



Odyssey Access Client for Windows

Administration Guide

**Enterprise Edition
FIPS Edition**

*Release 5.0
March 2009*

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

Part Number: 530-028166-01

Copyright Notice

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Copyright © 2009 Juniper Networks, Inc. All rights reserved.
Printed in the USA.

FCC Statement

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

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

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

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

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

U.S. Government Rights

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

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

Disclaimer

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

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

End User License Agreement

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").
2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper equipment.
3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:
 - a. Customer shall use the Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
 - b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius software on multiple computers requires multiple licenses, regardless of whether such computers are physically contained on a single chassis.
 - c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
 - d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 3D-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 3D-day trial period.
 - e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services. The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.
4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Embedded Software on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.
5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.
6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.
7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19; or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>. and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation are and will be in the English language)).

Table of Contents

Preface	ix
Audience	ix
Conventions	x
Documentation	xi
Release Notes and Product Documentation	xii
Context-Sensitive Help	xii
Request Technical Support	xii
Self-Help Online Tools and Resources	xii
Open a Case with JTAC	xiii
Chapter 1 Understanding Odyssey Access Client Administrator	1
OAC Network Authentication Overview	1
Plan an OAC Configuration	3
Odyssey Access Client Administrator Tools Overview	5
Connection Settings	5
Initial Settings	6
Machine Accounts	6
Permissions Editor	6
Merge Rules	7
Custom Installer	7
Script Composer	7
PAC Manager	7
Chapter 2 Configuring a User Account	9
Initial Settings Tool Overview	9
Tools Menu Options for Initial Settings	10
Process Flow for Initial Settings	12
Configure Initial Settings	13
Manage Windows Logon Settings	14
Caution on Overriding Default Windows Logon Settings	15
Configure the Login Name Format	15
Configure Connection Timing for a User Account	17
Test Configuration Settings	17
Test Machine Connection Settings	18
Control Network Adapters and Other Wi-Fi Suppliants	18
Chapter 3 Configuring a Machine Account	21
Machine Account Tool Overview	22
Process Flow for Machine Account Settings	23
Enable a Machine Account Connection	24
Configure Machine Account Settings	24
Machine Account Profile Options	25

Chapter 4	Configuring How and When Network Connections Occur	29
	Connection Settings Tool Overview.....	29
	Process Flow for Configuring Connection Settings.....	31
	About Network Connection Timing.....	32
	Configure a User Account Connection.....	33
	Connect After Windows Logon, Before the Desktop Appears.....	33
	Connect Prior to Windows Logon.....	34
	Configure a Machine Account Connection.....	35
	Configure Machine Account Connection Settings.....	36
	Configure Machine-Only Connections.....	36
	Configure Machine Connections that Switch to User Connections.....	37
	Configure a Prior to Windows Logon Connection with GINA.....	38
	Install the Odyssey GINA Module.....	38
	Remove the Odyssey GINA Module.....	38
	Use a Third-Party GINA Module and Odyssey GINA.....	39
	GINA Compatibility with Other Modules Running at Windows Logon.....	39
	Use GINA with Smart Cards.....	39
Chapter 5	Setting Permissions for Individual OAC Features	43
	Permissions Settings Overview.....	43
	Authentication Protocols.....	43
	TTLS Inner Authentication Protocols.....	44
	TTLS Inner EAP Protocols.....	44
	PEAP Inner Authentication Protocols.....	44
	Profile Properties.....	44
	Options.....	44
	Network Properties.....	44
	Odyssey Control.....	44
	User Interface Settings.....	45
	User Interface—Hide Configuration Sections.....	45
	User Interface—Disable and Hide Configuration Sections.....	45
	Set Permissions or Restrictions.....	45
	Guidelines for Using Permissions Editor.....	46
Chapter 6	Managing Updates Using Merge Rules	49
	Merge Rules Overview.....	49
	Use Cases for Merge Rules.....	49
	Merge Rule Settings.....	50
	Set Merge Rules.....	50
	Set Merge Rules for Profiles.....	51
	Set Merge Rules for Networks.....	51
	Set Merge Rules for Individual Networks.....	52
	Set Merge Rules for Auto-Scan Lists.....	52
	Set Merge Rules for Intranet Controllers.....	53
	Set Merge Rules for Trust.....	53
	Set Merge Rules for the Other Tab.....	54
Chapter 7	Deploying Odyssey Access Client	55
	Custom Installer Tool Overview.....	55
	Open the Custom Installer Tool.....	55
	Process Flow for Deployment.....	57
	Create a New Installer File.....	58

Guidelines for Creating a New Custom Installer File	58
Create a Custom Update File.....	59
Process Flow for Updating User Account Settings	60
Export a Preconfiguration File.....	61
Use the Silent Install Option	62
Preconfigure OAC for a Group of Users	62
Set Up an OAC Configuration	62
Configure OAC Updates for Distribution to Multiple Users	63
Exceptions to Preconfigured Network Connections.....	64
Task Summary: Merge Update Settings for Machine Accounts	64
Process Flow for Updating Machine Account Settings	66
Deploy OAC with Scripts	67
Script Composer Overview	67
Create a Script	68
Add or Set Profiles with a Script	69
Remove a Profile with a Script.....	69
Activate a Profile for a Wired Connection with a Script	69
Add or Set Networks with a Script	70
Remove a Configured Network with a Script	70
Activate a Network for a Wired Connection with a Script	70
Add or Set Auto-Scan Lists with a Script	71
Remove Auto-Scan Lists with a Script.....	71
Manage Settings in the Other Tab with a Script	71
Add or Set a Trust Tree with a Script	72
Replace Options Settings with a Script.....	72
Remove Networks Using SSIDs with a Script	72
Set or Replace FIPS Options (FE Only) with a Script	73
Deploy Incremental Updates with a Script	73
Create and Load OAC Scripts Using Commands	74
Chapter 8	Managing Protected Access Credentials
	77
Refresh the PAC Manager Display	77
Delete a PAC	77
Exit from the PAC Manager.....	77
Chapter 9	Sample Administrative Workflows
	79
Single SignOn for TTLS or PEAP.....	79
Configure a Prior to Windows Logon Configuration Using GINA.....	80
Specify User Account Connection Settings and Installing OAC GINA	80
Test Prior to Windows Logon Settings.....	80
Index	83

Preface

This guide describes how to use Odyssey Access Client Administrator tools to configure, update, and deploy Odyssey Access Client (OAC) to users. In corporate networks, OAC negotiates with 802.1X wireless access points, 802.1X switches, and Infranet Controllers for authenticated, secure access to protected networks. An authentication server, such as Juniper Networks Steel-Belted Radius, must validate each user. In a Juniper Networks Unified Access Control (UAC) network, the user's endpoint computer is checked for security compliance before being allowed to access protected resources on the network. In networks with 802.1X-enabled switches, the switches are enforcement points in the network security architecture.

This release supports two licensed editions of OAC:

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

This guide identifies any differences in product features or options based on the type of license.

You can deploy OAC in a network that includes the Juniper Networks Unified Access Control security solution where authenticated access to protected network resources is managed by an Infranet Controller. You can also deploy OAC in a traditional network without an Infranet Controller and where OAC negotiates directly with an AAA server for authenticated access.

This guide is available in PDF format on the Juniper Networks Web site at:

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

Audience

This guide is for network administrators whose responsibilities include managing secure wired and wireless network access for corporate users. It is particularly directed to those administrators who are responsible for configuring and deploying OAC to users, for configuring EAP authentication protocols, and for configuring which OAC features users can view or configure.

OAC offers a wide range of configuration options and controls, for administrators and for individual users. It is the administrator who determines how much flexibility and control users have, based on corporate security policies and on the configuration settings in Odyssey Access Client Administrator. All administrators responsible for managing OAC should be familiar with using OAC and with the information presented in the *Odyssey Access Client User Guide*. See “Documentation” on page xi.

Some of the information in this document pertains to configuration tasks specific to the Juniper Networks Unified Access Control (UAC) security solution. If you use OAC on a UAC network, refer to the *Unified Access Control Administration Guide* on the Web at:

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

Conventions

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

Table 1: Notice Icons




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

Table 2: Text Conventions

Convention	Description
Plain sans serif type	Filenames and directory names.
<i>Italics</i>	<ul style="list-style-type: none"> ■ Terms defined in text. ■ Variable elements for which you supply values. ■ Book titles.
+ (plus sign)	Key names linked with a plus sign indicate that you must press two or more keys simultaneously.

Table 3: CLI Conventions

Convention	Description
Bold type	Commands that you enter; command names and options.
Plain sans serif type	<ul style="list-style-type: none"> ■ Filenames and directory names. ■ Code and system output.

Table 3: CLI Conventions (continued)

Convention	Description
<i>Italics</i>	Variables for which you supply values.
[] Square brackets	Elements in square brackets indicate optional keywords or variables.
Pipe symbol	Elements separated by the pipe symbol indicate a choice between mutually exclusive keywords or variables.
{ } Braces	Elements in braces indicate required keywords or variables.

Table 4: GUI Conventions

Convention	Description
> (chevron)	Navigation paths through the UI.
Bold type	User interface elements that you select in a procedure, such as tabs, buttons, and menu options.
<i>Italics</i>	Variables for which you supply values.

Documentation

Table 5 lists the OAC and the UAC documentation sets and how to access them online.

Table 5: OAC/UAC Documentation Set

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

Table 5: OAC/UAC Documentation Set

Title	Purpose
<i>Unified Access Control Deployment Scenarios Guide</i>	Provide recommendations for deploying the Unified Access Control solution.

Release Notes and Product Documentation

You can access the product release notes, the *Odyssey Access Client Quick Start Guide*, and the *Odyssey Access Client User Guide* on the Web at:

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

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

Context-Sensitive Help

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

To get 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.

Request Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings—<http://www.juniper.net/customers/support/>
- Find product documentation—<http://www.juniper.net/techpubs/>

- Find solutions and answer questions using our Knowledge Base—
<http://kb.juniper.net/>
- Download the latest versions of software and review your release notes—
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications—
<http://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum—
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Manager—
<http://www.juniper.net/customers/cm/>
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool—
<https://tools.juniper.net/SerialNumberEntitlementSearch/>

Open a Case with JTAC

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

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

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

Chapter 1

Understanding Odyssey Access Client Administrator

This topic is an overview of Odyssey Access Client Administrator—a suite of tools for configuring, updating, and deploying OAC to users and for controlling which OAC features users can access. You access the Odyssey Access Client Administrator through the OAC Manager menu bar. Click **Tools > Odyssey Access Client Administrator**.

Also included is a discussion of the components and processes required for secure network authentication and a summary of topics to consider when planning to configure and deploy OAC to users.

OAC is 802.1X network access client software. It provides full support for Extensible Authentication Protocols (EAP) required for secure wireless LAN access. Together with an 802.1X-compatible RADIUS server such as Juniper Networks Steel-Belted Radius, OAC secures the authentication and connection of WLAN users, ensuring that only authorized users can connect, that login credentials are not compromised, and that data privacy is maintained over the wireless link. OAC also serves as a client for enterprises that are deploying identity-based (wired 802.1X) networking. OAC provides wireless access to enterprise networks, home Wi-Fi networks, and public hotspots.

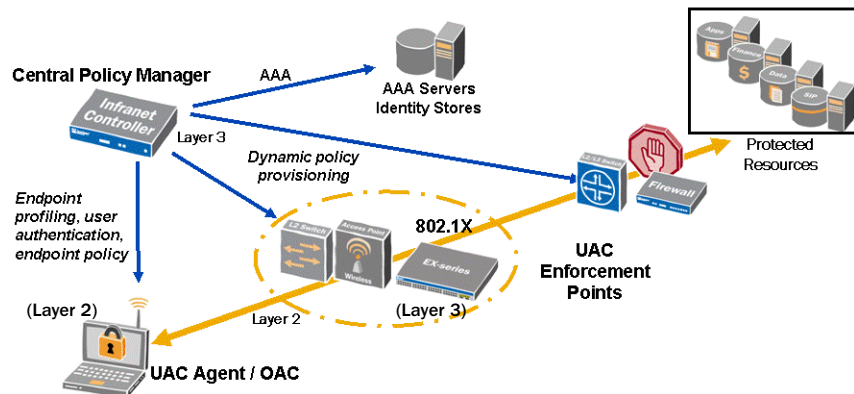
The Juniper Networks Unified Access Control (UAC) solution combines user identity and device security state information with network location to create a unique access control policy for each user. The solution can be enabled at Layer 2 using 802.1X, or at Layer 3 using an overlay deployment. UAC can also be provisioned in mixed mode using 802.1X for network admission control and Layer 3 for resource access control. At the center of this solution is the 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 is a firewall for the Infranet Controller to enforce security policies. The Infranet Enforcer is deployed in front of the Infranet Controller and protected network resources.

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.

For background information on network security and authentication, see Appendix A, “Network Security Concepts” in the *Odyssey Access Client User Guide*.

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 the logon process completes. In an IEEE 802.1X network, those events include user or machine authentication using Extensible Authentication Protocol (EAP) methods. In a UAC network, both the user and the machine must comply with network security policy.

The following basic events must occur for authenticated network access include:

1. OAC attempts to make an authenticated network connection. Depending on the corporate network infrastructure, the network connection can include a Layer 2 connection to an 802.1X switch or wireless access point or a Layer 3 connection to an Infranet Controller or to a switch that does not support 802.1X authentication. (An Infranet Controller is a server that verifies your identity and your computer’s compliance with security requirements before allowing you to access protected resources.)
2. 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.
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.
4. An authentication server then sets up an encrypted tunnel used to negotiate secure wireless authentication.
5. Successful wired or wireless authentication gives the user access to a VLAN and the appropriate protected network resources.

