i	Y[a]	N[b]
	xSec	Y	Y

a.Supported if a FIPS-compliant driver is installed.
b.No FIPS-compliant driver is available.

NOTE: IPsec is not enabled when FIPS mode is enabled.

FIPS Adapter and Driver Requirements

If your computer is running a version of Windows other than Windows Vista, you need a FIPS-compliant network adapter and the appropriate adapter drivers to operate in FIPS mode. Contact Juniper Networks for the latest list of verified wireless adapters or see the Odyssey Access Client User webpage (http://www.juniper.net/customers/support/products/aaa_802/oac_client_user.jsp.) for information about adapter drivers you can use with the OAC FIPS module:

You may not be not required to install a new driver if you use xSec association. See "Selecting a FIPS Association Mode (FIPS Edition Only)" on page 75.

Certificate Requirements for FIPS Compliance

If you use EAP-TLS for authentication, a user certificate must be installed on your computer before it is configured for FIPS–compliant connections. This operation should be performed only by a network administrator.

For FIPS 140-2 compliance, private key operations must be performed by a FIPS-validated module. Some cryptographic providers conform to this requirement. For example, the Microsoft Cryptographic provider used in the Microsoft Certificate Store conforms to these standards for the following operating systems:

- All versions of Windows XP
- Windows Vista
- Windows 7

Some older versions of Windows do not meet the NIST standards for private key protection. You can use OAC to perform the FIPS-compliant encryption required to protect the private key on the system. To do so, you must make sure that the private key of the user certificate is marked as **Exportable**.

Network Requirements for FIPS Compliance

Your network must support WPA2 or xSec association and AES encryption if you want to use OAC in FIPS mode. Refer to "Using FIPS Secure Encryption (FIPS Edition Only)" on page 75 for information on how to set up a FIPS-compliant authentication profile.

You should configure your network servers as trusted servers in OAC. For more information, see "Managing Trusted Servers" on page 89.

Chapter 2

Installing Odyssey Access Client

This chapter discusses how to install OAC for Windows in a UAC network that includes an Infranet Controller and in a traditional wired or wireless network.

Before You Begin

Before you begin installing OAC, you should verify you have the appropriate access privileges and verify that Fast User Switching is disabled.

Verifying Access Privileges

You may require administrative privileges on your computer to install OAC. If the installer service is running on your machine, you do not need those privileges. However, some OAC tools, such as Odyssey Access Client Administrator, require that you have administrative privileges to use them.

Install a network adapter and associated driver software if your computer does not have one built in.

Disabling Fast User Switching

Fast user switching allows users to switch between user accounts on a computer without quitting applications and logging out. Fast User Switching can represent a security vulnerability, since non-authenticated user sessions might access desktop connections after an authenticated user logs into a protected network.

Fast User Switching can interfere with OAC operation when Remote Desktop (RDP) is running. After you disable Fast User Switching, Remote Desktop and OAC can interoperate without a problem.

By default, Fast User Switching is disabled for Windows XP computers that are part of a domain, and enabled for Windows XP computers that are part of a workgroup. Fast User Switching is enabled for domain users and workgroup users on computers running Windows Vista.

To disable Fast User Switching:

1. Select **Start > Control Panel > User Accounts > Change the way users log on or off**.

   The **Change the way users log on or off** setting does not appear unless you are part of a workgroup.

2. Clear the setting for **Fast User Switching**.

Requirements

This section describes the software and hardware requirements for OAC.

Supported Windows Operating Systems

OAC runs on the following Windows operating systems:

- Windows XP Professional with Service Pack 3
- Windows Vista Business Edition (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)

For information on supported platforms and Web browsers, see: https://www.juniper.net/techpubs/software/uac/4.xrelnotes/j-uac-ic-4.0r1-b14913-supportedplatforms.pdf.

Network Adapter Cards

On Windows XP, OAC is compatible with any wireless adapter card that supports standard 802.11 interfaces.

FIPS Edition Only: To use FIPS 140-2 compliant secure encryption, you must have an adapter driver installed that is compatible with the Juniper Networks FIPS module.

Wireless Adapter Requirement for Windows Vista and Windows 7

OAC requires native operating system WLAN miniport drivers for wireless network access. OAC does not support legacy XP WLAN miniport drivers on Vista or Windows 7. If you try to configure legacy wireless adapters in OAC, they display as an unknown adapter type.

Browsers

If your network includes an Infranet Controller, you must have Internet Explorer 6.0 or later installed, because OAC uses services present in Internet Explorer 6.0 to communicate with the Infranet Controller.

License

You must have a valid license to run OAC. Each OAC edition has a corresponding license key. See your system administrator for information about your license.

OAC for Windows supports Enterprise Edition and FIPS Edition licenses. If you install a FIPS Edition license on a computer running 64-bit Windows Vista, OAC operates in Enterprise Edition mode (not FIPS mode) with support for xSec.

You can purchase license keys from Juniper Networks. To install an OAC license, select **Help > License Keys**.

Installing OAC in a UAC Network

This section describes how to download OAC to your computer in a UAC network—one that includes an Infranet Controller.

1. Open a Web browser and navigate to the IP address for your Infranet Controller.

   Ask your administrator for the address information needed to access the Infranet Controller.

2. When you access the Infranet Controller, enter your authentication credentials, such as your username and password.

   After you are authenticated, the Infranet Controller downloads and installs a preconfigured copy of OAC to your computer based on your access privileges (realm and role). This default configuration provides the exact settings you need. Subsequent connections to the Infranet Controller might require that your OAC configuration be updated, in which case the update will be downloaded automatically to your system. The old version of OAC is removed before the new version is downloaded and your current configuration settings are maintained.

During installation, the following components are installed to support OAC in a UAC network:

- Network agent
- Juniper Universal Network Service (JUNS)
- Trusted Network Computing (TNC) client
- Tunnel manager

If you try to access the Web or protected resources on your corporate network before OAC is running, a network firewall might redirect your browser to a Web portal page that downloads and installs OAC on your system.

Network administrators can deploy OAC to multiple users with an MSI (Microsoft Installer) file. OAC may have default configuration settings but may not yet be configured specifically for the network resources you need to access. After OAC is running, navigate to an Infranet Controller, to download your initial OAC configuration settings automatically.

About Agentless Clients

For roles with restricted access, such as guest accounts, the Infranet Controller provides a transparent (“agentless”) connection through a web interface. When you access a protected network from an agentless connection, you do not configure settings.

Using Automatic Trust for Infranet Controllers

OAC is configured to trust an Infranet Controller automatically if it can verify that the Infranet Controller is passing a valid certificate. For this verification to occur, the trusted root CA certificate for the Infranet Controller must be installed on your computer. If the CA certificate is not installed, you cannot sign into the Infranet Controller.

During OAC installation, the Infranet Controller automatically installs the CA certificate on your computer. If you are prompted during installation, you must allow the installation of the CA certificate. If the trusted root CA certificate is preinstalled on your computer, then the prompt does not appear during installation.

Adding a Certificate to the Trusted Server Database

The first time that you navigate to the Web portal, you might be prompted to add a certificate to your trusted server database. This happens only if you do not have the certificate on your computer and if the certificate is available from the local trust server. If you choose not to accept the certificate and do not have temporary trust enabled, authentication to that trust server fails. See “Adding Authentication Servers or Intermediate CA Nodes” on page 93 for temporary trust settings.

Installing OAC for Windows in a Traditional Network

This section discusses methods for installing OAC in a network environment that does not include an Infranet Controller.

1. Run the OAC installer using one of the following procedures:

   - Insert the installation CD-ROM into your CD-ROM drive. The installation process starts automatically. If the installation process does not start, double-click setup.exe on the CD-ROM.

   - Download and double-click the installer for the OAC file (OdysseyAccessClient.msi).

   The installation wizard displays a series of installation prompts. Respond to each prompt and click **Next** to continue.

2. Click **Install** to begin the installation process.

After OAC is installed, you might be prompted for additional information needed to use OAC.

NOTE: If your administrator configures the OAC single (automatic) sign-on feature, you are not prompted for credentials.

Chapter 3

Using Odyssey Access Client Manager

This chapter presents an overview of how to use the Odyssey Access Client Manager application to configure OAC.

Opening Odyssey Access Client Manager

OAC runs as a service on Windows computers. To open Odyssey Access Client Manager, double-click the OAC icon in the system tray or choose **Start > Programs > Juniper Networks > Odyssey Access Client > Odyssey Access Client Manager**.

Logging In to Odyssey Access Client Manager

When you open Odyssey Access Client Manager, a dialog box may prompt you for authentication credentials. The specific credentials required depend on your company's authentication policy. The credential types that you can use with OAC include the following:

- Login name and password.
- Certificate (required for EAP-TLS authentication).
- Soft token.
- SIM card. You can use this method with a SIM card reader and, most commonly, with the Windows Mobile version of OAC.
- Smart card.

The methods allowed vary based on your company and whether or not you are connecting remotely. In most cases, a login dialog box indicates what is required. Ask your administrator about the required login credentials for your corporate network.

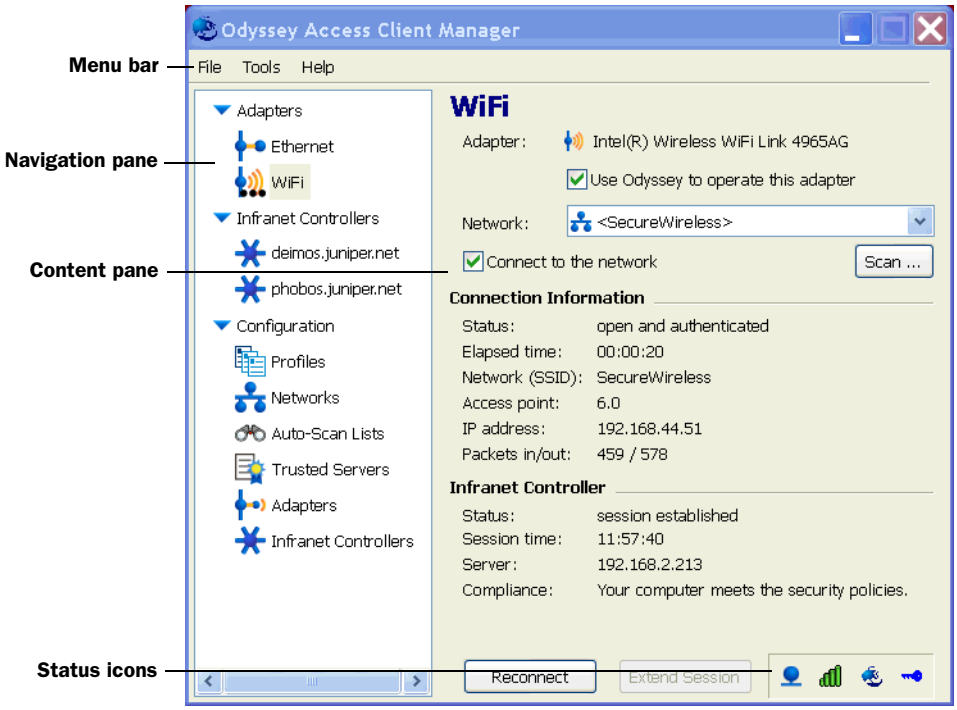
Using Single Sign-On

If OAC has been configured for single (automatic) sign-on, there is no prompt for credentials before Odyssey Access Client Manager opens. Similarly, if an Infranet Controller has been configured for single sign-on, there is no prompt for credentials. In both cases, your Windows login credentials are used.

Odyssey Access Client Manager User Interface

Figure 4 on page 14 identifies the components of a standard window in the Odyssey Access Client user interface.

Figure 4: Odyssey Access Client User Interface



The Odyssey Access Client Manager user interface consists of the following:

- The menu bar provides a range of options. See “Odyssey Access Client Manager Menu Bar” on page 15 for information on the Odyssey Access Client Manager menu bar.
- The navigation pane displays lists of configured adapters and Infranet Controllers and a set of named icons that you can use to perform configuration tasks. See “Navigation Pane” on page 18 for information on the Odyssey Access Client Manager navigation pane.
- The content pane displays the user interface controls that correspond to the selection you make in the navigation pane. See “Content Pane” on page 21 for information on the Odyssey Access Client Manager content pane.
- The status icons at the bottom right indicate your current security compliance status, wireless signal power, authentication status, and encryption status. See “Informational Graphics and Detailed Status” on page 19 for information on how to interpret the OAC status icons.

If you are new to OAC, you should spend some time exploring each option to become familiar with the Odyssey Access Client Manager user interface.

Odyssey Access Client Manager Menu Bar

The Odyssey Access Client Manager has three menus: File, Tools, and Help. A fourth menu (View) may appear in the menu bar if your network administrator has configured Odyssey Access Client Manager to hide one or more settings by default.

File Menu

The File menu includes the following items:

- **Forget Password**—Discards the current password or PIN that you used to log on. If your password is required later, a dialog box prompts you for it. If you do not select this option, OAC remembers your password for the duration of the session. See "Using Forget Password" on page 33.

- **Forget Temporary Trust**—Discontinues a temporary trust setting for a server. See "Using Server Temporary Trust" on page 35 and "Adding a Trusted Server" on page 91.

- **Clear Cached Credentials** (**FIPS Edition Only**)—Securely clears all cryptographic keys and other critical security parameters from memory. While this process takes place, it briefly interrupts network traffic, which requires OAC to reestablish a new connection and negotiate new cryptographic keys.

  Use this option any time you leave your computer unattended or when you need to transfer control of a shared computer to another user.

- **Close**—Closes the Odyssey Access Client Manager window display. To reopen it, double-click the program icon in the system tray.

- **FIPS Mode On / FIPS Mode Off** (**FIPS Edition Only**)— Turns FIPS mode on or off.

  Use this option if your network security policy requires FIPS encryption. This option does not appear unless you have installed an OAC FIPS license. See "About FIPS Mode (FIPS Edition Only)" on page 6.

View Menu (Hidden Settings)

Your network administrator can configure Odyssey Access Client Manager to hide OAC features and settings that you do not need. The View menu appears only if any of the settings listed below have been hidden:

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

- Infranet Controllers

Use the View menu to show hidden options or to hide them again.

Locked Settings

An administrator can lock (restrict) access to specific features or options even though they appear in the UI. For example, auto-scan lists may be disabled for all users or for logical groups of users based on a role. If you attempt to use such options or features, the top of the dialog box for the option indicates that it is "read only," meaning that you cannot use it.

Tools Menu

The Tools menu includes the following items:

- Odyssey Access Client Administrator—Manages and deploys OAC configurations. It is only available if you have administrative privileges.
- SIM Card Manager—Manages SIM card PIN settings. See "Managing SIM Card PIN Settings" on page 32.
- Survey Airwaves—Displays Wi-Fi and peer-to-peer networks in your vicinity. See "Surveying Local Wi-Fi Airwaves" on page 30.
- Logs—Opens the Log Viewer and displays the current contents of the debuglog.log file. See "Viewing Logs" on page 99.
- Diagnostics—Displays a variety of diagnostic information that is helpful for troubleshooting. See "Viewing Diagnostics" on page 100.
- Run Script—Runs scripts to update your OAC configuration. See "Running a Script Manually" on page 31.
- Check New Scripts—Checks the default directory for new scripts deployed by your administrator. See "Checking for New Scripts" on page 31.
- Preferences—Toggles the display of the system tray icon, the control panel icon, and the OAC splash screen.
- Windows Logon Settings—Overrides the default setting for network connection timing. See "Managing Windows Login Settings" on page 38.
- Options—Accesses the following tabbed areas:
  - Security
    - Enable session resumption—Restricts session resumption for any session older than the time that you set. See "Using Session Resumption" on page 33.
    - Enable automatic reauthentication—Enables periodic automatic reauthentication and sets the reauthentication frequency setting. See "Using Automatic Reauthentication" on page 34.

- Enable server temporary trust—Allows you to be authenticated on a network whose authentication server is not yet configured as trusted in the Trusted Servers dialog box. See “Using Server Temporary Trust” on page 35.
- Enable temporary network support—Lets you control whether OAC maintains or deletes an SSID from a scanned wireless connection. See “Using Temporary Network Support” on page 36.
- Prompt for smart card PIN—Enables OAC to prompt for a smart card personal identification number (PIN). See “Managing SIM Card PIN Settings” on page 32.

- Interfaces
  - Wireless suppression—Defaults to a wired network connection whenever it is available to preserve wireless bandwidth for users who do not have a wired connection. See “Using Wireless Suppression” on page 30.
  - Manage wired/wireless adapters—Enables OAC to automatically configure any wired or wireless adapter. See “Managing Global Settings for Adapters” on page 44.
- Preemptive Networks—Specifies an auto-scan list of networks that, if found, take precedence over any network or auto-scan list currently enabled in the connection dialog box when searching for a network.

NOTE: Preemptive networks affect *which* networks to search for and in what order to search. They do not affect *when* to search. If you select the Switch to a preferred network check box for an auto-scan list, OAC actively monitors the SSIDs being broadcast so that, if an SSID higher up on the list is detected, OAC switches to that network. This feature requires SSIDs to be broadcast to be effective.

- EAP-FAST—Controls when OAC prompts for EAP-FAST credentials. See “Managing EAP-FAST Credentials” on page 36.
- Notifications—Controls the display of notification messages relating to authentication and network connection status. See “Managing Notification Settings” on page 37.
- Default Login Name—Modifies the default login name format that appears in any authentication profile you create. The option appears in Odyssey Access Client Manager only if your administrator has enabled it. Rarely used, it allows you to set up a login name format when the network to which you need to connect has a different login name format requirement from the configured default.

