



Odyssey Access Client Administration Guide





Juniper Networks
Odyssey Access Client

Administration Guide

Enterprise Edition
FIPS Edition

Release 4.6
December 2006

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

Copyright© 2002-2006 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	vii
	Audience	vii
	Conventions	viii
	Documentation	ix
	Unified Access Control Documentation	ix
	Release Notes	ix
	Web Access	ix
	Context-Sensitive Help and Other Product Information	ix
	Glossary	ix
	Contacting Customer Support	x
Chapter 1	Administration Overview	1
	OAC Network Authentication Overview	1
	Overview of OAC Administrator Tools	2
	Planning an OAC Configuration	3
	Opening the Odyssey Access Client Administrator Tools	4
	Connection Settings	4
	Initial Settings	5
	Machine Accounts	5
	Permissions Editor	5
	Merge Rules	5
	Custom Installer	5
	Script Composer	5
	PAC Manager	5
Chapter 2	Configuring Network Connection Settings	7
	Connection Settings Tool	8
	About Network Connection Timing	8
	Machine-Level Connection Options	8
	User-Level Connection Options	9
	Configuring a User Account	9
	Using a Prior to Windows Logon Connection	10
	Specifying Initial Settings for a Network Configuration	10
	Connecting After the Windows Desktop Appears	11
	Configuring a Machine Account	12
	Configuring Machine Account Connection Settings	13
	Configuring a Network Connection with GINA	13
	Using a Third-Party GINA Module Together with Odyssey GINA	14
	Installing the Odyssey GINA Module	15
	Removing the Odyssey GINA Module	15
	GINA Compatibility with Other Modules Running at Windows Logon	15
	Using GINA with Smart Cards	16
	Restrictions on Early Network Connections	16

Chapter 3	Configuring Initial Settings	19
	Using the Initial Settings Tool.....	20
	Caution on Overriding Default Windows Logon Settings.....	21
	Configuring Prior to Windows Logon Connections.....	21
	Options for Login Name Format	22
	Specifying a Custom Login Name Format	23
	Domain-Decorated or Undecorated Logon Names	24
Chapter 4	Setting Up a Machine Account	25
	Machine Account Tool.....	26
	Enabling a Machine Account Connection.....	26
	Machine Account Profile Options.....	27
	Setting Machine Account Password Credentials	27
	Setting Automatic Certificate Selection for EAP-TLS	27
	Trust Configuration Requirements for Machine Authentication	27
	Restrictions for Machine Account Settings.....	27
	Configuring a Machine Password	28
	EAP Methods that Support Machine Credentials.....	29
Chapter 5	Using the Permissions Editor	31
	Permissions Editor Tool Settings	32
Chapter 6	Setting Merge Rules	35
	How Merge Rules Apply to User Configurations	35
	Use Cases for Merge Rules.....	35
	Merge Rule Settings	36
	Merge Rules Tool Overview.....	37
	Setting Merge Rules for Profiles	39
	Setting Merge Rules for Networks.....	39
	Setting Merge Rules for Individual Networks	39
	Setting Merge Rules for Auto-Scan Lists	40
	Setting Merge Rules for Intranet Controllers	40
	Merge Rules Settings in the Other Tab.....	41
Chapter 7	Using the Custom Installer	45
	Custom Installer Tool	45
	Using the Custom Installer	46
	Creating a Custom Update File	46
	Creating an Installer File.....	47
Chapter 8	Using Scripts	49
	Script Composer Options	49
	Creating Scripts with Script Composer	50
	Adding or Setting Profiles with Scripts.....	51
	Removing a Profile	51
	Activating a Profile for a Wired Connection	52
	Adding or Setting Networks with Scripts.....	52
	Removing a Configured Network.....	52
	Activating a Network for a Wired Connection.....	53
	Adding or Setting Auto-Scan Lists	53
	Removing Auto-Scan Lists	53

	Managing Other Setting with Scripts.....	53
	Adding or Setting a Trust Tree.....	53
	Replacing Options Settings.....	54
	Removing Networks Using SSIDs	54
	Setting or Replacing FIPS Options (FE Only)	54
Chapter 9	Using PAC Manager	57
	Using PAC Manager to Provision PACs to Clients	57
	Using the PAC Manager Tool.....	57
	Importing a PAC	58
	Refreshing the Pac Manager Display	58
	Deleting a PAC	58
	Exiting from the PAC Manager.....	58
Chapter 10	Sample Administrative Workflows	59
	Sample Administrative Workflows	59
	Testing Configuration Settings.....	60
	Testing User Connection Settings	60
	Testing Machine Connection Settings	60
	Preconfiguring OAC for a Group of Users	61
	Setting Up an OAC Configuration	61
	Exceptions to Network Connection Options.....	62
	Custom Install: Provide Printable Documentation	62
	Configuring User Authentication with No Machine Connection	63
	Connecting Before Windows Logon.....	63
	Connecting After Windows Logon (with or without GINA)	64
	Configuring Machine-Only Connections	64
	Configuring Machine Connections that Switch to User Authentication	64
	Creating Scripts for Incremental Updates	65
	Notes on the Directory for Scripts.....	66
	Command-Line Code to Create and Load OAC Manager Scripts	67
	Configure OAC Updates for Mass-Distribution to Users	68
	Using Smart Cards with GINA	69
	Configuring Single Sign On for TTLS or PEAP.....	71
	Prerequisites.....	71
	Setting Up a Prior to Windows Logon Configuration Using GINA	72
	Specifying User Account Connection Settings and Installing OAC GINA... ..	72
	Testing Prior to Windows Logon Settings	72
	Configuring Required FIPS Mode Connections (FE Only).....	73
Appendix A	Glossary	75
	Index	89

About This Guide

This guide describes how to configure, update, and deploy Odyssey Access Client (OAC) to users for wired or wireless network access. It addresses two licensed editions of OAC:

- OAC Enterprise Edition (referred to in this guide as EE)
- OAC FIPS Edition (referred to in this guide as FE)

These editions of OAC have similar but not identical sets of features. Where there are distinctions or differences in product features and options among them, the manual discusses and points out those differences where they apply.

You can read this manual in PDF format. It is provided on the OAC CD and available on the Juniper Networks web site at:

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

Audience

This manual is for network administrators whose responsibilities include managing secure network access. It is particularly directed to those administrators who configure and deploy OAC to network users and who determine which OAC features to preconfigure and lock and which features users can modify.

OAC offers a broad range of configuration options and controls, both for administrators and for client users. It is the administrator who determines how much flexibility and control users need based on corporate security policies.

All administrators who are responsible for managing OAC should be familiar with using OAC and with the *Odyssey Access Client User Guide*.

Some of the information in this document also pertains to configuration tasks that relate specifically to the Juniper Unified Access Control security solution and in particular to connecting to and using Infranet Controllers. If you use OAC on a network that includes Juniper's Unified Access Control security solution, refer to the *Unified Access Control Administration Guide* available on the Web at:

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

Conventions

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

Table 1: Notice Icons




Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates that you 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>Infranet Controller</i> is a server that verifies your identity and your computer's compliance with security requirements before you can access protected resources. ■ Variable element: When adding a trust server, specify the server name using as <i>domain_name.com</i>. ■ Book name: See the <i>Odyssey Access Client User Guide</i>.

Documentation

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

Unified Access Control Documentation

If you use OAC on a network that includes Juniper's Unified Access Control security solution, refer to the *Unified Access Control Administration Guide* available on the Web at:

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

Release Notes

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

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

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

Web Access

To view the OAC documentation on the Web, go to:

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

Context-Sensitive Help and Other Product Information

Odyssey Access Client Administrator includes online help that you can access from your computer. To invoke the help system, select the **Help > Help Topics** menu command.

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

You can use the **Help > View Readme File** menu command to open the `readme.txt` file. This file might have important information about OAC that is not included in this manual.

Glossary

This manual includes an extensive Glossary.

Contacting Customer Support

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

Chapter 1

Administration Overview

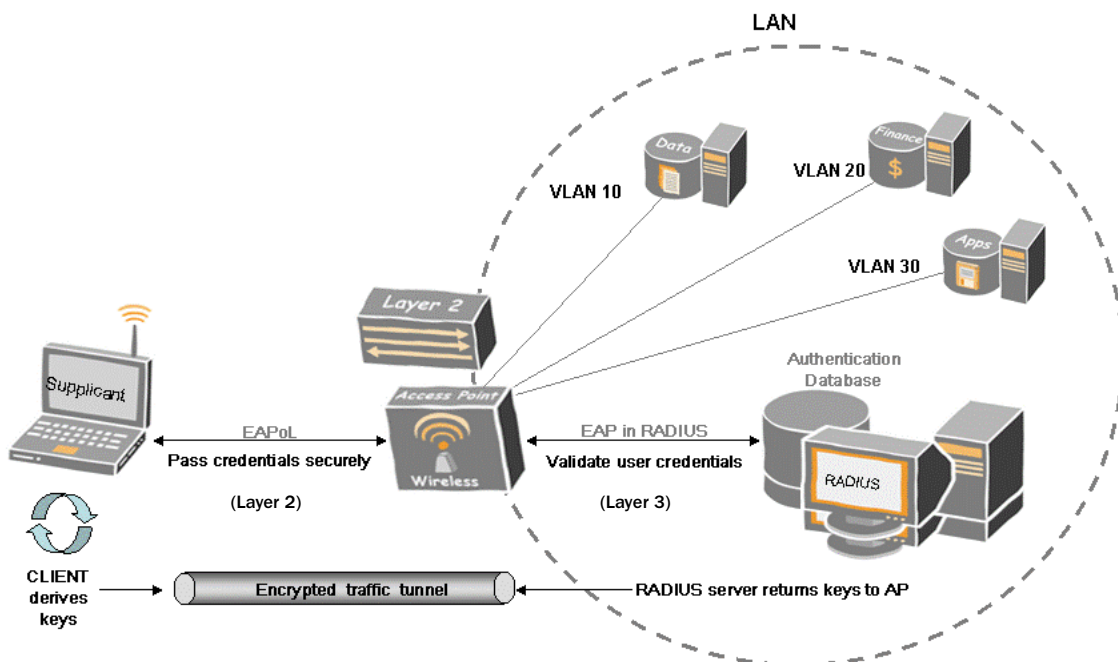
This chapter is an overview of the Odyssey Access Client Administrator—a suite of tools for configuring, updating, and deploying Odyssey Access Client (OAC) to users and for controlling which features that users can add or modify. To access the Odyssey Access Client Administrator, go to the **Tools** menu in the OAC Manager.

To access and use Odyssey Access Client Administrator, you must be using OAC Enterprise Edition or FIPS Edition. This chapter also includes an overview of the components and processes required for secure network authentication and a summary of topics to consider when planning for configuring and deploying OAC to users.

OAC Network Authentication Overview

When OAC attempts a secure network connection, a series of negotiated transactions takes place before that connection is complete. Figure 1 summarizes the basic network components and transactions involved in such a connection.

Figure 1: Network Authentication Events



A user or a machine (computer) must be recognized and authenticated before gaining access to protected network resources. Such a connection requires a series of events to occur before a user completes the Windows logon process. In an 802.1X network, this includes user or machine authentication using EAP (Extensible Authentication Protocol) methods.

The basic events required for authenticated network access include:

- Attempt an authenticated network connection. Depending on the corporate network infrastructure, the network connection can include any of the following connection types:
 - Layer 2 connection to an 802.1X switch or wireless access point.
 - Layer 3 connection to an Infranet Controller for to a switch that is not capable of 802.1X authentication.
- For a wired OAC client, authentication occurs through authentication ports on an 802.1X switch (at Layer 2) to the authentication server. For a network switch that does not support 802.1X, the network connection occurs at Layer 3.
- A wireless OAC client communicates with the authentication server through an 802.1X access point. The client and the authentication server conduct a public/private key exchange.
- An authentication server then sets up an encrypted tunnel used to negotiate secure wireless authentication.
- Successful wired or wireless authentication gives the user access to a VLAN and the appropriate protected network resources.

Overview of OAC Administrator Tools

You can preconfigure OAC and deploy a common configuration to multiple users at the same time with “push” software deployment products. You can update existing clients with new or modified configuration settings that reflect your current network security policy. The Odyssey Access Client Administrator tools enable an administrator to select individual OAC features and select or disable (lock) them before deploying the configured OAC client to users.

The Odyssey Access Client Administrator tools each have a particular purpose and work collectively to produce a final configuration image. The settings that you make in one tool can influence the settings that you make in other tools. For instance, after setting up configuration settings, you can lock the configured authentication protocols to prevent users from changing them. Once the basic configuration settings have been made, you can specify rules for how configuration updates apply to individual users or machines.

Use these tools to deploy a secure configuration of OAC to your users.

Planning an OAC Configuration

Consider the following questions when you plan an OAC configuration:

- Which outer EAP authentication protocols should you use? In a UAC network, you can use either TTLS or PEAP. In a traditional network, check your corporate security policy or ask your CIO about which protocols are supported.
- If you use TTLS or PEAP, which inner authentication protocols should you use? In a UAC network, you must use JUAC.
- Which encryption method(s) apply? The encryption methods available to you depend on the access points deployed on your network and on the association mode you select (WEP, WPA, or WPA2). If you are using the OAC FIPS Edition (FE), there are specific constraints on encryption methods, based on whether FIPS Mode has been selected. Contact your network security officer if you are unsure about which methods your network supports.
- Should you allow users to access and update network auto-scan lists? Auto-scan lists might pose risks of man-in-the-middle attacks or other applications designed to attract wireless connections. Consider using preemptive networks as part of your wireless network configuration
- For wireless networks, what are the SSIDs for your wireless access points? The SSIDs that you use to configure wireless networks must match those of the wireless access points on your network.
- Does wireless suppression make sense for your users? Wireless suppression disables wireless connections as long as the client has a wired network connection. A wired connection usually provides greater network bandwidth and preserves the wireless network bandwidth for users who need a wireless connection.
- Should you allow users to access ad hoc networks? While access to ad hoc networks might be useful for some users, they can present an added security risk to a corporate network.
- Should you allow users to modify any of the configuration settings after you deploy them? The degree of flexibility that you allow users reflects your corporate security policy and the technical sophistication of your users. You can set up OAC with as many or as few options for users as you like.
- Should you allow users to add, remove, or modify trusted servers and certificates? You might want to prevent users from modifying trust configuration settings. You can do this using the Permissions Editor tool.
- If your network includes Infranet Controllers, what network profile configuration settings apply? Should these settings be locked so that users cannot change them? Each Infranet Controller requires a separate profile.
- How will you deploy the configuration? In a UAC network, you can push preconfigured clients from an Infranet Controller. In a traditional network, you can use an .msi file and update scripts.

Read through this guide and the *Odyssey Access Client User Guide* carefully before configuring OAC for users and become as familiar as possible with all of the options available.

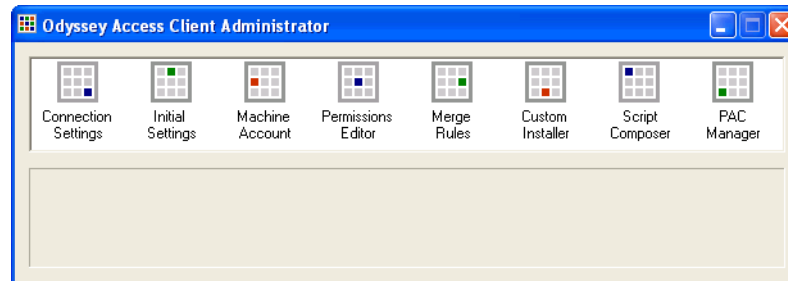
“Sample Administrative Workflows” on page 59 provides several sample workflows for performing common administration tasks, such as setting up single sign on for users.