Plan an OAC Configuration

Consider the following questions when you plan your OAC configuration:

- Will you be authenticating users, machines, or both? If you are setting up individual endpoints that support multiple users, consider using machine authentication. The method you use determines the flow of steps for configuring the client settings.
- Do you need the client machines to connect to the network before the user desktop interface appear? If you need to run setup scripts or other processes that run earlier, you can configure OAC user account settings to support this ability.
- How many variations of OAC configuration do you need? Based on the user roles configured on the Infranet Controller, you can configure OAC and export the settings to the Infranet Controller and map those settings to specific roles.
- Which outer EAP authentication protocols do you need? In a UAC network, you can use either Tunneled Transport Layer Security (TTLS) or Protected EAP (PEAP). In a traditional network, check your corporate security policy or ask your network security officer about which protocols are supported.
- If you use TTLS or PEAP, which inner authentication protocols do you need? An inner authentication protocol is one transmitting and/or receiving communications within a tunnel provided by a tunneling protocol, such as TTLS. In a UAC network, you must use Juniper Networks UAC (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—Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or WPA2. If you are using the OAC FIPS Edition (FE), there are specific constraints on encryption methods, based on whether FIPS mode is 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 service set identifiers (SSIDs) for your wireless access points and should you broadcast them? The SSIDs that you use to configure wireless networks must match those of the wireless access points on your network. Without the SSID, OAC can detect a wireless network but cannot connect to it.
- 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, it can present an added security risk to a corporate network.
- Should you allow users to modify any configuration settings after you deploy them? The degree of configuration flexibility that you give individual users reflects your corporate security policy and the technical sophistication of your users. One benefit of this flexibility is that you can provide a simpler set of controls and options for many users whom you do not want to change predefined configuration settings. The administrative tools allow you to hide, disable, and lock individual configuration settings.
- Should you allow users to add, remove, or modify trusted servers and certificates? You can prevent users from modifying trust configuration settings by turning off access to trust settings so that they do not appear in Odyssey Access Client Manager.
- Which network profile configuration settings apply if your network includes Infranet Controllers? Should these settings be locked so that users cannot change them? Each Infranet Controller requires a separate profile.
- Should you allow Fast User Switching for Windows Vista users? Fast User Switching is enabled for Windows Vista and is not disabled by default for domain users as it is for Windows 2000 and Windows XP.

This means that all concurrent user sessions on a given Windows Vista system can access the current desktop connections to networks and Infranet Controllers. Thus, if one user has a current network connection, other users logged in on the same machine can access the same network connections. This can be a security risk. A background process running in one user session can piggyback onto the network access granted to another session and access resources to which the user should not have access rights. We recommend that you disable Fast User Switching for Windows Vista users.

- What configuration is best if you want to restrict and simplify the OAC configuration for most of your users? Which optional settings should you hide and which ones should you disable so that they cannot be accessed?
- Should you allow access to other wireless supplicant programs or do you prefer to enforce the use of OAC? You can configure OAC to manage all network adapters and prevent users from exiting OAC, thus preventing them from using other Wi-Fi supplicant programs.
- How will you deploy the configuration?
 - In a UAC network, you can create and save preconfigured OAC settings and save them in a ZIP file to be uploaded to an Infranet Controller. The IC administrator can then associate a specific OAC configuration to a specific role and download preconfigured clients from the 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* thoroughly before configuring OAC for users and become as familiar as possible with all of the options available.

Chapter 9, “Sample Administrative Workflows,” provides sample workflow scenarios for performing common administration tasks, such as setting up single sign-on for users.

Odyssey Access Client Administrator Tools Overview

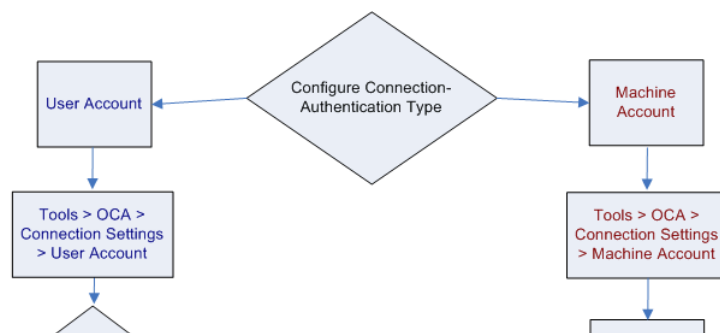
You can preconfigure OAC and deploy a common configuration to multiple users with “push” technology software deployment products. These are third-party products used to distribute software to multiple users at the same time. You can also update existing clients with new or modified configuration settings that reflect your current network security policy. The Odyssey Access Client Administrator tools let you select individual OAC features and hide, disable, or lock individual settings before deploying the configured OAC client to users.

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

To use the Odyssey Access Client Administrator, select **Tools > Odyssey Access Client Administrator** from the Odyssey Access Client Manager menu bar. You can also double-click the `odClientAdministrator.exe` application in the directory where OAC is installed. The default location is `C:\Program Files\Juniper Networks\Odyssey Access Client\Odyssey Access Client Manager`.

When you open the Odyssey Access Client Administrator, the available administrative tools appear as icons as shown in Figure 2 on page 5. To open any of the tools, double-click the icon above the name.

Figure 2: Odyssey Access Client Administrator Icons



Connection Settings

Use this tool to configure specific network connection timings—when the network connection occurs. These connection settings offer flexibility for controlling when authentication completes and accommodates processes such as running startup scripts. The options are:

- Connect to the network after the Windows desktop appears. This connection type requires user login credentials.
- Connect to the network after Windows logon but before the Windows desktop appears. This connection type requires user login credentials.

- Connect to the network before Windows logon. This connection type requires that you install the OAC Graphical Identification and Authentication module (GINA). See “Connect Prior to Windows Logon” on page 34 and “Install the Odyssey GINA Module” on page 38. This connection type requires user login credentials.
- Connect to the network at the machine hardware level (not at the user level) at Windows startup time. See “Configure a Machine Account Connection” on page 35.
- Install and use GINA. See “Configure a Prior to Windows Logon Connection with GINA” on page 38.

See “Process Flow for Configuring Connection Settings” on page 31.

Initial Settings

Use this tool to perform one or more of the following tasks for a user account configuration:

- Preconfigure OAC for groups of users. See “Configure Initial Settings” on page 13 and “Export a Preconfiguration File” on page 61.
- Set up the networks and authentication profiles for users before deploying OAC.
- Create and test preconfigured settings before creating a new custom installer or an update file. See “Test Machine Connection Settings” on page 18.
- Manage SIM cards and SIM card PIN settings. See Chapter 4 in the *Odyssey Access Client User Guide* for details.

See “Process Flow for Initial Settings” on page 12.

Machine Accounts

Use this tool to configure an authenticated network connection for the physical machine rather than for a user. Machine accounts provide a persistent network connection when no user is logged in. See “Configure a Machine Account Connection” on page 35.

See “Process Flow for Machine Account Settings” on page 23.

Permissions Editor

Use this tool to apply customized feature-by-feature restrictions on a user’s ability to use or modify OAC specific features in the configuration. This tool lets you disable settings that you do not want users to change and, in some cases, hide rather than disable some features that users can choose to turn on from a View menu on the Odyssey Access Client Manager tool bar.

Merge Rules

Use this tool to specify the rules for creating a settings update file or a new custom installer file. Merge rules determine how configuration items are added to existing user configurations. You can assign rules that modify current configurations or that prevent users from editing the configurations. You can also use this tool to lock profiles, networks, auto-scan lists, Infranet Controllers, and other settings so that users cannot modify them.

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.

You can also use Custom Installer to merge updated configuration settings with existing machine account (only) settings.

See the following topics:

- “Process Flow for Deployment” on page 57.
- “Process Flow for Updating User Account Settings” on page 60.
- “Process Flow for Updating Machine Account Settings” on page 66.

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 protected access credentials (PACs) for EAP-FAST.

Chapter 2

Configuring a User Account

Use the Initial Settings tool to preconfigure OAC for deployment to one or more users. Configure these settings before you use the Connection Settings tool to configure user account connection timing. Use a dedicated 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.

If you preconfigure OAC for your users, then when a user launches OAC for the first time, OAC opens with those settings. Without preconfigured settings, a user sees the default configuration from Juniper Networks with no networks, profiles, or adapters configured.

Use the Initial Settings tool to define the network connections for a custom installer or a settings update file. The Permissions Editor tool and the Merge Rules tool might also factor into either of these types of configuration.

The settings you choose in the Initial Settings tool become the configuration settings for the rules that you apply using either the Permissions Editor or the Merge Rules tool. Similarly, merge rules apply to those user configurations deployed through custom installers for update files. See “Managing Updates Using Merge Rules” on page 49 and “Process Flow for Deployment” on page 57. You can use the Initial Settings tool to configure features before you apply any merge rules to them.

Initial Settings Tool Overview

The Initial Settings tool looks very much like the Odyssey Access Client Manager. The side bar is identical in either view, so you can configure each of the settings for profiles, networks, auto-scan lists, trusted servers, adapters, and Infranet Controllers in the same way. There are some differences in the options, however, the most significant being that if you are creating a preconfigured copy of OAC for deployment to multiple users, you must use the Initial Settings tool rather than Odyssey Access Client Manager.



NOTE: If you have a FIPS license, the File menu displays options for turning FIPS mode on and off.

The options on the Tools menu in the Initial Settings tool differ from the options on the Odyssey Access Client Manager Tools menu. The File menu in the Initial Settings tool does not include the Forget Password and Forget Temporary Trust options available in Odyssey Access Client Manager. These are local user options that do not apply for a configuration distributed to multiple users.

Tools Menu Options for Initial Settings

The Tools menu in Initial Settings tool includes the following options:

- Reload and Test Initial Settings—Tests the initial configuration before deploying it to users. See “Configure Connection Timing for a User Account” on page 17.
- SIM Card Manager—A Subscriber Identity Module (SIM) card is an electronic card present in some mobile wireless device and used to identify a subscriber to the network. You can use a SIM card for OAC authentication if your client computer has a SIM card reader.

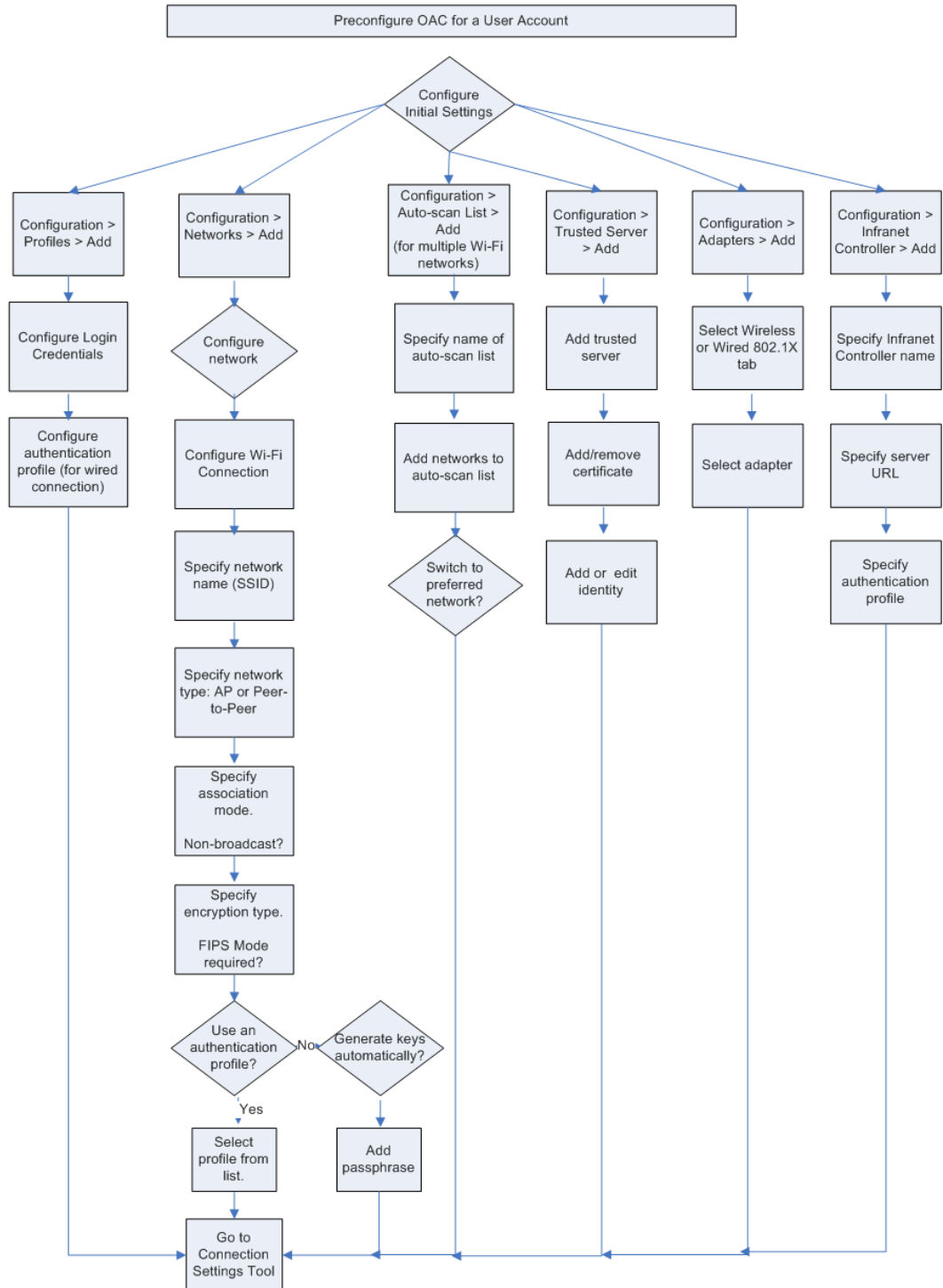
You can use OAC to manage the Personal Identification Number (PIN) on your SIM card hardware. See the discussion on managing SIM card PIN settings in the *Odyssey Access Client User Guide*.

- Logs—Displays the current contents of the `debuglog.log` file. See the discussion on viewing log files and diagnostics in the *Odyssey Access Client User Guide*.
- Preferences—Toggles the display of the system tray icon, the control panel icon, or the Odyssey Access Client Manager splash screen.
- Windows Logon Settings—Allows you to override the default network connection timing for all users to whom you deploy the default configuration image. See the discussion on managing Windows logon settings in the *Odyssey Access Client User Guide*.
- Options—Shows the following categories of settings organized as separate tabs:
 - Security
 - Enable session resumption: Restricts session resumption for any session older than the time that you set.
 - Enable automatic reauthentication: Enables periodic automatic reauthentication and sets the reauthentication frequency setting.
 - Enable server temporary trust: Lets you authenticate to a network whose authentication server is not yet configured as trusted in the Trusted Servers dialog box.
 - Prompt for smartcard PIN: Prompts for a smart card PIN.
 - Interfaces
 - Wireless suppression: Defaults to a wired network connection whenever it is available in order to preserve wireless bandwidth for users who do not have a wired connection.