Help Menu

The Help menu includes the following items:

- Help Topics—Opens the OAC online help interface.
- License Keys—Shows when the current OAC license expires and whether to add or remove an OAC license key if you have permission.
- Odyssey Access Client User Page—Accesses the Juniper Networks Customer Support webpage.
- Juniper Networks Home Page—Accesses the home page for Juniper Networks.
- Purchase Information—Accesses the Juniper Networks webpage to buy other products.
- About—Shows the specific release version of OAC.

Navigation Pane

The navigation pane contains a group of options, each of which contains one or more items that you can configure or use for connecting to the network. The selection that you make determines which content dialog box appears. If this is your first experience with the Odyssey Access Client Manager, explore the options and the selections that you can make and notice how the content area changes for each selection.

Adapters List

The Adapters list shows the wired and wireless adapters configured in OAC. Select an adapter from this list to display its network connection status in the content pane on the right.

Infranet Controllers List

The Infranet Controllers list shows each Infranet Controller that has been configured in OAC. Select an Infranet Controller from this list to display its connection status and settings.

Configuration

The Configuration folder lists categories of OAC configuration settings.

Profiles

Sets up collections of login and authentication configuration information, such as your password or certificate. See Chapter 6, “Configuring Authentication Profiles” on page 49.

Networks

Configures settings for wired and wireless networks, such as a network's connection type, encryption type, and whether to use 802.1X authentication. You can use these networks to populate your auto-scan lists. See Chapter 7, "Configuring Wireless Networks" on page 73.

Auto-Scan Lists

Sets up an ordered list of wireless networks with which you want to establish a network connection. Auto-scan lists are convenient when you move your computer from one location to another, since OAC can scan for networks in the list to keep you connected automatically. See Chapter 8, "Managing Auto-Scan Lists" on page 81.

Trusted Servers

Configures trusted network servers and sets certificate and identity information for the servers that can authenticate you when you connect. Configuring trusted servers is required for protocols that implement mutual authentication. See Chapter 10, "Managing Trusted Servers" on page 89.

Adapters

Configures wired and wireless adapters for your computer. See Chapter 5, "Managing Network Adapters" on page 43.

Infranet Controllers

Configures the names and URLs of Infranet Controllers to which you need to connect. See Chapter 9, "Managing Infranet Controller Connections" on page 85.

Informational Graphics and Detailed Status

Status icons in the lower right corner of the Odyssey Access Client Manager window indicate the power, authentication, and encryption status of your OAC connections. Click a status icon to displayed detailed status information.

Signal Power Status Icons

Signal power status icons indicate the wireless signal strength between your PC and an access point. More colored bars indicate a stronger signal.

Figure 5: Signal Power Status Icons

When an adapter dialog box is active, you can press Alt + 1 to display signal power information.

Connection Status Icons

The OAC icon identifies the current authentication and connection status between OAC and a network or Infranet Controller:

- Empty icon (no color)—No connection. OAC is disabled or is not maintaining a network or Infranet Controller connection.

- Red icon—A connection has failed authentication. This condition does not reflect a connectivity failure.

- Black icon—A Layer 2 or Layer 3 connection is open but has not been authenticated.

- Blue icon—An authenticated Layer 2 or Layer 3 connection is open.

If the state of a connection changes, the color of the icon changes accordingly.

When an adapter dialog box is active, you can press Alt + 2 to display connection status information.

Encryption Key Status Icons

The encryption key status icon indicates whether encryption keys are in use for this connection:

- Blank key icon—Data is not encrypted.

- Black key icon—Data is encrypted using static keys.

- Blue key icon—Data is encrypted using dynamic keys (802.1X).

When an adapter dialog box is active, you can press Alt + 3 to display encryption key information. Encryption status details include the following types of information:

- Global encryption—The size (in bits) of global encryption keys
- Access point encryption—The size (in bits) of the encryption key.
- Global encryption— Pairwise Cipher and Group Cipher encryption status
- Access point encryption—The size (in bits) of access point encryption key

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

Content Pane

The content pane displays the user interface controls that correspond to the selection you make in the navigation pane. For example, if you select a network adapter from the Adapters list in the navigation pane, the content pane displays connection status information for the specified adapter. Similarly, if you choose Profiles from the Configuration list in the navigation pane, the content pane displays the profiles you have configured and lets you add, remove, or modify profiles.

Exiting from Odyssey Access Client Manager

To exit from Odyssey Access Client Manager, do one of the following:

- hoose **File > Close** or right-clickthe OAC icon in the system tray and select **Exit**.

You can relaunch Odyssey Access Client Manager at any time by double-clicking the system tray icon.

Chapter 4

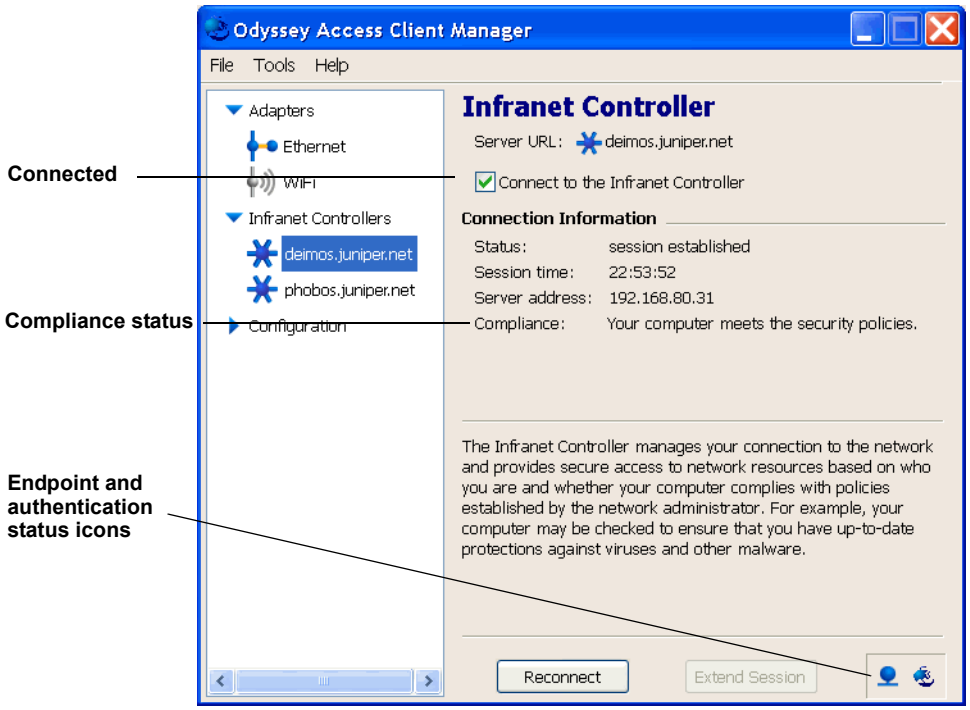
Managing Connections

This chapter describes how to use Odyssey Access Client to connect to Infranet Controllers and wired/wireless networks.

Connecting to an Infranet Controller

You must be authenticated before you are allowed access to protected network resources. This means that the first time you connect to an Infranet Controller during an OAC session, you must sign on by providing the required credentials. See Figure 6 on page 23.

Figure 6: Infranet Controller Dialog Box



To connect to an Infranet Controller:

1. Click **Infranet Controllers** in the navigation pane.
2. Choose the Infranet Controller to which you want to connect.

An Infranet Controller dialog box displays the IP address of the Infranet Controller in the **Server URL** field.

If the Infranet Controller you want does not appear in the list, you may need to configure it. Refer to Chapter 9, "Managing Infranet Controller Connections" on page 85 for information on configuring Infranet Controllers.

3. Select the **Connect to the Infranet Controller** check box.

4. When the prompt appears, enter your username and credentials to sign on to the Infranet Controller. You may need to select a realm and a role. (See "Setting a Preferred Realm and Role" on page 70.) After being authenticated, you can access the protected network resources to which you have been granted access.

NOTE: When you connect to an Infranet Controller, a pop-up window might prompt you to install a newer version of OAC if one is available.

After you are connected, the Infranet Controller dialog box displays your trust status. If your computer does not meet security policy requirements, you might be redirected to a remediation VLAN—a restricted-access network where your computer is updated for security compliance—before you can be authenticated by the Infranet Controller. See "Compliance Failure and Remediation" on page 25.

The Reconnect button at the bottom of the dialog box reinitializes the connection. Sometimes an authentication or connection request may be in an unknown state. For example, the authentication server may drop the request if it is particularly busy. Click **Reconnect** to reestablish your connection to the Infranet Controller.

Managing Concurrent Infranet Controller Sessions

A *session* is a single authenticated connection between your computer and an Infranet Controller. You can connect to multiple Infranet Controllers or to the same Infranet Controller with multiple concurrent sessions. This typically requires that you have an authentication profile for each Infranet Controller.

You might maintain connections to more than one Infranet Controller if you need access to network resources protected by different Infranet Controllers. To connect to multiple Infranet Controllers, create a profile and Infranet Controller configuration for each instance.

Infranet Controller Session Limits

Your administrator can restrict the number of simultaneous Infranet Controller sessions per realm that you can maintain. If you try to open an additional session when you have the maximum number of sessions running, you are prompted to terminate an existing session or cancel the new session request.

Extending the Current Infranet Controller Session

Click **Extend Session** (located at the bottom of the Infranet Controller session dialog box) to reset the counter on your current session. The counter shows the amount of time remaining for the session. This feature is intended for situations where you need more time to accomplish a task than remains in the session.

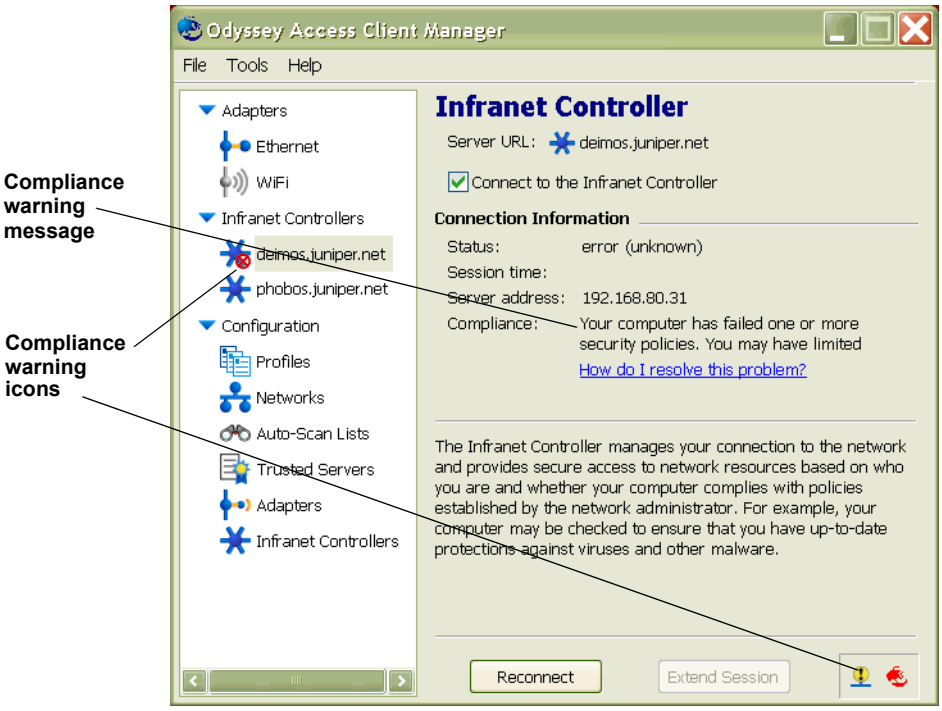
You may be prompted to reenter your authentication credentials to extend your session. For example, if you use a token card for authentication, OAC may prompt for a new token ID.

NOTE: Access to this option depends on the role defined for you on the Infranet Controller. If Extend Session is disabled for users with your role, the button is dimmed.

Compliance Failure and Remediation

If your computer hardware or software does not comply with the network security policy, the connection icons indicate that there is a compliance problem (see Figure 7). If a compliance issue is detected, the connection might be rejected or you might be prompted to take remediation action. In some cases, remediation is automatic. In other cases, the connection dialog box displays a message with instructions on what to do.

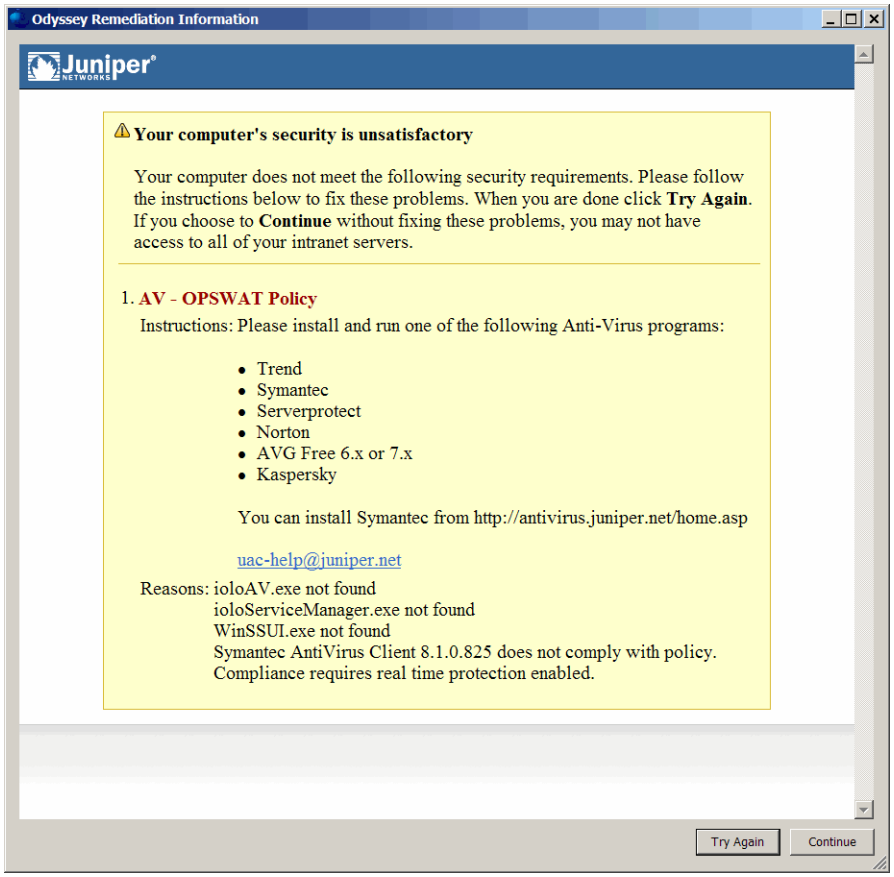
Figure 7: Compliance Failure Indicators



Responding to Remediation Messages

Click the **How do I resolve this problem?** link for specific instructions on updating your computer to meet compliance requirements. The remediation instructions that you see might vary from the sample shown in Figure 8.

Figure 8: Remediation Instruction Dialog Box



Disconnecting from an Infranet Controller

Disconnecting from an Infranet Controller signs you off and terminates the current connection to the protected resources to which you had access. The Infranet Controller remains part of the OAC configuration unless you remove it. Thus, you can connect to the same Infranet Controller later.

To disconnect from an Infranet Controller:

1. Click the **Infranet Controllers** list in the navigation pane.
2. Select the Infranet Controller from which you intend to disconnect.
3. Clear the **Connect to the Infranet Controller** check box.

Connecting to a Wired Network

OAC provides authentication support for 802.1X networks. You must have a 802.1X-capable network adapter configured in OAC. You must also have a valid authentication profile for each wired network.

OAC does not provide authentication services for switches that do not support 802.1X.

To connect to a wired 802.1X network:

1. Click **Adapters** in the navigation pane and select the appropriate wired adapter (which may be called Ethernet in the Adapters list).

2. Select an authentication profile from the **Profiles** list.

   Refer to Chapter 6, "Configuring Authentication Profiles" on page 49 for information on how to set up an authentication profile.

3. Select the **Connect to the network** check box to start the network connection.

The dialog box shows the connection status. If there are connection errors, the OAC icon in the system tray changes colors and may display a message indicating the cause of the failure.

Connecting to a Different Network

To change networks or use a different adapter:

1. In the Wi-Fi or Ethernet adapter dialog box, clear the **Connect to the network** check box.

2. Based on the type of wired or wireless adapter you are using, select a network or profile name from the drop-down list that corresponds to the network to which you want to connect.

3. Select the **Connect to the network** check box.

Reconnecting to a Network

Click the **Reconnect** button (located at the bottom of the Adapter dialog box) to reinitialize your network connection if the current connection does not seem to be performing as expected.

The reconnect option disconnects the existing connection for the selected adapter and starts a new connection to the network. The new connection might be to a different access point (on the same network) from your previous access point connection. If you are authenticated for access the network, you will remain authenticated when the new connection starts. Any dynamic encryption keys are refreshed with the reconnection.

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

Disconnecting from a Network

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

To disconnect from the current wireless network:

1. Click **Adapters** and select the adapter that you want to disconnect from the network.

2. Clear the **Connect to the network** check box. When you disable the connection to the network, the adapter icon changes to gray.

Connecting to a Wireless Network

To connect to a wireless network:

1. Click **Adapters** in the navigation pane and select the appropriate wireless adapter (which may be called WiFi in the Adapters list). See Figure 9 on page 29.

