

Radia Client Automation Enterprise

For the Windows, Linux, and Macintosh ® operating system

Software Version: 9.00

Installation and Upgrade Guide

Document Release Date: April 2013

Software Release Date: June 2013



Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Persistent Systems shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Persistent Systems or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Persistent Systems.

Copyright Notice

© Copyright 2013 Persistent Systems, its licensors, and Hewlett-Packard Development Company, LP.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Android™ is a trademark of Google Inc.

IOS is a registered trademark of Cisco in the U.S. and other countries and is used under license by Apple.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software written by Daniel Stenberg (daniel@haxx.se).

This product includes OVAL language maintained by The MITRE Corporation (oval@mitre.org).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://support.persistentsys.com/>

This site requires that you register for a Persistent Passport and sign in. Register online at the above address.

For more details, contact your Persistent sales representative.

Support

Persistent Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Submit enhancement requests online
- Download software patches
- Look up Persistent support contacts
- Enter into discussions with other software customers
- Research and register for software training

To access the Self-solve knowledge base, visit the [Persistent Support](#) home page.

Note: Most of the support areas require that you register as a Persistent Support user and sign in. Many also require an active support contract. More information about support access levels can be found on the [Persistent Support](#) site.

To register for a Persistent Support ID, go to: [Persistent Support Registration](#).

Contents

Installation and Upgrade Guide	1
Contents	5
Introduction	11
About this Guide	11
Terminology	11
Abbreviations and Variables	13
RCA Documentation	13
Documentation Map	14
RCA Features	19
Inventory Management	19
Software Management	20
Virtual Application Management	20
Application Usage Metric Collection	20
Patch Management	20
Security and Compliance Management	21
Out of Band Management	21
Operating System Management	22
Remote Management	22
Settings Management	23
Application Management Profiles	23
Mobile Device Management	23
Internet Clients Management	23
RCA Components	25
Radia Client Automation Core Server	26
Functions of the Core Server	26
Radia Client Automation Satellite Server	28
Functions of the Satellite Server	30

Radia Client Automation Agent	31
Installing RCA Core Server	35
Hardware and Software Requirements	35
Installation Prerequisites	35
Core Communication Ports	36
Create the RCA Database	38
Create a Microsoft SQL Server Database for the RCA Core	38
Prerequisites	38
Creating a Microsoft SQL Server Database for the RCA Core	39
Create an Oracle Database for the RCA Core	40
Prerequisites	40
Creating an Oracle database for the RCA Core	40
Installing Core	42
Post Installation Configuration	43
Installing Core in Silent Mode	44
Installing Core Using msixexec.exe	45
Installing Core Using setup.exe File	46
Windows Services	46
Installing RCA Satellite Server	47
Hardware and Software Requirements	47
Installation Prerequisites	48
Installing RCA Satellite Server	49
Post Installation Configuration	50
Unattended Configuration of RCA Satellite Server	51
Using the Customized XML File	52
unattended.xml File Parameters	53
Using the Default unattended.xml File	54
Proxy Server on Linux	55
Installation Prerequisites	55
Installing Proxy Server on Linux	55
Starting and Stopping the Proxy Server for Linux	57
Windows Services	57

Installing RCA Administrator Tools	59
Installing RCA Administrator Tools on Windows	59
Installation Prerequisites	59
Installing RCA Administrator Tools Using Wizard	60
Installing RCA Administrator Tools using Command Line	61
Installing RCA Administrator Tools on Linux and Macintosh	63
Installation Prerequisites	63
Installing RCA Administrator Tools Using Graphical User Interface	64
Installing RCA Administrator Tools Using Command Line	65
Installing Batch Publisher	66
Installation Prerequisites	66
Installing RCA Batch Publisher for Windows	66
Installing RCA Batch Publisher for Linux	67
Installing Batch Publisher on Linux using Graphical User Interface	67
Installing Batch Publisher on Linux using non-Graphical Method	68
Post Installation Task	68
Installing Application Usage Manager Administrator	69
Installing RCA Agent	71
Installing RCA Agent on Windows	71
Hardware and Software Requirements	71
Installation Prerequisites	72
Agent Communication Ports	72
Preparing for RCA Agent Installation	73
[Properties] Section in Install.ini	74
[Args] Section of Install.ini	77
[Objects] Section of Install.ini	80
Using Customized Scripts	81
Installing RCA Agent using Wizard	83
Installing RCA Agent on Standalone Device	85
Installing RCA Agent Using Command Line	85
Installing RCA Agent using Logon Script	87
Installing RCA Agent in Lockdown Mode	87

Adding Lockdown Properties	88
Adding [SecurityFolders] Section in Install.ini	88
Setting Access Control Lists (ACLs)	89
Installing RCA Agent on Linux and Macintosh	91
Hardware and Software Requirements	91
Installation Prerequisites	92
Prerequisites for running RCA on 64-bit Red Hat Enterprise Linux	93
Graphical Installation	93
Local Installation	94
Remote Installation	95
Silent Installation	96
Customizing the Installation Configuration File	96
Using Customized Scripts	98
Non Graphical Installation	99
RCA Daemons	100
Installing RCA Agent on HP Thin Client Devices	101
Installing RCA Agent on Windows Thin Client Devices	101
Installing RCA Agent using Wizard	102
Installing RCA Agent in Silent Mode	102
Installing RALF	103
Installing RALF in Silent Mode	103
RALF Command Line Parameters	103
Installing RCA Agent on a Linux Thin Client Devices	104
Installing RCA Agent on Linux based Thin Client Devices	105
Installing RALF on Linux (Debian or ThinPro)	105
Uninstalling RCA	107
Uninstalling RCA Core Server	107
Repairing RCA Core	107
Uninstalling RCA Satellite Server	108
Repairing RCA Satellite Server	108
Uninstalling RCA Administrator Tools	108
Uninstalling RCA Administrator Tools on Windows	108

Uninstalling RCA Administrator Tools on Linux and Macintosh	109
Uninstalling Batch Publisher	109
Repairing RCA Administrator Tools	110
Repairing RCA Administrator Tools on Windows	110
Modifying RCA Administrator Tools	110
Modifying RCA Administrator Tools on Windows	111
Uninstalling RCA Agents	111
Uninstalling RCA Agent from Windows	112
Uninstalling RCA Agent from Linux and Macintosh	112
Uninstalling RCA Agent on HP Thin Client Devices	113
Repairing RCA Agent	113
Repairing RCA Agent on Windows	113
Modifying RCA Agent Installation	114
Modifying RCA Agent Installation on Windows	114
Upgrading RCA	117
Upgrading RCA Core Server	117
Hardware and Software Requirements	118
Installation Prerequisites	118
Upgrade Process	118
Task 1: Back up the Existing RCA Core Server Installation	119
Task 2: Upgrade the Core Server	120
Task 3: Restore RCA Data	121
Task 4: Upgrade the SQL/Oracle Database	123
Task 5: Update HP Live Network Content	124
Task 6: Set the Patch Management Options	124
Task 7: Upgrading Deployed Components	124
Upgrading RCA Satellite Servers	125
Hardware and Software Requirements	125
Installation Prerequisites	125
Upgrade Process	125
Task 1: Back up the Existing Satellite Server Installation	125
Task 2: Upgrade the Satellite Server	126

Task 3: Restore RCA Data	127
Task 4: Synchronize Satellite	128
Upgrading Satellite Server Using RCA Console	128
Upgrading Proxy Servers	129
Upgrading Proxy Server to Satellite Server	129
Upgrading Proxy Server to Satellite Server Using RCA Console	130
Upgrading RCA Agent	131
Prerequisites	131
Upgrading RCA Agent on Windows	132
Upgrading Using RCA Installation Service	132
Upgrading Agent Using RCA Core Console	134
Upgrading Using Installation Media	134
Upgrade Scenarios: Lockdown and Non-Lockdown Mode	134
Upgrading RCA Agent on Linux and Macintosh	137
Upgrading Using RCA Installation Service	138
Upgrading Using Installation Media	146
Upgrading RCA Administrator Tools	148
Upgrading the RCA SQL/Oracle Database Manually	149
SQL Database Tables that must be Upgraded	150
Troubleshooting	155
Planning RCA Deployment	157
Separating Roles Among Satellites	157
Distributing Messaging Load	158
We appreciate your feedback!	161

Chapter 1

Introduction

Radia Client Automation Enterprise is a real-time, policy-based, desired state management client management solution that automates the administrative tasks for the physical and virtual clients in highly complex and ever changing environments.

The desired state approach ensures that all client devices in your infrastructure are in adherence with the state information stored for the device in a central database. To achieve the desired state, RCA enforces policies and delivers the required configurations or data files to the client device without any manual intervention.

About this Guide

This guide provides a general understanding of RCA as well as instructions for installation and basic configuration of the RCA infrastructure. This guide also provides information to help you understand how RCA fits into an existing enterprise environment by introducing, at a high-level, the RCA components, their capabilities, and how they relate to one another.

This guide provides information on how to upgrade RCA from a supported older version to the latest RCA version.

Terminology

The following terms are used frequently in this publication:

Administrator

The system administrator who uses the RCA Core Console, RCA Satellite Console, and Radia Client Automation Administrator tools to configure and maintain the RCA environment.

Agent computer

A computer (workstation or server) that has the RCA agent software installed on it. It can also be referred to as a device.

Current computer

A device that is currently in use or is active in the network.

Desired state

The state of a device as defined by the configuration parameters you set in the RCA Configuration Server Database (CSDB). These parameters include policy for software and patches.

Device

A piece of hardware, such as a computer or ATM, that can be either a managed device or a target device.

Radia Client Automation Administrator

A set of Radia Client Automation Administrator tools (including the Agent Explorer, Packager, Publisher, CSDB Editor, and the AMP Editor) that you use to manage the RCA environment.

RCA agent

The agent software (such as the RCA Application Manager, RCA Patch Manager, RCA Inventory Manager, and RCA OS Manager agents) that runs on the managed device and communicates with the RCA Core and Satellite server.

RCA agent connect

The process by which a managed device communicates with the RCA Core and Satellite server.

RCA Configuration server (Configuration server)

A server that configures and maintains the desired state for your enterprise devices and agent computers. In conjunction with RCA Configuration Server Database, Configuration server stores application data and RCA agent-device information, and distributes application packages based on the policies that are established by an administrator. The Configuration server can manage an RCA agent's desired state, deliver and maintain RCA policies, contact devices causing them to initiate data requests and desired-state requests.

RCA Configuration Server Database (CSDB)

An object-oriented database that stores all the information needed to manage assets on a device, including software, patches, OS images, and data that RCA distributes. The database also stores policies that determine which users are entitled to which resources, and security and access rules for administrators. CSDB contains data organized in a hierarchical structure with four levels: files, domains, classes, and instances.

RCA Core server

A central server that maintains the authoritative data repository, policy entitlements, and desired state configuration parameters for all resources being managed on clients. The Core server includes a complete set of RCA infrastructure necessary for authentication, centralized administration, reporting, configuration, resource deployment, and Satellite server communications.

RCA Satellite server

A server that acts as an access point for RCA agent communications and resources. The Satellite server is an intermediary between the Core server and the RCA agents. In a typical corporate computing environment, numerous Satellite servers are located in "network proximity" to the RCA agents that they serve to enhance the performance. Satellite servers synchronize with an upstream server that enables Satellite servers to provide the resources requested by RCA agents.

Managed device

A computer, ATM, or other piece of hardware, that is managed by RCA.

Non-current computer

A device which no longer exists in the network for various reasons, such as, the device has been removed from the network or it has been renamed.

Package

A unit of software or data that can be published to the CSDB.

Policy

A rule that defines the services that are entitled to a subscriber, an agent computer, or a managed device.

Resolution

The process by which a managed device achieves its desired state.

Service

A group of related packages, methods, or behaviors organized into manageable units.

Target device

A workstation or server on which you want to install, replace, or update a software.

User or subscriber

The person who uses managed applications on a managed device.

Abbreviations and Variables

Abbreviations Used in this Guide

Abbreviation	Definition
RCA	Radia Client Automation
Core and Satellite	RCA Enterprise environment consisting of one Core server and one or more Satellite servers.
CSDB	Configuration Server Database

Variables Used in this Guide

Variable	Description	Default Values
<i>InstallDir</i>	Location where the RCA server is installed	For a 32-bit OS: C:\Program Files\Hewlett-Packard\HPCA For a 64-bit OS: C:\Program Files(x86)\Hewlett-Packard\HPCA
<i>SystemDrive</i>	Drive label for the drive where the RCA server is installed	C:

RCA Documentation

The RCA documentation is available on the media at the following location : <media_root>\Documentation. After installing the Core server, you can access the documentation using the Windows **Start** menu or the Client Automation Enterprise Documentation shortcut link on the desktop. You can also access the documentation using any computer that has access to the

Core server computer using the following URL: `http://<HPCA_HOST>:3466/docs` where, *HPCA_HOST* is the name of the server where RCA Core server is installed.

Documentation Map

The following table lists all documents available for Radia Client Automation 9.00

RCA 9.00 Documentation Set

Guide Name	Description
RCA Enterprise Administrator User Guide	Describes the RCA Administrator tools for the Windows, Linux, and Macintosh operating systems and how to use these tools to administer the Radia Client Automation environment. The details of using RCA Administrator CSDB Editor are explained in the RCA Enterprise CSDB Editor Online Help.
RCA Enterprise Application Management Profiles User Guide	Describes how to enable the deployment and management of complex software products that are typically required on the managed clients and servers in a Client Automation environment. For example, Symantec Antivirus, Microsoft® Office 2007, Microsoft SQL Server, Oracle, Apache, and Internet Information Server.
RCA Enterprise Application Manager and Application Self-Service Manager Reference Guide	Describes the reference information for RCA Application Manager and Application Self-Service Manager. For example, using RCAagent in lockdown mode and understanding various message codes generated in RCAenvironment.
RCA Enterprise Application Manager and Configuration Server REXX Programming Guide	Describes how to create RCA REXX methods to customize processing for your RCA-managed computing environment.
RCA Enterprise Application Self-Service Manager Online Help (Linux and Macintosh)	Describes how to use the Application Self-Service Manager on Linux and Macintosh platforms.
RCA Enterprise Application Self-Service Manager Online Help (Windows)	Describes how to use the Application Self-Service Manager on Windows platform.
RCA Enterprise Application Usage Manager Reference Guide	Describes how to assess and obtain reports on software usage in your RCA environment. For example, you can know who is using what applications, and how often.

RCA Enterprise Configuration Server Database Reference Guide	Describes all domains and classes used in RCA.
RCA Enterprise Configuration Server Messages Guide	Describes informational, warning, and error messages, grouped numerically and by Configuration server tasks. It lists Configuration server return codes and reason codes.
RCA Enterprise Configuration Server Reference Guide	Describes the reference information about Configuration server. For example, Configuration server directories, tuning the Configuration server, and customizing the Configuration server processing.
RCA Enterprise CSDB Editor Online Help	Describes how to use the RCA CSDB Editor.
RCA Enterprise Distributed Configuration Server Reference Guide	Describes how to manage multiple Configuration Server Databases (CSDBs) in a networked environment.
RCA Enterprise Installation and Upgrade Guide	Describes step-by-step installation and upgrade procedures for all RCA components. It also describes the features of RCA.
RCA Enterprise Inventory Manager Reference Guide (Unix)	Describes different types of auditing and how to configure the auditing process on UNIX platform.
RCA Enterprise Inventory Manager Reference Guide (Windows)	Describes different types of auditing and how to configure the auditing process on Windows platform.
RCA Enterprise Messaging Server Reference Guide	Describes how to configure and tune Messaging server in your RCA environment.
RCA Enterprise Multicast Server Reference Guide	Describes how to configure and customize the Multicast server processing in your RCA environment.
RCA Enterprise Online Help	Describes all RCA tasks that you can perform through RCA Core Console.
RCA Enterprise OS Management Reference Guide	Describes how to configure OS Management on Suse and RedHat operating systems.

(SUSE AutoYaST and Red Hat Kickstart)	
RCA Enterprise OS Management Reference Guide (Windows)	Describes how to configure OS Management on Windows operating systems.
RCA Enterprise OS Manager Hardware Configuration Management User Guide	Describes how to manage hardware configuration on managed devices before installing the operating systems.
RCA Enterprise Out of Band Management Online Help	Describes how to use out of band management features in RCA.
RCA Enterprise Out of Band Management User Guide	Describes how to configure out of band management in your RCA environment.
RCA Enterprise Patch Management Reference Guide	Describes how to discover, analyze, and deploy patches in your RCA environment.
RCA Enterprise Policy Server Reference Guide	Describes the reference information about Policy server. For example, how to connect to LDAP.
RCA Enterprise Portal Reference Guide	Describes the reference information about Portal, a back-end component in RCA environment. The guide explains the Portal zones and Portal zones containers.
RCA Enterprise Proxy Server Reference Guide	Describes reference information about Proxy server. For example, when to use a Proxy server and how to enhance performance of a Proxy server.
RCA Enterprise Release Notes	Describes what is new in the RCA current release.
RCA Enterprise Reporting Server Reference Guide	Describes the advance features of the Reporting server and how to customize the reports.
RCA Enterprise SSL Implementation Guide	Describes how to set up and use SSL in RCA environment.

RCA Enterprise Troubleshooting Guide	Describes various problems that you may encounter in your RCA environment and their solutions. This guide also describes how to enable trace levels for various RCA components and respective log files.
RCA Enterprise User Guide	Describes various features of RCA and how to perform various RCA tasks to manage the RCA environment.
RCA Enterprise Virtual Application Management User Guide	Describes how to publish, update, and deploy virtual applications—VMware ThinApp and Microsoft Application Virtualization (Microsoft App-V)—in RCA environment.
RCA Enterprise Windows Terminal and Citrix Server Management User Guide	Describes how to manage Windows Terminal Server and Citrix applications in RCA environment.

For information on migrating RCA Classic installation to RCA Core and Satellite installation, see the *Radia Client Automation Enterprise Migration Planning and Best Practices Guide* from HP Live Network at https://hpln.hp.com/system/files/HPCA_Classic_to_Core-Sat_Migration_Planning_and_Best_Practices.pdf.

Chapter 2

RCA Features

RCA provides a suite of features that perform administrative tasks for the physical and virtual clients in highly complex and ever changing environments. These features are designed to replace ad hoc, error-prone, manual processes. RCA automates the deployment, configuration, and management for software, patches, and operating systems. For example, by using Operating System management, you can install or replace operating systems on a device and maintain the device according to policy. By using Patch management, you can automate the process to acquire, install, and maintain patches in your environment. By using Software management, you can manage and deploy packaged software to the managed devices in the environment. By using Security and Compliance management, you can monitor and manage security vulnerabilities and assess which devices are out of compliance across your environment.

RCA provides the following capabilities:

- ["Inventory Management " below](#)
- ["Software Management" on next page](#)
- ["Application Usage Metric Collection" on next page](#)
- ["Patch Management" on next page](#)
- ["Security and Compliance Management" on page 21](#)
- ["Out of Band Management " on page 21](#)
- ["Operating System Management" on page 22](#)
- ["Remote Management" on page 22](#)
- ["Settings Management" on page 23](#)
- ["Application Management Profiles" on page 23](#)
- ["Mobile Device Management" on page 23](#)
- ["Internet Clients Management" on page 23](#)

Inventory Management

RCA enables you to collect device hardware and software information for reporting. The feature is available for managed HP devices and includes BIOS configuration information. You can use a central console to view the inventory information collected on devices. Built-in reporting tools present the data in detailed or graphic views that can be filtered to show devices matching specific criteria.

Administrators can specify what inventory management data is to be collected. An inventory connect is then run on the target computer to retrieve the desired , which is then sent to the RCA server for reporting.

Inventory management enables you to:

- Automatically gather information about software and hardware configurations and consolidates the results into web-based reports.
- Increase manageability of enterprise data by maintaining current inventory information collected across LAN, Internet, and dial-up links, and across a wide array of heterogeneous devices and operating systems.

Hardware Alert Reporting

RCA enables you to configure managed devices centrally to monitor and gather hardware related alerts and events for reporting. The alerts include events such as overheating of the processor, fan stall, memory CRC errors, and hard disk smart errors.

Software Management

RCA enables you to manage and deploy packaged software to the managed devices in your environment. Software management enables:

- Policy-driven distribution of software.
- RCA administrators to automatically deploy required software.
- End users to install the authorized *elective* software.

Virtual Application Management

RCA enables you to publish and update virtual applications in RCA environment. The following two types of virtual applications can be published, deployed, and managed in RCA environment:

- VMware ThinApp
- Microsoft Application Virtualization (Microsoft App-V)

Application Usage Metric Collection

RCA enables you to assess patterns of application usage in your environment. Application usage metric collection enables you to:

- Ensure license compliance within your enterprise.
- Implement license tracking, giving you the ability to purchase and maintain only those licenses that are required.
- Enable OS migration support by prioritizing software distribution based on actual usage.
- View the actual use of application resources using reports.

Patch Management

RCA enables you to discover, analyze, and deploy patches in your environment. Patch management enables you to:

- Acquire patches from vendor web sites.
- Determine the vulnerabilities on the managed devices.
- Deploy applicable patches to managed devices.
- Verify applied patches on managed devices to ensure compliance and security.
- Generate reports that provide information on which acquired and applicable patches have or have not yet been applied to a managed device.

Security and Compliance Management

RCA enables you to detect security and compliance problems on managed devices in your enterprise and quickly assess the severity and scope of the related risk. You can then take steps to remediate these problems. Security and compliance management enables you to monitor and manage the following across your environment:

- **Security vulnerabilities:** Identifies software security and vulnerability issues in the enterprise.
- **Configuration compliance:** Identifies software configuration problems on managed devices in the enterprise.
- **Security tools management:** Identifies what type of security tools are present and enabled on managed devices in the enterprise.

HP Live Network is integrated with RCA. HP Live Network is a subscription service that delivers content updates for Client Automation Enterprise. You can configure RCA to automatically download new security and compliance management content from the HP Live Network on a periodic basis, rather than depend on a manual process. This content includes scanners for clients and detailed information about security vulnerabilities, compliance benchmarks, and security tools—including suggested remediation solutions.

Out of Band Management

RCA enables you to perform out of band management operations on a device when the device is in one of the following states:

- The computer is plugged in but not actively running (off, standby, hibernating).
- The operating system is running.
- The operating system is not loaded (software or boot failure).
- The software-based management agent is not available.

RCA supports Out of Band management (OOBM) for Intel vPro devices and DASH-enabled devices.

OOBM enables you to:

- **Discover**
OOBM enables you to identify hardware and software assets in your environment. This helps you determine specifications for the hardware on devices, identify applications on devices, and compatibility issues.

- **Heal**
OOBM uses KVM (Keyboard, Video, and Mouse) remoting to diagnose and repair software, operating system, and hardware failures.
- **Protect**
OOBM helps you protect vPro devices from malicious software and worm proliferation.

Operating System Management

RCA enables you to configure and deploy operating systems based on the target device's capabilities. You can deploy operating systems to bare metal devices (no existing operating system) or to devices currently running an existing operating system. Operating system management enables you to:

- Reduce the learning curve for administrators because it is a fully integrated component of RCA.
- Improve speed and reliability of operating system deployment.
- Maintain operating systems in the desired configuration and increases service levels.
- Reduce IT costs by simplifying and streamlining the OS management process across multiple platforms.

Using the operating system management features in RCA, you can also perform pre-operating system provisioning tasks that include applying configuration settings to hardware on your target device. You can update the BIOS firmware, configure a disk array controller, or configure the non-volatile RAM of a target device.

Personality Backup and Restore

RCA enables you to migrate individual user settings and data. The details of user files and settings for applications and operating system on individual managed devices are saved on the server before migration. These details are then restored to the original device or a new device after completing the migration.

Thin Client Management

RCA enables you to deploy operating systems and software to HP thin clients, such as HP t5550 Thin Client and HP t5565 Thin Client, running Windows XPE, Windows CE, and embedded Linux.

Remote Management

RCA enables administrators to access and manage devices remotely. Remote management enables you to:

- Take control of problem devices with integrated remote control capabilities in the console.
- Use additional power management capabilities, such as:
 - Power down devices.
 - Reboot devices.
 - Wake-on-LAN.
- Access devices remotely in either the internal or external repository using one of the following connection types:

- Windows Remote Desktop Connection
- Virtual Network Computing (VNC)
- Windows Remote Assistance

Settings Management

RCA enables you to create, modify, and delete settings profiles. The settings profile consists of customized configuration settings for devices, which include settings related to applications, operating systems, and hardware. By creating or modifying a settings profile, you can analyze and parameterize configuration control data for target softwares. Settings management enables you to:

- Create groups of configuration settings for software installed on the managed devices in your environment.
- View reports about the run-time data of the software.

Application Management Profiles

RCA enables you to create and modify application management profiles. These profiles enable you to deploy and manage complex software products (such as Microsoft Office 2007, Symantec Antivirus, and Citrix Presentation Agent) in an RCA environment.

Mobile Device Management

You can manage mobile devices in your enterprise using RCA. A mobile device can either be a smartphone or a tablet running on Android or iOS operating systems. Using RCA, you can entitle software applications, perform audits (collect inventory), and deploy security profiles to these mobile devices. For more information on the supported operating system versions, see the Radia Client Automation Support Matrix available at http://h20230.www2.hp.com/sc/support_matrices.jsp.

Internet Clients Management

Using RCA, you can manage the devices that are outside your corporate network (VPN) similar to the devices inside corporate network. The devices are managed to comply with their desired state. You can manage inventory, software, patching, and vulnerabilities for the devices. OS management is not supported on Internet clients. For more information, see the Managing Internet Clients section in the Radia Client Automation *Enterprise User Guide*.

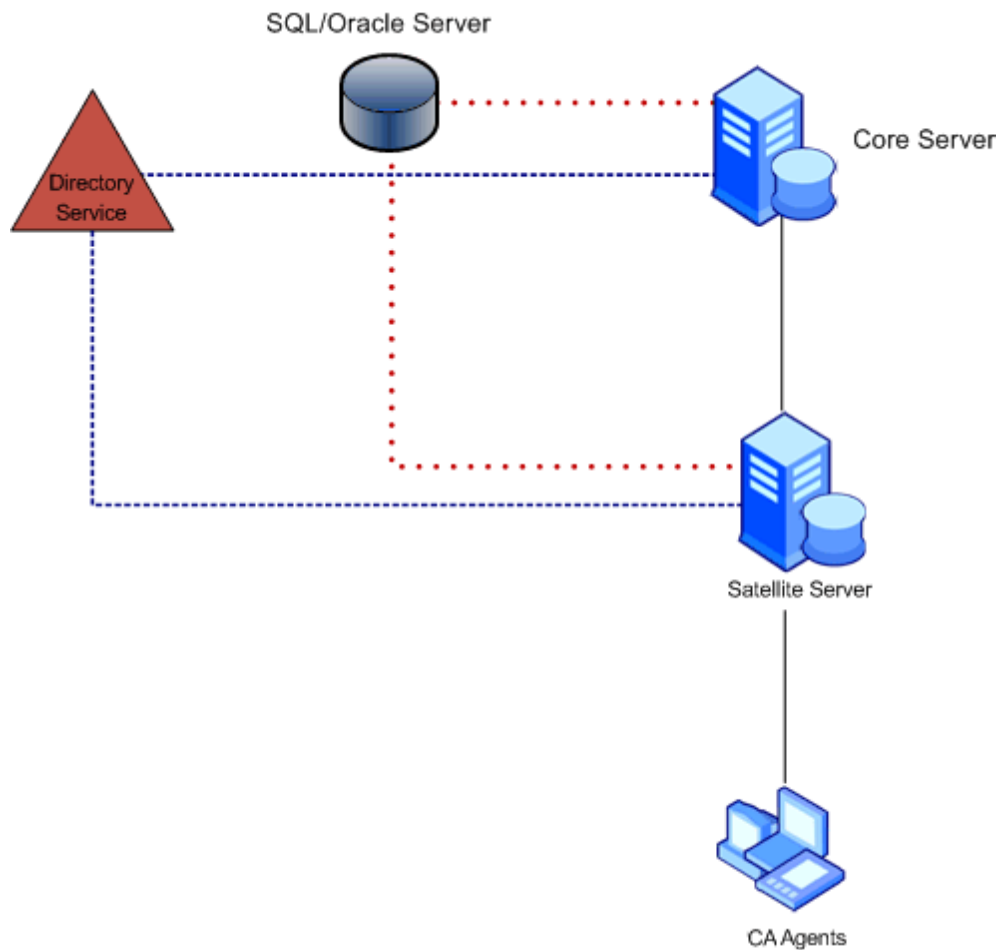
Chapter 3

RCA Components

This chapter explains the components that work together to frame an RCA environment. RCA uses client-server architecture, in which the individual client devices are connected to a central computer known as Core server. You can implement Satellite servers to enhance the performance of your RCA infrastructure. The Satellite servers act as access point to the RCA infrastructure for all RCA client devices. There are three main components required to build your RCA environment:

- Core server
- Satellite server
- Agents

The following image shows how these components are arranged in RCA environment:



Radia Client Automation supports **IP version 4 (IPv4)** and **IP version 6 (IPv6)**. You can use IPv4 or IPv6 for external communication among RCA Core server, Satellite server, and RCA Agents.

Radia Client Automation Core Server

The **Radia Client Automation Core (Core) server** is the critical *authoritative repository* of data for an Radia Client Automation environment. It is the authoritative source for all configuration information and managed content. The Core server maintains all configuration parameters, policy entitlements, and data resources, such as, applications, patches, and OS images, used to manage your clients. The Core server contains all content acquisition sub-systems, such as Patch management, Compliance management, Security Tools management, Settings management, and Vulnerability management. The Core server is also the point of integration with any third-party systems from HP, ISV's, or a customer's own environment.

The Core server provides a central administration point for all of its subservient ("downstream") components, and offers reporting information on their configuration and status. The **RCA Core Console** is the web interface that an administrator uses to centrally manage devices, software, operating systems, and patches, as well as create and view reports based on those managed devices. For example, the RCA Console provides Security and Compliance Management dashboards that show the status of your enterprise at a glance. You can view the aggregated regulatory compliance and security tools information for each managed client device in your enterprise. The features available on the console depend on the privileges assigned to the console user.

The **RCA Administrator (Administrator)** tools are installed as part of Core server installation. These tools provide centralized control of RCA objects and policies. Administrators use these tools to manage the CSDB, prepare applications for management, view RCA agent objects, package and publish software into the CSDB, and customize their environments. You can also publish applications through command line using **RCA Batch Publisher**. Note that RCA Batch Publisher is available as a separate installer and is not installed with RCA Administrator tools. For more information, see ["Installing Batch Publisher" on page 66](#).

The Core server communicates with either Satellite servers or managed devices. The purpose of these communications is to:

- Synchronize data caches with downstream servers.
- Synchronize CSDB with downstream servers.
- Request for policy resolution.
- Send informational messages that provide the status of activities among the servers and managed devices.

Functions of the Core Server

The Core server contains several built-in components that perform various functions to enable you to discover client devices in your network and add these client devices as managed devices to your RCA environment. You can then monitor, configure, audit, and maintain these devices.

By default, the components described in the following table are installed with the RCA Core server installation. These components are pre-configured; minimal information is required during or after the installation.

RCA Core Server Components and Essential Function

Core Server Component	Enabled by Default	Function
Application Usage Manager Administrator *	No	Provides interface to create rules that define the data that is used to create usage reports for the managed devices.
Boot server (PXE)	No	Windows-based Pre-execution Environment (PXE) server for the OS Manager environment.
Boot server (TFTP)	No	Windows-based Trivial File Transfer Protocol (TFTP) server for the OS Manager environment.
Configuration server	Yes	Configures and maintains desired-state information for your managed devices.
Configuration Server Database (authoritative repository)	Yes	Stores the desired-state configuration in a hierarchical structure. The master CSDB on a Core server is the authoritative repository for the replicated CSDB on a Satellite server.
Distributed Configuration server (DCS) (Source)	Yes	Provides support for CSDB synchronization with the downstream server. On a Core server, defines the source for downstream replications of the CSDB to a target Satellite server CSDB.
RCA Core Console*	Yes	A web-based, agent-management interface that enables you to view the status of your enterprise. You can also manage software, patches, and inventory and administer policy for devices in your environment.
Knowledge Base server*	No	Routes the managed device usage data to the database. The Knowledge Base (KB) server monitors a pre-defined location configured by the administrator for managed device usage data and posts this data to the database.
Messaging server	Yes	Routes and posts data that is reported by RCA agents to the appropriate reporting database or server (such as Inventory, Portal, Patch management, Security and Compliance management, Inventory and Application management profile data).
Mobile server	Yes	Routes the configuration data to the Android and iOS mobile devices.
Multicast server	No	Simultaneously sends a single data stream to multiple RCA agents.
OS Manager server	No	Provision and manage operating systems on RCA agent devices.

Core Server Component	Enabled by Default	Function
Patch Management server*	No	Acquires, publishes, and deploys vendors' security patches and bulletins.
Policy server	Yes	Enables administrators to entitle policies to users and devices defined in an existing LDAP data structure. The policy server enables single point of control to authenticate user, access policies, and entitle subscriber. You can use your existing Directory Services also.
Portal*	Yes	A set of web-services that are used to deploy agents and manage RCA infrastructure using a web browser. Provides job-engine support for certain classes of jobs, such as RCA agent deployment.
Reporting server*	Yes	A web-based reporting engine that accesses data from multiple SQL databases for consolidated reporting. It is used to provide reports for Patch management, Usage management, Inventory management, Application management profiles, and Security and Compliance management.
Thin Client server	No	Manage agents on Windows CE thin clients.
Virtualization Management Server (VMS)	Yes	Enables you to manage Microsoft App-V applications. It also imports settings content, and security and compliance content from HP Live Network. Security and Compliance content includes vulnerability content, Security Tools Management (STM) scanner content, and Compliance content.