Opening the Odyssey Access Client Administrator Tools

The Odyssey Access Client Administrator tools are individual icons in the Odyssey Access Client Administrator management interface.

To use the Odyssey Access Client Administrator, select **Tools > Odyssey Access Client Administrator** (see Figure 2) from the Odyssey Access Client Manager. You can also double-click the `odClientAdministrator.exe` application in the directory where OAC is installed.

Figure 2: Odyssey Access Client Administrator Tools



The following sections summarize the Odyssey Access Client Administrator tools. To open one of the tools, double-click the icon.

Connection Settings

Use this tool to configure one of the following network connection timings:

- Connect to the network at the machine hardware level (not at the user level) at Windows startup time. See “Configuring a Machine Account” on page 12.
- Connect to the network before Windows logon. Require user credentials. See “Using a Prior to Windows Logon Connection” on page 10 and “Installing the Odyssey GINA Module” on page 15.
- Connect to the network after Windows logon but before the Windows desktop appears. Require user credentials.
- Connect to the network after the Windows desktop appears. Require user credentials.

Initial Settings

Use this tool to perform one or more of the following tasks:

- Preconfigure the initial settings for all new users of this machine. See “Using the Initial Settings Tool” on page 20.
- Set up the user network and profile for user authentication that takes place before Windows logon.
- Create and test preconfigured settings before creating a new custom installer file. See “Using the Custom Installer” on page 45.
- Create and test configuration updates before distributing them to users.

Machine Accounts

Use this tool to configure a network connection that authenticates the credentials for the physical machine.

Permissions Editor

Use this tool to apply customized feature-by-feature restrictions on users’ ability to modify OAC configurations. This tool lets you lock settings that you do not want users to change.

Merge Rules

Use this tool to specify the rules for creating a settings update file or for a new custom installer file. These rules determine how configuration items are added to existing user configurations. You can also assign rules that modify current configurations or that prevent users from editing the configurations.

Custom Installer

Use this tool to create a preconfigured installer (.msi) file or a settings update file from the initial user or machine settings that you have configured with Odyssey Access Client Administrator tools. Use custom installer files for upgrades and new user installations. Once you have the .msi file, you can deploy the OAC configuration to users with a variety of mass-distribution deployment tools.

Script Composer

Use this tool to create configuration scripts to update OAC configurations that add new settings, replace existing settings, or remove settings.

PAC Manager

Use this tool to manage and provision Protected Access Credentials (PACs) for EAP-FAST.

Chapter 2

Configuring Network Connection Settings

Use the Connection Settings tool to configure options that control the type and timing of network connections from OAC.

By default, OAC connects to a network after the Windows desktop appears. However, in some cases it might be necessary to establish an authenticated connection earlier, especially when it is necessary to enable domain authentication before the user logs on.

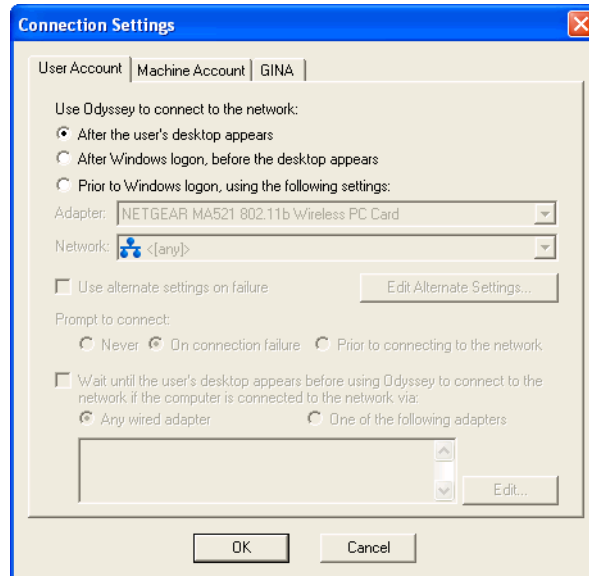
There are three general categories of configuration options in this tool:

- Specifying whether to authenticate and connect to the network at the machine level or at the user level. At the machine level, the network connection uses the credentials of the physical computer. A machine connection persists as long as the machine (computer) is running Windows. At the user level, the network connection requires user's logon credentials and persists as long as the user is logged on.
- Configuring the timing for when an authenticated network connection should occur. You can configure network connection timing settings to take place at various points: before, during, or after the Windows login process.
- Using the Odyssey Graphical Identification and Authentication (GINA) module to control exactly when user-level authentication occurs during Windows startup.

Connection Settings Tool

Use the Connection Settings tool to configure the type and timing of network connections. To open the Connection Settings tool (Figure 3), double-click **Connection Settings** in Odyssey Access Client Administrator.

Figure 3: Connection Settings Tool



The Connection Settings tabs are:

- **User Account**—Use these settings to configure the default timing of user network connections.
- **Machine Account**—Use these settings to configure a machine-level network connection at Windows startup time using machine credentials.
- **GINA**—Use these settings to enable the ability to connect to the network before Windows logon. Various vendors have their own versions of GINA. The Odyssey GINA module is designed to interact with OAC.

About Network Connection Timing

You can control when network connections occur based on events such as Windows startup and user logon. Connection timings can apply at either the machine connection level or the user logon level and are mutually exclusive. The settings described in this section show the options available for configuring when to connect.

Machine-Level Connection Options

A machine connection to the network uses the physical computer's credentials instead of user credentials.

The following configuration options are available for a machine connection:

- A machine-level connection to the network occurs when Windows starts up. With this connection type, the machine remains accessible over the network even if the user is not logged on, as long as the machine is still running. This option is useful for deploying update scripts and backups whether or not the user is logged on.
- A machine-level connection to the network occurs at Windows startup time and switches to a user-level connection and authentication immediately before the user logs on to Windows.
- A machine-level connection to the network occurs at Windows startup time and switches to user-level connection and authentication after the user logs on to Windows but before the desktop appears.
- A machine-level connection to the network occurs at Windows startup time and switches to user-level connection and authentication after the desktop appears.

User-Level Connection Options

- A user-level connection to the network occurs based on user credentials immediately before the user logs on to Windows.
- A user-level connection to the network occurs based on user credentials after the user logs on to Windows but before the desktop appears.
- A user-level connection to the network occurs based on user credentials after the Windows desktop appears.

Note that some of these configurations are enabled or disabled based on other features that you select. See “Restrictions on Early Network Connections” on page 16 for more information.

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

- “Configuring User Authentication with No Machine Connection” on page 63
- “Configuring Machine Connections that Switch to User Authentication” on page 64

Configuring a User Account

This section discusses the options for configuring default settings for a network authentication based on user logon credentials.

The success of a network connection might depend on the timing that you select. The safest option is to establish the network connection after the desktop appears. However, if you require users to connect to the network before the desktop appears—for example, if you run startup scripts from the network—select an earlier connection time.

Use the **User Account** tab (Figure 3) in the Connection Settings tool to configure a connection to occur before or after the Windows logon prompt appears.

The options listed under **Use Odyssey to connect to the network** selection at the top of the **User Account** tab are for configuring the timing of a user-level connection. The options are:

- **After the user’s desktop appears:** Select this option if you do not want the user to establish a network connection before the desktop appears.
- **After Windows logon, before the desktop appears:** Select this option if you want the user to establish a network connection before the desktop appears but not before the Windows logon.
- **Prior to Windows logon, using the following settings:** Select this option if you want the user to establish a network connection before logging on to Windows.

To configure Windows logon features for a custom installer or for a settings update file template, follow the guidelines in “Configuring Prior to Windows Logon Connections” on page 21.

Using a Prior to Windows Logon Connection

To be able to configure Prior to Windows logon connection settings, go to the **GINA** tab of the Connection Settings tool and install the Odyssey Access Client GINA module first. Refer to “Installing the Odyssey GINA Module” on page 15 and “GINA Compatibility with Other Modules Running at Windows Logon” on page 15.

If you select **Prior to Windows logon**, select the adapter and network or auto-scan list from the lists provided on the **User Account** tab of the Connection Settings tool.

If you are configuring settings for a wired 802.1X connection, select a profile rather than a network or auto-scan list.

Specifying Initial Settings for a Network Configuration

If your network configuration is based on a profile that uses a password-based authentication method, select **Use Windows password** on the **Password** subtab of the **User Info** tab in the Profile Properties dialog.

If your network configuration is based on a profile that uses EAP-TLS or any other certificate-based authentication method, select **Use the logon certificate from my smart card reader** on the **Certificate** subtab of the **User Info** tab in the Profile Properties dialog.



NOTE: Turning FIPS Mode on disables OAC smart card management.

The available options are:

- **Use alternate settings on failure**—Provide an alternate wired 802.1X adapter and profile (or wireless adapter network) for connections that take place before Windows logon. The alternate configuration applies if 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 occur before Windows logon.

Configure the alternative adapter and profile in the Initial Settings tool before you configure alternate settings for this option.

After selecting this option:

- a. Select **Use alternate settings on failure**.
 - a. Select **Edit Alternate Settings**.
 - b. Select the alternative adapter and profile.
- **Prompt to connect**—Require a prompt screen to appear before the network connection at logon time based on one of the following choices:
 - **Never**—Select this option if you do not want your users to be prompted to connect, even if the connection attempt fails.
 - **On connection failure**—Select this option if you want your users only to be prompted when a connection attempt fails.
 - **Prior to connecting to the network**—Select this option if you want your users to be prompted each time they log on to Windows.
 - **Wait until the user's desktop appears before using Odyssey Access Client to connect to the network**—Override the prior to Windows logon connection setting when users can connect with a network adapter.

Then select **Any wired adapter**. When you do so, OAC connects after the desktop appears.

Connecting After the Windows Desktop Appears

You have two choices for the conditions under which the connection takes place after the desktop appears:

- Defer the connection whenever users of this machine are connected to your network through a wired adapter. Do this by selecting **Any wired adapter is already connected**. This option applies even if the wired adapter is not connected to an 802.1X hub or switch.
- Defer the connection whenever users are connected to your network through one or more specified adapters. Do this by selecting **One of the following adapters**. This option is valid for any adapter listed.

To edit the list of adapters:

- a. Select **Edit**. The Select Adapters dialog appears.
- b. Select any adapters that you want used for network connections that occur after the desktop appears.
- c. Select **OK** to close the Select Adapters dialog.

The selected adapters appear in the list next to the **Edit** button on the **User Account** tab of the Connection Settings tool.

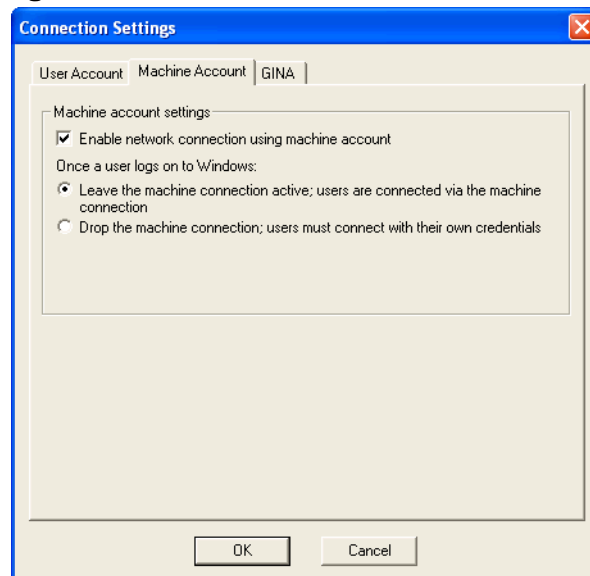
Configuring a Machine Account

The purpose of a machine account is to connect and authenticate a physical machine (the computer), rather than a user, to the network. This process includes having an IP address assigned to the machine. The network connection occurs before the user logs on. This can be useful for setting up domain-level resources and drive mappings before the user tries to connect.

User authentication is different from authenticating a machine because different credentials are required to connect to the network. While the physical machine might have network access, a separate process is needed for a user to log on and be authenticated. Thus, a machine account and a user account are mutually exclusive.

To connect to the network at machine startup time with machine (rather than user) credentials, select **Enable network connection using machine account** from the **Machine Account** tab (Figure 4) on the Connection Settings tool.

Figure 4: Machine Account Tab



If you configure machine account connections, you must also configure profile options (such as which credentials and network to use) for machine account connections using the Machine Account tool. (See “Machine Account Profile Options” on page 27.) Once you select **Enable network connection using machine account**, select one of the following mutually exclusive options:

- **Leave the machine connection active; users are connected via the machine connection**—Maintains the machine-level network connection after a user logs on. This option gives users less control of their network connections but they still have access to the network resources. They can view status information and reconnect or reauthenticate to the network but cannot change the existing OAC configuration.

A use case for this option is an environment where multiple users perform similar tasks, such as in a travel agency, and use any available computer in the office to do work. The machine must be authenticated but the users do not.

- **Drop the machine connection; users must connect with their own credentials**—Drops the machine connection and automatically establishes a network connection based on the user’s Windows credentials when the user logs on. With this connection type, users have less restricted network access than when the machine connection is still active. Once authenticated, users can modify or view connection settings using the Odyssey Access Client Manager.

If you select this option, set the timing for the user connection under the **User Account** tab.

Select one of the following timing options:

- After the user’s desktop appears
- After Windows logon, before the desktop appears
- Prior to Windows logon, use the following settings

Configuring Machine Account Connection Settings

To configure your connection settings based on your selections:

1. Double-click the **Connection Settings** icon in the Odyssey Access Client Administrator.
2. Select a machine network connection option from the **Machine Account** tab.
3. Configure the network connection settings for machine connections in the Machine Account tool.
4. If you want users to connect with their own credentials after the machine connection is established, double-click the **Initial Settings** icon in the Odyssey Access Client Administrator to configure new user account settings.

See “Restrictions on Early Network Connections” on page 16 for a listing of features unavailable when you configure a machine account connection.

Configuring a Network Connection with GINA

GINA is the OAC Graphical Identification and Authentication module, a replaceable DLL (downloadable library) component that runs before the Windows logon process to gather user credentials. GINA is instrumental in enabling a network connection to occur before Windows logon. It captures user logon credentials from the Windows logon dialog and delays the actual Windows logon to enable other setup processes and scripts to run first.

The Odyssey GINA implementation enables you to set up an OAC configuration to enable Windows users to connect to the network using Windows logon credentials before Windows logon. Connecting before Windows logon can be helpful when users have startup processes that require network connections. This is also a useful tool if your company uses Active Directory or Novell eDirectory as a user database.



NOTE: You must install the Odyssey GINA module to be able to use this type of network connection.

Odyssey GINA is an advanced configuration tool intended for administrators who are familiar with the Windows GINA module and who understand how to use it. The Odyssey GINA module preempts Windows GINA and is intended for use with OAC connection and authentication only.