2. Select a wireless network from the **Network** list in the Wi-Fi dialog box.

3. Click **Connect to the network** to start the network connection.

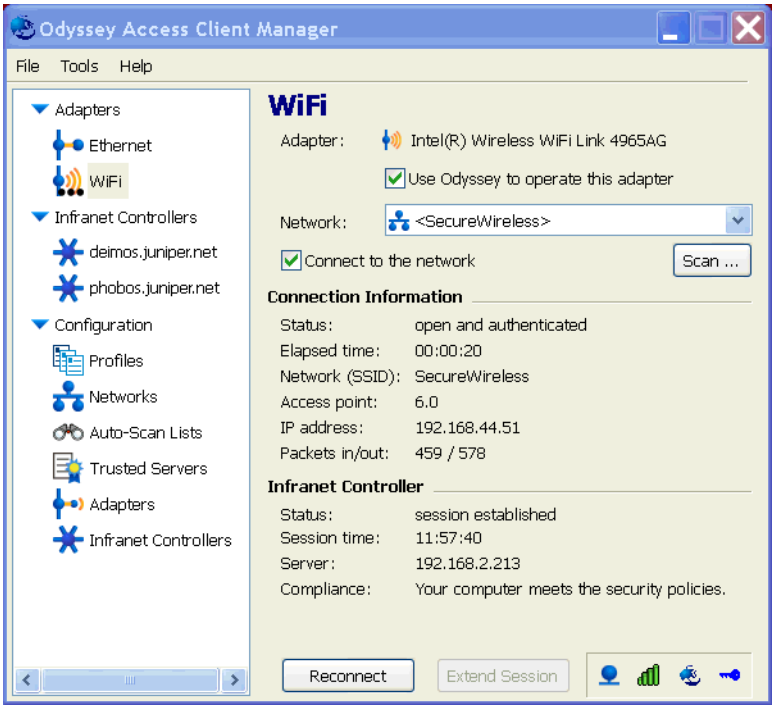
The network list displays the networks that you configured in the Networks dialog box and the auto-scan lists that you created in the Auto-Scan Lists dialog box. Network names appear in angle brackets, after any network description text that you have specified. Networks and auto-scan lists use the following icons:

 = auto-scan lists

 = networks

The Wi-Fi dialog box shows connection status. If a connection error occurs, the OAC icon in the system tray changes colors and may display a message indicating the cause of the failure.

Figure 9: WiFi Dialog Box



Reconnecting to a Wireless Connection

Wireless network connections are not always as reliable and stable as a wired connection and, from time to time, need to be refreshed. Click the **Reconnect** button at the bottom of the dialog box to reinitialize the connection.

Scanning for a Wireless Network

An *SSID* (service set identifier) is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must use the same SSID to communicate with each other. Public WLANs (such as those found in airports or coffee shops) frequently broadcast their SSID to facilitate user access.

OAC can scan for wireless networks that broadcast an SSID. To connect to a wireless network by scanning:

1. Click **Scan** in the Wi-Fi dialog box.

   OAC displays tabs listing the names and relative signal strengths of wireless networks being offered by access points and by network peers.

2. Select the network you want from the appropriate scan list.

3. Click **OK**.

NOTE: If a wireless access point does not broadcast a network SSID, you must obtain the network SSID and configure the network in OAC before you can connect to it.

Using Auto-Scan Lists

An auto-scan list is a prioritized list of previously configured wireless networks. With an auto-scan list, OAC surveys the airwaves looking for a preferred network, and connects to a preferred network if one becomes available. See Chapter 8, “Managing Auto-Scan Lists,” on page 81 for information about creating and using auto-scan lists.

Making Concurrent Network Connections

Each adapter on your computer can connect to a different network. If you have both wired and wireless adapters, you can maintain simultaneous network connections.

Use the Adapter list to monitor the status of your network connections.

Using Wireless Suppression

Wireless suppression lets you default to a wired network connection and to use a wireless network connection only when a wired connection is not available. Wireless suppression lets you use the fastest connection available to you, and preserves wireless bandwidth for users who do not have a wired connection.

To configure wireless suppression:

1. Click **Tools > Options > Interfaces.**
2. Select the **Wireless suppression: Use wireless connection only when no wired (Ethernet) connection is present** check box.
3. Click **OK**.

Session Management Tasks

Odyssey Access Client Manager provides several tools and options for managing your session after you are connected. The following sections describe those tools and options and how to use them.

Surveying Local Wi-Fi Airwaves

Surveying airwaves for available Wi-Fi networks lets you see detailed information about the Wi-Fi networks in your location. The Airwaves Survey dialog box displays the name and relative signal strength of each wireless network, along with information about access channels and association types.

To survey airwaves for available wireless networks, select **Tools > Survey Airwaves**

Viewing Network Signal Strength

The relative signal strength of each network is indicated graphically on the far left of the Airwaves Survey dialog box. Stronger signals are indicated with more colored bars than weaker signals. The networks that broadcast a weaker signal are shown in yellow with two bars, while the networks that broadcast a stronger signal are shown in green with three or four bars.

You can sort the list of networks by clicking a column heading. For example, to sort by service set identifier (SSID), click the **SSID** heading.

To view broadcast details about a network, select the network in the list and click click **Details**. The BSSID Information dialog box displays Basic Service Set Identifier settings and rates for the network.

Using Scripts

Scripts let you update your Odyssey Access Client configuration settings quickly and easily. Scripts can be distributed as email attachments, as files on memory cards or CD. OAC supports manual scripts (which you run from the Odyssey Access Client Manager user interface) and automatic scripts (which run without user interaction).

The default storage location for Odyssey Access Client scripts is:

C:\Documents and Settings*username*\Application Data\Funk Software\Odyssey Client\newScripts

The \Application Data directory might be hidden on your machine. If so, contact your administrator for information on how to proceed.

Running a Script Manually

Your network administrator might ask you to run a script to update your OAC configuration. The instructions from the administrator might include a path location to the script.

To run a script:

1. Select **Tools > Run Script** from the Odyssey Access Client Manager menu bar. The Select Script File dialog box appears.
2. Navigate to the location containing the script that your administrator has instructed you to run.
3. Select the script and click **Open** to run the script.

Checking for New Scripts

To check for new scripts:

1. Select **Tools > Check New Scripts** from the Odyssey Access Client Manager menu bar. The New Odyssey Client Scripts dialog box displays a list of new configuration scripts.
2. Click **Run** to run the script and update your OAC configuration. You can run only one script at a time.
3. Click **Delete** to delete the script.

Managing SIM Card PIN Settings

A SIM (Subscriber Identity Module) card is an electronic card present in some mobile wireless devices and used to identify a subscriber to the network. You can use a SIM card for OAC authentication if it is inserted in your client computer. You can also use OAC to manage the PIN on your SIM card hardware.

Opening SIM Card Manager

Select **Tools > SIM Card Manager** from the Odyssey Access Client Manager menu bar. The SIM Card Manager dialog box appears. You can perform the following tasks:

- Disable the PIN for a SIM card.
- Change the PIN for a SIM card.
- Unblock the SIM card.

Disabling a SIM Card PIN

To disable the PIN for your SIM card:

1. From the SIM Card Manager dialog box, select **Disable PIN** to open the Disable PIN dialog box.
2. Enter your PIN.
3. Click **OK**.

Changing a PIN for a SIM Card

To change the PIN for your SIM card:

1. From the SIM Card Manager dialog box, select **Change PIN** to open the Change PIN dialog box.
2. Enter the current PIN in the **Please enter the current PIN** box.
3. Enter the new PIN in the **Please enter the new PIN** box.
4. Enter the same new PIN in the **Please confirm the new PIN** box.
5. Click **OK**.

Unblocking a SIM Card

If you enter the wrong PIN too many times, your SIM card might become blocked.

To unblock a SIM card:

1. From the SIM Card dialog box, select **Unblock Card** to open the Unblock Card dialog box.
2. Follow the instructions on the Unblock Card dialog box.
3. Click **Close** to close the SIM Card Manager dialog box.

Enabling the Prompt for a Smart Card PIN

Select **Tools > Options > Security** tab from the Odyssey Access Client Manager menu bar. Odyssey Access Client Manager prompts for a smart card Personal Identification Number (PIN). The PIN unlocks the certificate stored on the smart card so it can be used for authentication credentials. The option is enabled by default.

With the option disabled, the smart card middleware manages PIN prompts and PIN caching.

To have Odyssey Access Client Manager prompt for a smart card PIN, your authentication profile must be enabled by selecting **Permit login using my certificate** and **Use the login certificate from my smart card reader**. See "Using Certificates for Authentication" on page 53.

Caching a Smart Card PIN

Select the **Cache PIN** option to cache the smart card PIN that you enter so OAC does not prompt again for the same PIN. If you disable this option, OAC clears the PIN information from the cache and does not cache the PIN when a PIN prompt occurs. The cache is also cleared when you log out. This option is enabled by default.

NOTE: (FIPS Edition Only) Smart card prompts and caching are disabled if FIPS mode is enabled.

Using Forget Password

When you are authenticated for the first time, you must enter a valid password as part of the login process—except in the case of single sign-on. OAC remembers the password that you enter and uses it for any subsequent authentications without prompting you. Normally, OAC remembers the password that you provide until you reboot your computer or restart OAC.

If you leave your system unattended and want to protect OAC from unauthorized access or if you share a computer with other users (such as in a test lab), you might want to select the **Forget Password** option from the Odyssey Access Client Manager menu bar as a security measure.

To discard (forget) the current password or PIN you used to start an authenticated network connection, select **File > Forget Password**. If your password is required again, you are prompted to enter it.

Using Session Resumption

After you have been authenticated for network access and a network connection is open, your network session begins. During a session, any subsequent authentications to the same network server can be accelerated by reusing the secret information that is derived during the first authentication. This is called *session resumption*. With session resumption enabled, you can restrict session resumption for any session older than the time that you set. The default is 12 hours.

You can configure client-side session resumption features that apply to certificate-based protocols (such as TLS) using OAC. See “Session Resumption” on page 114.

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

Enabling Session Resumption

To enable session resumption:

1. Select **Tools > Options > Security** from the Odyssey Access Client Manager menu bar.
2. Click **Enable session resumption**.
3. Set the maximum number of hours that a session can last before requiring reauthentication in the **Do not resume sessions older than** box. After the time limit has elapsed, OAC requires a new authentication sequence.

Disabling Session Resumption

To disable session resumption:

1. Select **Tools > Options > Security** from the Odyssey Access Client Manager menu bar.
2. Clear **Enable session resumption**.

Using Preemptive Networks

You can create a preferred auto-scan list, for which OAC scans before connecting to other networks. For information on using a preemptive auto-scan list, see “Specifying a Preemptive Auto-Scan List” on page 82.

Using Automatic Reauthentication

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

If enabled, this option enables periodic automatic reauthentication and sets the reauthentication frequency setting. The default is one hour. 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 computer and access point. The access point might use these shared keys to refresh the keys used to encrypt data. By frequently refreshing keys, you can thwart cryptographic attacks.

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

Enabling Automatic Reauthentication

To enable automatic reauthentication:

1. Select **Tools > Options > Security** from the Odyssey Access Client Manager menu bar.
2. Click **Enable automatic reauthentication**.
3. Enter the frequency (in hours) in the Reauthenticate every box.

Disabling Automatic Reauthentication

To disable automatic reauthentication:

1. Select **Tools > Options > Security** from the Odyssey Access Client Manager menu bar.
2. Clear the **Enable automatic reauthentication** check box.

Using Server Temporary Trust

Most of the time, you can use the Trusted Servers dialog box to configure the servers you trust for authentication. However, there might be times when you request authentication from a network whose authentication server is not yet configured as trusted in the Trusted Servers dialog box. In this case, you might want the ability to enable temporary trust for that untrusted server.

If enabled, this option enables temporary trust of a server and sets the maximum length of time for trusting that server.

If temporary trust is enabled, you can trust an untrusted server temporarily during a network authentication. Consequently, the temporary trust feature provides an alternative to configuring trusted servers in OAC.

Enabling Temporary Trust

Temporary trust is enabled by default. If you need to enable temporary trust:

1. Select **Tools > Options > Security** from the Odyssey Access Client Manager menu bar.
2. Click **Enable server temporary trust**.
3. Specify the maximum time (in hours) for OAC to continue to trust a server.

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

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

Disabling Temporary Trust

Temporary trust is enabled by default. To disable temporary trust:

1. Select **Tools > Options > Security** from the Odyssey Access Client Manager menu bar.
2. Clear the **Enable server temporary trust** check box.

Using Temporary Network Support

By default, when you connect to a wireless network by scanning the airwaves, OAC saves the network SSID. While this is a convenience, storing a discovered SSID might represent a security risk, since an attacker can broadcast an SSID to spoof a trusted network.

By enabling temporary networks, you can set a time-out value so that if you disconnect from that network and do not reconnect to it before the time-out value expires, OAC discards that network SSID. The network SSID in the scan list includes a prefix to indicate that it has been deleted.

OAC supports only one temporary network at a time. Thus, with temporary networks enabled, if you scan and connect to a second temporary network, the first temporary network is deleted.

Enabling Temporary Network

To enable a temporary network and set a time-out value:

1. Select **Tools > Options > Security** from the Odyssey Access Client Manager menu bar.
2. Click **Enable temporary network support**.
3. Specify a time-out value from 1 minute to 6 hours. The default value is 20 minutes.

NOTE: A temporary network cannot be added to an auto-scan list.

Managing EAP-FAST Credentials

EAP-FAST is similar to EAP-PEAP in that both methods use a secure encrypted tunnel and inner authentication methods. EAP-FAST uses protected access credentials (PACs) instead of digital certificates to set up the encrypted tunnel. EAP-FAST supports both IEEE 802.1X and IEEE 802.11i.

To enable EAP-FAST authentication:

1. Select **Tools > Options > EAP-FAST** from the Odyssey Access Client Manager menu bar.

2. Select one or both of the following options to determine when to prompt for PAC credentials:

   - **Prompt before acquiring credentials from a new server** —Prompts for new credentials whenever you are authenticated by a new server.

   - **Prompt before replacing credentials from a known server when your existing credentials have failed**—Prompts for new credentials if a previous authentication attempt fails.

Managing Notification Settings

Notifications are text messages in a pop-up balloon or dialog box indicating that the status of a network connection or authentication has changed. Notifications appear because of network issues or because of changes in your compliance with your network security policy.

Managing How Notifications Appear

If you want Odyssey Access Client Manager to display notifications in dialog boxes instead of pop-up balloons:

1. Select **Tools > Options > Notifications**.

2. Click **Use dialog boxes instead of balloons.**

To disable notifications:

1. Select **Tools > Options.**

2. Click the **Notifications** tab.

3. Click **Disable notifications**. With notifications disabled, the only indicator of a state change is a change in the color of the OAC icon in the Windows system tray.

Controlling the Display Time for Notifications

You can set the duration of a notification message and the amount of time to wait between notifications:

1. Select **Tools > Options.**

2. Click the **Notifications** tab.

3. Specify how long notifications should remain open in the Display notifications for field.

4. Specify how long subsequent warning and failure messages should remain open in the **Subsequent warning messages** and **Subsequent failure messages** fields.

5. Click **OK**.

Managing Windows Login Settings

This option lets you control network connection timing if it is present in your configuration. Your administrator can disable this option for individual users.

NOTE: Changing your login timing may affect other startup processes. Check with your administrator before using this option.

To modify the default timing of Window login:

1. Select **Tools > Windows Logon Settings**.
2. Select the **Override default settings for Windows logon** check box.
3. Select from the following Windows login timing options (if they are available):
   - **After my desktop appears**—Establishes your network connection after all Windows startup, login, and desktop processes are completed. This is the latest possible time that you can make a network connection.
   - **After Windows logon, before the desktop appears**—Establishes your network connection after your Windows startup and Windows login processes are completed but before your desktop processes take place.
   - **Prior to Windows logon**—Establishes your network connection prior to Windows login.
4. If you selected **Prior to Windows logon**, perform the following required tasks and options:
   a. Select the adapter and network (or profile, in the case of a wired connection) from the lists provided. Note the following:
      - You must associate a profile with any network that you configure. Select **Configuration > Profiles > Properties > Authentication** from the navigation pane. OAC uses your Windows login credentials.
      - You cannot assign a profile that uses a stored password for this network connection.
      - If you configure the network to encrypt your data using WEP, select **Keys will be generated automatically** for data privacy on the Network Properties dialog box for the selected network.

   b. Select the **Use alternate settings on failure** option if you can provide an alternate wired 802.1X adapter and profile (or wireless adapter) to use for connections that take place prior to Windows login when a connection attempt using the displayed adapter or network pair fails.

A practical use of this option is to provide an alternate 802.1X wired adapter and profile for connections that take place prior to Windows login. After selecting this option, click **Edit Alternate Settings** to select the alternative adapter and profile. Configure the alternative adapter and profile before you can configure alternate settings for this option.

c. Select an option to be prompted prior to making the network connection at login time according to the choices under Prompt to connect.

- **Never**—Does not prompt to connect, even if the connection attempt fails.
- **On connection failure**—Prompts only on connection failure. This can be useful if you experience network authentication problems, as it lets you opt out of connecting to the network at login time.
- **Prior to connecting to the network**—Prompts each time you connect.

5. If you select either of the prior to desktop connection timing options, you can defer the timing of such connections under certain circumstances. To do so, select **Wait until my desktop appears before using Odyssey to connect to the network**. You have two options that depend on the adapter type for a connection that takes place after the desktop appears:

- Select **Any wired adapter**. You can use this option even if your wired adapter is not connected to an 802.1X hub or switch.
- Select **One of the following adapters**. This option applies to any adapter listed on the Windows Logon Settings dialog box.

Editing the List of Adapters

If you select **One of the following adapters** in the previous step, select the adapters as follows:

1. Select **Tools > Windows Logon Settings**.
2. Select the **Override default settings for Windows logon** check box.
3. Select **After Windows logon, before the desktop appears**.
4. Click the **Wait until my desktop appears before using Odyssey to connect to the network** check box, and then click the **One of the following adapters** option button. Then do the following:
5. Click **Edit** to open the Adapters dialog box.
6. Select any adapters that you want to use for a network connection that occurs after the desktop appears.
7. Click **OK** to close the Select Adapters dialog box.
8. Click **OK** to close the Windows Logon Settings dialog box.