* These components are unique to Core server; they are not installed on Satellite servers.

Radia Client Automation Satellite Server

The **Radia Client Automation Satellite (Satellite) server** acts as an access point to the RCA infrastructure for all RCA agents. The Satellite servers contain *recoverable* information only because their content is always replicated from the CSDB on the Core server. The Satellite servers can, therefore, be rebuilt or recovered at any time by synchronizing the Satellite server with the Core server or upstream Satellite server.

The Satellite server is an intermediary between the Core server and the RCA agents. In a typical corporate computing environment, numerous Satellite servers are located in “network proximity” to the RCA agents that they serve to enhance their performance. There are no restrictions or limitations on how many Satellite servers can be used. The use of Satellite servers is determined by an administrator and should be based on necessity—the size, scope, and topology of the infrastructure.

Satellite servers synchronize with an upstream Core server. The synchronization enables Satellite servers to provide the resources requested by RCA agents.

It recommends that administrators *do not* make changes to the Satellite server CSDB. A Satellite server's CSDB is a replication of its upstream server's metadata (either a Core server or another Satellite server) and any database changes at this level are lost on the next synchronization with that upstream server.

Satellite servers are configured to enable the appropriate infrastructure services (for example, Configuration services, Messaging services, Proxy services). You can enable a service either by configuring the installation or by making changes in the Satellite Console. You can configure the Satellite servers in the following modes:

- Full-service mode: Typically a data center back-end server with support enabled for Configuration and Messaging services. Full-service Satellite servers can handle nearly all RCA agent requests on their own, without having to forward the request to an upstream Core server. The table [RCA Satellite Server Components and Essential Functions](#) lists the services that are enabled on a full-service Satellite server.
- Streamlined mode: Typically a server that services proxy file services to managed devices. Only proxy services and messaging services are enabled on a streamlined Satellite server. Streamlined Satellite servers have limited functionality. The agent requests that cannot be fulfilled by streamline Satellite server are directed to an upstream full-service Satellite server or Core server. For example, streamlined Satellite servers:
 - May be primarily used to cache and deploy software and patch content to the RCA agents.
 - May have configuration services disabled. Without a local Configuration service enabled, the Satellite servers forward agent requests for desired-state resolution to an upstream full-service Satellite server or Core server.
- Custom mode: The Satellite servers in custom mode enables you to select specific services to enable on the Satellite server. You can also enable configuration services on the Satellite servers in the custom mode.

The **Radia Client Automation Satellite Console** is the web interface that makes it easy to customize or reconfigure the component services. For example, you can designate specific Satellite servers as dedicated OS Manager servers, and disable unnecessary services on those Satellite servers. The features available on the console depend on the privileges assigned to the console user.

The Satellite server provides the following services to its RCA agents:

- Agent Maintenance
- Data Delivery
- Service Catalog
- Service Delivery
- Service Reporting

The Satellite server communicates with either Core server or other Satellite servers. The purpose of these communications is to:

- Synchronize resources.
- Synchronize metadata.
- Request for policy resolution.

- Exchange informational messages between Core server and Satellite servers. These information messages provide the status of activities between the Satellite server and managed devices.

Functions of the Satellite Server

The Satellite server contains several built-in components that perform various functions to enable you to monitor, configure, audit, and maintain managed devices. You can use web interface to customize or reconfigure the component services. The Satellite server components are enabled based on the deployment mode for the Satellite server.

By default, the components described in the following table are installed with the RCA Satellite server installation. These components are pre-configured; minimal configuration is required during or after the installation.

RCA Satellite Server Components and Essential Functions

Satellite Server Component	Function
Boot server (PXE)	Windows-based PXE server for the OS Manager environment.
Boot server (TFTP)	Windows-based TFTP server for the OS Manager environment.
Configuration server	Configuration server that configures and maintains the desired state for client devices in your enterprise.
Configuration Server Database (CSDB) (replicated)	Replicated CSDB that stores the desired state configuration in a hierarchical structure and enables the Satellite servers to resolve the desired state of agents that connect to them.
Distributed Configuration server (DCS) (Source and Destination)	As a target, replicates the Core server CSDB to this Satellite server CSDB. As a source, replicates this Satellite server CSDB to a downstream Satellite server CSDB.
Messaging server	Automatically routes and posts data that is reported by RCA agents to the appropriate reporting database or Core server (such as Inventory, Portal, Patch management, Security and Compliance management, Inventory and Application management profile data). The Messaging server service is always enabled and cannot be disabled.
Mobile server	Routes the configuration data to the Android and iOS mobile devices.
Mobile Device Management	Performs the mobile device management tasks for iOS devices.

Satellite Server Component	Function
server	
Multicast server	Simultaneously sends a single data stream to multiple RCA agents.
OS Manager server	Provisions and manages operating systems on RCA agent devices. OS Manager services store local caches of OS images for deployment to managed devices.
Patch Gateway server	Downloads the patch binary data from vendor websites when requested by the agent and caches it for other agents to use.
Policy server	Uses existing, non-RCA directory services to store and implement RCA policy entitlements. Policy Services enables an external policy directory, such as an Active Directory, to be accessed directly from the Satellite server, for Agent resolution.
Proxy server	<p>Use cache management over HTTP to store and dynamically transmit application data. Proxy server stores local caches of software, patch, and OS image resource data for content delivery to agents. The data is distributed using unicast or multicast. Multicast requires Multicast service to be enabled.</p> <p>RCA Satellite server consists of Apache server data cache and Integration server-based Proxy server components. The Apache server data cache is used to store Patch Manager Gateway (Patch MGR) binaries. The Integration server-based Proxy server data cache is used to store CSDB resource data, such as software, OS Manager, audit, and security data.</p>
Satellite Console	A web-interface using which various administrative and configuration tasks can be performed.
Thin Client server	Manage agents on Windows CE thin clients.

Radia Client Automation Agent

The RCA agent is a software that runs on a client device and communicates with the Core server. The RCA agent consists of RCA Application Manager, RCA Inventory Manager, RCA Patch Manager, and RCA OS Manager agents. If you install RCA Application Manager, you get the sub-features, such as RCA Application Self-Service Manager, PlusHP, and Personality Backup and Restore.

RCA Agent Sub-Features

RCA Agent Feature	Description
RCA Application Manager	This feature enables you to distribute mandatory applications throughout the enterprise.
RCA Application Self-Service Manager	This sub-feature enables users to install, remove, and update optional applications that are available to them in a service list.
RCA Inventory Manager	This feature enables you to collect hardware information and send it to RCA Inventory Manager for collection and reporting.
RCA OS Manager	This feature controls the provisioning of operating systems.
RCA Patch Manager	This feature analyzes and manages patches.
Personality Backup and Restore	This sub-feature enables you to migrate individual user settings and data.
PlusHP	This sub-feature provides Self Monitoring, Analysis, and Reporting Technology (SMART) Drive Alert Monitoring and HP Hardware Alert Monitoring based on HP CMI for HP hardware devices.
RCA Usage Manager	This feature enables you to assess and obtain reports on software usage throughout the enterprise. This feature is not available by default.

The RCA agent is installed on client devices that an RCA administrator wants to manage using RCA. The installation brings the target device under the control of the RCA environment, thereby making it a **managed device**. An administrator deploys the RCA agent to a device, entitles, and then installs software and patches directly to that device or to the group that this device is part of.

The RCA agent enables an administrator to:

- Automate deployment
- Update, repair, and delete applications
- Inspect hardware and software
- Ensure security of the data

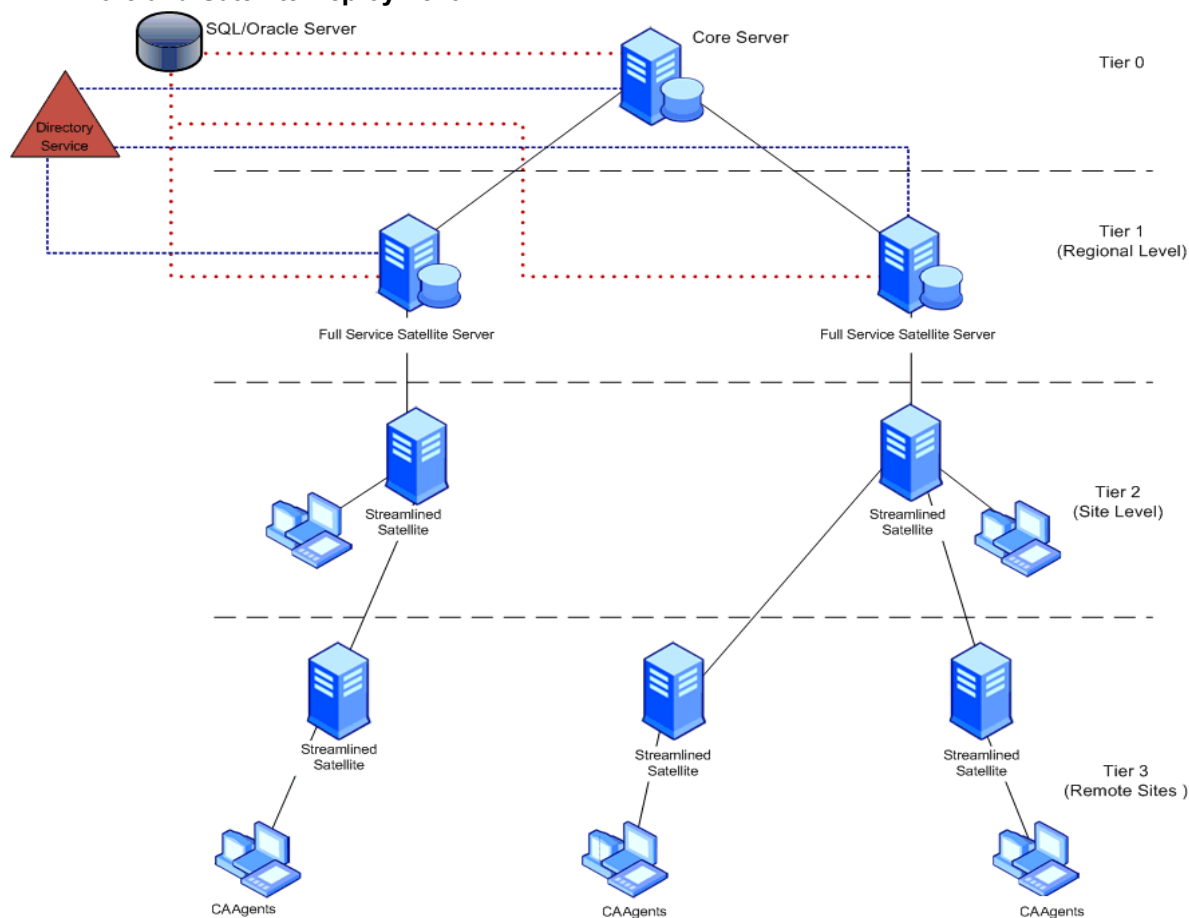
RCA Agent Lockdown Mode

The RCA agent lockdown mode ensures the integrity, confidentiality, and availability of the content and methods that are stored and used by the management agent. This prevents non-privileged users from tampering with critical system-level content or breaching confidentiality by viewing

content they should not have access to. For more information, see the *Radia Client Automation Application Manager and Application Self-Service Manager Installation and Configuration Guide*.

The following figure illustrates how you can deploy RCA components in a distributed and tiered environment.

RCA Core and Satellite Deployment



A typical environment includes a Core server at tier-0 that serves as the upstream host for full-service Satellite servers at tier-1. The Satellite servers configured with tier-1 Satellite server as the upstream host are designated as tier-2 Satellite servers (Streamlined Satellite servers, but can be another set of full-service Satellite servers). You can add more tiers based on your requirement. Streamlined Satellite servers that are at the remote site are the lowest tier of Satellite servers.

You can customize your default RCA environment to improve the overall performance by modifying the default behavior of Satellite servers as described in the appendix "[Planning RCA Deployment](#)" on page 157.

Chapter 4

Installing RCA Core Server

The chapter contains installation requirements to install RCA Core server, and guides you through the process of installing and configuring RCA Core server.

Hardware and Software Requirements

Caution: The Core server should be installed on a clean computer. If the Core server is installed on a computer that already hosts an RCA Satellite server, you receive an error message and the installation ends.

System Requirements for Core Server

The following are the minimum system requirements for installing Core server:

Caution: Some of these requirements are for initial RCA-environment setups. As your RCA environment grows, the space requirements will inherently grow as well, in order to accommodate database expansion and caching.

- 4 GB RAM
- Dedicated server with dual-core processor
- 2 GHz CPU speed
- 8 GB free hard disk space

Platform Support

For the operating system requirements for this release, see the *Radia Client Automation Support Matrix* available at the URL: http://h20230.www2.hp.com/sc/support_matrices.jsp.

You must have an HP passport ID to access this web site.

The *Radia Client Automation Support Matrix* is also located on the distribution media for this product in the \Documentation directory.

You can use Radia Client Automation Enterprise in a Microsoft Direct Access enabled environment. For more information on Microsoft Direct Access, see Microsoft documentation.

Installation Prerequisites

The following prerequisites should be met before installing RCA Core server:

- **Communication Ports**

RCA Core server has default listening ports that *must* be enabled before starting the installation process. For more information on Core server communication ports, see "[Core Communication Ports](#)" below.

- **RCA Database**

Before installing the Core server, you must create an ODBC-compliant database to be used by RCA for management-reporting objects. This database can be either a Microsoft SQL Server Database or an Oracle® Database. For information on how to create databases specifically for the Core server, see "[Create the RCA Database](#)" on page 38.

- **Windows AIK Installation**

If you plan to use RCA for OS provisioning, you should install the Windows AIK on the computer that hosts the RCA Core server and ensure that copies of these utilities are placed at the appropriate location.

You can download the Windows AIK from the Microsoft Download Center (<http://www.microsoft.com/downloads>).

- **Microsoft Data Access Components (MDAC)**

You must install MDAC on the Core server to use Patch management and Usage management. The minimum required version is 2.8. The media for this (MDAC_TYP.EXE) is available in the Microsoft folder of the Setup-Core directory.

Core Communication Ports

Ports **3464** and **3466** are the primary ports used for Core server communications when SSL is not enabled. When SSL is enabled on a Satellite server, SSL is used for all inbound communications. If a firewall is in place on the RCA server's host computer, these ports *must* be added to the firewall "exceptions" list.

To verify if the port is enabled and listening, open the command prompt and type `netstat -a`.

The default ports on which the Core server communicates within RCA environment are listed in the following table:

RCA Core Server Communication Ports

Port	Port Type	Description
127.0.0.1:3461	TCP	RCA Messaging server (nvdkit-hpca-ms.exe)
0.0.0.0:3464	TCP	Default port for RCA Configuration server (ZTOPTASK.exe). It must be available for Core servers.
0.0.0.0:3466	TCP	RCA Apache server (httpd.exe) Main HTTP port that Core server uses for communications with Satellite servers and RCA agents. All unicast data downloads are handled on this port.
127.0.0.1:3467	TCP	RCA Patch Manager server (nvdkit-hpca-patch.exe)
127.0.0.1:3468	TCP	RCA Policy server (nvdkit-hpca-pm.exe)

Port	Port Type	Description
127.0.0.1:3469	TCP	RCA OS Manager (<code>nvdkit-hpca-osm.exe</code>)
0.0.0.0:3466	UDP	RCA OS Manager (<code>nvdkit-hpca-osm.exe</code>) Port required only when the RCA OS Manager is enabled on a Satellite server (by default, it is disabled). It is used by the low-level PXE BootLoader to determine whether a device should be provisioned or re-provisioned.
127.0.0.1:3470	TCP	RCA Thin Client management server (<code>nvdkit-hpca-mms.exe</code>)
127.0.0.1:3471	TCP	RCA Portal (<code>nvdkit-hpca-rmp.exe</code>)
127.0.0.1:3472	TCP	RCA Multicast server (<code>nvdkit-hpca-mcast.exe</code>)
127.0.0.1:3482	TCP/UDP	RCA Mobile server (<code>nvdkit-hpca-mdm.exe</code>)
2xx.0.0.0:9100	UDP	Default port for RCA Multicast server (<code>nvdkit-hpca-mcast.exe</code>)
127.0.0.1:3473	TCP	RCA DCS (<code>nvdkit-hpca-dcs.exe</code>)
127.0.0.1:3474	TCP	RCA Directory Service (<code>slapd.exe</code>)
127.0.0.1:3476	TCP	RCA (<code>hpca.exe</code>)
127.0.0.1:3477	TCP	RCA Tomcat (<code>tomcat.exe</code>)
127.0.0.1:3478	TCP	RCA Tomcat (<code>tomcat.exe</code>)
127.0.0.1:3479	TCP	RCA Database (<code>mysqld-nt.exe</code>)
443	SSL	Port used for “secure HTTP” (HTTPS) communications.
444	SSL	Port used for “secure TCP” (TCPS) communications for RCA Configuration server.
5228, 5229, 5230	TCP/UDP	This port is required to enable communication with the Google Cloud Messaging (GCM) service. RCA uses GCM to send notification messages to the Android mobile devices.
For OOB Management Console-to-vPro Device Communications		

Port	Port Type	Description
162	SNMP	Port for alert management. Port 162 is a standard SNMP port. Alert management conflicts if you are already running an SNMP receiver on the RCA Core server.
9999		Default starting port for communication between the SOL display applet and the server's web application. This can be configured by editing the <code><Install Dir>\OOBM\conf\config.properties</code> file.

Create the RCA Database

Note: If you do not know how to create an ODBC-compliant database, contact your database administrator. You must also define an ODBC DSN for each database you create. If you do not know how to create an ODBC DSN, contact your database administrator.

The following sections provide information on the prerequisites and procedures for creating Microsoft SQL Server and Oracle databases.

- ["Create a Microsoft SQL Server Database for the RCA Core" below](#)
- ["Create an Oracle Database for the RCA Core" on page 40](#)

RCA Patch and Usage Management

If RCA Patch management or RCA Usage management is enabled, you can create an additional Patch management-specific database or Usage management-specific database to store Patch management data or Usage management data respectively.

It recommends that you define additional Patch management-specific database or Usage management-specific database to keep Patch management data or Usage management data separate from device, inventory, and application information. To define additional Patch management database, use the Patch Management section in the Configuration tab of the Console, after you install the Core server. To define additional Usage management database, use the Usage Management section in the Configuration tab of the Console, after you install the Core server.

Create a Microsoft SQL Server Database for the RCA Core

Follow the instructions in this section to create a Microsoft SQL Server database for the reporting objects for the Core server. If you do not have security rights to create the database, contact your Microsoft SQL Server database administrator.

Prerequisites

The following prerequisites should be met before you create a Microsoft SQL Server database:

- Microsoft SQL Server *must* be locally installed or remotely accessible from the RCA server.
- If Microsoft SQL Server is installed on a server other than the RCA server, firewall rules may be added to enable communications between them. For more information on opening required ports for Microsoft SQL Server, see the Microsoft Knowledge Base article **841251** at <http://support.microsoft.com/kb>.
- Microsoft SQL Server *must* be configured to use static ports. For information on how to use static ports, refer to your Microsoft SQL Server documentation.
- Microsoft SQL Server *must* be configured to use **mixed-mode authentication** and *must* have TCP/IP support enabled.
- Windows 32-bit ODBC DSNs: When using ODBC drivers on a Windows 64-bit operating system, create the ODBC System DSN for the database using 32-bit drivers. On a 64-bit operating system, you can access the 32-bit ODBC Data Source Administrator by running `C:\Windows\SysWOW64\odbcad32.exe` to create or modify the System DSNs that are required for RCA.
- The “storage” sizes that are documented in this section are recommendations only.

Creating a Microsoft SQL Server Database for the RCA Core

To create a Microsoft SQL Server database for the RCA Core server:

1. On the Microsoft SQL Server, create a database with the following recommended settings:

General tab	Name: Specify name for database. Do not use space or underscore (for example, RCACORE).
Data Files tab	Initial Size: 500 MB Select Autogrow by 20%
Transaction Log tab	Change initial size: 100 MB

2. Use SQL Server Authentication.
3. Change the default database to the database name that you used in step 1.
Note: The SQL Server name, admin user ID, and password are required during RCA installation.
4. Provide the user with the minimum role membership of db_datareader, db_datawriter, and db_ddladmin for the Microsoft SQL Server database.
5. Create an ODBC System DSN with a name of your choice (for example, **RCAODBC**) on the computer that hosts the Core server. Point the ODBC System DSN to the new Core server database you created in step 1 on the Microsoft SQL Server.

The database is now connected. Install RCA Core server as described in "[Installing RCA Core Server](#)" on page 35.

Create an Oracle Database for the RCA Core

Follow the instructions in this section to create an Oracle database for the reporting objects for the Core server. If you do not have security rights to create the database, contact your Oracle database administrator.

Prerequisites

The following prerequisites should be met before you create an Oracle database:

- It recommends that you use the latest available patch set for Oracle when using an Oracle database.
- You *must* use the Oracle Corporation's ODBC drivers that are specific to the Oracle version in your environment—not those that are supplied by Microsoft.
- Make sure that your Oracle server ODBC driver versions exactly match your Core server; the connection to an Oracle database can fail if ODBC driver versions are mismatched. For more information, contact your Oracle database administrator.
- You *must* install 32-bit Oracle client on the Core server to interact with Oracle database on 32-bit computers.
- The “storage” sizes that are documented in this section are recommendations only.
- Windows 32-bit ODBC DSNs: When using ODBC drivers on a Windows 64-bit operating system, create the ODBC System DSN for the database using 32-bit drivers. On a Windows 64-bit operating system, access the 32-bit ODBC Data Source Administrator by running `C:\Windows\SysWOW64\odbcad32.exe` to create or modify the System DSNs that are required by RCA products.

Creating an Oracle database for the RCA Core

To create an Oracle Server database for the RCA Core server:

1. On the Oracle server, create a data tablespace with the following recommended settings.

Tablespace Name	Specify name for data tablespace (for example, HPCACOREDATA).
Status	Online
Type	Permanent
Datafile	Fully qualified path and name of the data file, such as HPCACOREDATA.dbf
Storage	Minimum Size 200 MB and Max size unlimited
Extent Management	Locally managed with automatic allocation
Segment Space Management	Automatic
Logging	No

2. Create a temporary tablespace with the following recommended settings.

Tablespace Name	Specify name for temporary tablespace (for example, HPCACORETEMP).
Status	Online
Type	Temporary
Datafile	Fully qualified path and name of the datafile, such as HPCACORETEMP.dbf
Storage	Size 1000 MB
Extent Management	Locally managed with automatic allocation
Segment Space Management	Automatic
Logging	No

3. Create a user; associate the data and temporary tablespaces with the user with a default profile.

Username	Specify name for user (for example, HPCACORE).
Password	Create a password based on your enterprise's security recommendations
Default tablespace	HPCACOREDATA
Temporary tablespace	HPCACORETEMP

Profile	DEFAULT or a PROFILE NAME used for this schema
Roles	CONNECT and RESOURCE
System Privileges	CREATE ANY VIEW SELECT ANY TABLE UNLIMITED TABLESPACE UPDATE ANY TABLE

4. On the computer that hosts the Core server, create an ODBC System DSN with a name of your choice (such as, **HPCAODBC**) that points to the new Core server database on the Oracle server.

The database is now connected. Install the RCA Core server as described in the next section.

Installing Core

Install the RCA Core server to a dedicated server in your environment. It recommends that you do not modify configuration of the Core server or its components other than those specifically documented in this guide. For security reasons, it also recommends to enable SSL in your RCA environment.

Note: You can install RCA Core server in a High Availability (HA) Cluster environment. This reduces disruptions in Core server availability to the minimum because of the failover mechanism of cluster environment. To implement this, install the Core server with same hostname on two or more nodes of a cluster with the Core server data directory or the complete install directory on a shared cluster drive. You may also install the Satellite servers in a clustered environment.

If `setup.exe` is used to run the installation, the default installation location can be altered in `setup.ini` (with the `log.filename` entry in the options section) before the installation.

Note: It recommends that you always specify the fully qualified domain name when prompted for RCA Core server name. This practice ensures the proper mapping to the Core servers when “downstream” Satellite servers and RCA agents are installed.

To install RCA Core server:

1. Log on as a user with Administrative privileges on the computer where you plan to install the RCA Core server.
2. Navigate to the `Setup-Core` directory to access the Core server installation files.
3. Double-click the **setup.exe** file. The Radia Client Automation Core Installer window opens.
4. Click **Next**. The Radia Client Automation Software License Agreement page opens.
5. Review the Radia Client Automation Core license terms, select **I accept the license agreement** and click **Next**. The Radia Client Automation Installation Folder page opens.

6. The Installation Folder page displays the default installation directory for the RCA Core server. Accept the default location, or click **Browse** to select a different location, and then click **Next**. The Radia Client Automation Data Folder page opens.
7. The Data Folder page displays the default directory for the RCA Core server data files. Accept the default location, or click **Browse** to select a different location, and then click **Next**. The Radia Client Automation Host Name page opens.
8. Select a name for this RCA server and click **Next**. The Radia Client Automation Server Ports window opens.
9. Accept the default ports, or specify Web Server and Configuration Server ports, and then click **Next**. The Radia Client Automation Installation Confirmation page opens. You can also select **Modify Windows Firewall** to enable communications by using these ports if you want to automatically enable ports 3464 and 3466. For more information, see "[Core Communication Ports](#)" on page 36.
10. Click **Next** to start the installation. The installation process initiates the different configuration scripts that can run for several minutes.
11. Click **Finish** to complete the Radia Client Automation Core server installation.

After installing RCA Core server, run the First Time Setup Wizard to set up the Core server as described in the next section.

Post Installation Configuration

After installing RCA Core server, the RCA Core Console automatically opens. The login window opens in your default browser.

1. On the login window, specify the default user name, password, and directory source.
 - The default user name is **admin** and the password is **secret**.

Note: It recommends that you change the default user name and password. To change the default user name and password, click **Configuration** tab > **Access Control** > **Users**, and then click the **Create New User** icon in the Users area.

- **Zone:** **HP** is the RCA internal directory store in which internal users are stored.
2. Click **Sign In**. The First Time Setup Wizard opens and prompts you for initial configuration settings for your RCA environment. You can modify these settings in the various panels of the RCA Console also.
 3. Click **Next** on the Introduction page to begin the wizard.
 4. On the License page, copy and paste the contents of your HP-issued, product-specific license file into the License Data box and click **Next**. If you do not have a license at this point, a temporary RCA Enterprise edition evaluation license is generated that is valid for 30 days after you install RCA. This license provides limited functionality within the Console.
 5. On the Database Source page, click one of the following options for an ODBC connection based on your database and click **Next**.
 - *For SQL Users:* SQL Server database users can select either **Use an existing ODBC connection already on the server** or **Create and configure a new database**.

- *For Oracle Users:* Oracle database users must select **Use an existing ODBC connection already on the server**.
6. On the Database Settings page, specify the appropriate values in the following mandatory fields:
 - DSN: Name of the database.
 - Server Host: Hostname of the database server.
 - Server Port: Port number used by the database server.
 - User ID: User ID to access to the database.
 - Password: Password to access the database.
 7. Click **Next**.
 8. On the Services page, select the RCA services that this RCA server should provide and click **Next**. The configuration selections are saved.
 9. On the Complete page, click **Finish** to complete the configuration tasks.

For more information on configuring these services in the RCA Console, see the *Configuration* chapter in the *Radia Client Automation Enterprise User Guide*.

Default Installation Directories

The RCA Core server installation creates the following directories by default; alternative directories for the server and data files can be selected during the installation.

- The Core server files are installed to `Hewlett-Packard\HPCA` in the default 32-bit Program Files directory.
- The Core server data files are installed to `Hewlett-Packard\HPCA\Data` in the default 32-bit Program Files directory.

Caution: Make sure that you exclude all the RCA directories when running an anti-virus scan, anti-spyware scan, or anti-malware scan. Including RCA directories during these scans may affect the RCA functioning.

Installation Log Files

The RCA Core server installation creates two log files, which are placed in the `Local Settings\Temp` directory of the user who ran the installation:

- The file, `hpca-install.log`, is always created.
- A server-specific log file (`HPCACore_setup.log`) is also created—regardless of whether the installation was run using the `.msi` or `.exe` file.

Installing Core in Silent Mode

This section details the silent installation of the RCA Core server using `msiexec.exe` and `setup.exe`.

Note: Silent installation is supported for Core server only.

Installing Core Using msixec.exe

The syntax to install Core server in silent mode using `msiexec.exe` is:

```
msiexec.exe /I "fully qualified path to Core MSI file" /lv* "fully  
qualified path to installation log repository" INSTALLDIR="fully  
qualified path to installation directory" DATADIR="fully qualified  
path to data directory" /qn
```

Note: If the installation is run in the silent mode by using the `.msi` file, the name and location of the log file can be altered by using the `/l msiexec` command-line option.

Syntax Notes

- The keywords and values for this syntax are case-sensitive. Make sure that you specify the keywords in UPPERCASE (as shown), and the values in the appropriate case.
- The directory paths to the Core server installation media and the installation log repository must be fully qualified. If there are any spaces in the directory path, the entire path must be enclosed in quotation marks.
- The installation fails, if a non-existent installation-log directory path is specified.
- The `qn` in the syntax is the instruction for a silent installation. To initiate the GUI installation from a command line, replace `qn` with `qb` in the syntax.

Syntax Parameters Descriptions

The following are the silent installation syntax parameters:

- **INSTALLDIR** (optional): By default, the Core server is installed to 32-bit Program Files directory. If **INSTALLDIR** is not specified, default value is used.
- **DATADIR** (optional): By default, the Core server data files (Proxy server cache and CSDB) are installed to `Hewlett-Packard\HPCA\Data` in the default 32-bit Program Files directory. You can also specify an alternate installation directory path.

Example

The following is a sample command to install Core server silently:

```
msiexec.exe /i "Setup-Core\HPCACore.msi" /lv* "C:\Program  
Files\Hewlett-Packard\HPCA\install.log" DATADIR="C:\Program  
Files\Hewlett-Packard\HPCA\Data" /qn
```

The path to the Satellite server installation (MSI) file is: `Setup-Satellite\HPCASatellite.msi`

Results

The silent installation command that is presented in the Example section installs:

- The Core server to the default location, `C:\Program Files\Hewlett-Packard\HPCA`.
- The data files to `C:\Program Files\Hewlett-Packard\HPCA\Data`.
- The installation log to `C:\Program Files\Hewlett-Packard\HPCA`.

Installing Core Using setup.exe File

You can also install the Core server silently by using the `setup.exe` file. The `setup.exe` file can be customized and run as described in this section.

To install the Core server using `setup.exe` file:

1. Copy all of the RCA installation files from the RCA media to your hard drive.
2. Open, edit, and save the `setup.ini` file.
3. Run `setup.exe`.

Windows Services

After you install the Core server, it runs as a Windows service - **RCA Core**.

The start mode of the RCA Core service is set to "Automatic." As this service is an internal part of the RCA Core server, do not stop the service when Core server is running.

In addition to the RCA services, several sub-services are automatically installed with the RCA Core server. These are easily identified in Windows services because they are prefixed with "RCA." The start mode for these sub-services is "Manual."

It recommends that you use only the Console to stop and start these sub-services because of cross-service dependencies. If the RCA Core service is stopped, the sub-services automatically stop along with the RCA Core service.

Chapter 5

Installing RCA Satellite Server

Before you start the Satellite server installation, you must consider the following factors that help you determine the positioning of Satellite servers in your environment:

- Capacity – Add Satellite server to support more numbers of agents.
- Availability – Add Satellite servers to ensure high availability of service and data.
- Network Proximity – Add Satellite servers for network optimization.

This chapter contains installation requirements to install RCA Satellite server. This chapter also guides you through the process of installing and configuring RCA Satellite server.

Hardware and Software Requirements

Caution: The Satellite server should be installed on a computer with only operating system installed.

The following are the minimum system requirements for installing Satellite servers:

Full-service Mode

- 2 GB RAM
- Dual-core processor
- 2 GHz CPU speed
- 2 GB free disk space

Streamlined Mode

- 1 GB RAM
- Dual-core processor
- 1.6 GHz CPU speed
- 2 GB free disk space

Platform Support

For the operating system requirements for this release, see the *Radia Client Automation Support Matrix* available at the URL: http://h20230.www2.hp.com/sc/support_matrices.jsp.

You must have an HP passport ID to access this web site.

The *Radia Client Automation Support Matrix* is also located on the distribution media for this product in the \Documentation directory.

Installation Prerequisites

RCA Satellite server has default listening ports that *must* be enabled before starting the installation process. Ports **3464** and **3466** are the primary ports used for Satellite server communications when SSL is not enabled. When SSL is enabled on a satellite, SSL is used for all inbound communications. If a firewall is in place on the RCA server's host computer, the primary ports *must* be added to the firewall "exceptions" list.