Using a Third-Party GINA Module Together with Odyssey GINA

To use a third-party GINA module in addition to the Odyssey GINA module, install the Odyssey GINA module *after* you install the third-party GINA module.

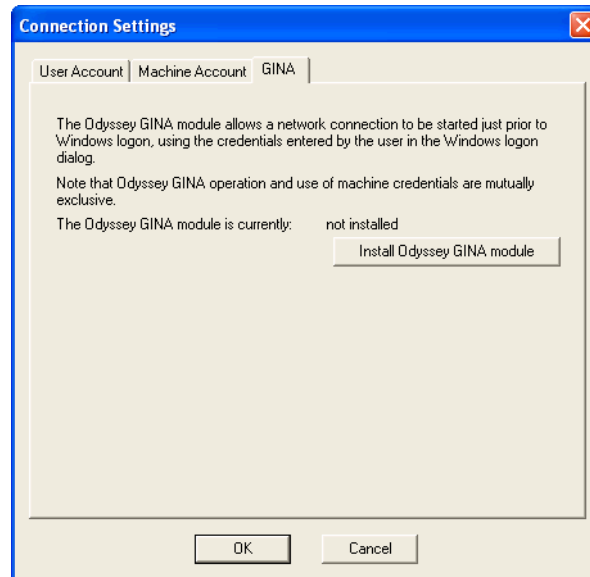
If you install the Odyssey GINA module before installing a third-party GINA module:

1. Remove the Odyssey GINA module using the directions in “Removing the Odyssey GINA Module” on page 15.
2. Install the third-party GINA module.
3. Install the Odyssey GINA module using the instructions in “Installing the Odyssey GINA Module” on page 15.
4. Reboot your computer. The GINA module installation is not complete until you reboot the machine.

Installing the Odyssey GINA Module

Install the Odyssey GINA module from the **GINA** tab on the Connection Settings tool.

Figure 5: GINA Tab of the Connection Settings Tool



To install the GINA module, click the **Install Odyssey GINA module** button in the **GINA** tab of the Connection Settings tool (Figure 5). After you click this button, you can configure prior to Windows logon connection settings under the **User Account** tab of the Connection Settings tool.

Removing the Odyssey GINA Module

To remove the Odyssey GINA module, select the **Remove Odyssey GINA module** button from the **GINA** tab of the Connection Settings tool.

The GINA module removal is not complete until you reboot the machine.

GINA Compatibility with Other Modules Running at Windows Logon

The Odyssey GINA module works by hooking into the Windows GINA module that presents the Windows Logon dialog.

Note the following about the interaction between OAC and other logon modules:

- You might be prompted for credentials by OAC for some applications that replace the Microsoft Windows logon screen.
- OAC is compatible with a number of logon modules, preserving single sign on behavior.
- In the case of Novell Client for Windows, OAC uses your Novell credentials at logon time without prompting for credential information.

Using GINA with Smart Cards

Install the Odyssey GINA module if users authenticate with a profile that has **Permit login using password** selected on the **Password** subtab of the **User Info** tab in the Profile Properties dialog. Install the Odyssey GINA module with smart card use even when users authenticate after Windows logon.

You can configure a prior to Windows logon machine authentication that includes both EAP-TLS with smart card certificates *and* a password-based protocol such as EAP-TTLS. In this case, the authentication method depends on whether the user chooses to use a smart card or a Windows password to log on. The login prompts with both options and the user must select one.

If the user logs on with a smart card, EAP-TLS is the protocol used with the smart card certificate during network authentication requests.

If the user logs on with a Windows password, a password-based protocol such as TTLS is negotiated according to the protocol ordering on the **Authentication** tab of the Profile Properties dialog. See “Using Smart Cards with GINA” on page 69 for information about smart card multi-protocol configuration details.



NOTE: Turning FIPS Mode on disables OAC smart card management.

Restrictions on Early Network Connections

There are no restrictions for user account network connections that occur after the desktop appears. However, there might be restrictions on the features that you can use when you select particular network connection timing options in the Connection Settings tool. Table 3 summarizes the restrictions. A Yes in a column indicates the feature applies for that connection setting, while No indicates that it does not.

Table 3: Early Network Connection Restrictions

Profile or Network Connection Feature	Machine Account at Windows Startup	User Account prior to Windows Logon	User Account After Logon, but Before Desktop
Ad-hoc (peer-to-peer) network connections specified in the network description	Yes	No	Yes
Preconfigured WEP keys used with the network description	Yes	Only when configured from the Initial Settings tool	Yes
Windows password on the profile description	No	Yes	Yes
Machine password on a profile description from a Machine Account profile	Yes	No	No
Prompt for password option on the profile description	No	Yes	No

Table 3: Early Network Connection Restrictions (continued)

Profile or Network Connection Feature	Machine Account at Windows Startup	User Account prior to Windows Logon	User Account After Logon, but Before Desktop
Prompt for PIN option on the profile description (with EAP-SIM or EAP-AKA)	No	No	No
Use the following password option (enter the password) on a profile description	Yes	No	Yes
EAP-TLS option for the profile description	Yes	Only with smart card certificates configured from an Initial Settings profile	Yes
EAP-TTLS/PAP/Token Card option for the profile description	No	Yes	No
EAP-GenericTokenCard option for the profile description	Only when profile is not configured to prompt for token. See “Machine Account Tool” on page 26.	Yes	Only when profile is not configured to prompt for token. See the <i>Odyssey Access Client User Guide</i> .
EAP-FAST configured with the profile description	Only when profile is not configured to prompt for a token. See Chapter 5, “Managing Profiles” in the <i>Odyssey Access Client User Guide</i> .	Yes	Only when configured not to prompt for token. See Chapter 5, “Managing Profiles” in the <i>Odyssey Access Client User Guide</i> .
EAP-POTP configured with the profile description (as an inner or outer EAP method)	Only when profile is not configured to prompt for a token. See Chapter 5, “Managing Profiles” in the <i>Odyssey Access Client User Guide</i> .	Yes	Only when configured not to prompt for token. See Chapter 5, “Managing Profiles” in the <i>Odyssey Access Client User Guide</i> .
Unauthenticated network connections (networks without profiles)	Yes	Only when configured from a network description in the Initial Settings tool	Yes
Preshared WPA or WPA2 passphrase to generate encryption keys configured with the network description	Yes	Only when configured from the Initial Settings tool	Yes
Temporary trust	No	No	No
Clear the Validate server certificate setting.	Yes	No	Yes

Note the following:

- You can configure all of the default user account network settings in the Initial Settings tool. However, the restricted options are not disabled by default in the Initial Settings tool, so be sure to configure the network connection properly.
- Features that apply only when you configure default Windows logon settings in the Initial Settings tool are not available if your users override default Windows logon settings from the **Tools > Windows Logon Settings** menu in the Odyssey Access Client Manager.
- You can configure all of the machine account network settings in the Machine Accounts tool. The restricted options are disabled for you in the Machine Account tool.
- The password, token, and PIN prompt restrictions apply to the listed protocols whenever they are in use (either as inner or outer authentication protocols).

Chapter 3

Configuring Initial Settings

The Initial Settings tool enables an administrator to preconfigure OAC for new users. When a user launches OAC the first time, the Odyssey Access Client Manager displays the predefined settings in the configuration dialogs. You can specify initial settings for any or all OAC Manager configuration options. When you preconfigure OAC, use your own desktop computer or a lab machine to set up the configuration settings. You will save these settings later to an .msi installation file using the Custom Installer tool.

The machine that you use to create the initial configuration must be the same machine that you use to deploy it because you are pushing out the configuration image (settings) from that copy of OAC.

You can also use the Initial Settings tool to define the network connections part of a configuration image for a custom installer or a user settings update file. The Permissions Editor tool and the Merge Rules tool might also factor into the configuration.

With the Initial Settings tool, you can configure any the adapter, user profile, and network settings for connections that take place before Windows logon process begins.

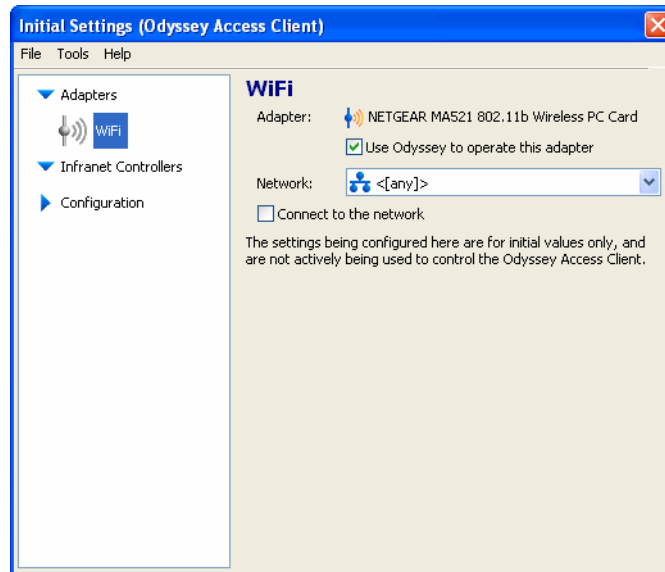
You can also specify how login names appear in user profiles and, if required, specify text that prompts users with a required login name format.

The settings you choose in the Initial Settings tool become the configuration settings for the rules that you select in the Merge Rules tool. Similarly, the rules that you set in the Merge Rules tool apply to those user configurations deployed through custom installers or update files to user machines. See Chapter 6, “Setting Merge Rules” and Chapter 7, “Using the Custom Installer” for more information. You can use the Initial Settings tool to configure features before you apply any merge rules to them.

Using the Initial Settings Tool

To open the Initial Settings tool (see Figure 6), double-click **Initial Settings** in the Odyssey Access Client Administrator.

Figure 6: Initial Settings Dialog



You can preconfigure the following network configuration features in the Initial Settings tool in much the same way that you configure these features in the Odyssey Access Client Manager:

- Profiles—Preconfigure the authentication for this user or for a configuration image to deploy to multiple users.
- Networks—Preconfigure the default networks to which a user can connect.
- Auto-Scan lists—Preconfigure and order the networks for an auto-scan list for this user or for a configuration image to deploy to multiple users.
- Trusted servers—Preconfigure the trusted root CA or intermediate CA certificate in the local machine certificate store of the machine that you use for configuration. Then configure a trusted server in the Initial Settings tool.
- Adapters—Preconfigure wired or wireless adapters for a custom installer file. Users are not required to have exactly the same adapter you have (the names and models can differ), as long as you install a similar type (wired or wireless) of adapter on their client machines.
- Infranet Controllers—Preconfigure the Infranet Controller for this user or for a configuration image to deploy to multiple users.
- Networks—Configure the default networks that are accessible for this user or for a configuration image to deploy to multiple users.

When users run OAC for the first time, they see the settings configured in the Initial Settings tool. You can also use these same settings for:

- A custom installer
- A settings update file



NOTE: Before you create a custom installer or a settings update file, use the Merge Rules tool to specify how the Initial Settings tool configuration applies to updated or new user configurations.

Caution on Overriding Default Windows Logon Settings

The **Tools > Windows Logon Settings** menu in the Odyssey Access Client Manager gives users the option to override the default network connection timing.



NOTE: Do not select **Override default settings for Windows logon** in the Initial Settings tool unless you want to enable users to override the network connection settings you configure in the **GINA** tab of the Connection Settings tool.

If you install the OAC GINA module, users can configure a network connection that takes place before Windows logon. If you do not install the GINA module, users have only the two post-logon connection options available to them through this menu on the Odyssey Access Client Manager.

Users can override default network connection settings that you configure unless you have locked them with the Permissions Editor.

Users cannot override configured trusted servers if their configuration is set up to connect before Windows logon. The only way to change the trust setting for a Windows logon connection is for you (or someone with administrative privileges) to modify those settings in the Trusted Servers dialog of the Initial Settings tool.

Configuring Prior to Windows Logon Connections

When you install OAC on Windows, you can configure automatic network connections that occur when the user logs on to Windows. This can be helpful when users have startup processes that require network connections. You can accomplish this using the OAC Windows logon settings. See Table 3 on page 16 for more restrictions that apply to this type of login connection.

Note the following additional points for any user account connections that you want to configure to occur before Windows logon:

- You must associate a profile and adapter (for wired connections) or a network (or auto-scan list) and adapter (for wireless connections) with a Windows logon configuration. When you configure a prior to Windows logon network configuration, you must select items from the **Network** (or **Profile**) and **Adapter** lists on the **User Account** tab in the Connection Settings tool. The items in these lists reflect the adapters, networks, auto-scan lists, and profiles that you specify in the Initial Settings tool.

- When you are setting up user defaults for your machine or for a new custom installer file, you are not required to associate a profile with any network that you configure in the Initial Settings tool.
- If you select a profile for a network connection that occurs before Windows logon and that uses EAP-TTLS, EAP-TLS, or EAP-PEAP, the server certificate is validated automatically during user authentication.
- OAC uses the user's default logon name. If you specify a name, OAC uses the name that you enter instead of the user's default logon name.
- You cannot assign a profile that uses a stored password. See “Restrictions on Early Network Connections” on page 16 for more information.
- You must install a trusted root CA or intermediate CA in the local machine store in the Trusted Servers dialog of the Initial Settings tool. The trust relationship that you configure must include a certificate authority in the signing chain of the trusted server. If you have not already installed the certificate in the machine store on your machine, you must do so prior to configuring this trust.



NOTE: The OAC logon feature might be incompatible with similar features in other products.

Options for Login Name Format

When you select **Tools > Options** from the Initial Settings tool, you can specify the default login name (or format). This name or format applies to all new OAC users. The default login name option that you specify might require some user input if you specify a custom format. In that case, the user is prompted once for the custom login name.

The resulting user default login name, which can be viewed when the user selects **Tools > Options** from the Odyssey Access Client Manager, applies under the following circumstances:

- The default logon name appears automatically in the **Login Name** field of any new Odyssey Access Client Manager authentication profile the user creates.
- If you preconfigure authentication profiles for deployment to multiple users, you can leave the **Login name** field blank. When a user to whom you deploy the profile runs OAC, the **Login name** field will be populated with the individual user's Windows login name.
- The default logon name is filled in automatically for profiles when a user imports an OAC script that includes a profile with a blank user name. See “Alternatively, you can use a command line interface to export the entire configuration to a script.” on page 49.



NOTE: You do not need the Merge Rules tool to lock the default login name that is used by a custom installer or settings update file. The default login name option that you specify in the Initial Settings tool is automatically used in any custom installer or settings update file.

You can specify the login name format from the Options dialog. Refer to following topics:

- “Specifying a Custom Login Name Format” on page 23—Use this for inserting text to prompt the user with the correct login name format the first time they use OAC.
- “Domain-Decorated or Undecorated Logon Names” on page 24—Use this for specifying the Windows logon name format to use in all profiles.

Specifying a Custom Login Name Format

You can configure a prompt to show users the login name format to use the first time that they run OAC for user authentication. The login name that the user enters is populated automatically for the following profiles:

- All new authentication profiles that the user creates.
- Any authentication profiles that you configure with blank login names for distribution to your users through settings update files and custom installers.