- Manage wired/wireless adapters: Configures OAC for any wired or wireless adapter automatically.
- Preemptive Networks—Lets you specify an auto-scan list of preferred networks that always overrides any network or auto-scan list currently enabled in the Wi-Fi connection dialog box.
- EAP-FAST—Controls when OAC prompts for EAP-FAST credentials.
- Notifications—Manages the display of notification messages relating to authentication and network connection status.
- Default Login Name—Lets you modify the default login name prompt format that appears in any authentication profile you create. The option appears in Odyssey Access Client Manager only if your administrator has enabled it. Infrequently used, it allows you to set up a login name format when the network to which you need to connect has a different login name format requirement from the configured default.

Process Flow for Initial Settings

Figure 3: Process Flow for Initial Settings



Configure Initial Settings

Double-click the **Initial Settings** tool in the Odyssey Access Client Administrator.

Configure the following sets of features in the Initial Settings tool in much the same way that you configure them in the Odyssey Access Client Manager. Do this for an individual user or for a group of users to which you deploy a common configuration image. You can create more than one configuration image if different groups of users require different settings or if you need to apply more restrictions to one group than for another.

The following categories of settings appear under Configuration in the Initial Settings tool sidebar.

- Profiles—Preconfigure the authentication settings that correspond to a specific network that requires authenticated access. See the *Odyssey Access Client User Guide* for instructions on configuring authentication profiles. (A wired 802.1X connection required an authentication profile.)



NOTE: Your authentication server may not support all of the EAP authentication methods available in OAC. Best practices recommend knowing in advance which methods the authentication server allows before setting up authentication in OAC.

- Networks—Configure the default networks for this user or for a configuration image to deploy to multiple users. See the *Odyssey Access Client User Guide* for instructions on configuring networks.
- 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. See the *Odyssey Access Client User Guide* for instructions on configuring auto-scan lists and features such as wireless suppression.
- 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 updates. Then configure a trusted server for users in the Initial Settings tool. You can configure the trust settings individually. See the *Odyssey Access Client User Guide* for instructions on configuring trusted servers and adding or removing certificates.

To manage merge rule settings for Trust configuration, refer to “Set Merge Rules for Trust” on page 53. You can now manage merge rule settings, such as locking, for individual certificate and identity entries.

- Adapters—Preconfigure the wired or wireless adapters users can have. 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 machines. See the *Odyssey Access Client User Guide* for instructions on managing network adapters.

- Infranet Controllers—Preconfigure one or more Infranet Controllers for users. When you preconfigure Infranet Controllers for your users, note that the **User may not disconnect from this IC** option in the Initial Settings tool lets you lock a user connection to a specific Infranet Controller so that the user cannot disconnect from it. This feature maintains host checker policies and endpoint integrity checks as long as the user is connected to the Infranet Controller. This option is available only in the Initial Settings tool.

When users run OAC for the first time, they typically see the settings that have been preconfigured in the Initial Settings tool. You can use the same configuration settings for:

- A custom installer
- A settings update file
- Preconfigured settings for export to an Infranet Controller



NOTE: Before creating 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.

Manage Windows Logon Settings

Select **Tools > Windows Logon Settings** to override the default setting for network connection timing. This option supports users whose configuration is based on a preconfigured GINA connection timing and provides the ability to override the default setting. This lets a user connect to a network other than the default connection configured for OAC, in which case logon credentials might be different. See “Connect Prior to Windows Logon” on page 34 for a complete description of the logon timing options.



NOTE: Changing the login timing can affect other startup processes.

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

For example, if users can log on to a domain with cached credentials and if the network connection is configured to occur prior to Windows logon, users can change the connection timing to connect to the network after the desktop appears.

Caution on Overriding Default Windows Logon Settings

The **Tools > Windows Logon Settings** option in the Odyssey Access Client Manager lets users override the default network connection timing. This is normally set up using the Connection Settings tool. The purpose of this setting is to accommodate users who have different connectivity requirements at login time. For example, an OAC configuration distributed to multiple users might contain predefined networks for most corporate users. However, users in a remote location may need to connect to other networks and the requirements for login timing may differ. This option lets those users override the default login setting without needing administrative privileges. This option is not used frequently.



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

If default login settings are overridden and if you use the OAC GINA module, users can configure a network connection that takes place before Windows logon. Users can override default network connection settings that you configure unless you have restricted them with the Permissions Editor.

Users cannot override trusted server configuration if OAC is set up to connect before Windows logon. The only way to change the trust setting for a Windows logon connection is to modify those settings in the Trusted Servers dialog box of the Initial Settings tool.

Configure the Login Name Format

Select **Tools > Options Default Login Name** from the Initial Settings tool to specify the default login for all new OAC users. The default login name option that you specify might require user input if you specify a custom format. In that case, the user see a prompt for the custom login name. See “Specify a Custom Login Name Format” on page 16.

The resulting user default login name applies under the following circumstances:

- The default login name appears automatically in the Login Name box 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 box blank. When a user to whom you deploy the profile runs OAC, the Login name box will be populated with the individual user’s Windows logon name.
- The default login name is populated automatically for profiles when a user imports an OAC script that includes a profile with a blank user name.



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.

Specify a login name format from the Options dialog box. See the following topics:

- “Specify a Custom Login Name Format” on page 16—Use this for inserting text to prompt the user with the correct login name format the first time they use OAC.
- “Configure Domain-Decorated or Undecorated Login Names” on page 16—Use this for specifying the Windows logon name format to use in all profiles.

Specify 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 could 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 box appears. Select the **Default Login Name** tab.
2. Select **Prompt for login name using the following prompt**.
3. Enter the prompt text to instruct users on how to enter the login name.
4. Select **OK**.

Configure Domain-Decorated or Undecorated Login Names

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

1. Select **Tools > Options** from the Initial Settings tool. When the Options dialog box appears, select the **Default Login Name** tab.
2. Select one of the following Windows logon name formats:
 - **Decorated Windows logon name**—Use the default domain-decorated Windows logon name format of *Domain_name\Logon_Name*.
 - **Undecorated Windows logon name**—Use the Windows logon name without any domain name decoration.
3. Select **OK**.

Configure Connection Timing for a User Account

If you are not using machine-level authentication, users connect to the network by providing login credentials. Note, however, that there are timing options for network authentication that determine when the authenticated connection completes. Configure these settings after you have completed the user account configuration settings using the Initial Settings tool.

To configure a user network connection:

1. Double-click the **Connection Settings** tool.
2. Select the **User Account** tab.
3. Select the connection timing option you prefer. See “About Network Connection Timing” on page 32 for specific instructions and details.
4. Save your settings and close the Connection Settings tool.
5. Disable any configuration features you that need to restrict or lock using the Permissions Editor tool.

Test Configuration Settings

This topic describes about how to test the configuration for users or machine connections before you create a custom installer to deploy it.

The Reload and Test Initial Settings option loads the configuration defined in the Initial Settings tool to Odyssey Access Client Manager and attempts a network connection. If the connection fails, try to troubleshoot the failure like any other failed connection, based on error messages and the entries in the log file.

To test your user connection settings, follow these steps:

1. Double-click the **Initial Settings** tool.
2. Select **Tools > Reload and Test Initial Settings** from the Initial Settings tool.
3. Select **OK**. This permanently deletes your current Odyssey Access Client Manager settings and loads your settings from the Initial Settings tool into the Odyssey Access Client Manager.
4. Test all the connections through the Wi-Fi or Ethernet connection dialog box of Odyssey Access Client Manager. Any modifications that you make in the Odyssey Access Client Manager are not reflected in the Initial Settings tool.
5. Return to the Initial Settings tool to correct any connection problems and retest the connections as necessary.

Test Machine Connection Settings

The network connections you want to test must be configured and set for connection type configured in the Machine Accounts tab of the Connection Settings tool.

To test machine connection settings:

1. Double-click the **Connection Setting** tool.
2. Select the **Machine Account** tab.
3. Select **Leave the machine connection active**.
4. Select **OK**.
5. Double-click the system tray icon to open the Odyssey Access Client Manager, and view the status of your connection(s).
6. Return to the Machine Account tab to correct any connection problems and retest these connections, if necessary.
7. If you modified your connection settings, select the **Machine Account** tab in the Connection Settings dialog box and restore the previous settings.

Control Network Adapters and Other Wi-Fi Supplicants

You can control the degree of flexibility users have to manage network adapters or to use other Wi-Fi supplicant programs. (OAC is the Juniper Network Wi-Fi supplicant program.) By default, users can add or remove network adapters from the OAC configuration and exit from OAC.

In many cases, it may be beneficial to allow users this type of flexibility. For example, users can use adapters with third-party wireless supplicants to access test networks.

However, this flexibility can also be used to defeat corporate network policies. Using a wireless access client other than OAC may allow users to bypass restrictions set in Odyssey Access Client Administrator. For example, users could use a Wi-Fi adapter with another wireless supplicant program to access non-corporate networks using unapproved protocols in a locked-down configuration. Users could also use unapproved protocols that are disabled in OAC.

A user with a non-802.1X wired network card that is not managed by OAC could transmit unencrypted data.

You can manage this risk as follows:

- You can prevent such scenarios by configuring OAC to automatically manage any wired or wireless adapter present on the user's endpoint computer and then lock this setting in the Merge Rules tool before deploying OAC.

Select **Tools > Options > Interfaces** options from the Initial Settings tool and configure OAC to automatically configure and bind to any wired or wireless network adapter on the machine. As long as OAC is running, it configures any network adapter attached to the user's machine.

- You can use the Permission Editor to prevent users from exiting OAC. Select **Do not allow users to exit Odyssey**.
- OAC has a feature that allows external programs to disable the OAC service. You can use the Permission Editor to prevent external programs from disabling OAC. Select **Do not allow users to disable Odyssey**. You can also use the Merge Rules tool to lock settings and prevent users from changing them.

Chapter 3

Configuring a Machine Account

This topic contains the following information:

- Machine Account Tool Overview on page 22
- Process Flow for Machine Account Settings on page 23
- Enable a Machine Account Connection on page 24

A machine account configuration authenticates a physical machine to a network, instead of a user. This type of configuration 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 statically defined user account consists of any valid login credentials whether or not they exist in Active Directory.

Use a machine account to connect a machine to the network before a user logs in. This can be done using a preconfigured user name and password or, in a Windows environment, with the machine's actual Active Directory credentials or a certificate.

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

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

Machine authentication and user authentication are not the same. However, you can configure a machine connection to transition to a user-level connection once the user logs in to the network and then resume a machine connection after the user logs out.



NOTE: After configuring a machine account and saving the settings in a file, a reboot is required once the configuration settings have been installed on the client machine.

Machine Account Tool Overview

The Machine Account tool is similar to the Initial Settings tool. The sidebar is identical in either view, so you can configure each of the settings for profile, networks, auto-scan lists, trusted servers, adapters, and Infranet Controllers in the same way. There are some differences in the options, however.

Double-click **Machine Account** in the Odyssey Access Client Administrator to open the Machine Account tool.

The File menu in the Machine Account tool does not include the Forget Password or Forget Temporary Trust options available in Odyssey Access Client Manager. These are local user options that do not apply for a broad-based configuration.

The Tools menu options in the Machine Account tool has fewer options than the Odyssey Access Client Manager Tools menu.

Click **Tools > Options** in the Machine Accounts tool. You see these tab categories:

- Security
- Interfaces
- Preemptive Networks
- Notifications

The options in each of these categories are the same as selecting **Tools > Options** in Odyssey Access Client Manager.



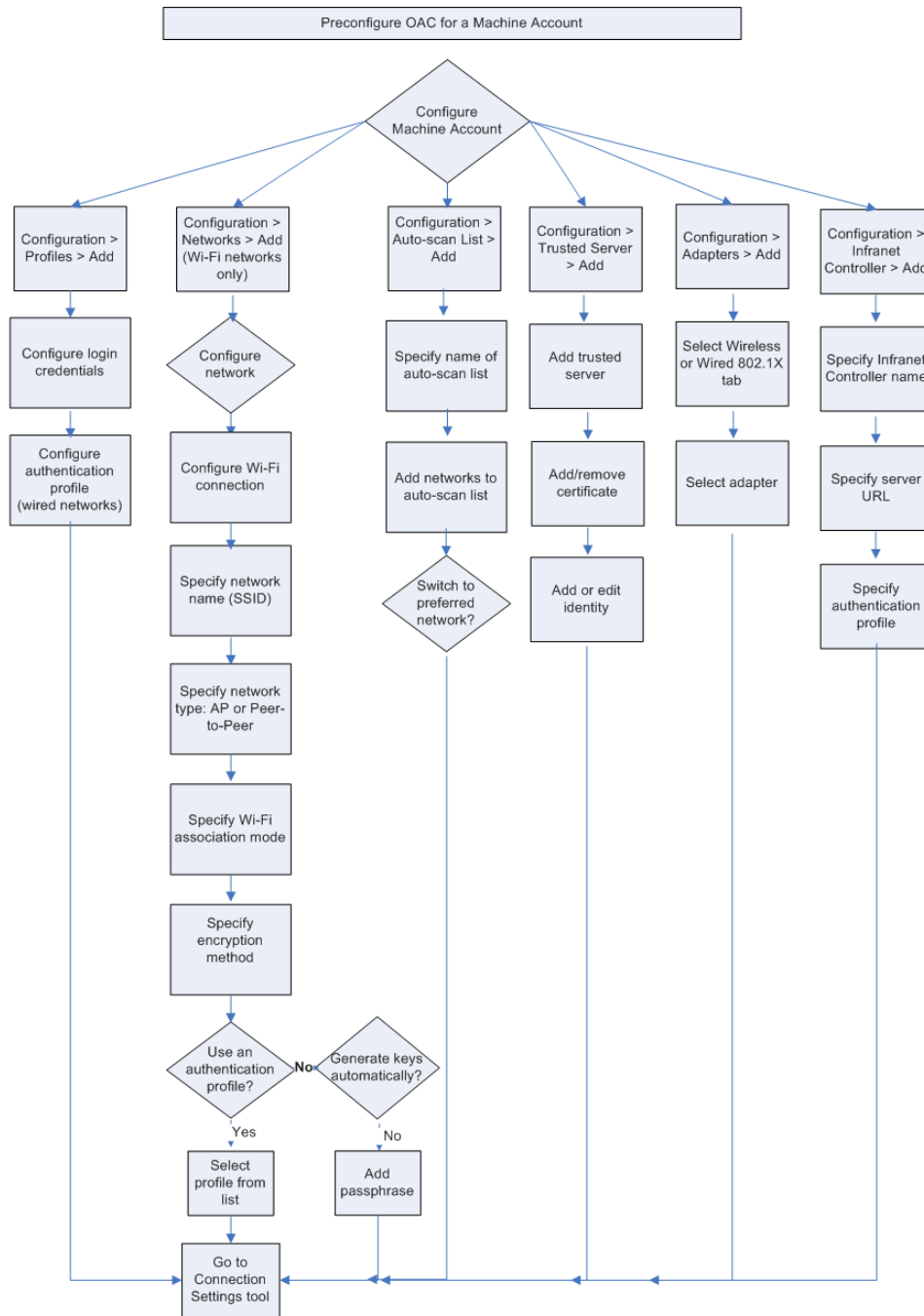
NOTE: Two options, **Enable server temporary trust** and **Prompt for smartcard PIN**, appear dimmed in the Machine Accounts tool because they are unavailable.

