



Juniper Networks
Odyssey Access Client for Windows

User Guide

Enterprise Edition
FIPS Edition

Release 4.7
October 2007

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

Part Number: OAC-TD-UG47W

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

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

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

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

Table of Contents

	About This Guide	ix
	Audience	ix
	Conventions	ix
	Documentation	x
	Product Documentation and Release Notes	x
	Context-Sensitive Help	xi
	Contacting Customer Support	xi
Chapter 1	Odyssey Access Client Overview	1
	How OAC Operates in a Network	2
	Authentication in a Unified Access Control Network	2
	Endpoint Security Enforcement	4
	Quarantine and Remediation	5
	Authentication in a Traditional Network (Without UAC)	5
	Using OAC in FIPS Mode (FE Only)	6
	Authentication Method for FIPS Mode	7
	Understanding Network Security	8
Chapter 2	Installing OAC	9
	Before You Begin	9
	Disabling Fast User Switching	9
	Fast User Switching Difference on Windows Vista	10
	Requirements	10
	Operating Systems	10
	Network Adapter Cards	10
	Wireless Adapter Requirement for Windows Vista	10
	Network Hardware	11
	Browsers	11
	Licenses	11
	Installing OAC in a UAC Network	11
	Agentless Clients	12
	Automatic Trust Configuration for Infranet Controllers	12
	Loading a Certificate to the Trusted Server Database	12
	Installing OAC in a Traditional Network	13
Chapter 3	Odyssey Access Client Manager	15
	Menu Options	16
	File Menu Options	16
	View Menu (Hidden Settings)	17
	Tools Menu Options	17
	Help Menu	19
	Sidebar	19

Adapters List.....	19
Infranet Controllers List	19
Configuration Folder	19
Profiles.....	20
Networks	20
Auto-Scan Lists.....	20
Trusted Servers	20
Adapters	20
Infranet Controllers.....	20
Content Dialog Box	20
Informational Graphics and Detailed Status	21
Viewing Signal Power Status.....	21
Viewing Connection Status	21
Viewing Encryption Key Information.....	22
Viewing Endpoint Trust Status	22
Tray Icon Status Indicators	23
Basic Tray States	23
Event Categories that Display a Notification Dialog Box.....	23
Shortcut Keys.....	23
Exiting from OAC Manager	24
Chapter 4	Using Odyssey Access Client Manager
	25
Opening Odyssey Access Client Manager.....	25
Authentication Credentials	25
Connection Types	26
Connecting and Signing on to an Infranet Controller	26
Managing Concurrent Infranet Controller Sessions.....	27
Infranet Controller Session Limits	27
Compliance Failure and Remediation.....	28
Disconnecting from an Infranet Controller	29
Making a Wireless Network Connection	29
Reinitializing a Wireless Connection	30
Scanning for Wireless Networks.....	30
Making Concurrent Network Connections.....	31
Using Wireless Suppression	31
Making a Wired Network Connection	31
Connecting to a Different Network	32
Reconnecting to a Network	32
Disconnecting from a Network	32
Session Management Tasks	32
Surveying Local WiFi Airwaves	33
Viewing Network Signal Strength	33
Running a Script	33
Checking for New Scripts.....	34
Managing SIM Card PIN Settings.....	34
Disabling the SIM Card PIN	34
Changing the PIN for a SIM Card.....	34
Unblocking a SIM Card.....	35
Enabling the Prompt for a Smart Card PIN.....	35
Cache PIN	35
Using Forget Password	35
Using Session Resumption.....	36
Using Automatic Reauthentication.....	36
Enabling Server Temporary Trust	37

Managing EAP-FAST Credentials	38
Managing Windows Logon Settings	38
Configuring Network Connection Timing	39
Prior-to-Windows-Logon Behavior and Smart Cards	41
Odyssey Access Client Administrator	41
Troubleshooting	41
Viewing and Saving Log Files	41
Running Diagnostics	41
Chapter 5	Managing Network Adapters
	43
Adding Network Adapters	43
Global Management Settings for Adapters	44
Renaming an Adapter	44
Removing an Adapter	45
Removing an Adapter Using the Adapter Dialog Box	45
Removing an Adapter Using the Sidebar Icon	45
Managing Adapter Connections to a Network	45
Selecting an Adapter	46
Connecting to a Network	46
Making a Wireless Network Connection	47
Making a Wired Network Connection	47
Making Concurrent Connections	48
Disconnecting from a Network	48
Scanning for Wireless Networks	48
Reconnecting to a Network	49
Checking Adapter Status	49
Connection Status Information	50
OAC Interaction with Other Adapter Software	51
Chapter 6	Configuring Authentication Profiles
	53
Adding or Modifying a Profile	54
Specifying Profile Names	54
Specifying User Info	55
Specifying a Login Name	55
Setting Passwords	55
Using Certificates	57
Using Certificates for Authentication	57
Using Soft Tokens	58
Using SIM Cards	59
Setting a SIM Card ID	59
Managing PIN Settings	60
Configuring EAP-SIM Identity	60
Setting Up Authentication	60
Selecting Authentication Protocols	61
Validating a Server Certificate—Mutual Authentication	61
Setting Token Card Credential Options	62
Setting an Anonymous Name	63
TTLS Settings	63
Selecting an Inner Authentication Protocol	64
EAP Inner Authentication Protocols	65
Using Certificates with EAP-TTLS Authentication	65
PEAP Settings	66
Using Certificates with EAP-PEAP Authentication	67

EAP-POTP Run-Time Options.....	67
Configuring EAP-POTP as an Inner Authentication Method	68
Configuring Authentication for Infranet Controllers	68
Setting JUAC as an Inner Authentication Protocol for TTLS	69
Setting JUAC as an Inner Authentication Protocol for PEAP	70
Setting a Preferred Realm and Role	70
Authenticating with Token Cards.....	71
Removing a Profile.....	71
Sample Profile Configuration	71
Chapter 7 Configuring Networks	73
Configuring Network Settings.....	73
Adding or Modifying Network Properties	73
Network Settings	74
Specifying a Network Name (Network SSID)	74
Connecting to Any Available Network	74
Scanning for Available Networks.....	74
Adding a Network Description	75
Specifying a Network Type.....	75
Specifying a Channel.....	75
Specifying an Association Mode	75
Encryption Methods for an Association Mode	76
FIPS Association Mode (FE Only)	76
FIPS Secure Encryption (FE Only)	77
Configuring Networks that Do Not Broadcast an SSID	77
Specifying an Authentication Profile.....	78
Automatic Key Generation	78
Preconfigured Key Settings	78
Preshared Keys (WPA or WPA2)	79
Preconfigured Keys (WEP)	79
Removing a Network	80
Sample Network Configuration Setups	81
Sample Configuration for a Corporate WiFi Network	81
Sample Configuration for a Wireless Hotspot Network	81
Sample Configuration for a Home Wireless Network	82
Chapter 8 Managing Auto-Scan Lists	83
Adding an Auto-Scan List	84
Using Preemptive Networks	85
Modifying an Auto-Scan List.....	85
Viewing the Networks in an Auto-Scan List	86
Removing an Auto-Scan List.....	86
Chapter 9 Managing Infranet Controller Connections	87
Adding an Infranet Controller to the OAC Configuration	88
FIPS Mode Constraint	88
Signing on to an Infranet Controller.....	88
Viewing Infranet Controller Status	89
Infranet Controller Connection Types (L2 versus L3)	89
Compliance Failure and Remediation	90
Disconnecting from an Infranet Controller	90

Chapter 10	Managing Trusted Servers	91
	Overview of Trust Configuration	91
	Configuring Trust in OAC	92
	Using the Simple Method to Configure Trust	93
	Adding a Trusted Server Entry	93
	Server Identity	94
	Removing a Trusted Server Entry	94
	Editing a Trusted Server Entry	95
	Using the Advanced Method to Configure Trust	95
	Displaying a Trust Tree	95
	Adding Certificate Nodes	96
	Adding Authentication Servers or Intermediate CA Nodes	96
	Adding Identity	96
	Removing Nodes	98
	Viewing Certificate Information	98
	Managing Untrusted Servers	98
Chapter 11	Viewing Log Files and Diagnostics	101
	Accessing Log Files	101
	Log Viewer Controls	101
	Settings	101
	Find	102
	Clear	102
	Save All	102
	Copy	102
	Freeze	102
	Flow	102
	Accessing Diagnostics	102
	IPsec Diagnostics	103
	IPsec Configuration	103
	Network Agent Diagnostics	103
	Host Enforcer Configuration	103
	Network Configuration	104
	Route Configuration	104
	Save All Diagnostics	104
Appendix A	Network Security Concepts	105
	Network Security	105
	Encryption and Association for Secure Authentication	106
	Authentication Overview	106
	Odyssey Access Client Features for a Secure Network	107
	802.11 Wireless Networking	108
	Types of 802.11 Wireless Networks	108
	Access Point Networks	108
	Peer-to-Peer Networks	108
	Wireless Network Names	109
	Wired-Equivalent Privacy	109
	WiFi Protected Access and its Encryption Methods	110
	FIPS 140-2 Encryption Using AES and WPA2 or XSec	111
	802.1X Authentication	111
	Extensible Authentication Protocol	112
	Mutual Authentication	112
	Certificates	113

EAP-TLS	114
EAP-TTLS	114
EAP-PEAP	115
EAP-FAST	115
EAP-JUAC	115
EAP-POTP	115
EAP-SIM and EAP-AKA	115
EAP-LEAP	115
Reauthentication	116
Session Resumption	116

Appendix B	Glossary	119
	Index	133

About This Guide

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

- OAC Enterprise Edition (EE)
- OAC Federal Information Processing Standards (FIPS) Edition (FE)

OAC can be deployed in a network that includes Juniper's Unified Access Control security solution, where authenticated access to protected network resources is managed by an Infranet Controller. OAC can also be deployed in a traditional network where OAC negotiates with a AAA server for authenticated access. Where there are differences in product features or options based on licenses or the type of network where OAC is deployed, this guide identifies those differences where they apply.

You can read this manual in PDF format. It is on the Juniper Networks web site at:

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

Audience

This manual is intended for all users of OAC who need wired or wireless network access and who need to manage and configure the available features and controls. Depending on the corporate security policies in place at your company, some features of the OAC might be preconfigured and restricted to administrators.

This manual is also intended for network administrators who are responsible for configuring and maintaining OAC configurations for users.

Conventions

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

Table 1: Notice icons




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

Table 2: Text conventions (except for command syntax)

Convention	Description	Examples
Bold typeface	Indicates buttons, field names, dialog box names, and other user interface elements.	Use the Scheduling and Appointment tabs to schedule a meeting.
Plain sans serif typeface	Represents: <ul style="list-style-type: none"> ■ Code, commands, and keywords ■ URLs, file names, and directories 	Examples: <ul style="list-style-type: none"> ■ Code: certAttr.OU = 'Retail Products Group' ■ URL: Download the JRE application from: http://java.sun.com/j2se/
<i>Italics</i>	Identifies: <ul style="list-style-type: none"> ■ Terms defined in text ■ Variable elements ■ Book names 	Examples: <ul style="list-style-type: none"> ■ Defined term: An <i>RDP client</i> is a Windows component that enables a connection between a Windows server and a user's machine. ■ Variable element: Documents and Settings > <i>username</i> > Application Data > Funk Software > Odyssey Access Client > newScripts ■ Book name: <i>Odyssey Access Client User Guide</i>.

Documentation

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

Product Documentation and Release Notes

To access release notes and product documentation for Odyssey Access Client go to:

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

You can find the *Odyssey Access Client Administration Guide* there. If you use Odyssey Access Client on a network with Juniper's Unified Access Control security solution, refer to the *Unified Access Control Administration Guide* also available on the same Juniper Networks Web site. Refer also to the

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

To access context-sensitive help for the OAC, press F1 on the keyboard. The resulting help provides information that is relevant to your current OAC context.

Contacting Customer Support

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

Chapter 1

Odyssey Access Client Overview

Odyssey Access Client (OAC) is networking software that runs on endpoint computers (PCs, laptops, 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 Steel-Belted Radius, must validate each user. In a Juniper Unified Access Control (UAC) network, the user's endpoint 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 the wireless networks that you access.
- Configure and use authentication profiles to connect to secure networks.
- Connect to a Juniper 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.
- Use scripts to update your current OAC configuration.

FE Only:

- 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 a AAA (authentication) server.

With 802.1X, you get authenticated to a network based on matching authentication (EAP) protocols and on your user credentials, such as a password, certificate, or a token card. For details about configuring EAP protocols, see “Selecting Authentication Protocols” on page 61. For details about setting up credentials, see “Specifying User Info” on page 55.

OAC can be deployed in two distinct network environments:

- A traditional network manages authentication with a standard AAA server, such as Steel-Belted Radius.
- A network with Juniper’s Unified Access Control (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.

Authentication in a Unified Access Control Network

Unified Access Control (UAC) provides enhanced security measures that not only authenticate users but verifies that the software running on the endpoint computer complies with corporate security policies. See “Endpoint Security Enforcement” on page 4.

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 endpoint’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. Examples of compliance might be that you have the correct antivirus software version and security setting or that you have the latest operating system patch level installed.

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

In a UAC network, OAC users can authenticate to the network in the following ways:

- A wired (Layer 2) connection through an 802.1X switch (Figure 2).
- A wireless (Layer 2) connection through an 802.1X wireless access point (Figure 2).
- 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 (Figure 1).

The Infranet Controller performs the authentication for each of these connection methods. You can also connect to both a network (wired or wireless) and to an Infranet Controller. Ask your network administrator for the recommended connection methods for your network.

In a UAC network, you can connect to one or more networks and to one or more Infranet Controllers. Your network connection might be authenticated by a AAA server that is integrated with the Infranet Controller (in a UAC network) or by a separate AAA server external to the Infranet Controller. Figure 1 and Figure 2 show the difference in network connections for a network without 802.1X support and a network with 802.1X support.

Figure 1: OAC Authentication in a Network without 802.1X (Layer 3)

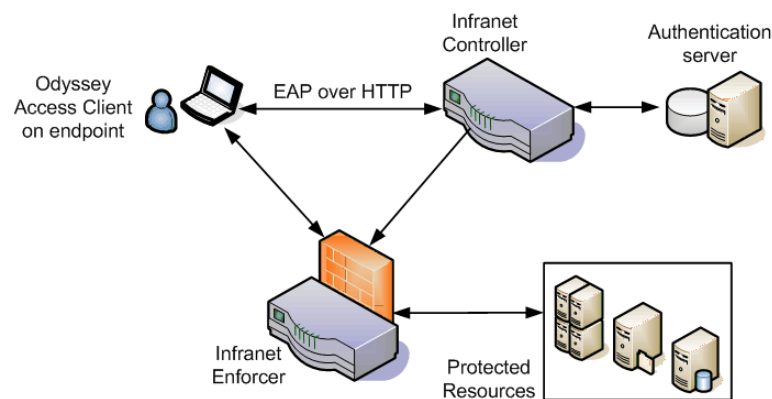
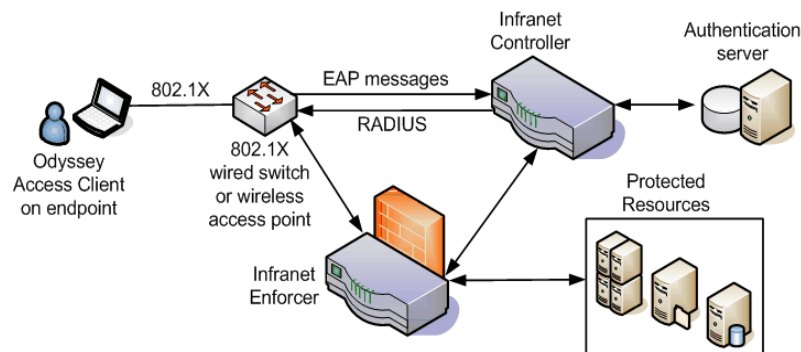


Figure 2: OAC Authentication in a Network with 802.1X (Layer 2)

In a UAC network, OAC communicates with the Infranet Controller to authenticate the user and the endpoint and to establish security compliance. The Infranet Controller authenticates you as a user and determines which protected resources you can access based on your user name and the realm and role to which you belong. (See “Setting a Preferred Realm and Role” on page 70.) The Infranet Controller then informs another appliance on the network, called the Infranet Enforcer, about the resources that you are allowed to access. The Infranet Enforcer is a firewall that enables or denies you access to the resources.

For a broader discussion of UAC components and concepts, refer to the *Juniper Networks Unified Access Control Administration Guide*.

Endpoint Security Enforcement

Networks that include an Infranet Controller perform security enforcement checking to ensure that all endpoints (computing devices) comply with the network’s security policy. The purpose of security checking is to enhance the security of the network and to reduce problems that can result from network security threats, such as viruses, spyware, and other software security problems.

For endpoints that comply with network security policies, users can have full access to protected networks based on the policies configured in the Infranet Controller for the user’s realm and role.

For endpoints that do not comply with network security policies, users can expect one of the following results:

- The endpoint might be denied network access until it meets compliance requirements. In some case, network access might be prevented only momentarily during automatic remediation— for example, while the endpoint’s anti-virus software settings are modified to conform to the network’s security policy.
- The endpoint might be granted access to protected networks while being brought into compliance in the background.

- The endpoint might be granted limited access to a special quarantine network or VLAN while being brought into compliance. Compliance involves performing the actions specified by remediation instructions, such as installing Windows update patches, after which the endpoint might be granted access to protected resources.

Quarantine and Remediation

The Infranet Controller checks your computer (endpoint) regularly for compliance with all prescribed security requirements, such as anti-virus software that is running on your computer.