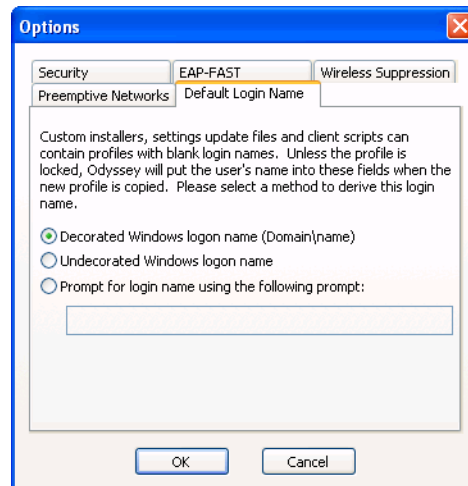
For example, you might require users to use the following format for the login name:

UserName@Domain

To specify instructional text that prompts a new user for a login name when the new user logs in, follow these steps:

1. Select **Tools > Options** from the Initial Settings toolbar. The Options dialog (Figure 7) appears. Select the **Default Login Name** tab.

Figure 7: Default Login Name Options Dialog



2. Select **Prompt for login name using the following prompt**.

3. Enter the appropriate prompt text to instruct users how to enter the login name.
4. Select **OK**.



NOTE: When you specify the login name prompt text, the **Default Login Name** tab appears on the **Tools > Options** menu of Odyssey Access Client Manager. This enables users to modify the default login name that appears in all profiles that they create.

Domain-Decorated or Undecorated Logon Names

To specify the default login name for all user profiles as the domain-decorated or undecorated Windows logon name, follow these steps:

1. Select **Tools > Options**. The Options dialog (Figure 7) appears. Select the **Default Login Name** tab.
2. Select one of the following Windows logon name formats:
 - **Decorated Windows logon name**, to use the default domain-decorated Windows logon name format of *Domain_name\Logon_Name*.
 - **Undecorated Windows logon name**, to use the Windows logon name without any domain name decoration.
3. Select **OK**.

Chapter 4

Setting Up a Machine Account

A machine account configuration is for authenticating a physical machine to a network, rather than the user. It uses either a statically defined user account or the machine credentials that were created when the machine ID was set up in an Active Directory.

A machine account connection is the earliest time that OAC can connect to the network. A machine account is useful for administrative tasks such as nightly backups or update processes that take place whether or not the user is not logged on. It is also used for Active Directory domain policy scripts that run during startup.

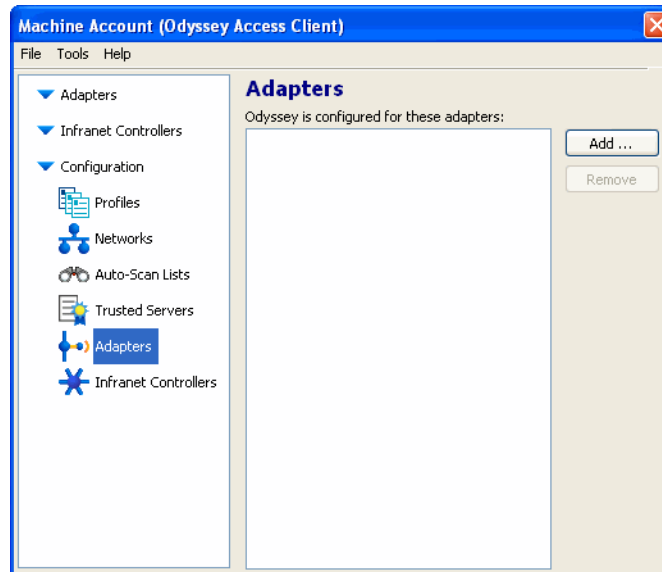
A machine (PC or laptop) has a name and password that is transmitted to the network before the user logs in. With a machine connection enabled, a network IP connection persists even when a user is not logged on, as long as the machine is running.

Machine authentication and user authentication are mutually exclusive. However, you can configure a machine connection to transition to a user-level connection once the user logs on to the network and then resume a machine connection after the user logs out.

Machine Account Tool

To open the Machine Account tool (Figure 9), double-click **Machine Account** in the Odyssey Access Client Administrator.

Figure 8: Machine Account Dialog

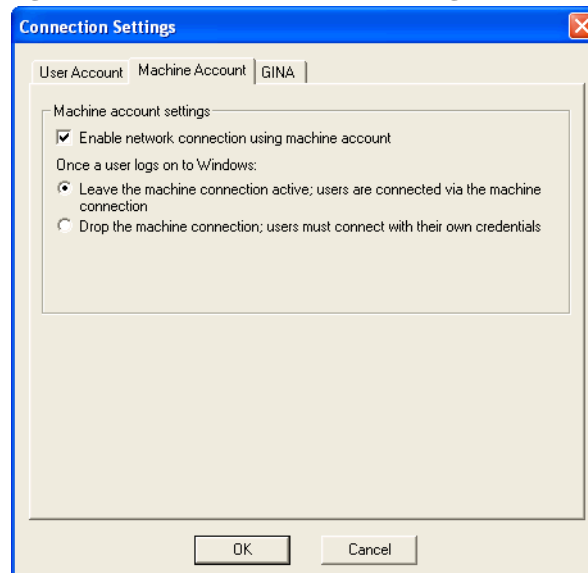


Enabling a Machine Account Connection

To set up a machine account configuration in the Connection Settings tool:

1. Go to the **Connection Settings > Machine Account** tab (Figure 9).

Figure 9: Enable Machine Account Dialog



2. Select **Enable network connection using machine account**.
3. Select **Leave the machine connection active; users are connected via the machine connection**. In this case, the machine account is active even when the user is not logged into Windows.

After you set up a machine-level network connection in the Connection Settings tool, use the Machine Account tool to configure the machine network connection settings for a profile. This type of configuration is similar to how you configure connection settings for Odyssey Access Client Manager.

A machine account can be assigned to a different VLAN from the one set up for a user account. If you configure the machine account to transition to a user account when the user logs in, the IP address for the machine might change because of a different VLAN assignment. Similarly, when the user logs off, if the account is configured to transition back to a machine account, the IP address and VLAN assignments might change back again.

Machine Account Profile Options

You can configure multiple networks, profiles, and adapters for a Machine Account. The only active networks, adapters, or profiles that are used for machine connections are those for which you select **Connect to network** (for wireless connections) or **Connect using profile** (for wired connections) on the Connection dialog of Machine Account.

Setting Machine Account Password Credentials

If you enter a password in a machine account profile and intend to create a custom installer, the credentials that you enter are used by all copies of OAC that use this installer. It is better to enter credentials on each client machine manually if user credentials are required.

Setting Automatic Certificate Selection for EAP-TLS

If you require EAP-TLS for authentication and plan to distribute this configuration to multiple users, select **Use automatic certificate selection** on the profile you use for the machine connection. Refer to the directions in Chapter 5, “Managing Profiles,” in the *Odyssey Access Client User Guide*.

Trust Configuration Requirements for Machine Authentication

Configure a trusted root CA or intermediate CA certificate for a machine connection from the Trusted Servers dialog of the Machine Account tool. Before you do so, make sure that you have the certificate installed in the certificate store on the machine that you use for configuration. See Chapter 9, “Managing Trusted Servers,” in the *Odyssey Access Client User Guide* for information about how to add certificates.

Restrictions for Machine Account Settings

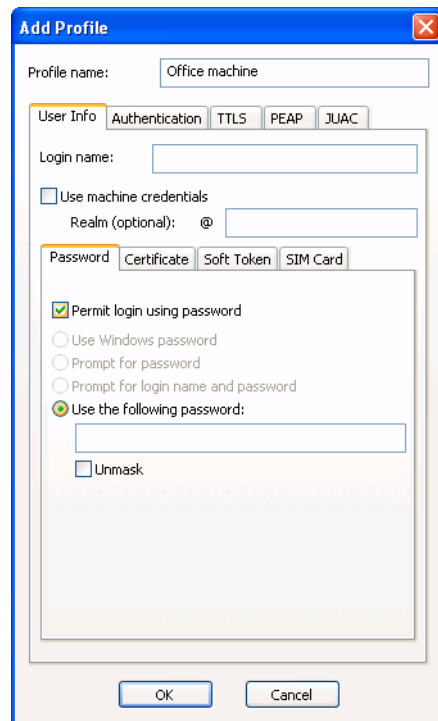
Default login name and EAP-FAST options do not apply for machine account settings nor are authentication methods that require user interaction, such as those associated with tokens. As a result, the Profile Properties dialog in the Machine Account tool varies slightly from that of the Odyssey Access Client Manager.

See “Restrictions on Early Network Connections” on page 16 for all restrictions on machine account connections.

Configuring a Machine Password

You can configure machine credentials (machine name and machine domain password) when authenticating the machine to RADIUS servers that check the machine credentials against an Active Directory listing. The machine credentials are created automatically when the machine joins the domain.

Figure 10: Machine Account Credentials



To use machine credentials for authentication:

1. Create a profile from the Profiles dialog of in the Machine Account tool and select **Use machine credentials** on the **User Info** tab of the Add Profile dialog.
2. If you require that a realm name to decorate the machine credentials, type the name of the realm in the **Realm (optional): @** field (located just below the **Use machine credentials** field). Otherwise, leave this field blank.

You might require a realm name decoration if the RADIUS authentication server is set up to support RADIUS proxies.

3. Keep **Permit login using password** selected.

EAP Methods that Support Machine Credentials

Machine credentials are valid only with EAP-TTLS or EAP-PEAP. Select at least one of these authentication methods for the profile. Then configure the authentication options on the **TTLS Settings** tab or **PEAP Settings** tab of the Profiles Properties dialog, as necessary. See Chapter 5, “Managing Profiles,” in the *Odyssey Access Client User Guide* for information about selecting authentication protocols for a machine account profile.

Chapter 5

Using the Permissions Editor

The Permissions Editor tool lets you select or disable individual OAC features, thereby controlling which features users can access or modify.

Use this tool when you are setting up a predefined configuration to deploy to multiple users. For example, you might want to enable users to create new profiles but restrict the available authentication protocols to EAP-TTLS, EAP-PEAP, and EAP-FAST. Similarly, you might want to restrict access to other features such as the Odyssey Access Client Administrator or license keys. This tool helps you to set up OAC to conform with your network security policies by “locking” specific configuration settings.

The categories of features that you can control in the Permissions Editor include:

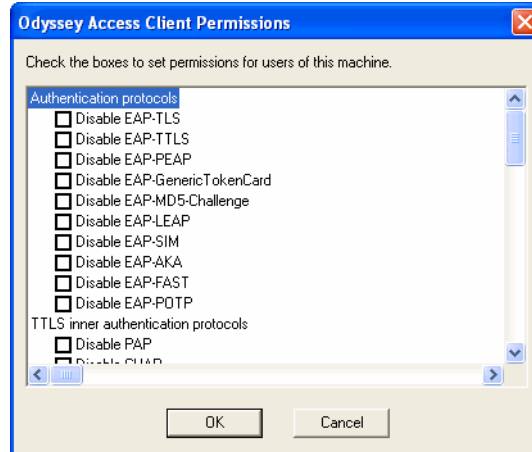
- Authentication protocols
- TTLS inner authentication protocols
- TTLS inner EAP protocols
- PEAP inner authentication protocols
- Profile properties
- Options (temporary trust)
- Network properties
- User interface settings

The settings that you configure in the Permissions Editor tool are applied automatically to your current machine—the machine that you are using to preconfigure OAC for deployment. You can also create a file to export the permission configuration to a one or more users. See “Configure OAC Updates for Mass-Distribution to Users” on page 68.

Permissions Editor Tool Settings

To set up permission/restrictions for individual configuration settings, double-click **Permissions Editor** in the Odyssey Access Client Administrator to open the Permission Editor management interface (see Figure 11).

Figure 11: Permissions Editor Tool



To restrict permissions for Odyssey Access Client Manager features:

1. Select the features that you want to restrict user from seeing or modifying by selecting the check box next to the feature. Some features, such as the Odyssey Access Client Administrator, do not appear in Odyssey Access Client Manager if they are disabled.
2. When you select the features to restrict, select **OK**.

To remove a restriction, select the check box again so that the check mark no longer appears.

Note the following:

- Any features that you restrict (lock) in the Merge Rules tool are exempt from constraints that you configure in the Permissions Editor Tool Settings.
- Features or options that you restrict might remain visible to your users, even though they cannot configure or use them.
- If you select **Disable [any] networks**, users cannot connect to unspecified networks using the **[any]** network feature. See Chapter 6, “Managing Network Access,” of the *Odyssey Access Client User Guide* for a description of this feature.
- If you select **Disable ad-hoc networks**, users cannot make peer-to-peer connections.

- If you select **Remove Odyssey Client Administrator from Settings menu**, users cannot access the Odyssey Access Client Administrator from the Odyssey Access Client Manager. Thus, you can restrict access to Odyssey Access Client Administrator which is usually available to users in the EE and FE licenses.
- If you select **Remove License Keys from Help menu**, users cannot modify or view license keys.
- If you select any of the **Disable unauthenticated** options, users cannot create a network configuration using the specified encryption protocol if they do not assign a profile to the network connection. The **Disable unauthenticated clear connections** option applies to network descriptions configured for no encryption (**none** is selected as the encryption method on the Network Properties dialog).
- If you select any of the **Disable authenticated** options, users will not be able to create a network configuration using the specified encryption protocol when they assign a profile to the network connection.

See “Configure OAC Updates for Mass-Distribution to Users” on page 68 for information about applying permission restrictions to user configurations.

Chapter 6

Setting Merge Rules

Use the Merge Rules tool to control and manage how OAC configuration settings apply for one or more users. Configuring merge rules enables you to add, set, or lock features that you configure in the Initial Settings tool that have to do with authentication profiles, networks, auto-scan lists, Infranet Controllers, and other options.

The settings that you configure in the Merge Rules tool are applied to user configurations when use custom installers or update files to deploy them to users. This tool offers flexibility in how you apply preconfigured settings. For example, you can add new authentication profiles or Infranet Controllers to existing user configurations only if the user does not have those settings already. You can replace current profile configurations with updated settings and even lock them so that they cannot be modified by users.

For networks that include Infranet Controllers, this tool lets you add, update, and lock Infranet Controller configurations for your network users. The Merge Rules tool helps to maintain the transparency of OAC administration and configuration to your users.

How Merge Rules Apply to User Configurations

Merge rules apply to user configurations in the following ways:

- They can apply to any user of any machine for which merge rules have been configured.
- They can apply to configurations for any machine to which you use the Custom Installer tool to apply a settings update file.

Use Cases for Merge Rules

The following situations describe sample use cases in which you might configure rules for using your OAC Administrator configuration to update current user configurations.

- You can provide periodic OAC updates to a group of users and their machines.
- You can add new Infranet Controllers to user configurations. You might also want to lock an Infranet Controller or the corresponding profile configuration, particularly if users are required to connect to a specific Infranet Controller.

- You can create a new custom installer file to upgrade users with a newer version of OAC. Merge rules enable you specify how features are merged into existing user configurations.
- You can create a new custom installer file for configuring OAC for new machines. In this case, you have the option to lock the configured features as they are installed on a new machine using the Merge Rules tool. (The default setting is to enable all configuration settings.)