The default ports on which the Satellite server communicate within RCA environment are listed in the following table:

RCA Satellite Server Communication Ports

Port	Port Type	Description
127.0.0.1:3461	TCP	RCA Messaging server (<code>nvdkit-hpca-ms.exe</code>)
0.0.0.0:3464	TCP	Default port for RCA Configuration server (<code>ZTOPTASK.exe</code>) It must be available on Satellite servers that are set to the full-service mode.
0.0.0.0:3466	TCP	RCA Apache server (<code>httpd.exe</code>) Main HTTP port that Satellite server uses for communications with Core server and RCA agents.
127.0.0.1:3468	TCP	RCA Policy server (<code>nvdkit-hpca-pm.exe</code>) It must be available on Satellite servers that are set to the full-service mode.
127.0.0.1:3470	TCP	RCA Thin Client management server (<code>nvdkit-hpca-mms.exe</code>) It must be available on Satellite servers that are set to the full-service mode.
127.0.0.1:3472	TCP	RCA Multicast server (<code>nvdkit-hpca-mcast.exe</code>) It must be available on Satellite servers that are set to the full-service mode.
127.0.0.1:3482	TCP/UDP	Mobile server (<code>nvdkit-hpca-mdm.exe</code>) It must be available on Satellite servers that are set to the full-service mode.
2xx.0.0.0:9100	UDP	Default port for RCA Multicast server (<code>nvdkit-hpca-mcast.exe</code>) It must be available on Satellite servers that are set to the full-service mode.
127.0.0.1:3473	TCP	RCA DCS (<code>nvdkit-hpca-dcs.exe</code>)
127.0.0.1:3481	TCP	RCA Proxy server (<code>nvdkit-hpca-ps.exe</code>)

Port	Port Type	Description
443	SSL	Port used for “secure HTTP” (HTTPS) communications.
444	SSL	Port used for “secure TCP” (TCPS) communications for RCA Configuration server.
2195	TCP/UDP	Enable access to this port on the address block 17.0.0.0/8. The access can be either through a SOCKS proxy or directly from the Satellite server. This port is required to enable communications between Mobile Device Management (MDM) server and Apple Push Notification Service (APNS).

Installing RCA Satellite Server

You can install a Satellite server manually on a device or deploy the Satellite server from the Console. For information about deploying a Satellite server from the Console, see the *Radia Client Automation Enterprise User Guide*. Silent installation is not supported for Satellite servers. For security reasons, it recommends to enable SSL in your RCA environment.

Caution: It recommends that you do not modify configuration of the Satellite server or its components other than those specifically documented in this guide.

To install Satellite server manually on a device:

1. Log on as a user with administrative privileges on the computer where you plan to install the Satellite server.
2. Insert the installation media and navigate to the `Setup-Satellite` directory to access the Satellite server installation files.
3. Double-click **setup.exe**. The Radia Client Automation Satellite Installer window opens.
4. Click **Next**. The Radia Client Automation Software License Agreement page opens.
5. Review the Radia Client Automation Satellite license terms, select **I accept the license agreement** and click **Next**. The Radia Client Automation Installation Folder page opens.
6. The Installation Folder page displays the default installation directory for the Satellite server. Accept the default location, or click **Browse** to select a different location, and then click **Next**. The Radia Client Automation Data Folder window opens.
7. The Data Folder page displays the default directory for the RCA Satellite server data files. Accept the default location, or click **Browse** to select a different location, and then click **Next**. The Radia Client Automation Host Name page opens.
8. Type a name for this Satellite server and click **Next**. The Radia Client Automation Server Ports page opens.
9. Accept the default ports, or specify Web Server and Configuration Server ports. You can also select **Modify Windows Firewall** to enable communications by using these ports if you want to automatically enable ports 3464 and 3466.

10. Click **Next** to start the installation. The installation process initiates the different configuration scripts that can run for several minutes.
11. Click **Finish** to complete the Radia Client Automation Satellite server installation.

After installing RCA Satellite server, run the First Time Setup Wizard to set up the Satellite server as described in the next section.

Note: After installation, you may see some errors in the log file. These errors self-correct after you run the First Time Setup Wizard, and setup of the product is complete.

Post Installation Configuration

After installing RCA Satellite server, the RCA Satellite Console automatically opens. The login window opens in your default browser.

1. On the login window, specify the default user name and password. The default user name is `admin` and the password is `secret`.

Note: It recommends that you change the default user name and password. To change the default user name and password, click **Configuration** tab > **Access Control** > **Users**, and then click the **Create New User** icon in the Users area.

2. Click **OK**. The First Time Setup Wizard opens and prompts you for initial configuration settings for your RCA environment. You can modify these settings in the various panels of the Satellite Console also.
3. Click **Next** on the Introduction page to begin the wizard. The Upstream Server page opens.
4. Specify a valid upstream host and click **Next**. The License page opens, which is pre-populated with license information from the Satellite server's upstream server.
5. Click **Next** to continue to the Services page.
6. Select the RCA services that this RCA server should provide and click **Next**. The configuration selections are saved.

Note: The services that are presented in this window are recommended for RCA environments but they do not have to be enabled here. They can subsequently be enabled on the **Configuration** tab of the Satellite Console.

7. Click **Next**. The configuration selections are saved.
8. On the Complete page, click **Finish** to complete the configuration tasks.

Default Installation Directories

The Satellite server installation creates the following directories by default. You can select alternate directories for the server and data files during the installation.

- The Satellite server files are installed to `Hewlett-Packard\HPCA` in the default 32-bit Program Files directory.

- The Satellite server data files are installed to `Hewlett-Packard\HPCA\Data` in the default 32-bit `Program Files` directory.

Installation Log Files

The Satellite server installations create two log files, which are placed in the `Local Settings\Temp` directory of the user who ran the installation:

- The file, `hpca-install.log`, is always created.
- A server-specific log file (`HPCASatellite_setup.log`) is also created—regardless of whether the installation was run using the `.msi` or `.exe` file.

Unattended Configuration of RCA Satellite Server

In a multi-tier RCA environment, you can replicate the settings applied to one Satellite server to multiple Satellite servers. The “unattended” configuration feature enables an RCA administrator to capture configuration settings from a Satellite server installation and apply them to subsequent Satellite server installations. The administrator does not have to specify identical settings multiple times for multiple Satellite servers. This enables an RCA administrator to:

- Replicate configuration settings to multiple Satellite servers, rather than having to specify identical settings multiple times for multiple Satellite servers.
- Make minor changes that are targeted at specific Satellite servers without the changes affecting all Satellite server installations.

The unattended Satellite server configuration is done in an XML file, and it enables an administrator to specify various settings that will be applied to the server as part of its installation. With the XML file, an RCA administrator can:

- Enable and disable RCA services on the Satellite.
- Configure LDAP settings for RCA Policy Servers.
- Configure upstream host and port settings.
- Configure SSL server settings.
- Increase the speed of installations.

The XML File

The Satellite server installation and configuration settings are captured in a pre-configured XML file, `unattended.xml` file that can be used to set up more Satellite servers in your environment. You can perform the following actions:

- Customize the settings in the `unattended.xml` file by using a three step (obtain-customize-apply) procedure as described in ["Using the Customized XML File" on next page](#). This method enables you to customize the XML file and create multiple copies that can be used for different Satellite server installations.
- Automatically retrieve and apply the default settings in the `unattended.xml` file by using the command line procedure as described in ["Using the Default unattended.xml File" on page 54](#).

This method prevents any customizations to the settings in the file. It automatically retrieves all of the configuration settings in the file, and applies them to the Satellite server as part of its installation.

Using the Customized XML File

You *must* perform the following tasks to customize the settings for the unattended configuration of Satellite server installations contained in the pre-configured `unattended.xml` file:

1. Obtain the XML file.
2. Customize the XML file.
3. Apply the XML file.

Obtain the XML File

The `unattended.xml` file is not included on the RCA media. It *must* be downloaded from a Satellite server after it has been installed.

To obtain the `unattended.xml` file from the RCA Satellite server:

1. Install the RCA Satellite server (see ["Installing RCA Satellite Server" on page 49](#)).
2. Complete the First Time Setup Wizard as described in ["Post Installation Configuration" on page 50](#).
3. Open an Internet browser and in the Address field, specify:
 - `localhost:3466/sm/config`, if you are on a Satellite server.
 - `http://servername:3466/sm/config`, if you are not on a Satellite server, where, *servername* is the IP address of the Satellite server from where you are downloading the `unattended.xml` file.

Use your preferred download utility, such as Wget, to download the `unattended.xml` file. This provides a customizable XML output of the configuration for the current Satellite server that can be copied and customized as required.

Note: If you use the `unattended.xml` file for Satellite server installations, you can bypass the First Time Setup Wizard because all the required settings are already specified in the configuration file. This ability, however, must be set in the configuration file with the `servermanager` service name. For an example, see ["unattended.xml File Parameters" on next page](#).

Customize the XML File

You can copy and customize the `unattended.xml` file to specify varying configuration parameters for the Satellite servers in your environment. For example, you can create multiple copies of the `unattended.xml` file (with different names) that can be used for different Satellite server installations.

To customize the `unattended.xml` file for the Satellite server installation:

1. Copy and paste the `unattended.xml` file to a different location.
2. Rename the copied file.

3. Open the renamed file and customize the various configuration settings that are to be applied to subsequent Satellite server installations.
4. Save and close the file.

Apply the XML File

The customized XML file can be referenced to apply specific configuration options to the Satellite server installation. Make sure that you reference the correct XML file (with the UNATTENDEDFILE property in `setup.ini`) when you run the Satellite server installation.

To apply the customized XML file to the Satellite server installation:

1. Copy the `\Setup-Satellite` folder from RCA installation media and paste it to a temporary location on the computer where you want to install the Satellite server. For example, `C:\temp`.
2. Navigate to the `C:\temp\Setup-Satellite` folder and open the `setup.ini` file.
3. Locate the UNATTENDEDFILE property.
4. Specify the name of the XML file that contains the configuration parameters for the Satellite server.

Note: If the XML file is not in the same directory as `setup.exe`, specify the fully qualified path and file name.

5. Save and close the file.
6. Run `setup.exe` to trigger the installation.
The installation uses the configurations defined in the `setup.ini` file. The upstream server and configured services details added in the customized XML file are automatically applied to this Satellite server.

After running the Satellite server installation using the unattended configuration method, the `config.log` file in `Console\logs` can be used to troubleshoot any unexpected issues.

unattended.xml File Parameters

The following table describes the settings of the `unattended.xml` file:

unattended.xml Parameters

Parameter	Description
<code>attr name</code>	Specifies any additional configuration settings. These additional settings do not apply to other areas of this XML file.
<code>certificates</code>	Indicates the area in which this Satellite server's SSL certificates information (server, private, and cacertificate) is listed. For more information on the various types of certificates and their function, see the <i>Radia Client Automation SSL Implementation Guide</i> .
<code>config</code>	Indicates the start of a general container area to specify configuration settings that are not covered by a parent type.

Parameter	Description
configuration	Indicates the start of the customizable configuration settings.
data	The license string text as read in from the RCA Configuration server <code>edmprof</code> file.
database	Indicates the start of the area to specify database settings.
enable	Enables or disables the service under which this parameter is listed. Valid values are true and false .
license	Indicates the start of the area to specify RCA product license settings.
password	The password that is associated with the user ID (<code>user</code> parameter).
port	The port on which this Satellite server communicates with its upstream RCA server.
server	This Satellite server's upstream RCA server on which the CSDB resides.
service name	The name of an RCA service. Use the <code>servermanager</code> service with an <code>attr_name</code> of <code>already.configured</code> and a value of 1 to bypass the First Time Setup Wizard in unattended Satellite server installations.
services	Indicates the start of the area to specify and enable or disable additional RCA services.
ssl	Indicates the start of SSL-based communications with this Satellite server's upstream RCA server. Valid values are true and false . This parameter also indicates the start of the area in which SSL configuration options are set.
type	The type of database. Valid values are sql and ldap .
upstream	Indicates the start of the area to specify configuration settings for this Satellite server's upstream server that houses the CSDB.
user	The name of the user that has access to the upstream server.

Using the Default `unattended.xml` File

Use the following TCL command to automatically captures the current settings of the Satellite server and apply them to the `unattended.xml` file.

Note: You cannot customize the configuration settings using this method.

```
exec ./nvdkit.exe "C:/Program Files/Hewlett-Packard/HPCA/ApacheServer/apps/console/sm.kit/bin/config.tcl"  
%XMLFILEPATH%
```

The XML input (`%XMLFILEPATH%`, in the above-listed command) is optional. You can remove this parameter for a GET request of the server configuration. However, you must include this parameter if you also want to SET the server configuration.

Proxy Server on Linux

Proxy server is the primary repository for RCA agent data. After the RCA agent determines the resources required based on its desired state, it can request these resources from the Proxy server. The Proxy server has the ability to service multiple, concurrent RCA agent requests.

Proxy server for Windows is installed by default with the Satellite server installation. However, you have to use a separate installer to install Proxy server on a Linux computer.

Installation Prerequisites

To install the Proxy server on a Linux operating system, you must log on as `root`, and should have adequate rights to create and update the target installation directory.

System Requirements

To install Proxy server on Linux, you should have a connection to the computer running the upstream server.

Platform Support

For the operating system requirements for this release, see the *Radia Client Automation Support Matrix* available at the URL: http://h20230.www2.hp.com/sc/support_matrices.jsp.

You must have an HP passport ID to access this web site.

The *Radia Client Automation Support Matrix* is also located on the distribution media for this product in the `\Documentation` directory.

Installing Proxy Server on Linux

To install the Proxy server to a local computer for Linux operating system:

1. From the RCA installation media, navigate to the `Media/extended_infrastructure/proxy_server/linux` directory to locate the Proxy server media for Linux. You can also access the Proxy server media for Linux, after installing RCA Core server, from the following location:
`<InstallDir>\Media\extended_infrastructure\proxy_server\linux`
2. Copy the `linux` folder to a temporary directory on the computer where you want to install Proxy server for Linux.
3. Open the command prompt and change your current directory to the temporary directory where you copied the `linux` folder.
4. Type `chmod -R +x *` and press **Enter**.
5. Type `./setup` and press **Enter**. The Welcome window for the Proxy server Setup program opens.
6. Click **Next**. The End-User License Agreement window opens. You *must* accept the terms before the Proxy server can be installed.

7. Click **Accept** to agree to the terms of the software license and continue with the installation. The installation directory window opens for you to select or type the base directory for the Proxy server install.

The default Proxy server install directory is:

```
/opt/HP/CM/IntegrationServer
```

8. Accept the default Proxy server location. You can also type or browse to an alternate directory where you want to install the Proxy server. This Proxy server base directory specifies the location of the Integration server component, installed with the product.
9. Click **Next**. The License File window opens.
10. Type the location and name of your License File or click **Browse** to select the file from the Browse dialog box.
11. Click **Next**. The RCA Configuration Server IP Address window opens.
12. Type the IP Address or hostname of the host upstream server, that the Proxy server should connect to during a preload to obtain its static cache resolution and static cache files (resource data).

Note: The Proxy server preload process must always connect to the upstream host server specified in the Server IP Address field for its static cache resolution. However, you can configure the Proxy server to obtain the static cache files from another Proxy server, if required. For more information, see the *Preloading Using HTTP* section in the *Radia Client Automation Enterprise Proxy Server Installation and Configuration Guide*.

13. Click **Next**. The RCA Configuration Server Port window opens.
14. Accept or type the TCP port number of the upstream server to be used to connect to the Proxy server for the static cache preload resolution. The default port number is 3464.
15. Click **Next**. The RCA Configuration Server User ID window opens.
16. Type the user ID that the Proxy server should use to connect to the upstream server to obtain its static cache preload resolution. The default is RPS.

Note: The user ID entered must correspond to an instance in the Primary.Policy.User class of the CSDB, where the static cache desired state policy for this Proxy server is defined. For more information, see the *Configuring the CSDB for the Static Cache Preload* section in the *Radia Client Automation Enterprise Proxy Server Installation and Configuration Guide*.

17. Click **Next**. The Installation Settings window opens.
18. Review the installation settings. To change the settings, click **Back** to get to the appropriate window. After modifying, click **Next** to return to the Installation Setting windows again.
19. Click **Install** to begin the Proxy server installation. The Installation Progress window opens.
20. When the installation is complete, the Successful Installation window opens.
21. Click **Finish** to exit the installation program.

By default, the Proxy server for Linux is installed into the following folder:


```
/opt/HP/CM/IntegrationServer
```

Installing the Proxy server for Linux adds the `static` and `dynamic` subdirectories to the `IntegrationServer/data` folder, which stores the Proxy server's static and dynamic cache.

After installation, the RCA Proxy Server service does not start automatically on the Linux platforms. To start or stop the Proxy server for Linux, use the commands described in the next section.

Starting and Stopping the Proxy Server for Linux

To start the Proxy server for Linux:

1. Change your current directory to the directory where you installed the Proxy server (`/opt/HP/CM/IntegrationServer` by default).
2. Type `./nvdkit httpd.tkd`
3. Press **Enter**.

The Proxy Server service starts on your computer.

To stop the Proxy server for Linux:

Note: The following are general guidelines and the commands are examples that can vary slightly depending on the Linux type you are using.

1. Obtain the process ID for the Proxy server by listing all the Linux processes and extracting the process ID for `nvdkit`.

```
ps -f | grep nvdkit | sed /grep/d | awk '{ print $2 }'
```

 - a. Run the following command:

```
kill <PID>
```

where, `<PID>` is the process identification number for `nvdkit` that you received as output in step 1.

The Proxy Server service stops on your computer.

Windows Services

After you install the RCA Satellite server, it runs as a Windows service - **RCA Satellite**.

The start mode of the RCA Satellite service is set to "Automatic". As this service is an internal part of the RCA Satellite server, do not stop the service when Satellite server is running.

In addition to the RCA services, several sub-services are automatically installed with the RCA Satellite server. These are easily identified in Windows services because they are prefixed with "RCA". The start mode for these sub-services is "Manual".

It recommends that you use only the Console to stop and start these sub-services because of cross-service dependencies. If the RCA Satellite service is stopped, the sub-services automatically stop along with the RCA Satellite service.

Chapter 6

Installing RCA Administrator Tools

The RCA Administrator tools are automatically installed as part of the Core server installation on Windows operating system. You can install the Administrator tools to another computer by deploying the Administrator service or by using the installation file included on the RCA media. RCA administrator tools can be installed on a Windows, Linux, or Macintosh operating system.

It recommends that you do not install RCA Administrator tools and RCA agent on the same computer.

Installing RCA Administrator Tools on Windows

To install the RCA Administrator tools on a computer other than that which hosts the Core server, you should install it manually. You can install RCA Administrator tools manually for Windows by using one of the following methods:

- "Installing RCA Administrator Tools Using Wizard" on next page
- "Installing RCA Administrator Tools using Command Line" on page 61

Installation Prerequisites

The following are the minimum system requirements to install Administrator tools:

- A computer with only the target device's operating system installed.
- TCP/IP connection to the RCA Core server.
- Administrative rights to the computer.

Platform Support

For the operating system requirements for this release, see the *Radia Client Automation Support Matrix* available at the URL: http://h20230.www2.hp.com/sc/support_matrices.jsp.

You must have an HP passport ID to access this web site.

The *Radia Client Automation Support Matrix* is also located on the distribution media for this product in the `\Documentation` directory.

Installation Files

The following files are used for installing Administrator tools:

- `setup.exe`

The `setup.exe` is located in the RCA installation media folder, `\Setup-Core\Media\admin\default\win32`. It accepts command line parameters and passes them to Windows Installer.

You can also create a Windows Installer Administrative Installation Point (AIP) for network installations. The AIP starts the Windows Installer and passes command line parameters to it.

Note: A Windows Installer Administrative Installation Point (AIP) is also known as an Administrative Control Point (ACP).


To create the Windows Installer Administrative Installation Point (AIP) in a specified target directory:


- a. Open the command prompt and navigate to the `\Setup-Core\Media\admin\default\win32` directory.
 - b. Type `SETUP.EXE /a TARGETDIR=drive:\targetdirectory /qb` where, `targetdirectory` is the directory where you want to create Windows Installer AIP. The target directory contains `HPCAE-ADMIN.MSI`, the installation folders, and `setup.exe`.
- `HPCAE-ADMIN.MSI`
`HPCAE-ADMIN.MSI` is the MSI file that contains the default configuration information for the installation. This file is stored on the RCA installation media folder, `\Setup-Core\Media\admin\default\win32`.

Installing RCA Administrator Tools Using Wizard

To install RCA Administrator tools on Windows using the wizard:

1. From the Core server installation media, navigate to the `\Setup-Core\Media\admin\default\win32` directory, and run `setup.exe` file. RCA Administrator Installation Wizard opens.
You can also copy the files from the installation media to a temporary directory and start the installation procedure.
2. Click **Next** to begin the installation. The End-User License Agreement window opens.
3. Read and accept the License Agreement and click **Next**. The Destination Folder window opens. If you want to select a different destination for RCA Administrator tools, click **Browse**. Navigate to the appropriate destination folder and click **OK** to continue.
4. Click **Next**. The RCA Configuration Server window opens.
5. In the IP Address text box, type the IP address of the RCA Configuration server.
6. In the Port text box, type the port number (default is 3464) of the RCA Configuration server.
7. Click **Next**. The License window opens.
8. Click **Browse** to select the license file for RCA.
9. Click **Next**. The Select Features window opens.

- Click  to select the features that you want to install.

Note: If you want to set the same options for all of the features, you can click  next to Radia Client Automation Admin and select the appropriate option to apply the setting to all features.

Each time you click , a shortcut menu for that feature opens.

- From the shortcut menu, select an installation option. The following table contains description of these options.

Feature Settings for the Administrator Tools

Option	Description
Will be installed on local hard drive	Installs the top-level feature on the local hard drive, but not any sub-features.
Entire feature will be installed on local hard drive	Installs the entire feature, including sub-features. Note: In this installation program, selecting this option or the "Will be installed on local hard drive" option for any of the features results in the same installation because these features do not contain sub-features.
Entire feature will be unavailable	The feature is not installed. If previously installed, the feature is removed.

Note: You can click **Disk Cost** to see an overview of the disk space required for the installation.

- Click **Next**. The Ready to Install the Application window opens.
- Click **Install** to begin the installation. When the installation is complete, RCA Administrator has been successfully installed window opens.
- Click **Finish** to exit the installation.

Installing RCA Administrator Tools using Command Line

Open the command prompt and navigate to the directory that contains RCA Administrator tools installation files. Type the following command:

```
SETUP.EXE NVDOBJZMASTER_ZIPADDR=<IP Address of the Core server>  
FeatureStateArgument=Feature1,Feature2,FeatureN [AdditionalParameter]
```

where,

FeatureStateArgument is one of the arguments listed in the table [RCA Administrator Tools Feature State Arguments](#).

Feature1, Feature2, FeatureN can be any of the arguments listed in the table [RCA Administrator Tools Features Arguments](#).

[AdditionalParameter] can be any of the arguments listed in the table [Command Line Arguments](#).

Examples

If you want to install only RCA Administrator Packager on a computer, type the following command line:

```
SETUP.EXE ADDLOCAL=NVDINSTALLPACKAGER
```

If you want to install RCA Administrator CSDB Editor and RCA Administrator Agent Explorer on a computer, type the following command line:

```
SETUP.EXE ADDLOCAL=NVDINSTALLSYSTEMEXPLORER,NVDINSTALLCLIENTEXPLORER
```

RCA Administrator Tools Feature State Arguments

Arguments	Description
ADDLOCAL	Type a comma-delimited list of features that you want to set to "Will be installed on local hard drive".
ADDSOURCE	Type a comma-delimited list of features that you want to set to "Will be installed to run from network".
ADVERTISE	Type a comma-delimited list of features that you want to set to "Feature will be installed when required".
REMOVE	Type a comma-delimited list of features that you want to set to "Entire feature will be unavailable". This removes the features only, not the entire product. Therefore, if you use the REMOVE property and type each of the feature names, the RCA Administrator product is stored on your computer. If you want to remove the entire product, type REMOVE=ALL.

RCA Administrator Tools Features Arguments

Administrator Tools Feature	Feature Argument
Agent Explorer	NVDINSTALLCLIENTEXPLORER
Packager	NVDINSTALLPACKAGER
Publisher	NVDINSTALLPUBLISHER
Screen Painter	NVDINSTALLSCREENPAINTER
CSDB Editor	NVDINSTALLSYSTEMEXPLORER
AMP Editor	NVDINSTALLAMPEDITOR

Command Line Arguments

Argument	Description
/qn	Performs a silent installation.
/qb	Displays the progress bar only during the installation.
/l*v drive:\install.log	Creates a detailed Windows Installer log. Note: Using this option may affect the performance of the installation.
/a TARGETDIR= drive:\targetdirectory	Creates a Windows Installer AIP in the specified target directory. The target directory contains <code>HPCAE-ADMIN.MSI</code> , the installation folders, and <code>setup.exe</code> . After you create the AIP, you can run <code>setup.exe</code> and pass the appropriate command line parameters. This starts the Windows Installer and passes the specified parameters to it.
INSTALLDIR=	Specify the installation directory to be used. Use quotes for paths that contain spaces.
LICENSEFILE=	Specify the full path of the license file to be used. Use quotes for paths that contain spaces. In case this property is not specified, the installer looks for <code>license.nvd</code> in the <code>setup</code> folder, by default.

Installing RCA Administrator Tools on Linux and Macintosh

RCA Administrator for Linux and Macintosh contains two tools: RCA Administrator Publisher and RCA Administrator Agent Explorer. You can install RCA Administrator tools manually for Linux and Macintosh using one of the following methods:

- ["Installing RCA Administrator Tools Using Graphical User Interface" on next page](#)
- ["Installing RCA Administrator Tools Using Command Line" on page 65](#)

Installation Prerequisites

The following prerequisites should be met before you install RCA Administrator tools on Linux or Macintosh operating system:

- TCP/IP connection to a computer running the RCA Core server.
- It recommends that you install and run RCA Administrator tools as **root** (or as a Mac OS X administrator user ID capable of issuing **sudo** commands). Root authority is required to apply owner and group designators to managed resources.

- Install the RCA Administrator tools on a local file system.
- To install RCA Administrator tools using GUI mode, set the Linux environment variable, `DISPLAY`. Set this variable to indicate the host name or IP address of the device to which you want to redirect the graphical display.
To set the variable `DISPLAY`:
 - In C shell, type `setenv DISPLAY <IP address or hostname>:0.0`
 - In Bourne, Bash, or Korn shell,
 - i. Type `DISPLAY=<IP address or hostname>:0.0` and press **Enter**.
 - ii. Type `export DISPLAY`

Note: If the `DISPLAY` environment variable is not set in your environment, the installation defaults to a non-graphical installation.

Installing RCA Administrator Tools Using Graphical User Interface

To install RCA Administrator tools on Linux or Macintosh using a GUI:

1. Open the command prompt and change your current working directory to the Administrator tools platform subdirectory on the installation media.
For example:

In Linux operating system, change your working directory to:
`/Setup-Core/Media/admin/default/linux`

In Macintosh operating system, change your working directory to:
`/Setup-Core/Media/admin/default/macx86`
2. Type `./install` (for Mac OS X, type `sudo ./install`) and press **Enter**. The Welcome window opens.

3. Click **Next**. The HP Software License terms window opens.
4. Read the software license terms and click **Accept**. RCA Administrator Location window opens.
5. Type the name of the directory where you are installing RCA Administrator tools or click **Browse** to navigate to it.

6. Click **Next**. If the specified directory already exists you are prompted to verify this location.
 - a. If you want to update the existing directory, click **OK**.
 - b. If you want to change the directory location, click **Cancel**.

The Lib Directory window opens.

7. Type the name of the directory where you want to store proprietary information created by RCA (the `lib` directory) or click **Browse** to navigate to it.
8. Click **Next**. The Log Directory window opens.

9. Type the name of the directory where you want to store the log files generated by RCA or click **Browse** to navigate to it.
10. Click **Next**. The RCA Configuration Server IP Address window opens.
11. Type the IP address (format: xxx.xxx.xxx.xxx) or host name of the Configuration server where you want to publish the applications.
12. Click **Next**. The RCA Configuration Server Port Number window opens.
13. Type the port number of your RCA Configuration server (default is 3464).
14. Click **Next**. The Package Settings window opens.
15. Review the settings displayed in the Package Settings window. To change the settings, click back to get to the appropriate window.
16. When you are ready to proceed, click **Install**. RCA Administrator tools are installed.

Installing RCA Administrator Tools Using Command Line

To install RCA Administrator tools on Linux or Macintosh using command line:

1. Open the command prompt and change your current working directory to the Administrator tools platform subdirectory on the installation media.
For example:

In Linux operating system, change your working directory to:
`/Setup-Core/Media/admin/default/linux`

In Macintosh operating system, change your working directory to:
`/Setup-Core/Media/admin/default/macx86`
2. Type `./install -mode text` (for Mac OS X, type `sudo ./install -mode text`) and press **Enter**. RCA Administrator tools installation begins.
3. Type `C` and press **Enter**.
4. Specify the installation location for RCA Administrator tools and press **Enter**.
5. Specify the location for the RCA proprietary objects (`IDMLIB`) and press **Enter**.
6. Specify the location for the log files created by RCA (`IDMLOG`) and press **Enter**.
7. Specify the IP address of the RCA Core server and press **Enter**.
8. Specify the port number of the RCA Core server and press **Enter**.
9. Review the installation settings you have chosen. If you want to install RCA Administrator tools with these settings, press **Enter** to accept the default (Y) and begin the installation. You can type `N` to re-enter your installation information.
10. To complete the configured installation process, press **Enter**. The RCA Administrator tools are installed.

Installing Batch Publisher

RCA Batch Publisher dynamically creates package instances and names them (with date and sequence number) to accommodate multiple publishing sessions.

The RCA Batch Publisher can be installed on Windows and Linux operating systems.

Installation Prerequisites

The minimum system requirements for RCA Batch Publisher are:

- Network connectivity to RCA Core server.
- A minimum of 2 MB of hard disk space.
- Access to directories from which you want to publish.
- Administrative rights to the computer.

It recommends that you stop any programs that are running before installing the RCA Batch Publisher.

Platform Support

For the operating system requirements for this release, see the *Radia Client Automation Support Matrix* available at the URL: http://h20230.www2.hp.com/sc/support_matrices.jsp.

You must have an HP passport ID to access this web site.

The *Radia Client Automation Support Matrix* is also located on the distribution media for this product in the `\Documentation` directory.

Installing RCA Batch Publisher for Windows

To install the RCA Batch Publisher for Windows:

1. From the Core server installation media, navigate to the `\Media\extended_infrastructure\publishing_adapter\publisher\win32` folder, and run `setup.exe`. The Welcome window opens.
2. Click **Next**. The HP Software License Terms window opens.
3. Read the license terms and click **Accept**. The Directory Location window opens.
4. Type the name of the directory where you want to install the RCA Batch Publisher or click **Browse** to navigate to it. By default, RCA Batch publisher is installed in the `C:\Program Files\Hewlett-Packard\CM\BatchPublisher` directory.
5. Click **Next**. If the directory you specified already exists, you are prompted to replace it. If the directory you specified already exists, you are prompted to overwrite the existing directory. To specify a new directory, click **Cancel** to return to the previous step or click **OK** to proceed. The Installation Settings window opens.
6. Click **Install**.
7. When the installation is complete, click **Finish**.

You have successfully installed the Batch Publisher for Windows.

Installing RCA Batch Publisher for Linux

If you are installing the RCA Batch Publisher on a Linux operating system that supports graphics, the graphical installation automatically begins after you initiates the installation program.

For Linux operating systems that support graphics, see ["Installing Batch Publisher on Linux using Graphical User Interface" below](#).

For Linux operating systems that do not support graphics, the non-graphical installation program automatically starts when you initiate the installation program. If you are installing the RCA Batch Publisher on a Linux operating system that supports graphics, but you want to use the non-graphical mode instead, change your directory to the location of the installation program on the installation media, and then type: `./install -mode text`. This starts the non-graphical installation of the RCA Batch Publisher. For more information, see ["Installing Batch Publisher on Linux using non-Graphical Method" on next page](#).

Installing Batch Publisher on Linux using Graphical User Interface

To install the RCA Batch Publisher using the graphical interface:

1. Open the command prompt and change your current working directory to the `/Media/extended_infrastructure/publishing_adapter/publisher/linux` subdirectory on the installation media.
2. Type `./install` and press **Enter**. The Welcome window opens.
3. Click **Next**. The HP Software License Terms window opens.
4. Read the agreement and click **Accept**. The Directory Location window opens.
5. Type the name of the directory where you want to install the Batch Publisher or click **Browse** to select a location. By default, RCA Batch publisher is installed in the `/opt/HP/CM/BatchPublisher` directory.
6. Click **Next**.
7. If the directory you specified already exists, you are prompted to overwrite the existing directory. To specify a new directory, click **Cancel** to return to the previous step or click **OK** to proceed. The Installation Settings window opens.
8. Click **Install**.
9. When the installation is complete, click **Finish**.

You have successfully installed the Batch Publisher for Linux. Before using the RCA Batch Publisher in a Linux environment, you should modify the `filters all` parameter in the configuration file as described in the section ["Post Installation Task" on next page](#). This is specific to the configuration file-based publishing method (`promote.cfg`).