Using Prior-to-Windows-Login Behavior and Smart Cards

If you are connecting prior to Windows logon with a profile that is configured for smart card certificate use with EAP-TLS, as well as one or more password-based authentication protocols, then Odyssey Access Client behaves differently if you log on with your smart card PIN:

- If you log in to Windows with your smart card PIN, then the smart card certificate is used with EAP-TLS throughout the session. None of the password-based protocols are negotiated.
- If you log in to Windows with your password, then the password-based protocols are negotiated according to their listed order on the profile, and EAP-TLS is never negotiated.

Odyssey Access Client Administrator

Odyssey Access Client Administrator is a set of tools for managing and deploying OAC configurations. These are advanced tools that are not available to all users. See the *Odyssey Access Client Administration Guide* before using this tool. Your configuration may not provide access to this tool.

Troubleshooting

The following sections provides basic troubleshooting tips.

Viewing Log Files

Your network administrator may ask you to use the Log Viewer tool if you are experiencing problems with OAC.

To use the Log Viewer tool:

1. Select **Tools > Logs** to display the current contents of the debuglog.log file.
2. Set the level of logging information displayed by clicking **Settings**. See “Viewing Logs” on page 99.

Running Diagnostics

Use this tool to enable and display diagnostic information and send the data in an e-mail message for troubleshooting.

To run diagnostics:

1. Select **Tools > Diagnostics**.
2. Select the type of diagnostics from the drop-down list:
   - IPsec diagnostics
   - IPsec configuration
   - Network agent diagnostics

- Host Enforcer configuration
- Network configuration
- Route configuration

See “Viewing Diagnostics” on page 100.

Chapter 5

Managing Network Adapters

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

NOTE: OAC does not support tuning the performance of wired or wireless network adapters or related drivers.

NOTE: OAC requires native Vista WLAN miniport drivers for wireless network access. OAC does not support legacy XP WLAN miniport drivers on Vista. If you try to configure legacy wireless adapters in OAC on Vista, Odyssey Access Client Manager identifies them as an unknown adapter type.

Adding a Network Adapter

After you add a network adapter to the OAC configuration, OAC binds to and controls it. You cannot use a different wireless supplicant program with that adapter unless you remove the adapter from the OAC configuration. See “Removing an Adapter” on page 45.

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

To add a network adapter:

1. Install or insert the network adapter card in your computer. Most current laptop computers include a built-in wired and a wireless network adapter.
2. Select **Adapters** from the Configuration list in the navigation pane.
3. Click **Add**. The Add Adapter dialog box appears.

   Only adapters that you have not added to the Adapters dialog box appear in the display.
4. Select the adapter to be added from the list and click **OK**.

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

Managing Global Settings for Adapters

You can configure OAC so that it configures all wired or wireless adapters automatically, even if you add a different adapter after the initial OAC configuration is in place. This relieves you from having to configure individual adapters if you tend to use different ones at different times, particularly in a test lab.

Your administrator might preconfigure OAC to manage all adapters, in which case the administrative settings override your local control of this option.

To set this option:

1. Select **Tools > Options > Interfaces** from the Odyssey Access Client Manager navigation pane.
2. Select either or both of the following options:
   - **Manage all wireless (Wi-Fi) adapters**—Automatically manages all of your Wi-Fi adapters.
   - **Manage all wired (Ethernet) adapters**—automatically manages your wired adapter.
3. Click **OK**.

Renaming an Adapter

When an adapter is added to an OAC configuration, it appears in the navigation pane in the Adapters list. If you use multiple wireless adapters, you can rename them as you like to further distinguish one from another.

NOTE: Non-802.1X Ethernet adapters do not appear in OAC configurations.

To rename an adapter:

1. Right-click the adapter icon in the navigation pane.
2. Click the **Rename** option, which highlights the adapter name.
3. Replace the current, highlighted name with the new name. (This is the same method used to rename a file in a Windows Explorer directory tree.)

Removing an Adapter

You can remove an adapter using the Adapters dialog box or by using the Adapter icon. When you remove an adapter, OAC stops using it.

Removing an Adapter By Using the Adapters dialog Box

To remove an adapter using the Adapters dialog box:

1. Select **Configuration > Adapters** from the Odyssey Access Client Manager navigation pane.
2. Select the wired or wireless adapter that you want to remove in the Adapters dialog box.
3. Click **Remove**.

Removing an Adapter By Right-Clicking the Adapter Icon

To remove an adapter using the navigation pane icon:

1. Right-click the adapter icon in the navigation pane.
2. Select **Remove**. The dialog box prompts you for confirmation before removing the adapter.
3. Click **OK**.

NOTE: When you remove an adapter from the OAC configuration, check the Windows Control Panel setting to ensure that the adapter is enabled for Windows again. Select **Start > Control Panel > Network Connections >** *adapter name* **> Properties > Wireless Networks** and select the **Use Windows to configure my network settings** check box.

Checking Adapter Status

One way to check adapter status is to view the adapters in the Adapters list. If an adapter is disconnected from the network, the adapter appears dimmed.

To check adapter status:

1. Select **Adapters** at the top of the navigation pane.
2. Select the adapter whose status you want to check.

Connection Information

The Connection Information pane displays summary information about the connection status of the specified adapter. This information includes:

Connection status () shows summary information about the current adapter and network connection, which includes:

- Status—Status of the connection. See Table 7 for an explanation of connection status messages.
- Elapsed time—Duration (in hours, minutes, and seconds) of current network connection. When moving from one access point to another (wireless roaming) in the same network session, the elapsed time resets each time you connect to another access point.
- Network (SSID)—Name of the wireless network to which the adapter is connected.
- Access point—The device name or MAC address of the wireless access point to which the adapter is connected.
- IP address—The IP address assigned to the adapter for the specified network.
- Packets in/out—The number of data packets sent and received during the current network connection.

Table 7: Connection Status Information

Status Message	Definition
open and authenticated	The connection is authenticated and you are connected.
open / authenticating	Reauthentication is in progress and you are connected.
open / requesting authentication	You have requested reauthentication and you are connected.
open	The connection is not authenticated but you are connected.
peer-to-peer	The network type is peer-to-peer (ad hoc) and you are connected.
authenticating	You are not yet connected but authentication is in progress.
requesting authentication	You are not yet connected but you have requested authentication from the access point.
waiting to authenticate	You are not yet connected and the last authentication failed but you are waiting to retry. If you see this message for a considerable length of time, there might be an association problem. If so, select the association mode required for your access point.
searching for access point	You are not connected and communication with an access point on the requested network has not been established. This might occur when your adapter does not support 802.1X or if your access point is not within range.
disconnected	You are not connected and Connect to the network might not be enabled.
OAC is disabled	You are not connected and OAC has been disabled.
adapter not present	You are not connected and the configured adapter is not available. This might occur when your adapter does not support 802.1X.
cable unplugged	You are not connected. This can occur if you have a wired connection but your cable is unplugged.

Table 7: Connection Status Information (continued)

Status Message	Definition
adapter in use by another program	Your adapter is being used by another program installed on your machine.
disabled by wired connection	Your wired connection has disabled your OAC wireless connection based on your security settings.

Infranet Controller Information

The information displayed in the Infranet Controller dialog box shows Layer 2 network connection session information for the Infranet Controller that authenticated the network connection.

- Connection status—Status of the connection.
- Session time—Duration (in hours, minutes, and seconds) of the current connection to the Infranet Controller.
- Server address—IP address of the Infranet Controller.
- Compliance—Message indicating whether your computer meets the network security policies.

For more information about Infranet Controllers and default settings, see the *Unified Access Control Administration Guide*.

OAC Interaction with Other Adapter Software

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

In most cases, OAC and the user interface that comes with your wireless adapter can coexist. However, we recommend that you not use both products for similar purposes. This helps to avoid conflicts that could result when both programs are attempting to control the adapter at the same time. If you use OAC for network communications, use the software supplied with your adapter to operate only those features that cannot be controlled by OAC.

Chapter 6

Configuring Authentication Profiles

This chapter describes how to set up an OAC *profile* for an authenticated network connection. A profile contains all of the information necessary to authenticate a connection to a specific network. This includes information such as your user credentials and the EAP protocols used to authenticate your access to that network.

Authentication Profile Overview

In most large corporations, an administrator or security office is responsible for deciding which authentication methods and protocols to support. Therefore, individual users may not be allowed to modify settings that could conflict with the company security policy. Thus, OAC may be configured by your administrator before distributing it to various user groups or departments.

However, there may be occasions when you need to configure authentication settings for a network outside of your corporate network or to update specific authentication profile settings if your administrator directs you to do so. Therefore, being familiar with how to configure authentication settings in a profile is helpful.

NOTE: Your authentication server may not support all of the EAP authentication methods available in OAC. Try to determine in advance which methods the authentication server allows before setting up authentication in OAC.

The tasks for managing a profile include:

- Create or modify an authentication profile.
- Specify user credentials.
- Specify EAP authentication settings.
- Specify authentication settings for an Infranet Controller.

You must have a profile for each network to which you connect and authenticate. You can have profiles for various corporate office locations, particularly if the authentication requirements differ. Similarly, you can have profiles for various customer networks and for wireless networks at airports, train stations, and coffee shops.

Adding or Modifying a Profile

This section describes how to create an authentication profile.

The Profiles dialog box lists the profiles configured for OAC. The list might include a default profile containing preconfigured settings. You can use this as a template for setting up additional profiles.

To add or modify a profile:

1. Select **Configuration** in the Odyssey Access Client Manager navigation pane.
2. Click **Profiles** to open the Profiles dialog box.

- To add a profile, click the **Add** button in the Profiles dialog box.
- To modify profile properties, click **Properties** in the Profiles dialog box.

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

- Profile name—The name of the profile that you are creating or editing.
- User information—Your login name and the means used to authenticate your identity (password, certificate, or other user credentials).
- Authentication—The authentication protocol to be used. Depending on the authentication protocol that you specify, there are other settings that might apply. See “Managing SIM Card PIN Settings” on page 32.
- TTLS—The EAP-TTLS outer protocols and, where applicable, one or more inner protocols. See “Configuring TTLS Inner Authentication Protocols” on page 63.
- PEAP—The EAP-PEAP outer protocols and, where applicable, one or more inner protocols. See“Configuring PEAP Inner Authentication Protocols” on page 67 and “Using Certificates for EAP-PEAP Authentication” on page 69.
- JUAC—If you intend to connect to and be authenticated by an Infranet Controller, you must use JUAC as an inner authentication protocol. Your administrator might have preconfigured your Infranet Controller access already.

If you are configuring your own settings, see the following sections:

- “Setting JUAC as an Inner Authentication Protocol for TTLS” on page 66
- “Setting JUAC as an Inner Authentication Protocol for PEAP” on page 68
- “Setting a Preferred Realm and Role” on page 70

Specifying a Profile Name

When you add a profile to OAC, specify a unique name for the profile in the Profile name box of the Profile Properties dialog box. If you use hotspot networks frequently, you can create named profiles for each of them.

You cannot change the name of a profile after you save it. However, you can modify other profile properties.

Configuring User Information

The User Info tab is located in the Profile Properties dialog box. It contains a series of tabs for configuring the login name, password, certificate, soft token, or SIM card based on the login credentials that you need. See "Using SIM Cards for Authentication" on page 57 for details on using SIM cards. This information is likely to be different for each network and requires a separate profile.

Specifying a Login Name

Enter your username in the **Login name** box. This is the name presented to the network when you request a network connection. See your network administrator for the required format. See "Login Credential Formats" on page 51.

The **Profile Properties > User Info** tab has these configuration categories:

- Password—Configure this setting when you use authentication protocols that require or permit a password (such as EAP-TTLS). You can specify how the password should be retrieved. See "Using Passwords for EAP Authentication" on page 52.
- Certificate—Configure this setting when you use authentication protocols that require a client-side certificate (for example, EAP-TLS), or if you use a smart card for authentication. See "Using Certificates for Authentication" on page 53.
- Soft Token—Configure this setting when you are required to use a soft token for authentication. See "Using Soft Tokens for Authentication" on page 55.
- SIM Card—Configure this setting when you use a mobile wireless device with a Subscriber Identity Module (SIM) card for authentication. See "Using SIM Cards for Authentication" on page 57.

Login Credential Formats

Your username is the name presented to the network when you request authentication. If you attempt authentication against a Windows Active Directory, use the form *domain**username* (for example, Acme\george). Otherwise, see your network administrator for the required format. Note the following:

- If you are logged into a network domain, OAC populates this box with the standard Windows network form, *domain**username*, where *username* is your username.
- If you are logged in to your client machine (instead of a network domain), OAC populates this box with your username.
- You might need to add some text after your login name for the purpose of routing your authentication to the proper server. For example, acme\george@sales.acme.com. Your network administrator can tell you how to set this box correctly.

- If your network administrator has configured OAC to prompt for a customized login name format that is used as the default value for the Login name box for all new profiles that you create, you can modify this value by selecting **Tools > Windows Logon Settings**.
- If you are configuring this profile for use with a SIM card, make sure that your login name is of the form that is required by your provider. The standard format is *username@realm*.

Using Passwords for EAP Authentication

The following EAP authentication methods require a password:

- EAP-TTLS with an inner protocol of PAP
- EAP-TTLS with an inner protocol of CHAP
- EAP-TTLS with an inner protocol of MS-CHAP
- EAP-TTLS with an inner protocol of MS-CHAPV2
- EAP-TTLS with an inner protocol of EAP-MS-CHAP-V2
- EAP-TTLS with an inner protocol of EAP-MD5-Challenge
- EAP-PEAP with an inner protocol of MS-CHAP-V2
- EAP-PEAP with an inner protocol of EAP-MS-CHAP-V2
- EAP-MD5-Challenge
- EAP-LEAP
- EAP-SIM
- EAP-AKA

If you configure one of the following protocols, you can use a password instead of a token:

- EAP-FAST
- EAP-PEAP with an inner protocol of GTC
- EAP-PEAP with an inner protocol of POTP

Configuring a Password

To configure a password:

1. Select **Configuration > Profiles > Properties > User Info > Password**.
2. Click **Permit login using password**.

Now you can enable the authentication methods that use your password for authentication.

You can configure a password in one of the following ways:

- **Use Windows password**—Uses your Windows login credentials as authentication information when you use this profile to request a connection to a network.

NOTE: Do not select this option if you plan to log in to your client device with a smart card PIN unless your administrator has installed the GINA module.

- **Prompt for password**—Configures OAC to prompt you for a password when you request a connection to the network.
- **Prompt for login name and password**—Configures OAC to prompt you for a username and password when you request a connection to the network.
- **Use the following password**—Specifies a standard password to use for login credentials when you use this profile to request a connection to a network.

NOTE: If you subsequently change your login password, be sure to update the password in the **Use the following password** box.

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

You might have to reenter your password when connecting to the network under some conditions, including the following:

- You enter an incorrect password or some other authentication failure occurs. This feature is in place, in part, to prevent accidental lockout resulting from the reuse of bad passwords.
- You need to change your password periodically and are accessing the network with EAP-TTLS, EAP-PEAP, or EAP-FAST authentication before Windows login.

Using Certificates for Authentication

A *certificate* is cryptographic data that guarantees a particular public key is associated with the private key of a particular entity. The entity can be an individual or a computer. A certificate contains information that is used for mutual authentication. See “Certificates” on page 112 for a broader discussion of this section.

OAC reads personal certificate information from one of the following sources:

- The personal certificate store on your computer or device.
- A smart card reader, if you have one installed.

Use EAP-TLS, EAP-PEAP, and/or EAP-TTLS as an authentication protocol for this profile to negotiate authentication using certificate credentials.

If you select EAP-PEAP, use EAP-TLS as the inner authentication protocol. See "Configuring PEAP Inner Authentication Protocols" on page 67.

If you select EAP-TTLS, choose one of the two certificate-based options on the TTLS settings tab.

TLS is the only EAP protocol that requires a client certificate for authentication but you can use client certificates with TTLS and PEAP.

TLS, TTLS, and PEAP support mutual authentication between the authentication server and the client machine. *Mutual authentication* means that while the server authenticates you as a valid user, you can validate the server as well. The default behavior for OAC is to authenticate (validate) the server's certificate.

NOTE: If you use a FIPS Edition license with the **FIPS Mode** option enabled, any client certificate you use must be associated with a FIPS-approved Cryptographic Service Provider DLL.

To use a certificate for authentication:

1. Select **Configuration > Profiles > Properties > User Info > Certificate**.
2. Select **Permit login using my certificate** to select authentication methods that use your certificate for authentication. Select one of the following options:
   a. **Use automatic certificate selection**—Lets OAC select your certificate automatically (from a smart card reader or from your personal certificate store) at authentication time.

      Note the following:

      - With this option, you are not required to provide a login name for this profile if you do not use any password-based authentication methods.
      - If you select this option, OAC does not check that your certificate is installed. If your certificate is not installed at authentication time, your authentication request fails.

b. **Use the following certificate**—Selects a personal certificate from your computer. To select a personal certificate, click the **Browse** button to display a list of your personal certificates, select a certificate, and click **OK**. After you configure a certificate, you can click **View** to view the contents of the certificate.

NOTE: Before you can create a profile that uses a personal certificate from your computer, you must install the certificate in the correct location on your computer.

On Windows systems, from the Internet Explorer menu bar, select **Tools > Internet Options > Content > Certificates.** Consult your network administrator for help with this.

See your network administrator for information about installing and selecting a user certificate for authentication if you require one.

c. **Use the login certificate from my smart card reader**—Allows you to keep the default smart card reader selection (any reader) or select a specific smart card reader from the list of readers installed on your machine.