Merge Rule Settings

You can control the current the Initial Settings configuration for all users of your current machine (or to a new custom installer file or to a configuration update file). Select one of the following modes:

- **None**—Configure settings for new users of a given client PC on your network based on selected items that you configure in the Odyssey Access Client Administrator. This is the default for some items on the **Other** tab (described in “Merge Rules Settings in the Other Tab” on page 41). You could use this mode, for example, if you have recently updated your license and you want to update a configuration for all new user settings on client machines with settings for the latest features. This mode has no effect on the configurations of current users of an OAC installation. After a user begins to use OAC, the user can modify any of these settings.
- **Add if not present**—Add selected Odyssey Access Client Administrator settings to the current settings of your users without overwriting settings with the same names. This is the default option for all tabs of the Merge Rules tool except for some items on the **Other** tab, for which this option is not available. This mode affects the configurations for new users, as well as current users of your OAC installations. All users are able to modify these settings.
- **Set, replace if present**—Add selected Odyssey Access Client Administrator settings to the current settings of your users and overwrite settings with the same names if they already exist. This mode affects the configurations for new users as well as current users of your OAC installations. All users are free to modify these settings.
- **Lock except user info**—Overwrite all current user settings with selected Odyssey Access Client Administrator settings, except for user credential information (username, password, or user certificate) associated with a profile. This option is only available for profiles. This prevents your users from editing any portions of a locked profile except for their credentials. Do not fill in the username and password or user certificate for any profile that you create in the Initial Settings tool to which you plan to apply this type of profile locking.
- **Lock**—Set or overwrite all current user settings with selected Odyssey Access Client Administrator settings and prevent your users from editing them. When you lock a feature, OAC deletes all current user settings for features with the same name and prevents new and current users from editing this feature. Users of Odyssey Access Client Manager see one of the following indicators for locked features:

- Title bars of dialogs are marked as read-only if every feature shown on the dialog is locked.
- Information text that appears on a tab of a dialog indicates that the features on the selected tab are locked.

The settings that you make in Merge Rules affect settings for all users of the machine that you are configuring. The changes take effect as soon as you close Merge Rules. You can then use these merge rules when you provide configuration updates to your users or when creating a new installer file.

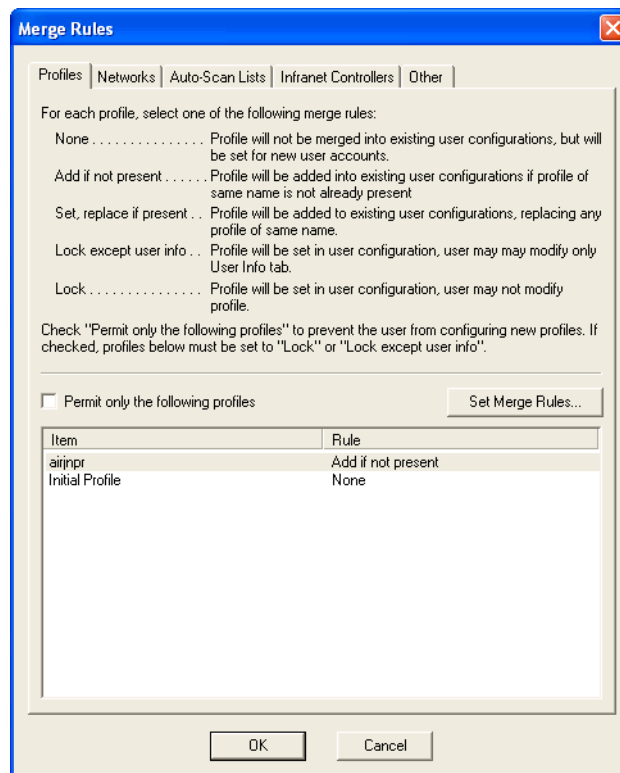
Merge Rules Tool Overview

Use the Merge Rules tool to assign rules for applying the initial settings and Windows logon configuration to the current machine or to a configuration file you create in Custom Installer. Merge rules apply to the following categories of user configuration settings:

- Profiles
- Networks
- Auto-scan lists
- Infranet Controllers
- Other Merge Rules for Profiles

To set merge rules for a profile:

1. Double-click **Merge Rules** in the Odyssey Access Client Administrator. The Merge Rules tool (Figure 12) appears.

Figure 12: Merge Rules Tool

2. To lock one or more profiles, select the **Profiles** tab. (Similarly, to lock networks, auto-scan lists, or Intranet Controllers, select the appropriate tab in the dialog.)
3. Select **Permit only the following profiles** to lock all profiles listed. This option affects configurations as follows:

- Users can use only the profiles that you configure through the Initial Settings tool.
- All options (aside from user credentials) for all user profiles are locked.
- Users cannot add new profiles to their configurations.
- Users can edit their credentials for each of the locked profiles that you configure.
- Profiles configured previously are hidden from users and are disabled.

To make these visible to your users, clear **Permit only the following profiles**.

- If, in addition to locking all profiles, you want to lock user credentials for one or more of these locked profiles, select the profiles whose user credentials you want to lock, use the mouse button to select **Lock**.

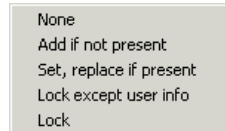
4. Select **OK**.

Setting Merge Rules for Profiles

To set merge rules for one or more profiles, follow these steps:

1. Use the right mouse button to select one or more profile configurations from the list, select a profile, and select **Set Merge Rules**. A context menu (Figure 13) listing all available merge modes appears.

Figure 13: Context Menu for the Merge Rules Tool



2. Select one of the five configuration modes (**None**; **Add if not present**; **Set, replace if present**; **Lock except user info**; **Lock**) from the menu.
3. Repeat these steps for as many of the other merge rule modes that you want to apply to any profile(s) that you configure in the Initial Settings tool.

Setting Merge Rules for Networks

To set merge rules for a network configuration:

1. Select the **Networks** tab of the Merge Rules tool. You can lock all networks or set merge rules for individual networks:
2. Select **Permit only the following networks** to lock all networks listed. When you do so, the following changes apply:
 - Users can use only those networks configured with the Initial Settings tool.
 - All components of all user networks are locked.
 - Users cannot add new networks to their configurations.
 - Any networks that were configured previously in OAC are hidden from your users and disabled. The only way to make these visible to your users again is to clear **Permit only the following networks**.

Setting Merge Rules for Individual Networks

To set merge rules for one or more networks

1. Select one or more network configurations from the list.
2. Select one of the configuration modes from the context menu that appears:
 - **None**
 - **Add if not present**
 - **Set, replace if present**
 - **Lock**



NOTE: Lock any networks for which FIPS mode is required. **(FE Only)**

3. Repeat this step for as many of the other merge rule modes that you want to apply to any network(s) that you configure in the Initial Settings tool.
4. Select **OK**.

Setting Merge Rules for Auto-Scan Lists

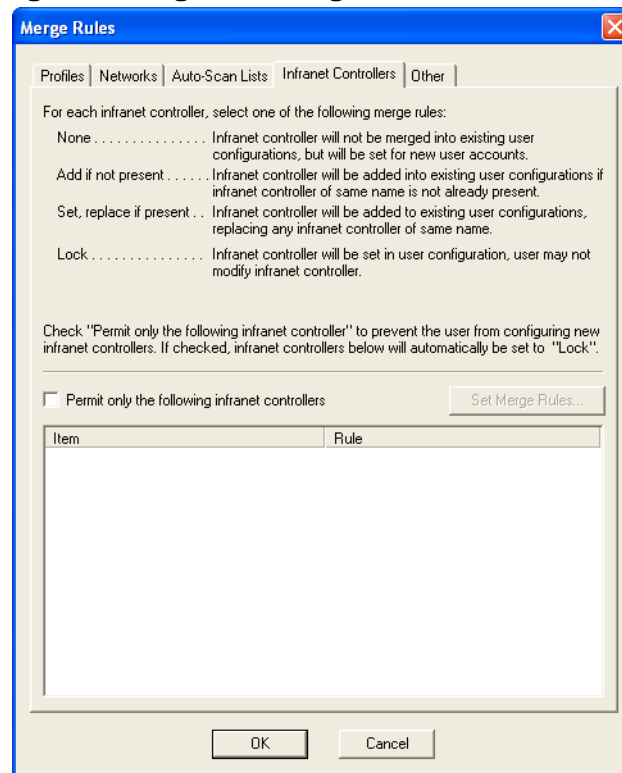
To set merge rules for auto-scan lists:

1. Select the **Auto-Scan Lists** tab of the Merge Rules tool. You can lock all auto-scan lists or set merge rules for individual auto-scan lists.
2. Select **Permit only the following auto-scan lists** to lock all auto-scan lists. The consequences of locked auto-scan lists are as follows:
 - Your users can use only the auto-scan lists that you configure through the Initial Settings tool.
 - All components of all user auto-scan lists are locked.
 - Users cannot add new auto-scan lists to their configurations.
 - Any auto-scan lists that were configured previously in OAC are hidden from your users and disabled. To make these visible to your users again, clear the setting for **Permit only the following auto-scan lists**.
 - To set merge rules for one or more individual auto-scan lists, select one or more auto-scan lists from the list. Use the right mouse button to select one of the four configuration modes (**None**; **Add if not present**; **Set, replace if present**; **Lock**) from the menu that appears. Repeat this step for as many of the other merge rule modes that you want to apply to any auto-scan list(s) that you configure in Initial Settings tool.

Setting Merge Rules for Infranet Controllers

To set merge rules for Infranet Controllers:

1. Select the **Infranet Controllers** tab of the Merge Rules tool (see Figure 14). You can lock all Infranet Controllers or set merge rules for individual Infranet Controllers.

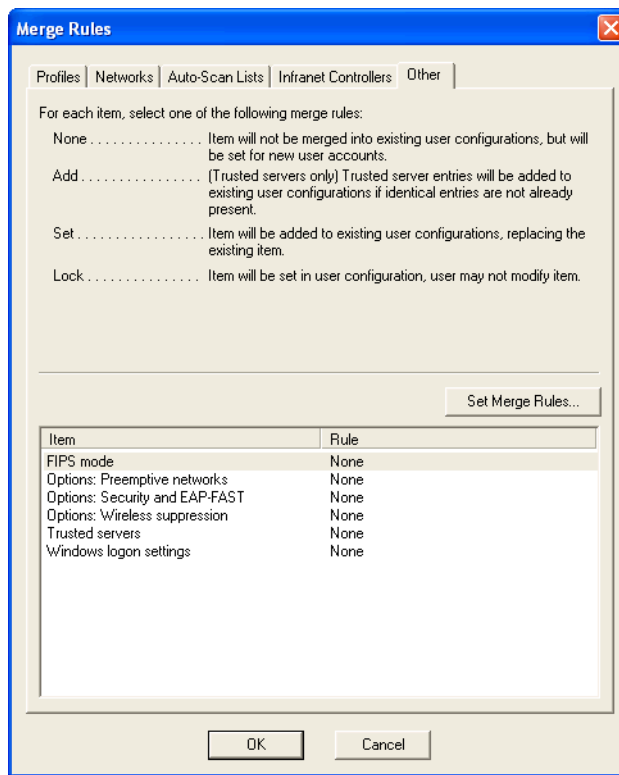
Figure 14: Merge Rules Dialog for Infranet Controllers

2. Select **Permit only the following Infranet Controllers** to lock all Infranet Controllers. The consequences of locked Infranet Controllers are as follows:
 - Your users can use only the Infranet Controllers that you configure through the Initial Settings tool.
 - All components of all Infranet Controllers are locked.
 - Users cannot add new Infranet Controllers to their configurations.
 - Any Infranet Controllers that were configured previously in OAC are hidden from your users and disabled. To make these visible to your users again, clear the setting for **Permit only the following auto-scan lists**.
3. Select **OK**.

Merge Rules Settings in the Other Tab

To set Merge Rules for the settings under the **Other** tab, select the **Other** tab of the Merge Rules tool (Figure 15).

Figure 15: Merge Rules Dialog for Other Settings



You can use this tab to assign configuration update rules for the following:

- Security and EAP-FAST options that you configure from the Options dialog that appear when you select **Tools > Options** in Initial Settings tool. See the *Odyssey Access Client User Guide* for information about these settings. Select **Options: Security and EAP-FAST** for this option.
- Wireless suppression options that you configure from the Options dialog that appear when you select **Tools > Options** in Initial Settings tool. See the *Odyssey Access Client User Guide* for information about these settings. Select **Options: Wireless Suppression** for this option.
- Trusted servers that you configure in Initial Settings tool. See the *Odyssey Access Client User Guide* for information about configuring trusted servers.

Note the following about trusted servers:

- You can also select **Add** for trusted servers. In this case, you can add trusted server entries to an existing list of trusted servers if they are not present.
- When you set or lock trusted servers, you replace the entire trust tree for all users.
- When you lock trusted servers, your users cannot modify the trust that you configure.

- **(FE Only)** FIPS mode settings that you configure in the Initial Settings tool. See the *Odyssey Access Client User Guide* for information about these settings. If you require FIPS mode connections in your network, it is recommended that you set **FIPS Mode On** in the Initial Settings tool and lock **FIPS mode** in the Merge Rules tool, so that all user connections attempt to connect in FIPS mode.
- Windows logon settings that you configure in Initial Settings. See the *Odyssey Access Client User Guide* for information about the Windows logon settings.

For each of these items, use the right mouse button to select one of the three configuration modes (**None**; **Set, replace if present**; **Lock**) from the menu that appears.

See “Configure OAC Updates for Mass-Distribution to Users” on page 68 for information about applying your merge rules to a set of users.



NOTE: A warning or error message might appear when you select **OK** to close the Merge Rules tool. For example, if you attempt to assign an invalid merge rule, an error message appears. These error messages contain helpful information to address merge rule errors or inconsistencies.

Chapter 7

Using the Custom Installer

You can distribute the preconfigured settings that you define with the Initial Settings, Machine Account, Permissions Editor, and Merge Rules tools to your users as:

- A preconfiguration to new users and machines.
- Updated OAC configurations for existing users and machines.
- License updates.

The preconfigured settings can be distributed as a Microsoft installer (.msi) file for a new installation or as a settings update file.

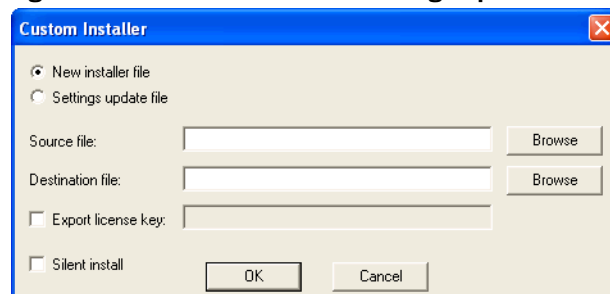
Use the Custom Installer to create an .msi file to deploy the configuration template to client machines. An .msi file can contain any configuration options defined using Initial Settings, Machine Account, Permissions Editor, and Merge Rules tools. The .msi file can contain the OAC license key.

You can also configure the custom installer file to install “silently”—without requiring interaction by the client system user.

Custom Installer Tool

Double-click **Custom Installer** in the Odyssey Access Client Administrator. The Custom Installer dialog (Figure 16) appears.

Figure 16: Custom Installer and Settings Update File Tool



Using the Custom Installer

Use the installer file to upgrade current user configurations or to create installers for new client machines. You can also configure custom updated user configuration files. Custom installer files and updated user configuration files derive their configuration from the features you set in the Odyssey Access Client Administrator, and not in the Odyssey Access Client Manager.