If an endpoint does not comply with an organization's security policies, the Infranet Controller can isolate the endpoint to a quarantine (restricted) network. The quarantine network might provide access to limited network resources, such as a file server, but prevent the endpoint from connecting to (and possibly infecting) the rest of the organization's network.

Remediation is the process of bringing an endpoint into compliance with an organization's security policies. The remediation process brings the endpoint into compliance by sending remediation instructions to the endpoint. In most cases, remediation happens automatically in the background.

When a quarantined endpoint complies with the security policies of the protected network, the Infranet Controller redirects it to the protected network automatically.

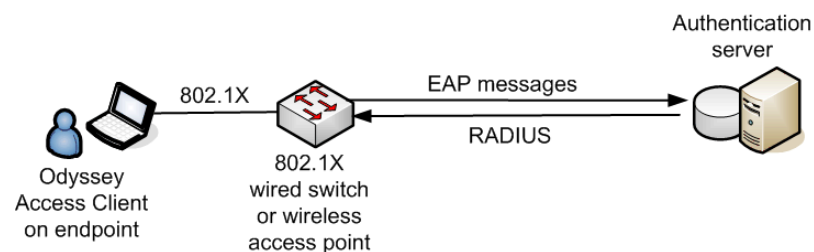
Note that remediation does not necessarily require quarantine. Some administrators choose to allow most or all endpoints onto the protected network while performing automatic remediation on those endpoints.

Authentication in a Traditional Network (Without UAC)

When deployed in traditional networks that do not include UAC components, OAC negotiates authentication to the network either through an 802.1X switch or through an 802.1X wireless access point.

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

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



The steps in a typical 802.1X authentication process are:

1. When a wireless client attempts to connect to an 802.1X network, it signals an access point that it is making an authentication request. This step is commonly known as *association*.

2. Whether you are making a wired or a wireless connection, the network access device (an access point or 802.1X switch) forwards your authentication request to the authentication server.

The authentication process might involve establishing a secure tunnel between the wireless access point and the authentication server.

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

3. If the authentication succeeds, the server informs the network access device to allow access to the client endpoint. Depending on the information returned for the user, the server might restrict the user's access to specific networks or resources.
4. The network access device then instructs the client that it has been authenticated and now has access to the network.

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

Using OAC in FIPS Mode (FE Only)

OAC supports a special FIPS (Federal Information Processing Standards) Edition license for use by government agencies with specific requirements for OAC. FIPS mode is an advanced feature. Consult your network administrator before changing any current FIPS mode configuration settings.

To use the OAC FIPS 140-2 (level 1) compliant secure encryption module, you must satisfy the following requirements:

- You must have a FIPS-compliant adapter and network hardware:
 - Install an adapter driver that is compatible with the Juniper Networks, Inc. FIPS encryption module. OAC FE requires a modified driver to enable the wireless adapter to run 802.11i in FIPS mode. Contact Juniper Networks for the latest list of verified wireless adapters. See “Adding Network Adapters” on page 43 for information about configuring adapters for use with OAC.
 - You are not required to install a new driver if you use xSec association. See “FIPS Association Mode (FE Only)” on page 76.
 - Refer to the OAC User Web Page at http://www.juniper.net/customers/support/products/aaa_802/oac_client_user.jsp for more information about the appropriate adapter drivers for use with the OAC FIPS module.
- A user certificate must be installed on the client machine prior to configuring OAC for FIPS-compliant connections. This operation should only be performed by a network administrator. Note the following about the user certificate for FIPS-compliant network connections:

For FIPS 140-2 compliance, the private key of a user's personal certificate must be protected using encryption that has been approved by the National Institute of Standards and Technology (NIST) for FIPS 140-2. 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
- Versions of Windows 2000 that have applied the correct service pack

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

- You enable FIPS Mode by selecting **File > FIPS Mode On**.
- The profile that you create for your FIPS-compliant network must have the certificate-based EAP-TLS as the sole authentication method configured. See “SIM Card Manager Use Case for this Option” on page 18 for profile configuration instructions.
- You must create a network that uses WPA2 (or xSec) association and AES encryption and associate the network with this profile. In addition, enable **FIPS mode required** when you create or edit the network if you require FIPS encryption for all connections to this network. Otherwise, do not enable this item. See “FIPS Secure Encryption (FE Only)” on page 77.
- You must configure trust for the network server. See “Managing Trusted Servers” on page 91.

To disable FIPS mode, select **File > FIPS Mode Off**. Do not disable FIPS mode if you require FIPS mode connections.

Authentication Method for FIPS Mode

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

The only outer authentication method supported for FIPS mode is EAP-TLS; no inner authentication methods are supported. This means that when FIPS mode is on, users cannot connect to an Intranet Controller. See “Connecting and Signing on to an Intranet Controller” on page 26.

Understanding Network Security

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

Chapter 2

Installing OAC

This chapter discusses how to install OAC in a UAC network that includes an Infranet Controller and in a traditional network that uses a AAA server for authenticating user access. The installation methods differ depending on which type of network you have. The specific OAC installation requirements are also identified in this chapter.

Before You Begin

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

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.

Perform the following administrative tasks before installing OAC:

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

Disabling Fast User Switching

Running Remote Desktop (RDP) with Fast User Switching turned on in Windows 2000 or Windows XP interferes with OAC operation and RDP operation. Fast User Switching is disabled by default for computers that are part of a domain. However, for computers in a workgroup, you must disable Fast User Switching manually.

To disable Fast User Switching:

1. Go to **Start > Control Panel > User Accounts > Change the way users log on or off**.
2. Clear the setting for **Fast User Switching**.

With Fast User Switching turned off, Remote Desktop and OAC can run together without a problem.

Fast User Switching Difference on Windows Vista

Fast User Switching is enabled for domain users on Windows Vista. On Windows XP, Fast User Switching is disabled by default for domain users.

This means that all concurrent user sessions on a Windows Vista system can access current desktop connections—both networks and Infranet Controllers. Thus, if one user has a current network connection, other users logged in to the same Vista system can access that connection. This can pose a security risk. For example, a background process running in one user session can piggyback onto the network access granted to the active session and access resources to which that user should not have access rights.

Requirements

The following sections are software and hardware requirements for OAC.

Operating Systems

OAC runs on the following operating systems:

- Windows 2000 Professional with SP 4.
- Windows XP Professional SP 2.
- Windows Vista Business Edition (on 32-bit systems only).

Network Adapter Cards

On Windows 2000 and Windows XP, OAC is compatible with any wireless adapter card that supports standard 802.11 interfaces.



NOTE: For wired network authentication, your network must include at least one 802.1X-compliant switch or hub and a AAA server.

FE Only:

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

Wireless Adapter Requirement for Windows Vista

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, they display as an unknown adapter type.

Network Hardware

For network authentication, you need:

- An 802.1X-compliant network switch (for wired authentication).
- An 802.1X-compliant access point (for wireless authentication).
- A AAA (authentication, authorization, and accounting) server, such as Juniper Steel-Belted Radius.
- An Infranet Controller and an Infranet Enforcer. This applies only if your network includes Juniper Unified Access Control (UAC) solution. An Infranet Controller includes a AAA server, so there is no need for a separate implementation.

FE Only:

To associate to a network using xSec, your network must include at least one switch that is capable of implementing the xSec protocol. OAC FE requires a modified driver to enable the wireless adapter to run 802.11i in FIPS mode. For more information about FIPS mode, see “FIPS Mode On / FIPS Mode Off (FE Only)” on page 17.

There are no special adapter or driver requirements for using xSec in FIPS mode.

Browsers

If your network includes an Infranet Controller, you must have Internet Explorer 6.0 or later installed. OAC uses some services present in Internet Explorer 6.0. You can use any browser but your system must have the required version of Internet Explorer installed.

Licenses

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.

You can purchase licenses from Juniper Networks, Inc. For details, select **Help > License Keys** from the OAC Manager tool bar.

Installing OAC in a UAC Network

This section describes ways of downloading OAC to your computer in a network that includes an Infranet Controller. To install OAC on your system:

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.

When you access the Infranet Controller, it will prompt you for authentication credentials, such as your user name and password. If 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.

If you attempt to access the Web or protected resources on your corporate network before having OAC installed on your system, a network firewall might redirect you automatically to a special Web portal that downloads and installs OAC on your system (if your system has been configured to include a captive firewall). This type of Web portal is optional and might not be present on your network.

A network administrator might deploy OAC to multiple users with an MSI (Microsoft Installer) file. In this case, OAC may have default configuration settings but may not yet be configured specifically for the network resources you need to access. Once OAC is running, navigate to an Infranet Controller, whereupon initial OAC configuration settings will be downloaded automatically.

The initial configuration provides minimal configuration settings that allow you to connect or disconnect from the network.

Agentless Clients

For some roles, such as guest accounts or other roles with restricted access, the Infranet Controller provides a transparent (“agentless”) connection. There is no management interface like the one provided for OAC. Access to the Infranet Controller is through a Web interface.

Automatic Trust Configuration for Infranet Controllers

OAC is configured automatically to trust an Infranet Controller 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 the endpoint. 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 pre-installed on your computer, then the prompt does not appear during installation.

Loading 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 endpoint 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 will fail. See “Enabling Temporary Trust” on page 23 for more information about temporary trust settings.

Installing OAC in a Traditional Network

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

To install OAC, follow these steps:

1. Run the OAC installer using one of the following procedures:
 - Insert the installation CD into your CD-ROM drive. The installation process starts automatically. If the installation process does not start up, double-click **setup.exe** on the CD.
 - If you downloaded (or otherwise obtained) the OAC installer (**OdysseyAccessClient.msi**) file, double-click the installer for OAC.
2. The installation wizard prompts with a series of questions. Your answers determine how to install and configure OAC.
3. Click **Install** to begin the installation process.
4. 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, there is no prompt for credentials.

Chapter 3

Odyssey Access Client Manager

Odyssey Access Client Manager is the management interface from which you can connect to networks, sign on to Infranet Controllers, and manage your network sessions.

This chapter discusses the layout of Odyssey Access Client Manager, where to look for specific information (such as status), and summarizes the options that are available. Your administrator can disable features in the OAC configuration to provide just the features you need, so some of the options shown in Figure 4 may not appear in your copy of OAC.

The Odyssey Access Client Manager display consists of the following sections:

- The *menu bar* at the top of the display provides a range of pull-down options.
- The *sidebar* on the left displays lists of configured adapters and Infranet Controllers and a set of configuration folders that you can use to perform configuration tasks.
- The *content dialog box* to the right of the sidebar is for viewing status, establishing network connections, and making configuration settings based on the configuration folder that you select.

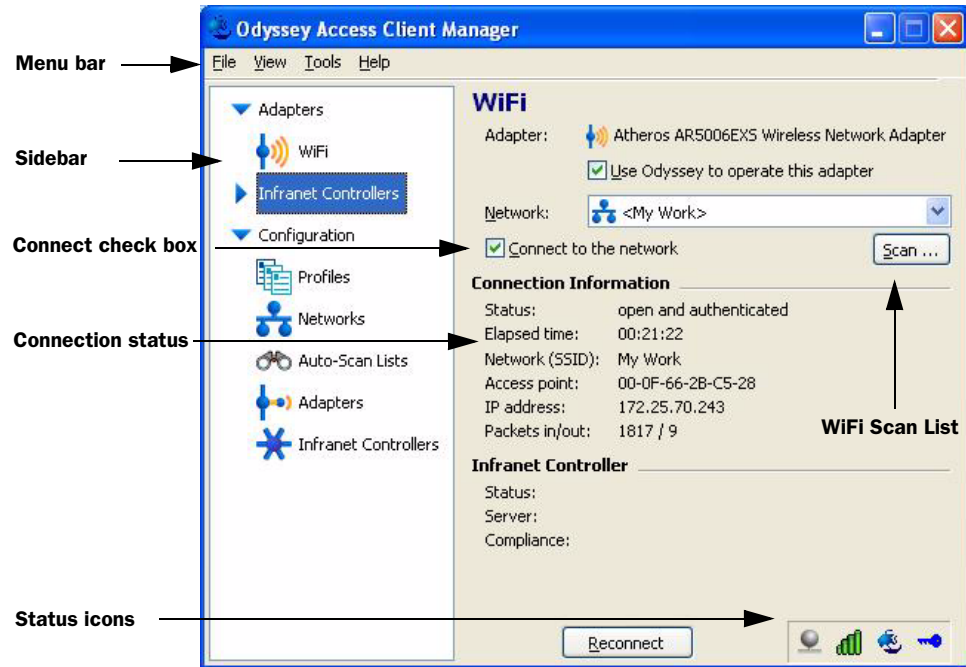
If you select a network adapter from the **Adapters** list or an Infranet Controller from the **Infranet Controllers** list, a connection dialog box displays connection status information and a button to connect to or disconnect from the network or the Infranet Controller, respectively.

Each of the selections in the **Configuration** folder has a corresponding content dialog box for configuring options.

- The **Connection Information** and **Infranet Controller** status areas in the dialog box provide session information for the adapter or Infranet Controller connection.
- The **Reconnect** button reinitializes the connection to the network. See “Reinitializing a Wireless Connection” on page 30.
- The icons at the bottom right indicate current status for security compliance, wireless signal power, authentication status, and encryption status. See “Informational Graphics and Detailed Status” on page 21.

Figure 4 shows the initial screen that appears when you open Odyssey Access Client Manager. Each of the key areas in the dialog box are pointed out.

Figure 4: Odyssey Access Client Adapter Connection Dialog Box



Menu Options

The Odyssey Access Client Manager menu bar contains the option categories discussed in the following sections. The options available in each category are summarized here and discussed in more detail in the cross-referenced sections.

File Menu Options

The **File** menu options are:

- **Forget Password**—Discard the current password or PIN that you used to logon. If your password is required later, a dialog box prompts you for it. If you do not enable this option, OAC remembers your password for the duration of the session. See “Using Forget Password” on page 35.
- **Forget Temporary Trust**—Discontinue a temporary trust setting for a server. See “Enabling Server Temporary Trust” on page 37 and “Managing Trusted Servers” on page 91 for more information about trusted servers.
- **Close Window**—Closes the Odyssey Access Client Manager display. To reopen it, double-click the program icon in the system tray.
- **FIPS Mode On / FIPS Mode Off (FE 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 are using the OAC FIPS Edition. See “Using OAC in FIPS Mode (FE Only)” on page 6.

View Menu (Hidden Settings)

The **View** menu shows settings that have been hidden by your administrator so that you see only those OAC features and options that you typically 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.

Tools Menu Options

The **Tools** menu lists the following session control options:

- **Odyssey Access Client Administrator**—Used for managing and deploying OAC configurations and available only if you have administrative privileges. See “Odyssey Access Client Administrator” on page 41.
- **SIM Card Manager**—Manages SIM card PIN settings. See “Managing SIM Card PIN Settings” on page 34.
- **Survey Airwaves**—Displays Wi-Fi and peer-to-peer networks in your vicinity. See “Surveying Local WiFi Airwaves” on page 33.
- **Logs**—Opens the Log Viewer and displays the current contents of the `debuglog.log` file. See “Accessing Log Files” on page 101 for more information about log files.
- **Diagnostics**—Displays a variety of diagnostic information that is helpful for troubleshooting. See “Accessing Diagnostics” on page 102 for more information about log files.
- **Run Scripts**—Use this option to run scripts to update your OAC configuration. See “Running a Script” on page 33 and “Checking for New Scripts” on page 34.
- **Preferences**—Toggles the display of the system tray icon, the control panel icon, or the OAC splash screen.

- **Windows Logon Settings**—Overrides the default setting for network connection timing. See “Managing Windows Logon Settings” on page 38.
- **Options**—Offers four categories of settings organized under separate tabs:
 - **Security**
 - **Enable session resumption:** With session resumption enabled, you can restrict session resumption for any session older than the time that you set. See “Using Session Resumption” on page 36.
 - **Enable automatic reauthentication:** If enabled, this option enables periodic automatic reauthentication and sets the reauthentication frequency setting. See “Using Automatic Reauthentication” on page 36.
 - **Enable server temporary trust:** This option lets you authenticate to a network whose authentication server is not yet configured as trusted in the Trusted Servers dialog box. See “Enabling Server Temporary Trust” on page 37.
 - **Prompt for smartcard PIN:** Enable this option to have OAC prompt for a smart card Personal Identification Number (PIN). See “Managing SIM Card PIN Settings” on page 34.
 - **Interfaces**
 - **Wireless suppression:** This option defaults to a wired network connection whenever it is available in order to preserve wireless bandwidth for users who do not have a wired connection. See “Using Wireless Suppression” on page 31.
 - **Manage wired/wireless adapters:** Enable this option to have OAC any wired or wireless adapter configured automatically. See “Global Management Settings for Adapters” on page 44.
 - **Preemptive Networks**
 - Use this option to specify an auto-scan list of preferred networks that will always override any network or auto-scan list currently enabled in the WiFi connection dialog box. See “Using Preemptive Networks” on page 85.
 - **EAP-FAST**
 - Use this option to control when OAC prompts for EAP-FAST credentials. See “Managing EAP-FAST Credentials” on page 38.
 - **Default Login Name**
 - Use this option modify 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 options are summarized below:

- **Help Topics**—Opens the OAC online help interface.
- **License Keys**—Shows when the current OAC license expires and may let you add or remove an OAC license key if you have permission.
- **Register Odyssey Access Client**—Lets you register OAC.
- **Odyssey Access Client User Page**—Opens the Juniper Customer Support Web page.
- **Juniper Networks, Inc. Home Page**—Opens the home page for Juniper Networks.
- **Purchase Information**—Access the Juniper Networks Web page to buy other products.
- **About**—View the specific release version of OAC and see how to buy OAC.