Installing Batch Publisher on Linux using non-Graphical Method

To install the RCA Batch Publisher using the non-graphical method:

1. Open the command prompt and change your current working directory to the `/Media/extended_infrastructure/publishing_adapter/publisher/linux` subdirectory on the installation media.
2. Type `./install -mode text` and press **Enter**. The RCA Batch Publisher installation begins.
3. Type `C` and press **Enter**.
4. Press a key to view the End User License Agreement. After you read the agreement, type `Accept` and press **Enter**.
5. Press **Enter** to accept the default location for the RCA Batch Publisher (`/opt/HP/CM/BatchPublisher`), or specify a different location.
If the directory you specify already exists, you are prompted to overwrite the existing directory.
If the directory does not exist, the installation program displays the Installation Settings.
6. Type `Y` and press **Enter** to start the installation. If you do not want to start the installation, type `N` and press **Enter**.
7. To complete the configured installation process, press **Enter**.

You have successfully installed the RCA Batch Publisher for Linux. Before using the RCA Batch Publisher in a Linux environment, you should modify the `filters all` parameter in the configuration file as described in the section ["Post Installation Task" below](#). This is specific to the configuration file-based publishing method (`promote.cfg`).

Post Installation Task

Modifying the `filters all` parameter in the configuration file

The default values are:

```
filters all {  
  
  typefile  
  classfile  
  exclude "*.log *.bak"  
  include ""  
  distroot{}  
  
}
```

To modify the `filters all` parameter, change the `class` parameter from its default of `file` to `unixfile`.

```
filters all {  
  
  typefile  
  classunixfile  
  exclude "*.log *.bak"
```

```
include "*"
distroot{}

}
```

Installing Application Usage Manager Administrator

The Application Usage Manager (AUM) Administrator Provides interface to create rules that define the data that is used to create usage reports for the managed devices. Install this component on the computer where Core server is installed.

To install the AUM Administrator, complete the following steps :

1. Navigate to the `<InstallDir>\Media\usage` directory.
2. Double-click **UsageManagerAdministrator.msi** to start the installation.
3. Click **Next**. The end-user license agreement dialog box opens.
4. Read and accept the HP Software License terms and click **Next**. The installation location dialog box opens, showing the default location.
5. If you want to install the AUM Administrator at a different location, click **Browse** to navigate to the location.
6. Click **Next**. The Ready to Install dialog box opens.
7. Click **Install**.
8. When the installation is complete, click **Finish**.

The AUM Administrator is installed and a shortcut is created in the **Start** menu as RCA Usage Manager Administrator. After an ODBC connection to a database is established, use the **Start** menu shortcut or the `RADPIMGR.exe` file to access the AUM Administrator. By default, `RADPIMGR.exe` is located in the following directory:

```
[ProgramFilesPath]\Hewlett-Packard\CM\Usage Manager Administrator\bin\.
```


Chapter 7

Installing RCA Agent

The RCA agent is installed on end-user computers that an RCA administrator wants to manage using RCA. You can install agent software on the Windows, Linux, and Macintosh operating systems. You can also deploy the RCA agent to Windows and Linux based HP thin client devices.

It recommends that you do not install RCA Administrator tools and RCA agent on the same computer.

Installing RCA Agent on Windows

You can install RCA agent on Windows using one of the following methods:

- ["Installing RCA Agent using Wizard" on page 83](#)
- ["Installing RCA Agent Using Command Line" on page 85](#)
- ["Installing RCA Agent using Logon Script" on page 87](#)

You can also deploy RCA agents by using Core Console. For more information, see the *Radia Client Automation Enterprise User Guide*. You can deploy RCA Usage Manager agent by using Core Console as described in *Deploying the Usage Collection Agent* section in the *Radia Client Automation Enterprise User Guide*.

You can install RCA agent in lockdown mode to ensure non-privileged users are not able to access critical system-level confidential content. For more information, see ["Installing RCA Agent in Lockdown Mode" on page 87](#).

Hardware and Software Requirements

The following are the minimum system requirements for the computer where you want to install RCA agents:

- 1 GB free disk space.
- Microsoft .NET runtime 1.1 (required for RCA Application Self-Service Manager only). The .NET installation program is available in the `Media\client\default\win32\dotnet` folder on the RCA Core media. If .NET does not exist on the RCA agent computer, the .NET installation program runs automatically during installation. Microsoft .NET requires Microsoft Internet Explorer 5.01 or later.
- TCP/IP connection to a computer running the RCA Core server.
- Windows NTFS-based file system with Access Control Lists (ACLs) support to install RCA agent in Lockdown mode.
- Administrative rights to the computer to install the RCA agents.

Platform Support

For the operating system requirements for this release, see the *Radia Client Automation Support Matrix* available at the URL: http://h20230.www2.hp.com/sc/support_matrices.jsp.

You must have an HP passport ID to access this web site.

The *Radia Client Automation Support Matrix* is also located on the distribution media for this product in the `\Documentation` directory.

Installation Prerequisites

The following prerequisites should be met before installing RCA agent:

- **Communication Ports**

RCA agents communicate with RCA Core and Satellite servers using ports listed in the "[Agent Communication Ports](#)" [below](#) section. These ports should be enabled on the agent computer.

- **Internet Proxies**

You must enable the RCA agent to discover and use Internet proxies by setting the following properties in the `Install.ini` file:

`USEPROXY=Y` and `DISCOVER=Y`

Note: You can also set the Internet proxies after installing RCA agents. For more information, see *Radia Client Automation Enterprise Administrator User Guide*.

The next RCA agent connect to the Core server uses the Internet proxy that is specified.

Agent Communication Ports

You must enable the following port on the RCA agents in the RCA environment to enable communication with Core and Satellite servers:

RCA Agent Communication Port

Port	Port Type	Description
3465	TCP	Required to receive incoming notify requests from Core server and to communicate with the Satellite servers.
3460	TCP	Required when you deploy MSI-based applications that are published in Advanced mode.
3463	TCP	Required when you plan to deploy RCA agent remotely. For example, deploying agent through RCA Core server.

For Out of Band Management, enable the following additional ports on the RCA agents (vPro device or DASH device) to allow inbound and outbound traffic:

Out of Band Management Ports

Port	Description
vPro Device	

Port	Description
16992	Port for web service traffic over TCP.
16993	Port for web service traffic over TLS (with client authentication).
16994	Port for SOL/IDE-R over TCP.
16995	Port for SOL/IDE-R over TLS (with client authentication).
9998	Port for communications between the OOB management Console and the agent during Remote Configuration of vPro devices.
9999	Port that must be available on the client browser computer for applet-to-server socket communications for SOL.
DASH Devices	
623	Port for communications with DASH devices.
9999	Port that must be available on the client browser computer for applet-to-server socket communications for SOL.

Preparing for RCA Agent Installation

The RCA agent installation program can be distributed as an executable (`setup.exe`) or as a Windows Installer **Administrative Installation Point** (AIP). The installation process remains same regardless of the method you choose to install RCA agent. You can customize many aspects of the installation including which RCA agents to install and to which directory the installation files should be copied. If you want to customize the installation process, you should be familiar with the following files:

- **setup.exe**: Stored in the `\Setup-Core\Media\client\default\win32` directory on the RCA Core media. It accepts standard Windows Installer command-line parameters and passes them to the Windows Installer service.
You can also create an AIP for network installations. An Administrative Installation Point is also known as an **Administrative Control Point** (ACP).

To create the Windows Installer AIP in a specified target directory:

- Open the command prompt and navigate to the `\Setup-Core\Media\client\default\win32` directory.
- Type `setup.exe /a TARGETDIR=drive:\targetdirectory /qb` where, `targetdirectory` is the directory where you want to create Windows Installer AIP. The target directory contains `HPCAE-MgmtApps.msi`, the installation folders, `setup.exe`, and files such as, `Install.ini` or Visual Basic scripts stored in the same directory as `setup.exe`.

After you create the AIP, you can copy the contents of the target directory to the target device to install the RCA agent. You can then run the `setup.exe` and pass the command-line parameters. This starts the Windows Installer and passes the specified parameters to it.

- **HPCAE-MgmtApps.msi**

This MSI file is stored in the `\Setup-Core\Media\client\default\win32` directory on the RCA Core media and contains the default configuration information for the installation.

- **args.xml**

The RCA Application Self-Service Manager arguments file created from information stored in the [ARGS] section of `Install.ini`. This file is stored in `IDMLIB` directory, `<InstallDir>\Agent\Lib\`, on the RCA agent computer and controls the behavior of the RCA Application Self-Service Manager.

- **Customized scripts**

You can use pre-install scripts to customize the installation and post-install scripts to run the processes after installing RCA agents as described in ["Using Customized Scripts" on page 81](#).

- **Install.ini**

Use `Install.ini` to customize the installation or the RCA agent arguments file, or to create or set attributes for RCA objects that are created after installing RCA agent. You can also control folder access for users. Settings in `Install.ini` override the defaults stored in `HPCAE-MgmtApps.msi`. You can create your own customized `install.ini` file.

Note: New objects or properties must be defined in `Install.ini`. You can use a pre-install script to override a value for the object or property, but any attempt to specify a new object or property in the pre-install script is ignored.

A sample `Install.ini` is available in the `\Setup-Core\Media\client\default\win32` directory on the RCA Core media.

Note: When you modify the `Install.ini` file sections, make sure that all the `Install.ini` files located in the following folders are modified:

- `<InstallDir>\Media\client\default\win32`
- `<InstallDir>\ManagementPortal\media\default\win32`

The following sections describe the three `Install.ini` file sections:

- ["\[Properties\] Section in Install.ini" below](#)
- ["\[Args\] Section of Install.ini" on page 77](#)
- ["\[Objects\] Section of Install.ini" on page 80](#)

[Properties] Section in Install.ini

Use the [Properties] section to modify agent installer properties or HP-specific properties to customize the behavior of the installation program. The values that you set in this section override the default values stored in the `HPCAE-MgmtApps.msi` file.

Note: All properties such as `INSTALLDIR` must be typed in uppercase.

[Properties] Section in Install.ini

Argument	Description
ADDLOCAL	Specify the RCA agent sub-features that you want to install on the local hard drive. There is no default for this argument.
ARPNOREMOVE	<p>Set to 1 to disable the ability to remove the RCA agent from the computer using Add/Remove Programs in the Control Panel.</p> <ul style="list-style-type: none"> For Windows 2003 and supported operating systems above Windows 2003, the Remove button is disabled. For supported operating systems before Windows 2003, the RCA agent is not listed in Add/Remove Programs in the Control Panel. <p>Setting to 0 does not disable this option because of a Windows Installer issue. If you want to enable your subscribers to remove the RCA agent from the computer using Add/Remove Programs, place a semi-colon (;) in front of the ARPNOREMOVE argument in Install.ini.</p>
INSTALLDIR	<p>Specify the directory in which to install the RCA agent. The default is C:\ProgramFiles\Hewlett-Packard\HPCA\Agent.</p> <p>This value is overridden if a new directory is specified in the Destination Folder window in the RCA Agent Installation Wizard.</p>
NVDENABLEUSER	<p>Indicate whether to show or hide the Set User window in the Installation Wizard.</p> <ul style="list-style-type: none"> Specify Y (the default) to show the window. Specify N to hide the window. If you hide the window, the Create RCA Application Self-Service Manager icon on the desktop check box will no longer be available to your subscribers. Specify D to show the window, but disable the User Name field. The Create RCA Application Self-Service Manager icon on the desktop check box is still available.
NVDENABLEIP	Indicate whether to show or hide the Configuration Server window in the Installation Wizard. The default is Y .
NVDENABLEPROXY	Indicate whether to show or hide the Proxy Information

Argument	Description
	<p>window in the Installation Wizard. The default is N.</p> <p>If you want to use a Proxy server during the RCA agent connect, show this window.</p> <p>The information that is specified in the Proxy Information window is stored, by default, in the PROXYINF object in the RCA agent computer's IDMLIB directory.</p>
NVDENABLESHORTCUT	<p>Indicate whether to show the Create RCA Application Self-Service Manager icon on the desktop check box in the Set User window. The default is Y.</p> <p>Selecting this check box installs a shortcut on the subscriber's desktop for RCA Application Self-Service Manager.</p>
NVDSHORTCUT	<p>Indicate whether to install a desktop shortcut for the RCA Application Self-Service Manager on the subscriber's computer. The default is Y.</p>
NVDSTARTMENUICON	<p>Indicate whether to install an icon in the Start Menu for the RCA Application Self-Service Manager on the subscriber's computer. The default is Y.</p>
NVDSTARTWMICFGMGR	<p>Indicates whether to install the shortcuts for Windows Management Instrumentation (WMI) provider. The default is Y.</p>
NVDRAMSHORTCUT	<p>Indicate whether to install a desktop shortcut for the RCA Application Manager on the subscriber's computer. The default is N. When you double-click the shortcut, RCA System Tray icon appears in the System Tray area of the Task Bar.</p>
NVDRAMSTARTMENUSHORTCUT	<p>Indicate whether to install an icon in the Start Menu for the RCA Application Manager on the subscriber's computer. The default is N.</p>
NVDRAMCONNECT	<p>Specify the command line to run when the RCA Application Manager is opened. The default value is <code>radntfyc localhost radskman dname=SOFTWARE</code>.</p>
NVDMAINTDIR	<p>Specify a directory where you want to store the RCA agent maintenance files. The default is the <code>MAINT</code> sub-directory of the folder that contains <code>setup.exe</code>.</p> <p>Specify a value only if you want to store maintenance files in a directory other than the default. If files in this directory are more recent than the installation files, they</p>

Argument	Description
	<p>are copied into the RCA agent's <code>IDMSYS</code> directory. <code>IDMSYS</code> is specified in <code>NVD.INI</code>. The default location of <code>NVD.INI</code> is <code><InstallDir>\Agent\Lib</code>.</p> <p>If you are using a post-install script, you <i>must</i> place the script in the <code>\maint</code> folder of the RCA agent install.</p>
<code>NVDLOCALNOTIFYONLY</code>	If set to <code>Y</code> , the RCA agent enables RCA Notices from the local host only. The default is <code>N</code> .
<code>NVDRADTRAYSTART</code>	Set to <code>Y</code> to display the RCA System Tray icon automatically if the RCA Application Manager is selected during the RCA agent installation process. The default is <code>N</code> .
<code>NVDNOTIFYINTERACT</code>	Set to <code>Y</code> to enable the RCA Notify Daemon to interact with the desktop. The default is <code>N</code> .
<code>NVDREDIRECTORINTERACT</code>	Set to <code>Y</code> to enable the MSI Redirector to interact with the desktop. The default is <code>N</code> .
<code>NVDSCHEDULERINTERACT</code>	Set to <code>Y</code> to enable the RCA Scheduler to interact with the desktop. The default is <code>N</code> .
<code>NVDPRECAPATH</code>	Specify the fully qualified path and filename of a custom Visual Basic pre-install script. There is no default for this argument.
<code>NVDPOSTCAPATH</code>	<p>Specify the fully qualified path and filename of a custom Visual Basic or REXX post-install script. There is no default for this argument.</p> <p>For more information, see "Using Customized Scripts" on page 81.</p>

[Args] Section of Install.ini

Use the [Args] section to control the behavior of the RCA Application Self-Service Manager. The information in this section is used to build the RCA Application Self-Service Manager arguments file, `args.xml`, which is stored in `IDMLIB` on the RCA agent computer. The default directory for `IDMLIB` is `<InstallDir>\Agent\Lib\`.

Note: The XML tags (arguments) that are described in this section are not case-sensitive when you type them in `Install.ini`. However, they are automatically converted to uppercase in `args.xml`. If you are using the RCA Application Manager, any of the parameters in the [Args] section can be added to the `RADSKMAN` command line.

[Args] section of Install.ini

Argument	Mandatory or Optional	Description
askconfirm	Optional	Controls the display of a confirmation message to your subscribers. For example, some instances in which a confirmation message might display are: <ul style="list-style-type: none"> • A restart is required. • There is insufficient disk space during deployment. • A data download is interrupted. The default is Y .
channelname	Mandatory	The CSDB domain from which applications are retrieved. The default is SOFTWARE .
default_catalog	Optional	Add the parameter to set the default catalog that is selected when the RCA Application Self-Service Manager starts. There is no default for this argument.
default_catalog_only	Optional	Add the parameter and set to Y to make only the default_catalog available when the RCA Application Self-Service Manager starts. The default is N .
identification	Optional	Identifies the RCA agent to the Configuration server by defining the value for the ZUSERID variable in the ZMASTER object. The default is \$MACHINE . This value is overridden if a different User Name is specified in the Set User window in the RCA Agent Installation Wizard. If you do not want this value to be modified, set <code>NVDENABLEUSER=N</code> in the [PROPERTIES] section of <code>Install.ini</code> . Valid values are: <ul style="list-style-type: none"> • \$MACHINE: Name of the subscriber's computer. • \$USER: Logon ID for the subscriber currently logged on.
CUSTOM		Literal custom specification
log	Optional	Specifies the name of the log stored in <code>IDMLOG</code> . <code>IDMLOG</code> is specified in <code>NVD.INI</code> . The default is <code>connect.log</code> . The default location of <code>NVD.INI</code> is <code><InstallDir>\Agent\Lib</code> .
logsize	Optional	Specifies (in bytes) the size of the log file. The default is 1000000 . When the size of the log file reaches 1000000 bytes, a backup

Argument	Mandatory or Optional	Description
		file (.bak) is created. By default, this file is <code>connect.bak</code> . If a backup file already exists, it is overwritten.
logonpanel	Optional	Controls the display of the logon panel. The default is N .
managerurl	Optional	Specifies the address as <code>http://hostname:port/nvdurl</code> for the Configuration server to be used for HTTP object transfer. There is no default for this argument.
providername	Mandatory	The name of the Configuration server, as set during its installation. The default is radia . This is used to name the folder below the STARTDIR on the RCA agent computer. For information on STARTDIR, see "startdir" on next page .
redirect	Optional	Specifies an alternate start-up file, <code>filename.xml</code> that can be accessed using a network path or URL. There is no default for this argument. If the redirect tag is set in <code>args.xml</code> , the RCA Application Self-Service Manager uses the properties that are specified in the alternate file.
resolutionmanager	Mandatory	The IP address of the Configuration server. You can also use the Configuration server hostname. There is no default for this argument. This value is overridden if a different IP address is specified in the Configuration server window in the RCA Agent Installation Wizard. To prevent this value from being modified, set <code>NVDENABLEIP=N</code> in the [PROPERTIES] section of <code>Install.ini</code> .
resolutionport	Mandatory	The port for the Configuration server. There is no default for this argument. This value is overridden if a different port is specified in the Configuration server window in the RCA Agent Installation Wizard. To prevent this value from being modified, set <code>NVDENABLEIP=N</code> in the [PROPERTIES] section of <code>Install.ini</code> .
root_catalog_name	Mandatory	Use this to customize the name of the root catalog display name. The default is All Software .
sslmanager	Optional	The address of the Configuration server that is used for SSL.

Argument	Mandatory or Optional	Description
		<p>communications. There is no default for this argument.</p> <p>If you want self-maintenance to use SSL communications, append <code>: : SM</code> to the end of the specified IP address or host name, as in <code>sslmanager=hostname: : SM</code>.</p> <div> <p>Caution: Consider the following when using the <code>: : SM</code> switch:</p> <p>The file (<code>cacert.pem</code>) that contains the CA root certificates cannot be maintained. If the corresponding CA root certificate for the certificate in use by the Configuration server should ever become expired, revoked, or corrupt, it results in disabling SSL communications to the Configuration server.</p> </div>
sslport	Optional	The TCP/IP port (usually 444) on which the SSL Manager task is listening. There is no default for this argument. The sslport specification takes the form <code>sslport=port</code> .
startdir	Optional	Specify a directory where you want to store the RCA agent objects. The default is the <code>SYSTEM</code> . Type <code>startdir=foldername</code> . If the folder name contains spaces, enclose the entire name in quotation marks (“ ”).
uioption	Optional	Controls the display of the status window. The default is N .
uioptmsi	Optional	Controls the display of the MSI status window. The default is N .

[Objects] Section of Install.ini

Use the [Objects] section to specify RCA objects to be created on the RCA agent computer and to set their default values. The format is `clientobject_attribute`. For example, if you want to set the IP address for your Configuration server, set `ZMASTER_ZIPADDR`.

[Objects] section of Install.ini

Argument	Description
ZMASTER_ZDSTSOCK	The port setting for the Configuration server. The default is 3464 .
ZMASTER_ZIPADDR	The IP address for the Configuration server. There is no default for this argument.
ZMASTER_ZNTFPORT	The port on which the RCA agent's Notify daemon is “listening.” The default is 3465 .

Argument	Description
ZMASTER_ZNTFYSEC	This attribute enables a Notify operation to run programs from the IDMSYS directory only. This is used for security during Notify operations. The default is Y .
ZMASTER_ZTIMEO	The duration (in seconds) that the RCA agent waits for a response from the Configuration server before it times out. The default is 240 . Valid values are numerals from 0 through 3200.
ZMASTER_ZTRACE	Indicates whether communication buffer information is included in the log; also generates unique logs for create methods. The default is N . <ul style="list-style-type: none"> • Y enables Communication and Method Tracing. • S enables Communication summary information; Method Tracing is not enabled. • N disables Communication Tracing and Method Tracing.
ZMASTER_ZTRACEL	The level of tracing that is generated in the RCA agent log files. The default value is 040 . The syntax is xxx. The valid values are numerals from 0 through 999, where 0 = minimal tracing, 40 is acceptable for most activity, and 999 = maximum tracing.
ZMASTER_ZUSERID	The user ID. The default is the name of the user that is currently logged on to the computer.
ZMASTER_ZVRFYUID	Specify Y to verify the user ID that was sent by the Configuration server's Notify command. This verification uses the ZUSERID field from the RCA agent's ZMASTER object. The default is N .
PROXYINF_USEPROXY	Specify Y or N to indicate whether a Proxy server should be used when connecting to the Configuration server. The default is N .
PROXYINF_DISCOVER	<i>Applicable to Microsoft Internet Explorer only.</i> Specify Y to discover Internet Explorer's proxy settings. The default is N .
PROXYINF_PROXADDR	The IP address and port number of your proxy server. The default is xxx.xxx.xxx.xxx:1080 .
RADSETUP_COP	Set to Y to enable Client Operations Profiles. The default is N .

Using Customized Scripts

You can use customized scripts to customize properties that affect the installation or run processes after installing RCA agents. This section details the pre-install scripts and post-install scripts.

Caution: It recommends that only experienced users use the customized scripts.

Using a Pre-Install Script

Use Visual Basic scripts to customize MSI properties that affect the installation. The following is a very simple Visual Basic script example.

You *must* use the NVDPRECAPATH argument to specify the fully qualified path and file name of a custom Visual Basic pre-install script in `Install.ini` or on the command line. For information on NVDPRECAPATH, see "[Properties] Section in Install.ini" on page 74.

` The following sample demonstrates fetching an MSI property, then setting the same property.

` The property values are displayed in message boxes for debugging purposes.

Option Explicit

msgbox Session.Property("ALLUSERS")

Session.Property("ALLUSERS") = "1"

msgbox Session.Property("ALLUSERS")

You can use a pre-install script to override the property settings of the arguments that control the behavior of the RCA Application Self-Service Manager, such as those in the [ARGS] section of `Install.ini`, as well as the attribute values for RCA objects, such as those specified in the [OBJECTS] section of `Install.ini`.

To override property settings or attributes for objects:

Caution: Make sure that you type the name of the property or the object and its attribute such as NVDOBJMASTER_ZDSTOCK in uppercase letters.

- Use the prefix **NVDARG** to override property settings.
For example, to override the value set for the identification property, which identifies the subscriber session to the Configuration server, type:

```
Session.Property("NVDARGIDENTIFICATION")="jenns"
```

- Use the prefix **NVDOBJ** to override object attributes.
For example, if you want to override the value set for the ZDSTOCK attribute of the ZMASTER object, which is the port setting for the Configuration server, type:

```
Session.Property("NVDOBJMASTER_ZDSTOCK")="3462"
```

Using a Post-Install Script

Use custom Visual Basic, REXX, or Tcl scripts to run processes after installing RCA agents. For example, your post-install script can initiate a connection to the Configuration server to process mandatory applications.

You *must* use the NVDPSTCAPATH argument to specify the fully qualified path and filename of the custom Visual Basic or REXX post-install script in `Install.ini` or on the command line. For information on NVDPSTCAPATH, see "[Properties] Section in Install.ini" on page 75. For example, if you want to run a script named `radstart.rex`, uncomment NVDPSTCAPATH argument, and set the value as `NVDPSTCAPATH=C:\Progra~1\Hewlett-Packard\HPCA\Agent\radstart.rex`.

Note: In RCA, REXX is an interpreted language that provides a simple way to customize various aspects of RCA processing. For more information on using REXX in RCA

environment, see *Radia Client Automation Application Manager and Configuration Server REXX Programming Guide*.

Place the script in the `\maint` folder of the RCA agent install. It is automatically copied into IDMSYS.

Installing RCA Agent using Wizard

The following steps describe the standard installation procedure. These steps can vary based on `Install.ini` or any arguments passed during the installation.



1. From the Core server installation media, navigate to the `\Setup-Core\Media\client\default\win32` directory, and run `setup.exe`. The RCA Agent Installation Wizard opens.

Note: You can initiate `setup.exe` from a command line or a logon script. For more information, see "Installing RCA Agent on Windows" on page 71.

2. Click **Next**. The End-User License Agreement window opens.
3. After reading and accepting the license agreement, click **Next**. The Destination Folder window opens.

The default location for the RCA agents is `<InstallDir>\Agent`.

If you want to select a different destination for the RCA agent, click **Browse** and navigate to the appropriate destination folder. This overrides the value set for `INSTALLDIR` in `Install.ini`.


4. Click **OK** to continue.
5. Click **Next**. The Set User window opens.
6. In the User Name text box, type the name of the subscriber for whom you are installing the RCA agents. This overrides the value set for `IDENTIFICATION` in `Install.ini`.
7. Select **Create RCA Application Self-Service Manager icon on the desktop** check box.
8. Click **Next**. The Configuration Server window opens.
9. In the IP Address or Hostname text box, type the IP address or hostname of the Configuration server. This overrides the value set for `RESOLUTIONMANAGER` in `Install.ini`.
10. In the Port text box, type the port number of the Configuration server. This overrides the value set for `RESOLUTIONPORT` in `Install.ini`.
11. Click **Next**. The Select Features window opens.
12. Click  to select the sub-features that you want to install. Each time you click , a shortcut menu for that sub-feature opens.

Note: Install only the RCA agent sub-features for which you are licensed.

13. From the shortcut menu, select an installation option. These options are described in the following table.

RCA Agent Sub-Feature Selection

Option	Description
Will be installed on local hard drive	Installs the selected sub-feature only.
Entire feature will be installed on local hard drive	<p>Installs the entire feature, including all sub-features.</p> <p>Note: To install all RCA agent sub-features, select RCA Agent at the top of the Select Features window.</p> <p>Selecting the option "Entire feature will be installed on local hard drive" or the "Will be installed on local hard drive" option for the RCA Application Self-Service Manager, RCA Application Manager, or RCA Inventory Manager results in the same installation.</p>
Entire feature will be unavailable	The sub-feature will not be installed. If previously installed, this sub-feature will be removed.

Note: If you want to set the same options for all of the sub-features, you can click  RCA Agent and select the appropriate option. Click **Disk Cost** to see an overview of the disk space required for the installation.

14. Click **Next**.
 If .NET is not installed on the target computer and you select the option to install the RCA Application Self-Service Manager, .NET is installed during the RCA agent installation. However, if you copied the installation program to your computer and did not include the \dotnet folder, the DotNet Settings message opens.

 If Microsoft .NET Framework is not installed, Microsoft .NET will be installed message appears. Complete the following steps to install Microsoft .NET Framework:
 - a. Click **Install**. The Microsoft .NET Framework 1.1 Setup window opens.
 - b. After reading and accepting the license agreement, click **Install**. When the installation is complete Microsoft .NET Framework 1.1 is installed message appears.
15. Click **OK**.
16. Click **Install** to begin the installation.
17. Click **Finish** to close the Installation Wizard.

Installing RCA Agent on Standalone Device

You can manually install the RCA agent to manage client devices that are not always connected to the network. For this, a separate installation file is included with the RCA media.

1. On the target device, insert the RCA media.
2. Use a command line and navigate to `\Setup-Core\Media\client\default\win32` directory on the media.
3. Type `setup-standard.cmd host`, where *host* is the host name or IP address of your RCA Core server.
4. Press **Enter**.

The RCA agent is installed and the device is ready to be managed by RCA.

Installing RCA Agent Using Command Line

Before performing an installation from command line, determine:

- Which RCA agents you want to install. For more information, see the table [RCA Agent Sub-Feature Command-Line Mnemonics](#).
- How the user can access the RCA agent installation program. The user can access the RCA agent installation program using a web page, an FTP site, a mapped drive, a CD-ROM, or an e-mail.

Navigate to the directory that contains RCA Agent installation files. Open the command prompt and type the following command:

```
SETUP.EXE Sub-FeatureStateArgument=Sub-Feature1,Sub-Feature2,Sub-FeatureN [AdditionalParameter]
```

where,

Sub-FeatureStateArgument is one of the arguments listed in the table [RCA Agent Sub-Feature State Arguments](#).

Sub-Feature1, *Sub-Feature2*, *Sub-FeatureN* can be any of the arguments listed in the table [RCA Agent Sub-Feature Command-Line Mnemonics](#).

[AdditionalParameter] can be any of the arguments listed in the table [Command Line Arguments](#).

Examples

- The following is an example of a command line that silently installs the RCA Application Self-Service Manager and creates a detailed Windows Installer log.

```
SETUP.EXE ADDLOCAL=NVDINSTALLRSM /qn /L*v C:\Hewlett-Packard\HPCA\Agent\install.log
```
- The following is an example of a command line that installs the RCA Application Manager and RCA Application Self-Service Manager.

```
SETUP.EXE ADDLOCAL=NVDINSTALLRAM,NVDINSTALLRSM
```

RCA Agent Sub-Feature State Arguments

Argument	Action
ADDLOCAL	Type a comma-delimited list of sub-features that you want to set as “Will be installed on local hard drive.”
REMOVE	<p>Type a comma-delimited list of sub-features that you want to set as “Entire feature will be unavailable.”</p> <p>This removes the sub-features only, not the entire product. Therefore, if you use the REMOVE property and type each of the sub-feature names, only the sub-features are removed. The RCA agent product is still stored on the computer.</p> <p>To remove the RCA agent product, type REMOVE=ALL.</p>

RCA Agent Sub-Feature Command-Line Mnemonics

Sub-Feature	Mnemonic
Application Manager	NVDINSTALLRAM
Application Self-Service Manager	NVDINSTALLRSM
Inventory Manager	NVDINSTALLRIM
Local AIP Extension	NVDINSTALLRLAE
OS Manager	NVDINSTALLROM
Patch Manager	NVDINSTALLPATCH
Personality Backup and Restore Utility	NVDINSTALLPBR
PlusHP	NVDINSTALLPLUSHP

Command Line Arguments

Argument	Action
/qn	Performs a silent installation.
/qb	Displays the progress bar during the installation.
/L*v SystemDrive:\install.log	<p>Creates a detailed Windows Installer log.</p> <p>Note: Using this option may affect the performance of the installation.</p>
/a TARGETDIR=SystemDrive:\ <i>targetdirectory</i>	Creates a Windows Installer AIP in the specified target directory.
NVDINIFILE= <i>path\INIfilename</i>	To rename the installation INI file, pass this parameter to the command line. Make sure that you include the fully qualified path.

Argument	Action
	By default, the installation program refers to <code>Install.ini</code> , which is located in the <code><InstallDir>\Media</code> directory and contains <code>setup.exe</code> .
<code>INSTALLDIR=</code>	Specify the installation directory. Use quotation marks if the path contains spaces.

Installing RCA Agent using Logon Script

You can use logon script on a Windows computer to automate the RCA agent installation.

Note: To automatically install RCA agent on a subscriber's Windows computer, subscribers must have administrator rights on their local computers, and a domain controller must authenticate each subscriber's logon.

The following is an example of a code that you can add to the logon script to install the RCA agents. If the RCA agents are not already installed when the subscriber logs on to the client device, this logon script runs the RCA agent installation program.

Sample Logon Script

```
:begin
@echo off
if exist C:\progra~1\Hewlett-Packard\HPCA\Agent\LIB\
zmaster.edm goto skipinst
start setup.exe /qn
:skipinst
```

To determine if the RCA agent already exists, the script checks for the ZMASTER object (ZMASTER.EDM) in its default location on the computer. If ZMASTER:

- Exists, the script skips the installation.
- Does not exist, the RCA agent installation program launches.

Note: The ZMASTER object begins the resolution process. The ZMASTER object is the first object that is exchanged during the RCA agent connect.

In the sample logon script, the command, `start setup.exe /qn` instructs the program to perform a silent installation of the RCA agents.

Installing RCA Agent in Lockdown Mode

Lockdown Mode is supported on Windows operating system only.

To install the RCA agent in Lockdown Mode, complete the following tasks:

1. Add the Lockdown properties to the [Properties] section of the `Install.ini` file.
2. Add the [SecurityFolders] section in the `Install.ini` file. This is an optional step. You can add [Security Folders] section if you want to modify or override the default directories.
3. Set the ACL permissions.

Adding Lockdown Properties

To install the RCA agent in Lockdown Mode, add the following Lockdown properties to the [Properties] section of `Install.ini` file:

```
LOCKDOWN=Y
```

```
LOCKDOWNSCRIPT=<Customized script>
```

Customized script is the script you create using the sample `setaccls.bat` file.