Using Soft Tokens for Authentication

With certain token-based authentication options, you can use a software-based token rather than a token from a physical token card. These soft token authentication options include the following:

- EAP-Generic Token Card as an outer authentication method. Select **Prompt for token information** under EAP-Generic Token Card on the Authentication tab. See "Configuring EAP Authentication Settings" on page 58.
- EAP-TTLS as an outer authentication method used with either PAP/Token Card or EAP/EAP-Generic Token Card as the inner method. See "Supported TTLS Inner Authentication Protocols" on page 64.
- EAP-PEAP as an outer authentication method with EAP-Generic Token Card as the inner method. Select **Prompt for token information** under EAP Generic Token Card on the Authentication tab. See "Configuring PEAP Inner Authentication Protocols" on page 67 for information on selecting inner authentication methods for EAP-PEAP.

To use a soft token for authentication:

1. Create a profile that uses only soft token authentication methods (recommended for soft token authentication configuration).
2. Select **Configuration > Profiles > Properties > User Info > Password**.
3. Clear the **Permit login using password** check box.
4. Select the **Soft Token** tab.
5. Select the **Permit login using my RSA Soft Token** check box.
6. Choose one of the following options:

- **Use any token**—You have only one token installed in your client machine.
- **Use the following token** and click **Browse**—You have more than one token installed and you want to choose a specific token. When you do so, the RSA Soft Tokens dialog box appears. Select the soft token that you require and click **OK** to close the RSA Soft Tokens dialog box.

7. Configure one of the soft token-based authentication options listed at the beginning of this section.

8. Click **OK** to save the profile.

Runtime Authentication Dialog for Soft Tokens

After you have configured soft token authentication, click **Connect to the network** on the Wi-Fi or Ethernet dialog box. OAC then begins to negotiate with the RSA server and display a series of authentication dialog boxes related to your state in the RSA server response/challenge process.

If the software token is protected by a passphrase, you will need to specify a passphrase the first time you use it.

There are two basic modes of operation for Odyssey Client RSA soft token authentication:

- **Token Mode**—Use this to apply your PIN and send a new token after the token is updated.
- **New PIN Mode**—Use this to create and verify a new PIN before you can apply a PIN and send a new token.

Configuring Token Mode for RSA Soft Token Authentication

In token mode, you already have a PIN. In most cases, you need only enter a 4- to 8-digit PIN. To enter the PIN in token mode:

1. Enter a PIN in the **Enter PIN** box. Check **Unmask** to view your PIN in cleartext.

2. Click **OK** to complete the authentication request. Your RSA soft token is automatically included with the authentication request.

Configuring Other Token Mode States

If you cannot connect with the simple PIN request service dialog box, you may be prompted one or more times. (The message text varies based on the context.) The following scenario is a sample of the sequence of dialog boxes for token mode.

1. In the **Respond to RSA Soft Token Request** dialog box, enter your PIN and click the **Apply PIN** button.

2. Click **Send** next to the **Current Password** box. You may, instead, be prompted to specify the next pass code.

NOTE: Click the **Unmask** check box to see a PIN in clear text before clicking **Send**.

Configuring a New PIN

When you are prompted to enter a new PIN, follow these steps:

1. Click **Send** next to Current Token mode.You are in New PIN mode if you do not have a PIN or if your PIN has been reset by the token server.

2. Click **OK** before entering the PIN.

3. At the subsequent prompt, enter your new 4- to 8-digit PIN in the New PIN box and click **Send**.

4. At the next prompt, enter the new PIN again in either the **New PIN** box or other response box.

   In some cases, a different dialog box might prompt you to wait for the code on your token card to change. In this case, follow these steps:

   a. Enter your new PIN in the **PIN** box.

   b. When the displayed token code updates, click **Apply PIN**.

   c. Click **Send** next to Next PASSCODE.

Using SIM Cards for Authentication

You can configure Subscriber Identity Module (SIM) card authentication from the SIM Card subtab of the User Info tab of the Profile Properties dialog box.

To use a SIM for authentication, you must configure an OAC user profile for use with your SIM card and assign EAP-SIM and/or EAP-AKA as the authentication protocol(s).

Your SIM card contains an International Mobile Subscriber Identity (IMSI)— the calling number issued by your service provider—for identification. If you do not use the IMSI from the SIM card for SIM authentication, OAC uses the name you specify as a Login name. See “Configuring EAP-SIM Identity” on page 58.

To use OAC with your SIM card:

1. Create a profile that uses only soft token authentication methods (recommended for soft token authentication configuration).

2. Select **Configuration > Profiles > Properties > User Info > Password**.

3. Clear the **Permit login using password** check box.

4. Select the **SIM Card** tab.

5. Select **Permit login using my SIM card**.

Setting a SIM Card ID

Configure OAC to make SIM card connections in one of two ways:

- Use any SIM card that is installed. For this option, select **[any]** from the SIM card ID list.
- Use a specific SIM card ID. For this option, enter your SIM card ID in the SIM card ID list or, if you have already inserted your SIM card into your PC, select your SIM card ID from the SIM card ID list.

Managing SIM Card PIN Settings

You might have already set a PIN on your SIM card hardware. You have the following choices for PIN settings:

- **PIN is not required** (default)—You are not required to use the PIN for your connections (you have no PIN assigned to your SIM card).
- **Prompt for PIN**—You want to use a PIN with your SIM card and you want to be prompted for your SIM card PIN each time that you connect. You might want to use this option for security reasons. You must use this option when you select **[any]** from the SIM card ID list (as opposed to a specific SIM card ID).
- **Use the following PIN**—You want to use the PIN that you have enabled for use with your specified SIM card ID. In this case, enter the PIN in the box provided. With this option, the PIN is stored and you are not prompted to enter it when you make a network connection.

Configuring EAP-SIM Identity

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

Choose one of these methods to enter your SIM identity:

- **Use the IMSI from my** SIM card (default)—Your provider requires you to use your IMSI for identification.
- **Use the login name I entered in this profile**—You must use an identity (usually of the form *username@realm*) rather than your IMSI. In this case, make sure that your login name is in the form that is required by your provider. Note that when you select this option and if you allow more than one authentication protocol with this profile, there might be a conflict with your login name. If you are required to select this option, create a separate configuration for connections that use protocols other than EAP-SIM or EAP-AKA.

Configuring EAP Authentication Settings

Corporate networks use a variety of authentication methods and settings. You need the correct settings configured for your network. Before changing or specifying any authentication settings in OAC, consult your network administrator to determine if those changes reflect corporate policy. If your settings are incorrect, you might not be granted access to your network. In many cases, authentication settings might be preconfigured and possibly restricted by your network administrator.

The four tabs in the Profile Properties dialog box for configuring authentication settings:

- **Authentication**—Lets you configure one or more outer authentication protocols and arrange them in a top-down priority order. Some outer protocols do not support inner authentication protocols. If you intend to use TTLS or PEAP, select those protocols first in this tab and then go to the TTLS or PEAP tab to configure the corresponding inner authentication protocols. The authentication protocols specified on the Authentication tab are used to create a secure tunnel between OAC and the authentication server. Some authentication protocols, such as PEAP and TTLS, require that you also specify an inner authentication method.

NOTE: EAP-TTLS, EAP-PEAP, and EAP-FAST all use inner (tunneled) protocols. EAP-FAST uses EAP-GenericTokenCard as the inner protocol. You can choose one or more inner protocols for EAP-TTLS or EAP-PEAP. See "Configuring TTLS Inner Authentication Protocols" on page 63 and "Using Certificates for Authentication" on page 53.

- **TTLS**—Lets you configure the inner authentication protocols to be used inside an EAP-TTLS tunnel. If you select EAP as an inner protocol, you can subsequently select one or more inner EAP protocols from a list. Note that the EAP-JUAC inner protocol is configured by default. You need this inner protocol to connect to an Infranet Controller.

- **PEAP**—Lets you configure the inner authentication protocols to be used inside an EAP-PEAP tunnel. If you select EAP as an inner protocol, you can subsequently select one or more inner EAP protocols from a list. Note that the EAP-JUAC inner protocol is configured by default. You need one of these inner protocols to connect to an Infranet Controller.

- **JUAC**—EAP-JUAC is a Juniper Networks protocol developed specifically for connecting to an Infranet Controller. The JUAC tab allows you to specify the realm and role used for this connection. See "Setting a Preferred Realm and Role" on page 70.

Authentication Protocols for FIPS Mode (FIPS Edition Only)

When operating in FIPS mode, OAC protects all wireless data connections with FIPS-validated cryptography. Some authentication protocols and features permit non-validated cryptography methods and are disabled when FIPS mode is on.

The outer authentication protocols supported for FIPS mode are:

- EAP-PEAP
- EAP-TLS
- EAP-TTLS

There are no restrictions for inner authentication protocols.

With FIPS Mode on, FIPS constraints apply to each network to which you connect.

Configuring Outer EAP Authentication Protocols

The Authentication protocols list shows the outer authentication protocols that you have selected. You can have one or more authentication protocols in the list and add more if necessary. If you have more than one protocol in the list, you can order them sequentially to indicate your preference. The sequence determines the protocol that the server uses if it has more than one protocol in common with the ones that you select here. Consult your network administrator before changing these settings.

Select **Configuration > Profiles > Properties > Authentication**.

NOTE: (FIPS Only) Outer EAP protocols supported for OAC FIPS Edition are EAP-PEAP, EAP-TLS, and EAP-TTLS only.

Table 8 lists the set of outer authentication protocols and how they apply across OAC and Infranet Controllers.

Table 8: List of Outer Authentication Protocols

Outer Protocols Supported Only by OAC	Outer Protocols Supported by Both OAC and Infranet Controllers	Outer Protocols Supported Only by Infranet Controllers
EAP-AKA	EAP-GenericTokenCard (GTC)	PAP
EAP-FAST	EAP-MD5-Challenge	CHAP
EAP-LEAP	EAP-PEAP	MS-CHAP
EAP-POTP	EAP-TLS	MS-CHAP
EAP-SIM	EAP-TTLS	MS-CHAP-V2

Adding an Outer EAP Authentication Protocol

To add a protocol to the list:

1. Open the Profile Properties dialog box.
2. Click the **Authentication** tab.
3. Click **Add** to open the Add EAP Protocol dialog box.
4. Select the protocol or protocols that you want to add.

   To select more than one protocol at a time, hold down the Ctrl key as you select each protocol. A protocol that has already selected does not appear in this dialog box.
5. Click **OK.**

Removing an Outer EAP Protocol

To remove a protocol from the list:

1. Open the Profile Properties dialog box.
2. Click the **Authentication** tab.
3. Select the protocol you want to remove.
4. Click **Remove**.

Reordering Protocols

To reorder protocols:

1. Open the Profile Properties dialog box.
2. Click the **Authentication** tab.
3. Select the protocol you want to move.
4. Use the Up or Down arrow button to change the order of protocols in the list.

Server Validation—Mutual Authentication

Certain protocols, such as EAP-TTLS, EAP-PEAP, and EAP-TLS, let you validate the authentication server while the server verifies your identity. This is called *mutual authentication*. Server verification is an important security measure that protects you from connecting to a server that might be mimicking ("spoofing") the actual server to which you intend to connect, which can leave your computer vulnerable to a hostile attack. Validation involves assuring the authenticity of the server's certificate.

To see this option, select **Configuration > Profiles > Properties > Authentication.** The default OAC behavior is to validate server certificates and we recommend that you do not disable it. This ensures a secure, authenticated connection to the server.

NOTE: Mutual authentication requires that you have the same root CA or intermediate CA as the server certificate chain installed in the trusted root or intermediate certificate store of your machine.

On Windows systems, from the Internet Explorer menu bar, select **Tools > Internet Options > Content > Certificates.** Consult your network administrator for help with this.

Select **Disable server verification** to turn off server verification. For example, if you are unable to configure trust because you do not have an intermediate root CA certificate installed on your machine, you might want to turn off certificate verification.

NOTE: Do not turn off server verification unless your network administrator directs you to do so. Disabling server verification can expose your password and credentials to an untrusted server.

Setting Token Card Credential Options

EAP-GenericTokenCard (GTC) can be configured as the inner authentication protocol inside a TLS tunnel. EAP-GTC defines an EAP envelope to transport one-time passwords generated by token cards. You can use EAP-GTC in the following circumstances:

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

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

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

NOTE: These settings do not apply if you configure EAP-GenericTokenCard or EAP-POTP as an EAP inner authentication method for EAP-TTLS. Additionally, these settings do not apply when you choose EAP-POTP or EAP-GenericTokenCard as an outer authentication method.

Using an Anonymous Login Name

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

You can have two identities when you use EAP-TTLS, EAP-PEAP, or EAP-FAST:

- An inner identity, your login name, which is taken from the Login name box in the User Info tab.
- An outer identity that can be completely anonymous. You can set your outer identity by selecting **Profiles > Properties > Authentication** and filling in the **Anonymous name** box.

Note the following guidelines:

- Anonymous outer identities are implemented only if you enter a name in the **Anonymous name** box.
- When you leave the Anonymous name box blank, your inner identity is used as your outer identity. (This does not apply for TTLS.)

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

- In some cases, you might need to add additional text. If the outer identity is used to route your authentication to the proper server, you might be required to use a format such as anonymous@acme.com.
- Anonymous EAP-PEAP authentication may not work with your network authentication server, in which case leave the Anonymous name box blank.

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

Configuring TTLS Inner Authentication Protocols

EAP-TTLS creates a secure encrypted tunnel through which your credentials are presented to the authentication server. If you use EAP-TTLS with password credentials, an inner authentication protocol completes the authentication. See “EAP-TTLS” on page 111.

TTLS and PEAP support inner authentication tunnels. Inner authentication provides an additional level of security by transferring password credentials through an encrypted tunnel between the client and the authentication server. Table 9 on page 64 lists the inner protocols for TTLS.

Select **Configuration > Profiles > Properties > TTLS** to configure EAP-TTLS as an authentication protocol. These settings are relevant only if you select EAP-TTLS as an authentication protocol in the Authentication tab.

Use the Inner authentication protocol list to select the inner authentication protocol to use. Consult you network administrator for the recommended corporate settings for your network. See Table 10 on page 64 for a list of supported inner EAP protocols.

Table 9: Supported TTLS Inner Authentication Protocols

Inner Protocols Support Only by OAC	Inner Protocols Supported by Both OAC and Infranet Controllers	Inner Protocols Supported Only by Infranet Controllers
EAP-SIM	CHAP	CHAP
EAP-AKA	EAP	EAP-MS-CHAP-V2
EAP-POTP	EAP-GenericTokenCard (GTC)[a]	MS-CHAP
	EAP-JUAC[b]	PAP[c]
	EAP-MD5-Challenge	
	MS-CHAP	
	MS-CHAP-V2[d]	
	PAP/Token Card	

a. EAP-GenericTokenCard is preferable to PAP.
b. OAC clients should use EAP-JUAC.
c. An Infranet Controller manages the nuances of PAP vs. PAP/Token Card transparently.
d. EAP-MS-CHAP-V2 is preferable to MS-CHAP-V2 and MS-CHAP-V2 is preferable to MS-CHAP.

NOTE: When configuring an authentication profile for an Infranet Controller connection, you must select JUAC as an inner EAP protocol.

Table 10: Supported Inner EAP Authentication Protocols for TTLS

Inner Protocols Support Only by OAC	Inner Protocols Supported by Both OAC and Infranet Controllers	Inner Protocols Supported Only by Infranet Controllers
EAP-SIM	EAP-GenericTokenCard (GTC)[a]	CHAP
EAP-AKA	EAP-JUAC[b]	EAP-MS-CHAP-V2
EAP-POTP	EAP-MD5-Challenge	MS-CHAP
	MS-CHAP-V2[c]	PAP

a. EAP-GenericTokenCard is preferable to PAP.
b. OAC clients should use EAP-JUAC.
c. EAP-MS-CHAP-V2 is preferable to MS-CHAP-V2 and MS-CHAP-V2 is preferable to MS-CHAP.

Selecting Inner Authentication Protocols for TTLS

To select an inner authentication protocol:

1. Select **Configuration > Profiles > Properties**.
2. Select either the **TTLS** or the **PEAP** tab, based on the outer EAP authentication method being used.
3. Select an inner authentication protocol from the list. See Table 9.

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

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

PAP/Token Card is the protocol to use with token cards if you cannot use EAP-POTP authentication. When you use PAP/Token Card, the password value that you enter into the Password dialog box is never cached, because any token-based password is good for one use.

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

Adding EAP Inner Authentication Protocols

If you select EAP as your inner authentication protocol, you must configure the Inner EAP protocols list on the TTLS tab of the Profile Properties dialog box with one or more protocols. See Table 10 on page 64.

To add an inner EAP protocol:

1. Select **Configuration > Profiles > Properties > TTLS**.
2. Select **EAP** from the list of inner authentication protocols.
3. Click **Add** to display the list from which you can choose inner EAP protocols.
4. Select one or more of the following inner EAP protocols:
   - EAP-GenericTokenCard
   - EAP-MD5-Challenge
   - EAP-SIM
   - EAP-AKA
   - EAP-POTP
5. Click **OK**.
6. Add other inner EAP protocol to the list by repeating this procedure.

See Table 8 on page 60 for a list of outer EAP protocols and Table 10 on page 64 for the corresponding inner protocols.

Removing EAP Inner Authentication Protocol

To remove a protocol:

1. Select **Configuration > Profiles > Properties > TTLS**.
2. Select **EAP** from the list of inner authentication protocols.
3. Select the protocol to remove.
4. Click **Remove**.

Setting JUAC as an Inner Authentication Protocol for TTLS

If you intend to be authenticated by an Infranet Controller, you must use JUAC as your inner authentication protocol.

NOTE: For a Layer 3 connection to an Infranet Controller, use TTLS or PEAP with JUAC as the inner protocol.