Sidebar

The sidebar contains a group of folders, each of which contains one or more items that you can enable and 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 folders and the selections that you can make and notice how the content dialog box changes for each selection.

Adapters List

The **Adapters** list shows the wired and wireless adapters currently configured in OAC. Select an adapter from this list to display a network connection dialog box that shows connection status and a **Connect to the network** check box to toggle the connection on or off.

Infranet Controllers List

The **Infranet Controllers** list shows each Infranet Controller currently configured. Select an Infranet Controller from this list to display a connection dialog box that shows connection status and a **Connect to the Infranet Controller** check box to toggle the connection on or off.

This dialog box also shows current endpoint trust status.

Configuration Folder

Use the **Configuration** folder to add, delete, or modify configuration settings for any of the options that appear in this folder.

Profiles

Use this folder to set up logon and authentication configuration information, such as your password or certificate. See “Adding or Modifying a Profile” on page 54.

Networks

Use this folder to configure individual networks and their connection, encryption type, and whether to use 802.1X authentication. You can use this to set up an ordered list of networks to use with an auto-scan list. See “Configuring Networks” on page 73.

Auto-Scan Lists

Use this folder to set up an ordered list of wireless networks that you have configured. The auto-scan list is convenient when you are moving your computer from one wireless network to another. OAC uses it to scan the list of networks and make the first possible connection automatically. See “Managing Auto-Scan Lists” on page 83.

Trusted Servers

Use this folder to add, remove, and configure trusted network servers and to set certificate and identity information for the servers that might authenticate you when you connect. Configuring this feature is required for protocols that implement mutual authentication and is a recommended security measure. See “Managing Trusted Servers” on page 91.



NOTE: Contact your system administrator before changing any trust configuration settings.

Adapters

Use this folder to configure wired and wireless adapters for your computer. See “Managing Network Adapters” on page 43.

Infranet Controllers

Use this folder to configure individual Infranet Controllers to which you need to connect. See “Managing Infranet Controller Connections” on page 87.

Content Dialog Box

A content dialog box shows configuration options and controls for the option that you select. For example, if you select an adapter from the **Adapters** list or an Infranet Controller from the **Infranet Controllers** list, a dialog box displays the network address for the adapter or the Infranet Controller, a variety of session status information, and a check box to enable or disable a connection.

If you click an Infranet Controller from the **Infranet Controllers** list, a connection dialog box displays connection and endpoint status information and a button to connect to or disconnect from a network.

Each of the selections in the **Configuration** folder has a corresponding content dialog box for setting up and configuring the related options such as networks, Infranet Controllers, and trust.

Informational Graphics and Detailed Status


Status icons appear in the lower right part of the connection dialog box to provide visual status for your connection. You can use the mouse or the keyboard to view detailed connection status for any status icon. Use the mouse to point to a graphical status button with the mouse and hold down the left mouse button.

Figure 5 is a sample endpoint compliance status display for an Infranet Controller connection.


Viewing Signal Power Status

The signal power graphic shows you how strong the signal is between your PC and the access point. The more bars that are filled in, the stronger the signal. You can interpret the signal power status graphic as follows:

 Strong signal power

 Moderate signal power

 Weak signal power


 Faint signal power


 No signal power

Viewing Connection Status

The connection status icon (the OAC “sail boat” icon) shows the current state of your connection and whether you are authenticated. The icons below appear in the Odyssey Access Client Manager dialog box to indicate the authentication status of a single connection to a network or to an Infranet Controller.

The same icons appear in the Windows tray but indicate the authentication status for all current connections so that if any individual connection status should fail or deteriorate, the icon color changes to indicate that state change. This is useful, especially if Odyssey Access Client Manager is not currently open on your desktop. See “Tray Icon Status Indicators” on page 23.

 (outline)—Not connected

 (red)—Not connected, due to failed authentication

 (black)—Connected, but authentication not in use

 (blue) – Connected and authenticated

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

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

Viewing Encryption Key Information

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

 (outline)—Data is not encrypted

 (black)—Data is encrypted using static keys

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

Status details for these icons can show the following types of information:

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

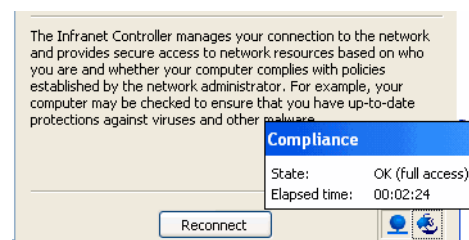


NOTE: A WEP encryption key has a secret part whose length is either 40 or 104 bits and a 24-bit non-secret part that changes for each packet. Thus, the total key length is either 64 or 128 bits. OAC reports the length of the secret part, which is either 40 or 104 bits.

Viewing Endpoint Trust Status

Figure 5: In a UAC network, the Endpoint Trust Status section near the bottom of the connection dialog box includes an icon that indicates endpoint trust status.

Status Icon Details







 Endpoint trust status indicator

Tray Icon Status Indicators

The OAC icon also appears in the system tray to provide additional status information. If connection status degrades, the system tray icon displays a pop-up dialog box with specific information related to the status change. The red, blue or black indicates a state change for any current connection to a network or an Infranet Controller and can include a warning icon (a yellow triangle superimposed over the bottom of OAC boat icon) to indicate that there is a TNC failure (the health of your computer is not good).

Basic Tray States

-  (outline) – OAC is either disabled or there are no network adapter or Infranet Controller connections.
-  (red) – At least one connection has failed due to authentication (authentication failures or protocol) failure. This condition does not reflect a connectivity failure.
-  (black) – There is at least one Layer 2 or Layer 3 connection configured but no connections have yet been made, even though there are no failures.
-  (blue) – There is at least one Layer 2 or Layer 3 connection and all configured connections are valid.

Event Categories that Display a Notification Dialog Box

Three general event types cause a notification dialog box to appear above the OAC tray icon:

- Connection failures related to authentication or integrity checking.
- Limited connectivity related to authentication or integrity checking.
- Disconnection from the network.

Shortcut Keys

In addition to using the mouse to access buttons, tabs, and dialog boxes in OAC, you can use your keyboard to access OAC features.

On Windows XP systems, press the Alt key to see the shortcut keys available on any given screen. For older Windows versions, the shortcut keys are always underlined.

To move between the dialog boxes of the OAC, press the up and down arrows on your keyboard. You can use the keyboard arrows to move through option button (mutually exclusive) selections.

You can use the following keyboard shortcuts to select the graphical information buttons on the Connection dialog:

- Alt + 1 to display the signal power information
- Alt + 2 to display the connection status information

- Alt + 3 to display the encryption key information

Press Alt in conjunction with the appropriate arrow key on the keyboard to implement the corresponding arrow button features, such as those in the Auto-Scan Lists dialog.

Exiting from OAC Manager

To exit from Odyssey Access Client Manager, right-click the OAC icon in the system tray and click **Exit**. Odyssey Access Client Manager closes but you can re-launch it at any time by double-clicking the same tray icon. OAC runs as a Windows service unless you remove it, so you can run OAC or re-launch Odyssey Access Client Manager at any time.


Chapter 4

Using Odyssey Access Client Manager

Odyssey Access Client Manager allows you to configure connection settings and monitor connection status. Depending on the edition (license) of OAC that you are using, some sections might not apply. Those distinctions are identified clearly.

This chapter addresses individual tasks and specific options that are available in OAC during a network session.

Opening Odyssey Access Client Manager

When OAC is installed on your computer, it runs as a Windows service. However, the OAC user interface, called Odyssey Access Client Manager, might not be open on the desktop. You can tell if it is open by checking the system tray on the lower right of your screen for the OAC icon . (The system tray is in the lower right corner of the monitor display where some program icons are shown.)

Open Odyssey Access Client Manager in one of the following ways:

- From the system tray, double-click the OAC icon or right-click it and select Odyssey Access Client Manager.
- From the Windows task bar, go to **Start > Programs > Juniper Networks > Odyssey Access Client > Odyssey Access Client Manager**.

Authentication Credentials

The first time that 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. For example, you might be prompted for your username and a password, a soft token, or a smart card PIN. In most cases the dialog box will indicate what is required. Your administrator can also tell you the specific logon credentials you need.

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 the Infranet Controller has been configured for single sign on, there is no prompt for credentials. In both cases, your Windows logon credentials are used.

Connection Types

Once Odyssey Access Client Manager is open, you need to establish a network connection. OAC supports the following connection types:

- Connection to an Infranet Controller.
- Connection to a wireless 802.1X network.
- Connection to a wired 802.1X network.
- Connection to a public or home WiFi network.

Connecting and Signing on to an Infranet Controller

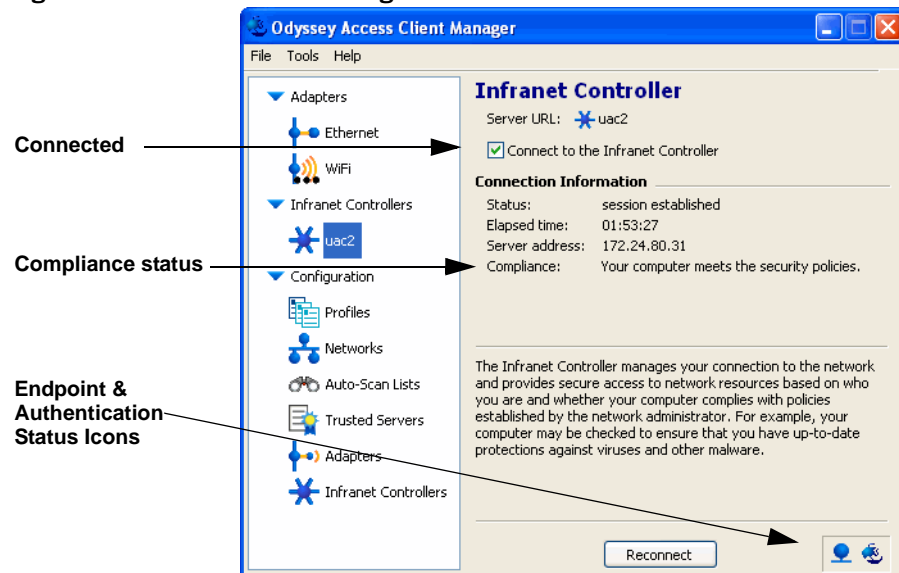
You must be authenticated before you are allowed access to protected network resources. This means that the first time you connect to an Infranet Controller during an OAC session, you must sign on by providing the required credentials.

To sign on to an Infranet Controller:

1. Open the **Infranet Controllers** list in the sidebar.
2. Select the Infranet Controller to which you want to connect.
3. An Infranet Controller dialog box opens (see Figure 6 on page 27) and shows the IP address of the Infranet Controller in the Server URL field. Below that is a **Connect to the Infranet Controller** check box.
4. Enable the check box to connect to the Infranet Controller.
5. Sign on to the Infranet Controller when the prompt appears. The first time to connect to an Infranet Controller you must provide authentication credentials. After you have been authenticated, you can complete the sign on process and access the protected network resources to which you have been granted access.



NOTE: When you connect to an Infranet Controller, if there is a newer version of OAC available, a pop-up dialog prompts you to install it.

Figure 6: Infranet Controller Dialog Box

When you are connected, the connection dialog box displays your endpoint trust status. If the endpoint does not meet security requirements, you might be redirected to a remediation VLAN—a restricted-access network where your endpoint is updated for security compliance—before you can be authenticated by the Infranet Controller. For more information about remediation, see “Compliance Failure and Remediation” on page 28.

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. Using **Reconnect** to reinitialize the request can clear this up.

Managing Concurrent Infranet Controller Sessions

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

To connect to multiple Infranet Controller, create a profile and Infranet Controller configuration for each instance. You might need to do this is to access protected resources that are in different locations.

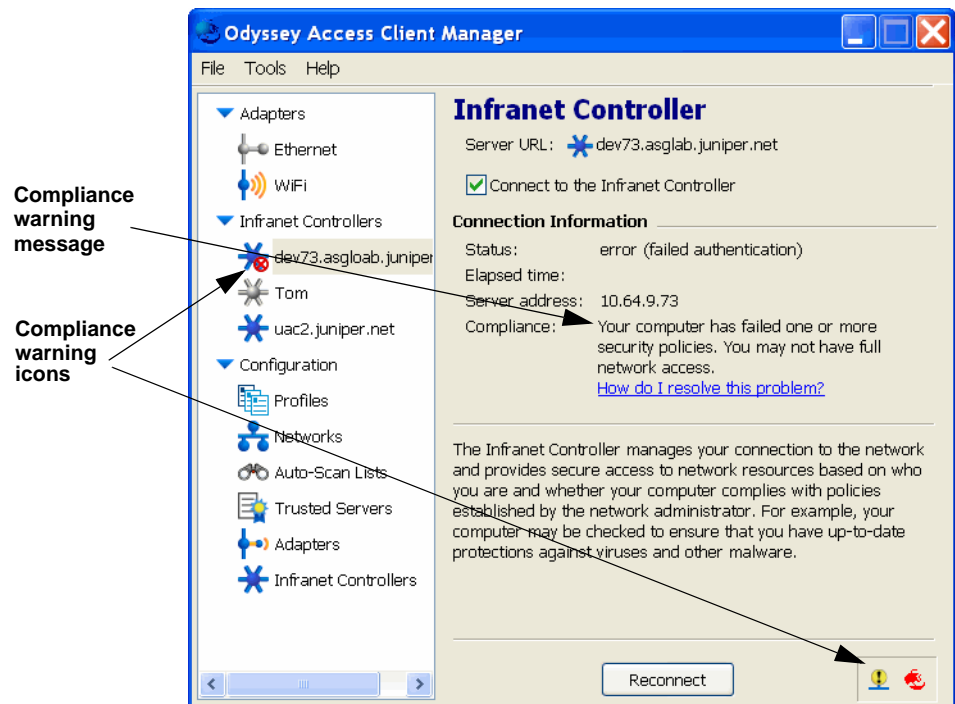
Infranet Controller Session Limits

Your administrator can restrict the number of simultaneous Infranet Controller sessions per realm that you are permitted to have so that those resources can be shared equally among users. If you already have the maximum number of sessions running and attempt to establish another one, a dialog box appears to let you know that you have the maximum number of sessions running. If this happens, you can terminate an existing session or cancel the current attempt to start a new session.

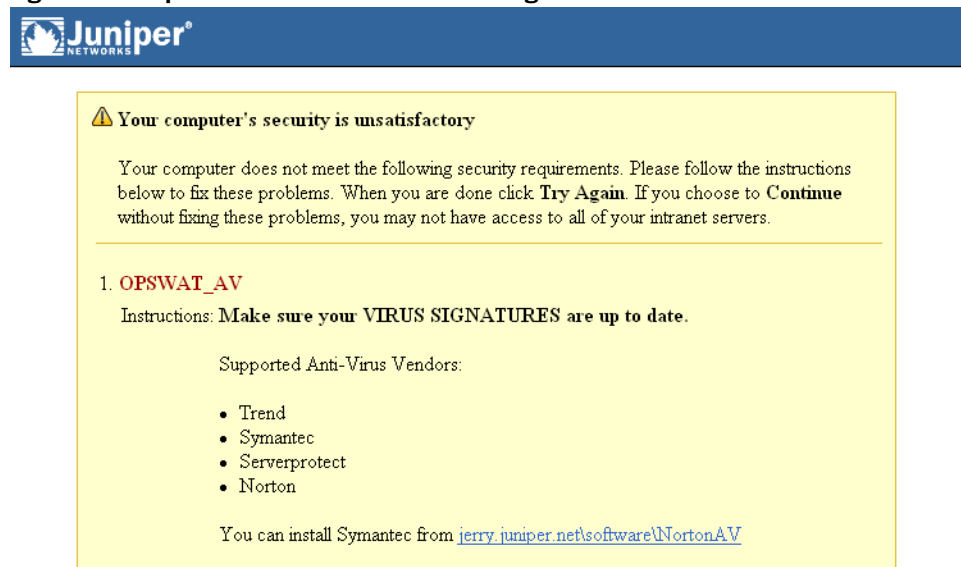
Compliance Failure and Remediation

If your computer or the software running on it does not comply with the network security policy, the connection and status icons will indicate that there is a compliance problem (see Figure 7). If there is a compliance issue, the connection might be rejected or you might need to update the endpoint software, such as the anti-virus settings or operating system patch level. This is called *remediation*. In some cases, remediation is automatic. In other cases, the connection dialog box displays a message with instructions for what to do.

Figure 7: Compliance Failure Dialog Box



When you select the **How do I resolve this problem?** link, another dialog box provides you with specific instructions for updating your computer so that it meets compliance requirements. The remediation instructions that you see might vary from the sample shown in Figure 8.

Figure 8: Sample 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. From the **Infranet Controllers** list in the sidebar, select the Infranet Controller from which you intend to disconnect.
2. In dialog box showing the Infranet Controller name, clear the **Connect to the Infranet Controller** check box.



When you are no longer connected to the Infranet Controller, the status icon changes from blue to gray.

Making a Wireless Network Connection

To connect to a wireless network:

1. From the **Adapters** list in the sidebar, select the wireless adapter to use. The WiFi dialog box opens and the **Adapter type** field indicates the type of adapter (**WiFi**) you have selected.
2. Select a wireless network from either the **Network** list or from the **Scan** list in the WiFi dialog box.
3. Click **Connect to the network** to start the network connection.

The **Connect to the network** list displays the individual networks that you have created in the Networks dialog and the auto-scan lists that you have created in the Auto-Scan Lists dialog. Any auto-scan list that you have created appears at the top of the list. These are followed by the names of configured networks. Network names appear in angle brackets, after any network description text that you have specified. Networks and auto-scan lists are distinguished by the following icons:

-  = auto-scan lists
-  = networks

The WiFi dialog box shows 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.