The following options that are present in Odyssey Access Client Manager do not appear in the Initial Settings tool:

- Odyssey Access Client Administrator
- Survey Airwaves
- Diagnostics
- Run Script
- Check New Scripts

Process Flow for Machine Account Settings

Figure 4: Process Flow for Machine Account Settings



Enable a Machine Account Connection

To configure a machine account in the Connection Settings tool:

1. Double-click **Connection Settings** and select the **Machine Account** tab.
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 configure 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.

Configure Machine Account Settings

Configure the following sets of features in the Machine Account Settings tool in much the same way that you configure them in the Odyssey Access Client Manager. Do this for an individual user or for a group of users to which you deploy a common configuration image. You can create more than one configuration image if different groups of users require different settings or if you need to apply more restrictions to one group than for another.

The following categories of settings appear under Configuration in the Initial Settings tool sidebar.

- Profiles—Preconfigure the authentication settings that correspond to a specific network that requires authenticated access. Refer to the *Odyssey Access Client User Guide* for instructions on configuring authentication profiles. (A wired 802.1X connection required an authentication profile.)



NOTE: Your authentication server may not support all of the EAP authentication methods available in OAC. Best practices recommend knowing in advance which methods the authentication server allows before setting up authentication in OAC.

- Networks—Configure the default networks for this user or for a configuration image to deploy to multiple users. Refer to the *Odyssey Access Client User Guide* for instructions on configuring networks.

- 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. Refer to the *Odyssey Access Client User Guide* for instructions on configuring auto-scan lists and features such as Wireless Suppression.
- 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 updates. Then configure a trusted server for users in the Initial Settings tool. You can configure the trust settings individually. Refer to the *Odyssey Access Client User Guide* for instructions on configuring trusted servers and adding or removing certificates.

To manage merge rule settings for Trust configuration, refer to “Set Merge Rules for Trust” on page 53. You can now manage merge rule settings, such as locking, for individual certificate and identity entries.

- Adapters—Preconfigure the wired or wireless adapters users can have. 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 machines. Refer to the *Odyssey Access Client User Guide* for instructions on managing network adapters.
- Infranet Controllers—Preconfigure one or more Infranet Controllers for users. Click the **User may not disconnect from this IC** check box to lock a user connection to a specific Infranet Controller. The use case for this feature is to be able to maintain host checker policies and endpoint integrity checks as long as the user is on the network. This option is available only in the Initial Settings tool. Refer to the *Odyssey Access Client User Guide* for instructions on configuring networks.

Machine Account Profile Options

You can configure networks, profiles, auto-scan lists, trusted server, adapters, and Infranet Controllers for a machine account. The only networks, profiles, adapters, or Infranet Controllers that are used for machine connections are those you configure in the Machine Account tool.

Set 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.

Set 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. See the discussion on configuring authentication 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 box 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 the discussion on 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, EAP-FAST options, and authentication methods that require user interaction, such as those associated with tokens, do not apply for machine account settings. Thus, the Profile Properties dialog box in the Machine Account tool varies slightly from that of the Odyssey Access Client Manager.

Configure 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.

To use machine credentials for authentication:

1. Select **Configuration > Profiles > Add** in the Machine Account tool and select **Use machine credentials** on the **User Info** tab of the Add Profile dialog box.

If you select **Use machine credentials**, OAC uses the machine credentials created when the computer is joined to a domain for authentication. If you do not select this option, OAC uses whatever username is provided as a login name.

2. (Optional) Select a realm name to decorate the machine credentials in the Realm (optional): @ box (located below the Use machine credentials check box). 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. Select the **Permit login using password check box** unless you are authenticating with TLS.

When you have configured the machine credentials, open the Connection Settings tool. Select the **Machine Account** tab and select **Enable network connection using machine account**.

EAP Methods that Support Machine Credentials

Machine credentials are valid only with EAP-TTLS or EAP-PEAP. Select one or both 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 box, as necessary. See the *Odyssey Access Client User Guide* for instructions on selecting authentication protocols for a machine account profile.

Enable Machine Authentication

OAC in a UAC network supports Active Directory machine authentication and endpoint assessment. This means that you can configure a machine account for integrity checking.



NOTE: Once you install an OAC machine account on a user machine, you must reboot the machine (manually) after the installation process is complete.

To enable this feature:

1. Double-click the **Machine Account** tool and click the **Profiles** icon from the sidebar.
2. In the User Info tab, specify a login name or select **Use machine credentials**. Optionally, specify a realm name other than the default.
3. Click the **TTLS** tab and select **EAP** as the inner protocol; then select **JUAC** as the inner EAP protocol. (These settings are in place by default.)



NOTE: If an endpoint integrity check fails for a machine-level connection, there are no remediation instructions or other notifications displayed because there is no user interface. (The connection is established before Windows logon completes.) In this case, the machine could be redirected to a protected VLAN where auto-remediation can occur, depending on the policy defined for machine authentication.

Chapter 4

Configuring How and When Network Connections Occur

This topic contains the following information:

- Connection Settings Tool Overview on page 29
- Process Flow for Configuring Connection Settings on page 31
- Configure a User Account Connection on page 33
- Configure a Machine Account Connection on page 35
- Configure a Prior to Windows Logon Connection with GINA on page 38

Connection Settings Tool Overview

The Connection Settings tool lets you configure options that control the type and timing of OAC network connections.

By default, OAC connects to a network after the Windows desktop appears. This is the most common case in which there is no special processing required early in the Windows start-up sequence. However, in some cases you might need to establish an authenticated connection earlier. For example, it might be necessary to enable domain authentication before a user logs in or to execute scripts at specific times during the startup process.

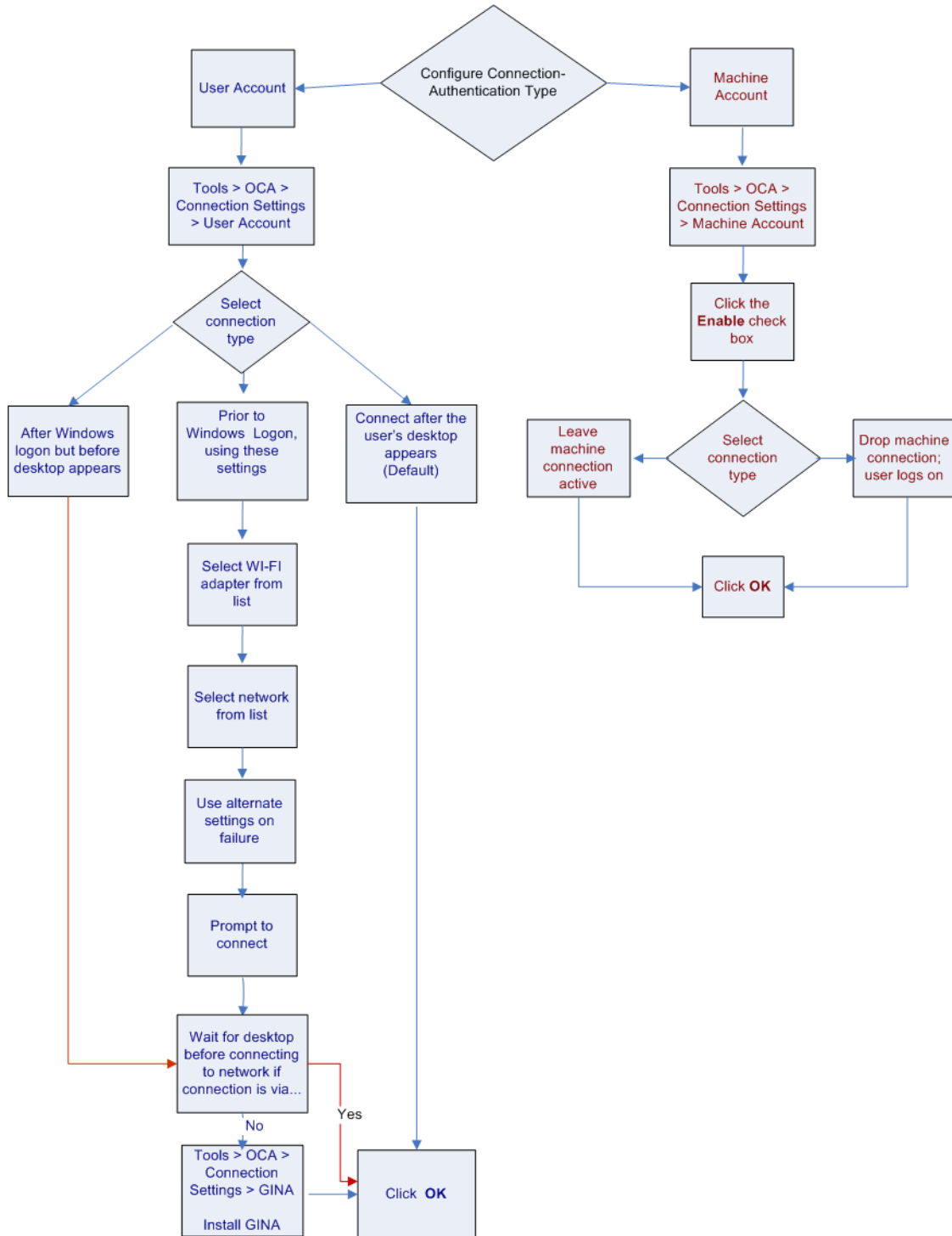
Double-click the **Connection Settings** tool in Odyssey Access Client Administrator. The Connection Settings dialog box contains three tabs:

- **User Account**—Use these settings to configure the default timing of user network connections. At the user level, the network connection requires a user's login credentials and persists as long as the user is logged in.
- **Machine Account**—Use these settings to configure a machine-level network connection at Windows startup time using machine credentials. At the machine level, the network connection uses the credentials of either a user or of a physical computer. A machine connection can persist as long as the machine (computer) is running Windows, regardless of which user is logged in.

- GINA—Use Odyssey Graphical Identification and Authentication (GINA) to control authentication before Windows startup. GINA is a replaceable dynamic link library (DLL) that runs before the Windows logon process in order to gather user credentials needed for authentication. GINA is instrumental in enabling a network connection to occur before Windows logon. Various vendors have their own versions of GINA. The Odyssey GINA module is designed to interact with OAC and is compatible with GINA modules from other vendors. See “Configure a Prior to Windows Logon Connection with GINA” on page 38.

Process Flow for Configuring Connection Settings

Figure 5: Process Flow for Connection Settings.





NOTE: Before configuring user account connection settings, use the Initial Settings tool to configure the user account. Similarly, before configuring machine account connection settings, use the Machine Account tool to configure the machine account settings.

About Network Connection Timing

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

User-Level Connection Options

The three types of user-level connection are as follows:

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

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:

- “Configure Machine-Only Connections” on page 36.
- “Configure Machine Connections that Switch to User Connections” on page 37.

Machine-Level Connection Options

A machine connection to the network can use either the physical computer’s login credentials or the user’s.

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 in, 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 in.
- 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 in 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 in 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.

Configure a User Account Connection

The success of a network connection may depend on the timing you choose. The default option establishes 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—you can select an earlier connection time.

Select the **User Account** tab in the Connection Settings tool to configure a connection to occur before or after the Windows logon prompt appears. Use the options listed under Use Odyssey to connect to the network. The following options control when the login prompt appears:

- 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. This is the default setting.
- 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. See “Connect After Windows Logon, Before the Desktop Appears” on page 33.
- Prior to Windows logon, using the following settings—Select this option if you want the user to establish a network connection before logging in to Windows. See “Connect Prior to Windows Logon” on page 34.

To configure Windows logon features for a custom installer or to update configuration settings, follow the guidelines in “Configure the Login Name Format” on page 15.

Connect After Windows Logon, Before the Desktop Appears

There are two choices for the conditions under which the connection takes place after the Windows 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**. 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 box appears.
- b. Select any adapter that you want used for network connections that occur after the desktop appears.
- c. Select **OK** to close the Select Adapters dialog box.

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

Connect Prior to Windows Logon



NOTE: Before you can configure Prior to Windows Logon connection settings, first select the **GINA** tab in the Connection Settings tool and install the Odyssey GINA module first. See “Install the Odyssey GINA Module” on page 38 and “GINA Compatibility with Other Modules Running at Windows Logon” on page 39.

If your network configuration has a profile that requires a password for authentication, select **Configuration > Profiles > Properties > User Info** and click **Use Windows password** box on the Password subtab. See the discussion on configuring authentication profiles in the *Odyssey Access Client User Guide*.