To add JUAC as an inner authentication protocol for TTLS:

1. Select **Configuration > Profiles > Properties**.
2. Click the **TTLS** tab.
3. Select **EAP** from the Inner EAP protocols, in order of preference list.
4. Click the **Add** button to display the Add EAP Protocol dialog box and select **JUAC** and any other inner EAP protocols to add by highlighting one or more of them.
5. Click **OK**.

Setting the Preferred Order of Inner EAP Protocols

To set a preferred order of inner EAP protocols:

1. Select **Configuration > Profiles > Properties**.
2. Click the **TTLS** tab.
3. Select one of the inner EAP protocols from the list.
4. Use the arrow button to move the protocol up or down in the list.
5. Repeat this procedure until the list reflects the preferred order.

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

Removing JUAC as an Inner Authentication Protocol for TTLS

To remove JUAC as an inner authentication protocol for TTLS:

1. Select **Configuration > Profiles > Properties**.
2. Click the **TTLS** tab.
3. Select **JUAC** from the list of inner EAP protocols.
4. Click **Remove**.

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

Using Certificates for EAP-TTLS Authentication

To select EAP-TTLS personal certificate options:

1. Select **Configuration > Profiles > Properties > User Info > Certificates**.
2. Select **Permit login using my certificate**.
3. Select the **TTLS** tab and select one of the following personal certificate options:
   - **Use only my certificate for authentication**—Configures EAP-TTLS certificate-based authentication without a password.

     If you select this option and do not select a password-based authentication method, clear the **Permit login using password** setting on the **Configuration > Profiles > Properties > User Info > Password** subtab. See "Using Passwords for EAP Authentication" on page 52 for a list of password-based authentication methods.

NOTE: If you are configuring a profile for an Infranet Controller connection and are using EAP-TTLS with a certificate, you must have a valid inner authentication protocol, such as JUAC.

   - **Use my certificate and perform inner authentication**—Configures EAP-TTLS certificate-based authentication and tunnel password credentials for use with an inner authentication protocol.
   - **None**—Configures EAP-TTLS without a client-side certificate. This option is the most typical use of EAP-TTLS authentication. Select this option unless you intend to use a client certificate as part of EAP-TTLS authentication.
4. Click **OK**.

Configuring PEAP Inner Authentication Protocols

Select **Configuration > Profiles > Properties > PEAP** to configure EAP-PEAP as an authentication protocol. These settings are relevant only if you select EAP-PEAP as an authentication protocol in the Authentication tab.

You can add, remove, or reorder any EAP-PEAP inner protocols from the **PEAP** tab of the Profile Properties dialog box. Table 11 lists the inner protocols for PEAP.

Table 11: Supported PEAP Inner Authentication Protocols

Inner Protocols Support Only by OAC	Inner Protocols Supported by Both OAC and Infranet Controllers	Inner Protocols Supported Only by Infranet Controllers
EAP-POTP	EAP-GenericTokenCard (GTC)	EAP-SOH
	EAP-JUAC[a]	
	EAP-TLS	
	MS-CHAP-V2	

a. OAC clients should use EAP-JUAC.

Selecting Inner Authentication Protocols for PEAP

To add an inner PEAP protocol:

1. Select **Configuration > Profiles > Properties > PEAP**. The list of inner EAP authentication methods appears.
2. Click **Add** to display the list from which you can choose inner EAP protocols. Any protocols that you selected previously are not listed.
3. Select an inner EAP protocol from the list and click **OK**.

Setting JUAC as an Inner Authentication Protocol for PEAP

If you intend to connect to and be authenticated by an Infranet Controller, you must use JUAC as an inner authentication protocol.

If you have PEAP as an outer authentication protocol, JUAC is configured automatically as an inner EAP protocol.

Setting the Preferred Order of Inner EAP Protocols

If you have more than one inner EAP protocol selected, you can order the list of preferred protocols as follows:

1. Select one of the inner EAP protocols from the list.
2. Use the arrow button to move the protocol up or down in the list.
3. Repeat this procedure until the list reflects the preferred order.

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

NOTE: If you select **EAP-TLS** for inner authentication, configure certificate-based user credentials on the Certificates subtab of the User Info tab.

Removing JUAC as an Inner Authentication Protocol for PEAP

To remove JUAC as an inner authentication protocol for PEAP:

1. Select **JUAC** in the list of inner EAP protocols.
2. Click **Remove**.

Removing Inner PEAP Protocols

To remove a protocol:

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

Using Certificates for EAP-PEAP Authentication

To select EAP-PEAP personal certificate options:

1. Select **Configuration > Profiles > Properties > User Info > Certificates**.
2. Click **Permit login using my certificate**.
3. Select the **PEAP** tab.
4. Select **Use my certificate to authenticate to the network**.
5. Select one of the following personal certificate options:
   - **Not performed**—Inner authentication is not performed. Use my personal certificate.
   - **Optional**—Inner authentication is optional (determined by the authentication server).
   - **Required**—Inner authentication is required. Use a personal certificate too.
6. Click **OK**.

Configuring EAP-POTP for Inner Authentication

EAP-POTP (protected one-time password) is an authentication method used with one-time password (OTP) tokens, such as RSA, and is well suited for use with USB token readers. It provides an added measure of security by maintaining secure transfer of data between the endpoint and the RSA server.

You can configure OAC to use EAP-POTP as an inner authentication method with EAP-TTLS or EAP-PEAP. (You can also configure EAP-POTP as an outer authentication method.)

NOTE: EAP-POTP is not a supported protocol in a UAC network.

To configure EAP-POTP as an inner authentication method:

1. Configure a network connection that relies on EAP-POTP.
2. Select **Connect to the network** on the Connection dialog box.

OAC presents one or more authentication dialog boxes based on your state in the token card authentication server response/challenge process. Enter the PIN followed by the current sequence of digits shown on your hardware token card.

Under some circumstances, you might need to provide a new PIN. You have the choice of creating your own PIN or using a system-generated PIN:

- Select **System-generated PIN** to use the PIN provided. Memorize this PIN for future use.
- Select **User-defined PIN** to define your own PIN and follow this procedure:

  a. Follow the instructions located after the text box to enter a new PIN in the **Please enter your PIN** box.

  b. Select **Unmask** to see your PIN as you enter it.

  c. Reenter the PIN in the **Please confirm your PIN** box.

  d. Click **OK**.

After you create your new PIN, you are prompted to enter the new PIN again, followed by your token information.

Configuring Authentication for Infranet Controllers

You need a separate profile for each Infranet Controller that you use to access protected network resources.

NOTE: This section applies only if you are using OAC in a UAC network.

The Infranet Controller profile configuration requirements are similar to those used for a network authentication profile. Configure the following settings:

- Profile name.
- Username.
- Password or other credentials.
- Outer authentication protocol (TTLS or PEAP).
- Inner authentication protocol: EAP-JUAC. See “Setting JUAC as an Inner Authentication Protocol for TTLS” on page 66.
- Realm name and role (optional). See “Setting a Preferred Realm and Role” on page 70

Setting a Preferred Realm and Role

This section describes the JUAC tab in the Profile Properties dialog box and how to specify a preferred realm and role for connecting to an Infranet Controller. Connecting to an Infranet Controller might require that you specify a valid realm and role.

- An authentication realm is determined by an authentication server and the authentication policy on that server. It is similar in some ways to a network domain in that it represents the set of protected resources that is available to you.

- An authentication role reflects a job title, department or group, and the privileges needed to access specific resources for that department. An administrator or a manager typically has broader access rights than other employees in that department or group.

  The resources you can access after being granted access to an Infranet Controller reflect the intersection of your realm and your role. Most users have a single realm and role and those are preconfigured as default settings by an administrator. Some users, such as managers, can have more than one realm and role, in which case it may be necessary to specify the realm and role when signing on to an Infranet Controller.

The Infranet Controller might prompt you for a realm and a role when you try to connect. If you have only a single realm and role, there is no prompt.

Setting a Preferred Realm and Role

To set a preferred realm and role:

1. Select **Configuration > Profiles > Properties**.
2. Click the **JUAC** tab.
3. Enter the name of your preferred realm. If you do not know the realms defined for you, see your network administrator.
4. Enter the name of your preferred role. If you do not know the roles defined for you, see your network administrator.

Having a preferred realm and role defined in a profile means that you do not have to re-specify those values each time you connect to the same Infranet Controller.

Using a Token Card for Authentication

If you use one or more token card authentication methods and then select **Connect to the network** to establish a network connection, an exchange of messages begins between OAC and the token card authentication server. The message exchange, known as the *challenge-response dialog box*, takes place as the server prompts (challenges) the user to enter private information (response). OAC presents one or more authentication dialog boxes based on your state in the token card authentication server challenge-response process.

If a dialog box prompts you for a valid PIN, enter the PIN followed by the current sequence of digits displayed on your hardware token card.

Configuring a New Token Card PIN f

Under some circumstances, you might be required to provide a new token card PIN. For example, your PIN can expire and you need to create a new one.

To enter a new PIN:

1. Select **Configuration > Profiles > Properties > User Info**.
2. Click the **Soft Token** tab.

3. Click **Permit login using my RSA Soft Token**.
4. Click **Use following token**.
5. Enter a new 4- to 8-digit PIN and click **OK**.

   Select **Unmask** to see your PIN in clear text before you click **OK**.
6. Reenter a new 4- to 8-digit PIN and click **OK**.

Removing an Authentication Profile

To remove an authentication profile,:

1. In the navigation pane, select **Configuration > Profiles**.
2. When the Profile Properties dialog appears, select one of the existing profiles in the list.
3. Click **Remove**.

Chapter 7

Configuring Wireless Networks

This chapter describes how to configure the wireless networks to which you connect.

Adding or Modifying a Wireless Network

You can add a new network by selecting **Add** in the Network Properties dialog box. You can modify an existing network configuration by selecting **Properties**. The dialog boxes display the same options in both cases.

To configure the settings for connecting to a wireless network:

1. Select the **Configuration** folder from the navigation pane.
2. Select **Networks.** The Networks dialog box opens.

   Each configured network appears in the Networks dialog box.

NOTE: If OAC has been configured by your network administrator, the corporate networks you need may be listed already.

Specifying a Network Name (SSID)

The network name or service set identifier (SSID) is the name of a wireless network. The network SSID can be broadcast by a network access point so that all wireless devices within range of the access point can identify and negotiate with it for network access. The network names that are configured appear in the Network dialog box.

Specify a network name consisting of up to 32 alphanumeric characters. The name is case sensitive.

Scanning for Available Wireless Networks

Instead of entering the name of a configured wireless network in the Network name box, you can scan for wireless access points that are broadcasting network SSIDs:

1. Click **Scan** in the Wi-Fi dialog box.
2. When the Wi-Fi dialog box displays the list of available networks, select the name of the network to which you want to connect.

3. Click **OK**.

Connecting to Any Available Network

OAC provides a special network configuration called [any] that you can use to connect to any available network, regardless of the network name. The [any] network is useful when you are moving between locations that provide open wireless network access or that use identical access credentials.

Select **Connect to any available network** to create a network configuration that lets you connect to any compatible Wi-Fi network without having to configure it.

Using a Network Description

An SSID is an explicit network identifier. In some environments, more than one wireless network can have the SSID. You can use the Network Description field to distinguish between networks with the same SSID.

Specifying a Network Type (Channel)

Select either of the following network types:

- Access Point (infrastructure mode)—Select this option if you are connecting to a Wi-Fi network.
- Peer-to-peer (ad-hoc mode)—Select this option if you must specify a channel on which all peers share data. 802.11b networks provide 14 channels for communication; 802.11a networks provide 12 channels. Choose the default channel or select a channel from the Channel list.

Specifying an Association Mode

Before authentication can occur, your client machine must connect to an access point and request network access. The association mode that you choose depends on the access point hardware configuration. Choose one of the following association modes:

- **Open**—Use this setting to connect to a network through an access point or switch that implements 802.1X authentication. Choose this mode if you are not required to select shared mode or Wi-Fi Protected Access (WPA).
- **Shared**—Use this setting to connect to a network through an access point that requires at least one preconfigured wired-equivalent privacy (WEP) key for association.
- **WPA**—Use this setting to connect to a network through an access point that implements WPA.
- **WPA2**—Use this setting to connect to a network through an access point that implements WPA2, the second generation of WPA that satisfies 802.11i.
- **xSec (FIPS Edition Only)**—Use this setting for a secure Layer 2 connection. This requires Layer 2 xSec-compliant hardware in your network in addition to the access points. If you choose this option, you must select AES encryption.

If you have a FIPS Edition license on a Windows client, you can use xSec without FIPS mode enabled. This lets you to configure xSec for use with Aruba switches.

Selecting an Encryption Method

Your choice of encryption method depends on the access point requirements. The choices available to you depend on the association mode you choose. Each association mode supports specific encryption types. See "Wired-Equivalent Privacy" on page 107 and "Wi-Fi Protected Access and Encryption Methods" on page 108.

Choose one of the following encryption options:

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

Selecting a FIPS Association Mode (FIPS Edition Only)

xSec and WPA2 are the only association modes supported for FIPS secure encryption. If you configure FIPS mode with WPA2 and AES, you can authenticate using either a passphrase or a profile. You must associate xSec networks with a profile that uses EAP-TTLS, EAP-PEAP, or EAP-TLS.

If you are running Windows Vista or Windows 7, xSec is available as a wireless association mode even if you are not running in FIPS mode.

Using FIPS Secure Encryption (FIPS Edition Only)

If you require FIPS encryption each time that you connect to a specific wireless network, select **FIPS mode required** as part of setting up a configuration for that network. If not, clear the box.

Whether you configure xSec or WPA2 as the association mode for FIPS security, you must use AES as the encryption method.

Configuring a Network That Does Not Broadcast an SSID

When OAC scans for available wireless networks, it detects and lists the networks within range that are broadcasting an SSID (network name). If a network does not broadcast its SSID, you must configure it manually in OAC. Configuring a nonbroadcast network lets you include it in an auto-scan list and makes sure that OAC will try to connect to it in the sequence specified in the auto-scan list. See "Adding an Auto-Scan List" on page 81.

To configure a network that does not broadcast an SSID:

1. Select **Configuration > Networks** and click **Add**. The Add Network dialog box appears.
2. Specify the network name (SSID) of the nonbroadcast network in the **Network** name box.
3. Configure the association mode and encryption mode settings, including the encryption key settings needed.
4. Optionally, enable the **Non-broadcast** check box. With this setting enabled, OAC remembers the network during subsequent scans for available Wi-Fi networks. In this case, OAC polls for the specific, nonbroadcast network rather than trying to detect an SSID.
5. Specify an authentication profile if the network requires authenticated access.
6. Click **OK**.

Specifying an Authentication Profile

To specify an authentication profile for your login credentials:

1. Click the **Authenticate using profile** check box in the Add Network dialog box. See "Adding or Modifying a Profile" on page 50.
2. Select the profile to use for authentication from the drop-down list. You must have a current profile that has been configured for this network.

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

After you select **Authenticate using profile** and select a profile, OAC performs an 802.1X authentication using the options configured in the selected profile.

NOTE: If the profile you select for this network specifies MD-5 Challenge or EAP-GenericTokenCard as an outer authentication method, you must use a preconfigured WEP key for data encryption to authenticate using 802.1X. See "Preconfigured Keys (WEP)" on page 77.

Using Automatic Key Generation

If the authentication method specified in the selected profile results in the creation of dynamic WEP keys for use between your computer and the access point, then select **Keys will be generated automatically for data privacy**. Certain authentication methods, such as EAP-TTLS, EAP-PEAP, EAP-FAST, EAP-POTP, and EAP-TLS, generate keys; others do not. You can use any of these authentication methods if your access point implements 802.1X authentication.

Using generated keys is more secure than using static (preconfigured) keys and is available with all encryption methods (other than None), as long as you are not associating in shared mode.

Clear the **Keys will be generated automatically for data privacy** check box if you use preconfigured WEP keys or a preshared WPA key.

Using Preconfigured Key Settings

The wireless network might require that you preconfigure WEP keys or that you share a WPA/WPA2 passphrase. Enter the keys in the lower portion of your network properties description, based on the selected association method.

Preshared Keys (WPA or WPA2)

If you associate using WPA or WPA2 and if you do not generate encryption keys automatically when associating an authentication profile to the network connection, you must specify a preshared passphrase in the Passphrase box. The passphrase is used as a seed to generate the required keys.

A preshared key is typically used in home and small office networks that do not support 802.1X authentication. Each user has a unique passphrase required for access to the network. A passphrase consists of 8- to 63 ASCII characters or 64 hexadecimal digits (256 bits). Passphrases and static WEP keys apply if you are connecting to a network that does not use 802.1X authentication, such as home networks, hotspots, and small offices.

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

Preconfigured Keys (WEP)

Configure wired-equivalent privacy (WEP) if you select **open** or **shared** as the association mode for a wireless connection and configure at least one WEP key. See “Wired-Equivalent Privacy” on page 107 and “Specifying an Association Mode” on page 74.

WEP keys serve these purposes:

- They allow you to associate with an access point before a connection is established (shared mode).
- They encrypt data between your machine and the access point (or other computers in a peer-to-peer network).

If you do not select an authentication profile for a network configuration—that is, you are not connecting to an 802.1X network—you must provide at least one WEP key in the Pre-configured keys section of the Network Properties dialog box.

Wireless access points can be configured to use a static WEP key instead of dynamically generating encryption keys using 802.1X. Static WEP key configuration defines four key slots, 0 to 3, corresponding to 802.11 key IDs of 0 to 3. One of these keys is designated on the access point as the *default key*, which is used to encrypt communications with wireless clients. OAC supports up to four WEP keys to be specified for Key IDs 0 to 3.

When configuring OAC network settings with WEP keys, the WEP key corresponding to the access point's default key must be present in the same key slot in the OAC network configuration. For example if your access point has a default or “transmit” key configured in the fourth key slot, configure the same key in OAC for the fourth key slot.