After configuring and testing your custom installer template in the Odyssey Access Client Administrator, you can double-click **Custom Installer** in the Odyssey Access Client Administrator to create a new OAC installer file with the defaults that are configured from your template.

For information about using your current Odyssey Access Client Administrator configuration to create an updated user configuration file, see “Configure OAC Updates for Mass-Distribution to Users” on page 68.

Use cases for the customer install process are described in Chapter 10, “Administrative Workflows.”

Creating a Custom Update File

A settings update file contains the configuration template settings. The difference between a settings update file and a new installer file is that the new installer file also contains the software for installing OAC.

To create a custom installer update file:

1. Select **Settings update file**.
2. Specify the source installer (.msi) file. Enter the file name (and path) or select the top **Browse** button. The **Select Source File** dialog appears.
3. Use the **Files of type** drop-down list at the bottom of the Select Source File dialog to search for the correct file type. You can use the original OAC installer file from any current or previous release (**OdysseyClient.msi**) as the source file. Locate this file in the **Client** directory on the product CD if you have not archived it. Double-click the source file in the window or select **Open**.
4. Select **Browse** to browse for the desired destination directory if required. The Save Destination File dialog appears. Select the name of the new (destination) .msi file. Enter the name of the file or select an existing file in the current directory, and then select **Save**.
5. Optionally, select **Export license key**, and enter a license key that is valid for the number of copies that you intend to distribute.
6. Optionally, select **Silent install** if you want the installation to run without displaying any dialogs during the install process. Note that if you select this option and you do not export a license key, the license for the installed product expires in 30 days.
7. Select **OK** to create the custom installer file.

Creating an Installer File

To create an installer file:

1. Select **New installer file**.
2. Specify the source installer (.msi) file. This file must be a full product installer file for OAC. You can enter the file name (along with its path) or select the top **Browse** button. The **Select Source File** dialog appears.

Use the **Files of type** drop-down list at the bottom of the Select Source File dialog to search for the correct file type. You can use the original OAC installer file from any current or previous release (**OdysseyClient.msi**) as the source file. Locate this file in the **Client** directory on the product CD if you have not archived it. Double-click your source file in the window or select **Open**.

3. Select **Browse** to browse for the desired destination directory if required. The Save Destination File dialog appears. Select the name of the new (destination) .msi file. Either enter the name of the file or select an existing file in the current directory, and then select **Save**.
4. Optionally, select **Export license key**, and type in a license key that is valid for the number of copies you intend to distribute.
5. Optionally, select **Silent install** if you want the installation to run without displaying any dialogs during the install process. Note that if you select this option and you do not export a license key, the license for the installed product expires in 30 days.
6. Select **OK** to create the custom installer file.



NOTE: All locking rules that you specify in the Merge Rules tool apply to new custom installer files. If you select the **Settings update file** option of the Custom Installer, you can create a configuration file that includes administrative updates from the merge rules and permission restrictions you configure in the Merge Rules and Permissions Editor tools. You cannot use settings updates for new installers or for version upgrades, however. See “Configure OAC Updates for Mass-Distribution to Users” on page 68.

Chapter 8

Using Scripts

The Script Composer Tool is a delivery mechanism for distributing configuration updates to a group of users. The updates apply to networks, profiles, and auto-scan lists. After you have set up and deployed an initial configuration using the Custom Installer tool, the Script Composer tool lets you update network connection settings. You can use a single script to distribute updates for profiles, networks, scan-lists. The data format of a script is XML.

The Script Composer Tool uses the Odyssey Access Client Manager settings on the machine where those settings have been configured.

You can also use scripts to modify settings for trusted servers, security and EAP-FAST, wireless suppression, preemptive networks, and Windows logon timing settings.

Script Composer Options

The types of controls you can exercise with scripts are:

- Add settings that are not currently defined in the user configuration. Those updates are applied when the script runs—only if the user's configuration does not have components with the same name. The configuration settings that you can select to add must be ones that are in the copy of OAC on your local machine.
- Set or replace current settings. The configuration settings that you can select to add or replace must be ones that are in the copy of OAC on your local machine.
- Remove any configuration settings. The settings do not have to be part of the configuration on your local machine.
- Enable automatic connections. You select a profile for a wired connection or a network or auto-scan list for a wireless connection. The adapter used is the first appropriate adapter configured in OAC for the user.

Alternatively, you can use a command line interface to export the entire configuration to a script.

If a configuration setting imported to a client machine in a script has the same name and type as a setting that is currently locked on the client configuration (see “Permissions Editor Tool Settings” on page 32), the setting defined in the script will be stored in the Windows Registry but actually updated in the client as long as that setting remains locked. Once the setting is unlocked, the values that you imported in the script become visible and take effect. This situation might occur if the user has access to the Odyssey Access Client Administrator and has locked some settings locally.

Once you create and distribute a script file, users can access this script from the **Commands > Check New Scripts** menu command on the Odyssey Access Client Manager. See “Creating Scripts for Incremental Updates” on page 65 for more information.

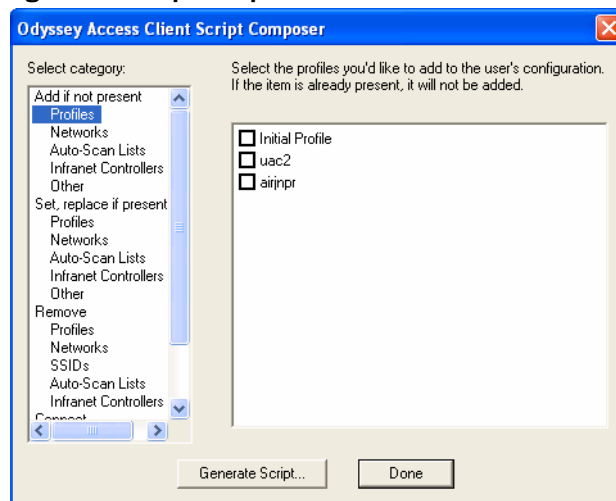
After you distribute a script file, users can access the script from **Tools > Configuration Scripts > Check New Scripts** on the Odyssey Access Client Manager. See “Creating Scripts for Incremental Updates” on page 65 for more information.

Creating Scripts with Script Composer

To create scripts with Script Composer:

1. Set up the configuration template to include the configuration components that you want to add or modify. See the *Odyssey Access Client User Guide* for more information about the individual configuration settings.
2. Double-click **Script Composer** in the Odyssey Access Client Administrator. The Script Composer dialog (Figure 17) appears.

Figure 17: Script Composer Tool



3. For each script that you want to generate, configure all items that you want to add, remove, or modify using the Connection Settings, Initial Settings, Permissions Editor, and Merge Rules tools (as needed).
4. Select **Generate Script**. The Select Destination File dialog appears.

5. Specify the file format for your script. You can save scripts in one of two formats:
 - To save your script as an autoscript so that OAC executes the script transparently, select the `.odyClientScriptAuto` file type.
 - To save your script so that your users have the choice of running the script, select the `.odyClientScript` file type.
6. Enter a name for the file after selecting a file type.
7. Select **Save**.
8. Select **Done**.
9. Put the scripts in the correct directory on your users' machines. See "Creating Scripts for Incremental Updates" on page 65.

Adding or Setting Profiles with Scripts

You can add and/or set any number of profiles that you have configured in Odyssey Access Client Manager in the same script.

To add or set profiles, follow these steps:

1. Select **Profiles** under the action category (**Add** or **Set**). All profiles that you configured in Odyssey Access Client Manager appear listed on the right.
2. Select all of the profiles that you want to include in this action category.
3. Select **Done** when you have made your changes.

Note the following:

- If you include user identity information in your selected profiles (names and/or passwords), these are conveyed to the users who run the resulting script. Passwords are encrypted.
- If you leave the user identity information in your selected profiles blank, then OAC attempts to replace the name and/or password with the user's Windows identity when the script is run. If this is not possible, the user is prompted for identity credentials the first time the user connects to the network OAC.
- Certificate information is not passed on through the script.

Removing a Profile

You can remove any profiles that your users have configured as long as you have the names of the profiles that you want to remove.

To remove a profile, follow these steps:

1. Under **Remove**, select **Profiles**.
2. Enter the name of any profile you want to remove in the text area provided.

Activating a Profile for a Wired Connection

To activate a profile for OAC wired connections:

1. Select the profile under **Connect**.
2. Select **Done**.

Adding or Setting Networks with Scripts

You can add or set (replace if present) one or more networks that you have configured in Odyssey Access Client Manager in the same script.

To add or set networks, follow these steps:

1. Select **Networks** under the desired category (**Add** or **Set**). All networks that you have configured in Odyssey Access Client Manager appear listed on the right.
2. Select all of the networks that you want to include in this category.
3. Select **Done** when you have made your changes.

Removing a Configured Network

You can remove any networks that your users have configured as long as you have the correct names (SSIDs) and corresponding descriptions. Alternatively, you can remove all networks with the same SSIDs, and you do not have to separately specify each of the descriptions.

You can remove any configuration components. You do not have to configure components to be removed in OAC Manager. Components whose names you enter for removal by a script are removed from the user configuration when the resulting script is run.

To remove one or more networks, follow these steps:

1. Select **Networks** under **Remove**.
2. Enter the name (SSID) and corresponding description (if there is any) of the network that you want to remove in the text area provided. You must use the special network description syntax that appears on Odyssey Access Client Manager. You must provide the name/description pair in the following format:

description SSID

3. To enter additional networks to remove with this script, press Enter after typing the name and description of each network you want to remove.

You can remove only those networks with descriptions that do not contain angled brackets in their definitions. Use Removing Networks Using SSIDs to remove networks in this case.

4. Select **Done** when you have made your changes.

Activating a Network for a Wired Connection

To activate a network for OAC wireless connections:

1. Select the network under **Connect** in Script Composer.
2. Select **Done**.

Adding or Setting Auto-Scan Lists

To add or set auto-scan lists that you configured in Odyssey Access Client Manager, follow these steps:

1. Select **Auto-Scan Lists** under the category (**Add** or **Set**) in Script Composer. All auto-scan lists that you have configured in Odyssey Access Client Manager appear listed on the right.
2. Select all of the auto-scan lists that you want to include in this category.
3. Select **Done**.

Removing Auto-Scan Lists

To remove one or more auto-scan lists:

1. Select **Auto-Scan Lists** under **Remove**.
2. Enter the name of any auto-scan list that you want to remove in the text area provided.
3. To enter additional names of auto-scan lists to remove with this script, press **Enter** after typing the name of each auto-scan list that you want to remove.
4. Select **Done**.

To activate an auto-scan list to be used for OAC wireless connections, select the auto-scan list under **Connect** in Script Composer.

Managing Other Setting with Scripts

Depending on which Script Composer action categories you select (**Add** or **Set**), you have one or more options for modifying trusted servers and security settings.

You can create a script to replace trusted servers, Windows logon settings, and Adding or Setting Other Options in the Script Composer Tool if you select **Other** in Script Composer.

Adding or Setting a Trust Tree

To add or set the complete trust tree that you configured in the Trusted Servers dialog of Odyssey Access Client Manager:

1. Select **Other** under the action category (**Add** or **Set**) in Script Composer.

2. Select **Trusted servers**. Note that when users run the resulting script for trust trees that you *add*, new trust entries are spliced into an existing tree. When users run the resulting script for trust trees that you *set*, the entire trust tree is replaced.
3. Select **Done**.

Replacing Options Settings

To set (replace) the options settings that you configured in **Tools > Options**:

1. Select **Other** under **Set** in Script Composer.
2. Optionally, select **Options > Security** and **EAP-FAST** to include settings that you configure on the **Security** and **EAP-FAST** tabs of the **Tools > Options >** dialog in Odyssey Access Client Manager.
3. Optionally, select **Options > Wireless suppression** to include settings that you configure on the **Wireless Suppression** tab of the **Tools > Options >** dialog in Odyssey Access Client Manager.
4. Optionally, select **Options > Preemptive networks** to include settings that you configure on the **Preemptive Networks** tab of the **Tools > Options >** dialog in Odyssey Access Client Manager.
5. Select **Done**.

Removing Networks Using SSIDs

You can remove networks by SSID, rather than by using network name/description syntax. When a user runs the script that removes one or more SSIDs, all networks with the specified SSIDs are removed from the user's OAC configuration.

To remove one or more networks by SSID, follow these steps:

1. Select **SSID** under **Remove**.
2. Enter the SSID of a network that you want to remove in the text area provided. You are not required to use any special syntax.
3. To enter additional names of SSIDs to remove with this script, press **Enter** after specifying the name of each SSID you want to remove.
4. Select **Done**.



NOTE: To remove several network descriptions that specify the same SSID, it is easier to use the **SSIDs** category for removal of all networks with this SSID, rather than entering each network separately in the **Networks** category in Script Composer.

Setting or Replacing FIPS Options (FE Only)

You can set or change the **FIPS Mode** setting for users in Initial Settings.

To select or clear FIPS Mode for users:

1. Open the Initial Settings tool.
2. Under the File menu option, select **FIPS Mode On** or **FIPS Mode Off**.

Chapter 9

Using PAC Manager

Protected Access Credentials (PAC) are used to perform mutual authentication with an ACS authentication server during EAP-FAST authentication. PACs have a randomly-generated encryption key to set up a TLS tunnel and are used instead of certificates.

Consult your ACS documentation for discussions of Protected Access Credentials and how they are created and provisioned on the server.

If you are not using a Cisco ACS authentication server, skip this chapter.

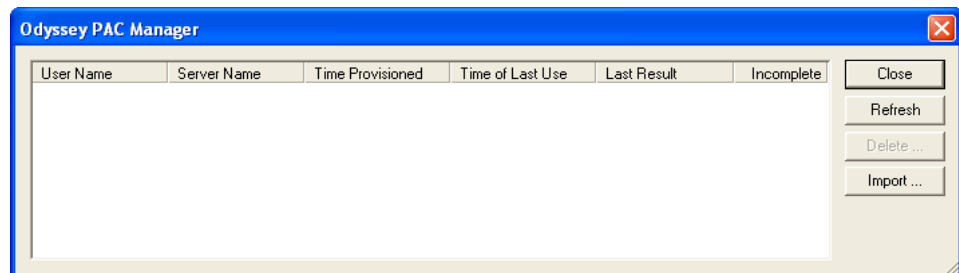
Using PAC Manager to Provision PACs to Clients

Use the PAC Manager tool to provision PACs manually for use with EAP-FAST authentication.

Using the PAC Manager Tool

To open the Odyssey PAC Manager tool (Figure 18), double-click **PAC Manager** in Odyssey Access Client Administrator.

Figure 18: PAC Manager Tool



Importing a PAC

To import a PAC:

1. Select **Import**.
2. When the **Open** dialog appears, browse for the directory containing the PAC file and double-click it to import.

If the PAC file that you select is protected by a password, specify a valid password when prompted.

Refreshing the Pac Manager Display

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

Deleting a PAC

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

Exiting from the PAC Manager

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

Chapter 10

Sample Administrative Workflows

This chapter presents a series of common administrative tasks and provides the workflow steps for accomplishing them. These tasks require familiarity with the OAC Manager and the Odyssey Access Client Administrator.