Lockdown Properties

Properties	Description
LOCKDOWN	Specify <code>Y</code> to install the RCA agent in Lockdown Mode. Specify <code>N</code> , to disable the Lockdown Mode. This is the default option.
LOCKDOWNSCRIPT	The sample <code>setaccls.bat</code> file is used to add directory permissions that isolate USER from SYSTEM content. You can customize this sample file. Make sure that the customized file is in the same directory as <code>Install.ini</code> and <code>setup.exe</code> .

Adding [SecurityFolders] Section in Install.ini

Add the [SecurityFolders] section in the `Install.ini` file to control the folder access for the users. These folder settings control the isolation of SYSTEM and USER access, therefore, you must maintain separate USER and SYSTEM access to ensure security.

Add the following lines of code in the `Install.ini` file:

```
[SecurityFolders]

IDMUSRMSI="<InstallDir>\Agent\usermsi"

IDMSHRDATA="<InstallDir>\Agent\shareddata"

IDMPUBLIC="<InstallDir>\Agent\public"

IDMUSR=CSIDL_LOCAL_APPDATA\HPCA\Agent
```

Note: If you change the paths for these parameters, make sure that you end the directory path with the name of the directory only; *do not include a closing backslash*. If the directory path is closed with an ending backslash, the `setaccls.bat` run fails and the directories are not

secured. USER-based parameters that are prefixed with `IDMUSR...` create subdirectories in a folder for each user of the managed device.

The RCA agent installation program does not prompt for the locations of these directories. They should be specified in the `Install.ini` file before running the installation program.

[SecurityFolders] Parameters

Parameter	Description
IDMUSRMSI	A directory that contains MSI installations and related MSI content for each USER.
IDMSHRDATA	A directory from which MACHINE and USER share information. Using the default permission settings, the MACHINE context writes SYSTEM objects into this directory and the USER context reads from it to fulfill software update requirements.
IDMPUBLIC	A directory for USER to write files. For example, the System Tray or radtray, writes its configuration file (<code>uiconfig.xml</code>) into the <code>IDMPUBLIC</code> folder for others to use.
IDMUSR	A directory for USER objects.

Setting Access Control Lists (ACLs)

To enable Lockdown Mode, an Administrator must set the required ACL permissions so that certain directories are not accessible by Windows “Standard Users”.

The implementation of security permissions is the responsibility of the RCA administrator. Sample processing script `setaccls.bat` file can be used to create a customized script to set ACLs that isolate USERS from the SYSTEM and other USERS.

The ACLs should be customized based on the environment. For example, if multiple users are included in an Administrators group on the devices, but you do not want all of these users to have access to the secured folders, you must do one of the following:

- Revise the memberships of the Administrators group to include only the users that are authorized to access the secured folders.
- Remove access for the Administrators group and specify which users can access the secured folders.

The sample `setaccls.bat` file contains statements that you can use to create a new script. If you do not customize the `setaccls.bat` file, ACLs are set using the sample statements provided in the `setaccls.bat` file.

The RCA agent installer creates temporary environment variables, so that the batch script can access them. These variables are created for the exclusive use by the batch script; they are automatically deleted at the conclusion of the installation process.

- `MSI_NVD_IDMSYS`
- `MSI_NVD_IDMUSRMSI`

- MSI_NVD_IDMPUBLIC
- MSI_NVD_IDMSHRDATA

The script blocks access to the following services by standard users, who are not authorized to run these service. Only the MACHINE can access these modules.

- Radexecd: This is the RCA Notify Daemon.
- Radsched: This is the RCA Scheduler Daemon.
- Radstgms: This is the RCA MSI Redirector.

The script also blocks access to the following two standalone applications for standard users, who are not authorized to run these applications. Only the MACHINE can access these modules.

- Radtimeq: This is the create method that runs when the application to which the timer is attached is created, updated, verified, or deleted.
- Upgrdmaint: This is the RCA maintenance module that processes all maintenance activities.

The following table describes the access levels for the new directories, along with the applicable mnemonic from `Nvd.ini` file.

- SYSTEM access is read-write for all these directories.
- USER access values are: read-only (**R**), read-write (**RW**), no access (**N**).

New Directory Access Levels

Mnemonic	User Access	Example
IDMSHRDATA	R	C:\PROGRA~1\HEWLET~1\HPCA\Agent\SHARED\DATA\
IDMPUBLIC	RW	C:\PROGRA~1\HEWLET~1\HPCA\Agent\PUBLIC\
IDMUSR	RW	CSIDL_LOCAL_APPDATA\HPCA\Agent\
IDMUSRMSI	RW	C:\PROGRA~1\HEWLET~1\HPCA\Agent\USERMSI\
IDMSYS	R	C:\PROGRA~1\HEWLET~1\HPCA\Agent\
IDMLIB	N	C:\PROGRA~1\HEWLET~1\HPCA\Agent\Lib\
IDMLOG	N	C:\PROGRA~1\HEWLET~1\HPCA\Agent\Log\
IDMDATA	N	C:\PROGRA~1\HEWLET~1\HPCA\Agent\Lib\Data\
NONE-CACertificates	R	C:\PROGRA~1\HEWLET~1\HPCA\Agent\CACertificates\
NONE-DEFAULTS	R	C:\PROGRA~1\HEWLET~1\HPCA\Agent\DEFAULTS\
NONE-Language specific folders	R	<ul style="list-style-type: none"> • C:\PROGRA~1\HEWLET~1\HPCA\Agent\de • C:\PROGRA~1\HEWLET~1\HPCA\Agent\es

Mnemonic	User Access	Example
		<ul style="list-style-type: none"> • C:\PROGRA~1\HEWLET~1\HPCA\Agent\fr • C:\PROGRA~1\HEWLET~1\HPCA\Agent\it • C:\PROGRA~1\HEWLET~1\HPCA\Agent\ja • C:\PROGRA~1\HEWLET~1\HPCA\Agent\pt • C:\PROGRA~1\HEWLET~1\HPCA\Agent\zh-CHS
NONE-Architecture based folders	R	<ul style="list-style-type: none"> • C:\PROGRA~1\HEWLET~1\HPCA\Agent\amd64 • C:\PROGRA~1\HEWLET~1\HPCA\Agent\x86
NONE-Other folders	R	<ul style="list-style-type: none"> • C:\PROGRA~1\HEWLET~1\HPCA\Agent\etc • C:\PROGRA~1\HEWLET~1\HPCA\Agent\Help

Installing RCA Agent on Linux and Macintosh

Caution: Install only the RCA agents for which you have licenses. If you do not have a license, the agent does not authenticate with the Configuration server.

This section describes both the graphical (using a GUI) and non-graphical (using a command line) installations of the RCA agent.

Including Maintenance Files with RCA Agent Installation

If additional maintenance files are available, for example, service packs or hot fix, you can include these files with your RCA agent installation by creating a maintenance tar file.

Within your RCA agent installation media /ram directory, create a `maint.tar` file that includes all updated files. The RCA agent installation checks for `maint.tar` and if found, the client installation extracts all updated files into the `IDMSYS` directory.

Hardware and Software Requirements

The following are the system requirements for installing RCA agent on Linux and Macintosh:

- TCP/IP connection to a computer running Core server.
- RCA agent requires 1 GB free disk space.

Platform Support

For the operating system requirements, see the *Radia Client Automation Support Matrix* available at the URL: http://h20230.www2.hp.com/sc/support_matrices.jsp.

You must have an HP passport ID to access this web site.

The *HP Client Automation Support Matrix* is also located on the distribution media for this product in the `\Documentation` directory.

Installation Prerequisites

The following prerequisites should be met to install RCA Agent on Linux or Macintosh operating system:

- RCA agents communicate with RCA Core and Satellite servers using ports listed in the "[Agent Communication Ports](#)" on page 72 section. These ports should be enabled on the agent computer.
- It recommends that you install RCA agents as root (or with a Mac OS X user ID capable of issuing sudo commands). Root authority is required to apply owner and group designators to managed resources.
- Install the RCA agent on a local file system.
- The installation program *must* be run from within Linux or Mac OS X. It recommends that you do not perform other tasks and operations during the installation process.
- If you intend to run any graphical components of the agent software on a Linux operating system, make sure the Linux environment variable DISPLAY is set in your environment. If it is not, you should set this variable to indicate the host name or IP address to which you want to redirect the graphical display.
To set the variable DISPLAY:

- In C shell, type `setenv DISPLAY <IP address or hostname>:0.0`
- In Bourne, Bash, or Korn shell,
 - i. Type `DISPLAY=<IP address or hostname>:0.0` and press **Enter**.
 - ii. Type `export DISPLAY`

Caution: If the agent is already installed in the current working directory, make sure you back up your existing agent installation files before beginning installation. If you choose to overwrite your existing RCA agent, all your customized data is lost.

You *must* set the standard Linux environment variables after installing the agent. These environment variables should include the fully qualified path of the installed client exe files, the path to the operating system-specific Motif libraries, and the standard Linux operating system paths for operating system exe files and shared libraries. It recommends that you include these as part of the logon scripts of the Linux user ID who installs and maintains the agents.

Linux Environment Variable Example

`LD_LIBRARY_PATH=/lib:/usr/lib:$IDMSYS:$LD_LIBRARY_PATH`

where, `$IDMSYS` represents the fully-qualified path to the agent executables, often referred to as the `IDMSYS` location. Motif represents the fully-qualified path to the Motif libraries installed with the operating system.

Note: The Motif libraries are required to run RCA agent or RCA Administrator graphical tools such as RCA Administrator Publisher, Administrator Agent Explorer, and the presentation of the agent logon panel.

After the agent is installed, the file `.nvdr` is placed in the `HOME` directory of the Linux user ID who performed the installation. This file enables you to set the required environment variables. It recommends that you add a line to the appropriate logon scripts to invoke this shell script:

```
. $HOME/.nvdr
```

After you perform an installation, make sure the RCA Application Manager is successfully connected to the Configuration server. You can verify the connection if the message 'CONNECTED TO THE CONFIGURATION SERVER' appears in the `connect.log` file located in the `\Agent\Log` folder on the client device.

Prerequisites for running RCA on 64-bit Red Hat Enterprise Linux

The following library files are required to run the RCA agent on 64-bit Red Hat Enterprise Linux x86:

- `glibc`
- `libXau`
- `libXdmcp`
- `libX11`
- `zlib`

Install these library files using the appropriate package for your operating system. For example,

- For 64-bit Red Hat Enterprise Linux 5, the library files can be installed using the following packages:
 - `glibc-2.5-12.i686.rpm`
 - `libXau-1.0.1-3.1.i386.rpm`
 - `libXdmcp-1.0.1-2.1.i386.rpm`
 - `libX11-1.0.3-8.el5.i386.rpm`
 - `zlib-1.2.3-3.i386.rpm`
- For 64-bit Red Hat Enterprise Linux 6, the library files can be installed using the following packages:
 - `glibc-2.12-1.7.el6.i686.rpm`
 - `libX11-1.3-2.el6.i686.rpm`
 - `nss-softokn-freebl-3.12.7-1.1.el6.i686.rpm`
 - `zlib-1.2.3-25.el6.i686.rpm`

You must also install the dependent packages for the listed `rpm` files.

Graphical Installation

This section describes how to install the agents both on a local and on a remote computer using a graphical user interface (GUI).

Local Installation

This section describes how to install the agents on a local computer using a GUI.

1. Open the command prompt and change your current working directory to the agent subdirectory on the installation media.
Agent subdirectory for Linux: `/Setup-Core/Media/client/default/linux`
Agent subdirectory for Mac: `/Setup-Core/Media/client/default/macx86`
2. Type `./install`, (for Mac OS X, type `sudo ./install`) and press **Enter**. The Welcome window opens.
You can also install the RCA agent in the graphical mode with no animations. Type `./install -mode plain`, (for Mac OS X, type `sudo ./install -mode plain`). This is useful for remote installations when network bandwidth is low.
3. Click **Next**. The End User License Agreement window opens.
4. Read the agreement and click **Accept** to continue. The Select Components to Install window opens.
5. Select the check boxes for the agents you want to install.
6. Click **Next**. The Daemons window opens.
7. *For Linux Users:* Specify when you want the daemons to start. The daemons run on the client computer and perform RCA management tasks. For more information, see ["RCA Daemons" on page 100](#).
 - Select **Start after installation** to start the daemons after the RCA Agent installation is complete.
 - Select **Automatic start after reboot via init scripts** to configure the daemons to start automatically each time the device is restarted.
8. *For Linux Users:* Click **Next**. The WBEM Server (OpenPegasus) Libraries window opens.
9. *For Linux Users:* Select **Create Links to libraries** to create a link to existing WBEM server libraries. Type the location in the Library Search Path (s) text box. You can create links after the RCA Agent is installed.
10. *For 64-bit Linux Users:* the CIM login dialog box opens.
Enter the credentials for the CIM server in the Username and Password fields. CIM is a common information model for describing management properties that is not bound to a particular implementation. For more information on CIM, refer the CIMSERVER documentation on Linux.
11. Click **Next**. The Select Installation Type window opens.
12. Select **Local Install** to install the agent on a local computer.
13. Click **Next**. The Agent Location window opens.
14. Type the name of the directory where you want to install the agent, or click **Browse** to navigate to it.
15. Click **Next**.
If the specified directory already exists, you will be prompted to verify this location.

- a. If you want to update the existing directory, click **OK**.
- b. If you want to specify a different location, click **Cancel**.

The Lib Directory window opens.

16. Type the name of the directory where you want to store proprietary information created by RCA (the lib directory), or click **Browse** to navigate to it.
17. Click **Next**. The Log Directory window opens.
18. Type the name of the directory where you want to store the log files generated by RCA, or click **Browse** to navigate to it.
19. Click **Next**. The Configuration Server IP Address window opens.
20. Type the IP address (format: xxx.xxx.xxx.xxx) of the Configuration server to which the agent should connect. Specify a valid IP address or hostname recognized by the agent workstation.
21. Click **Next**. The Configuration Server Port Number window opens.
22. Type the Configuration server's port number (default is **3464**).
23. Click **Next**. The Package Settings window opens.
24. Review the settings displayed in the Package Settings window. If you want to change any of the settings, click **Back** until you get to the appropriate window.
25. Click **Install** to install the agent with these settings.
26. After the installation is complete, click **Finish** to exit the program.

The RCA Agent is installed successfully. The default installation location for the RCA agent on Linux is `/opt/HP/CM/Agent`. The default installation location for the RCA agent on Mac OS X is `/Applications/HP/CM/Agent`.

Remote Installation

This section describes how to create an agent installation configuration file that can be used to install the RCA agent in silent mode or to a remote computer.

Your RCA system administrator can perform a Remote Installation Setup process that creates a remote installation package. This process stores the installation media in a selected directory path and a configuration file is saved in a directory you specify. You can use the installation media and configuration file to install the RCA agent in silent mode or to a remote computer. Subsequent agent installations can be initiated from any number of intended agent workstations provided they can access the directory path selected during the Remote Installation Setup process.

The remote installation is identical to the local install with the exception of two additional steps required for creating the remote installation package. Follow the steps for a local installation as described in the previous section, and when prompted in step 12, select **Remote Install**, and then type the following information for creating the remote installation package:

1. In the Package Location text box, type the fully qualified path to a directory where you want to store the agent installation media for future client installations, or click **Browse** to navigate to it.
2. Click **Next**. The Package Configuration Name window opens.

3. In the Package Configuration Name text box, type the fully qualified path to a configuration file that you want to use for silent installations, or click **Browse** to navigate to it. The configuration file you specify contains the installation information you chose during the Remote Installation Setup.

4. After the remote installation package is created, you can install RCA agent using the following syntax:

```
./install -cfg <install.cfg>
```

where *<install.cfg>* is the name of the configuration file that was created during Remote Installation Setup Process. The configuration file is used during the installation. For more information, see ["Customizing the Installation Configuration File" below](#).

Silent Installation

The following prerequisites must be met before you start the silent installation process:

- Create a package using the Remote Installation Setup installation method.
- The workstation running the silent installation must have access to the directory path where the installation media is stored.

Use the following syntax to install RCA agent in silent mode:

```
./install -mode silent -cfg <install.cfg>
```

This installs the agent in silent mode based on the parameters set in the configuration file. For information about configuration files, see ["Customizing the Installation Configuration File" below](#).

Customizing the Installation Configuration File

Performing an installation from a customized configuration file provides the following benefits:

1. Replication of precise installation details on multiple clients.
2. Ability to use a pre-installation method that runs any script or executable before the agent installation.
3. Ability to use a post-installation method, which runs any script or executable after the agent is installed.
4. You can configure the installation to force a client connection to the Configuration server immediately after the installation.
5. You can pre-configure the IP address and port number of the Configuration server to which the agent connects.
6. Ability to use an object update text file that can be used to update objects after the installation.

A configuration file provides the default responses for silent agent installations.

The variables available in the configuration file are described in the following table.

Configuration File Variables

Variable	Sample Value	Description
REMOTE	0	0 designates a local installation. 1 designates a Remote Installation Setup.
INSTDIR	For Linux: /opt/HP/CM/Agent For Macintosh: /Applications/HP/CM/Agent	The default installation directory.
IDMLOG	For Linux: /opt/HP/CM/Agent/log For Macintosh: /Applications/HP/CM/Agent/log	This can be defined to designate a directory for IDMLOG other than the default INSTDIR/log.
IDMLIB	For Linux: /opt/HP/CM/Agent/lib For Macintosh: /Applications/HP/CM/Agent/lib	This can be defined to designate a directory or IDMLIB other than the default INSTDIR/lib.
PREPROC		The fully qualified name of a script or executable to be run before installation.
PREPARAM		Parameters that are required by the pre-installation method specified in the variable PREPROC.
POSTPROC		The fully qualified name of a script or executable to be run post-installation.
POSTPARAM		Parameters required by the post-installation method specified in the variable POSTPROC.
MGRIP	xxx.xxx.xxx.xxx	The default IP address for connection to the Configuration server.
MGRPORT	3464	The default port number for connection to the Configuration server.
NTFYPORT	3465	The default Notify port.
CONNECT	Y	Connects to the Configuration server immediately after the

Variable	Sample Value	Description
		installation. Default value is N. Set to Y if you want the agent to connect to the Configuration server automatically after the installation.
OBJECTS	<p><code>./object.txt</code></p> <p>The following is an example of a valid object file:</p> <pre>ZMASTER ZTRACEL 000</pre>	<p>The file used to create or update RCA attributes after the installation. This file enables you to specify the fully qualified path to a filename that contains data in the form:</p> <pre>OBJECT_NAME VARIABLE_NAME VARIABLE_VALUE</pre> <p>When creating an object text file:</p> <ul style="list-style-type: none"> • A pound sign (#) at the beginning of a line indicates a comment. • A pound sign (#) at any other part of a line is considered data. • The VARIABLE_VALUE text should not be enclosed by any special characters.
DUAL	1	<p>0 designates Application Manager only selected.</p> <p>1 designates more than one component selected.</p>
SelectComponent	<p>0</p> <p>Example, <code>SelectComponent RAM 1.</code></p>	<p>0 signifies that the specified component is not installed or upgraded.</p> <p>1 signifies that the specified component is installed or upgraded.</p>

Using Customized Scripts

You can create and run custom executables or shell scripts before or after the silent installation of an agent. For example, your post-installation script can initiate a connection to the Configuration server to process mandatory applications. The following example is part of a shell script that initiates the connection to the Configuration server and processes mandatory applications.

```
#!/bin/sh
#
```

```
cd /opt/HP/CM/Agent

# ZIPADDR is the IP address or hostname of the manager
ZIPADDR="xxx.xxx.xxx.xxx"
# ZDSTOCK is the TCP port the manager is running on ZDSTOCK="3464"

# To manage the machine
# 1. .edmprof must exist in root's home directory
# 2. The connect must be run as root

/opt/HP/CM/Agent/radskman mname=NVDM,dname=SOFTWARE,ip=$ZIPADDR,
port=$ZDSTOCK,cat=prompt,ind=y,uid=$MACHINE,startdir=SYSTEM,ulogon=n
```

Non Graphical Installation

The following instructions guide you through the local non-graphical installation of the agent:

1. Open the command prompt and change the current working directory to the agent subdirectory on the installation media.
Example:
Agent subdirectory for Linux: /Setup-Core/Media/client/default/linux
Agent subdirectory for Mac OS: /Setup-Core/Media/client/default/macx86
2. Type `./install -mode text` (for Mac OS X, type `sudo ./install -mode text`) and press **Enter**.
3. Type `c` and press **Enter** to view the License Agreement.
4. Read the license agreement, type `Accept` and press **Enter**.
5. In the next few steps, select which agents to install. Type `Y` or `N` and press **Enter** at each prompt.
 - Client Automation Enterprise Application Manager
 - Client Automation Enterprise Inventory Manager
 - Client Automation Enterprise Application Self-Service Manager
 - Client Automation Enterprise OS Manager
 - Client Automation Enterprise Patch Manager
 - Client Automation Enterprise Application Management Profiles Agent
6. *For Linux Users:* You are prompted to start the Daemons after installation. Press **Enter** to accept the default (Y) and start the Daemons after install or type `N` and press **Enter** to start them later.
7. *For Linux Users:* You are prompted to automatically start the Daemons after a restart using `init` scripts. Press **Enter** to accept the default (N) and *not* start the Daemons each time the device is restarted or type `Y` and press **Enter** to enable Daemons to automatically start when the device is restarted.

8. *For Linux Users:* You are prompted to create links to WBEM Server (OpenPegasus) Libraries. Press **Enter** to accept the default (Y) and create links to WBEM libraries or type **N** and press **Enter** if you do not want to create links to WBEM libraries.
9. *For Linux Users:* Select the type of installation. The default is 1, a local installation.
 - Type 1, and press **Enter** to install the agent locally.
or
 - Type 2, and press **Enter** to set up remote installation media.
10. Specify the installation location for the agent, and press **Enter**.
11. Specify the location for the RCA proprietary objects (`IDMLIB`), and press **Enter**.
12. Specify the location for the log files created by RCA (`IDMLOG`), and press **Enter**.
13. Specify the IP address of the Configuration server, and press **Enter**.
14. Specify the port number for the Configuration server, and press **Enter**.
15. Review the installation settings.
16. If you want to install the agent with these parameters, press **Enter** to accept the default answer, **Y**.
If you want to change any of these settings, type **N** to re-enter the installation information.
17. Press **Enter** to install the agent.

RCA Daemons

The agent installation program installs the following daemon executables:

- **Notify** (default port **3465**)
Use Notify, **radexecd** to push updates to subscribers or to remove applications. A Notify message is sent from the Configuration server to this daemon. When the daemon receives the Notify message, RCA Application Manager connects to the Configuration server and performs the action initiated by the Notify operation.
- **Scheduler**
Use the Scheduler service, **radsched** to schedule timer-based deployments of applications.

The installation of **radexecd** and **radsched** as services on a Linux workstation is not automated within the context of the installation. The starting of services on Linux workstations depends on the operating system. For information about installing RCA daemons as system services at boot time, contact your Linux system administrator or refer to your Linux operating system's manual.

The installation of **radexecd** and **radsched** as services under Mac OS X installs sample startup scripts under Mac OS X POSIX style path `/Library/StartupItems/Radexecd` and `/Library/StartupItems/Radsched`.

Sample Shell Scripts

The installation of the agent includes a subdirectory named `sample`. It contains a sample shell script named `daemons.sh` that can be used to start, stop, and restart the **radexecd** and **radsched** daemons.

- To start the **radexecd** and **radsched** daemons, type `daemons.sh start`.
- To stop the **radexecd** and **radsched** daemons, type `daemons.sh stop`.

- To stop, and then restart the **radexec** and **radsched** daemons, type `daemons.sh restart`.

Installing RCA Agent on HP Thin Client Devices

You can deploy the RCA agent to HP thin client devices with the HP Registration and Loading Facility (RALF) installed and registered with the RCA infrastructure.

RCA Registration and Loading Facility

The RCA Registration and Loading Facility (RALF) is an agent component that is available for thin client devices and is managed by RCA infrastructure. RALF automatically registers the device with the RCA infrastructure, and manages the RCA agent installation initiated from the main console. Although RALF is part of the RCA agent for some devices, it may be pre-installed on the HP thin client factory images so registration can occur on startup. If it is not on the factory image being used, RALF can be installed and configured on the gold image that is used for subsequent OS deployments.

RALF Configuration and Operation

Depending on the HP thin client image, RALF may be pre-installed. In this case, it is configured using a default RCA server hostname defined as "hpcaserver." For RALF installations, "hpcaserver" or the host name defined using the RALF installation parameters *must* be included in DNS. The host name of the RCA server must also be included in DNS when the RCA agent is installed from the RCA Console. RALF can also be reconfigured to define a different hostname using the command line options that are described in this section. However, if you are installing the RCA agent manually, you can use the files that are provided on the RCA media to install RALF (if it is not present) before the RCA agent installation.

After it has been installed, RALF runs as a daemon that periodically probes for the RCA server. This probing continues for 24 hours, and then RALF shuts down. It starts this 24-hour probe again on reboot. After the server is contacted, RALF registers the device with the RCA infrastructure and waits to accept the request to install the RCA agent. After the agent is installed, RALF periodically contacts the server and verifies device registration attributes.

You can use additional command line parameters when configuring RALF as described in "[RALF Command Line Parameters](#)" on page 103. These parameters are applicable to the Windows and Linux based thin client devices.

Installing RCA Agent on Windows Thin Client Devices

The following prerequisites must be met before you install the RCA agent on the Windows thin client devices:

- Install RALF before you install or deploy RCA agent. If RALF is not present, install RALF on thin client devices as described in the section, "[Installing RALF](#)" on page 103.
- Minimum 7 MB free space.
- Enable port 3466 on RCA agent in the RCA environment to communicate with Core and Satellite servers.

Installing RCA Agent using Wizard

To install the RCA Agent on Windows XPE and Windows Embedded Standard (WES):

1. Access the RCA media from the Windows XPE thin client device.
2. Navigate to `\Setup-Core\Media\client\default\win32xpe`.
3. Run **setup.exe**.
4. Follow the installation steps.
When prompted for the IP address and port number, specify the Core server details.
5. Reboot the device when the RCA agent installation is complete.

To install the RCA Agent on Windows CE:

1. Open the RCA media from the Windows CE thin client device, and navigate to `\Setup-Core\Media\client\default\win32ce` directory.
2. Double-click **Standard.X86.CAB**.
3. Specify the hostname or IP address and Port number of the Configuration server.
4. Click **OK**.
5. Reboot the device when the RCA agent installation is complete.

Installing RCA Agent in Silent Mode

To install the RCA agent on Windows XPE and WES in silent mode:

Navigate to `\Setup-Core\Media\client\default\win32xpe` directory and open the command prompt. Type the following command:

```
Setup.exe NVDOBJZMASTER_ZIPADDR=<server_ip> NVDOBJZMASTER_ZDSTSOCK=<server_port> /qn
```

where, `<server_ip>` is the IP address of your Core server and `<server_port>` is the port number of your Core server.

The following optional logging parameter can be added:

```
/l*v <logfile>
```

where `<logfile>` is the complete path where Windows Installer log file is created.

To install the RCA agent on Windows CE 6.0 in silent mode:

Navigate to `\Setup-Core\Media\client\default\win32ce` directory and open the command prompt. Type the following command:

```
Setup.exe NVDOBJZMASTER_ZIPADDR=<server_ip> NVDOBJZMASTER_ZDSTSOCK=<server_port> /qn
```

where, `<server_ip>` is the IP address of your Core server and `<server_port>` is the port number of your Core server.

Installing RALF

To install RALF on Windows XPE and WES:

1. On the RCA media, navigate to \Setup-Core\Media\client\default\win32xpe\HPCARALF directory.
2. Double-click HPCARalf.msi file to install RALF on Windows XPE devices.

To install RALF on Windows CE 6.0:

1. On the RCA media, navigate to \Setup-Core\Media\client\default\win32ce\HPCARALF directory.
2. Double-click ralf.X86.cab file to install RALF on Windows CE devices.
3. Specify the IP address and port number (**hpcaserver** and **3466**, by default) of the Configuration server.

Installing RALF in Silent Mode

To install RALF on Windows XPE and Windows Embedded Standard (WES):

Navigate to \Setup-Core\Media\client\default\win32xpe\HPCARALF directory and open the command prompt. Type the following command:

```
msiexec /i HPCARalf.msi RALF_HOST=<HOSTNAME> RALF_PORT=<portnumber> /qn
```

where *<HOSTNAME>* is the hostname of your Configuration server and *<portnumber>* is the port number of the Configuration server.

To install RALF on Windows CE 6.0:

Navigate to \Setup-Core\Media\client\default\win32ce\HPCARALF directory and open the command prompt. Type the following command:

```
msiexec /i HPCARalf.msi RALF_HOST=<HOSTNAME> RALF_PORT=<portnumber> /qn
```

where *<HOSTNAME>* is the hostname of your Configuration server and *<portnumber>* is the port number of the Configuration server.

RALF Command Line Parameters

RALF supports the following command line options.

Note: These command line parameters are provided here for documentation purposes, as most are used internally.

RALF Command Line Options

Option	Description
probe	Triggers the RCA server probe.
host <host>	Specifies optional RCA server host for probing and registration.
port <port>	Specifies optional RCA server port for probing and registration.
debug	Specifies debugging logging level.
trace	Specifies tracing logging level.
silent	Enables silent mode during -get, -instagent, and -uninstagent processes.
version	Displays version of <code>ralf.exe</code> .
reginit	Defines RALF application configuration file entries for test environments.
md5 <file>	Calculates the MD5 checksum of a file.
get <file>	Downloads a file or media from the RCA server directory.
instagent <media>	Downloads and installs RCA agent.
uninstagent	Uninstalls RCA agent.
install	Installs RCA-RALF service.
uninstall	Uninstalls RCA-RALF service.
help	Displays RALF information.

Installing RCA Agent on a Linux Thin Client Devices

The following prerequisites must be met before you install the RCA agent on the Linux thin client devices:

- Install RALF before you install or deploy RCA agent. If RALF is not present, install RALF on thin client devices as described in the section, "[Installing RALF on Linux \(Debian or ThinPro\)](#)" on [next page](#)
- Minimum 7 MB free space on the `/opt` file system.
- Enable port 3461 on Linux clients to use `radsched` successfully.
- The BIOS must contain a valid serial number and device UUID to manage thin client devices. It recommends that you set the asset tag .

Installing RCA Agent on Linux based Thin Client Devices

To install RCA Agent on HP Thin Client Devices:

1. Login to the target HP thin client device as root. If you are using the ThinPro operating system, create a custom connection for xterm as follows:
 - a. From the HP menu in the lower left corner, select **Shutdown**.
 - b. From the **Thin Client Action** drop down, select **switch to admin mode** and specify the Administrator password (default password is **root**).

Note: Control Center background changes from blue to red.

- c. From the Control Center, click **Add** from the list and select the custom option.
- d. Set Name to `xterm`.
- e. Set Command to run to: `sudo xterm -e bash &`.
- f. Click **Finish**.

You now have a connection you can use to open an xterm session.

2. Create a new directory `/opt/hpca`.
3. Copy the install media from the appropriate Linux thin client sub-directory on the RCA media to a temporary directory such as `/tmp`.
4. Change the working directory to the new temporary directory and run the installation by typing:
`./install -i HPCAS_Server`
where `HPCAS_Server` is the hostname or IP address of the RCA Configuration server.
5. Restart the device when the agent installation is complete.

Installing RALF on Linux (Debian or ThinPro)

To install RALF on Linux (Debian or ThinPro):

Note: You must have root authority to install RALF to Linux devices.

1. On the RCA Media, navigate to `Setup-Core/Media/client/default/linux/c/hpcaralf` directory.
2. Copy the install media to `/tmp` on the Linux device.
3. Change the current directory to the `/tmp` directory.
4. On Debian devices, run `dpkg -i hpcaralf.deb`
5. On Thinpro devices (with read only root file system):
 - a. Run `fsunlock` (to mount the file system as read-write).
 - b. Run `/usr/share/hpkg/.hpkg_util -i hpcaralf.deb`
 - c. Run `fslock` (to remount the file system as read-only).

6. After the installation is complete, either restart the device or run `/etc/init.d/hpcaralf` to start and initialize RALF.

You can use the script `/etc/init.d/hpcaralf` to start and stop the RALF daemon on the device.

Chapter 8

Uninstalling RCA

This chapter details how to uninstall, repair, or modify various components in the RCA infrastructure.

Do not use the Windows Control Panel applet **Add/Remove Programs** to remove RCA Core or Satellite server. All the RCA files are not removed using this option. Some files and folders (for example, the directory `C:\Program Files\Hewlett-Packard\HPCA` and any files that were added or changed since the initial installation) remain on the server and should be manually removed.

Uninstalling RCA Core Server

Use the RCA installation program to uninstall RCA Core server.

To uninstall RCA Core server:

1. Log on as a user with Administrative privileges on the RCA Core server.
2. Navigate to the `Setup-core` directory.
3. Double-click **HPCACore.msi**. The Radia Client Automation Core window opens.
4. Select **Remove the Radia Client Automation Core from this computer** and click **Next**.
5. At the Removal Confirmation message, click **Next**.
6. After RCA Core server is removed, click **Finish**.

Repairing RCA Core

The Windows Installer installation program provides the ability to repair the RCA Core server. You can use this option to repair the RCA Core files, registry values, and shortcuts on RCA Core server.

Note: Using this option might override the customizations to the registry.