Some installations may configure access points with multiple keys and periodically change which slot to use as the default key, although this does not significantly increase the security of the network; we recommend using dynamic WEP keys through 802.1X.

NOTE: Windows Vista allows only a single static WEP key to be configured for OAC. Configuring multiple keys is not recommended.

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

NOTE: An access point can have multiple keys configured but one of them must be identified as the “default” or “transmit” key. Devices that need to communicate with that access point must have the same key configured in the same slot. Other keys configured must also correspond to the same slots on the client being used.

Entering WEP Keys

Enter the WEP keys in the Key 0 through Key 3 boxes. (Some devices use 1 through 4 as the key fields.) The values entered here must match those of the access point or peer computer to which you connect. You can enter keys as ASCII text characters or hexadecimal characters.

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

To enter WEP keys:

1. Select **Configuration > Networks**.
2. When the Network Properties dialog box, opens, select an association mode of open or shared.
3. Use the **Format for entering keys** list to select **ASCII characters** or **hexadecimal digits** to specify the format for your WEP keys.
4. Enter each WEP key in the Key 0 through Key 3 text boxes.

Removing a Network

To remove a network:

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

Chapter 8

Managing Auto-Scan Lists

An *auto-scan list* is a prioritized list of configured wireless networks. With an auto-scan list, you do not have to manually specify a new wireless network connection each time you move from one location to another. This is convenient when you move regularly to different locations and networks.

An auto-scan list can contain as many networks as you like. OAC attempts to connect to the first network SSID and then cycles through the list. For example, if you set up an auto-scan list that includes your corporate networks and your home office, OAC can help you remain connected automatically.

OAC remembers your last network connection so that if you disconnect and reconnect, OAC tries that connection again automatically. The exception to this rule is that OAC goes through the auto-scan list from the beginning each time if the SSIDs are being broadcast.

Having your office wireless network in the same auto-scan as a hotspot network across the street might increase the likelihood of accidentally connecting to the hotspot network. Select **Preemptive Networks** from the Odyssey Access Client Manager menu bar to control the list of wireless networks to which you connect. Refer also to "Specifying a Preemptive Auto-Scan List" on page 82.

NOTE: Each of the networks in an auto-scan list must be configured in the Networks dialog box. See "Adding or Modifying a Wireless Network" on page 73.

Adding an Auto-Scan List

To add an auto-scan list:

1. Select **Configuration > Auto-Scan Lists** from the navigation pane.
2. Click **Add** in the Auto-Scan Lists dialog box. The Add Auto-Scan List dialog box appears.
3. Enter a unique name for the auto-scan list in the **Auto-Scan list name** box.
4. Use the Left and Right arrow buttons to move networks between the **Available networks** and **Networks in list** lists.

5. Use the Up and Down arrow buttons to specify the sequence of networks within in the auto-scan list. Place the highest priority networks at the top of the list.

   Optionally, select **Switch to preferred network when available, even if currently connected**. If you use this option, OAC scans continuously through the networks in the list and forces a connection to a higher-priority network if it becomes available. The higher-priority network must broadcast its SSID for this function to work.

6. Select **OK**.

NOTE: You should test the availability of each network in your auto-scan list separately. If a network on the auto-scan list is configured incorrectly, authentication fails each time the auto-scan list is used, wasting time.

To test a network connection, go to the connection dialog box of the Odyssey Access Client Manager and select **Connect to the network** after selecting the network you want to test.

Specifying a Preemptive Auto-Scan List

A preemptive auto-scan list identifies the set of networks that, if found, take precedence over any network or auto-scan list currently enabled in the connection dialog box when searching for a network.

NOTE: Preemptive networks affect *which* networks to search for and in what order to search. They do not affect *when* to search. If you select the Switch to a preferred network check box for an auto-scan list, OAC actively monitors the SSIDs being broadcast so that, if an SSID higher up on the list is detected, OAC switches to that network. This feature requires SSIDs to be broadcast to be effective.

To identify a preemptive network list:

1. Create the auto-scan list that you want to use for preemptive networking. This preemptive auto-scan list can contain one network or several networks. See “Managing Auto-Scan Lists” on page 81.

2. Select **Tools > Options > Preemptive Networks**.

3. Enable the **Use preemptive auto-scan list** check box and select the appropriate auto-scan list you created in Step 1 from the **Preemptive Auto-scan** list.

4. Select one or both of the following options:

   - **Preempt any selected network**—Connect to a network from the preemptive list if it becomes available, dropping the connection to a previously selected network if necessary.

- **Preempt any selected auto-scan list**—Connect to a network from the preemptive list if it becomes available, dropping the connection to a network selected from another auto-scan list if necessary.

5. Click **OK**.

Modifying an Auto-Scan List

To modify an auto-scan list:

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

Viewing Networks in an Auto-Scan List

To view the networks in an auto-scan list:

1. select **Configuration > Auto-Scan Lists** from the navigation pane.
2. Double-click the name of the auto-scan list in the Auto-Scan List dialog box.

Removing an Auto-Scan List

To remove an auto-scan list:

1. Select **Configuration > Auto-Scan Lists** from the navigation pane.

1. Select the name of the auto-scan list you want to delete.
2. Click **Remove**.

Chapter 9

Managing Infranet Controller Connections

This chapter describes how to configure an Infranet Controller in OAC. You can skip this chapter if your network does not include an Infranet Controller.

NOTE: An Infranet Controller may need to download an updated OAC configuration before allowing a connection, in which case a dialog box prompts you to accept the update. You may also see a prompt to trust one or more servers. Ask your administrator if you are unsure of which servers to trust.

About Infranet Controllers

An Infranet Controller is a central policy management server in a UAC network that validates user identity and endpoint security compliance and enforces network security policies. An Infranet Controller manages your connection to protected network resources based on who you are and whether your computer complies with network access policies.

You must have an authentication profile for each Infranet Controller to which you connect. The authentication profile contains the configuration settings for your connection credentials and the EAP authentication methods that apply. See "Configuring Authentication for Infranet Controllers" on page 70.

Infranet Controller Connection Types (Layer 2 versus Layer 3)

You can establish an Infranet Controller connection at either Layer 2 or Layer 3.

Connecting to a corporate network through an 802.1X switch or wireless access point is a Layer 2 network connection. Your computer does not receive an IP address until after you have been authenticated on the network. This type of connection occurs at the hardware adapter level.

Connecting to a corporate network through a network switch that is not 802.1X enabled is a Layer 3 connection. In this case, your computer receives an IP address automatically as soon as you connect but before authentication. When you attempt a Layer 3 connection to an Infranet Controller, you are prompted for your authentication credentials as the first step in the sign-on process. If your authentication fails for any reason, you cannot access the resources protected by the Infranet Controller.

Adding an Infranet Controller

Your initial OAC configuration might include settings for one or more Infranet Controllers. If your configuration allows you to configure additional Infranet Controllers, use the following procedure:

1. Select **Configuration > Infranet Controllers** in the navigation pane. The Infranet Controllers dialog box appears.
2. Select **Add** to open the Add Infranet Controller dialog box.
3. Enter a name for the Infranet Controller in the **Infranet Controller name** box.
4. Enter the DNS name or the IP address of the Infranet Controller to which you intend to connect in the **Server URL** box.
5. Use the **Authentication profile** list to select the name of the authentication profile you want to use for the Infranet Controller. The profile provides all the information needed for authenticated access to that Infranet Controller. See “Adding or Modifying a Profile” on page 50 for details about setting up a profile.
6. Click **OK**.

Connecting to an Infranet Controller

To connect to an Infranet Controller:

1. Open the **Infranet Controllers** list in the navigation pane.
2. Select the Infranet Controller to which you want to connect.

   An Infranet Controller dialog box (Figure on page 23) displays the DNS name of the Infranet Controller in the **Server URL** box.
3. Click the **Connect to the Infranet Controller** check box to open a connection to the Infranet Controller.
4. Enter your authentication credentials in the Odyssey Access Client dialog box.
5. Click **OK**.

After you have been authenticated, you can access the protected network resources to which you have been granted access.

Viewing Infranet Controller Status

To view the status of an Infranet Controller:

1. Open the **Infranet Controllers** list in the navigation pane.
2. Select the Infranet Controller for which you want status information.

Infranet Controller status information includes the following:

- Server URL—Name or IP address of the Infranet Controller
- Status—Status of the connection.
- Session time—Amount of time (in hours:minutes:seconds) remaining in the session with the Infranet Controller. The default session time is configured by your network administrator. You can extend your session by clicking the **Extend Session** button.
- Server address—IP address of the Infranet Controller.
- Compliance—Message indicating whether your computer meets the network security policies.

Disconnecting from an Infranet Controller

To disconnect from an Infranet Controller:

1. Select **Infranet Controllers** in the navigation pane.
2. Select the Infranet Controller from which you want to disconnect.
3. Clear the **Connect to the Infranet Controller** check box.

Chapter 10

Managing Trusted Servers

This chapter describes trusted servers and how to manage trust, trusted servers, certificates, and certificate authorities.

Trust Configuration Overview

Trust configuration is a critical part of secure network communication. OAC lets you authenticate the servers to which you are connecting so that you can be certain you are connecting to the intended server. Authenticating server trust protects you from intrusion or hostile attacks from someone pretending to represent that server.

You can configure trust for authentication servers if you use EAP-TTLS, EAP-TLS, or EAP-PEAP authentication. Configuring trust settings is required for protocols that implement mutual authentication and is a recommended security measure. See “Server Validation—Mutual Authentication” on page 61. Refer also to “Certificates” on page 112 and “Mutual Authentication” on page 110 for more information.

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

When EAP authentication occurs using the EAP-TTLS, EAP-TLS, or EAP-PEAP protocols, the authentication server sends a server certificate that represents the server’s trust credentials to your computer. OAC verifies the server certificate before it continues communicating with the server. If OAC cannot verify the server’s trust credentials, it ends the authentication process and terminates communication with the server.

NOTE: To configure a trusted server with OAC, the root certificate authority (CA) or intermediate CA for the server certificate chain must be installed in the trusted root or intermediate certificate store.

To configure OAC to trust a server, you specify the name of the server and the certificate chain to which the server belongs. You can allow OAC to trust any server that bears a specified signed certificate.

Methods for Configuring Trust in OAC

There are two methods for configuring trust, a simple method and an advanced method. In most cases, the simple method is sufficient. The advanced method provides considerably more granularity for configuration and is intended for large enterprises. It is also intended for users who are experienced with trust.

Table 12 summarizes the differences between the simple and the advanced methods of configuring trust.

Table 12: Trust Configuration Methods and Differences

Trust Option	Trust Setting	Trust Method
Certificate name	Regardless of its name (any)	Simple or Advanced
Certificate name	Exact match	Simple or Advanced
Certificate name	Server name must end with the following name	Advanced
Certificate name type	Domain Name in Subject Alternative Name or Common Name	Advanced
	Domain Name in Subject Alternative Name	Advanced
	Subject Name	Advanced
Signed certificate	Specify	Simple or Advanced
Maximum number of intermediate certificates		Advanced

Simple Trust Configuration

Simple trust configuration requires that you know only the following information:

- You know the name of the certificate authority (CA) that signed your server certificate.
- You have the CA certificate installed in the Trusted Root Certificate store on your endpoint machine.

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

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

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

- A certificate from any certificate authority in your certificate authority chain. This could be the certificate of a root or an intermediate certificate authority.

To configure trust using the simple method:

1. Specify the authentication server or intermediate CA server domain name or the ending of the domain name (for example, acme.com).

2. Specify a certificate from any certificate authority in your certificate authority hierarchy. This can be the certificate of a root or an intermediate certificate in the hierarchy.

Adding a Trusted Server

To add a trusted server:

1. Select **Configuration > Trusted Servers** from the Odyssey Access Client Manager navigation pane.

2. Select **Add** in the Trusted Servers dialog box.

3. When the Add Trusted Servers Entry dialog box opens, specify identity and certificate information for the trusted server or servers.

   - To specify a server by name, enter the identity of the trusted server in the **Server name must end with** box.

     Each server has a unique name that the server certificate uses to identify itself. That name is commonly located in the Subject CN box of the server certificate. It may sometimes be located in the Subject Alternative Name field or in the Common name field.

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

   - To trust all servers that use the specified signed certificate, select **Trust any server with a valid certificate regardless of its name**. When you select this option, OAC displays < any > in the **Server name must end with** box.

4. Specify the name of the root CA that issued the certificate associated with the trusted server.

   a. Click **Browse** to display the Select Certificate dialog box, which lists the trusted root CAs for which you have a certificate.

   b. Select the appropriate certificate from the list and click **OK**.

The **Server certificate must be issued by** box displays the name of the selected root CA. The name that appears need not be the name of the certificate authority that directly issued the server certificate. The server certificate might be issued by any authority in the chain.

5. Optionally, click **View** to display the contents of the root CA certificate.

6. Select **OK** to close the Add Trusted Servers Entry dialog.

Removing a Trusted Server

To remove an entry from the trusted servers list:

1. Select **Configuration > Trusted Servers** from the Odyssey Access Client Manager navigation pane.

2. Select the entry you want to remove in the Trusted Servers dialog box.

3. Select **Remove**.

Editing a Trusted Server Entry

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

To edit an entry in the trusted servers list:

1. Select **Configuration > Trusted Servers** from the Odyssey Access Client Manager navigation pane.

2. Select the entry from the Trusted Servers dialog box.

3. Select **Edit**.

The Trusted Server Properties dialog box appears. From this dialog box, you can change the server domain and select a different certificate. See “Adding a Trusted Server” on page 91.

Advanced Trust Configuration

Use the advanced method for more detailed control over trust configuration. This method displays the entire trust tree and shows trusted servers added using the simple method and those added using the advanced method. Advanced trust configuration lets you to specify server identity in more detail and to specify how many intermediate CAs to trust.

Each path through the trust tree defines a set of rules for matching a certificate chain. See “Displaying a Trust Tree” on page 93. OAC trusts an authentication server only if its certificate chain matches at least one path through the trust tree.

NOTE: If you do not understand certificates and certificate chains, do not attempt to configure trust using the advanced method. Consult your network administrator as to how to configure trusted servers.

A path through the trust tree contains two or more nodes:

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

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

Displaying a Trust Tree

To display the trust tree:

1. Select **Configuration > Trusted Servers**.
2. **Advanced**. The Trusted Servers dialog box appears and lets you view the trust tree.

Adding Certificate Nodes

In the advanced trust configuration method, before you configure a certificate, add the certificate first, then add the identity using the <any> setting.To add a new certificate to the top level of the trust tree:

1. Select **Configuration > Trusted Servers**.
2. Click **Advanced**.
3. Select the **Add Certificate** button. The Select Certificate dialog box appears.
4. Select a certificate from the list and select **OK**. You can select a certificate from the list of intermediate or trusted root certificates.

Adding Authentication Servers or Intermediate CA Nodes

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

To add an authentication server or intermediate certificate authority to the tree, follow these steps from the Trusted Servers dialog box:

1. Select **Configuration > Trusted Servers**.
2. Click **Advanced**.
3. Select the node in the tree below which you want to add the new item.
4. Select **Add Identity** in the Trusted Servers dialog box. The Adding Identity dialog box appears. Fill it in according to the directions in "Adding Identity" on page 94.
5. Enter the information that defines the rules that OAC uses to match a certificate in the server's certificate chain to this node.
6. Select **OK**.

Adding Identity

When you select **Add Identity** in the Trusted Servers dialog box, the Add Identity dialog box appears.

To set the matching rules for a single node in the trust tree from the Add Identity dialog box:

1. For Trust a server or intermediate CA with a valid certificate, select one of the following options:
   - **Regardless of its name**—Match any certificate, provided that it is signed by the certificate authority in the node above it.
   - **If its name matches the following name exactly**—Require that the name in the certificate match the name that you specify.
   - **If its name ends with the following name**—Require that the name in the certificate is subordinate to the name you specify. For example, a certificate with name sales.acme.com would match an entry of acme.com.
2. **Server or intermediate CA**—Enter the name (or final elements of a name) that you want to match. This box is not required if you select **Regardless of its name**. The form of the name depends on your choice of server or intermediate CA name type.
3. **Server or intermediate CA name type**—Indicate how the name is interpreted and where in the certificate the name is found.

   Select one of the following:

   - Select **Domain Name in Subject Alternative Name or Common Name** if the domain name (for example, acme.com) is found in the Subject Alternative Name box in the certificate or, if that is not present, the Common Name within the Subject box of the certificate. This is the most typical choice.

- Select **Domain Name in Subject Alternative Name** if the domain name is found in the Subject Alternative Name box in the certificate. This is similar to but more restrictive than the previous choice.

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

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

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

NOTE: If you enter text with commas, enclose them with single quotation marks.

4. For Maximum number of intermediate certificates, set the number of certificates that might appear in the chain between this node and the node directly above this node. Select a number between 0 and 5 or Unlimited:

   - If you select **0**, if the certificate that matches this node must have been signed using the certificate that matches the node above this node.

   - If you select **1**, if the certificate that matches this node might have been signed by the certificate that matches the node above or by a certificate that in turn has been signed by the certificate that matches the node above.

   - If you select a number between 2 and 5, if that number of certificates might appear in the chain between the certificate that matches this node and the one that matches the node above it.

   - If you select **Unlimited**, if any number of certificates might appear in the chain between the certificate that matches this node and the one that matches the node above.

5. Select **OK**.

Removing Trust Tree Nodes

The node you remove can be any of the following:

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

To remove a node:

1. Select the node in the tree to remove.
2. Select **Remove**. The selected node and any node beneath it is removed.

Viewing Certificate Information

To display detailed information about any certificate at the top level of the trust tree:

1. Select **Configuration > Trusted Servers**.
2. Click **Advanced**.
3. Select a certificate.
4. Select **View Certificate** from the Trusted Servers dialog box.