Reinitializing a Wireless Connection

Use the **Reconnect** button at the bottom of the dialog box to reinitialize the connection. Sometimes an authentication or connection may be in an unknown state. Wireless network connections are not always as reliable and stable as a wired connection and, from time to time, need to be refreshed. Using **Reconnect** to reinitialize the request reinitializes the connection without prompting again for authentication credentials.

Scanning for Wireless Networks

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

To connect to a wireless network that is not configured:

1. Enable **Scan** in the WiFi dialog box.

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

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

Using Auto-San Lists

An auto-scan list is a prioritized list of configured networks. Auto-scan lists appear at the top of the network list in the **WiFi** or **Ethernet** adapter connection dialog box. With an auto-scan list, OAC attempts to connect to the *first* network in the list and attempts to connect to each network in the list until it finds a network to which it can connect. See “Adding an Auto-Scan List” on page 84 for a full discussion of creating and using auto-scan lists.



NOTE: OAC can detect any wireless network that broadcasts a beacon—a data frame that represents the network’s “heartbeat.” If the beacon does not include a an SSID, OAC cannot connect to that network. To connect to such a network, you must obtain the SSID and configure the network in the OAC Networks dialog box. See “Configuring Networks that Do Not Broadcast an SSID” on page 77.

Making Concurrent Network Connections

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

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

Using Wireless Suppression

Your administrator might recommend that you enable wireless suppression. This feature defaults to a wired network connection whenever it is available in order to preserve wireless bandwidth for users who do not have a wired connection.

The purpose of wireless suppression is to conserve wireless bandwidth for users who do not have access to a wired connection.

To enable this feature, go to **Tools > Interfaces** and enable **Wireless suppression: Use wireless connection only when no wired (Ethernet) connection is present**.

Making a Wired Network Connection

If your corporate network includes network switches that support 802.1X authentication, OAC supports such connections. You must have a suitable 802.1X network adapter for this connection type and it must be configured in OAC.

OAC does not interact with switches that do not support 802.1X authentication.

To connect to a wired 802.1X network

1. From the **Adapters** list in the sidebar, select the wired adapter to use. The Ethernet dialog box opens and the **Adapter type** field indicates the type of adapter (**Ethernet**) you have selected.
2. Select an authentication profile from the **Profile** list.

The profiles that appear in this list are the ones that you have created in the Profiles dialog box. See “Adding or Modifying a Profile” on page 54.

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

Reconnecting to a Network

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

This option is useful when you are moving from one access point to another on the same network. Enabling **Reconnect** 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 currently 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. Select the adapter from the **Adapters** folder 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.

Session Management Tasks

OAC provides a variety of tools and option for managing your session once you are connected.

Surveying Local WiFi Airwaves

This option is similar to the information that you see if you click **Scan** in the WiFi connection dialog box, but **Survey Airwaves** provides more detailed information. **Survey Airwaves** displays the relative signal strength of each network along with specific details about individual access points on the network. The display presents separate tabs for information about access point and peer-to-peer networks.

To survey wireless airwaves:

Open the **Tools > Survey Airwaves** dialog.

Viewing Network Signal Strength

After selecting **Tools > Survey Airwaves** from the OAC main window, you can select the following tabs to view information:

- Access point networks
- Peer-to-peer networks

The relative figure strength of each network is indicated graphically on the far left of the Airwaves Survey dialog. 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 displayed data by clicking a column heading. For example, to sort by SSID, click the **SSID** column heading.

To refresh your airwaves survey, click **Refresh**.

To view broadcast details about any selected network listed in Airwaves Survey, click **Details**. The BSSID Information dialog appears.

To close the Survey Airwaves dialog, click **Close**.

Running a Script

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 from a known location:

1. Select **Tools > Run Script**.
2. In the Select Script File dialog box, navigate to the folder 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

Use the **Tools > Check New Scripts** option to check for new scripts or to run scripts. Your administrator might send you email with scripts to run, in which case you must save the scripts in the following directory before running them:

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.

To check for new scripts:

1. Select **Tools > Check New Scripts**.

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 device 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.

Select **Tools > SIM Card Manager** from the OAC main window to open the SIM Card Manager dialog to perform the following tasks:

- Disable the PIN for a SIM Card
- Change the PIN for a SIM Card
- Unblock the a SIM Card

Disabling the SIM Card PIN

To disable the PIN for your SIM card:

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

Changing the PIN for a SIM Card

To change the PIN for your SIM card, follow these steps:

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

Unblocking a SIM Card

If you enter the wrong PIN too many times, your SIM card might become blocked. If your card is blocked, you can unblock it by following these steps:

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

Enabling the Prompt for a Smart Card PIN

With this option enabled in the **Options > Security** tab in the Odyssey Access Client Manager, OAC 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 use this option, your authentication profile must be configured with **Permit login using my certificate** and **Use the login certificate from my smart card reader** enabled. See “Using Certificates for Authentication” on page 57 for more information about using smart card certificates for authentication.

Cache PIN

With the **Cache PIN** option enabled, OAC caches the smart card PIN that you enter and does not prompt again for a 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: Smart card prompts and caching are disabled if FIPS Mode is enabled. (FE Only)

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 again. Normally, OAC remembers the password that you provide until you reboot your PC 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 as a security measure.

If you want OAC 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 will be prompted to enter it.

If you leave your computer unattended but do not want to lock access to it completely, you can use this option to prevent unauthorized access to OAC and the protected network resources to which you have access.

Using Session Resumption

After you have been authenticated to the network and a network connection is open, your network session begins. During a session, any subsequent authentications to the same network server can be accelerated by reusing the secret information that is derived during the first authentication. This is called *session resumption*. 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 the certificate-based protocols (such as TLS) using OAC. See “Session Resumption” on page 116 for more information.

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.

To enable session resumption:

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

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

Using Automatic Reauthentication

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

If enabled, this option enables periodic automatic reauthentication and sets the reauthentication frequency setting. The default is 1 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 PC 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.

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

To enable automatic reauthentication:

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

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

Enabling 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 authenticate to 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. The default is 12 hours. See “Managing Untrusted Servers” on page 98 for more information about establishing trust.

If temporary trust is enabled, you have the following options:

- Trust an untrusted server temporarily during a network authentication. See “Managing Untrusted Servers” on page 98.
- Add the server to your trust tree in the Trusted Servers dialog box. Consequently, the temporary trust feature serves as an alternative to configuring trusted servers through the Trusted Servers dialog box.

To enable temporary trust:

1. Go to **Tools > Options > Security**.
2. Click **Enable server temporary trust**.
3. Set **Maximum time for temporary trust** to the maximum time (in hours) that you want OAC to continue to trust a server once you accept it. By default, temporary trust is enabled. The maximum time that a particular server is temporarily trusted after you accept it is 12 hours.

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

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



NOTE: These settings do not apply to servers that you choose to trust permanently if you enable **Add this trusted server to the database** when you are prompted for temporary trust. See “Managing Untrusted Servers” on page 98.

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.

When you use EAP-FAST authentication, enable one of the options that determine when to prompt for PAC credentials. The options are:

- **Prompt before acquiring credentials from a new server.** Use this option to be prompted 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.** Use this option to be prompted for new credentials if a previous authentication attempt fails.

Both EAP-FAST options are enabled by default. To restore the defaults, click **Reset Defaults**.

Managing Windows Logon Settings

Use the **Tools > Windows Logon Settings** option to override the default setting for network connection timing. This option supports users whose configuration is based on a preconfigured GINA connection timing and provides the ability to override the default timing. A use case for this option is the need to connect to a network other than the default connection configured for OAC.



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

The Windows logon options are:

- **Connect prior to logging on to Windows.** This option allows user to access a domain controller and have full access to the network at logon time. Without this option, users who have not logged on previously to a given machine cannot log on. This setting also allows logon scripts to run.
- **Connect after logging on to Windows, but before your desktop appears.** This option prevents users without cached credentials from logging on to a machine.
- **Connect after your desktop appears. This is the default option for OAC.** This option gives a user access to the network after the Windows desktop starts.

Any of these options can be configured as your default network connection timing, depending on how your network administrator sets up OAC. Additionally, your network administrator might allow you to modify the timing of default network connection settings. In this case, you can override the default network connection settings.

For example, if you can log on to your domain using cached credentials and if your administrator configured your network connection to occur prior to Windows logon, you can change your connection timing so that you connect to the network after your desktop appears.

Configuring Network Connection Timing

To modify your network connection timing, select **Tools > Windows Logon Settings** to open the Windows Logon Settings dialog. Your network administrator might have disabled some of the Windows logon features.

To modify the default timing for network connections through Odyssey Access Client, select from the following Windows logon timing options (if they are available):

- Select **After my desktop appears** to establish your network connection after all Windows startup, logon, and desktop processes are completed. This is the latest possible time that you can make a network connection.
- Select **After Windows logon, before the desktop appears** to establish your network connection after your Windows startup and Windows logon processes are completed but before your desktop processes take place.
- Select **Prior to Windows logon** to establish your network connection prior to Windows logon.

If you select **Prior to Windows logon**, then perform the following required tasks and options:

- Select the adapter and network (or profile, in the case of a wired connection) from the lists provided. Note the following:
 - Associate a profile with any network that you configure. You can configure profiles in the **Authentication** tab in the Profile Properties dialog. OAC uses your Windows logon credentials.
 - Select **Validate server certificate** on the **Authentication** tab in the Profile Properties dialog for the selected profile.
 - 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 for the selected network.

- If you select the **Use alternate settings on failure** option, you can provide an alternate wired 802.1X adapter and profile (or wireless adapter) to use for connections that take place prior to Windows logon when a connection attempt using the displayed adapter/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 logon. After selecting this option, enable **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.

- Select an option to be prompted prior to making the network connection at logon time according to the choices under Prompt to connect.
 - Select **Never** if you do not want to be prompted to connect, even if the connection attempt fails.
 - Select **On connection failure** if you want to be prompted only on connection failure. This can be useful if you experience network authentication problems, as it gives you the option to opt out of connecting to the network at logon time.
 - Select **Prior to connecting to the network** if you want to be prompted every time that you connect.

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:

- To connect after the desktop appears when you are connected to your network through a wired adapter, select **any wired adapter**. You can use this option even if your wired adapter is not connected to an 802.1X hub or switch.
- To connect after the desktop appears when you are connected to your network through one or more selected adapters, select **one of the following adapters**. This option applies to any adapter listed on the Windows Logon Settings dialog.

To edit the list of adapters:

1. Click **Edit** to open the Adapters dialog.
2. Select any adapters that you want to use for a network connection that occurs after the desktop appears.
3. Click **OK** to close the Select Adapters dialog.
4. Click **OK** to close the Windows Logon Settings dialog.

Prior-to-Windows-Logon 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. Refer to the Odyssey Access Client *Administration Guide* before using this tool.

Troubleshooting

Viewing and Saving Log Files

Your network administrator may ask you to use the **Tools > Logs** tool if you are experiencing problems with OAC. Use this option to open the OAC Log Viewer, which displays the current contents of the `debuglog.log` file. You can set the level of logging information displayed by changing the **Log level** setting. See “Accessing Log Files” on page 101 for more information about log files.

Running Diagnostics

Use the **Tools > Diagnostics** option to enable and display the following categories of diagnostic information and send the data in an email message for troubleshooting:

- IPsec diagnostics
- IPsec configuration
- Network Agent diagnostics
- Host Enforcer configuration
- Network configuration
- Route configuration

See “Accessing Diagnostics” on page 102 for more information about log files.

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.

Use the **Configuration** folder in the Odyssey Client Manager sidebar to manage the **Adapters**. An adapter must be installed on your computer before you can configure it in OAC. To use more than one adapter at a time, hold down the Ctrl key and select the entries using your mouse. At the top of the sidebar, the **Adapters** folder shows all of the network and wired adapters configured currently in OAC.



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 Client Manager identifies them as an unknown adapter type.

Adding Network Adapters

Once you add a network adapter to the OAC configuration, OAC binds to and controls it. You cannot use a different 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. See “Making Concurrent Connections” on page 48.

To add a network adapter:

1. If necessary, install or insert the network adapter card in your computer. Most current laptop computers include a wired and a wireless network adapter.
2. Open the **Configuration** folder in the sidebar on the left and click **Adapters**.
3. Click **Add**. The Add Adapter dialog box appears.
4. Select the **Wireless** tab to add a wireless network adapter or the **Wired 802.1X** tab to add a wired network adapter. Note that only adapters that you have not yet added to the Adapters dialog box appear in the display.
5. 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 non-wireless 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.

Global Management Settings for Adapters

You can configure OAC so that it automatically configures all wired or wireless adapters, 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. Go to **Tools > Options > Interfaces**.
2. Select either or both of the following options:
 - Enable the **Manage all wireless (WiFi) adapters** check box to automatically manage all of your WiFi adapters.
 - Enable the **Manage all wired (Ethernet) adapters** check box to automatically manage your wired adapter.

Renaming an Adapter

When you add an adapter to the OAC configuration, the adapter appears in the sidebar in the **Adapters** folder. A wired adapter has the default name **Ethernet**. A wireless adapter has the default name **WiFi**. If you use multiple wireless adapters, you can rename them to distinguish one from another.

To rename an adapter:

1. Right-click the adapter icon in the sidebar.
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

There are two ways to remove an adapter.

Removing an Adapter Using the Adapter Dialog Box

To remove an adapter using the Adapter dialog box:

1. Open the **Configuration** folder in the sidebar on the left and click **Adapters**.
2. In the Adapter dialog box, click the wired or wireless adapter(s) that you want to remove.
3. Enable **Remove**.

Removing an Adapter Using the Sidebar Icon.

To remove an adapter using the sidebar icon:

1. Right-click the adapter icon in the sidebar.
2. Select **Remove**.
3. When dialog box prompts you for confirmation before removing the adapter, click **OK** to proceed.

When you remove an adapter, OAC stops using it. Even if the adapter is still installed, it does not operate with OAC unless you add it back to the configuration.

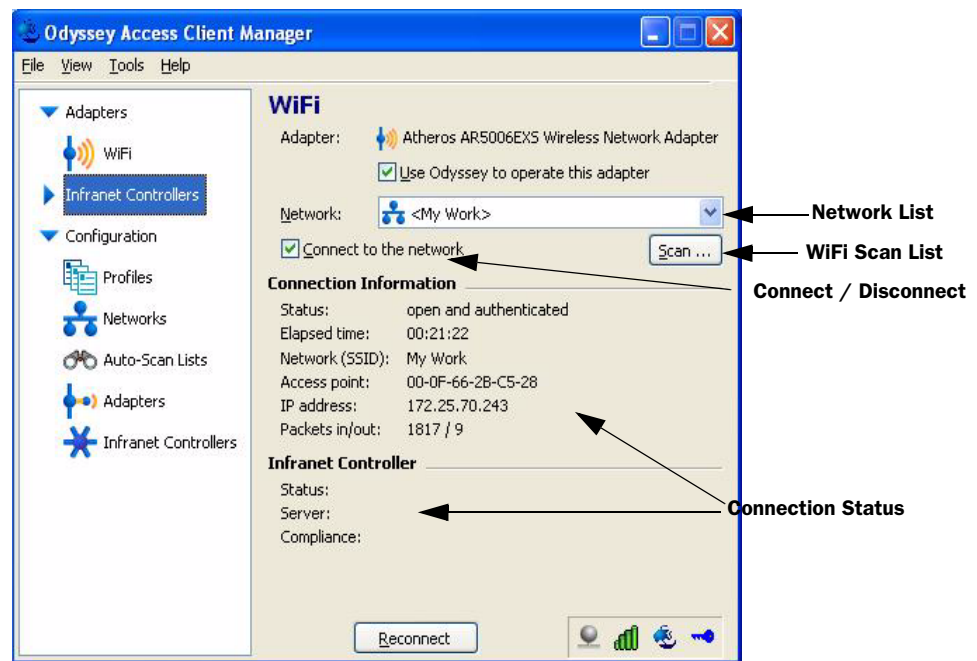


NOTE: When you remove an adapter from the OAC configuration, check the Windows Control Panel setting to ensure that the adapter is enabled for Windows again. Go to **Control Panel > Network Connections > adapter name > Properties > Wireless Networks** and enable the **Use Windows to configure my network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

Managing Adapter Connections to a Network

This section describes how to use OAC to connect to a specific network. The adapter dialog box name is either **WiFi** or **Ethernet** (Figure 9), depending on the type of adapter you use and allows you to perform the following tasks:

- Select a wired or wireless adapter from the list of configured adapters.
- Connect to a specific network.
- Disconnect from the network.
- Scan for available wireless networks.
- Reconnect to the network.

Figure 9: Adapter Dialog Box

NOTE: You or your network administrator can configure OAC so that it controls all of your network adapters. In this case, the **Use Odyssey to operate this adapter** check box is disabled (grayed out) in the connection dialog box. See “Interfaces Tab” on page 21.

Selecting an Adapter

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

To select a network adapter:

1. Open the **Adapters** folder in the sidebar.
2. Click the wired or wireless adapter to use.

Once you select an adapter, the **Adapter type** field on the Connection panel indicates the type of adapter (WiFi or Ethernet) you have selected.

Connecting to a Network

When you connect to a network, OAC uses the adapter that you want to establish an authenticated 802.1X connection to the network. If you attempt a wired connection to a network switch that does not support 802.1X—for example, to a wired network at home—OAC makes the connection without any authentication.