To repair RCA Core server using the RCA installation program:

1. Log on as a user with Administrative privileges on the RCA Core server.
2. Navigate to the `Setup-core` directory.
3. Double-click **HPCACore.msi**. The Radia Client Automation Core window opens.
4. Select **Repair the Radia Client Automation Core files, registry values, and shortcuts on this computer** and click **Next**.
5. At the Repair Confirmation message, click **Next**.
6. After RCA Core server is repaired, click **Finish**.

Uninstalling RCA Satellite Server

You can use the RCA installation program to uninstall RCA Satellite server.

To uninstall RCA Satellite:

1. Log on as a user with Administrative privileges on the RCA Satellite server.
2. Navigate to the `Setup-satellite` directory.
3. Double-click **HPCASatellite.msi**. The Radia Client Automation Satellite window opens.
4. Select **Remove the Radia Client Automation Satellite from this computer** and click **Next**.
5. At the Removal Confirmation message, click **Next**.
6. After RCA Satellite server is removed, click **Finish**.

Repairing RCA Satellite Server

The Windows Installer installation program provides the ability to repair your RCA Satellite server. You can use this option to repair the RCA Satellite files, registry values, and shortcuts on RCA Core server.

Note: Using this option might override the customizations to the registry.

To repair RCA Satellite server using the RCA installation program:

1. Log on as a user with Administrative privileges on the RCA Satellite server.
2. Navigate to the `Setup-satellite` directory.
3. Double-click **HPCASatellite.msi**. The Radia Client Automation Satellite window opens.
4. Select **Repair the Radia Client Automation Satellite files, registry values, and shortcuts on this computer** and click **Next**.
5. At the Repair Confirmation message, click **Next**.
6. After RCA Satellite server is repaired, click **Finish**.

Uninstalling RCA Administrator Tools

This section describes how to uninstall RCA Administrator tools for Windows, Linux, and Macintosh operating systems. The section also provides information on how to uninstall Batch Publisher for Windows and Linux operating systems.

Uninstalling RCA Administrator Tools on Windows

The Windows Installer installation program provides the ability to uninstall RCA Administrator tools. This section describes how to uninstall the RCA Administrator tools using the Installation Wizard and using command line.

To use the Installation Wizard to uninstall the Administrator tools:

1. Navigate to the `<InstallDir>\setup-core\media\admin\default\win32` folder and double-click **setup.exe**. The Radia Client Automation Administrator Application Maintenance window opens.
2. Select **Remove**.
3. Click **Next**.
4. Click **Remove**.
5. Click **Finish**.

To use a command line to uninstall the Administrator tools:

Navigate to the `\Setup-Core\Media\admin\default\win32` directory and type the following command:

```
SETUP.EXE FeatureStateArgument=Feature1,Feature2
```

where *FeatureStateArgument* is one of the arguments listed in the table [RCA Administrator Tools Feature State Arguments](#) and *Feature1*, *Feature2* can be any of the arguments listed in the table [RCA Administrator Tools Features Arguments](#).

For example, type the following command to remove RCA Administrator CSDB Editor and RCA Administrator Agent Explorer silently:

```
SETUP.EXE REMOVE=NVDINSTALLSYSTEMEXPLORER, NVDINSTALLCLIENTEXPLORER /qn
```

Uninstalling RCA Administrator Tools on Linux and Macintosh

To uninstall the Administrator tools:

1. Navigate to the directory where RCA Administrator tools is installed.
 - For Linux, the default installation directory is `/opt/HP/CM/Agent`.
 - For Macintosh, the default installation directory is `/Applications/HP/CM/Agent`.
2. Delete the folder `Agent` to uninstall Administrator tools.

Uninstalling Batch Publisher

To uninstall the Batch Publisher:

1. Navigate to the directory where Batch Publisher is installed.
 - For Windows, the default installation directory is `C:\Program Files\Hewlett-Packard\CM\BatchPublisher`.
 - For Linux, the default installation directory is `/opt/HP/CM/BatchPublisher`.
2. Delete the folder `BatchPublisher` to uninstall Batch Publisher.

Repairing RCA Administrator Tools

This section describes how to repair RCA Administrator tools for Windows, Linux, and Macintosh operating systems. You can use this option to repair the RCA Administrator tools files, registry values, and shortcuts on RCA Administrator tools. Using this option might override the customizations to the registry.

Repairing RCA Administrator Tools on Windows

The Windows Installer installation program provides the ability to repair RCA Administrator. This section describes how to repair the RCA Administrator tools using the Installation Wizard and using command line.

To use the Installation Wizard to repair the Administrator tools on Windows:

1. Navigate to the `<InstallDir>\setup-core\media\admin\default\win32` folder and double-click **setup.exe**. The Radia Client Automation Administrator Application Maintenance window opens.
2. Select **Repair**.
3. Click **Next**. The Radia Client Automation Administrator Ready to Repair the Application window opens.
4. Click **Install**.
5. Click **Finish**.

To use a command line to repair RCA Administrator tools on Windows:

Navigate to the `\Setup-Core\Media\admin\default\win32` directory and type the following command line:

```
SETUP.EXE FeatureStateArgument=Feature1,Feature2
```

where *FeatureStateArgument* is one of the arguments in the table [RCA Administrator Tools Feature State Arguments](#) and *Feature1* and *Feature2* are arguments in the table [RCA Administrator Tools Features Arguments](#).

For example, type the following command to repair RCA Administrator packager:

```
SETUP.EXE ADDLOCAL=NVDINSTALLPACKAGER
```

Modifying RCA Administrator Tools

This section describes how to modify RCA Administrator tools for Windows, Linux, and Macintosh operating systems. You can use the Modify option to remove specific tools of RCA Administrator tools. The section also provides information on how to modify Batch Publisher for Windows and Linux operating systems.

Modifying RCA Administrator Tools on Windows

The Windows Installer installation program provides the ability to modify RCA Administrator. This section describes how to modify the RCA Administrator tools using the Installation Wizard and using command line.

Note: To remove specific tools of RCA Administrator tools, use the **Modify** option on the Application Maintenance window.

To use the Installation Wizard to modify the Administrator tools on Windows:

1. Navigate to the `<InstallDir>\setup-core\media\admin\default\win32` folder and double-click **setup.exe**. The Radia Client Automation Administrator Application Maintenance window opens.
2. Select **Modify**.
3. Click **Next**. The Radia Client Automation Administrator Select Features window opens.
4. Select the features that you want to modify and click **next**. The Radia Client Automation Administrator Ready to Modify window opens.
5. Click **Install**. For information on feature settings, see ["Installing RCA Administrator Tools Using Wizard" on page 60](#).
6. Click **Finish**.

To use a command line to modify RCA Administrator tools on Windows:

Navigate to the `\Setup-Core\Media\admin\default\win32` directory and type the following command line:

```
SETUP.EXE FeatureStateArgument=Feature1, Feature2
```

where, *FeatureStateArgument* is one of the arguments in the table [RCA Administrator Tools Feature State Arguments](#) and *Feature1* and *Feature2* are arguments in the table [RCA Administrator Tools Features Arguments](#).

For example, type the following command to install RCA Administrator Packager to the local hard drive, and to make RCA Administrator CSDB Editor and RCA Administrator Agent Explorer unavailable:

```
SETUP.EXE ADDLOCAL=NVDINSTALLPACKAGER  
REMOVE=NVDINSTALLSYSTEMEXPLORER, NVDINSTALLCLIENTEXPLORER
```

Uninstalling RCA Agents

This section describes how to uninstall RCA Agent for Windows, Linux, and Macintosh operating systems.

Note: In a Lockdown enabled environment, if you apply Access Control List (ACL) settings to the RCA agent directories, make sure you revert the ACL settings before you perform the remove, repair, or modify operations for an RCA agent installer.

Uninstalling RCA Agent from Windows

The Windows Installer installation program provides the ability to uninstall your RCA agents. This section describes how to uninstall the RCA agent using the Installation Wizard and using command line. You can also uninstall RCA agents by using Core Console. For more information, see the *Radia Client Automation Enterprise User Guide*.

To use the Installation Wizard to uninstall the Agent on Windows:

Note: To remove sub-features of the RCA agent, use the Modify option on the Application Maintenance window. For more information, see ["Modifying RCA Agent Installation" on page 114](#).

1. Navigate to the `\Setup-Core\Media\client\default\win32` folder and double-click **setup.exe**. The Application Maintenance window opens.
2. Select **Remove**.
3. Click **Next**. The RCA Agent Uninstall window opens.
4. Click **Remove**. The files for all RCA agents are removed from the computer. The RCA agent has been successfully uninstalled window opens.
5. Click **Finish**.

To use a command line to uninstall Agent on Windows:

Navigate to the `\Setup-Core\Media\client\default\win32` directory and type the following command line:

```
SETUP.EXE REMOVE=ALL
```

For additional arguments, see ["Installing RCA Agent Using Command Line" on page 85](#).

or

To remove a single RCA agent, on the command line type a comma-delimited list of the sub-features that you want to remove.

For example, type the following command to remove RCA Application Self-Service Manager and RCA Application Manager silently:

```
SETUP.EXE REMOVE=NVDINSTALLRSM,NVDINSTALLRAM /qn
```

Note: This removes the sub-features only, not the entire product. Therefore, if you use the REMOVE argument and type each of the sub-feature names, the core product will still be stored on your computer.

Uninstalling RCA Agent from Linux and Macintosh

To uninstall the RCA agent:

1. Kill the following services:
 - `radsched`
 - `radexecd`
2. Navigate to the directory where RCA agent is installed.
 - For Linux, the default installation directory is `/opt/HP/CM/Agent`.
 - For Macintosh, the default installation directory is `/Applications/HP/CM/Agent`.
3. Delete the folder `Agent` to uninstall RCA agent.

Uninstalling RCA Agent on HP Thin Client Devices

This section describes how to uninstall the RCA agent on Windows and Linux based thin client devices.

To uninstall the Agent from a Windows XPE and WES:

1. From `\Setup-Core\Media\client\default\win32xpe` folder, double-click **setup.exe**
2. Select **Remove**.
3. Click **OK**.

To uninstall the Agent from a Windows CE:

Use the Windows Control Panel applet **Add/Remove Programs** to remove RCA agent from Windows CE.

To uninstall the Agent from a Linux-based HP Thin Client device:

1. Login to the target HP thin client device as **root**.
2. Change the current directory to `/opt/hpca/agent`.
3. Type `./uninstall` and press **Enter**.

Repairing RCA Agent

This section describes how to repair RCA Agent for Windows, Linux, and Macintosh operating systems. You can use this option to repair the RCA Agent files and registry values on RCA Agents. Using this option might override the customizations to the registry.

Repairing RCA Agent on Windows

The Windows Installer installation program offers the ability to repair your RCA agents. For example, if an RCA agent module is not available, you can use this option to repair the installation. Using this option does not overwrite modules that exist on the agent computer if they are newer than the ones provided with the installation.

To use the Installation Wizard to repair the Agent on Windows:

1. Navigate to the `\Setup-Core\Media\client\default\win32` folder and double-click **setup.exe**. The Radia Client Automation Application Manager Agent Application Maintenance window opens.

2. Select **Repair**.
3. Click **Next**. The Radia Client Automation Application Manager Agent Ready to Repair the Application window opens.
4. Click **Next**. When the repair is complete, the RCA agent has been successfully installed window opens.
5. Click **Finish**.

To use a command line to repair Agent on Windows:

Navigate to the `\Setup-Core\Media\client\default\win32` directory and type the following command:

```
msiexec /f HPCAE-MgmtApps.msi
```

Modifying RCA Agent Installation

This section describes how to modify RCA Agent for Windows, Linux, and Macintosh operating systems.

Modifying RCA Agent Installation on Windows

The Windows Installer installation program offers the ability to modify the RCA agent installation by adding or removing individual sub-features. This section describes how to modify the installation of RCA agents using the Installation Wizard and using command line.

To use the Installation Wizard to modify the Agent on Windows:

1. Navigate to the `\Setup-Core\Media\client\default\win32` folder and double-click **setup.exe**. The Application Maintenance window opens.
2. Select **Modify**.
3. Click **Next**. The Select Features window opens. For information, see ["Installing RCA Agent using Wizard" on page 83](#).
4. Click **Next**. The Ready to Modify the Application window opens.
5. Click **Next**. The RCA agent has been successfully installed window opens.
6. Click **Finish** to close the installation program.

To use a command line to modify Agent on Windows:

Navigate to the `\Setup-Core\Media\client\default\win32` directory and type the following command line:

```
SETUP.EXE FeatureStateArgument=feature1,feature2
```

where *Sub-FeatureStateArgument* is one of the arguments listed in the table [RCA Agent Sub-Feature State Arguments](#) and *Sub-Feature1*, *Sub-Feature2* can be any of the arguments listed in the table [RCA Agent Sub-Feature Command-Line Mnemonics](#).

For example, type the following command to install RCA Application Self-Service Manager and to make the RCA Inventory Manager and RCA Application Manager unavailable.

```
SETUP.EXE ADDLOCAL=NVDINSTALLRSM REMOVE=NVDINSTALLRIM,NVDINSTALLRAM
```

For additional arguments, see ["Installing RCA Agent Using Command Line" on page 85](#).

Chapter 9

Upgrading RCA

This chapter explains how to upgrade your Radia Client Automation Enterprise environment to RCA version 9.00 while preserving your data. You must apply the latest patch available to your current RCA version before starting the upgrade process.

You must contact HP Support to obtain a new license for accessing the mobile device management (MDM) feature.

Note: This chapter applies only to RCA Enterprise Edition Core and Satellite installations; it does not apply to RCA “classic” (component-based) installations. For information on migrating RCA Classic installation to RCA Core and Satellite installation, see the *Radia Client Automation Enterprise Migration Planning and Best Practices Guide* from HP Live Network at https://hpln.hp.com/system/files/HPCA_Classic_to_Core-Sat_Migration_Planning_and_Best_Practices.pdf.

Use procedures listed in this chapter to upgrade the following RCA Core and Satellite versions to the latest version of RCA Core and Satellite:

- RCA Enterprise Edition Core and Satellite version 7.50
- RCA Enterprise Edition Core and Satellite version 7.80
- RCA Enterprise Edition Core and Satellite version 7.90
- RCA Enterprise Edition Core and Satellite version 8.10

Note: To access the latest RCA Core and Satellite 9.00 migration framework posted on HP Live Network, download the migrate_CoreToCore_9_00.zip file from <https://hpln.hp.com/node/13815/attachment>.

Upgrading RCA Core Server

This section provides information on how you can upgrade the RCA Core server.

Consider the following before upgrading RCA Core server:

- If you have customized the RADISH Rexx script by replacing it with the RADISHSS Rexx script, you can use the out-of-the-box solution supplied with RCA 9.00 to do the single service optimization.
- When upgrading RCA Administrator Batch Publisher 9.00, the configuration files are not upgraded, which enables you to retain the previous customized publishing configurations to use with the updated software.
- The RCA Administrator tools are automatically installed with the Core server. The existing RCA Administrator tools on the same computer as Core server are automatically upgraded to the

latest version. To upgrade RCA Administrator tools on another computer, see the "[Upgrading RCA Administrator Tools](#)" on page 148.

- Any customizations done to the UMCOLLCT, UMCONFIG, UMDESTPT, UMINVENTclasses will not be migrated automatically during the upgrade process. You need to do the customizations again using the CSDB Editor after successful upgrade of RCA.

Hardware and Software Requirements

For the hardware and software requirements, see the "[Hardware and Software Requirements](#)" on page 35. The hardware requirements to upgrade RCA Core server may vary based on the database size.

Installation Prerequisites

The following prerequisites should be met before upgrading RCA Core server:

- Make sure that the RDBMS version you use is supported by RCA 9.00. For information on supported RDBMS, see the *Radia Client Automation Support Matrix* available at the URL: http://h10230.www2.hp.com/sc/support_matrices.jsp. For more information on how to upgrade your Oracle or Microsoft SQL Server database, check the respective database documentation.
- You must block the access to the Core server communication ports until the upgrade and restoration of the Core server is complete. The agent and Satellite server connections to the Core server during the upgrade process can result in duplicate device entries.
- You must ensure that the drive contains adequate free space to store the backup before upgrading RCA Core server.
- The upgrade process updates the existing RCA database schema through the upgrade scripts automatically.
- If you are upgrading RCA Core server and want to retain the OOBM configuration and data files for later use, you must manually copy and replace the configurations.
- After upgrade, all managed devices in the RCA environment must be connected to the RCA Core server once for Role-Based Access Control (RBAC) feature to work as expected.
- After upgrade, you must unentitle the previous existing DISCOVER_SECTOOLS_AV_AS_FW service; update HP Live Network to download new security templates; entitle the default DISCOVER_SECTOOLS_HP_SECTOOLS_MGMT_ALL_V001 or a new customized service and run a security connect for all managed devices.

Upgrade Process

The RCA Core server upgrade process includes the following tasks:

- "[Task 1: Back up the Existing RCA Core Server Installation](#)" on next page
- "[Task 2: Upgrade the Core Server](#)" on page 120
- "[Task 3: Restore RCA Data](#)" on page 121
- "[Task 4: Upgrade the SQL/Oracle Database](#)" on page 123

- "Task 5: Update HP Live Network Content" on page 124
- "Task 6: Set the Patch Management Options" on page 124
- "Task 7: Upgrading Deployed Components" on page 124

Task 1: Back up the Existing RCA Core Server Installation

Backup the existing Core server installation and database to prepare for the upgrade.

To back up the existing installation:

1. From the RCA installation media, copy the `\Setup-Core\migrate` folder to a temporary location (for example, `C:\migrate`) on the existing Core server. You *must* copy this folder to a temporary location on the existing Core server since the upgrade scripts cannot be run directly from the RCA media.

2. Open command prompt and change the directory to the newly copied `migrate` folder.

3. Type the following command:

```
hpcabackup drive
```

where, *drive* is the drive label for the drive where you want to store the backup files. Ensure that the drive contains free space to store the backup files. The script detects the available space and provides an estimate for the required space. The space required is approximately same as the currently installed size.

For example, to store the files on `C:` drive, enter the following command:

```
hpcabackup C
```

The current installed version of the Core server is detected and, if adequate space is available, the upgrade process begins to store the backup files in `C:\HPCABackup\HPCABackup` directory.

Caution: Do NOT move the `HPCABackup` folder to another drive. If you move this folder, the restore operation does not work.

4. After the script identifies the tasks that are to be completed to initiate the backup, the `HPCA-preview-report.html` opens in the default web browser. Review the preview report carefully before you continue with the backup process.
If you are migrating from HPCA Core and Satellite version 7.90 or prior, the COP resolution process has changed. A few new classes have been added to the CLIENT domain to support the Satellite Management feature.
5. After reviewing the preview report, type `y` to start the backup process.
6. During migration, a new instance is created in the CLIENT.SUBNET class for each location in the CLIENT.LOCATION class. The CLIENT.SUBNET instance use the `LOCATIONNAME_SUBNETMASK` format. The value for LOCATIONNAME is retrieved from the CLIENT.LOCATION class in the CSDB and the value for SUBNETMASK is retrieved from the DeviceConfig table in RDBMS. If SUBNETMASK is not available in the DeviceConfig table, the backup process generates a warning that an inconsistency is identified in the CLIENT

domain, and prompts if you want to continue with the backup process. You can choose to continue or end the backup process. If all SUBNETMASKS are retrieved from the DeviceConfig table, backup process completes without any prompt.

- If you get a prompt for SUBNETMASK, browse to the CLIENT.LOCATION class in the CSDB Editor and verify if the LOCATION instance is valid. If the LOCATION instance is not required, delete the instance and run the backup process again. If you are not able to decide whether to keep or delete the location instance, contact HP Support.

Note: The subnet masks details are saved in the SUBNET_CREATE_INSTANCES.txt file located at

C:\HPCABackup\HPCABackup\rcs\database\CLIENT after the backup process is complete.

7. After the backup tasks are completed, the command prompt displays the following message:

```
Info: Action completed
Info: Backup Completed Successfully
Press [ENTER] to end
```

Note: If the backup script is run again, a new backup folder is created. The existing

C:\HPCABackup\HPCABackup folder is renamed to a timestamp folder (for example,

C:\HPCABackup\HPCABackup-1263495101) and a new

C:\HPCABackup\HPCABackup folder is created.

8. The hpca-backup-report.html file opens in the default browser. Verify this file to determine the tasks that were completed during the backup process. This file also directs you to the respective logs that you must refer to for an error or a warning message. You *must* review all error and warning messages in this file as these may indicate the need for manual intervention to ensure that settings are upgraded as per your requirement.

Task 2: Upgrade the Core Server

After you back up the existing Core server installation and database, upgrade your Core server.

To upgrade the Core server:

1. Navigate to the Setup-Core directory on RCA 9.00 installation media, and run the HPCACore.msi. The Radia Client Automation Core Installer window opens.
2. Click **Next**. The installer detects an upgrade and prompts you to confirm that you have read the migration guide and completed the prerequisite backup steps before continuing.

Caution: Failure to complete the prerequisite backup task before running the upgrade results in data loss.

4. Click **Yes** to continue with the upgrade. The Radia Client Automation Core Installer window opens.
5. Click **Next**. The Radia Client Automation Software License Agreement page opens.

6. Review the Radia Client Automation Core license terms, select **I accept the license agreement** and click **Next**. The Radia Client Automation Installation Folder page opens.
7. The Installation Folder page displays the default installation directory for the RCA Core server. Type the location where you installed previous version of the Core server and click **Next**. The Radia Client Automation Data Folder page opens.
8. The Data Folder page displays the default directory for the RCA Core server data files. Enter the location where you saved your `Data` folder for previous version of the Core server and click **Next**. The Radia Client Automation Host Name page opens.
9. Enter the hostname of the previous version of the Core server and click **Next**. The Radia Client Automation Server Ports page opens.
10. Enter the Web Server and Configuration Server ports used for previous version of the Core server and click **Next**. The Radia Client Automation Installation Confirmation page opens.
11. Click **Next** to start the installation. The existing installation is removed, and a new version is installed.
12. Click **Finish** to complete the RCA Core server installation. The RCA Core Console automatically opens, and the login window is displayed in the default browser.
13. On the login window, specify the default user name, password, and directory source. The default user name is `admin` and the password is `secret`.

Note: During upgrade, the administrator password for user `admin` is reset to `secret`.

14. Click **Sign In**. The First Time Setup Wizard opens and prompts you for initial configuration settings for your RCA environment.
15. Close this browser window. Do *not* run the First Time Setup Wizard. The settings are automatically applied during the upgrade process.
16. If you are prompted to reboot the server, click **Yes** to reboot.

Caution: You must reboot immediately when prompted. If you do not reboot when prompted, files marked for deletion are not deleted completely.

Task 3: Restore RCA Data

After you upgrade the Core server, restore the existing data into the new environment.

To restore RCA data:


1. Open the command prompt and navigate to the `migrate` folder that you created in Task 1.
2. Run `hpcarestore.cmd` followed by the drive on which you stored the backup files in Task 1. For example, to restore the files from `C:`, type:
`hpcarestore C`
 - a. After the script identifies the restore tasks to be completed, the file `HPCA-preview-report.html` opens in the default web browser. Review any `actionrequired` messages in the preview report carefully before you continue with the restore operation.

- You must review the changes required for the `rca` module. The `rca` migration logic detects any customizations you made to the CSDB class schema and attempts to merge these forward. If CSDB class schema customizations are identified, an `actionrequired` message is created for the `rca` module. The `ZEDMAMS` script is generated to migrate these CSDB customizations forward. The scripts can be located in the `\HPCABackup\HPCABackup\rca\database\CLIENT\` directory. Each such script should be manually reviewed and, if necessary, modified before continuing with the restore operation.
 - You must also review the information about the subnets that are being imported into the CLIENT domain.
 - The preview report contains an `actionrequired` message for the Policy server with the description "Policy Server processing and configuration settings has been changed since the version you are migrating from, please refer to the migration documentation for additional information on new policy server operation". The directory services configured in RCA environment for policy management are automatically mounted on Policy server for policy resolution. During this process, a `.cfg` file is created for each directory service. These configuration files include parameters used to connect to the directory services and to perform policy resolution. If you have not applied any customization to these configuration files in your environment, ignore this message. However, if you have modified the default Policy server configurations manually, complete the following steps:
 - Compare the configuration files in the `<InstallDir>\PolicyServer\etc\ldap` directory to the configuration files backed up from the previous installation to identify the additional parameters for policy resolution on a specific directory service.
 - Manually add the additional parameters in the `overrides` section of the individual configuration file.
3. After reviewing the preview report, type `y` in the command prompt to continue with the restore operation.
The data stored in the `HPCABackup` folder is upgrade into the new RCA environment.
- In case of a failure, the restore operation is triggered again from where it was left off. To perform a fresh restore, you must remove the `HPCA-restore*` files from the `HPCABackup` folder.
4. The `hpca-restore-report.html` file opens in the default web browser. Review the file to determine the changes during the restore process.
It is important to review all warning messages, as these may indicate the need for manual intervention to ensure that settings are upgraded as per your requirement.

Note: If there are unhandled errors, take corrective actions, and start the restore operation again. You *must* review the actions taken in the preview report again, and then complete the restore operation.

It is common to receive warnings during execution of the "rms" component when upgrading from version 7.50. The problems indicated by these warnings are corrected when you run `sqlmigrate` in "Task 4: Upgrade the SQL/Oracle Database" on next page.

After a successful upgrade, you can verify the subnet details by clicking **Core Console - >Configuration ->Infrastructure Management -> Satellite Management -> Subnets**. A

caution  icon is displayed with each invalid subnet. If the subnet is not required, delete the instance. If you are not able to decide whether to keep or delete the subnet, contact HP Support.

Task 4: Upgrade the SQL/Oracle Database

This task is required when upgrading from version 7.50 only. If you already have a FOREIGN KEY CONSTRAINT set to the DEVICECONFIG.DEVICE_ID column on Inventory database tables, you can skip this step.

Caution: This step should only be performed by an experienced database administrator.

After you upgrade your RCA Core server and restore your data, you must upgrade the RCA database. RCA uses `sqlmigrate` script to upgrade the database.

The `sqlmigrate` script performs the following tasks:

1. Export the contents of database tables listed in ["SQL Database Tables that must be Upgraded" on page 150](#).
2. Drop these tables.
3. Re-create these tables.
4. Import the data into the updated table structure.

You can also perform these steps manually as described in ["Upgrading the RCA SQL/Oracle Database Manually" on page 149](#).

To upgrade the RCA database:

1. Stop the RCA Core service.
2. Open command prompt and navigate to the local copy of the `migrate` folder. Change your current directory to `sql` folder. For example: `cd C:\migrate\sql`

3. Run the following command:
`sqlmigrate DriveLetter`

where, *DriveLetter* is the drive where the script stores exported data and any error information created during the subsequent import. Data is stored at the following location:

`DriveLetter:\HPCABackup\SQLMigrate`

For large databases, this upgrade step may take many hours.

Note: If the `sqlmigrate` script is run again, a new data folder is created. The `C:\HPCABackup\SQLMigrate` folder is renamed to a timestamp folder as `C:\HPCABackup\SQLMigrate-timestamp` where, *timestamp* indicates when the data folder was created.

4. Verify the contents of the `C:\HPCABackup\SQLMigrate\errors` folder to ensure that the upgrade was successful. If errors occurred during the upgrade of a particular table, the following files are created in this folder.
 - `tablename.log` contains the insert statement and any errors that occurred.
 - `tablename.tsv` contains the rows (if any) that failed to import.
 - `tablename.sql` is a SQL script for insert statement that failed, where, *tablename* corresponds to the name of the pertinent database table. You *must* run this script manually to fix the errors.

Verify these files to determine if you need to perform any manual restoration of data.

For a list of the tables upgraded by the `sqlmigrate` script, see ["SQL Database Tables that must be Upgraded" on page 150](#).

5. Restart the RCA Core service.

Task 5: Update HP Live Network Content

To update your HP Live Network Content:

1. Open a web browser and log on the Core Console using the following URL:
`http://HPCA_host:3466`
Where *HPCA_host* is the Core server's host name.
2. Enable remote access to the Core server communication ports.
3. Validate your HP Live Network configurations and perform a full HP Live Network update to ensure that you have downloaded the latest service content.

Task 6: Set the Patch Management Options

Set the following patch management options:

- During upgrade, the **Agent Updates Version** under **Core Console > Configuration > Patch Management > Agent Updates** is set to the newer version. If you do not plan to upgrade the Patch Agent to the newer version on the client devices, you must set the version to the previous version that was applied before upgrading.
- During upgrade, the **Enable Download of Patch Metadata only** option under **Core Console > Configuration > Patch Management > Distribution Settings** is set to enabled. You must disable the **Enable Download of Patch Metadata only** option after upgrading if you do not want to use the metadata model for Microsoft bulletins.

Task 7: Upgrading Deployed Components

After upgrading the Core server, upgrade the following RCA components deployed in your environment:

- ["Upgrading RCA Satellite Servers" on next page](#)
- ["Upgrading RCA Agent" on page 131](#)
- ["Upgrading RCA Administrator Tools" on page 148](#)

Upgrading RCA Satellite Servers

This section provides information on how to upgrade the RCA Satellite server.

Hardware and Software Requirements

For the hardware and software requirements, see the ["Hardware and Software Requirements"](#) on page 47

Installation Prerequisites

You must ensure that the drive contains adequate free space to store the backup before upgrading RCA Satellite server.

Upgrade Process

If you have a customized set-up that uses resources from the CSDB on the Satellite server, make sure that the dataless parameter value is set to 0 in the dmabatch.rc file on the Satellite server. Doing this, the backup and restore procedure automatically takes backup of the resources on Satellite and restores them during the restore procedure. This prevents the download of all resources from the Core server when the initial synchronization happens after Satellite upgrade.

The RCA Satellite server upgrade process includes four tasks:

- ["Task 1: Back up the Existing Satellite Server Installation"](#) below
- ["Task 2: Upgrade the Satellite Server"](#) on next page
- ["Task 3: Restore RCA Data"](#) on page 127
- ["Task 4: Synchronize Satellite"](#) on page 128

You can also upgrade the Satellite servers by using RCA Console as described in the section ["Upgrading Satellite Server Using RCA Console"](#) on page 128.

Task 1: Back up the Existing Satellite Server Installation

Backup the existing RCA Satellite server installation to prepare for the upgrade.

To back up the existing RCA Satellite server installation:

1. From the RCA installation media, copy the `\Setup-Satellite\migrate` folder to a temporary location on the RCA Satellite server (for example, `C:\migrate`). You *must* copy this folder to a temporary location since the migration scripts cannot be run directly from the RCA media.
2. Open command prompt and change the directory to the newly copied `migrate` folder.
3. Type the following command:
`hpcabackup drive`

where, *drive* is the drive label for the drive where you want to store the backup files.

For example, to store the files on C : drive, enter the following command:

```
hpcabackup C
```

The current version of the Satellite server is detected and, if adequate space is available, the upgrade process begins to store the backup files in C : \HPCABackup\HPCABackup

4. After the script identifies the tasks that are to be completed to initiate the backup, the `hpcapreview-report.html` opens in the default web browser. On the command prompt, type **y** to start the backup tasks.
5. After the backup tasks are completed, the command prompt displays the following message:
Info: Action completed
Info: Backup Completed Successfully
Press [ENTER] to end

Caution: Do *not* move the HPCABackup folder to another drive. If you move this folder, the restore operation does not work.

Note: If the backup script is run again, a new backup folder is created. The C : \HPCABackup\HPCABackup folder is renamed to a timestamp folder (for example, C : \HPCABackup\HPCABackup-1263495101) and a new C : \HPCABackup\HPCABackup folder is created.

6. The `hpcapreview-report.html` file opens in the default browser. Verify this file to determine the tasks that were completed during the backup process. You *must* review all error and warning messages in this file, as these may indicate the need for manual intervention to ensure that settings are migrated properly.

Task 2: Upgrade the Satellite Server

After you backup the existing Satellite server installation, upgrade your Satellite server.

To upgrade the Satellite server:

1. Navigate to the `Setup-Satellite` directory on RCA 9.00 installation media, and run the `HPCASatellite.msi`. The Radia Client Automation Satellite Installer window opens.
2. Click **Next**. The installer detects an upgrade and prompts you to confirm that you have read the migration guide and completed the backup task before continuing.
3. Click **Yes** to continue with the upgrade. The Radia Client Automation Satellite Installer window opens.
4. Click **Next**. The Radia Client Automation Software License Agreement page opens.
5. Review the Radia Client Automation Satellite license terms, select **I accept the license agreement**, and then click **Next**. The Radia Client Automation Installation Folder page opens.
6. The Installation Folder page displays the default installation directory for the RCA Satellite server. Type the location where you installed previous version of the Satellite server and click **Next**. The Radia Client Automation Data Folder page opens.

7. The Data Folder page displays the default directory for the RCA Satellite server data files. Enter the location where you saved your `Data` folder for previous version of the Satellite server and click **Next**. The Radia Client Automation Host Name page opens.
8. Enter the hostname of the previous version of the Satellite server and click **Next**. The Radia Client Automation Server Ports page opens.
9. Enter the Web Server and Configuration Server ports used for previous version of the Satellite server and click **Next**. The Radia Client Automation Installation Confirmation page opens.
10. Click **Next** to start the installation. The existing installation is removed, and the new version is installed.
11. Click **Finish** to complete the RCA Satellite server installation. The Windows Security login window opens in your default browser.
12. On the login window, specify the default user name, password, and directory source. The default user name is `admin` and the password is `secret`.

Note: During upgrade, the administrator password for user `admin` is reset to `secret`.