Sample Administrative Workflows

Several types of configuration tasks require using the Odyssey Access Client Administrator:

- “Specifying a Custom Login Name Format” on page 23.
- “Domain-Decorated or Undecorated Logon Names” on page 24.
- “Testing Configuration Settings” on page 60.
- “Preconfiguring OAC for a Group of Users” on page 61.
- “Configuring User Authentication with No Machine Connection” on page 63.
- “Configuring Machine Connections that Switch to User Authentication” on page 64.
- “Configuring User Authentication with No Machine Connection” on page 63.
- “Creating Scripts for Incremental Updates” on page 65.
- “Command-Line Code to Create and Load OAC Manager Scripts” on page 67.
- “Configure OAC Updates for Mass-Distribution to Users” on page 68.
- “Using Smart Cards with GINA” on page 69.
- “Configuring Single Sign On for TTLS or PEAP” on page 71.
- “Configuring Required FIPS Mode Connections (FE Only)” on page 73.

Testing Configuration Settings

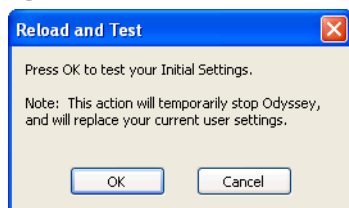
You can test your configuration for user and machine connections before creating a custom installer.

Testing User Connection Settings

To test your user connection settings, follow these steps:

1. Open the **Initial Settings** tool.
2. Select **Tools > Reload and test user defaults** from the Initial Settings tool.

Figure 19: Reload and Test Dialog



3. Select **OK**. This permanently deletes your current OAC Manager settings and loads your settings from the Initial Settings tool into the OAC Manager. It then starts the OAC Manager through the **Configure and Enable Odyssey Access Client Wizard**. Whatever you see in this wizard is what your users see when they first use the product.
4. Test all the connections through the Connection dialog of OAC Manager. Note that any modifications that you make in the OAC Manager are not reflected in the Initial Settings tool.
5. Return to the Initial Settings tool to correct any connection problems and retest these connections, as necessary.



NOTE: This test replaces any settings that you configured in OAC Manager with settings from OAC Administrator.

Testing Machine Connection Settings

To test your machine connection settings:

1. Make sure that the network connections that you want to test are configured and set for connection in the Connection dialog of Machine Accounts. See the *Odyssey Access Client User Guide* and “Configuring User Authentication with No Machine Connection” on page 63 for configuration information.
2. Select the **Machine Accounts** tab in Connection Settings.
3. Select **leave the machine connection active**.
4. Select **OK**.

5. Double-click the system tray icon to open the OAC Manager, and select the status of your connection(s).
6. Return to Machine Accounts to correct any connection problems and retest these connections again, if necessary.
7. If you modified your connection settings, select the **Machine Accounts** tab in Connection Settings and restore the previous settings.

Preconfiguring OAC for a Group of Users

You can preconfigure profiles and networks for a group of users by creating a custom installer.

You can create a customized installer that is based on a configuration that defines settings to be used by a group of new users. The configuration settings that you create with the custom installer define a configuration that you can deploy to users. Each copy of OAC that you install with this customized installer has a default network configuration.

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

For those users who do not require a new installation of OAC, you can use the same settings to update their configurations. See “Configure OAC Updates for Mass-Distribution to Users” on page 68.

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

- “Setting Up an OAC Configuration” on page 61
- “Configuring Network Connection Settings” on page 7
- “Using the Custom Installer” on page 45
- “Custom Install: Provide Printable Documentation” on page 62

Setting Up an OAC Configuration

The configuration that you construct using the tools available in Odyssey Access Client Administrator can be used to deploy an initial configuration that users can modify later (unless you lock the settings). You can set up a configuration that specifies exact settings for connection timing, authentication protocols, networks that users are not allowed to change but that lets users add or modify other settings, such as Wi-Fi adapters and profiles for use in a home office. Once you have set up a configuration, you can deploy it to any or all OAC users.

If you have not installed OAC on the Windows 2000 or Windows XP computer on which you are specifying your configuration, follow these steps before you define a configuration for a custom installer:

- Configure network configuration and connection options. There are several configuration options. Follow one of the procedures described in these topics:
 - “Configuring User Authentication with No Machine Connection” on page 63
 - “Configuring Machine-Only Connections” on page 64
 - “Configuring Machine Connections that Switch to User Authentication” on page 64
- Configure feature access or control restrictions to be included in this preconfigured installer in Permissions Editor. See “Using the Permissions Editor” on page 31.
- Configure locking options to be included in this preconfigured installer in the Merge Rules tool. See “Setting Merge Rules” on page 35.
- Test network connections. When you define the default configuration, you can test each network connection. See “Testing Configuration Settings” on page 60.

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

Exceptions to Network Connection Options

There are a few exceptions to the network connection options you can specify in a configuration as noted below:

- You cannot preconfigure client certificates. If you select **EAP-TLS** under the **Authentication** tab in the Add Profile dialog (in the Profiles dialog of either the Initial Settings or Machine Accounts tool), users are prompted to select a client certificate the first time OAC runs on a client machine. You can, however, configure certificates for any trusted root server in the Trusted Servers dialog of Initial Settings or Machine Accounts tool.

OAC supports automatic certificate selection; that is, if a user has only one certificate, OAC uses it silently, without prompting. If the user has no certificate installed or has more than one, OAC prompts the user to specify a certificate. If the user has only one certificate but it is expired, OAC searches for a certificate with the same common name.

- You cannot preconfigure stored passwords or login names.

Custom Install: Provide Printable Documentation

The custom installer file that you create using the methods described in “Creating an Installer File” on page 47 includes the online help for the product but does not include documentation in PDF format.

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

- OdysseyClientAdmin.pdf
- OdysseyClientMan.pdf

OdysseyClientAdmin.pdf includes these administration topics, while OdysseyClientMan.pdf does not.

In addition to the .msi file that you create, you can provide your users with the product documentation file, OdysseyClientMan.pdf, to give them access to printable documentation that does not include information about administrative tasks.

Configuring User Authentication with No Machine Connection

You can connect all users to the network using only their user credentials. There are timing options for network authentication with user credentials. For example, if you require network-related startup processes, you can have users connect to the network before Windows logon.

To configure a user network connection, follow these steps:

1. Double-click **Initial Settings** in OAC Administrator. The **Initial Settings** dialog (Figure 6 on page 20) appears.
 - a. Use the dialog settings needed to configure your user network connection. This includes the Networks dialog, the **Trusted Servers** dialog, the **Adapters** dialog, and the Profiles dialog.
 - b. Close the Initial Settings tool after you make the settings.
2. Disable any configuration features you that need to restrict or lock using the Merge Rules tool.
3. Double-click **Connection Settings** in the OAC Administrator.

Connecting Before Windows Logon

To have users connect to the network prior to Windows logon time:

1. Select **Install the Odyssey Access Client GINA Module**, if it is not installed already.
2. Select **Prior to Windows logon** and select a wireless adapter and network (or a wired adapter and profile) that you have already configured
3. Select **OK**.

Connecting After Windows Logon (with or without GINA)

To require users to connect to the network after Windows logon time, independent of whether you install the Odyssey GINA module:

1. Select one of the two available user authentication timing options under the **User Account** tab.
2. Select **OK**.

You can have the users authenticate to the network before or after the desktop appears.

Configuring Machine-Only Connections

To identify a client machine on the network while not relying on user credentials, you can connect all client machines to the network using machine authentication. This can be useful if you have any machine-related startup processes. You can use this feature to maintain network connections for the client machine even when users are logged off.

To configure a machine-only connection, follow these steps:

1. Double-click **Connection Settings** in OAC Administrator.
2. On the **Machine Account** tab of Connection Settings, select **Enable network connection using machine account**
3. Select **leave the machine connection active**.
4. Select **OK**.

Double-click **Machine Account** in the OAC Administrator. The Machine Account dialog (Figure 9 on page 26) appears. Use the dialog settings that are required for setting up your machine network connection, including Networks, Adapters, and Profiles, and close the Machine Account tool. See “Configuring a Machine Password” on page 28 for details about specifying machine account profiles.

Configuring Machine Connections that Switch to User Authentication

You can connect all client machines to the network using machine credentials and then require user authentication when the user logs on. This option enables you to perform network tasks at Windows startup, before users log in, and then switch to an authenticated user-level network connection when the user logs on. This enables you to run maintenance scripts and backups at night or during hours when users are typically not in the office.

To configure a machine connection followed by user authentication, follow these steps:

1. Double-click **Connection Settings** in the OAC Administrator.
2. On the **Machine Account** tab of Connection Settings, select **Enable network connection using machine account**.
3. Select **drop the machine connection**.
4. Select one of the available user authentication timing options under the **User Account** tab of Connection Settings and select **OK**.

Select either **authenticate at the desktop** or **authenticate after login but before the desktop**

5. Double-click Machine Account in the OAC Administrator. The Machine Account dialog (Figure 9 on page 26) appears.
6. Use the dialog settings to configure your machine network connection. This includes the Networks dialog, the Trusted Servers dialog, the Adapters dialog, and the Profiles dialog. See “Configuring a Machine Password” on page 28 for details about specifying machine account profiles.
7. Close the Machine Account tool.
8. Double-click **Initial Settings** in the OAC Administrator. The Initial Settings tool dialog (Figure 6 on page 20) appears.
9. Use the dialog settings needed to configure your user network connection. This includes the **Networks** dialog, the **Trusted Servers** dialog, the **Adapters** dialog, and the **Profiles** dialog.
10. Lock any configuration features that require locking using the Merge Rules tool.
11. Close the Initial Settings tool when you are done.

Creating Scripts for Incremental Updates

You can update OAC configurations for one or more users. For example, if you add new SSIDs to your network, you can configure the network once with Odyssey Access Client Administrator and then create a script that deploys the updated configuration to one or more users.

There are two types of configuration scripts for updating OAC settings for users:

- You can deliver a script that runs automatically whenever OAC polls for new scripts.
- You can deliver a script that the user can select to run. See *Odyssey Access Client User Guide* for more information about user interaction with scripts.

To provide configuration scripts to update user configurations:

1. Generate one or more scripts using the Script Composer tool or the command-line interface.
 - See “Using Scripts” on page 49 for information about creating scripts using the Script Composer tool. Make sure that you save your scripts with the correct extension for autoscripts or regular scripts.
 - See “Command-Line Code to Create and Load OAC Manager Scripts” on page 67. Users cannot run encrypted scripts that you create using the command-line interface.
2. Deliver the script(s) to the following directory on your user’s computer:

```
system_volume:\Documents and Settings\username\Application Data\
Juniper Networks, Inc.\OAC\newScripts
```

OAC polls this directory for new scripts frequently. New scripts are treated as follows:

- Autoscripts run automatically when detected by OAC.
- Users can run or delete other scripts when they select **Tools > Configuration Scripts > Check New Scripts**.

If the script is not an autoscript—that is, if it must be run manually—there is no specific location in the file system where the script must be stored.

Note that if you want merge rules or permission restrictions to apply to your user configurations, follow the directions in “Configure OAC Updates for Mass-Distribution to Users” on page 68.

Notes on the Directory for Scripts

Depending on your operating system, the physical path to the **Application Data** folder described in Step 2. of “Creating Scripts for Incremental Updates” on page 65 might vary. It is always the **CSIDL_APPDATA** path used by Windows shell programmers. Once you locate the **Application Data** folder, you can place the scripts in this folder under **OAC\newScripts**.

A typical path is as follows:

```
C:\Documents and Settings\username\Application Data\OAC\newScripts
```



NOTE: In order to view the **Application Data** directory, you must make hidden files and folders visible.

Command-Line Code to Create and Load OAC Manager Scripts

You can use a command-line interface to create scripts that export the entire OAC Manager configuration. The syntax is as follows:

odClientAdministrator *arguments*

The arguments that you can use to save (export) the OAC Manager configuration or restore (import) a saved configuration to OAC Manager are:

```
/E[xport] = filename
/I[mport] = filename
/Key = encryptionKey
/N[otSavePrivateData]
/S[ilent]
```

You can use any of the following argument combinations:

- /E = filename
- /E = filename /N
- /E = filename /S
- /E = filename /K = encryptionKey /N
- /E = filename /K = encryptionKey /N /S
- /E = filename /K = encryptionKey
- /E = filename /K = encryptionKey /S
- /I = filename
- /I = filename /S
- /I = filename /K = encryptionKey
- /I = filename /K = encryptionKey /S

Note the following about the behavior of this command-line interface:

- Only users with administrative privileges can import or export scripts from the command line. However, users can import scripts from the **Tools > Run Script** command in OAC Manager. Use the `.odyClientScript` file extension when you save a configuration if you want users to import the saved configuration from the **Tools > Run Script** command in OAC Administrator.
- Use the `.odyClientScript` file extension when you save an unencrypted configuration script for users to run manually. When you use this extension, you can provide this script to your users with instructions to select **Tools > Run Script** from the OAC Manager and browse for an unencrypted script you create using this command-line interface.

- Use the `.odyClientScriptAuto` file extension when you save an unencrypted configuration that is intended for use as an autoscript. OAC runs autoscripts automatically when you deliver them according to the directions in the procedure described in “Creating Scripts for Incremental Updates” on page 65.
- If you use multiple switches, leave a space between each switch command.
- The OAC Administrator always displays a message after your import or export unless you use the `/S` (silent mode) switch.
- An error level is always returned, so you can use the `errorlevel` command in a batch file to return the error level. A `0` indicates success. Failures return nonzero values.
- The script that you create using this command-line interface adds any new items to an OAC Manager configuration, and replaces existing items if they have the same names.
- If you do not specify an encryption key, OAC encrypts passwords, WEP keys, and passphrases so that any users with OAC installed can run this script. If you specify the `/K` encryption key switch with an exported script, the encryption key you supply must also be used when you or someone else imports this OAC Manager configuration script.
- If you specify the `/K` switch when you export a script, you cannot use the following symbols for this key: `|`, `&`
- If you specify the `/N` switch when you export a configuration, then none of your personal data (user name, password, and any WEP keys you supply) is exported.
- Certificates are never exported using this command-line interface.
- Adapter types (wired or wireless) are exported, but the adapter details are not.
- Like OAC scripts created using the Script Composer tool, exported features are not locked, even if they are locked in your OAC Manager. To lock features, use the Merge Rules tool and create a custom update file. See “Configure OAC Updates for Mass-Distribution to Users” on page 68.

Configure OAC Updates for Mass-Distribution to Users

You can update OAC configurations for a large number of users. For example, if you want to update user configurations with new OAC features, you can create an updated customized configuration file through the **Settings Update file** option of Customer Installer.

When you create a customized OAC configuration setup file using this option, you can distribute this file to users to update their configurations. You cannot, however, use this option for version upgrades of OAC.

Before you create an OAC update configuration file, you can configure merge rules to specify how your updated OAC configuration is applied to user machines.

You can create an updated configuration file that is based on your connection settings from the Connection Settings tool, machine account settings in the Machine Accounts tool, user settings in the Initial Settings tool, lock options in the Merge Rules tool, and set specific feature constraints in the Permissions Editor tool.