Before you can connect to a network with a wired or wireless adapter, you must configure at least one network and one authentication profile. See “Adding or Modifying Network Properties” on page 73 and “Adding or Modifying a Profile” on page 54.

Making a Wireless Network Connection

To connect to a wireless network:

1. From the **Adapters** list in the sidebar, select the wireless adapter to use. The WiFi dialog box opens and the **Adapter type** field indicates the type of adapter (**WiFi**) you have selected.
2. Select a network or auto-scan list from the **Network** list.

The networks in this list are the ones that are created already in the Networks dialog box. To add a new network, see “Adding or Modifying Network Properties” on page 73.

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

The dialog box shows the connection status and whether or not your connection to the network is successful. If there are connection errors, the OAC icon in the system tray changes colors and might display a pop-up message about the cause of the failure.

Making a Wired Network Connection

If your corporate network includes network switches that support 802.1X authentication, OAC supports such connections. You must have a suitable 802.1X network adapter for this connection type and it must be configured in OAC.

To connect to a wired 802.1X network:

1. From the **Adapters** list in the sidebar, select the wired adapter to use. The Ethernet dialog box opens and the **Adapter type** field indicates the type of adapter (**Ethernet**) you have selected.

1. Select an authentication profile from the **Profile** list.

The profiles that appear in this list are the ones that you have created in the Profiles dialog box. See “Adding or Modifying a Profile” on page 54.

2. Enable **Connect to the network** to start the network connection.

To connect to a different network:

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

Making Concurrent Connections

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

Your administrator might recommend that you enable wireless suppression, which defaults to a wired connection whenever you have one. The purpose of wireless suppression is to conserve wireless bandwidth for users who do not have access to a wired connection.

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

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 currently 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. Select the adapter from the **Adapters** folder 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.

Scanning for Wireless Networks

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

To connect to a wireless network that is not configured:

1. Enable **Scan** on the Connection dialog box.

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

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

See “Adding an Auto-Scan List” on page 84 and “Using Preemptive Networks” on page 85 for more information on scanning and creating scan lists.



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

Reconnecting to a Network

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

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

Checking Adapter Status

One way to check adapter status is to view the adapters in the **Adapters** folder. If an adapter is currently disconnected from the network, the adapter icon is gray.

You can check other adapter status, as described below.

To check adapter status:

1. Open the **Adapters** folder at the top of the sidebar.
2. Select the adapter whose status you want to check.

The adapter dialog box displays the following information:

- The adapter name (such as Intel PRO/Wireless 2200BG Network Connection).
- The adapter type (“Ethernet” or “WiFi”).
- A network name and, next to it, a pull-down list of the current configured networks. (See “Connecting to a Network” on page 46.)
- A **Connect to the network** check box for toggling a connection on or off.
 - If you are using a wired adapter, use the **Profiles** pull-down list to select an authentication profile.
 - If you are using a wireless adapter, use the **Network** pull-down list to select the network to which you want to connect.
- Connection status
- Endpoint status

Connection Status Information

Connection status (see Table 3) shows summary information about the current adapter and network connection, which includes:

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

Table 3: Connection Status Information

Status Message	Definition
open and authenticated	The connection is authenticated and you are connected.
open / authenticating	Reauthentication is in progress and you are connected.
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. See “Connecting to a Network” on page 46 for information about how to connect.
OAC is disabled	You are not connected and OAC has been disabled.

Table 3: Connection Status Information (continued)

Status Message	Definition
adapter not present	You are not connected and the configured adapter is not currently 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.
adapter in use by another program	Your adapter is being used by another program installed on your machine.
disabled by wired connection	Your wired connection has disabled your OAC wireless connection based on your security settings. See “Tools Menu Options Attack this section, slim it down, and relocate the details.” on page 18.

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 non-standard features of your wireless adapter to which OAC has no access.

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

Chapter 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 for authenticating a connection to a specific network. This includes information such as your identity (user credentials) and the EAP protocols used to authenticate to that network. You need a profile for each network to which you need authenticated access.

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 may be helpful.

The tasks for managing a profile include:

- Creating or modifying an authentication profile.
- Specifying user credentials.
- Specifying EAP authentication settings.
- Specifying 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.

To configure a profile:

1. Open the **Configuration** folder in the sidebar.
2. Click **Profiles** to open the Profiles dialog box.

The Profiles dialog box lists the currently configured profiles. The list might include a default profile, called **Initial Profile**, containing preconfigured settings. You can use this as a guideline for setting up other profiles.

Adding or Modifying a Profile

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

- To add a profile, click **Add**.
- To modify profile properties, click **Properties**.

Both dialog boxes display the same settings. Use either one.

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

- Profile name—The name of the profile that you are creating or editing.
- User information—Your logon 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 “SIM Card Manager Use Case for this Option” on page 18.
- TTLS—The EAP-TTLS outer protocols and, where they apply, one or more inner protocols. See “TTLS Settings” on page 63.
- PEAP—The EAP-PEAP outer protocols and, where they apply, one or more inner protocols. See “PEAP Settings” on page 66 and “Using Certificates with EAP-PEAP Authentication” on page 67.
- 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, refer to the following sections:
 - “Setting JUAC as an Inner Authentication Protocol for TTLS” on page 69.
 - “Setting JUAC as an Inner Authentication Protocol for PEAP” on page 70.
 - “Setting a Preferred Realm and Role” on page 70.

Specifying Profile Names

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

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

Specifying User Info

From the **User Info** tab, configure the logon name and your password, certificate, soft token, or SIM card based on the logon credentials that you need to use. See “Using SIM Cards” on page 59 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 user name in the **Login name** field. This is the name presented to the network when you request a network connection. If you authenticate against a Windows Active Directory, use the form *domain\user_name* (for example, **Acme\george**). See your network administrator for the required format.

The **User Info** tab has sections you can configure:

- **Password**—Configure this section when you use authentication protocols that require or permit a password (such as EAP-TTLS). You can specify how the password should be retrieved (“Setting Passwords” on page 55).
- **Using Certificates**—Configure this section 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 57).
- **Soft Token**—Configure this section if you are required to use a soft token as part of authenticating to the network when you log in.
 - **SIM Card**—Configure this section when you use a mobile wireless device to authenticate to a network Soft Token: You must configure this section when you require soft token authentication for one of the token-based authentication methods.

Setting Passwords

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 MSCHAP
- EAP-TTLS with an inner protocol of MSCHAPV2
- EAP-TTLS with an inner EAP protocol of MD5-Challenge
- EAP-PEAP with an inner protocol of MSCHAPV2

- EAP-MD5-Challenge
- EAP-LEAP

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

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

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

- Enable **Use Windows password** if you want to authenticate to the network using the same password that you present when you log in to Windows.



NOTE: Do not enable 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.

- Enable **Prompt for password** to have OAC prompt you when you connect to the network. In general, this is the most secure option.
- Enable **Prompt for login name and password** to have OAC prompt you when you connect to the network.



NOTE: This is the least secure option because the password prompt occurs *before* the pre-authentication health check on a UAC network and, thus, does not provide a security guarantee.

- Enable **Use the following password** and enter a password in the box below this option to have OAC save your password and use it each time you authenticate with this profile.



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

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

You might have to enter 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 due to the reuse of bad passwords.
- You need to change your Windows password periodically and are accessing the network with EAP-TTLS, EAP-PEAP, or EAP-FAST authentication before Windows logon.



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

Using Certificates

A *certificate* is cryptographic data which guarantees that 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 113 for more information.

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

- The personal certificate store on your computer or device.
- Your smart card reader, if you have one installed. See “Security Tab” on page 20 for more information about using smart cards and caching PIN information.

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

If you enable EAP-PEAP, use EAP-TLS as the inner authentication protocol. See “PEAP Settings” on page 66 for configuring inner EAP-PEAP protocols.

If you enable EAP-TTLS, choose one of the two certificate-based options on the **TTLS Settings** tab.

Using Certificates for Authentication

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

TLS, TTLS, and PEAP all support mutual authentication between the authentication sever and the client machine. *Mutual authentication* means that while the server authenticates you as a valid user, you can validate the server’s certificate, (To authenticate the server, use the Validate server certificate option on the **Authentication** tab of the Profile Properties dialog box.) See “Certificates” on page 113 for more information on certificates.

To use certificate credentials for authentication:

1. Open the **Certificate** subtab of the **User Info** tab:.
2. Enable **Permit login using my certificate** to enable authentication methods that use your certificate for authentication. Select one of the following options:
 - a. Enable **Use automatic certificate selection** to let 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.
 - ❑ When 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. You can allow OAC to automatically select your certificate from a smart card reader or from your personal certificate store.
 - b. Enable **Use the following certificate** then click **Browse** to select a personal certificate from your computer. A list of your personal certificates appears. Select a certificate and click **OK**. Once you configure a certificate, you can click **View** to view the certificate.



NOTE: Before you can create a profile that uses a personal certificate from your computer (as opposed to a smart card certificate), you must install the certificate in the `current_user` store of your computer. See your network administrator for information about installing and selecting a user certificate for authentication if you require one.

- c. If you have a smart card installed on your client machine, you can use the certificate from your smart card. For this option, enable **Use the logon certificate from my smart card reader**. With this option, you can 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. (See “Security Tab” on page 20 and read the section about **Prompt for smart card PIN** for the FIPS constraints.)

Using Soft Tokens

With certain token-based authentication options, you can use a software-based token rather than a token from a physical token card. See “Setting Up Authentication” on page 60. To use software-based token information, enable this soft token feature and select the token from the **Soft Token** subtab of the **User Info** tab.

To enable soft token authentication:

1. To create a profile that uses only soft token authentication methods (recommended for soft token authentication configuration), clear the **Permit login using password** setting on the **Password** subtab of the **User Info** tab in the Profile Properties dialog box.
2. Enable **Permit login using my RSA Soft Token** on the **Soft Token** subtab of the **User Info** tab.
3. Choose one of the following options:
 - Enable **Use any token** if you have only one token installed in your client machine.
 - Enable **Use the following token** and click **Browse** to choose a specific token that is installed in your client machine when you have more than one token installed. 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.
4. Configure one of the soft token-based authentication options listed at the beginning of this section.
5. Click **OK** to save the profile.

Using SIM Cards

You can configure SIM card authentication from the **SIM Card** subtab of the **User Info** tab of the Profile Properties dialog.

To use a SIM card when you connect to a network through OAC, 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 IMSI (International Mobile Subscriber Identity)— 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 60.

To use OAC with your SIM card, enable **Permit login using my SIM card**. You can configure three more items under the **SIM Card** subtab of the **User Info** tab.

Setting a SIM Card ID

You can 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, you can select your SIM card ID from the **SIM card ID** list.

Managing PIN Settings

You might have already set a PIN on your SIM card hardware. You have two choices for the **PIN field** for OAC:

- Enable **PIN is not required** (default) if you are not required to use the PIN for your connections (you have no PIN assigned to your SIM card).
- Enable **Prompt for PIN** if you enable a PIN for your use 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]** under **SIM card ID** (as opposed to a specific SIM card ID).
- Enable **Use the following PIN** to use the PIN that you have enabled for use with your specified SIM card ID. In this case, type 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.

The choices for entering your SIM identity are:

- Enable **Use the IMSI from my SIM card** (default) if your provider requires you to use your IMSI for identification.
- Enable **Use the login name I entered in this profile** if you are required to use an identity (usually of the form *username@realm*) rather than your IMSI. In this case, make sure that your login name is in the form that is required by your provider. Note that when you enable 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 enable this option, create a separate configuration for connections that use protocols other than EAP-SIM or EAP-AKA.

Setting Up Authentication

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 authenticated to access your network. In many cases, authentication settings might be preconfigured and possibly restricted by your network administrator.

Open the **Authentication** tab in the Profile Properties dialog box.

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



NOTE: EAP-TTLS, EAP-PEAP, and EAP-FAST all use inner (tunneled) protocols. EAP-FAST uses EAP-GenericTokenCard as its inner protocol. You can choose one or more inner protocols for EAP-TTLS or EAP-PEAP. See “TTLS Settings” on page 63 and “Using Certificates with EAP-TTLS Authentication” on page 65.

Selecting Authentication Protocols

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



NOTE: If FIPS mode is enabled, there is only one outer authentication protocol supported, EAP-TLS, and no inner authentication protocols. **(FE Only)**

To add a protocol to the list:

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

To enable more than one protocol at a time, hold down the Ctrl key as you select them with your mouse. Any protocols already selected are not listed in this dialog.

To remove a protocol from the list:

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

To reorder protocols:

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

Validating a Server Certificate—Mutual Authentication

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

Enable **Validate server certificate** (set by default) to verify the identity of the authentication server based on its certificate when authenticating with EAP-TTLS, PEAP, and EAP-TLS.



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

To check this on Windows systems, select Internet Explorer under **Tools > Internet Options > Content > Certificates**. Consult your network administrator for help with this.

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

Do this only if your network administrator directs you to do so.

Setting Token Card Credential Options

EAP-GenericTokenCard 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. There are circumstances where EAP-GenericTokenCard can be the inner protocol for tunneled authentication are:

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

- Enable **Use my password** if your network requires that you use the password credentials assigned with this profile instead of your token card ID for authentication.
- Enable **Prompt for token information** if 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 from the Setting Up Authentication tab.

Setting an Anonymous Name

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

You can have two identities when you use any of the following protocols:

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

Note the following:

- Anonymous outer identities are implemented only if you enter a name in **Anonymous name**.
- When you leave **Anonymous name** 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 field 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** blank.



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

TTLS Settings

Use the **TTLS Settings** tab to configure EAP-TTLS as an authentication protocol. These settings are relevant only if you enable EAP-TTLS as an authentication protocol in the **Authentication** tab.

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 114 for more information about this protocol.

Selecting an Inner Authentication Protocol

TTLS and PEAP support inner authentication tunnels. Inner authentication provides an additional level of security by transferring password credentials through an encrypted tunnel between the client and the authentication server. Table 4 on page 64 lists the compatible inner and outer authentication protocols for TTLS and PEAP.

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

Table 4: Outer EAP Protocols and Supported Inner Protocols

Compatible Inner Authentication Methods	EAP-TTLS for Outer Authentication	EAP-PEAP for Outer Authentication
PAP	Yes	No
CHAP	Yes	No
MS-CHAP (Note: not valid for Windows platforms)	Yes	No
MS-CHAP-V2	Yes	Yes
PAP/Token Card	Yes	No
EAP	Yes	No
GenericTokenCard	No	Yes
POTP	No	Yes
TLS	No	Yes
JUAC	Yes	Yes



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

To enable an inner authentication protocol:

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

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

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

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.

EAP Inner Authentication Protocols

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

To add an inner EAP protocol:

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

See Table 4 on page 64 for a list of outer EAP protocols and the corresponding inner protocols.

To remove a protocol:

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

To reorder protocols:

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

Using Certificates with EAP-TTLS Authentication

To enable EAP-TTLS personal certificate options:

1. Enable **Permit login using my certificate** on the **Certificate** subtab of the **User Info** tab.
2. In the **TTLS** tab of the Profile Properties dialog, select one of the following personal certificate options:

- **Use only my certificate for authentication**—Configure EAP-TTLS certificate-based authentication without a password. If you enable this option and you do not enable any password-based authentication methods for this profile, you can clear the **Permit login using password** setting on the **Setting Passwords** subtab of the **Specifying User Info** tab. See “Setting Passwords” on page 55 for a list of password-based authentication methods.
- **Use my certificate and perform inner authentication**—Configure EAP-TTLS certificate-based authentication and tunnel password credentials for use with an inner authentication protocol.
- **None**—Configure EAP-TTLS authentication without a client-side certificate. This option specifies the most typical use of EAP-TTLS authentication. Enable this option unless you intend to use a client certificate as part of EAP-TTLS authentication.

3. Click **OK**.

PEAP Settings

If you use EAP-PEAP as an authentication method in the **Authentication** tab, Table 4 on page 64 shows the valid inner EAP authentication methods for PEAP.

You can add, remove, or reorder any EAP-PEAP inner protocols from the **PEAP Settings** tab of the Profile Properties dialog. See “Outer EAP Protocols and Supported Inner Protocols” on page 64.

To add an inner PEAP protocol:

1. From the **PEAP** tab in the Profile Properties dialog, select EAP from the pull-down list of inner authentication protocols.
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**.

To add other inner EAP protocol to the list, repeat this procedure.

To remove a protocol:

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

To reorder protocols:

1. Select a protocol to move.
2. Use the up and down arrow buttons on the **TTLS Settings** tab of the Profile Properties dialog box to reposition the protocol on the list. If you select EAP-GenericTokenCard as one of your PEAP inner authentication methods, you can configure the EAP-GenericTokenCard settings under the Setting Up Authentication tab. These settings allow you to choose to use your password credentials or your token card ID for authentication.
3. Click **OK** to update the profile configuration.



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

Using Certificates with EAP-PEAP Authentication

To enable EAP-PEAP personal certificate options:

1. Enable **Permit login using my certificate** on the **Certificate** subtab of the **User Info** tab on the Profile dialog.
2. In the **PEAP** tab of the Profile Properties dialog, enable **Use my certificate to authenticate to the network**.
3. Enable 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.
4. Click **OK**.

EAP-POTP Run-Time Options

EAP-POTP (Protected One-Time Password) is an authentication method used with One-Time Password (OTP) tokens and is well suited for use with USB token readers. 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.)

Configuring EAP-POTP as an Inner Authentication Method



NOTE: EAP-POP is not currently a supported protocol on Infranet Controllers.

To configure EAP-POTP as an inner authentication method:

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

OAC then 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 on your hardware token card.