Managing Untrusted Servers

Under the following conditions, you can trust a previously untrusted server during network authentication:

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

In this case, a Service dialog box appears while you are authenticating to the network. The Service dialog box shows the entire certificate chain between the authentication server and a trusted root certificate authority.

Trusting a Server Permanently

To trust a server permanently:

1. Select **Add this trusted server to the database.**
2. Select **Yes**.

The server is added to the list of trusted servers, using the name shown in the **Server name must end with** box (see "Adding a Trusted Server" on page 91). You can edit the server name. For example, if the server name is auth2.acme.com, you can change it to acme.com if you want to trust all authentication servers belonging to the acme.com domain.

Displaying Certificate Information

To see detailed information for a certificate in the chain:

1. Select the certificate.
2. Select **View**.

To trust this server temporarily while you authenticate and connect to the network, select **Yes**; otherwise, select **No**.

You might be prompted to enter your password, depending on the profile that you set up for this connection. If you select **Yes**, temporary trust is sustained until you restart OAC or select **File > Forget temporary trust** from the Odyssey Access Client Manager menu bar.

Chapter 11

Viewing Log Files and Diagnostics

This chapter describes how to access and view log files and diagnostics information. A Juniper Networks technical support member might ask you to access this type of information if you are troubleshooting an OAC problem.

NOTE: Some log file and diagnostic options may not apply if you are running OAC in a traditional (non-UAC) network.

Viewing Logs

A log file for OAC shows the events and transactions that transpire during a network session. Among those events and transactions might be messages that indicate a problem or an error. A technical support member can use information from the log file to isolate, detect, and diagnose specific problems that occur and might ask you to display the log file and possibly send the contents by e-mail.

To display a log file:

1. Select **Tools > Logs** from the Odyssey Access Client Manager menu bar. The Log Viewer appears.

2. Click **Settings**. The Settings dialog box appears and displays the current log messages.

Log Viewer Controls

The Log Viewer contains the following controls:

- **Settings**—Controls Log Viewer preferences for debug level, buffer size, and appearance. The Settings dialog box contains the following options:

  - **Debug Level**—Sets the debug level, which ranges from 0 (minimal logging) to 5 (verbose logging).

  - **Maximum number of lines to buffer**—Configures the maximum number of log lines that appear in the log viewer.

NOTE: The more number of lines you specify, the greater the memory consumption when the log viewer is running.

  - **Text Color/Window Color/Font**—Configures the appearance of the text displayed in the log viewer window.

- **Find**—Locates specific text in the log messages displayed in the log viewer.
- **Clear**—Clears the current contents of the log viewer.
- **Save All**—Save the log files in a single .zip file. You can browse to a preferred location and specify the name of the file.
- **Copy**—Copies selected text in the log viewer window to the Windows clipboard.
- **Freeze**—Stops automatic scrolling of the log viewer window.
- **Flow**—Resumes automatic scrolling in the log viewer window.
- **Annotate**—Inserts a specified text marker into the current log file, such as "Begin annotation." This option lets you bracket a section of the log file to make it easier for technical support staff to locate and diagnose a problem without having to read through the entire log file.

  For example, if you are experiencing a reproducible problem, insert a beginning annotation comment, such as "Start here" and then reproduce the problem behavior. After the problem has occurred, add an "End here" annotation comment to locate the beginning and end of the events in question.

  Save the log file and send it to your technical support agent. This makes it easier and faster for your technical support agent.

Viewing Diagnostics

There are six categories of diagnostics information.

1. Select **Tools > Diagnostics** from the Odyssey Access Client Manager menu bar.
2. Select one of the following diagnostic functions from the drop-down options.
   - IPsec Diagnostics
   - IPsec Configuration
   - Network Agent Diagnostics
   - Host Enforcer Configuration

- Network Configuration
- Route Configuration

NOTE: In a UAC network, access to protected resources behind an Infranet Enforcer can be configured to use IPsec to encrypt protected data. That data is encrypted while it is transferred between a server and an endpoint.

IPsec Diagnostics

This option shows you the current IPsec routing policies that have been downloaded to OAC from the Infranet Controller configuration and used with the IPsec service on your computer. The IPsec diagnostics information is global. It shows encrypted packets sent or received for all IPsec policies (for all Infranet Controllers connected) that apply.

IPsec Configuration

This option shows you configuration information for the IPsec policies that apply to the current session and information about the Infranet Enforcers to which the OAC can connect. These are the current IPsec routing policies that have been downloaded to OAC from the Infranet Controller configuration and used with the IPsec service on your computer. The policies shown are for all of the Infranet Controllers to which you are connected.

NOTE: The UAC network might be configured for IPsec encryption and Network Address Translation-Traversal (NAT-T) to access protected resources. In this case, when you use the **ipconfig** command to check a machine IP address, you might notice addresses for multiple physical machine adapters as well as an IP address for a Juniper Network Agent Virtual Adapter. The appearance of a virtual adapter address indicates that NAT-T is part of the network configuration. This information might also appear in the configuration and diagnostic data for IPsec.

Network Agent Diagnostics

Use this option if you are asked by your network administrator or by a technical support member to display the diagnostics and send the data in an e-mail message for troubleshooting.

Host Enforcer Configuration

This option shows you configuration information for all of the Host Enforcer policies being enforced. OAC downloads these policies from the Infranet Controller after you sign in to the Infranet Controller. The policies shown are for all Infranet Controllers to which you are connected. If your Infranet Controller Role changes, additional policies might be applied or removed.

Network Configuration

This option shows the current configuration for all available network adapters. The output is the same as that for the ipconfig /all command. The adapters are either real adapters (wired or wireless) or virtual adapters, such as those that might be configured for IPsec.

Route Configuration

This option shows the current IP route table for the system. The output is the same as that for the route print command.

Refresh

Click this button to refresh the current data display.

Save All Diagnostics

Click this button to collate the output of all the diagnostic functions and save the output to a file. You can then archive the file or send it to the technical support member for analysis.

NOTE: It can be helpful to the technical support staff if you provide the approximate time of the event you are reporting.

Appendix A

Network Security Concepts

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

Network Security

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

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

OAC enables you to make secure network connections using protocols that adhere to one or more of the following standards:

- IEEE (Institute of Electrical and Electronic Engineers) standards for wireless LANs. These include 802.11a, 802.11b, and 802.11g. See "802.11 Wireless Networking" on page 105.
- IEEE 802.11i enhancements to 802.11. These were introduced to overcome some of the security weaknesses of 802.11.
- The Wi-Fi Alliance second generation of Wi-Fi protected access. Wi-Fi protected access 2 (WPA2) (with advanced encryption standard (AES) encryption) adheres to the strong 802.11i enhancements. See "Wi-Fi Protected Access and Encryption Methods" on page 108 for definitions.
- Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP), which complies with a subset of 802.11i. While WPA is not as strong as WPA2, it addresses some of the security weakness of 802.11. See "Wi-Fi Protected Access and Encryption Methods" on page 108 for definitions.
- The IEEE 802.1X standard. 802.1X supplements the 802.11 standards with secure server-based wireless network connections. See "802.1X Authentication" on page 109.

- IP Security (IPsec) is a set of protocols used to secure (encrypt) IP data packets being exchanged on a network. For network security, data being transferred between protected network resources and endpoint computers should be encrypted. A Juniper Networks UAC network can include a firewall that provides an IPsec gateway deployed in front of protected resources to enforce your security policies. OAC supports IPsec encryption as part of conforming to those policies.

Encryption and Association for Secure Authentication

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

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

- Data encryption is used to secure data that is exchanged between a client device and an access point (or another computer).

- Encryption keys are a sequence of characters that an encryption algorithm uses to make plain text unreadable unless you share the encryption keys to decode the encrypted message. Encryption keys are key components of data encryption algorithms. Encryption keys might also be used for access point association.

- After a wireless client has connected with an access point, the user of that client device can be authenticated for network access. Authentication is used to secure the relationship between a user of a wireless-equipped computer and an authentication server. For example, wireless network authentication that is based on the 802.1X standard can use cryptographically strong (and dynamically generated) encryption keys.

Authentication Overview

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

- Preconfigured secrets, called WEP (wired-equivalent privacy) keys. These keys are intended to encrypt the data transferred between the client and the access point and can be used to keep unauthorized users off the wireless network and to encrypt the data of legitimate users. See “Wired-Equivalent Privacy” on page 107 for a description of WEP-based encryption that complies with 802.11 standards.

- Preshared passphrases used to generate keys for WPA or WPA2 association. Preshared passphrases enable you to configure a simple phrase that is used to generate cryptographically strong encryption keys to be used with AES or TKIP encryption. AES and TKIP periodically change the encryption keys in use. The generated keys keep unauthorized users off the wireless network and encrypt the data of legitimate users. See "Wi-Fi Protected Access and Encryption Methods" on page 108 for a description of AES or TKIP encryption methods that enhance the 802.11 standards.

- Authentication using an 802.1X-based protocol. This method uses a variety of underlying authentication protocols to control network access. The stronger protocols provide cryptographically protected mutual authentication of the user and the network. In addition, you can configure OAC so that keys that are used to encrypt wireless data are generated dynamically. 802.1X-based authentication can use WEP, AES, or TKIP encryption, depending on network hardware/firmware. See "802.1X Authentication" on page 109 for information about authentication using 802.1X. See "Wi-Fi Protected Access and Encryption Methods" on page 108 for a description of some of the strongest available association and encryption modes.

OAC Features for a Secure Network

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

- You can require user authentication. A user must be authenticated by the network before being allowed access to the network and make it safe from intruders. See "Extensible Authentication Protocol" on page 109 for an overview of the OAC authentication protocols. For protocol configuration details, see "Adding or Modifying a Profile" on page 50.

- You can require data encryption between the wireless client and the access point. The wireless connection between a client and an access point must be encrypted so that eavesdroppers cannot access private data. For configuration details, see "Selecting an Encryption Method" on page 75.

- You can configure server trust for mutual authentication. The network must be authenticated (trusted) by the user before the user credentials can be released to the network to make a network connection. This prevents a wireless device that might be posing as a legitimate network from impersonating the network and gaining access to the user's computer. For configuration details, see "Methods for Configuring Trust in OAC" on page 90.

- Mutual authentication between user and network must be cryptographically protected. This type of mutual authentication requires 801.1X-based protocols and prevents connections to phony networks.

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

Types of 802.11 Wireless Networks

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

Access Point Networks

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

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

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

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

When you connect to a network through an access point, you are using the 802.11 *infrastructure mode*. See “Specifying a Network Type (Channel)” on page 74 and for information about configuring infrastructure network connections.

Peer-to-Peer Networks

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

The 802.11 standard refers to peer-to-peer network connectivity as *ad-hoc mode*. See “Specifying a Network Type (Channel)” on page 74, and “Specifying an Association Mode” on page 74 for information about configuring ad-hoc network connections.

Wireless Network Names

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

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

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

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

Wired-Equivalent Privacy

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

- Shared—Use this mode when the access point requires that you preconfigure a WEP key for association. When 802.11-based preconfigured (static) WEP keys are in use, the client and the access point share the same secret keys and a client is not allowed to access the network unless it can prove it knows the preconfigured WEP keys assigned to the access point. This is not as secure as authenticating with 802.1X methods. See “802.1X Authentication” on page 109. You can configure shared association following the directions in “Specifying an Association Mode” on page 74.

- Open—Use this mode for WEP-based data encryption when the access point does not require that you preconfigure a static WEP key for association. You can configure open association using the directions in “Specifying an Association Mode” on page 74.

NOTE: You can obtain stronger network security when you use dynamic encryption key generation and 802.1X-based authentication. For shared association, a preconfigured key that is used only for access point association is still required. See “802.1X Authentication” on page 109 and “Extensible Authentication Protocol” on page 109.

See the following sections on how to select an association mode in OAC:

- “Selecting an Encryption Method” on page 75 for directions on selecting WEP encryption when using the shared or open association mode.

- “Preconfigured Keys (WEP)” on page 77 to use static WEP keys with OAC.

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

Wi-Fi Protected Access and Encryption Methods

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

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

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

NOTE: With access points enabled for WPA2 or WPA, you can obtain the stronger network security when you use dynamic encryption key generation and 802.1X-based authentication. See “802.1X Authentication” on page 109 and “Extensible Authentication Protocol” on page 109.

See the following sections:

- “Specifying an Association Mode” on page 74 to use WPA2 or WPA association mode with OAC
- “Specifying an Association Mode” on page 74 to use AES or TKIP encryption with WPA2 or WPA association
- “Selecting an Encryption Method” on page 75 to configure a passphrase that is used in encryption key generation.
- “Using FIPS Secure Encryption (FIPS Edition Only)” on page 75 for information about this data encryption security module.

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

FIPS 140-2 Encryption Using AES and WPA2 or XSec

Federal Information Processing Standard (FIPS) that are issued by the National Institutes of Standards and Technology (NIST) include standards for cryptographic security (FIPS 140-2). With the appropriate licensing and configuration, OAC implements level 1 of this secure encryption standard using WPA2 or xSec association mode and AES encryption. OAC provides approved cryptographic algorithms and approved modes of operation for the Cryptographic Module Specification and provides the strongest cryptographic key management mechanisms.

802.1X Authentication

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

The WEP protocol has various shortcomings when preconfigured keys are in use. Preconfigured WEP keys contribute to administrative overhead and pose security weaknesses. Although the encryption methods calculated from keys generated from preshared passphrases are stronger than WEP encryption calculated from static WEP keys, the use and distribution of passphrases can pose administrative and security problems. The use of 802.1X protocols in wireless networks addresses these problems.

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

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

Extensible Authentication Protocol

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

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

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

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

- EAP-TTLS (tunneled transport layer security)
- EAP-PEAP (protected EAP)
- EAP-TLS (transport layer security)
- EAP-FAST (flexible authentication through secure tunneling)
- EAP-JUAC (an inner EAP protocol for connecting to an Infranet Controller)
- EAP-POTP (protected one-time password)
- EAP-SIM and EAP-AKA (authentication and key agreement)
- EAP-LEAP (lightweight EAP)

Mutual Authentication

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

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

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

EAP-TLS

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

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

EAP-TTLS

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

EAP-TTLS authentication is performed using a password or other credentials. Password-type credentials are transported in a securely encrypted "tunnel" that is established using the server certificate. Within the EAP-TTLS tunnel, you can employ any of a number of inner authentication protocols. With tunneled password credentials, user authentication can be performed against the same security database that is already in use on the corporate LAN. For example, Windows Active Directory or an SQL or LDAP database might be used. See "Configuring TTLS Inner Authentication Protocols" on page 63.

If your enterprise has a user-based certificate infrastructure in place, you have the option to configure user certificate-based credentials for EAP-TTLS authentication, with or without tunneled password credentials. See "Using Certificates for EAP-TTLS Authentication" on page 67.

EAP-PEAP

EAP-PEAP is comparable to EAP-TTLS, both in its method of operation and its security. However, EAP-PEAP is not as flexible as EAP-TTLS and it does not support the range of inside-the-tunnel authentication methods that EAP-TTLS supports. Commercial implementations of this protocol that started appearing at the beginning of 2003 had interoperability problems. Nevertheless, this protocol is in widespread use. EAP-PEAP is a suitable protocol for performing secure authentication against Windows domains and directory services. See "List of Outer Authentication Protocols" on page 60.

EAP-FAST

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

EAP-JUAC

EAP-JUAC is an inner EAP protocol developed by Juniper Networks for authenticating access to an Infranet Controller. EAP-JUAC is compatible with TTLS and PEAP.

EAP-POTP

EAP-POTP is a protocol developed by RSA Security, Inc. With this protocol, users can request authentication using their RSA SecurID token cards for password credentials.

This secure two-factor authentication protocol provides cryptographically strong end-to-end mutual authentication, AES data encryption, personal identification number (PIN) management, and session resumption. The EAP-POTP protocol does not rely on certificates or require a certificate infrastructure. EAP-POTP has strong encryption, data integrity, and authentication support.

EAP-SIM and EAP-AKA

EAP-SIM and EAP-AKA (authentication and key agreement) are the two EAP methods that you can use for wireless network authentication based on your SIM card credentials.

EAP-LEAP

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

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

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, e-mail, and many other types of data exchange.

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

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

- A public key
- A private key

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

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

Your enterprise certificate authority might issue certificates to smart cards. OAC supports all types of user certificates, including smart card certificates.

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

There is a date on which each certificate expires. Additionally, a certificate granting authority can revoke a certificate. Expired or revoked certificates are not valid, but certificates can be reissued 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 and consist of:

- An end entity certificate
- An intermediate certificate (optional)
- A root certificate

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

Certificates and Server Trust

A server certificate is a cryptographic object that uniquely identifies a RADIUS or Infranet Controller server. The server certificate contains a chain of parent certificates that provide a chain of trust. The certificates between the server certificate and the top or root certificate are called *intermediate certificates*.

The topmost entity in the certificate chain is the *trusted root certificate.*

To trust a server, you must trust the server certificate and all the certificates in the certificate chain.

Defining Trust for OAC

You define trust by installing the server certificate's root into your root certificate store. Odyssey does this for you the first time you attempt to contact a server. A network administrator typically configures server trust.

Reauthentication

During reauthentication, 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 computer and access point. The access point might use these shared keys to refresh the keys used to encrypt data. By frequently refreshing keys, you can thwart cryptographic attacks.

See "Using Automatic Reauthentication" on page 34 for information about configuring this feature.

Session Resumption

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

After 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. This feature is particularly useful when you have a wireless connection and are moving ("roaming") from one access point location in a building to another. With this feature enabled, along with automatic reauthentication, your network connection is not interrupted and there is no need to reconnect.

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

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

See “Enabling Session Resumption” on page 34.

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

Index

Numerics

A

C

D

E

F

G

H

R

S

T

U

W

X