To create the update configuration file:

1. Double-click the Custom Installer tool in the OAC Administrator.
2. Select **Settings update file**.
3. Select **Browse** to locate a destination directory. The Select Destination File dialog appears.
4. Type the name of the configuration file that you want to save next to **Destination File**.
5. Select **Save**.
6. Select **OK** to close the Custom Installer tool.
7. Install the file on your user machines. Only users with administrative privileges on their machines can run the custom update file on their own machines.

Using Smart Cards with GINA

If you install GINA using the directions in “Installing the Odyssey GINA Module” on page 15, you can configure an authentication profile for users logging in to Windows with or without smart cards. Do this by configuring certificate and password-based protocols within the same profile.



NOTE: You can configure a profile that uses both smart card and password-based protocols for authentication before or after Windows logon if you install GINA.

To configure network connections for users who might log in with a smart card or, if the smart card is not available, to use a password-based protocol, follow these steps:

1. Create a profile in the Initial Settings tool as follows:
 - a. Name the profile, and leave the login name blank.
 - b. Add the protocols to the protocols list on the **Authentication** tab of the profile description to be used for smart card login:
 - ❑ EAP-TTLS, select the **Use only my certificate for authentication** option on the **TTLS Settings** tab of the Profile Properties dialog
 - ❑ EAP-PEAP, for which EAP-TLS is the inner method
 - ❑ EAP-TLS



NOTE: Turning FIPS Mode on disables OAC smart card management.

- c. Add one or more protocols to the list of authentication protocols on the **Authentication** tab of the profile description to be used for password-based login. Note that if you configure EAP-TTLS for smart card logon, you cannot use EAP-TTLS for password-based logon in the same protocol.
 - d. Remove any protocols listed on the **Authentication** tab that you do not require.
 - e. Order the protocols listed on the **Authentication** tab according to negotiation preference. Note that the password-based methods listed are not used when the smart card is present. Similarly, the certificate based methods listed on the profile are not used when the smart card is not installed.
 - f. On the **User Info > Certificate** subtab of the Profile Properties dialog, select **Permit login using password**.
 - g. On the **User Info > Password** subtab of the Profile Properties dialog, select **Permit login using password**. Modify TTLS settings based on the TTLS Settings and/or modify the PEAP settings based on the PEAP Settings in the *Odyssey Access Client User Guide* based on the smart card protocol that you selected in Step b.
 - ❑ Select EAP-TLS as the inner method for EAP-PEAP on the **PEAP Settings** tab of the profile if you require EAP-PEAP as a smart card certificate-based method.
 - ❑ Select **Use only my certificate for authentication** on the **TTLS Settings** tab of the profile if you require EAP-TTLS as a smart card certificate-based method.
 - h. Modify TTLS settings according to **TTLS Settings** and/or PEAP settings according to **PEAP Settings**, using the password-based protocol you select in Step c.
 - ❑ Select an inner method for EAP-TTLS from the **TTLS Settings** tab of the profile if you require EAP-TTLS as a password-based method.
 - ❑ Select an inner method (other than EAP-TLS) from the **PEAP Settings** tab of the profile if you require EAP-PEAP as a password-based protocol. Note that you can use EAP-PEAP as both a password-based protocol and a smart card certificate-based protocol if you select an inner method in addition to EAP-TLS for use with EAP-PEAP.
 - i. Select **OK** to save the profile.
2. Configure a network and server trust using to the directions in the *Odyssey Access Client User Guide*. Make sure that you associate the profile in Step 1 with this network.

3. Configure any options you require from **Tools > Options** in the Initial Settings tool.
4. Close the Initial Settings tool.
5. Open Connection Settings and perform the following:
 - a. Install GINA if it is not already installed, using the directions in “Installing the Odyssey GINA Module” on page 15.
 - b. Set up the appropriate prior to Windows logon connection option on the **User Account** tab of Connection Settings and select the network that you configured in Step 2.
6. Open the Merge Rules tool and lock the profile that you created in Step 1. In addition, lock any other features that require locking.

See “Using GINA with Smart Cards” on page 16 for more information about how OAC behaves when your users connect to the network prior to Windows logon (with or without smart cards).

Configuring Single Sign On for TTLS or PEAP

Connecting prior to Windows logon can be helpful when users have start-up processes that require network connections. You can configure OAC for EAP-TTLS or EAP-PEAP authentication with prior to Windows logon using the Odyssey Access Client Administrator and the OAC GINA module. Use the OAC GINA module to enable Windows users to connect to the network using Windows logon credentials before logon.



NOTE: You cannot use this feature without installing the OAC GINA module.

Prerequisites

You must have installed (and know the name of) the Certificate Authority (CA) certificate that is used for server validation. The certificate must be installed in the trusted root certificate store on the local machine.

To configure OAC for prior to Windows logon connections:

1. Create the network configuration with the Initial Settings tool.
2. Set up a user account and GINA connection settings using Connection Settings.
3. Test the connection settings and update any configuration settings in the Initial Settings tool and/or Connection Settings as necessary.

Setting Up a Prior to Windows Logon Configuration Using GINA

Before you can complete the connection settings for prior to Windows logon, you must first define the network configuration in the Initial Settings tool. The network configuration steps for are identical to those for OAC Manager:

1. Set up an adapter.
2. Create a profile. Leave the login name blank when you create a profile for use with GINA.
3. Add a network.
4. Set up a trusted server certificate.
5. Connect to the network.

See the *Odyssey Access Client User Guide* for instructions for each of these steps.

Specifying User Account Connection Settings and Installing OAC GINA

To configure the Connection Settings and install Odyssey GINA:

1. Double-click **Connection Settings** in Odyssey Client Administrator.
2. Select the **GINA** tab and select **Install Odyssey GINA Module**. If the GINA module is installed, skip this step.
3. Select the **User Account** tab and select **prior to Windows logon, using the following settings**.
4. Select **OK** after you complete the configuration settings.

If you require authentication at machine startup time, you can configure machine account settings to have users connect to the network using the machine account at machine startup time and then drop that connection to connect to the network with user credentials prior to Windows logon. In this case, configure machine account settings on the Machine Account tab of Connection Settings before you select **OK**.

If you intend to use OAC for single sign on authentication to an external database other than Windows, select **Prompt before connecting to the network** before you select **OK** to close Connection Settings.

Testing Prior to Windows Logon Settings

To test prior to Windows logon settings:

1. Select **Commands > Reload and Test Initial Settings**.
2. Open OAC Manager.
3. Select the connection status on the Connection dialog.
4. Modify any settings in the Initial Settings or Connection Settings tool and re-test as necessary from the Initial Settings tool.

Configuring Required FIPS Mode Connections (FE Only)

If your enterprise network is FIPS-compliant, you can require that all connections to your enterprise network use OAC FIPS mode.

Follow this procedure to secure required FIPS mode connections to your network:

1. Configure FIPS mode connections that are authenticated with machine or user credentials (or first machine, and then user credentials):
 - a. Follow the instructions in the Initial Settings tool to configure FIPS-compliant connections that the user sets through user credentials. Remember to select **FIPS mode required** for the FIPS-compliant network descriptions that you create.
 - b. Follow the instructions in the Machine Account tool to configure FIPS-compliant connections for the machine using machine credentials. Remember to select **FIPS mode required** for the FIPS-compliant network descriptions you create.
2. Configure the connection settings in the Connection Settings tool using one of the following procedures:
 - a. “Configuring User Authentication with No Machine Connection” on page 63
 - b. “Configuring Machine Connections that Switch to User Authentication” on page 64
3. Lock the FIPS-compliant networks that you create in Step 1 under the **Networks** category in the Merge Rules tool. In addition, lock **FIPS Mode On** under the **Other** category in the Merge Rules tool. See “Use Cases for Merge Rules” on page 35 for more information.
4. Create a custom installer or settings update file with these custom configuration settings using Custom Installer. See “Preconfiguring OAC for a Group of Users” on page 61.
5. Distribute the custom installer files to computers on which you have not yet installed the FIPS Edition of OAC. Use settings update files for computer on which the FIPS Edition of OAC is installed.

Appendix A

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 data 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 of data based on an algorithm. The result is called a hashed value.

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

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

EAP-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

A

Active Directory	
machine account	28
administrative tools	
overview.....	2
alternate adapter	
wired 802.1X.....	10
alternate settings	
edit.....	11
authentication	
certificate-based	10
flow of events.....	2
Layer 2	2
Layer 3	2
no machine logon.....	63
password-based.....	10
profile for smart card log on.....	69
auto-scan list	
add with script	53
hide	40
lock	40
autoscript	
creating	51
delivery	65

C

certificate	
automatic selection for machine account	27
CA for machine account	27
configure with password-based protocols.....	69
machine account.....	28
scripting	51
smart card	
with GINA.....	16
client updates	68
command-line	
export scripts	67
scripts from	67
compatibility	
GINA.....	15
configuration	
alternate.....	10
client update.....	68
custom	
installer, creating.....	45
deploy settings	36
lock settings	36
machine connection	26
machine name	28

mass distribution	46
Merge Rules effects.....	35
new users only	36
planning	2
predefined	
restrict features	31
push	68
remove settings	49
replace settings.....	36
restrictions	
set	32
set or replace settings.....	49
testing settings.....	60
connection	
control Windows logon timing.....	10
settings	
GINA requirement	10
test	60
without machine logon.....	63
Connection Settings	
overview.....	7
uses	4
constraints	
user	32
create script	50
credentials	
machine	28
Custom Installer	
administrative tools.....	45
include documentation	62
notes	62
settings update file.....	68
uses	5, 45

D

defaults	
set for initial users	20
deploy	
configuration update.....	45
license update.....	45
new configuration.....	45
disable	
configuration options.....	31
features	32
documentation	
include in custom configuration.....	62
domain password	
machine	28

E

EAP methods
 for machine credentials 29

EAP-FAST options
 for machine account 27

EAP-TTLS
 smart cards 70

export
 command line 67
 license key 46
 restrictions 31
 scripts 67

F

FIPS mode
 configuration 73
 lock 43

G

GINA
 compatibility with other products 15
 install 13, 15
 Novell Client credentials 15
 overview 13
 remove 15
 restrictions 16
 uses for 14
 with smart cards 16

Graphical Identification and Authentication
 See GINA

I

import scripts
 command-line 67

Infranet Controller
 lock 35, 41

initial configuration
 machine requirement 19

Initial Settings
 administrative tools 20
 and customer installer 21
 and Merge Rules 19
 options 10
 overview 19
 uses 5

inner authentication
 protocols for smart card log on 69

install
 GINA 13
 silent 46

installer
 create and customize 45
 new file 46
 update file 46

L

license keys
 OAC editions vii

remove from help menu 33

lock
 auto-scan list 40
 features
 Merge Rules 37
 FIPS mode setting 43
 Infranet Controller 41
 network 39
 OAC features 31
 profile 38
 trusted servers 42
 Windows logon setting 43

logon
 capture credentials 13
 configure default name 22
 custom name 23
 set name formats 19
 Windows
 compatibility with other modules 64
 configuration notes 21
 features 64
 override defaults 21
 trust, setting 21

M

machine account
 administrative tools 26
 certificates 28
 connection
 before user logon 64
 without user logon 64
 connection settings 12, 27
 connections
 configuring 26
 credentials 28
 domain password 28
 enable 26
 overview 25
 password credentials 27
 restrictions 27
 test connection 60
 uses 25

Machine Accounts
 uses 5

machine name
 configuration 28

machine-level connection
 purpose 9
 settings 12
 timing 9

Merge Rules
 assign 37
 custom installers 62
 for auto-scan lists 40
 for EAP-FAST options 42
 for Infranet Controllers 40
 for networks 39
 for profiles 39
 for security options 42

- for trusted servers 42
 - for wireless suppression 42
 - overview 35
 - periodic updates 35
 - set 37
 - settings 36
 - use cases 35
 - uses 5, 37
- N**
- network
 - add or replace with script 52
 - disable ad-hoc 32
 - disable any 32
 - enable automatic connection 49
 - lock or restrict 39
 - machine authentication 12
 - remove with script 52
 - scripts 52
 - network connection
 - before Windows logon 10
 - control timing of 8
 - earliest 25
 - early
 - restrictions 16
 - machine and user 64
 - machine-level 8
 - options 8
 - machine-only 64
 - require prompt screen 11
 - restrictions 16
 - timing options 10
 - user, without machine 63
 - Novell Client for Windows
 - compatibility with GINA 15
- O**
- odClientAdministrator.exe 4
 - odyClientScriptAuto 51
 - Odyssey Access Client Administrator
 - disable 33
 - Odyssey GINA 14
 - OdysseyClient.msi 46
 - override
 - default connection settings 21
 - Windows logon 11
- P**
- PAC Manager
 - uses 5
 - password
 - for machine account 27
 - machine 28
 - permissions
 - enable or disable 32
 - set user 32
 - Permissions Editor
 - option controls 31
 - uses 5
- preconfigured settings 20
 - prior-to-Windows logon
 - override 11
 - profile
 - activate with script 52
 - configure with scripts 51
 - restrict or lock 38
 - prompt to connect
 - options 11
 - push
 - configurations 68
- R**
- realm
 - machine credentials 28
 - release notes ix
 - remove auto-scan list
 - with script 53
 - restrictions
 - authentication protocols 31
 - logon settings 18
 - OAC features 31
 - password 18
 - PIN prompt 18
 - remove 32
 - token 18
 - user account settings 18
- S**
- save
 - custom installer 45
 - scripts 51
 - settings update files 68
 - script
 - activate a profile 52
 - add auto-scan list 53
 - add or replace network 52
 - add or set profile 51
 - automatic 51
 - certificates 51
 - command-line, from 67
 - data format 49
 - deliver files to users 65
 - destination file 50
 - directions 65
 - networks 52
 - profiles 51
 - remove auto-scan list 53
 - remove network 52
 - remove profile 51
 - save 51
 - SSIDs, removing 54
 - Script Composer
 - defined 49
 - options 49
 - uses 5
 - settings
 - initial user defaults 20
 - Merge Rules 37

predefined.....	19	compatibility with Odyssey GINA	14
update file	46	Windows logon	
update files.....	69	configuration notes.....	21
silent		delay	13
install	47	lock settings	43
script export.....	67	override defaults.....	21
Single sign-on	4	skip	11
smart card		timing options	9
EAP-TTLS	70	wireless suppression	
management		Merge Rules for	42
FIPS constraint	10		
required authentication protocol	16		
use with GINA for Windows log on.....	69		
with GINA.....	16		
SSID			
removing with scripts.....	54		
T			
template			
custom installer, for	45		
test			
administrative settings	60		
user connections	60		
trust			
machine account requirements	27		
trusted server			
override.....	21		
trusted servers			
lock	42		
Merge Rules for	42		
U			
update			
connection settings	49		
EAP-FAST settings	49		
preemptive network setting	49		
profile	49		
scan list	49		
security settings	49		
trusted server settings	49		
user configuration	45, 68		
user licenses.....	45		
Windows logon timing settings	49		
wireless suppression setting.....	49		
upgrade			
custom installers for	45		
user account			
restricted options	18		
user-level connection			
manage timing of	9		
options	9		
settings.....	9		
V			
VLAN			
for machine account	27		
W			
Windows GINA			

Juniper *your* Net™

www.juniper.net

CORPORATE HEADQUARTERS

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

Juniper Networks, Inc. has sales offices worldwide.

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



Printed on recycled paper

ODR-ZA-ODYCAAG, Revision A00