13. Click **OK**. The First Time Setup Wizard opens, and prompts you for initial configuration settings for the RCA environment.
14. Close this browser window. Do *not* run the First Time Setup Wizard. Your settings are automatically applied during the upgrade process.

If you are prompted to reboot the server, click **Yes** to reboot.

Caution: You must reboot immediately when prompted before continuing further. If you do not reboot, files marked for deletion are not deleted completely.

Task 3: Restore RCA Data

After you upgrade the Satellite server, restore your existing data into the new environment.

To restore RCA data:

1. Open the command prompt and navigate to the `migrate` folder that you created in Task 1.
2. Run `hpcarestore.cmd` followed by the drive on which you stored the backup files in Task 1. For example, to restore the files from `C:`, type:
`hpcarestore C`
3. After the script identifies the restore tasks to be completed, the file `HPCA-preview-report.html` opens in the default web browser. Review this preview report.
4. After reviewing the preview report, type `y` in the command prompt to continue with the restore operation.
The data stored in the `HPCABackup` folder is migrated into the new RCA environment.

If a failure occurs during restore, subsequent restore attempts are triggered from where restore operation left off. To perform a fresh restore, you must remove the `HPCA-restore*` files from the `HPCABackup` folder.

5. The `hpca-restore-report.html` file opens in the default web browser. You must review all error and warning messages in this file, as these may indicate the need for manual intervention to ensure that settings are migrated as per your requirement.

Note: If there are unhandled errors, take corrective actions, and start the restore operation again. You *must* review the actions taken in the preview report again, and then complete the restore operation.

Note: RCA resource data is converted from Apache format to the Integration-based Proxy server format and moved to the Proxy server Data location during the restore process for versions 7.50, 7.80, and 7.90. For example, after restore process is complete, the converted RCA resource data is copied to the `\Data` directory. Default location of `\Data` directory is `C:\Program Files\Hewlett-Packard\HPCA\Data\ProxyServer\static`.

Task 4: Synchronize Satellite

After you upgrade a Satellite server, you must synchronize it with its Core server.

To synchronize a Satellite server:

1. Open a web browser and browse to the following URL to open the Satellite Console :
`http://<localhost>:3466`
where, `<localhost>` is the IP address of the Satellite server.
2. Logon to the Satellite server using the default user name and password. The default user name is `admin` and the password is `secret`.
3. On the Operations tab, click **Server Status**.
4. Click **Synchronize satellite now**.

You have now successfully upgraded your Satellite server.

Upgrading Satellite Server Using RCA Console

To upgrade your existing Satellite server using RCA Core Console, complete the following steps:

1. On the Core server, logon to the Core Console.
2. On the **Configuration** tab, go to the **Infrastructure Management > Satellite Management** area.
3. Click the **Servers** tab.
4. Select the device on which you want to upgrade the Satellite server in the Satellite Servers list.
5. Click the **Install the Satellite Server** toolbar button to launch the wizard.
6. Type the User ID and Password to be used for deployment. This account must have administrator-level access on the target device.
7. Click **Next**. The Properties window opens.

8. Select the Installation Drive, Data Drive, and Deployment Mode. You must select same settings as used for Satellite server before upgrading.
9. Click **Next**. The Schedule window opens.
10. Specify the run schedule for the deployment job. Select **Run: Now** to deploy the Satellite server immediately after you complete the steps in the wizard, or select **Run: Later** to schedule a date and time for deployment.
11. Click **Next**. The Summary window opens.
12. Review the summary information.
13. Click **Submit**. A Satellite Server Deployment job is created. The deployment may take a long time with limited bandwidth. You can check the status of the job in the **Jobs Management** area on the **Management** tab.
14. Click **Close** to exit the wizard.

Note: After a successful Satellite server upgrade for versions 7.50, 7.80, and 7.90, RCA resource data is converted from Apache format to Integration-based Proxy server format and moved to the Satellite server data location. The default Satellite server data location is `<InstallDir>\Data\ProxyServer\static`.

Upgrading Proxy Servers

This section provides information on how to upgrade the classic Proxy server on Windows. You can upgrade classic Proxy server on Windows using the media or by using the Core server console as described in the next sections.

You cannot upgrade classic Proxy server on Linux. Install the Proxy server on Linux again to use the Proxy server on Linux with RCA 9.00.

Upgrading Proxy Server to Satellite Server

To upgrade the classic Proxy server (RPS) installed on Windows to the Satellite server:

1. Copy the `\Setup-Satellite` folder from RCA installation media and paste it to a temporary location on Proxy server computer. For example, `C:\Temp`.
2. Navigate to the `C:\temp\Setup-Satellite` folder.
3. Open the command prompt and type the following command:
`migrate-satellite-unattended.cmd -proxyserver-cache-dir
<proxyserver-cache-dir_path>[-logfile <logfile_path>]`

where,

- `<proxyserver-cache-dir_path>` is the full path of the current target Proxy server cache directory. For example, `C:\Program Files\Hewlett-Packard\HPCA\Data\ProxyServer`.
- `logfile` is full path and file name of the log to which messages should be written. This parameter is optional. For example, `C:\temp\proxy-migration.log`.

Following is a sample command:

```
migrate-satellite-unattended.cmd -proxyserver-cache-dir "C:\Program  
Files\Hewlett-Packard\HPCA\Data\ProxyServer" -logfile  
"C:\temp\proxy-migration.log"
```

4. After you upgrade to the Satellite server, run the First Time Setup Wizard (see "[Post Installation Configuration](#)" on page 50) to apply post-install configurations to this Satellite server.
5. Synchronize the Satellite server with its upstream host. For more information, see "[Task 4: Synchronize Satellite](#)" on page 128.

Note: After a successful upgrade from Proxy server to Satellite server, RCA resource data is moved to the Satellite server data location. Following are the default Satellite server data locations for static and dynamic cache:

```
<InstallDir>\Data\ProxyServer\static  
<InstallDir>\Data\ProxyServer\dynamic
```

Upgrading Proxy Server to Satellite Server Using RCA Console

Use the Satellite Server Deployment Wizard to upgrade the Classic Proxy server (RPS) and enable remote services, such as data caching.

To upgrade the Proxy server on Windows:

Task 1: Add the Proxy server on Windows to the Core and Satellite servers group.

For information on how to add a device to the Core and Satellite group, see the *Add a Satellite Server* section in the *Radia Client Automation Enterprise User Guide*.

Task 2: Upgrade the Proxy server on Windows as follows:

1. On the **Configuration** tab, go to the **Infrastructure Management**, and then click **Satellite Management**.
2. Click the **Servers** tab.
3. Select the Proxy server computer that you added to the Core and Satellite servers group in Task 1.
4. Click the **Install the Satellite Server** toolbar button to launch the wizard.
5. Type the User ID and Password to be used for deployment. This account must have administrator-level access on the target device.
6. Click **Next**. The Properties window opens.
7. Select the Installation Drive, Data Drive, and Deployment Mode.
8. Click **Next**. The Schedule window opens.

9. Specify the run schedule for the deployment job. Select **Run: Now** to deploy the Satellite server immediately after you complete the steps in the wizard, or select **Run: Later** to schedule a date and time for deployment.
10. Click **Next**. The Summary window opens.
11. Review the summary information.
12. Click **Submit**. A Satellite Server Deployment job is created. The deployment may take a long time with limited bandwidth. You can check the status of the job in the **Jobs Management** area on the **Management** tab.
13. Click **Close** to exit the wizard.
14. After you upgrade to the Satellite server, run the First Time Setup Wizard (see "[Post Installation Configuration](#)" on page 50) to apply post-install configurations to this Satellite server.
15. Synchronize the Satellite server with its upstream host. For more information, see the "[Task 4: Synchronize Satellite](#)" on page 128.

Note: After a successful upgrade from Proxy server to Satellite server, RCA resource data is moved to the Satellite server data location. Following is the default Satellite server data location:

```
<InstallDir>\Data\ProxyServer\static  
<InstallDir>\Data\ProxyServer\dynamic
```

Note: After successful Satellite server upgrade, the synchronization status fields on the **Configuration** tab > **Infrastructure Management** > **Servers** tab do not show any values. The synchronization status fields are populated after the Satellite servers are synchronized with upstream server.

Upgrading RCA Agent

The following sections describe how you can upgrade RCA agent on a Windows, Linux, and Macintosh device.

Use the upgrade procedures described in this section to upgrade the RCA agent from the following versions:

- RCA Agent version 7.50
- RCA Agent version 7.80
- RCA Agent version 7.90
- RCA Agent version 8.10

You can verify `upgrade.log` in the `%IDMLOG%` directory to check the status of the agent upgrade.

Prerequisites

The following prerequisites must be met before you start the upgrade process:

- When scheduling the agent migration, ensure that the agent does not have other connects scheduled at the same time. The connects can be resumed after the agent upgrade is complete.
- Modify the `identification` and `startdir` parameters in the [Args] section of the `Install.ini` file, such that the device does not have a SYSTEM connect. If these values are not modified, the `Install.ini` overwrites the default values in the existing `args.xml` file after the upgrade and the RCA Application Self-Service Manager has a SYSTEM connect.
- Ensure that you meet all the requirements described in the sections "[Hardware and Software Requirements](#)" on page 71 and "[Installation Prerequisites](#)" on page 72.

Upgrading RCA Agent on Windows

When upgrading, the RCA agent is installed in the existing agent installation directory. By default, the agent is installed in the following directory:

- RCA 7.5x and above: `C:\Program Files\Hewlett-Packard\RCA\Agent`

You can upgrade the RCA Agent using the following methods:

- "[Upgrading Using RCA Installation Service](#)" below
- "[Upgrading Agent Using RCA Core Console](#)" on page 134
- "[Upgrading Using Installation Media](#)" on page 134

RCA supports direct upgrade, which means that you are not required to uninstall an earlier agent version from the managed device before upgrading.

Upgrading Using RCA Installation Service

This section describes how to use the RCA agent installation service to perform the RCA agent upgrade. The upgrade is a two-step process, where you must first import the RCA agent installation service to the RCA CSDB, and then configure this service for distribution.

Task 1: Importing the Decks

Complete the following steps to import the decks:

1. Stop the RCA Configuration Server service.
 - Using command prompt: Run the command `net stop ztoptask`.
 - Using Control Panel: Click **Start > Control Panel > Administrative Tools > Services**. From the list of services, select **RCA Configuration Server** and click **Stop the service**.
2. Navigate to the `Setup-Core\Media\client\Migration` directory on the RCA installation media folder. Copy the RCA agent installation service files, `HPCA_AGENT_90_UPGRADE_WIN.XPI` and `HPCA_AGENT_90_UPGRADE_WIN.XPR` and paste them to the `\bin` directory of the RCA Configuration server.
3. Open command prompt and change the directory path to:
`<InstallDir>\ConfigurationServer\bin`.

4. Type the following command to import the instances and press **Enter**:
`ZEDMAMS VERB=IMPORT_INSTANCE,FILE=HPCA_AGENT_90_UPGRADE_
WIN.XPI,PREVIEW=NO`
5. Review the `ZEDMAMS.LOG` file created in the `\bin` directory to ensure that there are no errors and that the import completed successfully with Return Code (RC) 0.
6. Type the following command to import the resources and press **Enter**:
`ZEDMAMS VERB=IMPORT_RESOURCE,FILE=HPCA_AGENT_90_UPGRADE_
WIN.XPR,PREVIEW=NO`
7. Review the `ZEDMAMS.LOG` file created in the
`<InstallDir>\ConfigurationServer\bin` directory to ensure that there are no errors and that the import completed successfully with RC 0.
8. Close the command prompt window.
9. Start the RCA Configuration Server service.
 - Using command prompt: Run the command `net start ztoptask`.
 - Using the Control Panel: Click **Start > Control Panel > Administrative Tools > Services**. From the list of services, select **RCA Configuration Server** and click **Restart the service**.
10. Use the RCA Administrator CSDB Editor to view the new service in `PRIMARY.SOFTWARE.ZSERVICE`.

Task 2: Configuring the RCA Agent Installation Service

Complete the following steps to configure the RCA Agent installation service:

1. Open the RCA Administrator CSDB Editor.
2. On the Options menu, click **Advanced tab** and select **Show Edit Replace and Add Component options for File type components**.
3. Navigate to the `Install.ini` resource of the RCA 9.00 update service.
4. Right-click **Install.ini** in the tree view and select **Edit this Component** from the shortcut menu.
5. The Editor Selector for `Install.ini` dialog box opens. Use this dialog box to select the resident editor you want to use to make the changes to this file. For example, select **Notepad** to open the `Install.ini` file with `Notepad.exe`.
6. Save and close the `Install.ini` file.
7. Connect the service to the appropriate users for distribution.

After the service is distributed to a user and the RCA agent upgrade is complete, the service is not available to the user. This service is automatically removed from the RCA agent desktop. There is a ZSTOP expression in the RCA agent upgrade (ZSERVICE) instance that evaluates to TRUE after the RCA agent is upgraded. After the expression evaluates to TRUE, the temporary service folder and the RCA agent installation files are removed.
8. Reboot the agent device.

Upgrading Agent Using RCA Core Console

You can deploy the latest version of the Agent to the devices in your infrastructure by scheduling an agent deployment job in the RCA Core Console.

Using the Radia Client Automation Core Console, complete the following tasks to upgrade an existing agent version:

1. Click **Management** tab.
2. Under Directories area, click **Devices**.
3. Select the devices for which you want to upgrade the agent and click **Launch the RCA Agent Deployment Wizard**. The Step 1 screen for Agent Deployment Wizard opens.
4. Specify the credentials that have administrative privileges to deploy the Agent.
5. Select **Silent Install** check box for silent installation and click **Next**. The Step 2 screen for Agent Deployment Wizard opens.
6. Type the schedule information for when the Agent Deployment job should run and click **Next**. The Step 3 screen for Agent Deployment Wizard opens.
7. Review the job summary and click **Submit**. The agent deployment job is created. You can check the status of the job using the **Jobs** area in the **Management** tab.

Upgrading Using Installation Media

You can use the RCA agent installer to upgrade your managed devices. You can find the RCA agent installer in the RCA DVD media in the `<media_root>\Setup-Core\Media\client\default\win32` directory. When you run the `setup.exe` file to initiate the agent upgrade, this file checks if a previous version of the agent is installed. If an earlier version is detected, the `setup.exe` file calls the `upgrdmaint.exe` file, which performs the RCA agent upgrade. Thereafter, the RCA Agent Installation Wizard opens and the normal installation process is followed. For more information on how to install an agent using the wizard, see the section ["Installing RCA Agent using Wizard" on page 83](#).

Upgrade Scenarios: Lockdown and Non-Lockdown Mode

This section includes upgrade scenarios for:

- RCA agent 7.80 or 7.90 Non-Lockdown to RCA agent 9.00 Non-Lockdown mode.
- RCA agent 7.80 or 7.90 Non-Lockdown to RCA agent 9.00 Lockdown mode.
- RCA agent 7.8.1 or 7.90 Lockdown to RCA agent 9.00 Lockdown mode.
- RCA agent 7.8.1 or 7.90 Lockdown to RCA agent 9.00 Non-Lockdown mode.

Upgrading from Non-Lockdown to Non-Lockdown Mode

The RCA agent 7.80, 7.90, and 8.10 can be upgraded to RCA agent 9.00 with Non-Lockdown mode by using a simple upgrade. For information on the upgrade steps, see ["Upgrading RCA Agent on](#)

[Windows" on page 132.](#)

Upgrading from Non-Lockdown to Lockdown Mode

Complete the following tasks to upgrade RCA agent in Lockdown enabled mode:

Task 1: Update the install.ini file

Set the following Lockdown parameters in the [Properties] section of the `Install.ini` file:

```
[Properties]
```

```
LOCKDOWN=Y
```

```
LOCKDOWNSCRIPT=<Customized-Script>
```

where, customized script is the script you can use to set the Access Control Lists (ACLs) to the agent folders in the RCA environment. It provides a sample file, `setaccls.bat` that contains sample statements that you can use to create a customized script. Ensure that the customized script is in the same directory as the `Install.ini` and `setup.exe` files.

Task 2: Upgrade the agent

Upgrade the agent using the procedures listed in the section "[Upgrading RCA Agent on Windows" on page 132.](#)

Task 3: Migrate the User Data to the User Profile

Transfer the user data to the respective user profiles. You can retain the user data in the respective user profiles by running the `secure_migrate.tcl` script. The `secure_migrate.tcl` script automatically reads all the data objects in the `IDMROOT` folder, `<InstallDir>\Agent\Lib`, for each user and moves the data objects to the user profile set in the script.

- On Windows XP and Windows 2003 Server, the Administrator user contents are moved to:
`C:\Documents and Settings\Administrator\Local Settings\Application Data\HPCA\Agent`
- On Windows Vista, Windows 7, and Windows 2008 Server, the Administrator user contents are moved to:
`C:\Users\Administrator\AppData\Local\HPCA\Agent`

Note: If you need to run the customized script for setting ACLs as well as the `secure_migrate.tcl` script, you can append the contents of the `secure_migrate.tcl` script to the customized script. Use this customized script in the `LOCKDOWNSCRIPT` parameter in the [Properties] section of the `Install.ini` file.

To migrate the user data to the respective user profiles, follow these steps:

1. Copy the `secure_migrate.tcl` file from `Setup-Core\Media\client\default\win32` folder to the `IDMSYS` folder.
2. Open command prompt and type the following command:
`nvdkit secure_migrate.tcl -idmsur <User-Folder-path> -usrmsi <User-Msi-Folder-path>`
On Windows Vista, Windows 7, and Windows 2008 Server, the `User-Folder-path` is:
`C:\Users\<username>\AppData\Local\HPCA\Agent`

On Windows XP and Windows 2003 Server, the *User-Folder-path* is:

C:\Documents and Settings\<username>\Local Settings\Application Data\HPCA\Agent

Tip: You can move the data objects of all the users at the same time by replacing the <username> with the value ZUSERID in the above mentioned paths.

The *User-Msi-Folder-path* is the IDMUSRMSI path

IDMUSRMSI=" <InstallDir>\Agent\usermsi"

Upgrading from Lockdown to Lockdown Mode

Complete the following tasks before upgrading to RCA agent 9.00 in Lockdown enabled mode:

Task 1: Retain ACL Settings:

In RCA 7.8.1, the `setsecure.bat` file is used to enable the Lockdown mode and to set the Access Control Lists (ACLs) to the agent folders. Complete the following steps, to retain the ACL settings:

1. Copy the customized script you had previously created for RCA 7.8.1, 7.90, and 8.10 to the folder `Setup-Core\Media\client\default\win32`. The contents of this folder are delivered to the target device during remote deployment.
2. Set `LOCKDOWN=Y` in `Install.ini` file of RCA 9.00 to enable Lockdown.
3. Set `LOCKDOWNSCRIPT=<Customized-Script>`.

Note: It recommends that when you upgrade to RCA 9.00, do not use the default `setsecure.bat` and `setaccls.bat` files in the `LOCKDOWNSCRIPT` parameter. Update these files based on your requirements.

Task 2: Retain User Contents after Upgrade:

Modify the [Properties] section of `Install.ini` file of RCA 9.00 for `IDMUSR` to retain the user contents after a successful upgrade. Set the `IDMUSR` value in the latest version to the `IDMUSR` value used in the previous version of agent installation.

Task 3: Update the Registry for NVD.INI file Location:

In a Non-Lockdown enabled mode, the `NVD.INI` file resides in the `IDMROOT` folder, `<InstallDir>\Agent\Lib`. The `NVD.INI` file location saved in the registry file is `HKEY_LOCAL_MACHINE\Software\Novadigm\Radia\Settings\INIPath`.

When the Lockdown mode is enabled, the `NVD.INI` file is moved from the `IDMROOT` folder to the `IDMSYS` folder, `<InstallDir>\Agent`. After the `NVD.INI` file is moved, it is no longer available to the user.

After the Lockdown mode is enabled, the location of the `NVD.INI` file is changed to the `IDMSYS` folder, however, the path for `IDMROOT` folder is retained in the registry file. When upgrading to RCA agent 9.00 in Lockdown enabled mode, update the registry file to reflect the new location of the `NVD.INI` file. This prevents a new installation of the RCA agent.

Use one of the following methods to ensure that the registry contains the correct location of the `NVD.INI` file:

- Modify the registry using command line or batch mode (preferred method) as follows:
 - a. Create an `updateINIPath.txt` file with the following content, `HKEY_LOCAL_MACHINE\SOFTWARE\Novadigm\Radia\SettingsINIPath = REG_SZ "C:\PROGRA~1\HEWLET~1\HPCA\Agent\"`
 - b. From the command line, run the command `regini updateINIPath.txt`. You can also run this command on all the target devices before the upgrade.
- Ensure that the `NVD.INI` file resides in both the `IDMSYS` and the `IDMROOT` folder. You can write a script to copy the `NVD.INI` file from the `IDMSYS` folder to `IDMROOT` folder.
- Uninstall the existing agent and install the RCA agent 9.00 with Lockdown enabled mode. Only the SYSTEM or an Administrator user can uninstall the RCA agent.

Task 4: Upgrade the agent

Use the simple upgrade process to upgrade the agent as described in ["Upgrading RCA Agent on Windows" on page 132](#).

Upgrading from Lockdown to Non-Lockdown Mode

To upgrade to RCA agent in Lockdown mode 9.00 with Non-Lockdown mode, complete the following steps:

1. Uninstall the existing agent from the target device.
2. Install the RCA agent 9.00 without setting the Lockdown parameters in the [Properties] section of the `Install.ini` file.

Note: Upgrading Lockdown enabled RCA 7.8.1 or 7.90 agent to RCA agent 8.10 with Non-Lockdown mode is not supported.

Upgrading RCA Agent on Linux and Macintosh

Use the upgrade procedures described in this section to upgrade the Linux or Macintosh RCA agents to version 9.00.

You can upgrade the RCA agent using the following methods:

- ["Upgrading Using RCA Installation Service" on next page](#)
- ["Upgrading Using Installation Media" on page 146](#)
- Upgrading using sample services:
It provides the following sample services that can be used to perform an agent upgrade to the current RCA version:
 - **HPCA_AGENT_90_UPGRADE_LINUX**
Installation of this service upgrades a pre-existing Red Hat Linux (Intel architecture) or SUSE agent to the current version.

- **HPCA_AGENT_90_UPGRADE_MACX86**

Installation of this service upgrades a pre-existing Macintosh x86 agent to the current version.

All of the parameters pertaining to the agent upgrade that can be configured are specified in the UPGRADE instance in the RCA Core server entitlement model.

Upgrading Using RCA Installation Service

This section describes how to perform an agent upgrade using the export decks. These are included on the RCA installation media in the `/Setup-Core/Media/client/Migration` directory.

- **UPGRADE.XPC**

This is a class export of a new class required for the agent upgrade. It contains the definition of the PRIMARY.SOFTWARE.UPGRADE class.

- RCA Agent installation service files

- **For RedHat and SUSE Linux:**

- `HPCA_AGENT_90_UPGRADE_LINUX.XPI`
- `HPCA_AGENT_90_UPGRADE_LINUX.XPR`

- **For Macintosh:**

- `HPCA_AGENT_90_UPGRADE_MACX86.XPI`
- `HPCA_AGENT_90_UPGRADE_MACX86.XPR`

Task 1: Importing the Classes, Instances, and Resources

To distribute the RCA agent as a RCA service, you must import the agent **UPGRADE** class definition as well as upgrade service data into your RCA CSDB.

Note: RCA Core server is supported only on a Windows platform. However, the RCA agent supports backward compatibility. Therefore, the export decks can be imported into the RCA Core server running on a Linux platform.

To import the required classes, instances, and resources:

1. Stop the RCA Configuration Server service.
 - **For Microsoft Windows:**
 - Open the command prompt and run the `net stop ztoptask` command.
 - Click **Start > Control Panel > Administrative Tools > Services**. From the list of services, select **RCA Configuration Server** and click **Stop the service**.
 - **For Linux:**
 - Run the script `killmgr` located in the `/opt/HP/CM/ConfigurationServer/bin` directory.
2. Copy the appropriate export decks (as listed above) into the RCA Configuration server `binary` or `executable` directory, `<InstallDir>\Configuration Server\bin`, if the RCA Configuration server is running on a Microsoft Windows platform.

Note: Consider the following when transferring the XPI and XPR files from one device to another using FTP:

- XPR files are binary and should be transferred in binary mode.
- XPI files are ASCII and should be transferred in ASCII mode.

3. Open the command prompt and change your current working directory to the RCA Configuration server `binary` or `executable` directory where you copied the export decks in step 2.
4. Import the UPGRADE class by running the following command:

```
ZEDMAMS VERB=IMPORT_CLASS,FILE=UPGRADE.XPC,PREVIEW=NO.
```
5. Review the `zedmams.log` file created in the RCA Configuration server `binary` or `executable` directory to ensure that there are no errors and that the import completed successfully with RC 0.
6. Import the required instances by running the following example command:

```
ZEDMAMS VERB=IMPORT_INSTANCE,FILE=HPCA_AGENT_90_UPGRADE_LINUX.XPI,  
PREVIEW=NO
```

or

```
ZEDMAMS VERB=IMPORT_INSTANCE,FILE=HPCA_AGENT_90_UPGRADE_MACX86.XPI,  
PREVIEW=NO.
```
7. Review the `zedmams.log` to ensure that there are no errors and that the import completed successfully with RC 0.
8. Import the required resources by running the following example command:

```
ZEDMAMS VERB=IMPORT_RESOURCE,FILE=HPCA_AGENT_90_UPGRADE_LINUX.XPR,  
PREVIEW=NO
```

or

```
ZEDMAMS VERB=IMPORT_RESOURCE,FILE=HPCA_AGENT_90_UPGRADE_MACX86.XPR,  
PREVIEW=NO.
```
9. Review the `zedmams.log` to ensure that there are no errors and that the import is completed successfully with RC 0.
10. Close the command prompt.
11. Start the RCA Configuration Server service as follows:
 - Run the `net start ztoptask` command from the command prompt.
 - Click **Start > Control Panel > Administrative Tools > Services**. From the list of services, select **RCA Configuration Server** and click **Restart the service**.

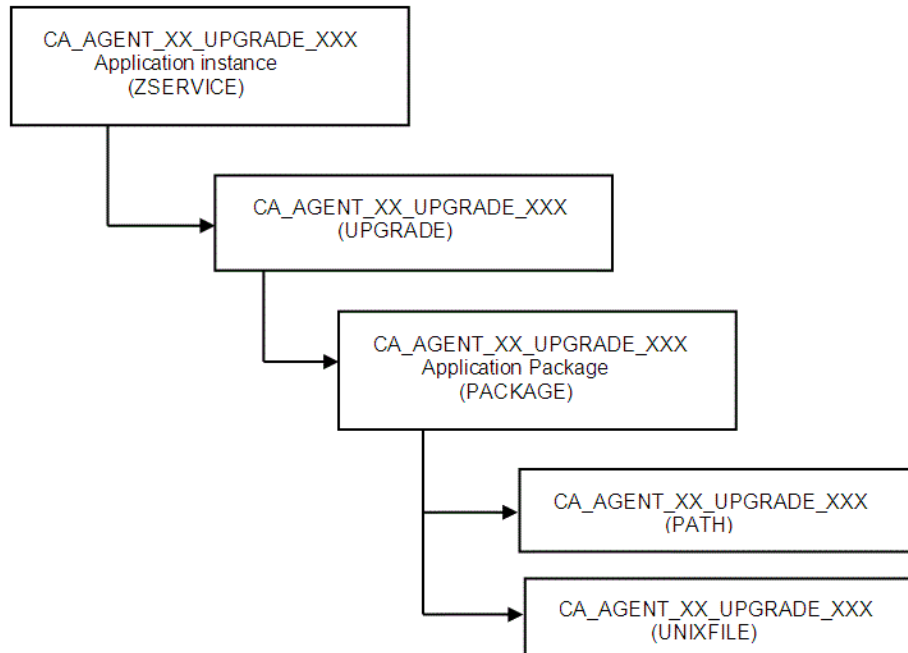
Use the RCA Administrator CSDB Editor to view the new UPGRADE class and service specific data. After the successful completion of the above steps, you can find:

- A new class named **UPGRADE** within the PRIMARY.SOFTWARE domain.
- Sample RCA agent upgrade Application Services within your SOFTWARE.ZSERVICE class.
- Sample UPGRADE instance data within the PRIMARY.SOFTWARE.UPGRADE class.
- Sample PACKAGES within the PRIMARY.SOFTWARE domain.

These imported services are mandatory services distributed to RCA agents by using the RCA Application Manager.

The following figure displays the model for the supplied agent Upgrade Application Services.

Model for the Agent Upgrade Service



UPGRADE Class

The UPGRADE class instance is connected between the upgrade SERVICE and PACKAGE instances. It is responsible for the resolution of the agent upgrade decks as well as for launching the agent upgrade process. All upgrade configuration options are defined within the UPGRADE class instance.

ZSTOP Expressions

The sample UPGRADE instances contain multiple ZSTOP expressions that identify the specific operating system for which the UPGRADE applies and for the RCA Application Manager Agent version. The purpose of these expressions is to enable the resolution for a specific operating system and to prevent the resolution for an agent that has been upgraded already.

For example, in the SOFTWARE.UPGRADE.HPCA_AGENT_90_UPGRADE_LINUX instance, the first ZSTOP expression `WORDPOS (EDMGET (ZMASTER, ZOS) , ' UNIXLNUX') =0` causes the resolution to continue only if the agent operating system is Red Hat Linux or SuSE.

For Macintosh, in the SOFTWARE.UPGRADE.HPCA_AGENT_90_UPGRADE_MACX86 instance, the first ZSTOP expression `WORDPOS (EDMGET (ZMASTER, ZOS) , ' MACOSX') =0` causes the resolution to continue only if the agent operating system is Macintosh.

The other ZSTOP expressions cause the resolution to continue only if the ZPKGREL variable in the current RCA Application Managers agent ZMASTER object contains a value less than the

current version. This expression stops the deployment of the agent upgrade to agents that are already running the latest version.

You can find these same expressions in the sample SERVICE instances provided.

Always Connection

The ALWAYS connection in the upgrade instance creates an association with the operating system-specific package that contains the agent upgrade decks. (For example, the SOFTWARE.UPGRADE.HPCA_AGENT_90_UPGRADE_LINUX instance has an Always Connection of: SOFTWARE.PACKAGE.HPCA_AGENT_90_UPGRADE_LINUX, the package that contains the Linux Agent upgrade decks). The value of this attribute in any UPGRADE instance should contain the name of the PACKAGE instance that is prefixed with the operating system-specific designator that matches the intended target operating system.

Create Method (ZCREATE)

The sample UPGRADE instance contains a create method that causes the upgrade script to be launched with the values specified in the UPGRADE class instance attributes. This method is called only when the agent upgrade materials are initially installed on disk.

Verify Method (ZVERIFY)

The sample UPGRADE instance contains a verify method that causes the upgrade script to be launched with the values specified in the UPGRADE class instance attributes. This method is called only after the verify method is successful. The upgrade process starts again if the agent upgrade fails when you install the upgrade decks. The agent upgrade may fail because of disk space or agent in use.

Update Method (ZUPDATE)

The sample UPGRADE instance contains an update method value that launches the upgrade script with the values specified in the UPGRADE class instance attributes. This method is called only after the update method is successful. If the agent upgrade fails when you install the upgrade decks first, and updated agent upgrade decks are available in the connected RCA Configuration server, the update method is launched after the successful installation of these updated materials, initiating the upgrade process again.

Media Directory (MEDIADIR)

The media directory attribute MEDIADIR contains the value of & (ZMASTER.ZSYSDIR) /ClientUpgrade. This is the default location where the upgrade process expects to find the agent upgrade decks, when they are downloaded to the agent workstation.

Retry Attributes (ATTEMPTS and INTERVAL)

When the agent upgrade service finds that the agent is in use, it attempts the upgrade a number of times at a specified interval. The ATTEMPTS attribute sets the number of times to retry the

upgrade, although the INTERVAL attribute specifies the number of seconds the upgrade waits between retry attempts. The default value for both the ATTEMPTS and INTERVAL attributes is 60.

A value of zero in the ATTEMPTS attribute causes the upgrade process to retry indefinitely.

Command Line (CMDLINE)

The command line attribute, CMDLINE, is used to specify the command line arguments to be passed to the agent upgrade process. As all arguments specified after the `-c` option are passed directly to the agent installer, any arguments that can be specified on the agent install command line can be specified here except for the `-mode` argument, which is automatically set by the upgrade script to perform a silent install or upgrade.

The leading text `-c` in the command line attribute named CMDLINE is required.

Note: The command line arguments following the `-c` option must be placed inside double quotes.

The `-installcomp` command line option is used to specify the specific features to be upgraded or installed on the agent computer.

Valid agent components include:

- ram- RCA Application Manager
- rim- RCA Inventory Manager
- rsm- RCA Application Self-Service Manager
- svr- RCA Applications Management Profiles (AMP) Agent
- patch- RCA Patch Manager
- rom- RCA OS Manager

For example, to upgrade or install your RCA Application Manager, the RCA Inventory Manager, and RCA Application Self-Service Manager, you would specify `"-installcomp ram,rim,rsm"`.

Note: When multiple features are specified, the RCA product acronyms must be comma separated.

The `-mgrip` and `-mgrport` command line options specify the RCA Configuration server IP address and port that the upgraded agent uses for its ZMASTER object and sample shell scripts. When you upgrade or install the RCA Application Self-Service Manager, the configuration file `args.xml` is populated with RCA Configuration server IP address and port number specified with the `-mgrip` and `-mgrport` command line options. These parameter values do not have to be the same value as the RCA Configuration server IP and port, from which the agent is receiving the upgrade service. The default value for `-mgrport` is 3464.