If your network configuration requires a profile that specifies EAP-TLS or any other certificate-based authentication method, select **Use the login certificate from my smart card reader** on the Certificate subtab of the User Info tab in the Profile Properties dialog box. The options for configuring this type of connection are as follows:

- **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 and a failure code is returned.

One use of this option is to provide an alternate 802.1X wired adapter (and profile) for connections that occur before Windows logon. Another use is to provide an alternate adapter and network in the event of failure. OAC uses the alternate settings automatically to try to establish a connection.



NOTE: The alternate settings option applies to a connection of the same type; that is, if a wireless connection fails, the alternate adapter and network must also be wireless. Failing over from a wireless to a wired connection, or from wired to wireless, is not valid.

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

After selecting this option, select the **Edit Alternate Settings** button and then select an alternate adapter and network.

- **Prompt to connect**—There are three options available that control whether a prompt screen should appear before the network connection at login time. The options are:
 - **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.

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

Configure a Machine Account Connection

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 (a Layer 2 network connection). The network connection and IP address assignment occurs before the user logs in. This is useful for setting up domain-level resources and drive mappings before a user connects.

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.

When you configure machine account connections, you must also configure authentication profile options (such as the credentials and network to use) for machine account connections. See “Machine Account Profile Options” on page 25.

Select the **Machine Account** tab in the Connection Settings tool to connect to the network at machine startup time with machine (rather than user) credentials, and select the **Enable network connection using machine account** check box. Then 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 in. 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 to the network but cannot change the existing OAC configuration.

This option supports 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 are 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 in. 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.

Use this option when the endpoint machine must be connected even when no one is logged in. The machine connection is used to support remote administrative tasks or system service scripts that run during off hours. A user who needs network access from that machine must provide his or her own credentials.

When the user logs off, the connection reverts to a machine account.

If you select this option, set the timing for the user connection by clicking 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, using the following settings

Configure Machine Account Connection Settings

To configure your connection settings based on your selections:

1. Double-click the **Connection Settings** tool in the Odyssey Access Client Administrator to open it.
2. Select a machine network connection option from the Machine Account tab.
3. Configure the network connection settings.
4. Double-click the **Initial Settings** tool to configure new user account settings to let users connect using their own credentials after the machine connection has been established.

Configure Machine-Only Connections

To identify a client machine on the network without 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. In this way, the machine is always connected to the network, even if no user is logged in, as long as the machine is on and Windows is running. This is useful for running scripts at off hours and for remote administrative tasks.

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

1. Double-click the **Connection Settings** tool.

2. Click the **Machine Account** tab and select **Enable network connection using machine account**.
3. Select **Leave the machine connection active**.
4. Select **OK**.
5. Double-click the **Machine Account** tool. Set up your machine network connection, including networks, adapters, and profiles, and close the Machine Account tool. See “Configure a Machine Password” on page 26 for details about specifying machine account profiles.

Configure Machine Connections that Switch to User Connections

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

To configure a machine connection that can switch to a user connection:

1. Double-click the **Connection Settings** tool in the Odyssey Access Client Administrator.
2. Click the **Machine Account** tab and select **Enable network connection using machine account**.
3. Select **Drop the machine connection**.
4. Select the **User Account** tab, select one of the available user authentication timing options, and then select **OK**.
5. Double-click the **Machine Account** tool. The Machine Account dialog box appears. Configure your machine network connection by using the Networks dialog box, the Trusted Servers dialog box, the Adapters dialog box, and the Profiles dialog box. See “Configure a Machine Password” on page 26 for details about specifying machine account profiles.
6. Close the Machine Account tool.
7. Double-click the **Initial Settings** tool. The Initial Settings tool dialog box appears. Configure your user network connection by using the Profiles, dialog box, the Networks dialog box, the Trusted Servers dialog box, and the Adapters dialog box.
8. Double-click the **Merge Rules** tool to lock any configuration features that require locking.
9. Close the Initial Settings tool when you are done.

Configure a Prior to Windows Logon Connection with GINA

GINA is the OAC Graphical Identification and Authentication module. GINA is a replaceable dynamic link library (DLL) that runs before the Windows logon process completes. GINA is instrumental in enabling a network connection to occur before Windows logon. It captures user login credentials from the Windows logon dialog box and delays the actual Windows logon to enable other setup processes and scripts to run first. As soon as a user enters Windows logon credentials, GINA captures and uses them to authenticate the user before the login process and the network connection are complete. In this way, users are authenticated on the network before they have a connection.

Connecting before Windows logon can be helpful when users have startup processes that require network connections to run. This is also a useful tool if your company uses Active Directory 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.



NOTE: On Windows Vista systems, the capabilities described here for GINA are provided by Credential Providers. Odyssey GINA screens are identical on both platforms; that is, the dialog boxes refer to the Credential Provider tool as GINA.

There is a separate login tile (or icon) for GINA accounts on Vista systems. The tile shows the OAC icon .

Install the Odyssey GINA Module

To install the GINA module:

1. Click the **Install Odyssey GINA module** button in the GINA tab of the Connection Settings tool.
2. Configure the prior to Windows logon connection settings under the User Account tab in the Connection Settings tool.

Remove the Odyssey GINA Module

To remove the Odyssey Access Client GINA module:

1. Select the **Remove Odyssey GINA module** button from the GINA tab of the Connection Settings tool.
2. Reboot your machine to complete the GINA module removal.

Use a Third-Party GINA Module and 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 “Remove the Odyssey GINA Module” on page 38.
2. Install the third-party GINA module.
3. Install the Odyssey GINA module using the instructions in “Install the Odyssey GINA Module” on page 38.
4. Reboot your computer. The GINA module installation is not complete until you reboot the machine.

GINA Compatibility with Other Modules Running at Windows Logon

The Odyssey GINA module works by running before the Windows GINA module that presents the Windows Logon dialog box.

Note the following about the interaction between OAC and other login 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 login modules, preserving single sign-on behavior.
- In the case of Novell Client for Windows, OAC uses your Novell credentials at login time without prompting for credential information.

Use GINA with Smart Cards

If you plan to use smart cards with GINA authentication, you need to do the following:

1. Select **Configuration > Profiles > Profile Properties** to create an authentication profile that uses a certificate-based authentication protocol such as EAP-PEAP, EAP-TTLS, or EAP-TLS (with TLS as the inner authentication protocol).
2. Select the **User Info** tab and enter a text string in the Login name box. (If you leave the Login name box blank, authentication will fail.)

If you are using Juniper Networks Steel-Belted Radius for authentication, any text string is acceptable. If you have a different AAA authentication server, the requirements for this string differ.

3. Select the **User Info > Certificate** tab and then select both **Permit login using my certificate** and **Use the login certificate from my smart card reader**.



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. EAP-TLS works only with smart cards at GINA logon time.

4. Select **OK** to save the profile.
5. Configure a network and server trust using the directions in the *Odyssey Access Client User Guide*. Make sure that you associate the profile in Step 1 with this network.
6. Configure any options you require by selecting **Tools > Options** from the Initial Settings tool.
7. Close the Initial Settings tool.
8. Double-click the **Connection Settings** tool and do the following:
 - a. Install GINA if it is not already installed, using the directions in “Install the Odyssey GINA Module” on page 38.
 - b. Set up the appropriate prior to Windows logon connection option on the User Account tab and select the network that you configured in Step 2.
9. Double-click the **Merge Rules** tool and lock the profile that you created in Step 1. In addition, lock any other features that require locking.



NOTE: Turning FIPS mode on disables OAC smart card PIN management.

Note the following about setting up GINA connections:

- You can configure all 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 by selecting **Tools > Windows Logon Settings** from the Odyssey Access Client Manager menu bar.
- You can configure all of the machine account network settings from the Machine Account 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).

- 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.

Chapter 5

Setting Permissions for Individual OAC Features

Permissions Settings Overview

The Permissions Editor tool lets you enable, disable, or hide individual OAC configuration settings and control which features users can see or access. Permissions Editor allows you to decide which authentication protocols are supported on your network, control which wireless network properties your network will support, and disable parts of the Odyssey Access Client Manager interface to provide a simple interface for users who only need to connect and disconnect from a network or Infranet Controller.

You can give advanced users access to more features, such as the ability to create and configure networks or change trust settings. In this case, create and deploy a separate predefined configuration tailored for those users and use Permissions Editor to enable the options appropriate to that group of users. The range of options is extensive, so you can control configurations with the flexibility you need.

Use this tool to apply customized feature-by-feature restrictions on a user's ability to use or modify OAC specific features in the configuration. This tool lets you disable settings that you do not want users to change and, in some cases, hide rather than disable some features that users can turn on from a View menu.

The settings that you configure in the Permissions Editor tool are applied automatically to the machine you use to preconfigure OAC for deployment. You can also create a file to export the permissions configuration to one or more users. See “Task Summary: Merge Update Settings for Machine Accounts” on page 64.

Options that you disable in the Permissions Editor that are not specific to controlling the appearance of the Odyssey Access Client Manager still appear in a menu or dialog box. If users attempt to access disabled options, a dialog box instructs the user that the administrator has disabled that option.

Authentication Protocols

The options in this category enable or disable individual outer EAP protocols, such as EAP-SIM. When individual protocols are disabled, they still appear in the list of protocol choices. However, when a user attempts to save the profile settings by clicking **OK**, an error message identifies which protocols are invalid and prevent the save operation from succeeding until all the settings have been validated.

TLS Inner Authentication Protocols

The options in this category enable or disable individual protocols, such as MS-CHAP. When individual protocols are disabled, they still appear in the list of protocol choices. However, when a user attempts to save the profile settings by clicking **OK**, an error message identifies which protocols are invalid and prevent the save operation from succeeding until all the settings have been validated.

TLS Inner EAP Protocols

The options in this category enable or disable individual inner EAP protocols, such as EAP-GenericTokenCard. When individual protocols are disabled, they still appear in the list of protocol choices. However, when a user attempts to save the profile settings by clicking **OK**, an error message identifies which protocols are invalid and prevent the save operation from succeeding until all the settings have been validated.

PEAP Inner Authentication Protocols

The options in this category enable or disable individual inner PEAP protocols, such as EAP-POTP. When individual protocols are disabled, they still appear in the list of protocol choices. However, when a user attempts to save the profile settings by clicking **OK**, an error message identifies which protocols are invalid and prevent the save operation from succeeding until all the settings have been validated.

Profile Properties

The options in this category enable or disable the requirement for a valid certificate as part of login authentication.

Options

The options in this category enable or disable temporary trust for users. This option still appears in the Security tab of the Initial Settings > Tools > Options menu even after it has been disabled. Users cannot change it as long as it is disabled.

Network Properties

The options in this category enable or disable specific network options, such as peer-to-peer networks or specific encryption protocols. One of the options in this category lets you disable access to networks that do not broadcast an SSID. This setting turns off access to any wireless network that does not broadcast an SSID, even if that network has been configured in OAC with an SSID. The Permissions Editor settings override the current settings in OAC.

Odyssey Control

This is a security option that prevents users or external programs from editing the Windows Registry to disable OAC. In conjunction with the options in the Initial Settings tool for managing all adapters, it prevents users from using a different and unauthorized wireless client to access protected network resources. See “Control Network Adapters and Other Wi-Fi Supplicants” on page 18.

User Interface Settings

Use the settings in this category to remove the Odyssey Access Client Administrator or License Keys in the Help menu. You can also turn off the display of individual settings in the Odyssey Access Client Manager sidebar, and prevent users from editing the Windows Registry to disable OAC in order to use a different wireless access client to circumvent the network security policy.



NOTE: When disabling access to Odyssey Access Client Administrator, you can disable your own access to this tool. You can restart it from *drive:\Program Files\Juniper Networks\Odyssey Access Client\odClientAdministrator.exe*.

User Interface—Hide Configuration Sections

The options in this category hide individual configuration folders in the sidebar (Profiles, Networks, Auto-Scan Lists, Trusted Servers, Adapters, and Infranet Controllers) or hide the entire Configuration section in the sidebar.

Any setting configured as hidden (but not disabled) appears in a View menu in the Odyssey Access Client Manager menu bar. A user can see which settings are hidden in the View menu and turn those settings on again one at a time. When you configure a setting as hidden in the Permissions Editor, that setting resets to being hidden each time the user starts the Odyssey Access Client Manager.

If you do not hide any of the configuration options, the View menu does not appear in the Odyssey Access Client Manager menu bar.

User Interface—Disable and Hide Configuration Sections

The options in this category disable and hide individual configuration folders in the sidebar (Profiles, Networks, Auto-Scan Lists, Trusted Servers, Adapters, and Infranet Controllers) or hide the entire Configuration section in the sidebar. Features that are hidden and disabled are under the administrator's control and do not appear in the View menu. Only the administrator can re-enable them.

Set Permissions or Restrictions

To set up permission or restrictions for individual configuration settings, open the Permissions Editor tool. The settings in the Permissions Editor can have the following states:

- Enable
- Disable
- Hide

Hidden settings are for user interface controls only.

To restrict permissions for Odyssey Access Client Manager features:

1. Select the check box to set the indicated restriction, such as **Disable EAP-SIM**. (Some features, such as the Odyssey Access Client Administrator, are not visible to users if they are disabled.)
2. Select the features to restrict and then select **OK**.

To remove a restriction, clear the check box.

Guidelines for Using Permissions Editor

The following guidelines apply when you set or change permissions or restrictions.

- Any features that you restrict (lock) in the Merge Rules tool are exempt from constraints that you configure in the Permissions Editor tool.
- 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 the discussion on managing network access in the *Odyssey Access Client User Guide*.
- If you select **Disable ad-hoc networks**, users cannot make peer-to-peer connections.
- If you select **Remove Odyssey Access Client Administrator from Tools 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 box).
- If you select any of the Disable authenticated options, users cannot create a network configuration using the specified encryption protocol when they assign a profile to the network connection.
- If you hide (rather than disable) settings, the Odyssey Access Client Manager menu bar displays a View menu showing the hidden settings. Users can toggle options on or off by selecting them. When there are no hidden settings configured, the View menu does not appear.

- You can prevent users from exiting OAC by selecting **Do not allow users to exit Odyssey**. Enabling this settings removes the Exit selection from the OAC icon in the system tray. You can use this setting along with the options to manage all wireless (Wi-Fi) adapters and manage all wired (Ethernet) adapters to prevent users from using a different wireless supplicant program and potentially bypassing the network access security policy.



NOTE: You can lock individual categories of configuration settings to prevent users from changing them by using the Merge Rules tool.

Chapter 6

Managing Updates Using Merge Rules

Merge Rules Overview

Merge rules let you add, replace, or lock configuration settings defined in the Initial Settings tool. Merge rules are intended to help manage OAC configuration updates. Merge rules can be applied to the following categories of configuration settings, each of which is represented by a tab in the Merge Rules dialog box:

- Profiles
- Networks
- Auto-Scan lists
- Infranet Controllers
- Trust
- Other

Use Cases for Merge Rules

Sample use cases for which you might configure rules that affect updates to current user configurations are:

- Updating OAC periodically to a group of users or machines.
- Adding networks, profiles, auto-scan lists, or Infranet Controllers to existing configurations.
- Upgrading users with a newer version of OAC.
- Setting up a locked configuration to be installed on a new machine. (The default setting is to enable all configuration settings.)
- Locking specific settings, such as FIPS Mode or trust settings, that you do not want users to change. You can also lock an Infranet Controller or the corresponding profile configuration and require users to connect to a specific Infranet Controller.

Merge Rule Settings

The individual merge rule settings are as follows. Note that based on the category of settings to which rules are being applied, not all of these rules are available.

- **None**—Do not merge these settings into the existing user configuration but set them for new user accounts.
- **Add if not present**—Add the settings to the existing user configuration but do not overwrite settings with the same names, such as a network or profile name. This is the default option for all tabs of the Merge Rules tool except for the 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. Users can modify these settings.
- **Set, replace if present**—Add the settings to the existing user configuration and overwrite any 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. Users can modify these settings.
- **Lock except user info**—Overwrite all existing user configuration settings, except for any user credential information (username, password, or user certificate) associated with a profile.

This option is available for profiles only. It prevents users from editing any portions of a locked profile except for credentials. Do not specify a username, password, or user certificate for any profile you create in the Initial Settings tool if you plan to apply this type of locking.

- **Lock**—Set or replace all existing user configuration settings and prevent users from editing them. When you lock a feature, OAC deletes the current user settings with the same name and prevents new and current users from editing them. Users see one of the following indicators for locked features:
 - Title bars of dialog boxes are marked as read-only if every feature shown on the dialog box is locked.
 - Text that appears on a tab of a dialog box indicates that the features on the selected tab are locked.

The settings that you make in the Merge Rules affect the 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.

Set Merge Rules

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.

To begin setting merge rules:

1. Double-click the **Merge Rules** tool. The Merge Rules dialog box appears.

2. Select the **Profiles** tab to manage updates for one or more profiles. (Similarly, to manage updates for networks, auto-scan lists, or Infranet Controllers, select the appropriate tab in the dialog box.)
3. Select **Permit only the following profiles** to manage updates for the 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 the **Permit only the following profiles** check box.

 - 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 and use the mouse button to select **Lock**.
4. Select **OK**.

Set Merge Rules for Profiles

To set merge rules for one or more profiles:

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 listing all available merge modes appears.
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.

Repeat these steps for other merge rule modes that you need for updates to authentication profile(s).

Set Merge Rules for Networks

To set merge rules for a network configuration:

1. Select the **Networks** tab in 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**.

Set 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 five configuration modes (**None**; **Add if not present**; **Set, replace if present**; **Lock except user info**; **Lock**) from the menu.



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

3. Select **OK**.

Repeat these steps for other merge rule modes that you want to apply to any profile(s) that you configure in the Initial Settings tool.

Set Merge Rules for Auto-Scan Lists

To set merge rules for auto-scan lists:

1. Select the **Auto-Scan Lists** tab in 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:
 - Users can access only the auto-scan lists you configure in Initial Settings.
 - All components of all user auto-scan lists are locked.
 - Users cannot add new auto-scan lists to their configurations.
 - Any auto-scan lists configured previously in OAC are hidden from users and disabled. To make these visible to users, clear the setting for **Permit only the following auto-scan lists**.

To set merge rules for one or more individual auto-scan lists:

1. Select one or more auto-scan lists from the list.
2. Use the right mouse button to select a configuration mode (**None**; **Add if not present**; **Set, replace if present**; **Lock**) from the menu that appears.
3. Repeat this step for other merge rule modes that you need for updates to auto-scan list(s).

Set Merge Rules for Infranet Controllers

To set merge rules for Infranet Controllers:

1. Select the **Infranet Controllers** tab in the Merge Rules tool. You can lock all Infranet Controllers or set merge rules for individual 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**.

Set Merge Rules for Trust

In previous releases of OAC, merge rule settings for Trust were located in the tab marked Other and merge rule settings applied uniformly to the entire trust table. Trust configuration now offers granular configuration for merge rules and is located in a separate Merge Rules Trust tab.

For example, Acme Corporation has its own Certificate Authority (CA) that was issued by a well-known and widely trusted root CA, such as Verisign:

```
Verisign CA      (set, replace)
  Acme CA       (lock)
    <any>       (lock)
```

The Acme CA can issue certificates for its own purposes, such as for Infranet Controllers. Acme employees must trust those certificates in order for user authentication to succeed. A security officer does not typically expect individual users to configure their own trust settings. Thus, the security officer sets up trust configuration using the Initial Settings tool and uses merge rules to disseminate a locked-down trust configuration to users.

A security officer can update trust settings to add other subordinates to the root (Verisign) or remove them as necessary. In this use case example, Acme CA and all of its subordinates are trusted as long as the Verisign CA is trusted.

Notes on Setting Merge Rules for Trust

- You can add trusted server entries to an existing list of trusted servers. You can also add subordinate certificate identities and set merge rules for them.
- You can configure merge rule settings to lock individual nodes in the trust tree. If you lock an entry in the trust tree, users cannot modify the trust settings for that entry. Lock settings propagate from a node to its descendants.

- Merge rules for either **Add if not present** or **Set, replace if present** that you set for an individual trust node also apply to its ancestors (parent nodes). The rule does not apply to the node's descendants (children) unless you set them separately.
- You can undo a merge rule by selecting **None**.

Set Merge Rules for the Other Tab

Select the **Other** tab in the Merge Rules tool. Use this tab to assign configuration update rules for the following setting categories:

- Windows logon settings
- Security and EAP-FAST
- FIPS Mode
- Options: Interfaces (wireless suppression and network adapters)
- Options: Preemptive networks
- Options: Notifications (settings that control the appearance and display timing for warning and failure messages)

FIPS Mode Settings

(FE Only) Configure your FIPS mode settings 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, you can select **FIPS Mode On** in the Initial Settings tool and lock the **FIPS mode** setting as a merge rule.

See “Task Summary: Merge Update Settings for Machine Accounts” on page 64 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

Deploying Odyssey Access Client

This chapter discusses the methods available for deploying new and updated OAC configurations to one or more users. This includes the ability to export a configuration in XML format (contained in a ZIP file) that can be subsequently imported by an Infranet Controller. The deployment methods are:

- Use an MSI file to deploy preconfigured settings.
- Use an MSI file to deploy updated configuration settings.
- Export configuration settings for use on an Infranet Controller.
- Use a script to deploy updated configuration settings.

Custom Installer Tool Overview

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. You can also use this tool to deploy OAC license keys with the configuration. Once you have the configurations settings saved in an MSI file, you can deploy them using mass-distribution, push technology software, such as SMS. Alternatively, you can export the settings in a ZIP file to be used for deployment from an Infranet Controller.

The configuration settings that you deploy to users are those configured in the Initial Settings, Machine Account, Permissions Editor, and Merge Rules tools as:

- A preconfigured copy of OAC to one or more users and machines.
- Updated OAC configurations for existing users and machines.
- New or updated licenses.

Open the Custom Installer Tool

To open the Custom Installer tool, double-click **Custom Installer** in the Odyssey Access Client Administrator.

Custom installer files and updated user configuration files derive their configuration from the features you set using the Odyssey Access Client Administrator tools, not in the Odyssey Access Client Manager.

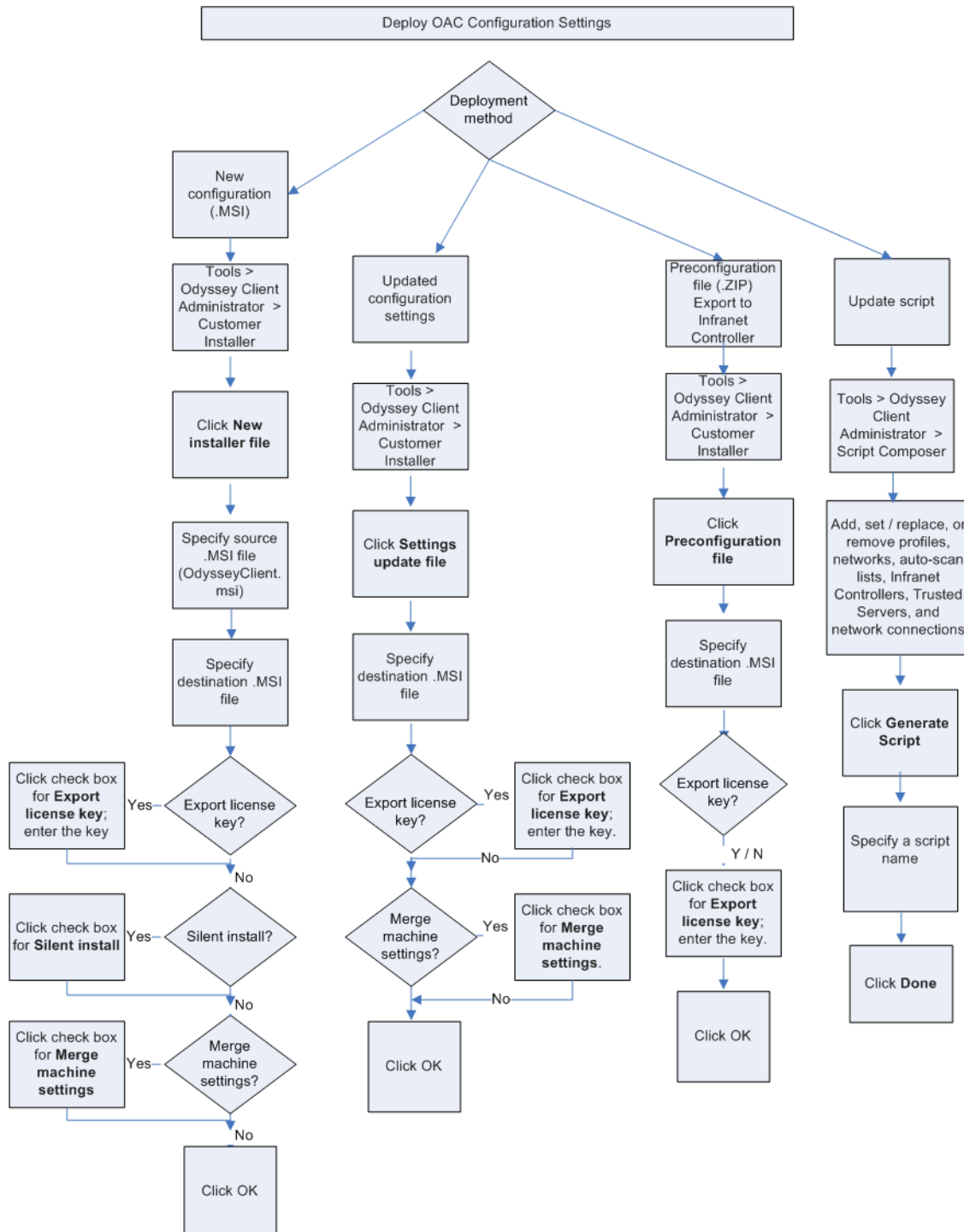
After configuring and testing your configuration settings in the Odyssey Access Client Administrator, use the Custom Installer tool in the Odyssey Access Client Administrator to create a new OAC installer file with the defaults that are configured from your template. See “Configure Connection Timing for a User Account” on page 17 for more information on testing configuration settings. Refer also to “Task Summary: Merge Update Settings for Machine Accounts” on page 64.



NOTE: After configuring a machine account and saving the settings in an MSI file, a reboot is required once the configuration settings have been installed on the client machine.

Process Flow for Deployment

Figure 6: Process Flow for Deployment



Create a New Installer File

To create an installer file:

1. Select the **New installer file** option button.
2. Specify the source installer (**MSI**) file. This file must be a full product installer file for OAC. Enter the filename (along with the path) or select the top **Browse** button. The Select Source File dialog box appears.
3. Use the **Files of type** list at the bottom of the Select Source File dialog box 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. Double-click the source file in the window or select **Open**.
4. Select **Browse** to browse for the desired destination file if required. The Select Destination File dialog box 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; then select **Save**.

Alternatively, you can select **Export license key** and enter a valid license key for the number of copies you intend to distribute.

5. Optionally, select **Silent install** if you want the installation to run without displaying any dialog boxes during the install process. Note that if you select this option and 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.

Guidelines for Creating a New Custom Installer File

Note the following guidelines when you are preparing a new custom installer file for deployment:

- If you create a new custom installer file and do not export a license key, the license for the installed product expires in 30 days.
- The default OAC license in a UAC network is built into the product, so there is never a prompt for a license key. Thus, a custom installer based on the default license key is always a silent install because there is no need to prompt for a license key.
- 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 in the Custom Installer tool, 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. See “Task Summary: Merge Update Settings for Machine Accounts” on page 64.

Create a Custom Update File

A custom update file contains any updated configuration settings you have made. 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 update file:

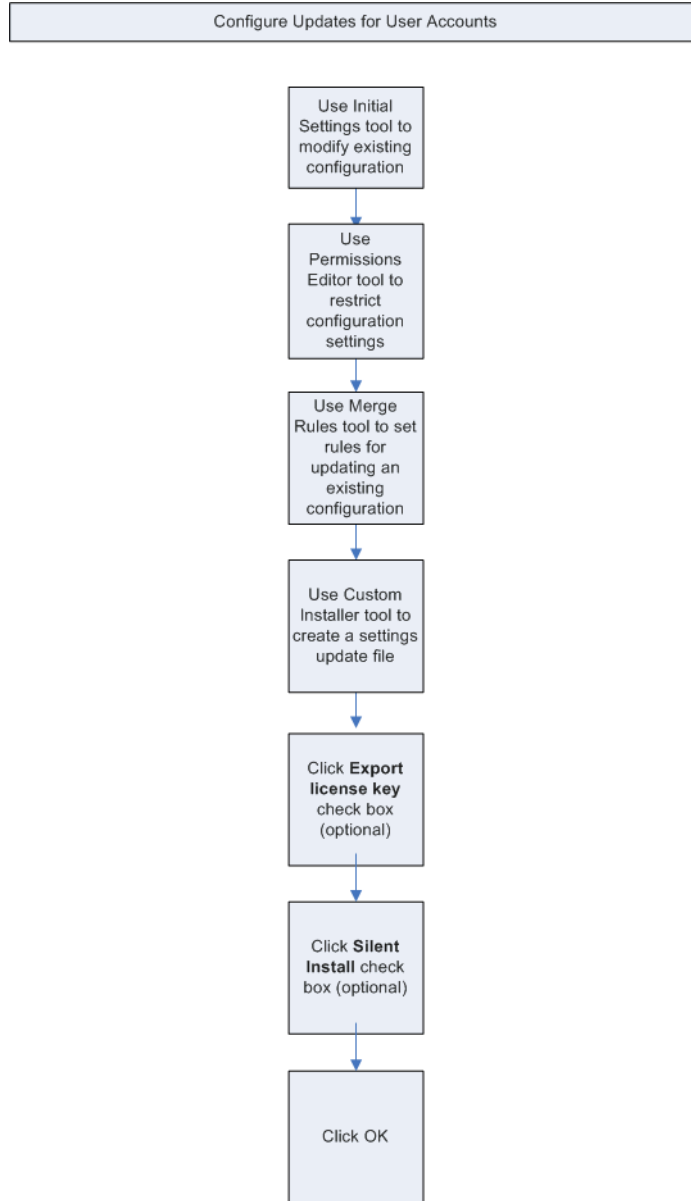
1. Double-click **Settings update file**.
2. Specify the source installer (MSI) file. Enter the file name (and path) or select the top **Browse** button. The **Select Source File** box appears.
3. Select the **Files of type** list at the bottom of the Select Source File dialog box to search for the correct 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 find the desired destination directory if required. The Select Destination File dialog box 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. Select **Silent install** if you want the installation to run without displaying any dialog boxes during the install process.
7. Select **OK** to create the custom installer file.

See Figure 7, “Process Flow for Updating User Account Settings,” on page 60.

To use this tool to update the settings for machine accounts, see “Task Summary: Merge Update Settings for Machine Accounts” on page 64.

Process Flow for Updating User Account Settings

Figure 7: Process Flow for Updating User Account Settings



Export a Preconfiguration File

Use this option to export a detailed OAC configuration file that can be imported by an Infranet Controller and mapped to specific user roles when being deployed to users. In this way, you can tailor OAC configuration files to specific user roles.



NOTE: This option pertains specifically to deploying OAC configurations from an Infranet Controller in a UAC network in which configurations are associated with specific user roles. For details on using this feature, see the discussion on using a preconfigured installer in the *Unified Access Control Administration Guide*.

The following Odyssey Access Client Administrator tools are valid for creating the preconfiguration file:

- Connection Settings
- Initial Settings
- Machine Account
- Permissions Editor
- Merge Rules

The following information may be included in the preconfiguration file:

- All of the preconfigured settings using the Odyssey Access Client Administrator tools listed above.
- A license key (optional).
- A flag to indicate if GINA is installed. Thus, the preconfiguration file can control whether GINA is installed as part of an installation or upgrade.

The preconfiguration file option lets you save OAC settings in a ZIP file so that an Infranet Controller administrator can import them for deployment to users. The contents of the ZIP file include:

- XML files (preconfig.xml and properties.xml)
- Certificates (.pfx files)

To create a preconfigured settings file for import to an Infranet Controller:

1. Select **Preconfiguration file**.
2. Select the **Browse** button and navigate to a location for saving the settings in a ZIP file. The Save Destination File dialog box 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**.

3. Optionally, select **Export license key** and enter any valid license key (Enterprise or FIPS Edition) for the copies of OAC to distribute for a given role.
4. Click **OK**.

For more information about importing a preconfigured ZIP file and mapping that file to user roles on an Infranet Controller, see the discussion on initial configuration of the Infranet Controller in the *Unified Access Control Administration Guide*.

Use the Silent Install Option

You can deploy the custom installer file to install updates “silently” (without requiring interaction by the client user) by selecting the **Silent install** option in the Custom Installer dialog box.

Preconfigure OAC for a Group of Users

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

Set Up an OAC Configuration

The configuration you define 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.

1. If you have not installed OAC on the Windows computer on which you are specifying your configuration, follow these steps before you define a configuration for a custom installer:
2. Configure network configuration and connection options. There are several configuration options. Follow one of the procedures described in these topics:
 - Configure Connection Timing for a User Account on page 17
 - Enable a Machine Account Connection on page 24
 - Configure Machine Connections that Switch to User Connections on page 37
3. Configure feature access or control restrictions to be included in this preconfigured installer in Permissions Editor. See “Setting Permissions for Individual OAC Features” on page 43.

4. Configure locking options to be included in this preconfigured installer in the Merge Rules tool. See “Managing Updates Using Merge Rules” on page 49.
5. Test network connections. When you define the default configuration, you can test each network connection. See “Configure Connection Timing for a User Account” on page 17.

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

Configure OAC Updates for Distribution to Multiple 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 by selecting the **Settings Update file** in the Custom Installer tool.

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.
2. Select **Settings update file**.
3. Select **Browse** to locate a destination file. The Select Destination File dialog box appears.
4. Type the name of the configuration file that you want to save in the Destination box.
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.

Exceptions to Preconfigured Network Connections

The following are exceptions to the network connection options you can specify in a configuration.

- You cannot preconfigure client certificates. If you select **EAP-TLS** under the Authentication tab in the Add Profile dialog box (in the Profiles dialog box 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 box of the Initial Settings or Machine Account tool.

OAC supports automatic certificate selection; that is, if a user has only one certificate, OAC installs it 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.

Task Summary: Merge Update Settings for Machine Accounts

Select the **Merge machine settings** option in the Custom Installer dialog box to update OAC configuration settings for users so that settings are merged with the existing configuration, thus preserving specific parts of the existing OAC configuration. When creating a preconfigured installer for an upgrade or settings update on a system with existing machine account settings configured, you can enable the **Merge machine settings** check box to merge the existing machine settings for Networks, Profiles, Infranet Controllers, and Auto-Scan Lists with the new settings from the custom installer. For any duplicate names, the new setting overwrites the old setting. Auto-scan lists have a slightly different behavior. In the case of matching auto-scan lists, the networks in the new auto-scan list will be added to the bottom of the list.



NOTE: This feature applies to machine accounts only.

This option applies only when creating a custom installer or settings update file. Select the **Merge machine settings** option to perform the following tasks:

- Add new auto-scan lists, Infranet Controllers, networks, or authentication profiles on the target system.

When updating a network, if the SSIDs and network names match the corresponding settings in the current network, the updated network replaces the current version.

The updated configuration overrides individual settings in the current network configuration. If the current network uses AES encryption and the update specifies TKIP, the updated encryption setting replaces the existing one.

- Replace existing Infranet Controllers, networks, or profiles on the target system.

For authentication profiles and Infranet Controllers, if the profile or Infranet Controller name in the update matches the current profile or Infranet Controller name, the update replaces the current version.

The updated configuration overrides individual settings in the current network configuration. If the current profile uses TLS authentication and the update specifies PEAP, the updated authentication setting replaces the existing one.

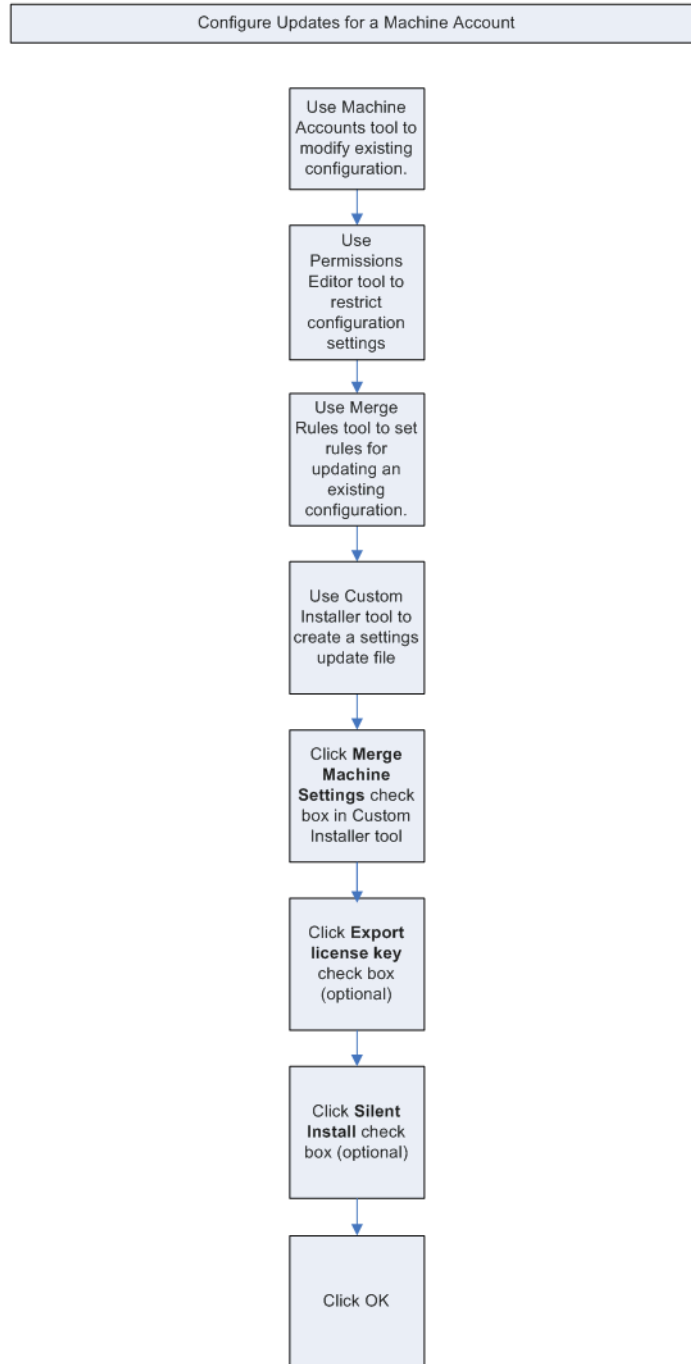
- Merge auto-scan lists from the installer with those on the target machine. If the name of an auto-scan list matches the name of a current auto-scan list, the contents of the update are merged with the current one, thus preserving any existing networks in the current file that are not contained in the update.

This option does not apply to adapters or adapter settings nor does it pertain to the configuration settings defined in the Initial Settings tool. See Figure 8, “Process Flow for Updating Machine Account Settings,” on page 66.

To enable this option, select the **Merge machine settings** check box.

Process Flow for Updating Machine Account Settings

Figure 8: Process Flow for Updating Machine Account Settings



Deploy OAC with Scripts

Use the Script Composer to distribute updated configuration settings to 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 existing configuration settings. You can use a single script to distribute updates for profiles, networks, and scan-lists. The data format of a script is XML.



NOTE: Certificates cannot be included in scripts created with the Script composer.

Script Composer Overview

Use the Script Composer to create configuration scripts to update OAC configurations that add new settings, replace existing settings, or remove settings. You can use scripts to deploy preconfigured OAC settings to platforms other than Windows desktop versions—such as Macintosh, Linux, and Windows Mobile/CE—that do not include the Odyssey Access Client Administrator and, therefore, must be configured on a Windows desktop machine and deployed as a script rather than as an MSI file.



NOTE: The Script Composer uses the Odyssey Access Client Manager settings on the machine where those settings have been configured. Scripts are composed from user data on a template machine, not from system data (settings configured in the Initial Settings tool).

Scripts differ from configuration files in that they are specifically oriented toward data that affects the user running the script, as opposed to system wide data or initial configuration data.

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

The tasks you can accomplish with scripts are:

- **Add**—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 in the copy of OAC on your local machine.
- **Set**—Set or replace current settings. The configuration settings that you can select to add or replace must be in the copy of OAC on your local machine.
- **Remove**—Remove any configuration settings. The settings do not have to be part of the configuration on your local machine.
- **Connect**—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.



NOTE: If there is a configuration setting (such as a network) in a script with the same name and type as a setting that is locked by a merge rule in the current client configuration, the update setting in the script is not updated in the client until that setting is unlocked in the Merge Rules tool. Once the setting is unlocked, the updated values 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.

After you create and distribute a script file, users can access this script by clicking **Tools > Check New Scripts** menu command on the Odyssey Access Client Manager. See “Deploy Incremental Updates with a Script” on page 73.

Create a Script

To create scripts with Script Composer:

1. Set up the configuration to include the settings that you want to add or modify. The Script Composer uses the Odyssey Client Manager settings on the machine where those settings have been configured. Scripts are composed from user data on a template machine— not from system data (settings configured in the Initial Settings tool).

See the *Odyssey Access Client User Guide* for more information about the individual configuration settings.

2. Double-click the **Script Composer** tool. The Script Composer dialog box appears.
3. For each script that you want to generate, configure the Script Composer settings for all items that you want to add, remove, or modify.
4. Select **Generate Script**. The Select Destination File dialog box appears.
5. Specify the file format for your script.
 - To save your script as an autoscript, so that OAC executes the script without user intervention, 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.

Add or Set Profiles with a Script

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

To add or set profiles from the Script Composer:

1. Select **Profiles** under the Add or Set category in the scrolling list. 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 guidelines:

- If you include user identity information such as names or passwords in your selected profiles, 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.

Remove a Profile with a Script

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. Select **Profiles** under Remove category in the scrolling list.
2. Enter the name of any profile you want to remove in the text area provided.

Activate a Profile for a Wired Connection with a Script

To activate a profile for OAC wired connections:

1. Select **Profile** under the Remove category in the scrolling list.
2. Select **Done**.

Add or Set Networks with a Script

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 Add or Set category. 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.

Remove a Configured Network with a Script

You can remove any configured networks as long as you have the correct names (SSIDs) and corresponding descriptions. Alternatively, you can remove all networks with the same SSID 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 Odyssey Access Client 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 the Remove category in the scrolling list.
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. Enter additional networks to remove with this script and press Enter after typing the name and description of each network you want to remove.
4. Select **Done** when you have made your changes.

Activate a Network for a Wired Connection with a Script

To activate a network for OAC wireless connections:

1. Select **Network** under Connect in Script Composer.
2. Select **Done**.

Add or Set Auto-Scan Lists with a Script

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

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

Remove Auto-Scan Lists with a Script

To remove one or more auto-scan lists:

1. Select **Auto-Scan Lists** under the Remove category.
2. Enter the name of any auto-scan list that you want to remove in the text area provided.
3. Enter additional names of auto-scan lists to remove with this script and 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.

Manage Settings in the Other Tab with a Script

Depending on which Script Composer action categories you select (Add or Set), you have one or more options for modifying settings for each of these categories:

- Trusted servers
- Security and EAP-FAST
- Interfaces (wireless suppression and network adapters)
- Preemptive networks
- Notifications (settings that control the appearance and display timing for warning and failure messages)
- Windows logon settings

See the *Odyssey Access Client User Guide* for information about configuring these settings.

Add or Set a Trust Tree with a Script

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

1. Select **Other** under the Add or Set category in Script Composer.
2. Select the **Trusted servers** check box. When users run the resulting script for trust trees that you *add*, new trust entries are inserted in an existing trust tree. When users run the resulting script for trust trees that you *set*, the entire trust tree is replaced.
3. Select **Done**.

Replace Options Settings with a Script

To set (replace) the options settings that you configured by selecting **Tools > Options** in the Odyssey Access Client Manager:

1. Select **Other** under Add or Set in Script Composer.
2. Optionally, select **Tools > Options > Security** or **Tools > Options > EAP-FAST** to include settings that you configure on the Security and EAP-FAST tabs.
3. Optionally, select **Tools > Options > Interfaces > Wireless suppression** to include settings that you configured on the Interfaces tab.

The **Tools > Options > Interfaces** tab also includes options to manage all wired (ethernet) adapters and to manage all wireless (Wi-Fi) adapters.

4. Optionally, select **Tools > Options > Notifications** to manage the appearance of warning and failure notification messages displayed to OAC users.
5. Optionally, select **Tools > Options > Preemptive Networks** to include settings that you configure on the **Tools > Options > Preemptive Networks** dialog box in Odyssey Access Client Manager.
6. Select **Done**.

Remove Networks Using SSIDs with a Script

You can remove networks by SSID instead of using a network name or description syntax. When a user runs the script to 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:

1. Select **SSIDs** under the Remove category in the scrolling list.
2. Enter the SSID of a network to remove in the text area provided. You are not required to use any special syntax.
3. Enter additional SSIDs to remove with this script by pressing the Enter key 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.

Set or Replace FIPS Options (FE Only) with a Script

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

To select or clear FIPS Mode for users:

1. Double-click the **Initial Settings** tool.
2. Select **FIPS Mode On** or **FIPS Mode Off** under the File menu option. These options appear only if you are using a FIPS license.

Deploy Incremental Updates with a Script

You can update OAC configurations for one or more users. For example, if you add new SSIDs to a 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 the *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 Script Composer or the command-line interface.
 - See “Deploy OAC with Scripts” on page 67 for information about creating scripts using Script Composer. Make sure that you save your scripts with the correct extension for autoscripts or regular scripts.
 - See “Create and Load OAC Scripts Using Commands” on page 74. Users cannot run encrypted scripts that you create using the command-line interface.
2. Deliver the script(s) to the directory described by the following path on your user’s computer:

Application Data\Funk Software\Odyssey Client\newScripts

where *Application Data* is typically located in:

volume:\Documents and Settings*username*\Application Data

This may differ for non-English versions of the OS.



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

Depending on your operating system, the physical path to the **Application Data** folder is always the **CSIDL_APPDATA** path used by Windows shell programmers. Once you locate the **Application Data** folder, you can access the scripts under **Odyssey Access Client\newScripts**.

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

- Autoscpts run automatically when detected by OAC.
- Users can run or delete other scripts when they select **Tools > Check New Scripts** from Odyssey Access Client Manager.

If the script is not an autoscpt—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 “Task Summary: Merge Update Settings for Machine Accounts” on page 64.

Create and Load OAC Scripts Using Commands

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

odClientAdministrator *arguments*

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

```
/E[xport] = filename
/I[mport] = filename
/Key = encryptionKey
/N[oSavePrivateData]
/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 guidelines 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 by selecting **Tools > Run Script** in Odyssey Access Client Manager. Use the `.odyClientScript` file extension when you save a configuration if you want users to import the saved configuration by selecting **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 Odyssey Access Client 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 “Deploy Incremental Updates with a Script” on page 73.
- If you use multiple switches, leave a space between each switch command.
- The Odyssey Access Client 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 Odyssey Access Client 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 user 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 Odyssey Access Client 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.
- As with OAC scripts created using the Script Composer tool, exported features are not locked, even if they are locked in your Odyssey Access Client Manager. To lock features, use the Merge Rules tool and create a custom update file. See “Task Summary: Merge Update Settings for Machine Accounts” on page 64.

Chapter 8

Managing Protected Access Credentials

The PAC Manager tool manages (views or deletes) protected access credentials (PACs) for EAP-FAST.

PACs are used to perform mutual authentication with a secure access control server (ACS) 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.

Double-click the **PAC Manager** tool to view or delete the protected access credentials currently in use.

Refresh the PAC Manager Display

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

Delete a PAC

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

Exit from the PAC Manager

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

Chapter 9

Sample Administrative Workflows

This topic presents 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.

Connecting prior to Windows logon can be helpful when users have startup processes that require network connections. For example, you can configure OAC for EAP-TTLS or EAP-PEAP authentication with prior to Windows logon using OAC and the OAC GINA module. Use the OAC GINA module to enable Windows users to connect to the network using Windows logon credentials before login.



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

Single SignOn for TTLS or PEAP

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 the Connection Settings tool.
3. Test the connection settings and update any configuration settings in the Initial Settings tool, the Connection Settings tool, or both, as necessary.

Configure 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.

To configure the network configuration, the steps are identical to those described 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 *Juniper Networks Odyssey Access Client User Guide* for instructions for each of these steps.

Specify User Account Connection Settings and Installing OAC GINA

To configure the Connection Settings and install Odyssey GINA:

1. Double-click the **Connection Settings** tool in Odyssey Access 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 the Connection Settings tool.

Test Prior to Windows Logon Settings

To test prior to Windows logon settings:

1. Double-click the **Initial Settings** tool and select **Tools > Reload and Test Initial Settings**.
2. Open OAC Manager.
3. Check the connection status on the Wi-Fi or Ethernet dialog box, based on the type of network connection you have (wireless or wired).
4. Modify any settings in the Initial Settings or Connection Settings tool and re-test as necessary from the Initial Settings tool.

Index

A

Active Directory	
machine account	26
administrative tools	
overview	5
alternate adapter	
wired 802.1X	34
alternate settings	
edit	34
authentication	
certificate-based	34
flow of events	2
Layer 2	2
Layer 3	2
password-based	34
preconfigure settings	13, 24
profile for smart card log on	40
user	17
automatic reauthentication	10
auto-scan list	
add with script	71
hide	52
lock	52
preconfigure contents	13, 25
autoscript	
delivery	73

B

bypassing Odyssey	35
-------------------------	----

C

certificate	
automatic selection for machine account	25
CA for machine account	26
configure with password-based protocols	40
machine account	26
scripting	69
smart card	
with GINA	41
client updates	63
command-line	
export scripts	74
scripts from	74
compatibility	
GINA	39
configuration	
alternate	34
client update	63
custom	

installer, creating	55
deploy settings	50
export to an Infranet Controller	14
lock settings	50
machine connection	22
machine name	26
planning	3
push	63
remove settings	67
replace settings	50
set or replace settings	67
testing settings	17
configuration settings	
test	10
connecting	
wired networks	
overriding Odyssey GINA	35
connection	
control Windows logon timing	33
settings	
GINA requirement	34
Connection Settings	
overview	29
uses	5
create script	68
credentials	
machine	26
Custom Installer	
administrative tools	55
settings update file	63
uses	7, 55

D

default networks	
configure	13, 24
defaults	
set for initial users	13
deploy	
configuration update	55
license update	55
disable	
configuration options	43
features	45
domain password	
machine	26

E

EAP methods	
for machine credentials	26

EAP-FAST options	
for machine account	26
EAP-TTLS	
smart cards	40
export	
command line	74
license key	59, 62
restrictions	43
scripts	74
G	
GINA	
compatibility with other products	39
install	38
Novell Client credentials	39
overview	38
remove	38
with smart cards	39
Graphical Identification and Authentication	
See GINA	
H	
help menu options	11
I	
import scripts	
command-line	74
Infranet Controller	
lock	49, 53
preconfigure	14, 25
Initial Settings	
administrative tools	13
and customer installer	14
and Merge Rules	9
overview	9
uses	6
inner authentication	
protocols for smart card log on	40
install	
GINA	38
silent	59
installer	
create and customize	55
new file	59
update file	59
L	
license keys	
OAC editions	ix
remove from help menu	46
lock	
auto-scan list	52
features	
Merge Rules	50
FIPS mode setting	54
Infranet Controller	53
network	51
OAC features	43
profile	51
trusted servers	53
Log Viewer	10
login name	
decorated	16
logon	
capture credentials	38
configure default name	15
custom name	16
Windows	
override defaults	15
trust, setting	15
M	
machine account	
administrative tools	22
certificates	26
connection	
before user logon	37
without user logon	36
connection settings	24, 35
connections	
configuring	22
credentials	26
domain password	26
enable	24
overview	21
password credentials	25
restrictions	26
test connection	18
uses	21
Machine Accounts	
uses	6
machine name	
configuration	26
machine-level connection	
purpose	32
settings	35
timing	32
Merge Rules	
custom installers	63
for auto-scan lists	52
for Infranet Controllers	53
for networks	51
for profiles	51
periodic updates	49
set	50
settings	50
use cases	49
uses	7, 50
N	
network	
disable ad-hoc	46
disable any	46
enable automatic connection	67
lock or restrict	51
machine authentication	35
preemptive	11
preferred	11

- remove with script 70
- scripts 70
- network adapters 13, 25
- network connection
 - before Windows logon 33
 - control timing of 32
 - earliest 21
 - machine and user 37
 - machine-level 32
 - options 32
 - machine-only 36
 - require prompt screen 35
 - set timing 14
 - timing options 33
- network connection timing
 - override default setting 10
- networks
 - configure default 13, 24
- Novell Client for Windows
 - compatibility with GINA 39

O

- odClientAdministrator.exe 5
- odyClientScriptAuto 68
- Odyssey Access Client Administrator
 - disable 46
- OdysseyClient.msi 59
- online help xii
- override
 - default connection settings 15
 - Windows logon 35

P

- PAC Manager
 - uses 7
- password
 - for machine account 25
 - machine 26
- permissions
 - enable or disable 45
- Permissions Editor
 - uses 6
- preconfigure 13, 25
 - Infranet Controller 14, 25
 - root CA 13, 25
- preconfigured settings 13, 24
- prior-to-Windows logon
 - override 35
- product documentation xii
- profile
 - activate with script 69
 - configure with scripts 69
 - restrict or lock 51
- prompt to connect
 - options 35
- push
 - configurations 63

R

- realm
 - machine credentials 26
- reauthentication
 - automatic 10
 - frequency setting 10
- release notes xii
- remove auto-scan list
 - with script 71
- restrictions
 - logon settings 40
 - OAC features 43
 - password 40
 - PIN prompt 40
 - remove 46
 - token 40
 - user account settings 40

S

- save
 - custom installer 55
 - settings update files 63
- script
 - activate a profile 69
 - add auto-scan list 71
 - add or replace network 70
 - add or set profile 69
 - certificates 69
 - command-line, from 74
 - data format 67
 - deliver files to users 73
 - destination file 68
 - directions 73
 - manage EAP-FAST settings 71
 - manage network adapters 71
 - manage notifications 71
 - manage preemptive networks 71
 - manage security settings 71
 - manage trust settings 71
 - manage Windows login settings 71
 - manage wireless suppression 71
 - networks 70
 - profiles 69
 - remove auto-scan list 71
 - remove network 70
 - remove profile 69
 - SSIDs, removing 72
- Script Composer
 - defined 67
 - uses 7
- session resumption 10
- settings
 - initial user defaults 13
 - Merge Rules 50
 - predefined 9
 - update files 63
- silent
 - install 58
 - script export 74

SIM Card Manager	10	timing options	33
Single sign-on	5	Windows logon settings	14
skipping Odyssey	35		
smart card			
EAP-TTLS	40		
use with GINA for Windows log on	40		
with GINA	40		
SSID			
removing with scripts	72		
Subscriber Identity Module	10		
T			
template			
custom installer, for	55		
test			
administrative settings	17		
test configuration settings	10		
trust			
machine account requirements	26		
trusted root CA			
preconfigure	13, 25		
trusted server			
override	15		
preconfigure	13, 25		
trusted servers			
lock	53		
U			
update	9		
connection settings	67		
EAP-FAST settings	67		
preemptive network setting	67		
profile	67		
scan list	67		
security settings	67		
trusted server settings	67		
user configuration	55, 63		
Windows logon timing settings	67		
wireless suppression setting	67		
upgrade			
custom installers for	55		
user account			
restricted options	40		
user-level connection			
manage timing of	32		
options	32		
settings	33		
V			
VLAN			
for machine account	24		
W			
Windows GINA			
compatibility with Odyssey GINA	39		
Windows logon			
delay	38		
override defaults	15		
skip	35		