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

- Enable **System-generated PIN** to use the PIN provided. Memorize this PIN for future use.
- Enable **User-defined PIN** to define your own PIN and follow this procedure:
 - a. Follow the instructions located after the text field to enter a new PIN under **Please enter your PIN**.
 - b. Optionally, you can enable **Unmask** to see your PIN as you type it.
 - c. Re-type the PIN under **Please confirm your PIN**.
 - d. Click **OK**.

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

Configuring Authentication for Infranet Controllers

Connecting to an Infranet Controller requires an authentication profile. Best practices recommend that you have an authentication 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 Juniper UAC network.

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

- Profile name
- User name
- 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 69)
- Realm name and role (optional). For more information about realms and roles, see “Setting a Preferred Realm and Role” on page 70.

JUAC is an inner EAP protocol developed by Juniper Networks for authenticating access to an Infranet Controller. JUAC is compatible with TTLS and PEAP. This section describes how to set up JUAC as an inner authentication protocol for TTLS and for PEAP.

Setting JUAC as an Inner Authentication Protocol for TTLS

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

To add JUAC as an inner authentication protocol for TTLS:

1. Open the Profile Properties dialog.
2. Open the **TTLS** tab.
3. From the pull-down list of **Inner EAP protocols, in order of preference**, select **EAP**.
4. Click the **Add** button to display the Add EAP Protocol dialog box and enable **JUAC** and any other inner EAP protocols to add by highlighting one or more of them.
5. Click **OK**.

To set a preferred order of inner EAP protocols:

1. Select one of the inner EAP 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 **TTLS Settings** tab of the Profile Properties dialog.

To remove JUAC as an inner authentication protocol for TTLS:

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

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

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.

PEAP supports the inner authentication protocols shown in Table 4 on page 64. If you have PEAP as an outer authentication protocol, JUAC is configured automatically as an inner EAP protocol.

To set a preferred order of inner EAP protocols:

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

1. Select one of the inner EAP 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 Settings** tab of the Profile Properties dialog.

To remove JUAC as an inner authentication protocol for PEAP:

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

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. Part of connecting to an Infranet Controller might include specifying a realm and a 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 are available to you.

Your role maps to your job title, department or group, and the privileges that you have to access specific resources for members of 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.

If you leave these fields blank, the Infranet Controller might prompt you for a realm and a role when you try to connect.

To set a preferred realm and role:

1. Open the **JUAC** tab in the Profile Properties dialog.

2. In the **Realm** field, specify the name of your preferred realm. If you do not know the realms defined for you, see your network administrator.
3. In the **Role** field, specify 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 means that you do not have to re-specify those values each time you connect to the same Infranet Controller.

Authenticating with Token Cards

If you use one or more token card authentication methods and then Enable **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*, 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 for a valid PIN, enter the PIN followed by the current sequence of digits displayed on your hardware token card.

Under some circumstances, you might be required to provide a new PIN.

To enter a new PIN:

1. Enter a new 4–8 digit PIN and click **OK**.
 Enable **Unmask** to see your PIN in clear text before you click **OK**.
2. Re-enter a new 4–8 digit PIN and click **OK**.

Removing a Profile

To remove an authentication profile, select the profile name in the list and click **Remove**.

Sample Profile Configuration

This section shows a sample authentication profile for a corporate network. (You do not a profile for a hotspot or a home WiFi network.)

Table 5: Sample Profile for a Corporate Network

Setting	Value
Profile name	ACME_NYC
Login name	this user
Permit using password	Yes
Use Windows password	Yes
Authentication	EAP-TTLS

Table 5: Sample Profile for a Corporate Network

Setting	Value
Validate server certificate	Yes
Token card credentials	Use my password
TTLS inner authentication	EAP-JUAC &EAP-MS-CHAP-V@ (See Table 4 on page 64.)

Chapter 7

Configuring Networks

This chapter describes how to configure the networks to which you connect. Before connecting to any network with OAC, you must configure that network and name it. Your networks can include one or more corporate wired and wireless networks, your home wireless network, and one or more public hotspot networks. Each network is unique and requires a unique name and accurate configuration settings.

Configuring Network Settings

To configure the settings for connecting to a network:

1. Open the **Configuration** folder from the sidebar.
2. Select **Networks**. The Networks dialog box opens.

Each configured network appears in the Networks dialog box.



NOTE: If OAC has been preconfigured by your administrator, the corporate networks you need may be configured already. Open an adapter connection dialog box and check the **Networks** list next to **Connect to the Network**.

Adding or Modifying Network Properties

Whether you add a network by selecting **Add** or modify network properties by selecting **Properties**, the dialog boxes display the same settings.

The dialog box has three configuration categories:

- **Network**—Use these settings to provide a name for the network that you are configuring, to configure the method used to connect to the network, and to specify the encryption method to use.



NOTE: (FE Only) If you use the OAC FIPS edition, the Add Network and the Network Properties dialog boxes show a **FIPS mode required** check box next to the **Encryption method** field. If you require FIPS encryption each time that you connect to this network, select **FIPS mode required**. If not, leave the box cleared. Contact your administrator before altering this setting.

- **Authentication**—Use these settings to specify whether you will use an authentication profile or WEP keys to authenticate.
- **Pre-configured keys (WEP)**—Use these settings to specify the WEP keys.

Each network that you configure in OAC requires some or all of the network settings from the categories listed below. The settings required depend on whether the network that you are configuring uses authentication and encryption.

Network Settings

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

Specifying a Network Name (Network SSID)

The *network name* is also known as the SSID (Service Set Identifier). It is the unique name of the wireless network to which you want to connect and that information is usually 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 format of network names that are currently configured appears in the Network Properties dialog box. A network name can be up to 32 alphanumeric characters and it is case sensitive. You must enter the name correctly to connect.

If the network is locally accessible, you might be able to view the name using the **Scan** button in the Network Properties dialog box. However, not all access points broadcast a network SSID. Contact your administrator to be sure of the correct network name and format.

Connecting to Any Available Network

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

To do this, select **Connect to any available network**.



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

Scanning for Available Networks

Instead of entering the name of a configured network in the **Network name** field, you can select **Scan** to select from a list of all the wireless networks that OAC can detect—those that are within range and that broadcast an SSID. If you are in the vicinity of the network that you are configuring, selecting **Scan** is easier than manually entering the network name and guarantees that the name is set correctly. Select the network from the scan list.

Adding a Network Description

Network names are arbitrary text chosen by an administrator, so two unrelated networks could have the same name. Use the **Description** field to add text to distinguish between networks that have similar names.

Use the network description field to distinguish connections to the same network with different profiles. For example, you might want to use different credentials at different times. The **Description** field is optional.

Specifying a Network Type

If you do not select **Scan** to select a network, specify the type of network by choosing one of the options from the **Network type** drop-down list.

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

Specifying a Channel

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

Specifying an Association Mode

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

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

In an airport or train station, select **[any]** as the network. The network prompts for credit card payment information to use to connect to the network. Finally, a Web page displays the configuration information for that network, such as the association mode and encryption method, if any.

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 WiFi 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 (FE Only)**— Use this for a Layer 2 secure encryption protocol. 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. You must associate xSec networks with a profile that uses EAP-TTLS, EAP-PEAP, or EAP-TLS.

Encryption Methods for an Association Mode

Your choice of encryption method depends on the access point requirements. The choices available to you depend on the association mode you choose. See “Wired-Equivalent Privacy” on page 109 and “WiFi Protected Access and its Encryption Methods” on page 110 for more information.

The encryption options that you can configure depend on the association mode you use. Each association mode supports specific encryption types. The options are:

- **None**—Use this setting to select 802.1X authentication without WEP keys. This option is available to you only when you configure access point association in open mode. This is a typical setting to use for wireless hotspots.
- **WEP**—Use this setting to use WEP keys for data encryption. This is an option for open mode association and is required when you associate in shared mode. When you use WEP encryption, 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**. You must choose WEP encryption when the access points in your network require shared mode association with WEP keys or when your access points require WEP encryption.
- **TKIP**—Use this setting to use the temporal key integrity protocol. Choose this option when the access points in your network require WPA or WPA2 association and are configured for TKIP data encryption.
- **AES**—Use this setting to use the advanced encryption standard protocol. Choose this option when the access points in your network require WPA or WPA2 association and are configured for AES data encryption. If your client hardware and access point support AES, use AES encryption when you associate in WPA2 or WPA mode. You must use this method for encryption when associating to hardware that supports xSec.

FIPS Association Mode (FE Only)

All FIPS network configurations require that you use TLS for EAP authentication.

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.

FIPS Secure Encryption (FE 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, leave the box cleared.

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



NOTE: This is an advanced feature. See your network administrator if you have questions about using FIPS encryption. If you are an administrator and if you require FIPS-compliant network connections for your users, you can configure and lock this type of connection using the Odyssey Access Client Administrator tools.

Configuring Networks that Do Not Broadcast an SSID

When OAC scans for available WiFi networks, it detects and lists the networks within range that are broadcasting an SSID. A WiFi network that does not broadcast an SSID can appear in the list of scanned networks but you cannot connect to it without the SSID, so you must configure that network to access it.

Configuring a non-broadcast network lets you include it in an auto-scan list and makes sure that OAC will try to connect to it in the order listed in the auto-scan list. See “Adding an Auto-Scan List” on page 84.

You must have the correct configuration information for this network in advance (the SSID, association mode, encryption method, and any encryption key information necessary). To configure a network that does not broadcast an SSID, do the following:

1. Open the Networks dialog box and click **Add**.
2. In the Network Properties dialog box, specify the network name (SSID) of the “non-broadcast” network in the **Network name** field.
3. Configure the appropriate association mode and encryption mode settings, including the encryption key settings needed. (You must know this information in advance.)
4. Enable the **Non-broadcast** check box. With this setting enabled, OAC remembers the network during subsequent scans for available WiFi networks. In this case, OAC “polls” for the specific, non-broadcast network rather than trying to detect an SSID.
5. If the network requires authenticated access, specify the authentication profile to be used.



NOTE: Networks that do not broadcast an SSID can never cause OAC to switch to that network as a preferred network when you are already connected to a lower priority network, even if the current network is also marked as non-broadcast network. This feature may be disabled by your administrator, in which case OAC will not detect non-broadcast networks and will not scan for them

See “Specifying a Network Name (Network SSID)” on page 74.

Specifying an Authentication Profile

To establish an authenticated 802.1X wireless connection to a network, you must specify a valid authentication profile. To authenticate using your personal credentials:

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

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

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



NOTE: If the profile you select for this network specifies MD-5 Challenge or EAP-GenericTokenCard as an outer authentication method, you must use a preconfigured WEP key for data encryption to authenticate using 802.1X. See “Preconfigured Keys (WEP)” on page 79.

Automatic Key Generation

This option also applies to an authenticated 802.1X wireless connection. If the authentication method specified in the selected profile results in the creation of dynamic WEP keys for use between your PC and the access point, 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.

If you associate this network with a profile that uses EAP-TTLS, EAP-PEAP, EAP-FAST, EAP-POTP, or EAP-TLS as an authentication protocol, select this box. You can use any of these authentication methods if your access point implements 802.1X authentication.

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

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

Preconfigured Key Settings

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

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

Preshared Keys (WPA or WPA2)

If you associate using WPA or WPA2 and if you do not generate encryption keys automatically when associating an authentication profile to the network connection, you must specify a preshared 8–63 character ASCII passphrase in the **Passphrase** field. 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 from 8 to 63 ASCII characters or 64 hexadecimal digits (256 bits). Passphrases and static WEP keys apply if you are not connecting to a network that uses 802.1X authentication, such as home networks, hotspots, and small offices.



NOTE: If you supply a 64-character passphrase that could form a hexadecimal number, Odyssey interprets it as a 32-byte hexadecimal value used as the master key. See your administrator for more information about this.

Preconfigured Keys (WEP)

WEP keys serve the following purposes:

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

See “Wired-Equivalent Privacy” on page 109.

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

- You associate in shared mode. See “Specifying an Association Mode” on page 75.
- You select WEP encryption for the open association mode and you do not generate encryption keys automatically. See “Encryption Methods for an Association Mode” on page 76.

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**), you do not need to enter preconfigured WEP keys for data privacy. However, it is possible to use preconfigured WEP keys for authentication in addition to 802.1X. For example, EAP-MD5 does not generate WEP keys for data encryption, so you must supply an encryption WEP key when your profile is set to authenticate with this method.

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

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

Table 6: WEP Key Specifications

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

To enter any preconfigured WEP keys:

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

Removing a Network

To remove a network:

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

Sample Network Configuration Setups

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

Sample Configuration for a Corporate WiFi Network

Table 7: Sample Configuration for a Corporate WiFi Network

Setting	Value
Network name (SSID)	ACME_NYC_WiFi
Connect to any available network	No (setting is optional as long as your corporate network has been configured in OAC)
Description	Corporate office wireless network
Network Type	Access point (infrastructure mode)
Association mode	WPA2
Encryption mode	AES
Authenticate using profile	ACME_NYC
Keys will be generated automatically for data privacy	Yes

Sample Configuration for a Wireless Hotspot Network

Table 8: Sample Configuration for a Hotspot Network

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

Sample Configuration for a Home Wireless Network



Table 9: Sample Configuration for a Home Wireless Network

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

Chapter 8

Managing Auto-Scan Lists

An *auto-scan list* is a prioritized list of configured networks. Any auto-scan lists appear at the top of the network list displayed next to the **Connect to the network** check box the WiFi dialog box. Network names appear in angle brackets. Networks and auto-scan lists are distinguished by these icons:

-  = networks
-  = auto-scan lists

If you use an auto-scan list, you do not have to specify a new network connection each time that 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 want. When you use an auto-scan list, OAC attempts to connect to the *first* network SSID starting at the top of the list and then tries the next one the list until there is a connection.

OAC remembers the last connection so that if you disconnect and reconnect, OAC selects 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. An auto-scan list can contain as many networks as you like. When OAC uses an auto-scan list, it attempts to connect to the *first* network in the list, then the next one, and so on.

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. Refer to the **Tools > Options > Preemptive Networks** option to help control the list of wireless networks to which you connect. Refer also to “Using Preemptive Networks” on page 85.



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

Adding an Auto-Scan List

To add an auto-scan list:

1. Open the **Configuration** folder and select **Auto-Scan Lists**.
2. Click **Add** in the Auto-Scan Lists dialog box. The Add Auto-Scan List dialog box appears.
3. Enter a name for the auto-scan list in the **Auto-Scan list name** field. You must fill in this field in before you click **OK**. You cannot use the same name as another current auto-scan list.
4. Select networks to add to the auto-scan list from the list of configured networks listed under **Available Networks** on the left. Use the right arrows to move networks from the left to the **Networks in list, in priority order** on the right.
5. Order the selected networks based on the frequency with which you expect to connect to them. Place the highest priority networks at the top of the list. A network on this list is considered to be *preferred* over the networks listed below it. You can select one or more networks and use the up and down arrows to reorder the list.

Optionally, you can 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 the uppermost available network on this list any time that you connect to this auto-scan list from the WiFi dialog box. If the preferred network is available, OAC connects to that network even if you are connected to a different network on this list at the time.

- Preemptive network setting influences which networks are scanned first.
- Preferred network setting influences when that scan takes places.

An access point must broadcast an SSID to connect to it with this option.

6. Select **OK** when you complete the set up for the auto-scan list

The next section talks about creating an auto-scan list that overrides any network connection you configure on the WiFi dialog box. This link provides information on how this option is treated if you or your administrator configure a preemptive auto-scan list.

Using Preemptive Networks

Use this option to specify an auto-scan list that always overrides the current network or auto-scan list connection. With preemptive networks, OAC scans the networks in the auto-scan list before connecting to a different network or auto-scan list you have selected in the WiFi connection dialog box. This option lets you ensure that you always connect to a preferred network if it is available.



NOTE: OAC scans for the networks in a preemptive auto-scan list *before* connecting to a any other network. If you configure an auto-scan list to preempt other network connections and if none of those networks are available, OAC tries to connect to the network you select on the WiFi connection dialog box.

To use preemptive networks:

1. Create an auto-scan list with your networks in order of preference (top-down).
2. In the **Tools > Options > Preemptive Networks** tab, enable **Use preemptive auto-scan list**.
3. Select the auto-scan list to use from the **Preemptive auto-scan** list in the **Preemptive Networks** tab.
4. Select one or both of the following options:
 - Select **Preempt any selected network** to connect to this auto-scan list rather than to any individual networks that you specify for connection on the Configuration panel of the Odyssey Client Manager.
 - Select **Preempt any selected auto-scan list** to connect to this auto-scan list rather than to any individual auto-scan lists that you specify for connection on the Configuration panel of the Odyssey Client Manager. You must enable at least one of these options.

The **Switch to preferred network when available, even if currently connected** check box in Add Auto-Scan List menu scans continuously for a preferred network and connects to the highest priority network available in this list.

The preemptive network setting affects which networks are scanned first. The preferred network setting affects when that scan takes places.

Modifying an Auto-Scan List

To modify an auto-scan list:

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

Viewing the Networks in an Auto-Scan List

To view the networks in an auto-scan list, double-click the name of the auto-scan list in the Auto-Scan List dialog box. The Auto-Scan List Properties dialog box displays the networks in the auto-scan list.



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

Removing an Auto-Scan List

To remove an auto-scan list:

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

Chapter 9

Managing Infranet Controller Connections

An Infranet Controller is a central policy management server that validates user identity and endpoint security compliance and enforces network security policies.

This chapter describes how to:

- Add an Infranet Controller to your OAC configuration.
- View the status of an Infranet Controller session.
- Recognize security compliance errors and remediation instructions.

If your network does not include an Infranet Controller, ignore this chapter.

After installing and running OAC, you can establish an authenticated connection to one or more Infranet Controllers. 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. Best practices recommend that you have an authentication profile for each Infranet Controller that you use to access protected network resources. See “Configuring Authentication for Infranet Controllers” on page 68.

The Infranet Controller configuration settings, including those for profiles and networks, might have been created by your administrator. For more information about Infranet Controllers and default settings, refer to the *Unified Access Control Administration Guide*.



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.

Adding an Infranet Controller to the OAC Configuration

Your initial OAC configuration typically includes at least one Infranet Controller. If your configuration permits you to configure additional Infranet Controllers, use the following procedure:

1. Select **Infranet Controllers** in the **Configuration** folder located in the sidebar.
2. In the Infranet Controllers dialog box, select **Add** to set up the configuration for that Infranet Controller.
3. In the **Infranet Controller name** field, assign a name for the Infranet Controller you are adding. Depending on how OAC has been installed on your computer, this information might be configured already.
4. In the **Server URL** field, enter the DNS name or the IP address of the Infranet Controller to which you intend to connect.
5. In the **Authentication Profile** field, specify the name of a profile for authenticating to a specific Infranet Controller. The profile provides all the information needed for authenticated access to that Infranet Controller. See “Adding or Modifying a Profile” on page 54 for details about setting up a profile.

FIPS Mode Constraint

The only outer authentication method supported for FIPS mode is EAP-TLS; no inner authentication method is supported, including JUAC. This means that, when FIPS mode is on, users cannot connect to an Infranet Controller.

Signing on to an Infranet Controller

To sign on to an Infranet Controller:

1. Open the **Infranet Controllers** list in the sidebar.
2. Select the Infranet Controller to which you want to connect.
3. An Infranet Controller dialog box opens (see Figure 6 on page 27) and shows the IP address of the Infranet Controller in the Server URL field. Below that is a **Connect to the Infranet Controller** check box.
4. Enable the check box to connect to the Infranet Controller.

Sign on to the Infranet Controller when the prompt appears. The first time you connect to an Infranet Controller you must provide authentication credentials. After you have been authenticated, you can complete the sign-on process and access the protected network resources to which you have been granted access.

Viewing Infranet Controller Status

One way to check Infranet Controller status is to view the Infranet Controllers in the **Infranet Controllers** folder. If an Infranet Controller is currently disconnected from the network, the Infranet Controller icon is gray and the **Connect to the Infranet Controller box** is not enabled. The **Reconnect** button is also gray in this case.

To check status of an Infranet Controller, open the Infranet Controller dialog box. The dialog box displays the following information:

- The server name or address.
- A connection check box.
- Connection information.
- A **Reconnect** button, which is used to reinitialize an existing connection.
- Endpoint status (see “Compliance Failure and Remediation”).

Infranet Controller Connection Types (L2 versus L3)

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 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.

There are two different places in the Odyssey Access Client Manager that can show Infranet Controller session status. One is the adapter (wired or wireless) adapter connection dialog box.

Layer 2 and Layer 3 Infranet Controller Status Information

A WiFi or Ethernet adapter connection dialog box shows two categories of status information: **Connection Information** and **Infranet Controller**. The information under **Connection Information** is network adapter connection status. It shows information about the type and duration of the network adapter connection.

The information displayed in **Infranet Controller** dialog box shows Layer 2 network connection session information for the Infranet Controller that authenticated the network connection. Both categories of information in this dialog box show Layer 2 connection status.

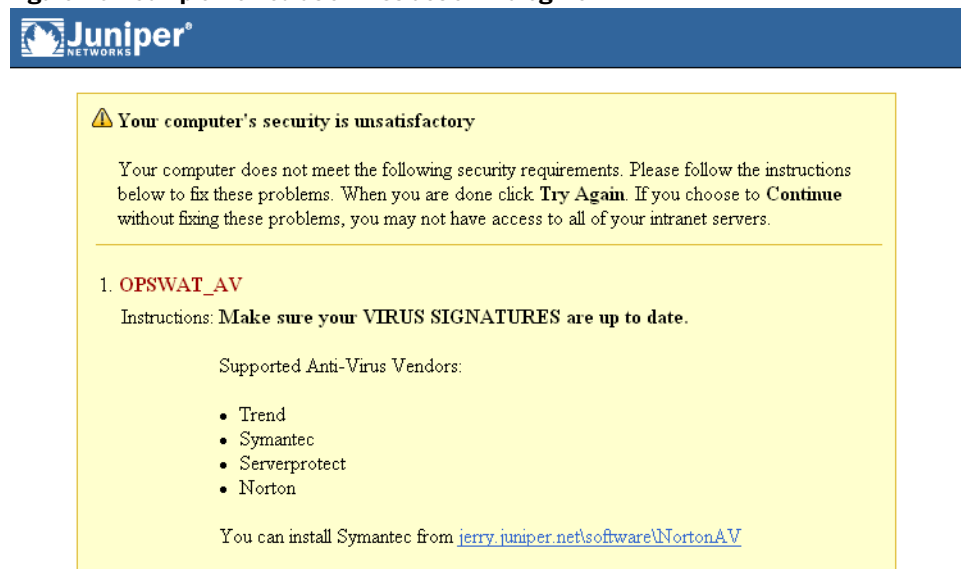
Status information displayed in an Infranet Controller dialog box shows session information for a Layer 3 connection to one Infranet Controller. If you have more than one Infranet Controller configured, you can connect to each one separately and view session information for each Infranet Controller connection.

Compliance Failure and Remediation

If your computer does not comply with the network security policy, the connection might be rejected or you might need to update the endpoint software, such as the anti-virus settings or operating system patch level. This is called *remediation*. In some cases, remediation is automatic. In other cases, the connection dialog box displays a message with instructions for what to do (Figure 7 on page 28).

When you select the **How do I resolve this problem?** link, another dialog box provides you with specific instructions for updating your computer so that it meets compliance requirements. The remediation instructions that you see might vary from the sample shown in Figure 8 on page 29. Your network administrator determines the detail level of information or instruction that you see.

Figure 10: Sample Remediation Instruction Dialog Box



Disconnecting from an Infranet Controller

To disconnect from an Infranet Controller:

1. Open the **Infranet Controllers** folder in the sidebar.
2. Select the Infranet Controller from which you intend to disconnect.
3. After a dialog box opens showing the Infranet Controller name, clear the **Connect to the Infranet Controller** check box.

Chapter 10

Managing Trusted Servers

This chapter describes trusted servers and the configuration tasks that pertain to managing trust, trusted servers, certificates, and certificate authorities. Use this feature to add, remove, and configure trusted network servers and to configure certificate and identity information for the servers that might authenticate you when you connect. Configuring this feature is required for protocols that implement mutual authentication and is a recommended security measure. See “Validating a Server Certificate—Mutual Authentication” on page 61. Refer also to “Certificates” on page 113 and “Mutual Authentication” on page 112 for background 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.

You can configure trust for authentication servers if you use EAP-TTLS, EAP-TLS, or EAP-PEAP authentication.

When EAP authentication occurs using any of these protocols, the authentication server sends a server certificate to OAC. The certificate represents the server’s trust credentials. OAC must trust the server certificate before it can continue communicating with that server. If OAC does not trust the server, the authentication process terminates.

Overview of Trust Configuration

Trust configuration is fundamental to secure network communication between you and a network server. OAC gives you the tools to authenticate the server to which you are connecting and to ensure that you are connecting to the intended server. Authenticating server trust protects you from intrusion or hostile attacks from anyone who might be pretending to represent that server.

This chapter describes how to perform the following trust-based tasks in OAC:

- Add a trusted server.
- Edit a trusted server.
- Remove a trusted server.
- Display the current trust tree hierarchy.

- Add or remove certificate nodes.
- Add authentication servers or intermediate certificate authority (CA) nodes.
- Remove CA nodes.
- View certificate information.
- Manage untrusted servers (temporary trust).

For more background about authentication, trusted certificates, and the protocols that use them, see the following topics:

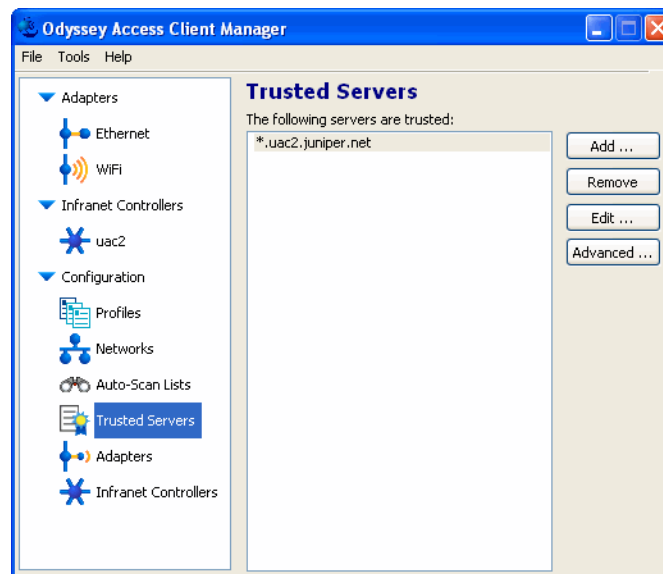
- “Extensible Authentication Protocol” on page 112
- “Certificates” on page 113

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.

1. Open the **Configuration** folder in the sidebar.
2. Select **Trusted Servers** to display the Trusted Servers dialog (Figure 11).

Each trusted server that is currently configured appears in the Trusted Servers dialog.

Figure 11: Trusted Servers Dialog

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.

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

Using the Simple Method to Configure Trust

The simple method of trust configuration provides two options for creating a list of trusted servers in OAC:

You can specify a list of servers to be trusted using domain names.

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 chain. This can be the certificate of a root or an intermediate certificate authority.

Adding a Trusted Server Entry

The simple method of configuring trust offers you two choices for adding a trusted server:

- Trust all servers whose certificates are issued by a specified (root or intermediate) CA.

- Use an intermediate CA or authentication server domain name to filter the certificate chain when you install the certificate that specifies the issuer of the trusted server certificates.

To add a trusted server:

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

To set **Server certificate must be issued by** field:

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

Server Identity

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

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

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

Removing a Trusted Server Entry

To remove an entry from the trusted servers list:

1. Select the entry from the Trusted Servers dialog.

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

The Trusted Server Properties dialog appears. From this dialog, you can change the server domain and select a different certificate. See the directions in “Adding a Trusted Server Entry” on page 93.

Using the Advanced Method to Configure Trust

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.

Each path through the trust tree defines a set of rules for matching a certificate chain. See “Displaying a Trust Tree” on page 95. 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, select **Advanced** on the Trusted Servers dialog. The dialog that appears enables you to navigate the trust tree and add certificates.

Adding Certificate Nodes

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

1. Select the **Add Certificate** button. The Select Certificate dialog appears.
2. Select a certificate from the list and select **OK**. You can select a certificate from the list of intermediate or trusted root certificates.

To display detailed information about any certificate before you add it:

1. Select the certificate.
2. Select **View** on the Select Certificate dialog.

Adding Authentication Servers or Intermediate CA Nodes

All nodes below the top level identify either 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:

1. Select the node in the tree below which you want to add the new item.
2. Select **Add Identity** in the Trusted Servers dialog. The Adding Identity dialog appears. Fill it in according to the directions in “Adding Identity” on page 96.
3. Enter the information that defines the rules that OAC uses to match a certificate in the server’s certificate chain to this node.
4. Select **OK**.

Adding Identity

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

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

1. For **Trust a server or intermediate CA with a valid certificate**, select one of the following:
 - Choose **Regardless of its name** to match any certificate, provided that it is signed by the certificate authority in the node above.
 - Choose **If its name matches the following name exactly** to require that the name in the certificate match the name that you specify.
 - Choose **If its name ends with the following name** to require that the name in the certificate is subordinate to the name you specify. For example, a certificate with name **sales.acme.com** would match an entry of **acme.com**.

2. For **Server or intermediate CA name**, enter the name (or final elements of a name) that you want to match. This field is not required if you select **Regardless of its name**. The form of the name depends on your choice of **Server or intermediate CA name type**.
3. For the certificate authority **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** field in the certificate or, if that is not present, the Common Name within the **Subject** field of the certificate. This is the most typical choice.
- Select **Domain Name in Subject Alternative Name** if the domain name is found in the **Subject Alternative Name** field in the certificate. This is similar to but more restrictive than the previous choice.
- Select **Subject Name** if the name is an X.500 name and is found in the **Subject** field in the certificate. If you enter a full or partial **Subject** name, it must be in X.500 form. It matches any certificate **Subject** name that is equal or subordinate to it.

For example, if you enter **OU = acme.com, C = US**, 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 choose **0**, the certificate that matches this node must have been signed using the certificate that matches the node above this node.
 - If you choose **1**, the certificate that matches this node 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 choose a number between **2** and **5**, that number of certificates might appear in the chain between the certificate that matches this node and the one that matches the node above.
 - If you choose **Unlimited**, 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 Nodes

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 from the tree.

The node you remove can be any of the following:

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

Viewing Certificate Information

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

1. Select the certificate.
2. Select **View Certificate** from the Trusted Servers dialog.

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 example below, the certificate is issued by **AcmeRootCA**.)

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

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 will be sustained until you restart OAC or select **Forget temporary trust** from the **Tools** menu.

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** field (see “Adding a Trusted Server Entry” on page 93). 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.

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 network— that is, without at least one Infranet Controller connection.

Accessing Log Files

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 email.

To display a log file:

1. Select **Tools** > **Logs** to open the Odyssey Log Viewer.
2. Click the **Settings** option to select a debug level. The following sections discuss each of the Log Viewer options and settings.

Log Viewer Controls

This section describes each of the controls available in the Log Viewer.

Settings

Use this option to control Log Viewer preferences for text color, window color, and font.

Debug Level

Use this option to set the debug level, which ranges from 0 (minimal logging) to 9 (verbose logging).

Maximum number of lines to buffer

Use this option to configure the maximum number of log lines that appear in the log viewer.



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

Text Color/Window Color/Font

Use this option to configure the appearance of the text displayed in the log viewer window.

Find

Use this option to locate specific text in the log messages currently being displayed in the log viewer.

Clear

Use this option to clear the current contents of the log viewer.

Save All

Use this option to save the log files in a single .ZIP file. You can browse to a preferred save location and specify the name of the file.

Copy

Use this option to copy selected text in the log viewer window to the Windows clipboard.

Freeze

Use this option to stop automatic scrolling of the viewer window.

Flow

Use this option to resume automatic scrolling of the viewer window.

Accessing Diagnostics

There are four categories of diagnostics information available from the **Tools > Diagnostics** menu. Select one of the following diagnostics from the pull-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

IPsec Diagnostics 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 currently apply.

IPsec Configuration

IPsec Configuration 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 currently connected.



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 email message for troubleshooting.

Host Enforcer Configuration

Host Enforcer Configuration shows you configuration information for all of the Host Enforcer policies currently 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 currently connected. If your Infranet Controller Role changes, additional policies might be applied or removed.

Network Configuration

Use this option to see 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

Use this option to see the current IP route table for the system. The output is the same as that for the `route print` command.

Save All Diagnostics

Use this option 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 for 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 Odyssey Access Client operates in a network, particularly from the standpoint of network security and authentication.

Network Security

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

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

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

- IEEE (Institute of Electrical and Electronic Engineers) standards for wireless LANs. These include 802.11a, 802.11b, and 802.11g. See “802.11 Wireless Networking” on page 108.
- IEEE 802.11i enhancements to 802.11. These were introduced to overcome some of the security weaknesses of 802.11.
- The WiFi Alliance second generation of WiFi protected access. WiFi protected access 2 (WPA2) (with advanced encryption standard (AES) encryption) adheres to the strong 802.11i enhancements. See “WiFi Protected Access and its Encryption Methods” on page 110 for definitions.
- WPA (with AES or temporal key integrity protocol (TKIP) encryption), which complies with a subset of 802.11i. While WPA is not as strong as WPA2, it addresses some of the security weakness of 802.11. See “WiFi Protected Access and its Encryption Methods” on page 110 for definitions.
- The IEEE 802.1X standard. 802.1X supplements the 802.11 standards with secure server-based wireless or wired network connections. See “802.1X Authentication” on page 111.

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

Encryption and Association for Secure Authentication

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

- Association is the method by which a client establishes a relationship with an access point.
- Data encryption is used to secure data that is exchanged between a client device and 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.
- Once a wireless client has associated with an access point, the user of that client device can be authenticated to the network. Authentication is used to secure the relationship between a user 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 109 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 “WiFi Protected Access and its Encryption Methods” on page 110 for a description of AES or TKIP encryption methods that enhance the 802.11 standards.
- Authentication using an 802.1X-based protocol. This method uses a variety of underlying authentication protocols to control network access. The stronger protocols provide cryptographically protected mutual authentication of the user and the network. In addition, you can configure Odyssey Access Client so that keys that are used to encrypt wireless data are generated dynamically. 802.1X-based authentication can use WEP, AES, or TKIP encryption, depending on network hardware/firmware. See “802.1X Authentication” on page 111 for information about authentication using 802.1X. See “WiFi Protected Access and its Encryption Methods” on page 110 for a description of some of the strongest available association and encryption modes.
- The 802.1X methods are viable for wired 802.1X-based network connections.

Odyssey Access Client Features for a Secure Network

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

- You can require user authentication. A user must be authenticated by the network before being allowed access to the network and make it safe from intruders. See “Extensible Authentication Protocol” on page 112 for an overview of the Odyssey Access Client authentication protocols. For protocol configuration details, see “Adding or Modifying a Profile” on page 54.
- 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 “Encryption Methods for an Association Mode” on page 76.
- 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 PC. For configuration details, see “Configuring Trust in OAC” on page 92 and “Viewing Certificate Information” on page 98.
- You can use mutual authentication between user and network must be cryptographically protected. This type of mutual authentication requires 801.1X-based protocols and prevents connections to phony networks. For configuration details, see “SIM Card Manager Use Case for this Option” on page 18.

802.11 Wireless Networking

There are many types of wireless communication. Odyssey Access Client is designed to work over networks that adhere to the IEEE 802.11 Wireless LAN standards, as well as the WiFi 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 PC establishes a wireless connection to a device called an *access point*. The access point links your wireless PC to the rest of the network. An access point provides general network connectivity for many PCs.

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

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

When you connect to a network via an access point, you are using the 802.11 *infrastructure mode*. See “Specifying a Network Type” on page 75 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 PCs that are located within range of each other. As a result, this networking mode does not involve an authentication server and cannot use 802.1X-based authentication.

The 802.11 standard refers to peer-to-peer network connectivity as *ad-hoc mode*. See “Specifying a Channel” on page 75, and “Specifying an Association Mode” on page 75 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 111. You can configure shared association following the directions in “Specifying an Association Mode” on page 75.
- **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 75.



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 111 and “Extensible Authentication Protocol” on page 112 for more information.

See the following topics:

- for directions for selecting an association mode in Odyssey Access Client.
- “Encryption Methods for an Association Mode” on page 76 for directions for selecting WEP encryption when using the shared or open association mode.

- “Preconfigured Keys (WEP)” on page 79 to use static WEP keys with Odyssey Access Client.



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

WiFi Protected Access and its Encryption Methods

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

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

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



NOTE: With access points enabled for WPA2 or WPA, you can obtain the stronger network security when you use dynamic encryption key generation and 802.1X-based authentication. See “802.1X Authentication” on page 111 and “Extensible Authentication Protocol” on page 112 for more information.

See the following topics:

- “Specifying an Association Mode” on page 75 to use WPA2 or WPA association mode with Odyssey Access Client
- “Specifying an Association Mode” on page 75 to use AES or TKIP encryption with WPA2 or WPA association
- “Encryption Methods for an Association Mode” on page 76 to configure a passphrase that is used in encryption key generation.

- “FIPS Secure Encryption (FE Only)” on page 77 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 Standards (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, Odyssey Access Client implements level 1 of this secure encryption standard using WPA2 or xSec association mode and AES encryption. Odyssey Access Client provides approved cryptographic algorithms and approved modes of operation for the Cryptographic Module Specification and provides the strongest cryptographic key management mechanisms.

For instructions about operating Odyssey Access Client in FIPS mode, see “FIPS Mode On / FIPS Mode Off (FE Only)” on page 17.

802.1X Authentication

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

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

When preconfigured WEP keys are used, it is the wireless client PC that is authenticated to the network. With 802.1X, it is the *user* who is authenticated to the network with the user credentials, which 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 PC and many access points can share a single RADIUS server to perform the authentication. This makes it much easier for the network administrator to control access to the network.

Extensible Authentication Protocol

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

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

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

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

- EAP-TTLS (tunneled transport layer security)
- EAP-PEAP (protected EAP)
- EAP-TLS (transport layer security)
- EAP-FAST (flexible authentication via secure tunneling)
- EAP-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 Odyssey Access Client when you configure it to validate the certificate of the authentication server using EAP-TTLS, EAP-PEAP, or EAP-TLS. If the certificate identifies a server that you trust and if the authentication server can prove that it is the owner of that certificate, then you can safely connect to this network. These are the strongest authentication methods available and, consequently, it is highly recommended that you use these methods for network authentication within your enterprise wireless network.

Certificates

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

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

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

- A public key
- A private key

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

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

Your enterprise certificate authority might issue certificates to smart cards. Odyssey Access Client supports all types of user certificates, 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 re-issued or renewed.

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

- An end entity certificate
- A root certificate

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

EAP-TLS

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

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

EAP-TTLS

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

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

If your enterprise has a user-based certificate infrastructure in place, you have the option to configure user certificate-based credentials for EAP-TTLS authentication, with or without tunneled password credentials. See “Using Certificates with EAP-TTLS Authentication” on page 65.

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 “Using Certificates with EAP-TTLS Authentication” on page 65 for more information about configuring inner protocols for EAP-PEAP authentication.

EAP-FAST

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

Reauthentication

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

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

Periodic reauthentication serves two purposes:

- As a general security measure, it verifies that you are still on a trusted network.
- It results in distribution of fresh shared keys to your PC 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 “Enabling Automatic Reauthentication” on page 24 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 PC and on the network authentication server. Private keys must be used to encrypt or sign data, signatures on certificates must be validated, and password credentials must be selected.

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

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 MOVE ALL OF THESE DETAILS TO A PROCEDURES CHAPTER” on page 23 for more information about using this feature.



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

Appendix B

Glossary

A

AAA—Authentication, Authorization, and Accounting.

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

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

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

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

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

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

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

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

ARP—Acronym for Address Resolution Protocol.

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

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

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

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

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

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

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

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

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

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

B

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

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

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

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

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

C

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

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

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

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

Certificate revocation—The act of invalidating a digital certificate.

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

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

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

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

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

COMSEC—Communications security.

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

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

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

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

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

D

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

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

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

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

DES—Data Encryption Standard.

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

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

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

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

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

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

DNS—Acronym for domain name system.

E

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

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

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

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

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

EAP-JUAC—JUAC is an EAP authentication protocol specific to Juniper Unified Access Control networks and is required when connecting to a Juniper Infranet Controller.

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

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

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

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

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

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

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

F

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

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

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

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

G

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

H

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

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

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

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

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

HTML—Hypertext Markup Language.

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

I

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

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

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

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

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

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

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

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

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

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

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

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

ISP—Internet Service Provider.

IT—Information technology.

K

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

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

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

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

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

L

Layer 2 Tunneling Protocol (L2TP)—A technology used with VPN to establish a communication tunnel between communicating parties over insecure media. L2TP permits a single logical connection to transport multiple protocols between a pair of hosts. L2TP is a member of the TCP/IP protocol suite and is defined in RFC 2661.

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

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

M

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

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

MD4—Message digest algorithm 4.

MD5—Message digest algorithm 5.

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

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

N

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

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

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

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

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

O

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

P

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

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

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

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

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

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

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

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

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

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

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

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

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

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

R

RC4—Rivest cipher 4.

RC5—Rivest cipher 5.

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

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

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

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

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

RSA—Referring to the principles: Ron Rivest, Adi Shamir, and Len Adleman. The RSA algorithm is used in cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.

S

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

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

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

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

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

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

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

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

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

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

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

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

T

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

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

TCP/IP—Abbreviation for Transmission Control Protocol/Internet Protocol.

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

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

Tunnel—A secure virtual connection through the Internet.

U

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

UDP—Abbreviation for User Datagram Protocol.

V

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

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

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

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

W

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

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

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

WLAN—Wireless Local Area Network.

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

X

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

Index

Numerics

802.11	
ad-hoc mode	108
defined	106
infrastructure mode	108
802.1X	
authentication	78
overview	111

A

access point	
ad-hoc mode	75
infrastructure mode	75
introduction	108
network	108
adapter	
add network	43
folder	19
remove	45
select	46
wireless	43
ad-hoc mode	
defined	108
setting	75
AES	
configuration	76
overview	110
peer-to-peer	111
use with association mode	76
airwaves	
survey	17, 33
anonymous name	
for logon	63
protocol restriction	63
set	63
any	
as a network	74
network, configuring connections	74
SIM card, using	59
association mode	
defined	106
methods	75
open	75
shared	75
WPA	76
WPA2	76
asymmetric cryptography	113
authentication	
802.1X	107

certificate-based	66
profile	54
protocols	61
servers, adding	96
setting in profile properties	60
status	21
traditional networks	5
tunneled	62
user	107
wireless	106
without password	66
X.500 names	96
authentication protocols	
add	61
inner	
most common	64
order of	64
multiple	61
ordering	61
remove	61
select inner	64
auto-scan list	
add	84
defined	30, 83
modify	85
preferred networks	84
preferred order of networks	84
remove	86
switching networks	84
testing	86
uses	83
view names in	86
auto-scan lists	
connecting to	46

B

beacon	
defined	49

C

certificate	
add to trusted server database	12
defined	113
for authentication	57
for inner authentication	66
for Windows logon	57
overview	57, 113
smart card	35
validate	62

- validation 61
- certificate authority
 - chain 93
 - defined 113
 - intermediate 94
 - root 113
- certificate chain
 - defined 114
 - trust trees 95
- channel
 - peer-to-peer 75
- compliance
 - security policy 2
- configuration
 - adapter 43
 - folder 19
 - network 73
 - profile 53
 - route 41
- configuring
 - connection to any network 74
- connect
 - to Infranet Controller 26, 88
 - to network 45
- connecting
 - wireless networks 46
- connection
 - multiple network 31, 48
 - status 21, 50
 - types 31, 48
- content dialog 15, 20
- credentials
 - secure 63

D

- data encryption
 - purpose 106
- diagnostics
 - Host Enforcer configuration 103
 - IPsec 41
 - IPsec configuration 103
 - Network Agent 41
 - network agent 103
 - options 102
 - view 102
- disconnect
 - from Infranet Controller 29, 90
 - from network 32, 48
 - from wireless network 46
- DNS name
 - Infranet Controller 88
- domain
 - controller
 - EAP interaction 115
 - login name 55
- driver software 9
- dynamic encryption keys
 - reconnection effects 32, 49

E

- EAP
 - as inner authentication 65
 - definition 112
- EAP protocols
 - outer and inner 64
- EAP-AKA
 - configuration 59
 - overview 115
 - with SIM card 60
- EAP-Cisco Wireless 115
- EAP-FAST 112
 - credentials 38
 - overview 115
 - token card 62
 - tunneled method 62
- EAP-JUAC 112, 115
 - overview 115
- EAP-LEAP 112
 - overview 115
- EAP-over-HTTP 3
- EAP-PEAP 112
 - generic token card options 62
 - inner protocols, selecting 66
 - overview 115
- EAP-POTP 112
 - and token card 65
 - overview 115
 - password option 62
 - PIN 67
- EAP-SIM
 - configuration 59
 - identities 60
 - overview 115
 - with SIM card 60
- EAP-TLS 112
 - key generation 78
 - overview 114
- EAP-TTLS 112
 - certificate options 63
 - generic token card options 62
 - key generation 78
 - overview 114
 - settings 63
- encryption 22
 - dynamic keys 78
 - method, Networks panel 76
 - methods 110
 - methods for association mode 76
 - pre-configured keys 74
 - private key 113
 - secure 10
 - status 22
- endpoint trust status 22
- exportable, private key, FIPS 7
- Extensible Authentication Protocol 112

F

- file menu options 16

- FIPS
 - adapter requirements 6
 - certificate requirement 6
 - compliance 10
 - encryption 111
- FIPS mode
 - certificate requirements 7
 - description 111
 - on/off 6
 - required 76, 77
- forget
 - temporary trust 16
- G**
- generic token card
 - options 62
- H**
- help menu options 18
- Host Checker
 - defined 2
- Host Enforcer
 - configuration 41, 103
 - defined 3
- I**
- identity
 - server 94
 - SIM 60
 - SIM card 60
- IMSI
 - SIM card 60
- informational graphics 21
- Infranet Controller
 - add to configuration 88
 - connect to 26, 88
 - defined 2
 - disconnect from 29, 90
 - DNS name 88
 - folder 19
 - IP address 88
 - profile requirements 87
 - status 89
- Infranet Enforcer
 - defined 2
- infrastructure mode
 - access point 75
 - defined 108
- initial profile 54
- inner authentication 61
 - defined 63
 - select protocol 64
- inner authentication protocols
 - add 65
 - EAP 65
 - remove 65
- installation
 - OAC in traditional network 13
 - OAC in UAC network 11
- intermediate CA
 - adding 96
 - advanced usage 95
 - overview 114
- International Mobile Subscriber Identity 59
- IP address
 - Infranet Controller 88
- IPsec
 - configuration 41, 103
- K**
- keyboard shortcuts 23
- L**
- LAN, defined 105
- Layer 2 3
- Layer 3 3
- LDAP 114
- leaf node 95
- LEAP 115
- license key
 - check expiration 19
 - overview 11
 - types 11
- lightweight EAP 115
- log files
 - setting levels 41
 - view 41, 101
- log level
 - set 101
- login credentials
 - certificate 55
 - password 55
 - SIM Card 55
 - soft token 55
- login names
 - specifying 55
- M**
- menu bar 15
- multiple
 - connections 31, 48
- mutual authentication 61, 112
 - 802.1X 107
 - explained 112
 - server trust 107
- N**
- network
 - any network, configuring 74
 - association 75
 - configuration 41, 73
 - configuring
 - connection to any 74
 - description field 75
 - encryption methods 76
 - hardware requirements 11
 - multiple connections 31, 48
 - name

SSID	74	PIN	
overview	74	caching	35
peer-to-peer	75	EAP-POTP	67
preemptive	18	SIM card	60
preferred	18	SIM card settings	60
properties		preferred network	
add or modify	73	auto-scan lists	84
reconnecting	32, 49	preshared passphrase	107
sample configuration	82	private key	113
scan for available	74	profile	
scan for available connection	30, 48	add	54
security policies	2	configure	53
select	73	defined	53
settings	73	initial	54
type	75	modify	54
WEP keys	78	name	54
wireless 802.11	108	password	55
Network Agent		sample configuration	71
diagnostics	103	user info	55
network connection		user information	59
set timing	18, 38	provider-specific settings	
network name		SIM	60
defined	74	public key	113
O		R	
OAC		RADIUS server	111
defined	1	realm	
deployment environments	2	defined	70
in traditional network	2, 5	realms	
installing	9	setting, EAP-SIM	60
register	19	reauthentication	36
OAC Manager	25	purpose	116
exit	24	uses	36
open mode		reconnecting	
WEP	75	effect on encryption keys	32, 49
definition	109	to network	32, 49
operating system		release notes	x
supported releases	10	remediation	28, 90
P		defined	5
PAP/Token Card		instructions	29, 90
password caching	65	requirements	
passphrases		browser	11
hexadecimal	79	installation	10
password		roaming	116
caution	56	wireless	36
configure in profile	55	role	
forget	16	defined	3
generic token card	62	root certificate authority	113
POTP options	62	RSA soft token	58
PEAP		S	
overview	115	scan	
settings in profile properties	66	list	84
token card options	62	wireless networks	33
peer-to-peer network		scripts	
definition	108	check new	34
IP addresses	108	run	17, 33
personal certificate		secure authentication	
options for EAP-TTLS	65	methods	106

- secure encryption
 - FIPS 6
 - Layer 2 protocol 76
- security
 - enforcement 4
- server
 - identity 94
 - identity formats 94
 - name 94
 - temporary trust 37
 - validate certificate 61
- service set identifier 109
 - see SSID
- session resumption 36
 - defined 36
 - enable 36
- shared mode
 - WEP 78
 - defined 109
- shortcut keys 23
- sidebar 15
 - folders 19
- signal power, viewing 21
- SIM card
 - any, selecting 59
 - authentication 59
 - configure 59
 - for authentication 59
 - IDs, entering 59
 - IMSI 59, 60
 - login names 60
 - manager 17, 34
 - PIN 60
 - PIN settings 60
 - set ID 59
- simultaneous connections
 - establishing 31, 48
- single sign on 25
- smart card
 - certificate 57
 - certificates 113
 - FIPS constraint 35
 - PIN prompt 35
- soft token
 - authentication options 58
 - configuration 58
 - enable 58
 - for authentication 58
- SQL 114
- SSID
 - auto-scan list switching 84
 - defined 109
- status
 - adapter 49
 - connection 21, 50
 - encryption 22
 - endpoint trust 22
 - Infranet Controller 89
 - signal power 21
- switch
 - 802.1X 108
 - switching networks, lists 84
- T**
- temporary trust
 - untrusted servers 98
- TKIP
 - implementing 76
 - overview 110
 - peer-to-peer 111
 - use with association mode 76
- TLS
 - overview 114
- token card
 - authentication
 - password 62
 - settings 64
- tools menu options 17
- trust
 - all servers 93
 - configuration
 - simple method 93
 - temporary 37
- trust trees 95
- trusted server
 - add 93
 - add certificate 12
 - Advanced button 95
 - advanced method 95
 - any 93
 - editing 95
 - entering 93
 - leaf nodes 95
 - removing 94
- TTLS
 - overview 114
 - settings 63
- tunnel
 - encrypted 63
 - password credentials 66
- U**
- Unified Access Control 2
- untrusted server
 - dialog 98
- user info
 - SIM card settings 59
- W**
- Web portal 12
- WEP keys 74
 - any network connection 74
 - defined 109
 - dynamic 78
 - open mode 109
 - peer-to-peer 110
 - preconfigured 78, 79
 - shared mode 78
 - specify 78

- static 78
- use with association mode 76
- Wi-Fi network
 - scan for 30, 48
- Windows logon settings..... 18, 38
- wired network
 - connect to 31, 47
- Wired-Equivalent Privacy..... 109
- wireless
 - beacon 49
 - networks
 - scan 30, 48
- wireless adapter
 - compatibility 51
- wireless network
 - connect to 46
 - disconnect from 46
- wireless roaming 36
- WPA 76
 - implementing..... 75
 - overview 110
 - passphrases..... 79
- WPA2 76
 - overview 110
 - passphrases..... 79
- X**
- X.500 names 96
- xSec
 - configuration
 - wireless 802.1X 76
 - encryption mode requirement 76
 - FIPS requirements..... 11
 - hardware requirements..... 11