Note: Sample UPGRADE instances specify a CMDLINE attribute value of: `-c "-instcomp ram,rim -mgrip rcs001 -mgrport 3464"` which upgrades Application Manager and Inventory Manager agent components and pre-configures the upgraded agent to receive new applications from the RCA Configuration server named rcs001 running on port 3464. Make sure

that you update the value of the UPGRADE instance CMDLINE attribute to reflect your preferred RCA Configuration server IP address and port.

You can use symbolic substitution for the values passed by using the `-mgrip` and `-mgrport` command line arguments, when the RCA Configuration server from which the agent receives the agent upgrade Service is the same as RCA Configuration server from which you want the upgraded agent to receive future Application Services. For example, the `UPGRADE.CMDLINE` attribute can be configured to read:

```
-c "-instcomp ram,rim,rsm -mgrip &(ZMASTER.ZIPADDR) -mgrport  
&(ZMASTER.ZDSTSOCK)
```

This upgrades Application Manager, Inventory Manager, and Application Self-Service Manager on the agent receiving the service and pre-configures the upgraded agent to receive new applications from the RCA Configuration server from which it installed the Agent Upgrade Service.

It recommends minimal use of the following upgrade command line options: `-instcomp`, `-mgrip`, and `-mgrport`.

You can append the text `-loglevel 9` in the command line to set maximum logging for the agent upgrade or install. This command line option is typically used for diagnostic purposes.

You can specify a command line to use an agent install configuration file. For more information, see ["Remote Installation" on page 95](#).

If you have an installation configuration file already on the agent workstations, you can upgrade the agent using this configuration file. You can specify `-cfg<configfilename.cfg>` in the `CMDLINE` attribute, where `<configfilename.cfg>`, specifies a fully qualified path name to a configuration file.

Note: It recommends that you do not specify both, configuration file and command line options `-installcomp`, `-mgrport`, or `-mgrip` because the command line options override the values specified in the configuration file.

For example, the command line specification of `-c " -loglevel 9 -cfg /tmp/myown.cfg"` relies exclusively on the variables set in the `/tmp/myown.cfg` configuration file to determine which RCA components are to be upgrades or installed and which RCA Configuration server IP address and port to use as well as other upgrade or install options.

Task 2: Configuring the Agent Upgrade

To configure the agent upgrade:

1. In the RCA Administrator CSDB Editor, navigate to the HP supplied Application Service applicable to the target operating system for which you intend to apply the agent upgrade. For example, `SOFTWARE.ZSERVICE.HPCA_AGENT_90_UPGRADE_LINUX`. The Service instance is connected to an UPGRADE class instance that contains the configuration options relevant to the agent upgrade.
2. Go to the UPGRADE instance (`PRIMARY.SOFTWARE.UPGRADE`) for example, `HPCA_AGENT_90_UPGRADE_LINUX`.

3. In the right-hand pane, double-click **CMDLINE**. This enables you to define specific agent upgrade options and behaviors. This attribute is used to specify the agent components you want to upgrade or install as well as the preferred Configuration server IP address and port number.
4. In the Editing Instance dialog box, edit the value to include all the agent components you want to upgrade as well as the preferred RCA Configuration server IP address and port number. Valid agent components include:
 - ram- RCA Application Manager
 - rim- RCA Inventory Manager
 - rsm- RCA Application Self-Service Manager
 - svr- RCA AMP Agent
 - patch- RCA Patch Manager
 - rom- RCA OS Manager

Note: The command line arguments following the `-c` option must be placed inside double quotes. When multiple agent features are specified, the feature acronyms must be comma separated.

For example, to specify upgrades for the RCA Application Manager and the RCA Inventory Manager and also have these upgraded agent components configured to connect to a RCA Configuration server named **rcs001** running on port **3464**, type the following sample command:

```
-c "installcomp ram,rim -mgrip rcs001 -mgrport 3464"
```

5. Click **OK** and click **Yes** to confirm your changes.
6. If you want to change the values for the number of times the RCA agent attempts to install the agent upgrade as well as the time interval between attempts, change the values of the **ATTEMPTS** and **INTERVAL** attributes in the same manner. The remaining attributes should retain their default values for optimum performance.
7. Connect the OS specific sample service to the appropriate users or devices for distribution. For more information, see the *Radia Client Automation Application Manager and Application Self-Service Manager Installation and Configuration Guide*.

Note: Before connecting an upgrade service to any agent instances, make sure any users and devices that are configured to receive the agent upgrade service are not connected to self-maintenance for version before the 5.1x agents. If self-maintenance is not disconnected, and the upgrade is installed and completed, you may run the risk of back-leveling the upgraded agent by the application of agent maintenance for earlier versions of the agents on the agent's next connect to the RCA Configuration server.

To save disk space after a successful upgrade, remove the **ZSERVICE.UPGRADE** instance to uninstall the install media deployed at `$IDMSYS/ClientUpgrade`.

Note: The **ZSTOP** expressions in the sample Upgrade Application Service (**ZSERVICE**) instances as well as the supplied **UPGRADE** instances are OS-specific. These expressions

are used to ensure that the appropriate agent upgrade materials are distributed to agents that match the OS identifier contained in the expression.

Task 3: Customizing the Agent Upgrade Services

You can create your own agent upgrade Application Service (ZSERVICE instance and UPGRADE instance) to meet your enterprise requirements. It recommends that you copy one of the supplied sample instances to a new name, and ensure that the instance prefix (used to denote the target operating system) used as the source of the copy matches the intended target operating system. This is to ensure that the new instance has the necessary ZSTOP expression applicable to the operating system to which the upgrade applies. By performing the copy instance function within the UPGRADE class, the custom UPGRADE instance should already have a connection to the appropriate SOFTWARE.PACKAGE instance for the intended target operating system. You should then, connect the custom UPGRADE instance to the custom ZSERVICE instance replacing the pre-existing UPGRADE instance connection in the Application Service instance.

Ensure that agent upgrade service has connections as depicted in the figure *Model for the Agent Upgrade Service* in section "[Task 1: Importing the Classes, Instances, and Resources](#)" on page 138.

Task 4: Adding the UPGRADE Class to the Master Connection Rules

You can add new ZSERVICE/UPGRADE instances for the agent upgrade as per your enterprise requirements. You can use the RCA Admin CSDB Editor to enable the connections list for the new UPGRADE class before adding the new instances.

Complete the following steps, such that the UPGRADE class appears as a connectable class from the ZSERVICE class, and the PACKAGE class appears as a connectable class from the UPGRADE class using the Show Connections feature of the RCA Admin CSDB Editor.

To add the Upgrade class to the Master Connection Rules:

1. Use the RCA Admin CSDB Editor and go to the PRIMARY.ADMIN.ZCONNECT class.
2. Right-click **Connection Rules (ZCONNECT)** and select **Edit class**.
3. In the Editing Class window, scroll to the bottom of the class list, select the last template entry, and then click **Add After**.
4. Add a new class connection field similar to the existing connection fields.
5. Name the new connection field UPGRADE and assign it a length of 50 and a description of UPGRADE Connect List.
6. Click **OK** and **Yes**.
7. Right-click the **PRIMARY.ADMIN.ZCONNECT.MASTER_CONNECTION_RULES** instance and select **Edit Instance**.
8. For the new UPGRADE attribute, add the value `ZLIST.CONNECT_UPGRADE_TO_RULES`.

9. Right-click the **PRIMARY.ADMIN.ZLIST.CONNECT_ZSERVICE_TO_RULES** instance and select **Edit Instance**.
10. Add the value `UPGRADE` in the first empty variable slot.
11. Click **OK**.
12. To add a new instance name to the ZLIST class, right-click **Name Lists (8) (ZLIST)** and select **New Instance**.
13. Name the new instance `CONNECT_UPGRADE_TO_RULES`.
14. Right-click the new instance and select **Edit Instance**.
15. Add the value `PACKAGE` to the first empty variable entry.
16. Click **OK**.

Agent Upgrade Process when applied as an RCA Service

After a user or device's policy entitlement model is configured to include the agent upgrade decks, and the agent connects and receives one of the mandatory application services (for example, `HPCA_AGENT_90_UPGRADE_LINUX`) containing the agent upgrade materials, RCA downloads all of the necessary materials to perform a agent upgrade.

The default location of the upgrade media, when downloaded using an agent connect is `&(ZMASTER.ZSYSDIR)/ClientUpgrade` (the location, as defined in `UPGRADE.MEDIADIR` attribute) in the device's entitlement model. The installation of the Upgrade Service runs a method named "install_upgrade" (with additional command line parameters) which waits for agent processes to finish before upgrading the agent binaries. The `install_upgrade` method exits with a return code of 1, which results in a 709 radconct return code. This behavior tells the agent that the upgrade is not complete. For reporting purposes, an `APPEVENT` is sent that identifies the `ZSERVICE` with an `ERRORNUM` of 324 and `STATUS` of "Install/Upgrade is not complete." Depending on the level of radconct, `install_upgrade` may have to do a second connect to verify the upgrade status. The `install_upgrade` and upgrade logs can be found at `$IDMLOG` folder for troubleshooting purposes.

When the agent processes are complete, the actual agent upgrade begins. The upgrade process stops the agent daemons (`radsched` and `radexecd`) if they are running and upgrades the agent components specified by the `-installcomp` parameter of the `UPGRADE` class instance or the `SelectComponent` section of the specified configuration file. After upgrading, the agent process restarts the agent daemons that were running when the upgrade was initiated.

To save disk space after a successful upgrade, remove the `ZSERVICE.UPGRADE` instance to uninstall the media deployed at `$IDMSYS/ClientUpgrade`.

Upgrading Using Installation Media

To upgrade the Agent using the local upgrade method:

1. Logon to the Linux or Macintosh workstation as root.

2. Navigate to `/Setup-Core/Media/client/default/<platform>` folder on the installation media, where `<platform>` is the operating system on which you are performing the agent upgrade.

3. Open the command prompt and run the following command:

```
./upgrade -c "-installcomp <PARMS>-mgrip<IP>-mgrport<PORT>"
```

where:

- `<PARMS>` is either a single argument or a comma separated list of agent components that you want to upgrade.
Valid agent components include:
 - ram- RCA Application Manager
 - rim- RCA Inventory Manager
 - rsm- RCA Application Self-Service Manager
 - svr- RCA AMP Agent
 - patch- RCA Patch Manager
 - rom- RCA OS Manager
- `<IP>` is the IP address of the RCA Configuration server from which you want the upgraded agent to receive new applications.
- `<PORT>` is the port number on which the RCA Configuration server is running.

The upgrade command line is used to specify the command line arguments to be passed to the agent upgrade process. All arguments specified after the `-c` option are passed directly to the agent installer, therefore, any arguments that can be specified on the agent install command line can be specified here except for the `-mode` argument, which is automatically set by the upgrade script to perform a silent install or upgrade.

Note: The command line arguments following the `-c` option must be placed inside double quotes.

The `-installcomp` command line option is used to specify the specific products to be upgraded or installed on the agent workstation. For example, to upgrade your Application Manager and also install the Inventory Manager and Application Self-Service Manager, you would specify "`-installcomp ram,rim,rsm`".

Note: When multiple features are specified in the command line arguments the product acronyms must be comma separated.

The `-mgrip` and `-mgrport` command line options specify the RCA Configuration server IP address and port that the upgraded agent will use for its ZMASTER object and sample shell scripts. If you upgrade or install the Application Self-Service Manager, its configuration file, `args.xml` is populated with RCA Configuration server IP address and port number specified with the `-mgrip` and `-mgrport` command line options. The default value for `-mgrport` is **3464**.

You can specify `-loglevel 9` in the command line to set maximum logging for the agent upgrade/install.

Upgrading using an Existing Configuration File

You can use the installation configuration file created by the Remote Installation Setup process of the agent installer to perform an agent upgrade.

To upgrade the agent using an installation configuration file:

1. Create a configuration file by running the agent installation. For instructions on running a remote installation setup, see the ["Remote Installation" on page 95](#).
2. Log on to the workstation as root.
3. Open the command prompt.
4. Navigate to `/Setup-Core/Media/client/default/<platform>` folder on the installation media, where `<platform>` denotes the operating system on which you are performing the RCA agent upgrade.
5. Run the following:

```
./upgrade -c "-cfg configfilename.cfg"
```

The *configfilename.cfg* specifies a fully qualified path name to an install configuration file that contains the components selection and desired configuration options.

For information about installer configuration files (created by the Remote Installation Setup process of the agent installer), see *Radia Client Automation Application Manager and Application Self-Service Manager Installation and Configuration Guide* and *Radia Client Automation Inventory Manager Reference Guide*.

Note: HP recommends that you do not specify both configuration file and command line options `-installcomp`, `-mgrport`, or `-mgrip` because the command line options override the values specified in the configuration file.

For example, the command line of `-c " -loglevel 9 -cfg /tmp/myown.cfg"` would rely exclusively on the variables set in the `/tmp/myown.cfg` configuration file to determine what RCA components to upgrade or install and what RCA Configuration server IP and port to use as well as other upgrade or install options.

Upgrading RCA Administrator Tools

Caution: The RCA Agent upgrade removes a previous version of the RCA Administrator tools if one is installed on the device.

The RCA Administrator tools are automatically installed during the RCA Core server version 9.00 installation. If existing RCA Administrator tools are present during the RCA Core server installation, they are updated during the installation process.

You can upgrade to the latest version of the RCA Administrator tools in the following two ways:

- Using the installation files:
 - a. Remove the existing version of the RCA Administrator tools installed on the computer to upgrade the RCA Administrator tools on a computer other than the Core server.
 - b. Use the RCA Administrator tools installation files for Windows, Linux, and Macintosh operating systems to upgrade the RCA Administrator tools.

- **For Windows:** Run `setup.exe`, the RCA Administrator tools installation command located in the `\Setup-Core\Media\admin\default\win32` directory on the RCA installation media.
- **For Linux:** Remove the existing RCA Administrator tools and run the `./install` command from the `\Setup-Core\Media\admin\default\linux` directory.
- **For Macintosh:** Remove the existing RCA Administrator tools and run the `sudo ./install` command from the `\Setup-Core\Media\admin\default\macx86` directory.
- Using the `HPCA_ADMINTOOLS` service:
Deploy the `HPCA_ADMINTOOLS` service in `SOFTWARE` domain to the managed device from the RCA Core Console.

Caution: If you are migrating from a version before 7.90, do not deploy the legacy `CCM_PUBLISHER` service in a 9.00 environment. This service can be deleted from the CSDB as it is no longer required.

Upgrading the RCA SQL/Oracle Database Manually

This step is not required when upgrading from version 7.80, 7.90, or 8.10. It is required when upgrading from version 7.50. If you already have a `FOREIGN KEY CONSTRAINT` set to the `DEVICECONFIG.DEVICE_ID` column on Inventory database tables, you can skip this step.

Instead of using the `sqlmigrate.cmd` script, you can upgrade the RCA SQL database manually after restoring your data.

Caution: This process should be performed only by an experienced database administrator.

The database tables listed in "[SQL Database Tables that must be Upgraded](#)" on next page have schema changes that require the tables to be re-created to generate the correct primary and foreign keys. Data from these tables should be exported and stored in temporary tables before beginning the manual upgrade process.

To upgrade the RCA SQL database manually:

1. On the computer hosting the RCA Core server, stop the RCA Core service.
2. Export (or store in temporary tables) the data in the tables listed in "[SQL Database Tables that must be Upgraded](#)" on next page.
3. Drop all the tables listed in the next section.

Caution: Ensure that you drop the tables in the same order as listed in the next section.

4. Restart the RCA Messaging Server service (to re-create the table schema).

5. Re-import your data into the tables.

Caution: Ensure that you import the tables in the reverse order as listed in the next section.

During the import process, data that violates database integrity is not imported. Make sure that you review the data to determine if it is still valid and required.

6. Start the RCA Core service.

SQL Database Tables that must be Upgraded

The following tables have had schema changes that require the tables to be re-created to generate the correct primary and foreign keys for RCA version 9.00. This process is performed automatically by the `sqlmigrate.cmd` script.

```
rWin32_WinSAT
rWin32_VideoController
rWin32_UserAccount
rWin32_USBController
rWin32_TimeZone
rWin32_SystemEnclosure
rWin32_SystemDriver
rWin32_StartupCommand
rWin32_SoundDevice
rWin32_SoftwareFeature
rWin32_SoftwareElement
rWin32_Share
rWin32_Service
rWin32_SerialPort
rwin32_quickfixengineering
rWin32_Product
rWin32_Processor
rWin32_Process
rWin32_Printer
rWin32_PortResource
rwin32_portablebattery
rWin32_PointingDevice
```

rWin32_PnPEntity
rWin32_PhysicalMemory
rWin32_ParallelPort
rWin32_PageFileUsage
rWin32_PageFileSetting
rWin32_PageFile
rWin32_OperatingSystem
rWin32_NetworkLoginProfile
rWin32_NetworkConnection
rWin32_NetworkAdapterConf
rWin32_NetworkAdapter
rWin32_MotherboardDevice
rWin32_MemoryDevice
rWin32_MemoryArray
rWin32_LogicalProgramGroup
rWin32_LogicalMemoryConf
rWin32_LogicalDisk
rWin32_LoadOrderGroup
rWin32_Keyboard
rWin32_IRQResource
rWin32_IDEController
rWin32_Group
rWin32_FloppyDrive
rWin32_FloppyController
rWin32_Environment
rWin32_DMAChannel
rWin32_DisplayControllerConf
rWin32_DisplayConf
rWin32_DiskPartition
rWin32_DiskDrive
rWin32_DeviceMemoryAddress
rWin32_DesktopMonitor
rWin32_Desktop

rWin32_ComputerSystemProduct
rWin32_ComputerSystem
rWin32_CDROMDrive
rWin32_CacheMemory
rWin32_Bus
rWin32_BootConf
rWin32_BIOS
rwin32_baseboard
rWiFi_NetworkAdapter
rRegistry
rNVD_WBEMStatus
rNVD_UserAccount
rNVD_SolarisPatch
rNVD_Product
rNVD_PDASystem
rNVD_NISUserAccount
rNVD_NISGroupAccount
rNVD_MulticastStatistics
rNVD_INSTALLED_UNINSTALL
rNVD_INSTALLED_APPS
rNVD_GroupMember
rNVD_GroupAccount
rNVD_DownloadStatistics
rMSSD_FailurePredictStatus
rMSSD_AttributeData
rhp_biosstring
rhp_biossensor
rhp_biospassword
rhp_biosorderedlist
rhp_biosinteger
rhp_biosevent
rhp_biosenumeration
rCIM_UnixOperatingSystem

rCIM_UnixLocalFileSystem
rCIM_UnixComputerSystem
rCIM_StorageVolume
rCIM_SoftwareFeatureElements
rCIM_SoftwareFeature
rCIM_SoftwareElement
rCIM_Service
rCIM_SCSIInterface
rCIM_SCSIController
rCIM_ResidesOnExtent
rCIM_ProductSoftwareFeatures
rCIM_Product
rCIM_Processor
rCIM_Process
rCIM_ParallelController
rCIM_OperatingSystem
rCIM_NFS
rCIM_MediaPresent
rCIM_LogicalDiskBasedOnVolume
rCIM_LogicalDisk
rCIM_IDEController
rCIM_HPUX_SwBundles
rCIM_Export
rCIM_EthernetAdapter
rCIM_DVDDrive
rCIM_DiskDrive
rCIM_Directory
rCIM_ComputerSystem
rCIM_CDROMDrive
DeviceUserGroup
SMBiosInfo
Query
DeviceNotify

FileAudit
DeviceZRStates
DeviceZRState
DeviceSynopsis
HDeviceStatus
DeviceStatus
HDeviceState
DeviceState
DeviceServices
DeviceMap
HDeviceErrors
DeviceErrors
Audit_Type
Audit_Attrs
Audit_Event
Audit_Cat
Audit_AttrNames
HAppEvent
AppEvent
HAppRNPEvent
AppRNPEvent
HAppMSIEvent
AppMSIEvent
JOBTASK
HJOBSTAT
JOBSTAT
JOBPARM
ADInfo
HDeviceConfig
DeviceConfig

Chapter 10

Troubleshooting

This section covers troubleshooting tips for the issues that you may face during or after RCA installation and upgrade.

Upgrade Issues

Problem	Solution
<p>The following error message appears during restore.</p> <pre>"LDIF export failed. bdb_db_open: unclean shutdown detected; attempting recovery. Recovery skipped in read-only mode"</pre>	<p>To resolve the error, perform the following steps:</p> <ol style="list-style-type: none">1. Stop the RCA Core service.2. Open the command prompt.3. Navigate to the <code>HPCABackup/rmp/openldap</code> directory where you have taken the backup.4. Run the following command. <code>slapd -h ldap://localhost:3474 -f slapd.conf -d 256</code> <p>Sample output of the above command:</p> <pre>@(#) \$OpenLDAP: slapd 2.4.23 (Jul 25 2010 18:24:14) \$ @RIVER:/home/matth/sol_R_2_4_23/build/openldap.NT_i686/servers/slapd bdb_db_open: database "cn=foobar,cn=hpca": unclean shutdown detected; attempting recovery. slapd starting</pre> <ol style="list-style-type: none">5. Type CTRL + C to terminate the command prompt.6. Restart the RCA Core service.7. Run the restore operation again.
<p>The following error message appears during database migration for ORACLE database.</p> <pre>MIG: SQL migrate script Error processing INSERT INTO DEVICECONFIG [Oracle][ODBC][Ora]ORA- 00001: unique constraint (CMDATAMIG78.SYS_ C0019388) violated</pre>	<p>Ignore the error message as it does not affect the ORACLE database migration process. The error message appears because the unique constraint of some of the tables in the latest version of RCA are different from that of the previous versions.</p>

Problem	Solution
After the satellite upgrade process, it is needed for a customized configuration to have the resources as well, but these are again synced from the Core server.	If you have a customized set-up that uses resources from the CSDB on the Satellite server, make sure that the dataless parameter value is set to 0 in the dmabatch.rc file on the Satellite server. Doing this, the backup and restore procedure automatically takes backup of the Satellite resources and restore them after upgrading the Satellite server.

Appendix A

Planning RCA Deployment

In an RCA environment, the unavailability of the Core server is the only single point of failure, which can disrupt the functioning of configuration services and data services.

This appendix provides information on how you can configure your environment, such that there is no single point of failure, and the features are available when the Core server is down.

Before setting up your environment, consider the following options:

- Preload the Satellite server: Configure the Satellite servers for preload. The external policy for software and patches is available if the content is preloaded to the Satellite server. For more information on how to preload the Satellite server, see the *Radia Client Automation Enterprise User Guide*.
- Distribute data messages load: Configure the tier-1 full-service Satellite server for directly posting the agent messages to the RDBMS, instead of forwarding the messages to the Core server. This configuration though reduces the load and the overall dependency on the Core server, it however, adds an additional load on the Satellite servers to direct the data to the RDBMS. To overcome the issue of additional load on Satellite servers, you can separate the messaging role and agent resolution role for the higher tier Satellite servers. For more information on how to setup your environment for distributing the messages load and dependency on the Core server, see the sections "[Distributing Messaging Load](#)" on next page and "[Separating Roles Among Satellites](#)" below.

Separating Roles Among Satellites

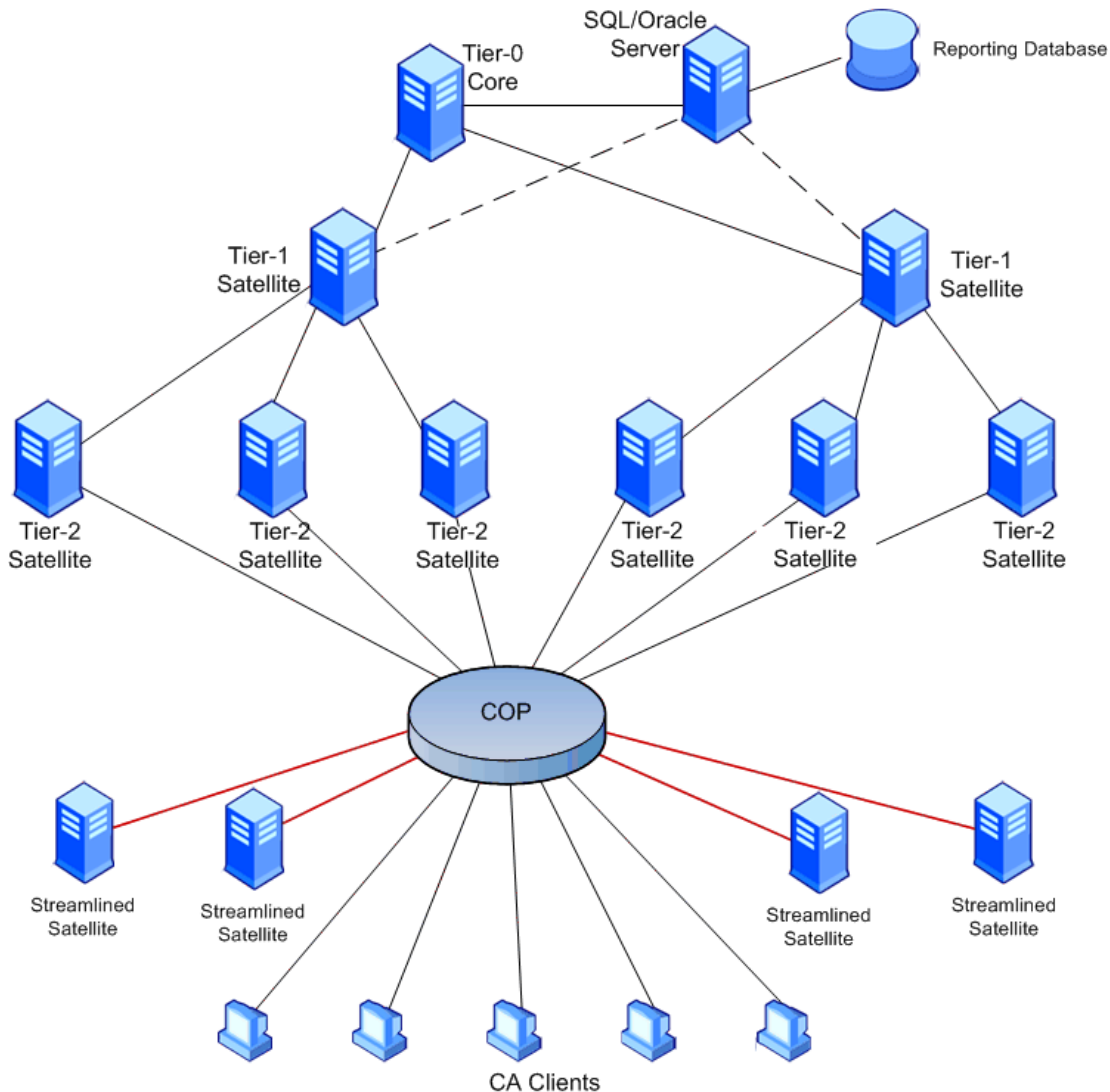
You can improve performance for data messaging and resolution services by separating the roles among higher tier Satellite servers. You can configure Satellite servers, such that the functions performed by the Core server and tier-1 Satellite servers in the default configuration are separated into two roles:

- A Satellite role dedicated to data posting functions.
- A Satellite role dedicated to client resolution services.

Tier-1 Satellite servers can be configured to post data and tier-2 Satellite server can be configured to handle client requests.

The following diagrams illustrate this configuration from the roles perspective:

Separating Roles Among Satellites



The Core server at tier-0 performs administrative functions and is not directly involved in client resolution or message handling. This server uses the default Messaging server configuration.

The group of Satellite servers at tier-1 are dedicated to synchronize data and post messages to the relational database. The tier-1 Satellite servers do not service client requests directly, however, these servers serve as upstream hosts for tier-2 Satellite servers. This configuration reduces the load on the tier-2 Satellite servers responsible for client resolution services. The load is distributed evenly across tier-1 Satellite servers that reduces the backlog of message queues. The data synchronization for the Satellite servers should be performed in a phased manner, such that a few Satellite servers are available at all times.

Distributing Messaging Load

To reduce the dependency on the Core server and to provide better load distribution for messaging traffic without increasing the server count, configure the full-service Satellite servers to directly post data to the RDBMS. You can configure tier-1 Satellite servers to post client messaging data directly to the reporting database. This reduces the load from the Core server, which can now primarily

focus on the administrative tasks. The tier-0 Core server uses default Messaging server configuration.

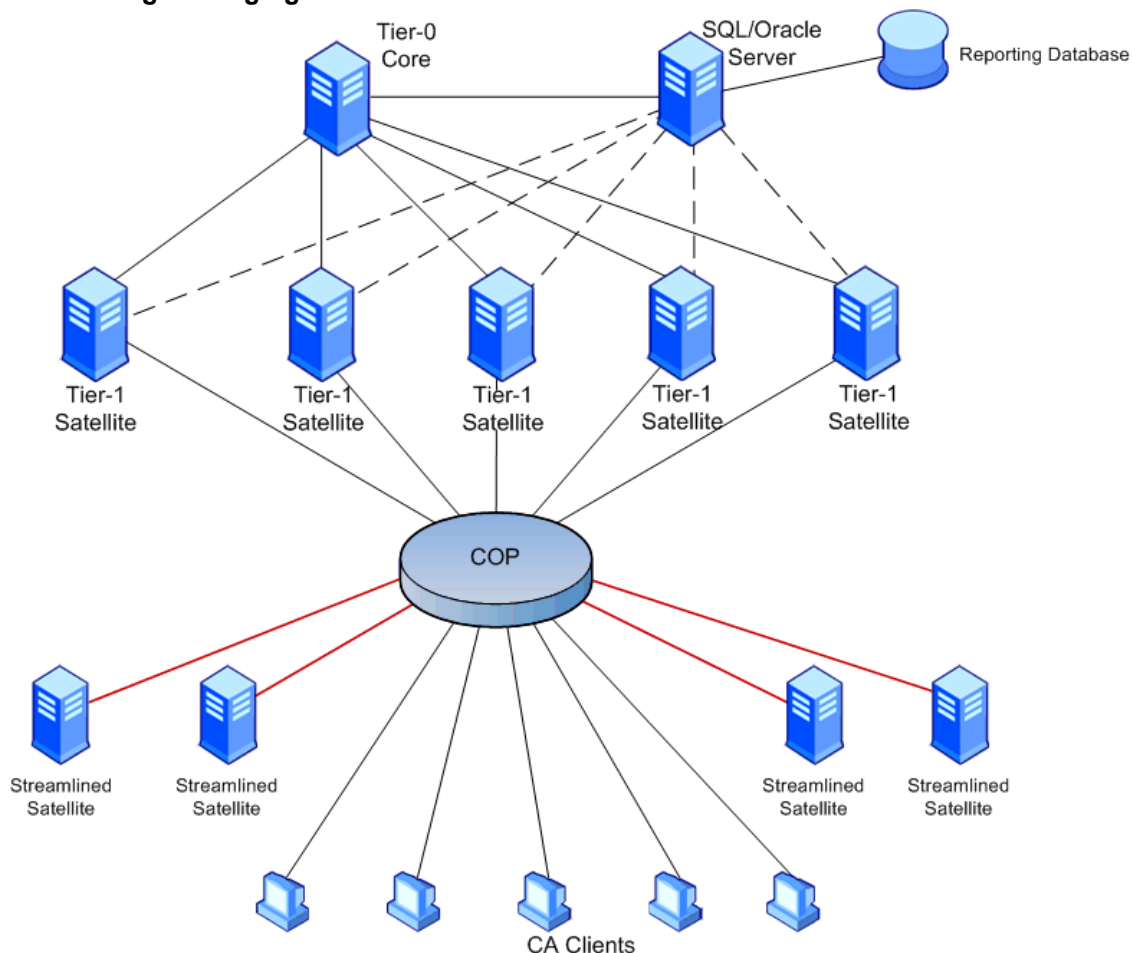
For more information on how to configure a Satellite server for directly posting the data to RDBMS, see the *Radia Client Automation Enterprise User Guide*.

The primary benefit of this configuration model is to distribute the ODBC posting loads across multiple servers. This reduces the possibility of severe bottlenecks in the reporting data queues, especially if the Core server is either removed from service or experiences an outage.

You can extend the architecture by including remote full-service Satellite servers that should not post messaging data directly to the RDBMS. These servers use the default Messaging server configuration and forward their data to a tier-1 Satellite server for posting. The tier-2 Satellite servers also synchronize metadata and resources from the same upstream tier-1 host.

The following diagram illustrates the configuration from the messaging perspective:

Distributing Messaging Load



The additional load on tier-1 can be addressed by appropriately scaling to the required number of servers based on the volume of management activity being performed on a routine or worst case basis. You can also separate the roles among Satellite servers to reduce the load on tier-1, as explained in the section ["Separating Roles Among Satellites"](#) on page 157.

In this scenario, the Client Operations Profile (COP) is configured for optimal distribution of client loads for resolution services and fail-over. You can define all tier-1 servers at equal priority using a wild-card naming strategy.

It recommends that you perform data synchronization for the Satellite servers in a phased manner, such that a few Satellite servers are available at all times.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click [here](#).

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to radiadocfeedback@persistent.co.in.

Product name and version: Radia Client Automation Enterprise, 9.00

Document title: Installation and Upgrade Guide

Feedback:

